NTT Communications
Transform. Transcend.

“IT戦略＝ビジネス戦略”の具現化を支えるリスクマネジメントの在り方

～レジリエンス強化に向けた５つの注力ポイント～

2018年9月20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

IT戦略がビジネス競争力を左右する!?

- 総合的な競争力の高い国はデジタル競争力が高い傾向に（Top10の内8カ国）
- 総合競争力は「経済やインフラ状況」の他に「ビジネスの効率性」等が指標

（IMD世界競争力ランキング2018より）

総合的な競争力（Top10）	*1	デジタル競争力 *2
米国	1 ↑	1 ↑
香港	2 ↓	11 ↓
シンガポール	3 →	2 ↓
オランダ	4 ↑	9 ↓
スイス	5 ↓	5 ↑
デンマーク	6 ↑	4 ↑
アラブ首長国連邦	7 ↑	17 ↑
ノルウェー	8 ↑	6 ↑
スウェーデン	9 →	3 ↓
カナダ	10 ↑	8 ↑

総合的な競争力（11位～20位）	*1	デジタル競争力 *2
ルクセンブルク	11 ↓	24 ↓
アイルランド	12 ↓	20 ↑
中国	13 ↑	30 ↑
カタール	14 ↑	28 →
ドイツ	15 ↓	18 ↓
フィンランド	16 ↓	7 ↓
台湾	17 ↓	16 ↓
オーストリア	18 ↑	15 ↑
オーストラリア	19 ↑	13 ↑
英国	20 ↓	10 ↑
日本	25 ↑	22 ↑

*1) 総合競争力の指標は、企業にとってビジネス環境の優位性について「経済状況」「政府の効率性」「ビジネスの効率性」「インフラ状況」の４つの指標で評価。
*2) デジタル競争力の指標は、デジタル技術の活用のために開発または適用されている度合いについて「知識」「技術」「将来への備え」の３つの指標で評価。

出典：IMD WORLD COMPETITIVENESS CENTER YEARBOOK 2018

DXがもたらすビジネス環境の光と影

DX＝デジタルトランスフォーメーション

様々なものが繋がる社会

情報を集約し利活用する社会

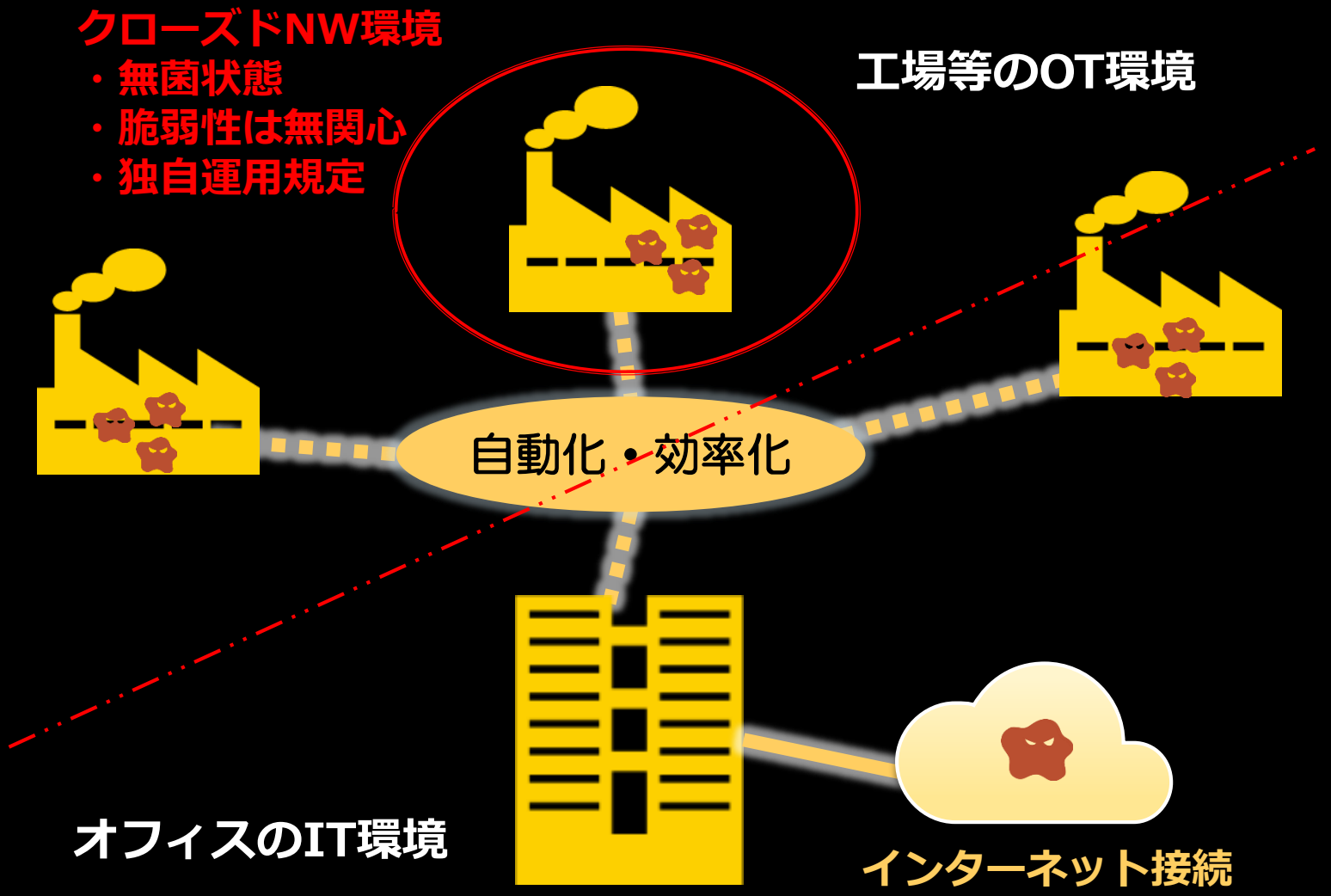
【好ましい影響】

- 新たな価値を創造する
- 新たな価値が市場を変革する
- 情報連携／活用し自動化する

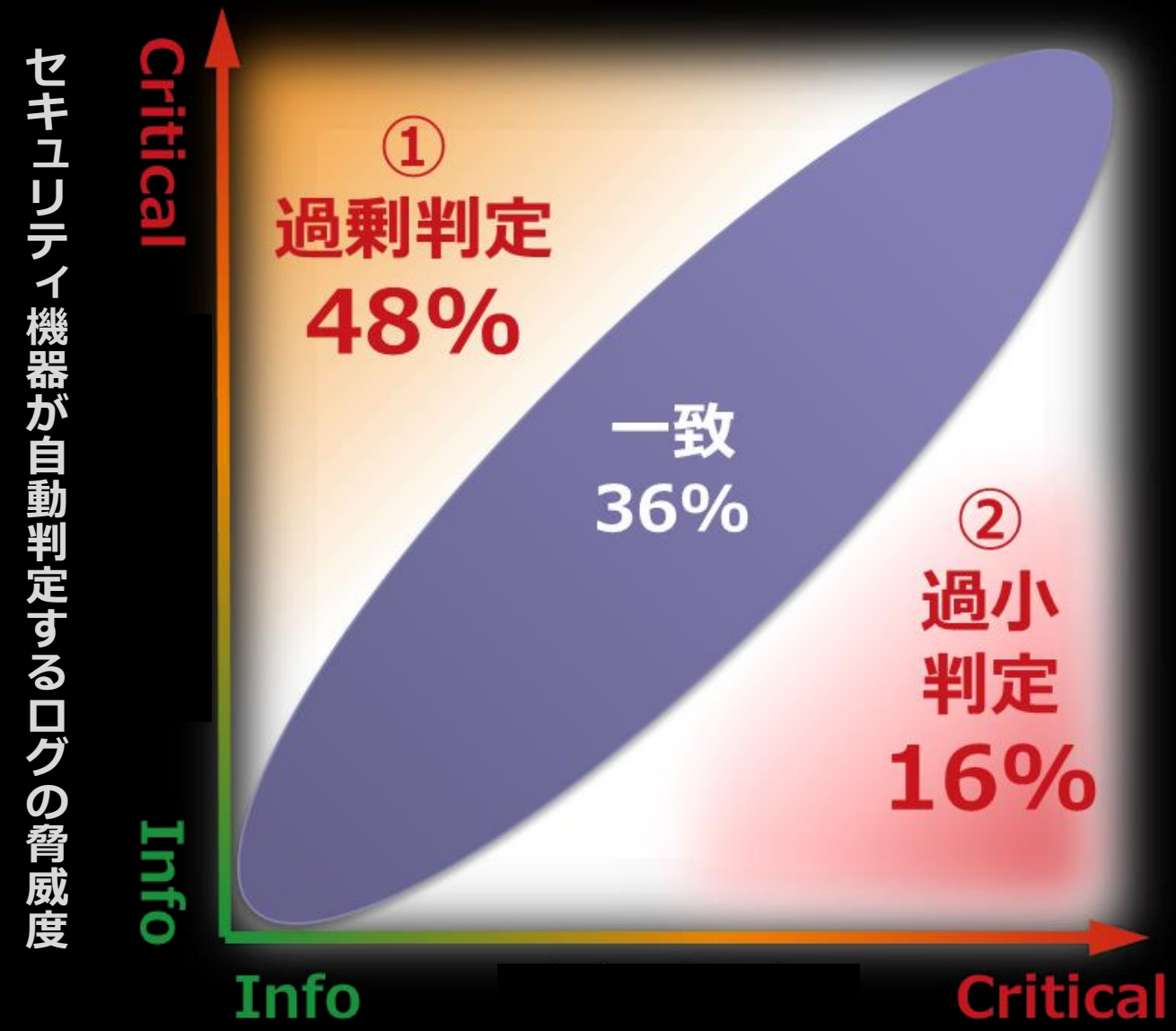
【好ましくない影響】

- 未知のリスクが発生する
- 潜在リスクが顕在化する
- 一撃で脅威が伝搬しダウンする

脆弱性の放置が業務停止を引き起こすリスク

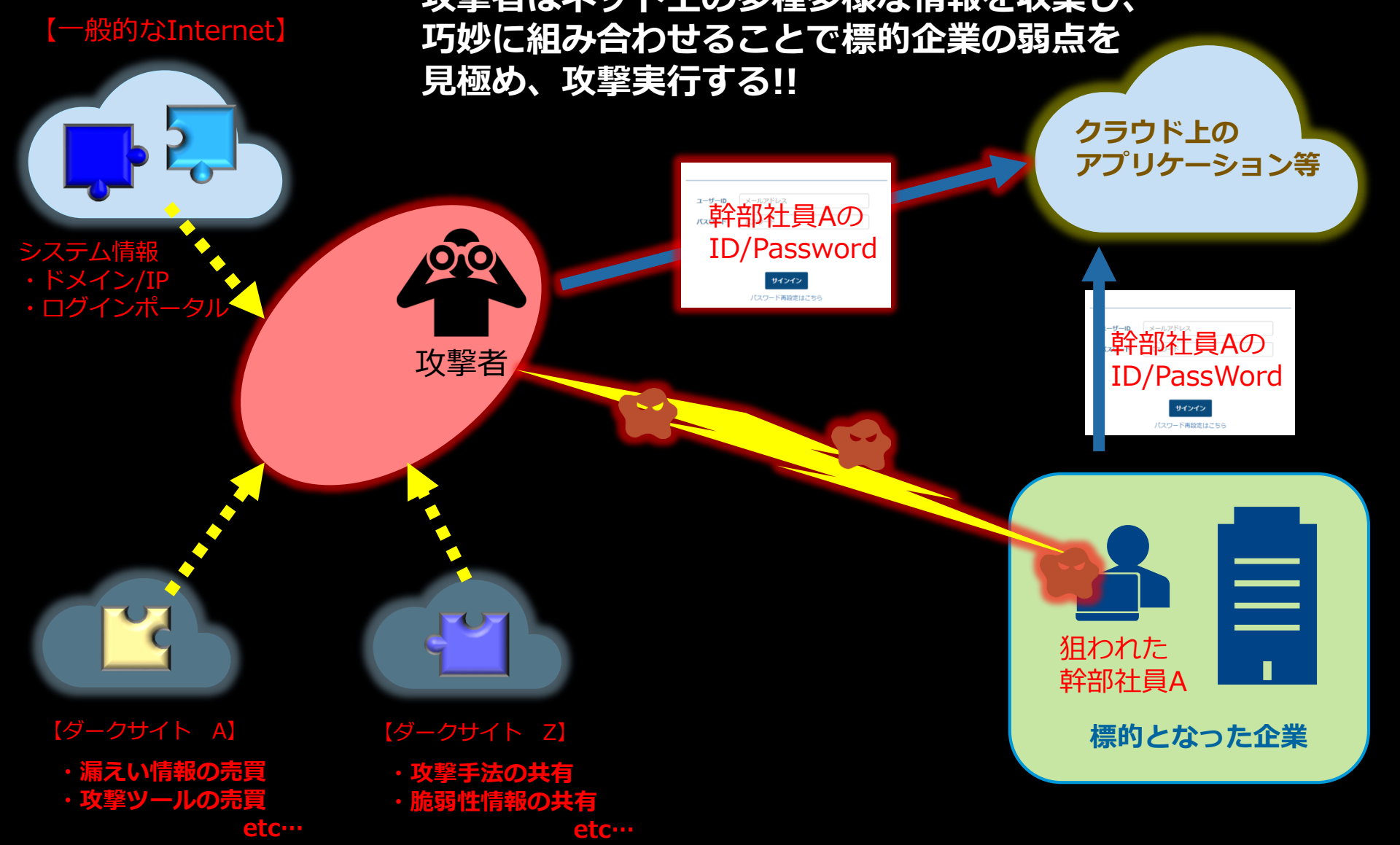


運用体制の不備がセキュリティ投資を無駄にするリスク



ネット上の情報を利活用する標的型攻撃のリスク

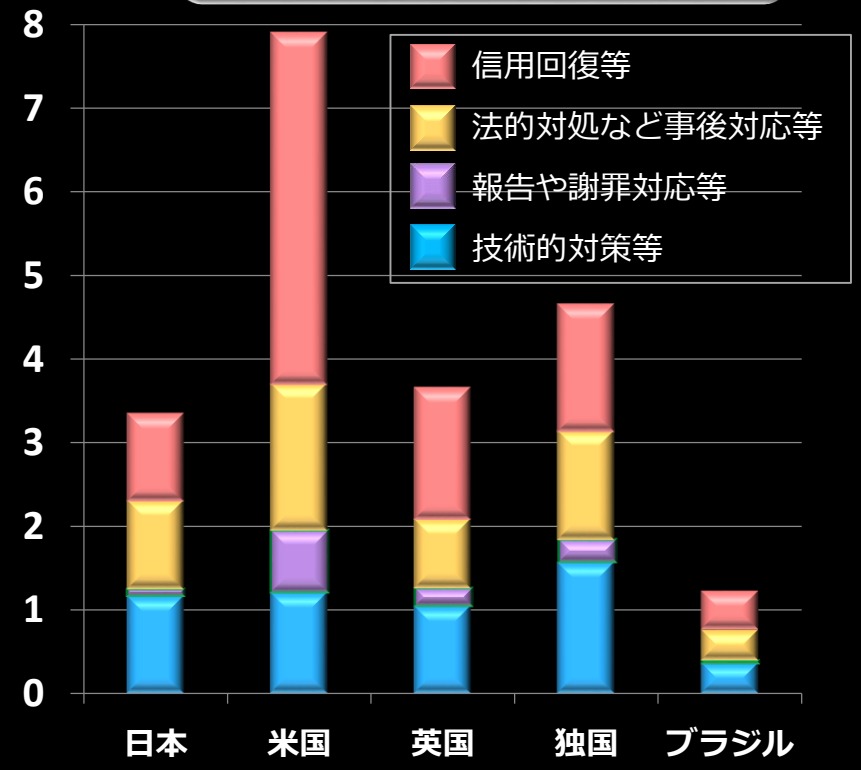
攻撃者はネット上の多種多様な情報を収集し、
巧妙に組み合わせることで標的企業の弱点を
見極め、攻撃実行する!!



情報漏洩事故の実態と加害者化のリスク

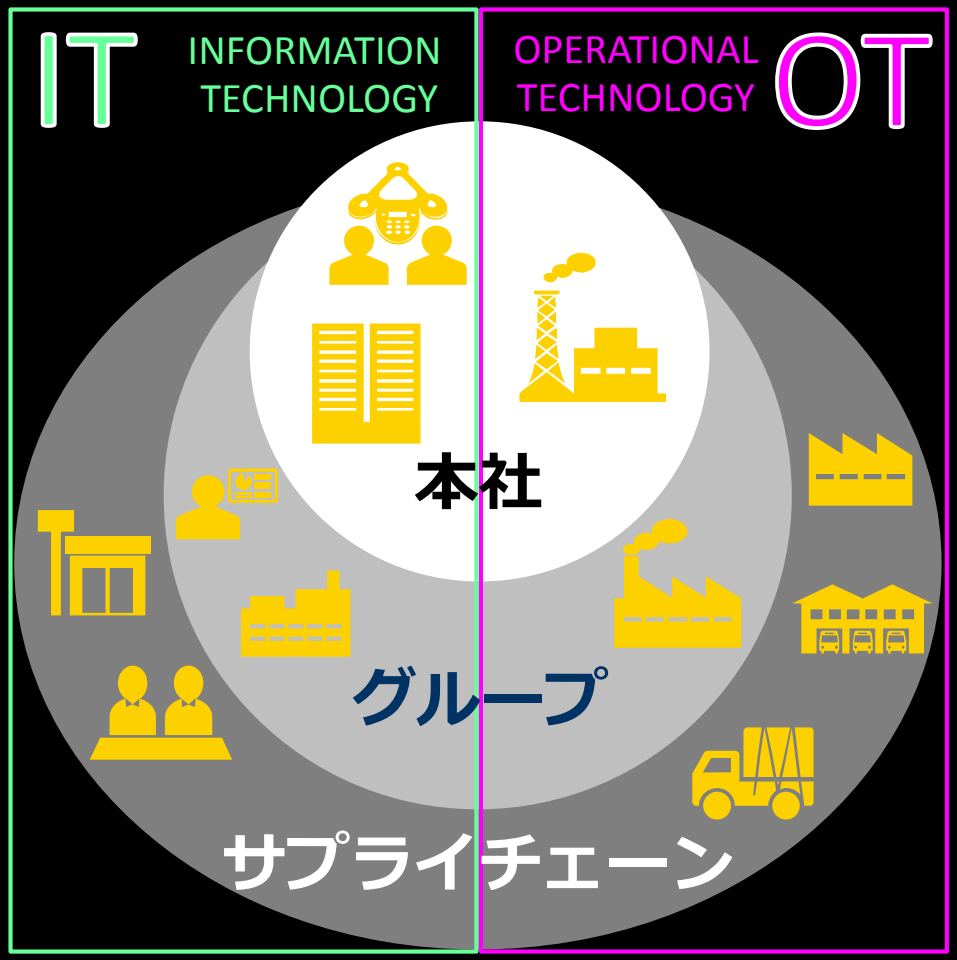
10万人規模の情報漏洩事故の経営インパクト

（2017年、15か国/477件の平均値）
4.3億円



出典：2018年7月　Ponemon Institute
「The　2018 Cost of Data Breach Study: Global Overviiew」

サプライチェーンの事故で経営責任を問われるリスク



【2017年11月】
経済産業省がサイバーセキュリティ経営ガイドラインVer. 2.0を公表。
「指示9ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」に、サプライチェーン対策強化に関する記載を追記。

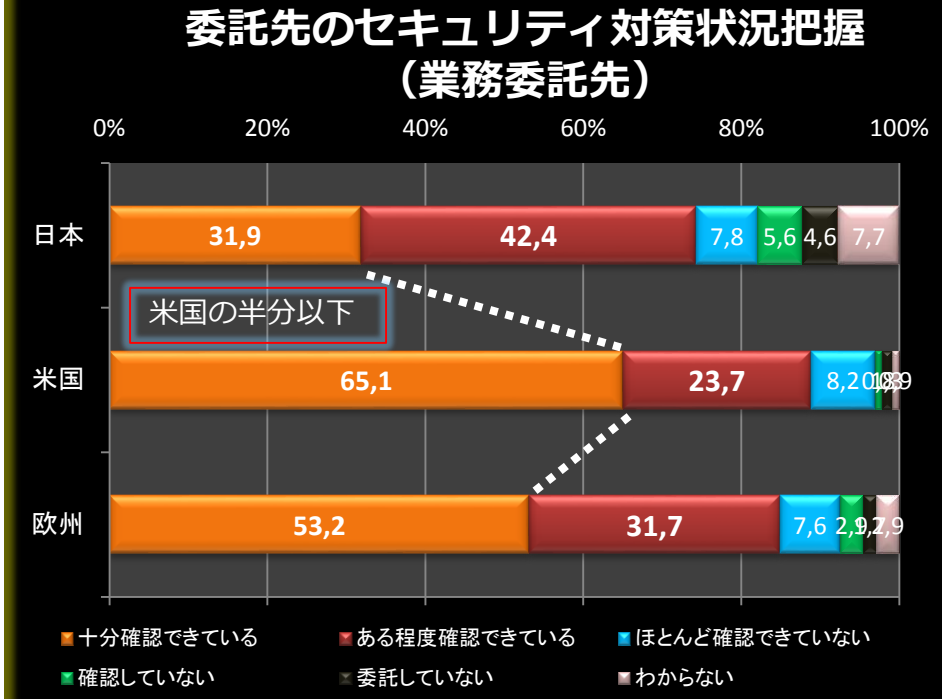
【2017年12月】
NISTがCybersecurity FrameworkのVer. 1.1_Draft2を公表。
Draft1のパブリックコメントを踏まえサプライチェーンのリスク管理の重要性を強調。

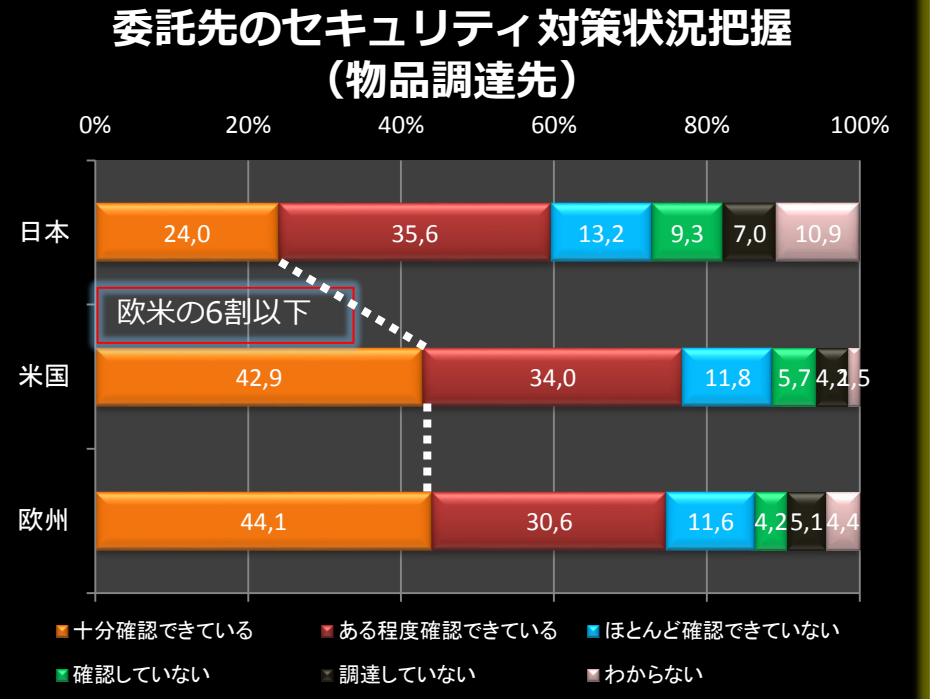
NIST：米国国立標準技術研究所

委託先のセキュリティ対策は大丈夫ですか？

・日本は欧米と比してサプライチェーン（委託先/調達先）のセキュリティ対策状況を把握できていない。

➡ 委託先/調達先企業に起因するセキュリティ事故リスクが高い





出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017」調査報告書（2017年4月13日）
・日本、米国、欧州（英・独・仏）の従業員数300人以上のCISO/情報システム/情報セキュリティ責任者/担当者等にアンケートを実施（2016年10~11月）
・有効回答は日本（755件）、米国（527件）、欧州（526件）

2018年4月　経済産業省 サイバー産業研究会 資料（商務情報政策局 作成）より抜粋

セキュリティ事故発生時の説明責任は果せるか！？

「いつ、誰が、どこから、何で、何を、どうした」を説明する

- 情報資産の管理（情報種別や保管場所）
- ID管理とアクセス制御（誰が、何に、アクセスできる）
- 情報流通の制御（何を媒介して、流通の範囲は）
- ログ収集（可用性）
- ログ管理（職責分離と相互監視による機密性と完全性）
- 分析体制の準備（高スキル者のタイムリーな運用）　等々

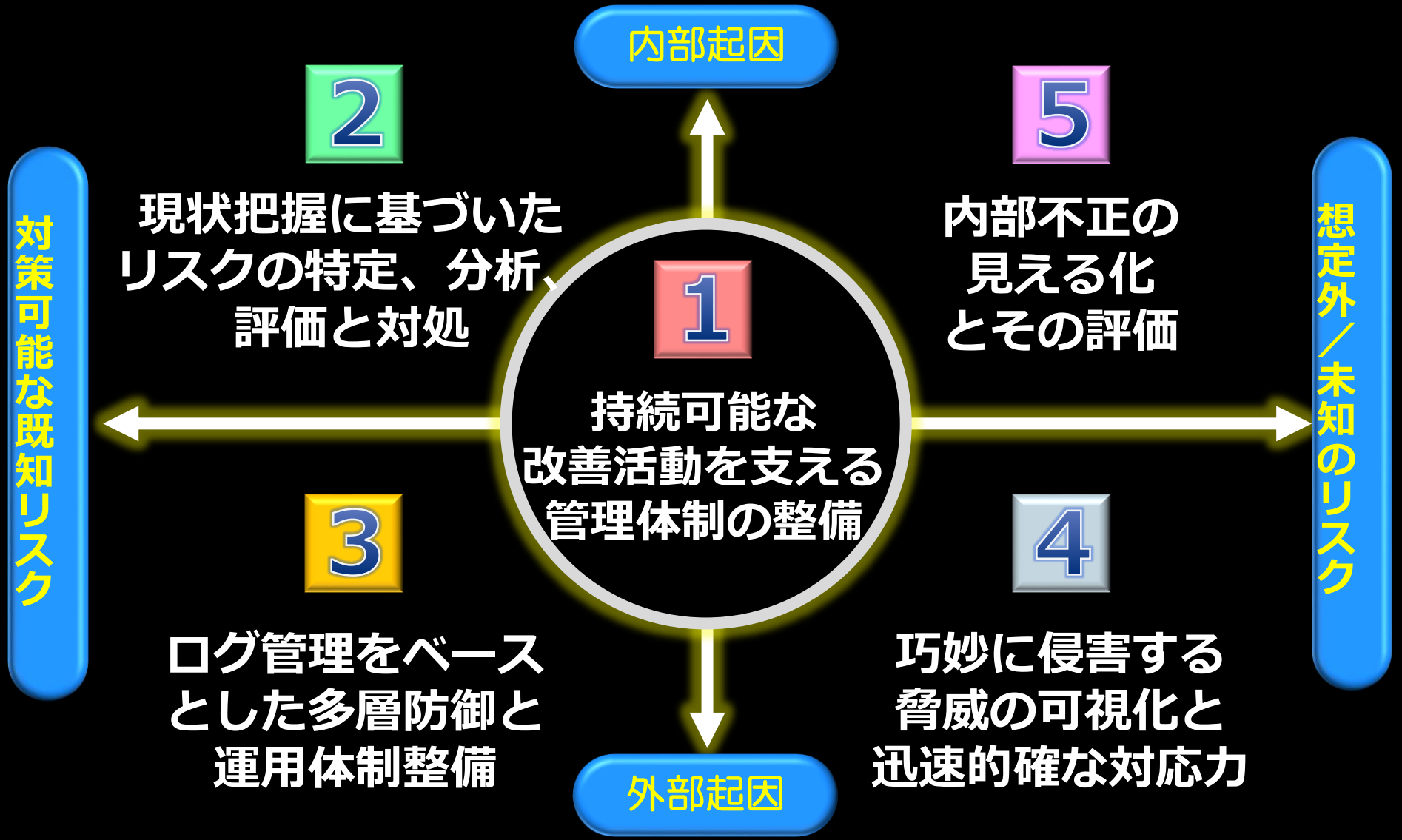
Accountability(説明責任)
＝会計用語＝

行政・企業などが業務内容について対外的に説明をする責任

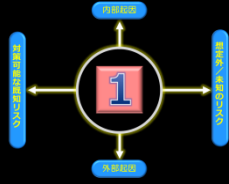
Accountability(責任追跡性)
＝情報セキュリティ用語＝

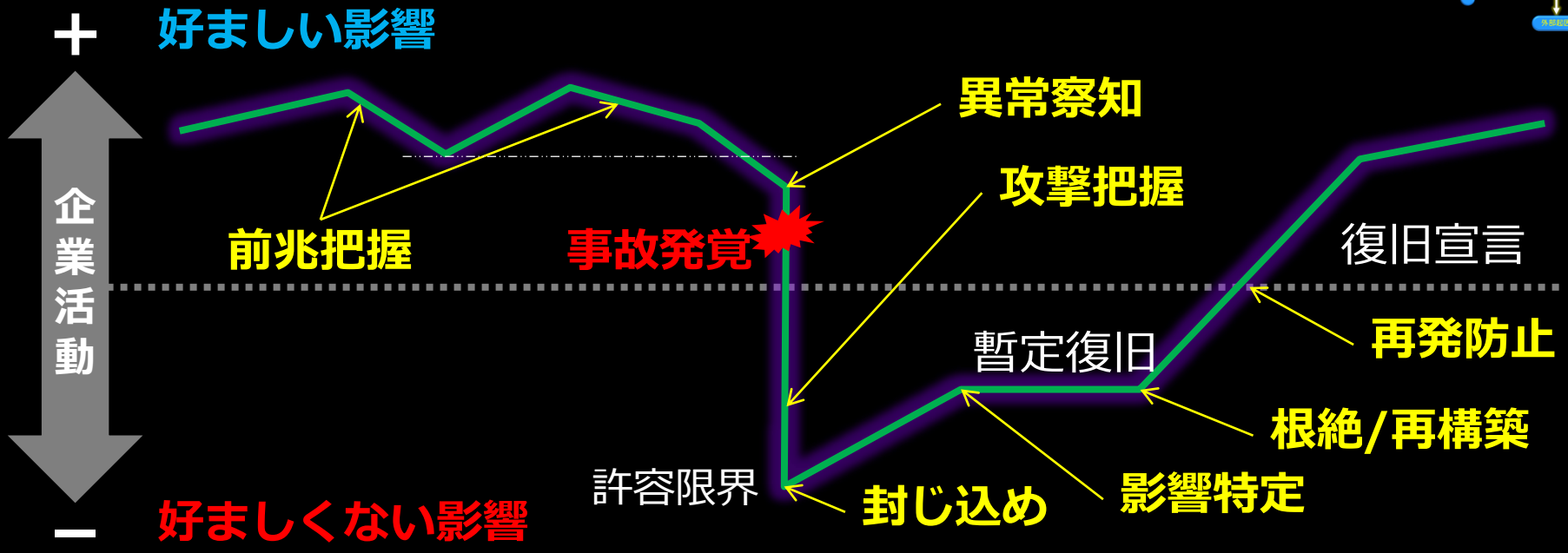
情報資産に行われたある操作についてユーザと動作を一意に特定でき、過去に遡って追跡できること

レジリエンス強化に向けた５つの注力ポイント



持続可能な改善活動を支える管理体制の整備





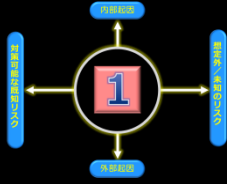
リスクマネジメントのスコープ

【平常時】
- 正常性把握、定期的な公表
- 持続的なカイゼン活動
- 事故を前提とした準備

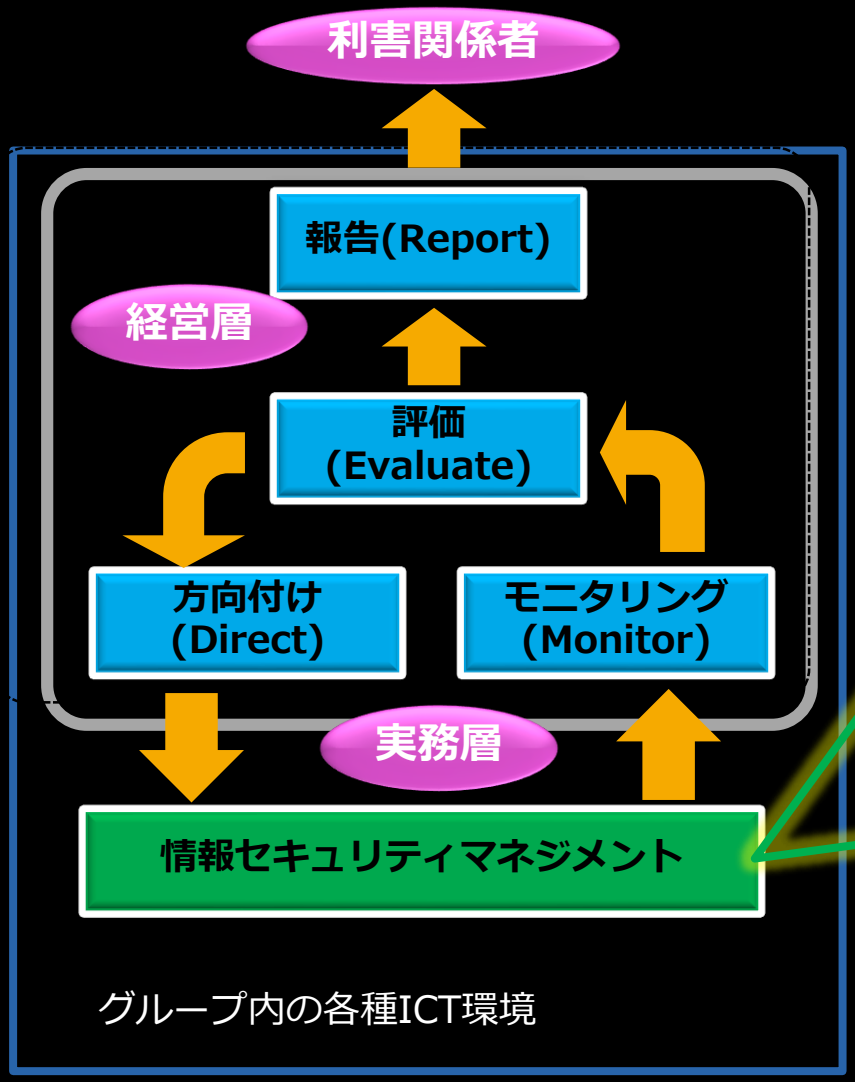
【事故発覚～復旧】
- 影響範囲の最小化
- 事業継続（再開）の対処
- 復旧宣言に向けた取り組み

事後スタートの危機管理

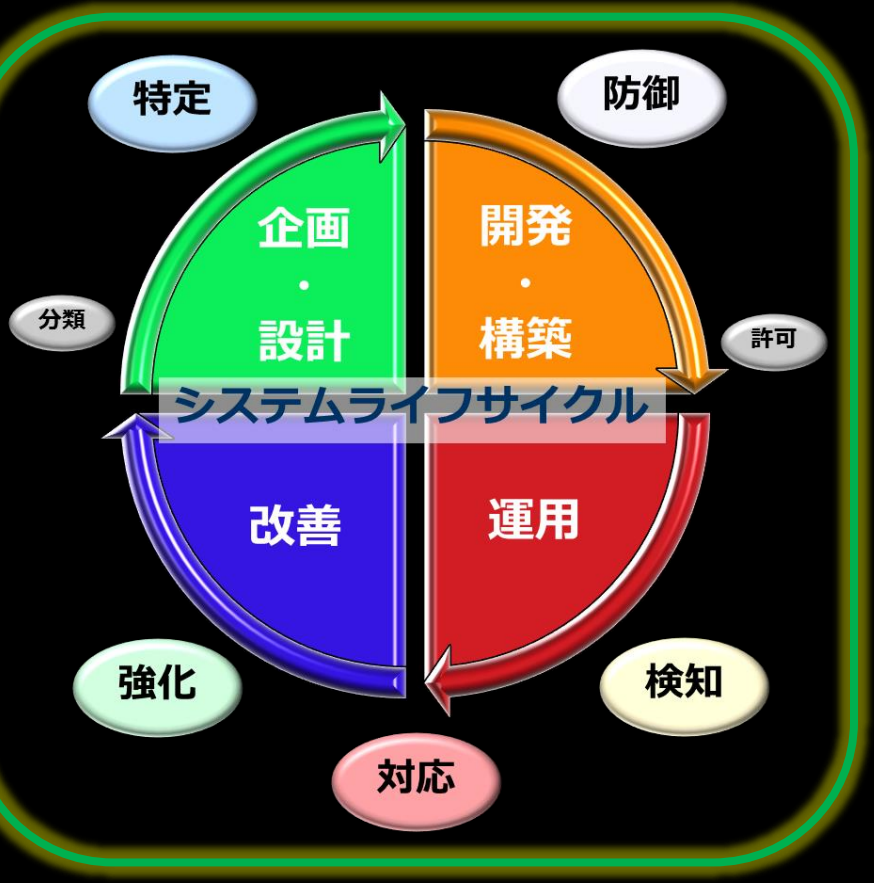
平常時における改善サイクルの確立



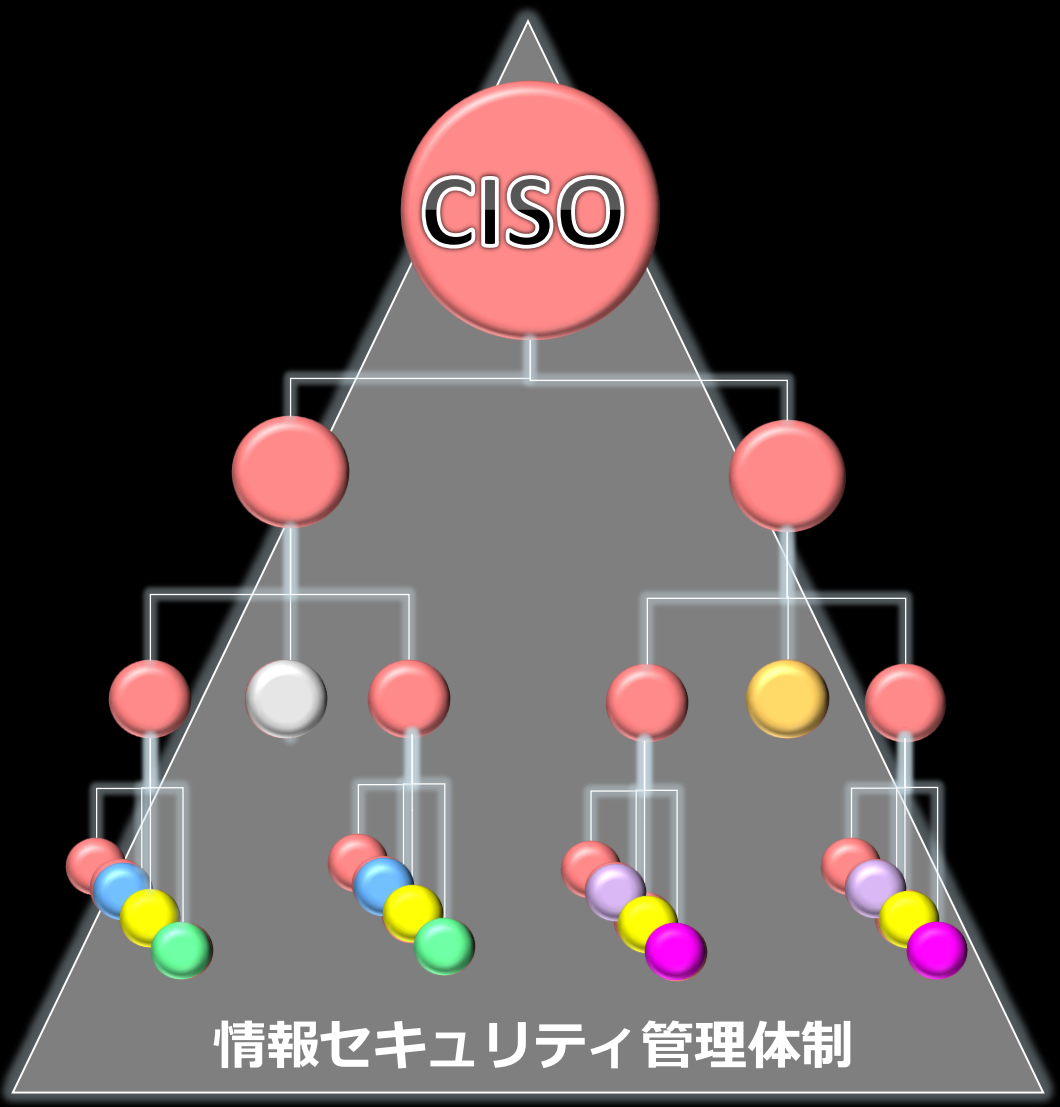
【グループ全体の改善サイクル】



【システム単位の改善サイクル】

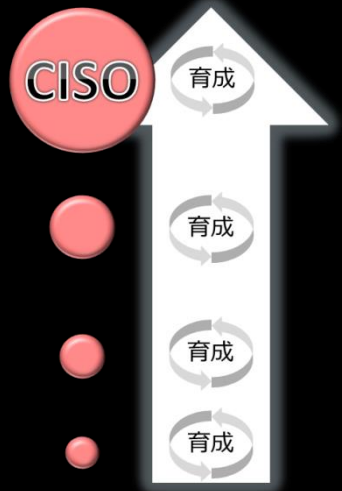


管理体制のコア業務を見極めて実行力を強化する



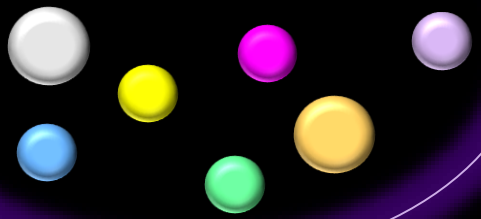
●：役割／職務

処遇制度の確立と社員教育の実行

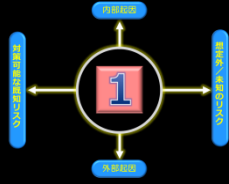


＋

アウトソーシング戦略の展開



セキュリティ事故時の説明責任を担保する体制化



戦略的

短期的

長期的

技術的

戦略・管理

- 戦略立案
- 予算管理
- 監督／監査
- 事業継続性／危機管理
- 経営や利害関係者への報告

etc　・・・

CSIRT

- 教育・演習計画／実行／評価
- インシデント対応活動の指揮
- 情報統制

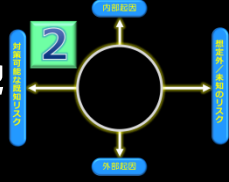
etc　・・・

情シス（委託先）

- セキュリティ機器の導入／運用
- 管理基盤の導入／運用
- インテリジェンスの集積／発信
- IR対応（検知、分析、フォレンジクス等）

etc　・・・

現状把握に基づいたリスクの特定、分析、評価と対処



・社員教育（性善説から性悪説へ）
・NWのマルチセグメンテーション

リスクを低減する

リスクの回避

発生する可能性を低減する

リスクの除去

・構成管理と脆弱性対策
・不要ポートの閉塞

発生時の影響を低減する

・BCP導入
・重要リソースの分散配置
・データ保護、暗号化

リスクをとる

リスクの共有（移転）

・保険
・クラウド利用
・SOCなどアウトソーシング

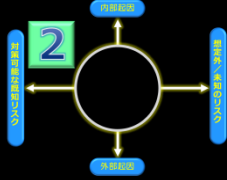
リスクの保有（許容）

リスクが発生する可能性
【脅威】×【脆弱性】

リスク発生時の影響の大きさ
【資産価値】

（参考：ISO31000におけるリスク対応の７つの選択肢）

攻撃者の視点からみたIoT環境の侵害ポイント



【risk⑧】
DMC内の内部不正

正規化
分析
補完／新価値創出
情報発信
収集／蓄積
セキュリティ等
NFV
データ管理センタ
（DMC）

【risk④】
センサーが
加害者化

【risk⑤】
センサーが
DMCへ
不正アクセス

【risk⑥】
外部からDMCへ不正アクセス

【risk⑦】
製造現場等の
内部不正

【risk③】
外部からセンサーへ
不正アクセス

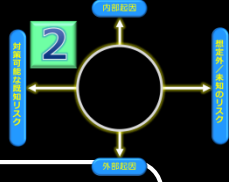
GW

【risk②】
センサーの
改造と悪用

IoT
IoT
IoT

【risk①】
センサーへの
脅威の埋め込み

リスク低減の要は煩雑な脆弱性管理業務の効率化



【経営者】
事業継続判断

報告
指示（システム停止など）

【CSIRT】
ICT環境全体の脆弱性把握

【システム管理者】
脆弱性対応

パッチ適用
システム停止

脆弱性
システム(A)
システム(B)
システム(C)
脆弱性
システム(Z)

ルールベースやプロセスなどの定義

報告

登録

対策対象一覧
1.システム(A)
- OS: STU - AP:XYZ
リスクレベル=3
対処=XX
2.システム(B)
- OS: STU - AP:XYZ
リスクレベル=5
対処=YY

情報更新

マッチング

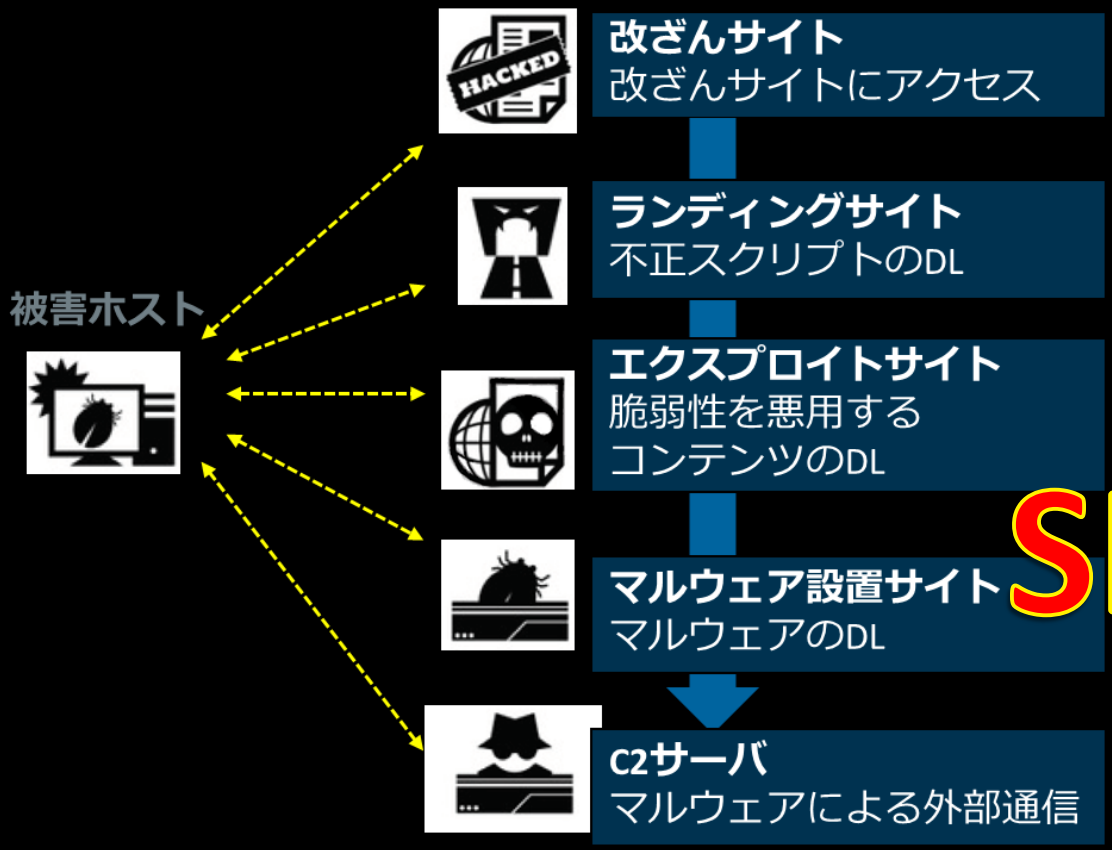
資産管理DB

脆弱性DB

ログ管理をベースとした多層防御と運用体制整備

【従来】　セキュリティ製品の多層化でパターンマッチング機能を向上

【今後】　SIEMと高度分析の運用体制を確立し脅威の検知精度を向上



不正や異常なアクセスをリアルタイムに検出し写真を撮るように記録

SIEM

侵害された端末と攻撃者サイトの通信を映像を撮るように記録

SIEMによるログ分析で巧妙な攻撃を可視化する

SIEM (Security Information Event Management)

４４１億件 (＊1)

ログ／パケット収集

ICT環境のログを収集し相関分析の環境を提供

１３００万件 (＊1)

分析エンジン

独自の分析アルゴリズムで潜在的リスク等を可視化

３４４件 (＊1)

アナリスト分析

イベントログを詳細分析し危険度や誤検知を判断

通知

(＊1)SOC顧客実績（約150件）
集計期間：2018年4月

AI技術の導入

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。

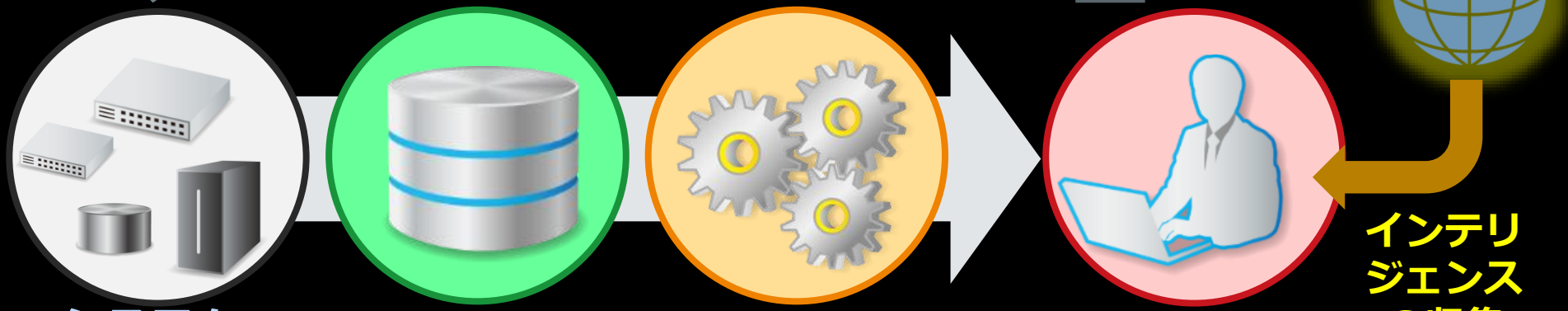
能動的な防御機能が求められるSOC現場の実態

SOC (Security Operation Center)

・脆弱性情報／攻撃手法
・マルウェア解析情報
・グローバルでの検知状況
・実際のアラート解析結果

カスタムシグネチャと
ポリシーチューニング

分析ルールや
アルゴリズムの更新



システム
構成機器

ログ集積

ログ分析

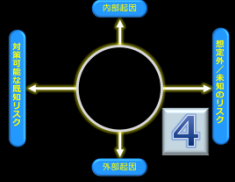
アナリスト

インテリ
ジェンス
の収集

ハニーポットなど
で捕捉したマウェ
アの解析情報

ブラックリスト

巧妙に侵害する脅威の可視化と迅速的確な対応力



情報

・標的となる個別の脅威
・攻撃者（組織）の動向
・脆弱性、攻撃ツール、攻撃手法

プロセス

・事象とアクションの定義
・アクション体制の準備
・実行手続や方法のマニュアル化

Intelligence
敵を知る

Response
被害最小化

Detection
異常察知

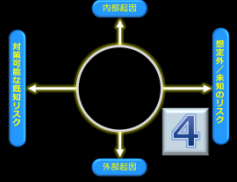
人

・有効活用できるスキルの育成、確保
・的確に展開できる組織力

技術

・高精度な脅威検知（SIEM）
・MDR／EDR
・ハニーポッド
・マルウェア解析

攻撃者優位に対するインテリジェンスの有効活用



攻撃者の行動パターン

偵察 → 準備 → 配送 → 攻撃 → 実装 → 操作 → 達成

攻撃者コミュニティ
の攻撃情報を掴む

いま活動している
攻撃サイトのブラックリスト

攻撃手法の把握

適材適所でインテリジェンス活用

MDR：Managed Detection & Responseとは

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

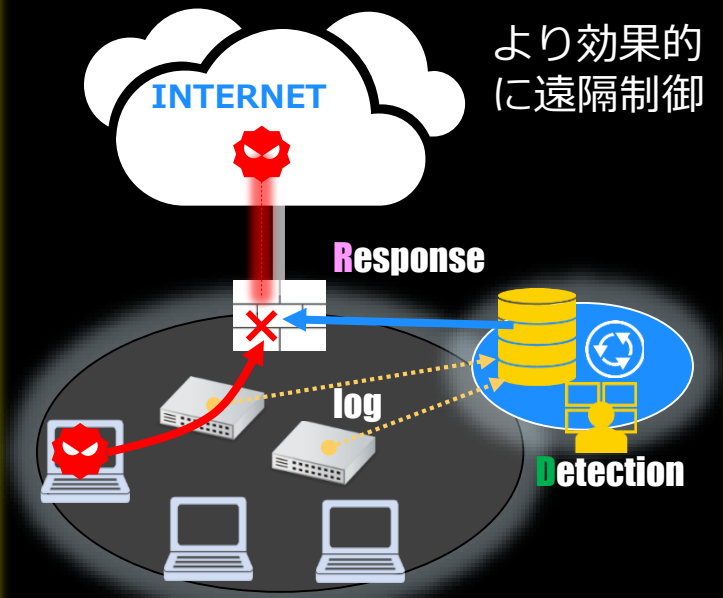
高精度な脅威検出
迅速的確な遠隔制御

NW型MDR

EDR

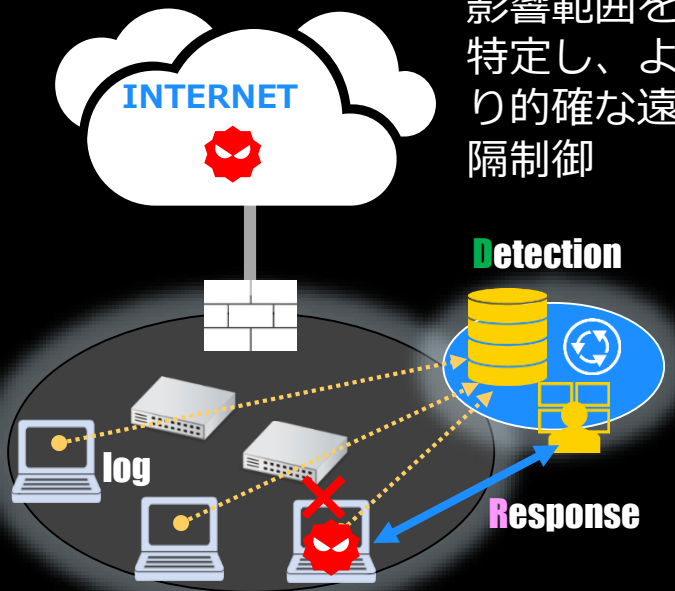
EDR:Endpoint Detection & Response

NW型MDR



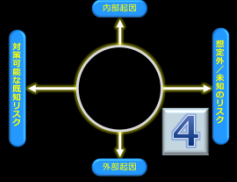
より効果的に遠隔制御

EDR



影響範囲を特定し、より的確な遠隔制御

グループを守るインテリジェンス共有と連携防御



脅威情報／脆弱性情報

Intelligence

グループ
セキュリティ
共通基盤

グループ経営
のスコープ

Detection

Response

【本社】

【営業所】

【海外事務所】

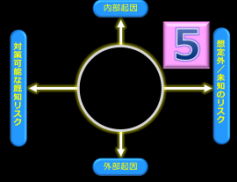
対策状況
？？？

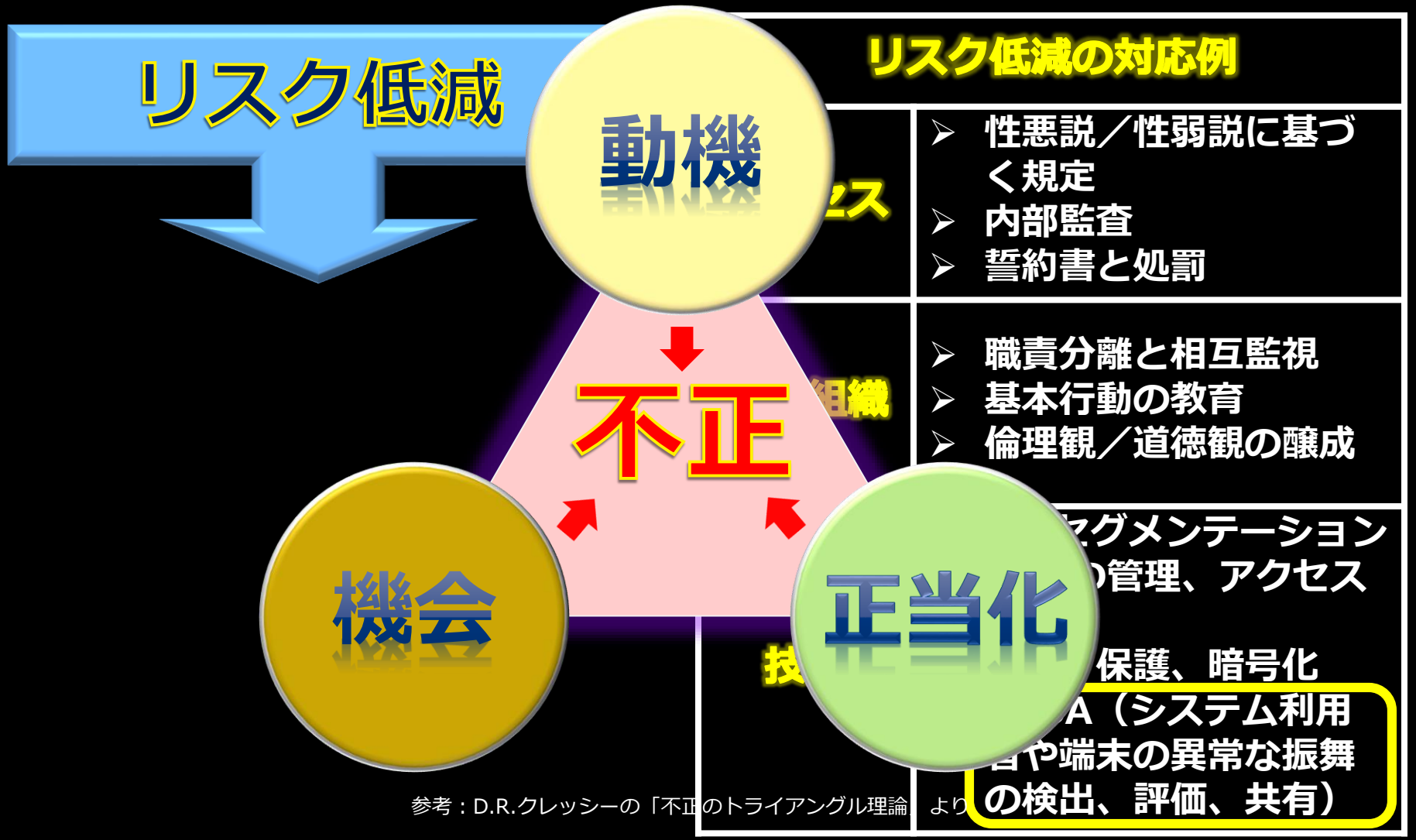
【取引先会社】

（セキュリティ対策の強度）

High Low

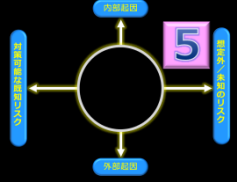
内部不正の見える化とその評価

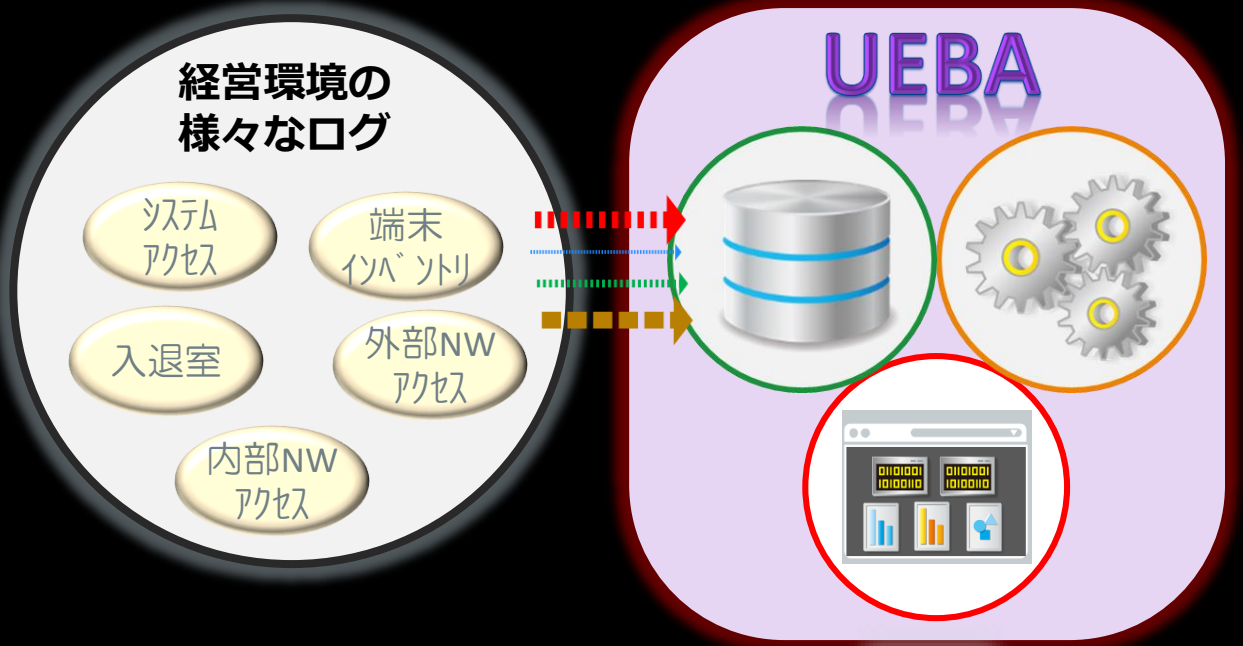




参考：D.R.クレッシーの「不正のトライアングル理論」より

UEBA : User & Entity Behavior Analytics





- ✓ **異常な振る舞い、兆候**
- ✓ **確信犯／過失の挙動**
- ✓ **未知マルウェアの侵害**
- ✓ **システム環境の設定不備**

etc・・・

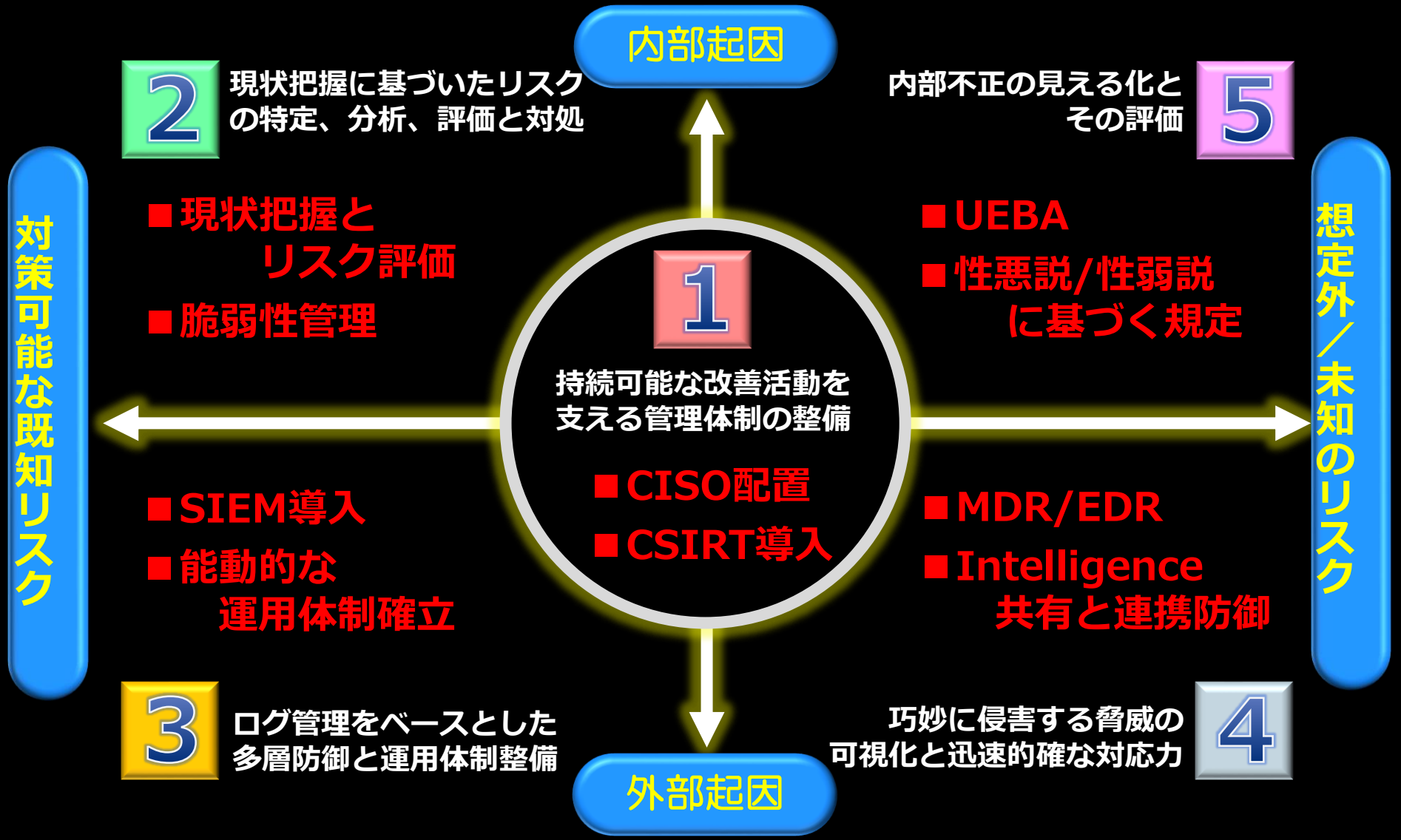
【経営者】

コンプライアンス管理の他、社員満足度や経営環境の脆弱性を把握

【社員等】

監視の明示による不正抑止しと、セルフサービスでコンプラ違反を認識

（まとめ）５つの注力ポイントと対応策のキーワード



ご清聴ありがとうございました