Câmara de Comércio e Indústria Japonesa no Brasil

運輸サービス部会主催

IT Seminar 2017

第一部：キーワードで解説する企業の「デジタル・トランスフォーメーション」

第二部：経営視点から考える日本企業の情報セキュリティ

第三部：IoT（Internet of Things：モノのインターネット）最新動向と導入事例

グローバル経営における
リスクマネジメント
～サイバー攻撃への耐性をもつ組織やICTとは～

2017年10月19日

NTTコミュニケーションズ株式会社
セキュリティエバンジェリスト
経営企画部　MSS推進室
室長　竹内文孝　CISSP

講師のご紹介

NTT Communications
Transform. Transcend.

- **竹内　文孝（たけうち ふみたか）**
- **NTTコミュニケーションズ株式会社**
- **経営企画部　マネージドセキュリティサービス推進室　室長**
- **セキュリティ・エバンジェリスト**

＜来歴＞
2001年　NTTコミュニケーションズ（NTTコム）で、
　　ウイルス対策サービスを開発し、
　その運用に従事
2003年　NTTコム直営のセキュリティオペレーションセンターを設立し、
　その運営、およびNTTコムのセキュリティ事業全般に従事
2009年　INTEGRALIS社のPMIプロジェクトに参画
2012年　NTTコムグループの世界共通MSSメニューを開発
2013年　NTTコムセキュリティ株式会社　代表取締役社長に就任
　　NTTコムグループの新セキュリティブランド『WideAngle』のサービス開発に従事
2016年8月1日　現職

●主な担当分野：セキュリティ
●主な講演：
・一般社団法人日本新聞協会向けプライベートセミナー
　「御社の標的型サイバー攻撃の対策レベルは？～実現可能な対応策の次の一手を考える～」
・電気三学会関西支部 専門講習会
　「進化する標的型サイバー攻撃と闘うための対策とは」
・Gartner Security & Risk Management Summit 2016
　「サイバー攻撃に強いサステイナブルな組織・ICTの再構築ステップ」
●主な執筆活動：
　地銀協月報「企業を取り巻くサイバー攻撃の脅威と対策」

本日お話したい内容

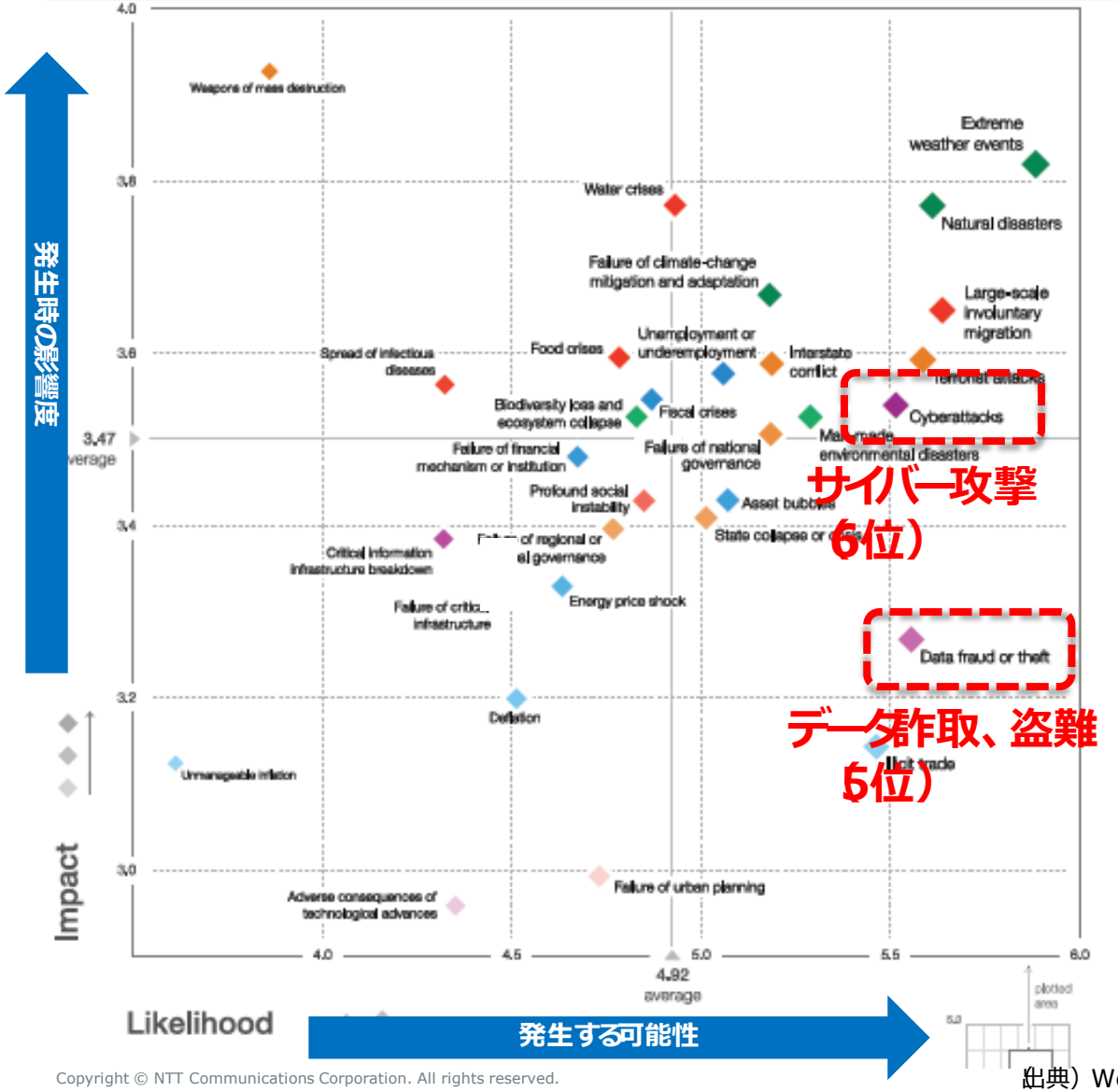
1. ネット社会の現状リスクと対策方針

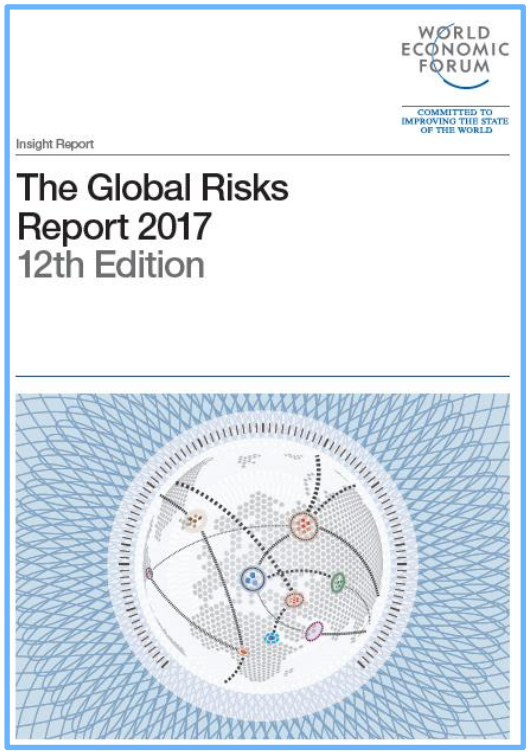
2. 他人事ではない！セキュリティ事故の実態

3. 持続可能なリスクマネジメント体制とは

セキュリティ対策はグローバル共通課題に

「サイバー攻撃」や「重要情報インフラの故障」は重大な悪影響を及ぼす可能性が高いリスクに！！





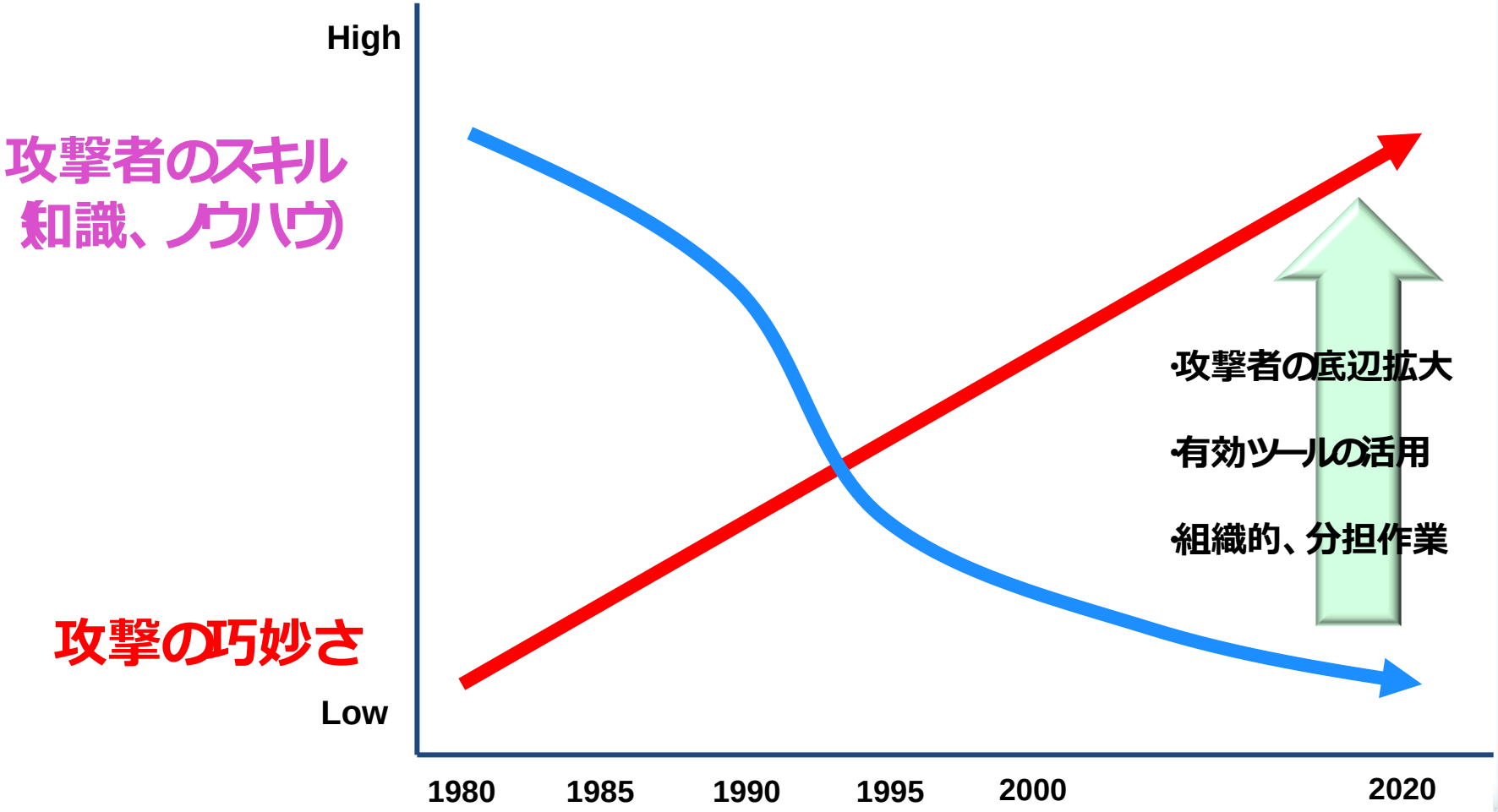
■2017年は30リスク（経済：9、環境：5、地政学：6、社会：6、技術：4）が評価対象。

■注目すべきリスクは、異常気象、自然災害、大規模な移民、テロ、サイバー攻撃、水資源危機、気候変動対応。

（出典）World Economic Forum 「Global Risks 2017」

サイバー空間における攻撃者側の動向

攻撃者のスキル（ ）but ツールによる攻撃の巧妙さ（ ）

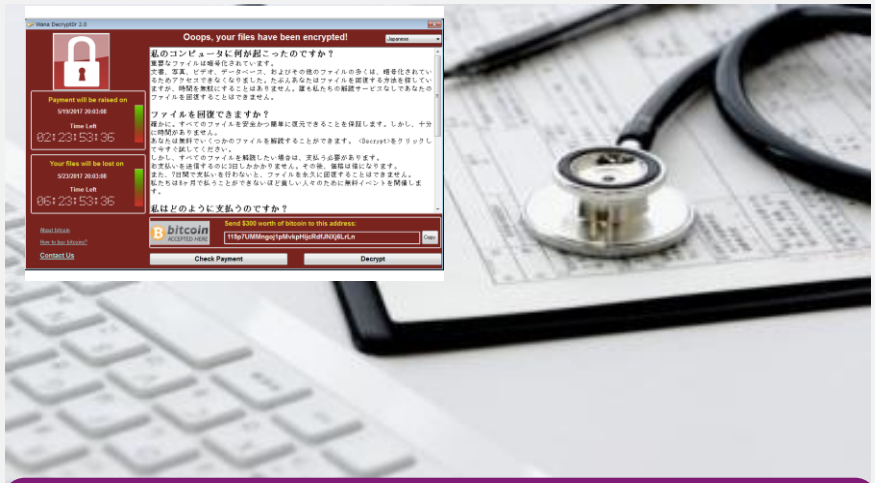


社会インフラに対する事故事例（海外報道ベース）

SF地下鉄システムハッキング
2016年11月 :2日間システム停止 :運賃無料

コネクテッドカーを遠隔操作
2015年7月 :クライスラー社が約140万台を自主的リコール。

マルウェア感染等による大規模停電
2015年12月 :ウクライナで6時間の停電



WannaCryが世界的規模で感染
2017年5月 :病院が感染し診察や治療に影響

インターネットに繋がってなくても安心できない

日本の情報漏えい事件インシデント（2016年1月-2017年3月）

業種	企業名	漏えい件数	漏えい日	タイプ	漏えい元
旅行	JTB	7,930,000	2016/4/13	個人情報	悪意のある部外者
教育	佐賀県教育委員会	210,000	2016/6/8	個人情報	悪意のある部外者
物販	資生堂/イブサ	420,000	2016/12/3	金融情報	悪意のある部外者
物販	YJFX（Yahoo Forex）	185,626	2016/1/28	個人情報	悪意のある部外者
物販	江崎グリコ ネットショップ	83,194	2016/1/29	個人情報	悪意のある部外者
物販	カゴヤ	48,865	2016/9/20	個人情報	悪意のある部外者
教育	富山大学	1,492	2016/10/10	機密情報	悪意のある部外者
金融	スタンダード銀行	1,600	2016/5/15	金融情報	悪意のある部外者
金融	日本経済新聞	100	2016/11/30	アカウント情報	悪意のある部外者
政府	防衛庁/自衛隊	不明	2016/11/5	機密情報	悪意のある部外者
金融	南アフリカスタンダード銀行	不明	2016/5/25	金融情報	悪意のある部外者
その他	秋吉台サファリランド	不明	2016/3/19	アカウント情報	悪意のある部外者
自治体	静岡県湖西市	1,992	2017/2/16	個人情報	誤送信
病院	北里大学東病院	1,917	2017/1/23	個人情報	紛失
物販	JINS オンラインショップ	1,188,355	2017/3/22	個人情報	悪意のある部外者
金融	GMO ペイメントゲートウェイ	719,830	2017/3/9	金融情報	悪意のある部外者
サービス	日本郵便（国際郵便マイページ）	29,116	2017/3/13	個人情報	悪意のある部外者
金融	B.LEAGUE（ぴあ）	155,000	2017/3/17	金融情報	悪意のある部外者
物販	東商マート	49,468	2017/3/31	金融情報	悪意のある部外者

出所）EnterpriseZine，ジェムアルト社発表 2017年6月2日などから作成

ネット社会で加害者になるリスク

『我が社の公開サイトは大丈夫ですよ』
●機密情報や個人情報は無いし・・・
●ダウンしても業務影響は無いよ・・・

標的となる
公開サイト

被害者

公開サイト

改ざん

攻撃サイトへ
の誘導

不特定の
被害者

機密情報

攻撃者

被害者から加害者へ

企業価値の低迷

サイバーセキュリティは 国家戦略」としての認識の高まり

2014年11月 サイバーセキュリティ基本法の成立

2015年 9月 サイバーセキュリティ戦略の策定

2015年12月 サイバーセキュリティ経営ガイドライン 初版策定

2016年12月 サイバーセキュリティ経営ガイドラインVer1.1策定

改訂ポイントは一つ!!

「セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい」

「経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である」

2020年、その後に向けた基盤形成 ・更なる強化へ

出典）サイバーセキュリティ戦略 平成27年9月4日）より

サイバーセキュリティのパラダイムシフト!!

ITマネジメント

リスクマネジメント

グループ経営を守るリスクマネジメントとは・・・

- リスク低減：グループ経営のICT環境をシンプルに見直し明確化
- リスク管理：未知のリスクを想定した改善サイクル（PDCA）の確立
- 異常察知力：事故の前兆や挙動を監視および分析する運用体制の確立
- 事業回復力：事実把握と影響特定を迅速的確に行う実行力の体制化
- 組織的予防：被害最小化のためのインテリジェンスの共有と連携防御

本日お話したい内容

1. ネット社会の現状リスクと対策方針

2. 他人事ではない！セキュリティ事故の実態

3. 持続可能なリスクマネジメント体制とは

身近な職場環境で何が起きているのか・・・

不平不満

不注意

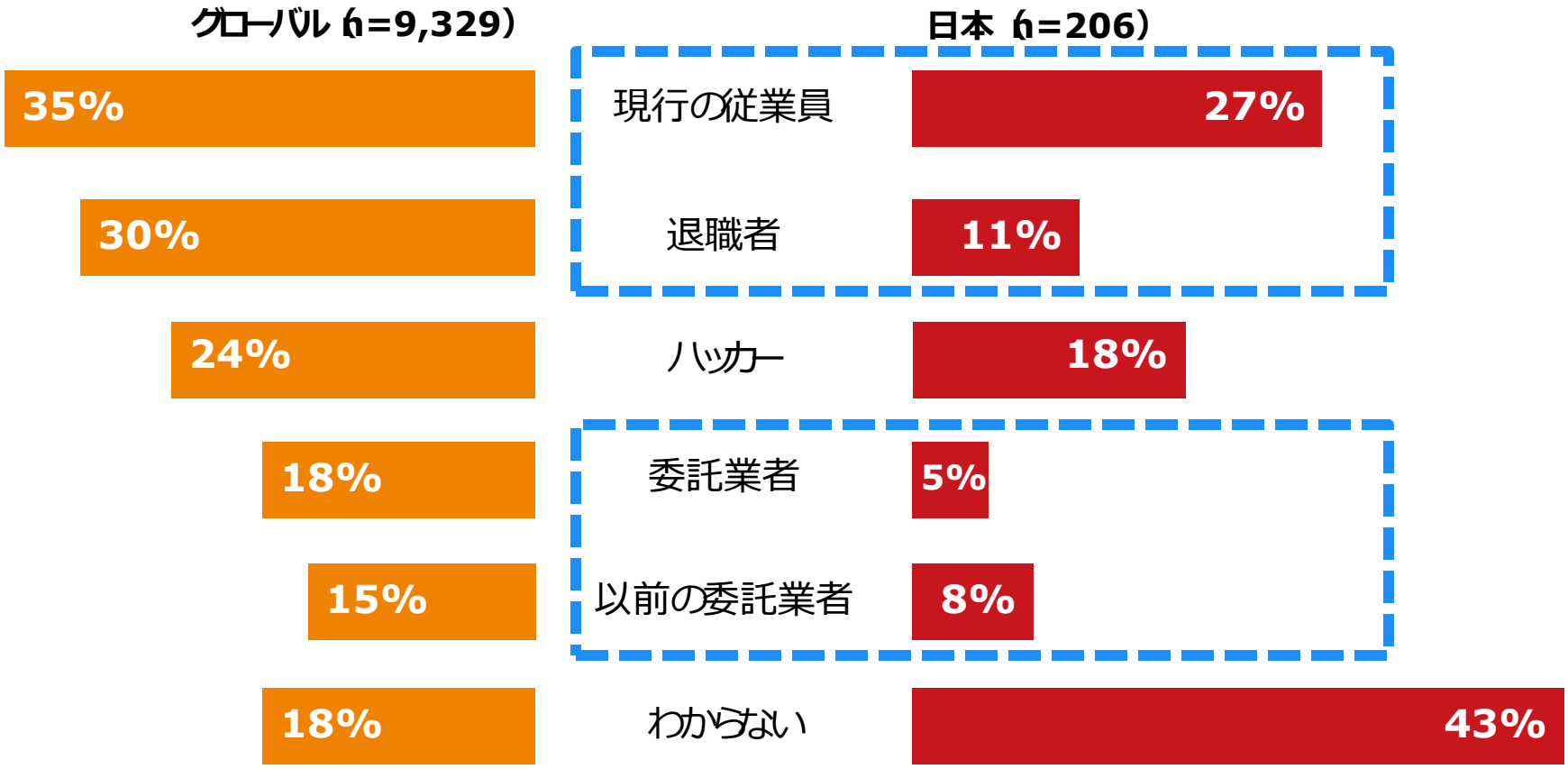
出来心

だまされた!?

セキュリティ事故を前提とした回復力の高いICT環境とは・・・

企業や団体等におけるセキュリティ事故の原因

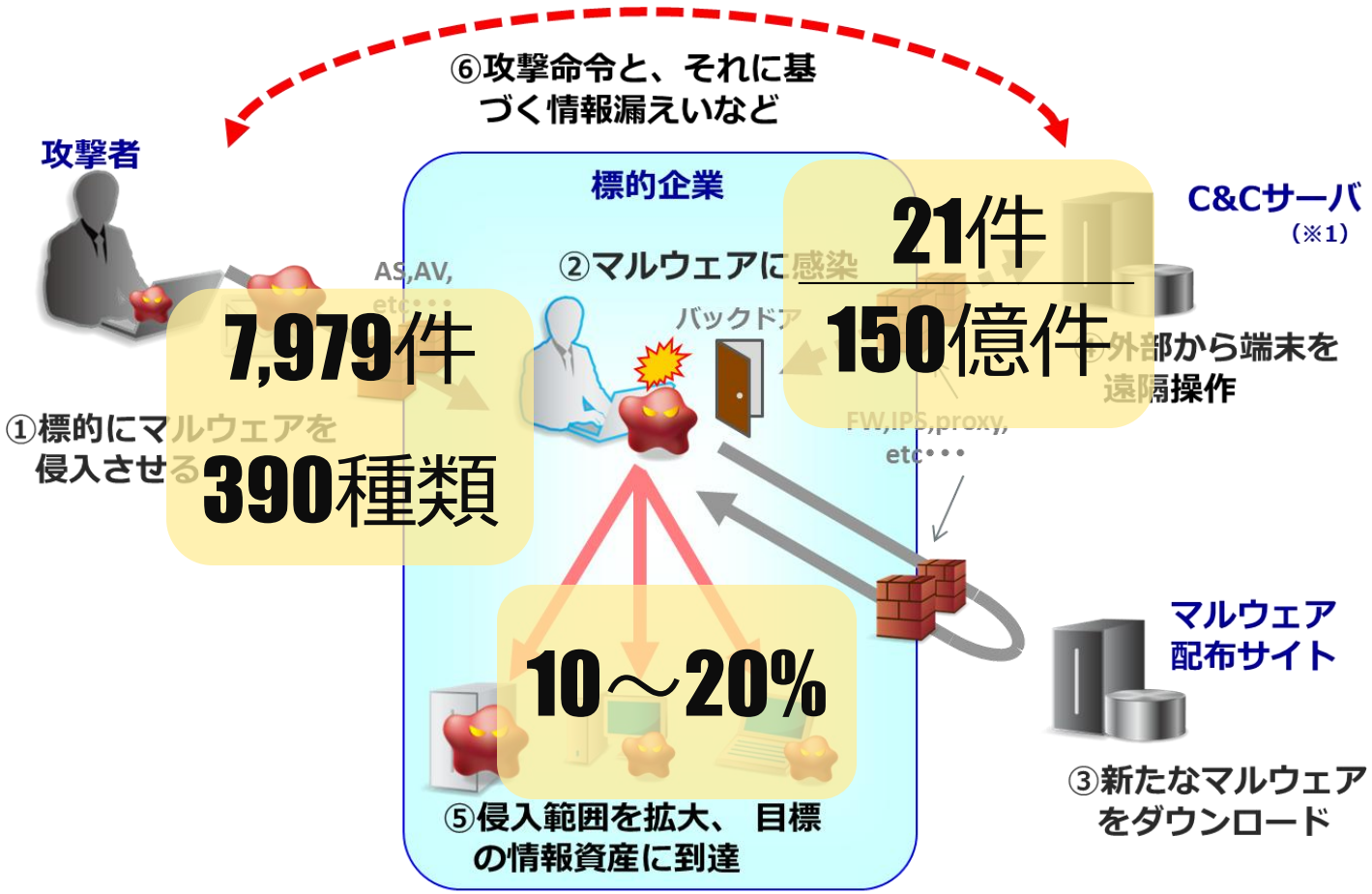
内部関係者が51% ⇒ 内部不正は経営責任



出典：PwC「相互につながった世界におけるサイバーリスクマネジメント グローバル情報セキュリティ調査2015」）

MSS事業者の現場から見える4つの事実

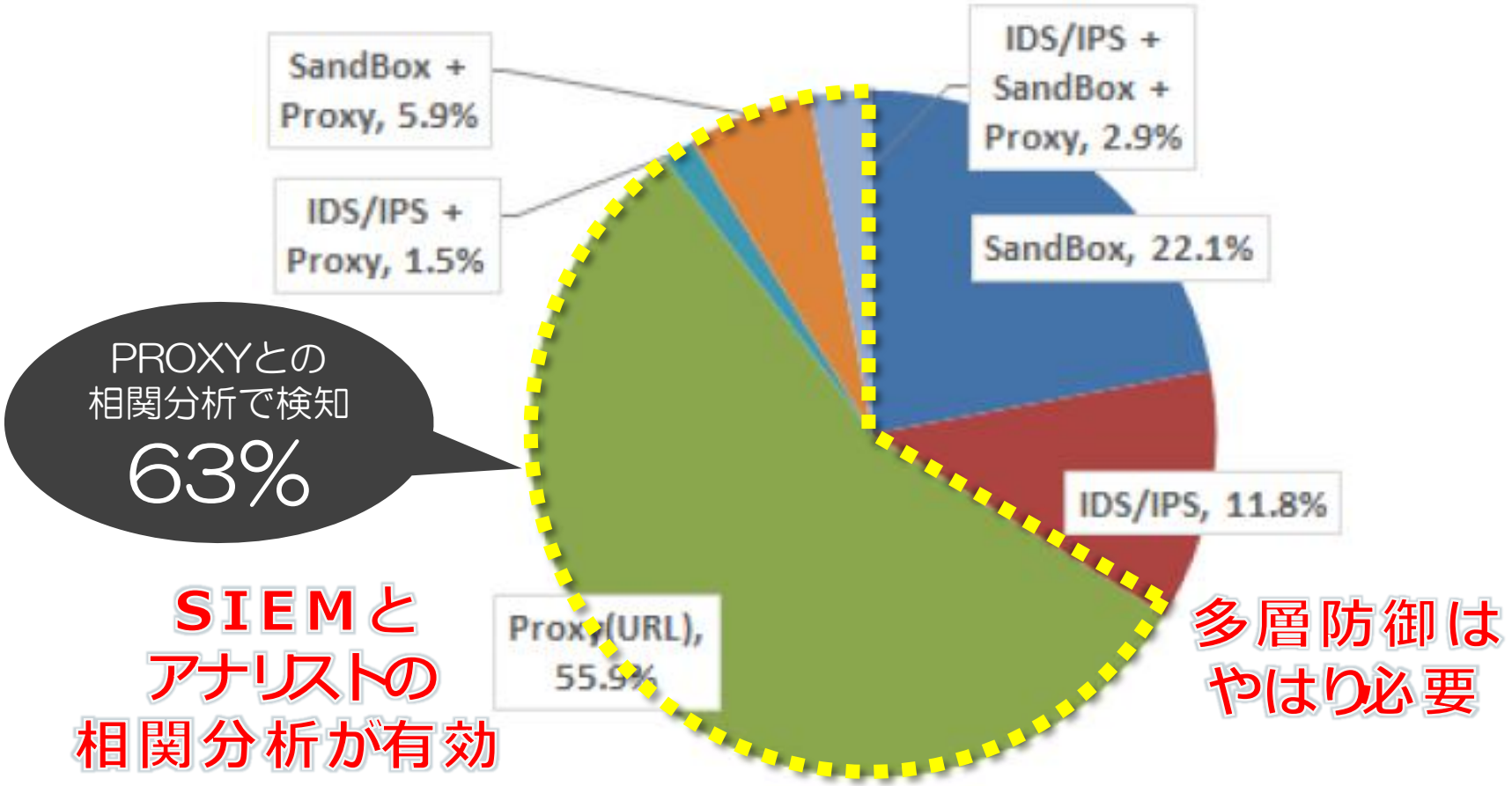
1 ウイルスは入口をすり抜ける・・・！？
出口で不正を可視化するのは至難の業！！



MSS事業者の現場から見える4つの事実

2

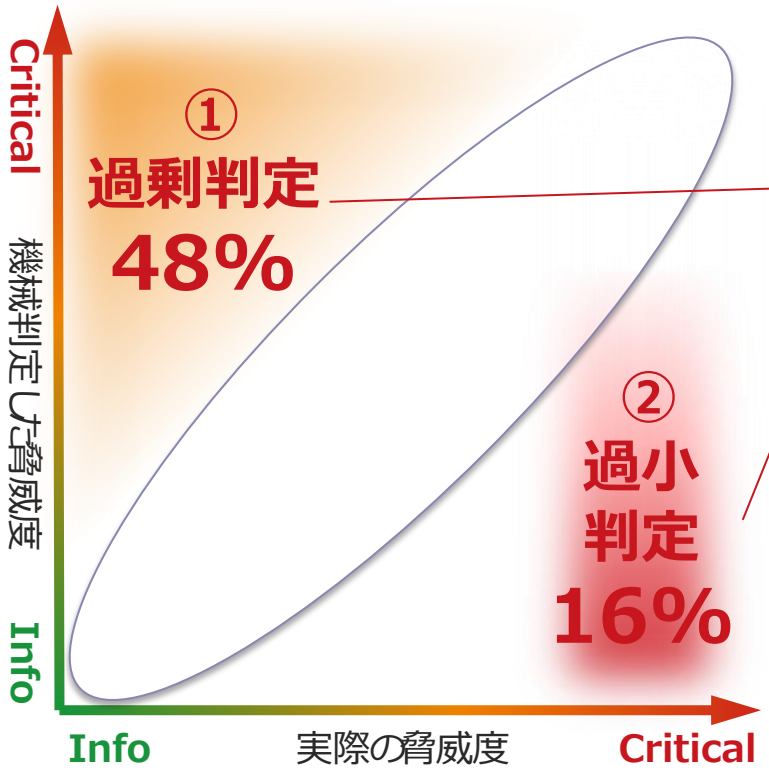
セキュリティ機器1機種が検知した真の脅威イベントは30%以下？



※相関分析サービスご利用中のお客様13社における2016年4月～2017年3月の観測結果

MSS事業者の現場から見える4つの事実

3 セキュリティ機器の危険度判定は
48%が過剰判定、16%が過小判定



①全体的に過剰判定の傾向

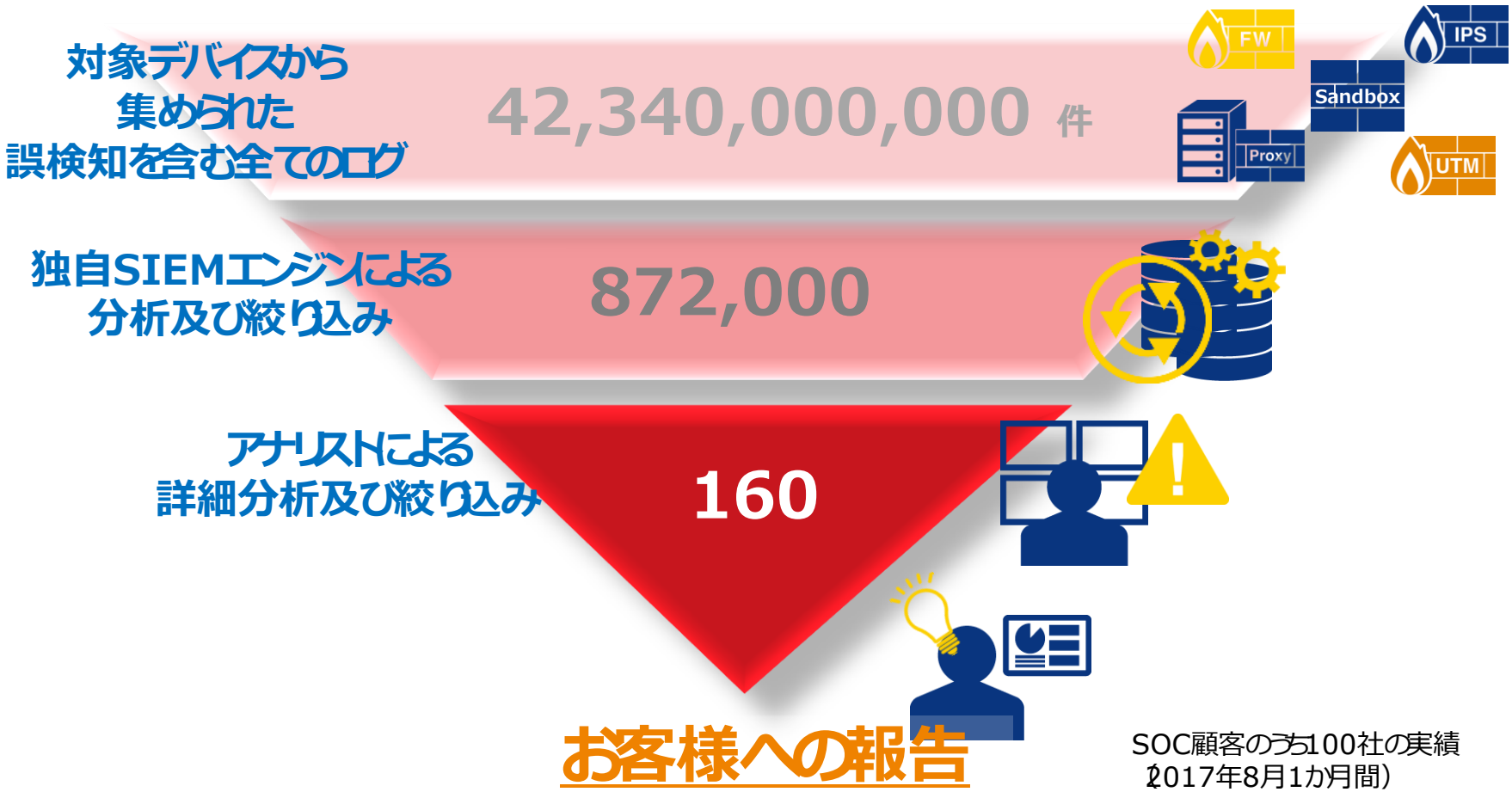
不必要に迫られる無駄な対応

②アラートの16%は見逃し?

セキュリティインシデントの見逃しのリスクが内在するため, Infoレベルのアラートまで調査する必要がある

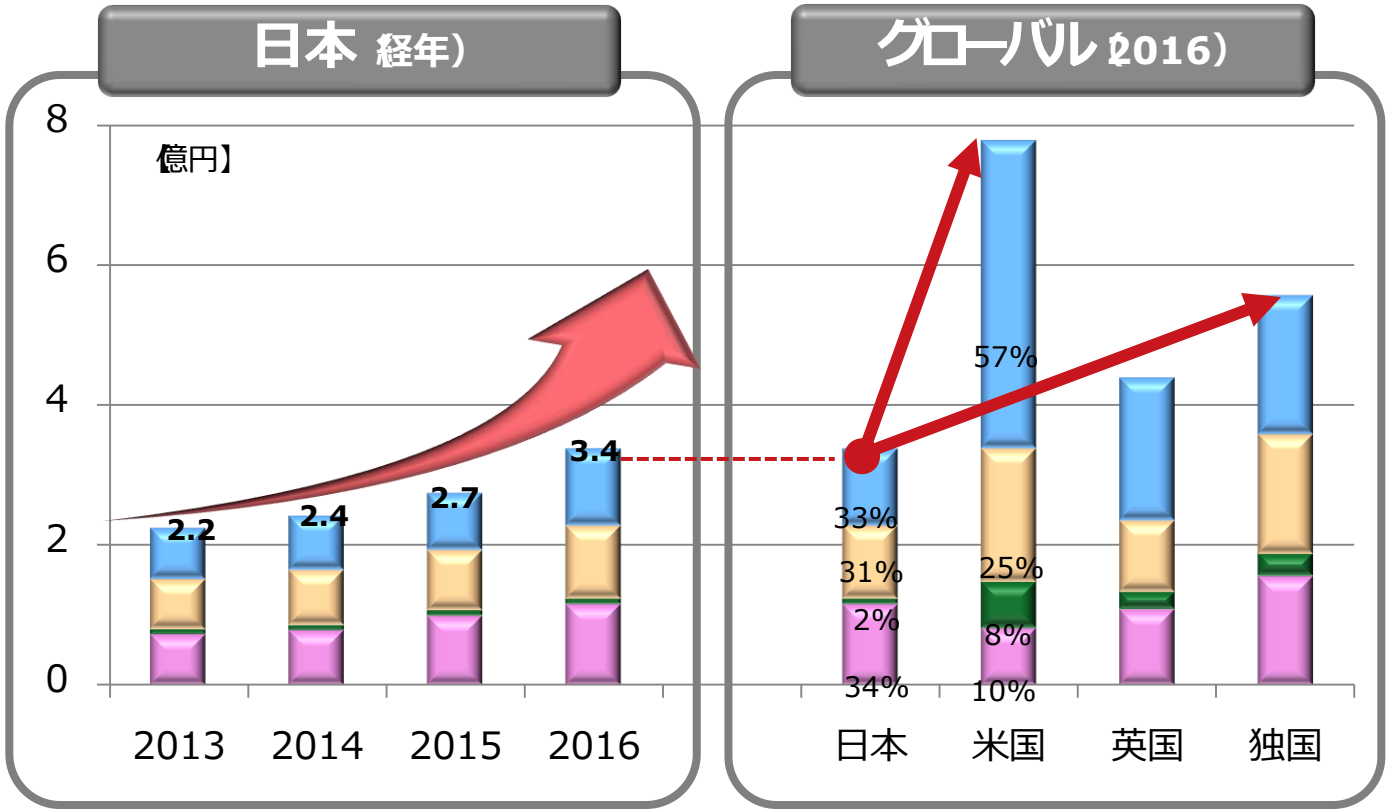
MSS事業者の現場から見える4つの事実

4 「独自SIEM＋アナリスト」による相関分析により 423億件の証跡から160件の真の脅威を絞り込み



SOC顧客のうち100社の実績
（2017年8月1か月間）

情報漏洩時に発生するコストの調査



（2016年の世界平均）
4.4億円

- 信用回復等に係わるコスト
  - ビジネス機会損失
  - 顧客離れ
  - 株式評価の低下
  - 信用の失墜
  - 新規顧客の開拓
- 是正措置、法的対処などの事後対応
- 各種報告対応等
- 技術的な対応等

医療3.9万円　教育2.7万円、医薬品2.4万円、金融2.4万円、
サービス2.3万円、生命科学2.1万円、小売1.9万円、通信1.8万円

平均1.7万円 :漏洩した個人情報1件当たりコスト

工業1.7万円、エネルギー/テクノロジー1.6万円、メディア1.4万円
運輸1.4万円、リサーチ1.2万円、公共0.89万円

出典 Ponemon Institute「2016 Cost of Data Breach Study: Global Analysis」
「2016 Cost of Data Breach Study: Japan」をベースにJPY/USD＝111円で換算

本日お話したい内容

1. ネット社会の現状リスクと対策方針

2. 他人事ではない！セキュリティ事故の実態

3. 持続可能なリスクマネジメント体制とは

リスクマネジメントの強化ポイント“1. 2. 3.”

Step 1 社内体制の整備

Step 2 実行レベルの強化

Step 3 グループ全体の底上げ

「企業価値向上」「社会的責任」の達成！

経営を守る

情報資産を守る

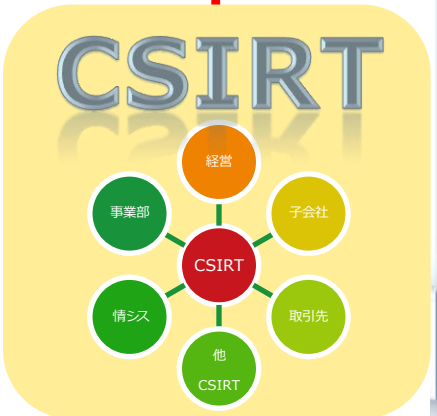
3. 情報セキュリティガバナンスの確立

2. 事故発生を前提とした対応プロセスの強化

1. セキュリティ対策を底上げするためのフレームワーク確立

■株式市場の高評価とブランド価値向上
■事故時のネガティブな反応の抑制　等

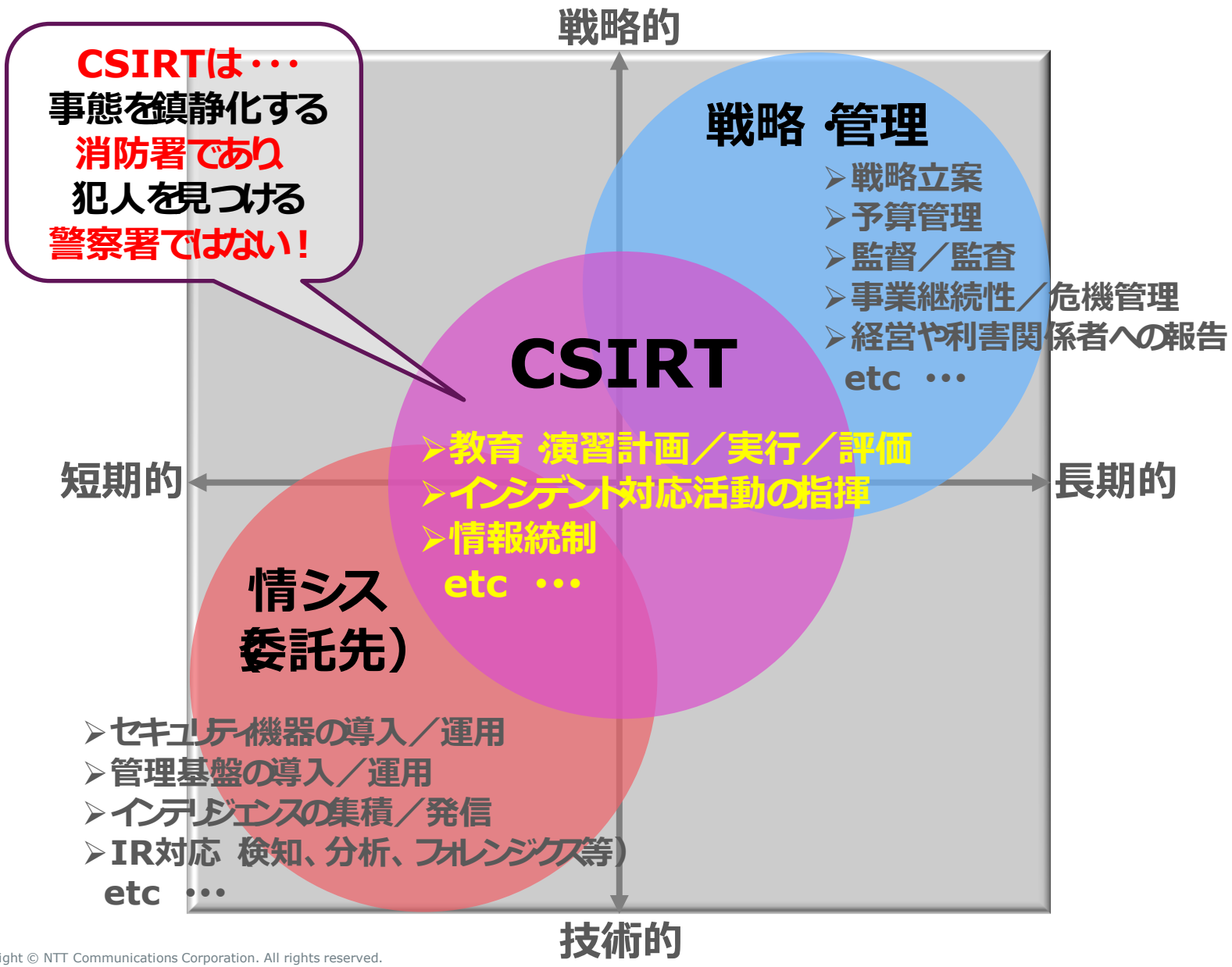
＋



情報セキュリティガバナンス“成熟度モデル”

成熟度	プロセス	人／組織	技術
Level 5	継続的に最適化している段階 ■評価に基づく改善策の立案・実行	評価・処遇制度の導入 ■セキュリティ人材キャリアパスの明確化	迅速・的確なインテリジェンスの共有と連携防御 ■情報セキュリティガバナンスの共通基盤
Level 4	定量的な制御がある段階 ■測定可能な品質目標の設定とその評価	教育・育成モデルの確立 ■社員スキル底上げ、核要員の持続的確保	潜伏した脅威の識別と封じ込め ■エンドポイントの異常検出と遠隔制御
Level 3	規定、標準実施手順がある段階 ■持続可能なフレームワークが確立	適材適所のリソース配置 ■ロア業務の見極めと外注による補強	侵入・感染活動の検知と脅威の洗出し ■Proxyサーバ等を含むログの相関分析
Level 2	管理された方法がある段階 ■繰り返し可能だが、直感的な要素あり	リスク管理体制の組織化 ■経営層（CISO）が関与した管理体制	未知脅威の侵入検知と連携防御 ■NW型サンドボックスによる精密検査
Level 1	非公式な段階 ■ポリシーはあるが手順等に一貫性なし	役割と責任の定義 ■必要なスキルセットの明確化	既知脅威の侵入検知と防御 ■FW,IPS,AV,URLフィルタリングなど

リスクマネジメント体制におけるCSIRTの位置づけ



レジリエンス強化のためのプロセス確立とは・・・

**インシデントを前提とした対策と
その実行力の強化が求められる・・**

標準実施手順（プロセス）を策定し、個人と組織の対応力を維持向上!!

【準備】
- プロセスの整備
- 人の体制化
- 技術の導入

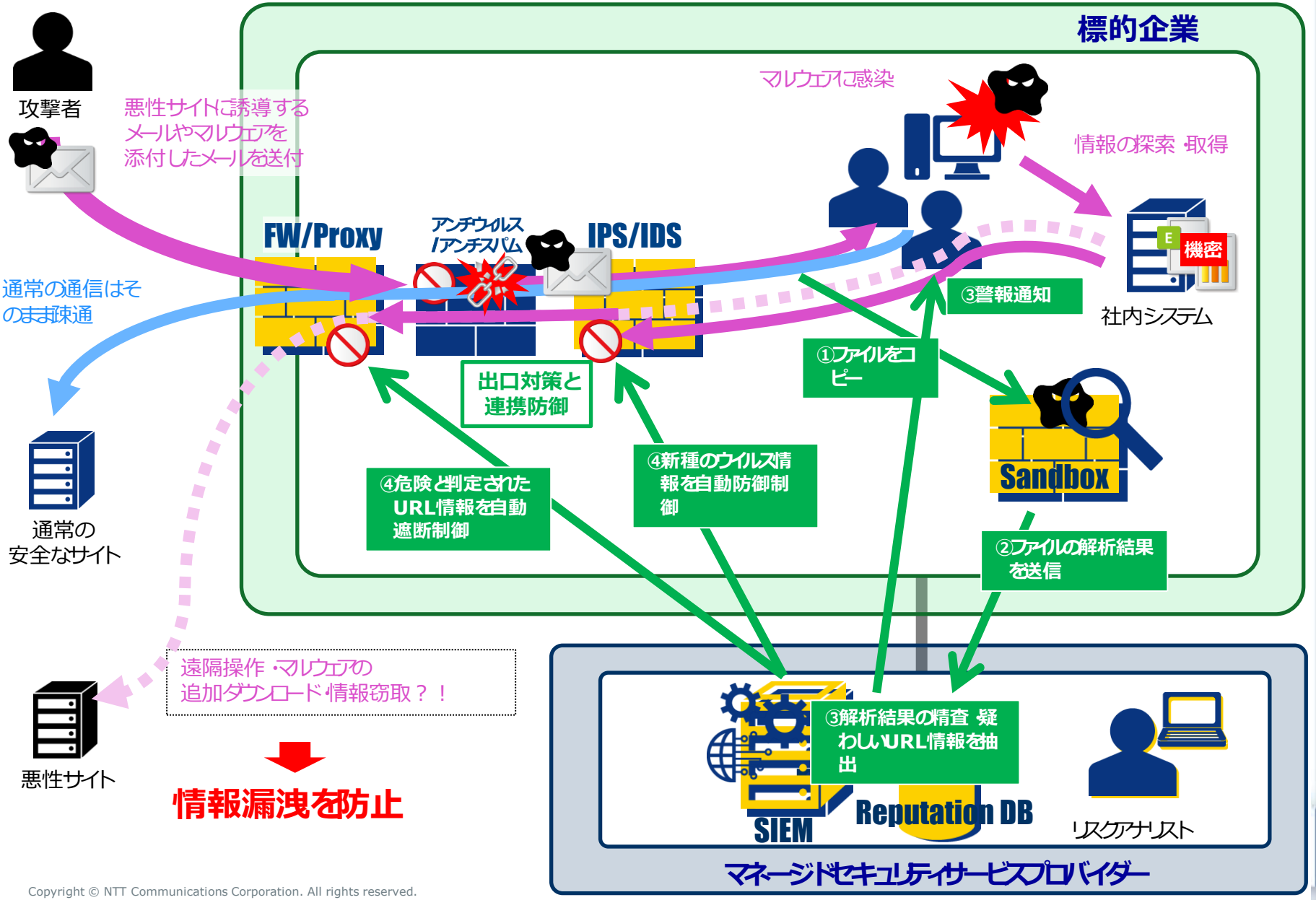
【事故後の活動】
- 事故全容の把握
- コストの把握
- 再発防止策の立案

【検知と分析】
- 前兆を知る
- 事実を掴む
- 攻撃を把握する

【封込、根絶、復旧】
- 封じ込めの実行
- 感染源の識別と駆除
- 封じ込めの解除

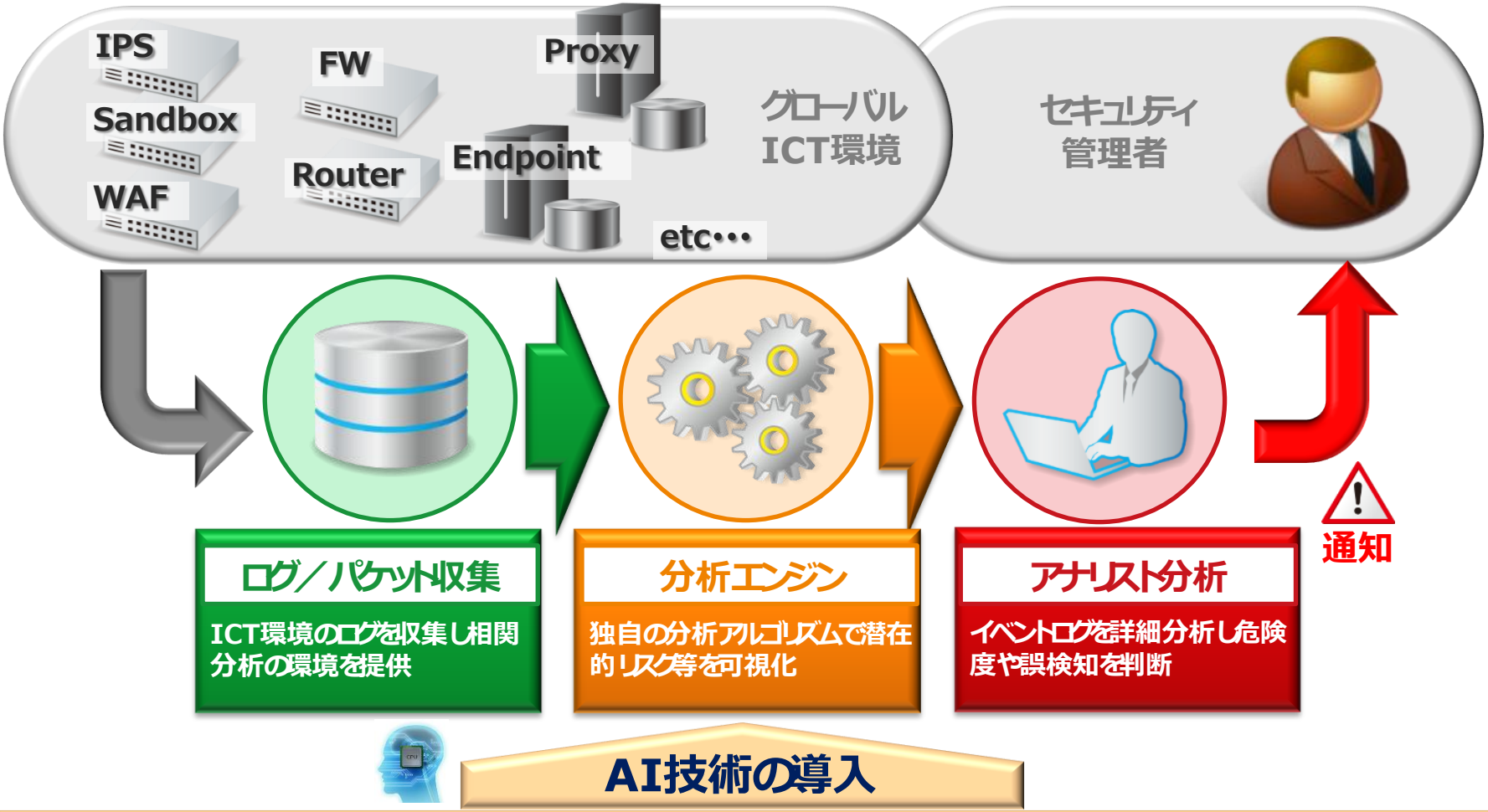
*出典：NIST (National Institute of Standards and Technology)発行「Guide to Malware Incident Prevention and Handling」（マルウェアによるインシデントの防止と対応のためのガイド）の Figure 4-1. Incident Response Life Cycle」（インシデント対応のライフサイクル）

マネージドセキュリティサービスの多層防御と連携防御（事例）



SIEMによるビッグデータ解析で巧妙な攻撃を可視化する

SIEM (Security Information Event Management)



①マルウェアが自動生成するドメインネーム（ホームページのアドレス）を99.5%の確率で検知。

②マルウェアの時間軸を含む様々な特徴を学習し、FWやProxyログから同一パターンを検出、感染IP等を特定。

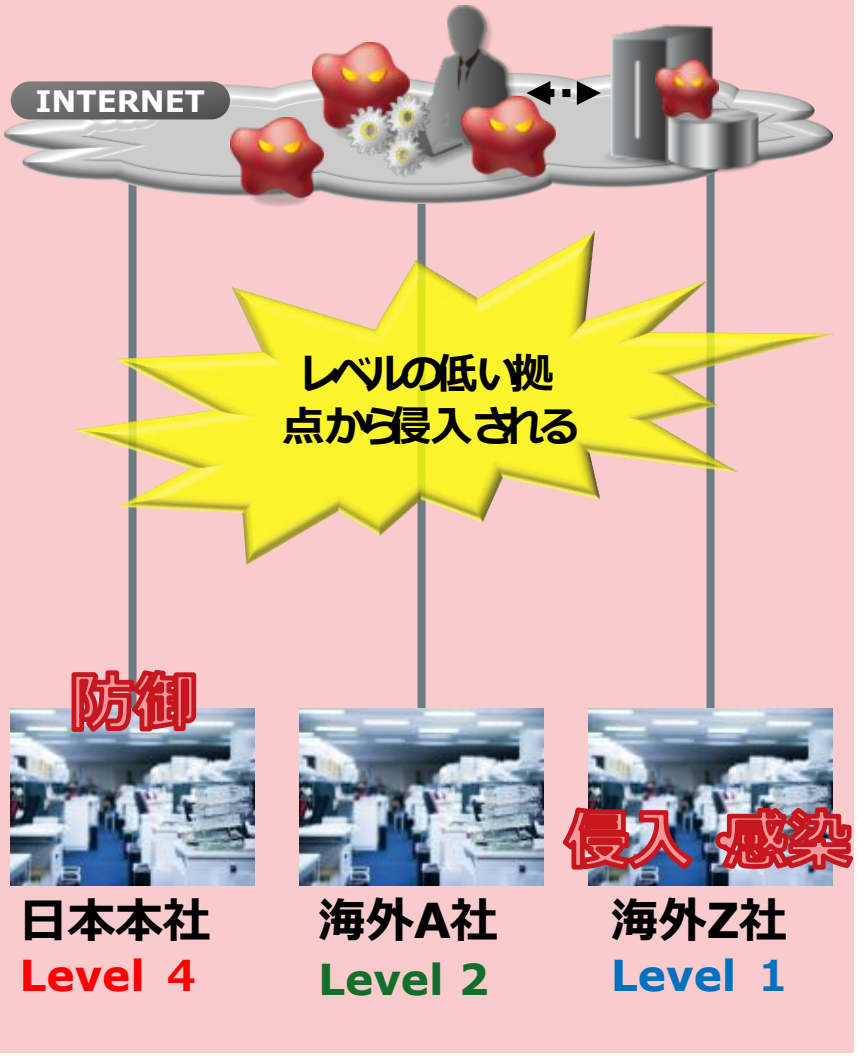
③スイッチ・ルーター・FWなどの通信ログから、マルウェア挙動と合致したケースを検出、クラスタリングし、感染IP等を特定。

④Webサーバーの正常な利用状況を学習し、外部からの異常な振舞や攻撃行動を検知。

グループ経営を守るインテリジェンス共有と連携防御

グループ全体のレベルアップ（IT基盤・体制の統合化、攻撃者情報等の共有）

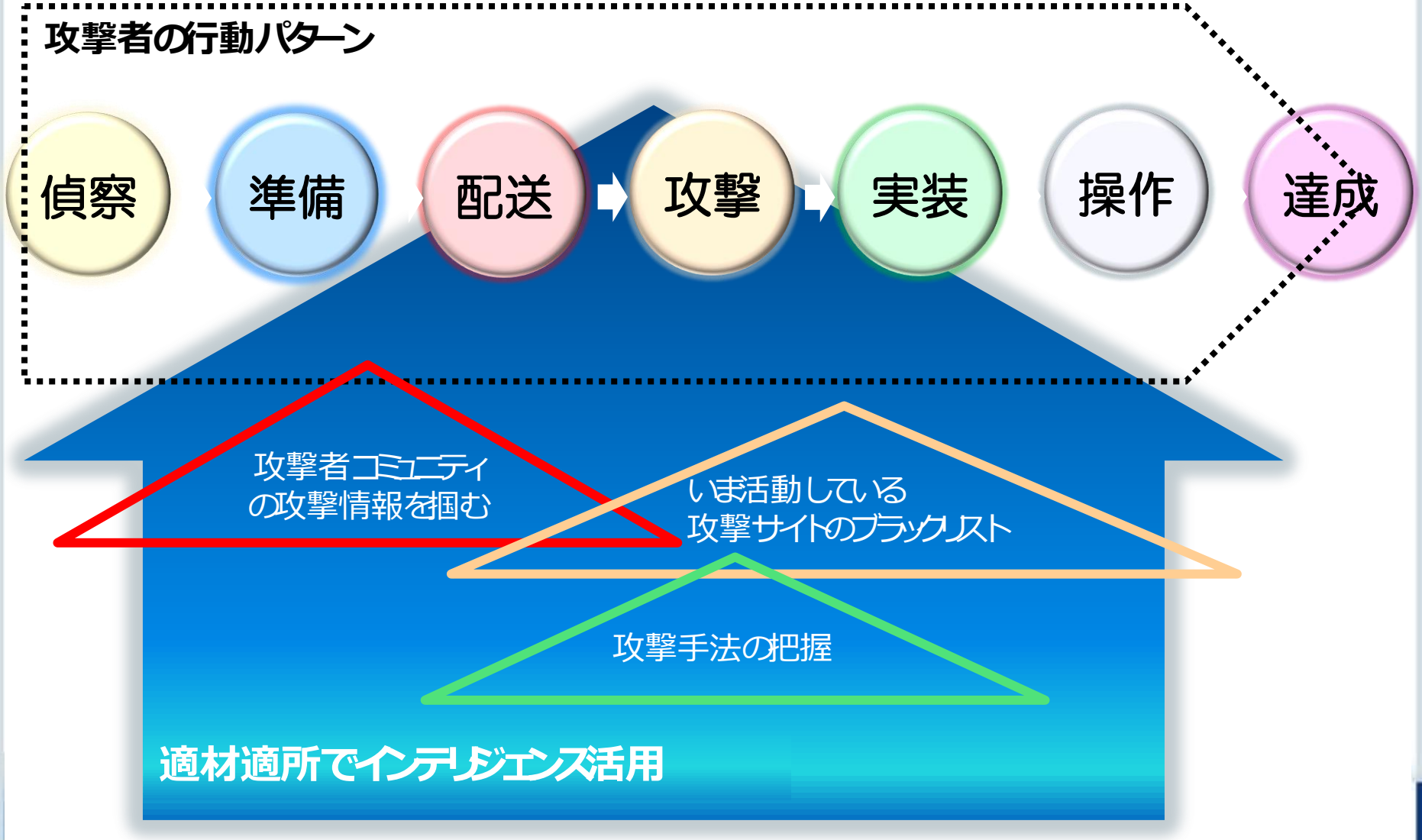
Before



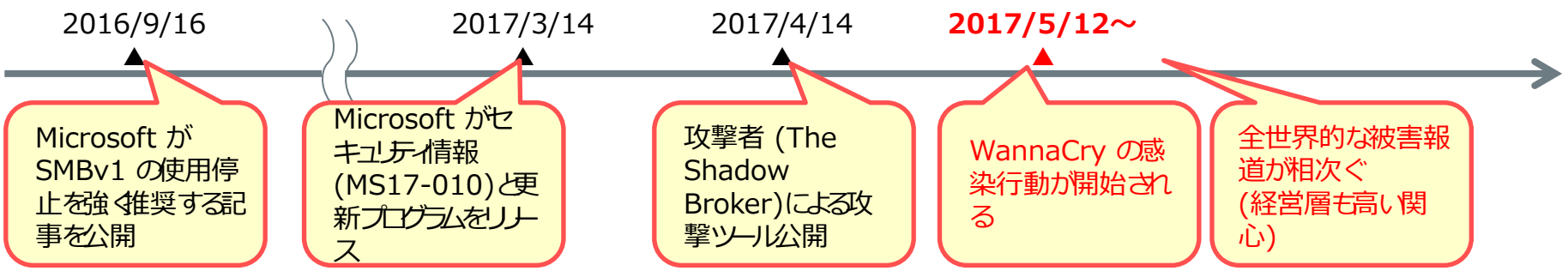
After

セキュリティ対策共通基盤の導入により、グループ全体のレベルアップを実現!!

攻撃者優位のギャップを埋めるインテリジェンスの活用術



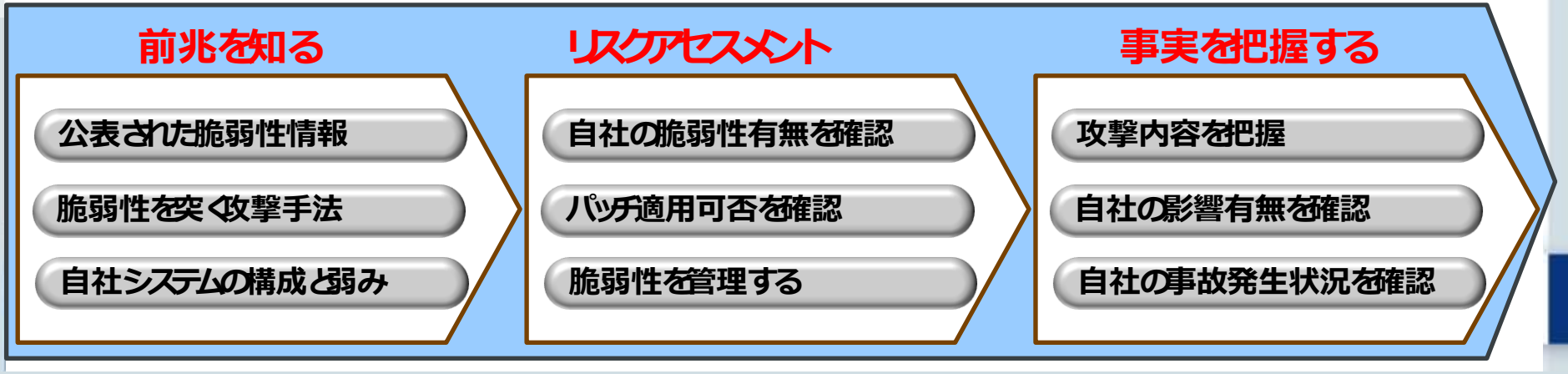
WannaCryから見えたセキュリティ管理体制の課題



課題】CSIRTがない / CSIRTはあるがセキュリティ管理体制が十分機能していない企業・団体

- 脆弱性情報を認識していない
- 自社既存システムの構成と脆弱性を把握していない
- 脆弱性情報を認識しても影響有無が判断できない
- 影響があっても網羅的な緊急対策が打てない

- CSIRTによるセキュリティ管理体制が効果的に機能するプロセスや業務イメージ



企業ICT環境のリスクマネジメントを総合的にサポートするソリューション

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

- プロフェッショナルサービス
- セキュリティ対策機器/ソフトウェアの導入サービス
- マネージドセキュリティサービス


ご清聴ありがとうございました。
WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT
総合リスクマネジメントサービス「WideAngle」
http://www.ntt.com/business/services/security/security-management/wideangle.html
竹内文孝のFacebookページ
https://www.facebook.com/fumitaka.takeuchi.ntt