経営層に「ゼロトラスト・アーキテクチャー」を理解いただく方法

2021 年 5 月

名和 利男

はじめに

深刻度を加速させているサイバー攻撃が、企業経営に打撃を与えるようになってきていたことを受けて、経営層自らがサイバーセキュリティ対策強化の号令をかけ始める企業を見かけるようになってきた。

そのような企業に共通して見られることの一つは、「セキュリティ対策の実務や現場を預かる方々」（以下、現場の方々）が新たなソリューションの導入を検討しようと、付き合いの長いベンダーから提案を受けたり、独自にインターネットで検索したりするなどして、有効性の高そうなプロダクトやサービスに関する情報を収集する中で、「ゼロトラスト」に関心を持ち始めていることである。

最近、多くのセキュテリィベンダーや IT 関連のメディアが、「ゼロトラスト」について非常に素晴らしい解説を広く提供していることもあり、現場の方々の理解は深まってきていると感じている。特に、筆者が行っている「セキュリティチームに対する能力向上支援」の中で、直近で実務担当者からいただく"ゼロトラスト"に関する質問の多くが、以前とは異なり、その前提や概念を十分に把握されていることが伺える。

セキュリティ実務者の悩みは経営層のゼロトラスト理解

しかしながら、現場の方々が、「ゼロトラスト」を自社内に組み込もうとする努力の中で、さまざまな課題や悩みを持っている。その中でもっとも大きな難題は、「経営層やサイバーセキュリティ対策の責任者からの理解と予算の獲得」である。

筆者が、現場の方々から「経営層や責任者から投げかけられる質問」の一部に対する回答の作成を支援する中で、特に強く印象に残っている「ゼロトラスト」に関するいくつかの質問を紹介する。（一部の語調や言い回しを変えている。）

- 「これまで（多額の予算をつけて）セキュリティ対策を任せていたのに、なぜ、より高額なソリューションを必要と言ってくるのか？」

- 「今あるもの（セキュテリィ対策の製品やサービス）で強化できないのか？ 社員に対するセキュリティ教育を増やすとか、ルールを徹底するなどの方策があるはず。易きに流れているのではないか？」
- 「仕組みは理解したが、業者（メーカー）の言いなりにならず、これ（ゼロトラスト）で本当に効果が出るのかを説明してほしい。」
- 「まずは、社内ネットワークを徹底的に安全にするために実施してきた対策をもう一度見直して、本当に困難であるのかを検証すべきではないか？」

このような発想をしてしまう、あるいはそうせざるを得ない経営層において、相応の背景や理由があるはずであるが、経営層との対話機会が限定的である「現場の方々」が、経営層のメンバーの思いを汲み取り、それに寄り添うことは、そうたやすいものではない。

経営層の思考と視点

それぞれの経営層が置かれている状況は千差万別であるため一概に言えないが、筆者は経営層との対話や支援提供の中で、次のような状況を感じている。

- それぞれの経営層メンバーは、業績に対する責任を強く持っている。その業績は、企業の事業活動という「意思決定の連続」の結果である。そして、（未だ）多くの日本企業の組織階層はピラミッド型であり、そこで行われる意思決定は合意形成が基本となる。したがって、どうしても組織内調整やコミュニケーション量が膨大になり、それらに忙殺されるため、経営層そのものが「変革が芽生えにくい体質」になりやすい。

一部の経営層は、損益管理やリスクマネジメントなどの管理業務に明け暮れている。必然的に、それぞれの業務を簡素化しようとする行動姿勢が生まれ、各部門からの報告や説明を簡潔なものにするよう求め、認識すべき状況を単純に捉えようとする。近年、ますます高度化および複雑化するサイバー脅威によるリスクまでも単純に捉えようとしてしまうと、「重要事項の取りこぼし」や「的を外した方針の策定」をしてしまう恐れがある。

このような状況は、さまざまな企業に対する調査結果にも現れている。たとえば、JEITA（電子情報技術産業協会）が IDC Japan と共同で実施した「2020 年日米企業の DX に関する調査[1]」の結果では、日本

[1] JEITA 2020 年日米企業の DX に関する調査 （2021 年 1 月公表）
https://www.jeita.or.jp/japanese/topics/2021/0112.pdf

企業はデジタルトランスフォーメーション（DX）の目的を業務オペレーションの改善といった「既存業務の収益改善」と捉えている傾向があることが明らかになった。ちなみに、米国企業は、半数以上で経営層が DX の戦略策定や実行に自ら関与し、新規事業および自社の取り組みの外販化などの「事業拡大」を目的とする傾向が見られた。

経営層に「ゼロトラスト」を理解していただく方法

最近のサイバー脅威は、「従来のネットワークの境界防御を"あっさりと"破り、"安全であると信じられていた"内部ネットワークに侵入して、組織内／施設内／家庭内のアプリケーションに不正アクセスする」ことが目立ってきている。このような攻撃の変化を肌感覚で把握している「現場の方々」は、従来のセキュリティモデルからゼロトラストセキュリティモデルに移行することが必要であることを十分に理解している。

しかし、以前の情報セキュリティ脅威を主体的に把握してこなかった経営層が、この変化を直感的に理解することや腑に落ちることはそれほど多くない。特に経営層全体となると、一部で理解することを拒否するような姿勢をとられることもある。

このような状況の改善策について、筆者が複数の企業経営者とディスカッションをさせていただいた際、次のようなアイディアを頂いた。

- 大株主から経営層に対して圧力を与えていただく。
- 事業に影響を与える政府機関（特に規制当局）から強い指針やガイドラインを出していただく。
- 経営層に業界団体や競合他社が取り組んでいる状況と成果を見せつける。

これらのアイディアは、それぞれ相応の効果が期待できるものであると推察するが、残念ながら、現場の方々の努力で簡単に実現できるものではない。

そこで、現場の方々から経営層に対する提案と説明により、実際にゼロトラストへの移行を始めることができた、複数の企業と対話をさせていただいた。いくつかの大きな発見があったが、各社に共通していたのは現場の方々が経営層への説明に「ストーリーテリング」の手法を用いていたことであった。

「ストーリーテリング」手法で経営層に伝える

ストーリーテリングとは、語り手が、相手に伝えたい思いやコンセプトなどについて、印象的な体験談やエピソードなどの「ストーリー（物語）」を引用したり例示したりすることで、聞き手に共感を与え、感情的にアプローチすることである[2]。

筆者も、聴講者や相手の行動変容を促すことを求められる講演やレクチャーの一部において、このストーリーテリングの手法を利用している。

そこで、「ゼロトラスト」をストーリーテリングの手法に基づいて説明をしてみたいと思う。

「ゼロトラスト」ストーリーの基本設計

まず、ストーリーを組み立てるための基本的な設計として、古代ギリシアの哲学者アリストテレスの 7 つのエレメント（要素）に基づ[3]き、ストーリーに盛り込む要素を書き出してみる。

- 構想（Plot：相手は何を達成／克服しようとするのか？）
  - 経営層が、大きく変化した「サイバー環境」と「サイバー攻撃」を理解し、それらに適合した対策（ゼロトラスト）に切り替え、あるいは移行する。
- キャラクター（Character：相手の背景、ニーズ、願望、感情は何か？）
  - 「変革が芽生えにくい体質」の環境の中で、「意思決定の連続」に忙殺している経営層
  - 経営層は、サイバー脅威によるリスクから事業を守りたいと思っているが、「重要事項の取りこぼし」や「的を外した方針の策定」に陥っていることに気づけないことがある。
- テーマ（Theme：相手が達成するために、どのようにして信頼／実感できる存在物／可視化物を確立するか？）
  - ネットワーク境界で防御することができていたが、「サイバー環境」と「サイバー攻撃」の変化が進展したことで、その境界防御が限界を迎えてしまった背景や流れを大局的に（経営層の視点で）可視化する。

---

2 Storytelling That Moves People
https://hbr.org/2003/06/storytelling-that-moves-people

3 Aristotle’s 7 Elements of Good Storytelling
https://public-media.interaction-design.org/pdf/Aristotles-7-Elements-of-Good-Storytelling.pdf

- 対話/語法（Dialogue/Diction：上記の構想、キャラクター、テーマの設計に基づいたストーリーについて、具体的に何をどのように伝えるか？）
    - 「サイバー環境」と「サイバー攻撃」の変化の進展について、語り手が相手と一緒に学ぶ姿勢に基づいて口調にする。
- メロディ/コーラス（Melody/Chorus：上記の構想、キャラクター、テーマの設計に基づいたストーリーについて、どのようなパターンで相手の感情に訴えるか？）
    - ストーリー上の変化による気づきや驚きを示すことで共感を獲得する。
    - 「攻撃する側」と「守る側」の 2 つの人間味のある人物を登場させ、双方の心理戦を追加することでストーリーの流れを作る。
- 装飾（Décor：どのようにして信頼／実感できる存在物／可視化を提示するか？）
    - 境界防御で守られる対象領域（内部ネットワーク）と、脅威主体（攻撃者）が活動可能な領域（インターネット）をシンプルな図（グラフィック）で提示する。
- 視覚的な強い印象（Spectacle：どのようにして相手の記憶に残るように設計を際立たせるか？）
    - 攻撃者は、変化した「サイバー環境」により「セキュリティ上の隙間」が増加していく様子を、装飾として作成する図（グラフィック）上にレイヤー（層）として追加する。
    - 多くの方が、幼少期において楽しんだ「めくり絵（Lift-The-Flap Book）」のイメージを提供する。

この基本設計に基づいた経営層との対話において提供するストーリーを作成すると、次のようになる。

「サイバー環境の変化」ストーリー例

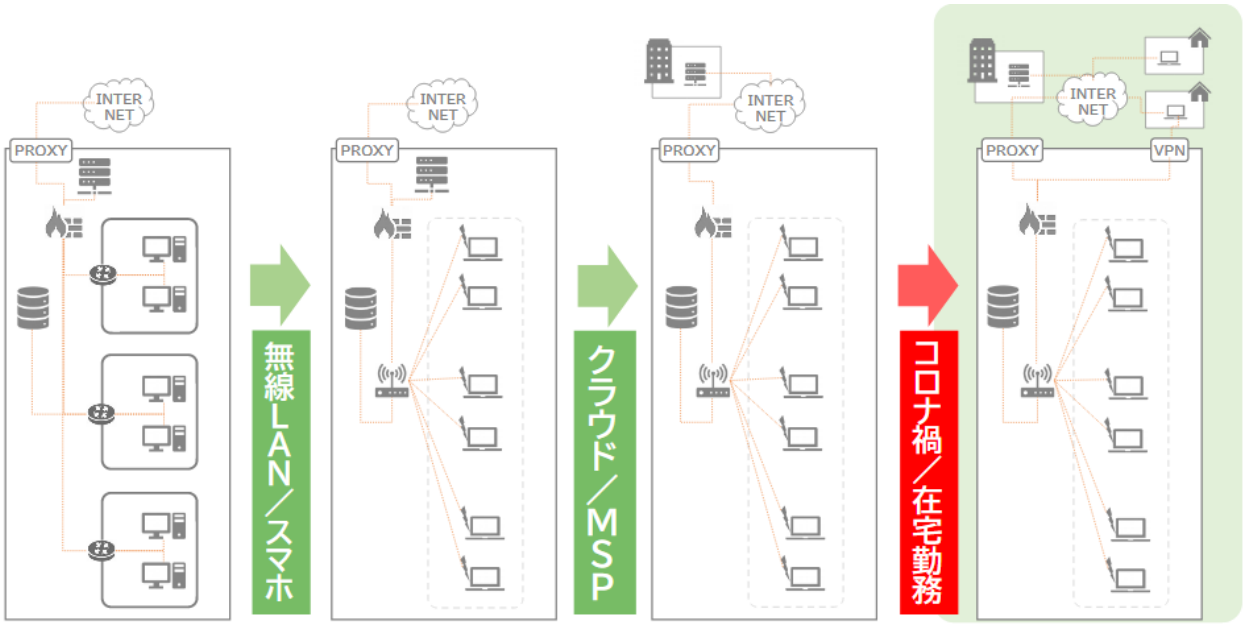

図 1　サイバー環境の変化

1. 日本企業がインターネットを主に業務効率化のために導入した当初、社内ネットワークの構成は、有線 LAN で構築されていた。当時の大半のオフィスは「対応島型」（デスクを対向させて社員同士が向かい合い、端に上長を配置させるレイアウト）であったため、一つの島にネットワークの単位（セグメント）を合わせていた。
    - これにより、IT に詳しくない社員でも、直接視認できる有線 LAN で島単位の境界防御がされている状況を理解することができていた。
2. その後、マーケットの変化や多様化する顧客ニーズに対応するために事業の再構築や新規事業の立ち上げなどにより、オフィス環境が持続的に変化していく中で、有線 LAN が足かせになることが目立ってきた。そこで、テクノロジー進展の恩恵を取り込む形で、低コストで利便性の高い無線 LAN への移行が進んだ。
    - これにより、社内のピラミッド型組織構成に合わせるように構築されていた多層な境界防御を段階的に喪失していった。しかし、このようなセキュリティレベルの低下が積極的に問題視されることはなく、見過ごされていった。
3. さらに、ビジネスのスピートが加速していったことにより、外部拠点や契約会社との連携活動をより効率的かつ迅速にする必要性から、クラウドサービスや MSP（マネージドサービス・プロバイダ）の利用が進んだ。それまで手元のコンピュータで利用していたデータやソフトウェアを、

ネットワーク経由で第三者の企業が提供するサービスを利用することで、より低コストでシームレスな連携を実現することができた。

- これにより、情報セキュリティにおいて最も重要な要素である「管理策（セキュリティコントロール）」において、自社が責任を持って直接対応することが困難な領域が増えていった。

4. 昨年（2020 年）春の突然のコロナ禍により、テレワークを導入する企業が増え、急ごしらえの VPN が増加した。セキュリティ教育が不十分な状態で、社員がさまざまなクラウドサービスの利用を増やしている。また、在宅が多くなったことを受けて、動画ストリーミング、オンラインゲーム、オンラインショッピングなどのプライベートでのインターネットアクセスが増加した。

   - これにより、「管理策（セキュリティコントロール）」が困難な領域に加え、ソフトウェアに依存した仕組みが急増したことで、攻撃対象領域（攻撃者が、ソフトウェア環境にデータの入力や抽出を試みることができる、さまざまな攻撃ベクターの総計）が急拡大した

「サイバー攻撃の変化」ストーリー例

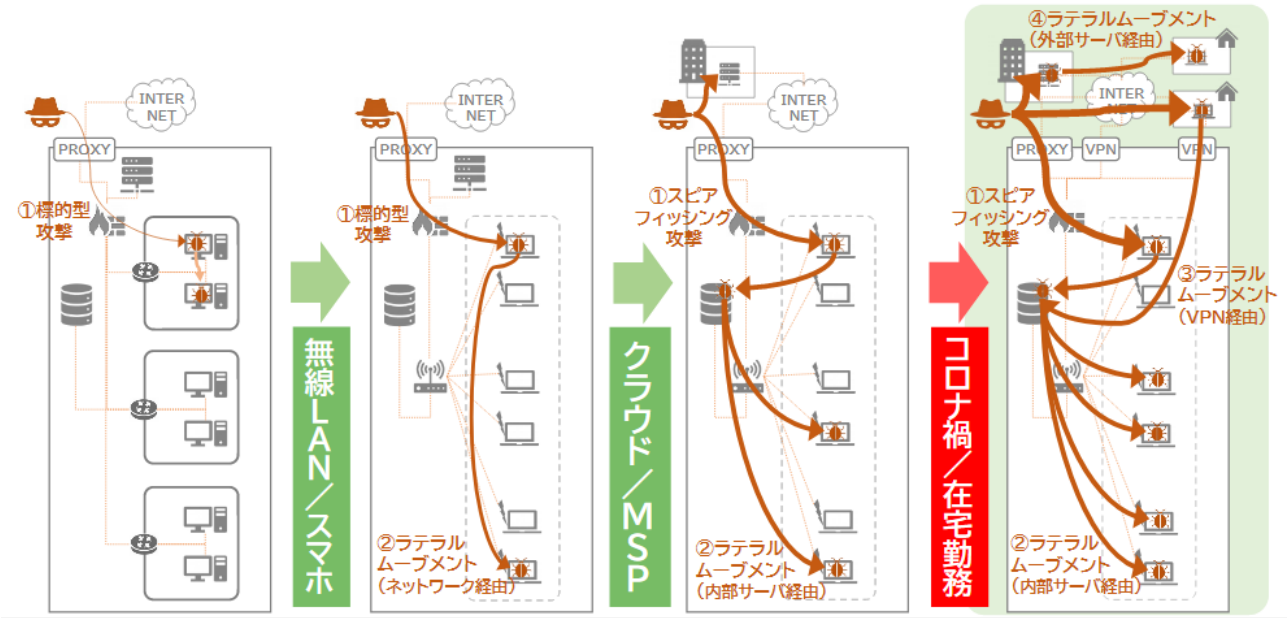

図 2　サイバー攻撃の変化

1. かつて、攻撃対象となりうる会社の内部ネットワークが、オフィス内の島に対応した多層的な構造になっていた場合、フィッシング詐欺メールを送りつけて、受信者に開封させてマルウェア感染に成功したとしても、容易に感染拡大できる範囲は限られており、攻撃目的を達成することは困難であった。

- この段階におけるセキュリティ対策は、ネットワーク上のファイアウォール、端末毎のウィルス対策ソフトなどが基本であった。

2. その後、攻撃対象となりうる会社の内部ネットワークが、無線 LAN に移行したため、マルウェア感染させた端末から感染拡大できる範囲が一気に広がり、攻撃目的を達成することが困難でなくなった。
    - この段階におけるセキュリティ対策として、ネットワーク上のIDS／IPS、SIEM、電子メールゲートウェイなどが加わった。
3. さらに、攻撃対象となりうる会社が、クラウドサービスや MSP の利用を増やしていったことにより、マルウェア感染や不正アクセスを成功させるまでの手段や経路が増えたことで、攻撃目的を達成することが容易になった。
    - この段階におけるセキュリティ対策として、CASB（Cloud Access Security Broker）、EDR（Endpoint Detection and Response）などが加わった。
4. 昨年（2020 年）春の突然のコロナ禍により、攻撃対象となりうる会社が、急ごしらえの VPN を構築したことにより、脆弱性を残存させることが多くなったことで、容易に会社内部へ侵入することができるようになった。また、ネットアクセスの増加にもかかわらず、セキュリティ対策がほとんど行われていない在宅環境に、日常的に侵入することが可能になった。
    - この段階におけるセキュリティ対策は、これまでの「ネットワーク及び端末から悪意のある挙動を検知する」という方向性を持つ機能では限界を超え、多額なコストおよび大量の人的リソースをかけたとしても不可能に近い。そのため、コンピュータ・ネットワークのアーキテクチャー（構造や仕組み）を変革させる必要がある。

以上のストーリーテリングは、一つの例示である。他の観点を取り込むことで、さまざまな体験談やエピソードなどを追加することができる。例えば、「ID 管理の厳格化」、「SNS による情報流通の構造変化」、「スマホアプリによるサービス増加（公的手続き／デマンドサービス／取引・決済など）」、「サイバー犯罪マーケットの活性化」、「国家が支援するサイバー攻撃グループの台頭」などがある。

「ゼロトラスト」の言葉を使わなくとも構造変革は必要

「ゼロトラスト」の理解は、上述のストーリーテリングの最後の話に続く、「内部のネットワークが危険にさられる可能性が飛躍的に高まり、私達はそれを検知することすら困難になってきたこと」を受け入れることができるか否かで、大きく異なってくる。

これを他の観点で言い換えると、以前の情報セキュリティのアプローチは「攻撃者を内部ネットワークから遠ざけることに重点をおくもの」であったが、私たち自らの意思で変えていった「サイバー環境」を守るためにセキュリティ対策を何度も積み上げて努力をしてきたが、「とうとう攻撃者を遠ざけることができなくなった」状況を理解できるかどうか、となる。

一般に、経営層に対して、「ゼロトラスト」の機能を説明するだけでは、適切な理解をいただくことは難しいため、「既存対策の限界と困難な状況になっている実情をまず理解していただく」ことに専念することが重要となる。

最後に、経営層からゼロトラストの端的な説明を求められた場合、「内部ネットワークにおいても、ユーザーまたはデバイスに攻撃者ではないことを証明するように要求する仕組みのこと」のように、その機能だけを説明するのではなく、経営層の視点でサイバー環境の変化をストーリー的な表現で説明し印象付けをすることで、経営層が行う大局的な判断を支援することができると考える。

（了）