2023 年 11 月

マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

今回のテーマ：　ランサムウェアによる被害と対策

2022 年 10 月、大阪急性期統合医療センターがランサムウェアの攻撃を受け、電子カルテシステムを含む重要な情報システムに対するアクセスが遮断されました。さらに 2023 年 6 月には、国内外の主要なクラウドサービスを活用し自社 SaaS サービスを展開する国内上場企業が同様の攻撃に遭遇し、数千ユーザーがサービス利用を停止させられるなど、セキュリティ侵害が企業にとって重大な課題として浮上しています。

「ランサムウェア」とは、悪意あるソフトウェアがコンピューターシステムに侵入し、データを暗号化して利用不能にするサイバー攻撃用ソフトウェアです。攻撃者は、データ暗号化を解除するための身代金を要求しますが、支払いをしてもデータが復元される保証はありません。このような攻撃は、医療機関を含むあらゆる組織にとって重大な脅威となり、迅速な対策と予防が必要とされています。

感染経路について

ランサムウェア感染において、VPN（Virtual Private Network）設備の脆弱性とアカウント管理は、組織のセキュリティ体制における重要なリスク要因と考えられます。VPN はインターネット経由で遠隔地の従業員が企業ネットワークに安全にアクセスするための手段を提供しますが、その脆弱性がランサムウェアを利用するサイバー攻撃者の格好な標的といえます。同様に、アカウント管理の不備はこれら攻撃者によるアクセス権の乱用や権限の昇格を許し、ランサムウェアを実行する手段として悪用される危険性があります。

感染しない努力・感染後の対策について

しかしながら、ランサムウェアの完全な防御は現実的には不可能であり、感染の可能性は常にあります。そのため、感染予防対策と共に感染後迅速に対応する準備も必要です。また、最先端のクラウドサービスを活用してもランサムウェアは完全には防げません。セキュリティ対策はクラウドプロバイダーと利用者(開発者)の共同責任であり、連携してリスク対策を行う必要があります。

① 定期的なパッチ適用（最新の OS やセキュリティが適用されているか確認します）
② 脆弱性アセスメント（脆弱性診断を定期的に実行し事前に検知したリスクを修正します）
③ 社員教育（サイバーセキュリティ教育を行い、様々な攻撃手法を学びます）
④ データ復元の検証（安全なバックアップからデータとシステムの復元が可能か確認します）
⑤ 協力体制の確立（社内外のセキュリティ事故対応チームの編成が推奨されます）

お見逃しなく！

ランサムウェア攻撃の迅速な回復と将来のリスク軽減を実現するため、組織は事前の防止策と事後の対応策をバランス良く備え、セキュリティの強化とともに、有効な対応策を常に準備する必要があります。これにより、潜在的なリスクに対するレジリエンス（危機に直面した際、それら状況への迅速な適応や回復する能力）を保ち、実際の脅威発生時にダウンタイムと損害を最小限に抑制します。