金融機関向け
セキュリティサービスについて

2026年3月27日

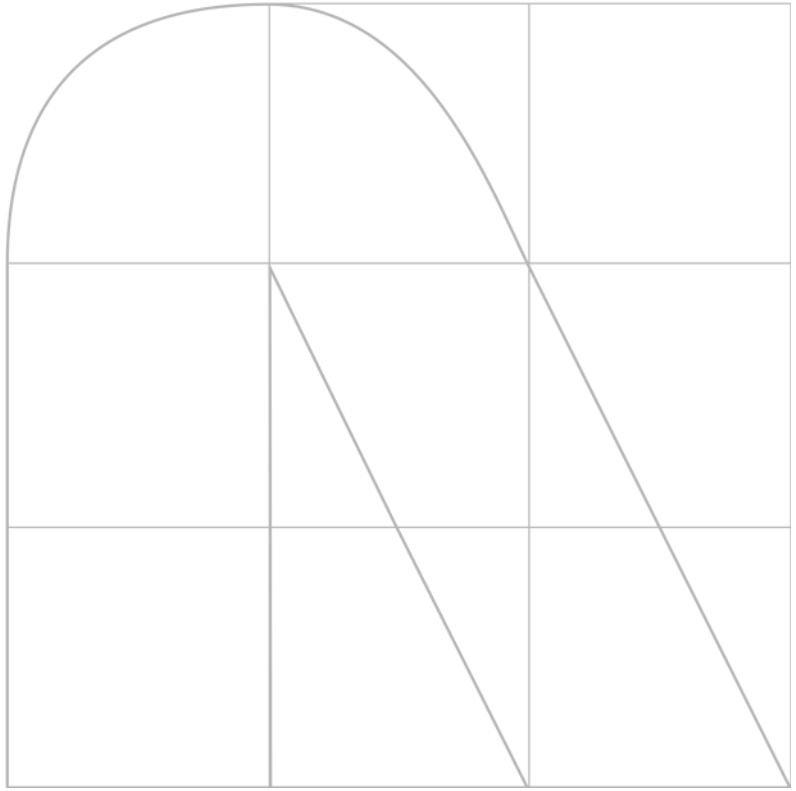
金融イノベーション本部 ビジネスデザイン室
第二金融事業本部 営業企画推進部

AGENDA
アジェンダ

- 金融機関を取り巻く状況
- NTTデータが提供する
  「金融総合セキュリティサービス™」
- 共同利用型SOCサービス「FinSOC® 」

01

金融機関を取り巻く状況



金融機関を取り巻く現状と課題

組織化・高度化するサイバー攻撃や、量子コンピューターによる暗号解読リスクの高まり等、セキュリティリスクは急速に増加しています。一方、金融機関ではセキュリティ人材の不足・継続的なコスト負担などにより、新たな脅威に対して継続的かつ高度な対策を講じることが大きな課題となっています。

激甚化するサイバー攻撃

社会的影響が大きいサイバー攻撃が相次いで発生。
サイバー攻撃は業種・規模を問わず拡大しており、経営リスクの一部として対策強化が求められています。

ランサムウェアによる業務停止

大手飲料会社や物流会社等がランサムウェア攻撃を受け、生産・物流システムが一時停止

- ✓ 約 9,000 件のデータ流出の可能性
- ✓ 出荷・受注業務の一部停止

証券口座のっとりによる金銭被害

大手証券会社等において口座の乗っ取りや不正売買による資金流出被害が急増

- ✓ 不正取引件数：約8,700件
- ✓ 累積売買額：約6,800億円

不正アクセスによる情報漏えい

法人向けメールセキュリティサービスへの不正アクセスにより、契約企業のメールアカウント情報や送受信データが漏えい

- ✓ 約580契約で情報流出
- ✓ 約30万件のメールアカウントに影響の可能性

DDoS攻撃によるサービス停止

金融機関・航空会社などを標的にDDoS攻撃が相次ぎ、オンラインサービスの一時停止・遅延が発生

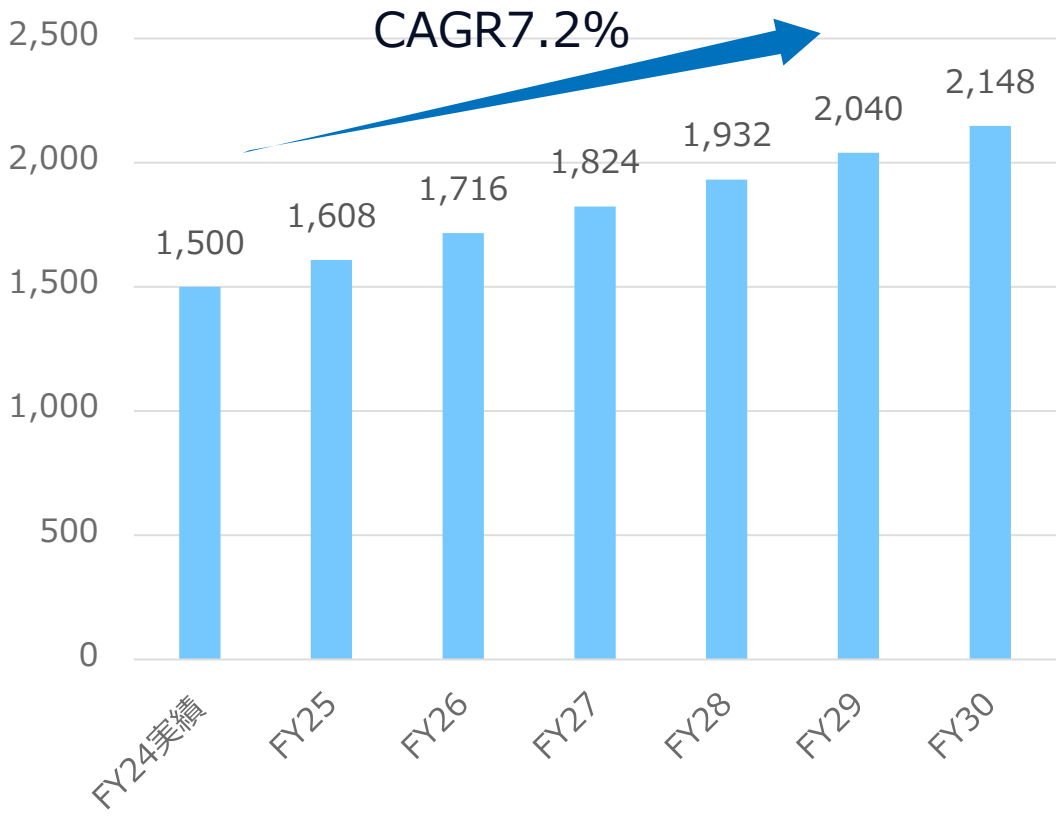
- ✓ 攻撃の標的となった国内企業：46社以上

※ 影響や件数等は、各種報道・公表資料の情報をNTTデータがとりまとめたもの

金融機関におけるセキュリティ市場規模

金融機関におけるセキュリティ市場規模は拡大傾向、
2024.10には金融庁がサイバーセキュリティガイドラインを公表（以降、当局ガイドライン）。

金融機関におけるセキュリティ市場規模（億円）



出典： IDC Japan(国内セキュリティ市場、ユーザ支出額予測)より引用

対話ベース

ルールベース

FY2022

- ■「サイバーセキュリティセルフアセスメント」実施（日本銀行・金融庁）
- ■「サイバーセキュリティ強化に向けた取組方針v3.0」の公表（金融庁）

FY2023

- ■合同演習やセルフアセスメント強化への推進策

FY2024

- **■「金融分野におけるサイバーセキュリティに関するガイドライン」を公表（金融庁）**
- ■FISCによる安全対策基準書第13版の改訂

FY2025

AIや耐量子暗号など先進技術が脆弱性としても注目される中、金融機関では戦略的な投資と態勢整備が求められる局面に

金融分野におけるサイバーセキュリティに関するガイドライン

実質的な規制として、各金融機関にてサイバーセキュリティガイドライン対応が必要です。

大項目	小項目
サイバーセキュリティ管理態勢の構築	経営陣の役割等
	規程等及び業務プロセスの整備
	経営資源の確保、人材の育成
	リスク管理部門による牽制
	内部監査
サイバーセキュリティリスクの特定	情報資産管理
	情報システム及び外部システムサービス
	ハードウェア・ソフトウェア等
	情報（データ）
	データフロー図・ネットワーク図
	脅威情報及び脆弱性情報の収集・分析
	リスクの特定・評価
	リスク対応
	継続的な改善活動
	ハードウェア・ソフトウェア等の脆弱性管理
	脆弱性診断及びペネトレーションテスト
	演習・訓練

大項目	小項目
サイバー攻撃の防御	認証・アクセス管理
	教育・研修
	データ保護
	ハードウェア・ソフトウェア管理
	ログ管理
	セキュリティ・バイ・デザイン
	インフラストラクチャ（ネットワーク等）の技術的対策
	クラウドサービス利用時の対策
サイバー攻撃の検知	監視
サイバーインシデント対応及び復旧	インシデント対応計画及びコンティンジェンシープランの策定
	初動対応（検知・受付、トリアージ）
	分析
	顧客対応、組織内外の連携、広報
	封じ込め
	根絶
	復旧
サードパーティリスク管理	―

当局ガイドライン対応における各金融機関の取り組み

当局ガイドライン公開以降、多くの金融機関では現状評価や対応計画策定を実施。
今後は当局ガイドラインで求められる基本的な対策(組織的および技術的)を実施し、対応が望ましい事項への対策が進むものと考えられます。

当局ガイドライン対応における各金融機関の取り組み

これまで

現状評価

- ✓ ガイドラインへの自社の対応状況をチェック

課題整理

- ✓ ガイドラインの要求充足に向けた課題の整理

対応計画策定

- ✓ 対応策の検討
- ✓ 対応計画策定
- ✓ 社内の承認

今後

対応策実施

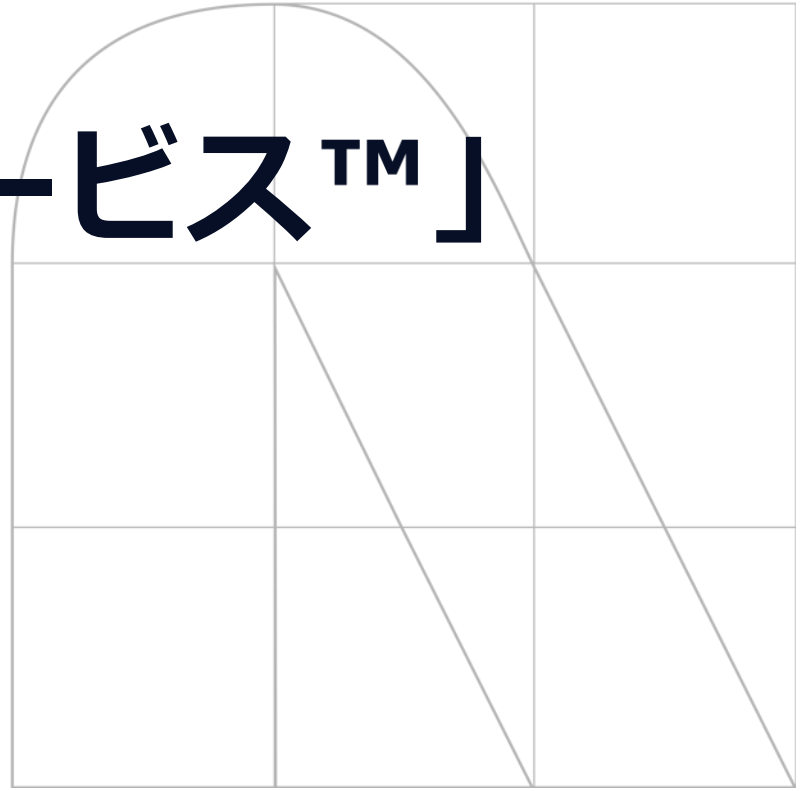
? → 

- **経営陣の関与**
- **規定類の整備**
- **技術的な対策**

- ✓ **基本的な組織的対策**
  例：基本方針・規程策定
- ✓ **基本的な技術的対策**
  例：IT資産管理・脆弱性管理
- ✓ **対応が望ましい事項への対策**
  例：TLPT実施、PQC対応

02

NTTデータが提供する「金融総合セキュリティサービス™」



「金融総合セキュリティサービス™」について

NTTデータのサイバーセキュリティのノウハウと金融ITベンダとして蓄積したノウハウを組み合わせ、金融庁ガイドラインに対応した「金融総合セキュリティサービス」を提供します。

サイバーセキュリティのノウハウ

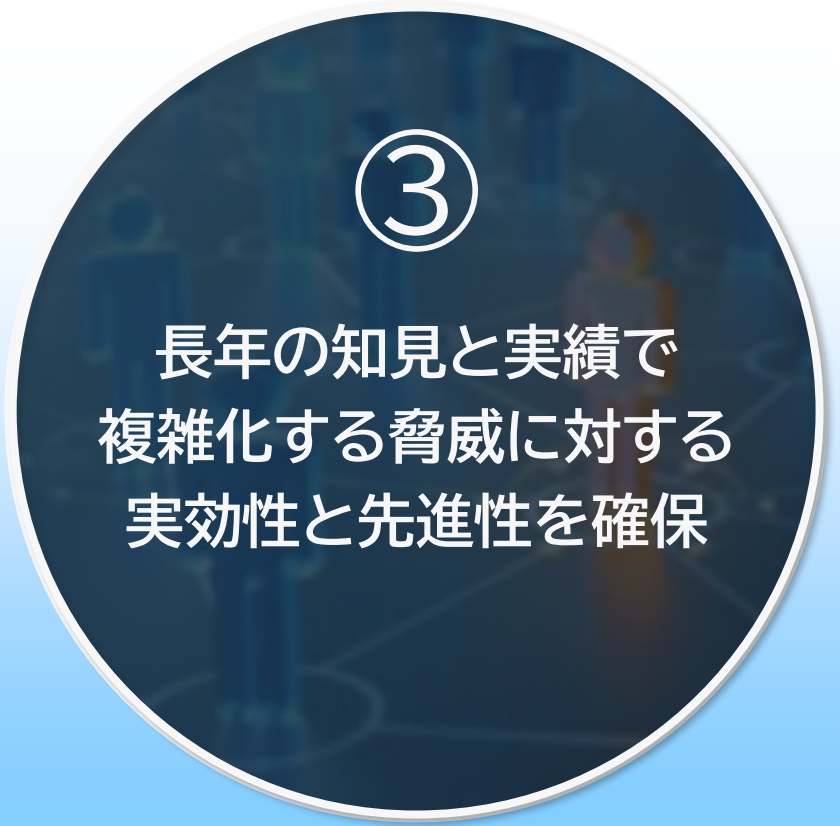
- ✓ CSIRT運用支援
- ✓ SOC運用支援
- ✓ インシデントハンドリング
- ✓ セキュリティ訓練・教育
- ✓ セキュリティポリシー策定

金融業界のノウハウ

- ✓ 金融機関向けシステム・業務運用の豊富な実績と専門知識
- ✓ 不正送金やフィッシング等、金融犯罪への対応
- ✓ 金融業界のガイドライン対応
- ✓ 金融業務特性への理解
- ✓ 外部機関との連携による金融セキュリティ動向の把握

「金融総合セキュリティサービス™」の特長

金融機関の勘定系システムを長年運用してきた実績とノウハウに加え、NTTデータが得意とする共同型サービスを強みに金融機関のセキュリティ対策をコンサルティングから実装・運用まで一気通貫で支援。



特長①：一気通貫で支援

金融庁ガイドラインに対応し、統制・コンサルティングから導入・運用・改善までを一気通貫で支援。

―統制― 管理態勢整備	―特定― リスク コンサルティング	―防御― ソリューション導入	―検知― 運用・監視	―対応・復旧― 継続的改善
				

サービス例

CISO支援	ロードマップ策定	ゼロトラスト環境構築	検知ルール高度化	インシデント対応計画
規定整備	ASM	IT資産管理・脆弱性管理	UEBA	インシデント レスポンスサービス
CSIRT整備	3rdパーティリスク管理	CSPM,SSPM	TLPT	ランサム対応バックアップ
FinSOC®				

凡例：　基本的な対策(組織的)　基本的な対策(技術)　対応が望ましい事項

現状分析・アセスメントによるリスク・強化ポイントの可視化と最適対策方針の策定
ソリューション選定・導入から、24時間365日の監視・運用までの包括的支援

製品導入にとどまらず、経営視点を踏まえた実効性のあるセキュリティ強化を実現し、継続的な高度化を支援

特長②：共助のセキュリティモデル

サービスとしてのナレッジやリソースの共助、セキュリティ対策としての脅威情報の共有から
非競争領域のサイバーセキュリティは“個の防御”から“共助の強化”へ。

よくある課題例

技術
- 限られたリソースでの運用態勢構築
- リスク報告整備の負荷増

ガバナンス
- 規程・マニュアルの形骸化
- 外部基準類の追い付き対応の劣後

訓練
- 社員教育や机上訓練はしているが、インシデント発生時の対応に不安

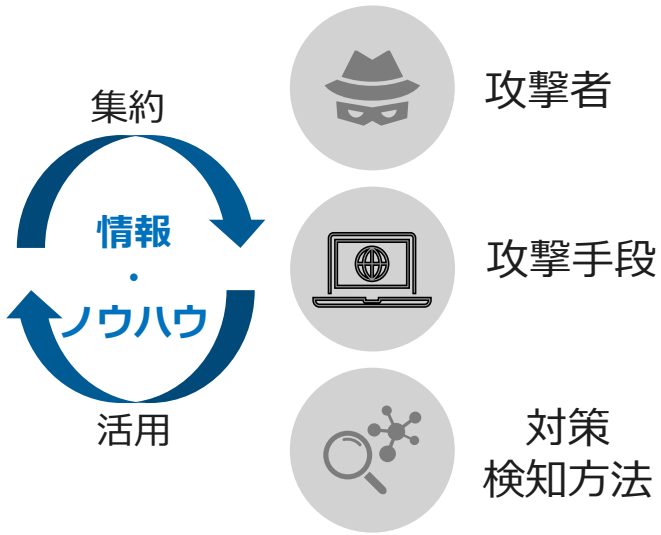
共助モデル

監視、IT資産管理、脆弱性管理の領域で**共同利用、横断展開の実施**

金融機関横断で活用可能な**「共通テンプレート／モデル」**を提供

インシデント演習・訓練、教育・研修等を**協同実施**

セキュリティ対策の共助



人財・予算の確保が困難なセキュリティ領域で、
当社のベストプラクティスとスケールメリットを活かし、コスト効率化と対応の高度化を両立

サイバーセキュリティの高度化を“コスト”ではなく、“信頼を生む経営資産”へ

特長③：長年の知見と実績

**金融分野・セキュリティ分野で培った知見に基づく、当局ガイドライン対応に対応した
実務・規制・他社動向や先進技術の潮流も見据えた、現実的で実効性のある態勢整備を支援。**

金融機関のシステム・業務運用に対する豊富な実装の実績・専門知識の保有

7,500+

Cybersecurity Professionals

NTT DATAには、世界中の様々な産業や技術に高度に精通した7,500人以上のセキュリティプロフェッショナルがいます。

No.2

In Gartner Market Share Analysis MSS 2022

NTT DATAは、これまでのインシデント対応の経験、および自社で構築した世界最大のゼロトラスト環境から得たノウハウを活用したサービスを提供しています。
これにより、グローバルでのMSS市場をリードしています。

外部機関との連携による金融セキュリティ動向の把握

80+

Cybersecurity Delivery Centers

NTT DATAには、世界中に80以上のサイバーセキュリティデリバリーセンターがあります。
これにより、コストと法規制を遵守するソリューションを提供できます。

30+years

Cybersecurity Experience

NTT DATAは、30年以上にわたり、サイバーセキュリティに関連するサービスを提供し続けており、蓄積されたノウハウを活用しています。

サイバーセキュリティ合同訓練、共助型ペネトレーションテスト・TLPT

共同化を通じ効率化とコスト最適化を図り、インシデント対応力を強化。

共助型ペネトレーションテスト・TLPT

- ✓ サイバーインシデント発生時に想定される初動・各部の連携・外部報告等を演習形式で実施し、一連の対応を評価するサービスをご提供
- ✓ **DeltaWall運営実績で培ったノウハウ**を活かしプログラム策定・当日事務局、演習後の各行様の評価を実施。年2回の開催を予定

金融庁等の評価観点踏まえた本番対応に向けた準備を支援

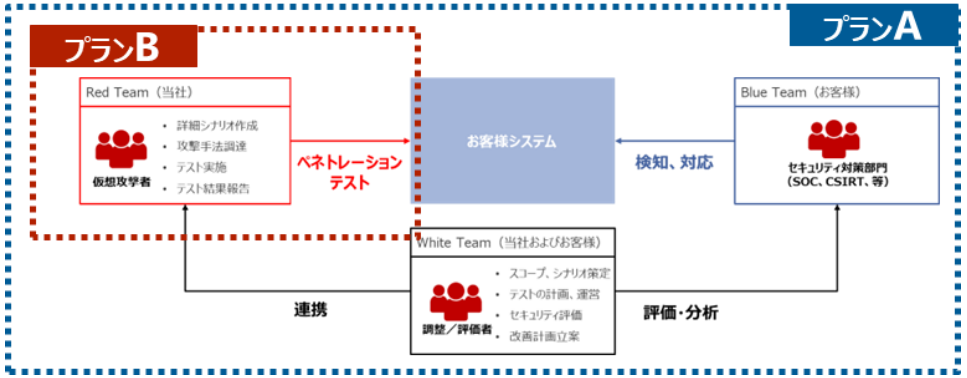
複数行合同実施による、N割効果で費用負担を軽減
（参加行統一シナリオ・同一スケジュール）

参加行の平均点や共通した改善点・傾向等をフィードバック。
横展開により各行様の効率的な振り返りに活かしていただく。

単独実施との比較で**40%**費用削減実績あり

サイバーセキュリティ合同演習

- ✓ 金融機関システムへの疑似攻撃を通じ、**被害拡大リスクや脆弱性を検出する「ペネトレーションテスト」**、侵入被害に対する**検知・封じ込め等の防衛能力も含めた総合的な確認を行う「TLPT」**の共同対策
- ✓ **共通シナリオを用意することで、事前準備の期間やコストを抑制。**また、**テスト結果を相互に共有**することで効率的な対応能力強化に貢献



ペストネーションテスト　単独実施との比較で**30%**費用削減実績あり

TLPT　単独実施との比較で**50%**費用削減実績あり

IT資産管理×脆弱性管理サービス

共同化により、資産可視化から脆弱性情報の収集～突合～分析プロセスを標準化・高度化。

IT資産管理×脆弱性管理サービス	
導入サービス	✓設計・構築/設定を含む初期導入を実施 • 基本設定（アカウント/権限） • ルール実装 • 運用フロー整備 • 自行システムとの情報連携
運用・保守サービス	✓システム基盤の運用保守を実施 • 標準：システム基盤維持のためのバージョンアップ対応 • 追加オプション： 脆弱性スキャン結果に対する助言、改善提案 保守支援（チケットアサインルール、リスク評価基準の調整、ダッシュボードやレポート機能のカスタマイズ）
製品提供	✓IT資産管理と脆弱性管理の製品の提供 • 資産管理製品および脆弱性管理製品のライセンスの交渉・調達・提供
コンサルサービス	✓オプション：IT資産管理と脆弱性管理に関する規定整備等のコンサル支援

[金融機関の実現事項]

✓IT資産管理と脆弱性管理に関する規定整備
✓IT資産の“詳細情報“可視化
✓脆弱性情報の自動収集と管理
✓定義済ルールに基づき、優先度や対応期限を自動設定
✓自動チケット化と適切な対象者アサイン

[金融機関のメリット]

✓ **当局ガイドライン**
「サイバーセキュリティリスクの特定」に対応
・IT資産情報の詳細把握
・脅威・脆弱性を収集・分析
・リスクベース（影響度の組み合わせ）の評価

✓ **自行業務プロセスの標準化・高度化**

「金融総合セキュリティサービス™」の展開方針

非競争領域であるセキュリティ分野において、銀行のみならず金融業界横断で展開。
銀行、協同組織金融機関、保険会社など幅広い金融機関でご利用可能。

金融業界横断での展開

銀行 | 信用金庫 | 信用組合 | 信託銀行 | 保険 | 証券





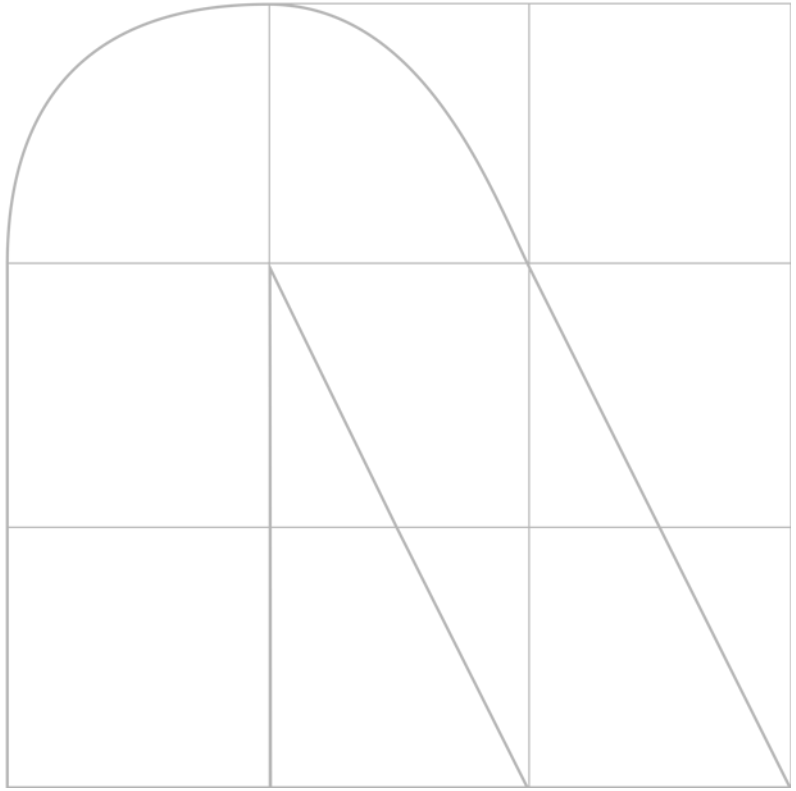

特に地域金融機関においては、金融庁発表の「地域金融力強化プラン」における
持続的成長と経営基盤強化を支えるセキュリティ高度化を本サービスで実現

共助

金融業界全体のサイバーレジリエンス強化と、安心・安全なデジタル社会の実現に貢献していきます。

03

新サービス「FinSOC®」



「FinSOC®」共同利用型セキュリティオペレーションセンター

複数金融機関で共同利用できるSOCサービスにより、先進的防御と継続的にセキュリティ対策を高度化。
監視・24/365の運用・分析を通じた改善支援で金融機関の負荷軽減・コスト効率化。

サービス概要

複数の金融機関が共同で利用可能な
セキュリティ・オペレーション・センター（SOC）サービス

NTT DATA

- 24/365のセキュリティ監視運用
- セキュリティアナリストによる高度な分析
- 速報、ユーザ部へのヒアリング業務
- 監視運用月次レポート
- インシデントレスポンス
- 脅威インテリジェンス活用

共同化によるメリット

SOC運用の高度化・効率化

- 金融庁ガイドラインに対応し、**共同サービス化**により、新たな脅威に対するノウハウ蓄積と共有し、SOC運用の高度化・効率化が可能。
- 複雑化・高度化するサーバセキュリティリスクに横断的に対応
- **金融機関ごとに異なるシステム構成に柔軟に対応。**
  IRサービスも**金融機関のニーズに応じてオプション選択可能。**

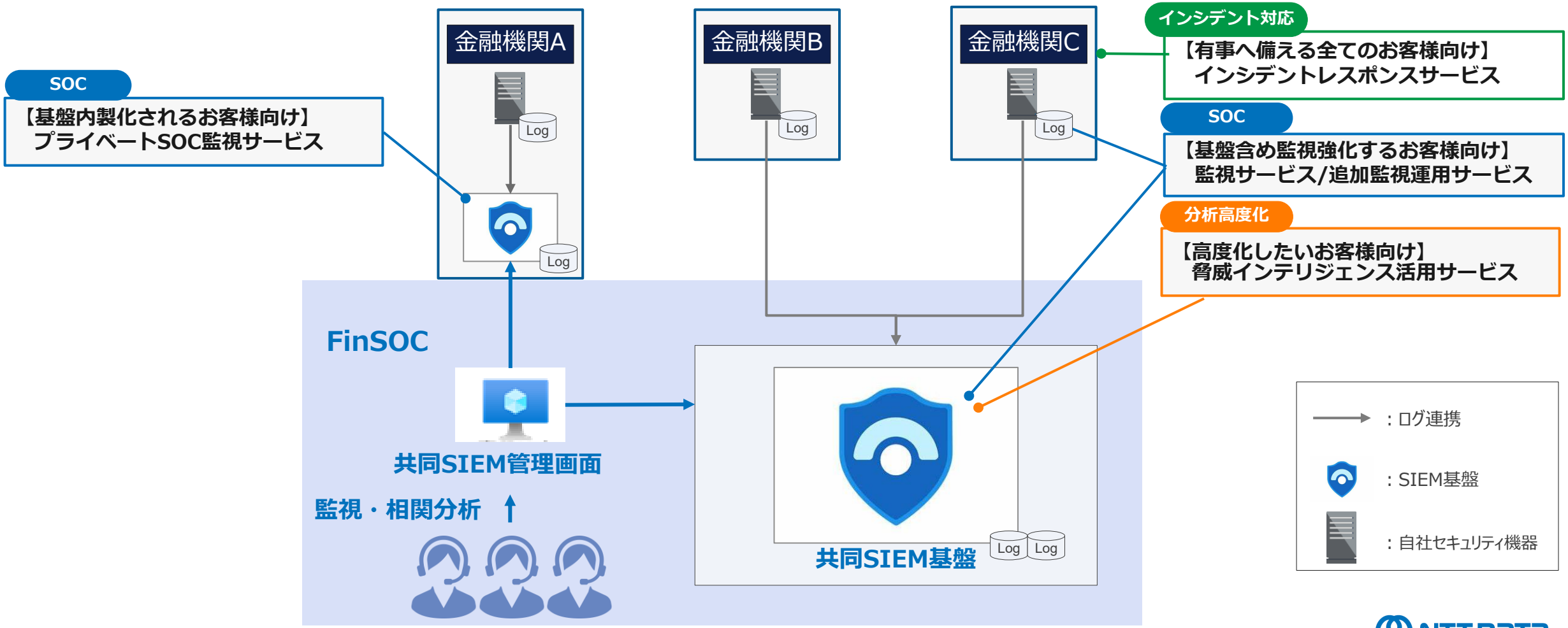
高度なセキュリティ人財の確保

- 金融系幹システムのノウハウを有した人財を**セキュリティスペシャリスト**として継続育成することで、**安定した運用体制**を実現。
- 20年以上にわたる**SOC運用・インシデント対応の実績**と知見をもとに、**24時間365日の監視**を実施。

NTT DATA

「FinSOC®」のサービス全体像

監視拠点のオペレータやセキュリティアナリスト、セキュリティ機器のログをNTTデータが集約。
共同利用型のプライベートSOC機能も提供可能。



「FinSOC®」のサービス提供範囲

監視サービスなどの一般的なSOC業務に加え、
サイバー攻撃などのインシデント発生時のCSIRT業務の一部もサービス提供範囲に含みます。

SOC 「監視サービス/追加監視運用サービス」「プライベートSOC監視サービス」

インシデント対応 「インシデントレスポンスサービス」

	SOC業務		CSIRT業務	
役割	**Tier1**	**Tier2**	**Tier3**	**Tier4**
	標準化可能な分析業務	セキュリティアナリストによる非定型な分析業務	・自社の意思決定業務 ・より高度な分析業務支援	全体管理
SOCマネジメント	• パフォーマンス測定		• パフォーマンス評価	• SOC運用管理
監視/インシデント対応	• 発報受理、チケット発行 • 誤検知判定 ＊手順化された誤検知判定 • 対応 ＊ネットワーク遮断連絡 ＊緊急連絡、等 ＊Tier2へのエスカレーション ＊チケットクローズ	• 発報受理、チケット発行 • 誤検知判定 ＊SIEM相関分析 ＊脅威情報との突合 ＊ユーザヒアリング等 • 対応 ＊ネットワーク遮断連絡 ＊緊急連絡、等 ＊チケットクローズ • 監視運用レポート作成	• インシデントレスポンス支援 ＊インシデント対応の総合的支援 • デジタルフォレンジック ＊検体やイメージの解析 • 報告書作成	• 外部機関連携 • 経営層報告、公表 • 事後対応

分析高度化 「脅威インテリジェンス活用サービス」

今後について

ＮＴＴデータは、急速に進化するサイバー脅威に対応するために、
AIを活用したログ解析や不正アクセス対応の迅速化・自動化、
PQC（耐量子計算機暗号）対応、生成AI活用時におけるセキュリティ
ガバナンス支援など、先進的なセキュリティレベルを維持してきます。

これらの取り組みを通じて、
金融業界全体のサイバーレジリエンス強化と
安心・安全なデジタル社会の実現に貢献します。


NTT DATA