

2022年12月27日

サイバー攻撃被害によるシステム障害のお知らせ（第2報）

社会医療法人生長会

本年11月7日付でお知らせ（第1報）しました当法人の給食提供施設であるベルキッチンにおけるサイバー攻撃による障害発生につきまして、患者様をはじめご関係の皆さまには多大なご心配とご迷惑をお掛けしており、深くお詫び申し上げます。これまでに判明している事項を、以下の通りお知らせいたします。

【1】サイバー攻撃発生からの経過

2022年10月31日早朝、ベルキッチンにおいて給食システムの不具合を確認しました。周辺状況から直ぐにサイバー攻撃を疑い、同日7時20分頃、ベルキッチンから委託元病院（当法人外の4病院、当法人内の4病院）のサテライト職員に対し、給食システムにかかるネットワーク接続を遮断するよう指示をしました。

また、同日9時20分には、一部のサーバに保存しているファイルが暗号化されていることを確認しました。なお、同日より、配食については、すでに印刷していた献立情報を用いて手書きで運用することにより実施しました。

翌11月1日には、委託元4病院に対し現状報告を行うと共に、大阪府、堺市及び大阪府警察に対しても報告を行ないました。また、同月2日には、厚生労働省に対しても報告を行いました。その後、各関係機関との連絡協議を経て、同月7日には独立行政法人情報処理推進機構（以下「IPA」といいます。）に支援要請を行うと共に、個人情報保護委員会および関係自治体に対し、サイバー攻撃に関する所定の報告を行いました。

さらに、同月8日にはITセキュリティ専門企業にフォレンジック調査を依頼し、12月6日に調査結果の最終報告を受け、今回のサイバー攻撃に関しての全容が概ね明らかになりました。なお、現在も給食システムの完全復旧に向けて、関係機関と調整しながら作業を進めております。

【2】サイバー攻撃による被害範囲について

ベルキッチンのサーバ3台・NAS（ネットワークアタッチトストレージ）3台が、ランサムウェアの実行により暗号化されたことを確認しました。なお、当法人内および法人外の病院における電子カルテシステムの被害は、地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター様以外では確認しておりません。

【3】給食システムの復旧の見通し

給食システムの運用に必要なコンピューターは全て新規調達し、新たなサーバへデータ移行後、まずは当法人内の病院から試験的に先行して来年1月中旬頃までに復旧作業をいたします。その後、当法人内の病院の給食システムの復旧に問題がないことが確認された段階で、当法人外の病院につきましても、順次ネットワーク接続を開始し復旧させる予定です。なお、全ての病院の給食システムの復旧は、来年1月下旬から2月上旬頃になる見通しです。

【4】原因調査

フォレンジック調査から、本年10月31日午前3時32分に、何者かが、委託業者が利用していたリモートメンテナンス用VPNのFortiOS（セキュリティオペレーティングシステム）の脆弱性をつき、ベルキッチン内のサーバに侵入した痕跡がありました。その後、ベルキッチン内のサーバより、水平展開が行われ他のコンピューターに被害が拡大したと考えられます。

【5】個人情報の流出について

個人情報の流出については、攻撃者が使用したランサムウェアに情報漏洩機能は確認されなかったこと、また攻撃者がFileZilla（ファイル転送プロトコル）などのツールを使用して外部へファイルを送信した事実は確認されなかったことから、本サイバー攻撃によって個人情報が流出した可能性は極めて低いと報告されました。

【6】給食の配送遅延について

サイバー攻撃による給食システムの障害発生から3～5日間にわたり、提供時間に30分から3時間程度の遅れが発生し、患者様をはじめご関係の皆さまには大変ご迷惑をお掛けしました。なお、6日目は、通常通りのスケジュールによる配送を実施しております。

【7】その他

本年12月12日に、大阪府警察本部サイバー犯罪捜査課に被害届を受理して頂いております。

このたびは、ベルキッチンへのサイバー攻撃により給食システムが停止したことで、患者様をはじめご関係の皆さまには多大なご心配とご迷惑をお掛けしましたこと、重ねて深くお詫び申し上げます。

今後も、調査の進展に伴い新たに判明した事項がございましたら、適宜公表させていただく予定です。

以上

本件に関する問合せ先（平日9:00～17:00）

ベルキッチン菱木・サイバー攻撃被害緊急対策本部

メール：kikaku@seichokai.or.jp

ご質問はメールでくだされば幸甚に存じます。

年末年始12月30日（金）～1月3日（火）にいただいたお問い合わせは、1月4日（水）以降に順次ご連絡させていただきます。