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

通知後の対応

インシデントレスポンス (Incident Response)

- IDSからの通知で攻撃または不正行為の発生を知る
  - ⇒ 調査のきっかけ
- ログ等の記録から攻撃内容を把握
- 原因、影響範囲の特定、復旧計画の立案
- 防御改善策、再発防止のためのレポート作成

IDSの問題点

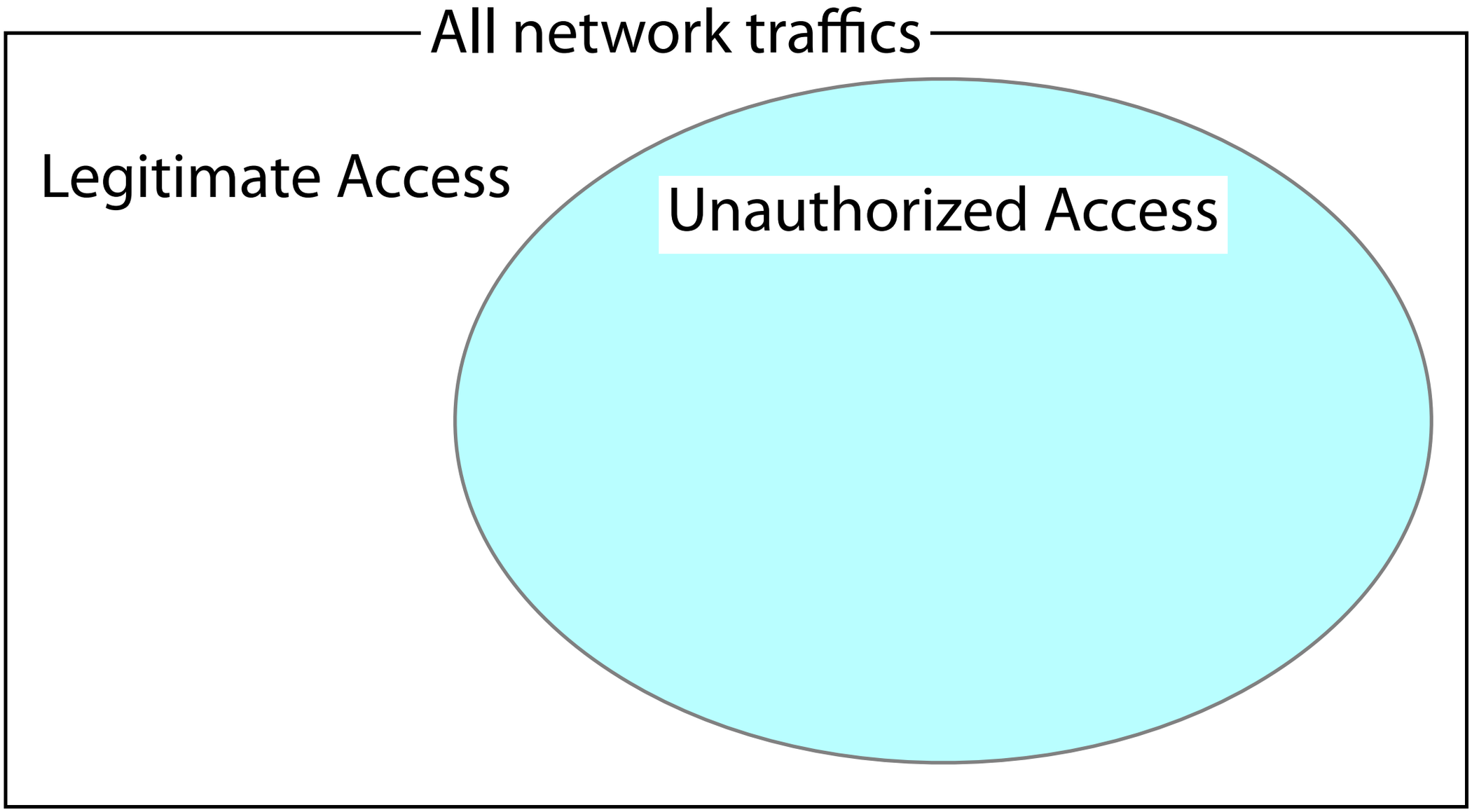
- 誤検知
  - 検知回避
- 運用管理と監視
- 法的問題 (Privacy)

誤検知

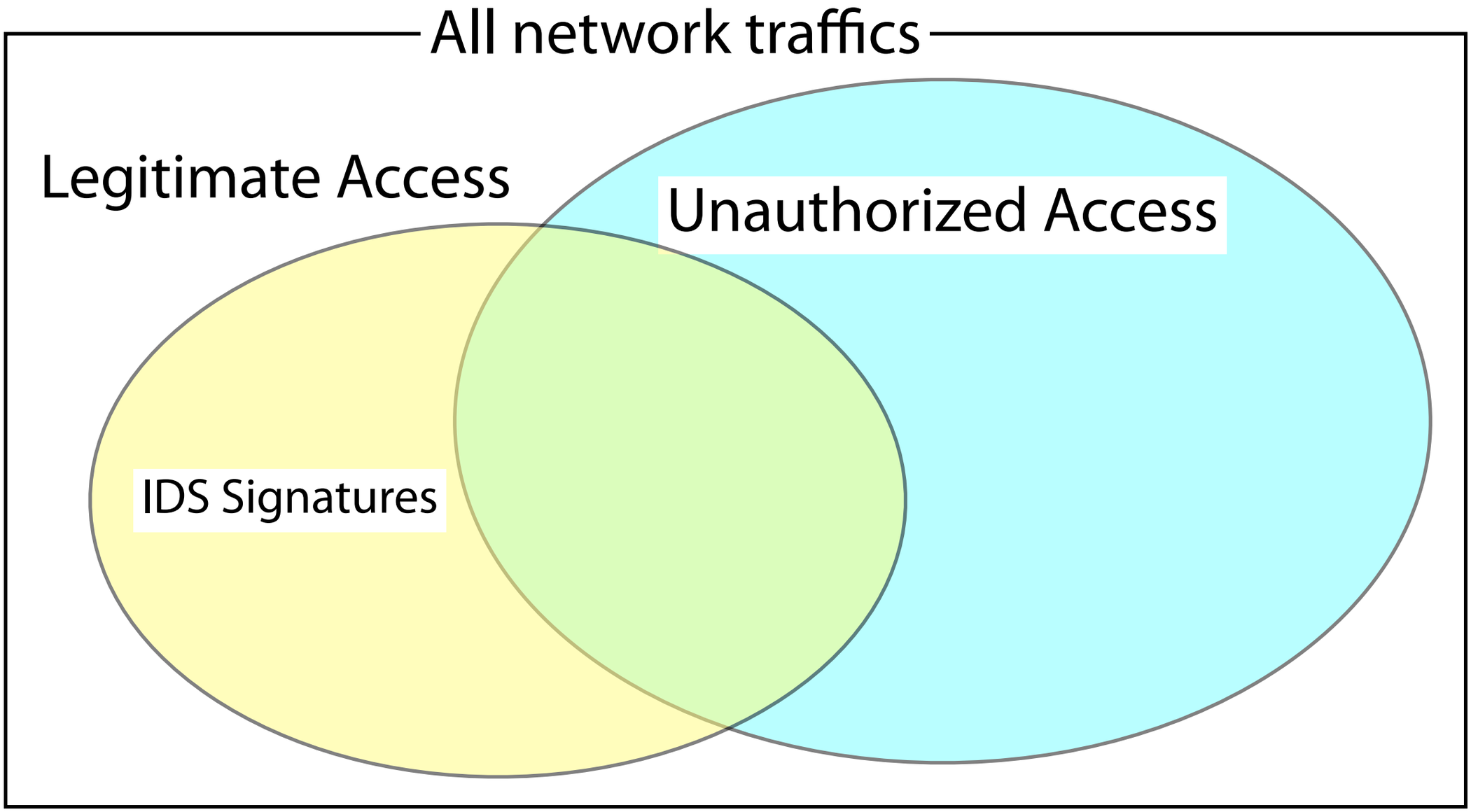
- 誤検知 ⇒ 不正侵入の判定誤り
  - IDSの性能評価項目の1つ
- ２種類ある
  - **false positive**
    - 不正侵入ではないものを「不正侵入」と判定
  - **false negative**
    - 不正侵入を「不正侵入ではない」と判定

理想的にはどちらもゼロ

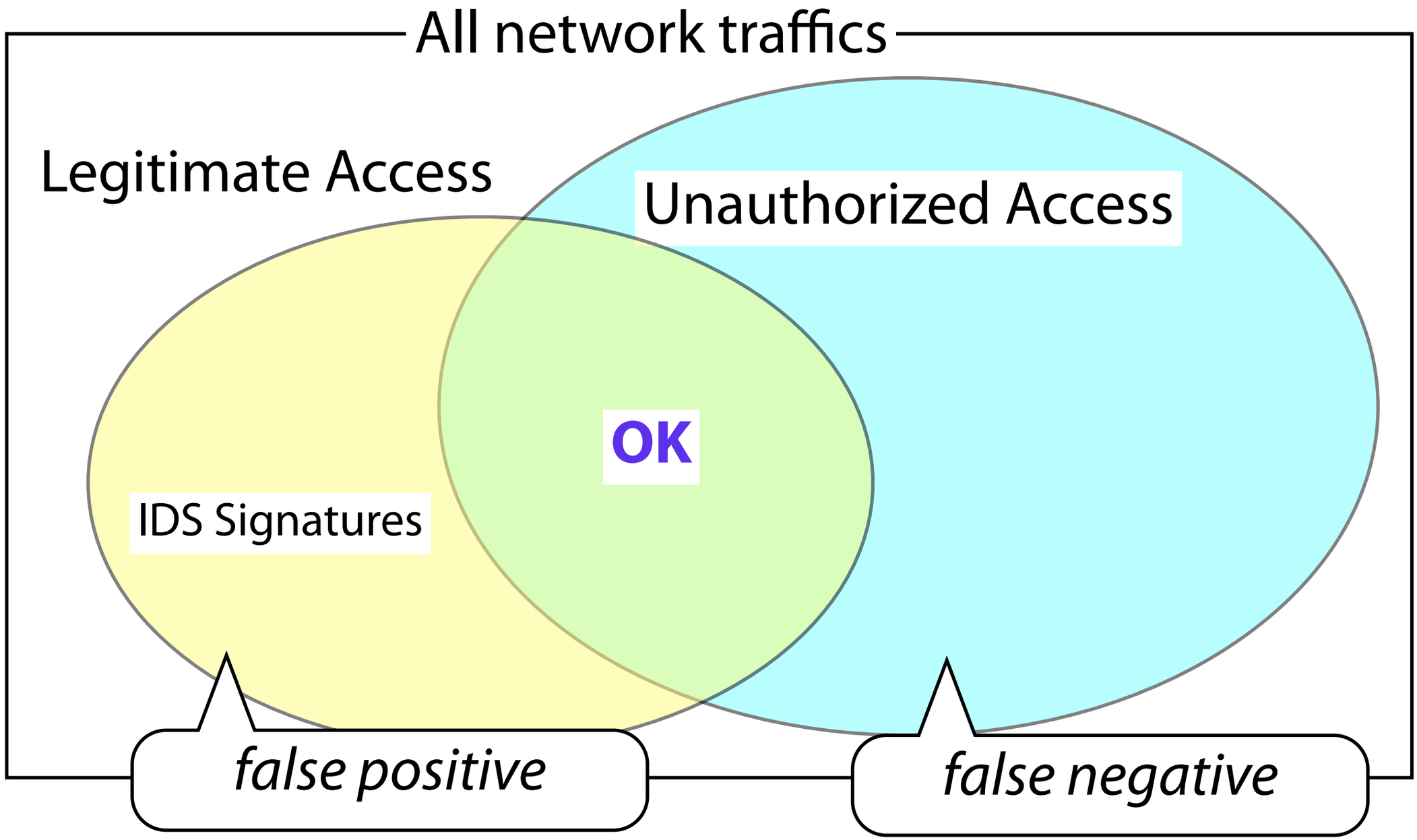
図解 - 誤検知


All network traffics
Legitimate Access
Unauthorized Access

図解 - 誤検知


All network traffics
Legitimate Access
Unauthorized Access
IDS Signatures

図解 - 誤検知


All network traffics
Legitimate Access
Unauthorized Access
OK
IDS Signatures
false positive
false negative

誤検知 (Cont.)

- false positive が多いと...
  - ⇒ 不正侵入のアラート(通知)が多数発生
    - 「正常事象」が不正侵入として多数警告される
  - ⇒ 運用担当者が通知を無視し始める
    - 多くの警告は「正常事象」だったから...
    - ⇒「ま、大丈夫だろう」(IDSの形骸化)

誤検知 (Cont.)

- false negative が多いと...
  - ⇒ IDSの意味がない
    - 検知すべき「不正侵入」が検知されない
  - 誤った現状認識を生む
    - A氏:「今日もIDSからの警告ないな」
    - B氏:「我が社のサーバを攻撃する人なんていないさ」
    - 現実: IDSが検知すべき事象を検知できていなかった...

誤検知と検知手法の関係

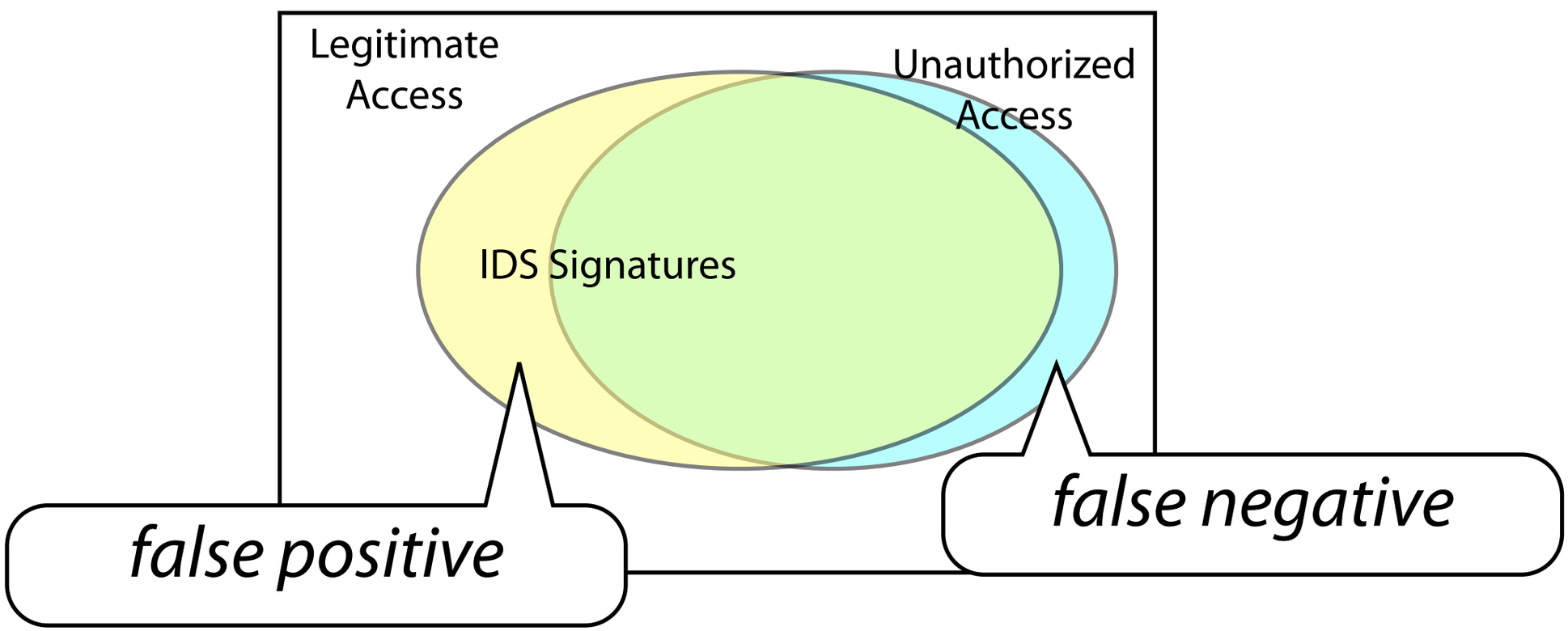
	不正検出 (Misuse)	異常検出 (Anomaly)
false positive	低い	高い
false negative	低い (条件付き)	低い (条件付き)

誤検知 - 考察

(1) 不正検出のfalse negativeが低くなる条件

発生しうるすべての不正侵入手法の特徴情報を
Signatureとして保持していることが前提

⇒ **容易ではない(困難)**



誤検知 - 考察

(2) 異常検出のfalse negativeが低くなる条件

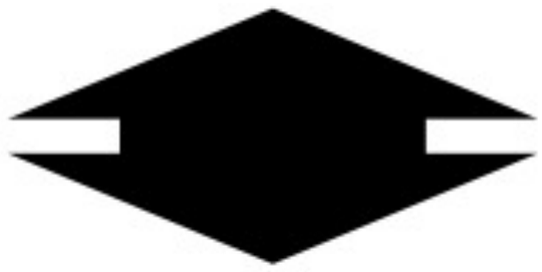
- false positiveが高いことの裏返し
  - ささいな事象も「不正侵入疑い」として検知すれば、false negativeは低下
- ⇒ **誤検知が多発、運用が大変に**

誤検知 - 考察

現状はトレードオフの関係

false positiveを意図的に低くする

検知すべき不正行為に対しても**鈍感**になる



false negativeを意図的に低くする

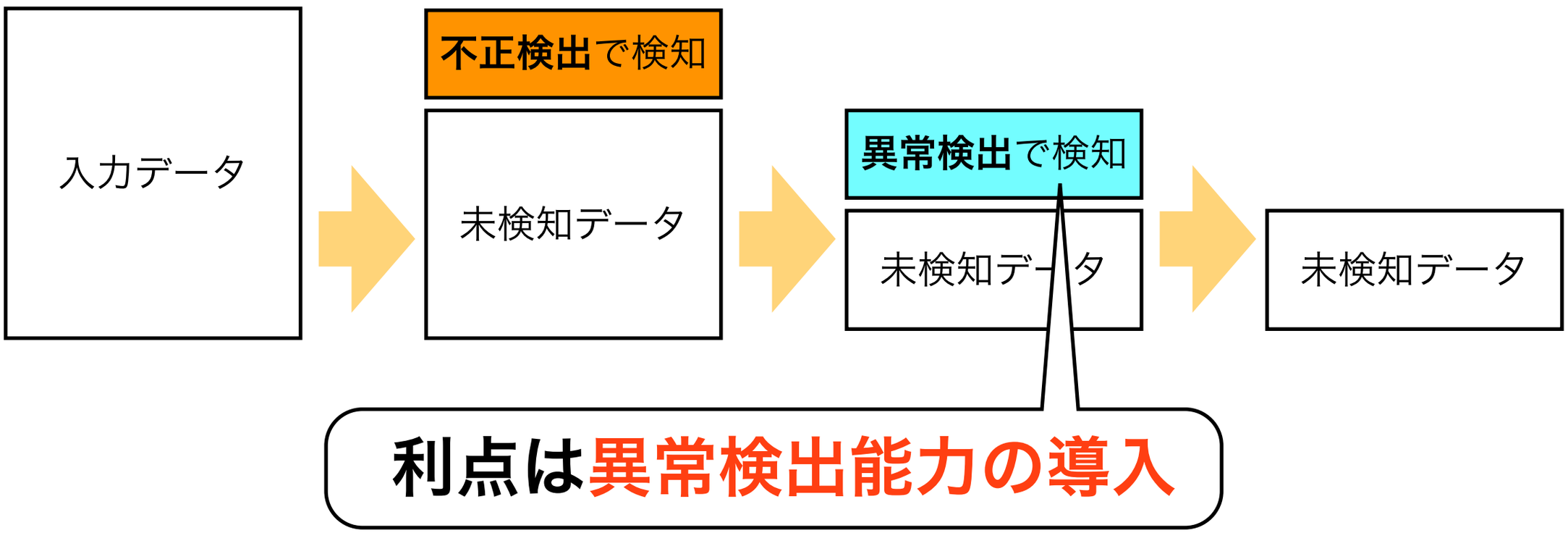
不正行為でないものまで不正行為として検知

どれが真に注意を払うべき警告か不明確になる

ハイブリッド検出

不正検出と異常検出を組み合わせた手法

1) まず不正検出で不正侵入検知
2) 特徴情報のない不正を異常検出で検知



検知回避

- 誤検知
  - IDS自身の問題
- 検知回避
  - 攻撃者: IDSに検知されずに攻撃したい
    - IDSや設置環境、Networkの仕組みを逆手にとる

主な方法

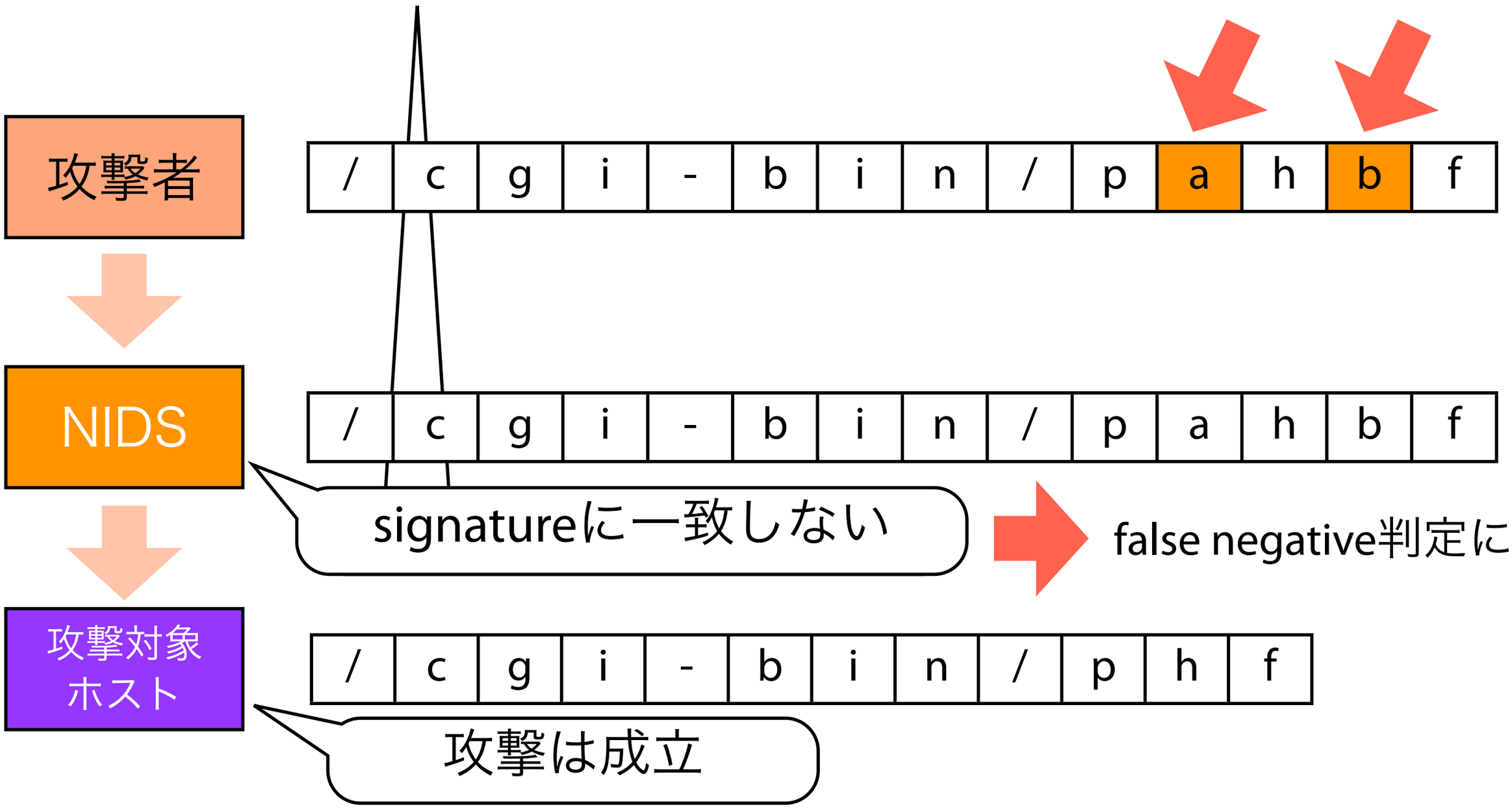
- Insertion (挿入) と Evasion (回避)
  - どちらも「攻撃対象ホスト」と「IDS」が認識するデータが異なるように細工する手法

Insertion (挿入)

- 以下のデータを意図的に挿入
  - IDSは、データとして認識する
  - 攻撃対象では、データ処理されない
- 「IDSは、攻撃対象ホストよりもpacketの検査/処理が厳格ではない」という特性を利用

Insertion (挿入)

仮定:“/cgi-bin/phf”というsignatureがIDSに存在する

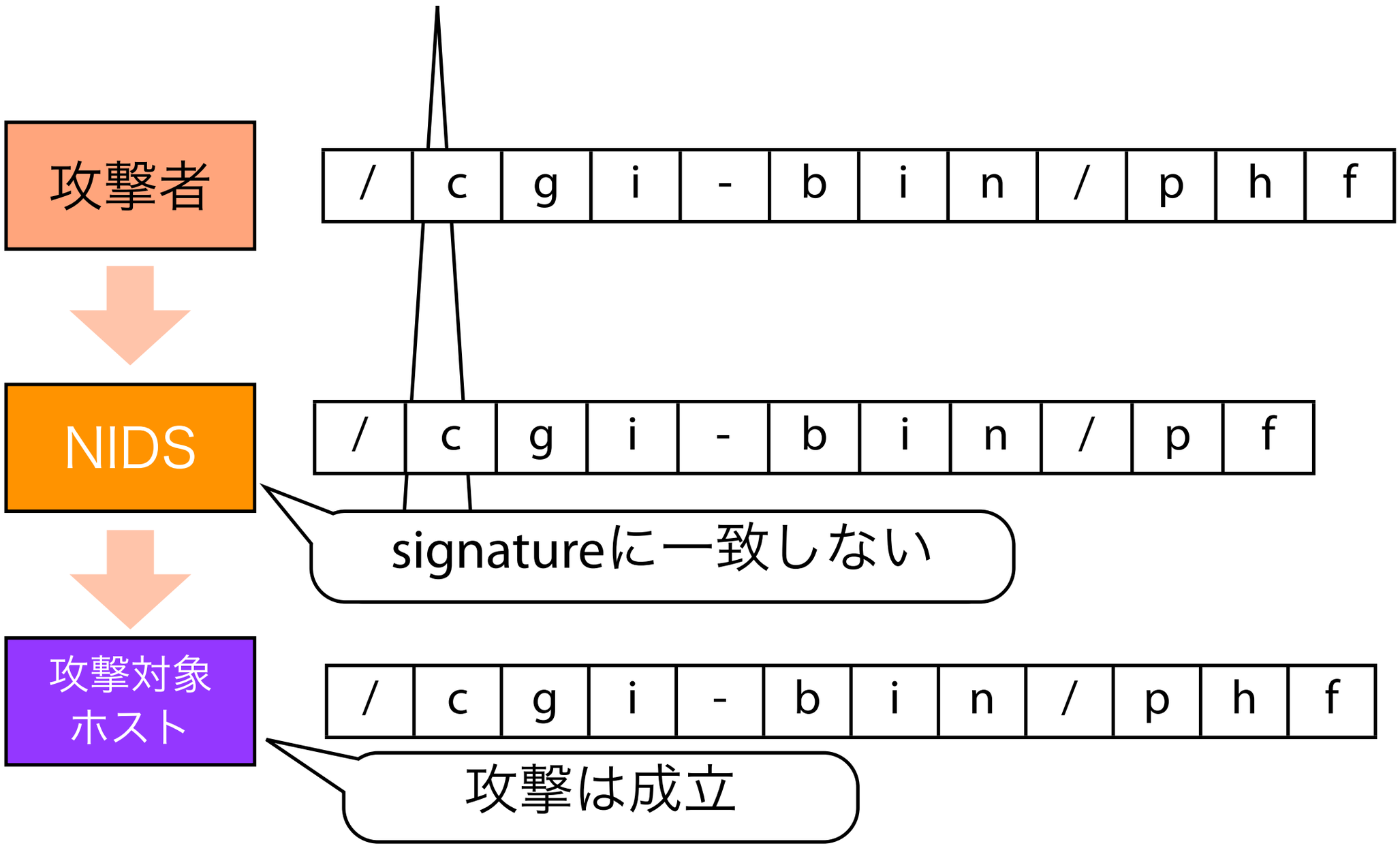


Evasion (回避)

- Insertion による検知回避を避ける
  - ⇒ IDSにおける packetの検査/処理を厳格化
- 逆の問題が発生する
  - 攻撃対象では、データ処理される
  - IDSでは、データとして処理されない
- targetが明確ではない(複数である)ことが多いがゆえの問題

Evasion (回避)

仮定:“/cgi-bin/phf”というsignatureがIDSに存在する



使われる手法

- IDSと攻撃対象で処理が異なるnetwork packet
  - 例)
    - IP checksumが誤っているIP packet
    - 存在しないMac addressのethernet frame
- IDSはすべてのpacket/frameを受信し、処理するためこれらのデータは処理される．しかし一般の計算機は無視または破棄 ⇒ Insertionが成立

使われる手法

- IDSまで届くが攻撃対象には届かないpacket
  - 例)
    - IP packet の Time To Liveを調整する
      - IDSと攻撃対象にRouterが存在すれば...
    - SizeのSizeの大きなpacketをDF flag付きで配送
      - 通信経路上に、packet sizeに上限のある通信路があれば...
- どちらもNetworkや設置環境を応用

使われる手法

- IP fragmentation
  - これもIDSと攻撃対象ホストの動作差を利用
    - 攻撃対象ホスト: 再構築
    - IDS: 再構成しないものがある
    - IDS: 再構成するものの、先着順再構築
      - offsetを見ない...
    - 同一packetが重複して受信した場合の再構築法の差
      - Protocol stackの実装による ⇒ 包括対応が困難

使われる手法

- TCP 処理の悪用
  - IP fragmentと同様の回避手法
    - 攻撃対象ホスト: TCP stackの実装に基づき処理
    - IDS: IDSの実装に基づき処理
  - TCP segment分割に関する細工
  - Sequence番号に関する細工
  - TCP headerの偽装 (ありえない状態の意図的作成)
  - 3-way handshakeによる錯乱

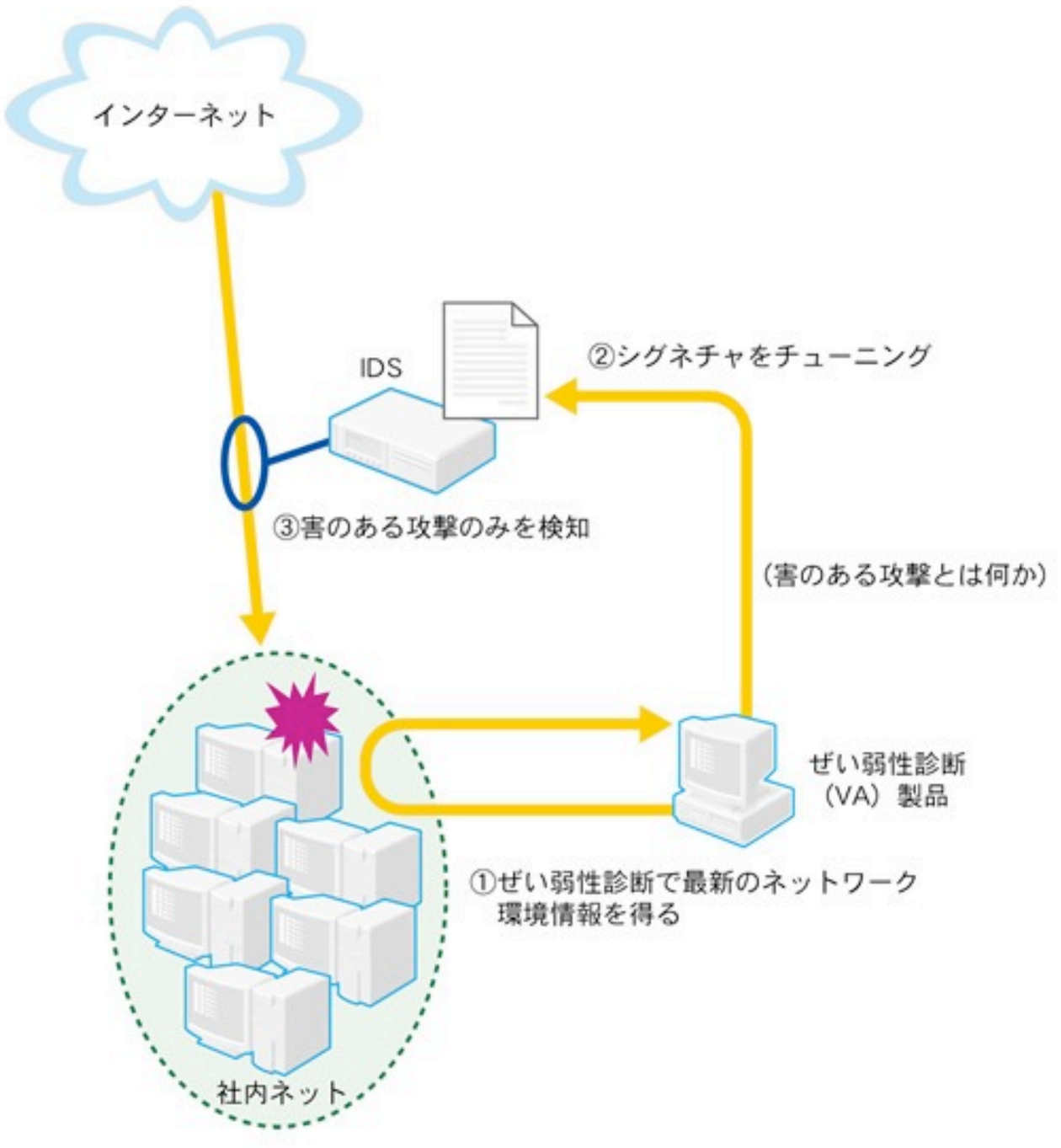
Dos攻撃

- NIDSを対象とした妨害方法
  - 情報収集もれ
  - 検知処理もれ
  - 通知不能
- 容量よりも単位時間あたりのpacket数がIDSのbottle-neckになる傾向

運用管理と監視

- 継続が重要
  - 「知る・守る・**続ける**」
- 人間の対応 (運用管理 - system administration)
  - 不正検知：Signatureの更新と調整
    - 誤検知を低減．監視対象システムへの適応
    - 新たな脅威への対応
  - 通知後の対応
    - 緊急対応や誤報判定
    - 「インシデント前」レスポンス

Signatureのチューニング



- 監視対象の脆弱性を評価(VA: Vulnerability Assessment)
- 残されている脆弱性のSignatureのみをIDSのRule databaseへ
- 監視対象にとって実害のある通信を検知

図引用: http://itpro.nikkeibp.co.jp/article/lecture/20070903/280956/

環境構築

- NIDS
  - Switching機器による情報収集の問題
  - 暗号化trafficに対する対応
- HIDS
  - 監視対象からの情報収集を可能にする設定
  - 脆弱にすることなく、上記目的を達成する

法的問題

- Privacyの問題
- NIDSはDPIによる処理が基本
  - DPI: Deep Packet Inspection
    - ⇒ Packet payload内の情報を基に処理を行うこと
- Network packetのpayload部分を許可なく見ることは「通信の秘密」に関する法律違反
  - Security Policyの制定、利用者への事前周知は必須

学内でも

9.1 情報セキュリティインシデント発生の把握

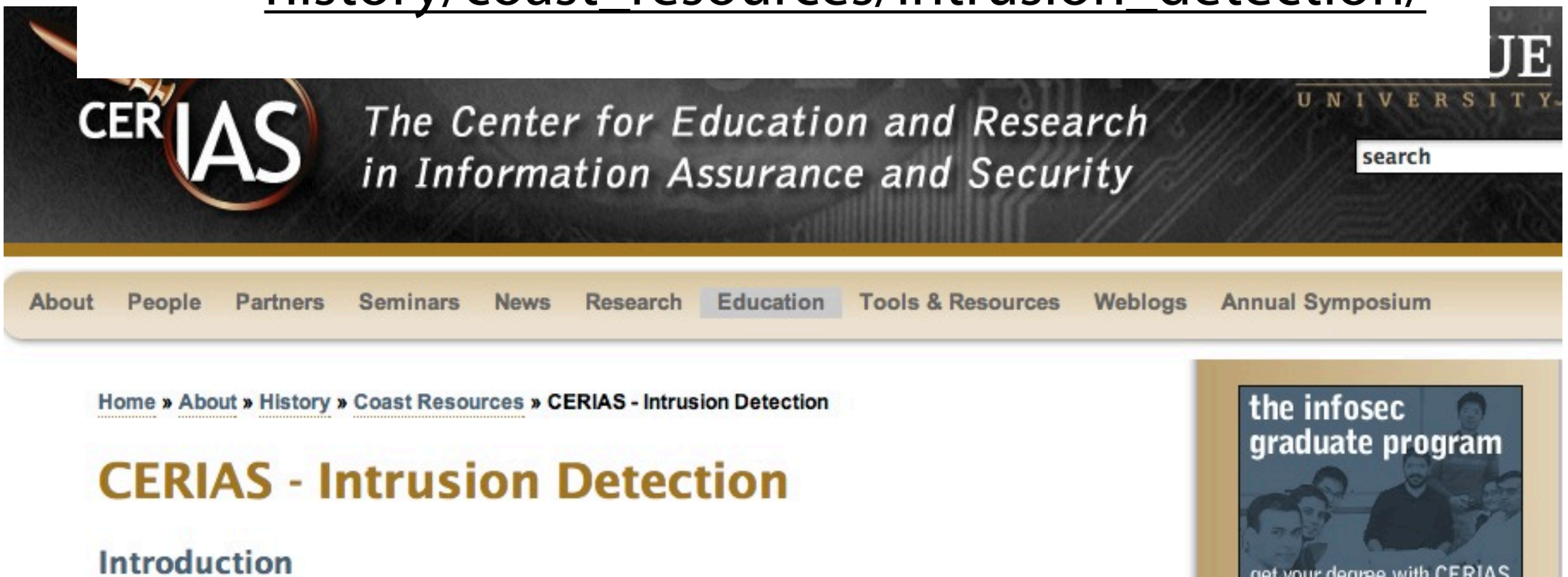
侵入検知システムを含む情報システムのログ情報、学外にある公開情報、学外からの通報等により、インシデントが発生したと確認する。

情報システム運用・管理実施手順書の運用開始について

http://www.cc.uec.ac.jp/info/news/2014/01/20140108manual.html

システム例

- 商用およびOpen sourceまで多様なシステム
  - 研究Project一覧 - CERIUS Intrusion Detection
  - http://www.cerias.purdue.edu/site/about/history/coast_resources/intrusion_detection/



OSSのHIDS

- 多機能HIDS (複数台の集中監視、ログ監視、file改ざん検知、Rootkit検出、即時対応)
  - OSSEC

- fileの改ざん検知システム
  - AIDE - Advanced Intrusion Detection Environment
  - Tripwire

OSS = Open Source Software

OSSのNIDS

- Snort
  - 最も著名

- Bro - The Bro Network Security Monitor
- Suricata - Open Source IDS/IPS/NSM engine

IDSの評価項目

- **検知機能**　　的確に不正を検知
- **通知機能**　　迅速かつ確実な通知
- **診断機能**　　攻撃診断が可能 (どんな攻撃手法か？)
- **検知対象領域**　検知対象手法の多様性
- **使用資源**　　必要な計算資源の量
- **負荷耐性**　　高負荷時における検知性能劣化度
- **利用可能性**　　どんな機器/情報源/設置場所が必要か