2024 年 10 月 3 日

お取引先様 各位

KISCO 株式会社
代表取締役社長 岸本 剛一

第三者によるランサムウェア攻撃被害とその対応について

8 月 24 日に発生しました弊社におけるランサムウェア攻撃による被害とその対応状況についてお知らせいたします。お取引先様をはじめ、多くの関係者の皆様にご迷惑とご心配をおかけしたことを重ねてお詫び申し上げます。

本件につきましては、被害の拡大を防ぐため、被害発生後直ちに社内システム、サーバー、パソコン等をネットワークから切り離し、停止措置を行いました。その後、業務への影響を最小限に抑えるために、新たにパソコンを調達するとともに、既存ネットワークとは別のネットワークを構築する等の対応を進める一方で、外部セキュリティ専門家による被害状況、原因調査を行いました。本ご案内では、調査結果ならびに外部専門家の助言をもとにした、現時点での弊社の対応状況を報告申し上げます。

記

1. 概況

第三者が弊社社内の複数のサーバー等に対して、8 月 24 日未明にランサムウェアによるファイルの暗号化を実行し、ファイルが判読不能になったほか、サーバーシステムが停止するに至りました。

その後、外部専門家の調査の結果、第三者による侵害がないと判断された主要なシステムについては、使用を再開しております。

また、外部専門家の調査、調査結果に基づく IT 施策提言への対応、及び、外部専門家によるグローバルなサーバー・パソコンの継続的な監視で新たな攻撃等が検出されていない状況などを踏まえ、外部専門家から本インシデントは終息した旨のコメントを受領しております。

2.原因と対応状況

1)原因

本件の原因は、海外拠点社員向けにリモートアクセスを提供していたファイアーウォールへ攻撃者による侵害を受けたことが起点と判断しております。当該ファイアー

ウォールのアクセスポリシーが変更された後、社内システムへの侵入、システムの管理者アカウントの ID 及びパスワードの盗取が行われ、複数の業務システムにアクセスされたものと考えます。

2)対応状況

初動対応として、侵害を受けた可能性のある全てのサーバー、及びパソコンをネットワークから切断するとともに、二次被害拡大防止のためにインターネット回線の切断を行いました。

現在は外部専門家の調査結果及び助言を踏まえ、新たにより強固なセキュリティツール（XDR）を、国内外グループ会社を含めて導入し、24 時間/365 日の外部専門会社による監視下のもと運用を再開しております。

メールシステムについては、新たな方式での送受信をご案内させて頂きましたお取引先様から、メールによる連絡を再開しています。

新たなネットワークの構築にあたっては、外部専門家の指導のもとセキュリティを強化いたしました。

3.再発防止策

KISCO およびグループ子会社のサーバー、パソコン等のエンドポイントに対して EPP（Endpoint Protection Platform）ツールの見直しと XDR ツール導入を行い、これらと連携する 24 時間/365 日の外部監視サービスを受けることで、インシデント発生の予防、検知、対応を一元的かつ早期に行えるように致します。

また、各システムへのアクセスに対して、新たにグローバルに SASE(Secure Access Service Edge)ネットワークの構築、多要素認証の導入などによるセキュリティ強化を実施致します。

ファイルの保管についても、ストレージ環境、保管ルールの見直しを行うほか、重要度の高いデータについては暗号化する方針です。

【本件に関するお問い合わせ先】

KISCO 株式会社 経営統括 Div. 社長室長 家村 英二
TEL ：03-3663-0258
E-mail ：toiawase@kisco-net.com

以上