令和 2 年 11 月 18 日

各　位

鉄建建設株式会社

サイバー攻撃による被害と復旧状況について（第三報）

このたびは弊社システムの長期にわたる障害の継続により、お客さまや関係者の皆さまに大変なご迷惑とご心配をおかけしており、誠に申し訳ございません。また、被害が大きく復旧に長時間を要したことについてお詫び申し上げます。

9 月 23 日午前より発生しているシステム障害について、被害が拡大した理由等がシステム専門会社の協力を得て明らかとなりました。また、不通となっておりました当社ドメインのメールが 11 月 18 日（水）10 時より順次復旧いたしますのでお客さまや関係者の皆さまにご報告いたします。

調査により、システム障害発生前の 9 月 17 日（木）社員に届いた取引先を装うメールに、マルウェアを含むファイルが添付されていたことが判明しました。社員がこれを開封し使用していた PC がウイルスに感染したことが、当該 PC のログ解析及び社員ヒアリング結果より明らかとなりました。また、攻撃者は当該 PC を含め合計 3 台の PC に次々とリモートアクセスを行い、弊社が保有する認証サーバへ辿りつき管理者権限を奪い取るに至ったとシステム専門会社より報告を受けました。

その後 9 月 23 日（水）早朝、再び攻撃者は弊社認証サーバ等サーバ群に不正アクセスを行い、各種サーバの暗号化及び社員使用 PC のアンチウイルスソフトの削除プログラムを実行し、被害が全社に拡大したことが判明いたしました。データの窃取量や具体的に窃取されたデータの内容については、調査を継続しておりますが、特定には至っておりません。新たな報告事項が発生した場合は弊社ウェブサイトを通じてお知らせいたします。

復旧状況について、暗号化を受けたサーバ群（約 70 台）についてはクリーンナップ作業を終え、順次バックアップ等をもとに復旧作業が進んでおります。社員使用 PC においては被害状況をレベル分けし、被害レベルの低い PC ではウイルス駆除を行い、被害レベルの高い PC ではクリーンインストールを実施した上で、弊社ネットワーク内で使用を再開しております。また、メールサーバが 11 月 18 日 10 時より順次復旧し、お客さまや関係者の皆様と電子メールで連絡できる環境が整いました。

今後同様の事態を防ぐために、弊社ネットワーク上に通常とは異なるような通信や不審なデータの流れを検知する新たな機器の設置と、アンチウイルスソフトに各 PC の挙動を監視する新たな機能を付加いたしました。これによりパターンファイルによる既知ウイルスへの対応に加え、通信やデータの流れなどから未知のウイルスにまで対応が可能となります。また、メール利用再開前に全社員に今回の事象を踏まえた情報セキュリティに関する社員教育を実施いたしました。

長い期間お客さまや関係者の皆さまにご迷惑とご心配をおかけしていることをあらためてお詫び申し上げます。全システムの完全復旧まで、外部の専門家と協力し全社で対応に当たります。また、弊社ネットワークシステム全体を見直し、より高いセキュリティ機能を有する新たなシステムへの移行に向けた検討も開始したところです。今回の事案を教訓として、お客さまや関係者の皆さまと安心して取引できる環境を維持継続したいと考えております。

お問い合わせ先
鉄建建設株式会社　経営企画本部　広報部
03-3221-2297