Cisco Identity Services Engine

目次

Cisco® Identity Services Engine（ISE）は、セキュリティポリシー管理を合理化し、運用コストを削減するためのワンストップソリューションです。ISE を使用すると、企業ネットワークへの有線、ワイヤレス、および VPN 接続を介したアクセスを制御するユーザとデバイスを確認できます。

製品の概要

Cisco ISE では、ユーザとデバイスに非常にセキュアなネットワークアクセスを提供します。これにより、誰が接続しているか、どのようなアプリケーションがインストールされ、実行されているかなど、ネットワーク内で起こっていることを把握するのに役立ちます。また、ユーザやデバイスのアイデンティティ、脅威、脆弱性などの重要なコンテキストデータを、シスコのテクノロジーパートナーから統合したソリューションと共有し、脅威をより迅速に特定し、封じ込めて、修復することができます。

お客様の利点

Cisco ISE は、ネットワーク アクセス セキュリティに対して包括的に取り組みます。ISE を展開すると、次のような多くの利点が得られます。

高度なセキュリティを備えたビジネスおよびコンテキストベースのアクセスは企業のポリシーに基づいています。ISE は、ネットワークデバイスと連携して、ユーザ、時間、場所、脅威、脆弱性、アクセスタイプなどの属性ですべてを包括するコンテキスト アイデンティティを作成します。このアイデンティティを使用すると、そのアイデンティティのビジネスロールに一致する安全性の高いアクセスポリシーを適用できます。IT 管理者は、ネットワーク上のエンドポイントについて、誰が、何を、いつ、どこで、どのように許可するかを正確に制御できます。ISEは、Cisco TrustSec® ソフトウェア定義のセグメンテーションなど、複数のメカニズムを使用してポリシーを適用します。

合理化されたネットワークの可視性を、シンプルで柔軟性が高く、使いやすいインターフェイスにより実現します。ISE は、ネットワークに接続しているすべてのエンドポイントと、ネットワーク上のユーザ（ゲスト、従業員、請負業者などのタイプを含む）の詳細な属性履歴を、エンドポイント アプリケーションの詳細やファイアウォールのステータスまでのすべてを保存します。

広範にポリシーを適用することで簡単で柔軟性の高いアクセスルールを定義し、変化し続けるビジネス要件を満たします。ネットワークやセキュリティ インフラストラクチャ全体にわたって適用することで、中央のロケーションからすべてを制御します。IT 管理者は、登録されているユーザやデバイスをゲストと差別化するポリシーを一元的に定義できます。ユーザとエンドポイントは、場所に関係なく、ロールとポリシーに基づいてアクセスが許可されます。Cisco TrustSec セキュリティグループタグ（SGT）を使用すると、組織は IP アドレスやネットワーク階層ではなく、ビジネスルールに基づいてアクセス制御を行うことができます。これらの SGT により、ユーザとエンドポイントは、リソースがドメイン間を移動するときに常に維持される最小特権ポリシーでアクセスできます。スイッチ、ルータ、およびファイアウォールルールの管理が容易になり、IT 運用が 80 % 削減され、変更の実装時間が 98 % 短縮されることが示されています。

堅牢なゲストエクスペリエンスがネットワークへの複数レベルのアクセスで実現されます。コーヒーショップタイプのホットスポットアクセス、セルフサービス登録アクセス、またはスポンサーアクセスを介したゲストアクセスを提供できます。ISE では、動的なビジュアルツールを提供するオンボックスまたはクラウドで提供されるポータルエディタを使用して、さまざまなゲストポータルを高度にカスタマイズできます。ポータル画面のリアルタイムプレビューと、ゲストがネットワークに接続したときのエクスペリエンスを確認できます。

セルフサービス デバイス オンボーディングで企業の BYOD（Bring Your Own Device）ポリシーまたはゲストポリシーを実現する。ユーザは、IT 管理者が定義したビジネスポリシーに従ってデバイスを管理できます。IT スタッフは、セキュリティポリシーに準拠するために必要な自動デバイスプロビジョニング、プロファイリング、およびポスチャリングを行います。同時に、従業員は IT の支援を必要とせずにデバイスをネットワークに導入できます。

Cisco DNA Center の統合

Cisco DNA Center は、シスコのインターネットベース ネットワークの中心にある基盤コントローラであり、分析プラットフォームでもあります。Cisco DNA Center によって、ネットワーク管理が簡素化され、ゲストや BYOD などのさまざまな ISE サービスをネットワーク全体で迅速かつ簡単に設定できます。また、Cisco DNA Center では、ポリシーの設計、プロビジョニング、適用を日単位ではなく分単位でネットワーク全体にわたって簡単に行えるようにします。分析とアシュアランスでは、ネットワークインサイトを使用してネットワークのパフォーマンスを最適化します。Cisco DNA Center は pxGrid を使用して ISE 2.3 以降と統合し、ビジネスニーズに基づいてグループベースのセキュアアクセスとネットワークセグメンテーションを展開します。Cisco Cisco DNA Center と ISE を使用すると、ポリシーをネットワークデバイスではなくユーザとアプリケーションに適用できます。グループベースのポリシーは、ネットワークアクセスを制御し、セキュリティポリシーを適用し、コンプライアンス要件を満たすためのソフトウェア定義のセグメンテーションを提供します。

自動デバイスコンプライアンスチェックは、Cisco AnyConnect® Unified Agent を使用したデバイスポスチャおよび修復オプションが対象。AnyConnect® エージェントは、デスクトップやラップトップのチェック用の高度な VPN サービスも提供します。ISE は、市場をリードするモバイルデバイス管理/エンタープライズモビリティ管理（MDM/EMM）ベンダーとも統合されます。MDM の統合により、ネットワークへのアクセスが許可される前に、モバイルデバイスがセキュアでポリシーに準拠していることを確認できます。

ユーザとデバイスの詳細を共有する機能はネットワーク全体を網羅。Cisco pxGrid（Platform Exchange Grid）テクノロジーは、接続されたユーザとデバイスに関する詳細なコンテキストデータをシスコやシスコのセキュリティ テクニカル アライアンス ソリューションと共有するために使用できる堅牢なプラットフォームです。ISE のネットワークやセキュリティパートナーは、このデータを使用して独自のネットワークアクセス機能を向上させ、脅威を特定し、軽減し、迅速に封じ込める能力を高めます。

中央ネットワークデバイス管理では TACACS+ を使用。Cisco ISE では TACACS+ セキュリティプロトコルを使用してネットワークデバイスを管理し、ネットワークデバイスの設定を制御および監査できます。ISE は、誰がどのネットワークデバイスにアクセスでき、関連付けられたネットワーク設定を変更できるかについて簡単に詳細に制御できるようにします。

機能とメリット

Cisco ISE は、表 1 に示すように、さまざまな方法で組織を強化します。

表 1. 機能とメリット

機能	利点
集中管理	• 管理者が 1 つの Web ベースの GUI コンソールから、プロファイラ、ポスチャ、ゲスト認証、および許可サービスを一元的に設定し、管理できるようにします。 • 1 つのペインから統合管理サービスを提供することで、管理を簡素化します。
コンテキストが豊富なアイデンティティとビジネスポリシー	• ルールベースで属性主体のポリシーモデルにより、柔軟性の高いビジネス関連アクセスの制御ポリシーを実装します。 • ユーザおよびエンドポイントのアイデンティティ、ポスチャ検証、認証プロトコル、デバイスアイデンティティ、およびその他の外部属性などの属性が含まれます。これらの属性は、動的に作成して後で使用するために保存しておくことができます。 • Microsoft Active Directory、Lightweight Directory Access Protocol（LDAP）、RADIUS、RSA ワンタイムパスワード（OTP）、認証と許可の両方のための認証局、Open Database Connectivity（ODBC）、SAML プロバイダーなどの複数の外部アイデンティティリポジトリと統合します。
アクセス コントロール	• ダウンロード可能なアクセスコントロールリスト（dACL）、仮想LAN（VLAN）の割り当て、URL リダイレクション、名前付き ACL、Cisco TrustSec テクノロジーを使用したセキュリティグループ ACL（SGACL）など、さまざまなアクセス制御オプションを提供します。

機能	利点
Easy Connect による サプリカントレス ネットワーク アクセスの保護	• アプリケーション層全体にわたってログイン情報から認証と許可を取得することで、エンドポイントに 802.1X サプリカントが存在しなくても、ユーザアクセスを許可し、安全性の高いネットワークアクセスを迅速に展開できるようにします。
Cisco TrustSec/ グループベースのポリシー	• シスコのグループベースのポリシー/TrustSec ソフトウェア定義のセグメンテーションにより、セキュリティグループタグ（SGT）を使用したセグメンテーションがシンプルになります。IETF のオープンテクノロジーであり、OpenDaylight 内で使用でき、サードパーティ製プラットフォームやシスコのプラットフォームでサポートされています。 • ISE は、スイッチ、ルータ、ワイヤレス、およびファイアウォールのルールの管理を簡素化するセグメンテーション コントローラです。 • グループ情報は、データパス内のネットワークデバイス間（インラインタギング）、またはデバイスが SGT を使用してパケットにタグ付けする機能を持たない場合はセキュリティグループタグ交換プロトコル（SXP）IP-to-SGT バインディング情報を介して SGT を伝達します。
ゲストのライフサイクル管理	• ゲストのネットワークアクセスを実装してカスタマイズするための合理化されたエクスペリエンスを提供します。 • 数分で企業ブランドのゲストエクスペリエンスを広告とプロモーションで作成します。ホットスポット、スポンサー、セルフサービス、およびその他の多くのアクセスワークフローに対するサポートが組み込まれています。 • ゲストフロー設計の効果を実現するリアルタイムのビジュアルフローによる管理を提供します。 • ネットワーク全体のアクセスを追跡し、セキュリティ、コンプライアンス、および完全なゲスト監査を実現します。時間制限、アカウントの有効期限、および SMS の検証によりセキュリティ管理を強化します。 • ゲストがソーシャルメディアのクレデンシャルを使用して接続できるように、アクセスを合理化します。
デバイスのオンボーディングの合理化	• 標準の PC やモバイルコンピューティングのプラットフォームのサプリカント プロビジョニングと証明書登録を自動化します。よりセキュアなアクセスを提供し、IT ヘルプデスクのチケット数を削減し、より優れたエクスペリエンスをユーザに提供します。 • エンドユーザがセルフサービスポータルでデバイスを追加および管理できるようにし、Web ポータル用の SAML 2.0 をサポートします。 • モバイルデバイスのコンプライアンスと登録のために MDM/EMM ベンダーと統合します。
組み込み **AAA** サービス	• 標準 RADIUS プロトコルを使用して、認証、許可、およびアカウンティング（AAA）を行います。 • さまざまな認証プロトコルをサポートします（PAP、MS-CHAP、Extensible Authentication Protocol（EAP）-MD5、Protected EAP（PEAP）、EAP-Flexible Authentication via Secure Tunneling（FAST）、EAP-Transport Layer Security（TLS）、EAP-Tunneled Transport Layer Security（TTLS）など）。 注：Cisco ISE は、マシンとユーザのクレデンシャルの EAP チェーンをサポートする唯一の RADIUS サーバです。
デバイス管理アクセスの制御と監査	• TACACS+ プロトコルをサポート • クレデンシャル、グループ、ロケーション、およびコマンドに基づいてユーザにアクセスを許可します。 • ネットワーク内のすべての変更の監査証跡を保持しながら、知っておく必要がある事柄と対処する必要がある事柄に基づいてデバイス設定にアクセスできます。
内部認証局	• 展開しやすい内部認証局が備わっています。 • エンドポイントと証明書を管理する単一のコンソールが備わっています。証明書のステータスは、標準ベースの Online Certificate Status Protocol（OCSP）によって確認されます。証明書は自動的に失効します。 • スタンドアロン展開、pxGrid で統合された製品、および下位の製品（つまり、認証局が既存のエンタープライズ公開キーインフラストラクチャ（PKI）と統合された製品）をサポートします。 • 高度なセキュリティでデバイスをネットワークに接続するための、一括または単一の証明書とキーのペアの手動作成を容易にします。
デバイスのプロファイリング	• IP フォン、プリンタ、IP カメラ、スマートフォン、タブレットなど、さまざまなタイプのエンドポイント用に事前に定義されたデバイステンプレートが入力されています。医療、製造、ビルディングのオートメーションなどの特殊なデバイス用に追加のデバイステンプレートを使用できます。 • カスタム デバイス テンプレートを作成して、エンドポイントをネットワークに接続した際に、管理者が定義したアイデンティティを自動的に検出、分類、関連付けします。 • デバイスタイプに基づいてエンドポイント固有のポリシーを関連付けます。 • パッシブ ネットワーク モニタリングとテレメトリを使用してエンドポイント属性データを収集します。

機能	利点
デバイスプロファイル フィード サービス	• 複数のベンダーのさまざまな IP 対応デバイスに対してシスコの検証済みデバイスプロファイルの更新を自動的に配信します。最新の IP 対応デバイスのライブラリを最新に維持するタスクを簡素化します。 • パートナーとお客様は、シスコが検査し、再配布するようにカスタマイズされたプロファイル情報を共有できます。
エンドポイント ポスチャサービス	• ネットワークに接続されたエンドポイントに対してポスチャアセスメントを実行します。 • 永続的なクライアントベースのエージェント、一時的なエージェント、または外部 MDM/EMM へのクエリによって、エンドポイントに適切なコンプライアンスポリシーを適用します。 • 最新の OS パッチのチェック、最新の定義ファイル変数（バージョン、日付など）、マルチウェア対策パッケージ、レジストリ設定（キー、値など）、パッチ管理、ディスクの暗号化、モバイルの PIN ロック、ルート化ステータスまたはジェイルブレイクステータス、アプリケーションプレゼンス、および USB 接続メディアを確認するなど強力なポリシーを作成する機能を提供します。 • PC クライアントの自動修復の他、優れたエンタープライズパッチ管理システムとともに定期的な再アセスメントをサポートし、エンドポイントが企業のポリシーに違反していないことを確認します。 • 完全なネットワーク可視性を実現するためにハードウェアインベントリを提供します。 • 次の OS プラットフォームでポスチャアセスメントを行うには、AnyConnect 4.x エージェントが必要です。 ◦ Windows 10、8.1、8、7 ◦ Mac OS X 10.8 以降
広範なマルチフォレスト Active Directory のサポート	• マルチフォレスト Microsoft Active Directory ドメインに対する包括的な認証と認可を提供します。 • 複数の結合されていないドメインを論理グループにグループ化します。 • ソリューションの移行と統合を円滑にするための柔軟なアイデンティティ書き換えルールが含まれています。 • Microsoft Active Directory 2003、2008、2008R2、2012、2012R2、および 2016 をサポートします。
モニタリングと トラブルシューティング	• モニタリング、レポート、およびトラブルシューティング用の組み込みヘルプ Web コンソールが備わっています。 • すべてのサービスに対して堅牢な履歴およびリアルタイムのレポートを提供します。すべてのアクティビティをログに記録し、ネットワークに接続しているすべてのユーザとエンドポイントのリアルタイムのダッシュボードメトリックを提供します。
認定	• 連邦情報処理標準（FIPS）140-2、コモンクライテリアおよび統合機能承認済み製品リストの要件に準拠しています。 • IPv6 対応。 **注：**すべてのリリースで認定を利用できない場合や、承認の状態が異なる場合があります。現在の認定およびリリースは、Global Government Certifications で確認できます。
アップグレード準備ツール（URT）	• アップグレード前チェックを実行します。 • 実際のアップグレードをシミュレートします。 • アップグレードの成功/失敗に関するガイダンスを提供します。 • ノードごとのアップグレード時間に関するガイダンスを提供します。 • 更新と学習を常に提供します。
IPv6 のサポート	• RADIUS および TACACS+ ベースのネットワークデバイス用の IPv6。 • ISE は、IPv6 管理ネットワークを介して管理できます。これには、ISE 管理インターフェイスへの接続（Web または CLI）、Active Directory への接続、syslog メッセージの送信、SNMP トラップの送信、REST API over IPv6、DNS の解決、および NTP 時刻の同期が含まれます。

統合型ソリューション

Cisco pxGrid は、複数のセキュリティツールが相互にリアルタイムで自動的に通信するための拡張性に優れた IT クリアリングハウスです。Cisco ISE 2.4 では、新しい WebSocket クライアントを提供し、基盤となるオペレーティングシステムと言語への依存を排除する pxGrid 2.0 を導入しています。シスコおよびサードパーティベンダー（特に pxGrid を使用して OT エンドポイント情報を ISE に提供する Cisco Industrial Network Director（IND））からは 50 を超え

る統合を利用できます。さらに、pxGridを使用して、エンドポイントに関する IP-to-SGT 情報を共有し、セキュリティ製品がSGTを使用してセキュリティグループアクセスコントロールを適用できるようにします。

Cisco Rapid Threat Containment は、セキュリティイベントに応じてネットワークの軽減アクションと調査のアクションを簡素化および自動化します。Cisco ISE とシスコのセキュリティ テクノロジー パートナーのソリューションをさまざまなテクノロジー領域に統合します。Threat-Centric Network Access Control（TC-NAC）を使用すると、CVSS 脆弱性と STIX 脅威スコアに基づいてユーザアクセスを変更できます。Cisco pxGrid Adaptive Network Control（ANC）を使用すると、エンドポイントのネットワーク アクセス ステータスをリセットし、ポートの隔離、隔離解除、バウンス、またはシャットダウンを実行することができます。

プラットフォームサポートと互換性

ISE は、物理アプライアンスまたは仮想アプライアンスとして使用できます。物理展開と仮想展開の両方を使用して、重要な企業ネットワークの規模、冗長性、およびフェールオーバーの要件を提供できる ISE クラスタを作成できます。

ISE 仮想アプライアンスは、VMware ESXi 5.x および6.x、Red Hat 7.x のKVM、および Microsoft Windows Server 2012R2 以降の Microsoft Hyper-V でサポートされています。

ISE 物理アプライアンスの詳細については、『Cisco Secure Network Server Data Sheet』を参照してください。

ライセンスの概要

図 1 に示すように、4 つのプライマリ ISE ライセンスを使用できます。この柔軟性の高いモデルでは、ライセンスの数と組み合わせを選択して、必要な機能のセットを取得できます。

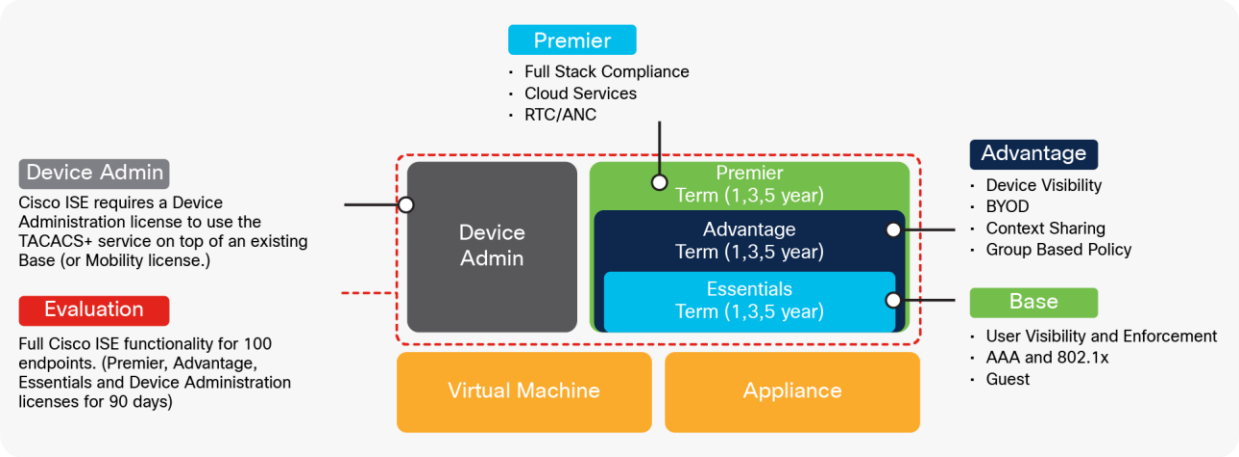

図 1.
Cisco ISE ライセンスパッケージ

注文情報

Cisco ISE 注文ガイドは、ISE の展開を最大限に活用するためのさまざまなモデルとライセンスタイプを理解するのに役立ちます。購入方法については、「購入案内」を参照してください。ISE ソフトウェアをダウンロードするには、Cisco Software Center にアクセスしてください。

サービスおよびサポート

シスコでは、多様なサービスプログラムをご用意しています。これらの画期的なプログラムは、さまざまな人材、プロセス、ツール、パートナーを組み合わせて提供されるものであり、お客様からも高い評価を受けています。シスコ

のサービスは、お客様のネットワーク投資を保護してネットワーク運用を最適化するだけでなく、ネットワーク インテリジェンスの強化や事業拡張に向けた新しいアプリケーションの導入準備という面でもサポートします。シスコのサービスの詳細については、シスコ テクニカル サポート サービスまたはシスコセキュリティサービスを参照してください。

保証の関する情報はこちらで確認できます。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

購入方法

購入オプションを確認し、シスコの営業担当者に問い合わせるには、https://www.cisco.com/c/ja_jp/buy.html にアクセスしてください。

詳細情報

Cisco ISE ソリューションの詳細については、
https://www.cisco.com/c/ja_jp/products/security/identity-services-engine/index.html を参照するか、お最寄りのシスコ代理店までお問い合わせください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-656174-20JA 20.11