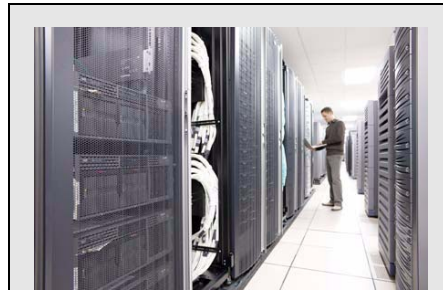


Cisco IT GRC セキュリティ評価サービス

情報保護に関するビジネス戦略とテクノロジー戦略を一致させ、セキュリティとコンプライアンスのリスクとコストを削減

課題：セキュリティの脅威とコンプライアンス要件に、限られたリソースで効率的に対処

情報化社会におけるセキュリティの問題は、減るどころか増える一方です。Web 2.0 などの新しいテクノロジーを使って情報共有やコラボレーションを行う場合は、プライバシーを保護すると同時に、情報資産の管理にも注意を払う必要があります。対外的には、行政、業界、顧客から要求されるコンプライアンス要件を満たす必要があり、リソースがより限られるようになっている中、こうした懸念事項は増え続けています。



セキュリティに対する IT GRC のアプローチ

Cisco IT GRC セキュリティ評価サービスは、絶え間なく進化する情報セキュリティの脅威から企業を守ると同時に、対外的なコンプライアンス要件の増加に対応するという、2つの課題の解決に貢献します。このサービスは、企業に次のようなメリットを提供します。

- 全社的なセキュリティの強化：全社的な観点からセキュリティを捉えることで、可視性とアカウントバリエーションが強化されます。
- コストの削減：ビジネス戦略とテクノロジー リソースを 1つのプログラムに統合することで、作業の重複やコストの無駄を省くことができます。
- コンプライアンス上の障害が減少：あらゆるコンプライアンス要件と、それらを満たすために必要なコントロールについての可視性が高まり、コンプライアンスの継続的な監視と強化が可能になります。
- 長期的な管理への対応：セキュリティおよびコンプライアンス プログラムを継続的に管理するためのフレームワークを作成し、長期にわたって資産を確実に保護することができます。

多くの企業は、セキュリティの脅威から組織を保護すると同時に、対外的なコンプライアンス要件を果たすために、絶えず奮闘しています。これらの企業では通常、この状況に対処する方法として、多数の異なるプログラムを使用しています。その結果、非効率、作業の重複、見落とし、コストの増大といった問題が生じています。

ソリューション：1つの包括的なプログラムによって、コストの削減、可視性の向上、セキュリティとコンプライアンスの強化を実現

IT Governance, Risk management, and Compliance (IT GRC) は、情報保護に関するビジネス戦略とテクノロジー戦略を一致させることによって、情報セキュリティ リスクの軽減と、法規制および業界のコンプライアンス コストの削減を可能にする共同プログラムです。ビジネス戦略では、法令および業界で定められた情報保護に関する要件を満たす必要があります。一方、テクノロジー戦略では、リスクや不確実性に対処するための効果的なインフラストラクチャが要求されます。これらの取り組みに不整合があると、セキュリティ インシデント、データの損失、監督機関による監視といった問題が起こりやすくなります。これらが正しく一致していれば、顧客満足度の向上、収益の増加、競争上の差別化を強化することができます。

シスコはお客様の IT GRC セキュリティ プログラムの実施と維持を支援するために、次の 4 つのフェーズすべてに対応する総合的なサービスおよびセキュリティ製品スイートを提供しています。

- **定義**：セキュリティの脅威からの保護と、コンプライアンス要件への対応に必要なコントロールを定義します。
- **評価**：実装している既存のセキュリティ コントロールを評価し、不備や脆弱性を明らかにして、これらを解決するための優先的な措置を提案します。
- **改善**：ポリシーとテクノロジーの開発または拡張を行い、優先度の高いコントロールの不備を解決します。
- **維持**：コントロールの運用と修正を通じて、脅威、コンプライアンス要件、ビジネス目標の変化に対応します。

サービスの概要

シスコは、IT GRC セキュリティ プログラムについて、企業のあらゆるニーズに対応する製品とサービスを幅広く提供しています。その中で Cisco® IT GRC セキュリティ評価サービスは、次の 4 つの工程において、「定義」および「評価」段階を設けて企業を支援します。

- 共通のコントロール フレームワークの定義
- セキュリティ ポリシーの評価
- セキュリティ アーキテクチャの評価
- セキュリティ体制の評価

共通のコントロール フレームワークの定義

Cisco IT GRC セキュリティ評価サービスの最初の作業は、共通のコントロール フレームワークの作成です。このフレームワークは、対外的なコンプライアンス要件への効率的な対応と、情報セキュリティの脅威からの保護を実現する、統一的なセキュリティ コントロールのセットです。この作業では最初に、企業のセキュリティ コントロールに関する目標を判別して組み込みます。これらのコントロール要件は、Sarbanes-Oxley (SOX 法) などの法令のほか、International Organization for Standardization (ISO) 27000 シリーズや Payment Card Industry (PCI) データ セキュリティ基準などの業界基準、さらにはセキュリティに関する企業独自のベスト プラクティスによって策定されます。

次に、各基準間にコントロールを対応付け、重複をなくします。残ったコントロールについて、企業のリスクおよびセキュリティ戦略に基づいて見直しを行い、企業の環境に適さないコントロールを排除します。最後に、企業の資産およびリスク許容度に応じて、共通のコントロール フレームワークの優先順位を決定し、後続のサービスおよび製品ソリューションを含めて、以降の活動方針についての確な判断が下せるようにします。

この共通のコントロール フレームワークが、IT GRC プログラムの基盤になります。これは企業のセキュリティとコンプライアンスに関するニーズを満たす、必要最小限のセキュリティ コントロールのセットです。この段階では、共通のコントロール フレームワークとコントロール選択の根拠を記した適用宣言書のほか、今後の評価および見直し作業で優先すべき重要なコントロールの一覧が提出されます。

セキュリティ ポリシーの評価

セキュリティ ポリシーの評価では、共通のコントロール フレームワークで規定されたコンプライアンス要件への対応に必要なコントロールと照らし合わせて、企業の既存のポリシー インフラストラクチャを見直します。シスコの専門家がさまざまなポリシー評価技法を使用して、ポリシー アーキテクチャのアクセシビリティ、強制力、および管理性を判断します。セキュリティ ポリシーの評価では、既存のポリシーの強みと弱み、改善のための推奨事項を記載したレポートが提出されます。

セキュリティ アーキテクチャの評価

セキュリティ アーキテクチャの評価では、共通のコントロール フレームワークでの要件に基づいて、企業の技術インフラストラクチャを綿密に評価します。この評価では、重要な資産のリスクの原因となる不備を特定し、セキュリティ コントロールを実装または強化するための提案を行います。セキュリティ アーキテクチャの評価は、ISO 27000 シリーズ セキュリティ モデルおよび業界のベスト プラクティスに準拠した、ベンダーに依存しない共通のセキュリティ フレームワークに基づいているので、シスコ ネットワークとマルチベンダー ネットワークの両方に対応します。最先端のツールおよび方法論を使用し、シスコの製品開発部門およびサポート部門との密接な連携のもとで評価を行います。

セキュリティ体制の評価

共通のコントロール フレームワークで使用するポリシーと技術コントロールの評価が終わった段階で、これらのコントロールが保護およびコンプライアンスを提供するために適切に実装され運用されているかを確認することが重要です。したがって、セキュリティ体制の評価では、管理された安全な条件下で、境界、内部、ワイヤレス ネットワーク経由での悪質な攻撃をシミュレートしたり、施設に物理的に侵入する目的で利用される可能性のあるソーシャル エンジニアリングを用いて、企業のセキュリティ ポリシー、設計、アーキテクチャの実効性について、現時点での検証を行います。判明した脆弱性については、シスコの Security Intelligence Operations データベースと照合して相関付けを行います。このデータベースは、500 人以上のセキュリティ アナリストによって維持され、誤認をなるべく排除すると共に、脆弱性に対し実績のある軽減対策を提供します。

表 1 に、Cisco IT GRC セキュリティ評価サービスのアクティビティと利点を示します。

表 1. Cisco IT GRC セキュリティ評価サービスの内容と利点

アクティビティ	利点
<ul style="list-style-type: none"> セキュリティに関するビジネス目標と要件を見直します。 対外的なコンプライアンス要件とセキュリティに関するベスト プラクティス要件を共通のコントロール フレームワークに組み込み、情報保護に関するビジネス戦略とテクノロジー戦略を一致させます。 コンプライアンス要件への対応に必要なコントロールと照らし合わせて、既存のポリシー インフラストラクチャを見直します。 共通のコントロール フレームワークに関する要件と照らし合わせて、既存のセキュリティ アーキテクチャおよびインフラストラクチャ設計を見直します。 セキュリティ ポリシー、設計、アーキテクチャの実装と運用の有効性を検証します。 リスクを考慮して、解消すべき不備と脆弱性に優先順位を付けます。 所見を提示し、判明した弱点に対処するための優先的な推奨事項を示します。 	<ul style="list-style-type: none"> 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。 セキュリティおよびコンプライアンス プログラムの重複をなくすことで、コストを削減します。 企業固有の環境の要件に対応する 1 つのプログラムに、セキュリティおよびコンプライアンス関連の取り組みを一本化します。 セキュリティおよびコンプライアンス プログラムの実効性を明確に把握できます。 セキュリティおよびコンプライアンス関連の作業を継続的に管理するためのフレームワークを提供し、セキュリティの有効性を強化します。 内部コントロールを見直す機会を明確にし、データ保護を強化します。 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。

シスコのサービスが選ばれる理由

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て、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。

シスコとパートナーの専門知識

Cisco IT GRC 評価サービスは、セキュリティに関する専門知識が豊富なシスコのコンサルタントおよびシスコ認定パートナーが提供します。シスコのコンサルタントおよびパートナーは、さまざまな業界および官公庁に関する専門知識を有し、技術面と経営面からのアドバイスを提供します。その基盤には、最先端のツール、最良の方法例、シスコの製品開発部門およびサポート部門との密接な連携があります。シスコの専門家およびパートナーがお客様を支援し、セキュリティ コントロールの定義や潜在的な脆弱性の発見を行うことで、「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ぐと共に、全社的なコンプライアンスのニーズを満たすことが可能になります。

利用地域と発注

Cisco IT GRC 評価サービスは、シスコおよびシスコ認定パートナーを通じて全世界でご利用いただけます。地域によって細部が異なる場合があります。

関連情報

Cisco IT GRC 評価サービスの詳細については、シスコ代理店にお問い合わせください。

シスコのセキュリティ サービスの詳細については、www.cisco.com/jp/go/services/security/をご覧ください。

©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