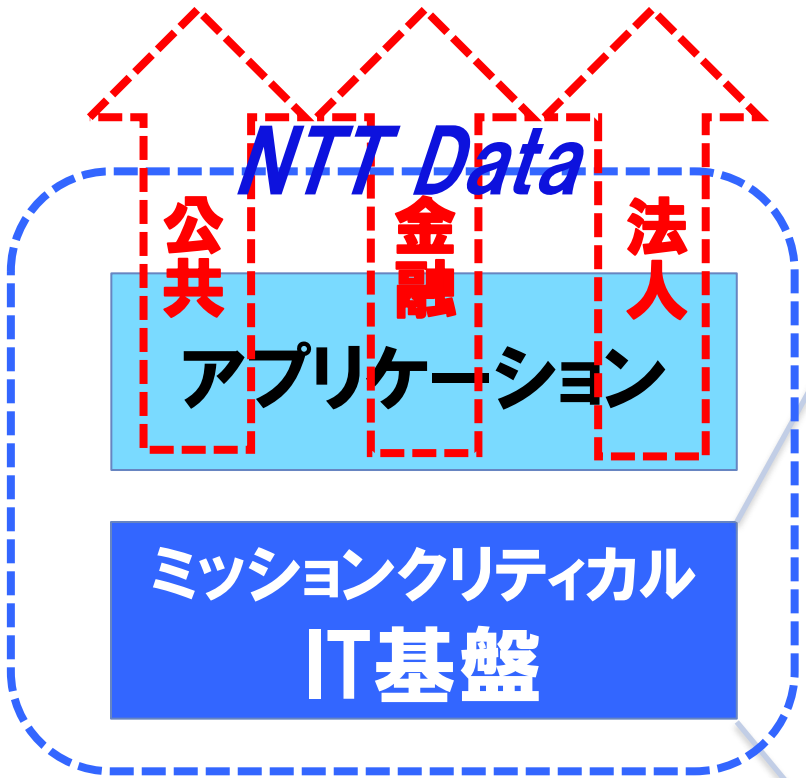
テリロジー社講演

経営層のための情報セキュリティ

2016年11月15日
NTTデータ先端技術株式会社
代表取締役社長、CISSP　三宅功

NTT DATA
NTTデータ 先端技術株式会社

NTTデータ先端技術とは？



2011．7

NTT データ先端技術

- プラットフォーム事業部
- Blue3事業部
- オラクル事業部
- ソリューション事業部
- ITアウトソーシング事業部
- セキュリティ事業部
- 環境テクノロジ事業部

とんでも事例　ー　笑えない話(ごく一部)

NTT DATA

■ Webサーバがハッキングされ、IRが要請される。
→早期のサービス再開が要請されたためWAFを入れる。
→後で、請求書を持っていったら、「払えない、会社がつぶれる」と言われた。

■ 標的型攻撃により大規模に個人情報が漏えい。マルウェアはメール経由で拡散したことが特定された。
→数カ月間、メールサービスを停止。その間、業務は電話とFAX

■ プリンタに寄生するマルウェアが発見された。
→で、社内システムを１日止めた。

■ ランサムウェアにやられた
→「ビットコインで支払え」と言われたが、支払方法がわからず期限切れ。

■ セキュリティ対策でUTMを入れた。
→入れただけで、ログも見ず、シグニチャもパッチもアップデートしてなかった。
→で、やられた

■ ある大手セキュリティベンダさんがAPT対策製品を売り込みにきた
→ところで、その製品御社の中で活用されてますか？と聞いてみた
→答えが返ってこなかった

■ CISOやれと言われました。
→その前は、法務担当。ハッカー雇えばいいんでしょうか？と聞かれた。

経営視点で考えると

NTT DATA

【顕在化しているリスク】

・業務委託管理：協力会社社員等委託先を含めた情報セキュリティ管理

・外部に向けたWebサーバのセキュリティ管理

【潜在的なリスク】

・自社開発環境及び、クラウドの利用時のセキュリティ管理と
　→機密情報の流出だけでなく、危ないのは踏み台化

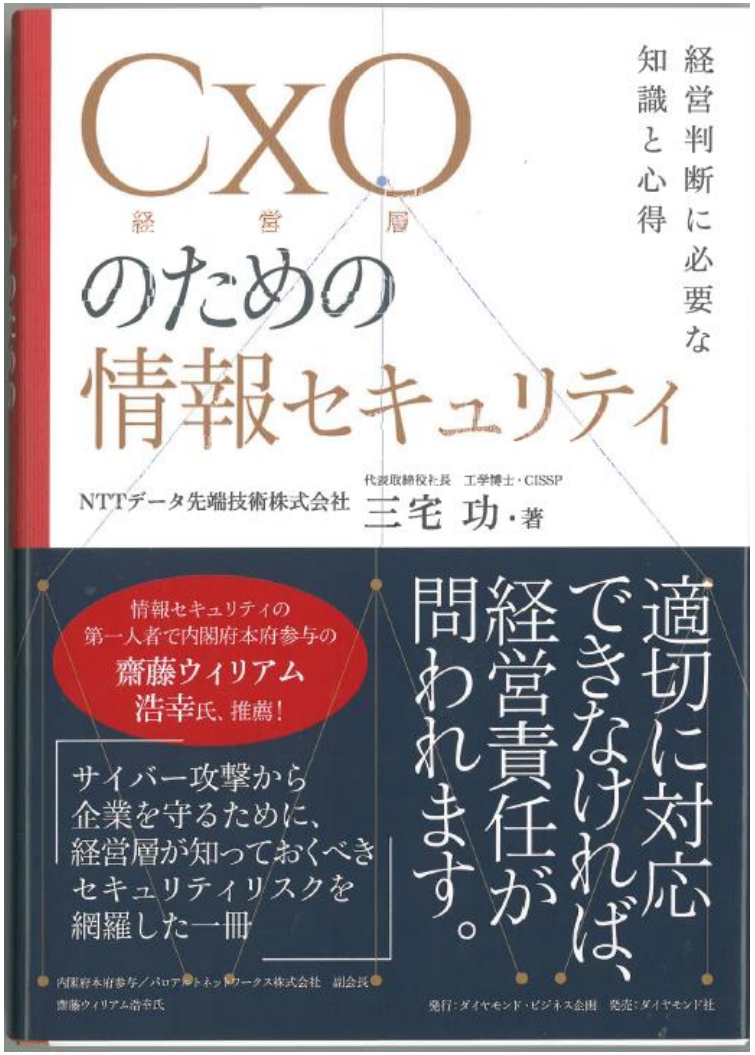
・本格的な標的型攻撃，APT
　→すでに親会社は受けている

【経営者として悩ましい点】

・潜在的なリスクに対してどこまで対応しておくべきか？
　→費用対効果の判断が難しい

・社員（協力会社含む）の情報セキュリティに対する意識の維持、向上
　→業務の効率化とセキュリティ対策のモチベーションをどうバランスさせるか？

で、何ができるか？



・経営層はリスクを俯瞰できることが求められる。そこから絞り込み。

・リスク対策とそれに対する投資判断はトップダウンが必要

・事が起こった場合は、先頭にたって「決断」と「断行」が必要

・そのためには、日頃からスキルを持った人材と必要な情報の存在を把握しておく必要がある　→　兵を養う

イノベーション＆リーダシップ　vs.　マネージメント

【マネージメント】

組織が効率的に運営され、目的の結果が達成されるように指揮指導する

そのために、

業務プロセスを整備し、現場の環境を整え、現場の状況を把握し、場合によっては直接介入し、若しくは影響を与える

【イノベーション＆リーダシップ】

環境の変化に対応し、組織を持続的に成長させる

そのために、

新技術、市場、生産手段等をどう現状から変えるかを考え、リスクを恐れず将来への投資、人財の育成、業務プロセスの変更などを行う

両者は相反するアクションが必要になり、経営者は両者をどうバランスさせるか？が問われる。

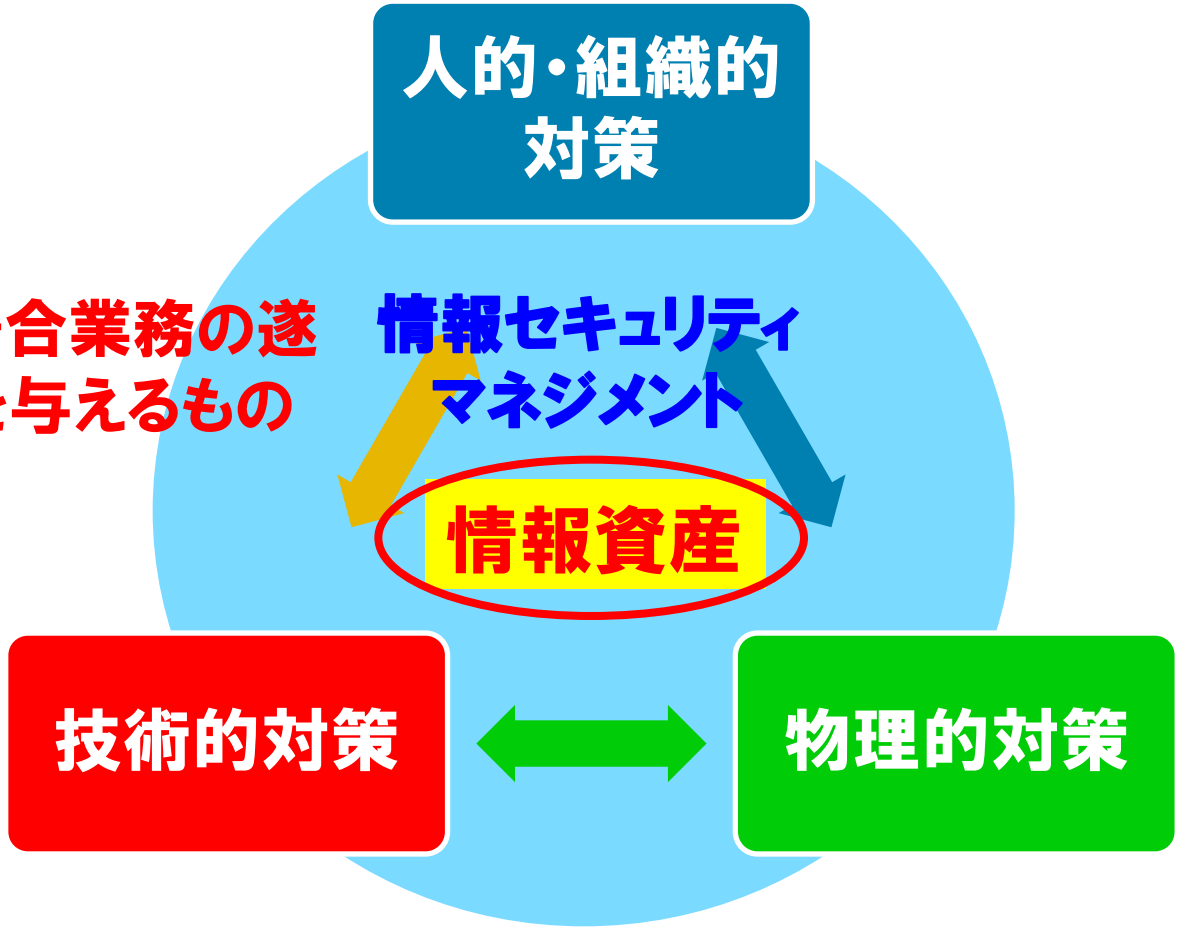
「鳥の目、虫の目」

IT企業における想定されるビジネスリスク一覧

災害リスク	事業運営上のリスク	情報セキュリティリスク
自然災害	営業契約における規定違反に起因する損失	サイバー攻撃
パンデミック	購買契約における規定違反に起因する損失	お客様・社員情報等の漏洩
テロ等の外部からの攻撃	プロジェクトに関する不適切な会計処理	機密情報の持出し
火災	知的財産権の侵害	協力会社社員による機密情報の持出し
事業環境リスク	不適切な委託行為	情報の滅失
社外からの風評攻撃	技術輸出に関する法令違反	犯罪リスク
政府調達制度の変更	建設業法違反	電磁的記録不正作出、供用
環境汚染による損害	派遣業法違反	私的非違行為
金融市場変動リスク	補助金適正化法違反	現金・預金の着服・窃取
諸外国の諸情勢管理	売上の計上時期の操作	固定資産・備品の窃取
戦略リスク	架空取引、循環取引	贈収賄
人材確保困難	資産・負債の不正な計上	労務リスク
デリバティブ取引による経済的損失	開示すべき重要な情報の隠蔽	労働災害
企業の合併・分割	経費の不正申請	長時間労働にかかる法令違反等
財務リスク	委託先からの請求書の偽造	社員のメンタル不調
問題プロジェクト	会社に不利益な取引の実行	差別行為
回収不能債権による経済的損失	キックバック	各種ハラスメント行為
資金調達	談合、不当廉売	給与支払の不正
事故・故障リスク	顧客、委託先との癒着	社員の不祥事
システムサービス停止	反社会的勢力への利益供与	社員の疾病
社内システムトラブル	インサイダー取引／株価操縦	モラル（良識）・モラ―ル（士気）の低下

情報セキュリティ対策の基本

それが失わ得た場合業務の遂行に甚大な損害を与えるもの



3つの対策は連携して行われる必要がある

“リスクベース”という考え方

NTT DATA

“Implement industry standards and best practices, don’t rely on compliance.”

A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Compliance requirements help to establish a good cybersecurity baseline to address known vulnerabilities, but do not adequately address new and dynamic threats, or counter sophisticated adversaries. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

・コンプライアンス（内部統制）準拠と言う発想ではなく、より積極的なリスク対策を行う必要がある。
・そのためには、業界毎のベストプラクティを参考に、自社に適した経済的な情報セキュリティを”リスクベース”の視点で行うことが望ましい

情報資産とリスクの特定とは？

NTT DATA

人／組織

経営・マーケティング

営業

経理・購買

開発

運用

コールセンタ

ビジネスプロセスに対応した情報資産

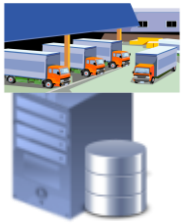
R&D・マーケティング → 営業 → 調達 → 構築・開発・試験 → 運用・保守 → バックオフィス

ITシステム

SFA

CRM

SCM



ERP

EDI

SFA

業界別セキュリティ脅威の状況

No Exception	職務の分離の徹底 職務に不要な情報は持たない
No Privacy	挙動監視、強制休暇
No Negotiation	ルールは問答無用に適用

「決定と実行」vs.「決断と断行」

「決定と実行」とは、計画を承認(決定)してその通り実行すること

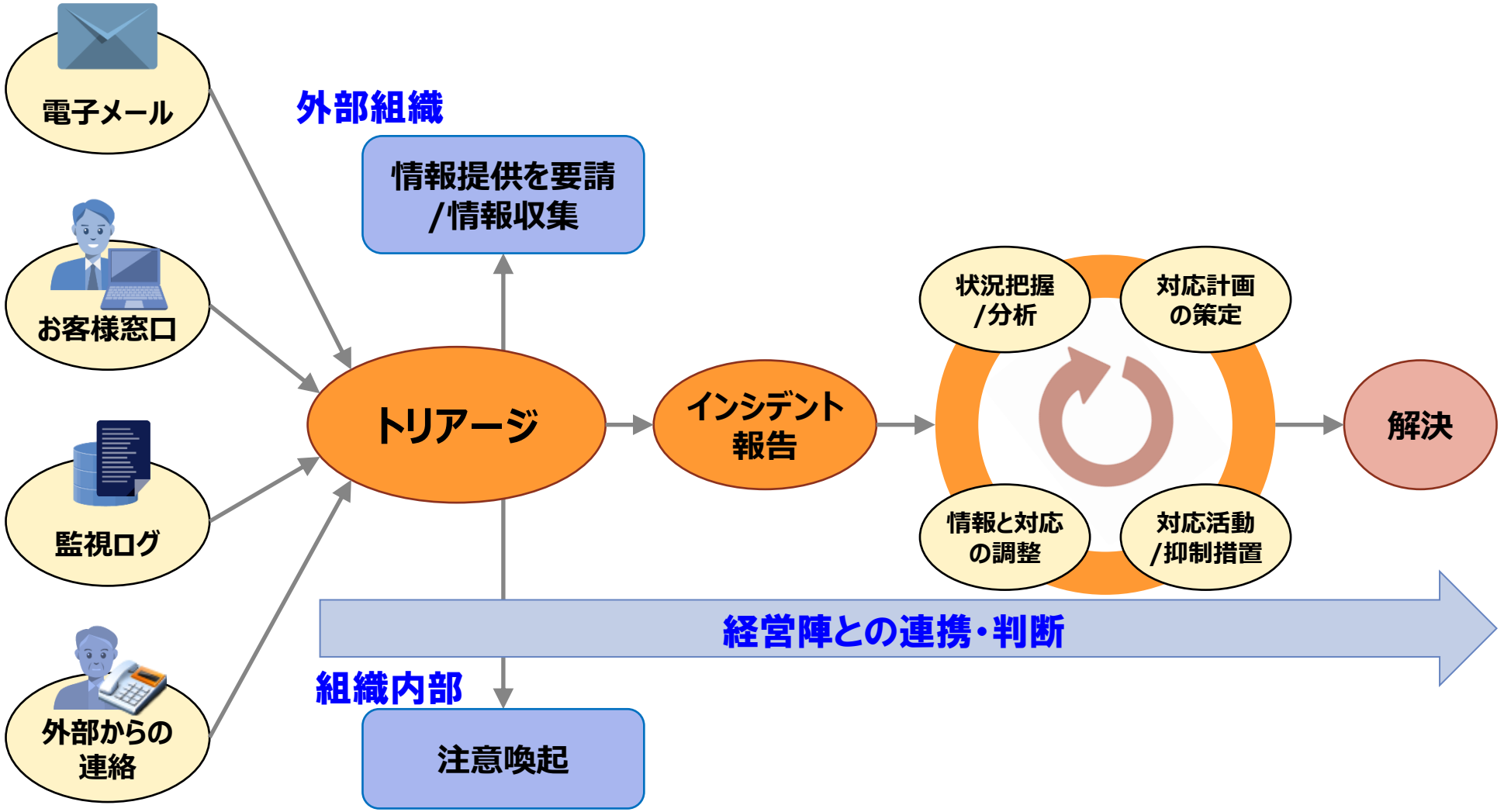
「決断と断行」とは、不確実な状況下で情報を収集・分析し、選択肢を列挙し、選んで実行すること。

OODAループ
Observe(観察), Orient(情勢判断), Decide(意思決定), Act(行動)

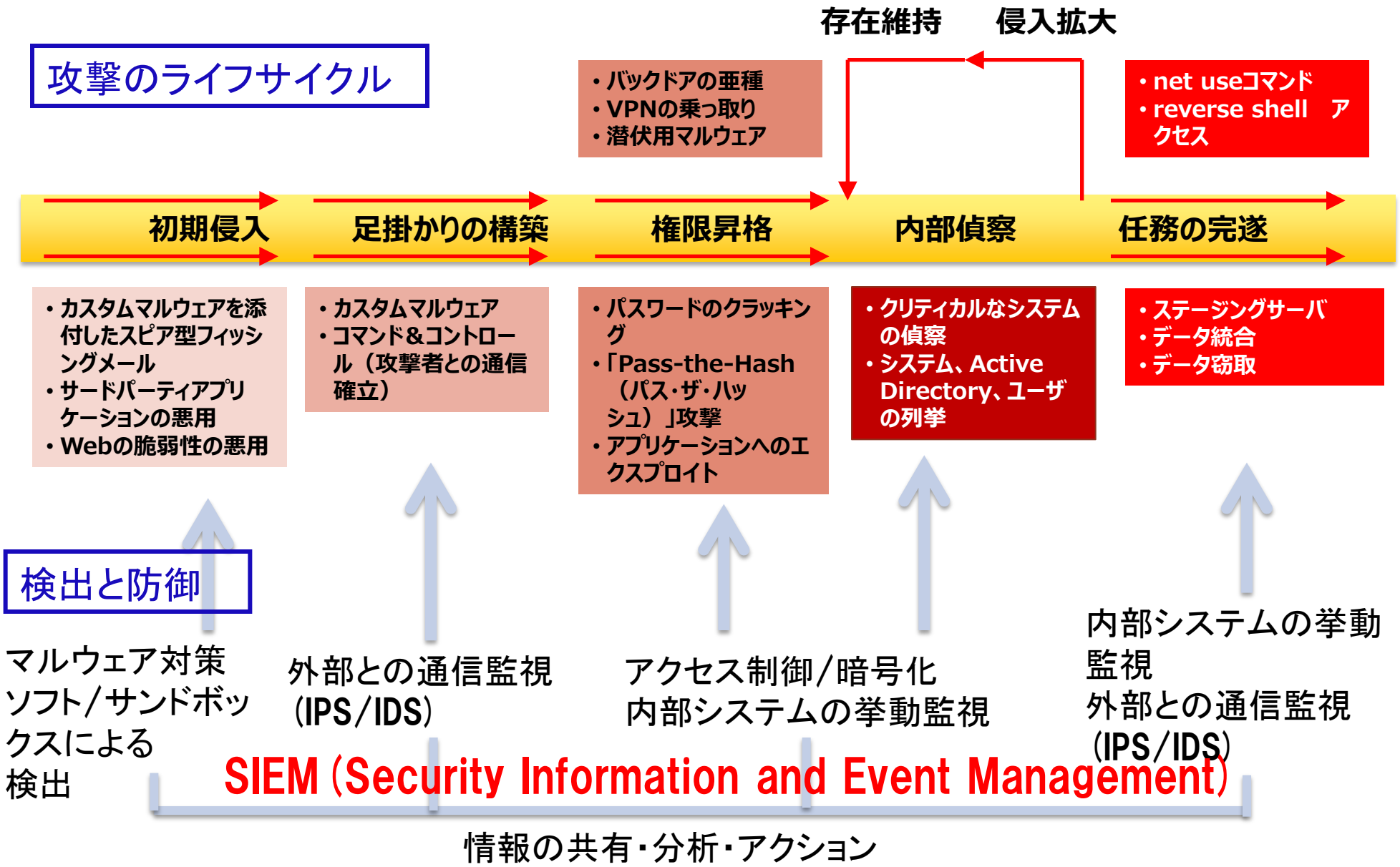
経営者はあらゆる局面で、「決断と断行」が求められる。
ex. 重大インシデント対応

このような状況下で起こりがちなこと:非難の応酬
→「罪を憎んで、人を憎まず」「プレーヤーを憎むな、ゲームを憎め」
→「根本的な帰属の誤り(Fundamental Attribution Error)

インシデントハンドリングの流れ



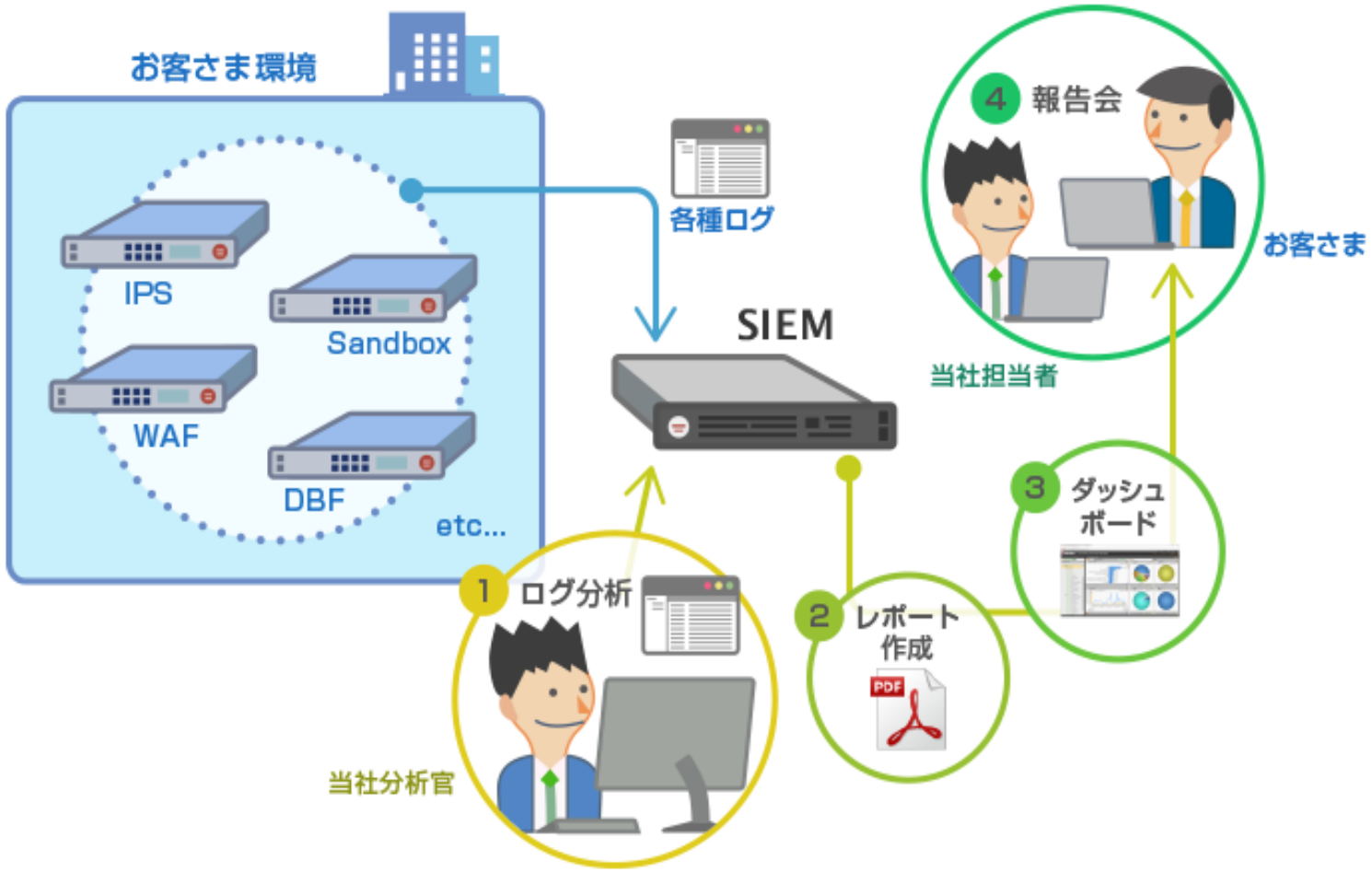
標的型攻撃のライフサイクルと対策



スポットログ評価サービス　LogDiver™

NTT DATA

仮想アプライアンス版SIEMをお客さま環境へ評価導入し、お客さま環境のログを当社のセキュリティ分析官により侵害の兆候をはじめとする、実際の脅威動向をベースとした分析観点にのっとりログを確認・抽出し、レポートを作成します。
また、作成したレポートを元に報告会を実施するサービスとなっています。　一種のPoCサービス。



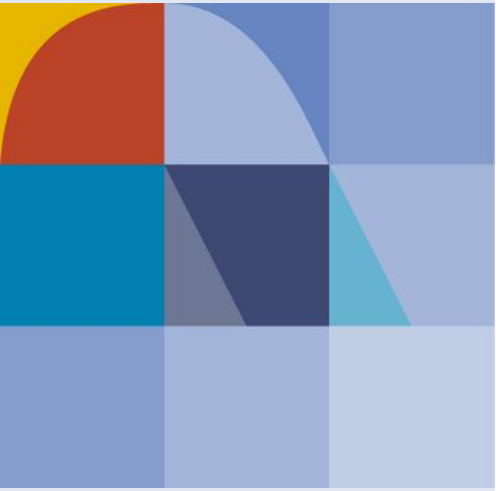
まとめ： 情報セキュリティマネジメントの鉄則

■ 100％防御することは困難
→侵入を困難にする、早期に発見できるようにする、侵入されても機密情報を抜かれないようにする。

■ 何が、重要な情報資産か？特定する。 If, What?
→リスクベースでのマネジメントの徹底。

■ 常にプロセスを見直す。PDCA
→攻撃手法は変化する、リスクは変化する。外部の動向にも常に注意を払ってプロセスを見直す。

■ 事態が発生した場合は迅速に行動
→ Observe（観察）, Orient（情勢判断）, Decide（意思決定）, Act（行動）
→ そのための事前の準備を怠らない



NTT DATA

変える力を、ともに生み出す。

（必要のない場合は注釈を削除してください）