NISTサイバーセキュリティ・フレームワークへの準拠

米NIST(アメリカ国立標準技術研究所)は米国政府機関がデータシステムのコンプライアンスに従うべき運用や業務の標準、またはガイドラインの為にRMF(リスク管理フレームワーク)を策定しています。
NISTによればこのような標準やガイドライン及びベストプラクティスは、サイバーセキュリティ関連のリスク管理の本質ともいうべきものだそうです。
サイバーセキュリティ・フレームワーク(訳注1)の優先度付けされた柔軟で費用対効果の高いアプローチは、重要なインフラ基盤だけでなく、経済及び国家保障の重要分野に対する防御と回復力の促進に有効です。

各機能はフレームワーク中の最上位の概念です。これらはフレームワーク中の他の全要素を系統づける「中核の支え」として働きます。
これらの5つの機能は効果的かつ統合的なサイバーセキュリティ・プログラムの5本の柱を表します。また企業がサイバーセキュリティのリスクを高いレベルでありながら容易に表示したり、リスク管理の決定を下せるように支援します。

SentinelOne Endpoint Protection Platformは機械学習と自動化により強化された専用のシングルエージェントに、防御と検知、対処の機能を統合しています。SentinelOne Endpoint Protection Platformはあらゆる攻撃に対する防御と検知、完全に自動化された素早い脅威排除、ポリシーベースの対処能力、そしてリアルタイムフォレンジックとフルコンテキストによる端末環境の完全な可視化を提供します。

(訳注1) サイバーセキュリティ・フレームワーク
NIST Cybersecurity Framework Version 1.1 (April 2018)
Framework for Improving Critical Infrastructure Cybersecurity
原文 https://www.nist.gov/cyberframework/framework
対訳 https://www.ipa.go.jp/security/publications/nist/

SentinelOneにできること

SentinelOneのSentinelOne Endpoint Protection Platformは、端末に関する企業のセキュリティ体制がリスクガイドラインのベストプラクティスに合致するよう、これら5つの機能に対応しています。
以下の表はNISTフレームワーク「中核」の5つの機能に対するSentinelOneの対応内容となります。

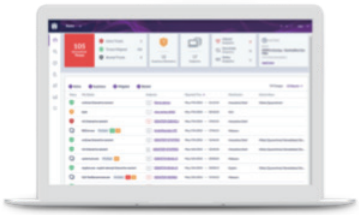
機能	SentinelOneの対応
特定  特定機能は、システムや社員、資産、データ、そして能力に対するサイバーセキュリティのリスクを管理し、組織的な理解を確立するために有用です。 ビジネス状況や重要な機能を支援するリソース、それらに関連するサイバーセキュリティリスクへの理解が、企業のそれらの取り組みに対し集中したり優先順位付けを行ったり、リスク管理戦略やビジネス要求へ合致させることを可能にします。	SentinelOneはアプリケーション・脆弱性リスクスコアによりこの要求を解決します。SentinelOneエージェントは、スキャンすることなく、全管理端末から全てのアプリケーションインベントリを自動収集しアプリケーションのバージョンと既知の脆弱性とを照合します。 このディスカバリ機能は企業内のリスク特定を自動化することによりリスク管理体制を即座に強化し、パッチ管理の仕組みを優先度付けし、効果的に働くようにします。 SentinelOneは更に感染端末やユーザーを自動的に特定します。企業は誰が影響を受けているのかをピンポイントで把握することが可能です。
防御  防御機能は、重要なインフラサービスを確実に提供するための適切な対策の概略です。 防御機能は、潜在的なサイバーセキュリティインシデントの影響を制限または遮断するための機能を支援します。	SentinelOneはWindowsやMac、Linux端末を多様な攻撃から防御することに特化しています。 例えば、ファイル形式のマルウェア、スクリプトベースの攻撃、エクスプロイト、インメモリ攻撃、セロデイキャンペーン等です。 SentinelOneはこの比類無いレベルの防御機能をシングルエージェント内のマルチAIモデルで実現しています。 これによりSentinelOneはファイル実行前に検知してブロックし、危険なプロセスを実行時に特定し停止します。 これらの多層防御は全ての端末において深いレベルの防衛をもたらします。 またSentinelOneはデバイス制御とファイアウォールコントロールも提供します。 これにより不要なUSBの接続や未承認のネットワーク接続を制御できます。

機能	SentinelOneの対応
検知  検知機能は適切な挙動を定義しておき、サイバーセキュリティイベントの発生を特定します。検知機能はサイバーセキュリティイベントをタイムリーに見つけることができます。	SentinelOneは脅威がどのように到達したかにかかわらず、組織内の端末環境全てにわたって攻撃を自動検知します。エージェントが複数の検知エンジンでディスクに書かれるファイルをスキャンするだけでなく、動的AIエンジンで実行プロセスを監視してシステム上で実行される最新の攻撃を検出します。 SentinelOneのActive EDRは、90日間に渡るコンテキスト化された端末のフォレンジックデータにより脅威内容を特定します。 これはSentinelOneの自動脅威検知を補完する有用な可視化情報として利用出来ます。 SentinelOne VigilanceはSentinelOne社の熟練セキュリティ分析官が24時間365日で高度なレベルの脅威監視を提供するMDRサービスです。
対応  対応機能は、検出したサイバーセキュリティインシデントに対処するための適切なアクションを意味します。また潜在的なサイバーセキュリティインシデントの影響を封じ込める機能も提供します。	SentinelOneは効果的な対応操作を、特許取得済みの端末修復機能で提供します。SentinelOneエージェントは感染端末内のマルウェアによる変更箇所を特定し、ワンクリックでクリーンな状態に戻します。これにより攻撃された端末の原状回復時間は大幅に短縮が可能です。 SentinelOneはさらに端末への完全なリモートシェル機能を提供し、迅速かつ効果的に更なる対応作業を始めることができます。 SentinelOne VigilanceはSentinelOne社の熟練セキュリティ分析官が24時間365日で高度なレベルの対応作業を提供するMDRサービスです。 検出された脅威の全てに対して、いついかなる時間にも対応します。
復旧  復旧機能は、復旧計画を維持し、サイバーセキュリティインシデントにより損なわれた機能やサービスを復旧させるための適切な行動を特定します。 復旧機能は、通常運用への迅速な復旧をサポートし、サイバーセキュリティインシデントの影響を最小限とします。	SentinelOneはロールバックという復旧機能を提供します。ロールバックはWindows端末を攻撃以前の状態に復旧しますが、機器の回復だけでなく、ファイルシステム情報も自動回復してくれます。 例えばランサムウェアなどの攻撃に対しても、文字通り「巻き戻し」することにより、感染端末を運用可能な状態にします。

すべての面における優位性

他の製品と異なり、SentinelOneは統合された専用エージェントであり、最新のWindowsからXPまで、10種類以上のLinuxディストリビューション、そしてmacOSもサポートします。

あらゆる OS	あらゆる デプロイメント方式	あらゆる コネクション状態	あらゆる 連携	あらゆる 利用者	あらゆる 対応
Windows	Cloud	Online	300+ APIs	Big team	Automated
Linux	GovCloud	Offline		One person	
macOS	On-prem			No team	
Virtualization	Hybrid				



製品詳細や検証（PoC）のご相談はこちら > https://cn.teldevice.co.jp/product/sentinelone/form.html

※原文：SentinelOne、翻訳：SentinelOne代理店 東京エレクトロンデバイス

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/

新宿：〒163-1034 東京都新宿区西新宿3-7-1 新宿パークタワー S34階
Tel.03-5908-1990　Fax.03-5908-1991

つくば：〒305-0033 茨城県つくば市東新井15-4 関友つくばビル7階
Tel.029-848-6030　Fax.029-848-6035

名古屋：〒451-0045 愛知県名古屋市西区名駅2-27-8 名古屋プライムセントラルタワー8階
Tel.052-562-0826　Fax.052-561-5382

大阪：〒540-6033 大阪府大阪市中央区城見1-2-27 クリスタルタワー33階
Tel.06-4792-1908　Fax.06-6945-8581

Dec 2019