強いインシデント･レスポンスの基本

園田道夫
vp5m-snd@asahi-net.or.jp
http://www.asahi-net.or.jp/~vp5m-snd/sec/
http://d.hatena.ne.jp/sonodam/

自己紹介

- 1962年生まれ厄年を抜けてヽ(´ー`)ノ
- 2004年1月1日よりフリー
- SISS（日本セキュリティ情報流通協議会）監事
- JNSAハニーポットWG、セキュリティスタジアムWGリーダー
- 技術者教育をテーマに、教育講座企画中
- セキュリティ夜話（http://www.asahi-net.or.jp/~vp5m-snd/sec/）
- 極楽せきゅあ日記（http://d.hatena.ne.jp/sonodam/）
- vp5m-snd at asahi-net.or.jp

インシデントとは何か

- インシデントの意味：事件、出来事
- セキュリティにおける「インシデント」の意味
  - 公開サーバーが不正アクセスされた
  - 情報が漏洩した
  - ワームが発生した
  - メールサーバーが踏み台になった
- セキュリティを脅かすような出来事はすべてインシデント
- 情報セキュリティリスクが発現した状態（http://www.ipa.go.jp/security/ciadr/word_idx.html）

インシデントにレスポンス（対応）するというのはどういうことか

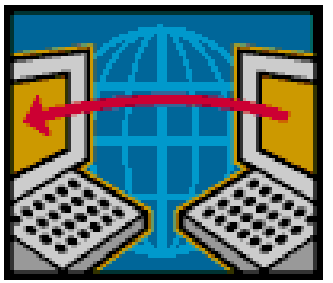
- JPCERT/CCに不正アクセスを受けたことを報告することだけが、インシデント対応ではない
- 警察やIPAに届け出ることだけでもない
- 不正アクセス、情報漏洩、ワーム発生などに対処することがレスポンス（対応）
- インシデントの発生に際して、それを検知し、関係組織と連絡をとり、被害の拡大を防ぐと共に、再発を防止するための原因究明と改善を行う、一連の組織的活動をいう。
（http://www.ipa.go.jp/security/ciadr/word_idx.html）

レスポンス(対応)するためには何が必要か

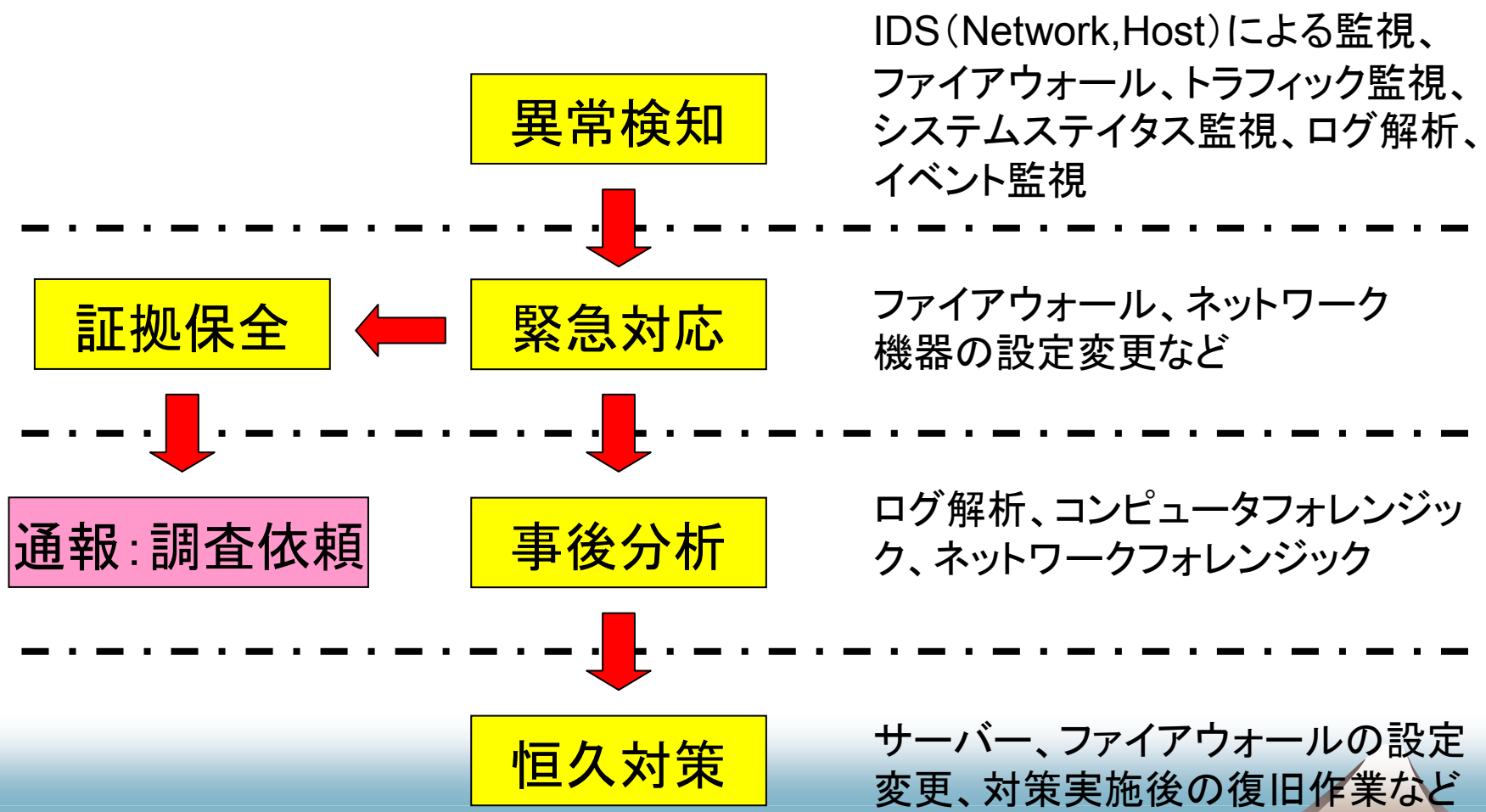
- まずは検知できなければ始まらない
  - 何が起こっているのが察知できなければ、インシデントが起きているのに「わかっていない」「把握できていない」ということになる
  - ワームに感染していても「なんか調子悪いなー」
  - メールサーバーが踏まれていても気付かない
- 検知するには仕掛けが必要
- 検知するには日常的な管理・運用が肝心

検知するための仕掛けやデータにはどのようなものがあるのか

- 侵入検知システム（IDS）、ファイアウォール、ハニーポット
- システムログ、アプリケーションログ、ファイアウォールログ、ネットワーク機器のログ
- イベント監視、ステイタス監視
- トラフィック監視、SNMPによる監視
- ユーザーPCのインベントリー管理
  - 各仕掛け、データの特徴は別紙参照



異常検知から対策までの流れ



仕組みの特徴

- 事後解析系
  - ログ解析、コンピュータフォレンジック、ネットワークフォレンジック、イベント監視、ログ監視
  - 取得した記録を解析して突き合せ、インシデントを炙り出す（というよりも、相関解析でしか事実は明らかにできないし、侵入者はログを改ざんするものだと思っていたほうが良い）
- リアルタイム（に近い）検知系
  - IDS、ファイアウォール、ハニーポット、（イベント監視、ログ監視）
  - 緊急対処のための警報装置としての期待→リアルタイム検知への要望は高まってきている

IDS、ハニーポット

- IDS（侵入検知システム）は実際に運用に入っているサイトが増えてきている
- ネットワークトラフィックを監視し、不正アクセスのパターンに合致した通信を捕捉するタイプ（Network型IDS）と、サーバーに常駐しサーバーリソースへのアクセス等を監視するタイプ（Host型IDS）がある
- （トンネルも含む）暗号化通信が増えていくことが予想されるので、Host型にシフトしていく？
- Host型の一種、ハニーポットは、まだ実験的な立場でしかない

IDSによる検知の限界

- 通信パターンのマッチングが主な技術（Network型）なので、どうしても誤差（誤検知）がある
- ノイズ除去などのノウハウがまだ必要
  - ・・・ということはまだまだ手間がかかる仕組みであるということ
  - IDS運用にはノウハウを持ったアナリストが必要
  - 分析やフィルタリングを経由する＝結果が出るまで時間がかかる＝まだリアルタイムとは言い切れない
- 未知のパターンに対応できない
- IDP（Intrusion Detection and Prevention）として信頼性高く動作するまでにはまだ時間がかかる？

トラフィック解析

- もっとシンプルにインシデントを検知できる仕組みが無いか？
- 切り口を変えて機械的に異常検知し、IDPの役割に近づけたい
  - 単にトラフィックの増減を見て、異常を捉えることができるのではないか？
  - 総量だけでなく、いろいろな切り口での量的変化を捉える
- リアルタイムにより近い検知→防御策をそれだけ素早く講じることができる

レスポンス(対応)にはどのような方法・手順があるのか

- 危険なコンピュータ、サーバーの隔離
  - とにかく被害を拡げないことが重要
- 通信の隔離
  - あやしい通信を遮断、回避する
- 証拠保全
  - その状態を損なわないよう保全する
- 捜査機関等への通報:調査(捜査)依頼
- 内偵(事後分析)
- リスク回避、暫定的なサービス運用
- 広報、告知

レスポンス（対応）のための準備

- 手順の策定
- 仕組みと仕掛けの準備
  - 隔離、暫定的なサービス運用、代替策
  - 復旧、恒久的な対策実施
- 作業記録フォーマット
- レビューとリハーサル
- 組織と体制、非常時権限の明確化とオーソライズ

企業･組織としての事後対策

- 広報･告知活動
- 訴訟
- 懲戒･解雇
- 処罰
- 損害の計算
- 報告

今日この後の予定

- 検知について（渡辺勝弘さん）
- 対応について（園田）