2025年7月17日
ユニデンホールディングス株式会社

当社におけるランサムウェア被害についてのご報告とご説明

平素は格別のご高配を賜り、誠にありがとうございます。
このたび、当社のサーバに保管されていたデータが、外部からの不正アクセスにより、ランサムウェアに感染し暗号化されるという事案が発生いたしましたことをご報告申し上げます。

当社では、発覚直後より社内の専門部署及び外部の専門機関と連携し、速やかに原因調査と影響範囲の特定に努めてまいりました。その結果、暗号化されたデータの中に、当社がお預かりしているお客様及びお取引先様の個人情報並びに当社の一部従業員の個人情報が含まれていたことを確認しております。
しかしながら、当該情報はいずれも、当社が従来より運用しているNotesシステムにより複雑かつ多層的な暗号化処理が施された状態で保管されており、専門家の見解としても、第三者による解読や閲覧は困難であると確認されております。
さらに、現在までの調査においては、以下のような事実は一切確認されておりません。
・当該情報が外部に流出したことを示す事実
・攻撃者による情報の公開
・第三者からの金銭的要求や脅迫行為

これらの状況を総合的に勘案し、現時点において情報が外部に流出した可能性は低く、また、漏えいによる二次的な被害のおそれも限定的であると判断しております。
お客様、お取引先様をはじめ関係者の皆様におかれましては、本件によりご不安・ご心配をおかけしましたことを、深くお詫び申し上げます。
しかしながら、上記のとおり当社では速やかかつ冷静に対応を進めており、現時点で確認されている情報に基づく限りにおいて、実害が発生する可能性は低い状況にあるとご理解いただければ幸いです。
当社は今後も、再発防止に向けた取り組みを一層強化するとともに、監視体制の強化や社内教育の徹底など、情報セキュリティ体制全体の強化に努めてまいります。万一、新たに確認すべき事象が判明した場合には、速やかに関係者の皆様にご報告させていただきます。

今回のご報告に至った経緯について
なお、本件に関するご報告がこのタイミングとなりました理由につきましても、以下のとおりご説明申し上げます。
当社は2024年8月29日に本件発生後、個人情報保護委員会に対し、同年9月2日に速報を提出し、同年10月25日に確報を行いました。その後も、当該データが被害前において「高度な暗号化その他の個人の権利利益を保護するために必要な措置」（個人情報の保護に関する法律施行規則第7条第1号かっこ書き）を満たしていたか否かについて、同委員会との間で継続して検討を進めてまいりました。そしてこのたび、個人情報保護委員会との検討が終了したことを受け、あらためて本件に関する調査結果及び当社の見解を、関係者の皆様にご報告させていただくに至った次第でございます。ご不明点やご懸念がございましたら、何なりとお問い合わせいただければと存じます。今後とも、何卒ご理解とご協力を賜りますよう、よろしくお願い申し上げます。

記

1. 発生した事象の概要及び原因
・2024 年 8 月 29 日: 当社は、当社のサーバがランサムウェアに感染していることを感知し、当該サーバ内に保管されていたデータが暗号化されていることを確認したため、同日中に、関連するサーバをネットワークから切り離す等の緊急措置を講じました。
・2024 年 8 月 30 日: 当社は、外部専門家の協力のもと被害の原因及び影響範囲等の調査（以下「本件調査」といいます。）を開始しました。
・2024 年 9 月 13 日: 本件調査の結果、以下のとおり、外部からの侵入によりランサムウェア被害が発生したことが判明しました。
- 当社のオーストラリア拠点における当社のコンピュータに存在したセキュリティホールより外部からの侵入があり(2024 年 6 月 17 日)、オーストラリア拠点における当社のネットワーク（日本拠点における当社のネットワークと VPN を通じて相互に接続されていた。）において、VPN アカウントの侵害を受けた。
- ランサムウェアが当社のオーストラリア拠点と日本拠点間の VPN を経由して、日本拠点へ伝播し、当該両拠点において、ドメイン管理者アカウントによって、ランサムウェアが実行され、当社の IT 環境内のバックアップシステムを含むサーバの大部分及びコンピュータの一部が暗号化された（2024 年 8 月 28 日及び同月 29 日)。

2. 影響を受けた情報の範囲及び二次被害のおそれ
本件調査の結果、暗号化されたデータには、当社がお客様及びお取引先様よりお預かりした個人情報並びに当社の一部従業員の個人情報が含まれていることを確認いたしました。影響を受けた個人情報の詳細は、以下のとおりです。
・製品の交換・修理などを希望されたお客様の氏名、住所、電話番号、ファックス番号
・お取引先様のご担当者様の氏名、所属会社の電話番号及びメールアドレス
・在職中及び退職済の一部従業員の氏名、生年月日、性別、住所、電話番号、メールアドレス　計　約 4000 件
しかしながら、上述のとおり、当該個人情報が漏えいした可能性及び漏えいによる二次被害のおそれは低いものと判断しております。

3. 再発防止策の実施
上記「１．発生した事象の概要及び原因」記載のとおり、関連するサーバをネットワークから切り離した等のほか、現時点までに、以下の再発防止策を実施しております。
・各種パスワードの変更及び VPN 等に対する二要素認証パスワードの設定
・各セグメントにおけるアクセス制限ポリシーの見直し及び設定
・保守切れのファイヤーウォールの切り離し
・振る舞い検知プログラムの入れ替え（当該プログラムを利用できないコンピュータはネットワーク接続不可へと変更）
・サーバからの in/out のアクセスの制御等
・アカウントへの特権付与プロセスの明確化及び非特権アカウントに付与した特権の削除
・エンドポイント端末のセキュリティ・組織によるコントロールの強化
・パスワード複雑さ要件の変更
・ログ記録ポリシー及びバックアップの増強

4. 今後の対応
今回、当該情報の対象となるお客様には当社より郵便・電子メール等にて個別にご連絡させていただきます。なお、個別のご連絡が困難なお客様については、本公表をもってご連絡に代えさせていただきます。

5. お問い合わせ窓口

本件に関するお客様のお問い合わせ窓口を以下の通り設置いたしました。ご不明点やご不安な点がございましたら、以下のお問い合わせ窓口までご連絡いただきますようお願い申し上げます。

当社から個人のお客様へご連絡し個人情報をお尋ねすることは一切ございません。不審な連絡を受けた場合は対応せず、直ちに当社までご連絡ください。

本件に関するお問い合わせ窓口：security@uniden.co.jp

以　上