

令和2年10月9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

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、応急復旧作業を最優先したため、システム障害発生から今回の報告まで時間を要したことを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、現在、システム専門会社の協力を得て、弊社情報システム部門を中心に復旧作業と原因の調査を全力で実施しております。しかし、完全な復旧にはもう少し時間を要する見込みであり、これまでに判明した事実と現在の状況をお客さまや関係者の皆さまにご報告いたします。

9月23日7時頃に社内システムの障害を検知いたしました。情報システム部門で社内ネットワークの状況を確認したところ、コンピュータウイルスによる感染の恐れがあったため、同日9時頃、全社員使用PCと社内ネットワークを切断する対応を取ると同時に、システム専門会社への連絡を行いました。

弊社ではサーバと社員使用の全PCにおいて、アンチウイルスソフトによる対策を実施しておりました。しかし、調査を進めると新しいタイプのランサムウェアによる被害と確認いたしました。

なお、今回の弊社の被害等について、所轄の警察への相談を行っています。

現在、インターネット回線とは完全に遮断した環境下で、システム専門会社による復旧作業と並行して、被害範囲および侵入経路の特定などの調査を行っています。具体的には暗号化されたサーバのログや不具合の認められる社員使用PCの解析などを進めております。

時系列

日時		内容
9月23日(水)	7時	社内システムへアクセスできないことを確認。
	9時	・ウイルス感染が疑われたため、全社員使用PCの切断指示。 ・復旧作業と原因調査を開始。
	10時	被害サーバ内に英文による攻撃者への連絡先URLの存在を確認。
9月24日(木)		・システム障害対策本部設置、対応を開始。 ・弊社ウェブサイトにてシステム障害について第一報を掲載。 ・攻撃者とは連絡を取らないことを意思決定。
9月27日(日)		データの一部が窃取されたことを、システム専門会社を通じて確認。
9月28日(月)		復旧対応、事業継続、広報対応など細分化して対応開始。

9月30日（水）	<ul style="list-style-type: none"> ・アンチウイルスソフトが削除された PC へのアンチウイルスソフト再インストール開始。 ・基幹システムサーバ復旧完了。
10月1日（木）	外部と安全に連絡をとるため、外部臨時メールシステム契約。
10月4日（日）	ファイルサーバ復旧完了。
10月9日（金）	弊社ウェブサイトにて被害と復旧状況を掲載。

現在判明している被害状況は、弊社保有サーバ約 70 台のうち、台数で約 95%が暗号化などの被害を受けております。加えて、社員使用 PC 約 3000 台のうち、アンチウイルスソフトがアンインストールされる被害が約 10%の PC において確認されています。また、被害を受けたサーバに記録されていたデータの一部が窃取され、特殊サイトに掲載されていることを、システム専門会社の調査を通じて確認いたしました。現在のところ、お客さまや関係者の皆さまに影響を及ぼす二次被害などは確認されておりません。引き続き新たな情報の掲載がないか継続的な監視を行っております。データの窃取について新たな事実が判明した際には、その都度ご報告いたします。

復旧作業について、業務継続に向け被害の少なかったサーバより順次復旧作業を進めています。すでに一部のサーバではバックアップによる復元を完了しています。一方、メールサーバの被害が大きく、復旧にはさらに時間を要する見込みとなっております。このため、今回、被害を受けたシステムとは別に外部の臨時メールシステムを契約し、お客さまや関係者の皆さまと安全に連絡を取れるよう、対応を進めております。ご不便をおかけしますが、何卒ご理解のほどよろしくお願いいたします。また、約 3000 台の社員使用 PC について、最新版のアンチウイルスソフトの再インストールやパターンファイルの更新作業を順次進めております。

一日も早くこれまで通りの企業活動へ回復すべく、外部の専門家と協力し全社で対応に当たっております。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。

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

以上