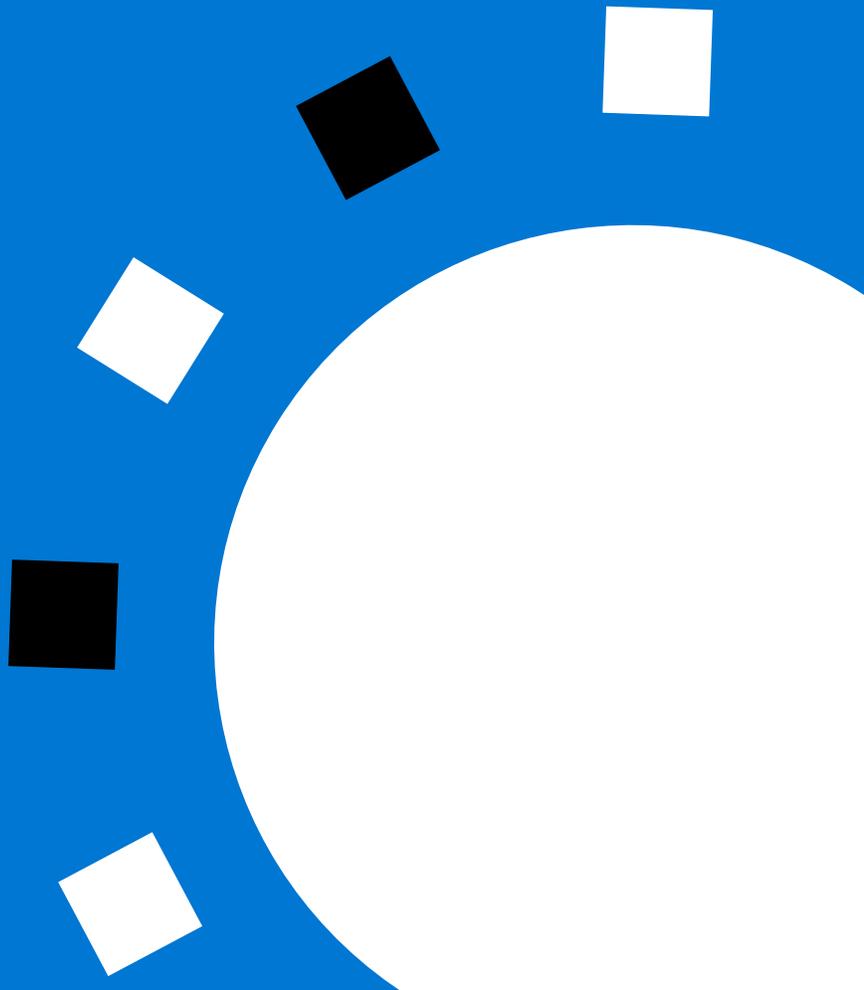


ゼロトラストを 考察する

エグゼクティブによる討論会

討論会について	3
鍵となるインサイト	5
モダン セキュリティのためのゼロ トラスト戦略	7
ゼロ トラストの導入を促進する要素	8
ID を新しい境界と考える	9
コーポレート ネットワークのセグメンテーション	13
デバイスをセキュリティで保護する	15
アプリケーションのセグメンテーション	16
ロールとアクセス制御を定義する	17
ゼロ トラストへの道のり	19
小さく始めて自信をつける	21
フル スタックに拡張する	22
決して信用せず、常に検証する	24
詳細情報	26

討論会について





2020年12月1日、Microsoft とクラウド セキュリティ アライアンス (CSA) はバーチャルでエグゼクティブ討論会を開催しました。この目的は、現状についての対話を持ち、ゼロ トラスト セキュリティのビジョンを伸展させることです。Ann Johnson (Microsoft のセキュリティ、コンプライアンス、ID 事業開発担当 CVP) が進行役を務めたこの討論会には、エネルギー、金融、保険、製造の各分野の傑出した企業でセキュリティを担当しているエグゼクティブ リーダー 10 名が参加しました。リーダーそれぞれの見識に加えて、ゼロ トラストへの道のりを歩むなかで得られた教訓も語ってもらいました。

鍵となるインサイト





この討論会に出席したリーダーたちは、デジタル トランスフォーメーションにおける情報セキュリティの重要性を論じました。情報セキュリティに対する戦略的アプローチの構築について、および全体的な情報セキュリティ態勢向上のためにゼロ トラストの基本的要素を採用することについて、実例も交えてそれぞれの経験を話しました。

このような背景で、参加者が強調していたのは次のトピックです。

- 境界セキュリティの先を考えて、総合的なセキュリティアプローチに移行する。
- ゼロ トラスト導入の行程を進むには、まず小さく開始し、その上に積み重ねていく形で、情報セキュリティの個々の面に対処していく。
- ゼロ トラスト セキュリティの導入を組織全体にわたって向上させる。

モダン セキュリティのための ゼロトラスト戦略

ゼロトラスト セキュリティとは、1つの製品やソリューションのことではありません。

これはモダン セキュリティのための幅広い戦略であり、今日のビジネス環境の複雑さに適応し、モバイルワークフォースを受け入れ、人、デバイス、アプリ、データを、その場所を問わず保護するためのものです。すべての資産を1つの「安全でコンプライアンスも万全な」ネットワークに閉じ込めようとする従来のアプローチとは異なり、ゼロトラストの焦点は資産のセキュリティとコンプライアンスであり、その資産の物理的またはネットワーク上の場所を問いません。

コーポレート ファイアウォールの内側にあるものはすべて安全と信じるのではなく、侵害は起こりうるものと考えて、要求の一つ一つを、未制御ネットワークからのものであるかのように検証します。その要求がどこからのもので、どのリソースにアクセスしようとしているかにかかわらず、ゼロトラストは「決して信用せず、常に検証する」重要性を教示します。

ゼロトラスト戦略を作るにあたっては、まず基本原則と、脅威に対する保護を実現し、その後で二次的な利点（シンプル化など）が得られるようにする必要があります。

基本的な利点

セキュリティ侵害の抑制の向上	32%
脅威の検知と修復のスピードアップ	30%
顧客データ保護の強化	29%

ユーザーの ID からアプリケーションのホスティング環境に至るまで、あらゆるものを使用して侵害を防止します。マイクロセグメンテーションと最小特権アクセスの原則を適用して横方向の移動を最小限に抑え、同時に、豊富なインテリジェンスと分析によって可視性を向上させ、脅威の検知を促進します。何が起きたのか、何が侵害されたのか、どのように再発を防止するかを特定することによって、防御を強化します。



ゼロトラストの 導入を促進する 要素

ゼロトラスト フレームワークを作るには、コントロールとテクノロジーをすべての基本的要素に対して実装する必要があります。その要素とは、ID、デバイス、アプリケーション、データ、インフラストラクチャ、ネットワークです。これらの要素それぞれが、シグナルの発信源であり、施行のコントロール プレーンであり、そして守るべき重要なリソースです。そのため、その一つ一つが重点投資領域でもあります。



ID を新しい境界と考える

この討論会での会話が進む中で、ある重要な気付きが浮上しました。それは、初めにユーザー認証と本人確認の強化に注力する必要があるということです。セキュリティ侵害の多くは資格情報の盗難が関与しているからです。

サイバー衛生が欠如していると、個々の従業員そして組織全体のリスクが増大するため、包括的な ID 管理は、承認されたユーザーのみがビジネス データにアクセスできるようにするうえで不可欠です。



ID を新しい境界と考える

ID を使用してアクセスを制御する

ID (アイデンティティ) は、人、サービス、IoT デバイスを表すものであり、ネットワーク、エンドポイント、アプリケーションの間での共通項です。ゼロトラストセキュリティモデルにおいては、データへのアクセスを柔軟に細分化して制御するための強力な手段となります。どの ID がどのリソースにアクセスしようとするときでも、管理プロセスで次のことを行う必要があります。

- その ID の真正性を強力な認証で検証する。
- アクセスが各種規則に準拠していること、その ID に対して典型的なものであることを確認する。
- その ID が最小特権アクセスの原則に従っていることを確認する。

ある参加者は、強力な ID とアクセス管理から開始することを強調しました。「かつての境界はなくなりました。新しい境界は ID であり、検証された強力な ID が必要です。ここからプロジェクトが始まりました。アクセス管理は手作業ではできないため、自動化されたプロセスとなることは必須です。適切な自動化と適切なログインならば、期待どおりに機能します。」





ID を新しい境界と考える

認証をレベルアップさせる

組織の情報セキュリティ態勢を大幅に向上させる方法があります。それは、多要素認証 (MFA) または継続的認証を ID 管理戦略に組み込むことです。このアプローチの力を、討論会の参加者の一人が強調しています。この参加者の組織では、ID 管理を継続的認証プロファイルで拡張することによって、今では ID の検証を、ユーザーの IP アドレスや日常的な行動パターンが変化したときでもできるようになりました。

ID を現場オペレーショナル テクノロジで確立することに関連して、ある参加者に「対応する必要がある重要な ID は、人間とマシンのどちらであるか」という質問がありましたが、その答えはこうでした。「両方です。人間、特に技術者が、現場に向いて多要素認証を有効にする必要があります。以前は簡単なことではありませんでしたが、今ではとても簡単にできるようになりました。これで、最大の問題はマシンツーマシンの認証となりました。人間がいなくときに、2 番目の要素をどう要求しますか?」





ID を新しい境界と考える

パスワードレス認証を取り入れる

ゼロトラストの進化に伴い、生体認証やその他のイノベーションを情報セキュリティに対するモダンなアプローチの一環として使うことが一般的になってきています。MFA の形態の一つであるパスワードレス認証は、従来のパスワードを安全な代替手段で置き換えるものです。この種の認証では、2 つ以上の検証要素が必要であり、これらは暗号キーペアで保護されます。デバイスが登録されると、公開キーと秘密キーが作成されます。秘密キーのロックを解除する方法は、ローカルなジェスチャー（たとえば PIN や生体認証）のみです。ユーザーは、生体認証（指紋スキャン、顔認証、または虹彩スキャン）で直接サインインするか、デバイスのロックと保護に使用されている PIN でサインインするかを選択することができます。

パスワードレス認証がゼロトラストの有効性に与える影響について質問したところ、ある参加者はこう答えました。「向上させると思います。1 年にわたる Microsoft Windows Hello の概念実証を経て、現在は全社的に展開しています。ゼロトラストは、エンドユーザーにとって透明でなければ機能しないため、簡単で透明性の高いものにする必要があります。認証を実施したい間隔が 5 分でも 1 秒でもかまいません。エンドユーザーが何もしないで済むならば、これには、その他の方法で検証できることが条件になります。たとえば、エンドポイントを MFA の要素の 1 つにすることができます。」





コーポレート ネットワークのセグメンテーション

ネットワーク セグメンテーションは、この討論会での議論が白熱したトピックの 1 つです。ある参加者は、セグメンテーションをしすぎると事態が悪化するという信念を持っていました。さまざまなパーツごとに設計し、境界ネットワークをセグメンテーションするということを始めると、もはやフラットな IT ネットワークではなくなってしまいます。これは、企業の IT 担当者にとって悩みの種となっています。ファイアウォールはセグメンテーションの始まりであり、その結果として、開発とテストに困難がつかまとうことになるためです。結局、IT チームはセキュリティ チームに依存しなければ、ネットワークング、接続性、アクセスの問題を解決できなくなります。

しかし、モバイルとクラウドを最優先する世界では、ビジネスに不可欠なデータへのアクセスはすべて、ネットワーク インフラストラクチャを経由します。ネットワークングの制御は、可視性を高めるための、およびネットワーク内での攻撃者の横移動を防ぐための重要な機能となります。つまり、組織は引き続きネットワークをセグメント化するとともにネットワーク内のマイクロセグメンテーションをより深く実施することに加えて、リアルタイムの脅威対策、エンドツーエンドの暗号化、監視、分析を導入する必要があります。

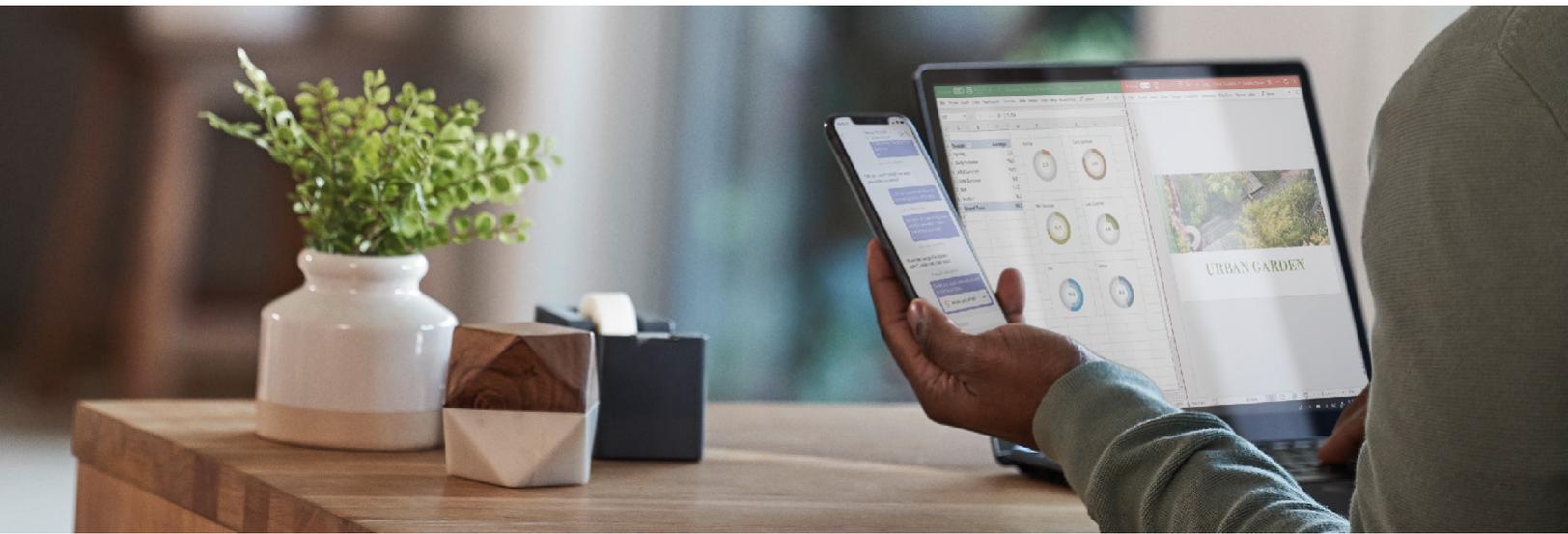
ある参加者はこう述べています。「まず、ネットワークのマイクロとマクロのセグメンテーションを行いました。データセンターとオフィスから開始し、続いてアプリケーションをセグメント化しました。これで、ユーザーが VDI や VPN を介してアクセスしてきたときに、特定のアプリ スタックだけを使うように制限できます。この方法で（ユーザーを）セグメント化しておけば、VPN に到達したユーザーに白紙委任アクセスを許してしまうことはありません。」



セグメンテーションについての議論をさらに進めて、参加者に「ゼロトラストフレームワークはオンプレミスの資産にも拡張できるのか、それともクラウド環境だけに留める方が良いのか」と質問しました。その答えとして、ある参加者が次のように自身の経験を語りました。「私たちはオンプレミスから開始し、今後もこれを維持します。横方向への移動防止などのためのマイクロセグメンテーションに必要だからです。オンプレミスについては何も変わらず、今はクラウドへと拡張しているところです。金融サービス業である私たちは、すべてをクラウドに移行するつもりはありません。常にオンプレミスとクラウドを組み合わせることになります。これから考える必要があるのは、さまざまな境界すべてをこれからどうするのか、このパラダイムをどうやって全体に広げるかです。」

別の参加者は次のように述べています。「私のところでも、最初に多くのマイクロセグメンテーションと NAC を行いました。次の VLAN をまったく信用していませんでした。ファイアウォールを通過しなければなりません。認可を受けていなければ、そこに到達できません。そこで必要になったのは、セグメントからセグメントへと確実に移動できるようにすることです。その移動は双方向、一方向で。そこが真のスタートでした。」





デバイスをセキュリティで保護する

現代の組織は、データにアクセスしようとするエンドポイントの多様さに向き合わなければならない、ということに異論の余地はないでしょう。その一方で、討論会の参加者の一人はデバイスそのものが軽視されているという懸念を示しています。すべてのエンドポイントが管理対象とは限らず、場合によってはその組織の所有でもないため、結果として、いくつものデバイス構成とソフトウェア パッチレベルが存在するという状態に陥ります。先に述べたように、ゼロトラストの原則は「決して信用せず、常に検証する」です。エンドポイントに関して言えば、すべてのエンドポイントを常に検証するということです。請負業者、パートナー、ゲストのデバイスだけでなく、従業員が仕事のデータにアクセスするために使用するアプリやデバイスも含まれます。デバイスを誰が所有するかを問いません。

ゼロトラストモデルでは、デバイスが会社所有でも個人所有でも同じセキュリティポリシーが適用されます。また、デバイスが完全にITの管理下にあるか、アプリとデータだけがセキュリティ保護されているかを問いません。ポリシーはすべてのエンドポイントに、つまりWindows PC、Mac、スマートフォン、タブレット、ウェアラブル、IoTデバイスに適用されます。そのデバイスがどこから接続するか、つまり安全なコーポレートネットワークか、家庭用ブロードバンドか、公共のインターネットかを問いません。

デバイスのセキュリティに関する議論の中で、ある参加者が特に説得力のある例を挙げました。「BYODの世界では、デバイスは爆発物扱いです。パッチ未適用のデバイスにネットワークへの接続を許可すると、不発弾を持ち込まれるようなものであり、即座に悪い方向に進んでしまいます。ですからまず、外でテストすることをおすすめします。時間とともに、人々はセキュリティ対策（たとえばデバイスのパッチ適用）を指示されることに慣れ、当然のものと考えようになります。ユーザーはリマインダーを予期してデバイスのセキュリティを保つようになります。」



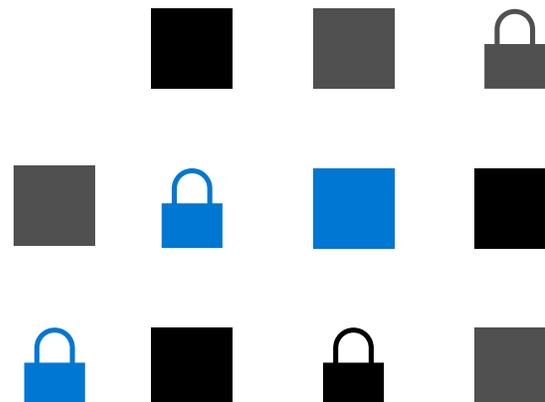


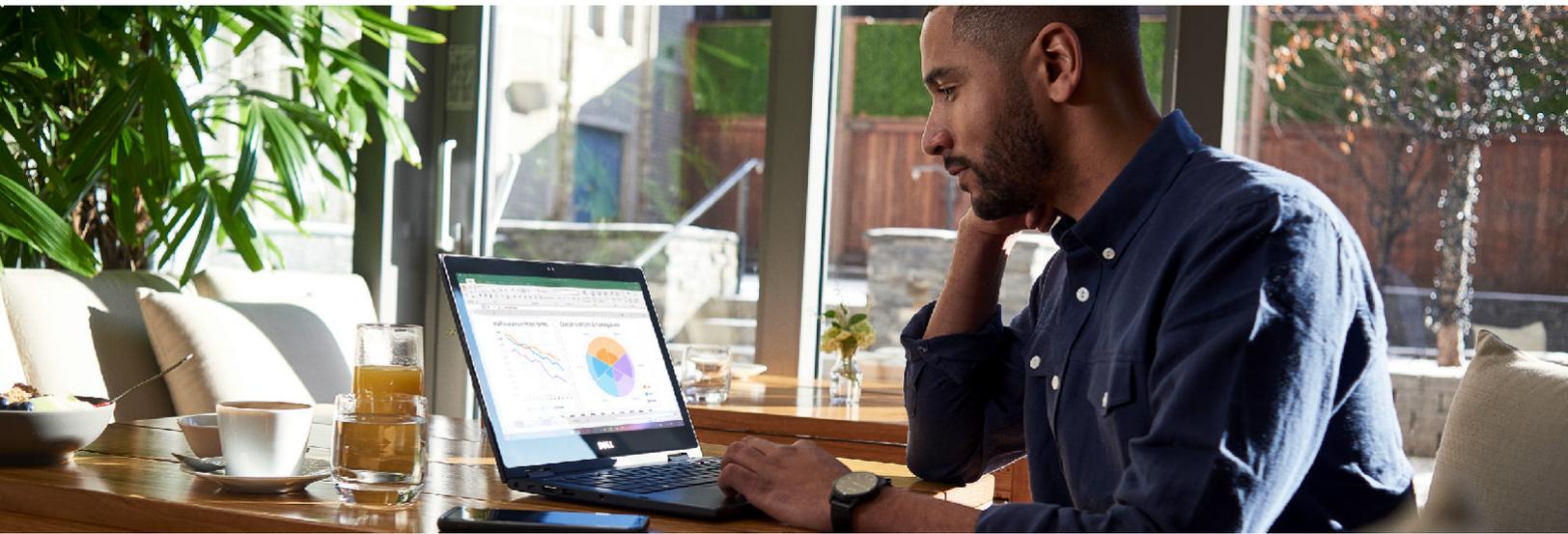
アプリケーションのセグメンテーション

特筆すべきは、討論会の参加者の何人かが、アプリケーションレベルのセキュリティに関する懸念に会話を誘導したことです。その中で強調されたのは、SaaS でもデータセンター内でも、アプリケーションに対するアクセス許可のサイズを適切にすることです。このことは、ゼロトラスト戦略の実行を成功させる上で重要な役割を果たします。

確かに、クラウドのアプリやサービスの利点をフルに活用するには、アクセス権を与えることとコントロールを維持することの間で適切なバランスを取る必要があります。アプリと、その中のデータを確実に守るためです。コントロールとテクノロジーを適用してシャドウ IT を発見し、アプリ内のアクセス許可を適切に与え、リアルタイム分析に基づくアクセス遮断を行い、異常な行動を監視で探し、ユーザーのアクションを制限し、安全な設定オプションを検証します。

ゼロトラストへの道のりについて議論する中で、ある参加者がアプリケーションのセキュリティに関する考えを述べました。「アプリケーション間のセグメンテーションがさらに簡単になり、達成しやすくなってきています。過度の特権/ロールベースアクセス権を提供できることが、ポリシーエンジンの一部になりつつあります。このパズルにおけるアプリケーションというピースは、時とともに、よりインテリジェントに自己解決されていくように思われます。このアプローチが正しいことは、エンドユーザーが問題を特定できると聞かたびに確信できます。」



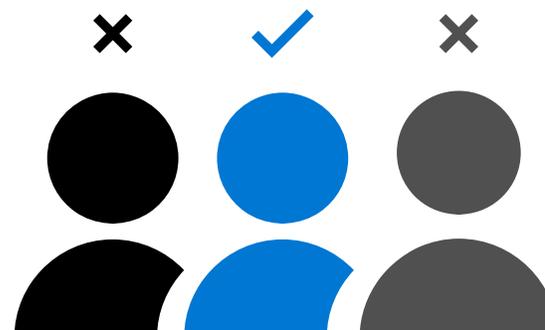


ロールとアクセス制御を定義する

今日の最も差し迫った問題である、リモートワークの急増についてはこの討論会でも多くの時間が割られました。多くの従業員がリモートで働いている現在、組織はモダンなセキュリティコントロールを実現するための代替手段を検討する必要があります。ある参加者はオペレーションに真正面から焦点を当て、ユーザーのロールをポリシーで管理することは情報セキュリティのパズルの重要なピースであると述べました。この考えが展開され、議論は効果的なロール管理の必要性にまで及びました。ロールをポリシーに結び付けることを、認可、シングルサインオン (SSO)、パスワードレスアクセス、セグメンテーションなどの一部として行うことについてです。

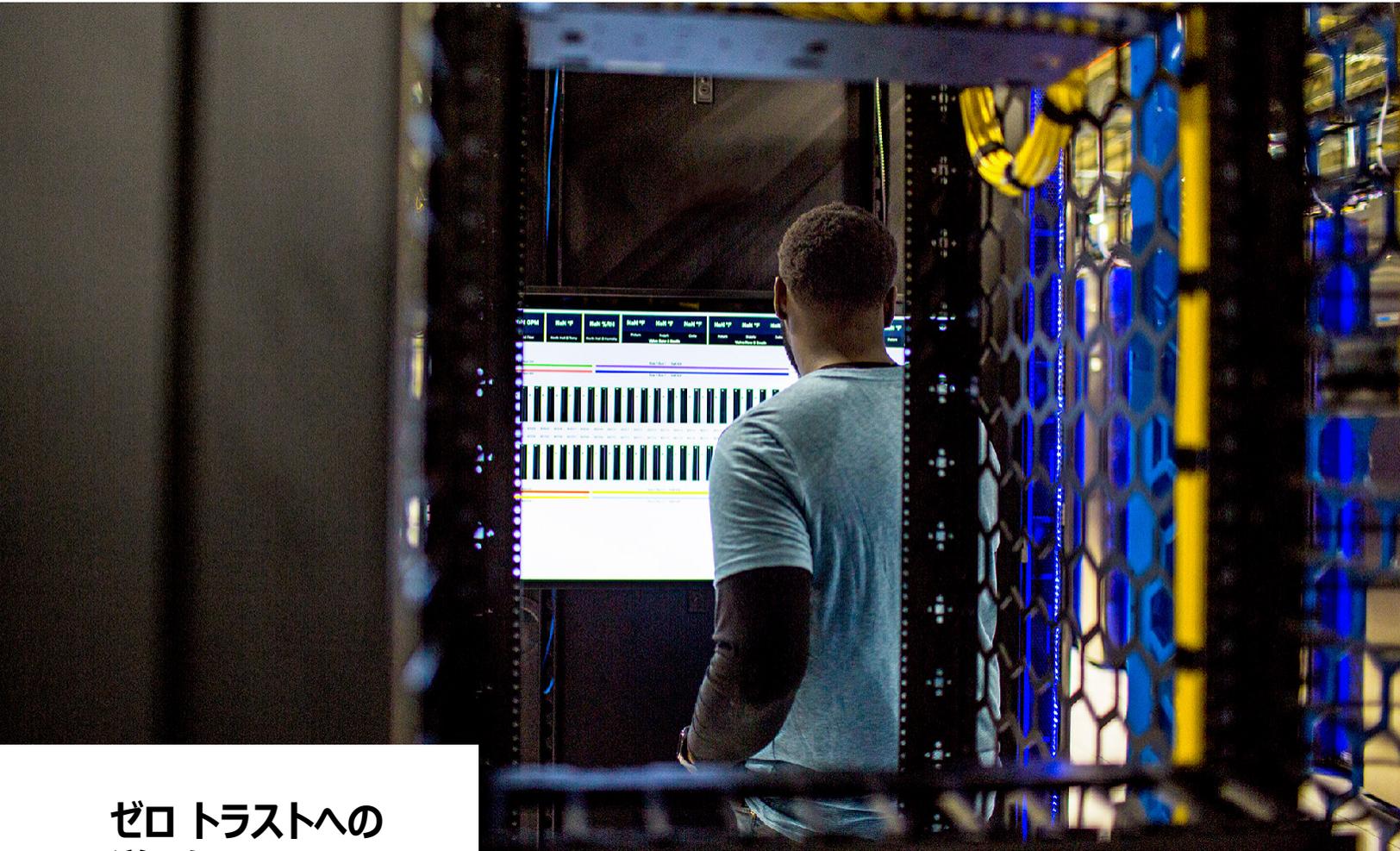
そこで気になるのが、ロールをオペレーションレベルで管理すること、ポリシー管理に結びつけることはどれだけ効果的であるか、という問題です。ある参加者によると、ロールをオペショナライズすることは実際に不可欠です。SSO やパスワードレス機能を実現するには、適切なロールが定義されていないからなんです。しかし、この参加者はロールを増やしすぎることに反対の立場を取っています。定義されるロールはどれも、その管理が現在だけでなく将来も必要ですが、このことは無秩序とリスクを生み出す可能性があります。ロールが監視されずに放置されたり、必要以上の特権が与えられたりする可能性があるからです。

ロールを効果的に定義することについて、ある参加者の意見です。「認可の粒度を非常に高くしたいと考えるかもしれませんが、その粒度に達するために 1,000 個ものロールを組織内に作成することになれば、将来的に管理の問題が発生するでしょう。最終的には膨大な量のアカウントが更新されないままになり、そこで侵害が発生することになります。たとえば、組織内で異動したときに、それまでの特権を（不要になったにもかかわらず）新しいロールにそのまま持ち込むような場合です。」





別の参加者が、ロール管理の進化の可能性について興味深い見解を述べています。「ロールの未来は、属性ベースの管理からトークンベースの管理になり、最終的にはロールをトークンに合わせることになるでしょう。ユーザーに割り当てられているトークンは、どのタイプでもかまいません。どのトークン スキームを使用するかによります。ロールの未来は、これに合わせることになるでしょう。ロール管理は非常に重要であり、それが理由で、継続的アクセス制御/継続的アクセス管理が不可欠です。」



ゼロトラストへの道のり

討論会の参加者がそれぞれのゼロトラストの経験を、どのように始めたか、そして現在どこまで進んでいるかという点から話さず、いくつかの共通するパターンが浮かび上がってきました。最も関心が高かったのは、情報セキュリティの範囲を理解して出発点を特定することの必要性でした。ある参加者は、ゼロトラストの行程をユーザーのIDとアクセス管理からスタートし、他の参加者はネットワークのマクロとマイクロのセグメンテーションから開始し、さらに別の参加者はアプリケーション側を検討しました。最終的には全員が、ゼロトラスト成熟状態である「誰も、何も信用しない」に向けて進んでいます。壁の内側でも外側でも、エンドポイント上でも、サーバー上でも、クラウド内でも。全員の意見が一致したのは、ゼロトラストが進化するにつれて、終着点がないという認識も強くなったことです。つまりこれはずっと続く旅のようなものです。

ある参加者は、ゼロトラストセキュリティへの道のりをID管理から開始したと述べています。SSO機能を導入したいと考えていましたが、この機能を在宅勤務にも拡張できることに気づきました。

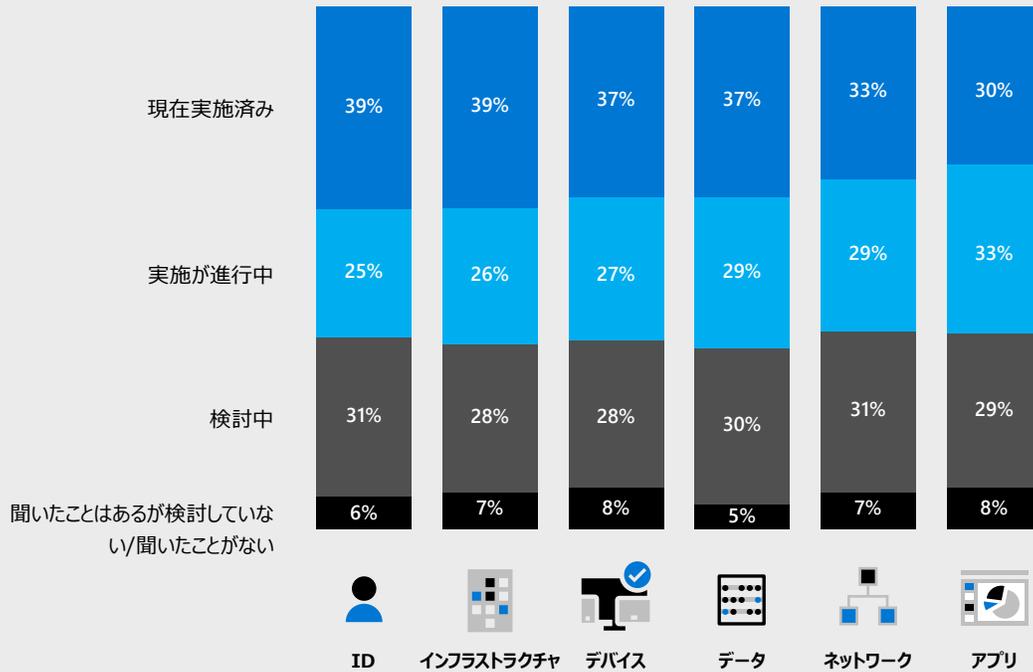
ゼロトラストに取り組むための総合的な戦略を立てることは、きわめて重要です。ゼロトラストに向けた適切な行程を定義して実行するためには、会社としての優先事項、テクノロジー、プロセス、さらには変更の影響を考慮する必要があります。

この討論会での一致した見解:

小さく始めて、自信をつけてから、ゼロトラストを組織全体にロールアウトすることによって最適な保護を目指します。

ゼロトラストはエンドツーエンドの戦略であり、すべての柱にわたって実施されます

ゼロトラスト アクティビティの現状
合計 (n=300)





小さく始めて自信をつける

組織の要件、既存のテクノロジ、セキュリティのステージのすべてが、ゼロトラスト実施の計画に影響します。ゼロトラストセキュリティが最も効果を発揮するのは、デジタル資産全体にわたって統合されたときですが、多くの組織では段階的なアプローチが必要となります。つまり、その組織のゼロトラスト成熟度、利用可能なリソース、優先順位に基づいて、特定の領域を対象とすることになります。投資のそれぞれが慎重に検討され、現在のビジネスニーズに沿ったものであることが必要です。その行程の第一歩が、クラウドベースのセキュリティツールへの大規模なリフトアンドシフトである必要はありません。

同様に、ゼロトラストを開始するためにインフラストラクチャを完全に再構築することも必要ありません。最も成功するソリューションとは、ハイブリッド環境を覆うレイヤーとなってその環境をサポートするものであり、既存の投資を完全に置き換えるものではありません。

組織の規模にかかわらず、ゼロトラストの導入は小さな部分から始める必要があります。複数の大きな変更を同時に完了しようとするのは、現実的ではないことが多いからです。成功を達成できるのは一般的に、クラウドでの新しいグリーンフィールドプロジェクトから開始するか、開発テスト環境で実験するという方法を取った場合です。

ある参加者は、小さく始めることについて、次のように意見を述べています。「最も重要な部分から始める必要がありますが、すべてをやらうとしないでください。ゼロトラストを展開しながら、他の複数のことを同時にしようとするのは不可能です。」

別の参加者は、大組織を説得してゼロトラストを小さく始めさせたという実体験を紹介しています。「ある大手銀行とのワークショップを開催し、小さく始めましょうと提案しました。その返答は、『小さく 5,000 人で始めます』でした。先方の感覚ではそれでも小さいのですが、私は『最初は 50 人で』と答えました。銀行側は同意せず、約 2,500 人で開始しました。約 8 週間後、その銀行から再び連絡がありました。スコープの再評価を希望しており、パイロット計画はどのようなものになるかと言うのです。その銀行は 25 人で再スタートしました。現在 2 年目になりますが、確実に前に進んでいます。」

フル スタックに拡張する

最初の一步を踏み出して自信がいたら、ゼロ トラスト モデルをデジタル資産全体に拡張しますが、同時にこのモデルが、統合型のセキュリティ哲学となりエンドツーエンド戦略となる必要があります。ゼロ トラスト戦略をフル スタックに適用するときは、完全なセキュリティ態勢をカバーする必要があります。

アクセス要求それぞれについて、アクセス権を付与する前に強力な検査を行い、異常の有無を調べる必要があります。ユーザーの ID からアプリケーションのホスティング環境に至るまで、あらゆるものが認証と認可の対象となります。マイクロセグメンテーションと最小特権アクセスの原則を使用し、これによって横方向の動きを最小限に抑えます。

要約すると、ゼロ トラストのセキュリティ モデルを一様に、包括的に実装するには、基本の要素のすべて、つまり ID、デバイス、アプリケーション、データ、インフラストラクチャ、ネットワークのすべてを考慮する必要があります。また、以下の検討事項にも対処する必要があります。

- リソースにアクセスしようとするすべてのユーザーとデバイスについて、対象リソースにアクセスするのに十分な信頼性があるかどうかを検証する必要があります (対象リソースの秘密度に基づいて)。
- 組織のポリシーをすべてのリソースに一様に適用するために、単一のゼロ トラスト ポリシー エンジンを使用します (エンジンが複数の場合はそれぞれの構成が異なる可能性があります)。
- 信頼性の判断に含まれている測定項目のうち、通常の行動を反映するものが多いほど、攻撃者にとっては正当なサインインの試みとアクティビティを模倣することが困難になり、コストも高くなるため、攻撃者の損傷能力を阻止または低下させることとなります。
- システム運用は、常に安全な状態を維持する必要があります。失敗した、または誤った判断をした後でもです (たとえば、生命/安全とビジネス価値を、機密性、完全性、可用性の保証を通じて維持する)。
- 安全な状態を維持することが特に重要になるのは、組織がレガシまたは静的なコントロールに依存しているためインバウンドのアクセス試行の信頼性を動的に測定して実施することができない場合です (たとえば、レガシのアプリケーション、サーバー、またはデバイスに対して静的ネットワーク制御を行っている)。

ゼロ トラストの準備状況を評価する

組織のゼロ トラストの準備状況を評価して、デジタル資産全体の保護向上のための計画を始めるときは、以下の主要領域への投資を検討する必要があります。これは、スムーズで効果的なゼロ トラスト実施の推進に役立ちます。

強力な認証: 強力な MFA とセッション リスクの検知をアクセス戦略の主軸にすることによって、ID 侵害のリスクを最小限に抑えます。

ポリシーベースの適応型アクセス: リソースに対する許容可能なアクセスポリシーを定義し、その施行には一貫性のあるセキュリティ ポリシー エンジンを使用します。これで、ガバナンスが可能になるとともに相違に対するインサイトが得られます。

マイクロセグメンテーション: 単純な中央集中型のネットワークベース境界から、ソフトウェア定義のマイクロ境界を使用する包括的で分散型のセグメンテーションに移行します。

自動化: アラート発出と修復に投資することによって、攻撃に対応するまでの平均時間を短縮します。

インテリジェンスと AI: クラウド インテリジェンスと、利用可能なすべてのシグナルを使用して、アクセスの異常をリアルタイムで検出し、対応します。

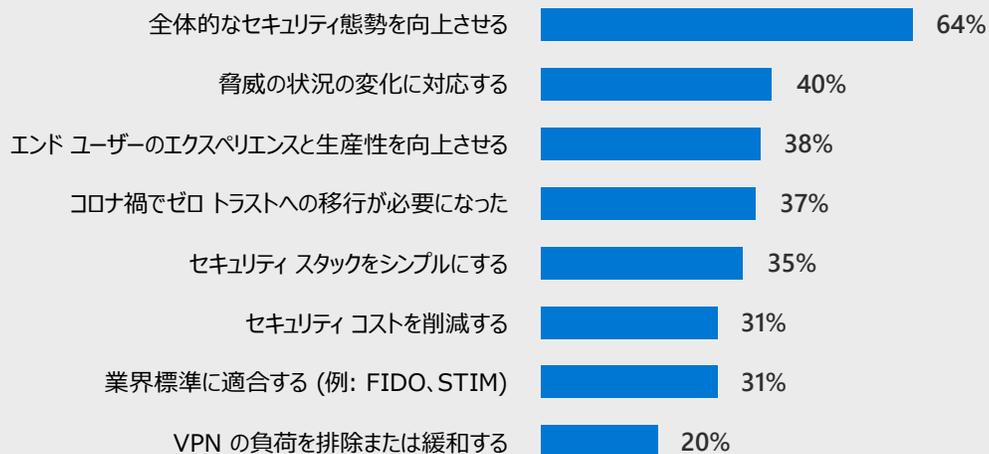
データの分類と保護: 機密性の高いデータを発見、分類、保護、監視します。悪意のある、または偶発的な流出による暴露を最小限に抑えます。

ゼロトラスト成熟度向上についての各組織の経験を紹介する中で、ある参加者のコメント:

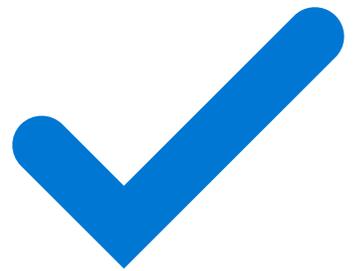
「私たちが始めたのはごく基本的な行程です。手作業でマイクロセグメンテーションを行い (SDP が登場する前)、それから NAC を実装しました。そこから、IoT とクラウドを導入し、内部と外部の境界があいまいになり、進化はゼロトラストのその他の面へと続きました。たとえば、アプリケーションのセグメンテーション、ネットワークのセグメンテーション、ID のフェデレーション、継続的な認可、多要素認証ですが、現在は完全に成長したエコシステムとなっています。」

全体的なセキュリティ態勢の向上がゼロトラスト戦略採用の最大の動機であり、セキュリティ脅威の進化がこれに続いています

ゼロトラストの動機
合計 (n=300)



決して信用せず、
常に検証する





ゼロトラストというセキュリティモデルによって、ビジネスクリティカルな情報とシステムに対する効果的な制御が確立し、適切な人が適切なタイミングで適切なデータにアクセスすることが確実にになります。「決して信用せず、常に検証する」という原則に基づくゼロトラストは、未知または管理対象外のデバイスを排除するとともに、横方向への移動を制限することによって、会社のリソースのセキュリティ保護に役立ちます。ゼロトラストはエンドツーエンドの戦略であり、フルスタック（ID、インフラストラクチャ、デバイス、データ、アプリケーション、ネットワーク）を包含するものであるため、真のゼロトラストモデルを実装するには、これらの要素すべてが検証され、信頼性を証明できることが必要です。

ゼロトラストモデルの達成は簡単ではありませんが、どの長期的モダン化計画にも欠かせない要素です。ゼロトラストを採用したいと考えている組織は、セキュリティコントロールを小さな部分に適用することから始める必要があります。複数の大規模なコントロールを同時に実施しようとしてはなりません。セキュリティコントロールの適用が段階的アプローチで成功したら、ゼロトラストセキュリティをデジタル資産全体に拡大することができます。理想的なゼロトラスト環境とは、強力なID認証が行われ、デバイスがデバイス管理に登録されており、ユーザーには最小特権が付与され、サービス正常性が検証されているというものです。



詳細情報

[ゼロ トラスト セキュリティについて知る](#)

[ゼロ トラストへの行程をどこまで進んでいるかを評価する](#)

[Microsoft ゼロ トラスト展開センター](#)