ERI0665A

2026 年 11 月 20 日

お客様各位

株式会社アシスト
ビジネスインフラ技術本部 システム基盤技術統括部

Ericom Shield Cloud セキュリティインシデントに関するご報告(中間報告)

拝啓
貴社益々ご清栄のこととお慶び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。貴社にてご利用いただいております Ericom Shield Cloud のセキュリティインシデントにてご迷惑をおかけしており、誠に申し訳ございません。下記の通り中間報告をいたします。ご査収の程お願い申し上げます。

敬具

記

1) インシデント内容
2) 不正アクセス発生日時
3) 不正アクセスの原因
4) Ericsson 社における検知と対応
5) 漏洩した可能性がある情報
6) 漏洩した情報の影響
7) Ericsson 社にて対応済みの内容
8) お客様へご協力のお願い
9) 今後の対応について

1) インシデント内容

Ericom Shield Cloud をホストするクラウドインフラを経由し、第三者による Ericom Shield Cloud への不正アクセスが発生しました。

2) 不正アクセス発生日時

現時点で確認できている情報は、以下となります。

●Ericsson 社における検知日
2026 年 11 月 3 日

●最初の不正アクセス発生日
2026 年 10 月 22 日

3) 不正アクセスの原因

第三者により、Ericom Shield Cloud をホストしているクラウドインフラを経由してシステム侵害があり、Ericom Shield Cloud の各テナントの管理者情報が奪取されました。

4) Ericsson 社における検知と対応

●事象の検知
2026 年 11 月 3 日

●調査開始
2026 年 11 月 3 日

詳細調査については、Ericsson 社内外のフォレンジック専門機関が行っております。
既存の脅威監視ツールで不審な活動が検知されなかった理由についても、
並行して調査中となります。

●封じ込め対応
2026 年 11 月 8 日

後述の封じ込め対応により、第三者によるアクセスは遮断されております。
クラウドインフラやご契約の Ericom Shield Cloud の各テナントへの再アクセスの
可能性はございません。

5) 漏洩した可能性がある情報

●クラウドインフラ
・管理者情報
・Ericom Shield Cloud のご利用に必要なルート証明書と秘密鍵

●Ericom Shield Cloud の各テナント
・管理者情報
・設定情報
・S3 や Splunk 連携用トークンや API キー(ご使用されている場合)
・第三者が不正アクセスした日から最大過去 30 日分の各テナントのログ
(2026 年 10 月 22 日から起算し、最大で 2026 年 9 月 22 日以降のログ)
－ユーザーがアクセスした Web サイトのドメインの URL と日時。
※Cookie、および渡されたデータ(クエリ文字)は含まれません。
－ダウンロードしたファイルのファイル名。
※実際のファイル自体は含まれません。
－Data Loss Prevention オプションをご契約いただいている場合、
ブロックされた条件。
※実際のデータ自体は含まれません。

6) 漏洩した情報の影響

●管理者情報が漏洩したことによる影響
第三者に、各テナントの設定情報やログが閲覧された可能性があります。
また、S3 や Splunk 連携用トークン、API キーをご利用の場合は、連携先システムへの
不正データの送信や、管理者同等の操作が行われた可能性が考えられます。

※後述の封じ込め対応により、第三者によるアクセスは遮断されております。
クラウドインフラやご契約の Ericom Shield Cloud の各テナントへの再アクセスの
可能性はございません。
S3 や Splunk へのログ出力を実施されている場合は、各テナントにて設定を変更いただく
必要がございます。

●ログが漏洩したことによる影響
第三者に、不正アクセスした日から最大過去 30 日分のお客様の Web サイトへの
アクセスログが閲覧された可能性があります。

●ルート証明書と秘密鍵が漏洩したことによる影響
万が一、第三者がお客様のネットワーク通信を強制的に別の場所へリダイレクトする手段を
持っていた場合、正規の Ericom Shield Cloud サービスを装って通信を傍受するリスクが
あります。

※旧ルート証明書の削除を行うことで、当リスクを完全に排除することが可能です。

7) Ericsson 社にて対応済みの内容

封じ込め対応として、以下の対応が完了しております。

●対応済みの内容
・クラウドインフラの管理者情報の変更
・Ericom Shield Cloud の各テナントの管理者情報の変更
・新しいルート証明書を使用して Ericom Shield Cloud を使用する構成への変更

不正アクセス対策として、以下の対応を実施済みとなります。

●対応済みの内容
・追加のログ取得、およびモニタリング体制の導入
・クラウドインフラのアクセスに対する Just-In-Time 認証の導入

8) お客様へご協力のお願い

安全にご利用いただくために、現時点までにお願いさせていただいている内容と、追加のお願い内容について記載させていただきます。

●現時点までにお願いさせていただいている内容
- ・クライアント PC や中継機器にインストールいただいているルート証明書の入れ替え
- ・旧ルート証明書の削除
- ・S3 や Splunk 連携用トークンや API キーの変更(ご使用されている場合)

●追加のお願い
- ・お客様がご使用されているテナントのアクセスログの確認
  第三者による不正なアクセスや設定変更が行われていないか。

- ・不正なアクセスや設定変更があったか確認する方法
  テナントにログオンし[監査]-[全て]にて確認が可能です。
  詳細については、弊社サポートセンターまでお問い合わせください。

9) 今後の対応について

原因究明と第三者の特定について、Ericsson 社内外のフォレンジック専門機関にて詳細調査が行われております。
Ericsson 社からは、分析対象のログが膨大であるため、今後数週間調査に時間がかかると想定されると連絡を受けております。

弊社から Ericsson 社へ、不正アクセスが発生してから検知できるまで時間を要したこと、検知してから封じ込め対応に時間を要したこと、各対応に関するより詳細な日時、詳細な調査結果の情報について継続して報告を提出するよう求めております。

確認できた内容について、ご希望のお客様へは Ericsson 社から直接ご連絡させていただきます。
また、弊社からは日本語で日本のお客様への報告書をご提出させていただきます。

以上