Cisco Secure Firewall ISA3000

目次

非常に過酷な産業環境にも耐えるように開発された産業用ファイアウォールです。産業環境での運用を念頭に置いた設計で、優れたエンドツーエンドのセキュリティを提供します。

製品の概要

Cisco® Secure Firewall ISA3000 は、実績のあるエンタープライズクラスのセキュリティに基づいて OT をターゲットにした保護を提供する、真の産業用ファイアウォールです。

ISA3000 は、4 つのデータリンクを備えた DIN レールマウント設計の堅牢なアプライアンスであり、非常に過酷な産業環境の要求にも応える多様なアクセス制御、脅威制御、アプリケーション制御を提供します。

図 1.
2 つの銅線ポートと 2 つの光ファイバポート（左）または 4 つの銅線ポート（右）を備えた Cisco Secure Firewall ISA3000

ISA3000 は、Omron、Rockwell、GE、Schneider、Siemens などの主要な自動化ベンダーによって開発された産業用プロトコルおよびアプリケーションの可視性と制御を備えた、Cisco Secure Firewall の実証済みのセキュリティをバンドルしています。ISA3000 は、IT と OT のセキュリティの統合を開始し、産業用デジタル化の成果を得るための鍵となります。

IoT と OT のセキュリティジャーニーの基盤となるコンポーネントとして、ISA3000 は、産業用ネットワークをセグメント化し、潜在的な脅威から OT 資産を保護するための理想的かつ堅牢なファイアウォールです。NERC-CIP、ISA99/IEC62443、CFATS、ANSI/AWWA G430 などのさまざまな産業標準、規制、およびガイドラインに準拠して構築されています。

ISA3000 は、最も要求の厳しい業界（電力会社、石油およびガス、輸送、採掘、製造、水道など）で導入できることが実証済みです。小規模の分散型産業用サイトを接続し、大規模な内部ネットワークのセグメンテーションを実施し、VPN 接続を管理して、リモート資産の安全な管理とシームレスな分散運用を実現する DMZ ファイアウォールとして広く使用されています。

ISA3000 は、産業プロセスと脆弱な制御機器を保護します。また、Cisco Talos® が作成した業界をリードする脅威検出ルールおよび脆弱性エクスプロイト保護ルール（業界に特化した数千のルールを含む）を活用します。産業用プロトコルの OpenAppID とディープ パケット インスペクション（DPI）を使用して、独自のカスタムディテクタを作成してアラートを作成し、最も重要な産業アプリケーションフローに基づいてトラフィックをブロックまたは許可することもできます。Cisco Advanced Malware Protection（AMP）も組み込まれており、疑わしいファイルの伝達を継続的に追跡します。

使いやすいオンボックスのデバイスマネージャ、オンプレミスの集中管理、またはクラウドベースの管理ソリューションのいずれかを介して管理される ISA3000 は、産業に特化したすぐに使用可能な設定とシンプルな運用管理を提供します。また、これらの管理ツールは、IT ドメイン内のシスコファイアウォールですでに使用しているツールと同じであるため、IT セキュリティを OT に拡張し、ドメイン全体で一貫したセキュリティポリシーを容易に適用できます。

シスコの包括的なセキュリティポートフォリオの一部として、ISA3000 は既存のツールと連携して、統合された IT/OT セキュリティワークフローを実現します。Cisco Cyber Vision は、意味のあるコンテキストに応じたセキュリティポリシーの構築を可能にするホスト属性情報を提供します。Cisco Identity Services Engine（ISE）は、セキュリティ適用のためにセキュリティグループタグ（SGT）を使用して、統合されたポリシー更新やホストコンテキスト情報を交換するために利用できます。ISA3000 は、Cisco Stealthwatch® と NetFlow 情報を交換して、ネットワークレベルのコンテキスト情報も提供できます。ISA3000 は、イベントのトリアージと関連付けを合理化するために Cisco SecureX™ に洞察とアラートを提供し、調整されたシングルクリック防御を可能にします。

ISA3000 を使用すると、セキュアな IoT/OT インフラストラクチャを構築し、既存の IT セキュリティツールと専門知識を活用して、生産の整合性、継続性、および安全性を確保できます。

産業用ファイアウォールの導入向けの堅牢な選択肢

Cisco Secure Firewall ISA3000 は次の機能を提供します。

- 製造セルまたは工業地帯との間のトラフィック、およびそれらの間のトラフィックの制御
- 変電所および隔離された産業資産向けのセキュアな WAN 接続
- 柔軟でセキュアなエンタープライズクラスのリモートアクセス
- IP ルーティング、NAT、DNS、DHCP などの重要なネットワーク インフラストラクチャ サービス
- スイッチ、ルータ、OS、コンピューティング インフラストラクチャから、産業用のコントロールシステムにいたるまで、ネットワーキングとコンピューティングのあらゆるレベルにおける比類なき脅威からの保護
- 産業空間と企業空間の両方で、あらゆるレベルのアプリケーションを可視化および制御するための産業用プロトコルの幅広いサポート
- 産業空間における他の製品よりも高いレベルのトラフィック継続性と安全性
- IT セキュリティ証明書のコモンクライテリア

表 1.　Cisco Secure Firewall ISA3000 の一般的な機能

機能	特長
堅牢な産業用デザイン	• 過酷な環境と温度範囲（-40 ～ 70° C（-40 ～ 158° F））に耐える設計 • 振動、衝撃、サージ、電気ノイズ耐性のために強化されている。 • 4 つのギガビット イーサネット アップリンク ポートにより、複数の復元力の高い設計オプションを実現（銅線 X 4、または銅線 X 2 と光ファイバ X 2） • 多業種における産業オートメーション、高度道路交通システム（ITS）、変電所環境向けの仕様に準拠 • 産業用システムと機器の稼働時間、パフォーマンス、安全性を向上 • コンパクトな DIN レールユニット設計、および産業用 LED 機能による容易なモニタリング • 可動部をなくし耐久性を高めたファンレス対流冷却 • IEEE 1588v2 Precision Time Protocol（PTP）クロック同期（デフォルトプロファイルをサポート） • 外部機器へのモニタリングとシグナリング用のアラーム I/O。
使いやすい GUI デバイス マネージャ	• Cisco Firepower® Device Manager を使用したローカル認識と即時制御のためのオンデバイス管理 • Cisco Firepower Management Center を使用した集中管理設定、ロギング、モニタリング、およびレポート作成 • Cisco Defense Orchestrator で利用可能なクラウドベースの管理オプション • 数百台のデバイスに対応したマルチデバイス管理 • ユーザ固有アクセスと制御のカスタマイズ
トラフィックの継続性と保護	• 完全な「Lights Out」のトラフィックバイパス銅線ポート • デフォルトのパッシブ展開学習モード • トラフィック損失のないソフトウェアアップデート • DoS 攻撃からトラフィックを保護するための接続制限 • 遅延の検出および軽減機能 • QoS ポリシー

機能	特長
OT および ICS プロトコルのサポート	• BACnet • Common Industrial Protocol（CIP）（個々の CIP アプリケーションの AppID を使用可能） • Companion Specification for Energy Metering（COSEM） • Connection Oriented Transport Protocol（COTP） • 分散ネットワークプロトコル（DNP3） • イーサネット/IP • Generic Object Oriented Substation Events（GOOSE） • Generic Substation Events（GSE） • Emission Control Protocol • Fujitsu Device Control • Honeywell Control Station/NIF Server • Honeywell Esperion DSA Server Monitor • IEC 60870-5-104（個々のコマンドの AppID を使用可能） • IEC 61850 MMS（個々のコマンドの AppID を使用可能） • ISO Manufacturing Message Specification（MMS） • Modbus • Omron FINS • OPC Unified Architecture（OPC-UA） • Q.931 • Siemens S7 • SRC • TPKT

表 2. アクセス制御機能

機能	特長
実績ある拡張可能なアクセス制御	• ISA99/IEC 62443 セグメンテーションのニーズの適用 • ステートフル インスペクション（レイヤ 2 ー 7） • トランスペアレントおよびルーテッドファイアウォール動作モード • NERC-CIP 準拠の電子セキュリティ境界（ESP）を有効にする機能の提供 • 次世代侵入防御システム（NGIPS） • ID ベースのアクセス コントロール ポリシー（ユーザ、デバイス、SGT など） • VPN：リモートアクセス、サイトツーサイト
アプリケーション制御	• すべての DMZ インフラストラクチャの可視性と制御 • 産業アプリケーションの可視性と制御 • 各種プロトコルのコマンドや値の可視性と制御 • ICS/OT プロトコルの可視性と制御

機能	特長
リモートアクセスの有効化と制御	• Cisco AnyConnect® によるネットワーク アクセス コントロール • Cisco ISE のサポート • サイト間 VPN • リモートアクセス VPN • Cisco Secure Desktop • Citrix および VMware クライアントレス接続のサポート
マルチレベルアクセス制御	• グローバルブロックリスト：自動または手動 • グローバル許可リスト • サードパーティのインテリジェンスフィードの利用 • ファイル許可リスト • ファイルブロックリスト • アプリケーションレベルのアクセス制御 • 802.1X のサポート
Cisco TrustSec® の制御	• インバンドおよびアウトオブバンド ID • Active Directory の統合 • SGT に基づくポリシー • 802.1X のサポート • MACsec および MAC 認証バイパス（MAB）のサポート • リモートアクセスへのエンドポイントセキュリティ状態の適用

表 3. 侵入検知および防御機能

機能	特長
妥協のない脅威検出と防御	• Cisco Talos の研究チームが開発した業界トップのルールを活用 • 55,000 を超えるルールによって、あらゆる場所での幅広い保護を提供 • 産業用に特化した数百のルール • 産業機器のエクスプロイト保護ルール • プロトコルの悪用の識別 • Web ベースのコントロールシステムの保護 • ネットワーク動作分析 • パッシブデバイス検出
脅威のネットワークマッピング	• パッシブデバイス ID • モバイルデバイス ID • アプリケーション ホスト ネットワーク マッピング • 脆弱性/ホスト ネットワーク マッピング • ユーザ/ホスト ネットワーク マッピング

機能	特長
脅威の検出	• 侵害の兆候（IOC）のトラッキング • OpenAppID：オープンコミュニティ ID システム • 相関ポリシーと応答 • トラフィックのバリアンス検出 • ルータベースの修復アクション • NetFlow トラッキング • 55,000 以上の脅威識別子 • カスタマイズ可能な識別子 • まったく新しい識別子を作成可能 • 幅広い識別子のコントリビュータシップ
ファイルトラッキング	• 承認済みファイルのトレース • 疑わしいファイルのトレース • マルウェアの照合

表 4. ネットワーキング機能

機能	特長
DMZ インフラストラクチャ	• DNS サービス • Dynamic Host Configuration Protocol（DHCP）サービス • 認証、許可、アカウンティング（AAA）のサポート • IP ルーティング（v4 および v6）
レイヤ 3 ルーティング	• IPv4 静的ルーティング • ダイナミックルーティング（Routing Information Protocol（RIP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、およびボーダー ゲートウェイ プロトコル（BGP））
ネットワーク アドレス変換（NAT）	• スタティック NAT • ポート変換、一対多、非標準ポート • ダイナミック NAT • 動的ポート アドレス変換（PAT） • アイデンティティ NAT
レイヤ 2 IPv6	• IPv6 ホストサポート、IPv6 を介した HTTP、IPv6 を介した Simple Network Management Protocol（SNMP）
トランキング	• 802.1q トランクのサポート
ログ	• ローカルログ、syslog、Security Analytics and Logging（SAL）、eStreamer、および管理アプリケーションのログイン • 主要なセキュリティ情報イベント管理（SIEM）システム（QRadar、Splunk など）との実証済みの統合
クロック同期	• IEEE 1588（ハードウェア対応 PTP）

パフォーマンス仕様

表 5. Cisco Firepower Threat Defense（FTD）を使用したパフォーマンス

機能	パフォーマンス
スループット：**NGIPS（1024B）**	500 Mbps
スループット：ファイアウォール（**FW**）**+ Application Visibility and Control**（**AVC**）（**1024B**）	375 Mbps
スループット：**FW + AVC +** 侵入防御システム（**IPS**）（**1024B**）	350 Mbps
同時セッションの最大数（**AVC** を使用した場合）	50,000
1 秒あたりの最大新規接続数（**AVC** を使用した場合）	2700
IPSec VPN スループット（**1024B TCP**、ファストパス対応）	50 Mbps
VPN ピアの最大数	25
Application Visibility and Control（**AVC**）	4,000 以上のアプリケーションと地理位置情報、ユーザ、および Web サイトをサポートする標準
URL フィルタリング	80 以上のカテゴリ 分類済みの 2 億 8 千万以上の URL
定義済みのインターフェイス	200、400（ASA の SecPlus ライセンスを使用）、400（FTD）
VLAN 数	5、100（ASA の SecPlus ライセンスを使用）、100（FTD）
IPv4 MACsec アクセス制御エントリ（**ACE**）	デフォルトの TCAM テンプレートで 1000
NAT	適切に設計されている場合に、数万の変換済みエントリにまで拡張できる、双方向の一意のサブネット NAT エントリ（128 個）

セキュリティ機能の仕様

表 6. セキュリティ機能

機能	サポート情報
Transport Layer Security（**TLS**）の暗号解読	対応
AVC：カスタム、オープンソース、アプリケーション検出機能に対する **OpenAppID** サポート	標準
Cisco Security Intelligence	標準。IP、URL、および DNS の脅威インテリジェンス
Cisco Firepower NGIPS	使用可。エンドポイントとインフラストラクチャの脅威相関を受動的に検出し、 IoC インテリジェンスを提供
Cisco Secure Firewall（旧 **Cisco AMP for Networks**）	使用可。標的型マルウェアや執拗なマルウェアの検出、ブロッキング、追跡、分析、封じ込めを行い、連続的な攻撃に攻撃中および攻撃後のいずれのタイミングでも対応可能。また、オプションで Cisco Secure Endpoint（旧 Cisco AMP for Endpoints）による統合脅威相関

機能	サポート情報
	機能を使用可能
Cisco Secure Malware Analytics（旧 Cisco Threat Grid）サンドボックス分析	Available
自動化された脅威フィードと IPS シグネチャの更新	あり：Cisco Talos グループ（https://www.cisco.com/c/ja_jp/products/security/talos.html）により、業界トップクラスの Collective Security Intelligence（CSI）を提供
サードパーティおよびオープンソースのエコシステム	サードパーティ製品との統合を可能にするオープン API：Snort® および OpenAppID のコミュニティリソースにより新しい脅威および特定の脅威に対応
高可用性とクラスタリング	アクティブ/スタンバイ フェールオーバー
Cisco Trust Anchor テクノロジー	サプライチェーンとソフトウェア イメージ アシュアランス用の Trust Anchor テクノロジーを含む

ハードウェア仕様

表 7 に物理仕様、表 8 に安全基準と適合規格仕様、表 9 にネットワーキング規格に関する情報を示します。

表 7. 物理仕様

説明	仕様
ハードウェア	• 4 コア Intel® Atom® プロセッサ（工業用温度） • 8 GB DRAM（ハンダ付け） • 16 GB オンボード フラッシュ メモリ • mSATA 64 GB • 1 GB のリムーバブル SD フラッシュメモリカード（工業用温度） • コンソール用のミニ USB コネクタ • RJ-45 従来型コンソールコネクタ • 専用の 10/100/1000 管理ポート • ハードウェアベースの偽造/改ざん防止チップ • 工場出荷時設定オプション
アラーム I/O	• オープンまたはクローズのドライ接点を検出する 2 つのアラーム入力 • フォーム C アラーム出力リレー X 1
寸法（幅 X 高さ X 奥行）	• 11.2 X 13 X 16 cm（4.41 X 5.12 X 6.30 インチ）
重量	• 1.9 kg（4.2 ポンド）

説明	仕様
電源と範囲	• 二重内部 DC • 公称：± 12 V、24 V、または 48 V DC • 最大範囲：9.6 V ～ 60 V DC • 消費電力： 24 W
平均故障間隔（MTBF）	• ISA-3000-4C：398,130 時間 • ISA-3000-2C2F：376,580 時間

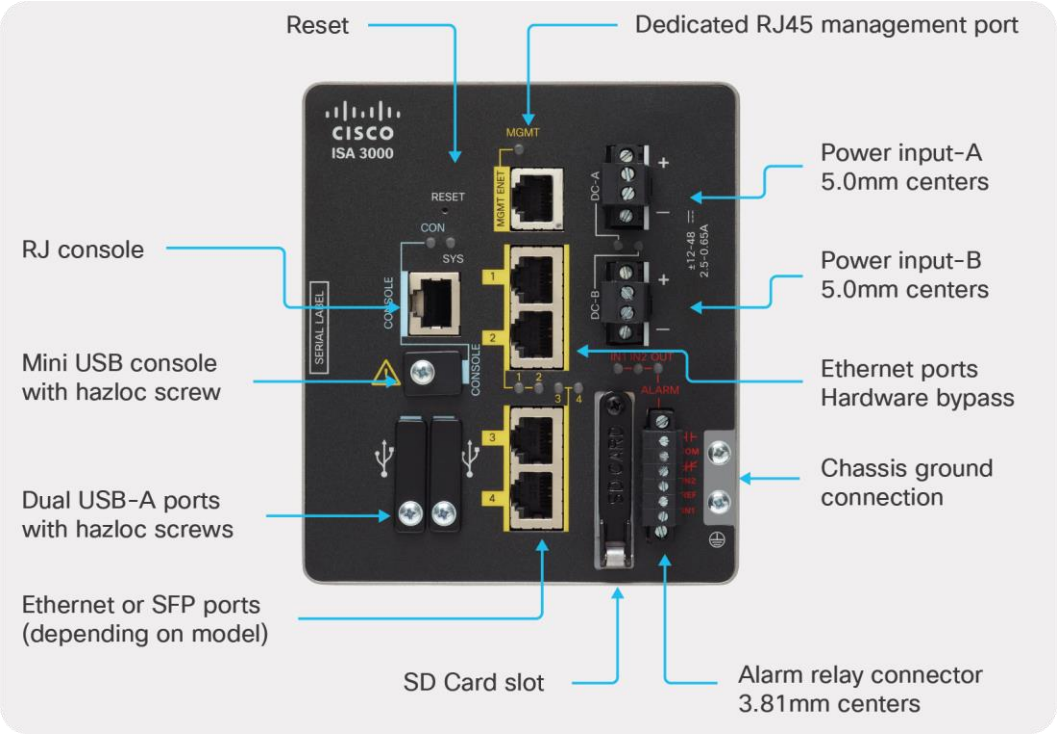

図 2.
Cisco Secure Firewall ISA3000 ポートの概要

表 8. 安全基準と適合規格仕様

タイプ	標準
電磁放射	FCC 47 CFR Part 15 クラス A EN 55022A クラス A VCCI クラス A AS/NZS CISPR 22 クラス A CISPR 11 クラス A CISPR 22 クラス A ICES 003 クラス A CNS13438 クラス A KN22
電磁イミュニティ	EN55024 CISPR 24 AS/NZS CISPR 24 KN24 EN 61000-4-2 静電放電 EN 61000-4-3 放射電磁波 EN 61000-4-4 電気的高速過渡 EN 61000-4-5 サージ EN 61000-4-6 伝導電磁波 EN 61000-4-8 電源周波数磁界 EN 61000-4-9 パルス磁界 EN 61000-4-18 減衰振動波 EN 61000-4-29 DC 電圧ディップと中断 AS/NZS 62368.1
業界規格	EN 61000-6-1 軽産業環境のイミュニティ EN 61000-6-2 産業環境のイミュニティ EN 61000-6-4 産業環境の排出基準 EN 61326 産業制御 EN 61131-2 プログラマブル コントローラ IEEE 1613 発電所コミュニケーション ネットワーキング IEC 61850-3 変電所コミュニケーション ネットワーキング NEMA TS-2 EN50121-3-2 EN 50121-4 EN 50155

タイプ	標準
安全基準と認定	情報処理機器 • UL/CSA 60950-1 • EN 60950-1 • CB（IEC 60950-1）（国別の変更事項をすべて含む） • NOM（NOM-019-SCFI、パートナーおよびディストリビュータによる） 産業フロア（制御機器）： • UL 508 • CSA C22.2、No 142 • EN/IEC 61010-2-201 • UL/CSA 61010-1 危険な場所：* • ANSI/ISA 12.12.01（クラス I、ディビジョン 2 A-D） • CSA C22.2 No 213（クラス 1、ディビジョン 2 A-D） • UL/CSA 60079-0、-15 • IEC 60079-0、-15（IECEx テスト レポート クラス I、ゾーン 2、グループ II ガス） • EN 60079-0、-15 ATEX 認定（クラス I、ゾーン 2、グループ II ガス） * Cisco ISA 3000 の製品マニュアルおよびコンプライアンスに関する情報 [英語]（https://www.cisco.com/c/dam/en/us/td/docs/security/Firewalls/ISA3000/ISA3000-PDOC.pdf）で説明されている IP54 エンクロージャなどの導入要件を満たす必要があります。
動作環境	動作温度： -40° ～ +74°C（-40° ～ +165°F） -40° ～ +70°C（-40° ～ +158°F）（開放型ラック動作時） -40° ～ +60°C（-40° ～ +140°F）（密閉型ラック動作時） -40° to +75°C (-40° to +167°F）（ファンまたはブロワー装備のラック動作時） EN 60068-2-21 EN 60068-2-2 EN 61163
保管環境	温度：-40° ～ +85°C（40° ～ +185°F） 高度：0 ～ 4572 m（0 ～ 15,000 フィート） IEC 60068-2-14
湿度	相対湿度：5 ～ 95% IEC 60068-2-30
侵入に対する保護（IP）等級	IP30

タイプ	標準
衝撃および振動	IEC60068-2-6 および IEC60068-2-27 MIL-STD-810、Method 514.4 船舶 EN60945 産業 EN61131-2/IEC61131-2 鉄道 EN61373 CAT 1B スマート グリッド EN61850-3 IEEE 1613
腐食	ISO 9223：腐食 クラス C3-Medium クラス C4-High EN 60068-2-52（塩水噴霧） EN 60068-2-60（混合ガス流）
その他	RoHS 準拠 中国 RoHS 準拠 TAA（政府） CE（ヨーロッパ） Regulatory Compliance Mark（RCM）
保証	すべての ISA3000 製品 ID に対する 5 年間のハードウェア限定保証 保証の詳細については、データシートの最後にあるリンクを参照してください。

表 9. ネットワーク標準規格

説明	仕様	
IEEE 標準規格	• IEEE 802.1D MAC ブリッジ、スパニングツリープロトコル（STP） • IEEE 802.1p Layer2 サービスクラス（CoS）優先順位付け • IEEE 802.1q VLAN • IEEE 802.1s 多重スパニングツリー • IEEE 802.1w 高速スパニングツリー • IEEE 802.1x ポート アクセス認証 • IEEE 802.1AB Link Layer Discovery Protocol（LLDP） • IEEE 802.3ad Link Aggregation Control Protocol（LACP）	• IEEE 802.3ah 100BASE-X シングルモードファイバ（SMF）/マルチモードファイバ（MMF）のみ • IEEE 802.3x 10BASE-T での全二重 • IEEE 802.3 10BASE-T 仕様 • IEEE 802.3u 100BASE-TX 仕様 • IEEE 802.3ab 1000BASE-T 仕様 • IEEE 802.3z 1000BASE-X 仕様 • IEEE 1588v2 PTP

説明	仕様	
RFC 準拠	• RFC 768：User Datagram Protocol（UDP） • RFC 783：Trivial FTP（TFTP） • RFC 791：IPv4 • RFC 792：Internet Control Message Protocol（ICMP） • RFC 793：TCP • RFC 826：Address Resolution Protocol（ARP） • RFC 854：Telnet • RFC 951：BOOTP • RFC 959：FTP • RFC 1157：SNMPv1 • RFC 1901、1902 ～ 1907：SNMPv2 • RFC 2273 ～ 2275：SNMPv3 • RFC 2571：SNMP 管理 • RFC 1166：IP アドレス • RFC 1256：ICMP ルータ ディスカバリ	• RFC 1305：NTP • RFC 1492：TACACS+ • RFC 1493：ブリッジ MIB オブジェクト • RFC 1534：DHCP および BOOTP 相互運用 • RFC 1542：ブートストラップ プロトコル • RFC 1643：イーサネット インターフェイス MIB • RFC 1757：RMON • RFC 2068：HTTP • RFC 2131、2132：DHCP • RFC 2236：IGMP v2 • RFC 3376：IGMP v3 • RFC 2474：DiffServ による優先制御 • RFC 3046：DHCP リレーエージェント情報オプション • RFC 3580：802.1X RADIUS • RFC 4250 ～ 4252：SSH プロトコル

発注情報

表 10 および表 11 に使用可能な ISA3000 製品 ID、表 12 に SFP モジュール、表 13 に ISA3000 で使用可能な電源を示します。

表 10. Cisco Secure Firewall ISA3000 モデル

製品番号	銅線 10/100/1000（すべてバイパス対応）	SFP 光ファイバポート
ISA-3000-2C2F-K9	2	2
ISA-3000-4C-K9	4	0

表 11. オプションで発注可能な機能

製品番号	機能
オプションで発注可能な機能（ASA + FP）	
L-ISA3000SEC+-K9	Security Plus：HA 対応、SSL VPN、接続数の追加、VLAN トランキング
脅威/アプリケーション サブスクリプション ライセンス	
L-ISA3000-TA-1Y	1 年間のサブスクリプション（脅威/アプリケーション）
L-ISA3000-TA-3Y	3 年間のサブスクリプション（脅威/アプリケーション）
L-ISA3000-TA-5Y	5 年間のサブスクリプション（脅威/アプリケーション）

製品番号	機能
Threat Defense Malware Protection ライセンス	
L-ISA3000-AMP-1Y	1 年間のサブスクリプション（Threat Defense Malware Protection）
L-ISA3000-AMP-3Y	3 年間のサブスクリプション（Threat Defense Malware Protection）
L-ISA3000-AMP-5Y	5 年間のサブスクリプション（Threat Defense Malware Protection）
Threat Defense URL フィルタリングライセンス	
L-ISA3000-URL-1Y	1 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
L-ISA3000-URL-3Y	3 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
L-ISA3000-URL-5Y	5 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
Threat Defense Threat および URL フィルタリングライセンス	
L-ISA3000-TC-1Y	1 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
L-ISA3000-TC-3Y	3 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
L-ISA3000-TC-5Y	5 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
Threat Defense Threat および Malware Protection ライセンス	
L-ISA3000-TM-1Y	1 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
L-ISA3000-TM-3Y	3 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
L-ISA3000-TM-5Y	5 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
Threat Defense Threat、Malware Protection、および URL フィルタリングライセンス	
L-ISA3000-TMC-1Y	1 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）
L-ISA3000-TMC-3Y	3 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）
L-ISA3000-TMC-5Y	5 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）
オプションで発注可能な機能（FTD）	
脅威/アプリケーション サブスクリプション ライセンス	
L-ISA3000T-T-1Y	1 年間のサブスクリプション（脅威/アプリケーション）
L-ISA3000T-T-3Y	3 年間のサブスクリプション（脅威/アプリケーション）
L-ISA3000T-T-5Y	5 年間のサブスクリプション（脅威/アプリケーション）

製品番号	機能
Threat Defense Malware Protection ライセンス	
L-ISA3000T-AMP-1Y	1 年間のサブスクリプション（Threat Defense Malware Protection）
L-ISA3000T-AMP-3Y	3 年間のサブスクリプション（Threat Defense Malware Protection）
L-ISA3000T-AMP-5Y	5 年間のサブスクリプション（Threat Defense Malware Protection）
Threat Defense URL フィルタリングライセンス	
L-ISA3000T-URL-1Y	1 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
L-ISA3000T-URL-3Y	3 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
L-ISA3000T-URL-5Y	5 年間のサブスクリプション（Threat Defense URL フィルタリングライセンス）
Threat Defense Threat および URL フィルタリングライセンス	
L-ISA3000T-TC-1Y	1 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
L-ISA3000T-TC-3Y	3 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
L-ISA3000T-TC-5Y	5 年間のサブスクリプション（Threat Defense Threat および URL フィルタリングライセンス）
Threat Defense Threat および Malware Protection ライセンス	
L-ISA3000T-TM-1Y	1 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
L-ISA3000T-TM-3Y	3 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
L-ISA3000T-TM-5Y	5 年間のサブスクリプション（Threat Defense Threat および Malware Protection ライセンス）
Threat Defense Threat、Malware Protection、および URL フィルタリングライセンス	
L-ISA3000T-TMC-1Y	1 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）
L-ISA3000T-TMC-3Y	3 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）
L-ISA3000T-TMC-5Y	5 年間のサブスクリプション（Threat Defense Threat、Malware Protection、および URL ライセンス）

表 12.　サポートされるシスコの高耐久性 SFP*

製品番号	タイプ
GLC-SX-MM-RGD=	高耐久性 1000 BASE-SX
GLC-LX-SM-RGD=	高耐久性 1000 BASE-LX/LH
GLC-FE-100FX-RGD=	高耐久性 100 BASE-FX
GLC-FE-100LX-RGD=	高耐久性 100 BASE-LX

*サポートされているすべての SFP モジュールの一覧については、https://www.cisco.com/c/ja_jp/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html を参照してください。

MM = マルチモード光ファイバ

SM = シングルモード光ファイバ

表 13.　推奨電源

製品番号	詳細
PWR-IE50W-AC-IEC	AC ～ DC 24 V/2.1 A DIN レール電源、入力 100 ～ 240 V AC/1.25 A 50 ～ 60Hz、出力 24 V DC/2.1 A、IEC プラグ
PWR-IE50W-AC	AC ～ DC 24 V/2.1 A DIN レール電源、入力 100 ～ 240 V AC/1.25 A または 125 ～ 250 V DC/1 A、出力 24 V DC

保証情報

保証情報については、https://www.cisco-servicefinder.com/warrantyfinder.aspx から入手できます。

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを次の表に示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

シスコおよびパートナーの提供サービス

シスコでは、お客様の TCO を最小限に抑えることに全力を注いでおり、お客様の成功を促進する幅広いサービスプログラムを提供しています。当社の革新的なプログラムは、スタッフ、プロセス、ツール、パートナーをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。シスコ 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。お客様がシスコ サービスから得られる主な利点を次に示します。

- プロアクティブまたは迅速な問題解決を可能にすることでリスクを軽減します。
- シスコの専門知識とノウハウを駆使し、TCO（総所有コスト）を削減します。
- ネットワークのダウンタイムを最小化します。
- 既存のサポートスタッフの労力を軽減し、他の生産性の高い活動に集中できるようにします。

シスコサービスに関する詳細については、シスコ テクニカル サポート サービスまたはシスコアドバンスドサービス（https://www.cisco.com/web/services/）を参照してください。

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。

詳細情報

Cisco Secure Firewall ISA3000 の詳細については、https://www.cisco.com/jp/go/isa3000 を参照するか、地域のアカウント担当者にお問い合わせください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明	日付
新しい OS バージョン関連の更新		2020 年 1 月 20 日
新しい使用可能なライセンス	表 10 および表 11	2020 年 1 月 20 日
機能リストの再編成		2021 年 2 月 6 日
パフォーマンスデータを更新	表 5	2021 年 4 月 8 日
製品名を更新		2021 年 4 月 8 日

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

C78-735839-06JA 21.06