ゼロトラスト・セキュリティ強化に向けた日立の取り組み

昨今，これまで主流とされていた境界型セキュリティに代わる新たなセキュリティモデル「ゼロトラスト・セキュリティ」が注目を浴びている。日立はこのゼロトラスト領域の事業化に先んじて社内IT環境での先行導入に早期より着手し，現在ではグローバル33か国の日立グループ会社内で活用している。
本稿では，この取り組みの背景として日立が抱えていた課題やその解消に向けた施策を紹介するとともに，日立が考えるゼロトラスト・アーキテクチャの構成要素とそのソリューション事業の内容について述べる。

久永 達也 | Hisanaga Tatsuya
坏 毅 | Akutsu Takeshi
上村 ゆりか | Kamimura Yurika
田村 健介 | Tamura Kensuke

1. はじめに

従来のセキュリティモデルでは，「社内ネットワークは安全で信頼されたネットワークである」という思想を根底とした境界型防御モデルが広く導入されてきた。この境界型防御では，社内ネットワークをFW（Firewall）やVPN（Virtual Private Network：仮想専用線）などの複数のセキュリティ技術で多層防御し，保護すべき情報資産を社内ネットワークに配置することでセキュリティを担保してきた。

しかし，テレワークを中心としたワークスタイルの多様化やクラウドサービスの急速な普及により，情報資産が社外ネットワーク上やクラウド上で活用されるケースが急増し，境界外でのデータ保護が求められるようになった。また，サイバー攻撃の高度化に伴い社内ネットワークへの侵入を許してしまうケースも発生し，境界内の情報資産は必ずしも安全であるとは言えなくなってきた。

このような背景から従来の境界型防御でのセキュリティ確保は限界を迎えており，これに代替する形で「すべての情報資産へのアクセスは信頼できないものである」という思想を前提としたゼロトラスト・セキュリティモデルへのシフトが広がりつつある。

日立はゼロトラスト・セキュリティの社内導入に早期に乗り出し，現在ではグローバル33か国・約2,400拠点においての社内IT環境のゼロトラスト化を実現している。本稿では，日立社内のゼロトラスト化の施策内容について解説するとともに，ゼロトラスト事業の中で重要視するポイントとその事業内容を紹介する。

2. 社内ITのゼロトラスト・セキュリティに向けた取り組み

日立は2017年5月にランサムウェア「WannaCry」による被害を受け，境界型防御のさらなる強化を推進してきた。しかし，クラウドサービスの活用や他社との協業・協創を推進していく中では，保護すべき情報資産が必ずしも社内ネットワーク内に存在するとは限らない。また事業再編の一環として進めているM&A（Mergers and Acquisitions）においては，異なるセキュリティポリシーの会社を日立のネットワーク境界内に取り込むことに時間を要し，事業機会を損失するなどの課題が顕在化してきた。そこで，ネットワーク環境に依存せず，事業環境の変化にも柔軟に対応するITインフラをめざし，ゼロトラスト・セキュリティの導入を推進してきた。

導入にあたって，ネットワークの場所に依存しないクラウドベースのIDaaS（Identity as a Service）や，未知のマルウェア対策をするEDR（Endpoint Detection and Response）を採用することで，セキュリティ課題や事業課題を解決した（**図1**参照）。

日立におけるゼロトラスト・セキュリティの主な施策は以下のとおりである。

(1) ネットワークセキュリティのクラウド移行推進

Webプロキシやリモートアクセスの機能をオンプレミスからインターネット側に移行し，クラウドサービスへの通信やオンプレミスへの通信をWebプロキシでアクセス制御すると同時に，人やデバイスの安全性に基づいて動的にアクセス制御を行う。これによりセッションレベルでの安全性を確保するよう進めている。また，本Webプロキシをハブと位置づけ，通信を経由させることにより，セキュリティポリシーの異なるM&A企業と互いのシステムを安全に利用でき，早期に事業シナジーを得ることが可能となる。

(2) エンドポイントセキュリティ強化

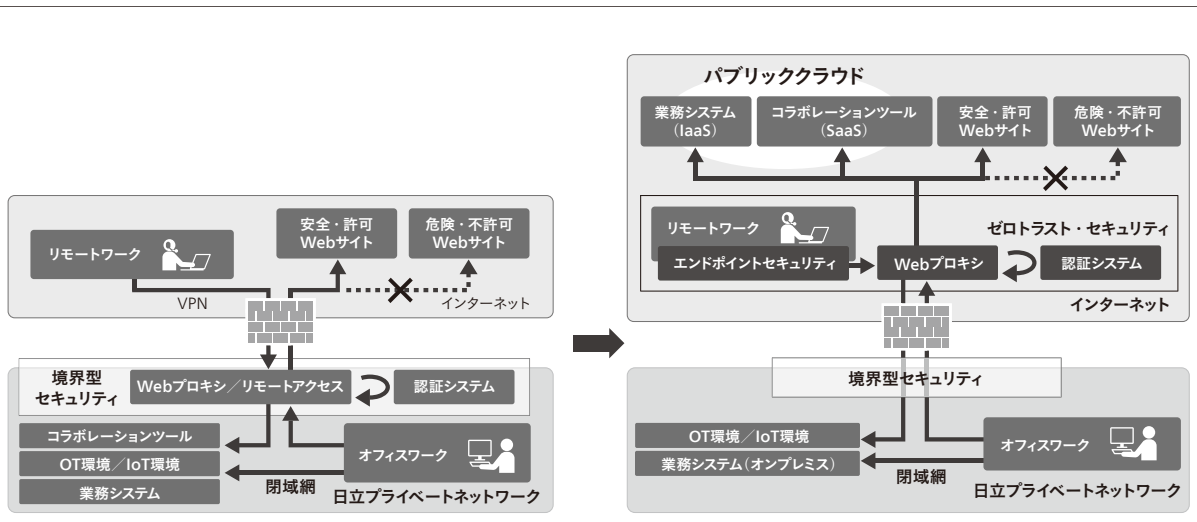
従来のEPP（Endpoint Protection Platform）による既知マルウェア対策に加え，EDRでの未知マルウェア対策（振る舞い検知）をPC端末へ導入した。今後，PC端末やスマートデバイスを一元管理するべく統合エンドポイント管理（UEM：Unified Endpoint Management）を導入し，パッチ適用やポリシー制御の強化・効率化を行う。またさらなるセキュリティ強化策として，シャットダウン時にPC端末内の情報資産を消去し，物理的なセキュリティリスク（紛失・盗難）にも対応した，ファットクライアント型「PCデータ揮発型セキュリティサービス」を開発し，安全に在宅勤務できるテレワーク環境を実現した。

(3) クラウドベースの認証基盤の採用と多要素認証による認証強化

ゼロトラスト・セキュリティでは複数要素の認証や動的リスクに対しての制御が必要である。日立ではクラウドサービスのIDaaSを採用し，デバイスや生体などの複

図1｜ゼロトラスト・セキュリティを基本とする日立のITプラットフォーム

コラボレーションツールに加えて，Webプロキシや認証基盤をクラウドに移行する。通信に加えて，人・デバイスの安全性を基に動的にアクセス制御を行う。



(1)「境界型セキュリティ」を基本とするITプラットフォーム　(2)「ゼロトラスト・セキュリティ」を基本とするITプラットフォーム

注：略語説明
IaaS（Infrastructure as a Service），SaaS（Software as a Service），OT（Operational Technology），IoT（Internet of Things），VPN（Virtual Private Network）

数要素やネットワークの場所に関係なく認証できる強固な認証システムを実現し，各種SaaS（Software as a Service）の認証をIDaaSで実施している。

ここまで日立の社内ITのゼロトラスト化に向けた取り組みを紹介してきたが，日立にはものづくりの現場があり，OT（Operational Technology）環境やIoT（Internet of Things）機器の中には，PC端末のようにゼロトラスト・セキュリティの対策が実装できないものがあるため，社内IT全体としては，ネットワーク境界で守る境界型セキュリティと，ゼロトラスト・セキュリティのハイブリッド構成となる。今後も，日立の事業拡大を支援し，DX（デジタルトランスフォーメーション）推進を加速する最適なITプラットフォームの構築を継続的に推進する。

3. ゼロトラストを推進するうえで重要となる三つのポイント

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）が公開している「NIST SP 800-207 Zero Trust Architecture」では，ゼロトラストの基本理念として七つの原則を定義している（**表1**参照）。

これらの基本理念を満たすための構成技術として，日立は「エンドポイント強化」，「動的アクセス制御」，「可視化」の三つのアーキテクチャがゼロトラストの重要な構成要素だと考える（**図2**参照）。

「エンドポイント強化」においては，EPP/EDRによる既知／未知マルウェア対策を行うとともに，UEMによりパッチ適用制御や非認可アプリケーションのブロックなど，一元的なエンドポイント制御を行う。これにより，組織のモバイルデバイスを外部脅威から保護するとともに，ユーザーの内部不正操作やセキュリティリスクの高い操作を未然に防ぐことで，組織的なサイバーハイジーンを実現する。

「動的アクセス制御」においては，IDaaSを利用しクラウドベースのID管理を行い，さらに多要素認証やリスクベース認証※1）により認証強化を図る。また，SWG（Secure Web Gateway）やSDP（Software Defined Perimeter）を導入することにより，接続元のロケーションやネットワークに依存しないシームレスかつセキュアなWebプロキシ制御／リモートアクセス制御へのアクセスコントロールを実現する。

「可視化」においては，ユーザーのクラウドサービス利用に対する安全性を検証し，可視化するCASB（Cloud Access Security Broker），機密情報の不正持ち出しなどを検知・ブロックするDLP（Data Loss Prevention），業務で利用するIT資産からログ情報を収集・分析してセキュリティインシデントや内部不正操作を早期検知するSIEM（Security Information and Event Management）/UEBA（User and Entity Behavior Analytics）など，さまざまなアプローチからシステム全体の情報収集を行い，セキュリティ状態の見える化を行う。これにより，システム全体のセキュリティリスクの事前検知やインシデント発生時の早期対処が可能となり，セキュリティ被害の未然防止や極小化を図る。

4. 日立が提供するワンストップ・ソリューション

日立が提供するゼロトラスト・セキュリティ・ソリューションでは，これまで社会インフラや金融機関を中心として幅広い業種の顧客の多種多様なニーズに合わせて培ってきたインテグレーション・運用の実績を基に，顧客の事業ビジョンに最適化したコンサルティングから

※1）認証要求元のデバイス種別や場所／時間などの行動パターンなどから不審なアクセスを検知し認証要求レベルを動的に変える認証方式。

表1｜NISTが定めるゼロトラストの基本理念

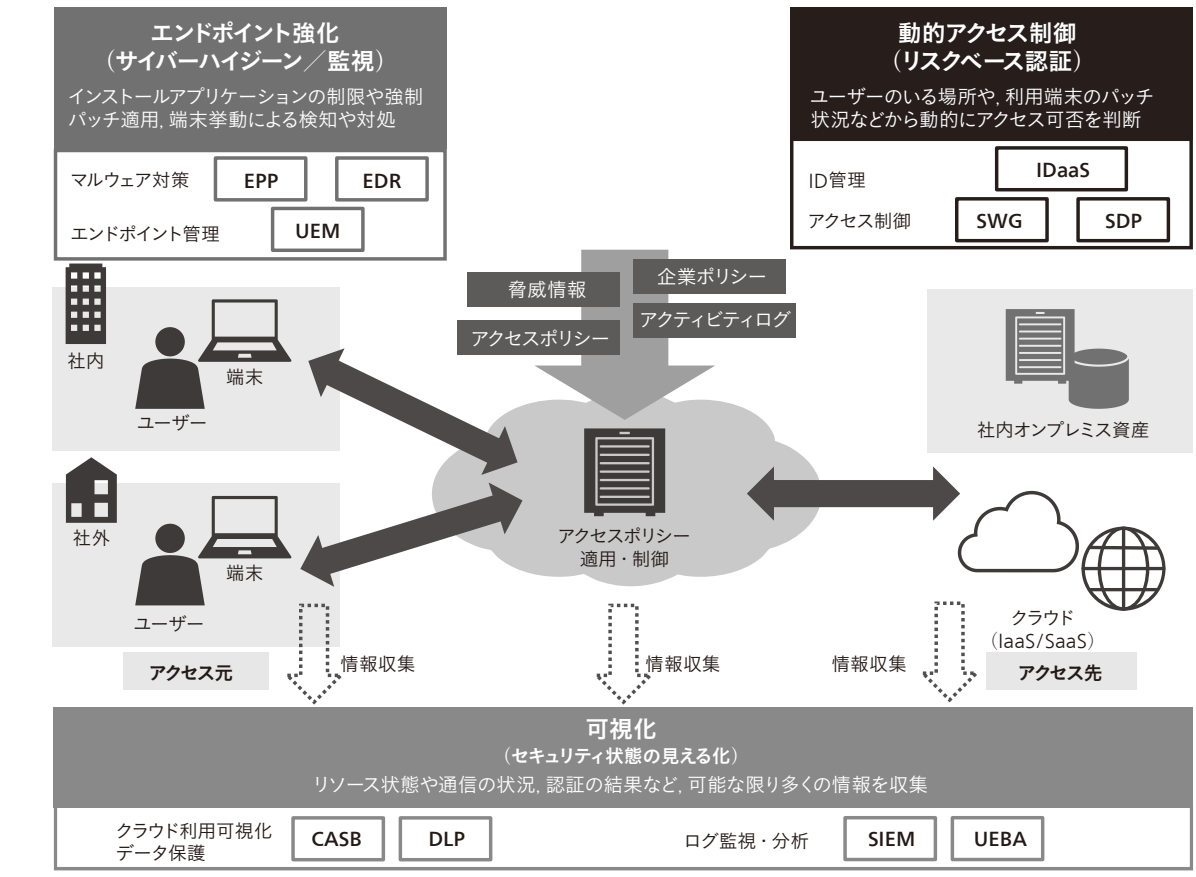
ゼロトラストを実現するうえでの理想的な考え方を定義する。組織の求めるTo-Beに応じて，すべてもしくは取捨選択した一部の基本理念の実現をめざす。

ゼロトラストの基本理念
(1) すべてのデータソースとコンピューティングサービスをリソースとみなす。
(2) ネットワークの場所に関係なく，すべての通信を保護する。
(3) 企業リソースへのアクセスは，セッション単位で付与する。
(4) リソースへのアクセスは，クライアントアイデンティティ，アプリケーション／サービス，リクエストする資産の状態，その他の行動属性や環境属性を含めた動的ポリシーにより決定する。
(5) すべての資産の整合性とセキュリティ動作を監視し，測定する。
(6) すべてのリソースの認証と認可を動的に行い，アクセスが許可される前に厳格に実施する。
(7) 資産，ネットワークインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ態勢の改善に利用する。

出典：米国国立標準技術研究所「NIST SP 800-207 Zero Trust Architecture」

図2｜日立が考えるゼロトラスト・アーキテクチャ基本構成

エンドポイント強化・動的アクセス制御によってデバイスや利用者の状況に応じた柔軟なセキュリティ対策を実現し，可視化によりセキュリティリスクの早期検知を実現する。



注：略語説明
EPP（Endpoint Protection Platform），EDR（Endpoint Detection and Response），UEM（Unified Endpoint Management），IDaaS（Identity as a Service），SWG（Secure Web Gateway），SDP（Software Defined Perimeter），CASB（Cloud Access Security Broker），DLP（Data Loss Prevention），SIEM（Security Information and Event Management），UEBA（User and Entity Behavior Analytics）

導入(サービスインテグレーション)，運用に至るまでのワンストップ・サービスを提供する（**図3**参照)。

コンサルティングでは，システム導入計画の段階から顧客に寄り添い，将来的な事業ビジョンに合わせた要件分析を実施する。要件確定後は，顧客要件にフィットするサービスの組み合わせの選定とめざすべきTo-Be像とAs-IsのGap分析を行い，ゼロトラストシステム全体のグランドデザインを行う。また，日立の社内ITのグローバル展開で培った経験を基に，国内外を問わず多数の拠点に対し，システム導入および拠点展開計画，サービスイン後の運用計画，レガシーシステムの改廃計画支援などを含めた安全かつ確実な移行ロードマップを策定し，提供する。

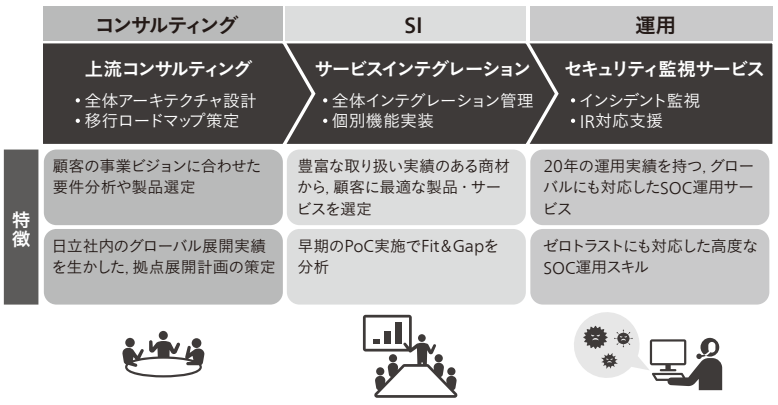
サービスインテグレーションでは，これまで幅広く取り扱い，導入実績を重ねてきた多種多様な製品・サービスの中から顧客に最適な商材を選定し，いち早くPoC（Proof of Concept）を試行することで顧客の求めるTo-Be像とのFit & Gapを分析する。製品・サービスの確定後は，製品ベンダーと一丸となって顧客ニーズに合わせたゼロトラスト環境を早期に構築するとともに，インターネットブレイクアウトを前提とした拠点展開と安全なシステム切り替えを実現する。日立の社内ITのゼロトラスト化の一環として行った大規模認証基盤の実装※2)におけるノウハウが，このインテグレーションにおいて強みを発揮する。

運用においては，24時間365日にわたり日立がグローバル提供しているSOC（Security Operation Center）運用サービスが存在しており，金融機関などを中心にこれまで20年以上にわたって多業種の顧客へセキュリティ監視業務を提供している。このSOC運用サービスは，従来の境界型セキュリティに対するレガシーなSOC運用に固執することなく，ゼロトラスト・アーキテクチャに

※2）日立社内ではグローバル約34万人（2017年当時）のグループ従業員を対象に認証基盤を統合。

図3｜日立のゼロトラスト・セキュリティ・ソリューション概要

企画立案から導入・運用まで一気通貫でのトータル・ソリューションを提供することで，顧客のニーズに適したゼロトラストを実現する。



注：略語説明
PoC（Proof of Concept），SOC（Security Operation Center），SI（Service Integration），IR（Investor Relations）

も対応する先進的な技術習得を推進することで，時代の潮流に応じた幅広く高度なSOC運用スキルを有している。この実績と先進技術を生かし，導入したゼロトラスト・セキュリティシステムに対しても高度な相関分析監視や迅速なインシデント対応を支援し，顧客のセキュリティ運用を継続的にサポートする。

5. おわりに

日立はゼロトラスト・セキュリティの社内導入に向けて先進的な活動を行ってきたが，ゼロトラストの分野はまだ発展途上の領域であり，今後のゼロトラスト・セキュリティ技術の進歩に合わせて，さらなる社内セキュリティ拡充を行っていく予定である。

この社内ITにおける先進的な取り組みから最新のセキュリティ技術動向をキャッチし，ここで培った実績やノウハウをソリューション事業にナレッジトランスファーしていくことで，日立グループが一丸となってより顧客に最適なゼロトラスト・セキュリティ環境を今後も提案・提供していく。

参考文献など

1）米国国立標準技術研究所，NIST SP 800-207 Zero Trust Architecture（2020.8），
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

執筆者紹介

久永 達也
日立製作所 サービスプラットフォーム事業本部
セキュリティイノベーション本部
サイバーセキュリティソリューション部 所属
現在，サイバーセキュリティ事業におけるSIEM／ゼロトラスト関連のSI業務に従事

坏 毅
日立製作所 サービスプラットフォーム事業本部
セキュリティイノベーション本部
サイバーセキュリティソリューション部 所属
現在，サイバーセキュリティ事業における企画立案やプロジェクト取りまとめ業務に従事

上村 ゆりか
日立製作所 ITデジタル統括本部
グローバルソリューション第2本部 戦略推進部 所属
現在，社内ITサービス（インフラ領域）の戦略・企画立案に従事

田村 健介
日立製作所 ITデジタル統括本部
グローバルソリューション第2本部 戦略推進部 所属
現在，社内ITサービス（インフラ領域）の戦略・企画立案に従事