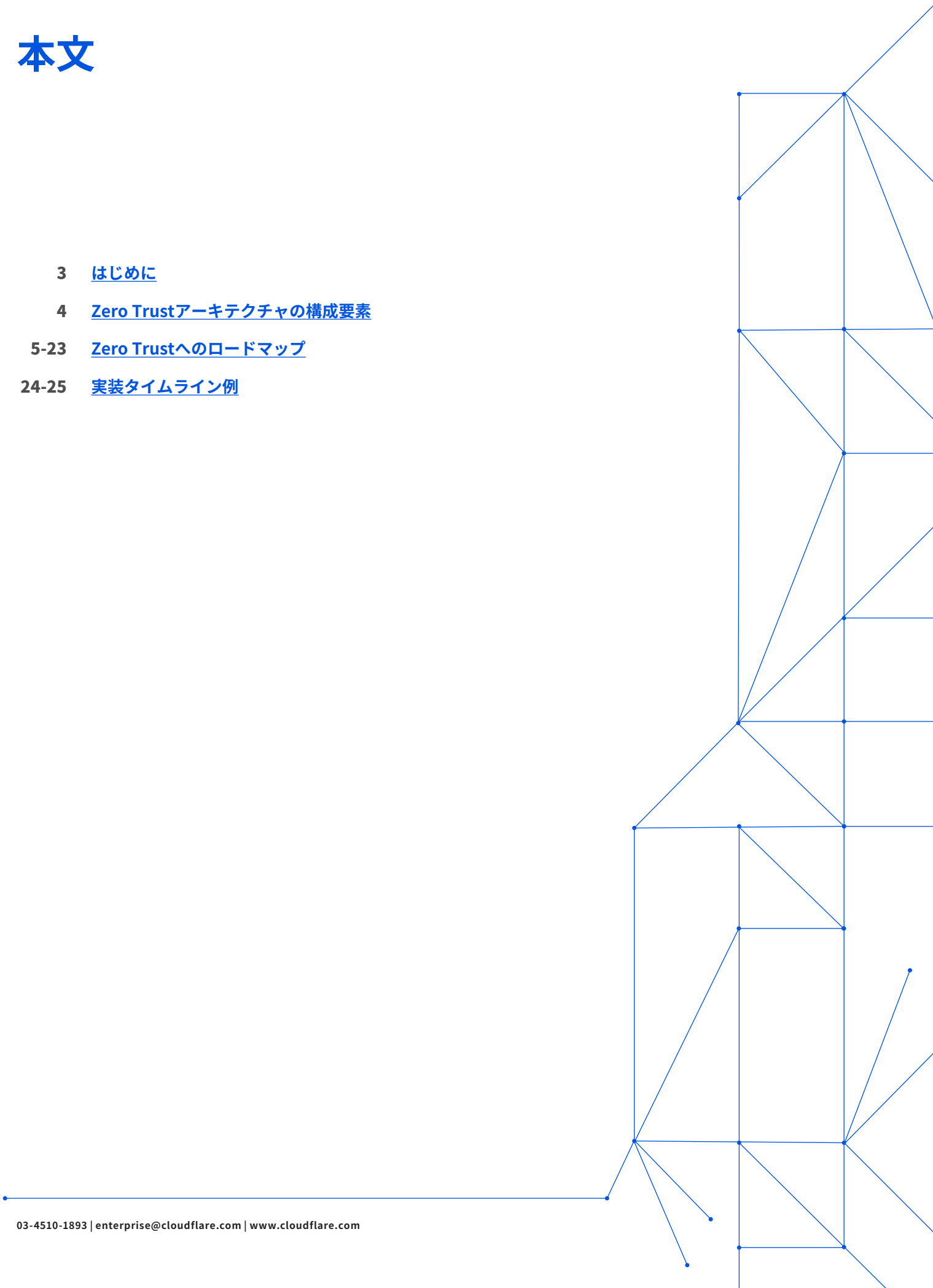
CLOUDFLARE

ホワイトペーパー

Zero Trustアーキテクチャへのロードマップ

ネットワークを変革し、セキュリティを近代化するために必要なステップ、ツール、チームについて学ぶ

本文



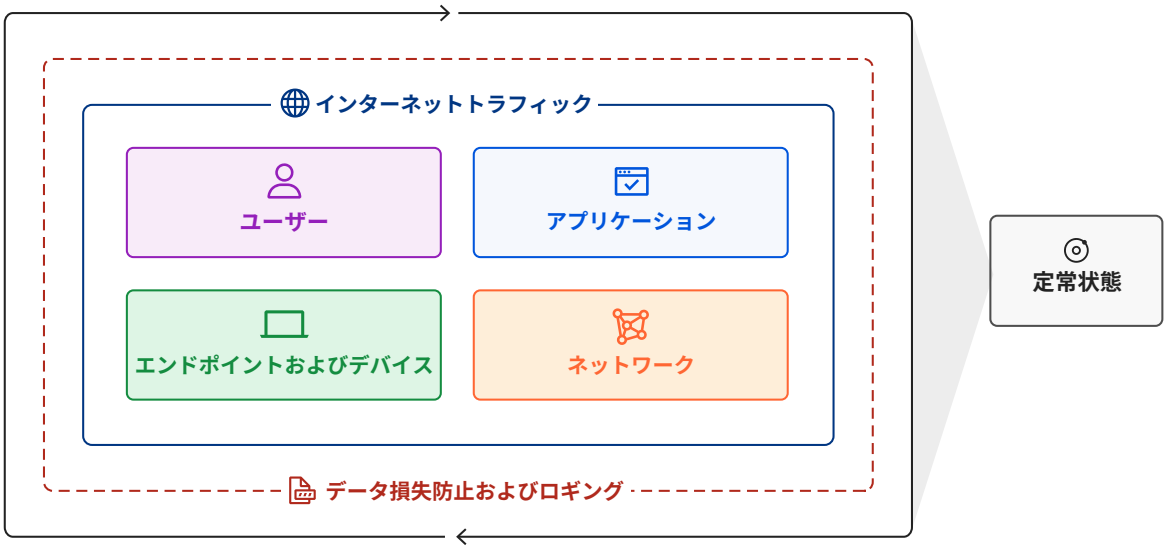
はじめに

従来のネットワークアーキテクチャは、境界ネットワークというコンセプトで構築されており、誰かがネットワークに接続すれば、暗黙のうちに信頼関係が築かれていました。クラウドホスティングやリモートワークなどの近代化への移行により、従来の境界ネットワークアーキテクチャでは課題が生じました。

これらの課題は、Zero Trustアーキテクチャを実装することで対処できます。これにより、ビジネス内外のすべてのトラフィックは確実に検証され、承認されます。Zero Trustアーキテクチャの実装は、従業員の生産性や接続性を阻害することなく、段階的に行うことができます。

このガイドは、セキュリティの専門家が、ベンダーにとらわれないZero Trustアーキテクチャと実装のタイムライン例を提供するために作成されました。このタイムラインは、組織がゼロからZero Trustの行程を始めることを想定していますが、すべての組織にとって有用であることを意図しています。

組織のセキュリティには、包括的なZero Trustアーキテクチャを導入する際に考慮しなければならない7つの主要な要素があります。実装の順番は、以下の要素とリファレンスアーキテクチャのセクションに記載されている方法と一致させる必要はありません。



Zero Trustアーキテクチャの構成要素

	構成要素	目的	作業労力のレベル	ページ
フェーズ1	インターネットトラフィック	グローバルDNSフィルタリングの導入	▮	9
	アプリケーション	インバウンドメールの監視とフィッシング攻撃の排除	▮	13
	DLPおよびログ	SaaSツールの設定ミスや公に共有されたデータの特定	▮	20
フェーズ2	ユーザー	コーポレートアイデンティティの確立	▮▮	5
	ユーザー	すべてのアプリケーションに基本的なMFAを適用	▮	6
	アプリケーション	HTTPSおよびDNSSECを適用する	▮	17
	インターネットトラフィック	SSLの背後にある脅威をブロックまたは隔離	▮▮	9-10
	アプリケーション	パブリックアドレス可能なアプリへのZTポリシーの適用	▮	14-16
	アプリケーション	レイヤー7攻撃からアプリケーションを保護	▮	16
	ネットワーク	アプリ配信のためにインターネットに開放されているすべてのインバウンドポートを閉じる	▮	12
フェーズ3	アプリケーション	すべての企業内アプリケーションのインベントリ作成	▮▮	13-14
	アプリケーション	SaaSアプリケーションへのZTポリシーの適用	▮▮	14-16
	ネットワーク	ユーザーのネットワークアクセスをセグメント化	▮▮▮	11
	アプリケーション	重要でプライベートアドレス可能なアプリケーションのためのZTNA	▮	14-16
	デバイス	MDM/UEMの導入による企業デバイスの制御	▮▮	7
	DLPおよびログ	機密性の高いデータと、それが存在する場所を定義	▮▮	18-19
	ユーザー	ハードウェアベースの認証トークンの送信	▮▮	6
	DLPおよびログ	既知の脅威要因に関する最新情報の入手	▮	21
フェーズ4	ユーザー	ハードウェアトークンベースのMFAを適用	▮▮	6
	アプリケーション	すべてのアプリケーションのZTポリシーの適用とネットワークアクセス	▮▮▮	14-16
	DLPおよびログ	ログレビュー、ポリシーの更新、緩和を行うSOCの確立	▮▮	20
	デバイス	エンドポイント保護の導入	▮▮	7
	デバイス	すべての企業デバイス、API、サービスのインベントリ作成	▮	8
	ネットワーク	支店間接続にブロードバンドインターネットを利用する	▮▮▮	11-12
	DLPおよびログ	機密性の高いアプリでの従業員のアクティビティの記録および確認	▮▮	18
	DLPおよびログ	アプリケーションからの機密データの流出を阻止	▮▮▮	19
	定常状態	新規リソースのポリシー適用のためのDevOpsアプローチ	▮▮	22
	定常状態	オンランプリソースのオートスケーリングの実装	▮▮▮	22-23

それぞれのステップに必要な作業労力のレベルを、以下のように定義しています。

- ▮ - **小規模な作業労力**：これは個人または小さなチームでできることです
- ▮▮ - **中規模な作業労力**：これにはチームと事前準備が必要です
- ▮▮▮ - **大規模な作業労力**：これには複数のチームとプロジェクト計画が必要です

Zero Trustへのロードマップ

ユーザー

ユーザーには、従業員、請負業者、顧客が含まれます。Zero Trustを実現するためには、組織はまず、誰が何を信頼すべきなのかを正確に把握する必要があります（これは「アイデンティティ」とも呼ばれるものです）。また、ユーザーのアイデンティティを安全に認証する方法を確立しなければならなりません。

コーポレートアイデンティティの確立

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• IDプロバイダを担当するチーム（通常はセキュリティまたはIT） • 従業員やパートナーが利用する社内アプリを管理する管理者
製品名	Microsoft Azure AD、Okta、Ping Identity PingOne、OneLogin
まとめ	企業のアプリケーションにアクセスするユーザーを正確に認証・承認するためには、統一されたコーポレートアイデンティティが必要です。一貫性のあるコーポレートアイデンティティは、アプリケーションのきめ細かなポリシー適用をよりシームレスにします。 **その他の考慮すべき点：** • あなたの会社はM&Aに意欲的なのか？アイデンティティストアをどのように統合するのか？ • ウェブベース以外の認証プロトコルを使用しているか（アクティブディレクトリ、ntlm、kerberosなど）
手順	1. すべての企業ユーザーをIDプロバイダーに追加します a. これらの値は、多くの場合、WorkdayやADPなどの人事システムから同期させることができます 2. 各ユーザーの情報が正しいかどうかを確認します 3. 新規ユーザーの登録情報を送信し、ログイン認証情報を設定します

すべてのアプリケーションで多要素認証を実施する

作業労力のレベル	- **小規模な作業労力**（基本的なMFAを適用する場合） - **中規模な作業労力**（ハードキーを使用する場合）
関与するチーム	• IDプロバイダを担当するチーム（通常はセキュリティまたはIT） • 社員やパートナーが利用する社内アプリを管理する管理者
製品名	**IDプロバイダー：**Microsoft Azure AD、Okta、Ping Identity PingOne、OneLogin **アプリケーションリバースプロキシ：**Microsoft Azure ADアプリプロキシ、Akamai EAA、Cloudflare Access、Netskope Private Access、Zscaler Private Access (ZPA) **ハードキー：**Yubico
まとめ	多要素認証（MFA）は、フィッシングや情報漏えいによって盗まれたユーザー認証情報に対する最良の防御策です。ほとんどのMFAは、IdPで直接有効にすることができます。 IdPと直接統合されていないアプリケーションの場合、アプリケーションの前にアプリケーションリバースプロキシを使用してMFAの適用を検討してください。
手順	1. 内部ユーザーに対して、近々実施されるMFAを警告します。SMSまたはアプリベースの認証にサインアップするオプションを提供します 2. IdPでMFAを有効化します 3. IdPと統合されていないアプリケーションの前で、アプリケーションリバースプロキシを有効化します 4. （ボーナス）従業員へハードウェアキーを郵送または直接配布します 5. （ボーナス）最も機密性の高いアプリケーションに、ハードウェアキーのみのMFAを適用します

エンドポイントおよびデバイス

エンドポイントとデバイスには、組織内のあらゆるデバイス、API、ソフトウェアサービス、または組織のデータにアクセスするものが含まれます。組織はまず、デバイス、API、およびサービスの完全なセットを理解する必要があります。そして、デバイス、API、サービスのコンテキストに基づいてZero Trustポリシーを実装することができます。

モバイル端末管理の導入

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• ITチーム
製品名	**Mac：**Jamf、Kandji **Windows：**Microsoft Intune
まとめ	Zero Trustアーキテクチャの多くは、少なくともユーザーマシンのサブセットにソフトウェアをインストールする必要があります。モバイル端末管理（MDM）は、多くの企業がユーザーデバイスのインベントリ全体にわたってソフトウェアと構成を管理する方法です。
手順	詳細については、MDMベンダーのサイトをご覧ください。

エンドポイント保護の導入

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• セキュリティチーム • ITチーム
製品名	VMWare Carbon Black、Crowdstrike、SentinelOne、Windows Defender
まとめ	エンドポイント保護ソフトウェアは、ユーザーのマシンにインストールされ、デバイスに影響を与える既知の脅威をスキャンします。エンドポイント保護ソフトウェアは、OSのパッチやアップデートのコンプライアンスを強制するためにも使用することができます。エンドポイント保護ソフトウェアからの信号は、アプリケーションのアクセスコントロールポリシーに使用することができ、また、使用する必要があります。
手順	1. MDMを使用して、ユーザーのマシンにエンドポイント保護ソフトウェアをインストールします 2. エンドポイント保護プラットフォームで、脅威からの保護とコンプライアンス制御を可能にします

デバイス、API、サービスのインベントリ作成

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• セキュリティチーム • ITチーム
製品名	**デバイスのインベントリ：**VMWare Carbon Black、 Crowdstrike、SentinelOne、Windows Defender、 Oomnitza **API/サービスのインベントリ：**Cloudflare アプリケーションコネクタ、Zscaler Private Access (ZPA)
まとめ	エンドポイント保護ソフトウェアや資産管理ソフトウェアを使用して、ユーザーに配布されたすべてのデバイスを追跡することができます。どのデバイスが有効で、特定のアプリケーションにアクセスする必要があるかを追跡するために、デバイスの正確なリストを維持する必要があります。 また、APIやサービスも検知し、インベントリとして管理する必要があります。ネットワークスキャンを活用することで、内部または外部ネットワーク上で通信可能な、新しく目にしたAPIやソフトウェアサービスを特定することができます。
手順	1. MDMを使用して、ユーザーのマシンにエンドポイント保護ソフトウェアをインストールします 2. ネットワーク内にAPI/サービススキャナーをインストールします

インターネットトラフィック

インターネットトラフィックには、組織の管理外のWebサイトを目的としたすべてのユーザートラフィックが含まれます。これは、ビジネス関連のタスクから個人的なWebサイトの使用まで多岐にわたります。すべてのアウトバウンドトラフィックは、マルウェアや悪意のあるサイトの影響を受ける可能性があります。組織は、インターネットに向かうユーザートラフィックの可視化と制御を確立する必要があります。

既知の脅威や危険な宛先へのDNSリクエストをブロックする

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• ルーターまたはマシン設定のいずれかにアクセス可能なITチーム • セキュリティチーム
製品名	**DNSフィルタリング：**Cisco Umbrella DNS、Cloudflare Gateway、DNSFilter、Zscaler Shift
まとめ	DNSフィルタリングは、ルーターの設定によって、またはユーザーマシンで直接適用することができます。既知の悪意のあるWebサイトからユーザーを保護する最も迅速な方法の1つです。
手順	**DNSフィルタリング：**オフィス無線LANのDNS解決設定を更新し、適切なDNS解決サービスを指すようにします。これは、既知の悪意のあるサイトをブロックするために使用することができます。

SSL/TLSの背後にある脅威をブロックまたは隔離する

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• ルーターまたはマシン設定のいずれかにアクセス可能なITチーム • セキュリティチーム
製品名	**TLSの復号化：**Cloudflare Gateway、Netskope次世代SWG、Zscaler Internet Access (ZIA) **ブラウザ分離：**Cloudflareブラウザ分離、Zscaler Cloudブラウザ分離

SSL/TLSの背後にある脅威をブロックまたは隔離する（続き）

まとめ	脅威の中には、SSLの背後に隠れていて、HTTPSインスペクションだけではブロックできないものがあります。ユーザーをさらに保護するために、TLSの復号化を活用し、SSLの背後にある脅威からユーザーをさらに保護する必要があります。
手順	**TLSの復号化：** 1. 正しいクライアントソフトウェアが、ユーザーマシンにインストールされていることを確認します a. デバイスのアウトバウンドWebトラフィックを妨害する可能性のあるVPNやその他のソフトウェアがないか確認します 2. TLS復号化のためのルート証明書をデバイスに設定します 3. ユーザートラフィックの復号化を回避するタイミングのポリシーを有効化します a. 証明書のピン留めを使用しているサイトでは、この作業を行う必要があります b. 一部の企業では、ユーザーの個人的なトラフィック（銀行、ソーシャルメディアなど）についても復号化を回避しています **ブラウザ分離：** 1. ブラウザ分離は、デバイス上のクライアントソフトウェア、または分離リンクを介して展開することができます。両方のアプローチを検討する必要があります

ネットワーク

ネットワークには、組織内のすべてのパブリックネットワーク、プライベートネットワーク、および仮想ネットワークが含まれます。組織はまず、既存の一連のネットワークを理解し、それらをセグメント化して、横方向の移動を防止する必要があります。そして、ユーザー、エンドポイント、デバイスがアクセスできるネットワークのセグメントをきめ細かく制御するZero Trustポリシーを作成することができます。

ユーザーのネットワークアクセスのセグメント化

作業労力のレベル	**- 大規模な作業労力**
関与するチーム	• セキュリティチーム • ITチーム
製品名	**Zero Trustネットワークアクセス（ZTNA）：**Cloudflare Zero Trust（AccessとGatewayを併用）、Netskope Private Access、Zscaler Private Access (ZPA)
まとめ	ユーザーは通常、VPNを使用して、またはオフィスネットワーク内にいながら、プライベートネットワーク全体にアクセスすることができます。Zero Trustのフレームワークでは、ユーザーは与えられたタスクを完了するために必要なネットワークの特定のセグメントにのみアクセスすることが要求されます。Zero Trustネットワークソリューションでは、ユーザーがローカルネットワークにリモートアクセスすることを可能にしますが、ユーザー、デバイス、その他の要因に基づいたきめ細かいポリシーが設定されています。
手順	1. プライベートネットワークをZTNAで利用できるようにします a. 一般的に、アプリケーションコネクタ、GREまたはIPSecトンネルを使用します 2. MDMを使用してユーザーデバイスにZTNAクライアントをインストールします 3. プライベートネットワーク上のユーザーアクセスをセグメント化するためのポリシーを設定します

支店間接続にブロードバンドインターネットを利用する

作業労力のレベル	**- 大規模な作業労力**
関与するチーム	• ネットワークエンジニアリングチーム • ITチーム
製品名	Cloudflare Magic WAN、Cato Networks、Aryaka FlexCore

支店間接続にブロードバンドインターネットを利用する（続き）

まとめ	プライベートネットワーク拠点間の接続性（例：データセンターと支店）は、一般的に、マルチプロトコルラベルスイッチング（MPLS）回線、または通信事業者が提供する他の形態のプライベート回線で構築されています。このようなMPLSリンクは一般的に高価ですが、商用インターネットが高品質になったことにより、組織はわずかなコストで安全なトンネルを介してインターネット上にトラフィックをルーティングし、同じレベルの安全なアクセスを提供することができます。
手順	1. まず、MPLS接続された2つの拠点を選びます。これらの拠点では、何らかの形でインターネットに接続する必要があります。 2. インターネット回線からクラウドWANプロバイダーのエッジネットワークまで、エニーキャストGREまたはIPsecの一対の冗長トンネルを確立します。 3. これらのトンネル間の正常性と接続性を確認します。トラフィックワークロードのパフォーマンス（スループット、レイテンシー、パケットロス、ジッター）を、可能な限り本番トラフィックに近い形でテストします。 4. 本番トラフィックをMPLSからインターネットトンネルに移行するために、ルーティングポリシーを変更します。 5. 次のMPLS接続先でも繰り返します。 6. MPLS回線を破棄します。

アプリケーション配信のために、インターネットに開いているすべてのインバウンドポートを閉じる

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• ネットワークエンジニアリングチーム
製品名	**Zero Trustリバースプロキシ：**Akamai EAA、Cloudflare Access、Netskope、Zscaler Private Access (ZPA)
まとめ	開いているインバウンドネットワークポートは、スキャン技術を使って見つけることができ、一般的な攻撃ベクトルとなります。Zero Trustリバースプロキシを使用すると、インバウンドポートを開くことなくWebアプリケーションを安全に公開することができます。アプリケーションのDNSレコードは、一般公開される唯一のアプリケーションのレコードです。また、DNSレコードはZero Trustポリシーで保護されています。セキュリティの追加レイヤーとして、Zero Trustネットワークアクセスサービス（詳細は後述）を利用して、内部/プライベートDNSを活用することができます。
手順	1. リバースプロキシアプリケーションコネクタのインストール—通常、同一ネットワーク上のどこかにデーモンまたは仮想マシンを設置します 2. リバースプロキシアプリケーションを、アプリケーションコネクタに接続します 3. ファイアウォールルールで、プライベートネットワーク上のすべてのインバウンドポートを閉じます

アプリケーション

アプリケーションには、組織のデータが存在する、あるいはビジネスプロセスが実行されるあらゆるリソースが含まれます。組織はまず、存在するアプリケーションを理解し、各アプリケーションに対してZero Trustポリシーを確立するか、場合によっては未承認のアプリケーションをブロックする必要があります。

Eメールアプリケーションを監視し、フィッシング攻撃をフィルタリングする

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• メールプロバイダの設定を担当するチーム（通常はIT部門）
製品名	**クラウドメールセキュリティ：**Cloudflare Area 1 Email Security、Mimecast、TitanHQ **ブラウザ分離：**Cloudflareブラウザ分離、Zscaler Cloudブラウザ分離
まとめ	メールは、攻撃者が従業員に自由にアクセスできる数少ない通信経路の一つです。悪意のあるメールや信頼できないメールが従業員に届かないようにするためには、安全なメールゲートウェイを導入することが重要なステップとなります。さらに、セキュリティチームは、完全にブロックするほど疑わしいものではないリンクを、分離したブラウザで隔離するオプションも検討する必要があります。
手順	1. ドメインのMXレコードを設定して、安全なメールゲートウェイサービスを指すようにします 2. 最初の数週間は誤検知を監視します 3. （ボーナス）疑わしい境界線上のメールリンクに対して、リンクベースのブラウザ分離アプローチを実装します

すべての企業内アプリケーションのインベントリ作成

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• セキュリティチーム
製品名	**Shadow IT Discoveryを備えたセキュアWebゲートウェイとCASB：**Cloudflare Gateway、Microsoft Defender for Cloud Apps、Netskope次世代SWG、Zscaler Internet Access (ZIA)

すべての企業内アプリケーションのインベントリ作成（続き）

まとめ	セキュリティチームにとって、ビジネスで使用されるアプリケーションのすべてのインベントリを把握することは非常に重要です。「シャドーIT」とも呼ばれるように、セキュリティチームは、承認されていない、あるいは未知のアプリケーションがビジネス上で使用されていることをよく発見します。TLS復号化機能を持つセキュアWebゲートウェイを使用することで、アプリケーションを特定することができます。セキュアWebゲートウェイは、承認されていないアプリケーションやアプリケーションのテナントをブロックするために使用することもできます（個人のDropboxアカウントなど）。
手順	1. セキュアWebゲートウェイでシャドーITのスキャンを有効にします 2. セキュアWebゲートウェイクライアントが、ユーザーのデバイスにインストールされていることを確認します 3. ユーザーからのトラフィックを2〜3週間分確保します 4. 特定されたアプリケーションのリストを確認します 5. 未承認のアプリケーションは、セキュアWebゲートウェイポリシーでブロックする必要があります 6. 承認されたアプリケーションは、Zero Trustポリシーで保護する必要があります

アプリケーションへのZero Trustポリシーの適用

作業労力のレベル	- **小規模な作業労力**（最も重要なアプリケーション向け） - **大規模な作業労力**（すべてのアプリケーション向け）
関与するチーム	• セキュリティチーム • アプリケーション開発チーム • ITチーム
製品名	**Zero Trustリバースプロキシ：**Azureアプリプロキシ、Cloudflare Access、Netskope Private Access、Zscaler Private Access (ZPA) **Zero Trustネットワークアクセス（ZTNA）：**Cloudflare Access、Netskope Private Access、Zscaler Internet Access (ZIA) **CASB：**Cloudflare CASB 、Netskope CASB、Zscaler CASB **リモートブラウザ分離：**Cloudflareブラウザ分離、Zscaler Cloudブラウザ分離

アプリケーションへのZero Trustポリシーの適用（続き）

まとめ	アプリケーションは、認証とアクセス許可の前に、ユーザーアイデンティティ、デバイス、ネットワークコンテキストを考慮するZero Trustポリシーで保護する必要があります。特に機密データを含むアプリケーションには、最小特権を強制するきめ細かいポリシーを設定する必要があります。アプリケーションの種類は大きく分けて3つあり、それぞれの種類に応じてZero Trustセキュリティモデルも異なります。主なアプリケーションの種類は以下の通りです： 1. プライベートセルフホスト型アプリケーション（企業ネットワーク内でのみアドレス指定可能） 2. パブリックセルフホスト型アプリケーション（インターネット上でアドレス指定可能） 3. クラウドベースのアプローチ **注：**デバイスコンテキスト、またはコンプライアンスステータスが必須のセキュリティポリシーの場合、通常、デバイス上のクライアントソフトウェアが必要です。
手順	**プライベートセルフホスト型アプリケーション** 1. アプリケーションとZero Trustポリシーレイヤーとの間に暗号化トンネルを構築します。通常、これは「アプリケーションコネクタ」、GREまたはIPSecトンネルになります 2. ZTNAデバイスクライアントのユーザーが、プライベートDNSリゾルバーを利用できるようにします 3. ユーザー、デバイス、ネットワークのコンテキストに基づいたポリシーを構築し、アプリケーションにアクセスできるユーザーを確立します **パブリックセルフホスト型アプリケーション** 1. 権威DNSまたはCNAMEレコードをアプリケーションリバースプロキシに移動します 2. アプリケーションのネットワークで、すべてのインバウンドポートが閉じられていることを確認します 3. ユーザー、デバイス、ネットワークのコンテキストに基づいたポリシーを構築し、アプリケーションにアクセスできるユーザーを確立します **クラウドベースのアプローチ** SaaSアプリケーションにZero Trustポリシーを適用するには、いくつかの異なるオプションがあります **プロキシID** Cloudflare、Netskope、およびZscalerは、リバースプロキシのセルフホスト型アプリケーションと同じポリシーの適用を可能にするプロキシIDを提供しています。この場合、プロキシIDがSaaSアプリケーションのSSOプロバイダとして設定されていることが必要です。 1. SaaSアプリへの既存のSSO統合がある場合は、それを削除します 2. IdentityプロキシとSaaSアプリケーションを統合します 3. ユーザーの作成と更新のために、正しいSAML属性が送信されていることを確認します 4. ユーザー、デバイス、ネットワークのコンテキストに基づいたポリシーを作成します

アプリケーションへのZero Trustポリシーの適用（続き）

手順	**セキュアWebゲートウェイとシングルサインオン** もう1つの方法は、既存のシングルサインオンプロバイダーを使用して、SaaSアプリケーションにアクセスできるユーザーとできないユーザーを制御することです。そして、専用のIPアドレスを持つセキュアWebゲートウェイを使用することで、トラフィック検査を行った管理対象機器のユーザーだけがSaaSアプリケーションにアクセスできるようにすることができます。 1. SaaSアプリケーションをSSOプロバイダーに追加します 2. どのユーザーに権限を与えるか、ポリシーを作成します 3. セキュアWebゲートウェイインスタンスのIPアドレスを、SaaSアプリケーションのIP許可リストに追加します（ほとんどのSaaSアプリケーションは、基本セキュリティ設定でIP許可リストをサポートしています） 4. SaaSアプリケーションにアクセスできるユーザーを制御するセキュアWebゲートウェイポリシーを作成します

レイヤー7攻撃（DDoS、インジェクション、ボットなど）からアプリケーションを保護する

作業労力のレベル	- **小規模な作業労力**
関与するチーム	• セキュリティチーム • アプリケーション開発チーム
製品名	Akamai、AWS、Azure、Cloudflare、GCP
まとめ	セルフホスト型アプリケーションは、DDoS、コードインジェクション、ボットなどを含むレイヤー7攻撃を受けやすいものです。セキュリティチームは、プライベートおよびパブリックアドレス可能なすべてのセルフホスト型アプリケーションの前に、Webアプリケーションファイアウォールと DDoS攻撃対策を配備する必要があります。
手順	1. 任意のパブリックアプリケーションの権威DNSレコードを追加します 2. WebアプリケーションファイアウォールとDDoS防御を有効にします

HTTPSおよびDNSSECを適用する

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• セキュリティチーム • アプリケーション開発チーム
製品名	Akamai、AWS、Azure、Cloudflare、GCP
まとめ	セルフホスト型のWebアプリケーションは、HTTPSとDNSSECを利用する必要があります。これにより、パケットスニッフィングやドメインハイジャックの可能性を防ぐことができます。
手順	1. 任意のパブリックアプリケーションの権威DNSレコードを追加します 2. HTTPSをstrictに設定し、DNSSECを有効にします

データ損失防止およびロギング

ここまででアーキテクチャのZero Trust要素をすべて確立したら、アーキテクチャは、ネットワーク内で起きていることに関する大量のデータを生成するようになります。この時点で、データ損失防止およびロギングを導入する必要があります。これらの一連のプロセスとツールは、機密データを企業内部に保持し、データ漏洩の可能性がある場合は注意を与えることに重点を置いています。組織はまず、機密データがどこに存在するかを把握する必要があります。そして、機密データへのアクセスや流出をブロックするためのZero Trust制御を確立することができます。

機密性の高いアプリケーションのトラフィックを記録・レビューするプロセスを確立する

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• セキュリティチーム
製品名	**セキュアWebゲートウェイ（SWG）：** Cisco Umbrella、Cloudflare Gateway、Netskope次世代SWG、Zscaler Internet Access (ZIA) **セキュリティインシデントおよびイベント監視（SIEM）：** DataDog、Splunk、SolarWinds
まとめ	セキュアWebゲートウェイソリューションは、ユーザーのトラフィックログをSIEMツールに渡す機能を備えています。セキュリティチームは、機密性の高いアプリケーション宛てのトラフィックログを定期的に確認する必要があります。SIEMでは、異常なトラフィックや悪意のあるトラフィックに対する特定のアラートを設定し、時間をかけてチューニングすることが可能です。
手順	1. 機密性が高いアプリケーションに向けられたすべてのユーザートラフィックが、SWGを使用してプロキシされていることを確認します 2. SWGおよびSIEM間のログのプッシュ/プル機能を有効化します 3. セキュリティチームがトラフィックログを確認する間隔を設定します 4. 時間の経過に伴う発見をもとにSIEMでアラートを設定します

機密性の高いデータと、それが存在する場所を定義する

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• セキュリティチーム • コンプライアンス／法務関連チーム
製品名	**セキュリティインシデントおよびイベント監視（SIEM）：** DataDog、Splunk、SolarWinds

機密性の高いデータと、それが存在する場所を定義する（続き）

まとめ	機密情報は業種によって大きく異なります。技術系企業はソースコードの保護を懸念し、医療系企業はHIPAAコンプライアンスに大きな関心を寄せています。自社にとって機密データとは何か、それはどこに存在するかを明確にすることが重要です。 機密データの正確な定義とインベントリは、データ損失防止ツールの導入に役立ちます。
手順	1. SIEMツールまたはセキュアWebゲートウェイで直接トラフィックログを確認し、対象となるアプリケーションとデータストアを特定します 2. 既存の機密データのインベントリを作成します

アプリケーションからの機密データの流出を防止する

作業労力のレベル	**- 大規模な作業労力**
関与するチーム	• セキュリティチーム • ITチーム • コンプライアンス／法務関連チーム
製品名	**In-line Data Loss Prevention (DLP)：**Cisco Umbrella、 Cloudflare Gateway、 Netskope Next Gen SWG、 Zscaler Internet Access (ZIA)
まとめ	インラインDLPソリューションは、ユーザーのトラフィックやファイルのアップロード/ダウンロードを検査し、機密データを検出します。機密データは、既知の事前定義されたリスト（PII、SSN、クレジットカードなど）または特定のパターンを、管理者が手動で設定できます。DLP制御は、機密性の高いアプリケーションに対して有効にする必要があり、すべてのユーザートラフィックに対して拡張できます。
手順	1. DLPプロバイダーからクライアントソフトウェアをインストールします 2. 接続性を妨げる既存のVPNや他のツールがないことを確認します 3. TLS復号化が有効で、各ユーザーのマシンにルート証明書が存在することを確認します 4. DLP制御を有効にします 5. DLPブロックイベントを監視し、それが有効か誤検知かを検証します

SaaSツールの設定ミスや公に共有されたデータの特定

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• セキュリティチーム
製品名	**APIベースのクラウドアクセスセキュリティブローカー（CASB）：** Cloudflare CASB 、DoControl、Netskope、Zscaler CSPM
まとめ	CASBは、主要なSaaSアプリケーションとAPI連携で統合します。そしてCASBは、SaaSアプリケーションの既知のセキュリティ設定ミスや、一般に共有されているデータをスキャンします。セキュリティチームは、CASBの発見をレビューするために定期的なスケジュールを確立する必要があります。
手順	1. 各SaaSアプリケーションを、プロバイダーのAPI統合手順で接続します 2. 各SaaSアプリケーションのスキャンを実行します 3. スキャン結果を確認し、各SaaSアプリケーションの適切な修復を開始します

ログレビューおよびポリシーの更新と緩和のためのセキュリティオペレーションセンター（SOC）の設立

作業労力のレベル	**- 中規模の作業労力**
関与するチーム	• セキュリティチーム
製品名	**なし**
まとめ	SOCは、Zero Trustのフレームワークにおけるセキュリティチーム内の重要な機能です。それによってログ情報やセキュリティアラートを確認し、すべてのコアセキュリティ製品でZero Trustポリシーの調整に重点を置く必要があります。
手順	1. SIEMまたはセキュリティ製品に直接記録されたログを確認します 2. アラートまたは異常なアクティビティを特定します 3. 調査結果をもとに、各ツールのZero Trustポリシーを更新します

既知の脅威要因に関する最新情報の入手

作業労力のレベル	**- 小規模な作業労力**
関与するチーム	• セキュリティチーム
製品名	**脅威インテリジェンスプロバイダー：**Cloudflare Radar、CISA、OWASP
まとめ	複数のプロバイダーが、既知の脅威要因や悪意のあるWebサイトのリストを作成することに注力しています。これらの脅威フィードはセキュアWebゲートウェイに自動的にロードされ、ユーザーを攻撃から保護することができます。
手順	1. 脅威フィードをセキュアWebゲートウェイに接続します 2. DNSとHTTPのフィルタリングで脅威からの保護を有効にします

定常状態

組織の他のすべての要素についてZero Trustアーキテクチャを構築した後、組織をZero Trustの定常状態に移行し、アーキテクチャの一貫性を確保するために一連のアクションを実行することができます。

DevOpsアプローチを採用して、すべての新しいリソースに対して一貫したポリシーを適用する

作業労力のレベル	**- 大規模な作業労力**
関与するチーム	• セキュリティチーム • アプリケーション開発チーム
製品名	**インフラ自動化：**Ansible、Puppet、Terraform
まとめ	インフラ自動化ツールにより、開発者はアプリケーション開発パイプラインの一部として、Zero Trustセキュリティを自動的に導入できます。Zero Trustリバースプロキシによる保護が適用されたアプリケーションを展開した場合に、起動する内部テストを確立します。
手順	1. 新規アプリケーションの標準ポリシーを定義します 2. アプリケーションの展開プロセスに、Zero Trustリバースプロキシによる保護を必要とするテストを追加します

オンランプリソースのオートスケーリングの実装

作業労力のレベル	**- 大規模な作業労力**
関与するチーム	• セキュリティチーム • アプリケーション開発チーム
製品名	**ロードバランサー：**Akamai、Cloudflare **インフラ自動化：**Ansible、Puppet、Terraform

オンランプリソースのオートスケーリングの実装（続き）

まとめ	ロードバランサーは、個々のアプリケーションインフラが過負荷にならないようにするための効果的なツールです。また、1台のアプリケーションサーバーに障害が発生した場合にも、冗長性を確保することができます。 インフラ自動化ツールを使用すると、特定のトラフィックしきい値を超えた場合に新しいリソースをスピンアップすることができます。
手順	1. Zero Trustリバースプロキシアプリケーションコネクタの前に、ロードバランサーを設定します 2. トラフィック量やユーザーの地理的位置に基づいて、負荷分散ルールを有効にします 3. 特定のアプリケーションに十分な負荷が発生した場合に、新しい仮想マシンをプロビジョニングするインフラ自動化ポリシーを実装します

実装タイムライン例

Zero Trustアーキテクチャの導入はすべてユニークですが、ほとんどのプロジェクトが従う共通の手順があります。これは、Zero Trustアーキテクチャの実装に着手する企業に推奨されるタイムラインです。

タイムライン		目的	関連製品
フェーズ1	☐	グローバルDNSフィルタリングの導入	Cisco Umbrella DNS、Cloudflare Gateway、DNSFilter、Zscaler Shift
	☐	インバウンドメールの監視とフィッシング攻撃の排除	クラウドメールセキュリティ：Cloudflare Area 1 Email Security、Mimecast、TitanHQ ブラウザ分離：Cloudflareブラウザ分離、Zscaler Cloudブラウザ分離
	☐	SaaSツールの設定ミスや公に共有されたデータの特定	Cloudflare CASB、DoControl、Netskope、Zscaler CSPM
フェーズ2	☐	コーポレートアイデンティティの確立	Microsoft Azure AD、Okta、Ping Identity PingOne、OneLogin
	☐	すべてのアプリケーションに基本的なMFAを適用	IDプロバイダー：Microsoft Azure AD、Okta、Ping Identity PingOne、OneLogin アプリケーションリバースプロキシ：Microsoft Azure ADアプリプロキシ、Akamai EAA、Cloudflare Access、Netskope Private Access、Zscaler Private Access (ZPA)
	☐	HTTPSおよびDNSSECを適用する	Akamai、AWS、Azure、Cloudflare、GCP
	☐	SSLの背後にある脅威をブロックまたは隔離	TLSの復号化：Cloudflare Gateway、Netskope次世代SWG、Zscaler Internet Access (ZIA) ブラウザ分離：Cloudflareブラウザ分離、Zscaler Cloudブラウザ分離
	☐	パブリックアドレス可能なアプリへのZTポリシーの適用	Zero Trustリバースプロキシ：Azureアプリプロキシ、Cloudflare Access、Netskope Private Access、Zscaler Private Access (ZPA)
	☐	レイヤー7攻撃からアプリケーションを保護	Akamai、AWS、Azure、Cloudflare、GCP
	☐	アプリ配信のためにインターネットに開放されているすべてのインバウンドポートを閉じる	Akamai EAA、Cloudflare Access、Netskope、Zscaler Private Access (ZPA)
フェーズ 3	☐	すべての企業内アプリケーションのインベントリ作成	Shadow IT Discoveryを備えたセキュアWebゲートウェイとCASB：Cloudflare Gateway、Microsoft Defender for Cloud Apps、Netskope次世代SWG、Zscaler Internet Access (ZIA)
	☐	SaaSアプリケーションへのZTポリシーの適用	Zero Trustネットワークアクセス（ZTNA）：Cloudflare Access、Netskope Private Access、Zscaler Internet Access (ZIA) CASB：Cloudflare CASB 、Netskope CASB、Zscaler CASB

	☐ ユーザーのネットワークアクセスのセグメント化	**Zero Trustネットワークアクセス（ZTNA）：** Cloudflare Zero Trust（AccessとGatewayを併用）、Netskope Private Access、Zscaler Private Access (ZPA)
	☐ 重要でプライベートアドレス可能なアプリケーションのためのZTNA	Cloudflare Access、Netskope Private Access、Zscaler Internet Access (ZIA)
	☐ MDM/UEMの導入による企業デバイスの制御	**Mac：** Jamf、Kandji **Windows：** Microsoft Intune
	☐ 機密性の高いデータと、それがどこにあるのかを定義する	DataDog、Splunk、SolarWinds
	☐ ハードウェアベースの認証トークンの送信	**ハードキー：** Yubico
	☐ 既知の脅威要因に関する最新情報の入手	Cloudflare Radar、CISA、OWASP
フェーズ4	☐ ハードウェアトークンベースのMFAを適用	**ハードキー：** Yubico
	☐ すべてのアプリケーションへのZTポリシーの適用とネットワークアクセス	Cloudflare Access、Netskope Private Access、Zscaler Internet Access (ZIA)
	☐ ログレビュー、ポリシーの更新・緩和を行うSOCの確立	該当なし
	☐ エンドポイント保護の導入	VMWare Carbon Black、Crowdstrike、SentinelOne、Windows Defender
	☐ 企業内のすべてのデバイス、API、サービスのインベントリ作成	**デバイスのインベントリ：** VMWare Carbon Black、Crowdstrike、SentinelOne、Windows Defender、Oomnitza **API/サービスのインベントリ：** Cloudflareアプリケーションコネクタ、Zscaler Private Access (ZPA)
	☐ 支店間接続にブロードバンドインターネットを利用する	Cloudflare Magic WAN、Cato Networks、Aryaka FlexCore
	☐ 機密性の高いアプリケーションにおける従業員のアクティビティを記録・レビューするプロセスの確立	**セキュアWebゲートウェイ（SWG）：** Cisco Umbrella、Cloudflare Gateway、Netskope次世代SWG、Zscaler Internet Access (ZIA) **セキュリティインシデントおよびイベント監視（SIEM）：** DataDog、Splunk、SolarWinds
	☐ アプリケーションからの機密データの流出を防止する（例：PII、クレジットカード、SSN、その他）	Cisco Umbrella、Cloudflare Gateway、Netskope次世代SWG、Zscaler Internet Access (ZIA)
	☐ DevOpsアプローチを採用して、すべての新しいリソースにポリシーを適用する	Ansible、Puppet、Terraform
	☐ オンランプリソースのオートスケーリングの実装	**ロードバランサー：** Akamai、Cloudflare **インフラ自動化：** Ansible、Puppet、Terraform

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3584.2022AUG09