情報セキュリティ: 事後対策の重要性

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

事後対策の重要性

- 予防だけでは不十分
  - 予防対策は完全ではない
  - 使用している技術が変化する
- 技術的対策だけでは完全ではない
  - 必ず人が関与している: 情報システムの利用者、管理者
  - 人の行動が弱点となる: 設定ミス、情報持ち出し、端末放置
- 攻撃側は進化する
  - Zero Day 攻撃: 対策前の脆弱性を突く
- 社会、法律も変化する

インシデントが起こると

例えば、不正侵入が起こったら、いろいろと対応しなければならない。

- 重要な情報の漏えいは無いか
- どこから侵入されたのか
- 他にも侵入されていないか
- 誰に報告すべきか
- 記者会見しなければならないのか
- そもそも、誰が対応の指揮をとるのか

同種のインシデントが再発したら

- 前回のインシデントの原因は分析したか
- 前回のインシデントに対して再発防止対策はしたか
- 誰が、再発防止の指揮をとったのか
- 再び、記者会見しなければならいのか

事後対策の準備

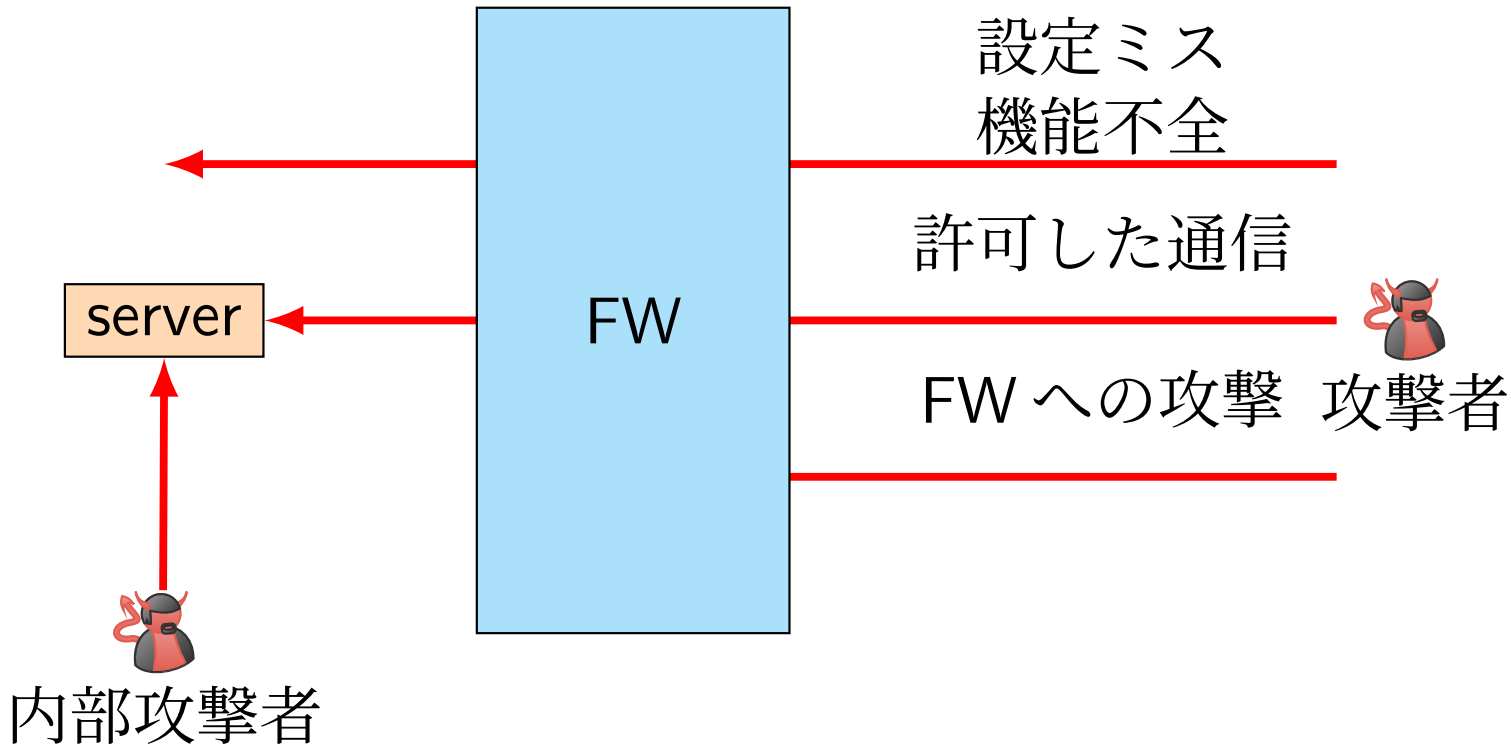
- インシデント発生を想定した対策
  - 被害を拡大しないための対策
  - インシデントの兆候を把握するための対策
- インシデント発生後の準備
  - 調査や応急措置の体制
  - 連絡・報告の体制
  - 広報の必要性の検討
- 再発防止策

PC にウィルス対策ソフトを導入しても、対策は完全ではありません。その理由を考えましょう。

なぜ予防策は完全ではないのか

例: Firewall 対策

- 設定は完全か: 設定の見落としは無いか
- FW は設定通りに動いているか: 機能・性能に課題はないか
- 許可した通信を通じた攻撃は無いか
- FW の内側に攻撃元の機器が入ってしまったらどうなる
- FW 装置そのものの脆弱性を突く攻撃への耐性は


設定ミス
機能不全
許可した通信
FW への攻撃
攻撃者
server
FW
内部攻撃者

なぜ予防策は完全ではないのか

例: Web のログイン認証を使った利用者制限

- パスワード漏えい
- Web サーバの脆弱性
- Web サーバが稼働する OS への不正侵入
- 正当なユーザの PC が乗っ取られる
- 内部犯行

インシデント発生を想定した対策

- 不正侵入
  - FW、IDP、サービスなどのログ分析
  - 設定確認
- パスワード漏えい
  - 証跡管理 (認証ログ)
  - 多要素認証導入
  - 容易に破られるパスワードを許さない対策
  - 使われていない ID の削除
- 重要情報の改ざん、喪失
  - データバックアップ
  - 書き換え不能な媒体の利用
  - 分散保存

- 重要情報の漏えい
  - 暗号化
  - 分散保存
- LAN 内の PC がウィルス感染
  - FW や IDP による通信モニタ
  - LAN 内の通信モニタ
  - 監査アプリケーション

被害拡大を抑止するための対策

以下を実施するための、体制、規則、手順を準備する

- 通信の遮断
  - 何をどのようにして止めるか
    例: 通信切断、システム停止
  - 影響が及ぶ範囲の確認
  - 止めても大丈夫かの整理
    業務への影響、機会損失、記録喪失
- 被害状況の確認
  - どこまで侵入されたか
  - 他の機器の状況
  - 情報漏洩や情報破壊の有無
  - 情報漏洩の場合、その情報が外部で流通していないか

- システム停止等は関係者、利用者への大きな制限となる
  - 誰が何の権限で実施するかを明確に
  - 組織内外への説明
  - 関係者、利用者の理解を求める行動

報告・連絡の体制・制度

- 発見者はどのように行動すべきか
  - 誰に報告すべきか
  - 報告先は周知されているか
- 報告を受けた者は何をすべきか
  - 緊急退避策の指示
  - 上位職への通報
- 組織的体制を構築
  - 責任者
  - 連絡網
  - 手順書
- 被害拡大抑止と再発防止が目的であることを周知
  - 被害者を責めない

報告連絡体制の整備にあたって、「被害拡大抑止と再発防止が目的」であることを強調する理由はなにでしょう。

参考: ヒューマンエラー対策

https://www.abc.jp/service/anakenshu/he/

再発防止

- 状況把握と原因究明
  - 侵入経路と手段
  - 記録保持が重要
- 再発防止策
  - 設定確認
  - 設定見直し
  - 新規対策導入
  - 教育
- コストを考慮
  - 対策にはコスト (機材、人) が必要
  - どこまでやるべきかの判断が必要

CSIRT: Computer Security Incident Response Team

- 情報セキュリティインシデントは、組織にとって大きなダメージ
  - 重要情報の漏えい
  - 業務の停滞や停止
  - 場合によっては、謝罪や慰謝料
  - 信用失墜
  - 組織イメージの棄損
- 組織的な対策が必要

https://www.cc.saga-u.ac.jp/use/security/csirt

- CSIRT: インシデント対応時に緊急対応するチーム
- 状況を把握して、緊急避難をする
  - 対象機器をネットワークから切断する
  - インシデントが発生している LAN を切断する
  - 対象ユーザの利用を停止する
  - 対象システムを停止する
- 対象の管理者へ連絡
- インシデントレベルに応じて、上位職へ報告
- 対象の対応状況に応じて、制限解除

例: あるPCが危険なURLへアクセスした

- 当該PCのネットワーク接続を切断する
  - スイッチでの切断など
- 当該PCの利用者へ対応を指示
  - 接続は意図的であったか
  - マルウェア等をインストールしてしまったか
  - 重要情報は無いか
- 危険が無いと判断した場合には、ネットワーク切断を解除
- 危険があると判断した場合
  - PC内の詳細調査
  - 重要情報の流出の有無を確認
  - 必要ならば再インストール

各自の PC について、ウィルス対策ソフトウェアの状態を確認し、パターンファイルが最新であることを確認しなさい。