

2023年7月7日

お取引先各位

【状況報告】ランサムウェア被害の調査結果について

日本コンクリート工業株式会社
全社対策本部

今般のランサムウェア感染被害につきましては、皆様に多大なるご心配とご迷惑をおかけし、誠に申し訳ありません。

この影響による決算関連業務の遅延により、2023年6月29日開催の第92回定時株主総会で計算書類等の報告が出来ず、7月28日開催の継続会で報告する予定であり、有価証券報告書の提出も7月28日まで約1ヶ月延期いたしました。

本件被害発生以来、外部専門家による調査と復旧に向けた作業を行ってまいりましたが、調査結果が報告されたことから、現時点での状況をご説明いたします。

1. 調査結果概要

- ・ 調査機関 外部専門家（サイバーセキュリティー、ウィルス感染対応の専門業者）
- ・ 調査目的 感染原因経路調査、サーバー感染有無、クライアントPC影響確認等

(1)感染原因

- ・ 外部攻撃者によるファイアウォールVPN機能の既知の脆弱性を衝いた不正アクセス。
- ・ 不正アクセスは5月3日(水)から開始され、5月5日(金)深夜に本格化。
- ・ 攻撃者はネットワークに侵入後、パスワード総当たり攻撃で管理者パスワードを取得、情報資産にログインし順次ランサムウェアによる暗号化を展開。

(2)感染被害状況

- ・ 調査対象サーバー15台中11台が暗号化。
- ・ PCは100台中5台にアクセスを試みた形跡が認められたが、全台感染していないことを確認。
- ・ 暗号化されたファイルの復号（暗号の解除）は不可能（現時点で復号のためのキー情報が解明されていない）。

(3)データ漏洩

- ・ 侵害期間における大量のデータ外部流出の痕跡はなく、現時点で具体的な情報漏洩の事実は確認されていない。また、今回のランサムウェアは、様々なセキュリティーベンダーのレポートでデータ持出しをしないことが確認されている。
⇒当社としては現時点で情報漏洩は無いものと判断しております。

(4)再発防止策

- ・ ファイアウォールのセキュリティー強化
- ・ 全サーバーへのアンチウイルスソフトのインストール
- ・ セキュリティーポリシーの変更
- ・ ファイルサーバーのバックアップ方法の再検討
- ・ セキュリティー製品の導入

2. システム復旧について

(1) 基本対応方針

- ・ 業務システムの大部分が暗号化され復号不可能であることから、現行システムの完全復旧は困難と判断し、以前より計画していた新システムへの移行(2024年4月予定)を進める。
- ・ 新システム稼働までの間は、暫定的なデータ入力方法を構築することで感染を免れたシステムを継続利用し、現時点で再稼働している経理システムに繋げる。

(2) スケジュール概要

- ・ 経理システムの各事業所での利用再開 本社：6月1日、事業所：7月3日
- ・ 社内ネットワーク復旧 8月1日
- ・ 第1四半期(4～6月)データ入力作業 8～9月
- ・ 第1四半期決算作業 10～11月(予定)
- ・ 新システム稼働 2024年4月(予定)

※スケジュールについては現時点での計画であり、変更になる場合があります。

以 上