

# インシデント マネジメント



情報処理振興事業協会  
セキュリティセンター

## 講演内容

- インシデントマネジメント
  - 平時におけるインシデント対応の準備
  - 情報セキュリティ侵害を検出する
  - 情報セキュリティインシデントに対応する
  - 改善する

# 講演の目標

組織体において効果的にインシデントに対応するためには、**事前に準備しておく必要がある。**

インシデント対応の一連の手続きを理解し、その中で**事前に準備しておくべき項**を理解する。

## 平時におけるインシデント対応の準備

- セキュリティポリシー等の中で手順を明記
- 平時に行われていなければならないこと
  - 定期的バックアップ
  - システムの通常状態の把握
  - 外部情報収集と修正プログラムの適用
  - 予行演習
- 技術的手段の準備

## 情報セキュリティ侵害を検出する

- 検出・認識の方法
  - 既知の侵害を検出する
  - 異常な状態を認識する
  - 他者からの連絡
- ツールの利用
  - 平時の準備が必要
- 次に何をすべきか？

## インシデントに対応する

- インシデント対応手順の確認
- 報告する
  - 組織体内部のコミュニケーション  
あらかじめ定められた手順
  - 関連組織とのコミュニケーション  
参考資料: JPCERT/CC 技術メモ  
関係サイトとの情報交換

# インシデントに対応する

- 暫定的対応と本格的対策
  - 暫定的対策：
    - ネットワークの遮断 / システムの停止
  - 本格的対策: 攻撃者にシステム特権を奪われたとき
    - クリーンなシステムの再構築
    - 修正プログラムの適用
    - データの復旧

## インシデント後

- 報告書
  - 時系列報告
  - 今回対応のよかった点 / 悪かった点
- 改善する
  - 対応手順に反映・集約
  - 技術的な改善

# 事前に準備しておくべき事項

- 対応手順の文書化
  - バックアップ
  - ツールの設定