ISR G2 プラットフォーム向けのネットワーク セキュリティ機能

このデータ シートでは、Cisco 1900、2900、3900 シリーズ サービス統合型ルータを含む、シスコ® 第 2 世代サービス統合型ルータ（ISR G2）プラットフォームで利用できるネットワーク セキュリティ機能の概要を説明します。

製品概要

業界で最も包括的なセキュリティ サービスとともに提供されるシスコのサービス統合型ルータ。そのプラットフォーム ポートフォリオには、データ、セキュリティ、音声、ワイヤレス機能がインテリジェントに組み込まれており、ミッションクリティカルなアプリケーションを迅速かつスケーラブルに提供します。

Cisco 1900、2900、3900 シリーズ サービス統合型ルータは、ルーティング性能と IPSec VPN、さらに、従来のサービス統合型ルータの最大 5 倍に達するファイアウォール アクセラレーションを装備し、小規模企業やブランチ オフィスに最適です（図 1）。このルータは、リモート オフィス、テレワーカー、モバイル ユーザ、そしてパートナーのエクストラネットやサービス プロバイダーの管理する顧客宅内機器（CPE）を接続する、豊富で統合されたソリューションを提供します。

統合型ルータ セキュリティ ソリューションは、実績のある Cisco IOS® ソフトウェアの機能と、世界水準のネットワーク セキュリティ機能を備えた業界最先端の LAN および WAN 接続を組み合わせたソリューションであり、既存のネットワーク設計と運用面のベスト プラクティスの利点を生かしながら、最新のブランチオフィス のサービス要件を満たすコスト効率の高いアプローチを提供します。

究極のエクスペリエンス

ブランチ オフィス エクスペリエンスを高めると同時に、ネットワークをあらゆる脅威から保護します。

- 前世代のルータに比べパフォーマンスが**最大 5 倍向上**
- **セキュアなコラボレーションおよびビデオ ネットワーク**：高度な VPN および Cisco IOS ファイアウォール機能によって、セキュアで高品質な音声とビデオを提供すると同時に、通話の盗聴や通話料金詐欺、サービス不能（DoS）から保護します。
- 802.11n ワイヤレス統合による**セキュアなモビリティ**

ボーダレスなサービス

ボーダレスなサービスによって、既存のインフラストラクチャを使用しながらブランチオフィスの接続をセキュアに保つことができます。追加ハードウェアを導入することなく、既存のネットワーク インフラストラクチャを活用して、リモート サイトにおけるセキュリティ上の脅威の管理および WAN 帯域幅の節約を実現します。また、ファイアウォール、侵入防御システム（IPS）、コンテンツ フィルタリング、VPN などのセキュリティ機能をネットワーク内のどこにでも柔軟に適用し、セキュリティ上の利点を最大化することができます。最新の機能には次のようなものがあります。

- **セキュアなクラウド コンピューティング サービス**：Group Encrypted Transport VPN によってコンプライアンスに準拠するとともに、特に転送中データの観点からセキュアなクラウド コンピューティングを実現します。
- **セキュアな統合モバイル アーキテクチャ**：このアーキテクチャは、シスコのセキュリティ、VPN、および public-key-infrastructure（PKI; 公開鍵インフラストラクチャ）のテクノロジーをモバイル

サービスのプロビジョニング、展開、および管理に利用することで、スマート フォン向けのオープン フレームワークを提供します。音声、ローミング、Wi-Fi、電子メールなど、多様なサービスのためのセキュアなモバイル インフラストラクチャを提供します。

- **サービスとしての Cisco Virtual Office**:このサービスにより、災害やパンデミック時におけるビジネスの耐障害性を維持することができ、最新のセキュアなテレワーキングが実現します。

総所有コスト(TCO)

ルータベースのネットワーク セキュリティ ソリューションは、デバイス数、およびトレーニングや管理性、電力、サービス契約に関するコストを低減することにより、資本コスト(CapEx)と運用コスト(OpEx)の両方を削減します。また、セキュリティ バンドルによって、ルータとセキュリティ機能を個別に購入した際に比べ大幅に費用を節約できます。

- **ワンタッチ PSIRT 更新**:このルータベースのソリューションは、Cisco.com から Product Security Incident Response Team(PSIRT)レスポンスを自動的にダウンロードできます。また更新のオプションとして、PSIRT の推奨対策を実行することもできます。
- **高度なインスツルメンテーション**: ルータベースの高度なインスツルメンテーション機能によって、有効化されたデバイス、ネットワーク、サービスに対し、プロビジョニング、モニタリング、保守、ネットワーク パフォーマンス評価、データ収集と評価、トラブルシューティングを行うことができます。
- **より強固なセキュリティ基盤**:ネットワーク内のルータとあらゆるエントリ ポイントを、ハッキングや Distributed DoS(DDoS; 分散型サービス不能)などの攻撃から保護します。

図 1 Cisco 1900、2900、3900 シリーズ サービス統合型ルータ ポートフォリオ

Cisco 1900、2900、3900 シリーズ サービス統合型ルータのセキュリティ機能と利点

Cisco IOS ソフトウェア リリース 15.0 は、新たに改善されたソフトウェア パッケージです。Cisco 1900、2900、3900 シリーズ サービス統合型ルータに単一のユニバーサル イメージが付属し、これまで 8 つの異なるソフトウェア イメージで提供されていたいくつかのフィーチャ セットの全ソフトウェア機能が、この単一のイメージに含まれます。

3 つの Cisco IOS テクノロジー パッケージ ライセンス(セキュリティ、ユニファイド コミュニケーション、データ)が基本イメージへのアドオンとして利用できます。たとえば、セキュリティ テクノロジー パッケージを有効にする際は、新しいライセンス キーを購入して有効化します。このキーによってセキュリティ機能のロックが即時に解除されるため、更新をダウンロードしたりリモート オフィスの機器を更新したりする必要はなくなります。

セキュリティ テクノロジー パッケージ ライセンスを含むシスコの ISR G2 向けセキュリティ バンドルをご注文されることを推奨します。

セキュリティ テクノロジー パッケージ ライセンスのほか、ソフトウェア アクティベーション機能ライセンスおよびサブスクリプション ライセンスが必要な機能もあります。これには Cisco IOS Secure Sockets Layer（SSL）VPN、Cisco IOS 侵入防御システム（IPS）、Cisco IOS コンテンツ フィルタリングが含まれます。

表1 に機能と、Cisco 1900、2900、3900 シリーズ サービス統合型ルータで各機能を使用するために必要な機能ライセンスを示します。

表 1 Cisco 1900、2900、3900 シリーズ サービス統合型ルータのセキュリティ ライセンス要件

機能	必要なライセンス
認証、許可、アカウンティング（AAA）、NetFlow、Network-Based Application Recognition（NBAR）、アクセス コントロール リスト（ACL）、Cisco IOS Flexible Packet Matching（FPM）、802.1x、Cisco IOS Network Foundation Protection	なし（基本イメージで利用可能）
標準 IP セキュリティ（IPSec）、Group Encrypted Transport VPN、ダイナミック マルチポイント VPN（DMVPN）、Easy VPN、Enhanced Easy VPN、仮想トンネル インターフェイス（VTI）、Multi-Virtual Route Forwarding（VRF）カスタマー エッジ（CE）（IPSec、ファイアウォール、IPS）、IPSec ハイ アベイラビリティ、Cisco IOS Zone-Based Firewall、高度なアプリケーション インスペクションおよび制御、セキュアなユニファイド コミュニケーション向けファイアウォール、VRF 対応ファイアウォール、ファイアウォール ハイ アベイラビリティ、トランスペアレント ファイアウォール、Cisco IOS IPS、トランスペアレント IPS、VRF 対応 IPS、セキュア プロビジョニングおよびデジタル証明書、Cisco IOS 証明書サーバおよびクライアント	セキュリティ テクノロジー パッケージ ライセンス
Cisco IOS SSL VPN	セキュリティ テクノロジー パッケージ ライセンス + SSLVPN 機能ライセンス
Cisco IOS コンテンツ フィルタリング	セキュリティ テクノロジー パッケージ ライセンス + コンテンツ フィルタリング サブスクリプション ライセンス
Cisco IOS IPS サブスクリプション サービス	セキュリティ テクノロジー パッケージ ライセンス + IPS サービス

ライセンスの購入についての詳細は、「発注情報」のセクションを参照してください。

表 2 に、Cisco 1900、2900、3900 シリーズ サービス統合型ルータに組み込まれているセキュリティ機能と利点を示します。これらの機能の詳細については、http://www.cisco.com/go/isrG2/ [英語] の詳細なネットワーク セキュリティ機能データ シートを参照してください。

表 2 Cisco 1900、2900、3900 シリーズ サービス統合型ルータに組み込まれている主なセキュリティ機能と利点

機能	説明と利点
セキュアな接続	
標準 IPSec	対応している IPSec 規格は、暗号化に Digital Encryption Standard（DES）、Triple DES（3DES）、Advanced Encryption Standard（AES 128、192、256）、認証に Rivest、Shamir、Aldeman（RSA）アルゴリズム シグニチャ、Diffie-Hellman、データ整合性に Secure Hash Algorithm 1（SHA-1）または Message Digest Algorithm 5（MD5）ハッシング アルゴリズムを含みます。
Group Encrypted Transport VPN	Group Encrypted Transport VPN により、プライベート WAN 環境において、データ プライバシーのためにネットワーク インテリジェンスを犠牲にする必要がなくなります。Group Encrypted Transport VPN は VPN のプロビジョニングと管理を簡略化するので、サービス プロバイダーはプロビジョニングと管理の問題に直面することなく、管理された暗号化を提供することができます。Group Encrypted Transport VPN は、トンネルを使用しない VPN という新しいカテゴリです。
DMVPN	これはサイト間 VPN におけるシスコの革新技術で、複数の場所の間で仮想フルメッシュ型の IPSec 接続を確立するスケーラブルで柔軟な方法を提供します。遅延が許容されない音声アプリケーションのパフォーマンスを向上する高度なスポーク間の機能を備えています。従来のハブアンドスポーク モデルに対し、導入の複雑さを大幅に軽減します。

機能	説明と利点
Easy VPN および Enhanced Easy VPN	IPSec 規格に高度な付加価値を提供するこれらの機能は、中央ヘッドエンド ルータからリモート サイトに新しいセキュリテイ ポリシーを積極的にプッシュすることで、ポイントツーポイント VPN の管理と制御を容易にします。Enhanced Easy VPN 機能はダイナミック VTI と統合して、最大限の使いやすさとユーザ単位およびトンネル別の高度な機能を実現します。
Cisco IOS SSL VPN	Cisco IOS SSL VPN は Web ブラウザとネイティブ SSL 暗号化のみを使用し、リモートユーザが公衆インターネットを介して企業リソースにセキュアにアクセスできるようにします。
VTI	さまざまな仮想インターフェイスを、IPSec で直接構成することができます。VTI は、総称ルーティング カプセル化（GRE）内で IPSec をカプセル化するなどの代替手段より、大幅に VPN 構成と設計を簡略化します。ユーザ単位の属性およびトンネル別機能が可能になるため、管理者は細かい要求に対応する柔軟性を得ることが出来ます。スタティックとダイナミックの両方の VTI がサポートされています。
マルチ VRF および Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）セキュア コンテキスト	ブランチ オフィスで部門、関連会社、顧客を分離するための複数の独立したコンテキスト（アドレス指定、ルーティング、インターフェイス）をサポートします。すべてのコンテキストが 1 つのコアへのアップリンク接続（たとえば IPSec VPN、Frame Relay、または ATM）を共有しながら、相互間のセキュアな分離性を維持します。
IPSec ハイ アベイラビリティ	IPSec ステートフル フェールオーバーおよび Reverse Route Injection（RRI; 逆ルート注入）での Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）などのオプションにより、Cisco VPN は冗長性およびロード バランシングの導入における数々の機能をサポートします。
統合型脅威コントロール	
Cisco IOS ファイアウォール	ネットワークへの WAN エントリ ポイントを保護するセキュリティとルーティングの理想的な単一デバイス ソリューションです。重要な機能には、ゾーンベースのポリシー、HTTP および電子メールに対する高度なアプリケーション インスペクションおよび制御、セキュアなユニファイド コミュニケーション向けファイアウォール、VRF 対応ファイアウォール、ファイアウォール ハイ アベイラビリティが含まれます。
Cisco IOS IPS	ネットワーク攻撃を効果的に軽減する、詳細なパケット検査ベースのインライン ソリューションを提供します。トラフィックをドロップし、アラームを送信したり、ローカルで接続を回避またはリセットすることができ、セキュリティ上の脅威にルータが即時に対応してネットワークを保護します。重要な機能には、インライン機能（パケットをドロップ可能）、既成の「ありがちな」シグニチャ ファイル パッケージ、Cisco Security Intelligence Operation（SIO）全世界ウィルス検出、カスタマイズ可能なシグニチャ、トランスペアレント IPS、VRF 対応 IPS が含まれます。
Cisco IOS コンテンツ フィルタリング	中小企業（SMB）および中堅企業向けにカテゴリベースの生産性およびセキュリティ評価を提供します。コンテンツに対応したセキュリティ評価で、マルウェア、悪意のあるコード、フィッシング攻撃、スパイウェアから保護します。URL およびキーワード ブロックにより、従業員がインターネットにアクセスしているときの生産性を確約します。このサブスクリプションベースでホストされたソリューションは、クラウド内脅威データベースを活用でき、Cisco IOS ソフトウェアと密接に統合されています。
NetFlow	DDoS 攻撃の変則性に基づいて検出を行い、攻撃元の追跡および攻撃に対するリアルタイムでの対応に役立つデータを提供します。
NBAR	この詳細な検査メカニズムによって、多様なアプリケーションの認識と分類ができ、それらに対するコントロールが可能になります。アプリケーションが分類された後、ネットワークはそのアプリケーションに対して特定のサービスを提供できます。
FPM	パケット ヘッダやペイロード内の深部にまで柔軟で詳細なレイヤ 2 ～ 7 のパターン照合を行い、ネットワーク上の脅威および注意が必要なワームやウィルスに対する迅速な第一線の防御を提供します。
信頼性とアイデンティティ	
PKI クライアント（x.509 デジタル証明書）	Cisco IOS ソフトウェアは、暗号化およびアイデンティティ情報の配布、管理、廃止に対し、スケーラブルでセキュアなメカニズムを提供する組み込み型 PKI クライアント機能をサポートします。高度なプロビジョニング機能を使用した強力なメカニズムによって、新規リモート ノードが最大限のセキュリティを装備したネットワーク インフラストラクチャに自動的に登録されます。
Cisco IOS 証明書サーバ	Cisco IOS ソフトウェアは、スケーラブルで管理が容易な組み込み型の証明書サーバを含んでおり、これによってルータはネットワーク上での認証権限者として機能します。
標準 802.1x ベースのアイデンティティ サービス	標準 802.1x アプリケーションは有効なアクセス認定証を必要とするため、保護された情報リソースに対する不正アクセスおよびセキュアでないワイヤレス アクセス ポイントの展開がより困難となります。
AAA	管理者は AAA を利用し、認証の種類およびライン単位（ユーザ単位）またはサービス単位（たとえば IP、Internetwork Packet Exchange [IPX] またはバーチャル プライベート ダイヤルアップ ネットワーク [VPDN]）で必要な許可をダイナミックに構成することができます。
シスコ ネットワーク基盤の保護	
AutoSecure	AutoSecure が提供する単一のコマンドライン インターフェイス（CLI）コマンドを使って、ルータのセキュリティ ポスチャを瞬時に設定し、また、必須ではないシステムのプロセスとサービスを無効にできます。これによって、潜在的なセキュリティの脅威を解消します。

機能	説明と利点
コントロール プレーン ポリシングおよび保護	DoS 攻撃を含む不要なまたは悪意あるレベルのトラフィックから、ルート プロセッサを保護します。
CPU およびメモリしきい値の通知	特定の処理について、指定された CPU リソース利用率を超過した場合、または一定の時間特定のしきい値を下回ったときに syslog 通知を送信します。
ルーティング保護	MD5 ピア認証と再配布保護を利用して、ルーティング ピアを検証し、ルーティングの安定性を高め、過負荷に対する保護を提供します。
ACL 保護	ルータ宛先アドレスに送信できる正規のトラフィックを制限することにより、悪意のあるトラフィックからルータを保護します。
セキュア アクセス モード（サイレント モード）	ルータのコントロール プレーンからの応答メッセージを抑止し、ハッカーが利用できるネットワークの偵察情報を制限します。
Raw IP トラフィック エクスポート	LAN インターフェイスからインバウンド パケットおよびアウトバウンド パケットのコピーを送信することで、分析ツールまたは侵入検知システム（IDS）ツールによってパケットを効率的にキャプチャすることができます。
発信元ベースの Remote-Triggered Black Holing（RTBH）フィルタリング	IP ルーティング機能の組み合わせを利用し、DDoS 攻撃に対するワイヤ レート、リアルタイムの防御を提供します。
Unicast Reverse Path Forwarding（uRPF）	uRPF は検証可能な IP 送信元アドレスを持たない IP パケットを廃棄することで、ネットワークへの不正またはなりすまし IP 送信元アドレスの侵入によって起こる問題を軽減します。
デジタル イメージ署名	ダウンロードされたすべての Cisco IOS ソフトウェア イメージの真正性を確約する SHA-512 ハッシングと RSA 2048 ビット キー暗号化メカニズムを提供します。
Cisco IOS ソフトウェア ログイン拡張機能	潜在的な辞書攻撃を遅らせ、不正なデバイス アクセスを阻止する方法を提供します。
ロールベース CLI アクセス	ビューベースでの CLI コマンドへのアクセスが可能で、ネットワーク操作、セキュリティ操作、およびエンド ユーザ間で、ルータを非常にセキュアかつ論理的に分離できます。
Secure Shell（SSH）プロトコル バージョン 2	SSHv2 はリモート ネットワーク管理向けに SSH の旧バージョンを強化し、パスワード長を隠すことで辞書攻撃をより困難にします。ユーザ認証中の中間者（man-in-the-middle）攻撃に対する SSHv1 の脆弱性を解決しています。
SNMP（簡易ネットワーク管理プロトコル）バージョン 3	SNMPv3 は、カスタマー アプリケーション向けデバイスの標準ベースのセキュアな管理とコントロールを提供します。

USB ポートおよびリムーバブル認定証

Cisco 1900、2900、3900 シリーズ サービス統合型ルータはオンボード USB 1.1 ポートを搭載した設計で、重要なセキュリティおよびストレージ機能を実現します。この機能により、セキュアなユーザ認証、セキュアな VPN 接続確立のためのリムーバブル認定証の格納、構成ファイルのセキュアな配布、そしてファイルおよび構成用のバルク フラッシュ メモリ ストレージの提供をサポートします。

USB ポートを利用することで、USB eToken でセキュアに構成の配布ができ、導入用の VPN 認定証を格納できます。また、USB フラッシュ メモリにイメージおよび構成を格納することができます。

シスコの侵入防御システム ネットワーク モジュール

Cisco 1900、2900、3900 シリーズ サービス統合型ルータ内で、シスコの侵入防御システム ネットワーク モジュール（IPS NME）を導入することができます。これは、ブランチ オフィスや小規模企業におけるハードウェアベースの侵入防御です。セキュリティ上の脅威の複雑化と高度化によって、ネットワークの各ポイントはリスクにさらされる危険性があります。Cisco IPS はワーム、スパイウェア、マルウェア、アドウェア、ネットワーク ウィルス、アプリケーション不正使用などを含む、悪意のあるトラフィックを正確に識別、分類、および阻止します。この隙のない防御によってビジネスの継続性を実現し、侵入の悪影響を最小限に抑えます。Cisco IPS NME は、Cisco IPS センサー ソフトウェアを実行して最大 75 Mbps のトラフィックを監視でき、複数の T1/E1 および T3 環境に適しています。Cisco IPS NME は多様な Cisco IOS ソフトウェア セキュリティ機能を組み込んでいます。

Cisco IPS NME の詳細については、http://www.cisco.com/en/US/products/ps8395/index.html [英語] を参照してください。

Cisco NAC ネットワーク モジュール

Cisco Network Access Control（NAC）ネットワーク モジュールを使用することにより、Cisco 2900 および 3900 シリーズ サービス統合型ルータに豊富な機能を持つ Cisco NAC アプライアンス サーバ機能を追加できます。Cisco NAC アプライアンス（旧称 Cisco Clean Access Server）は迅速に導入可能な NAC 製品で、ネットワーク管理者は有線、無線、リモートのユーザ、およびそのマシンを認証、許可、評価、修復してから、ネットワークへのログオンを許可することができます。

サービス統合型ルータのネットワーク モジュールに Cisco NAC アプライアンス サーバ機能を組み込むことによって、ネットワーク管理者はブランチ オフィスの 1 台のデバイスで、データ、音声、セキュリティ要件の管理を行うことができ、ネットワークの複雑性、IT スタッフのトレーニング、機器の設置空間、保守費用を低減することができます。

Cisco NAC ネットワーク モジュールの詳細については、
http://www.cisco.com/web/JP/product/hs/ifmodule/cnm/nacnm/index.html を参照してください。

セキュリティ管理

Cisco Configuration Professional

Cisco Configuration Professional は、中堅企業および大企業のブランチ オフィスでルータを導入しているネットワーク管理者およびチャネル パートナー向けの、重要な生産性向上ツールです。このアプリケーションを使用すると、少ないコストで確実かつ容易にルータ、ユニファイド コミュニケーション、セキュリティ、および無線ネットワークを実装できます。Cisco Configuration Professional の設定は、Cisco Technical Assistance Center（TAC）においてその内容が確認されたものです。また、Cisco Configuration Professional を使用することで、ルータのパフォーマンス統計情報、システム ログ、およびセキュリティ ログをリアルタイムでプロアクティブに監視し、ネットワークの潜在的な問題を回避することもできます。

Cisco Configuration Professional にはスマート ウィザードが用意されており、シスコの LAN および WAN インターフェイス、Network Address Translation（NAT; ネットワーク アドレス変換）、ステートフルなアプリケーション ファイアウォール ポリシー、IPS、IPSec VPN、QoS、および NAC ポリシー機能の詳細設定がサポートされます。このアプリケーションは、ネットワーキングのテクノロジーと用語を理解していることを前提としていますが、Cisco CLI に慣れていないユーザもサポートします。

シスコのセキュリティ管理スイート

シスコのセキュリティ管理スイートは、シスコの自己防衛型ネットワークに対するスケーラブルなポリシー管理と適用のために設計された製品群およびテクノロジーのフレームワークです。この統合型ソリューションによって、構成、監視、分析、応答などのセキュリティ管理操作に関連するタスクを簡略化および自動化できます。このソリューションの主要なコンポーネントは次のようになります。

- **Cisco Security MARS（Cisco Security Monitoring, Analysis, and Response System）**：これはネットワークおよびセキュリティ管理者がセキュリティの脅威を監視、識別、排除して、その攻撃に対応できるようにするアプライアンスベースのソリューションです。
- **Cisco Security Manager**：このエンタープライズクラスの管理アプリケーションは、シスコのネットワークおよびセキュリティ デバイスに、ファイアウォール、VPN および侵入防御システム（IPS）のセキュリティ サービスを構成するために設計されています。このアプリケーションはポリシーベースの管理技術を使用して、小規模ネットワークから数千のデバイスで構成される大規模な

ネットワークまで、さまざまな規模のネットワークで使用できます。Cisco Security Manager リリース 3.3.1 は、Cisco 1900、2900、3900 シリーズ サービス統合型ルータに対応しています。

これらのアプリケーションは統合されることで、脅威の発生に対し、ネットワークのセキュリティを継続的に監視および改善する強力な機能を提供します。

認定

シスコは、世界中のお客様に対する積極的な製品セキュリティ認定および評価プログラムの維持に取り組んでいます。シスコは、このような検証が統合型セキュリティ戦略の重要コンポーネントであると認識しており、連邦情報処理標準（FIPS）および Common Criteria への準拠を推し進めています。

詳細については、http://www.cisco.com/go/securitycert [英語] を参照してください。

発注情報

シスコ製品の購入方法の詳細は、「購入案内」を参照してください。

セキュリティ バンドルはセキュリティ テクノロジー パッケージ ライセンスを含んでおり、後でセキュリティを追加するより低価格なため、ROI が大幅に向上します。Cisco 1900、2900、3900 シリーズ サービス統合型ルータ セキュリティ バンドルの総合一覧は http://www.cisco.com/go/securitybundles [英語] を参照してください。

セキュリティ テクノロジー パッケージ ライセンスは、セキュリティ バンドルの一部でないルータのアップグレードに必要です。書面ライセンスは郵送で届けられます（書面形式）。電子配布（eDelivery）ライセンスは電子メールで即時に送付されます。表 3 に、セキュリティ テクノロジー パッケージ ライセンス製品番号の一覧を示します。

表 3 Cisco 1900、2900、3900 シリーズ サービス統合型ルータ向けセキュリティ テクノロジー パッケージ ライセンス製品番号

ライセンス	説明
SL-19-SEC-K9(=)	Cisco 1941 用セキュリティ ライセンス（書面）
SL-29-SEC-K9(=)	Cisco 2901-2951 用セキュリティ ライセンス（書面）
SL-39-SEC-K9(=)	Cisco 3925/3945 用セキュリティ ライセンス（書面）
L-SL-19-SEC-K9=	Cisco 1941 用セキュリティ ライセンス（電子配布）
L-SL-29-SEC-K9=	Cisco 2901-2951 用セキュリティ ライセンス（電子配布）
L-SL-39-SEC-K9=	Cisco 3925/3945 用セキュリティ ライセンス（電子配布）

さらに、機能ライセンスおよびサブスクリプション ライセンスが必要な機能もあります。表 4 ～ 5 に、利用可能な製品番号を示します。

表 4 Cisco 1900、2900、3900 シリーズ サービス統合型ルータ向け SSL VPN 機能ライセンス製品番号

ライセンス	説明
FL-SSLVPN10-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（書面）– 10 クライアントレス ユーザ
FL-SSLVPN25-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（書面）– 25 クライアントレス ユーザ
FL-SSLVPN100-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（書面）– 100 クライアントレス ユーザ
L-FL-SSLVPN10-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（電子配布）– 10 クライアントレス ユーザ
L-FL-SSLVPN25-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（電子配布）– 25 クライアントレス ユーザ
L-FL-SSLVPN100-K9(=)	Cisco SSLVPN クライアントレス機能ライセンス PAK（電子配布）– 100 クライアントレス ユーザ

表 5 Cisco 1900、2900、3900 シリーズ サービス統合型ルータ向けコンテンツ フィルタリング サブスクリプション ライセンス製品番号

ライセンス	説明
FL-19-CNFIL-1Y(=)	Cisco 1941 ～ 1941W 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（書面）
FL-29-CNFIL-1Y(=)	Cisco 2901 ～ 2951 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（書面）
FL-39-CNFIL-1Y(=)	Cisco 3925 ～ 3945 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（書面）
L-FL-19-CNFIL-1Y(=)	Cisco 1941 ～ 1941W 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（電子配布）
L-FL-29-CNFIL-1Y(=)	Cisco 2901 ～ 2951 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（電子配布）
L-FL-39-CNFIL-1Y(=)	Cisco 3925 ～ 3945 向け IOS コンテンツ フィルタリング 1 年間サブスクリプション ライセンス PAK（電子配布）

Cisco Services for IPS は、シグニチャ ファイルの更新、Cisco Intellishield 検索へのアクセス、および脅威対策掲示板に加えて、ハードウェア更新およびオンサイト部品交換オプション、オペレーティング システム更新、および年中無休 24 時間体制の TAC サポートを提供します。表 6 に、Cisco IOS IPS および Cisco IPS NME 向けの Cisco Services for IPS 製品番号を示します。

表 6 Cisco 1900、2900、3900 シリーズ サービス統合型ルータ向け Cisco Services for IPS 製品番号

ライセンス	説明
CON-SU1-XXXXXXXX*	CISCO SERVICES FOR IPS 8X5XNBD 19xx、29xx、39xx 向け Cisco IPS
CON-SU2-XXXXXXXX*	CISCO SERVICES FOR IPS 8X5X4 19xx、29xx、39xx 向け Cisco IPS
CON-SU3-XXXXXXXX*	CISCO SERVICES FOR IPS 24x7x4 19xx、29xx、39xx 向け Cisco IPS
CON-SU4-XXXXXXXX*	CISCO SERVICES FOR IPS 24x7x2 19xx、29xx、39xx 向け Cisco IPS
CON-SUO1-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 8X5XNBD 19xx、29xx、39xx 向け Cisco IPS
CON-SUO2-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 8X5X4 19xx、29xx、39xx 向け Cisco IPS
CON-SUO3-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 24x7x4 19xx、29xx、39xx 向け Cisco IPS
CON-SUO4-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 24x7x2 19xx、29xx、39xx 向け Cisco IPS

*末尾の xxxxxxxx は Cisco 1900、2900、3900 シリーズ専用の製品識別番号

シスコとパートナーによるブランチ向けサービス

シスコとシスコ認定パートナーが提供するサービスは、ボーダレス ネットワークにおけるブランチ エクスペリエンスの変革と、ビジネス革新および成長の促進を実現します。シスコはさまざまなテクノロジーを導入する際、わかりやすく複製可能で最適化されたブランチ ネットワークを構築するために必要な、幅広い専門知識を提供します。計画および設計によってテクノロジーとビジネス目標との整合性を図ることによって、展開の正確性、速度、および効率性を向上することができます。テクニカル サービスは、運用効率、費用の節約、およびリスクの緩和に貢献します。また最適化サービスは、パフォーマンスの向上に継続的に努めるとともに、お客様が新しいテクノロジーを使用して成功を収められるよう設計されています。

関連情報

Cisco 1900、2900、3900 シリーズ サービス統合型ルータのネットワーク セキュリティに関する詳細情報については、http://www.cisco.com/web/JP/product/hs/security/irs/index.html を参照するか、最寄りのシスコ代理店にお問い合わせください。

お問い合わせ先

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
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/

10.04