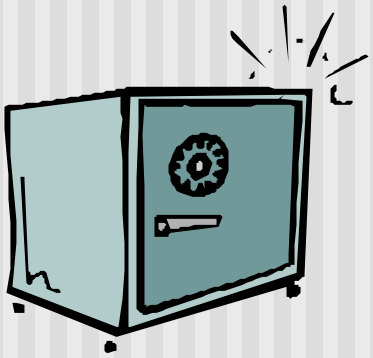
IIJ Internet Initiative Japan

IIJネットワーク侵入検知サービス

IIJ Network Intrusion Detection Service

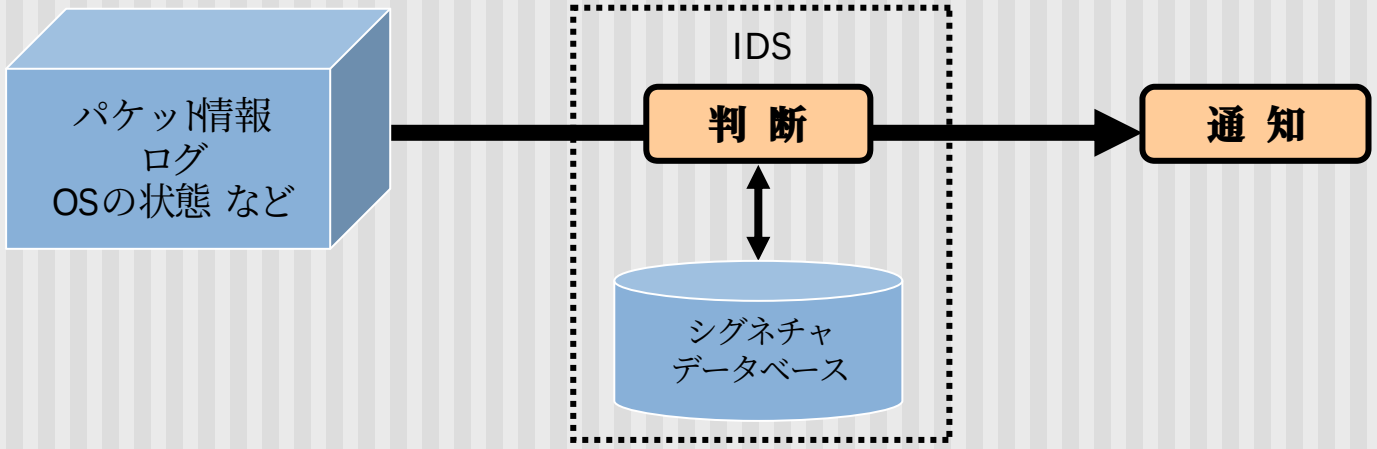
IDS: Intrusion Detection System / 侵入検知システム

- IDSの役割
  - 不正侵入(第三者によるシステムへの侵入、悪用)や
    サービス妨害攻撃の検出
  - 不正侵入の情報の記録
- IDSの仕組み
  - 知識に基づく検知 (misuse detection): signature
  - 挙動に基づく検知 (anomaly detection): profiling
- IDSの必要性
  - ファイアウォールがあればIDSは不要か
    - 誰でも触りたい放題の金庫は安全か」



IDS: Intrusion Detection System / 侵入検知システム

- IDSの種類
  - ホストベースのIDS
    - 特定のホストにおける通信やOS、アプリケーションの状態を監視する
  - ネットワークベースのIDS
    - ネットワーク上を流れるパケットを監視する
- IDSの基本的な動作

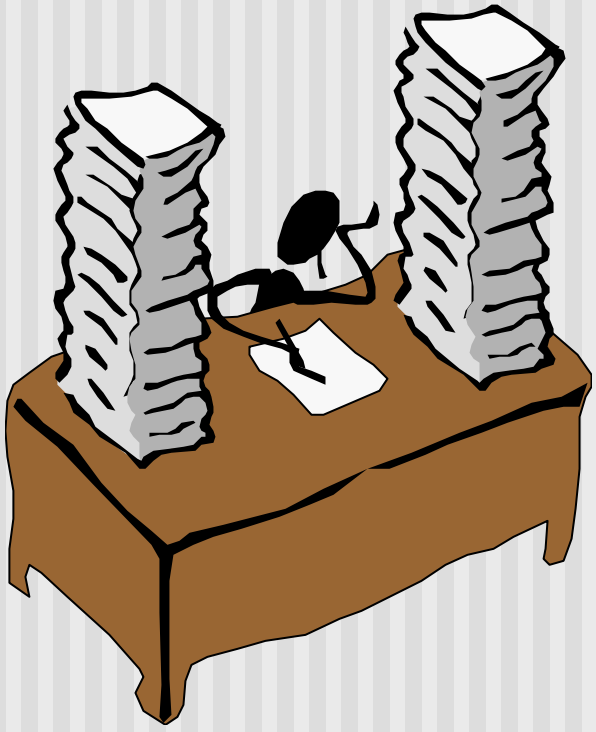


IDS: Intrusion Detection System / 侵入検知システム

- IDSの問題点
  - 検知の誤り
    - 誤検知 (false positive): 正常な現象を異常と判断してしまう
    - 検出漏れ (false nagative): 異常な現象を正常と判断してしまう
  - 情報の質と量
    - たくさんの警告
    - 情報を整理できているか
    - 実際の現象を的確に示しているか
    - 結局は人による検査が必要
  - 動作の負荷
    - Signatureの数 = 検査処理の量
    - 負荷予測が非常に困難

マネージドIDSサービスの必要性

- IDSの運用管理
  - 導入
    - 環境に合わせたシグネチャ定義
    - システムのチューニングが必要
  - 運用
    - アラート情報の重要度の判断
    - 重要度にあわせた対応
    - 対応(なにをすべきか)の意思決定
    - 安全かつ効果的な運用管理



IIJネットワーク侵入検知サービス

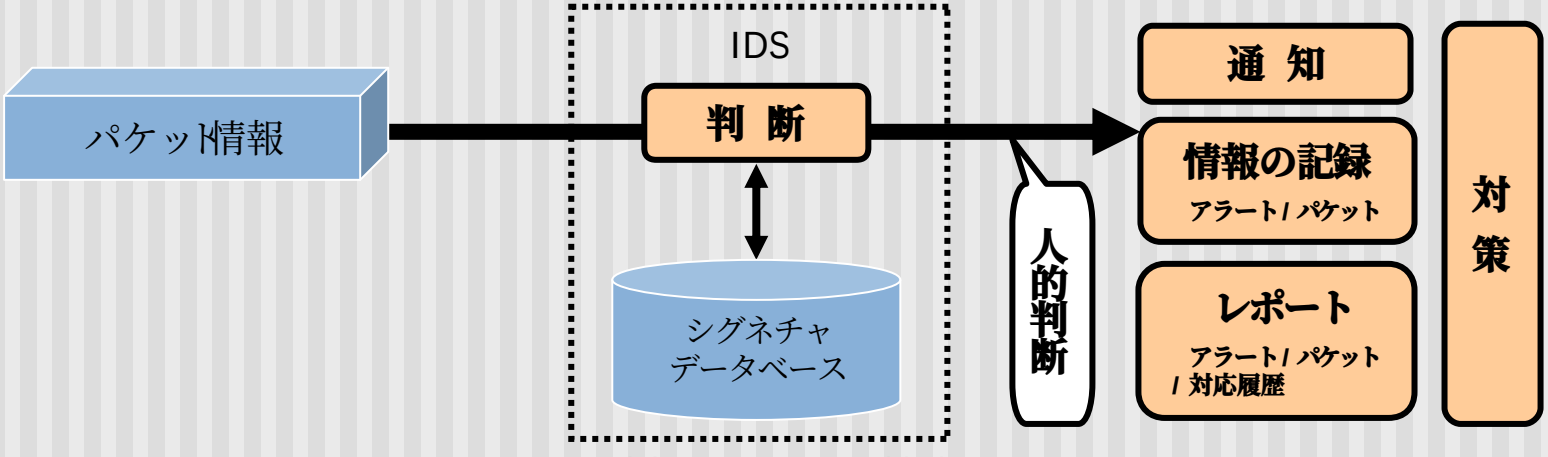
- 背景
  - 製品評価
    - 1997年～
    - NFR (Network Flight Recoder)
      - http://www.nfr.com/
      - VAR (Value Added Reseller)
        - full source code
        - IIJでの開発
  - サービス展開
    - 1998年～
    - NS-M: IIJネットワークセキュリティサービス モニタリング
    - 事実上、個別開発サービスとして提供していた

✓ signatureの全面見直し
✓ 警告の元となる通信のパケット情報を保存する機能
✓ リモートマネージメント機能
✓ レポート機能の拡張
など多くの改良

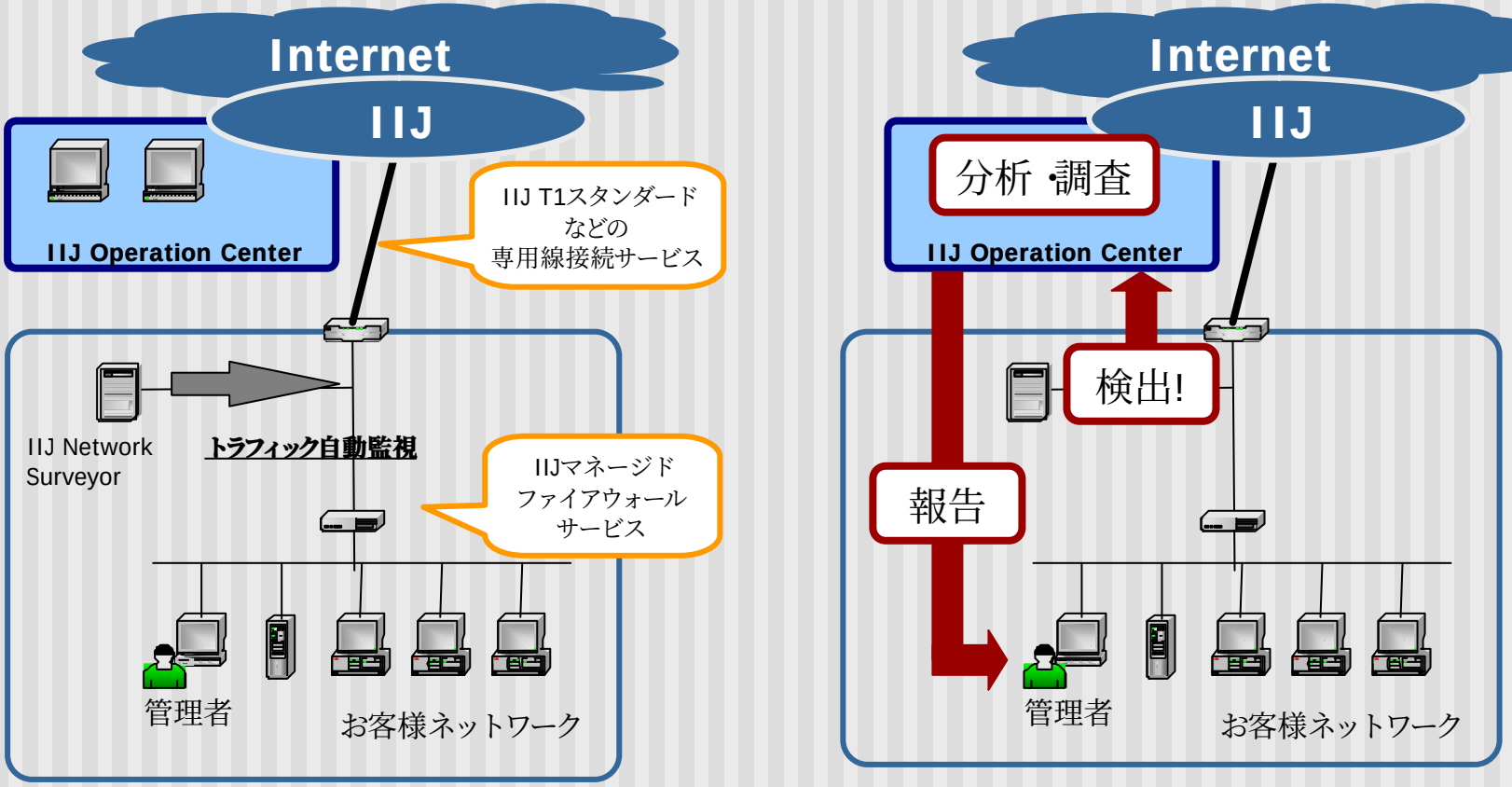
IIJネットワーク侵入検知サービス

- サービス概要
  - お客様側ネットワークにIDSを設置し、インターネットからの 脅威を監視
  - リモートによる運用管理、24時間365日の監視体制
  - 不正アクセスを検出した場合、アラートとして報告
  - IIJマネージドファイアウォールサービスとの連携による対応
  - Webインタフェースによるレポート

- IIJネットワーク侵入検知サービスの基本的な動作



サービスイメージ



IIJネットワーク侵入検知サービス

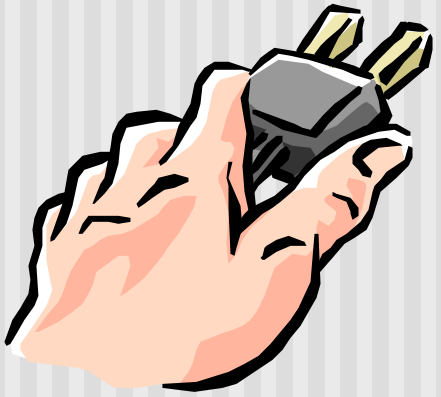
- サービスの特徴とメリット
  - システム：「IIJ Network Surveyor」
    - 多くの導入実績と高信頼性を誇る米NFR Security, Inc.のNFR Network Intrusion Detection(NFR NID)をベースとし、IIJにて拡張を加えた独自システム
  - 検出した不正アクセスに関連するパケットだけでなく、それに対するネットワーク機器の反応を検査し、対応の緊急度合いを適切に分類
  - 検出した不正アクセスの通知だけでなく、関連したパケット情報を記録
    - 事後の解析や証拠保全に活用
  - IIJによるリモートマネージメント
    - 設定変更やバージョンアップなどをリモートで行うことで、お客様にかかる運用管理の手間を大幅に削減
  - IIJマネージドファイアウォールサービスとの連携
    - 不正アクセス検出時にファイアウォール側で一時対応

サービス詳細

- 提供するもの
  - システム
    - OS: 4.4BSDベースの強化型PC Unix
    - IDSソフトウェア: NFR NIDベースの独自システム「IIJ Network Surveyor」
    - CPU: Pentium III 1GHz 以上
    - メモリ: 256MB
    - インタフェース: 10/100 自動認識 Ethernet x 2
    - ハードディスク: SCSI 18G～30GB x 3 (RAID1+Hot Swap)
    - 外寸: 幅 437mm, 高45mm, 奥 580mm (1U rack mount)
    - 重量: 10Kg
    - 電源: 250W
  - HUB

サービス詳細

- お客様にご用意いただくもの
  - インターネット専用線接続
  - ファイアウォール
  - システムに割り当てるIPアドレス
  - システム設置、稼働のための電源、場所の確保
  - リモート管理のためのアクセスに必要となる設定
    (ルーティング、IPsec、SSHの通過)
  - 運用管理担当者の設置



監視～アラート

- ネットワークを24時間365日体制で監視し、IIJが対応が必要と判断した不正アクセスを検出した場合、お客様にご連絡
- アラートの通知
  - TEL / FAX / E-Mail
- 緊急時の連絡手段 (いずれかを選択)

■即時型連絡

- 連絡手段: 電話
- 連絡内容:
  - アラート発生時刻、内容、対策のご相談
  - ファイアウォールサービスでの対策とその内容のご相談

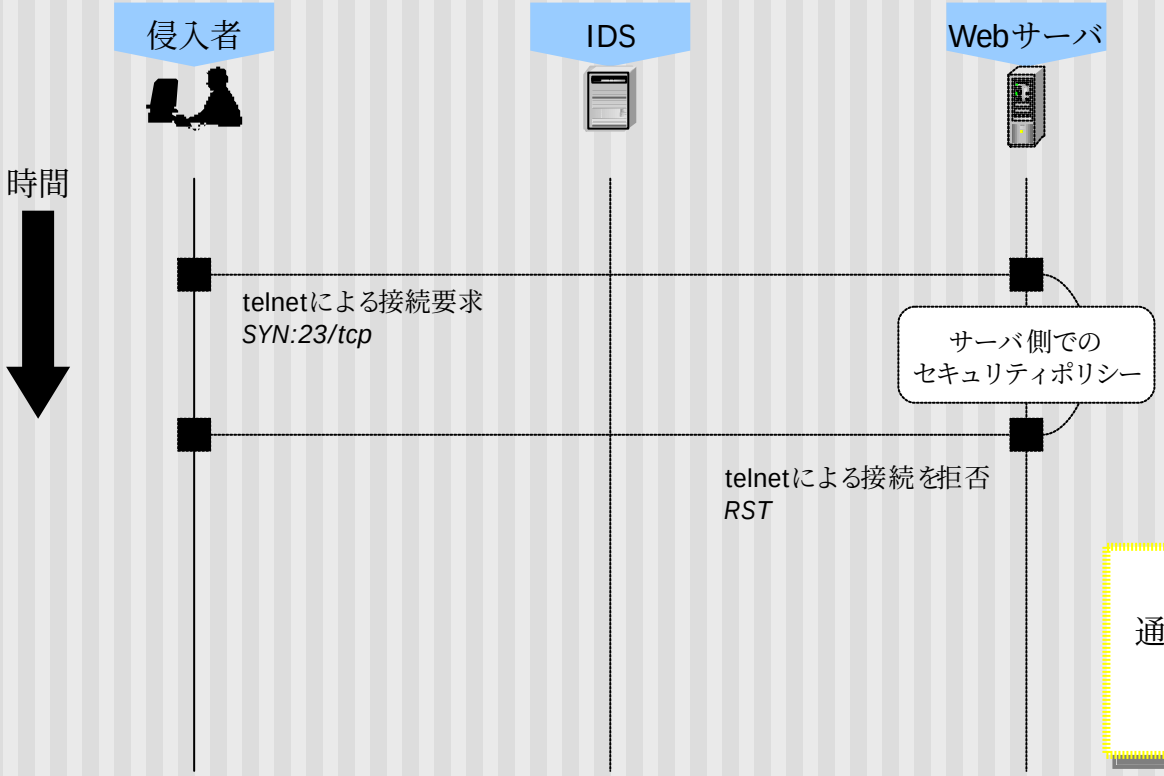
※ 連絡先の優先順位付けやスケジューリングを設定することができます(予定)

■蓄積型連絡

- 連絡手段: E-Mail、FAX
- 連絡内容:
  - 障害(復旧)情報
  - アラート発生時刻、内容
  - ファイアウォールサービスでの対策とその内容

アラートハンドリング

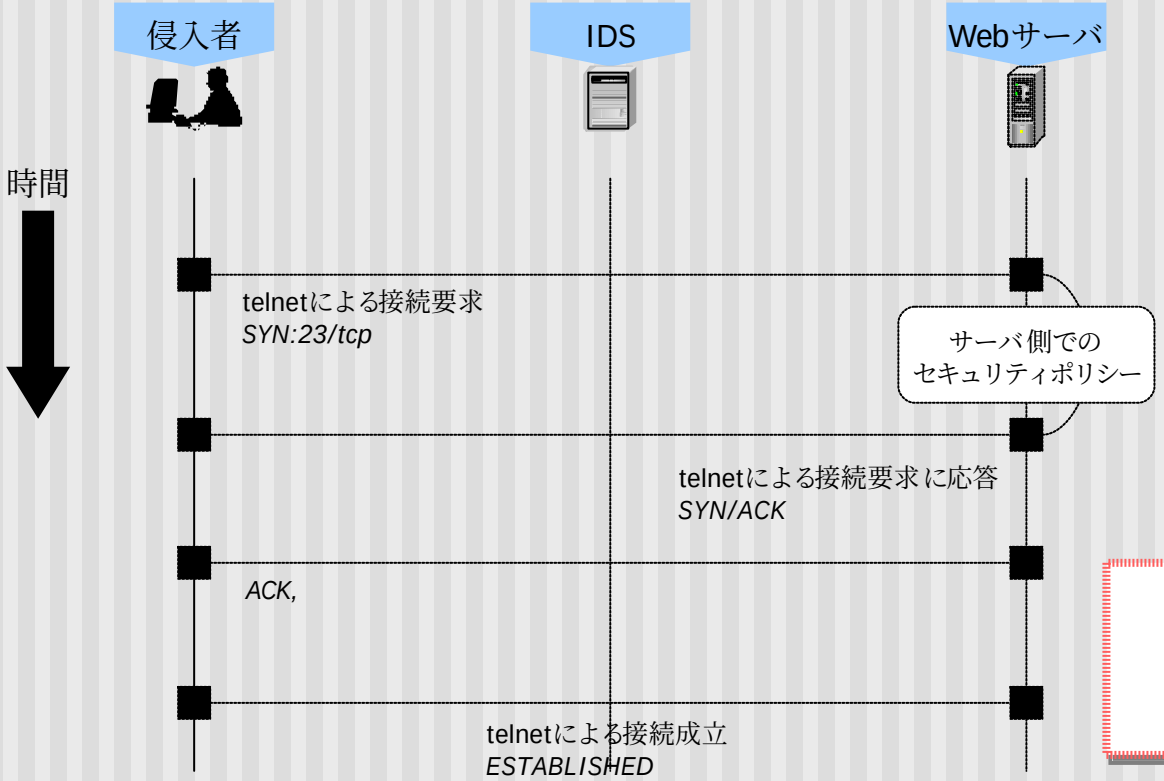
- 動作例1 :アクセスポリシー違反 → 通信不成立



warning
通信が成立していないため、サービスとしては 情報の記録」のみで、即時対応は行わない

アラートハンドリング

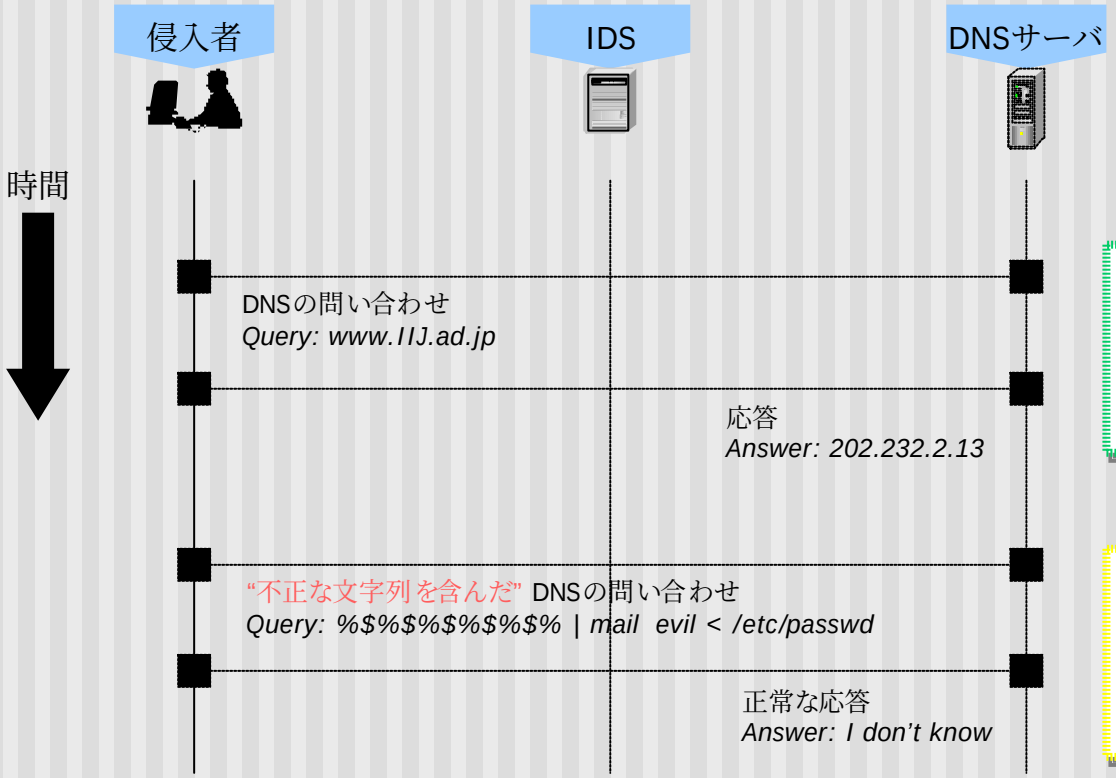
- 動作例2 :アクセスポリシー違反 → 通信成立



alert !!
通信が成立したため、
「アラート」としてお客様に通知

アラートハンドリング

- 動作例3 :Buffer Overrun → 不正アクセス不成立

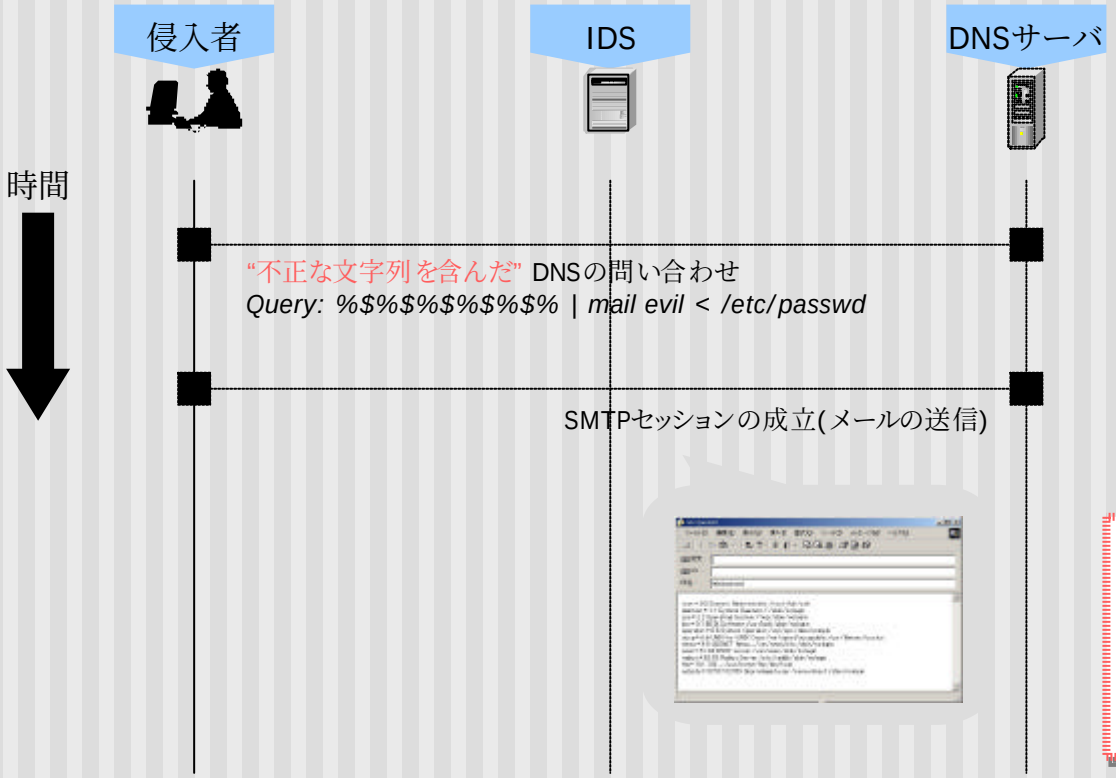


info
通常のDNSのやり取りであるため、
統計データとして保存

warning
不正アクセスの試みがあったものの、
攻撃が成立していないため、
情報の記録」のみで、即時対応なし

アラートハンドリング

- 動作例4 :Buffer Overrun → 不正アクセス成立



alert !!
DNSプロトコル以外の不正と思われる
通信が成立したため、
「アラート」としてお客様に通知

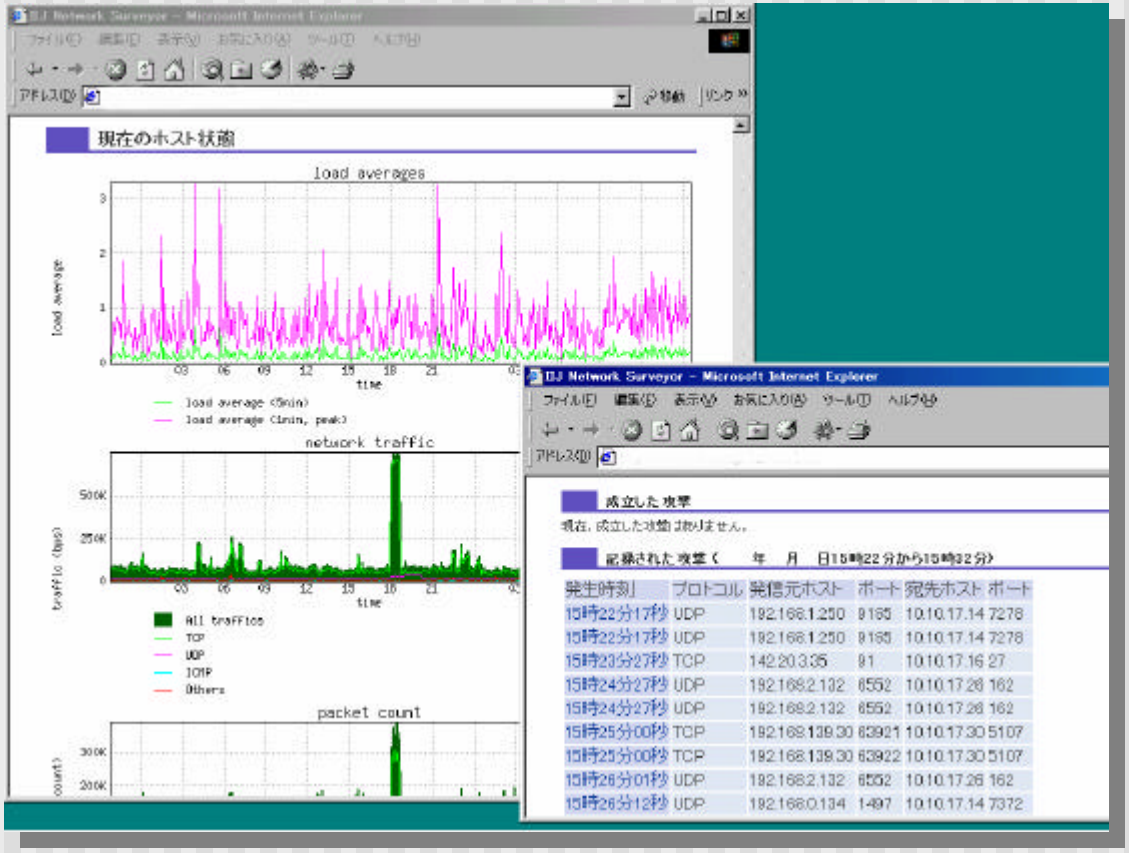
レポート

- パケット情報をIDSでキャプチャし、その情報を元にレポートを生成
- ユーザサポートページで参照可能な情報
  - 月次レポート
    - 通信状況サマリ
    - アラートサマリ
  - アラート履歴
- IDSで参照可能な情報
  - 日時レポート
    - 通信状況サマリ
    - 通信種別サマリ
    - アラート発生状況
  - 調査モード
    - アラートパケットの表示
    - 関連パケットの表示、検索

- 情報の保存期間 (参考値)
  - ユーザサポートページで参照可能な情報
    - すべての情報: 1年間
  - IDSで参照可能な情報 (1.5Mbpsの場合)
    - 全てのパケット情報: 6時間
    - アラート対象となったパケット情報: 1ヶ月 *
    - アラートメッセージ情報: 3ヶ月 *
    - 日次レポート: 3ヶ月

* アラートの発生量により保存期間が変動する場合があります

レポートサンプル

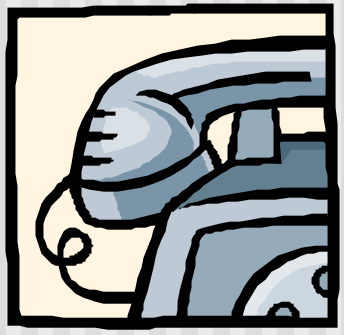


レポート画面のサンプル

※ 画面は開発中のものです

サポート

- テクニカルサポート
  - 土日祝日を除く平日9:30-17:30
  - TEL/FAX/E-Mail
- 設定変更受付・対応
  - 土日祝日を除く平日9:30-17:30
  - TEL/FAX/E-Mail
- 監視～アラート・障害対応
  - 24時間365日
  - TEL/FAX/E-Mail



制限事項 •注意事項

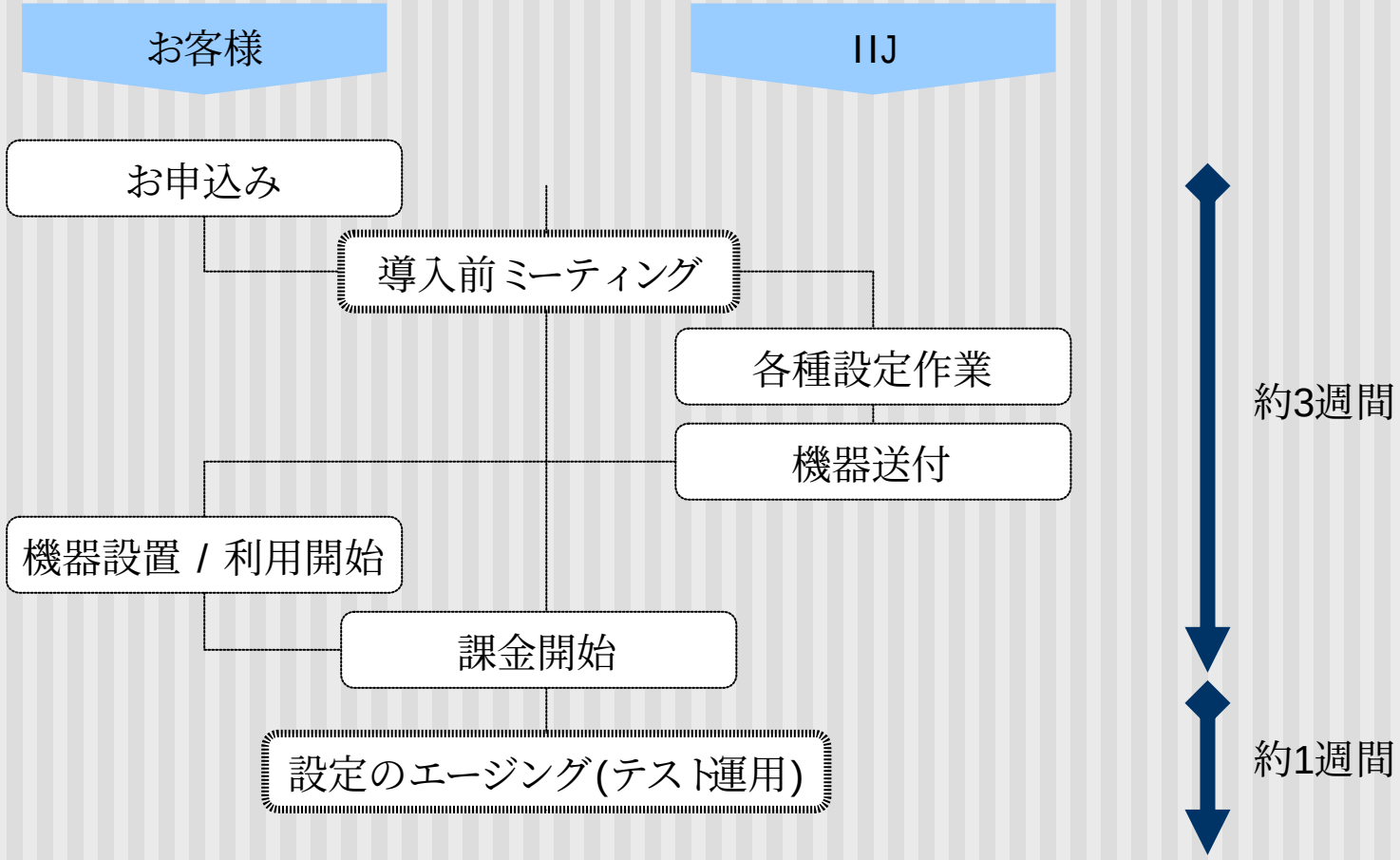
- サービスの提供にあたって、監視対象となる通信の当事者の了承が必要となります
- IIJ以外の接続サービスをご利用の場合でもサービス提供は可能ですが、
  IIJオペレーションセンターとの経路上の障害などにより運用管理
  サービスの一部機能が提供できないことがあります
- ファイアウォールの内側(プライベートネットワーク側)やDMZを監視対象ネットワークと
  することはできません
- 本サービスのご利用に際し、お客様ネットワークの環境変更をお願いする場合があります
- 本サービスは監視対象となるネットワークへの完全な侵入検知を保証するものでは
  ありません
- IIJの判断によりIDSのポリシー変更を行うことがあります

料金

品目	初期費用	月額費用
1.5Mbps	300,000 円	300,000 円
10Mbps		550,000 円
100Mbps		1,000,000 円

- 品目とは、監視対象となるネットワーク上に流れるトラフィック流量の最大帯域を指します。
- 品目を変更する場合は、解約新規の扱いとなります。
- 最低利用期間は1年間です。
- 最低利用期間内にサービスの解約を行う場合は、サービス規約に定める違約金が発生します。

お申込みからサービス開始まで



まとめ

- IDSのポイント
  - 情報を目に見えない脅威から守らなければいけない時代になってきた
  - ファイアウォールだけでなく複合的なセキュリティ対策が必要
  - ますます複雑多様化する脅威に立ち向かうにはどうしたら良いか?
- IIJネットワーク侵入検知サービスのポイント
  - IDSの提供だけでなく、その「運用管理」までを提供するサービス
  - 利用する製品において、full source codeの提供を受けている
  - 適切な検知、情報の視覚化、リモートマネージメント...