個人情報取り扱いに関する事故等のご報告

掲題に関し以下ご報告申し上げます。

１）発生日時

2021 年 9 月 25 日(土)午前 7 時 26 分頃

２）事故発生内容

外部からの不正アクセスにより当社サーバー（以降：感染サーバー）が攻撃されたことが確認。このﾗﾝｻﾑｳｪｱ攻撃により、感染サーバー内に保管されていた業務関連データファイルの一部が不正圧縮暗号化され復元出来ないことが判明した。更には感染サーバー管理 PC のデスクトップ上に身代金要求の英文を確認。
仮想サーバーを含め 10 台の感染サーバー内の 7 ファイルが圧縮暗号化された。

３）対応状況

当該感染サーバーおよびネットワーククライアントパソコンの LAN ケーブルの切断。
感染圧縮ファイルの拡張子、動作を調査し、ﾗﾝｻﾑｪｱ化した Recuva.exe（ﾚｷｭｰﾊﾞ.ｴｸﾞｾﾞ）を削除停止させ、その後感染サーバー内での感染ファイルの拡散停止確認。
また業務クライアント PC 全台をウィルスソフト(ESET ENDPOINT ANTIVIRUS)で再スキャンチェックしクライアント PC が感染されてないことと同不正圧縮ファイルが残ってないことを確認した。
同日 11:00 頃に感染サーバー内で発見したﾗﾝｻﾑｳｪｱと感染ファイルが動作していないか再度確認し当社内サーバー室から遮断されたサーバー内保管確認した。
現時点では、お客様の業務関連データがインターネット上に公開されるなどの具体的な情報漏洩の事実は確認されていません。今後とも情報漏洩の事実確認のため、専門家の助言の下、インターネット上の情報などについて調査・監視を継続する。
現在、弊社の通常業務については、データの復元に努めるとともに、セキュリティ対策の強化を進め安全を確保した上で業務を継続している。

４）発生原因

今回の事案を誘発した原因として、「当社のネットワークには、管理されたパソコンや USB 機器以外は接続出来ない」という基本的なルールが徹底されておらず管理外機器の接続やテレワーク等で増えた VPN 機器等のリモートアクセス環境管理の不備を突き侵入したと思われる。またネットワークにおいてもウイルス攻撃を許したシステム的な予防対策が不十分であったこともウイルス感染の要因。外部と接続されないはずのサーバー内システムが外部と接続された状況となり、サーバー内への侵入・コンピューターウイルスへの感染に至った可能性が高いと推測する。

５）防止策

不正アクセス、ウイルス攻撃を二度と発生させないため、ガバナンスの強化とシステム的対応の観点から再発防止策を策定する。

＜ガバナンスの強化＞

① 情報セキュリティ組織の見直し、
② 緊急時における対応の見直し、
③ 社員研修・訓練、
④ 運用管理規程と運用管理体制の見直し

＜システム的対応＞

システム開発全体への技術的対策の強化

① 短期的対策

全社全グループ内、パソコン・USB 機器のセキュリティ更新
機器等の管理システムへの完全登録管理
リモートパソコン USB 使用のルール見直し

② 中長期的対策

サポート終了ＯＳの残存調査
ウイルス対策製品の一元化、最新化、最新情報入手の方法見直し
インターネットゲートに URL や通過ファイルを制御する機器の導入
Cloud 共有ファイル導入
インターネットネットワークの管理強化（SKYSEE）

個人情報管理体制を整えプライバシーマークを取得している弊社として、問題の発生を深く反省し再発防止に努めていく所存です。

2021 年 12 月 15 日
オビサン株式会社
代表取締役社長
小嶋寛之