ネットワーク型侵入検知システムの歴史と進化

ーTarget Based IDSへのシフトー

三井物産セキュアディレクション株式会社
CTO　Ph.D.　伊藤 良孝

MITSUI BUSSAN SECURE DIRECTIONS, INC.

IDSとは?（1）

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- **IDS (Intrusion Detection System：侵入検知システム)とは**
  - **U.S. Critical Infrastructure Assurance Office**
    Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network…
    http://www.ciao.gov/ciao_document_library/glossary/I.htm (現在リンクなし)
  - **U.S. Navy, Naval Facilities Engineering Service Center**
    An electronic system designed to protect a specific portal, volume or area, using technologies designed to sense movement, sound or a specific act such as opening a door. This security alarm system consists of various types of sensors (vibration, capacitance, volumetric, etc.) to detect the unauthorized intrusion into a facility…
    http://atfp.nfesc.navy.mil/atfp_glossary.html
  - **yourencyclopedia**
    An Intrusion-Detection System (IDS) is a tool used to detect attempted attacks or intrusions by crackerss or automated attack tools, by identifying security breaches such as incoming shellcode, viruses, malware or trojan horses transmitted via computer system or network…
    http://www.yourencyclopedia.net/Intrusion detection system.html
  - **渡辺 勝弘氏 (NT-Committee2 2003/3)**
    コンピュータやネットワークに発生した不正アクセスを素早く検知し、管理者に通報する機能を持ったシステムである
    http://www.hidebohz.com/Meeting/20030322/watanabe.ppt

IDSとは?（2）

MITSUI BUSSAN SECURE DIRECTIONS, INC.

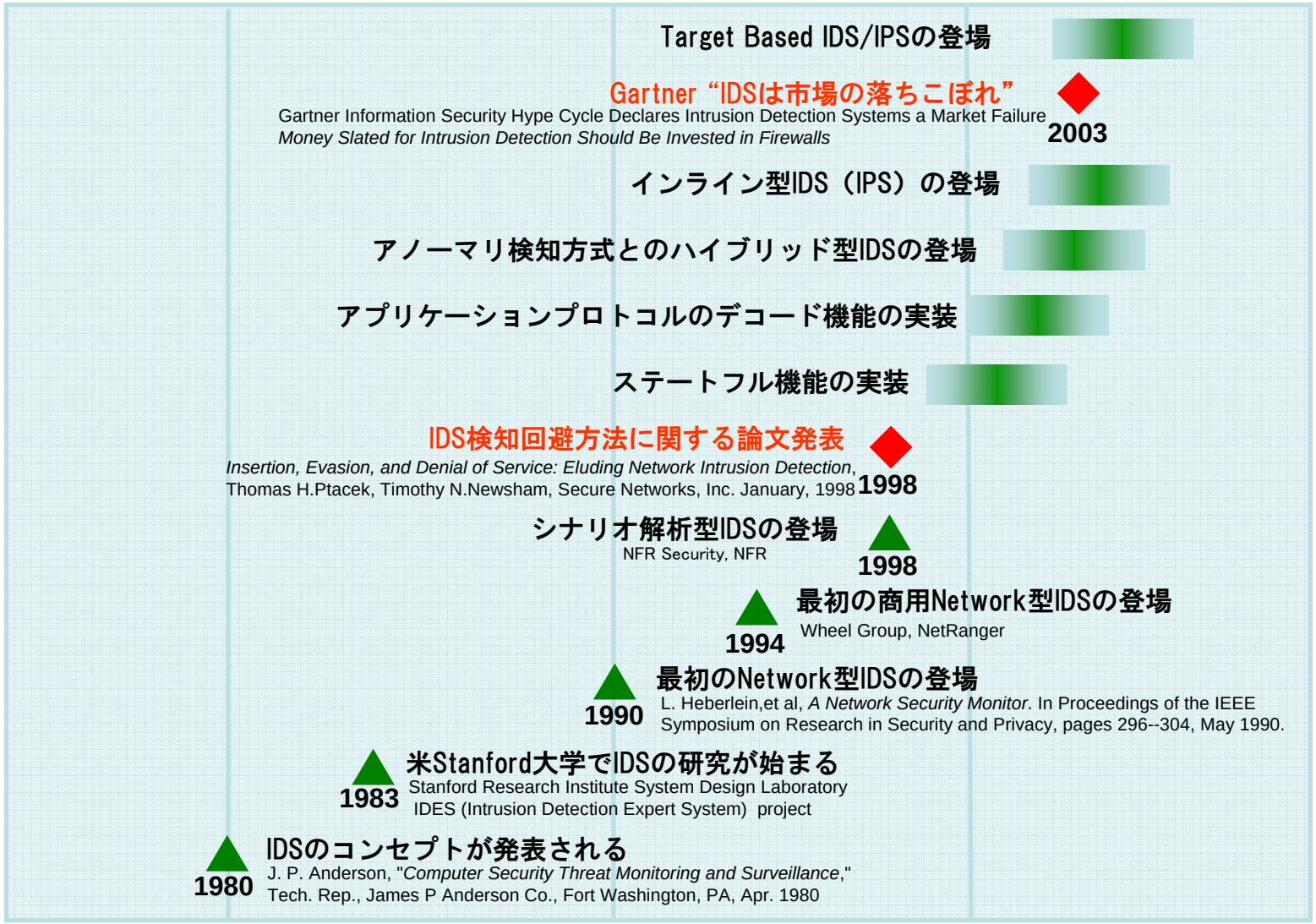
- IDSの分類
  - データソースによる分類　http://www.networkintrusion.co.uk/ids.htm

分類	概要	備考
ネットワーク型	ネットワークに流れるトラフィックデータを検知ソースとするもの	・Network IDS ・Network node IDS
ホスト型	ホストに存在するログファイルやシステムコール状況等を検知ソースとするもの	・Host based IDS
ハイブリッド型	上記の複合型	・Hybrid IDS
その他	広義の意味での侵入検知システム	・Attack Mitigation System ・Honey-pot system ・System Integrity Checker

  - 検知方式による分類

分類	概要	備考
ミスユース検知方式	予め登録してある攻撃パターンと情報ソースの内容を比較する	Signature方式ともよばれる
アノーマリ検知方式	正常状態からのどれぐらい乖離しているかを比較する	・プロトコルアノーマリ ・統計的アノーマリ ・プロファイルアノーマリ ・動作アノーマリ…等様々

IDSの歴史


Target Based IDS/IPSの登場
Gartner “IDSは市場の落ちこぼれ”
Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure
Money Slated for Intrusion Detection Should Be Invested in Firewalls
2003
インライン型IDS（IPS）の登場
アノーマリ検知方式とのハイブリッド型IDSの登場
アプリケーションプロトコルのデコード機能の実装
ステートフル機能の実装
IDS検知回避方法に関する論文発表
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection,
Thomas H.Ptacek, Timothy N.Newsham, Secure Networks, Inc. January, 1998
1998
シナリオ解析型IDSの登場
NFR Security, NFR
1998
最初の商用Network型IDSの登場
Wheel Group, NetRanger
1994
最初のNetwork型IDSの登場
L. Heberlein,et al, A Network Security Monitor. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 296--304, May 1990.
1990
米Stanford大学でIDSの研究が始まる
Stanford Research Institute System Design Laboratory
IDES (Intrusion Detection Expert System) project
1983
IDSのコンセプトが発表される
J. P. Anderson, "Computer Security Threat Monitoring and Surveillance,"
Tech. Rep., James P Anderson Co., Fort Washington, PA, Apr. 1980
1980
1980
1990
2000
2010

NIDSに対する不信感

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- それまでは…（～1998）
  - IDSとは不正侵入や攻撃行為を正確に検知できる魔法の箱であった
- 最初のトリガー…(1998)
  - IDSに対する検知回避方法を記述した論文の発表
    - ここで早くからIDSに興味を持っている人間は市販IDSに疑問を感じた
- 危惧が現実に…(2001)
  - Whisker, Snot, Stick等のAnti IDS toolによる攻撃の顕在化
    - この時点で多くのIDSはこれらのツールによる攻撃を検知できないか、アラートを上げっぱなしの状態になった（単なるノイズジェネレーター）
    - ユーザーの不満が一気に爆発！
      - 検知してくれるんだったら、防御してくれてもいいだろ！
      - 内部でどんな処理をしているのか不明、しかもベンダーに聞いても分からない

…でも面倒を見るのは、俺？　＿|￣|○

- ダメ押し…(2003)
  - Gartnerからの発表：IDSに投資するんだったらFirewallに投資するべき
    - 淡い期待（今度こそ魔法の箱になる!)による買い控え!?
- トドメの一発…??

何が間違っていたのか?

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- IDSがユーザの希望した通りに動作してくれなかった
  - 期待した魔法の箱ではなかった…
- IDS業界自身が、IDSの限界や不具合を隠して、製品を供給していた
  - IDSの内部動作公開はセキュリティ上の問題を引起こす為お教えできません!
    - 実はベンダーやSIerさえも中身や動作を知らない….
  - 弊社のIDSは100Mbpsのトラフィックを完全に処理する能力があります。
    - 結果だけ公開。処理能力の測定条件は未公開…
  - 誰も検証しようとしなかった(メーカ発表を鵜呑みにしてしまった….)
- 何の目的でIDSを使用するのかが明確ではなかった
  - 自分の資産がどんな攻撃にさらされているのかを見たい
  - 自分の資産に対して影響のある攻撃を実際に検知したい
    - 多くのユーザ、SIerはこれを明確にしないままIDSを導入しはじめた
- 古典的なIDSは資産を防御しなかった(Prevention機能がない)

それでも、IDS市場が復活してきている、今日この頃….

NIDSの進化の方向性のキーワード

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- ハードウェア化の進行
  - 急激に広帯域化するネットワークに対応する
    - ASIC （Application Specific Integrated Circuit）
    - NP/AP (Network Processor/Application Processor)
      - 違いは微妙かも… 要はRe-writableかどうか？
- 防御機能の強化
  - Intrusion Detection and Prevention System
    - Gartnerの言うFirewall（In-lineで設置されるNetwork Traffic scrubber）
    - 新しい手法による防御（例えばL2 でTrafficをコントロールする）
    - 3rd Party Vender製品との防御機能の連携
- Contextの認識
  - Target Based IDSへの進化

現在は新世代のIDSが出現している端境期！

Target Based IDSとは?

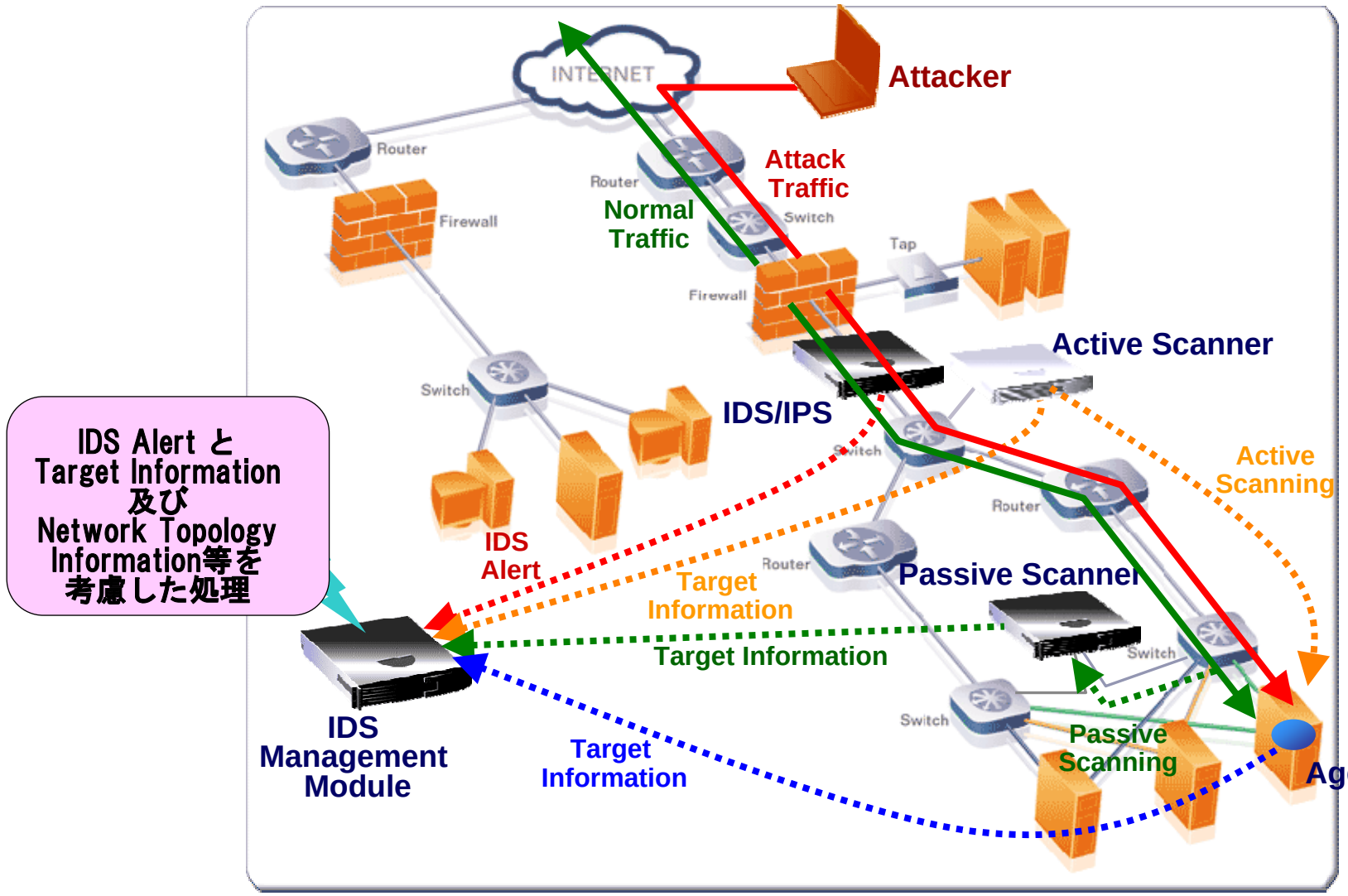
- 明確な定義はまだない?
  - ベンダーによってその意味が異なってくる　(by Marty 

)

    でも、こんな感じ....
    - 防御対象や置かれている環境の情報（=Context)を認識し、それを発生したIDS Alertと結び付けて処理できるIDS
      - 興味のある人はhttp://seclists.org/lists/focus-ids/2004/Jan/0044.html
- 効能
  - IDS チューニングの簡素化（自動Signature選定等）
  - IDS Alertのリダクション
  - IDS 検知回避攻撃への対応
- 実現方法
  - IDSに対してContextをフィードバックする必要がある
    - Passive Scan方式によって情報を得る
    - Active Scan方式によって情報を得る
    - Target Host Agent方式によって情報を得る

Target Based IDSの構成

MITSUI BUSSAN SECURE DIRECTIONS, INC.



Target Based IDSの効用 (1)

- IDSアラートのリダクション
  - IDSの生成するアラートをこんな感じで分類してみると…

    - Target effective alert（ターゲットに対して有効な攻撃アラート）
      - Positive alert (Incident alert)
        - » 実際に攻撃行為が発生し、ターゲットに影響を与えた可能性のある場合
      - False positive alert
        - » 実際には攻撃は発生していないがIDSが攻撃として検知したもの。但し、検知した攻撃はターゲットに大して影響を与える可能性のものである場合
    - Target non-effective alert（ターゲットに対して無効な攻撃アラート）
      - Positive alert (Incident alert)
        - » 実際攻撃行為が発生したが、この攻撃はターゲットに影響を与えない（ターゲットに対して有効でない）場合
      - False positive alert
        - » 実際には攻撃は発生していないがIDSが攻撃として検知したもの。但し、検知した攻撃はターゲットに大して影響を与えない可能性のものである場合

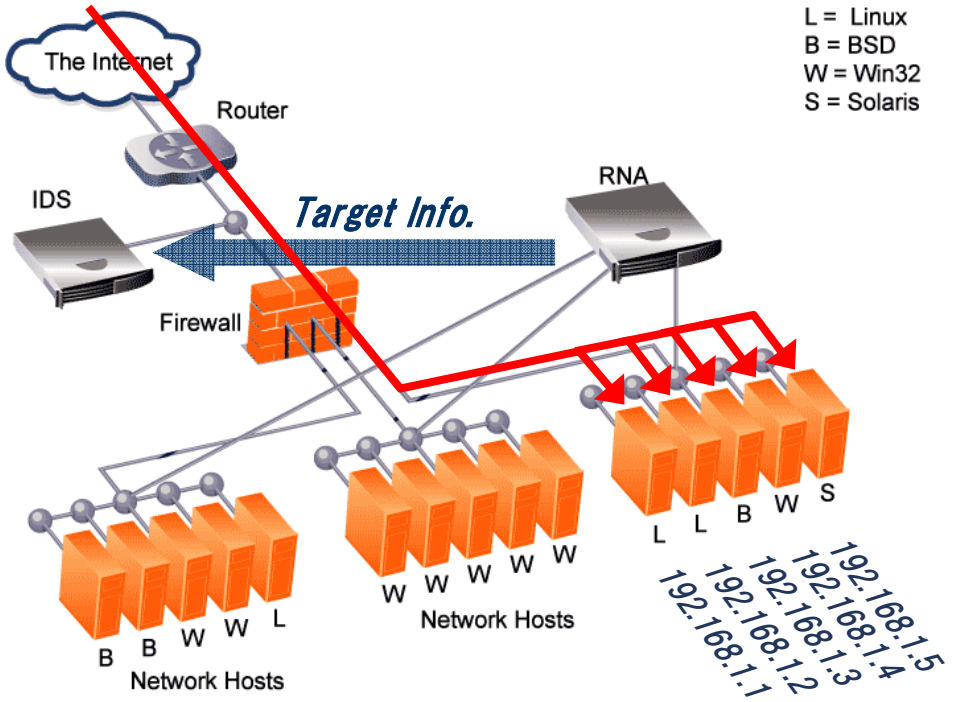
例1

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- IDSは“攻撃”と思われる行為の検出を通知するのみ

＋

- 攻撃行為の、Targetに対する有効性
- Targetの実際の状況



IDS Alert + Target Info.

- NimdaAttack to 192.168.1.1 : 危険度 Low
- NimdaAttack to 192.168.1.2 : 危険度 Low
- NimdaAttack to 192.168.1.3 : 危険度 Low
- NimdaAttack to 192.168.1.4 : 危険度High
- NimdaAttack to 192.168.1.5 : 危険度 Low

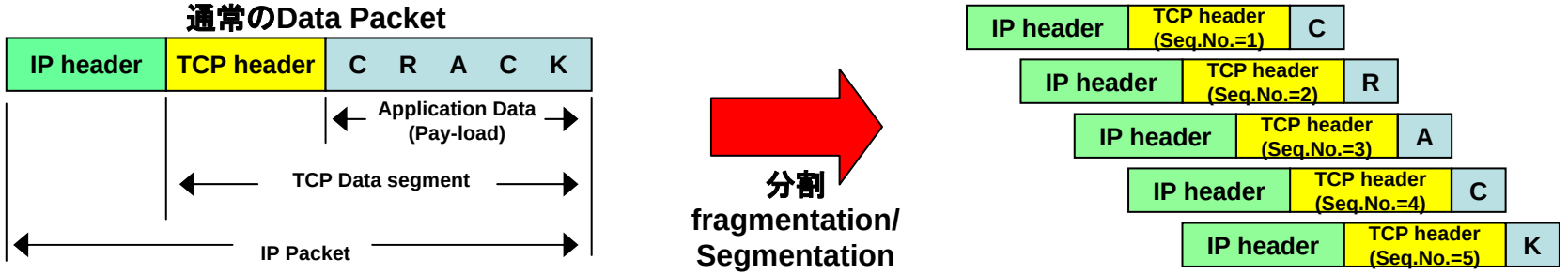
Incident Responseの為の明確な優先順位付与
.... 最終的には検知ルールの自動設定まで

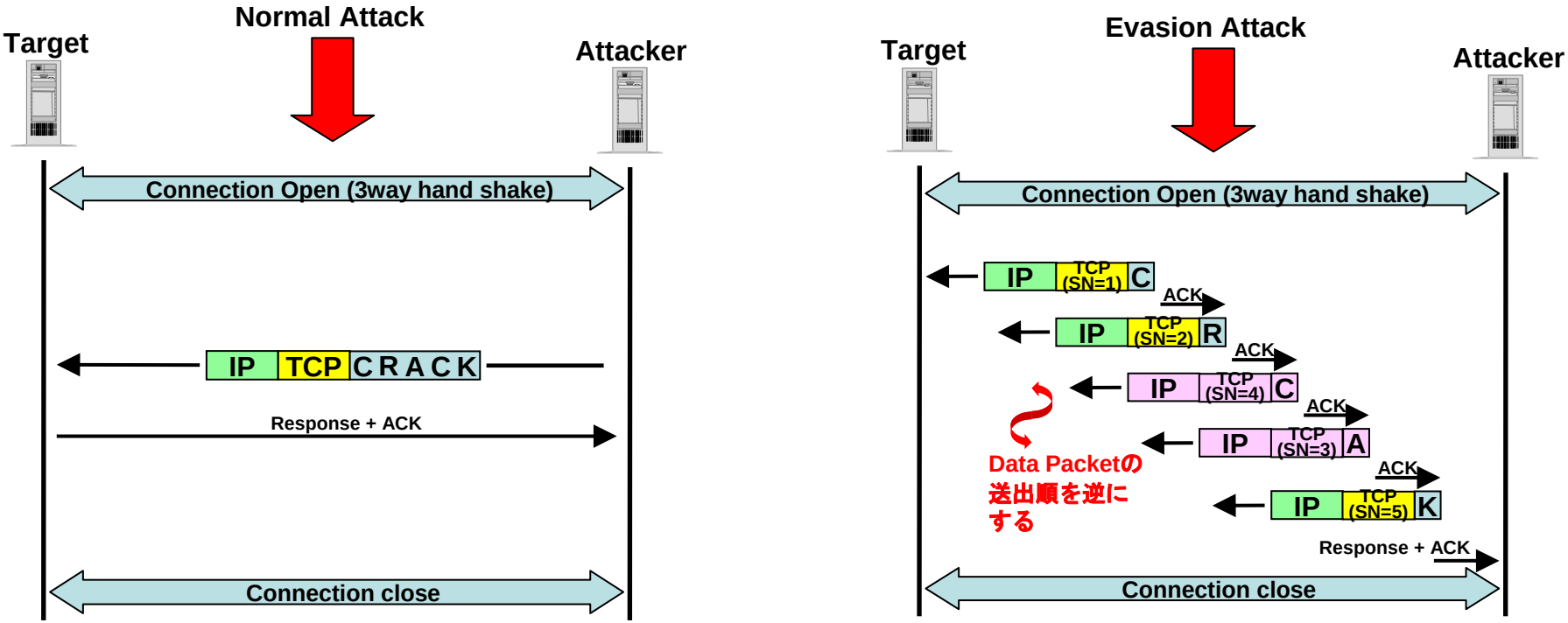
Target Based IDSの効用 (2)

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- IDS検知回避攻撃への対応
  - IDS検知回避攻撃 (IDS evasion)の例
    - Packet fragmentation/Data segmentation (パケット/データを分割して送信)
    - Invalid packet/data insertion (意味の無いパケット/データを挿入)
    - Packet/Data re-ordering (パケット/データの送信順序を変える)
    - Character encoding (データをエンコードして送信)
      - Packet/Data re-assembly errors
      - TCP state de-synchronization (Stateful errors)
      - Signature avoidance
  - なぜ可能なのか?
    - IDSの検知エンジンそのもののバグ
    - IDSに処理エンジンそのものが未実装 (SnortでいえばPre-processorの部分)
    - IDSとターゲットのネットワーク上の地理的位置特性
      - 同じコネクションでもTargetとIDSで観測するパケット/データが異なる
    - パケット/データに対するTargetの処理とNIDSの処理が異なる
      - TCP/UDP/IPスタックの実装におけるRFCの解釈の違い等
  - 例えば...

Evasion Attackの例





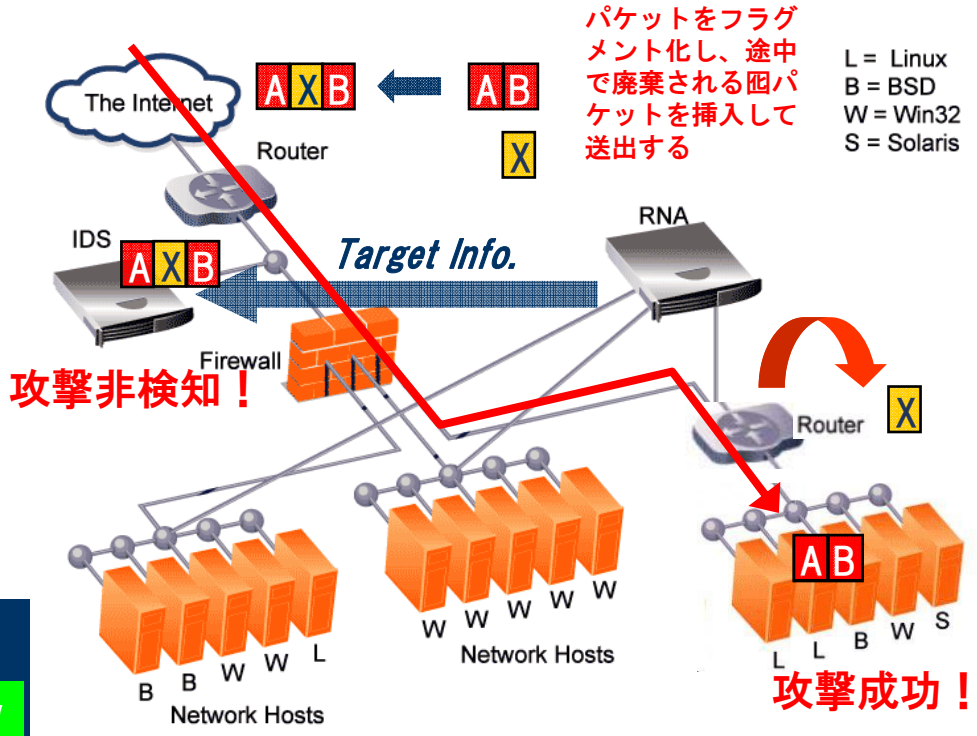
例2

- IDSは“Target：防御対象”の実際の動作特性やNetwork Topology等の情報を考慮していない

＋

- Targetの動作特性
- Network Topologyの特性

IDS Alert + Target Info.
NimdaAttack to 192.168.1.1 : 危険度 Low
NimdaAttack to 192.168.1.2 : 危険度 Low
NimdaAttack to 192.168.1.3 : 危険度 Low
NimdaAttack to 192.168.1.4 : 危険度High
NimdaAttack to 192.168.1.5 : 危険度 Low



IDSに対する検知回避攻撃等への防御
.... 最も効果的な防御ポイントの選択まで

残る課題

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- IDSは今後も進化します。でもたぶん“魔法の箱”にはなりえない…?
  - ハードウェア化の進行でIDS/IDPの処理能力は追いつくのか?
    - IDS/IDPの処理負荷 >> Network Device (ex. Router)の処理負荷
      - Application レベルのより深いところを処理する必要がある宿命は変わらない
      - インライン設置ではよりクリティカルな問題を引き起こす可能性がある
        - » VoIP Packet, Real-time Streamingの遅延
  - 防御機能は正しく働くのか?
    - 現在Application Layerのプロトコルは非常に多種にわたっている
      - Application LayerでConnection Stateを管理する機能が必要
        - » UDP通信でもApplication LayerでのConnection Stateが存在する
        - » Connection Stateを管理しなければならない=Denial of Service攻撃の可能性
    - 検知と防御の為のSignatureの作成方法は本来違うもの?
      - 検知…攻撃行為を広範囲に検知するSignatureが必要 >> False Positiveを内在
      - 防御…攻撃行為を正　確に検知するSignature が必要>> False Negativeを内在
    - もともとIDSはin-houseで作りこまれた脆弱性の検知は苦手
      - Web applicationの攻撃等に代表される様に、この手の攻撃が非常に増加している
  - コンテキストの認識はどこまで正確なのか?
    - Active ScanでもPassive Scanでも突き詰めれば“推測”でしかない
      - 最も正確なのはTarget Host Agent型であるが、得られる情報の範囲が狭い

最後に

MITSUI BUSSAN SECURE DIRECTIONS, INC.

- 前のページで終わったら、あまりにもミもフタもないので…

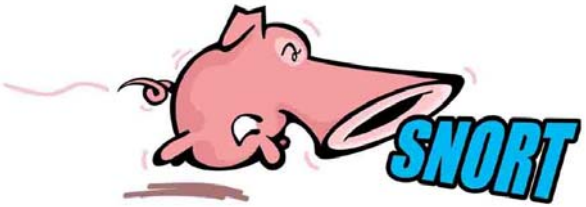
  - IDS/IPSは不正侵入行為等の検知・防御を行う為の強力な対抗手段である事実には変わりはありません。

    要は、IDS/IPSにその力を最大限に発揮してもらう為には、

    - 何をさせたいのか？…… 導入目的
    - 何ができて、何ができないのか？…… 機能特性
    - どこまでできるのか？…… 性能特性
    - どんな環境（状態）で動いているのか？… 動作環境

      さらに！
    - 何を監視・防御させたいのか？…… Targetの特性！

    を飼い主がしっかり理解・把握して、足りない部分を補いながら、愛情をもって、育てていく必要があることをお忘れなく!



ご静聴ありがとうございました。

MITSUI BUSSAN SECURE DIRECTIONS, INC.