Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

制御システムセキュリティカンファレンス 2014

企業組織に迫りくるセキュリティ脅威への備えと対策

2014年2月5日（11:30-12:00）

JPCERTコーディネーションセンター
理事・分析センター長　真鍋　敬士

本日お話ししたいこと

最近のサイバー攻撃例

インシデントへの対応

サイバー攻撃事例

- サイバー攻撃事例 -

ある日…

製造業の株式会社αからJPCERT/CCにインシデント情報の提供
- ✓ ネットワーク監視サービスで不審な通信の報告
- ✓ 乗換検索サイトβにアクセスした際に感染
- ✓ 感染したマルウエアに関する情報を提供

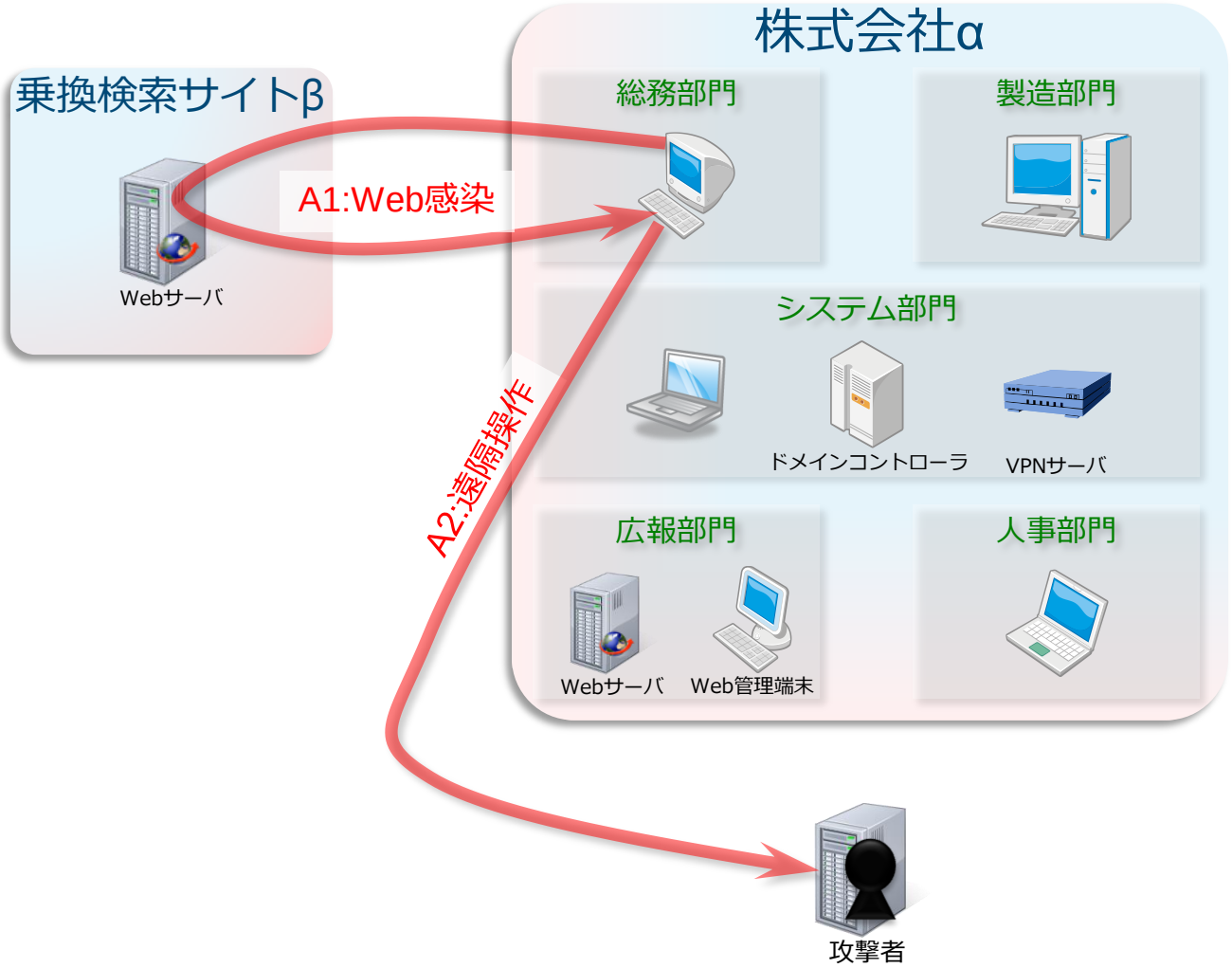
一見すると
ウェブ改ざん

侵入型の
マルウエア

乗換検索サイトβを運営する組織に情報を提供

当該ウェブや不審な通信先に関する情報を展開

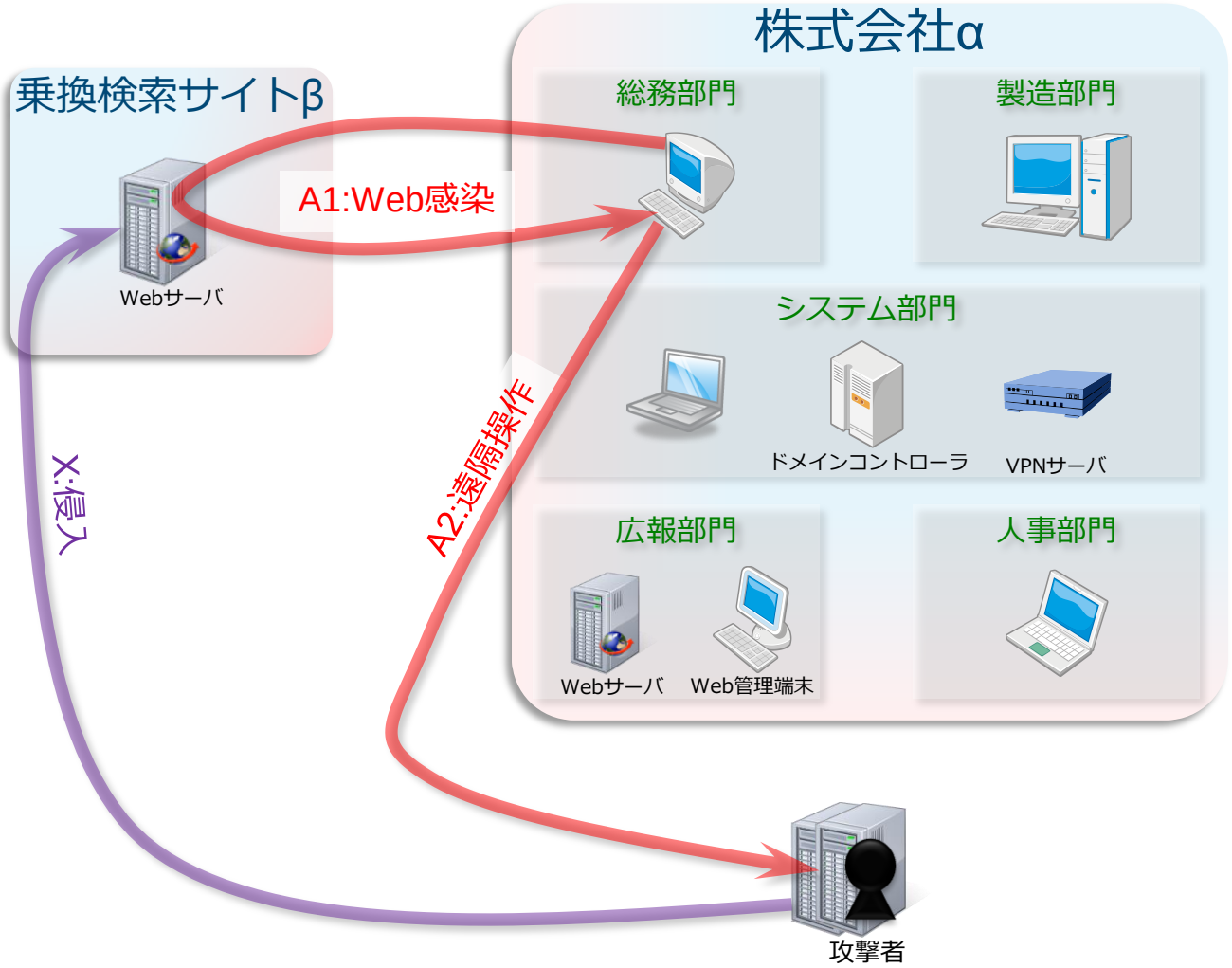
1日目：αからの最初の情報提供



【αでの調査】

- 総務部門のPCが不審なサイトに通信していた。
- ファイアウオールでサイトへの通信をブロックした。
- 当該PCを隔離して調査した。
- βにアクセスした時にマルウエアをダウンロード・実行させられていることが判明した。
- βへのアクセスは日常業務で、直前までは異常なかった。

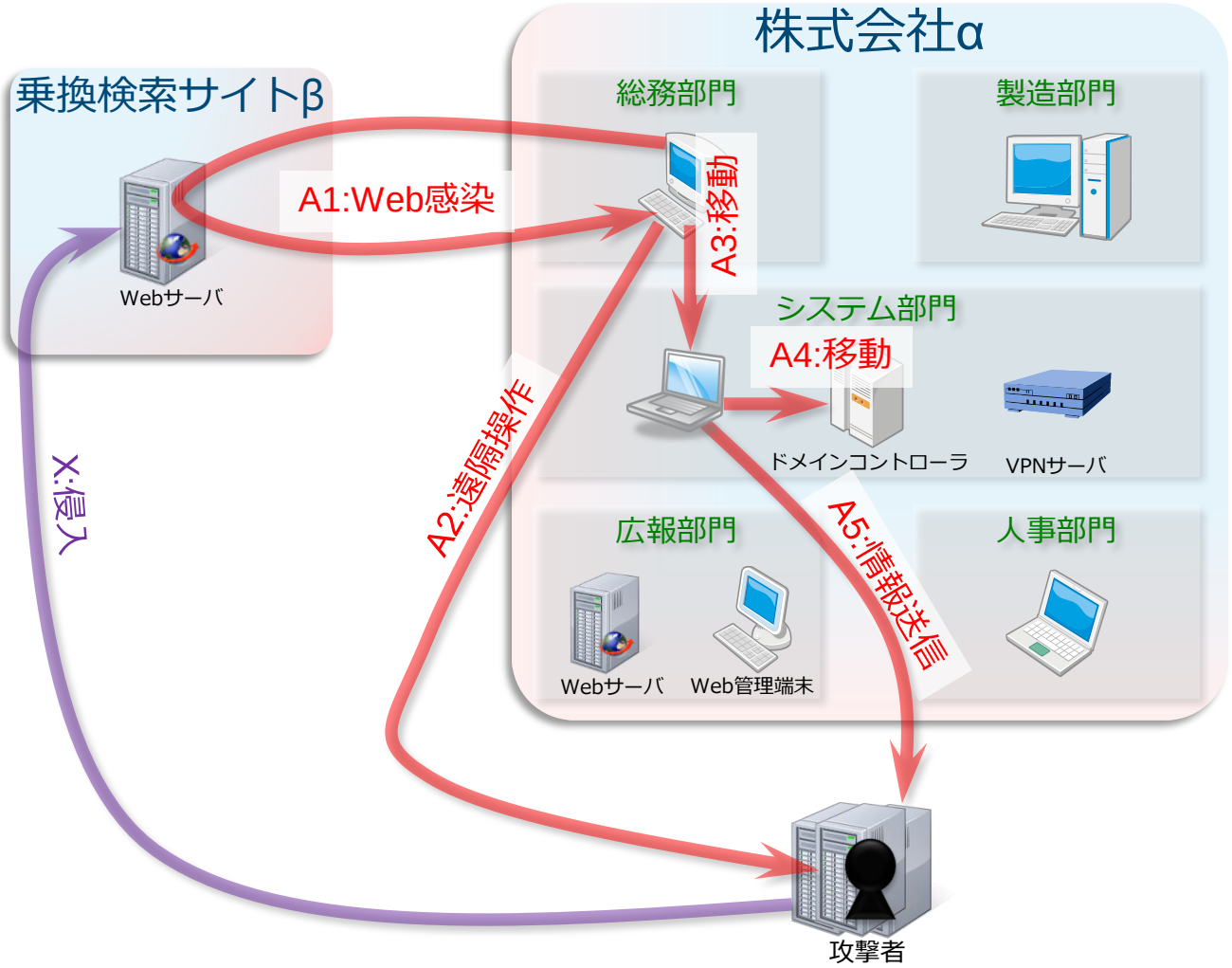
2日目：βからの情報提供



【βでの調査】

- 1ケ月前に外部から侵入されていた。
- 特定のアクセス元に対して不審なサイトへリダイレクトする設定が追加されていた。

2週目：αからの追加情報提供

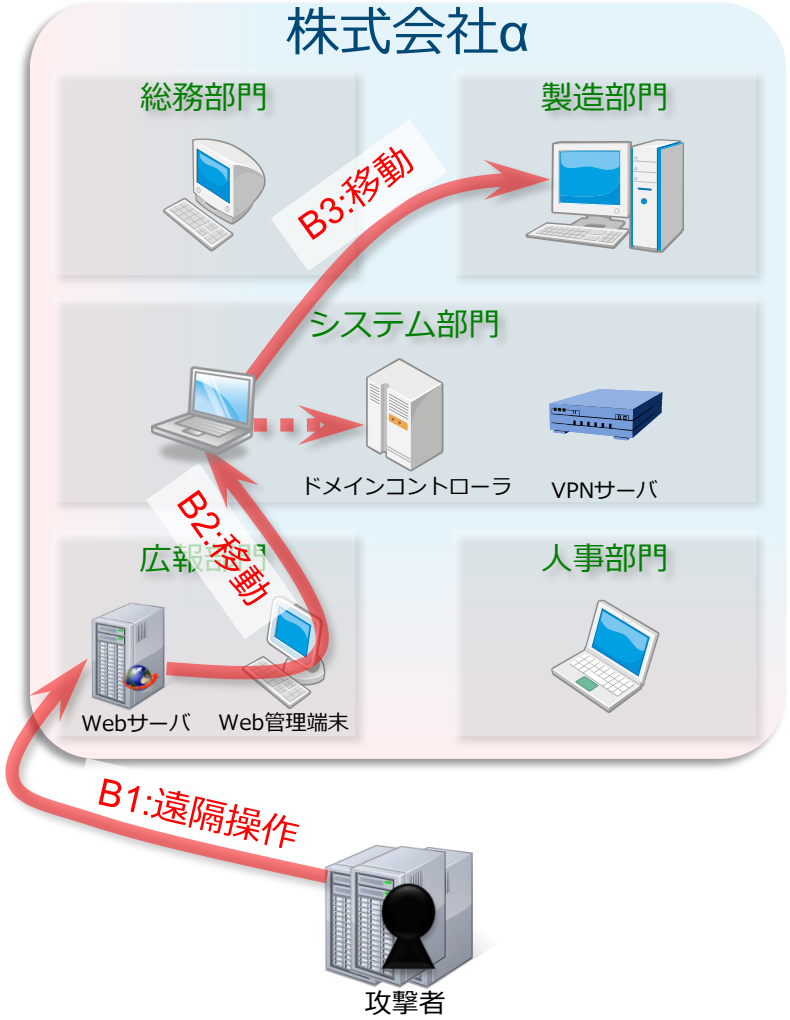


【αでの調査】

- 管理用PCとドメインコントローラに侵入されていたことが判明した。
- 管理用PCから不審なサイトに情報送信された痕跡があった。
- ファイアウオールでサイトへの通信をブロックした。
- 全アカウントのパスワードを変更した。

3週目：αからの情報提供（再侵入）

【再侵入の調査】
- ドメインコントローラへの侵入の試みを検知した。
- Webサーバから Web管理端末と管理用PCを経由して侵入を試みていた。
- 製造部門のPCにも侵入されていた。
- 前回の侵入時にWebサーバとWeb端末に裏口が設置されていた。



前回の侵入に対して
関係部門のみ
（総務とシステム）
で対応を進めていた

全社を対象に調査

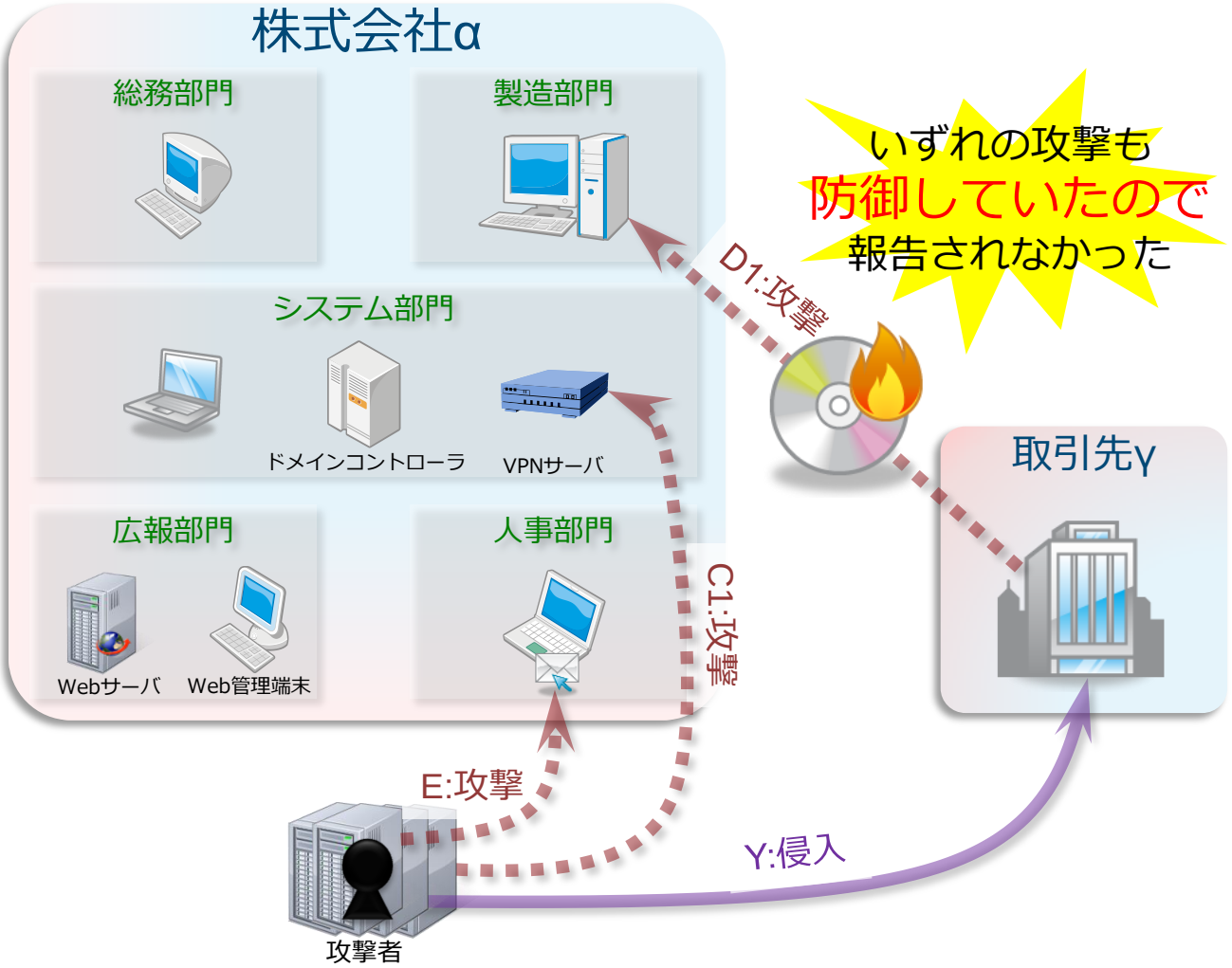
4週目：αからの情報提供（全社調査結果）

【人事部門】
先週から不審なメールが何通も届いている。

【システム部門】
先々週からVPNサーバへの不審な接続試みが続いている。

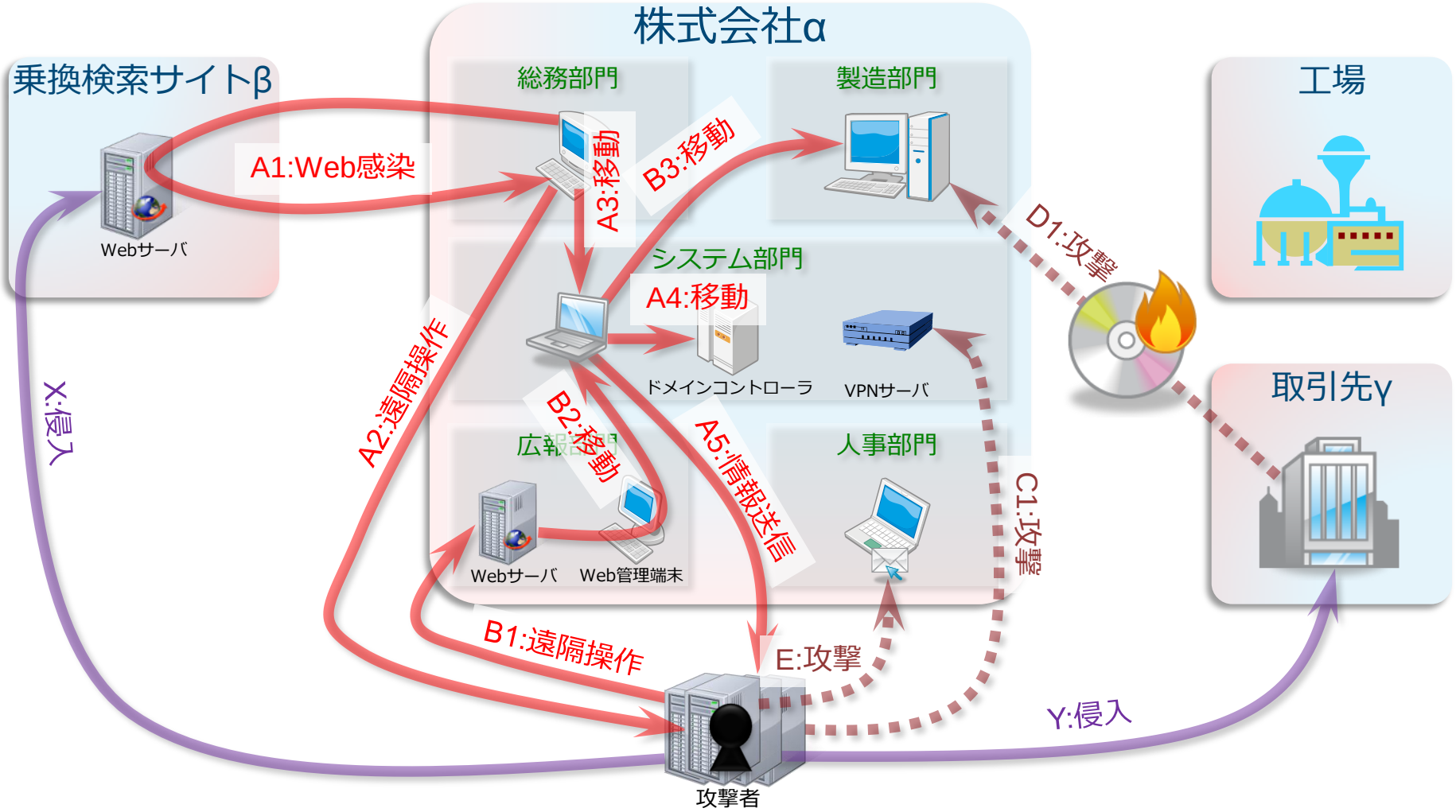
【製造部門】
先々週にマルウエアが混入したDVD-Rが届いていた。

【取引先γ】
6ヶ月前に外部から侵入されていた。



攻撃の全容

他組織も巻き込んで**様々な手段**で**次々**と攻めてくる…



インシデントへの対応

取組みから見た「二つの脅威」

使われる技術や手段には共通性もある
成果がやりとりされている可能性もある
でも、簡単に見分けられるとは限らない

- 直接的な被害をともなう
- 短期間で行われる
- 変化しながらも単純に繰り返される

- 被害がわかりにくい
- 必要に応じて長期間かけて行われる
- 様々な手段で継続的に繰り返される

守りを固めて排除する ⇔ 対応の違い ⇔ 観察して避ける

- インシデントへの対応 -

対応プロセス

マネージメントの積極的関与

外部との情報連携

外部からの情報で
インシデントが発覚する
ケースが多い

攻撃を特徴づける情報

ここが
最も重要

一般的に
ここが起点になる

外部と共有

準備 → **検知・分析** → 封じ込め → 根絶 → 修復 → 教訓

役立つのは…
- ✓通信ログ（ファイアウオール、プロキシ等: 内部⇒外部や内部⇒内部）
- ✓証跡データ（端末ログ、IT資産管理システム等）
- ✓IT資産管理情報

※ログ類は状況により6カ月～1年以上遡る

平常時の備え

有事における対応

侵入事例での対応を振り返る

- 早く全社調査していればWebサーバやWeb管理端末の裏口を発見・駆除できていたかもしれない。
- 全社調査が遅くなれば、再々侵入を許していたかもしれない。

再侵入を防ぐことはできなかったのか？

被害は何だったのか？
攻撃者の狙いは？

- ユーザや端末の情報以外にもデータを持ち出された可能性はあるが内容は特定できていない。
- 他の組織や工場が本来のターゲットだった可能性もある。

- 様々な手段で攻撃が繰り返される。
- 継続的に観察できることが対策に繋がる。

終息宣言は？

想定される被害は？

- 情報漏えい
  - 注目されるのは個人情報の漏えい
    - 「攻撃者はあらゆる情報に価値を見出す」と考えるべき
  - 盗まれた情報を完全に特定することはほぼ不可能
    - 全ての情報アクセスと全ての通信を記録する必要がある
    - 盗まれることを前提に情報を無効化するという考えも
- インフラの乗っ取り
  - サプライチェーンに対する攻撃の温床
    - 「自組織には盗まれて困る情報はない」という思い込み
  - 自爆的な攻撃
    - インフラを使って攻撃メールを派手にばらまく
    - 取引先やメディアへの対応に翻弄される
- 対応のために発生したコスト
  - サーバ・端末、ログ類の調査費用
  - サーバ・端末の調査・復旧にともなう業務停止

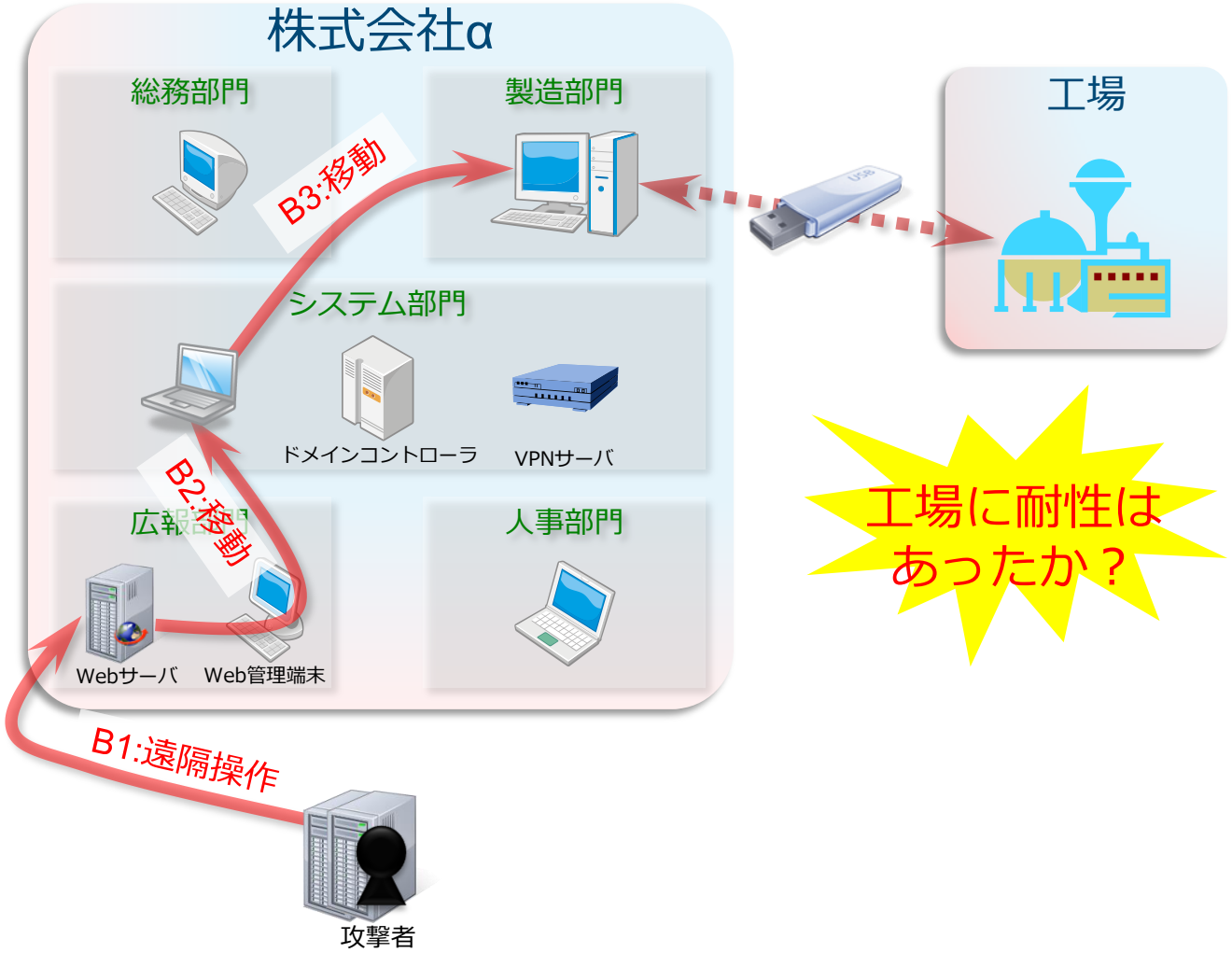
外部への情報発信時の焦点になりやすい問題

当事者になって初めて思い知らされる問題

発覚後に捻出しなければならない費用

もし工場がターゲットだったら…

【工場】
正常部門との間でUSBメモリを使ってデータのやりとりをしている。



脅威への対応と対策

事後対応

- 緊急対応体制の起動
  - 組織内の統制
  - 対応スケジュールの検討
- サーバ・端末やログ等の調査
  - 侵入経路や影響範囲の特定
  - クリーンナップ
- 外部への情報発信
  - 二次被害の危険性のある対象への注意喚起
  - メディア等への対応
  - セキュリティベンダ等への情報提供

ゼロからの対応は困難

事前対策

- 情報集約と情報連携の取組み
  - CSIRT機能の構築
  - 情報連携の取組みへの参加
- 攻撃との共存を意識した環境作り
  - セキュリティ教育・トレーニング
  - ログ設定のチューニング
  - メールのアーカイブ・検索
  - 次世代ファイアウォール等の導入検討
- 情報資産の把握・保護
  - ネットワークやシステムの構成把握
  - 保護すべき情報の洗い出し

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。