IDSの仕組みと
効果的な利用について

インターネットセキュリティシステムズ（株）

INTERNET
SECURITY
SYSTEMS

www.iss.net

IDSについて

INTERNET SECURITY SYSTEMS

- IDSとは
- IDSの利用目的
- FWを設置してもIDSは必要か
- IDSの分類

IDSについて：IDSとは

INTERNET SECURITY SYSTEMS

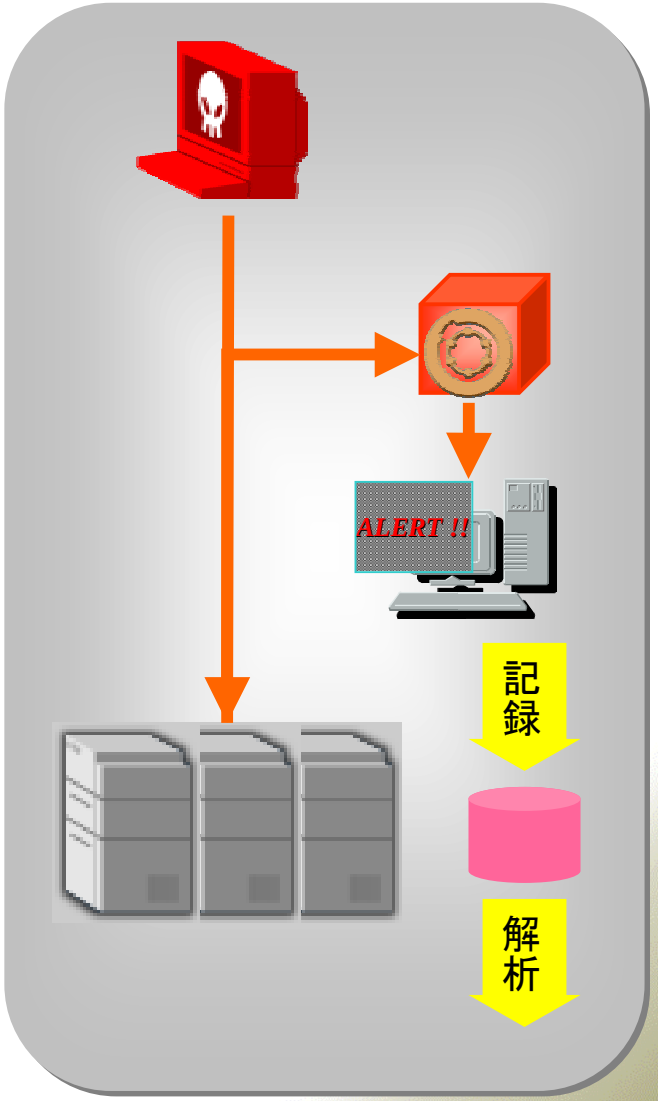
- Intrusion Detection Systemの略で、日本では「不正侵入検知装置」と呼ばれる

- コンピュータおよびネットワークに対する不正侵入を検知するためのシステムで、一般的にネットワーク上を流れるパケットから不正侵入を検知するシステム（ネットワーク型IDS）と、コンピュータ上のログやシステムコールから不正侵入を検知するシステム（ホスト型IDS）がある

IDSについて:IDSの利用目的

INTERNET SECURITY SYSTEMS

- 不正侵入の状況を把握する
  - 不正アクセスや、疑わしい挙動を記録し、サイトやホストがどのような脅威に直面しているかを把握する目的でIDSを利用する
- 不正侵入に対する迅速な対応を行う
  - サイトやホストに対する不正アクセスの兆候を検出し、侵入を防止する
  - 危険な不正アクセスを検知し、必要な対処を迅速に実施し、被害の防止や軽減を図る
- 不正侵入に関する情報を記録する
  - 不正アクセスに関連する情報を記録し、証拠として利用する



IDSについて：
FWを設置してもIDSは必要か 1/2

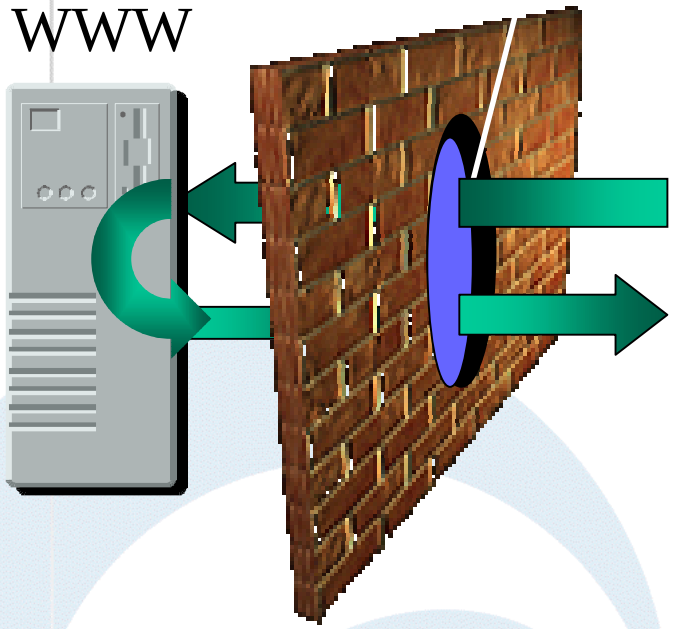
INTERNET SECURITY SYSTEMS

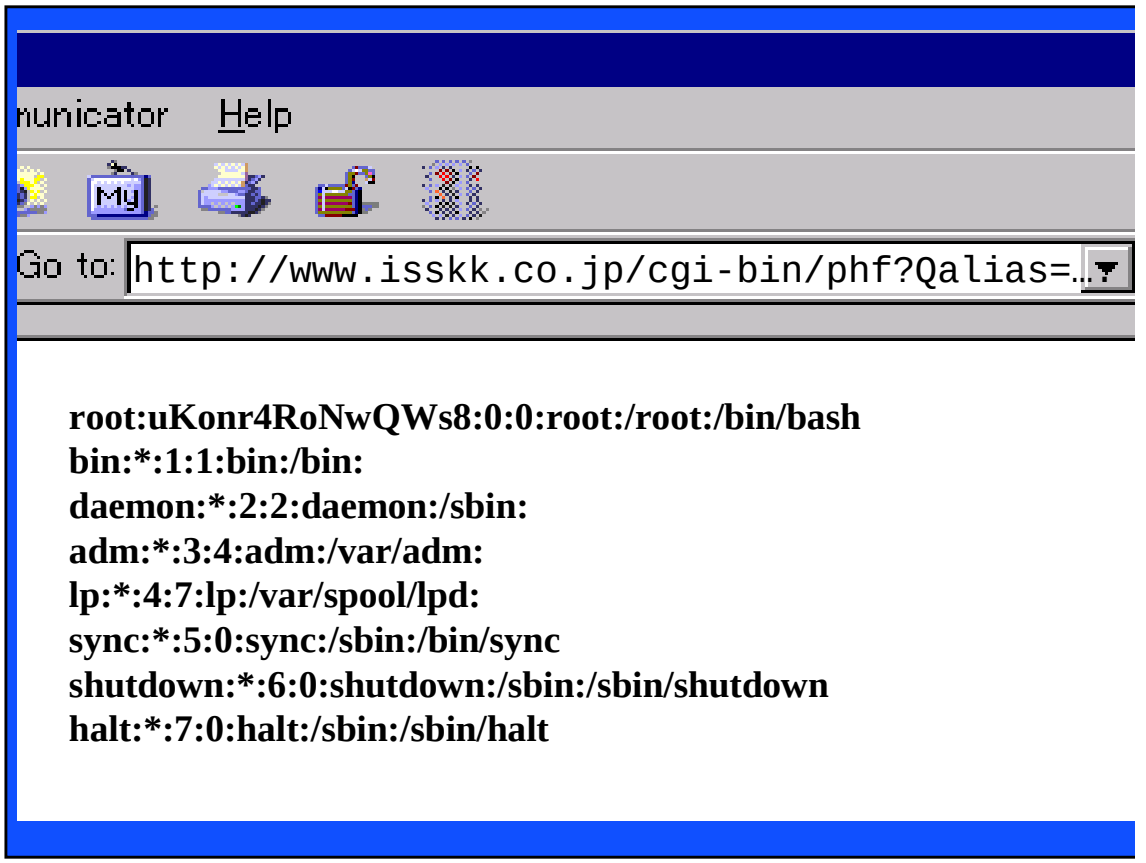
The Power to Protect

http = OK!

許可されたリクエストだが...

パスワードを取得





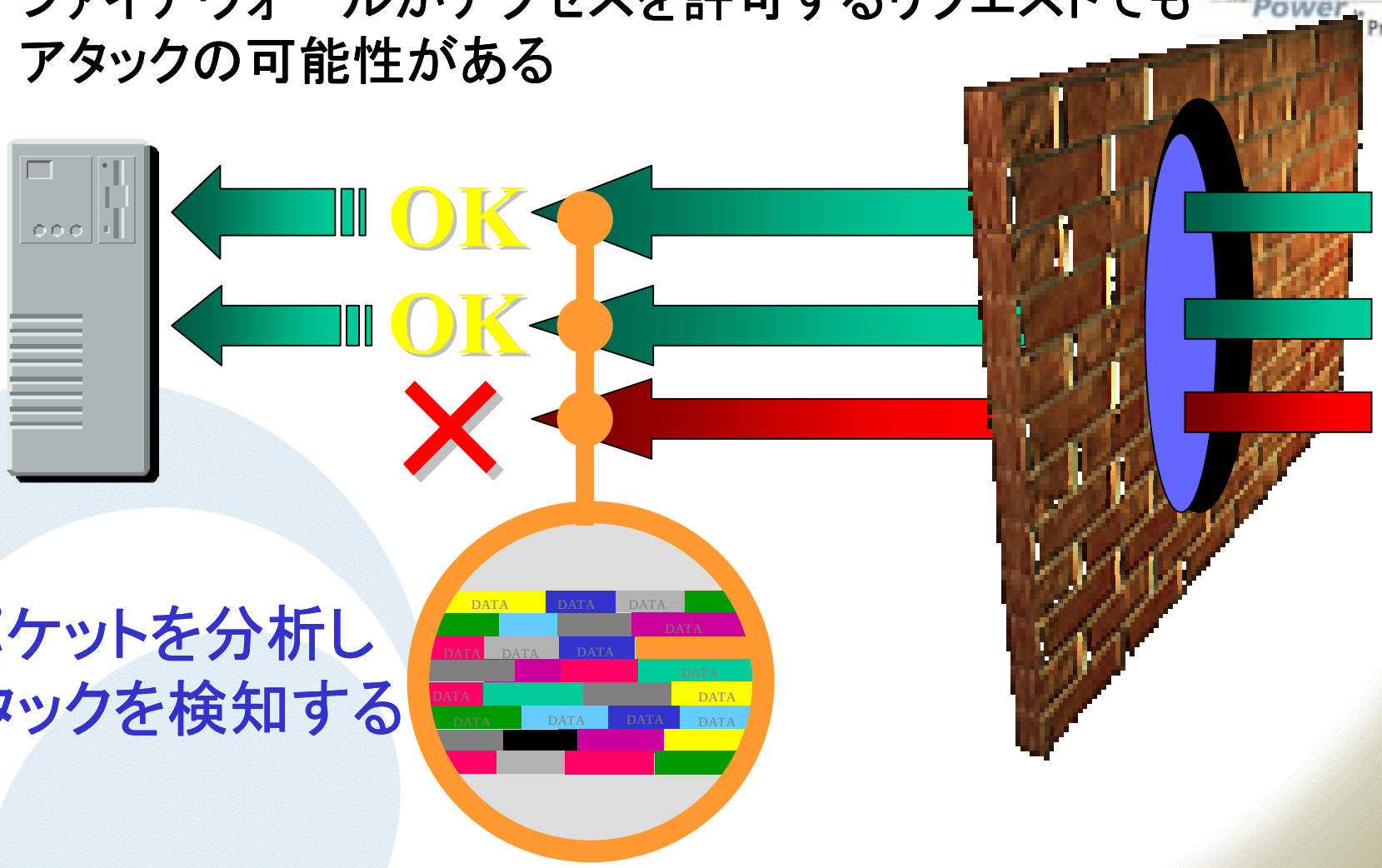
ファイアウォールは
攻撃パターンを
認識しない

IDSについて:
FWを設置してもIDSは必要か 2/2

INTERNET SECURITY SYSTEMS

The Power to Protect

ファイアウォールがアクセスを許可するリクエストでも
アタックの可能性がある



パケットを分析し
アタックを検知する

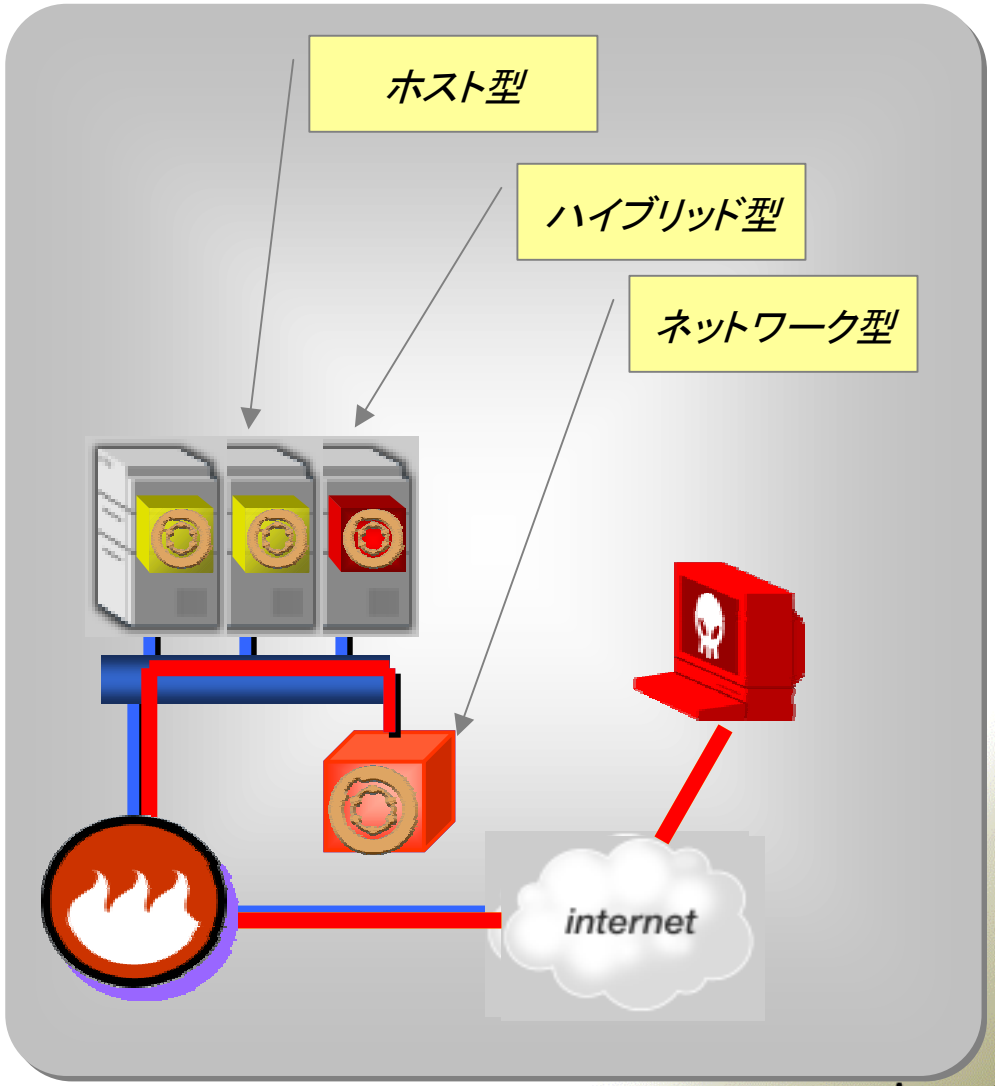
IDSについて：
IDSの分類（形態からの分類）

INTERNET SECURITY SYSTEMS

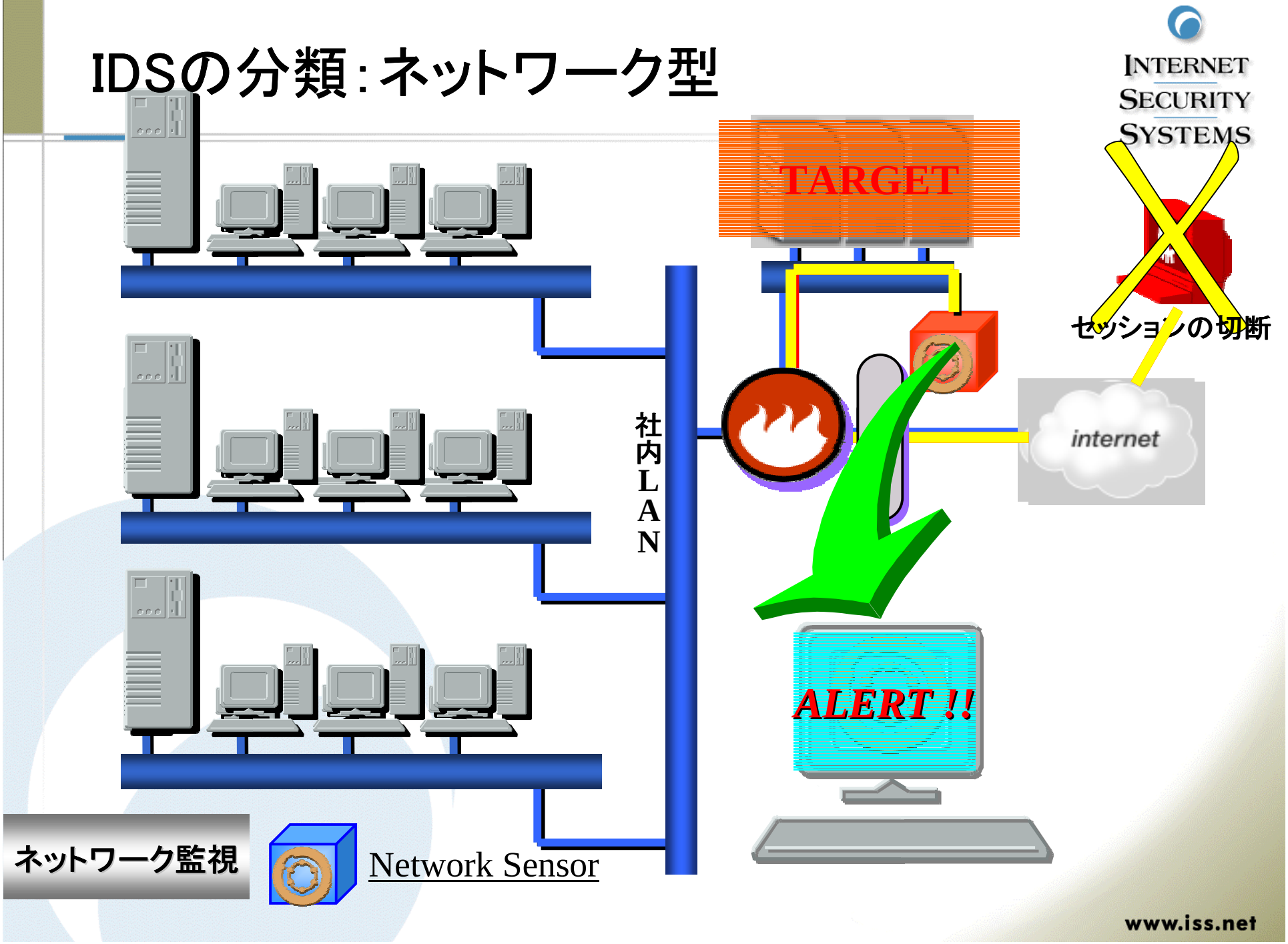
- IDSの主な形態として以下のものがある

  ここでは、それぞれのIDSの基本的な動作を解説する

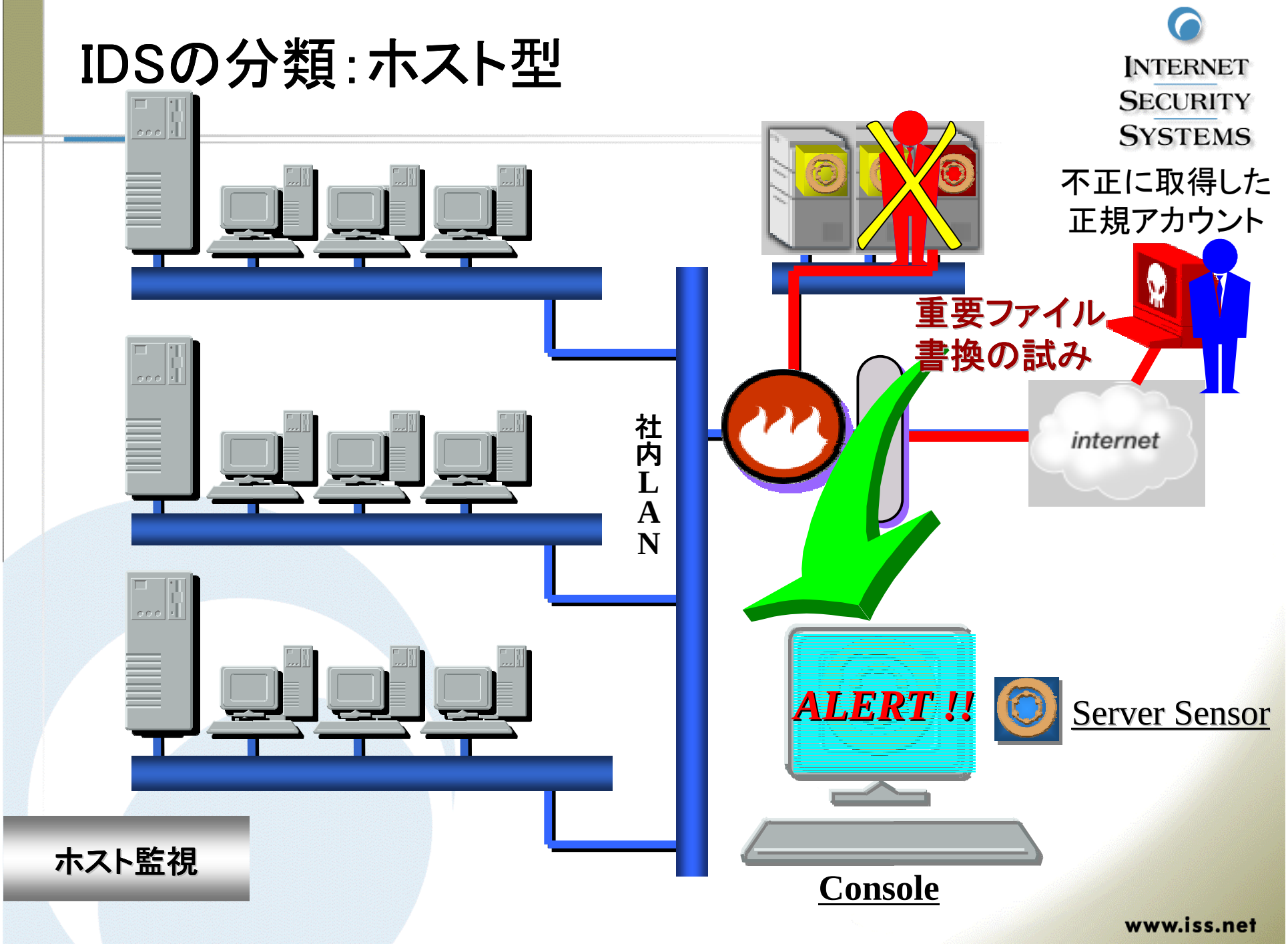
  - ネットワーク型
  - ホスト型
  - ハイブリッド型



IDSの分類：ネットワーク型



IDSの分類：ホスト型


INTERNET
SECURITY
SYSTEMS
不正に取得した
正規アカウント
重要ファイル
書換の試み
社内LAN
internet
ALERT !!
Server Sensor
Console
ホスト監視
www.iss.net

IDSの分類：ハイブリッド型

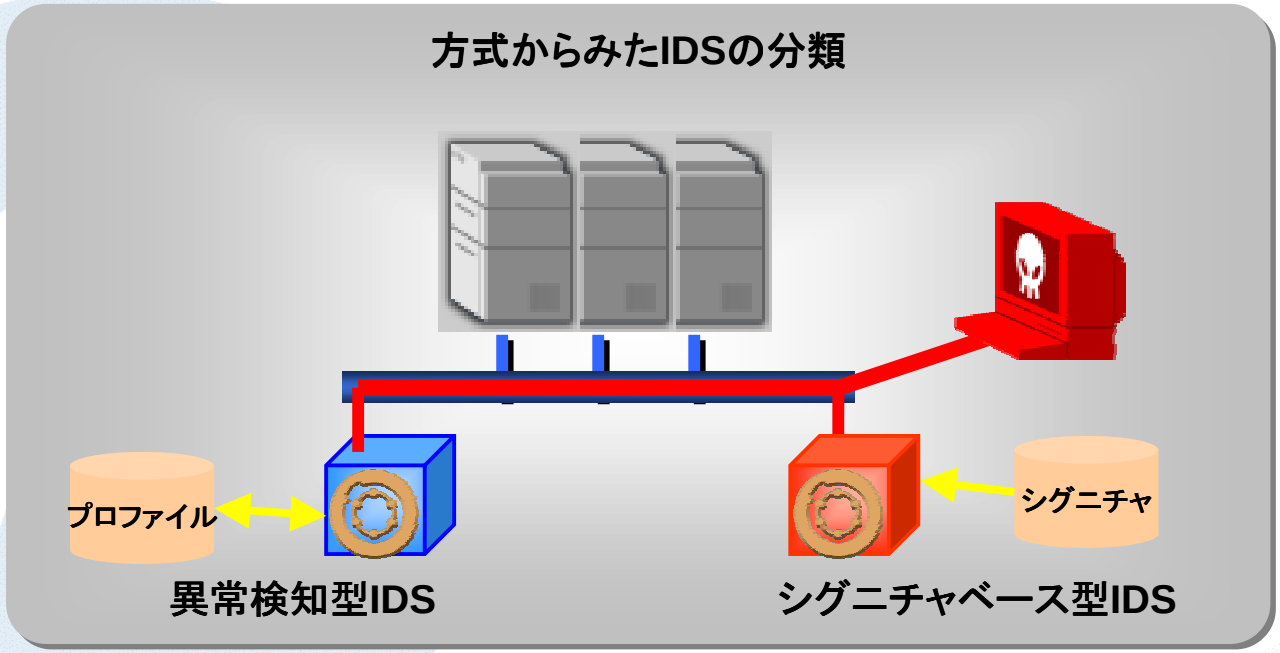
INTERNET SECURITY SYSTEMS

ログを分析し
アタックを検知する

IDSの分類（方式からの分類）

INTERNET SECURITY SYSTEMS

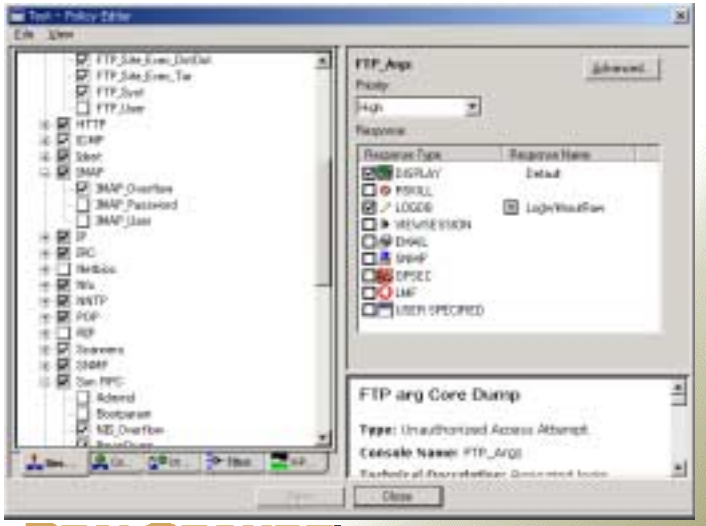
- 不正アクセスの検知手法に以下のものがある
  ここでは、それぞれの検知方法の特徴について解説する
  - シグニチャ（パターン・ルール）ベース
  - 異常検知（Anomaly Detection / Misuse Detection）



IDSの分類：シグニチャベース

INTERNET SECURITY SYSTEMS

- シグニチャ（パターン）を利用した不正アクセス検出
  - 概要
    - 現在実用的に利用されているほとんどIDSがこのタイプ
    - 特に、ネットワーク型は、シグニチャベースが多い
  - 利点
    - 検出精度にかなりの正確性がある
    - 新しいアタックに対して、迅速なシグニチャのアップデートが行われている製品がある
  - 課題
    - 未知のアタックを検出することは難しい



IDSの分類：異常検知 1/2

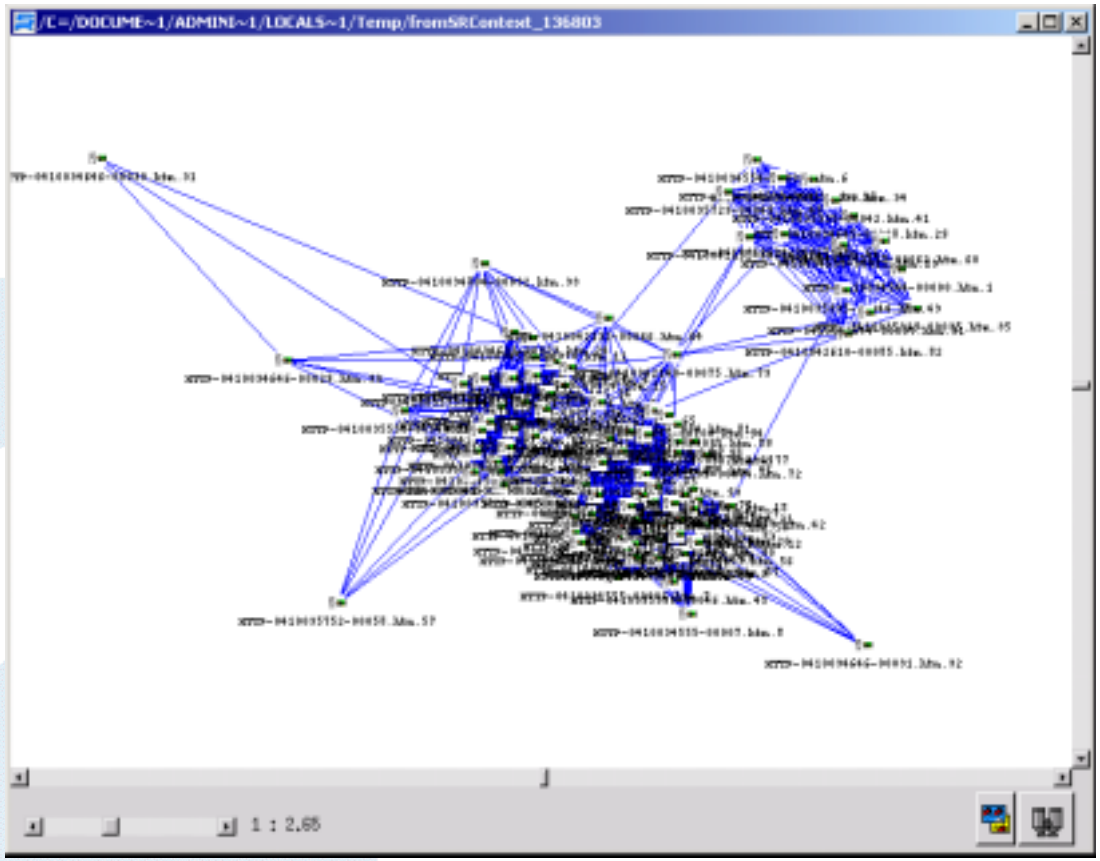
INTERNET SECURITY SYSTEMS

- 通常と異なるパターンから異常を検出検出
  - 概要
    - ユーザの振る舞いやトラフィックの状況から正常と異なる振る舞いを、異常として検出する
    - ホスト型のIDSは、ある種以上検知型であることが多い
  - 特長
    - 未知のアタックを検出することができる
    - 正常な権限で実行された不正アクセスについても検知することができる
  - 課題
    - 実用的な精度が得られない（正常を定義することが難しい）
    - 正常と異常の境界値の設定が困難
  - その他
    - 簡単な異常検知は、シグニチャとして組み込まれていることが多い
    - 異常検知（Anomaly Detection)に対応しているIDSも、シグニチャベースと同様の単純な異常検知のみ行っていることもある

IDSの分類：異常検知 2/2

INTERNET SECURITY SYSTEMS

- ネットワークパターン分析による異常検知の例



SilentRunner™

IDSの課題

INTERNET SECURITY SYSTEMS

- ネットワークの高速化・複雑化
- 暗号化
- 未知のアタックの検知
- 検知精度
- 不正アクセスに対する動的な対応

IDSの課題：
ネットワークの高速化・複雑化

INTERNET SECURITY SYSTEMS

- ネットワークの高速化

  ローカルセグメント：　10M -> 100M -> G

  インターネット接続：　1.4K-> 64K-> 1.5M -> 100M

  – ネットワーク型のIDSにとって、ネットワークの高速化に追従することは大きな課題となっている。
    - IDSの高速化やロードバランシングよって対応している
    - ハイブリッド型のIDSによる解決も図られている

- ネットワークの複雑化

  スイッチセグメント　　アクセスコントロール

  冗長構成　　ロードバランシング

  – ネットワークIDSはコリジョンドメインにおけるパケットキャプチャリングが基本となっているため、これらの構成では単純には配置できない
    - ミラーポートやTAPなどを使って対応している
    - ハイブリッド型による解決も図られている

IDSの課題：暗号化

INTERNET SECURITY SYSTEMS

- SSLやIPsecなど暗号化されたパケットはネットワーク型のIDSでは解析できない
  - 暗号化された通信や、トネリングされた通信においては、ネットワーク型のIDSが解析を行う事ができない
  - ネットワーク型IDSとホスト型IDSのハイブリッド型
    - ホストベースのIDSに、ネットワーク型のIDSの機能を追加したハイブリッド型のIDSが発表されている。
  - このタイプのIDSは、以下の特徴的な機能を持つ
    - ホストのパケットキャプチャ部において、通常のパケットに対する解析を行う
    - アプリケーションの最下層部において、復号化されたパケットの解析を行う

IDSの課題：未知のアタックの検知

INTERNET SECURITY SYSTEMS

- 新たな手法が次々と開発されている

  シグニチャベースのIDSでは、この状況に迅速な対応が行えない

  – シグニチャベースIDSの対応
    - シグニチャの迅速な配布
      – シグニチャ部分をプログラムから独立させ、シグニチャだけの配布を行うことで、迅速な対応を図っている
  – 異常検出（Anomaly / Misuse Detection）の試み

    通常とは異なる状態を検知することで、不正アクセスを検知する試みが行われている
    - 正確な解析を行うためには、膨大な情報の蓄積と、高度な統計処理が必要となる。

シグニチャの更新

RealSecure

X-press Update

IDSの課題：検出精度

INTERNET SECURITY SYSTEMS

- IDSには誤報がつきもの

  IDSは、障害検知とことなり、ある程度の誤報を避けることができない

  – 運用におけるアプローチ
    - IDS利用の目的により、検出シグニチャをコントロールする

  – プロダクトのアプローチ
    - 脆弱性検査と不正侵入検知（IDS）の連携
      – システム上脆弱ではないアタックと、脆弱点を突いたアタックを区別する
      – この区別を行うため、脆弱性検査の結果をIDSに取り込む試みが行われている。

IDSの課題：動的な対応

INTERNET SECURITY SYSTEMS

- 不正アクセスを検知するだけではなく対応が求められる場合がある

  セキュリティ技術者の絶対数が少ない事や、迅速な対応を図るといった理由から、IDSが不正アクセスを検知した際に、不正アクセスを中断させる事が試みられている

  - 動的な対応（ダイナミックディフェンス）の種類
    - Kill Session, Firewallとの連動、パケットのドロップなど
  - 動的な対応（ダイナミックディフェンス）を行う際の注意点
    - 検出の精度
    - 対応効果（UDPに対しては、Kill Sessionは効果が無い）
    - 正常な通信に対する影響

IDSの今後の動向について

INTERNET SECURITY SYSTEMS

- 管理機能の強化
  - 大量のセンサのハンドリング
    - 大規模なシステムにおいて多数のIDSを利用するケースや、ネットワーク型・ホスト型を併用するケースが増えている。
  - 脆弱点と脅威の管理
    - システムに有効なアタックのみに焦点をあてる事を目的として、脆弱性検査の結果を自動的にIDSに反映する仕組みが必要
- IDS以外の装置との連携
  - 動的な対応（ダイナミックディフェンス）に対する要望は、今後より強くなると考えられる。

IDSの利用

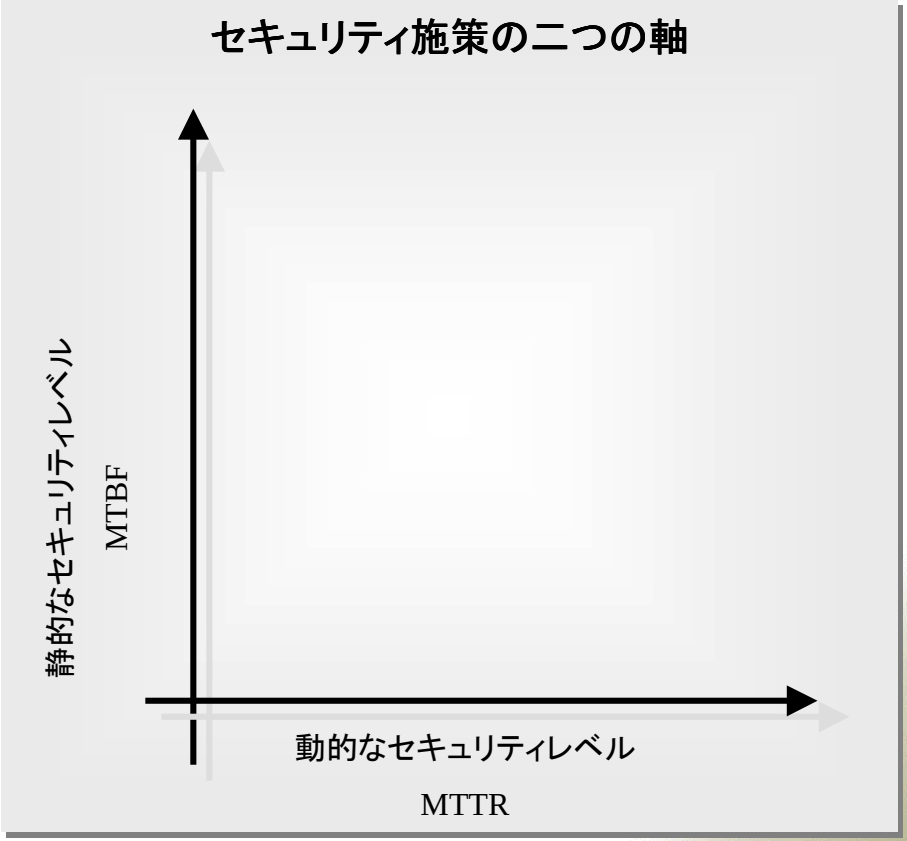
INTERNET SECURITY SYSTEMS

- IDSを利用する際の基本的な考え方
- 効果的な配置
- キャパシティプランニング
- 検知におけるフレームワーク
- 動的な対応について

IDSの利用：
IDSを利用する際の基本的な考え方

INTERNET SECURITY SYSTEMS

- IDSは、一般的な意味でのセキュリティレベル（静的なセキュリティレベル：MTBF）の向上に寄与しない。
- IDSは、不正アクセスに対する迅速な対応を行う事（動的なセキュリティレベル：MTTR）の向上に寄与する技術である。

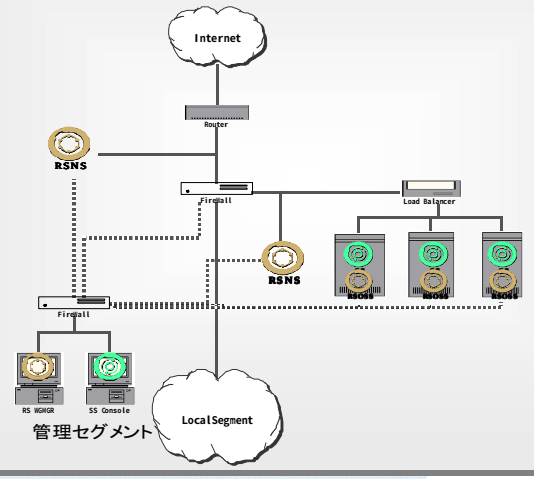


IDSの利用：効果的な配置

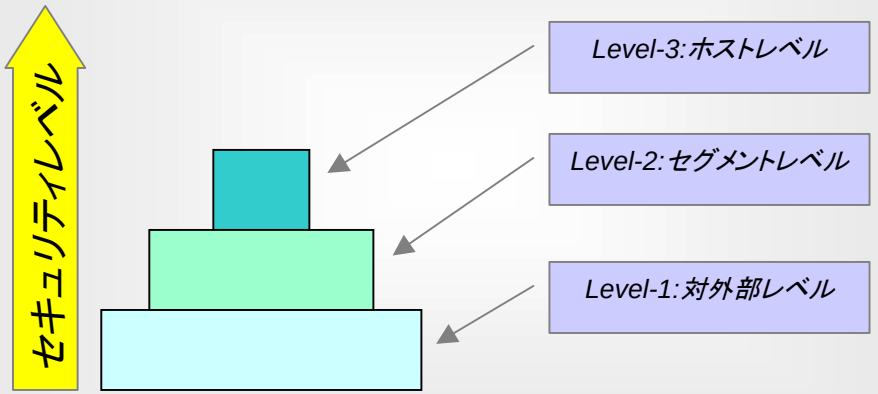
INTERNET SECURITY SYSTEMS

- IDS利用の目的から配置を考える
  - 傾向の分析を行うか、インシデントの対応を行うか＝＞FWの内側、外側など
- 必要とするセキュリティレベルから配置を考える
  - ネットワーク型、ホスト型、ハイブリッド型など
- ネットワークの特性に合わせて配置を考える
  - 高速ネットワーク、スイッチセグメント、ロードバランシングなど

IDSの配置例



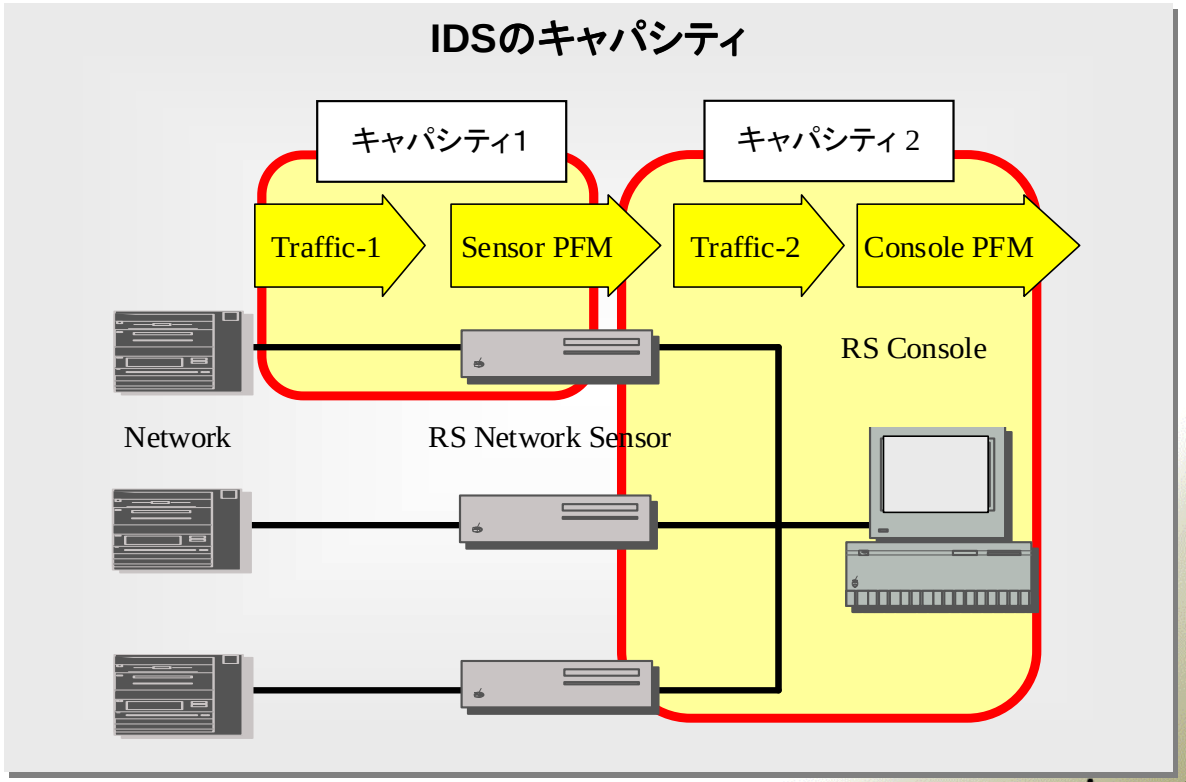
セキュリティレベルとIDSの適用



IDSの利用：
キャパシティプランニング

INTERNET SECURITY SYSTEMS

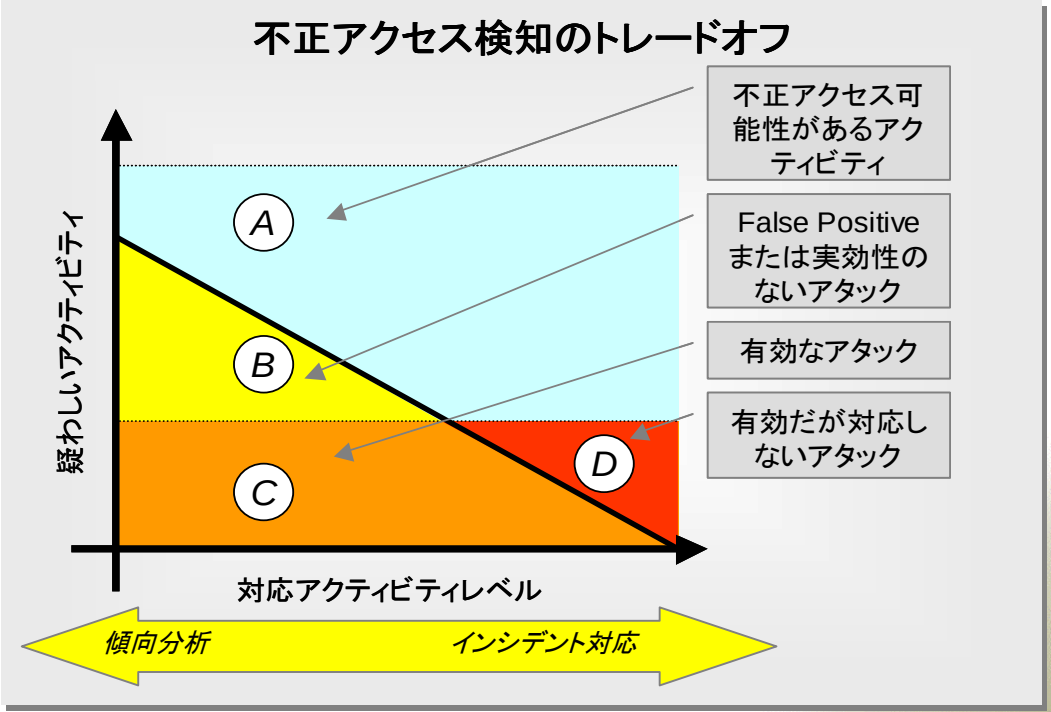
- IDSのキャパシティ
  - センサーのキャパシティ（ポリシ設定・ロードバランシング）
  - センサと管理コンソールのキャパシティ



IDSの利用：
検知におけるフレームワーク 1/2

INTERNET SECURITY SYSTEMS

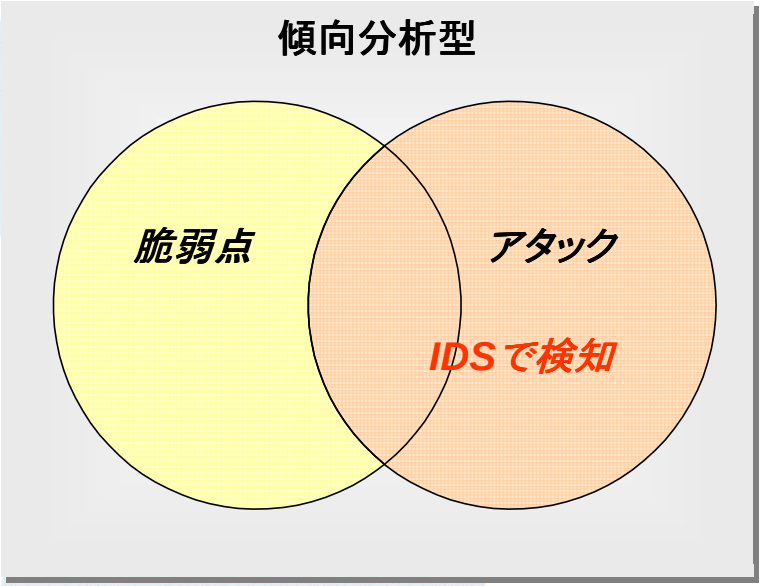
- IDSの主たる目的として以下の二つが存在する
  - 傾向分析型の利用
  - インシデント対応型の利用

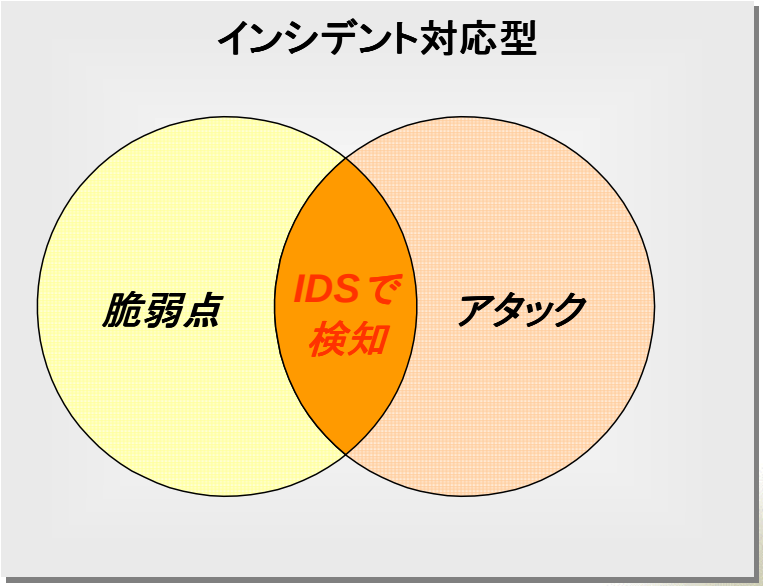


IDSの利用：検知におけるフレームワーク 2/2

INTERNET SECURITY SYSTEMS

- 傾向分析型
  - アタックや疑わしいアクティブティをできるだけ記録する
- インシデント対応型
  - 脆弱点に対するアタックに焦点をあてて検出する

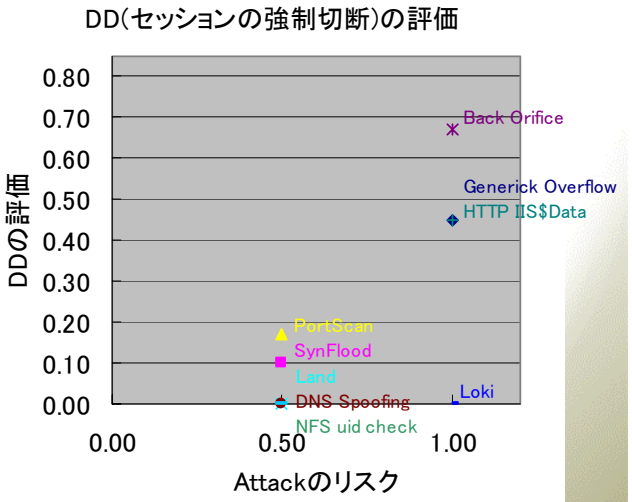




IDSの利用：
動的な対応について

INTERNET SECURITY SYSTEMS

- 動的な対応（ダイナミックディフェンス）
  - ダイナミックディフェンスを行うにあたっては、以下の観点から対応を評価する
    - 検出の精度
    - 対応効果（UDPに対しては、Kill Sessionは効果が無い）
    - 正常な通信に対する影響
  - 動的な対応とあわせて人員・組織面に置ける対応も同時に設計する必要がある。



JNSA ダイナミックディフェンスWG

まとめ

INTERNET SECURITY SYSTEMS

- IDSで直接的なセキュリティレベルは向上しない
  - セキュリティのMTBFとMTTR
- IDSを利用するにあたっては目的を明確にする
  - 傾向分析・解析 / インシデント対応
- 目的に応じたIDSを導入する
  - ネットワーク型、ホスト型、ハイブリッド型
  - シグニチャベース、異常検出
- 目的とセグメントに応じたキャパシティプランを行う
  - センサーのキャパシティプラン
  - センサと管理コンソールのキャパシティプラン

INTERNET SECURITY SYSTEMS

mtakahashi@isskk.co.jp

Director of Professional Service Organization