NTT Communications
Transform. Transcend.

ゼロトラスト時代のアカウンタビリティ

～サイバーリスクへの対策強化に向けて～

2019年8月15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推進室長
竹内文孝　,CISSP

What is “Zero Trust"

ビジネス変革 → ICT環境変革 → セキュリティ変革

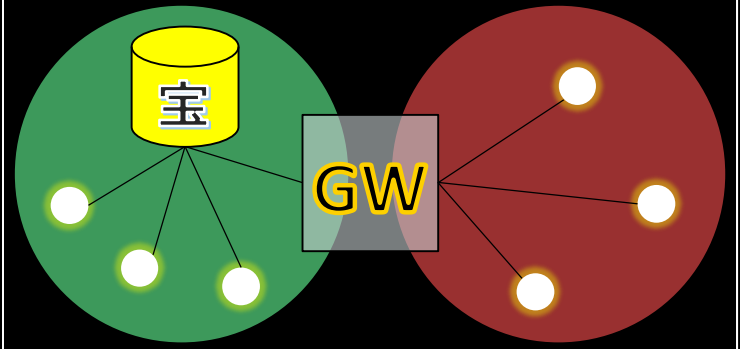
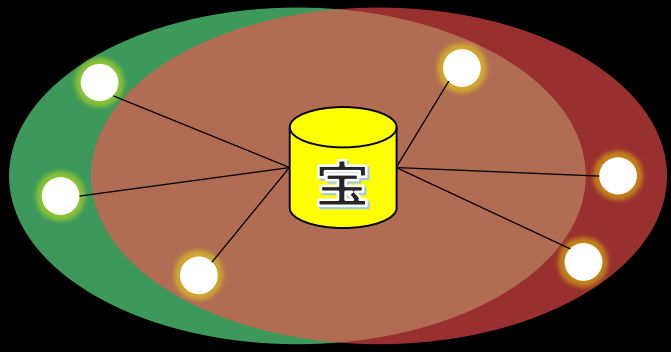
DX × **闇市場** = **Zero Trust**

- 事業競争力の強化
- 働き方改革
- 新たな価値の創出

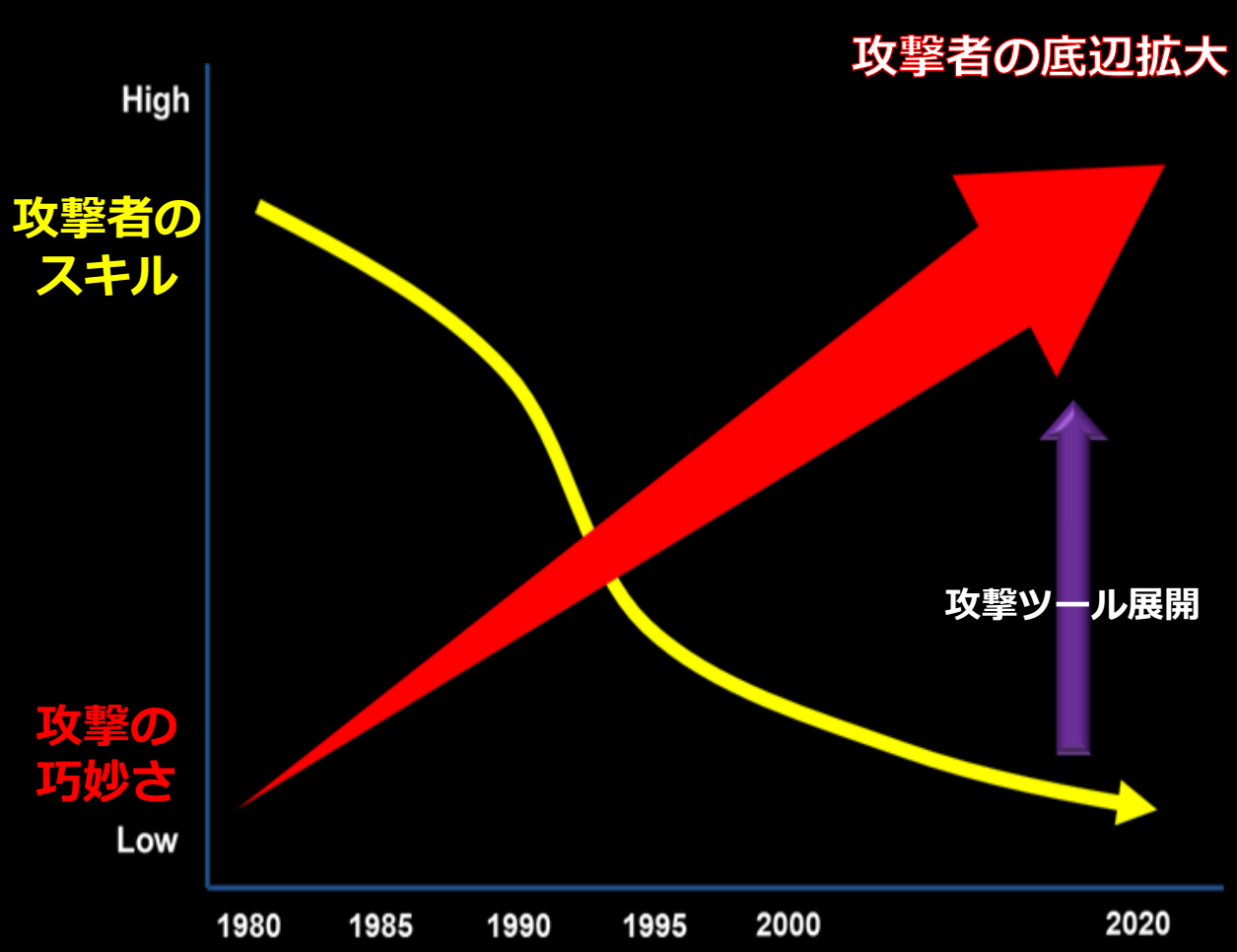
- 攻撃者の多様化、巧妙化
- 攻撃者の組織化
- 闇市場の拡大

- 流動的なICT環境
- 境界防御の限界
- 侵害前提の対応策

What is difference

比較項目	境界防御モデル（従来）	ゼロトラストモデル
ICT環境	 信用する領域 内部NW　信用しない領域 外部NW	 第三のプラットフォーム クラウド、ビッグデータ モバイル、ソーシャル
利便性	外部NWは条件付きで	いつでも、どこでも
想定脅威	内部は安全、外部は危険	内部も、外部も
リスク対策	性善説（内部）	性悪説、性弱説

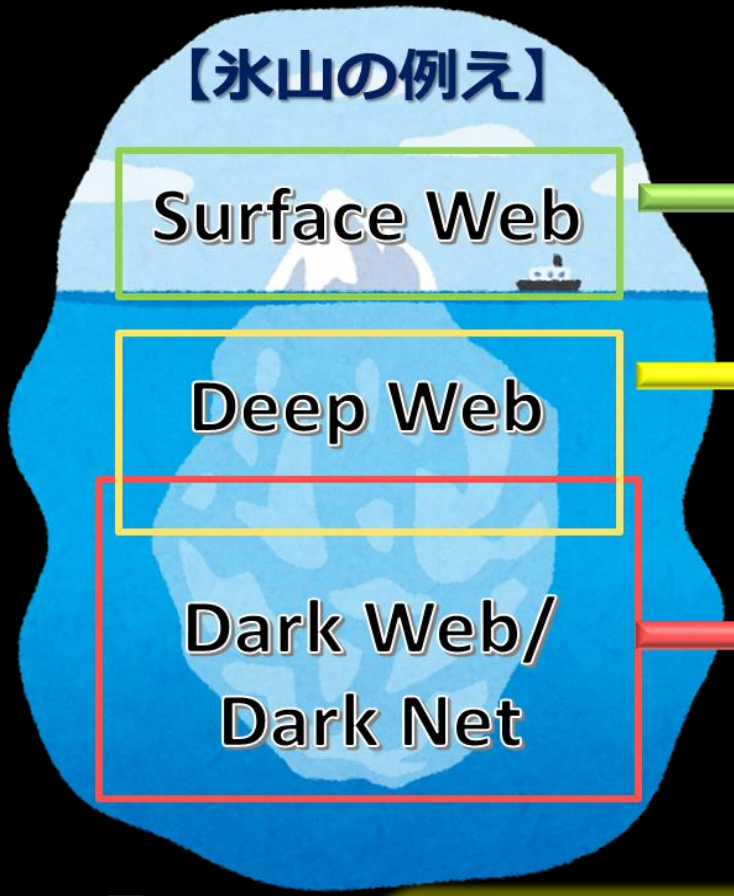
攻撃者の組織化、分業化による底辺拡大



闇市場を利用した
組織化／分業化

攻撃者のスキル（ ）but ツールによる攻撃の巧妙さ（ ）

Dark Web/Dark Netによる闇市場の拡大



Googleなど一般的に利用可能な検索エンジンで見つけられるサイト。

通常の検索エンジンではみつからないウェブ情報。検索エンジンの巡回を拒否したり、パスワード保護がかけられたサイト。

Torブラウザ等で接続するウェブ空間で、犯罪活動に関連するウェブサイトが多い。
マルウェア、海賊版コンテンツ、盗まれたアカウントやクレジットカード情報、ハッキング技術など、ビットコインにより匿名で売買が成立する闇市場

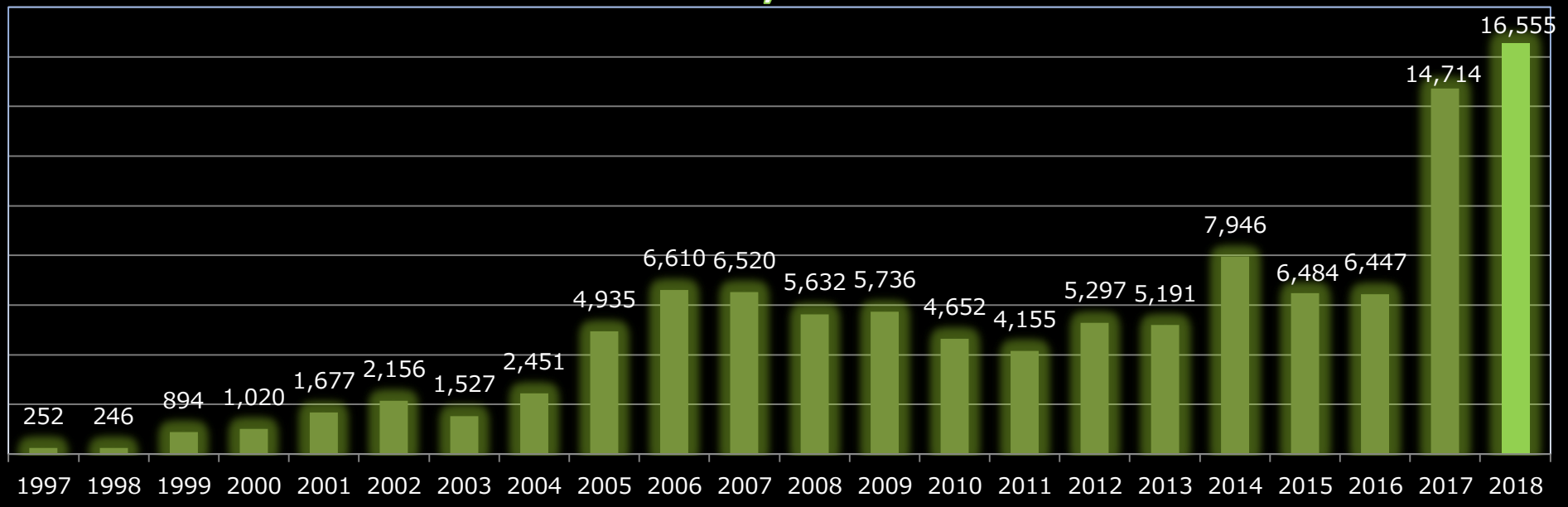
闇市場実態

DDoS請負サービス「Webstresser.org」が2018年4月に閉鎖されて以降、欧州でのDDoS攻撃が約60%減少した。

（参照）https://www.link11.com/en/blog/number-of-ddos-attacks-significantly-declines-after-shutdown-of-webstresserorg/

サイバーリスクの根源となる脆弱性の発生状況

2018年の脆弱性報告件数は16,555件



出展：https://www.cvedetails.com/browse-by-date.php

「偵察」「準備」「配送」から始まる標的型攻撃

IPAの情報セキュリティ10大脅威2019で『標的型攻撃』は組織向け脅威の第１位

- 標的になる企業情報
- ソーシャルメディア

【一般的なウェブサイト】

「配送」

標的企業または
個人情報を収集、
ビックデータ化

攻撃情報等の
「偵察」と「準備」

過去に漏えい
した個人情報

【ダークウェブ A】

標的企業の
放置された弱点等

【ダークウェブ Z】

IPA：独立行政法人情報処理推進機構

サプライチェーンの弱点を悪用した攻撃

IPA（独立行政法人情報処理推進機構）の情報セキュリティ10大脅威2019で4位に初ランクイン

ターゲットは
本社の機密情報

グループ経営基盤

宝

本社直轄グループ会社

M&Aなどグループ会社等

物品や役務の取引先等

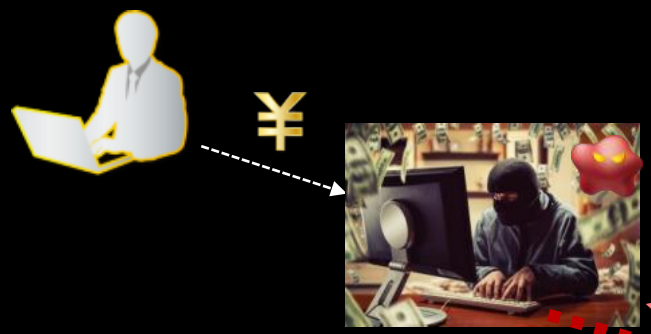
強

セキュリティガバナンス

弱

『我が社の弱点がグループ
全体の企業価値を下げる
ことに・・・』

市販品に潜むサプライチェーンリスクの実態



サプライチェーン

工場

M&A

営業所／研究所

本社

（2018年10月4日）
サーバーへの悪性チップ埋め込み疑惑

国家スパイによる攻撃が、米国のテクノロジーサプライチェーンを襲い、アマゾンやアップル等を含む約30の米国企業に危険が及んだとBloombergが報じた（2018.10.4）

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

経営環境の潜在的悪影響を最小化するために

NIST CSF “サイバーセキュリティフレームワーク”

NIST:米国国立標準研究所

特定 → 防御 → 検知 → 対応 → 復旧

アカウンタビリティ

経営レベル

リスク対応策の方針展開

現場レベル

平常時の対応（サイバー衛生管理）

- 人材育成、教育、演習
- インテリジェンス展開
- 異常察知力、脅威検知力
- アクセス制御、連携防御

事故時の対応

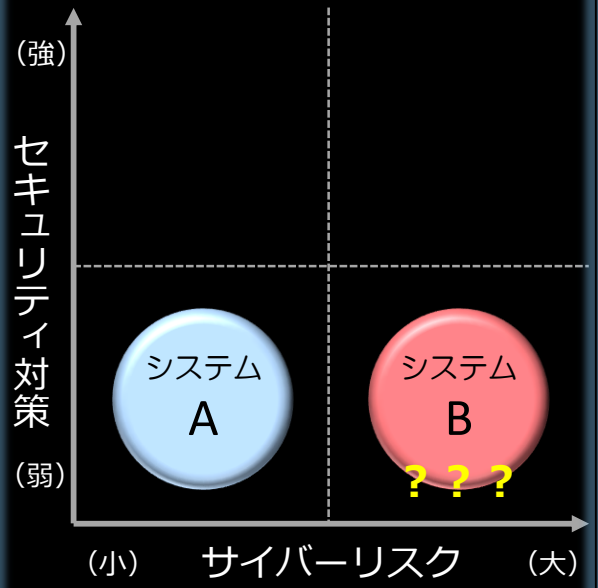
- 脅威の封じ込め
- 事業継続性（暫定）確保
- 原因分析、影響特定
- 再発防止策の実行、改善

サイバーリスクのアカウンタビリティ

説明責任　経営の透明性、健全性、適正性、遵法性を確保し、利害関係者に事態や対応方針などを説明する義務

責任追跡性　情報資産に行われたある操作についてユーザと動作を一意に特定でき、過去に遡って追跡できること

健全性／適正性



責任追跡性

- 事故発生時に５W1Hを明文化するための仕組みづくり
- 情報資産の定義と管理
- システム運用規定の確立
- 運用状態の記録
- 有事の際、運用状態の分析
- 平時の定点観測と定期報告

透明性

- 組織ぐるみ／個人的な過失
- 構造的／偶発（突発的）
- 嘘や隠蔽の有無
- 発表のタイミング
- 事象の再発性
- 経営者が理解した上で、分かり易く、誠実に、伝える努力

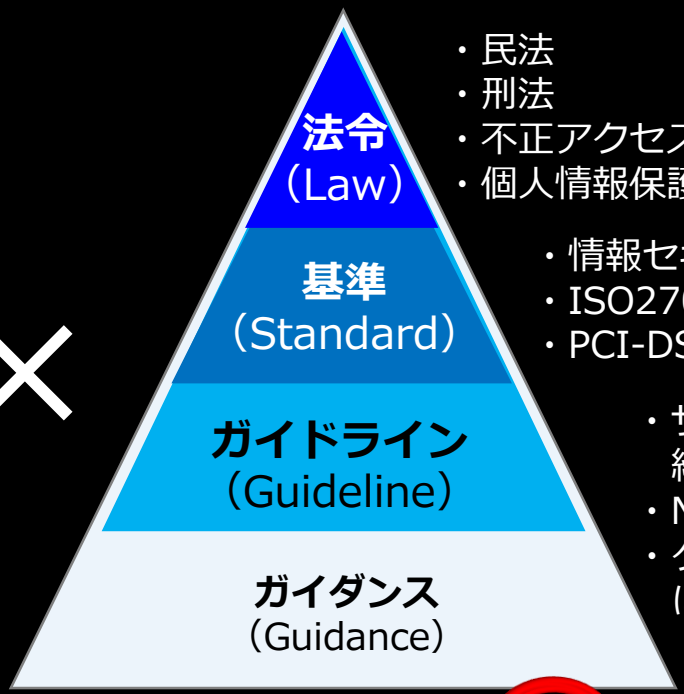
組織全体への戦略展開と一定レベルの実行力確保

CMMI	成熟度	プロセス	人／組織	技術
最適化している ■定量的評価のFB ■継続的カイゼン活動	5	経営課題の一環として継続的PDCAが確立した段階	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
定量的に管理された ■組織目標の設定 ■定量的な理解と制御	4	全社的な品質目標が設定され定量的な制御がある段階	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	事象に応じた対応策の明確化に基づく遠隔制御体制の確立
定義された ■標準化、統合化 ■組織的ノウハウ共有	3	本社統治の規定をベースに個別規定を融合した段階	適材適所のリソース配置 ■コア業務の見極めと外注による補強	ログ管理方法の標準化、分析ノウハウを統合するSIEM導入
管理された ■規律がある ■反復できる	2	本社指示による個別の繰り返し可能な規定に基づく	リスク管理体制の組織化 ■経営層（CISO）が関与した管理体制	情報資産やICT環境の現状把握とタイムリーな脆弱性管理
初期 ■場当たり的 ■個人の努力に依存	1	全社的に一貫性のない個別/非公式なルールに基づく	役割と責任の定義 ■必要なスキルセットの明確化	外部NWから侵害する既知脅威の侵入検知と防御

CMMI : Capability Maturity Model Integration　能力成熟度モデル統合

持続的な情報セキュリティガバナンスの確立

×



- 民法
- 刑法
- 不正アクセス禁止法
- 個人情報保護法

- 情報セキュリティ管理基準
- ISO27001
- PCI-DSS

- サイバーセキュリティ経営ガイドライン
- NIST SP800
- クラウドサービス利用に関するガイドライン

改善

環境変化

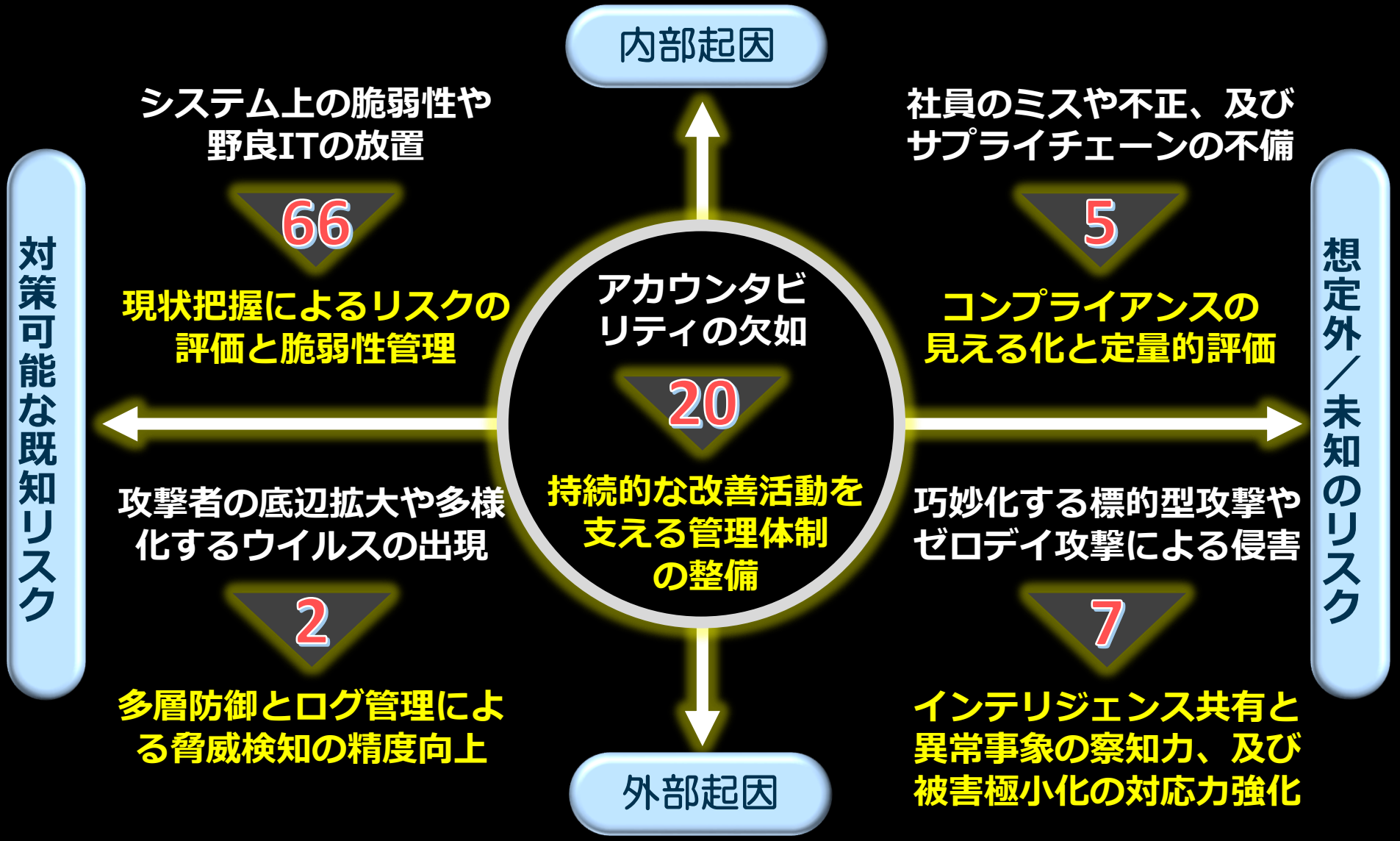
改訂

企業理念等に基づき、法令／基準／ガイドラインを
組み合わせて個社毎に最適な物差しを確立

健全性や適正性の
定期的な監査

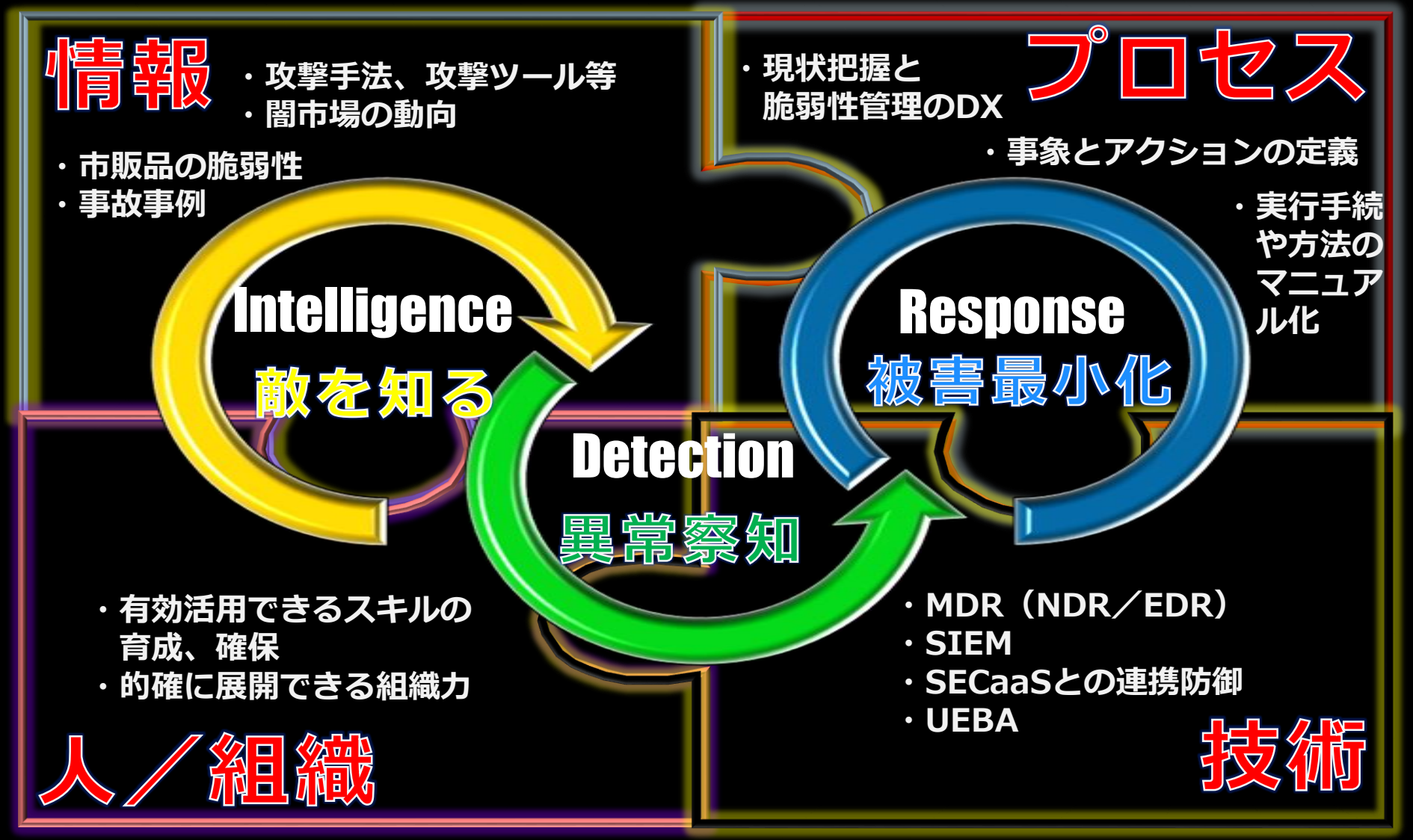
成熟度モデル

ゼロトラスト時代のサイバーリスク対応策



図中の数字はNIST SP800-53が定義するCIセキュリティ要件（18ファミリ240件）の分布状況（%）

ゼロトラスト時代のソリューションモデル



脅威インテリジェンスの活用術

インテリジェンスの情報ソース

人/組織向けインテリジェンス

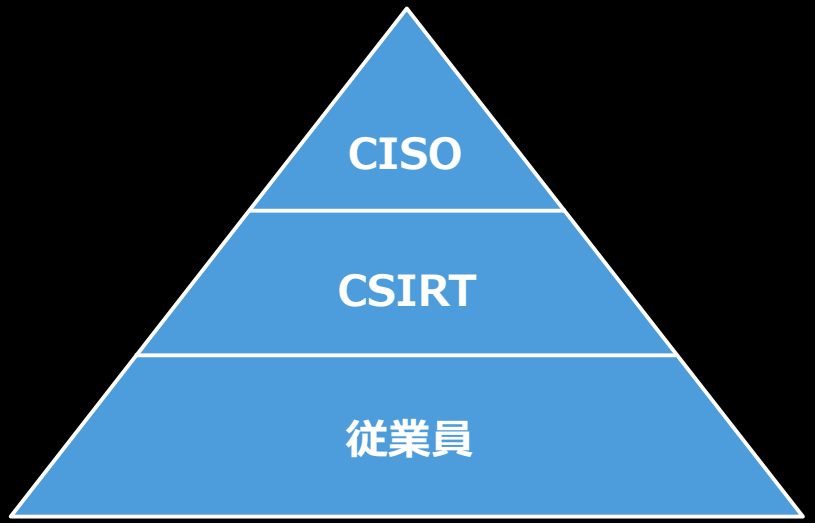
デバイス向けインテリジェンス

セキュリティコンサルタント

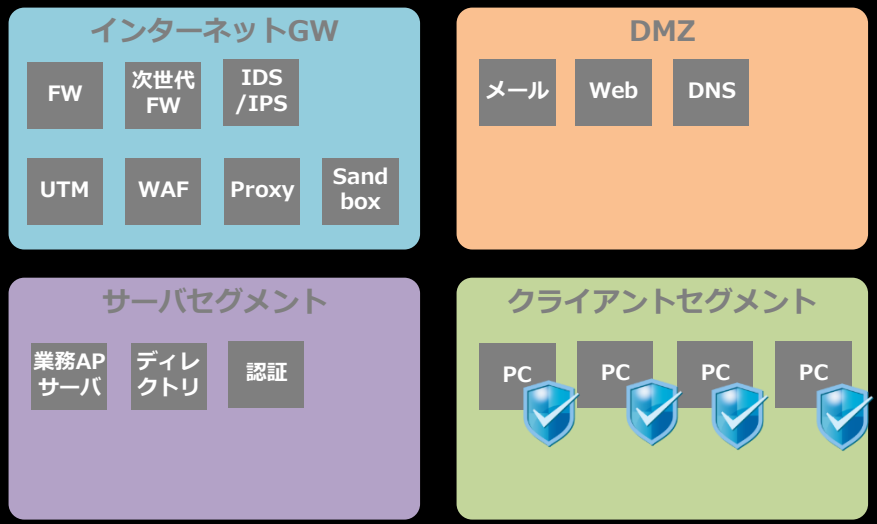
SOC

メルマガ、ニュース、レポート、見える化ツール

パターンファイル、シグネチャー、ブラックリスト



お客さま セキュリティガバナンス



お客さま ICT環境

MDR：Managed Detection & Response

セキュリティ運用管理工程

監視 → 検知 → 分析 → 通知 → 遮断・隔離 → 調査・根絶 → 復旧 → 改善・予防

MDRの種類と業務スコープ

高精度な脅威検出
迅速的確な遠隔制御

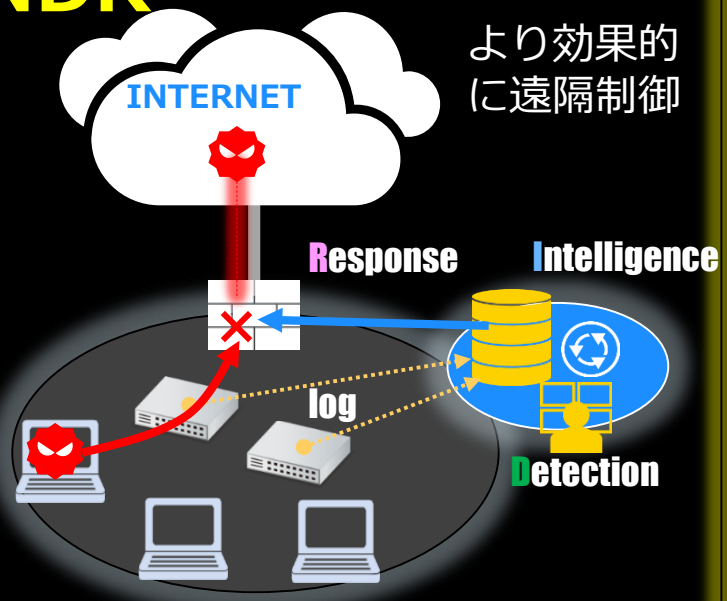
NDR
EDR

NDR:Network Detection & Response

EDR:Endpoint Detection & Response

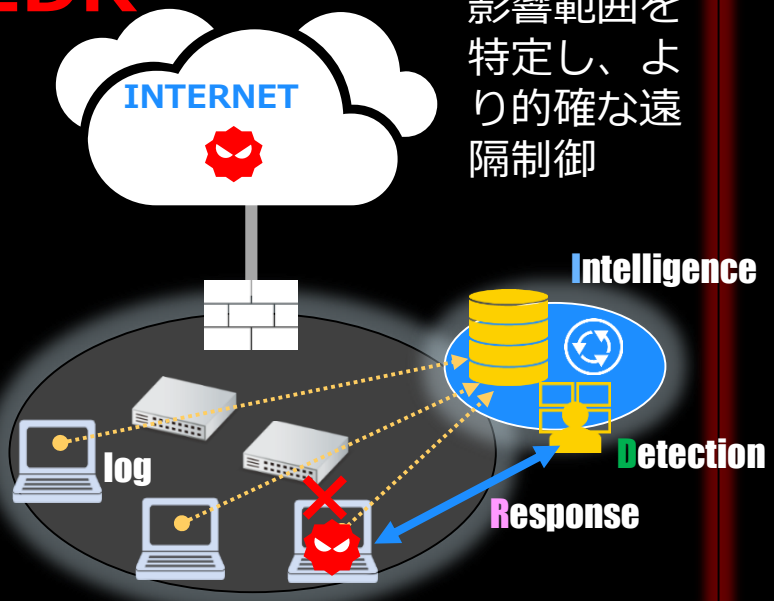
NDR

より効果的に遠隔制御



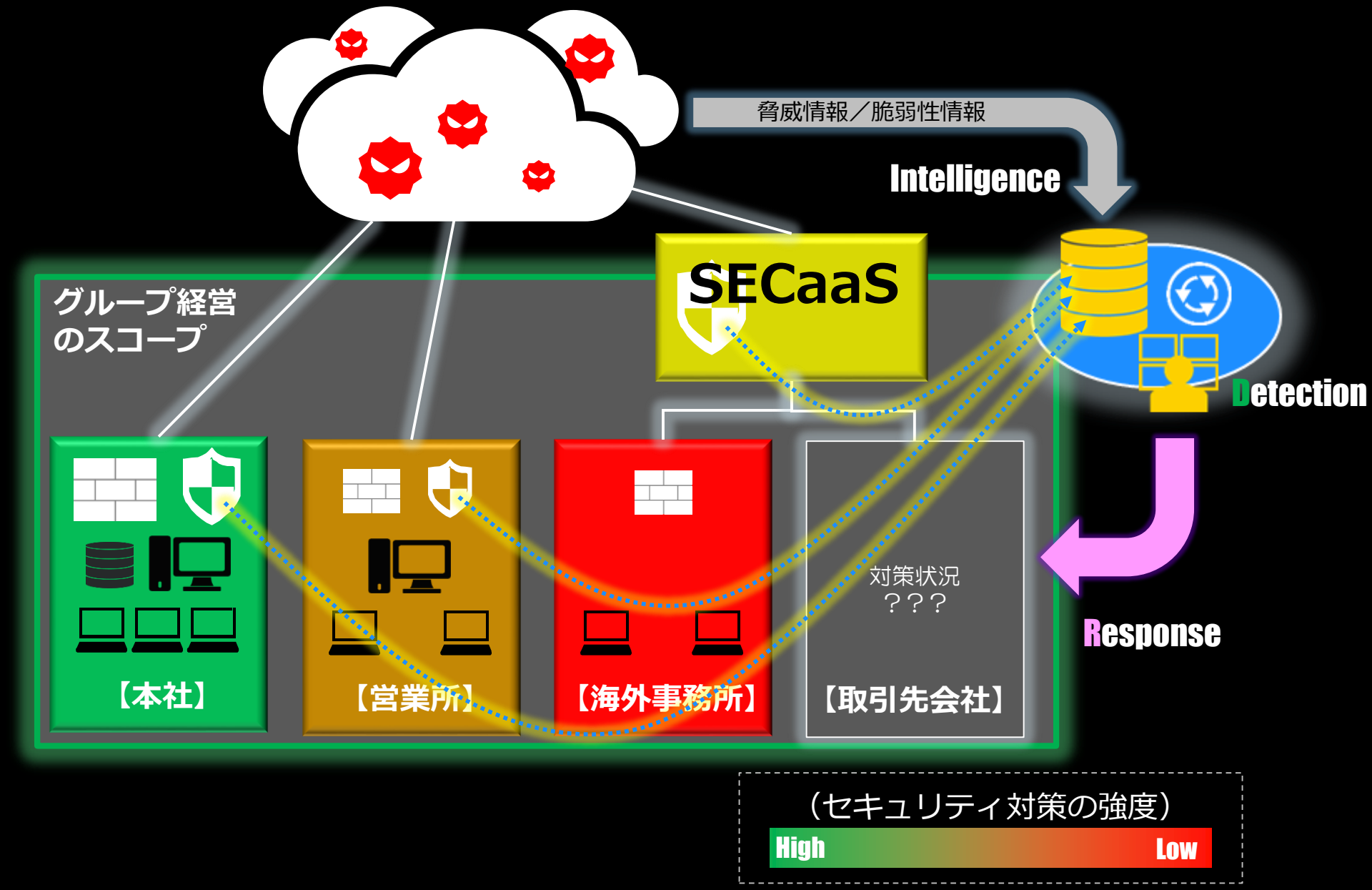
EDR

影響範囲を特定し、より的確な遠隔制御



グループ経営環境を効率的に守るSECaaSとの連携防御

SECURITY as a Service



まとめ

- ✓ DXにおけるゼロトラスト時代の認識
- ✓ リスク対応策を方向付けるアカウンタビリティ
- ✓ 持続的なガバナンス強化のためのRMF確立
- ✓ サイバーリスクの把握と対応策の展開
- ✓ ゼロトラスト時代のソリューションモデル

“Intelligence , Detection & Response”

ご清聴ありがとうございました

WIDE ANGLE

INFORMATION SECURITY AND RISK MANAGEMENT

免責事項

情報の正確性について
可能な限り正確な情報を掲載するよう努めていますが、最新性、正確性を保証するものではありません。

無断転載の禁止について
本資料にあります文章や画像、動画等の著作物の情報を無断転載することを禁止します。