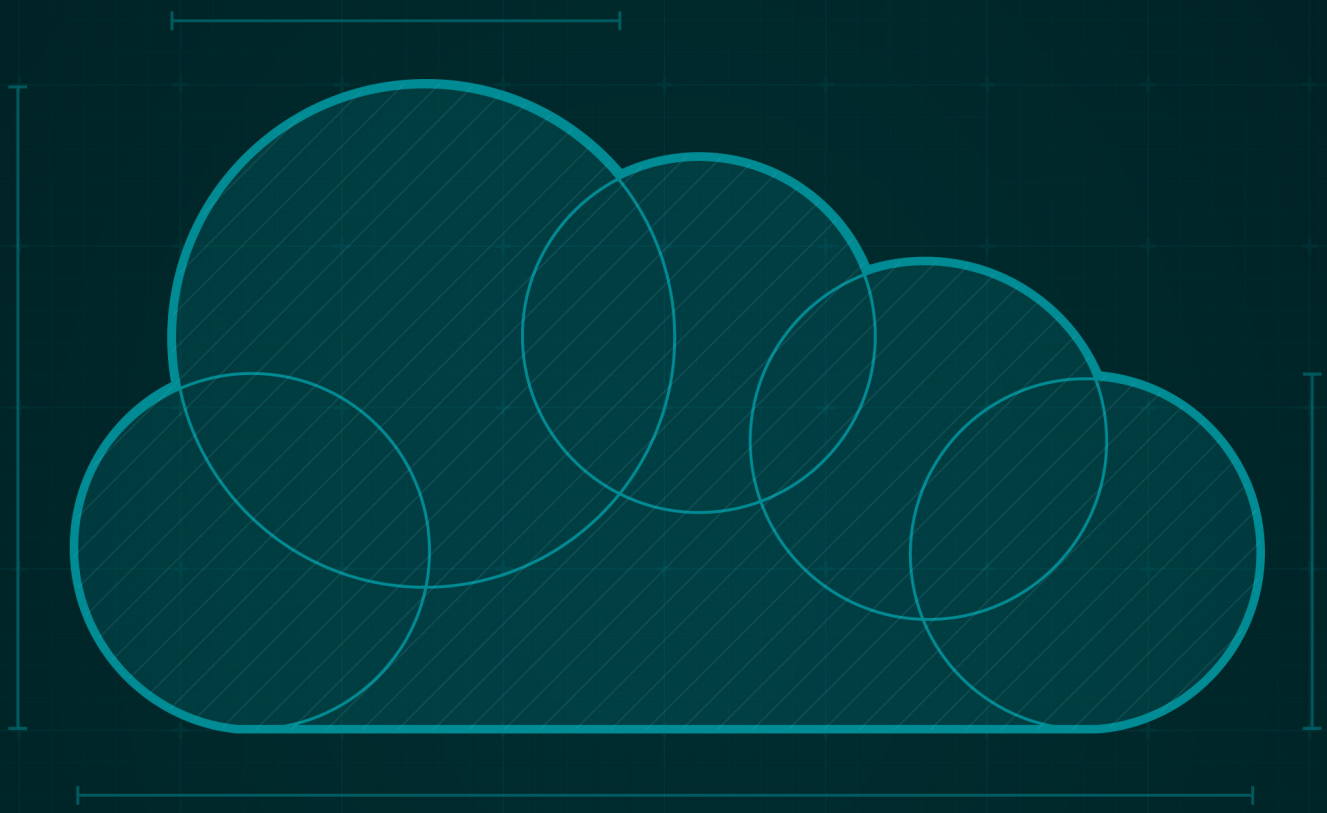
netskope

ホワイトペーパー



SASEアーキテクチャで描くゼロトラストの青写真

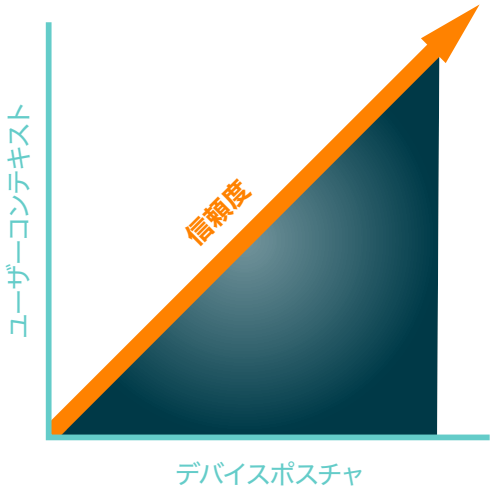
ゼロトラストおよびSASEの導入に不可欠な要素である
継続的なアダプティブトラストを採用するための鍵とその方法

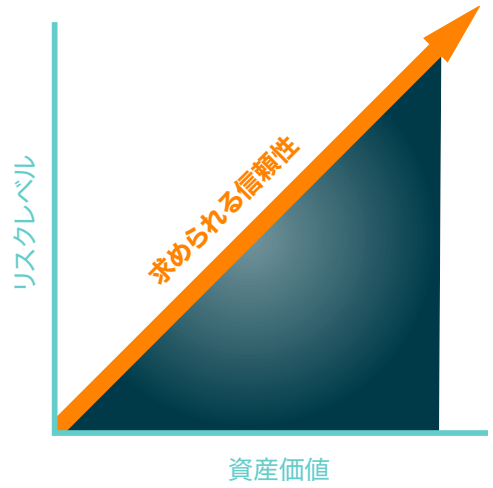
ゼロトラストという用語をよく耳にするようになりました。しかし、ゼロトラストアプローチの目標とそのアプローチがもたらす成果について、あまり適切な記述がされていないのが現状です。ゼロトラストの導入を検討している企業は、互換性のない複雑なレガシーIT、完了の兆しが見えないことや定義の不一致など困難な課題に直面しています。クラウドへの移行、在宅勤務の増加、デジタルトランスフォーメーションは、マルチクラウドに対応するSASE（Secure Access Service Edge）アーキテクチャに特化したゼロトラストの重要性を明確にできる格好の機会となります。Netskopeでは、SASEやハイブリッド環境におけるゼロトラストは、ユーザー、デバイス、ネットワーク、アプリケーション、データ全体で継続的かつ柔軟な適応型の信頼（アダプティブトラスト）を確立し、ポリシー適用に対する信頼性も高めると考えています。

ゼロトラストアプローチでは、「信頼しているが検証する」から「検証してから信頼する」という概念に切り替えて対策を講じることを第一の目標としています。リソースはもはや、接続先となるあらゆるものに対して暗黙的な信頼（IPアドレスなど）を置いていません。ユーザーやデバイスのアイデンティティ、セキュリティ体制、時間帯、地理的情報、ビジネス上の役割、データの重要度など複数のコンテキスト要素を評価することで、特定のインタラクションに対してのみ、特定のリソースに対してのみとリソース側で適切な信頼度を判断することができます。例えば、デバイスの環境を反映した豊富なテレメトリデータを報告できるエージェントのほうが、デバイスが以前に指定したMACアドレスしか報告できないエージェントよりもユーザーの信頼度は高くなると言えます。

しかし、アクセスの開始時に信頼度を評価するだけでは不十分であり、コンテキストの継続的な評価が必要です。コンテキストの変化は、信頼度に影響を及ぼし（増加または減少する）、リソースへのアクセスの仕方も変わる可能性があります。

「すべてのアクセスを許可」と「すべてのアクセスを禁止という二者択一では、現代の新しいワークスタイルに求められる柔軟性を欠いています。例えば、従業員の生産性向上のためにはリスクの高いSaaSアプリケーションも必要な場合がありますが、「すべてのアクセスを許可」または「すべてのアクセスを禁止」という単純なアクセス権では管理できない場合もあります。アクセスは信頼性とリスクのバランスを考慮したうえで、状況に応じて判断する必要があります。リスクの高い状況では、





本来のゼロトラストアプローチとは、暗黙的な信頼を排除し、アイデンティティ、アダプティブアクセス、および包括的な分析に基づいて、ユーザーとデバイスの信頼性を継続的に評価することでリスクの低減やビジネスアジリティを高めることにあります。

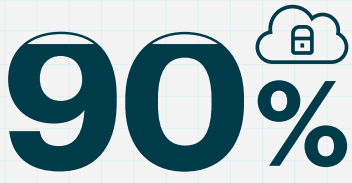
70%

のユーザーが在宅勤務を継続している
（2021年6月末時点）

Webゲートウェイトラフィックの
半数以上がクラウドアプリや

クラウドサービスによるもの

トラフィックの90%がTLSで
暗号化*されている



TLS暗号化

*Google HTTPS Transparency Report Worldwide Windows Platforms 14 November 2020

アクセスが制限されるものの完全にはブロックされないため、一部の作業を行うことができます。リスクの低い状況では、アクセス範囲を拡大することで、特定の管理責任（多要素認証や会社の管理下にあるデバイスなど）を減らすことができます。継続的なアダプティブアクセス　モデルでは、アクセスする資産の価値に合わせて信頼度への要件が変化します。アダプティブアクセスは、アプリケーションやアクティビティのリスク、ユーザーのリスク、データの機密性、デバイスポスチャ、ユーザーの位置情報などの情報に基づいて、許可、拒否、制限、リダイレクトだけでなく、ユーザーへのコーチングをリアルタイムで判断します。

アダプティブアクセスは、リスクの許容レベルに合わせてポリシーを設定するため、必要に応じてアクセスの取り消しを行うことも可能です。

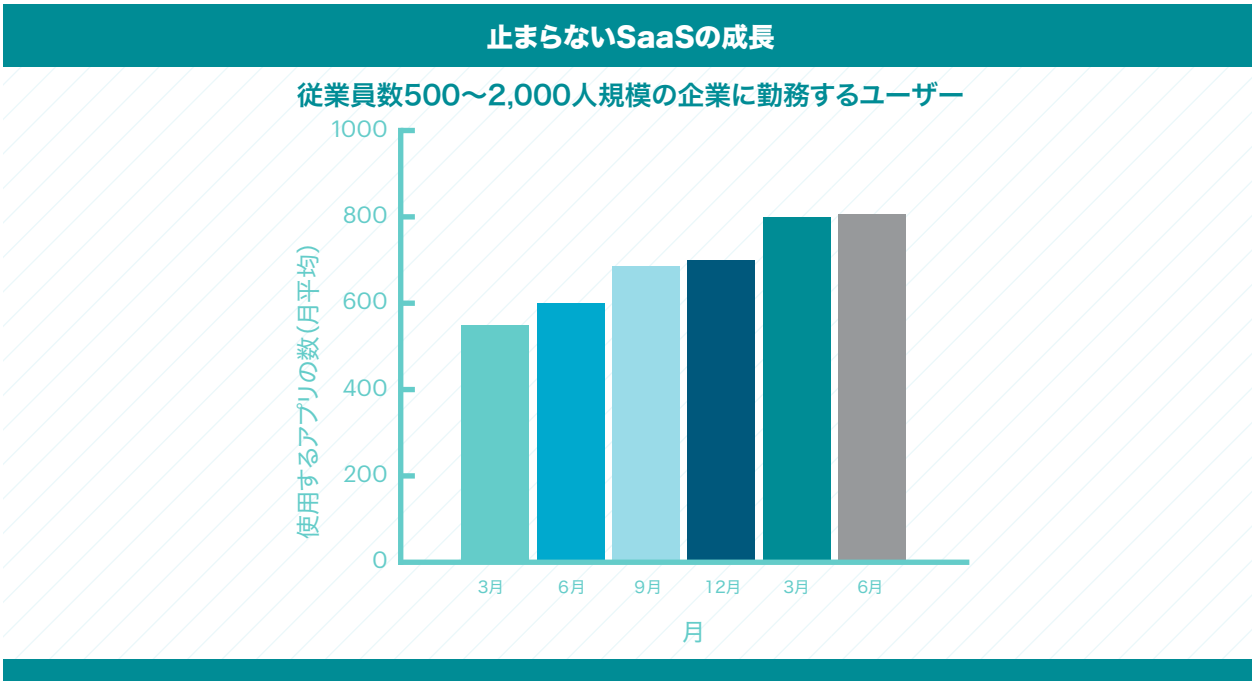
ゼロトラストアプローチが掲げる第二の目標は、ネットワーク環境がいつでも侵害される可能性があること、あるいはすでに侵害されていることを想定して設計するということです。このような新たな考え方で設計すれば、パターンや手法の展開が円滑に進み、攻撃対象領域を最小限に抑えるほか、ラテラルムーブメント（横方向の移動）の制限、迅速かつ正確な脅威防御を実現することができます。

ゼロトラストは、「最小限の特権アクセス」と「リソースを隠す」という一般的かつ重要な2つのセキュリティ原則を改めて提唱することが目的ではありません。確かに、ゼロトラストアプローチでは、承認されたユーザーは許可されたリソースのみに対して必要最低限のアクセス権しか与られず、許可されていないリソースを見ることはもちろん、アクセスすることもできません。しかし、ここで重要なことは、暗黙的な信頼を排除し、アイデンティティ、アダプティブアクセス、および包括的な分析により得られるコンテキストに基づいてユーザーとデバイスの信頼性を継続的に評価することで、リスクの低減やビジネスアビリティを高めるということが本来のゼロトラストアプローチであるということです。

なぜ今、ゼロトラストが注目されているのか

従来のネットワークは、オフィスで働く従業員がオンプレミスのデータセンターで稼働する、業務用アプリケーションにアクセスする時代に合わせて誕生しました。企業は当初、物理的セキュリティと同様の方法でネットワーク セキュリティを構築していました。つまり、危険は外部に潜んでいて、内部は安全だと思い込んでいました。インバウンドの脅威に対してある程度の防御対策ができていたため、企業の多くはゼロトラスト ネットワークという新しい概念に興味は持ったものの、なんらかの行動へ移すことはありませんでした。当面はネットワークの境界での防御だけで十分と考え、ITやセキュリティチームは別の緊急課題に取り組んでいました。

その後、世界は変わり、アプリケーション、ユーザー、データがネットワーク境界を越えるようになりました。そこで豊富なオプションとその導入のしやすさに惹かれて、ビジネスプロセスにSaaS（Software-as-a-Service）アプリケーションを利用する企業が増加しました。実際、従業員数500～2,000人規模の企業では、平均して805種類の*SaaSアプリケーション*が利用されています。

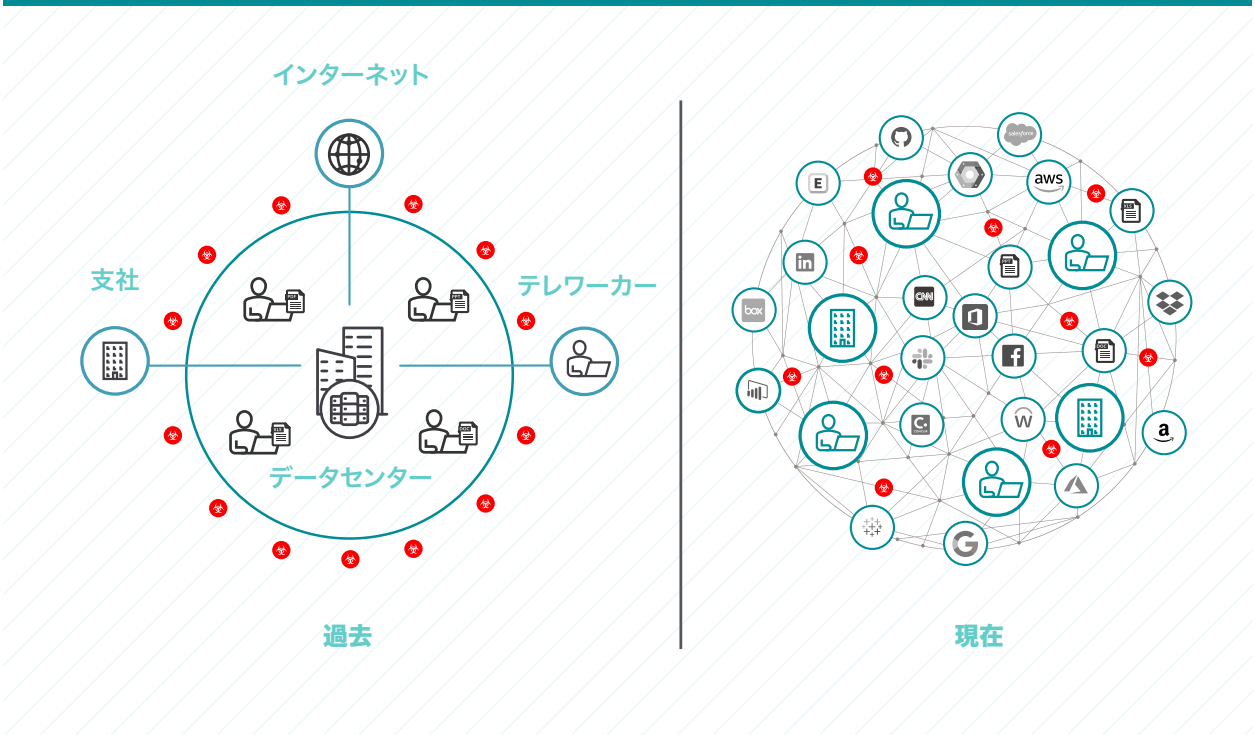


出典：Netskopeのクラウドと脅威に関するレポート 2021年7月版

もちろん、ビジネスプロセスの中には、カスタムアプリケーションが必要な場合もあります。企業は、IaaS（Infrastructure-as-a-Service）やPaaS（Platform-as-a-Service）といったパブリッククラウドのほうが、従来のデータセンターよりもアジリティに優れていると気づき、新しいアプリケーションの多くでパブリッククラウドを利用するようになりました。事実、現在では多くの企業がマルチクラウド戦略を取り入れており、アプリケーション要件や開発者の能力・スキルに応じて複数のハイパースケールクラウドプロバイダーを選択しています（既存のアプリケーションをパブリッククラウドに移行する「リフト＆シフト」手法はそれほど普及していません。適切でないアーキテクチャやセキュリティを選択してしまうという問題を、クラウドが増幅してしまう場合があるためです）。

2020年に従業員の多くが突如、在宅勤務への切り替えを余儀なくされましたが、企業は大規模な変化に対応できることを証明しました。この変化は当初、破壊的なものでした。すべての業界が在宅勤務を適用できるわけではありませんし、推進する必要もありません。しかし、多くの企業にとって、在宅勤務はすでに新しい働き方（ニューノーマル）となっています。アプリケーションが保存されている場所を問わず（オンプレミス、SaaS、パブリッククラウド）、従業員とそのビジネスパートナーがあらゆるデバイス（会社の管理下にあるかに関わらず）からアクセスできる状態にする必要があります。

過去と現在の比較



ゼロトラストは、このようなニーズを満たす理想的なモデルです。大きく分けて、このモデルを実装した製品には、「ZTNA（Zero Trust Network Access：ゼロトラストネットワークアクセス）」と「アイデンティティベースのセグメンテーション（マイクロセグメンテーション）」の2つに分けられます。

ZTNA製品は、ユーザーがアプリケーションを利用できるようにするプロセスにゼロトラストの原則を適用しています。

ゼロトラストベースのアプローチにより、プライベートアプリケーションの場合はオンプレミスでもパブリッククラウドでも、SaaSアプリケーションの場合は接続するネットワークに関わらず、特定のユーザーにアクセス権を付与することができます。アクセス範囲は、その通信のコンテキストに応じて決まり、それを基にセッションの妥当性を考慮して信頼度が提供されます。例えば、会社の管理下にないデバイスのユーザーに対して、公開データを処理する会社の管理下にあるアプリケーションへはすべてのアクセスを許可、機密データを処理する会社の管理下にあるアプリケーションへは読み取り専用、機密データを処理するアプリケーションへはすべてのアクセスを禁止といったアクセス権を付与することができます。さらに、アプリケーション機能を理解したうえで過去のユーザーの振る舞いと組み合わせて分析することで、大惨事を引き起こす前に脅威を検出・緩和することができます。

アイデンティティベースのセグメンテーション（ガートナー社の提唱）は、マイクロセグメンテーションの新たな考え方です。マイクロセグメンテーションは、どのリソース（デバイス、ワークロード、コンテナなど）が相互に通信できるかを判断する静的なルールを適用した分離方式です。アイデンティティベースのセグメンテーションは、マイクロセグメンテーションの概念を拡張したもので、アクセスを許可するかを判断する材料となるアイデンティティやその他の属性を評価する動的なルールを追加したものです。リソースのアイデンティティは移動可能で、基盤となるネットワークに依存しません。アイデンティティに加え、リアルタイムで測定される追加コンテキストに基づいたセグメンテーションにより、セグメンテーション制御とポリシーの柔軟性、アジリティ、拡張性が向上します。

もちろん、ゼロトラストモデルには、管理面である程度のオーバーヘッドが発生することを認識する必要があります。リソースの所有者は、そのリソースに対して許可したユーザーを慎重に評価し、継続的に調整する責任があります。これをエンタイトルメント管理と言います。エンタイトルメント管理は主に手作業で行われますが、新たに登場した技術は、自動化を活用することで手作業によるミスを減らすことができます。さらに、ゼロトラストアプローチでは、エンタイトルメント管理だけでなく、リソースとの通信に必要な信頼度を同時に判断しながら、さらに属性やコンテキスト要素の定義が求められます。実際、従来のアクセスモデルや認証モデルが十分に定義できない環境では、コンテキストを追加することでより正確な信頼性の評価が可能になります。

SASEアーキテクチャとは

セキュリティの原点はネットワークにあります。時の流れとともに、数多くのツールが管理者の目に留まるようデータセンター内で競い合っている状態に変わってきました。これらのツールは、アプリケーションやデータがオンプレミスで保存され、ユーザーがオフィスで仕事をしている場合には効果的でした。ツールの中には、ユーザー同士が通信するためのメカニズムを提供するものもありました。しかし、テレワーク、データやアプリケーションのクラウド移行が進むにつれ、従来のツールで対応することが難しくなりました。これらのツールは、「アプリケーション、データ、ユーザーが静的である」という大きな前提の下で動作していましたが、もはやこの前提が成立しないため、ツールはその適合性の多くを失ってしまいました。連携しない、拡張性がない、一元管理ができないのはもちろん、そしてなによりデータが別のインフラストラクチャに保存・処理される場合にはその機能を発揮することができていません。

ガートナー社が2019年に提唱したアーキテクチャであるSASEは、多すぎるツールやコンソールの数を最小限に抑えます。SASEは、共通のネットワーク機能（SD-WAN、WAN最適化、QoS、ルーティング、CDNなど）と共通のセキュリティ機能（SWG、CASB、ZTNA、VPN、FWaaS、RBIなど）を統合し、一元管理するアーキテクチャです。あらゆるアプリケーションやサービスにアクセス制御のポリシーを適用し、すべてのユーザーやリソースを対象に機密情報の移動を監視・制御します。SASEは、ネットワークとセキュリティの機能をクラウド経由で提供し、ユーザーやアプリケーションの場所を問わず一貫したユーザーエクスペリエンスを実現します。

出典：ガートナー社「SASEの戦略的ロードマップ：2021年」 ID：G00741491
https://www.gartner.com/document/3999828

優れたSASEアーキテクチャは、ゼロトラストの原則を実装しています。SASEは、リソースへのあらゆるアクセス方法を統一し、信頼性評価やアクセス権の付与を中立の立場で判断します。ゼロトラストの原則は、アクセス権の付与や一連の条件に基づいた信頼性の監視を求める一方で、どのような技術的アーキテクチャに対しても中立性を保ちます。SASEとゼロトラストを組み合わせることで、企業によるデジタル資産を保護する方法が根本的に変わります。事実SASEは、ユーザー、アプリケーション、データがあらゆる場所に存在する完全なハイブリッド環境に対応できる効果的なゼロトラストプログラムを開発するうえで大きな基盤となります。

ベンダーの能力にもよりますが、ゼロトラストの原則に沿ったSASEアーキテクチャは以下を実現します。

- ユーザーのリスクとアプリケーションのリスクに関するインサイトを取得し、様々な条件下で許可されたアクセスに対する信頼度を判断した後に、その信頼度に基づいてアクセス権を適用します。
- ゼロトラストの原則をプライベートアプリケーションだけでなく、WebアプリケーションやSaaSアプリケーションにまで拡張します。柔軟なポリシーとポスチャを考慮したリスクに関するインサイトに基づいて適用します。
- アプリケーションのリスクを把握し、特定のアクティビティへのアクセスを制御します（信頼度が低い場合、閲覧やコメントを許可するが、共有や削除は禁止するなど）。
- リスクや信頼性の評価を基に、リモートブラウザ分離や高度な情報漏洩対策などのセキュリティサービスを追加します。
- 信頼性の再評価やコンテキストの変化を継続的に監視します（再認証、段階的な認証、権限の変更、アクセスの増加／減少など）。
- プロトコルやサービスの公開を避けることで、全体的な攻撃対象領域を縮小します。

ビジネスとユーザーにもたらされる成果

現代のデジタルビジネスは、誰かの許可を待つということはありません。その一方で、インターネット経由で提供されるアプリケーションやデータへ依存する傾向があります（事実、セキュリティを考慮して設計されていません）。企業は、セキュリティリスクプログラムとデジタルトランスフォーメーション計画に継続的なアダプティブトラストの原則を予め組み込むことで、セキュリティのトレードオフが発生することなく、ビジネス目標を達成することができます。

ビジネスにおけるアジリティ

ビジネスアジリティには、ボリュームやロケーションの規模と新しいサービスやアプリケーションの幅の両方において、インフラストラクチャやサービスの弾力性を求められます。ゼロトラスト原則に基づいて、SASEとハイブリッドクラウドアーキテクチャ達成できる、あるいは想定される成果は以下の通りです。

- 調和のとれたユーザーエクスペリエンス：ユーザーがどこにいても、どのようなデバイスを利用していてもアクセスできます。
- 場所に依存しない：アプリケーションへのアクセスは、基盤となるネットワークの設計とは別物です。そのため、ユーザーの習慣を変えることなくアプリケーションをオンプレミスからパブリッククラウドに移行できます。
- アクセス権を拡大する：セキュリティに関する決定事項の多くを「拒否」から「条件付きで許可」へ変更する。
- サプライヤーやパートナー向けにローカルユーザーアカウントを作成することなく、また相手側のコンピューティング環境に負担をかけることなく、コラボレーションを促進します。
- アプリケーションを展開してからアクセスを追跡して保護するという事後対応でなく、先を見据えたセキュリティ対策でアプリケーションの増加に対応します。

リスクの低減

サイバーリスクは、多くの取締役会で議題にあがる優先事項です。どの業界の企業でも、自社のリスク許容度を決定する必要に迫られています。リスク管理は、長く不透明なサプライチェーンへの依存、クラウドサービスやアプリケーションの普及、曖昧な規制環境などによって複雑化しています。このような新たな環境でリスクを抑えるには、以下のようなゼロトラストアプローチが必要です。

- リソースの公開を非公開へ変更することでインターネットから遮断し、強力なアクセス権のあるユーザーや信頼性を証明できたユーザーのみに見えるようにする
- 不適切なアクセスを制限し、侵害を受けたアカウントの拡大範囲を最小限に抑える
- 機密性の高いデータの種類、場所、移動に対する可視性を向上し、定期的に改善を試みる
- 分析により、許容されるポリシーと振る舞いの全体像を把握することで、リスクや脅威（異常なアクティビティや悪意のあるアクティビティ）を素早く表面化させ、迅速な封じ込めと排除を行う
- 全体的なセキュリティ体制を改善し、攻撃者の標的から外れる

製品の導入および保守プロセスの合理化

ビジネスアジリティとリスク低減には、以下のような適切なアーキテクチャが必要です。

- クラウドネイティブなセキュリティサービス：ビジネスニーズに応じて拡張可能で、ハードウェアのセキュリティアプライアンスにありがちな導入の複雑さや容量の制約を解消します。
- 単一のクラウドプラットフォーム、シングルパスによる通信の検査およびポリシーの強制的な適用：単一のコンソールとポリシーエンジンを使用し、すべてのチャネルで一貫したセキュリティポリシーを適用します。
- シングルベンダー：相互運用性が未検証または確認されていない特性を持つ製品のトラブルシューティングや修理に伴う遅延を解消します。

NETSKOPEを使用した継続的なアダプティブトラスト実現に向けた5つのフェーズ

Netskopeは、企業が継続的なアダプティブトラストの目標を達成するためのサポートを行っています。その道のりは、企業によって異なります。業界、クラウド導入の程度、既存のレガシーシステムなどによって、スタート地点だけでなく、作業量も変わります。

始める前の簡単な手順です。まずは以下の作業を行ってください。

- 典型的なビジネス上の役割を反映したユーザーペルソナ(想定される人物モデル)のセットを考案する。各ペルソナに共通するアクセス要件をリストアップする。元からある役割ベースのアクセス定義に頼らずゼロから始める。
- すべてのプライベートアプリケーションとSaaSアプリケーションのインベントリ管理を行う。アプリケーションとそのコンポーネントまたは企業の外部リソースとどのように相互作用しているかを示すマップを作成する。
- すべてのデータ資産を対象にデータ資産の場所、感度、ビジネス機能、および耐用年数を特定する。

継続的なアダプティブトラストプロジェクトを成功させるためには、アイデンティティとアクセスにおける堅固な管理プログラムが必要です。正確で信頼性の高いアイデンティティの記録システムがなければ、信頼性が高いと判断したり推測したりすることはできません。人、デバイス、オブジェクトを問わず、すべてのエンティティは、他のエンティティでも検証できるアイデンティティを提示しなければなりません。幸いなことに、多くの企業はすでになんらかのID管理システムを導入しています。ゼロトラストで重要なことは、そのシステムが SAML、OpenID Connect、OAuth のような標準規格との互換性があるかであり、これは多くの企業が求めていることです。アイデンティティフェデレーションは、異なるアイデンティティ管理範囲間の信頼度を確立し、ある範囲で認証されたユーザーが別のアイデンティティを持っていなくても他の範囲で許可されたリソースにアクセスできるようにします。

これらの情報を基理解したうえで、次のページに記載される5つのフェーズを計画・実行することができます。

フェーズ 0

始める前に

- ペルソナを設定してアクセス要件を割り当てる
- すべてのSaaSおよびプライベートアプリケーションのインベントリ管理を行う
- すべてのデータ資産のイベントリ管理を行う

フェーズ 1

ゼロトラストアクセス

- アイデンティティに対して信頼できる情報を決定する
- ユーザーとアプリケーションのマッピングを行う
- 古くなった、または使用していないエンタイトルメントを削除する
- すべてのアクセスをポリシーエンフォースメントポイントで管理し、直接アクセスのリスクを排除する

ゼロトラストアクセスのベースラインを確立

フェーズ 2

アダプティブアクセス

- アクセスポリシーにコンテキストを追加する
- 強力な認証を必要とするかどうかをコンテキストで判断する
- コーチングにコンテキストを組み込む
- アクセスポリシーを継続的に調整する

アプリケーションのアクティビティに関する認証で信頼性のベースラインを強化

フェーズ 3

オンデマンド型の分離

- 危険なサイトや評価の低いサイトへのアクセスにリモートブラウザ分離を活用する
- コマンド&コントロール攻撃やその他の異常な振る舞いを監視する

送信先に明示的な信頼制御を適用

フェーズ 4

継続的なデータ保護

- 会社の管理下にあるデバイスと管理下にないデバイスでアクセスを区別する
- コンテキストに基づいたアクセスポリシーを適用する
- クラウドリソースを適切に設定する
- 機密情報を特定し、公開範囲を管理する
- 共有権限とアプリ間の統合を継続的に評価する

継続的な調査で過剰な信頼による権限を排除、またあらゆる場所で最小特権モデルを採用し、その原則を適用

フェーズ 5

リアルタイム分析による情報共有と改善

- アプリケーションとリスクの可視性を維持する
- クラウドとWebのアクティビティを検査し、ポリシーの適切な評価と調整を行う
- 様々なステークホルダーに合わせて可視化を行う
- 継続的な監視と管理で改善を行う

継続的な監視と管理を改善することでセキュリティ体制と信頼ポスチャを強化

フェーズ1

ゼロトラストアクセス：匿名によるアクセスを許可しない

最初にアクセスした時点でコンテキストを構築します。まず、アイデンティティとアクセスの管理（ロールとそのロールのメンバーシップを含む）、プライベートアプリケーションの検出、承認されたSaaSアプリケーションとWebサイトのカテゴリ別リストを強化することから始めます。ラテラルムーブメントの機会を減らし、フィンガープリント、ポートスキャン、脆弱性の調査からアプリケーションを隠します。SSO（Single Sign-On：シングルサインオン）にMFA（Multi-Factor Authorization：多要素認証）を適用します。

Netskope Security CloudはSSOと連携し、Webサイト、プライベートアプリケーション、数万ものSaaSアプリケーション（様々な部門で使用されているシャドーITを含む）のさらに柔軟なアダプティブアクセス制御を実現します。Netskope Private Accessは、プライベートアプリケーションのディスカバリからアプリケーションレベルのアクセスにいたるまでZTNAの機能を最大限活用します。会社が把握しているユーザーやサードパーティの業者、M&Aのユースケースなど幅広く対応します。Netskopeの次世代SWGは、WebやSaaSへのアクセス制御ポイントとして、多くの企業が直面している最大の脅威と言われるSaaS、Webメール、クラウドストレージなどの認証情報を狙ったフィッシング攻撃などを阻止します。

具体的なタスク：

- アイデンティティに対して信頼できる情報と連携可能なアイデンティティソースを決定します。
- 強力な認証が必要な状況を設定します。
- ユーザー（従業員やサードパーティ）とアプリケーションをマッピングできるデータベースを構築・維持します。これは、ビジネス部門との定期的な対話や連携が不可欠です。責任者を決め、チームを作成します。
- 役割の変更、退職、契約終了などで不要となった従業員やサードパーティのエンタイトルメントを削除することで、アプリケーションアクセスを合理化します。
- すべてのプライベートアプリケーションや内部アプリケーション（ZTNA）、SaaS、Webへのアクセス（CASB、SWG）をポリシーエンフォースメントポイント（ポリシーを適用する場所）で管理することで、直接接続を排除します。
- リアルタイムで、アプリケーションへのアクセスやユーザーの状況を管理します。ユーザーのアプリケーションやサービスへのアクセスを制御します。

フェーズ2

アダプティブアクセス：明示的な信頼モデルを維持する

より多くのコンテキストを追加することで、アクセスコントロールが適応できるようになり、明示的な信頼モデルを維持できるようになります。アプリケーションのリスク評価、ユーザーのリスク評価、エンドポイントポスチャー管理、ユーザー、アプリケーション、データの場所などの情報を評価します。ステップアップ認証、アプリケーションの使用を続行する、またはキャンセルするかをユーザーに知らせるアラート表示、続行するためのビジネス上の正当な理由を提示させたり、承認されたアプリケーションへのリアルタイムのコーチングなどを行うアダプティブ ポリシーを実装します。

Netskope Security Cloudは、検査されたWebとクラウドのトラフィック全体についての詳細なコンテキストを提供し、アプリケーションのリスク評価とインサイト、ユーザーのリスク評価をリアルタイムで提供するほか、ユーザーの振る舞いに基づいたUEBAから取得したインサイトも継続的に提供します。これらの評価により、ユーザー、データ、アプリケーションに最適なポリシーに基づいて、段階的な認証、プロセスの終了など、リアルタイムなアダプティブ ポリシーアクションを実施します。

具体的なタスク：

- デバイスが管理されているかを確認する方法を決定します。
- アクセスポリシーにコンテキストを追加します（条件に応じて、特定のアクティビティをブロック、読み取り専用、許可する）。
- 環境リスクが高い場合には強力な認証を使用し（プライベートアプリケーションやSaaSへリモートでアクセスする場合はコンテンツを削除するなど）、リスクが低い場合にはその使用を減らします（会社の管理下にあるデバイスがローカルアプリケーションにアクセスする場合は読み取り専用にするなど）。
- ユーザーのリスクを評価し、特定のアプリケーションのカテゴリに関するアクセスについてコーチングします。
- アプリケーションの進化、新しいアプリケーションの登場、不要となったアプリケーションの削除など変化するビジネス要件を反映しながらポリシーを継続的に調整します。
- アプリケーションのアクティビティに関する認証の中で、信頼性のベースラインを確立します。

フェーズ3

オンデマンド型の分離：脅威の影響を最小限に抑える

RBI（Remote Browser Isolation：リモートブラウザ分離）を導入し、ブラウザの機能をディスプレイデバイスとしての機能に限定します。また、デバイスのファイアウォールを有効にして、デバイスの接続先を制限します。

Netskope RBIは、ネイティブかつシングルパスで、既存のデータ保護や脅威除去機能と統合されています。さらに、従来のプロキシやネットワークゲートウェイに、サービスチェーン化されたRBI製品では得られない、高いパフォーマンスを実現します。暗黙的な信頼を排除するということを念頭に、リスクのあるWebリソースへの直接アクセスは、特にユーザーが会社の管理下にあるアプリケーションと同時にやり取りする場合は最小限に抑える必要があります。

オンデマンド型の分離、つまりリスクの高い状況下で自動的に分離を適用することで、不正なユーザーや危険なWebサイトからの影響範囲を最小限に抑えます。

また、Netskope Cloud Firewallは、攻撃者が所有するコマンド&コントロールノードとの通信を阻止するうえで非常に効果的な構造となっています。

具体的なタスク：

- 評価の低い危険なWebサイトにアクセスするためのパスに、リモートブラウザ分離を自動適用します。
- リモートブラウザ分離を設定し、会社の管理下にないデバイスからプライベートアプリケーションにアクセスします。
- URLが書き換えられSaaSアプリケーションが正常に動作しない場合に、CASBリバースプロキシの代替としてリモートブラウザ分離を評価します。
- 脅威とユーザーダッシュボードをリアルタイムで監視することで、コマンド&コントロール攻撃や異常を検知します。

フェーズ4

継続的なデータ保護：シングルパスのデータポリシーを適用する

承認済み・未承認のSaaSアプリケーション、Webサイト、パブリッククラウドのストレージ、パブリッククラウドのカスタムアプリケーション、および送信メールを経由した機密情報の移動を監視・制御します。移動データに対しては検査済みのWeb、メール、クラウドへのトラフィック全体に、保存データに対してはシングルパスのデータ保護ポリシーをAPI経由で適用します。

Netskope Security Cloudは、意図しない、または許可されていないデータの移動を制御するだけでなく、すべての検査済みデータアクティビティを対象に詳細な分析を行います。従来の防御対策では、クラウドのトラフィックを解読することできないため、特に承認済みや未承認アプリケーションの個人インスタンスに十分なデータ保護を適用することができません。Netskope Cloud Firewall-as-a-Service（FWaaS）は、リモートユーザーや支社のあらゆるポートとプロトコルにアウトバウンドネットワークアクセス制御を適用することで、コマンド＆コントロール攻撃やデータ流出を軽減します。

具体的なタスク：

- 会社の管理下にあるデバイスと管理下にないデバイスによるデータアクセスを区別する全体的な定義を作成する。
- アダプティブポリシーの詳細を追加し、コンテキストに基づいてコンテンツにアクセスする（会社の管理下にないデバイスを使用する場合、公開されているコンテンツはすべてのアクセスを許可、機密性の高いコンテンツは読み取り専用にしたり、ダウンロードをブロックするなど）。
- CSPM（Cloud Security Posture Management：クラウドセキュリティポスチャ管理）で、パブリッククラウドサービスの構成を継続的に評価することで、データ保護・コンプライアンス準拠を実現します。
- Web、会社の管理下にあるSaaS、シャドーIT、パブリッククラウドサービス、メールに対するインライン用DLPルールとポリシーの使用状況を評価することで、データ保護・コンプライアンス準拠を実現します。
- 会社の管理下にあるSaaSおよびIaaS環境に対して保存データ用DLPルールとポリシーを定義します。特に、クラウドストレージにあるファイルの共有許可や、データの共有と移動を可能にするアプリケーション間の統合などが挙げられます。
- 必要に応じてユーザーやグループの属性を追加することで、ポリシーを微調整します。
- 継続的に調査することで、過剰に与えられていた信頼による権限を取り除きます。あらゆる場所で最小特権モデルを採用し、その原則を適用します。

フェーズ5

リアルタイム分析と可視化による情報共有と改善

リアルタイムのポリシー強化・改善を行います。ユーザーの動向、異常なアクセス、アプリケーションの変更、データ感度の変化に基づいて、既存ポリシーの適合性を評価します。リスクの許容範囲を超えないようにポリシーを適切に調整します。

具体的なタスク:

Netskopeのリアルタイム分析と可視化は、Netskope Security Cloud全体に関するインサイトを提供し、特定のアプリケーションセットで会社が所有するデータを扱ってもいい人(または、扱ってはいけない人)を特定します。セキュリティオペレーション、ネットワークオペレーション、脅威ハンティングの各チームと連携しながら、セキュリティプログラムの成果を幹部社員やアプリケーションに携わる関係者に報告します。

分析から取得したインサイトは、企業がセキュリティプログラムの方向性や次の取り組みを計画・検討するうえで役立ちます。

- 企業が使用しているアプリケーションやサービス、それらに関連するリスクレベルを可視化します。
- 個人情報にアクセスできる人、できない人を判断し、アクセスを最小限に抑えることで、情報漏洩を防止します。
- クラウドやWebのアクティビティを可視化し、詳細に把握することで、データや脅威に対するポリシーを継続的に調整・監視します。
- セキュリティおよびリスク管理プログラムの主要なステークホルダー(CISO/CIO、法務、CFO、SecOpsなど)を特定し、彼らが理解できるようにデータを可視化します。
- ダッシュボードを作成して、これらのコンポーネント(サイト、アプリケーション、インスタンス、ユーザー、アクティビティ、ファイル、送信元/送信先など)を可視化します。
- 他のセキュリティチームとの共同作業を行えるように、ダッシュボードをインポート/エクスポートする機能を確保します。
- 継続的な監視と管理によりポリシーを改善することで、セキュリティ体制と信頼ポスチャを強化します。

デジタルトランスフォーメーションは、2020年に発生したコロナウイルスによって加速し続けています。現在のニーズを満たすためには、ネットワークやセキュリティのインフラストラクチャとプログラムを再構築する方法を評価する必要があります。マルチクラウドやハイブリッドクラウドアーキテクチャ全体で、シンプルかつ効果的なリスク管理制御を行いながら満足のいくユーザーエクスペリエンスを迅速に提供するためには、新たなアプローチが不可欠です。

Netskopeは、ネットワークの内外を問わず、あらゆるデバイスからユーザーをインターネット、アプリケーション、インフラストラクチャに安全かつ迅速に直接接続します。Netskope Security Cloudは、CASB、SWG、ZTNAを単一のプラットフォームにネイティブに組み込んでいます。データ保護と脅威防止にゼロトラストの原則を適用しながら、特許取得済みの技術を用いて最もきめ細かいコンテキストを提供することで条件付きアクセスやユーザー認識を可能にします。Netskopeのグローバルセキュリティプライベートクラウドは、エッジでのコンピューティング機能を最大限に活用することで、強力なセキュリティ、優れたパフォーマンス、信頼性の高いグローバルネットワーキングを実現します。