2020年の大事な時期に認識しておくべき サイバー空間の変化

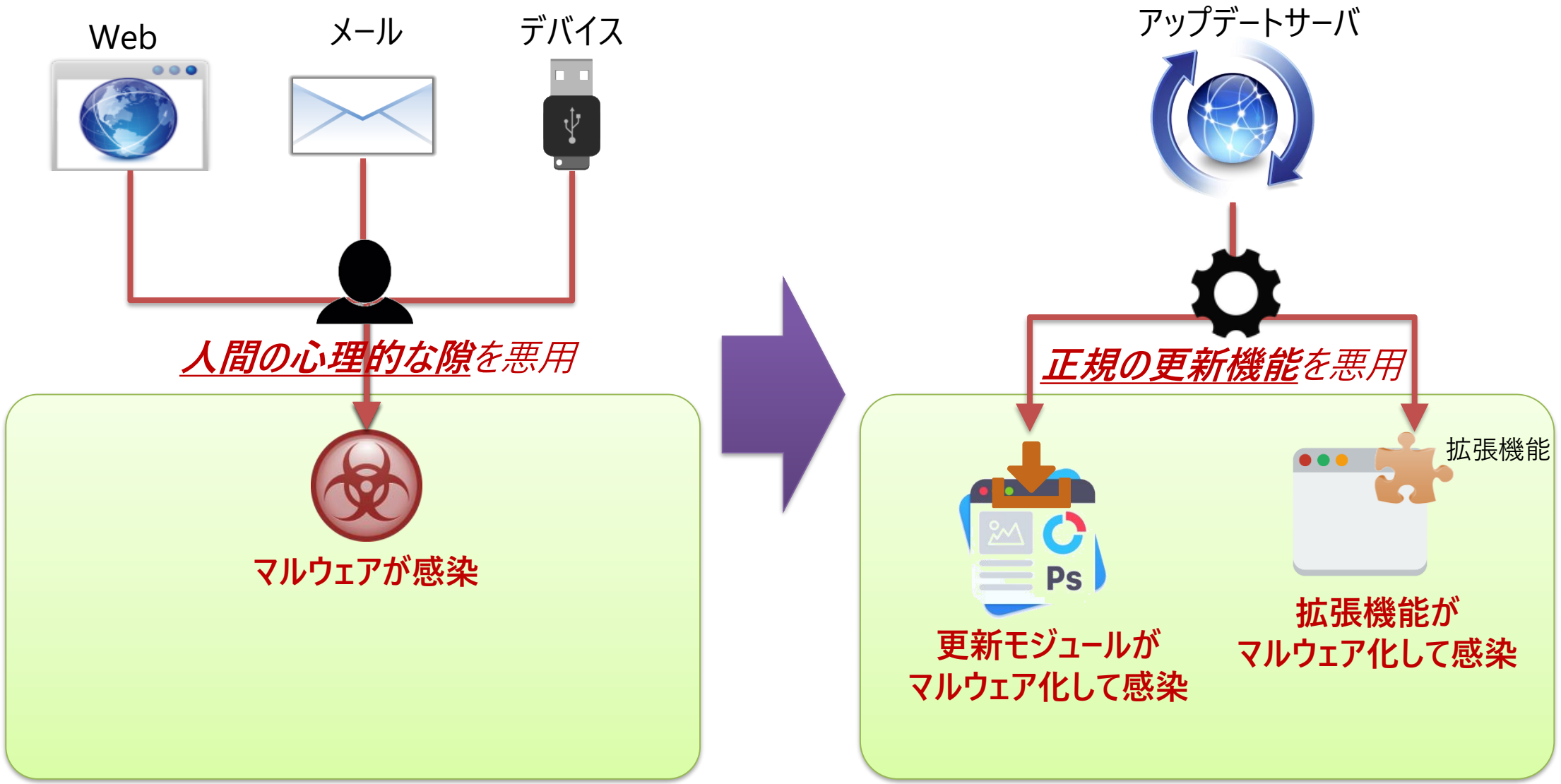
2020年 2月

名和 利男

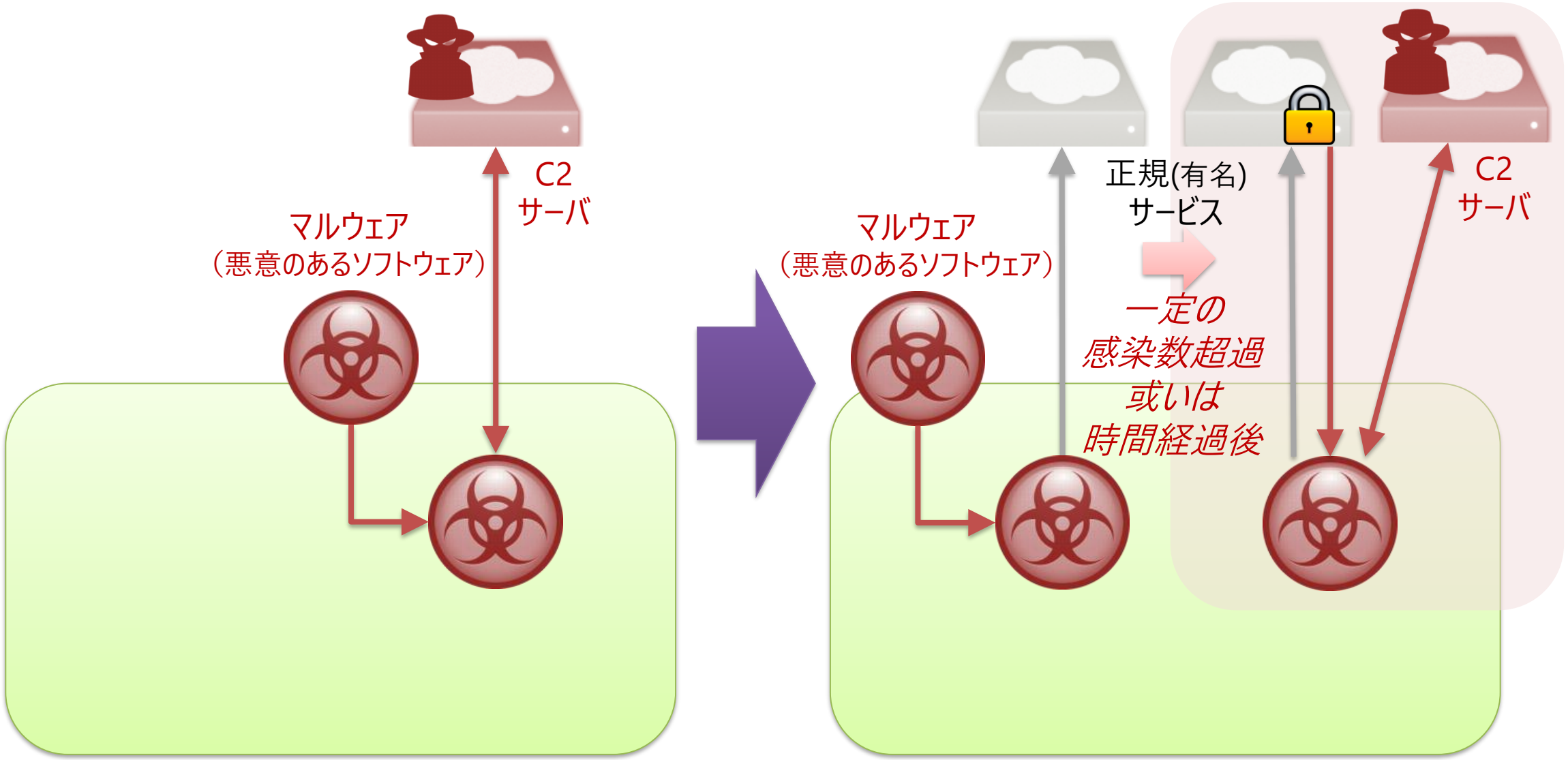
トピック１

直近数年で**大きく変化したサイバー攻撃**

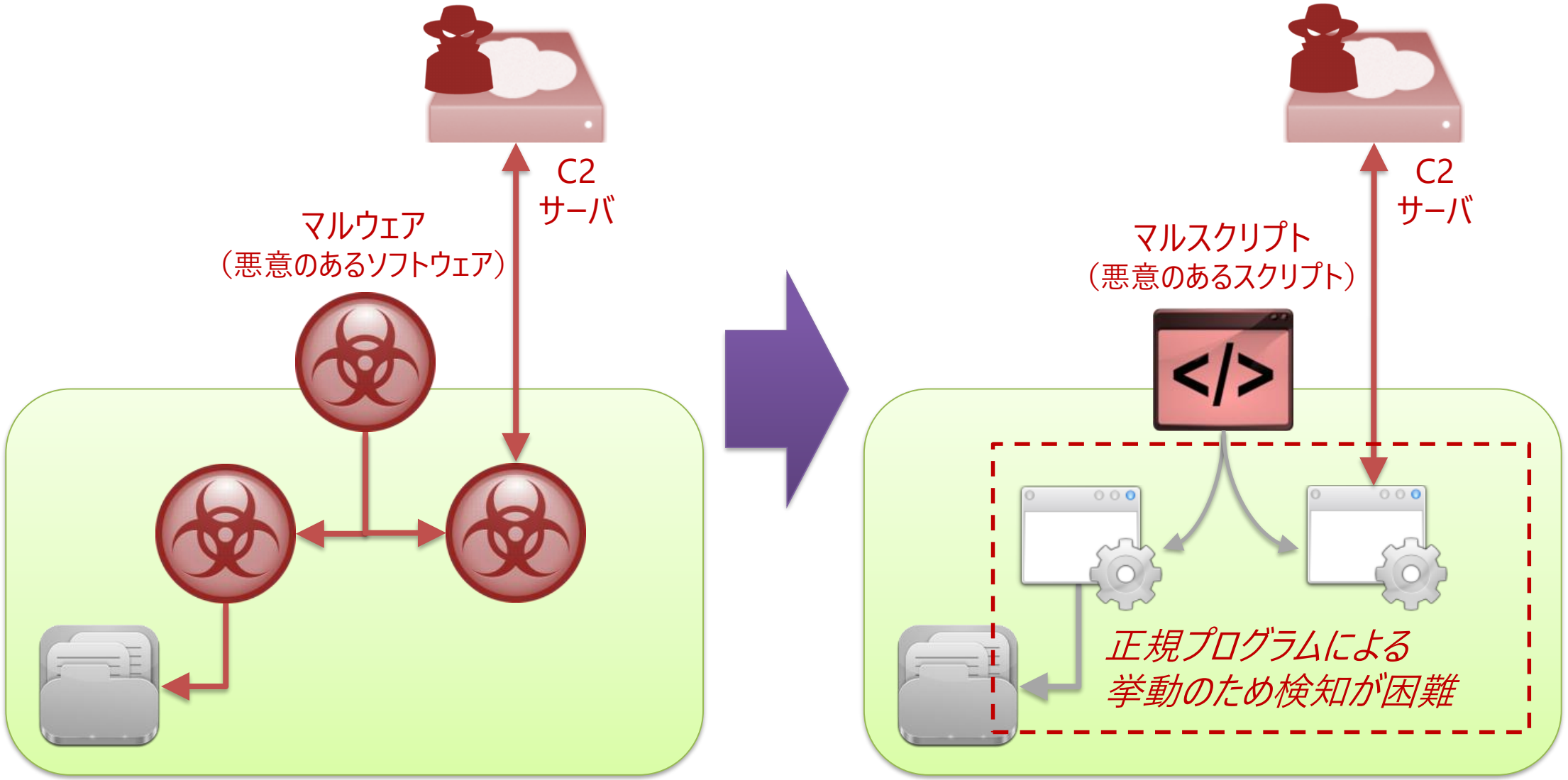
正規の更新機能を利用するマルウェア感染



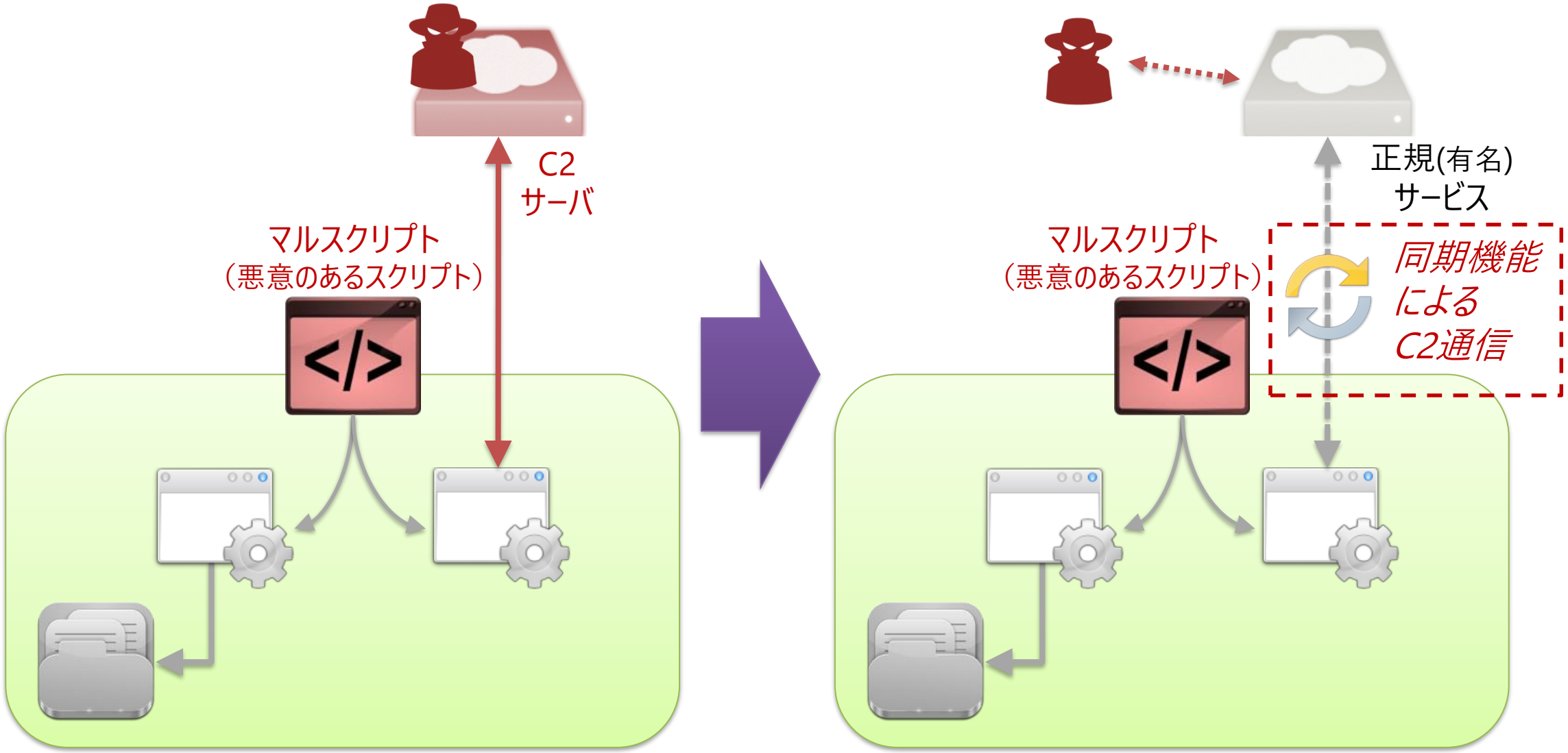
正規(有名)サービスを(時間差で)踏み台にするC2通信



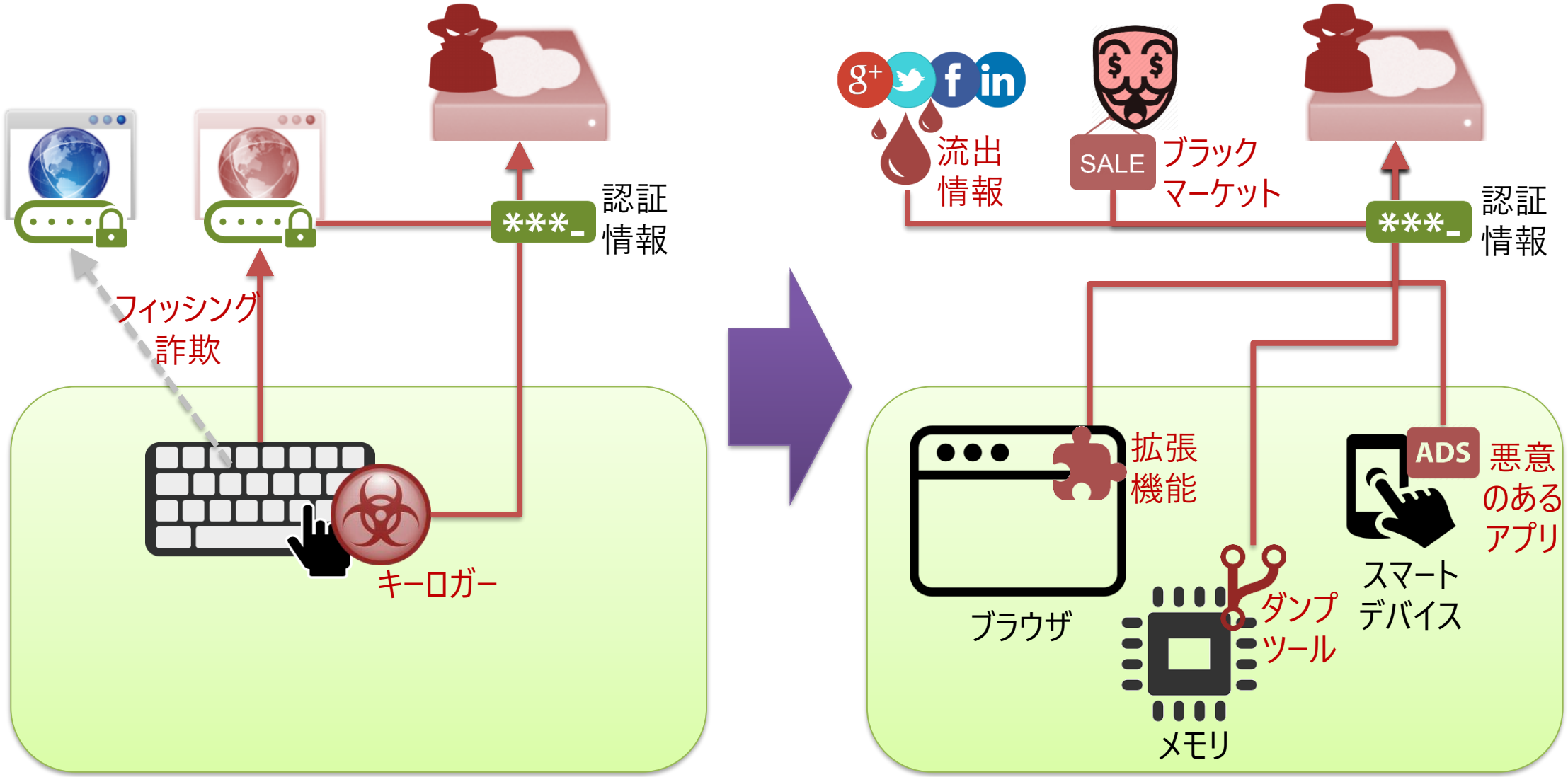
スクリプト実行環境を利用した正規プログラムによる挙動



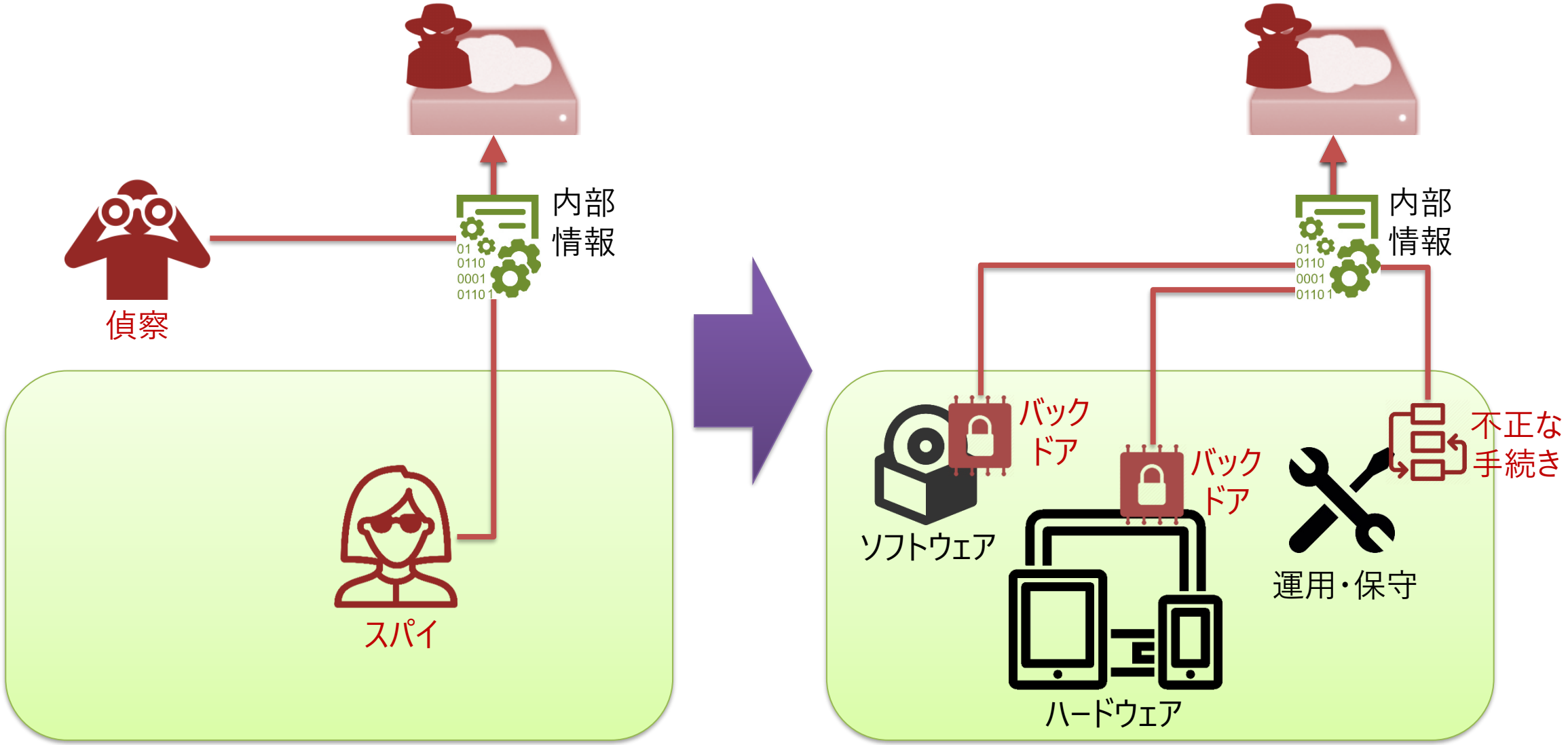
正規(有名)サービスの同期機能を利用するC2通信



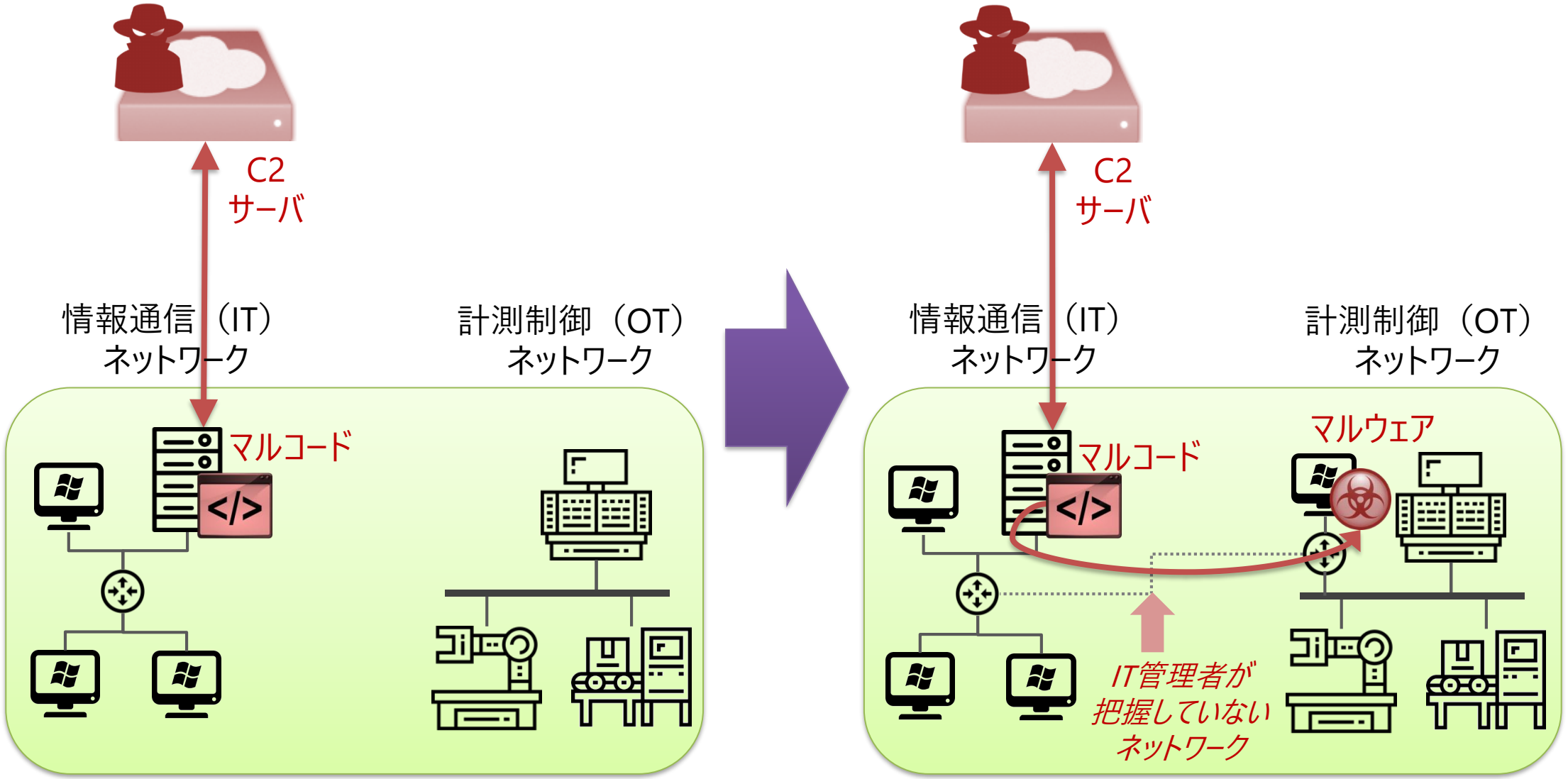
様々な対象から**調達・窃取した認証情報**の悪用



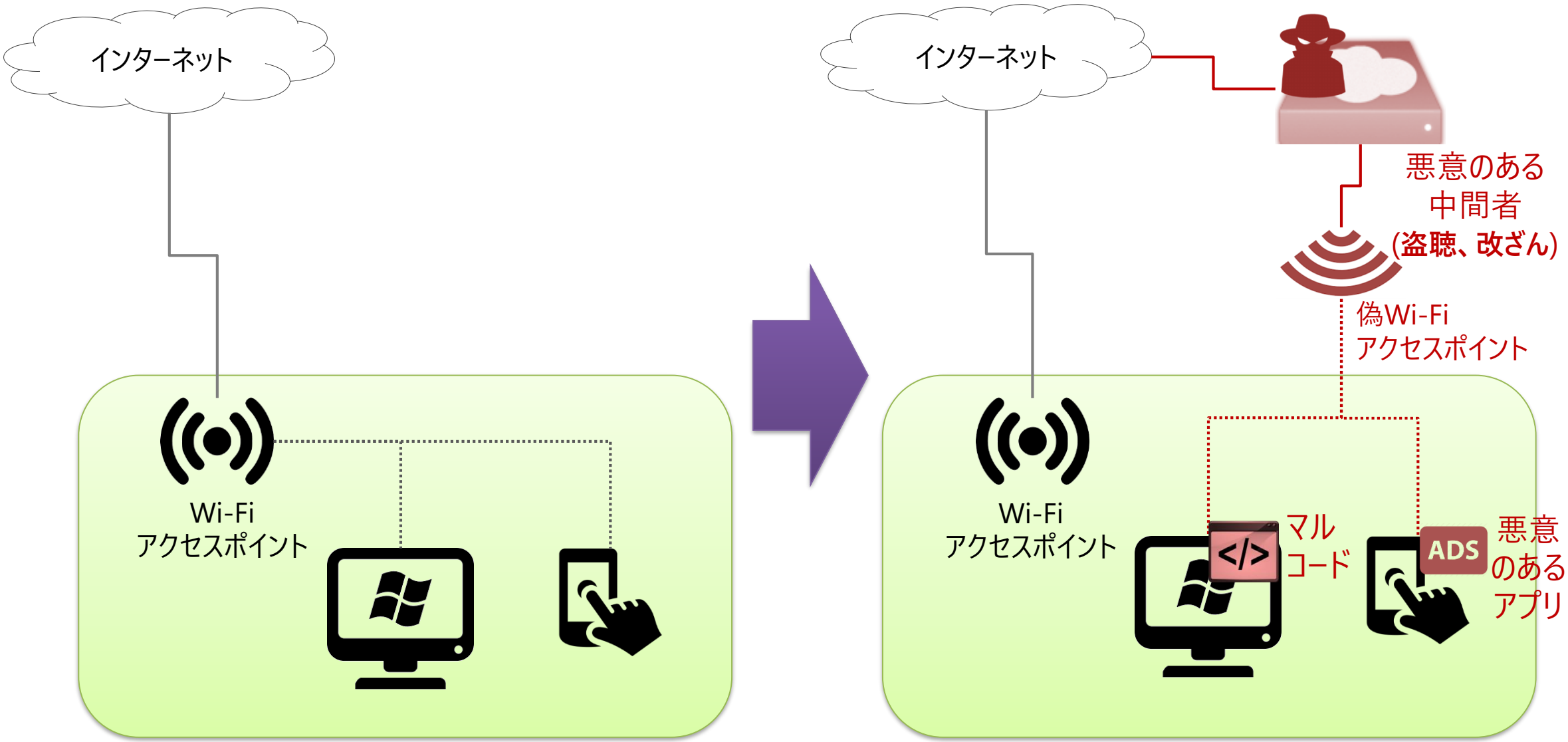
敵対国のソフトウェアやプロダクトからのデータ流出



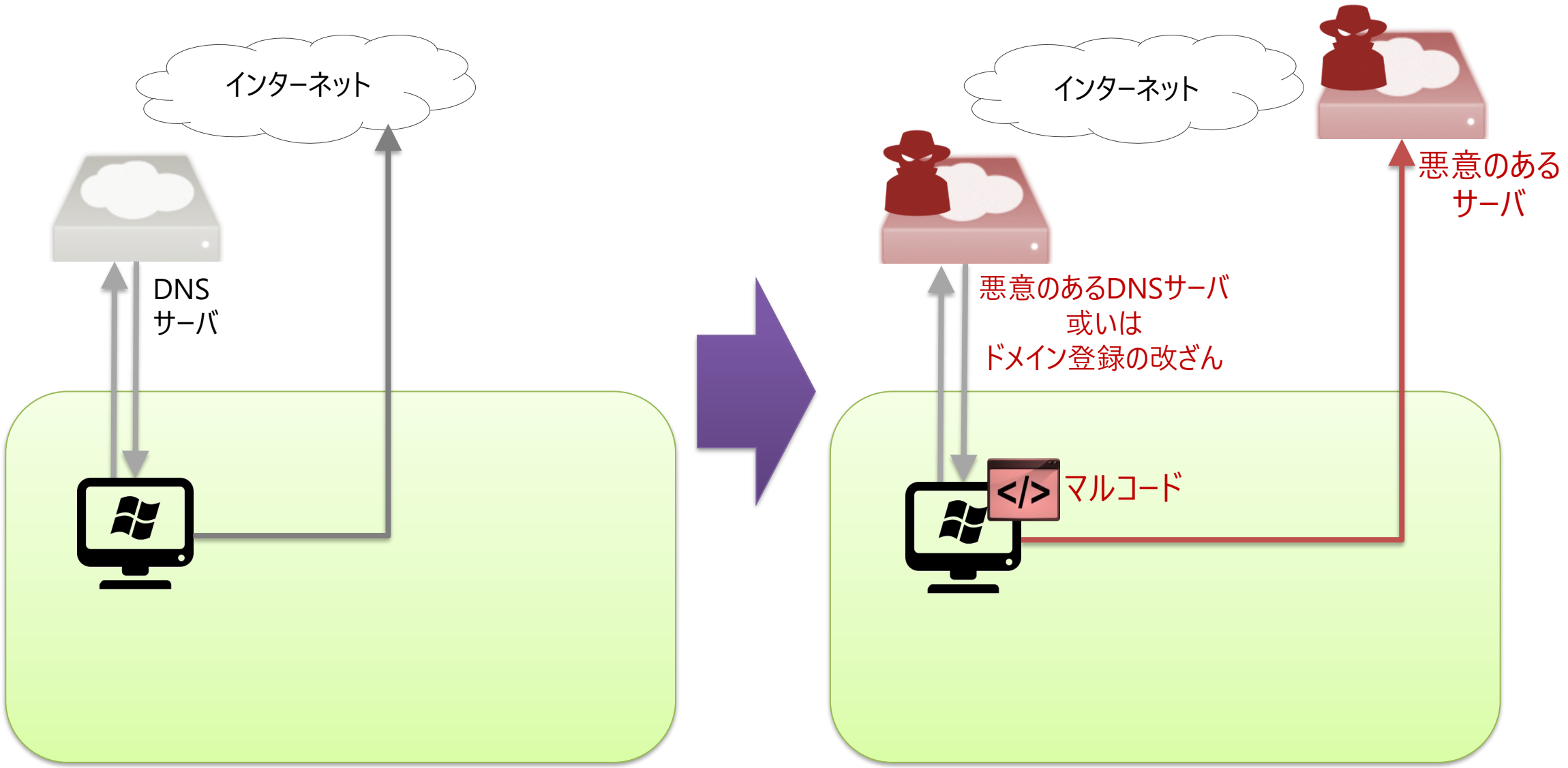
機械設備のPCに対するマルウェア感染



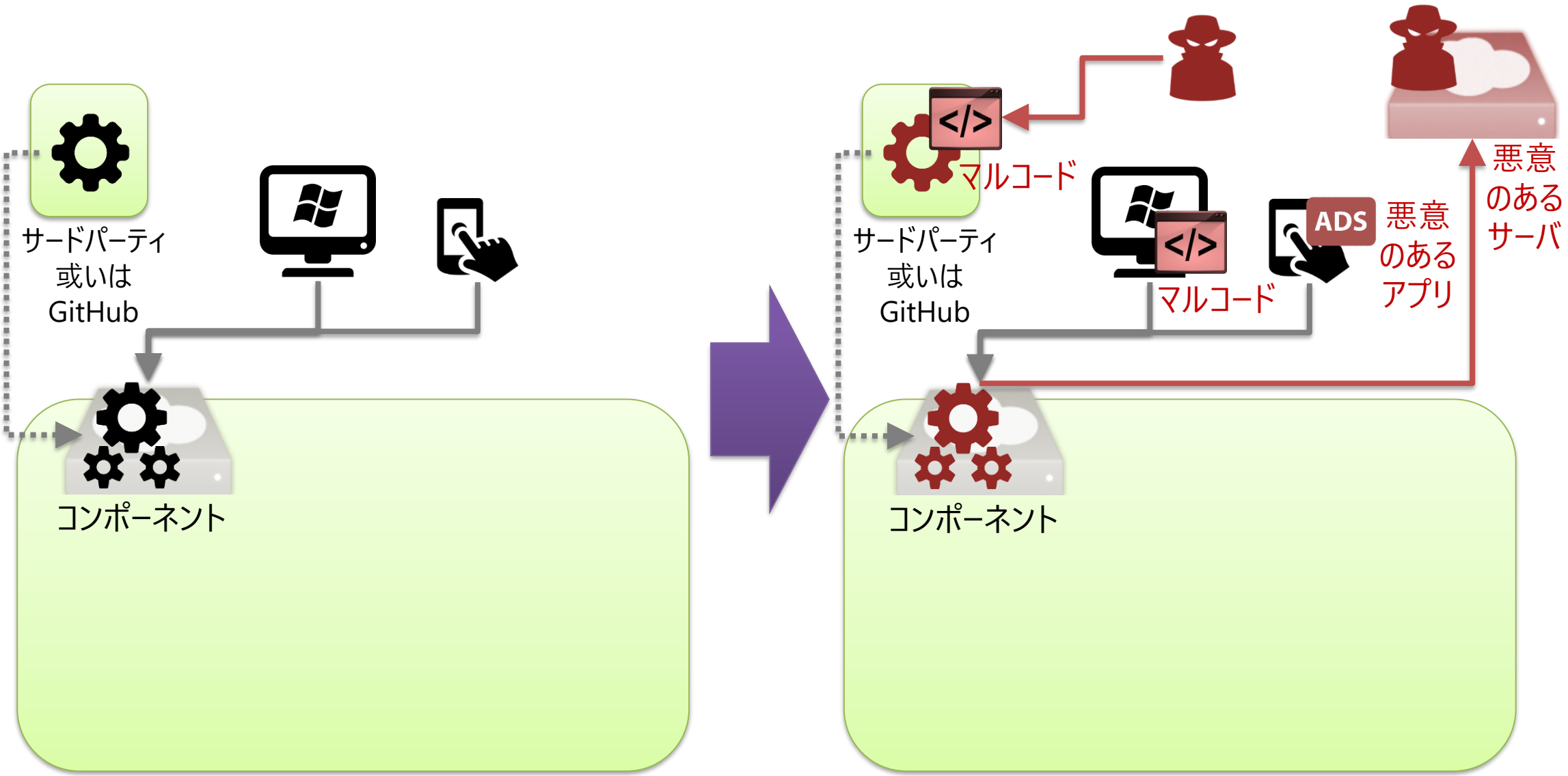
偽Wi-Fiアクセスポイントによる中間者攻撃



悪意のあるDNSサーバによるC2通信



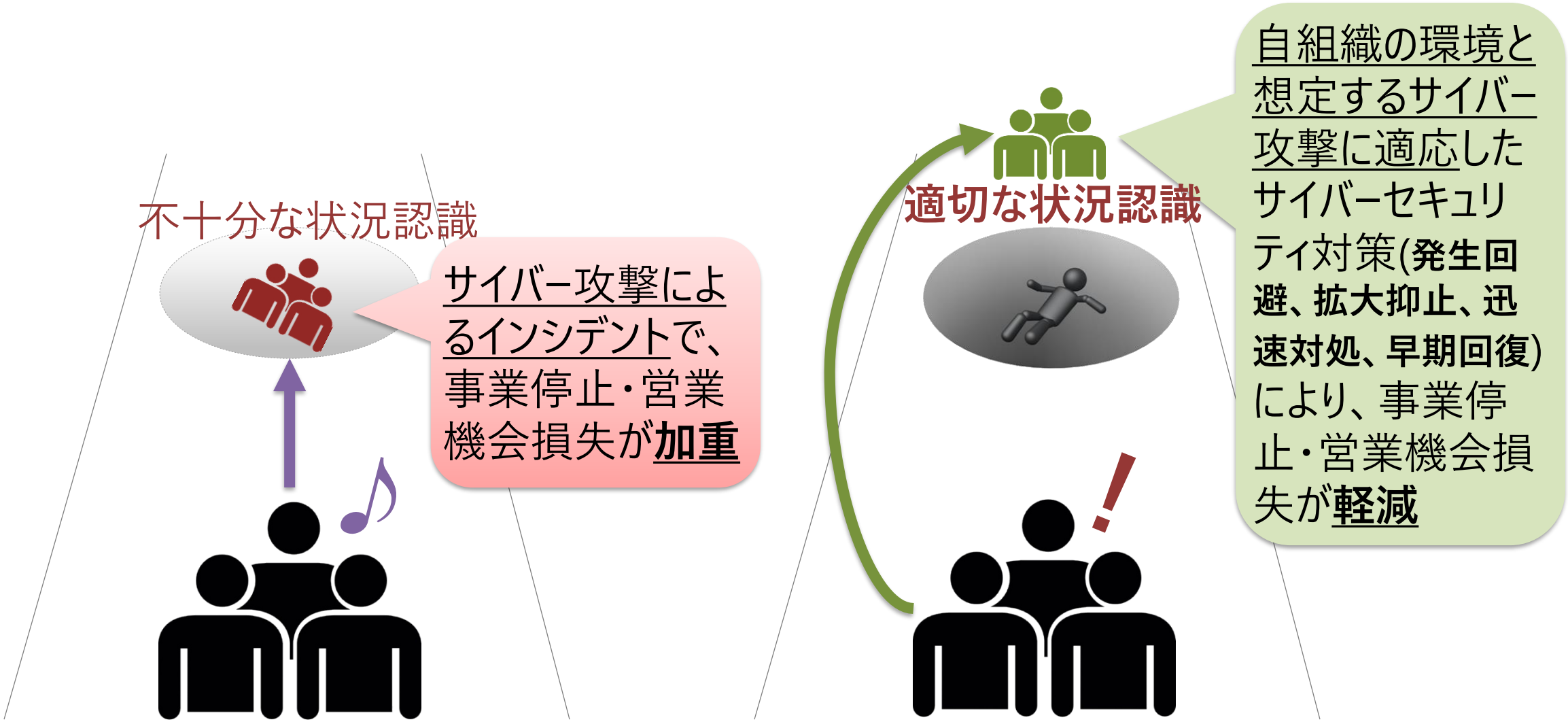
ソフトウェア・サプライチェーンによる不正挙動



トピック 2

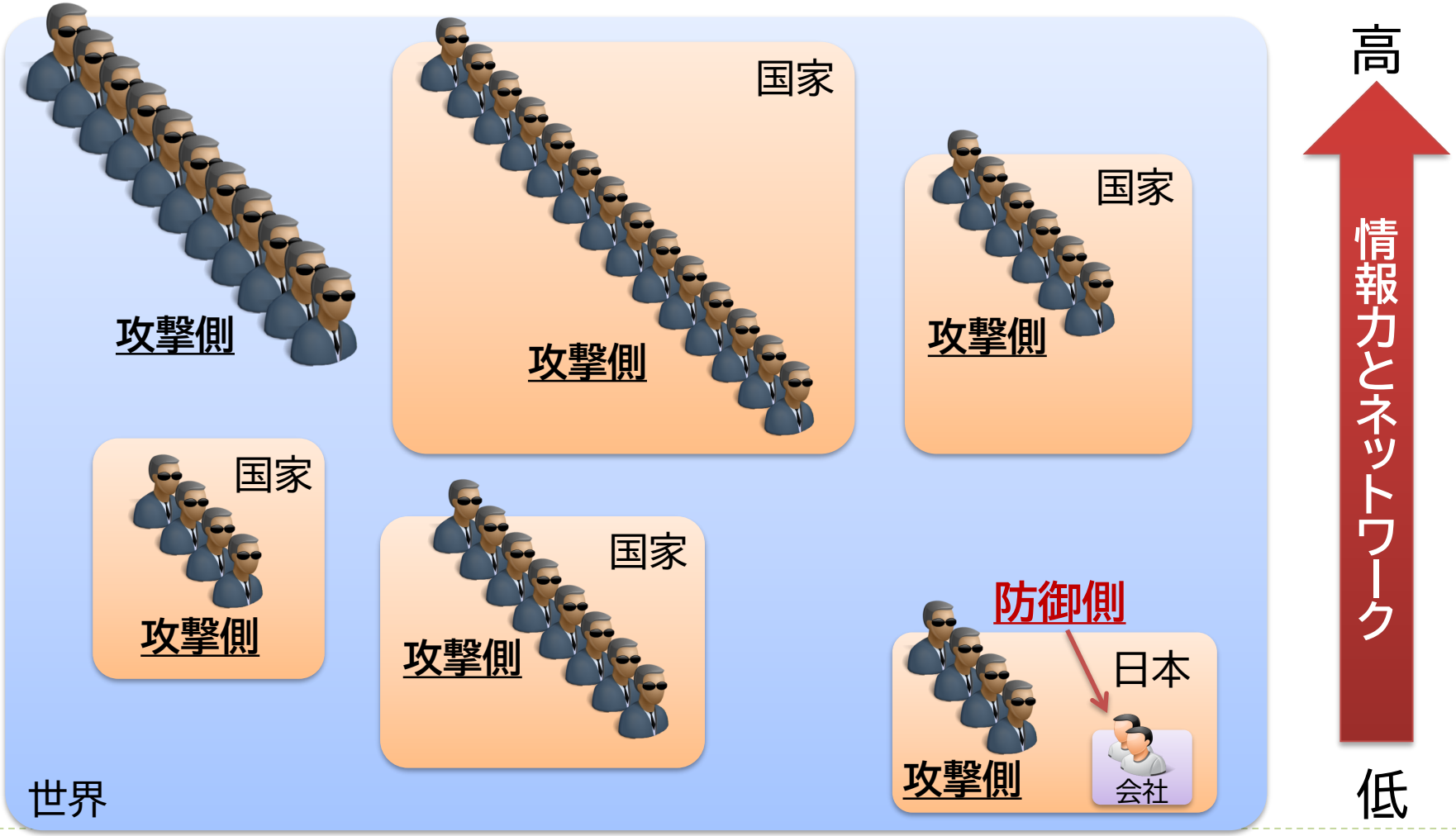
「防御側」の現実

不十分な状況認識 vs 適切な状況認識



「防御側」における **情報力とネットワーク** の圧倒的な低さ

- サイバー攻撃は、攻撃側の事前偵察(窃取)した情報と互助関係にあるネットワークで増大。
- サイバー攻撃は「非対称」であるが、**攻撃側と防御側の情報力とネットワークは「対称」**。



「防御側」における 情報(資産の)保証(IA)に偏重 したセキュリティ対策

- APT攻撃の重点事項は、CND(Computer Network Defense)概念に基づく「システムによる多層的な防御」である。
- IA(Information Assurance)概念に基づいたセキュテリィ対策は、「情報資産の単層的な防御」になりがちである。（IAを重点事項にした場合、システム管理者に対し「*適切に・・・せよ。*」という現場任せの指示になりやすい。）

- 「外部漏洩させない」セキュリティ対策
- 「IA的なインシデント ＝ 情報漏えい」
- 攻撃プロセスの後半で認識
- システム所有者(発注者)が対応

「情報資産」をベースにしたセキュリティ対策

- 「侵入させない」セキュリティ対策
- 「CND的なインシデント ＝ 侵入」
- 攻撃プロセスの前半で認識
- システム保守管理者(委託者)が対応

「システム防護」をベースにしたセキュリティ対策

「防御側」における **厳しい環境と現実**

攻撃側

攻撃の**強い意図や目的**を有する
（経済的利得、主義主張の達成等）

➢攻撃者は、利己的行動の特性を持つ

試行錯誤の侵入行為や
マルウェア作成等による**経験の蓄積**

➢攻撃者は、豊富な（攻撃）経験を持つ

攻撃技術や対象組織に関する情報を
円滑かつ迅速に共有

➢攻撃者は、互いの情報共有が活発

攻撃を実施しやすい
IT環境の獲得と積極的な利用

➢攻撃者は、ITリテラシーを高く発揮できる環境

経済的困窮や利益確保のための
攻撃者の急激な増加

➢攻撃者は、インセンティブを得やすい環境

防御側 (インシデントレスポンダー)

(組織)防御に係る高い目的意識と
活動意欲を有する

➢防御者は、利他的行動の特性を持つ

インシデント対処の**経験の蓄積**
（サイバー演習による擬似的経験）

➢防御者は、豊富な(防御活動)経験を持つ

防御技術や攻撃主体に関する情報を
円滑かつ迅速に共有

➢防御者は、他と情報共有を活発にする

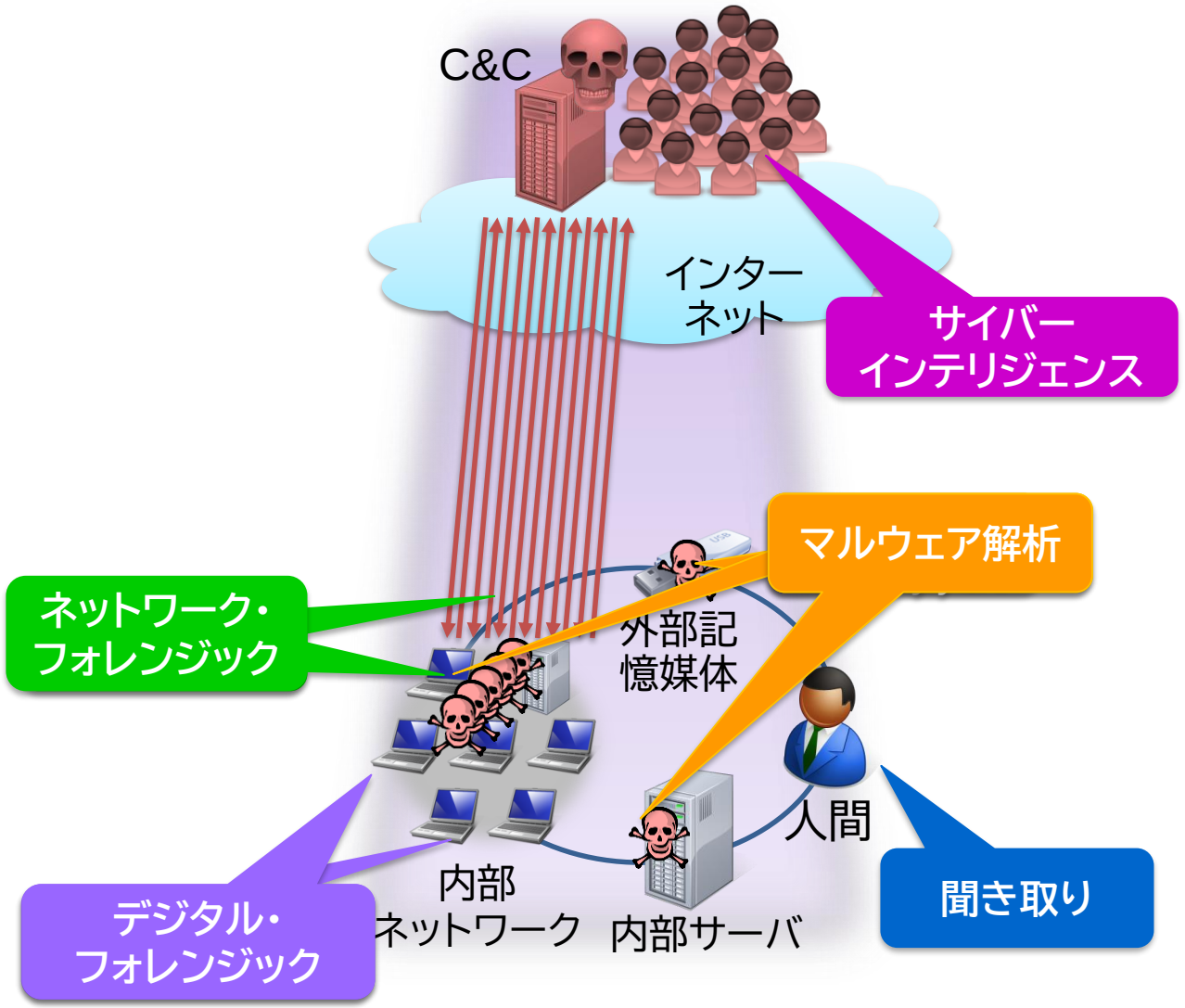
防御を実施しやすい
IT環境の獲得と積極的な利用

➢防御者は、ITリテラシーを高く発揮できる環境

防御活動によるインセンティブのある
対処要員の増強

➢防御者は、インセンティブを得やすい環境

「防御側」に求められる **過度な対処能力**



現場で必要な対処能力

＝

デジタル・フォレンジック

＋

ネットワーク・フォレンジック

＋

マルウェア解析

＋

聞き取り

＋

サイバーインテリジェンス

「防御側」に求められる **過度な対処能力**

以前までの対処活動	デジタル・フォレンジック	**コンピュータシステム上の痕跡**(特にファイルシステムの履歴)、及び搭載されている**ソフトウェアによる様々な記録情報**を分析すること。
	聞き取り	
	マルウェア解析	残存していたマルウェアの静的及び動的解析により、マルウェアの**活動実態やその目的を把握**するために行う分析のこと。
最近の対処活動	インシデントハンドリング／コーディネーション	現場の運用者や技術者だけではなく、責任を持つ管理職や経営層がどのような方針や手順で**インシデント解決までの道筋**(インシデントハンドリング)を立てるか、または、解決のために複数の組織や部署を巻き込む必要のある場合の**組織間連携**(インシデントコーディネーション)をどのようにすべきかなどのアドバイスや方法論・ノウハウを提供すること。
	ネットワーク・フォレンジック	マルウェアの挙動や内部データ(ファイル)の流出経路などを解明する、或いは不正な挙動を確認するも、マルウェアが発見できない場合などに、**サーバ／プロキシ／ファイアウォール等のログを分析**したり、コンピュータシステムにおいてネットワークコマンドやシステム管理コマンドで得られる全ての出力データを総合的に分析すること。
	サイバーインテリジェンス	技術的な分析のみでは解明が困難な場合、同じ分野のレスポンスチームやCSIRTで経験して明らかになっている**攻撃手法や技術、攻撃者コミュニティで流通している手法**、その他、類似したマルウェアによる事例等を収集し、それらの情報との類似性に着目して分析すること。

「防御側」に求められる **過度な対処能力**

以前までの対処活動

デジタル・フォレンジック

聞き取り

マルウェア解析

最近の対処活動

インシデントハンドリング／コーディネーション

ネットワーク・フォレンジック

サイバーインテリジェンス

（技術的能力）

- インターネットのアーキテクチャ、理念、将来像に関する知識
- ネットワークインフラのリテラシーと設計思想の理解
- ネットワークプロトコルの深い理解
- ネットワークアプリケーション、サービス、関連プロトコルの理解
- セキュリティの基本原則
- コンピュータ及びネットワークに対するリスクと脅威の理解
- セキュリティの脆弱性や弱点、及びそれを利用した攻撃の理解
- ネットワークセキュリティ対策とその問題に関する知識と理解
- 暗号化技術、デジタル署名、ハッシュアルゴリズムの理解
- プログラミング、ネットワークコンポーネント、基本ソフトの理解と経験

（管理的能力）

- **安全管理/危機管理/危機対応能力**
- コミュニケーション（対人）能力、言語能力
- 作業編成能力
- 強い目的意識と不屈の精神

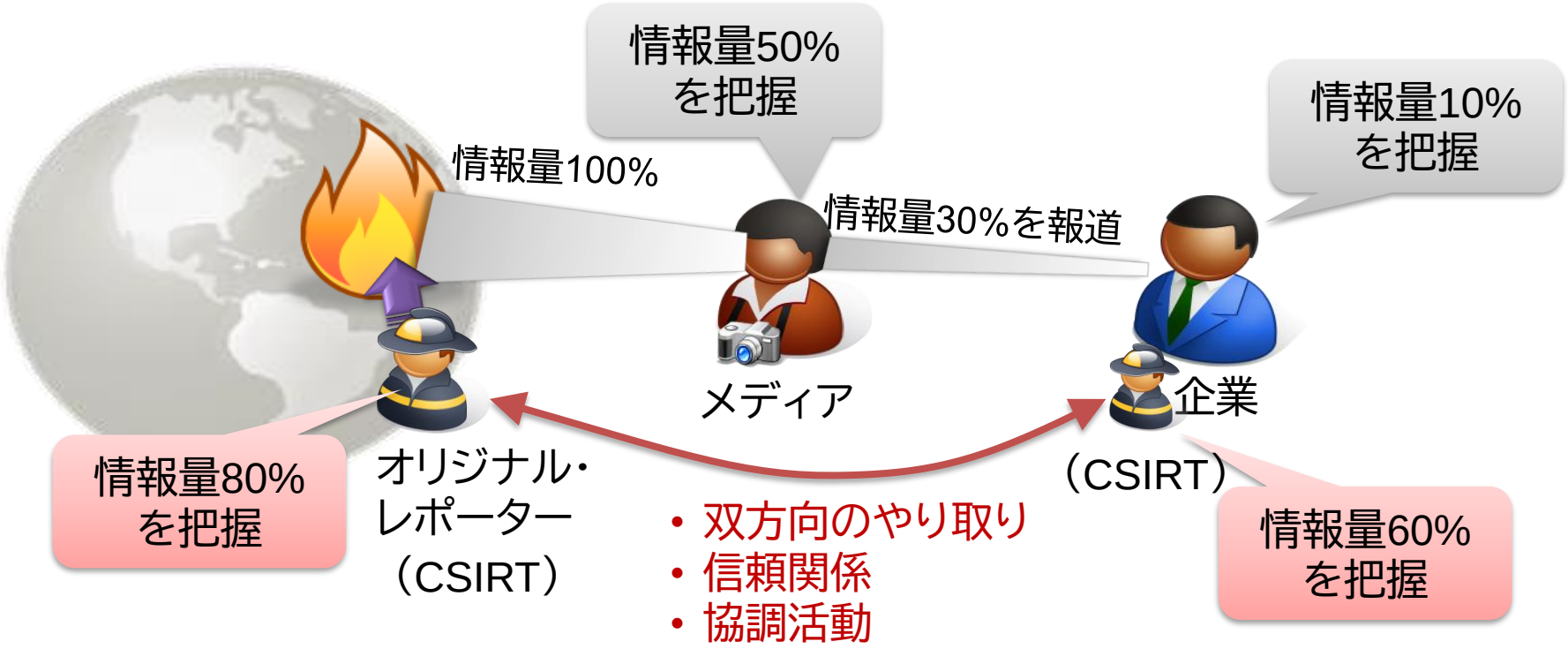
防御側

トピック３

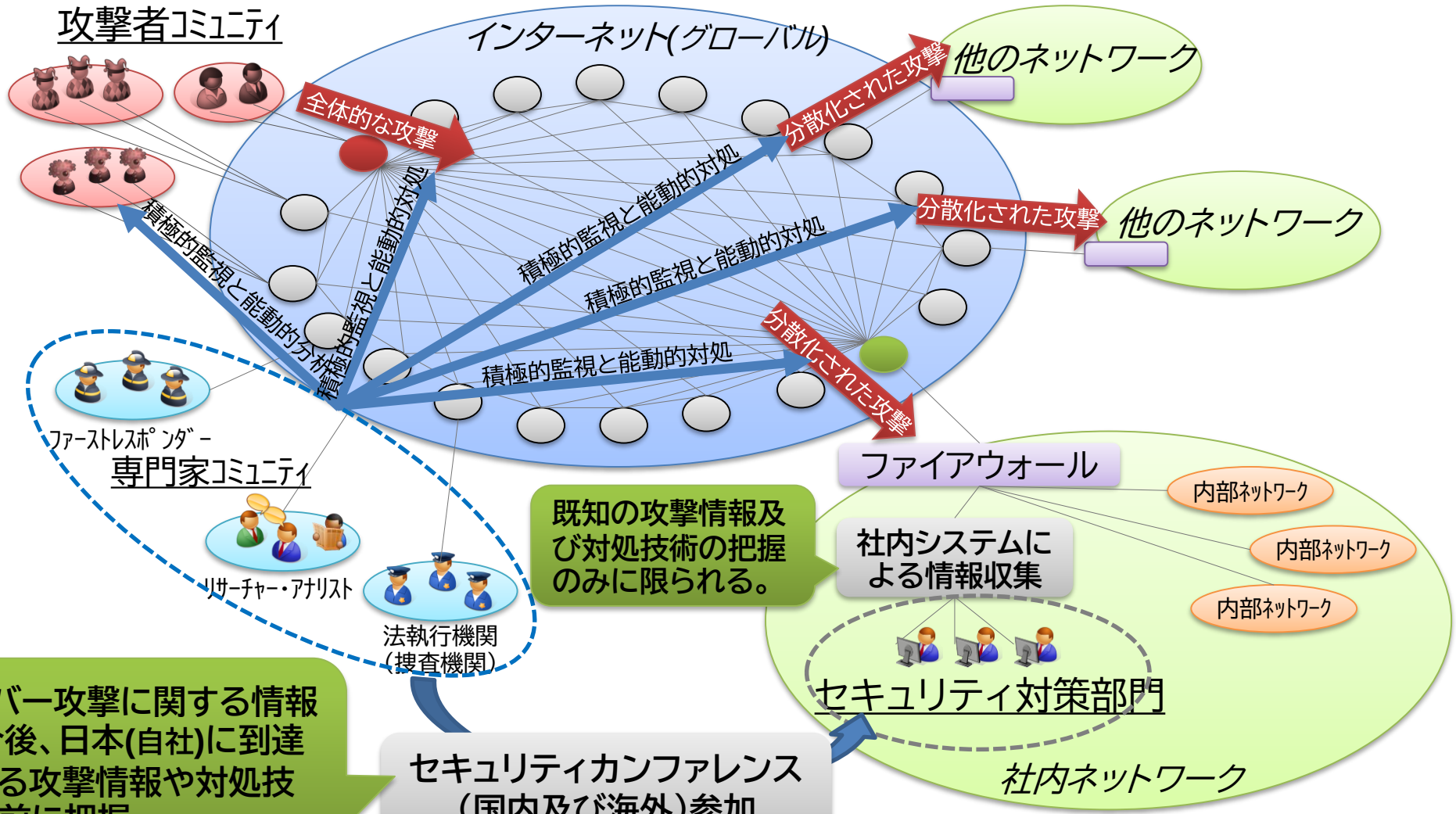
対策・対処のあり方

① サイバー攻撃に関する**正確な事実把握**を行う

- 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。

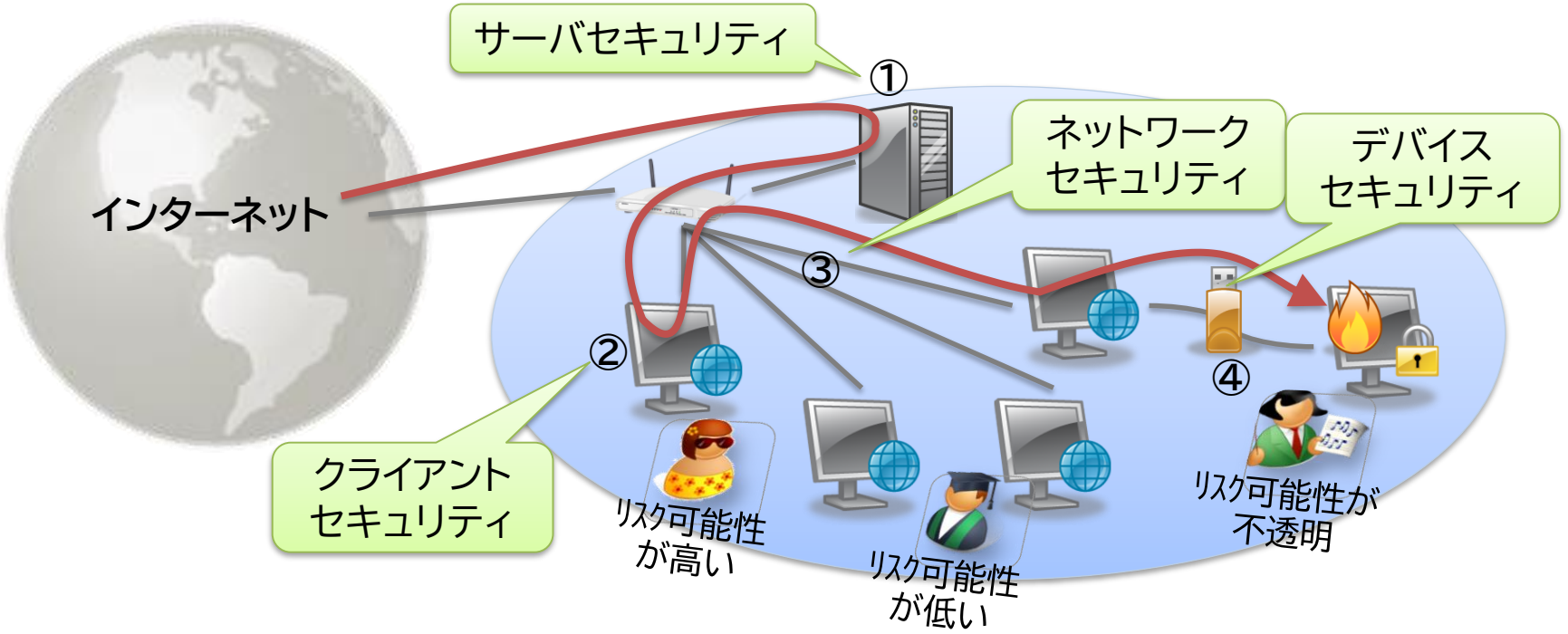


② サイバー空間における**動向情報を積極的に収集**する



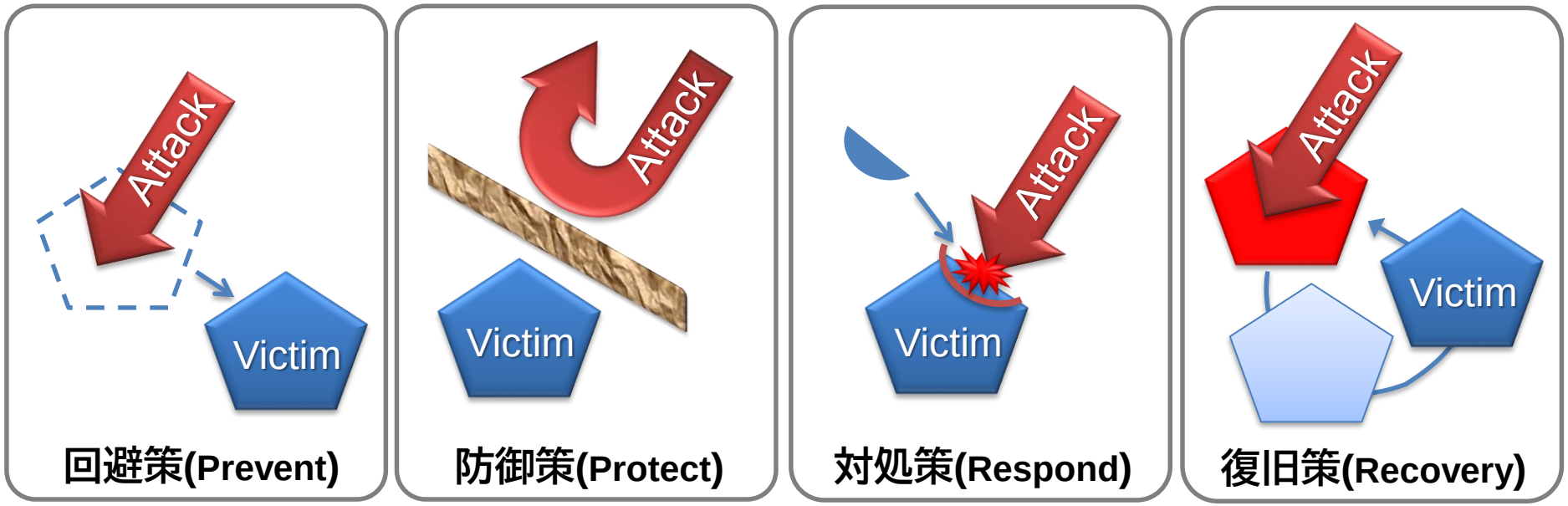
③ **攻撃経路**を見出した上で、多層防御のセキュリティ対策を行う

- 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



④ すべてのサイバー攻撃対処に**明確な目的を設定**する

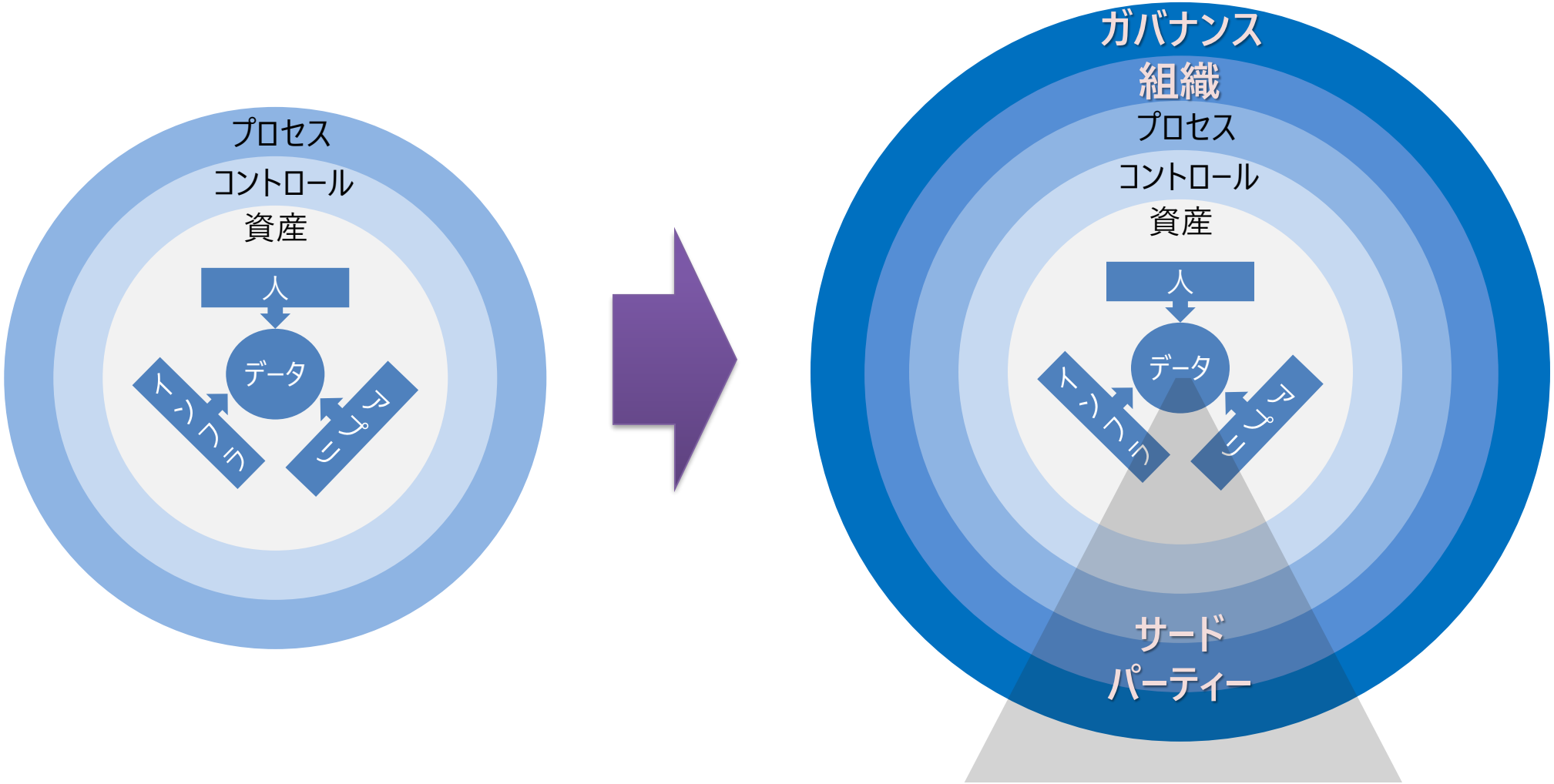
- サイバー脅威に対して、**網羅性の高い対策**を検討し、実装及び確実な運用をすること。
  - 日本国内の対策は、「防御策(Protect)に偏重」しているため、いたずらにコストがかかってしまう状況。
  - 最近のサイバー防衛策におけるベストプラクティス(最善策)は、対処策(Respond)である。
    （最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。）
  - 基本的な対策コンセプトは、次の4つのとおり。



【参考】組織が取り組むべき**サイバーリスク・マネジメント**のアプローチ

古典的なサイバーセキュリティの焦点

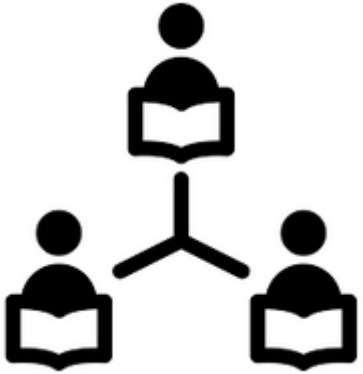
包括的なサイバーリスク・マネジメントのアプローチ



【参考】組織としてのサイバーセキュリティ向上のためのプログラム

オンライン・セミナー

カンファレンス／セミナー



オンライン・コラボレーション

サイバー・レンジ

アナリスト・ミーティング

オンライン・カンファレンス

ミーティング

セキュリティ評価

本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01