

企業向け「サイバー攻撃被害を想定した防災訓練」を提供開始 ～事業継続に必要なシステム復旧を実地で確認。年に 1、2 回めやすに継続実施～

独立系の IT インフラサービス企業、レック・テクノロジー・コンサルティング株式会社（本社：東京都港区、以下「レック」）は、企業向け「サイバー攻撃の防災訓練」の提供を 2026 年 10 月から開始しました。事業継続に最低限必要なシステムを復旧できるかを実地で確認し、訓練で見つかった課題の改善まで支援するものです。サイバー攻撃被害からの復旧を支援するサービス「Re:BIRTH（リバース）」の一環として提供します。

AI を悪用したサイバー攻撃が巧妙化しており、企業のセキュリティ対策が大きな課題となっています。国内では 2026 年上半期に 123 件のランサムウェア被害が報告され、企業活動が長期間妨げられる被害も続いています※1。

こうした事態に備えるには、日頃の防御対策に加え、被害を受けても迅速にビジネスを再開する備えが欠かせません。地震や火災を想定した防災訓練と同じように、サイバー攻撃でも、システムが使えなくなったときの復旧手順を実際に練習しておく必要があります。

バックアップを取り、復旧用の環境を準備していても、その後のシステム変更によって手順が合わなくなったり、担当者の交代で作業が引き継がれなくなったりすることがあります。実際に復旧手順を動かすことで、こうした問題を平時に見つけ、備えを見直すことが訓練の目的です。

訓練では、顧客企業のシステムや業務、その時々への攻撃の傾向を踏まえ、当社が被害を想定したシナリオを作成します。あらかじめ復旧対象と、どの状態になれば復旧できたと判断するかを定め、担当者が手順に沿って実地テストを行います。保護していたバックアップデータの復元や、別のクラウド環境に必要なシステムを立ち上げる作業などを確認します。

復旧対象は、事業を継続するために最低限、必要な機能を優先して決めます。業務の再開に必要なシステムやログイン環境を備えた、いわば「仮設の仕事場」を用意し、早期の再開につなげる考え方です。訓練の基本範囲はシステムの復旧確認とし、お客様のご要望に応じて、担当者が非常時の環境にアクセスする練習なども行います。

訓練で目標に到達できなかった場合や、作業に時間がかかった場合には、その原因や手順上の問題を洗い出します。結果を踏まえて復旧マニュアルや自動化のためのプログラムなどを見直し、次の訓練と実際の被害への備えに反映します。年 1～2 回を一つの目安に、顧客の事情に合わせて継続的に実施します。

Re:BIRTH では、訓練を行うための環境整備も支援します。まず、被害後に事業を継続できる仕組みや体制があるかを診断し、不足する点と改善の順序を整理します。そのうえで、バックアップを改変・削除から守る保管環境、感染を広げないためのネットワークの隔離・遮断、非常時に使う代替システムなどを構築します。

ネットワーク、クラウド、バックアップなどを専門とする当社のエンジニアが連携し、診断から環境構築、復旧訓練、その後の改善までを支援します。企業規模に対して IT 部門の人員や専門知識の確保に課題を抱える企業にも、実行できる復旧の備えを整えていただくことを目指します。

業種や BtoB・BtoC の別を問わず、相談を受け付けます。訓練は Re:BIRTH の導入企業向けに提供し、実施する範囲、日数、頻度は個別に調整します。費用は対象システムや支援内容に応じて見積もります。

この訓練を通じ、悪質なサイバー攻撃に動じない企業を 1 社でも多く増やし、社会の安定に寄与して参ります。

出典

※1 警察庁「令和 8 年上半期におけるサイバー空間をめぐる脅威の情勢等について」本文 9 ページ
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

【この件に関するお問い合わせ先】

レック・テクノロジー・コンサルティング株式会社（レック）

所在地：東京都港区新橋 2-9-17

広報担当：相澤 那月

TEL：03-6382-7403

Email：req_solution@reqtc.com