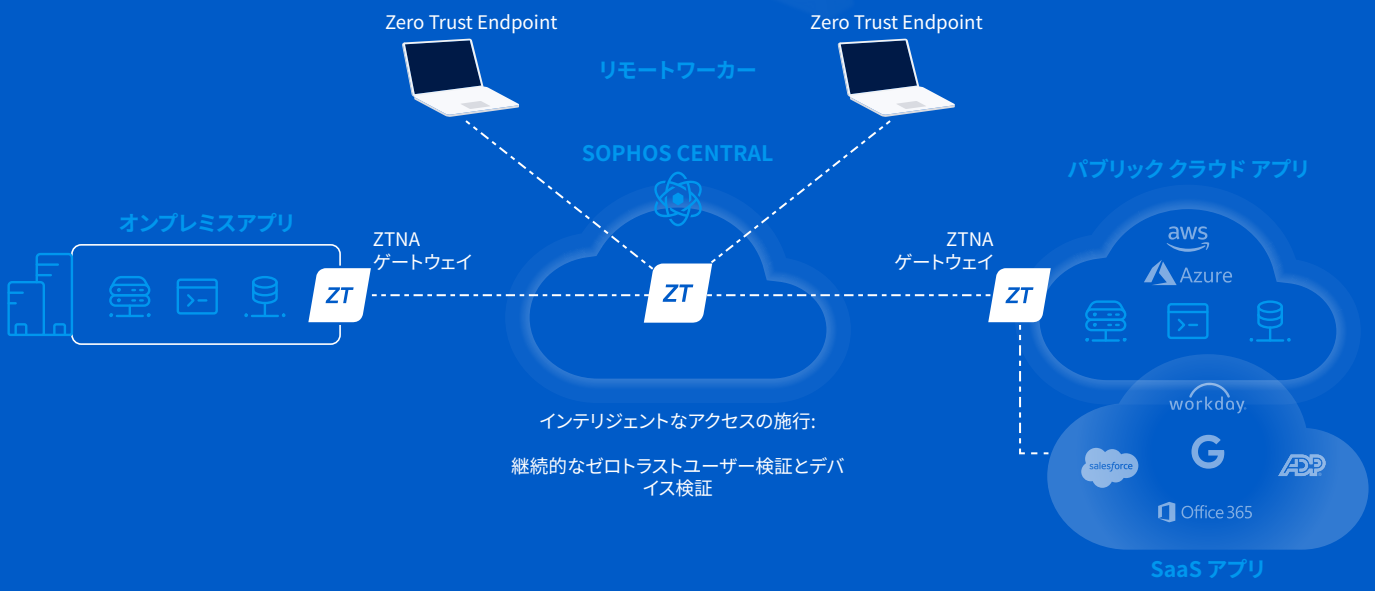
SOPHOS

Sophos ZTNA 導入チェックリスト

Sophos ZTNA の導入は、業界で最も信頼性の高いサイバーセキュリティ管理プラットフォームである Sophos Central を介してクラウドで提供・管理されるので、迅速かつ簡単に実現できます。このチェックリストを使用して、スムーズな導入に必要な対応テクノロジーを利用できることを確認してください。



クイックスタート導入チェックリスト：

- ✔ ネットワーク内、または AWS にホストされている管理対象アプリケーションをマイクロセグメント化し、リモートユーザーに安全なアクセスを提供したいと考えている。
- ✔ ZTNA ゲートウェイが対応しているハイパーバイザー プラットフォームやクラウドプロバイダを利用している。
- ✔ Azure や Okta など、最新の ID プロバイダ(以下 IdP)を利用している。Azure は、基本的な IdP サポートを提供する場合は無償となることが多く、オンプレミスの Active Directory と迅速に統合できます。
- ✔ Windows 10 または macOS 環境でシックアプリケーションへのアクセスが可能である。また、Web アプリケーションへのクライアントレスのブラウザベースのアクセスを、すべてのプラットフォームで提供したいと考えている。
- ✔ Sophos Synchronized Security と Intercept X を使用して、必要に応じて、デバイスのセキュリティ状態をアクセスポリシーに統合したいと考えている。

詳細な考慮事項：

すべての管理対象アプリケーションを特定する：マイクロセグメント化して、安全なリモートアクセスを提供するアプリケーションを特定します。Sophos ZTNA では、これらのアプリケーションをオンプレミス、データセンター、ホスティングプロバイダー、または Amazon Web Services (AWS) パブリッククラウドでホストする必要があります。また、Sophos ZTNA は、IP アドレス制御の制限を提供する SaaS アプリケーションへのアクセスも制御できます。

ゲートウェイ戦略を決定する：Sophos ZTNA ゲートウェイは、アプリケーション側で安全な接続を促進します。ZTNA ゲートウェイは、各アプリケーションのホスティングの場所のネットワークゲートウェイで必要です。たとえば、2つの異なるデータセンターと AWS でアプリケーションをホストしている場合、3つの ZTNA ゲートウェイが必要になります。

次の 2種類のゲートウェイが利用可能で、ハイブリッド方式で混在させることが可能です。

- クラウドゲートウェイ – オンプレミスに導入された軽量のゲートウェイで、各地域の Sophos Cloud の接続点を介して Sophos Cloud に自動的に接続します。このソリューションは、ファイアウォールの構成を必要とせずに、究極に合理化された導入を提供し、結果としてアプリケーションをより不可視にして安全にします。
- オンプレミスゲートウェイは、エンドポイントとアプリケーション間のプライベートデータプレーン接続を直接提供します。 このソリューションは、クラウドの接続点経由のレイテンシーについて懸念があるお客様に最適です。

どのオプションを選択しても、Sophos ZTNA ゲートウェイは必要な台数だけ自由に導入できます。プラットフォームのサポートについては、下の表を参照してください。このようなプラットフォームをゲートウェイの導入で使用できることを確認してください。

使用する IdP を定義する：ユーザーを認証するためには、Sophos ZTNA が対応している IdP が必要です。IdP の一覧は、以下の表を参照してください。Sophos ZTNA は、対応している IdP と統合された、ほとんどの多要素認証 (MFA) ソリューションと連携します。オンプレミスの Active Directory を使用して、ユーザーベースのポリシー作成のために、ディレクトリツリーを Sophos Central にインポートすることができますが、これはリモートアクセス IdP ソリューションとしては十分ではありません。

ユーザー数を決定する：ZTNA ライセンスは、非常にシンプルなユーザーベースのライセンスです。安全なアプリケーションアクセスを必要とするユーザーの数が、ライセンスの数となります。 クライアントへの導入を容易にするために、Sophos Client は、Sophos Central から Intercept X エンドポイントエージェントとともに簡単に導入できますが、他のデスクトップ用マルウェア対策製品と並行して個別に導入することもできます。

デバイスのセキュリティ状態に基づいた戦略を検討する (任意)。これは、デバイスのセキュリティ状態やコンプライアンス状態に基づいて、アプリケーションへのアクセスを制御する、任意の追加セキュリティレイヤーです。現在 Sophos ZTNA は、デバイスのセキュリティ状態とコンプライアンス状態を活用して、Sophos Security Heartbeat に対応しています。これには、Sophos Intercept X が必要で、Sophos Intercept X は、単一の画面でサイバーセキュリティのニーズすべてを管理する Sophos Central によって管理されます。Intercept X は、デバイスのセキュリティ状態を Sophos ZTNA と共有し、これはアプリケーションへのアクセスポリシーで使用することができます。

Sophos ZTNA の対応プラットフォーム

対応プラットフォーム	現在	今後
IdP (Identity Provider)	Microsoft Azure および Okta	オンデマンドでの追加の IdP
ZTNA ゲートウェイのプラットフォーム	VMware ESXi 6.5+、Hyper-V、および AWS	Azure、Nutanix、および GCP
ZTNA クライアントのプラットフォーム	Windows 10 1803 以降、macOS 11 (Big Sur)以降	iOS および Android
ZTNA デバイスのセキュリティ状態	Sophos Security Heartbeat (Intercept X)	Windows セキュリティセンターでの セキュリティ状態の追加評価を計画中

Sophos ZTNA Cloud Gateway の接続点 (PoP)

Sophos Cloud Gateway を展開する場合、接続点は次の地域で使用できます。

- ヨーロッパ (アイルランドおよびフランクフルト)
- 北米 (オハイオ州およびオレゴン州)
- アジア太平洋地域 (ムンバイおよびシドニー)

Sophos ZTNA ライセンス

- Sophos ZTNA は、ユーザー数によってライセンス数が決定します。
- Sophos ZTNA ゲートウェイは、必要な数だけ無償で導入できます。
- Sophos Central での管理は追加料金なしで利用できます。
- Sophos ZTNA は、Sophos Intercept X および Sophos Firewall と連携することでより効率的に動作します。(もちろん、他のエンドポイント製品やファイアウォール製品とも完全に連携します。)

参考資料

Sophos ZTNA の導入をさらに詳細に計画するには、次の資料を参照してください。

- Sophos ZTNA ドキュメント
- Sophos Community にある ZTNA 資料

Sophos ZTNA の
30日間無償評価版
sophos.com/ztna

ソフォス株式会社営業部
Email: sales@sophos.co.jp

23-01-10 JA (DD)