ゼロトラストにおけるアクセス制御と可視化の重要性

岩竹智之

要　約　昨今、サイバー攻撃の高度化により重大な被害に遭う企業・団体が増加している。クラウドサービスの利用とテレワークの増加により、「安全な社内」と「危険な社外」を分ける境界型セキュリティーでは対応が困難になっている。そこで「全てを信用しない」を前提にした「ゼロトラスト」がセキュリティー対策のトレンドになっている。しかし、ゼロトラストを実現するための対策で見落とされがちな項目がある。それらを補う施策であるアクセス制御と攻撃の可視化については、現状と目標レベルのギャップを明確化し優先順位を持って実施しなければならない。対策は複数のソリューションの組み合わせ、すなわちアクセス制御を行う次世代リモートアクセスソリューションのZTNAと、ログを管理し攻撃を可視化するSIEM/EDR/SOAR/XDRが有効である。ユニアデックスはセキュリティー成熟度診断と統合クラウドセキュリティーソリューション「CloudPas®」を提供して顧客のゼロトラスト対策を支援している。

1. はじめに

サイバー攻撃がこれほどに活発化しているのは事業として成り立ってしまうからである。犯罪をいとわない組織にとっては、物理的に強盗に入るより低いリスクで、金銭を手に入れることが可能なため、効率の良い手段に見えるのだろう。バングラデシュ中央銀行のシステムにマルウエアが侵入し、不正送金によって1,000億円が窃取された事件[1]は衝撃であった。サイバー攻撃の多くはデータを人質にとる行為であり事業継続性を脅かす経営課題のひとつである。また反社会的な組織に資金が流れないように対策を打つことは社会的責任でもある。

ユニアデックス株式会社（以降、ユニアデックス）は高度化するサイバー攻撃からの被害を防ぐため、ゼロトラストアーキテクチャに基づいたセキュリティー対策ソリューションを提供している。それらの導入実績とセキュリティー成熟度診断結果の傾向から、顧客のセキュリティー対策における取り組みの濃淡が見えてくる。本稿では、そのような状況を読者に共有する。2章にて各種資料に基づく被害や対策の状況を示し、3章ではゼロトラストと可視化を紹介し、4章でアクセス制御ソリューション、5章でユニアデックスの取り組みについて述べる。

2. 被害状況

実際のマルウエアの活動状況を見てみる。図1は2022年4月20日のJPCERT/CCのマルウエア注意喚起情報[2]で報告された「Emotetに感染しメール送信に悪用される可能性のあるJPドメインのメールアドレス数」である。Emotetはマルウエアの一種で、不正なメールに添付され、ファイルを開くと感染するウイルスであり、2022年3月は2020年の感染ピーク時の5倍以上となっている。

また図2～図6は警察庁の資料「令和3年におけるサイバー空間をめぐる脅威の情勢等について」[3]から引用したデータである。まず図2から被害が顕著に増加しているのがわかる。

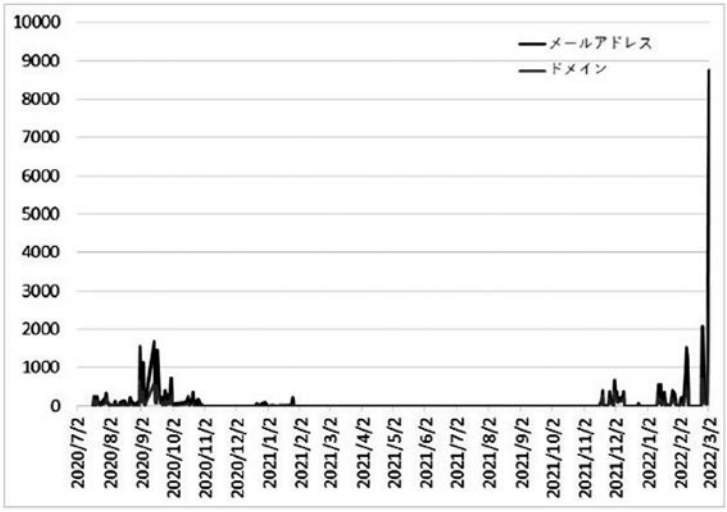

図 1　Emotet に感染しメール送信に悪用される可能性のある .jp メールアドレス数の新規観測の推移[2]

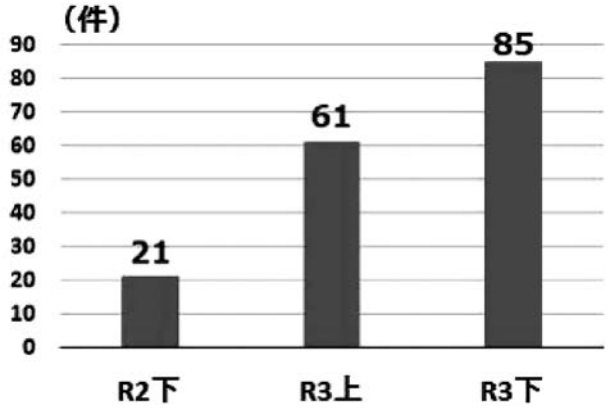

図 2　企業・団体等におけるランサムウエア被害の報告件数の推移

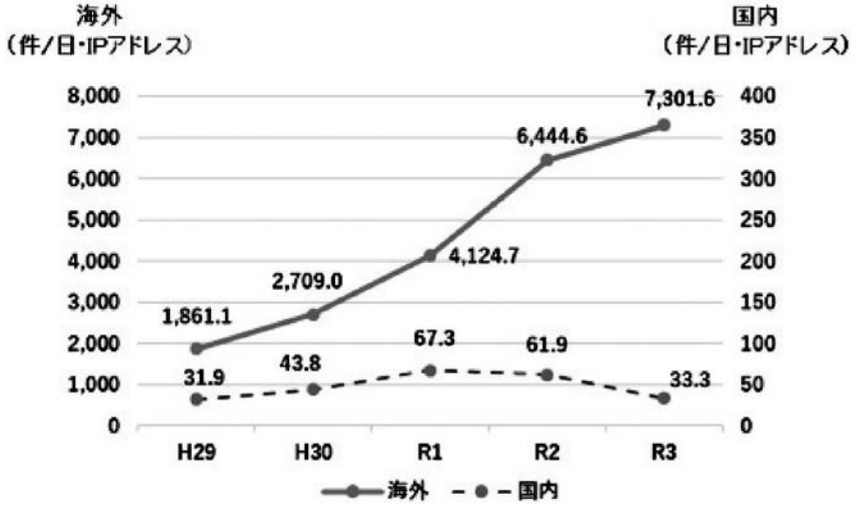

図 3　検出したアクセスの送信元で比較した 1 日・1IP アドレスあたり件数の推移

図３は同資料の「検知したアクセスの送信元で比較した１日・1IP アドレス当たり件数の推移」のグラフである。警察庁がインターネット上に設置したセンサーに対して送られてくる通信パケットを集計したアクセス数である。攻撃者によるインターネットに接続された各種機器の脆弱性の探索行為等の事象を表している。2021 年（令和３年）においては国内のアクセス数の減少がみられるものの海外からのアクセスが多くなっていることがわかる。これは犯罪をいとわない国際組織がサイバー攻撃を資金調達手段としていることと無縁ではないだろう。

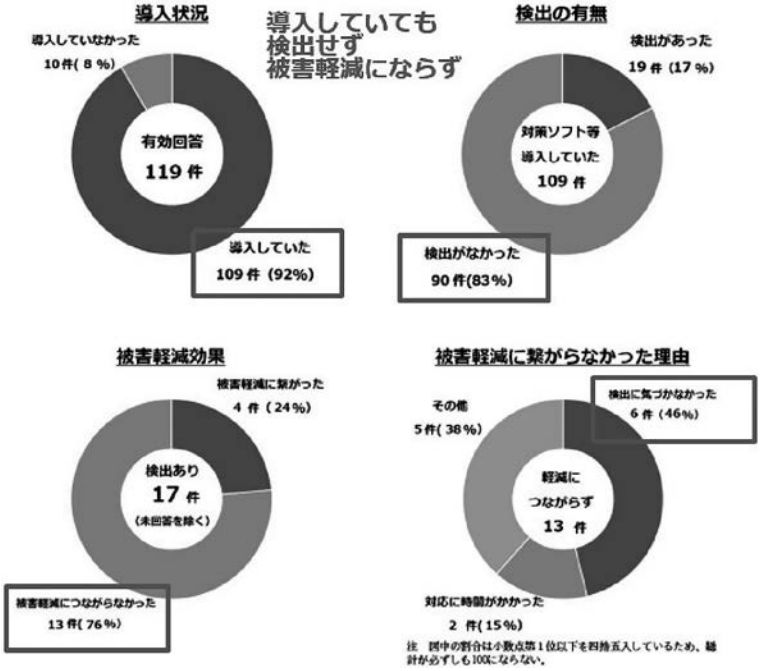

図４　被害企業・団体等のウイルス対策ソフト等の導入・活用状況

図４は被害企業・団体等のウイルス対策ソフト等の導入・活用状況である。被害にあった企業のデータから、ウイルス対策ソフトは導入されているものの、検出できず被害軽減につながらなかったケースが多くみられる。この要因として従来型のパターンマッチング方式のウイルス対策ソフトでは検知されない高度な攻撃が増加したと考えられる。

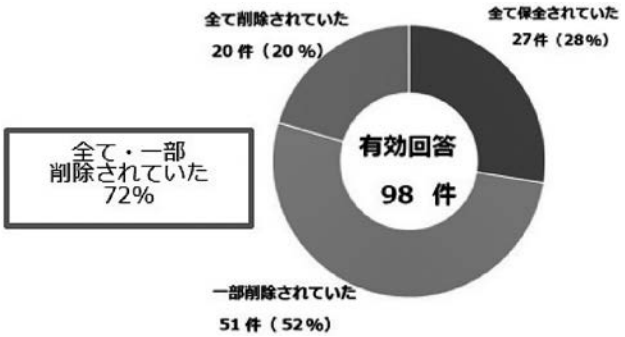

図５　ランサムウエア被害における被害企業・団体等のログの保全状況

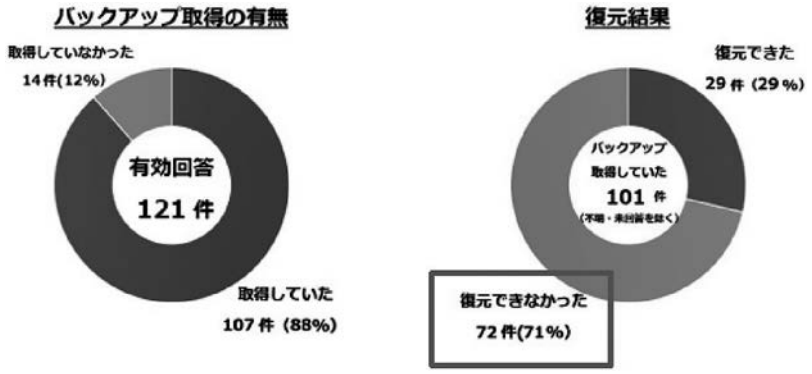

図 6　被害企業・団体等のバックアップ取得・活用状況

図 5、図 6 はログの保全とバックアップの状況である。被害にあった端末のログが消去されていることにも注目したい。サイバー空間ではログこそが証跡になるため侵入者は痕跡を残さないようにしている。バックアップが復元できなかった例が多いのは、バックアップも暗号化されてしまうケースがあるためである。書き換えできないストレージの導入など復元可能な対策を行い、定期的に復元できることを確認しておくことが望まれる。

サイバー攻撃の多くはメールとリモートアクセスからの侵入である。メールについては組織内で「怪しいメールは URL をクリックしない、ファイルを開かない」などの注意喚起が日常的に行われているが、昨今のフィッシングメールは現実にありそうな件名や差出人名で送られてくるため、注意していてもクリックしてしまう。クリックしたくらいで感染しないと思う人は多いだろう。しかしブラウザに脆弱性などが存在していれば感染は免れない。実際に感染しても当人が気づくことなくマルウエアは行動を開始する。そうして社内 LAN に侵入したマルウエアは Active Directory の脆弱性を利用し Administrator 権限を奪取し、次々にファイルサーバーやアプリケーションサーバー、データベースサーバーへの侵入を果たす。

VPN の脆弱性に対するメンテナンスを怠っている組織が少なくない。日本病院会の報告書によると対象の病院では 25％が機器のバージョンを把握していない状況である[4]。2019 年から脆弱性に関する注意喚起が JPCERT/CC より行われているにも関わらず、放置された機器から侵入を許している。脆弱性の対策はその時だけではなく、常に新しい脆弱性が発見されているため確認とアップデートを繰り返さなければならない。脆弱性に対する感度は欧米と比べ日本は鈍いという内容が石川県警のサイバーニュース[5]で取り上げられている。テレワークによるリモートアクセスが増えている状況で VPN の脆弱性の放置は危険極まりない。IT ベンダーのリモートメンテナンス用に設置されている VPN があれば忘れずに確認するべきである。

コロナ禍や DX 推進もあって ICT 環境は社内ネットワークに限定せず利用が広がっている。従来型のセキュリティー対策のままでは社内ネットワークへの侵入は困難なものでは無くなってきている。社内ネットワークは安全という考え方はもう通用しない。すべてのリソースは全く信用できないという前提に立ち、すべてを確かめる「ゼロトラスト」という考え方で対策を打つことが求められている。これは働き方改革や災害対策としてテレワーク、リモートワークといったどの場所でも働ける環境を整える際の考え方とも一致しており、たくさんの企業が取り組みを始めている。次章ではゼロトラストについて説明する。

3. ゼロトラストと可視化

標的型攻撃が猛威を振るっていた2010年代の初め頃、FirewallやIPS/IDS、ゲートウェイ型ウイルス対策、Sandboxなどといったゲートウェイ型セキュリティーとエンドポイントに導入するウイルス対策ソフトでは被害を止められなくなっていた。そんな時にForrester ResearchのJohn Kindervag氏が、信頼できる内部ネットワークと、信頼できない外部ネットワークの考え方を破棄し、すべてのネットワークトラフィックを信頼できないものと見なし、ゼロトラストを構成する以下の三つの原則を唱えた[6]。

1）すべてのリソースは、場所に関係なく、安全な方法でアクセス
2）アクセス制御は役割に応じて厳密に実施
3）すべてのトラフィックをログに記録し、確認する

その後、2020年8月に米国国立標準技術研究所（NIST）がSP 800-207[7]ゼロトラストアーキテクチャを正式に公開し、本ドキュメントによりゼロトラストは以下のように定義された。『ゼロトラストは、ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体のことである。ゼロトラストアーキテクチャは、ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシー等を含むサイバーセキュリティー計画のことである。』また、このようなことも記載されている。『これまで政府機関（および一般的な企業ネットワーク）では、ネットワークの境界防御に重点を置いており、認証された主体には、内部ネットワークに入った後、広範なリソースの集まりにアクセスする権限が与えられている。その結果、環境内での不正な水平移動（ラテラルムーブメント）は、連邦政府機関にとって最大の課題の一つとなっている。』そしてゼロトラストの基本理念として以下の7項目を掲げている。

1. 全てのデータとコンピュータサービスをリソースとみなす
2. 全ての通信はネットワークの場所に関わらず保護する
3. 企業リソースへのアクセスはセッション毎に許可する
4. リソースへのアクセスは、ふるまいや動的ポリシー（IDやアプリ、識別可能なクライアントの状態、アクセス先）によって決定する
5. 所有及び関連する全てのデバイスは可能な限り最も安全な状態とし、資産を監視し、状態を維持することを企業は確認する
6. 全てのリソースの認証と認可はアクセス許可の前に動的に厳密に行う
7. ネットワークインフラと通信の現在の状態に関するできるだけ多くの情報を収集し、それを使用して企業はセキュリティーの状態を改善する

2021年9月、米国政府機関がゼロトラストアーキテクチャを実現するために利用できるロードマップの一つとして、CISA：米国サイバーセキュリティー・インフラセキュリティー庁は「ゼロトラスト成熟度モデル」[8]をリリースした。

「Identity」「Device」「Application Workload」「Network/Environment」「Data」の五つの柱と「Visibility and Analytics」「Automation and Orchestration」「Governance」を横断的に

掛け合わせ、三つのレベル（Traditional、Advanced、Optimal）で成熟度を表している。表1は各項目のレベル毎に求められる対応を示している。

表1　ゼロトラスト成熟度

	レベル1 従来型	レベル2 先進型	レベル3 理想形
可視化＆分析	基本、静的属性	基本属性集約と分析	行動分析
自動化	アカウント手動管理	自動オーケストレーションとID統合	IDのライフサイクル管理、動的同期
ユーザーID	パスワード・MFA 簡易リスク診断	SSO、IDaaS	リスク、コンテキストベース
デバイス	資産管理	コンプライアンス遵守 デバイスポスチャ	常時監視、リアルタイム分析
ネットワーク	広いセグメント分け 最小限の暗号化	マイクロセグメント 基本的な分析	完全マイクロセグメント、機械学習脅威対策、すべて暗号化
ワークロード（アプリ）	ローカル認証 最小限ワークフロー 一部クラウド許可	一元化された認証 ワークフローに基本的な統合	継続的にアクセス検証、ワークフローに完全統合
データ	不十分なインベントリ管理、暗号無し	特権の最小化 暗号化	動的な対応 すべて暗号化

では、実際のゼロトラストを実現するためにはどのようなソリューションを選択すべきか。残念ながらひとつのソリューションで実現できるものはまだない。求められる主な機能は「厳密な本人認証、デバイス認証」「厳密なアクセス制御」「可視化と対応」である。

「厳密な本人認証、デバイス認証」は今日ではIDaaS（ID as a Service）とMDM（Mobile Device Management）によって実現される。IDaaSは利用者の役割に応じて柔軟に認可を定義し、各種アプリケーションにSAML（Security Assertion Markup Language）ベースのパスワードレスによる認証連携SSO（Single Sign-On）を実現する。またIDaaSへの認証時には高度なMFA（Multi Factor Authentication）機能が用意されており、最近ではパスワードレス認証を採用するケースが出てきている。フィッシングによるパスワード窃取やパスワードの使いまわしなどの不適切な運用によりパスワードの存在はリスクとなっており、生体認証とデバイス認証を組み合わせたパスワードレス認証が今後の主流になると予想される。またデバイス認証はデバイス証明書による認証に加えて、そのデバイスの設定やアップデート状況が正しい状態であることを確認することで安全性を向上できる。MDMによりOS設定やアップデート管理、セキュリティーソフトウェアの状態管理を行い、正しい状態のデバイスのみに認証を許可する。

次の「厳密なアクセス制御」の「アクセス制御」とは、利用者の役割に応じてアクセス先を制限する機能である。「厳密な」とは、従来のアクセス制御は社員であればほとんどの社内リソースにアクセスを許可していたものに対し、社員の個々の役割に応じてアクセスできる先を最小限にすることである。業務に不要なサイトへのアクセスを禁止するだけでなく、マルウエアのダウンロードのブロックやマルウエア感染時のC&C通信[*1]をブロックするといったインターネットへのアクセスを制限する機能に加え、社内ネットワークであっても利用者の業務に

関係しないアプリケーションサーバーへのアクセスを制限することも求められる。これは利用者端末がマルウエアに感染した際の水平移動（ラテラルムーブメント）を制限することに効果を発揮する。この考え方は今までの社内ネットワークの設計とは異なるため、見直しを迫られることになる。すべての社内アプリケーションサーバーはデータセンターに設置し、利用者の役割に応じてアクセスを制御できるネットワークを用意する。方法としては認証・認可・プロキシーの機能を持つIAP（Identity Aware Proxy）の導入、もしくはZTNAと呼ばれる次世代型のリモートアクセスサービスの利用がある。いずれもユーザーの役割に応じて接続先を制御するソリューションである。従来型のリモートアクセスは接続口をインターネットに公開しているがゆえに攻撃に遭いやすい欠点がある。ZTNAの多くはアクセスポイントをインターネットに公開しない方式を採用しており、攻撃者は見つけることができず安全性が高い。次世代リモートアクセスと呼ばれる所以である。ZTNAについては4.1節にて詳述する。

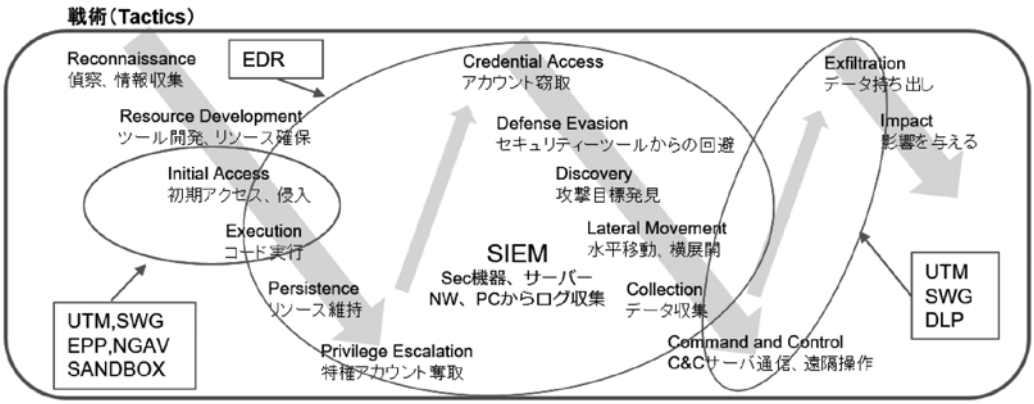

図7　MITRE ATT&CKの戦術とソリューション

最後に「可視化と対応」を説明する。攻撃側の手法などを整理したものとして米国のMITRE社が2013年から公開しているナレッジデータベースのMITRE ATT&CK®[9]がある。攻撃手法、戦術、事例、緩和策、検知方法などの情報を提供している。図7は戦術に対するソリューションを併記した図である。各段階での攻撃を検知するには、各所での監視が重要であることがわかる。

セキュリティー監視は主にエンドポイント管理とネットワーク監視がある。エンドポイントはPCやサーバー上でマルウエアが実行される状況を監視し、ネットワークは出入口のセキュリティー機器等のログを監視する。エンドポイントの可視化と対応にはEDR（Endpoint Detection and Response）が有効なソリューションである。サイバー攻撃は防げないものとして、エンドポイントでの攻撃の状況を可視化し、必要に応じて隔離を行い、被害を最小限にする。EDRはPCやサーバーの可視化に有効であり、ネットワークの情報を照らしわせることでさらに詳しい情報を得ることができる。このように拡大して可視化できるものとしてXDR（Extended Detection and Response）がある。また、SIEM（Security Information and Event Management）と呼ばれるソリューションはあらゆるログを取り込み、相関分析により不正アクセスの兆候を可視化することで、不正アクセスを未然に防止するとともに、被害範囲の特定に有効である。SIEMはログの保全にも役立つ。そして、SOAR（Security Orchestration,

Automation and Response）を利用した自動化も注目されている。特定のアラートが発生した場合、あらかじめアラートに応じた対応手順をプレイブックに登録しておくことで、通信を止めるなどの動作を自動で各種機器に設定することができる。EDR、XDR、SIEM、SOAR については 4.2 節にて詳述する。

4. ゼロトラストで見落とされがちなものと対策ソリューション

ユニアデックスでは 2022 年より「セキュリティー成熟度診断」を無償で実施している。国内外の各種基準を参考にユニアデックスが独自に作成した 59 個の質問から技術面にフォーカスしてセキュリティー対策の成熟度を可視化する。現状のレベル（AS-IS）と目指すべきレベル（TO-BE）を明示するので、今後のセキュリティー対策の計画を立てる際に有効である。この診断は既に 40 を超す企業や団体に実施しており診断データが蓄積されている。図 8 に示す通り過去の診断データからセキュリティー対策への各社の取り組みの濃淡が垣間見える。

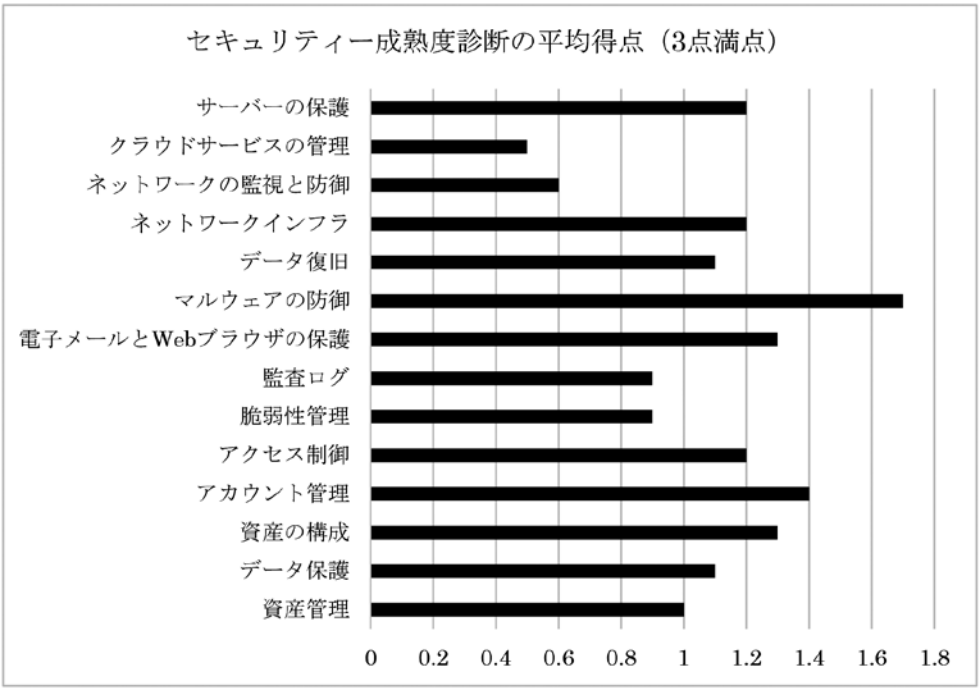

図 8　成熟度診断のカテゴリ別平均得点

「セキュリティー成熟度診断」では、各カテゴリの対策状況に応じて 3 点満点で評価している。1 点は最低限行うべきレベル、2 点は一般の組織が目指すべきレベル、3 点は公共性の高いサービスや社会インフラに影響するサービスを提供している組織がとるべきレベルとしている。1 点に満たない場合、基本的な対策が不足しているということでリスクが極めて大きく、早急な対策が求められる。各カテゴリの平均値のグラフから、1 点未満の項目は「クラウドサービスの管理」「ネットワークの監視と防御」「監査ログ」「脆弱性管理」である。これらの課題は対策が後回しにされているということであり、つまり見落とされがちなものである。

「クラウドサービスの管理」にはクラウドサービスの契約状況の管理や、利用する際のルー

ルやポリシーの確認、クラウドサービスの安全性評価などの項目がある。クラウドサービスを積極利用している場合は、対象サービスの品質確認や不適切設定の排除などの対策を強化すべきである。次の「ネットワークの監視と防御」は、ログの一元管理と相関分析やIPS導入、リモートアクセス時のデバイス健全性確認などの質問が含まれる。「監査ログ」は、ログの一元化と時刻同期やログ項目、90日以上の保存、相関分析などの質問が含まれる。「脆弱性管理」は、OSとソフトウェアの毎月のアップデートと公開サーバーへの脆弱性スキャンなどが含まれる。脆弱性管理はランサムウエアをはじめとしたサイバーセキュリティー対策の基本である。しかし現場の意見として、アプリケーション側がOSのアップデートをサポート対象外とするケースがあるため、アップデートできないといった問題が生じることがある。その場合は最低限、仮想パッチなどで対策する。また、2章で述べたようにVPNの脆弱性を狙った攻撃が多発する中、その脆弱性管理は最重要課題である。そして、攻撃の兆候を察知するにも被害状況を把握するにもログ管理が重要である。本章後半ではVPNに代わり注目されている次世代リモートアクセス制御ソリューションのZTNAと、ログを管理し攻撃を可視化するSIEM/EDR/SOAR/XDRを紹介する。

4.1　次世代リモートアクセスZTNA（Zero Trust Network Access）

ZTNAは2019年に紹介された、ユーザーの役割に応じてアクセス先を制限する仕組みである。2014年ごろに提唱されたSDP（Software Defined Perimeter）の考え方にリモートアクセスが加わり、インターネットから安全にアプリケーションサーバーにアクセスする方法として注目を浴びている。代表例のひとつとしてZscaler™のZTNAソリューションであるZscaler Private Access（ZPA）を紹介する。ZPAの最大の特徴はリモートアクセスソリューションであるにも関わらず、社内LANへの接続口のIPアドレスをインターネットに公開しなくてよい点である。社内LANに設置された仮想アプライアンスはアウトバウンド通信（443ポート）で、インターネット上のZscalerクラウドにトンネルを張るため、VPN装置のように入口のIPアドレスをインターネットに晒さずに済む。これによりインターネットから攻撃する際に直接の入口が無いという点でリスクを大幅に減らしている。また、Zscalerクラウドは SaaSで提供されており、脆弱性のアップデート運用はサービス提供者が行う。仮想アプライアンスについても自動でアップデートされるため、情シス運用者の手間が削減される。そしてユーザーの役割に応じたアクセス制御は、各アプリケーションに対してFQDN単位で接続の制限をかけることができるため、社内LAN全部が丸見えになるということがない。これは攻撃の被害拡大を招くラテラルムーブメント（水平移動）の防止となり、厳密なアクセス制御を実現するのに有効である。またユーザーの端末からはZscalerクラウドに向かって接続を行い、SAMLベースの認証を行う。MFAやデバイス認証などで厳密な認証を行うことも可能である。接続の際には端末のアップデート状況の確認などの健全性チェックを行う。

ZPAの特徴としてもう一つ大きなメリットがある。Zscaler Internet Access（ZIA）との統合である。ZIAはインターネットを安全に利用するためのサービスで、URLフィルタリング機能やフィッシング対策機能などがある。モバイルユーザーにとってインターネットへの直接のアクセスはリスクが大きいが、ZIAにより強制的にZscalerのクラウドを通過させるため安全性を担保できる。図9はこのZIAとZPAが統合した構成のイメージである。ユーザーは社内のアプリケーションであろうと、クラウドサービスであろうとZscalerクラウドに接続すれ

ばどちらもシームレスにアクセスできるため、VPN をつなぐ、切るといった操作が不要になりエクスペリエンスが向上するという利点がある。

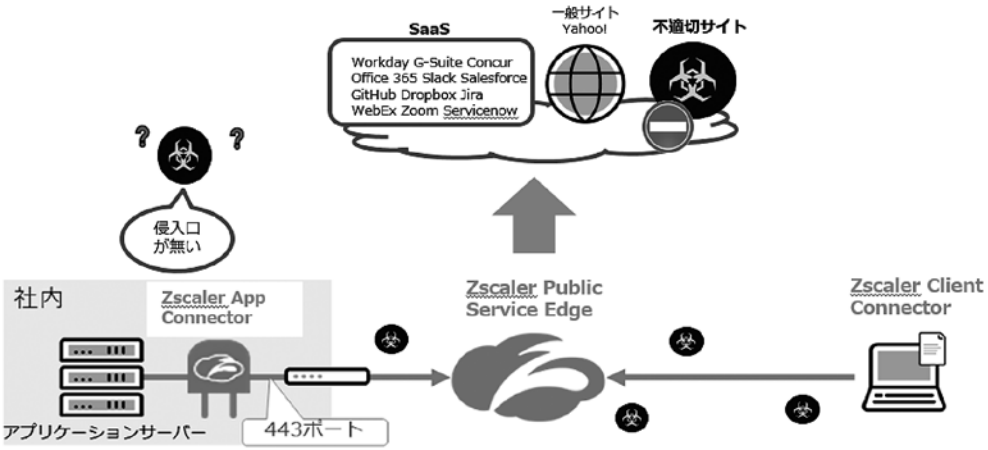

図 9　Zscaler の概念図

4. 2　可視化と対応（SIEM/EDR/SOAR/XDR）

2012 年ごろ可視化を代表するものとして SIEM が登場した。バラバラに存在していたセキュリティー機器やネットワーク機器、サーバー等のログを集約し長期保存、相関分析を行うことでインシデントの検知を行う。全体像を分析するために有効なものとして政府、金融事業者、大企業、SOC（Security Operation Center）事業者に多く導入されている。従来はアプライアンスや高機能サーバーにソフトウェアをインストールするモデルであったが、現在はクラウドサービスでも提供されている。エンドポイントのセキュリティー対策は従来から導入されているパターンマッチングによる検出や駆除を行うウイルス対策ソフトとして EPP（Endpoint Protection Platform）がある。またパターン更新前あるいはファイルレスで侵入するゼロデイ攻撃の対策として、NGAV（Next Generation Anti-Virus）と呼ばれる振る舞いを検知するタイプの対策ソフトがある。2013 年ごろに登場した EDR（Endpoint Detection and Response）は、EPP や NGAV でも止められなかった侵入に対し、攻撃を可視化し PC の隔離などの対応を支援するものであり、現在普及期に入っている。その後エンドポイントとは異なる監視方法として、ネットワークの監視を行う NDR（Network Detection and Response）が登場した。また同時期にセキュリティー運用の自動化を支援するものとして SOAR（Security Orchestration, Automation and Response）が登場する。例えばマルウエアによる C&C 通信を SIEM で検知した場合、一定の条件を基に SWG（Secure Web Gateway）の URL フィルタリングの API を利用して自動的にブラックリストに不審な URL を追加するといった運用ができるようになる。この時に条件があいまいになると、人の判断や承認行為を加えるといったことが求められる。それを解決するのが SOAR である。SOAR は各種セキュリティーソリューションに対して自動で設定変更を行う管理ツールである。プレイブックと呼ばれる手順書を作成し、情報共有や承認などのプロセス管理を行う。人間の判断を要する複雑な事象に対応することが可能となる。そして近年注目されているのが XDR（Extended detection and response）である。エンドポイント、ネットワーク、クラウド、ワークロードなど広範囲に情報収集し、監視、分

析を行い、対応を自動化するものである。比較的新しい分野で今後成長が見込まれる。SIEM/EDR/NDR/SOAR/XDR においては各社でアプローチが異なっており、それぞれに特徴がある。本節ではユニアデックスで取り扱っている SIEM/SOAR の Sumo Logic® と EDR/XDR の Cybereason を例として紹介する。

4. 2. 1　Sumo Logic

Sumo Logic は図 10 に示すようにクラウドやオンプレミスから出力される大量のログを保管し、分析や監視を行うクラウドサービス型の SIEM である。2010 年に設立され、設立当初はクラウドのサービス可視化がメインであったが、現在では SIEM/SOAR を含んだサービスに成長している。SIEM は古くからあるソリューションで、インシデントの事後対応に備えてログを長期保存するために導入されているケースが多かった。あるいは SOC 事業者がリアルタイム分析のために利用していた。従来の SIEM 製品はアプライアンス型かソフトウェア型のため、ログ量のピークに合わせたサイジング設計となり、そのスペックを満たすマシンの調達コストが導入のハードルを上げていた。またログの取り込みや分析において高いスキルが求められ、SOC 業者もしくは人材豊富な企業でなければ導入が難しかった。Sumo Logic はそれらの課題を解決してくれるサービスである。特徴的な機能について以下 1) ～ 4) にて紹介する。

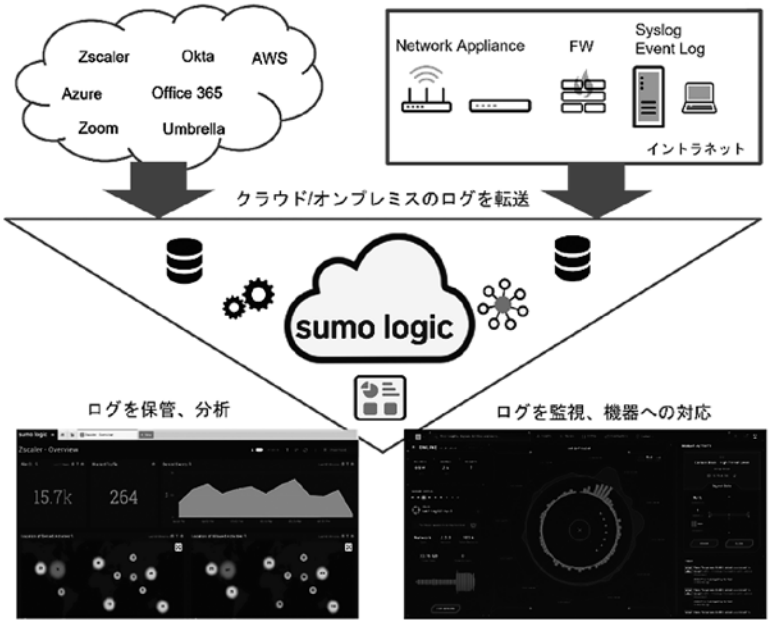

図 10　Sumo Logic の概念図

1)　クラウドネイティブプラットフォーム

Sumo Logic はクラウドで提供することを前提に設計されており、マルチテナントにも対応したサービスである。クラウドサービスのため処理量に応じてリソースが割り当てられ、急峻なログの増加があってもリソース不足になることがない。バージョンアップやストレージ拡張、ハードウェア更改といった運用負荷も削減できる。また料金もログ量の最大値ではなく実際に使う分を購入すればよいため余計な負担がない。

2） 分析機能（脅威インテリジェンス、自動相関分析、高度な分析）

サイバー攻撃の各種情報をデータベース化した「脅威インテリジェンス」を標準搭載している。脅威インテリジェンスを利用することで危険な通信ログを見つけることができる。通常、脅威インテリジェンスは高価なものであるが、エントリーモデルのライセンスでも利用することができる。自動相関分析は大量のアラートから調査すべき情報を絞り込むことができるため、人的リソースの枯渇している組織においては頼もしい機能である。相関分析ルールはあらかじめ 600 個以上のルールがあり、設計を助ける。アラートが発報された際に状況をより詳しく分析しなければならない場合がある。その際に大量のログの中から関連するイベントを探すことになる。ここで役立つ分析機能として Log Reduce がある。Log Reduce は大量のログをパターン化しノイズ除去を行うため根本原因のログを見つけやすくなる。また傾向分析機能により通常から大きく外れた値を検知する Outlier Detection も異常を検知するのに有効な機能である。

3） 豊富なテンプレート

SIEM はたくさんの種類のログを収集し、分析を行う。ログは各機器メーカー独自のフォーマットを持っており、取り込む際に正規化しなければならない。ここで役に立つのが App Catalog と呼ばれるテンプレートである。あらかじめログのフォーマットとダッシュボードのテンプレートが用意されており、ログを取り込んだ際に手間をかけずにダッシュボードに表示することができる。また、自社開発アプリなどで標準テンプレートがない場合でも容易にフォーマット化できる GUI も用意されている。

4） SOAR 機能

SIEM で脅威を発見した後、次のアクションを管理するのが SOAR の役割である。インシデントの状態を SOC チーム内で共有し、プレイブックと呼ばれるワークフローを作成し、必要に応じて承認プロセスを経てセキュリティー機器に対してブロックなどの指示を行う。例えば C&C 通信の傾向を発見した場合、SWG の URL フィルタリングに対して当該 IP アドレスをブラックリストに追加するといったことを自動で行う。自動実行前にワークフローによる承認を入れることもできる。SOC の運用負荷を軽減できるためセキュリティー人員不足を補える。

4. 2. 2 Cybereason

Cybereason は 2012 年に設立された。マルウエアの侵入は止めることができないという前提に立ち、被害を最小限にするためのエンドポイントの監視、解析、対処を行うために開発された。図 11 に示すようにエンドポイントのデータ収集、監視、解析を行う。現在は EDR だけでなく NGAV 機能や XDR への拡張が行われている。主な特徴を以下 1）～ 5）にて紹介する。

1） 進行する攻撃を直感的に可視化

Cybereason EDR は攻撃の根本原因を特定するための情報をクラウドに集約し攻撃タイプを分析する。感染端末の台数や時系列での感染状況、使用されたツールなどの情報を各エンドポイントから集約しダッシュボードに直感的にわかりやすく表示する。

2） 遠隔から、即座にワンクリック対処

問題が発生している複数の端末に対し、ダッシュボードからワンクリックで、エンドポイントの隔離やプロセス停止、ファイル隔離、レジストリ削除などの対処ができる。

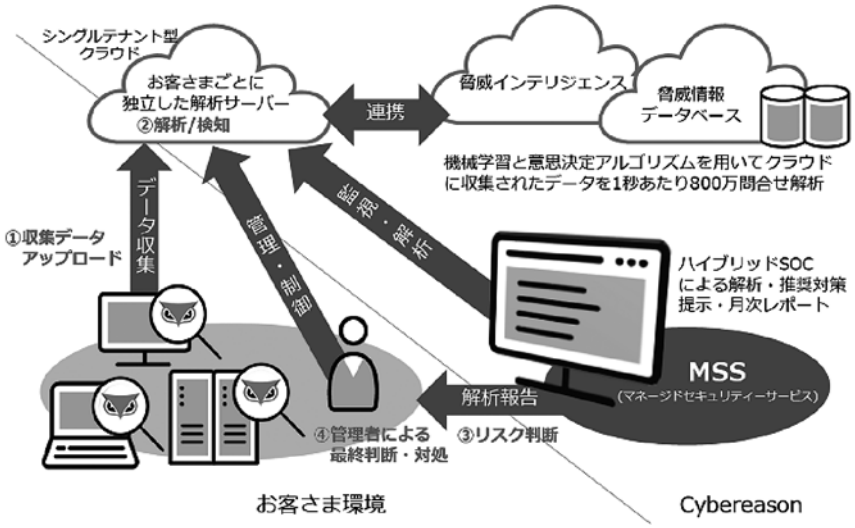

図 11　Cybereason の概念図

3)　日本語レポートをボタン一つで自動生成

セキュリティー業務の負荷を軽減する自動レポート生成機能を持つ。概要やタイムライン、通信、端末、ユーザーなどを含む日本語のレポートを自動生成することができる。

4)　ランサムウエア対策機能

振る舞い分析や、おとりファイルによるランサムウエアの検知機能を持つ。またマスターブートレコード監視によるランサムウエア検知にも対応している。

5)　NGAV 機能

シグネチャーベース検知や機械学習解析、ファイルレスマルウエアブロックといった次世代型アンチウイルスの機能オプションも用意されている。

5.　ユニアデックスの取り組み

ユニアデックスはゼロトラストの概念によるセキュリティー対策を行うため、図 12 に示すように「CloudPas®」ブランドとして各分野のセキュリティーソリューションを取りまとめ、提案、設計、構築、保守、運用といったライフサイクルを通じて顧客に安心と安全を提供している。

セキュリティーは多種多様な要件があり、様々なリスクに対応するために優先度を考え、計画しなければならない。優先度を考える際、各種ガイドラインが参考になる。図 13 は 4 章冒頭でも述べた、ユニアデックスが無償で行っている「セキュリティー成熟度診断」の診断報告書のイメージである。顧客の現状と目指すべきゴールから、対策としてのソリューションを提案するものである。本診断は国内外のガイドラインを参考に独自に作成したもので、59 個の質問に回答することで技術的課題を網羅的に診断する。診断はゼロトラスト成熟度にも対応しており、取るべき対策を可視化する。診断結果は AS-IS と TO-BE を明確にし、GAP を埋めるための対策として、最低限行うべき対策、一般企業が行うべき対策、理想的な対策の三つのレベルを提示しており、対策の優先度も明確にする。診断結果を基に優先度と予算に応じてソリューションの導入を支援する。

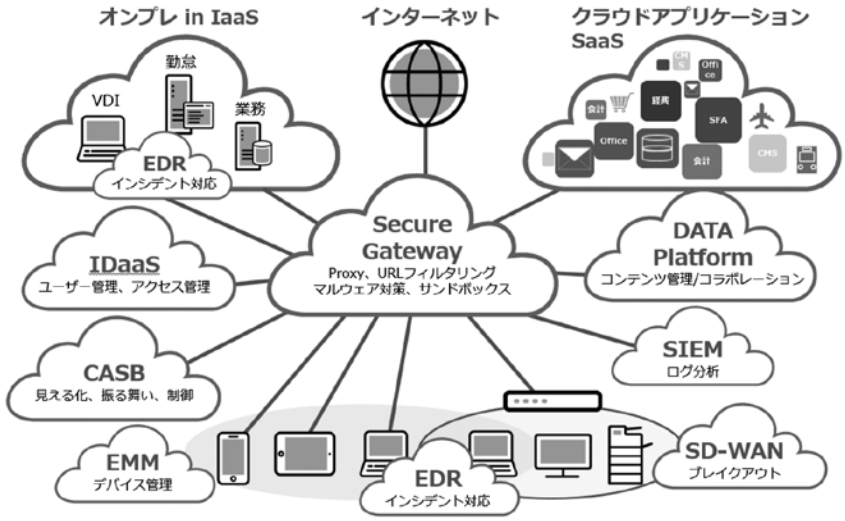

図 12　CloudPas の概念図

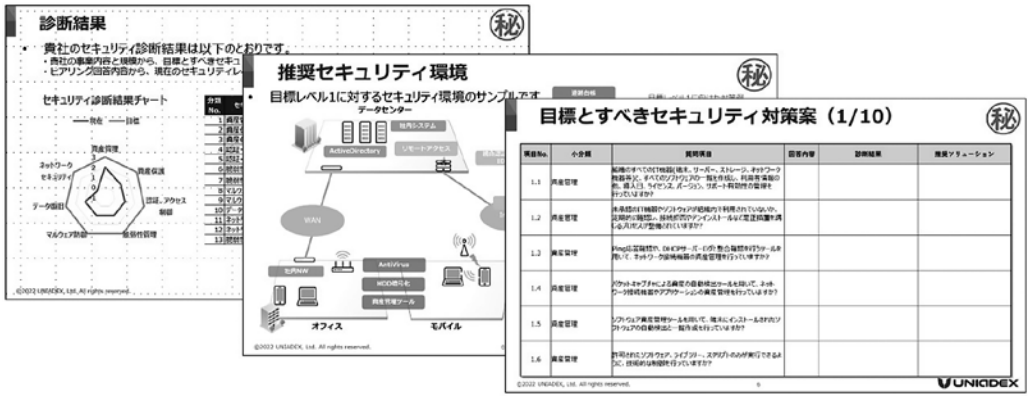

図 13　セキュリティー成熟度診断結果

図 14　CloudPas MSS のサービスメニュー

新しいソリューションを導入するたびに使用方法を学び直し、運用手順を考え直すことは大変な労力を伴う。そのためユニアデックスでは運用支援サービスとして「CloudPas MSS」を提供している。「CloudPas MSS」は統合クラウドセキュリティーサービス「CloudPas」のマ

ネージドセキュリティーサービスであり、サポートデスク、運用代行、レポーティング、セキュリティー監視などのサービスを提供している（図 14）。昨今の DX 推進により情報システム部門は新たな企画を期待されており、セキュリティー運用を受け持つ人材の確保が難しくなってきている。そのような顧客の課題を「CloudPas MSS」で解決できるようサービス開発を推進している。

6. お わ り に

本稿は、2022 年 6 月に開催された BIPROGY FORUM 2022 オンラインセッション『ゼロトラストで忘れられた大事なものは？　～ランサムウエア対策もゼロトラストも「可視化」が大事～』の内容をベースとして、最近のセキュリティー被害状況や対策のトレンドを再整理し、企業が取り組むべきセキュリティー対策について記述したものである。セキュリティー対策はわかりやすい「防御」のソリューションが注目されがちであるが、「アクセス制御」と「可視化」の重要性にフォーカスし読者に気付きを与える一助になれば幸いである。

最後に本稿の執筆にあたり、ご支援いただいた皆様に深く感謝いたします。

＊ 1　C&C 通信とは Command and Control 通信の略で、PC に侵入したマルウエアが攻撃者の命令を受け取るためにインターネット上に設けられたサーバーに接続する通信のことである。

参考文献
［1］ サイバー空間における脅威の概況 2022，公安調査庁.
https://www.moj.go.jp/content/001371280.pdf
［2］ マルウエア Emotet の感染再拡大に関する注意喚起，JPCERT コーディネーションセンター，2022 年 4 月 22 日.
https://www.jpcert.or.jp/at/2022/at220006.html
［3］ 令和 3 年におけるサイバー空間をめぐる脅威の情勢等について，広報資料，警察庁，2022 年 4 月 7 日.
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
［4］ 電子カルテシステム等のセキュリティ対策状況について，日本病院会 ICT 推進委員会，2023 年 2 月 2 日.
https://www.hospital.or.jp/pdf/06_20230202_01.pdf
［5］サイバーニュース 第 3 号，石川県警察本部生活安全部サイバー犯罪対策課，2022 年 4 月.
https://www2.police.pref.ishikawa.lg.jp/security/upload/03-202204.pdf
［6］ Zero Trust Network Architecture with John Kindervag – Video, Palo Alto Networks, 2023.
https://www.paloaltonetworks.jp/resources/videos/zero-trust
［7］ SP 800-207 Zero Trust Architecture, NIST, August 2020.
https://csrc.nist.gov/publications/detail/sp/800-207/final
［8］ Zero Trust Maturity Model, CISA, June 2021.
https://www.cisa.gov/zero-trust-maturity-model
［9］ MITRE ATT&CK®, The MITRE Corporation.
https://attack.mitre.org/

※　上記参考文献に含まれる URL のリンク先は，2023 年 4 月 10 日時点での存在を確認.

執筆者紹介　岩　竹　智　之（Tomoyuki Iwatake）
2005年ユニアデックス(株)入社、セキュリティー商品の企画、開発、販売支援業務に従事。2017年よりクラウドセキュリティーサービスの商品企画をきっかけにゼロトラストの提案活動に取り組んでいる。