TLP:WHITE

図解で理解するサイバー脅威と『思い切って』変革すべき対策の考え方

2022年 7月

名和 利男

アジェンダ

1. 図解で理解するサイバー脅威

2. 受け入れなければならない現実

3. 『思い切って』変革すべき対策の考え方

TLP:WHITE

TLP:WHITE

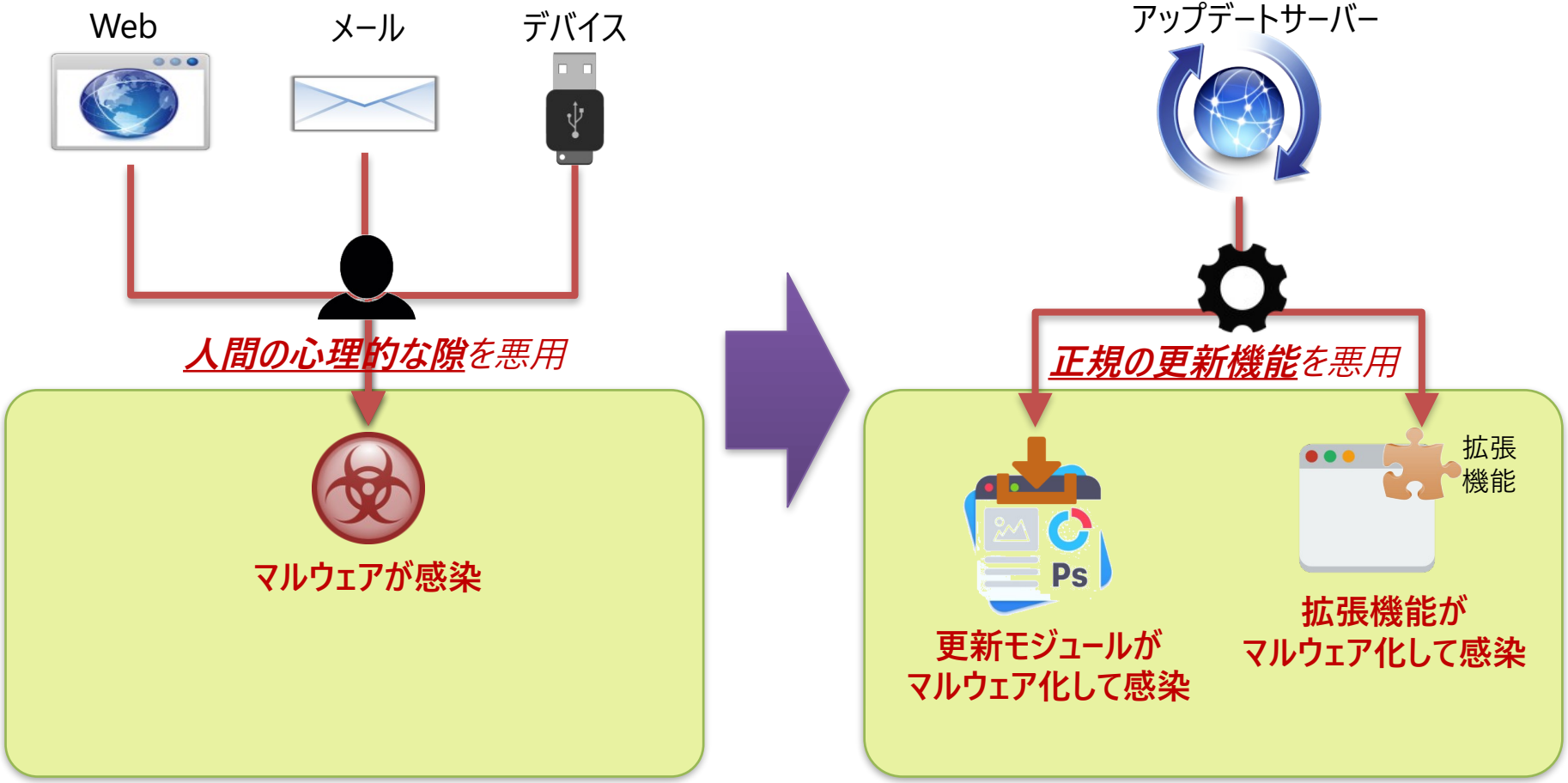
トピック１

図解で理解するサイバー脅威

図解で理解するサイバー脅威

1. **正規の更新機能**を利用するマルウェア感染
2. **正規（有名）サービス**を（時間差で）踏み台にするC2通信
3. 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
4. **正規（有名）サービス**の同期機能を利用するC2通信
5. 様々な対象から**調達・窃取した認証情報**の悪用
6. **敵対国のソフトウェアやプロダクト**からのデータ流出
7. **機械設備のPC**に対するマルウェア感染
8. **偽Wi-Fiアクセスポイント**による中間者攻撃
9. **悪意のあるDNSサーバ**によるC2通信
10. **ソフトウェア・サプライチェーン**による不正挙動

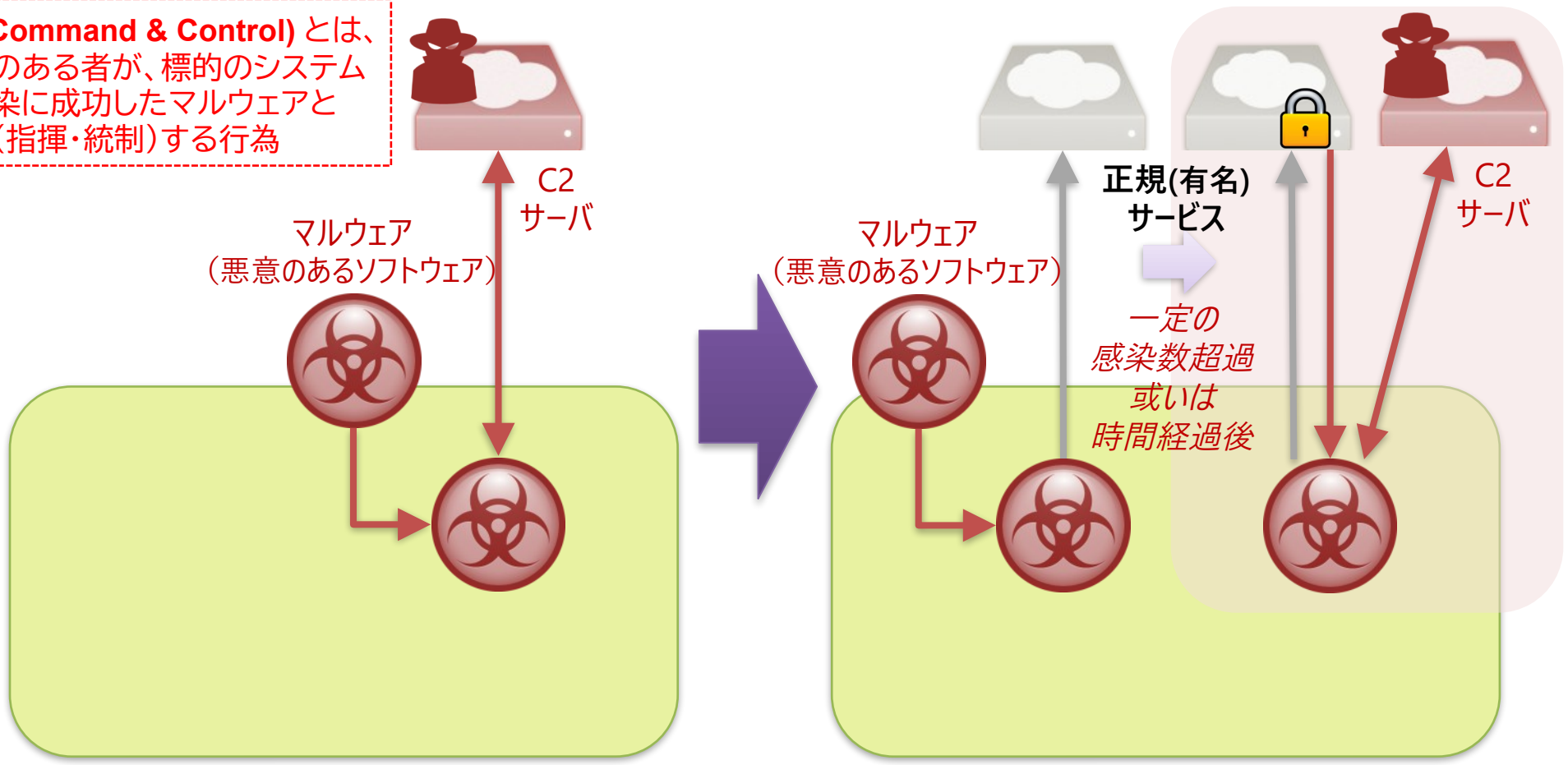
1. 正規の更新機能を利用するマルウェア感染



TLP:WHITE

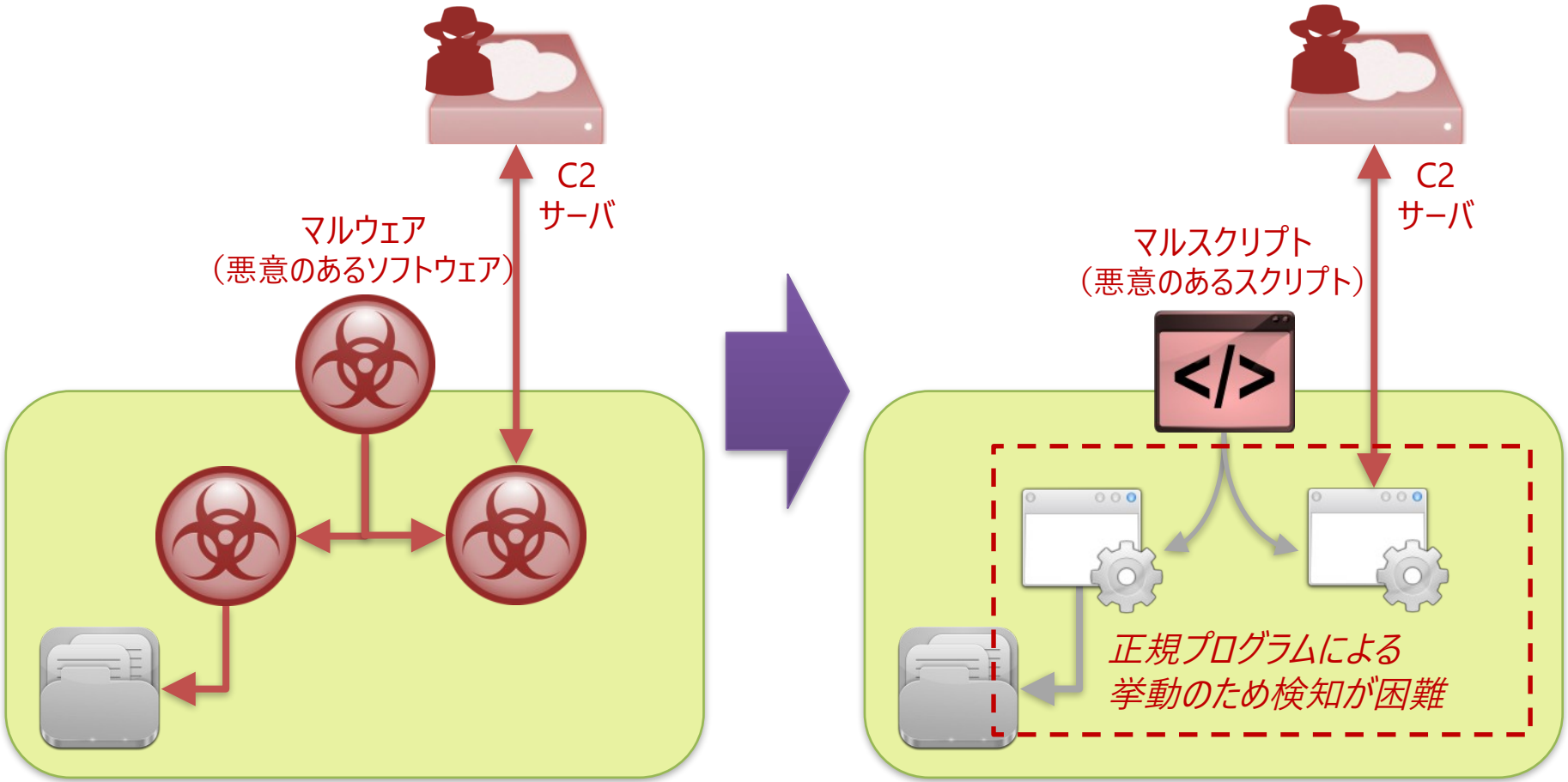
2. 正規(有名)サービスを(時間差で)踏み台にするC2通信

C2 (Command & Control) とは、悪意のある者が、標的のシステムに感染に成功したマルウェアと通信(指揮・統制)する行為



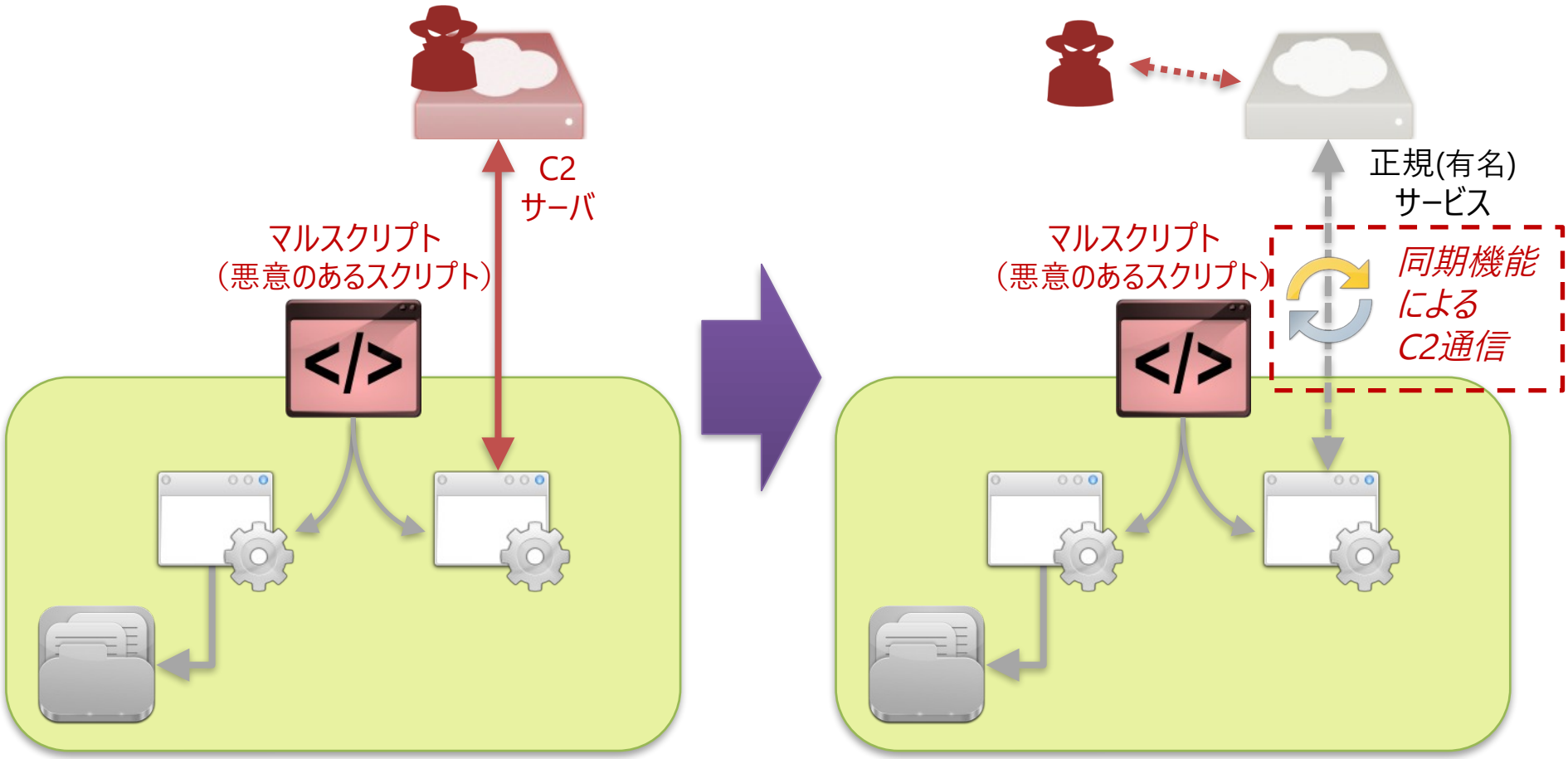
TLP:WHITE

3. 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



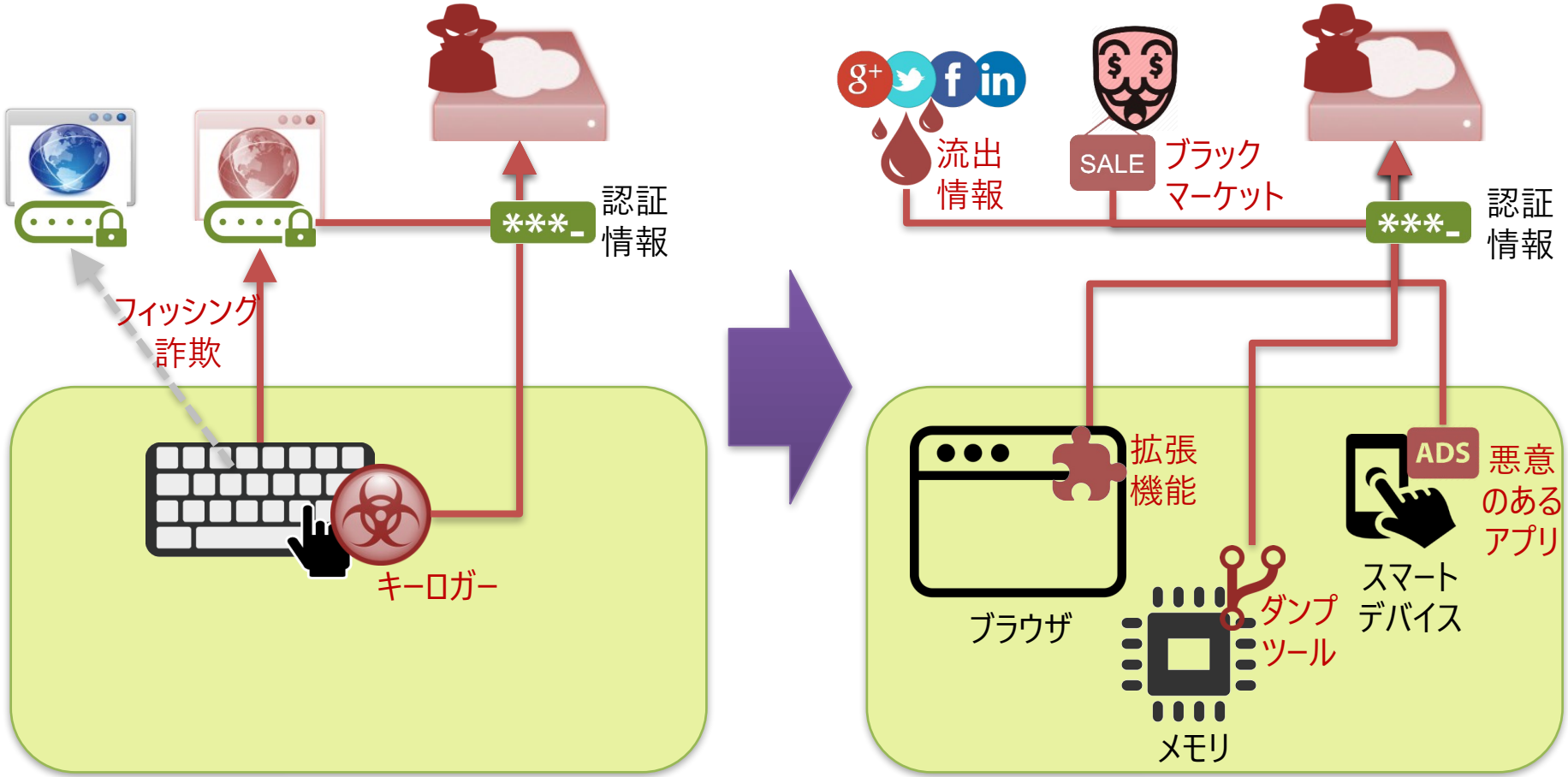
TLP:WHITE

4. 正規(有名)サービスの同期機能を利用するC2通信



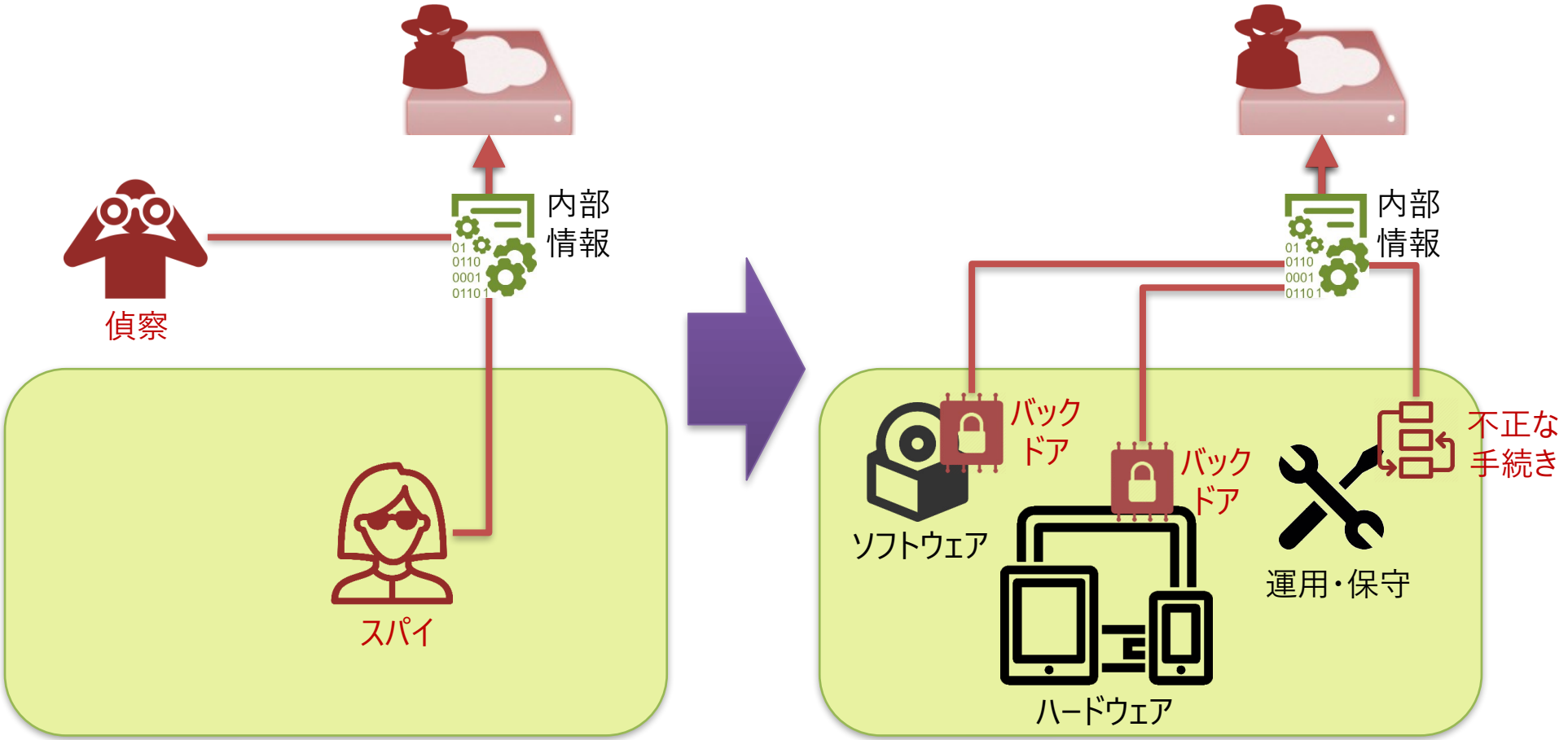
TLP:WHITE

5. 様々な対象から**調達・窃取した認証情報**の悪用



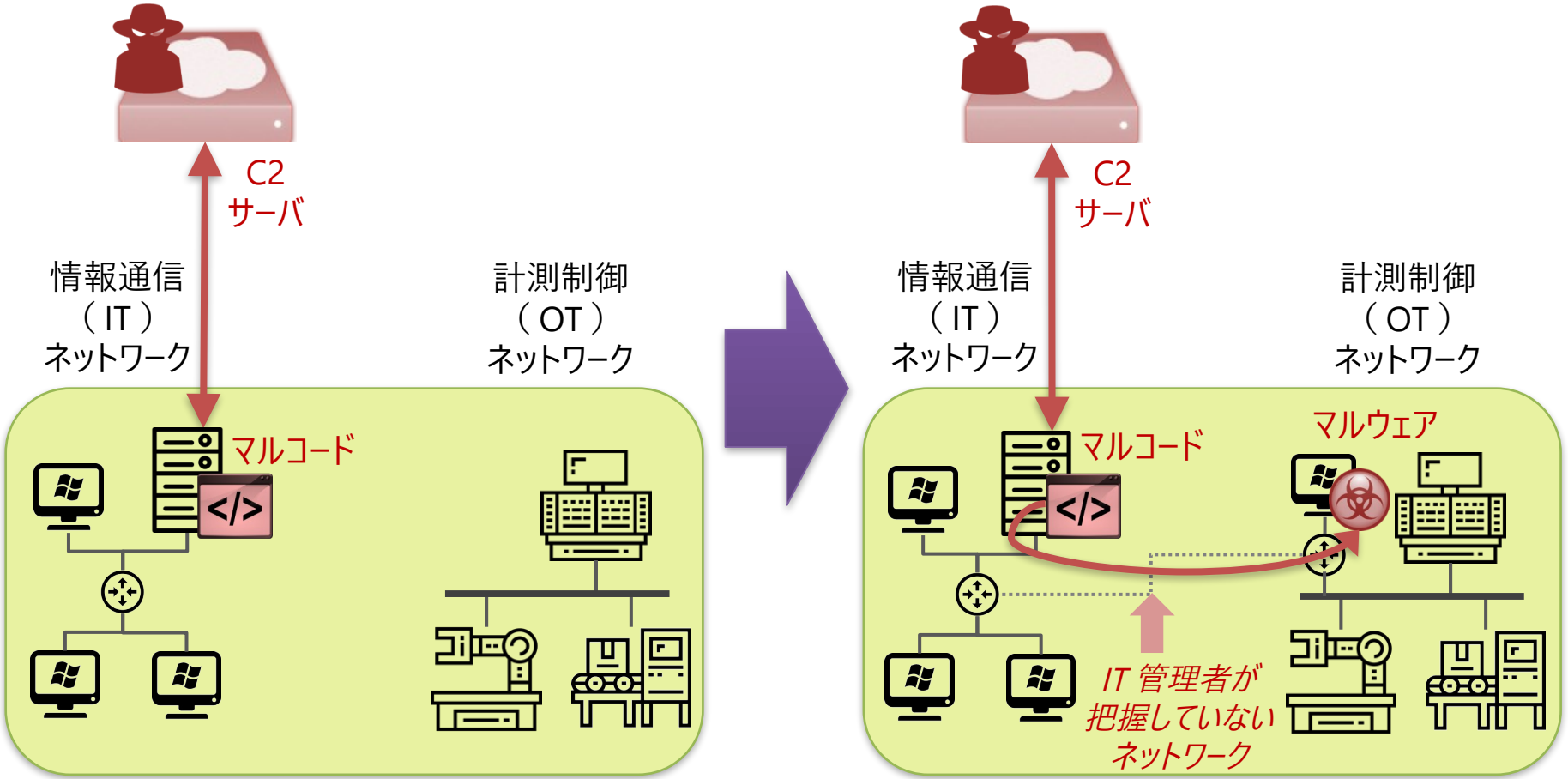
TLP:WHITE

6. 敵対国のソフトウェアやプロダクトからのデータ流出



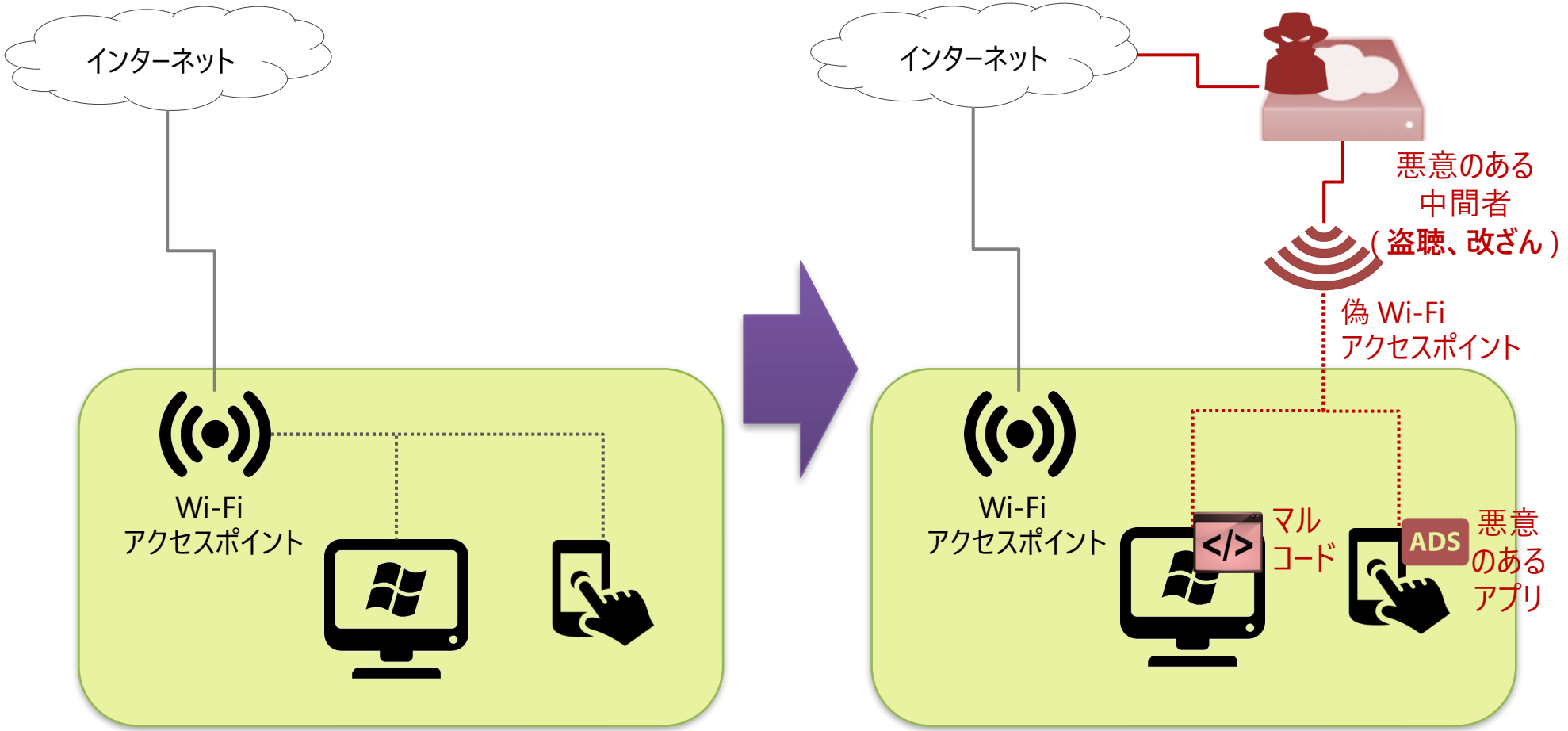
TLP:WHITE

7. 機械設備のPCに対するマルウェア感染



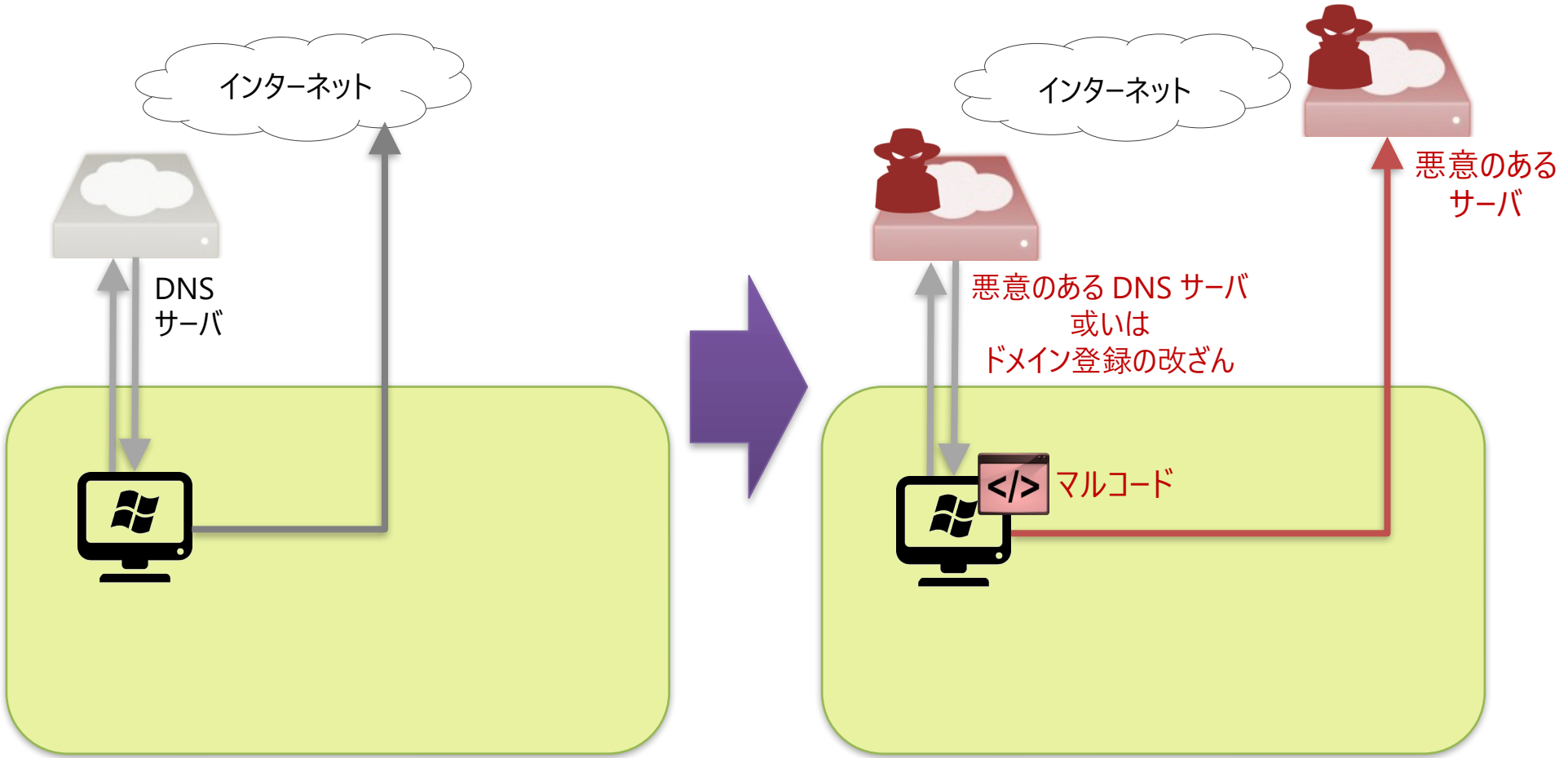
TLP:WHITE

8. 偽Wi-Fiアクセスポイントによる中間者攻撃



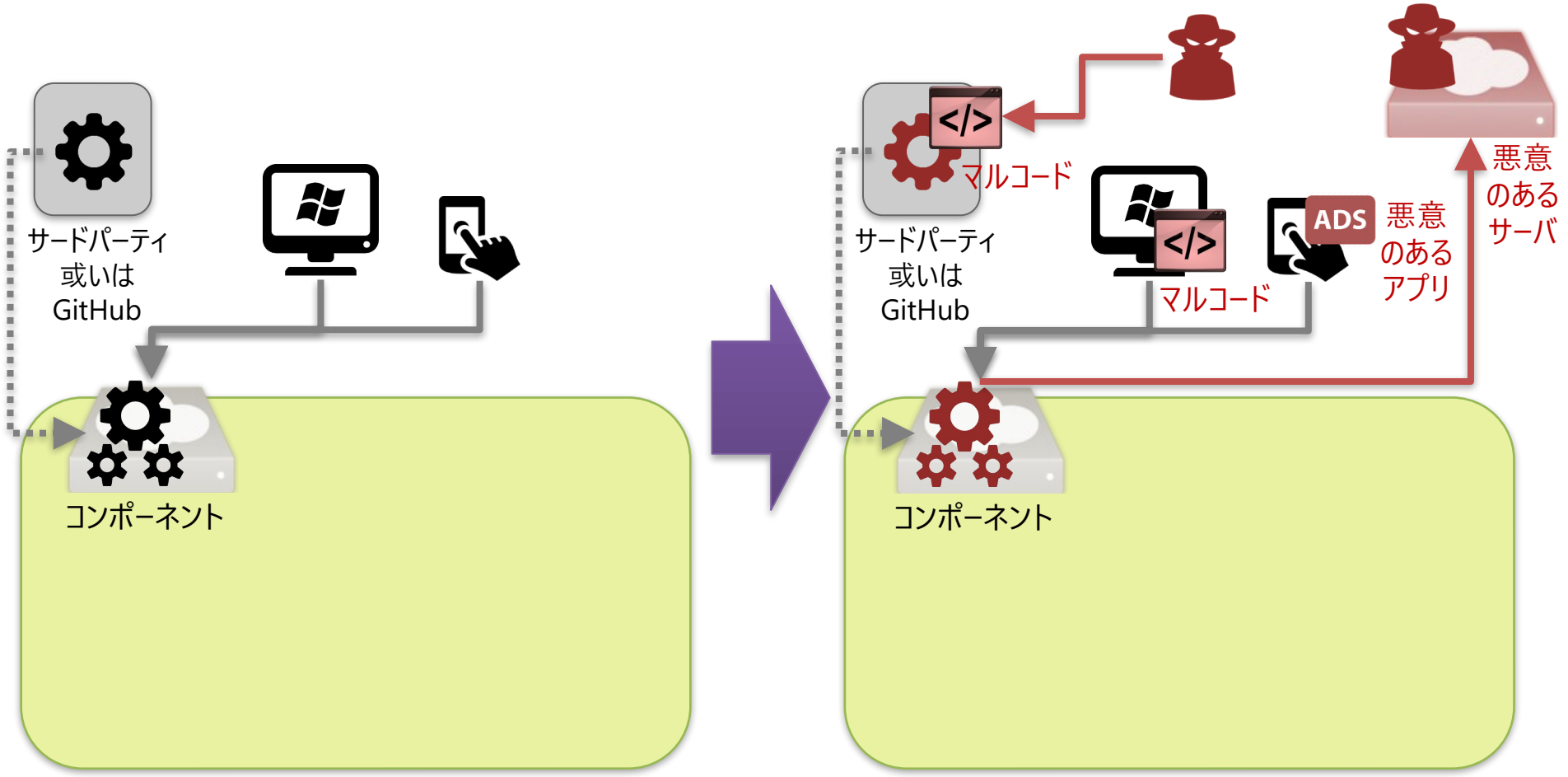
TLP:WHITE

9. 悪意のあるDNSサーバによるC2通信



TLP:WHITE

10. ソフトウェア・サプライチェーンによる不正挙動



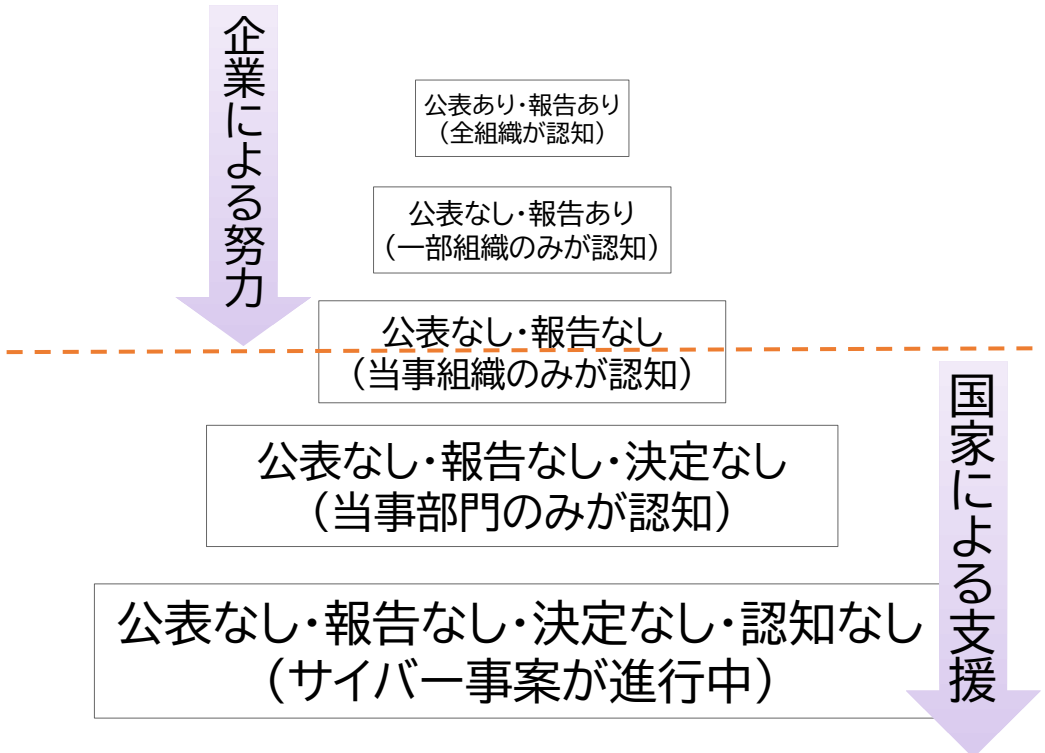
TLP:WHITE

トピック２

受け入れなければならない現実

サイバー脅威の状況認識の獲得は難しい

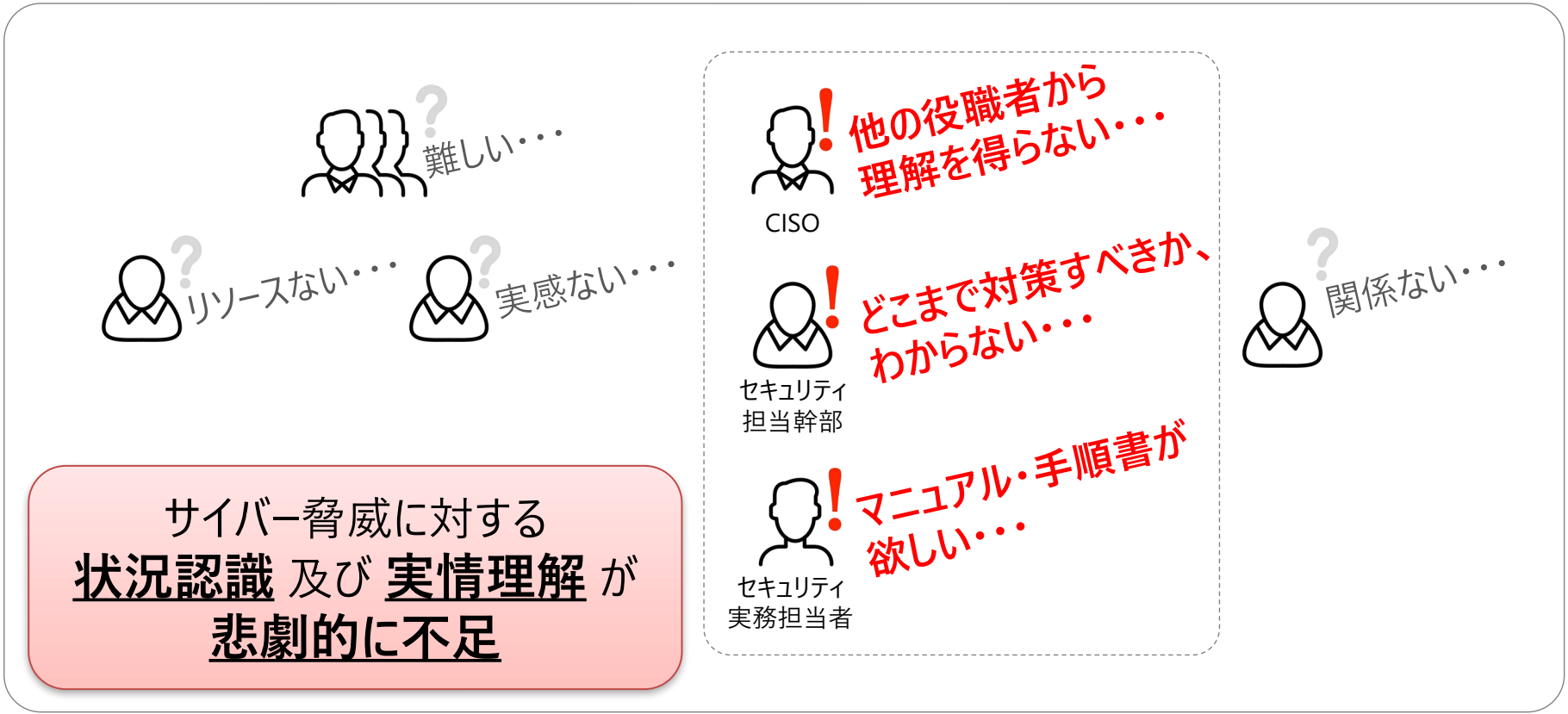
- 不特定多数に公表される**「サイバー攻撃事例」が少ない**。



TLP:WHITE

担当者への**丸投げ**

- サイバーセキュテリィ担当を決めて、**（ほぼ）丸投げ**している。



TLP:WHITE

方向性の異なる準備姿勢

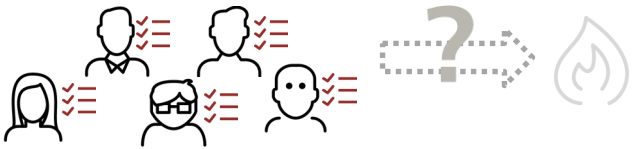
- 情報セキュリティの管理策（英語では Security Control）の影響により、セキュリティ対策における実行主体の性質が「体制」をベースにしている。
- サイバー攻撃対処の観点においては、「態勢」でなければならない。
- それぞれにおいて**取るべき行動の準備姿勢が大きく異なる**。

– **態勢**: 事態に対処するための準備ができている状態のこと。（**前もっての身構え**）

本当に事態対処できるかどうかが重要

– **体制**: 基本原理・方針によって秩序づけられている組織のこと。（**政治支配の様式**）

組織内の役割分担（責任所在）が重要



TLP:WHITE

情報(資産の)保証に偏重したセキュリティ対策

- サイバー攻撃の重点事項は、CND（Computer Network Defense）概念に基づく「**多層的なシステムによる防御**」である。
- IA（Information Assurance）概念に基づいたセキュテリィ対策は、「**単層的な情報資産の防御**」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」ためのセキュリティ対策
- 「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

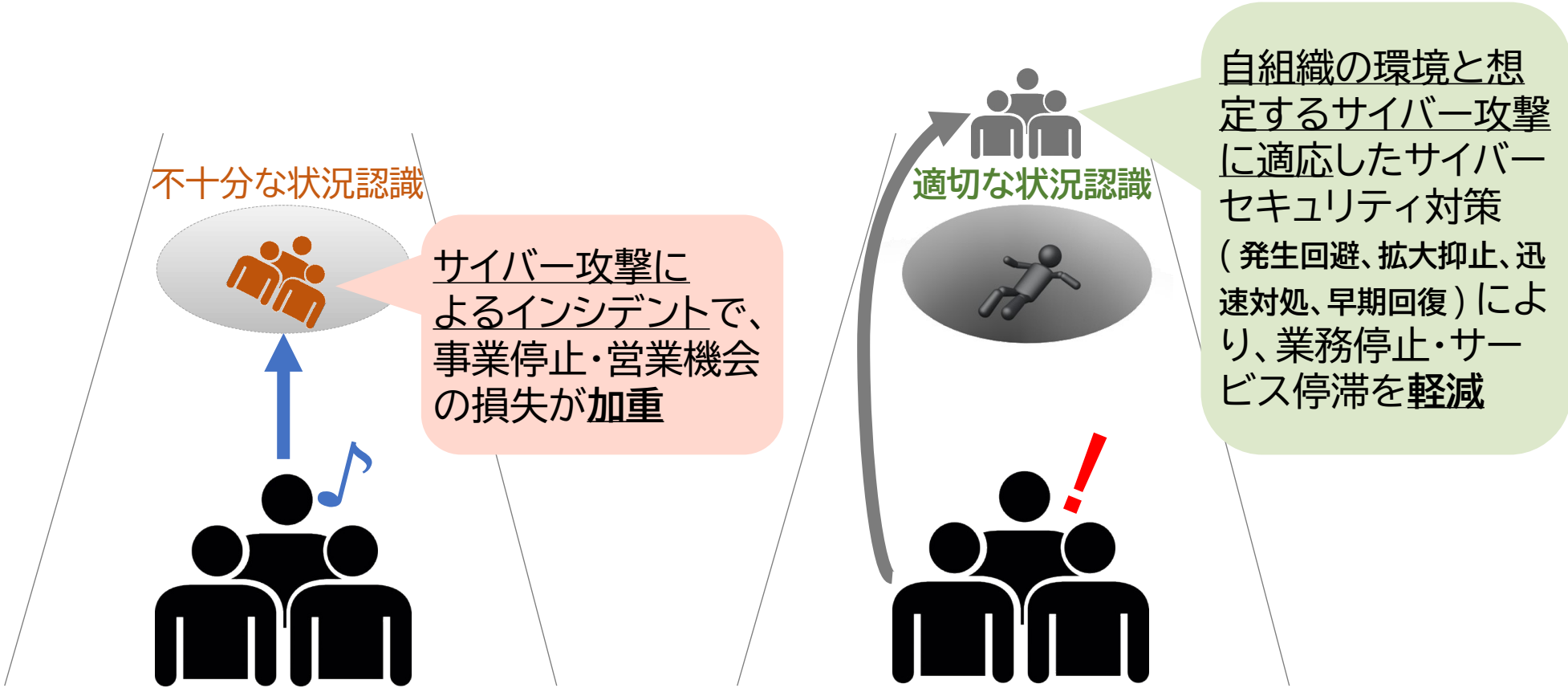
「**情報資産**」をベースにしたセキュリティ対策

- 「侵入させない」ためのセキュリティ対策
- 「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

TLP:WHITE

状況認識の不足による**想像力の欠如**



TLP:WHITE

ほぼすべてにおいて意思決定プロセスが遅い

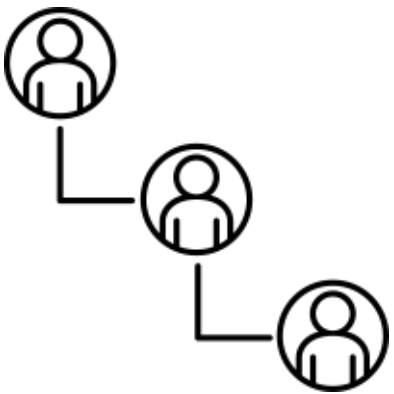
依然として「表面的な組織構造」と「内面的な組織構造」の2つが共存している。

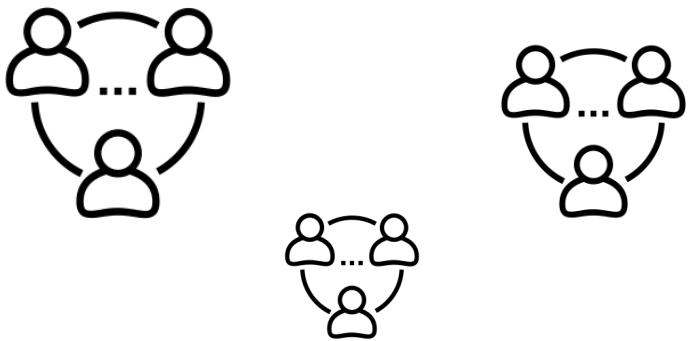
表面的な組織構造

- ピラミッド型の階層化された権限
- トップダウン型の上意下達
- 規律やルールによるガバナンス（統制）

内面的な組織構造

- 同じ階層における社員間の**非公式なやり取り**
- **横並び意識**と**同調圧力**の場の空気
- 上位階層への**忖度**と隣接領域への**根回し**





トピック３

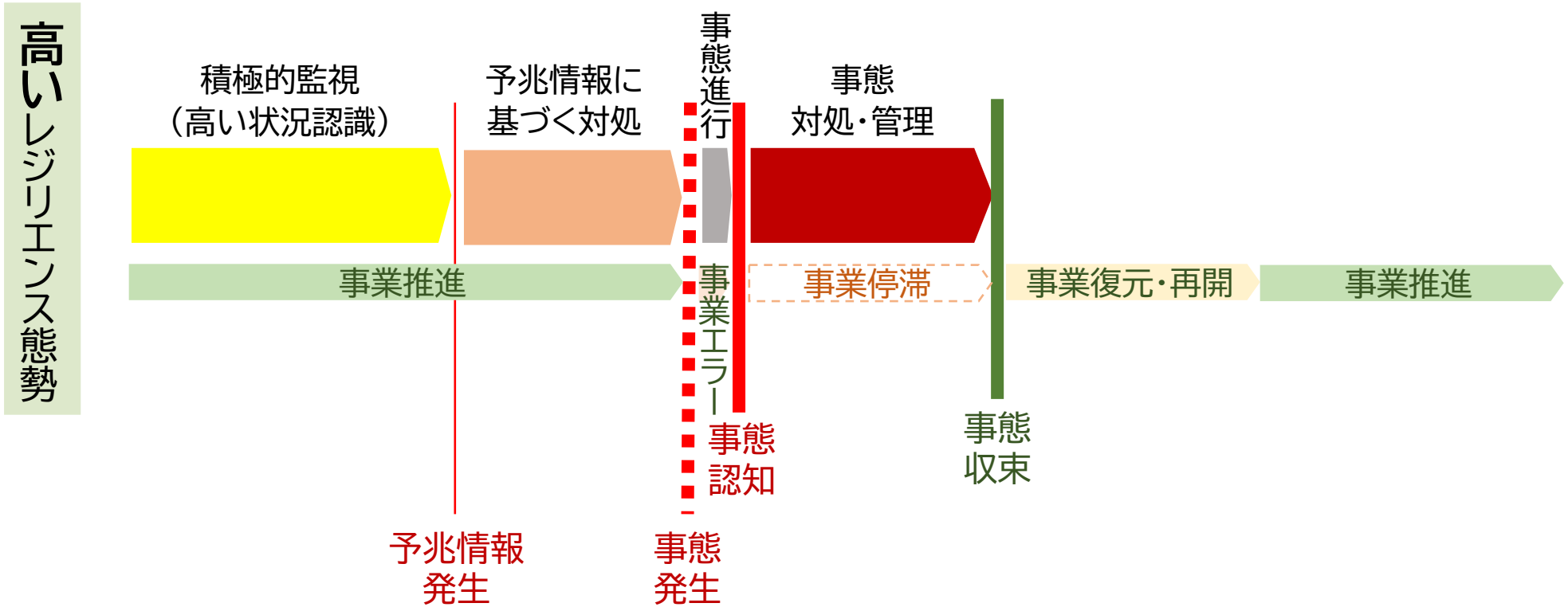
『思い切って』変革すべき対策の考え方

「サイバーレジリエンス態勢」を高める

- サイバー空間に依存している事業におけるレジリエンス(Resilience)とは
  - 悪意のあるサイバーイベント(セキュリティ侵害等)が発生しても、**意図した結果(Intended outcome)を継続的に提供する企業・組織の能力**のこと
- 「サイバーレジリエンス態勢」を高めることで、事業の継続性を脅かすサイバー侵害を受けても、**早期に正常な事業環境を復元し、通常の事業を再開できる**ようにする。

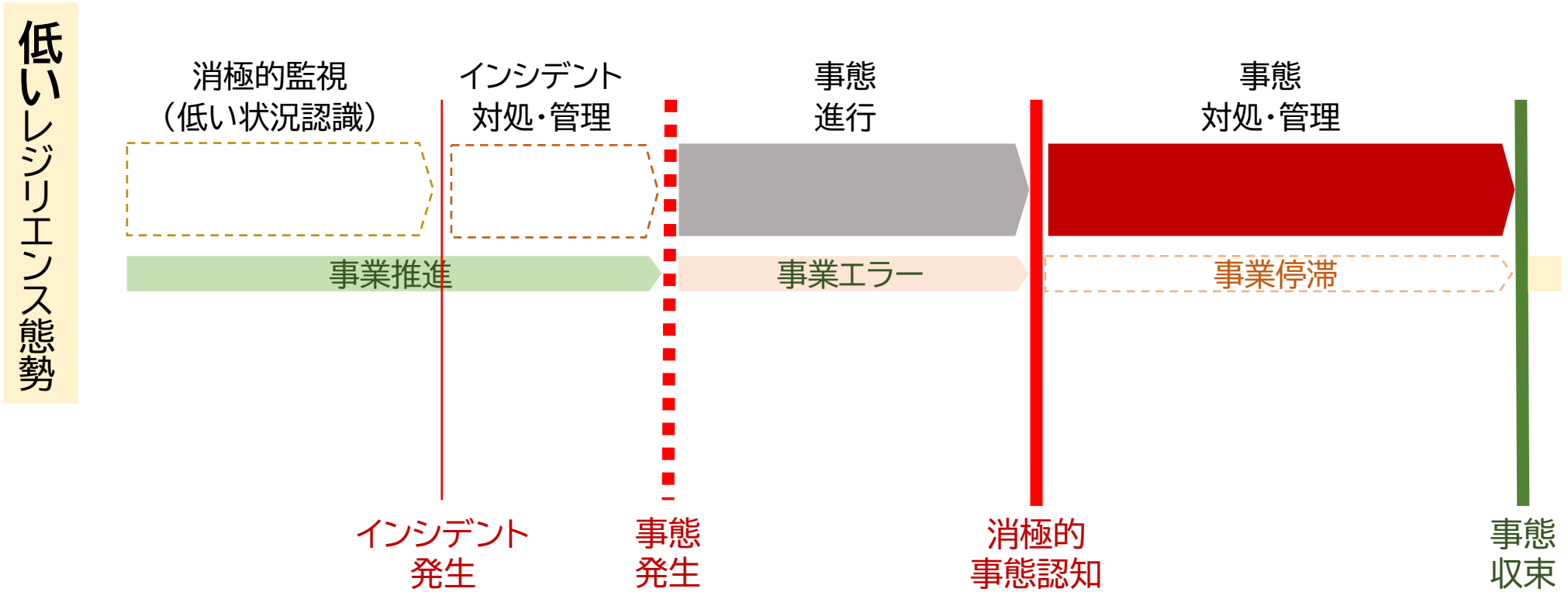
「レジリエンス(Resilience)」は、
対象に圧力がかかった状態に対する
「復元力」や「回復力」「弾力性」などと
意訳され、物理学、生態学、心理学等
で使用されている。

【参考】「高いレジリエンス態勢」のイメージ



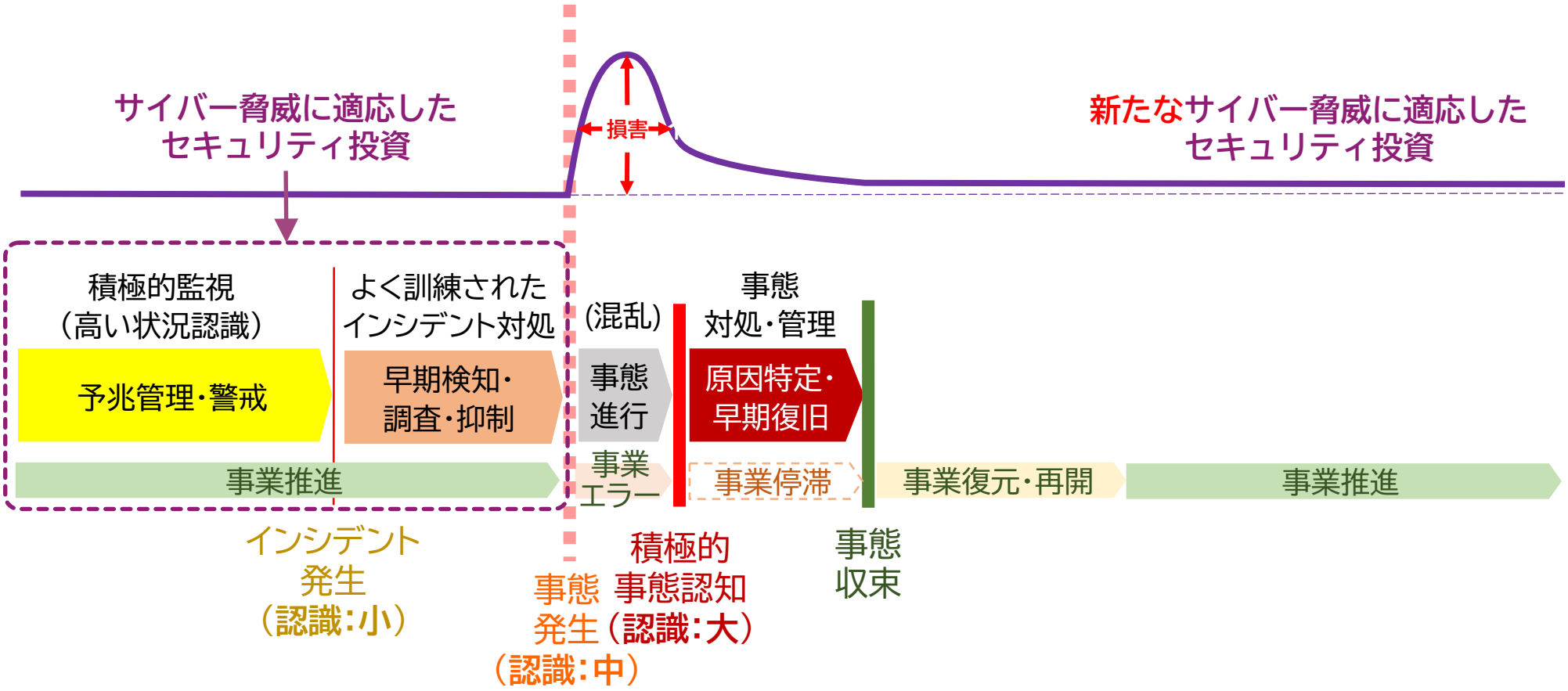
TLP:WHITE

【参考】「低いレジリエンス態勢」のイメージ



TLP:WHITE

実現すべき「サイバーレジリエンス態勢」のイメージ



TLP:WHITE

「組織を守るため」の努力方法

- 従来の情報セキュリティの概念や体制では、**組織を守れない**ことを受け入れること。
  - 最近の**サイバー脅威に適合したセキュリティフレームワーク**を選択することが必要。
- 組織運営において、**サイバーレジリエンスの成熟度向上**を優先事項にすること。
  - **上層部の意識改革**と実務担当者の知識と経験の習得が必要。
- すべての組織構成員（職員員等）に対して、**意識向上トレーニング**を行うこと。
  - 特に、フィッシングメールを**識別する機会**を提供。（開封率は、必然的な結果であり目標ではない。）
- 定期的に**セキュリティ監査**を実施すること。
  - 特定のテクノロジーがどのように実行されているかについての**洞察を獲得**。
- 最大限のパフォーマンスを発揮するために**自動化を推進**すること。
  - 特に、セキュリティ部門のパフォーマンスを向上させるために**ソリューションを導入**。

本資料に関する連絡先

名和 利男（ Toshio NAWA ）

SITE: https://www.nawa.to

PGP: 0xE38B4E01