JPCERT Coordination Center
電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2021.11.18 14:34:19 +09'00'

JPCERT CC®

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

本資料について

- 本資料は、組織内CSIRTにおける情報管理と設備に関して考慮すべき事項と例を示すことによって、組織内CSIRTの設備と情報管理の設計の助けとなることを目的としている

Copyright ©2021 JPCERT/CC All rights reserved.

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

Copyright ©2021 JPCERT/CC All rights reserved.

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を安全な状態で取り扱わなければならない
  - 機微な情報を含むことが多い
    - 攻撃に利用可能な情報が含まれている
  - サービス対象者からの期待
    - 「自分に関係するインシデント情報は適切に管理される」という期待
  - 規制等への準拠
    - 個人情報やその他の規制対象となる情報が含まれることがある
  - 証拠としての利用
    - 法廷での使用に耐える保管と記録が求められることがある
  - データに対する侵害の可能性
    - 扱うデータは第三者にとって価値ある情報となることがある

Copyright ©2021 JPCERT/CC All rights reserved.

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
  - インシデント報告
  - 脆弱性報告
  - 電子メール
  - 共有および印刷された文書
  - 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

Copyright ©2021 JPCERT/CC All rights reserved.

どの物理的設備を安全にするのか

- データの保管場所（サーバー等）およびデータの伝達経路（ネットワーク）を安全にする
  - ファイルサーバー
  - Web サーバー、アプリケーションサーバー、データベースサーバー
  - 個人用 PC
  - 施設内 LAN（有線、無線）
  - ルーターおよびファイアウォール
  - プロキシおよびフィルタリングの器材
  - 入退室管理設備

Copyright ©2021 JPCERT/CC All rights reserved.

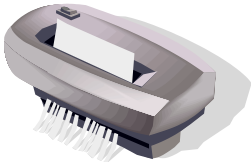
情報（データ）保護で留意すべき点 1

- 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
- 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

Copyright ©2021 JPCERT/CC All rights reserved.

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
- プリンター
  - プリントアウトされるデータが機微な情報を含む可能性がある
  - 安全な場所に設置されなければならない
- シュレッダー
  - シュレッダーにかける前の用紙は、安全に保管されなければならない



Copyright ©2021 JPCERT/CC All rights reserved.

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
  - ネットワーク
    - インターネット回線、施設内LAN、ルーター、ファイアウォール等
      - インシデント報告、利害関係者との連絡、CSIRTオフィスへのリモートアクセス等
  - サーバーおよびシステム
    - ファイルサーバー、Webサーバー、アプリケーションサーバー、データベースサーバー、ログ保存サーバー等
    - 情報共有、分析・検証、その他のインシデント対応業務に必要なシステムやツール等
  - 電話、携帯電話
    - 業務時間外の報告受付や時間外の緊急対応のために、留守番電話や転送機能などを活用
  - PC
    - Webブラウザー、メーラー、オフィス製品等のソフトウェア
  - プロジェクター、ホワイトボード
    - CSIRT内のミーティング等のため
  - プリンター、ファイルキャビネット、シュレッダー
    - 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

Copyright ©2021 JPCERT/CC All rights reserved.