ExtraHop

ノイズを乗り越える。

ゼロトラストの導入をエンドツーエンドの可視性と摩擦なしのコラボレーションで加速

公的機関におけるゼロトラスト展開の計画、実装、運用、セキュア化に向けた重要な検討事項

エグゼクティブ・サマリ

あらゆる公的機関において、ゼロトラストの取り組みの重要性が高まっています。ゼロトラスト採用の必要性は明白ですが、成功への道のりはそうではありません。

このホワイト・ペーパーでは、連邦、州、地方の政府機関の IT チームがゼロトラスト・セキュリティ・モデルを展開する際に直面し得る課題について説明します。また、ゼロトラストという必須課題をより迅速に達成するための、実践的な検討事項も提供します。さらに、このガイドラインではエンドツーエンドの可視性と摩擦なしのコラボレーションが、あらゆる展開段階において不可欠の成功要因であることも示します。

目次

はじめに

ゼロトラスト・セキュリティ・モデルの評価と実装に着手している官公庁や公的組織が増加しています。ゼロトラストの導入は、従来型のネットワーク・セキュリティ・コントロール（境界ファイアウォール、侵入検知システム、VPN）がサイバー攻撃やデータ侵害のリスク軽減に関してもはや効果的ではないという認識の表れです。

> **「ゼロトラストはリモート・ユーザや BYOD（Bring Your Own Device）、企業所有ネットワークの境界内にないクラウドベースの資産といった、企業ネットワークのトレンドに対する答えである。」**
>
> **- NIST Special Publication 800-207 - "Zero Trust Architecture" (August 2020)**

公的セクターでは、クラウド・コンピューティングが広範囲にわたり発達し導入されていることから、IT インフラストラクチャの一層のハイブリッド化が進んでいます。もはやユーザやデバイスの信頼性をネットワーク内の位置のみに基づいて判断することは不可能となっており、数十年にわたって利用されてきた多層防御によるサイバーセキュリティ・フレームワークの有効性が損なわれています。

ゼロトラスト原則ではそれに代わり、信頼性（と信頼可能性）がユーザの位置に関係なく動的に決定されます。アクセス特権は、単にひとたびユーザやデバイスの ID が認証されれば与えられるのではなく、継続的に検証されます。アプリケーションやリソースへの認証は精細であり、特定のトランザクションの間に限り必要に応じて持続します。暗黙的に信頼される資産やネットワーク・セグメントはありません。

> **「信頼とはすなわち脆弱性です。セキュリティは『決して信頼してはいけない、常に検証せよ』という戦略に基づいて設計する必要があります。」**
>
> **- Forrester Blog - "A Look Back at Zero Trust: Never Trust, Always Verify" (August 2020)**

新型コロナウイルスの世界的なパンデミックを受け、リモート・ワーカーの数はこれまでになく増加しています。また敵対者が何か月間も発見されずに活動できるという厳しい現実も明らかになっており、これはたとえば 2020 年の SUNBURST 攻撃 [1] のようなサプライチェーン・リスクに関連する事件によって示されています。公的セクターにおけるゼロトラスト・アプローチの必要性は、これらの事実によって一層高まっています。

しかし、効果的なゼロトラスト・ソリューションの実装は複雑かつ困難な試みとなります。単一の製品を展開したり、新しいポリシーや一連の手続きを制定したりするだけでは達成できません。組織が既存のインフラ投資すべてを完全に放棄して新しいゼロトラスト・アプローチを展開するのは不可能であるため、サイロ化していることも多い IT チーム（NetOps、SecOps、CloudOps など）間での緊密な調整・連携が強く求められることになります。

このような事情から、どの公的団体でも当面は、特定のユーザ集団やリソース・グループのみがゼロトラスト・アプローチの下で活動するという、ハイブリッド・ゼロトラスト・アーキテクチャ展開を徐々に発展させていくことになるでしょう。

こうした複数のアクセス・モデルの維持、そしてオンプレミス・システムとクラウドベース・ソリューションとの併用の広がりは、可視性のギャップにつながっています。このように適切な可視性が欠如していると、公的機関が生産性とセキュリティを保つために必要となる状況認識や管理的監視が妨げられてしまいます。

以上のような課題とリスクを踏まえると、ゼロトラストのミッション目標達成を成功させるにはマインドセットのシフト以上のことが求められると言えます。ゼロトラスト・アーキテクチャに対する包括的な可視性や、IT 部署間でのコラボレーションの向上がなければ、ゼロトラスト・セキュリティ・モデルは、保護を得られているという誤った認識をもたらすばかりか、望ましい保護は一切得られないまま生産性に影響を与える混乱を招く恐れすらあります。

エンドツーエンドの可視性や摩擦なしのコラボレーションといった不可欠な成功要因を導入のあらゆる段階で考慮していれば、公的機関はゼロトラストという必須課題をより迅速かつ低リスクで達成することができます。

公共セクターにおけるゼロトラストの促進要因

ゼロトラストは、当時 Forrester Research のアナリストを務めていた John Kindervag 氏によって 2010 年に広められた用語であり[2]、新しい概念ではありません。その起源は数十年前にさかのぼることができます。当時、先見の明を持った IT 組織は、インターネット接続が遍在化すると究極的には企業ネットワークの「非境界化」が生じるという認識に至りました。信頼性、そして信頼できるコンピューティング・リソースへのアクセス権を、企業ファイアウォールの内側にある IP ネットワークに接続しているかどうかでは定義できなくなることが予想されたのです。

Jericho Forum[3] のようなグループがそうした概念を紹介してから 20 年近くが経過する中で、世界は実際に変化を遂げました。ほとんど至る所で高速のインターネット接続が利用できるようになったことから、ネット接続デバイスの数やクラウド・コンピューティングの導入例が加速度的に増加しました。誰もが場所と時間を問わず摩擦なしに働けることは、ただ可能であるだけでなく、今や当然の期待となっています。

> 非境界化が生じた。これは現在も進行中で、不可避である。集中型の保護は有効性を失いつつある。
>
> **JERICHO FORUM COMMANDMENTS**

2019 年 7 月に防衛イノベーション委員会（DIB）[4] が発表したレポートでは、米国国防総省（DoD）のネットワーク全体における「セキュリティとデータ共有の有効性」を確保するため、ゼロトラストへ移行することが必須であると主張されています。

> *「DoD のサイバーセキュリティは重要な岐路に立たされている。当省のネットワークは規模と複雑性が増大している。……こうした拡大により既存のサイバーセキュリティ機構が限界に追い込まれている。ユーザとエンドポイントのますますの増加によってネットワークのアタック・サーフェスが広がっているためだ。……ネットワーク境界内のユーザやデバイスに対する無条件の信頼を継続させることはできない。」*
>
> - "The Road to Zero Trust (Security)" by Kurt DelBene, Milo Medin, Richard Murray (July 2019)

このような新たな現実は、アメリカの軍事関係者に特有のものではありません。連邦、州、地方レベルのあらゆる公的機関が、ユーザの生産性向上に向けたアクセス増加という要求と、データのプライバシーおよび完全性の保護という要件とを両立させる課題に直面しています。

公的セクターにおけるゼロトラスト原則導入の促進要因としては、さらに以下のような事項が挙げられます。

- **IT モダナイゼーションの取り組みに対する要求。**コストの節約、アジリティの向上、サイバーセキュリティ体制の改善といった目標を背景に、公的セクターの CIO は IT インフラストラクチャの統合・最適化に向けた、一層高まる圧力に直面しています。そういった連邦レベルで義務付けられている要件の例には、データセンター最適化イニシアチブ（DCOI）[5] やトラステッド・インターネット接続ポリシー（TIC 3.0）[6] のようなプログラムが挙げられます。このような要求への対応は、結局のところレガシーなオンプレミスの内製システムを放棄することと、パブリック・クラウドや SaaS の代替物へと移行することに行き着きます。モダナイゼーションは多くの利点を伴いますが、一方で組織のアタック・サーフェスを急速に拡大させます。

- **分散したリモート・ワーカーの増加。**新型コロナウイルスの影響で流行が加速する前から、リモート・ワークはすでに拡大しつつありました。Upwork の「未来の働き方動向報告 2020 年版（2020 Future Workforce Pulse Report）」によると、2025 年にはリモートで働く米国人がパンデミック以前の水準と比べて 87%増加し、3,600 万人以上に達します[7]。このような広く分散した働き手に対応する必要から、クラウド・サービスの導入が予想以上のスピードで進んでおり、それによって境界ベースの監視の有効

性が大いに妨げられています。同時期には 5G ネットワークの増強を受けて 5G モバイルの契約者数が 19 億人増加すると予測されており[8]、広く分散した働き手への対応に向けた能力や期待がさらに後押しされています。従来型の VPN やネットワーク境界ベースのセキュリティ・コントロールでは、もはやこのようなトラフィック量に対応し続けることができません。リモート・デバイスからインターネットに向かうトラフィックを検査のためにバックホールすることは不可能になるか、少なくとも非現実的となります。

- **機関の相互依存とデータ共有。**インフラストラクチャ統合の要求と同様のこととして、市民を代表している公的機関は共有とコラボレーションによってサービスをより効果的に提供し、それらの市民に利益を与えることも迫られています。データのポータビリティとアクセスは、そうした取り組みを実現するために欠かせない要素です。電子カルテ（EHR）によって患者のエクスペリエンスが高速化・改善されているのと同様、類似の活動が公共政策の改善を意図して実行されています。あらゆるセクターにまたがったデータ共有が変革的な力を発揮することには疑いの余地がほとんどないものの[9]、アクセスがチェックされないままであれば、プライバシーに関わる重大なリスクも生じます。

- **契約労働者やパートナーに対する依存の増加。**地域の公的機関にさまざまなサービスを提供するためにオペレーションを拡大したことで、サードパーティへの依存が高まっています。短期契約者の追加であるか専門サービス業者の追加であるかを問わず、毎年数百万人の契約労働者[10]が連邦、州、地方の各機関のミッションを支援しています。ますます多くの契約労働者が作業達成のために機密データへの一時的なアクセス権を得て、機関のネットワークにリモート接続していることから、侵害リスクは高まる一方となっています。弱点は利用される恐れがあります。さらに、検出されないままであれば生命を脅かす結果にもつながりかねません。政府機関の契約労働者がサイバーセキュリティ成熟度モデル認証（CMMC）[11]の要件に従わなければならない期限が迫っていますが、そのことからも上述のようなリスクの重大性ははっきりと示されています。

- **モノのインターネット（IoT）とオートメーションの導入の加速。**IoT アプリケーションへの需要は、今後数年のうちに大幅に増大することが予想されています。IoT ソリューションのグローバル市場の規模は、2025 年までに約 1.6 兆ドルに達すると見られています[12]。Gartner によると、そのうち公共安全の向上に向けたソリューションに限っても、2021 年には 170 億ドル以上の支出が見込まれています[13]。その結果として供給されるのが、機密データをネットワーク越しに共有する数百万個のスマート・センサです。公共団体はマシン主導のデータ分析と自動化を採用して、こうしたリアルタイム・データの価値を最大化し、速やかな対応を行わなければなりません。ますます多くの機械学習アルゴリズムやロボティック・プロセス・オートメーション（RPA）・ボットのような「人間以外のユーザ」が、機密データやアプリケーションへのアクセスを要求するようになっています。残念ながら、こうした IoT デバイスやオートメーションの多くは管理されておらず、サイバー攻撃者による侵害の格好の標的になっています。一旦悪用されると、それらは公的機関のトラステッド・ネットワークで横方向に移動するための足がかりとされます。

ゼロトラストの導入が至急必要であることは、上記の事実によって示されています。ネットワーク境界が一旦侵害されると、境界ベースのセキュリティ・モデルでは組織内での横方向の不正な移動に対する保護をほとんど、もしくはまったく提供することができません。

> “ゼロトラストはリモート・ユーザや BYOD（Bring Your Own Device）、企業所有ネットワークの境界内にないクラウドベースの資産といった、企業ネットワークのトレンドに対する答えである。
>
> **NIST SPECIAL PUBLICATION 800-207 - "ZERO TRUST ARCHITECTURE"**

ゼロトラスト・アーキテクチャの実現を成功させるうえでのリスクと課題

どの公的機関にもゼロトラストの採用が必要であることは明白ですが、成功への道のりはそうではありません。

それを始めるに当たって、新しいツールを購入したり、チェックリストの手順をやり遂げたり、新しいリスク管理フレームワークの遵守を証明したりするだけでは不十分です。必要とされるのは、組織の現在のセキュリティ・コントロールやカルチャーを一から再検討することです。また、組織のあらゆるリソースの包括的な特定および分類も要求されます。こういった作業だけでも、IT 部門にとってミッション目標の支援が最優先である場合には難しい注文です。そして以下のような要因により、成功はさらに難しくなっています。

- **対象について知らなければ保護することもできない。**今日の企業インフラストラクチャは複雑であり動的な性質も持っているため、ネットワーク上のデータやネットワークを通過するデータについて知ることは困難、もしくは不可能となっています。どの組織もハードウェア、アプリケーション、データによって構成される膨大なワークフローを抱えており、しかもそうした構成要素はエッジ、コア、リモート拠点、クラウド展開、物理的施設、動員されている人員といった範囲に広がっています。それについて必要な目録を作成する手法は、しばしば手作業であったり、時間がかかったり、不完全であったりします。ある時点でのスキャン結果や Excel のスプレッドシートでは古くなった不適切な一覧しか提供できないため、ネットワーク・セキュリティの盲点が生み出されます。

- **「飛行中に飛行機を組む」必要がある。**基本的にはどのゼロトラストの実装も、既存のエンタープライズ環境の上に展開されることになります。実装作業中における生産性の損失のリスクは、深刻な影響をもたらします。ユーザは自分の職務遂行に必要なアプリやデータに対する、中断のないアクセスを期待しています。手違いや構成ミスがあると、アクセスが遮断されたり、機密リソースが意図せず流出したりする可能性があります。損なわれたユーザ・エクスペリエンス、侵害、悪意のある活動を IT 部署が検出するまでに時間がかかりすぎると、悪影響は非常に大きくなります。

- **ネットワークの境界だけでなくカルチャーの境界にも対処する必要がある。**ゼロトラストには組織全体のコミットメントと、組織のミッションのあらゆる面を隔てる障壁を打ち壊す変更管理プログラムが要求されます。ミッション関係者と IT 部門の間に協力関係がないと、ゼロトラストはミッションクリティカルな要件と見なす必要があるというマインドセットの変化が妨げられます。不正なアクターや悪意のあるソフトウェアによりネットワークがすでに侵害されている可能性がある、という想定を共有することが非常に重要です。また、古くから残る職務上のサイロや IT グループ間の調整不足によってゼロトラストの実装と運用が遅らされてはならない、という了解も同じく重要です。

- **マイクロセグメンテーションに頼るだけでは済まない。**ソフトウェア定義のネットワーキングやマイクロセグメンテーションは、ゼロトラストに対する実践的なネットワークベースのアプローチになり得ます。しかし、多くのマイクロセグメンテーション・ソリューションでは、関与するエンドポイントにエージェントをインストールすることが求められます。このためエージェントを配置できないユーザ、プロセス、デバイス、リソースは制限を受けます。その具体例としては IoT デバイス、BYOD（Bring Your Own Device）資産、ボット、クラウド・サービス、組織が所有していない環境で動作する SaaS アプリが挙げられます。ゼロトラストを機能させるには、保護を減じることなしに調整を施さなければなりません。

以上のような導入に際しての課題は、**完全な可視性**と**コラボレーションの向上**という 2 つの原則によって軽減できます。

> “ゼロトラストは購入するものではありません。セキュリティ・コンセプト、戦略であり、アーキテクチャ設計のためのアプローチなのです。
>
> ACT-IAC WHITE PAPER: "ZERO TRUST CYBERSECURITY CURRENT TRENDS"

ゼロトラストのロールアウト時における可視性とコラボレーションについての検討事項

ゼロトラストの実現は一般的に、計画、実装、運用、セキュア化という 4 つの段階をたどります。各段階について、IT 部門とセキュリティ部門には成功の可能性を事前に高めるチャンスがあります。以下に提供するのは、各段階に対しての考察です。どの段階についても、完全な可視性とコラボレーションが不可欠となります。

計画

広範囲の取り組みを行うときは、計画マイルストーンが重要になります。プロジェクトに投資される予算の 11.4%はパフォーマンスの低さのために無駄になるということが、プロジェクトマネジメント協会（PMI）の最近の調査によって明らかになっています[14]。多くの場合、その根本的な原因は計画の不十分さにあります。またリスクはそれにとどまりません。ゼロトラスト・アーキテクチャ実現計画の不十分さは、予算の無駄以上の結果につながる恐れもあります。公的機関がミッション目標を達成するうえでの致命的な妨げにもなりかねません。

ポリシーを効果的に定義し、適切なセキュリティ・コントロールを選択するには、その前に以下のような点についての可視性が必要となります。

- どのような人やモノが自組織のネットワーク上で通信しているか？
- それらはどのように通信しているか？
- どのような資産がどこに存在するか？
- それらをどのように分類すべきか？
- それらはゼロトラスト環境への参加準備ができているか？

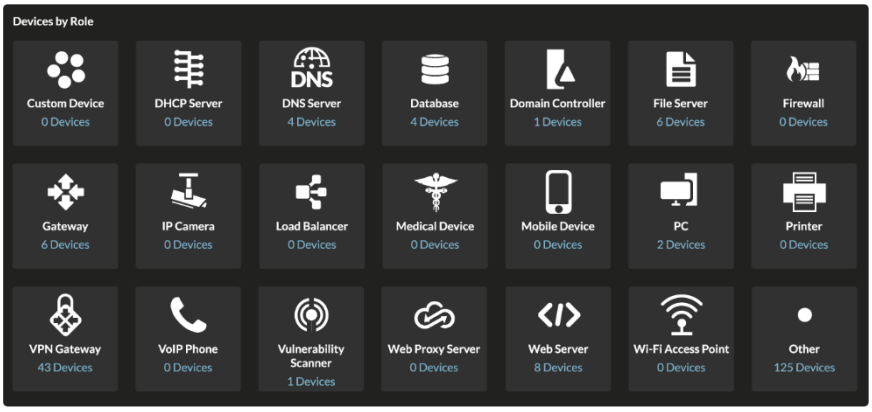
> 自組織のネットワーク上のデバイスすべてを検出可能かという点について、非常に高いレベルの自信があると答えたのは15%にとどまった。
>
> SANS NETWORK VISIBILITY AND THREAT DETECTION SURVEY

以上の質問に対する答えを見つけるには、以下のようなことを行う必要があります。

すべての資産の包括的な目録作成と分類を実行する

計画の最初のステップは、ネットワークで*通信しているもの*、*通信しているべきもの*、*通信しているべきではないもの*をすべて検出することです。この目標の達成に向けては多数の技法がありますが、それらは手作業で、今日の公的セクターの IT インフラストラクチャが持つハイブリッドかつ動的な特性に対処できないことが多くあります。

それに代わって必須となるのが、継続的かつリアルタイムの検出です。加えて、スキャンされたプロファイルだけでなく観察した振る舞いに基づいて検出済み資産を自動的に分類するメカニズムも用意する必要があります。これを達成するための最適な方法は、すべてのネットワーク・トラフィックに対するリアルタイムのフルコンテンツ分析です。レイヤ 2～4 のトラフィックの流れだけでなく、エンタープライズ・アプリケーション・プロトコルに対する完全な理解力を利用して、資産間の通信の特性を把握します。



すべてのワークフローをマッピングし依存関係を把握する

痛みを伴う混乱や意図しない機密リソースの流出を避けるには、ネットワーク中のあらゆるアプリケーション・アクティビティに対する可視性を獲得しなければなりません。それらの関係性のマッピングに向けても、さまざまな技法が存在しています。最も効果的なアプローチは、オンプレミスからクラウドまでのアプリケーション・デリバリ・チェーン全体にわたるエンドツーエンドの可視性を達成することです。

ネットワークベースのトラフィック分析は、あらゆるトランザクションをリアルタイム、客観的、全面的に把握するための最適な手法です。これを高度な機械学習アルゴリズムやコンテキスト分析と組み合わせると、これまで不透明だった関係性は依存関係の明瞭なマップに変わり、ゼロトラストに関わる何らかの改変を施す前にぜひとも考慮に入れるべきものとなります。またぜひ知っておきたいのは、ますます増えている暗号化トラフィック（TLS 1.3 で暗号化されたトランザクションなど）に対処できない手法では、不完全な全体像しか得られないということです。

> “ゼロトラストから恩恵を受けるには、アーキテクチャの各コンポーネントはもちろん、それらがアクセスしているサービスやデータについてまで知る必要がある。
>
> **国家サイバー・セキュリティ・センター（英国）**

ゼロトラストへの準備状況を評価・修復する

ゼロトラスト・アーキテクチャの展開に備えるうえで成功を左右するのは、ID 管理、ポリシー管理、デバイス正常性監視、ネットワーク・セグメンテーションをはじめとする、多数の基本的なコンポーネントが効果的に機能しているかどうかです。脆弱な暗号スイートや期限切れの証明書を使っているデバイスが参加している場合に、それが特定され対処されるようにすることが、混乱や脆弱性の解消のためには不可欠となります。また、日々のネットワーク利用の中で埋もれてしまいがちな、認証メカニズムまたは DNS 解決に関して以前から存在する問題や、その他のよくあるエラー状態について明らかにしておくことも、ゼロトラスト・インフラストラクチャへの準備を整えるうえで大きな効果を発揮します。

こういった検疫やコンプライアンスに関わる活動はスタック全体に影響を与えるため、すべての IT 部署が緊密に連携して、信頼できる唯一の情報源に基づいて作業し、修復が完全に済んだことを確認することが非常に重要です。

実装

すでに述べたように、ゼロトラストは 1 つの製品、ポリシー、手続きを用いるだけで達成できるものではありません。ゼロトラスト・アーキテクチャを実装する段において成否を分けるのは、あらゆる面に対する完全な可視性を持っているかどうかです。実装の際、IT やセキュリティ関連の諸部門が総力を結集するに当たっては、発生した問題のトラブルシューティングのために各チームがばらばらのツールを用いているといった、古くから残るグループ間のサイロを打ち壊すことが必要となります。

ポリシーの確認とマイクロセグメンテーション

最も簡単な言い方をすれば、ゼロトラストとは適切な資産に適切なポリシーをリアルタイムで割り当て、対象（ユーザおよび人間以外のプロセス）やリソース（データ、アプリケーション、サービス）の間の適切な通信を促進することです。簡単そうに聞こえますが、そうした期待通りの結果が設計通りに達成されていることの確認に必要な証拠すべてをつなぎ合わせるのは、なかなか難しいことです。サーバ、コンテナ、ネットワーク・スイッチ、認証サービスからの個々のログを解析しようとすると、これは非常に困難なタスクとなります。

> 一貫したユーザ・エクスペリエンスを維持しましょう。私たちはゼロトラスト・ネットワークへの移行を、ユーザに対する影響を最小限に抑えたものにしたいと考えていました。
>
> MICROSOFT IT SHOWCASE

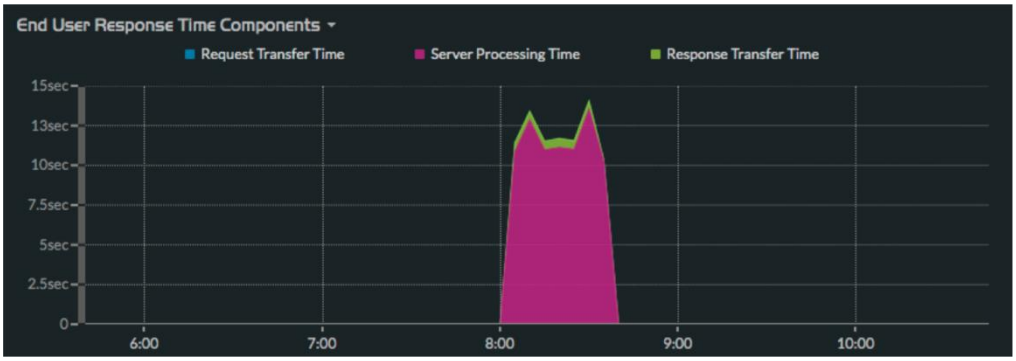
このやり方を改善するには、そういった動作部分すべてを 1 か所から完全に把握できるようにする必要があります。これは生のネットワーク・トラフィックを、ゼロトラスト環境で起こっているあらゆる事象の極めて包括的な記録へと変換することによってのみ達成できます。そうすることで、あらゆる可視性のギャップが解消され、リアルタイム分析に必要な入力や、エンドツーエンドのユーザ・エクスペリエンスに対する実践的な洞察が得られます。

しかし、それで終わりというわけにはいきません。ゼロトラストの実装に欠かせないセキュリティ・コントロールとして、事実上、あらゆるネットワーク・トラフィックは暗号化されることになるからです。期待通りにポリシーが適用されていることの確認は、ペイロードをセキュアに復号化して、そうした通信の整合性やプライバシーをリスクにさらすことなく、カプセル化されたレイヤ 7 プロトコルをディープ解析できる場合にのみ可能となります。

ロールアウトの前、途中、以後のユーザ・エクスペリエンスの詳細な測定値

大部分のゼロトラスト実装はパイロット段階にとどまっていたり、ユーザの一部分のみを対象としていたりします。その理由は多くありますが、1 つ挙げられるのは、ゼロトラストがユーザ・エクスペリエンスに与える影響が明確になっていないことです。自信を持ってゼロトラストを展開するには、ゼロトラストを実施する前に、そうしたエクスペリエンスの基準測定に向けた信頼できる方法を用意する必要があります。ロールアウト段階の最中とその後に詳細な測定値を得ることで、運用開始後の公共セクターの IT チームは、生産性が低下していないという経験的証拠を得られます。

ここまで言及してきたさまざまな要因のため、その達成は個々の監視チームが従来型のツールや手法を使用していると、困難または不可能とすらなり得ます。（インフラストラクチャ全体とアプリケーション・スタック全体、両方の）ユーザ・エクスペリエンス全体のパフォーマンス指標を記録、分析、保持することは、あらゆるネットワーク・トランザクションに対する包括的かつリアルタイムの可視性を通じてのみ可能となります。フォレンジックのための十分なルックバック・データですべての運用チームを支援できるデータセットを収集・保存することは、容易なタスクではありません。チームがある程度のバニティ・メトリクス（見せかけの指標）を得ることで満足してしまうのではなく、この取り組みを完遂するためにより多くを追求することが肝要です。



ユーザ・エクスペリエンスに対する影響を軽減するため、各段階で応答時間を測定する。

損なわれたユーザ・エクスペリエンスの速やかな解決

重たい、またはバグのあるユーザ・エクスペリエンスは、生産性に悪影響を与えたり、組織が義務を遂行する能力を損ねたりする恐れがあります。ゼロトラストの実装中に、IT 運用チーム間で責任がたらい回しにされていると、解決はその分だけ遅れてしまいます。根本的な原因を判断するには、動的にセグメント化されたネットワーク全体にわたるアプリケーション・スタックのさまざまな部分から集められた、ばらばらなシグナルをつなぎ合わせる必要があります。

ログやエージェントに基づいている従来型の監視ツールは、提供できる可視性に制限があり、トリアージとトラブルシューティングを遅らせる盲点につながります。このような事態は、ゼロトラスト・アクセス・ポリシーの適用により複雑性が増したことで、さらに悪化します。

実装作業中のアプリケーションやネットワーク・パフォーマンスの問題をあらかじめ検出・調査して対処するための手段を用意することは、ゼロトラストに対する組織の自信向上にじかにつながります。

運用

運用段階への到達は決して小さくない成果ですが、それはまた、ゼロトラスト・セキュリティ・モデル導入の成功に向けたプロセスの始まりに過ぎないとも言えます。ゼロトラスト環境を運用するということは、上述のような新しい動的なアクセス・ポリシーの継続的な有効性を確保すると同時に、ポリシー適用を遂行するインフラストラクチャの運用正常性も保つことを意味します。ユーザ・エクスペリエンスとすべてのサイバー防御については継続的に監視し、停止についても侵害についても事前的に対処する必要があります。

> “エンドポイントやネットワークのあらゆるレイヤのあらゆるアクティビティに対する完全な可視性を確立し、疑わしいアクティビティを検出できる分析機能を実現する。
>
> NSA CYBERSECURITY GUIDANCE ON ZERO TRUST SECURITY MODEL

完全なカバー範囲とリアルタイムの可視性

公的セクターの IT インフラストラクチャはそのハイブリッド性のため、パフォーマンス関連の問題を監視・診断したり、セキュリティ・リスクを特定したりすることが、すでに十分困難になっています。そのネットワークにゼロトラスト・モデルまでもが重なると、既存のツールやプロセスでは負担に耐えきれず、その有効性が失われてしまう恐れがあります。しかし、エンドツーエンドの可視性はゼロトラスト・モデルにとって最も重要です。

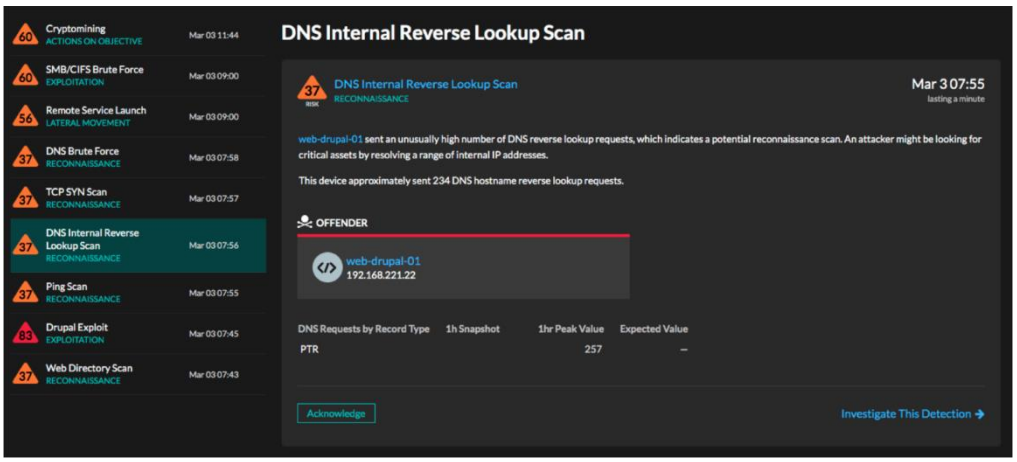
ゼロトラスト導入ジャーニーや IT モダナイゼーションの取り組みのどの段階においても、リアルタイム洞察の最も信頼できるソースとして、ネットワーク自体の代わりになれるものなどありません。最良のアプローチは、たとえ暗号化されていても非構造化パケットをレイヤ 7 に至るまで、ラインレートでパッシブに監視・解析することです。

さらに、ネットワークベースのアプローチを用いると、エージェントを配置できず管理されていない資産を特定・監視できるようになります。ネットワークからはあらゆるものが見えるので、IoT デバイス、VoIP 電話、プリンタ、BYOD エンドポイント、さらにはリモート・ユーザであっても検出・監視できます。

高度な機械学習と行動分析の利用

データ量、ワークフロー・トランザクションの速度、そして公的機関ネットワークに対するリスクの高度化といった要因は、インシデントの特定や、それに対する調査・対応を十分難しいものにしています。それに加えて、後れを取るまいと努めている IT 運用チームはリソース不足で負担がかかりすぎており、本当に大事なことに集中するのがいかなるときも不可能に近いということは容易に察せられます。問題は、数週間または数か月にわたって検出されないままかもしれません。一旦検出された後も、その影響や全貌を評価するのは大変な仕事になるかもしれません。

1 つのより良い方法としては、高度な分析と機械学習を適用して、一見ばらばらに見えるイベント同士を自動的に関連付け、事前的な通知につなげることが挙げられます。アラートを受けた後はインシデントの完全なコンテキストへ即座にアクセスでき、これによって調査と対応が加速されます。こうすることで状況認識や分析者の生産性が向上します。さらに重要な点として、こうすることでゼロトラスト・アーキテクチャの有効性を減じることなく、自信と信頼性を再び得られることが挙げられます。



高度な分析がばらばらのイベント同士を自動的に関連付け、実用的な通知につなげる。

IT 運用部門とセキュリティ部門の間のコラボレーション向上

ゼロトラストは、公的機関の環境のあらゆる側面と関わりを持っています。そして、このように緊密に絡み合った関係性があるために、IT 部門とセキュリティ部門の伝統的なサイロ間で、同様の運用モデルが要求されることになります。

脅威対応のワークフローとユーザ・エクスペリエンスの問題のトラブルシューティングとを合理化することで、公的セクターの IT チームはゼロトラストの取り組みの成功を促進し、かつ確実化できます。可視性や調査に関して同一のツールを使用することに重点を置く、より連携的なアプローチを導入すると、ツールの不必要な氾濫を解消でき、それによって運用コストを削減できます。またミッションの達成と、優れたユーザ・エクスペリエンスの提供との間には障壁が存在する場合がありますが、それも解消できます。

ゼロトラスト環境を支える運用チーム間のコラボレーション向上を支援するには、信頼できる唯一の可視性ソースがハイブリッド・インフラストラクチャ全体、水平方向のトラフィック、垂直方向のトラフィックをギャップや盲点なしに完全にカバーする必要があります。

> “ネットワーク運用チームとセキュリティ・オペレーション・チームは、敵対者ではなくパートナー同士になる必要がある。
>
> SHAMUS MᶜGILLICUDDY, EMA

セキュア化

ゼロトラスト・アーキテクチャのセキュア化も、ゼロトラストが提供を目指している保護にとって不可欠です。ゼロトラストの運用に求められる多数のコンポーネントの可用性と完全性を維持する必要があります。ゼロトラスト環境の機能維持のために IT 運用チーム同士が協力して警戒を続けなければならない領域はいくつもあり、例を 2 つ挙げれば ID ストアが侵害されていないか、ポリシー適用ポイントが正常に稼働しているかといった点があります。

また公的団体は、多数のリスク管理フレームワークやその他の IT ガバナンス要件へのコンプライアンスを証明することも期待されています。ネットワーク化されたリソースの動的なセグメンテーションや、ゼロトラストのその他の副作用は、コンプライアンスについての監査と報告を難しくします。

すでに述べてきたように、保護機構を保護するためには完全な可視性とコラボレーションが重要となります。

継続的な監視と自動化されたコンプライアンス

リアルタイムの状況認識と継続的診断および対策（CDM）は、公的機関が厳格なコンプライアンス要件に対応するうえでなくてはならないものです。リスク管理フレームワーク（RMF）の報告義務や NIST のガイドラインを遵守するには、速やかな回答が必要となります。プライバシー規制には、インシデント対応チームに迅速かつ正確な調査の遂行を迫る、厳格な開示要件がますます含まれるようになっています。さまざまなログに目を通し、手作業のプロセスを踏まなくてはいけないとなると、ただでさえ忙しい IT チームはさらなる圧迫を受けることになります。

境界およびエンドポイントの監視やアセット管理で対応できる範囲には限界があり、あらかじめ管理下に置かれていないデバイスのコンプライアンスを継続的に監視・維持するうえで、助けにはなりません。一方、エージェントを使わないネットワークベースのトラフィック解析アプローチを用いると、パフォーマンスに悪影響を一切与えることなく、ログや人間の力を合わせるよりも高い正確度で、複雑な質問に対する即時の回答を行うことができます。

重要なアラートへの対応

セキュリティ脅威は高度化の一途をたどっており、攻撃者にひとたび内部に侵入されてしまうと、それを検知するのは極めて困難な場合があります。ゼロトラストはそうしたリスクの軽減に大いに役立ちますが、マイクロセグメンテーションが動的な特性を持っていることや、信頼しているユーザの資格情報も侵害されている可能性があることから、どのアラートに即座の対応が必要なのかを知ることはより一層重要となります。

インシデント対応チーム、特にスキル不足に直面しているチームには、検出を行ったり調査の優先順位を決めたりするためのより優れた方法が必要となります。それはつまり、疑わしいアクティビティについてアラートを受けたら、待機中のアナリストに豊富なローカル・コンテキストと、あらゆる検出に対応する直観的な調査フローとを供給することです。そのインシデントについてのトランザクション記録や関連するパケットの提示により、摩擦が軽減され、対応が加速されます。リアルタイムの可視性と高度な行動分析を確保して、関連するイベント同士を自動的にまとめ上げたり、コンテキストを理解したりすることが、こうした目標を達成するためのカギとなります。

既存の投資物の統合と対応の自動化

公的セクターのセキュリティ・チームには、リーン・オペレーションを実行しながら、さらにインシデントの修復にかかる時間を最小限に抑えることが期待されます。それと同時に、ゼロトラストはこれまで投資対象となってきたセキュリティに関する多数のツールやテクノロジを利用します。それらのどれも孤立させて運用することはできませんし、そうすべきでもありません。セキュリティ・インシデントが検出され、早急な対応が必要とされる場合はなおさらです。そこで少ないもので多くを達成することと、自動化を利用することが必要となります。

成功するアプローチの核となるのは、即座にトリガされ完全に自動化された即時の対応を実現でき、さらに手作業の調査・修復も強化できる脅威対応です。そのようなソリューションは、ゼロトラスト・アーキテクチャやセキュリティ・ワークフローのあらゆるコンポーネントに適合し、ファイアウォール、ID ストア、ポリシー適用ポイント、エンドポイントでの検知と対応（EDR）、SIEM システムなどの統合に向けた既定オプションおよびカスタム・オプションを提供する必要があります。

ゼロトラストをクラウド対応ネットワーク検出・対応で加速

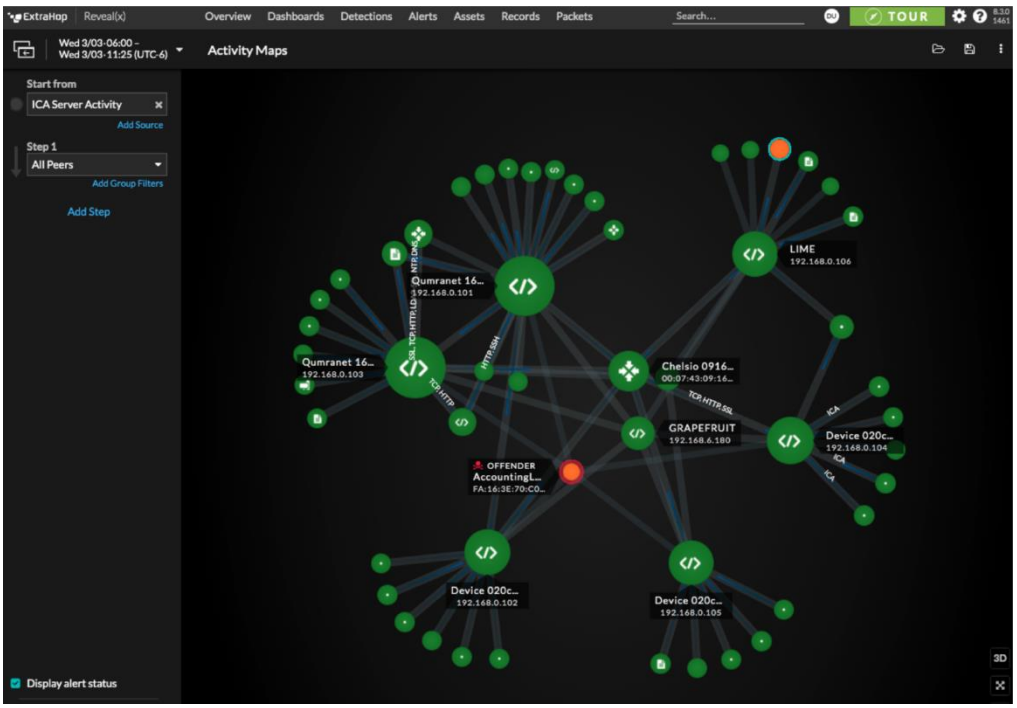
ExtraHop Reveal(x)は公共組織の脅威検出・対応に必要とされるスケール、スピード、可視性を提供し、ハイブリッド・ネットワーク・アーキテクチャ、コンテナ化アプリケーション、クラウドのますますの複雑化によるノイズを乗り越える、唯一のクラウド対応ネットワーク検知・対応（NDR）製品です。

固定のエージェントやゲートウェイ・デバイスに頼った、境界に焦点を合わせるツールとは違い、エージェントレスのネットワーク・トラフィック解析ツール Reveal(x)は、あらゆるネットワーク・インタラクションをパッシブに監視します。その結果得られるのが、IT およびセキュリティ・チームがゼロトラストの目標を達成するために必要とされる、完全なカバー範囲、エンドツーエンドの可視性、リアルタイムの検出、そしてインテリジェントな対応です。Reveal(x)を用いることで、公的セクターの IT 部門は運用チーム間のサイロを打ち壊し、全部分を把握できる一元的な場所と信頼できる唯一の情報源での標準化によって新たなレベルのコラボレーションを実現できます。

自組織のゼロトラスト・アーキテクチャに対する完全な可視性

- ハイブリッド・ネットワーク、クラウド・トランザクション、種々のデバイス・タイプに対する 360 度の可視性をエージェントなしに達成。
- ネットワーク上のあらゆる資産の検出を自動化。
- エンタープライズ IoT を含め、管理されているデバイス、されていないデバイス、未承認のデバイスすべてを特定およびプロファイリング。

> “ExtraHop のおかげで、安全でない接続を容易にサーチ・特定し、いつか問題となる前にその脅威を緩和できます。
>
> **米国立点火施設 CIO、Marvin Christensen 氏**



ゼロトラストの保護機構に対する破壊的な脅威のリアルタイム検出

- サイバー・チーム、ネットワーク運用チーム、クラウド・チーム、DevSecOps チームに向けた単一の統合ワークフローでオペレーションを合理化。
- 高度な機械学習と行動分析を利用して疑わしいアクティビティを検出し、脅威とパフォーマンスの異常を高い正確度で特定。
- SSL/TLS 暗号化トラフィックを含め、ネットワーク・トラフィックを最大 100Gbps でリアルタイムに監視・保護し、セグメンテーションの結果を検証。

ゼロトラスト環境全体を統合するインテリジェントな対応

- カスタマイズしたダッシュボードと、あらゆるインシデントに対してクリック 1 つで得られる関連パケットで、調査ワークフローを加速。
- アナリストの時間を節約し、調査について大きな責任を負えるよう運用スタッフのレベルを自動的に向上。
- CrowdStrike、Phantom、Demisto、Palo Alto Networks などのソリューションと統合し、修復を自動化。

Reveal(x)を用いることで、公的セクターの IT チームは組織のミッションを支援する能力を犠牲にすることなく、より迅速に、自信を持って、コスト効率よく、ゼロトラストのゴールを達成できます。

出典

[1]出典： ExtraHop “SUNBURST: An Origin Story” (January 2021)
[2]出典： Dark Reading: Forrester Pushes ‘Zero Trust’ Model for Security (September 2010)
[3]出典： Visioning White Paper - What is the Jericho Forum? (February 2005)
[4]出典： DIB Zero Trust White Paper: The Road to Zero Trust (Security) (July 2019)
[5]出典： M-19-19: Memorandum for Chief Information Officers of Executive Departments and Agencies (June 2019)
[6]出典： CISA Trusted Internet Connections
[7]出典： Upwork Study Finds 22% of American Workforce Will Be Remote by 2025 (December 2020)
[8]出典： Statista Forecast number of mobile 5G subscriptions worldwide from 2019 to 2024 (May 2020)
[9]出典： Accelerating the Sharing of Data Across Sectors to Advance the Common Good (July 2019)
[10]出典： Marketplace - The U.S. Government is becoming more dependent on contract works (January 2019)
[11]出典： Office of the Under Secretary of Defense for Acquisition & Sustainment
[12]出典： Statista Forecast end-user spending on IoT solutions world from 2017-2025 (January 2021)
[13]出典： Gartner Press Release (October 2020)
[14]出典： Project Management Institute: Pulse of the Profession 2020 (February 2020)

結論

連邦、州、地方の政府機関によるゼロトラスト導入の促進要因は明白です。最初のきっかけになったのは、インターネット・アクセスの遍在化、モバイル・デバイスの増加、クラウド・コンピューティング導入の加速といった新たな現実でした。そして今や公的機関は、広く分散した多様な働き手への対応に向けたモダナイゼーションという、新しい要求に直面しています。また組織間のコラボレーションという新しいモデルも活用するようになっています。管理されていないデバイス、IoT アプリケーション、自動化が爆発的に増加していることを併せて考えると、従来型の境界防御ではもはや不十分であることが容易に察せられます。ネットワーク境界はもはや信頼の判定基準となり得ません。

ゼロトラストの重要性は明白ですが、実装を成功させるためのジャーニーはリスクと困難に満ちています。ゼロトラストは新しいツールの購入や、新しいリスク管理フレームワークの導入によって達成できるものではありません。セキュリティ・コントロール、アクセス・モデル、組織のカルチャーを一から再検討することが求められるのです。こうしたゴールの達成を成功させるには、組織の IT インフラ全体に対する新たなレベルの可視性と、IT 運用に携わるすべてのチーム間での新たなレベルのコラボレーションが必要になります。

エンドツーエンドの可視性や摩擦なしのコラボレーションといった不可欠な成功要因を導入のあらゆる段階に組み込んでいれば、公的機関はゼロトラストという必須課題をより迅速かつ低リスクで達成することができます。

ExtraHop Reveal(x)は公共組織に必要とされるスケール、スピード、可視性を提供する、唯一のクラウド対応ネットワーク検知・対応（NDR）製品です。Reveal(x)は他のツールであれば見逃してしまうような盲点を解消し、公的セクターの IT チームに組織のミッションを支援する能力を犠牲にすることなくゼロトラストのゴールを達成できるという自信をもたらします。

ExtraHop について

ExtraHop は、アクティブな脅威に立ち向かってセキュリティ侵害を阻止できるよう、セキュリティ・チームの武装に尽力しています。クラウド規模の AI を活用した ExtraHop Reveal(x) 360 プラットフォームは、クラウドとネットワークのすべてのトラフィックをリアルタイムで密かに復号、分析し、盲点を解消して、他のツールが見逃す脅威を検知します。継続的に収集したペタバイト規模のテレメトリに高度な機械学習モデルを適用し、ExtraHop のお客様が疑わしい動作を特定して、1,500 万件を超える IT 資産、200 万台の POS システム、5,000 万件の患者の記録を保護できるように支援します。ExtraHop は、ネットワークでの検知と対応における市場シェア・リーダです。当社が最近受賞した業界の賞は、Forbes AI 50、Cybercrime Ransomware 25、SC Media Security Innovator など 30 件に及んでいます。

セキュリティ侵害を 84%迅速に阻止。**www.extrahop.com/freetrial で開始しましょう。**

ExtraHop

info@extrahop.com
www.extrahop.com