ゼロトラストの次に目指すところ ――経営と現場をつなぐ「サイバーセキュリティー・メッシュアーキテクチャー」

佐　藤　大　介

要　約　サイバーセキュリティーは、境界型からゼロトラストへと進化した。次に目指すべきは、分散するセキュリティー対策の統合プラットフォーム戦略である「サイバーセキュリティー・メッシュアーキテクチャー」である。これにより、セキュリティーの有効性向上、中央制御、強固な本人確認、運用と監視の集約が実現される。本稿では、増え続けるセキュリティーツールの網羅ではなく、守るべき七つの領域を網羅することで、今後のサイバーセキュリティー戦略の理想形を提言する。これからは AI がセキュリティーにおける防御と攻撃両方の基準を上げる。ゼロトラストの踏襲が AI 中心の未来に通用する保証はない。ゼロトラストの次にサイバーセキュリティー・メッシュアーキテクチャーを目指すべきである。

1. はじめに

セキュリティーの重要性を口にしない経営者は、まずいないだろう。一方で、セキュリティーへの支出は、重要な投資か、それとも必要な経費か、経営者の意見は分かれる。将来の収益を左右する DX やデジタルビジネスをセキュリティーが支えると考えれば、セキュリティーへの支出は経営目標の実現に必要な戦略的経費である。

サイバーセキュリティーは、境界型からゼロトラストへと進化した。次に目指すべきは、分散するセキュリティー対策の統合プラットフォーム戦略である「サイバーセキュリティー・メッシュアーキテクチャー」である。これにより、セキュリティーの有効性向上、中央制御、強固な本人確認、運用と監視の集約が実現される。

本稿では、ユニアデックス株式会社（以下、ユニアデックス）がゼロトラストの次に目指す戦略「サイバーセキュリティー・メッシュアーキテクチャー」について解説する。ゼロトラストの次を示すことで、サイバーセキュリティー管理態勢の構築に今まで以上に向き合う経営陣やセキュリティー人材を自発的に志す仲間が増えることを願っている。

2 章でセキュリティーの変遷とゼロトラストの課題に触れ、3 章でサイバーセキュリティー・メッシュアーキテクチャーを紹介し、4 章で AI とセキュリティー運用の未来について述べつつ、サイバーセキュリティーに関する提言を試みる。

2. セキュリティーの変遷とゼロトラストの課題

2.1 節でセキュリティーの変遷、2.2 節でゼロトラストの課題について記述する。

2.1 セキュリティーの変遷

以前のサイバー空間におけるセキュリティーは、ファイアーウォールや VPN 装置といった境界型防御を代表するデバイスに支えられてきた。今なお、これらのデバイスはサイバー空間

で多数稼働しており、セキュリティービジネスの中で大きな市場を形成している。

ユニアデックスは、境界型防御が全盛の時代に、5G が今後の企業 LAN に取って代わりクラウド上で業務を行う企業が増える未来を予見し、クラウドセキュリティーソリューション群を包括的に提供する「CloudPas[1]」を 2019 年 10 月にリリースした。この予見は思わぬ形で現実のものとなった。CloudPas リリース直後の 2019 年 12 月に始まったパンデミック「新型コロナウイルス感染症の世界的流行」である。このコロナ禍を境に、人々は行動が制限された中で業務を継続するため、クラウド中心で働くようになった。世界中で、社外はもちろん社内もすべてを信用しないセキュリティーの考え方である「ゼロトラスト」へのシフトが一気に加速していった。

世界保健機構（WHO）は、2020 年 1 月に新型コロナウイルスに関する「国際的に懸念される公衆衛生上の緊急事態」を宣言し、2023 年 5 月に同宣言の終了を発表した。コロナ禍は終息したが、ゼロトラストは今も数多くの組織の業務を支えている。

そして、2024 年 2 月にユニアデックスは、ゼロトラストの次に目指すべき「サイバーセキュリティー・メッシュアーキテクチャー（CSMA）構想[2]」を公表した（3 章で説明）。サイバーセキュリティーは、境界型からゼロトラストへ、そしてこれからはサイバーセキュリティ・メッシュアーキテクチャーへと変遷していく（図 1）。

図 1　セキュリティーの変遷

2. 2　ゼロトラストの課題

セキュリティーの変遷を踏まえると、ゼロトラストの課題が見えてくる。従来の境界型防御の時代は、ファイアーウォールの内側に情報資産を配置することでセキュリティーを確保してきた。ゼロトラストの時代に入ってからは、情報資産がファイアーウォールの外側にも配置されるようになった。クラウドの利用拡大や IoT デバイスの普及など、働く環境が変化したためである。それにより、セキュリティー確保の方法も大きく変わることとなった。

ランサムウエアに代表されるマルウエアが巧妙にファイアーウォールの内側へ侵入することも、境界型防御の全盛期には危険とされたファイアーウォールの外側でのリモートワークも、

今では日常的なこととして捉えるべきである。そのため、企業は内側も外側も信用しないゼロトラストの概念を持ち込まざるを得なくなった。ゼロトラストを前提とした環境は、図2に示す通りである。

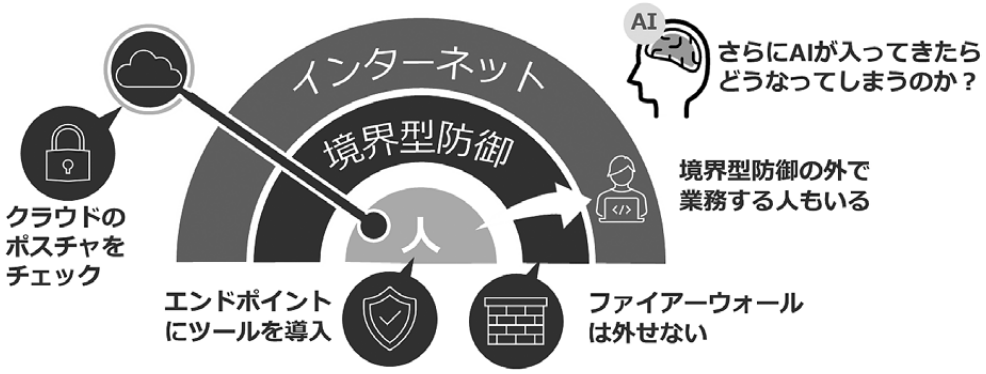

図2　ゼロトラスト環境

ゼロトラスト環境では、ファイアーウォールの内側にも外側にも配置される情報資産を守るため、セキュリティーツールも分散配置される。

分散配置されたセキュリティーツールの運用者は疲弊している。例えば、たった一つの設定ミスでクラウド上の内部情報が外部に漏えいし、たった1カ所の内部への侵入が取り返しのつかない被害に拡大する。重要な何かを見逃していないか、常に神経を擦り減らしている運用者は多い。

攻撃者が運用者の疲弊を認識していることが、よりリスクを高める。セキュリティーアラートに疲れた運用者の隙を突いて、攻撃を仕掛けてくる。さらにAIが攻撃を高度化させたら、セキュリティー運用者が疲弊する状況はますます悪化する。セキュリティーツールが正しく運用されていれば多くのセキュリティー被害は防げるはずである。しかし実際には、セキュリティー運用者が疲弊し、それが正しい運用を妨げる一因となっている。

ゼロトラストの課題は、情報資産が分散配置されることにより、セキュリティー運用者の疲弊が大きくなったことと、組織に導入されたセキュリティーツールが正しく運用されず、被害が減らないことである。

3.　サイバーセキュリティー・メッシュアーキテクチャー

本章では、戦術と戦略の違いを述べた後、ユニアデックスの目指す戦略であるサイバーセキュリティー・メッシュアーキテクチャーの概要について説明する。

3.1　戦術と戦略

戦術は、英語にすると「タクティクス（tactics）」である。戦術とは、持っている戦闘力を運用する術のことである。セキュリティーツールという戦闘力を持っていたら、それを運用して、内外の攻撃者にどう打ち勝つか、これが戦術である。戦術は、現在の戦いに勝利するためにある。

一方、戦略は、英語にすると「ストラテジー（strategy）」である。戦略とは、特定の目的

を達成するために長期的視野で力や資源を総合的に運用することである。すでに持っているセキュリティーツールで十分か、人員やルールは今のままでよいか、より盤石なセキュリティーを確保するにはどうすべきか、将来のリスクを見越して戦術が実行できる状態を整える、これが戦略である。戦略は、未来の戦いに勝利するためにある。

戦略が組織内で共有されると、部門間のセクショナリズムを超えて、馴れ合いとは異なる「一体感」が生まれる。戦略なき一体感は、時に曖昧な関係性を生み、いざという時の結束力に欠ける。一方、戦略を共有し、同じ方向を向いて行動できる一体感のある組織は、まず情報交換の大切さをお互い認識している。そして、各部門がそれぞれの戦術を実行しながらも、セキュリティーインシデント発生時には強い結束力を発揮する（図3）。

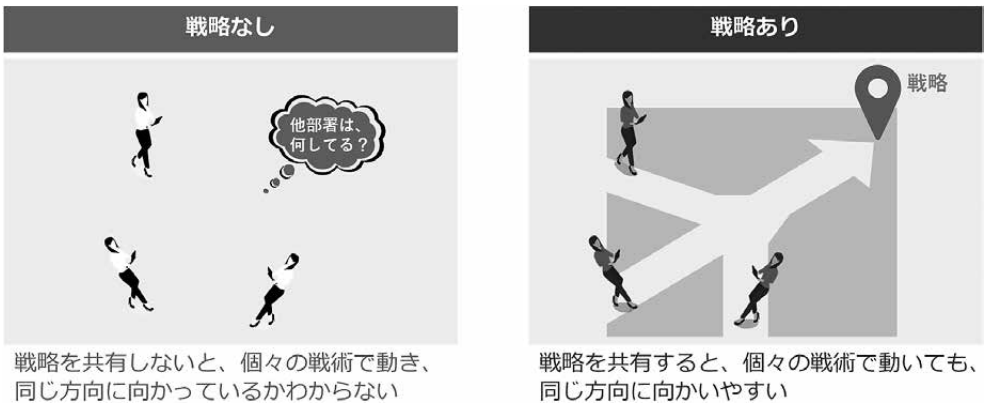

図3　戦略の有無と一体感

3.2　サイバーセキュリティー・メッシュアーキテクチャーとは？

サイバーセキュリティー・メッシュアーキテクチャーは、戦術ではなく戦略である。サイバーセキュリティー・メッシュアーキテクチャーへの支出は、将来的なデジタルビジネスの収益を左右し得る戦略的経費と言うことができる。

3.2.1　サイバーセキュリティー・メッシュアーキテクチャーの四つのポイント

ユニアデックスでは、サイバーセキュリティー・メッシュアーキテクチャーを「分散するサイバーセキュリティー対策の統合プラットフォーム戦略」と定義し、ポイントを四つ挙げている（表1）。

表1　サイバーセキュリティー・メッシュアーキテクチャーの四つのポイント

#	ポイント	概　　要
①	セキュリティーの有効性向上	セキュリティーツール全体の有効性を向上させる
②	分散するセキュリティーを制御	分散型セキュリティー・コントロールを構築する新たなアプローチ
③	機能の集中と共通基盤による強固な本人確認	分析、実行など機能の集中化、共通のアイデンティティ・ファブリック
④	セキュリティー運用と監視の集約	安全かつ集中的なセキュリティー運用と監視を実現できる

①「セキュリティーの有効性向上」とは、セキュリティーツールをただ導入すればよいわけではなく、日々有効性の維持と向上に努めることを指している。セキュリティーツールを導入しただけで安心してしまった組織から情報漏えいするケースは少なくない。

②「分散するセキュリティーを制御」とは、ゼロトラストの課題で述べた通り、セキュリティーツールが分散状態であるからこそ、それらを中央で制御する新たなアプローチが不可欠であることを指している。

③「機能の集中と共通基盤による強固な本人確認」とは、分析などの機能を集中させることに加え、特にゼロトラストでは重要とされる「本人確認」を共通のアイデンティティ・ファブリック、つまり共通認証基盤で行うことを指している。

④「セキュリティー運用と監視の集約」とは、セキュリティー運用に加え、セキュリティー監視を集約することを指している。

3. 2. 2　サイバーセキュリティー・メッシュアーキテクチャーの構成要素

ユニアデックスのサイバーセキュティー・メッシュアーキテクチャー戦略は、Network から Application まで、守るべき七つの領域にサイバーセキュリティー対策が張り巡らされた、網羅的で包括的な戦略である。その中でも、セキュリティーログの統合に役立つ XDR、リスクに晒された IT 資産の様々な脆弱性、つまりエクスポージャーを管理する CTEM をサイバーセキュリティー・メッシュアーキテクチャーの重要なツールと位置付けている（図 4）。

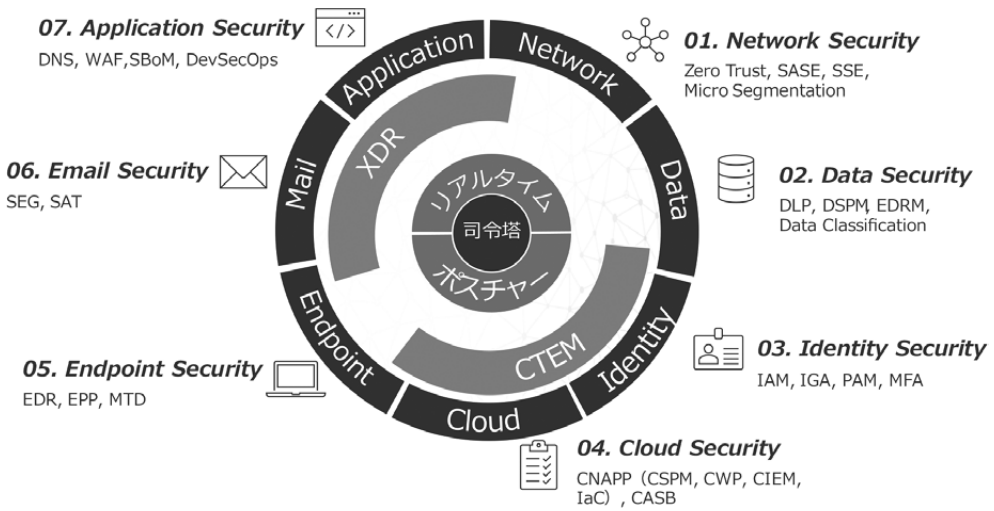

図 4　ユニアデックスのサイバーセキュリティー・メッシュアーキテクチャー戦略

司令塔の役割は、セキュリティーインシデントの発生前後でポスチャーとリアルタイムに分けられる。ポスチャーは、セキュリティーインシデント発生前の平時において、主に CTEM を駆使して、組織のダメージの発生を未然に防ぐ司令塔である。リアルタイムは、セキュリティーインシデント発生後の有事において、主に XDR を駆使して、組織のダメージを制御する司令塔である。ユニアデックスは、これらを包括するマネージドセキュリティーサービスを提供する。

例えば、従業員の端末でセキュリティーアラートが上がった場合、多くの組織がランサムウ

エアなどの侵入の形跡を調査する。並行して、データを外に持ち出された形跡があるかどうかネットワークを調査する。調査すべきポイントが多いほどセキュリティー運用者は疲弊する。

サイバーセキュリティー・メッシュアーキテクチャー戦略は、調査すべきポイントを大幅に削減し、セキュリティー運用者の疲弊を緩和し、セキュリティーツールが正しく運用される状態を目指している。セキュリティーツールが正しく運用されれば、セキュリティーインシデント発生後の組織のダメージを大幅に減らすことができる。

次に、サイバーセキュリティー・メッシュアーキテクチャーを構成する各要素を表2に列挙する。なお、これらはいくつかの要素を組み合せて、用途に合わせた段階的・部分的な導入にも対応できる。

表2　サイバーセキュリティー・メッシュアーキテクチャーの構成要素

#	分　類	概　　要
01	Network Security	ゼロトラストの代表的な要素であるSASE/SSEや今後重要性を増すマイクロセグメンテーションなどが含まれ、ネットワーク上でできるセキュリティー対策全般を指す。
02	Data Security	ゼロトラストの要素であるDLPやAI時代に重要性を増すDSPMなどが含まれ、データに関するセキュリティー対策全般を指す。
03	Identity Security	ゼロトラストの重要な要素であるIAMや特権アカウントの権限管理を行うPAMなどが含まれ、認証・本人確認に関するセキュリティー対策全般を指す。
04	Cloud Security	ゼロトラストの代表的な要素であるCSPM・CWPP・CIEM・IaCを包含するCNAPPやコンテナ保護などが含まれ、クラウドの設定や権限の不備・ワークロードの保護などのセキュリティー対策全般を指す。
05	Endpoint Security	ゼロトラストの重要な要素であるEDRやスマートデバイスを保護するMTDなどが含まれ、エンドポイントに関するセキュリティー対策全般を指す。
06	Email Security	標的型攻撃メールやビジネスメール詐欺などメールを利用した攻撃へのセキュリティー対策全般を指す。メール訓練・アウェアネストレーニングなども含む。
07	Application Security	DNSファイアーウォールやWAFなどアプリケーションへの攻撃に効果的なセキュリティー対策全般を指す。SBoMやDevSecOpsなども含む。
—	XDR（Extended Detection and Response）	EDRやファイアーウォールなど複数システムに記録されるログ・テレメトリーデータの集約と相関分析を行い、サイバー脅威の検出やインシデント発生時の事後対処を支援するセキュリティーツールのこと。
—	CTEM（Continuous Threat Exposure Management）	サイバー脅威に晒されたIT資産全般の脆弱度を継続的にチェックし、リスク状況の確認やインシデント発生前の予防を支援するセキュリティーツールのこと。IT資産全般はパソコン、サーバー、ネットワークからクラウドまで含む。
—	ポスチャー	セキュリティーインシデント発生防止のために、システムが正しい状態を維持できていることを主体的に確認する司令塔のこと。セキュリティー運用・監視機能を有する。
—	リアルタイム	セキュリティーインシデント発生に伴い、リアルタイムかつ主体的に対応する司令塔のこと。インシデントレスポンス機能を有する。

3.3　サイバーセキュリティー・メッシュアーキテクチャーの意義

サイバーセキュリティー・メッシュアーキテクチャーは、組織にとってどのような意義があるか、本章で述べた内容を基に整理する。

セキュリティー運用者は、統合プラットフォームにより調査すべきポイントが大幅に削減され、疲弊を軽減できると述べた。また、セキュリティーツールが正しく運用されれば、セキュリティーインシデント発生後の組織のダメージを大幅に軽減できるとも述べた。組織のダメージ軽減は、業務を停止させず、経営目標を達成するうえで極めて重要である。

また、サイバーセキュリティー管理態勢を強化するためには、経営と現場が共通の戦略目標を持つことが重要である。共通の戦略目標を持つことで、経営と現場のコミュニケーションが円滑になり、それが大きな意義を持つ。

組織において、セキュリティーの現場責任者と経営とのコミュニケーションが円滑でなければ、セキュリティーの現場責任者はその役割を十分に果たすことが難しい。仮にセキュリティーリスクを感じる場面があっても、経営とのコミュニケーションが円滑でなければ、そのリスクが経営にうまく伝わらない。うまく伝わらなければ、経営がセキュリティーへの支出を承認することもなく、リスクは放置される。その結果、セキュリティーインシデントが発生する。

円滑なコミュニケーションこそが、組織のサイバーセキュリティー管理態勢の強化において極めて重要である。ゼロトラストが定着してきた今、次の戦略としてサイバーセキュリティー・メッシュアーキテクチャーを打ち出すことは、経営と現場が中長期的にコミュニケーションを図る場を提供することになる。その意義の大きさは計り知れない。

4.　AIとセキュリティー運用の未来

AIはあらゆる分野に入り込むと考えられており、セキュリティーも例外ではない。本章では、サイバーセキュリティー・メッシュアーキテクチャーが、AIとセキュリティー運用の未来にどうつながるのかを述べる。

4.1　AI

AIとセキュリティーの関係性を表す言葉に、AIのためのセキュリティー「Security for AI」とセキュリティーのためのAI「AI for Security」の二つがある。AIのためのセキュリティーは、AIそのものが攻撃者の標的になるケースやAIを介して機密情報が流出するケースなど、AIを取り巻く新たな脅威への対応が主である。セキュリティーのためのAIは、セキュリティーツールに組み込まれたAIが運用者を支援する機能の開発が主である。

その一方で、AIは攻撃者にも大きな影響を与える。攻撃者は一般的に、収入が労力を上回れば、その対象を攻撃する。AIは攻撃者の労力を抑える手段となっており、簡単、高速、高精度な無差別攻撃を低コストで実行できるようになった。そのため、これまで攻撃対象になりにくかった組織でも、収入が労力を上回りやすくなり、今後は標的とされるリスクが高まると予見される。AIを使った攻撃例を図5に示す。

図5　AIを使った攻撃例

フェイクニュースは、少しの真実を混ぜつつ偽物のメディアやコンテンツをAIに生成させ、人々を騙す攻撃である。高度なITを使わずに、人の心理やミスに付け込んで重要情報を窃取する攻撃をソーシャルエンジニアリングと呼ぶ。フェイクニュースはソーシャルエンジニアリング攻撃を高度化する。例えば、ゴーストアカウントやゾンビアカウントと呼ばれる長期間使われていないアカウントを乗っ取り、フェイクニュースをツイートして、真実と思い込ませ、攻撃対象を騙すことが考えられる。今後は、ランサムウエアなどに感染しなくても、フェイクニュースに騙された人たちが、攻撃者の欲しい重要情報を外部に漏えいさせるかもしれない。

4.2　セキュリティー運用の未来

現在のセキュリティー運用が、未来でも通用するとは限らない。例えば、リスクに晒されているIT資産のエクスポージャーを管理するCTEMは、日々発見される脆弱性が多過ぎる課題に対して、優先順位を付けるテクノロジーを実装している。1日に公開される脆弱性の数は、数十件を超えることも珍しくない[3]。組織によっては、現在のセキュリティー運用を踏襲して、決められた時期に脆弱性検査を実施しているかもしれないが、発見される脆弱性の数が年々増加する中で、定期的な脆弱性検査で足りるとは思えない。

AIはセキュリティーにおける防御と攻撃両方の基準を上げる。今年のセキュリティー運用を踏襲しても、来年通用しなくなるリスクは、より一層高まると予見される。

サイバーセキュリティー・メッシュアーキテクチャーは、「分散するサイバーセキュリティー対策の統合プラットフォーム戦略」と述べた。この統合プラットフォームは、テレメトリー*1やログのデータを集約し、AIと掛け合わせる未来への布石である。つまり、サイバーセキュリティー・メッシュアーキテクチャーは、すべてのセキュリティー従事者を支援するための戦略であり、人が主役のサイバーセキュリティー管理態勢を構築する構想である。

ゼロトラストに関連したセキュリティーツールは既存サービスを踏襲する時代を迎えている。しかし、ゼロトラストの踏襲がAI中心の未来に通用する保証はない。ゼロトラストの次にサイバーセキュリティー・メッシュアーキテクチャーを目指すべきであると提言する理由はここにある。

5. お わ り に

本稿を含め、セキュリティーに関して執筆する際は、できる限り易しい言葉遣いを心掛けている。その理由は、顧客システムの担当者からセキュリティーを敬遠するご発言を聞くことが少なくなく、このままでは日本のセキュリティーが発展しないと危惧しているからである。セキュリティー従事者の仲間を増やすため、今後も社内外で活動範囲を拡げていきたい。

最後に本稿を執筆する機会を与えてくれた関係者やご協力いただいた皆様に深く感謝を申し上げます。

＊1　テレメトリーとは、遠隔で収集するデータ。元は軍事上のインテリジェンスから来た用語。人に示唆や洞察を与えるためのデータとして過去の記録のログと使い分けられている。

参考文献　［1］「クラウド時代のセキュリティー」，ユニアデックス(株)，https://www.uniadex.co.jp/lp/zerotrust/
［2］「サイバーセキュリティー・メッシュ・アーキテクチャーとは？」，ユニアデックス(株)，https://www.uniadex.co.jp/column/annex-security/usefulinfo/csma.html
［3］ JVN iPedia 脆弱性対策情報データベース，独立行政法人 情報処理推進機構（IPA），https://jvndb.jvn.jp/

※　上記参考文献に記載の URL のリンク先は、2025 年 4 月 4 日時点での存在を確認。

執筆者紹介　佐　藤　大　介（Daisuke Sato）
2005 年ユニアデックス(株)（旧(株)ネットマークス）に入社。2018 年度までの約 14 年間金融担当の営業部門に在籍し、1 万台規模の IP 電話システムの全国展開案件等を多数経験。2019 年度よりセキュリティー関連のリサーチ業務や戦略立案業務に従事。2024 年に CISSP を取得。