脅威の管理

日新電機株式会社
情報通信開発事業部
ELNIS

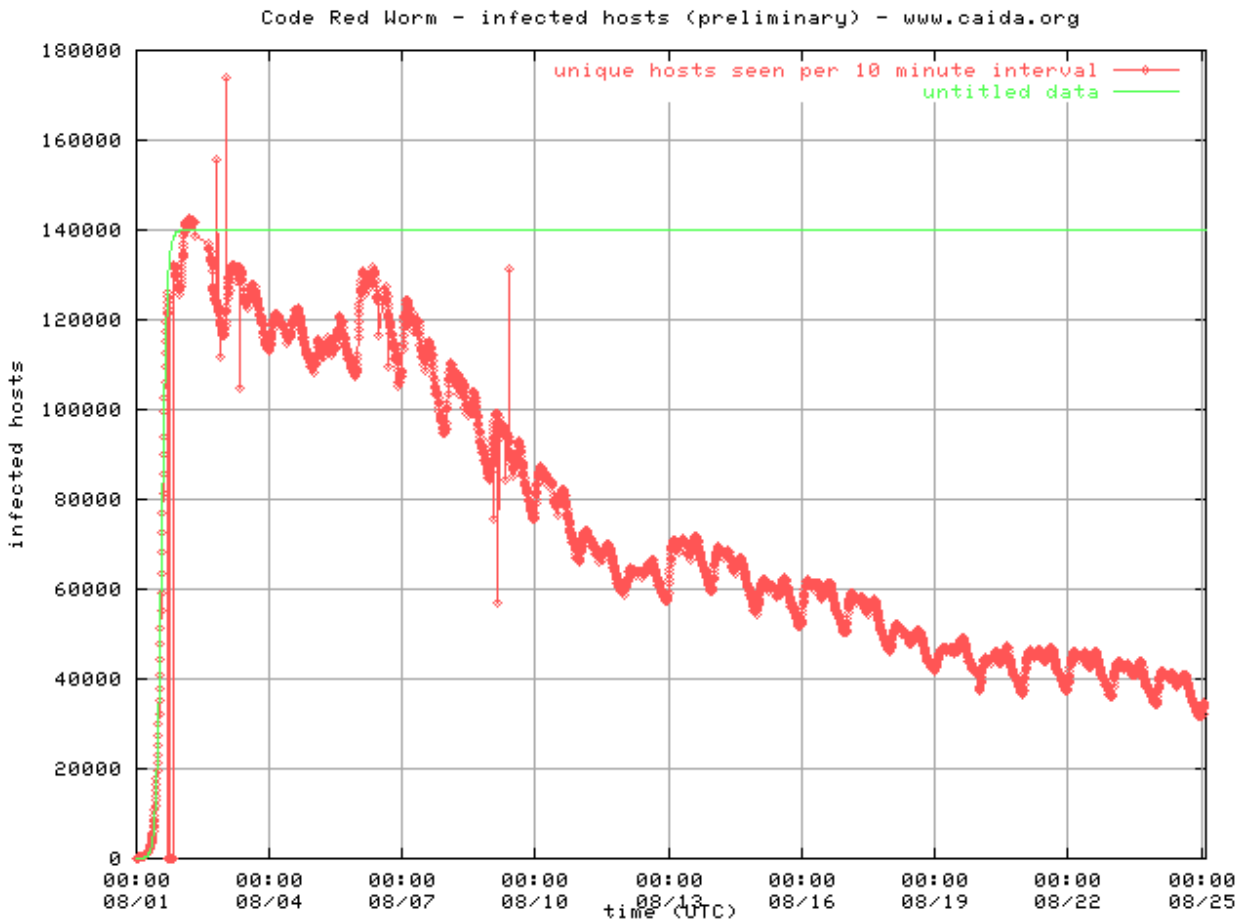
ワーム、ワーム…ワーム！

- IIS/sadmind
  - ’01/5
    - JPCERT-AT-2001-0009
  - Sadmindバッファ・オーバーフロー
  - IIS　Unicode デコード
- CodeRed
  - ’01/7
    - JPCERT−AT−2001−0013, 2001-0014, 2001-0017, 2001-0018
  - MS-IIS .ida 脆弱性
    - JPCERT−AT−2001−0010
- CodeRed II
  - ’01/8
    - JPCERT-AT-2001-0019, 2001-0020
  - MS-IIS .ida 脆弱性
  - バックドア

ワーム、ワーム…ワーム！

- CodeBlue
  - MS-IIS Directory Traversal 脆弱性
  - IDA、IDQマッピングを削除
  - 多数のプロセス起動

Code Red 感染統計



出展：www.caida.org

SANS Top 10 List – ’01-1

- BIND
  - CVE-1999-0833, CVE-1999-0009, …
- CGI、アプリケーション拡張
  - CVE-1999-0067, CVE-1999-0068, CVE-1999-0270, CVE-1999-0346, CVE-2000-0207,…
- RPC
  - CVE-1999-0687, CVE-1999-0003, CVE-1999-0693, CVE-1999—696, CVE-1999-0018, CVE-1999-0019
- RDS
  - CVE-1999-1011
- Sendmai, MIME
  - CVE-1999-0047, CVE-1999-0130, CVE-1999-0203, …

SAN Top 10 List

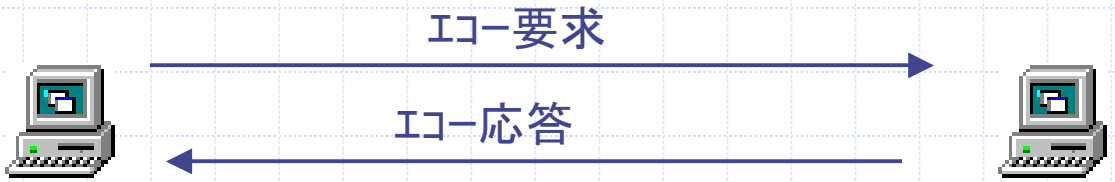
- Sadmind, mountd
  - CVE-1999-0977, CVE-1999-0002
- NetBIOSファイル共有, NFS
  - CAN-1999-0520, CAN-1999-0554
- パスワード設定（パスワードなし／簡単に類推可能）
  - CAN-1999-0501, …
- IMAP, POP バッファ・オーバーフロー
  - CVE-1999-0005, CVE-1999-0006, …
- SNMP community – public, private
  - CAN-1999-0517, CAN-19999-0517, …

秘密のチャネル…Loki

ICMP echo request あるいは echo reply ﾊﾟｹｯﾄ

Lokiのﾃﾞｰﾀがechoﾊﾟｹｯﾄの
ﾍﾟｲﾛｰﾄﾞの中に含まれる

注: ﾄﾝﾈﾘﾝｸﾞはどんな
ﾀｲﾌﾟのﾊﾟｹｯﾄでも実現
できるが、Lokiは
ICMP echo ﾊﾟｹｯﾄを
使っている



ｸﾗｲｱﾝﾄはｻｰﾊﾞｰに侵入し
ｺﾏﾝﾄﾞを実行できる

ｻｰﾊﾞｰはｸﾗｲｱﾝﾄからの
ｺﾏﾝﾄﾞに答える

秘密のチャネル…Covert Channels

- Loki
  - ’96/8 Phrack
  - ICMPトンネル： echo request, echo reply
  - TFN(Tribal Flood Network), BO2K(Back Orifice 2000)
- Daemonshell-UDP
  - UHT1(Unix Hacking Tools)
  - TCP or UDP channel
- ICMP Backdoor
  - ICMPトンネル：echo reply
- 007Shell
  - ’98/12
  - ICMPトンネル：echo reply
  - ライブラリ、サーバ／クライアント、シェル
- Rwwwshell
  - ’99/5
  - HTTPトンネル

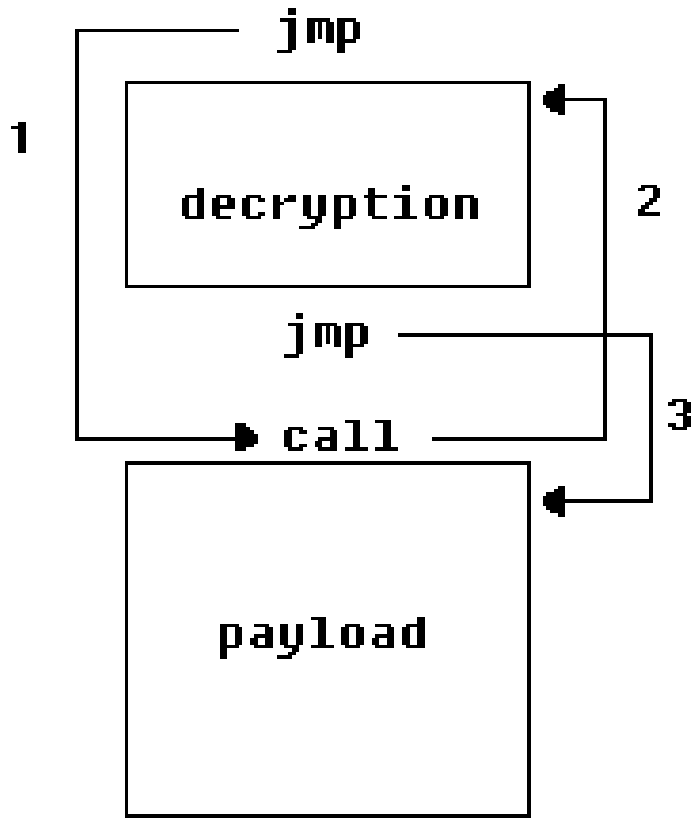
IDSをすり抜ける…Evasion

- ネットワーク・レイヤー
  - IP フラグメンテーション
  - データ詐称
- アプリケーション・レイヤー
  - データ
    - Unicode
    - オペレータの変更 (.. = .¥.)
  - コード／データ・エンコーディング
    - 暗号化、他
    - Polymorphism

隠す…各パートをステルスに

- バッファ・オーバーフローの例
  - リターン・アドレス
    - 複数のリターン・アドレスを持つものが多い
    - バッファ・サイズが既知であれば、リターン・アドレスは1つで構わない
  - ペイロード
    - インストラクションのオフセット／順序を変更
    - インストラクション自体を変更
    - 別のレジスタを使用
    - ペイロードを暗号化
  - NOP
    - NOPに換え、影響のないインストラクションを使用
    - インストラクション・スタッキング

ペイロードの暗号化



Polymorphism

- Polymorphism…
  - 多様な形態、形式
  - 同一機能を達成する方法ー複数の方法
  - 順序性
  - 実行されないコードをパディング
  - ランダム性
- ADMutate
  - ‘01/3 CanSecWest　K2
  - バッファ・オーバーフローのシグネチャを変更

リスクの特徴

- リスクは継承される
- 自然にリスクを排除しようと努力する
- *完全なリスク除去は不可能*
- リスク除去コスト
  - 許容可能な損失とリスク除去とのコスト比較
- 達成すべきリスク除去目標は、理にかなったものであるべき

リスク管理の公式

IDSの対象

$$\text{リスク} = \frac{\text{脅威} \times \text{脆弱性}}{\text{対策}} \times \text{インパクト}$$

最近のアタックの特徴

- アタック･コードの開発スピードが早い
  - 変種
  - より早い対応が必要
- 旧知の脆弱性
  - 全ての脆弱性を除去するのは困難
  - 内部
- アタック／ハッキング技術の高度化
  - Covert Channel
  - イベージョン
  - Polymorphism
  - …

脅威の管理へ

1997-1998	1999-2000	2001 -

Threat Management

Intrusion Detection

Firewalls

少数のユーザ
少数のアタック
ー　3,734 attacks (CERT)
インターネットとの境界防御

LANベース
単一サイト
9,859 attacks (CERT)
不正侵入

ハイスピード／スイッチ　ネットワーク
ユーザ／サイト数激増
15,167 attacks (CERT)
不正侵入, DoS/DDoS, 内部不正
ネットワークが複雑にグローバル化
データセンター

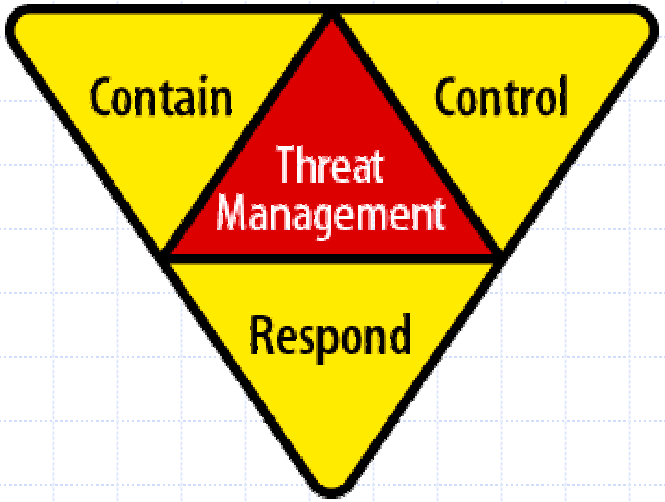
脅威を管理するには…

ー　IDSの課題

- シグネチャ・ベース
  - シグネチャの開発／アップデート
- パフォーマンスの制約　(<100Mbps)
- セグメント毎にセンサーが必要
- フォルス・ポジティブ
- 大規模ネットワークへの適用
  - 管理が困難
  - 情報が共有／集約されない

Recourse Technologies社のソリューション

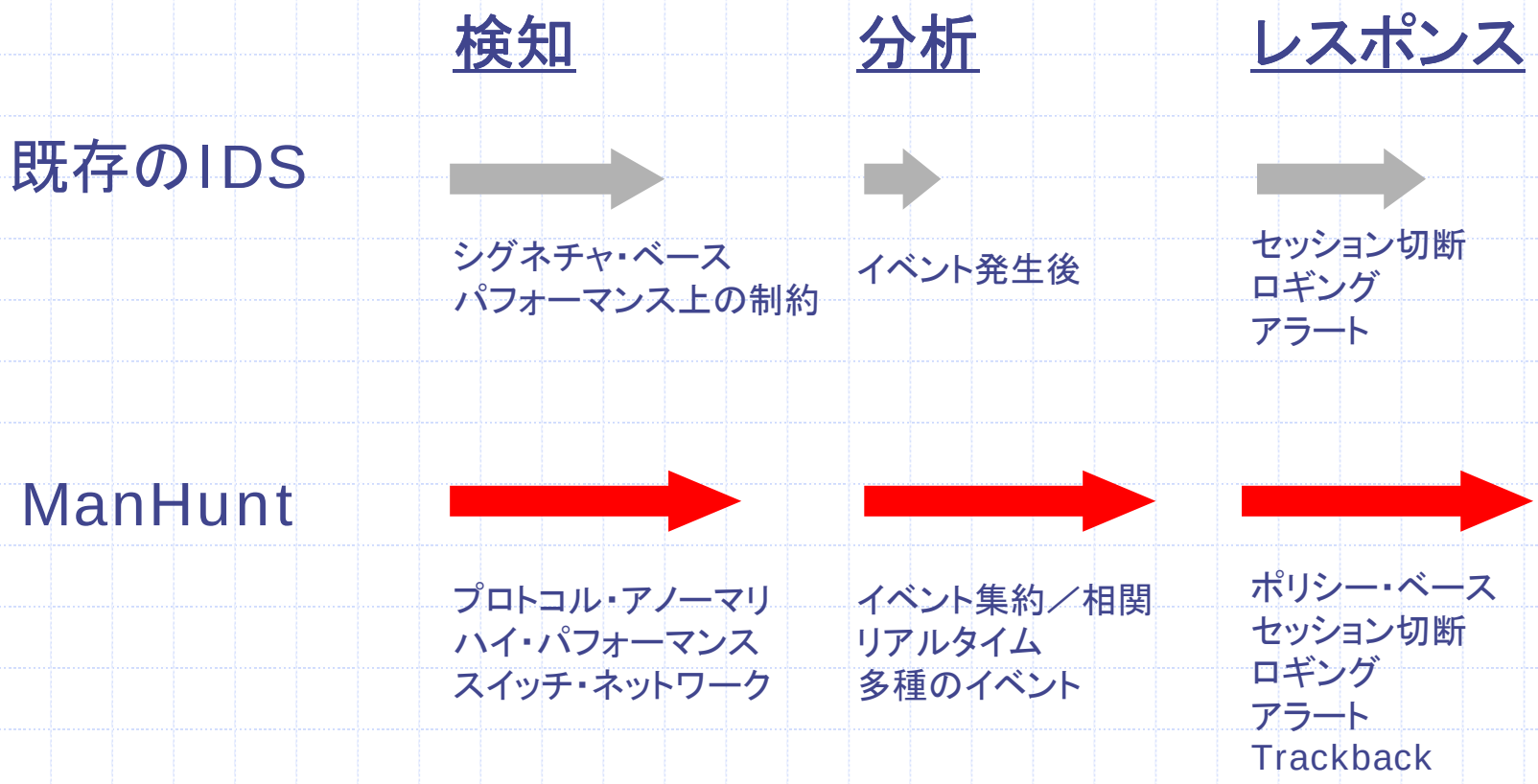
- Recourse Technologies社の脅威管理ソリューション
  - コンピュータアタックを封じ込め、制御、対応
  - 侵入、内部犯罪、DoS/DDoS
  - 検出、分析と対応
  - セキュア、日常業務に無影響
- ManHunt™
  - 脅威管理システム
- ManTrap®
  - セキュア・ハニーポット・システム



脅威管理のコンポーネント

- 管理すべき脅威（対象）
  - DoS アタック、DDoS アタック、不正侵入…
  - 新種のワーム、内部不正
- 検知
  - 直接的、間接的
- 分析
  - 分析、相関、Analysis, correlation, presentation
  - 多種イベントソースに対応
- レスポンス
  - Policy driven alternatives

ManHunt


検知
分析
レスポンス
既存のIDS
シグネチャ・ベース
パフォーマンス上の制約
イベント発生後
セッション切断
ロギング
アラート
ManHunt
プロトコル・アノーマリ
ハイ・パフォーマンス
スイッチ・ネットワーク
イベント集約／相関
リアルタイム
多種のイベント
ポリシー・ベース
セッション切断
ロギング
アラート
Trackback

ManHunt ：検知

- ハイ・スピード・センサー
  - ネットワーク・イベント検出
  - プロトコル・アノーマリ
  - Known and novel attacks
  - Flooding 検出用レート・カウンター
  - “ローミング” ― センサーのカバー率を最大化
  - ハイ・スピード (最大 1 Gb/s)

検知 -> 分析 -> レスポンス

ManHunt: 分析

- イベントの集約／相関
  - イベントの集約　－　プライオリティを付けたインシデント
  - 分散配置されたManHuntからのイベントを分析
  - 分析によってフォルス・ポジティブを軽減
  - アーキテクチャ：3rdパーティ製品からのイベントをインテグレート

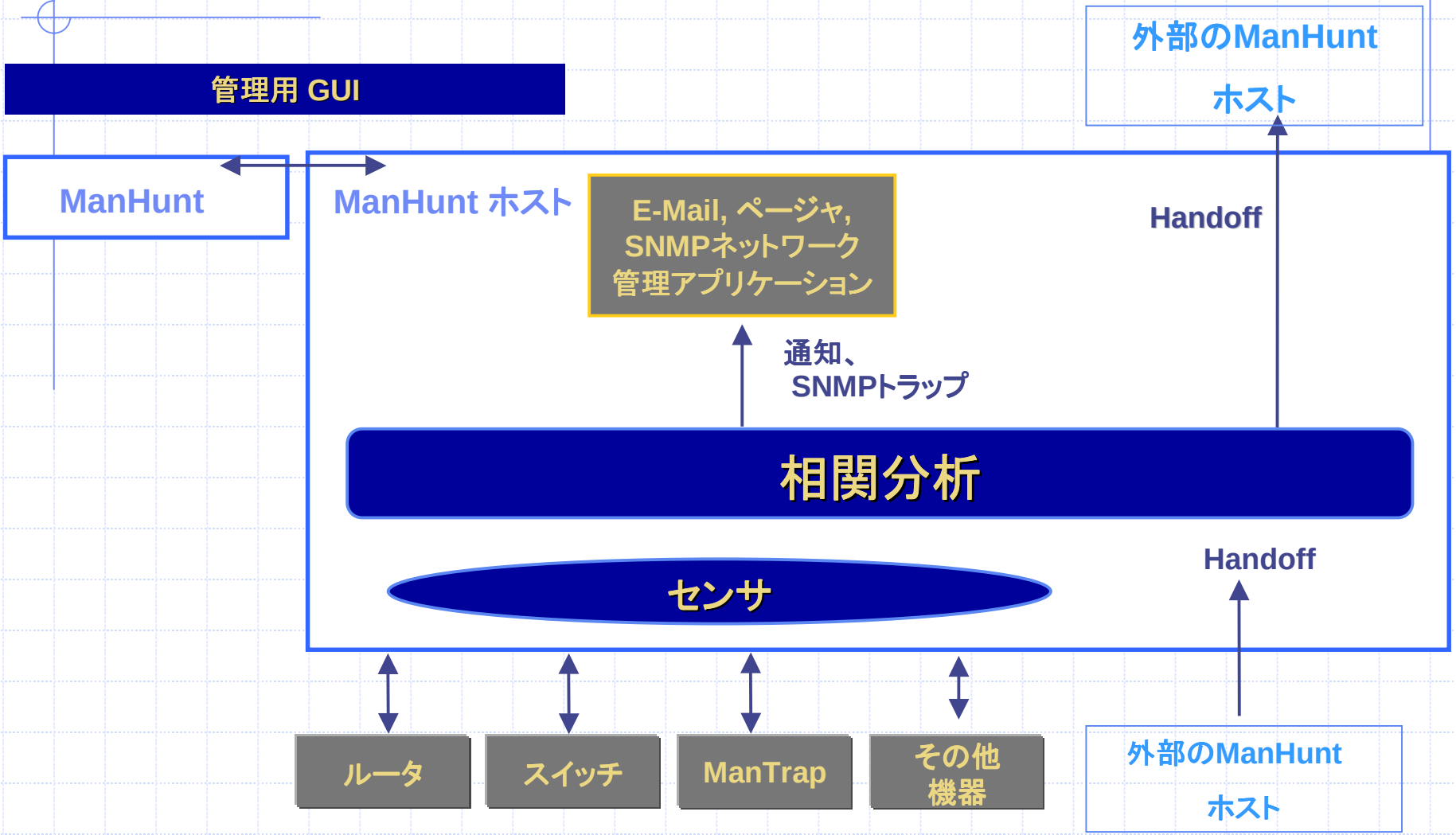
検知　->　**分析**　-> 統合

ManHunt： レスポンス

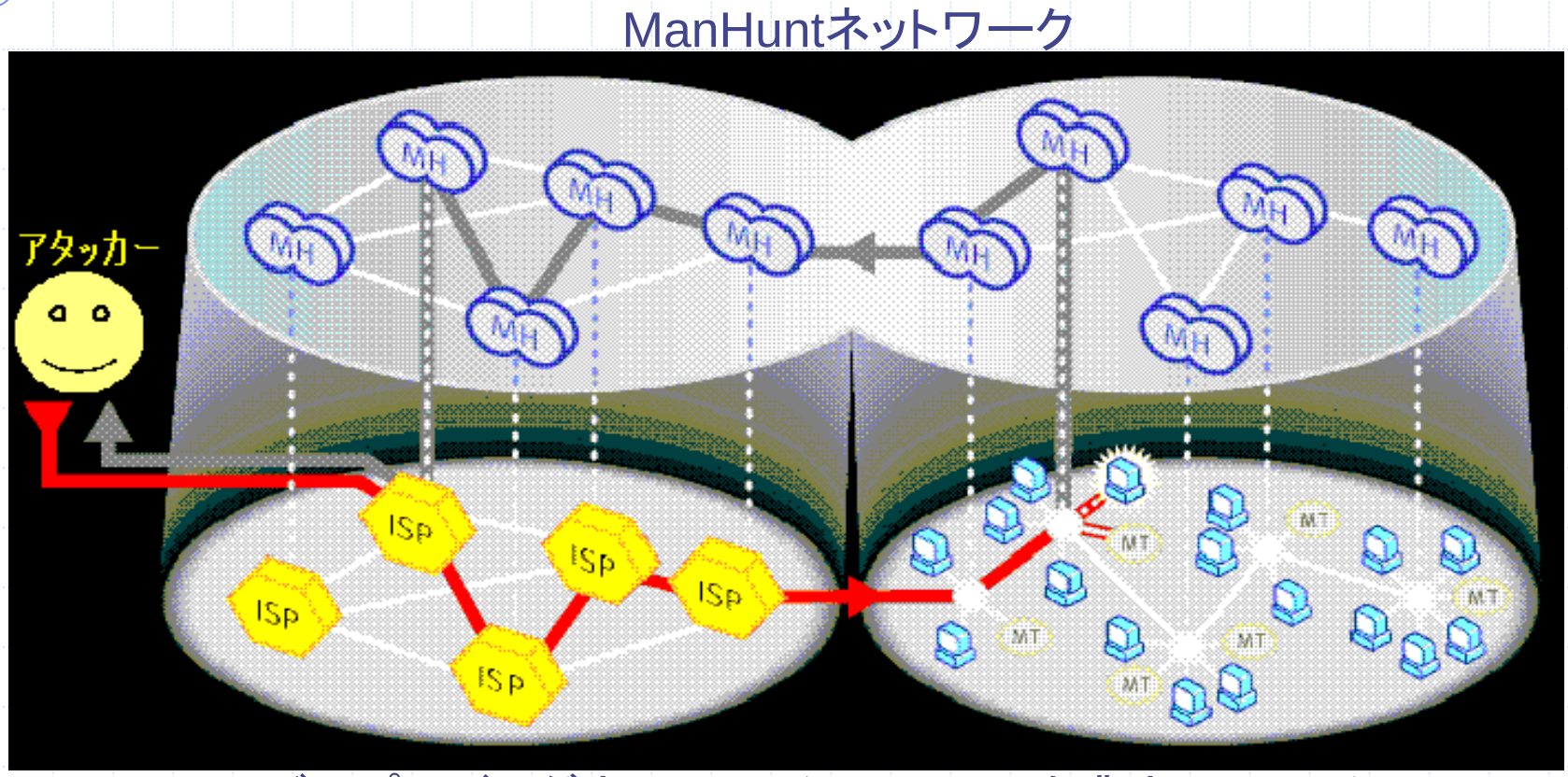
- 多様な基準に基づいたレスポンス設定
  - イベント・ターゲット, アタック・タイプ, イベント・インターフェイス, 優先度
- レスポンス
  - TCP セッション切断
  - アラート ー SMTP ／SNMP
  - Track Back
    - Flowchaser ー アドレス詐称されたパケット・ソースも同定
  - Handoff
    - 調査とレスポンスの継続のため、上位プロバイダへの自動通知

検知 -> 分析 -> **レスポンス**

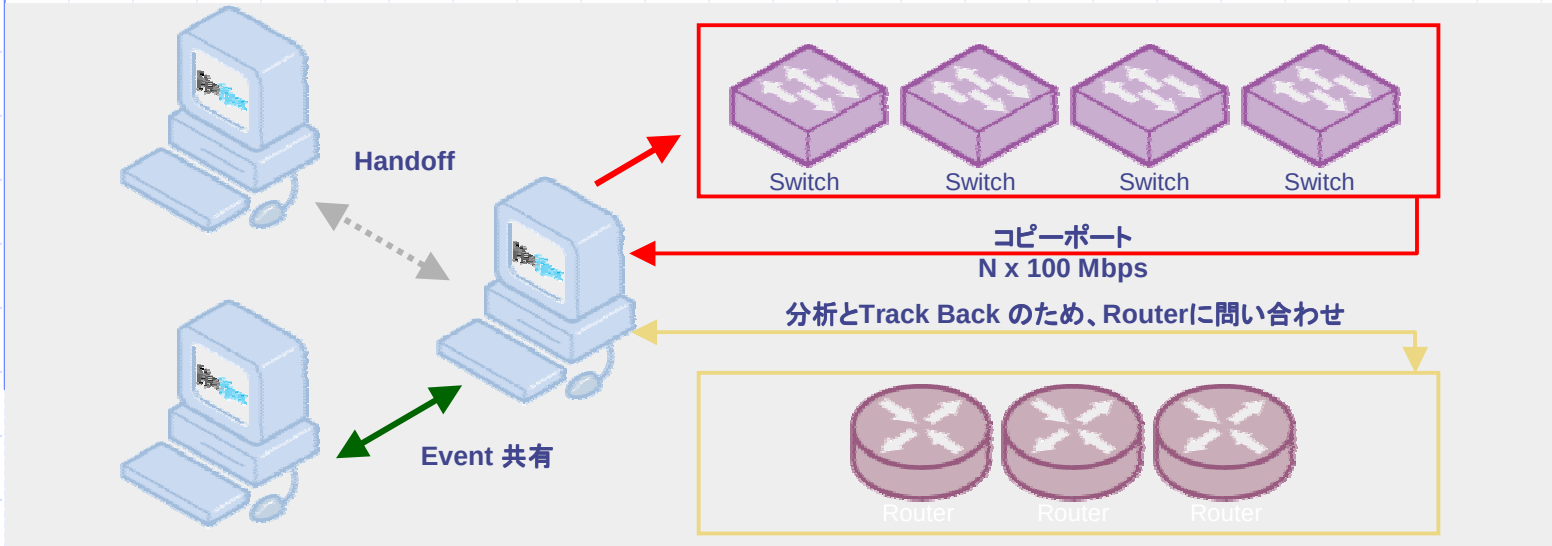
ManHunt アーキテクチャ



Track Back

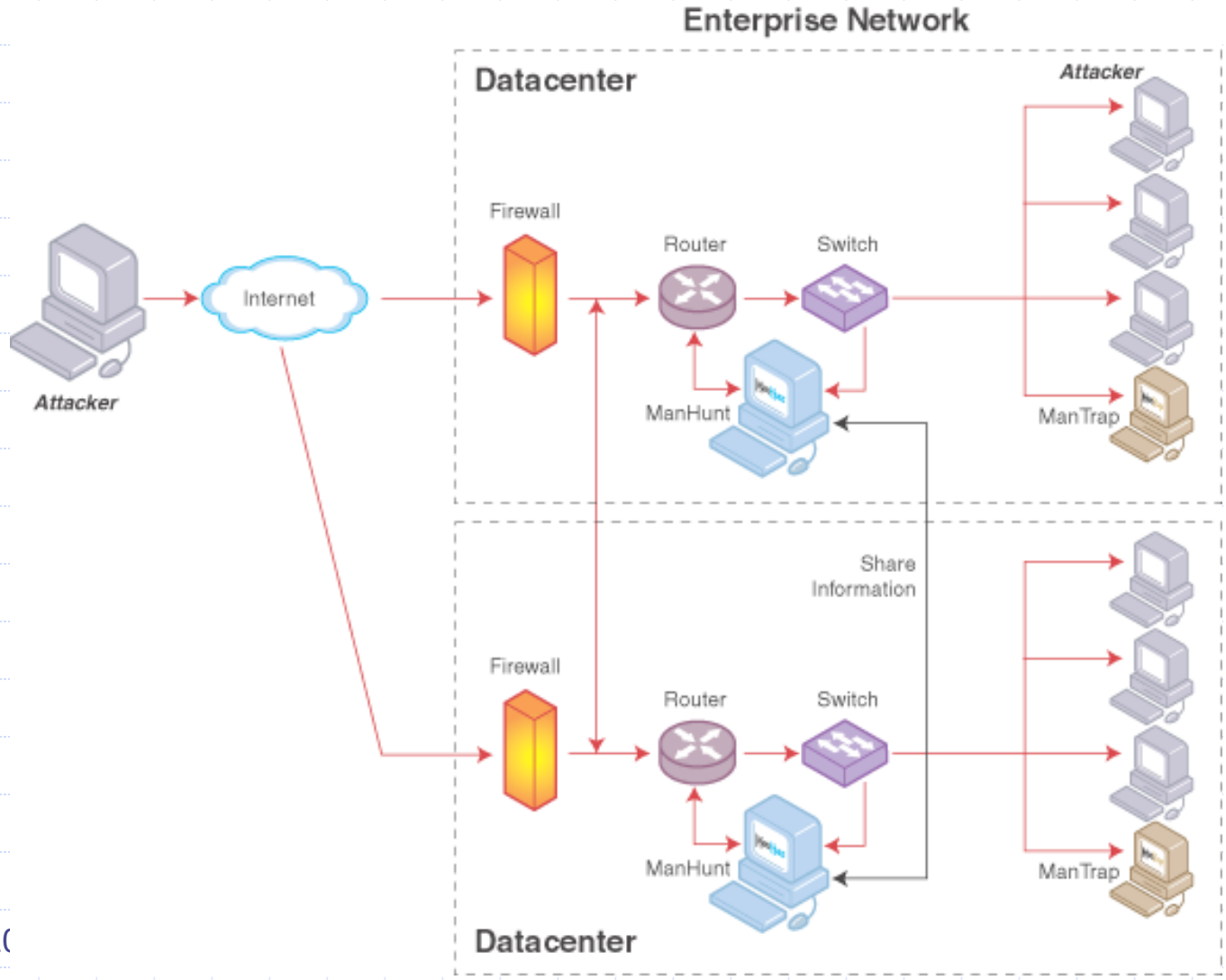


ManHunt 配置



- ルーター／スイッチと接続
  - Sun U5/E250/E450 クラス　－　ネットワーク･サイズに依存
- 監視スイッチ毎に接続
  - 1 ネットワーク･インターフェイス／デバイス
- ManHunt（管理用）通信用にネットーワーク

全社展開


Enterprise Network
Datacenter
Attacker
Firewall
Router
Switch
Internet
Attacker
ManHunt
ManTrap
Share
Information
Firewall
Router
Switch
ManHunt
ManTrap
Datacenter

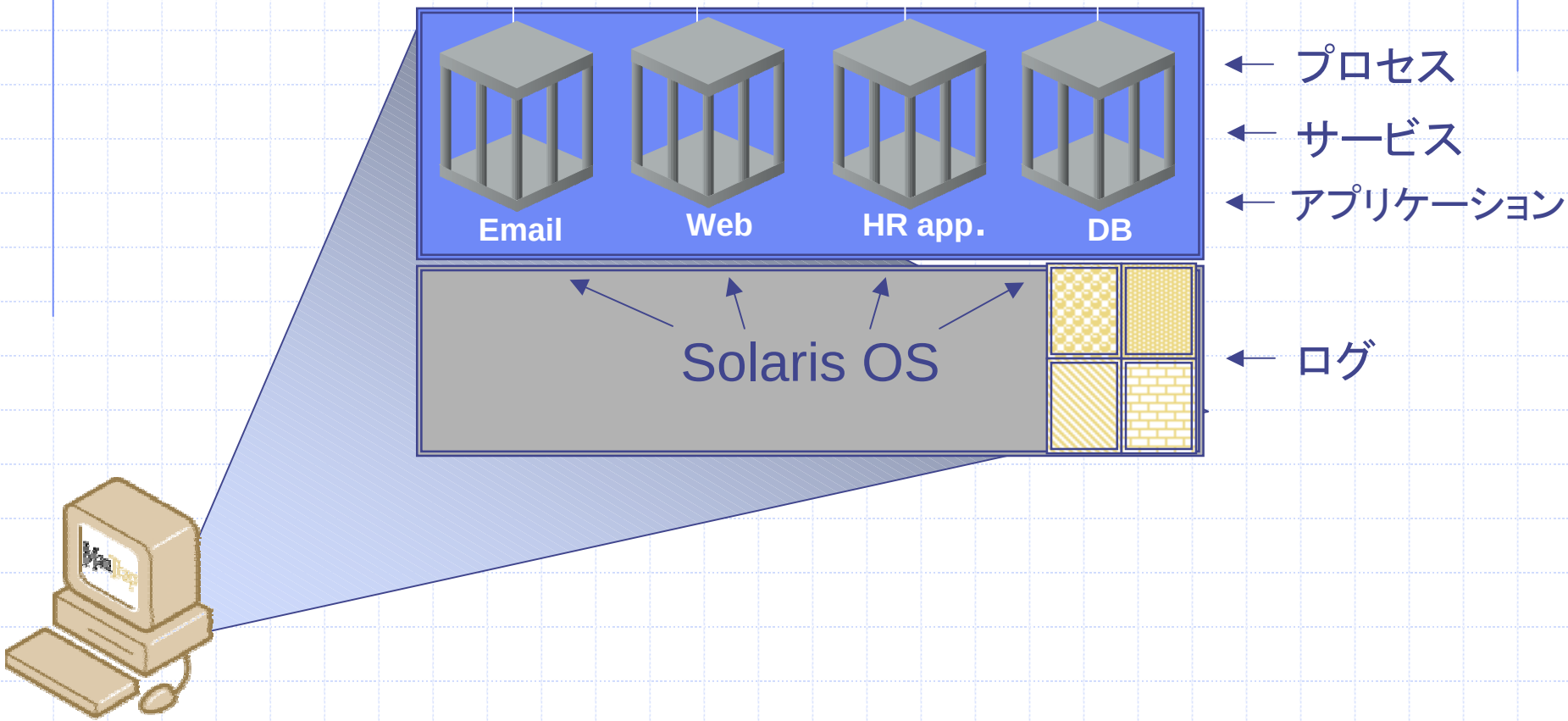
ManTrap

- ManTrap:
  - デセプション・システム
    - 信頼できるシステムを構築
  - 侵入者のアクティビティをリアルタイムに収集
  - アタックに対応する時間を提供

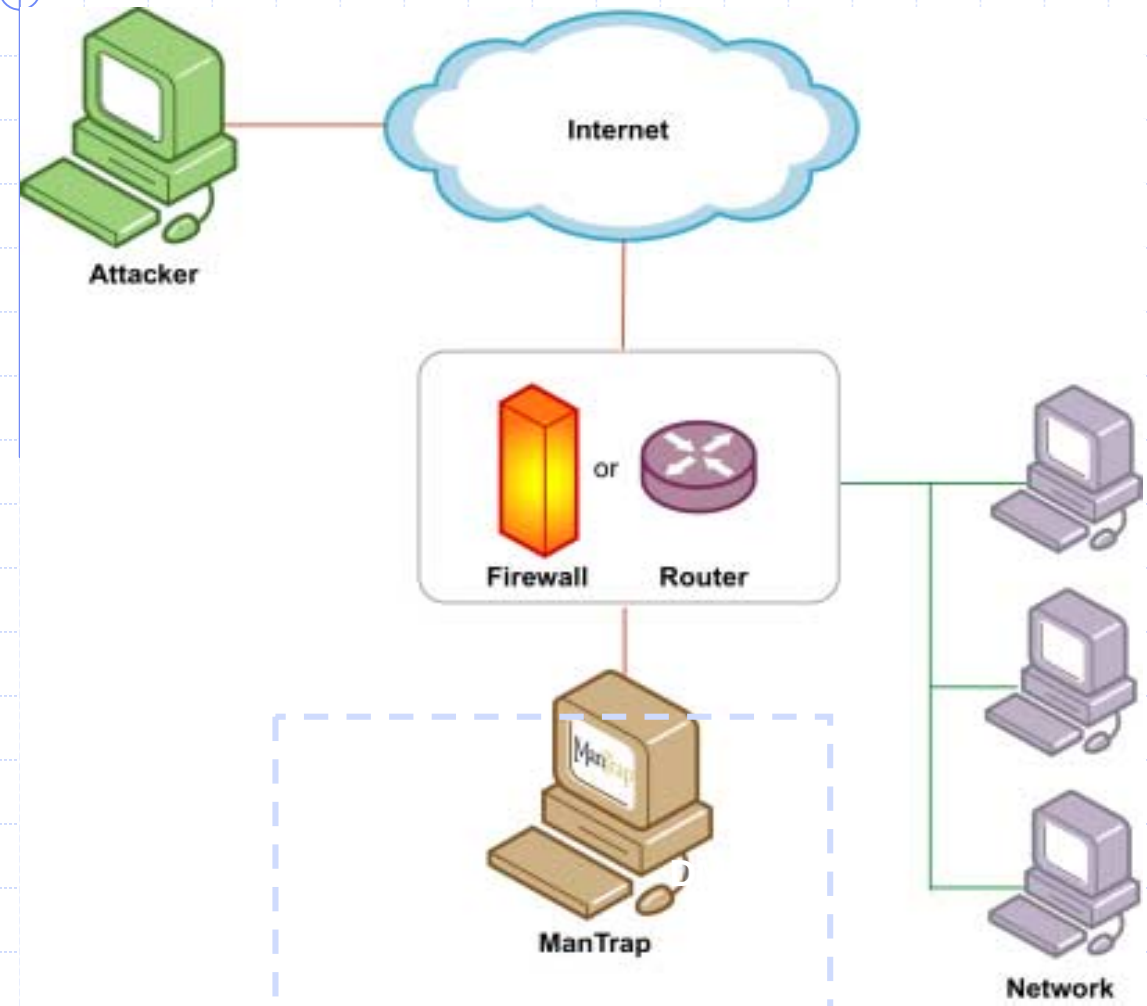
特徴

- ライブなSolaris Server
  - ‘real thing’
- 最大4 ManTrap Hosts/Server
- アラーティング設定可能
- アクティビティ・ロギング
  - アタッカーの全アクティビティを記録
- Content Generation　モジュール
  - ランダム／カスタム・コンテンツを生成　(SMTP)
- セキュア・ログ (デジタル署名)
- 複数ホスト管理
  - 複数ホスト／ケージを一箇所から管理可能
- no ‘false positives’

ケージ



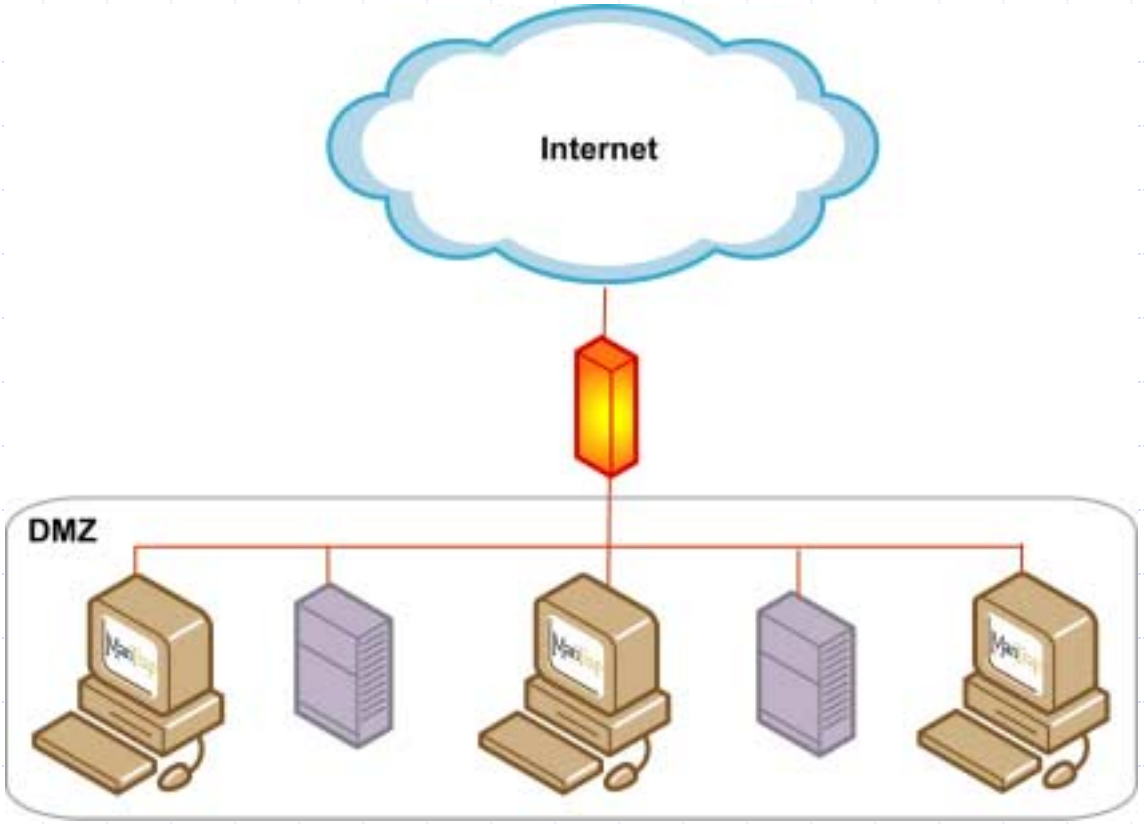
ManTrap 配置



- 疑わしいコネクションを ManTrap へ誘導
- ケージ:
  - サーバをミラー
  - DMZに配置

ManTrap 配置

- 高価値サーバ間に ManTrap を配置



デモンストレーション、Q&A