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における３つの特徴軸

- 監視対象 (入力情報)
- 検知手法
- 設置場所 (配置方法)

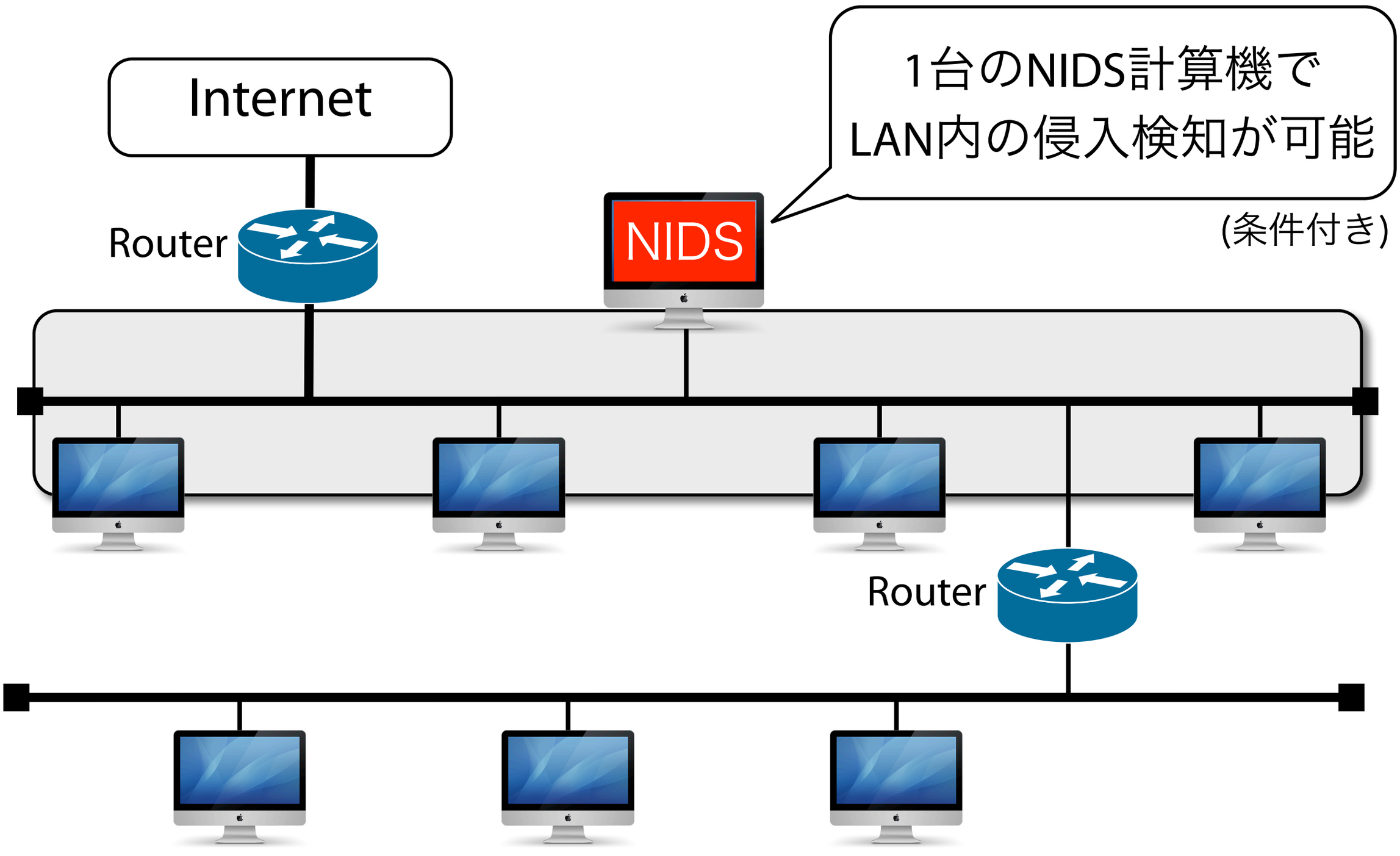
監視対象

- 監視対象 = IDSへの入力情報
  - Network を対象
    - 入力: Network packet
      - Network-based IDS = **NIDS**と呼ばれる
  - Host (計算機内の情報) を対象
    - 入力: files、 system logs、 resource usage
    - Host-based IDS = **HIDS**と呼ばれる

NIDSの利点

- 監視コスト ⇒ **低**
  - Networkを一台のNIDSで監視可能
- 監視対象への影響 ⇒ **低**
  - NIDS専用計算機で稼働
    ⇒ 他の計算機 / Networkへ影響を及ぼすことなく運用可能
- IDSへの侵入可能性 ⇒ **低くすることが可能**
  - ステルス監視 (⇒ IDSへのアクセスを不能に)

NIDSの利点

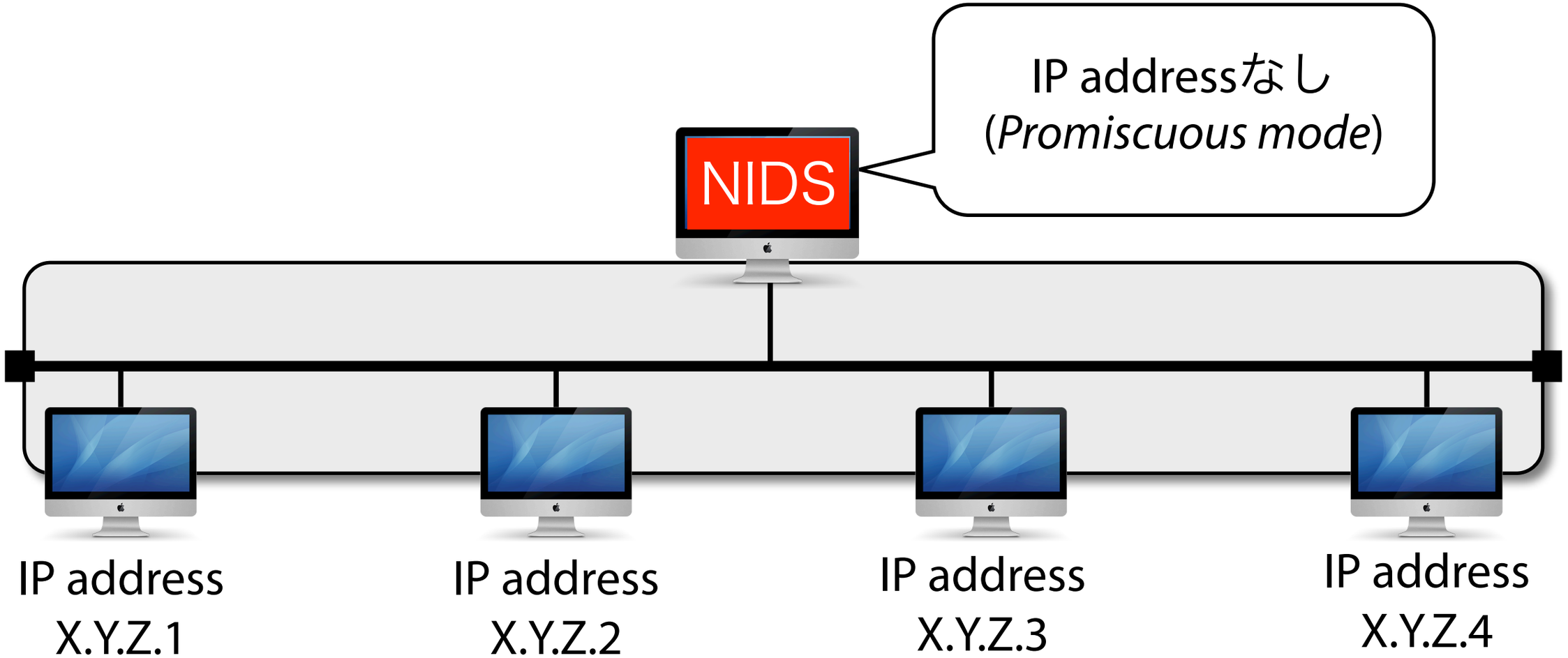

Internet
Router
NIDS
1台のNIDS計算機で
LAN内の侵入検知が可能
(条件付き)
Router

NIDSの利点

ステルス監視

IP addressを付与せず計算機をLANに設置

⇒ 外部からのアクセスは不能



Promiscuous modeとは？

- NIC (Network Interface Card)の動作状態の一つ
- 通常時
  - 自分宛のPacketのみを処理 (NICのMac addressで判断)
- Promiscuous mode時
  - 受信したすべてのpacketを処理
    ⇒ Network情報の収集に応用
  - 本来はTrouble調査、開発(デバッグ)のための動作モード

HIDSの利点 (1/2)

- 多様な情報源
  - Network packet ＋ 「Host内情報」
- 監視精度の高さ
  - 監視対象が特定 ⇒ 多様な情報源 + 判断基準の明確化
- 結果に基づく監視
  - 攻撃行為の結果に基づいた被害の有無判断

HIDSの利点 (2/2)

- 高Network Traffic下でも監視可能
  - NIDSで処理可能なnetwork trafficには限界あり
- 暗号化通信の監視可能
  - Application / Serverが処理した結果に応じて判定
    - ⇒ Application/Server が生成する log message
- 不正行為への対処可能
  - Host内での稼働 ⇒ 改ざんファイルの復旧、
    不正アカウントの停止などが可能

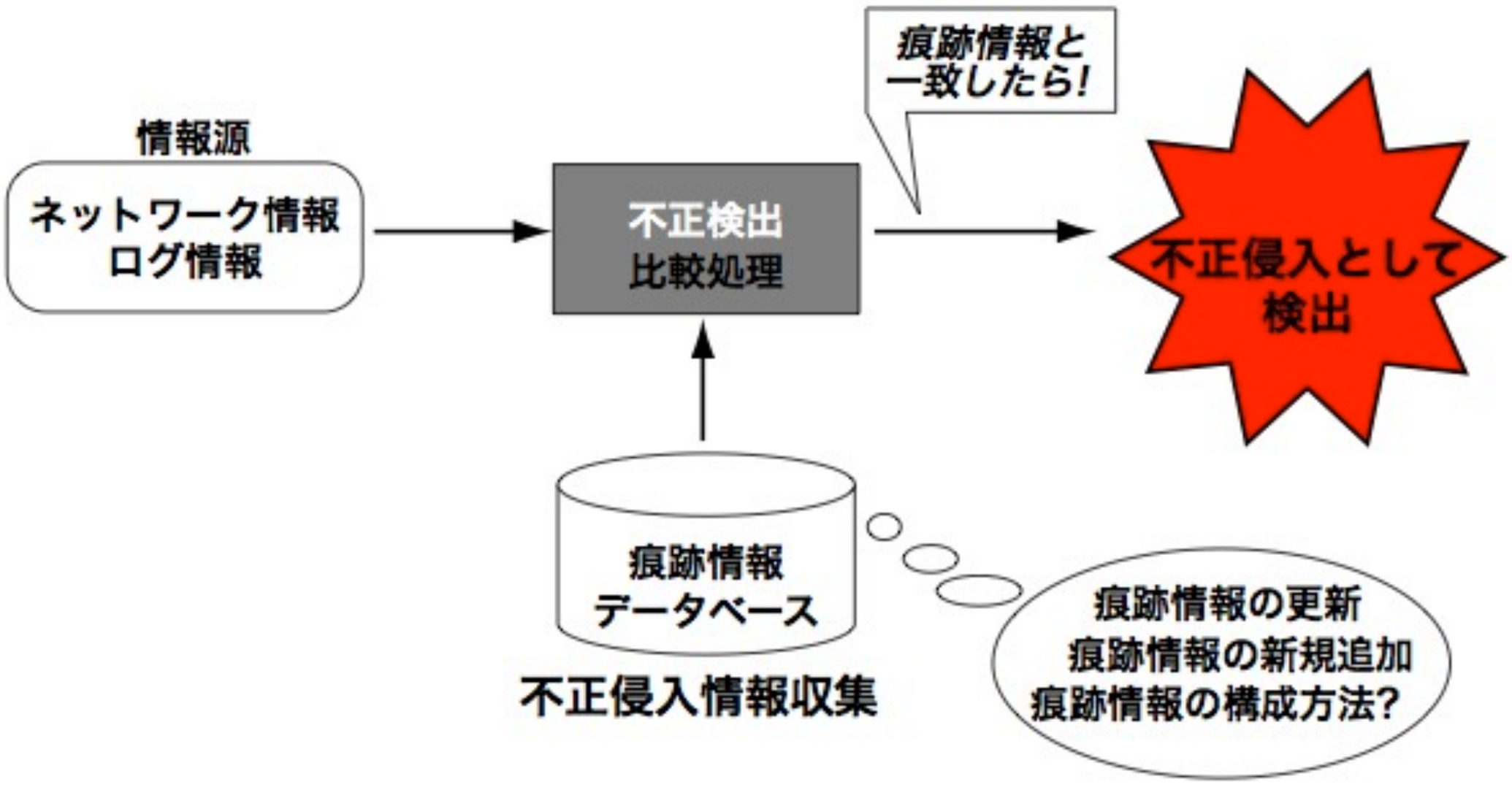
検知手法

- 不正検知 (Misuse detection)
- 異常検知 (Anomaly detection)

不正検知

- **既知**の不正行為を検出
- シグネチャーマッチング (Signature matching)
  - 攻撃に特有の特徴情報をdatabase化
  - 入力が特徴情報と一致したら不正侵入と判定
    - Anti-Virus softwareと同じ仕組み
- Databaseに事前に登録された攻撃のみ検出

不正検出 (Cont.)


情報源
ネットワーク情報
ログ情報
不正検出
比較処理
痕跡情報と
一致したら!
不正侵入として
検出
痕跡情報
データベース
不正侵入情報収集
痕跡情報の更新
痕跡情報の新規追加
痕跡情報の構成方法?

解析事例

ログ情報

```
Jan  7 12:43:22  in.telnetd[6852]: connect from r.manuke.foo.a.ac.jp
Jan  7 17:51:23 in.telnetd[7334]: connect from 1.2.3.12
Jan  7 17:57:52 in.ftpd[7361]: connect from 1.2.3.23
Jan  7 18:35:51 in.telnetd[7475]: connect from aaa.manuke.foo.a.ac.jp
Jan  7 20:17:36 in.telnetd[7803]: connect from r.manuke.foo.org
Jan  8 05:30:11 in.telnetd[8698]: connect from pae320d.fch7.ap.so-net.ne.jp
Jan  8 09:55:01 in.telnetd[8975]: connect from r.manuke.foo.a.ac.jp
Jan  8 09:57:33 in.ftpd[8995]: connect from r.manuke.foo.a.ac.jp
Jan  8 12:13:07 in.telnetd[9207]: connect from bbb.manuke.foo.a.ac.jp
Jan  8 13:59:18 in.telnetd[9409]: connect from bbb.manuke.foo.a.ac.jp
Jan  8 14:00:23 in.ftpd[9433]: connect from bbb.manuke.foo.a.ac.jp
Jan  8 14:55:21 in.ftpd[9700]: connect from boketa1.baka.foo.a.ac.jp
Jan  8 14:55:40 portscan detected from boketa1.baka.foo.a.ac.jp
Jan  8 14:57:01 in.ftpd[9708]: connect from boketa1.baka.foo.a.ac.jp
Jan  8 16:27:06 in.telnetd[88]: connect from rainbow.manuke.foo.a.ac.jp
Jan  8 18:51:04 in.ftpd[988]: refused connect from 1.2.3.20
Jan  8 18:55:07 in.ftpd[997]: refused connect from 1.2.3.20
Jan  8 20:28:32 in.ftpd[1297]: refused connect from 1.2.3.20
Jan  8 20:36:05 in.telnetd[1312]: connect from yyy.manuke.foo.a.ac.jp
Jan  8 21:35:20 in.ftpd[1440]: refused connect from 1.2.3.20
Jan  8 23:15:13 in.telnetd[1697]: connect from r.manuke.foo.a.ac.jp
。。。。
```

**このログの中から以下の規則に
あてはまるログを抽出する**

1. **国外ドメインからのアクセス情報**
2. refused connect **というキーワード**
3. portscan detected**というキーワード**

国外ドメイン
⇒ not .JPドメイン

解析事例 (Cont.)

ログ情報

Jan 7 12:43:22 in.telnetd[6852]: connect from r.manuke.foo.a.ac.jp
Jan 7 17:51:23 in.telnetd[7334]: connect from 1.2.3.12
Jan 7 17:57:52 in.ftpd[7361]: connect from 1.2.3.23
Jan 7 18:35:51 in.telnetd[7475]: connect from aaa.manuke.foo.a.ac.jp
Jan 7 20:17:36 in.telnetd[7803]: connect from r.manuke.foo.org
Jan 8 05:30:11 in.telnetd[8698]: connect from pae320d.fch7.ap.so-net.ne.jp
Jan 8 09:55:01 in.telnetd[8975]: connect from r.manuke.foo.a.ac.jp
Jan 8 09:57:33 in.ftpd[8995]: connect from r.manuke.foo.a.ac.jp
Jan 8 12:13:07 in.telnetd[9207]: connect from bbb.manuke.foo.a.ac.jp
Jan 8 13:59:18 in.telnetd[9409]: connect from bbb.manuke.foo.a.ac.jp
Jan 8 14:00:23 in.ftpd[9433]: connect from bbb.manuke.foo.a.ac.jp
Jan 8 14:55:21 in.ftpd[9700]: connect from boketa1.baka.foo.a.ac.jp
Jan 8 14:55:40 portscan detected from boketa1.baka.foo.a.ac.jp
Jan 8 14:57:01 in.ftpd[9708]: connect from boketa1.baka.foo.a.ac.jp
Jan 8 16:27:06 in.telnetd[88]: connect from rainbow.manuke.foo.a.ac.jp
Jan 8 18:51:04 in.ftpd[988]: refused connect from 1.2.3.20
Jan 8 18:55:07 in.ftpd[997]: refused connect from 1.2.3.20
Jan 8 20:28:32 in.ftpd[1297]: refused connect from 1.2.3.20
Jan 8 20:36:05 in.telnetd[1312]: connect from yyy.manuke.foo.a.ac.jp
Jan 8 21:35:20 in.ftpd[1440]: refused connect from 1.2.3.20
Jan 8 23:15:13 in.telnetd[1697]: connect from r.manuke.foo.a.ac.jp
。。。。

特徴情報

1. 国外ドメインからのアクセス情報
2. refused connect というキーワード
3. portscan detectedというキーワード

6件の不正侵入痕跡を検出

利点

- 高速処理が可能
- 実装、設置が容易
- 検知内容の理解が容易
- 誤検出が少ない

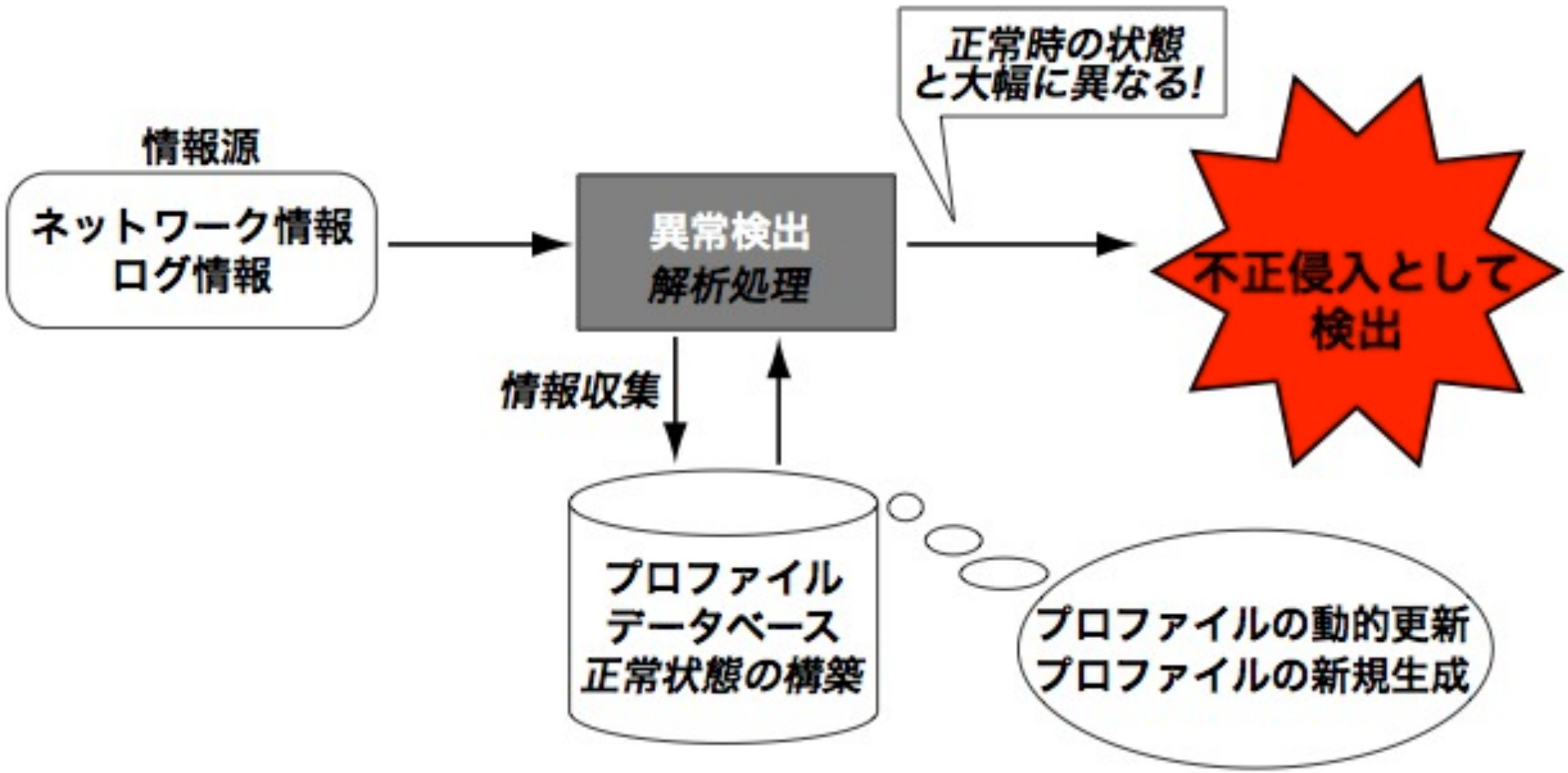
欠点

- 既知の不正侵入しか検知できない
- 特徴情報(Signature)の更新が必要
- “あざむく”のも容易
  - 攻撃者がSignatureを手に入れれば...

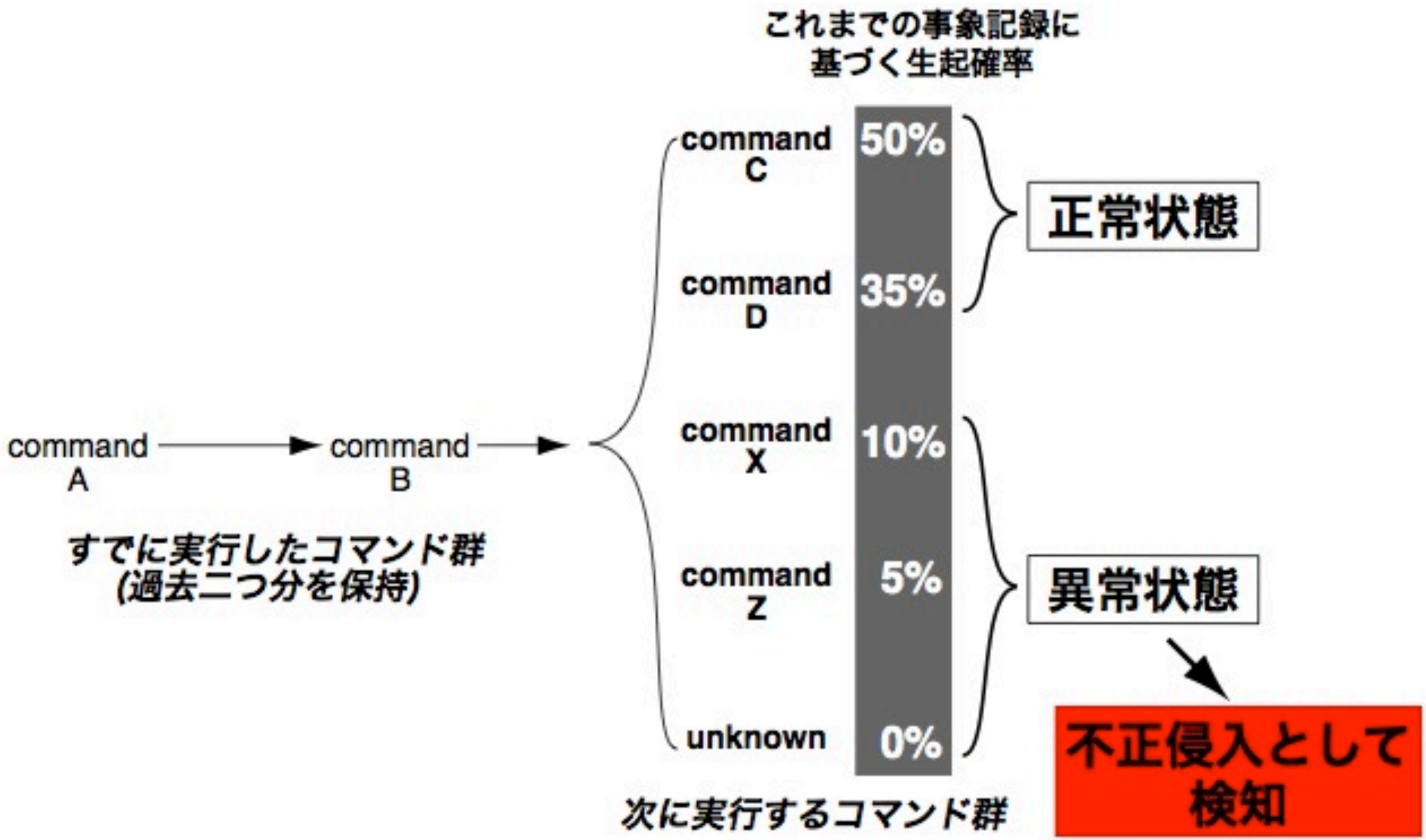
異常検知

- システムの正常状態を基準とし、そこからの乖離(**ズレ**)を異常(不正侵入)として検出
  - 正常状態の定義
    - Profile (プロファイル) - 統計的傾向
      - 例) 通信量とその時間変化
    - 管理者による定義 (仕様や運用ルールによる)
      - 例) 勤務時間による定義
        (深夜に業務サーバにアクセスする人はいない)

異常検出 (Cont.)


情報源
ネットワーク情報
ログ情報
異常検出
解析処理
情報収集
正常時の状態
と大幅に異なる!
不正侵入として
検出
プロファイル
データベース
正常状態の構築
プロファイルの動的更新
プロファイルの新規生成

解析事例


これまでの事象記録に
基づく生起確率
command
A
command
B
すでに実行したコマンド群
(過去二つ分を保持)
command
C
50%
command
D
35%
command
X
10%
command
Z
5%
unknown
0%
次に実行するコマンド群
正常状態
異常状態
不正侵入として
検知

利点

- 未知の不正侵入を検知可能
- 検知のための「基準情報(しきい値)」の更新維持頻度低

欠点

- 検知のための明確な基準がない
  - ⇒ 検知理由が明確でない
- 誤検出率が高い
- 正常状態を攻撃者に操作される可能性

検出手法の関係

	不正検出 (Misuse)	異常検出 (Anomaly)
Signature-based	Signatureとの一致を侵入と判定	
Profile-based		正常状態との乖離を侵入と判定

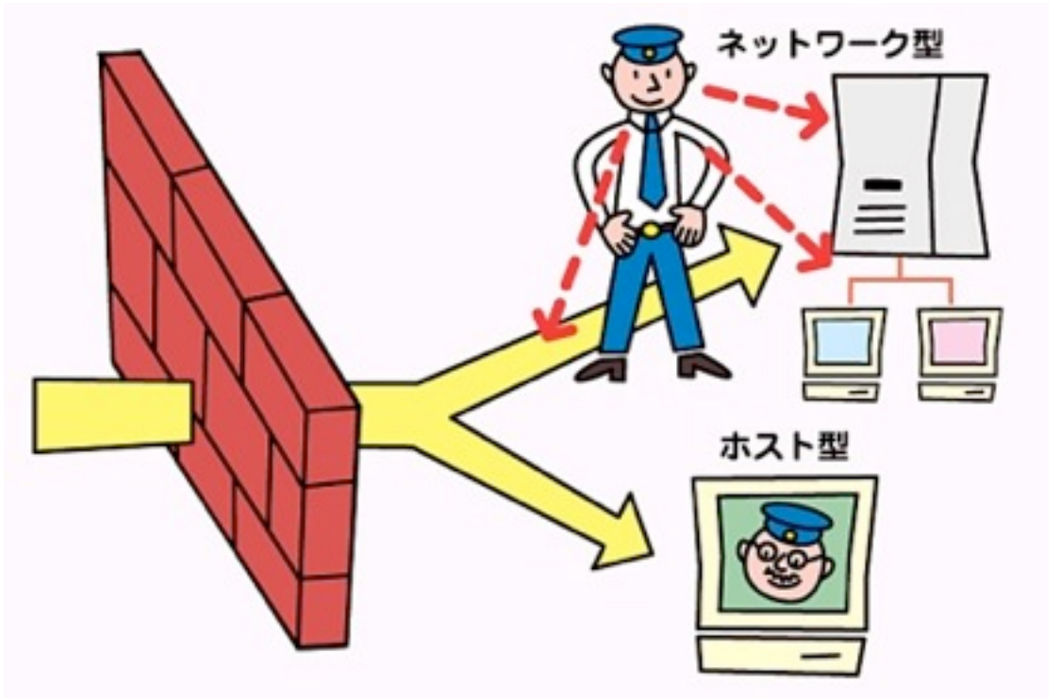
検出手法の関係 (Cont.)

	不正検出 (Misuse)	異常検出 (Anomaly)
Signature-based	Signatureとの一致を侵入と判定	**正常Signature**と不一致の時、侵入と判定
Profile-based	ない	正常状態との乖離を侵入と判定

異常検出の*Signature(*正常*signature)*は
更新する必要が少ない

設置場所

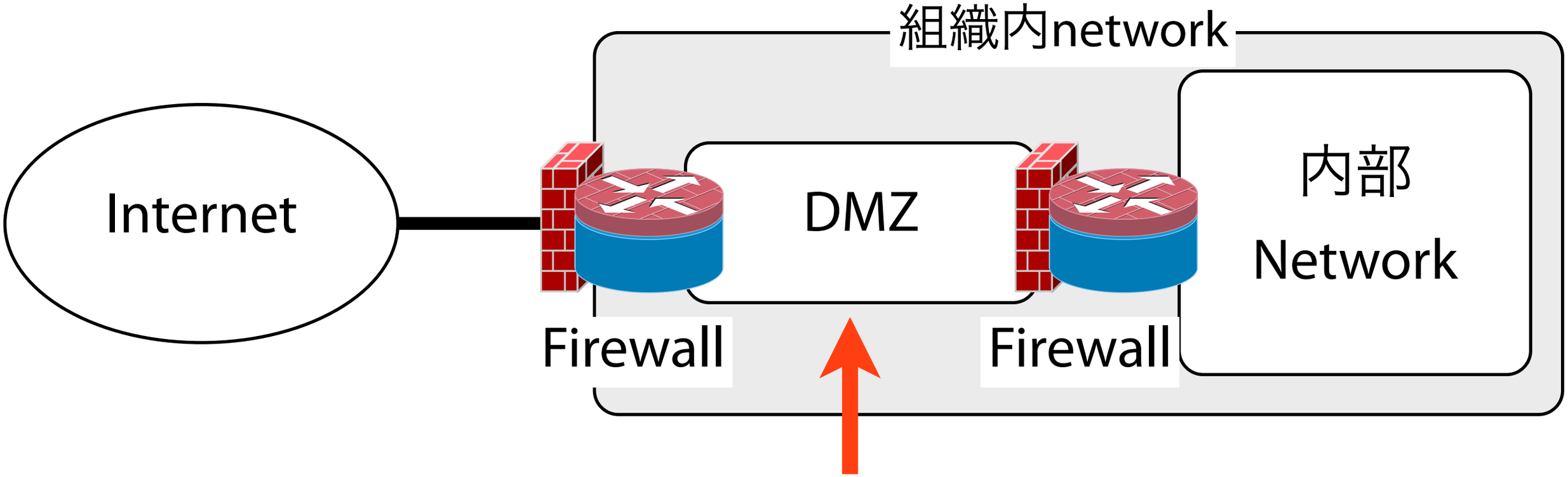
- Network型
  - Firewall の外側
  - DMZ(Demilitarized Zone) 内
  - 社内ネットワーク(Intranet内)
- ホスト型
  - サーバ内
  - クライアント内



図引用: http://www.atmarkit.co.jp/fsecurity/special/19fivemin/fivemin03.html

一般的なNetwork接続構成

三層構造



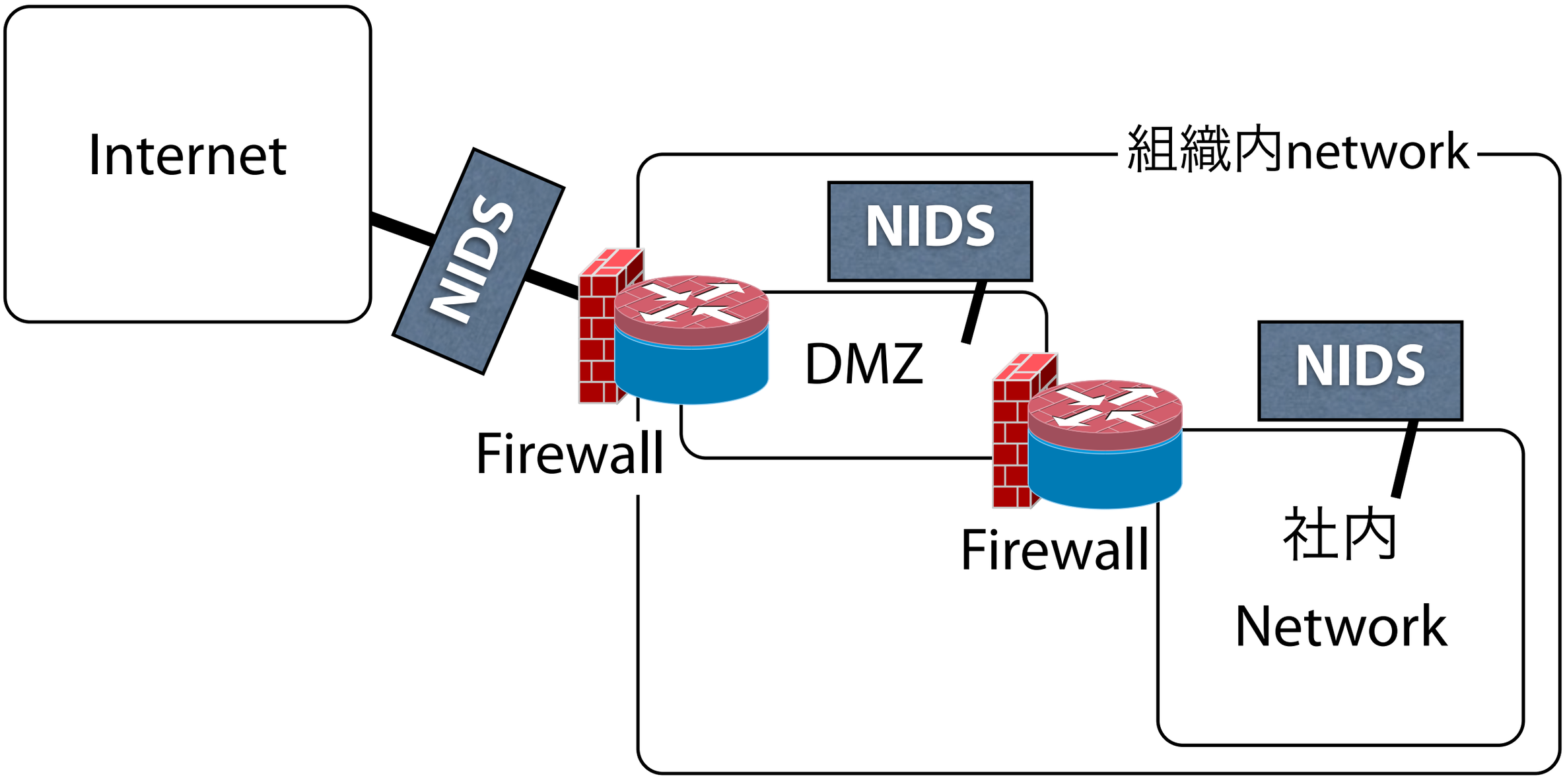
DMZは、緩衝地帯 (中間保護層)

NIDSの配置場所

NIDS
(接続Network内の全packetが検査対象)

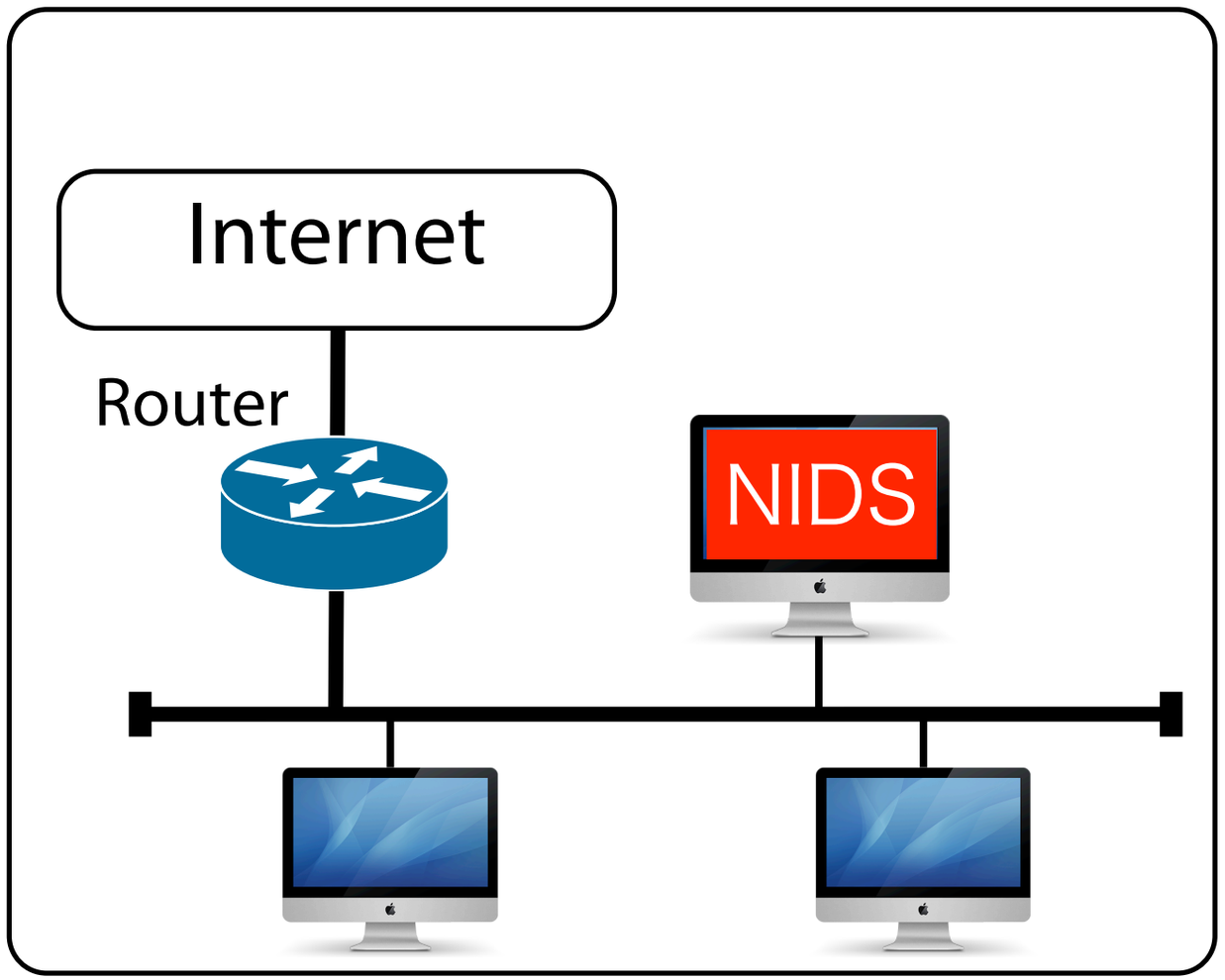
- Firewall の外側
- DMZ
- 社内ネットワーク内

NIDSの設置場所

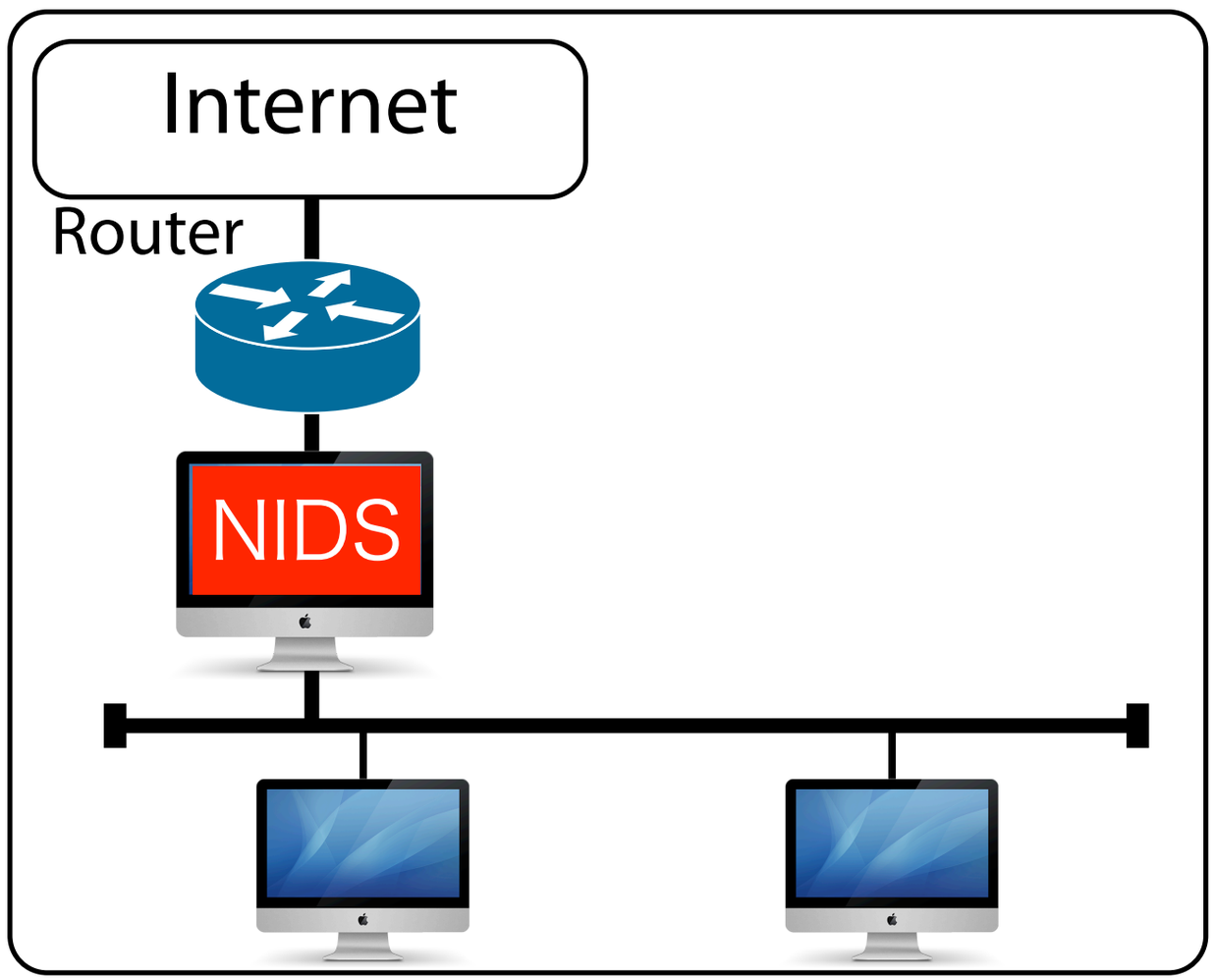


設置場所により収集可能な情報が異なる

NIDSの設置法



タップ型

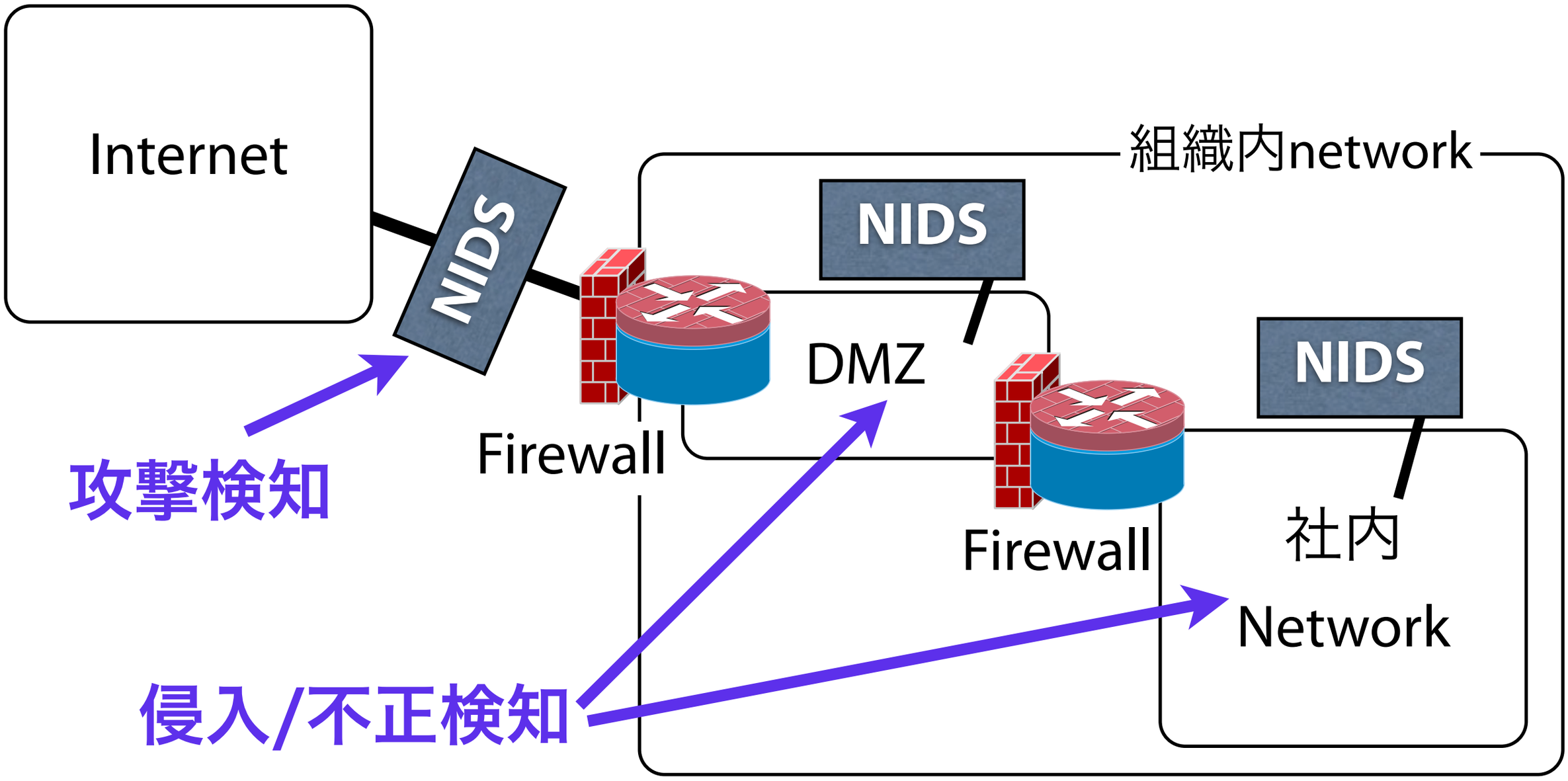


インライン型

NIDSの設置場所

設置場所により収集可能な情報が異なる

⇒ 目的も異なる



どちらがよいか

理想的には**両方配置**

- **攻撃検知**
  - システム管理の苦労を正当化する証拠集め
  - コスト大 (運用管理・性能維持)
- **侵入検知**
  - 侵入検知
  - 内部不正への監視、抑止効果
  - 法的、Privacy問題

HIDSの配置場所

- 計算機内に設置
- サーバー or クライアント
- 入力情報が監視計算機に限定

HIDS

NIDS
(監視 対象計算機への
packetのみ対象)

IDSの出力

- 基本
  - ログ記録 (text file, databaseへ)
  - 管理者へ通知 (電子メール、Console)
- 応用
  - 直接対応：改ざんfileの復元など
    - 他のapplicationとの連携 (特定App.起動)
  - 不正通信の遮断 (⇒ Firewallとの連携)

通知における注意点

- **注意をひく**
  通知が有効に機能するよう方法、内容の精査
  (無視されないように)

- **通知経路の保護**
  通知機能が不正侵入者により攻撃される
  ⇒ 通知機能の無効化

- **通知タイミング**
  即時性と確実性、運用の問題
  ⇒ その都度通知すると、誤通知に圧倒されて無視へ
  ⇒ Port scanはいつの時点で検知と判定し通知するか？