NTTデータが取り組むゼロトラスト業務環境

働き方改革やデジタルトランスフォーメーション（DX）の推進で，企業は従業員に対して場所や端末によらず業務実施可能な環境を提供する必要がでてきました．NTTデータでは，従来からシンクライアントを活用してセキュアな執務環境を確保してきましたが，それに加え，より快適なコミュニケーション手段や開発環境提供のため，ゼロトラスト技術を活用してセキュリティを確保したFAT環境の導入を開始しました．ここではこの取り組みについて説明します．

はじめに

現在，NTTデータグループには世界53カ国・地域，225都市，約13万3000人の社員がいます．M&Aにより急速な拡大をしており，海外従業員は全従業員の約78%に達しています．ここでは，デジタルトランスフォーメーション（DX）[*1]・働き方改革やグローバル化というキーワードを中心に，急速なグローバル化でNTTデータが直面した課題とその対策として実施した，ゼロトラスト技術を用いたセキュアな執務環境の導入について紹介します．

*1　経済産業省の「デジタルトランスフォーメーションを推進するためのガイドライン」（DX推進ガイドライン）では，「企業がビジネス環境の激しい変化に対応し，データとデジタル技術を活用して，顧客や社会のニーズを基に，製品やサービス，ビジネスモデルを変革するとともに，業務そのものや，組織，プロセス，企業文化・風土を変革し，競争上の優位性を確立すること」と定義しています．

「Digitalを活用した働き方の改革」の必要性

2021年9月1日にデジタル庁が設立され，デジタル社会の形成を図るため，行政機関をはじめとする各方面のデジタル化推進の政策が本格化しています．厚生労働省が主幹となり「働き方改革」の実現に向け，さまざまな取り組みが進められています．日本経済団体連合会は，「企業の働き方改革」を支援するさまざまな活動を行ってきました．

NTTデータグループは，M&Aを急速に拡大してきたため，海外従業員は全従業員の約78%に達しており，多様な人材が業務に携わっています．NTTデータでは，コロナ禍以前より「Digitalを活用した働き方の改革」を中期経営計画にも掲げ，どのように実現するかを検討していました．特に「いろいろな端末」で「どこからでも」「クラウドサービス」を実現する，「新たな業務環境」をめざし構築を推進する必要があると考えていました（**図1**）．

図1　「Digitalを活用した働き方の改革」を実現させるために必要なこと

グローバルに対応したセキュリティガバナンス

M&Aにより新規にグループに参加した企業のIT環境はさまざまです．NTTデータグループ全体では，情報共有のための共通ネットワークが整備されていますが，共通ネットワークに接続する各拠点のセキュリティレベルには格差がありました．NTTデータグループ全体のセキュリティ対策レベルを調査すると，海外グループの平均値が本社水準の約半分という結果となりました．セキュリティレベルの低い拠点がサイバー攻撃の踏み台となり，グローバル全体が脅威にさらされることになります．このため，グローバル全体のセキュリティレベルをいかに底上げしていくかが課題でした．

また，リージョンごとの法律や商習慣の違いもあります．例えば，日本流のセキュリティ対策は，アジア太平洋（APAC）にとっては過剰であり，北米・欧州連合（EU）にとっては時代遅れととらえられており，セキュリティ対策の方針統一が困難でした（**表**）．

NTTデータグループのガバナンスの考え方

NTTデータグループにおけるガバナンスのあり方を考えるにあたっては，サイバーセキュリティ対策の考え方と，グローバルガバナンスの両面からアプローチを行いました．

サイバー攻撃は，攻撃者側が圧倒的に有利という非対称性を持っています．脆弱性は日々新しいものが発見されており，攻撃手法も日々変化しています．クラウドサービスの活用においては特にその傾向が顕著です．こういった情勢にあって，防御側（企業）がすべての攻撃を防ぐことは不可能です．「攻撃は受けるもの」として考え，セキュリティ対策のトレンドは「防災」から「減災」へシフトしています．これまでの防御に加えて，検知および対応・復旧の対策を如何に適切に行うかがより重要になります．NTTデータグループでもこの点を踏まえて対策を実施しました（**図2**）．

一方のグローバルガバナンスについては「リージョン最適型」の組織モデルを採用しました．M&Aにより拡大したグループ会社は業種も業態もさまざまであり，一方的なガバナンスの統合は困難です．商習慣の違いやGDPR（General Data Protection Regulation）等の規制への対応とグローバル経営効率化の観点から，グローバルHQ（Head Quarter：日本のNTTデータ）が策定したポリシーに基づきリージョンHQでルールを策定し，グローバルHQが監査を実施するような体制としました．また，その決定にあたっては世界各地域のグループ会社のCISO（情報セキュリティ最高責任者）が集まり，セキュリティ対策の策定や運用についてグローバルで連携を図りながら合意形成を進め，各社が納得したうえで施策を推進してきました（**図3**）．

グローバル全体でのセキュリティ対策の統一

グローバル全体でガバナンスを向上させるため，ソリューションの導入にあたっては以下の5点を要件としました．

① コスト（最重要要件はコストである）
② マルチテナント（会社単位で，分析を可能とする．M&Aによる会社の増減を考慮する）
③ 場所（グローバルで購入ができる製品であること）
④ 言語（グローバルでサポートが可能であること．英語は必須）
⑤ 機能（NTTデータが実施しているリスク分析の結果，重大リスクに該当するリスクに対して，適切な機能を持っていること）

グローバル各社の強みを活かし，海外グループ会社で導入済みの先進的なソリューションを採用し，APACへは

表　リージョンにおけるセキュリティ対策の違い

	APAC	日本	欧米
重視するポイント	コスト＞セキュリティ	無停止＞セキュリティ	セキュリティ＞無停止
管理対象の機器数	少ない ・拠点は少数 ・管理が容易	中程度 ・拠点は多いが国内 ・人手による管理がギリギリ	多い ・拠点は複数国に渡る ・人手による管理限界を超えている
商用ネットワークと社内ネットワークの分離	混在	分離	混在

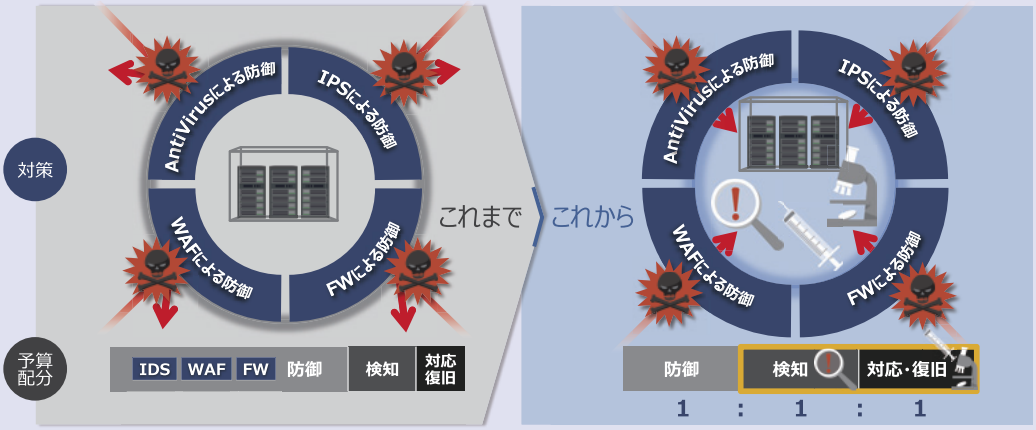

図 2　今後のセキュリティ対策は「検知」「対応・復旧」がより重要に

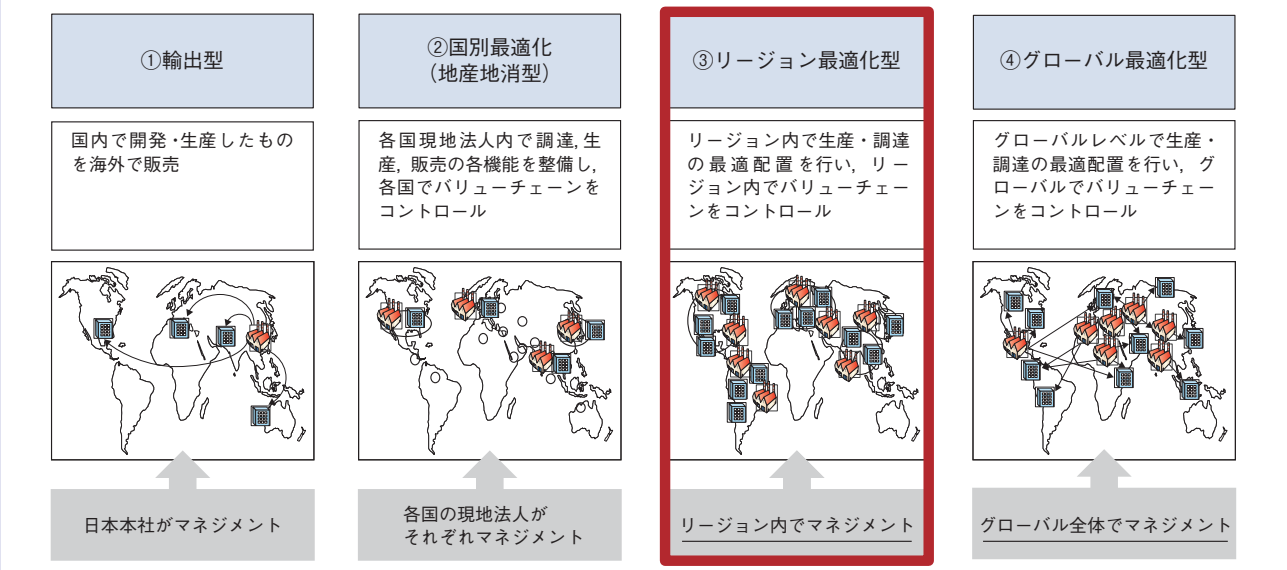

図 3　グローバルビジネスの主なパターン

HQの実績・ノウハウの展開を実施するかたちで，短期間で効果的な対策の導入を進めました．実際にNTTデータグループで採用したソリューションとNIST（National Institute of Standards and Technology）のサイバーセキュリティフレームワークとのマッピングを**図 4** に示します．

グループシナジーの創出

単にソリューションを導入するだけでは，セキュリティレベルは向上しません．並行してガバナンスの統一も必要となります．

従来は，グローバルHQが定めたルールをベースとしたガバナンスを行っていましたが，「リージョン最適化型」を実現するため，グローバルスタンダードとなるようにポリシーの見直しを実施し，グローバルセキュリティポリシー

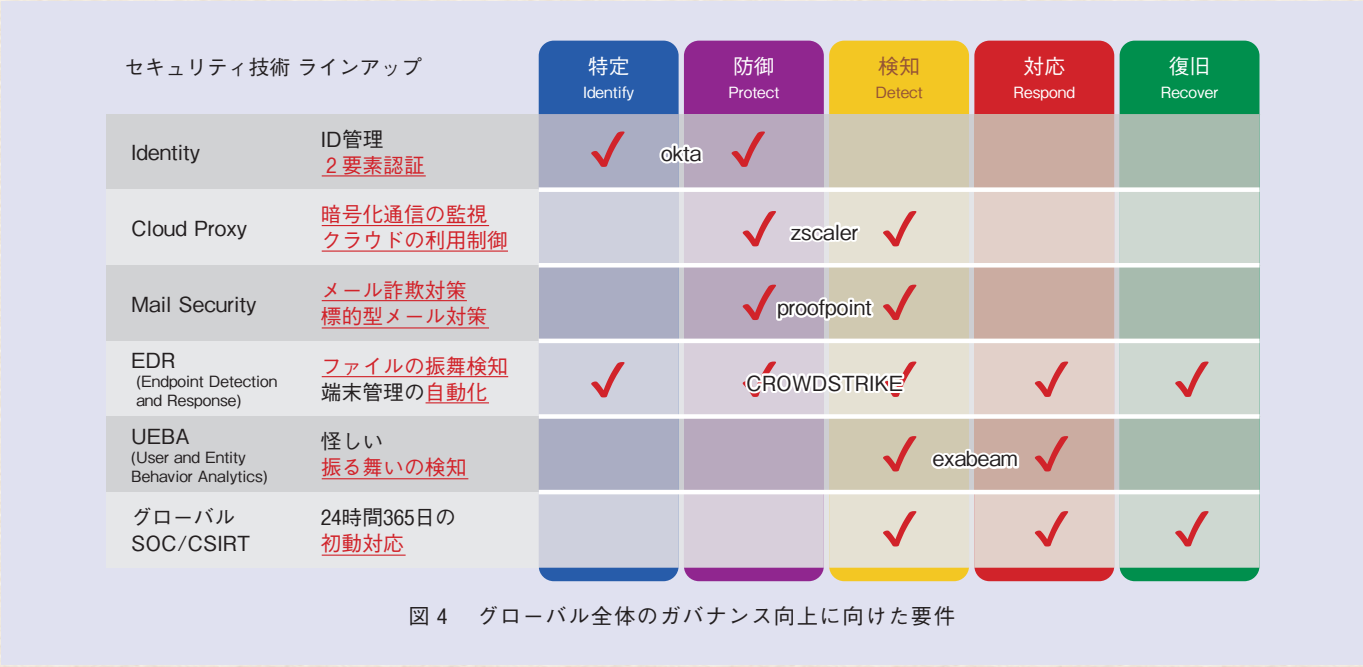

図 4　グローバル全体のガバナンス向上に向けた要件

はグローバル全体で共通化しました．ポリシーでは，グループ全体の保つべきセキュリティ水準を明確にし，ポリシーに基づく具体的なルールについては商習慣への対応や規制遵守のためリージョン単位で作成する方針としました．現在は，世界6カ所（Japan，China，APAC，Italy，Spain，U.S.A.）に監視体制を確立し，グローバル全体でリージョンごとに体制を整備しています．

また，グローバルでのポリシーおよび対策の統一にあたっては，コストや要員の面から，現実問題として対応が難しいグループ会社も存在しました．この問題については，HQによるライセンス一括購入（ボリュームディスカウント）によるコスト削減や，一部拠点の作業をHQで巻き取りつつ，ノウハウやテンプレートを各社に展開することで拠点負荷軽減・セキュリティレベル担保を図りました．

インシデント対応レベルを統一し，共通の仕組みのうえで「対応」「復旧」手順を統一することで，グローバルで戦略的な人材・ノウハウ還流を実現し，グループシナジーを生み出しつつグローバル全体でのセキュリティの底上げをすることに成功しました．

NTTデータグループのゼロトラスト

前述の施策と合わせてセキュリティ対策の管理方針を，「ルールに依存した管理」を「システムによる管理」に移行することで，さらなるガバナンス強化を実現しました．

DXの推進にあたっては，クラウドサービスなどのデジタル技術を活用することが前提となります．従来のNTTデータのルールでは，クラウドサービスの利用については原則禁止であり，業務上必要なケースに限り逸脱申請により許可していました．また，クラウドサービス利用に関するログ取得が不十分でセキュリティ監視が不可能なケースでは，チェックリストで逸脱がないことを本人に確認するといった性善説に立った対応を実施しており，私物PCなどからのアクセスも防ぐことが困難でした．今回の取り組みでは，クラウドプロキシやクラウド連携可能な認証サービスを活用することで，適切な利用者・端末のみアクセス許可し，クラウド利用上のログ取得も取得しながら十分な監視が可能となりました．

その他，セキュリティ基盤の効果をいくつか例示します．

- 従業員が社内利用禁止のクラウドサービスを不正利用して機密情報を持ち出ししようとするようなケースにおいて，クラウドプロキシが未認可のサービスへの接続を遮断することで，情報漏洩を防ぐ．
- セキュリティ対策が適切に取られたオフィス以外ではアクセスしてはいけないクラウドサービス上の情報に対して，社外からアクセスしようとした場合でも，認証サービスにて接続元IPアドレス制限を有効にすることで接続を拒否する．
- 攻撃者が不正取得したID/パスワードでクラウドサービスを利用しようとした場合でも，認証サービスにて二要素認証を有効化することで，従業員に成りすましたアクセスを防ぐ．

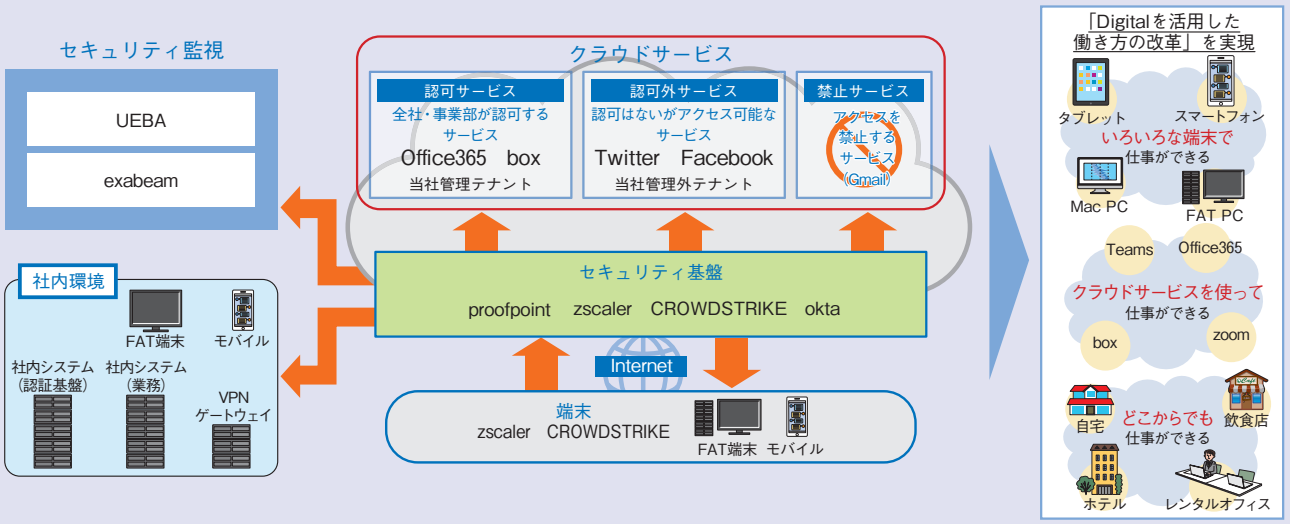

図5　ゼロトラスト技術を活用したセキュリティ基盤

・EDRやメール対策により端末へのマルウェアの混入を防ぎつつ，仮にマルウェアに感染して端末が乗っ取られた場合でも，UEBA（User and Entity Behavior Analytics）*2により通常のユーザと異なる振る舞いを検出する．

クラウド利用のためのセキュリティ技術を活用することで，端末からクラウドサービスへのアクセスに対するセキュリティ確保するセキュリティ基盤を構築しました．セキュリティ基盤を活用することで，従業員の働く場所や端末によらず適切なセキュリティを確保してクラウドサービスを利用させる「ゼロトラスト」のセキュリティ対策を実現しています．この仕組みにより，NTTデータグループはデジタル化・働き方・環境の変化との両立を実現しました（**図5**）．

NTTデータのノウハウをお客さまへ

NTTデータグループがグローバル全体で推進してきたゼロトラストを活用したDX化・働き方改革の取り組みについて説明しました．導入にあたってはさまざまな課題がありましたが，グループ全体で協議しながらもスピード感を持って解決してきました．

DX化・働き方改革は，当社に限らずどの企業でも直面している課題です．本取り組みのノウハウを最大限活用し，すでにいくつかのお客さまに対して，コンサルティングやソリューション導入の支援を実施しています．また，当社が提供するBizXaaS Office®でもBMWS（BXO Managed Workspace）という名称でゼロトラストのセキュリティ基盤提供を開始しています(1)．

今後も，当社グループ内にて蓄積したノウハウを速やかにお客さまに活用していただけるよう，改善を進めていきます．

*2　UEBA：ログ等を分析してユーザや端末などの通常の挙動を機械学習し，不正アクセスにつながる疑わしい挙動を検出する仕組み．

■参考文献

(1)　https://www.bizxaas.com/application/office/bmws/

◆問い合わせ先

NTTデータ
技術革新統括本部 システム技術本部 セキュリティ技術部
TEL　050-5545-6976
E-mail　Shusuke.Maeda@nttdata.com