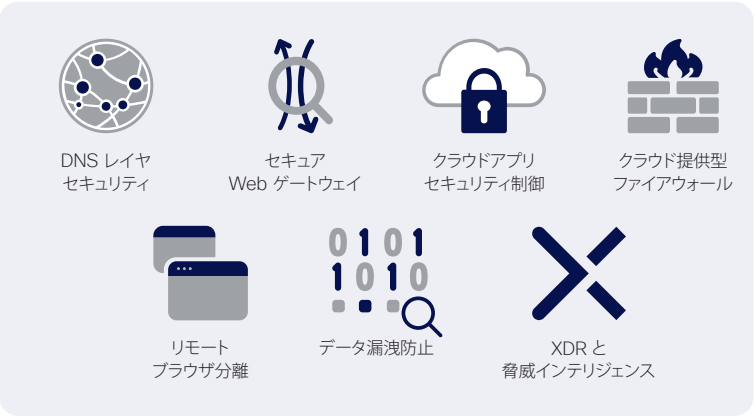
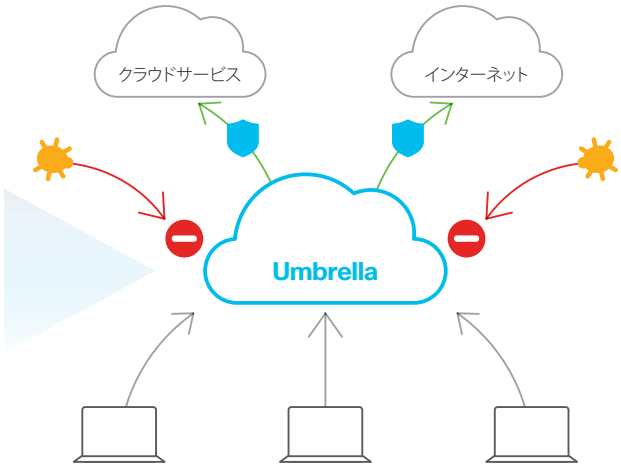
シスコ セキュリティ

Cisco Umbrella

簡単かつ迅速に導入できる、シンプルなクラウド提供型セキュリティ

Cisco Umbrella は、インターネット上の脅威を防御するための最前線として機能するセキュア インターネットゲートウェイ［Secure Internet Gateway（SIG）］です。DNS レイヤのセキュリティをベースに次のような幅広いセキュリティサービスをクラウドで提供、一元管理できます。小規模企業が簡単かつ迅速に導入できるシンプルなセキュリティであると同時に、SD-WAN や SASE など最先端のテクノロジーやフレームワークにも最適なソリューションです。





パッケージ別機能比較

セキュリティサービス			DNS セキュリティ		SIG	
			Essentials	Advantage	Essentials	Advantage
DNS レイヤセキュリティ	マルウェアやフィッシング、ボットネットなど、危険性が高いドメインをブロック		✓	✓	✓	✓
	SecureX、Splunk や Anomali などとの統合、エンフォースメント API によるカスタムリストに基づいてドメインをブロック		✓	✓	✓	✓
	DNS をバイパスする C2 コールバック対策として、直接 IP トラフィックをブロック			✓	✓	✓
セキュア Web ゲートウェイ（SWG）	Web トラフィックのプロキシと検査［SSL（HTTPS）トラフィック対応］			危険なドメインのみ	✓	✓
	Web フィルタリング（カテゴリベース）	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	カスタマイズ可能なブロック / 許可リスト	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	アンチウイルスおよびレピュテーション（AMP）によって危険なファイルをブロック			危険なドメインのみ	✓	✓
	Secure Malware Analytics（旧 Threat Grid）で疑わしいファイルを分析（サンドボックス）				1 日あたり 500 サンプル	無制限
	無害なファイルが危険なファイルに変化しても特定できる、遡及可能なセキュリティ				✓	✓
クラウドアプリセキュリティ制御（CASB）	クラウドアプリの検出とブロック	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	クラウドアプリ別にきめ細やかに制御（アップロードやファイル添付、投稿の禁止など）				✓	✓
	契約クラウドのファイルストレージをスキャン、マルウェアを除去 NEW				2 アプリ	4 アプリ *1
クラウド提供型ファイアウォール（CDFW）	IP/ ポート / プロトコルを可視化および制御				✓	✓
	アプリケーションの可視化と制御、および侵入防御システム NEW				オプション	✓
	IPsec トンネル終端対応				✓	✓
データ漏洩防止（DLP）	Web およびクラウドアプリのトラフィックをインラインで検査、機密データを保護 NEW				オプション	✓
リモートブラウザ分離（RBI）	危険な Web サイト、Web アプリ、または任意の宛先へ安全にアクセス NEW				オプション	オプション
XDR（拡張型検知 / 対応）と脅威インテリジェンス	SecureX との統合（API）によって、シスコのセキュリティ製品全体で脅威の調査と修復を高速化および効率化	レポーティング API およびエンフォースメント API	✓	✓	✓	✓
		すべての API		✓	✓	✓
	ドメイン、IP、ASN ベースで、シスコによる詳細な分析データにアクセスして迅速に調査			✓	✓	✓

*1　継続的に追加。

サブスクリプション ライセンス *1

Cisco Umbrella ライセンス

製品型番	製品説明
UMB-DNS-ESS-K9	Umbrella DNS セキュリティ Essentials ユーザ別ライセンス
UMB-DNS-ADV-K9	Umbrella DNS セキュリティ Advantage ユーザ別ライセンス
UMB-SIG-ESS-K9	Umbrella SIG Essentials ユーザ別ライセンス
UMB-SIG-ADV-K9 NEW	Umbrella SIG Advantage ユーザ別ライセンス
UMB-WLAN	Umbrella WLAN アクセスポイント別ライセンス（5 AP ～）

Cisco Umbrella SIG アドオンライセンス NEW

製品型番	製品説明
UMB-L7-CDFW	レイヤ 7 アプリ対応 CDFW ライセンス *2
UMB-DLP	インライン DLP ライセンス *2
UMB-RBI-RISKY	RBI（Isolate Risky）ライセンス
UMB-RBI-WEBAPP	RBI（Isolate Web Apps）ライセンス
UMB-RBI-ALL	RBI（Isolate Any）ライセンス

*1　1、3、または 5 年間のサブスクリプション。CCW では UMB-SEC-SUB が必要。詳細は発注ガイドを参照。　*2　Umbrella SIG Essentials 用アドオン（Umbrella SIG Advantage ではデフォルトでサポート）。

Cisco Umbrella SIG Advantage パッケージ NEW

Cisco Umbrella の製品パッケージに、新しく **Cisco Umbrella SIG Advantage** がラインアップ。従来の Cisco Umbrella SIG Essentials で提供する機能に加えて、次の新機能を提供します。

- デフォルトで提供：レイヤ 7 アプリケーションおよび侵入防御システム対応クラウド提供型ファイアウォール（Cloud Delivered FireWall；CDFW）
- デフォルトで提供：データ漏洩防止（Data Loss Prevention；DLP）
- オプションで提供：リモートブラウザ分離（Remote Browser Isolation；RBI）

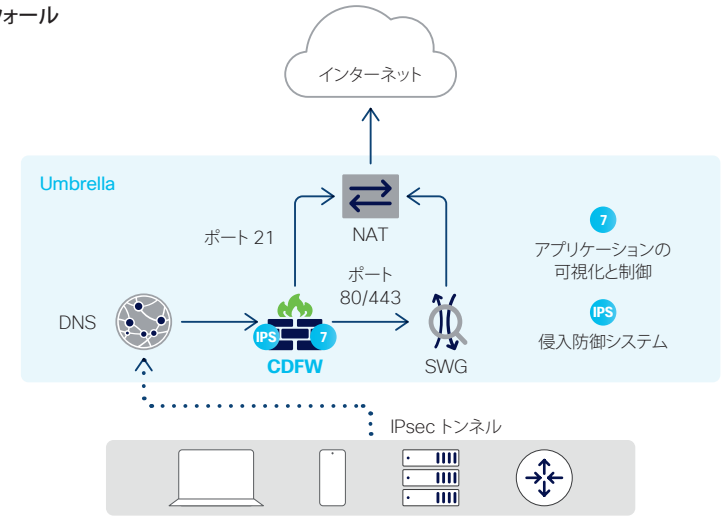
Umbrella SIG Essentials を導入済みのお客様は、Cisco Umbrella SIG アドオンライセンスによって、これらの機能を個別に追加することができます。

レイヤ 7 アプリケーションおよび侵入防御システム対応クラウド提供型ファイアウォール

インターネット送信に使用するポートとプロトコルを可視化および制御するレイヤ 3 およびレイヤ 4 ファイアウォールに加えて、Umbrella SIG Advantage ではアプリケーションを可視化および制御するレイヤ 7 ファイアウォール、さらに侵入防御システムもサポートします。

- クラウドベースではない約 2,800 のアプリケーションを可視化（継続的に追加）
- Snort 3 対応侵入防御システム、40,000 以上の膨大なシグネチャを使用（Talos から継続的に追加）
- 不必要なトラフィックや望ましくないトラフィックを、ポート、プロトコル、さらにアプリケーションおよび侵入防御システムベースのポリシーで制御（許可 / ブロック）

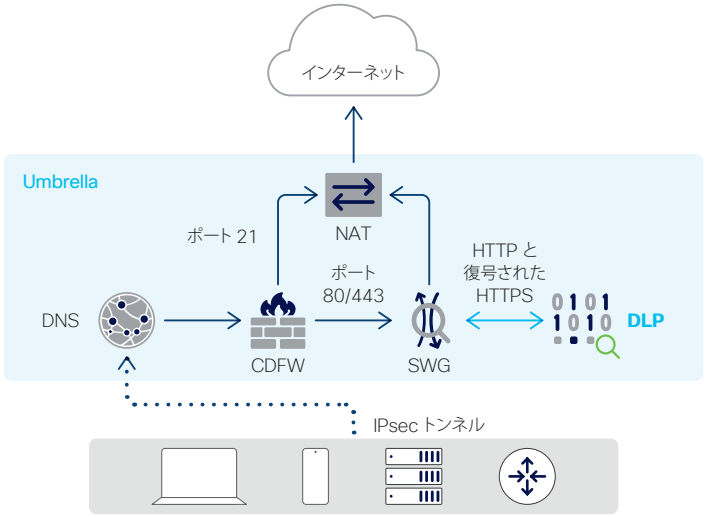
クラウド提供型ファイアウォールを使用するためには、Cisco Secure Firewall や Cisco Meraki MX、Cisco ISR など IPsec 対応デバイスとのトンネル設定が必要になります。



データ漏洩防止

インターネットに向かうトラフィックを監視、事前に定義した機密データの有無をリアルタイムで分析し、機密データが流出する前にブロックします。セキュア Web ゲートウェイと連携するため、暗号化されたトラフィックにも対応します。

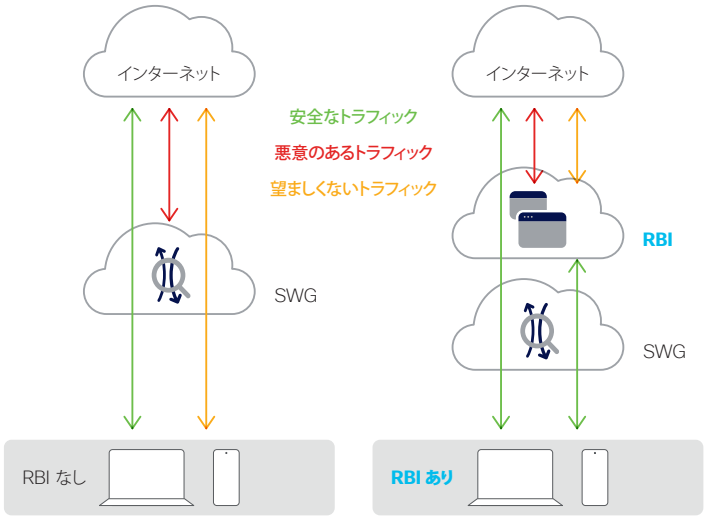
- PII、PCI、PHI を含む 80 以上の機密データ辞書を内蔵
- 任意のフレーズ（プロジェクトコードなど）を含むユーザ定義の辞書を作成可能
- 特定のアイデンティティや宛先に適用するなど、カスタマイズ可能なポリシー
- しきい値や近接度の設定によって、誤認識を軽減
- 機密データの使用に関する詳細なレポートで、不正使用を特定



リモートブラウザ分離

ブラウジング中のプログラムの実行など、ブラウザ機能をデバイスから切り離されたクラウドの仮想環境で提供することで、リスキーなユーザを保護、あるいはリスキーな Web サイト閲覧を無害化します。次の 3 つのパッケージから選択可能、既存のブラウザ設定を変更せずに迅速に導入できます。

- Isolate Risky
  未分類、または潜在的に危険なセキュリティカテゴリの Web サイト閲覧を分離
- Isolate Web Apps
  Box や Slack、Gmail など特定のアプリ、または SNS やファイルストレージなど特定のカテゴリでアプリを分離
- Isolate Any
  任意の宛先（ドメイン、URL、IP アドレス）、任意のコンテンツカテゴリ、任意のアプリを制限なく分離



Cisco Secure Access by Duo

ユーザとアプリケーションを保護する、シンプルかつパワフルなアクセスセキュリティ

Cisco Secure Access by Duo は、SASE やゼロトラストなど、モダンなセキュリティフレームワークを実現するための主要製品の 1 つです。アプリケーションにアクセスしようとするユーザおよびデバイスに対して、ユーザの多要素認証（Multi-Factor Authentication；MFA）やデバイスのセキュリティ健全性、さらに適応型のアクセスポリシーに基づいてアクセスを許可することで、あらゆるアプリケーションアクセスを保護します。また、多要素認証によって低下しがちなユーザエクスペリエンスを逆に向上させるシングルサインオン（Single Sign-On；SSO）や、VPN なしで社内のアプリケーションやサーバを安全に利用できるリモートアクセスも提供します。

ユーザトラスト（多要素認証；MFA）
多要素認証でユーザの信頼性を確立

デバイストラスト（デバイスの可視化）
デバイスの健全性を可視化して信頼性を確立

トラストモニタ
アクセス時のふるまい分析で脅威を検知

適応型認証 / ポリシー
さまざまな条件に基づく柔軟なアクセスポリシー

シングルサインオン（SSO）
セキュリティを損なわないユーザフレンドリな SSO

リモートアクセス
VPN なしで実現する安全なリモートアクセス

エディション別機能比較

セキュリティサービス		DuoFree	Duo MFA	Duo Access	Duo Beyond
ユーザトラスト（多要素認証；MFA）	iOS および Android 向けモバイルアプリ Duo Mobile のプッシュ通知による認証	✓	✓	✓	✓
	アプリや SMS、電話着信、ハードウェアトークンによるパスコード認証、U2F と WebAuthN による生体認証など	✓	✓	✓	✓
	1 ユーザあたり年間 100 クレジット分の電話着信認証および SMS 認証		✓	✓	✓
	ユーザによる自己登録と自己管理		✓	✓	✓
デバイストラスト（デバイスの可視化）	アプリケーションにアクセスする、すべてのデバイスを把握できるダッシュボード		✓	✓	✓
	危険なデバイスを監視および識別			✓	✓
	ノート PC およびデスクトップ PC のセキュリティ健全性を可視化（Duo デバイスヘルス アプリケーション）			✓	✓
	モバイルデバイスのセキュリティ健全性を可視化			✓	✓
	ノート PC およびデスクトップ PC が企業所有か個人所有か識別				✓
	モバイルデバイスが企業所有か個人所有か識別				✓
	アンチウイルスやアンチマルウェアなどサードパーティ製エージェントが有効かどうか識別				✓
トラストモニタ NEW	アクセス時のふるまい（どのユーザが / どのアプリケーションで / どのデバイスから / いつ / どこで / どんな認証方法で）を分析、脅威を検知			✓	✓
適応型認証 / ポリシー	セキュリティポリシーをアプリケーション全体またはアプリケーション別に割り当て		✓	✓	✓
	ネットワークが承認済みかどうかに基づいてポリシーを適用		✓	✓	✓
	ユーザの場所に基づいてポリシーを適用			✓	✓
	ユーザグループ別にセキュリティポリシーを割り当ておよび適用		✓	✓	✓
	匿名ネットワークをブロック			✓	✓
	異常なアクセスや危険なアクセスを検知			✓	✓
	ソフトウェアのサポート期限、暗号化やファイアウォールの有無など、セキュリティ健全性に基づいてノート PC およびデスクトップ PC にデバイストラストポリシーを適用			✓	✓
	暗号化や改ざん、画面ロック、生体認証の有無など、セキュリティ健全性に基づいて、モバイルデバイスにデバイストラストポリシーを適用			✓	✓
	セキュリティ健全性が低い場合はデバイスを修正するようにユーザに通知			✓	✓
	Landesk や JAMF、Microsoft Intune など、エンドポイント管理システムでの登録状況に基づいて、デバイスのアプリケーションアクセスを制限				✓
	AirWatch や MobileIron、Microsoft Intune など、モバイルデバイス管理（MDM）での登録状況に基づいて、モバイルデバイスのアプリケーションアクセスを制限				✓
シングルサインオン（SSO）とリモートアクセス	無制限でアプリケーション統合	✓	✓	✓	✓
	SAML 2.0 対応アプリケーションにクラウドベースの SSO を提供 *1 NEW		✓	✓	✓
	Duo Central からアプリケーションに簡単アクセス		✓	✓	✓
	社内 Web アプリケーションに安全アクセス（Duo Network Gateway）				✓
	SSH 経由で特定の社内サーバに安全アクセス（Duo Network Gateway）				✓
	AWS、Azure、GCP でホストされているアプリケーションに安全アクセス（Duo Network Gateway）				✓

*1 オンプレミスベースの SSO は Duo Access Gateway で提供。

サブスクリプション ライセンス & アクセサリ

Cisco Duo ライセンス *1

製品型番	製品説明
DUO-MFA	Duo MFA ユーザ別ライセンス
DUO-ACCESS	Duo Access ユーザ別ライセンス
DUO-BEYOND	Duo Beyond ユーザ別ライセンス

*1 1 ～ 5 年間のサブスクリプション。CCW では DUO-SUB が必要。詳細は発注ガイドを参照。

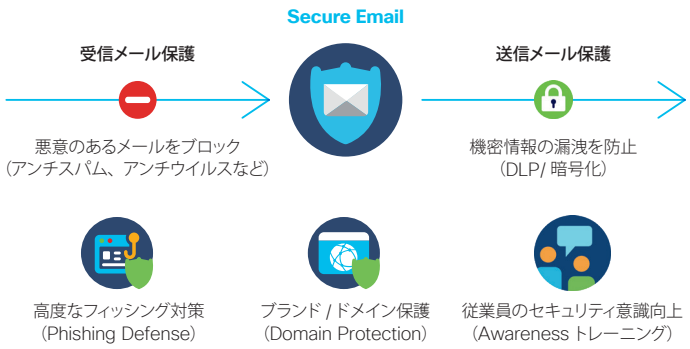
Cisco Duo ハードウェアトークン

製品型番	製品説明
DUO-TOKEN-10PACK	ハードウェアトークン（10 パック）

Cisco Secure Email（E メールセキュリティ）

あらゆる規模や業種の組織で柔軟に導入できる、マルチレイヤの電子メールセキュリティ

電子メールは最も重要なビジネスコミュニケーション ツールであると同時に、脅威の侵入および情報の流出の主要な経路でもあります。Cisco Secure Email はマルチレイヤのメールセキュリティによって、スパムやフィッシング、メール詐欺、マルウェア、情報漏洩、さらに企業ブランド（ドメイン）の悪用など、さまざまな攻撃から電子メールを保護します。Microsoft 365 のセキュリティを補完する Cisco Secure Email Cloud Mailbox[*1] や、クラウド、オンプレミス、さらにハイブリッド構成や段階的な移行もサポートする柔軟な導入オプションによって、あらゆる規模や業種の組織に最適なソリューションを提供します。



*1　旧称は Cisco Cloud Mailbox Defense。

サブスクリプション ライセンス

本カタログでは、Secure Email Cloud Mailbox、および Secure Email のバンドルライセンスとオプションライセンスに絞って掲載しています。Secure Email のバンドルライセンスにアラカルトで機能を追加できるアドオンライセンスの詳細は、データシートおよび発注ガイドをご覧ください。

Cisco Secure Email Cloud Mailbox ライセンス [*1]

製品型番	製品説明
CMD-ESS-LIC	Secure Email Cloud Mailbox Essential ライセンス。Microsoft 365 と API で連携、迅速に導入可能。可視化、および Microsoft 365 のセキュリティを補完。

*1　1、3、または 5 年間のサブスクリプション。CCW では CMD-SEC-SUB が必要。詳細は発注ガイドを参照。

Cisco Secure Email ライセンス [*1]

製品型番		メール受信				メール送信		Mcrosoft 365	
		アンチスパム フィルタリング	アウトブレイク フィルタ	アンチウイルス フィルタリング	アンチマルウェア / サンドボックス	DLP（データ漏洩防止）	暗号化	Mcrosoft 365 に最適化	API 連携 [*2]
クラウド	CES-O365ESS-BNDL	✓	✓	[*4]	[*5]	[*5]	[*5]	✓	[*5]
	CES-O365PREM-BNDL	✓	✓	[*4]	[*5]	✓	✓	✓	[*5]
	CES-ESSENTL-BNDL	✓	✓	✓	[*5]	[*5]	[*5]		[*5]
	CES-ESSN-AMP-BNDL	✓	✓	✓	✓	[*5]	[*5]		[*5]
	CES-OUTBOUND-BNDL					✓	✓		[*5]
	CES-PREMIUM-BNDL	✓	✓	✓	[*5]	✓	✓		[*5]
	CES-PREM-AMP-BNDL	✓	✓	✓	✓	✓	✓		[*5]
オンプレミス [*3]	ESA-ESI-LIC	✓	✓	✓	[*5]	[*5]	[*5]		
	ESA-ESI-AT-LIC	✓	✓	✓	✓	[*5]	[*5]		
	ESA-ESO-LIC					✓	✓		
	ESA-ESP-LIC	✓	✓	✓	[*5]	✓	✓		
	ESA-ESP-AT-LIC	✓	✓	✓	✓	✓	✓		
ハイブリッド [*3]	H-ESA-ESI-LIC	✓	✓	✓	[*5]	[*5]	[*5]		[*5]
	H-ESA-ESI-AT-LIC	✓	✓	✓	✓	[*5]	[*5]		[*5]
	H-ESA-ESO-LIC					✓	✓		[*5]
	H-ESA-ESP-LIC	✓	✓	✓	[*5]	✓	✓		[*5]
	H-ESA-ESP-AT-LIC	✓	✓	✓	✓	✓	✓		[*5]

*1　1、3、または 5 年間のサブスクリプション（100 ユーザ～）。CCW では EMAIL-SEC-SUB が必要。詳細は発注ガイドを参照。　*2　Secure Email Cloud Mailbox に相当する機能。
*3　Secure Email アプライアンス（物理または仮想）が必要。　*4　Microsoft 365 で提供。　*5　アドオンライセンスで追加可能。

Cisco Secure Email 用 Cisco Secure Email Phishing Defense ライセンス

製品型番	製品説明
L-ESA-APP-*n*Y-S*m* [*1 *2]	オンプレミス用 Phishing Defense ライセンス [*5]
L-ESA-APPC-*n*Y-S*m* [*1 *3]	オンプレミス用 Phishing Defense ライセンス [*6]
L-CES-APPC-*n*Y-S*m* [*1 *4]	クラウド用 Phishing Defense ライセンス

Cisco Secure Email 用 Cisco Secure Email Domain Protection ライセンス

製品型番	製品説明
L-ESA-DMP-*n*Y-S*m* [*1 *7]	オンプレミス用 Domain Protection ライセンス
L-CES-DMP-*n*Y-S*m* [*1 *8]	クラウド用 Domain Protection ライセンス

*1　*n* = 1、3（年間）。*m* = 1 ～ 15（バンド）。
*2　CCW では L-ESA-APP-LIC= が必要。
*3　CCW では L-ESA-APPC-LIC= が必要。
*4　CCW では L-CES-APPC-LIC= が必要。
*5　オンプレミスセンサーでメールのメタデータのみ Phishing Defense クラウドに送信。
*6　クラウドセンサーでメールデータを Phishing Defense クラウドに送信。
*7　CCW では L-ESA-DMP-LIC= が必要。
*8　CCW では L-CES-DMP-LIC= が必要。
*9　1、3、または 5 年間のサブスクリプション。CCW では SA-SEC-SUB が必要。

Cisco Secure Email 用 Cisco Security Awareness トレーニング ライセンス [*9]

製品型番	製品説明
SA-SS-LIC	Security Awareness シミュレーション ライセンス
SA-SLT-LIC	Security Awareness シミュレーション & トレーニング ライセンス

ハードウェア仕様

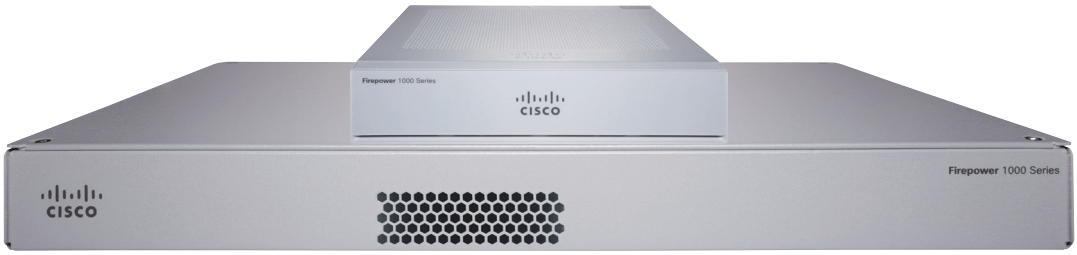
本カタログでは、Secure Email 物理アプライアンスに絞って掲載しています。仮想アプライアンスの詳細は、データシートおよび発注ガイドをご覧ください。

Cisco Secure Email アプライアンス

製品型番	ストレージ		メモリ	CPU		ダウンリンク / アップリンク		電源二重化	ラックマウント
	構成	RAID		コア	クロック	1GE RJ45	10GE SFP+		
ESA-C195-K9	2 × 600 GB	1	16 GB	8	2.1 GHz	2		[*1]	1 RU
ESA-C395-K9	2 × 600 GB	1	16 GB	12	2.1 GHz	6		✓	1 RU
ESA-C695-K9	8 × 600 GB	10	32 GB	12	2.1 GHz	6		✓	2 RU
ESA-C695F-K9	8 × 600 GB	10	32 GB	12	2.6 GHz		2	✓	2 RU

*1　電源モジュール（CCS-PSU1-770AC）の追加が必要。

Cisco Secure Firewall（次世代ファイアウォール）



次世代ファイアウォール（NGFW）　次世代侵入防御システム（NGIPS）　高度なマルウェア保護（AMP）　URL フィルタリング　IPsec/SSL VPN　1GE RJ45　1GE SFP　10GE SFP+　ネットワークモジュール

ハードウェア / ソフトウェア仕様

本カタログでは、Firepower 1000/2100 および Secure FTD Virtual に絞って掲載しています。その他の製品の詳細は、Web サイトをご覧ください。

Cisco Firepower 1000 シリーズ

製品型番		最大スループット *1			AVC セッション		VPN ピア最大数	ダウンリンク / アップリンク				電源二重化	ラックマウント
FTD モデル（FTD イメージで出荷）	ASA モデル（ASA イメージで出荷）	FW + AVC	FW + AVC + IPS	VPN	同時セッション数	新規接続（秒単位）		1GE RJ45	1GE SFP	10GE SFP+	NM スロット		
FPR1010-NGFW-K9	FPR1010-ASA-K9	890 Mbps	880 Mbps	400 Mbps	100,000	6,000	75	8*2					1 RU*3
FPR1120-NGFW-K9	FPR1120-ASA-K9	2.3 Gbps	2.3 Gbps	1.2 Gbps	200,000	15,000	150	8	4				1 RU
FPR1140-NGFW-K9	FPR1140-ASA-K9	3.3 Gbps	3.3 Gbps	1.4 Gbps	400,000	22,000	400	8	4				1 RU
FPR1150-NGFW-K9	FPR1150-ASA-K9	5.3 Gbps	4.9 Gbps	2.4 Gbps	600,000	28,000	800	8	2	2			1 RU

*1　FTD イメージのパフォーマンス指標。　*2　PoE 給電対応 2 ポートを含む。　*3　ラックマウントキット（FPR1K-DT-RACK-MNT=）が必要。

Cisco Firepower 2100 シリーズ

製品型番		最大スループット *1			AVC セッション		VPN ピア最大数	ダウンリンク / アップリンク				電源二重化	ラックマウント
FTD モデル（FTD イメージで出荷）	ASA モデル（ASA イメージで出荷）	FW + AVC	FW + AVC + IPS	VPN	同時セッション数	新規接続（秒単位）		1GE RJ45	1GE SFP	10GE SFP+	NM スロット		
FPR2110-NGFW-K9	FPR2110-ASA-K9	2.6 Gbps	2.6 Gbps	950 Mbps	1,000,000	14,000	1,500	12	4				1 RU
FPR2120-NGFW-K9	FPR2120-ASA-K9	3.4 Gbps	3.4 Gbps	1.2 Gbps	1,500,000	18,000	3,500	12	4				1 RU
FPR2130-NGFW-K9	FPR2130-ASA-K9	5.4 Gbps	5.4 Gbps	1.9 Gbps	2,000,000	30,000	7,500	12	4		1*2	✓	1 RU
FPR2140-NGFW-K9	FPR2140-ASA-K9	10.4 Gbps	10.4 Gbps	3.6 Gbps	3,000,000	57,000	10,000	12	4		1*2	✓	1 RU

*1　FTD イメージのパフォーマンス指標。　*2　8 × 1GE SFP（FPR2K-NM-8X1G）や 8 × 10GE SFP+（FPR2K-NM-8X10G）など、各種ネットワークモジュールをサポート。詳細は発注ガイドを参照。

Cisco Secure Firewall Threat Defense Virtual（旧 Cisco Firepower Threat Defense Virtual/Cisco Firepower NGFW Virtual）

製品型番	仮想マシン構成		最大スループット			AVC セッション		VPN ピア最大数
	仮想 CPU	仮想メモリ	FW + AVC	FW + AVC + IPS	VPN	同時セッション数	新規接続（秒単位）	
FPRTD-V-K9 FTD-V-*n*S-BSE-K9*1	4	8 GB	3.0 Gbps	3.0 Gbps	1.1 Gbps	100,000	20,000	250
	8	16 GB	5.5 Gbps	5.5 Gbps	2.0 Gbps	250,000	20,000	250
	12	24 GB	10.0 Gbps	10.0 Gbps	4.0 Gbps	500,000	40,000	750

*1　階層型サブスクリプション ライセンス製品型番。CCW では FTDV-SEC-SUB が必要。*n* = 5、10、または 20（4 × 仮想 CPU が必要）、30（8 × 仮想 CPU が必要）、50（12 × 仮想 CPU が必要）。詳細はデータシート（英語）を参照。

サブスクリプション ライセンス

Cisco Secure Firewall Threat Defense ライセンス（旧 Cisco Firepower Threat Defense ライセンス）

製品型番例	対応モデル
L-FPR1010T-*x*-*n*Y*1	Firepower 1010
L-FPR1120T-*x*-*n*Y*1	Firepower 1020
L-FPR1140T-*x*-*n*Y*1	Firepower 1040
L-FPR1150T-*x*-*n*Y*1	Firepower 1050
L-FPR2110T-*x*-*n*Y*1	Firepower 2110
L-FPR2120T-*x*-*n*Y*1	Firepower 2120
L-FPR2130T-*x*-*n*Y*1	Firepower 2130
L-FPR2140T-*x*-*n*Y*1	Firepower 2140
L-FPRTD-V-*x*-*n*Y*2	Secure FTD Virtual*4
FTD-V-*m*S-*x*-*3	Secure FTD Virtual*5

製品型番に含まれる文字列（*x*）	対応セキュリティサービス
T	脅威保護
AMP	マルウェア保護
URL	URL フィルタリング
TM	脅威保護 + マルウェア保護
TC	脅威保護 + URL フィルタリング
TMC	脅威保護 + マルウェア保護 + URL フィルタリング

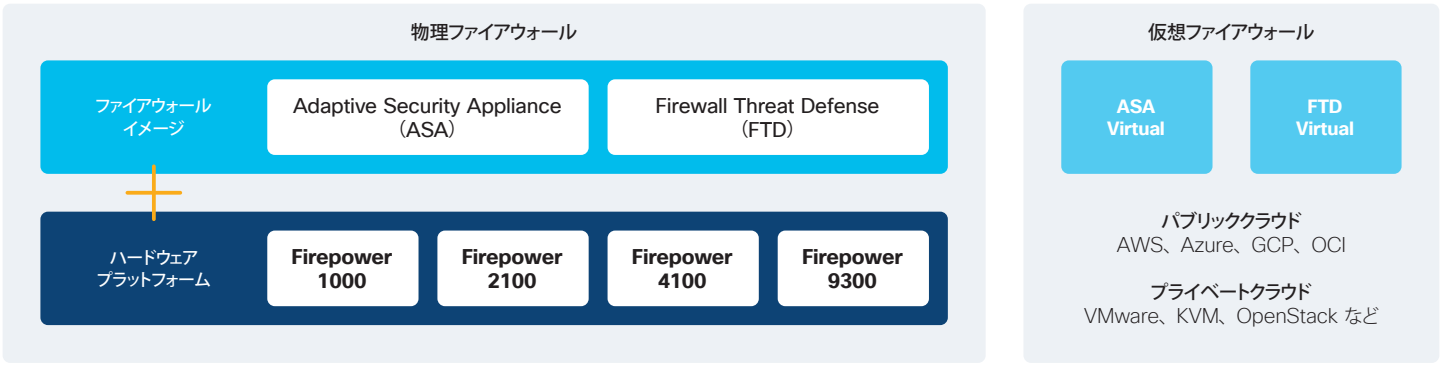
製品型番に含まれる数字（*n*）	期間
1	1 年間
3	3 年間
5	5 年間

*1　CCW では FPR*nnnn*T-x または L-FPR*nnnn*T-*x*= が必要（*nnnn* は対応モデル番号、*x* は対応セキュリティサービス）。詳細は発注ガイドを参照。
*2　CCW では L-FPRTD-V-*x*= が必要（*x* は対応セキュリティサービス）。詳細は発注ガイドを参照。
*3　CCW では FTDV-SEC-SUB が必要。　*m* = 5、10、20、30、50。詳細はデータシート（英語）を参照。
*4　従来型ライセンス（FPRTD-V-K9）に対応。
*5　階層型サブスクリプション ライセンス（FTD-V-*n*S-BSE-K9）に対応。

Cisco Secure Firewall ポートフォリオ

Forrester 社の『The Forrester Wave: Enterprise Firewalls, Q3 2020』でシスコがエンタープライズ ファイアウォール分野のリーダーに選出されました。

シスコの各種ファイアウォール製品が「Cisco Secure Firewall」としてリブランド、ポートフォリオがシンプルになりました。



Cisco Secure Firewall の選び方

Cisco Secure Firewall はオンプレミスにもクラウドにも導入可能、複数の製品を一元管理できる運用管理ツールもオンプレミスおよびクラウドに導入可能です。

1. 物理ファイアウォールまたは仮想ファイアウォールを選択
2. ファイアウォールイメージを選択
   - 従来のレイヤ 3 および レイヤ 4 ファイアウォールと VPN のみ必要な場合：**Cisco Secure Firewall Adaptive Security Appliance（ASA）**[*1]
   - 次世代ファイアウォールや次世代侵入防御システムなど、高度な脅威対策機能も必要な場合：**Cisco Secure Firewall Threat Defense（FTD）**[*2]
3. スループットなど要件に応じて、シリーズやモデル、ライセンスを選択
4. 必要に応じて、一元管理ツールを選択
   - 複数の ASA をオンプレミスで一元管理したい場合：**Cisco Security Manager**
   - 複数の FTD をオンプレミスで一元管理したい場合：**Cisco Secure Firewall Management Center**[*3]
   - 複数の ASA および FTD をクラウドで一元管理したい場合：**Cisco Defense Orchestrator**

*1 旧称は Cisco Adaptive Security Appliance。
*2 旧称は Cisco Firepower Threat Defense。
*3 旧称は Cisco Firepower Management Center。

Cisco Secure ASA & FTD 主な機能比較（物理ファイアウォール）

製品型番（サンプル）	ASA	FTD
ビルトイン管理ツール	• Adaptive Security Device Manager	• Firepower Device Manager
一元管理 / 自動化ツール	• Security Manager • Defense Orchestrator	• Secure Firewall Management Center • Defense Orchestrator
ファイアウォール動作モード	• トランスペアレント • ルーテッド	• トランスペアレント • ルーテッド • マルチインスタンス [*1]
ファイアウォール	• ステートフル ファイアウォール • レイヤ 7 プロトコル検査 • NAT	• ステートフル ファイアウォール • レイヤ 7 プロトコル検査 • NAT
次世代ファイアウォールなど高度な脅威対策		• アプリケーションの可視化と制御 • 侵入防御システム（Snort 3 対応 NEW） • 高度なマルウェア保護（AMP） • Secure Malware Analytics（旧：Threat Grid）連携 • URL フィルタリング • Web セーフサーチと Youtube for Schools • SSL 復号（ハードウェア アクセラレーション）
サイト間 VPN	• IPsec IKEv1/v2	• IPsec IKEv1/v2
リモートアクセス VPN	• AnyConnect • クライアントレス VPN • サードパーティクライアント	• AnyConnect
アクセス制御	• IP アドレスベース • VLAN ベース • ポートベース • ユーザ ID/ グループベース • SGT ベース	• ゾーンベース • IP アドレスベース • ジオロケーションベース • VLAN ベース • ポートベース • ユーザ ID/ グループベース • アプリケーション ID ベース • SGT ベース
アイデンティティ制御	• SGT ベースでトラフィックポリシーを適用	• SGT ベースでトラフィックポリシーを適用 • ISE 連携で迅速に脅威を封じ込め
ネットワークディスカバリ		• ネットワーク / アプリケーション / ユーザ ディスカバリ • インパクト解析
ログと分析	• デバイスヘルス • SecureX 連携（Defense Orchestrator のみ）	• デバイスヘルス • SecureX 連携 • カスタマイズ可能なレポート

*1 Firepower 4100/9300 のみ対応。

Cisco **AnyConnect** Secure Mobility Client

セキュアなテレワークを実現する、マルチセキュリティ対応 VPN クライアント

Cisco AnyConnect Secure Mobility Client は、モジュール式のマルチセキュリティ対応 VPN クライアントです。Cisco Secure Firewall などヘッドエンドとの IPsec IKEv2 や SSL 接続によって安全なリモートアクセスを提供するだけでなく、さまざまなセキュリティモジュールによってシスコのセキュリティサービスと連携可能。たとえば、Umbrella ローミングセキュリティ モジュールや AMP イネーブラ モジュールによって、Cisco Umbrella や Cisco Secure Endpoint のクライアントとしても動作するため、これらのセキュリティサービスをシンプルかつ迅速に展開できます。

Cisco AnyConnect Secure Mobility Client は、Windows や macOS、Linux、iOS、Android、Windows Phone/Mobile、BlackBerry、ChromeOS など、幅広いプラットフォームに対応しています。

ライセンス仕様比較

セキュリティサービス	Plus	Apex
デバイスまたはシステム VPN（Cisco Phone VPN を含む）	✓	✓
サードパーティ IPsec IKEv2 リモート アクセス VPN クライアント（非 AnyConnect クライアント）	✓	✓
アプリケーション別 VPN	✓	✓
クライアントレス（ブラウザベース）VPN 接続		✓
Suite B または次世代暗号化（サードパーティ IPsec IKEv2 リモート VPN クライアントを含む）		✓
ASA マルチコンテキストモードのリモートアクセス		✓
SAML 認証		✓
Umbrella ローミングセキュリティ モジュール *1	✓	✓
Secure Endpoint イネーブラ モジュール *2	✓	✓
クラウド Web セキュリティ モジュール	✓	✓
ネットワークアクセス管理モジュール	✓	✓
ネットワーク可視化モジュール		✓
ISE ポスチャ モジュール *3		✓

*1 Umbrella ライセンスが必要。 *2 Secure Endpoint ライセンスが必要。
*3 ISE Apex ライセンスが必要。

サブスクリプション ライセンス

Cisco AnyConnect Plus ライセンス *1

製品型番			ユーザ数 対象範囲
1 年間	3 年間	5 年間	
L-AC-PLS-1Y-S1	L-AC-PLS-3Y-S1	L-AC-PLS-5Y-S1	25 ～ 99
L-AC-PLS-1Y-S2	L-AC-PLS-3Y-S2	L-AC-PLS-5Y-S2	100 ～ 249
L-AC-PLS-1Y-S3	L-AC-PLS-3Y-S3	L-AC-PLS-5Y-S3	250 ～ 499
L-AC-PLS-1Y-S4	L-AC-PLS-3Y-S4	L-AC-PLS-5Y-S4	500 ～ 999

*1 CCW では L-AC-PLS-LIC= が必要。999 ユーザまでの SKU に絞って掲載。詳細は発注ガイドを参照。

Cisco AnyConnect Apex ライセンス *1

製品型番			ユーザ数 対象範囲
1 年間	3 年間	5 年間	
L-AC-APX-1Y-S1	L-AC-APX-3Y-S1	L-AC-APX-5Y-S1	25 ～ 99
L-AC-APX-1Y-S2	L-AC-APX-3Y-S2	L-AC-APX -5Y-S2	100 ～ 249
L-AC-APX-1Y-S3	L-AC-APX-3Y-S3	L-AC-APX -5Y-S3	250 ～ 499
L-AC-APX-1Y-S4	L-AC-APX-3Y-S4	L-AC-APX -5Y-S4	500 ～ 999

*1 CCW では L-AC-APX-LIC= が必要。999 ユーザまでの SKU に絞って掲載。詳細は発注ガイドを参照。

永続ライセンス *1

Cisco AnyConnect Plus ライセンス *2

製品型番	ユーザ数	製品型番	ユーザ数
AC-PLS-P-25-S	25	AC-PLS-P-250-S	250
AC-PLS-P-50-S	50	AC-PLS-P-500-S	500
AC-PLS-P-100-S	100	AC-PLS-P-1K-S	1,000

*1 本カタログでは、AnyConnect Plus ライセンスに絞って掲載しています。AnyConnect VPN Only ライセンスの詳細は発注ガイドをご覧ください。
*2 CCW では L-AC-PLS-P-G が必要。1,000 ユーザまでの SKU に絞って掲載。詳細は発注ガイドを参照。

Cisco Secure Endpoint（AMP for Endpoints）

EPP + EDR：エンドポイントを脅威から保護、さらに脅威の検知、調査、対応も実現する、統合型エンドポイントセキュリティ

Cisco Secure Endpoint は、最新の高度な脅威にも迅速に対抗できる、統合型エンドポイント セキュリティです。EPP（Endpoint Protection Platform）と EDR（Endpoint Detection & Response）を兼ね備えたセキュリティによって、既知の脅威の侵入を阻止してエンドポイントを保護できるだけでなく、未知の脅威が侵入してしまっても迅速に検知、調査、および対応できます。

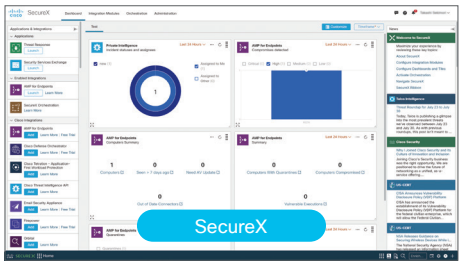
- ファイルレスマルウェアから保護
- ふるまい分析で悪意のある動作から保護
- アンチウイルスで保護
- 機械学習で検知および保護
- 各種プラットフォームと連携、攻撃対象を削減

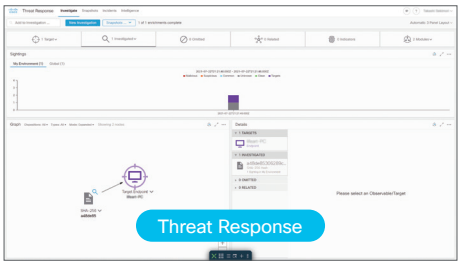
- ファイルやプロセスのアクティビティを継続的にモニタリング
- エンドポイント内部の詳細な情報をリアルタイムで検索
- サンドボクシングで高度な解析
- IoC（侵害の痕跡）によるふるまい検知とフォレンジック調査
- 脆弱なソフトウェアを特定、攻撃パスを遮断
- イベント検出時のフォレンジック スナップショット取得
- SecureX 脅威ハンティングで高度な脅威検知、MITRE ATT&CK フレームワークとマッピング
- SecureX プラットフォームによる XDR

- ファイルやネットワーク ラフィックの許可 / ブロックリスト
- アプリケーションの許可 / ブロックリスト
- エンドポイントを隔離
- SecureX リボンで迅速な調査
- SecureX 経由で各種セキュリティ プラットフォームと統合、脅威対応を迅速化および自動化

XDR：シスコの各種セキュリティプラットフォームとの統合によって、より高度かつ迅速な脅威の検知、調査、対応を実現

Cisco Secure Endpoint は、シスコの各種セキュリティ ソリューションを統合する **Cisco SecureX** プラットフォーム、エンドポイント内部の情報を収集および追跡するための各種クエリをサポートする **Cisco Orbital**、脅威を伝播経路も含めて可視化する **Cisco Threat Response** と連携することで、より高度かつ迅速な脅威の検知、調査、対応を実現する XDR（Extended Detection & Response）も標準で提供します。





ライセンス別機能比較

セキュリティサービス		Essentials	Advantage	Premier
アンチマルウェア	ファイルレスとファイルベース、両方の攻撃を検知する強力な保護エンジンによって、既知の脅威を自動ブロック	✓	✓	✓
アプリケーション制御	256 ビットのハッシュ値ベースでアプリケーションを個別に許可 / ブロック（カスタムアプリケーション対応）	✓	✓	✓
動的なファイル分析	ビルトインのサンドボックスで疑わしいファイルを実行、詳細に分析	✓	✓	✓
ファイルとプロセスをモニタリング	ファイルやプロセスの疑わしいふるまいを検知、動作を防止	✓	✓	✓
脆弱性を特定	脆弱性のあるソフトウェアを特定、それらを実行しているエンドポイントを一覧表示	✓	✓	✓
エンドポイント隔離	感染したエンドポイントをワンクリックで隔離、脅威の拡大を防止	✓	✓	✓
Orbital クエリで高度な調査	事前に定義された 100 以上のクエリを含む複雑なクエリをエンドポイントで迅速に実行、情報収集		✓	✓
Secure Malware Analytics クラウドサンドボックス	Secure Malware Analytics（旧 Threat Grid）クラウドサンドボックスで高度かつ動的なファイル分析		✓	✓
SecureX 脅威ハンティング	上級アナリストによる高度な調査で脅威を特定、対策を提示			✓
プライベートクラウドで導入	物理または仮想アプライアンス導入オプションで、パブリッククラウドの利用に制限がある組織もサポート *1	✓		

*1　詳細は発注ガイドを参照。

サブスクリプション ライセンス *1

製品型番	製品説明
AMP4E-CL-LIC	Secure Endpoint Essentials エンドポイント別ライセンス
AMP4E-ADV-CL-LIC	Secure Endpoint Advantage エンドポイント別ライセンス
AMP4E-PRE-CL-LIC	Secure Endpoint Premier エンドポイント別ライセンス

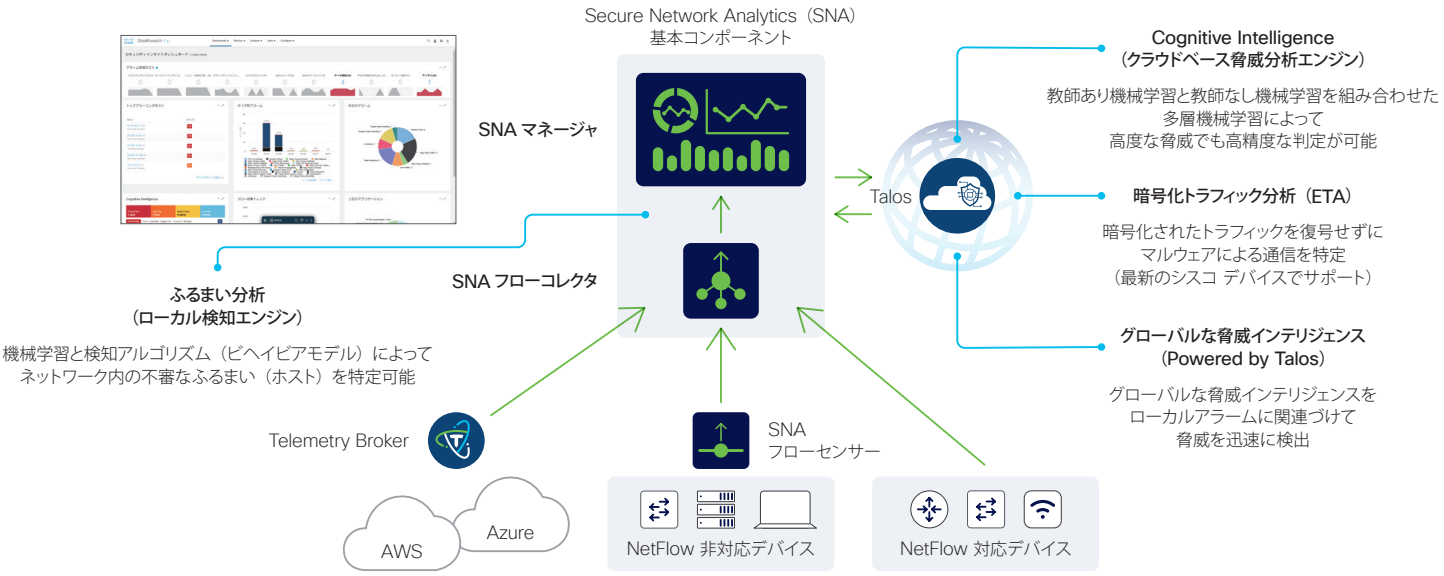
*1　1、3、または 5 年間のサブスクリプション。CCW では AMP4E-SEC-SUB が必要。詳細は発注ガイドを参照。

Cisco Secure Network Analytics（Stealthwatch）

ネットワークを包括的に可視化、業界最先端の機械学習とビヘイビアモデルで脅威を分析

Cisco Secure Network Analytics は、包括的なネットワーク可視化およびセキュリティ分析ソリューションです。既存のネットワークインフラからテレメトリデータを収集、可視化して、業界最先端の機械学習、ビヘイビアモデル、およびグローバルな脅威インテリジェンスで分析、脅威を検出します。

ネットワークインフラが Cisco Catalyst 9000 シリーズ スイッチなど最新のシスコ デバイスで構成される場合は、**暗号化トラフィック分析**（Encrypted Traffic Analytics；ETA）によって暗号化されたトラフィックも可視化および分析できます。



サブスクリプション ライセンス

本カタログでは、主要なライセンスに絞って掲載しています。
その他のライセンスの詳細は、データシートおよび発注ガイド（英語）をご覧ください。

Cisco Secure Network Analytics フローレート ライセンス *1

製品型番	製品説明
ST-FR-100-LIC	Secure Network Analytics フローレート ライセンス（100 FPS パック）

*1　1 ～ 5 年間のサブスクリプション。
CCW では ST-SEC-BUN または ST-SEC-BUN-DISTI を推奨。

ハードウェア / ソフトウェア仕様

本カタログでは、主要なハードウェア / ソフトウェアに絞って掲載しています。
その他のハードウェア / ソフトウェアの詳細は、データシートおよび発注ガイド（英語）をご覧ください。

Cisco Secure Network Analytics フローコレクタ

製品型番	ノード	フロー（秒単位）	インターフェイス	エクスポータ	フローストレージ		メモリ	CPU		イーサネットポート *2			電源二重化	ラックマウント
					容量	RAID		コア	クロック	1GE RJ45	10GE RJ45	10GE SFP+		
ST-FC4210-K9		200,000*1	65,535	4,096	4 TB	6	512 GB	2 × 16	2.1 GHz	2	2	2	✓	1 RU
ST-FC5210-K9	エンジン	300,000	65,535	4,096			256 GB	2 × 16	2.1 GHz	2	2	2	✓	1 RU
	データベース				6 TB	10	512 GB	2 × 16	2.1 GHz	2	2	2	✓	2 RU

*1　データストアなしの場合。データストアありの場合は 250,000 ～ 500,000。　*2　構成はスペックシート（ST-FC4210-K9/ST-FC5210-K9）を参照。

Cisco Secure Network Analytics フローコレクタ（Virtual Edition）*1

製品型番	仮想マシン構成		フロー（秒単位）	インターフェイス	エクスポータ
	仮想 CPU	仮想メモリ			
L-ST-FC-VE-K9	2	24 GB	10,000	65,535	1,024
	6	32 GB	30,000	65,535	1,024
	8	64 GB	60,000	65,535	2,048
	12	128 GB	120,000	65,535	4,096

*1　システム要件の詳細はインストールガイドを参照。

Cisco Secure Network Analytics マネージャ

製品型番	フローコレクタ管理数	データストレージ		メモリ	CPU		イーサネットポート *1			電源二重化	ラックマウント
		容量	RAID		コア	クロック	1GE RJ45	10GE RJ45	10GE SFP+		
ST-SMC2210-K9	25	4 TB	6	512 GB	2 × 16	2.1 GHz	2	2	2	✓	1 RU

*1　構成はスペックシートを参照。

Cisco Secure Network Analytics マネージャ（Virtual Edition）*1

製品型番	仮想マシン構成		フローコレクタ管理数	同時接続ユーザ
	仮想 CPU	仮想メモリ		
L-ST-SMC-VE-K9	4	32 GB	5	～ 9
	8	64 GB	25	10 ～

*1　システム要件の詳細はインストールガイドを参照。

TIP バンドルについて

Secure Network Analytics 製品は、セキュリティバンドル（ST-SEC-BUN または ST-SEC-BUN-DIST）による購入を推奨します。

Cisco Identity Services Engine

高度な可視化とセグメンテーションで脅威に対策できる、統合認証サーバ

Cisco Identity Services Engine (ISE) は、RADIUS および TACACS+ 認証サービスを中心とした、さまざまなコンポーネントで構成される統合認証サーバです。ID データベース連携 *1 だけでなく、エコシステム連携による高度な脅威対策も実現。あらゆるユーザ、モノ、それらが接続するネットワークを適切に保護できます。

セキュアアクセス
802.1X 認証などによる有線 / 無線アクセス
証明書の発行 / 配布サービス
リモートアクセスやゲストアクセス

セグメンテーション
わかりやすい GUI による グループベースのアクセスポリシー
IP アドレスや VLAN に依存しない ネットワークアクセス制御

プロファイリング
接続するエンドポイントを 可視化および分析
セキュリティポスチャを自動更新 組織のリスクを低減

脅威の封じ込め
脆弱性や脅威スコアに基づく エンドポイント自動隔離
サードパーティのエコシステムと API で連携可能

検疫
エンドポイントのポスチャ評価 コンプライアンス準拠を確認
AnyConnect および EMM/MDM と連携可能

*1 Active Directory、LDAP、OTP（ワンタイムパスワード）、SAML ID プロバイダなど、各種データベースと連携。

ライセンス別機能比較

本カタログでは、ISE 3.0 以降の新ライセンスモデルを掲載しています。
旧ライセンスモデルの詳細は発注ガイド、旧ライセンスモデルからの移行方法は移行ガイド（英語）をご覧ください。

セキュリティサービス		Essentials	Advantage	Premier
セキュアアクセス	基本的な RADIUS 認証、許可、アカウンティング（802.1X、MAC 認証バイパス、Easy Connect、Web 認証を含む）	✓	✓	✓
	MACsec	✓	✓	✓
	SSO、SAML、ODBC ベースの認証	✓	✓	✓
	ゲストポータルおよびスポンサーサービス	✓	✓	✓
	Representational State Transfer（モニタリング）API	✓	✓	✓
	外部 RESTful サービス（CRUD）対応 API	✓	✓	✓
	PassiveID（シスコのサブスクライバ）	✓	✓	✓
	PassiveID（シスコ以外のサブスクライバ）		✓	✓
	有線およびワイヤレスのセキュアアクセス	✓	✓	✓
	デバイス登録（My Devices ポータル）、およびビルトインの認証局（CA）を使用した BYOD プロビジョニング		✓	✓
セグメンテーション	セキュリティグループタグ（TrustSec SGT）の割り当てと ACI の統合		✓	✓
プロファイリング	基本的なアセット可視化と制御（プロファイリング）		✓	✓
	基本的なアセットフィードサービス		✓	✓
	高度なアセット可視化（エンドポイント分析）		✓	✓
	高度なアセット制御（エンドポイント分析）			✓
	ロケーションベースの統合に基づく可視化と制御		✓	✓
脅威の封じ込め	コンテキスト共有とセキュリティエコシステムの統合		✓	✓
	エンドポイント保護サービス（Endpoint Protection Services；EPS）			✓
	迅速な脅威の封じ込め（Rapid Threat Containment；RTC、適応型ネットワーク制御とコンテキスト共有を使用）			✓
検疫	ポスチャの可視化と制御			✓
	エンタープライズモビリティ管理（EMM）およびモバイルデバイス管理（MDM）の統合による可視化と適用			✓
	脅威中心型ネットワークアクセス制御			✓

サブスクリプション ライセンス *1

製品型番	製品説明
ISE-E-LIC	ISE Essentials ライセンス（100 セッション～）
ISE-A-LIC	ISE Advantage ライセンス（100 セッション～）
ISE-P-LIC	ISE Premier ライセンス（100 セッション～）

*1 1、3、または 5 年間のサブスクリプション。CCW では ISE-SEC-SUB が必要。詳細は発注ガイドを参照。

永続ライセンス

製品型番	製品説明
L-ISE-TACACS-ND=	ISE デバイス管理ノード ライセンス *2
L-ISE-IPSEC	ISE IPsec ライセンス *2 *3

*1 ポリシーサービスノード別に必要。 *2 ポリシーサービスノード別に最大 150 トンネルをサポート。

ハードウェア / ソフトウェア仕様

Cisco Secure Network Server for Cisco Identity Services Engine

製品型番	同時接続エンドポイント数（セッション数）		ストレージ		メモリ	CPU		ダウンリンク / アップリンク		電源二重化	ラックマウント
	スタンドアロン構成	分散構成	構成	RAID		コア	クロック	1GE RJ45	10GE SFP+		
SNS-3615-K9	10,000	10,000	1 × 600 GB		32 GB	8	2.1 GHz	4	2		1 RU
SNS-3655-K9	25,000	50,000	4 × 600 GB	10	96 GB	12	2.1 GHz	4	2	✓	1 RU
SNS-3695-K9	50,000	100,000	8 × 600 GB	10	256 GB	12	2.1 GHz	4	2	✓	1 RU

Cisco Identity Services Engine Virtual Machine *1

製品型番	仮想マシン構成		同時接続エンドポイント数（セッション数）	
	仮想 CPU *2	仮想メモリ	スタンドアロン構成 *3	分散構成 *4
R-ISE-VMS-K9=	16	32 GB	10,000	10,000
R-ISE-VMM-K9=	24	96 GB	25,000	50,000
R-ISE-VML-K9=	24	256 GB	50,000	100,000

*1 VMware ESXi（5.x、6.x、7.x）、VMware Cloud on AWS、Azure VMware Solution、Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V、QEMU 1.5.3-160 上の KVM に対応。システム要件の詳細はインストールガイドを参照。
*2 SSE 4.2 対応 CPU が必要。
*3 デフォルトのスタンドアロン構成 1 ノード、または 2 ノードによる高可用性構成で運用する場合。
*4 複数ノードによる分散構成のポリシーサービス専用ノードとして運用する場合。

シスコ セキュリティ製品 Web サイトのご紹介

本カタログでは、一部のセキュリティ製品に絞って掲載しています。すべてのセキュリティ製品の詳細は、Web サイトをご覧ください。

www.cisco.com/jp/go/security