Customer Confidential

NTT DATA UnifiedMDR® for Cyber Resilience のご紹介

2025年2月12日
株式会社NTTデータ
セキュリティ＆ネットワーク事業部

※UnifiedMDRは日本国内における株式会社NTTデータの商標です

目次：全体

INDEX

目次：個別サービス

目次：セキュリティを取り巻く概況

INDEX

セキュリティを取り巻く概況の3つの変化

近年の顧客環境のグローバル化、サプライチェーン攻撃に代表されるサイバー攻撃の変化、および法規制の動き、
等の内外環境の変化に伴い、国内およびグローバルでの**高度なセキュリティ運用の実現が急務**になってきています。

1 ビジネス環境の変化

働き方改革やDXの推進
- テレワークやクラウドなど社内外境界線の撤廃
- 攻撃手法の急速な変化と対策範囲の拡大

ビジネスのグローバル展開
- 企業の海外進出、多国籍化
- サプライチェーンの多様化
- 国・地域間の地政学リスクへの対応

2 規制・規則の変化

米国
・2021年：国家のサイバーセキュリティ向上に関する大統領令（EO 14028）

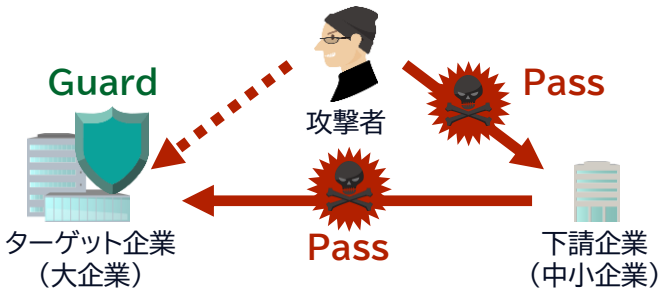
日本
・2022年：経済安全保障推進法

EU
・2022年：サイバーレジリエンス法案

中国
・2023年：国外へのデータ越境移転規制強化

3 サイバー攻撃の変化

- 本丸ではなく弱い進入口狙い（サプライチェーン攻撃）
- 海外拠点、委託/取引先、クラウドが標的に



課題

- ワークスタイルの変化によるリスクの増大
- グローバル拠点におけるガバナンス不足
- サプライチェーンセキュリティ対策の負荷増大
- セキュリティ対応要員のリソース不足
- インシデントへの早期かつ適切対応の必要性増大

「変化」に乗じたインシデントも発生

実際に、前述の課題に紐づく以下のようなインシデントも発生しており、リスクを抑えるためにも喫緊の対策が求められます。

- ワークスタイルの変化によるリスクの増大
- グローバル拠点におけるガバナンス不足
- サプライチェーンセキュリティ対策の負荷増大
- セキュリティ対応要員のリソース不足
- インシデントへの早期かつ適切対応の必要性増大

インシデント発生

年	被害組織	インシデントの種類	概要	POINT
2021	食品業A社	ランサムウェア	A社全ての拠点で使用する基幹システムとファイルサーバーがランサムウェアなどのサイバー攻撃を受けた事件。バックアップも含め全て暗号化されシステム起動が不可能な状態になり、第1、第2、第3四半期の決算報告を延期する事態に発展した。	▸ セキュリティ対策を取っていたにもかかわらず被害が発生 ▸ 早期復旧は困難、被害影響もBCP想定を超過した
2021	通信業B社	内部不正	B社元社員が同業他社E社に転職する際、前社の基地局情報などを含めた機密情報を不正に持ち出した事件。B社は1,000億円の損害賠償請求権を元社員とE社に求めて係争中である。	▸ 機密情報は複数回に分けてメールやクラウドストレージ等の手段で外部に持ち出されていた
2022	決済代行業C社	不正アクセス	C社のデータベースに対して同社Webアプリケーションの脆弱性を悪用した外部からの不正アクセスが発生し、個人情報を含む最大460,395件の情報を外部へ持ち出された事件。	▸ 攻撃開始から4か月間被害に気付けず、発覚後もシステム停止の判断が出来ず1カ月以上も攻撃が継続した
2022	通信業D社	法令違反	D社の海外子会社が提供する顧客管理システムの個人データ処理手順に関し、EUが定める一般データ保護規則（GDPR※）の違反があると当局から制裁金を科せられた事件。	▸ 日本では合法的なデータの取り扱い方法が海外では違法となるケースが存在する

※ GDPR: neral Data Protection Regulationの略称で、個人データ保護やその取り扱いについて詳細に定められたEU域内の各国に適用される法令のこと（2018年施行）

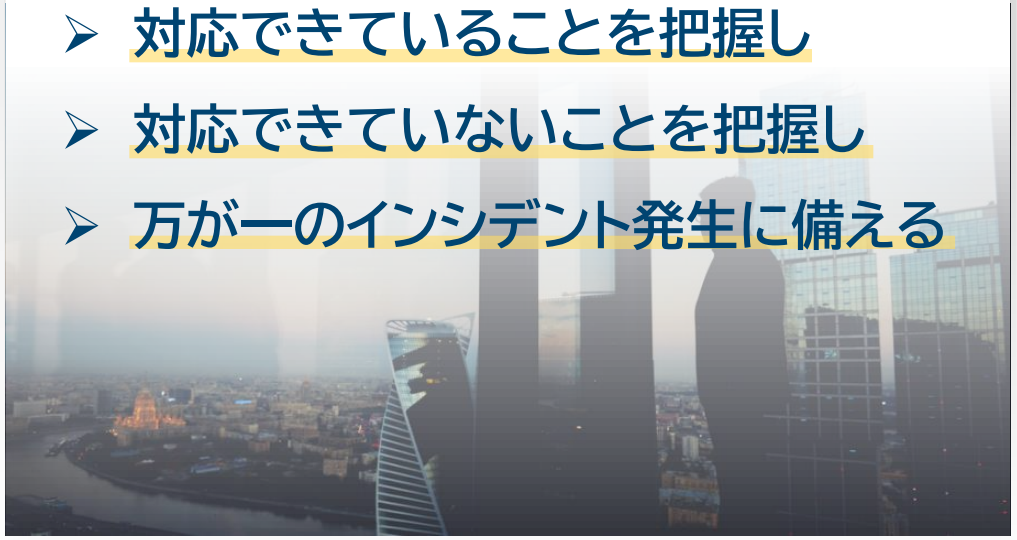
求められることは…

グローバル全体のセキュリティ体制やニューノーマルな働き方も含め、最新のセキュリティ情勢に対応したセキュリティ施策が必要です。

経営層

海外拠点/サプライチェーンを含めて

- リスクを可視化し
- 対応できていることを把握し
- 対応できていないことを把握し
- 万が一のインシデント発生に備える



従業員

FAT PC / スマートフォン / タブレット / Mac PC

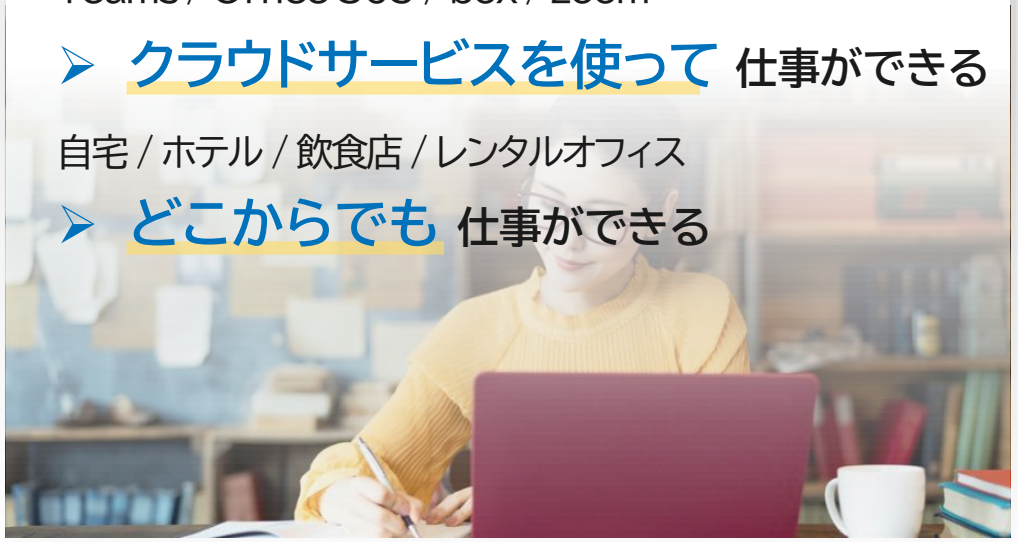
- いろいろな端末で 仕事ができる

Teams / Office 365 / box / zoom

- クラウドサービスを使って 仕事ができる

自宅 / ホテル / 飲食店 / レンタルオフィス

- どこからでも 仕事ができる



目次：NTT DATA Groupの取り組み

INDEX

NTTデータグループが抱えていたセキュリティの課題

NTTデータグループ世界70ヵ国、約20万人全体を守るグローバルセキュリティを実現するためには、全拠点のセキュリティレベルを上げる事と、高度化する最新のサイバー攻撃に備えるべく**横断的なセキュリティ監視・対応を行う必要**がありました。

＋

＋

NTT DATA Groupが抱えるセキュリティ上の課題

- ワークスタイルの変化によるリスクの増大
- グローバル拠点におけるガバナンス不足
- サプライチェーンセキュリティ対策の負荷増大
- セキュリティ対応要員のリソース不足
- インシデントへの早期かつ適切対応の必要性増大

NTTデータグループが実現した「グローバルで統一された社内セキュリティ環境」

NTTデータグループは、「Rule」「Technology」「People」の3つの軸で**レジリエンス（MDR）x ガバナンス**を強化してきました。現在では、様々な苦労を乗り越え、**世界70ヵ国、約20万人規模のゼロトラスト環境を実現**※しております。

トラディショナル → ゼロトラスト

	Stage 1 ～2017年	Stage 2 ～2018年	Stage 3 2019～2020年
	海外子会社ができ始めた M&A直後で統一感無し	**インターネット境界の セキュリティ強化**	**モバイル/クラウド利用 安全性と利便性の両立**
Rule	ガラパゴス状態	最低限のポリシーを統一	グローバルスタンダードへ
Technology	各会社でバラバラ	検知＋対応・復旧 “Exabeam”	ゼロトラスト Okta+Zscaler +CrowdStrike+Proofpoint
People	各会社の担当者が担当	各会社の担当者が担当	全体で一体感を醸成

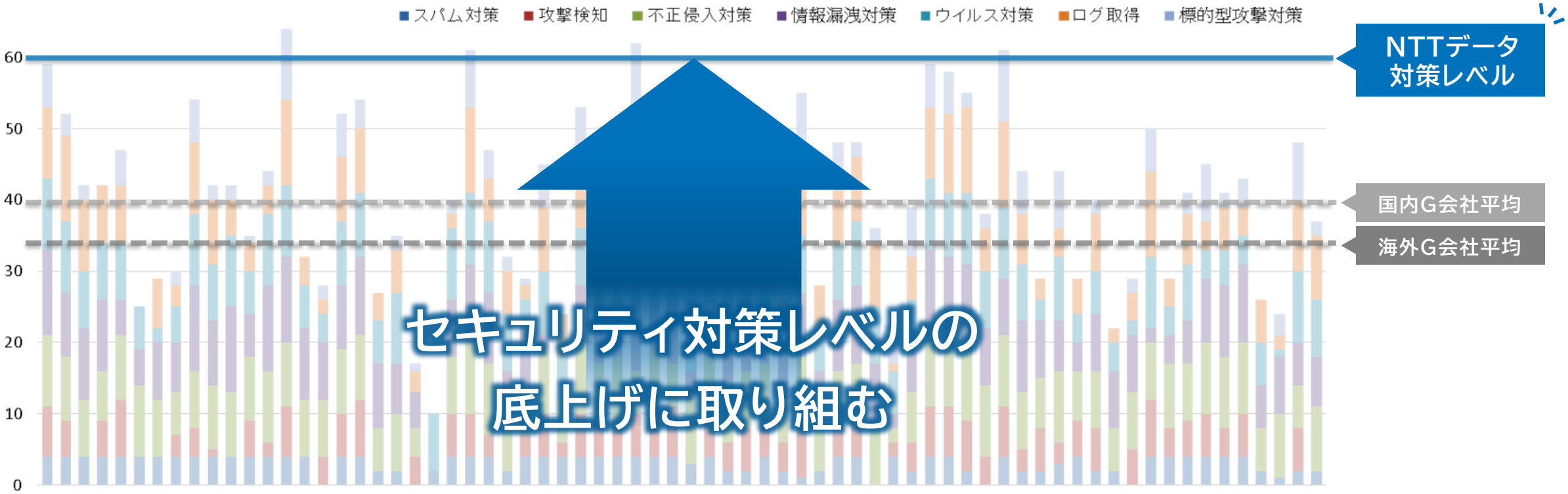
※世界最大級

グローバル全体でのセキュリティ対策レベルの底上げを実施

Rule Stage 1

セキュリティの低い拠点が侵入口とされる攻撃(サプライチェーンなど)によるリスクを低減するため、
国内外の全ての拠点を含めた**NTTデータグループ全体のセキュリティ対策レベルを底上げ**する活動を実施いたしました。

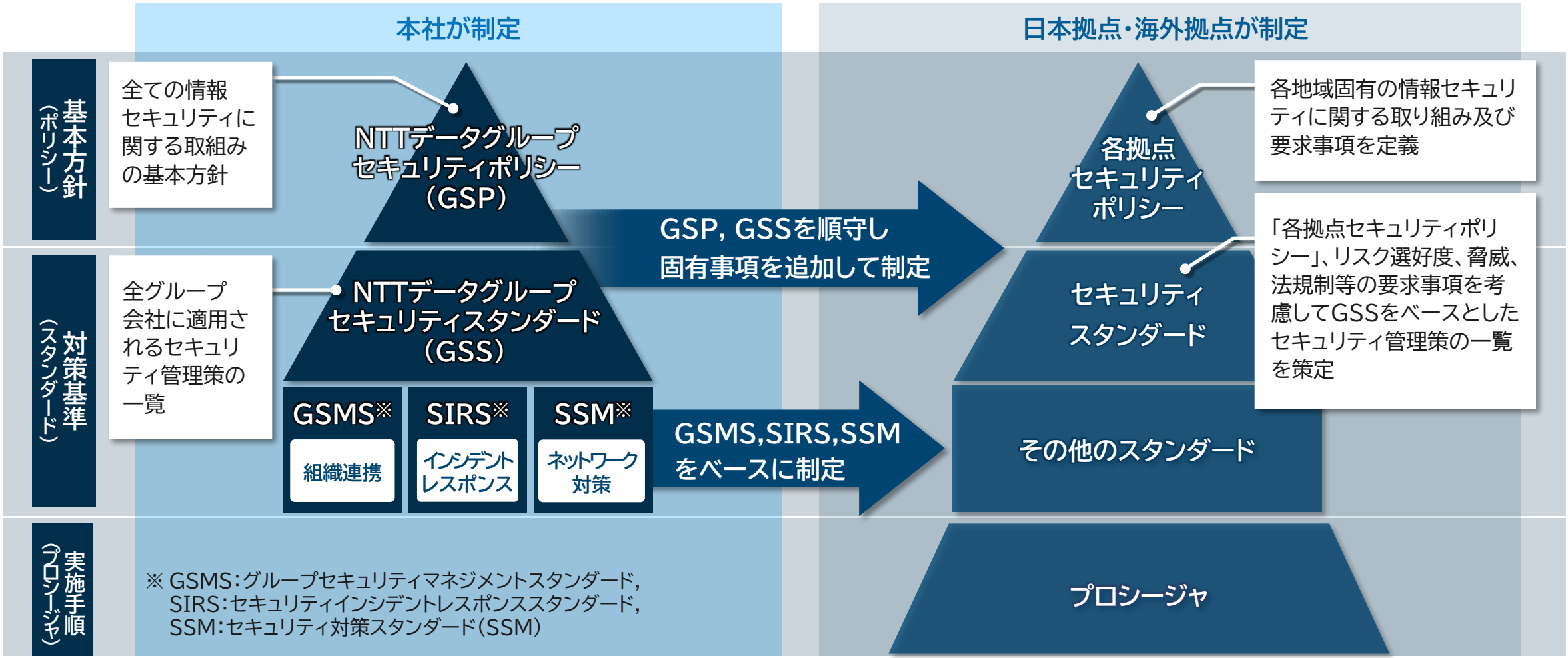
【グループ会社のセキュリティ対策状況】



グローバルセキュリティポリシー・スタンダードの統一

Rule Stage 3

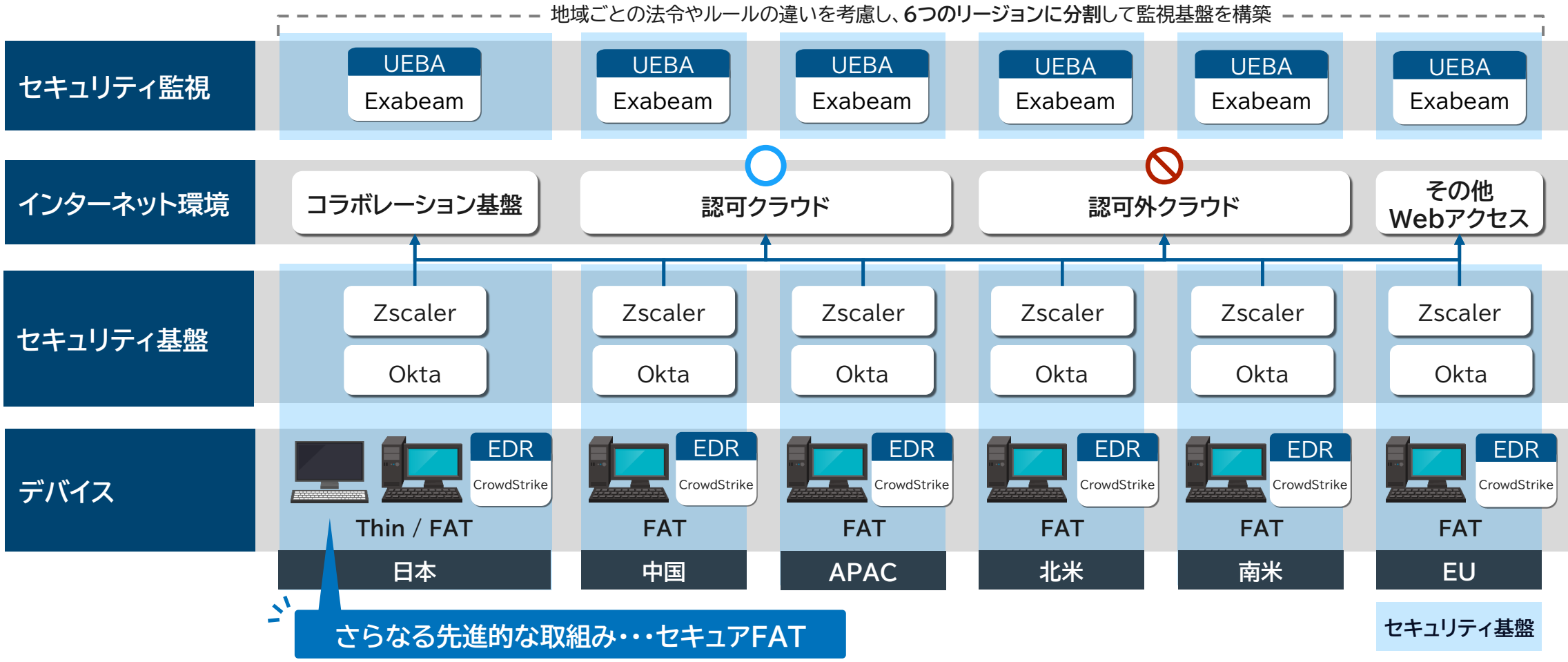
統一された**共通のグローバルポリシー・スタンダード**と、各地域の商習慣や法律に応じた**個別のポリシー・スタンダード**を制定しました。



横断的セキュリティ監視・対応基盤の構築

Technology Stage 3

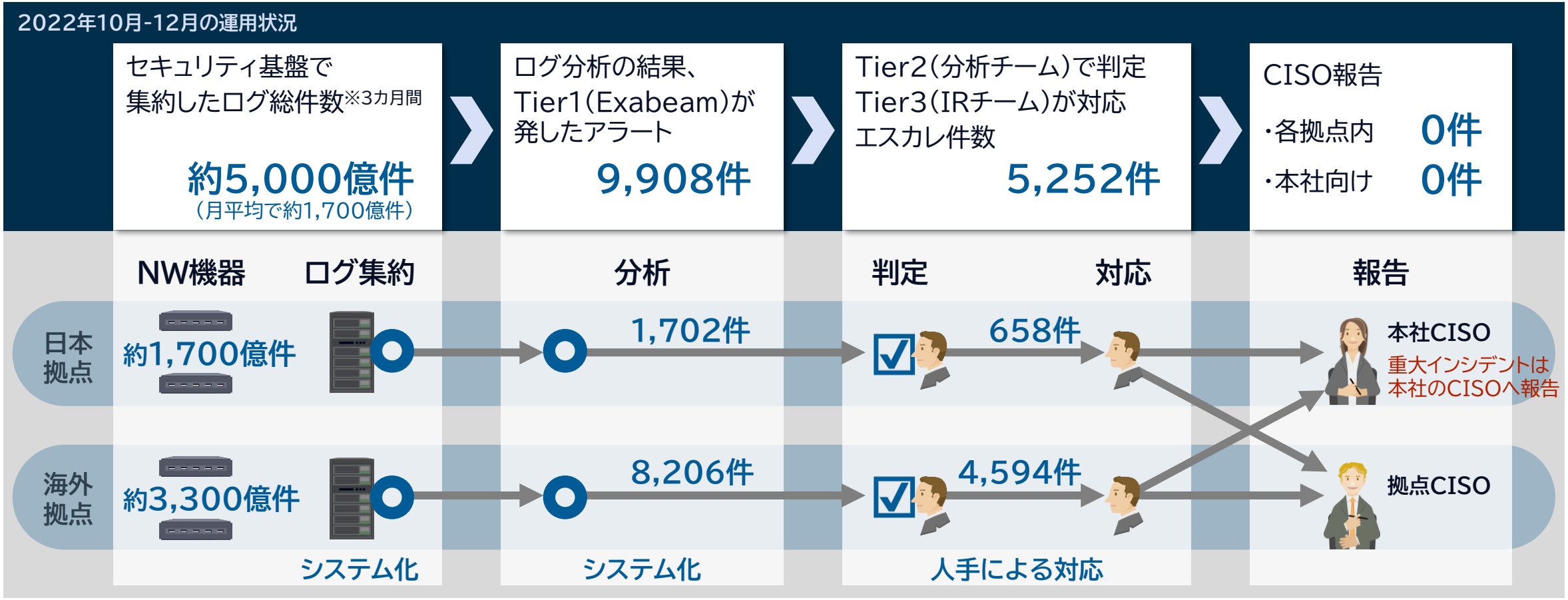
社員約20万人が活用可能な**セキュリティ基盤をグローバルで統一して構築**しており、
グローバル全拠点のシステム利用ログを取得/分析し、**24時間365日のリアルタイム監視運用**を実現しております。



インシデント対応 ～迅速なエスカレーションプロセス

Technology Stage 3

全拠点から集約される**約1,700億件/月のログを自動分析**し、怪しい挙動を検出した際は専門家チームが更に分析してインシデントの予兆検知と早期対応を行うほか、**重大なインシデントの発生時は24時間以内にCISOへ報告**可能なスキームを構築しております。



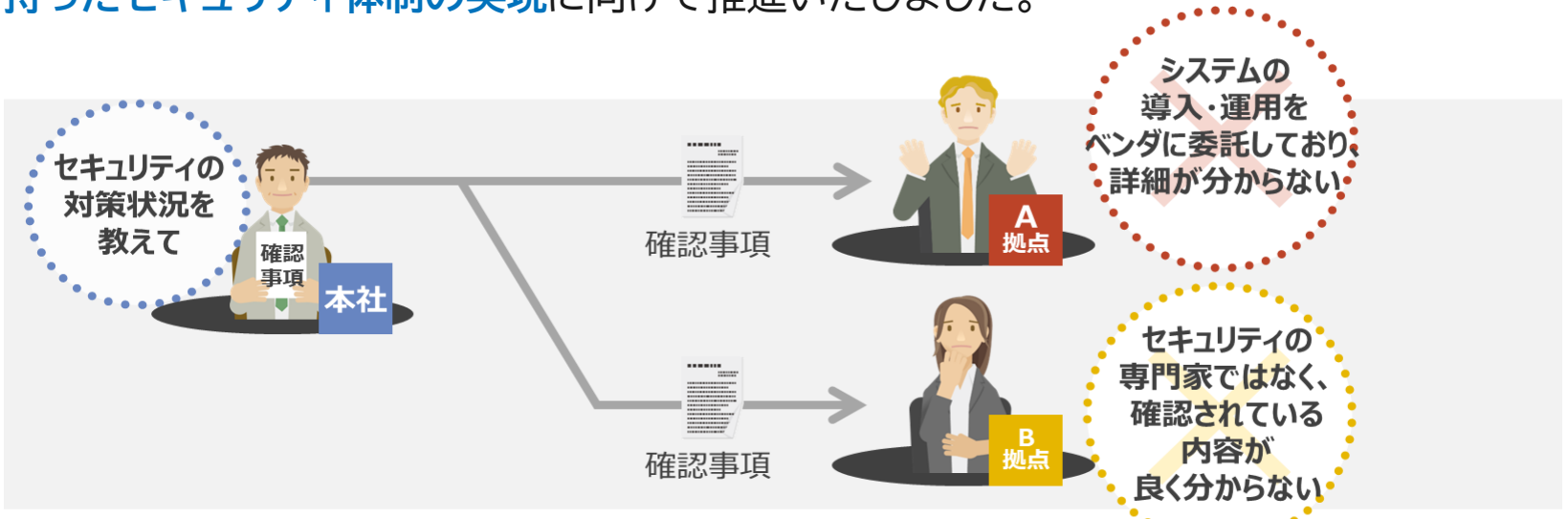
One NTTDATA：人・一体感・信頼

People Stage 1 Stage 2

グローバル全体のセキュリティ体制を統一する際、各拠点の担当者に話を聞くだけでは現状を正確に把握できないという課題に直面しました。そこで、各拠点を直接訪問して担当者と共に実際の構築/運用を行っているベンダにもヒアリングを行いつつ信頼関係を構築。**グローバルで一体感を持ったセキュリティ体制の実現**に向けて推進いたしました。

課題

各拠点の担当者に聞くだけでは現状把握できない



対策

拠点を訪問の上、担当者と信頼関係を構築し、一体感を醸成

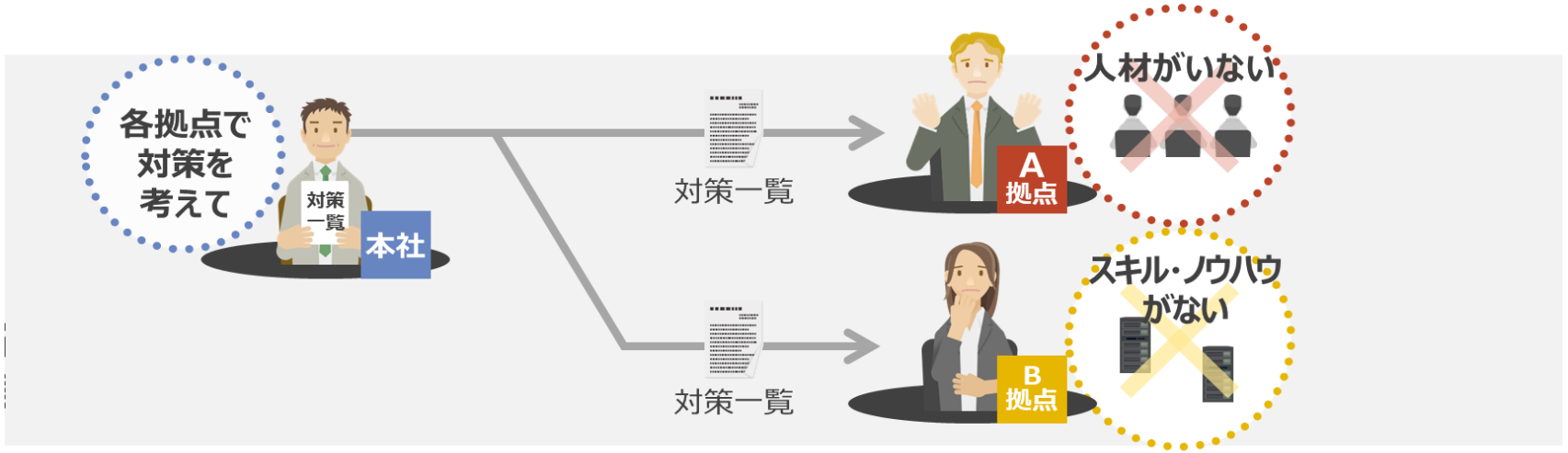
One NTTDATA：人・一体感・信頼

People Stage 1 Stage 2

また、各拠点に適切なスキルとノウハウを有した人材がおらず、各拠点ごとに具体的な対策立案を実施するのは難しいという課題にも直面しました。そこで、**HQ（日本本社）主導で対策立案を実施し、各拠点へ展開**するといった方針を選択しました。

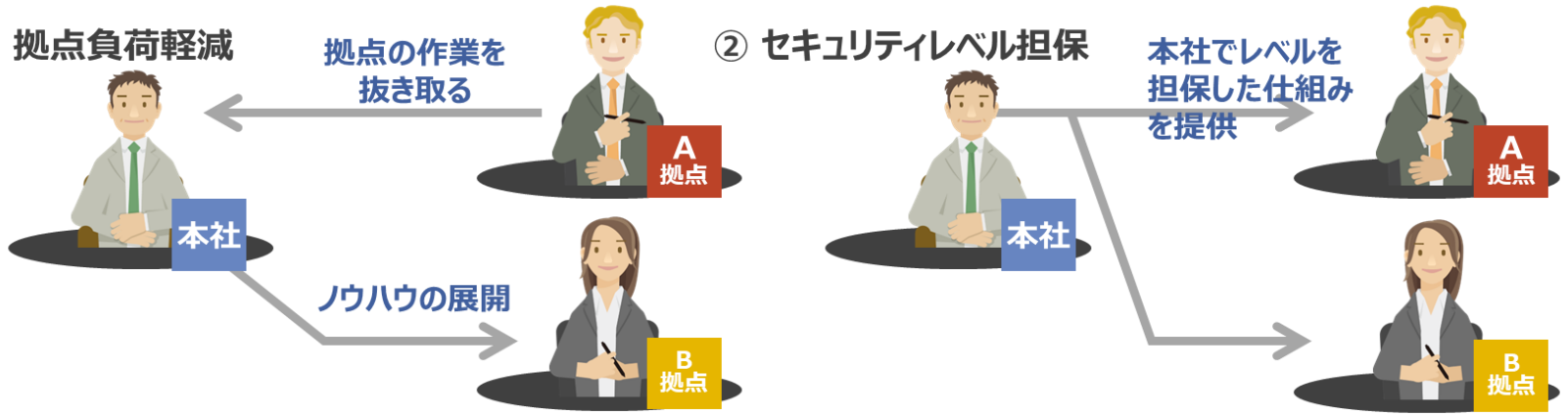
課題

各拠点で対策立案を実施するのは難しい



対策

本社主導での対策立案を実施



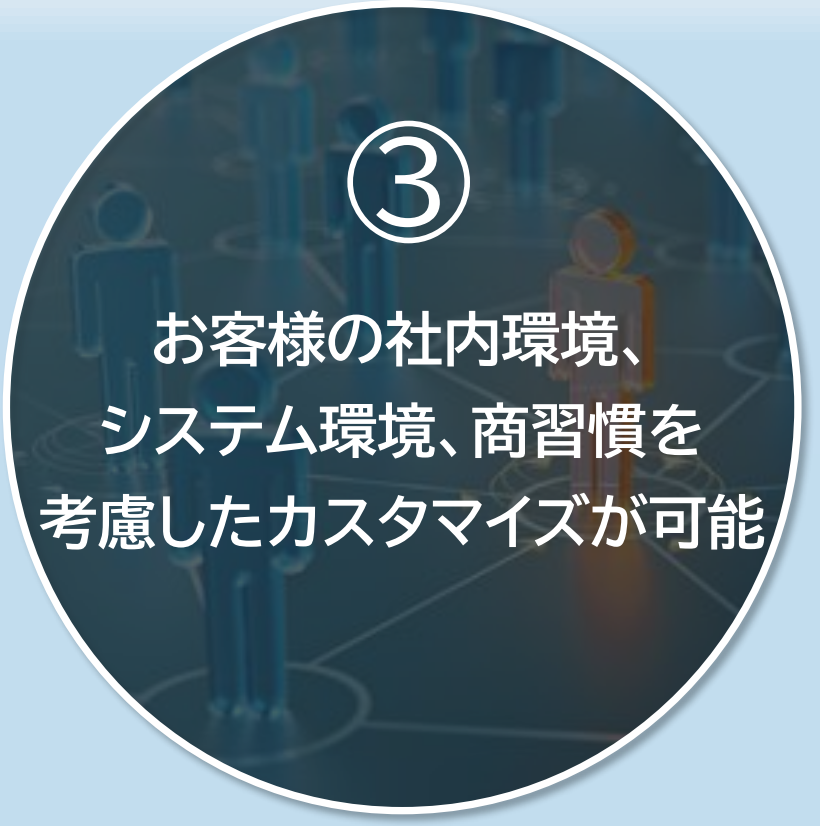
目次: NTT DATA UnifiedMDR® for Cyber Resilienceのご紹介

INDEX

本サービスの特徴

UnifiedMDR®では、下記特徴を備える本サービスをご提供することでお客様環境におけるセキュリティを向上させます。

Cyber Resilience 3つの特徴



本サービスの特徴　①ポリシー策定からセキュリティ運用・改善まで全領域に対応

NTTデータグループが**グローバルで統一されたセキュリティ環境を実現する中で得た経験やノウハウをお客様向けに展開**し、海外特有の事情にも対応可能な、コンサルから構築、運用、改善までの全領域に対応した一気通貫のサービスを提供しております。

＋

＋

ノウハウをお客様へ展開

コンサルから構築、運用、改善までの全領域を“一気通貫”でサービス提供可能

コンサルティング			ソリューション構築	運用（平時）		運用（有事）	
ポリシー策定	リスクアセスメント	セキュリティ訓練/教育		SOC運用	CSIRT運用	インシデントハンドリング	インシデント対策フォロー

本サービスの特徴　②NTTDATA-CERTによる長年のセキュリティ運用で培ったノウハウを展開

弊社グループのインシデント対応専門組織「NTTDATA-CERT」では、平時活動において、攻撃監視、ログ分析等を実施し、インシデントの発生を未然に防止しております。また、インシデント発生時においては、早期対応によってセキュリティ被害を極小化し、迅速な対応と再発防止策を徹底しております。これらの**長年に渡るセキュリティ運用で培ったノウハウをお客様に展開**いたします。

【NTTDATA-CERTの活動例】

平時の活動

サイバー攻撃動向やリスクの分析に基づいたインシデントの未然防止、早期検知、対応体制の構築

① 情報セキュリティ推進
「Ⅰ. 外部からのサーバー攻撃」及び「Ⅱ. 内部不正も含めたウィルス感染・情報漏洩」への対策強化を実施

② ルール整備／教育訓練
情報セキュリティ対策の推進、対応手順の策定、教育訓練、啓発活動等

③ 情報収集／発信
脆弱性情報、脅威情報、他社事例など収集、メールやWEBで情報発信

④ 対外連携／PR
NTTグループ内連携、社内セミナー開催、社外コミュニティ活動、執筆、講演など

⑤ インシデント監視
攻撃監視、ログ分析、検知連絡

効率化／利活用　フィードバック

緊急時の活動

早期対応によるセキュリティ被害の極小化と迅速な復旧および再発防止策の徹底

インシデント発生

⑥ インシデント対応

Ⅰ. 原因分析
- ✓ インシデント証拠保全
- ✓ 関係者へのヒアリング
- ✓ 被害状況把握　など

Ⅱ. 被害極小化
- ✓ 各種機器の緊急停止
- ✓ 影響範囲の確認
- ✓ 業務継続策検討　など

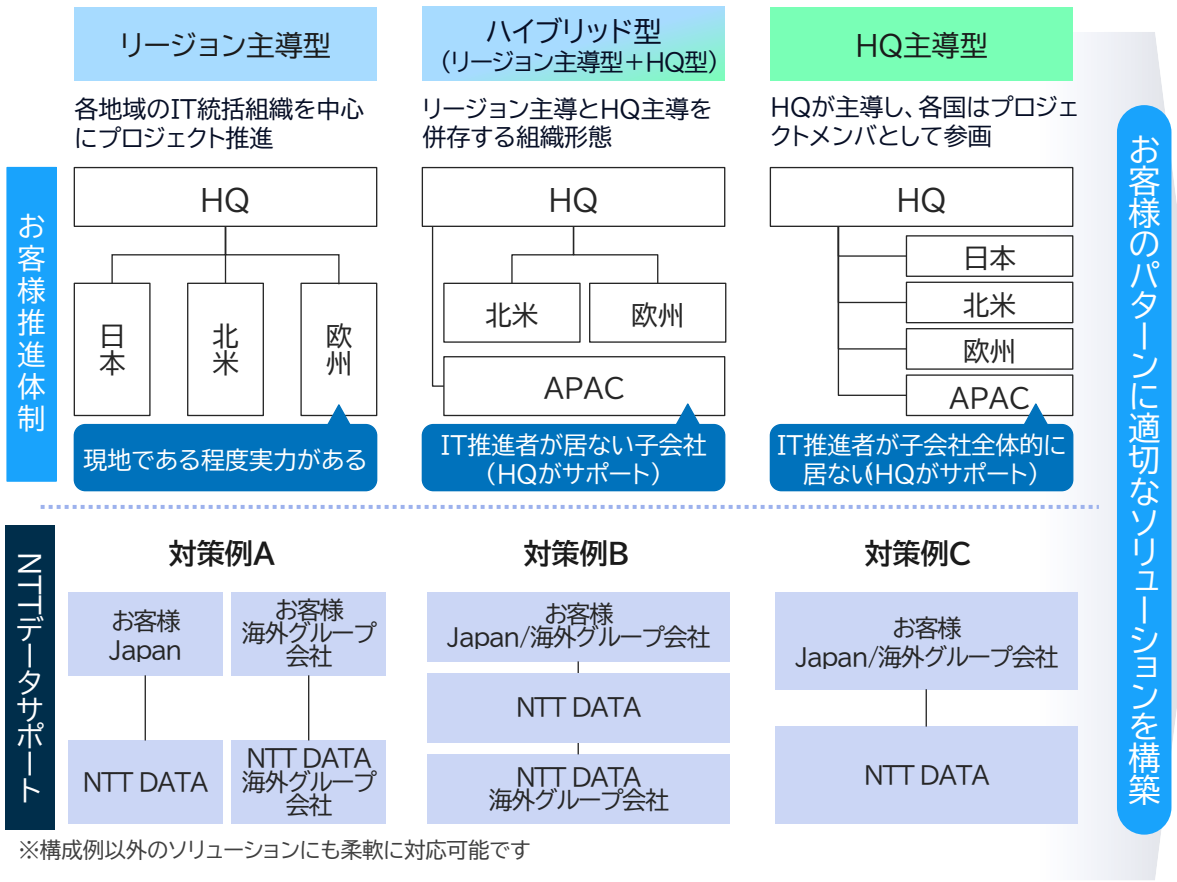
Ⅲ. 復旧
- ✓ 設定変更や機器最新化
- ✓ 流出データの削除
- ✓ 紛失データの検索　など

Ⅳ. 再発防止
- ✓ 再発防止策の実施／展開
  - ・技術的対導入
  - ・教育の実施
  - ・ルール制定、体制整備

本サービスの特徴　③お客様の社内環境、システム環境、商習慣を考慮したカスタマイズが可能

グローバルビジネスのパターンはお客様の戦略や経営効率化の観点から多くの種類があり、そのパターンに応じIT部門の組織構成やシステム構成も変わります。本サービスでは、**お客様のパターンに適切な体制とソリューションを構築してプロジェクトを推進**いたします。

お客様プロジェクト推進モデル



※構成例以外のソリューションにも柔軟に対応可能です

導入ソリューションの構成例

ソリューション	特定 Identify	防御 Protect	検知 Detect	対応 Respond	復旧 Recover	構成例※
Identity ID管理 2要素認証	✓	✓				Microsoft Entra ID Okta
Hygiene 未管理端末の把握 パッチ適用/状況把握	✓			✓	✓	Microsoft Intune Tanium
SWG 暗号化通信の監視 クラウドの利用制御		✓	✓			Microsoft Defender for Cloud Apps Zscaler
Mail Security メール詐欺対策 標的型メール対策		✓	✓			Microsoft Defender for O365 Proofpoint
EDR ファイルの振舞検知 端末管理の自動化			✓	✓	✓	Microsoft Defender for Endpoint CrowdStrike
UEBA 怪しい振る舞いの検知			✓	✓		Azure Sentinel Exabeam

目次：個別サービスのご紹介

INDEX

NTT DATA UnifiedMDR® for Cyber Resilience サービス一覧

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

SOC

- SOC構築サービス
  - 監視基盤構築
  - 運用体制構築
- SOC運用サービス
  - セキュリティログ監視

CSIRT

- CSIRT構築サービス
- CSIRT運用サービス（平時）
  - IRディレクター
- CSIRT運用サービス（有事）
  - インシデントハンドリング
  - フォレンジック
  - IR対策フォロー

コンサルティング

- セキュリティポリシー策定サービス
- リスクアセスメントサービス
- SOC/CSIRT成熟度評価サービス
- IR教育/訓練サービス
- TLPTサービス

ソリューション構築

- ゼロトラスト環境構築サービス

NTT DATA UnifiedMDR® for Cyber Resilience 全体像サービスカット [1/2]

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

SOC

SOC構築サービス

- SOC運用の監視基盤となるSIEM構築を支援（オプションでSOAR、UEBA等も追加）
- 現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

- 監視基盤構築
- 運用体制構築

SOC運用サービス

- お客様のアラートを監視/分析し、お客様の運用負担の軽減およびインシデントの早期解決実現

- セキュリティログ監視

CSIRT

CSIRT構築サービス

- 世界各地でのインシデントレスポンスを行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

CSIRT運用サービス（平時）

- インシデントレスポンス（IR）に備えた技術、体制、規則の改善および将来の目指す姿に向けたロードマップを作成/提案

- IRディレクター

CSIRT運用サービス（有事）

- 経験豊富なセキュリティ専門家が、インシデント発生から終結までトータルで支援/代行

- インシデントハンドリング
- フォレンジック
- IR対策フォロー

NTT DATA UnifiedMDR® for Cyber Resilience 全体像サービスカット［2/2］

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

コンサルティング

セキュリティポリシー策定サービス

- 統一された共通グローバルポリシー・スタンダードの制定および、各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

リスクアセスメントサービス

- システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

SOC/CSIRT成熟度評価サービス

- セキュリティ対応組織の業務につき、業界団体ガイドライン、弊社知見をもとにした評価基準を用いて機能整備状況、運用状況を評価し成熟度を可視化

IR教育/訓練サービス

- お客様のご要望や組織が目指すセキュリティの目的に応じて多種多様な教育プログラムを計画/実施し、サイバーセキュリティの専門家育成を支援

TLPTサービス

- 疑似インシデントを計画、実行し、システムのセキュリティ対策状況およびSOC/CSIRTの対応力を評価、改善策提示

ソリューション構築

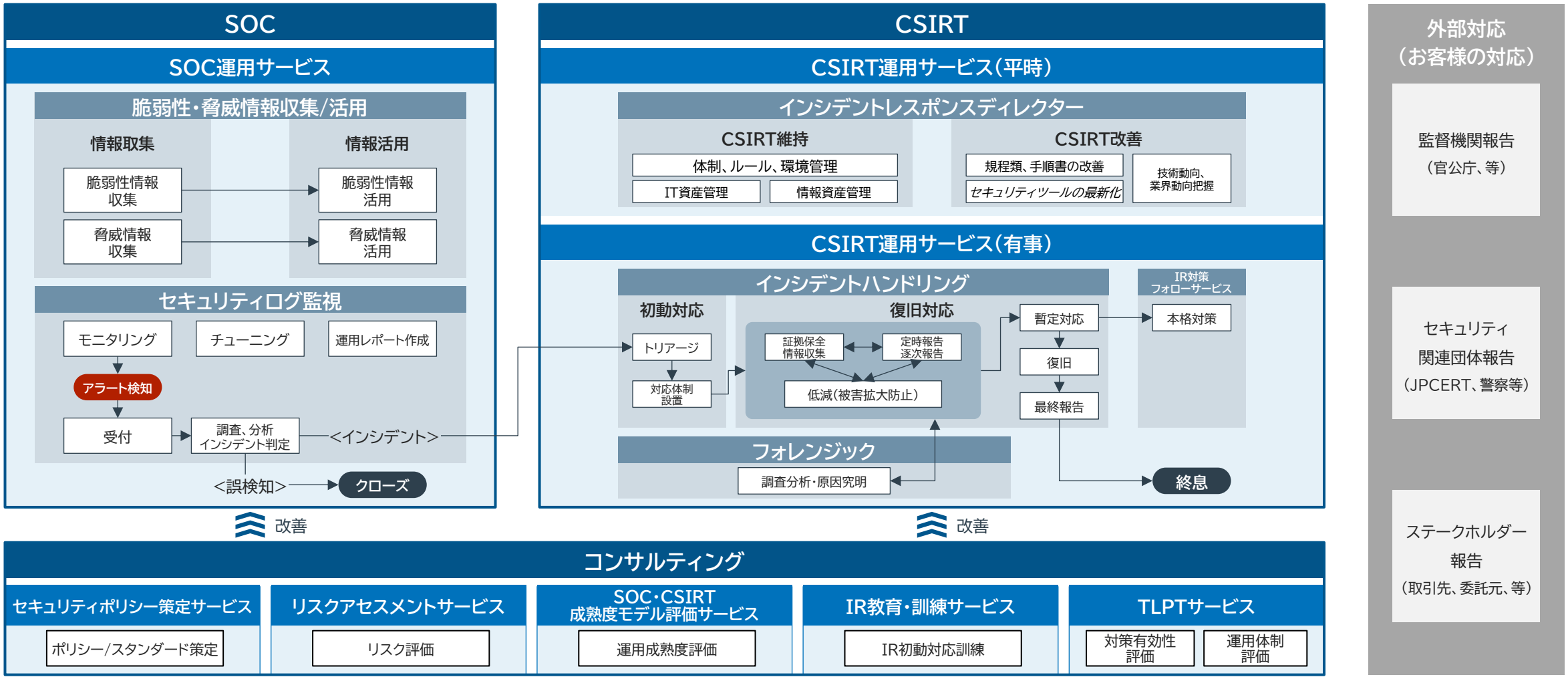
ゼロトラスト環境構築サービス

- ゼロトラスト環境を構築していく上で必要となるセキュリティソリューションの導入/構築を支援

＜導入を支援するセキュリティソリューションの一例＞
・IDaaS ・SWG etc.

各サービスの機能・役割分担について

本サービスでは、各サービスの機能・役割を下記のように分類しております。



01

SOC構築／運用サービスのご紹介

NTT DATA UnifiedMDR® for Cyber Resilience 全体像サービスカット

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

SOC

SOC構築サービス

- SOC運用の監視基盤となるSIEM構築を支援（オプションでSOAR、UEBA等も追加）
- 現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

- 監視基盤構築
- 運用体制構築

SOC運用サービス

- お客様のアラートを監視/分析し、お客様の運用負担の軽減およびインシデントの早期解決実現

- セキュリティログ監視

CSIRT

CSIRT構築サービス

- 世界各地でのインシデントレスポンスを行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

CSIRT運用サービス（平時）

- インシデントレスポンス（IR）に備えた技術、体制、規則の改善および将来の目指す姿に向けたロードマップを作成/提案

- IRディレクター

CSIRT運用サービス（有事）

- 経験豊富なセキュリティ専門家が、インシデント発生から終結までトータルで支援/代行

- インシデントハンドリング
- フォレンジック
- IR対策フォロー

SOC構築/運用サービス 提供効果

本サービスでは、**SOCの要件定義から設計・構築・展開・運用までをワンストップでお客様へサービスを提供**いたします。
また、ワンストップでの提供を可能としつつ**個別サービスも用意**しておりますので、お客様のご要望に応じた形でのサービス提供が可能です。

お客様のお悩み	対応サービス	サービス提供による効果
自組織の情報資産を監視・保護する仕組みが整っておらず、まずは**監視基盤の導入から始めたい**	➢ **監視基盤構築サービス**	SOC運用に必要となる**監視基盤を、お客様のニーズに合わせて最適な形で設計・構築**します
SIEMなどの監視基盤を構築したものの、**適切な運用体制の整理が出来ていない**	➢ **運用体制構築サービス**	現状の運用体制・手順を整理し直し、手順策定やドキュメント整備、人員の確保など、**お客様の組織に適合したSOC運用体制を構築**します
自組織SOCの品質に懸念がある他、**セキュリティ人材も慢性的に不足**しており、セキュリティ運用の品質とリソース不足を改善させたい	➢ **セキュリティログ監視サービス**	お客様SOC調査/分析結果に対する**セカンドオピニオン**を実施して自社SOC組織の品質を向上できる他、**監視業務の代行**も承ります
日本国内におけるSOC組織は存在するが、**海外拠点ごと、またはグローバル全体でのSOCについては未検討**	➢ **監視基盤構築サービス** ➢ **運用体制構築サービス** ➢ **セキュリティログ監視サービス**	地域・国ごとの商習慣に適応した**グローバルSOC**を、要件定義から設計・構築・運用まで**ワンストップにトータルでサポート**します

SOC構築 監視基盤構築サービス 【1/2】

- SOC運用の監視基盤となるSIEM構築を支援

提供価値

■グローバル規模のセキュリティに対応した、お客様独自のSOCを一気通貫に構築

- 弊社グループの世界規模（70ヵ国、約20万人）でのセキュリティ組織を構築/運用する中で培ったノウハウを元に、お客様のビジネス/業界ニーズに沿った実効性のある最適なSOCを構築します。

■セキュリティ経験豊富な専門家による対応

- 業界内最高峰の弊社組織内SOCを構築/運用している専門家が、お客様組織に適切なSOC監視基盤の構築をご支援します。

実施事項

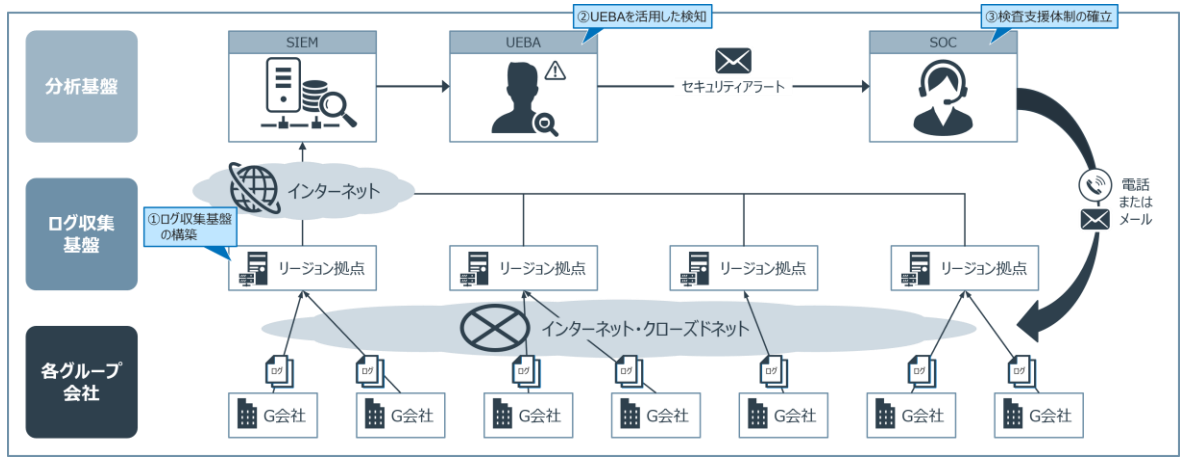
	1. 要件定義	2. PoC実施	3. 設計/構築		4. 展開/運用/改善
実施事項	• システム構成検討 • ユースケース検討	• サンプルログ確認 • PoC（概念実証）の実施 • パーサ開発	• 運用ドキュメント作成 • 分析基盤SIEMの導入		• チューニング • 試運転支援
実施概要	‣ お客様の組織体制や機器構成などを整理/分析し、システム構成や要件を検討 ‣ 実際の運用場面を想定したユースケースを検討し、監視対象や収集すべきログソースを可視化	‣ ログソースからサンプルログを取得し、SIEMに取り込む上での変更要否の確認などを実施 ‣ お客様環境のログにSIEMを構築し、PoCを実施 ‣ 各種機器からのログを解析するためのパーサを開発	‣ PoCの結果を踏まえて、基本設計書など各種ドキュメントを作成 ‣ 整備ドキュメントに基づきSIEMソリューションを導入。要件に応じてオプションにてSOAR、UEBA等の導入も実施		‣ 仮運用の期間中、ログの取り込み設定や検知ロジックなど各種チューニングを随時サポート ‣ 本番稼働に向け、構築された環境の試運転を支援1か月程度）試運転期間中に発生した課題、チューニングなどの対処を行うことにより、円滑な本番稼働への切り替えを実現
成果物	✓ 要件定義書	✓ PoC結果報告書	✓ 基本設計書 ✓ 運用ドキュメント ✓ パラメーターシート	✓ 構築されたSIEM	✓ チューニング内容一覧

SOC構築 監視基盤構築サービス【2/2】

- SOC運用の監視基盤となるSIEM構築を支援

サービスイメージ

■構成イメージ



■対象製品一覧※

分類	処理概要	製品名
EDR (Endpoint Detection and Response)	▪ ファイルへのアクセスやコピー、削除など、端末内の挙動・ふるまい検知 ▪ 端末管理の自動化	• CrowdStrike • Microsoft Defender for Endpoint • VMware Carbon Black EDR
SIEM (Security Information and Event Management)	▪ セキュリティ情報管理 ▪ セキュリティイベント管理 ▪ セキュリティログ相関分析	• Exabeam • Splunk • QRadar
UEBA (User and Entity Behavior Analytics)	▪ 機械学習による各ユーザー・エンティティの行動パターンの学習 ▪ 監視対象への自動スコアリングによる怪しい振る舞いの検知	• Exabeam Security Analytics • Microsoft Sentinel
SOAR (Security Orchestration, Automation and Response)	▪ プレイブックにもとづくセキュリティ運用の自動化・効率化	• QRadar • ServiceNow

導入実績

➢ 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

※ 上記表に記載外の製品に関しても、ご相談に応じて対応可能です。

SOC構築 監視運用体制構築サービス【1/2】

- 現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

提供価値

■グローバル規模のセキュリティに対応した、お客様独自のSOCを一気通貫に構築

- 弊社グループの世界規模（70ヵ国、約20万人）でのセキュリティ組織を構築/運用する中で培ったノウハウを元に、お客様のビジネス/業界ニーズに沿った実効性のある最適なSOCを構築します。

■セキュリティ経験豊富な専門家による対応

- 業界内最高峰の弊社組織内SOCを構築/運用している専門家が、お客様組織に適切なSOC監視基盤の構築をご支援します。

実施事項

	1. 要件定義	2. PoC実施	3. 設計/構築	4. 展開/運用/改善
実施事項	• ヒアリング • ドキュメント調査 • Gap分析	• 構築タスクの洗い出し • 計画策定	• 運用ドキュメント作成 • SOC要員の調整	• 試運転支援
実施概要	‣ お客様へのヒアリングや既存文書の確認等を通じて、お客様のセキュリティ監視運用に関わる既存の体制、ルール/プロセス、技術的環境の状況を把握 ‣ お客様のビジネス/ミッションに沿ったTo-Be像を具体化することで、As-IsとTo-BeのGapを可視化	‣ Gap分析結果を元に、Gapを埋める構築タスクの洗い出し ‣ お客様のビジネス/ミッションに沿って構築タスクの優先度を決定し、お客様の予算およびスケジュールを考慮した計画を策定	‣ リアルタイム基本分析手順、問い合わせ対応フロー、各種管理簿などを策定 ‣ SOC運用に必要な要員のスキルセットや人数を決定。お客様にて要員確保が困難な場合、弊社が提供するSOC運用サービスにて構築から運用までを一気通貫でサポート	‣ 本番稼働に向け、構築された環境の試運転を支援（1か月程度）。試運転期間中に発生した課題、チューニングなどの対処を行うことにより、円滑な本番稼働への切り替えを実現
成果物	✓ Gap分析結果報告書	✓ 構築タスク一覧 ✓ 計画書	✓ 運用ドキュメント	✓ 試運転課題一覧

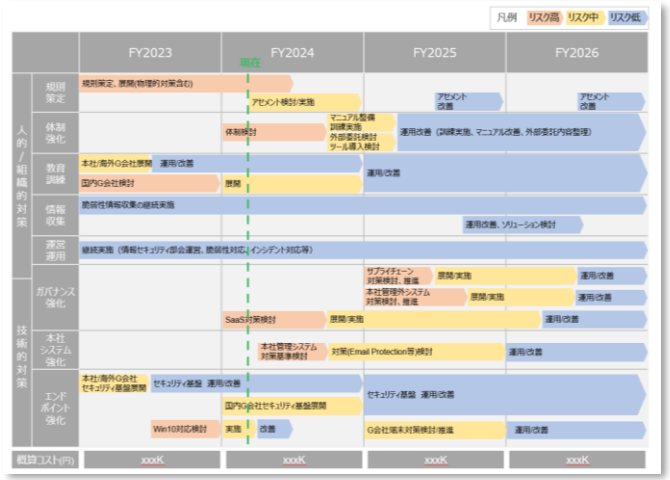
SOC構築 監視運用体制構築サービス【2/2】

- 現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

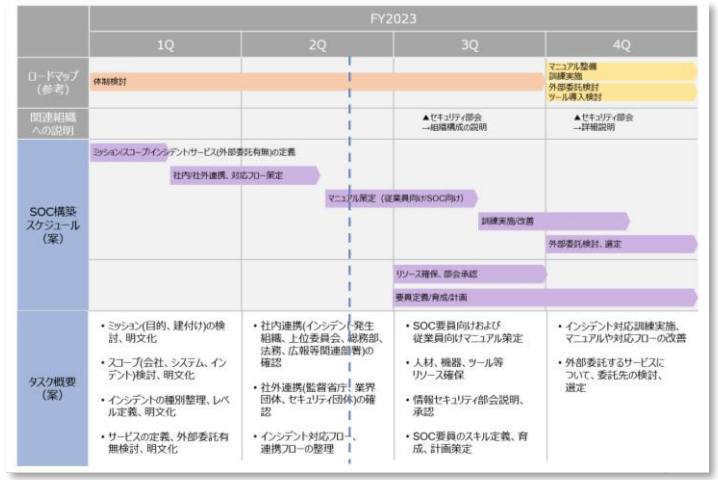
サービスイメージ

■成果物例

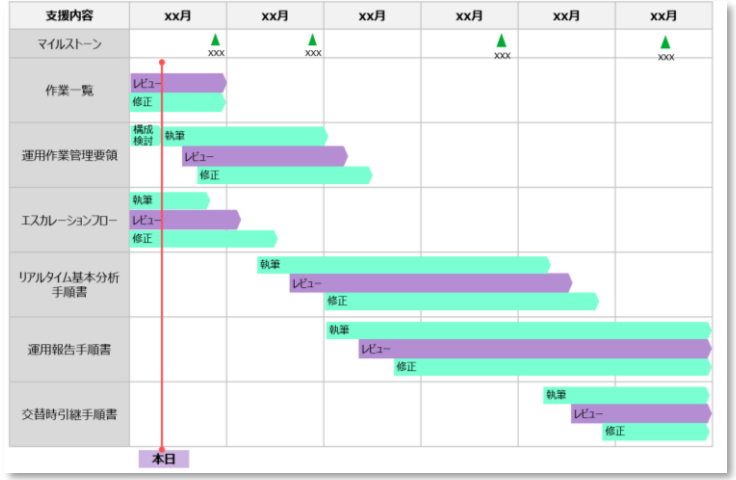
【 SOC構築ロードマップ 】



【 運用体制構築 年間スケジュール例 】



【 運用ドキュメント作成支援スケジュール 】



導入実績

➢ 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

※ 上記表に記載外の製品に関しても、ご相談に応じて対応可能です。

SOC運用 セキュリティログ監視サービス 【1/2】

- お客様のアラートを監視/分析し、お客様の運用負担軽減およびインシデントの早期検知・解決を実現

提供価値

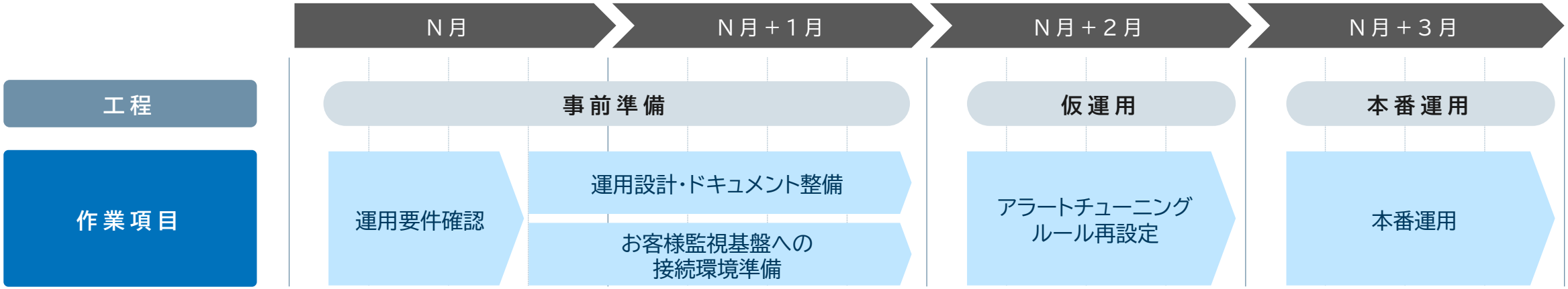
■効率的なアラート対応および、正誤判定を含む詳細なログ調査が可能

- SIEM/UEBAなどセキュリティ機器の検知ルールを適切にチューニングすることで、誤検知/過検知を抑制して真に危険なアラートのみ調査可能となります。
- 高度なセキュリティ知識を有したセキュリティアナリストが分析を行うことで、相互分析によるインシデント早期解決や正誤判定が可能となります。

■セカンドオピニオンによる品質向上

- お客様SOCの調査/分析結果に対するセカンドオピニオンを実施し、自社SOC組織の品質を向上させます。

導入スケジュール例（既存SOCが存在する場合）※



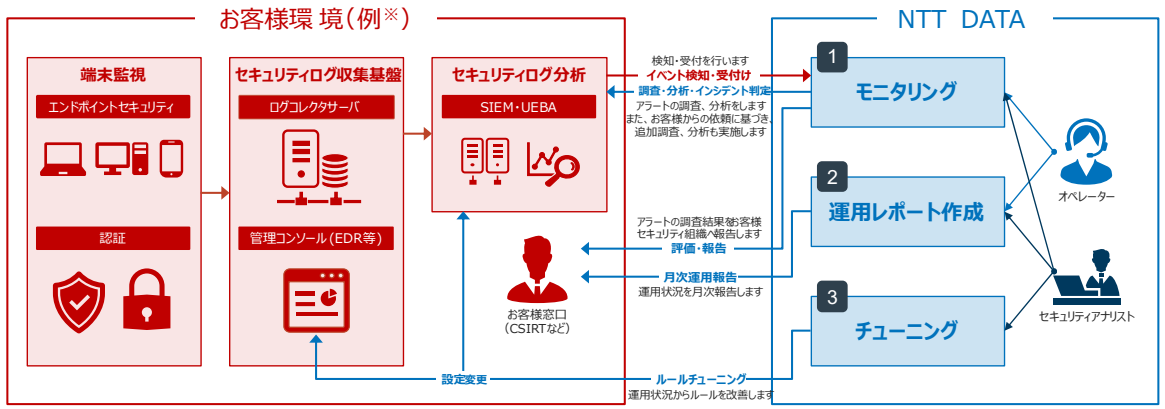
※ 既存SOCが存在しない場合は、弊社の提供するUnifiedMDR® SOC構築サービスをご検討下さい

SOC運用 セキュリティログ監視サービス 【2/2】

- お客様のアラートを監視/分析し、お客様の運用負担軽減およびインシデントの早期検知・解決を実現

サービスイメージ

■サービス提供体制イメージ



■対象製品一覧※

分類	処理概要	製品名
Identity	▪ ID管理 ▪ 二要素認証	• Okta • Microsoft Entra ID
Hygiene	▪ 未管理端末の把握 ▪ パッチ適用/状況把握	• Tanium • Microsoft Intune
SWG	▪ 暗号化通信の監視 ▪ クラウドの利用制御	• Microsoft Defender for Cloud Apps
EDR (Endpoint Detection and Response)	▪ ファイルのふるまい検知 ▪ 端末管理の自動化	• CrowdStrike • Microsoft Defender for Endpoint
UEBA (User and Entity Behavior Analytics)	▪ 怪しい振る舞いの検知	• Exabeam Security Analytics • Microsoft Sentinel

導入実績

➢ 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

※ 上記表に記載外の製品に関しても、ご相談に応じて対応可能です。

02

CSIRT構築／運用サービスのご紹介

NTT DATA UnifiedMDR® for Cyber Resilience 全体像サービスカット

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

SOC

SOC構築サービス

- SOC運用の監視基盤となるSIEM構築を支援（オプションでSOAR、UEBA等も追加）
- 現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

- 監視基盤構築
- 運用体制構築

SOC運用サービス

- お客様のアラートを監視/分析し、お客様の運用負担の軽減およびインシデントの早期解決実現

- セキュリティログ監視

CSIRT

CSIRT構築サービス

- 世界各地でのインシデントレスポンスを行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

CSIRT運用サービス（平時）

- インシデントレスポンス（IR）に備えた技術、体制、規則の改善および将来の目指す姿に向けたロードマップを作成/提案

- IRディレクター

CSIRT運用サービス（有事）

- 経験豊富なセキュリティ専門家が、インシデント発生から終結までトータルで支援/代行

- インシデントハンドリング
- フォレンジック
- IR対策フォロー

CSIRT構築/運用サービス 提供効果

本サービスでは、**CSIRTの構想立案から要件定義・設計・構築・展開・運用・インシデント対応までをワンストップでお客様へサービスを提供**いたします。また、ワンストップでの提供を可能としつつ**個別サービスも用意**しておりますので、お客様のご要望に応じた形でサービス提供が可能です。

お客様のお悩み	対応サービス	サービス提供による効果
インシデント発生時に対応する専門組織が自組織に存在しないため、**CSIRTの設立が必要**	➢ **CSIRT構築サービス**	インシデント対応の要となる**CSIRT体制を、お客様のニーズに合わせて最適な形で構築**します
CSIRTの組織自体は存在するものの、**運営まで手が回らず品質に懸念**が残る	➢ **IRディレクターサービス**	お客様CSIRTの現状の運用体制・手順を整理し直し、実際に起こり得るインシデント発生を想定した**適切なインシデント対応体制に整備します**
CSIRT運営自体には問題ないが、メンバーの経験不足など**インシデント発生時の対応に不安**が残る	➢ **インシデントハンドリング** ➢ **フォレンジック**	経験豊富なセキュリティ専門家が**インシデント発生から終結までトータルで支援/代行**し、迅速なインシデント終息を実現します
インシデント対応の終息後、**再発防止に向けた反省・改善活動の支援**が欲しい	➢ **IR対策フォロー**	インシデント対応終息後のフェーズにおける、**類似事象発生箇所の点検や、再発防止策を含む対策計画/ロードマップを提案**いたします

CSIRT構築サービス 【1/2】

- 世界各地でのインシデント対応を行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

提供価値

■グローバル規模のセキュリティに対応した、お客様独自のSOCを一気通貫に構築

- 弊社グループの世界規模（70ヵ国、約20万人）でのセキュリティ組織を構築/運用する中で培ったノウハウを元に、お客様のビジネス/業界ニーズに沿った実効性のある最適なSOCを構築します。

■セキュリティ経験豊富な専門家による対応

- 業界内最高峰の弊社組織内SOCを構築/運用している専門家が、お客様のインシデントレスポンス組織の構築と運用体制の整備をご支援します。

実施事項

	1. 要件定義	2. PoC実施	3. 設計/構築	4. 展開/運用/改善
実施事項	• ヒアリング/ドキュメント調査 • Gap分析	• 構築タスクの洗い出し • 計画策定	• 運用ドキュメントの作成 • CSIRT要員の調整	• 試運転支援
実施概要	▸ お客様へのヒアリングや既存文書の確認等を通じ、お客様のCSIRTやインシデント対応に関わる既存の組織、体制、ルール、プロセス等の状況を詳細に把握 ▸ アセスメントや業界基準をベンチマークとし、お客様のビジネス/ミッションに沿ったTo-Be像を策定することで、As-Is（現状）とTo-Be（理想）のGapを可視化	▸ Gap分析結果を元に、Gapを埋める構築タスクの洗い出し ▸ お客様のビジネス/ミッションに沿って構築タスクの優先度を決定し、お客様の予算およびスケジュールを考慮したロードマップを策定	▸ アラート発生時のインシデントレスポンスフロー、トリアージ基準、運用マニュアルなどを策定 ▸ CSIRT運用に必要な要員のスキルセット、人数を提案 ・ お客様にて要員確保が困難な場合、弊社CSIRT運用サービスにて、構築後の運用を一気通貫でご支援いたします	▸ 本番稼働に向け、構築された環境の試運転を支援。試運転期間中に発生した課題、チューニングなどの対処を行うことにより、円滑な本番稼働への切り替えを実現
成果物	✓ 要件定義現状確認書	✓ 構築PJ計画書 ✓ 予定表	✓ 運用ドキュメント	✓ IR試運転結果（IR訓練結果） ✓ 課題一覧

CSIRT構築サービス 【2/2】

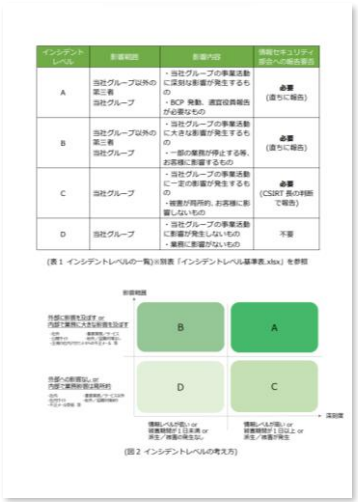
- 世界各地でのインシデント対応を行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

サービスイメージ

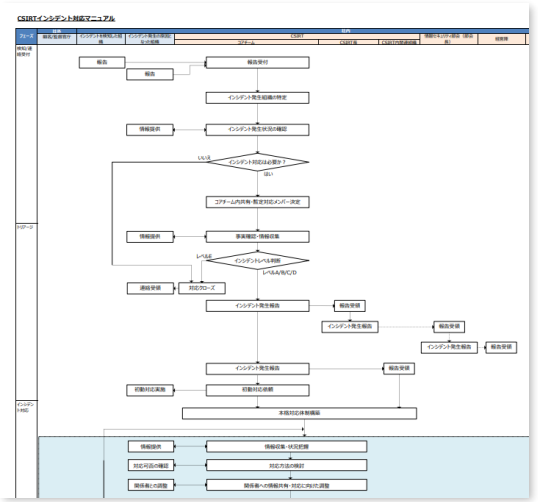
■CSIRT構築のロードマップ策定例

	FY202x			
	1Q	2Q	3Q	4Q
ロードマップ（参考）	体制検討			マニュアル整備 訓練実施 外部委託検討 ツール導入検討
CSIRT構築スケジュール（案）	ミッション/スコープ/インシデント/サービス(外部委託有無)の定義	社内/社外連携、対応フロー策定	マニュアル策定（従業員向け/CSIRT向け）	訓練実施/改善 外部委託検討、選定
			リソース確保、部会承認 要員定義/育成/計画	
タスク概要（案）	• ミッション(目的、建付け)の検討、明文化 • スコープ(会社、システム、インデント)検討、明文化 • インシデントの種別整理、レベル定義、明文化 • サービスの定義、外部委託有無検討、明文化	• 社内連携(インシデント発生組織、上位委員会、総務部、法務、広報等関連部署)の確認 • 社外連携(監督省庁、業界団体、セキュリティ団体)の確認 • インシデント対応フロー、連携フローの整理	• CSIRT要員向けおよび従業員向けマニュアル策定 • 人材、機器、ツール等リソース確保 • 情報セキュリティ部会説明、承認 • CISRT要員のスキル定義、育成、計画策定	• インシデント対応訓練実施、マニュアルや対応フローの改善 • 外部委託するサービスについて、委託先の検討、選定

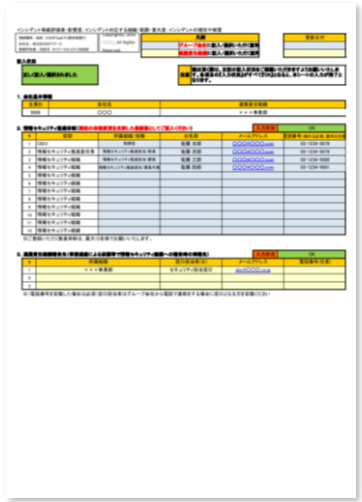
■CSIRT構築の運用ドキュメント例



【インシデントレベルに応じた対応書】



【インシデントレスポンスフロー】



【インシデントレスポンス連絡先管理簿】

導入実績

➢ 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

CSIRT運用（平時） IRディレクターサービス 【1/2】

- インシデントレスポンス（IR）に備えた技術、体制、規則の改善および将来の目指す姿に向けたロードマップを作成/提案

提供価値

■経営視点に基づく優先度を加味したロードマップの提示

- インシデントレスポンスに対するルール、技術、人の状況を確認し、経営層視点で改善案および優先順位を付けたロードマップをお客様とともに策定します。

■インシデント発生の予防活動、およびインシデントの早期対応を目指した準備活動の支援/代行

- お客様CSIRT組織の運用体制/環境を最適化すべく整備を行い、インシデント発生を抑制する予防活動と、インシデント発生時に早期対応を可能とする準備活動を支援/代行します。

実施事項

	1. 現状把握	2. ロードマップ策定	3. 改善
実施事項	• 現状把握	• ロードマップ策定	• 試運転支援インシデント予防活動 • CSIRTドキュメント管理 • CSIRT運用の改善提案
実施概要	▸ お客様業務の理解を深めるとともに、CSIRT組織の機能と運用レベルを分析/評価して解決すべきセキュリティ上の課題を可視化。 お客様組織に適切なセキュリティレベルの目標を設定し、明確にした強化/改善ポイントを整理する	▸ 現状把握の結果を基に、経営層視点を交えながらCSIRT組織の改善計画を立案/整理。セキュリティ製品の導入、CSIRTメンバの教育、インシデントレスポンスフローの見直しなど、お客様CSIRT組織の課題解決に向けたロードマップを策定	▸ ロードマップに基づき、経験豊富なセキュリティ専門家が、CSIRT運用における各業務が最適に実施されるように運用体制/環境を整備しながら、お客様組織内CSIRTをサポート
成果物	✓ CSIRT運用分析評価レポート	✓ ロードマップ	✓ CSIRT改善活動レポート

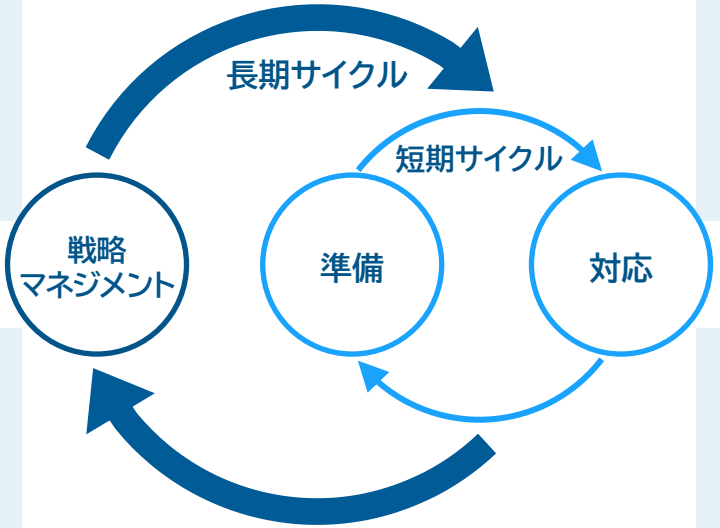
CSIRT運用（平時） IRディレクターサービス 【2/2】

- インシデントレスポンス（IR）に備えた技術、体制、規則の改善および将来の目指す姿に向けたロードマップを作成/提案

サービスイメージ

■戦略マネジメント：現状把握、ロードマップ策定

- 現在機能/運用レベルの評価と可視化
- 目標レベルと強化/改善ポイントの整理
- 上記の結果を基にロードマップを策定します



■対応：CSIRTドキュメント管理

- 定期的にアラート管理簿、インシデント管理簿、IT資産管理簿などのドキュメント類の棚卸管理/支援を実施します

■準備：インシデント予防活動

- 経験豊富なセキュリティ専門家が、CSIRT運用における各業務が最適に実施されるように運用体制/環境を整備しながら、お客様組織内CSIRT運用を支援します

■対応：CSIRT運用の改善提案

- セキュリティ時事情報、動向からのドキュメント見直し提案、セキュリティツールの最新化対応等によりセキュリティ運用を見直します

導入実績

➢ 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

※ 上記表に記載外の製品に関しても、ご相談に応じて対応可能です。

CSIRT運用(有事) インシデントハンドリングサービス 【1/2】

- 経験豊富なセキュリティ専門家が、インシデント発生から終結までトータルで支援/代行

提供価値

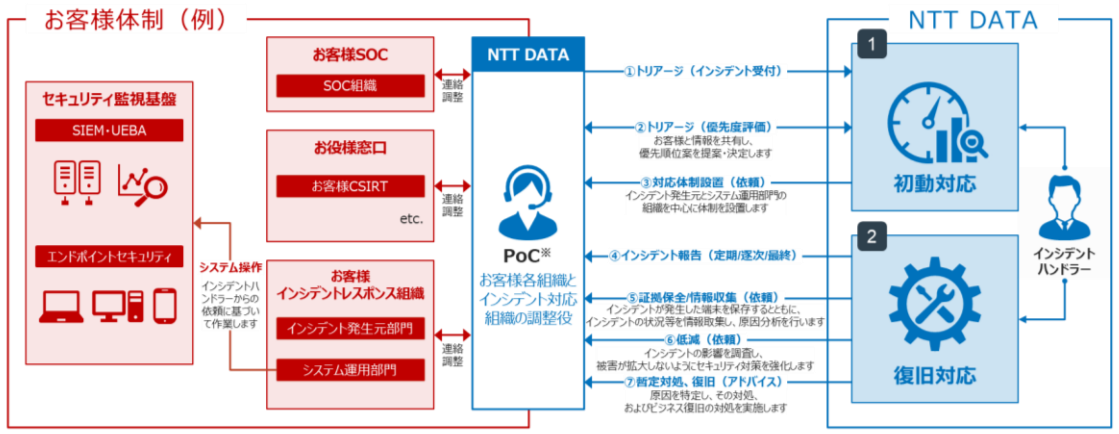
■経験豊富なセキュリティ専門家が、インシデントレスポンスをクロージング

- 重大なサイバーインシデント発生時に、経験豊富なセキュリティ専門家を派遣し、クロージングまで責任もって対応いたします。
- 技術的対応はもちろんのこと、インシデントに関する最終報告までもご支援いたします。

サービスイメージ

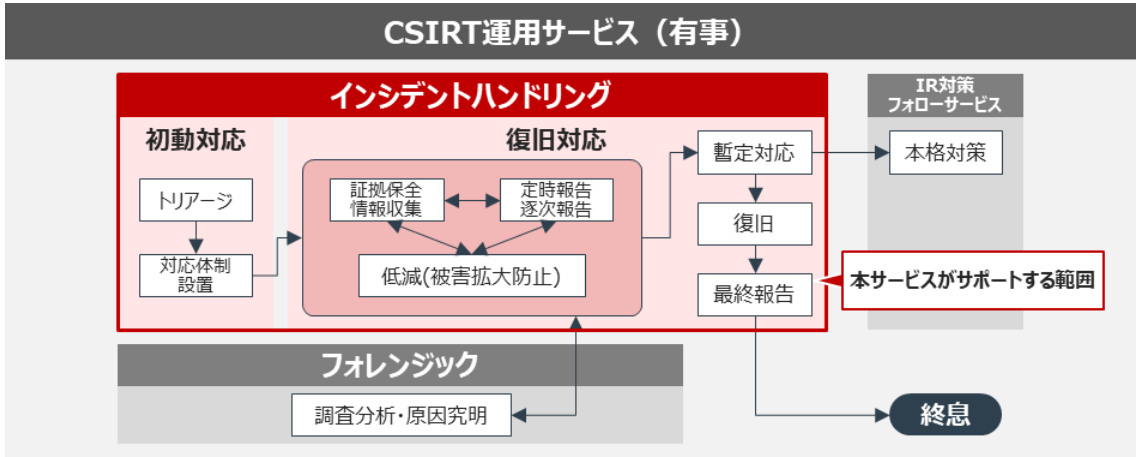
■サービス提供体制例

- インシデントハンドラーは、お客様のセキュリティ・システム担当部署と連携を取りながらトリアージやNW遮断など対処の判断や指示を出します。



■業務スコープ

- インシデントハンドリングサービスの業務スコープは以下となります。

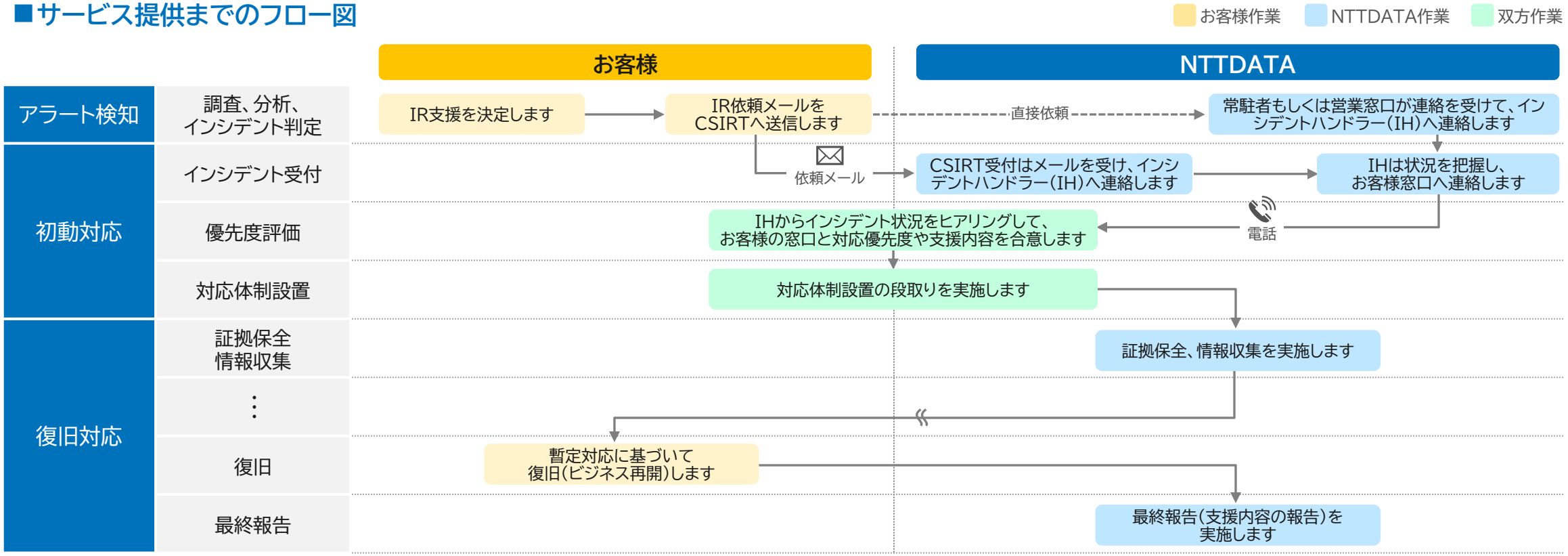


CSIRT運用(有事) インシデントハンドリングサービス 【2/2】

- 経験豊富なセキュリティ専門家が、インシデント発生から終結までトータルで支援/代行

サービスイメージ

■サービス提供までのフロー図



導入実績

- 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

CSIRT運用(有事) フォレンジックサービス 【1/2】

- 経験豊富なセキュリティ専門家が、インシデントの調査分析、原因究明を実施

提供価値

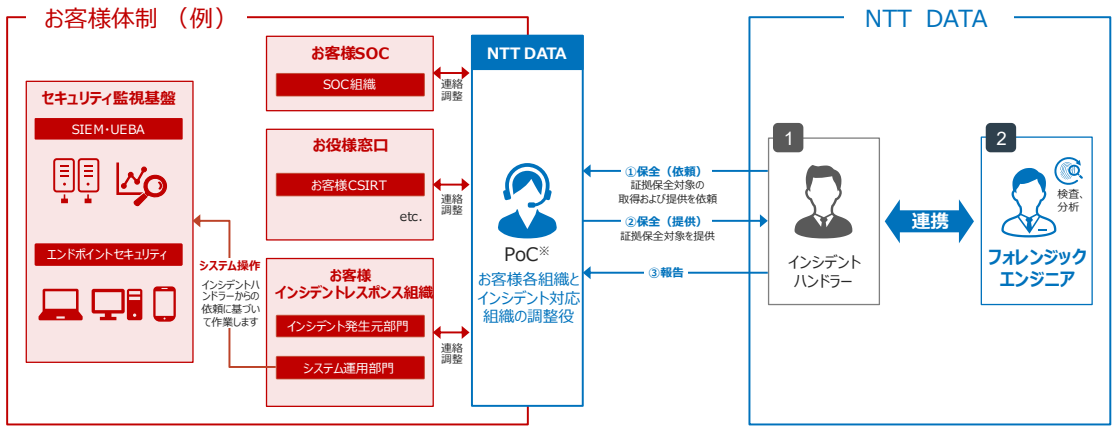
■多様なインシデント事象の調査

- 標的型攻撃、マルウェア感染、不正アクセス、情報漏洩等、多様なインシデント事象について調査します。
- またネットワークフォレンジック、ホストフォレンジック、マルウェア解析、ログ分析等、適切な調査手法/ツールを用いて効率的/効果的に調査します。

サービスイメージ

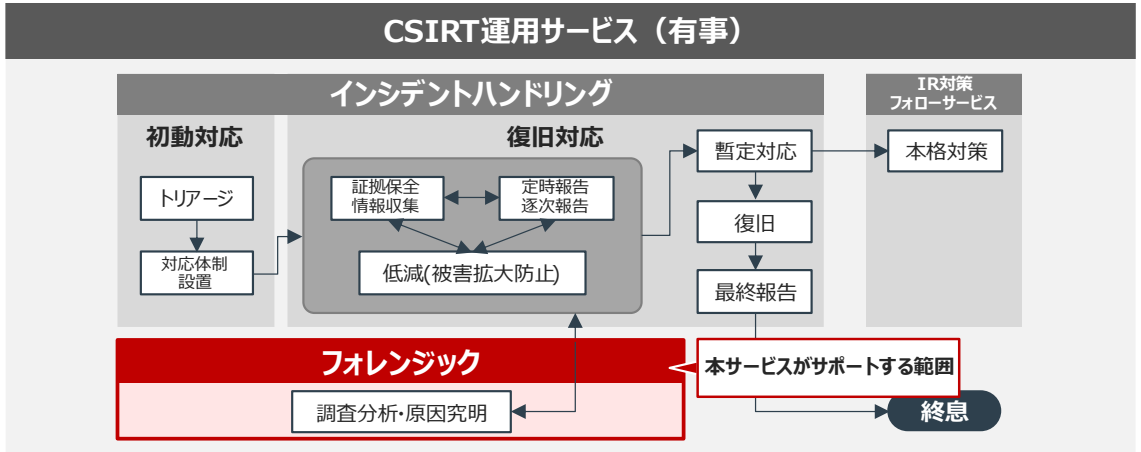
■サービス提供体制例

- フォレンジックエンジニアが、インシデント対応の証拠保全から受領した端末等を調査分析/原因究明を行い、お客様内部で何が起きているのかを判断します。



■業務スコープ

- フォレンジックサービスの業務スコープは以下となります。



CSIRT運用(有事) フォレンジックサービス 【2/2】

- 経験豊富なセキュリティ専門家が、インシデントの調査分析、原因究明を実施

サービスイメージ

■調査手法例

ファスト フォレンジック

EDR製品が導入済みである場合は該当製品のログを活用し、未導入である場合は、調査用の情報収集ツールを使用する。また、被疑対象を特定するため、短期間に広範囲の調査を実施する。

フル フォレンジック

被疑端末特定後、メモリダンプ、ファイルスタンプ分析、ストレージ(HDD等)のデータ復元などを含んだ詳細な調査を実施する。

ネットワーク フォレンジック

攻撃の経路上にあると想定されるFWやProxyなどのネットワーク機器に関するログをもとに、被疑対象への通信有無の調査、被疑対象に対する通信内容(時間帯・データ量)の調査を実施する。

導入実績

- 官公庁、金融機関、大手製造業など、様々な業種/業態での導入実績があります。

CSIRT運用(有事) IR対策フォローサービス 【1/2】

- インシデントレスポンス後の類似事象発生個所の点検、再発防止策を含む対策を提案します。

提供価値

■お客様の資産を守るセキュリティのあるべき姿を可視化し、再発防止に向けた事後活動をサポート

- インシデント対応後に再発防止に向けた改善活動を支援すべく、お客様組織へのヒアリング、ドキュメント調査、Gap分析を通じて現状を把握・分析いたします。
- 現状分析を基に、経験豊富なセキュリティ有識者が対策案や優先度を整理し、お客様における今後のあるべき姿を想定した対策導入ロードマップをご提示いたします。

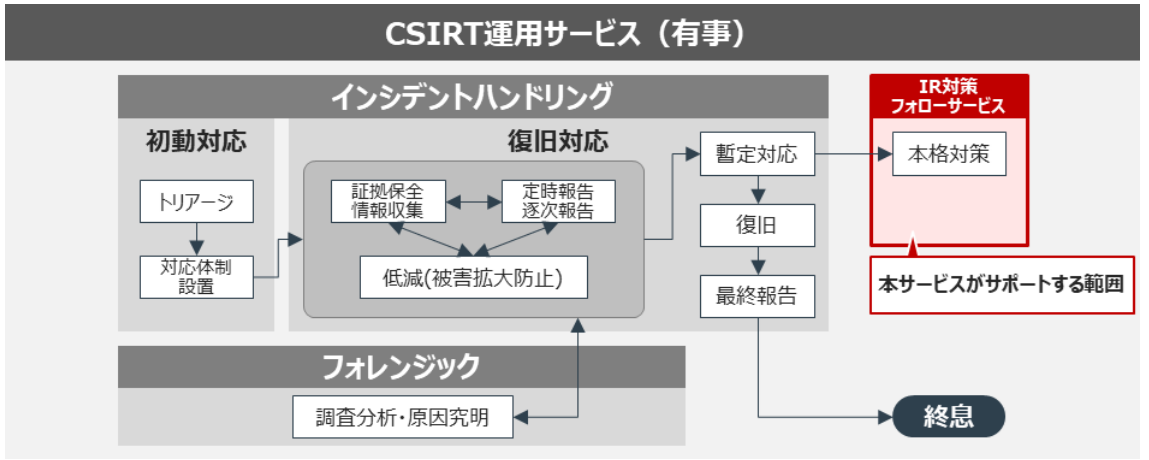
サービスイメージ

■実施事項

	1. 現状把握	2. ロードマップ策定
実施事項	• ヒアリング • ドキュメント調査 • Gap分析	• 対策タスクの洗い出し • ロードマップ策定
実施概要	‣ お客様へのヒアリングやインシデント報告書等の確認等を通じて、インシデントの暫定対応とお客様のセキュリティ監視運用に関わる既存の体制、ルール/プロセス、技術的環境の状況を把握 ‣ 類似を含めたインシデントを再発しないようにTo-Be像を具体化することで、As-IsとTo-BeのGapを可視化(Gap分析)	‣ Gap分析結果を元に、Gapを埋める横展開を含めた対策タスクの洗い出し ‣ お客様のビジネス/ミッションに沿って対策タスクの優先度を決定し、お客様の予算およびスケジュールを考慮したロードマップを策定
成果物	✓ ヒアリング・調査報告書 ✓ Gap分析結果報告書	✓ 対策タスク一覧 ✓ ロードマップ

■業務スコープ

- IR対策フォローサービスの業務スコープは以下となります。



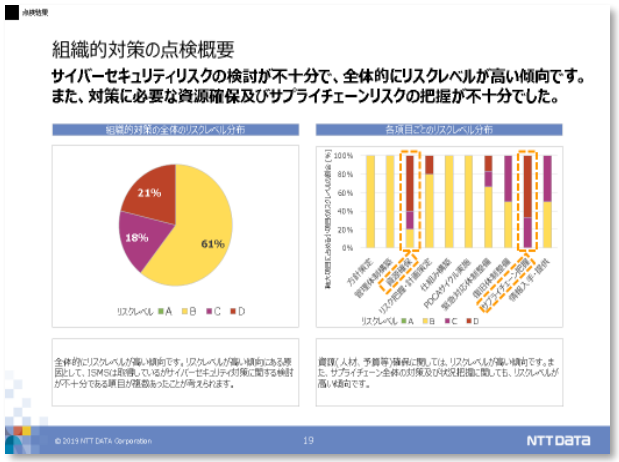
CSIRT運用(有事) IR対策フォローサービス 【2/2】

- インシデントレスポンス後の類似事象発生個所の点検、再発防止策を含む対策を提案します。

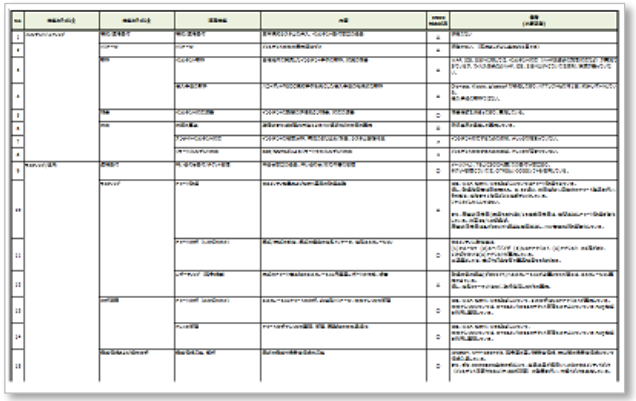
サービスイメージ

■成果物例

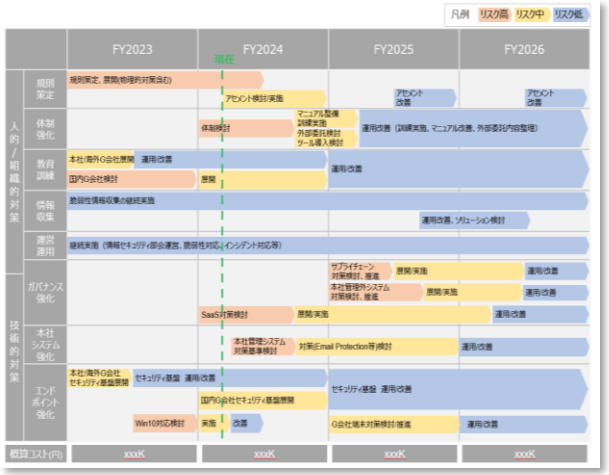
【 Gap分析結果報告書 】



【対策タスク一覧 】



【ロードマップ 】



導入実績

- 金融機関、金融機関向けシステム、鉄道事業者、運輸系企業グループ、通信系企業など、様々な業種/業態での導入実績があります。

03

コンサルティングサービスのご紹介

NTT DATA UnifiedMDR® for Cyber Reslience 全体像サービスカット

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

コンサルティング

セキュリティポリシー策定サービス

- 統一された共通グローバルポリシー・スタンダードの制定および、各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

リスクアセスメントサービス

- システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

SOC/CSIRT成熟度評価サービス

- セキュリティ対応組織の業務につき、業界団体ガイドライン、弊社知見をもとにした評価基準を用いて機能整備状況、運用状況を評価し成熟度を可視化

IR教育/訓練サービス

- お客様のご要望や組織が目指すセキュリティの目的に応じて多種多様な教育プログラムを計画/実施し、サイバーセキュリティの専門家育成を支援

TLPTサービス

- 疑似インシデントを計画、実行し、システムのセキュリティ対策状況およびSOC/CSIRTの対応力を評価、改善策提示

ソリューション構築

ゼロトラスト環境構築サービス

- ゼロトラスト環境を構築していく上で必要となるセキュリティソリューションの導入/構築を支援

＜導入を支援するセキュリティソリューションの一例＞
・IDaaS ・SWG etc.

コンサルティングサービス 提供効果

本サービスでは、経験豊富なセキュリティの専門家が、お客様が情報セキュリティ上で抱える課題に対し、診断や評価、セキュリティポリシーの作成、セキュリティ人材育成と言った形でお客様のセキュリティ向上に向けて適切な施策を提供します。

お客様のお悩み	対応サービス	サービス提供による効果
グローバルでのセキュリティポリシーやセキュリティ施策が統一出来ていない。	➢ セキュリティポリシー策定サービス	グローバル統一または各地域ごとのポリシー・スタンダードを策定することで、グローバルでの情報資産守るセキュリティ体制を円滑に運用できるようになります
自組織のセキュリティの状況が把握出来ていない。 また、どのようなリスクを抱えているかも不明瞭	➢ リスクアセスメントサービス ➢ SOC/CSIRT成熟度評価サービス ➢ TLPTサービス	お客様に起こり得るインシデントやセキュリティ体制上の弱点や特徴を分析し、セキュリティの現況把握や適切な対応施策のアドバイスを実施します
社内に**セキュリティ人材が不足**しており、 既存メンバーも**インシデント対応の経験が不足**	➢ IR教育/訓練サービス ➢ TLPTサービス	現実に発生しているインシデントに対応できる実戦的で高度なセキュリティ人材を育成し、セキュリティ専門家の不足を解消します

コンサルティング セキュリティポリシー策定サービス 【1/2】

- 統一された共通グローバルポリシー/スタンダードの制定および、各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

提供価値

■統一された共通グローバルポリシー・スタンダードの制定

- NTTデータグループが取り組んできた知見を活かし、地域、会社によらないグループ全体におけるセキュリティポリシー・スタンダードの策定を支援します。

■各地域の商習慣/法律に応じた個別ポリシー・スタンダードの制定

- グループ全体のセキュリティポリシー・スタンダードを作成後、現地の商習慣や法規制を鑑みてグローバルポリシー・スタンダードに準じた形で個別ポリシー・スタンダードの制定を支援します。

実施事項

	1. 方針検討	2. お客様体制整備	3. ポリシー改訂/基準作成	4. ポリシー/基準海外展開
実施事項	• 方針検討	• お客様体制整備 • ポリシー展開ロードマップ作製	• ポリシー改訂 • 基準作成	• ポリシー/基準海外展開
実施概要	▸ お客様へのヒアリングや既存文書の確認等を通じ、お客様のCSIRTやインシデント対応に関わる既存の組織、体制、ルール、プロセス等の状況を詳細に把握 ▸ アセスメントや業界基準をベンチマークとし、お客様のビジネス/ミッションに沿ったTo-Be像を策定することで、As-Is(現状)とTo-Be(理想)のGapを可視化	▸ Gap分析結果を元に、Gapを埋める構築タスクの洗い出し ▸ お客様のビジネス/ミッションに沿って構築タスクの優先度を決定し、お客様の予算およびスケジュールを考慮したロードマップを策定	▸ アラート発生時のインシデントレスポンスフロー、トリアージ基準、運用マニュアルなどを策定 ▸ CSIRT運用に必要な要員のスキルセット、人数を提案 ・お客様にて要員確保が困難な場合、弊社CSIRT運用サービスにて、構築後の運用を一気通貫でご支援いたします	▸ 本番稼働に向け、構築された環境の試運転を支援。試運転期間中に発生した課題、チューニングなどの対処を行うことにより、円滑な本番稼働への切り替えを実現
成果物	✓ 要件定義現状確認書	✓ 構築PJ計画書 ✓ 予定表	✓ 運用ドキュメント	✓ IR試運転結果(IR訓練結果) ✓ 課題一覧

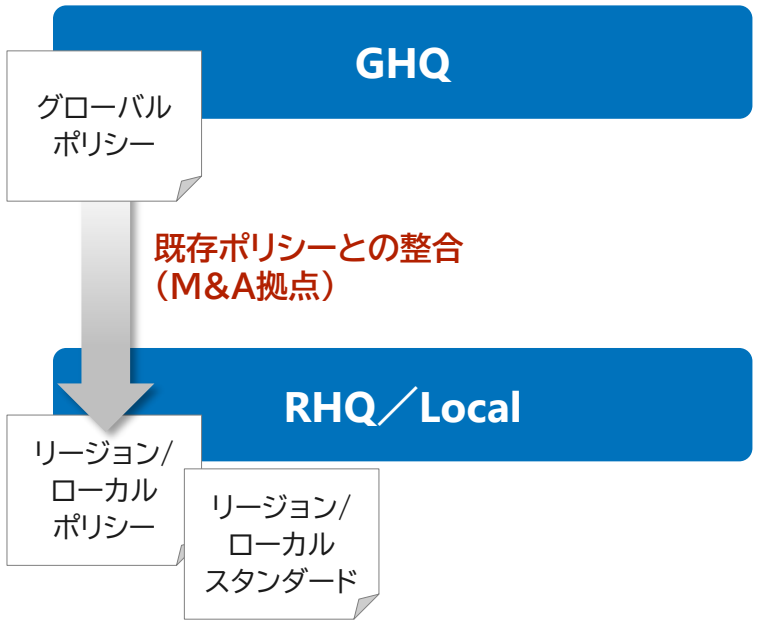
コンサルティング セキュリティポリシー策定サービス 【2/2】

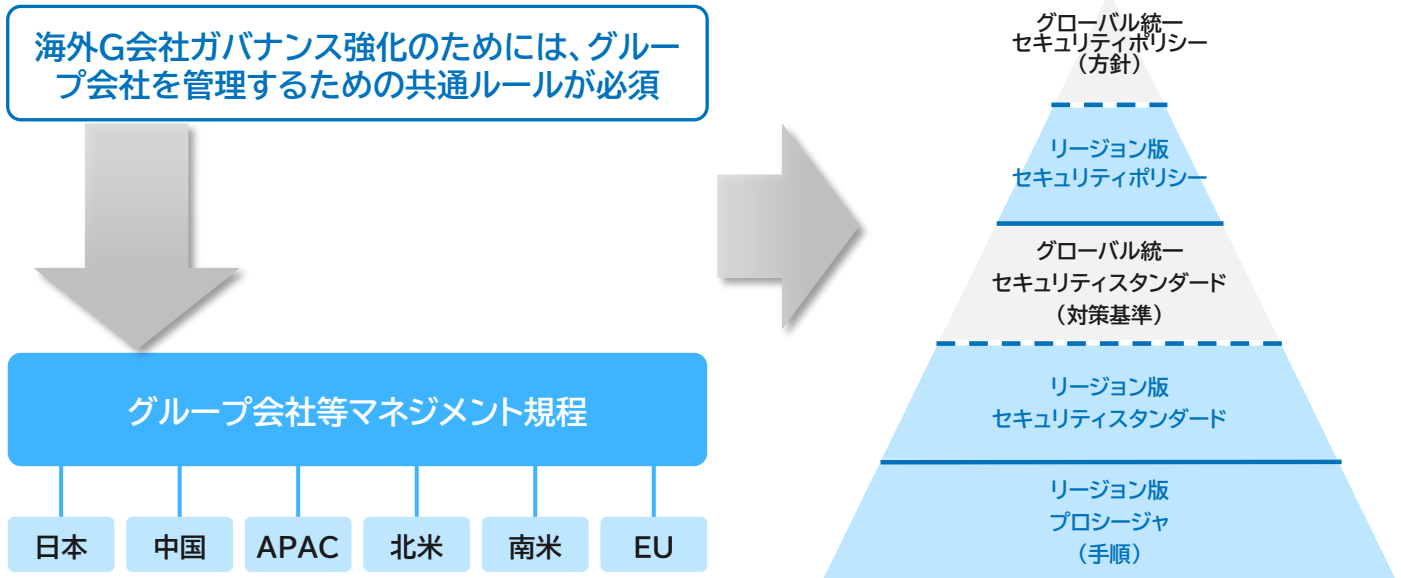
- 統一された共通グローバルポリシー/スタンダードの制定および、各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

サービスイメージ

■サービスイメージ図

- GHQにてセキュリティポリシーを作成、RHQもしくは海外拠点では、ローカルの慣習や法規制などを鑑みてグローバルポリシーに準じたポリシーやスタンダード類を作成する





導入実績

➢ 金融機関、金融機関向けシステム、鉄道事業者、運輸系企業グループ、通信系企業など、様々な業種/業態での導入実績があります。

コンサルティング リスクアセスメントサービス 【1/2】

- システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

提供価値

■セキュリティ対策の問題点を可視化

- システムや組織の対策状況を網羅的に点検することで、自組織で実施しているセキュリティ対策の問題点を洗い出すことが可能です。

■お客様のセキュリティのあるべき姿を可視化

- 本アセスメントを結果をもとに対策案や優先度を整理し、お客様のセキュリティ体制おける今後のあるべき姿を想定した対策導入ロードマップをご提示いたします。

実施事項

	1. 事前準備	2. 調査・ヒアリング	3. リスク分析・対策案検討	4. 報告
実施事項	• セキュリティ観点でのアセスメントシートの準備 • 現状分析ヒアリングシートの準備	• 調査・ヒアリングの実施 • 現地担当者へのリモートでのサポート	• リスク分析 • 対策案の検討と優先度付け・整理	• ご報告 • ロードマップの策定
実施概要	▸ アセスメントの実施計画策定 ▸ アセスメントシート作成 ▸ 現状分析ヒアリングシートの準備（ヒアリング内容：IT基本情報、NW構成図、管理表、体制等）	▸ アセスメントシートに基づき、現状分析ヒアリングシートを用いてのシステム部門や経営層へヒアリングを実施 ▸ ヒアリングの際には、弊社スタッフが現地担当者様をリモート説明会を実施するなどしてサポート	▸ ヒアリング結果に基づき、現状の問題点や改善点を整理しリスクを分析 ▸ リスク分析結果をもとに、優先すべき問題点・改善点の順位付けを行い、効率的な対策計画を検討	▸ 最終報告資料を作成し、報告 ▸ お客様のセキュリティ体制のあるべき姿を明確にし、その実現に向けたセキュリティ施策の計画・ロードマップを提示
成果物	✓ アセスメントシート ✓ 現状分析ヒアリングシート	✓ ヒアリング結果整理書	✓ リスク分析結果 ✓ 対策案検討一覧	✓ エグゼクティブサマリ ✓ 対策案ロードマップ

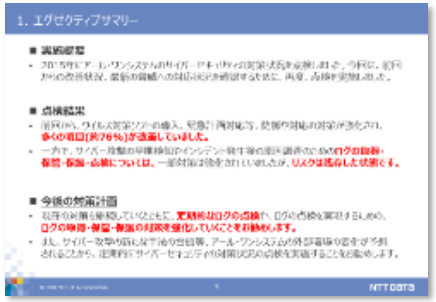
コンサルティング リスクアセスメントサービス 【2/2】

- システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

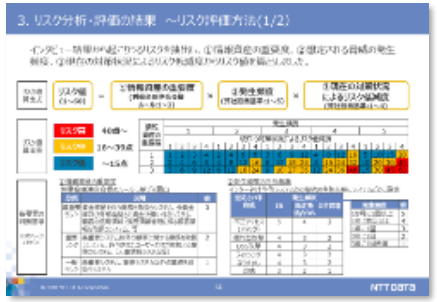
サービスイメージ

■成果物例※

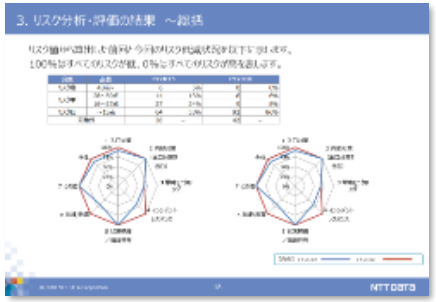
【エグゼクティブサマリ】



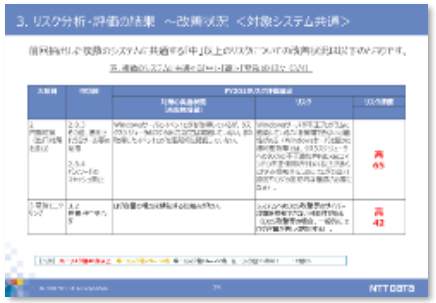
【評価方法】



【総括】



【リスク分析結果】



【対策案】

※注釈
成果物の書式はPowerPointまたは
Excelでのファイル形式を想定とします

導入実績

➢ 金融機関、金融機関向けシステム、鉄道事業者、運輸系企業グループ、通信系企業など、様々な業種/業態での導入実績があります。

※ 文書数などのボリュームは評価結果の内容により増減します。

コンサルティング SOC/CSIRT成熟度評価サービス 【1/2】

- 業界団体ガイドラインやNTTデータ独自の知見に基づく評価モデルを使用し、セキュリティ対応組織の機能整備・運用状況の成熟度を評価

提供価値

■SOC/CSIRT組織の現状を把握

- セキュリティ組織の成熟度を測る評価モデル(フレームワーク)を用いてお客様のセキュリティ組織を客観的に診断し、セキュリティ体制の到達度や課題・弱点を可視化します。

■セキュリティ機能強化項目の計画を支援

- お客様目指すべきセキュリティの理想像を設定するため、お客様状況を考慮した上で課題解決の優先度を決定し、機能強化項目の計画を支援します。

実施事項

	1. 既存SOC/CSIRT現状把握	2. 成熟度評価	3. 結果整理・目標設定
実施事項	• 実施計画策定 • ドキュメント調査・ヒアリング	• 課題整理 • アセスメント、報告書作成	• ご報告 • 方針提示
実施概要	▸ 評価対象となる組織やシステム範囲の確認や、調査の日程などを事前に調整しアセスメントの実施計画を策定 ▸ SOC/CSIRTとしての機能や役割が充足している項目、不十分な項目を明らかにするため、現状のSOC/CSIRT業務の内容、実施状況を既存文書から評価 ▸ お客様のセキュリティ担当部門関係者へヒアリングの実施	▸ 現状把握の結果を基に、成熟度評価モデルに基づき各項目ごとの分析・アセスメントを実施 ▸ 成熟度評価で明らかとなったお客様セキュリティ体制の強み・弱みといった特徴を数十の項目からなる報告書に整理	▸ 成熟度評価結果サマリーを最終報告書として提出 ▸ ロードマップに基づき、経験豊富なセキュリティ専門家がSOC/CSIRT運用における各業務が最適に実施されるよう、改善・強化ポイントについて助言と提案を実施
成果物	✓ アセスメント実施計画書 ✓ ヒアリング・ドキュメント類調査レポート	✓ 成熟度評価結果レポート	✓ 最終報告書 ✓ セキュリティ強化・改善策提案書

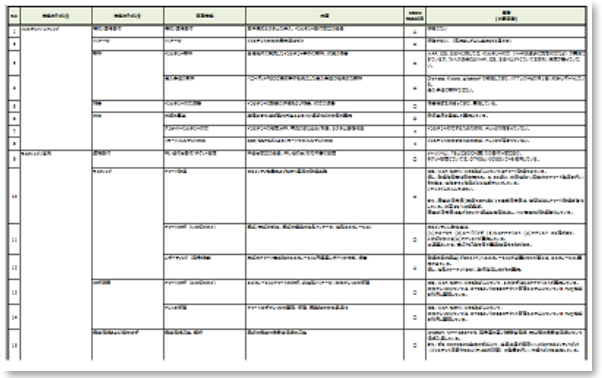
コンサルティング SOC/CSIRT成熟度評価サービス 【2/2】

- 業界団体ガイドラインやNTTデータ独自の知見に基づく評価モデルを使用し、セキュリティ対応組織の機能整備・運用状況の成熟度を評価

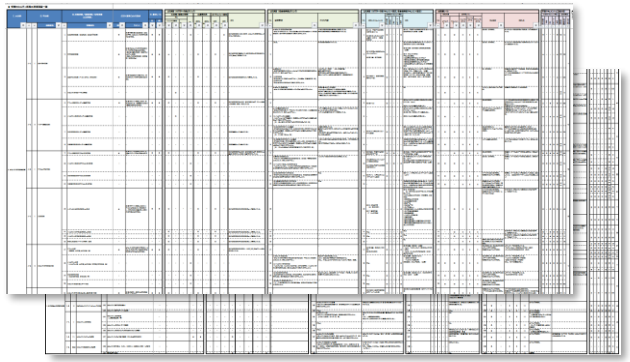
サービスイメージ

■成果物例※

【 Gap分析結果報告書 】



【対策タスク一覧 】



【ロードマップ 】

導入実績

➢ 金融機関、金融機関向けシステム、鉄道事業者、運輸系企業グループ、通信系企業など、様々な業種/業態での導入実績があります。

※ 文書数などのボリュームは評価結果の内容により増減します。

コンサルティング IR教育/訓練サービス 【1/2】

- 現状のインシデントレスポンスの手順、体制などにおける課題およびギャップを机上演習で明らかにする

提供価値

■サイバー攻撃対応に関する内容を理解し、適切に実践できることを支援

- 実際のサイバー攻撃を想定したシナリオに基づいた侵入・攻撃活動の検知、経営層、社外の利害関係者への告知・広報などの演習を総合的に実施することで、現実のサイバー攻撃によってもたらされるセキュリティインシデントへの対応を習得できます。

実施事項

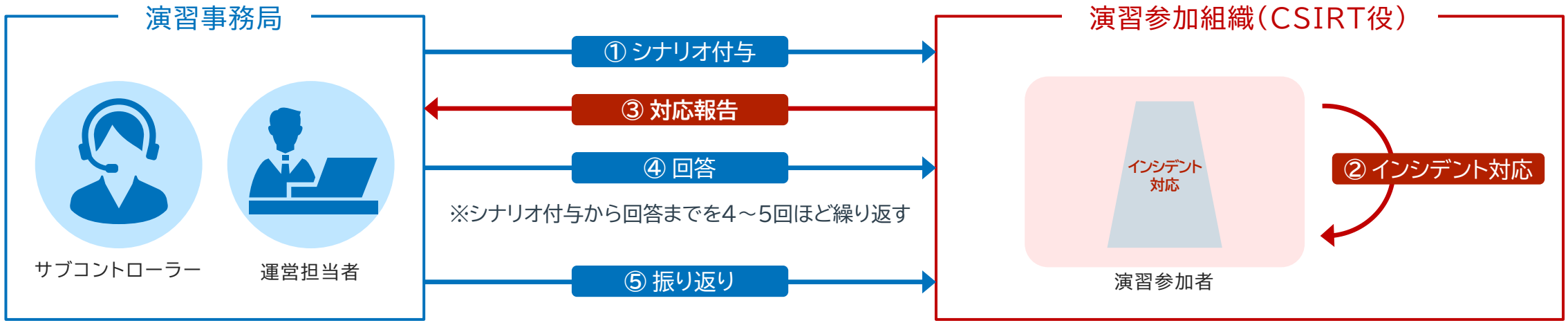
	1. 演習準備	2. 演習実施	3. 演習結果分析
実施事項	• 体制構築 • 演習/運営準備	• IR演習の実施	• ご報告 • 方針提示
実施概要	▸ IR演習を行う目的や評価テーマ、演習形式、演習対象組織をスコーピングし、IR演習シナリオを作成 ▸ 演習実施方法（オンライン/オフライン）や日程/環境を準備	▸ IR演習シナリオに基づきIR演習を実施し、評価する	▸ IR演習の評価結果から、IR演習の目的と演習参加者にの行動部分を分析する ▸ 分析結果を基に、結果報告資料を作成しお客様に報告を行う
成果物	—	—	✓ 結果報告書

コンサルティング IR教育/訓練サービス 【2/2】

- 現状のインシデントレスポンスの手順、体制などにおける課題およびギャップを机上演習で明らかにする

サービスイメージ

■サービス提供体制例



導入実績

- 金融、公共、通信、製造、運輸など、様々な業種/業態で導入実績があります

コンサルティング TLPTサービス 【1/2】

- 疑似攻撃に対するインシデント対応演習を実施し、攻撃者目線でお客様のサイバーインシデントへのレジリエンス強度を評価

提供価値

■攻撃者目線でシステムの安全性を評価

- 脅威インテリジェンス※を活用することで、現実世界で実際に起きている攻撃をもとにした疑似攻撃の演習シナリオを作成します。
- 今現在の現実世界で行われている攻撃に基づいた演習シナリオを実施することで、攻撃者目線でどのような攻撃手口や脆弱性が有効なのかを可視化することができます。

■インシデント発生時の被害・影響への復旧力（サイバーレジリエンス）の強化対策を支援

- 疑似攻撃を通じて組織や対応プロセスを含めて影響を評価することで、インシデント発生時の被害・影響の規模や範囲を可視化します。
- 可視化の分析結果をもとに、経験豊富なセキュリティ専門家の知見を踏まえたサイバーレジリエンス強化のためのアドバイスを提示します。

実施事項

	1. 事前準備	2. 攻撃シナリオ作成	3. 疑似攻撃実施	4. 総合評価・アドバイス
実施事項	• TLPT演習実施体制構築	• 脅威インテリジェンスによる分析 • 攻撃シナリオの作成	• 疑似攻撃詳細計画の作成 • 疑似攻撃実施	• 総合評価 • 対策方針アドバイス
実施概要	▸ お客様環境のヒアリングやリスクアセスメント資料をインプットし、TLPTのゴールを定める ▸ TLPTのスコープやチームの体制、スケジュール等を定めたプロジェクト実施計画書を作成	▸ 脅威インテリジェンスの調査・分析し、現実に発生が想定される脅威を特定する ▸ お客様環境に対して現実に発生する可能性があるサイバー攻撃のプロセスを攻撃シナリオとして作成	▸ 脅威インテリジェンスと攻撃シナリオを基に疑似攻撃に必要な「詳細計画」を作成 ▸ 詳細計画をもとに、お客様環境に疑似攻撃を実施	▸ 演習の防御側が適切な精度と期日でセキュリティインシデント対応（検知、調査、報告）を行えるかを管理・評価役が評価 ▸ 演習結果に対してコンサルタントの知見を踏まえ、今後の対策に向けたアドバイスを実施
成果物	✓ TLPT全体概要計画書	✓ 攻撃シナリオ調査結果報告書	✓ 疑似攻撃報告書	✓ 総合評価報告書（エグゼクティブサマリー）

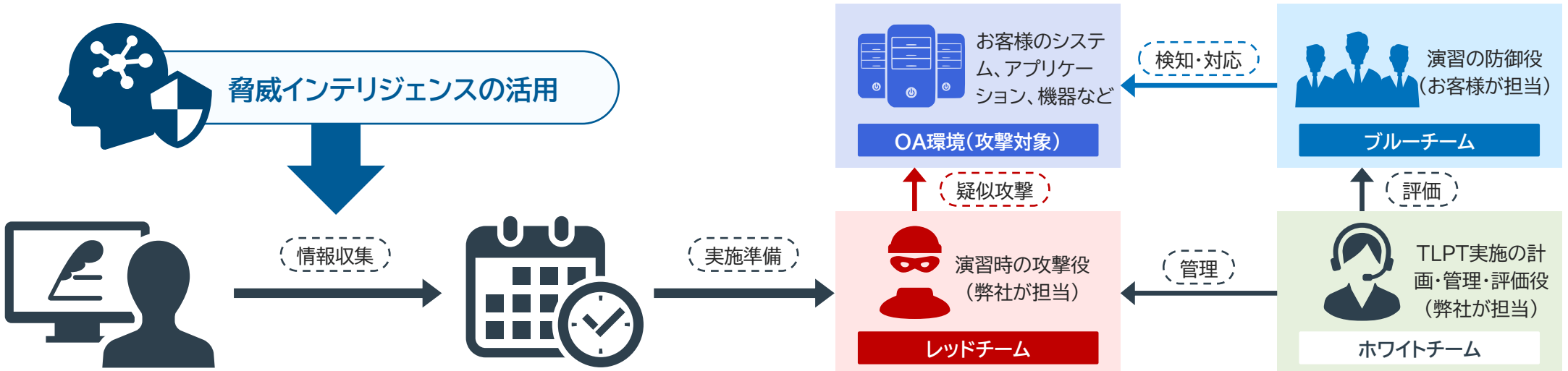
※脅威インテリジェンスとは、情報セキュリティの脅威に関する情報を収集・分析し、その根拠に基づいて専門家の知見が考慮された情報・データのことです。サイバー攻撃の防御に重要な役割を果たします。

コンサルティング TLPTサービス 【2/2】

- 疑似攻撃に対するインシデント対応演習を実施し、攻撃者目線でお客様のサイバーインシデントへのレジリエンス強度を評価

サービスイメージ

■サービス提供体制例



①攻撃シナリオ作成	②TLPT実施計画/管理	③疑似攻撃実施	④ブルーチーム評価

導入実績

- 金融、公共、通信、製造、運輸など、様々な業種/業態で導入実績があります

04

ソリューション構築サービスのご紹介

NTT DATA UnifiedMDR® for Cyber Reslience 全体像サービスカット

高度なセキュリティ運用を実現するため、下記サービスをご提供します。

コンサルティング

セキュリティポリシー策定サービス

- 統一された共通グローバルポリシー・スタンダードの制定および、各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

リスクアセスメントサービス

- システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

SOC/CSIRT成熟度評価サービス

- セキュリティ対応組織の業務につき、業界団体ガイドライン、弊社知見をもとにした評価基準を用いて機能整備状況、運用状況を評価し成熟度を可視化

IR教育/訓練サービス

- お客様のご要望や組織が目指すセキュリティの目的に応じて多種多様な教育プログラムを計画/実施し、サイバーセキュリティの専門家育成を支援

TLPTサービス

- 疑似インシデントを計画、実行し、システムのセキュリティ対策状況およびSOC/CSIRTの対応力を評価、改善策提示

ソリューション構築

ゼロトラスト環境構築サービス

- ゼロトラスト環境を構築していく上で必要となるセキュリティソリューションの導入/構築を支援

＜導入を支援するセキュリティソリューションの一例＞
・IDaaS ・SWG etc.

ソリューション構築サービス 提供効果

本サービスでは、世界70ヵ国、約20万人規模のゼロトラスト環境を構築した経験があるNTTデータの自社ノウハウを活用し、グローバル規模のセキュリティ体制に対応したゼロトラストセキュリティを構築支援いたします。

お客様のお悩み	対応サービス	サービス提供による効果
リモートワークなど**社外からの情報資産へのアクセス**が増え、従来型のセキュリティではセキュリティリスクに対応出来なくなった	➢ **ゼロトラスト環境構築サービス**	グローバル統一または各地域ごとのポリシー・スタンダードを策定することで、グローバルでの情報資産守るセキュリティ体制を円滑に運用できるようになります
内部犯による情報漏洩への対策を立てる必要がある	➢ **ゼロトラスト環境構築サービス**	内外問わず全ての通信を疑わしいものとして監視するゼロトラストセキュリティでは、内部からの不正なアクセスを検知・防御する仕組みを実現できます
グローバル各拠点ごとでバラバラに構築されている**セキュリティ環境を一つに統一**し、効率的なセキュリティ運用を実現したい	➢ **ゼロトラスト環境構築サービス**	グローバルで統一されたゼロトラスト環境を構築する事で、海外拠点で発生したインシデントに対しても統一されたプロセスで迅速に対応することができます

ソリューション構築 ゼロトラスト環境構築サービス 【1/2】

- インターネット利用の多様化に合わせたゼロトラスト環境構築

提供価値

■テレワーク等リモート環境の見直し

- 社外で使用する端末や社外からアクセスする機密情報を守るため、必要な対策を行います。

■本社、支社、海外拠点などのセキュリティポリシーの統一化

- 拠点ごとに異なるセキュリティ環境に対し、統一されたセキュリティポリシーを適用することでどの拠点からも同一に利用できるセキュリティ環境を実現できます。

実施事項

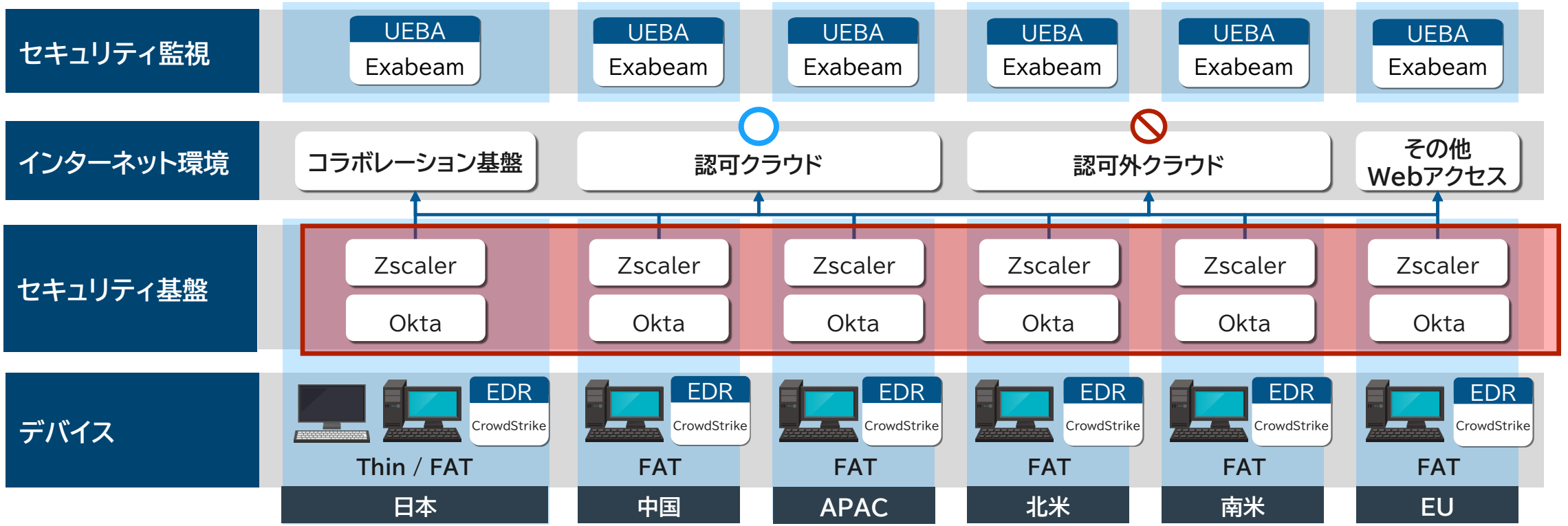
	1. 要件定義	2. 設計/PoC実施	3. 本格導入実施	4. 試運転支援
実施事項	• ヒアリング/ドキュメント調査 • Gap分析 • 構築タスクの洗い出し	• 設計書作成 • PoC	• ゼロトラストサービス/製品の本番環境導入	• 試運転支援
実施概要	▸ お客様へのヒアリングや既存文書の確認等を通じて、お客様のセキュリティ運用に関わる既存の体制、ルール/プロセス、技術的環境、課題を把握 ▸ お客様のTo-Be像を具体化することで、As-IsとTo-BeのGapを可視化 ▸ Gap分析結果を元に、Gapを埋める製品選定、構築タスクの洗い出し	▸ 選定したサービス/製品の導入に向けた設計、検証(PoC)を支援 ▸ PoCの結果を踏まえて、基本設計書など各種ドキュメントを作成	▸ PoCで得られたパラメータを反映した内容で、製品の本格導入を支援	▸ 本番稼働に向け、構築された環境の試運転を支援します(1か月程度)。 試運転期間中に発生した課題などの対処を行うことにより、円滑な本番稼働への切り替えを実現
成果物	✓ Gap分析結果報告書 ✓ 構築タスク一覧	✓ 設計書 ✓ PoC結果報告書	✓ 構築されたゼロトラスト環境 ✓ 試験結果	✓ 課題管理簿

コンサルティング TLPTサービス 【2/2】

- インターネット利用の多様化に合わせたゼロトラスト環境構築

サービスイメージ

■環境構築例（NTTデータの環境構築例）



導入実績

➢ 銀行、保険会社等の金融機関を中心に主要インフラ、自動車業界など、様々な業種/業態での導入実績があります。

※赤枠はゼロトラスト構築の対象製品です

05

Appendix

改訂履歴

版	改定日時	内容
1.0（初版）	2024/03/31	・初版を作成
1.1	2025/07/01	・陳腐化情報の削除、他
1.12	2026/02/12	・「世界59ヵ国、約19万人規模のゼロトラスト環境」の修正


NTT DATA