2025 年 9 月 10 日

当社サーバーにおける第三者からの不正アクセスの発生について（第二報）

当社は、2025 年 8 月 9 日に当社の一部サーバーにおいて、ファイルが暗号化されるランサムウェア被害が発生したことを公表いたしました。

本件につきましては、外部専門家と連携して影響の範囲等の調査と復旧への対応を進めておりましたが、この度、本件に関わる調査が完了し、最終報告を受領しました。

お取引先様、関係先の皆様には多大なるご心配とご迷惑をおかけすることになり、深くお詫び申し上げるとともに、当該調査結果および再発防止に向けた取り組みについて、ご報告いたします。

１．概　要

2025 年 8 月　9 日	ランサムウェアの被害を確認、すべてのネットワークを遮断 外部専門機関に協力を依頼し、当該サーバーの保全を実施 福岡県警察本部サイバー犯罪対策課へ被害報告 個人情報保護委員会へ報告
2025 年 8 月 10 日	外部専門機関にてフォレンジック調査を開始
2025 年 8 月 18 日	フォレンジック解析結果（速報）の報告
2025 年 9 月 2 日	フォレンジック解析調査結果の最終報告 ※調査結果は後述のとおり 再発防止策を実施したうえで個人情報保護委員会には 最終報告を行う予定です。

２．外部専門機関による調査結果

（１）侵入経路および攻撃活動

攻撃者は社外よりネットワーク経由でコンピュータに接続し、そのコンピュータにリモートで操作して不正アクセスを行い、複数の社内サーバーに接続。

最終的にランサムウェアを実行してファイルを暗号化するとともにサーバー内に脅迫文を残しました。

（２）ランサムウェアの種類

解析の結果、不正プログラムは、CrySiS/Dharma ランサムウェアの亜種であることを確認しました。脅迫文にはリークサイトに関する記述はなく、現在のところ、本ランサムウェアに関連するリークサイトは発見されておりません。

なお、本プログラムの特徴は以下のとおりです。

・本不正プログラム自身には永続性の機能はない。
・本不正プログラム自身には自身を感染コンピュータ以外のコンピュータに拡散させる機能はない。
・本プログラム自身には外部に通信する機能はない。
・本プログラム自身には情報漏洩機能および外部に送信する機能はない。
・本不正プログラムには暗号化以外のファイル改ざん機能はない。

（3）漏洩した可能性がある情報

2025 年 9 月 9 日現在、当社サーバーから漏洩した可能性がある情報の公開は確認されておりません。また解析対象となったサーバーやコンピュータからは外部への明確な情報漏洩の痕跡はありませんでした。
今後、情報漏洩が確認された場合は速やかにご報告いたします。

3．再発防止策

（1）ネットワークセキュリティ対策の強化

・ネットワーク接続時にすべてのユーザーアカウントに対して多要素認証を適用する。
・ネットワーク接続におけるログを適切に取得・保持出来るよう設定を見直す。
・サーバーおよびパソコン端末に保存されている認証情報(パスワード等) を変更する。
・パソコン・サーバーを問わず、エンドポイントセキュリティの対策を強化する。
（EPP、EDR 製品の導入、SOC＜セキュリティオペレーションセンター＞の検討）
・サプライチェーンに属する関連企業や委託先のセキュリティ管理体制を強化する。

（2）脆弱性管理の徹底

・管理者アカウントのパスワードポリシーの強化
・パソコン、サーバーOS、ネットワーク機器の最新アップデートへの更新と管理徹底

（3）ネットワークセキュリティに関する社員教育の再徹底

以上、本件に関する状況等について、ご報告いたします。
お取引先様、関係先の皆様にはご心配とご迷惑をおかけしておりますことを重ねてお詫び申し上げますとともに、この度の事態を真摯に受け止め、セキュリティと監視体制の更なる強化を実施し、再発防止に努めてまいります。

株式会社レイメイ藤井
代表取締役　藤井　章生

本件に関するお問合せ先
総務部　092-262-2280 または 092-262-2283　＜村上・永松・西本＞