情報漏洩防止に向けた セキュリティ対策の徹底

～ 大切な情報を守るのは、私たち一人ひとりの意識と行動です ～

セキュリティ対策責任者やシステム担当者の皆様へ

侵害は起こりうるものです！ 万が一に備え、以下の対策を**確実に実施**しましょう！

発生防止対策

① アクセス制御

業務に不要な人のアクセスを制限し、適切な権限管理を行いましょう。

② ソフトウェアの脆弱性対策

ソフトウェアのバージョンは常に最新状態に更新しましょう。

③ 利用機器に関する対策

端末やモバイル機器のセキュリティ設定を徹底し、不要なソフトウェアの導入を避けましょう。

④ 一定期間電源を落としていた機器に関する対応

一定期間電源を落としていた機器は、起動後にソフトウェア等の状態を確認しましょう。

⑤ 各種ログの確認

不正アクセスの痕跡がないか、各種ログを定期的に確認しましょう。

⑥ 不正プログラム感染の確認

PC等に不審な動作がないか確認し、感染が疑われる場合は、速やかに対処しましょう。

発生を想定した対策

① ＢＣＰの策定

サイバー攻撃やシステム障害は発生するものとして、事業継続計画(BCP)を策定し、被害発生時の対応や復旧手順を確認しておきましょう。

② 対応手順、連絡体制

インシデント発生時の対応手順や連絡体制をあらかじめ整備し、迅速に対応できるようにしましょう。

③ バックアップ

重要なデータは、定期的にバックアップを取り、バックアップしたデータはネットワークから切り離して保管するなどの対策を検討しましょう。

情報システム利用者の皆様へ

日常業務の中でも、以下のルールを守り、**情報漏洩を防止**しましょう！

① 機器やデータの持ち出しルールの確認と遵守

USBメモリ等の記録媒体や業務データの持ち出しは、ルールに従って行いましょう。

② 利用機器に関する対策

パソコンやスマートフォン等は常に最新の状態に保ち、リモートワーク時も社内と同様のセキュリティ対策（VPNの利用、画面ロック等）を徹底しましょう。

③ 電子メール

不審なメールのリンクや添付ファイルを開かない、怪しいメールは無視・削除しましょう。

侵害はいつ起こるかわかりません！ 今すぐ対策を！

一人ひとりが正しい知識を持ち、適切な対策を実践しましょう。

被害に遭ってしまったら 直ちに警察に通報・相談を！

- 最寄りの警察署又はサイバー犯罪相談窓口
  https://www.npa.go.jp/bureau/cyber/soudan.html
- 警察相談専用電話「#9110」番でも相談できます

香川県警察本部サイバー対策課　087-833-0110

サイバー攻撃を受けたら、すぐに対応しましょう！

～ 被害を広げない！ 証拠を残す！ 迅速な復旧につなげる！ ～



1 初動措置 ～ まずは被害拡大を防ぐ ～

❶ ネットワークから隔離

LANケーブルを抜く、Wi-Fiを無効にする。



❷ 証拠の保全

感染端末や機器の電源は切らず、再起動や初期化をしない。



❸ 速やかに報告

上司・情報システム部門（CSIRT）に連絡する。



❹ 早い段階での警察に通報・相談

サイバー攻撃の疑いを把握したら、速やかに最寄りの警察署に通報・相談しましょう！



特に注意！ ランサムウェア感染時の禁止事項

✕ 再起動・電源オフ　✕ フルスキャン　✕ OS・ファームウェア更新　✕ ログや不審ファイルの削除

2 継続対応措置 ～ 調査・復旧・再発防止 ～

❶ 被害状況の調査

感染範囲や情報漏えいの有無を確認する。



❷ 関係機関への報告・相談

警察、IPA、専門事業者等と連携し、必要に応じて顧客・取引先にも連絡する。



❸ 安全なシステム復旧

原因を除去し、バックアップの安全性を確認して段階的に復旧する。



❹ 再発防止

原因分析を行い、セキュリティ対策や対応マニュアルを見直す。



3 被害に備えて平時から準備を！

- ☑ 重要データのバックアップとネットワークからの分離保管
- ☑ ネットワーク機器・脆弱性・資産情報の管理
- ☑ 多要素認証とアクセスログの監視
- ☑ CSIRT・警察・専門事業者への連絡体制の整備
- ☑ サイバー攻撃を想定したBCPの策定

万が一に備え、日頃から準備を行いましょう！



被害に遭ってしまったら直ちに警察に通報・相談を！

香川県警察本部サイバー対策課　087-833-0110