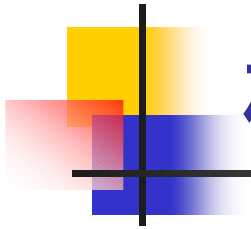
JPNIC・JPCERT/CCセキュリティセミナー第3回　　平成15年11月5日

『応：～インシデントに対応する(発見と調整)～』基調講演

# インシデントレスポンスと警察

警察庁技術対策課
サイバーテロ対策技術室
伊貝　耕



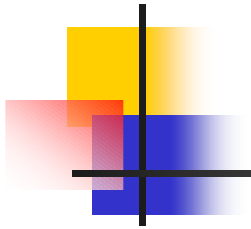
# 概要

- インシデントレスポンス
  - インシデントの概要、事例
  - インシデントレスポンスの概要、事例
- 警察の役割
  - インシデントと警察
  - インシデントの未然防止
  - インシデント発生時
- おわりに

# インシデントとは

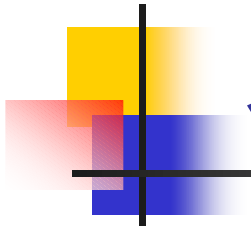
- 機密性、完全性、可用性に影響を及ぼす不測の事態
- インシデントの種類とその影響

| 事案 | 機密性 | 完全性 | 可用性 |
|---|---|---|---|
| ウイルス感染 | 中 | 大 | 小 |
| 不正アクセス | 大 | 大 | 小 |
| DoS | ー | ー | 大 |
| 情報漏洩 | 大 | ー | ー |
| 障害 | 小 | 中 | 大 |



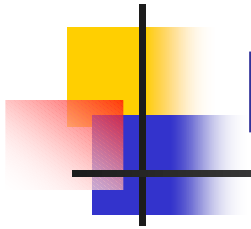
# ウイルス感染

- インシデント
  - 国内大手運送会社
    - 全国拠点をつなぐ内部ネットワーク
  - 米国大手鉄道会社
    - 列車運行管理システム
- 原因：不用意な端末の接続
- 遠因：閉鎖系ネットワークにおける脆弱性対策の欠如



# 不正アクセス

- 事例
  - 公益法人における産業スパイ事件
    - 契約メーカー社員の逮捕、有罪確定
  - 国立医療機関における不正アクセス事件
    - トロイの木馬
  - 政府系Webサイトでの改ざん疑惑事案
- 原因：部内犯行、外部からの攻撃
- 遠因：不適切な利用者管理、セキュリティ対策の欠如

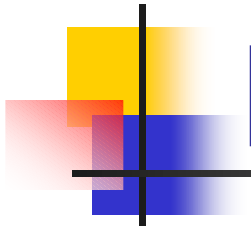


# DoS

- 事例
  - 教科書問題サイバーデモ
  - 業界団体WebサーバへのDoS攻撃
  - 公益法人Webサーバへのアクセス集中による DoS攻撃誤検知
- 原因：外部からの攻撃、負荷
- 背景：対策の欠如、システム設計の不備

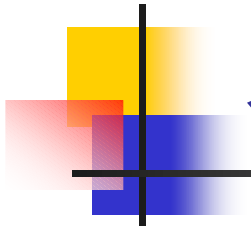
# 情報漏えい

- 事例
  - 美容関連企業による利用者情報の漏洩
  - 旅行会社による顧客情報の漏洩
- 原因：部外者による探索、公開
- 遠因：データ管理の不備、法制度の不備



# 障害

- 事例
  - 金融機関の合併に伴うシステム障害
  - 航空管制システム障害
  - 航空会社における乗客管理システム障害
  - ワームによる米国銀行ATM障害
- 原因：例外処理、システム変更等
- 遠因：不適切なシステム設計、バックアップシステムの不在

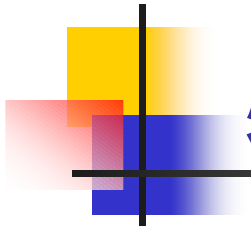


# インシデントの背景

- 情報通信システムへの依存
- システム基盤のオープン化
- インターネットへの接続
- インターネットのインフラ化
- セキュリティ意識・技術の不足

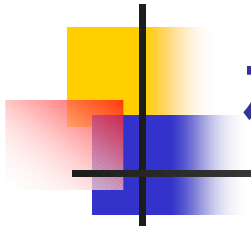
# インシデントレスポンス

- 目的
  - サービスの復旧
    - 再発防止
- フェーズ
  - 事前準備
  - 認知･原因究明
  - 制圧･根絶･回復
  - 再発防止



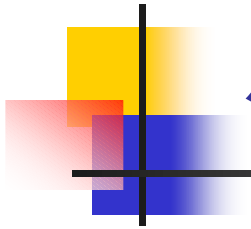
# 必要な要素

- 活動主体
  - コンピュータセキュリティ事案対処チーム (CSIRT)
- 検知、分析、対処用のツール類
  - IDS、ファイアウォール、ウイルス対策ソフト等
- 制度
  - セキュリティポリシー、対処マニュアル



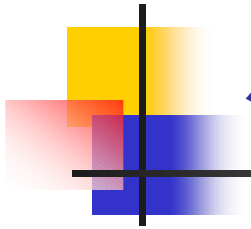
# 標準化動向

- ISO/IEC 18044　WD
  - 平成15年9月現在検討中
- NIST Special Publication 800-61 Draft
  - 平成15年9月15日公表（コメント締切10月15日）
  - http://www.nist.gov/
- その他
  - 米国司法省コンピュータ犯罪・知的所有権課
  - 各種書籍（CERT/CC等）



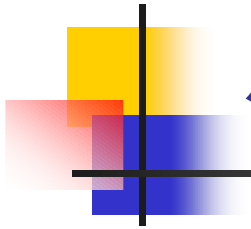
# ケーススタディ

- 事案概要
  Webサーバに対して、中国よりConnection Flood攻撃を受け、一般へのサービスが不能となったもの。
- Connection Flood攻撃
  サーバに対して多くの接続を確立してタイムアウト寸前まで接続を維持することで、サーバの同時接続数を占有し、DoS状態を発生させる攻撃。



# ケーススタディ

- 事前準備状況
  - サーバ管理は外部委託
  - Apacheでほぼデフォルト設定
    - 最大同時コネクション数150、タイムアウト300秒
  - ファイアウォール有、IDS無
- 認知
  - 一般閲覧者からの苦情

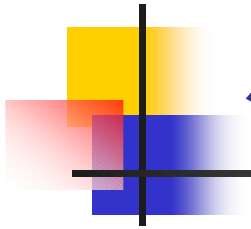


# ケーススタディ

- 原因究明
  - ファイアウォールの再起動
    → DoS状態に変化なし
  - 再起動直後にWebサーバのログにリザルトコード408（タイムアウト）が大量に記録
  - タイムアウトのログに記録された10余りのIPアドレスからの不審なコネクションが原因ではないかと推定

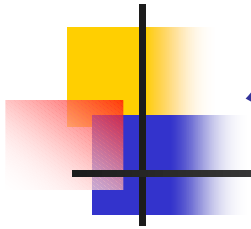
# ケーススタディ

- 制圧・回復
  - ファイアウォール上で、問題のIPアドレスからの接続を拒否するよう設定
  - サービスの回復を確認
- 根絶
  - 警察に連絡
    → 中国警察に国際捜査共助依頼
  - その後も数週間にわたって攻撃が継続



# ケーススタディ

- 再発防止
  - Apacheの各種パラメータの最適化
  - 同一IPアドレスからのセッション数の制限
  - サービス提供状況の定常的な監視体制の確立



# ケーススタディ

- 幸運
  - 高度の専門知識を有する者（ベンダー及びサイバーフォース）が対応
  - ファイアウォールの存在
  - ファイアウォールの再起動によるログ記録
- 不運
  - IDSがあっても検知が難しい攻撃手法

# 警察の役割

- 警察の目的
  「国民の生命、身体及び財産の保護」
- 警察の仕事
  「犯罪の予防、制圧及び捜査、犯人の逮捕」
- インシデントへの警察の基本姿勢
  インシデントの多くは犯罪
  → 防犯対策、被害者対策

# 警察の属性

- 無償
- 秘密保持義務
- 捜査権限
- 技術力
  - 60名のインシデント対応専従職員
  - 攻撃、防御技術の研究開発
  - 24時間監視センター
  - 電磁的記録解析センター

# インシデントの未然防止

- セキュリティ対策
  - @police(http://www.cyberpolice.go.jp/)
    - 脆弱性データベース
    - ワーム、ウイルスデータベース
    - 影響の大きい脆弱性の広報
    - 攻撃トレンドの分析
      （インターネット治安情勢、インターネット定点観測）
    - リテラシ教育
- ペネトレーションテスト

# インシデント発生時

- 重要インフラ事業者
  → 専従の対処班（全国９班）
- 一般
  → ハイテク犯罪相談窓口
  → セキュリティアドバイザ
  （都道府県警察本部）

# おわりに

- インシデントレスポンスとコスト
- 民間セキュリティ企業と警察
- 警察の有効活用を