
IVEX Logger Series

Viewer 管理者マニュアル

日本ナレッジ株式会社

-
- 本マニュアルの記載内容を一部または全部を無断で転写することを禁じます。
 - 本マニュアルの記載内容は将来予告なく変更されることがあります。
 - 本マニュアル及び、装置に記載されている各会社名、各製品名、各サービス名は、各社の商標または登録商標です。

目的

このマニュアルは、IVEX Logger Viewer の管理者マニュアルです。IVEX Logger Viewer を管理するための情報が記載されており、システム管理者として IVEX Logger Viewer の設定変更・管理を適切に行うことができること、システム管理者としてログの管理を適切に行うことができることを目的としております。

対象読者

本文書は主に IVEX Logger Viewer をシステム管理者として運用される方を対象にしております。主な対象読者は次の通りです。

- IVEX Logger Viewer を使用したシステムを導入される方
- IVEX Logger Viewer を使用してログ監視を行う方
- 製品の評価者として IVEX Logger Viewer をインストールし、評価される方

表記規則

マニュアルの表記規則は以下の通りです。

表 1 表記規則

表記	説明
太字(ボールド)	マニュアルの参照先を表す。(見出し、図表番号は除く)
斜体 (イタリック)	環境変数を表す。
等幅ゴシック体(タイプライタゴシック)	コマンドラインや実行例などユーザの入力・実行結果を表す。
赤字下線	製品の仕様やプラットフォームに関する注意事項を表す。
文頭の文字「#」	その文がコマンドラインでの入力コマンド、又はスクリプト内のコメント文であることを示す。
文末の文字「」	その文がコマンドラインでの入力コマンドの場合は[Enter キーの入力]を示し、スクリプト内の入力文字列の場合は[改行]であることを示す。

IVEX Logger Viewer 管理者マニュアル

目次

目次.....	2
第一部. IVEX Logger Viewer のシステム設定を行う.....	9
1. IVEX Logger Viewer を起動する.....	10
1.1. コンソールサーバを操作する.....	10
1.1.1. コンソールサーバを Windows サービスから起動する.....	10
1.1.2. コンソールサーバの起動を確認する.....	12
1.1.3. コンソールサーバを再起動する.....	13
1.1.4. コンソールサーバのバージョンを確認する.....	14
1.2. Windows 環境の LogGate を操作する.....	15
1.2.1. LogGate を Windows サービスから起動する.....	15
1.2.2. LogGate の起動を確認する.....	17
1.2.3. LogGate を再起動する.....	18
1.2.4. LogGate のバージョンを確認する.....	19
1.3. ログデータの検索可能状態を確認する.....	20
2. IVEX Logger Viewer を停止する.....	21
2.1. LogGate を操作する.....	21
2.1.1. LogGate を Windows サービスから停止する.....	21
2.1.2. LogGate の停止を確認する.....	22
2.2. コンソールサーバを操作する.....	23
2.2.1. コンソールサーバを Windows サービスから停止する.....	23
2.2.2. コンソールサーバの停止を確認する.....	23
2.3. コンソールサーバの停止可能状態を確認する.....	24
2.4. LogGate の停止可能状態を確認する.....	24
2.5. LogGate プロセス停止時のログデータの扱い.....	25
3. 通信の設定を行う.....	26
3.1. コンソールサーバの Web コンソールアクセスポートを設定する.....	26
3.2. FTP 関連ポートを設定する.....	27
3.3. LogGate 通信用ポートを設定する.....	30
3.4. コンソールサーバシャットダウン用ポートを設定する.....	31
3.5. LogGate のバインド IP アドレスを設定する.....	32
3.5.1. レシーバのバインド先を設定する.....	32
3.5.2. コンソールサーバとの接続ソケットのバインド先を設定する.....	34

3.6. コンソールサーバのバインド IP アドレスを確認する	35
3.7. セッションタイムアウトを設定する	36
3.8. コンソールサーバの HTTPS 通信を設定する.....	37
3.9. FTP レシーバの FTPS 通信を設定する.....	42
3.10. 内部データベースを設定する.....	47
3.10.1. 内部データベースの接続数を設定する.....	47
3.10.2. 内部データベースの再接続間隔を設定する.....	48
3.10.3. 内部データベースの接続先を設定する.....	49
4. レシーバを設定する.....	50
4.1. シーケンシャルログ出力ディレクトリを変更する.....	50
4.2. FTP レシーバを設定する.....	52
4.3. 収集ログ保存先を変更する	54
5. メモリ設定を行う	59
5.1. メモリ設定を行う	59
5.1.1. LogGate のメモリ設定を行う.....	59
5.1.2. コンソールサーバのメモリ設定を行う.....	60
6. グループ/ユーザを管理する.....	61
6.1. グループを作成する.....	61
6.2. グループを削除する.....	69
6.3. ユーザを作成する	72
6.4. ユーザを削除する	80
6.5. ユーザパスワードを変更する.....	82
6.5.1. 管理者によるパスワード変更.....	82
6.5.2. ユーザ自身によるパスワード変更.....	85
6.5.3. パスワード有効期限が切れた後のパスワード変更	87
6.6. 管理者グループの所属ユーザを変更する	89
6.7. ユーザをロックする、ロック解除する	94
6.7.1. ユーザをロックする.....	94
6.7.2. ユーザをロック解除する.....	100
7. ログソースを設定する	106
7.1. ログソース設定変更時の注意事項.....	106
7.1.1. ログソースを新規追加した場合(大規模対応時)	106
7.1.2. ログソースを削除した場合	106
7.1.3. ログソースを変更した場合	106
8. その他システム設定を行う.....	107
8.1. コンソールサーバ/LogGate が使用するメールサーバを設定する.....	107
8.2. 検索時に1回で取り出すログ量を設定する.....	111
8.3. 集計結果の表示とグラフ保存先を設定する	113

8.4. 検知の履歴削除スケジュールを設定する	115
8.5. レポートの添付サイズとレポート保存先を設定する	117
8.6. レポートの出力ファイル名を設定する	120
8.7. ユーザ認証を設定する	122
8.8. 条件の所有者を変更する	126
8.9. ログ出力の設定を行う	128
8.9.1. コンソールシステムログの出力設定を行う	128
8.9.2. LogGate システムログの出力設定を行う	134
8.9.3. 監査ログの出力設定を行う	139
8.10. LogGate 設定情報をダウンロードする	143
8.11. LogGate 設定情報をアップロードする	144
8.12. レポートを共有する	147
9. LogGate グループの設定を行う	149
9.1. LogGate の IP アドレスを変更する(全エディション)	149
9.2. LogGate の検索アルゴリズムを変更する(アドバンスド版のみ)	152
10. インポート・エクスポートを実行する	155
10.1. 各種条件や設定情報をインポートする(管理画面)	156
10.2. 各種条件や設定情報をエクスポートする(管理画面)	163
第二部. ログデータを管理する	171
11. ログデータの改竄チェックを行う	172
11.1. ログデータの改竄チェック機能	172
11.2. 改竄チェック機能を無効にする	173
11.3. ログデータの改竄チェックをする	176
12. ログデータを暗号化する	177
12.1. ログデータの暗号化機能	177
12.2. ログデータの暗号化を有効にする	179
13. ログデータをアーカイブする	182
13.1. ログデータのアーカイブ機能	182
13.2. 古い LogDB をアーカイブする	183
13.3. バックアップ目的で LogDB をアーカイブする	184
13.4. アーカイブした LogDB を削除する	185
13.5. アーカイブ時に残した LogDB を削除する	186
13.6. アーカイブコマンド停止時のログデータの扱い	187
14. ログデータをリストアする	188
14.1. ログデータのリストア機能	188
14.2. 古い LogDB をリストアする	189
14.3. システム復旧でアーカイブした LogDB をリストアする	190
14.4. リストアした LogDB を削除する	191

15. ログデータをエクスポートする	192
15.1. ログデータのエクスポート機能	192
15.2. 収集ログ保存先から IVEX Logger Viewer 形式のログデータをエクスポートする	193
15.3. LogDB から IVEX Logger Viewer 形式のログデータを分割してエクスポートする	194
15.4. スナップショットした LogDS から IVEX Logger Viewer 形式のログデータにエクスポートする	195
15.5. エクスポートした IVEX Logger Viewer 形式のログデータを削除する	196
15.6. IVEX Logger Viewer 形式のログ	197
16. LogDB を再作成する	199
16.1. ログデータ(LogDB)の再作成機能	199
16.2. 旧ログフォーマット定義で適用された LogDB を再作成する	202
16.3. LogDB 再作成コマンド停止時のログデータの扱い	208
16.4. LogDB 再作成が必要な場合	209
16.4.1. ログフォーマット定義の変更	209
16.4.2. 共有パラメータ化	210
16.4.3. LogDS 構成ファイル数削減	211
第三部. IVEX Logger Viewer を運用する	212
17. ディスクをチェックする	213
17.1. 収集ログ保存先の使用量をチェックする	213
17.2. IVEX Logger Viewer 関連ディレクトリの容量をチェックする	215
18. プロセスを監視する	216
18.1. LogGate のプロセスを監視する	216
18.2. コンソールサーバのプロセスを監視する	217
19. IVEX Logger Viewer のログをチェックする	218
19.1. 検知ログをチェックする	218
19.2. メモリログをチェックする	218
19.3. ログの受信ログをチェックする	219
19.4. illegal.log について	219
19.4.1. 形式不正	219
19.4.2. 一行のログサイズ超過	220
20. IVEX Logger Viewer 関連データのバックアップを行う	221
20.1. IVEX Logger Viewer の環境障害概要	221
20.2. IVEX Logger Viewer 関連データのバックアップ対象	222
20.3. バックアップを行う際の注意事項	223
21. LogDS・ワーク・シーケンシャルログをバックアップする	224
21.1. 収集処理のデータフロー	224
21.2. ワーク・シーケンシャルログをバックアップする	227
21.3. LogDS をバックアップする	229
21.3.1. スナップショットコマンド	229

目次

21.3.2. バックアップツール	231
21.4. バックアップソフトで収集ログ保存先をバックアップする	232
22. バックアップデータから IVEX Logger Viewer のシステムを復旧する	233
付録 A. 設定ファイル一覧	235
A.1. コンソールサーバ設定ファイル	237
A.2. LogGate 設定ファイル	237
A.3. Web サーバ設定ファイル	237
A.4. システムログ出力設定ファイル(コンソールサーバ)	237
A.5. システムログ出力設定ファイル(LogGate)	237
A.6. コンソールサーバ管理コマンド用ログ設定ファイル	237
A.7. LogGate 管理コマンド用ログ設定ファイル	237
A.8. LogDS 管理コマンド用ログ設定ファイル	237
A.9. 診断コマンド用ログ設定ファイル	238
A.10. セキュリティ設定ファイル	238
A.11. ライセンス・キー	238
A.12. FTP サーバ設定ファイル	238
A.13. FTP 設定ディレクトリ	238
A.14. FTP ユーザ設定ファイル	238
A.15. レポートディレクトリ	239
A.16. ブラウザ接続設定ファイル	239
A.17. ログ保存領域設定ファイル	239
A.18. 改竄検出機能用キースタ	239
A.19. RMI 設定ファイル	239
付録 B. ディレクトリー一覧	240
B.1. ホームディレクトリ	241
B.2. 収集ログ保存先	242
B.3. LogGate ワーク先	242
B.4. シーケンシャルログ出力先	242
B.5. システムログ出力先	243
B.6. 収集ログアーカイブ先	243
B.7. レポート保存先	244
B.8. グラフ集計時のワーク	244
B.9. 収集ログスナップショット先	244
B.10. 収集ログエクスポート先	244
付録 C. IVEX Logger Viewer 監査ログ一覧	245
C.1. <システム関連 メッセージ種別:COMMON>	246
C.2. <設定関連 メッセージ種別:SETUP>	247
C.3. <ユーザ関連 メッセージ種別:GROUP>	254

C.4. <ユーザ関連 メッセージ種別:USER>	255
C.5. <ログフォーマット定義 メッセージ種別:FORMAT>	256
C.6. <ログフォーマット定義 メッセージ種別:TAG>	258
C.7. <検索 メッセージ種別:SEARCH>	259
C.8. <集計 メッセージ種別:STATS>	260
C.9. <検知 メッセージ種別:SENSOR>	260
C.10. <レポート メッセージ種別:REPORT>	262
C.11. <共通メッセージ>	264
C.12. <設定 GUI(LogGate 設定)>	266
付録 D. IVEX Logger Viewer を再起動する操作	267
D.1. コンソールサーバを再起動する操作	267
D.2. LogGate を再起動する操作	267
付録 E. コマンドリファレンス	268
E.1. LogGate 管理コマンド	268
E.2. LogDS 管理コマンド	269
E.3. コンソールサーバ管理コマンド	270
E.4. アーカイブコマンド	271
E.5. リストアコマンド	273
E.6. LogDB 削除コマンド	274
E.7. スナップショットコマンド	276
E.8. LogGate 起動コマンド	277
E.9. LogGate 停止コマンド	278
E.10. レシーバ再起動コマンド	279
E.11. LogDB 再作成コマンド	280
E.12. 取り込み停止コマンド	282
E.13. 取り込み開始コマンド	284
E.14. 収集一時停止コマンド	285
E.15. 収集一時停止解除コマンド	286
E.16. 元ログエクスポートコマンド	287
E.17. LogGate 状態表示コマンド	289
E.18. LogDS 状態表示コマンド	292
E.19. LogGate バージョンコマンド	297
E.20. 改竄チェックコマンド	298
E.21. LogDS 管理中断コマンド	301
E.22. 過去ログデータのインデックス作成コマンド	303
E.23. 過去ログデータの改竄チェックコマンド	305
E.24. 過去ログデータの暗号化コマンド	306
E.25. IVEX Logger Viewer ユーザ/グループ管理コマンド	307

E.26. IVEX Logger Viewer ユーザー一覧表示コマンド.....	308
E.27. IVEX Logger Viewer ユーザ登録コマンド.....	309
E.28. IVEX Logger Viewer ユーザ削除コマンド.....	310
E.29. IVEX Logger Viewer ユーザロック解除コマンド.....	311
E.30. IVEX Logger Viewer グループ一覧表示コマンド.....	312
E.31. IVEX Logger Viewer グループ登録コマンド.....	313
E.32. IVEX Logger Viewer グループ削除コマンド.....	314
E.33. 条件・設定インポート・エクスポートコマンド.....	315
E.34. 条件・設定インポートコマンド.....	316
E.35. 条件・設定エクスポートコマンド.....	319
E.36. レポート管理コマンド.....	322
E.37. レポート作成条件一覧表示コマンド.....	323
E.38. レポート作成履歴一覧表示コマンド.....	324
E.39. レポート実行コマンド.....	325
E.40. レポート中断コマンド.....	326
E.41. 内部データベースバックアップコマンド.....	327
E.42. 内部データベースリストアコマンド.....	328
E.43. ログフォーマット定義 ID 表示コマンド.....	329
E.44. 診断コマンド(情報収集コマンド).....	330
E.45. 診断コマンド(LogDS ビューアコマンド).....	332
付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧.....	333
付録 G. FTP レスポンスコード.....	351
付録 H. 外部レポートエンジン仕様.....	353
H.1. レポートエンジンからの呼び出し書式.....	353
H.2. 終了コード.....	354
H.3. 外部レポートエンジンの内部仕様.....	355
H.4. レポートエンジンが出力する XML ファイルの仕様.....	355
付録 I. IVEX Logger Viewer が出力するログファイル一覧.....	356

第一部. IVEX Logger Viewer のシステム設定を行う

第一部では、IVEX Logger Viewer のシステム設定方法について説明します。

1. IVEX Logger Viewer を起動する

1. IVEX Logger Viewer を起動する

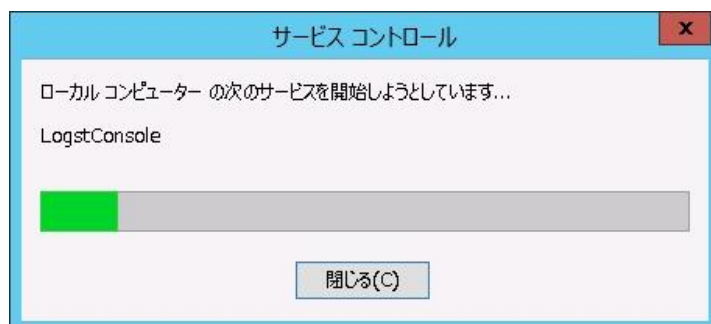
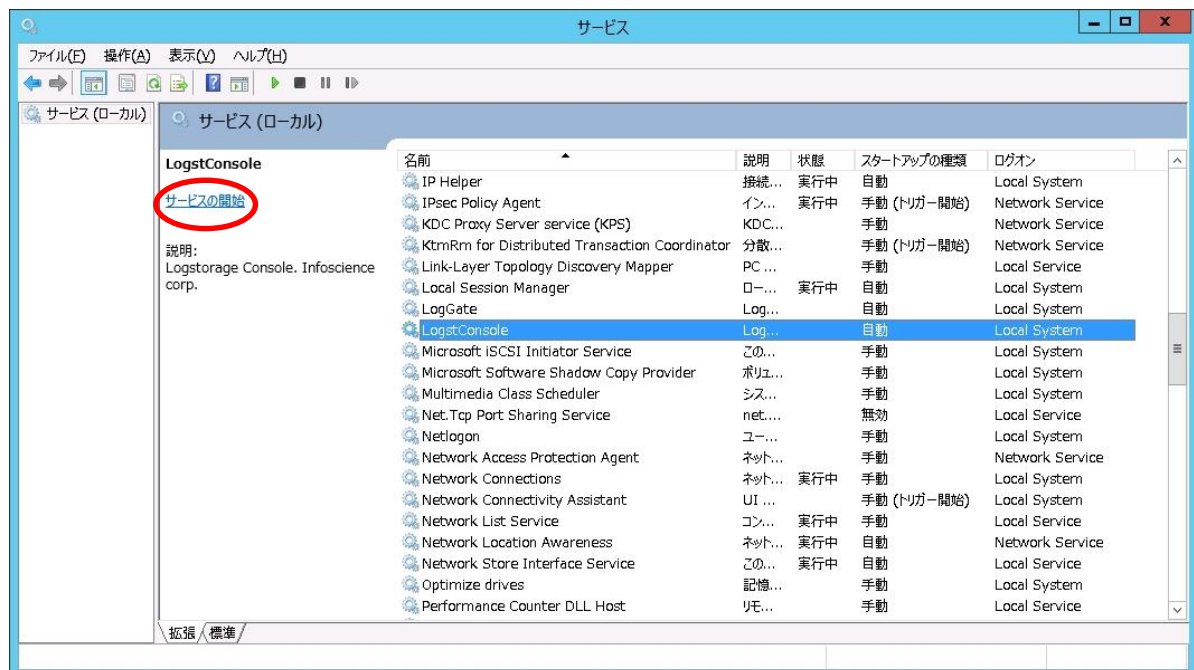
1.1. コンソールサーバを操作する

コンソールサーバの起動方法について説明をします。Windows 環境ではサービスから起動を行う方法とコマンドから起動を行う方法の 2 種類あり、それぞれについて説明します。

1.1.1. コンソールサーバを Windows サービスから起動する

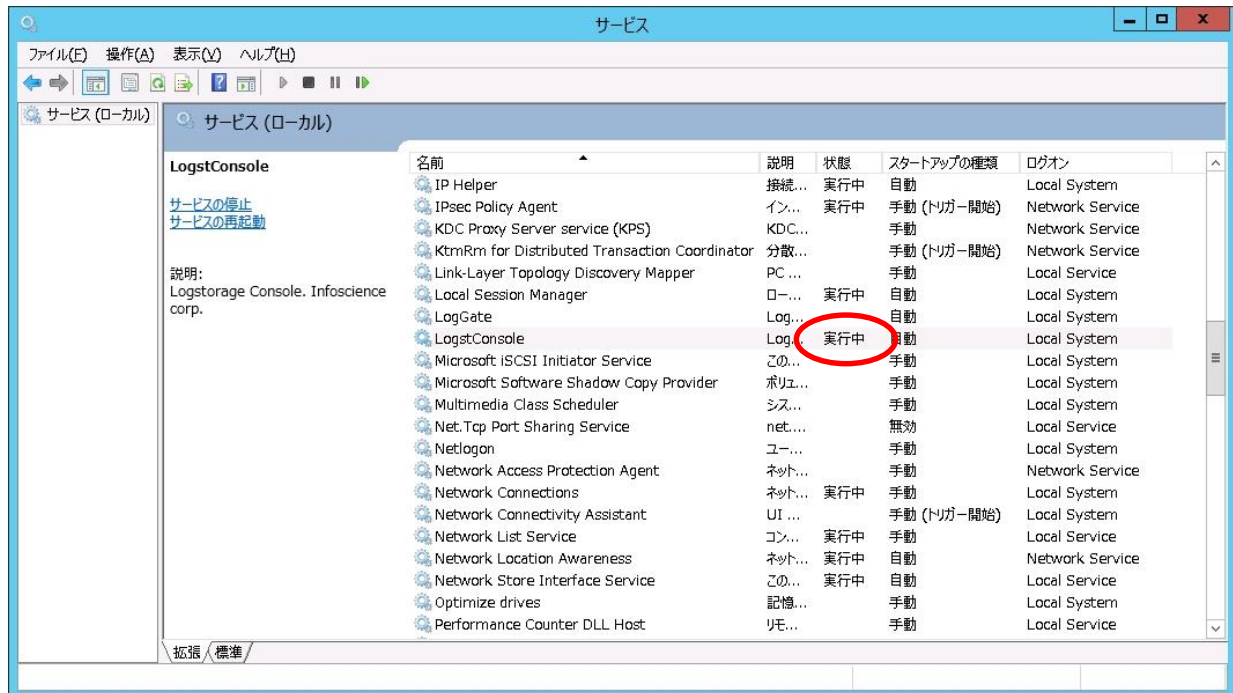
コンソールサーバを Windows サービスから起動するには、LogstConsole サービスの「サービスの開始」を選択します。

「スタート」→「設定」→「コントロールパネル」→「管理ツール」→「サービス」



1. IVEX Logger Viewer を起動する

以下のように、状態が「実行中」(若しくは「開始」)になっていることを確認します。



サービスの設定を編集する場合は以下のコマンドを実行します。この実行により、GUIによるサービス編集プログラムが起動します。%LOGST_HOME%\¥binにある ConsoleServerw.exe をダブルクリックで起動しても同様です。設定の反映には該当箇所を修正の後、サービスを再起動してください。

GUIによるサービス設定の編集

```
> %LOGST_HOME%\¥bin¥console.bat es^
```

1. IVEX Logger Viewer を起動する

1.1.2. コンソールサーバの起動を確認する

コンソールサーバの起動確認はブラウザよりコンソールサーバへアクセスすることで確認できます。

(1)ブラウザを起動して以下の URL にアクセスします。

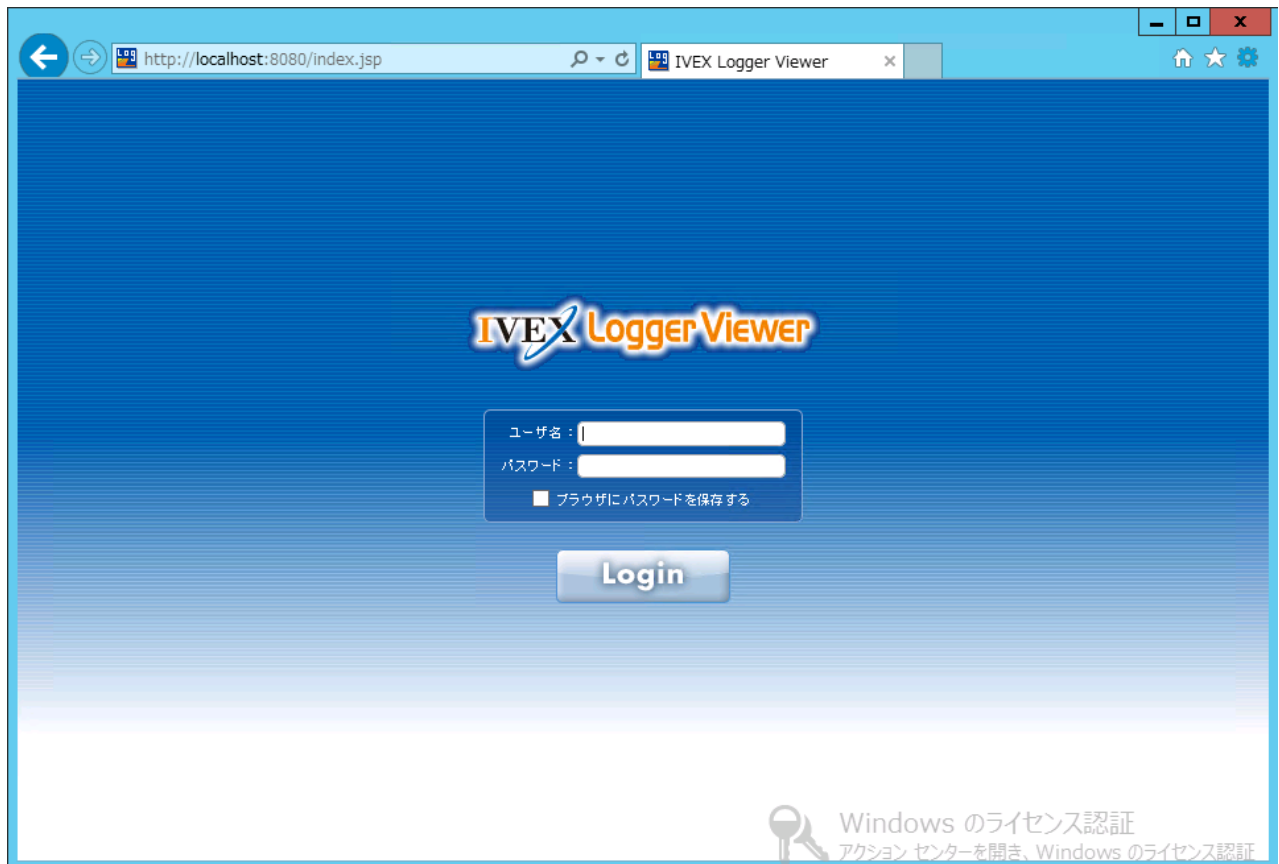
`http://[コンソールサーバの IP アドレスまたはホスト名]:8080/`

コンソールサーバのホスト名を「localhost」、ポート番号を「8080」とすると、

「http://localhost:8080/」となります。

※SSL を使用して通信を行う場合は、https://localhost:8443/ となります。

(2)コンソールサーバのログイン画面が表示されることを確認します。



以上がコンソールサーバの起動確認です。

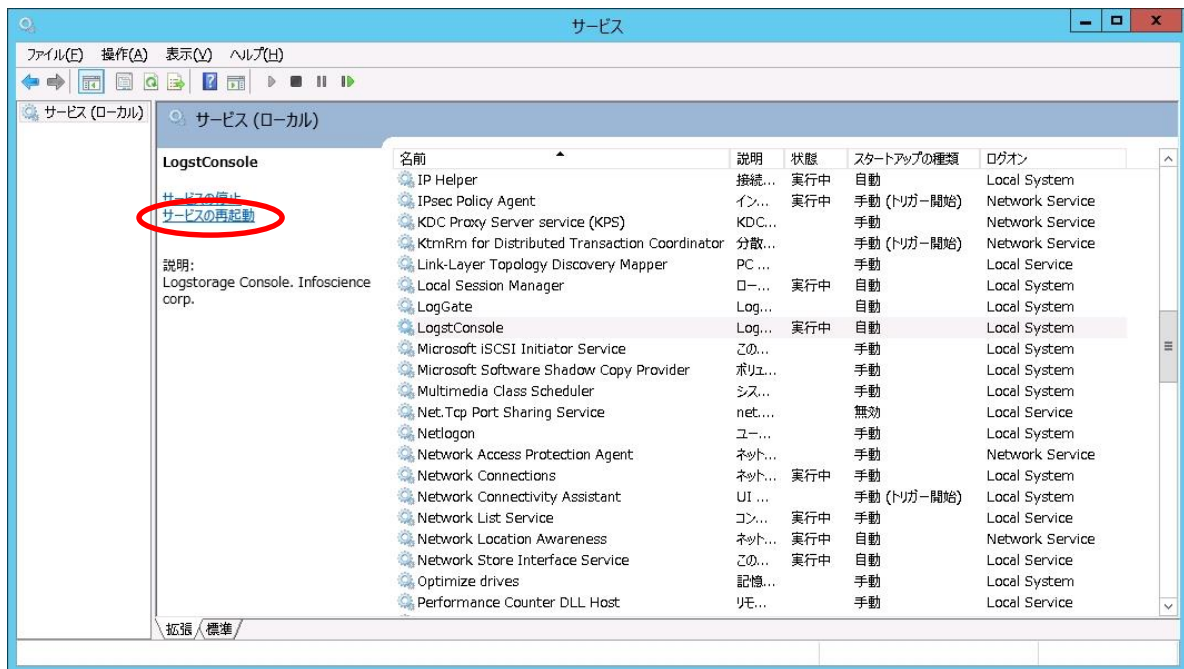
1. IVEX Logger Viewer を起動する

1.1.3. コンソールサーバを再起動する

サービスによるコンソールサーバの再起動は、コントロールパネルの管理ツール内のサービスで実行します。

(1)コントロールパネルの管理ツールからサービスを開きます。

(2)サービスのウィンドウから「LogstConsole」を選択して「サービスの再起動」を選択します。



以上がサービスによる再起動です。

1. IVEX Logger Viewer を起動する

1.1.4. コンソールサーバのバージョンを確認する

コマンドラインからコンソールサーバのバージョンを確認する方法は以下の通りです。

console.bat コマンドの version オプションを付けて実行することで、コンソールサーバのバージョンのみが表示されます。

<実行例 コンソールサーバのバージョン確認例>

```
> %LOGST_HOME%\bin¥console.bat version↵  
Console Server Version 4.6.1
```

LOGST_HOME は コンソールサーバのホームディレクトリです。

バージョンが 4.6.1 であれば、画面に「Console Server Version 4.6.1」と表示されます。

1. IVEX Logger Viewer を起動する

1.2. Windows 環境の LogGate を操作する

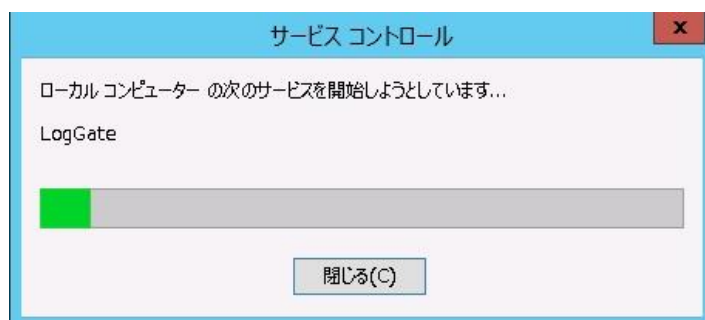
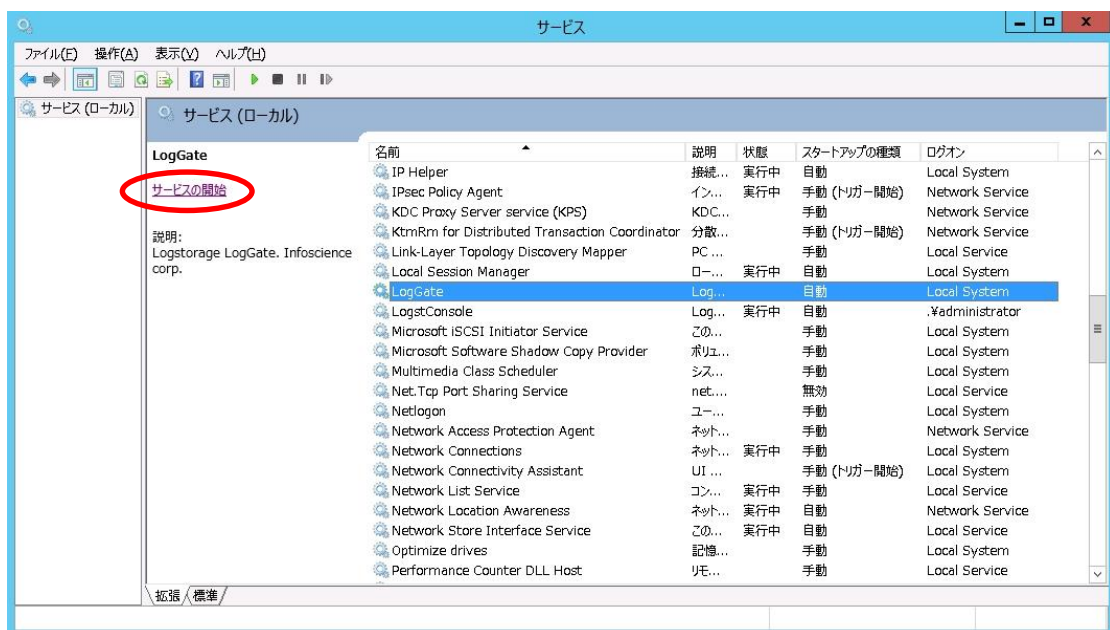
LogGate の起動方法について説明をします。Windows 環境ではサービスから起動を行う方法とコマンドから起動を行う方法の 2 種類あり、それぞれについて説明します。

1.2.1. LogGate を Windows サービスから起動する

起動する前にはコンソールサーバの設定で LogGate の登録を行う必要があります。

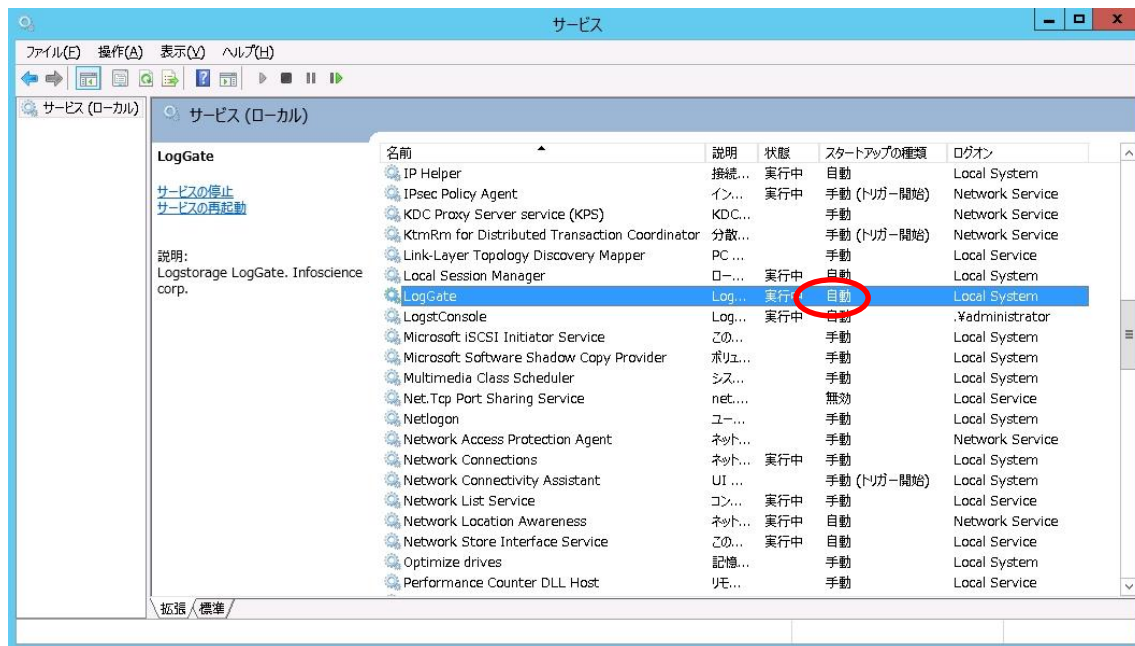
LogGate を Windows サービスで起動するには、LogGate サービスの「サービスの開始」を選択します。

「スタート」→「設定」→「コントロールパネル」→「管理ツール」→「サービス」→「サービスの開始」



1. IVEX Logger Viewer を起動する

以下のように、状態が「実行中」(若しくは「開始」)になっていることを確認します。



サービスの設定を編集する場合は以下のコマンドを実行します。この実行により、GUIによるサービス編集プログラムが起動します。%LOGST_HOME%\binにあるLogGate.exeをダブルクリックで起動しても同様です。設定の反映には該当箇所を修正の後、サービスを再起動してください。

GUIによるサービス設定の編集

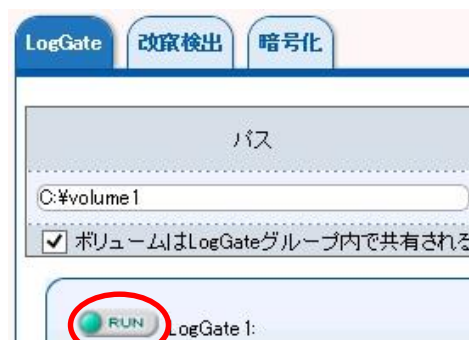
```
> %LOGST_HOME%\bin¥loggate.bat es↓
```

1. IVEX Logger Viewer を起動する

1.2.2. LogGate の起動を確認する

LogGate の起動確認はコンソールサーバにブラウザでアクセスして確認することができます。コンソールサーバの「LogGate グループ情報画面」で「RUN」が表示されることを確認します。

- (1)管理者で、コンソールサーバにログインします。
- (2)メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3)登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4)LogGate グループ情報画面で、起動した LogGate が「RUN」と表示されていることを確認します。



以上が LogGate の起動確認です。

また、以下のコマンドにより起動を確認することができます。停止中の場合は、LogGate is not running.というメッセージが表示されます。

<コマンド>

```
>%LOGST_HOME%\bin\loggate.bat status
Version          : 4.6.1
Runtime version   : 1.7.0_60-b19
:(中略)
SyslogTCPSelectReceiver : alive
SnmpTrapReceiver    : alive
Service[status] completed successfully.
```

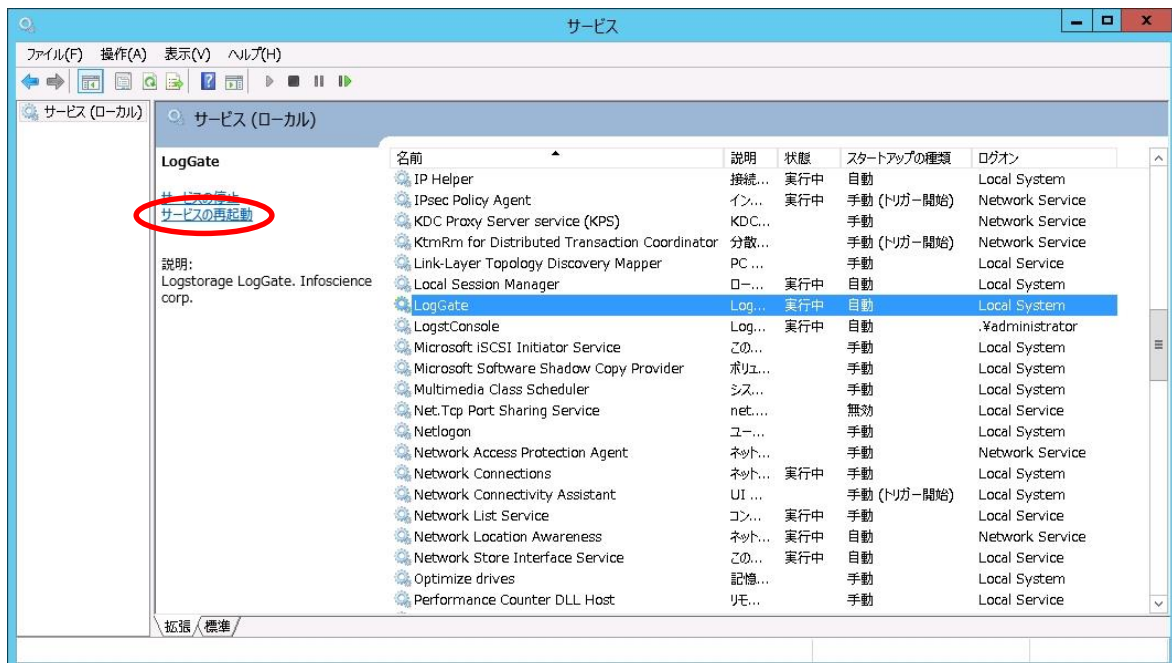
1. IVEX Logger Viewer を起動する

1.2.3. LogGate を再起動する

サービスによる LogGate の再起動は、コントロールパネルの管理ツール内のサービスで実行します。再起動はアドミニストレータ権限を持つユーザで行います。

(1) コントロールパネルの管理ツールからサービスを開きます。

(2) サービスのウィンドウから「LogGate」を選択して「サービスの再起動」を選択します。



以上がサービスによる再起動です。

1. IVEX Logger Viewer を起動する

1.2.4. LogGate のバージョンを確認する

LogGate のバージョンを確認するには、LogGate の起動時に表示されるメッセージの番号から確認できます。また、コマンドラインから LogGate のバージョンを確認する方法もあります。loggate.bat コマンドの version オプションを付けて実行することで、LogGate のバージョンのみが表示されます。

<実行例 LogGate のバージョン確認例>

```
> %LOGST_HOME%\bin¥loggate.bat version↵  
LogGate Version 4.6.1
```

LOGST_HOME は LogGate のホームディレクトリです。

バージョンが 4.6.1 であれば、画面に「LogGate Version 4.6.1」と表示されます。

1. IVEX Logger Viewer を起動する

1.3. ログデータの検索可能状態を確認する

以下の手順によりログデータの検索可能状態を確認することができます。

(1) コンソールサーバが起動されていることを確認します。

(2) LogGate が起動されていることを確認します。

(3) 検索したい期間のログデータが保存されていることを確認します。

以下のコマンドを実行することにより現在収集中のログデータの保存状態を確認することができます。以下の例では、2010 年 4 月 21 日 12 時 30 分 18 秒のログデータが一番新しい時間のログデータ(range の項目)として保存され、2010 年 4 月の LogDB に 6500 行のログデータ(data-block-1 の num of logs 項目)が保存されていることを表します。

<コマンド>

```
>%LOGST_HOME%\bin\logds.bat status<

Service[status] completed successfully.

logds      : logds
  version      : 1
  format id    : -1(up-to-date)
  sign id      : not-signed
  crypt id     : not-crypted
  last snapshot id : 14,407,604
  num of data-block : 1
  num of logs   : 6,500
  range(syslog)   : 20100421122654 - 20100421123007
  range(receive)  : 20100421122707 - 20100421123018
  running admin services : None
-----
data-block-1 : 201004
  format id   : -1(latest)
  num of logs : 6,500
  range(syslog) : 20100421122654 - 20100421123007
  range(receive) : 20100421122707 - 20100421123018
```

2. IVEX Logger Viewer を停止する

2.1. LogGate を操作する

2.1.1. LogGate を Windows サービスから停止する

サービスによる LogGate の停止は、コントロールパネルの管理ツール内のサービスで実行します。LogGate の停止にはコンソールサーバが起動していることを推奨します。

(1)コントロールパネルの管理ツールからサービスを開きます。

(2)サービスのウインドウから「LogGate」を選択して「サービスの停止」を選択します。

以上がサービスによる停止です。

2.1.2. LogGate の停止を確認する

LogGate の停止確認はコンソールサーバにブラウザでアクセスして確認することができます。コンソールサーバの「LogGate グループ情報画面」で「STOP」が表示されることを確認します。

- (1)管理者で、コンソールサーバにログインします。
- (2)メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3)登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4)LogGate グループ情報画面で、停止した LogGate が「STOP」と表示されていることを確認します。



以上が LogGate の停止確認です。

2.2. コンソールサーバを操作する

2.2.1. コンソールサーバを Windows サービスから停止する

サービスによるコンソールサーバの停止は、コントロールパネルの管理ツール内のサービスで実行します。

(1)コントロールパネルの管理ツールからサービスを開きます。

(2)サービスのウインドウから「LogstConsole」を選択して「サービスの停止」を選択します。

以上がサービスによる停止です。

2.2.2. コンソールサーバの停止を確認する

コンソールサーバの停止確認はコンソールサーバの タスクマネージャ確認することができます。

(1)コンソールサーバでタスクマネージャを起動しプロセスタブを開きます。

(2)プロセスに ConsoleServer.exe が存在しないことを確認します。以上がコンソールサーバの停止確認です。

2. IVEX Logger Viewer を停止する

2.3. コンソールサーバの停止可能状態を確認する

コンソールサーバが停止する際は下記の状態を考慮します。状態を確認して停止可能かどうかを判断してください。

(1) レポート作成処理を行っている場合

レポート作成処理中にコンソールサーバが停止する場合、レポート作成処理が中断され、レポート作成条件のステータスが中止となります。コンソールサーバ起動後は定期レポートの場合も含めて対象期間のレポート作成を手動で実行してください。

(2) ブラウザにて検索・集計実行中の場合

処理が中断されるか、エラーメッセージがブラウザに表示されます。コンソールサーバ再起動後に再度検索・集計を実行してください。

2.4. LogGate の停止可能状態を確認する

LogGate が停止する際は下記の状態を考慮します。状態を確認して停止可能かどうかを判断してください。

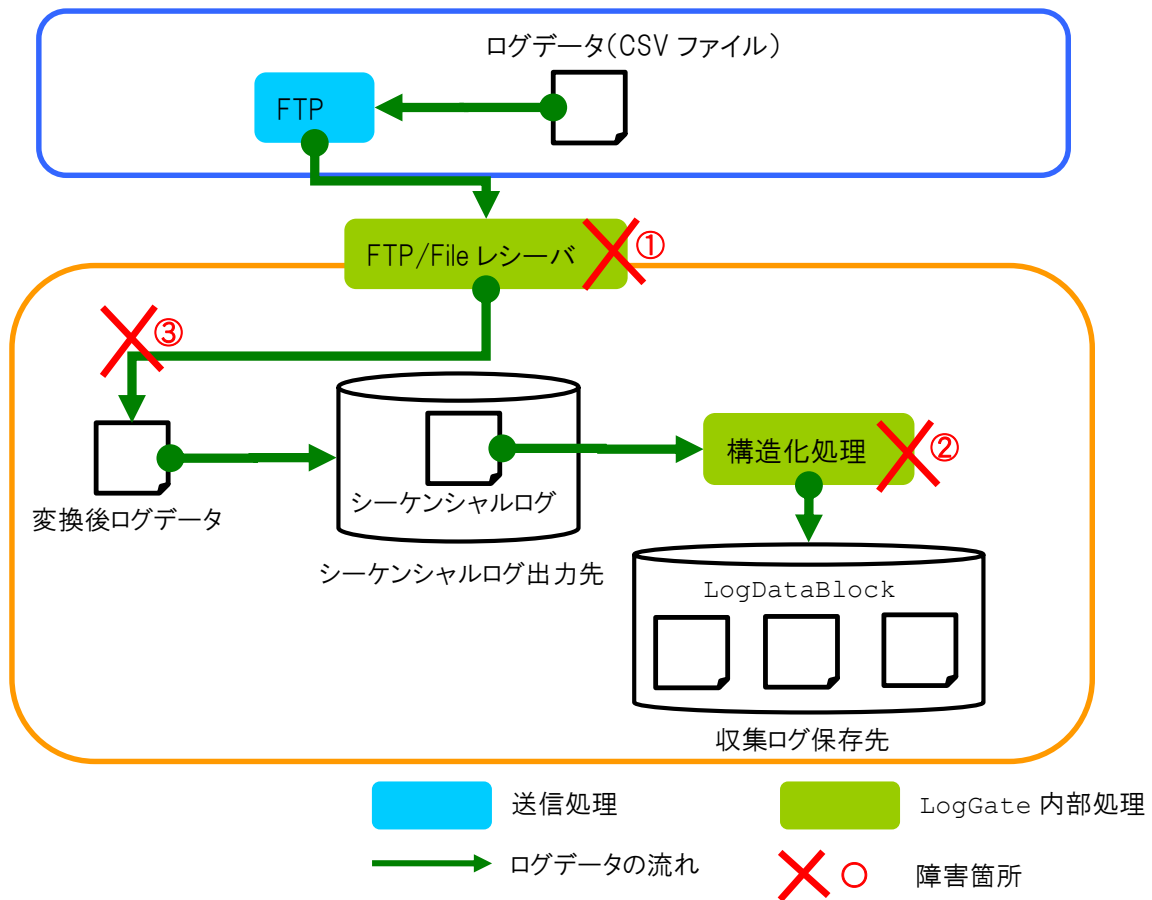
(1) ログソースがログを送信している場合

ログ送信中に LogGate が停止する場合、送信方法によりログデータの扱いが異なります。詳細は「2.5. LogGate プロセス停止時のログデータの扱い」をご覧ください。

(2) 受信したログデータが構造化処理中の場合

受信したログデータの構造化処理中に LogGate が停止する場合、構造化が中断されます。LogGate 再起動後に構造化処理が行われます。

2.5. LogGate プロセス停止時のログデータの扱い



① ログデータ受信中に停止した場合は、DataExchange タスクの再実行にて再送処理が行われます。

②の構造化処理中に停止した場合は、LogGate 再起動後に構造化処理を再開します。

③のログ変換処理中の場合は、LogGate 再起動後に構造化処理を再開します。

3. 通信の設定を行う

3. 通信の設定を行う

3.1. コンソールサーバの Web コンソールアクセスポートを設定する

ブラウザからコンソールサーバへアクセスする際のポート番号は、既定値では TCP/8080 ポートです。

ポート番号を変更する場合は、Web サーバ設定ファイル(server.xml)を変更し、コンソールサーバの再起動を行います。

以下に設定方法を記載します。

(1)エディタ等で Web サーバ設定ファイルを開き、以下の変更を行います。

<変更前>

```
<Connector port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"↵
    maxThreads="150" connectionTimeout="20000" redirectPort="8443"
/>↵
```

<変更後>

```
<Connector port="(ポート番号)"
protocol="org.apache.coyote.http11.Http11NioProtocol"↵
    maxThreads="150" connectionTimeout="20000" redirectPort="8443"
/>↵
```

上記の下線部にブラウザからコンソールサーバへアクセスする際のポート番号を指定します。

(2)コンソールサーバを再起動します。

(3)設定したポート番号でアクセスできるかどうかをブラウザから確認します。

3. 通信の設定を行う

3.2. FTP 関連ポートを設定する

LogGate の FTP レシーバでは、FTP での Active モードと Passive モードのどちらのモードでも受信することができます。どちらのモードで受信するかはログソース側の FTP ツールに依存します。

既定値では、両方受信ができるように設定されています。

以下に各モードで受信した際に使用されるポート番号を記載します。

表 2 FTP レシーバを使用する場合の使用ポートと接続先(既定値)

転送モード	LogGate 使用ポート	用途	ログソース 使用ポート	ログソース 接続先
Active	TCP/21	制御用コネクション	任意	-
Active	任意	データ送信用コネクション	任意	-
Passive	TCP/21	制御用コネクション	任意	localhost
Passive	任意	データ送信用コネクション	任意	localhost

上記の LogGate の使用ポートのうち、Active モード、Passive モードの制御用ポート(コネクション)及びデータ送信用ポートを変更することができます。

FTP 関連ポートの設定方法は以下の通りです。

- (1) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「FTP」を選択します。

3. 通信の設定を行う

(2)FTP 画面のバインドローカルポート(Active/Passive 共通の制御用ポート)を変更します。

LogGate設定
localhost(127.0.0.1)

設定を確認し保存 キャンセル

ステータス
ログ収集
Syslog年補正
Syslog(UDP)
Syslog(TCP)
Syslog(TLS)
LLTP
SNMP
FTP
ユーザ
FTP取り込み
接続モード

FTP

バインドローカルアドレス:

バインドローカルポート: 21

アイドル・タイムアウト: 300

最大同時ログイン: 10

匿名ユーザ有効: ☒

最大同時匿名ログイン: 10

連続ログイン失敗回数: 3

ログイン失敗後の待ち時間(ミリ秒): 500

FTPで受信したファイルを処理後に削除する: ☒

(3)LogGate 設定メニュー「FTP」→「接続モード」を選択します。

(4)接続モード画面のアクティブ FTP データ送信用ポートを変更します。既定値は全てのポート(任意)です。また、パッシブ FTP データ送信用ポート範囲リスト及びバインドアドレスを変更します。

LogGate設定
localhost(127.0.0.1)

設定を確認し保存 キャンセル

ステータス
ログ収集
Syslog年補正
Syslog(UDP)
Syslog(TCP)
Syslog(TLS)
LLTP
SNMP
FTP
ユーザ
FTP取り込み
接続モード
ファイルシステム監視

接続モード

アクティブFTP

アクティブ有効: ☒

バインドアドレス:

ポート: 20

IPチェック有効: ☐

パッシブFTP

ポート範囲リスト:

ポート範囲	削除
値が指定されていません(利用可能な全ポートを使用)	

追加

バインドアドレス:

外部アドレス:

(5)「設定を確認し保存」ボタンを選択します。

3. 通信の設定を行う

(6)「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

LogGate 及びコンソールサーバの再起動は不要です。

(7)設定したポートでアクセスできるかどうか確認します。

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

FTP サーバ設定ファイル(ftpd.xml)

```
<listeners>
<nio-listener name="default" port="<Active/Passive 共通制御用ポート>">
<data-connection implicit-ssl="false">
<active enabled="true" ip-check="true" local-port="<Active データ送信用ポート>" />
<passive ports="Passive データ送信用ポート" address="Passive ログソース接続先" />
</data-connection>
</nio-listener>
</listeners>
```

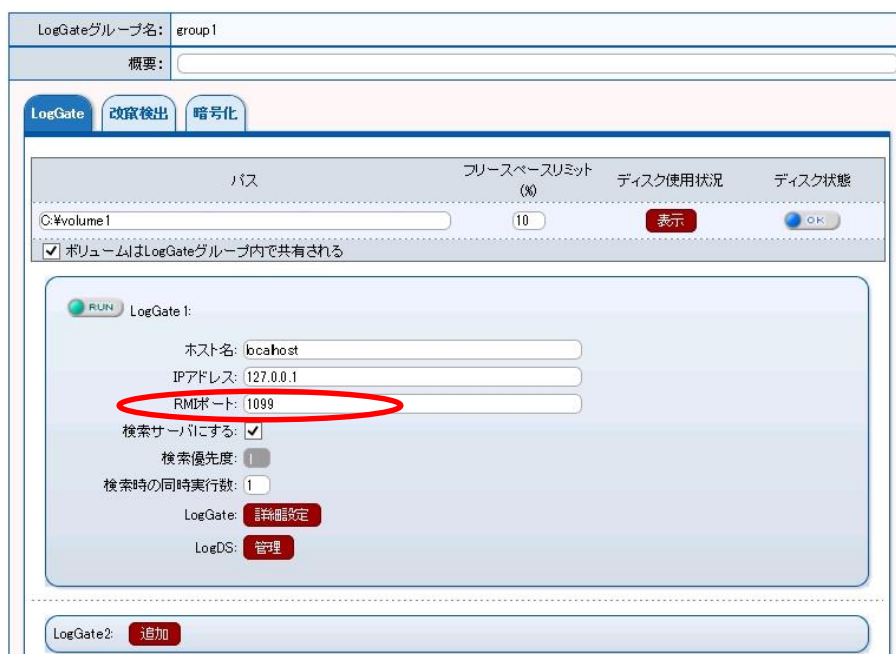
3. 通信の設定を行う

3.3. LogGate 通信用ポートを設定する

LogGate 通信用ポートを設定する方法を記載します。LogGate の管理用通信に使用する際のポート番号は、既定値では TCP/1099 ポートです。

(1) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」を選択します。

(2) LogGate タブ画面の RMI ポートを変更します。



(3) メニュー「ファイル」「上書き保存」ボタンを選択します。

(4) 変更完了のメッセージが表示されます。



(5) LogGate の再起動を行います。

※画面上では STOP になっていますが、実際は設定前の RMI ポートを使用して LogGate は起動中です。

3. 通信の設定を行う

3.4. コンソールサーバシャットダウン用ポートを設定する

コンソールサーバのシャットダウン用通信に使用する際のポート番号は、既定値では TCP/8005 ポートです。

ポート番号を変更する場合は、Web サーバ設定ファイル(server.xml)を変更し、コンソールサーバの再起動を行います。

以下に設定方法を記載します。

(1)エディタ等で Web サーバ設定ファイルを開き、以下の変更を行います。

<変更前>

```
<Server port="8005" shutdown="SHUTDOWN">
```

<変更後>

```
<Server port="(ポート番号)" shutdown="SHUTDOWN">
```

上記の下線部にコンソールサーバのシャットダウン用通信に使用する際のポート番号を指定します。

(2)コンソールサーバを再起動します。

(3)netstat コマンド等から設定したポートで起動できているかどうか確認します。

3. 通信の設定を行う

3.5. LogGate のバインド IP アドレスを設定する

ここでは LogGate がバインドする IP アドレスの設定方法について説明します。

3.5.1. レシーバのバインド先を設定する

レシーバは、既定値では LogGate がインストールされた筐体の全ての NIC(IP アドレス)に対してバインドしますが、特定の NIC(IP アドレス)のみをバインドすることもできます。以下にレシーバ毎の設定方法を記載します。

■FTP レシーバの場合

(1)コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「FTP」を選択します。

(2)FTP 画面のバインドローカルアドレス(Active/Passive 共通)を変更します。

The screenshot shows the LogGate configuration interface. On the left is a sidebar menu with 'LogGate設定' at the top, followed by '設定を確認/保存' and 'キャンセル' buttons. Below these are expandable sections: 'ステータス', 'ログ収集' (with sub-items: Syslog年補正, Syslog(UDP), Syslog(TCP), Syslog(TLS), LLTP, SNMP), 'FTP' (selected), 'ユーザ', 'FTP取り込み', and '接続モード'. The main panel is titled 'FTP' and contains several configuration fields: 'バインドローカルアドレス' (highlighted with a red circle), 'バインドローカルポート' (set to 21), 'アイドル・タイムアウト' (set to 300), '最大同時ログイン' (set to 10), '匿名ユーザ有効' (checked), '最大同時匿名ログイン' (set to 10), '連続ログイン失敗回数' (set to 3), 'ログイン失敗後の待ち時間(ミリ秒)' (set to 500), and 'FTPで受信したファイルを処理後に削除する' (checked). Each field has an information icon (i) to its right.

(3)LogGate 設定メニュー「FTP」→「接続モード」を選択します。

3. 通信の設定を行う

- (4) 接続モード画面のアクティブFTP データ送信用バインドアドレスを変更します。既定値は全ての IP アドレスをバインドします。また、パッシブFTP データ送信用バインドアドレスを変更します。外部アドレスはクライアントとの間に NAT があった場合に異なるサーバアドレス(NIC)を指定します。

The screenshot shows the LogGate configuration interface. On the left is a sidebar with 'LogGate設定' (LogGate Settings) and a tree view containing 'ステータス' (Status), 'ログ収集' (Log Collection), 'FTP', and 'ファイルシステム監視' (File System Monitoring). The main area is titled '接続モード' (Connection Mode). It contains two sections: 'アクティブFTP' (Active FTP) and 'パッシブFTP' (Passive FTP). In the 'アクティブFTP' section, 'アクティブ有効' (Active Enabled) is checked, and the 'バインドアドレス' (Bind Address) field is highlighted with a red circle. In the 'パッシブFTP' section, there is a table for 'ポート範囲リスト' (Port Range List) with columns 'ポート範囲' (Port Range) and '削除' (Delete). Below the table is a '追加' (Add) button. The 'バインドアドレス' (Bind Address) and '外部アドレス' (External Address) fields are highlighted with red circles.

- (5) 「設定を確認し保存」ボタンを選択します。
- (6) 「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。
LogGate 及びコンソールサーバの再起動は不要です。
- (7) 設定したポートでアクセスできるかどうか確認します。

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

FTP サーバ設定ファイル(ftp.xml)

```
<listeners>
<nio-listener name="default" port="21" implicit-ssl="false" idle-timeout="300"
local-address="Active/Passive 共通バインドアドレス">
<active enabled="true" ip-check="true" local-port="20" local-address="Active 用バインドアドレス"/>
<passive address="Passive 用バインドアドレス" external-address="Passive 用外部アドレス"/>
</data-connection>
</nio-listener>
</listeners>
```

3. 通信の設定を行う

3.5.2. コンソールサーバとの接続ソケットのバインド先を設定する

LogGate は起動時にコンソールサーバと接続をします。その際に使用するバインドする IP アドレスはコンソールサーバに登録した IP アドレスを自動的にバインドします。

バインドする IP アドレスを変更する場合は、コンソールサーバに登録した IP アドレスを変更してください。設定は以下の通りです。

(1)ブラウザでコンソールサーバにアクセスし、管理ユーザでログインします。

(2)フォルダリスト「システムの設定」→「LogGate グループ」を選択します。

(3)メニュー「ファイル」→「ファイル作成」を選択します。

(4)「LogGate タブ」の IP アドレスを変更します。

- IP アドレス :<LogGate の IP アドレスを入力>

(5)メニュー「ファイル」→「上書き保存」を選択します。

以下のメッセージが出力されます。

保存が完了しました。

設定の反映には LogGate の再起動が必要です。

LogGate タブの LogGate の構成を変更した場合、コンソールサーバの再起動も必要になります。

(6)LogGate を再起動します。

3. 通信の設定を行う

3.6. コンソールサーバのバインド IP アドレスを確認する

コンソールサーバは、コンソールサーバがインストールされた筐体の全ての NIC(IP アドレス)に対してバインドします。

例:コンソールサーバのバインド IP アドレス(既定値)

# netstat -an			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9999	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8005	0.0.0.0:0	LISTENING

特定の IP アドレスのみにバインドする場合は、以下の様に設定ファイルを修正しコンソールサーバのプロセスを再起動します。

<変更前>

```
<Connector port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" connectionTimeout="20000" redirectPort="8443"
/>
```

<変更後>

```
<Connector port="8080" address="(バインド IP アドレス)"
    protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" connectionTimeout="20000" redirectPort="8443"
/>
```

上記の下線部の address 属性とバインドする IP アドレスを追記します。

3. 通信の設定を行う

3.7. セッションタイムアウトを設定する

ブラウザからコンソールサーバへログイン後、一定時間操作が行われなかった場合は、セキュリティ保護の為にコンソールサーバは再ログインを要求します。操作情報を破棄するまでの時間をセッションタイムアウト時間と呼びます。

セッションタイムアウト時間は変更することができます。既定値ではセッションタイムアウト時間は 120 分です。セッションタイムアウト時間を変更する場合は `LOGST_HOME/logstd/WEB-INF/web.xml` ファイルを変更し、コンソールサーバを再起動します。値を 0 に設定するとセッションタイムアウトはしない設定になります。また、設定できる値の上限値はありません。

(1) エディタ等で `LOGST_HOME/logstd/WEB-INF/web.xml` ファイルを開き、以下の変更を行います。

<変更前>

```
<session-config>↵
    <session-timeout>120</session-timeout>↵
</session-config>↵
```

<変更後>

```
<session-config>↵
    <session-timeout>セッションタイムアウト時間(分)</session-timeout>↵
</session-config>↵
```

下線部にセッションタイムアウト時間(単位: 分)を指定します。

(2) コンソールサーバを再起動します。

(3) ブラウザでコンソールサーバにアクセスして、ログイン後指定したセッションタイムアウト時間までにセッションタイムアウトが無いことを確認します。

3. 通信の設定を行う

3.8. コンソールサーバの HTTPS 通信を設定する

ブラウザからのコンソールサーバへのアクセスは通常 HTTP で行いますが、ブラウザとコンソールサーバの通信を SSL にて暗号化することができます。

(1)コンソールサーバの起動ユーザでコンソールサーバがインストールされたホストにログインします。

コンソールサーバの起動ユーザは以下のようになります。

サービス起動ユーザとなります。サービス起動ユーザの既定値はローカルシステムアカウントです。

(2)コマンドプロンプトを開き、公開鍵暗号方式の鍵を作成します。

以下のコマンドを実行することで、鍵の生成と keystore ファイルを生成することができます。keystore ファイルは鍵の情報が保存されるファイルです。既定値では keystore ファイルの保存先は実行ユーザのホームディレクトリです。実行ユーザのホームディレクトリは以下のようになります。

ホームディレクトリ: 環境変数%HOMEPATH%で指定されるディレクトリです。

<コマンド>

```
# $LOGST_HOME/lib/jdk/bin/keytool -genkeypair -alias <エイリアス名>  
-keystore C:\logstorage\keystore -keyalg RSA
```

-alias を省略するとエイリアス名は mykey となります。

keytool コマンドの主なオプションと説明については、「表 4 keytool コマンドの主なオプション」をご覧ください。

3. 通信の設定を行う

<コマンド実行後の例>

```
# $LOGST_HOME/lib/jdk/bin/keytool -genkeypair -keyalg RSA -keystore
C:\logstorage\keystore
キーストアのパスワードを入力してください:IVEX Logger Viewer↵
新規パスワードを再入力してください:IVEX Logger Viewer↵
姓名を入力してください。
[Unknown]: IVEX Logger Viewer.example.com↵ ←サイト名を入力します。
組織単位名を入力してください。
[Unknown]:infoscience↵
組織名を入力してください。
[Unknown]:pdt↵
都市名または地域网を入力してください。
[Unknown]:minato-ku↵
州名または地方名を入力してください。
[Unknown]:Tokyo↵
この単位に該当する 2 文字の国番号を入力してください。
[Unknown]:JP↵
CN=IVEX Logger Viewer.example.com, OU=infoscience, O=pdt, L=minato-ku, ST=Tokyo,
C=JP でよろしいですか?
[いいえ]:はい↵
<mykey>の鍵パスワードを入力してください。
(キーストアのパスワードと同じ場合は RETURN を押してください):↵ ←[RETURN]を押下します。
```

※キーストアと証明書のパスワードは一致する必要があります。

keytool の詳細は下記サイトを参照してください。

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

3. 通信の設定を行う

(3)エディタ等で Web サーバ設定ファイルを開き、以下の変更を行います。

<変更前>

```
<!--  
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
        maxThreads="150" scheme="https" secure="true"  
        clientAuth="false" sslProtocol="TLS" keystorePass="39ogstorage"/>  
-->
```

<変更後>

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
    maxThreads="150" scheme="https" secure="true"  
    clientAuth="false" sslProtocol="TLS"  
    keystoreFile="(キーストアのファイルパス)"  
    keystorePass="(キーストアのパスワード)" />
```

コメントを外し、下線部にキーストアのファイルパス(フルパス)とパスワードを指定します。また、以前のアクセス(既定値で TCP/8080 ポートのアクセス)を無効にする場合は以下の変更も行います。

<変更前>

```
<Connector                                port="8080"  
protocol="org.apache.coyote.http11.Http11NioProtocol"  
maxThreads="150" connectionTimeout="20000" redirectPort="8443" />
```

<変更後>

```
<!--  
    <Connector                                port="8080"  
protocol="org.apache.coyote.http11.Http11NioProtocol"  
    maxThreads="150" connectionTimeout="20000" redirectPort="8443"  
/>  
-->
```

上記の下線部を追加し、コメントにします。

3. 通信の設定を行う

(4)コンソールサーバを再起動します。

(5)ブラウザからコンソールサーバにアクセスします。

URL は以下のようにプロトコルを https に、ポート番号を 8443 にします。

<https://localhost:8443>

以上がブラウザとコンソールサーバの通信を SSL にて暗号化した場合の設定です。

尚、HTTPS 通信設定を行った場合、以下の管理コマンドは実行に失敗します。

- Report(レポート管理コマンド)
- Impexp(条件・設定インポート・エクスポートコマンド)
- Admin(IVEX Logger Viewer ユーザ/グループ管理コマンド)

コマンド実行可能とするには、“localhost”のみからの HTTP 通信許可設定を行います。

(6)localhost からの HTTP 通信を許可

<変更前>

```
<!--  
    <Connector                                port="8080"  
    protocol="org.apache.coyote.http11.Http11NioProtocol"  
        maxThreads="150" connectionTimeout="20000" redirectPort="8443"  
    />  
-->
```

<変更後>

```
<Connector                                port="8080"  
    protocol="org.apache.coyote.http11.Http11NioProtocol"  
        maxThreads="150" connectionTimeout="20000" redirectPort="8443"  
        scheme="http" address="localhost"/>
```

3. 通信の設定を行う

(7)HTTPS 通信設定を HTTP 設定の後に記述されていることを確認

<変更後>

```
<Connector port="8080"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150"                connectionTimeout="20000"
redirectPort="8443"
scheme="http" address="localhost"/>

<Connector          port="8443"          protocol="HTTP/1.1"
SSLEnabled="true">
    maxThreads="150" scheme="https" secure="true">
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="(キーストアのファイルパス)"
    keystorePass="(キーストアのパスワード)"/>
```

3. 通信の設定を行う

3.9. FTP レシーバの FTPS 通信を設定する

FTP レシーバは SSL による FTP の通信 (FTPS) を行うことができます。手順については以下の通りです。

(1) LogGate の起動ユーザで LogGate がインストールされたホストにログインします。

LogGate の起動ユーザは以下ようになります。

サービス起動ユーザとなります。サービス起動ユーザの既定値はローカルシステムアカウントです。

(2) コマンドプロンプトを開き、公開鍵暗号方式の鍵を作成します。

以下のコマンドを実行することで、鍵の生成と keystore ファイルを生成することができます。keystore ファイルは鍵の情報が保存されるファイルです。既定値では keystore ファイルの保存先は実行ユーザのホームディレクトリです。ホームディレクトリは以下ようになります。

ホームディレクトリ: 環境変数 %HOMEPATH% で指定されるディレクトリです。

<コマンド>

```
# $LOGST_HOME/lib/jdk/bin/keytool -genkeypair -alias <エイリアス名>  
-keystore C:\logstorage\keystore -keyalg RSA
```

-alias を省略するとエイリアス名は mykey となります。

keytool コマンドの主なオプションと説明については、「表 4 keytool コマンドの主なオプション」をご覧ください。

3. 通信の設定を行う

<コマンド実行後の例>

```
# $LOGST_HOME/lib/jdk/bin/keytool -genkeypair -keyalg RSA -keystore
/usr/local/IVEX Logger Viewer/.keystore↵
キースアのパスワードを入力してください:IVEX Logger Viewer↵
新規パスワードを再入力してください:IVEX Logger Viewer↵
姓名を入力してください。
[Unknown]: IVEX Logger Viewer.example.com↵ ←サイト名を入力します。
組織単位名を入力してください。
[Unknown]:infoscience↵
組織名を入力してください。
[Unknown]:pdt↵
都市名または地域名を入力してください。
[Unknown]:minato-ku↵
州名または地方名を入力してください。
[Unknown]:Tokyo↵
この単位に該当する 2 文字の国番号を入力してください。
[Unknown]:JP↵
CN=IVEX Logger Viewer.example.com, OU=infoscience, O=pdt, L=minato-ku, ST=Tokyo,
C=JP でよろしいですか?
[いいえ]:はい↵
<mykey>の鍵パスワードを入力してください。
(キースアのパスワードと同じ場合は RETURN を押してください):↵ ←[RETURN]を押下します。
```

keytool の詳細は下記サイトを参照してください。

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

3. 通信の設定を行う

<鍵の登録内容確認例>

```
# $LOGST_HOME/lib/jdk/bin/keytool -list -v -alias mykey↵
キースタアのパスワードを入力してください: password↵
別名: mykey
作成日: 2007/10/01
エントリのタイプ: keyEntry
証明連鎖の長さ: 1
証明書[1]:
所有者: CN= 44 ogstorage.example.com, OU= 44 ogstorage 44 , O=pdt, L=minato-ku,
ST=Tokyo, C=JP
実行者: CN= 44 ogstorage.example.com, OU= 44 ogstorage 44 , O=pdt, L=minato-ku,
ST=Tokyo, C=JP
シリアル番号: 4700abf0
有効日: Mon Oct 01 17:12:32 JST 2007 有効期限: Sun Dec 30 17:12:32 JST 2007
証明書のフィンガープリント:
MD5: 37:90:EF:77:84:20:3D:B6:D2:A9:6C:48:8F:86:CE:A2
SHA1: 9C:68:34:F6:24:38:9D:41:F9:BA:F5:EF:E8:F8:8D:D6:AA:F3:75:05
```

3. 通信の設定を行う

(3)エディタ等でFTP サーバ設定ファイルを開き、以下の変更を行います。

<変更前>

```
<!-- <ssl>
<keystore file="mykeystore.jks" password="secret" key-password="otherSecret" />
<truststore file="mytruststore.jks" password="secret" />
</ssl> -->
```

<変更後>

```
<ssl>
<keystore file="keystore のファイルパス" key-alias="鍵のエイリアス" password="ストアパスワード" key-password="鍵のパスワード" />
<truststore file="keystore のファイルパス" password="ストアパスワード" />
</ssl>
```

コメントを外し、下線部を設定します。以下に FTP の SSL 設定に関する FTP サーバ設定ファイルの設定項目について記載します。本手順では truststore ファイルを別途用意していない手順ですが、truststore タグの属性値(file 及び password)には keystore タグと同じ設定を行う必要があります。

truststore を使用する場合は keytool のインポート(import オプション)にて CA 発行の証明書をインポートして、ファイルパス(必須)及びストアパスワード(任意)を設定します。

表 3 FTP の SSL 設定に関する FTP サーバ設定ファイルの設定項目

設定項目	説明
keystore/truststore file	キーストアのパスを指定します。
Keystore/truststore password	キーストアのパスワードを指定します。
keystore key-password	鍵パスワードを指定します。
keystore key-alias	鍵のエイリアス名を指定します。

(4)LogGate を再起動します。

(5)FTP クライアントから FTP レシーバに SSL 通信ができることを確認します。

以上が、FTP レシーバが SSL による FTP の通信(FTPS)を行う場合の設定です。

3. 通信の設定を行う

表 4 keytool コマンドの主なオプション

オプション	説明
-genkeypair	鍵を作成するオプション
-alias	鍵のエイリアス名です。指定しない場合は mykey です。
-keyalg	鍵のアルゴリズムです。指定しない場合は DSA です。指定できる値は、「DSA」と「RSA」です。
-keysize	鍵のサイズです。指定しない場合は 1024bit です。
-validity	証明書の有効期限です。指定しない場合は 90 日です。
-keystore	.keystore ファイルのパスです。指定しない場合はユーザホームディレクトリです。
-list	鍵の登録内容が確認できます。

3.10. 内部データベースを設定する

ここでは IVEX Logger Viewer の内部データベースの通信関連の設定を説明します。

3.10.1. 内部データベースの接続数を設定する

内部データベースへの最大接続数(コネクション数)は、ブラウザからコンソールサーバへアクセスするユーザ数及び LogGate の台数に応じて変更します。内部データベースの最大接続数は、一般的にはユーザの同時アクセス数と LogGate 数及び定期レポート数(の 2 倍目安)の合計に、更に3~5程度余裕値を含めて設定します。

内部データベースの接続数が足りなくなる場合、ブラウザからコンソールサーバへのアクセス等で接続待ち時間が発生します。接続待ち時間が発生する場合は、内部データベースへの最大接続数の変更をご検討下さい。

内部データベースの最大接続数を変更する場合は、コンソールサーバ設定ファイル(logstd.dcf)を変更し、コンソールサーバの再起動を行います。

(1)エディタ等でコンソールサーバ設定ファイルを開き、以下の変更を行います。

<変更前>

```
### DataBase Configuration
.....

db.maxconnections=15
db.initialconnections=3
```

<変更後>

```
### DataBase Configuration
.....

db.maxconnections=(最大接続数)
db.initialconnections=(初期コネクション数)
```

下線部に最大接続数及び初期コネクション数を指定します。

(2)コンソールサーバを再起動します。

3. 通信の設定を行う

3.10.2. 内部データベースの再接続間隔を設定する

コンソールサーバまたは LogGate は、コンソールサーバの内部データベースへ接続します。コンソールサーバまたは LogGate からコンソールサーバの内部データベースへ接続ができなくなった場合に、コンソールサーバまたは LogGate は、内部データベースへ再接続を行います。

コンソールサーバ及び LogGate の、内部データベースへの再接続設定を行う場合、コンソールサーバ設定ファイル(logstd.dcf)並びに LogGate 設定ファイル(loggate.dcf)を変更し、対象となるコンソールサーバ及び LogGate を再起動します。

(1)エディタ等でコンソールサーバ設定ファイル及び LogGate 設定ファイルを開き、以下の変更を行います。

<変更前>

```
##DB 接続再試行回数↵
db.retry=3↵
##DB 接続再試行間隔 (msec) ↵
#db.interval=10000↵
```

<変更後>

```
##DB 接続再試行回数↵
db.retry=(コネクション切断時のリトライ回数)↵
##DB 接続再試行間隔 (msec) ↵
db.interval=(再接続待ち時間(ミリ秒))↵
```

コメントを外し、下線部にコネクション切断時のリトライ回数及び再接続待ち時間(ミリ秒)を指定します。各パラメータに設定する値は以下の通りです。

表 5 内部データベースへの再接続に関する設定パラメータ

パラメータ	既定値	設定値
db.retry	3	コネクション切断時のリトライ回数を設定します。 0 を指定した場合、再接続は行いません。
db.interval	10000	再接続待ち時間をミリ秒で設定します。 db.retry が 1 以上の場合のみ有効です。

(2)コンソールサーバ及び LogGate を再起動します。

3. 通信の設定を行う

3.10.3. 内部データベースの接続先を設定する

コンソールサーバを複数台構成している場合(コンソールサーバの負荷分散構成)では、内部データベースを有するコンソールサーバは1つのみです。そのコンソールサーバ以外のコンソールサーバ及び LogGate は全て内部データベースを有するコンソールサーバの内部データベースへ接続する必要があります。

接続先の変更する場合は、コンソールサーバ設定ファイル(logstd.dcf)並びに LogGate 設定ファイル(loggate.dcf)を変更し、対象となるコンソールサーバ及び LogGate を再起動します。

(1)エディタ等でコンソールサーバ設定ファイル及び LogGate 設定ファイルを開き、以下の変更を行います。

<変更前>

```
### DataBase Configuration↵  
db.host=127.0.0.1↵  
db.port=9999↵
```

<変更後>

```
### DataBase Configuration↵  
db.host=(内部データベース IP アドレス)↵  
db.port=(内部データベースのポート番号)↵
```

下線部に内部データベースの IP アドレス及び内部データベースのポート番号を指定します。各パラメータに設定する値は以下の通りです。

表 6 内部データベースの接続先に関する設定パラメータ

パラメータ	既定値	設定値
db.host	127.0.0.1	内部データベースを格納しているサーバの IP アドレスを設定します。コンソールサーバと LogGate が同筐体に構築されている場合は 127.0.0.1 を設定します。
db.port	9999	内部データベースのポート番号を設定します。

(2)コンソールサーバ及び LogGate を再起動します。

4. レシーバを設定する

4.1. シーケンシャルログ出力ディレクトリを変更する

シーケンシャルログ出力ディレクトリには、レシーバによって受信したログを一時的に書き込むシーケンシャルログファイルが作成されます。シーケンシャルログ出力ディレクトリは、既定値ではLogGateワーク先以下ですが、変更することも可能です。大規模構成でLogGateを冗長構成にする場合はシーケンシャルログ出力先ディレクトリを共有ディスクにするよう変更が必要です。

(1)コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「ワーク先」を選択します。

(2)ワーク先画面のシーケンシャルログ出力ディレクトリを変更します。

The screenshot displays the LogGate configuration web interface. On the left is a sidebar with 'LogGate設定' (LogGate Settings) for 'localhost(127.0.0.1)' and a 'ログ収集' (Log Collection) menu. The main area is titled 'ワーク先' (Work Destination). It contains two sections: 'ワーク先の設定' (Work Destination Settings) with a text field for 'ワーク先: C:\loggateway' and an information icon; and 'シーケンシャルログの設定' (Sequential Log Settings) with a text field for 'シーケンシャルログ出力ディレクトリ: C:\loggateway\seqlog' (highlighted with a red circle) and another field for 'シーケンシャルログ ロテータサイズ (byte): 268435456'.

(3)「設定を確認し保存」ボタンを選択します。

(4)「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

(5)LogGate を停止します。

(6)手動で(2)で入力した変更後のシーケンシャルログ出力ディレクトリを作成します。

(7)変更前のシーケンシャルログ出力ディレクトリ内の全てのファイルを変更先のディレクトリにコピーします。

(8)LogGate を起動します。

4.レシーバを設定する

(9)変更前のシーケンシャルログ出力ディレクトリを削除します。

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

コンソールサーバ設定ファイル(logstd.dcf)／LogGate 設定ファイル(loggate.dcf)

com.IVEX Logger Viewer.engine.loggate.SequentialLogFileManager.sequentialLogDir

com.IVEX Logger Viewer.engine.loggate.receive.SequentialLogWriter.maxLength

各パラメータの既定値は以下の通りです。

表 7 シーケンシャルログ出力ディレクトリに関する設定パラメータ

パラメータ	既定値	設定内容
com.IVEX Logger Viewer.engine.loggate.SequentialLogFileManager.sequentialLogDir	[Windows] C:¥¥loggatework¥¥seqlog ※IVEX Logger Viewer インストール時に指定したワーク保存先ディレクトリ以下の seqlog ディレクトリ	シーケンシャルログ出力ディレクトリのパスを指定します。 例 E:¥¥loggatework¥¥seqlog (インストール時に指定したワーク先が E:¥¥loggatework の場合)
com.IVEX Logger Viewer.engine.loggate.receive.SequentialLogWriter.maxLength	268435456(256MB)	シーケンシャルログファイルのローテーションサイズを指定します。 シーケンシャルログファイルがこのサイズを超えた場合、シーケンシャルログファイルがローテートします。

4.レシーバを設定する

4.2. FTP レシーバを設定する

ここでは FTP レシーバの下記の設定方法について説明しています。バインドローカルアドレスとバインドローカルポートについては、「3.5.1.レシーバのバインド先を設定する」「3.2.FTP 関連ポートを設定する」で説明しています。

(1)コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「FTP」を選択します。

(2)FTP 画面の設定を変更します。

The screenshot shows the LogGate configuration interface. On the left, a sidebar menu includes 'LogGate設定' (LogGate Settings) and a list of services: 'ログ収集' (Log Collection), 'Syslog(UDP)', 'Syslog(TCP)', 'Syslog(TLS)', 'LLTP', 'SNMP', and 'FTP'. The 'FTP' option is selected. The main panel, titled 'FTP', contains the following settings:

- バインドローカルアドレス: (text input field)
- バインドローカルポート: 21 (text input field)
- アイドル・タイムアウト: 300 (text input field)
- 最大同時ログイン: 10 (text input field)
- 匿名ユーザ有効: ☒ (checkbox)
- 最大同時匿名ログイン: 10 (text input field)
- 連続ログイン失敗回数: 3 (text input field)
- ログイン失敗後の待ち時間(ミリ秒): 500 (text input field)
- FTPで受信したファイルを処理後に削除する: ☒ (checkbox)

A red rectangular box highlights the settings from 'アイドル・タイムアウト' to 'FTPで受信したファイルを処理後に削除する'.

(3)LogGate 設定メニュー「FTP」→「接続モード」を選択します。

(4)「設定を確認し保存」ボタンを選択します。

(5)「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

LogGate 及びコンソールサーバの再起動は不要です。

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

4.レシーバを設定する

FTP サーバ設定ファイル(ftpd.xml)

```
<server xmlns="http://mina.apache.org/ftpserver/spring/v1" ..省略..
  " id="logstFtpServer" max-logins="最大同時ログイン" max-anon-logins="最大同時匿名ログイン" anon-enabled="匿名ユーザ有効(true/false)" max-login-failures="連続ログイン失敗回数"
  login-failure-delay="ログイン失敗後の待ち時間(ミリ秒)">
  <listeners>
    <nio-listener name="default" port="21" implicit-ssl="false" idle-timeout="アイドル・タイムアウト"
    local-address="127.0.0.2">
```

コンソールサーバ設定ファイル(logstd.dcf)／LogGate 設定ファイル(loggate.dcf)

表 8 FTP レシーバの各設定に相当するパラメータ

パラメータ	既定値	説明/設定値
com.IVEX Viewer.engine.loggate.receive. LogstFtpplet.disableDelLogFile	Logger false	FTP レシーバで受信したログを取り込み後に削除するかどうかを設定します。 false :FTP レシーバで受信したログを取り込み後に削除します。 true :FTP レシーバで受信したログを取り込み後に削除しません。

4.3. 収集ログ保存先を変更する

収集ログ保存先は、構造化したログデータ(LogDB)を保存します。収集ログ保存先以下には1か月毎のLogDBを保存します。集ログ保存先はコンソールサーバのLogGate 設定画面にて変更します。収集ログ保存先を変更する場合は、コンソールサーバの管理画面から設定してLogGate の再起動を行います。

- (1)管理者で、コンソールサーバにログインします。
- (2)メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3)登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4)LogGate グループ情報画面で、パスを変更します。

※画面は WG 版です。AD 版の設定画面は後のページに記載しています。

LogGateグループ名: group1

概要:

LogGate 改竄検出 暗号化

パス	ブリースペースリミット (%)	ディスク使用状況	ディスク状態
C:\volume1	10	表示	OK

LogGate 1(Primary)

RUN

ホスト名: localhost

IPアドレス: 127.0.0.1

RMIポート: 1099

切り替えコマンド:

LogGate: 詳細設定

LogDS: 管理

Secondary: 追加

- (5)LogGate を再起動します。

以上が収集ログ保存先の変更方法となります。その他 LogGate タブの設定項目は以下の通りです。

4.レシーバを設定する

表 9 LogGate タブの設定項目

設定項目	概要/既定値
パス	収集ログ保存先です。 既定値:c:\volume1
フリースペースリミット	指定した%容量が確保できない場合には、Over という表示が出ます。書き込めなくなるとLogGate が停止します。
ディスク使用状況表示ボタン	現在のディスク使用状況(単位:MB)を表示します。ログデータの容量とそれ以外の容量と空き容量の3つで表されます。
ディスク状態	ディスク状態はディスクが正常に使用可能(OK)、障害等により使用不可またはLogGate 停止中のため状態取得不可(NG)、フリースペース上限(over)の3つで表されます。
LogGate の状態	LogGate の状態を表示します。RUN:LogGate は起動中です。STOP:LogGate は停止中です。
LogGate の識別	LogGate がプライマリかセカンダリかを表示します。Primary:プライマリLogGate であることを示します。Secondary:セカンダリLogGate であることを示します。
ホスト名	LogGate のホスト名を入力します。
IP アドレス	LogGate の IP アドレスを入力します。
RMI ポート	LogGate とコンソールサーバ間で使用する RMI ポートを入力します。
LogGate 詳細設定ボタン	主に LogGate のログデータ取り込み(レシーバ)に関する設定画面を表示します。
切り替えコマンド	セカンダリがプライマリ LogGate に切り替えを行う際に実行するコマンドを入力します。主に収集ログ保存先へのマウントコマンドを指定します。
LogDS 管理ボタン	収集したログデータの状態を表示します。また LogDB 再作成をすることができます。詳細は「16.LogDB を再作成する」をご覧ください。
追加/削除	セカンダリ LogGate を追加/削除する際に選択します。追加:新規にセカンダリ LogGate を設定します。削除:設定されたセカンダリ LogGate を削除します。
ハートビート間隔(秒)	セカンダリLogGate がプライマリLogGate の生存確認を行う時間間隔(秒)を設定します。既定値は1(秒)です。
未登録ログソースからのログを破棄する	ログソースとして登録されていない IP アドレスからのログを破棄するかどうかを設定します。チェック有り:ログを破棄します。 チェックなし:ログをログファイルに出力します。既定値はチェックなしです。 チェックなしの場合、ログソース以外のログも収集することができますが、ログソースを登録しない限り検索や集計の対象となりません。
キャンセル	行った設定値の変更を破棄し、LogGate グループリスト画面に戻ります。
更新(アイコン表示)	現在表示されている画面を更新します。LogGate の STOP 状態だった画面が、LogGate 起動後に更新すると RUN 状態になります。

4.レシーバを設定する

以下はアドバンス版(大規模構成用)の LogGate タブ画面です。

LogGate

改竄検出

暗号化

パス

フリースペースリミット (%)

ディスク使用状況

ディスク状態

C:\volume1

10

表示

OK

☒ ボリュームはLogGateグループ内で共有される

RUN

LogGate 1:

ホスト名: loggate1

IPアドレス: 192.168.0.1

RMIポート: 1099

検索サーバにする: ☒

検索優先度: 1

検索時の同時実行数: 1

LogGate: 詳細設定

LogDS: 管理

STOP

LogGate 2: 削除

ホスト名: loggate2

IPアドレス: 192.168.0.2

RMIポート: 1099

検索サーバにする: ☒

検索優先度: 1

検索時の同時実行数: 1

LogGate 3: 追加

検索サーバ選択アルゴリズム: ☒ ラウンドロビン

☐ 優先度

☐ 分散クエリ

☐ ローカルクエリ

☐ 未登録ログソースからのログを破棄する

LogGate タブの設定項目は以下の通りです。

4.レシーバを設定する

表 10 LogGate タブの設定項目

設定項目	概要/既定値
パス	収集ログ保存先です。
ボリュームは LogGate 内で共有されるチェックボックスにチェック	チェックを入れた場合 既定値:c:\¥volume1、以下に各 LogGate のホスト名のディレクトリを作成し、各 LogGate の収集ログ保存先とします。チェックを外す場合、各 LogGate の収集ログ保存先は個別のパスを指定する画面が表示されます。
フリースペースリミット	WG 版と同じです。
ディスク使用状況表示ボタン	WG 版と同じです。
ディスク状態	WG 版と同じです。
LogGate の状態	WG 版と同じです。
LogGate の識別	WG 版と同じです。
ホスト名	LogGate のホスト名を入力します。パスの設定項目の LogGate 内で共有されるチェックボックスにチェックを入れた場合、ここで入力した LogGate のホスト名は LogGate が書き込むディレクトリ名となります。そのため、ディレクトリに指定できない文字列は LogGate のホスト名には使用しないでください。また、環境を問わず大文字小文字を区別します。
IP アドレス	WG 版と同じです。
RMI ポート	WG 版と同じです。
LogGate 詳細設定	WG 版と同じです。
LogDS 管理ボタン	WG 版と同じです。
追加/削除	LogGate を追加/削除する際に選択します。追加:新規に LogGate を設定します。削除:設定された LogGate を削除します。
検索サーバにする	LogGate を検索サーバにするかどうかを設定します。 チェック有り:検索サーバにします。 チェック無し:検索サーバにしません。 既定値はチェック有りです。 検索サーバにチェックを付けることで LogGate を検索時に検索サーバとして自身のログまたは他の LogGate のログを検索するよう動作します。 少なくとも 1 つ以上の LogGate は検索サーバにしておく必要があります。 検索サーバに指定しない LogGate はログ収集に専念するサーバにすることができます。また検索サーバに指定した LogGate でレシーバを起動させないようにすることで、検索専用の LogGate にすることができます。

4.レシーバを設定する

検索優先度 ※「検索アルゴリズム」を優先度 にすると設定できます。	検索サーバへ接続する優先度を 1～99 の範囲で指定します。 値が大きい程、接続する確率が高くなります。検索サーバの能力にばらつき がある場合などに使用して下さい。
検索時の同時実行数 ※「検索アルゴリズム」をローカル クエリの場合は設定できません。	検索サーバの並列検索数を指定します。 値を 2 以上に設定することで、設定された検索サーバ内の検索を並列にす ることができます。
検索アルゴリズムの設定	選択した検索アルゴリズムの設定値を設定します。
追加/削除	LogGate を追加/削除する際に選択します。 追加:新規に LogGate を設定します。 削除:設定された LogGate を削除します。
検索アルゴリズム	IVEX Logger Viewer 内でのログを検索する際に使用するアルゴリズムを指 定します。 検索アルゴリズムについては「 ガイド 」をご覧ください。
未登録ログソースからのログを破 棄する	WG 版と同じです。

5. メモリ設定を行う

5. メモリ設定を行う

5.1. メモリ設定を行う

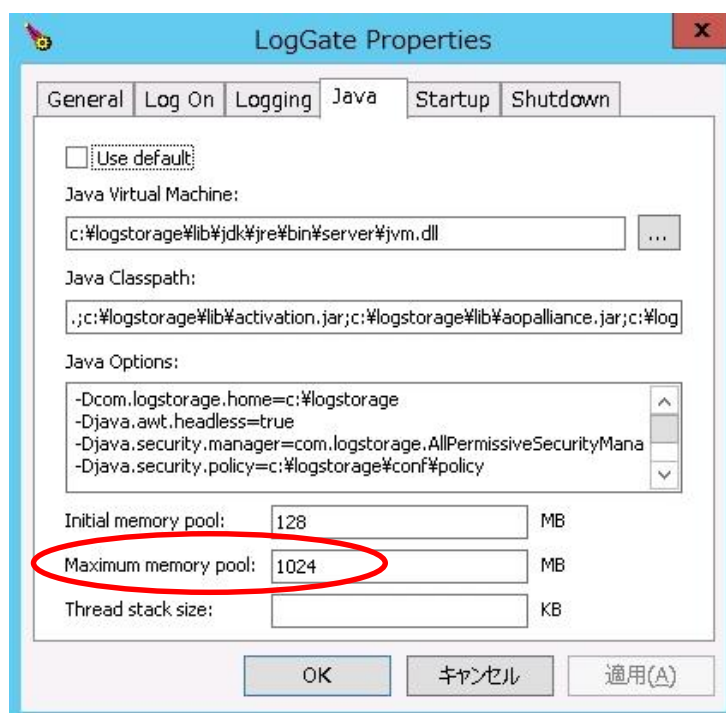
コンソールサーバサービス及び LogGate サービスが使用するメモリ容量を変更します。

5.1.1. LogGate のメモリ設定を行う

LogGate のメモリ設定を変更するには、LogGate サービスが使用するメモリ設定を変更します。

LogGatew.exeを実行してメモリの設定変更を行い、LogGate の再起動を行います。既定値は1024MBです。32bit 版ではメモリ最大割り当ては 1.5GB となります。64bit 版ではメモリ最大値制限はありません。(但し搭載物理メモリ分まで)

- (1) LogGatew.exe を実行(ダブルクリック)し、[Java]タブの Maximum memory pool の値を変更します。



Maximum memory pool に LogGate に設定するメモリ容量(単位:MB)を指定します。LogGate は設定されたメモリ容量を最大メモリ量として使用します。

- (2) LogGate の再起動を行います。

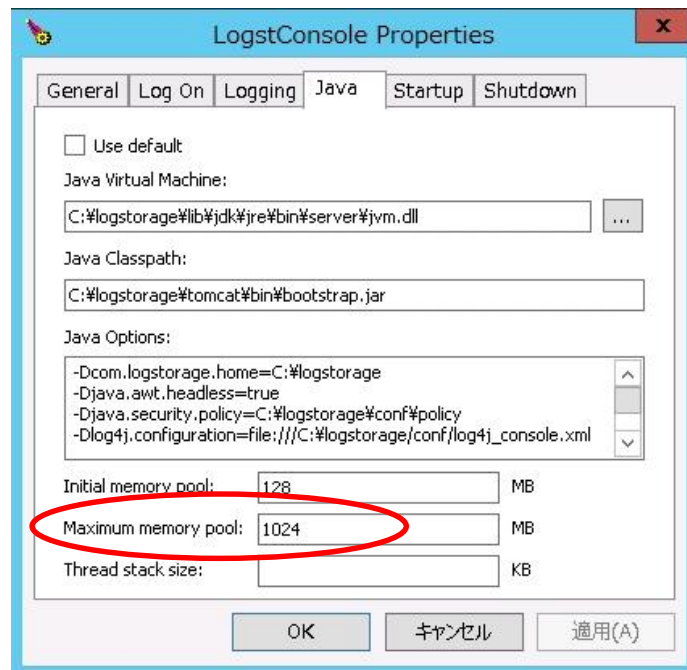
以上が Windows 環境での LogGate のメモリ設定の変更方法です。

5. メモリ設定を行う

5.1.2. コンソールサーバのメモリ設定を行う

コンソールサーバのメモリ設定を変更するには、コンソールサーバサービスが使用するメモリ設定を変更します。コンソールサーバサービスが使用するメモリ設定を変更するには、ConsoleServerw.exe を実行してメモリの設定変更を行い、コンソールサーバの再起動を行います。既定値は 1024MB です。32bit 版ではメモリ最大割り当ては 1.5GB となります。64bit 版ではメモリ最大値制限はありません。(但し搭載物理メモリ分まで)

- (1) ConsoleServerw.exe を実行(ダブルクリック)し、[Java]タブの Maximum memory pool の値を変更します。



Maximum memory pool にコンソールサーバに設定するメモリ容量(単位:MB)を指定します。コンソールサーバは設定されたメモリ容量を最大メモリ量として使用します。

- (2) コンソールサーバの再起動を行います。

以上がコンソールサーバのメモリ設定の変更方法です。

6. グループ/ユーザを管理する

6. グループ/ユーザを管理する

6.1. グループを作成する

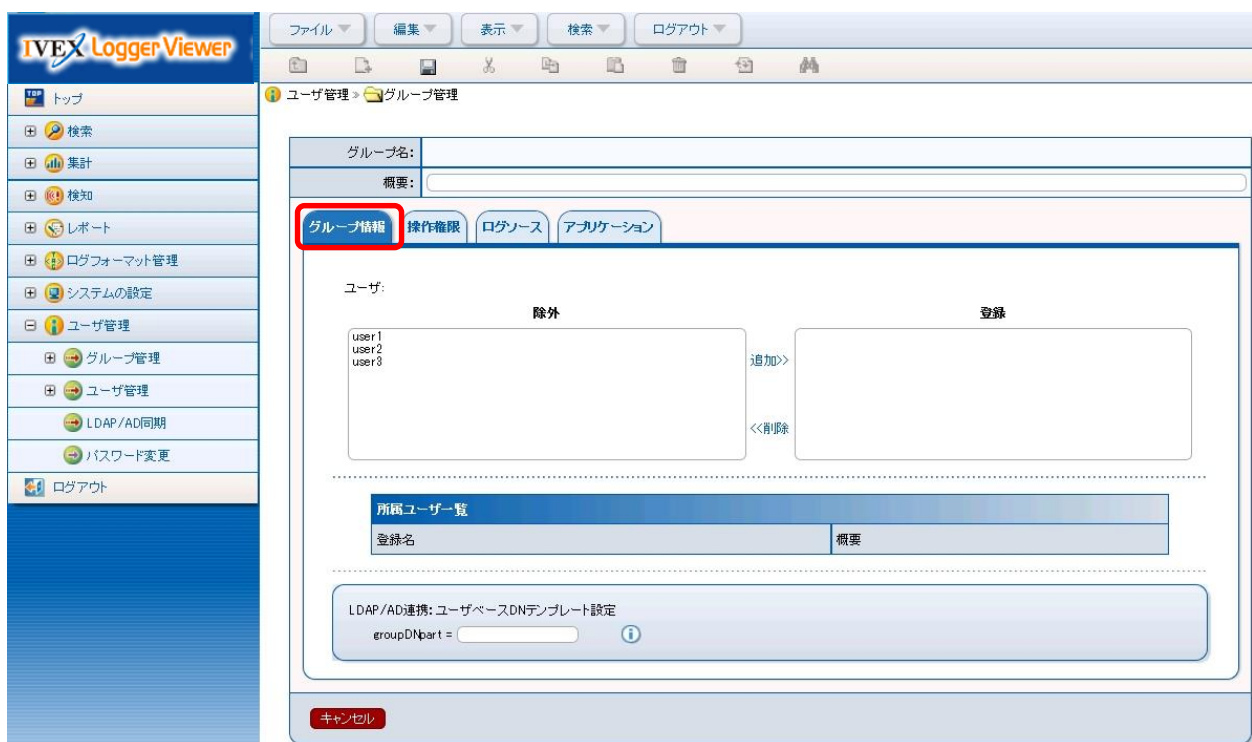
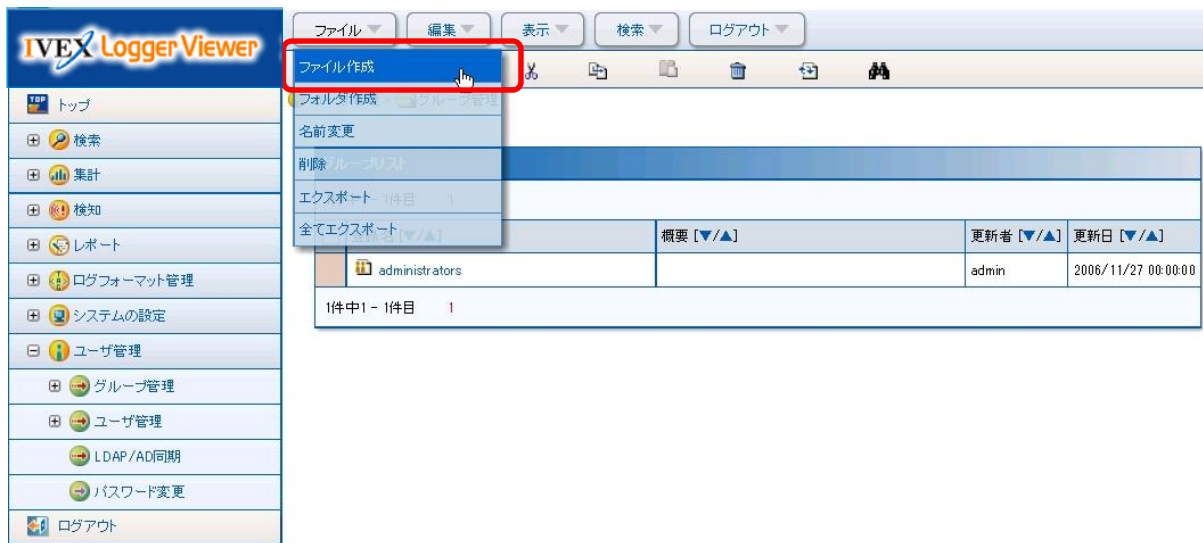
- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「グループ管理」を選択し、「グループリスト画面」を表示します。

The screenshot shows the IVE X Logger Viewer web application. The left sidebar contains a list of navigation items: トップ, 検索, 集計, 検知, レポート, ログフォーマット管理, システムの設定, ユーザ管理, グループ管理, ユーザ管理, LDAP/AD同期, パスワード変更, and ログアウト. The 'ユーザ管理' and 'グループ管理' items are highlighted with red boxes. The main content area displays the 'グループ管理' screen, which includes a breadcrumb trail 'ユーザ管理 > グループ管理' and a table titled 'グループリスト'. The table shows one group named 'administrators' with a user 'admin' and a creation date of '2006/11/27 00:00:00'.

登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	更新日 [▼/▲]
administrators		admin	2006/11/27 00:00:00

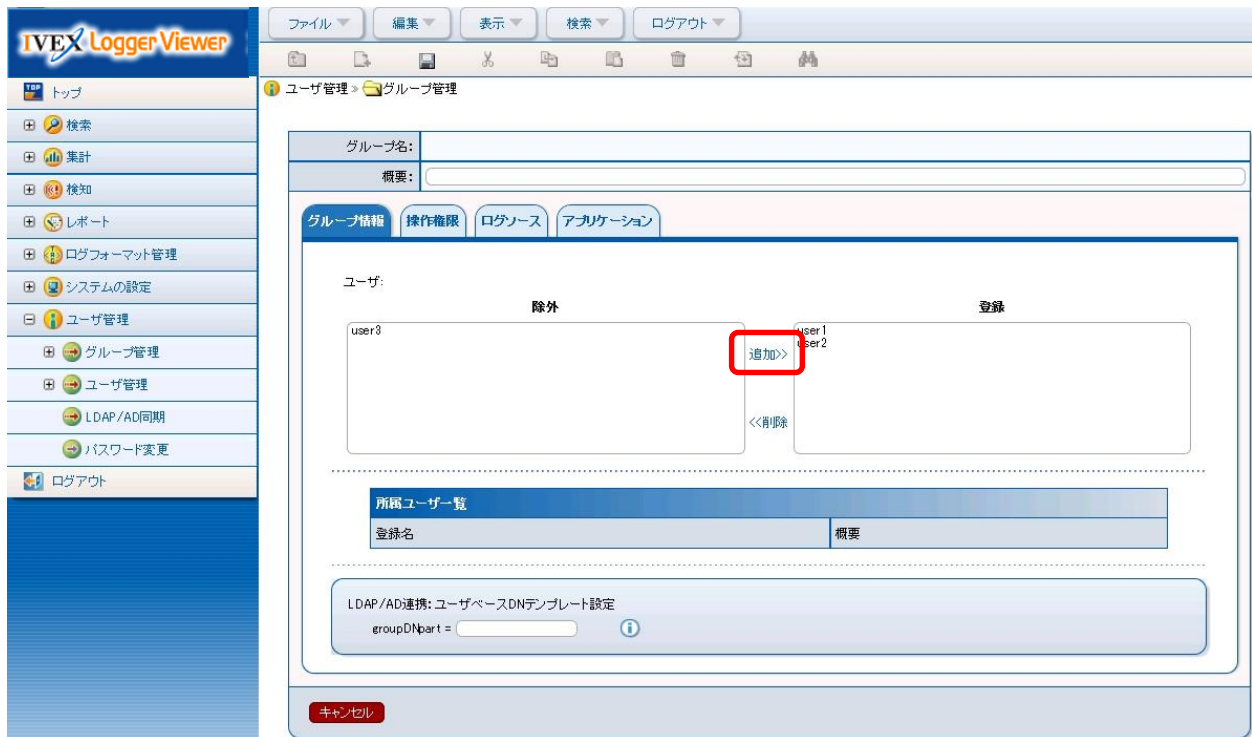
6. グループ/ユーザを管理する

(2) メニューの「ファイル」→「ファイル作成」を選択し、「グループ情報タブ画面」を表示します。



6. グループ/ユーザを管理する

(3)「グループ情報タブ画面」で当該グループに所属するユーザを選択し、追加>>ボタンを選択します。



以下は、LDAP/AD 認証を有効にしている場合にのみ設定します。

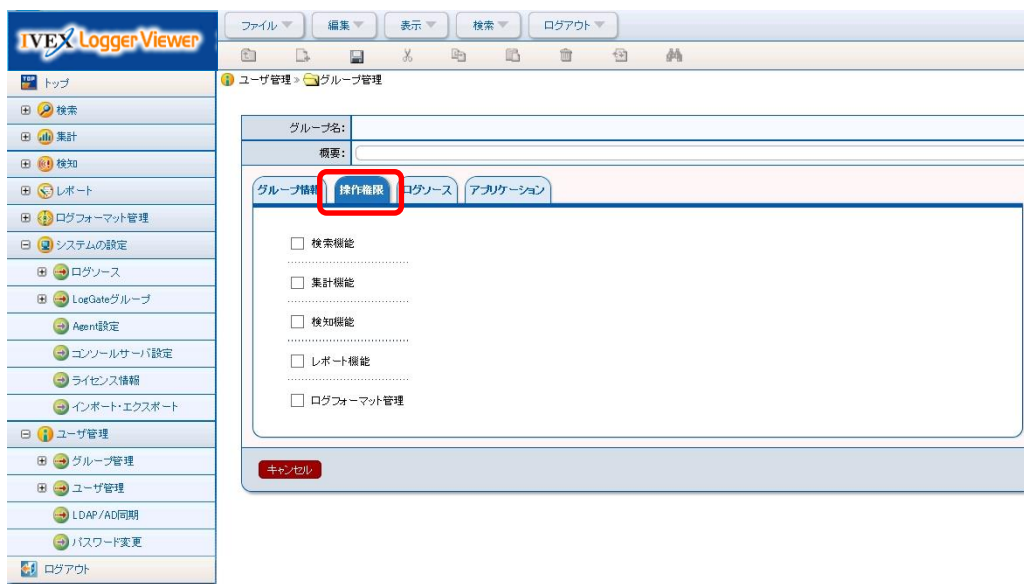
「groupDNpart=」に入力する値はユーザのベース DN テンプレートに対応します。以下のような設定がユーザのベース DN(suffix)に設定されていた場合、「groupDNpart=」に sales とすると、このユーザのベース DN(suffix)は「ou=People, dn=sales」となります。

[システムの設定] > [コンソールサーバ設定] > [ユーザ認証]タブ > [LDAP/AD 設定]欄

ユーザ設定	
ユーザのベースDN (suffix):	ou=People, dn={groupDNpart} ⓘ
ユーザ名の属性:	uid
ユーザのobjectClass:	person
ユーザ概要の属性:	
所属グループの属性:	

6. グループ/ユーザを管理する

(4)「操作権限タブ」を選択し、「操作権限タブ画面」を表示します。

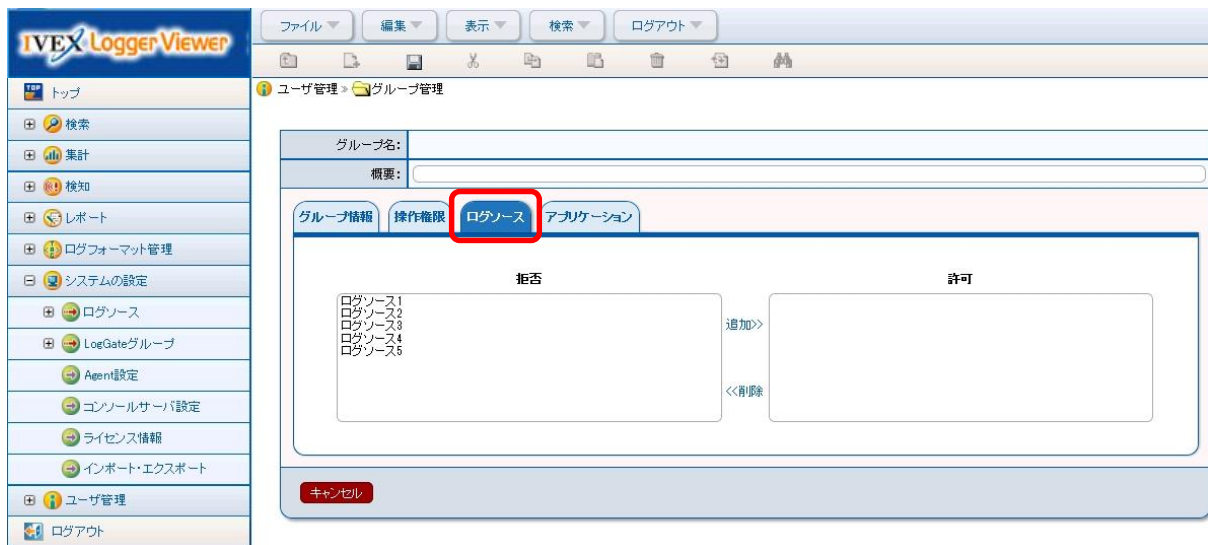


(5)「操作権限タブ画面」で当該グループに付与する権限にチェックします。



6. グループ/ユーザを管理する

(6)「ログソースタブ」を選択し、「ログソースタブ画面」を表示します。

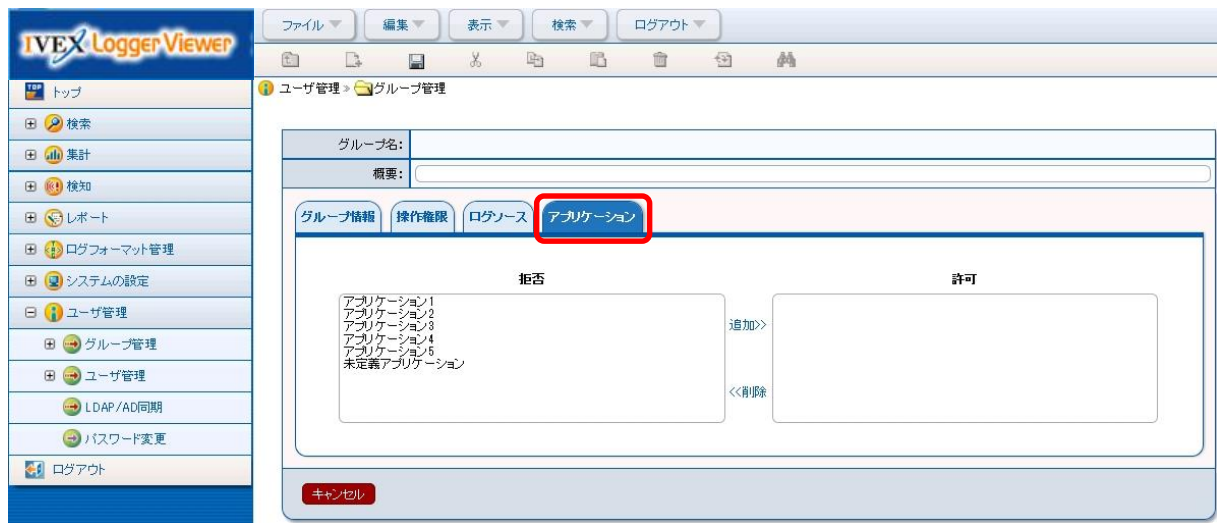


(7)「ログソースタブ画面」で当該グループが扱えるログソースのログファイルを選択し、追加>>ボタンを選択します。

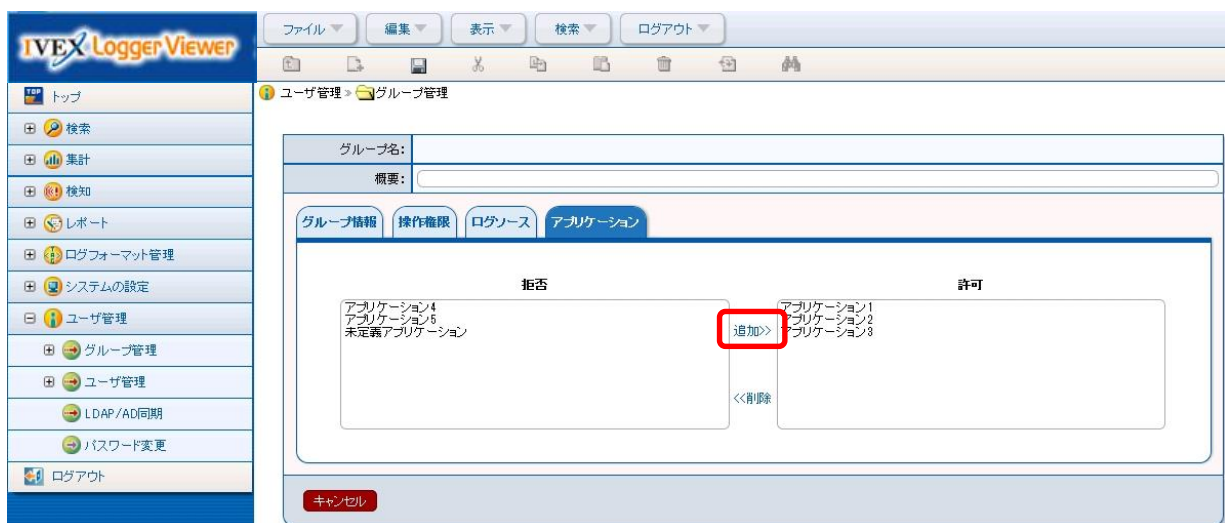


6. グループ/ユーザを管理する

(8)「アプリケーションタブ」を選択し、「アプリケーションタブ画面」を表示します。

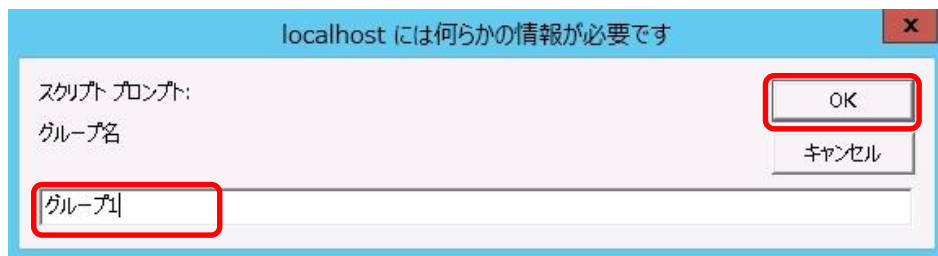


(9)「アプリケーションタブ画面」で当該グループが扱えるアプリケーションのログファイルを選択し、追加>>ボタンを選択します。



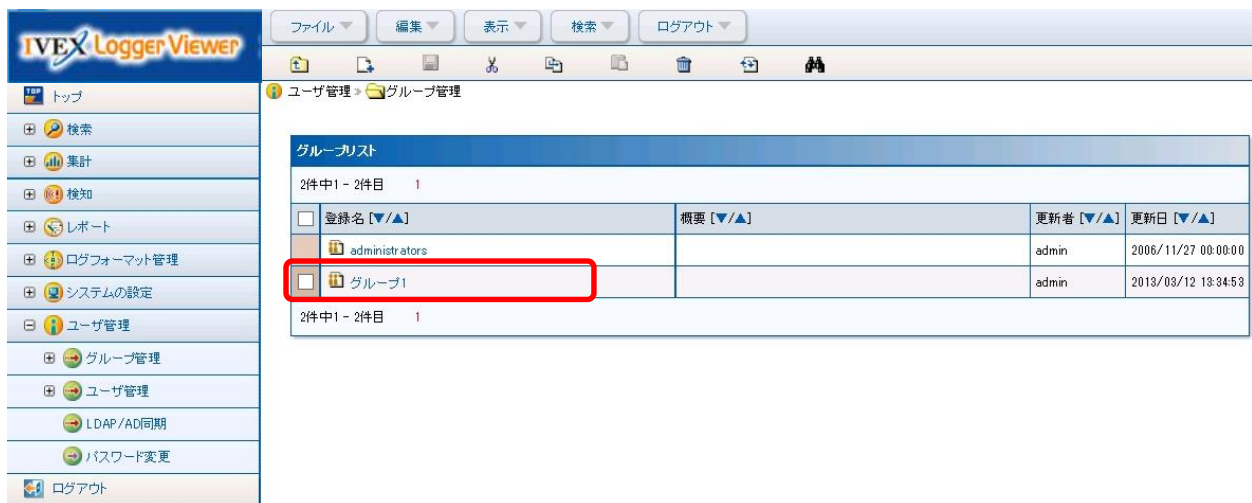
6. グループ/ユーザを管理する

(10)メニューの「ファイル」→「名前を付けて保存」を選択し、「グループ名」を入力し「OK」を選択します。



6. グループ/ユーザを管理する

(11)フォルダリストの「ユーザ管理」→「グループ管理」を選択し、「グループリスト画面」を表示し、作成したグループが表示されることを確認します。



登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	更新日 [▼/▲]
administrators		admin	2006/11/27 00:00:00
グループ1		admin	2013/03/12 13:34:53

以上がグループ作成の操作となります。

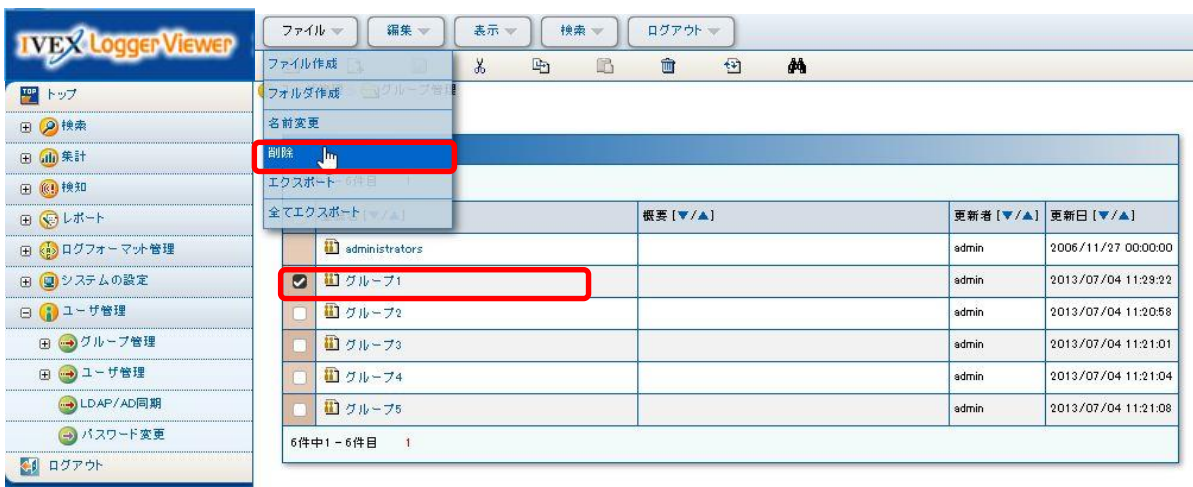
6. グループ/ユーザを管理する

6.2. グループを削除する

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「グループ管理」を選択し、「グループリスト画面」を表示します。

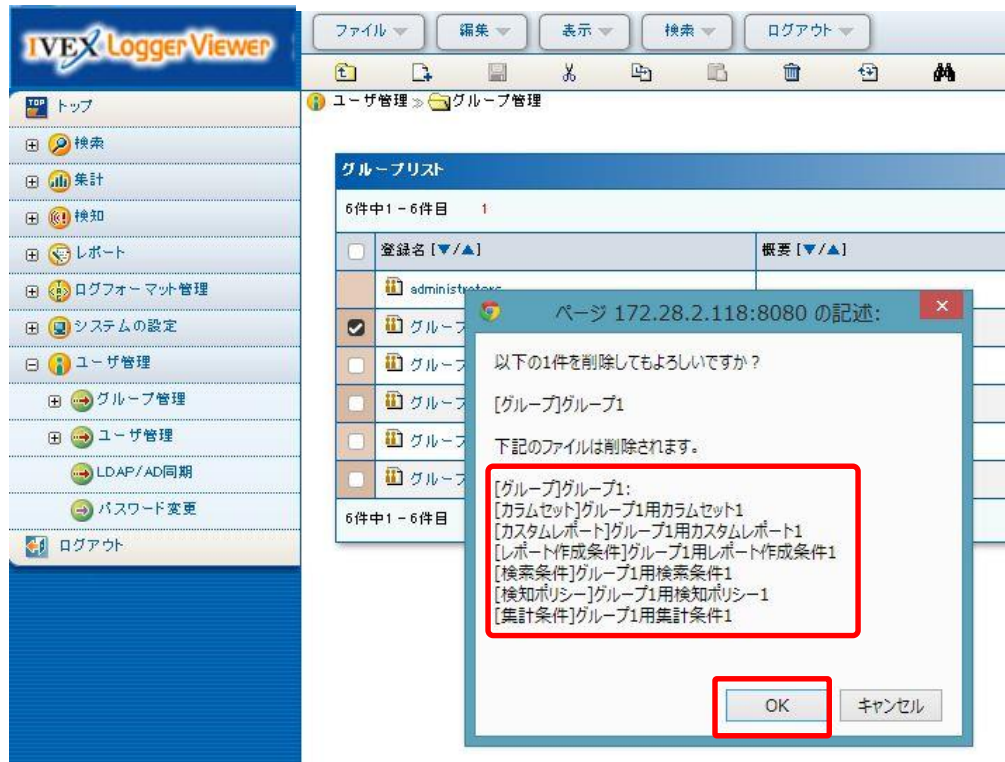


- (2) グループリスト画面で削除するグループにチェックを入れ、メニューの「ファイル」→「削除」を選択します。



6. グループ/ユーザを管理する

(3) 確認ダイアログの表示内容を確認し、問題がなければ「OK」を選択します。



グループ削除を実行すると上図内の赤枠の内容の通り、当該グループが所有者となっている下記の各種条件ファイルが同時に削除されます。

- 検索条件
- カラムセット
- 集計条件
- 検知ポリシー
- レポート作成条件
- カスタムレポート

6. グループ/ユーザを管理する

尚、削除対象となるグループに所属するユーザが存在する場合、下図のエラーダイアログが表示されます。事前に他のグループへの所属変更を行うか、「」記載のユーザ削除操作を行った上で実行してください。



(4) グループリスト画面から削除されたことを確認します。



以上がグループ削除の操作となります。

6. グループ/ユーザを管理する

6.3. ユーザを作成する

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。

The screenshot displays the IVE X Logger Viewer web application. On the left is a navigation menu with various icons and labels. The 'ユーザ管理' (User Management) option is highlighted with a red rectangle. The main content area shows a breadcrumb trail 'ユーザ管理 > ユーザ管理' and a table titled 'ユーザリスト' (User List). The table contains three rows of user data, with columns for selection, login name, summary, updater, authentication method, and update date. The first two 'ユーザ管理' options in the left menu are also highlighted with red rectangles.

<input type="checkbox"/>	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 13:17:41
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03

6. グループ/ユーザを管理する

(3) メニューの「ファイル」→「ファイル作成」を選択し、「グループ設定タブ画面」を表示します。

IVE X Logger Viewer

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

ファイル作成 (highlighted)

フォルダ作成 ユーザ管理
名前変更
削除 リセット
ロック 1件中1 - 3件目 1
ロック解除 1件中1 - 3件目 1
エクスポート 1件中1 - 3件目 1
全てエクスポート

	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
		admin	LOCAL	2013/03/12 13:17:26
		admin	LOCAL	2013/03/12 13:17:41
		admin	LOCAL	2013/03/12 13:18:03

3件中1 - 3件目 1

IVE X Logger Viewer

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

ユーザ管理 ユーザ管理

ユーザ名:
概要:

グループ設定 (highlighted) 操作権限 認証設定

所属グループ:

キャンセル

6. グループ/ユーザを管理する

(3)「グループ設定タブ画面」で当該ユーザが所属するグループを選択します。

The screenshot shows the IVE X Logger Viewer application window. The left sidebar contains a menu with options like 'トップ', '検索', '集計', '検知', 'レポート', 'ログフォーマット管理', 'システムの設定', 'ユーザ管理', 'グループ管理', 'ユーザ管理', 'LDAP/AD同期', 'パスワード変更', and 'ログアウト'. The main area is titled 'ユーザ管理' and 'ユーザ管理'. It features a 'ユーザ名:' field, a '概要:' field, and three tabs: 'グループ設定', '操作権限', and '認証設定'. The 'グループ設定' tab is active, showing a dropdown menu for '所属グループ: グループ1' with 'グループ1' selected. A red rectangle highlights the dropdown menu. At the bottom, there is a 'キャンセル' button.

(4)「操作権限タブ」を選択し、「操作権限タブ画面」を表示します。

The screenshot shows the IVE X Logger Viewer application window with the '操作権限' tab selected. The left sidebar is the same as in the previous screenshot. The main area is titled 'ユーザ管理' and 'ユーザ管理'. It features a 'ユーザ名:' field, a '概要:' field, and three tabs: 'グループ設定', '操作権限', and '認証設定'. The '操作権限' tab is active, showing a list of permissions with checkboxes: '検索機能', '集計機能', '検知機能', 'レポート機能', and 'ログフォーマット管理'. All checkboxes are currently unchecked. A red rectangle highlights the '操作権限' tab. At the bottom, there is a 'キャンセル' button.

6. グループ/ユーザを管理する

(5)「操作権限タブ画面」で当該ユーザに付与する権限にチェックします。



(6)「認証設定タブ」を選択し、「パスワード変更タブ画面」を表示します。



6. グループ/ユーザを管理する

(7)「認証設定タブ画面」でパスワードを入力します。

IVEX Logger Viewer 内部認証を使った場合

The screenshot displays the 'Authentication Settings' tab within the 'User Management' section of the IVE X Logger Viewer. The 'Logstorage内部認証' (Internal Authentication) option is selected, and the password fields are highlighted with a red rectangle. The interface includes a sidebar with various system management functions and a top navigation bar with options like 'File', 'Edit', 'View', 'Search', and 'Logout'.

パスワードの最小文字数は、フォルダリストの「システムの設定」から「コンソールサーバ設定」の「ユーザ認証の設定」タブで指定した値となります。また、パスワードは大文字、小文字の区別はありますが、半角文字であれば利用可能な文字の制限はありません。

6. グループ/ユーザを管理する

LDAP/AD 認証を使った場合

ユーザー名:

概要:

グループ設定 操作権限 認証設定

☒ ユーザーを利用可能にする

☐ Logstore内部認証

パスワード:

パスワード(確認):

☒ LDAP/AD認証

ベースDNテンプレート設定

userDNpart =

キャンセル

LDAP/AD を使用した認証です。

「userDNpart=」に入力する値はグループのベース DN テンプレートで {userDNpart} の代わりに置き換えられます。以下のような設定がグループのベース DN(suffix)に設定されていた場合、「userDNpart=」に user とすると、このユーザのベース DN(suffix)は「dn=user,ou=People」となります。

[システムの設定] > [コンソールサーバ設定] > [ユーザ認証]タブ > [LDAP/AD 設定]欄

グループ設定

グループのベースDN (suffix):

グループ名の属性:

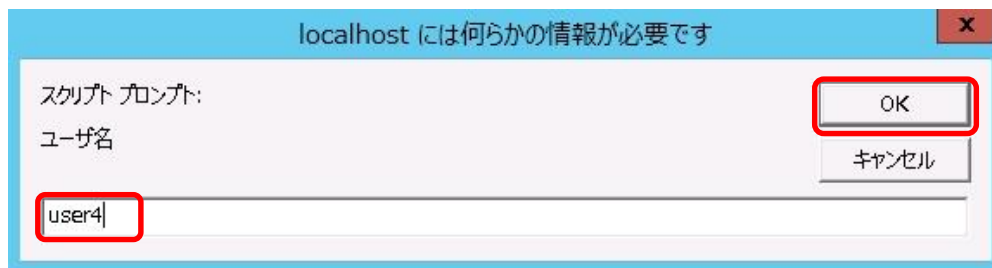
グループのobjectClass:

グループ概要の属性:

メンバーリストの属性:

6. グループ/ユーザを管理する

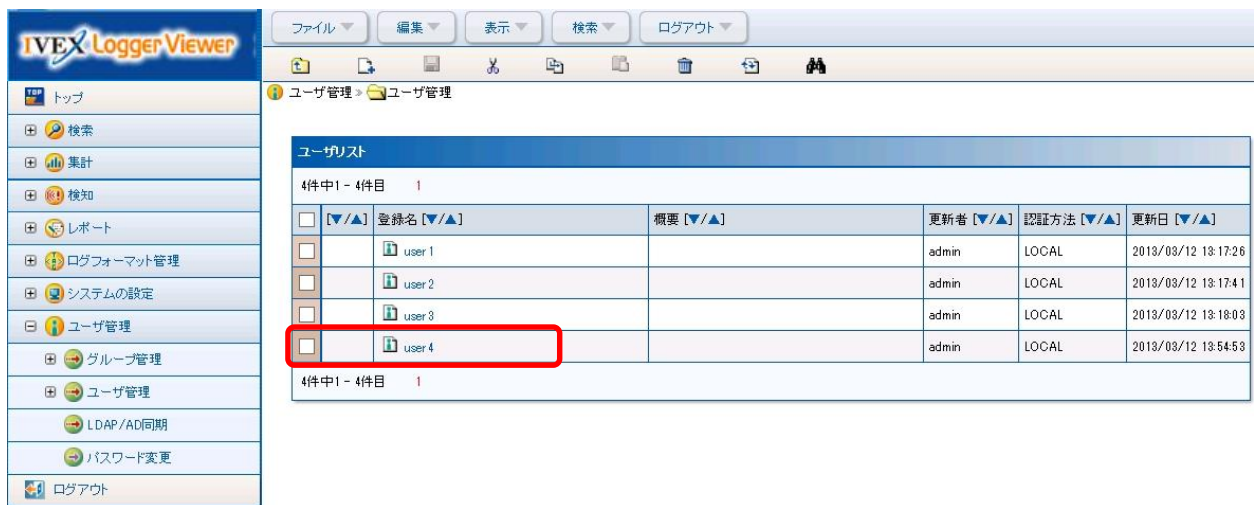
(8)メニューの「ファイル」→「名前を付けて保存」を選択し、「ユーザ名」を入力し「OK」を選択します。



IVEX Logger Viewer 内部認証のユーザ名の文字最大値は 1024 バイトです。また、大文字、小文字の区別はありますが、利用可能な文字の制限は特にありません。

6. グループ/ユーザを管理する

(9)フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示し、作成したユーザが表示されることを確認します。



The screenshot shows the IVE X Logger Viewer application interface. The left sidebar contains a list of menu items, with 'ユーザ管理' (User Management) selected. The main window displays the 'ユーザリスト' (User List) screen. At the top, there is a toolbar with buttons for 'ファイル' (File), '編集' (Edit), '表示' (View), '検索' (Search), and 'ログアウト' (Logout). Below the toolbar, there is a breadcrumb navigation bar showing 'ユーザ管理 > ユーザ管理'. The main content area is a table titled 'ユーザリスト' (User List) with the following columns: '登録名' (Registered Name), '概要' (Overview), '更新者' (Updater), '認証方法' (Authentication Method), and '更新日' (Update Date). The table contains 4 rows of data, with the first row highlighted by a red box. The data is as follows:

登録名	概要	更新者	認証方法	更新日
user 1		admin	LOCAL	2013/03/12 13:17:26
user 2		admin	LOCAL	2013/03/12 13:17:41
user 3		admin	LOCAL	2013/03/12 13:18:03
user 4		admin	LOCAL	2013/03/12 13:54:53

以上が一般ユーザの作成の操作となります。

6. グループ/ユーザを管理する

6.4. ユーザを削除する

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。

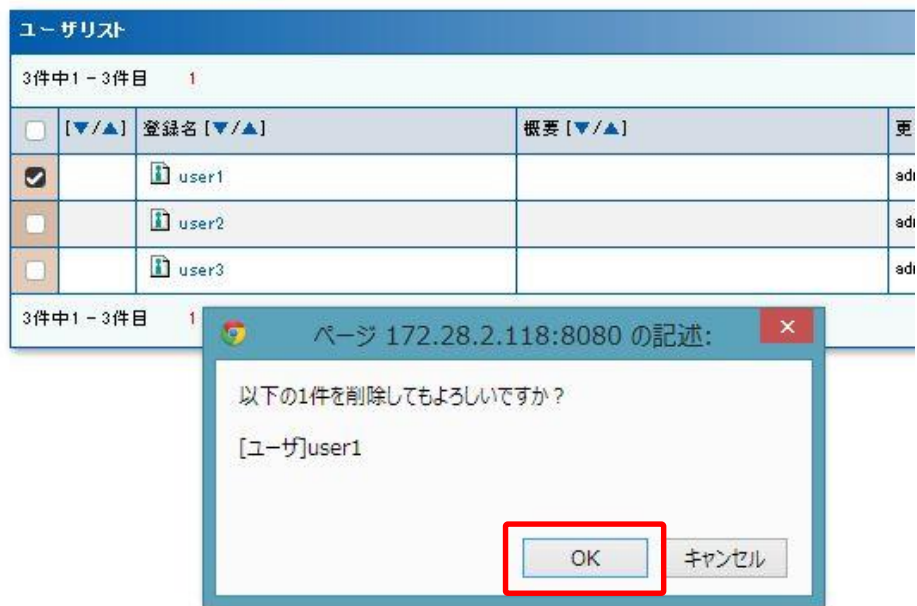


- (2) ユーザリスト画面で削除するユーザにチェックを入れ、メニューの「ファイル」→「削除」を選択します。



6. グループ/ユーザを管理する

(3) 確認ダイアログの表示内容を確認し、問題がなければ「OK」を選択します。



(4) ユーザリスト画面から削除されたことを確認します。



以上がユーザ削除の操作となります。

6. グループ/ユーザを管理する

6.5. ユーザパスワードを変更する

ユーザパスワードの変更は管理者によるものとユーザが自身で変更する場合と 2 通り存在します。また、パスワードを変更する契機として管理者(若しくは)ユーザが自ら変更する場合と、パスワードの有効期間が切れた後にログインする場合と 2 通りが存在します。

以降ではそれぞれについてパスワード変更手順を説明します。

6.5.1. 管理者によるパスワード変更

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。



- (2) 「ユーザリスト画面」からパスワードを変更するユーザの「登録名」リンクを選択して「グループ設定タブ画面」を表示します。



6. グループ/ユーザを管理する

- (3) 「認証設定」タブを選択し「IVEX Logger Viewer 内部認証」欄の「パスワードを変更する」にチェックし、新しいパスワードを入力します。

IVEX Logger Viewer

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

ユーザ管理 > ユーザ管理 > user1

ユーザ名: user1
概要:

グループ設定 操作権限 **認証設定**

ユーザを利用可能にする: ☒

☒ Logstorage内部認証

パスワードを変更する: ☒

パスワード:
パスワード(確認):

☐ LDAP/AD認証

ベースDNテンプレート設定
userDNpart =

キャンセル

- (4) メニューの「ファイル」→「上書き保存」を選択し、完了したことを確認します。

IVEX Logger Viewer

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

名前を付けて保存
上書き保存

user1

ユーザ名: user1
概要:

グループ設定 操作権限 **認証設定**

ユーザを利用可能にする: ☒

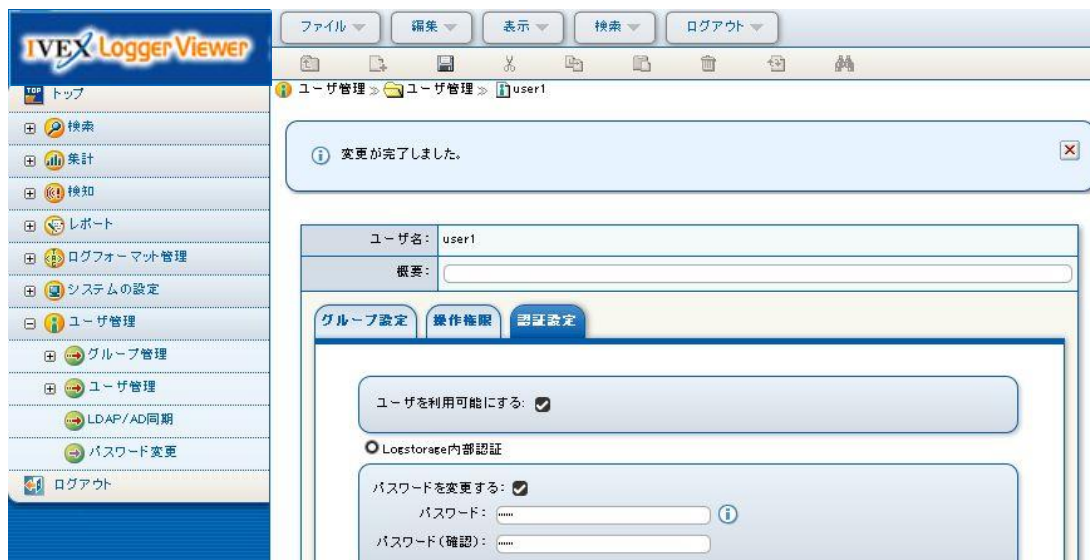
☒ Logstorage内部認証

パスワードを変更する: ☒

パスワード:
パスワード(確認):

☐ LDAP/AD認証

6. グループ/ユーザを管理する



以上がパスワード変更の操作となります。

6. グループ/ユーザを管理する

6.5.2. ユーザ自身によるパスワード変更

- (1) パスワードを変更するユーザでコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「パスワード変更」を選択し、「認証設定タブ画面」を表示します。

The screenshot shows the IVE X Logger Viewer application. The left sidebar contains a menu with items: トップ, 検索, 集計, 検知, ユーザ管理, パスワード変更, and ログアウト. The 'ユーザ管理' and 'パスワード変更' items are highlighted with red rectangular boxes. The main window displays the 'パスワード変更' screen. At the top, there is a header bar with buttons: ファイル, 編集, 表示, 検索, and ログアウト. Below this, a breadcrumb trail shows 'ユーザ管理 > パスワード変更'. The main content area has a tab labeled '認証設定'. Below the tab, there are three input fields: '現在のパスワード:', '変更したいパスワード:', and '変更したいパスワード(確認):'. The user name 'user1' is displayed in the top left of the main content area.

- (2) 表示されている「現在のパスワード」「変更したいパスワード」「変更したいパスワード(確認)」欄それぞれを入力します。

This screenshot is similar to the previous one, showing the 'パスワード変更' screen. A red rectangular box highlights the three password input fields: '現在のパスワード:', '変更したいパスワード:', and '変更したいパスワード(確認):'. The rest of the interface, including the sidebar and header, is identical to the previous screenshot.

6. グループ/ユーザを管理する

(3) メニューの「ファイル」→「上書き保存」を選択し、完了したことを確認します。

The image displays two screenshots of the IVE X Logger Viewer web application interface, illustrating the password change process.

Top Screenshot: The application is in the 'パスワード変更' (Password Change) section. The 'ファイル' (File) menu is open, and the '上書き保存' (Save Overwrite) option is highlighted with a red box. The breadcrumb trail shows 'ユーザ管理 > パスワード変更'. The form contains the following fields:

- ユーザ名: user1
- 概要:
- 認証設定 (tab):
- 現在のパスワード: [password field]
- 変更したいパスワード: [password field]
- 変更したいパスワード(確認): [password field]

Bottom Screenshot: The application shows a confirmation message: '変更が完了しました。' (Change completed.). The breadcrumb trail remains 'ユーザ管理 > パスワード変更'. The form fields are identical to the top screenshot.

以上がパスワード変更の操作となります。

6. グループ/ユーザを管理する

6.5.3. パスワード有効期限が切れた後のパスワード変更

- (1) パスワードの有効期限が切れたユーザでコンソールサーバへログインを行うと下図のパスワード変更画面が表示されます。

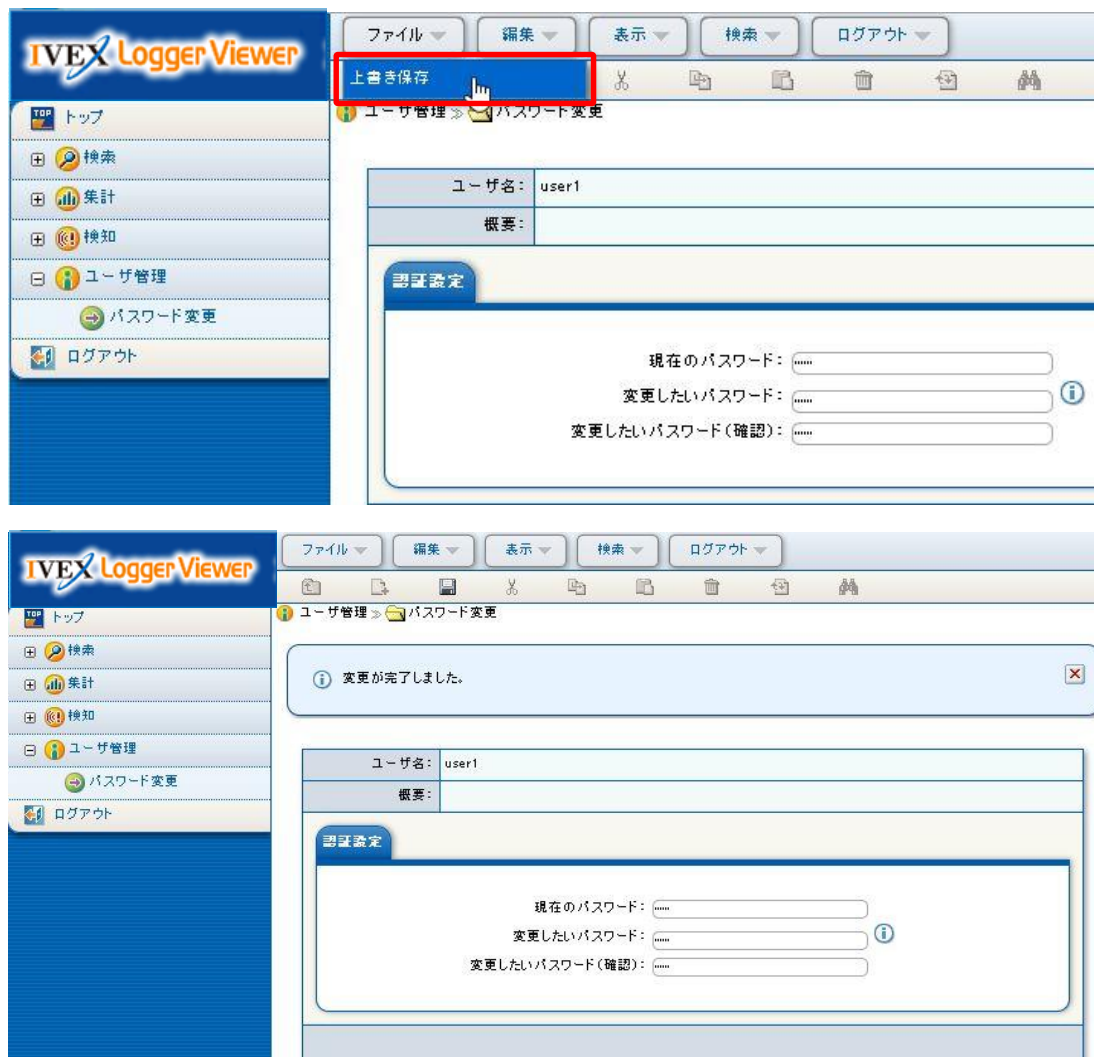
The screenshot shows a web interface for password management. At the top, there is a navigation bar with buttons: 'ファイル' (File), '編集' (Edit), '表示' (View), '検索' (Search), and 'ログアウト' (Logout). Below this is a toolbar with icons for file operations. The main content area has a header with 'ユーザ名: user 1' and '概要:'. Below the header is a section titled '認証設定' (Authentication Settings). Inside this section, there are three input fields: '現在のパスワード:' (Current Password), '変更したいパスワード:' (New Password), and '変更したいパスワード(確認):' (New Password Confirmation). An information icon (i) is located to the right of the new password fields.

- (2) 表示されている「現在のパスワード」「変更したいパスワード」「変更したいパスワード(確認)」欄それぞれを入力します。

This screenshot shows the same password change interface as the previous one, but with the three input fields highlighted by a red rectangle. The fields are: '現在のパスワード:' (Current Password), '変更したいパスワード:' (New Password), and '変更したいパスワード(確認):' (New Password Confirmation). Each field now contains a series of black dots, indicating that the user has entered a password. The information icon (i) remains to the right of the new password fields.

6. グループ/ユーザを管理する

(3) メニューの「ファイル」→「上書き保存」を選択し、完了したことを確認します。



(4) ログイン直後のトップページが表示されることを確認します。



以上がパスワード変更の操作となります。

6. グループ/ユーザを管理する

6.6. 管理者グループの所属ユーザを変更する

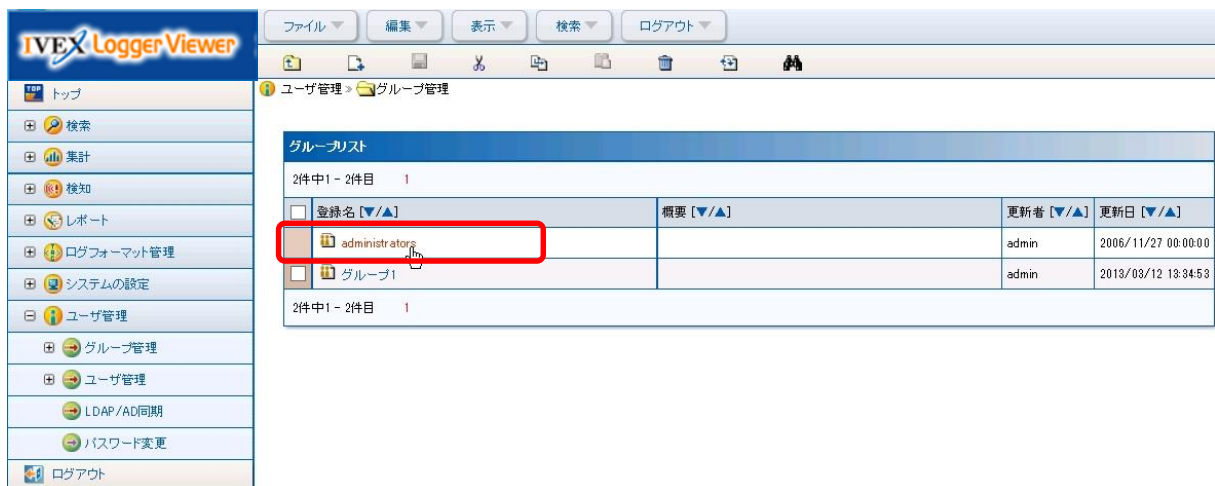
- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「グループ管理」を選択し、「グループリスト画面」を表示します。

The screenshot shows the IVE X Logger Viewer application interface. The left sidebar contains a list of menu items, with 'ユーザ管理' (User Management) and 'グループ管理' (Group Management) highlighted by red rectangles. The main content area displays the 'グループリスト' (Group List) screen, which includes a table of groups.

登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	更新日 [▼/▲]
administrators		admin	2006/11/27 00:00:00
グループ1		admin	2013/03/12 13:34:53

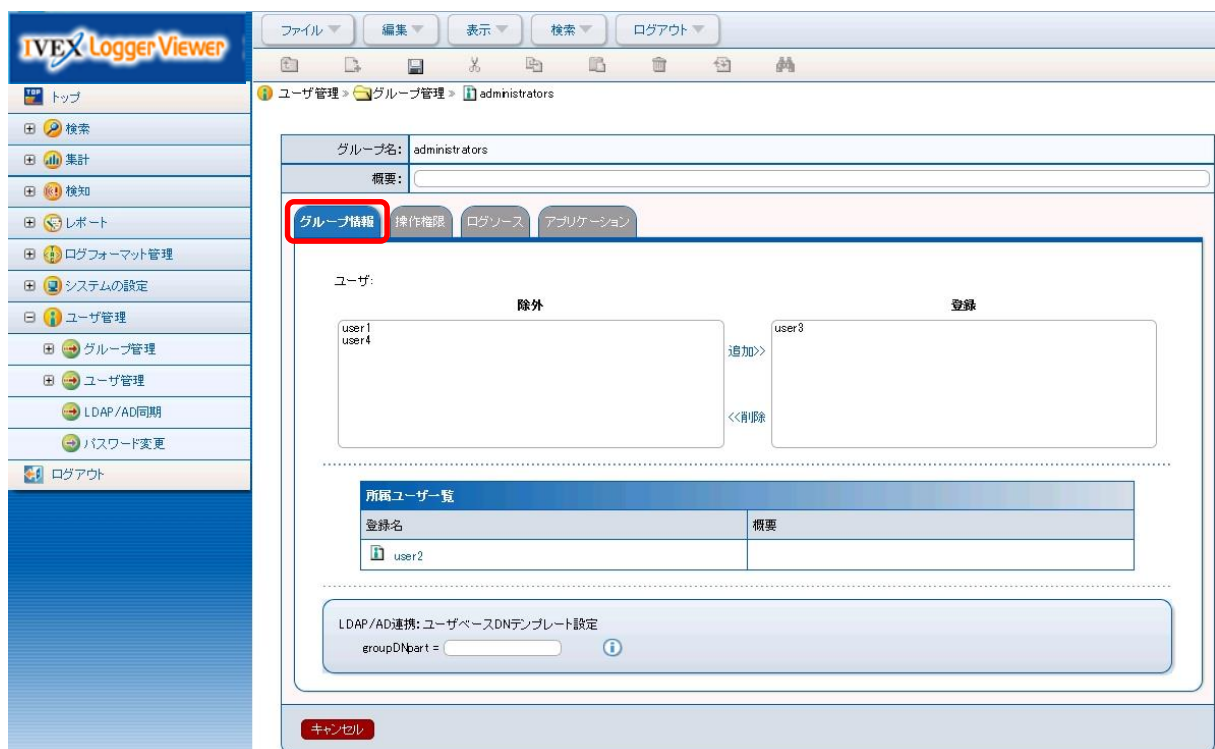
6. グループ/ユーザを管理する

(2)「グループリスト画面」から「administrators」を選択し、「グループ情報タブ画面」を表示します。



グループリスト

登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	更新日 [▼/▲]
administrators		admin	2006/11/27 00:00:00
グループ1		admin	2013/03/12 13:34:53



グループ名: administrators

概要:

グループ情報 | 操作権限 | ログソース | アプリケーション

ユーザ:

除外: user1, user4

登録: user3

追加>> <<削除

所属ユーザ一覧

登録名	概要
user2	

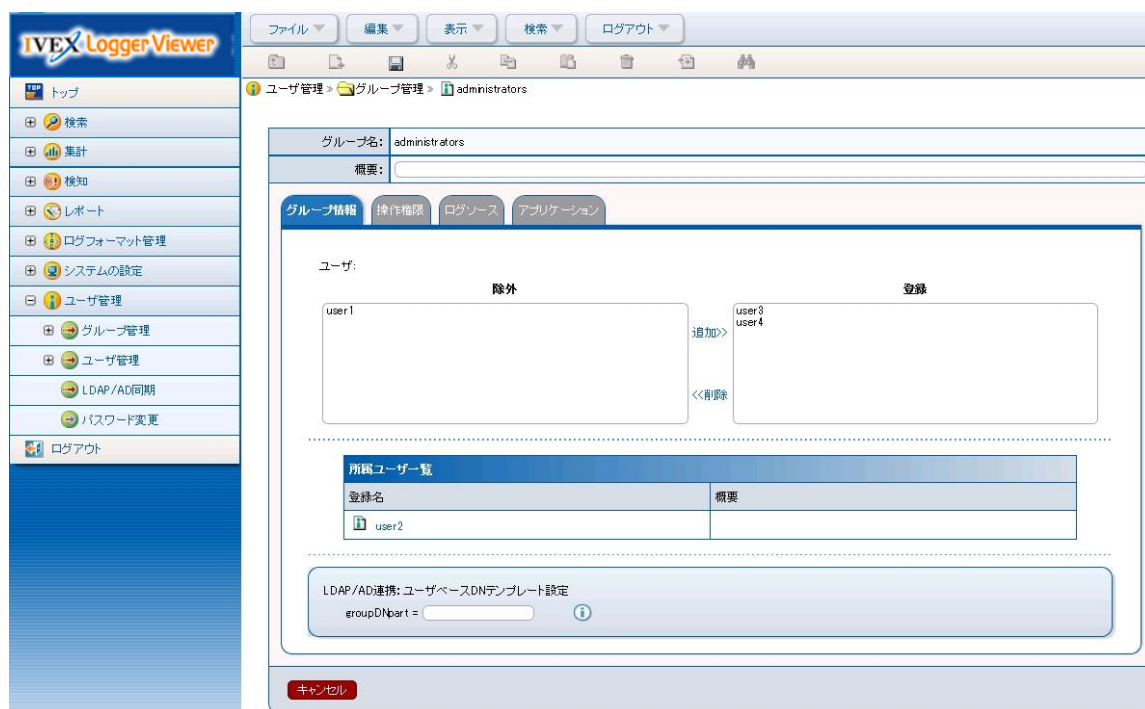
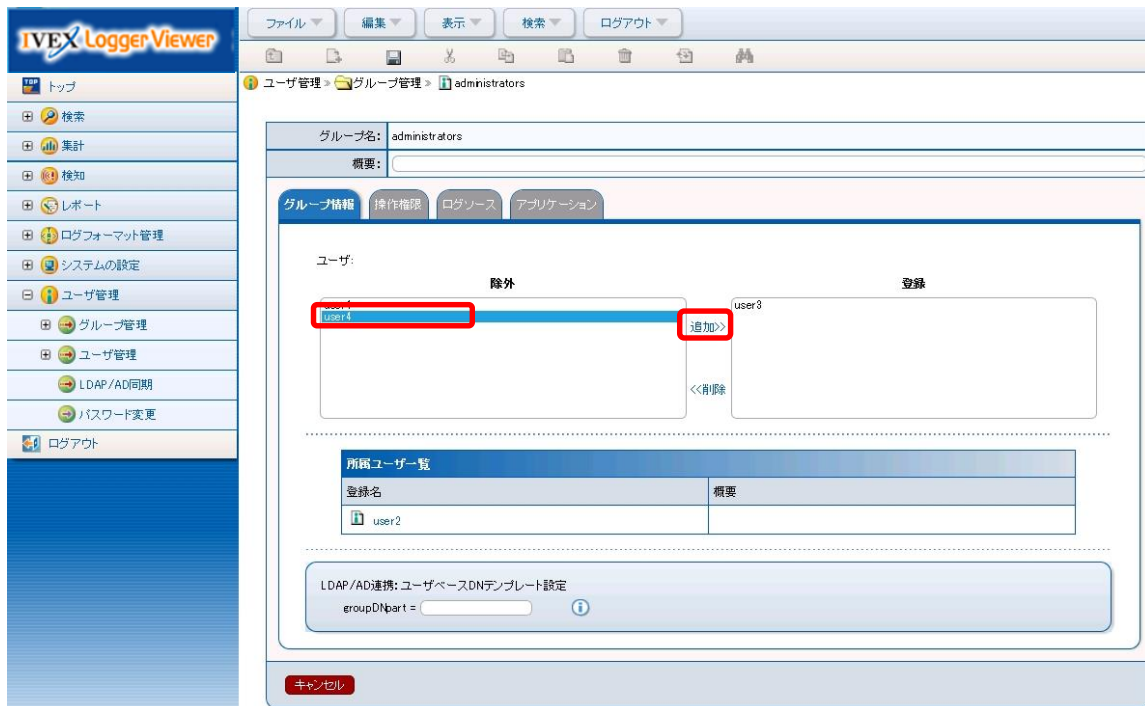
LDAP/AD連携: ユーザベースDNテンプレート設定

groupDNpart =

キャンセル

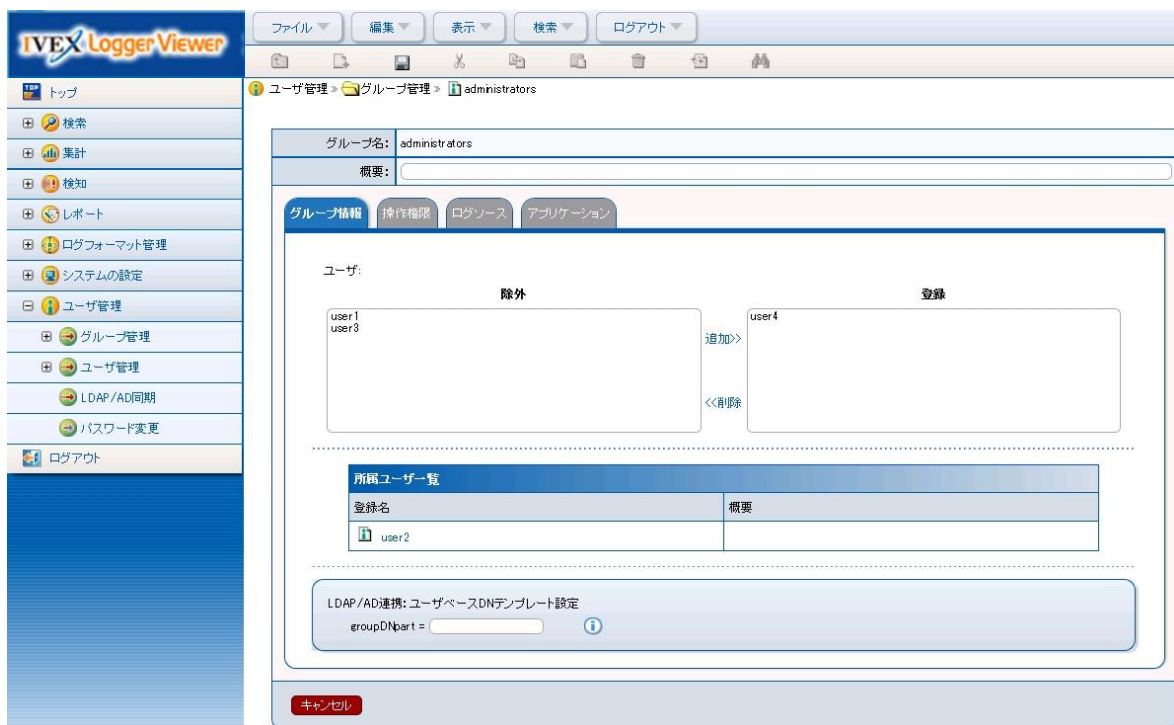
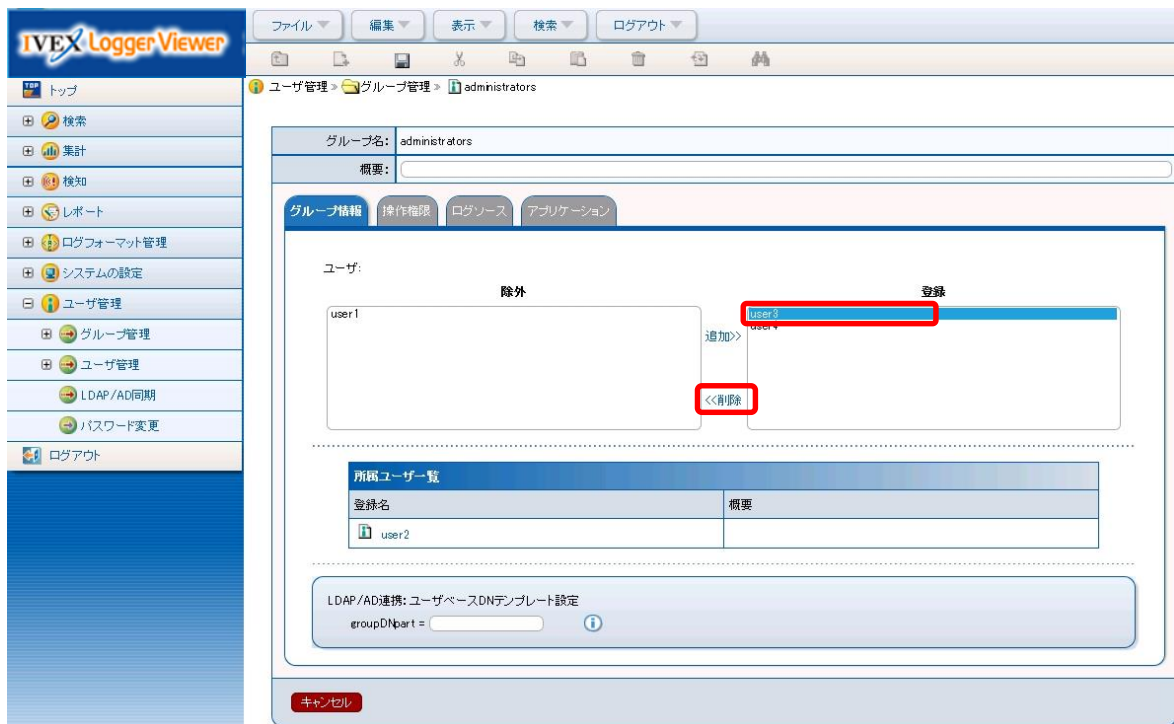
6. グループ/ユーザを管理する

(3)「グループ情報タブ画面」から管理者グループに所属させるユーザを選択し、追加>>ボタン選択します。



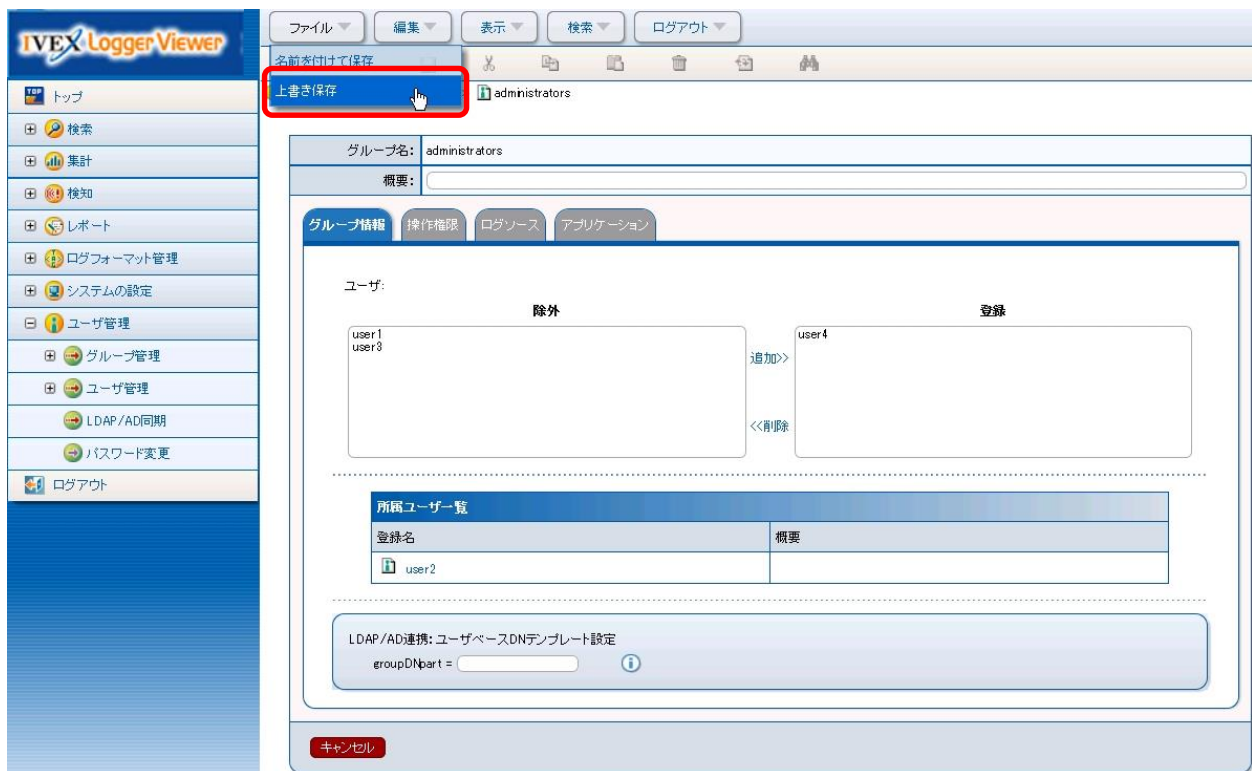
6. グループ/ユーザを管理する

(4)「グループ情報タブ画面」から管理者グループに所属させないユーザを選択し、<<削除ボタン選択します。



6. グループ/ユーザを管理する

(3) メニューの「ファイル」→「上書き保存」を選択します。



(3) 以下のメッセージが表示されます。

変更が完了しました。

以上が管理者グループの所属ユーザを変更する操作となります。

6. グループ/ユーザを管理する

6.7. ユーザをロックする、ロック解除する

ユーザのロック・ロック解除の方法について説明をします。

6.7.1. ユーザをロックする

画面よりユーザをロックする手順は、以下【A】【B】の2通りあります。また、ログインポリシーにてロックすることも可能です。ログインポリシーについては、「8.7.ユーザ認証を設定する」で説明しています。

【A】ユーザリスト画面よりロックする(複数指定可能)

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。



The screenshot displays the IVE X Logger Viewer application interface. On the left, a sidebar contains various management options, with 'ユーザ管理' (User Management) highlighted by a red rectangle. The main content area shows the 'ユーザリスト' (User List) table, which contains four users. The table has columns for selection checkboxes, login names, summaries, updaters, authentication methods, and update dates.

	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 13:17:41
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

6. グループ/ユーザを管理する

(2)「ユーザリスト画面」からロックしたいユーザを選択し、メニューの「ファイル」→「ロック」を選択します。

The screenshot shows the IVE X Logger Viewer application. On the left is a sidebar with various menu items. The main window has a top menu bar with 'ファイル' (File), '編集' (Edit), '表示' (View), '検索' (Search), and 'ログアウト' (Logout). Below the menu bar is a toolbar with icons for file operations. A dropdown menu is open under 'ファイル', showing options like 'ファイル作成', 'フォルダ作成', 'ユーザ管理', '名前変更', '削除', 'ロック' (highlighted with a red box), 'ロック解除', 'エクスポート', and '全てエクスポート'. Below the menu, there is a table of users. The first column has checkboxes, and the second column has user names. 'user 3' is highlighted with a red box, and its checkbox is checked. The table has columns for '更新者' (Updater), '認証方法' (Authentication Method), and '更新日' (Update Date).

	更新者【▼/▲】	認証方法【▼/▲】	更新日【▼/▲】
<input type="checkbox"/>	admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	admin	LOCAL	2013/03/12 13:17:41
<input checked="" type="checkbox"/>	admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	admin	LOCAL	2013/03/12 13:54:53

(3) 当該ユーザに鍵マークが表示されることを確認します。

The screenshot shows the IVE X Logger Viewer application with the 'ユーザ管理' (User Management) menu item selected. The main window displays a 'ユーザリスト' (User List) table. The first column has checkboxes, and the second column has user names. 'user 3' is highlighted with a red box, and a lock icon is visible next to its name. The table has columns for '更新者' (Updater), '認証方法' (Authentication Method), and '更新日' (Update Date).

	登録名【▼/▲】	更新者【▼/▲】	認証方法【▼/▲】	更新日【▼/▲】
<input type="checkbox"/>	user 1	admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2	admin	LOCAL	2013/03/12 13:17:41
<input checked="" type="checkbox"/>	user 3	admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4	admin	LOCAL	2013/03/12 13:54:53

6. グループ/ユーザを管理する

【B】ユーザの認証設定画面よりロックする

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。

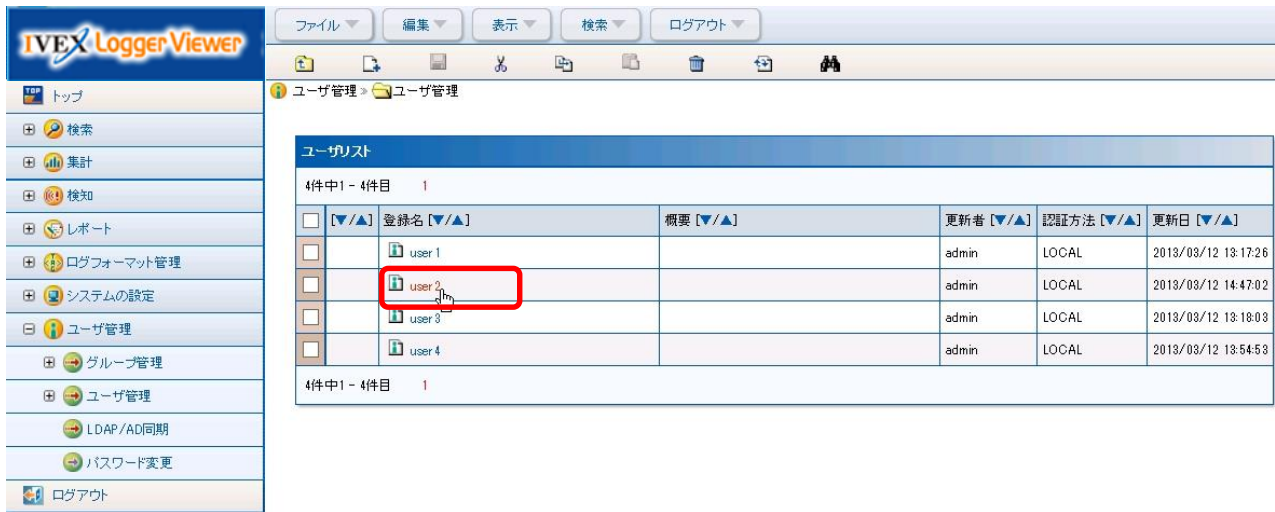


The screenshot shows the IVE X Logger Viewer application. The left sidebar contains a menu with the following items: トップ, 検索, 集計, 検知, レポート, ログフォーマット管理, システムの設定, ユーザ管理 (highlighted with a red box), グループ管理, ユーザ管理 (highlighted with a red box), LDAP/AD同期, パスワード変更, and ログアウト. The main area displays the 'ユーザリスト' (User List) table, which contains 4 items. The table has columns for selection, name, summary, updater, authentication method, and update date.

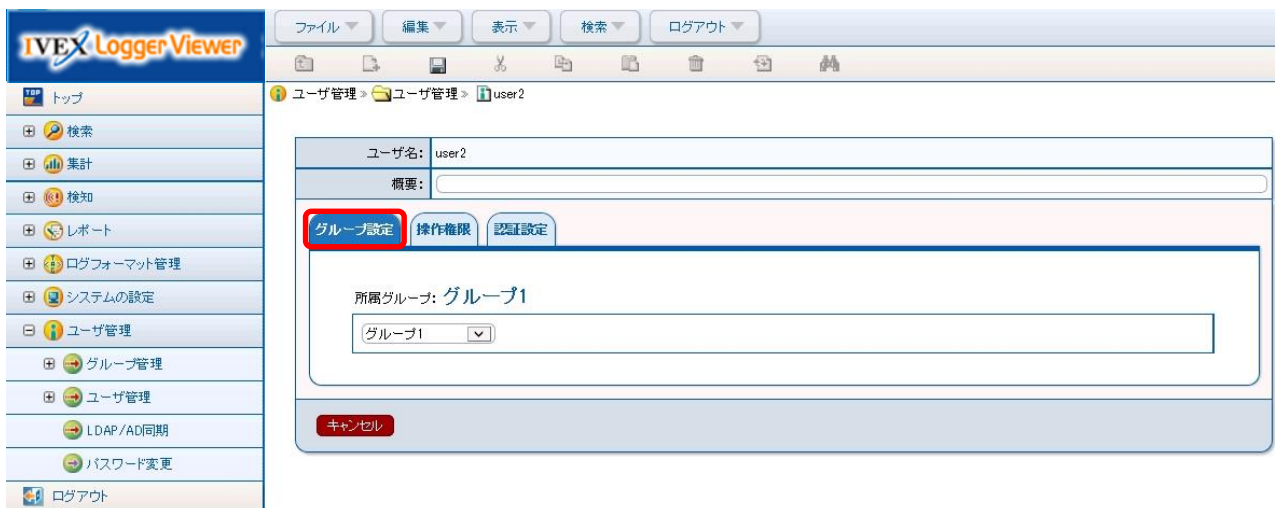
	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 13:17:41
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

6. グループ/ユーザを管理する

(2)「ユーザリスト画面」からロックしたいユーザを選択し、「グループ設定タブ画面」を表示します。



<input type="checkbox"/>	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input checked="" type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 14:47:02
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53



ユーザ名: user 2

概要:

グループ設定 | 操作権限 | 認証設定

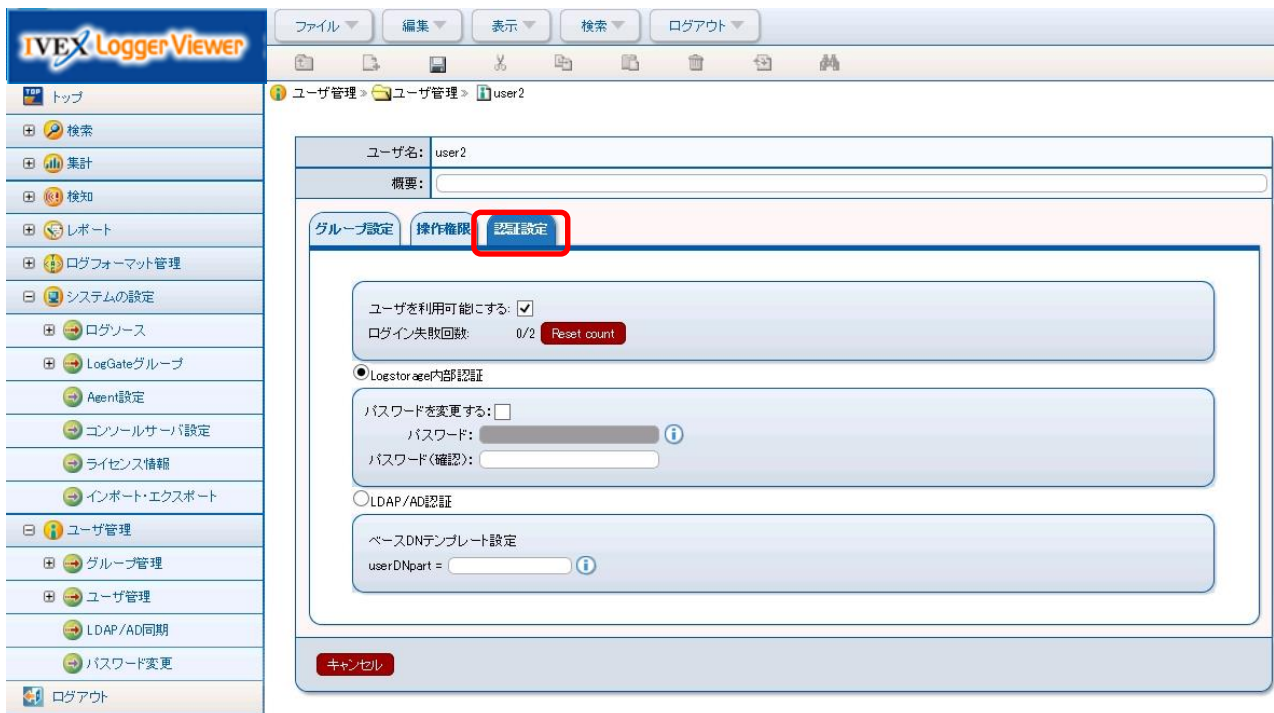
所属グループ: グループ1

グループ1 ▼

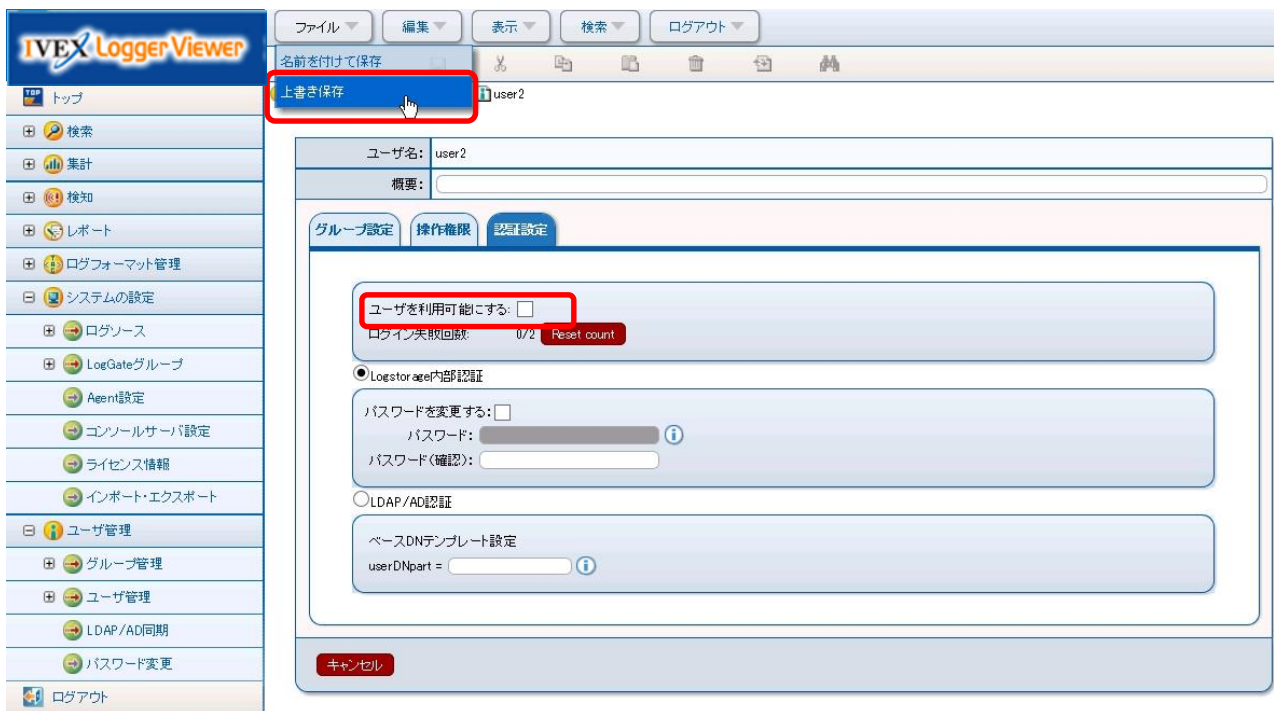
キャンセル

6. グループ/ユーザを管理する

(3)「認証設定タブ」を選択し、「認証設定タブ画面」を表示します。

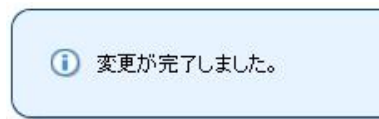


(4)「認証設定タブ画面」で「ユーザを利用可能にする」のチェックを外し、メニューの「ファイル」→「上書き保存」を選択します。



6. グループ/ユーザを管理する

(3) 以下のメッセージが表示されます。



以上がユーザロックの操作となります。

6. グループ/ユーザを管理する

6.7.2. ユーザをロック解除する

画面よりユーザをロック解除する手順は、以下【A】【B】の2通りあります。また、ログインポリシー及び管理コマンドにてロック解除することも可能です。ログインポリシーについては、「8.7.ユーザ認証を設定する」で説明しています。管理コマンドについては、「E.29.IVEX Logger Viewer ユーザロック解除コマンド」で説明しています（尚、製品インストール時に自動的にビルトインされるシステム管理ユーザ「admin」がロックされた場合も同章の管理コマンドを用いてロックを解除してください）。

【A】ユーザリスト画面よりロック解除する（複数指定可能）

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。

The screenshot displays the IVEX Logger Viewer web application. On the left, a sidebar menu contains various system management options, with 'ユーザ管理' (User Management) highlighted in red. The main content area shows the 'ユーザリスト' (User List) table. The table has columns for selection, login name, password, updater, authentication method, and update date. Four users are listed: user 1, user 2, user 3, and user 4. The 'user 4' row is highlighted in red.

<input type="checkbox"/>	登録名 [▼/▲]	パスワード [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 14:51:03
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

6. グループ/ユーザを管理する

(2)「ユーザリスト画面」からロック解除したいユーザを選択し、メニューの「ファイル」→「ロック解除」を選択します。

The screenshot shows the IVE X Logger Viewer application. On the left is a sidebar with various menu items. The main window has a top menu bar with 'ファイル' (File), '編集' (Edit), '表示' (View), '検索' (Search), and 'ログアウト' (Logout). Below the menu bar is a toolbar with icons for file operations. A dropdown menu is open under 'ファイル', showing options like 'ファイル作成', 'フォルダ作成', '名前変更', '削除ユーザリスト', 'ロック解除' (highlighted with a red box), 'エクスポート', and '全てエクスポート'. Below the menu is a table of users. The table has columns for selection, user name, summary, updater, authentication method, and update date. The row for 'user 4' is highlighted with a red box, and its selection checkbox is checked.

		概要【▼/▲】	更新者【▼/▲】	認証方法【▼/▲】	更新日【▼/▲】
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:18:03
<input checked="" type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

4件中1 - 4件目 1

(3) 当該ユーザに鍵マークが表示されないことを確認します。

The screenshot shows the IVE X Logger Viewer application with the 'ユーザ管理' (User Management) menu item selected. The main window displays a table titled 'ユーザリスト' (User List). The table has columns for selection, user name, summary, updater, authentication method, and update date. The row for 'user 4' is highlighted with a red box, and its selection checkbox is checked. The table shows 4 items in total, with the first item being 'user 4'.

	登録名【▼/▲】	概要【▼/▲】	更新者【▼/▲】	認証方法【▼/▲】	更新日【▼/▲】
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 14:51:03
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input checked="" type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

4件中1 - 4件目 1

6. グループ/ユーザを管理する

【B】ユーザの認証設定画面よりロック解除する

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「ユーザ管理」→「ユーザ管理」を選択し、「ユーザリスト画面」を表示します。



The screenshot shows the IVE X Logger Viewer application. The left sidebar contains a menu with the following items: トップ (Top), 検索 (Search), 集計 (Summary), 検知 (Detection), レポート (Report), ログフォーマット管理 (Log Format Management), システムの設定 (System Settings), ユーザ管理 (User Management), グループ管理 (Group Management), ユーザ管理 (User Management), LDAP/AD同期 (LDAP/AD Synchronization), パスワード変更 (Password Change), and ログアウト (Logout). The 'ユーザ管理' (User Management) item is selected and highlighted with a red box. The main area displays a table of users.

	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	認証方法 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	user 1		admin	LOCAL	2013/03/12 13:17:26
<input type="checkbox"/>	user 2		admin	LOCAL	2013/03/12 14:51:03
<input type="checkbox"/>	user 3		admin	LOCAL	2013/03/12 13:18:03
<input type="checkbox"/>	user 4		admin	LOCAL	2013/03/12 13:54:53

6. グループ/ユーザを管理する

(2)「ユーザリスト画面」からロック解除したいユーザを選択し、「グループ設定タブ画面」を表示します。

ユーザー管理

登録名	概要	更新者	認証方法	更新日
user 1		admin	LOCAL	2013/03/12 13:17:26
user 2		admin	LOCAL	2013/03/12 14:51:03
user 3		admin	LOCAL	2013/03/12 13:18:03
user 4		admin	LOCAL	2013/03/12 13:54:53

ユーザー名: user4

概要:

グループ設定 操作権限 認証設定

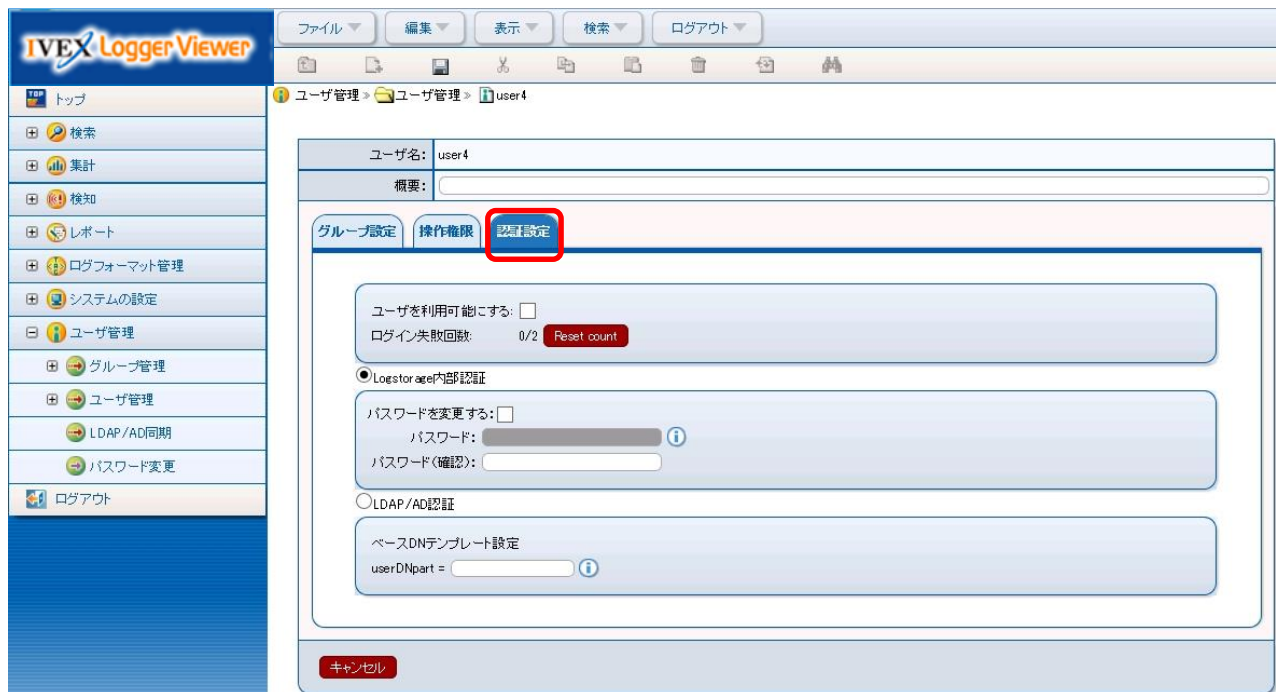
所属グループ: グループ1

グループ1

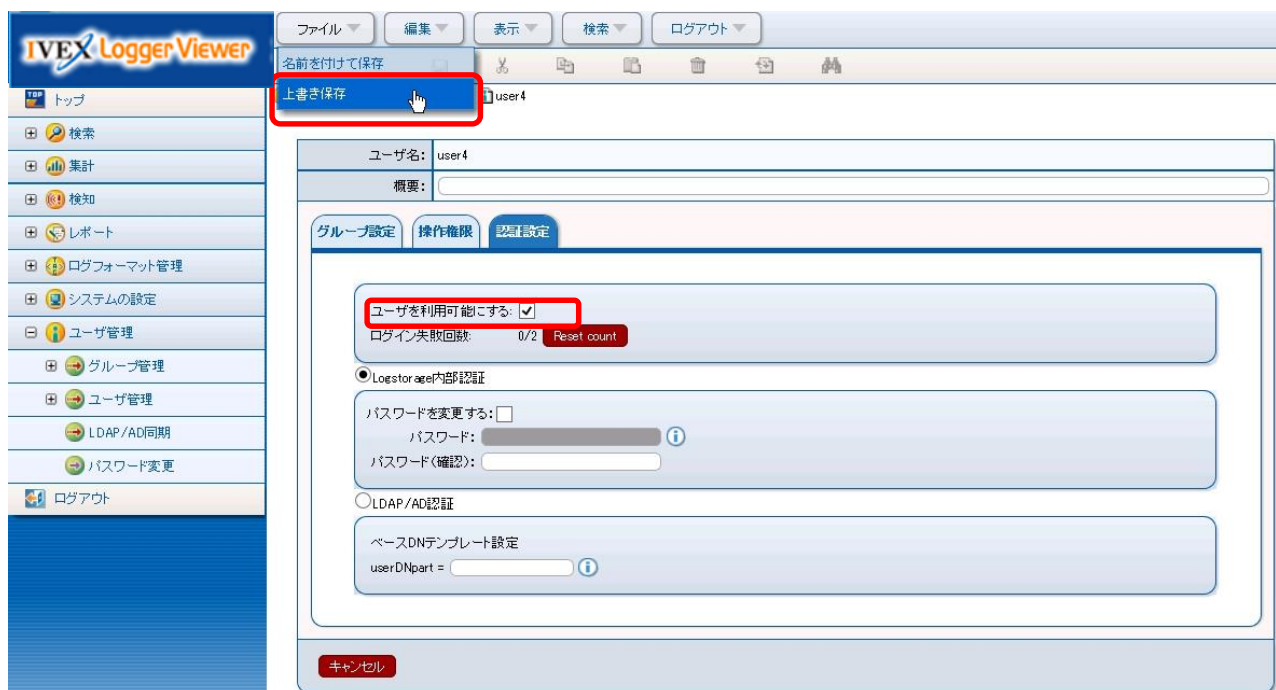
キャンセル

6. グループ/ユーザを管理する

(3)「認証設定タブ」を選択し、「認証設定タブ画面」を表示します。

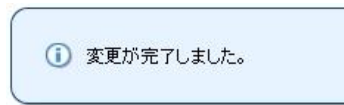


(4)「認証設定タブ画面」で「ユーザを利用可能にする」を選択し、メニューの「ファイル」→「上書き保存」を選択します。



6. グループ/ユーザを管理する

(3) 以下のメッセージが表示されます。



以上がユーザロック解除の操作となります。

7. ログソースを設定する

7.1. ログソース設定変更時の注意事項

管理対象機器のログデータを管理する場合はそのログデータを出力したログソース設定を行っておく必要があります。IVEX Logger Viewer が管理するログデータは、特定のログソースの IP アドレスが含まれます。コンソールサーバ上で操作するログデータの検索・集計・検知・レポート・ログフォーマット定義は、登録されたログソースのログデータを前提としています。

7.1.1. ログソースを新規追加した場合（大規模対応時）

ログソースが登録される以前に収集されたログも構造化します。ただし検索はできません。新しくログソースを追加した時点で検索ができるようになります。LogGate 設定タブで「未登録ログソースからのログを破棄する」にチェックがある場合、登録されていないログソースのログは受信時に破棄されます。そのため、ログソースを新規追加する前にログソースのログを受信しても破棄されます。

7.1.2. ログソースを削除した場合

既に検索・集計・検知・レポートの条件に該当するログソースが設定されている場合、ログソースの削除は出来ません。条件を変更あるいは削除してから、ログソースを削除してください。ログソースを削除してもそのログソースの LogDB 情報は保存されています。LogGate 設定タブで「未登録ログソースからのログを破棄する」にチェックがある場合、登録されていないログソースのログは受信時に破棄されます。そのため、ログソースを削除した際は、変更前のログソースのログは次回受信時に破棄されます。

7.1.3. ログソースを変更した場合

ログソースの名前を変更した場合は、既に設定されている検索・集計・検知・レポートの条件から該当するログソース部分の名前が変更されます。

IP アドレスを変更した場合は、変更した時点以降から該当する IP アドレスのログデータを検索できるようになります。以前に収集したログデータを検索するには当時の IP アドレスで別にログソースを登録する必要があります。なお、LogGate 設定タブで「未登録ログソースからのログを破棄する」にチェックがある場合、登録されていないログソースのログは受信時に破棄されます。そのため、ログソースを変更した際は、変更前のログソースのログは次回受信時に破棄されます。

8. その他システム設定を行う

8.1. コンソールサーバ/LogGate が使用するメールサーバを設定する

コンソールサーバ/LogGate が使用するメールサーバを設定する方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「メールタブ画面」を表示します。



The screenshot shows a web interface with a blue header bar containing several tabs: 'メール' (Mail), '検索機能' (Search Function), '集計機能' (Aggregation Function), '検知機能' (Detection Function), 'レポート機能' (Report Function), 'ユーザ認証' (User Authentication), and 'ロギング' (Logging). The 'メール' tab is selected and highlighted. Below the tabs, there are three input fields for email server configuration: 'メールサーバ:' (Mail Server) with the value 'localhost', '差出人:' (Sender) with the value 'admin@localhost', and 'お問い合わせ先:' (Contact Information).

8. その他システム設定を行う

(2)「メールタブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 11 メールタブ設定項目

設定項目	既定値	設定内容
メールサーバ	localhost	コンソールサーバがレポートに関するメールの送信時に使用するメールサーバ名を指定します。コンソールサーバからメールを送付する際、ヘッダは Shift_JIS で MIME(Base64)エンコードし、本文は Quoted-Printable となっております。 MIME エンコード(Shift_JIS)のヘッダをメールサーバ側で正しく扱えていない場合や、ヘッダ部分に機種依存文字を使用している場合は送信先のメールでメールが文字化けして届くことがあります。 なお、IVEX Logger Viewer 側でエンコーディングの設定は変更できません。
差出人	admin@localhost	IVEX Logger Viewer がメール送信時に使用するメールの差出人を設定します。 差出人はエンベロープ From に指定されるメールアドレスです。このメールアドレスでメールが受信できるようメールサーバに登録する必要はありません。
お問い合わせ先	空白 (試用版と正式版では既定値が異なります。)	コンソールサーバログイン後のトップページに表示されるお問い合わせ先を指定します。 試用版では試用中のお問い合わせ先が表示されます。正式版ではサポート契約者専用の窓口メールアドレスが表示されます。

8. その他システム設定を行う

(3) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate;詳細設定」ボタン→「検知」を選択します。

(4) 検知画面の設定を変更します。

The screenshot displays the LogGate configuration interface. On the left is a sidebar menu with the following items: ステータス, ログ収集 (expanded), ログ転送, ワーク先, 検知 (selected), ログ出力, and 設定管理. The 'ログ収集' section is expanded, showing sub-items: Syslog(年補正), Syslog(UDP), Syslog(TCP), Syslog(TLS), LLTP, and SNMP. The 'FTP' section is also expanded, showing: ユーザ, FTP取り込み, and 接続モード. The 'ファイルシステム監視' section shows: ファイル取り込み. The main content area is titled '検知' (Detection). It contains the following settings: '検知履歴を保存する' (Save detection history) with a checked checkbox and an information icon; '検知メールのメールサーバ' (Detection email mail server) set to 'localhost' with an information icon; '検知メールのメール送信者アドレス' (Detection email sender address) set to 'admin@localhost' with an information icon; and '検知スレッド数' (Detection thread count) set to '2' with an information icon. At the top of the sidebar, there is a 'LogGate設定' (LogGate Settings) header with the version 'b(127.0.0.1)' and two buttons: '設定を確認し保存' (Check settings and save) and 'キャンセル' (Cancel).

(5) 「設定を確認し保存」ボタンを選択します。

(6) 「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

LogGate 及びコンソールサーバの再起動は不要です。

8. その他システム設定を行う

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

コンソールサーバ設定ファイル(logstd.dcf)／LogGate 設定ファイル(loggate.dcf)

com.Logstorage.share.notice.ActionServer.history

com.Logstorage.share.notice.executer.NoticeMailExecuter.mailServer

com.Logstorage.share.notice.executer.NoticeMailExecuter.mailFrom

検知スレッド数については設定ファイルで変更できません。

表 12 検知画面の設定項目

パラメータ名	既定値	設定内容
com.Logstorage.share.notice.ActionServer.history	true	検知履歴を保存するかどうかのチェックです。 true: 検知履歴を保存する false: 検知履歴を保存しない
com.Logstorage.share.notice.executer.NoticeMailExecuter.mailServer	localhost	LogGate が検知アラートのメール送信時に使用するメールサーバ名を指定します。LogGate からメールを送付する際、ヘッダは Shift_JIS で MIME(Base64) エンコードし、本文は Quoted-Printable となっております。 MIME エンコード(Shift_JIS)のヘッダをメールサーバ側で正しく扱えていない場合や、ヘッダ部分に機種依存文字を使用している場合は送信先のメールでメールが文字化けして届くことがあります。なお、IVEX Logger Viewer 側でエンコーディングの設定は変更できません。
com.Logstorage.share.notice.executer.NoticeMailExecuter.mailFrom	admin@localhost	検知条件の通知設定でメールを選択した場合に送信されるメールの From を指定します。 差出人はエンベロープ From に指定されるメールアドレスです。このメールアドレスでメールが受信できるようメールサーバに登録する必要はありません。

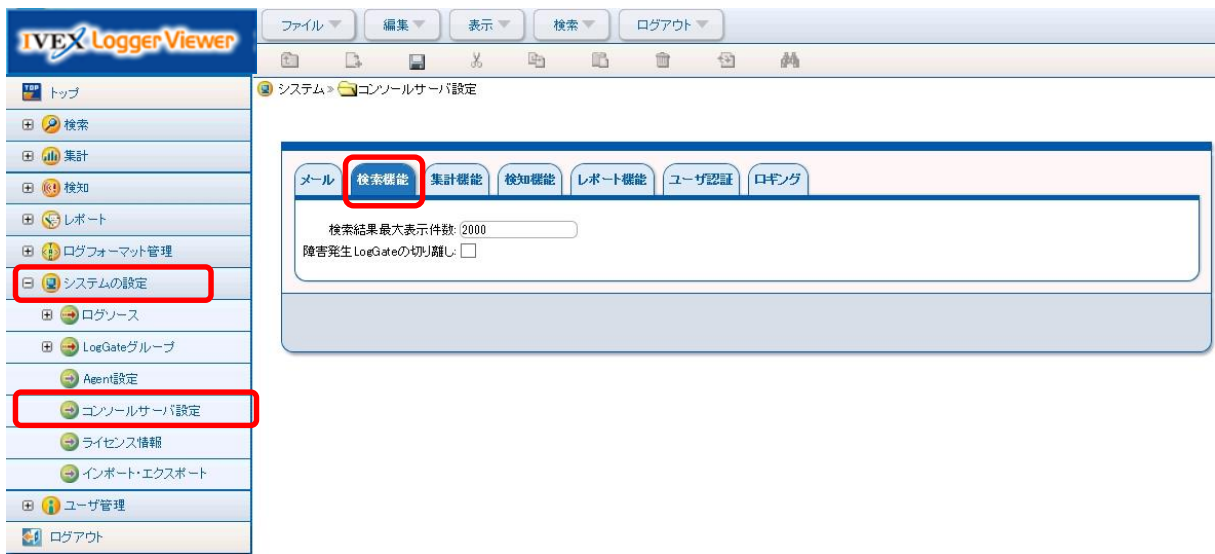
8. その他システム設定を行う

8.2. 検索時に1回で取り出すログ量を設定する

検索時に1回で取り出すログ量の設定する方法を記載します。

※メニュー項目「システム共通設定」は「コンソールサーバ設定」に名称変更しました。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「検索機能タブ画面」を表示します。



- (2) 「検索機能タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

8. その他システム設定を行う

表 13 検索機能タブ設定項目

設定項目	既定値	設定内容
検索結果最大表示件数	2000	検索結果タブに表示される検索結果の最大表示件数を設定します。検索処理での検索結果がここで設定した件数を超えた場合、検索処理を中断して検索結果を出力します。 既定値では検索結果の画面には 2,000 以上という表示が出ます。検索画面の遷移により 2,001 件を超えたログを検索すると次の 2000 件 (2,001 件～4,000 件) が検索結果に表示され、1～2,000 件は検索画面から削除します。1～2,000 件までを再度表示する場合は再検索を行ってください。
障害発生 LogGate の切り離し (アドバンス版のみ表示)	チェックなし	LogGateに障害が発生した場合、障害が発生したLogGateを切り離して運用(検索や集計、検知、レポート作成)を行うかどうかを設定します。 チェック有り: 障害が発生した LogGate を切り離して運用します。 チェックなし: 障害が発生した LogGate は切り離さずに運用します。

以上が検索機能に関する設定です。

8. その他システム設定を行う

8.3. 集計結果の表示とグラフ保存先を設定する

集計結果の表示とグラフ保存先を設定する方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「集計機能タブ画面」を表示します。



8. その他システム設定を行う

(2)「集計機能タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 14 集計機能タブ設定項目

設定項目	既定値	設定内容
集計グラフ出力ディレクトリ	C:¥logstorage¥stats	集計機能でのグラフ出力先ディレクトリを設定します。
数値で無い値の置換設定	文字列置換: #NAN	集計機能の表集計で集計対象ログに含まれる値が数値で無い値であった場合の表示を設定します。 文字列置換 : 設定した文字列を表示します。 (既定値: #NAN) 数値置換 : 設定した数値を表示します。入力する値は数値を設定します。 計算しない : 該当する値を無視します。
計算不能セルに表示する値	文字列置換: #NODATA	集計機能の表集計で該当するログが1件も無く計算ができなかったセルの表示を設定します。 文字列置換 : 設定した文字列を表示します。 (既定値: #NODATA) ゼロ置換 : 値を数値 0 とみなします。数値 0 以外の設定はできません。

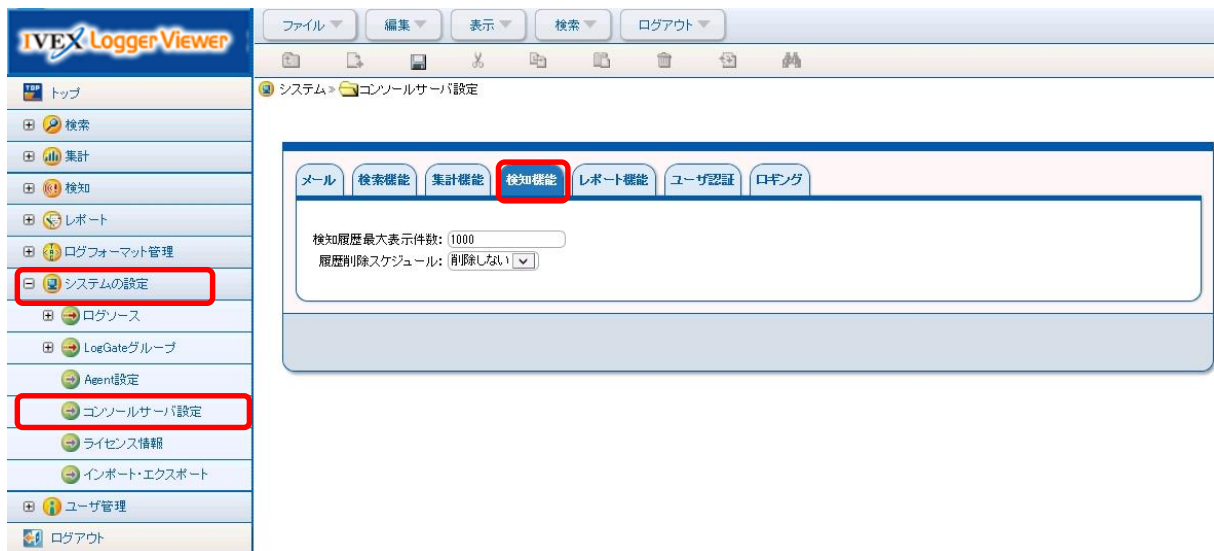
以上が集計機能に関する設定です。

8. その他システム設定を行う

8.4. 検知の履歴削除スケジュールを設定する

検知機能の履歴削除スケジュールの設定方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「検知機能タブ画面」を表示します。



8. その他システム設定を行う

(2)「検知機能タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 15 検知機能タブ設定項目

設定項目	既定値	設定内容
検知履歴最大表示件数	1000	検知履歴の検索結果に表示される検知履歴の最大表示件数を設定します。検知履歴の検索での検索結果がここで設定した件数を超えた場合、検索処理を中断して検索結果を出力します。
履歴削除スケジュール	削除しない	保存期間を過ぎた検知履歴を削除するタイミングを設定します。 毎時 : 実行時刻(分)を設定し、設定された時刻に保存期間を過ぎた全ての検知履歴を削除します。 毎日 : 実行時刻(時分)を設定し、設定された時刻に保存期間を過ぎた全ての検知履歴を削除します。 毎週 : 実行時刻(曜日、時分)を設定し、設定された時刻に保存期間を過ぎた全ての検知履歴を削除します。 毎月 : 実行時刻(日時分)を設定し、設定された時刻に保存期間を過ぎた全ての検知履歴を削除します。 削除しない: 全ての検知履歴を削除しません。

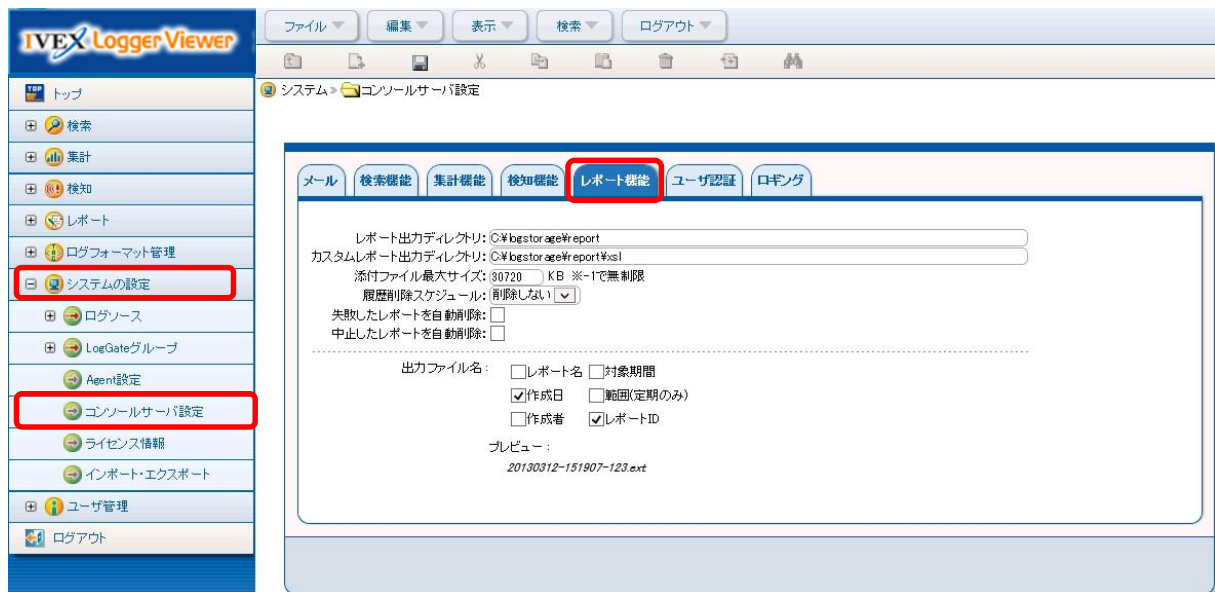
以上が検知機能に関する設定です。

8. その他システム設定を行う

8.5. レポートの添付サイズとレポート保存先を設定する

レポート機能の添付サイズとレポート保存先の設定方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「レポート機能タブ画面」を表示します。



8. その他システム設定を行う

(2)「レポート機能タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 16 レポート機能タブ設定項目

設定項目	既定値	設定内容
レポート出力ディレクトリ	[Linux] /var/logstd/report [Windows] C:¥logstorage¥report	レポート機能で作成したレポートの出力先ディレクトリを設定します。
カスタムレポート出力ディレクトリ	[Linux] /var/logstd/report/xsl [Windows] C:¥logstorage¥report¥xsl	アップロードされたカスタム XSL ファイルの保存先を設定します。
添付ファイル最大サイズ (メール送信時の添付ファイルの最大ファイルサイズ)	30720(KB)	レポート機能の出力タブで、メールによる通知及びレポートの添付を設定した際の、メールに添付するレポートの最大ファイル容量(KB)を設定します。 この設定値を超えたファイルはレポートが作成されてもメールに添付されません。 -1 を指定した場合、作成したレポートのファイル容量に関わらず、作成したレポートをメールに添付します。

8. その他システム設定を行う

履歴削除スケジュール (レポート作成履歴の保存期間設定)	削除しない	保存期間を過ぎたレポート作成履歴を削除するタイミングを設定します。 毎時: 実行時刻(分)を設定し、設定された時刻に保存期間を過ぎた全てのレポート作成履歴を削除します。 毎日: 実行時刻(時分)を設定し、設定された時刻に保存期間を過ぎた全てのレポート作成履歴を削除します。 毎週: 実行時刻(曜日、時分)を設定し、設定された時刻に保存期間を過ぎた全てのレポート作成履歴を削除します。 毎月: 実行時刻(日時分)を設定し、設定された時刻に保存期間を過ぎた全てのレポート作成履歴を削除します。 削除しない: レポート作成履歴を削除しません。
失敗したレポートを自動削除	無効 (自動削除しない)	作成に失敗したレポートのレポート作成履歴を自動的に削除するかどうかを設定します。 有効: 自動的に削除します。コンソールサーバ設定画面の[レポート機能]タブ、[履歴削除スケジュール]欄で設定したタイミングで削除します。 無効: 自動的に削除しません。
中止したレポートを自動削除	無効 (自動削除しない)	作成を中止したレポートのレポート作成履歴を自動的に削除するかどうかを設定します。 有効: 自動的に削除します。コンソールサーバ設定画面の[レポート機能]タブ、[履歴削除スケジュール]欄で設定したタイミングで削除します。 無効: 自動的に削除しません。

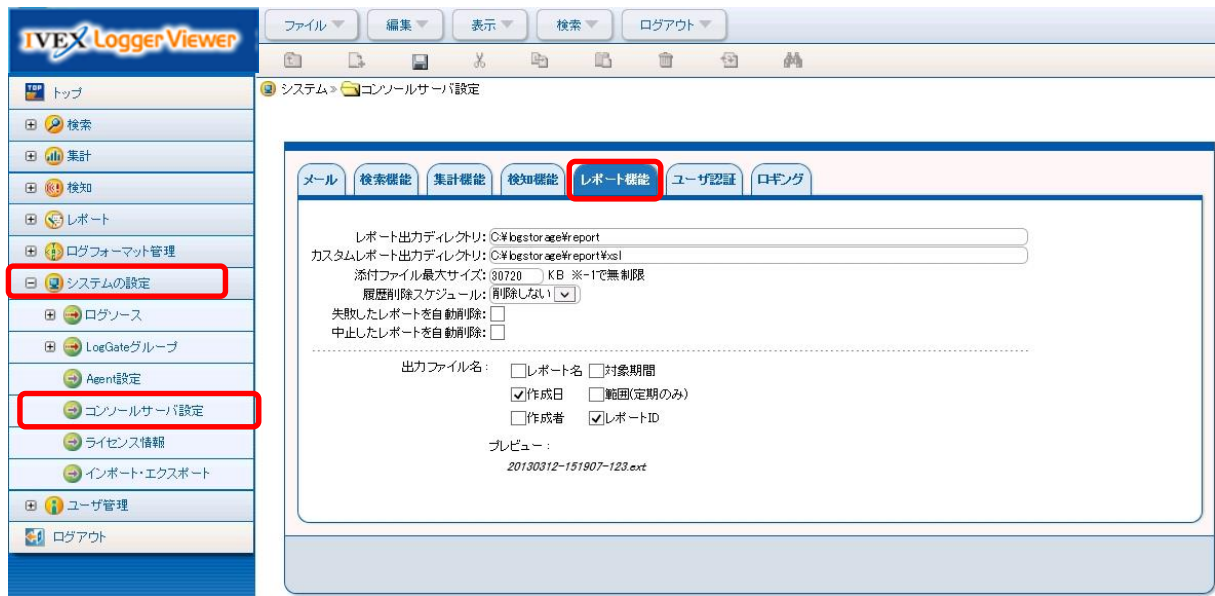
以上がレポート機能に関する設定です。

8. その他システム設定を行う

8.6. レポートの出力ファイル名を設定する

レポート機能のレポートの出力ファイル名の設定方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「レポート機能タブ画面」を表示します。



8. その他システム設定を行う

(2)「レポート機能タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 17 レポート機能タブ設定項目

設定項目	既定値	設定内容
出力ファイル名	レポート名、作成日、 作成者	出力ファイル名に指定する項目です。 レポート名:レポート作成条件の登録名です。 対象期間:レポート作成時の対象期間です。 作成日:レポート作成日です。 範囲(定期のみ):レポート作成条件の範囲です。 Hourly/Daily/Weekly/Monthly が入ります。 作成者:レポート作成条件の作成者が入ります。 レポートID:コンソールサーバが管理するレポートIDが入ります。
プレビュー	—	設定した出力ファイル名のプレビューです。プレビューに表示される文字列と出力ファイル名の対応は以下の通りです。 レポート名:reportName 対象期間:yyyyMMdd-hhmmdd-yyyyMMdd-hhmmdd 作成日:yyyyMMdd 範囲(定期のみ):Daily 作成者:ownerName レポートID:123 ※.ext は拡張子を表します。各レポート作成条件で設定したものが入ります。 ※全てのチェックを外すと noName.ext と表示されます。 noName は固定の値です。 ※noName など拡張子を含めて作成されるレポートのファイル名が同一になるような設定をした場合、レポート保存先に同名のファイルがあると自動的に名前を変更して保存します。(例:report1.pdf というファイル名が同一名であれば、report1~1.pdf となります。)

以上がレポートの出力ファイル名を設定する方法です。

8. その他システム設定を行う

8.7. ユーザ認証を設定する

ユーザ認証の設定方法を記載します。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「ユーザ認証タブ画面」を表示します。

The screenshot displays the IVE X Logger Viewer web application. On the left is a sidebar menu with various system management options. The 'システムの設定' (System Settings) option is highlighted with a red box. Below it, the 'コンソールサーバ設定' (Console Server Settings) option is also highlighted with a red box. The main content area shows the 'コンソールサーバ設定' page with several tabs: 'メール', '検索機能', '集計機能', '検知機能', 'レポート機能', 'ユーザ認証' (highlighted with a red box), and 'ログイン'. The 'ユーザ認証' tab is active, showing settings for password and login policies. Below these are sections for LDAP/AD settings, including basic, server, and user settings, and a test authentication section.

パスワード設定

パスワードポリシー

パスワードの長さ: 6 文字以上
パスワードの有効期間: 0 日 ※0で無制限

数字と英文字の両方を含むパスワードのみ許可する: ☐
同じ文字を繰り返すパスワードを使用させない: ☐
大文字と小文字の両方を含むパスワードのみ許可する: ☐
以前に利用した直近: 0 回目までのパスワードを使用させない: 0 回目
システム管理者に適用: ☐

ログインポリシー

指定回数ログインに連続で失敗したユーザをロックする: 2 回 (0の場合は無効)
指定時間経過後にユーザのロックを解除する: 30 分後 (0の場合は無効)
指定期間内にログインしていないユーザを利用不可にする: 0 日以内 (0の場合は無効)

LDAP/AD設定

基本設定

認証方式: SIMPLE
同期機能を有効: ☐
サブツリーを検索: ☐
サーバはDNを要求する: ☒
プレビュー: uid=admin,ou=People

サーバ設定

プロトコル: ldap
ホスト名:
ポート: 389

ユーザ設定

ユーザのベースDN (suffix): ou=People
ユーザ名の属性: uid

認証試行

ユーザ名:
パスワード:
認証

8. その他システム設定を行う

(2)「ユーザ認証タブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

表 18 ユーザ認証タブ設定項目 パスワードポリシー、ログインポリシー

設定項目	既定値	設定内容
パスワードポリシー設定		
パスワードの長さ	6(文字以上)	ユーザが設定するパスワードの最小文字数を設定します。 設定できる値は 0 以上の整数値です。
パスワードの有効期間	0(日)	ユーザが設定するパスワードの有効期限を日数で設定します。設定できる値は 0 以上の整数値です。0 を指定した場合、有効期限は無期限となります。
数字と英文字の両方を含む パスワードのみ許可する	チェックなし	設定するパスワードに対して、数字・英文字双方を含むものを強制します。
同じ文字を繰り返すパスワード を使用させない	チェックなし	設定するパスワードに対して、同じ文字の繰返しを許可しない設定です。
大文字と小文字の両方を含む パスワードのみ許可する	チェックなし	設定するパスワードに対して、大文字・小文字双方を含むものを強制します。
以前に利用した直近 x 回ま でのパスワードを使用させない	0(回)	パスワード変更の際、直近で使用していた x 回のパスワードは利用不可とする設定です。0 及び 1 を指定した場合は同じ動作となり、直前に設定していたパスワードの再設定は行えません。
システム管理者に適用	チェックなし	設定したパスワードポリシーを管理者である administrators グループのユーザに適用するかどうかを設定します。 チェック有り: administrators グループのユーザを含めた全てのユーザに適用します。 チェックなし: administrators グループ以外のユーザに適用します。
ログインポリシー設定		
指定回数ログインに連続で 失敗したユーザをロックする	0(回)	ロック対象とするログイン連続失敗回数を設定します。 設定できる値は 0 以上の整数値です。0 を指定した場合、本機能は無効になります。
指定時間経過後にユーザ のロックを解除する	30(分後)	ロック解除までの時間を設定します。 設定できる値は 0 以上の整数値です。0 を指定した場合、本機能は無効になります。
指定期間内にログインしてい ないユーザを利用不可にする	0(日以内)	ログインしていないユーザに対して、ユーザ有効期間を設定します。 設定できる値は 0 以上の整数値です。0 を指定した場合、本機能は無効になります。

尚、ログインポリシー設定はパスワードポリシー設定の「システム管理者に適用」設定に関わらず、管理者にも適用されます。

8. その他システム設定を行う

表 19 ユーザ認証タブ設定項目 LDAP/AD 設定

設定項目	既定値	設定内容
認証方式	SIMPLE	次のいずれかを選択します。 SIMPLE:LDAP/AD サーバへの接続時認証不要 DIGEST_MD5:DIGEST_MD5 認証 SASL Realm を指定可 CRAM_MD5:CRAM_MD5 認証 SASL Realm を指定可 KERBEROS:KERBEROS 認証 Kerberos Realm,KDC ホストを指定可
同期機能を有効	チェック無し	チェックを有効にするとコンソールサーバの LDAP/AD 同期画面から LDAP/AD のユーザ/グループ情報を閲覧してインポートすることができます。
サーバは DN を要求する	チェック有り	LDAP/AD へ問い合わせの際に DN を要求される場合はチェックします。
プレビュー	-	LDAP/AD にバインドする際にユーザを表す文字列のプレビューです。
KDC ホスト	-	Kerberos の Key Distribution Center(KDC)ホスト名を指定します。
Kerberos Realm	-	Kerberos の認証時に使用する Realm を指定します。
プロトコル	ldap	次のいずれかを選択します。 ldap :ldap プロトコル ldaps:ldaps プロトコル
ホスト名	-	LDAP/AD サーバのホスト名または IP アドレスを指定します。
ポート	389	整数で、0～999999 の間の数値を指定します。
SASL Realm	-	認証方法が DIGEST_MD5 または CRAM_MD5 の際に指定可能です。
ユーザのベース DN(suffix)	-	ユーザのベース DN が可変の箇所に指定します。 {userDNpart} :ユーザのカスタム DN 部分に置き換えられます {groupDNpart}:グループのカスタム DN 部分に置き換えられます ※テンプレート機能を利用する場合、サブツリー検索と LDAP/AD 同様機能の動きを保証できません。
ユーザ名の属性	-	IVEX Logger Viewer のユーザ名に該当する属性を指定します。
ユーザの objectClass	-	ユーザの objectClass を指定します。
ユーザ概要の属性	-	IVEX Logger Viewer のユーザ概要に該当する属性を指定します。
所属グループの属性	-	IVEX Logger Viewer のユーザが所属するグループに該当する属性を指定します。
グループのベース DN(suffix)	-	この項目はテンプレートではないため、{userDNpart}と{groupDNpart}の置き換えは出来ません。入力した文字列はそのままベース DNとして利用されます。
グループ名の属性	-	IVEX Logger Viewer のグループ名に該当する属性を指定します。
グループの objectClass	-	グループの objectClass を指定します。
グループ概要の属性	-	IVEX Logger Viewer のグループ概要に該当する属性を指定します。

8. その他システム設定を行う

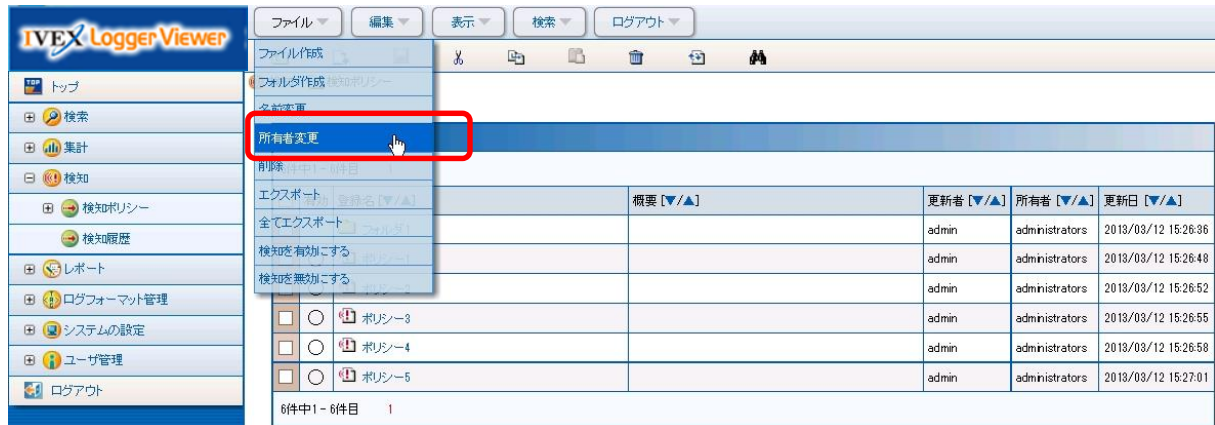
メンバーリストの属性	-	IVEX Logger Viewer のグループの所属ユーザに該当する属性を指定します。
アカウント変更	チェック無し	アカウントを変更します。既定値ではアカウントは設定されていません。
DN	-	IVEX Logger Viewer から LDAP/AD へ検索する際に使用する DN(アカウント)を指定します。
パスワード	-	IVEX Logger Viewer から LDAP/AD へ検索する際に使用する DN(アカウント)のパスワードを指定します。
ユーザ名	-	IVEX Logger Viewer に登録し、かつ認証方式が LDAP/AD であるユーザ名を指定します。
パスワード	-	ユーザ名に対応するパスワードを指定します。
認証ボタン	-	入力したユーザ名とパスワードで認証可能かの確認を実行します。

以上がユーザ認証に関する設定です。

8. その他システム設定を行う

8.8. 条件の所有者を変更する

(3) メニュー「ファイル」→「所有者変更」を選択後、変更する所有者(グループ)のリストが表示されます。



(3) 変更したいフォルダ/ファイルにチェックをつけ、変更したい所有者をリストから選択、「変更」ボタンを押します。



8. その他システム設定を行う

(3) 検知ポリシーリストの所有者が変更されます。

The screenshot shows the IVEX Logger Viewer application window. The left sidebar contains a menu with options like 'トップ', '検索', '集計', '検知', '検知ポリシー', '検知履歴', 'レポート', 'ログフォーマット管理', 'システムの設定', 'ユーザ管理', and 'ログアウト'. The main area displays a message '変更が完了しました。' (Change completed). Below this, there is a dropdown menu for '所有者' (Owner) set to 'グループ1' and a red '変更' (Change) button. A checkbox for 'フォルダ内の子要素にも適用する' (Apply to sub-elements in folder) is also present. The '検知ポリシーリスト' (Detection Policy List) table shows the following data:

有効	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	所有者 [▼/▲]	更新日 [▼/▲]
<input type="checkbox"/>	フォルダ1		admin	administrators	2013/03/12 15:26:36
<input type="checkbox"/>	ポリシー1		admin	administrators	2013/03/12 15:26:48
<input type="checkbox"/>	ポリシー2		admin	administrators	2013/03/12 15:26:52
<input type="checkbox"/>	ポリシー3		admin	グループ1	2013/03/12 15:29:12
<input type="checkbox"/>	ポリシー4		admin	グループ1	2013/03/12 15:29:12
<input type="checkbox"/>	ポリシー5		admin	グループ1	2013/03/12 15:29:12

The '所有者' (Owner) column for the last three policies (ポリシー3, ポリシー4, and ポリシー5) is highlighted with a red box, indicating the change to 'グループ1'.

8. その他システム設定を行う

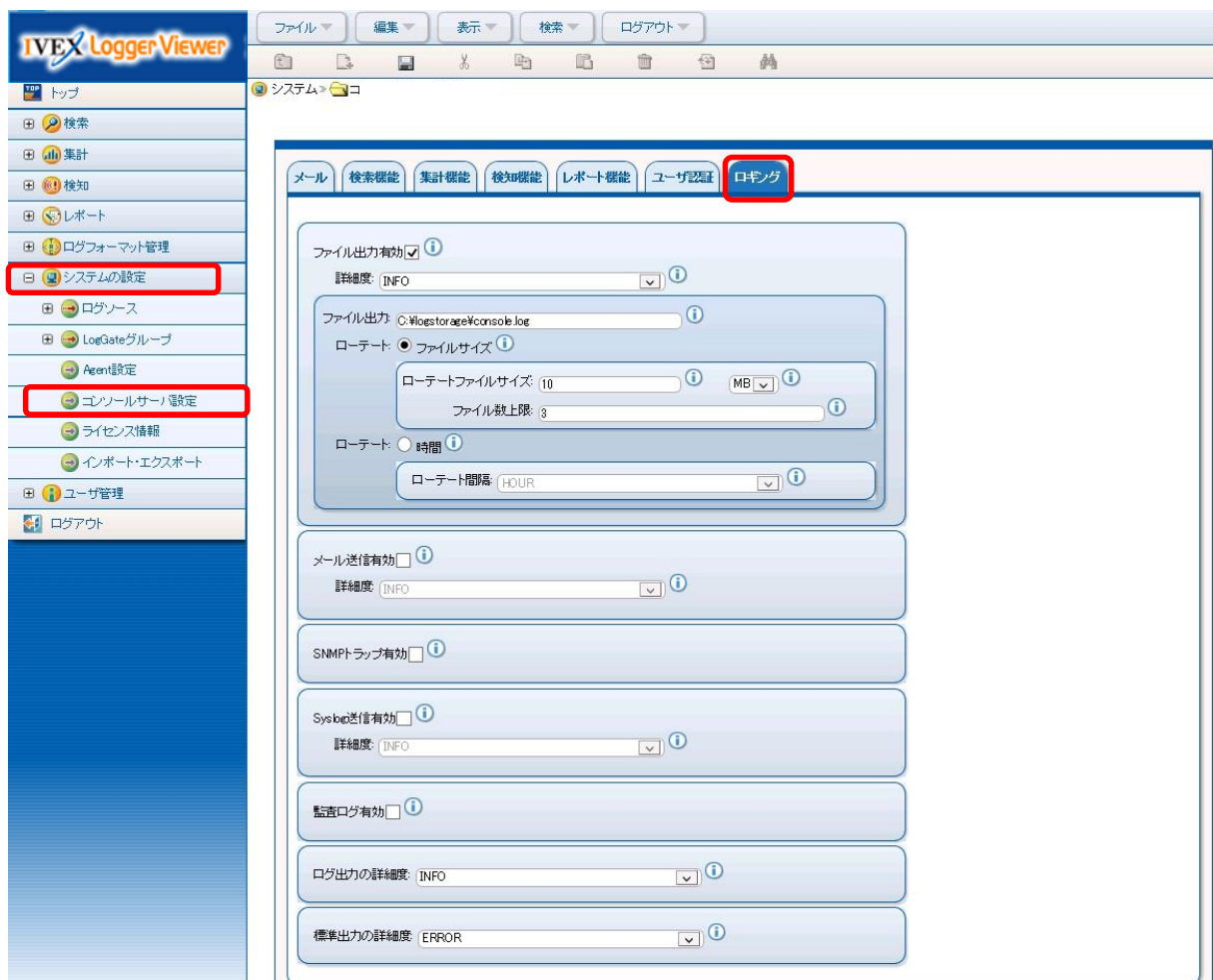
8.9. ログ出力の設定を行う

8.9.1. コンソールシステムログの出力設定を行う

コンソールシステムログは、IVEX Logger Viewer(コンソールサーバ)のエラーや動作が記録されています。

コンソールシステムログの設定方法は以下の通りです。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「ロギングタブ画面」を表示します。



8. その他システム設定を行う

(2)「ロギングタブ画面」で以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

既定値では以下のように出力する設定になっています。

設定	既定値
詳細度(ログの出力レベル)	INFO
ファイル出力	LOGST_HOME/console.log
ローテート	ファイルサイズ
ファイルサイズ	ファイルサイズが 25MB になったらローテーションする
ファイル数上限	20 ファイル
ローテート間隔	HOURL(毎時)

ローテートを時間にすると、時間ごとでファイルをローテーションします。ローテート間隔を DAY に設定した場合は、日付が変わった後にログ出力が無ければ、ログはローテーションしません。この場合、ローテートされたファイルの自動削除は行われませんので、定期的に蓄積したファイルを削除する等の対応を検討してください。

本設定関連のパラメータは以下の通りです。直接編集する場合はコンソールサーバの再起動を行ってください。

システムログ出力設定ファイル(コンソールサーバ)(log4j_console.xml)

```
<appender name="FILE" class="org.apache.log4j.RollingFileAppender">
  <param name="MaxFileSize" value="25MB" />
  <param name="MaxBackupIndex" value="20" />
  <param name="File" value="C:¥¥logstorage¥¥console.log" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d %-5p [%t] %C{2} (%F:%L) - %m%n"/>
  </layout>
</appender>
.....
<category name="com.IVEX Logger Viewer">
  <priority value="INFO" />
  <appender-ref ref="FILE" />
</category>
```

8. その他システム設定を行う

表 20 コンソールシステムログの出力設定項目

属性	既定値	設定内容
File	LOGST_HOME/console.log	ログを出力するファイル名を絶対パスで指定します。
MaxFileSize	25MB	ログファイルの最大ファイルサイズを指定します。 このサイズを超えた場合にローテーションが行われます。 指定できる単位は KB、MB、GB です。
MaxBackupIndex	20	ローテーションするファイル数を指定します。 0 または -1: バックアップを行わず、ログファイルはローテートされません。MaxFileSize に達するとログファイル内のログをクリアして同ファイルに書き込みを行います。 1 以上: 指定したログファイル数をバックアップします。
priority	INFO	ログの出力レベルを指定します。 指定できる出力レベルは「表 21 指定できるログの出力レベル」をご覧ください。

ログの出力ログレベルは以下のいずれかを指定することができます。

表 21 指定できるログの出力レベル

出力レベル	出力内容
FATAL	致命的なエラーが出力します。 IVEX Logger Viewer の再起動が必要。
ERROR	エラー（主に DB に関する障害）が出力します。
WARN	処理は継続できるが問題が発生したことを示します。
INFO	情報
DEBUG	デバッグ
TRACE	詳細情報
OFF	全レベルのログ出力を行いません。

8. その他システム設定を行う

また、コンソールシステムログは、既定値では以下の出力形式で出力します。

＜コンソールシステムログの出力形式＞

```
%d %-5p [%t] %C{2} (%F:%L) - %m%n
```

各パラメータで表示される内容は以下の通りです。

パラメータ	表示される内容
%d	ログが出力された日付と時間
%-5p	ログレベル(5 文字で表示)
%t	ログを生成したスレッド名
%C{2}	ログを生成したクラス名
%F	ログを生成したソースファイル名
%L	ログを生成した箇所のソースの行番号
%m	ログメッセージ
%n	改行コード

＜出力例＞

```
2008-09-18 14:50:17,796 DEBUG [Thread-1] dbm.DBPool (DBPool.java:127) - jdbc:hsqldb:hsqldb://127.0.0.1
2008-09-18 14:50:17,812 DEBUG [Thread-1] dbm.DBPool (DBPool.java:150) - db.interval [10000]
2008-09-18 14:50:17,812 DEBUG [Thread-1] dbm.DBPool (DBPool.java:151) - db.retry [3]
2008-09-18 14:50:18,156 DEBUG [Thread-1] stats.StatsEngine (StatsEngine.java:99) - STATS_TIMEOUT [0]
2008-09-18 14:50:18,171 DEBUG [Thread-1] stats.StatsEngine (StatsEngine.java:449) - Graph directory [C:\logstorage\stats]
```

8. その他システム設定を行う

ここでは日時ベースでローテートさせる場合に設定する設定項目について記載します。

```
.....

<appender name="FILE" class="org.apache.log4j.DailyRollingFileAppender">
  <param name="DatePattern" value="'.'yyyy-MM-dd-HH" />
  <param name="File" value="LOGST_HOME/console.log" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d %-5p [%t] %C{2} (%F:%L) - %m%n"/>
  </layout>
</appender>

.....

<category name="com.IVEX Logger Viewer">
  <priority value="INFO" />
  <appender-ref ref="FILE" />
</category>
```

表 22 コンソールシステムログの設定項目

属性	既定例	設定内容
DatePattern	'.'yyyy-MM-dd-HH	ローテートさせる日時の基準を指定します。 設定できる値については「表 23 DatePattern で設定できる値」をご覧ください。
File	LOGST_HOME/console.log	ログを出力するファイル名を絶対パスで指定します。
priority	INFO	ログの出力レベルを指定します。 指定できる出力レベルは「表 21 指定できるログの出力レベル」をご覧ください。

8. その他システム設定を行う

表 23 DatePattern で設定できる値

設定値	設定した場合のローテート形式
'.'yyyy-MM	月ごとにローテートします。 バックアップされるファイル名は、「出力ファイル名.yyyy-mm」となります。
'.'yyyy-ww	週ごとにローテートします。 バックアップされるファイル名は、「出力ファイル名.通算週番号」となります。
'.'yyyy-MM-dd	日ごとにローテートします。 バックアップされるファイル名は、「出力ファイル名.yyyy-mm-dd」となります。
'.'yyyy-MM-dd-a	各日での深夜と正午にローテートします。 バックアップされるファイル名は、「出力ファイル名.yyyy-mm-dd-AM」となります。
'.'yyyy-MM-dd-HH	時間ごとにローテートします。 バックアップされるファイル名は、「出力ファイル名.yyyy-mm-dd-HH」となります。
'.'yyyy-MM-dd-HH-mm	分ごとにローテートします。 バックアップされるファイル名は、「出力ファイル名.yyyy-mm-dd-HH-mm」となります。

なお、DatePattern パラメータの既定値は「.'.'yyyy-MM-dd」となります。

設定項目の内、画面下部に表示されている 2 つの項目の内容は以下の通りです。各項目で選択可能な値の一覧は「表 21 指定できるログの出力レベル」を参照してください。

設定項目	既定値	設定内容
ログ出力の詳細度	INFO	ログ出力のグローバルな設定です。ファイル出力やメール送信、SNMP トラップ等の各設定のベースとなる最低ラインの設定です。もし、ファイル出力の詳細度を DEBUG にしたとしても、この設定が INFO であった場合 DEBUG ファイルには INFO レベルで出力されます。INFO より下の動作ログを出力する場合は、この設定も DEBUG 以下に設定してください。
標準出力の詳細度	ERROR	標準出力に出力する動作ログのレベルを設定します。

8. その他システム設定を行う

8.9.2. LogGate システムログの出力設定を行う

LogGate システムログは、IVEX Logger Viewer(LogGate)のエラーや動作が記録されています。LogGate システムログの設定はシステムログ出力設定ファイル(LogGate)で設定されています。

(1)コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate 詳細設定」ボタン→「ログ出力」を選択します。

(2)ログ出力画面の設定を変更します。

The screenshot displays the LogGate configuration web interface. On the left is a sidebar menu titled 'LogGate設定' (LogGate Settings) for user 'b(127.0.0.1)'. It includes buttons for '設定を確認し保存' (Check and Save Settings) and 'キャンセル' (Cancel). The menu items are: ステータス (Status), ログ収集 (Log Collection), ログ転送 (Log Transfer), ワーク先 (Work Destination), 検知 (Detection), and ログ出力 (Log Output, which is highlighted with a red box). Under 'ログ収集', there are sub-items for Syslog (UDP, TCP, TLS), LLTP, SNMP, FTP, and File System Monitoring. The main area is titled 'ログ出力' (Log Output) and contains several configuration sections: 1. 'ファイル出力有効' (File Output Enabled) with a checked checkbox, '詳細度' (Detail) set to 'INFO', 'ファイル出力' (File Output) path 'C:\logstorage\loggate.log', 'ローテート' (Rotate) set to 'ファイルサイズ' (File Size), 'ローテートファイルサイズ' (Rotate File Size) set to '10 MB', and 'ファイル数上限' (File Count Limit) set to '3'. 2. 'ローテート' (Rotate) set to '時間' (Time), with 'ローテート間隔' (Rotate Interval) set to 'HOUR'. 3. 'メール送信有効' (Email Send Enabled) with an unchecked checkbox and '詳細度' (Detail) set to 'INFO'. 4. 'SNMPトラップ有効' (SNMP Trap Enabled) with an unchecked checkbox. 5. 'Syslog送信有効' (Syslog Send Enabled) with an unchecked checkbox and '詳細度' (Detail) set to 'INFO'. 6. 'ログ出力の詳細度' (Log Output Detail) set to 'INFO'. 7. '標準出力の詳細度' (Standard Output Detail) set to 'ERROR'.

(3)「設定を確認し保存」ボタンを選択します。

8. その他システム設定を行う

(4)「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

LogGate 及びコンソールサーバの再起動は不要です。

設定	既定値
詳細度(ログの出力レベル)	INFO
ファイル出力	LOGST_HOME/loggate.log
ローテート	ファイルサイズ
ファイルサイズ	ファイルサイズが 25MB になったらローテーションする
ファイル数上限	20 ファイル

ローテートを時間にすると、時間ごとでファイルをローテーションします。この場合、ローテートされたファイルの自動削除は行われませんので、定期的に蓄積したファイルを削除する等の対応を検討してください。

本設定関連のパラメータは以下の通りです。直接編集する場合は LogGate の再起動を行ってください。

システムログ出力設定ファイル(LogGate)(log4j_loggate.xml)

```
.....

<appender name="FILE" class="org.apache.log4j.RollingFileAppender">
  <param name="MaxFileSize" value="25MB" />
  <param name="MaxBackupIndex" value="20" />
  <param name="File" value="C:¥¥logstorage¥¥loggate.log" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d %-5p [%t] %C{2} (%F:%L) - %m%n"/>
  </layout>
</appender>

.....

<category name="com.IVEX Logger Viewer">
  <priority value="INFO" />
  <appender-ref ref="FILE" />
</category>

.....

<category name="org.apache.ftpserver">
  <priority value="INFO" />
  <appender-ref ref="FILE" />
</category>
```

8. その他システム設定を行う

表 24 LogGate システムログの出力設定項目

属性	既定値	設定内容
File	LOGST_HOME/loggate.log	ログを出力するファイル名を絶対パスで指定します。
MaxFileSize	25MB	ログファイルの最大ファイルサイズを指定します。 このサイズを超えた場合にローテーションが行われます。 指定できる単位は KB、MB、GB です。
MaxBackupIndex	20	ローテーションするファイル数を指定します。 0 または -1: バックアップを行わず、ログファイルはローテートされません。MaxFileSize に達するとログファイル内のログをクリアして同ファイルに書き込みを行います。 1 以上: 指定したファイル数をバックアップします。
priority	INFO	ログの出力レベルを指定します。 指定できる出力レベルは「表 25 指定できるログの出力レベル」をご覧ください。

ログの出力ログレベルは以下のいずれかを指定することができます。

表 25 指定できるログの出力レベル

出力レベル	出力内容
FATAL	致命的なエラーが出力します。 IVEX Logger Viewer の再起動が必要。
ERROR	エラー（主に DB に関する障害）が出力します。
WARN	処理は継続できるが問題が発生したことを示します。
INFO	情報
DEBUG	デバック
TRACE	詳細情報
OFF	全レベルのログ出力を行いません。

8. その他システム設定を行う

また、LogGate システムログは、既定値では以下の出力形式で出力します。

＜LogGate システムログの出力形式＞

```
%d %-5p [%t] %C{2} (%F:%L) - %m%n
```

各パラメータで表示される内容は以下の通りです。

パラメータ	表示される内容
%d	ログが出力された日付と時間
%-5p	ログレベル(5 文字で表示)
%t	ログを生成したスレッド名
%C{2}	ログを生成したクラス名
%F	ログを生成したソースファイル名
%L	ログを生成した箇所のソースの行番号
%m	ログメッセージ
%n	改行コード

＜出力例＞

```
2008-09-12 10:58:44,066 DEBUG [Thread-1] loggate.LogGate (LogGate.java:156) - LogG
ate boot start
2008-09-12 10:58:44,066 DEBUG [Thread-1] loggate.LogGate (LogGate.java:167) - LOGS
T_HOME [C:¥logstorage]
2008-09-12 10:58:44,128 DEBUG [Thread-1] dbm.DBPool (DBPool.java:127) - jdbc:hsqld
b:hsq1://127.0.0.1
2008-09-12 10:58:44,144 DEBUG [Thread-1] dbm.DBPool (DBPool.java:150) - db.interva
l [10000]
2008-09-12 10:58:44,159 DEBUG [Thread-1] dbm.DBPool (DBPool.java:151) - db.retry
[3]
2008-09-12 10:58:44,159 DEBUG [Thread-1] engine.Engine (Engine.java:44) - RMI_REGU
ITRY_PORT [1099]
```

8. その他システム設定を行う

設定項目の内、画面下部に表示されている 2 つの項目の内容は以下の通りです。各項目で選択可能な値の一覧は「表 25 指定できるログの出力レベル」を参照してください。

設定項目	既定値	設定内容
ログ出力の詳細度	INFO	ログ出力のグローバルな設定です。ファイル出力やメール送信、SNMP トラップ等の各設定のベースとなる最低ラインの設定です。もし、ファイル出力の詳細度を DEBUG にしたとしても、この設定が INFO であった場合 DEBUG ファイルには INFO レベルで出力されます。INFO より下の動作ログを出力する場合は、この設定も DEBUG 以下に設定してください。
標準出力の詳細度	ERROR	標準出力に出力する動作ログのレベルを設定します。

8. その他システム設定を行う

8.9.3. 監査ログの出力設定を行う

IVEX Logger Viewer では監査ログを出力することが可能です。いつ誰がコンソールサーバでどのような操作をしたかを追跡できます。監査ログは既定値では出力しないようになっています。

監査ログの設定方法は以下の通りです。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「コンソールサーバ設定」を選択し、「ロギングタブ画面」を表示します。

The screenshot displays the IVE X Logger Viewer web interface. On the left is a sidebar menu with various system management options. The main content area shows the 'ロギング' (Logging) tab, which is highlighted with a red box. Within this tab, the '監査ログ' (Audit Log) section is also highlighted with a red box. The '監査ログ' section contains settings for enabling audit logging, output file location, rotation method (by file size or time), rotation interval, and file size limits. The 'ファイル出力' (File Output) section is also visible, showing settings for the main log output.

Left Sidebar Menu:

- TOP
- 検索
- 集計
- 検知
- レポート
- ログフォーマット管理
- システムの設定**
- ログソース
- LogGateグループ
- Agent設定
- コンソールサーバ設定**
- ライセンス情報
- インポート・エクスポート
- ユーザ管理
- ログアウト

Main Content Area - Logging Tab:

- メール ☒ 検索機能 ☒ 集計機能 ☒ 検知機能 ☒ レポート機能 ☒ ユーザ認証 ☒ **ロギング**
- ファイル出力有効 ☒
 - 詳細度: INFO
 - ファイル出力: C:\logstorage\console.log
 - ローテート: ☒ ファイルサイズ
 - ローテートファイルサイズ: 10 MB
 - ファイル数上限: 3
 - ローテート: ☐ 時間
 - ローテート間隔: HOUR
- メール送信有効 ☐
 - 詳細度: INFO
- SNMPトラップ有効 ☐
- Syslog送信有効 ☐
 - 詳細度: INFO
- 監査ログ有効 ☒**
 - 監査ログ: ファイル出力有効 ☒**
 - ファイル出力: C:\logstorage\audit.log
 - ローテート: ☒ ファイルサイズ
 - ローテートファイルサイズ: 10 MB
 - ファイル数上限: 3
 - ローテート: ☐ 時間
 - ローテート間隔: HOUR
 - 監査ログ: Syslog送信有効 ☐

8. その他システム設定を行う

(2)「ロギングタブ画面」で監査ログ有効チェックボックスにチェックを入れ、以下の設定項目を入力し、メニューから「ファイル」→「上書き保存」を選択します。

既定値では以下のように出力する設定になっています。

設定	既定値
詳細度(ログの出力レベル)	INFO
ファイル出力	LOGST_HOME/audit.log
ローテート	ファイルサイズ
ファイルサイズ	ファイルサイズが 25MB になったらローテーションする
ファイル数上限	20 ファイル

ローテートを時間にすると、時間ごとでファイルをローテーションします。この場合、ローテートされたファイルの自動削除は行われませんので、定期的に蓄積したファイルを削除する等の対応を検討してください。

本設定関連のパラメータは以下の通りです。直接編集する場合はコンソールサーバの再起動を行ってください。

システムログ出力設定ファイル(コンソールサーバ)(log4j_console.xml)

```
.....

<appender name="AUDIT" class="org.apache.log4j.RollingFileAppender">
  <param name="MaxFileSize" value="25MB" />
  <param name="MaxBackupIndex" value="20" />
  <param name="File" value="C:¥¥logstorage¥¥audit.log" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d %m%n"/>
  </layout>
</appender>

.....

<category additivity="false" name="com.IVEX Logger Viewer.share.log.AuditLogger">
  <!--Disable Audit Log →
  <priority value="OFF" />
  <appender-ref ref="AUDIT" />
</category>
```

8. その他システム設定を行う

表 26 監査ログの出力設定項目

属性	既定値	設定内容
File	LOGST_HOME/audit.log	ログを出力するファイル名を絶対パスで指定します。
MaxFileSize	25MB	ログファイルの最大ファイルサイズを指定します。このサイズを超えた場合にローテーションが行われます。 指定できる単位は KB、MB、GB です。
MaxBackupIndex	20	ローテーションするファイル数を指定します。 0 または -1: バックアップを行わず、ログファイルはローテートされません。MaxFileSize に達するとログファイル内のログをクリアして同ファイルに書き込みを行います。 1 以上: 指定したファイル数をバックアップします。
Priority	OFF	ログの出力レベルを指定します。 OFF が指定された場合は、監査ログを出力しません。 指定できる出力レベルは「表 27 指定できるログの出力レベル」をご覧ください。

ログの出力ログレベルは以下を指定することができます。

表 27 指定できるログの出力レベル

出力レベル	出力内容
INFO	情報
OFF	全レベルのログ出力を行いません。

8. その他システム設定を行う

また、監査ログは、既定値では以下の出力形式で出力します。

＜監査ログの出力形式＞

%d %m%n

各パラメータで表示される内容は以下の通りです。

パラメータ	表示される内容
%d	ログが出力された日付と時間
%m	ログメッセージ
%n	改行コード

＜出力例＞

2008-09-18 09:24:51,953 admin 192.168.254.211 2974C982E90D69D953C04FFE0FBADD4F COM MON ドメイン管理者がログインしました 2008-09-18 10:25:17,250 User1 192.168.254.220 DD821E1B8DFEDD68B471B7AD1C1917C0 COM MON ユーザ User1 がログインしました 2008-09-18 11:25:10,109 admin 192.168.254.211 2974C982E90D69D953C04FFE0FBADD4F COM MON ドメイン管理者がログアウトしました 2008-09-18 12:25:20,015 User1 192.168.254.220 DD821E1B8DFEDD68B471B7AD1C1917C0 COM MON ユーザ User1 がログアウトしました

8. その他システム設定を行う

8.10. LogGate 設定情報をダウンロードする

LogGate 設定情報のダウンロードは現在の設定を新たに構築する IVEX Logger Viewer のシステム設定へ移行するために使用します。LogGate 設定情報をダウンロードする手順について説明します。

- (1) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「設定管理」を選択します。



- (3) ダウンロードボタンを選択します。

以上が LogGate 設定情報をダウンロードする手順です。

拡張子 lgs というファイルをダウンロードできれば終了です。

例: allSettings(2010-09-30 01-50-34).lgs

8. その他システム設定を行う

8.11. LogGate 設定情報をアップロードする

LogGate 設定情報のアップロードは現在の設定を新たに構築する IVEX Logger Viewer のシステム設定へ移行するために使用します。LogGate 設定情報をアップロードする手順について説明します。

- (1) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「システムの設定」→「LogGate グループ」→「LogGate グループリストの登録名」→「LogGate:詳細設定」ボタン→「設定管理」を選択します。



- (3) 参照ボタンを選択します。選択するファイルは拡張子 lgs というファイルです。

例: allSettings(2010-09-30 01-50-34).lgs

- (3) アップロードボタンを選択します。

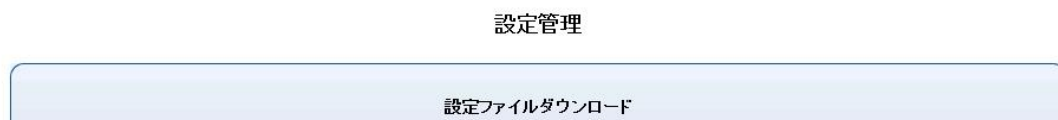
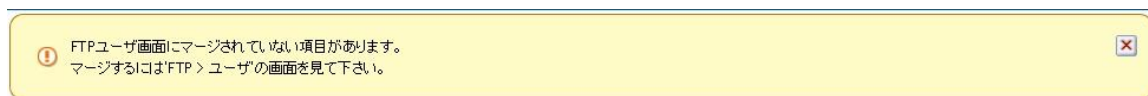
8. その他システム設定を行う

(4) 以下のようにメッセージが表示されることを確認します。



以上が LogGate 設定情報をアップロードする手順です。

以下のようにインポートした情報が既に登録されている場合は、マージするかどうかメッセージが表示されます。メッセージの表示にしたがって設定画面へ移動してマージしてください。下記の例では FTP ユーザをインポートしようとして既に登録されているユーザをマージすることを表しています。



FTP ユーザの設定画面へ移動すると以下のように表示されています。ユーザ名が重複しているため、ユーザ名をクリックし名前を変更した後に、リストに追加ボタンを押すことでマージすることができます。

ユーザ	ホームフォルダー	パスワード	書き込み権限	タイムアウト(秒)	最大転送速度(B/s)	最大受信速度(B/s)	削除
anonymous	c:\logstorage	クリックして変更	<input type="checkbox"/>	300	4800	4800	
admin	c:\logstorage	クリックして変更	<input checked="" type="checkbox"/>	100	3200	0	



8. その他システム設定を行う

(5)「設定を確認し保存」ボタンを選択します。

(6)「設定変更を確認して下さい」画面で「設定を LogGate に送信」ボタンを選択します。

LogGate 及びコンソールサーバの再起動は不要です。

8. その他システム設定を行う

8.12. レポートを共有する

作成したレポートを複数のユーザグループで共有するために使用します。

本マニュアルでは、ユーザグループ「グループ A」が所有するレポート作成履歴出力フォルダ「レポート共有用」フォルダを、ユーザグループ「グループ B」に共有する設定を説明します。

(1) コンソールサーバに Web ブラウザから管理者ユーザでログインし、フォルダリスト「レポート」→「レポート作成履歴」を選択します。

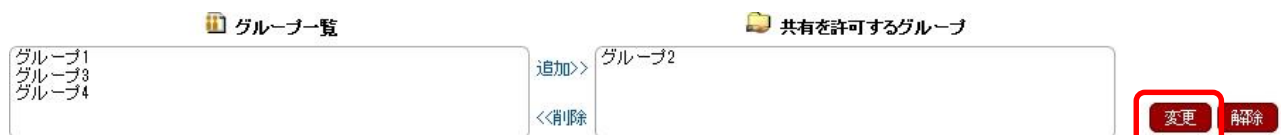
(2) 共有したいフォルダにチェックを入れ、メニュー「ファイル」→「フォルダ共有設定変更」を選択します。



(3) 共有を許可するグループを選択し、「追加」を押下します。

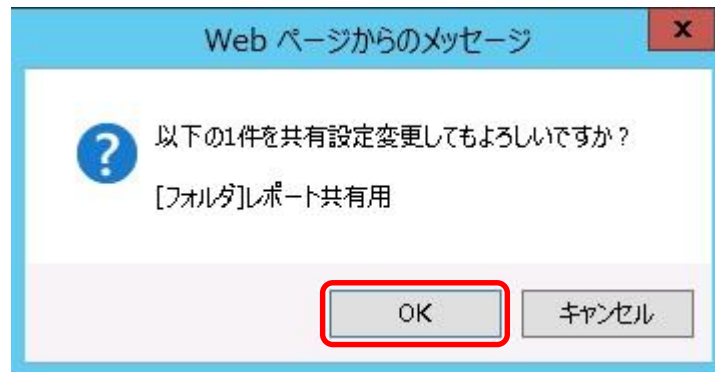


(4) 「変更」を押下します。



8. その他システム設定を行う

(3) メッセージを確認し「OK」を押下します。



(3) 以下のメッセージが表示されます。



(7) レポート作成履歴リストでは、共有設定をしたフォルダのアイコンが変更されます。また、アイコンにマウスオーバーすると共有しているグループが表示されます。

レポート作成履歴リスト					
4件中1 - 4件目 1					
<input type="checkbox"/>	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	所有者 [▼/▲]	開始
<input type="checkbox"/>	グループ1用		admin	administrators	
<input type="checkbox"/>	グループ2用		admin	administrators	
<input type="checkbox"/>	グループ3用		admin	administrators	
<input type="checkbox"/>	レポート共有用		admin	administrators	

レポート作成履歴リスト					
4件中1 - 4件目 1					
<input type="checkbox"/>	登録名 [▼/▲]	概要 [▼/▲]	更新者 [▼/▲]	所有者 [▼/▲]	開始
<input type="checkbox"/>	グループ1用		admin	administrators	
<input type="checkbox"/>	グループ2用		admin	administrators	
<input type="checkbox"/>	グループ3用		admin	administrators	
<input type="checkbox"/>	レポート共有用		admin	administrators	

共有グループ【グループ2】

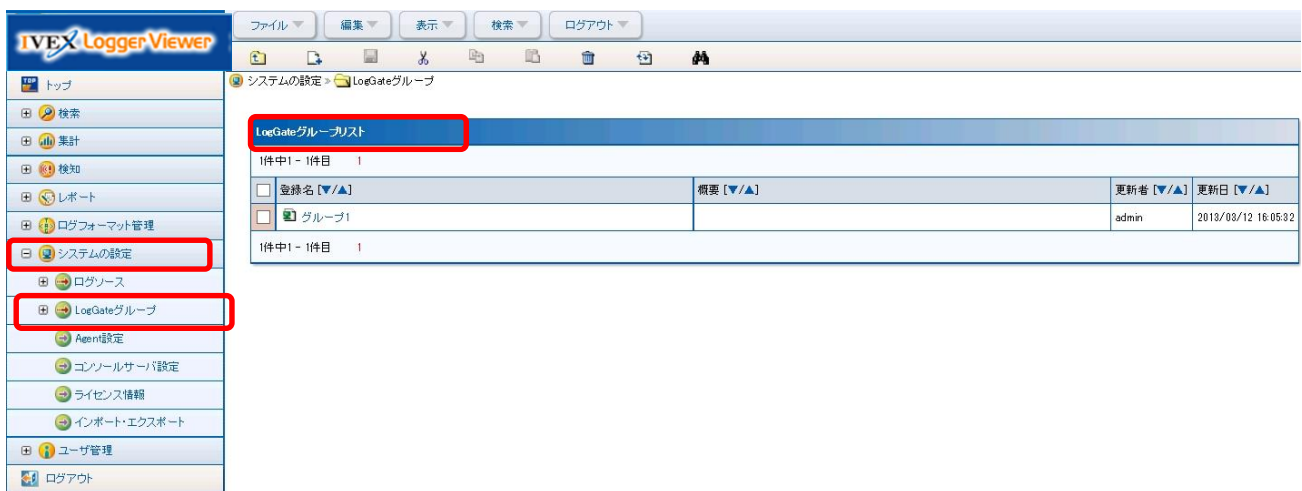
9. LogGate グループの設定を行う。

9. LogGate グループの設定を行う

9.1. LogGate の IP アドレスを変更する(全エディション)

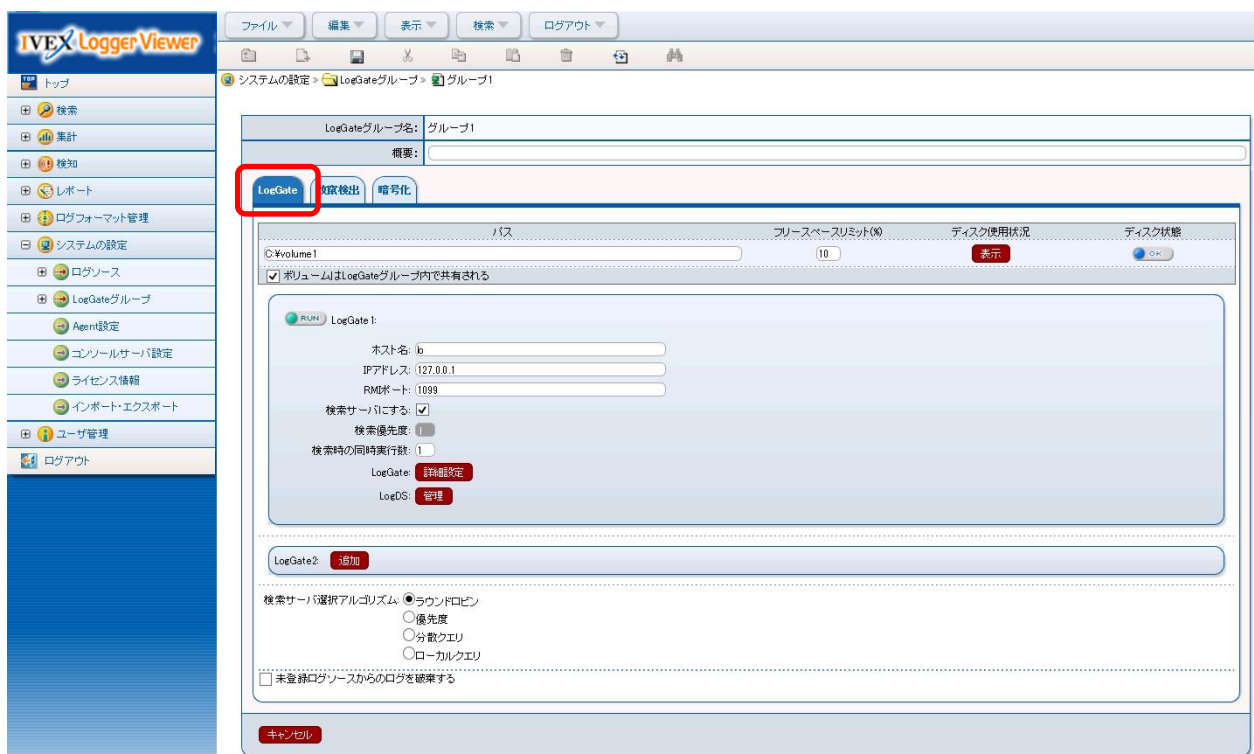
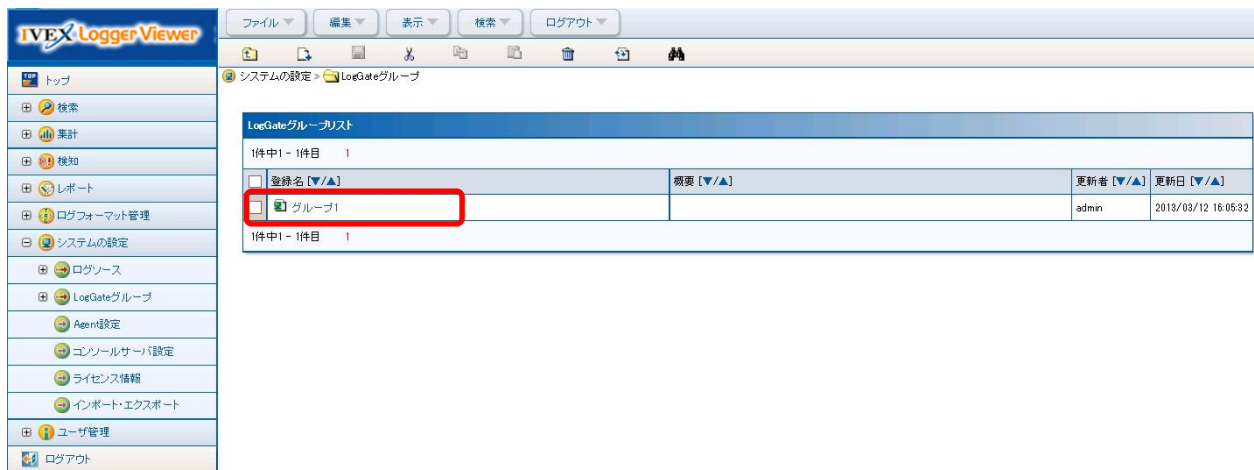
LogGate の IP アドレスを変更する方法について説明します。なお、変更の際、コンソールサーバは起動しておく必要があります。LogGate は起動または停止のいずれの状態でも変更可能です。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「LogGate グループ」を選択し、「LogGate グループリスト画面」を表示します。



9. LogGate グループの設定を行う。

(2) 「LogGate グループリスト画面」から設定を行う LogGate グループを選択し「LogGate タブ画面」を表示します。



9. LogGate グループの設定を行う。

(3) 「LogGate タブ画面」の IP アドレスに変更する IP アドレスを入力します。



LogGate 1:

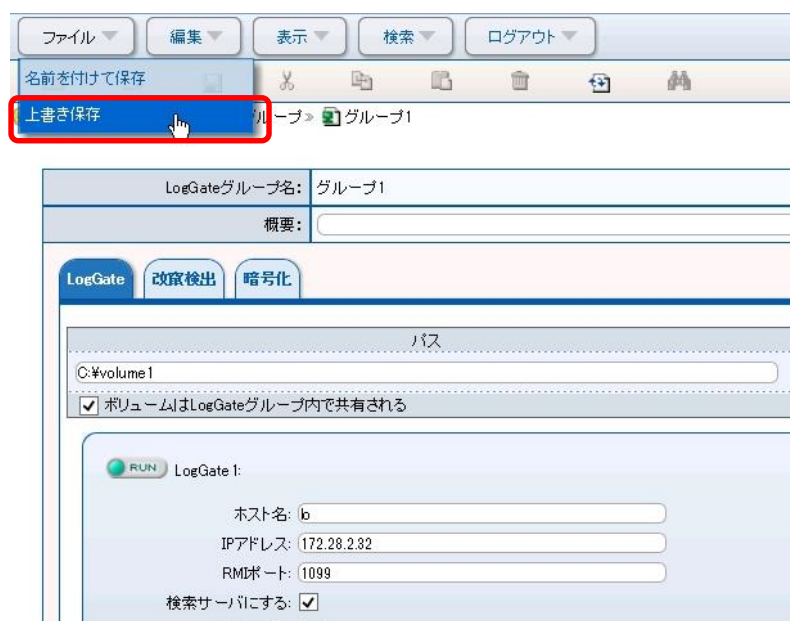
ホスト名: lb

IPアドレス: 172.28.2.32

RMIポート: 1099

検索サーバにする: ☒

(4) 設定項目の変更・修正後、メニューから「ファイル」→「上書き保存」を選択します。



ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

名前を付けて保存

上書き保存

LogGateグループ名: グループ1

概要:

LogGate 改竄検出 暗号化

パス

C:\volume1

☒ ボリュームはLogGateグループ内で共有される

LogGate 1:

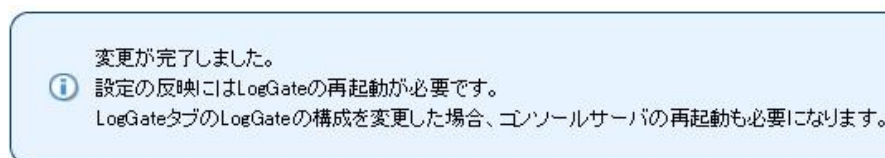
ホスト名: lb

IPアドレス: 172.28.2.32

RMIポート: 1099

検索サーバにする: ☒

(5) 確認画面が表示されますので LogGate の再起動を行います。再起動は、「エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。」をご覧ください。再起動後は、(4)の「更新ボタン」を押すことで LogGate の起動確認をします。なお、本操作ではコンソールサーバの再起動は不要です。



変更が完了しました。

① 設定の反映にはLogGateの再起動が必要です。

LogGateタブのLogGateの構成を変更した場合、コンソールサーバの再起動も必要になります。

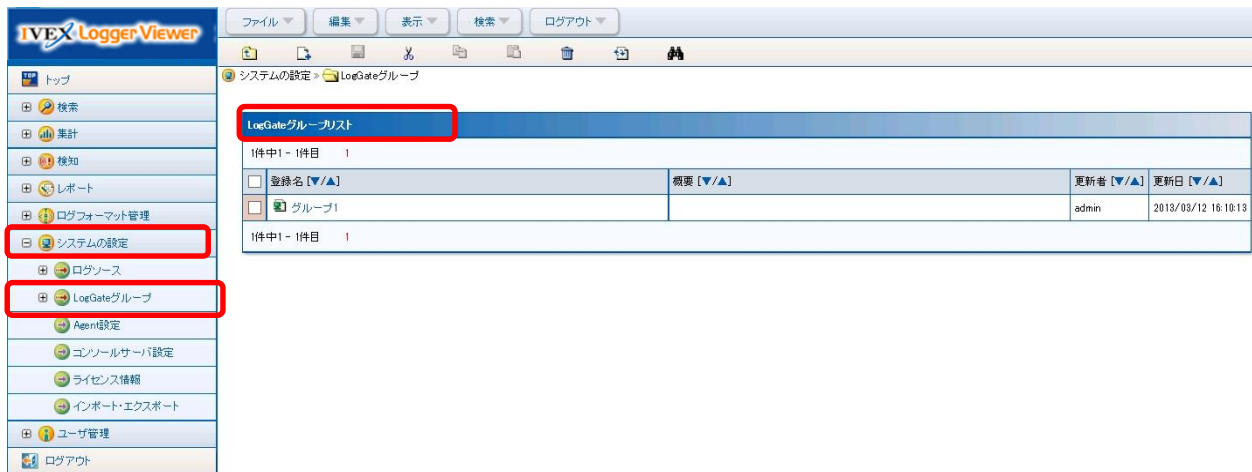
以上です。画面の詳細は、「4.3.収集ログ保存先を変更する」をご覧ください。

9. LogGate グループの設定を行う。

9.2. LogGate の検索アルゴリズムを変更する(アドバンス版のみ)

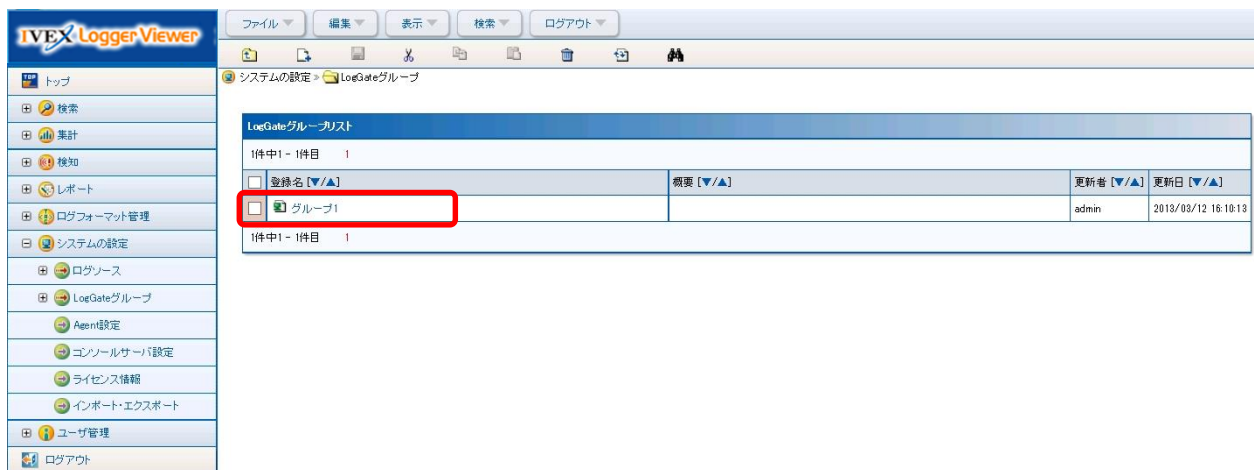
LogGate の検索アルゴリズムを変更する方法について説明します。なお、変更の際、コンソールサーバは起動しておく必要があります。LogGate は起動または停止のいずれの状態でも変更可能です。

- (1) 管理者でコンソールサーバへログイン後、フォルダリストの「システムの設定」→「LogGate グループ」を選択し、「LogGate グループリスト画面」を表示します。

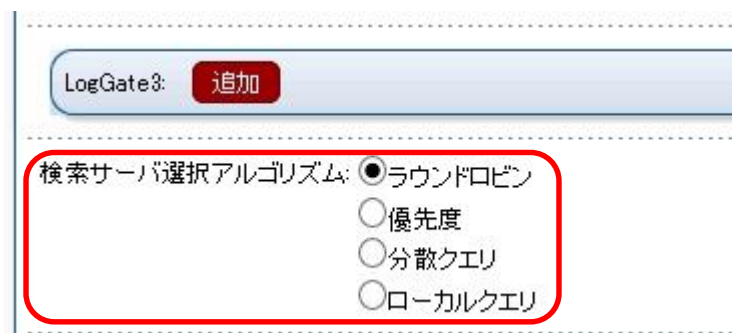


9. LogGate グループの設定を行う。

(2) 「LogGate グループリスト画面」から設定を行う LogGate グループを選択し「LogGate タブ画面」を表示します。



(3) 「LogGate タブ画面」で検索サーバ選択アルゴリズムの設定項目を変更・修正します。



各検索アルゴリズムの詳細は「IIVEX Logger Viewer ガイド」をご覧ください。

9. LogGate グループの設定を行う。

(4) 設定項目の変更・修正後、メニューから「ファイル」→「上書き保存」を選択します。

(5) 確認画面が表示され、全ての LogGate の再起動を行います。(4)の「更新ボタン」を押すことで LogGate の起動確認をします。

以上です。画面の詳細は、「4.3.収集ログ保存先を変更する」をご覧ください。

10. インポート・エクスポートを実行する

10. インポート・エクスポートを実行する

ここでは、IVEX Logger Viewer のシステム設定(インポート・エクスポート)として以下のことを説明します。

各種条件や設定情報のインポート

検索条件やレポート作成条件から LogGate グループ、一般グループ・一般ユーザ等の設定情報をインポートします。

各種条件や設定情報のエクスポート

検索条件やレポート作成条件から LogGate グループ、一般グループ・一般ユーザ等の設定情報をエクスポートします。

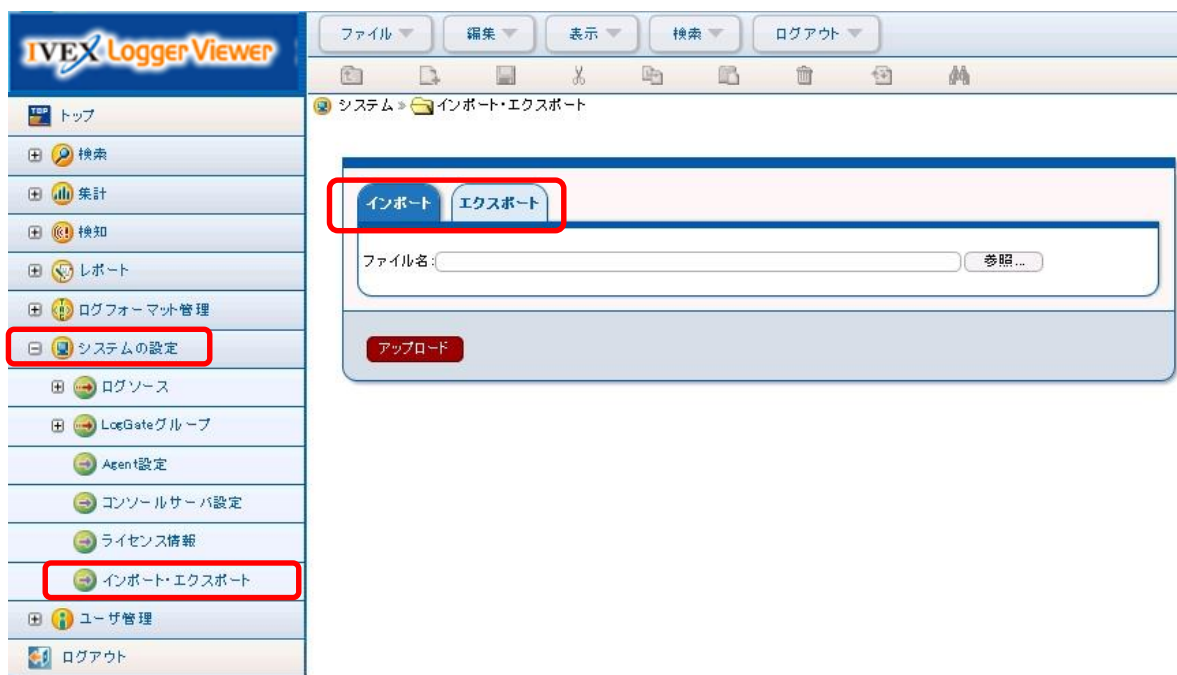
10. インポート・エクスポートを実行する

10.1. 各種条件や設定情報をインポートする(管理画面)

各種条件や設定情報のインポートが行えます。

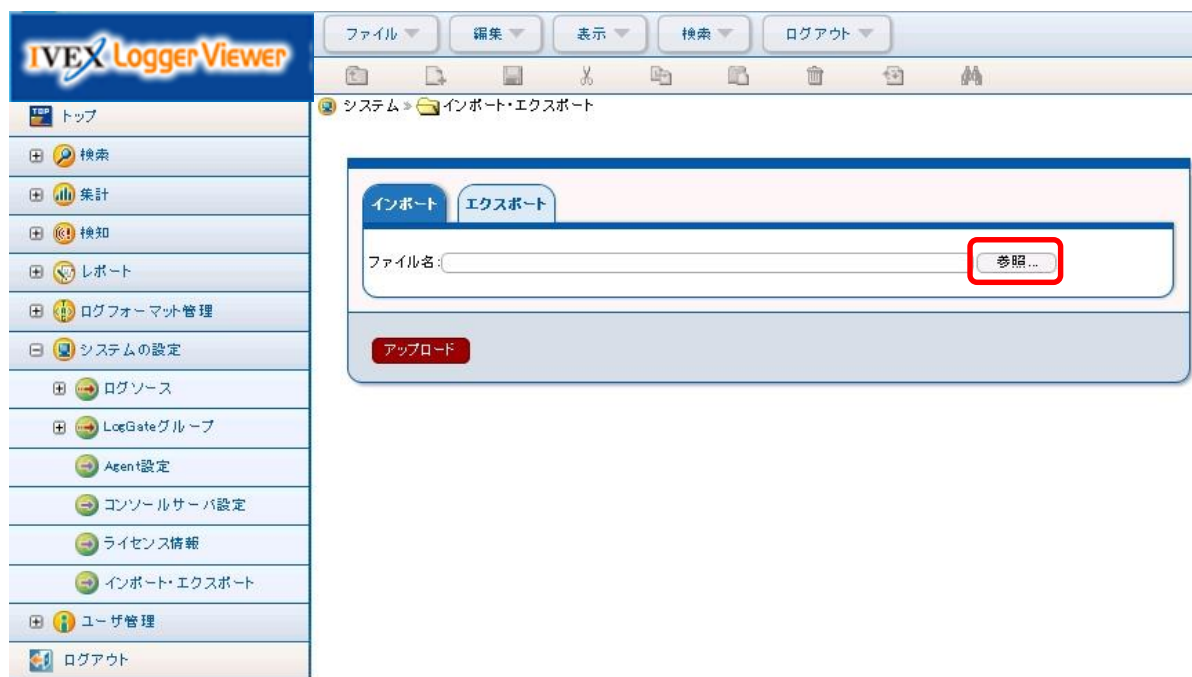
以下にインポート手順を記載します。

- (1) 管理者でログインし、フォルダリストの「システムの設定」を選択し、「インポート・エクスポート」を選択します。



10. インポート・エクスポートを実行する

(2) インポートタブの「参照」ボタンを選択して、インポートする各種条件や設定情報のファイルを選択します。



10. インポート・エクスポートを実行する

(3) 「アップロード」ボタンを選択すると、次の画面が表示されます。

インポート

エクスポート

ファイル名: [参照...](#)

ログフォーマット管理

ログフォーマット定義

<input checked="" type="checkbox"/>	登録名	種類	処理状況	解決方法
<input checked="" type="checkbox"/>	Apache	アプリケーション	-	マージ 上書き 変更

↑トップ

タグ定義

<input checked="" type="checkbox"/>	登録名	種類	処理状況	解決方法
<input checked="" type="checkbox"/>	URL	タグ	-	-
<input checked="" type="checkbox"/>	クライアントIPアドレス	タグ	-	-
<input checked="" type="checkbox"/>	ステータスコード	タグ	-	-
<input checked="" type="checkbox"/>	メソッド	タグ	-	-


↑トップ

アップロード

インポート項目確認へ

キャンセル

アップロード時に以下のようなメッセージが出た場合は、処理状況にあわせて解決方法を選択します。解決方法についての詳細は次の手順をご覧ください。

 データの整合性に問題が分かりました。処置状況に従い解決方法を選択してください。

10. インポート・エクスポートを実行する

- (4) アップロードされた各種条件や設定情報が画面に表示されるので、取り込む場合は、登録名の左チェックボックスをチェックし、取り込まない場合は登録名の左チェックボックスのチェックをはずします。

インポート

エクスポート

ファイル名: 参照...

ログフォーマット管理

ログフォーマット定義

<input checked="" type="checkbox"/>	登録名	種類	処理状況	解決方法	マージ	上書き	変更
<input checked="" type="checkbox"/>	+ Apache	アプリケーション	⚠ 正規表現重複	正規表現変更	<input checked="" type="radio"/> 自動	<input type="radio"/> 指定	

↑トップ

タグ定義

<input checked="" type="checkbox"/>	登録名	種類	処理状況	解決方法	マージ	上書き	変更
<input checked="" type="checkbox"/>	URL	タグ	⚠ XMLタグ重複	マージ(変更なし)	<input checked="" type="radio"/> 自動	<input type="radio"/> 指定	
<input checked="" type="checkbox"/>	クライアントIPアドレス	タグ	⚠ XMLタグ重複	上書き	<input checked="" type="radio"/> 自動	<input type="radio"/> 指定	
<input checked="" type="checkbox"/>	ステータスコード	タグ	⚠ XMLタグ重複	XMLタグ変更	<input checked="" type="radio"/> 自動	<input type="radio"/> 指定	statuscode
<input checked="" type="checkbox"/>	メソッド	タグ	⚠ XMLタグ重複	XMLタグ変更	<input checked="" type="radio"/> 自動	<input type="radio"/> 指定	

↑トップ

アップロード

インポート項目確認へ

キャンセル

10. インポート・エクスポートを実行する

表 28 インポートタブ設定項目

表示項目/設定項目/ボタン	設定/表示/実行内容
登録名	各種条件や設定情報の名前です。
種類	登録名の種類を表します。例：アプリケーション、タグなど
処理状況	登録済みの各種条件や設定情報があった場合、その重複状況を表します。何も表示が無い項目は、不整合なし又は解決済みの項目です。
解決方法(マージ)	登録済みの各種条件や設定情報を利用します。(変更なし) 解決方法(マージ)ボタンは、一括でマージする際のボタンです。
解決方法(上書き)	登録済みの各種条件や設定情報を上書きします。 解決方法(上書き)ボタンは、一括で上書きする際のボタンです。 子要素を持つ情報(アプリケーションなど)の場合は、解決方法「上書き」で子要素も上書きするオプションがあります。「子要素も上書きする」をチェックすると登録済み子要素が削除します。
解決方法(変更)	登録する各種条件や設定情報の値を変更してインポートします。「自動」チェックボックスにチェックを入れると、重複する登録名の後ろに「(2)」のような形で順に番号を振って登録します。数字は 2 以降がつきます。 「指定」チェックボックスにチェックを入れると、指定した登録名や値で登録します。解決方法(変更)ボタンは、一括で自動変更する際のボタンです。
<< >>マーク	登録する各種条件や設定情報が子要素を持つ場合は、展開します。
アップロード	指定したファイルをアップロードします。
インポート項目確認へ	アップロードした各種条件や設定情報をインポートする前の確認画面を表示します。
キャンセル	アップロードしたデータの編集を破棄し、インポートタブ画面に戻ります。

10. インポート・エクスポートを実行する

インポートする各種条件や設定情報が多い場合は、「1 2 NEXT」の項目が表示します。数字もしくはNEXTボタンを押してページを移動することで、次のリストを見ることができます。数字の横のマークは、登録済みの各種条件や設定情報と重複する項目やインポートの際に不整合となる項目があることを表します。それぞれのページへ移動して、重複を解決してください。

ログフォーマット管理

ログフォーマット定義

<input checked="" type="checkbox"/>	<< >>	登録名	種類
<input checked="" type="checkbox"/>	1  2 3 NEXT ▶		
<input checked="" type="checkbox"/>	+  Apache		アプリケーション
	1  2 3 NEXT ▶		

10. インポート・エクスポートを実行する

(5)「インポート項目確認へ」ボタンを選択すると、次の画面が表示されます。

The screenshot shows a web application interface for log format management. At the top, there are tabs for 'インポート' (Import) and 'エクスポート' (Export). Below the tabs, there are links for 'ログフォーマット管理' (Log Format Management) and 'ログフォーマット定義' (Log Format Definition). The main area contains a table with the following columns: '登録名' (Registered Name), '種類' (Type), '処理状況' (Processing Status), and '解決方法' (Solution Method). The table lists various log format items for Apache, including GET, access IP address, access time, status code, data size, protocol, method, user agent, request URL, referrer, country, search keywords, and authentication user. Each item has a '上書き' (Overwrite) button in the '解決方法' column. The table is paginated with '1 2 3 | NEXT >' at the bottom left and '↑ トップ' (Top) at the bottom right. At the bottom of the interface, there are buttons for 'インポート' (Import) and 'キャンセル' (Cancel).

登録名	種類	処理状況	解決方法
Apache	アプリケーション		上書き
GET	アクション		上書き
アクセス元IPアドレス	メッセージラメタ		上書き
アクセス日時	メッセージラメタ		上書き
ステータスコード	メッセージラメタ		上書き
データ量	メッセージラメタ		上書き
プロトコル	メッセージラメタ		上書き
メソッド	メッセージラメタ		上書き
ユーザエージェント	メッセージラメタ		上書き
リクエストURL	メッセージラメタ		上書き
リファラー	メッセージラメタ		上書き
国	メッセージラメタ		上書き
検索語句	メッセージラメタ		上書き
認証ユーザ	メッセージラメタ		上書き

(6)「インポート」ボタンを選択します。

(7)「インポートが完了しました。」メッセージが表示されます。

以上がインポートする手順です。

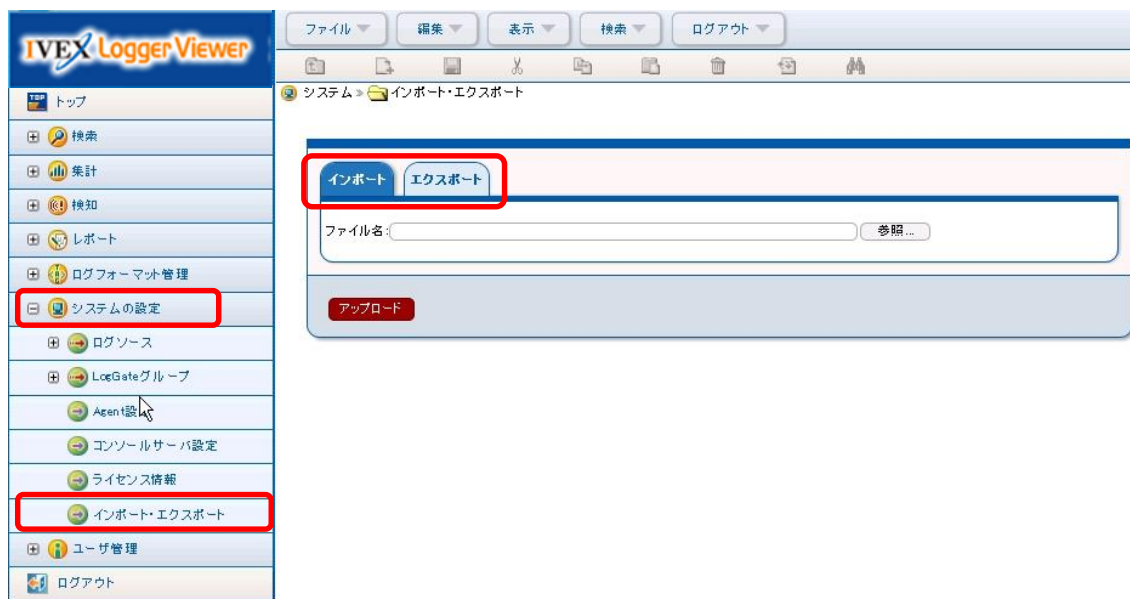
10. インポート・エクスポートを実行する

10.2. 各種条件や設定情報をエクスポートする(管理画面)

各種条件や設定情報のエクスポートが行えます。

以下にエクスポート手順を記載します。

- (1) 管理者でログインし、フォルダリストの「システムの設定」を選択し、「インポート・エクスポート」を選択して、インポートタブ画面を表示します。



10. インポート・エクスポートを実行する

(2) 「エクスポートタブ」を選択してエクスポートタブ画面を表示します。

インポート **エクスポート**

出力フォーマット: XML ▼

エクスポートXMLのバージョン: 1.6 (Logstorage 4.4.2) ▼

検索

☐ 検索条件 [詳細設定](#)

☐ カラムセット定義 [詳細設定](#)

集計

☐ 集計条件 [詳細設定](#)

検知

☐ 検知ポリシー [詳細設定](#)

レポート

☐ レポート作成条件 [詳細設定](#)

☐ カスタムレポート定義 [詳細設定](#)

ログフォーマット管理

☐ ログフォーマット定義 [詳細設定](#)

☐ タグ定義 [詳細設定](#)

システムの設定

☐ ログソース [詳細設定](#)

☐ LogGateグループ [詳細設定](#)

☐ コンソールサーバ設定

ユーザ管理

☐ グループ管理 [詳細設定](#)

☐ ユーザ管理 [詳細設定](#)

[エクスポート項目確認へ](#)

10. インポート・エクスポートを実行する

- (3) 各種条件や設定情報が画面に表示します。エクスポートする場合は、左チェックボックスをチェックします。エクスポートしない場合は、左チェックボックスのチェックを外します。

エクスポートXMLのバージョン: 1.6 (Logstorage 4.4.2)

検索

☒ 検索条件

☐ カラムセット定義

☐ 集計

☐ 集計条件

☐ 検知

☐ 検知ポリシー

☐ レポート

☐ レポート作成条件

☐ カスタムレポート定義

☐ ログフォーマット管理

☐ タグ定義

☐ システムの設定

☐ LogGateグループ

☐ エンロールサーバ設定

☐ ユーザ管理

☐ グループ管理

☐ ユーザ管理

詳細非表示

☒ 自動インポートポリシー:
フォルダーをマージ、他は自動変更

エクスポート対象指定:

登録名	概要	作成日	更新日	種類
<全て>				

詳細設定

詳細非表示

☐ アプリケーションの自動インポートポリシー:

☐ アクションの自動インポートポリシー:

☐ メッセージパラメータの自動インポートポリシー:

エクスポート対象指定:

登録名	概要	作成日	更新日	種類
<全て>				

詳細設定

詳細非表示

☒ 自動インポートポリシー:
全てマージ

エクスポート対象指定:

登録名	概要	作成日	更新日	種類
<全て>				

詳細設定

エクスポート項目確認へ

10. インポート・エクスポートを実行する

以下は、検索条件、カラムセット定義、集計条件、検知ポリシー、レポート作成条件、カスタムレポート定義、LogGate グループ、ユーザ管理のエクスポートタブ設定項目です。

表 29 エクスポートタブ設定項目(各種条件)

表示項目/設定項目/ボタン	設定/表示/実行内容
出力フォーマット	エクスポートするファイルのフォーマットです。XML、ZIP、CSV を選択することができます。CSV を選択した場合のみ、ログソース、グループ管理、ユーザ管理の3項目しか選択することができません。
エクスポート XML のバージョン	エクスポートするファイルの XML バージョンです。古いバージョンのコンソールサーバにインポートする際に指定します。
詳細設定	各種条件や設定情報を詳細にエクスポートする画面を表示します。
詳細設定(自動インポートポリシー)	インポート時に登録済みの各種条件や設定情報と重複した際のインポート方法を固定する設定です。「フォルダーをマージ、他は自動変更」、「フォルダーをマージ、他は上書き」、「全て自動変更」を選択することができます。
詳細設定(エクスポート対象指定)	エクスポートしたい各種条件や設定情報をプルダウンより選択します。選択後はプルダウン右側の追加ボタンを選択することでエクスポート対象となります。
詳細設定(登録名、概要、作成日、更新日、種類)	エクスポートしたい各種条件や設定情報の情報です。右側の削除ボタンを選択することでエクスポート対象から外すことができます。
エクスポート項目確認へ	エクスポートしたい各種条件や設定情報をエクスポートする前の確認画面を表示します。

10. インポート・エクスポートを実行する

以下は、ログフォーマット定義のエクスポートタブ設定項目です。

表 30 エクスポートタブ設定項目(ログフォーマット定義)

表示項目/設定項目/ボタン	設定/表示/実行内容
出力フォーマット	エクスポートするファイルのフォーマットです。XML、ZIP、CSV を選択することができます。CSV を選択した場合のみ、ログソース、グループ管理、ユーザ管理の3項目しか選択することができません。
エクスポート XML のバージョン	エクスポートするファイルの XML バージョンです。古いバージョンのコンソールサーバにインポートする際に指定します。
詳細設定	ログフォーマット定義を詳細にエクスポートする画面を表示します。
詳細設定(アプリケーションの自動インポートポリシー)	インポート時に登録済みのアプリケーションと重複した際のインポート方法を固定する設定です。「フォルダーをマージ、他は自動変更」、「フォルダーをマージ、他は上書き」、「全て自動変更」、「全てマージ」を選択することができます。
詳細設定(アクションの自動インポートポリシー)	インポート時に登録済みのアクションと重複した際のインポート方法を固定する設定です。「フォルダーをマージ、他は自動変更」、「全て自動変更」、「全てマージ」を選択することができます。
詳細設定(メッセージパラメータの自動インポートポリシー)	インポート時に登録済みのメッセージパラメータと重複した際のインポート方法を固定する設定です。「フォルダーをマージ、他は自動変更」、「全て自動変更」、「全てマージ」を選択することができます。
詳細設定(エクスポート対象指定)	エクスポートしたい各種条件や設定情報をプルダウンより選択します。選択後はプルダウン右側の追加ボタンを選択することでエクスポート対象となります。
詳細設定(登録名、概要、作成日、更新日、種類)	エクスポートしたいログフォーマット定義の情報です。右側の削除ボタンを選択することでエクスポート対象から外すことができます。
エクスポート項目確認へ	エクスポートしたいログフォーマット定義をエクスポートする前の確認画面を表示します。

10. インポート・エクスポートを実行する

以下は、タグ定義、ログソース、グループ管理のエクスポートタブ設定項目です。

表 31 エクスポートタブ設定項目(タグ定義等)

表示項目/設定項目/ボタン	設定/表示/実行内容
出力フォーマット	エクスポートするファイルのフォーマットです。XML、ZIP、CSV を選択することができます。CSV を選択した場合のみ、ログソース、グループ管理、ユーザ管理の3項目しか選択することができません。
エクスポート XML のバージョン	エクスポートするファイルの XML バージョンです。古いバージョンのコンソールサーバにインポートする際に指定します。
詳細設定	各種条件や設定情報を詳細にエクスポートする画面を表示します。
詳細設定(自動インポートポリシー)	インポート時に登録済みの各種条件や設定情報と重複した際のインポート方法を固定する設定です。「フォルダーをマージ、他は自動変更」、「フォルダーをマージ、他は上書き」、「全て自動変更」、「全てマージ」を選択することができます。
詳細設定(エクスポート対象指定)	エクスポートしたい各種条件や設定情報をプルダウンより選択します。選択後はプルダウン右側の追加ボタンを選択することでエクスポート対象となります。
詳細設定(登録名、概要、作成日、更新日、種類)	エクスポートしたい各種条件や設定情報です。右側の削除ボタンを選択することでエクスポート対象から外すことができます。
エクスポート項目確認へ	エクスポートしたい各種条件や設定情報をエクスポートする前の確認画面を表示します。

10. インポート・エクスポートを実行する

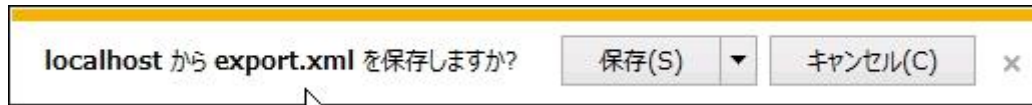
(4)「エクスポート項目確認へ」ボタンを選択します。

表 32 エクスポートタブ設定項目(エクスポート項目確認画面)

表示項目/設定項目/ボタン	設定/表示/実行内容
再編集	エクスポートする各種条件や設定情報を選択しなおします。
エクスポート	ダウンロード画面を表示します。

10. インポート・エクスポートを実行する

(5) 「エクスポート」ボタンを選択します。



(6) ファイルのダウンロード画面の「保存」ボタンを選択します。

設定ファイルは XML 形式の場合のファイル名は「export.xml」で出力します。ZIP 形式の場合は、「export.zip」、CSV 形式の場合は、「export.csv」となります。

以上がエクスポートする手順です。

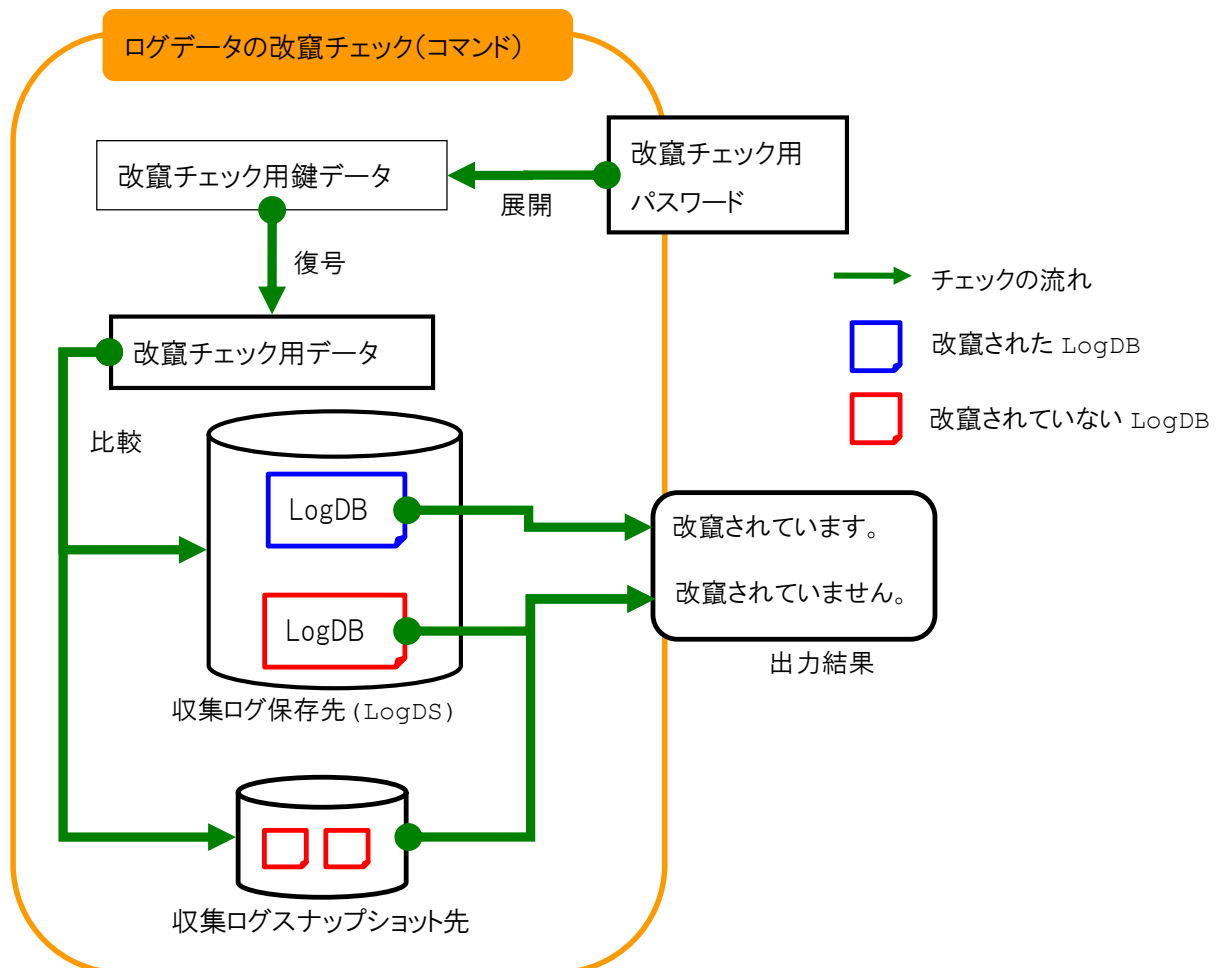
エクスポートする対象の項目に依存する要素があれば、自動的にエクスポートします。例えば、アプリケーションをエクスポートすると、それに関連するもの(例:メッセージパラメータ・タグ等)も同時にエクスポートします。(タグ定義のチェックを外していても必要なタグをエクスポートします)。また、その依存要素も設定をすることで個別に自動インポートポリシーを適用することができます。

第二部. ログデータを管理する

第二部では、ログデータに対する各種設定方法について説明します。

11. ログデータの改竄チェックを行う

11.1. ログデータの改竄チェック機能



LogDSに蓄積されたLogDBまたは収集ログスナップショット先のLogDBに対して改竄チェックをするコマンドがあります。改竄チェックは、主に検索した結果の基になるログデータやレポート結果の基になるログデータが改竄されていないかどうかをチェックする際に使用することを想定しています。改竄チェックには設定時に登録したパスワードが必要です。改竄されているログデータも検索やレポートに使用することができます。

11. ログデータの改竄チェックを行う

11.2. 改竄チェック機能を無効にする

改竄チェック機能は、新規インストール直後の時点で有効に設定されています（初期パスワード「logst」）。
機能を利用しない場合は以下の手順で無効にします。

- (1) 管理者で、コンソールサーバにログインします。
- (2) メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3) 登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4) 改竄検出タブを選択します。

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

システムの設定 > LogGateグループ > グループ1

LogGateグループ名: グループ1

概要:

LogGate 改竄検出 略号化

☒ 改竄検出機能を有効にする

改竄チェック用パスワード: logst

キャンセル

- (5) 改竄検出機能を有効にするチェックボックスのチェックを外します。

11. ログデータの改竄チェックを行う

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

システムの設定 >> LogGateグループ >> グループ1

LogGateグループ名: グループ1

概要:

LogGate 改竄検出 略号化

☒ 改竄検出機能を有効にする

改竄チェック用パスワード:

キャンセル

(6) メニュー「ファイル」→「上書き保存」を選択します。

LogGate の再起動を促すメッセージが表示されます。

ファイル ▼ 編集 ▼ 表示 ▼ 検索 ▼ ログアウト ▼

名前を付けて保存

上書き保存

グループ >> グループ1

LogGateグループ名: グループ1

概要:

LogGate 改竄検出 略号化

☐ 改竄検出機能を有効にする

改竄チェック用パスワード:

キャンセル

変更が完了しました。

i 設定の反映にはLogGateの再起動が必要です。
LogGateタブのLogGateの構成を変更した場合、コンソールサーバの再起動も必要になります。

(7) LogGate を再起動します。

以上が改竄チェック有効の設定方法となります。改竄検出タブの設定項目は以下の通りです。

11. ログデータの改竄チェックを行う

表 33 換算検出タブの設定項目

設定項目	概要/既定値
改竄検出機能を有効にする	チェックボックスにチェックをつけた場合、改竄検出機能を有効にします。 既定値は無効です。
改竄チェック用パスワード	改竄チェック用のパスワードを入力します。既定値は「logst」です。 パスワードは4文字以上です。

改竄チェック機能が無効にした後、再度有効にする場合、全て改竄されているとみなされます。有効にした直後に改竄チェックコマンドに-cl をつけて改竄チェック用データを作成してください。

```
logds.bat(sh) verify -cp XXXX -cl
```

XXXX は改竄チェック用のパスワードです。

尚、改竄チェック用パスワードを変更した場合の考慮は特にありません。LogGate の再起動以後、変更したパスワードでコマンドの実行が可能となります。

11. ログデータの改竄チェックを行う

11.3. ログデータの改竄チェックをする

収集ログ保存先(LogDS)の LogDB を改竄チェックします。

ログデータの改竄チェックをするコマンド

<コマンド例>

収集ログ保存先にある全てのログデータを対象に改竄チェックする。

```
C:¥logstorage¥bin>logds.bat verify -cp XXXX
```

XXXX にはパスワードを入力します。コマンド実行後、

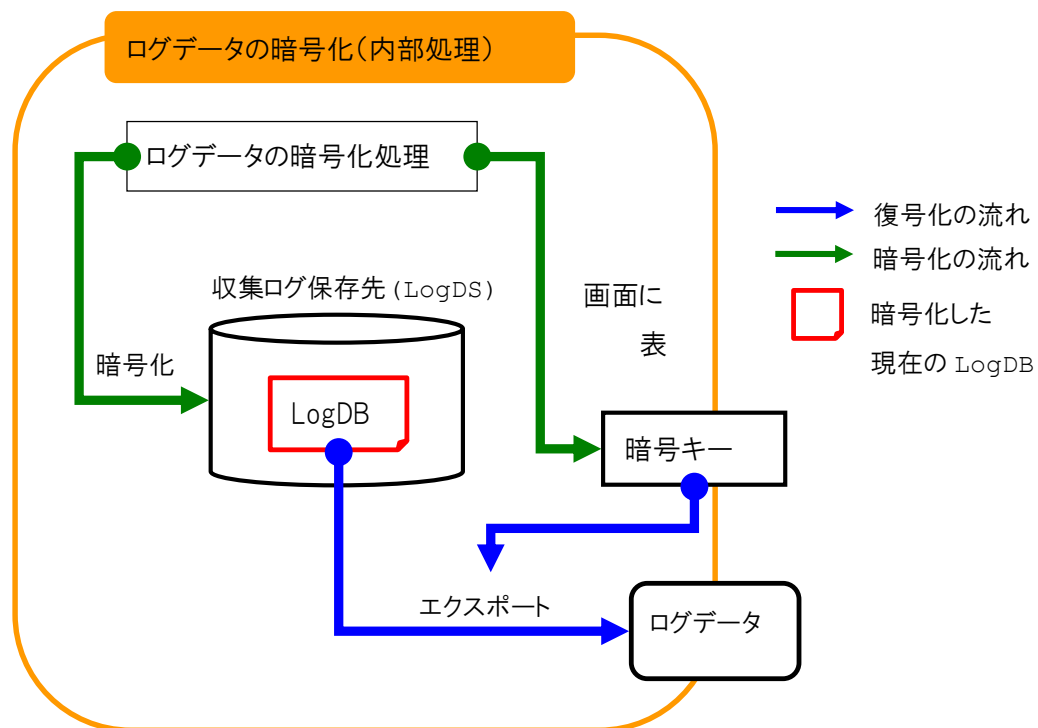
「[Verify success] C:¥volume1¥logds¥20130301」というメッセージが表示された場合は、その日(この例では 2013 年 3 月 1 日)のログデータが改竄されていないことを表します。

「[Verify failure] C:¥volume1¥logds¥20130301」というメッセージが表示された場合は、その日(この例では 2013 年 3 月 1 日)のログデータが改竄されていることを表します。

Windows のコマンドプロンプトでパスワードを入力する際に、パスワード文字列で「!」を使っている場合は制御文字として扱われてしまうため、「"^!"」のように、二重引用符で囲み、キャレット文字"^"でエスケープする必要があります。

12. ログデータを暗号化する

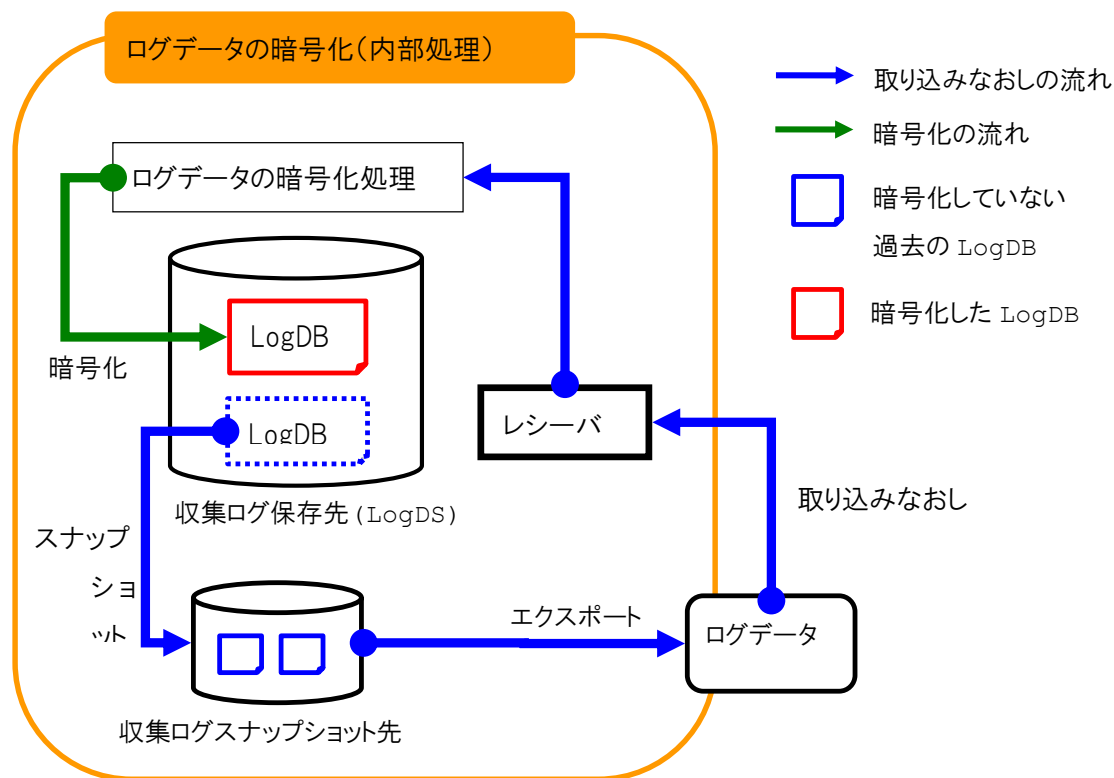
12.1. ログデータの暗号化機能



LogDS に蓄積された LogDB (ログデータ) に対して暗号化をする設定があります。設定時に1度のみ表示される暗号化キーは、収集ログ保存先や収集ログスナップショット先からログデータをエクスポートする際に使用します。

12. ログデータを暗号化する

途中でログデータの暗号化をする場合の暗号化の流れ



ログデータを収集している途中で暗号化設定を行った場合は、設定を有効にする直前か直後に暗号化していない過去のログデータを収集ログ保存先から退避する必要があります。過去のログデータで暗号化されていないログデータが混在することができません。暗号化されていないログデータが収集ログ保存先にある場合は LogGate 起動時にエラーとなり、起動できません。また、収集ログスナップショット先のログデータを暗号化する場合は一度エクスポートした後で再度 LogGate に取り込み直しをする必要があります。

手順の概略は以下の通りです。

1. 暗号化していない過去の LogDB をスナップショットで退避する
2. 収集ログ保存先(既定値:c:\¥volume1)を削除
3. ログデータの暗号化を有効にする
4. 1で取った収集ログスナップショット先からログデータをエクスポートする
5. レシーバを使ってログデータを取り込みなおし、取り込み完了後は収集ログスナップショット先を削除

12. ログデータを暗号化する

12.2. ログデータの暗号化を有効にする

- (1) 管理者で、コンソールサーバにログインします。
- (2) メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3) 登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4) 暗号化タブを選択します。

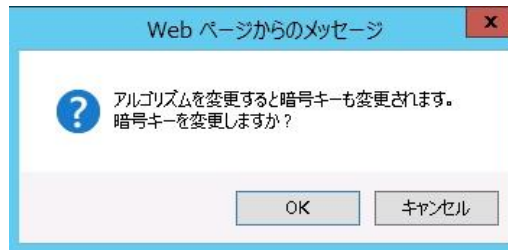


- (5) ログデータを暗号化するチェックボックスにチェックを入れ、暗号化アルゴリズムを選択します。



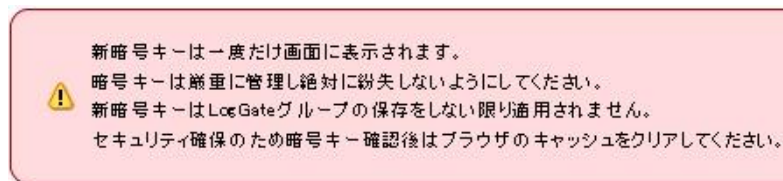
12. ログデータを暗号化する

(6) 以下のメッセージが表示され、OK ボタンを選択します。



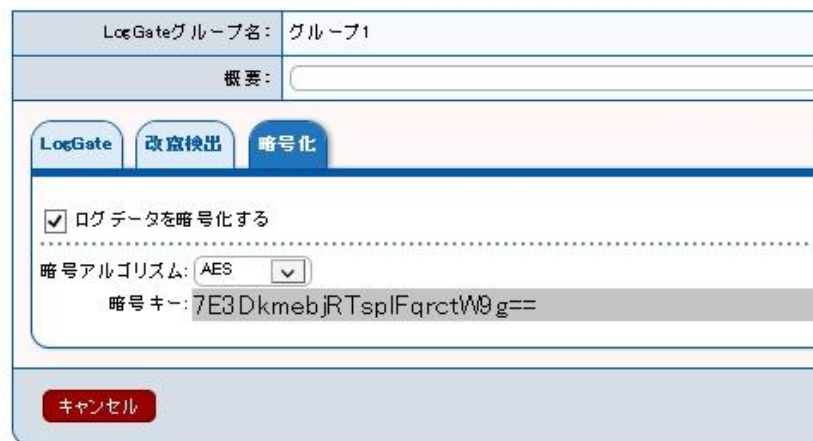
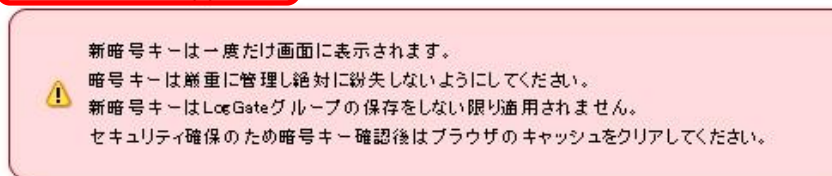
(7) 暗号化キーに関するメッセージが表示されます。

暗号化キー欄にある文字列をコピーして保管します。



(8) メニュー「ファイル」→「上書き保存」を選択します。

LogGate の再起動を促すメッセージが表示されます。



12. ログデータを暗号化する

変更が完了しました。
設定の反映にはLogGateの再起動が必要です。
LogGateタブのLogGateの構成を変更した場合、コンソールサーバの再起動も必要になります。

(9) LogGate を再起動します。

以上がログデータの暗号化を有効にする設定方法となります。暗号化タブの設定項目は以下の通りです。

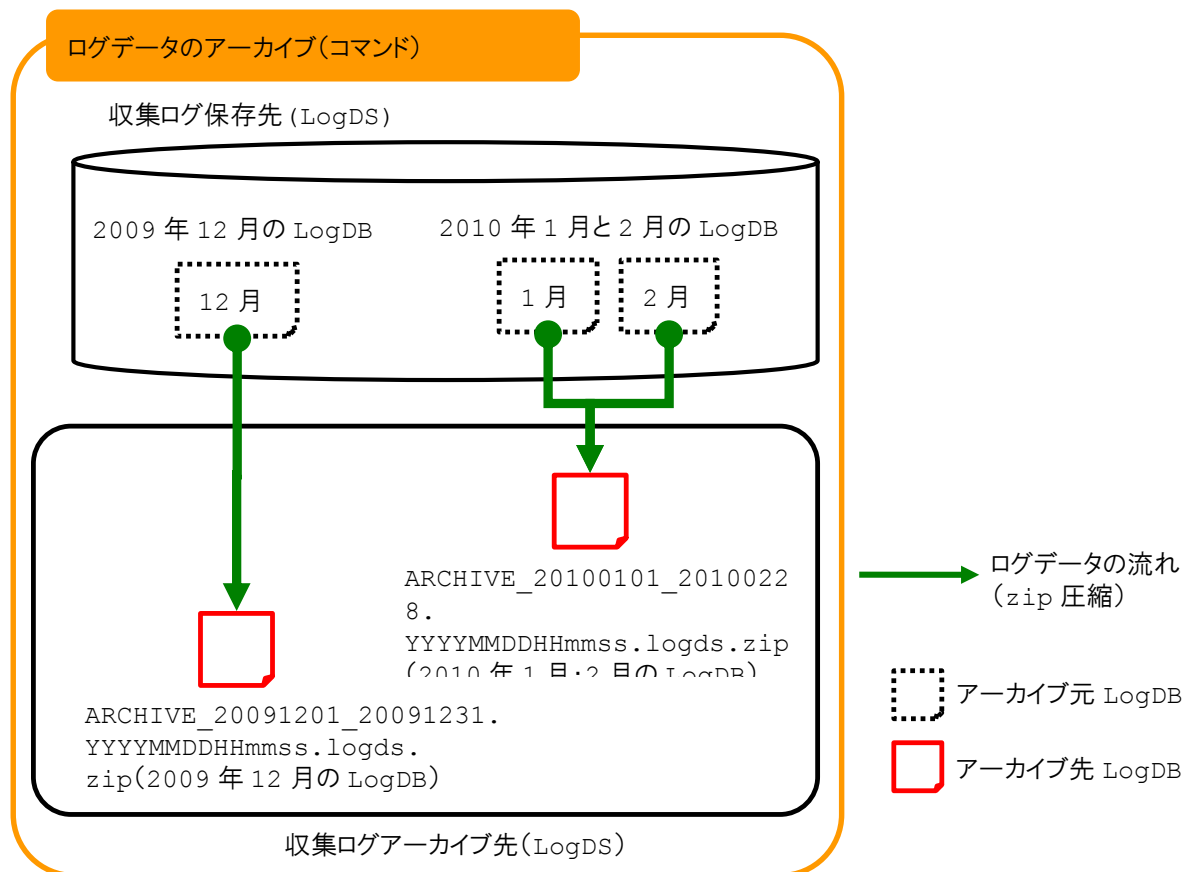
表 34 暗号化タブの設定項目

設定項目	概要/既定値
ログデータを暗号化する	チェックボックスにチェックをつけた場合、暗号化機能を有効にします。 既定値は無効です。
暗号アルゴリズム	暗号アルゴリズムです。-- AES Blowfish RC4 RC2 DESede DES から選択します。既定値は-無効です。
暗号キー	暗号キーはログデータをエクスポートする際に復号化で使用します。画面に1度だけ表示され、コピーして保管しておきます。既定値はありません。

13. ログデータをアーカイブする

13. ログデータをアーカイブする

13.1. ログデータのアーカイブ機能



LogDS に蓄積された LogDB をアーカイブするコマンドがあります。アーカイブは、主に検索やレポートで使わなくなった古い LogDB を長期間保存する際に使用することを想定しています。アーカイブした LogDB は zip で圧縮します。LogDB の複数指定はできません。収集ログ保存先にある、オンライン期間を過ぎた LogDB 全てが対象となります。

13. ログデータをアーカイブする

13.2. 古い LogDB をアーカイブする

LogDS には検索やレポートに使用する LogDB を残しておき、使わなくなった古い LogDB を定期的にアーカイブします。

古い LogDB をアーカイブするコマンド

<コマンド例>

検索やレポートに使用するログデータは直近 1 ヶ月分(2010 年 2 月分)とし、2010 年 3 月 1 日 12 時 00 分に使わなくなった 2010 年 1 月の 1 ヶ月分の LogDB を c:¥archive ディレクトリへ zip 形式でアーカイブする。2010 年 1 月の LogDB は削除する。

```
c:¥logstorage¥bin¥logds.bat archive -r -d c:¥archive¥ -tm 1
```

コマンドを実行した後は、c:¥archive¥(/var/archive/)以下に
ARCHIVE_20100101_20100131.20100301120000.logds.zip ファイルを作成します。

アーカイブはコマンドを実行した LogGate が管理する LogDS のみが対象です。アドバンスド版では個々の LogGate においてアーカイブコマンドを実行する必要があります。

13. ログデータをアーカイブする

13.3. バックアップ目的で LogDB をアーカイブする

LogDS には長期間分の LogDB を残しておき、バックアップの観点から LogDB をコピーします。

※フルバックアップについては LogDS のフルバックアップをするスナップショット機能で対応可能です。

LogDB を残してアーカイブするコマンド

<コマンド例>

2010 年 3 月 1 日 12 時 00 分に先月の 2 月より前(1月を含めた前)の LogDB を c:¥archive ディレクトリへ zip 形式で1ファイルにアーカイブする。2010 年 2 月 1 日より前の LogDB は残す。C:¥archive¥以下に ARCHIVE_20100101_20100131.20100301120000.logds.zip ファイルを作成する。

```
c:¥logstorage¥bin¥logds.bat archive -d c:¥archive¥ -tm 1
```

13. ログデータをアーカイブする

13.4. アーカイブした LogDB を削除する

収集ログアーカイブ先にアーカイブした LogDB が保管期間を過ぎた場合に LogDB を削除します。削除については OS のファイル削除コマンドを使用することで削除します。

アーカイブした LogDB を削除するコマンド

<コマンド例>

2010 年 1 月 10 日 14 時 15 分にアーカイブした 2009 年 12 月分の LogDB を削除する

```
del c:\¥archive¥ARCHIVE_20091201_20091231.20100110141500.logds.zip
```

13. ログデータをアーカイブする

13.5. アーカイブ時に残した LogDB を削除する

収集ログ保存先に残してアーカイブした LogDB を使わなくなったため削除します。

アーカイブ時に残した LogDB を削除するコマンド

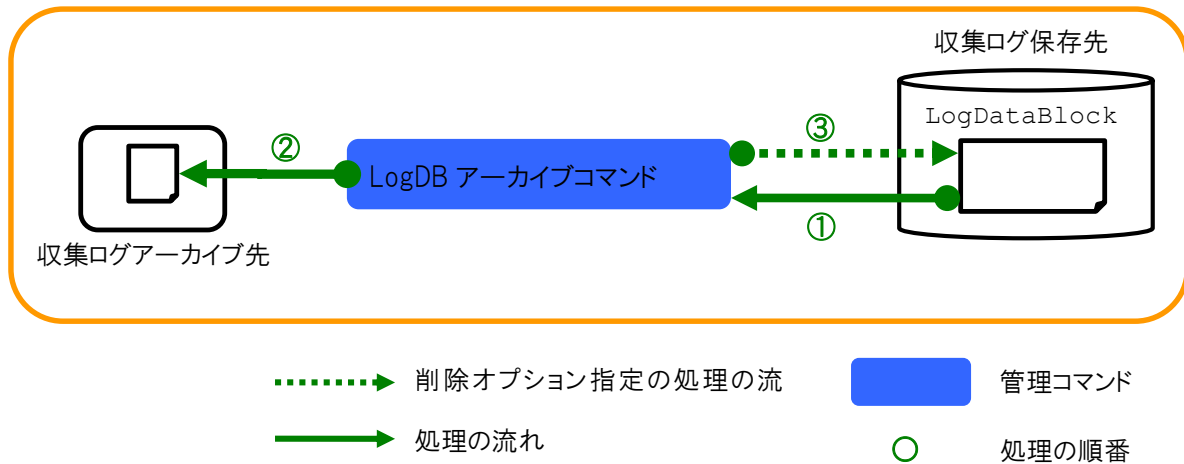
<コマンド例>

検索やレポートに使用するログデータは直近 1 ヶ月分(2010 年 2 月分)とし、2010 年 3 月 1 日 12 時 00 分に使わなくなった 2010 年 1 月の 1 ヶ月分の LogDB を削除する

```
c:¥logstorage¥bin¥logds.bat remove -tm 1
```


13. ログデータをアーカイブする

13.6. アーカイブコマンド停止時のログデータの扱い



①でアーカイブ対象期間のログデータを読み込みます。この時点でアーカイブコマンドが停止した場合は、再度コマンドを実行するようにプログラムしてください。この状態を確認する場合は、収集ログアーカイブ先に一時ファイル(tmp という名前の付いたファイル)があることで確認できます。一時ファイルの削除は必要ありません。

②で ZIP 形式のアーカイブファイルを指定した収集ログアーカイブ先に保存します。この時点で LogDB アーカイブコマンドが停止した場合は、再度コマンドを実行するようにプログラムしてください。この状態を確認する場合は、収集ログアーカイブ先にアーカイブファイルと一時ファイルがあることで確認できます。一時ファイルの削除は必要ありません。

③で削除オプション指定があった場合にアーカイブ対象期間のログデータを削除します。この時点で LogDB アーカイブコマンドが停止した場合は、LogDS 状態表示コマンドを実行して次の確認をしてください。

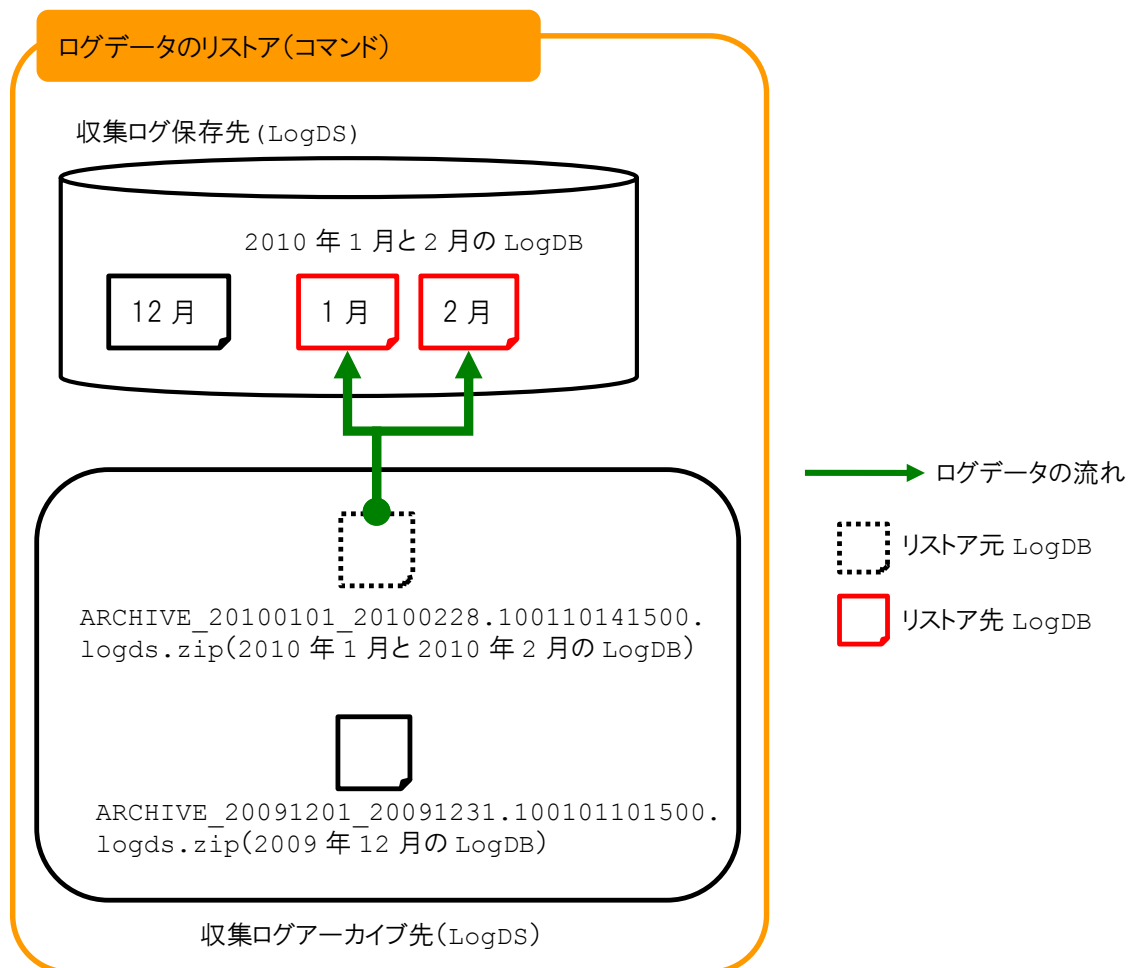
対象の LogDB に削除フラグが付いている場合は正常終了と同様に収集ログアーカイブ先のアーカイブファイルを扱って問題ありません。

対象の LogDB に削除フラグが付いていない場合は収集ログアーカイブ先のアーカイブファイルは正常終了と同様に扱って問題ありません。LogDS 内に対象の LogDB が残っているため、削除コマンドで対象の LogDB を削除してください。

14. ログデータをリストアする

14. ログデータをリストアする

14.1. ログデータのリストア機能



アーカイブした古い LogDB を LogDS へリストアするコマンドがあります。リストアは、主に古い LogDB を再度検索やレポートに利用する際に使用することを想定しています。

14. ログデータをリストアする

14.2. 古い LogDB をリストアする

アーカイブしておいた古い LogDB を検索やレポートに使用するために LogDB をリストアします。

古い LogDB をリストアするコマンド

<コマンド例>

2010 年 1 月 1 日 0 時にアーカイブした 2009 年 1 月から 2009 年 6 月までの LogDB を LogDS へリストアする。LogDS 内にリストアする対象期間の LogDB がある場合、エラーとせずスキップするには -m に skip を指定します。

```
c:¥logstorage¥bin¥logds.bat restore -a  
c:¥archive¥ARCHIVE_20090101_20090630.20100101000000.logds.zip -m error
```

2009 年 1 月から 2009 年 6 月までのアーカイブした LogDB のうち、1 月から 3 月のログをリストアする場合は、-m に skip を指定することで可能です。

14. ログデータをリストアする

14.3. システム復旧でアーカイブした LogDB をリストアする

IVEX Logger Viewer のシステム障害が発生し、システム復旧を行う際に過去にアーカイブした古い LogDB をリストアします。※システム復旧は LogDS のフルバックアップをするスナップショット機能でも対応可能です。

システム復旧でアーカイブした LogDB をリストアするコマンド

<コマンド例>

2010 年 1 月 1 日 0 時にアーカイブした 2009 年 1 月から 2009 年 6 月までのアーカイブした LogDB を全て LogDS へリストアする。LogDS 内にリストアする対象期間の LogDB がある場合は上書きする。

```
c:¥logstorage¥bin¥logds.bat restore -a  
c:¥archive¥ARCHIVE_20090101_20090630.20100101000000.logds.zip -m overwrite
```

14. ログデータをリストアする

14.4. リストアした LogDB を削除する

収集ログ保存先にリストアした LogDB を使わなくなったため削除します。

リストアした LogDB を削除するコマンド

<コマンド例>

リストアした 2009 年 12 月 1 ヶ月分の LogDB を削除する。ワイルドカード(*)を使用することによって 2009 年 12 月分の LogDB を一括指定することが可能です。

※ワイルドカード(*)を使用する場合、引数を二重引用符で囲む必要があります。

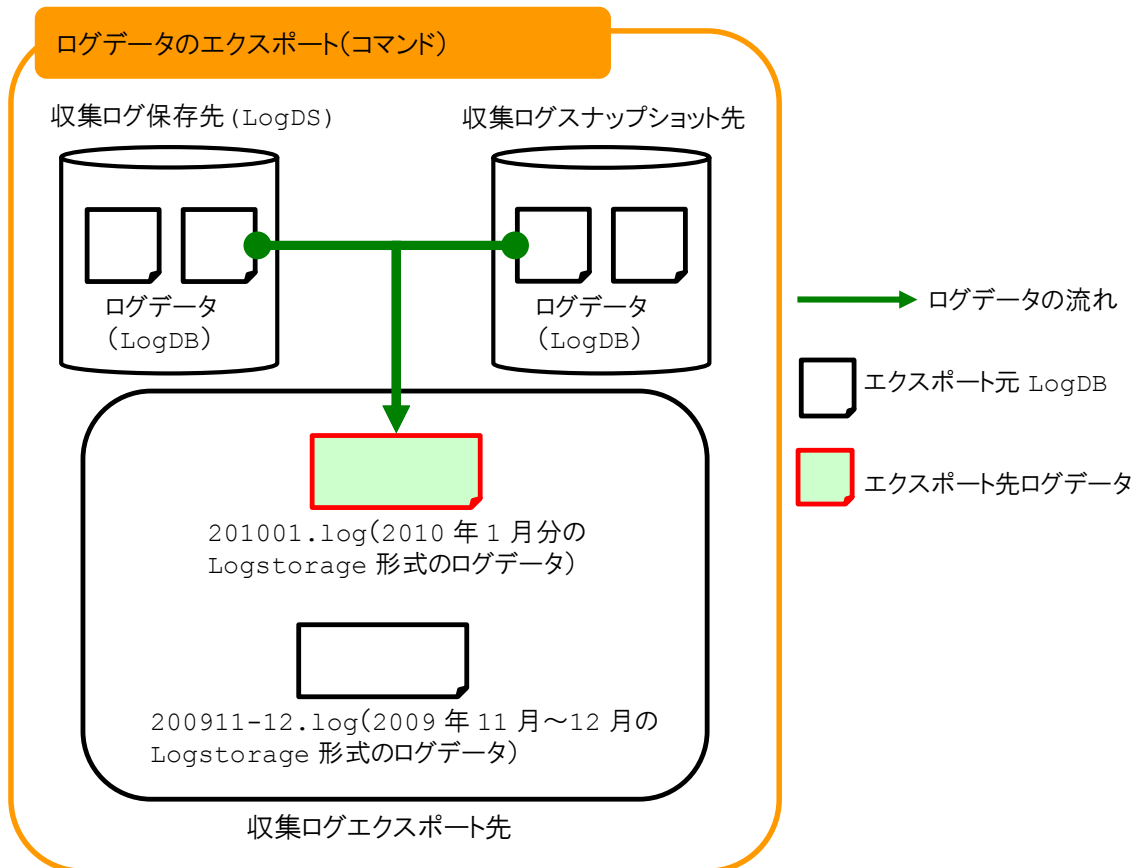
```
c:¥logstorage¥bin¥logds.bat remove -db "200912*"
```

複数の LogDB を指定する場合は、カンマ区切りで指定します。2009 年 11 月と 12 月を削除する場合は、
c:¥logstorage¥bin¥logds.bat remove -db "200911*,200912*" となります。

15. ログデータをエクスポートする

15. ログデータをエクスポートする

15.1. ログデータのエクスポート機能



収集ログ保存先(LogDS)または収集ログスナップショット先にある LogDB を IVEX Logger Viewer 形式のログデータにエクスポートするコマンドがあります。LogDB のエクスポート機能は主にログデータを外部に公開したり、別のツールを使って加工することを想定しています。ログデータが暗号化されている場合は、エクスポートするコマンドを使用して復号化する鍵を指定します。

15. ログデータをエクスポートする

15.2. 収集ログ保存先から IVEX Logger Viewer 形式のログデータをエクスポートする

ログデータの提出や別のシステムで加工するためにログデータをエクスポートします。

IVEX Logger Viewer 形式のログデータをエクスポートするコマンド

<コマンド例>

2010 年 1 月分のログデータを Windows:c:\¥exportlogs¥201001.log ファイルへエクスポートする。

```
c:\¥logstorage¥bin¥logds.bat export -o c:\¥exportlogs¥201001.log  
-s 20100101000000 -e 20100131235959
```

c:\¥snapshotlogs¥以下に 201001.log ファイルを作成する。

15. ログデータをエクスポートする

15.3. LogDB から IVEX Logger Viewer 形式のログデータを分割してエクスポートする

エクスポートする対象のログデータが大きいためファイルを分割してエクスポートします。

分割してエクスポートするコマンド

<コマンド例>

2009 年 11 月～2009 年 12 月分のログデータを c:\¥exportlogs¥200911-12.log へエクスポートし、100MB に達したらファイルを分割してエクスポートする。C:\¥exportlogs¥以下に 200911-12.log.0 ファイルを作成する。100MB に達したら 200911-12.log.1 ファイルを作成する。

```
c:\¥logstorage¥bin¥loggate.bat export -o c:\¥exportlogs¥200911-12.log  
-s 20091101000000 -e 20091231315959 -max 100M
```


15. ログデータをエクスポートする

15.4. スナップショットした LogDS から IVEX Logger Viewer 形式のログデータにエクスポートする

ログデータの提出や別のシステムで加工するためにスナップショットした LogDS からエクスポートします。

エクスポートコマンド

<コマンド例>

2010 年 2 月 10 日 14 時 15 分にスナップショットした LogDS から 2010 年 1 月分のログデータを c:¥exportlogs¥201001.log ファイルへエクスポートする。C:¥snapshotlogs¥以下に 201001.log ファイルを作成する。

```
c:¥logstorage¥bin¥logds.bat export
-ds c:¥snapshot¥SNAPSHOT_20100210141500.logds¥volume1¥logds
-o c:¥exportlogs¥201001.log
-s 20100101000000 -e 20100131235959
```

15. ログデータをエクスポートする

15.5. エクスポートした IVEX Logger Viewer 形式のログデータを削除する

必要の無くなった IVEX Logger Viewer 形式のログデータを削除します。削除については OS のファイル削除コマンドを使用することで削除します。

エクスポートした LogDS を削除するコマンド

<コマンド例>

2010 年 1 月分のエクスポートした IVEX Logger Viewer 形式のログデータを削除する

```
del c:¥exportlogs¥201001.log
```

15. ログデータをエクスポートする

15.6. IVEX Logger Viewer 形式のログ

ログソースから収集したログを IVEX Logger Viewer の検索処理や集計処理で使用するには、ログの形式が、IVEX Logger Viewer が扱える形式でなければいけません。IVEX Logger Viewer が扱えるログの形式を IVEX Logger Viewer 形式のログと呼びます。IVEX Logger Viewer 形式のログは以下の通りです。

YYYY-MM-DD hh:mm:ss IP アドレス (facility.priority) アプリケーション名: アプリケーションのログメッセージ

IP アドレス部分は ipv4 または ipv6 に対応します。

また、Agent や Syslog を使用した場合はログデータを送信する際に以下の形式でログを送信します。この形式では年情報が無いため、IVEX Logger Viewer 形式にする際 LogGate のシステム時間より年情報をつけて IVEX Logger Viewer 形式に変換します。

<PRI>MMM DD hh:mm:ss ログソース名 アプリケーション名 [プロセス ID]: アプリケーションが出力したログのメッセージ

No.	出力項目	概要	出力例
1	<PRI>	ファシリティとプライオリティを数字で表示します。	<174>
2	MMM	ログが出力されたタイムスタンプ(月)を英字(省略)で表示します。	Aug
3	DD	ログが出力されたタイムスタンプ(日)を数字(2文字、または空白+1文字)で表示します。	14
4	hh:mm:ss	ログが出力されたタイムスタンプ(時、分、秒)を表示します。	23:08:07
5	ログソース名	ログソースのホスト名、ipv4 アドレス、ipv6 アドレスのいずれかを表示します。なお、ipv6 リンクローカルアドレス(ZoneID)には対応していません。	Localhost
6	アプリケーション名	ログを出力したアプリケーション名(イベントログの場合はイベントソース名)を表示します。	Crond(pam_unix)
7	プロセス ID	ログを出力したアプリケーションのプロセス ID(イベントログの場合はイベント ID)を表示します。	6197
8	アプリケーションが出力したログのメッセージ	アプリケーションが実際に出力したログ(メッセージ)を表示します。	Session opened for user root by (uid=0)

なお、No.1～No.5 までを SYSLOG 形式のヘッダと呼びます。

表 35 ファシリティ一覧

ファシリティ	番号	内容
KERN	0	カーネルメッセージ
USER	1	ユーザ・プロセスメッセージ
MAIL	2	メール・サービスメッセージ
DAEMON	3	すべてのデーモン・プロセスメッセージ
AUTH	4	認証サービスメッセージ
SYSLOG	5	syslog メッセージ
LPR	6	印刷サービスメッセージ
NEWS	7	ニュースサービスメッセージ
UUCP	8	UUCP メッセージ
CRON	9	cron メッセージ
AUTH-PRIV	10	プライベート認証メッセージ
FTP	11	FTP メッセージ
NTP	12	NTP メッセージ
AUDIT (SECURITY)	13	セキュリティメッセージ
ALERT	14	アラートメッセージ
-	15	該当なし
LOCAL0~7	16~ 2 3	任意のメッセージ

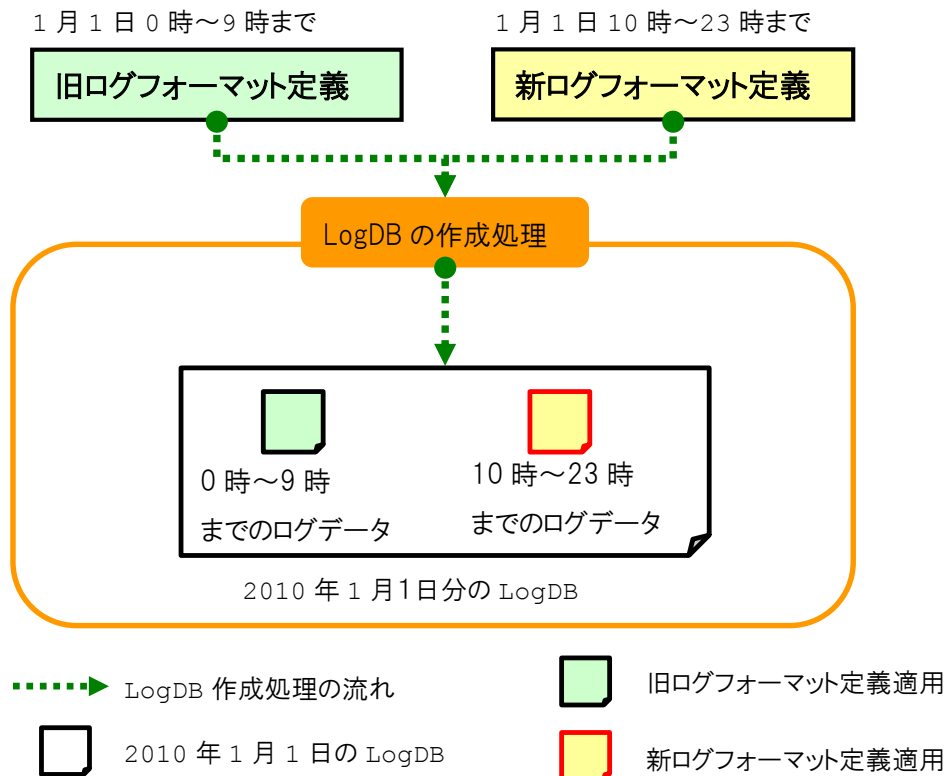
表 36 プライオリティ一覧

プライオリティ	番号	内容
EMERG	0	緊急
ALERT	1	アラート
CRIT	2	致命的
ERR	3	エラー
WARNING	4	警告
NOTICE	5	注意
INFO	6	各種情報
DEBUG	7	デバッグ

16. LogDB を再作成する

16.1. ログデータ(LogDB)の再作成機能

ある日の途中にログフォーマット定義が変わる際に LogDB を再作成する



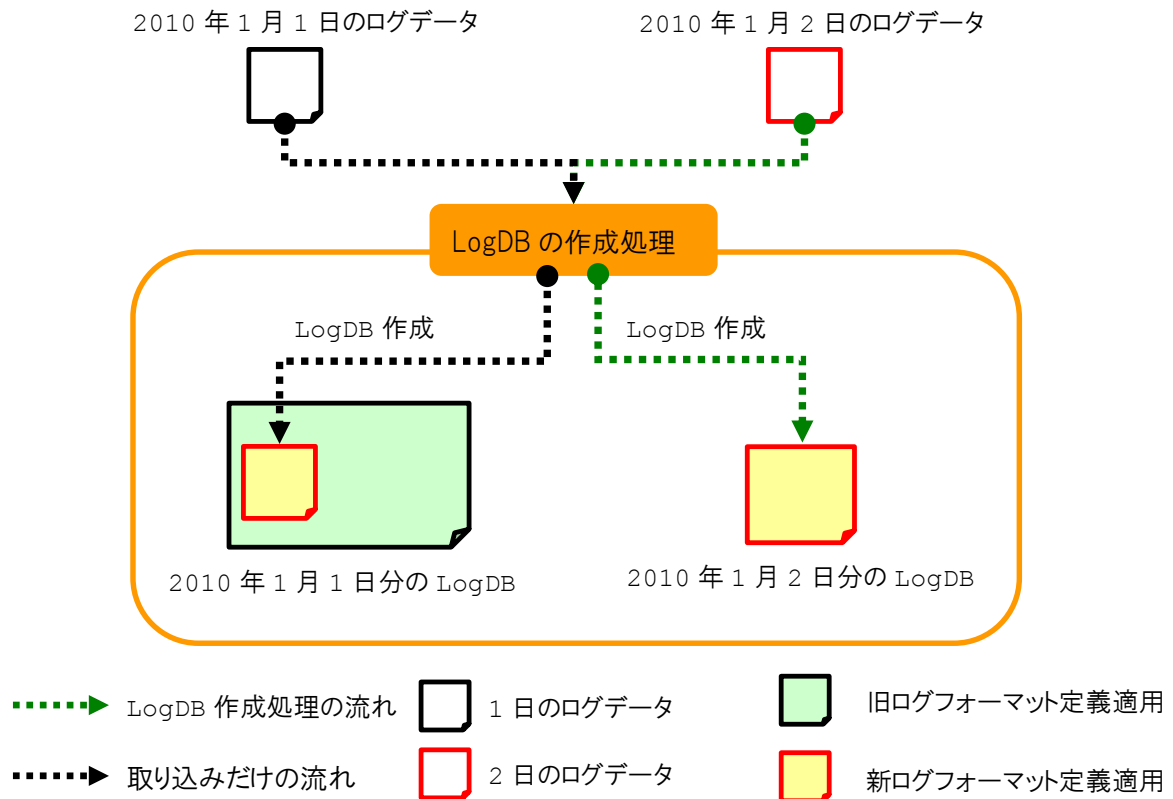
ログフォーマット定義を更新するタイミングによって LogDB 内に新旧のログフォーマット定義それぞれで構造化したログデータが混在することがあります。その際は古いログフォーマット定義で構造化したログデータを新しいログフォーマット定義を基に再作成する必要があります。

上記のケースでは、2010 年 1 月 1 日分の LogDB 内の 0 時～9 時までのログデータに対して再作成を行う必要があります。また、以前に収集したログデータを含む LogDB も旧ログフォーマット定義を適用しているため、検索等に利用する場合は、新ログフォーマット定義を適用するように LogDB を再作成する必要があります。

なお、再作成をせずに検索をした場合は、0 時～9 時までのログデータは旧ログフォーマットのまま検索されます。

16. LogDB を再作成する

古い日のログデータが届いた際に新ログフォーマット定義で LogDB を再作成する

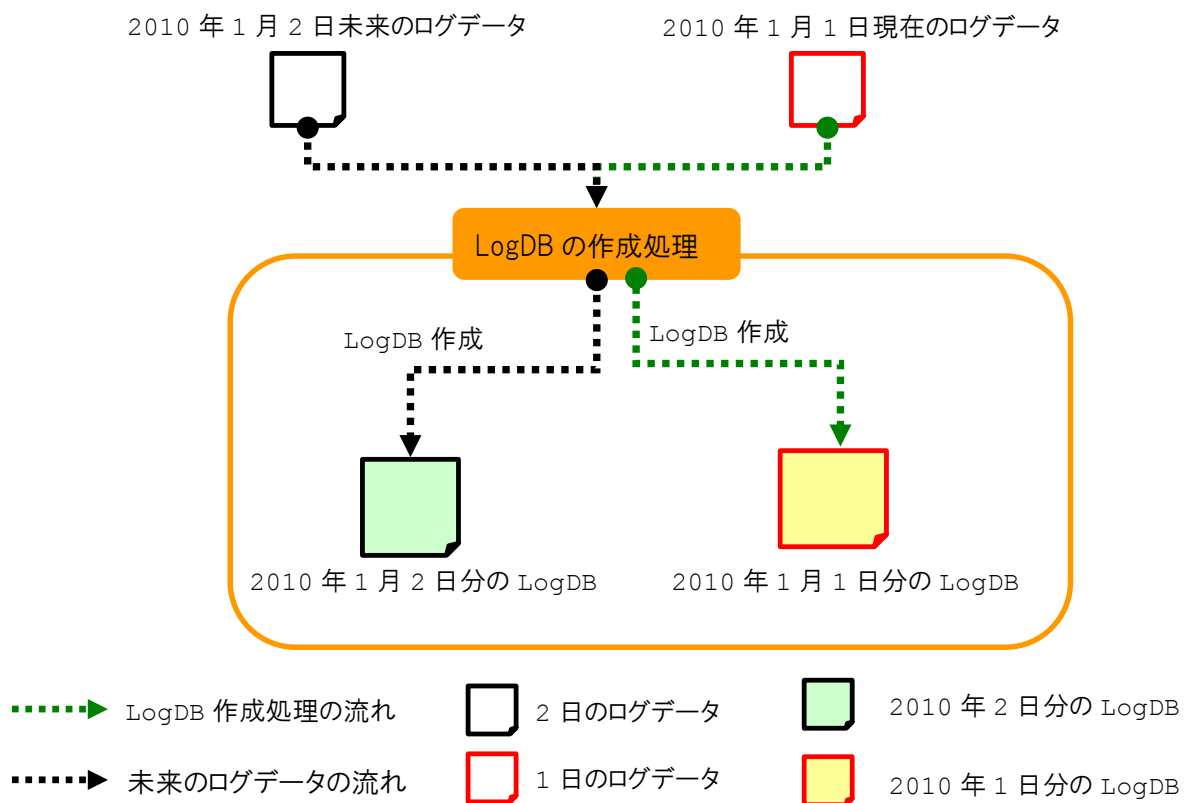


ログフォーマット定義を更新するタイミングによって LogDB ごとに新旧のログフォーマット定義が混在することがあります。また、現時点よりも古い(過去)のログデータが届くことがあります。古い(過去)のログデータについては、新ログフォーマット定義が適用され、1 つの LogDB 内にも新旧のログフォーマット定義が適用されたログデータが混在します。その際は、新しいログフォーマット定義を基に古い LogDB も再作成する必要があります。

上記のケースでは、2010 年 1 月 2 日現在に 2010 年 1 月 1 日分のログデータが届いた場合にログデータは新しいログフォーマット定義を基に 2010 年 1 月 1 日の LogDB へ取り込みます。再作成をせずに検索をした場合は、2010 年 1 月 1 日のログデータは旧ログフォーマットを基に、2010 年 1 月 2 日に届いた古い(過去)のログデータは新ログフォーマットで検索されます。

16. LogDB を再作成する

未来のログデータが届いた際は LogDB の再作成は不要です



古いログデータではなく、未来のログデータについてはその月の LogDB を作成します。

16. LogDB を再作成する

16.2. 旧ログフォーマット定義で適用された LogDB を再作成する

ログフォーマット定義を更新したため、旧ログフォーマット定義で構造化した LogDB を再作成します。再作成はコンソールサーバの管理画面から行います。

- (1)管理者で、コンソールサーバにログインします。
- (2)メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3)登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4)LogGate グループ情報画面で、LogDS の管理ボタンを押します。

The screenshot shows the LogGate configuration interface. At the top, there are tabs for 'LogGate', '改竄検出', and '略号化'. Below these, there are fields for 'パス' (Path) set to 'D:\volume1', 'フリースペースリミット (%)' (Free space limit (%)) set to '10', 'ディスク使用状況' (Disk usage status) with a '表示' (Show) button, and 'ディスク状態' (Disk status) with an 'OK' button. A checkbox labeled 'ボリュームはLogGateグループ内で共有される' (Volume is shared within the LogGate group) is checked. The main section is titled 'LogGate 1:' and contains a 'RUN' button, fields for 'ホスト名' (Host name) set to 'lio', 'IPアドレス' (IP address) set to '172.28.2.32', and 'RMIポート' (RMI port) set to '1099'. There are also checkboxes for '検索サーバにする' (Use as search server) which is checked, and a '検索優先度' (Search priority) dropdown set to '1'. A '検索時の同時実行数' (Number of concurrent searches) field is set to '1'. At the bottom of this section, there are buttons for 'LogGate: 詳細設定' (LogGate: Detailed settings) and 'LogDS: 管理' (LogDS: Manage), with the latter being highlighted by a red box. Below this section, there is a 'LogGate 2:' section with a '追加' (Add) button. At the bottom, there is a section for '検索サーバ選択アルゴリズム' (Search server selection algorithm) with radio buttons for 'ラウンドロビン' (Round robin), '優先度' (Priority), '分散クエリ' (Distributed query), and 'ローカルクエリ' (Local query). The 'ラウンドロビン' option is selected. At the very bottom, there is a checkbox for '未登録ログソースからのログを破棄する' (Delete logs from unregistered log sources) which is unchecked.

16. LogDB を再作成する

(3) 再作成したいログデータの期間を選択して実行ボタンを押します。

LogGate: lo

ウインドウ: [更新] [閉じる]

LogDS状態

- 再生成 オプション

☒ 期間指定

2013 年 1 月 から

2013 年 3 月 まで

☐ 全LogDBを再生成

実行

中止

+ LogDB表示フィルター

LogDS

LogDS:	lo
バージョン:	2
ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	全て最新ログフォーマット
電子署名設定ID:	無効
暗号化設定ID:	無効
最新スナップショットID:	46
データブロック数:	3
ログ総数:	46
シスログタイムスタンプ範囲:	2013/01/01 08:00:00 - 2013/03/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 14:34:57 - 2013/03/13 15:34:48
実行中管理操作:	なし

LogDB

[<< >>]

[▲]

+ 2013年1月

+ 2013年2月

+ 2013年3月

ウインドウ: [更新] [閉じる]

16. LogDB を再作成する

- (3) 更新ボタンを押して以下の「状態」欄の内容が「最新ログフォーマット」に変わったら対象の LogDB 再作成は終了です。

LogGate: lo

ウィンドウ: [更新] [閉じる]

LogDB 状態

再生成 オプション

LogDB再生成コマンドをLogGateに送信しました。

☒ 期間指定

2013 年 1 月 から
2013 年 3 月 まで

☐ 全LogDBを再生成

実行 中止

再生成結果

開始時間:	2013/03/13 15:38:12
終了時間:	-
成功:	-
失敗:	-
中止:	-

+ LogDB表示フィルター

LogDS

LogDS:	lo
バージョン:	2
ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	全て最新ログフォーマット
電子署名設定ID:	無効
暗号化設定ID:	無効
最新スナップショットID:	46
データブロック数:	3
ログ総数:	46
シスログタイムスタンプ範囲:	2013/01/01 08:00:00 - 2013/03/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 14:34:57 - 2013/03/13 15:34:48
実行中管理操作:	remake@logds

[<<] LogDB [▲]

- 2013年1月

月集計

ログ数:	34
シスログタイムスタンプ範囲:	2013/01/01 08:00:00 - 2013/01/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

201301

ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	再生成中 (OK) [中止]
ログ数:	34
シスログタイムスタンプ範囲:	2013/01/01 08:00:00 - 2013/01/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

- 2013年2月

月集計

ログ数:	10
シスログタイムスタンプ範囲:	2013/02/01 08:00:00 - 2013/02/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

201302

ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	待機中 [中止]
ログ数:	10
シスログタイムスタンプ範囲:	2013/02/01 08:00:00 - 2013/02/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

+ 2013年3月

ウィンドウ: [更新] [閉じる]

実行ボタンがグレー状態になっている場合は LogDB 再作成中です。

16. LogDB を再作成する

(3) 閉じるボタンを押して画面を閉じます。

以上が LogDB の再作成です。以下はその他の画面説明です。

以下のように「状態」が「再作成中」の状態でも閉じた後は継続して作成し続けます。右側の「中止」ボタンを選択すると LogDB 再作成が中断され、LogDB の内容は開始時の状態にロールバックされます。

- 2013年1月	
月集計	
ログ数:	34
シスログタイムスタンプ範囲:	2013/01/01 09:00:00 - 2013/01/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48
201301	
ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	再生 成中 (OK) [中止]
ログ数:	34
シスログタイムスタンプ範囲:	2013/01/01 09:00:00 - 2013/01/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

以下のようにログフォーマットID が赤色の場合は古いログフォーマット定義が適用されていることを表します。再作成を行い、最新にしてください。

- 2013年2月	
月集計	
ログ数:	10
シスログタイムスタンプ範囲:	2013/02/01 09:00:00 - 2013/02/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48
201302	
ログフォーマットID:	1113 [2013/03/12 16:44:04]
状態:	古いログフォー マット [再生 成]
ログ数:	10
シスログタイムスタンプ範囲:	2013/02/01 09:00:00 - 2013/02/01 10:00:00
受信タイムスタンプ範囲:	2013/03/13 15:34:48 - 2013/03/13 15:34:48

16. LogDB を再作成する

以下のように実行ボタンを押すと「再生成結果」というタイトルの表が表示されます。この表で LogDB 再作成の結果が分かります。また、この表は LogDB 再作成コマンド(logds.bat(sh) remake)が実行中の場合もその進捗状況を表示します。

LogGate: lo

LogDB状態

ウィンドウ: [更新] [閉じる]

- 再生成 オプション

☒ 期間指定

2013 年 1 月 から

2013 年 3 月 まで

☐ 全 LogDB を再生成

実行

中止

再生成結果

開始時間:	2013/03/13 15:43:17
終了時間:	2013/03/13 15:43:18
成功:	[201302]
失敗:	-
中止:	-

表 37 LogDB 再作成結果表の項目

項目	説明
開始時間	LogDB 再作成実行開始時間
終了時間	LogDB 再作成実行終了時間
成功	LogDB 再作成が正常に終了した LogDB
失敗	LogDB 再作成に失敗した LogDB -(ハイフン)は失敗無し
中止	LogDB 再作成をキャンセルした LogDB -(ハイフン)はキャンセル無し

16. LogDB を再作成する

LogDB 再作成コマンド

<コマンド例>

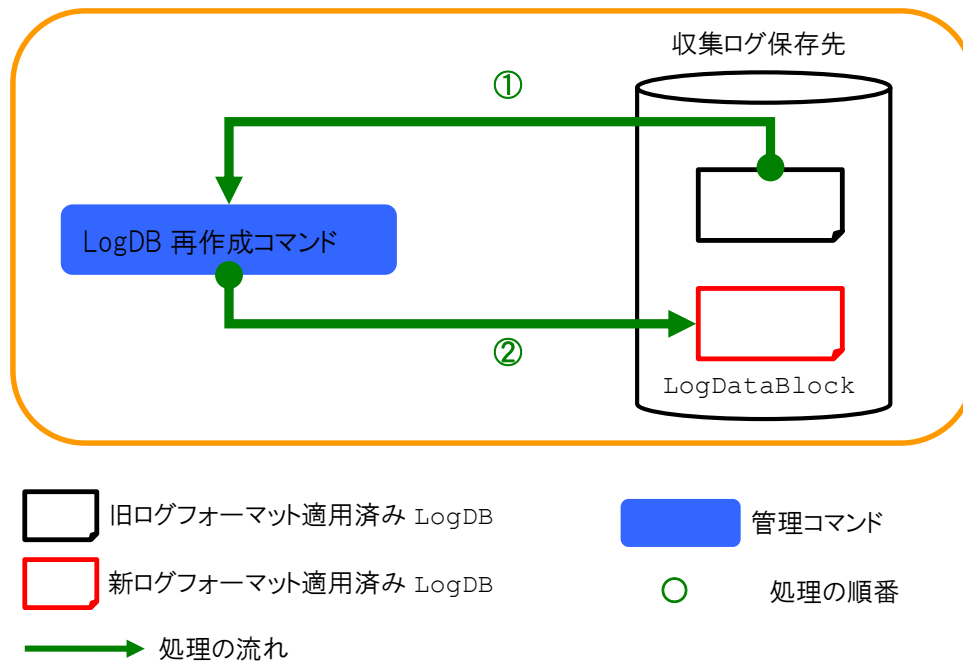
2010 年 1 月分の LogDB を再作成する

```
c:¥logstorage¥bin¥logds.bat remake -s 20100101000000 -e 20100131235959
```

LogDB が旧ログフォーマット定義で構造化されているかを確認するには LogDS 状態表示コマンドを使用します。

再作成の対象は LogDB(1 か月)単位です。日単位保存に変更していた場合は日単位での再作成になります。LogDB 再作成はコマンドを実行した LogGate が管理する LogDS 内の LogDB のみが対象です。アドバンスド版では個々の LogGate において LogDB 再作成コマンドを実行する必要があります。

16.3. LogDB 再作成コマンド停止時のログデータの扱い



①で再作成対象期間の LogDB を読み込みます。この時点で LogDB 再作成コマンドが停止した場合は、再度コマンドを実行するようにプログラムしてください。この状態を確認する場合は、LogDS 状態表示コマンドで旧ログフォーマット適用になっていることにより確認できます。

②で新ログフォーマット適用済み LogDB に保存します。この時点で LogDB 再作成コマンドが停止した場合は、再度コマンドを実行するようにプログラムしてください。この状態を確認する場合は、LogDS 状態表示コマンドで旧ログフォーマット適用になっていることにより確認できます。

16.4. LogDB 再作成が必要な場合

ログフォーマット定義の変更等、LogDB の再作成を必要とする場合について以降に説明します。

16.4.1. ログフォーマット定義の変更

以下はログフォーマット定義変更操作一覧です。緑色の箇所は LogDB 再作成が必要なログフォーマット定義変更操作です。ログフォーマット定義をする前(または変更前)にログデータを取り込んでいる場合において、緑色の箇所の操作を行った場合は LogDB の再作成を行ってください。

表 38 ログフォーマット定義変更操作一覧

項目	設定項目	変更内容	種別
アプリケーションリスト	アプリケーション	追加・削除	定義
アプリケーション定義	アプリケーション名	編集	表示
	概要	編集	表示
	アプリケーション識別	選択	定義
	正規表現	編集	定義
	ログソースリスト	追加・削除	定義
	区切り文字リスト	編集	トラッキング／表示
	優先度	編集	定義
	除外文字列	編集	トラッキング／表示
アクションリスト	アクション	追加・削除	定義
アクション定義	アクション名	編集	表示
	アクション概要	編集	表示
	正規表現	編集	定義
	ハイライト色	編集・選択	表示
	サンプルログ	編集	表示
	優先度	編集	定義
メッセージパラメータリスト	パラメータ	追加・削除	定義
メッセージパラメータ定義	パラメータ名	編集	表示
	概要	編集	表示
	正規表現	編集	定義
	正規表現グループ番号	編集	定義
	タグアサイン	選択	横断検索

16.4.2. 共有パラメータ化

Ver.5.0 以降、ログフォーマット定義において、1 アプリケーション内の複数のアクションで正規表現が同一であるメッセージパラメータは、1 度定義すれば全アクションに渡って共有できる様になりました(共有パラメータ)。

Ver.5.0 へバージョンアップした後、所定の操作に従ってログフォーマット定義の内容を共有パラメータ化する事でログフォーマット管理の負荷軽減だけでなく、LogDS の構成ファイル数の削減が見込めます。これにより、特にアドバンスド(AD)版環境で大量のログを複数台の LogGate で収集し、且つ LogDS を NAS に保存している場合にストレージ負荷を軽減する事が可能となります。定義の共有パラメータ化には、コンソールサーバの画面上での手動操作が必要です。詳細は「ユーザマニュアル」を参照してください。

本操作により、LogDB の再作成が必要となります(再作成により、LogDB のファイル構成が変更となります)。

16.4.3. LogDS 構成ファイル数削減

Ver.5.0 において LogDS の内部構造を変更し、構成ファイル数を削減しました。削減率はログ量やログフォーマット定義に依って大きく変動します。環境により、1/1000 程度までファイル数が削減できる場合があります。

複数の LogGate が NAS 上の LogDS に対してログの読書きをしている環境で、ファイル数の多さが原因で NAS に負荷を与えている場合、本バージョン以降の適用は特に改善効果が見込めます。

旧バージョンから Ver.5.0 以降にバージョンアップした場合、構成ファイル数削減の効果を享受する為には、LogDB の再作成が必要となります(尚、Ver.5.0 以降にバージョンアップ後に新たに作成された LogDB フォルダ以下の構成は、既にファイル数が削減された状態ですので LogDB 再作成は不要です。あくまで旧バージョンで既に作成されている LogDB のみが対象)。

第三部. IVEX Logger Viewer を運用する

第三部では、IVEX Logger Viewer の運用に関する設定方法について説明します。

17. ディスクをチェックする

17. ディスクをチェックする

17.1. 収集ログ保存先の使用量をチェックする

収集ログ保存先ディレクトリのディスク使用率(または使用量)をチェックし、ディスクフルになっているか、またはディスクフルになりそうかどうかを確認します。ディスクフルになる可能性がある場合は、ディスクの増設または収集したログのアーカイブ化等を行ってください。

- (1)管理者で、コンソールサーバにログインします。
- (2)メニューの「システムの設定」を選択して、「LogGate グループ」ボタンを押します。
- (3)登録された LogGate グループを選択して LogGate グループ情報画面を表示します。
- (4)LogGate グループ情報画面で、ディスク状態が OK であることを確認します。

LogGateグループ名: グループ1

概要:

LogGate 改竄検出 暗号化

パス: C:\volume1 フリー スペースリミット (%): 10 ディスク使用状況: 表示 ディスク状態: OK

☒ ボリュームはLogGateグループ内で共有される

☒ RUN LogGate 1:

ホスト名: lo

IPアドレス: 172.28.2.32

RMIポート: 1099

検索サーバにする: ☒

検索優先度: 1

検索時の同時実行数: 1

LogGate: 詳細設定

LogDS: 管理

LogGate 2: 追加

検索サーバ選択アルゴリズム: ☒ ラウンドロビン

☐ 優先度

☐ 分散クエリ

☐ ローカルクエリ

☐ 未登録ログソースからのログを破棄する

キャンセル

以上がディスク(収集ログ保存先)の使用量をチェックする方法です。

17. ディスクをチェックする

以下はディスク使用状況の画面です。



以下はディスク状態です。NG の状態では、LogGate が正常にログデータを受信できないため、ディスクを増やすなど対応をしてください。



17. ディスクをチェックする

17.2. IVEX Logger Viewer 関連ディレクトリの容量をチェックする

IVEX Logger Viewer 関連ディレクトリの中には運用中に容量が増えていくものがあります。以下のディレクトリについては容量の確認を行い、適宜対応をしてください。

IVEX Logger Viewer 内部データベース用ディレクトリ

コンソールサーバのホームディレクトリ以下の db ディレクトリは、コンソールサーバ上で行った設定情報を格納します。特に検知履歴やレポート作成履歴の蓄積により容量が増えていくことが予想されます。db ディレクトリの容量を定期的にチェックし、必要に応じてディスクの増設及び検知履歴やレポート作成履歴を削除してください。直接このディレクトリ内を操作しないようにしてください。

レポート保存先ディレクトリ

コンソールサーバのホームディレクトリ以下の report ディレクトリ(既定値)は、作成したレポートデータを格納します。レポート作成履歴の蓄積により容量が増えていくことが予想されます。レポート保存先ディレクトリの容量を定期的にチェックし、必要に応じてディスクの増設及びレポート作成履歴を削除してください。直接このディレクトリ内を操作しないようにしてください。

LogGate ワーク先

LogGate ワーク先はレシーバにより受信・取り込みしたログデータを一時的に格納します。受信・取り込みするログが一時的に増えることでこの LogGate ワーク先も容量が増えることが予想されます。時間の経過により LogGate ワーク先の容量は減りますが、受信・取り込みするログデータが定常的に増加している場合は必要に応じてディスクの増設をしてください。直接このディレクトリ内を操作しないようにしてください。

収集ログ保存先

収集ログ先はオンライン期間(検索・集計・レポート可能なログデータ保存期間)のログデータを格納します。ログデータは既定値では 1 ヶ月単位で保存します。当初想定したログデータが増えることでこの収集ログ保存先も容量が増えることが予想されます。このディレクトリの容量を定期的にチェックし、必要に応じてディスクの増設またはログデータの削除かアーカイブを行ってください。直接このディレクトリ内を操作しないようにしてください。

18. プロセスを監視する

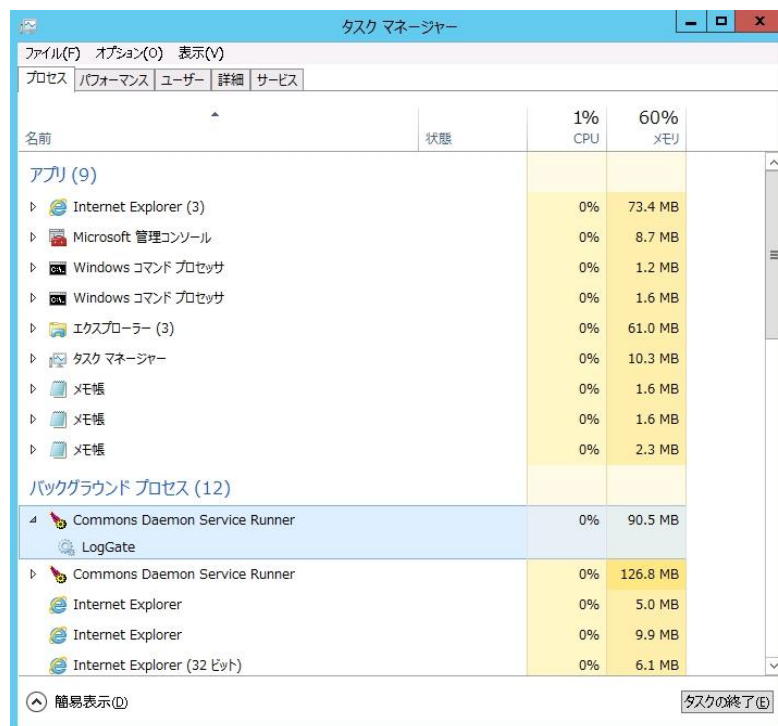
18. プロセスを監視する

IVEX Logger Viewer の起動プロセスを監視する際の参考となる情報として、LogGate・コンソールサーバの起動プロセス例について記載しています。

18.1. LogGate のプロセスを監視する

LogGate は起動時にプロセス ID ファイル(拡張子 pid)を /var/run/loggate.pid として用意します。このファイルを監視することで LogGate が起動されているかどうかを確認することができます。また、起動時のプロセスの状態は ps コマンドを使用して確認することができます。

例：LogGate の実行時のプロセス例(Windows タスクマネージャ)



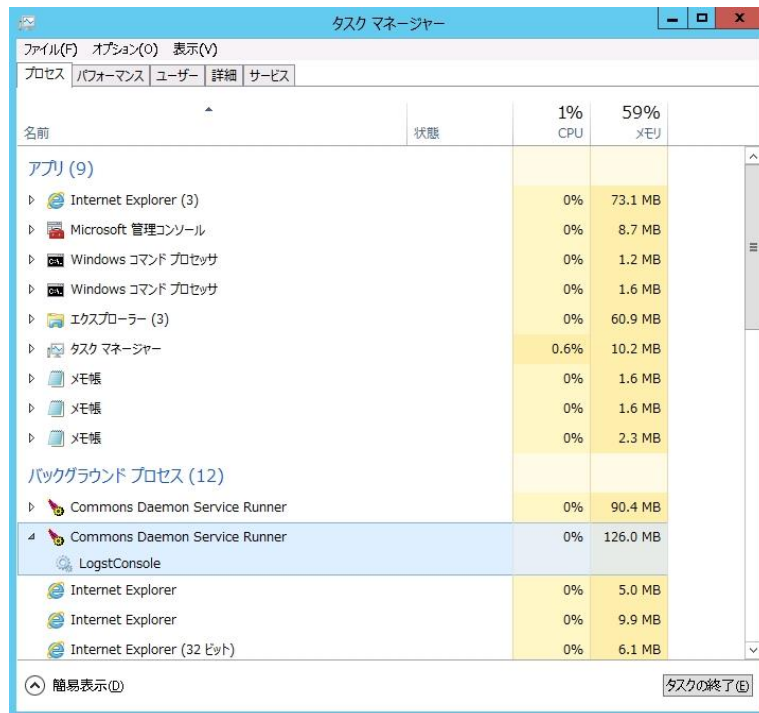
名前	状態	1% CPU	60% メモリ
アプリ (9)			
Internet Explorer (3)		0%	73.4 MB
Microsoft 管理コンソール		0%	8.7 MB
Windows コマンド プロセッサ		0%	1.2 MB
Windows コマンド プロセッサ		0%	1.6 MB
エクスプローラー (3)		0%	61.0 MB
タスク マネージャー		0%	10.3 MB
メモ帳		0%	1.6 MB
メモ帳		0%	1.6 MB
メモ帳		0%	2.3 MB
バックグラウンド プロセス (12)			
Commons Daemon Service Runner		0%	90.5 MB
LogGate		0%	126.8 MB
Commons Daemon Service Runner		0%	126.8 MB
Internet Explorer		0%	5.0 MB
Internet Explorer		0%	9.9 MB
Internet Explorer (32 ビット)		0%	6.1 MB

18. プロセスを監視する

18.2. コンソールサーバのプロセスを監視する

コンソールサーバは起動時にプロセス ID ファイル(拡張子 pid)を/var/run/logstd.pidとして用意します。このファイルを監視することでコンソールサーバが起動されているかどうかを確認することができます。また、起動時のプロセスの状態は ps コマンドを使用して確認することができます。

例:コンソールサーバの実行時のプロセス例(Windows タスクマネージャ)



名前	状態	1% CPU	59% メモリ
アプリ (9)			
Internet Explorer (3)		0%	73.1 MB
Microsoft 管理コンソール		0%	8.7 MB
Windows コマンド プロセッサ		0%	1.2 MB
Windows コマンド プロセッサ		0%	1.6 MB
エクスプローラー (3)		0%	60.9 MB
タスク マネージャ		0.6%	10.2 MB
メモ帳		0%	1.6 MB
メモ帳		0%	1.6 MB
メモ帳		0%	2.3 MB
バックグラウンド プロセス (12)			
Commons Daemon Service Runner		0%	90.4 MB
Commons Daemon Service Runner		0%	126.0 MB
LogstConsole			
Internet Explorer		0%	5.0 MB
Internet Explorer		0%	9.9 MB
Internet Explorer (32 ビット)		0%	6.1 MB

19. IVEX Logger Viewer のログをチェックする

19.1. 検知ログをチェックする

検知に関するログはLogGateシステムログに出力します。LogGateシステムログに以下のようなメッセージが出力された場合、検知バッファが足りていないことが想定します。

```
2011-03-02 10:26:32,673 WARN [StoreDirector] sensor.PolicyMatcher  
(PolicyMatcher.java:185) - Sensor buffer is full. [policy_name:10]
```

上記メッセージが出力された場合は、検知条件のバッファサイズを変更して下さい。メッセージの「policy_name」にバッファサイズが不足した検知条件名が出力します。

19.2. メモリログをチェックする

メモリに関するログはコンソールシステムログ及びLogGateシステムログに出力します。コンソールシステムログ及びLogGateシステムログに次のようなメッセージが表示された場合、コンソールサーバまたはLogGate上のメモリが足りなくなっている恐れがあります。

```
Java.lang.OutOfMemoryError
```

上記のメッセージが表示された場合は、コンソールサーバ及びLogGateが使用するメモリ容量を増加して下さい。コンソールサーバ及びLogGateが使用するメモリ容量の変更については、「5.メモリ設定を行う」をご覧ください。

19. IVEX Logger Viewer のログをチェックする

19.3. ログの受信ログをチェックする

LogGate システムログに次のようなログが出力された場合、ログフォーマット定義のメッセージパラメータの正規表現に誤りがある恐れがあります。

2011-04-01	10:48:32,923	WARN	[LogParse-1]	logging.LineParserImpl
(LineParserImpl.java:146) - No group 1				

上記メッセージの場合、「～何番目」の指定が間違っていることを表しており、～番目で示す「()」で括られたグループ番号が存在しないため、メッセージパラメータが取得できずにメッセージが出力されています。登録されたログフォーマット定義がログの出力形式と一致しているかを確認して下さい。

19.4. illegal.log について

illegal.log には LogGate でログを受信したものの、扱えない形式やサイズ超の理由により、LogDS に取り込まないと判断されたログが記録されます。

19.4.1. 形式不正

ログソースから収集したログを IVEX Logger Viewer の検索処理や集計処理で使用するには、ログの形式が、IVEX Logger Viewer が扱える形式でなければいけません。IVEX Logger Viewer が扱えるログの形式を IVEX Logger Viewer 形式(「15.6. IVEX Logger Viewer 形式のログ」参照)のログと呼びます。

一般的にログソースのアプリケーションから出力されるログや Windows のイベントログは、それぞれアプリケーション固有の形式や Windows のイベントログ固有の形式で出力します。

アプリケーションから出力されるログや Windows のイベントログは、LogGate へ収集される際に収集ツール (Agent や syslog や FTP 等) と IVEX Logger Viewer の各レシーバやログ変換スクリプトなどのツールにより、SYSLOG 形式に変換されて LogGate に収集します。

その後、SYSLOG 形式に変換されたログは、IVEX Logger Viewer のストアによってシーケンシャルログファイルに書き込まれる際に IVEX Logger Viewer 形式のログに変換されて書き込まれます。

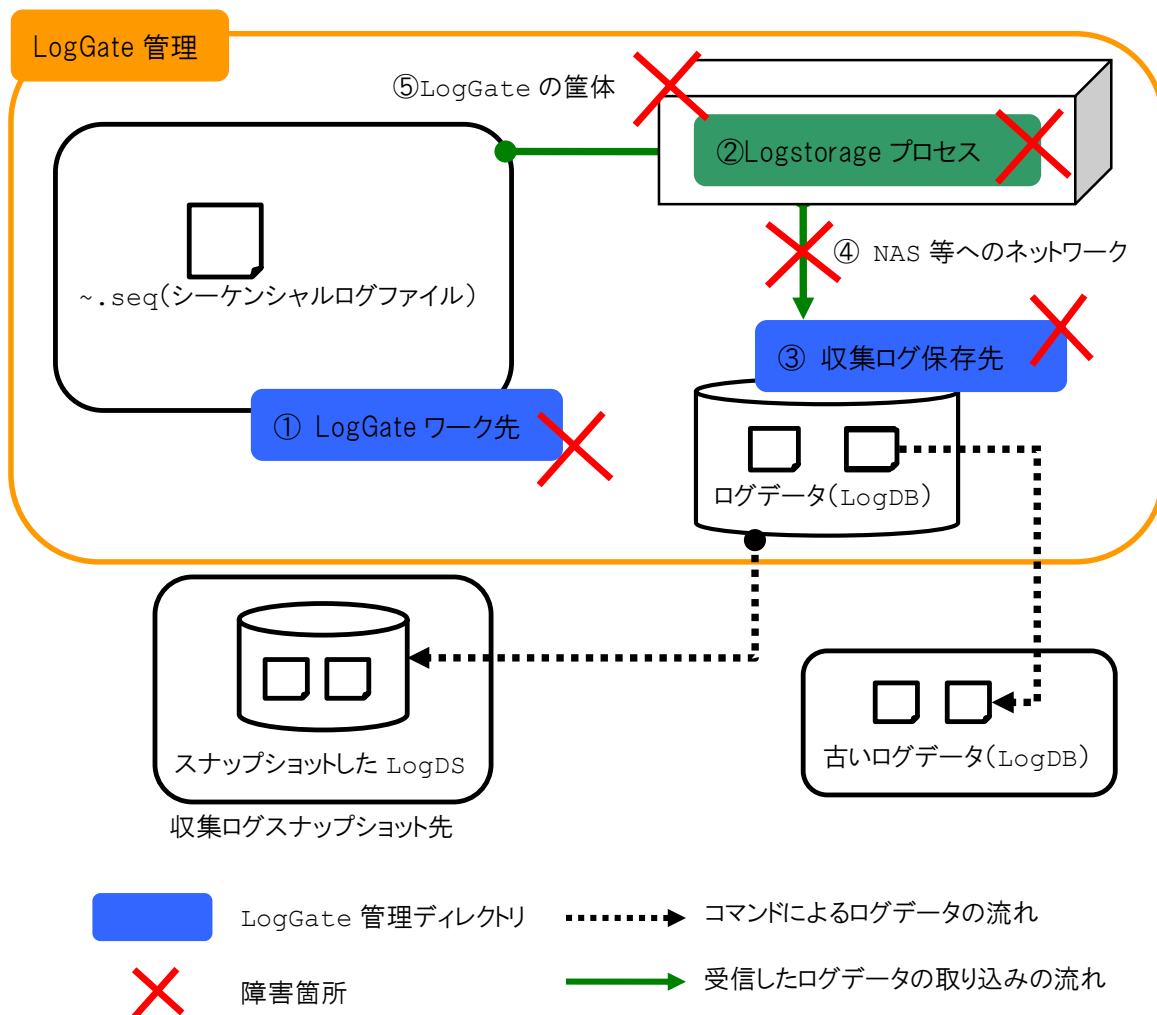
一方、IVEX Logger Viewer では受信したログが SYSLOG 形式ではないログの場合、受信したログを不正なログ(タイムスタンプやホスト名等が付加されていないため、信頼性の低いデータとして)として判断し、illegal.log に出力します。

19.4.2. 一行のログサイズ超過

LogDS が扱えるログ 1 行の最大長は 32KB(32,767Byte)です。これを超える長さのログは先頭 32KB のみを LogDS に取込み、受信した全行は illegal.log に出力されます。

20. IVEX Logger Viewer 関連データのバックアップを行う

20.1. IVEX Logger Viewer の環境障害概要



①は、構造化する前の受信したログデータを一時的に配置しています。取り込まれる前の状態のため、このディレクトリについては、RAID 等二重化を行うなどで障害対策を検討してください。

③は、構造化したログデータを保存します。バックアップソフトを使用せず、IVEX Logger Viewer のスナップショット機能を使用してフルバックアップを定期的に取り、バックアップソフトを使用して差分またはフルバックアップを定期的に取りなどで障害対策を検討してください。

②と④と⑤は、LogGate 冗長化や LogGate のシステムバックアップまたは、プロセス監視ツールなどで障害対策を検討してください。

20. IVEX Logger Viewer 関連データのバックアップを行う

20.2. IVEX Logger Viewer 関連データのバックアップ対象

IVEX Logger Viewer(コンソールサーバ及び LogGate)のシステム情報バックアップ対象ディレクトリは以下の通りです。

以下はコンソールサーバ管理画面による設定や LogGate システム設定の変更時に反映が関連するディレクトリです。設定変更時にバックアップすることを検討してください。

表 39 IVEX Logger Viewer バックアップ対象のディレクトリー一覧

ディレクトリ名	既定値でインストールした場合のパス	インストール対象サーバ
ホームディレクトリ	C:\logstorage	コンソールサーバ LogGate
レポート保存先	C:\logstorage¥report	コンソールサーバ
グラフ集計時のワーク	C:\logstorage¥stats	コンソールサーバ
LLTP 管理ファイル保存先	C:\loggateway¥lltp	LogGate

以下は容量が大きい場合、RAID 等二重化を行うなどで障害対策を検討してください。

LogGate ワーク先	C:\loggatewaywork	LogGate
シーケンシャルログ出力先	C:\loggatewaywork¥seqlog	LogGate

以下は長期間保存するものとして別途二次記憶媒体等へ退避を検討してください。

収集ログアーカイブ先	既定値はなし 指定ディレクトリ以下 ARCHIVE_対象開始年月日_対象終了年月日.作成時間.LogDS 名.zip ができる	LogGate
収集ログスナップショット先	既定値はなし 指定ディレクトリ以下に SNAPSHOT_時間.LogDS 名フォルダができる	LogGate
収集ログエクスポート先	既定値はなし 指定ディレクトリ以下に指定したファイルができる	LogGate

20. IVEX Logger Viewer 関連データのバックアップを行う

以下はその他関連するデータとしてバックアップを検討してください。

ディレクトリ名	既定値	インストール対象サーバ
サービス起動時の起動ユーザ情報	ローカルシステムアカウント	LogGate コンソールサーバ
時刻同期設定情報	既定値はなし	LogGate コンソールサーバ
プロセス監視情報	既定値はなし	LogGate コンソールサーバ
アーカイブプログラムの定期実行 (タスクスケジューラ/Crontab)	既定値はなし	LogGate
ログ変換スクリプトプログラム	既定値はなし FTP レシーバによるロファイル受信または ファイルレシーバによるログファイル取り込み時に使用	LogGate
外部レポートエンジンデータ	既定値はなし カスタマイズしたレポートの作成に使用	コンソールサーバ

20.3. バックアップを行う際の注意事項

IVEX Logger Viewer システムは、市販のバックアップツール、ソフトウェアを使って IVEX Logger Viewer を稼働させたままファイルのバックアップを行うことができます。IVEX Logger Viewer システムを稼働させたままファイルのバックアップを行う場合は、バックアップ時にファイルを排他制御にせずにバックアップを取得するように設定して下さい。ファイルを排他制御してバックアップを取得した場合、IVEX Logger Viewer がファイルを使用できずに異常終了する場合があります。

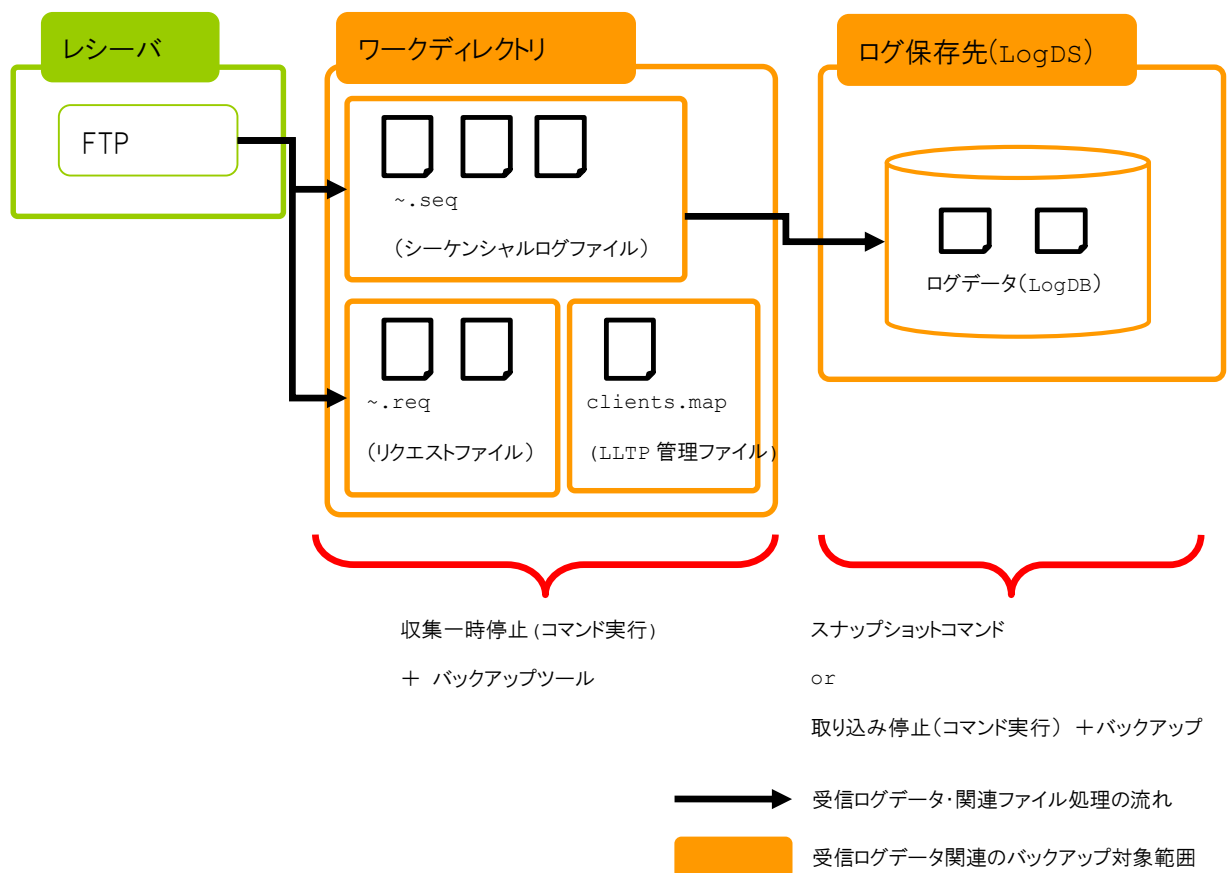
21. LogDS・ワーク・シーケンシャルログをバックアップする

LogGate が収集したログ(LogDS)と収集処理中に作成される各種ワーキングファイル、一時保存(シーケンシャルログ)ファイルの整合性を保ってバックアップする方法を説明します。

21.1. 収集処理のデータフロー

LogGate の各種レシーバはログを受信すると、シーケンシャルログファイル(既定ではワークディレクトリ下の“seqlog”ディレクトリに保存)に逐次追記を行い、一定のタイミングで LogDS に保存します。

この処理サイクルでは、レシーバの処理状況やログソースとの通信状態、シーケンシャルファイルの処理位置等の情報が、適宜所定のファイルに記録されていきます。従って、収集したログデータをバックアップする際はそれらの関連情報も含め、整合性が取れた状態で行う必要があります。以下は、レシーバが受信したログデータがワークディレクトリやログ保存先に格納されていくフローのイメージを表しています。



21. LogDS・ワーク・シーケンシャルログをバックアップする

ログ受信処理は止めずにログデータに不整合なく安全にバックアップを行うには、ワークディレクトリと LogDS を同じタイミングで定常状態(=収集プロセスによる各種ファイル書込みが行われていない、一定の処理が完了した状態)に遷移させる必要があります。図の様に、ワークディレクトリは収集一時停止コマンドとバックアップツール、LogDS はスナップショットコマンド若しくは LogDS 取り込み停止コマンドとバックアップツールによるバックアップを行います。

尚、LogDS はコンソールサーバの内部データベースが保持する「ログフォーマット定義 ID」に基づいてログデータを保存しており、LogDS 内でもこの定義 ID を保有しています。LogDS をリストアする際、LogDS 内のログフォーマット定義 ID がコンソールサーバ内部データベースの同値よりも新しい場合、リストアすることはできません。

従って、LogDS のバックアップと同時に内部データベースのバックアップを取得することを推奨します(リストア対象 LogDS 内のログフォーマット定義 ID が内部データベースの同値よりも古い場合はリストア可能ですが、LogDB の再作成が必要となります)。

内部データベースの取得タイミングは、後述の LogDS・ワーク・シーケンシャルログバックアップの取得手順内で行う必要性はありません。これらのバックアップ前後で、ログフォーマット定義が更新していないことを確認の上、取得してください。取得方法については、「E.41 内部データベースバックアップコマンド」を参照してください。リストア時のログフォーマット定義 ID 確認方法については「22 バックアップデータから IVEX Logger Viewer のシステムを復旧する」を参照してください。

- (1) LogDS 取り込み停止コマンドの実行(loggate.{bat|sh} stop storing)
- (2) 収集一時停止コマンドの実行(loggate.{bat|sh} pause)
- (3) ワークディレクトリ・シーケンシャルログのバックアップ(ファイルコピーやバックアップツールによる)
- (4) LogDS のバックアップ(以下何れかの方法を選択してください)
 - ・ファイルコピーやバックアップツールによるバックアップ
 - ・LogDS スナップショットコマンド(logds.{bat|sh} snapshot)の実行によるバックアップ
- (5) 収集一時停止解除コマンドの実行(loggate.{bat|sh} unpause)
- (6) LogDS 取り込み開始コマンドの実行(loggate.{bat|sh} start storing)

21. LogDS・ワーク・シーケンシャルログをバックアップする

スナップショットコマンドの場合、実行時点の LogDS 全てのデータを取得することになるため、収集ログ量や保存先のディスク I/O 性能などによっては取得時間がかかり、定期レポート処理など運用に影響が出る可能性があります。

スナップショットコマンドを使用しない場合は、バックアップ処理を IVEX Logger Viewer の機能外で実施する必要があります。バックアップツールなどを用いて差分を都度取得することで収集処理の停止時間を短くすることができますが、リストア時に差分で取得しておいたデータのマージなど作業手順を別途検討する必要があります。

上記を考慮し、運用に即したバックアップ方法を検討してください。

21. LogDS・ワーク・シーケンシャルログをバックアップする

21.2. ワーク・シーケンシャルログをバックアップする

ワークディレクトリとシーケンシャルログをバックアップする方法、手順は以下の通りです。

(1) LogDS 取り込み停止コマンドの実行

```
> %LOGST_HOME%\bin\loggate.bat stop storing
```

(2) 収集一時停止コマンドの実行

```
> %LOGST_HOME%\bin\loggate.bat pause
```

(3) ワークディレクトリ・シーケンシャルログのバックアップ

ワークディレクトリ、シーケンシャルログファイルを OS のコピーコマンドやバックアップツールでバックアップします。バックアップ対象は以下です。

尚、表内のファイルパス区切りは Windows 表記、%LOGGATE_WORK%、%LOGGATE_SEQ%は LogGate 設定画面で指定する項目（ワーク先、シーケンシャルログ出力ディレクトリ）を指します。

項目	説明
%LOGGATE_WORK%\filerceive	ファイルレシーバ利用時に作成されるディレクトリ。処理中の一時ファイル（リクエストファイル）や位置情報ファイル（ロケーションファイル）を格納。
%LOGGATE_WORK%\ftp	FTP レシーバ利用時に作成されるディレクトリ。処理中の一時ファイル（リクエストファイル）や位置情報ファイル（ロケーションファイル）を格納。
%LOGGATE_WORK%\logds	LogDS の処理状態の内、ロールバックや最適化に必要な情報を格納したディレクトリ。
%LOGGATE_WORK%\pause	LLTP レシーバ利用時の定常状態に遷移させた管理ファイルを格納したディレクトリ。
%LOGGATE_SEQ%	シーケンシャルログ出力ディレクトリ。インストール時の既定値は%LOGGATE_WORK%\seqlog

一時停止コマンド実行時点でファイル転送前の状態の FTP コネクションは強制的に切断され、クライアントにエラーが返されます。既にファイルが転送中の場合は強制的に中断されず、アップロードのみ行われる場合があります（但し後続のシーケンシャルログ書込み処理などは行われず、一時停止コマンド自体は正常終了、一

21. LogDS・ワーク・シーケンシャルログをバックアップする

時停止状態となっています)。この場合、以下の動作ログが出力されていますので、同ログが出力されていた場合は一時停止解除コマンド実行後、ファイルを再送してください。

```
Uploaded file [filename.log] will not be processed by Logstorage because no
Ftplets matched. Please check your Ftplet settings.
```

また、一時停止状態では FTP クライアントからの接続要求自体にエラーが返されます。

転送完了後、シーケンシャルログ書き込み処理の前にログ変換スクリプトを実行している場合は、この変換処理が完了した時点で一時停止状態となります。一時停止により中断した処理は、一時停止解除コマンド実行後、再開されます。

ファイル/アドホックファイルレシーバの場合は、監視対象ディレクトリの監視を停止します。後続のログ変換スクリプトやシーケンシャルログ書き込み処理については FTP レシーバと同じ動作となります。

原則として、ファイル転送や監視ディレクトリにファイル配置が行われない時間帯でバックアップを行ってください。

(4) LogDS のバックアップ

「21.3 LogDS をバックアップする」を参照してください。

(5) 収集一時停止解除コマンドの実行

```
> %LOGST_HOME%\bin¥loggate.bat unpause
```

(6) 取り込み開始コマンドの実行

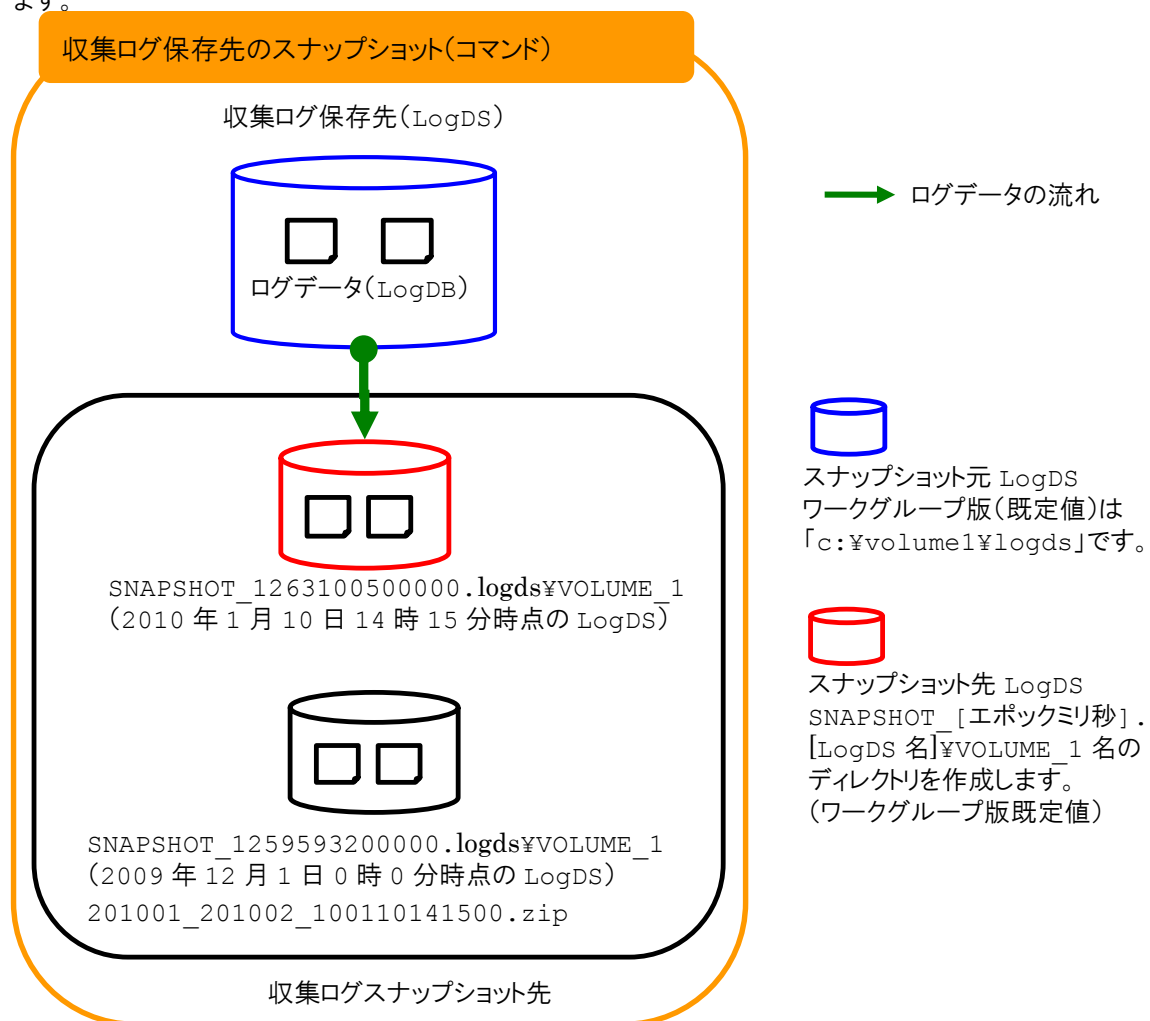
```
> %LOGST_HOME%\bin¥loggate.bat start storing
```

21.3. LogDS をバックアップする

LogDS のバックアップはスナップショットコマンドか、取り込み停止コマンドの実行及びバックアップツールでのファイルコピーによるバックアップで行います。バックアップのタイミングはワークディレクトリ、シーケンシャルログのバックアップと同タイミングを推奨します(「21.2 ワーク・シーケンシャルログをバックアップする」を参照)。

21.3.1. スナップショットコマンド

LogDS のスナップショットコマンドは、主にシステムの障害対策によるフルバックアップ用途で使用することを想定しています。このコマンドで取得したデータは IVEX Logger Viewer のシステム復旧時に手動でリカバリさせます。



21. LogDS・ワーク・シーケンシャルログをバックアップする

スナップショットコマンドの実行例(2010 年 1 月 10 日 14 時 15 分に実行した場合)は以下の通りです。

```
> %LOGST_HOME%\bin¥logds.bat snapshot -d c:¥snapshot
```

コマンド実行後、-d オプションで指定したディレクトリの下に「SNAPSHOT_[システムミリ秒].[LogDS 名]¥VOLUME_1」というディレクトリが作成され、その下に LogDS ディレクトリの「volume1」以下全てがコピーされます(バックアップツールが有する差分バックアップやスケジューリング機能はありません)。

コマンド実行中は、自動的にログ収集が停止した状態(取り込み停止コマンド実行と同じ状態)となり、シーケンシャルログファイルまでのログ受信状態となり、コマンド実行完了後、自動的に収集を開始し、シーケンシャルログからの取り込みを再開します。

尚、スナップショットコマンドの対象は、実行した LogGate が管理する LogDS ディレクトリのみです。アドバンスト版では個々の LogGate で同コマンドの実行が必要となります。

既を取得したスナップショットを削除する場合は、OS のコマンド等により手動で上記フォルダを削除してください。

21. LogDS・ワーク・シーケンシャルログをバックアップする

21.3.2. バックアップツール

バックアップツールによるバックアップ方法、手順は以下の通りです。アドバンスド版の場合、個々の LogGate で同じ手順にて実施してください。

(1) LogDS 取り込み停止コマンドの実行

```
> %LOGST_HOME%\bin¥loggate.bat stop storing
```

(2) バックアップツールの実行

取得対象はコンソールサーバの画面より、LogGate グループ情報画面の LogGate タブに表示される「パス」欄に記載のディレクトリ以下です。

バックアップツールの機能、LogDS 取り込み停止可能時間によって取得方法は様々です。運用方針に沿って最適なバックアップ方法を検討してください。バックアップに最低限必要な機能はファイルコピーのみです。

(3) LogDS 取り込み開始コマンドの実行

```
> %LOGST_HOME%\bin¥loggate.bat start storing
```

21. LogDS・ワーク・シーケンシャルログをバックアップする

21.4. バックアップソフトで収集ログ保存先をバックアップする

バックアップソフトで収集ログ保存先をバックアップする手順は以下の通りです。

(1) LogGate にて以下のコマンドを実行してログデータの取り込みを停止します。

アドバンスド版の場合、個々の LogGate にて以下のコマンドを実行してください。

```
c:¥logstorage¥bin¥loggate.bat stop storing
```

(2) バックアップソフトを使用して収集ログ保存先をバックアップします。

(3) バックアップ終了後、以下のコマンドを実行してログデータの取り込みを開始します。

アドバンスド版の場合、個々の LogGate にて以下のコマンドを実行してください。

```
c:¥logstorage¥bin¥loggate.bat start storing
```

以上がバックアップソフトで収集ログ保存先をバックアップする手順です。

22. バックアップデータから IVEX Logger Viewer のシステムを復旧する

バックアップを使用した IVEX Logger Viewer のシステム環境の再構築を行う手順を下記に示します。

(1) IVEX Logger Viewer を再インストールします。

インストール方法については製品に付属している「IVEX Logger Viewer インストールマニュアル」をご覧ください。なお、再構築前に稼働していたバージョンの IVEX Logger Viewer をインストールして下さい。

(2) 「20.IVEX Logger Viewer 関連データのバックアップを行う」でバックアップを取ったデータを使って上書きコピーをします。

※フルインストールの場合は LogGate とコンソールサーバのホームディレクトリは同じです。

(3) 「21.LogDS・ワーク・シーケンシャルログをバックアップする」で取得したワーク・シーケンシャルログ・LogDS をリストアします。

リストアの際、コンソールサーバの内部データベースとリストア対象の LogDS が保有するログフォーマット定義 ID が一致（若しくは LogDS 側が小さい値）することを確認してください。以下、ID=6 で一致する場合のコマンド例です（赤字箇所が一致していることの確認）。

```
> %LOGST_HOME%\bin\console.bat db logfmtid -t db-20130331.tar.gz
LogFormat ID : 6 [2013/03/02 14:58:12]
> %LOGST_HOME%\bin\logds.sh status - ds
c:\backup\SNAPSHOT_20130331002312046_FULL.gate1\volume1\gate1 (実際は 1 行)
LogDS: gate1
Version: 2
LogFormatID: 6
```

(4) その他、時刻同期設定やプロセス監視の設定を確認します。

この操作は必要に応じてコンソールサーバと LogGate に行います。

(5) コンソールサーバを起動します。

(6) LogGate を起動します。

22. バックアップデータから IVEX Logger Viewer のシステムを復旧する

(7) ブラウザからアクセスできることを確認します。

以上がバックアップから IVEX Logger Viewer のシステムを復旧する手順です。

付録A. 設定ファイル一覧

IVEX Logger Viewer の設定ファイルについて説明します。IVEX Logger Viewer を既定値でインストールした場合、設定ファイルは以下のディレクトリに保存します。

C:¥logstorage¥conf

C:¥logstorage¥logstd¥WEB-INF

IVEX Logger Viewer の設定ファイルは以下の通りです。

表 40 IVEX Logger Viewer の設定ファイル一覧

ファイル名	概要	設定対象サーバ
logstd.dcf	コンソールサーバ設定ファイル (兼 LogGate 設定ファイル)	コンソールサーバ ただしコンソールサーバと LogGate が同居構成の場合は 同居する LogGate も参照
loggate.dcf	LogGate 設定ファイル	LogGate (LogGate 単体構成の場合)
server.xml	Web サーバ設定ファイル	コンソールサーバ
log4j_console.xml	システムログ出力設定ファイル (コンソールサーバ)	コンソールサーバ
log4j_loggate.xml	システムログ出力設定ファイル (LogGate)	LogGate
log4j_admin-console.xml	コンソールサーバ管理コマンド用ログ設定ファイル	コンソールサーバ
log4j_admin-loggate.xml	LogGate 管理コマンド用ログ設定ファイル	LogGate
log4j_admin-logds.xml	LogDS 管理コマンド用ログ設定ファイル	LogGate
log4_supporttools.xml	診断コマンド用ログ設定ファイル	コンソールサーバ及び LogGate
policy	セキュリティ設定ファイル	コンソールサーバ及び LogGate
licensekey	ライセンス・キー	コンソールサーバ
ftpd.xml	FTP サーバ設定ファイル	LogGate
user.gen	FTP ユーザ設定ファイル	LogGate
ftp/	FTP 設定ディレクトリ	LogGate
report/	レポートディレクトリ	コンソールサーバ
web.xml	ブラウザ接続設定ファイル	コンソールサーバ
volume.properties	ログ保存領域設定ファイル	LogGate
.logst_keystore	改竄検出機能用キーストア	LogGate
rmi.properties	RMI 設定ファイル	LogGate

A.1. コンソールサーバ設定ファイル

コンソールサーバが使用する設定ファイルです。コンソールサーバと LogGate が同居構成(フルインストール時)の場合は、LogGate もこの設定ファイルを使用します。logstd.dcf ファイルには、コンソールサーバの設定情報、内部データベースの接続情報、LogGate の設定情報が記載されています。

A.2. LogGate 設定ファイル

LogGate が使用する設定ファイルです。LogGate が単体構成(単体インストール時)の場合は、LogGate はこの設定ファイルを使用します。loggate.dcf ファイルには、LogGate の設定情報が記載されています。

A.3. Web サーバ設定ファイル

コンソールサーバが使用する設定ファイルです。Web サーバの起動や接続に関する設定情報が記載されています。

A.4. システムログ出力設定ファイル(コンソールサーバ)

コンソールサーバが使用する設定ファイルです。コンソールサーバが出力するログに関する設定情報が記載されています。IVEX Logger Viewer が出力するログ及びログの出力設定方法については、「19. IVEX Logger Viewer のログをチェックする」をご覧ください。

A.5. システムログ出力設定ファイル(LogGate)

LogGate が使用する設定ファイルです。LogGate が出力するログに関する設定情報や IVEX Logger Viewer 形式ではないログを受信した際の保存先等の設定情報が記載されています。IVEX Logger Viewer が出力するログ及びログの出力設定方法については、「19. IVEX Logger Viewer のログをチェックする」をご覧ください。

A.6. コンソールサーバ管理コマンド用ログ設定ファイル

コンソールサーバ管理コマンドが使用する設定ファイルです。コマンドラインによるユーザ管理、レポート管理、インポート・エクスポートのコマンド実行記録を出力する設定情報が記載されています。

A.7. LogGate 管理コマンド用ログ設定ファイル

LogGate 管理コマンドが使用する設定ファイルです。コマンドラインによる取り込み停止、収集一時停止などのコマンド実行記録を出力する設定情報が記載されています。

A.8. LogDS 管理コマンド用ログ設定ファイル

LogGate が使用する設定ファイルです。LogDS 管理コマンドの実行結果(ログ)を出力する設定情報が記載されています。なお、LogGate が起動時の場合は loggate.log に LogDS 管理コマンドの実行結果が反映されます。この設定ファイルに記載の admin-logds.log には LogGate が停止中の場合の実行結果を反映します。

A.9. 診断コマンド用ログ設定ファイル

診断コマンドが使用する設定ファイルです。診断コマンドの実行結果(ログ)を出力する設定情報が記載されています。診断コマンドには情報収集コマンドと LogDS ビューアコマンドの 2 種類が存在します。

A.10. セキュリティ設定ファイル

コンソールサーバと LogGate の動作に関するセキュリティポリシーを設定するファイルです。コンソールサーバと LogGate が同居構成(フルインストール時)の場合は、LogGate もこの設定ファイルを使用します。このファイルは変更の必要はありません。

A.11. ライセンス・キー

コンソールサーバを起動するためのライセンス・キー情報です。コンソールサーバが使用します。licensekey ファイルが存在しない場合や、licensekey ファイルがテンポラリライセンス・キーで試用期限が切れている場合は、コンソールサーバを起動することはできません。

A.12. FTP サーバ設定ファイル

ログを FTP で受信する際の FTP サーバの動作(起動やシステム管理)に関する設定、IP アドレスによるアクセス制限情報が記載されています。LogGate が使用します。ログを FTP で受信する際に設定します。ftpd.xml ファイルはコンソールサーバから操作を行うことで更新されるため、基本的に直接操作することはありません。

A.13. FTP 設定ディレクトリ

ログを FTP で受信する際に動作する FTPlot (FTP レシーバが受信したログを処理するプログラム)の設定情報が記載されています。FTPlot に関する設定ファイルを FTPlot プロパティファイルと呼びます。設定はコンソールサーバの GUI 上で行います。このディレクトリは直接操作しません。

A.14. FTP ユーザ設定ファイル

ログを FTP で受信する際のユーザ情報が記載されています。主な情報は FTP サーバへ接続するユーザ、接続方法、ログ転送先ディレクトリ等に関する情報です。設定はコンソールサーバの GUI 上で行います。このファイルは直接操作しません。

A.15. レポートディレクトリ

コンソールサーバがレポートを作成する際の実出力フォーマットに関する設定ファイルを保存するディレクトリです。レポート機能の実出力フォーマットで設定できる項目は、それぞれこのディレクトリ以下にある設定ファイルによって対応付けられています。このディレクトリは通常変更することはありませんが、IVEX Logger Viewer 標準の実出力フォーマット定義ファイル(xsl または sxn ファイル)が保存されており、カスタムレポートを作成する際の参考に利用することができます。

A.16. ブラウザ接続設定ファイル

ブラウザとコンソールサーバ間のセッションを維持する時間間隔の設定情報が記載されています。また、IVEX Logger Viewer API 機能を有効にするための設定情報もこのファイルに含まれています。

A.17. ログ保存領域設定ファイル

LogGate が使用する設定ファイルです。このファイルは通常、直接操作することはありません。

A.18. 改竄検出機能用キーストア

LogGate が使用する設定ファイルです。このファイルは通常、直接操作することはありません。

A.19. RMI 設定ファイル

LogGate が使用する設定ファイルです。このファイルは通常、直接操作することはありません。

付録B. ディレクトリー一覧

IVEX Logger Viewer(コンソールサーバ及び LogGate)をインストールした際に作成されるディレクトリは以下の通りです。

表 41 IVEX Logger Viewer のディレクトリー一覧

ディレクトリ名	既定値でインストールした場合のパス	インストール対象サーバ
ホームディレクトリ	C:\logstorage	コンソールサーバ LogGate
収集ログ保存先	C:\volume1	LogGate
LogGate ワーク先	C:\loggatewaywork	LogGate
シーケンシャルログ出力先	C:\loggatewaywork¥seqlog	LogGate
システムログ出力先	C:\logstorage	コンソールサーバ LogGate
収集ログアーカイブ先	既定値はなし 指定ディレクトリ以下に ARCHIVE_対象開始月_対象終了月.作成時間.LogDS 名.ZIP ができる	LogGate
レポート保存先	C:\logstorage¥report	コンソールサーバ
グラフ集計時のワーク	C:\logstorage¥stats	コンソールサーバ
収集ログスナップショット先	既定値はなし 指定ディレクトリ以下に SNAPSHOT_時間.LogDS 名のディレクトリができる	LogGate
収集ログエクスポート先	既定値はなし 指定ディレクトリ以下に指定したファイルができる	LogGate

B.1. ホームディレクトリ

コンソールサーバと LogGate が使用するディレクトリです。インストール時に設定した「インストール先」と同様のパスになります。また、このディレクトリは、環境変数 `LOGST_HOME` の値として設定します。

なお、ホームディレクトリ内の構成は、インストールしたサーバ(コンソールサーバ又は LogGate)により以下のように異なります。コンソールと LogGate が同居構成(インストール時にフルインストールを設定)した場合は、それぞれのホームディレクトリ構成が集約された構成となります。

表 42 ホームディレクトリ構成(コンソールサーバ)

ディレクトリ名	説明
bin	コンソールサーバの起動コマンドが格納されています。
conf	コンソールサーバの設定ファイルが格納されています。
lib	コンソールサーバが使用するライブラリが格納されています。 <u>通常は操作することはありません</u>
db	コンソールサーバが使用する内部データベースが格納されています。 通常は操作することはありません
logstd	コンソールサーバのプログラム本体が格納されています。 <u>通常は操作することはありません</u>
tomcat	コンソールサーバが使用する Web サーバの設定ファイル等が格納されています。 <u>通常は操作することはありません</u>

表 43 ホームディレクトリ構成(LogGate)

ディレクトリ名	説明
bin	LogGate の起動コマンドやアーカイブコマンドなどが格納されています。
bin/compatible	旧バージョンのログデータに対する管理コマンドが格納されています。
conf	LogGate の設定ファイルが格納されています。
lib	LogGate が使用するライブラリが格納されています。 <u>通常は操作することはありません</u>

B.2. 収集ログ保存先

LogGate が収集したログデータを保存するディレクトリです。収集ログ保存先以下には既定値で 1 か月毎にログデータを管理します。

収集ログ保存先ディレクトリはインストール時に設定しますが、インストール後に変更することもできます。収集ログ保存先ディレクトリの変更方法については、「4.3. 収集ログ保存先を変更する」をご覧ください。

アドバンスド版では、各 LogGate の収集ログ保存先を共有する構成をとることができます。その場合、共有先では収集ログ保存先以下に各 LogGate のホスト名を付けたディレクトリを作成します。LogGate 側では収集ログ保存先をマウントして、受信したログを自身のホスト名が付いたディレクトリ以下にログを保存します。収集ログ保存先を共有しない場合は、LogGate 毎に任意のパスを収集ログ保存先として設定します。書き込み先では収集ログ保存先以下にその LogGate のホスト名が付いたディレクトリを作成します。

B.3. LogGate ワーク先

LogGate のワーク先です。LogGate が一時的に使用するディレクトリです。既定値ではシーケンシャルログ出力先のディレクトリです。

B.4. シーケンシャルログ出力先

LogGate のレシーバが受信したログを一時的に保存するディレクトリです。そのディレクトリに保存されるファイルをシーケンシャルログファイルと呼びます。

シーケンシャルログファイルにはログが受信順に書き込まれます。シーケンシャルログファイルは、レシーバとストアをつなぐ可変長キューの役割となります。ファイルサイズがしきい値に達すると新しいファイルを作成してログを書き込みます。シーケンシャルログファイルは、既定値として 1 ファイル 256MB に達して新しいシーケンシャルログファイルを作成します。シーケンシャルログファイルは再利用されることはなく、LogGate プロセスが再起動されると新しいシーケンシャルログファイルが作成します。

シーケンシャルログファイルのファイル名は、ファイル作成時刻のエポック秒が使用され拡張子は「.seq」となります。LogGate はファイル名のエポック秒が古いファイルから順に読み出し処理を開始します。シーケンシャルログファイルは自動的に削除します。削除タイミングは書き込まれたログデータが 256MB に達して全て読み出し終わり、次のシーケンシャルログファイルを読み出すタイミングでそのファイルは削除されます。次のシーケンシャルログファイルが無い場合はそのまま残ります。シーケンシャルログファイルは通常、直接操作することはありません。なお、シーケンシャルログファイルは暗号化されていないため、他のユーザから見られないよう OS 側でアクセス制限の設定をすることを推奨します。

シーケンシャルログ出力先ディレクトリはコンソールサーバ設定ファイル(コンソールと LogGate が同居構成の場合)又は LogGate 設定ファイル(LogGate が単体構成の場合)で設定します。

シーケンシャルログ出力先ディレクトリの設定方法については「4.1. シーケンシャルログ出力ディレクトリを変更する」をご覧ください。

B.5. システムログ出力先

コンソールサーバ及び LogGate 自身のシステムログを保存するディレクトリです。

システムログ出力先は、既定値ではホームディレクトリが設定します。システムログ出力先を変更する場合は、システムログ出力設定ファイル(log4j_console.xml 又は log4j_loggate.xml)で設定します。

IVEX Logger Viewer が出力するログ及びログの出力設定方法については、「19. IVEX Logger Viewer のログをチェックする」をご覧ください。

B.6. 収集ログアーカイブ先

ログデータ(LogDB)を保存するディレクトリです。収集ログアーカイブ先はアーカイブコマンドの引数で指定します。

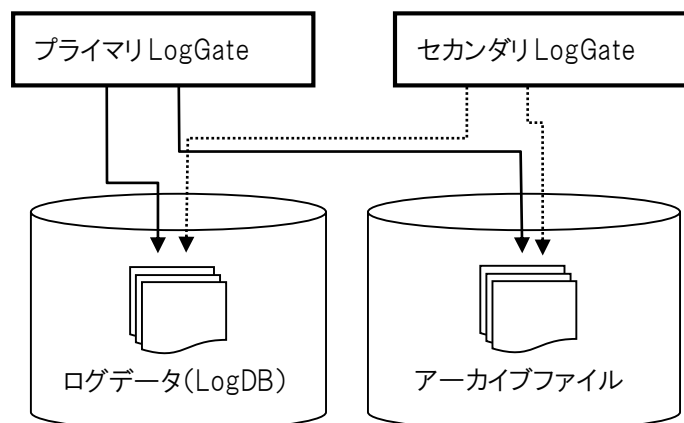


図 1 冗長構成での各 LogGate の収集ログアーカイブ先

アドバンスド版では、各 LogGate の収集ログアーカイブ先は共有する必要はありません。アーカイブコマンドは各 LogGate で実行するように設定してください。なお、アーカイブファイルをリストアする際はアーカイブした LogGate 自身の収集ログ保存先(LogDS)にしかリストアできません。他の LogGate のアーカイブファイルをリストアしないようにしてください。

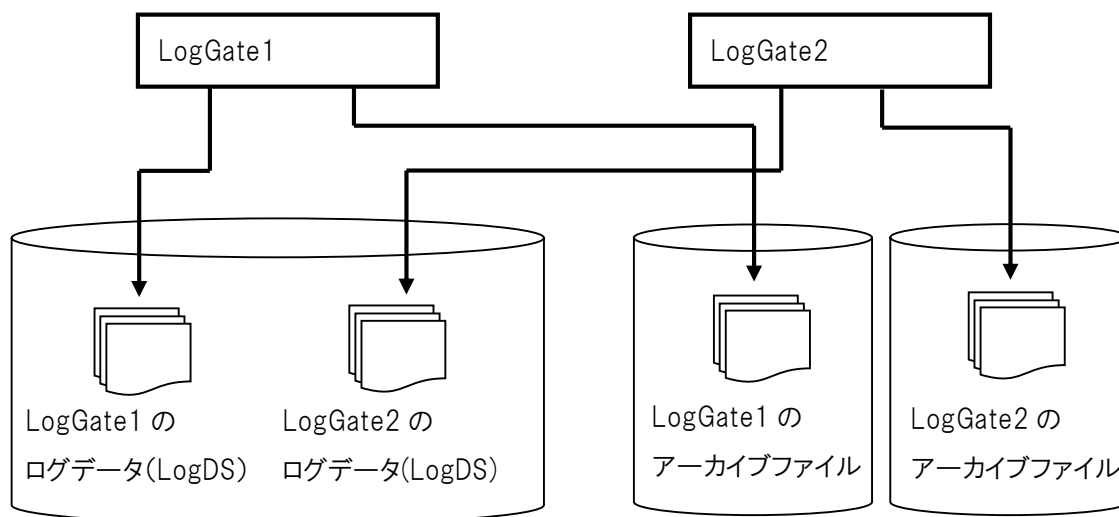


図 2 アドバンスド版での各 LogGate の収集ログアーカイブ先

B.7. レポート保存先

コンソールサーバが作成したレポートの保存先ディレクトリです。レポートが作成されるたびにこのディレクトリにレポートデータが蓄積されます。定期的にディスク容量を確認し、容量が足りなくなってきた場合は、コンソールサーバの管理画面にあるレポート作成履歴画面からレポートを消してください。

レポートは通常、直接操作することはありません。

B.8. グラフ集計時のワーク

コンソールサーバがグラフや集計表を作成する際に使用するワークディレクトリです。

グラフ集計データは通常、直接操作することはありません。

B.9. 収集ログスナップショット先

LogGate が使用するディレクトリです。スナップショット機能を使用して LogDS をバックアップする際に指定するディレクトリです。収集ログ保存先にあるログデータ(LogDB)の全てがこのディレクトリにスナップショットで退避されるため、収集ログ保存先と同等の容量を確保する必要があります。

B.10. 収集ログエクスポート先

LogGate が使用するディレクトリです。ログデータのエクスポート機能を使用して LogDB 内のログデータを IVEX Logger Viewer 形式のログデータに変換する際に出力先として指定するディレクトリです。

付録C. IVEX Logger Viewer 監査ログ一覧

下記に監査ログに出力される主なメッセージを記載します。

なお、監査ログに出力されるメッセージには以下のヘッダが付加されます。

yyyy-mm-dd HH:MM:DD,ミリ秒¥s ユーザ名¥t IP アドレス¥t セッション ID¥t メッセージ種別¥t メッセージ

¥t はタブ文字 ¥s はスペースを表します。

C.1. <システム関連 メッセージ種別:COMMON>

メッセージと監査ログ出力例	
<p>管理者がログインしました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 06:29:51,265 admin 127.0.0.1 16E726788341EF3D33F9DCCBE89853C2</pre> <p>COMMON 管理者がログインしました</p>	
<p>管理者がログアウトしました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 06:58:38,125 admin 127.0.0.1 722205860A5F1E4CAF48754DC0C902F7</pre> <p>COMMON 管理者がログアウトしました</p>	
<p>ユーザ xxx がログインしました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:57:23,750 user 127.0.0.1 657D195EC24357F2FA44C7FA75830182</pre> <p>COMMON ユーザ user がログインしました</p>	
<p>ユーザ xxx がログアウトしました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:57:25,921 user 127.0.0.1 657D195EC24357F2FA44C7FA75830182</pre> <p>COMMON ユーザ user がログアウトしました</p>	
<p>ユーザ xxx がログインに失敗しました (不正なパスワード)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 06:58:31,031 user 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</pre> <p>COMMON ユーザ user がログインに失敗しました (不正なパスワード)</p>	
<p>ユーザ xxx がログインに失敗しました (不正なユーザ名)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 06:58:41,968 usr 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</pre> <p>COMMON ユーザ usr がログインに失敗しました (不正なユーザ名)</p>	

C.2. <設定関連 メッセージ種別:SETUP>

メッセージ
<p>システム共通設定のパスワードポリシーが更新されました (パスワードの長さ xxx, パスワードの有効期間 yyy, システム管理者に適用 zzz)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定のパスワードポリシーが更新されました (パスワードの長さ 6, パスワードの有効期間 0, システム管理者に適用無効)</pre>
<p>システム共通設定のレポート機能が更新されました (レポート出力ディレクトリ xxx, カスタムレポート出力ディレクトリ xxx, 添付ファイル最大サイズ xxx)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定のレポート機能が更新されました (レポート出力ディレクトリ C:\logstorage\report, カスタムレポート出力ディレクトリ C:\logstorage\report\xsl, 添付ファイル最大サイズ 30,720)</pre>
<p>システム共通設定の検索機能が更新されました (検索結果最大表示件数 xxx)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定の検索機能が更新されました (検索結果最大表示件数 2,000)</pre>
<p>システム共通設定の検知機能が更新されました (検知履歴最大表示件数 xxx)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定の検知機能が更新されました (検知履歴最大表示件数 100)</pre>
<p>システム共通設定の集計機能が更新されました (集計グラフ出力ディレクトリ xxx)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定の集計機能が更新されました (集計グラフ出力ディレクトリ c:\logstorage\stats)</pre>

付録 C. IVEX Logger Viewer 監査ログ一覧

<p>システム共通設定が更新されました (メールサーバ xxx, 差出人 yyy, 障害発生 LogGate の切り離し zzz)</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:01:27,203 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP システム共通設定が更新されました (メールサーバ localhost, 差出人 admin@localhost, 障害発生 LogGate の切り離し無効)</pre>
<p>Agent 設定ウィーザートを使ってダウンロードされました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:13:10,734 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP Agent 設定ウィーザートを使ってダウンロードされました</pre>
<p>ログソース xxx (IP アドレス yyy) が作成されました¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:21:46,375 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP ログソースクライアント 1 (IP アドレス 192.168.10.10) が作成されました ク ラ イ ア ン ト 1 192.168.10.10</pre>
<p>xxxxyy が zzz に名前変更されました¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:22:07,875 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP ログソースクライアント 1 がログソース 1 に名前変更されました ログソース 1</pre>
<p>xxxxyy が削除されました¥tyyy</p> <p>監査ログ出力例:</p> <pre>2009-01-01 08:22:30,109 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP ログソースログソース 1 が削除されました ログソース 1</pre>
<p>ログソース xxx (IP アドレス yyy) が更新されました¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:22:22,656 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SETUP ログソースログソース 1 (IP アドレス 192.168.10.101) が更新されました ロ グ ソ ー ス 1 192.168.10.101</pre>

xxx 全ての yyy がエクスポートされました¥txxx¥t 全て

監査ログ出力例:

2009-01-01 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全てのタグがエクスポートされました タグ 全て

2009-01-01 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全てのシステム共通設定がエクスポートされました システム共通設定 全て

2009-01-01 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全てのログソースがエクスポートされました ログソース 全て

2009-01-01 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全てのグループがエクスポートされました グループ 全て

2009-01-01 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全ての検索条件がエクスポートされました 検索条件 全て

2009-07-22 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全ての LogGate グループがエクスポートされました LogGate グループ 全て

2009-07-22 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全てのレポートがエクスポートされました レポート 全て

2009-07-22 08:37:14,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート全ての集計条件がエクスポートされました 集計条件 全て

<<次ページへ続<>>

2009-07-22 08:37:14,312	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	SETUP	インポート・エクスポート全てのカスタムレポートがエクスポートされました	カスタムレポート 全て
2009-07-22 08:37:14,312	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	SETUP	インポート・エクスポート全てのユーザがエクスポートされました	ユーザ 全て
2009-07-22 08:37:14,312	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	SETUP	インポート・エクスポート全てのアプリケーションがエクスポートされました	アプリケーション 全て
2009-07-22 08:37:14,312	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	SETUP	インポート・エクスポート全ての検知ポリシーがエクスポートされました	検知ポリシー 全て
2009-07-22 08:37:14,312	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	SETUP	インポート・エクスポート全てのカラムセットがエクスポートされました	カラムセット 全て

xxxxyyzzz がエクスポートされました¥tyyy¥tzzz

監査ログ出力例:

2009-01-01 07:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートグループ group1 がエクスポートされました グループ group1

2009-01-01 07:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート検索条件検索条件 1 がエクスポートされました 検索条件 検索条件 1

2009-01-01 07:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート LogGate グループ group1 がエクスポートされました LogGate グループ group1

2009-01-01 07:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートレポート作成条件がエクスポートされました レポート レポート作成条件 1

2009-01-01 09:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート集計条件 Apache がエクスポートされました 集計条件 Apache

2009-01-01 08:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートカスタムレポート CustomReport がエクスポートされました カスタムレポート CustomReport

2009-01-01 08:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートユーザ user がエクスポートされました ユーザ user

2009-01-01 09:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートアプリケーション Apache がエクスポートされました アプリケーション Apache

2009-01-01 09:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポート検知ポリシー検知ポリシー 1 がエクスポートされました 検知ポリシー 検知ポリシー 1

2009-01-01 09:24:55,046 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

SETUP インポート・エクスポートカラムセット Apache がエクスポートされました カラムセット Apache

xxxxyyzzz (aaa) が bbb でインポートされました¥tyyy¥tzzz¥tbbb

監査ログ出力例:

付録 C. IVEX Logger Viewer 監査ログ一覧

```

2009-01-01 14:10:35,671 admin 127.0.0.1 FBFED26DE0C52542AC1284787B057BEB
      SETUP   インポート・エクスポート検索条件検索条件 1 () が-でインポートされました      検索条件 検索条件 1
-

2009-01-01 10:26:14,750 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートカスタムレポート ExternalReport () が上書きでインポートされました
      カスタムレポート      ExternalReport 上書き
※各種条件のインポートには aaa に値がありません。
Bbb の「-」は新規のインポートを表す

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートシステム共通設定 () が上書きでインポートされました      システム共通設定
      上書き

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートグループ group () がマージでインポートされました      グループ group
      マージ

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートユーザ user () が上書きでインポートされました      ユーザ user
      上書き

※システム共通設定、グループ、ユーザのインポートには aaa に値がありません。

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポート LogGate グループ group1 ([Loggate 名:loggate1,IP アドレ
ス:192.168.254.219]) が上書きでインポートされました      LogGate グループ group1 上書き

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートログソース 192.168.0.100 (IP アドレス:192.168.0.100) が上書きでイン
ポートされました      ログソース 192.168.0.100 上書き

2009-01-01 10:26:14,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A
      SETUP   インポート・エクスポートログソース 192.168.0.100 (IP アドレス:192.168.0.100) がマージでインポ
ートされました      ログソース 192.168.0.100 マージ

2009-01-01 10:26:14,734 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A

```

付録 C. IVEX Logger Viewer 監査ログ一覧

SETUP	インポート・エクスポートアプリケーション	Windows EventLog (Security) (正規表現: ^Security)	が上書きでインポートされました	アプリケーション	Windows EventLog (Security)	上書き
2009-01-01 13:42:32,390	admin	127.0.0.1	FBFED26DE0C52542AC1284787B057BEB			
SETUP	インポート・エクスポートアクション	Windows の起動 (正規表現: ^Security¥[512¥]) が-	でインポート	されました	アクション	Windows の起動 -
2009-01-01 13:42:32,390	admin	127.0.0.1	FBFED26DE0C52542AC1284787B057BEB			
SETUP	インポート・エクスポートメッセージパラメータイベント ID	(正規表現: Security¥([^¥]) *¥)) が-	で	インポート	されました	メッセージパラメータ イベント ID -
LogGate グループ xxx (ホスト名 yyy, IP アドレス zzz, 検知スレッド数 aaa) が作成されました¥txxx						
監査ログ出力例:						
2009-01-01 11:37:30,593	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A			
SETUP	LogGate グループ	group1 (ホスト名 loggate1, IP アドレス 192.168.0.100, 検知スレッド数 2)				
が作成されました group1						
LogGate グループ xxx (ホスト名 yyy, IP アドレス zzz, 検知スレッド数 aaa) が更新されました¥txxx						
監査ログ出力例:						
2009-01-01 11:37:30,593	admin	127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A			
SETUP	LogGate グループ	group1 (ホスト名 loggate, IP アドレス 192.168.0.100, 検知スレッド数 4) が				
更新されました group1						
LogGate xxx の LogDB 再作成は要求されました (対象期間: yyyy/mm/dd hh:mm:ss - yyyy/mm/dd hh:mm:ss)						
監査ログ出力例:						
SETUP LogGate loggate1 の LogDB 再作成は要求されました (対象期間: 2010/01/01 00:00:00 - 2010/04/30 23:59:59)						
LogGate xxx の LogDB yyy の再作成のキャンセルは要求されました						
監査ログ出力例:						
SETUP LogGate loggate1 の LOGDB 201004 の再作成のキャンセルは要求されました。						

C.3. <ユーザ関連 メッセージ種別:GROUP>

出力メッセージ		
グループ xxx が作成されました¥txxx		
監査ログ出力例:		
2009-01-01 11:37:52,578 admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
GROUP	グループ group が作成されました	group
グループ xxx が更新されました¥txxx		
監査ログ出力例:		
2009-01-01 11:38:50,578 admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
GROUP	グループ group が更新されました	group

C.4. <ユーザ関連 メッセージ種別:USER>

<p>システム管理者のパスワードが更新されました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 11:41:10,453 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A USER システム管理者のパスワードが更新されました</pre>
<p>ユーザ xxx (グループ yyy) が作成されました¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <pre>2009-01-01 07:57:17,875 admin 127.0.0.1 C821E46C70116D10A6AFCB8D7EFE4DDE USER ユーザ user (グループ group1) が作成されました user group1</pre>
<p>ユーザ xxx のパスワードが更新されました</p> <p>監査ログ出力例:</p> <pre>2009-01-01 11:41:10,453 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A USER ユーザ user のパスワードが更新されました</pre>
<p>ユーザ xxx (グループ yyy) が更新されました¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <pre>2009-01-01 11:41:21,984 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A USER ユーザ user (グループ group1) が更新されました user group1</pre>

C.5. <ログフォーマット定義 メッセージ種別:FORMAT>

出力メッセージ
<p>アプリケーション xxx にアクション yyy (正規表現 zzz) が作成されました¥t¥yy¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:50:53,070 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache にアクション GET (正規表現 GET) が作成されました GET GET</pre>
<p>アプリケーション xxx のアクション yyy (正規表現 zzz) が削除されました¥t¥yy¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:54:38,896 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache のアクション GET (正規表現 GET) が削除されました GET GET</pre>
<p>アプリケーション xxx にアクション yyy (正規表現 zzz) が更新されました¥t¥yy¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:54:54,661 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache にアクション GET (正規表現 GET) が更新されました GET GET</pre>
<p>アプリケーション xxx (正規表現 yyy, 区切り文字リスト zzz) が作成されました¥txxx¥t¥yy¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:50:38,896 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache (正規表現 apache, 区切り文字リスト “‘[](){}`’,) が作成されました apache apache “‘[](){}`’,</pre>
<p>アプリケーション xxx (正規表現 yyy, 区切り文字リスト zzz) が更新されました¥txxx¥t¥yy¥tzzz</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:51:40,721 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache (正規表現 apache, 区切り文字リスト “‘[](){}`’,) が更新されました apache apache “‘[](){}`’,</pre>
<p>アプリケーション xxx アクション yyy にメッセージパラメータ zzz (正規表現 aaa) が作成されました¥tzzz¥taaa</p> <p>監査ログ出力例:</p> <pre>2009-01-01 12:51:35,930 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache アクション GET にメッセージパラメータ URL (正規表現 (http://.*)¥s) が作成 されました URL (http://.*)¥s</pre>

付録 C. IVEX Logger Viewer 監査ログ一覧

アプリケーション xxx アクション yyy のメッセージパラメータ zzz (正規表現 aaa) が削除されました¥tzzz¥taaa 監査ログ出力例: 2009-01-01 12:54:48,802 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache アクション GET のメッ セージパラメータ URL (正規表現 (http://.*)¥s) が削除されました URL (http://.*)¥s		
アプリケーション xxx アクション yyy にメッセージパラメータ zzz (正規表現 aaa) が更新されました¥tzzz¥taaa 監査ログ出力例: 2009-01-01 12:54:48,802 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache アクション GET にメッ セージパラメータ URL (正規表現 URL) が更新されました URL URL		
ウィザード アプリケーション xxx (正規表現 yyy) が生成されました (zzz) アプリケーション ¥txxx¥t- 監査ログ出力例: 2010-09-30 13:44:41,781 admin 127.0.0.1 47D836DD2A66EFDD830B661FF158453 FORMAT ウィザード アプリケーショ ン Apache (正規表現: ^Apache:) が生成されました (-) アプリケーション Apache -		

C.6. <ログフォーマット定義 メッセージ種別:TAG>

出力メッセージ
<p>タグファイル名 xxx (<yyy>) が作成されました¥txxx¥t<yyy></p> <p>監査ログ出力例:</p> <pre>2009-01-01 13:41:28,421 admin 127.0.0.1 FBFED26DE0C52542AC1284787B057BEB TAG タグファイル名 (<logst_file_name>) が作成されました ファイル名 <logst_file_name></pre>
<p>タグ xxx (<yyy>) が更新されました¥txxx¥t<yyy></p> <p>監査ログ出力例:</p> <pre>2009-01-01 13:41:38,906 admin 127.0.0.1 FBFED26DE0C52542AC1284787B057BEB TAG タグファイル名 (<logst_file_name>) が更新されました ファイル名 <logst_file_name></pre>

C.7. <検索 メッセージ種別:SEARCH>

出力メッセージ
<p>カラムセット xxx が作成されました¥txxx</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:26:57,984 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH カラムセットカラムセット定義 1 が作成されました カラムセット定義 1</p>
<p>グループ規定値が設定されました (カラムセット xxx, グループ yyy) ¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:31:45,187 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH グループ規定値が設定されました (カラムセットカラムセット定義 1, グループ administrators)</p> <p>カラムセット定義 1 administrators</p>
<p>カラムセット xxx が更新されました¥txxx</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:27:03,531 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH カラムセットカラムセット定義 1 が更新されました カラムセット定義 1</p>
<p>検索条件 xxx (アーカイブ検索 yyy, 期間指定 zzz) が作成されました¥txxx¥tyyy¥tzzz</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:26:18,312 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH 検索条件検索条件 1 (アーカイブ検索無効, 期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) が作成されました 検索条件 1 無効 (2009/7/22 0:0:0 to 2009/7/22 23:59:59)</p>
<p>検索条件 xxx (アーカイブ検索 yyy, 期間指定 zzz) が実行されました¥txxx¥tyyy¥tzzz</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:24:38,281 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH 検索条件検索条件 1 (アーカイブ検索無効, 期間指定 (2004/4/22 17:45:0 to 2004/4/22 17:45:59)) が実行されました 検索条件 1 無効 (2004/4/22 17:45:0 to 2004/4/22 17:45:59)</p>
<p>検索条件 xxx (アーカイブ検索 yyy, 期間指定 zzz) が更新されました¥txxx¥tyyy¥tzzz</p> <p>監査ログ出力例:</p> <p>2009-01-01 12:24:45,921 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>SEARCH 検索条件検索条件 1 (アーカイブ検索無効, 期間指定 (2004/4/22 17:45:0 to 2004/4/22 17:45:59)) が更新されました 検索条件 1 無効 (2004/4/22 17:45:0 to 2004/4/22 17:45:59)</p>

C.8. <集計 メッセージ種別:STATS>

出力メッセージ		
集計条件 xxx (期間指定 yyy) が作成されました¥txxx¥tyyy		
監査ログ出力例:		
2009-07-22 12:39:41,937	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件集計条件 1 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) が作成されまし	
た	集計条件 1	(2009/1/1 0:0:0 to 2009/1/1 23:59:59)
集計条件 xxx (期間指定 yyy) の zzz が実行されました¥txxx¥tyyy¥tzzz		
監査ログ出力例:		
2009-07-22 12:39:29,156	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件名称未設定 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) の表出力が実	
行されました	名称未設定	(2009/1/1 0:0:0 to 2009/1/1 23:59:59) 表出力
2009-07-22 12:39:50,781	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件集計条件 1 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) の CSV 出力が	
実行されました	集計条件 1	(2009/1/1 0:0:0 to 2009/1/1 23:59:59) CSV 出力
2009-07-22 12:40:03,703	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件集計条件 1 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) のグラフ出力が	
実行されました	集計条件 1	(2009/1/1 0:0:0 to 2009/1/1 23:59:59) グラフ出力
2009-07-22 12:40:05,281	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件集計条件 1 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) の表出力が実	
行されました	集計条件 1	(2009/1/1 0:0:0 to 2009/1/1 23:59:59) 表出力
集計条件 xxx (期間指定 yyy) が更新されました¥txxx¥tyyy		
監査ログ出力例:		
2009-07-22 12:39:45,859	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB
STATS	集計条件集計条件 1 (期間指定 (2009/1/1 0:0:0 to 2009/1/1 23:59:59)) が更新されまし	
た	集計条件 1	(2009/1/1 0:0:0 to 2009/1/1 23:59:59)

C.9. <検知 メッセージ種別:SENSOR>

出力メッセージ		
検知履歴が xxx 件削除されました		
監査ログ出力例:		
2009-01-01 12:44:25,500	admin 127.0.0.1	6D3592EBE31438B6545BBAB85E4825AB

付録 C. IVEX Logger Viewer 監査ログ一覧

SENSOR 検知履歴が 10 件削除されました			
検知履歴の検索が実行されました¥txxx 監査ログ出力例: 2009-01-01 12:40:58,812 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知履歴の検索が実行されました (2008/4/1 0:0:0 to 2008/4/29 23:59:59)			
検知履歴の一括削除が実行されました¥txxx 監査ログ出力例: 2009-01-01 12:44:25,500 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知履歴の一括削除が実行されました (2008/4/1 0:0:0 to 2008/4/29 23:59:59)			
検知ポリシーxxx が yyy になりました¥txxx¥tyyy 監査ログ出力例: 2009-01-01 12:42:13,578 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知ポリシー検知ポリシー1 が無効になりました 検知ポリシー1 無効 2009-01-01 12:42:16,937 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知ポリシー検知ポリシー1 が有効になりました 検知ポリシー1 有効			
検知ポリシーxxx が作成されました¥txxx 監査ログ出力例: 2009-01-01 12:40:50,921 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知ポリシー検知ポリシー1 が作成されました 検知ポリシー1			
検知ポリシーxxx が更新されました¥txxx 監査ログ出力例: 2009-01-01 12:40:54,718 admin 127.0.0.1 6D3592EBE31438B6545BBAB85E4825AB SENSOR 検知ポリシー検知ポリシー1 が更新されました 検知ポリシー1			

C.10. <レポート メッセージ種別:REPORT>

出力メッセージ
<p>カスタムレポート xxx(XSL ファイル yyy, 拡張子 zzz, 外部レポートエンジン aaa) が作成されました ¥txxx¥tyyy¥tzzz¥taaa</p> <p>監査ログ出力例:</p> <p>2009-07-22 11:23:30,921 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT カスタムレポートカスタムレポート定義 1(XSLファイル custom.xml, 拡張子 pdf, 外部レポートエンジン c:¥logstorage¥lib¥perl¥bin¥perl c:¥script¥report.pl) が作成されました カスタムレポート定義 1 custom.xml pdf c:¥logstorage¥lib¥perl¥bin¥perl c:¥script¥report.pl</p>
<p>カスタムレポート xxx(XSL ファイル yyy, 拡張子 zzz, 外部レポートエンジン aaa) が更新されました ¥txxx¥tyyy¥tzzz¥taaa</p> <p>監査ログ出力例(登録済み XSL ファイルの削除を行った更新):</p> <p>2009-07-22 11:24:47,625 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT カスタムレポートカスタムレポート定義 1(XSL ファイル, 拡張子, 外部レポートエンジン c:¥logstorage¥lib¥perl¥bin¥perl c:¥script¥report.pl) が更新されました カスタムレポート定義 1 c:¥logstorage¥lib¥perl¥bin¥perl c:¥script¥report.pl</p>
<p>レポート作成履歴 xxx がダウンロードされました</p> <p>監査ログ出力例:</p> <p>2009-07-22 10:36:44,296 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成履歴 090101-073531-11.html がダウンロードされました</p>
<p>レポート作成条件 xxx が yyy になりました¥txxx¥tyyy</p> <p>監査ログ出力例:</p> <p>2009-07-22 10:36:24,484 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成条件レポート作成条件 1 が有効になりましたレポート作成条件 1 有効</p> <p>2009-07-22 10:36:27,875 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成条件レポート作成条件 1 が無効になりましたレポート作成条件 1 無効</p>
<p>レポート作成条件 xxx(起動タイミング yyy, 対象期間 zzz) が作成されました¥txxx¥tyyy¥tzzz</p> <p>監査ログ出力例:</p> <p>2009-07-22 10:38:48,109 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成条件 条件 1(起動タイミング指定なし, 対象期間 2009 年 7 月 1 日 0 時 0 分 0 秒から 2009 年 7 月 31 日 23 時 59 分 59 秒まで) が作成されました 条件 1 指定なし 2009 年 7 月 1 日 0 時 0 分 0 秒から 2009 年 7 月 31 日 23 時 59 分 59 秒まで</p> <p>2009-07-22 10:36:06,859 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成条件レポート作成条件 1(起動タイミング定期, 対象期間 0 時 0 分 0 秒から 24 時間) が作</p>

付録 C. IVEX Logger Viewer 監査ログ一覧

成されました	レポート作成条件 1	定期	0 時 0 分 0 秒から 24 時間
<p>レポート作成条件 xxx (起動タイミング yyy, 対象期間 zzz) が更新されました¥txxx¥tyyy¥tzzz</p> <p>監査ログ出力例:</p> <p>2009-07-22 10:38:21,953 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A</p> <p>REPORT レポート作成条件監査ログ集計レポート(起動タイミング指定なし, 対象期間 2006 年 1 月 30 日 0 時 0 分 0 秒から 2006 年 1 月 30 日 23 時 59 分 59 秒まで) が更新されました 監査ログ集計レポート 指定なし 2006 年 1 月 30 日 0 時 0 分 0 秒から 2006 年 1 月 30 日 23 時 59 分 59 秒まで</p> <p>対象期間 zzz について</p> <p>zzz の表示結果は起動タイミング yyy の「yyy」に以下が設定されている場合に異なります。</p> <p>毎日:h 時 MM 分 s 秒から h 時間</p> <p>毎時:M 分 ss 秒から M 分間</p> <p>毎月:d 日 hh 時 M 分 s 秒から m ケ月間</p> <p>毎週:h 時 M 分 s 秒から d 日間</p> <p>指定無し:yyyy 年 m 月 d 日 h 時 M 分 s 秒から yyyy 年 m 月 d 日 h 時 M 分 s 秒まで</p>			

C.11. <共通メッセージ>

出力メッセージ			
xxxxyyy がエクスポートされました¥tyyy			
監査ログ出力例:			
2009-01-01 07:32:43,968	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
TAG	タグファイル名がエクスポートされました	ファイル名	
2009-01-01 07:32:17,906	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
REPORT	レポート作成条件レポート作成条件 1 がエクスポートされました	レポート作成条件 1	
2009-01-01 07:32:07,359	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
SENSOR	検知ポリシー検知ポリシー1 がエクスポートされました	検知ポリシー1	
2009-01-01 07:31:57,812	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
STATS	集計条件集計条件 1 がエクスポートされました	集計条件 1	
2009-01-01 07:31:45,843	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
SEARCH	検索条件検索条件 1 がエクスポートされました	検索条件 1	
2009-01-01 07:32:33,500	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
FORMAT	アプリケーション Apache がエクスポートされました	Apache	
2009-01-01 07:33:29,593	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
USER	ユーザ user がエクスポートされました	user	
2009-01-01 07:33:18,593	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
GROUP	グループ一般グループがエクスポートされました	一般グループ	
2009-01-01 07:31:35,093	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
SETUP	ログソース localhost がエクスポートされました	localhost	
2009-01-01 07:32:51,859	admin 127.0.0.1	3048D70480A6BB318CDAC8C1E41E016A	
SETUP	LogGate グループ group1 がエクスポートされました	group1	

付録 C. IVEX Logger Viewer 監査ログ一覧

xxxyyy の所有者が変更されました¥tyyy 監査ログ出力例: 2009-07-22 10:30:15,000 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SEARCH 検索条件検索条件 2 の所有者が変更されました 検索条件 2			
xxxyyy が zzz にコピーされました¥tzzz 監査ログ出力例: 2009-07-22 10:29:29,640 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SEARCH 検索条件検索条件 1 が Copy 検索条件 1 にコピーされました Copy 検索条件 1			
xxxyyy が削除されました¥tyyy 監査ログ出力例: 2009-01-01 13:41:28,421 admin 127.0.0.1 FBFED26DE0C52542AC1284787B057BEB SEARCH 検索条件検索条件 1 が削除されました 検索条件 1 2009-01-01 13:41:28,421 admin 127.0.0.1 FBFED26DE0C52542AC1284787B057BEB TAG タグファイル名が削除されました ファイル名 2009-07-22 10:36:40,890 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A REPORT レポート作成履歴レポート作成条件 1 が削除されました レポート作成条件 1 2009-01-01 12:52:37,126 admin 127.0.0.1 C92809B9FA524AF18CEAA26754.5.0189A FORMAT アプリケーション apache が削除されました apache			
xxx が zzz に名前変更されました¥tzzz 監査ログ出力例: 2009-01-01 10:29:54,500 admin 127.0.0.1 3048D70480A6BB318CDAC8C1E41E016A SEARCH 検索条件 CopyApache ログ検索が検索条件 2 に名前変更されました 検索条件 2			

C.12. <設定 GUI(LogGate 設定)>

出力メッセージ
<p>[設定を LogGate に送信] ボタン押下時の監査ログ</p> <p>監査ログ出力例:</p> <pre>2010-11-26 09:51:08,140 admin 127.0.0.1 F2F1B639E0396F7A9F9BF9A9DD8BC927 SETTINGS_GUI localhost(127.0.0.1) に 設 定 を 送 信 し ま し た : Settings : SensorHistorySetting[{saveSensorHistory=true}], SensorMailSetting[{mailFrom=admin@localhost, mailServer=127.0.0.1}], Post-actions : SetSensorMailSetting, SetSaveSensorHistory</pre> <p>[この LogGate の設定を選択の LogGate へコピー] ボタン、或いは[最後の設定更新を選択の LogGate に適用] ボタン押下時の監査ログ</p> <p>監査ログ出力例:</p> <pre>2010-11-26 10:12:44,093 admin 127.0.0.1 F2F1B639E0396F7A9F9BF9A9DD8BC927 SETTINGS_GUI LogGate: localhost(127.0.0.1) に LogGate: logst15.dev(192.168.253.47) の 設 定 を 送 信 し ま し た : Settings : SensorHistorySetting[{saveSensorHistory=false}], Post-actions : SetSaveSensorHistory</pre> <p>※上記は 2 台の LogGate を選択して設定反映した場合、各 LogGate に対して 1 行ずつ (合計 2 行) 出力されます。</p>
<p>設定ファイル (拡張子 lgs) をアップロードした際の監査ログ</p> <p>監査ログ出力例:</p> <pre>2010-11-26 10:20:22,171 admin 127.0.0.1 9045E6DC47D1B23517D19B0F0989D86B SETTINGS_GUI LogGate: localhost(127.0.0.1) に LogGate 設 定 情 報 'diffSettings(2010-11-26 14-05-18).lgs'をインポートしました</pre>

付録D. IVEX Logger Viewer を再起動する操作

D.1. コンソールサーバを再起動する操作

- `LOGST_HOME/conf` ディレクトリ以下に用意されたコンソールサーバの設定ファイルの編集(`logstd.dcf` や `log4j_console.xml` など)
- `LOGST_HOME/logstd/WEB-INF/web.xml` の設定ファイルの編集
- `LOGST_HOME/bin` ディレクトリ以下のコンソールサーバの起動スクリプト(`console.sh (bat)`)の編集
- ライセンス・キーの更新(`LOGST_HOME/conf/licensekey` の置き換え)

D.2. LogGate を再起動する操作

- `LOGST_HOME/conf` ディレクトリ以下に用意された LogGate の設定ファイルの編集(`logstd.dcf` や `log4j_loggate.xml` など)
- `LOGST_HOME/bin` ディレクトリ以下の LogGate の起動スクリプト(`loggate.sh (bat)`)の編集
- コンソールサーバの LogGate グループ設定画面の変更(フォルダリスト「システム設定」→「LogGate グループ」→LogGate グループリスト画面)→「登録された LogGate グループ」→画面の全項目に対する変更)

再起動する対象の LogGate は LogGate グループに属する LogGate のみです。

付録E. コマンドリファレンス

ここでは、IVEX Logger Viewer で使用するコマンドについて説明しています。

※-s, -e オプションに対応するコマンド(archive, remove, verify, remake, export, status)については、指定期間が一部でもかかるLogDB が対象となります。特に、remove, archive では予期しないLogDB を削除する可能性がありますので、注意が必要です。

E.1. LogGate 管理コマンド

LogGate の管理コマンドです。

```
loggate.bat(sh) { start | stop [-f] | status | stop storing [-f] [-to <arg>]
| start storing | pause | unpause | receivers | ts | is | ds | es | version
| help }
```

	パラメータ	パラメータ概要
1	start	LogGate 起動コマンドです。詳細は E.8.LogGate 起動コマンドの章をご覧ください。
2	stop	LogGate 停止コマンドです。詳細は E.9.LogGate 停止コマンドの章をご覧ください。
3	status	LogGate 状態確認コマンドです。詳細は E.17.LogGate 状態表示コマンドの章をご覧ください。
4	stop storing	ログデータの取り込み停止コマンドです。詳細は E.12.取り込み停止コマンドの章をご覧ください。
5	start storing	ログデータの取り込み開始コマンドです。詳細は E.13.取り込み開始コマンドの章をご覧ください。
6	pause	ログ収集の一時停止コマンドです。詳細は E.14.収集一時停止コマンドの章をご覧ください。
7	unpause	ログ収集の一時停止解除コマンドです。詳細は E.15.収集一時停止解除コマンドの章をご覧ください。
8	receivers	レシーバ再起動コマンドです。詳細は E.10 レシーバ再起動コマンドの章をご覧ください。
9	ts	LogGate のテスト起動用コマンドです。通常は使用しません。
10	ds	Windows 環境での LogGate サービス削除コマンドです。
11	is	Windows 環境での LogGate サービス登録コマンドです。
12	es	Windows 環境での LogGate サービスプロパティ管理コマンドです。
13	version	バージョン確認コマンドです。詳細は E.19.LogGate バージョンコマンドの章をご覧ください。
14	help	LogGate の管理コマンドヘルプです。

E.2. LogDS 管理コマンド

LogDS の管理コマンドです。

```
logds.bat(sh) { export | status | remake | snapshot | restore | archive |
remove | verify | stop | help }
```

	パラメータ	パラメータ概要
1	export	元ログエクスポートコマンドです。詳細は E.16.元ログエクスポートコマンドの章をご覧ください。
2	status	LogGate 状態確認コマンドです。詳細は E.18.LogDS 状態表示コマンドの章をご覧ください。
3	remake	LogDB 再作成コマンドです。詳細は E.11.LogDB 再作成コマンドの章をご覧ください。
3	snapshot	LogDS スナップショットコマンドです。詳細は E.7.スナップショットコマンドの章をご覧ください。
5	restore	LogDB リストアコマンドです。詳細は E.5.リストアコマンドの章をご覧ください。
4	archive	LogDB アーカイブコマンドです。詳細は E.4.アーカイブコマンドの章をご覧ください。
7	remove	LogDB 削除コマンドです。詳細は E.6.LogDB 削除コマンドの章をご覧ください。
8	verify	改竄チェックコマンドです。詳細は E.20.改竄チェックコマンドの章をご覧ください。
9	stop	LogDS 管理コマンドの実行中断コマンドです。E.21.LogDS 管理中断コマンドの章をご覧ください。
10	help	LogDS の管理コマンドヘルプです。

E.3. コンソールサーバ管理コマンド

コンソールサーバの管理コマンドです。

```
console.bat(sh) { start | stop | report | impexp | admin | db | ts | is |  
ds | es | version | help }
```

	パラメータ	パラメータ概要
1	start	コンソールサーバの起動コマンドです。Windows 版ではテスト用起動に使用します。
2	stop	コンソールサーバの停止コマンドです。Windows 版ではテスト用起動の停止に使用します。
3	report	レポート実行・中断コマンドです。
4	impexp	条件・設定情報のインポート・エクスポートコマンドです。
5	admin	IVEX Logger Viewer ユーザ・グループの管理コマンドです。
6	db	コンソールサーバの内部データベース起動用コマンドです。通常は使用しません。
7	db backup	コンソールサーバの内部データベースバックアップコマンドです。
8	db restore	コンソールサーバの内部データベースリストアコマンドです。
9	db logfmtid	コンソールサーバが管理するログフォーマット定義 ID を表示するコマンドです。
9	ts	LogGate のテスト起動用コマンドです。通常は使用しません。
10	ds	Windows 環境でのコンソールサーバサービス削除コマンドです。
11	is	Windows 環境でのコンソールサーバサービス登録コマンドです。
12	es	Windows 環境でのコンソールサーバサービスプロパティ管理コマンドです。
13	version	バージョン確認コマンドです。
14	help	コンソールサーバの管理コマンドヘルプです。

E.4. アーカイブコマンド

LogDS 内の LogDB アーカイブコマンドです。このコマンドは古くなったログデータを長期間保存する目的で使
用します。アーカイブは ZIP 形式で保存します。実行後、-d の指定先以下に ARCHIVE_開始_終了.実行時
間.LogDS 名.zip を作成します。アドバンス版では ARCHIVE_開始_終了.実行時間.LogGate 名.zip です。

コマンド実行中は LogGate が起動中で[受信したログデータの取り込み開始]状態であれば[受信したログデ
ータの取り込み停止]状態になります。コマンド終了後はコマンド実行前の状態になります。また、このコマンドの
実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場
合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) archive -d <outPutDir> [-r] [-o] [-db <args>] [-e  
<yyyyMMddhhmmss>] [-h] [-s <yyyyMMddhhmmss>] [-td <day>] [-tm <month>]
```

戻り値: 正常終了時: 0

-d の出力先へ書き込みできない時: 0 以外

-d の出力先に重複したファイルがある時: 0 以外

指定した期間の LogDB がない時: 0

-d オプション指定がない時: 0 以外

-o オプションを指定せず収集ログアーカイブ先に出力するファイルがあった時: 0 以外

LogGate 停止/起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

付録 E. コマンドリファレンス

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-d	収集ログアーカイブ先です。アーカイブする先のディレクトリパスです。	必須/ファイル書き込み可能なディレクトリパス/ 既定値なし
2	-r	アーカイブ対象 LogDB をアーカイブ時に削除します。指定しない場合は削除しません。	任意/入力範囲なし/削除しない
3	-o	収集ログアーカイブ先に出力するファイルがあった場合に上書きします。指定しない場合は上書きをせずにエラーとします。	任意/入力範囲なし/上書きしない
4	-db	対象の LogDB を指定します。既定値は全ての期間を対象にします。 例:2010 年分の LogDB を表示する場合は 2010* です。Linux の場合は*をエスケープしてください。ワイルドカード以外に完全一致、カンマ区切り、レンジ指定ができます。	任意/ 000101-999912(*:ワイルドカード) YYYYMM(完全一致)、 YYYYMM,YYYYMM(カンマ区切り)、 YYYYMM-YYYYMM(レンジ指定) /000101-999912
5	-e	対象期間の終了時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 12 月 31 日の場合は、20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
6	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
7	-s	対象期間の開始時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 1 月 1 日の場合は、20100101000000 です。	任意 /00010101000000-99991231235959/ 00010101000000
8	-td	対象期間です。単位は日です。現在時刻を基準に、指定した日数より前の LogDB を対象とします。	任意/0 以上/0(前日)
9	-tm	対象期間です。単位は月です。現在時刻を基準に、指定した月数より前の LogDB を対象とします。	任意/0 以上/0(前月)

E.5. リストアコマンド

アーカイブした LogDB のリストアコマンドです。このコマンドはアーカイブした古いログデータを収集ログ保存先 (LogDS) に戻して利用する目的で使います。

コマンド実行中は LogGate が起動中で[受信したログデータの取り込み開始]状態であれば[受信したログデータの取り込み停止]状態になります。コマンド終了後はコマンド実行前の状態になります。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) restore -a <archiveFile> [-h] [-if] [-m <mode>]
```

戻り値: 正常終了時: 0

-a に指定した読み込みファイルがない時: 0 以外

指定したファイルが展開できない時: 0 以外

-a オプション指定がない時: 0 以外

収集ログ保存先へ書き込みできない時: 0 以外

-m error 指定時または -m 未指定時リストア先に重複した LogDB があった時: 0 以外

LogGate 停止/起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-a	アーカイブファイルパスです。	必須/ファイル読み込み可能なファイルパス/既定値なし
2	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
3	-if	ログフォーマット定義整合性チェックをスキップしてリストアする	任意/入力範囲無し/スキップしない
4	-m	収集ログ保存先(LogDS)へのリストア時に重複した LogDB があった場合のモードを指定します。 overwrite は重複する LogDB があった場合に上書きします。 skip は重複する LogDB があった場合にリストアせずに飛ばします。 error は重複する LogDB があった場合にエラーとし終了します。	任意/overwrite,skip,error/error

E.6. LogDB 削除コマンド

LogDS 内の LogDB 削除コマンドです。このコマンドは古くなったログデータの削除やリストアした LogDB を使わなくなった際に使用します。

コマンド実行中は LogGate が起動中で[受信したログデータの取り込み開始]状態であれば[受信したログデータの取り込み停止]状態になります。コマンド終了後はコマンド実行前の状態になります。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) remove [-db <arg>] [-e <arg>] [-h] [-s <arg>] [-td <arg>] [-tm  
<arg>]
```

戻り値: 正常終了時: 0

指定した期間の LogDB がない時: 0

-db, -s, -e, -tm, -td オプションの何れも指定がない時 : 0 以外

-db オプション指定値入力ミス: 0 以外

LogGate 停止/停止を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

付録 E. コマンドリファレンス

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-db	対象の LogDB を指定します。既定値は全ての期間を対象にします。 例: 2010 年分の LogDB を表示する場合は 2010* です。Linux の場合は * をエスケープしてください。ワイルドカード以外に完全一致、カンマ区切り、レンジ指定ができます。	任意/ 000101-999912(*:ワイルドカード) YYYYMM(完全一致)、 YYYYMM,YYYYMM(カンマ区切り)、 YYYYMM-YYYYMM(レンジ指定) /規定値なし
2	-e	対象期間の終了時間です。yyyyMMddHHmmss 形式で指定します。例: 2010 年 12 月 31 日の場合は、20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
3	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
4	-s	対象期間の開始時間です。yyyyMMddHHmmss 形式で指定します。例: 2010 年 1 月 1 日の場合は、20100101000000 です。	任意 /00010101000000-99991231235959/ 00010101000000
5	-td	対象期間です。単位は日です。現在時刻を基準に、指定した日数より前の LogDB を対象とします。	任意/0 以上/既定値なし
6	-tm	対象期間です。単位は月です。現在時刻を基準に、指定した月数より前の LogDB を対象とします。	任意/0 以上/既定値なし

※-db, -s, -e, -tm, -td の何れかは必須

E.7. スナップショットコマンド

LogDS のスナップショットコマンドです。バックアップソフトを使用しない場合にこのコマンドを使ってフルバックアップします。コマンド実行中は LogGate が[受信したログデータの取り込み開始]状態であれば[受信したログデータの取り込み停止]状態になります。コマンド終了後はコマンド実行前の状態になります。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。実行後、-d の指定先以下に SNAPSHOT_日付時間.LogDS 名のディレクトリを作成します。アドバンス版では、SNAPSHOT_日付時間.LogGate 名のディレクトリを作成します。

```
logds.bat(sh) snapshot -d <outPutDir> [-h] [-to <timeout>]
```

戻り値: 正常終了時 0:

-d の出力先へ書き込みできない時: 0 以外

指定したタイムアウトを超えた時: 0 以外

-d オプション指定がない時: 0 以外

LogGate 停止/起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-d	収集ログスナップショット先です。LogDS をフルバックアップする先のディレクトリパスです。このパラメータに c:\\$snapshot を指定した場合は、指定ディレクトリ以下に以下のディレクトリを作成します。アドバンス版以外は SNAPSHOT_日付時間.LogDS 名、アドバンス版は SNAPSHOT_日付時間.LogGate 名	必須/ファイル書き込み可能なディレクトリパス/既定値なし
2	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
3	-to	受信したログデータの取り込み停止にかかる時間のタイムアウト時間です。単位はミリ秒です。指定した時間以内に受信したログデータの取り込み停止ができなかった場合、スナップショット失敗となります。その場合はタイムアウト時間を大きく設定して再度コマンドを実行します。	任意/-1(無制限),1 以上/-1

E.8. LogGate 起動コマンド

LogGate 起動コマンドです。このコマンドを実行する際にはコンソールサーバを起動しておくことが前提です。また、コンソールサーバに LogGate を登録しておく必要があります。Windows 版ではテスト起動用のコマンドとして用意しており、起動は Windows サービスから行うようにしてください。このコマンドは LogGate を[ログデータの受信開始][受信したログデータの取り込み開始]状態にします。LogGate が起動した状態は、LogGate 状態確認コマンドで確認することができます。また、このコマンドの実行記録は、LogGate インストール先の loggate.log (既定値)に記録します。

```
loggate.bat (sh) start
```

戻り値: 正常終了時: 0

LogGate ワーク先へ書き込みができない時: 0 以外

収集ログ保存先へ書き込みできない時: 0 以外

LogGate 起動時: 0 以外

プロセス停止またはネットワーク切断等でコンソールサーバと通信ができない時: 0 以外

コンソールサーバとバージョンが異なる時: 0 以外

レシーバが使用するポート番号が取得できない時: 0 以外

LogDS 管理コマンド実行時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
	-	-	-

E.9. LogGate 停止コマンド

LogGate 停止コマンドです。このコマンドは LogGate を[ログデータの受信停止][受信したログデータの取り込み停止]状態にします。LogGate が停止した状態は、LogGate 状態確認コマンドで確認することができます。また、このコマンドの実行記録は、LogGate インストール先の loggate.log(既定値)に記録します。

なお、このコマンドを実行した際にアーカイブコマンドや LogDB 再作成コマンドなどが実行中の場合、それらの処理は中断して LogGate 停止コマンドが優先的に動作します。それぞれのコマンドは LogGate が再度起動した際に再実行してください。

```
loggate.bat(sh) stop [-f] [-h]
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

LogGate 起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 (loggate.bat(sh) 及び logds.bat(sh) の実行は中断されます。)

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-f	-f オプションを付与すると LogGate のプロセスを即時強制終了します。 [Windows サービス] > loggate.sh(bat) es を実行し shutdown タブの項目 Argument を「stop -f」として適用	無/入力範囲無し/既定値なし
2	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし

E.10. レシーバ再起動コマンド

FTP レシーバの再起動コマンドです。ログ変換スクリプトが何らかの理由で失敗した場合に、LogGate プロセスを再起動することなく、該当レシーバのみの再起動で復旧させることが可能です。

```
loggate.bat(sh) receivers [-h] restart ftp
```

戻り値: 正常終了時: 0

レシーバ未設定 / セカンダリ LogGate 実行時: 0

LogGate 停止時 / RMI 接続不可時: 1

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
2	restart	引数に指定したレシーバを再起動します。複数指定の場合は半角スペースでつなげます。	ftp 必須/なし/なし

E.11. LogDB 再作成コマンド

LogDB の再作成コマンドです。変更したログフォーマット定義にあわせて指定した LogDB 内を全て更新します。このコマンドは、ログフォーマット定義を変更したタイミングで変更前に収集したログデータを含む LogDB を新しいログフォーマット定義を使用して更新する際に使用します。LogGate が停止した状態では使用できません。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) remake [-db <arg>] [-e <arg>] [-h] [-s <arg>] [-td <arg>] [-tm <arg>]
```

戻り値: 正常終了時 0

指定した期間の LogDB がない時: 0 以外

収集ログ保存先へ書き込みできない時: 0 以外

LogGate 停止/起動を除く loggate.bat (sh) 及び logds.bat (sh) が実行中の時: 0 以外

プロセス停止またはネットワーク切断等でコンソールサーバと通信ができない時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

付録 E. コマンドリファレンス

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-db	対象の LogDB を指定します。既定値は全ての期間を対象にします。 例: 2010 年分の LogDB を表示する場合は 2010* です。Linux の場合は * をエスケープしてください。ワイルドカード以外に完全一致、カンマ区切り、レンジ指定ができます。	任意/ 000101-999912(*:ワイルドカード) YYYYMM(完全一致)、 YYYYMM,YYYYMM(カンマ区切り)、 YYYYMM-YYYYMM(レンジ指定) /000101-999912
2	-e	対象期間の終了時間です。 yyyyMMddHHmmss 形式で指定します。例: 2010 年 12 月 31 日の場合は、20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
3	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
4	-s	対象期間の開始時間です。 yyyyMMddHHmmss 形式で指定します。例: 2010 年 1 月 1 日の場合は、20100101000000 です。	任意 /00010101000000-99991231235959/ 00010101000000
5	-td	対象期間です。単位は日です。現在時刻を基準に、指定した日数より前の LogDB を対象とします。	任意/0 以上/0(前日)
6	-tm	対象期間です。単位は月です。現在時刻を基準に、指定した月数より前の LogDB を対象とします。	任意/0 以上/0(前月)

※-db, -e, -s, -td, -tm オプション指定が無い場合は、全期間が再作成対象となります。

E.12. 取り込み停止コマンド

受信したログデータの取り込み停止コマンドです。起動中の LogGate を[受信したログデータの取り込み停止]状態にします。LogGate が停止した状態では使用できません。このコマンドはバックアップソフトによる差分等のバックアップを行うタイミングで使用します。[受信したログデータの取り込み停止]状態は、受信したログデータの構造化処理が停止している状態で、[ログデータの受信停止]状態にはなりません。[受信したログデータの取り込み停止]状態時に受信したログはシーケンシャルログファイルに蓄積します。また、このコマンドの実行記録は、LogGate インストール先の loggate.log(既定値)に記録します。[受信したログデータの取り込み停止]状態は LogDS 状態表示コマンドで確認できます。

```
loggate.bat(sh) stop storing [-f] [-h] [-to <timeout>]
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

指定したタイムアウトを超えた時: 0 以外

受信したログデータの取り込み停止時: 0 以外

LogGate 停止を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

取り込み停止コマンド実行中の LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-to	受信したログデータの取り込み停止にかかる時間のタイムアウト時間です。単位はミリ秒です。指定した時間以内に受信したログデータの取り込み停止ができなかった場合、受信したログデータの取り込み停止失敗となります。その場合はタイムアウト時間を大きく設定して再度コマンドを実行します。 -to を指定しタイムアウトが発生した場合でも、状況によって取り込み停止状態となる場合があります。実行後は LogDS 状態表示コマンドで停止しているか確認をしてください。	任意/-1(無制限), 1 以上/-1
2	-f	メモリ上の取り込み待ちログデータの処理完了を待つことなく、強制的に取り込みを停止します。	任意/なし/なし

付録 E. コマンドリファレンス

3	-h	コマンドのヘルプ表示です。	任意/なし/なし
---	----	---------------	----------

E.13. 取り込み開始コマンド

受信したログデータの取り込み開始コマンドです。起動中の LogGate を[受信したログデータの取り込み開始]状態にします。LogGate が停止した状態では使用できません。このコマンドはバックアップソフトによる差分等のバックアップを行った後のタイミングで使用します。また、このコマンドの実行記録は、LogGate インストール先の loggate.log(既定値)に記録します。[受信したログデータの取り込み開始]状態は LogGate 状態表示コマンドで確認できます。

```
loggate.bat(sh) start storing
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

受信したログデータの取り込み開始時: 0 以外

LogGate 停止を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

取り込み開始コマンド実行中の LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-	-	-

E.14. 収集一時停止コマンド

LogGate が起動している状態で、ログ受信は継続したまま収集処理を一時停止するコマンドです。一時停止中、受信したログデータはワークディレクトリ下の `unpause` ディレクトリに切り替えてシーケンシャルログファイルに記録します。その他のワークディレクトリ下のファイルは LogGate による更新処理が止まりますので、安全にバックアップすることが可能です。

本コマンドを実行した後、収集一時停止解除コマンドを実行するまでの間、以下のコマンドは実行が抑制され、エラーとなります。

- ・ 取り込み開始コマンド
- ・ LogDB 再作成コマンド
- ・ 改竄チェックコマンド(情報更新オプション, `-cl`)
- ・ アーカイブコマンド(削除オプション, `-r`)
- ・ リストアコマンド
- ・ LogDB 削除コマンド
- ・ LogGate 設定 GUI による設定変更
- ・ レシーバ再起動コマンド

```
loggate.bat (sh) pause
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-	-	-

E.15. 収集一時停止解除コマンド

収集一時停止状態を解除するコマンドです。自動的に unpause ディレクトリ下のシーケンシャルログファイルをシーケンシャルログ保存先ディレクトリに移動し、収集処理を再開します。

```
loggate.bat (sh) unpause
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-	-	-

E.16. 元ログエクスポートコマンド

収集ログ保存先の LogDB から IVEX Logger Viewer 形式のログデータにエクスポートするコマンドです。このコマンドはログデータを外部に提出する場合や、別のシステムで加工する際に使用します。このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) export [-ds <LogDSPath>] -o <OutputPath> [-s  
<yyyyMMddHHmmss>] [-e <yyyyMMddHHmmss>] [-h] [-key <encryptionKey>] [-max  
<exportFileSize>] [-alg <encryptionAlgorithm>]
```

戻り値: 正常終了時: 0

暗号化ログデータに対する復号化失敗時 (暗号化キー値/アルゴリズム値入力ミス含): 0 以外

-ds の指定先がない時: 0 以外

LogDS 内に指定した期間の LogDB がない時: 0 以外

-ds 内に指定した期間の LogDB がない時: 0

-o の出力先へ書き込みできない時: 0 以外

-o オプションの指定がない時: 0 以外

LogGate 停止/起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-ds	エクスポート対象の LogDS を指定します。収集ログ保存先、収集ログスナップショット先ディレクトリを指定します。	任意/ 収集ログ保存先または収集ログスナップショット先 以下の SNAPSHOTxxxxx/volume1/logds /収集ログ保存先
2	-o	収集ログエクスポート先です。IVEX Logger Viewer 形式のログデータファイルを出力するファイルパスです。	必須/ファイル書き込み可能なファイルパス/既定値なし
3	-s	エクスポートする対象期間の開始時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 1 月 1 日の場合は、20100101000000 です。	任意 /00010101000000-99991231235959/ 00010101000000
4	-e	エクスポートする対象期間の終了時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 12 月 31 日の場合は、20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
5	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
6	-max	エクスポートファイルの最大サイズです。指定したサイズに達した場合、新しいファイルにログデータをエクスポートします。単位にキロバイト(K)とメガバイト(M)を指定します。新しいファイルの名前は -o で指定した「ファイル名.0~n(nは整数値)」です。	任意/ 1K 以上または 1M 以上/ 1 ファイルへ上限無くエクスポート
7	-key	暗号化した LogDB の復号化鍵です。LogDS に保存した LogDB に暗号化設定がされている場合に指定します。	暗号化設定時必須/ 有効な復号化鍵/ 既定値なし
8	-alg	暗号化した LogDB の復号化鍵の暗号アルゴリズムです。LogDS に保存した LogDB に暗号化設定がされている場合に指定します。	暗号化設定時必須/ AES,Blowfish,RC4,RC2,DESede,DES/ 既定値なし

E.17. LogGate 状態表示コマンド

LogGate 状態確認コマンドです。LogGate の状態を標準出力します。LogGate が停止した状態では使用できません。

```
loggate.bat (sh) status
```

戻り値: 正常終了時: 0

LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
-	-	-	-

表 44 LogGate 状態確認コマンドのステータス項目

ステータス項目	ステータス例	ステータス概要
Version	4.5.0	LogGate のバージョン番号
Runtime version	1.7.0 21-b11	LogGate が使用している JavaVM ランタイムバージョン番号
VM version	2013-b01	LogGate が使用している JavaVM のバージョン番号
OS	Windows 2008 Server	OS 名
OS version	5.1	OS バージョン番号
architecture	x86	OS(CPU)アーキテクチャ
Processors	2	LogGate が利用可能な論理プロセッサ数
SystemTime	Fri Jan 01 01:01:00 JST 2010	システム時間
LOGST_HOME	C:\logstorage	インストールディレクトリ
seqlog dir	c:\loggateway\seqlog	シーケンシャルログ出力ディレクトリ
Charset	MS932	ログキャラクタセット
advanced	True	true:アドバンスド版 false:アドバンスド版以外
loggateId	7	非公開
loggateGroupId	1	非公開
ipAddress	192.168.0.1	登録 IP アドレス
hostname	Loggate	登録ホスト名
primaryFlg	True	true:プライマリ LogGate false:セカンダリ LogGate
sensorThread	2	検知スレッド数 検知しない場合 0
searchServer	True	true:検索サーバ false:検索サーバでない
weight	1	検索時の重み
parallelNum	1	非公開
switchCmd	null	WG/EP 版冗長構成時の LogGate 切り替えコマンド
free memory	2,800,840	LogGate の使用可能メモリ量 (byte)
total memory	7,471,104	LogGate が確保済みメモリ量 (byte)
max memory	517,013,504	LogGate が要求する最大メモリ量 (byte)
status	online	online:ログ収集中 paused:収集一時停止中
storeDirector	alive	alive:受信したログデータの取り込み開始 dead:受信したログデータの取り込み停止
SyslogUDPReceiver	alive	alive:UDP レシーバ開始 dead:UDP レシーバ停止
SyslogTCP	alive	alive:TCP レシーバ開始

付録 E. コマンドリファレンス

SelectReceiver		dead:UDP レシーバ停止
SyslogLltpReceiver	alive	alive:LLTP レシーバ開始 dead:LLTP レシーバ停止
SnmpTrapReceiver	alive	alive:SNMPトラップレシーバ開始 dead:SNMPトラップレシーバ停止
SyslogSslReceiver	alive	alive:TLS レシーバ開始 dead:TLS レシーバ停止
FTPReceiver	alive	alive:FTP レシーバ開始 dead:FTP レシーバ停止
FileReceiver	alive	alive:ファイルレシーバ開始 dead:ファイルレシーバ停止
AdhocFileReceiver	alive	alive:アドホックファイルレシーバ開始 dead:アドホックファイルレシーバ停止
RelayDirector	connected=true,relayType=file,logType=IVEX Logger Viewer,protocol=file,connectTo=/var/log/loggateway/relayed/relay.log.2013030313,totalSent=3,started [Wed Apr 10 11:41:15 JST 2013]	ログ転送設定値

E.18. LogDS 状態表示コマンド

収集ログ保存先の状態確認コマンドです。LogDS と LogDB の状態を標準出力します。

```
logds.bat(sh) status [-d <arg>] [-db <arg>] [-ds <arg>] [-e <arg>] [-fmt  
<arg>] [-h] [-m] [-o <arg>] [-s <arg>] [-td <arg>] [-tm <arg>]
```

戻り値: 正常終了時 0

-db, -e, -s, -td, -tm オプションで指定された条件に該当する LogDB がない時: 0

LogGate 停止/起動を除く loggate.bat(sh) 及び logds.bat(sh) が実行中の時: 0 以外
コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-d	表示項目を指定します。既定値は all です。LogDS のみの場合は ds、LogDB のみの場合は db を指定します。	任意/all,db,ds/all
2	-db	対象の LogDB を指定します。既定値は全ての期間を対象にします。 例:2010 年分の LogDB を表示する場合は 2010*です。Linux の場合は*をエスケープしてください。ワイルドカード以外に完全一致、カンマ区切り、レンジ指定ができます。	任意/ 000101-999912(*:ワイルドカード) YYYYMM(完全一致)、 YYYYMM,YYYYMM(カンマ区切り)、 YYYYMM-YYYYMM(レンジ指定) /000101-999912
3	-ds	LogDS 状態表示対象の LogDS を指定します。	任意/ 収集ログ保存先または収集ログスナップ ショット先以下の SNAPSHOTxxxxx/volume1/logds /収集ログ保存先
4	-e	対象期間の終了時間です。 yyyyMMddHHmmss 形式で指定します。 例:2010 年 12 月 31 日の場合は、 20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
5	-fmt	表示する LogDB の種類を指定します。 -dso を指定すると-fmt は無効です。 fmtStatus には、latest,old,all を指定します。Latest は最新のログフォーマットが適用された LogDB の一覧を表示します。 Old は最新ではないログフォーマットが適用された LogDB の一覧を表示します。All は最新に関わらず全ての LogDB の一覧を表示します。「No LogDBs matched the specified filter.」というメッセージが表示された場合は、該当する LogDB がありません。	任意/latest,old,all/all
6	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
7	-m	月単位でサマリ表示を指定します。	任意/特になし/既定値なし
8	-o	表十結果のソートを指定します。既定値は asc です。Asc は昇順です。Desc は降	任意/asc,desc/asc

付録 E. コマンドリファレンス

		順です。	
9	-s	対 象 期 間 の 開 始 時 間 で す 。 yyyyMMddHHmmss 形式で指定します。 例：2010 年 1 月 1 日の場合は、 20100101000000 です。	任意 /00010101000000-99991231235959/ 00010101000000
10	-td	表示する対象期間です。単位は日です。 現在時刻を基準に、指定した日数より前 の LogDB を対象とします。	任意/0 以上/0(前日)
11	-tm	表示する対象期間です。単位は月です。 現在時刻を基準に、指定した月数より前 の LogDB を対象とします。	任意/0 以上/0(前月)

表 45 LogDS 状態確認コマンドのステータス項目

ステータス項目	ステータス例	ステータス概要
LogDS	localhost	LogDS 名です。
バージョン	1	LogDS の ID です。
ログフォーマット ID	2 [2010/01/01 00:00:00].(out-of-date)	LogDS に適用された最新ログフォーマットの ID です。 Out-of-date は LogDS 内に旧ログフォーマットが適用された LogDB があることを示します。 Up-to-date は LogDS 内の全ての LogDB に最新ログフォーマットが適用されていることを示します。
状態	All blocks are up-to-date	LogDS の状態を表します。
電子署名設定 ID	not-signed または 123456789123 [2010/01/01 12:00:04]	LogDS の改竄検出設定を表す内部的な識別子です。Not-signed の場合は、改竄検出機能が有効になっていないことを示します。 []の時間は改竄検出機能が有効にされた時間です。
暗号化設定 ID	not-crypted または 123456789123 [2010/01/01 12:00:04]	LogDS の暗号化設定を表す内部的な識別子です。Not-crypted の場合は、暗号化設定が有効になっていないことを示します。 []の時間は暗号化設定が有効にされた時間です。
最新スナップショット ID	10000	LogDS に対して付与する ID の最後です。
データブロック数	3	LogDS 内の全 LogDB 数です。
ログ総数	9876134133	LogDS 内の全 LogDB に含まれるログ件数です。
シスログタイムスタンプ範囲	20090101000000～ 20091224000000	syslog タイムスタンプ範囲です。ログデータに含まれる時刻の中で一番古い時刻から一番新しい時刻を示します。
受信タイムスタンプ範囲	20090101000000～ 20091224000000	受信タイムスタンプ範囲です。LogGate が受信したログデータの中で最初に受信した時刻から最後に受信した時刻を示します。
実行中管理操作	none	実行中の LogDS 管理コマンド名です。コマンド名には、status、export、remake、snapshot、restore、archive、remove、verify、stop があります。None はサービスが実行されていない状態です。

表 46 LogDB 状態確認コマンドのステータス項目

ステータス項目	ステータス例	ステータス概要
対象	201304	LogDB ディレクトリ名です。
ログフォーマット ID	1 [2010/01/01 12:00:04](latest)	LogDB に適用されている最も古いログフォーマットの ID です。 Old は LogDB 内に旧ログフォーマットが適用されたログデータがあることを示します。 Latest は LogDB 内の全てのログデータに最新ログフォーマットが適用されていることを示します。
ログ数	982734	LogDB に含まれるログ件数です。
シスログタイムスタンプ範囲	20090101000000～ 20091224000000	syslog タイムスタンプ範囲です。ログデータに含まれる時刻の中で最も古い時刻から最も新しい時刻を示します。
受信タイムスタンプ範囲	20090101000000～ 20091224000000	受信タイムスタンプ範囲です。LogGate が受信したログデータの中で最初に受信した時刻から最後に受信した時刻を示します。

logds.bat(sh) status -fmt all 指定時の実行例

```
# LOGST_HOME/bin/logds.bat(sh) -fmt all↵
201001 2 [2010/04/28 12:29:04] (old)
201002 3 [2010/04/28 13:29:04] (latest)
201003 3 [2010/04/28 13:29:04] (latest)
```

「No LogDBs matched the specified filter.」というメッセージが表示された場合は、該当する LogDB がありません。

E.19. LogGate バージョンコマンド

LogGate のバージョン確認コマンドです。

```
loggate.bat (sh) version
```

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-	-	-

E.20. 改竄チェックコマンド

LogDS が改竄されていないかチェックするコマンドです。このコマンドは LogDB 単位で改竄チェックを行い、改竄されているかどうかを確認する際に使用します。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat(sh) verify [-cc <arg>] [-cl] -cp <arg> [-db <arg>] [-ds <arg>]  
[-e <arg>] [-h] [-s <arg>] [-td <arg>] [-tm <arg>] [-v]
```

戻り値: 正常終了時: 0

-ds の指定先がない時: 0 以外

-cp で指定したパスワードが間違っている時: 0 以外

-db, -s, -e, -tm, -td オプションの何れも指定がない時 : 0 以外

-cp オプションの指定がない時: 0 以外

LogGate 停止/起動を除く loggate.bat (sh) 及び logds.bat (sh) が実行中の時: 0 以外

LogGate グループ設定画面で改竄検出機能が無効の時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

コマンド実行中の LogDS 管理中断コマンド実行時: 0 以外

付録 E. コマンドリファレンス

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-cp	改竄チェックを実行するためのパスワードです。	必須/改竄チェック用パスワードに使用できる文字列/既定値なし
2	-ds	改竄チェック対象の LogDS のパスを指定します。収集ログ保存先、収集ログスナップショット先ディレクトリを指定します。	任意/ 収集ログ保存先または収集ログスナップショット先以下の SNAPSHOTxxxxx/volume1/logds /収集ログ保存先
3	-v	詳細表示です。改竄チェックで改竄されている数とファイル情報を表示します。	任意/特になし/既定値なし
4	-cc	LogDB 内の改竄チェックで改竄されている状態の LogDB を表示する数を指定します。この数を超えた場合は途中で改竄チェックをストップします。	任意/0(すべて対象),1 以上/全て対象
5	-cl	改竄チェック結果をクリアして最新のチェック情報を作成します。 このオプションは改竄チェックに引っかかったログを正しいものとして扱うために改竄チェック情報を更新する際に使用します。通常運用中に使用することはありません。また、このオプションを指定する場合は LogGate が起動中であり、対象は収集ログ保存先(LogDS)のみとなります。	任意/特になし/既定値なし
6	-db	対象の LogDB を指定します。既定値は全ての期間を対象にします。 例:2010 年分の LogDB を表示する場合は 2010*です。Linux の場合は*をエスケープしてください。ワイルドカード以外に完全一致、カンマ区切り、レンジ指定ができます。	任意/ 000101-999912(*:ワイルドカード) YYYYMM(完全一致)、 YYYYMM,YYYYMM(カンマ区切り)、 YYYYMM-YYYYMM(レンジ指定) /00010101-99991231
7	-e	対象期間の終了時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 12 月 31 日の場合は、20101231235959 です。	任意 /00010101000000-99991231235959/ 99991231235959
8	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし
9	-s	対象期間の開始時間です。yyyyMMddHHmmss 形式で指定します。例:2010 年 1 月 1 日の場	任意 /00010101000000-99991231235959/

付録 E. コマンドリファレンス

		合は、20100101000000 です。	00010101000000
10	-td	対象期間です。単位は日です。現在時刻を基準に、指定した日数より前の LogDB を対象とします。	任意/0 以上/0(前日)
11	-tm	対象期間です。単位は月です。現在時刻を基準に、指定した月数より前の LogDB を対象とします。	任意/0 以上/0(前月)

E.21. LogDS 管理中断コマンド

LogDS 管理コマンド実行中の処理を中断するコマンドです。このコマンドは LogDS 管理コマンド(例えば LogDB 再作成コマンド)実行中に優先的に他の LogDS 管理コマンド(例えばアーカイブコマンド)を実行する際に LogDS 管理コマンド(LogDB 再作成コマンド)を安全に停止するために使用します。また、このコマンドの実行記録は、LogGate が起動中の場合インストール先の loggate.log に記録します。LogGate が停止中の場合インストール先の admin-logds.log に記録します。

```
logds.bat (sh) stop
```

戻り値: 正常終了時: 0

LogDS 管理コマンドが実行されていない時: 0 以外

コマンド実行中の LogGate 停止時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-	-	-

LogDS 管理中断コマンドの実行例は以下の通りです。以下は元ログエクスポートコマンドが中断されたこと(「was interrupted」行)及び、LogDS 管理中断コマンドが正常終了したこと(「completed successfully」行)を示しています。[]内は「<コマンド名>@<スクリプト名>」の形式で@以前には status、export、remake、snapshot、restore、archive、remove、verify、stop、stop storing、start storing、pause、unpause の何れか、@以降は logds、loggate の何れかが表示されます。

```
# logds.bat (.sh) stop
Service [export@logds] was interrupted.
Service [stop@logds] completed successfully.
```

中断された側には以下のメッセージが出力されます。

```
Service [export@logds] was canceled.
```

尚、LogDS 管理中断コマンドによって実行中のコマンドが中断された場合、対象のコマンドはキャンセルされて制御が戻りますが、LogGate 及び LogDS の内部では予定処理が完了するまで処理を継続します。LogGate 状態表示コマンドで確認の上、適切な処理を行ってください。

例えば、取り込み停止コマンド(stop storing)を中断した場合、コマンドを実行したプロンプトは LogDS 管理中断コマンドの実行によって制御が戻されますが、取り込み停止処理は完了するまで処理がバックグラウンドで継続しています。処理が完了すると LogGate 状態表示コマンド(loggate status)を実行結果に「storeDirector」

の値が「dead(収集停止状態)」と表示されますので、適切な処理を実施した上、取り込み開始コマンド(start storing)を実行して処理を再開してください。

E.22. 過去ログデータのインデックス作成コマンド

過去ログデータ(Ver.2/Ver.3 で収集したログデータ)のインデックス作成コマンドです。過去のログデータ互換検索有効時に使用する過去ログデータに対するインデックス作成コマンドです。変更したログフォーマット定義にあわせて指定した時間.log ファイルに対するインデックスデータを更新します。このコマンドは、ログフォーマット定義を変更したタイミングで使用します。また、このコマンドの実行記録は、loggate.log に記録します。

```
index.bat(sh) remake -m <mode> -t <target> [-d destination] [-I indexes]
```

戻り値: 正常終了時 0

-t で指定した先にログデータ(yyyyymmddhh.log)がない時: 0

-i で指定した先へ書き込みできない時: 0 以外

-t で指定した先がない時: 0 以外

プロセス停止またはネットワーク切断等でコンソールサーバと通信ができない時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-m	<p>再作成するモードを指定します。</p> <p>Make を指定するとインデックスファイルの無い対象のログファイルに対して新規作成を行います。</p> <p>Remake を指定すると全てのログファイルに対してインデックスファイルを作成します。既にインデックスファイルがあるものはそのファイルを削除します。</p> <p>Diff を指定すると新しく追加されたログデータに対して差分作成を行います。</p> <p>Rollforward を指定するとインデックスの一時ファイル进行处理して削除します。インデックス保存先にインデックス作成時の一時ファイルが残ることでディスク容量が取られることがあります。このコマンドで一時ファイル进行处理して削除します。</p>	<p>必須/ make,remake,diff,rollforward/ 既定値なし</p>
2	-t	<p>インデックス作成をする対象のファイルまたはディレクトリパスです。通常は収集ログ保存先を指定するか yyyyymmddhh.log ファイルパスを指定します。ディレクトリパス指定ではそのパス以下のファイルが対象となります。</p>	<p>必須/ 収集ログ保存先または yyyyymmddhh.log ファイルパス/ 既定値なし</p>

3	-d	<p>インデックス保存先を指定します。</p> <p>省略された場合は、logstd.dcf(または loggate.dcf)の com.IVEX Logger Viewer.engine.common.IndexFileManager.indexDir で指定し たディレクトリに出力します。</p> <p>アドバンスド版では、このディレクトリパス以下に LogGate 名が 自動的に付加されます。</p>	任意/インデックス保存先 /logstd.dcf の設定値
4	-i	<p>Ver.3 または Ver.2 のインデックス作成項目を指定します。省 略時は全インデックス作成項目を対象にします。</p> <p>HOST:ログソース FACILITY:ファシリティ PRIORITY:プライオリティ APPLICATION:アプリケーション ACTION:アクション MSGPARAM:メッセージパラメータ TAG:タグ VALUE:タグの値</p> <p>設定例;HOST,ACTION,TAG,VALUE</p>	任意/ HOST,FACILITY,PRIORITY,APPLIC ATION,ACTION,MSGPARAM,TAG,V ALUE/ 全てのインデックス作成項目が対 象となる

E.23. 過去ログデータの改竄チェックコマンド

過去ログデータ(Ver.2/Ver.3 で収集したログデータ)の改竄チェックコマンドです。このコマンドは過去のログデータ互換検索有効時に使用する過去ログデータに対する改竄チェックコマンドです。時間.log 単位で改竄チェックを行い、改竄されているかどうかを確認する際に使用します。また、このコマンドの実行記録は、LogGate インストール先の loggate.log に記録します。

```
sign.bat(sh) [-v <version>] -ks <keystoreFile> -sp <storePassword> -as  
             <alias> -kp <keyPassword> -ag <algorithm> <logfile or logdir>
```

戻り値: 正常終了時 0

-ks で指定した先にファイルがない時: 0

-sp で指定したパスワードが違う時: 0 以外

-kp で指定したパスワードが違う時: 0 以外

-as で指定したエイリアスがない時: 0 以外

logfile or logdir で指定したファイルがない時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-v	バージョンが表示されます。	任意/なし/既定値なし
2	-ks	KeyStore ファイルパスを指定します。	必須/ディレクトリパス/既定値はなし
3	-sp	KeyStore パスワードを指定します。	必須/パスワードで指定した文字/既定値はなし
4	-as	鍵のエイリアス名を指定します。	必須/エイリアスで指定した文字/既定値はなし
5	-kp	鍵パスワードを指定します。	必須/パスワードで指定した文字/既定値はなし
6	-ag	鍵のアルゴリズムを指定します。	必須/DSA,RSA/既定値はなし
7	logfile or logdir	改竄チェック対象ログファイル又はディレクトリパスを指定します。ディレクトリパスを指定するとそのディレクトリ以下にある全てのファイルをチェック対象とします。	必須/ファイルまたはディレクトリパス/既定値はなし

E.24. 過去ログデータの暗号化コマンド

過去ログデータ(Ver.2/Ver.3 で収集したログデータ)の暗号化/復号化コマンドです。過去のログデータ互換検索有効時に使用する過去ログデータに対する暗号化/復号化コマンドです。このコマンドの実行記録は、loggate.log に記録します。

```
crypto.bat(sh) -m <mode> -s <source> -d <dest> -k <key> -a <algo>
```

戻り値: 正常終了時 0

-d で指定した先へ書き込みできない時: 0 以外

-k で指定した暗号化キーが違う時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-m	暗号化するモードを指定します。 Encode は対象のログファイルに対して暗号化します。 Decode は対象のログファイルに対して復号化します。	必須/encode,decode/既定値なし
2	-s	暗号化または復号化する対象のログファイルまたはディレクトリを指定します。	必須/ yyyyymmddhh.log ファイルパス/ 既定値なし
3	-d	暗号化または復号化したファイルの保存先を指定します。	必須/ディレクトリパス/既定値なし
4	-k	暗号化キーを指定します。ここで指定する値は Ver.3 の暗号化設定で表示された暗号化キーです。	必須/暗号化キーの文字列/ 既定値なし
5	-a	暗号化キーに対する暗号アルゴリズムを指定します。ここで指定する値は Ver.3 の暗号化設定で指定した値です。	必須/ Blowfish,DES,DESede,AES,RC2,RC4/ 既定値なし

E.25. IVEX Logger Viewer ユーザ/グループ管理コマンド

IVEX Logger Viewer ユーザ及びグループを管理するコマンドです。

```
console.bat(sh) admin { -p | -u | -h } { users | adduser | deleteuser |  
enableuser | groups | addgroup | deletigroup | help }
```

	パラメータ	パラメータ概要
1	-p --adminpass	IVEX Logger Viewer ユーザ/グループを操作する IVEX Logger Viewer 管理者ユーザパスワードを指定します。 -p を指定しない場合はコマンドプロンプトの対話形式で入力します。
2	-u --adminuser	IVEX Logger Viewer ユーザ/グループを操作する IVEX Logger Viewer 管理者ユーザを指定します。 -u を指定しない場合は既定値として admin となります。
3	-h --help	IVEX Logger Viewer ユーザ/グループ管理コマンドのヘルプです。
4	users	IVEX Logger Viewer ユーザー一覧表示コマンドです。詳細は E.26. IVEX Logger Viewer ユーザー一覧表示コマンドを参照してください。
5	adduser	IVEX Logger Viewer ユーザ登録コマンドです。詳細は E.27. IVEX Logger Viewer ユーザ登録コマンドを参照してください。
6	deleteuser	IVEX Logger Viewer ユーザ削除コマンドです。詳細は E.28. IVEX Logger Viewer ユーザ削除コマンドを参照してください。
7	enableuser	IVEX Logger Viewer ユーザロック解除コマンドです。詳細は E.29. IVEX Logger Viewer ユーザロック解除コマンドを参照してください。
8	groups	IVEX Logger Viewer グループ一覧表示コマンドです。詳細は E.30. IVEX Logger Viewer グループ一覧表示コマンドを参照してください。
9	addgroup	IVEX Logger Viewer グループ登録コマンドです。詳細は E.31. IVEX Logger Viewer グループ登録コマンドを参照してください。
10	deletigroup	IVEX Logger Viewer グループ削除コマンドです。詳細は E.32. IVEX Logger Viewer グループ削除コマンドを参照してください。
11	help	IVEX Logger Viewer ユーザ/グループ管理コマンドのヘルプです。

E.26. IVEX Logger Viewer ユーザー一覧表示コマンド

コンソールサーバに登録された IVEX Logger Viewer ユーザーの一覧を表示するコマンドです。コマンドでユーザーの登録や削除をする際に現在の状態を確認するためのコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。

```
console.bat(sh) admin users [-v] [-c]
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-v --verbose	一覧表示を CSV 形式で出力します。 指定無しの場合はユーザー名のみ表示されます。 指定した場合、ユーザー名、所属グループ、認証方式、カスタム DN 部分、概要が CSV 形式で出力されます。	任意/なし/既定値なし
2	-c --columns	一覧表示をカラム形式で出力します。--verbose と合わせて指定することで有効になります。 指定無しの場合はユーザー名のみ表示されます。 指定した場合、ユーザー名、所属グループ、認証方式、カスタム DN 部分、概要がカラム形式で出力されます。	任意/なし/既定値なし

E.27. IVEX Logger Viewer ユーザ登録コマンド

コンソールサーバに IVEX Logger Viewer ユーザを登録するコマンドです。コマンドでユーザの登録を行う際に使用するコマンドです。このコマンドの実行記録は、admin-console.log に記録します。

```
console.bat(sh) admin adduser -name -password -group [--remark] [--auth]
[--customDNpart]
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--name	登録するユーザ名を指定します。	必須/文字列/既定値なし
2	--password	登録するユーザのパスワードを指定します。	必須/文字列/既定値なし ※LDAP の場合は任意
3	--group	登録するユーザの所属グループを指定します。	必須 / 存在する IVEX Logger Viewer グループ名/既定値なし
4	--remark	登録するユーザの概要を指定します。	任意/文字列/既定値なし
5	--auth	登録するユーザの認証方式を指定します。	任意/LOCAL,LDAP/LOCAL
6	--customDNpart	登録するユーザの customDNpart を指定します。	任意/文字列/既定値なし

E.28. IVEX Logger Viewer ユーザ削除コマンド

コンソールサーバの IVEX Logger Viewer ユーザを削除するコマンドです。コマンドでユーザの削除を行う際に使用するコマンドです。このコマンドの実行記録は、admin-console.log に記録します。

```
console.bat(sh) admin deleteuser -name
```

戻り値: 正常終了時 0

ユーザが存在しない時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--name	削除するユーザ名を指定します。	必須/文字列/既定値なし

E.29. IVEX Logger Viewer ユーザロック解除コマンド

コンソールサーバの IVEX Logger Viewer ユーザのロック解除をするコマンドです。コマンドでユーザのロック解除を行う際に使用するコマンドです。

```
console.bat(sh) admin enableuser --name
```

戻り値: 正常終了時 0

ユーザが存在しない時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--name	ロック解除するユーザ名を指定します。	必須/文字列/既定値なし

E.30. IVEX Logger Viewer グループ一覧表示コマンド

コンソールサーバに登録された IVEX Logger Viewer グループの一覧を表示するコマンドです。コマンドでグループの登録や削除をする際に現在の状態を確認するためのコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。

```
console.bat(sh) admin groups [-v] [-c]
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-v --verbose	一覧表示を CSV 形式で出力します。 指定無しの場合はグループ名のみ表示されます。 指定した場合、グループ名、カスタム DN 部分、概要が CSV 形式で出力されます。	任意/なし/既定値なし
2	-c --columns	一覧表示をカラム形式で出力します。--verbose と合わせて指定することで有効になります。 指定無しの場合はグループ名のみ表示されます。 指定した場合、グループ名、カスタム DN 部分、概要がカラム形式で出力されます。	任意/なし/既定値なし

E.31. IVEX Logger Viewer グループ登録コマンド

コンソールサーバに IVEX Logger Viewer グループを登録するコマンドです。コマンドでグループの登録を行う際に使用するコマンドです。このコマンドの実行記録は、admin-console.log に記録します。

```
console.bat(sh) admin addgroup --name [--remark] [--customDNpart]
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--name	登録するグループ名を指定します。	必須/文字列/既定値なし
4	--remark	登録するグループの概要を指定します。	任意/文字列/既定値なし
6	--customDNpart	登録するグループの customDNpart を指定します。	任意/文字列/既定値なし

E.32. IVEX Logger Viewer グループ削除コマンド

コンソールサーバの IVEX Logger Viewer グループを削除するコマンドです。コマンドでグループの削除を行う際に使用するコマンドです。このコマンドの実行記録は、admin-console.log に記録します。

```
console.bat(sh) admin deletegroup -name
```

戻り値: 正常終了時 0

ユーザが存在しない時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--name	削除するグループ名を指定します。	必須/文字列/既定値なし

E.33. 条件・設定インポート・エクスポートコマンド

条件・設定情報をインポート・エクスポートするコマンドです。

```
console.bat(sh) impexp 「 -p | -u | -h 」 「import | export 」 「Options」
```

	パラメータ	パラメータ概要
1	-p --adminpass	インポート・エクスポートする IVEX Logger Viewer 管理者ユーザパスワードを指定します。 -p を指定しない場合はコマンドプロンプトの対話形式で入力します。
2	-u --adminuser	インポート・エクスポートする IVEX Logger Viewer 管理者ユーザを指定します。 -u を指定しない場合は既定値として admin となります。
3	-h --help	条件・設定インポート・エクスポートコマンドのヘルプです。
4	import	条件・設定インポートコマンドです。詳細は E.34.条件・設定インポートコマンドを参照してください。
5	export	条件・設定エクスポートコマンドです。詳細は E.35.条件・設定エクスポートコマンドを参照してください。

E.34. 条件・設定インポートコマンド

検索条件やコンソールサーバの設定情報をインポートするコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。

```
console.bat(sh) impexp import [-ai] [-sc] [-t] [-h] -f import file
```

戻り値: 正常終了時 0

コンソールサーバが停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-ai --auto-import	<p>自動インポート設定(POLICY)を指定します。</p> <p>引数には、インポート表示項目(TYPE)=自動インポート設定(POLICY)の形で記述します。また、セミコロン区切りで、複数指定することができます。この指定は、-f で指定したファイルに記述の自動インポート設定より優先されます。</p> <p>TYPES SYSTEMPROPERTIES : コンソールサーバ設定 LOGGATEGROUP : LogGate グループ LOGSOURCE : ログソース USERGROUP : グループ USER: ユーザ TAG : タグ PARAM : メッセージパラメータ ACTION : アクション APPLICATION : アプリケーション COLUMNSET : カラムセット SEARCH : 検索条件 STATS : 集計条件 SENSOR : 検知ポリシー CUSTOMREPORT : カスタムレポート REPORT : レポート</p> <p>POLICIES MO フォルダをマージ、他は上書き MR フォルダをマージ、他は自動変更 R 全て自動変更</p>	任意/TYPE=POLICY(;セミコロンで複数指定可能)/ファイルに記述の自動インポートポリシー設定

		<p>M 全てマージ(マージ指定可能な項目(TYPE)は以下の通り)</p> <ul style="list-style-type: none"> - APPLICATION - ACTION - PARAM - TAG - LOGSOURCE - USERGROUP 	
2	<p>-sc</p> <p>--show-contents</p>	<p>指定したインポートファイルの内容の表示のみを行い、実際の更新は行いません。</p>	任意/なし/既定値なし
3	<p>-t</p> <p>--types-filter</p>	<p>インポートする項目(TYPE)を指定します。また、セミコロン区切りで、複数指定することができます。</p> <p>TYPES</p> <p>SYSTEMPROPERTIES : コンソールサーバ設定</p> <p>LOGGATEGROUP : LogGate グループ</p> <p>LOGSOURCE : ログソース</p> <p>USERGROUP : グループ</p> <p>USER: ユーザ</p> <p>TAG : タグ</p> <p>APPLICATION : アプリケーション</p> <p>COLUMNSET : カラムセット</p> <p>SEARCH : 検索条件</p> <p>STATS : 集計条件</p> <p>SENSOR : 検知ポリシー</p> <p>CUSTOMREPORT : カスタムレポート</p> <p>REPORT : レポート</p>	任意/ TYPE(;セミコロンで複数指定可能)/全ての TYPE が対象
4	<p>-h</p> <p>--help</p>	<p>インポートコマンドのヘルプを表示します。</p>	任意/なし/既定値なし
5	<p>-f</p> <p>--file</p>	<p>インポートするファイルのパスを指定します。</p>	必須/ファイルパス/既定値なし

自動インポートを指定しない場合、インポート不整合が発生するとインポートは失敗し、下記のメッセージが表示されます。その際は `-ai` オプションで指定して自動インポート設定を指定してください。

Import failed. Please check your automatic import settings.

Details:

データの整合性に問題が見つかりました。処置状況に従い自動インポートポリシーを指定してください。

E.35. 条件・設定エクスポートコマンド

検索条件やコンソールサーバの設定情報をエクスポートするコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。

```
console.bat(sh) impexp export [-ai] [-e] [-p] [-v] [-t] [-h] -f export file
```

戻り値: 正常終了時 0

コンソールサーバが停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-ai --auto-im port	<p>自動インポート設定(POLICY)を指定します。</p> <p>引数には、インポート表示項目(TYPE)=自動インポート設定(POLICY)の形で記述します。また、セミコロン区切りで、複数指定することができます。</p> <p>TYPES</p> <p>SYSTEMPROPERTIES : コンソールサーバ設定</p> <p>LOGGATEGROUP : LogGate グループ</p> <p>LOGSOURCE : ログソース</p> <p>USERGROUP : グループ</p> <p>USER : ユーザ</p> <p>TAG : タグ</p> <p>PARAM : メッセージパラメータ</p> <p>ACTION : アクション</p> <p>APPLICATION : アプリケーション</p> <p>COLUMNSET : カラムセット</p> <p>SEARCH : 検索条件</p> <p>STATS : 集計条件</p> <p>SENSOR : 検知ポリシー</p> <p>CUSTOMREPORT : カスタムレポート</p> <p>REPORT : レポート</p> <p>DEFAULT</p> <p>POLICIES</p> <p>MO フォルダをマージ、他は上書き</p> <p>MR フォルダをマージ、他は自動変更</p> <p>R 全て自動変更</p>	<p>任意/TYPE=POLICY(;セミコロンで複数指定可能)/規定値なし</p>

		<p>M 全てマージ(マージ指定可能な項目(TYPE)は以下の通り)</p> <ul style="list-style-type: none"> - APPLICATION - ACTION - PARAM - TAG - LOGSOURCE - USERGROUP 	
2	<p>-e --exclude</p>	<p>指定した項目以外全ての項目をエクスポートします。-e のみ指定の場合は、(項目)=(名前)を引数に指定します。</p> <p>タグ名が url 以外をエクスポートする例: -e tag=url</p> <p>-e に続けて -t を指定する場合は -e への引数は必要なく、-t に指定する項目の指定のみで実行可能です。</p> <p>例: -e -t loggategroup</p> <p>但し、指定した項目が他の項目から参照されている(タグがメッセージパラメータにアサインされている)場合、除外されずエクスポートされます。</p>	<p>任意/ TYPE(;セミコロンで複数指定可能)/DEFAULT</p>
3	<p>-p --preview</p>	<p>指定したオプションで生成されるファイルの内容の表示のみを行い、実際のエクスポートは行いません。</p>	<p>任意/なし/既定値なし</p>
4	<p>-v --version</p>	<p>エクスポートするファイルのバージョンを指定します。インポート先の IVEX Logger Viewer バージョンにあわせて指定します。</p> <p>1.0 : 1.0 (IVEX Logger Viewer 3.5.x)</p> <p>-f で指定するファイル名の拡張子に csv を指定した場合はこの設定は無視されます。</p>	<p>任意/なし/1.5</p>
5	<p>-t --types-filter</p>	<p>エクスポートする項目(TYPE)を指定します。また、セミコロン区切りで、複数指定することができます。</p> <p>TYPES</p> <p>SYSTEMPROPERTIES : コンソールサーバ設定</p> <p>LOGGATEGROUP : LogGate グループ</p> <p>LOGSOURCE : ログソース</p> <p>USERGROUP : グループ</p> <p>USER : ユーザ</p> <p>TAG : タグ</p> <p>APPLICATION : アプリケーション</p> <p>COLUMNSET : カラムセット</p> <p>SEARCH : 検索条件</p>	<p>任意/ TYPE(;セミコロンで複数指定可能)/DEFAULT</p>

付録 E. コマンドリファレンス

		STATS : 集計条件 SENSOR : 検知ポリシー CUSTOMREPORT : カスタムレポート REPORT : レポート DEFAULT : 全ての TYPE	
6	-h --help	エクスポートコマンドのヘルプを表示します。	任意/なし/既定値なし
7	-f --file	エクスポートするファイルのパスを指定します。 出力するファイル形式は、ファイル名の拡張子によって自動的に変わります。ファイル名の拡張子には zip, csv, xml を指定することができます。	必須/ファイルパス/既定値なし

E.36. レポート管理コマンド

レポートの実行・中断などレポートを管理するコマンドです。

```
console.bat(sh) report 「 -p | -u | -h 」 「list | history | start | stop | help 」  
「Options」
```

	パラメータ	パラメータ概要
1	-p --adminpass	レポート管理コマンドを実行する IVEX Logger Viewer 管理者ユーザパスワードを指定します。 -p を指定しない場合はコマンドプロンプトの対話形式で入力します。
2	-u --adminuser	レポート管理コマンドを実行する IVEX Logger Viewer 管理者ユーザを指定します。 -u を指定しない場合は既定値として admin となります。
3	-h --help	レポート管理コマンドのヘルプです。
4	list	レポート作成条件一覧表示コマンドです。詳細は E.37.レポート作成条件一覧表示コマンドを参照してください。
5	history	レポート作成履歴一覧表示コマンドです。詳細は E.38.レポート作成履歴一覧表示コマンドを参照してください。
6	start	レポート実行コマンドです。詳細は E.39.レポート実行コマンドを参照してください。
7	stop	レポート中断コマンドです。詳細は E.40.レポート中断コマンドを参照してください。
8	help	レポート管理コマンドのヘルプです。 引数に all を指定することで全てのコマンドのヘルプを確認することができます。

E.37. レポート作成条件一覧表示コマンド

コンソールサーバに登録されたレポート作成条件の一覧を表示するコマンドです。コマンドでレポートの実行をする際に現在の状態を確認するためのコマンドです。一覧表示にレポートID(ReportID)、レポート登録名、概要を出力します。このコマンドの実行記録は、admin-console.log に記録します。

```
console.bat(sh) report list [-c]
```

戻り値: 正常終了時 0

コンソールサーバ停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-c --columns	一覧表示をカラム形式で出力します。	任意/なし/既定値なし

E.38. レポート作成履歴一覧表示コマンド

コンソールサーバに登録されたレポート作成履歴の一覧を表示するコマンドです。コマンドでレポート作成履歴の中断をする際に現在の状態を確認するためのコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。

```
console.bat(sh) report history [--status] [-c]
```

戻り値: 正常終了時 0

コンソールサーバ停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	--status	<p>レポート作成履歴のステータスのレポート作成履歴のみを表示します。レポート作成履歴ステータスは、各レポート作成条件がスケジュール上どうなっているかを示します。</p> <p>待機中(wait)</p> <p>レポート作成条件が起動されるタイミングが来ているが、他のレポート作成が実行されているため実行できない状態。</p> <p>実行中(run)</p> <p>レポートの作成を行っている状態。</p> <p>中止(abort)</p> <p>レポート作成を強制的に中断した状態、またはレポート定義が無効状態となっている状態。</p> <p>失敗(fail)</p> <p>レポート作成中、何らかのエラーが発生した状態。</p> <p>完了(complete)</p> <p>レポートが正常に完了した状態。</p> <p>スケジュール登録済み(scheduled)</p> <p>レポート作成条件がスケジュールリングされているが、まだ実行されず待機前の状態。</p>	任意/なし/既定値なし
2	-c --columns	<p>一覧表示をカラム形式で出力します。レポート作成履歴 ID (HistoryID)・レポート登録名・概要・開始時刻・終了時刻・レポート作成ステータス・レポートファイル名を表示します。</p>	任意/なし/既定値なし

E.39. レポート実行コマンド

コンソールサーバに登録されたレポート作成条件を実行するコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。指定するレポート ID は、レポート条件一覧コマンドで取得することができます。また、実行後に表示されるレポート作成履歴一覧表示は、レポート作成履歴一覧コマンド と同じです。なお、レポート実行コマンドは、指定したレポート ID に対応するレポート作成条件を作成スケジュールに登録するまでです。既に他のレポート作成条件が実行状態にある場合は、待機中となります。

```
console.bat(sh) report start [-ids ReportID | all] [-c]
```

戻り値: 正常終了時 0

コンソールサーバ停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-ids --reportlds	実行するレポートIDを指定します。レポートID(ReportID)は、カンマ区切りで複数指定ができます。All を指定した場合は全てのレポートが対象となります。 All を指定しない場合でも、レポート作成条件の有効・無効を指定を問わず対象となる。	必須/レポートID(カンマにて複数指定可)または all/既定値なし
2	-c --columns	実行結果の一覧表示をカラム形式で出力します。	任意/なし/既定値なし

E.40. レポート中断コマンド

コンソールサーバに登録されたレポート作成履歴を中断するコマンドです。このコマンドの実行記録は、`admin-console.log` に記録します。指定したレポート作成履歴 ID のレポート作成を中断、またはキャンセルし、その結果をレポート作成履歴一覧表示します。中断・キャンセルできるレポートは実行中または待機中のみです。表示されるレポート作成履歴は、レポート作成履歴一覧表示コマンドと同じです。なお、レポート中断コマンドは、中断のタイミングや順序によって古い情報が表示されることがあります。指定したレポート作成履歴 ID が中止されていない場合は、レポート作成履歴表示コマンドを使ってしばらく経ってから確認してください。

```
console.bat(sh) report stop [-ids HistoryID | all] [-c]
```

戻り値: 正常終了時 0

コンソールサーバ停止時: 0 以外

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-ids --historyids	実行するレポート作成履歴 ID (HistoryID) を指定します。レポート作成履歴 ID は、カンマ区切りで複数指定ができます。all を指定した場合は全てのレポートが対象となります。	必須/レポート作成履歴 ID (カンマにて複数指定可) または all/既定値なし
2	-c --columns	実行結果の一覧表示をカラム形式で出力します。	任意/なし/既定値なし

E.41. 内部データベースバックアップコマンド

コンソールサーバの内部データベースをバックアップするコマンドです。このコマンドの実行結果は、標準出力に出力します。実行記録はログに出力しません。内部データベースには検索条件やログフォーマット定義・IVEX Logger Viewer のユーザ情報が記録されています。このコマンドはこれらのデータをバックアップする際に使用します。コマンドはコンソールサーバが起動・停止のどちらでも実行することができます。また、下記のバックアップファイルパスは必須です。バックアップするファイル名の拡張子には必ず[.tar.gz]を指定してください。

```
console.bat(sh) db backup [-f] [-h] バックアップファイルパス(拡張子.tar.gz)
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-f	実行時の確認(yes/no)を無視します。	任意/なし/規定値なし
2	-h	コマンドのヘルプを表示します。	任意/なし/既定値なし

E.42. 内部データベースリストアコマンド

コンソールサーバの内部データベースをリストアするコマンドです。このコマンドの実行結果は、標準出力に出力します。実行記録はログに出力しません。内部データベースには検索条件やログフォーマット定義・IVEX Logger Viewer のユーザ情報が記録されています。このコマンドはこれらバックアップされたデータをリストアする際に使用します。コマンドはコンソールサーバが停止のときのみ実行することができます。また、下記のバックアップファイルパスは必須です。バックアップファイル名の拡張子には必ず[.tar.gz]を指定してください。

```
Console.bat(sh) db restore [-f] [-h] バックアップファイルパス(拡張子.tar.gz)
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-f	実行時の確認(yes/no)を無視します。	任意/なし/規定値なし
2	-h	コマンドのヘルプを表示します。	任意/なし/既定値なし

E.43. ログフォーマット定義 ID 表示コマンド

コンソールサーバが管理しているログフォーマット定義 ID を確認するためのコマンドです。

ログフォーマット定義はコンソールサーバの内部データベースに保存されており、画面上で定義を更新する度に ID が増加していきます。LogDS ではこのログフォーマット定義 ID と自身が管理する構造化ログデータとを結び付けてログを保存しています。

下記のバックアップファイルパスは任意です。指定しない場合、稼働中の内部データベースに格納されているログフォーマット定義 ID を表示します。指定した場合は、当該バックアップファイル内に格納されているログフォーマット定義 ID を表示します。

```
console.bat(sh) db logfmtid [-h] [-t] [バックアップファイルパス(拡張子.tar.gz)]
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	-t	バックアップファイルのパスを指定します。指定されたファイル内のログフォーマット定義 ID を表示します。	任意/なし/規定値なし
2	-h	コマンドのヘルプを表示します。	任意/なし/既定値なし

E.44. 診断コマンド(情報収集コマンド)

情報収集コマンドは、動作ログや環境変数、各種設定ファイルなどを収集するコマンドです。弊社サポートセンターより実行を依頼する場合の利用を想定しています。収集した情報は zip 圧縮されて -z オプションに指定したディレクトリに出力します。

```
inspector.bat(sh) { full | min | custom } -z outputdir
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	full	以下の情報を収集します。 <ul style="list-style-type: none"> ・動作ログ ・バージョン情報 ・logds.bat(sh) status コマンド実行結果 ・LogDS 内部情報(ファイルリスト等) ・LogDS ビューアコマンド実行結果 ・ワークディレクトリ ・設定ファイル ・内部データベース ・環境変数 	full, min, custom 何れか必須/なし/ 既定値なし
2	min	以下の情報を取得します。 <ul style="list-style-type: none"> ・動作ログ ・バージョン情報 ・logds.bat(sh) status コマンド実行結果 ・LogDS 内部情報(ファイルリスト等) ・ワークディレクトリ ・設定ファイル ・環境変数 	full, min, custom 何れか必須/なし/ 既定値なし
3	custom	収集する情報を指定します。以下のオプション(複数指定可)を指定します。 <ul style="list-style-type: none"> -c --conf : 設定ファイル -l --log : 動作ログ -db --hsqldb : 内部データベース -ds --logds : LogDS 内部情報及び logds.bat(sh) status コマンド実行結果 -w --loggateway : ワークディレクトリ 	full, min, custom 何れか必須/なし/ 既定値なし custom 指定オプション何れか必須/なし/既定値なし

付録 E. コマンドリファレンス

		-v --version : バージョン情報	
	-z --zipdir	収集した情報の出力先ディレクトリ	必須/なし/既定値なし

E.45. 診断コマンド(LogDS ビューアコマンド)

LogDS ビューアコマンドは、LogDS 内部のデータ整合性や破損有無などの診断、及びログデータをテキストでエクスポートして破損有無(破損があった場合は想定される期間)を調査するコマンドです。弊社サポートセンターより実行を依頼する場合の利用を想定しています(その為、実際にコマンドのヘルプを表示した際に出力される内容と下表のパラメータ表記・説明内容とに差異があります)。

```
logdsViewer.bat(sh) { ds | exp } [options] [-h] <args>
```

戻り値: 正常終了時 0

エラー終了時: 0 以外

	パラメータ	パラメータ概要	必須有無/入力範囲/既定値
1	ds	LogDS 内部の状態を診断し結果を-d オプション指定先に出力します。その他、以下のオプションを指定します。 -ds : LogDS フォルダのパス -d : 診断結果の出力先 -alg : 暗号化アルゴリズム(暗号化設定オンの場合) -key : 暗号化キー(暗号化設定オンの場合) このコマンドの動作ログはコマンドを実行した際のカレントディレクトリに「logdsViewer.log」というファイル名で出力されます。	ds, exp 何れか必須/なし/規定値なし
2	exp	LogDS からログデータをテキストでエクスポートします。破損があった場合は、破損している期間も出力します。このコマンドを実行するには事前に「ds -d」を指定して診断情報を生成する必要があります。 -ds : LogDS フォルダのパス -o : エクスポートログデータの出力先 -b : 破損ログの出力先 -d : 「ds -d」コマンドで指定した診断結果出力先	ds, exp 何れか必須/なし/規定値なし
3	-h	コマンドのヘルプ表示です。	任意/特になし/既定値なし

付録F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

以下にコンソールサーバ設定ファイル(logstd.dcf)及び LogGate 設定ファイル(loggate.dcf)の設定項目(一覧)を記載します。

設定項目	既定値	設定内容
com.Logstorage.charset	MS932	ログファイルのファイルエンコーディング
db.host	127.0.0.1	内部データベースを格納しているサーバの IP アドレスを設定します。
db.port	9999	内部データベースのポート番号を設定します。
db.resource	logst	内部データベースのリソース名 ※通常変更する必要はありません。
db.user	sa	内部データベースのユーザ名 ※通常変更する必要はありません。
db.password	—	内部データベースのパスワード ※通常変更する必要はありません。
db.maxconnections	15	内部データベースへの最大接続数を指定します。
db.initialconnections	3	内部データベースへの初期コネクション数を指定します。
db.retry	3	コネクションが確立できなかった場合のトライ回数を設定します。 0 を指定した場合、再接続は行いません。
db.interval	10000(ミリ秒)	再接続待ち時間をミリ秒で設定します。 Db.retry が 1 以上の場合のみ有効です。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.receivers	com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver, com.Logstorage.engine.loggate.receive.SyslogUDPReceiver, com.Logstorage.engine.loggate.receive.SyslogFTPReceiver, com.Logstorage.engine.loggate.receive.SyslogFileReceiver, com.Logstorage.engine.loggate.receive.SyslogAdhocFileReceiver, com.Logstorage.engine.loggate.receive.SyslogSnmpTrapReceiver, com.Logstorage.engine.loggate.receive.SyslogLltpReceiver, com.Logstorage.engine.loggate.receive.SyslogSslReceiver	<p>起動するレシーバを指定します。※IVEX Logger Viewer では変更の必要はありません。</p> <p>起動するレシーバが複数ある場合は、レシーバ名をカンマ「,」区切りで記載します。レシーバ名は下記にあわせて記載して下さい。</p> <p>TCP レシーバ: com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver</p> <p>UDP レシーバ: com.Logstorage.engine.loggate.receive.SyslogUDPReceiver</p> <p>FTP レシーバ: com.Logstorage.engine.loggate.receive.SyslogFTPReceiver</p> <p>ファイルレシーバ: com.Logstorage.engine.loggate.receive.SyslogFileReceiver</p> <p>アドホックファイルレシーバ: com.Logstorage.engine.loggate.receive.SyslogAdhocFileReceiver</p> <p>SNMP ファイルレシーバ: com.Logstorage.engine.loggate.receive.SyslogSnmpTrapReceiver</p> <p>LLTP レシーバ: com.Logstorage.engine.loggate.receive.SyslogLltpReceiver</p> <p>TLS レシーバ com.Logstorage.engine.loggate.receive.SyslogSslReceiver</p>
com.Logstorage.engine.loggate.SequentialLogFileManager.sequentialLogDir	C:\¥¥loggatework¥¥seqlog	<p>シーケンシャルログディレクトリのパスを指定します。</p> <p>既定値では、IVEX Logger Viewer インストール時に指定された LogGate ワーク先ディレクトリ内の seqlog ディレクトリが指定されています。</p>

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.receive. SequentialLogWriter.maxLength	268435456(バイト) (256MB)	シーケンシャルログファイルのローテーションサイズを指定します。 シーケンシャルログファイルがこのサイズを超えた場合、シーケンシャルログファイルがローテーションします。なお、LogGate が稼働中の間は設定した値(デフォルト 256MB)を超えるまでシーケンシャルログファイルは削除されません。LogGate を再起動すると起動前に残っていたシーケンシャルログファイルは取り込み終了後に削除されます。
com.Logstorage.engine.loggate.receive. SyslogReceiver.adjustTimestamp	true	年補正機能を使用するかどうかを設定します。 true: 年補正機能を使用します。 false: 年補正機能を使用しません。
com.Logstorage.engine.loggate.receive. SyslogReceiver.adjustTimestamp.start	Dec 01 00:00:00	年補正機能を開始する日時を指定します。 年補正機能を使用する場合に有効になります。 補正開始時刻～12 月 31 日 23:59:59 のログには LogGate のシステム時刻に応じて以下の年のタイムスタンプが付加します。 システム時刻が 1 月～6 月:システム年-1 システム時刻が 7 月～12 月:システム年
com.Logstorage.engine.loggate.receive. SyslogReceiver.adjustTimestamp.end	Jan 31 23:59:59	年補正機能を終了する日時を指定します。 年補正機能を行う場合に有効になります。 1 月 1 日 0:00:00～補正終了時刻のログには LogGate のシステム時刻に応じて以下の年のタイムスタンプが付加します。 システム時刻が 1 月～6 月:システム年 システム時刻が 7 月～12 月:システム年+1

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.bindAddresses	全ローカルアドレス (0.0.0.0)	TCP レシーバがバインドする IP アドレスを指定します。 既定値では LogGate がインストールされた筐体の全ての IP アドレスをバインドします。
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.port	5140	TCP レシーバがログ受信で使用するポート番号を指定します。 既定値を変更した場合、ログソースの送信先ポート番号も変更する必要があります。
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.keepAlive	true	TCP レシーバとログソースとの接続を監視し、ログソースから送信されるログが一定時間ない場合、接続を切断するかどうかを設定します。 True: 接続を維持したままにします。 False: 接続を切断します。
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.maxConnection	512	TCP レシーバへ接続するログソースの最大数を設定します。 ログソースからの TCP レシーバへの最大接続数が既定値を超える場合に変更します。
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.pktlength	8192 (バイト)	TCP レシーバが受信したログの1レコード当たりの最大サイズを設定します。最大サイズを超えたログを受信した場合は、強制的に改行され、改めて IVEX Logger Viewer 形式に変換されて格納します。 既定値は 8,192 バイトです。 このパラメータを設定する場合は、本パラメータをコンソールサーバ設定ファイル(logstd.dcf)又は LogGate 設定ファイル(loggate.dcf)の任意の行に追記し設定します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.illegalAction	MESSAGE	<p>TCP レシーバで SYSLOG 形式ではないログを受信した場合の動作を、MESSAGE、ANY_MESSAGE、DESTROY から指定します。</p> <p>MESSAGE:ログに PRI 部がある場合、PRI 部はログに付加された値を使用し、新たにタイムスタンプとホスト名を付加しログとして扱います。ログに PRI 部がない場合、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>ANY_MESSAGE:ログに PRI 部がある場合でも、ログに付加された PRI 部は使用せず、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>DESTROY: 受信ログを破棄します。</p>
com.Logstorage.engine.loggate.receive.SyslogTCPSelectReceiver.hostAction	MESSAGE	<p>TCP レシーバで受信したログのヘッダに含まれるホスト名の IP アドレスを解決できない場合の動作を MESSAGE、IGNORE、DESTROY から指定します。</p> <p>MESSAGE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名以降をログのメッセージとして扱います。</p> <p>IGNORE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名より後ろをログのメッセージとして扱います。</p> <p>DESTROY: 受信ログを破棄します。</p>

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.bindAddress	全ローカルアドレス (0.0.0.0)	UDP レシーバがバインドする IP アドレス 既定値では LogGate がインストールされた筐体の全ての IP アドレスをバインドします。
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.port	514	UDP レシーバがログ受信で使用するポート番号 既定値を変更した場合、ログソースの送信先ポート番号も変更する必要があります。
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.pktlength	2048(バイト)	UDP レシーバで受信する 1 行あたりの最大ログサイズ(バイト)を設定します。 この値を超えるログを受信した場合はログを破棄します。
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.receiveBufferSize	131072 (128×1024) (バイト)	UDP レシーバで受信するログのバッファの長さ(バイト)を設定します。このバッファは取りこぼしを減らすためのバッファです。なお、バッファから溢れたログは失います。バッファが大きいほど取りこぼしが起きにくくなります。
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.illegalAction	MESSAGE	UDP レシーバで SYSLOG 形式ではないログを受信した場合の動作を、MESSAGE、ANY_MESSAGE、DESTROY から指定します。 MESSAGE:ログに PRI 部がある場合、PRI 部はログに付加された値を使用し、新たにタイムスタンプとホスト名を付加しログとして扱います。ログに PRI 部がない場合、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。 ANY_MESSAGE:ログに PRI 部がある場合でも、ログに付加された PRI 部は使用せず、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。 DESTROY: 受信ログを破棄します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.receive.SyslogUDPReceiver.hostAction	MESSAGE	UDP レシーバで受信したログのヘッダに含まれるホスト名の IP アドレスを解決できない場合の動作を MESSAGE、IGNORE、DESTROY から指定します。 MESSAGE: ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名以降をログのメッセージとして扱います。 IGNORE: ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名より後ろをログのメッセージとして扱います。 DESTROY: 受信ログを破棄します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.bindAddress</code>	全ローカルアドレス (0.0.0.0)	LLTP レシーバがバインドする IP アドレスを指定します。 既定値では LogGate がインストールされた筐体の全ての IP アドレスをバインドします。
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.port</code>	5141	LLTP レシーバがログ受信で使用するポート番号を指定します。 既定値を変更した場合、ログソースの送信先ポート番号も変更する必要があります。
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.keepAlive</code>	true	LLTP レシーバとログソースとの接続を監視し、ログソースから送信されるログが一定時間ない場合、接続を切断するかどうかを設定します。 true: 接続を維持したままにします。 false: 接続を切断します。
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.maxConnection</code>	512	LLTP レシーバへ接続するログソースの最大数を設定します。 ログソースからの TCP レシーバへの最大接続数が既定値を超える場合に変更します。
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.payloadLimit</code>	99999 (バイト)	LLTP レシーバが受信したログの1レコード当たりの最大サイズを設定します。最大サイズを超えたログを受信した場合は、超えた分のログ(文字列)は強制的に削除します。 既定値は 99,999 バイトです。 このパラメータを設定する場合は、本パラメータをコンソールサーバ設定ファイル(logstd.dcf)又は LogGate 設定ファイル(loggate.dcf)の任意の行に追記し設定します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.illegalAction</code>	MESSAGE	<p>LLTP レシーバで SYSLOG 形式ではないログを受信した場合の動作を、MESSAGE、ANY_MESSAGE、DESTROY から指定します。</p> <p>MESSAGE:ログに PRI 部がある場合、PRI 部はログに付加された値を使用し、新たにタイムスタンプとホスト名を付加しログとして扱います。ログに PRI 部がない場合、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>ANY_MESSAGE:ログに PRI 部がある場合でも、ログに付加された PRI 部は使用せず、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>DESTROY: 受信ログを破棄します。</p>
<code>com.Logstorage.engine.loggate.receiver.SyslogLltpReceiver.hostAction</code>	MESSAGE	<p>LLTP レシーバで受信したログのヘッダに含まれるホスト名の IP アドレスを解決できない場合の動作を MESSAGE、IGNORE、DESTROY から指定します。</p> <p>MESSAGE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名以降をログのメッセージとして扱います。</p> <p>IGNORE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名より後ろをログのメッセージとして扱います。</p> <p>DESTROY: 受信ログを破棄します。</p>

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.bindAddress</code>	全ローカルアドレス (0.0.0.0)	TLS レシーバがバインドする IP アドレスを指定します。 既定値では LogGate がインストールされた筐体の全ての IP アドレスをバインドします。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.port</code>	5143	TLS レシーバがログ受信で使用するポート番号を指定します。 既定値を変更した場合、ログソースの送信先ポート番号も変更する必要があります。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.keepAlive</code>	true	TLS レシーバとログ転送元との接続を監視し、転送元から送信されるログが一定時間ない場合、接続を切断するかどうかを設定します。 true: 接続を維持したままにします。 false: 接続を切断します。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.maxConnection</code>	16	TLS レシーバへ接続するログ転送元の最大数を設定します。 ログ転送元からの TLS レシーバへの最大接続数が既定値を超える場合に変更します。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.keyStore</code>	.keystore	TLS レシーバ自己証明の保存先です。keytool 等で作成したキースタアの保存先パスを設定します(フルパス)。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.keyStorePassword</code>	keyStorePassword	キースタアのパスワードを入力します。
<code>com.Logstorage.engine.loggate.receiver.SyslogSslReceiver.keyPassword</code>	keyPassword	キースタアに格納されている鍵のパスワードを入力します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
<code>com.Logstorage.engine.loggate.receive.SyslogSslReceiverillegalAction</code>	MESSAGE	<p>TLS レシーバで SYSLOG 形式ではないログを受信した場合の動作を、MESSAGE、ANY_MESSAGE、DESTROY から指定します。</p> <p>MESSAGE:ログに PRI 部がある場合、PRI 部はログに付加された値を使用し、新たにタイムスタンプとホスト名を付加しログとして扱います。ログに PRI 部がない場合、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>ANY_MESSAGE:ログに PRI 部がある場合でも、ログに付加された PRI 部は使用せず、新たにタイムスタンプとホスト名と PRI 部(user.notice)を付加しログとして扱います。受信したログは illegal.log にも出力します。</p> <p>DESTROY: 受信ログを破棄します。</p>
<code>com.Logstorage.engine.loggate.receive.SyslogSslReceiver.hostAction</code>	MESSAGE	<p>TLS レシーバで受信したログのヘッダに含まれるホスト名の IP アドレスを解決できない場合の動作を MESSAGE、IGNORE、DESTROY から指定します。</p> <p>MESSAGE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名以降をログのメッセージとして扱います。</p> <p>IGNORE:ホスト名にログを送信したホストの IP アドレスを使用します。解決できなかったホスト名より後ろをログのメッセージとして扱います。</p> <p>DESTROY: 受信ログを破棄します。</p>

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.share.notice.ActionServer.history	true	検知履歴の DB 保存フラグ
com.Logstorage.engine.loggate.receive.ReceivedLogNumberFileManager.lltpDir	同設定ファイル内パラメータ logFileDir 以下の lltp	LLTP 管理ファイル保存先のパスを指定します。 既定値では、収集ログ保存先以下の lltp ディレクトリが指定されています。アドバンスト版では、lltp ディレクトリ以下に LogGate ホスト名のついたディレクトリが自動的に作成します。アドバンスト版の場合 lltp ディレクトリは共通のディレクトリとして参照するように設定してください。
com.Logstorage.engine.loggate.workDir	C:¥¥loggatework(Windows の場合) /var/log/loggatework(Linux/Unix の場合)	ワークディレクトリのパスを指定します。
com.Logstorage.engine.logging.store.LogstDequeueTransaction.flushTimeout	30000	現在時刻のログファイルをコミットするタイムアウト間隔(ミリ秒)を指定します。 パラメータ省略時は 30000 が設定します。
com.Logstorage.engine.loggate.receive.LogstFtplet.disableDelLogFile	false	FTP レシーバで受信したログを取り込み後に削除するかどうかを設定します。 False:FTP レシーバで受信したログを取り込み後に削除します。 True:FTP レシーバで受信したログを取り込み後に削除しません。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.web.search.form.compatibleSearch	false	過去ログデータの互換検索機能を有効にする設定です。既定値は false です。true で有効にします。
Com.Logstorage.engine.common.FileManager.logFileDir	C:¥¥log	過去ログデータ(Ver.2 または Ver.3)の収集ログ保存先です。既定値は Ver.2.x/Ver.3.x と同様です。
Com.Logstorage.engine.common.ZipFileManager.archiveDir	C:¥¥log¥¥archive	過去ログデータのアーカイブ保存先です。既定値は Ver.2.x/Ver.3.x と同様です。
Com.Logstorage.engine.common.IndexFileManager.indexDir	C:¥¥log¥¥index	過去ログデータのインデックス保存先です。既定値は Ver.2.x/Ver.3.x と同様です。
Com.Logstorage.share.notice.executer.NoticeMailExecuter.mailServer	localhost	LogGate が検知アラートのメール送信時に使用するメールサーバ名を指定します。LogGate からメールを送付する際、ヘッダは Shift_JIS で MIME(Base64)エンコードし、本文は Quoted-Printable となっております。 MIME エンコード(Shift_JIS)のヘッダをメールサーバ側で正しく扱えていない場合や、ヘッダ部分に機種依存文字を使用している場合は送信先のメーラでメールが文字化けして届くことがあります。
Com..Logstorage.share.notice.executer.NoticeMailExecuter.mailFrom	admin@localhost	LogGate がメール送信時に使用するメールの差出人を設定します。差出人はエンベロープ From に指定されるメールアドレスです。このメールアドレスでメールが受信できるようメールサーバに登録する必要はありません。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.sensor.flushOnStopping	false	<p>検知ポリシーの同期処理が実行される前に、メモリ上の検知待ちバッファログが全て検知されるまで検知ポリシーの同期処理を待つオプションです。この flushOnStopping オプションは</p> <p>flushTimeoutOnStopping オプションとセットで設定してください。</p> <p>False: 即時同期処理実行します。(4.2.0 以前と同様の処理)</p> <p>true: バッファログの全検知を待ちます。</p>
Com.Logstorage.engine.sensor.flushTimeoutOnStopping	60000	<p>指定時間検知待ちを行い超えた場合は割り込み、検知ポリシーの同期処理を実施します。-1 を指定した場合はタイムアウト無し(無制限に待つ)です。flushOnStopping が false の場合、この設定値は無視されます。この flushTimeoutOnStopping オプションは flushOnStopping オプションとセットで設定してください。</p> <p>単位はミリ秒です。</p>
Com.Logstorage.engine.sensor.blockWhileRestarting	false	<p>検知ポリシーの同期処理が実行されている間、収集ログの LogDS 構造化処理をブロックし、シーケンシャルファイルまでの収集となります。同期処理完了後、シーケンシャルファイルからの LogDS 構造化、検知処理が再開されます。</p> <p>False: 同期中も LogDS 構造化を継続、検知をスキップします。(4.2.0 以前と同様の処理)</p> <p>true : LogDS 構造化をブロックします。</p>

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.logging.retry_to_raise	2(回)	セカンダリ LogGate からプライマリ LogGate へのハートビート確認リトライ回数を設定します。 この回数に達すると LogGate の切り替えが発生します。
com.Logstorage.engine.logging.wait_for_retry	3000(ミリ秒)	セカンダリ LogGate からプライマリ LogGate のハートビートが確認できなかった場合の、ハートビート確認のリトライ待ち時間を設定します。
com.Logstorage.engine.logging.time_out_lookup	10000(ミリ秒)	セカンダリ LogGate からプライマリ LogGate のハートビートを確認した場合の、タイムアウト時間を設定します。 この時間までにセカンダリ LogGate がプライマリ LogGate のハートビートを確認できなければ、セカンダリ LogGate はハートビートのリトライを行います。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.LogDBMapper	MONTHLY	LogDS の保存単位を指定します。原則月単位で運用します。

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

設定項目	既定値	設定内容
com.Logstorage.engine.loggate.send.SyslogSender.relayType	off	転送タイプを指定します。 off: 転送無効 socket: UDP/TCP/TLS 何れかで転送 file: ファイル転送
com.Logstorage.engine.loggate.send.SyslogSender.logType	Logstorage	転送先へ送信するログの形式を選択します。 Logstorage: Logstorage 形式のヘッダを付与します。 syslog: Syslog 形式のヘッダを付与します
com.Logstorage.engine.loggate.send.SyslogSender.destinationAddress	sendTo	名前解決可能なホスト名、若しくは IP アドレスを入力します。転送可能なホスト(IP アドレス)は 1 つに限られます。
com.Logstorage.engine.loggate.send.SyslogSender.destinationPort	5143	転送先のポートを入力します。
com.Logstorage.engine.loggate.send.SyslogSender.localAddress	-	バインドする IP アドレスを入力します。
com.Logstorage.engine.loggate.send.SyslogSender.localPort	0	バインドするポートを入力します。
com.Logstorage.engine.loggate.send.SyslogSender.protocol	tls	転送先との転送プロトコルを選択します。 tls: TLS で転送します。データ形式に Logstorage を指定した場合は tls のみ選択可能です。 udp: UDP で転送します。データ形式に syslog を指定した場合のみ選択可能です。 tcp: TCP で転送します。データ形式に syslog を指定した場合のみ選択可能です。
com.Logstorage.engine.loggate.send.SyslogSender.keep	true	転送先との接続を監視し、この LogGate から転送するログが一定時

付録 F. コンソールサーバ設定ファイル(LogGate 設定ファイル)設定項目一覧

Alive		間ない場合、接続を切断するかどうかを設定します。
com.Logstorage.engine.loggate.send.SyslogSender.trustStore	.trustStore	トラストストア(ファイル)のフルパスを入力します(TLS プロトコル選択時のみ)。
com.Logstorage.engine.loggate.send.SyslogSender.trustStorePassword	-	トラストストアのパスワードを入力します(TLS プロトコル選択時のみ)。
com.Logstorage.engine.loggate.send.SyslogSender.historyLastSent	100	転送したログの履歴を何件保存するかを入力します。履歴 1 件はログ 1 行の転送に相当します。
com.Logstorage.engine.loggate.send.SyslogSender.relayFile	relay.log	ログをファイルに転送する場合のファイル名を指定します。
com.Logstorage.engine.loggate.send.SyslogSender.relayRotate	1	ファイルにログを転送する場合のローテートファイル数を指定します。
com.Logstorage.engine.loggate.send.SyslogSender.relayRotateUnit	hour	ファイルにログを転送する場合のローテート単位数を指定します。 (hour/day)
com.Logstorage.engine.loggate.send.SyslogSender.filterEnabled	false	転送フィルタ有効・無効設定です。 true: 有効 false: 無効
com.Logstorage.engine.loggate.send.SyslogSender.relayFilter	-	転送フィルタ名(検索条件名)です。

付録G. FTP レスポンスコード

以下に LogGate サーバが提供する FTP サーバのレスポンスコードを記載します。

コード	メッセージ例	意味
110	Restart marker reply.	REST コマンドのためのマーカー返答である
120	Service ready in nnn minutes.	サービスは停止しているが、nnn 分後に準備できる
125	Data connection already open; transfer starting	データコネクションはすでに確立されている。このコネクションで転送を開始する
150	File status okay; about to open data connection	ファイルステータスは正常である。データコネクションを確立する
200	Command okay	コマンドは正常に受け入れられた
202	Command not implemented, superfluous at this site	コマンドは実装されていない。SITE コマンドで OS コマンドが適切でない場合など
211	System status, or system help reply	STAT コマンドに対するレスポンス
212	Directory status	STAT コマンドによるディレクトリ情報を示す
213	File status	STAT コマンドによるファイル情報を示す
214	Help message	HELP コマンドに対するレスポンス
215	NAME system type	SYST コマンドに対するレスポンス
220	Service ready for new user	新規ユーザー向けに準備が整った。ログイン時に表示される場合を想定している
221	Service closing control connection	コントロールコネクションを切断する。QUIT コマンド時のレスポンス
225	Data connection open; no transfer in progress	データコネクションを確立した。データの転送は行われていない
226	Closing data connection	要求されたリクエストは成功した。データコネクションをクローズする
227	Entering Passive Mode (h1,h2,h3,h4,p1,p2)	PASV コマンドへのレスポンス。H1～h4 は IP アドレス、p1～p2 はポート番号を示す
230	User logged in, proceed	ユーザーログインの成功
250	Requested file action okay, completed	要求されたコマンドによる操作は正常終了した
257	PATHNAME created	ファイルやディレクトリを作成したというのが RFC での意味だが、MKD コマンドの結果以外にも、実際には PWD コマンドの結果にも用いられる

付録 G. FTP レスポンスコード

コード	メッセージ例	意味
331	User name okay, need password	パスワードの入力を求める
332	Need account for login	ACCT コマンドで課金情報を指定する必要がある
350	Requested file action pending further information	他の何らかの情報を求めている
421	Service not available, closing control connection	サービスを提供できない。コントロールコネクションを終了する。サーバのシャットダウン時など
425	Can't open data connection	データコネクションをオープンできない
426	Connection closed; transfer aborted	何らかの原因により、コネクションをクローズし、データ転送も中止した
450	Requested file action not taken	要求されたリクエストはアクセス権限やファイルシステムの理由で実行できない
451	Requested action aborted. Local error in processing.	ローカルエラーのため処理を中止した
452	Requested action not taken	ディスク容量の問題で実行できない
500	Syntax error, command unrecognized	コマンドの文法エラー
501	Syntax error in parameters or arguments	引数やパラメータの文法エラー
502	Command not implemented	コマンドは未実装である
503	Bad sequence of commands	コマンドを用いる順番が間違っている
504	Command not implemented for that parameter	引数やパラメータが未実装
530	Not logged in	ユーザーはログインできなかった
532	Need account for storing files	ファイル送信には、ACCT コマンドで課金情報を確認しなくてはならない
550	Requested action not taken	要求されたリクエストはアクセス権限やファイルシステムの理由で実行できない
551	Requested action aborted. Page type unknown.	ページ構造のタイプの問題で実行できない
552	Requested file action aborted	ディスク容量の問題で実行できない
553	Requested action not taken	ファイル名が間違っているため実行できない

付録H. 外部レポートエンジン仕様

コンソールサーバのレポートエンジンが外部レポートエンジン呼び出す際の仕様について説明します。

H.1. レポートエンジンからの呼び出し書式

<コマンド>

外部レポートエンジン [外部レポートエンジン引数...] XML ファイル

以下にコマンドに付加するパラメータについて説明します。

パラメータ	説明
外部レポートエンジン引数	外部レポートエンジンのオプションです。 コンソールサーバのカスタムレポート追加画面に設定します。
XML ファイル	コンソールサーバのレポートエンジンが作成した XML ファイルの絶対パスです。 XML ファイルの出力先は、既定値では以下の通りです。 C:¥logstorage¥report ファイル名は一意に付けられます。

H.2. 終了コード

外部レポートエンジンが出力した終了コードをレポートエンジンが受け取り、その値によって処理を継続するか否かを判別します。

終了コードは IVEX Logger Viewer のログに以下の形式で出力します。

<終了コードの出力形式>

<code>exec command exit code = 終了コード</code>

以下に終了コードが出力された際のレポートエンジンの動作を記載します。

終了コード	レポートエンジンの動作
0	外部レポートエンジンが正常に処理を終了したとみなし、レポートエンジンは処理を継続します。
0 以外	外部レポートエンジンの処理が正常に終了しなかったとみなし、レポートエンジンはその後の処理をキャンセルします。

H.3. 外部レポートエンジンの内部仕様

- 外部レポートエンジンが XML ファイルの書き換えのみ行う場合は特に規定はありません。外部レポートエンジンが XML ファイルを書き換えた後、レポートエンジンが XSLT を使用してレポートを作成します。
- 外部レポートエンジンが XML ファイルの書き換えだけでなく、レポートを作成する場合は、外部レポートエンジンがレポート作成後に標準出力にファイル名を出力する必要があります。
- レポートエンジンは外部レポートエンジンの標準出力を全て受け取り、最後に標準出力に出力された文字列をレポートファイル名として処理します。

標準出力の最後の文字列と同じ名前を持つファイルが存在しない場合は、レポートエンジンが XSLT を使用してレポート作成を行います。

H.4. レポートエンジンが出力する XML ファイルの仕様

外部レポートエンジンはコンソールサーバのレポートエンジンが出力する XML ファイルを読み込みます。

コンソールサーバのレポートエンジンが出力する XML ファイル仕様は、コンソールサーバのホームディレクトリ以下にある conf/report/ディレクトリの dtd 及び xsd ファイルをご覧ください。

付録I. IVEX Logger Viewer が出力するログファイル一覧

IVEX Logger Viewer が出力するログには、以下のログがあります。

ファイル名	主に出力される内容
console.log	コンソールサーバの起動、動作、エラー等のログを出力します。
loggate.log	LogGate の起動、動作、エラー等のログを出力します。
audit.log	コンソールサーバへのログイン/ログアウト等の監査ログを出力します。
admin-logds.log	LogDS 管理コマンドに関するログを出力します。
admin-console.log	コンソールサーバ管理コマンドでユーザ管理、レポート管理、インポート・エクスポートに関するログを出力します。
admin-loggate.log	LogGate 管理コマンドに関するログを出力します。
admin-supporttools.log	診断コマンドに関するログを出力します。
commons-daemon.yyyy-mm-dd.log	サービスの起動、停止等のログを出力します。
consoleserver-stdout.yyyy-mm-dd.log	Tomcat の起動、動作等のログを出力します。
consoleserver-stderr.yyyy-mm-dd.log	Tomcat のエラー等のログを出力します。
loggate-stdout.yyyy-mm-dd.log	LogGate の起動、停止等のログを出力します。
loggate-stderr.yyyy-mm-dd.log	LogGate のエラー等のログを出力します。
catalina.out (Unix 版) catalina.yyyy-mm-dd.log (Windows 版)	Tomcat のエラー等のログを出力します。 出力先は以下の通りです。 %LOGST_HOME%/tomcat/logs/
illegal.log	受信したログが IVEX Logger Viewer 形式ではないログの場合、受信したログを不正なログとして判断し出力します。
illegalAddress.log	受信ログがシーケンシャルログに書き込まれ、LogDS へ格納する際に、IVEX Logger Viewer 形式の IP アドレス部が ipv4/ipv6 何れの形式でも無い場合不正ログと判断し出力します。

IVEX Logger Series Ver 5.2.0

最終更新日: 2016.1.29(初版)

日本ナレッジ株式会社 <<http://www.know-net.co.jp/>>

〒111-0042 東京都台東区寿 3-19-5 JSビル 9F

TEL: 03-3845-4784