侵入検知・防止システム

情報理工学部 総合情報学科

先端工学基礎課程

2016/07/25

IDSの評価項目

- **検知機能**　　的確に不正を検知
- **通知機能**　　迅速かつ確実な通知
- **診断機能**　　攻撃診断が可能 (どんな攻撃手法か？)
- **検知対象領域**　検知対象手法の多様性
- **使用資源**　　必要な計算資源の量
- **負荷耐性**　　高負荷時における検知性能劣化度
- **利用可能性**　　どんな機器/情報源/設置場所が必要か

評価項目と課題

- **環境依存**
  - IDS設置の目的や方法は組織によって異なる
- **評価項目の優先度**
  - 評価項目の重要度(優先度)は組織によって異なる

評価条件の普遍化は困難

IDS単体としての評価ではなく、導入目的や
環境との適合性を含めたSecurity対策としての評価を

IDSは計算機を安全にしない？

答えはYESである

不正侵入検知システムは検出 & 通知のみ
その後の対策作業は人間が行う必要がある

なぜ侵入されたのか調査し
その原因を修正する防止措置を行い
その侵入経路が塞がれたかを監査することで保証し
それができて運用に戻す

金言:

些細な不正侵入防御は、**大がかりな**不正侵入検知に勝る
セキュリティ上の問題を修正しない限り計算機は**安全にならない**

IDSに未来はない...

- Gartner report (June 11, 2003)
  - 投資にみあう効果なし．2005年には不要，と予測
- Information Security Hype Cycle declares IDS a Market failure; Money slated for IDS should be Investigated in Firewalls.
  ⇒ Network & Application levelのFirewallに移行せよ
- 不正行為は「遮断」しなければ意味がない

引用: http://www.thefreelibrary.com/Gartner+Information+Security+Hype+Cycle+Declares+Intrusion+Detection...-a0102982749

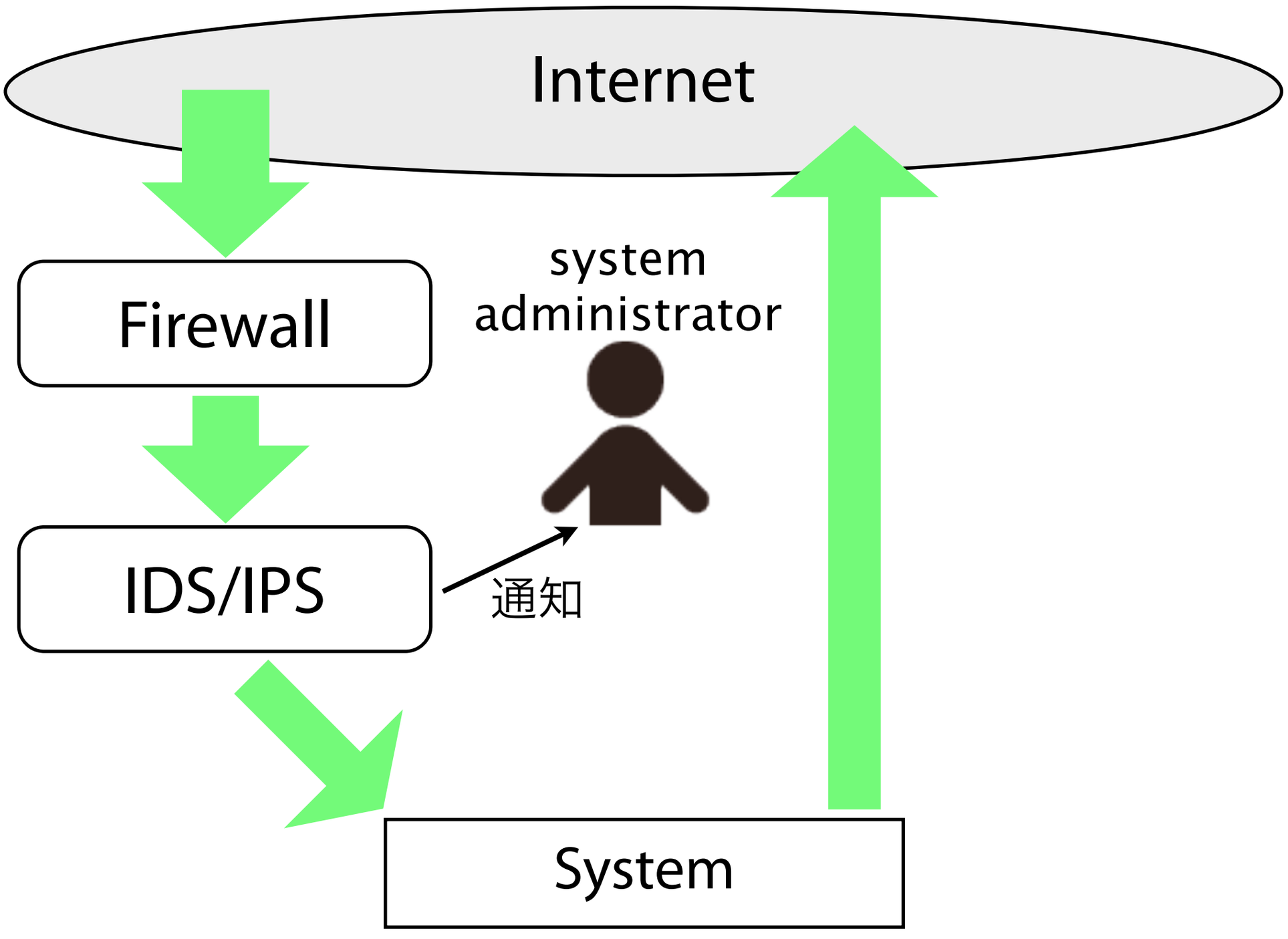
今後

- 処理能力（性能）向上
  - 専用ハードウェア化 ⇒“アプライアンス”
- Extrusion detection system
- 防御機能の追加 ⇒ IPS (IDPS) へ
- Unified Threat Management (UTM) 化
  Firewall, Anti Virus, Spam filterなどの機能と統合
- Honeypot (おとりサーバ)との連携

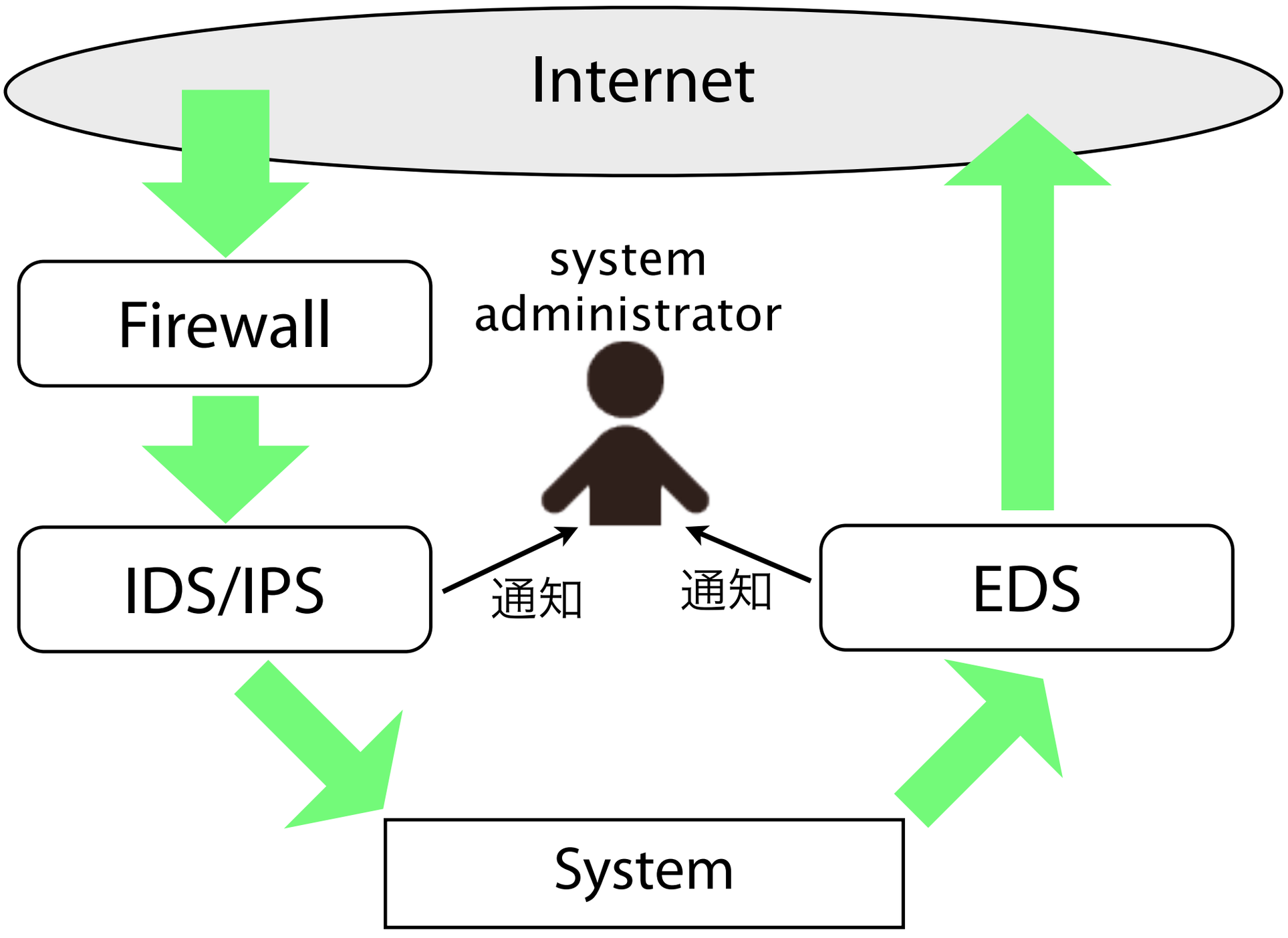
Extrusion Detection System (EDS / XDS)

- Intrusion Detection System (IDS):
  - 「組織外部から内部 (Inbound)」に対する攻撃を監視/検知
- Extrusion Detection System (EDS or XDS):
  - 「組織内部から外部 (outbound)」のnetwork traffic内に不正がないことを監視
    別名: “Outbound Intrusion Detection”
  - Identify attack attempts launched from an already compromised system in order to prevent them from reaching their target

Increasing threat awareness



Increasing threat awareness



EDS: Extrusion detection system

Firewall is not enough

- 「疑わしい通信」をもれなく制御するのは困難
  ⇒ 正規のProtocolを通じた攻撃は止められない
- Contentに依存する不正行為は防御しにくい
  ⇒ 関与したデータに依存
  (Firewallは，すべてを見ないことが多い)
- ひとたび侵入に成功した後に発生する攻撃は
  止めにくい
- Firewall自身が脆弱性を持つ場合もある
  ⇒ 別の独立した通信制御があるべき (多層防御)

外から内 vs. 内から外

- ルールの決めやすさ
  - Inbound (外から内)よりもOutbound (内から外)の方が困難
    ⇒ 組織が大きくなればなるほど、その傾向大
- FirewallよりもEDSの方が使い勝手が良い
  - 事後対応は必要、だがルールは定義済みを利用可

EDSの利用事例

- 内部不正者、自組織からの不正行為の検出
  - 情報漏洩対策 (Data loss prevention: DLP)
    - 権限を持つ利用者による「誤利用」検知
- Malwareの通信検知 (From compromised computer)
  - 感染済み計算機から第三者への通信
    - 通常時とは異なる相手との通信になる可能性大

EDSの利用事例

- Spam送出検知
  - E-mail serverでもない計算機からのメール送出
  - 通常とは異なる E-mail 送出数
  - 既定のサーバとは異なるSMTP(E-mail)サーバとの通信
- ルール作成は可能
  ⇒ 正常時の振る舞いを規定し、異常検出を実施

不正侵入防止システム (IPS)

- 英語名：**IPS** (**I**ntrusion **P**revention **S**ystem)
    - 別名
    - **IDPS**: Intrusion Detection and Prevention System
- 不正行為を「検知」し、かつ「**防御**」する

Firewall、IDS、IPSの関係

- **Firewall**
  - 防火壁
- **IDS**
  - 火災報知器
- **IPS**
  - スプリンクラー

利点

- 不正行為の防御/遮断
  - 既知の不正行為
  - 既存Protocolに乗じた不正行為
    - IDS同様の仕組み、通知+対抗措置の実行
- Firewallの補完
  - 利用(設置)場所は同一
  - 制御可能な不正行為は、こちらの方が広範
    - 「利用者既定の規則」⇔「専門家既定のsignature」

Virtual Patch (1/2)

- セキュリティ対策の基本
  - 脆弱性が発見 ⇒ Patch(修正プログラム)の適用
- Patch適用時の問題点
  - Patch適用時の提供/運用サービスへの影響
  - Patch自体の評価、それにかかわる
    環境/人的資源、費用
  - Patch適用後、不具合発生時の対応

安易にPatch適用ができない状況の存在

Virtual Patch (2/2)

- Patch適用 ⇔ システムの安定運用
  - 相反する．が、放置も認められない
- IPS導入によるpatchの代用
  - システムにPatchをあてられない、けれども
    セキュリティ対策は必要
  - IPSによる防御 = Patch適用のかわりとする
    ⇒「仮想的なPatch」
  - 「サポート切れOSへのSecurity対策」として

IBM ソリューション サービス 製品 サポート & ダウンロード My IBM 検索

ソフトウェア >

Windows XPサポート終了後のセキュリティー対策はIBM Virtual Patchで安心

Windows XP / Windows 2000 / Windows NT のサポート終了に伴うセキュリティー・リスクを軽減

↓ Windows XPクライアント保護ソリューション
↓ Windowsサーバー保護ソリューション

Windows XPに対するサポートは、2014年4月9日（日本時間）をもって終了します。

Windows 2000サーバーに対するサポートは、2005年6月にメイン・ストリーム・サポートが終了し、延長期間も2010年7月13日で終了しました。

しかし、現在使用中の業務アプリケーションがこれらのWindowsOS上で動いている場合も多く、企業のシステム管理者の皆様にとって、このサポート終了は頭の痛い問題のひとつかもしれません。

こちらのお問い合わせは下記からお申し込みください。弊社からご連絡させていただきます。

資料のダウンロードはこちら　お問い合わせのお客様はこちら

お問い合わせはこちら

まずはお気軽にご相談ください

メールを送る
見積を依頼する
電話番号: 0120-550-210
識別コード 109HJ03W

ゼロＤＡＹ攻撃に強い、IBM Security Network IPS

ネットワーク上でJava脆弱性を狙ったアプレットをブロック
→ 詳細はこちら

図引用: http://www-01.ibm.com/software/jp/cmp/virtualpatch/

Signatureの違い

- IDS
  - 攻撃への対応 (検出+通知)
  - Attack signatureが必要
    - Anti-Virusも原理的には同様
- IPS
  - 脆弱性への対応 (検出+防御)
  - Vulnerability signatureが必要

Vulnerability signature

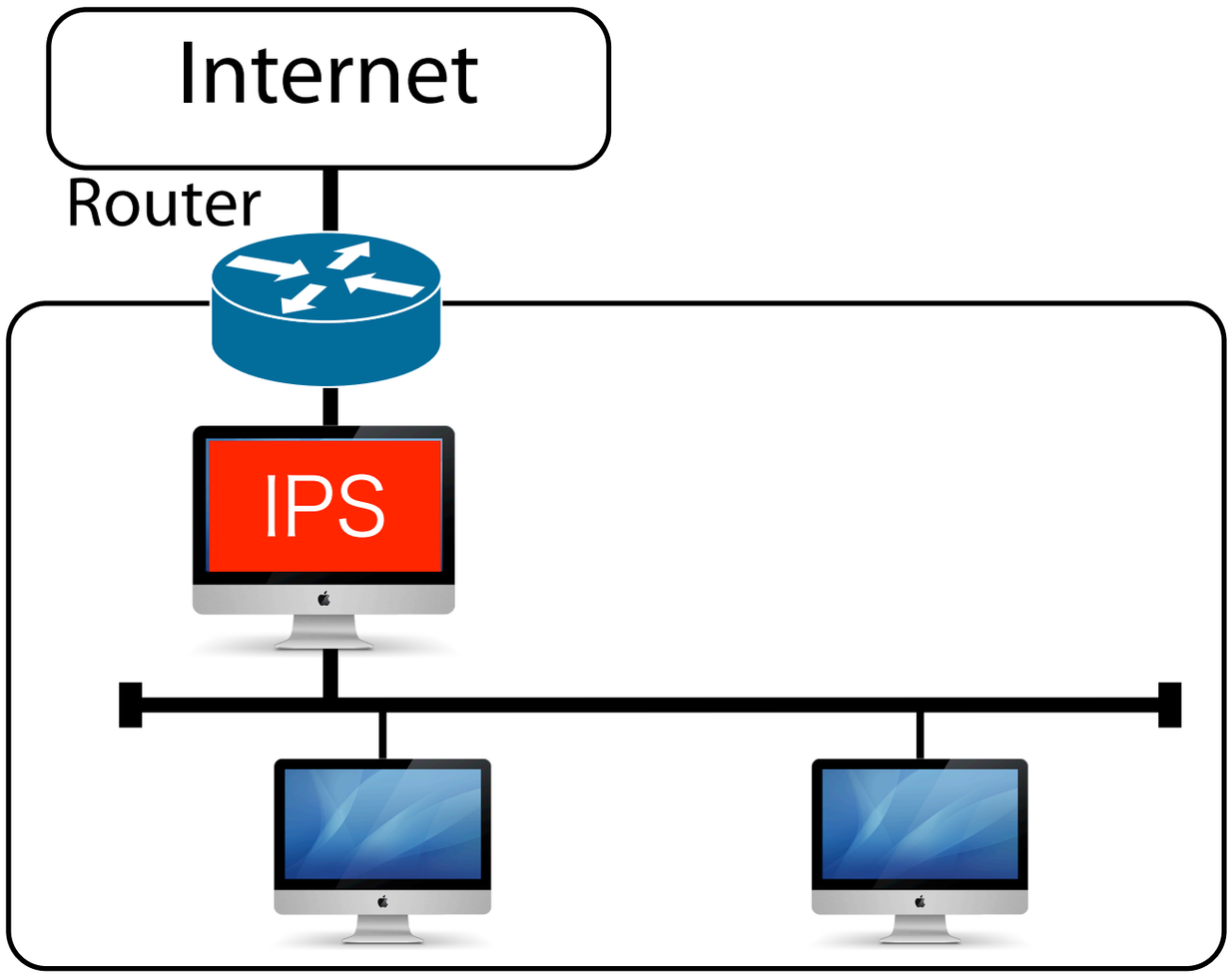
- 実際に脆弱性が悪用される条件を特徴情報化
- 脆弱性 と 攻撃方法の関係
  - 大抵の場合 ⇒ 「一 対 多」
    - 複数種の攻撃手法を1つのsignatureで対応可能に
- 早期対応の可能性
  - 悪用する攻撃手法が出回る前に対応
  - 公式Patch提供前の対応

欠点

- Network traffic量に応じた処理能力が必要
  - Networkのスループット確保
- 設置方法の制約
  - ネットワーク構成の変更 (後述)
- 過剰防御
  - 正規の通信を誤って遮断する
    - 誤判定
    - 故障、電源断
      ⇒ バイパス(fail open)処理 (通信機能の維持)

設置法

IPSの設置＝インライン型



- 理由
  - 不正な通信を遮断するため
    - タップ型では遮断できない
- Firewallの内側がbetter
  - 明らかな不正通信はFirewallで遮断
  - IPSの処理量削減
    ⇒ 処理負担軽減

防御機能について

- 検知したNetwork trafficの遮断方法
  - Firewallとの連携 (firewall rulesの動的生成)
    - 別名: Dynamic blocking
    - 単純に破棄 (Drop packet)
    - Network Protocolの規則を応用
      - 発信元へのICMP unreachable msg. (for ICMP/UDP)
      - TCP reset flag (接続強制遮断)
    - 偽の応答 (対 Port-scan)

運用について

- Signatureの更新
- 処理負荷およびNetwork遅延の監視
- 脆弱性検査 + (Firewall + IPS)の組み合わせ
  - 脆弱性診断の結果をもとに、Firewall & IPSの rule と signatureをチューニング
    ⇒ 致命的な脆弱性がなくなるように努める

脆弱性診断

- 実稼働システムに対して攻撃と同等の行為を行い、脆弱性の有無を調査
  - OSやApplicationの脆弱性、設定ミス
    - 未対策のホスト、サービス、アプリケーションの発見
- Firewall, IPSの設置と同様に重要な作業
  - 意図した通りの機能を果たしているか検証
  - PDCAサイクルのCheckとして活用

主な検査手順

- Discovery scan
  - Hostの有無と機器/Operating systemの推定
- Service scan
  - Network serviceとversionの推定 (Port scan)
- Vulnerability scan
  - Service scanに基づき脆弱性の有無を検査
- 侵入検査、DoS強度検査
  - 発見された脆弱性を実際に攻撃、負荷耐性測定

Discovery scan

- Network通信により、遠隔から機器の存在を知る (Sweep)

- ICMP (Ping)
- TCP/UDP connect

OS推定

- Operating system(OS)の特定は攻撃者にとって重要
  ⇒ セキュリティホールはOS依存であることが多い
- TCP/IP Stack fingerprinting
  - TCP通信が可能であれば、リモートから推定可能
  - TCP/IP stackの実装がOS依存 / RFCの解釈差を利用
    ⇒ 特定のpacketに対する応答がOSにより異なる

OS推定の例

PINGの応答におけるTTL値

Host A

```
64 bytes from 130.153.          icmp_seq=0 ttl=63  time=3.007 ms
64 bytes from 130.153.          icmp_seq=1 ttl=63  time=3.011 ms
64 bytes from 130.153.          icmp_seq=2 ttl=63  time=3.002 ms
64 bytes from 130.153.          icmp_seq=3 ttl=63  time=3.074 ms
```

Host B

```
64 bytes from 130.153.          icmp_seq=0 ttl=255 time=7.757 ms
64 bytes from 130.153.          icmp_seq=1 ttl=255 time=2.652 ms
64 bytes from 130.153.          icmp_seq=2 ttl=255 time=2.462 ms
64 bytes from 130.153.          icmp_seq=3 ttl=255 time=2.458 ms
```

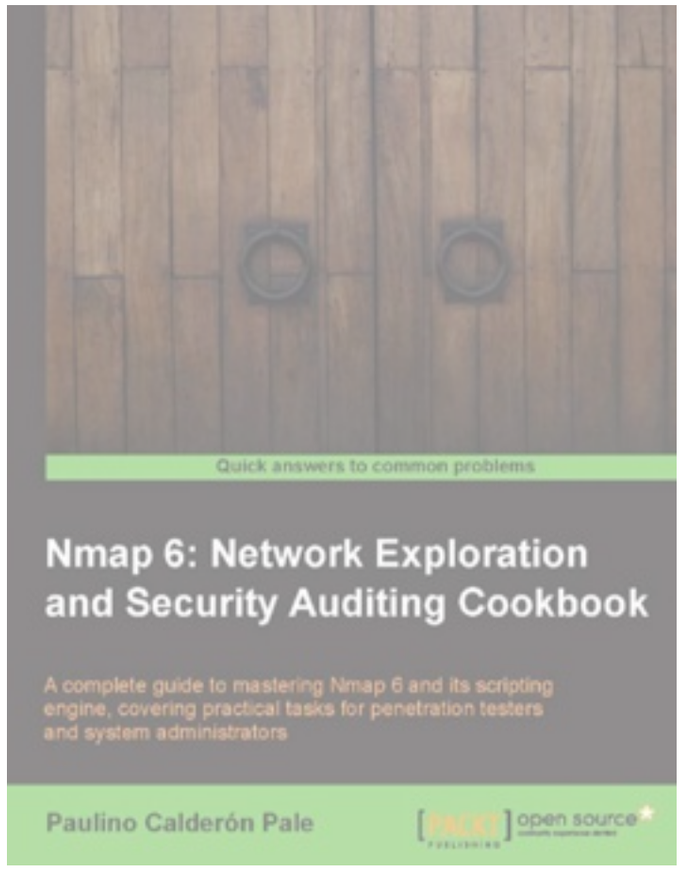
TTL値の初期値はOS毎に決まっていて異なる値

Windows : 128
Mac OS, Linux : 64
Solaris, Routerの一部: 255

→ OS推定に利用

Service scan

- 対象ノード(計算機)で稼働するサーバ群を知る
  - Port scan
    ⇒ “Nmap” というツールが著名
- 様々なScan方法がある
  - Scan対象に気づかれないようにする
  - Firewallや監視システムから回避



Vulnerability scan

- 既知の脆弱性が悪用可能かを検証
  - ２つの方法
    - 遠隔の計算機から (Network経由)
      - 不正操作が可能なnetwork serviceの有無
      - 悪用可能なSecurity holeの有無
    - ホスト内から
      - 未patchのsoftware, system componentの有無
      - 不適切なfile permission, user/group, 権限の存在
      - 安易なpassword, default (guest) accountの有無

Vulnerability scan

- 脆弱性探索 = 攻撃行為と同等行為の実施
  - システムの運用に支障をきたす可能性
  - データのBackup や 複製システムを構築し脆弱性スキャンを実施するなどを検討

専用環境の事例

サイボウズ脆弱性報奨金制度

2014年6月、脆弱性報奨金制度がスタートしました。弊社パッケージ製品・クラウドサービスの脆弱性を発見し報告いただいた方に謝礼として報奨金をお支払いします。報奨金は1件あたり1,000円から最大300,000円（1件の報告から複数の脆弱性が検出された場合の金額上限は1,000,000円）です。

本番環境への影響を考慮いただくことなく、安全に検証いただくため、「脆弱性検証環境提供プログラム」を用意しました。脆弱性を発見した方のご報告はこちらからお願いします。

サイボウズ製品とは？

――延べ400万のビジネスユーザーが利用するクラウドサービス及びパッケージ製品

ビジネスに関する膨大なデータが日々蓄積され、お客様から「サイボウズの中に会社がある」と言われるほど私達のサービスは社会のインフラとして機能しています。

cybozu.com　kintone on cybozu.com

サイボウズ10　Garoon　メールワイズ

引用: http://cybozu.co.jp/company/security/bug-bounty/

Honeypotとは？

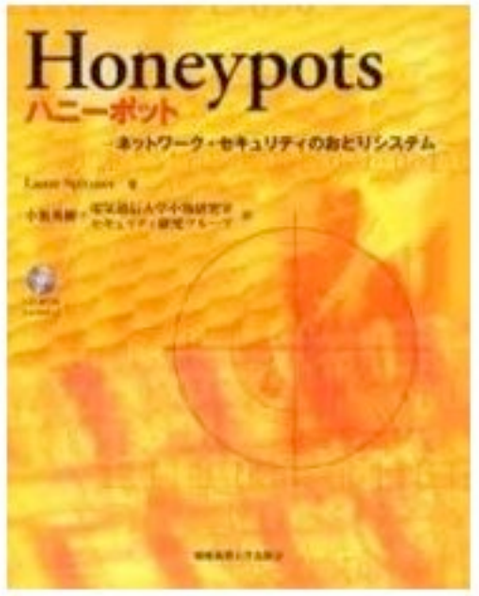
- 不正侵入者をおびきよせ、不正行為に関する情報を収集する仕組み
  - 例) 意図的に脆弱なサーバの設置
  - 別名: 誘い罠、HoneyTrap
- **未知の不正侵入行為に関する情報収集/時間稼ぎ**

必要要件

侵入したくなるようなサイトであること
侵入できること
計算機内での攻撃者の挙動を(すべて)記録できること
計算機を出入りするnetwork情報が記録できること
何者かが侵入したらすぐに警報が発せられること

Honeypotの利点/欠点

- 利点
  - 実現は比較的容易
  - 記録された情報は結果に基づくので信頼できる
  - 性能的な問題は発生しない
- 欠点
  - 正規のユーザが罠にかかる可能性
  - 踏み台として悪用される恐れ



不正侵入者をだましきれるか？ が一番の問題