

シマンテック コンプリート・ウェブ サイトセキュリティ コンソール

ウェブサイト セキュリティの統一と強化

時間と場所を問わず、ひとつの場所で、SSL/TLSサーバ証明書の管理、発行、操作が行えるようになりました。本コンソールは、さらに簡単な作業で、ウェブサイトをより安全にする目的でつくられています。

ソリューションの概要

証明書の可視性

より深い洞察と大きな自信から、より多くの成功を実現し、リスクをより軽減することが可能となります。具体的には次のことが行えます。

- ライフサイクル管理と、SSL/TLSサーバ証明書の検出、監視、分析を統合したクラウドベースのポータルを通じて、時間と場所を問わない可視性を獲得すること。
- SSL/TLSサーバ証明書の脆弱性やコンプライアンス上の問題を容易に検出し修正すること。
- 予期せぬSSL/TLSサーバ証明書の期限切れをなくし、解決を促進するための関連する高額な緊急コストがかからないようにすること。
- 手動による検出や更新プロセスを自動化する機能を使用して、人件費を引き下げること。
- コストの制御、運用の最適化、証明書のトラッキングの簡素化、強力なレポートングによる予測/予算編成/監査、カタログ化、データの可視化、証明書に関するインテリジェントな分析を実行すること。

SSL/TLSの管理

SSL/TLSサーバ証明書は、お使いのエコシステムにおける情報のデジタルフローを保護し、コンプライアンスを維持するために大きな役割を果たします。ただし、証明書の可視性、制御、セキュリティが不適切である場合、御社のビジネス、顧客、評判が危険にさらされる可能性があります。

ウェブサイトの停止を引き起こす証明書の期限切れは避けなければなりません。新たな証明書の脆弱性やコンプライアンスの変更に対して迅速かつ効率的に対処する必要があります。また、ウェブサイトの成長に影響を与えることなく、証明書に関するポリシーを実施できることも必要です。さらに、それを最小の作業とコストで実施する必要があります。

シマンテックのエンタープライズクラスのSSL/TLS管理は、適切な証明書の可視性、制御、スケーリング、セキュリティを通じて、これらのすべての問題に簡単に対処できるようにします。御社の信頼できるセキュリティのカウンセラーとして、弊社は、御社が攻撃性を増しているデジタル環境を生き抜くために必要となるリソースや専門家によるガイダンスを提供します。競合ソリューションでは必要となる複雑で高額なプロフェッショナルサービスは一切不要です。

主なメリット

- 証明書の期限切れにより引き起こされる機能停止を防止
- 統合されたウェブサイトセキュリティの可視性を提供
- 直観的に理解できるインターフェイス
- セットアップや学習が簡単で、使いやすい
- 統合されたツール
 - ツールや画面を切り替える必要はなく、必要とするすべてのものがひとつに集められている
- ワークフローの最適化
 - より少ないクリック回数で、より多くのことを実行できる
 - ステップバイステップのウィザードとインストールガイドに従うだけで、処理全体を完了できる。詳細なヘルプマニュアルやガイドは不要。
 - 優先順位付きのアラートを表示し、問題のある証明書を修正可能

コンプリート・ウェブ サイトセキュリティ ビュー：SSL/TLSサーバ 証明書管理用



SSL/TLSの管理



検出機能



自動化機能



リスク評価



修正

Discovery (検出機能)

証明書の可視性は、コンソールのDiscoveryを使うことで可能となります。同ツールを使うと、最も複雑なネットワーク環境であっても、SSL/TLSサーバ証明書の検索と監視を継続的に実施でき、証明書のトラッキングと監査を簡素化できます。すべての証明書情報は、セキュリティおよび脆弱性の評価と共に、実行可能なインテリジェンスへとカタログ化されます。これらの評価により、現在のステータスを常に知ることができるほか、期限切れ、不正利用、脆弱な証明書や非準拠の証明書に対処するために推奨される最良の措置を知ることができます。

Automation (自動化機能)

証明書管理は時間のかかる面倒な作業になりがちです。Automationを使うと、更新や置き換えを簡素化し迅速化できます。大規模環境での証明書管理を自動化することで、手動で証明書を管理する手間を一掃できるほか、ウェブサイトを危険にさらす期間を最小化できます。また、Automationは、複数のサーバ上での証明書の配備コストを、手動に比べて大幅に引き下げます。

Risk assessment (リスク評価)

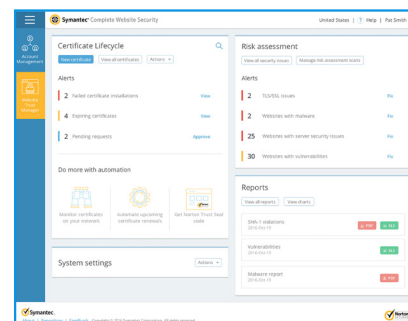
シマンテックのコンプライート・ウェブサイトセキュリティには、お使いのウェブサイトのページ、アプリケーション、サーバソフトウェア、ネットワークポートに関する毎週の脆弱性評価と、毎日のマルウェアスキャンが含まれています。これにより、お使いのウェブサイトをマルウェアから守ることができるほか、修復が必要な脆弱性に関するアラートを受け取ることで、御社のサイトがサイバー攻撃の標的となることを阻止できます。

プライベートSSL

シマンテックのプライベートSSL機能を使うと、お使いの内部(プライベート)およびパブリックSSL/TLSサーバ証明書の両者を同一のコンソール内に統合することで、お手持ちのポートフォリオに関するセキュリティと可視性を改善できます。また、弊社が提供するセキュアなホスティング型の「プライベートSSL」の階層を利用することもできれば、御社独自の階層をアップロードすることもできます。

コンソールの機能

- ダッシュボード**
 ダッシュボードは、御社のビジネス継続性や、業界ルールや規制のコンプライアンスに影響する可能性のある、クリティカルな証明書に関する問題の簡潔な要約を、優先順位付けした形式で表示します。
- 優先順位付けされたアラート**
 コンプライアンスを維持し業界標準を満たすためには、クリティカルな問題を認識している必要があります。コンソールは、アラートを素早く優先順位付けするため、どの問題が自分にとって最も緊急に対処すべきものであるかが分かります。これにより、時間を節約し、ビジネス継続性とセキュリティを確保できます。
- 強力な分析**
 SSL/TLS環境では一般に可視性が提供されていないため、どんな証明書がインストール済みであるかを知り、それらのステータスがどうなっているかを判定することが困難です。コンソールを使うと、インストール済みの証明書のステータスを分析し、それらが正しくインストールされているかどうかの判定が簡単に行えます。また、コンソールは、最も緊急なリスクの判定に役立つ、証明書とサーバの両方に関する評価を提供します。また、コンソールの動的フィルタリング機能を使用すると、各種の条件から選択することで、御社のウェブサイトセキュリティ環境についての明確なイメージを得ることができます。



レポートिंगとチャートライブラリ

ポリシーの実施は御社のビジネスにとってクリティカルです。御社がコンプライアンスを維持し、ポリシーと業界標準の両方を満たすことができるようにするために、デフォルトおよびカスタムのレポートングを使用して、ポリシー違反（アルゴリズム別の暗号化レベルや証明書を含む）を表示できるようになっています。また、詳細な分析や共有を行うために、データをエクスポートできます。

ロールベースのアクセス

委任管理権限とロールベースのアクセス権を持つ複数の証明書管理者間および証明書申請者間でロールや責任を分けることにより、セキュリティリスクを最小化します。

アカウントとサポート

単一の中央ロケーションから、各自のサブスクリプション、資格、ユーザーアクセス、認証を確認し管理できます。「Account and Support」セクションは、アカウントライフサイクル、サポートレベル、シマンテックとの契約の詳細に関する情報を提供します。本セクションでは、組織およびドメイン認証要求を発行することや、あらゆるサービスに関する自分の要求のステータスを確認することもできます。

コンプリート・ウェブサイトセキュリティについて

コンプリート・ウェブサイトセキュリティ

シマンテックのコンプリート・ウェブサイトセキュリティは、サイバーセキュリティのグローバルリーダーであるシマンテックが提供するソリューションであり、可視性、アジリティ、クラス最高のセキュリティにより、御社のウェブサイトの調和と強化を実現し、御社のビジネス、ブランド、顧客を、自信をもって保護できるようにします。

お問い合わせ

03-5114-4137またはmpki-ssl_jp@symantec.com
合同会社シマンテック・ウェブサイト セキュリティ
〒107-00052
東京都港区赤坂1-11-44 赤坂インターシティ
<https://www.symantec.com/ja/jp/website-security>