Deloitte.
デロイト トーマツ

デジタル・クラウド活用を下支えする ゼロトラスト

ビジネストランスフォーメーションに資する ゼロトラストアーキテクチャ

デロイト トーマツ コンサルティング合同会社
テクノロジーストラテジー・トランスフォーメーション

Introduction

ビジネストランスフォーメーションに資する
ゼロトラストアーキテクチャ

ビジネストランスフォーメーションwith デジタルの取り組みを進めるために、クラウド活用が不可欠となり、従来とは異なるセキュリティが前提として求められる。そのため、デジタル、クラウド、セキュリティ強化を三位一体として進めるゼロトラストアーキテクチャは経営が取り組むべきアジェンダとなってきている。

企業が持つ情報資産を安全に利用できるよう対策を実施し、ビジネスを推進するためにセキュリティは不可欠である

三位一体の経営アジェンダ（デジタル・クラウド・セキュリティ）

さまざまな業界でデジタル技術が活用される現在、国内の企業・組織を狙うサイバー攻撃が数多く確認されている。海外を見ても、過去には核燃料や電力、水道、医療機関などのあらゆるインフラ事業者がサイバー攻撃を受けた結果、物理的な破壊や稼働不能という事態に陥っている。こうした重要インフラへのサイバー攻撃によって、私たちの日常生活や経済活動に大きな影響を受けてしまう。また、近年は不安定な国際情勢に便乗したサイバー攻撃も報告されるようになり、国家の安全保障に影響を及ぼしかねない問題という認識も高まってきている。

図1：三位一体の経営アジェンダ（デジタル・クラウド・セキュリティ）

こうした事態を受け、日本の経済産業省や総務省などからサイバー攻撃のリスクに対して、インフラ事業者をはじめとする各企業・団体などに向けて注意喚起が出されている。2022年6月には、日本政府のサイバーセキュリティ戦略本部が「重要インフラのサイバーセキュリティー対策に係る行動計画」[1]の改訂を決定した。今回の改訂では、14分野の重要インフラ事業者に対して、経営層が内部統制システムを構築する際には適切なサイバーセキュリティを講じる義務が含まれることが明記された。重要インフラ事業者とは「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス」「医療」「水道」「物流」「化学」「クレジット」「石油」などの事業を展開する企業・組織が該当する。

このように、さまざまな業界でデジタル技術が活用される現在、高度なサイバーセキュリティへの対策が求められることが当たり前となってきている。さまざまな企業においてステークホルダーからの要請や必要性にかられ業務・事業の高度化やdX（ビジネストランスフォーメーションwith デジタル）の取り組みを進めているが、この取り組みについてはテクロジーの活用が切っても切り離せず、特にテクノロジーのベストプラクティスをas a serviceとして提供しているハイパースケーラーの活用は無視できない。クラウドシフトとも呼ばれるこのハイパースケーラークラウド活用を推進するなかで、従来のオンプレミスにおけるITとは異なるセキュリティが前提として求められるため、デジタル、クラウド、セキュリティ強化は三位一体として進めなければならない経営アジェンダとなってきている（図1参照）。

さて、情報セキュリティ強化の目的とは何だろうか。企業の持つな情報に対してウイルスに感染せず、情報漏えいしないように守りたければ、金庫に入れておいて厳重に管理し、ネットワークに繋がなければ、おそらく何事も起きないように守ることができる。しかし、これでは、その情報を利用することが一切できなくなってしまう。

このように考えると、情報セキュリティの目的は、単に情報をまもるということではなく、企業が持つ情報資産を安全に利用できるよう対策を実施し、ビジネスを推進するために、その環境を維持することと言える。企業は、ITシステムを用いて、情報資産を利用し、ビジネスを推進していくものであり、この際に安全に情報資産を利用できる状態にしておくことが、情報セキュリティの目的であるのだ。

脚注

1. 内閣サイバーセキュリティセンター,「重要インフラのサイバーセキュリティー対策に係る行動計画」, https://www.nisc.go.jp/policy/group/infra/siryou/index.html, June 17, 2022.

情報セキュリティ投資は、インシデントに遭った組織とそうでない組織で大きく異なっている

ネットワーク境界防御型モデル

ここで、セキュリティ対策の歴史を辿っておこう。従来のセキュリティ対策は、境界防御型モデル（図2参照）と呼ばれる対策である。これは、「城を堀で防御する」サイバーセキュリティモデルとも言われ、安全なネットワーク境界の存在や仮想プライベートネットワーク（VPN）経由での従業員アクセス、および第三者のリモートアクセスが前提となったセキュリティ対策となっている。具体的には、VPNでプライベートなネットワーク接続、IPS（Intrusion Prevention System）でネットワーク通信の監視と侵入検知、ファイアウォールでネットワークパケットのフィルタリング、AntiVirusでシグネチャベースでのウイルス検知、SandBoxで安全なネットワーク区画でのマルウェア実行と必要に応じた隔離、QoS(Quality of Service)でネットワークの帯域制御や優先制御などを行うといったように、ネットワークレイヤでいくつもの防御を行っていくものであった。

多層防御型モデル

ネットワーク境界防御だけでは、情報セキュリティを実現するには限界がある。ソーシャルエンジニアリングと呼ばれる、関係者を装って電話でパスワードを聞き出す（なりすまし）、肩越しに画面やキー入力を見る（ショルダーハッキング）、プリンタやデスクやごみ箱に残された書類を漁る（トラッシング）など、さまざまな手法が増えていく中で、ネットワーク装置だけではシステムを守ることは不可能となった。このような時代において、情報セキュリティの対策では、多層防御（図3参照）という概念が重要となる。

軍事用語で、Defense in Depth (縦深防御、深層防御)という言葉があるが、これは、何重もの壁で囲まれた城の防御のことを示す。何重もの壁で囲み、敵の攻撃が中心部まで到達することを遅らせる/回避するということを目的とした手法となる。

情報セキュリティの対策においては、多層防御という概念で、Defense in Depthと同様に、ITシステムにおいても、幾重にも多層でセキュリティ対策を施し、インシデントの発生の確率を下げる/インシデント発生を回避するということを目的とした対策を行うことが必要となっている。

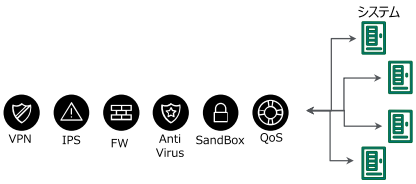

図 2：ネットワーク境界防御型モデル

サイバーキルチェーンへの対策

さらに時代が進むと、サイバー攻撃は、高度化、巧妙化していき、「防御」だけでは防げず、「侵入されることを前提」としていかに被害を最小限に抑えるかというセキュリティ対策を検討することが求められるようになった。これがサイバーキルチェーンへの対策（図4参照）である。

キルチェーンとは、もともと軍事用語で、攻撃の構造を以下の様にモデル化したもので、標的の特定(Target identification)、標的への武力の指向(Force dispatch to target)、標的を攻撃するかどうかの決心と命令(Decision and order to attack the target)、標的の破壊(Destruction of the target)というフェーズに分けて攻撃を捉えるという考え方である。

サイバーキルチェーンは、アメリカの大手軍需企業のロッキード・マーチン社が提唱したモデル化の考え方であり、標的型攻撃における攻撃者の一連の行動を、軍事行動になぞらえてモデル化したものである。標的型攻撃を受けると、大きくは、標的型攻撃等により端末がマルウェアに感染し、イントラネットを経由してマルウェア感染が蔓延し、内部通信を利用して機密情報にアクセスし、機密情報の外部漏洩が発生するということになる。そして、これらは瞬時に行われるのではなく数か月にわたって行われ続けられることがほとんどである。ここで、一番問題なのは、標的型攻撃メールで1台目の端末が感染してから、最終的に企業の情報を漏洩させるという攻撃者の目的を達するまでの数ヶ月の間、当該組織がこの事象に気付けないということだ。

図 3：多層防御型モデル

対策としては、ネットワークをマイクロセグメンテーション化して感染拡大を防止すること、感染している状態を可能な限り早期に検知できる状態を構築すること、内部への侵入を100％防げないかわりに内部から外部への情報の漏洩を出口でブロックすることが重要となる。攻撃を受け、かつ「侵入されることを前提」として、いかに被害を最小限に抑えるかという検討が求められるようになった。

この標的型攻撃への対策として導入するセキュリティソリューションは多岐にわたるため、特に欧米においてはセキュリティ対策にかかるコスト増大が問題になっている。ネットワークレベルでの侵入検知や侵入防止やアクセス制御に加えて、メールに対するセキュリティ対策や、サーバや端末に対するエンドポイントセキュリティ、各種ログを統合して監視しセキュリティインシデントを検知するためのSIEMソリューション、さらには、組織内ネットワークから外部ネットワークの疑わしい通信をブロックする出口対策ソリューションを導入することで、攻撃の連鎖の最後の鎖を断ち切るためにさまざまな対策が求められ、結果、セキュリティコストが増大するのだ。

一方、日本企業では実際にセキュリティインシデントに遭った一部の組織だけがサイバーキルチェーンへの対策を取っており、それ以外のほとんどの組織は境界防御モデルのセキュリティ対策のままであり、セキュリティにかける投資は極端に異なっている。

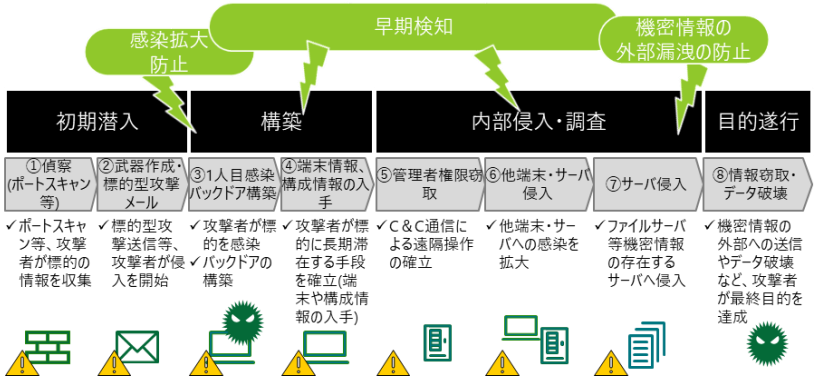

図 4 ：サイバーキルチェーンへの対策

ビジネストランスフォーメーションにクラウド活用が主流となり、アタックサーフェスが増大する中、ゼロトラストが不可欠となってきている

アタックサーフェス増加とゼロトラスト

クラウドやハイブリッドIT環境への移行により、クラウドベースのシステムや、リモートワーカー、接続デバイス数が増加していき、ネットワーク境界は絶えず拡大し雲散霧消していく。スマートデバイス、5G、エッジコンピューティングやAIの台頭により、さらに多くのデータ、接続ノード、および拡大したアタックサーフェス（攻撃可能面）を生み出している。

クラウドが主流となる現在、複数のクラウドプロバイダに跨ってサービスを利用する企業には、これらのテクノロジーを保護する責任が生まれている。企業がデータ、インフラや、各種アプリケーションなどのサービスを実現する際にas a serviceへの依存が多くなるにつれて、アタックサーフェス（攻撃可能面）が拡大する（図5参照）。

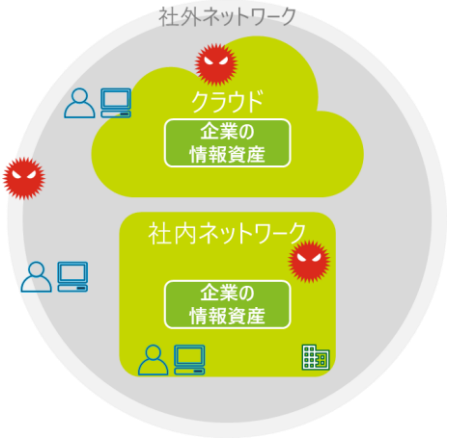

図5：拡大するアタックサーフェス（攻撃可能面）

ある調査[1]では、調査対象企業の59％が、ベンダーまたはそのほかの第三者に起因するデータ侵害を経験していた。別の調査[2]では、複数ベンダーのソリューション利用に起因するセキュリティインシデントは、単独のケースに比べ、13倍の経済的損失をもたらすと結論付けている。実際、従来の境界防御型セキュリティでは、組織内のネットワークに接続されているユーザとデバイスの信頼性を前提としている一方で、資格情報の盗難がセキュリティ侵害の4分の1以上を引き起こしているという調査結果[3]もある。

このような背景の中、ゼロトラストという観点でセキュリティ対策を行う必要性が出てきた。元々、ゼロトラストとは、Forrester Research社が2010年に提唱した言葉で、“社内（ネットワーク内）は安全である”という前提に、境界を守るやり方では守れなくなった現状を踏まえ、「すべてのトラフィックを信頼しないことを前提とし、検査、ログ取得を行う」というものである。2018年にForrester社が定義したComponent of the Zero Trust eXtended Ecosystem[4]においては、従来型ネットワーク環境と新たなクラウドベース環境双方を加味して考慮するべき7つの領域（データ、ワークロード、ネットワーク、デバイス、ピープル、視える化と分析、自動化とオーケストレーション）を定義している。

ゼロトラストについては、NIST (National Institute of Standards and Technology, NIST, アメリカ国立標準技術研究所) において、7つのゼロトラストアクセス原則が定義された[5]。これは、次のとおりである。

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はリソースと見なされる。
2. ネットワークの場所に関係なく、すべての通信が保護される。
3. 個々のエンタープライズリソースへのアクセスは、セッションごとに許可される。
4. リソースへのアクセスは、動的なポリシー（クライアントID、アプリケーション、および要求元の資産の監視可能な状態を含む）によって決定され、他の動作属性を含めることができる。
5. 企業は所有および関連するすべてのデバイスが可能な限り最も安全な状態であることを保証し、資産を監視し、それらが可能な限り最も安全な状態であることを確認する。
6. リソースの認証と承認はすべて動的であり、アクセスが許可される前に厳密に実施される。
7. 企業は、ネットワークインフラストラクチャと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。

脚注

1. Business Wire, “Opus & Ponemon Institute announce results of 2018 third-party data risk study: 59% of companies experienced a thirdparty data breach, yet only 16% say they effectively mitigate third-party risks,” November 15, 2018
2. RiskRecon, Ripples across the risk surface: A study of security incidents impacting multiple parties, accessed November 20, 2020.
3. Verizon, 2020 data breach investigations report, 2020
4. https://start.paloaltonetworks.com/2020-forrester-ztx-report
5. https://csrc.nist.gov/pubs/sp/800/207/final

目指すゼロトラストアーキテクチャで実現すべきことは、ID管理とアクセス制御の高度化、すべてのリソースの把握と検証、発見的統制の強化である

ゼロトラストアーキテクチャ

ゼロトラストアーキテクチャとは、全てのユーザ、デバイス、ワークロード、NWにおいて、セキュリティ脅威が存在することを前提とした考え方であり、３つの考え方と7つの構成要素で実現するものと捉えることができる（図7参照）。

ゼロトラストアーキテクチャ構築に必要となる考え方の1つ目が「ID管理とアクセス制御の高度化」である。これは、ゼロトラストの考え方では新たな「境界」として「ID（アイデンティティ）」をユーザ認証・認可に活用することに着目し、認証やアクセス制御の処理は動的かつトランザクションごとに制御したり、組織の保有するリソースに対してセッション単位でアクセス許可の制御を実施したり、動的なポリシーベース・コンテキストベースでの制御を実現する事となる。具体的には、IDaaS(Identity as a service)や、IGA（Identity Governance & Administration）と呼ばれるソリューションにて、ID認証、ID/パスワード管理、シングルサインオン、アクセス制御、IDのガバナンスと管理を行う。

ゼロトラストアーキテクチャ構築に必要となる考え方の2つ目が「すべてのリソースの把握・検証」である。これは、すべてのリソース（データソースとコンピューティングサービス等）はすべて守るべきリソースと見なして状態を把握し、ロケーション（ネットワークの場所）に関係なく、すべての通信の保護を実現することとなる。具体的なソリューションとしては、SWG(Secure Web Gateway)やCASB（Cloud Access Security Broker）にて利用者からクラウドへアクセスする通信の監視やアクセス制御を行い、IAP（Identity Awareness Proxy）にてクラウド上のノードを経由して、プライベートNW上のシステムへアプリケーション単位での接続を制御し、DLP(Data Loss Prevention)／DMaaS（Data Management as a Service）にて、機密情報の含まれたデータの情報漏えい防止／社内外にあるデータをクラウド上で一元的管理を行う。また、端末などのエンドポイントに対しては、UEM（Unified Endpoint Management）にてエンドポイントの統合的管理（ノートPCや、企業で使われるモバイルデバイス含む）を行い、EDP（Endpoint Detection and Response）にてマルウェア攻撃の検知・隔離、ログ監視による攻撃経路の特定・影響範囲の調査を実現する。

ゼロトラストアーキテクチャ構築に必要となる考え方の３つ目が「発見的統制の強化」である。これは、ネットワークと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、包括的なログ管理を実施し、組織の保有する全リソースに対し、正しくセキュリティが保たれるよう継続的な監視を実現することとなる。具体的なソリューションとしては、SIEM（Security Information and Event Management）やUEBA(User and Entity Behavior Analytics)にて、セキュリティ関連情報やユーザ行動を分析、異常な動作や潜在的な攻撃の検知を行う。

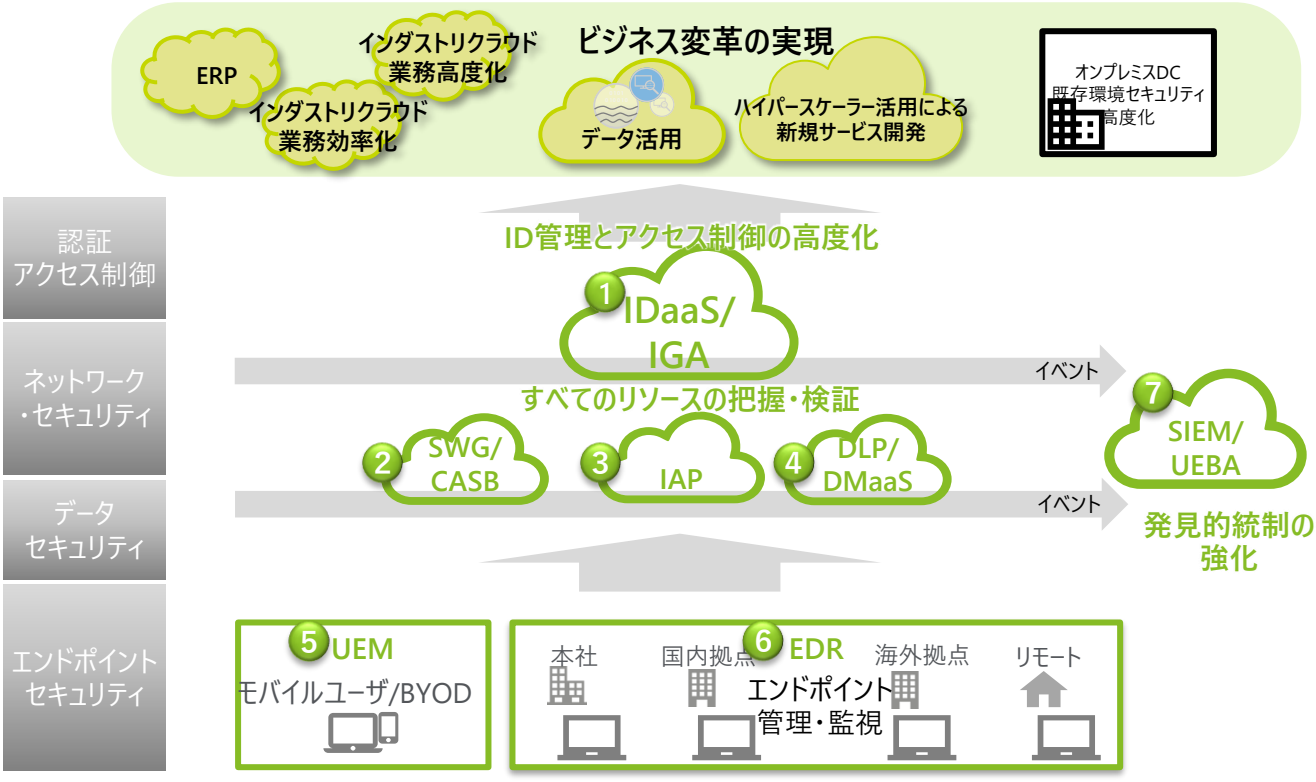

図6：ゼロトラストアーキテクチャ

ゼロトラストへのアプローチはビジネス目標とアラインした投資としての取り組みとすることが成功の要諦である

ゼロトラストに向けて取るべきアプローチ

ゼロトラストへの取り組みについては、大きくは、従来の境界防御モデルからゼロトラストを目指すアプローチと、現状既にサイバーキルチェーン対策をしている状態からゼロトラストを目指すアプローチの、2つのアプローチが考えられる（図8参照）。

日本企業では、欧米と異なり、セキュリティインシデントが実際に発生していない組織において従来の多層防御モデルの状態になっていることがほとんどであり、そもそもセキュリティ対策が不足している状態が多い。このため、標的型攻撃にあっているにも関わらずそれを検知できていないだけというリスクも多い。このような組織においてゼロトラストを目指す検討を始めた場合、ほとんどの組織においてセキュリティにかかるコストが増加することになり、ゼロトラストはコストがかかるので未だ対応する必要はないという結論になることが見受けられる。

また、サイバーキルチェーン対策を行っている企業においては、セキュリティ対策に対して十分コストをかけている自負があるということと、ゼロトラスト実現のために新たなソリューション導入が必要となる場合に、一時的に二重にセキュリティ対策にコストをかける必要が出てくるので、コスト面でゼロトラストへの取り組みを諦めてしまうことが多い。

ゼロトラストへの取り組みは、新たなセキュリティツールを導入することを目的とするのではなく、業務・事業の高度化やビジネス変革の取り組みを進めている中で、ハイパースケーラーやSaaSなどのas a service活用を進められる状態にすることが目的であり、ビジネスのトップライン向上のための投資と捉える必要がある。もし、従来の境界防御型のままで良いと思っている組織があるとしたら、それは、業務や事業の高度化などのdXの取り組みを不要であると言っているのと同義だと理解する必要があるだろう。また、サイバーキルチェーン対策の状態からゼロトラストに向けてコストが掛けられないというのは、コストではなくて「dXの取り組みに向けた投資」を行えないということと同義だと理解する必要がある。

ゼロトラストへの取り組みは長期的な取り組みとなるものの、ゼロトラストを実現できている状態というのは、セキュアな状態でよりビジネスの俊敏性や柔軟性を上げることができる。さらに、サイバーキルチェーン対策における何十ものセキュリティソリューション導入している状態に比べてアタックサーフェスを減らしシンプル化することにつながる。そのため、セキュリティにかかるコストも長期スパンでは削減することにつながることも期待できるものとなる。

このゼロトラストへの取り組みを進める上で組織の経営層が把握するべき重要なことが三点ある。一つ目はビジネス目標とセキュリティ目標の整合、二つ目は段階的なアプローチとすること、三点目はゼロトラスト体制の構築である。

❶ビジネス目標とセキュリティ目標の整合

一点目について、あくまでも、「ゼロトラスト」という冠の付いたソリューションを導入すること自体を目標としてはならないということである。

例えば働き方改革やCOVID-19への対応のためのテレワーク実現や、業務や事業の高度化のために、インダストリクラウドと呼ばれる業界・業種固有のベストプラクティスが取り込まれたSaaSを用いたり、ビッグデータ解析やAI活用、IoTの高度化にハイパースケーラーを用いるとした際、組織全体のプラットフォームがクラウドシフトし、クラウドセントリックなアーキテクチャとなっていく。このビジネス目標と整合する形で、ビジネス変革を実現するプラットフォームに対してセキュリティ投資をすることが不可欠となるのだ。

❷段階的アプローチ

二点目の重要なことは、現状構成から直ちにゼロトラストへ移行できないということである。喫緊課題へ対処しつつ、中長期的視野に基づいた段階的アプローチとすることが不可欠である。ゼロトラストへ向けた段階はおよそ4つのステージで表すことができる。

- ステージ1：コミュニケーションツール導入によるリモートワーク実現など、一部目的のためのデジタル・クラウド活用の状態に対して、オンプレミスとクラウドそれぞれサイロでのセキュリティ対策となっている状態である。
- ステージ2：バックオフィス・ミドルオフィス中心にアズアサービスを活用し業務効率化するなど、ノンコア効率化のためのデジタル・クラウド活用に対して、サイバーキルチェーン対策を強化したり社内認証を一部クラウドへフェデレーションしているような状態である。
- ステージ3：アズアサービス・ファーストにより、コアビジネス推進を迅速化し、認証基盤をクラウドに統合しているような状態である。
- ステージ4：アズアサービス・バイ・デフォルトとして、ビジネスの持続的成長、柔軟性と迅速性を兼ね備えて、経営環境の変化に先回り／アジャイルな取り組みを継続している状態であり、全社の基盤がクラウドセントリックになっているのと同時にゼロトラストを実現している状態である。

特にこの中で要となるのはIDである。デジタルやクラウド活用を進める中では既に境界防御が成り立たず、IDが新たなアクセス境界となるため、ユーザ、デバイス、ワークロード、ネットワークの全てとIDを連携させる取り組みが不可欠となる。ステージ3からステージ4にかけては、従業員、外部協力者等の人だけではなく、APIサービス、AI等の人間外のIDも管理対象とした上で、デバイス管理、クラウドプラットフォーム、ネットワークアクセス制御等、各セキュリティソリューションと、I&AMソリューションを連携し、ポリシーベースでの制御を行うことが求められる。

❸ゼロトラスト体制の構築

三点目の重要なことは、体制である。ゼロトラストはセキュリティソリューション導入だけでは実現できず、セキュリティ組織に加えて、企業組織全体で取り組むべき経営アジェンダとして取り組むことが必要となる。これについては次のセクションを参照されたい。

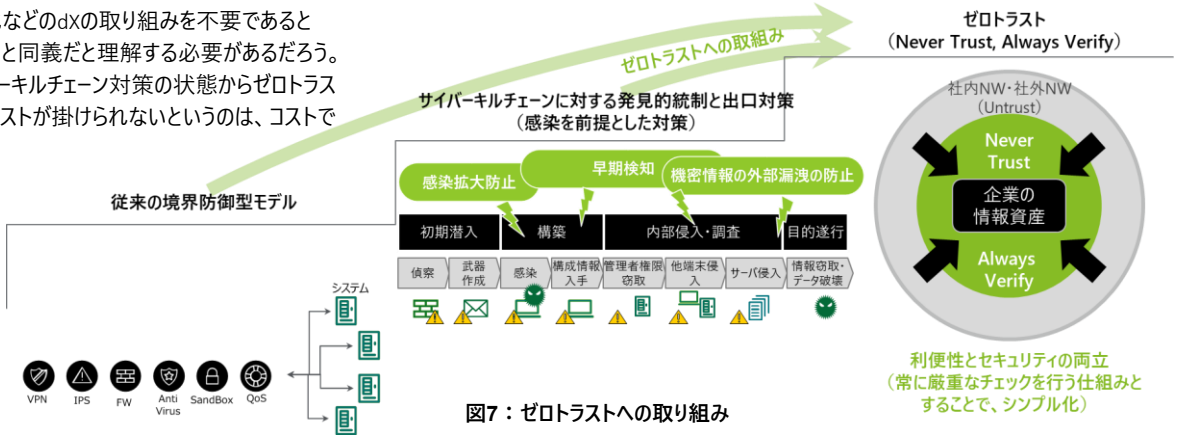

図7：ゼロトラストへの取り組み

ゼロトラスト体制構築は、ビジネス部門とコラボレーションした上で、継続的な取り組みとしていくことが不可欠である

ゼロトラスト体制構築に必要な3つの取り組み

❶サイバーハイジーン（サイバー衛生管理）の強化

体制構築に必要な取り組みの１つ目がサイバーハイジーン（サイバー衛生管理）の強化である。サイバーハイジーンとは、社内のIT資産を日頃から管理し、サイバー攻撃を防げる健全な状態を保つ取り組みのことを示す。基本的なサイバーハイジーンの実践に後れを取っている企業は、ゼロトラストのメリットを十分に享受することが難しい可能性がある。基本的な考え方は以下の通り。

- 構成管理およびパッチ管理・・・悪意のある攻撃者は、あらゆる脆弱性を悪用して 企業内に足場を築くことを狙ってくるため、組織のシステムについてベースラインとなる構成情報をきちんと管理し、適切なパッチ管理、パッチ適用後のテスト実施や、変更された構成情報の文書化を行うことが重要となる。
- IT資産の把握と攻撃可能面の管理・・・アタックサーフェス全体にわたるセキュリティ上の問題を特定できるよう、クラウドリソース、IPアドレス、ドメイン、アプリケーション、リポジトリ、ソーシャルメディアアカウント、そのほか利用している外部サービスなど、すべてのITリソースのインベントリ情報をリアルタイムに更新して管理し、自組織のIT／デジタル環境全体を理解することが重要となる。
- データの把握と分類・・・適切な信頼区間の設定とアクセス制御を行うために、データそのもの、データの重要度、データの格納場所、データの分類、タグ付けの方法と、データにアクセスする必要のあるユーザ及びアプリケーションを把握することが重要となる。
- IDおよびアクセス管理・・・適切なユーザ、デバイス、そのほかの資産に対して、テクノロジーリソースへのアクセスを適切に許可していくために、組織はIDライフサイクル管理プロセスを標準化し、自動化することが重要となる。
- ロギングおよびモニタリング・・・潜在的な悪意のあるインシデントや問題を特定できるようにするために、高度なAI機能と機械学習機能を備え、自動的にログを記録し監視を行う仕組みを整備することが重要となる。
- 第三者リスクの管理・・・自組織のリスクの全体像を完全に把握するため、第三者ベンダーからサプライヤを含めたサプライチェーンやエコシステムのパートナーに関連するサイバーリスクを明確に把握することが重要となる。

❷セキュリティの自動化とオーケストレーション

体制構築に必要な取り組みの２つ目が自動化とオーケストレーションである。セキュリティオペレーションセンター（SOC）チームは、自組織のテクノロジーやセキュリティ対策で大量の情報を扱っており、断片化されたセキュリティアーキテクチャや複数のツールからの連続したアラートやデータストリームを監視し、管理し、対応する必要がある。従来は、インシデントが発生したあとのアラートを頼りにインシデントの原因をログから追うこととなっていたと想定されるが、ゼロトラストを採用することで、リスクベースの認証やアクセス制御を実現することとなり、自動化が可能となる。また、ゼロトラストアーキテクチャ構築には、既存のセキュリティソリューションの活用も可能であるが、不必要で重複するテクノロジーを検出し、システムのセキュリティ保守と管理の複雑化につながるソリューションを排除することが必要となる。これにより、セキュリティスタックを簡素化し、セキュリティ自動化のベースとなるプラットフォームを活用し、システムとツールを統合できるようになる。このプラットフォームはSOAR（Security Orchestration, Automation, and Response）プラットフォームと呼ばれ、コンテキスト情報を追加して脆弱性を自動修正し、遅延なく対応することができるため、SOCチームの運用効率と精度が向上し、応答時間が短縮できるようになる。

❸ビジネスイニシアチブとのコラボレーション

体制構築に必要な取り組みの３つ目がビジネスイニシアチブとのコラボレーションである。ゼロトラストの原則を最初からすべてのビジネスイニシアティブに組み込むために、セキュリティチームとビジネス部門との間でより多くのコラボレーションが必要となる。例えば、業務システムの所有者は、セキュリティ計画にこれまで以上に深い関与を求められるようになる他、正常なシステム動作とアクセス要求をセキュリティチームがより深く理解できるよう、ビジネス部門は、誰がアプリケーションにアクセスし、どのように利用するのかを明示することが求められる。また、ビジネス領域では、アクセス権を制限することや、より細かく制御することなど、システムアクセスについてもっと意識を強めていくことも求められるようになる。

サイバーリスクは、CxOにとって高いリスクである。セキュリティ侵害が企業、株主、顧客に損害を与えると同時に、責任者の辞任につながることもあるからである。これに対し、ゼロトラストは、インフラ、ネットワーク、およびデータをより安全な方法で管理するための最新標準に急速になりつつあるが、その概念には幅広いメリットがあるにもかかわらず、多くの人はそれを単なるテクノロジーの課題だと考えている。これを変えるために、CxOは、今後 1年半から2年の間に、ゼロトラストへの適応を最優先課題と考えるべきである。CxOは、まず組織にとってのセキュリティ上のメリットを明確にし、各リーダーと協力して新しいアプローチの徹底を図り、最終的に、サイバーインシデントの頻度を減らしながら変革と歩調を合わせつつ、リスク体制とプロセスを進化させることが求められる。

そして、サイバーやIT部門から、ビジネス領域のシステム所有者やアプリケーションのエンドユーザまで、さまざまな関係者を巻き込むため、信頼構築が必要となる。

ゼロトラストへのアプローチは長期的取り組みであり、ビジネスの目指す方向性を踏まえてゼロトラストの目指す姿を構想することが変革の第一歩となる

まとめ

ゼロトラスト実現にかかる検討要素は多岐にわたる一方で、さまざまな技術要素に関連性があるため、個別領域ごとに検討を進めていくと、個別最適になるだけではなく、企業IT全体として目指す姿が総崩れになり、ゼロトラストだけでなくその先にあるDXやビジネス変革も失敗することになりかねない。

組織としてゼロトラストというものに取り組まなければならないということは何となくわかっても、具体的に何をすればよいのかということについては疑問や混乱があるようで、日本企業の担当者から実際に「ゼロトラスト製品を紹介してほしい」や「他社のゼロトラストソリューション導入事例を教えてほしい」といった問い合わせをよく耳にする。

日本では、ゼロトラストにかかる大きな誤解があり、特定の新しいソリューションを導入することで、ゼロトラストが実現されるという間違った理解が広まっているように感じる。これは、多くのベンダーが「ゼロトラスト」というキーワードを用いて、自社製品はゼロトラストソリューションであるというメッセージを発信していることに起因していると思われる。

重要なことは、ビジネスとして目指す方向性を踏まえ、ゼロトラストの目指す姿を定義して構想策定を行っていくことであり、近視眼的に既存環境の課題ベースでソリューション導入の追加投資をするかどうかを判断するということではない。全体俯瞰の視点を持てるようにするためには、外部リソースの活用も視野に入れて検討することもよいと考えられる。

例えば、デロイト トーマツがゼロトラスト検討の支援を行う際は必ず新しいビジネスや働き方の検討を踏まえ、ITインフラ環境をゼロトラスト化した場合のイメージをアーキテクチャとして可視化し、その達成に向けたポイントや主要なタスクを明確化するという進め方を行っている。外部リソース活用なども視野に入れながら、全体最適の観点を持ち、ゼロトラストの変革の取り組みを進めていただきたい。

プロフェッショナル

佐藤 岳彦
Technology Strategy & Transformation
執行役員 マネージングディレクター

外資コンサルティングファームを経て現職。
官公庁、金融、製造業を中心に、IT構想策定、全社IT/ dXアーキテクチャ策定、大規模ITプロジェクトのマネジメント等、テクノロジーコンサルタントとしてクライアントの変革を支援。
全社アーキテクチャ、クラウド、セキュリティに関するエキスパート。

メンバー

秋田 修吾
Technology Strategy & Transformation
シニアマネジャー

佐藤 佑哉
Technology Strategy & Transformation
シニアマネジャー

土田 泰徳
Technology Strategy & Transformation
シニアマネジャー

南野 香澄
Technology Strategy & Transformation
シニアマネジャー

関根 淳
Technology Strategy & Transformation
マネジャー

白石 智一
Technology Strategy & Transformation
マネジャー

須藤 正人
Technology Strategy & Transformation
マネジャー

※デジタルトランスフォーメーションを指す用語として、デロイト トーマツ グループでは、デジタルを導入することを主目的とした変革(DX)ではなく、デジタルを道具として駆使し、ビジネス自体を根本的に変革していくBusiness Transformation with digital = “dX”であると定義しています。

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの45万人超の人材の活動の詳細については、 www.deloitte.comをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生したいかなる損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory