

組織内 CSIRT 構築の参考資料 組織内CSIRT の情報管理と設備について

一般社団法人

JPCERT コーディネーションセンター

このドキュメントについて

- このドキュメントは、組織内 CSIRT において、情報管理と設備に関して配慮すべき事項とその簡単な例を示すことによって、情報管理と設備の整備の助けとなることを目的としている

目次

- CSIRT の情報（データ）の取り扱いについて
- どの情報（データ）を安全に保管するのか？
- どの物理的設備を安全にするのか？
- 情報（データ）保護で留意すべき点
- CSIRT の業務に必要な設備等について

CSIRT の情報（データ）の取り扱いについて

- CSIRT は、インシデントデータや関連するデータは、安全な状態で取り扱わなければならない
- 理由については、以下のとおり
 - 機微な情報を含むことが多い
 - 他の攻撃を誘発するに足りる情報が含まれている
 - サービス対象者からの期待
 - 己に関わるインシデントに関する情報がきちんと管理されているはず
 - 個人情報関連の規則
 - インシデントデータの中には個人情報が含まれていることがあるため
 - データへの不正侵入の可能性
 - 扱うデータが第三者にとって価値ある情報となり得ることがあるため

どの情報（データ）を安全に保管するのか？

- 安全に取り扱わなければならない情報の種類は、以下のとおり
 - インシデント報告
 - 脆弱性報告
 - 電子メール
 - 共有及び印刷された文書
 - 暗号鍵（PGP の秘密鍵）
 - 各種ログ情報
 - 攻撃者の情報（プロファイル、インディケータ）
 - その他、機微情報を含む文書等

どの物理的設備を安全にするのか？

- データを保管する場所（サーバ等）及びデータの伝達経路（ネットワーク）を安全にしなければならない
 - ファイル共有サーバ
 - Web サーバ、アプリケーションサーバ、データベースサーバ
 - 個人用 PC
 - 施設内 LAN（有線、無線）
 - ルータ及びファイアウォール
 - プロキシ及びフィルタリングの器材
 - 入退室管理の設備

情報（データ）保護で留意すべき点 1

- 電子媒体の再利用と破棄について
 - 再利用や破壊の前に、必ずデータを再生不可能な状態になるよう完全削除すること
- 機微な情報（データ）の保管場所
 - 安全な場所（制限区域、鍵のかかるキャビネット等）
 - 機微な情報（データ）に対するアクセス記録
- 災害発生等におけるデータ保護
 - 火事、地震、不審者の侵入等から保護すべきデータを明確化
 - バックアップデータの地理的な分散化

情報（データ）保護で留意すべき点 2

■ バックアップ

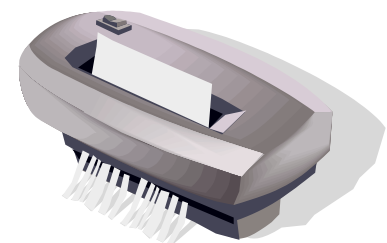
- 容易で確実な復旧が可能な状態
- データ保管時の暗号化
- 安全な場所

■ プリンタ

- プリントアウトされるデータが機微な情報の可能性がある
- 安全な場所になければならない

■ シュレッダー

- シュレッダーにかける前の用紙等の保管は、安全な場所でなければならぬ



CSIRT の業務に必要な設備等について

- CSIRT の業務に必要な設備の例については、以下のとおり。
 - ネットワーク
 - インターネット回線、施設内 LAN、ルータ、ファイアウォール等
 - インシデントの報告、利害関係者との連絡、CSIRT のオフィスに対するリモートアクセス等のため
 - サーバ及びシステム
 - ファイルサーバ、Web サーバ、アプリケーションサーバ、データベースサーバ、ログ保存サーバ等
 - 情報共有、インシデントハンドリングに必要なシステムやツール等
 - 電話、携帯電話
 - 業務時間外における報告のために、留守番電話及び転送機能が必要な場合がある。
 - PC
 - Web ブラウザ、メーラー、オフィス製品等のソフトウェアが必要
 - プロジェクター、ホワイトボード
 - プレゼンテーション、ミーティング等のため
 - プリンタ、ファイルキャビネット、シュレッダー
 - 用紙に出力されたデータの利用と管理
 - 会議用テーブル、個人用デスク、椅子等