Customer Confidential

NTT DATA UnifiedMDR® for Cyber Resilience のご紹介

2024年1月
株式会社NTTデータグループ
サイバーセキュリティ技術部

目次

目次

セキュリティを取り巻く概況の変化

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

- 場所や端末によらず、業務を実施可能な環境

ビジネスのグローバル展開

- 企業の海外進出
- サプライチェーンの多様化

2 規制・規則の変化

日本

- 2020年：サプライチェーン攻撃に関する注意喚起
- 2022年：経済安全保障推進法

米国

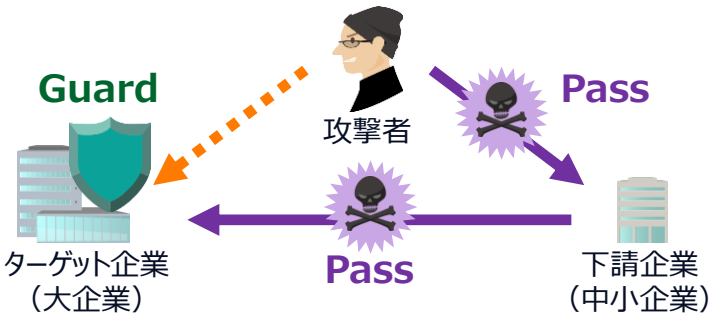
- 2021年：国家のサイバーセキュリティ向上に関する大統領令 (EO 14028)

EU

- 2022年：重要インフラセキュリティ対策強化
- 2022年：サイバーレジリエンス法案

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

「変化」に乗じたインシデントも発生

環境の変化に伴いインシデント原因や攻撃手法と目的も変化しており、セキュリティもその変化に対応していかなければなりません。

ワークスタイルの変化によるリスクの増大

- 急ごしらえのテレワーク環境は安全ですか？
- 社員のクラウド利用状況を把握できていますか？
- クラウドのセキュリティ設定に不備はありませんか？

年月	被害組織	攻撃	概要
2021/4	K社	VPN経由の攻撃	テレワーク推進で社内ネットワークが高負荷に。そこで緊急に設置した旧型VPN装置が狙われ、北米のVPN装置を経由して米国や日本のサーバから最大約39万人分の個人情報が流出。
2021/8	M社	シャドーIT (許可していないクラウドの利用)	再委託先企業の従業員が、取引先情報や個人情報などを含むデータを無許可でダウンロードし、個人利用の社外クラウドサービスへアップロード。
2021/1	R社	クラウドの設定不備	社外クラウドサービス上の保管情報が社外の第三者からアクセスされた。最大148万件の店舗・顧客情報が流出。

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**

国内・海外に拠点をお持ちの組織では
セキュリティレベルの弱い拠点がサイバー攻撃の入口となり
グローバル全体で脅威にさらされることも。

年月	被害組織	攻撃	概要
2021/10	S社	不正アクセス	インドネシア子会社に対し、ネットワーク上の不正アクセスで生産システムが一部停止。工場の一部で2日間稼働できず。
2020/12	K社	不正アクセス	タイ、インドネシア、フィリピン、米国などの海外拠点から日本国内のデータセンタへ不正アクセス。国内外のサーバ15台で不審な暗号化ファイルの形跡等、データ流出の疑い。
2020/10	S社	ランサムウェア	台湾現地法人でランサムウェア攻撃、パソコン使用不能、情報窃取の被害。機密情報や社員の個人情報がインターネット上に公開され、金銭支払いを要求された。

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56カ国、約19万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

- グローバル拠点におけるガバナンス不足
- セキュリティ対応要員のリソース不足
- ワークスタイルの変化によるリスクの増大

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56ケ国、208都市、約19万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

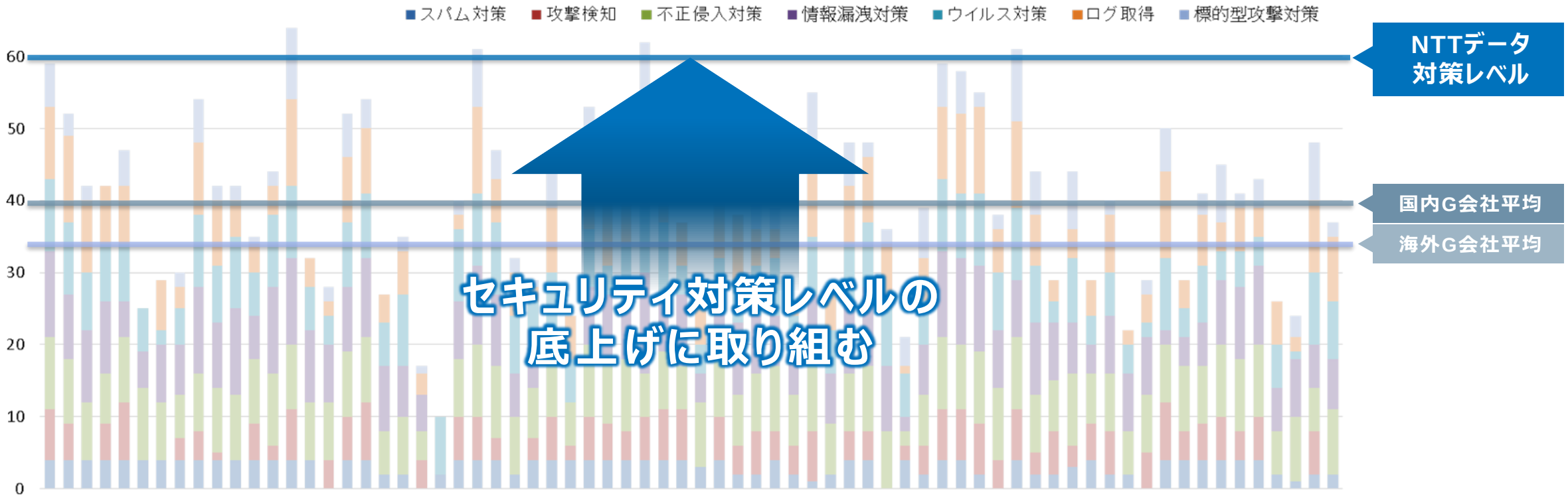
Rule

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

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

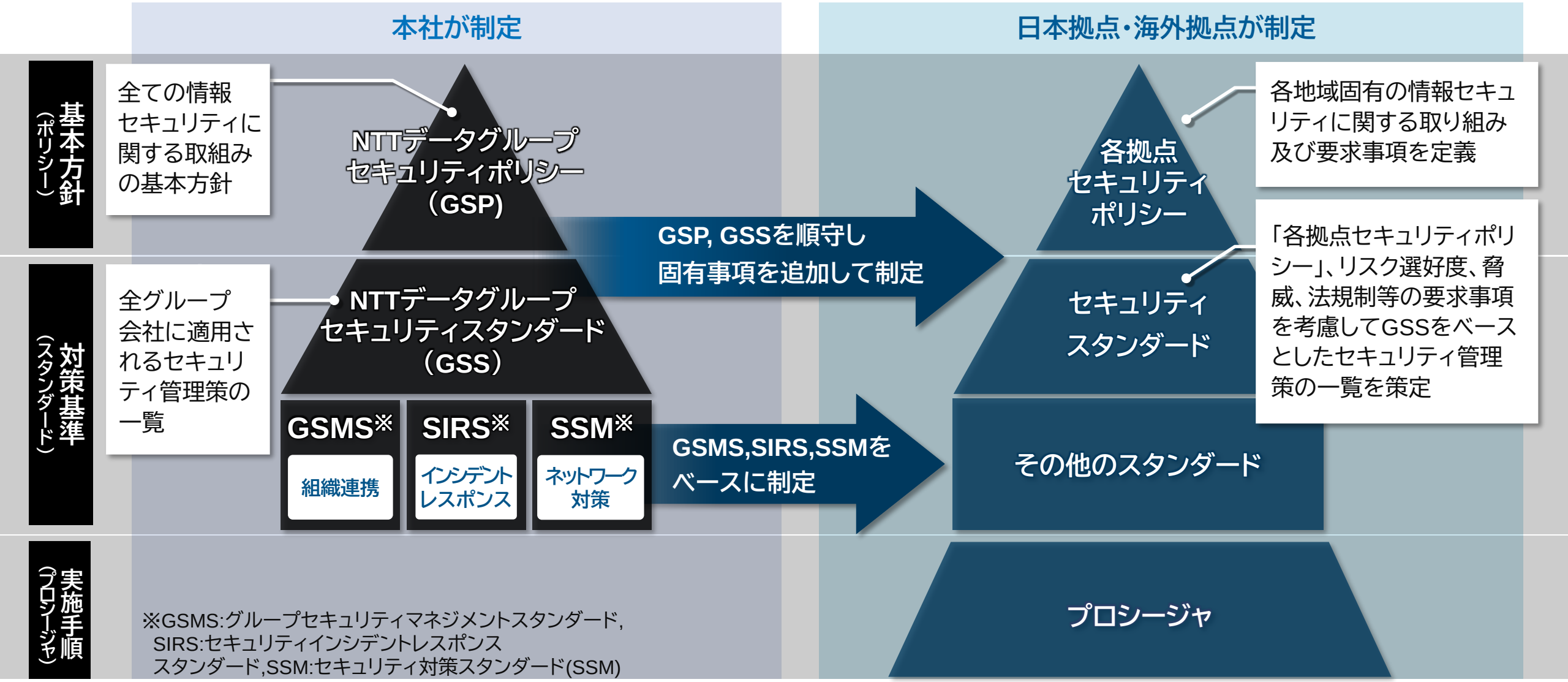


Rule

グローバルセキュリティポリシー・スタンダードの統一

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。



※GSMS:グループセキュリティマネジメントスタンダード,
SIRS:セキュリティインシデントレスポンス
スタンダード,SSM:セキュリティ対策スタンダード(SSM)

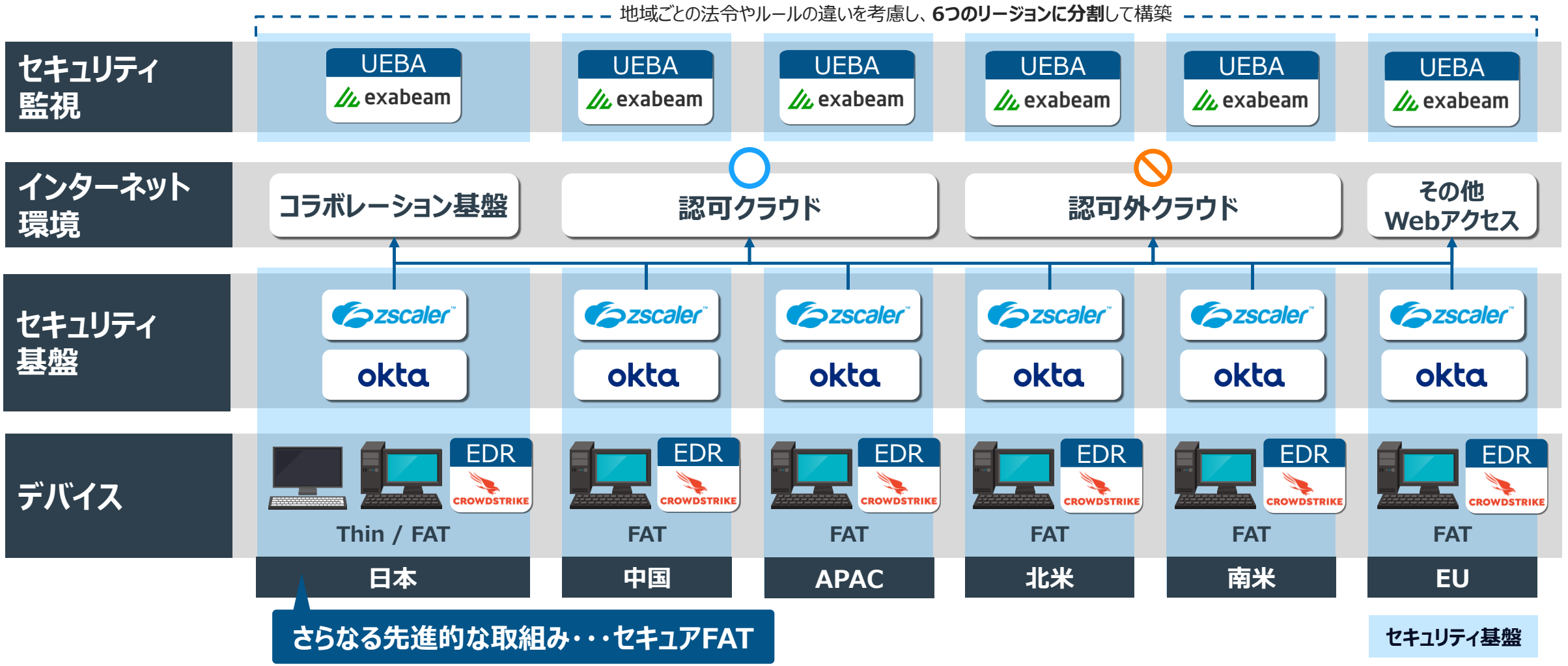
NTT DATA

Technology

横断的セキュリティ監視・対応基盤の構築

Stage 3

社員約19万人が活用可能な**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。



NTT DATA

Technology

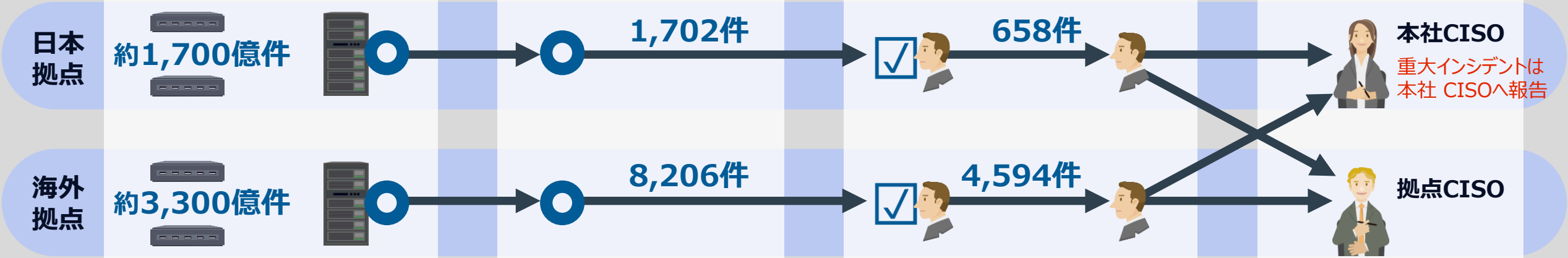
インシデント対応 ～迅速なエスカレーションプロセス

Stage 3

全拠点から集約される**約5,000億件/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。

2022年10月-12月の運用状況

セキュリティ基盤で集約したログ総件数	ログ分析の結果、Tier1(Exabeam)が発したアラート	Tier2(分析チーム)で判定 Tier3(IRチーム)が対応 エスカレ件数	CISO報告
約5,000億件	**9,908件**	**5,252件**	・各拠点内 **0件** ・本社向け **0件**



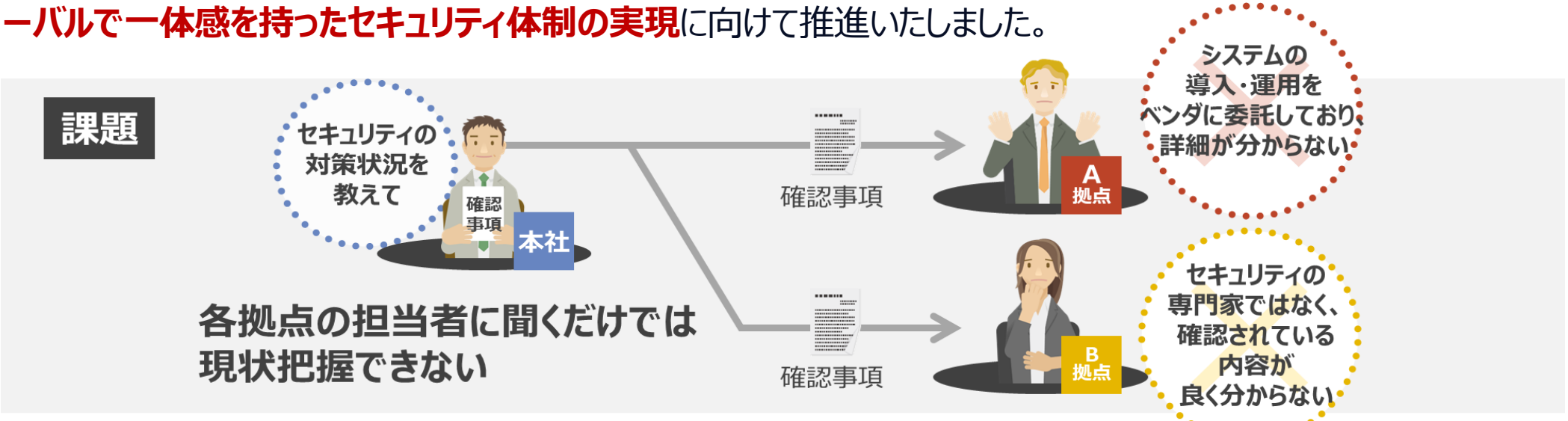
NTT DATA

People

One NTT DATA：人・一体感・信頼

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。

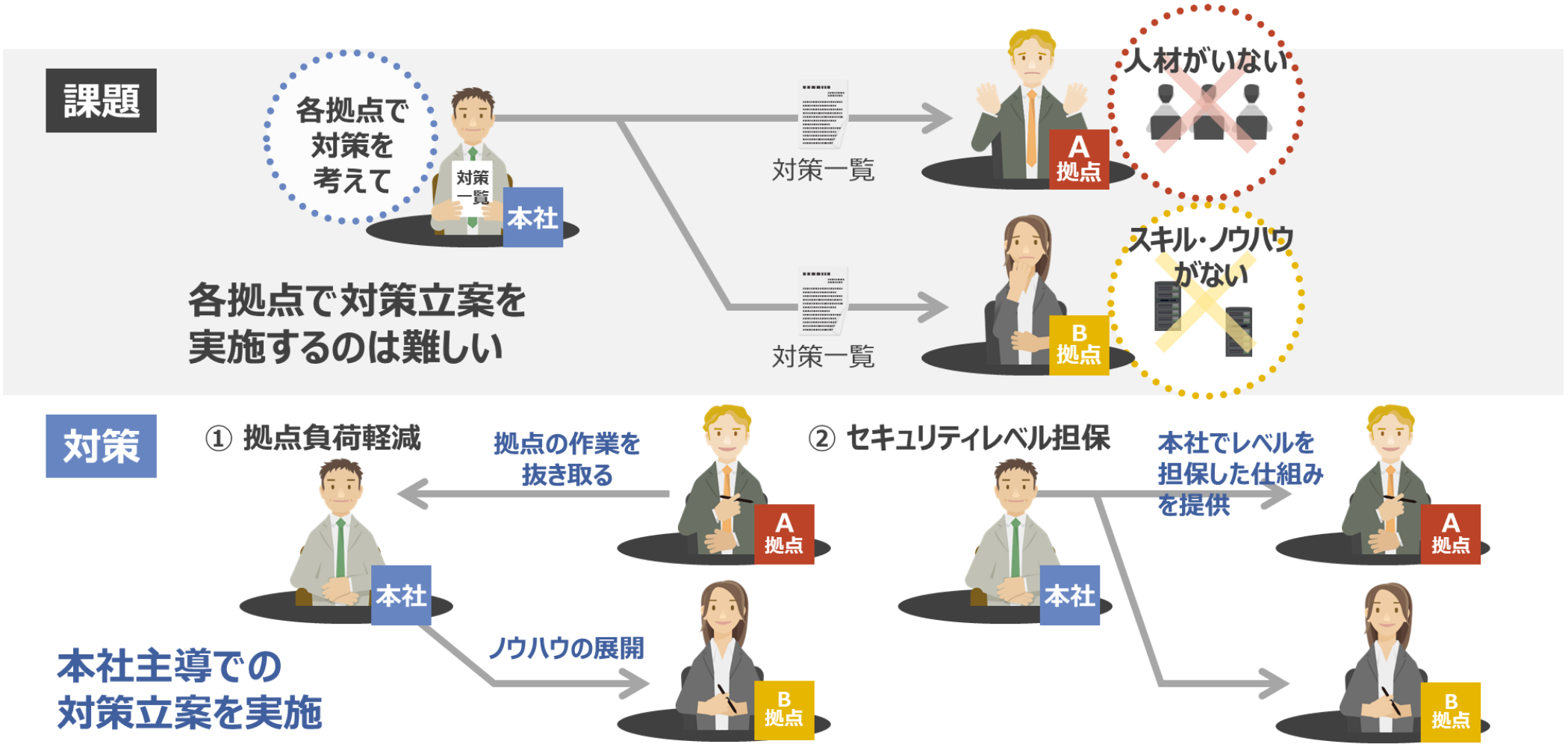


People

One NTT DATA：人・一体感・信頼

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。

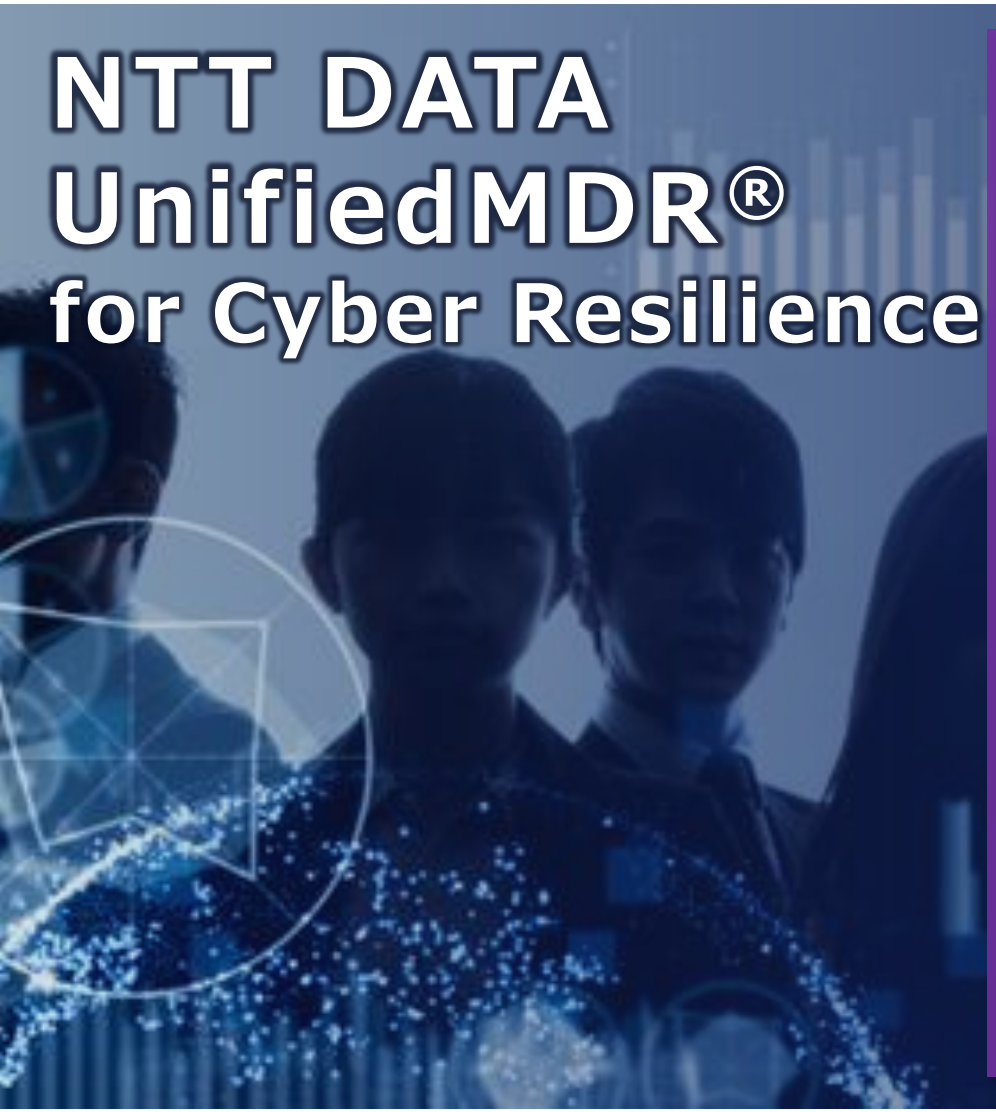


NTT DATA

目次

NTT DATA UnifiedMDR® for Cyber Resilience（UMDR）サービスのご紹介

最新のセキュリティ情勢に対応したグローバル規模のセキュリティをサポートする、弊社のセキュリティサービスUMDRをご紹介いたします。

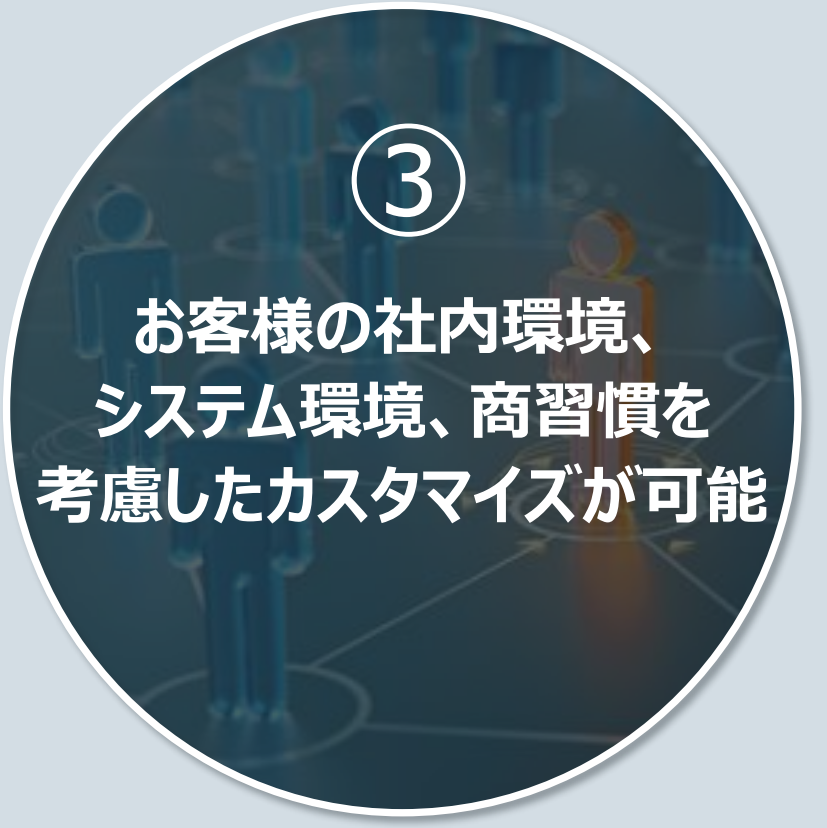


お客様のセキュリティ課題	NTT DATAが提供する価値
グローバル拠点における ガバナンス不足	グローバルガバナンス体制の 構築・運用実績
ワークスタイルの変化による リスクの増大	グローバルでの サービス提供体制
セキュリティ対応要員の リソース不足	大規模な プロジェクト実行力
サイバー攻撃の 高度化	NTTDATA-CERTの高度な インシデント対応力

本サービスの特徴

UMDR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。

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.外部からのサイバー攻撃」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

⑥インシデント対応

インシデント発生

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

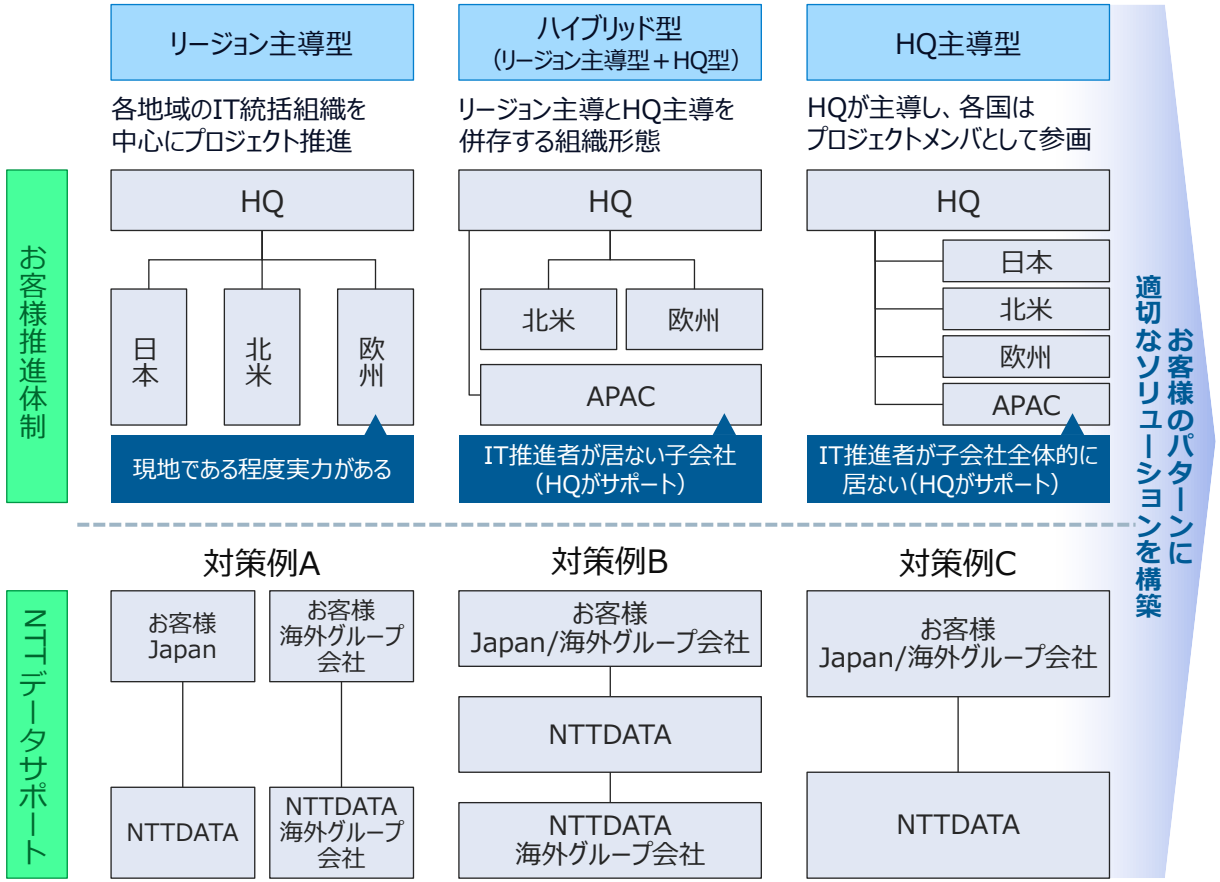
Ⅲ. 復旧
- ✓ 設定変更や機器最新化
- ✓ 流出データの削除
- ✓ 紛失データの検索、など

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/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	✓	✓				Azure Active Directory 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

本サービス　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を実現

▶ セキュリティログ監視

▶ 脆弱性情報収集/発信　Planning

▶ 脅威情報収集/発信　Planning

■ 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）※1

- 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※2

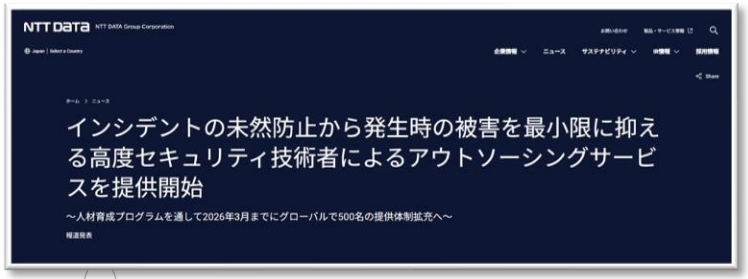
□ CSIRT運用サービス（有事）※1

- 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※2



2023年6月12日 ニュースリリースからの変更点
※1：「CSIRT運用サービス」を二つに分類
※2：サービスの性質よりCSIRT運用サービスへ集約

本サービス　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※3

- 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いて、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、目的に応じ、多種多様な教育プログラムを計画/実施

□ 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

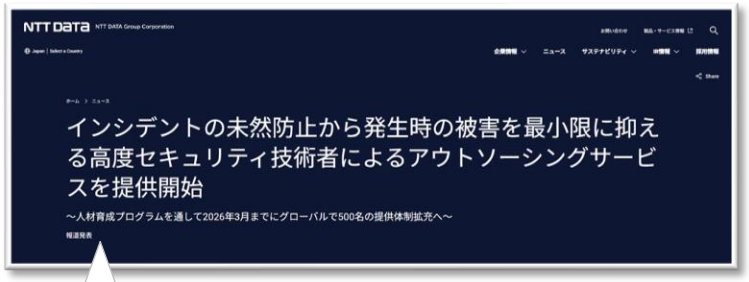
□ ゼロトラスト環境構築サービス※4

- 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..

▶ NTTDモデル提供

▶ MSモデル提供　Planning

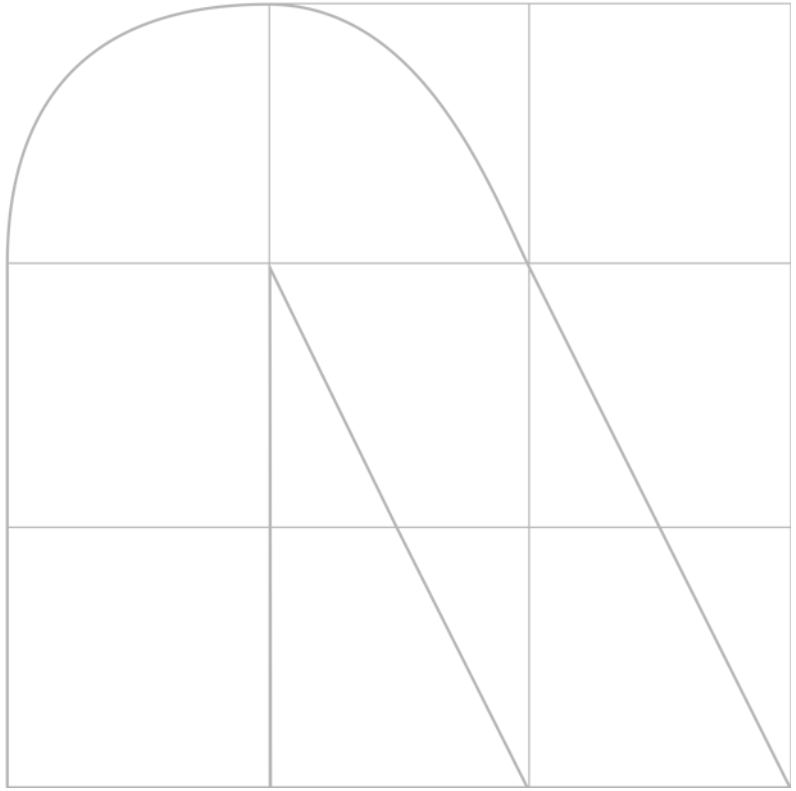


2023年6月12日 ニュースリリースからの変更点
※3：セキュリティポリシー策定サービスを追加
※4：「インプリメントサービス」を改名

目次

01

SOC



本サービス　全体像（サービスカット）　1/2

再掲

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を実現

▶ セキュリティログ監視

▶ 脆弱性情報収集/発信　Planning

▶ 脅威情報収集/発信　Planning

■ 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）※1

- 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※2

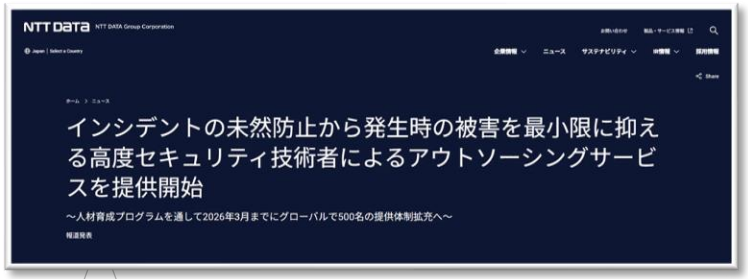
□ CSIRT運用サービス（有事）※1

- 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※2



2023年6月12日 ニュースリリースからの変更点
※1：「CSIRT運用サービス」を二つに分類
※2：サービスの性質よりCSIRT運用サービスへ集約

SOC構築/運用サービス 提供効果

■ SOC

本サービスについて

- 本サービスでは、SOCの要件定義、設計/構築、展開/運用と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
• SOC自体が存在しないため、構築したい	• 監視基盤構築	• お客様のニーズに応じて最適な設計を実施し、SOC運用に必要な監視基盤を構築。
• とりあえず監視基盤（SIEMなど）は構築したが、運用が整理できていない	• 運用体制構築	• 運用設計を実施し、手順策定やドキュメントを整備できる
• 自組織SOCの品質に懸念がある。品質を改善させたい	• セキュリティログ監視	• 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、自社SOC組織の品質を向上できる
• 日本国内におけるSOCは存在するが、グローバルSOCについては未検討	• 監視基盤構築 • 運用体制構築 • セキュリティログ監視	• お客様の戦略やビジネスモデル、商習慣に適応したグローバルSOCの要件定義/設計/構築/運用が可能となる

SOC構築サービス　監視基盤構築　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（56ヵ国、約19万人）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による、的確な監視基盤を構築します。

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

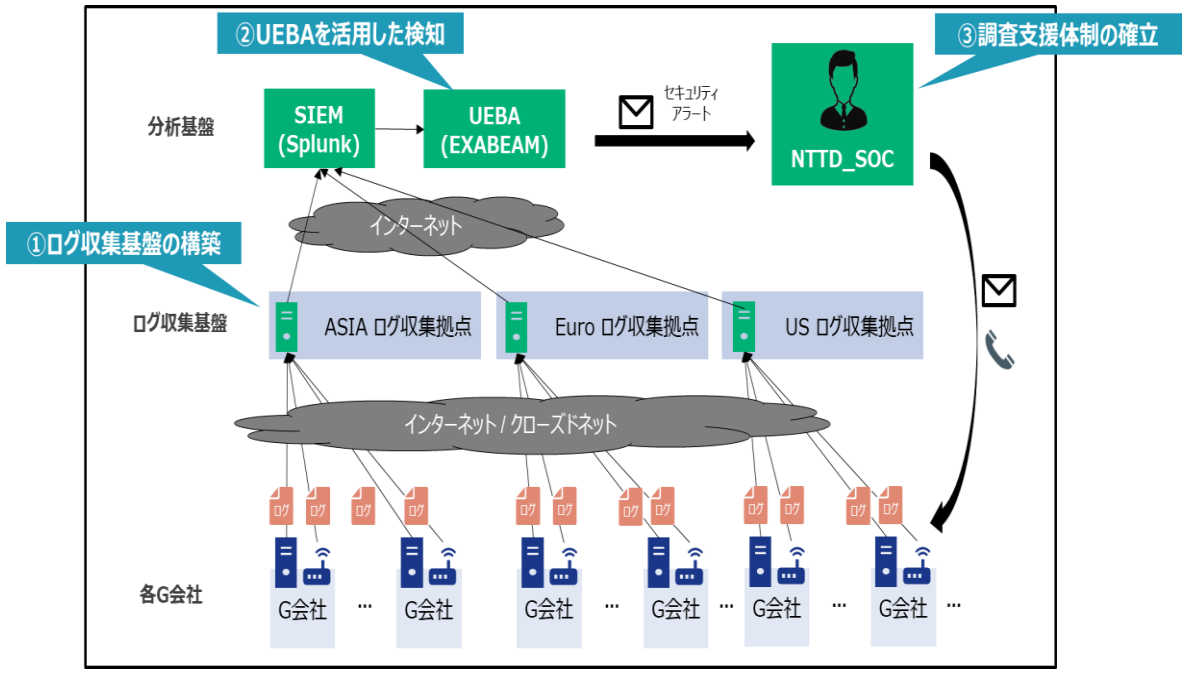
NTT DATA

SOC構築サービス　監視基盤構築　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)	ファイルの振る舞い検知 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	• Exabeam • Splunk • QRader
UEBA (User and Entity Behavior Analytics)	怪しい振る舞いの検知	• Exabeam Security Analytics • Microsoft Azure Sentinel
SOAR （Security Orchestration, Automation and Response）	セキュリティ運用の自動化及び効率化	• QRadar • ServiceNow

※上記製品以外は、別途ご相談

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。

SOC構築サービス　運用体制構築　1/2

■ SOC　■ SOC構築サービス

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（56ヵ国、約19万人）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による、的確なインシデントレスポンス体制整備を行います。

実施事項

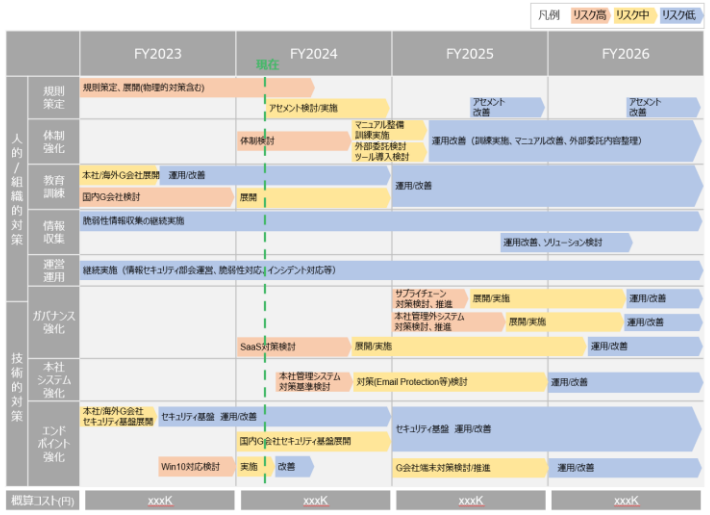
	1．要件定義	2．計画策定	3．設計/構築	4．展開/運用/改善
実施事項	• ヒアリング • ドキュメント調査 • Gap分析	• 構築タスクの洗い出し • 計画策定	• 運用ドキュメント作成 • SOC要員の調整	• 試運転支援
実施概要	➢ お客様へのヒアリングや既存文書の確認等を通じて、お客様のセキュリティ監視運用に関わる既存の体制、ルール/プロセス、技術的環境の状況を把握 ➢ お客様のビジネス/ミッションに沿ったTo-Be像を具体化することで、As-IsとTo-BeのGapを可視化	➢ Gap分析結果を元に、Gapを埋める構築タスクの洗い出し ➢ お客様のビジネス/ミッションに沿って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、人数を決定。お客様にて要員確保が困難な場合、弊社SOC運用サービスにて、運用まで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構築サービス　運用体制構築　2/2

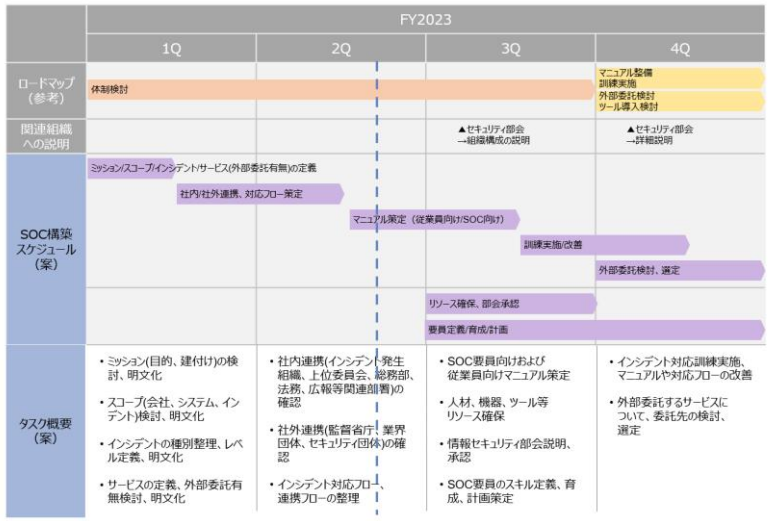
現状の体制、ルール、プロセス等を把握し、お客様にとって最適なSOC運用体制構築を支援

サービスイメージ

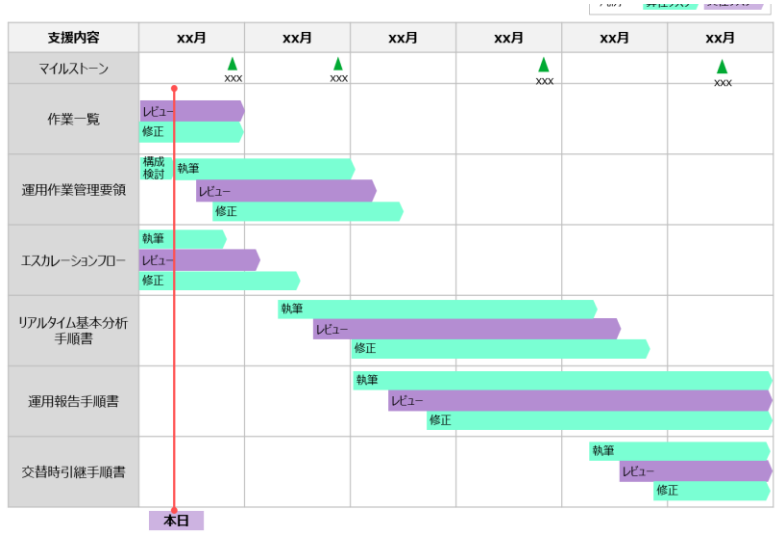
SOC構築ロードマップ



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。

SOC運用サービス　セキュリティログ監視　1/2

■ SOC　■ 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を実現

提供価値

■効率的なアラート対応および正誤判定含むログ調査が可能
- SIEM/UEBA含め、セキュリティ機器の検知ルールを適切にチューニングし、真に危険なアラートのみ調査可能となります。
- また、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がお客様環境に存在する場合のSOC運用サービスにおける作業スケジュール例は以下の通りです。

（**既存SOCが存在しない場合は、SOC構築サービスをご検討下さい**）

お客様が希望する作業内容に応じ、作業スケジュールは変更となるため、具体的な作業スケジュールの策定にあたり、事前に実施内容を確認させていただきます。

また、運用設計および運用実施にあたり必要となるドキュメントの整備には2か月必要となります。

	N月	N+1月	N+2月	N+3月	N+4月	N+5月
工程	事前準備			仮運用		本番運用
作業項目	運用要件確認	運用設計/ドキュメント整備 お客様監視基盤への接続環境準備		アラートチューニング ルール再設定		本番運用

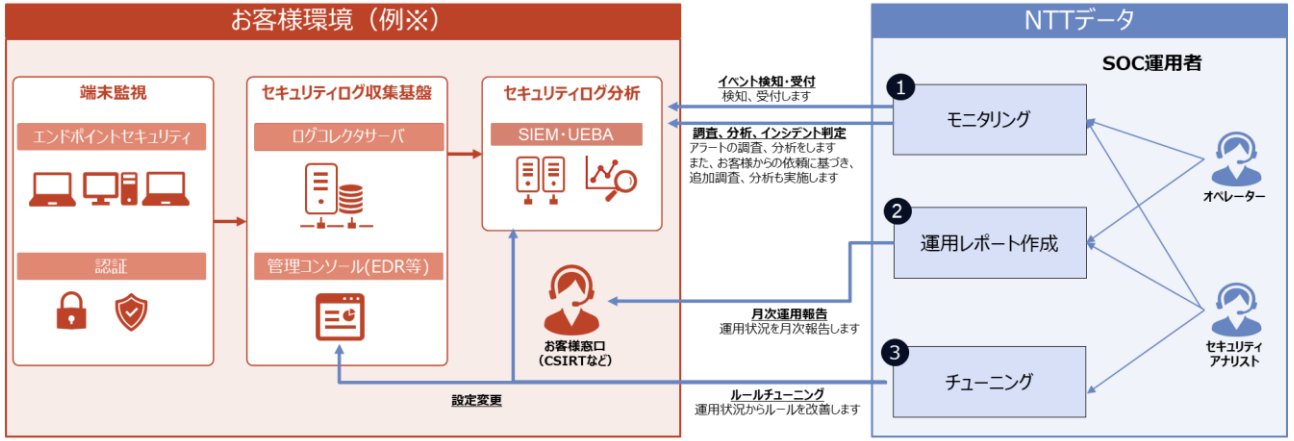
SOC運用サービス　セキュリティログ監視　2/2

■ SOC　■ 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を実現

サービスイメージ

お客様のセキュリティ監視基盤等を利用し、正誤判定含むモニタリングからチューニングまで、
お客様を支援します。



※セキュリティログ監視可能となるお客様環境例です。その他環境構成は別途調整させていただきます。

SOC運用サービスにおける監視対象は、以下の通りです（2023年7月1日時点）。
今後対応製品は拡充予定です。

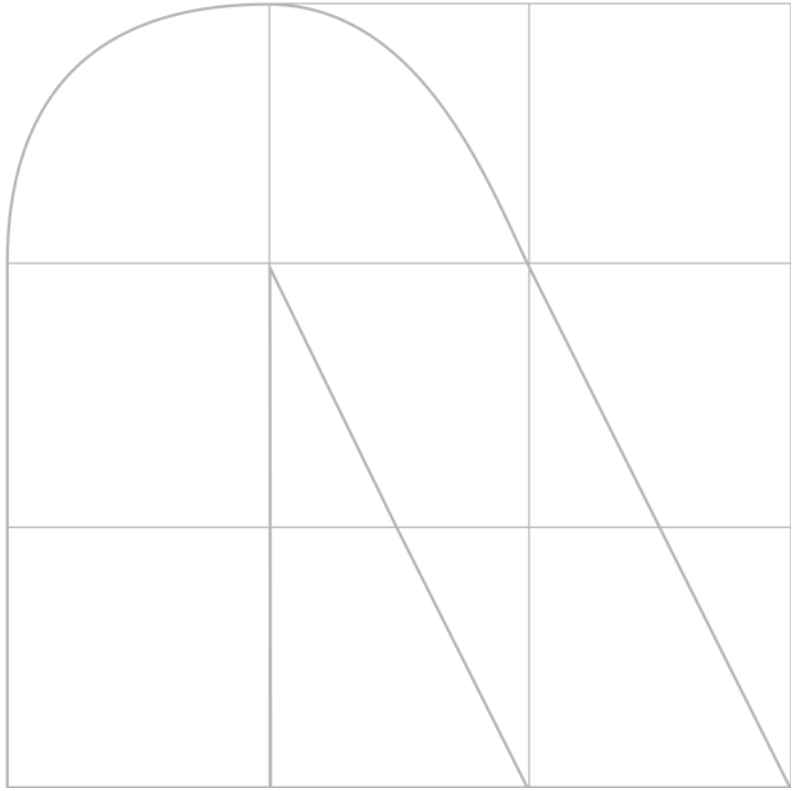
分類	処理概要	製品名
Identity	ID管理 2要素認証	• Okta • Azure Active Directory
Hygiene	未管理端末の把握 パッチ適用/状況把握	• TANIUM • Microsoft Intune
SWG	暗号化通信の監視 クラウドの利用制御	• Zscaler • Microsoft Defender for Cloud Apps
EDR (Endpoint Detection and Response)	ファイルの振る舞い検知 端末管理の自動化	• CROWDSTRIKE • Microsoft Defender for Endpoint • VMware Carbon Black EDR
UEBA (User and Entity Behavior Analytics)	怪しい振る舞いの検知	• Exabeam Security Analytics • Microsoft Azure 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。

02

CSIRT



本サービス　全体像（サービスカット）　1/2

再掲

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を実現

▶ セキュリティログ監視

▶ 脆弱性情報収集/発信　Planning

▶ 脅威情報収集/発信　Planning

■ 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）※1

- 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※2

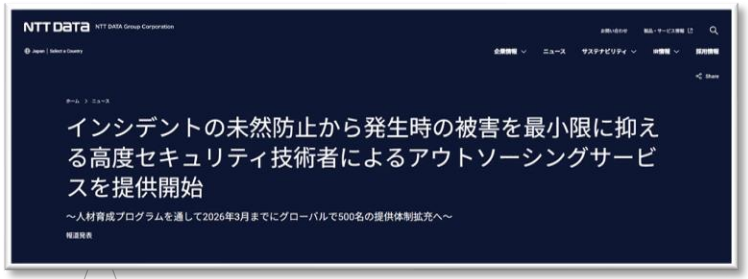
□ CSIRT運用サービス（有事）※1

- 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※2



2023年6月12日 ニュースリリースからの変更点
※1：「CSIRT運用サービス」を二つに分類
※2：サービスの性質よりCSIRT運用サービスへ集約

NTT DATA

CSIRT構築/運用サービス 提供価値

■ CSIRT

本サービスについて

- 本サービスでは、CSIRT構想立案から要件定義、設計/構築、展開/運用、セキュリティインシデントレスポンスと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
• CSIRT自体が存在しないため、構築したい。	• CSIRT体制構築サービス	• お客様に最適なCSIRTの構築、運用が可能となる
• CSIRT自体は存在するが、運営まで手が回っておらず、品質に懸念が残る	• IRディレクター	• 経験豊富なセキュリティ専門家がお客様CSIRT運用の改善を支援し、品質向上が可能となる
• CSIRTの運営自体は問題ないが、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/代行することで、迅速なインシデント終息が可能となる
• インシデント終息後の本格対処について、支援を受けたい	• IR対策フォロー	• インシデントレスポンス後の類似事象発生箇所の点検、再発防止策を含む対策およびロードマップを提案できる

CSIRT構築サービス　1/2

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

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CSIRTを一気通貫に構築

- 弊社グループの世界規模（56ヵ国、約19万人）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CSIRT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CSIRT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サポートします。

実施事項

	1．要件定義	2．計画策定	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て、お客様のCSIRTやインシデントレスポンス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、運用まで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。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	✓ 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

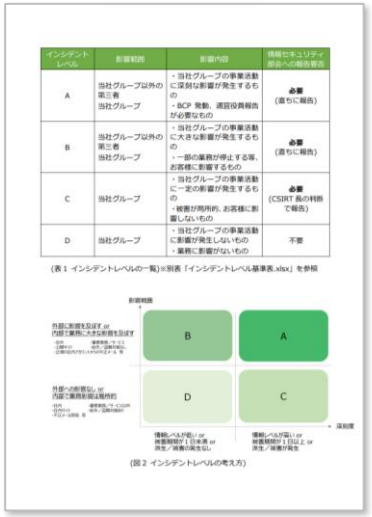
世界各地でのインシデントレスポンスを行うNTTデータの経験と実績を活かし、お客さま企業に最適なCSIRTを構築

サービスイメージ

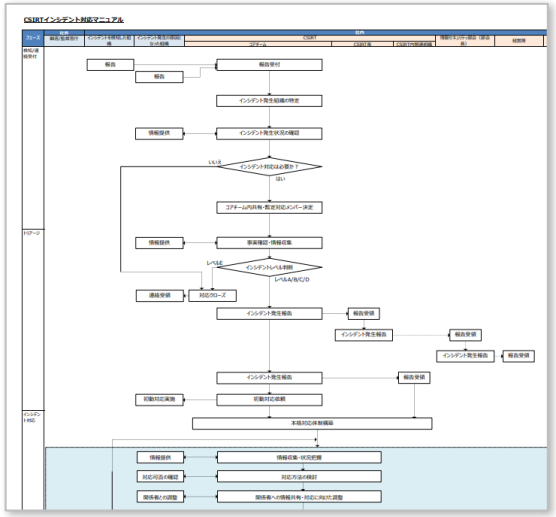
CSIRT構築のロードマップ策定例

	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） リソース確保、部会承認 要員定義/育成/計画	訓練実施/改善 外部委託検討、選定
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

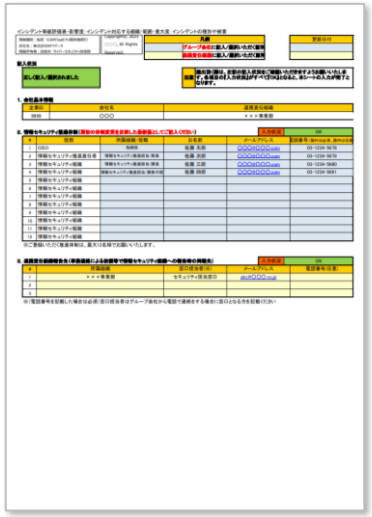
CSIRT構築の運用ドキュメント例



• 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

etc.

導入実績

• 通信、金融、製造、小売りなど、様々な業種/業態での導入実績があります。

CSIRT運用サービス　IRディレクター　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	• 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運用サービス　IRディレクター　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

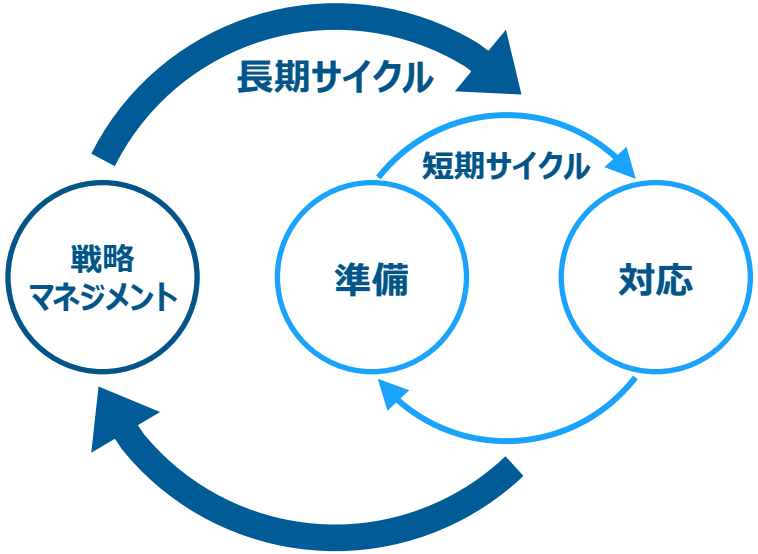
サービスイメージ

□ 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

□ 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運用をサポートします



□ 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資産管理簿などドキュメントの棚卸管理/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

- 大手銀行、大手保険会社、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運用サービス　インシデントハンドリング　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

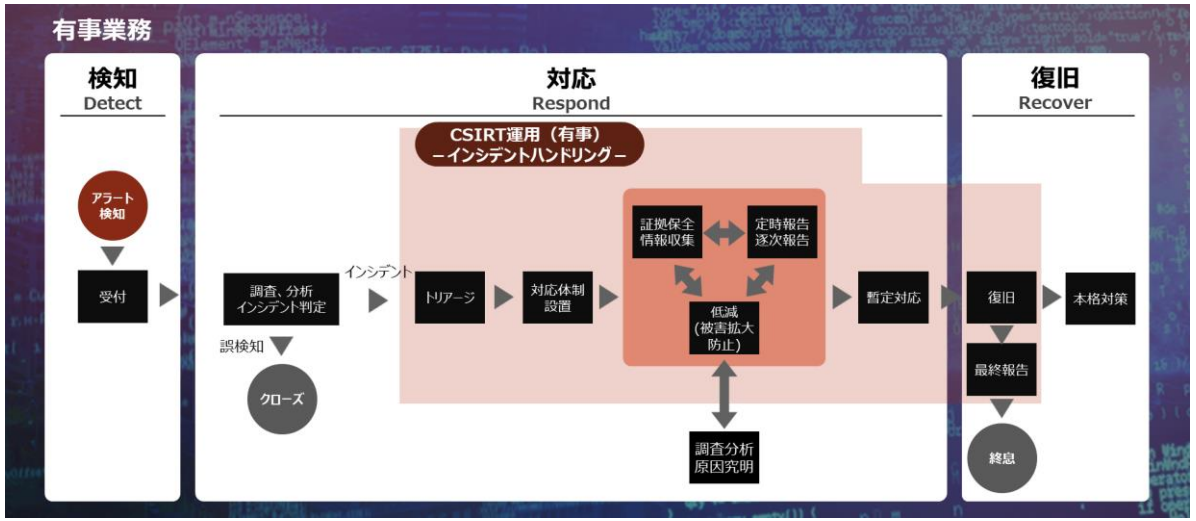
提供価値

■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

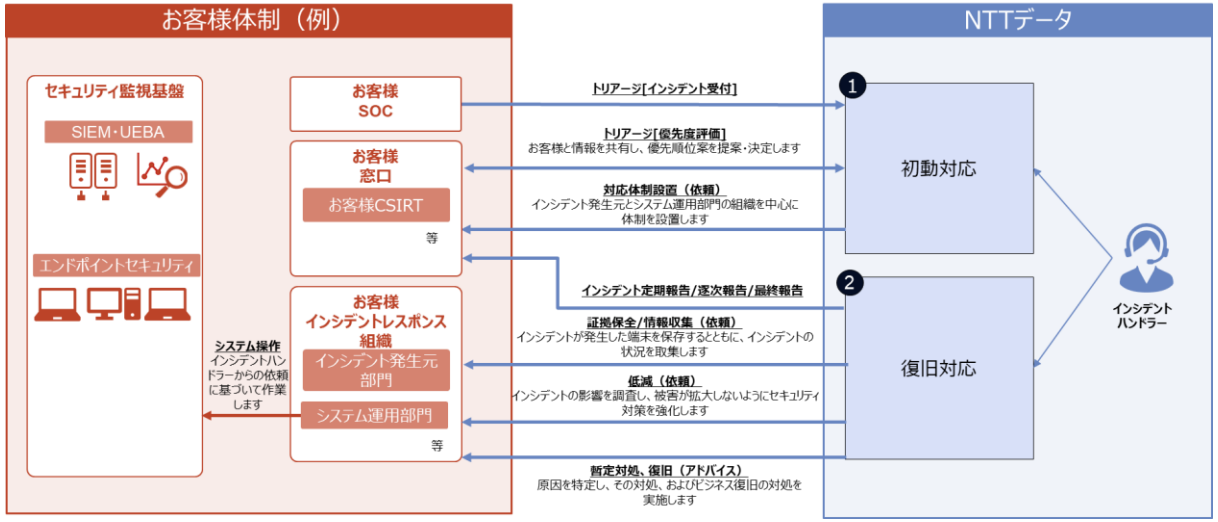
- 重大なサイバーインシデント発生時に、経験豊富なセキュリティ専門家を派遣し、クロージングまで責任もって対応いたします。
- 技術的対応はもちろんのこと、インシデントに関する最終報告までもご支援いたします。

サービスイメージ

インシデントハンドリングの業務スコープは以下となります。



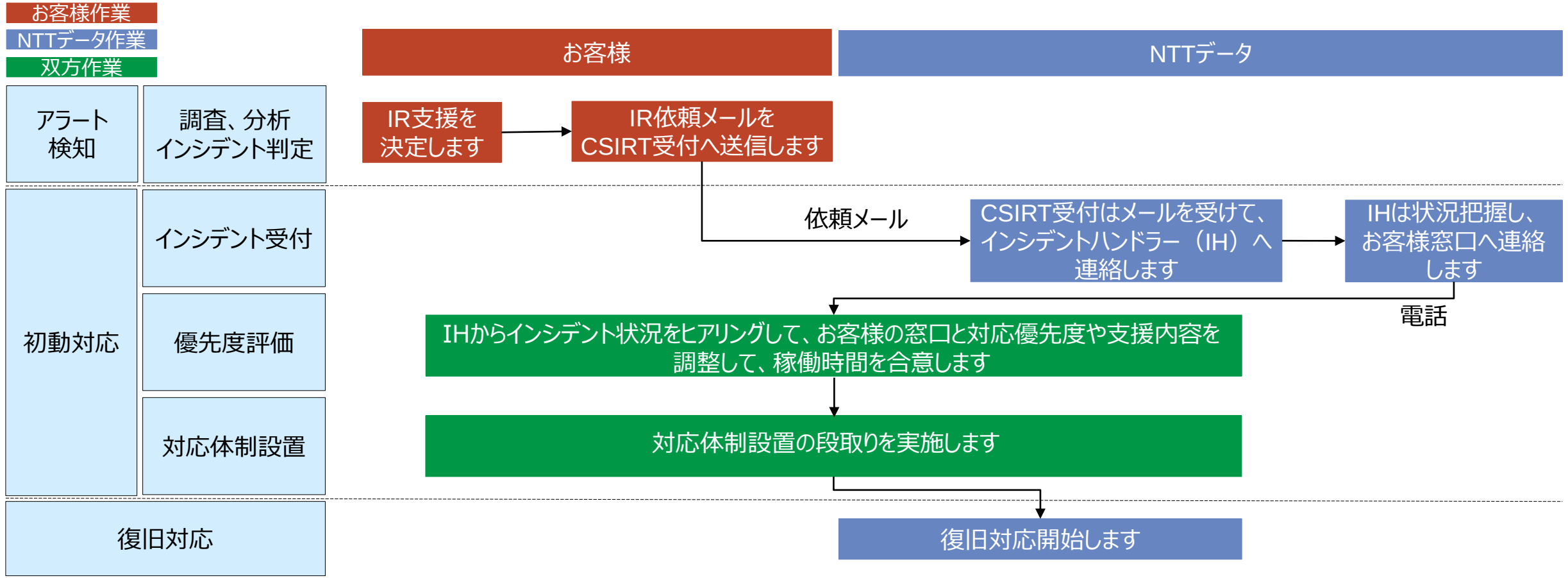
インシデントハンドラーは、インシデント発生から復旧まで支援/代行します



CSIRT運用サービス　インシデントハンドリング　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（インシデントレスポンス開始までの連絡フロー例）



導入実績

- 官公庁、海外自動車会社など、様々な業種/業態での導入実績があります。

CSIRT運用サービス　フォレンジック　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

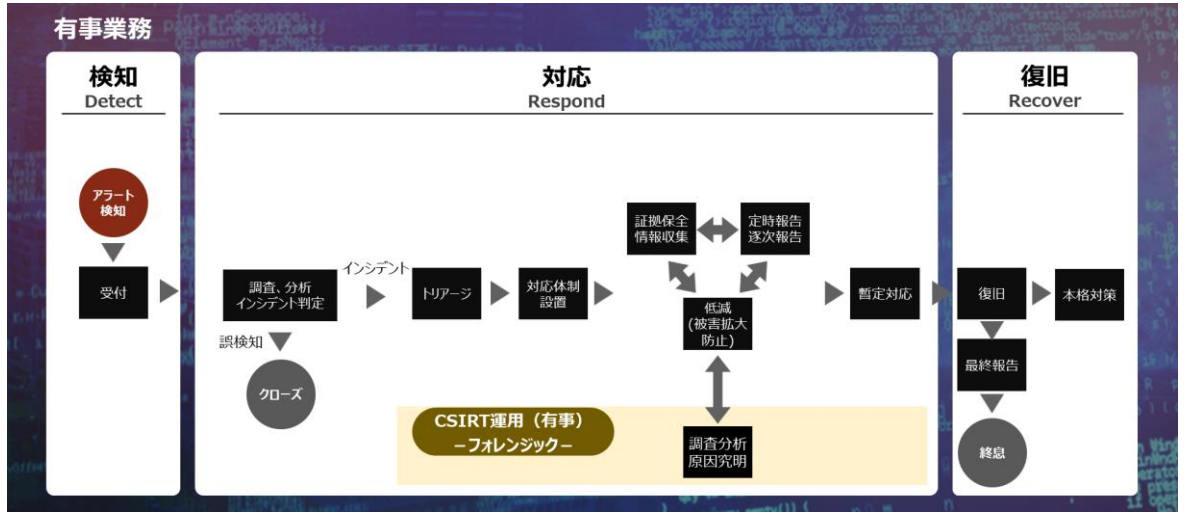
提供価値

■多様なインシデント事象の調査

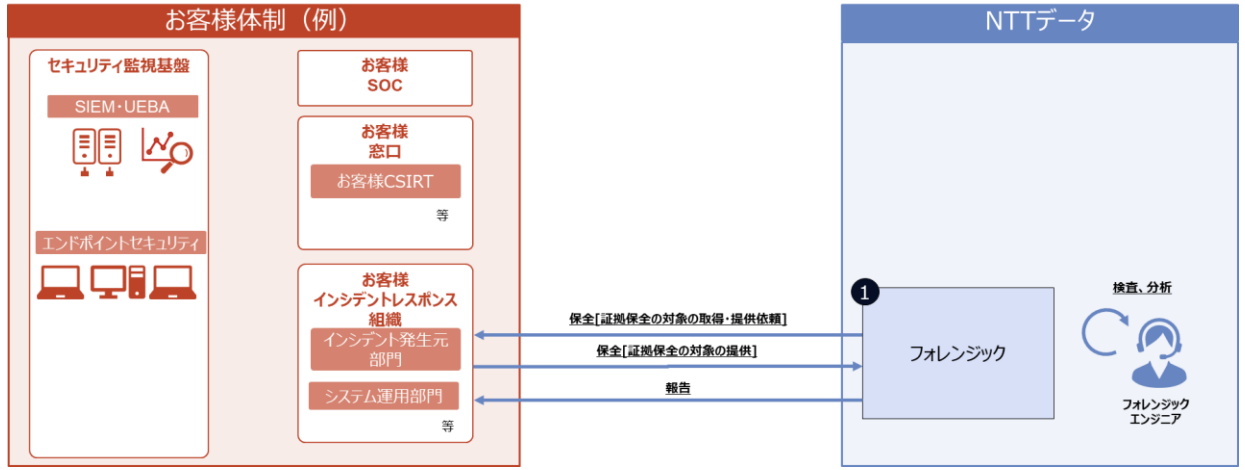
- 標的型攻撃、マルウェア感染、不正アクセス、情報漏洩等、多様なインシデント事象について調査します。
- またネットワークフォレンジック、ホストフォレンジック、マルウェア解析、ログ分析等、適切な調査手法/ツールを用いて効率的/効果的に調査します。

サービスイメージ

フォレンジックの業務スコープは以下となります。



フォレンジックエンジニアが、インシデントレスポンスの証拠保全からもらっ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。



CSIRT運用サービス　フォレンジック　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

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。 未導入である場合は、調査用の情報収集ツールを使用。被疑対象を特定するため、短期間に広範囲を調査。
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のログを基に、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)の調査などを実施。
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、HDDのデータ復元などを含む詳細な調査を実施。
マルウェア 解析	攻撃に利用されたマルウェアを解析することで、攻撃の種類、手口を特定。

導入実績

- 官公庁、海外自動車会社など、様々な業種/業態での導入実績があります。

NTT DATA

CSIRT運用サービス　IR対策フォロー　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

■お客様のあるべき姿を可視化

- インシデントレスポンスに長けたセキュリティ有識者が、お客様へのヒアリング、ドキュメント調査、Gap分析を通じ、現状を把握いたします。
- 現状分析を基に、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。

実施事項

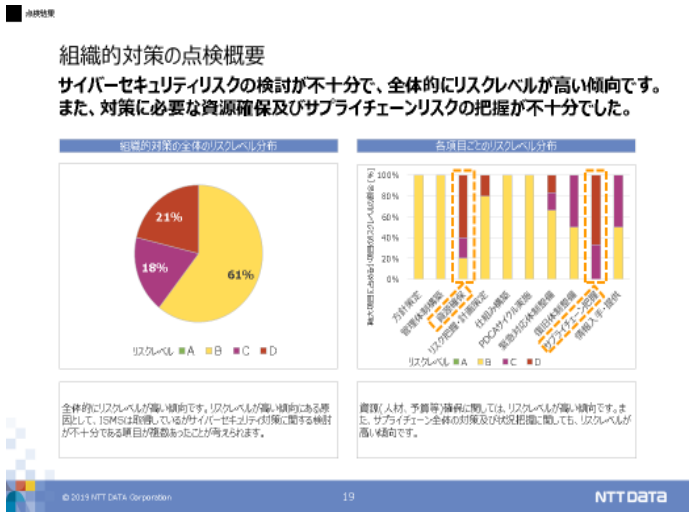
	1．現状把握	2．ロードマップ策定
実施事項	• ヒアリング • ドキュメント調査 • Gap分析	• 対策タスクの洗い出し • ロードマップ策定
実施概要	➢ お客様へのヒアリングやドキュメント(インシデント報告書等)の確認等を通じて、インシデントの(暫定)対応とお客様のセキュリティ監視運用に関わる既存の体制、ルール/プロセス、技術的環境の状況を把握 ➢ 類似を含めたインシデントを再発しないようにTo-Be像を具体化することで、As-IsとTo-BeのGapを可視化	➢ Gap分析結果を元に、Gapを埋める横展開を含めた対策タスクの洗い出し ➢ お客様のビジネス/ミッションに沿って対策タスク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

CSIRT運用サービス　IR対策フォロー　2/2

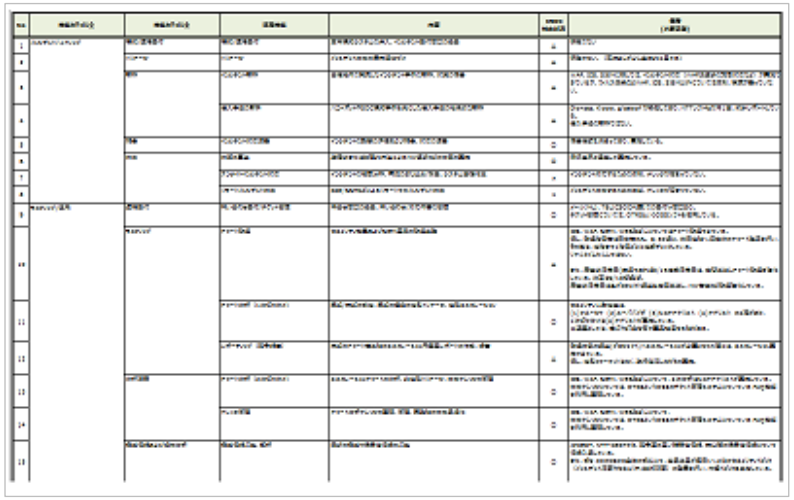
インシデントレスポンス後の類似事象発生個所の点検、再発防止策を含む対策を提案します。

成果物イメージ

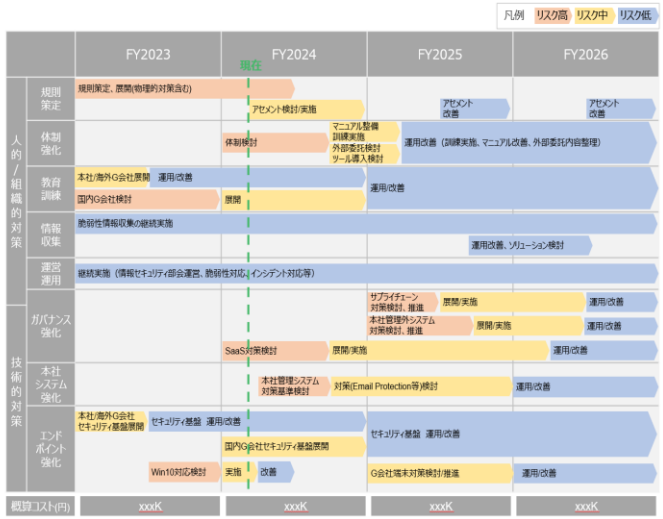
《Gap分析結果報告書》



《対策タスク一覧》



《ロードマップ》



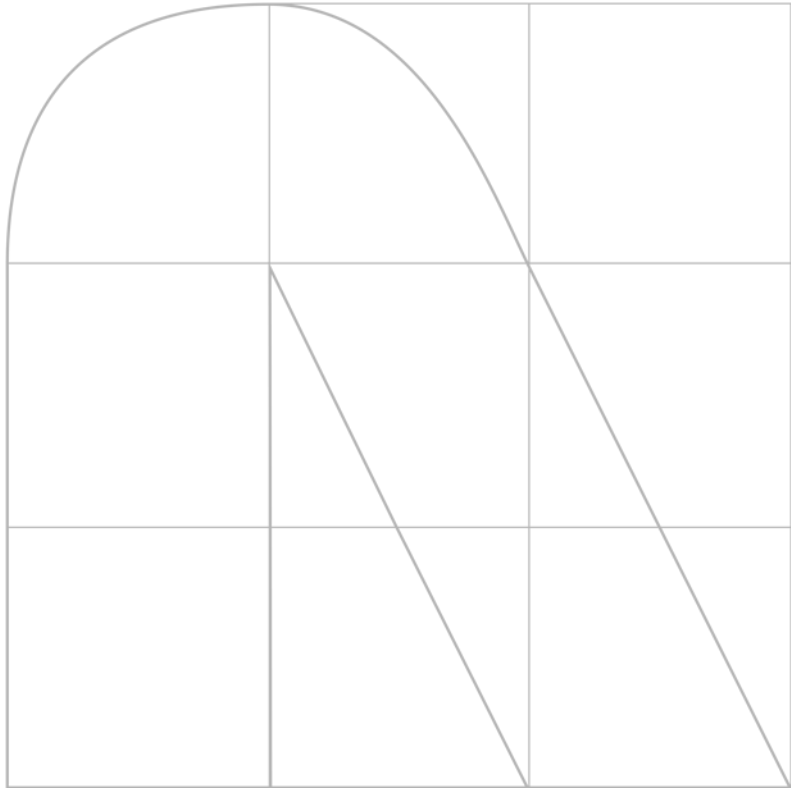
導入実績

- 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。

NTT DATA

03

コンサルティング



本サービス　全体像（サービスカット）　2/2

再掲

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※3

- 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いて、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、目的に応じ、多種多様な教育プログラムを計画/実施

□ 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

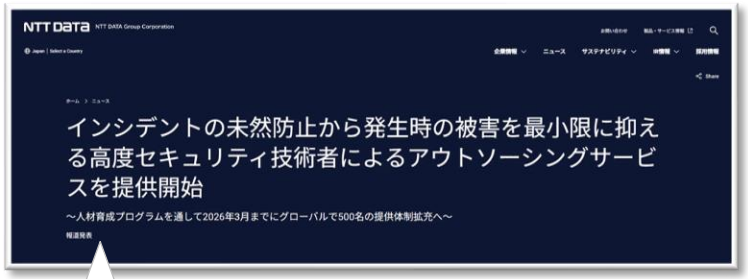
□ ゼロトラスト環境構築サービス※4

- 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..

▶ NTTDモデル提供

▶ MSモデル提供　Planning



2023年6月12日 ニュースリリースからの変更点
※3：セキュリティポリシー策定サービスを追加
※4：「インプリメントサービス」を改名

セキュリティポリシー策定サービス　1/2

■ コンサルティング

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
- グループ全体におけるポリシー/スタンダードを作成後、現地の商習慣や法規制を鑑み、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	➢ 日本および各国でのガバナンス推進体制の整備（CISO配置等） ➢ 既存のセキュリティポリシーおよびスタンダードが現状の業務に適しているかを確認し、改定の要否を判断 ➢ 作成、展開する基準のスコープを検討	➢ 方針検討で定めたスコープに基づき、お客様体制整備をご支援 ➢ スコープやお客様体制に基づいたポリシー展開ロードマップを作成	➢ 改訂すべきと判断したポリシーの改訂作業を支援 ➢ 追加作成する基準の選定支援	➢ ポリシー展開ロードマップに従い、改訂、作成したポリシーや基準の海外展開を支援
成果物	✓ 作業スコープ書	✓ ポリシー展開ロードマップ	✓ セキュリティポリシー ✓ 追加作成基準	✓ エグゼクティブサマリ

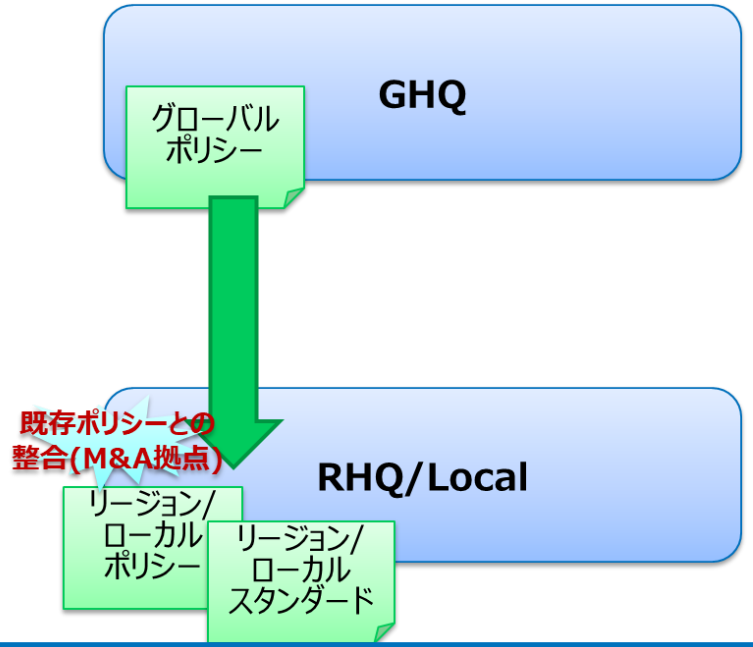
セキュリティポリシー策定サービス　2/2

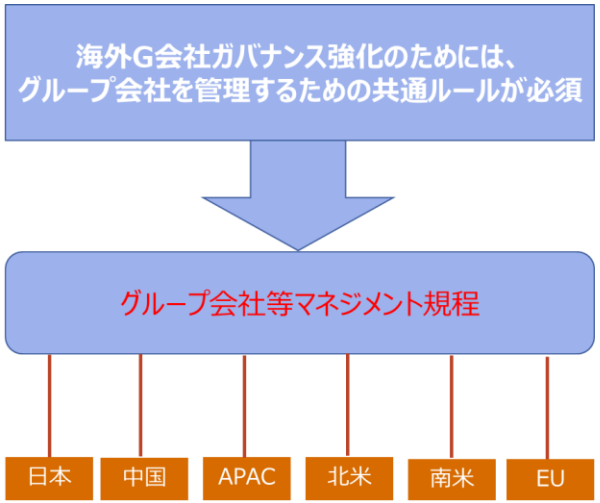
■ コンサルティング

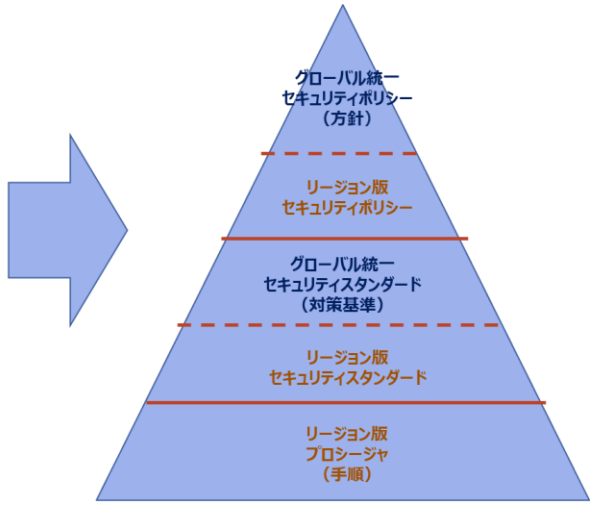
統一された共通グローバルポリシー/スタンダードの制定および、
各地域の商習慣/法律に応じた個別ポリシー/スタンダードの作成を支援

サービスイメージ

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。

リスクアセスメントサービス　1/2

■ コンサルティング

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。

■お客様のあるべき姿を可視化
- 本アセスメントを結果を基に、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。

実施事項

	1．事前準備	2．インタビュー	3．対策案検討	4．報告
実施事項	• セキュリティ観点でのチェックシートの準備 • 現状分析ヒアリングシートの準備	• インタビュー実施	• 対策案の検討 • 検討した対策案を優先度を重要度/緊急度等に応じて仕分け	• 報告 • ロードマップの策定
実施概要	➢ ITセキュリティチェックシート作成 ➢ 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）	• ITセキュリティチェックシートや現状分析ヒアリングシートを用いて、システム部門や経営層へのインタビュー実施	➢ インタビュー結果に基づき、問題点/改善点を整理 ➢ 問題点/改善点を解消するための対策案を優先度も加味し検討	➢ 最終報告資料を作成し、報告 ➢ お客様のあるべき姿実現に向けたロードマップを提示
成果物	✓ ITセキュリティチェックシート ✓ 現状分析ヒアリングシート	✓ インタビュー結果整理書	✓ 問題点/改善点整理書 ✓ 対策案検討一覧	✓ エグゼクティブサマリ、評価結果サマリ

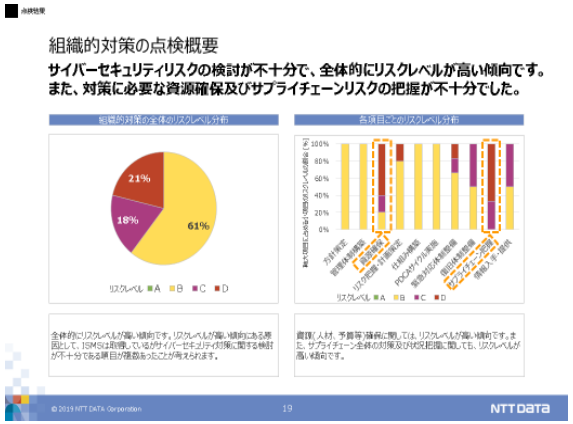
リスクアセスメントサービス　2/2

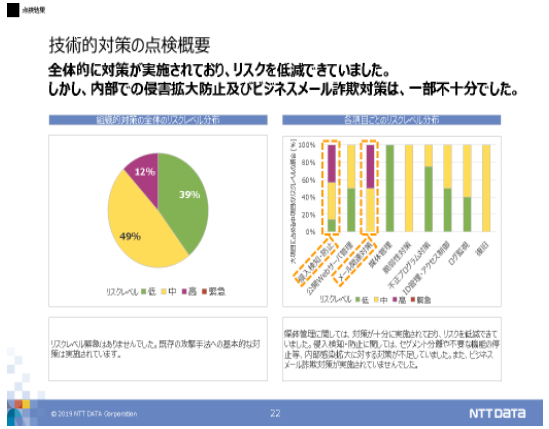
■ コンサルティング

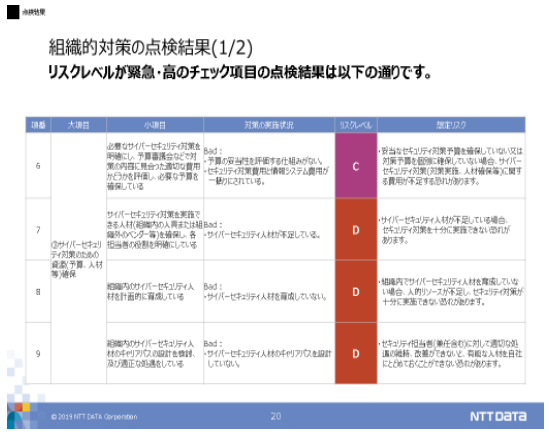
システムや組織におけるセキュリティ対策状況を網羅的に点検/確認し、問題点を洗い出した上で対策検討を支援

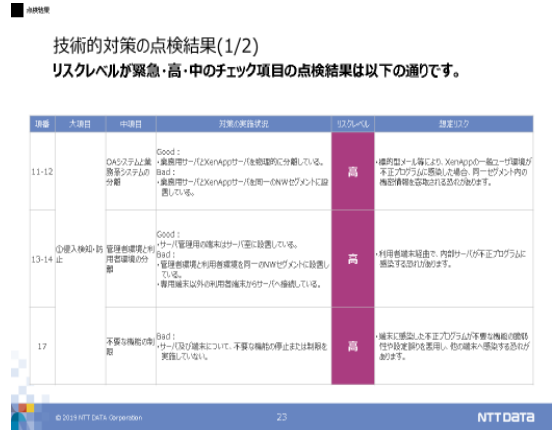
成果物イメージ

《調査結果サマリ》









※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。

（数十ページ程）

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。

NTT DATA

SOC/CSIRT成熟度評価サービス　1/2

■ コンサルティング

セキュリティ対応組織の業務について、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

提供価値

■SOC/CSIRT組織の現状を把握
- 成熟度を評価する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、セキュリティ上の課題や弱点を可視化します。

■機能強化項目の計画を支援
- お客様目指すべき像を設定するための課題解決の優先度を決定し、お客様状況を考慮した機能強化項目の計画を支援します。

実施事項

	1．既存SOC/CSIRTドキュメント評価	2．ヒアリング評価	3．結果整理/目標設定
実施事項	• ドキュメント評価	• ヒアリング調査	• 熟成度分析
実施概要	➢ SOC/CSIRTとしての機能/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	➢ ドキュメント評価では見えない範囲をお客様へヒアリングし実施状況を評価	➢「ドキュメント評価」、「ヒアリング評価」の評価結果に基づき、SOC/CSIRTの現状の「強み」、「弱み」を可視化 ➢ 評価結果に基づき、課題を整理 ➢ 優先順位を検討 ➢ 機能強化項目を設定
成果物	✓ ドキュメント評価結果	✓ ヒアリング調査結果	✓ 分析結果報告書

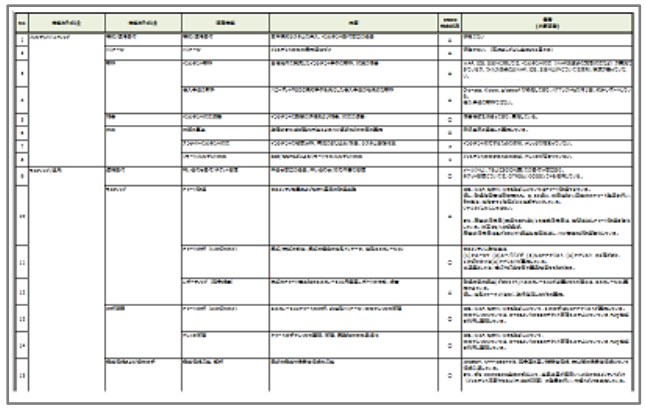
SOC/CSIRT成熟度評価サービス　2/2

■ コンサルティング

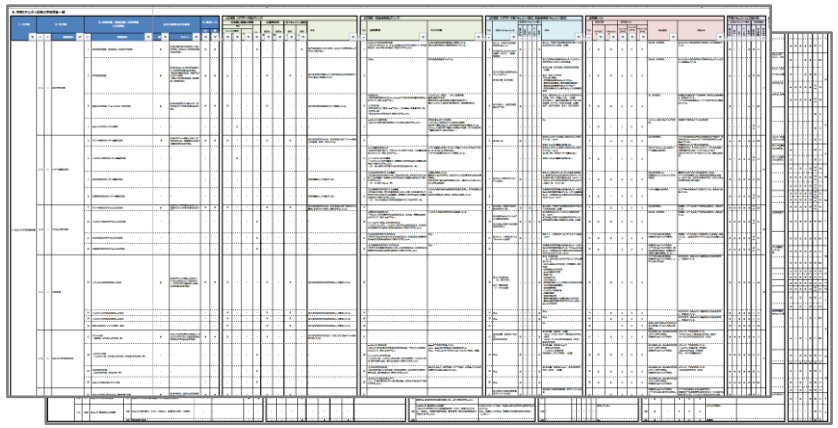
セキュリティ対応組織の業務について、業界団体ガイドライン、弊社知見をもとにした評価基準を用いて機能整備状況、運用状況を評価し成熟度を可視化

成果物イメージ

《評価項目一覧》



《ドキュメント評価/ヒアリング調査結果》



《分析結果報告書》

※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。

（数十ページ程）

導入実績

- 金融機関、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。

NTT DATA

IR教育/訓練サービス　1/2

■ コンサルティング

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き、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、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

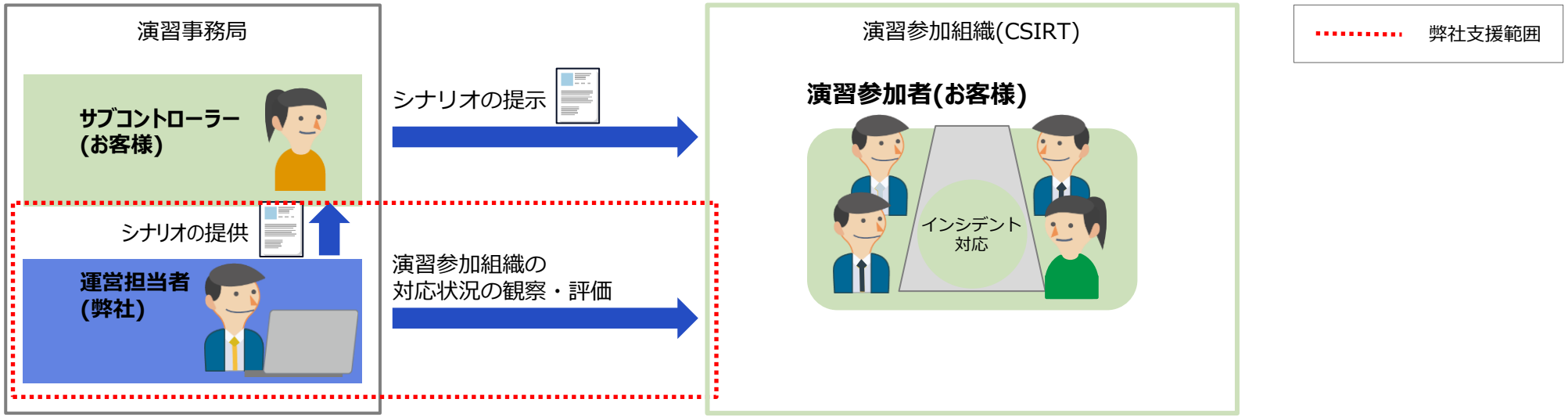
	1．演習準備	2．演習実施	3．演習結果分析
実施事項	• 体制構築 • 演習/運営準備	• IR演習の実施	• 評価内容分析 • 結果報告書の作成
実施概要	➢ IR演習を行う目的や評価テーマ、演習形式、演習対象組織をスコーピングし、IR演習シナリオを作成 ➢ 演習実施方法（オンライン/オフライン）や日程/環境を準備	➢ IR演習シナリオに基づきIR演習を実施し、評価する	➢ IR演習の評価結果から、IR演習の目的と演習参加者にの行動部分を分析する ➢ 分析結果を基に、結果報告資料を作成しお客様に報告を行う
成果物	-	-	✓結果報告書

IR教育/訓練サービス　2/2

■ コンサルティング

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



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

TLPTサービス　1/2

■ コンサルティング

脅威インテリジェンスを活用し、疑似攻撃を行ってセキュリティインシデントを発生させて、お客様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

- 現実世界で実際に起きている攻撃をもとにシナリオベースで疑似攻撃を実施することで、今現在の現実世界で行われている攻撃に対してどの程度対策が有効なのかを可視化します。

■インシデント発生時の被害や影響を明確化

- 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を「見える化」します。それをもとに、コンサルタントの知見を踏まえて、サイバーレジリエンス強化のための今後のアドバイスを提示します。

実施事項

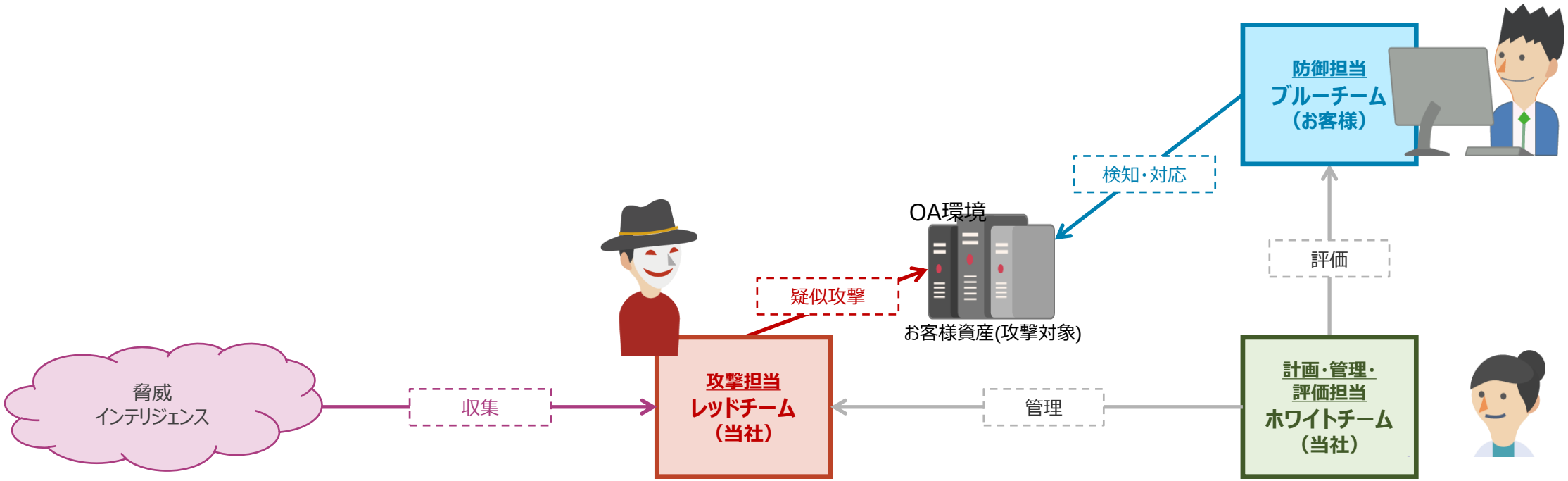
	1．実施体制構築	2．攻撃シナリオ作成	3．疑似攻撃実施	4．総合評価
実施事項	• 実施体制構築	• 脅威インテリジェンスによる分析 • 攻撃シナリオの作成	• 疑似攻撃詳細計画の作成 • 疑似攻撃実施	• 総合評価 • 対策方針アドバイス
実施概要	➢ お客様環境のヒアリングやお客様リスクアセスメント資料をインプットし、TLPTのゴールを定める ➢ TLPTのスコープやチームの体制、スケジュール等を定めたプロジェクト実施計画書作成	➢ 脅威インテリジェンスの調査・分析し、想定される脅威を特定する ➢ お客様環境に対して現実に発生する可能性があるサイバー攻撃のプロセスを攻撃シナリオとして作成	➢ 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	➢ ブルーチーム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）を行えるかをホワイトチームにて評価 ➢ コンサルタントの知見を踏まえて、今後の対策に向けたアドバイスを実施
成果物	ー	✓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

TLPTサービス　2/2

■ コンサルティング

脅威インテリジェンスを活用し、疑似攻撃を行ってセキュリティインシデントを発生させて、お客様のレジリエンス強度を評価

サービスイメージ

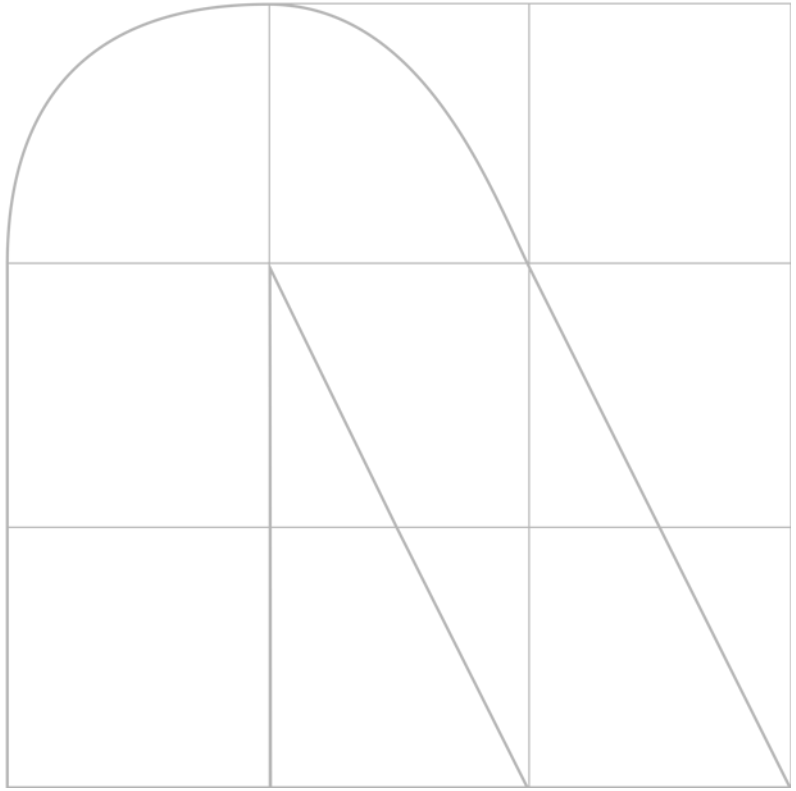


導入実績

- 金融機関を中心に主要インフラなど、様々な業種/業態での導入実績があります。

04

ゼロトラスト環境構築



本サービス　全体像（サービスカット）　2/2

再掲

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※3

- 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いて、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、目的に応じ、多種多様な教育プログラムを計画/実施

□ 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

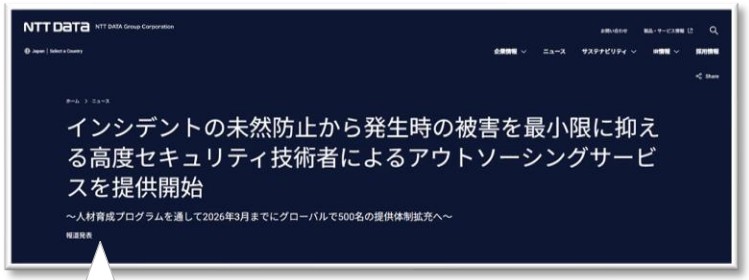
□ ゼロトラスト環境構築サービス※4

- 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..

▶ NTTDモデル提供

▶ MSモデル提供　Planning



2023年6月12日 ニュースリリースからの変更点
※3：セキュリティポリシー策定サービスを追加
※4：「インプリメントサービス」を改名

ゼロトラスト環境構築サービス　NTTDモデル提供　1/2

■ ソリューション構築

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に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て統一されたセキュリティポリシーを適用することにより、どの拠点で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

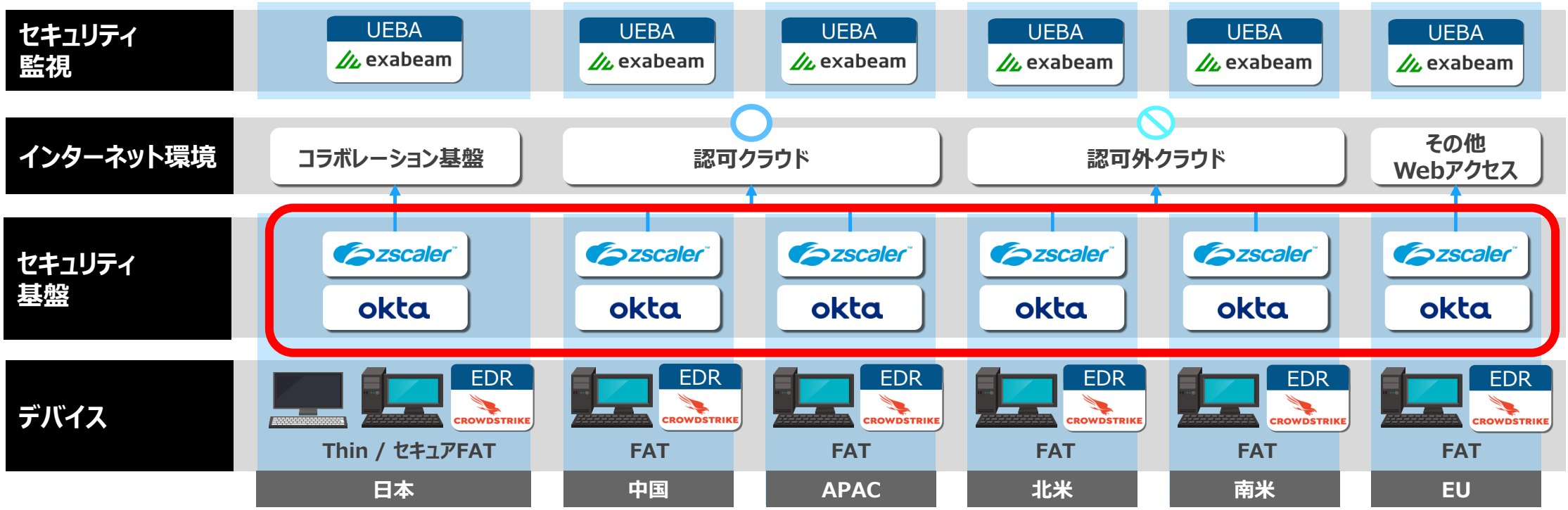
ゼロトラスト環境構築サービス　NTTDモデル提供　2/2

■ ソリューション構築

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　※赤枠はゼロトラスト構築対象（製品はNTTデータの事例）



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。


NTT DATA