CyberDefense

医療機関に見られるクローズネットワークへのサイバー攻撃の手口

2016年5月

サイバーディフェンス研究所
名和 利男

目 次

1. 激変するサイバー攻撃メカニズム

2. 攻撃側が（防御側に対して）圧倒的な優位性を得る
   背景・理由

3. クローズドネットワークからの情報窃取を可能にする
   攻撃シーケンス

4. 組織が取り組まなければならないこと

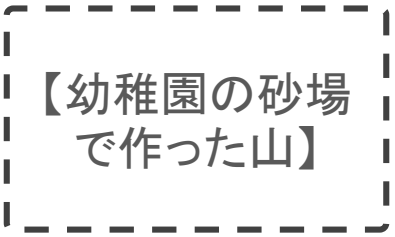
トピック 1

激変するサイバー攻撃メカニズム

激変するサイバー攻撃メカニズム

- 攻撃側と防御側の関係位置の変化

攻撃側



防御側

（著作権の都合上、写真等は削除）

激変するサイバー攻撃メカニズム

- 日本へのサイバー攻撃で利用される「日本特有の仕組み」

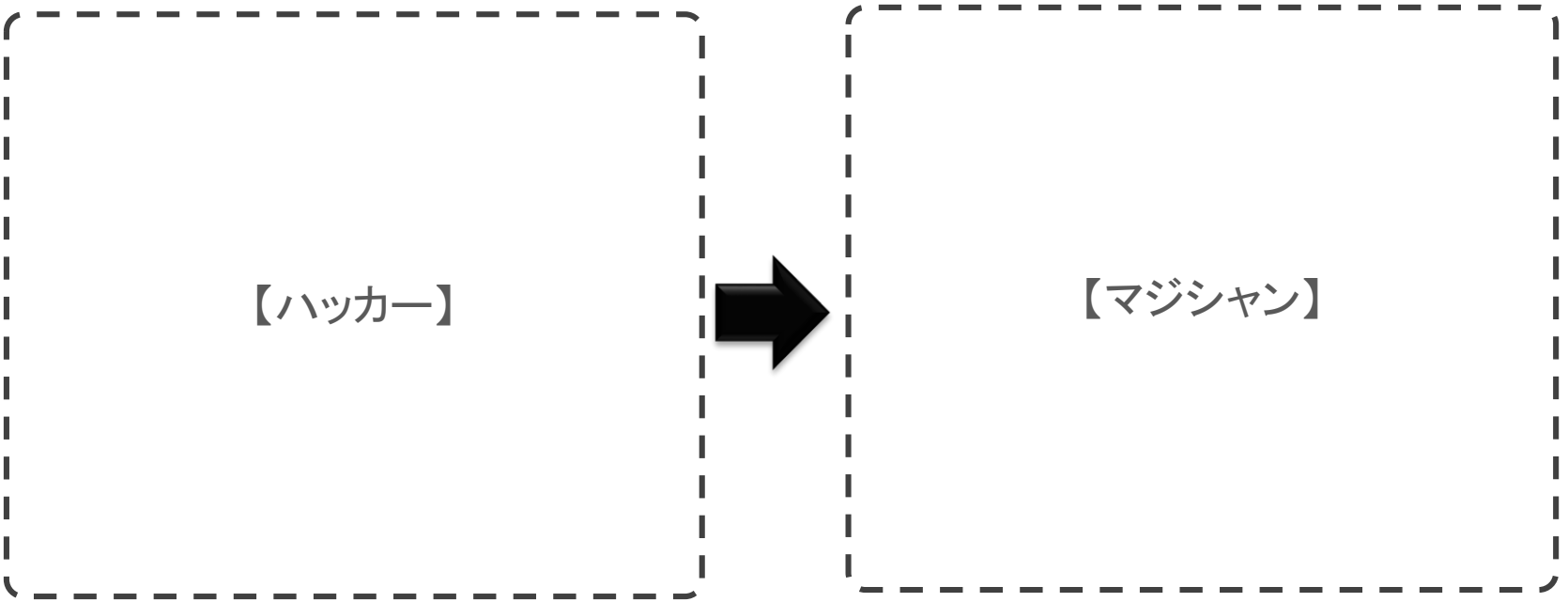
諸外国における
組織内ネットワークシステムの仕組み

日本における
組織内ネットワークシステムの仕組み

（著作権の都合上、写真等は削除）

激変するサイバー攻撃メカニズム

- 既成概念を覆す斬新な発想に基づく攻撃手法



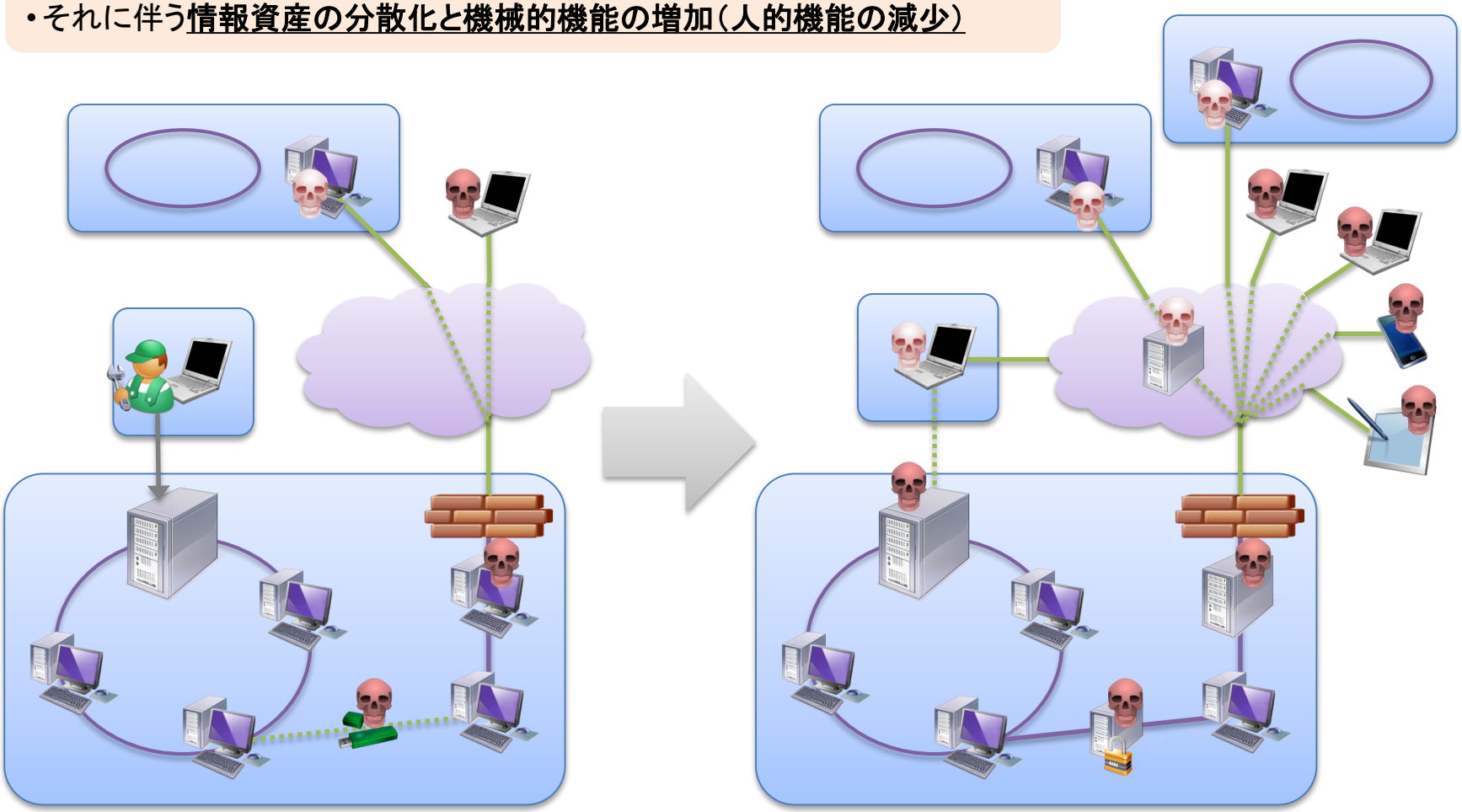
（著作権の都合上、写真等は削除）

トピック 2

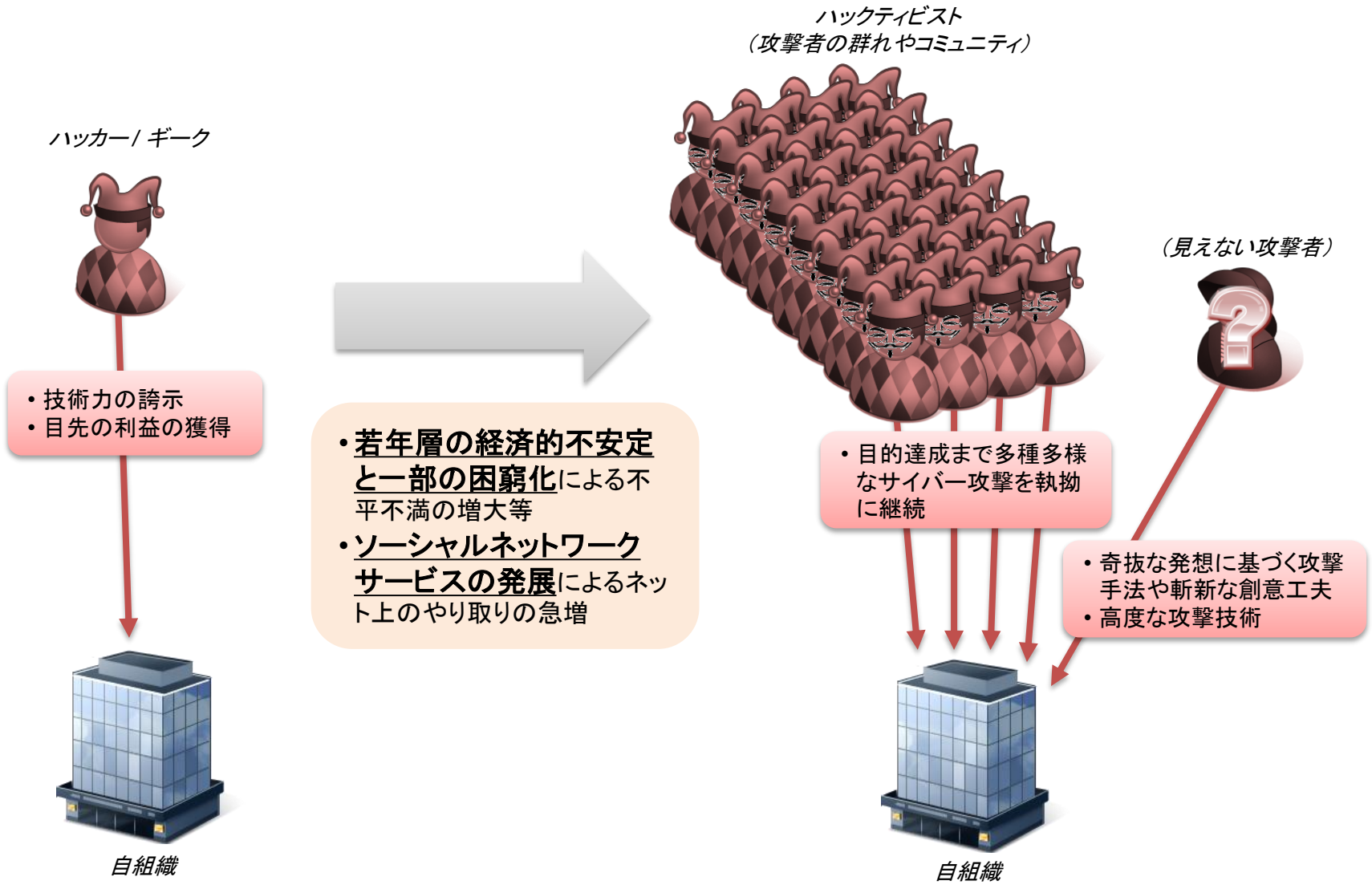
攻撃側が（防御側に対して）圧倒的な優位性を得る背景・理由

情報の分散化と流通の活性化
（業務効率化と迅速化のためのシステム導入 等）

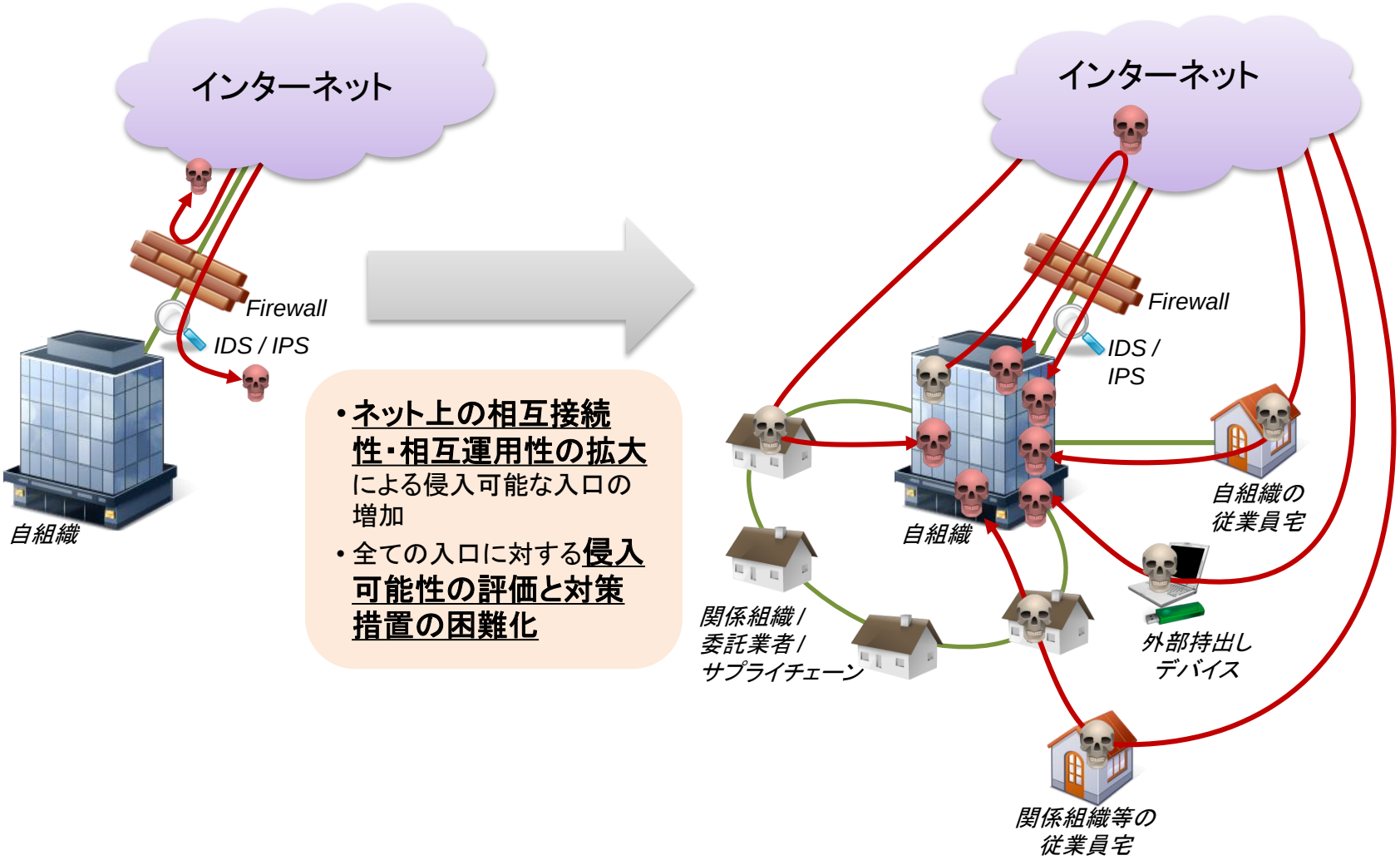
- 他組織と連携業務（サプライチェーンを含む）の**効率化と意思決定の迅速化**のための急激なネットワーク化
- それに伴う**情報資産の分散化と機械的機能の増加（人的機能の減少）**



攻撃側の状況変化
（若年層の困窮化と不正な経済的利得 等）

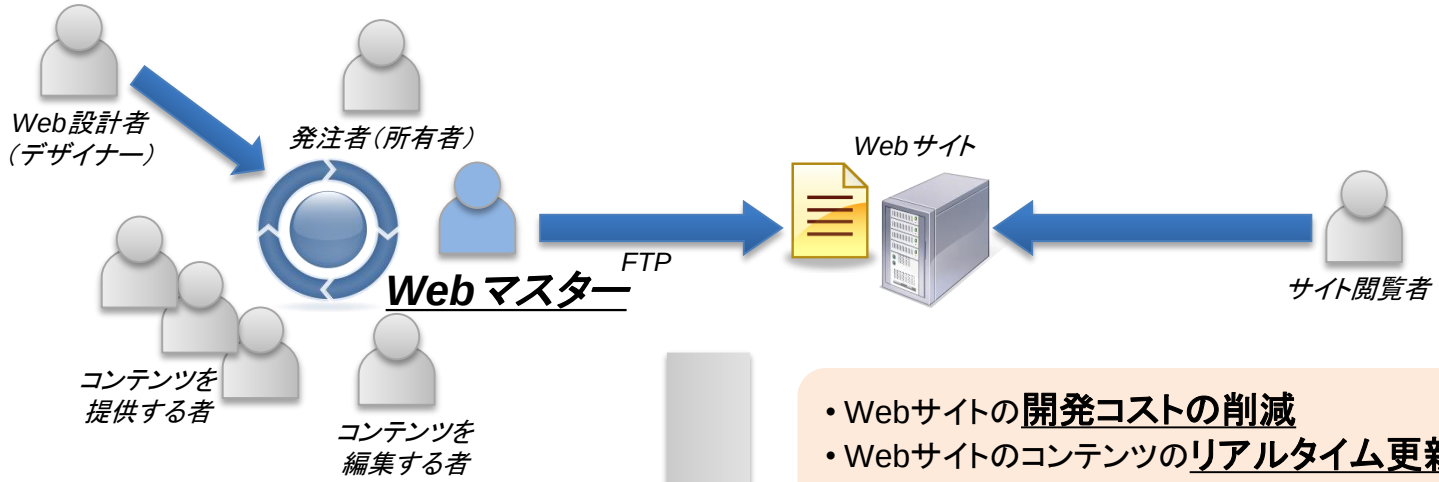


侵入可能な入口の増加
（ネット上の相互接続性と相互運用性の拡大 等）

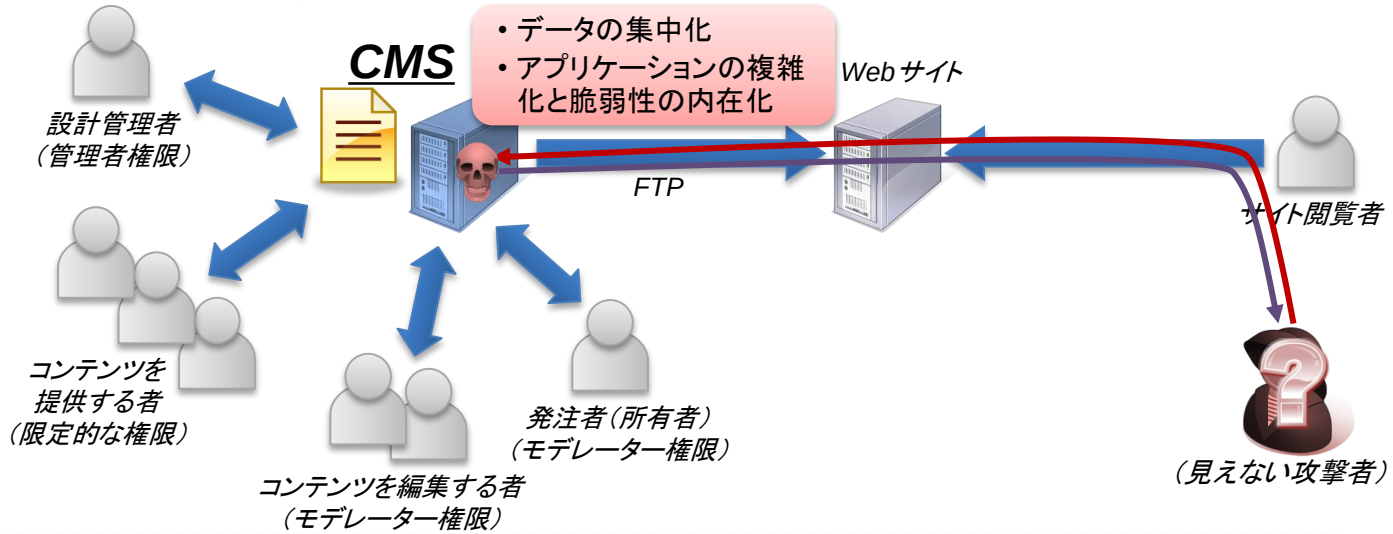


- **ネット上の相互接続性・相互運用性の拡大**による侵入可能な入口の増加
- 全ての入口に対する**侵入可能性の評価と対策措置の困難化**

価値あるデータの集中化
（高度で複雑なシステムへの高依存 等）



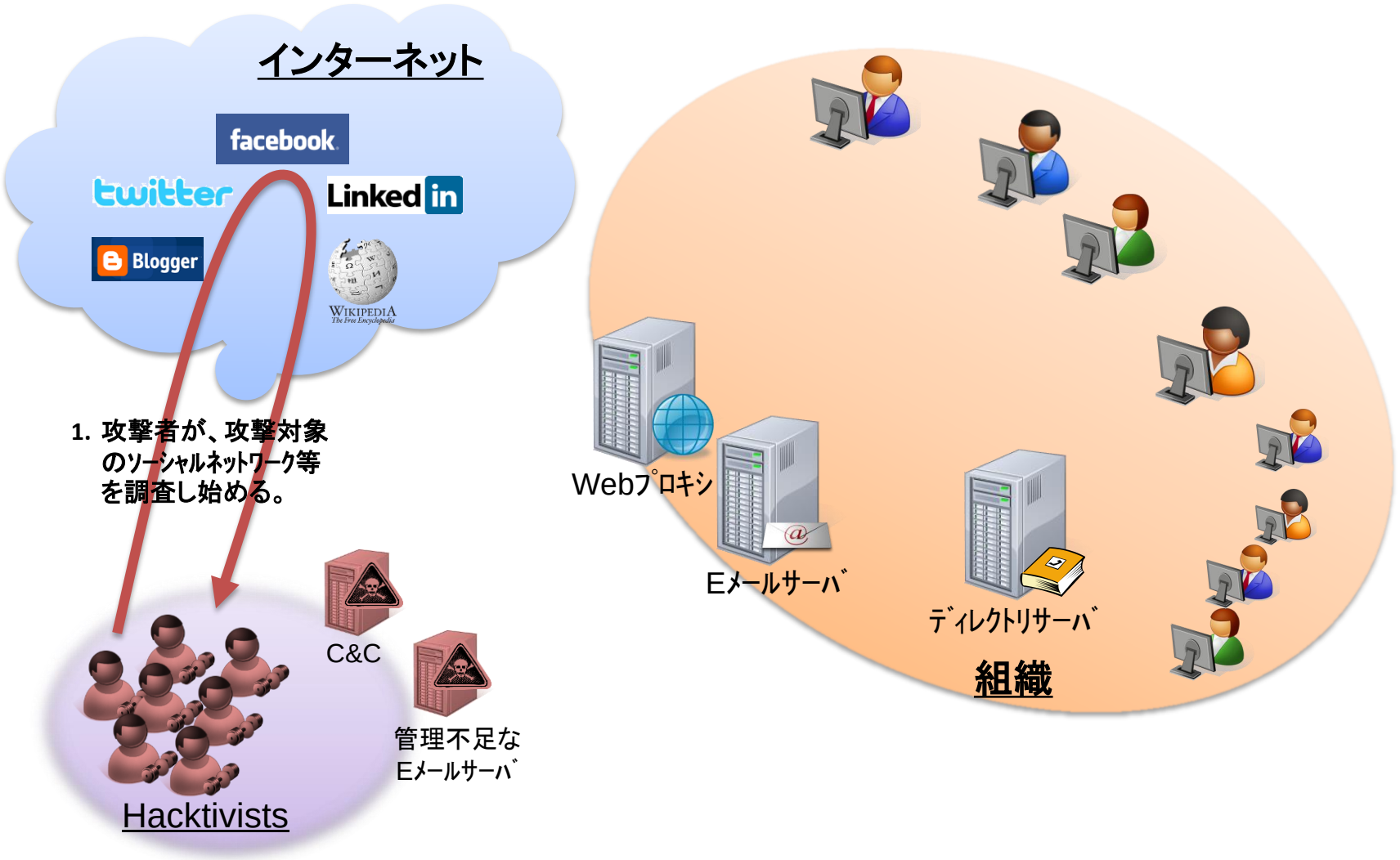
- Webサイトの**開発コストの削減**
- Webサイトのコンテンツの**リアルタイム更新の要請**
- Webサイト（システム）への**アクセスコントロールの必要**



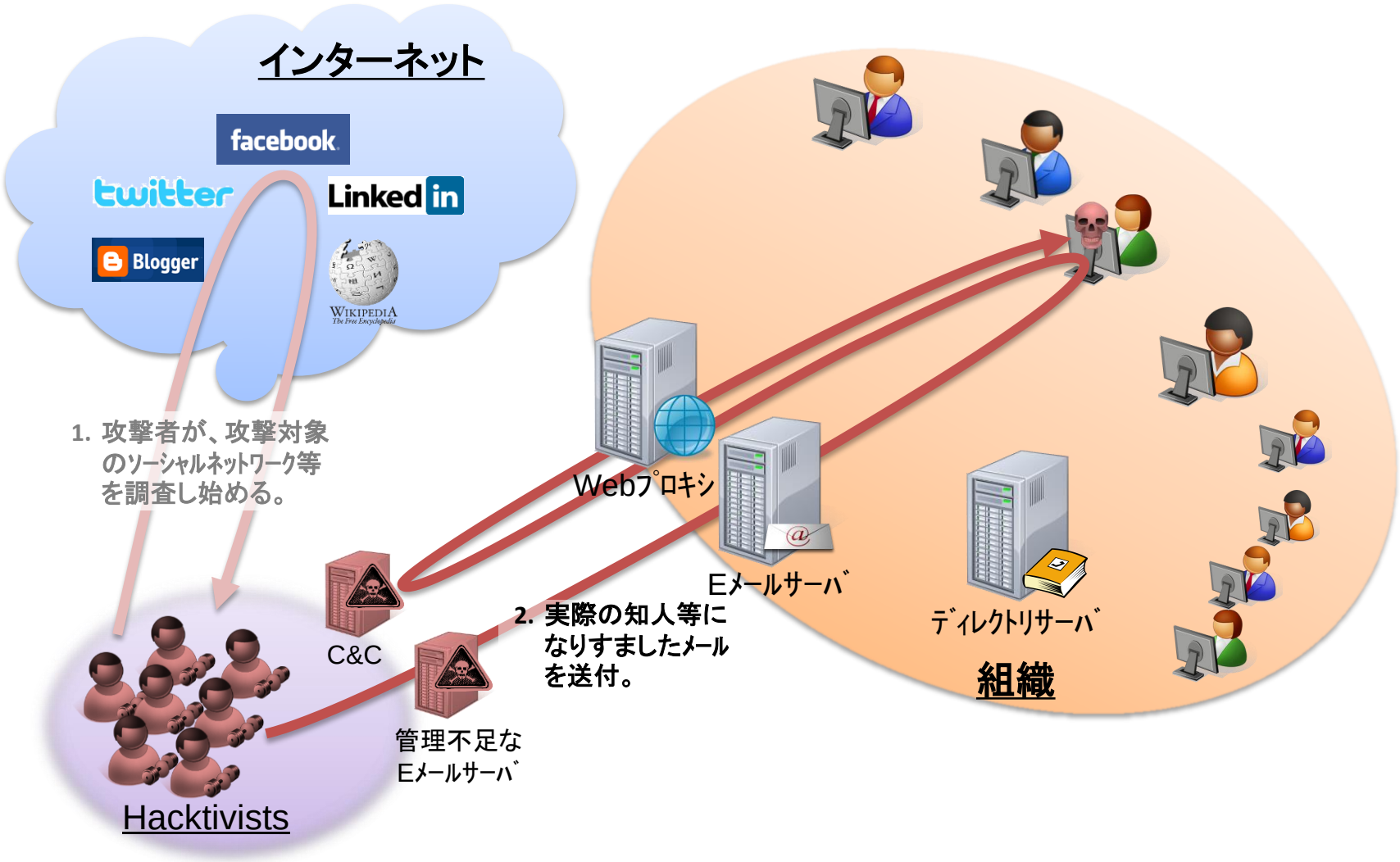
トピック 3

クローズドネットワークからの情報窃取を可能にする攻撃シーケンス

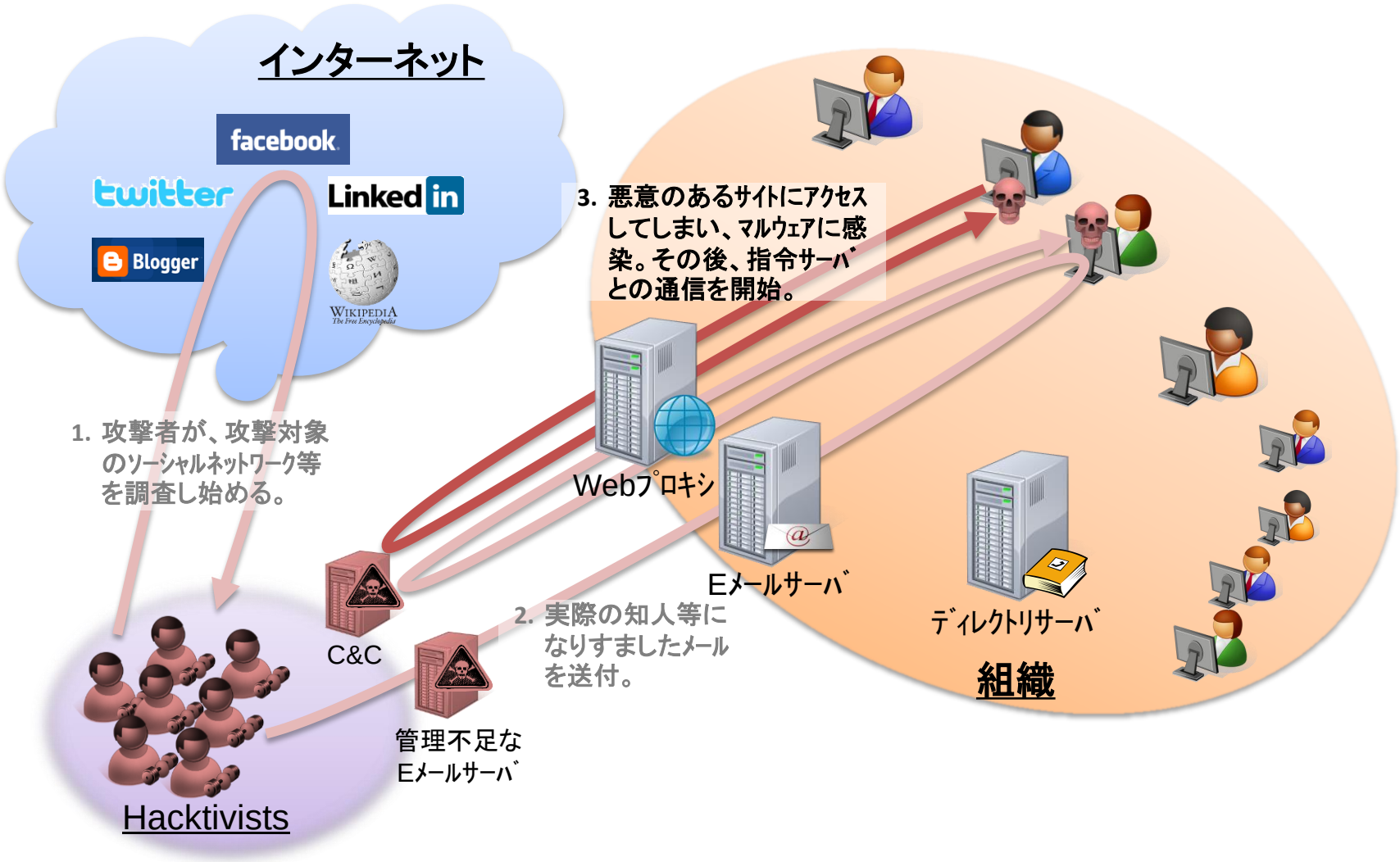
クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



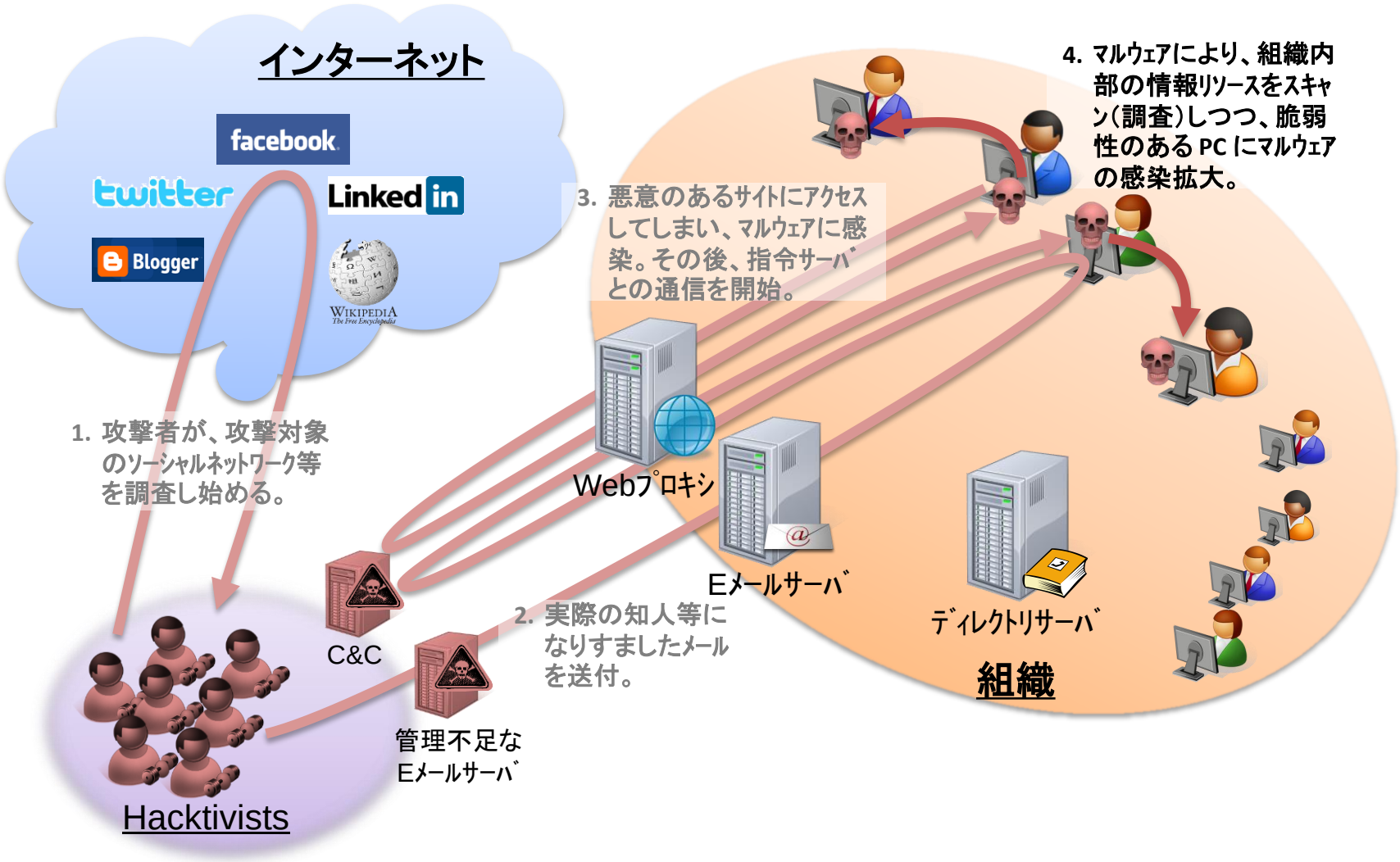
クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



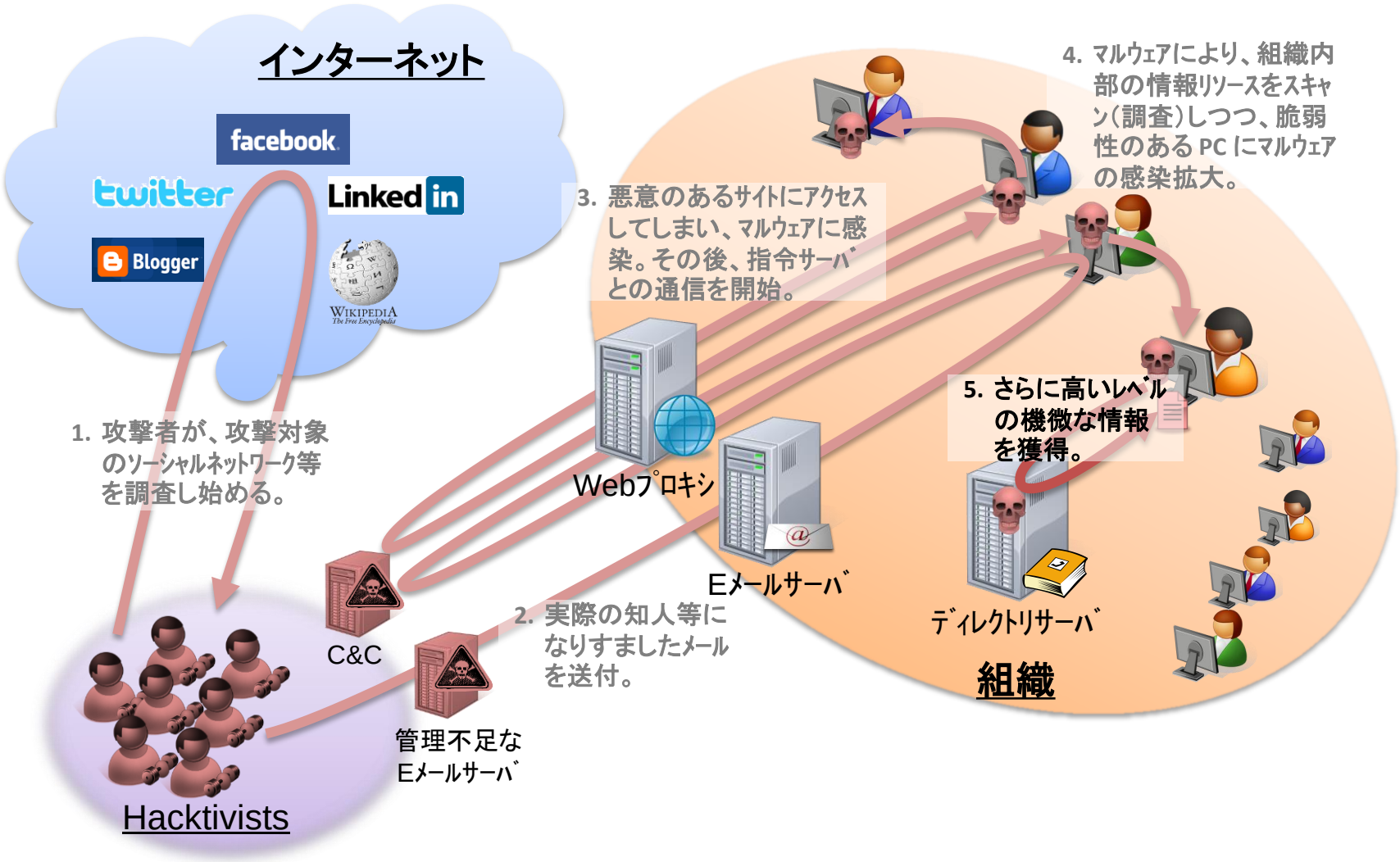
クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



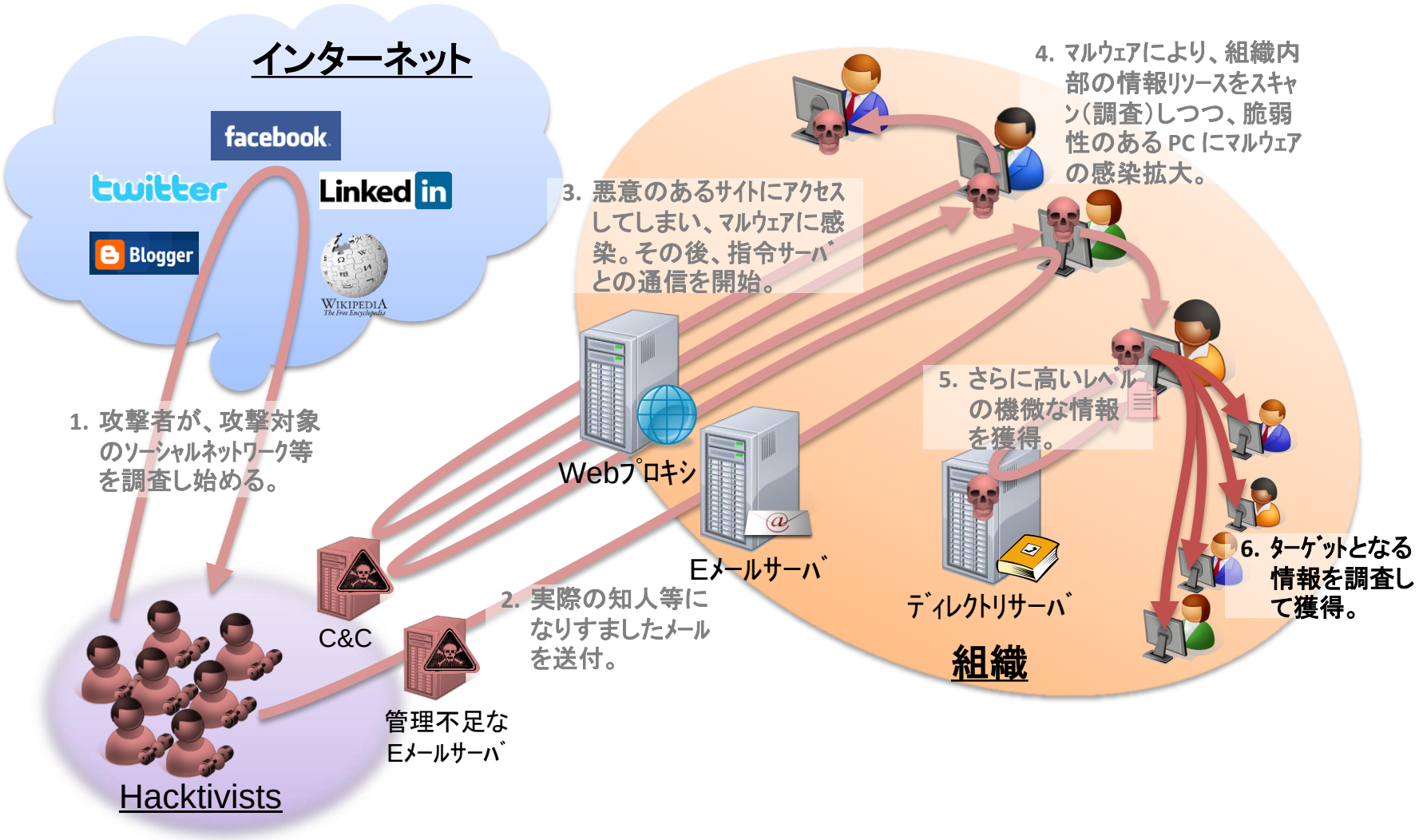
クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



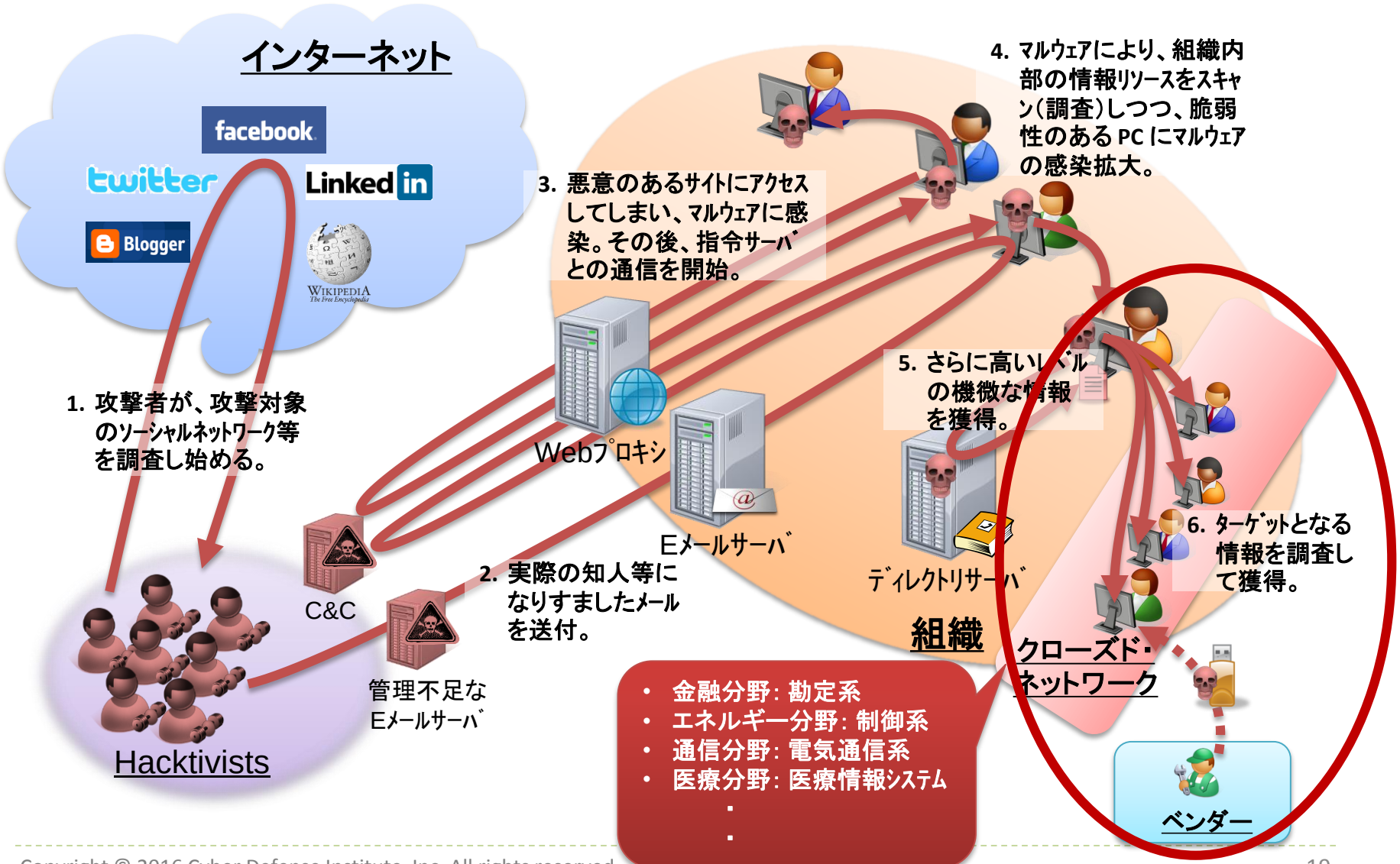
クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



クローズドネットワークからの情報窃取を可能にする攻撃シーケンス



クローズドネットワークからの情報窃取を可能にする攻撃シーケンス

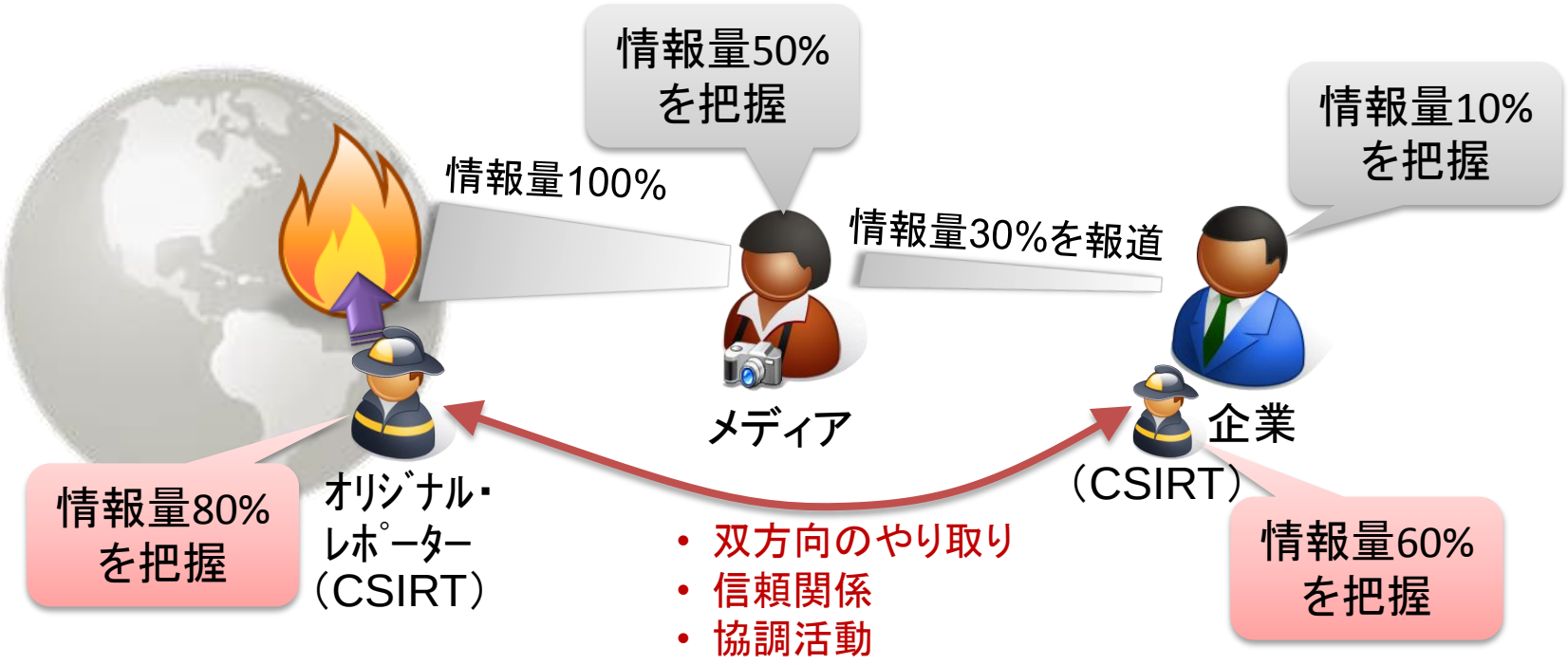


トピック4

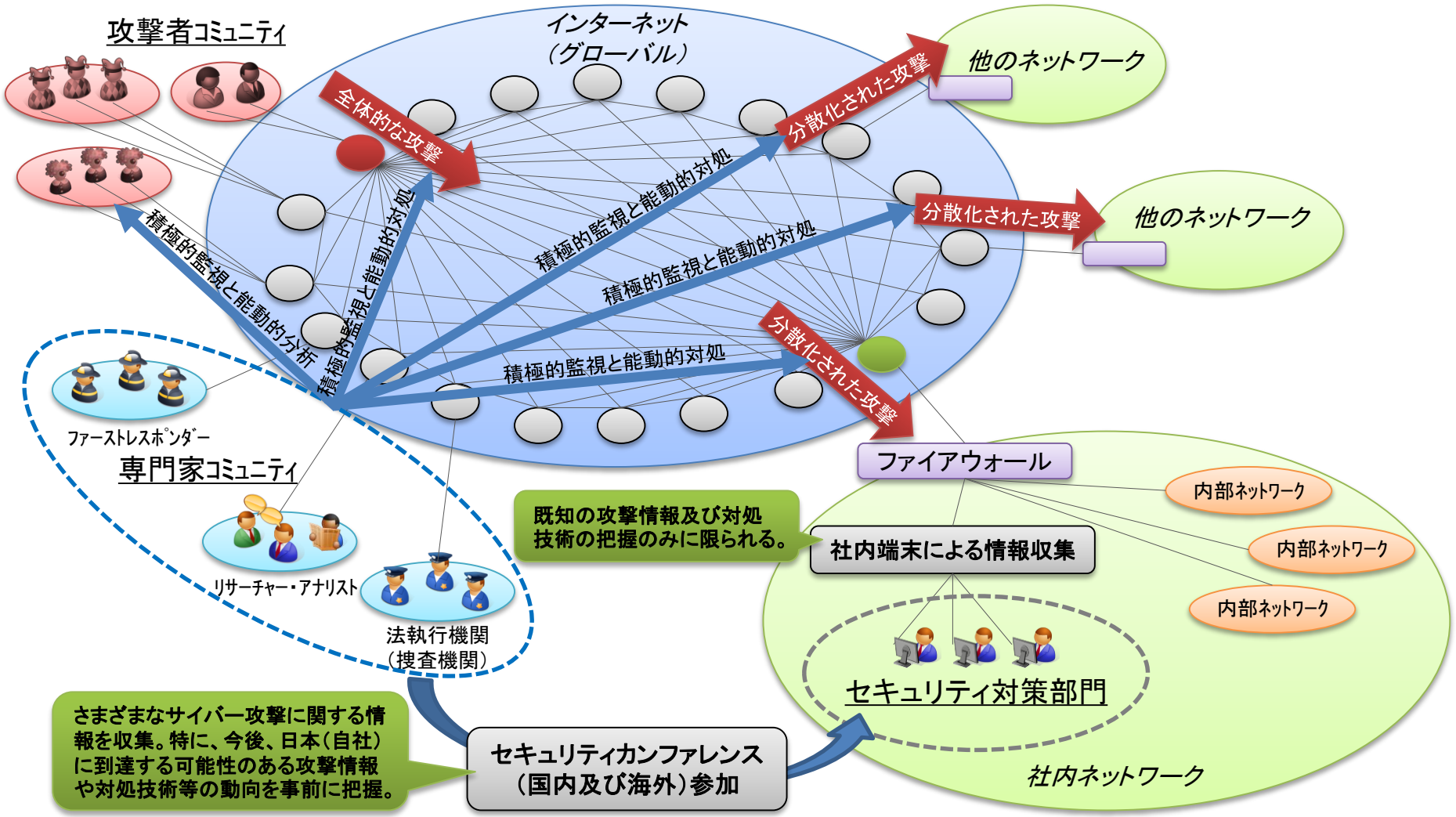
組織が取り組まなければならないこと

サイバー空間における脅威を適切に把握すること

- 一般メディア等が発信する情報を鵜呑みにしてはいけない。
- オジリナル・レポーター（Original Reporter）が発信する情報を追求する。

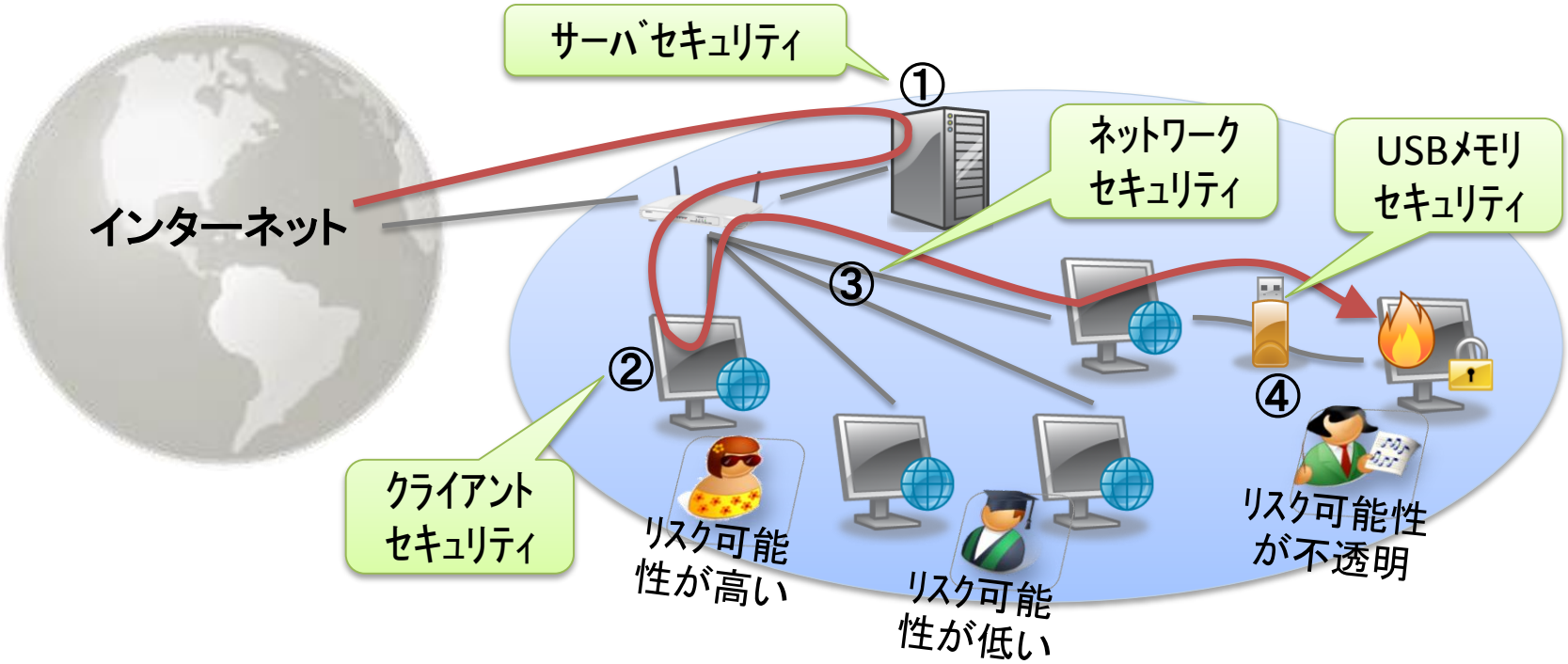


サイバー空間における動向情報を積極的に収集すること



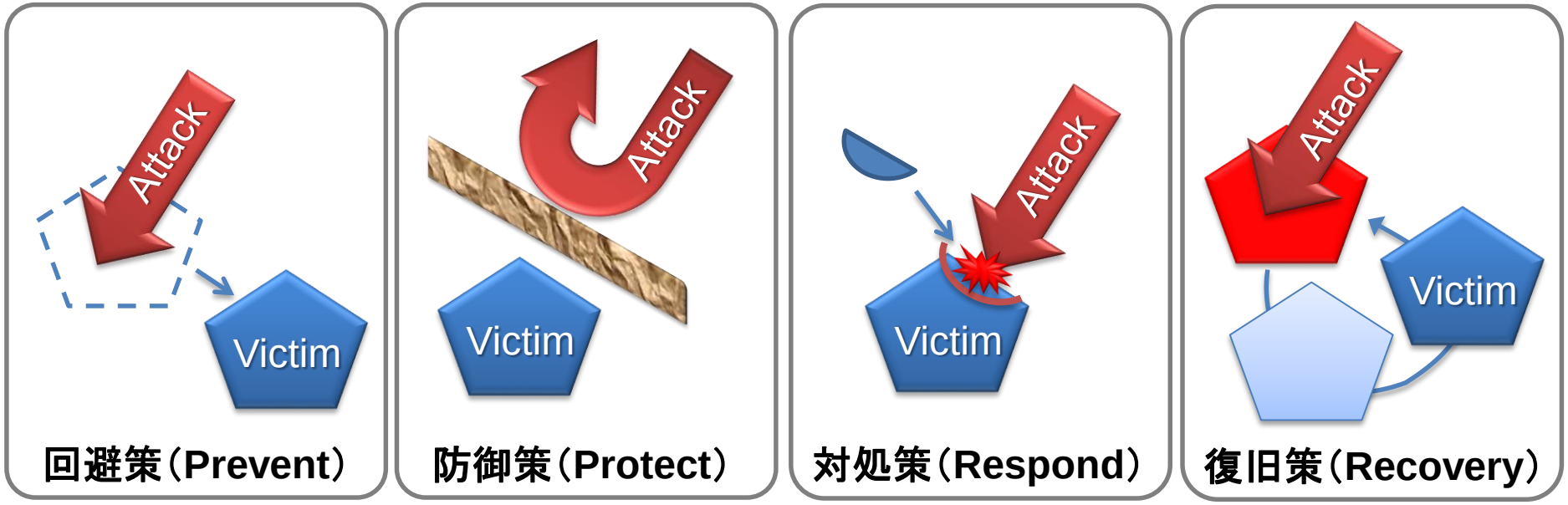
攻撃経路を見出した上で、適切なセキュリティ対策をすること

- ある程度の攻撃の仕組みを理解すること
  - サイバー攻撃を「静的な絵」として理解するのではなく、組織全般に渡る＆時間の流れのある「動的ストーリー」として理解することが必要
  - 主要な（攻撃）経路ポイントにおけるセキュリティ対策の要否及びレベルの設定には、業務慣習や部署風土も考慮することが必要



すべてのサイバー攻撃対処に明確な目的を設定すること

- サイバー脅威に対して、メリハリのついた対策を検討し、実装及び確実な運用をすること。
  - 日本国内の対策は、「防御策（Protect）に偏重」しているため、いたずらにコストがかかってしまう状況が見られる。
  - 最近のサイバー防衛策におけるベストプラクティス（最善策）は、対処策（Respond）である。（最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。）
  - 基本的な対策コンセプトは、次の4つのとおり。



本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
専務理事／上級分析官

Email: nawa@cyberdefense.jp
SNS: about.nawa.to
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp