2022 年 5 月 16 日

各　位

株式会社シーエックスアール
代表取締役　小早川 孝

弊社サーバーへの不正アクセスについて（第四報）

弊社は、2022 年 3 月 1 日、弊社および弊社の子会社が使用しております業務用サーバーの一部に不正アクセス（以下、「本不正アクセス」）を受けたことを公表いたしました。

この度、外部の専門企業の協力のもと進めてまいりました本不正アクセスの調査が完了しましたので調査結果及び再発防止策についてご報告いたします。

お客様を始め多くのご関係先にご心配とご迷惑おかけいたしましたことを、深くお詫び申し上げます。また、お取引先をはじめ関係各位のご支援には深く感謝申し上げます。

１．対応の経緯

2022/3/1	システム管理委託先よりサーバー暗号化の報告を受け復旧作業に着手
2022/3/2	広島県警サイバー犯罪対策課に通報
2022/3/3	HP へランサムウェア被害に関する第一報を掲載
2022/3/4	JPCERT/CC（以下：専門機関）へ通報
2022/3/7	サーバー復旧対応完了、HP へ復旧完了の第二報を掲載
2022/3/11	警察へ被害サーバデータ提出 セキュリティインシデント調査会社へ調査依頼
2022/3/15	HP へ第三報掲載
2022/3/16	フォレンジック調査開始
2022/3/18	システム管理委託先へ本件に関する質問状を提出
2022/3/25	関係者による情報共有会議を開催
2022/4/5	システム管理委託先より回答書を受領
2022/4/6	システム管理委託先と再発防止策について協議
2022/4/30	セキュリティインシデント調査会社より調査報告書を受領

２．被害の原因及び調査結果

2022 年 3 月 1 日に弊社システム管理委託先のデータセンター内にある VPN 機器に対して不正アクセスが行われ、ネットワークへの侵入を許したものと判明しております。また、当該機器に関しては、機器設置当初からセキュリティアップデートが適切に実施されておらず、2021 年 7 月時点で、当該機器の認証情報の流出が発生していたことが判

明しております。

侵入の原因となった当該機器と、被害にあったサーバー機器との間では運用の利便性の観点から、共通の認証情報により利用できることが判明しており、流出した認証情報により被害が拡大する結果となりました。なお、現時点では当該機器の脆弱性への対策は適切に実施されております。

攻撃者により暗号化が行われたファイルは、攻撃者がアクセス可能な状態にあったことから、攻撃者に流出している可能性は否定できませんが、フォレンジック調査により、攻撃者に情報が窃取されたことを示す直接の証拠は確認されておりません。攻撃発生以後、警察や専門機関、セキュリティインシデント調査会社にダークウェブ上の監視を依頼しておりましたが、データ流出等のリスク事象は確認されておりません。

3．再発防止策

本不正アクセスを踏まえ、被害機器につきましては、セキュリティソフトによるフルスキャンを実施後、セキュリティパッチを最新のものに更新しております。また、バックアップデータからの復旧により現在は通常稼働できる状態に移行しております。

本不正アクセスの原因となりましたネットワーク外からの VPN 接続については、現在利用を停止しており、二次被害が発生しないよう取り組んでおります。また、流出が確認された認証情報についてもすでに変更を実施しております。

現在検討している事項といたしましては、現状のシステム運用体制の抜本的な見直し（ネットワーク全体の設計・VPN 接続・セキュリティ強化等）を進めてまいります。あわせて、弊社社員に対してもセキュリティ教育を実施し、システムインシデント発生リスクの低減に努めてまいります。

4．情報流出懸念への対応

現在、警察及び専門機関に継続的な監視を依頼しておりますが、より精度の高い監視を継続するために、セキュリティインシデント調査会社にもダークウェブ調査を依頼し、継続的に監視を行ってまいります。これらの調査により情報の漏洩が確認された場合には、関係各所へ速やかに連絡を行い、対応を行ってまいります。

皆様には、多大なるご心配・ご迷惑をおかけしておりますことを改めてお詫び申し上げます。弊社では、今回の事態を真摯に受け止め、全社一丸となって再発防止に取り組んでまいりますので、何卒ご理解とご協力を賜りますようお願い申し上げます。

以上

【本件に対する問い合わせ先】
情報セキュリティ本部（管理部）
TEL：0823-22-4100