ワークスタイル変革に不可欠なセキュリティ基盤

Security Infrastructure that is Indispensable for Work Style Reform

岡 本 宏 之，増 井 博 行

要　約　従来の境界防御型モデル（ペリメータモデル）では，多様化するサイバー攻撃の被害を抑えることが困難になってきており，新たな考え方として「ゼロトラスト」というモデルが生まれている．ゼロトラストは，あくまでもコンセプト（概念）であり，特定のソリューションや製品を指すものではない．「どうやってゼロトラスト・アーキテクチャを実現するか」は企業なりの解釈に依る．

日本ユニシスグループでは，このゼロトラストのモデルを五つの施策（「ID 管理 / 認証」「デバイス管理」「クラウド Proxy」「クラウド SIEM」「CASB」）に落とし込み，実装はクラウドサービスを利用する方針とした．クラウドサービスの利用においては，選定基準を定め，事前検証によりセキュリティ要件に対して，とりうる対策の実現性と効果を検証した．これらセキュリティ基盤の更改により，ネットワーク境界に設置されているネットワーク機器のログに加え，クラウドアプリケーションなどのセキュリティ監視対象が増加し，運用業務の負荷が増えると想定されたことから，運用体制の再整備を行っている．

Abstract　It is becoming difficult to suppress the damage caused by diversifying cyber attacks by using the conventional boundary defense model (perimeter model), and a new concept called “Zero Trust” has been born. “Zero Trust” is just a concept, it does not refer to a specific solution or product. It is necessary for companies to interpret “How to realize a zero trust architecture”.

Nihon Unisys Group has split this “Zero Trust” model into five measures (“ID management”, “Device management”, “Cloud proxy”, “Cloud SIEM”, and “CASB”), and implemented it as a cloud service. In using cloud services, we set selection criteria and verified the feasibility and effectiveness of possible measures against security requirements by prior verification. Since the number of security monitoring targets such as cloud applications will increase in addition to the logs of network devices installed at the network boundary on the renewal of these security infrastructures, and the load of operation work is expected, we have redeveloped the operation system.

1. は　じ　め　に

近年，働き方の多様化や業務の効率化を目指しテレワークの導入や社内情報システムにおけるクラウドサービスの活用など，多くの企業がワークスタイル変革に取り組んでいる．ワークスタイル変革の推進は，業務効率性や利便性を高める一方で，情報の保護，デバイスの管理，テレワーク時やクラウドサービス利用時におけるセキュリティや統制の強化が不可欠である．また，働く場所も守るべき情報資産も「社内から社外」へと変わるため，セキュリティ境界が曖昧になり，これまでのセキュリティの考え方だけでは十分なセキュリティレベルを確保できない場合がある．このように，今，企業のセキュリティ対策は大きな変革の時期を迎えている．そんな中，「ゼロトラスト」というキーワードを耳にすることが増え，「ゼロトラスト・セキュ

リティ」ないしは「ゼロトラスト・ネットワーク」とも表現される新たなセキュリティモデルが唱えられている．本稿では，ゼロトラストモデルを適用した日本ユニシスグループのセキュリティ基盤更改の事例を紹介する．2章では新たなセキュリティモデルである「ゼロトラスト」の概念を解説し，3章ではゼロトラストモデルを考慮したセキュリティ基盤の適用事例について，4章ではセキュリティ基盤更改時に考慮すべきポイントについて記載する．

2. セキュリティ概念の変革

本章では，従来のセキュリティ対策の考え方と新たなアプローチであるゼロトラストについて解説する．

2.1 従来のセキュリティ対策の限界

従来のセキュリティ対策では，自社が構築した社内ネットワークとインターネット等の社外ネットワークとの間に境界を設け，多層防御（入口対策，内部対策，出口対策）を実装し，「企業ネットワークの外側は危険で内側は安全」という境界防御型モデル（ペリメータモデル）の考え方を採用してきた．

ところが，昨今の働く場所の多様化に加え，新型コロナウイルス感染拡大の影響を受け，在宅勤務やテレワークが拡大しており，社外ネットワークから社内ネットワークの情報資産やシステムへのリモートアクセスの頻度が増している．また，クラウドサービスの利用により，社内ネットワークから社外のクラウドサービスに情報資産を持ち出す場合がでてくるなど，ネットワーク境界が外部へ拡張され境界防御型モデルの根幹であった境界そのものが曖昧になりつつある．

また，情報システム部門が関知しない不適切なアプリケーションやクラウドサービスの利用（シャドーIT）から生じる情報漏洩リスクに加え，標的型攻撃やランサムウェアなどのサイバー攻撃も高度化・多様化しており，これまで一般的だったファイアウォールやゲートウェイでのウイルス対策といったネットワークの境界を防御するだけの対策では防ぎきれない，セキュリティリスクが増加している（図1）．

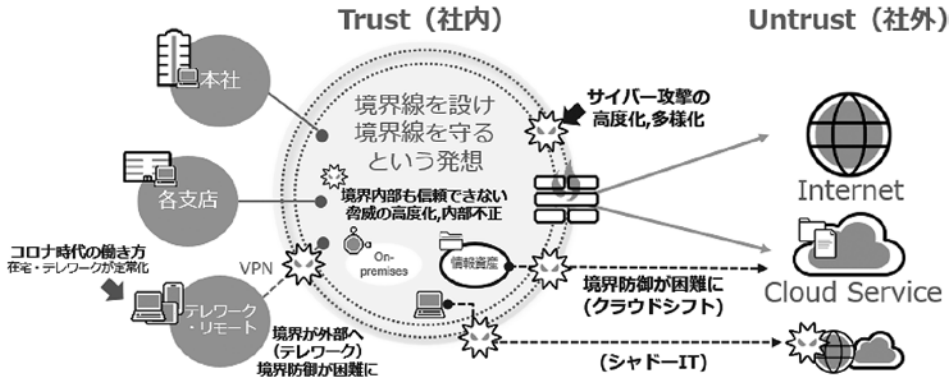

図1　境界防御型モデル（ペリメータモデル）の限界

2.2 ゼロトラストモデル

前節で解説した境界防御型モデルが置かれた状況とセキュリティ対策のリスクを解消するも

のとして，ゼロトラストモデルという新たなアプローチが注目されている．本節では，ゼロトラストの概念と米国標準技術研究所（NIST：National Institute of Standards and Technology）の定義「SP 800-207 Zero Trust Architecture（ZTA）」[1]およびゼロトラストの最初の構成を大幅に拡張し定義された「Zero Trust Extended（ZTX）エコシステムモデル」について解説する．

2.2.1　ゼロトラストの考え方

従来型のセキュリティ対策のリスクを解消するゼロトラストというキーワードが最初に世に出たのは2010年のことである．これは当時，Forrester Research社のアナリストであったJohn Kindervag氏（現Palo Alto Networks Field CTO）が自身のレポート[2]で提唱したセキュリティのコンセプト（概念）である．ゼロトラストは，文字通り「何も信頼しない」ことを意味しており，境界防御型モデルが「信用する，しかし検証する（Trust but verify）」という前提であったのに対し，ゼロトラストモデルは「検証し，決して信用しない（Verify but never trust）」を前提としている．曖昧な「境界」の概念を排除し，常に侵害があるものと考え，守るべき情報資産にアクセスするものは全て信用せずに検証することで，情報資産への脅威を防ぐという新しい考え方である．ゼロトラストモデルの考え方を図2に示す．

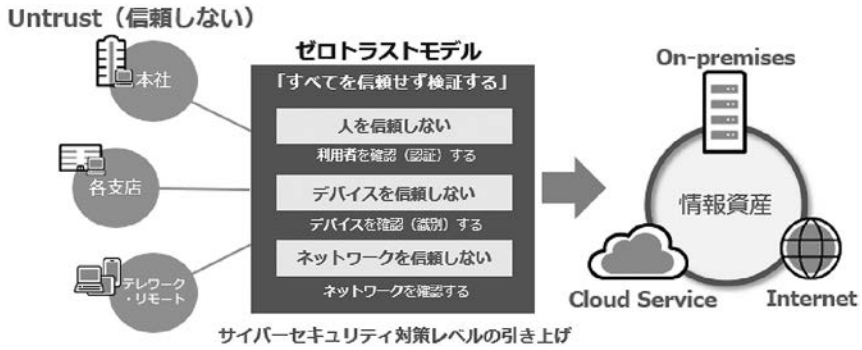

図2　ゼロトラストモデルの考え方

ゼロトラストは，あくまでもコンセプト（概念）であるため，特定のソリューションや製品を指すものではない．「どうやってゼロトラスト・アーキテクチャを実現するか」は企業なりの解釈に依る．

2.2.2　NISTのゼロトラストアーキテクチャー

ゼロトラストの定義や実現の方法については，セキュリティ企業各社で様々な検討が進められている．そのような中，NISTにおいてゼロトラストアーキテクチャーを定義しようという動きがあり，2019年9月23日「SP 800-207 Zero Trust Architecture（ZTA）」のDraft発行にはじまり，2020年8月11日には，そのFinal版[1]が発行された．

その冒頭で，ゼロトラストは，リソース（情報資産，サービス，ワークフロー，ネットワークアカウントなど）の保護に重点を置くものであると記載されおり，ネットワークロケーションは，もはやセキュリティ体制の主要なコンポーネントではなくなった．

物理的なネットワークのロケーションによる保護を前提とせず，企業が所有するネットワー

ク境界内に配置されていないリモートユーザーやクラウド上の情報資産を含め，ユーザー，資産，およびリソースを保護することに焦点を当て，情報資産またはユーザーアカウントに暗黙の信頼を付与せず，企業リソースへのセッションが確立される前に必ず認証と承認を行うものとしている．また，この記述の中でゼロトラストと，ゼロトラストアーキテクチャーという用語について以下のように定義している．本項の 1）と 2）で詳説する．

・Zero Trust（ZT）：ネットワークが侵害されることを前提に，情報システムおよびサービスの要求ごとに，正確なアクセス決定を実施する際の不確実性を軽減するように設計されたコンセプトとアイデアのコレクションを提供すること．
・Zero Trust Architecture（ZTA）：ゼロトラストの概念に基づき，コンポーネントの関係性，ワークフロー計画，およびアクセスポリシーを含めた企業のサイバーセキュリティ計画のこと．

1）ゼロトラストのアクセスモデル

ゼロトラストのアクセスモデルは，リソース保護に焦点を当てたサイバーセキュリティパラダイムであり，信頼が暗黙的に付与されることはなく，継続的に信頼性を評価することを前提としている（信頼せず，常に検証する）．ゼロトラストにおけるアクセス抽象モデルを図 3 に示す．

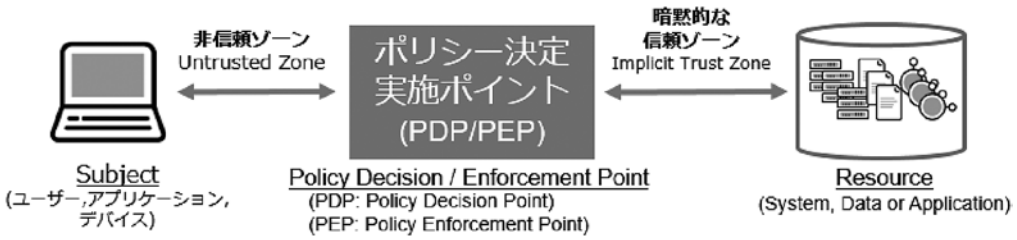

図 3　ゼロトラストのアクセス抽象モデル

NIST Special Publication 800-207 Zero Trust Architecture (Final)
2. Zero Trust Basic Figure 1: Zero Trust Access を基に記載.

このモデルでは，サブジェクト（ユーザーやアプリケーション，デバイス）が企業リソースにアクセスする際は，非信頼ゾーンからのアクセスであることを前提とし，必ず間に入るポリシー決定ポイント（PDP）および対応するポリシー実施ポイント（PEP）を介してアクセスを許可する．システムは，サブジェクトが本物であり，要求が有効であることを確認すべきであることを示している．

また，ポリシー決定ポイント（PDP）/ポリシー実施ポイント（PEP）は，サブジェクトがリソースにアクセスできるよう常に適切な判断を下す．これは認証と承認という二つの基本的な領域にゼロトラストが適用されることを示している．

そして，ポリシー決定ポイント（PDP）がアクセス要求を信頼したり適用するポリシーを決定したりする際の判断基準を，個々の企業リソースへのアクセス要求に対して正しく一貫して適用するようにシステムを設定するべきであるとしている．

2）ゼロトラストの七つの基本原則

Zero Trust Architecture（ZTA）では，ゼロトラストを実現する上での基本原則がまとめられている．これらの原則は理想的な目標であり，“すべての原則が特定の戦略に対し，最も純粋な形で完全に実装されるとは限らない”と記載されている．その七つの基本原則の要約を表1に記載する．

表1　ゼロトラストの基本原則

#	ゼロトラストの原則
1	All data sources and computing services are considered resources. すべてのデータソースとコンピューティングサービスはリソースと見なす．
2	All communication is secured regardless of network location. 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	Access to individual enterprise resources is granted on a per-session basis. 個々の企業リソースへのアクセスをセッションごとに許可する．
4	Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. リソースへのアクセスは，動的ポリシー（クライアントID，アプリケーション/サービス，および要求元の資産の観察可能な状態を含む）により決定され，他の動作および環境属性が含まれる場合がある．
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets. 企業は，所有および関連するすべての資産の整合性とセキュリティ体制を監視および測定する．
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed. すべてのリソース認証と承認は動的かつアクセスが許可される前に厳密に実施する．
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. 企業は，資産，ネットワークインフラストラクチャ，および通信の現在の状態について可能な限り多くの情報を収集し，それを使用してセキュリティ体制を改善する．

ゼロトラストの多くの定義と過去の議論では，「従来の境界型防御を除去する」という部分が強調されていた．しかし境界型防御の機能は，ゼロトラストを実現する機能の一部として，何らかの形でペリメータに関連するものとして取り入れられている．

重要なのは，従来の境界型防御の排除ではなく，これら七つの基本原則を満たす状態を作り込むことが理想的なゼロトラストであると定義されていることである．ただし，あくまでもこれらは理想的な目標であり，上述したように「すべての原則が特定の戦略に対し，最も純粋な形で完全に実装されるとは限らない」とされていることにも着目すべきである．

2. 2. 3　Zero Trust eXtended（ZTX）

Forrester Research社のChase Cunningham氏はゼロトラストの最初の構成を大幅に拡張し，Zero Trust eXtended（ZTX）エコシステムモデルとして改め，ゼロトラストモデルに求める要件を公開している[3]．

ゼロトラストモデルでは考え方や概念を示していたのに対し，Zero Trust eXtendedエコシステムモデルは，「People：アイデンティティ」「Devises：デバイス」「Data：情報資産」

「Workloads：ワークロード」「Networks：インフラ・ネットワーク」「Visibility and analytics：可視化と分析」「Automation and orchestration：自動化とオーケストレーション」という，相互関係にある七つの領域に落とし込んだ包括的なフレームワークである（図4）．これらの領域に既存の技術やソリューションをマッピングすることでゼロトラストセキュリティを実装するイメージを提供している（表2）．

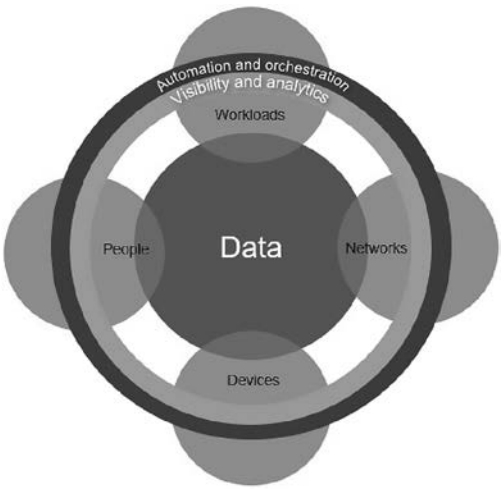

図4　The Zero Trust eXtended Framework
The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q3 2020 を基に記載

表2　ゼロトラストセキュリティで考慮すべき七つの領域

領　域	ゼロトラストの考え方	セキュリティ要件と代表的なテクノロジ
Data	守るべき情報資産の原則（分類，分離，暗号化）への準拠	データセキュリティ： DLP（Data Loss Prevention）[*1]
People	ユーザー認証やアクセス認可の強化	アイデンティティセキュリティ： IAM（Identity and Access Management）[*2]
Workloads		ワークロードセキュリティ： CWPP（Cloud Workload Protection Platform）[*3] CSPM（Cloud Posture Management）[*4]
Networks	不正アクセスの可能性があるネットワークの分離，ネットワークを小さな論理セグメント（マイクロセグメント）に分割	ネットワークセキュリティ： SWG（Secure Web Gateway）[*5]
Devices	企業リソースにアクセスする際のデバイスの識別と承認管理とデバイス保護	デバイスセキュリティ： EPP（Endpoint Protection Platform）[*6] EDR（Endpoint Detection and Response）[*7] MDM（Mobile Device Management）[*8]
Visibility and analytics	ログの取得と分析，可視化	可視化と分析： CASB（Cloud Access Service Broker）[*9] SIEM（Security Information Event Management）[*10]
Automation and Orchestration	組織全体のIT運用の自動化，異種システム全体の詳細な制御	自動化： SOAR（Security Orchestration and Automation Response）[*11]

The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q3 2020 を基に加筆して記載

3.　セキュリティ基盤へのゼロトラストモデル適用事例

本章では，ゼロトラストモデルを考慮したセキュリティ基盤の適用事例について紹介する．

3.1　セキュリティ基盤更改の位置づけと目標

日本ユニシスグループのサイバーセキュリティ戦略[4]では，サイバーセキュリティ経営を継続的に実践するためのビジョン，目標，活動計画等を定め，広範囲かつ多様なセキュリティ施策を，総合セキュリティ委員会配下の推進プロジェクト体制で統括し推進している．日本ユニシスグループのサイバーセキュリティ戦略の概略を図5に示す．

図5　日本ユニシスグループのサイバーセキュリティ戦略

この戦略において四つの施策を掲げているが，その中の一つ「システム施策/社内システム」において，“社員に対し安全な社内システム環境を継続的に提供すること”を目標として掲げている．この目標は，“社内システムで外部クラウドサービスを利用すること，働く場所が変化すること，多様なビジネスパートナーと密接に連携すること”などの環境変化への課題認識によるものである．「システム施策/社内システム」検討項目の一つとして，2019年9月から開始したセキュリティ基盤更改の検討により「働き方の変化に応じたセキュリティ対策ポイントの変化」と題した社内報告が提示され，以下のセキュリティ対策の強化が求められている．

・クライアントPCのセキュリティ対策・情報漏洩対策の強化（事故発生時の対応の最速化）
・クラウドサービスの利用拡大を前提にしたセキュリティ対策
・利用者の利便性，運用管理者の利便性，安全性の確保等

3.2　セキュリティ基盤強化に向けた五つの施策

前節で記載したセキュリティ基盤への要求を実現するため，ゼロトラストの考え方に基づき図6に示す五つの施策を定義した．各施策に対する実装は，ソリューション（クラウドサービス）を組み合わせて導入する方針とした．デバイスやロケーションに依存せず，ネットワーク境界を意識することのないセキュリティ対策と利用方式を目指し，段階的にセキュリティ基盤を更改していく計画とした（2020年4月着手）．

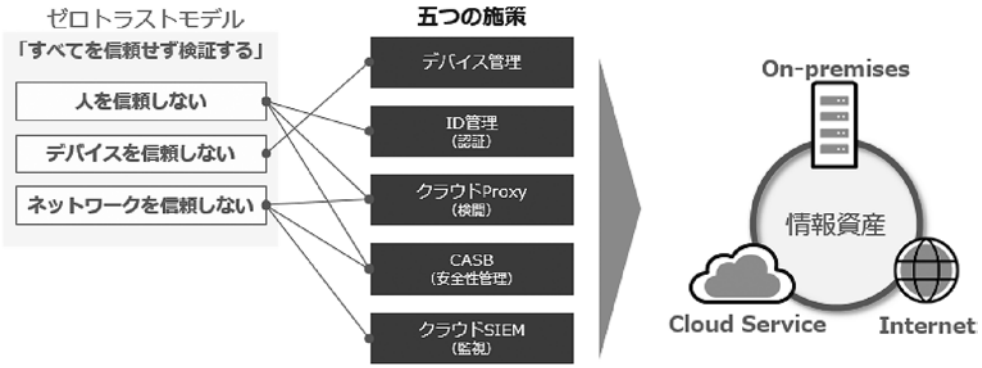

図 6　ゼロトラストモデルの要件を取り入れた五つの施策

五つの施策と Zero Trust eXtended（ZTX）で定義された七つの領域の関係を図 7 に示す.

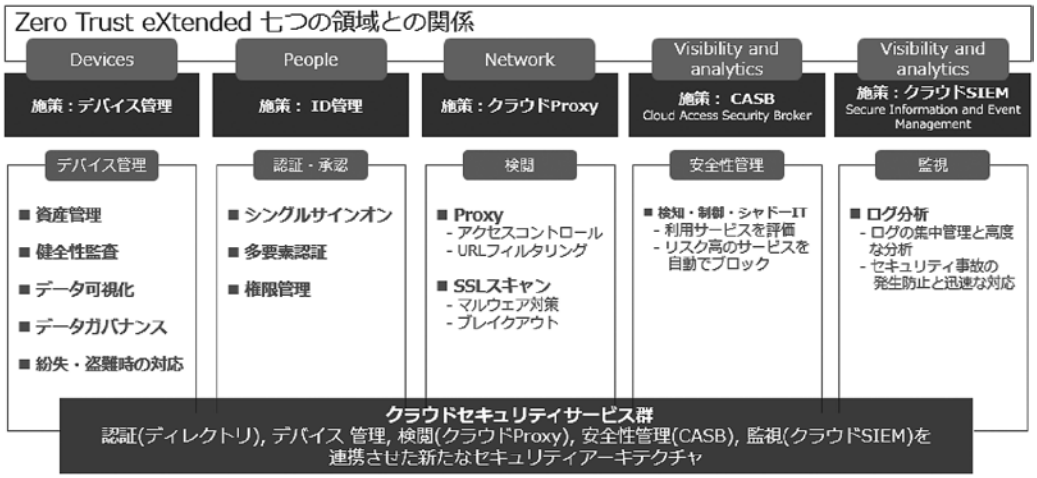

図 7　五つの施策と ZTX の七つの領域との関係

以下は施策実装の優先順位である.（ ）内は ZTX の七つの領域とのマッピング例である.

1）「ID 管理/認証」（People/アイデンティティセキュリティ）
2）「デバイス管理」（Device/デバイスセキュリティ）
3）「クラウド Proxy」（Network/ネットワークセキュリティ）
4）「クラウド SIEM」（Visibility and analytics/可視化と分析）
5）「CASB」（Visibility and analytics/可視化と分析）

ゼロトラストでは，“攻撃者が環境に存在し，企業が所有する環境が企業所有以外の環境と同じであるか，信頼できる環境ではない”ことを前提としており，“企業は暗黙の信頼を想定せず，情報資産とビジネス機能に対するリスクを継続的に分析および評価してから，これらのリスクを軽減するための保護を制定する必要がある”と定義している．また，これらの保護には通常，“アクセスが必要であると識別されたサブジェクト（エンドユーザー，アプリケーション，および情報を要求するその他の非人間的エンティティ）とアセットのみのリソース（デー

タ，コンピューティングリソース，アプリケーション/サービスなど）へのアクセスを最小限に抑え，各アクセス要求の ID とセキュリティ体制を継続的に認証および承認することを含めるべき”としている．

こうしたことから，セキュリティ対策の大部分において中心となるのが「ID 管理/認証」となると考え，「ID 管理/認証」を最優先とし，続けて「デバイス管理」とした．「検証し，決して信用しない（Verify but never trust）」というゼロトラストモデルに基づいたセキュリティ対策を実施するには，“アイデンティティセキュリティ”の要件をまず満たすことを考えた．

3. 2. 1　五つの施策の全体像

3.2 節の五つの施策の構成イメージ（全体像）は，図 8 のようになる．

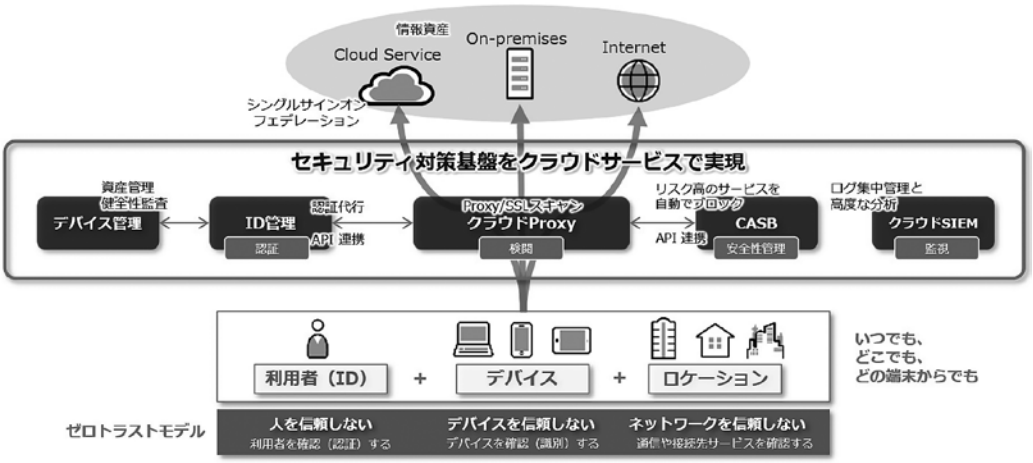

図 8　五つの施策展開全体像

ゼロトラストの考え方にあわせ，情報資産へのアクセスは，利用者の認証を「ID 管理/認証」で行い，利用デバイスおよびポリシー適用状態を「デバイス管理」で確認する．この時「ID 管理/認証」または「デバイス管理」のどちらか一方ではなく，双方による条件判定を常に行う．また，利用者プロファイルによるアクセス権限に応じて，「クラウド Proxy」で情報資産へのアクセス可否を判断する．

外部情報資産（クラウドサービスの利用等）へのアクセス時には必ず「クラウド Proxy」を介する構成とすることで，在宅勤務やテレワークなど社外にいる時に社内ネットワークを経由することなく直接インターネット回線を利用して外部情報資産へアクセスできるようにした．これにより利用者の利便性向上およびアクセス経路の統制によるセキュリティ向上を図っている．また出社時など社内にいる時の社内ネットワークから外部情報資産へのアクセスも「クラウド Proxy」を介する構成とし，アクセス経路を一元化した．

日本ユニシスグループでは，これらセキュリティ基盤を構成するものすべてにクラウドサービスを採用している．クラウドサービスを利用することにより，セキュアかつスケーラブルにセキュリティ対策基盤の構築や維持ができ，また，適用するサービスを置き換えることでセキュリティ技術の変化や進化に追従しやすいという利点がある．次項以降で各施策の対応内容の一部を紹介する．

3. 2. 2　ID 管理/認証

クラウドサービスの利用増加やワークスタイル変革への対応，および認証情報の統合を狙いとして，IDaaS（Identity as a Service）を活用し，認証基盤を再構成した．

クラウドサービス利用時の認証情報（ID）は，IDaaS 側で一元管理することで，社員の入社や人事異動など，イベント発生時の ID や属性情報の差異発生を防ぎ，シングルサインオンを実現し，利用者の利便性向上を図った．また，IDaaS が持つ機能を利用することで認証レベルの向上（多要素認証の採用等）ができる認証基盤とした．

ワークスタイル変革や昨今の新型コロナウイルス感染抑止のためのテレワーク拡大などから，社外で働くことが多くなっており，従来のように VPN ゲートウェイを利用した社内ネットワークからクラウドサービスにある情報資産を利用することは，利便性や生産性が良いとは言えない．VPN 環境では，利用する場所やデバイスに応じて接続の安全性を確認したり，条件に応じて多要素認証を行ったりすることもできない．そこで IDaaS を活用することにより，条件に応じたアクセス制限（利用者属性やデバイス管理との組み合わせによる判断）や多要素認証を機能として追加することができ，認証の際に接続環境（利用するデバイスも含め）を判断したうえで，社内からのアクセスでは ID/パスワード認証と統合 Windows 認証，社外からはもう一つの認証要素を加えて認証することを実現した．

認証情報の統合という視点では，アカウント情報データベース，ディレクトリ情報管理の仕組みとワークフローサービスによるアカウント情報/属性等の維持管理を行える仕組みを有しており，グループ会社を含めた ID 情報の維持管理を行っている．ID や属性情報の大元がこれらの仕組みによる管理となるため，IDaaS の採用に際してもこれらの仕組みと親和性の高いプロダクトを採用することで，IDaaS まで首尾一貫した情報リソースとなるよう構成した．また，IDaaS 上での ID・グループ情報の管理は，IDaaS へ連携する元の属性情報を条件として自動的にグルーピングすることで運用負荷を低減している（利用者種別：社員は社員グループ，派遣社員は派遣社員グループへ属させる，グループ A は，社員グループと派遣社員グループを属させるなど）．

以上のように，認証基盤は「ID 管理/認証」をベースとしゼロトラストの「信頼せず検証する」というモデルを適用している．

3. 2. 3　デバイス管理

日本ユニシスグループでは，主なデバイスとして OA 用 PC（Windows 10）とモバイルデバイス（Apple 社製 iPhone，iPad）を貸与しており，デバイス管理については，MAM（Mobile Application Management）[*12] と MDM（Mobile Device Management）[*8] の観点で見直した．

MAM の観点においては，モバイル利用時のデバイスへの情報ダウンロードからデータ漏洩に繋がるセキュリティ事故を懸念し，従来はセキュアブラウザを利用してきたが，MAM 対応のネイティブアプリケーションに限り利用することを許容した．これによりセキュアブラウザ利用に比べ，アプリケーション本来の UI や機能を利用できることやアプリケーション間のシングルサインオン（この点は「ID 管理/認証」と連携）など利便性の向上が図れている．

また，この MAM のデータ保護ポリシーにより，MAM 対象アプリケーションが動作する範囲内でのデータ保護ができ，MAM 対応以外のアプリケーションへのデータ移動を禁止するなどのセキュリティ保護ができる．さらに MDM と依存関係なしで利用できる MAM を採用

すれば，会社承認デバイスのみならず，個人利用デバイスでの MAM 対象アプリケーションの利用も視野に入れることができる．

MDM の観点では，「ID 管理/認証」との親和性が高いことや，Windows 以外の iOS や Android，macOS など複数のデバイスの一元管理と機能制御などの機能性を重視したプロダクト選定を行った．MDM により利用者が所有・利用するデバイスに一定のセキュリティレベルを保持させ，情報資産へのアクセス時にそれらのデバイス以外は信用しない（利用時に必ず検証する）というゼロトラストモデルへの対応を図っている．

また，「デバイス管理」は単体で考慮するのではなく，「ID 管理/認証」と密接に連携させ，「利用者もデバイスも信頼しない」というゼロトラストの考えに基づき，誰がどのデバイスでアクセスしているかを検証するモデルを実現している．

3. 2. 4　クラウド SIEM（Security Information and Event Management）

サイバー攻撃が高度化・巧妙化する中で，標的型攻撃など従来の境界面における対策では防ぎきれず，業務遂行上，正当な権限を持つ者による情報持ち出しなど，組織内部の者による情報漏えいリスクが存在している．日本ユニシスグループ内のセキュリティ監視機能であるプライベートセキュリティオペレーションセンター（以下，PSOC）が担う，脅威監視業務やイベント管理業務を支援する基盤として，脅威の侵入を前提とした検知や脅威発生の予兆を把握することを目的とし，「クラウド SIEM」を検討した．

従来は，ネットワーク境界の各種機器のログを採取・集中管理し，脅威の侵入の痕跡の確認や分析を行っていたが，セキュリティ基盤や情報資産を活用するクラウドサービスのログそれぞれを一元的に蓄積・管理し，保安上の脅威となる事象をいち早く検知・分析できるようにするため，クラウドサービスとも親和性の高いクラウド SIEM を選択した．

クラウド SIEM と連動して，管理データベースに SIEM が検知した脅威情報を蓄積するとともに，脅威の分析・対応内容の履歴を記録することで PSOC のナレッジベースとして機能するイベント管理システムを構築している．SIEM が各種センサーのログを分析し発生したイベントを管理することで，発生したイベントとその調査状況，イベントに対する調査内容や調査結果，対応内容等を記録することができる．PSOC を運用する中で，過去に調査を行ったイベントの情報を蓄積しておくことで，以後の調査において必要な情報を検索でき，調査の効率化を図ることができる．日本ユニシスグループの PSOC 運用においては，SIEM とイベント管理の役割を分け，それぞれの役割を担当するサーバーも分けている[5]．

3. 2. 5　クラウド Proxy

以下の二つの課題解消のためにクラウド Proxy の導入を検討した．

1）社外へ持ち出した PC から，直接インターネットへアクセスでき，マルウェアへの感染や本人の意思に関係なく情報が漏洩する危険性を孕んでいる

2）社外からの通信は，すべて VPN により社内ネットワークを経由しており，クラウドサービスの利用時の通信品質が VPN トラフィック量や本社拠点回線のトラフィック量に左右されている

一つ目の課題解決に向けて，クラウドProxyにより社内・社外からのアクセスルートを統制し，脅威の侵入経路となるWebトラフィックに対し，どの拠点からのアクセスも同一レベルのポリシーを適用させ，その管理の一元化や「ID管理/認証」と連携して利用者に対して同じポリシーが適用されることを考慮した．

また，社外からのアクセスの場合は，VPN環境をフル・トンネル方式[*13]からスプリット・トンネル方式[*14]へ移行し，社内イントラネットへの通信のみVPNを通し，インターネットへの通信はクラウドProxyを経由して直接インターネットへアクセスさせることで通信効率の向上を図った．

二つ目の課題は，ローカルブレークアウトにより解決する予定である．従来，本社拠点にインターネット環境を集約し，各拠点からのインターネット通信を行っているが，ここでいうローカルブレークアウトとは，本社以外の各拠点から直接インターネットへ接続できるようネットワークを再構成することであり，クラウドProxyを経由してクラウドサービスに直接通信できるようにし，セキュリティを担保しながら通信環境を最適化する（テレワーク環境からもオフィスからも同じネットワーク仕様となる）．これにより本社拠点への通信量が削減されることから本社拠点の回線削減等のコストセーブも期待できる．

また，上記以外にもクラウドサービスとして提供される専門的な機能の利用により，セキュリティ向上や基盤メンテナンスなどの運用面の省力化も期待できる．

加えて，クラウドProxyのログをクラウドSIEMやCASBに転送し，相関的なログ分析をすることにより，利用者の危険な行動をより細かくチェックすることも可能になる．

3. 2. 6　CASB（Cloud Access Security Broker）

CASBは，米ガートナー社が提唱したコンセプトであり，ガートナー社ではCASBを次のように定義している．“CASBs（Cloud access security brokers）とは，オンプレミスまたはクラウドベースのPEP（policy enforcement points：セキュリティポリシー実施ポイント）で，クラウド利用者とクラウドサービスプロバイダーの間に配置し，クラウド利用時の企業のセキュリティポリシーのガバナンスを実現する．認証，シングルサインオン，アクセス制御，デバイス管理，暗号化，トークン化，ログ取得，アラート機能，マルウェア対策など様々なタイプのセキュリティポリシーを統合的に適用するものである．”[4]

日本ユニシスグループではCASBの導入に際し，以下に挙げる五つの目的を定義・検討しており，2021年2月より選定製品の評価・検証を経て本番運用を迎える予定である．

1）クラウド利用申請の簡素化
- クラウドサービスの利用申請に対し，利用可否を判断する部署担当者が管理画面にログインし，対象サービスの評価値を参照できること
- このクラウドサービスの評価値により，対象サービスの利用許可・不許可判定の基準が得られること

2）危険なクラウドサービスの利用制限
- 評価（レーティング）の低いクラウドサービスへのアクセスを可視化・遮断する
- これにより利用者が危険なクラウドサービスを利用することによる事故発生リスクを低減する

3）オンライン会議の可視化
・利用者によるファイルのアップロード・ダウンロードといったアクティビティを詳細に可視化・分析できること
・これによりセキュリティ事故の原因追及ができること
4）アクセス先の可視化（オンライン会議以外）
・利用者の通信状況（いつ，どこから，どこへ）を可視化し，問題発生時に後追いで確認できること
5）利用者の行動分析
・大量のデータコピーやダウンロード等，不審な操作・アクセスの検知
・複数拠点での同時利用（同一アカウントでの東京と大阪の同時利用）などの不正検知

CASB が提供する機能として「可視化」「脅威防御」「コンプライアンス」「データ保護」の四つがガートナー社によって提唱されているが，これらの機能は CASB 特有のものではなく，「次世代セキュアファイアウォール」や「Secure Web Gateway」などにおいても同様な機能を提供しているものもある．上記の目的を実現するためのアプローチとして，CASB のみがもつ機能は CASB で実装し，利用情報の収集や遮断といった機能は，クラウド Proxy を通過するトラフィックからの情報を CASB および SIEM に連携・収集し，分析した結果を基に必要に応じてクラウド Proxy で通信を遮断する方針とした．昨今機能重複が見受けられる CASB とクラウド Proxy の設計実装の負荷を回避するためである．

3.3　エンドポイントセキュリティ

従来，社内ネットワークという守られた境界内で利用することが中心であった OA 環境が，テレワークやクラウドシフトにより境界外部に広がっていることを前述した．また「ゼロトラスト」の概念ではネットワークは信頼できないものとされ，インターネットを中心としたネットワークアクセスの仕組みが中核となる状況において，エンドポイントのセキュリティ対策や強化を図ることは重要である．

エンドポイントから直接インターネットを経由し，クラウドサービス上の情報資産へアクセスする方式においては，従来の社内ネットワークに設置されたセキュリティ製品によるセキュリティ対策では賄いきれない．これらのエンドポイント自体を脅威から守る方策は，Zero Trust eXtended（ZTX）では，ワークロードセキュリティやデバイスセキュリティ（EPP[*6] や EDR[*7]）の領域である．現在急速に拡大しているテレワークでは多くの PC が自宅インターネット回線でサイバー攻撃にさらされるリスクが増えており，エンドポイント保護強化の観点はゼロトラスト整備のリスク低減策の一環として重要となる．

日本ユニシスグループでは，3.2 節で挙げた五つの施策実施より前からエンドポイント対策を実施（EPP 製品を適用）していたが，この EPP 製品をクラウド対応版にアップデートし，社内・社外からのアクセスを問わずエンドポイント保護ができるよう対応している．

4. ゼロトラストモデルの適用ポイント

本章では，セキュリティ基盤更改時に考慮すべきポイントを紹介する．

4.1 セキュリティリスクの認識

セキュリティ基盤を更改するにあたり，自社の環境に内在するセキュリティリスクを事前に正確に認識し，セキュリティリスクに応じた対応策と優先順位を検討のうえ，環境にあったセキュリティ基盤を構築することが重要である．一般的に内在するセキュリティリスクの例を図9に，抽出したセキュリティリスクから検討した対応策と施策の例を表3に示す．

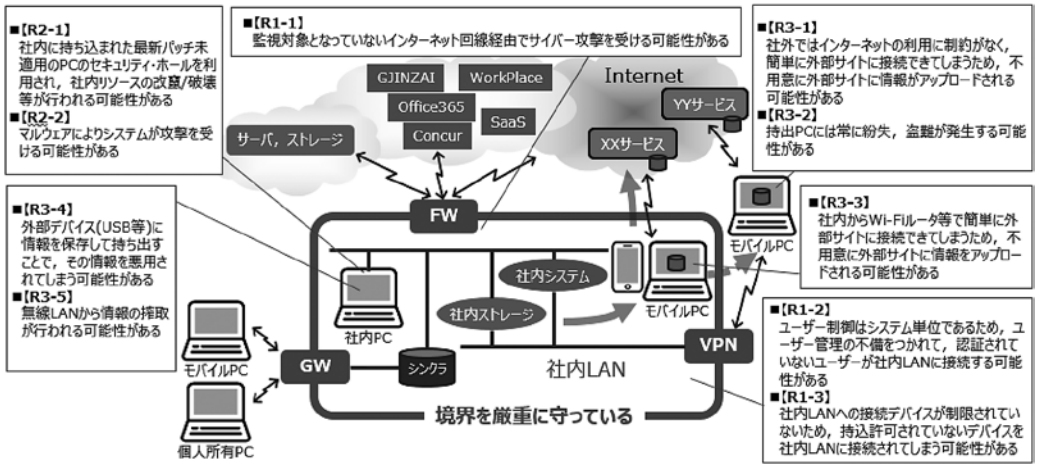

図9　一般的なセキュリティリスク例

表3　想定される事態と対応例

想定される事態		視点	セキュリティ基盤の施策概要	
R1-1	監視対象となっていないインターネット回線経由でサイバー攻撃を受ける可能性がある	ネットワーク	・社内外のデバイスの全ての通信をクラウドProxy経由とすることで，社内のシステムを非公開とし，不正なユーザーからのアクセスを防止する	クラウドProxy
R1-2	認証されていないユーザーが社内LANに接続する可能性がある	利用者	・セキュリティ対策の基本となる認証情報を統合，一元管理する ・認証レベルの向上（多要素認証の採用等）を可能とする ・SSO環境を実現することでセキュリティを強化するだけでなく，ユーザーの利便性も向上させる	ID管理/認証
		ネットワーク	・デバイス起動後，最初にネットワークを利用する時にユーザー認証することで，以降は個々のユーザーに対してサイト/サービスへのアクセス制御等のセキュリティルールを適用する ・認証情報を基にユーザーに対してどのデバイスを利用しても統一したセキュリティルールを適用する	クラウドProxy
R1-3	持込許可されていないデバイスを社内LANに接続されてしまう可能性がある	デバイス	・デバイスを一元管理し，対象外のデバイスから社内のリソースにアクセスできないようにする ・デバイスの接続時に検疫を行い，会社の指定するポリシー（安全性）が適用されていることを確認する	デバイス管理

想定される事態		視点	セキュリティ基盤の施策概要	
R2-1	最新パッチ未適用のPCのセキュリティ・ホールを利用され，改竄/破壊等が行われる可能性がある	デバイス	・デバイスを一元管理し，最新のパッチが適用されていないデバイスは利用できないようにするとともに，最新のパッチを強制的に適用する	デバイス管理

こうしたセキュリティリスクの抽出とセキュリティ基盤への要求事項の検討・施策化により，対応すべき範囲と実施アプローチを計画する．自社が置かれた状況によっては，全体的（広範囲）に包括したアプローチをする場合や対象範囲が見定められる場合には，サービス/製品を組み合わせて範囲を絞ってアプローチできる．優先順位付けは，セキュリティ被害を受けるリスクが高いものから優先して実施するなどが考えられる．

4.2　ソリューション選定の基準整備

日本ユニシスグループのサイバーセキュリティ戦略で掲げた施策の一つ「システム施策 / 社内システム」において“社内システムで外部クラウドサービスを利用すること，働く場所が変化すること，多様なビジネスパートナーと密接に連携すること”などの目標を掲げていることを前の章で紹介した．このセキュリティ基盤の実現に向けたクラウドサービスの選定においては以下のような基準を定義した．

1）ビジネス戦略との整合性
- ・自社のビジネス戦略に合致しているか
- ・自社の顧客へ提案・販売できるか

2）市場の評価
- ・第三者評価機関（Gartner Magic Quadrant 等）の評価はどのようになっているか

3）導入実績
- ・豊富な導入実績があるか
- ・同業他社における採用状況，評価はどのようなものか

4）導入/運用コスト
- ・該当製品分野の他製品/サービスと比較して優位性があるか

5）製品サポート/安定性/継続性
- ・長期間の利用に耐えうるサポート体制や能力を該当製品/サービスベンダーは持っているか

6）セキュリティ基盤を構成する他の選定製品/サービスとの親和性
- ・他製品/サービスとの連携機能を有しているか
- ・連携による機能強化が可能か

セキュリティ要求事項を整理し，要求事項に応じたソリューション（またはその組み合わせ）によりセキュリティ基盤を構築する際に，多くのセキュリティベンダーが自社製品の有効性をアピールしていることに加え，製品ごとに機能範囲が異なることや機能重複（例：SWG[*5] とCASB[*9]）が見られるなど，どの製品を採用するかを思い悩むことが多い．そのため，ソリュー

ション選定においては，自社の要求や選定基準を明確に定義し，選定したソリューションをPoC（Proof of Concept：概念実証）により評価するべきである．また，セキュリティ要求事項単体ではなくセキュリティ基盤全体で俯瞰した検討が重要になる．

4. 3　PoC（Proof of Concept）の実施

セキュリティ要求事項に対して，とりうる対策の実現性と効果を検証したうえで“投資判断”に向かうことが重要である．日本ユニシスグループでは，前節で紹介した選定基準に従い採用候補としたクラウドサービスに対して，基本機能および要件適合性を検証している．検証は「ID 管理/認証」「デバイス」「ネットワーク」の三つの視点で実施した．採用に至ったクラウドサービスの名称は伏せるが，評価結果の一部を抜粋して紹介する．

1）ID 管理/認証

基礎となる ID 管理機能，認証，これらを実装する構成が問題なく機能することを確認でき（表 4），ID 管理として選定した製品は認証だけでなく，デバイスへのポリシー設定もできることから，競合製品と比較して優位であると結論付けた．

2）デバイス

PC，iPhone 等の会社貸与デバイスを一元管理できること，各デバイスごとにポリシー設定ができること，「いつでも，どこでもクラウドサービスを安全に利用」できることを確認できた（表 5）．MDM として選定した製品は，選定した ID 管理との親和性と対応するデバイスの種類に関して他製品より優位であると結論付けた．

3）ネットワーク

クラウド Proxy を用いることで，社内からのアクセス時と同様に社外からのアクセス時も危険性の高い Web サイトへのアクセス制御ができることを確認できた（表 6）．クラウド Proxy として選定した製品のプロキシ機能は，優位性が広く世間に認められており，セキュリティ基盤を構成する他製品/他サービスとの連携と協調動作も確認できた．

表 4　PoC 評価結果抜粋（ID 管理/認証）

PoC 実施内容		対応するリスク（想定される事態）	PoC で確認した事項	結　果
①利用者	認証連携機能検証	R1-2　未認証ユーザーの社内 LAN 接続	認証：認証連携の機能を確認する（SSO の実現範囲の確認）	クラウド Proxy 経由の SSO で（製品名割愛）が利用可能
			許可：利用者単位に認可範囲を定め，その認可によるアクセス範囲の適正化を確認する	利用者の種別（従業員，準委任・請負）に応じて利用するアプリケーションを選別可能
			BCP 対策：認証，認可の仕組みの堅牢性，可用性の確認	オンプレ AD と（製品名割愛）が同期し，利用形態に応じた認証が可能
			認証：SSO 実現範囲を確認	社内/社外から SSO で 0365/Box が利用可能

表 5　PoC 評価結果抜粋（デバイス）

PoC 実施内容		対応するリスク（想定される事態）		PoC で確認した事項	結　果
②デバイス	デバイス管理機能検証 MDM ＋バックアップソフトウェア	R1-3	未許可デバイスの社内 LAN 接続	利用を許可されたデバイスを把握する 未許可デバイスの排除，施策の完全性を確認する台帳の作成	利用許可デバイスは（製品名割愛）に参加可能 未許可デバイスは（製品名割愛）に参加不可
		R2-1	PC のセキュリティ・ホールをついた攻撃	デバイスの各種インターフェースの制御（USB メモリの利用など）	（製品名割愛）によりデバイスが制御可能
		R3-2	持出 PC の紛失/盗難	デバイスの接続時検疫 会社の指定するポリシー（安全性）を接続時に確認する	（製品名割愛）によりデバイスごとにポリシー設定可能
		R3-4	USB 等外部デバイスによる情報持出	デバイス上データバックアップやリモート削除，運用性の確認	（製品名割愛）でバックアップ，リモートワイプ可能
				個人利用機器の使用を許容できるかどうかを確認する（PC 上のユーザー単位の制御等の確認）	（製品名割愛）によりデバイスが制御できることを確認

表 6　PoC 評価結果抜粋（ネットワーク）

PoC 実施内容		対応するリスク（想定される事態）		PoC で確認した事項	結　果
③ネットワーク	クラウド Proxy/CASB 基本機能及び要件適合性検証	R1-1	監視対象外ネットワークからの攻撃	CASB を用いた安全性の確認と運用	（製品名割愛）連携でセキュリティリスク高のサイトへのアクセスを検出・制限可能
		R1-2	未認証ユーザーの社内 LAN 接続	ログ採取集中管理による異常検知の検証	（製品名割愛）でログ集中管理が可能
		R1-3	未許可デバイスの社内 LAN 接続	利用される情報のトレーサビリティの検証	（製品名割愛）連携でセキュリティリスク高のサイトへのアクセスを検出可能
		R3-1	社外からの不正サイトへのアクセス	モバイル利用時においても不適切なサイトの利用制御検証	社内/社外から（製品名割愛）経由でクラウドサービス利用が適切にアクセス制御可能
		R3-3	社内からの不正サイトへのアクセス	PSOC 活動で必要な情報を得られることの検証	（製品名割愛）でログ集中管理が可能

4. 4　分散型運用体制の整備

セキュリティ基盤の再構成により，ネットワーク境界に設置されているネットワーク機器のログに加え，クラウドアプリケーションのログも監視対象となることから，セキュリティ監視業務の負荷が増えると想定される．セキュリティ監視対象が増えるにつれ，監視対象範囲の設計とともに，運用体制の再整備が望まれる．この対応として，専門性を要するセキュリティ監視業務とそれ以外の監視業務の実行組織を分離し，運用組織間でクラウド SIEM を共用することにより運用負荷の一極集中を減らす「分散型インフラ・セキュリティ運用体制」の整備を検討した．現行運用の関連組織を踏まえ，機能単位に 5 分割することを想定し，表 7 のような運用体制を整備中である．

表 7　分散型インフラ・セキュリティ運用体制案

#	運用機能の名称	役　　割	SIEM 共用	実行組織の案
1	インフラ運用全体統括	・ITIL 等の標準をベースにインフラ・セキュリティ運用管理の全体統制を図る	△	自社 IT 部門
2	ネットワークセキュリティ監視	・オンプレミスのインターネット境界に加えて，CSEC のクラウドセキュティサービス（クラウド Proxy，CASB）の運用監視を統合する ・ログ基盤はクラウド SIEM を共用（主担当）する	○	PSOC
3	エンドポイントセキュリティ運用監視	・エンドポイントセキュリティの運用監視を統合する ・MDM についてはログ基盤はクラウド SIEM を共用する	○	外部委託
4	クラウドアプリケーション運用監視	・新設．全社で利用するクラウドアプリケーションの運用監視を統合する ・（Office365，Box，Zoom 等）ログ基盤はクラウド SIEM を共用する	○	外部委託
5	ディレクトリ運用監視	・認証情報を格納するディレクトリサービスの運用監視を統合する ・ログ基盤はクラウド SIEM を共用する	○	自社 IT 部門

5. お　わ　り　に

サイバー空間の安全性の確保やセキュリティ対策への取り組みは，企業にとって重要な経営課題となってきている．また，今後も世の中は目まぐるしく変化していくことに疑いの余地はなく，引き続き多様な変化に追随できる仕組みや体制の構築が求められる．ゼロトラストモデルを適用したセキュリティ基盤更改という日本ユニシスグループの事例が少しでも参考となれば幸いである．このセキュリティ基盤更改の取り組みは，多数の関連部署にご協力いただき実施している．最後にこの場を借りて全ての関係各位に深く感謝申し上げる．

＊ 1　DLP（Data Loss Prevention）　機密情報や重要データなどの送信やコピーを制限し，紛失や外部への漏洩を防ぐシステム．

＊ 2　IAM（Identity and Access Management）　企業の情報資産へのアクセスに際し，適切なユーザーだけを適切なデータやアプリケーションにアクセスさせるために，ID とアクセスを管理する仕組み．

＊ 3　CWPP（Cloud Workload Protection Platform）　IaaS 上の仮想マシンやコンテナなどクラウド・ワークロードの監視と保護を行うための仕組み．

＊ 4　CSPM（Cloud Security Posture Management）　IaaS や PaaS といったパブリッククラウドに対し，API 連携によってクラウド側の設定を自動的に参照し，セキュリティ設定ミスやガイドラインの違反などがないかを一元的かつ継続的に確認する仕組み．

＊ 5　SWG（Secure Web Gateway）　Web アクセスをセキュアにするゲートウェイ機能．従来のプロキシに URL フィルタやアンチウイルス，サンドボックスなど，よりセキュアな機能を追加しクラウド型で提供する仕組み．

＊ 6　EPP（Endpoint Protection Platform）　マルウェア感染を防止することに特化し，組織内に侵入したマルウェアの検知と自動駆除など，マルウェアが実行されないようにする仕組み．

＊ 7　EDR（Endpoint Detection and Response）　マルウェアの感染防止を目的とする EPP とは異なり，標的型攻撃やランサムウェアなどによる攻撃を検出して対応するために使用するエンドポイントの監視を強化するための仕組み．

＊ 8　MDM（Mobile Device Management）　スマートフォンなどの携帯端末を業務で利用する際に，端末へのセキュリティポリシーやアプリケーションの配布や管理，アプリケーションや機能の利用制限等の一元的な管理のための仕組み．

＊9　CASB（Cloud Access Service Broker）　利用者（企業）と複数のクラウドプロバイダーの間に単一のポイントを設けることで，クラウドサービス利用状況の可視化や制御，一貫性のあるセキュリティポリシーの適用をする仕組み．

＊10　SIEM（Security Information Event Management）　情報システムを構成する様々な機器やソフトウェアの動作状況の記録（ログ）を一元的に蓄積・管理し，保安上の脅威となる事象をいち早く検知・分析するための仕組み．

＊11　SOAR（Security Orchestration and Automation Response）　セキュリティ脅威と脆弱性の管理やセキュリティインシデント対応，セキュリティ運用の自動化を行う三つの構成要素により構成され，セキュリティ運用の自動化と効率化を実現する仕組み．

＊12　MAM（Mobile Application Management）　スマートフォンなどの携帯端末を業務で利用する際にスマートフォンのシステム設定を企業側で一元的に管理し，利用する機能に制限をかけるなどの手法を実現させる仕組み．

＊13　フル・トンネル方式．データ送信者と受信者の間に仮想的なトンネルを作り（トンネリング）暗号化通信を行う VPN 接続の方式．すべての通信が VPN トンネルを通過することになる．

＊14　スプリット・トンネル方式．VPN 接続先（例：自社の社内 LAN）へは，VPN トンネルで通信し，インターネットへの通信は VPN トンネルを介さず，直接インターネットへ通信させる方式．

参考文献

［1］ NIST Special Publication 800-207 Zero Trust Architecture (Final) https://csrc.nist.gov/publications/detail/sp/800-207/final（2021.01.13 確認）

［2］ John Kindervag, Stephanie Balaouras, Kelley Mak, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture”, Forrester Research, Inc., November 15, 2012 https://www.forrester.com/report/Build+Security+Into+Your+Networks+DNA+The+Zero+Trust+Network+Architecture/-/E-RES57047#（2021.01.13 確認）

［3］ Chase Cunningham, Joseph Blankenship, Alexis Bouffard, Peggy Dostie, “The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020”, Forrester Research, Inc., September 24, 2020 https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+Ecosystem+Platform+Providers+Q3+2020/-/E-RES157494（2021.01.13 確認）

［4］ 澤田　雅広，「日本ユニシスグループのサイバーセキュリティ戦略」，ユニシス技報，日本ユニシス，Vol.39 No.2，通巻 141 号，2019 年 9 月

［5］ 石黒　怜，木埜　由紀子「サイバー脅威を検知するセキュリティ・オペレーション・センター」，ユニシス技報，日本ユニシス，Vol.39 No.2，通巻 141 号，2019 年 9 月

［6］ Cloud Access Security Brokers (CASBs), Information Technology Gartner Glossary https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs（2021.01.13 確認）

執筆者紹介

岡　本　宏　之（Hiroyuki Okamoto）

1992 年日本ユニシス・ソフトウェア(株)入社．公共系システム開発に従事．（2015 年日本ユニシス(株)に合併 ユニアデックス(株)に出向）．クラウドサービス，仮想化基盤のプリセールスに従事．2019 年より情報システムサービス部に異動，現職．

増　井　博　行（Hiroyuki Masui）

1985年日本ユニシス(株)入社，金融機関向けシステムの開発，保守を担当．サービス商品開発，運営業務を経て2016年より情報システムサービス部にて社内情報システムの企画業務に従事，現職．