⚠ 御社の備えは万全ですか？

ランサムウェア対策 インシデント訓練サービス

もしランサムウェア攻撃を受けたら
どんなことが起こるのか？ 現場ではどうするか？万が一の準備はできてますか？

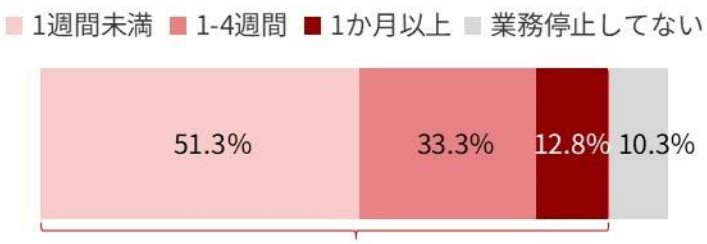
※本サービスはRubrik または Riviiv を導入されている企業様のみご利用いただけます。

こんな課題はありませんか？

- ⚠ バックアップしたシステムが起動しない
- ⚠ 復旧ポイントが判断できていない
- ⚠ マニュアルはあるが未検証のまま

❗ 復旧の遅れは大きな被害につながります

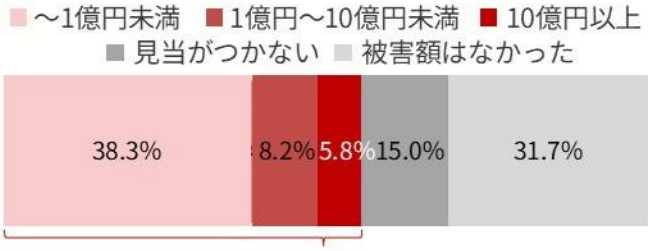
ランサムウェア攻撃による業務停止期間



平均10.2日業務停止

出典：トレンドマイクロ「セキュリティ成熟度と被害の実態調査 2024」

ランサムウェア攻撃による被害額



平均2億2千万円

出典：トレンドマイクロ「セキュリティ成熟度と被害の実態調査 2024」

インシデント訓練で解決しましょう！

実践型 インシデント対応訓練サービス

サービスの特長・訓練概要

既存資料を活用した訓練シナリオ

お客様の復旧計画書・フロー図・手順書などの既存資料をベースに訓練を実施。

手順と役割の見直し

既存の対応マニュアルや連絡網が、緊急時に機能するかを検証・棚卸し。

復旧の実働テスト

バックアップソフトウェアを用いたリストア作業を実際に実施しRTOを確認。

一連の流れを実践

検知・封じ込め・調査・復旧・報告までのライフサイクル全体を通して実施。

お問い合わせ・ご相談 訓練プランの詳細や費用感など、お気軽にお問い合わせください。

富士ソフト株式会社 ソリューション事業本部 営業統括部 ソリューション営業部

050-3000-2767 (受付時間 9:00-17:00) riviiv_sales@fsi.co.jp

※本訓練サービスは、お客様の本番環境への影響を考慮し、安全な方法で実施されます。

お問い合わせ
(QRコードをクリック)

Service Flow

FUJISOFT

インシデント訓練実施フロー

現状把握 ＞設計・計画 ＞実施・成果

01 現状の把握

重要資産・業務の特定

守るべき情報資産と優先して復旧すべき業務を洗い出し、現在の初動体制についてお客様内で振り返り・棚卸しができる状態にします。

危機意識の醸成

同業種の被害事例や最新の脅威動向を共有し、関係者全員が「自分事」として捉えられるよう意識改革を図ります。

02 シナリオ設計と計画

カスタムシナリオ設計

お客様の既存資料（復旧計画書、フロー図など）をベースに、実際に起こりうるランサムウェア感染時の対応シナリオへ更新・最適化を行います。

復旧支援体制の整備

既存の手順書等を用いて役割分担や意思決定フローを確認し、実効性のある訓練計画として実施できるよう準備します。

03 訓練の実施と成果

STEP 1 訓練実施 → STEP 2 ホットレビュー（直後） → STEP 3 報告会（後日）

得られる4つの主要な成果

- 指揮系統の明確化
- マニュアルの見直し
- リスクの可視化
- 初動手順の最適化

導入効果 Before & After

項目	Before (訓練前)	After (訓練後)
連絡体制	× 誰に連絡すればいいか不明で混乱	✓ 連絡フローが一元化され即時伝達
意思決定	× 判断者が不在でシステム停止が遅れる	✓ 権限委譲により現場で即時遮断
復旧作業	× 手順書がわからず、復旧ができない	✓ 検証済み手順で復旧を実現

お問い合わせ・ご相談 訓練プランの詳細や費用感など、お気軽にお問い合わせください。

富士ソフト株式会社 ソリューション事業本部 営業統括部 ソリューション営業部

050-3000-2767 (受付時間 9:00-17:00) riviiv_sales@fsi.co.jp

※本訓練サービスは、お客様の本番環境への影響を考慮し、安全な方法で実施されます。

お問い合わせ
(QRコードをクリック)