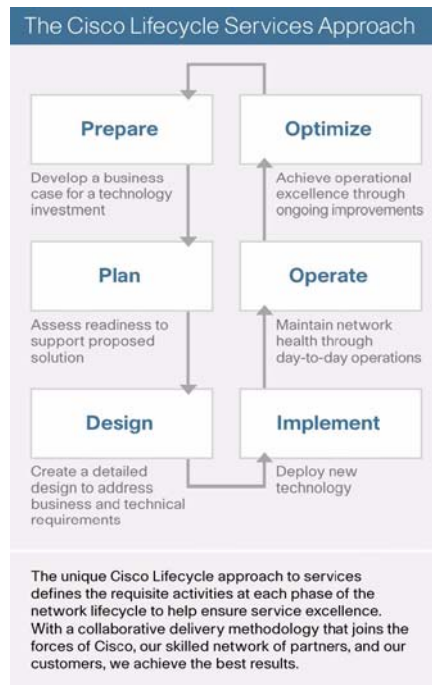


## Cisco セキュリティ最適化サービス

ネットワークをプロアクティブに強化し、進化するセキュリティの脅威と計画的/計画外のイベントへの対応を強化



### サービスの概要

ビジネス アプリケーションや情報資産を保護するために、強力な防御対策を常に維持することは、日々の課題です。ウイルス、フィッシング、トロイの木馬、侵入など、脅威の進化と複雑化に対処するには、企業システムのダウンタイム、損失、損害を最小限に抑える、プロアクティブな IT リスク管理とセキュリティ戦略が必要です。セキュリティに対するプロアクティブなアプローチを採用することによって、ビジネス要件が進化した場合にも、自社のセキュリティ インフラストラクチャを利用して堅牢かつ包括的な防御対策を確実に講じることができます。

もはや単独の製品やソリューションでセキュリティに対応することはできず、多層型のシステムがネットワーク全体に統合されている必要があると専門家は見ています。ネットワークのセキュリティ リスクに対処するには、ネットワークのライフサイクル全体に対応し、標準ベースのインフラストラクチャを基盤とする、体系的

なアーキテクチャ型のアプローチが理想的です。ネットワーク セキュリティを継続的に評価して強化することで、サービスの深刻な中断や、ビジネス資産およびアプリケーションが脆弱化する可能性を低減できます。

Cisco セキュリティ最適化サービスは、絶えず変化する脅威とコンプライアンス要件に対応するよう、セキュリティ システムの継続的な進化を支援します。Cisco セキュリティ最適化サービスでは、脅威を防止、検出、軽減するネットワーク機能のプロアクティブな評価および強化のために、広範囲の専門知識、ツール、方法論を採用しています。このサービスでは、シスコのセキュリティ専門家と協力して次の作業を行います。

- 耐障害性と信頼性に優れたセキュリティ インフラストラクチャの作成
- ビジネスの変化に応じて発展できる、ネットワーク セキュリティの最適化
- システムレベルのソリューションへの戦略的な投資

Cisco セキュリティ最適化サービスは、企業のセキュリティ インフラストラクチャを継続的に評価、開発、最適化するための統合型サービスです。専門家による計画立案、特化型ツール、四半期ごとの現地出張、継続的な分析と調整を通じて、シスコのセキュリティ チームが企業のセキュリティ インフラストラクチャを綿密に把握します。この情報と、高度なセキュリティ専門技術および情報資産を活用して、シスコのエンジニアリング チームがきわめて効果的で信頼性の高いサポートをお客様に提供します。

戦略的なプランニング、アーキテクチャの審査、継続的な評価を組み合わせることで、IT スタッフが絶えず変化するセキュリティ要件にプロアクティブに対処し、システムおよびネットワーク レベルでの脆弱性を識別し、コア インフラストラクチャに高度なテクノロジーを効率的に統合できるようになります。このサービスでは、シスコのセキュリティ専門家の支援により、長期のビジネス セキュリティおよびリスク管理をプロアクティブに実施するための戦略的な構想だけでなく、進化するセキュリティ脅威や侵入に対処する短期の戦術的ソリューションも分析することができます。

新しいセキュリティ ソリューションの展開、既存のセキュリティ インフラストラクチャの微調整、全社的なセキュリティ アーキテクチャの構築など、どのような目的でも、ビジネスを強力に保護できるようシスコのセキュリティ専門家が意思決定を支援します。Cisco セキュリティ最適化サービスでは、シスコのセキュリティ専門家が企業のソリューション設計、セキュリティ ポリシーの実装、重要なデバイスの設定を定期的に評価し、セキュリティ インフラストラクチャを高いコスト効果で最適化できるよう提案を行います。こういった効果的なサポートにより、優先的に改善が必要な部分が特定でき、セキュリティ インフラストラクチャを変更する際のリスクが減少します。

**Cisco セキュリティ最適化サービスの具体的な内容は、次の 8 つです。**

- セキュリティ テクノロジーのプランニングのサポート
- セキュリティ アーキテクチャの評価（内部および境界）
- セキュリティ体制の評価（境界）
- セキュリティ テクノロジーの準備状況の評価
- セキュリティ設計のサポート
- セキュリティ パフォーマンスのチューニング
- セキュリティに関する変更のサポート
- セキュリティに関する知識の伝達

**セキュリティ テクノロジーのプランニングのサポート**

アプリケーション、ソリューション、サービスだけでなく、セキュリティの脅威も絶えず進化している現状では、企業は防御対策の有効性を継続的に再評価する必要があります。ネットワーク セキュリティ担当者のスキルが高く、適切なポリシーを作成していても、次々と出現する脆弱性や、セキュリティのベスト プラクティスに機敏に対応するのは、きわめて困難です。

シスコの支援を利用して、セキュリティ リスクの管理にプロアクティブなアプローチを採用し、総合的なセキュリティ計画を実装することで、このような問題に対処できます。効果的なリスク軽減や、短期および長期にわたる効果的な保護を実現し、ネットワーク セキュリティへの投資に対する収益を拡大できるよう、シスコのセキュリティ専門家がお客様の意思決定を継続的に支援します。

セキュリティ テクノロジーのプランニングのサポートでは、シスコのセキュリティ アドバイザーが専門家としての助言と技術的な指導を提供し、お客様のセキュリティ戦略、テクノロジーの選択、アーキテクチャに関する意思決定を支援します。信頼できるアドバイザーの存在は、企業に次のようなメリットをもたらします。

- 継続的な助言と指導によって、IT スタッフのスキルを補強します。

- セキュリティ対策の強化と新しいソリューションの導入に関する短期および長期のセキュリティ ソリューション計画を策定します。
- 脆弱性の継続的な評価と変更サポートの最新情報を分析することで、ネットワークのセキュリティ体制を常に最新の状態に保ちます。
- ネットワーク環境を熟知したセキュリティ専門家との緊密な関係によって、セキュリティに関する意思決定がより効果的になります。

セキュリティ アドバイザーは、技術部門の責任者と戦略的プランニング担当部門に助言する目的で、定期的に行われるセキュリティ技術プランニング ミーティングに出席します。諮問ミーティングで討議するセキュリティ関連の議題は、お客様に決定していただきます。たとえば、現在進行中のセキュリティ プロジェクトに関する積極的な助言、長期のテクノロジープランニング構想に関する助言などが可能です。

#### セキュリティ アーキテクチャの評価（内部および境界）

セキュリティ アーキテクチャには、重要な業務サービスと資産を保護する、堅牢で総合的な防御対策が求められます。時間が経つにつれてネットワーク アーキテクチャが進化した場合に、ネットワーク セキュリティ テクノロジーが引き続きセキュリティ ポリシーやコンプライアンスの要件を満たしている必要があります。

セキュリティ アーキテクチャの評価は、企業のネットワーク セキュリティ アーキテクチャ、テクノロジー ポリシー、および管理手法について、詳細に検証するサービスです。この分析によって、「多層型」のネットワーク保護を実現し、予定外のコストの発生を防ぎ、コンプライアンス上の問題を減らすことで、ネットワーク セキュリティ インフラストラクチャを強化することができます。このサービスでは脆弱性を判別し、セキュリティ アーキテクチャを ISO 17799 セキュリティ モデル、業界のベスト プラクティス、企業のセキュリティ ポリシーにより適合させるための改善策を提案します。

セキュリティ アーキテクチャの評価には、次のようなメリットがあります。

- ビジネスに重点を置いたリスク回避手段を使用して、堅牢でスケーラブルなセキュリティ アーキテクチャを構築できます。
- アーキテクチャの脆弱性を判別し、セキュリティに関するベスト プラクティスに沿っていない部分を明らかにすることで、インフラストラクチャをより効果的に保護できます。
- セキュリティ リスクを軽減することで、従業員の生産性、重要な情報資産、機密扱いの顧客データを保護します。
- データの保護を強化するために、どの内部コントロールを改善すべきかを明らかにして、コンプライアンス要件に対応します。
- 将来的な脅威に対して従業員が予防、検出、対処する能力が強化されます。
- 既存インフラストラクチャのセキュリティ機能を拡張することで、投資が保護されます。

#### 内部セキュリティ アーキテクチャの評価サービス

内部から発生するプロトコルに依存しない巧妙なクライアントからの攻撃は、外部からのセキュリティ侵害よりも深刻な被害を引き起こす可能性があります。このサービスでは、このような脅威を防ぐために欠かせない、内部ネットワークのセキュリティ アーキテクチャを検証します（コア、キャンパス、および個々のサイトの WAN および LAN）。アクセス制御、ア

イデンティティ管理、ネットワーク管理、侵入の検知および防止、セキュリティ イベント管理、ロギングに適用される一般的なセキュリティ インフラストラクチャ コントロールも検証します。この評価は他のすべての評価の基準となります。

#### 境界セキュリティ アーキテクチャの評価サービス

内部ネットワークをインターネット、提携先、顧客、モバイル ワーカーに接続すると、ビジネスの可能性が大きく広がる反面、インフラストラクチャ、知的資産、顧客データ、中核的なビジネス サービスの可用性に相当なリスクが生じることになります。この評価では、内部ネットワークと外部ネットワークの境界を保護するセキュリティ アーキテクチャを検証します。具体的には、境界ファイアウォール、アクセス制御デバイス、ゲスト ネットワーク、従業員のリモート アクセス、E コマース サイトが含まれます。

シスコのセキュリティ専門家は最初のステップとして、企業のセキュリティに関する目標と要件について詳細な見直しを実施します。この情報に基づいて、セキュリティ インフラストラクチャ（ネットワーク トポロジ、ネットワーク デバイス、セキュリティ デバイス、アプリケーション デバイス、エンドポイントを含む）を綿密に分析します。さらに、セキュリティ アーキテクチャ全体のスケーラビリティ、パフォーマンス、管理性を評価します。

シスコの技術者が、インフラストラクチャに関する詳細なデータから、業界のベスト プラクティスに対する適合性を徹底分析し、アーキテクチャに見られる脆弱性と運用上のリスクを判別します。次に、運用上のリスクを軽減するために優先的に実施可能な推奨事項を提示します。これにはトポロジ、プロトコル、ポリシー、デバイス設定、管理ツールの改善が含まれます。これらのサービスでは、セキュリティ インフラストラクチャを包括的に評価することで、業務プロセスと情報の機密性、完全性、可用性に対する脅威を軽減し、企業のリスク管理の改善とコンプライアンス ニーズに対応できるよう支援します。

体系的かつ綿密なネットワーク セキュリティの評価は、リスクに対処し、コンプライアンス要件を満たし、業務プロセスと情報の機密性、完全性、可用性に対する脅威を軽減するうえで有効です。

#### セキュリティ体制の評価（境界）

企業の重要なビジネス アプリケーションおよびデータに対する、外部からのセキュリティ侵害を防止する必要があります。堅牢なセキュリティ防御対策を講じるには、現行のネットワーク、アプリケーション、システムに潜む脆弱性を明確に把握する必要があります。

境界セキュリティ体制の評価では、インターネットに接続するシステムおよびサービスに関連するセキュリティ リスクを識別します。この部分に脆弱性があると、信頼されない外部ネットワークから、信頼される内部ネットワーク、アプリケーション、システムへアクセスされる可能性があります。

境界セキュリティ体制の評価には、次のようなメリットがあります。

- IT 資産および情報に対する意図的または偶発的なアクセスのリスクを軽減することができます。
- 現行のインフラストラクチャのセキュリティ対策をテストすることで、悪質なアクティビティによる侵入やサービスの中断を確実に防止できます。
- IT インフラストラクチャにリスクをもたらすセキュリティ上の脆弱性を、プロアクティブに識別できます。

- 業務へのリスクに基づいて、リソース配分の優先順位を設定し、脆弱性に対処することが可能になります。
- 脆弱性を軽減するための推奨手順に従うことで、インフラストラクチャの全体的なセキュリティ状態を改善できます。
- セキュリティ評価が必要な法規制や業界基準により適切に準拠できるようになります。
- 新種の脆弱性への対応に必要な時間とリソースを節約できます。

シスコのセキュリティ専門家は最初のステップとして、企業のセキュリティに関する目標と要件について詳細な見直しを実施します。この情報に基づいて、内部と境界から IT インフラストラクチャを精査し、ワイヤレス ネットワークの調査とマッピングを行い、ソーシャルエンジニアリングの手法を用いて施設への侵入を試行します。この分析は、悪質な攻撃者の一般的な行動をシミュレートし、管理された安全な条件下で業務に支障を及ぼさずに実行されます。発見された脆弱性は分析され、業界のベスト プラクティスと比較し、誤認を排除するため Security Intelligence Operations による最新情報と照合されます。確認された脆弱性に基づいて結果を分析し、リスクにさらされている重要な資産とデータを特定します。その後、優先的に実施可能な推奨事項を、正式な報告書および役員へのプレゼンテーションを通じて提案します。

こうした包括的なアプローチを取ることによって、これらのサービスでは、セキュリティ インフラストラクチャの現状を評価し、セキュリティ体制を把握して改善するために必要な情報を企業に提供します。このプロセスを通じて、業務プロセスと情報の機密性、完全性、可用性に対する脅威を軽減し、企業のセキュリティ目標を達成することで、リスク管理を改善し、コンプライアンス ニーズに対応することができます。

#### セキュリティ テクノロジーの準備状況の評価

シスコのセキュリティ ソリューションの実装に先立つ準備の段階では、既存のネットワーク、運用手順、および管理ツールが、ソリューションの要件を満たしているかどうかを確認することが重要です。セキュリティ テクノロジーの準備状況の評価を通じて、既存のネットワークに新しいソリューションを円滑かつ確実に統合するために、どのような変更が必要かを確認できます。

セキュリティ テクノロジーの準備状況の評価には、次のようなメリットがあります。

- 必要なリソースと技術要件を明らかにし、必要なインフラストラクチャ変更を効果的に行う計画を立案することで、ソリューションの実装と移行に必要な期間を短縮できます。
- 一貫性のある統合型ソリューションの導入が可能になり、ネットワーク管理者と IT スタッフの全体的な生産性が向上します。
- ハードウェア、ソフトウェア リリース、および機能の正しい組み合わせを使用して、ソリューションのパフォーマンス、耐障害性、可用性を高めることができます。

ネットワーク技術者が導入要件を分析し、使用しているネットワーク デバイス、運用手順、アーキテクチャが、導入予定のソリューションをサポートできるかどうかを評価します。システム機能に対応しないコンポーネントを特定すると共に、拡大された規模での導入にネットワーク トポロジが対応できるかどうかを判別し、冗長性、スケーラビリティ、ハードウェアとソフトウェアのアップグレードの必要性について、綿密な影響分析を行います。

準備状況の評価に基づく推奨事項では、既存のネットワークでシスコのセキュリティテクノロジーを正しく運用するために必要な情報が提供されます。既存のインフラストラクチャの不備を明らかにし、その不備を補う設計を考案することで、無駄のない迅速な導入が可能になり、多額の費用をかけてネットワーク インフラストラクチャを補整する必要性を削減することができます。

#### セキュリティ設計のサポート

企業ネットワークの保護が、かつてないほど重要になっています。ネットワークへの脅威の存在を理解している企業でも、その脅威に対抗するために、ネットワークのセキュリティ設計を適応させるのは容易なことではありません。設計に欠陥があると、新しいセキュリティソリューションの有効性が損なわれ、導入に時間がかかり、統合にかかる費用の高騰を招く結果になります。

このサービスでは、シスコのコンサルタントが企業と共同で、強力なセキュリティ設計を策定します。シスコの設計方法論では、ネットワーク セキュリティのあらゆる側面と、コア ネットワーク インフラストラクチャとの統合が考慮されます。業界標準に基づく多層型構造のアプローチを採用し、ターゲットを特定したハッカー攻撃にも、ウイルスやワームによる無差別攻撃にも対抗できる、多層型の防御対策の開発を支援します。

セキュリティ設計のサポートには、次のようなメリットがあります。

- 多層型防御を提供する、企業固有のネットワーク セキュリティ設計を開発します。
- セキュリティソリューションの信頼性、保守性、パフォーマンスを改善します。
- 新しいテクノロジーの設計、実装、導入段階で生じる、代償の大きい遅れや問題の発生を抑制します。

アーキテクチャ型のアプローチによって、新しいビジネス アプリケーションの導入をサポートし、長期にわたって維持と進化が可能なセキュリティ インフラストラクチャの設計と構築ができます。全社的に応用できる、セキュリティ設計に関する共通の原則、ポリシー、慣例をシスコが指定します。その結果、ネットワーク セキュリティ管理に必要な時間とコストを節約し、ネットワークの総所有コスト（TCO）を削減できます。

シスコのネットワーク セキュリティ専門技術者が企業と共同で、ビジネス戦略および関連するセキュリティ目標、要件、基準を見直します。ネットワーク セキュリティ設計を綿密に分析し、ビジネス戦略や IT 戦略への適合性を判別します。ネットワークについて収集した情報に基づき、シスコの技術者がネットワークの脆弱性を詳細に見直し、実証済みのネットワーク セキュリティ設計のベスト プラクティスと照合してセキュリティ設計を評価します。

既存のネットワーク設計について脆弱性を評価した後、セキュリティソリューションのセキュリティ要件の識別と優先順位付けを行います。要件には、侵入検知、アドミッション コントロール、リモート アクセス、エンドポイント保護、脅威の抑制、境界制御、VPN が含まれます。シスコの推奨事項には、ネットワーク トポロジ、デバイスの配置、接続方式など、セキュリティ インフラストラクチャ設計の改善が含まれる場合があります。スケーラビリティ、パフォーマンス、管理性を含めて、ネットワークのあらゆる側面を考慮に入れ、個々のセキュリティ コンポーネントについて、プロトコル、ポリシー、機能面の改善を提案する場合があります。

### セキュリティ パフォーマンスのチューニング

今日の高度なセキュリティ ソリューションを効果的に運用するには、導入、設定、チューニング、およびネットワーク インフラストラクチャへの組み込みに際して注意を払う必要があります。侵入防御、ネットワーク アドミッション コントロール、自動監視および応答システムなどの先進的なテクノロジーは、セキュリティ攻撃を遮断するためにポリシーベースのアプローチを採用しているものが少なくありません。したがって、企業のビジネス目標とセキュリティ ポリシーを、最初からソリューションに緊密に統合する必要があります。

テクノロジー、業務プロセス、ネットワークへの脅威は絶えず変化しているので、企業のセキュリティ体制も変化していく必要があります。企業固有の環境向けにカスタマイズされ、組織のセキュリティ ポリシーに準拠し、適切に運用されているソリューションに対し、一貫してポリシーを適用し続けるには、システムの継続的な分析が重要です。

セキュリティのパフォーマンス チューニング サポートは、システム設計の定期的かつ継続的な分析を通じて、IT スタッフによる脅威の迅速な検証、セキュリティ インシデントへの対応、コンプライアンスの維持を可能にする、安全で高性能なネットワークを維持するためのサービスです。

セキュリティのパフォーマンス チューニング サポートには、次のようなメリットがあります。

- 設定に関するベスト プラクティスとポリシーの実装を継続的に分析し、セキュリティ システムを最適化します。
- 企業のセキュリティ ポリシーおよび手順に沿った形で、ネットワーク パフォーマンスが向上します。
- より適切なポリシーの設定とチューニングを推奨し、システム パフォーマンスを強化します。

セキュリティのパフォーマンス チューニング サポートは、Cisco Security Monitoring, Analysis, and Response System (CS-MARS)、Cisco Network Admission Control (NAC)、Cisco Security Agent などのポリシーベース ソリューションの継続的な分析とチューニングを行い、企業のセキュリティ ポリシーに従って、費用対効果を最大限に高める形で機器を使用できるように必要な変更を推奨します。シスコのセキュリティ専門家がデバイス設定とポリシーの実装を分析し、シスコのベスト プラクティスと比較したうえで、セキュリティ ソリューションの効果を最大限に高めるための推奨事項を提案します。その結果、企業のセキュリティ ポリシーおよび手順に沿った形で、セキュリティ デバイスのパフォーマンスが向上します。

### セキュリティに関する変更のサポート

セキュリティ インフラストラクチャを迅速かつ効率的に変更できるかは、安全なネットワークを維持するために必要な条件の 1 つです。潜在的な問題点を事前に発見し、顕在化していないイベントをすばやく解決することで、より効果的で安全なネットワークになります。

シスコのセキュリティ専門家が、セキュリティ ソリューションの計画的/計画外の変更をサポートします。このサービスの一環として、高度なセキュリティ テクノロジーの変更内容、実装計画、テスト計画、ロールバック計画をシスコの技術者が確認し、リスクを低減すると同時に、変更によって確実にネットワーク セキュリティを強化できるようにします。

セキュリティに関する変更のサポートには、次のようなメリットがあります。

- セキュリティ インフラストラクチャの重要な変更を行う際に、代償の大きい遅れや問題の発生を防ぎます。
- 実装、テスト、ロールバック計画を確認し、ソリューション環境の変更を円滑に実行できるようにします。
- 変更作業中に発生した問題を迅速に診断し、専門的な支援によってネットワークサービスの中断を未然に防ぎます。

シスコのセキュリティ技術者は、セキュリティ インフラストラクチャを熟知しており、セキュリティ テクノロジーの導入経験が豊富なため、技術的な課題や導入時の問題を迅速かつ効率的に解決することができ、ネットワークとビジネスへの影響を抑えることができます。

### セキュリティに関する知識の伝達

ネットワークを効果的に保護するために必要なスキルとテクノロジーは、絶えず変化しています。ネットワーク セキュリティのスタッフに、新しいテクノロジーとネットワーク セキュリティの状態について常に最新の情報を提供できるかどうかによって、ネットワークが脅威から保護された安全なものであるか、脅威にさらされてしまっているか、差が生じる場合があります。また、運用コストを削減するには、ネットワーク サポート部門のスキルを継続的に強化する必要があります。

セキュリティに関する知識の伝達および社内教育のサポートとして、今日のネットワーク セキュリティ専門技術者に要求される、絶えず変化するコンピテンシーに適応するために必要な知識を提供し、従業員の自己解決能力の向上を支援します。シスコのセキュリティ専門家がテレビ会議、ビデオ オン デマンド、プレゼンテーション、オンライン トレーニング、集合研修など、ニーズに応じた形式で情報を伝達します。

トレーニングの内容、方法、所要時間については、相談のうえ決定します。次のようなトレーニングが可能です。

- テクノロジーの最新情報
- 製品およびテクノロジーに関する詳細情報
- 技術者向けホワイトペーパー
- 運用に関するガイダンス
- パフォーマンス チューニングの技術的なヒント

シスコのセキュリティ技術者が、電話会議と電子メールによってスタッフと定期的に連絡を取ります。継続的なコミュニケーションによって体系化されたトレーニングを増やすことができ、ネットワークのライフサイクル全体を通じて全般的な知識の伝達が容易になります。

表 1. Cisco セキュリティ最適化サービスの概要

サービス	内容
セキュリティ テクノロジーのプランニングのサポート	<ul style="list-style-type: none"> <li>• 戦略的プランニングとロードマップ作成の継続的なサポート</li> <li>• テクノロジー移行のプランニング</li> <li>• ネットワーク セキュリティに関する分析と意思決定への提案</li> <li>• 四半期ごとのセキュリティ テクノロジーのプランニングのレポート</li> </ul>
セキュリティ アーキテクチャの評価（内部および境界）	<ul style="list-style-type: none"> <li>• セキュリティ アーキテクチャのワークショップ</li> <li>• セキュリティ アーキテクチャの分析</li> <li>• 不備の分析と推奨事項</li> <li>• セキュリティ アーキテクチャの評価レポート</li> </ul>

サービス	内容
境界セキュリティ体制の評価	<ul style="list-style-type: none"> <li>インターネットから認識できるシステムとサービスの特定</li> <li>侵入テストによる脆弱性の発見</li> <li>詳細な分析による重要な脆弱性の識別</li> <li>発見されたリスクを優先順位付けしたリストと推奨措置</li> <li>境界セキュリティ体制の評価レポート</li> </ul>
セキュリティ テクノロジーの準備状況の評価	<ul style="list-style-type: none"> <li>セキュリティに関する検出作業のワークショップ</li> <li>導入予定ソリューションの影響分析</li> <li>セキュリティ テクノロジーの準備状況の評価レポート</li> </ul>
セキュリティ設計のサポート	<ul style="list-style-type: none"> <li>セキュリティ設計と検出作業のワークショップ</li> <li>セキュリティ設計の見直し（不備の分析と推奨事項を含む）</li> <li>詳細なセキュリティ設計レポート</li> </ul>
セキュリティのパフォーマンス チューニング	<ul style="list-style-type: none"> <li>セキュリティ デバイスの検出</li> <li>基準設定テンプレートの分析</li> <li>デバイス設定の分析（チューニング要件を含む）</li> <li>反復的なパフォーマンス チューニング</li> <li>セキュリティのパフォーマンス チューニングのレポート</li> </ul>
セキュリティに関する変更のサポート	<ul style="list-style-type: none"> <li>実装計画の確認</li> <li>テスト計画の確認</li> <li>ロールバック計画の確認</li> <li>リモート エンジニアリングのサポート</li> <li>計画的なセキュリティ システム変更のサポート</li> <li>計画外のセキュリティ システム変更のサポート</li> </ul>
セキュリティに関する知識の伝達および社内教育	<ul style="list-style-type: none"> <li>知識の伝達に関する評価のワークショップ</li> <li>知識の伝達に関する要件のレポート</li> <li>四半期ごとの講義および/または技術プレゼンテーション</li> <li>集合研修およびリモート セッションでの知識の伝達</li> <li>電話会議および電子メールでの継続的なコミュニケーション</li> </ul>

## 利点

シスコの技術者はネットワーク保護のエキスパートです。どの技術者も、侵入検知、アドミッション コントロール、リモート アクセス、エンドポイント保護、脅威の抑制、境界制御、VPN など、シスコの高度なセキュリティ テクノロジーに関する豊富な知識を備えています。シスコは、長年にわたり世界有数の複雑なネットワークを保護してきた経験に基づいて、セキュリティ システムのパフォーマンスの最適化に関する実証済みの方法論を確立しています。今日のネットワークが直面しているさまざまな脅威についても、シスコの技術者は熟知しています。

Cisco セキュリティ最適化サービスを利用すると、戦略的プランニング、アーキテクチャの評価、設計、パフォーマンス チューニング、継続的な最適化のサポートを通じて、ネットワーク インフラストラクチャをプロアクティブに強化し、進化するセキュリティの脅威および計画的/計画外のイベントに対応することができます。

まとめると、これらのサービスは次のようなメリットをもたらします。

- セキュリティ テクノロジーのプランニングのサポート**：専門家によるプランニング、分析、意思決定により、セキュリティ リスクにプロアクティブに対処します。
- セキュリティ アーキテクチャの評価**：脆弱性やベスト プラクティスおよびポリシーから逸脱している点を識別し、ネットワークを強化します。
- セキュリティ テクノロジーの準備状況の評価**：ネットワークが新しいソリューションに対応可能であるかどうかを専門家が分析することによって、無駄のない迅速な導入を可能にします。

- **セキュリティ体制の評価**: IT 資産および情報に対する意図的または偶発的なアクセスのリスクを軽減することができます。
- **セキュリティのパフォーマンス チューニング**: システム設定とポリシーの実装を継続的に分析し、高度なソリューションをプロアクティブに最適化します。
- **セキュリティ設計のサポート**: ソリューション設計の信頼性、保守性、パフォーマンスを改善します。
- **セキュリティに関する変更のサポート**: セキュリティ インフラストラクチャの重要な変更を行う際に、代償の大きい遅れや問題の発生を防ぎます。
- **セキュリティに関する知識の伝達**: 継続的な対話型のラーニングおよびトレーニング セッションを通じて、スタッフのスキルを継続的に強化します。

### シスコのサービスが選ばれる理由

シスコのサービスは、ネットワークとアプリケーション、そしてこれらを利用する人々を連携させることで、より大きな成果を発揮させます。

今日のネットワークは、人、情報、およびアイデアの緊密な結び付きを必要とする世界における、戦略的プラットフォームとなっています。サービスと製品とを組み合わせ、ビジネスのニーズと機会に合わせたソリューションを作り上げれば、ネットワークはその力をさらに発揮します。

シスコのユニークなライフサイクル サービス アプローチでは、優れたサービスを提供するために、ネットワーク ライフサイクルの各段階において必要なアクティビティが定義されています。サービスの提供にあたっては、シスコだけでなく、高い技術力を持つパートナーと、お客様とが力を合わせるというコラボレーション的方法論に基づいて、優れた成果を達成します。

### 関連情報

Cisco セキュリティ最適化サービスの詳細については、  
<http://www.cisco.com/jp/go/services/security/> を参照してください。

©2009 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料に記載された仕様は予告なく変更する場合があります。



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/>

お問い合わせ先