# セキュリティ・コンプライアンス・モニタリング

近年のビジネス環境下で成功するためには、全世界の顧客やビジネス・パートナとのリアルタイムなコミュニケーションを持つことが必要不可欠といえます。そのためにインターネット等のオープンネットワークシステムを活用することが当然のごとく行われていますが、ただメリットだけを享受することはできず、セキュリティ・リスクもまた十分に考慮する必要が発生します。

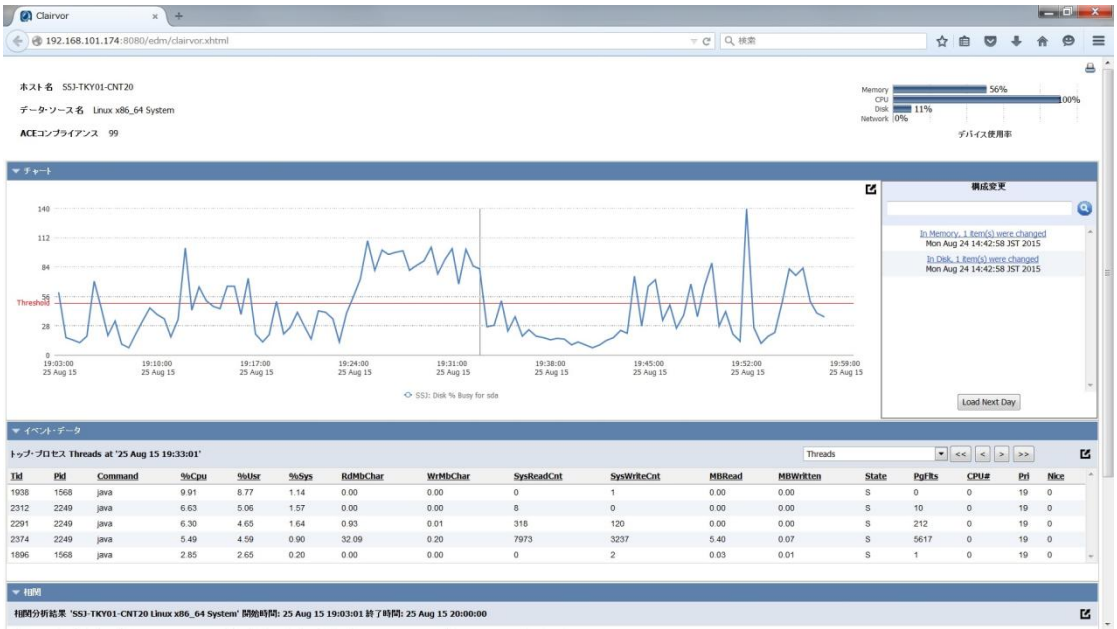
ファイアウォールやアンチ・ウイルス/マルウェア・ソフトウェア、侵入検知システム等の利用は、重要かつ必要不可欠なセキュリティ対策ですが、IT システム・インフラストラクチャやネットワークシステムの脆弱性を事前に検知することを役割とはしていません。近年のサイバー攻撃は、IT システム・インフラストラクチャやネットワークシステムの脆弱性部分に対して直接の攻撃を仕掛けてきます。

セキュリティ・コンプライアンス・モニタリングは、IT システム・インフラストラクチャやネットワークシステムの脆弱性を事前に検知し対策を可能とします。このソリューションにより、受動的なサイバーセキュリティ攻撃への対策から、能動的な対策へと進化することが可能となります。

## 予兆検知や根本問題分析の自動化が可能なセキュリティ・レイヤ

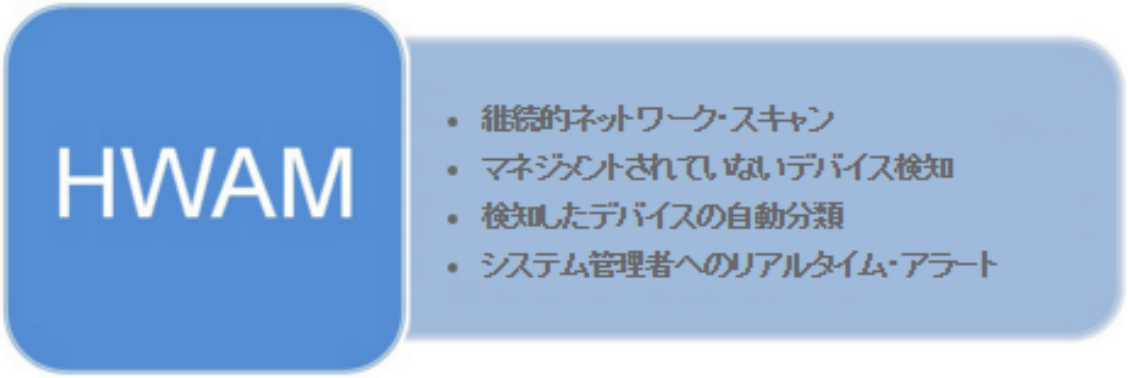
近年のクラウド環境の急速な普及により、アプリケーションの稼動する環境もクラウド化が進んでいます。企業はオンプレミスと同様にクラウド環境に対してもセキュリティとコンプライアンスの必要性を認識しています。

自動化されたリアルタイムの可視化と継続的なセキュリティとコンプライアンスに対してのポリシー施行/実施を実行することにより、これらの課題を解決します。セキュリティ・コンプライアンス・モニタリングとリアルタイム・パフォーマンス・モニタリングを統合することにより、既存の認知されている全ての脅威を認識することに加え、未知なる脅威に対しても事前に対策することができ、さらに通常とは逸脱した挙動からの潜在的な脅威を予兆検知や根本問題分析の自動化が可能なセキュリティ・レイヤを IT システム・インフラストラクチャ全体に追加することができます。




Java や Jboss のバージョンの変更、XML のコンフィグレーション・ファイルの変更、ポリシー違反したソフトウェアバージョンがパフォーマンスにどのように影響をするかを調べることができます。

## ハードウェア・アセット・マネジメント(ハードウェア資産管理)(HWAM)




セキュアに構築された IT システム・インフラストラクチャも許可されていない、あるいは不正なハードウェアやデバイスの接続により、安全性に脅威を及ぼす危険性があります。SightLine は継続的なネットワーク・スキャンの自動化を行うことにより、この脅威を予防します。

**継続的なネットワーク・スキャン**
マネジメント対象システムを継続的にネットワーク・スキャンを行い、許可されていないハードウェアやマネジメント対象外のハードウェアを検出することができます。

- ハードウェア/デバイス・タイプ
- 製造元
- モデル
- OS プラットフォーム
- パッチ・レベル
- etc...

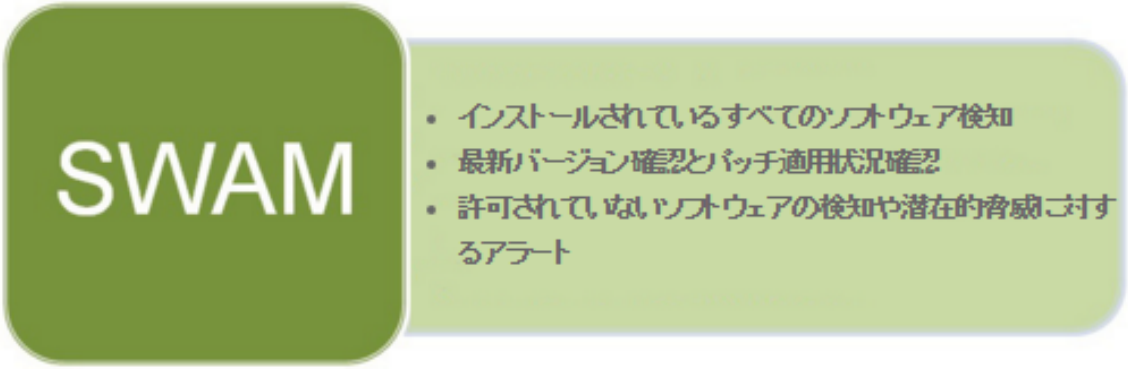
**未知のハードウェア/デバイス検出**
エンドポイント・デバイス上に特別なエージェントや構成を必要とせず、リモート・エージェントレス・スキャンを実行します。これによりマネジメント対象外のハードウェア/デバイスを検出することが可能となります。

**対象ハードウェア/デバイス**
物理、仮想やクラウド・ベース・インスタンスいずれのハードウェア/デバイスを対象とします。

- Windows、Linux、UNIX サーバ
- スイッチ
- ルータ
- ファイアウォール
- ロード・バランサ
- UTM
- etc...

**管理者への即時アラート**
未知のハードウェア等のデバイスが検出された場合、自動的に管理者(システム・アドミニストレータ)へアラート通知を行います。管理者は必要に応じて調査をおこない迅速な行動を取ることができます。さらに検出したデバイスの詳細情報の取得を試みます。

## ソフトウェア・アセット・マネジメント(ソフトウェア資産管理)(SWAM)




セキュアに構築された IT システム・インフラストラクチャも許可されていない、あるいは不正なソフトウェアや必要なソフトウェアやパッチを適応していないことにより、安全性に脅威を及ぼす危険性があります。SightLine は継続的なネットワーク・スキャンの自動化を行うことにより、この脅威を予防します。

**ソフトウェア・アセット情報の検出**
ソフトウェア・アセット情報を自動検出します。

- ソフトウェア名称
- バージョン
- 開発元
- インストール・パス
- インストール日付
- etc...

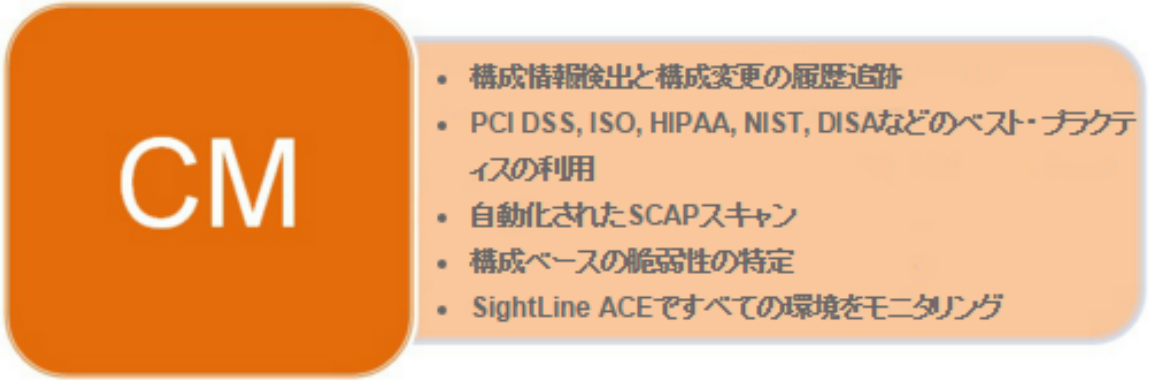
**アプリケーション・インストール/特定バージョンの自動検出**
アプリケーションがインストールされたり、特定のバージョンのアプリケーションが IT システムのサーバーに存在したときにアラート発生を行うことができます。

**脆弱性の存在するソフトウェア自動検知**
既知の脆弱性の存在するバージョンのソフトウェアが IT システムのサーバーに存在したときにアラート発生を行うことができます。

**必要ソフトウェアやパッチの確認**
サーバー上に必要であるべきソフトウェアのインストール状況を確認することができます。また、必要なパッチが適応されていない場合も検知することが可能です。

**カスタマイズ**
ユーザ作成アプリケーションや、IT システムに固有な目的のため、検出対象や方法をカスタマイズすることが可能です。

## コンフィグレーション・マネジメント(構成管理)(CM)




コンフィグレーションが適正でないサーバやネットワーク・デバイスは、多くのセキュリティやパフォーマンス問題の根本問題になる可能性があります。不適正なコンフィグレーションや、必要なパッチを適応していない場合に IT システム・インフラストラクチャに脆弱性をともなう危険性が発生する傾向があります。

不適正あるいは適正でないコンフィグレーションの範囲は不正なソフトウェアバージョンから XML ベースのコンフィグレーション・ファイルの不適切なパラメーター設定にまで広範囲にわたります。

**情報検出/変更の履歴追跡**
コンフィグレーション情報検出とコンフィグレーション変更の履歴追跡を行うことができます。

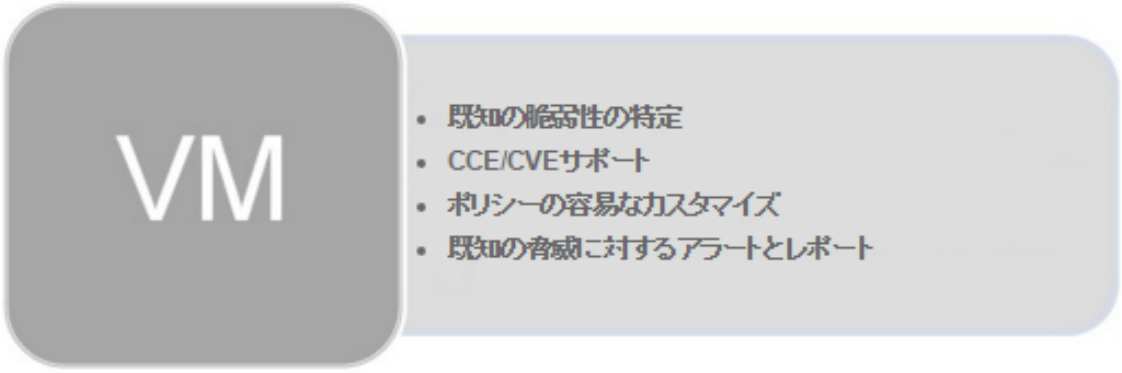
**ベスト・プラクティスの利用**
NIST および DISA 勧告に基づいたベスト・プラクティス・テンプレートを利用可能です。

**広範囲なハードウェア/デバイスタイプのカバレッジ**
Windows、Linux および UNIX サーバ、ESX ハイパーバイザー、スイッチ、ルータ、ロード・バランサなどのネットワークデバイスを含む幅広いハードウェア/デバイスを対象としています。

**カスタマイズ**
ユーザ作成やまたは専用ソフトウェアのコンフィグレーションに対して、独自のポリシーを設定することが可能です。

**SCAP スキャン**
SCAP に準じた自動化スキャンをサポートしており、OVAL や XCCDF ベースのポリシーを活用することができます。

## バルネラビリティ・マネジメント(脆弱性管理)(VM)




バルネラビリティ・マネジメントとは、ソフトウェアとハードウェアネットワーク上の IT システムに存在する脆弱性発見と改善/対策です。主要ハードウェア/ソフトウェア・プラットフォームや多くのアプリケーション対して、自動的に既存の脆弱性をスキャンすることが可能です。

**脆弱性スキャン**
Windows、UNIX および Linux サーバーに対して脆弱性スキャンを行うことによりの既知の脆弱性問題の特定/アラートが可能です。

**カスタマイズ**
ユーザ・アプリケーションや、特定の用途に対応するために、脆弱性スキャンをカスタマイズすることが可能です。

**CVE(共通脆弱性識別子)サポート**
CVE をサポートしているため、既存の脆弱性データベースより該当する改善対策や重症度と症状の最新情報を閲覧することができます。

## セキュリティ設定共通化手順 SCAP 対応

NIST(アメリカ国立標準技術研究所), DISA(アメリカ国防情報システム局), HIPAA, SOX が定義したベストプラクティスのセキュリティ設定を活用することができます。
SCAP 標準仕様のチェックリストを記述するための XCCDF(セキュリティ設定チェックリスト記述形式)や脆弱性やセキュリティ設定をチェックするための OVAL(セキュリティ検査言語)を利用して、ユーザカスタマイズのセキュリティポリシー定義をおこなえます。
脆弱性を識別するための CVE(共通脆弱性識別子)をサポートしているため NVD(National Vulnerability Database)等の脆弱性情報データベースを活用することが可能です。

## 参考 URL

独立行政法人 情報処理推進機構によるセキュリティ設定共通化手順 SCAP(Security Content Automation Protocol)等の概説
～情報セキュリティ対策の自動化と標準化を実現する技術仕様～

セキュリティ設定共通化手順 SCAP 概説:
https://www.ipa.go.jp/security/vuln/SCAP.html
セキュリティ検査言語 OVAL 概説:
https://www.ipa.go.jp/security/vuln/OVAL.html
セキュリティ設定チェックリスト記述形式 XCCDF 概説:
http://www.ipa.go.jp/security/vuln/XCCDF.html
共通脆弱性識別子 CVE 概説:
https://www.ipa.go.jp/security/vuln/CVE.html

日本サイトラインシステムズ株式会社
〒105-0014 東京都港区芝 2-29-10
ユニゾ芝二丁目ビル 3F
http://www.sightlinesystems.co.jp/
http://blog.sightlinesystems.co.jp/
http://www.facebook.com/SightLineSystemsJapan/
https://www.google.com/+SightlinesystemsCoJpPlus/
https://twitter.com/sightlinejapan/
http://www.youtube.com/user/SightLineSystemsJP/