Deloitte.

高度標的型攻撃の対応事例と現状課題

近年の脅威から考えるサイバー攻撃対応策

デロイト トーマツ リスクサービス株式会社
マネジャー
デロイト トーマツ サイバーセキュリティ先端研究所
主任研究員
岩井 博樹

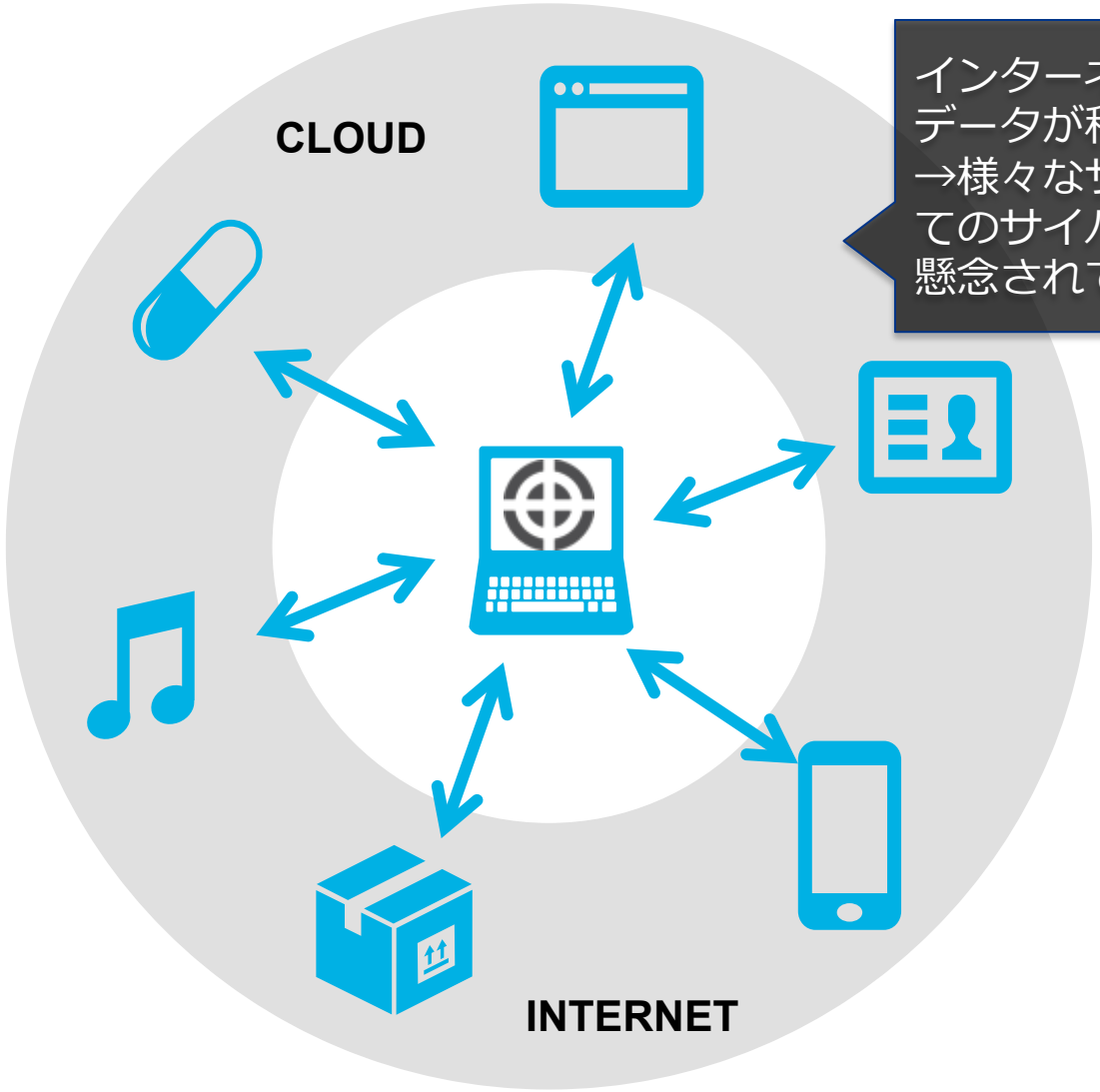
トーマツ.

本資料の意見に関する部分は私見であり、所属する法人の公式見解ではありません。

サイバー攻撃手法の変化

テクノロジーの変化と共の脅威も変化

データはインターネット上で管理することが一般的になった



インターネット上に様々なデータが移管されている。
→様々なサービスを利用してのサイバー攻撃の増大が懸念されている。

今年の標的型攻撃の特徴

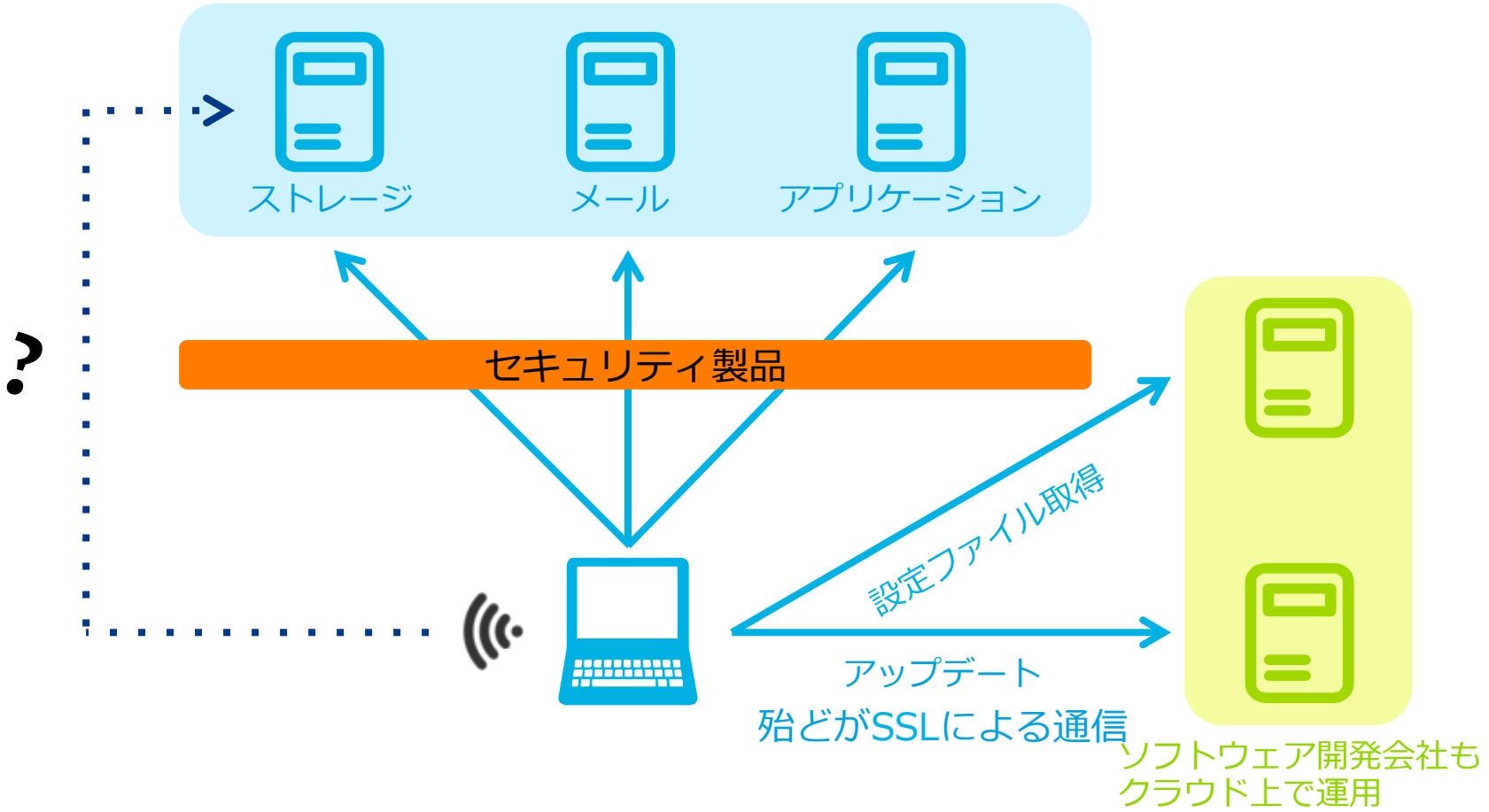
攻撃規模の絞り込みにより標的企業単体での検知は困難化

1. 侵入端末台数をより制限
2. 特定のセキュリティツールを回避
3. 攻撃期間は２、３日間と限定的

最近のサイバー攻撃を検知するためには初期段階での報告が重要度高

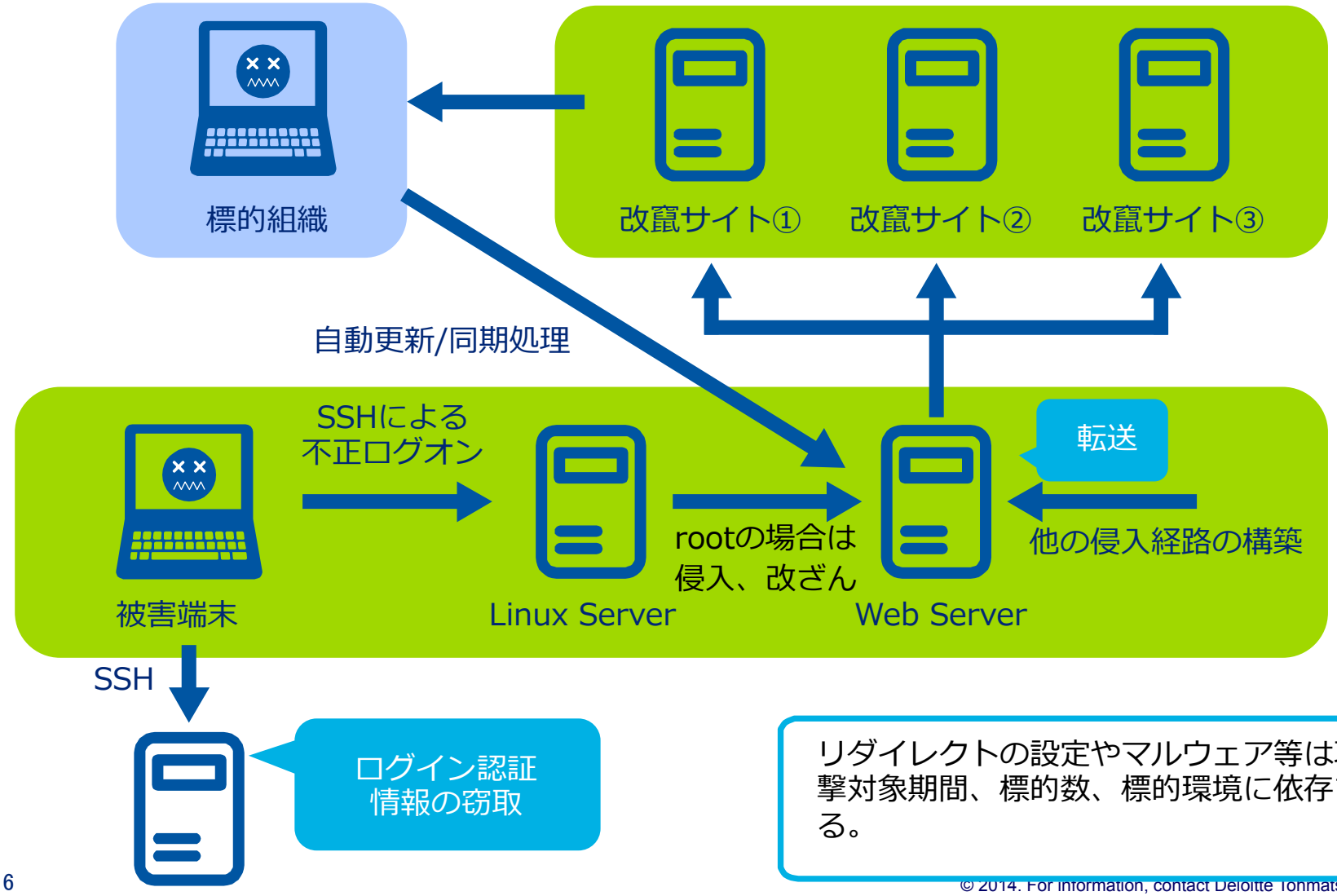
事例（Update Hijacking）

“自動アップデート”はクラウド環境を回避するには最適な機能



事例（Update Hijacking）

攻撃者は標的に対して能動的な行動はとっていないことが特徴



リダイレクトの設定やマルウェア等は攻撃対象期間、標的数、標的環境に依存する。

Update Hijackingの攻撃キャンペーン

時系列にみるキャンペーンの全容

※サンプルイメージです。

攻撃準備期間の手口の特徴

RATの開発とテスト期間

投影のみ

攻撃本番の手口の特徴

標的の複数組織への本攻撃は非常にシンプル

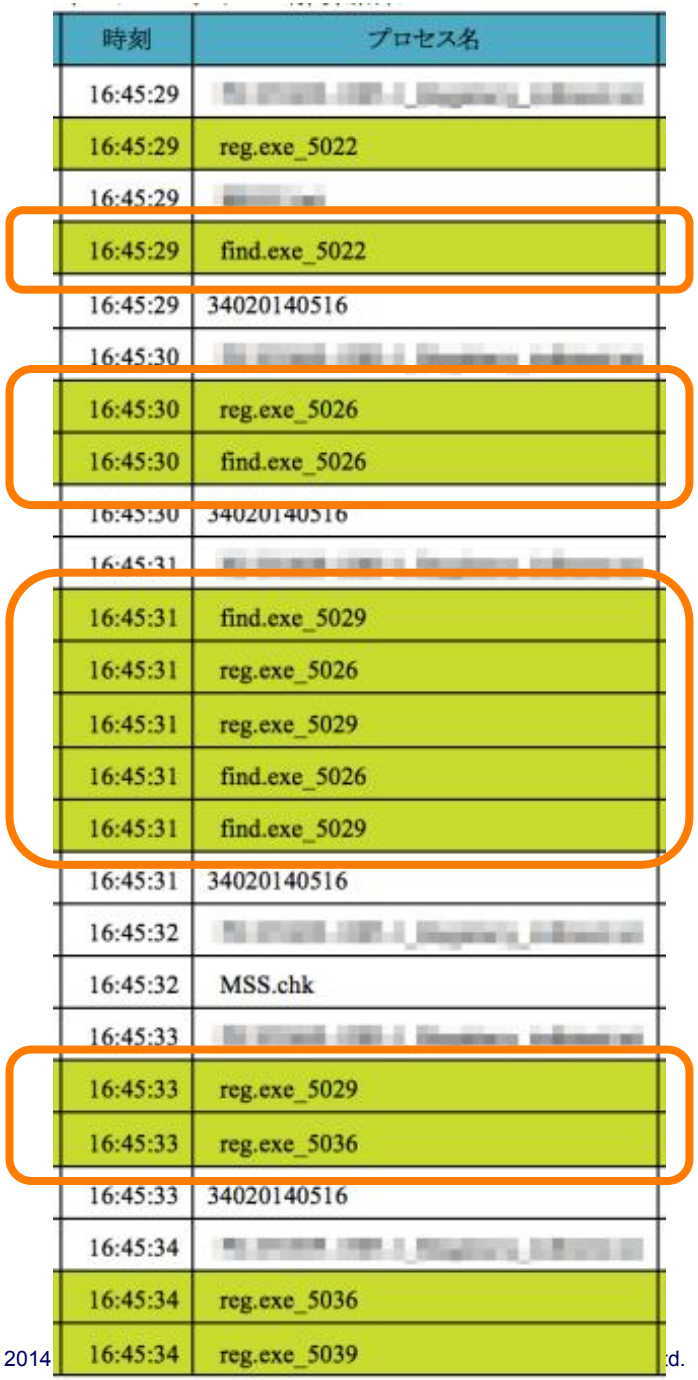
RAT	■ダウンローダー ■RAT 2 のみ（多少、汎用的な作りになっている）
リスクウェア	■利用した証跡は無し
ワークフォルダ	■C:¥Users¥ユーザ名¥AppData¥LocalLow¥Microsoft¥CryptnetUrlCache¥Content¥ （証明書のキャッシュフォルダ） ■C:¥Windows¥inf¥

＜参考＞攻撃者の狙いは特定情報の窃取

攻撃準備期間は探索行為を含んだ操作内容で繊細さ、注意深さが無い

・reg.exe , find.exe を多用
  - ジャーナルより連続で特定のプロセスが動作している ことを確認
・レジストリへの登録がサービス情報に追記のみで雑
・Rar.exeをリネームせずに利用（レジストリより）

不正プログラム駆除後のプロセスの状況
⇒　駆除に失敗している



時刻	プロセス名
16:45:29	[redacted]
16:45:29	reg.exe_5022
16:45:29	[redacted]
16:45:29	find.exe_5022
16:45:29	34020140516
16:45:30	[redacted]
16:45:30	reg.exe_5026
16:45:30	find.exe_5026
16:45:30	34020140516
16:45:31	[redacted]
16:45:31	find.exe_5029
16:45:31	reg.exe_5026
16:45:31	reg.exe_5029
16:45:31	find.exe_5026
16:45:31	find.exe_5029
16:45:31	34020140516
16:45:32	[redacted]
16:45:32	MSS.chk
16:45:33	[redacted]
16:45:33	reg.exe_5029
16:45:33	reg.exe_5036
16:45:33	34020140516
16:45:34	[redacted]
16:45:34	reg.exe_5036
16:45:34	reg.exe_5039

＜参考＞攻撃者の操作の差分

攻撃本番時の操作は効率的、且つ巧妙であり証跡

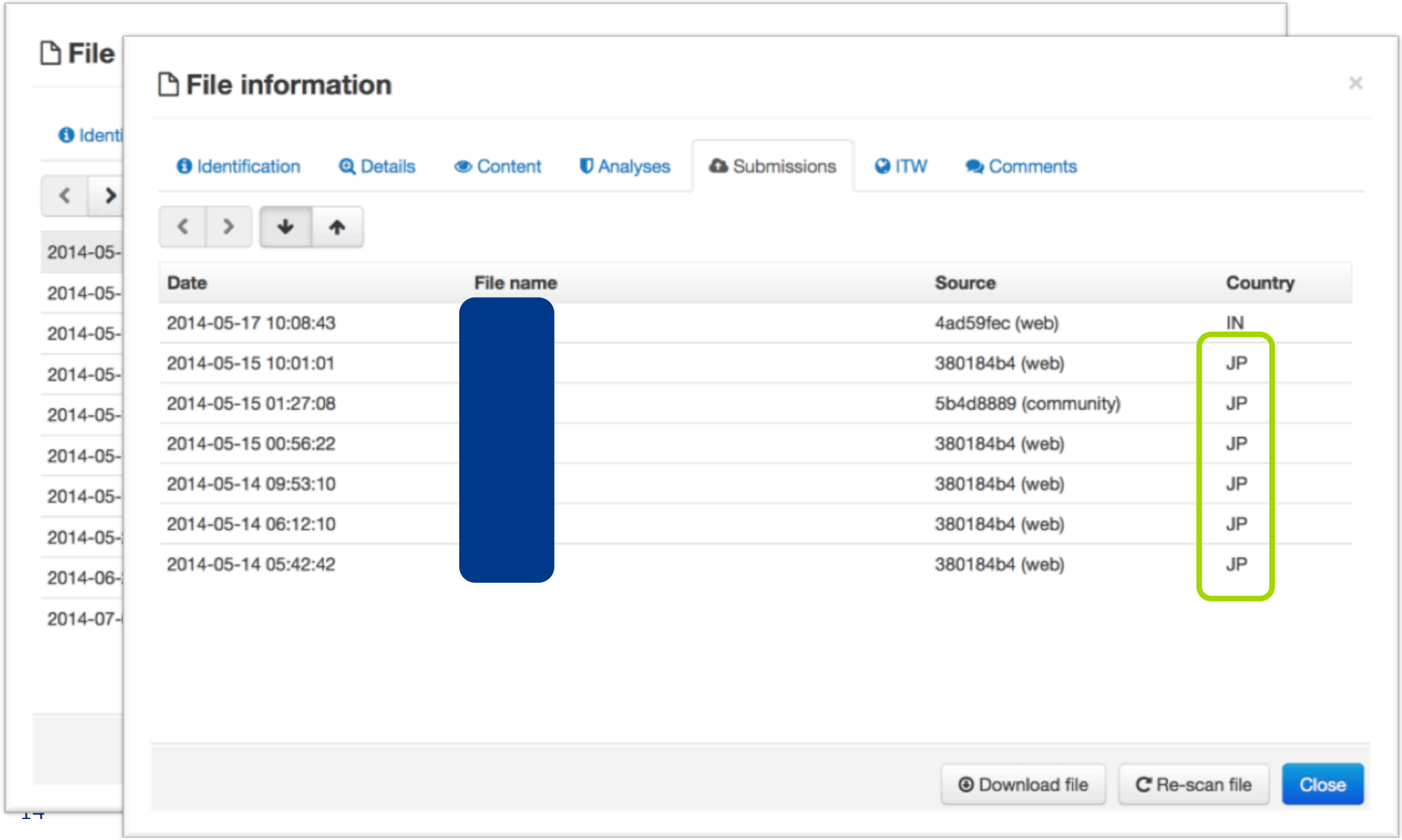
投影のみ

攻撃者の侵入後の操作の分析

攻撃本番時は計画性が高くインシデントの検出が難しい！？

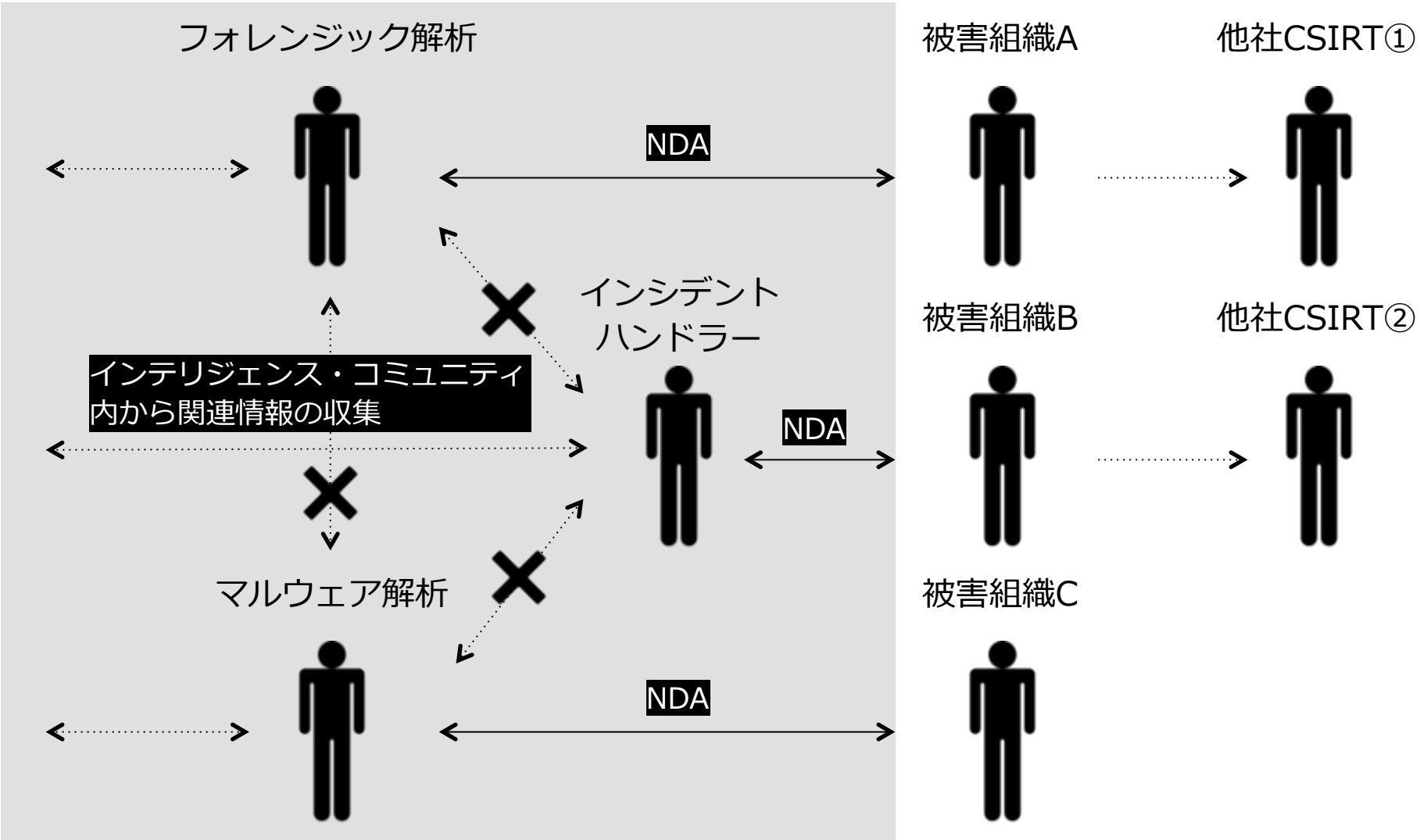
投影のみ

＜参考＞最終的に利用されたマルウェアの検出状況の推移



脅威の初期情報の共有が被害拡大防止に役立つのだが・・・

各被害箇所でのインテリジェンスが分断されていることが課題



今どきの対策の考え方

現状のセキュリティ対策の実装確認

NIST Cybersecurity Framework による質問例

【特定】資産の洗い出しは、
[redacted]を利用して実施している。

【防御】業務端末上の情報保護のため、
[redacted]の不正な変更を検知するためのツールを導入している。

【検知】社内からの監視は、
「IDS/IPS」「アプリケーションファイアウォール」「マルウェア対策製品」により**アプリケーションやマルウェアによる通信**を監視している。

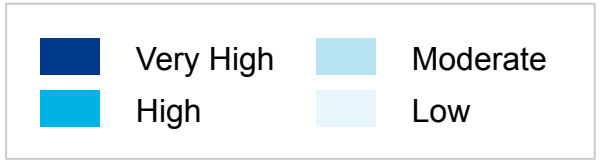
【対応】インシデント対応手順は、
フォレンジックを前提に、[redacted]についても記載がある。

【回復】組織内において定期的に、
インシデント対応から[redacted]を実施している。

※Cybersecurity Frameworkを参考に筆者が作成
Cybersecurity Framework：http://www.nist.gov/cyberframework/

仮想敵の設定をする

業種毎に仮想敵とインパクトは異なる



インパクト / 攻撃者	金銭窃取 / 詐欺	IPや戦略計画等の窃取	事業継続の不可	インフラ基盤破壊	風評被害	人命に関わる脅威	取締（当局）
組織犯罪							
ハクティビスト							
特定国家							
内部者							
ライバル企業							
ハッカー（個人）							

不正送金等を含む

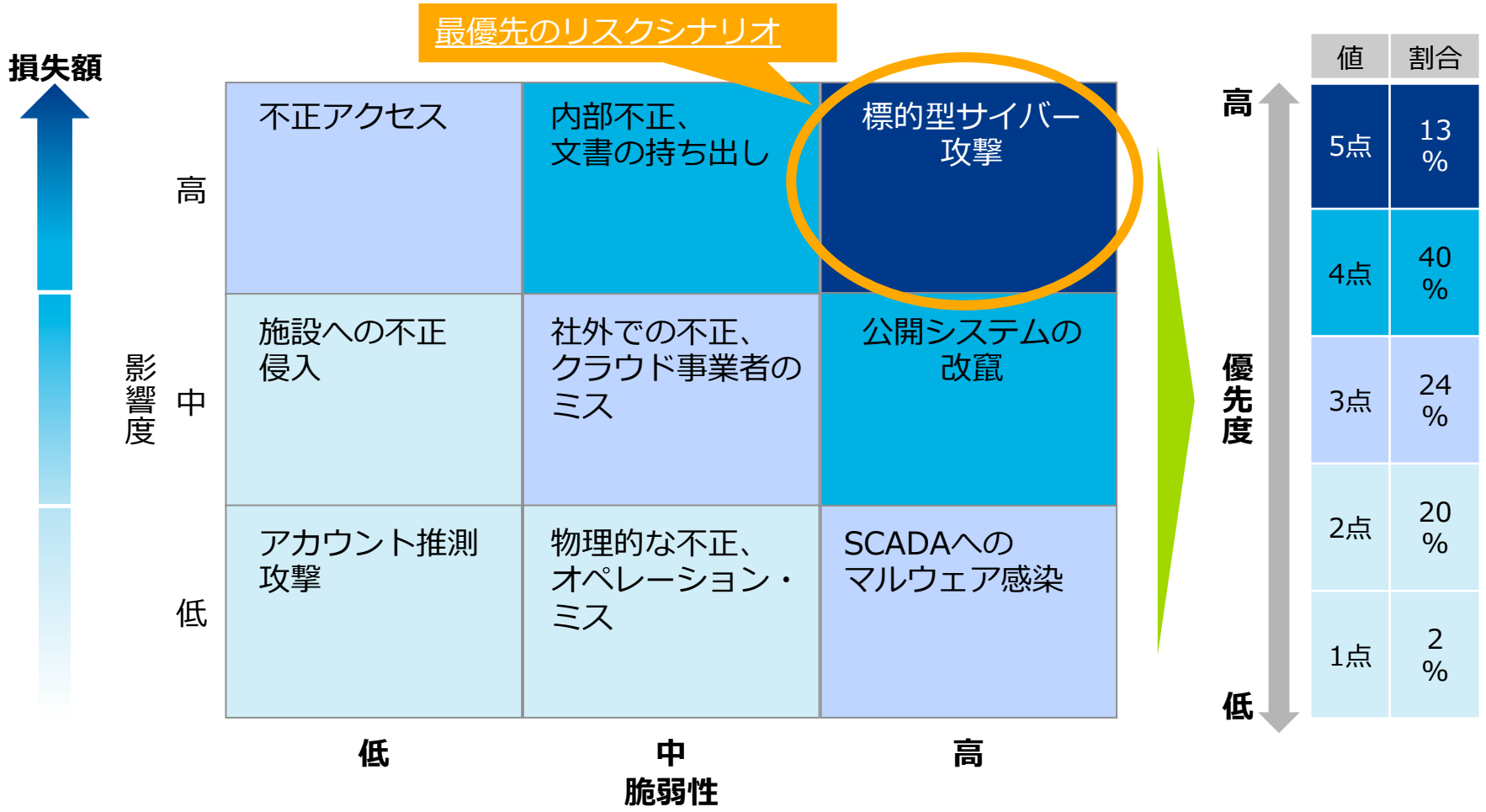
DoS攻撃等

韓国事案のようなケースを想定

9.18のDoS等

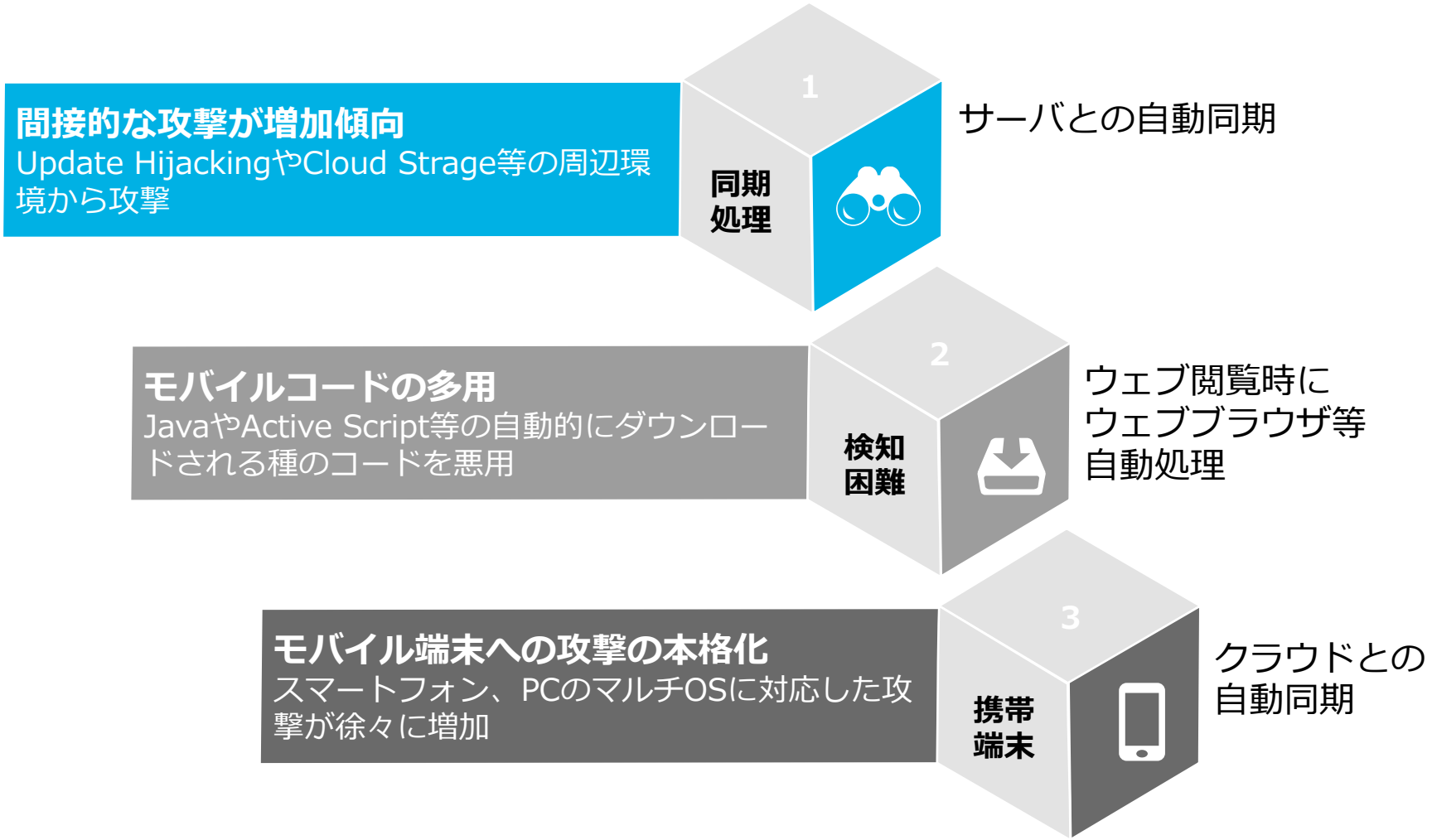
対策優先度の高いリスクを把握していますか？

企業毎に優先度の高いリスクは異なる



近年の攻撃内容の変化は主に３つ

“勝手に”動作する仕組みが悪用傾向にある



間接的な攻撃が増加傾向
Update HijackingやCloud Strage等の周辺環境から攻撃

モバイルコードの多用
JavaやActive Script等の自動的にダウンロードされる種のコードを悪用

モバイル端末への攻撃の本格化
スマートフォン、PCのマルチOSに対応した攻撃が徐々に増加

対策ツールの有効性は50/50

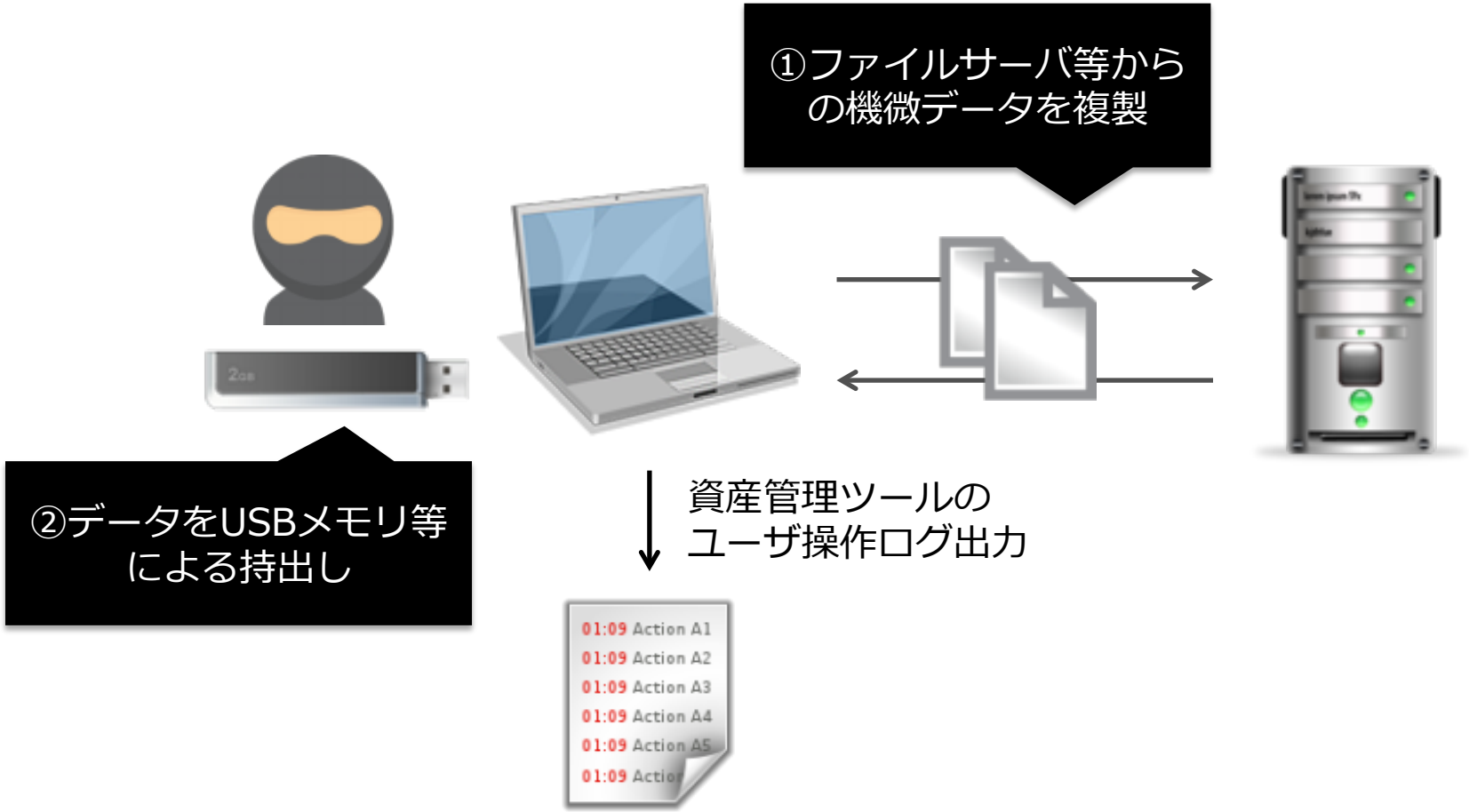
多層防御実装の有効性と運用における費用対効果のバランスを考える

対策項目	対応システム	課題キーワード
不正通信の検出	IDS，IPS，NGF	シグネチャ運用, 暗号通信
情報流出の検出	DLP	シグネチャ運用, 暗号通信
レイヤー7の監視	NGF	独自プロトコル
SSLの監視	NGF	ハードウェアのスペック
マルウェアの監視	NGF，MPS，AV	サンドボックス
ホストの監視	HIPS，AV	プロセス監視
モバイルコード	IDS，IPS，AV，NGF	JAVA, SWF, VBS

IDS：侵入検知システム
IPS：侵入防止システム
DLP: データ流出緩和システム
MPS：マルウェア防御システム
AV：アンチウイルスゲートウェイもしくはアンチウイルスソフト
NGF：アプリケーション層（レイヤー7）の監視が可能なセキュリティ製品

＜参考＞選ぶならどっち？

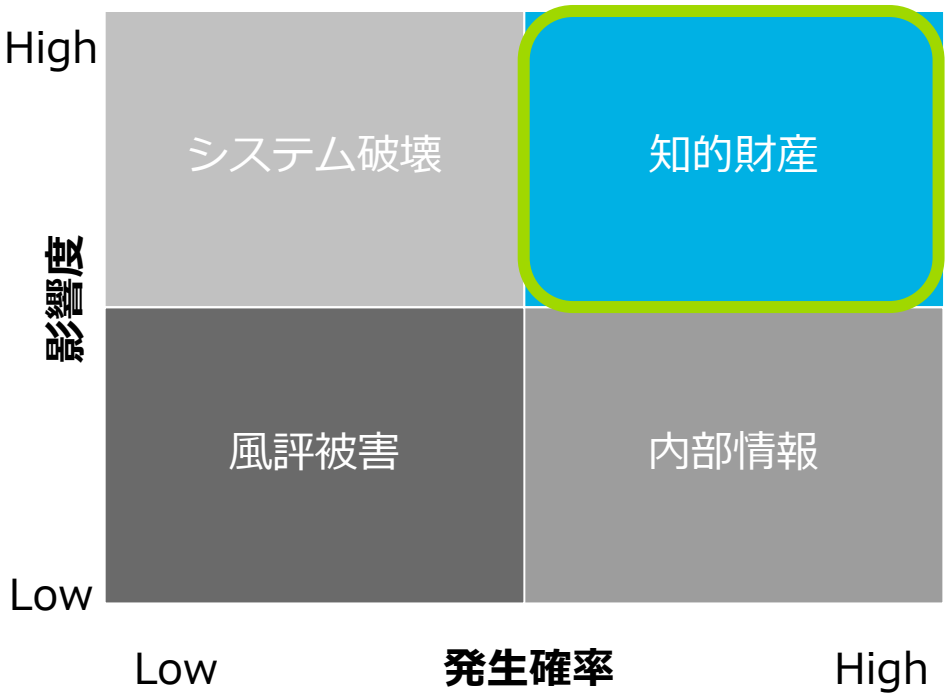
公判を見据えた製品を選択した方が良い



サイバー攻撃を前提に考えた場合の防御優先度

攻撃者目線と防御者目線は似て非なるもの

仮想敵は海外ライバル企業と仮定して考えた場合：



Q: 何を守るのが効率が良いか？

1) ファイルサーバ上のデータ
2) 従業員PC内のデータ
3) メールサーバ上のデータ
4) 従業員の頭の中
5) 役員PC内のデータ

今後気にしておきたいサービス

利用せざるを得ないサービスが攻撃の標的になる可能性が高い

実施しておきたいセキュリティ対策例

重要なのは被害検出と初動対応によるダメージコントロール

確認しておきたい項目

- クライアントPCのモニタリング強化
- アプリケーション・ファイアウォールの運用
- 外部への不正通信の監視補強
- インシデント対応手順の見直し

インシデント対応手順の見直し例

従来型のインシデント対応方法では対応が困難であるため見直しが必要

Step4. ネットワークログの収集
プロキシやセキュリティ機器等のログを収集

Step3. モバイル端末への初動対応
モバイル端末とデータを同期している可能性がある

Step2. 初期調査（特にメモリダンプ未取得時は重要）
端末が起動中の場合は接続先のサーバが調べられる場合は調べておく。

Step1. 初動対応（メモリダンプ, HDD物理コピー）
データがクラウド上に設置されている可能性があるため、全てが端末上で完結することは無い。

まとめ

企業毎に優先度の高いリスクは異なってくる

“自動処理”されているものは注意する

- 同期処理やクラウドはその代表格

セキュリティ対策には優先順位がある

- まずは最悪のケースを想定しての対策が重要

インシデント対応手順は見直し時期である

- セキュリティ・ベースラインを見直すことで全体のセキュリティ対策のバランスを調整

Deloitte. トーマツ.

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザリー株式会社および税理士法人トーマツを含む）の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約7,600名の専門家（公認会計士、税理士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト（www.tohmatsu.com）をご覧ください。

Deloitte（デロイト）は監査、税務、コンサルティングおよびファイナンシャル アドバイザリーサービスをさまざまな業種にわたる上場・非上場クライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約200,000名を超える人材は、“standard of excellence”となることを目指しています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.tohmatsu.com/deloitte/ をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

有限責任監査法人トーマツ 東京事務所 エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited