6学期講義

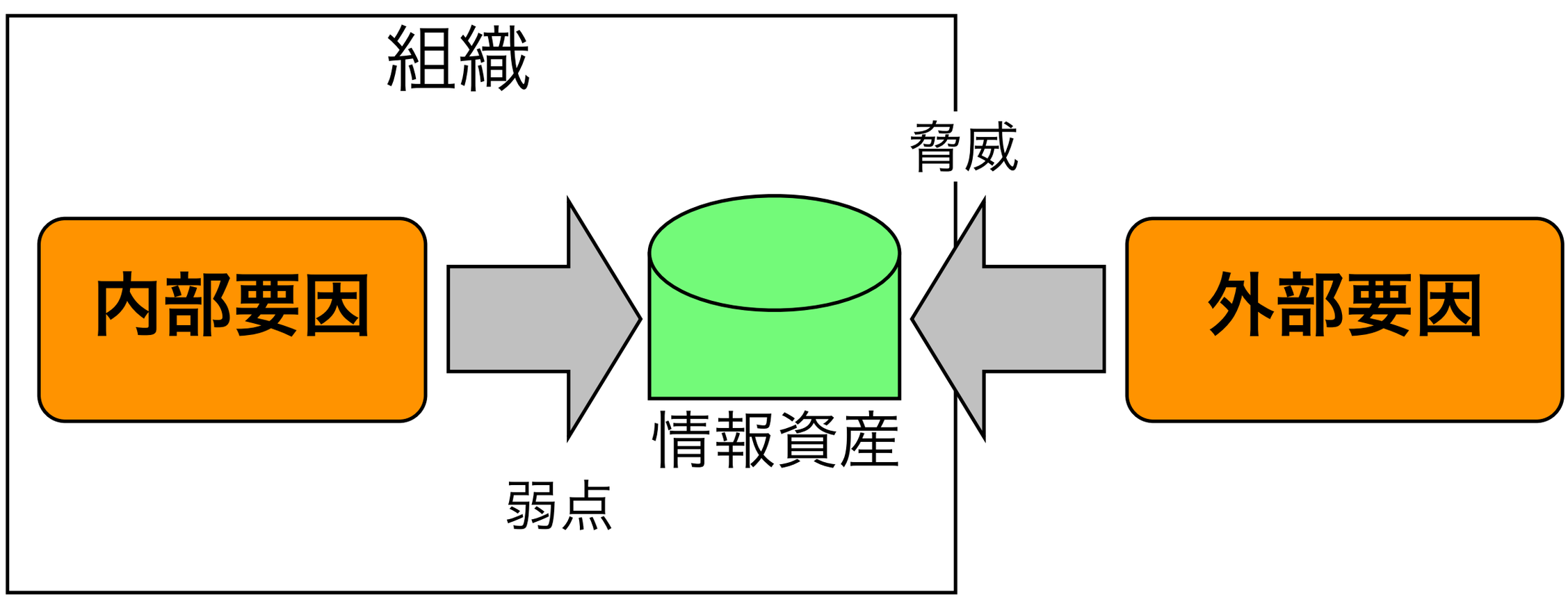
Network Security

Introduction

総合情報学科

リスク要因

- リスク要因: CIAの各要素が脅かされうる原因
- 組織の内外に存在 (境界は組織)



外部からのリスク要因

1. マルウェア (Malware)

2. 不正アクセス/不正侵入 (Intrusion)

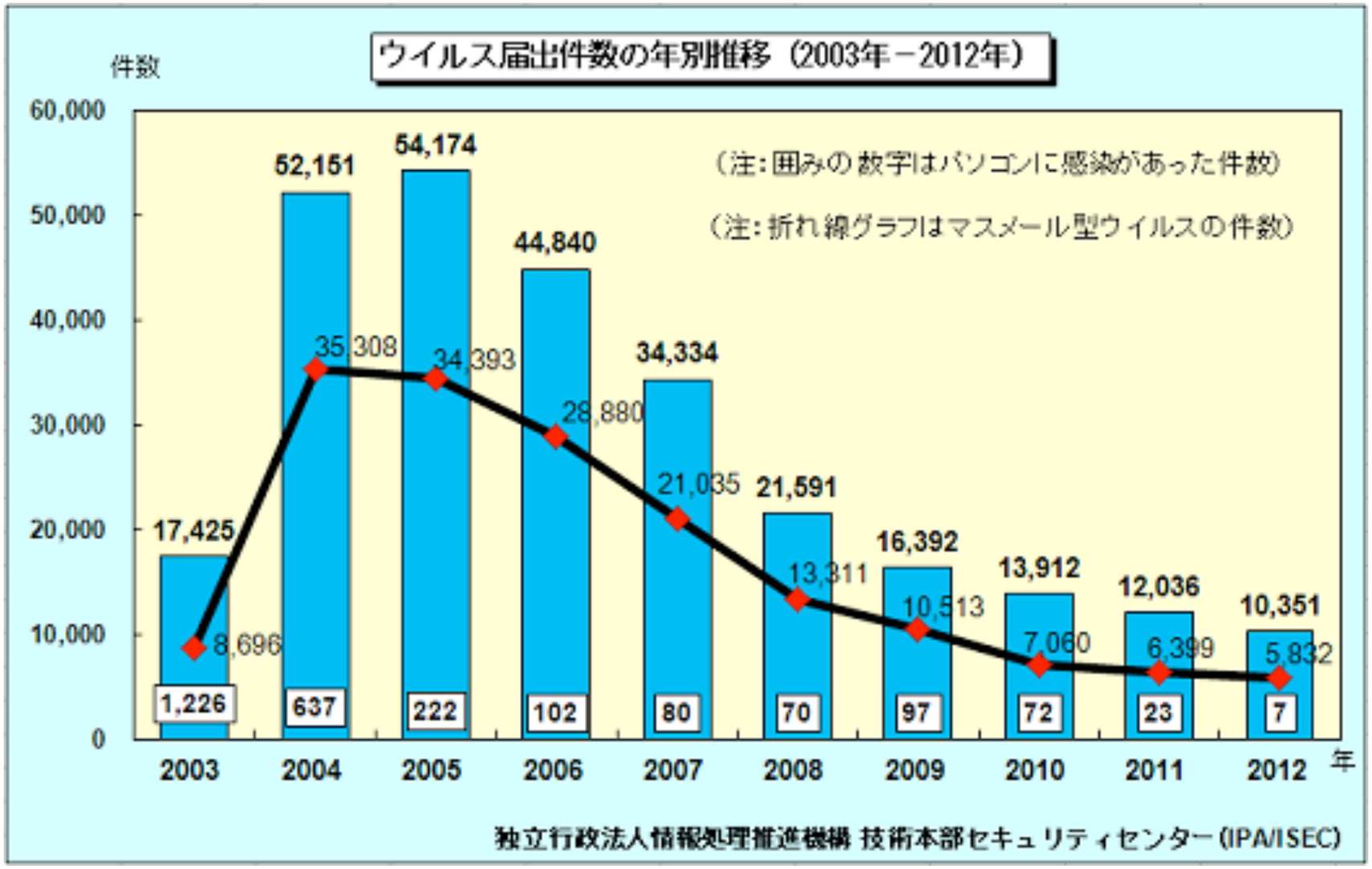
3. サービス妨害攻撃 (Denial of Service Attack)

マルウェアとは

- 不正かつ有害な動作を行うことを**意図して**作成されたソフトウェア
  - **Mal**icious Soft**ware** → **Malware**
- 以下の総称：
  ウィルス(Virus)、ワーム(Worm)、スパイウェア(Spyware)、トロイの木馬(Trojan horse)、ボット(bot)、ランサムウェア(ransom ware)...

ウィルス届出件数

報告数としては2005年をピークに減少傾向



引用: IPA, https://www.ipa.go.jp/security/txt/list.html

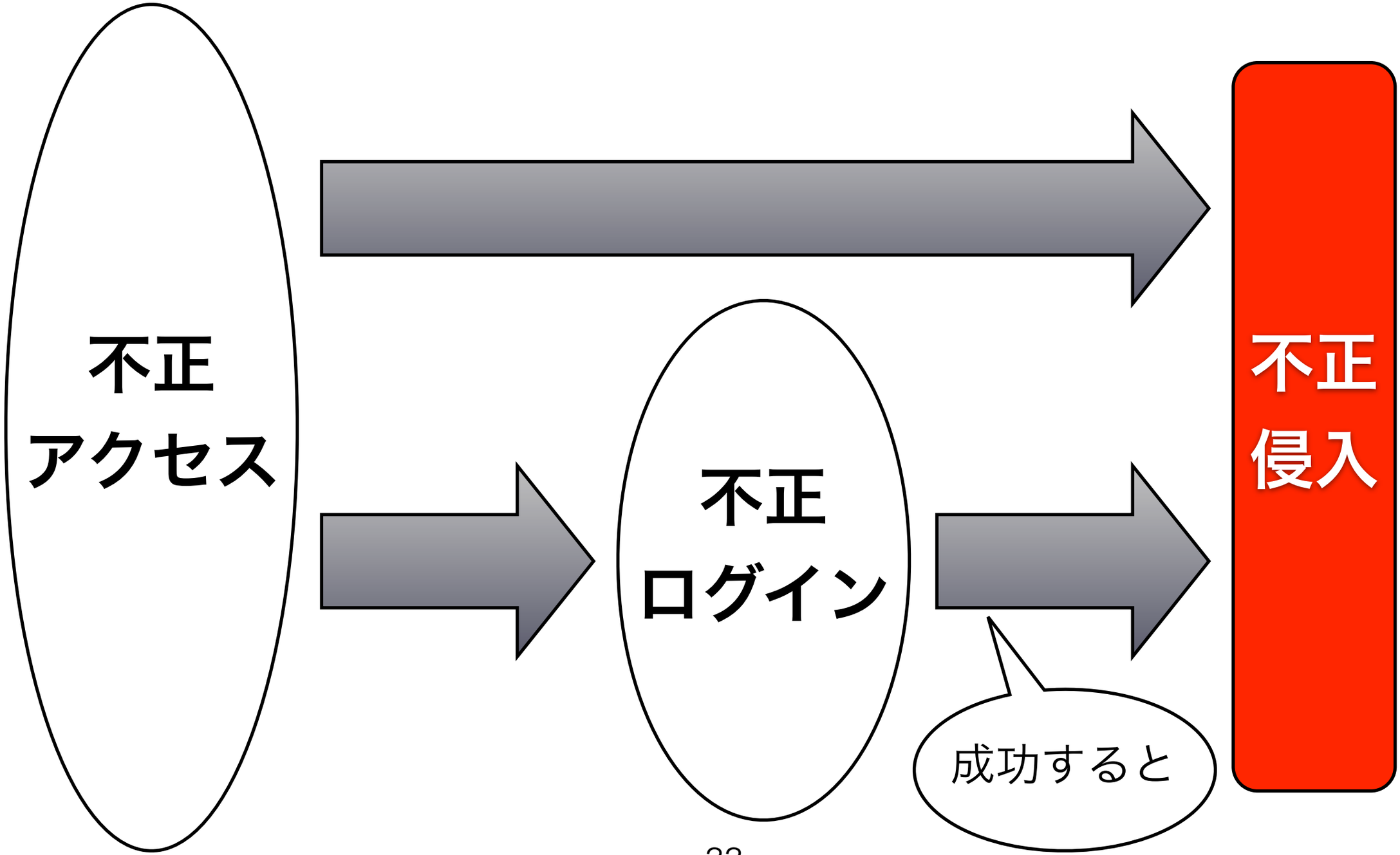
脅威の見えない化

- Malware感染の兆候が見えにくい
  - 実態(推測)：以前同様かそれ以上の被害数が存在する
- 理由：攻撃者の「流布動機」が変化
  - 以前: **能力誇示** ⇒ 現在: **金銭目的**
  - 攻撃者の理想：不正行為の長期間実行
    ⇒ 感染隠蔽の工夫が進化、巧妙化している

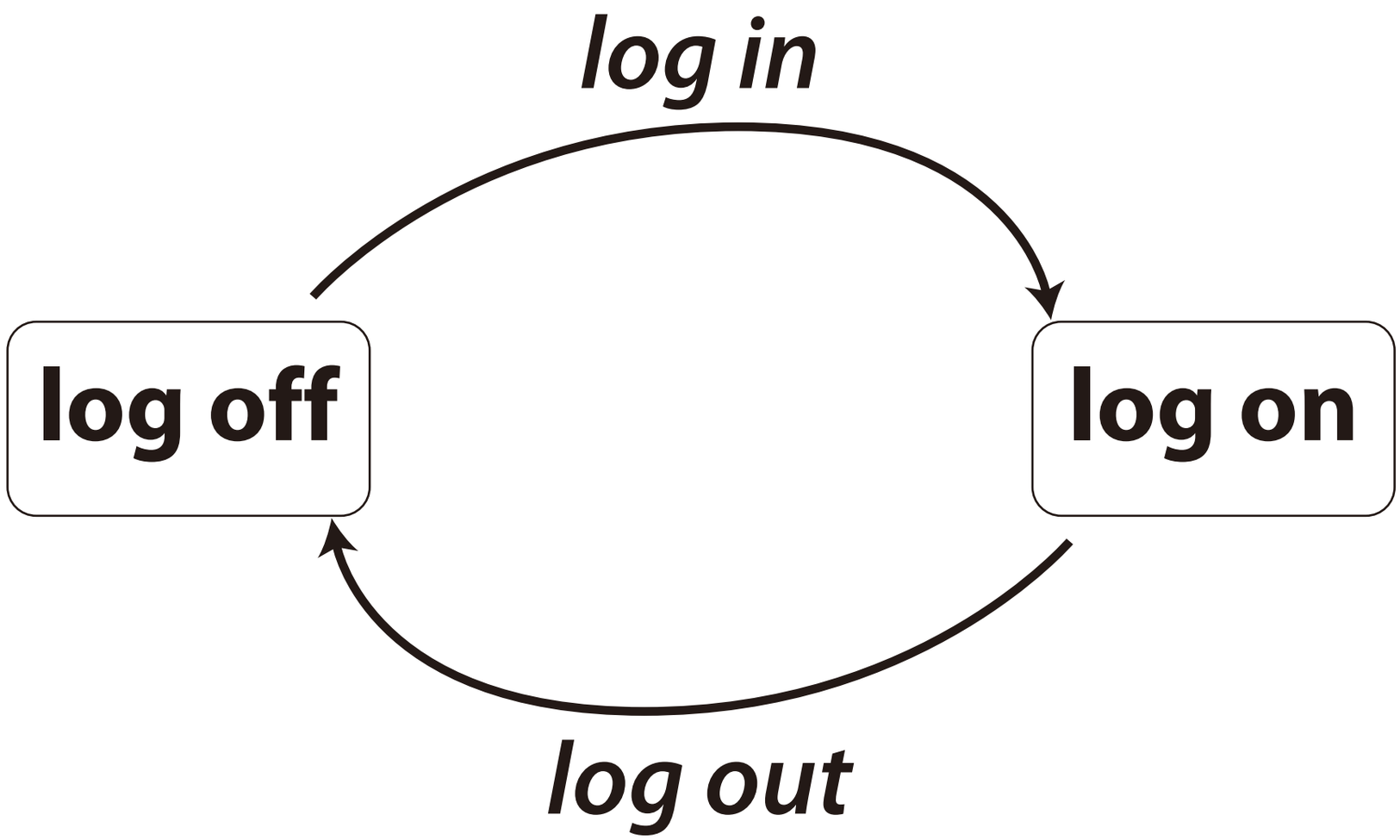
外部からの侵入(不正アクセス)

- 不正アクセス
  - 利用権限のない計算機にアクセスし、接続を試みること
- 不正ログイン
  - 利用権限のない計算機に対し、第三者のユーザ名とパスワードでログインを試みる行為
- 不正侵入
  - 利用権限のない計算機に侵入またはログインして、不正に利用する行為

これら3つの関係は?



4つの言葉の関係



“log on”,“log off”は状態を表し、”log in”,“log out”は行為を表す

不正侵入 ４つの手順

計算機への不正侵入

事前調査

権限取得

不正実行

後処理

住居侵入による窃盗

鍵のかけ忘れたドア
開いている窓の探索

住居へ侵入

金品の窃盗

指紋拭き取り
証拠隠滅

事前調査

- 攻撃対象となるシステム情報の収集
  - IPアドレス、サーバ名、サーバソフトウェア
  - OSの種類、バージョン
  - 提供されているネットワークサービス
    - Port scan (ポートスキャン)
- Webサイトの調査

権限取得

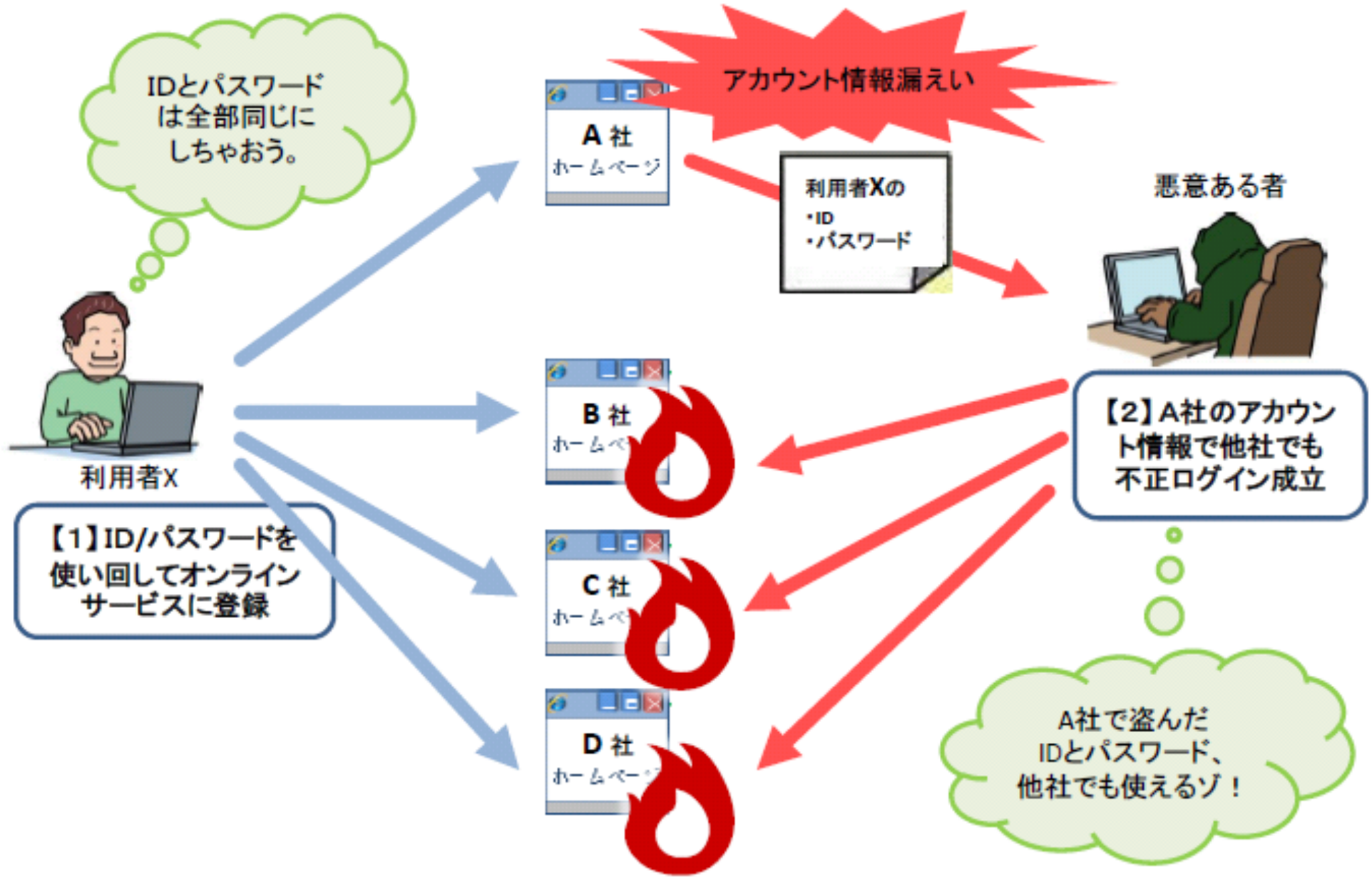
- パスワードクラッキング

  パスワードを取得 ⇒ 不正ログイン⇒ 権限取得

- パスワードクラッキングの手法
  - Brute-force攻撃 (総あたり攻撃)
  - 辞書攻撃

    ⇒ 特殊な辞書を使用して照合
  - 推測攻撃
  - パスワードリスト攻撃

パスワードリスト攻撃



図引用: IPA, https://www.ipa.go.jp/security/txt/2013/08outline.html

不正実行 (1/2)

- 盗聴
  - ネットワーク上のデータを不正入手
- 改ざん
  - データ/設定情報を不正に書き換え
- なりすまし
  - 自分以外の第三者をよそおい、悪事実行
- 破壊
  - データ/プログラムの削除、HDDの初期化

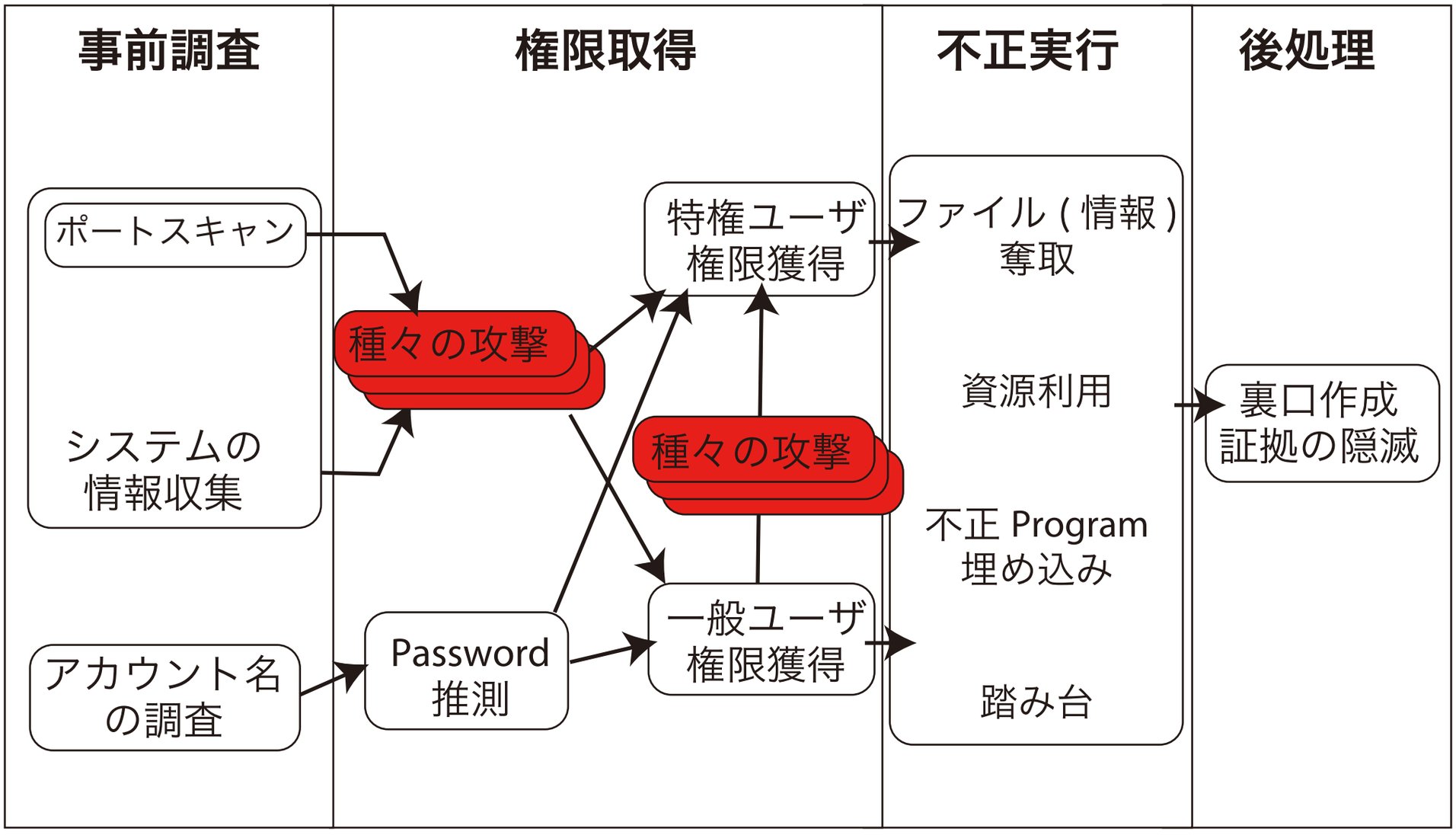
不正実行(2/2)

- 不正プログラムの埋め込み
  - 主な埋め込み先 ⇒ **Webページ**
  - 不正プログラムを利用者に気づかれずにインストール
- コンピュータ不正使用
  - 計算機を不正に使用する.
    - 例) 第三者の計算機を遠隔地から操作
- 踏み台
  - 不正アクセスの中継地点として他人の計算機を不正使用

後処理

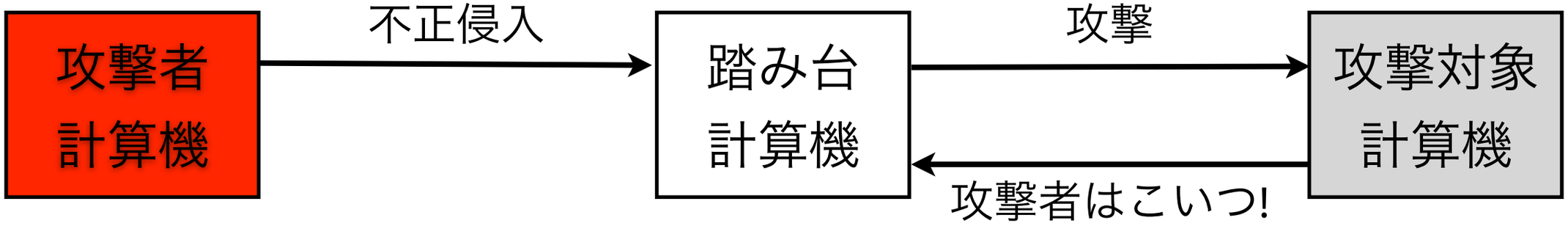
- 証拠隠滅
  - 不正侵入の形跡を消す
    - ログファイルの改ざん、削除
- バックドアの作成
  - 裏口(Back door)の作成
    - 次回以降の不正侵入を容易にする

一般的な不正侵入の流れ



踏み台って?

踏み台とは?



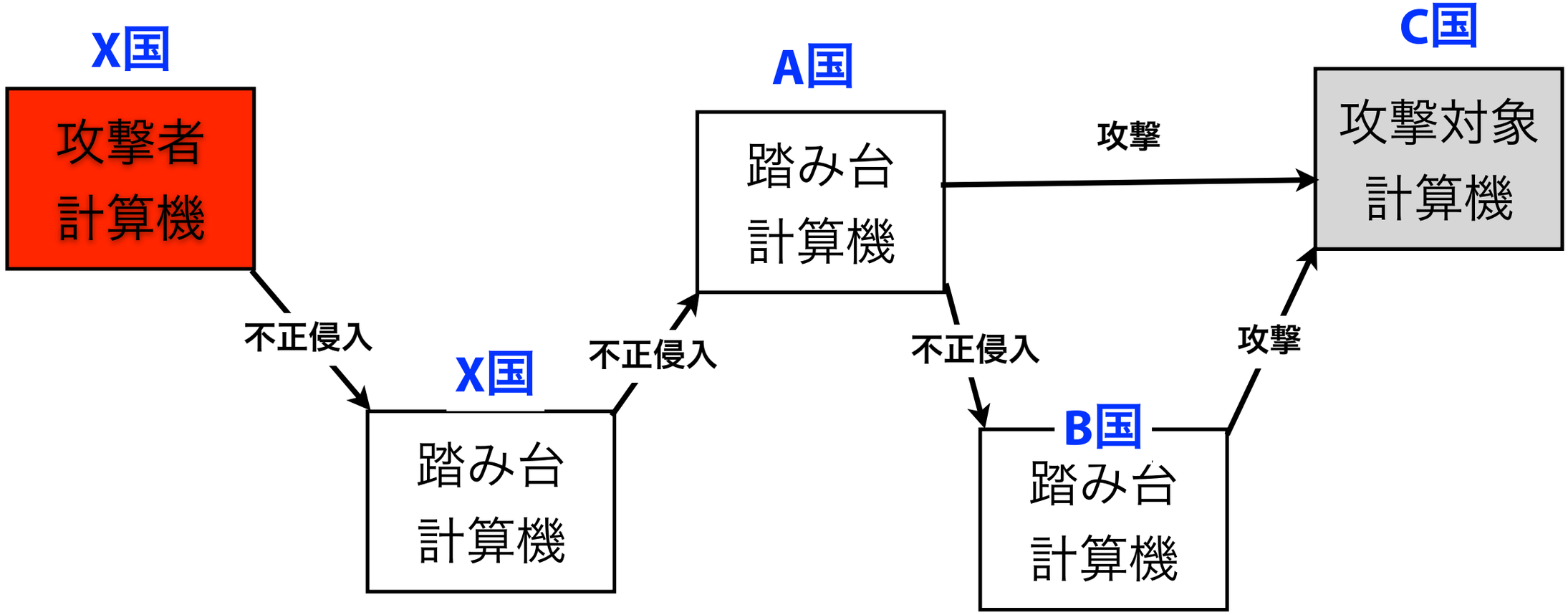
- 次のいずれかに該当する計算機を「**踏み台**」と呼ぶ
  - 攻撃者に攻撃拠点として悪用されている計算機
  - 攻撃者の身元隠蔽のために不正利用される計算機
    - なぜ踏み台を利用？ ⇒ 自分の計算機から直接攻撃すると自身の居場所が特定される恐れがあるため
    - IP address ⇒ 個人の特定は困難だが絞り込みは可能

IP addressからわかること

- DNSの逆引きによる**所属**の特定
- Whoisによる**所属**
- Geo location by IP addr.の存在
  - IP address ⇒ **国名、都市名**
    - Google Mapsなどでも使われている
- ISPの協力による**加入者情報**の提供
  - 捜査機関からの要請、裁判所命令などに限定

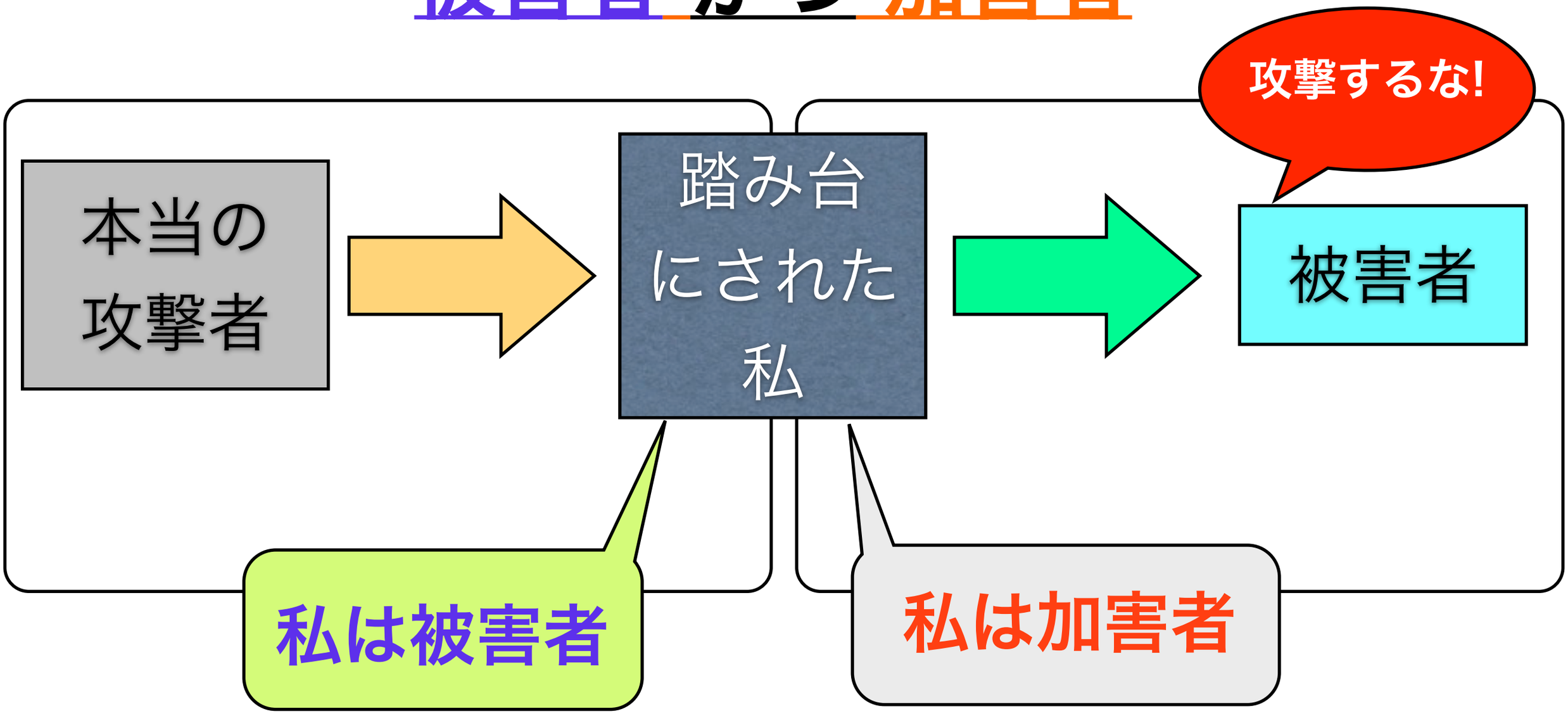
身元隠蔽

- 身元隠蔽を確実にするために
  - 複数の踏み台計算機を経由
  - 海外の計算機を経由



踏み台にされた人は

被害者 かつ 加害者



踏み台 事例

- 踏み台計算機がある所有組織に苦情やクレームがくる
  - 管理責任を問われ損害賠償を求められる可能性もある
    - (2003/08/26), “踏み台”にされた企業に賠償責任? - 高まる訴訟リスクに新対策、鍵はPolicyとForensics, ITPro
      - http://itpro.nikkeibp.co.jp/members/NIT/ITARTICLE/20030825/1/
    - (2003/09/12), セキュリティ法律相談 -- 踏み台, ITPro
      - http://itpro.nikkeibp.co.jp/members/NBY/techsquare/20030911/1/
- クレーム側も攻撃を受けた時、現状の攻撃元が攻撃者の真の居場所とは限らないことを認識する

(Mar, 2009)「踏み台にされないように」、総務省 国民のための情報セキュリティサイト, http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/homepage/server09.htm

英語標記

- Victim computer (犠牲になった計算機)
- Compromised computer (傷つけられた計算機)
- Zombie (操られている という意味から)
- Bot (命令の通り動く という意味から)

Hacker vs. Cracker

- ハッカー (Hacker)
  - コンピュータに対する高い知識を持つ人々を「尊敬する」呼称
- クラッカー (Cracker)
  - 技術を悪用し、ICT技術を利用して悪事を働く人たちの呼称

The Dark side: Hackers versus Crackers,
http://www.cs.utah.edu/~elb/folklore/afs-paper/node9.html

“White hat” vs. “Black hat”

- White hat
  - Security改善のために(合法的な理由で)
    hackingをする者 (=保安官)

- Black hat
  - 悪事を目的としてhackingをする者
    (=ならず者、犯罪者)

反撃(報復)

- 不正アクセス/不正侵入に対する報復論あり ⇒ ダメ
  - 理由
    - 踏み台問題：攻撃元が真の攻撃者とは限らない
    - 報復行為自体が攻撃行為：反撃と不正アクセスの区別は不能
- そういう技術を開発しようとした企業もあった
  - (2004/03/11), Cnet Japan, 「目には目を」は許されるか - 新たなSecurity製品に議論沸騰, http://japan.cnet.com/news/ent/20064816/
  - (2004/03/11), Could watch, 「逆襲型セキュリティソフト、ベンチャーが開発」,http://cloud.watch.impress.co.jp/epw/cda/foreign/2004/03/11/1634.html

Cyber Warfare

- サイバー戦争
  - サイエンス・フィクション ⇒ 現実へ
    - 諜報・煽動活動、破壊活動、民主化運動
    - 軍の専任部隊の存在 (米、中、北朝鮮他...)
- Hactivism (ハクティビズム)
  - 社会的、政治的活動の手段としてCracking
  - サイバーテロ