2024年5月31日

各　　位

会　社　名　　株式会社ほくやく・竹山ホールディングス
代　表　者　　代表取締役社長　　眞　鍋　　雅　信
（コード番号 3055　札証）
問 合 せ 先　　経営統括本部企画広報部長　　樋　栄　邦　直
TEL（011）611－1010

ランサムウェア被害に関する調査結果のご報告

本年２月５日にお知らせいたしましたとおり、弊社は本年２月３日未明に弊社サーバ等に対する第三者からの不正アクセスによるランサムウェア攻撃の被害を受けました。これまで、取引先様をはじめ、多くの関係者の皆様にご迷惑とご心配をおかけいたしましたことを深くお詫び申し上げます。

本件では、発覚後速やかに内閣府個人情報保護委員会への報告ならびに北海道警察への被害申告および相談を行うとともに、二次被害の防止対策、復旧作業や分析調査等の実施、また外部専門機関の助言のもと、被害状況、原因等の調査を進めてまいりました。このたび調査結果がまとまりましたので下記のとおりお知らせ申し上げます。

記

1. 被害の概要および原因

攻撃者は、弊社のSIMカード搭載のノートパソコン（以下「ノートPC」といいます。）に対して、リモートデスクトップ接続[1]による不正アクセスによって攻撃を開始し、弊社の業務用サーバ等に不正にアクセスしてランサムウェア「Enmity」を実行し、データの暗号化を行ったものと考えられます。暗号化されたデータは復号されていませんが、別に保管していたデータ等により、事業活動の目的に応じた適正利用が可能となっております。

アクセスに使用されたIDおよびパスワードは、ドメイン管理者の正規のもので、この際に使用されたIDおよびパスワードの漏洩または入手経路につきましては現在も調査中です。

なお、弊社グループ会社も本件事案に関連し同様の被害を受けましたが、本件調査において、㈱そえる、㈱モルス、㈱ノバメディカルにおいては、被害がなかったことが判明しております。

[1] 「リモートデスクトップ接続」：インターネット経由で離れた場所からアクセスし遠隔操作すること

2. データの漏洩等がなかったとの判断について

弊社では、これまで外部専門機関によるフォレンジック調査[2]を行いましたが、本件の暗号化の対象となったデータの漏洩等の痕跡は確認されませんでした。

しかしながら、不正アクセスを受けたファイルが漏洩した可能性を想定し、ダークウェブ調査[3]を併せて行いましたが、本件に係る漏洩データの検出はなく、これまで二次被害の情報もありません。

以上の調査結果から、弊社は、本件不正アクセス被害において、個人情報等のデータの漏洩等はなかったものと判断いたします。

3. 再発防止策に向けた取組

（1）より強固なセキュリティ対策ソフトの導入
（2）OS、アプリケーション、サーバ等に関する脆弱性管理の徹底
（3）多要素認証の導入など各種パスワード管理の強化
（4）従業員教育の強化とトレーニングの継続実施
（5）セキュリティポリシーの見直しと周知徹底
（6）バックアップシステムの改善

以上に留まることなく、再発防止策は、外部専門機関の意見を踏まえ、社内のサイバーセキュリティ対策委員会によって、常に最新情勢に応じた検討を行い実行してまいります。

4. お問い合わせ窓口

本件に関するお問い合わせ先は、以下のとおりです。
（受付時間：平日 9：00～17：00）

【メディア以外の方】
株式会社ほくやく・竹山ホールディングス　お問い合わせ窓口（担当：リスク管理部　林）
TEL　0120-22-6051（フリーダイヤル）、011-631-5143

【メディアの方】
株式会社ほくやく・竹山ホールディングス　企画広報部（担当：企画広報部　樋栄（ひえ））
TEL　011-611-1010

---

[2] 「フォレンジック調査」：不正アクセス等の原因や被害範囲等を明らかにするために、デジタル機器から証拠となるデータを抽出し、分析すること

[3] 「ダークウェブ調査」：匿名性・非公開性が高く、通常のインターネット検索では表示・発見されない Web サイト等に対する調査のこと