サイバー防犯通信

https://www.police.pref.hyogo.lg.jp/cyber/

令和８年３３号

兵庫県警察サイバーセンター
サイバー情報発信室

事業者のみなさま、対策できていますか？

事業者のみなさまに警戒していただきたい主な脅威

- **01　ランサムウェア攻撃**　・・・データの暗号化・窃取、業務停止や恐喝
- **02　サプライチェーンや委託先を狙った攻撃**　・・・自社だけでなく、業務委託先・取引先等から侵入
- **03　システムの脆弱性を悪用した攻撃**　・・・VPN・公開サーバ・API*やIDを狙う
- **04　機密情報を狙った標的型メール攻撃**　・・・メール文面等の巧妙化

＊　APIとは、異なるシステムやアプリ間をつないでデータや機能を共有する仕組み

確認すべき３つの事項

01　公開アプリケーションに係るサーバ
アクセス・エラーログの急増やアプリケーションがアクセスするサーバに関する不審な通信がないか確認

02　外部サービス（クラウド、VPN等）
普段と違うログイン・時刻、エラーログの急増、覚えのないアカウント等や権限変更がないか確認

03　資産管理（保有データ、資機材）
不要な個人情報は削除するなどし、各情報等の保管場所とアクセス権を確認

攻撃を防ぐ実施すべき５つの対策

01　多要素認証等の導入
認証機能を強化
アカウントへの権限付与を必要最小限にするなど見直す

02　脆弱性への迅速な対処
OS、アプリケーション等に対する最新のパッチを適用
不要なポート、サービス等を無効化

03　API経由のアクセスへの対応
アクセス回数を制限
悪意ある試みを防ぐために、アクセスの急増に注意
本人確認に加え、アクセス権限の有無をその都度確認

04　被害に備える
ログ保存、緊急時連絡先の確認、保守管理業者との対応手順を整備
ランサムウェアによって生じるシステム障害発生時の事業継続計画の策定

05　業務委託先のセキュリティ対策も確認



もしも被害が疑われたら

01　拡大を止める
まず、ネットワークから遮断する
専門家と相談し、侵害経路を遮断する

02　記録を残す
ログ・端末を保全する
時系列を記録する

03　適切に報告・連絡する
保守管理業者・経営層・関係機関への報告・連絡を判断
従業員は、システム担当者に報告・連絡すること

サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいちはやくお届けしています。

https://x.com/HPP_c3division