OSSによるIPSの実現

Linux Conference 2005

桝本　圭†

原田　季栄†

†（株）NTT DATA オープンソース開発センタ

➢ OSSのIDSを統合したIPSの構築

※OSS：オープンソースソフトウェア （Open Source Software）
IDS：侵入検知システム（Intrusion Detection System）
IPS：侵入防止システム（Intrusion Prevention System）

Snort 通信監視

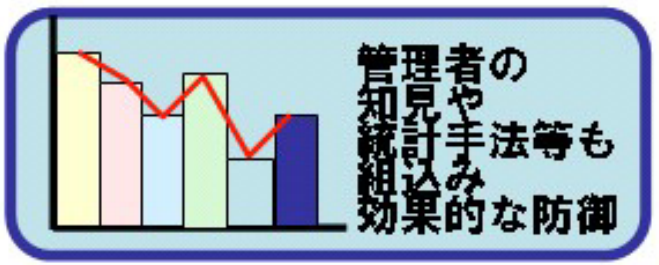
Tripwire 改ざん検知

Libsafe BOF対策

ModSecurity WebAPセキュリティ

Netfilter Firewall

CUTEA 通信遮断



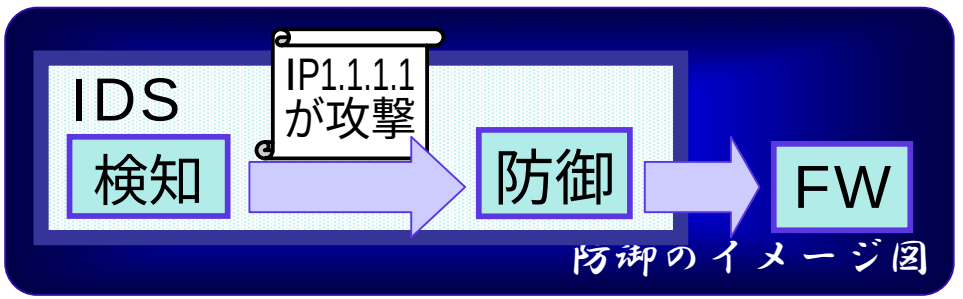
目次

1. OSSのIDSの充実、普及

- 安価で、新技術も実装されるが、商用製品のように「ほぼ全ての攻撃に対応」するパッケージの形式ではない。組合わせて使う必要がある。

2. IDS（検知のみ）からIPS（検知＋防御）へ

- IDSの検知情報を元にシステムを防御（ex.コネクション遮断）



➡ OSSのIDSを自由に組合わせた形式のIPS

「組合わせて作るIPS」の課題

1. 防御機能はIDS毎の開発となりコスト高。
   - IDS毎に警告形式は異なるため、防御機能もIDS毎になる。

2. 定期実行型IDSはIPSに適さない。
   - 一部のrootkit detector等は、定期的に管理者に実行される形式。
   - 攻撃発生時に検知しないと防御ができない（ただ検知能力は高い）。

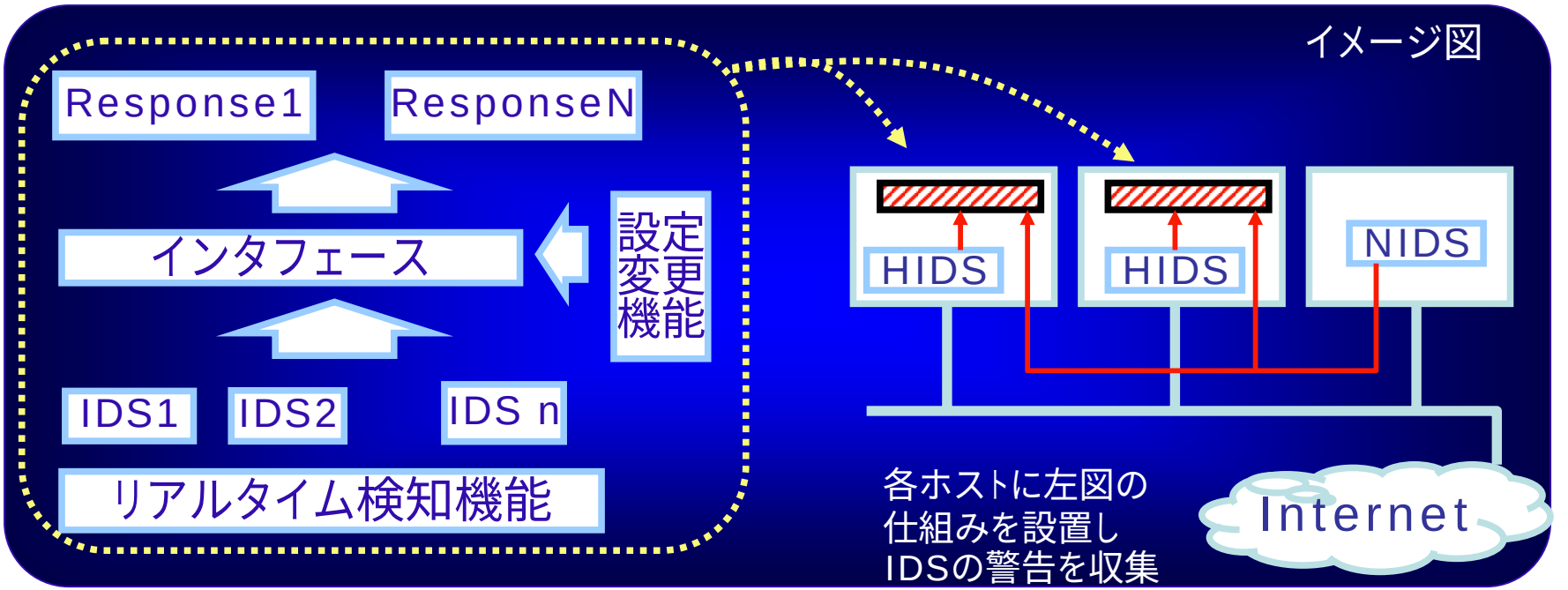
3. 実行する防御を事前に設定する方法は効果が薄い。
   - 人手で防御も行う場合、明らかに攻撃である場合に攻撃者に重度のペナルティを与えたり、正規ユーザへのサービス妨害がないよう考慮しながらに防御するが、この場合は考慮されない。

課題の解決指針

1. IDS毎に防御を用意
2. 定期実行型IDS

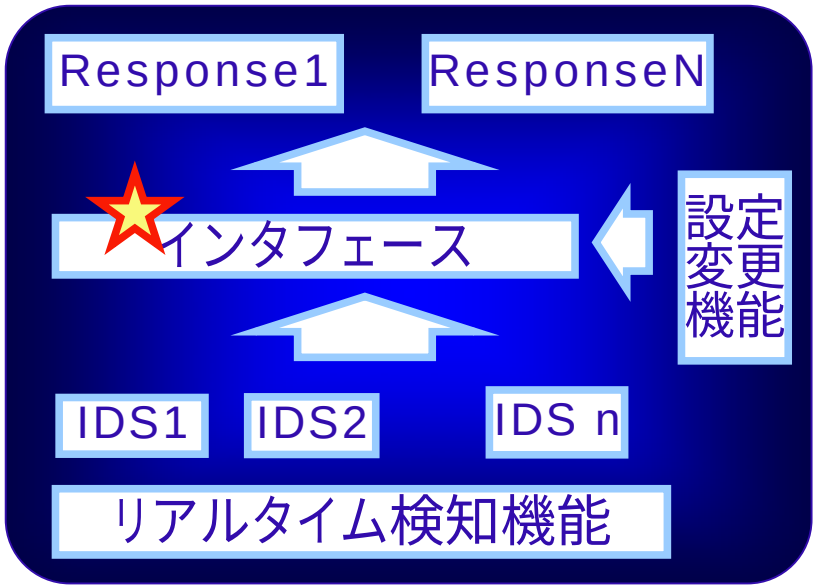
3. 「攻撃Aには防御B」

1.共通の防御機能を用意
2.攻撃発生時に検知させる
サポート
3.稼動中に防御手法を変更



課題の解決（１） 検知と防御の調停インタフェース

- 目的
  - ✓IDSの警告を、防御機能が求める形式に変換する。

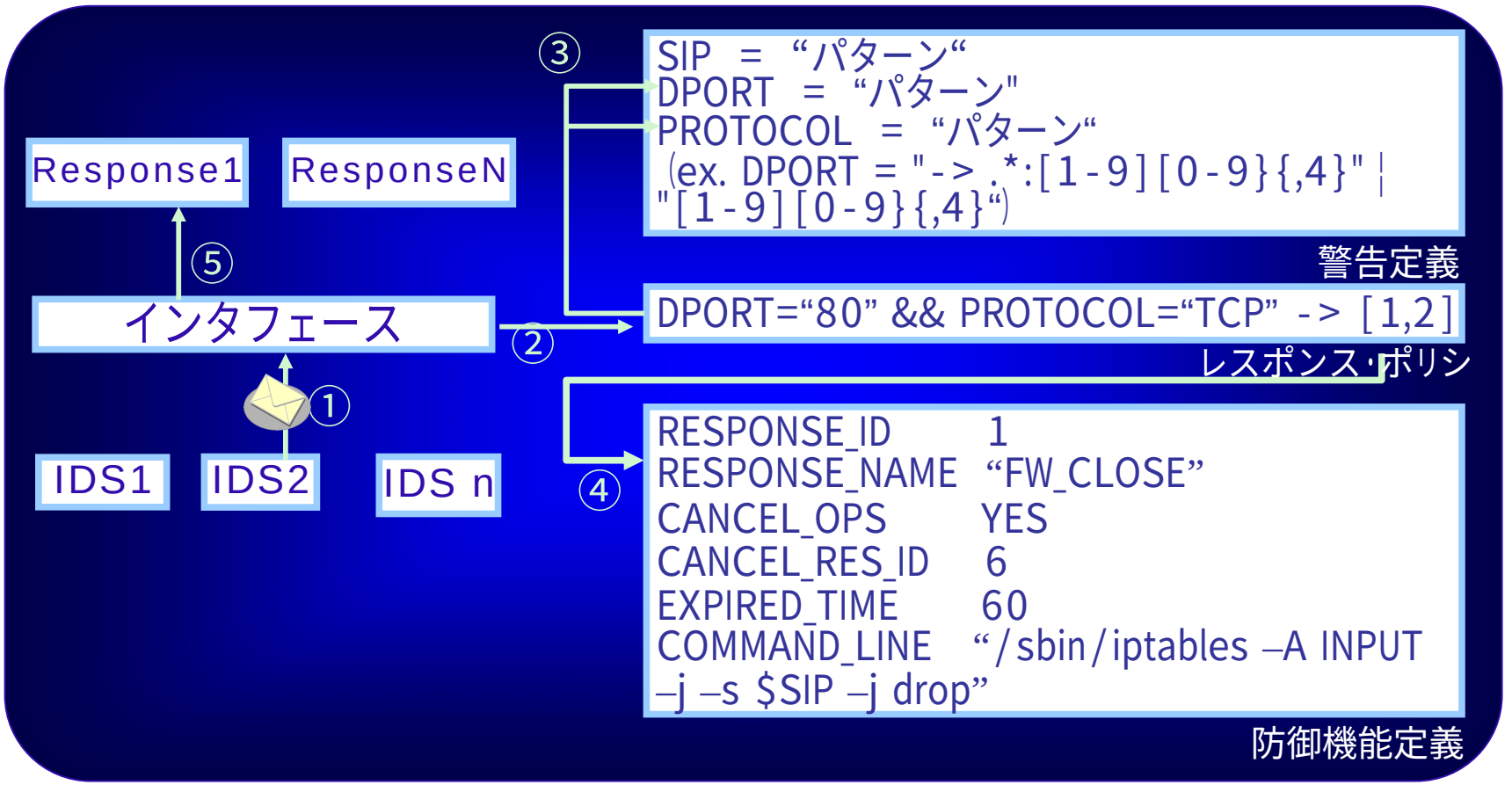


- 要件
  1. 一般性
     任意のIDSを組込み可能とする。
  2. 警告内にない情報は補完
     ex. インターネットからの攻撃をホストベースのIDSが検知した場合、攻撃元IPアドレスが警告に含まれない場合が多い

課題の解決（１） 検知と防御の調停インタフェース

➢ 解決指針

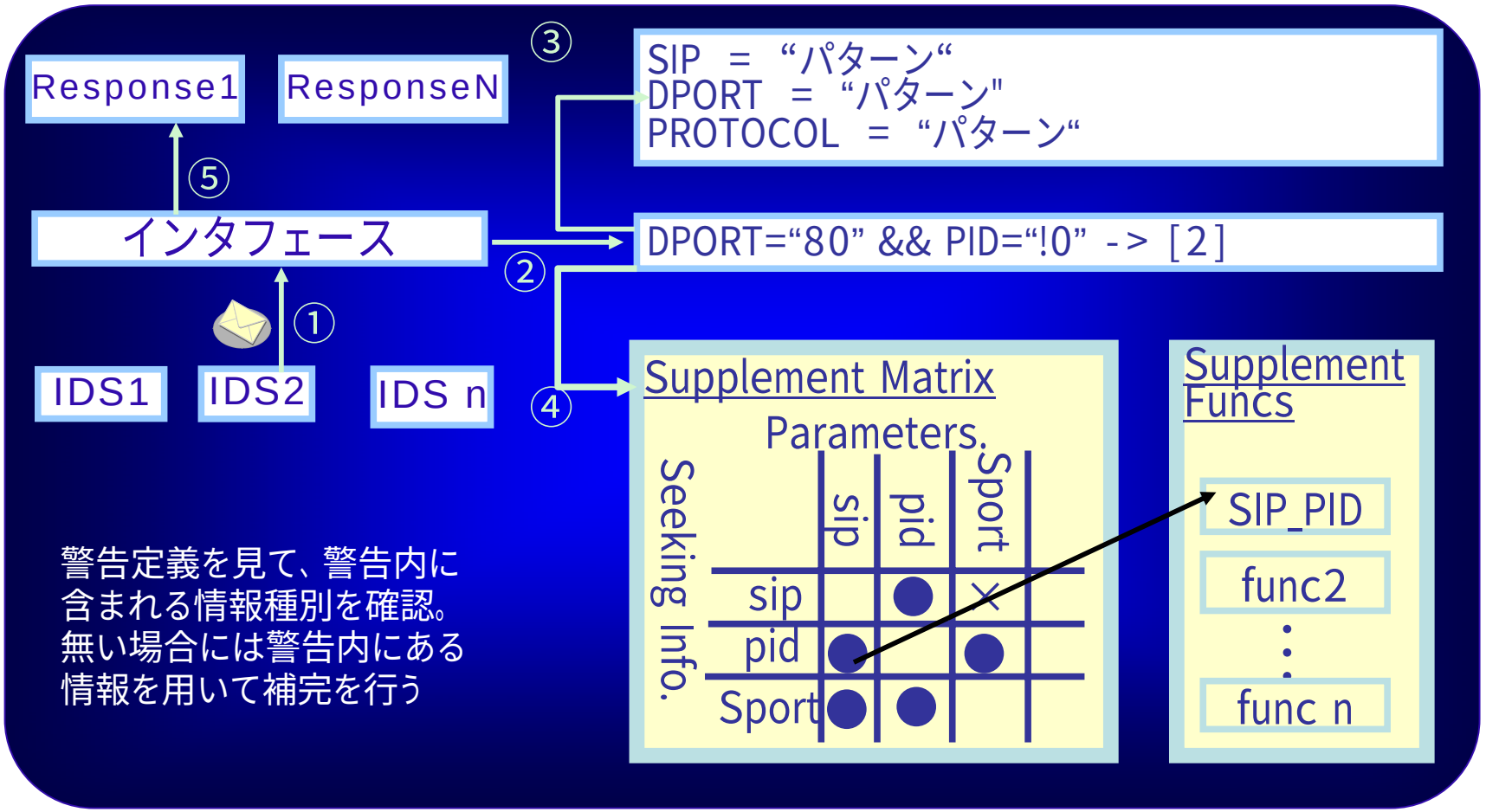
- ✓ IDSの警告定義を元にしたパターンマッチング



課題の解決（１） 検知と防御の調停インタフェース

➢ 解決指針

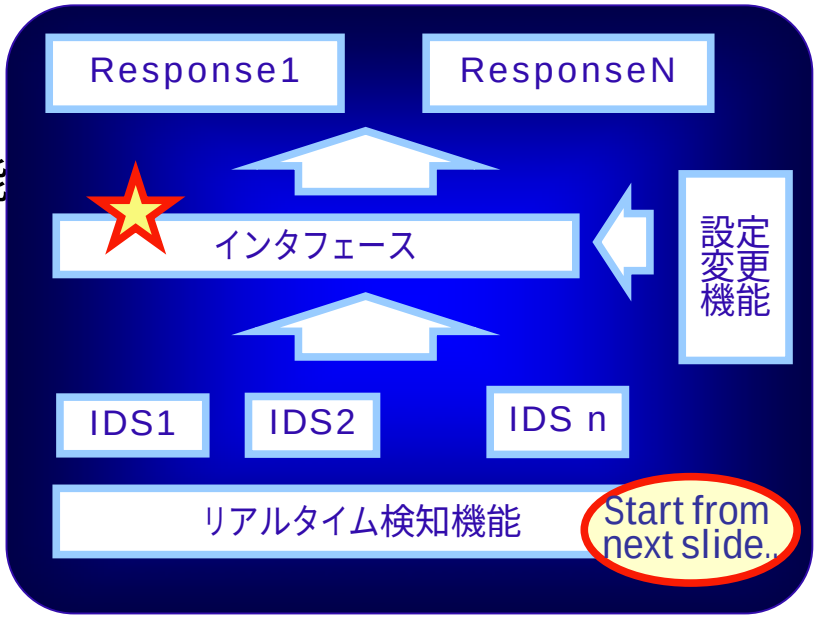
- ✓ 警告内の情報を元に、ＯＳ内から情報収集



課題の解決（１） 検知と防御の調停インタフェース

インタフェース部まとめ

- ✓ IDSに共通の防御機能 (Response 1....N) を使用させ防御が可能
- ✓ 警告内にない情報は自動補完するため、IDS～防御機能の自由度高
- ✓ 適用するIDS、防御機能は任意でよく、カスタマイズ可能

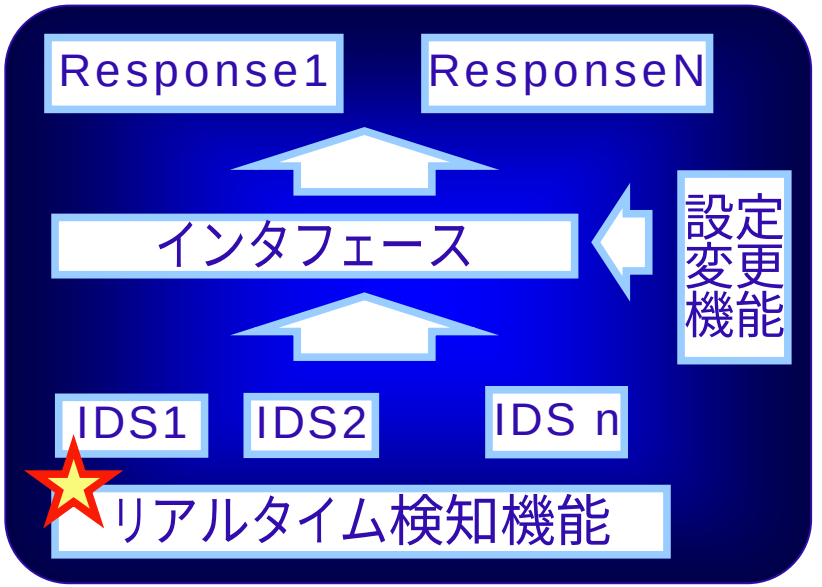


- ✓ ただし、攻撃発生時に検知しないようなIDSには対応不可能
  (次スライドから説明)

課題の解決（２） リアルタイム検知のサポート

➢ 目的

定期的に実行される型のIDSに
「攻撃発生時に検知させる」
サポートをする。



➢ 要件

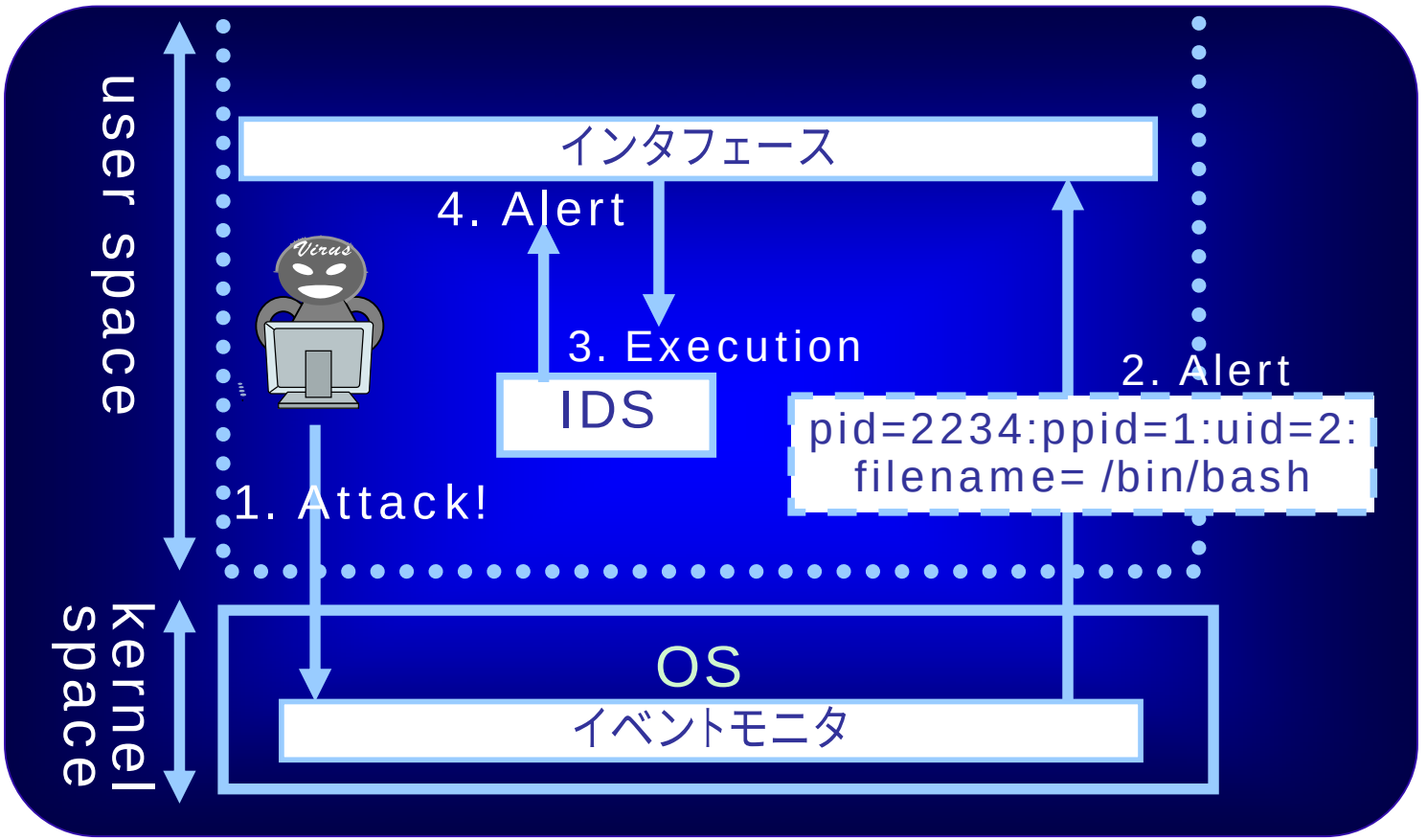
IDS自体の改造を伴わない。

➢ 解決方針

検知を開始する契機となるイベントの監視

課題の解決（２） リアルタイム検知のサポート

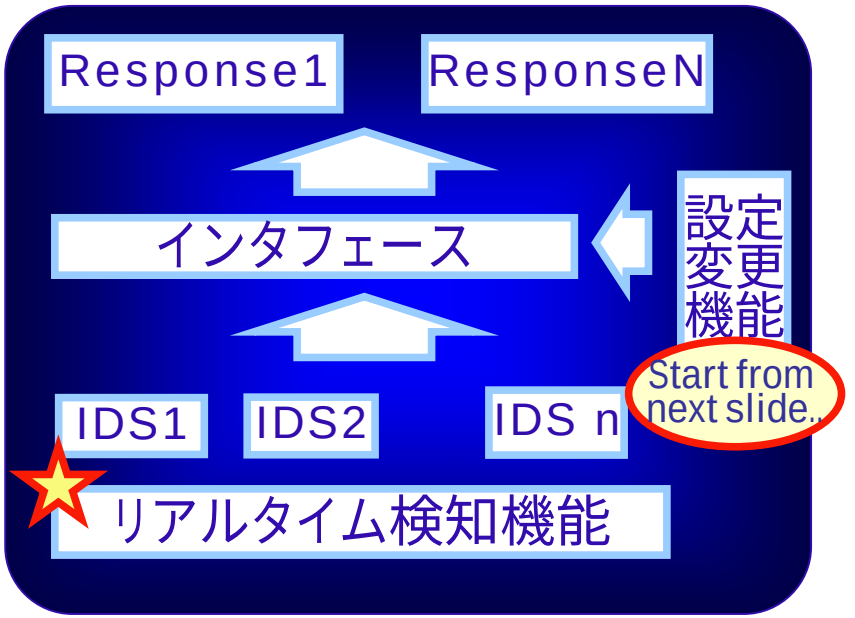
- OS内でシステムコールを監視・攻撃の兆候発生時にIDSを実行



※兆候とは、ここでは事前登録したファイル・ディレクトリ・リンク等の変更のこと

課題の解決（２） リアルタイム検知のサポート

- これまでのまとめ
  - ✓既存のIDSに共通の防御機能（Response 1....N）を適用可能
  - ✓侵入の兆候を契機として、IDSを実行することで、定期的に実行するIDSもIPSに適用可能となった。

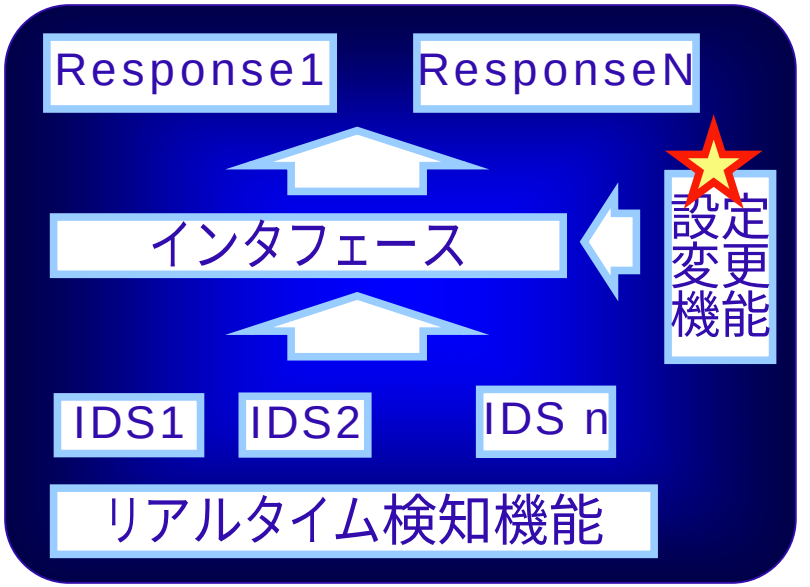


- ✓ただし、「事前設定に基づいて防御」しかできない。システム稼動中に発生した事象を参考にしながら効果的な防御を選択/実施可能とする。
  （次スライドから説明）

課題の解決（３） 動的設定変更

➢ 目的

✓稼動中に発生した事象を参考に効果的な防御を選択/実施



➢ 要件

✓ 目的に合わせ「防御選択基準」を適用可能

選択基準、手法は様々（攻撃回数、統計分析、管理者のTips...etc

➢ 解決方針

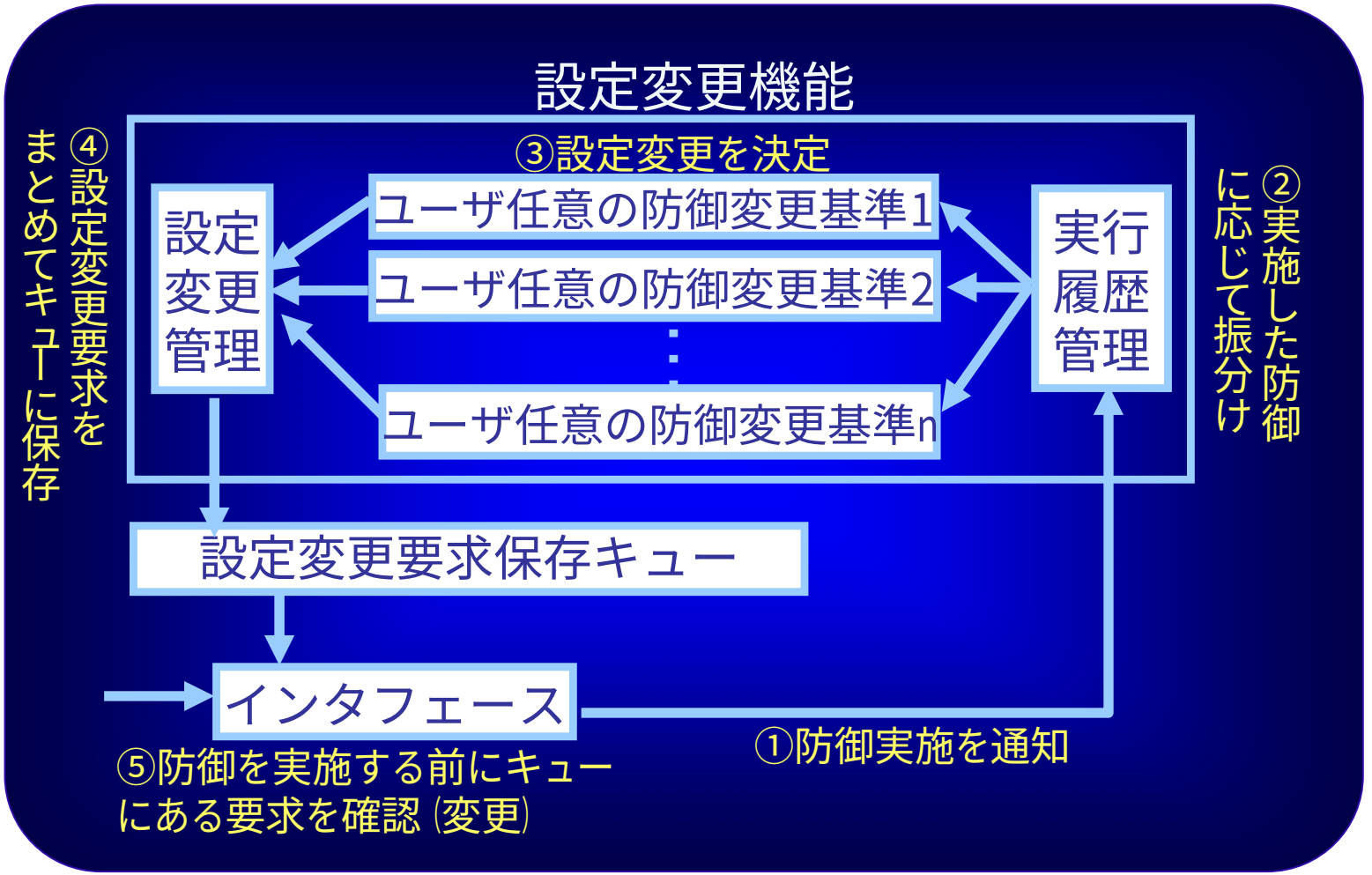
✓ 防御設定の動的変更※

✓ 変更タイミング、変更方法はユーザ任意の基準に基づく。

（※実施する防御の切替え、追加、延長、時間制約付実行をサポート）

課題の解決（３） 動的設定変更

➢ 基本動作



➢ 実施例：sshdへのポートスキャン

✓目的 ： 自サイト内でsshを提供する全ホストの露呈防止

```
Mar 13 08:02:51 69.243.174.94:3477 -> xxx.yyy.1.1:4899 SYN ******S*
Mar 13 08:02:51 69.243.174.94:3478 -> xxx.yyy.1.2:4899 SYN ******S*
Mar 13 08:02:53 69.243.174.94:3480 -> xxx.yyy.1.4:4899 SYN ******S*
Mar 13 08:02:51 69.243.174.94:3479 -> xxx.yyy.1.3:4899 SYN ******S*
Mar 13 08:02:53 69.243.174.94:3481 -> xxx.yyy.1.5:4899 SYN ******S*
[...]
```

全ホストに一斉スキャン！

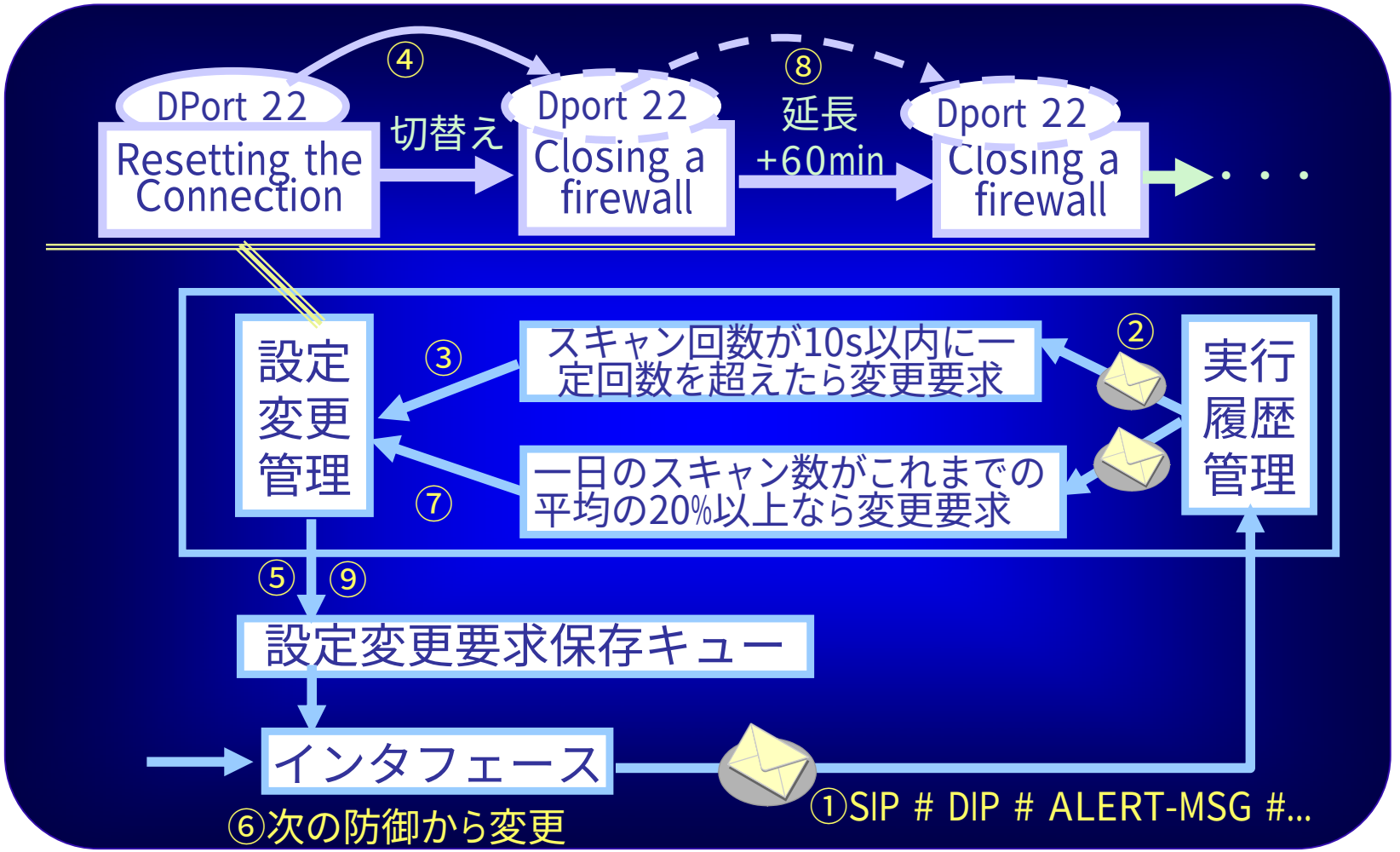
頻繁に発生するスキャンパターンの例 （出典： unilog-ML）

✓防御の困難性：解除のタイミング

✧「スキャン ⇒ 防御 ⇒ 防御解除」の繰り返しではいつかスキャン完了
✧ 攻撃者は任意の間隔でリトライ（一時間毎や頻繁にリトライ）
✧ 初めから「スキャン元は永遠にアクセス拒否」はサービス妨害の恐れ

課題の解決（３） 動的設定変更

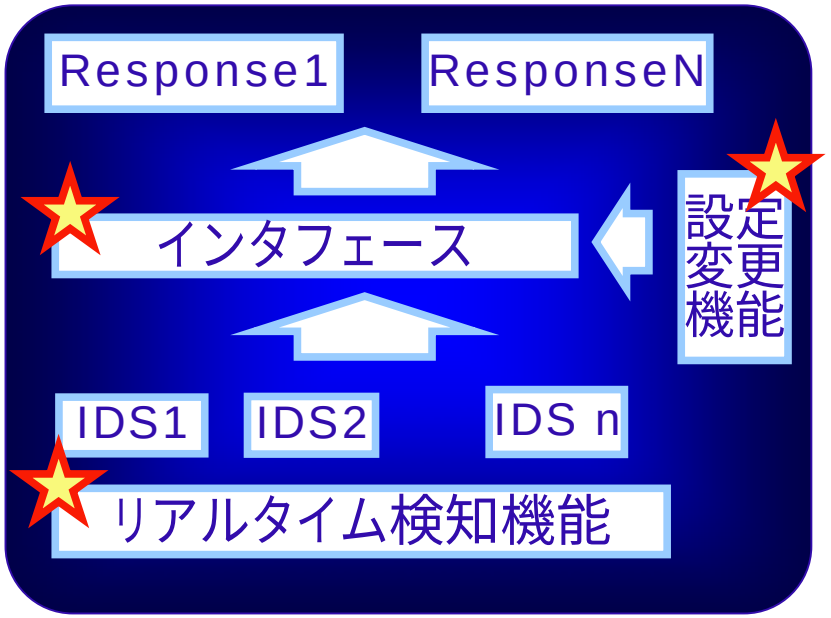
- 実施例・・リトライに対して除々に強力な防御を



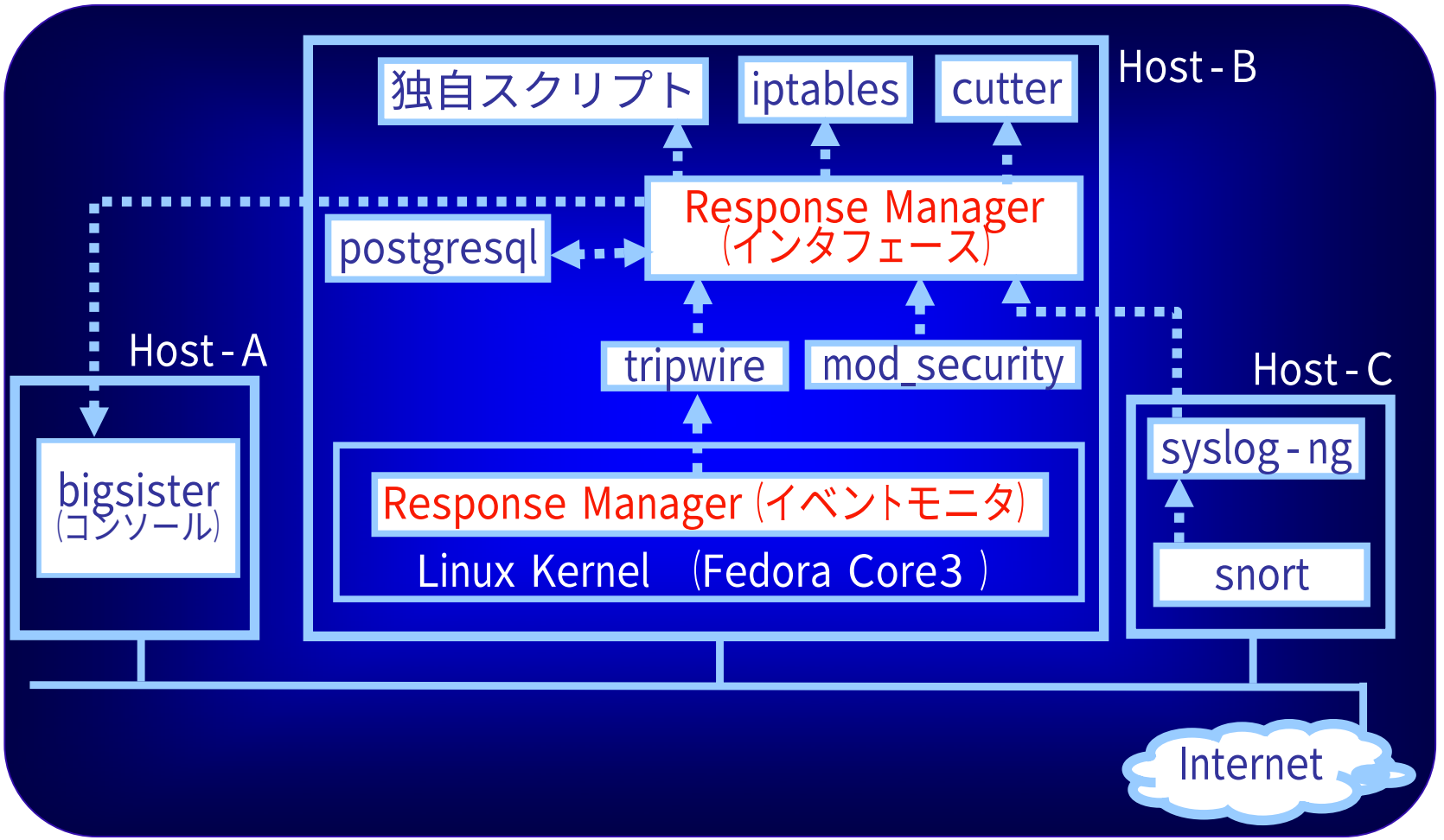
課題の解決（３） 動的設定変更

➢ まとめ

- ✓ 任意のIDSを用い、共通の防御機能（Response 1....N）を用いて防御が可能
- ✓ 侵入の兆候を契機として、IDSを実行することで、定期的に実行するIDSもIPSに適用可能となった。
- ✓ ユーザ任意の防御設定変更基準基づき、システムに行われた攻撃を元に、効果的な防御を選択可能



➢ OSSのIDSを統合してIPSを実現！

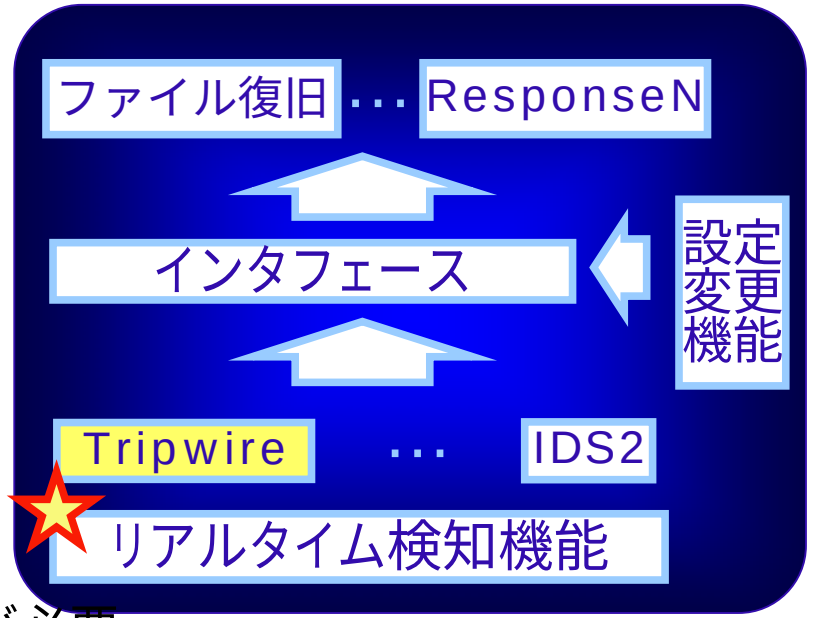


※Response Managerは開発コードです

利用例（1） 改ざんされたリソースの即時復旧

- 改ざん事件の多発
  - ✓ 2000～最近
    企業のウェブページ改ざん
    からファーミングまで

  未だ主要な攻撃手法の一つ



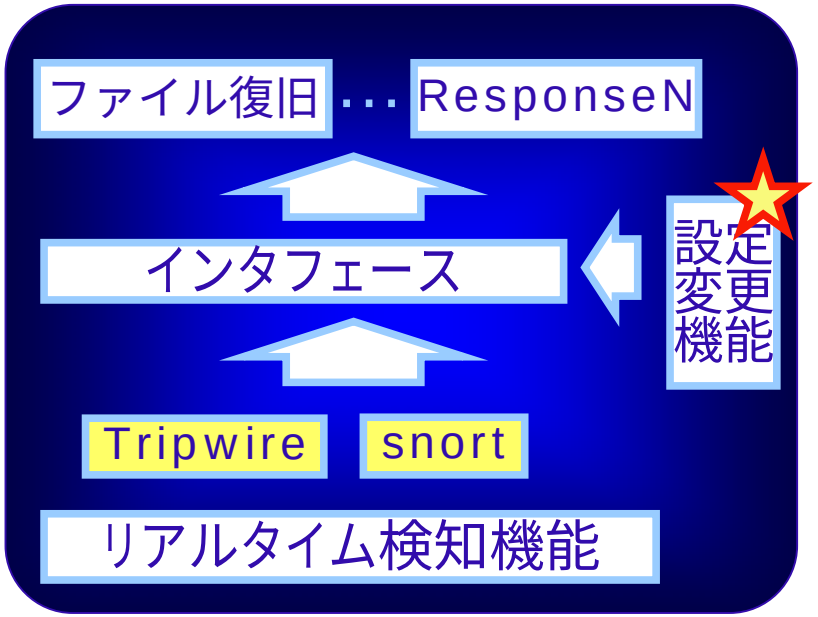
- 対策技術の課題
  - ✓ 「10分に一回チェック」では遅い
    改ざんによる被害がでる前に復旧が必要

- Response Managerの場合

  リアルタイム検知サポート機能で、改ざんの兆候を監視、
  Tripwireを起動させて詳細検査を実施可能であるため、
  改ざんによる被害が出る前に即時復旧が可能

利用例（２） WWWサービスへの適用

- WWWサーバへの攻撃
  - ✓ プロキシ配下に攻撃者と正規ユーザが混在（実際はそれすらわからない）



- 対策技術の課題
  - ✓ 正規ユーザを妨害しないよう軽度の防御となり、攻撃者に重度のペナルティが与えづらい。そのため攻撃者は、亜種攻撃等を何回も試していつか攻撃が成功する可能性

- Response Managerの場合

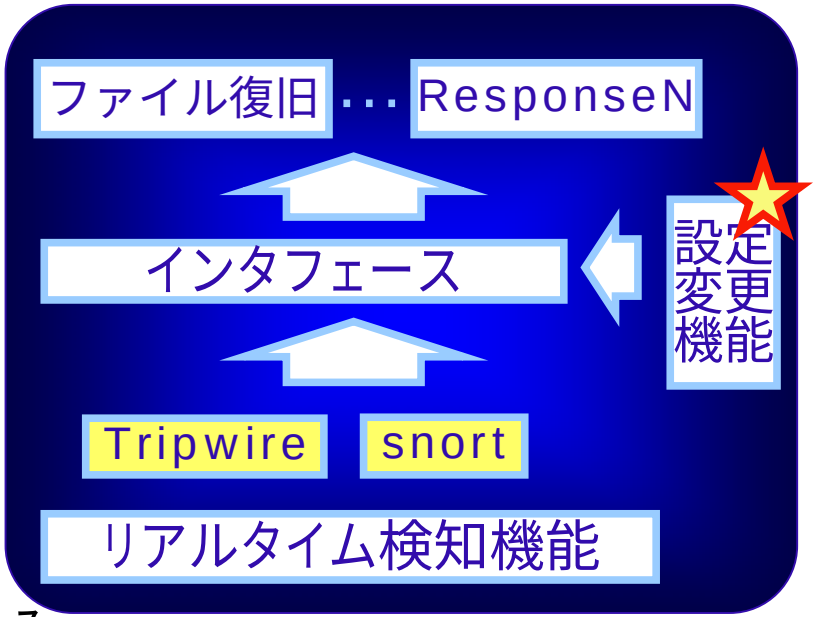
攻撃を多く行う攻撃者には強力な防御を徐々に適用

（攻撃発生時にコネクション遮断 ⇒「攻撃元IPアドレス+ポート番号」でアクセス拒否
⇒「攻撃元IPアドレス」でアクセス拒否⇒拒否時間延長 ・・・）

攻撃者が多く攻撃するほど、次の攻撃が困難になる。
攻撃者と正規ユーザの混在環境でも、正規ユーザへの妨害は少ない。
（サーバの認証通過履歴等の追加情報も考慮して防御変更を行えばより高い効果も期待）

利用例（３） 攻撃の時間/場所に注目した防御

- ウィルスによる攻撃
  - ✓拡散は、コンピュータの電源がONの時間帯に発生エリアから徐々に
- 人手による攻撃
  - ✓ 24時間攻撃が続くわけではなく、人の活動時間に限られる



- 通常の防御手法では
  - ✓事前に設定した内容に基づいて防御のみ
- Response Managerの場合

  日ごとに攻撃回数を集計、攻撃の多いIPアドレスを算出、
  多く攻撃する時間帯には、事前にアクセス拒否

亜種攻撃、新攻撃の発生時に、攻撃される前に防御する効果

まとめ

- OSSのIDSを統合させたIPSの構築
  - ✓ 防御機能を持たないIDSにも防御機能を付与するインタフェース
  - ✓ 定期実行型IDSの高機能な検知機能を生かした即時検知サポート
  - ✓ 稼動中に発生した事象を参考に適切な防御を選択する動的防御変更

  (一つ一つのOSSに適用した場合でも、各OSSの能力向上効果がある)

- OSSのIDSを適用した実装と利用例
  - ✓ 改ざんリソースの即時復旧による被害抑止効果
  - ✓ 段階的に防御を強めることによるサービス妨害抑止効果
  - ✓ 時間/場所の特性に注目した事前防御効果
- 今後の課題
  - ✓ 防御選択の動的変更に関して、利用例を増やす

ご静聴ありがとうございました
(*Questions?*)