資料５

一部非公開

第2回 産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環に向けての検討会

セキュリティ産業振興に係る意見について

政策・連携戦略推進部　都築 英之

世界中に展開する日本発のトランスナショナルカンパニー

国境のないサイバー領域において世界中で価値を提供しながらも
日本に本社を配置し日本市場にコミットする日本発グローバルサイバーセキュリティ企業です。

体制

- 日本に本社を配置
- グローバル全体の脅威情報へのアクセス・分析

強み

- Threat Intelligenceの収集力＆35年の蓄積
- 脆弱性発見/報告No.1

取り組み

- 地政学リスクへの対応
- ISMAPの取得
- 日本政府の政策への対応

当社戦略の変化：ツールからプラットフォームの提供へ

Prevention

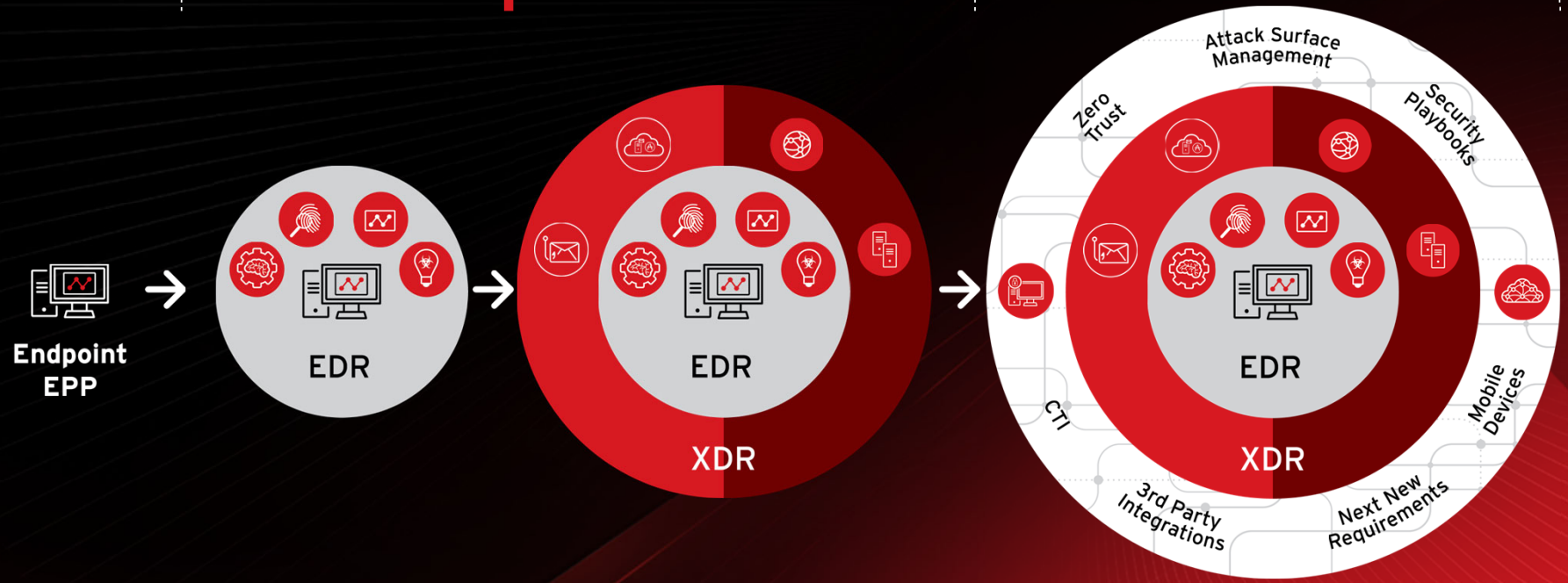
Detection only on managed devices

Multilayered:
Endpoint, Network,
Cloud Workloads, and E-mail

Cross Threat Detection, Correlation and Response

Trend Vision One™ - Advanced Cybersecurity Platform

EDR, XDR, Attack Surface Management, Zero Trust, Threat intel, Assessment



New Cyber Security Requirements & Challenges

Public

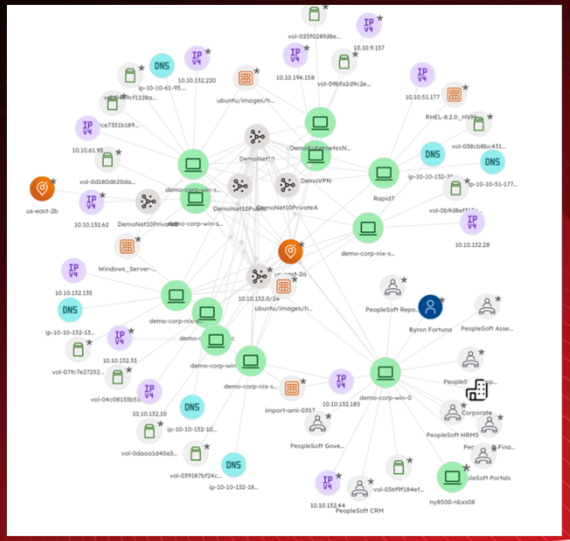
それぞれの検知をリスクシナリオとして認識することがポイント

サイバー脅威をリスクシナリオと関連付けるためには、サイバー攻撃の発生イベントを**より広範囲な収集データ**と多角的なインテリジェンスで分析し、また**検出情報の抽象化**を行う必要がある

守る側の思考モデル
Defenders think in list

- ✓ NIST cybersecurity framework
- ✓ Endpoint security
- ✓ Network security
- ✓ Cloud security
- ✓ Vulnerability management

攻撃者側の思考モデル
Attackers think in graphs



問題提起)組織で起きている経営層とセキュリティ運用の乖離

経営層で捉えている**経営/事業リスクとサイバーセキュリティ運用との関係性**が明確になっていないことが課題

脅威

- 機密情報の漏洩
- サイバー攻撃による業務停止
- 取引先・サプライチェーン構成企業への影響


攻撃者


メール


ウイルス


脆弱性


経営


運営


運用


ITサービス

コーポレートガバナンス
変化に対応した安全・安心な事業基盤の確立

サイバーセキュリティマネジメント
戦略的セキュリティリスク対応計画立案と推進

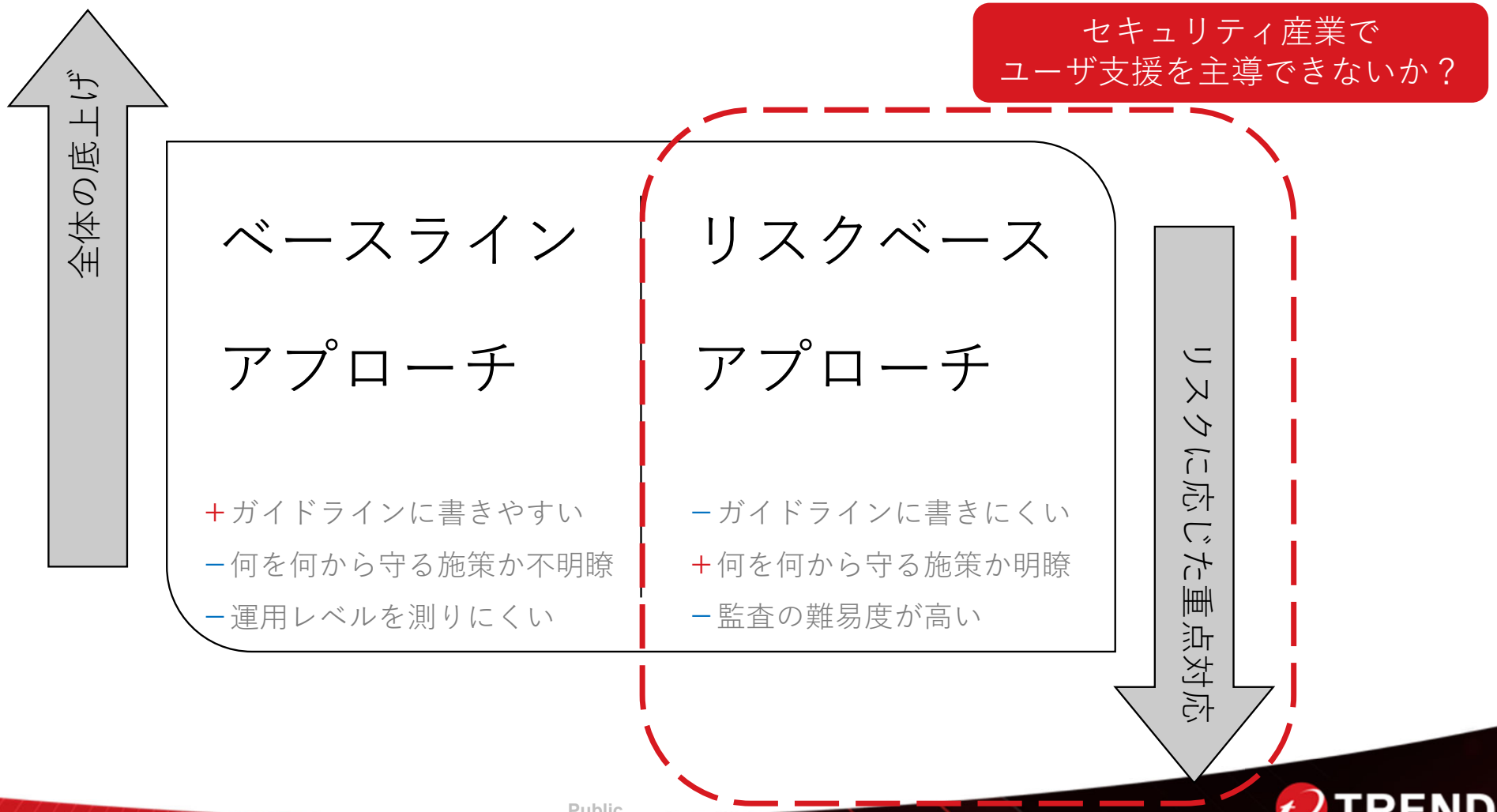
残存リスクの低減 | **被害・影響の最小化** | **インシデントからの早期復旧**

サイバーセキュリティオペレーション
デジタル基盤の安全性維持・向上

デジタル資産の把握と適切な対策

情報システム | 業務システム | IoTシステム・機器等

政策を考える上で２種類のアプローチ



参考)サイバーセキュリティ施策を考えるときの基本概念

適用例)サプライチェーン上の守るべき対象と紐づく一連の流れ(仮案)

任務保証の概念

データ

- 重要度に合わせた保護と利活用
- データライフサイクル
- データの委託・外部保管

システムインフラ

- 重要度に合わせた保護と利活用
- インフラ/ハードウェア
- ソフトウェア/クラウド
- ネットワーク/運用委託

サービス

- プロセスとステークホルダーの特定
- 被影響範囲・規模の特定
- システム・データ・人

目指す姿(案)

①ユーザサイド

自組織で何を何から守るかが分かっている状態

- 経営/事業リスクとしてのサイバーリスク認識
- 保護対象と影響範囲の特定
- リスクシナリオの想定と自組織における影響度
- 自組織の優先すべき価値観の合意形成

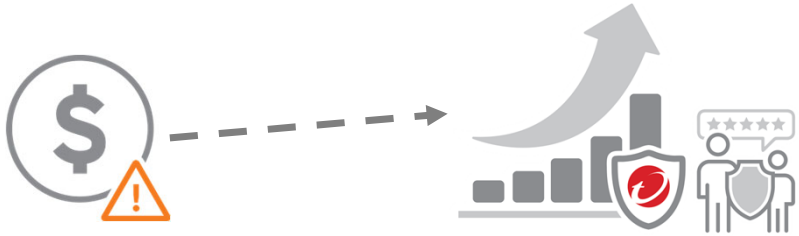
伴走型リスクコンサルと文化形成

②サプライサイド

セキュリティ主体で高付加価値提案が可能に

③セキュリティ価値転換

セキュリティを競争優位性の要素へ変換



④目指す好循環

需要と供給の相互刺激による好循環環境の形成

- 事業発展に資するセキュリティ産業の深化
  →高付加価値提案領域で国際ポジションの確立
- セキュリティ投資が事業収益につながる構造創出
  →市場規模の拡大と質の確保の両立
- 安全な事業推進、事業リスク対応市場の拡大
  →戦略的自律性/不可欠性の確保

構想案)サイバーセキュリティをコスト⇒競合優位性の要素へ

住宅/建物や自動車においてはセキュリティ要素が買い手に明示され、買い手はセキュリティ要素の追加にお金を支払う市場が形成されている。物理的なセキュリティは買い手も直感的に理解しやすい事情はあるものの、市場形成にあたって必要な要素の整備について参考にできるのではないか

・住宅性能表示制度での評価
  ・耐震等級３であること
  ・耐風等級２であること…etc
・ハザードマップ上でリスクが少ないこと
  ・地震、洪水、土砂災害…etc
・災害対策がきちんとしている自治体

・自動車安全性能がAランクであること：衝突、予防、通報装置
・衝突被害軽減ブレーキ認定を取得していること
・サポカーＳワイドに該当すること

・可視化
・基準化
・認定化
が必要？

リスクマネジメントの文化形成

IT・セキュリティ主幹課	原課(As Is)	原課(To Be)
• サイバーセキュリティの知識	• サイバーセキュリティの知識	• サイバーセキュリティの知識
• IT・デバイスの知識	• IT・デバイスの知識	• IT・デバイスの知識
• リスク評価の能力	• リスク評価の能力	• リスク評価の能力
• 業務プロセスの理解	• 業務プロセスの理解	• 業務プロセスの理解
• サプライチェーン	• サプライチェーン	• サプライチェーン
• リスクのインパクト	• リスクのインパクト	• リスクのインパクト
• 組織に対する知識	• 組織に対する知識	• 組織に対する知識
• 業種経験	• 業種経験	• 業種経験

ブレーキ役

アクセル役

現場課題を捉えた
DX推進

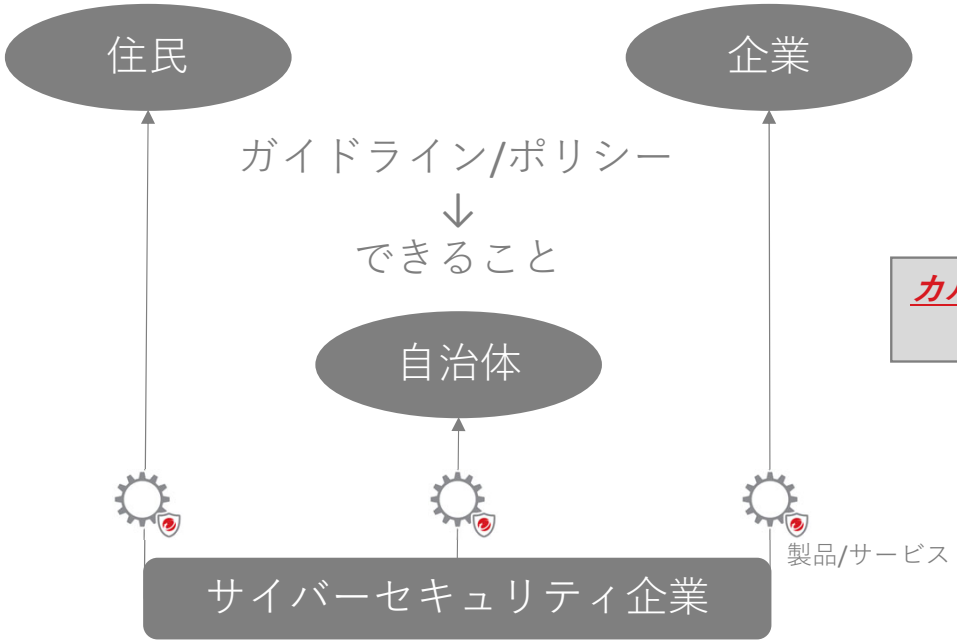
支援＆モニタリング

アクセル＆ブレーキ

Public

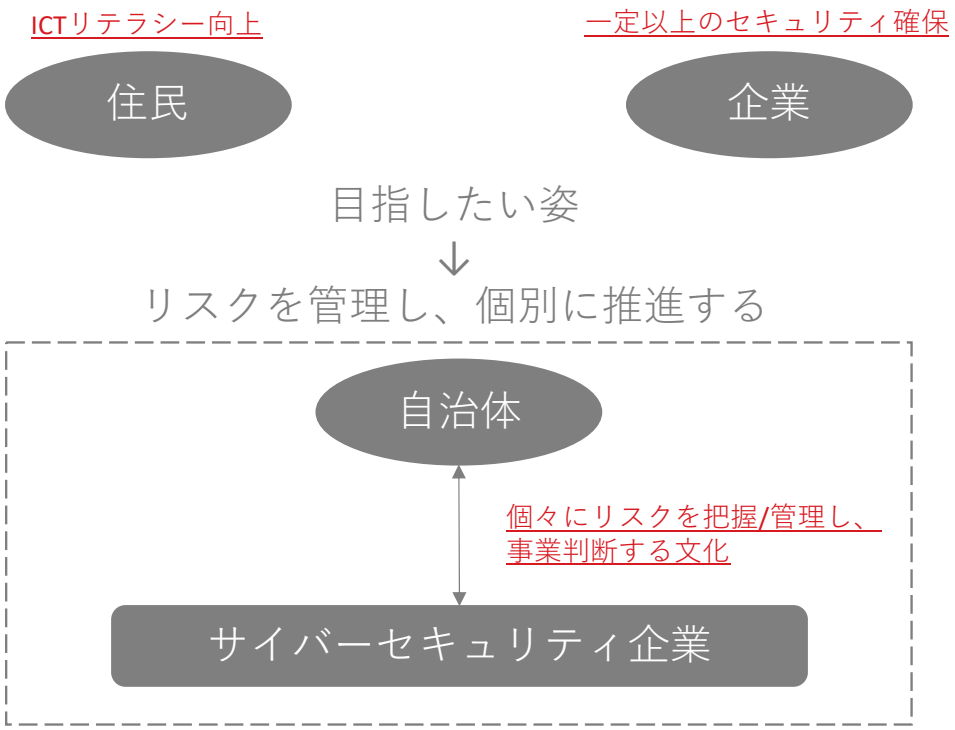
考え方)セキュリティを制約条件から推進要因へ：地方公共団体を例に

As Is ガイドライン等による制約内でのDX推進

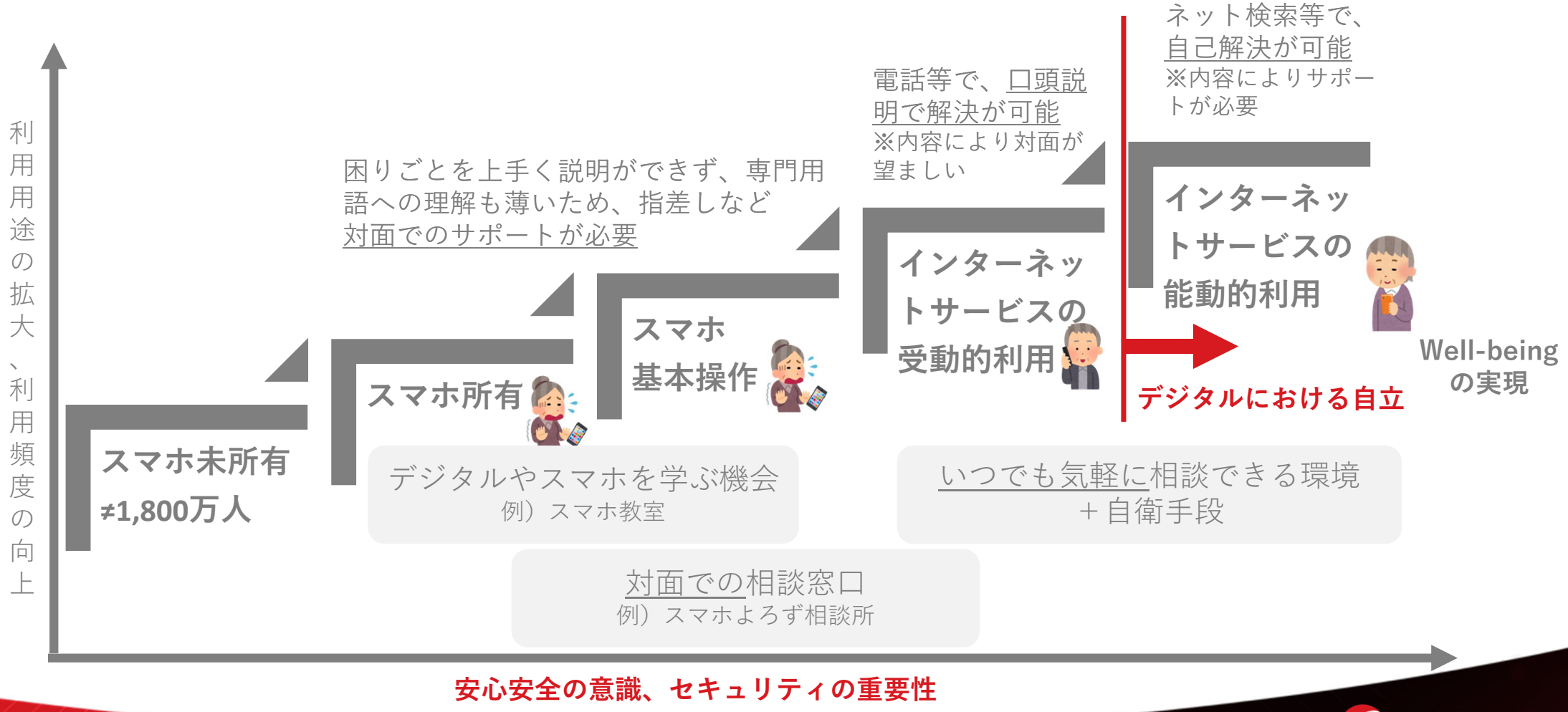


カルチャー変革

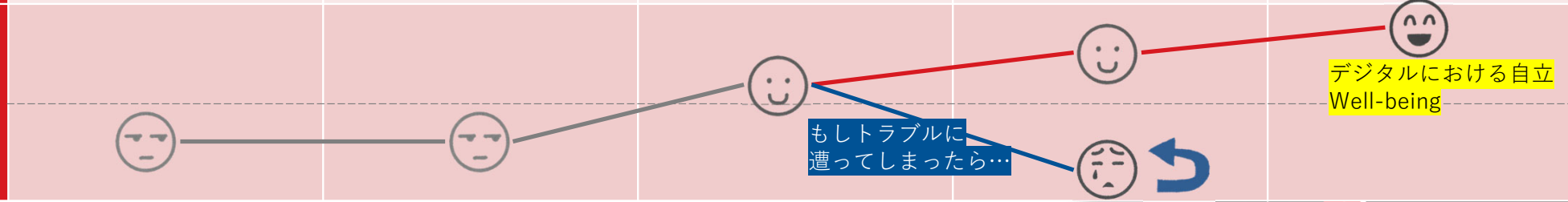
目指したい姿に対してリスクをマネジメント **To Be**



DXのボトルネック解消例)シニア世代のスマホ利活用推進



参考)デジタルレベルアップ支援ジャーニーマップ

レベル	スマホ未所有	スマホ所有	基本操作	受動的利用	能動的利用
行動	ガラケーが使えなくなるからスマホに変える必要がある	スマホを持ったはいいが、結局電話の受発信にしか使っていない	電話以外にカメラやLINE、SMSといったコミュニケーション機能も使えるようになってくる	日常的にスマホを利用するようになり、知人・友人に勧められたサービスも利用するようになる	自分で必要なサービスを選択し判断、利用、管理ができる。デジタルにおいてWell-Beingな状態。
思考・感情	ガラケーで十分、スマホは高いし、使いこなせない	スマホの使い方もよく分からないし、電話ができれば十分	カメラで撮った写真をLINEで送るにはどうしたらいいんだろう？（使うための悩みが出てくる）	明日のお出かけのために、お友だちが教えてくれた乗り換え案内アプリを使ってみよう	町内会のイベントのためにスライドショーをつくりたい、何か最適なサービスはないだろうか？
課題	スマホに変えるメリットを感じていない	スマホの操作方法が分からず、電話以外に関心が持てない	誰かに相談したいが、家族は遠方で忙しいし、携帯ショップは予約が必要だったり、営業されそうで緊張する	使い始めに障害があったとき、対面での相談の場を待っていると解決に時間がかかる、お勧めされるサービスが安全とは限らない	自分が主体的に必要なサービスやアプリを探すからこそ、詐欺サイトや不正なアプリに遭遇する機会も増える
必要な支援	経済的な支援やスマホを体験する機会 例）1年間の通信料補助	スマホの活用法や使い方を知る・学ぶ場 例）スマホ教室	対面で気軽に相談できる場 例）シニアコミュニティや自治体主催のよろず相談	いつでも気軽に相談できる場や自衛手段 例）電話サポート、セキュリティ対策	自衛手段といつでも気軽に相談できる場 例）セキュリティ対策、電話サポート
感情曲線					

会社説明補足スライド

TREND MICRO™

Public

世界にまたがるリサーチセンター、グローバル全体の脅威情報を広く網羅

- トレンドマイクロリサーチセンター
- サイバー犯罪に関してアンダーグラウンド調査（＝捜査協力）を行った国

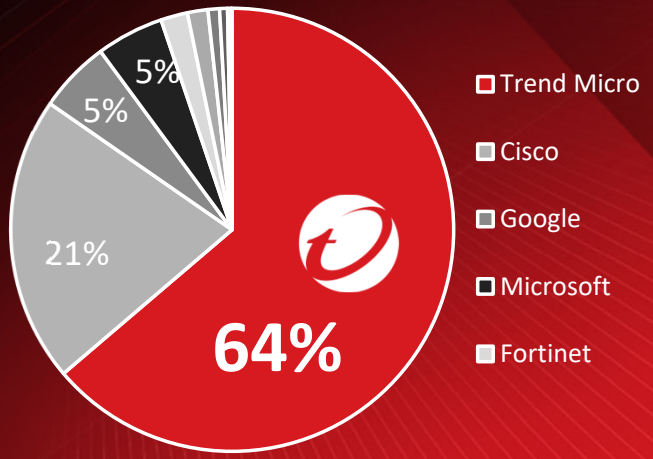
Public

Threat Intelligenceの収集・活用による事業展開

ZERO DAY INITIATIVE

10,000人

全世界に存在するセキュリティリサーチャー



Quantifying the Public Vulnerability Market, Omdia, May 2022

TREND MICRO

地政学リスクへの対応

地政学的リスクを抑えて、日本のお客さまに安心してご利用いただくために
当社製品・サービスを提供するデータセンターは日本にも設置し、日本主導でデータ管理を実施

日本の専任組織による
管理・運用改善

日本主導でデータ保管と運用

- ID・環境分離とデータ管理
- 機能・修正の本番環境への安全なリリース
- 監視と障害対応、復旧
- 障害時、円滑な社内連携によりスムーズな情報公開

トレンドマイクロ
日本 SRE

（登録番号：C23-0051-2）
https://www.ismap.go.jp/csm?id=cloud_service_list_detail&sys_id=8bfa8994c3faa11043ba9c777a013152

※ SRE = Site Reliability Engineering：サイト信頼性エンジニアリング
※ 一部SaaS製品は海外SREでの運用もありますが、日本SREと連携して管理運用を実施

関係者限り Public

スマートシティをカバーする幅広いソリューション

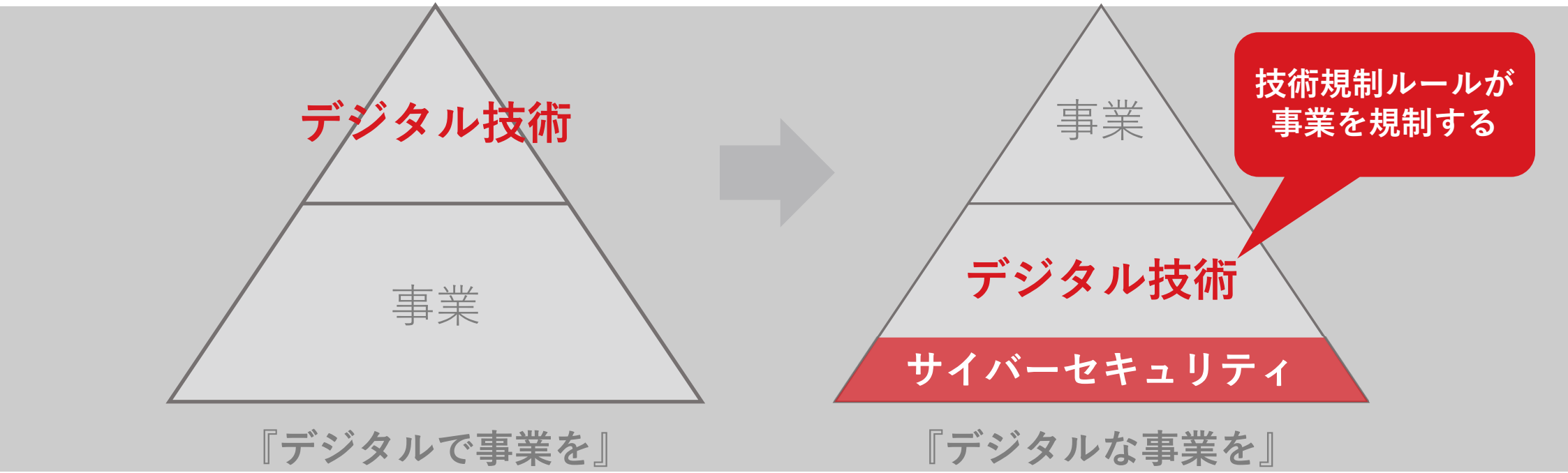
ユーザ層	サービス層	都市OS層	アセット層
			
PC/スマートフォン	サーバ/仮想環境	クラウドPF	IoT機器/IoT Gateway
不正サイト	クラウドPF	API Gateway	Local 5G/SIM
ID/パスワード保護	コンテナ	脆弱性/IPS	NW機器/IPS
サポート詐欺	脆弱性/IPS	通信/アカウント監視	ホワイトリスト

論点補足スライド

TREND MICRO™

Public

デジタル技術と事業の関係性の変化



サイバーセキュリティの役割は『事業を守る』ことへとシフトしている

参考)政府の考え方の変化

サイバーセキュリティ戦略本部
重要インフラのサイバーセキュリティに係る行動計画

セキュリティリスクへの備えを経営戦略として位置付け、**任務保証**について言及

重要インフラ14分野
「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」

§任務保障
企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方

１．重要インフラ防護の目的
重要インフラにおいて、任務保証1の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靱性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的とする

出典：重要インフラのサイバーセキュリティ対策に係る行動計画

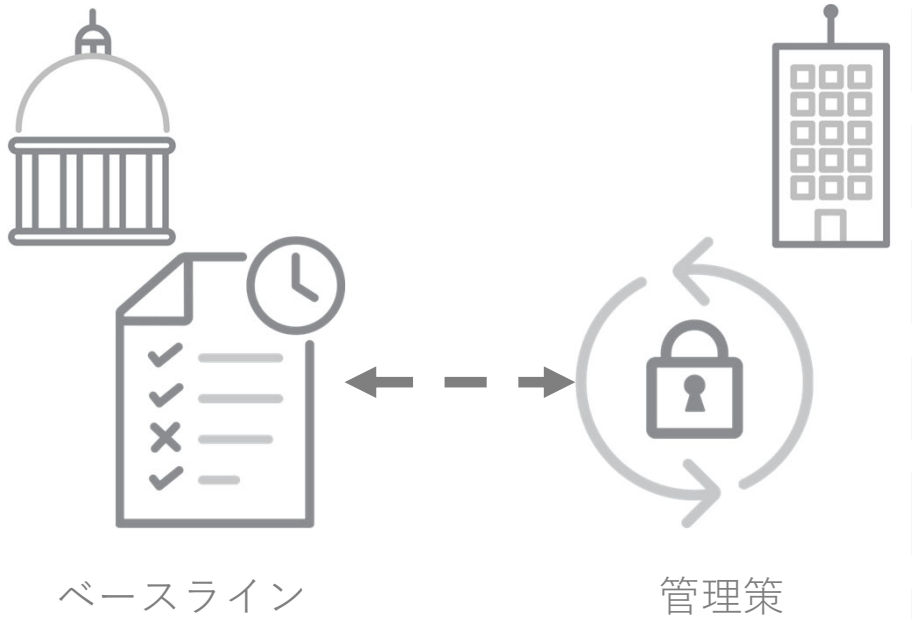
2種類のサイバーセキュリティとガイドライン記載の難しさ

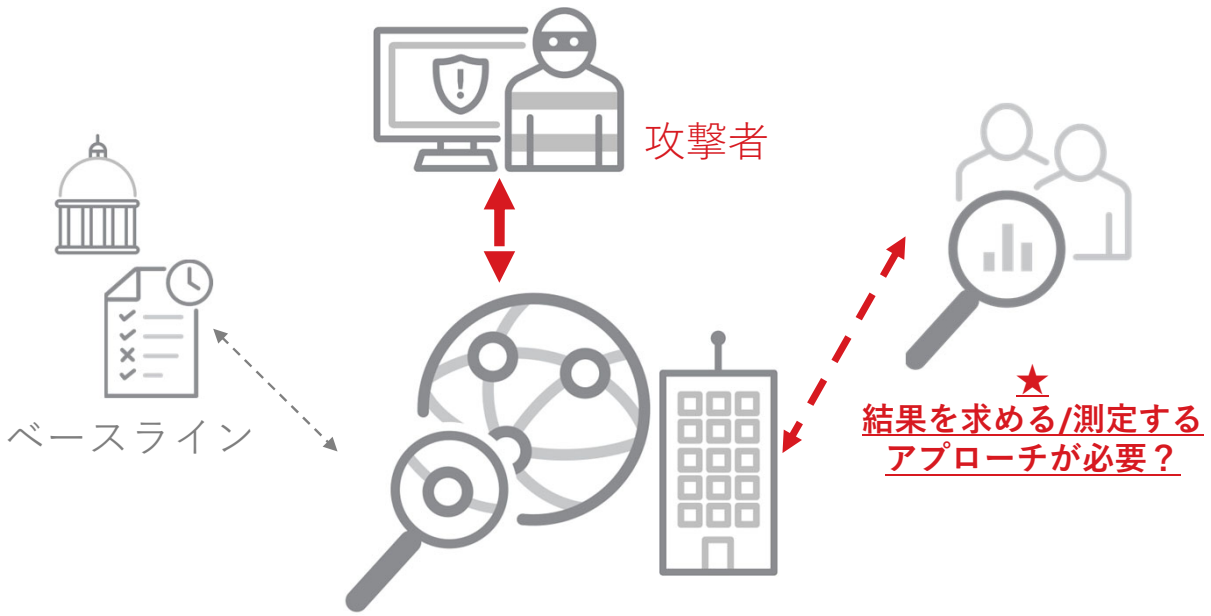
予防的統制

発見的統制

※顕在化リスクの発見
→対処を行う概念

識別 | 防御 | 検知 | **対応** | **復旧**



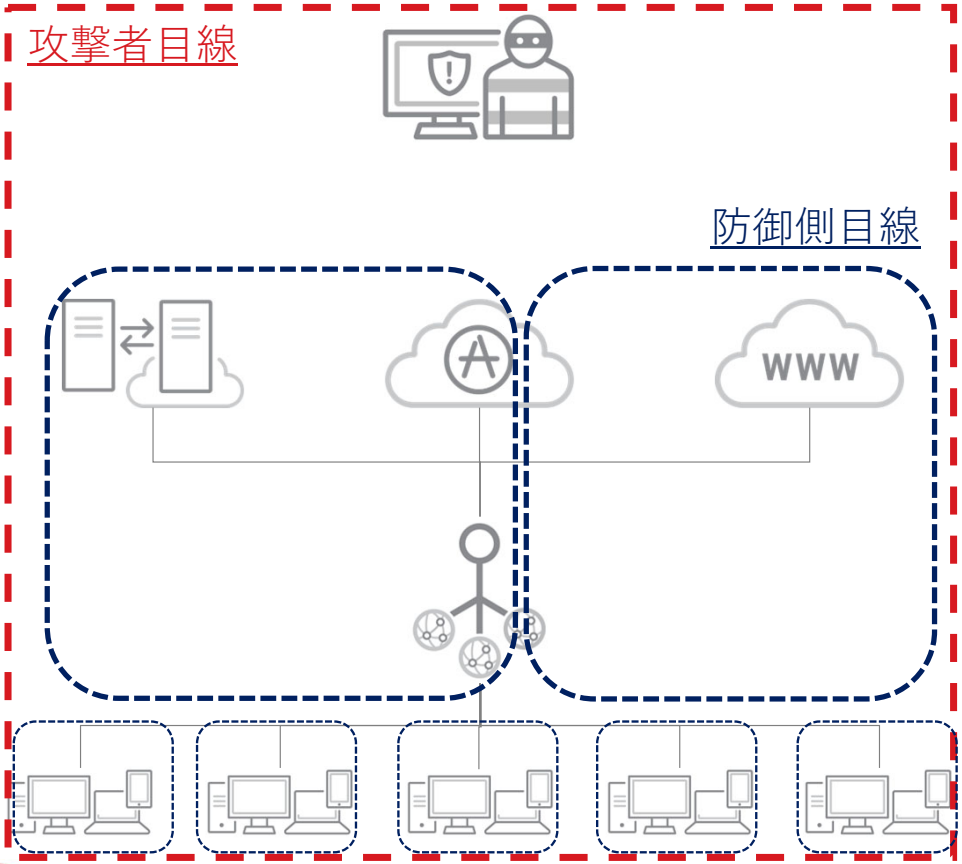


ベースラインに準拠した管理策が
実行できているか？

ベースラインに準拠した管理策を実行し、
自社を狙う攻撃から身を守れているか？

参考)攻撃側と防御側の意識と視点の違い

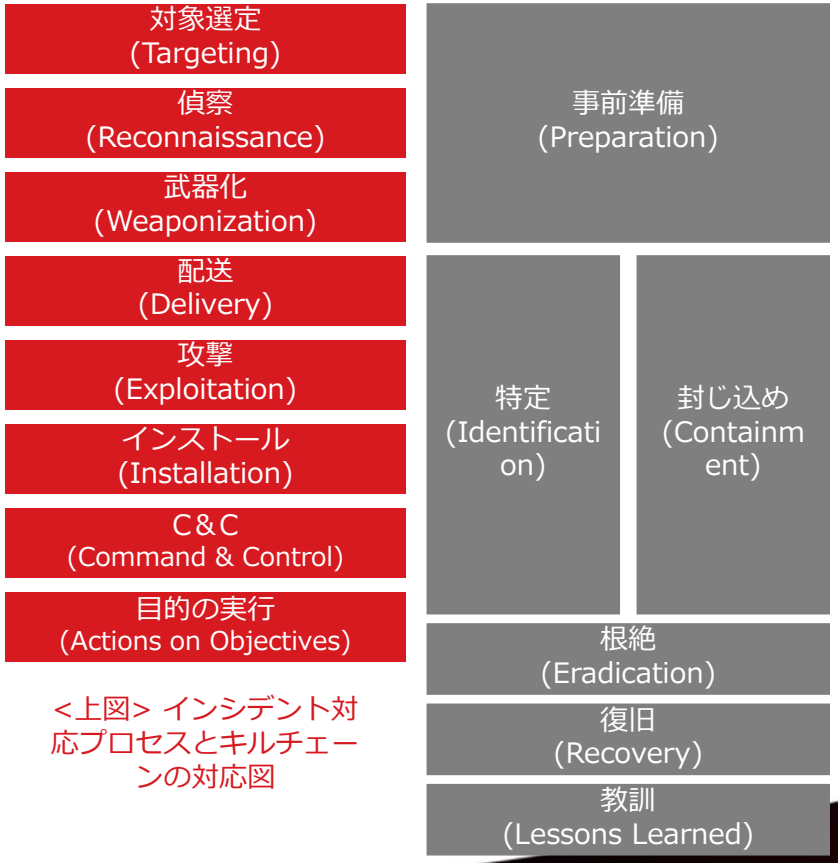
観点１：縦割りにより攻撃者と同じ目線で守れない



ランサムウェアの場合

5.82日

観点２：スピードの観点が抜けがち



<上図> インシデント対応プロセスとキルチェーンの対応図

<参考> インテリジェンス駆動型インシデントレスポンス（オライリージャパン, 2018年）