リスク管理フレームワークのためのSplunk

NIST 800-53コントロールの評価と監視

“...リスク管理のプロセスを通じて、リーダーは国益に対するリスクを考慮しなければならない。考慮すべきリスクには、サイバー空間を自らの利益のために利用する敵対者から生じるリスクと、軍事作戦、情報活動、事業活動の目的を達成するためにサイバー空間のグローバル性を利用する私たち自身の取り組みから生じるリスクがある...”

— 米国国防総省統合参謀本部、議長室
国家サイバー空間活動戦略(The National Strategy for Cyberspace Operations)

米国国防総省(DoD)は、2014年に発行した命令で、国防総省情報保証認証および認定プロセス(DIACAP)をリスク管理フレームワーク(RMF)に置き換えました。各情報システムのリスク管理体制は時間とともに変化するため、RMFは継続的プロセスとして管理することが想定されています。

ステップ1：分類

インパクト分析に基づき、情報システムとそのシステムが処理、保存、送信する情報を**分類**します。[1]

ステップ2：選定

セキュリティ分類に基づき、情報システムに適用するセキュリティコントロールのベースラインとなる初期セットを**選定**します。このセキュリティコントロールのベースラインは、組織におけるリスク評価と各地域の状況に基づき、必要に応じて調整および追補します。[2]

ステップ3：実装

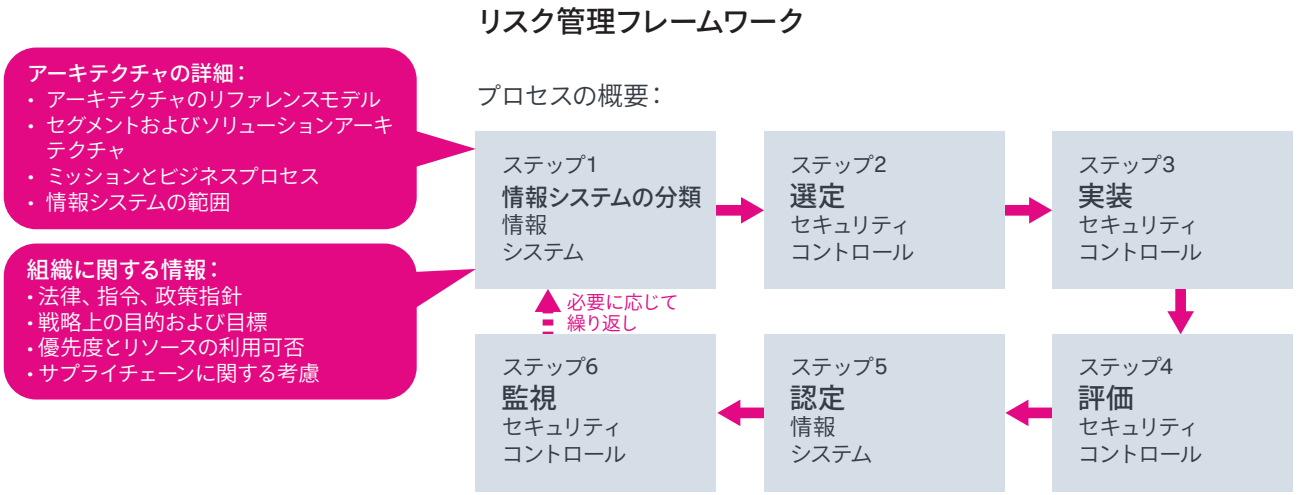
セキュリティコントロールを**実装**し、そのコントロールを情報システムや運用環境内へどのように展開したかを文書に記録します。

ステップ4：評価

そのシステムがセキュリティ要件を満たしているかという観点から、セキュリティコントロールが適切に実装されているか、意図したとおりに機能しているか、目指していた結果を出せているかについて、その度合いを適切な手続きによって**評価**します。

ステップ5：認定

組織の業務や資産、人、他の組織、国家に対して情報システム運用がもたらすリスクを判定し、そのリスクが許容可能であるという決定に基づいて、情報システム運用を**認定**します。



1.FIPS 199は国家以外のセキュリティシステムを対象としてセキュリティ分類の指針を提供するのに対し、CNSS Instruction 1253は国家セキュリティシステムを対象として同様の指針を提供します。

2.NIST Special Publication 800-53は国家以外のセキュリティシステムを対象としてセキュリティコントロール選定の指針を提供します。CNSS Instruction 1253は国家セキュリティシステムを対象として同様の指針を提供します。

ステップ6：監視

情報システムの選定したセキュリティコントロールを継続的に**監視**および評価します。これには、セキュリティコントロールの有効性評価、運用システムや運用環境に対する変更の文書記録、関連する変更のセキュリティインパクト分析の実施、しかるべき組織担当者へのセキュリティ状況の報告が含まれます。

Splunkのメリット

RMFのプロセスは、組織内において、明確に定義されたリスク管理タスクのセットとして、明確に定義された役割を持つ組織内の個人またはグループによって実行されます。Splunk®は、RMFプロセスの促進と有効化に取り組む行政機関で、特にステップ4(評価)とステップ6(監視)に活用できます。

Splunkはコスト効率と柔軟性に優れた統合ソリューションです。各種コンプライアンス要件に対応するだけでなく、さまざまな用途にも役立てることができます。以下のような要件を満たすためにもSplunkを活用できます。

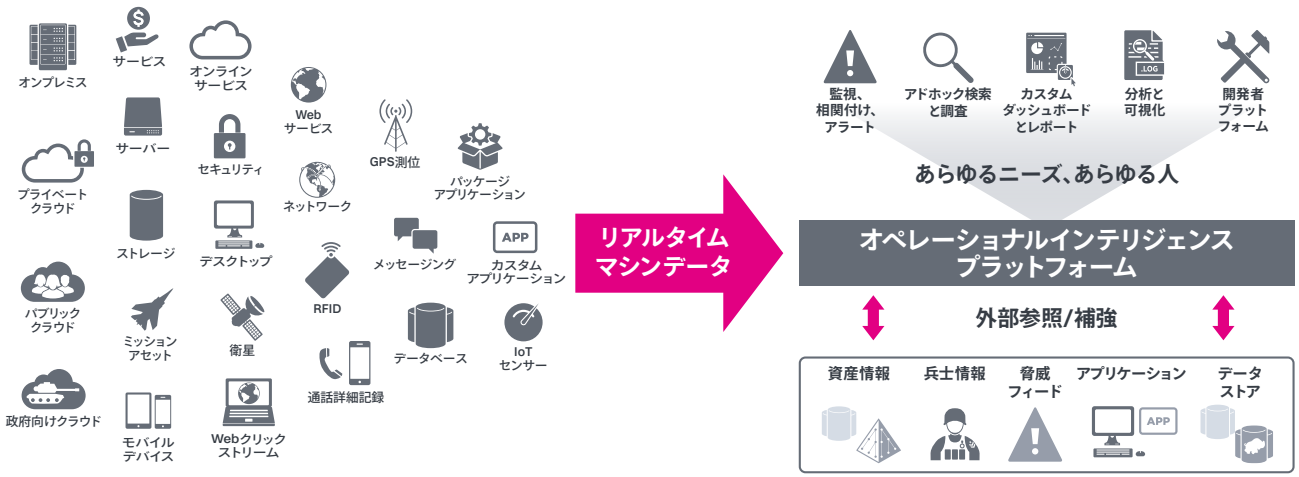
- セキュリティコントロールとその有効性を継続的に監視
- 監査証跡を収集してレポートを作成
- セキュリティコントロールの妥当性をリスクレベルの観点で判定
- コントロールの実装と有効性の評価
- あらゆる資産とアクティビティのログを収集、保持、検索し、アラートとレポートを生成

Splunkを利用することで、公共機関は自らが持つデータにアクセスして解釈し、公共機関としての透明性を確保できます。レポートやダッシュボードを簡単に作成でき、実装やその有効性をリアルタイムで可視化できるため、監査をよりシンプルに行うことができます。

Splunkの独自性は、組織全体のあらゆるソース、あらゆる形式のマシンデータを収集し、強力な可視化機能を備えた直感的なインターフェイス1つでそのデータを検索および分析できるところにあります。マシンデータには、ユーザー、住民、トランザクション、アプリケーション、サーバー、ネットワーク、モバイルデバイス、センサーなどのすべてのアクティビティや行動が明確に記録されています。ログだけでなく、設定、APIからのデータ、メッセージキュー、通話の詳細な記録、センサーデータも含まれています。RMFの導入を促進および円滑化するためのSplunkの主な機能は以下のとおりです。

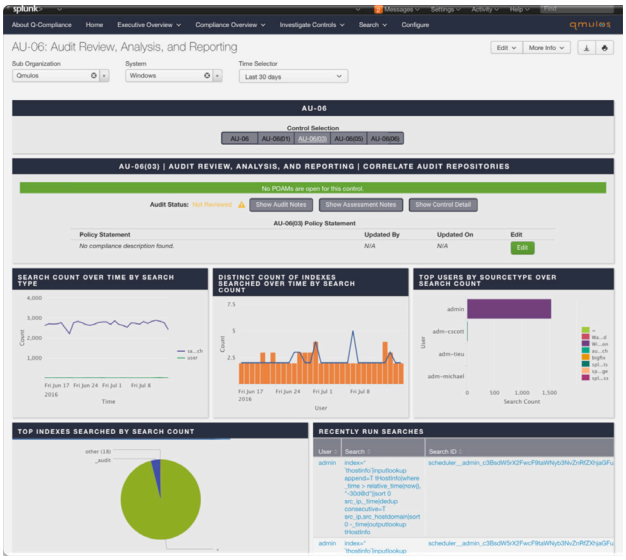
- 1日のデータ量がメガバイト級でもペタバイト級でも迅速に取り込み
- 1つのソースからでも数万のソースからでも、種類や形式を問わず、マシンデータを高い信頼性で収集してインデックスを作成
- 情報サイロを横断するエンドツーエンドのリアルタイムな可視性を単一のインターフェイスで提供
- 強力なサーチ機能で、すべてのデータを検索および分析
- 強力なレポート機能と可視化機能を提供

セキュリティコントロールを導入したら、許容可能なリスクレベルを決定する必要があります。Splunkはこのさまざまなセキュリティコントロールからマシンデータを収集できるため、リスク評価に使用できるだけでなく、データ中心のセキュリティ機能のすべてを1カ所に統合できます。



システムを認定したら、その後はセキュリティコントロールの監視を継続的に行う必要があります。これはSplunkの中核をなす機能です。RMFには反復的な要素が含まれているため、継続的監視が必要です。また、RMFのアプローチでは自動化ツールで合理化することが好ましいと考えられていますが、Splunkを使用すればマシンデータの収集、監視、アラート生成を自動化できます。

Splunkを使用すると、セキュリティイベントの監視を自動化するための要件を満たすことができます。ファイアウォール、アプリケーション、アクセス制御、IDS、その他のコンポーネントに関する監査証跡をインデックスして保存しておけば、あとはサーチのスケジュールとアラートルールを設定するだけです。アラートでは、メール、RSS、SMSを使用して通知を送信したり、スクリプトをトリガーしたりできます。既存のモニターコンソールとの統合も簡単です。新しい規制によって新しい監視要件が発生した場合でも、新しいデータソースとサーチを追加するだけで対応できます。



Splunk Assessment of Mitigation Implementations (SAMI)

サイバー脅威に対抗するため、そして傘下機関における適正な脅威軽減戦略の導入とセキュリティ体制の強化を支援するために、NSAの情報保証局(IAD)は「Top 10 Information Assurance Mitigation(情 報 保証のリスク軽減策トップ10)」という戦略リストを発行しました。各機関がこれらの戦略を適切かつ効果的に実装できるように、IADがSplunkを使用して開発したのが、SAMI (Splunk Assessment of Mitigation Implementations)というAppです。SAMIの目的は以下のとおりです。

- マシンデータを使用してリスク軽減策の実装を評価する
- 継続的な監視を通してリスク軽減策導入の進行状況を追跡する
- セキュリティ体制を追跡してレポートを生成する
- 設定のドリフト(差分)を特定する
- セキュリティ体制を強化するアクションを明確に示す

SAMIは、それぞれのリスク軽減策の実装に関するデータを監視し、推奨事項を優先度付きで返します。SAMIを使用することで、ネットワークにおけるリスク軽減策の実装状況を特定できます。また、継続的な監視によって改善を実証したり、リスク軽減策に悪影響を与える変更を特定したりすることもできます。各所見に対して望ましい対策がマッピングされ、問題を軽減するための対策の道筋が示されます。軽減策ごとに異なる施策が必要になるため、このSAMIの仕組みが実装面で大いに役立ちます。

行政機関でSplunkプラットフォームを使用すれば、可視性とインテリジェンスを取得し、コストの低減、セキュリティの強化、IT運用の合理化、コンプライアンスの確保、そして公共サービスの向上を実現できます。

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階
www.splunk.com/ja_jp
splunkjp@splunk.com

2020-Splunk-PF-Splunk-for-risk-management-framework-A4-JA-202012