ABSOLUTE®

# どこでも働ける時代における ゼロトラストの価値

WFA (Work From Anywhere: どこでも働ける ) 時代に、
ゼロトラスト・セキュリティ戦略を
よりよく理解し、活用、実施する方法

# ゼロトラストとは

ゼロトラスト (Zero Trust) は、最近よく使われるキーワードで、サイバーセキュリティの世界では多くの話題をさらっています。この言葉は 2010 年に Forrester Research によって作られましたが、それから 12 年以上が経過し、現代の、ハイパーにネットワークが接続されている世界におけるインフラストラクチャに対応する主要なセキュリティモデルとして浮上しています。

「ゼロトラスト」の定義は比較的簡単です。このコンセプトは、「決して信用せず、常に検証する」という概念を中心に展開されます。ネットワークやアプリケーションにアクセスしようとするデバイスやユーザーが無条件で信頼されることは決してなく、「信頼」や「アクセス」が与えられる前に、常に認証され、そのアイデンティティが検証される必要があります。

ゼロトラストは、IT チームやセキュリティチームにとって、必ずしも標準的なコンセプトではありませんでした。歴史的には、デバイスやユーザーが「信頼できるかどうか」を判断するために、トラディショナルな「境界線」が使用されてきました。たとえば、多くの場合、組織のオフィスネットワークや「境界」の内側から接続するユーザーは暗黙のうちに信頼されており、業務アプリケーションに接続するために何らかの検証を行う必要はありませんでした。

昨今ではリモートワークを行う従業員の数が増えているため、境界線型のモデルには課題がでてきました。ゼロトラスト・セキュリティは、従来の「オフィスの境界」の考え方をなくし、IT チームがアクセスする従業員のコンテキストを判断して、認証のための要件を独自に設定できるようにします。

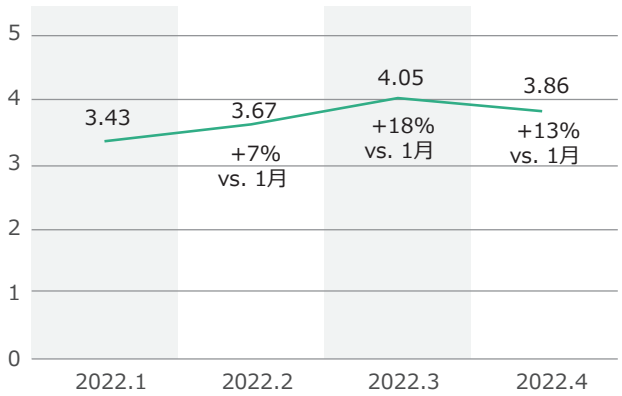
# ゼロトラストはなぜ重要か

2020 年に発生した COVID-19 によるパンデミックは、ネットワークとエンドポイントセキュリティの在り方を完全に変えました。唐突に 100% リモートワークが展開され義務づけられました。日本では、2020 年 7 月に予定されていた東京オリンピックの開催期間の対応に備えてリモートワークを試験的に検討している組織もありましたが、それ以外の組織にとっては準備期間もなく、突然の事態としてリモートワークが始まりました。多くの組織が、新しい WFA 世界において、エンドポイントやリモート接続の効果的な保護に、苦労を続けています。

リモートワークは今後も続くだろうか？と懐疑的になっている方もいると思います。すでに多くのスタッフをオフィスに戻している組織もありますし、出社とリモートの両方を採用するハイブリッドワークを採用している組織もあります。Absolute が導入されているデバイスからの匿名情報を集計し分析すると、WFA 環境はこれからも続く傾向にあると思われることがわかっています。

**図 1**

組織が所有しているデバイスが所在する場所の数の平均 ( 月ごと )



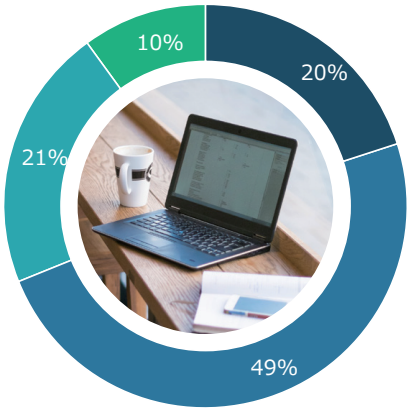

> WFA 時代の中、エンタープライズデバイスのモバイル化は進む

各月にジオロケーションデータが存在する組織所有のデバイス (510 万台 ) に基づく分析。ジオロケーションの方法には Wi-Fi Positioning/triangulation、GPS、Windows Location API、Google Geolocation API が含まれる ( 優先順位は記載の順 )

過去数カ月間のデータを見ると、組織のデバイスが接続する場所の数が顕著に増加しています。2022 年 1 月から 2 月、3 月、4 月にかけて、それぞれ 7%、18%、13% の増加が確認されています。

**図 2**

組織内平均デバイス使用量 (30 日間の平均 )




- 最小限の使用 (1日 1時間未満)
- ライトユーズ (1日 1-4 時間)
- 一般的な使用 (1日 4-8 時間)
- ヘビーユーズ (1日 8時間以上)

> エンタープライズデバイスは
> ヘビーユーズされている
> **5 台に 1 台**がヘビーユーズ、
> **約 70%** が **1 日 4 時間以上**使用されている

2022 年 4 月 19 日時点。過去 30 日間の平均的なデバイス利用データ。30 日間有効になっているデバイスを含む。エンタープライズの 420 万デバイス

また、これらのデバイスは毎日かなりの時間使用されています。エンタープライズ向けデバイスの 70% は、1 日あたり 4 時間以上使用されています。Absolute が導入されたデバイスによる調査結果ですが、このことから、従業員が WFA 環境での生産性を向上できるようになったことが示されています。

しかし、そのことはセキュリティにおいてどのような意味を持っているのでしょうか？

# リモートワークのリスク

使用されるデバイスの数が中程度から大規模になり、使用される場所も増えていることから、組織のリスクは増大しています。

**NetMotion by Absolute が行った調査**によると、調査対象となった IT 担当者の 97% が、リモートワーカーは少なくとも何らかの追加リスクにさらされていると考えており、そのうち約 47% はそのリスクは高い、もしくは非常に高いと考えていることがわかりました。

なぜ、このようなことが起こるのでしょうか。リモートワークがオフィスでの勤務よりリスクが高いとされる理由は無数にあります。これには、以下のような理由があります。

**セキュリティイベントへの対応は物理的に距離が近くないと難しい**

**ランサムウェアやその他のマルウェア攻撃の特定が難しい**

**レガシーなリモートアクセスにはハイリスクなアクセス要件がある**

**デバイスが常に最新に保たれ、設定されているとは限らない**

**ネットワークセキュリティの保護が限定的で、攻撃対象が広範囲におよぶ**

**潜在的な問題を診断する際のテレメトリが少ない**

**紛失、置き忘れ、盗難にあったデバイスの復旧が難しい**

**モバイルフィッシング攻撃が横行している(複数のフォームファクタとデバイスが攻撃される)**

これらのリスクは、最終的に悪意のある第三者が組織の機密データ、アプリケーション、ネットワークにアクセスする可能性を高める結果となります。WFA 時代におけるリスクの増加に対応するためには、どこにいてもワーカーのアイデンティティを確認できる包括的なセキュリティ戦略が必要です。

# エンドポイントとアクセスの現状

モバイル化が進んだ現在、組織はリスクの高まりにどのように対処しているのでしょうか。全世界の数百万台のアブソリュート対応デバイスから収集したデータから、傾向をたどります。

> エンタープライズデバイスの 16% は
> 暗号化されていない

データ：Absolute を導入している 420 万台以上のアクティブなエンタープライズデバイスから取得したもの

### 1. 暗号化されていないデバイス

暗号化されていないデバイスは、組織にとって大きなリスクとなる可能性があります。このリスクは、デバイスが組織のネットワーク境界の外側で使用されている場合、さらに大きくなります。

暗号化されていないということは、デバイスから送受信されるすべての通信が保護されていないことを意味します。デバイスが、組織が所有するネットワークに接続されている場合は必ずしも問題にはなりませんが、それ以外のネットワークに接続されている場合は、デバイスのデータが漏えいする可能性があるのです。

日常業務で使用される場所やネットワークが増える中、暗号化されていないデバイスを特定し、理想的にはロックダウンして漏えいを防ぐ必要があります。

> エンタープライズデバイスの 13% は
> 組織のドメインに接続されていない

データ：Absolute を導入している 420 万台以上のアクティブなエンタープライズデバイスから取得したもの

### 2. 見えないデバイス

組織のドメインに接続されていないデバイスは、IT チームにとっては頭痛の種です。基本的に、そのデバイスは IT チームやセキュリティ担当者によるチェックやバランスなしに、組織の管理範囲外で動作していることを意味します。このコンピューター、ノート PC、モバイル機器に機密データが保存またはダウンロードされている場合、組織が知らないうちにそれが構成されている可能性があることを意味します。

もちろん、組織がこのようなデバイスを認識し、できるだけ早く組織のドメインに接続するための措置を講じることが重要であることは明らかです。

> エンタープライズデバイスの 3 台中 2 台は、
> OS のバージョンが 2 世代以上遅れている
>
> エンタープライズデバイスは、77 日以内に
> 最新のパッチを適用していない

データ：400 万台以上の Absolute を導入したアクティブな Window 10 デバイスから取得したもの

### 3. ふるくなったデバイス

古い OS や最新のパッチを適用していないデバイスを使用することは、組織にとって必ずしも脅威とはいいきれませんが、多くの場合はそのデバイスが脆弱であることを意味します。Microsoft は、ハッカーがエンドポイントを攻撃するために利用できる既知の脆弱性から保護するために、Windows パッチと OS のアップデートをリリースしています。アップデートを行わないことは、一見無害にも見えますが、有害である可能性があります。

組織外での作業や様々な安全でないネットワークでの作業は、脆弱なデバイスが悪用される可能性を高めます。IT チームは、リスク許容度に応じて、アップデートを自動的にプッシュする必要があるかどうかを判断するために、エンドポイントに対する可視性を必要としています。

これらの状況を考えると、多くの組織が現在リスクを軽減する手段を持たないか、あるいは従業員のリモートエンドポイントとリモートアクセスを保護・管理する余地があるかのいずれかであることは確かです。

# ゼロトラストを導入する

ゼロトラスト・セキュリティ戦略は、ひとつのソリューションを購入すればそれだけで実現できるというものではありません。結局のところ、ゼロトラストはコンセプトであり、アイデンティティの徹底的な検証なしに信頼を与えることはできないのです。確実にゼロトラストを実現するためには、よく考えてセキュリティソリューションを組み合わせて組織内システムを構築する必要があります。

ゼロトラスト・セキュリティの実践の第一歩は、ZTNA（ゼロトラスト・ネットワーク・アクセス）ソリューションの採用です。Gartner は 2022 年、**ZTNA に関する最新の Market Guide** を発表し、市場の成熟と成長が続いているとしています。このガイドでは、Absolute が、この分野の他の主要企業とともに、代表的なベンダーのひとつとして認識されています。

Absolute は、ゼロトラストに、段階的な取り組みを提案しています。まず組織のネットワークへのすべての接続の安全性（セキュアアクセス）と、コンテキストに応じたアイデンティティを検証し、そして、この検証をエンドポイントのセキュリティにも拡大するというのが Absolute の考え方です。Absolute は、業界初の自己復活型レジリエント・ゼロトラスト・ソリューションを市場に提供しています。

# セキュアなアクセス

セキュアアクセスは、長年にわたって IT 戦略の重要な要素となっていますが、パンデミック以来、組織にとっての重要性が増しています。多くの組織が、1 カ所か 2 カ所の集中型オフィスから、何百もの個人用ホームオフィスへと移行しています。ゼロトラスト（情報漏えい防止）の観点から、ホームオフィスから組織ネットワークへの接続を特定し、保護することは不可欠です。

Absolute Secure Access 製品群はまさにこれを実現するもので、すべての接続をリアルタイムで分析し、さまざまな要因（日付、時間、場所、権限など）に基づく検証を確実に実行します。この解析はシームレスで、ネットワークやエンドポイントのパフォーマンスを阻害することはありません。Absolute のゼロトラスト・ポリシーは、エンドユーザーに最も近い場所であるエンドポイントで展開、実施されるため、遅延やデータの侵害を回避することができます。これは、最先端の NIST SP 800-207 Zero Trust Architecture 勧告に適合しています。さらに、Absolute Secure Access は、データ最適化技術を使用して、エンドユーザー・エクスペリエンスを積極的に向上させています。

多くの ZTNA ソリューションが同じような機能を提供していますが、Absolute は、さらに一歩進んで、レジリエンス（復活力）を提供しています。Absolute Secure Access が事故や故意によって削除されてしまっても自動で復活して、組織のネットワークアクセスを安全に守るのです。

# セキュアなエンドポイント

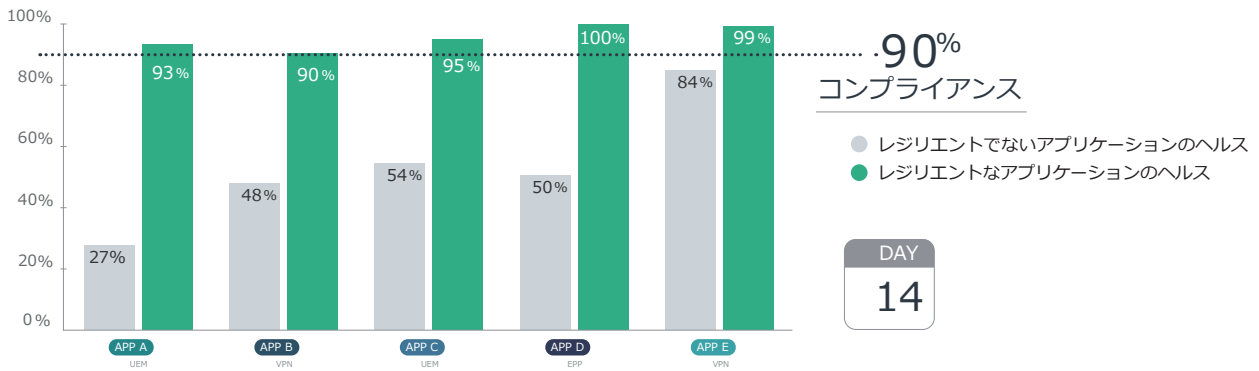
エンドポイントに設置される防御手段は、その運用を継続し、意図したとおりに機能する場合にのみ、効果を発揮します。たとえば、従業員が、サポートされていないサードパーティ製アプリケーションを業務用デバイスにインストールするという単純な作業を行うだけで、セキュリティ・アプリケーションの整合性と有効性を意図せずに損なってしまうことがよくあります。また、フィッシングなどの攻撃が蔓延する中、悪質な業者は、脆弱性や人為的ミスを突いて制御を回避し、悪意を持ってセキュリティ・アプリケーションを無効にするなど、その分野において非常にクリエイティブであることが実証されています。

レジリエンスを特長とする Absolute のセキュアエンドポイント製品群は、これまでの常識を完全に覆すものです。エンドポイントのファームウェアに組み込まれた Absolute パーシステンス技術は、特許を取得している技術で、非常に高い耐障害性を備えており、デバイスの再イメージ化、ハードディスクの交換、ファームウェアのフラッシュを行ったとしても、無効化しようとする試みを阻止する、唯一のソリューションです。Absolute は、ファームウェア内に組み込まれていて、削除不可能な自己回復の機能を、Absolute 自体はもちろん、サードパーティ・アプリケーションにまで拡大し、それらがインストールされたまま健全性を保ち、エンドユーザーのミスや、悪意ある行為、ソフトウェアの衝突、通常の崩壊に対抗する効果を保証しています。つまり、何らかの理由でデバイスから Secure Access ソリューションをアンインストールした場合や、マルウェアによってアプリケーションの整合性が損なわれた場合でも、管理者はデバイスの再起動時にソリュー ションを自動的に修正または再インストールするポリシーを事前に設定することができるのです。

もう少し詳しく見てみましょう。Absolute の Application Persistence テクノロジーを使用した場合と使用しない場合のアプリケーションの健全性を 2 週間にわたって評価したところ、使用しない場合、アプリケーションは非常に迅速に安全でなくなる可能性があることがわかりました。

**図 3**

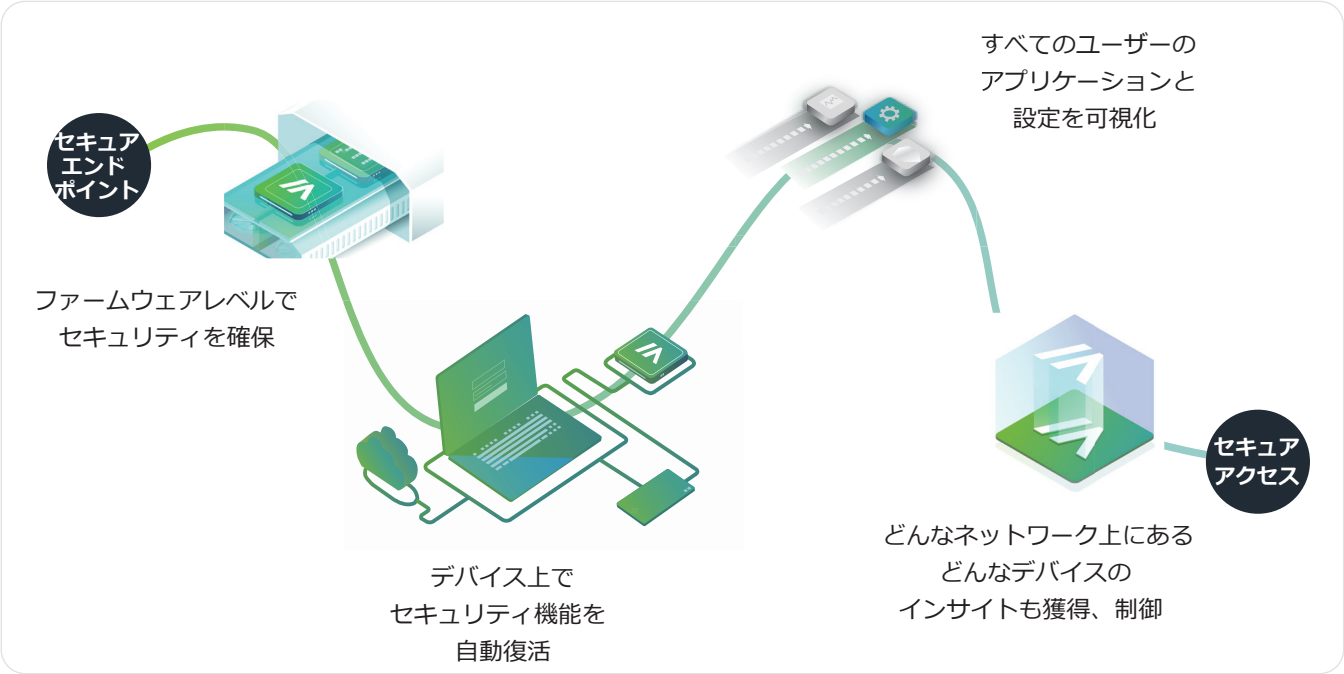
セキュリティの健全性と安定性は、自動復活によって向上する




3つの製品カテゴリ (EPP, VPN and UEM) の 5種類のアプリケーションを対象に、14日間、3.1Bレコードで行った分析

# ゼロトラストを確実に実現する

Absolute のレジリエント・ネットワークアクセス・ゼロトラストおよびレジリエント・エンドポイント・ゼロトラストを導入した際のイメージを下図に示します。




**Absolute が提供する、WFA 時代のレジリエント・ゼロトラスト・ソリューションの詳細はこちら**

**お問い合わせはこちら**

**メソドロジー：** このレポートの作成にあたっては、北米および欧州の 12,000 の顧客組織で稼働している約 500 万台の Absolute を導入しているデバイスの匿名化データ、および信頼できる第三者機関のデータおよび情報を分析しました。

**EMAIL:**
Sales-Japan@absolute.com

**SALES:**
netmotionsoftware.com/ja/contact-us-2

**PHONE:**
03-6427-1976

**WEBSITE:**
netmotionsoftware.com/ja

© 2022 Absolute Software Corporation. All rights reserved. ABSOLUTE、ABSOLUTE ロゴ、NetMotion、SELF-HEALING ENDPOINT、PERSISTENCE は Absolute Software Corporation の登録商標です。その他の会社名、システム名、製品名、ロゴは一般に各社の登録商標または商標です。 ABT-The Value of Zero Trust-WP-060322.