2026.08.31　CSM-005
株式会社シーエスエム
代表取締役　島﨑　淳

【重要】弊社ネットワークへの不正アクセスに関する最終結果報告

お客様各位
平素は格別のお引き立てを賜り、誠にありがとうございます。
この度、弊社のネットワーク環境に設置しておりますセキュリティ機器（FortiGate）に対して、外部の第三者による不正アクセスが行われた事案につきまして、専門調査会社（デジタルデータソリューション社）による調査が完了いたしましたので、最終的な調査結果をご報告申し上げます。

お客様ならびに関係者の皆様には、本件により多大なるご心配とご不安をおかけいたしましたこと、改めまして深くお詫び申し上げます。

専門調査会社による調査の結果、FortiGate に対する不正アクセスの事実は確認されましたが、弊社の社内ネットワーク上のサーバおよび端末への侵入、不審なプログラムの実行、マルウェア感染、ならびにお客様情報その他の情報資産の漏洩、流出を示す事実は確認されませんでした。

以下、調査結果および対応内容についてご報告いたします。

1. 事象の概要と発覚の経緯

令和 8 年 7 月 13 日、群馬県警より、FortiBleed において弊社 IP アドレスの存在が確認された旨のご連絡をいただき、確認および連携のご要請を受けました。これを受け、弊社より機器の保守委託先ベンダーに対して調査・確認を依頼したところ、7 月 16 日に FortiGate 上に意図しない管理者アカウントが存在していた事実がベンダーにより確認され、発覚いたしました。

2. 不正アクセスの原因と弊社の管理体制について

本件の不正アクセスは、FortiGate のプログラム上の脆弱性を第三者に悪用されたことが原因であることが判明しております。
当該機器の運用・保守および管理者権限の管理等につきましては、専門の保守ベンダーへ全面的に業務を委託しておりました。
セキュリティの仕様および運用体制上、弊社側からは当該機器の管理者アカウントの新規作成や権限変更といった操作は行えない状態であり、今回確認された「意図しない管理者アカウントの作成」は、弊社内部の操作や人為的な設定ミスによるものではないことを確認しております。

3. 専門調査会社による最終調査結果

事象発覚後、外部の専門調査会社を通じてフォレンジック調査およびダークウェブ調査を実施いたしました。

（1）FortiGate 配下の端末・サーバのフォレンジック調査【完了】

① ファストフォレンジック調査

FortiGate 配下の端末およびサーバを対象として、ファストフォレンジック調査を実施いたしました。
その結果、不正な通信、マルウェア感染や不正なコマンドの実行を示す痕跡は確認されませんでした。

② ディープフォレンジック調査

メインサーバを対象として、ディープフォレンジック調査を実施いたしました。
その結果、不正な通信、マルウェア感染や不正なコマンドの実行を示す痕跡は確認されませんでした。

(2) ダークウェブ調査【完了】

ダークウェブ調査を実施した結果、本インシデントに起因する情報の漏洩・公開は確認されませんでした。
※ダークウェブ調査は 2027 年 6 月まで継続的に行います。

(3) 総合的な調査結果

各調査の結果を総合的に確認した結果、今回確認された不正アクセスは FortiGate へのアクセスにとどまっており、FortiGate 配下の社内ネットワークへの侵入、お客様情報を含むデータへの不正アクセスや持ち出し等を示す痕跡は確認されませんでした。
以上のことから、今回実施した調査の範囲において、お客様情報その他の情報資産の漏洩・流出等を示す事象は確認されませんでした。

4. 実施済みの対応

セキュリティレベルの向上および再発防止のため、FortiGate によるネットワーク境界防御から、グローバル IP アドレスを変更するとともに、サイバー攻撃・不正通信対策、クラウド連携型ネットワーク防御を組み合わせた多層防御へ強化しております。

セキュリティ観点	従来構成	セキュリティ強化後の構成	セキュリティ上の強化
グローバル IP アドレス	既存のグローバル IP アドレス	グローバル IP アドレスを変更	外部から認識される接続先を変更し、既存 IP アドレスを対象とした攻撃リスクの低減
サイバー攻撃・不正通信対策	FortiGate による通信制御が中心	海外からの通信を中心に不要なパケットは破棄するサイバー攻撃・不正通信対策の導入	外部からの攻撃や悪性通信、情報流出につながる通信等への対策を強化
ネットワーク境界防御	FortiGate による境界防御	クラウド連携型ネットワーク防御の導入	ネットワーク境界における不正アクセスや悪意のある通信への防御を強化

【総括】

今回の事案につきましては、専門調査会社によるフォレンジック調査およびダークウェブ調査を含む必要な調査を完了し、お客様情報その他の情報資産の漏洩・流出等を示す事象は確認されませんでした。
これらの結果を受け、本件に起因する影響や追加の対応を要する事象は生じていないものと判断しております。
また、調査結果を踏まえ、グローバル IP アドレスの変更、サイバー攻撃・不正通信対策、クラウド連携ネットワーク防御等、セキュリティ対策および業務環境の見直し・強化を実施しております。
これらの調査および対策を完了したことから、現在、業務継続に支障となるセキュリティ上の事象は確認されておらず、強化したセキュリティ環境のもと、通常どおり安定した業務およびサービス提供を継続しております。

今後も、今回の事案を教訓として、専門のベンダーから継続的にアドバイスを受けながら、情報セキュリティ対策および監視体制の継続的な見直し・強化に取り組み、お客様に安心してお取引を継続いただける安全性の高い業務環境の維持・向上に努めてまいります。
この度は、お客様ならびに関係者の皆様にご心配とご不安をおかけしましたこと、改めまして深くお詫び申し上げます。
今後もお客様からの信頼にお応えできるよう、情報セキュリティのさらなる強化と安定したサービス提供に努めてまいりますので、何卒ご理解賜りますようお願い申し上げます。

以上