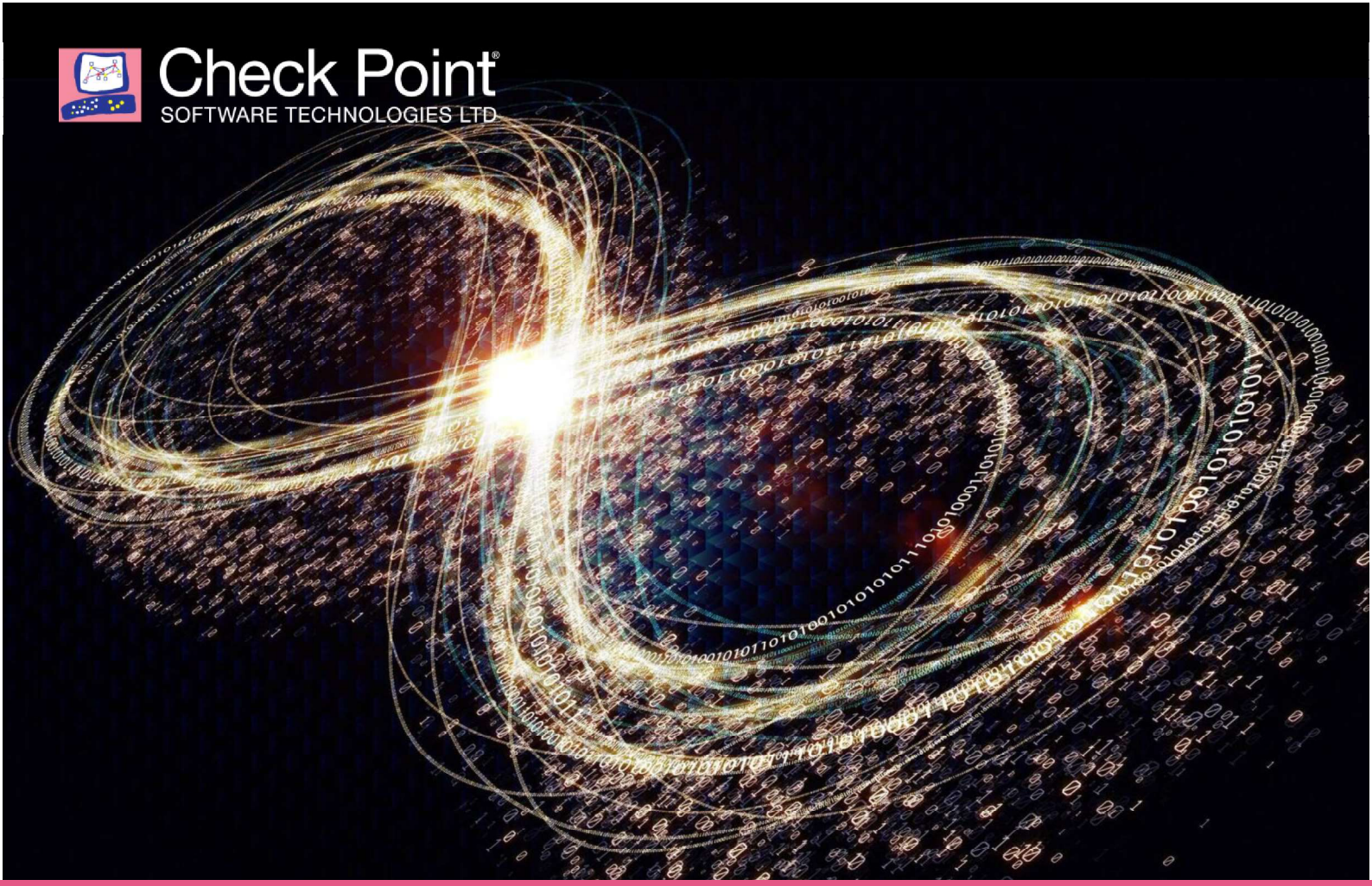


Zero Trust Security
完全ガイド

“Perimeter-everywhere” 環境におけるデータ保護のための
ベストプラクティス、技法、テクノロジー

エグゼクティブ サマリー

今日のようなデジタル、クラウド、分散、モバイルを特徴とする作業環境では、「*perimeter everywhere*」ーあらゆる場所に境界があるため、「セキュリティ境界の内側」という概念が通用しません。攻撃サーフェスがかつてないほど拡大し、サイバー犯罪者はこの新たな環境のエクスプロイトに精通しているということを考えると、サイバーセキュリティ上、大きな問題があります。

こうした「*perimeter everywhere*（あらゆる場所に境界がある）」の問題を克服するために最適なのがZero Trust セキュリティです。これは企業や組織のセキュリティ境界の外だけでなく、内側 にあるものも信用してはならない、という考え方で開発されたセキュリティ モデルです。

このガイドではZero Trustセキュリティ モデルの7つの原則を説明し、効果的な実装のためのベスト プラクティス、技法、テクノロジーを紹介します。

本書を読むと以下が可能になります。

- 詳細なネットワーク セグメンテーションにより、悪意のある水平方向の移動を防止
- コンテキストアウェアな認証によって、なりすましを防止
- すべてのデバイスを脅威から保護し、万が一攻撃された場合は切り離す
- 場所に関係なく、データを分類、保護、暗号化
- 可視化機能の強化と柔軟なポリシーによってワークロードを保護
- セキュリティ・リスクを一元表示して、脅威をすぐに検出、回避
- 豊富なAPIを使用してセキュリティ タスクやインシデント レスポンスを自動化

目　次

背景

常に変化するIT／脅威環境

現在、職場では革命的な変化が発生しており、これがサイバーセキュリティにもたらす影響は計り知れないものがあります。具体的には、動的でローミング環境の整った職場が多くなり、クラウドへの移行が加速しています。IoTデバイスが広く浸透し、それらを利用する従業員もかつてないほど多様化が進んでいます。また、パートナーや顧客のほか、フリーランスのスタッフがコーポレート・ネットワークに接続する機会も増えています。

つまり、セキュリティの世界では、閉じられたネットワーク インフラストラクチャ環境や詳細に定義されたセキュリティ境界の時代は終わりました。すべてのエンタープライズ データの保存、移動、使用がすべて境界内で行われていた時代は遠い昔のことです。

そしてサイバー犯罪者によるセキュリティ境界内への侵入、水平方向移動の成功率がかつてないほど高くなっていることも、問題を複雑化しています。一旦侵入を許すと、検出までの数か月間に貴重な機密データが収集されてしまうのです。

レガシー セキュリティ アプローチでは効果がない

現在、サイバー脅威は境界の内外に存在しており、レガシー・セキュリティ インフラストラクチャでは対応できなくなりました。

レガシー アプローチは主としてNorth-Southトラフィック、すなわちセキュリティ境界を出入りするクライアントとサーバー間のトラフィックに存在する脅威のスキャニングに重点を置いていました。

さらに、アクセス コントロールも境界に基づいており、各エンティティ（ユーザー、ワークロード、またはシステム）の境界に基づき企業のデータやアセットへのアクセスを許可してきました。そしてその判断にはほとんどの場合、IPアドレスを使用していました。

こうした「trust by default」（性善説）のアプローチは危険で過度な信頼につながり、ハッカーによるエクスプロイトのきっかけになっていました。

間違いなく、新しいセキュリティ パラダイムが必要な時がきました。

図1：「Perimeter-everywhere」環境

Zero Trustセキュリティ・モデル

新しいパラダイム：決して信じるな。常に検証。

新しいセキュリティ パラダイムは「Zero Trust」と呼ばれるものです。これはデータ中心でアイデンティティ認識)なセキュリティ モデルで、「perimeter-everywhere」環境での新たな課題に対応できるように設計されています。Zero Trustは企業や組織のセキュリティ境界の内外の誰も信じるな、という考え方に基づいています。このアプローチでは、アクセスを許可する前に、企業や組織のシステムにアクセスしようとしているあらゆるものを検証します。Zero Trustでは、セキュリティ チームがポリシーを設定することで、接続の試みと各デバイスを検証し、アクセスをインテリジェントに制限します。

ZERO TRUSTセキュリティ：7つの原則

Zero Trustは単なるコンセプトやアプローチではありません。Forresterが提供しているZero Trust Extended Securityモデルは、「Default Deny（デフォルトアクションをDeny（拒否）に設定する）」セキュリティ体制を可能にする7つの原則があり、一定の信頼性が確立されるまでシステムの強化と切り分けを行います。

チェック・ポイントが2019年8月に実施した調査では、複数の業界のセキュリティ専門家がZero Trustアプローチを広く採用していることがわかっています。回答者の半分以上（52%）が、自社がZero Trustアプローチの実装を開始済み、または完了していると答えました。また、18%が来年中に実装を開始する予定だと回答しました。

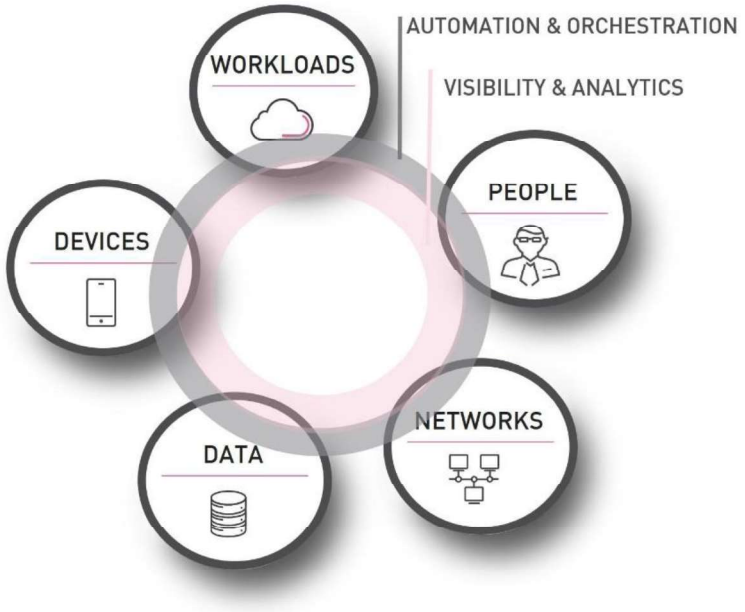
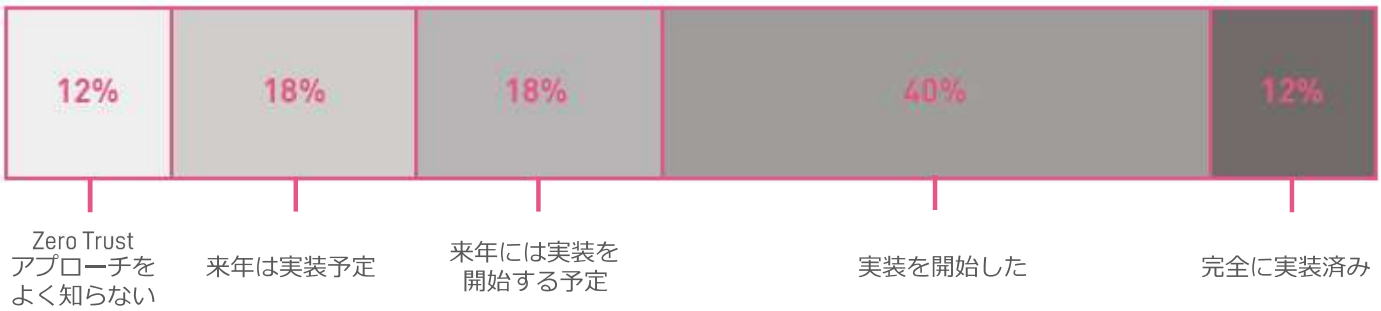


図2：ForresterのExtended Zero Trust Security

企業はセキュリティに対してZero Trustアプローチを導入し始めている。
御社はアプローチ導入のどの段階にあるのか？



1.

Zero Trust Networks – ネットワークを信用しない

詳細なネットワーク セグメンテーションにより、悪意のある水平方向の移動を防止

East-Westトラフィックが普及した結果、悪意のある不正な「水平方向」のトラフィックを抑制し、企業や組織内での攻撃拡散を回避する必要性が非常に高まっています。

このニーズに対応するために重要なのが、詳細なネットワーク セグメンテーションです。つまり貴重なアセットの周りにマイクロ境界を確立することで、ネットワークを分割、規制するのです。

こうしたマイクロ セグメンテーションによって、セグメント間で最低限必要な正当なトラフィックだけが許可され、その他すべては自動的に拒否されます。

Zero Trustネットワークのベスト プラクティス

1. **識別：**企業や組織にとってどのデータやアセットが貴重なのかを識別します。たとえば顧客データベース、ソース・コード、ビルのスマート管理システムなどが該当します。
2. **分類：**各アセットを機密レベル - 「highly restricted（厳重に制限）」など、に基づき分類します。たとえば顧客データベースは「restricted（制限）」とし、全社員に提供しているHRポータルには、コーポレート・ウェブサイトなどのパブリック・アセットの機密レベルを含みます。
3. **マッピング：**以下を含む全ネットワークのデータ フローをマッピングして関連付けます。
   a. Northバウンド トラフィック：コーポレート ネットワーク限定でマネージド デバイスを使ってSalesforce.comにアクセスしている営業チームなど。
   b. East-Westトラフィック：たとえばフロントエンド ウェブ ポータルからバックエンド サーバーまで。
   c. Southバウンド トラフィック：たとえばウェブサイト バックエンド サーバーからインターネット経由でGoogle Analyticsまで。
4. **グループ化：**類似の機能と機密レベルのアセットを同じマイクロ セグメントにグループ化します。たとえば、ソース コードやチケット管理システムなど、社内のR&Dアセットを1つのグループにします。
5. **導入：**仮想の、または物理的なセグメンテーション ゲートウェイを導入して、各セグメントを制御します。
6. **定義：**各アセットに「最低限の権限」のアクセスポリシーを定義します。たとえば各R&Dグループには、チーム内のソース コードへのアクセス権のみ付与します。

ヒント セグメンテーションの詳細度と、効果的、効率的に管理可能な境界またはマイクロセグメントの数の適切なバランスを見付けます。

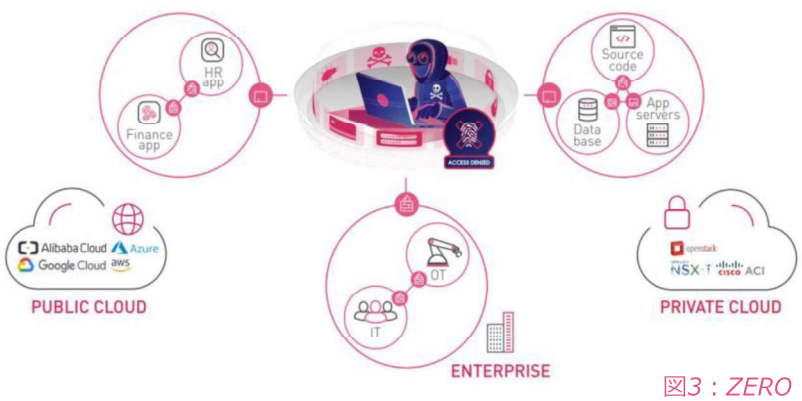


図3：ZERO TRUSTネットワーク

2.

Zero Trust People - 人を信用しない

コンテキストアウェアな認証によって、なりすましを防止

アイデンティティ盗難、すなわち「なりすまし」からの保護はますます重要になっています。データ漏えいの80%が盗まれたクレデンシャル、または弱いクレデンシャルによるものだからです（ユーザー名／パスワードを使ったアプローチでは効果が得られなくなっています）。

Zero Trustモデルはデータのアクセスや処理を行おうとするあらゆる人を決して信用しないことで、こうした問題を回避します。Zero Trustは、各ユーザーからの接続の試みを再確認し、アイデンティティを厳格に認証します。そして接続のあらゆるコンテキストを検査した後に、アクセス権を付与します。

Zero Trust Peopleのベスト プラクティス

1. **アプリケーション レイヤーではなく、ネットワーク レベルでユーザー アイデンティティを認証：**不良アクターはフロント ドアは使用しません。通常、ログイン ページをハッキングするという方法ではなく、アプリケーションの脆弱性を探して悪用します。セキュリティ ゲートウェイでユーザーを認証することで、ハッカーがシステムに近付けないようにし、攻撃サーフェスを最小化することができます。
2. **シングル・サインオン（SSO）によって認証プロセスを簡略化：**認証とアイデンティティ ディレクトリ サービス（Microsoft AD、Cisco ISEなど）を統合します。ユーザーは繰り返しの認証作業（ゲートウェイとアプリケーション）が不要になり、複数のクレデンシャルやパスワードによるリスクも回避できます。
3. **MFA（マルチ・ファクター認証）によるアイデンティティの保護強化：**非常に機密性の高いアプリケーションでは、MFAレイヤーを追加することで保護を強化できます。外部ネットワークから、または不慣れなデバイスを使用して接続する場合など、コンテキスト上、保護強化が必要な場合にもMFAが適しています。
4. **コンテキストアウェアなポリシーの設定：**接続の試みのコンテキストに関する複数の条件を追加して、認証済み接続の定義を狭めます。たとえば具体的な時刻、位置情報、接続方法（VPN/WIFI）、デバイスの種類などを指定します。
5. **異常を検出：**各接続の試みをベースラインと比較して、複数のログイン試行、未認証デバイス、通常とは異なる時間帯や場所など、疑わしい事象を検出します

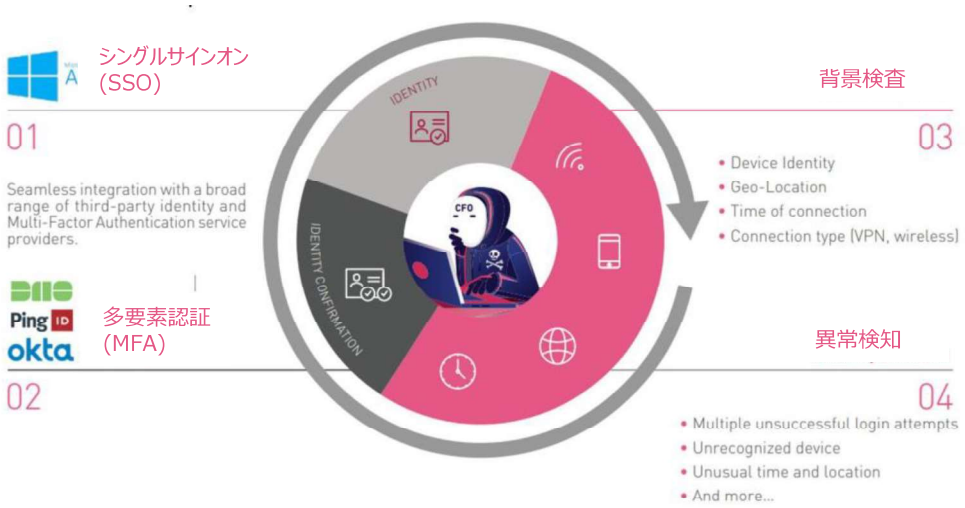


図4：Zero Trust Peopleのための4つのステップ

3.

Zero Trust Devices - デバイスを信用しない

すべてのデバイスを脅威から保護し、万が一攻撃された場合は切り離す

ハッキングの標的は増加し、多様化しています。その範囲もネットワークやワークステーションにとどまらず、多種多様なモバイル・デバイス（その多くが個人所有）、IoT対応デバイス、OT（運用テクノロジー）も含まれるようになりました。

IoTとOTデバイスの脆弱性は特に高いことが多いです。通常、コーポレート・ネットワークに接続され、パッチ未適用のソフトウェアで稼働しているからです。設定ミスも多く、セキュリティが低いプロトコルで通信していることも少なくありません。

この種のデバイスは脆弱性が高く、従来のソリューションではまったく保護されない、または十分に保護されないままです。

そのため、Zero Trustモデルではネットワーク上のすべてのデバイスを保護し、万が一攻撃された場合は切り離す必要があります。

Zero Trust Devicesのベスト プラクティス

1. **IoT/OT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によって、実践的なアプローチで攻撃サーフェースを最小化します。デバイスとのやり取りで発生するトラフィックを厳しく規制し、正常な機能のために最低限必要な通信だけを許可します。ファイアウォールとNACを使った従来のソリューションでは、範囲外のアクティビティを検出、ブロックするための可視性とコンテキストが得られません。専用のIoT/OTセキュリティ ソリューションを実装する必要があります。
2. **信頼できないネットワーク上でワークステーションとモバイル デバイスを保護：**すべての社員のデバイス（BYODを含む）にオンデバイス セキュリティ保護機能をインストールし、ゼロ・デイ マルウェア、悪意のあるアプリのインストール、フィッシング攻撃、bot攻撃などを防止します（MDMモバイル アプリの保護では不十分なため）。
3. **感染したまたは脆弱なデバイスをコーポレート・アセットからブロック：** コンテキストアウェアなアクセス ポリシーを導入し、デバイスのセキュリティ状態に基づき、コーポレート アセットへのアクセスを制限します。たとえば、マルウェアに感染したデバイスやジェイルブレイク(脱獄)されたデバイスやルーテッド モバイル デバイスからのアクセスは拒否する、ディスクを完全に暗号化したエンドポイントへのアクセスに限定する、といった制限が可能です。

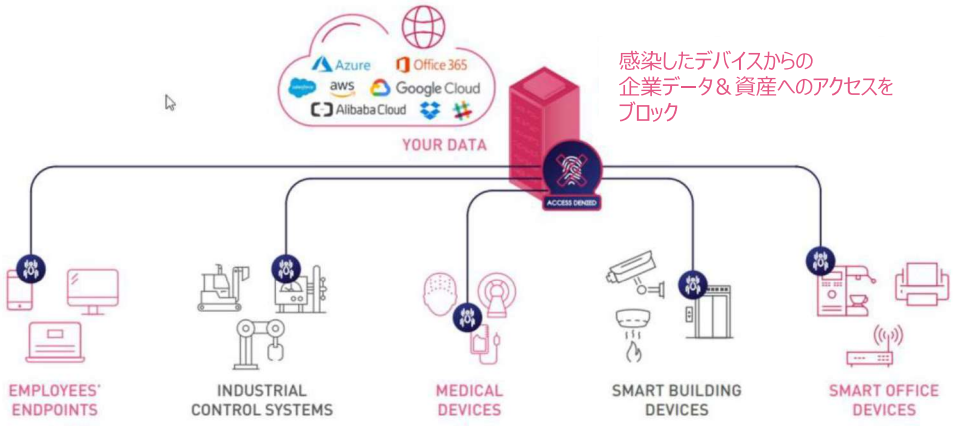


図5：*Zero Trust Devices* - 対象デバイスにはワークステーション、モバイル・デバイス、*IoT*、*OT*デバイスが含まれる。

4.

Zero Trust Data - データを信用しない

場所に関係なく、データを分類、保護、暗号化

今やネットワークは複雑化し、重要なビジネス・データがたどる道筋もリスクの多いものになっています。ワークステーション、モバイル・デバイス、アプリケーション・サーバー、データベース、SaaSアプリケーション、コーポレート・ネットワークやパブリック・ネットワークで絶え間なく共有されているデータを保護することは至難の業です。

データに対してZero Trustアプローチを採用することは必須で、そのためにはデータの場所に関係なく（保存中、移動中、使用中のいずれであっても）、暗号化、分類、保護を組み合わせて実施する必要があります。

セキュリティ専門家の50%が、社内での実装が最も困難なセキュリティの原則としてデータの暗号化、分類、保護を挙げています。（チェック・ポイントの調査による）

Zero Trust Dataのベスト プラクティス

1. **データの暗号化：** その場所に関係なく、また使用中や移動中、レンダリング中であっても、データを暗号化しておけば、万が一の盗難時にも保護されます。
    - エンドポイントのハード ドライブ上でディスク全体またはポータブル メディアの暗号化を行います。これにはユーザー データ、オペレーティング システム ファイル、一時ファイルや削除済みのファイルも含まれます。
    - アクセス コントロール、認証、暗号化を統合したリモート ユーザー向けのセキュア アクセスを提供します（たとえばIPsec VPN、認証プロキシ、モバイル セキュア コンテナー アプリケーションなど）。
2. **DLP（データ ロス防止）**

社員が機密ファイルを分類、保護できるようにする：移動先や共有方法（パブリック ネットワークまたは社内ネットワーク）に関係なく、社員一人ひとりに保護策として提供します。ファイルや文書に対して、特定ユーザーの様々な使用権限（表示、編集、共有など）を定義できます。

DLPソリューションをゲートウェイやSaaSアプリケーションに導入：機密データの動きを追跡、制御し、メール、ウェブ閲覧、ファイル共有サービスによってデータがコーポレート ネットワークの外に出ないようにします。

- コーポレート ポリシーまたは様々な規制（GDPR、HIPPA、CPI）に従って、ネットワーク上のどのデータが機密で、保護が必要なのかを識別します。
- たとえば社会保障番号、銀行口座番号、ソース コードなど、データ タイプごとに事前にラベルを定義します。
- ラベルを使用してコンテンツ アウェアなDLPポリシーを設定します。これによって機密データを正確に識別、処理でき、誤検出の数を減少させることができます。

ヒント

データ使用ポリシーに対する社員の認識を高め、セキュリティ ボトルネックを解消するために、自己修復型のDLPポリシーを設定することをお勧めします。これにより、データの不正処理があればユーザーにリアルタイムに通知し、問題の送信、破棄、確認という選択肢を選べるようになります。

5.

Zero Trust Workloads - ワークロードを信用しない

可視化機能の強化と柔軟なポリシーによってワークロードを保護

ワークロード、中でもパブリック クラウド上のワークロードのセキュリティ確保は特に重要です。この種のクラウド アセット（コンテナー、機能、VMなど）は脆弱で、悪意のあるアクターにとっては魅力的な標的になりやすいからです。

クラウドは非常に動的な環境で、IPアドレスは常に変化します。そのため、IPベースのコントロールがほぼ不可能です。さらに、クラウド ベースのアセットは非常に動的かつ高速にプロビジョニング／デコミッショニングするので、従来のセキュリティ コントロールでは識別することや、セキュリティ ポリシーを順応させることができません。

こうした課題を克服するには、変化の激しいパブリックおよびプライベート クラウド アセットを完全に把握する必要があります。

また、こうしたアセットのセキュリティ状態を常に判断できなければなりません。これにより、設定ミスやセキュリティ ギャップをすぐに検出し、ポリシーを能動的に適用することができます。

Zero Trust Workloadsのベスト プラクティス

1. たとえば財務アプリケーションなど、保護が必要なクラウド アセットを定義します。
2. このクラウド アセットに関連するすべてのワークロードを識別し、同じラベルを使ってグループ分けします。たとえば財務アプリケーションに属するすべてのVMには、「Financial App.」というラベルを付けます。
3. 「最低限の権限」に基づき、社内のセグメンテーションを定義します。たとえば、財務アプリケーションは顧客データベースとの通信を行う、と定義します。
4. 「Financial app」のラベルを使用してアクセス コントロール ポリシーを設定し、このセグメンテーションを適用します

Zero Trust Workloadsのセキュリティ チェック リスト

- **シームレスな統合：**プライベートおよびパブリック クラウド環境とそのネイティブ コントロールによってシームレスに統合します。AWS、GCP、Microsoft Azure、Oracle Cloud、IBM Cloud、Alibaba Cloud、NSX、Cisco ACI、OpenStackなどが含まれます。
- **クラウド可視化ツール：**セキュリティ グループ、インスタンス、ファイアウォールを含むクラウド アセット トポロジーをリアルタイムに構築します。
- **アセット中心のポリシー管理：**クラウド アセットを動的なオブジェクト（アプリケーション、セキュリティ グループなど）にグループ分けし、それぞれに対応したポリシー設定を行います。
- **North-Southトラフィックに対する脅威の防止：**ゲートウェイ（IPSやWAFなど）上で脅威を回避します。

図6：*Zero Trust Workloads*はパブリック・クラウドを使用している方にとっては特に重要

6.

可視性とアナリティクス

セキュリティ・リスクを一元表示して、脅威をすぐに検出、回避

「目に見えない、または理解できない脅威には対処できない。」
(Forrester)

データ漏えいが検出されないまま数か月も経過しまうことがよくあります。事実、漏えいの検出と対処に要する平均的な日数は66日です。

このような課題に対処するため、Zero Trustセキュリティ モデルはネットワーク上のあらゆるアクティビティの継続的な監視、ログ作成、関連付け、分析を行い、セキュリティ チームが全体的なセキュリティ状況を把握できるようにします。その結果、すぐに脅威を検出し、被害を回避することができます。

可視性を高めるためのベスト プラクティス

1. **一元化されたセキュリティ管理を確立：**各セキュリティ ポイントのあらゆる種類のイベントを一元化表示し、脅威の傾向と総合的なセキュリティ状況を完全に把握できるようにします。
2. **各アクティビティのログ：**エンドポイントを含むネットワーク全体（疑わしい場合も、そうでない場合も）のログを残します。これにより、インシデント調査に必要なフォレンジックや、ビッグ・データの分析が可能になります。
3. **ビッグ データ分析ツールの使用：**各ネットワーク、エンドポイント、クラウドのあらゆるセキュリティ イベントを集約して、相互関係を確かめ、悪意のあるアクティビティやセキュリティ違反を識別します。
4. **脅威インテリジェンス サービスの活用：**大規模でグローバルな顧客ベースから得た情報を集約し、総合的で最新の脅威インジケーターを提供します。そして、この情報を全セキュリティ エンドポイントの間で自動的に共有します。

セキュリティ専門家の44%が、脅威の可視化とアナリティクスの原則を実装することが最大の課題と回答している。
（チェック・ポイントの調査による）

7.

自動化とオーケストレーション

豊富なAPIを使用してセキュリティ タスクやインシデント レスポンスを自動化

今日のような動的で課題の多いセキュリティ環境では、エラーの可能性は決して小さくありません。そのため、時間がかかり、エラーが発生しやすい手作業に依存するのをやめて、エンタープライズ全体で自動化とオーケストレーションを導入することが重要です。

Zero Trustセキュリティ アーキテクチャを企業や組織のセキュリティおよびIT環境と統合し、スピードとアジリティを高める必要があります。これにより、インシデント対応、ポリシー精度、タスク委譲についても改善できます。

自動化とオーケストレーションのベスト プラクティス

1. **セキュリティ管理者の作業負担を軽減：**
    - 繰り返しのセキュリティ タスクをカスタム ワークフローに変換し、自動的に実行、スケジュールに従って実行、またはイベントによって実行をトリガーします。
    - セキュリティ ポリシー内のオブジェクトと外部オブジェクト ストア（たとえばMicrosoft Active DirectoryまたはCisco ISE）との確実な動的リンクによって、スタッフの作業時間や人的エラーによるリスクを大幅に削減します。
    - ポリシー管理を関連する企業や組織に委託することで、不要なコミュニケーションや調整が減少します。
2. **インシデントの検出と復旧を自動化：**SIEMシステムにセキュリティ コントロールを統合し、イベント ログや脅威インテリジェンスなど、セキュリティ インシデントに関する詳細なインサイトを提供します。どちらからも統合できることを確認し、SIEMで分析を行った後、ポリシー変更のトリガーや機能実行のためのIoC（Indication of Compromise）提供が行えるようにします。
3. **APIを活用してITエコシステム全体と統合：**

    セキュリティ ソリューションや製品のAPIを使用して、SIEM、ネットワーク管理、セキュリティ・アセスメント、アイデンティティ アウェアネス、コンプライアンス テストと監査、チケット、ワークフロー管理などのシステムと統合します。

興味深いインサイト

2019年8月にチェック・ポイントが実施した調査では、セキュリティ専門家に自社での実装が最も難しい原則を3つ挙げてもらいました。結果はZero Trust Data、可視性とアナリティクス、自動化とオーケストレーションでした。

御社内で実装が最も難しいと思われる原則は何ですか？
トップ3を挙げてください。

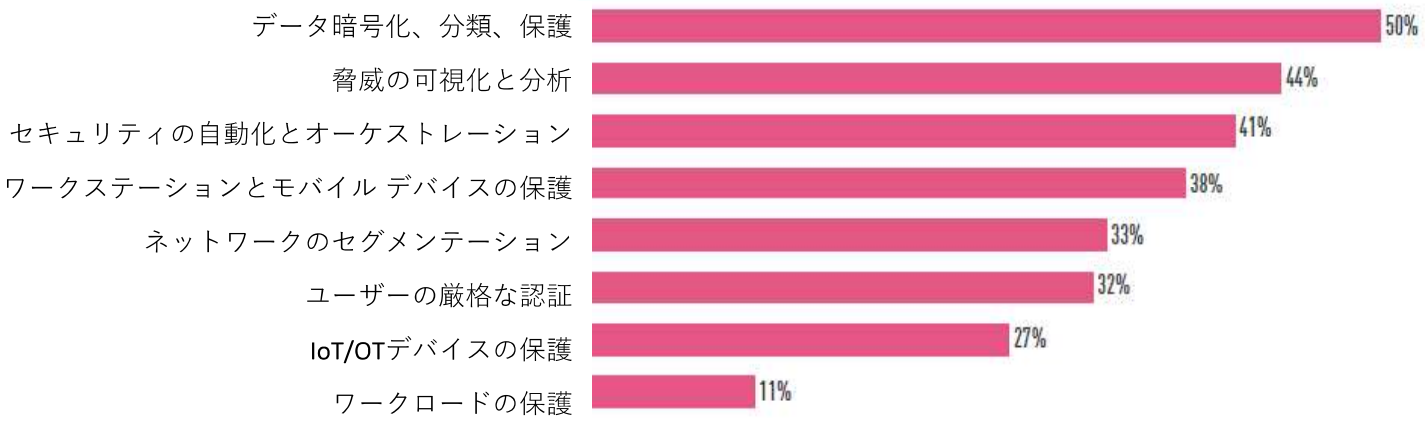


図7：チェック・ポイントがセキュリティ専門家を対象に実施した調査

Zero Trust：まとめ

今日のセキュリティ環境はかつてないほど複雑になっており、データ、アセット、ネットワークの保護がますます難しくなっています。

しかしZero Trust Securityの原則に従い、本書で紹介したベスト プラクティスやテクノロジーを実装することで、あらゆる企業や組織はセキュリティ環境を大幅に改善し、最も重要なデータ関連アセットの保護を強化することができます。

Check Point Infinityによる完全なZero Trust Security

ZERO TRUST SECURITYへの実践的かつ総合的なアプローチ

サイバー脅威を防止するためのZero Trust戦略を検討する場合、このアプローチを中心に個別のテクノロジーを使ってセキュリティ インフラストラクチャを新たに構築すると、複雑化してしまい、セキュリティ ギャップが発生する可能性があります。

こうしたリスクを克服するために、チェック・ポイントはAbsolute Zero Trust Security（完全なZero Trust Security）を提供しています。これはZero Trustを実装するための実践的かつ総合的なアプローチで、Check Point Infinityによる一元化された統合サイバーセキュリティ アーキテクチャがベースになっています。

チェック・ポイントのソリューションによって、企業や組織はZero Trustの原則をすべて完全に実装することができます。脅威の防止に重点を置き、一元化したセキュリティ コンソールで管理することで、他では得られないほど強力なセキュリティを高い効率で達成し、Zero Trustの実装を実現します。

COMPLETE

全てのZero Trustの原則を達成する

EFFICIENT

単一コンソールと統合ポリシーの使用で集中管理

PREVENTIVE

脅威防御に集中し、ゼロデイ攻撃から保護します。

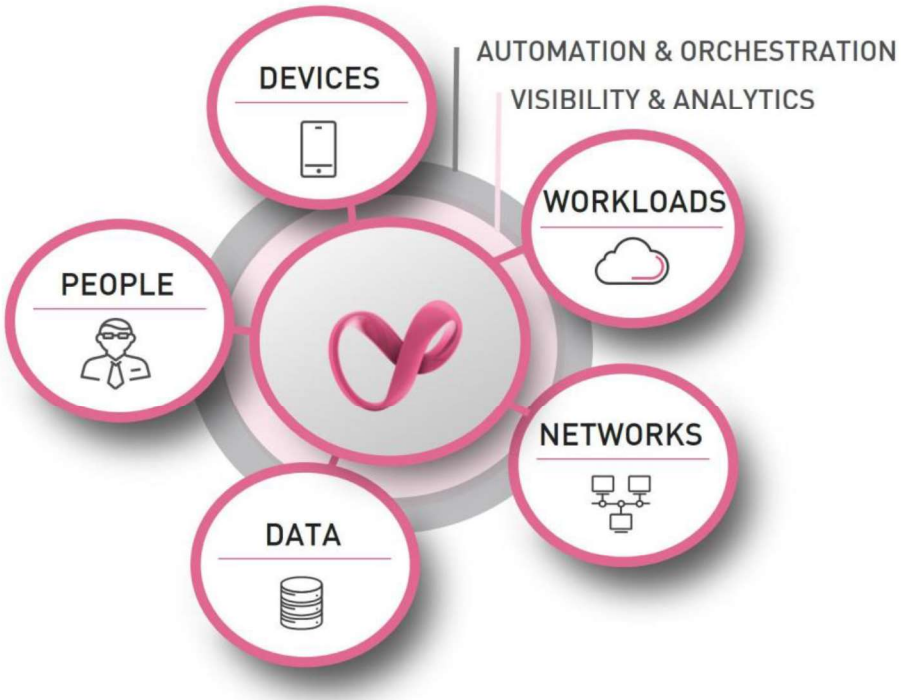


図8：Check Point InfinityによるAbsolute Zero Trust Security

業界初のZERO TRUST SECURITYワークショップ

ABSOLUTE ZERO TRUSTへのジャーニーを今すぐ始めましょう

Zero Trust実装への安全なジャーニーをサポートするため、チェック・ポイントは業界初のZero Trust Securityワークショップを開催します。

様々な業界で、規模の異なる企業や組織向けにZero Trust Securityモデルの設計、実装を行ってきた専門的なセキュリティ アーキテクト チームが作成、実施するワークショップです。

2日間のワークショップでは、お客様の既存のセキュリティ インフラストラクチャをあらゆる角度から確認した上で、カスタマイズしたZero Trust Security戦略を設計し、具体的なビジネス・ニーズに即した実装プランを提案します。

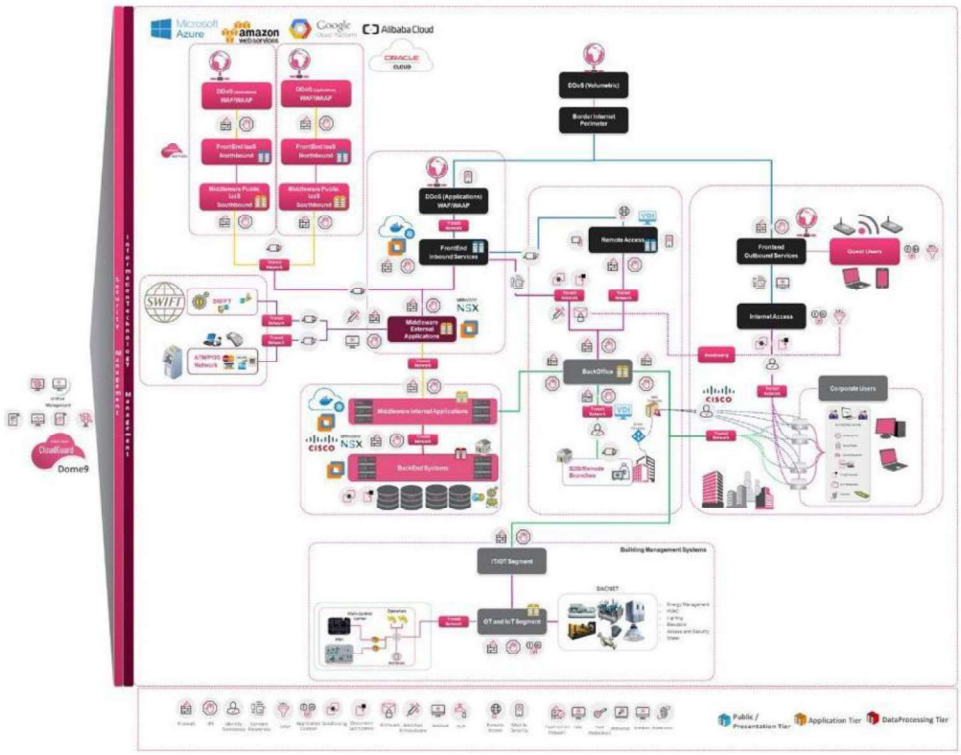


図9：チェック・ポイントのアーキテクチャ チームが設計したZero Trustアーキテクチャ設計図。

チェック・ポイントのZero Trust Securityワークショップの詳細は、お問い合わせください。

インターナショナル本社 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel：972-3-753-4555 | E-mail：info@checkpoint.com
https: // www.checkpoint.com

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
E-mail: info_jp@checkpoint.com
https: // www.checkpoint.com/jp

2019/11