部外秘　　- 取扱注意 -

文書番号: INC-2025-1106-001　　作成日: 2025年11月6日 14:30
報告者: インシデント対応チーム

ランサムウェア インシデント対応 1次報告書

本報告書は、2025年11月6日に発生したランサムウェア攻撃に関する
初動対応の内容をまとめたものです。

【インシデント概要】

検知日時: 2025年11月6日 13:15
発生場所: ファイルサーバー (file-srv-02) およびバックアップサーバー
影響範囲: 重大 (複数の業務システムに影響)
現在の状況: 感染端末を隔離済み・復旧作業準備中

【検知内容】

ファイルサーバー上の複数ファイルが暗号化され、拡張子が.encryptedに
変更されていることを確認。各ディレクトリに身代金要求メモ
(README.txt)が配置されていることを発見。
暗号化されたファイルの詳細分析を実施中。

【実施した対応】

1. 感染が確認された端末およびサーバーをネットワークから即時隔離
2. 全システムのマルウェアスキャンを実施
3. オフラインバックアップの健全性確認
4. 法執行機関への通報および外部セキュリティ専門家への連絡
5. 身代金要求メモの保全とフォレンジック解析開始

【今後の対応予定】

- 詳細なフォレンジック調査による侵入経路の特定
- バックアップからの復旧作業の実施
- 全端末のセキュリティパッチ適用状況の確認と更新
- 2次報告書の作成（24時間以内）

報告責任者: セキュリティ部門 主任 佐藤一郎
承認者: CISO 田中次郎
配布先: 経営層、IT部門、法務部門
次回報告: 2025年11月7日 14:30予定

重要: 身代金の支払いは行わない方針です。調査の進展により
本報告書の内容は変更される可能性があります。