RSA NETWITNESS® PLATFORM

# NetWitness Endpointクイック スタート ガイド

RSA NetWitness® Platform 11.3

## 連絡先情報

RSA Link( https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

## 商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

## 使用許諾契約

本ソフトウェアと関連ドキュメントは、Dellが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

## サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Link の製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

## 暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

## 配布

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

6月 2019

# NetWitness Endpointとは？

RSA NetWitness Endpointは、ネットワーク内のエンドポイントの動作を継続的に監視し、実行プログラムとプロセスの詳細を可視化して分析するためのEDR(エンドポイント検出/対応)ツールです。RSA NetWitness Endpointにより、新型、未知、標的型の各種攻撃を検出し、調査が必要な不審なアクティビティを特定し、異常な動作を解明し、セキュリティ侵害の範囲を特定できます。これにより、アナリストは高度な脅威に迅速に対応できるようになります。

## 本書について

このガイドでは、NetWitness Platform Endpointを構成し、Endpointの機能を使用するためのエンドツーエンドの手順を説明します。

## RSA Link上のRSA NetWitness Platform 11.3のドキュメント

NetWitness Platformの製品ドキュメントは、機能ラインに沿って編成されています。特定のガイドまたはバージョンをお探しの場合は、「バージョン11.x マスター目次」を参照してください。

RSA NetWitness Platform 11.3のドキュメントは次のリンクからアクセスできます。同じドキュメントが2つの形式で提供されます。

- HTML形式のガイドは、現在サポート対象の11.xバージョンの最新情報を提供します: RSA NetWitness Platform 11.xドキュメント
- PDF形式のガイドは、特定のバージョンの情報を提供します: RSA NetWitness Platform 11.3 PDFドキュメント

ソフトウェアのバージョンに関係ないドキュメントは次のリンクからアクセスできます。

- ハードウェア セットアップ ガイド: https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- フィード、パーサ、アプリケーション ルール、レポートなどのRSAコンテンツに関するドキュメント: https://community.rsa.com/community/products/netwitness/rsa-content

## はじめに

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
|  | |

| 説明 | 参考情報 |
| --- | --- |
| 製品の更新、改善、既知の問題に関する情報を確認します。 | リリース ノート |
| NetWitness Endpointについて理解します。 | 『*Netwitness Platformスタート ガイド*』の「NetWitness Platformの概要」および「調査」 |

## セットアップとインストール

### 新規インストール

次のタスクは、リストに記載された順序で実行する必要があります。

| 説明 | 参考情報 |
| --- | --- |
|  | |
| Endpoint Log Hybridのライセンスを取得します。 | ライセンス管理ガイド |
| サポート対象のハードウェアを確認します。 | 『*物理ホスト インストール ガイド*』の「サポート対象のハードウェア」 |
| NetWitness Endpointのアーキテクチャを確認します。エンドポイントの数、分布、場所に基づいて導入を計画します。次のいずれかを選択します。<br>• 単一のEndpoint Server<br>• 複数のEndpoint Server | 『*導入ガイド*』の「NetWitness Endpointのアーキテクチャ」 |
| ファイアウォールでポートを構成します。 | 『*導入ガイド*』の「ネットワーク アーキテクチャとポート」 |
| NetWitness Serverおよびその他のコンポーネントをインストールします。<br>単一のEndpoint Serverを導入する場合は、NetWitness Server、Endpoint Log Hybrid、およびESAをインストールする必要があります。<br>複数のEndpoint Serverの場合は、前述のコンポーネントに加えて、追加のEndpoint Log Hybrid、NetWitness Broker( Endpoint Brokerを含む) をインストールする必要があります。 | 物理ホストのセットアップ手順:『*物理ホスト インストール ガイド*』<br>仮想ホストのセットアップ手順:『*仮想ホスト インストール ガイド*』 |

| 説明 | 参考情報 |
| --- | --- |
| Endpoint Log Hybridをインストールします。 | 『*物理ホスト インストール ガイド*』の「RSA Netwitness Endpoint」 |
| インストールされたサービスを確認します。 | *ホストおよびサービス スタート ガイド* |
| **注**：デフォルトのポリシーを確認し、必要に応じて変更します。<br>ホストにEndpointエージェントをインストールします。 | 『*Endpoint構成ガイド*』の「エンドポイント ソース」トピック<br>*NetWitness Endpointエージェント インストール ガイド* |

### アップグレード

次のタスクは、リストに記載された順序で実行する必要があります。

| 説明 | 参考情報 |
| --- | --- |
|  | |
| 10.6.5から11.3へのアップグレード<br>NetWitness Platform 11.3へのアップグレード後に、Endpoint Log Hybridとその他のEndpointコンポーネントをインストールします。 | 物理ホストのアップグレードに関する手順：『*物理ホスト アップグレード ガイド*』<br>仮想ホストのアップグレードに関する手順：『*仮想ホスト アップグレードガイド*』 |
| 11.xから11.3への更新<br>Endpoint Serverとエージェントを更新します。 | *更新ガイド* |
| Endpointエージェントを11.1.xまたは11.2.xから11.3に更新します。 | 『*Endpointエージェント インストール ガイド*』の「エージェントのアップグレード」 |
| NetWitness Endpoint 4.4.0.xをNetWitness Platformに移行します。 | 『*NetWitness Endpoint 4.4.0.xからRSA NetWitness Platform 11.3への移行ガイド*』 |

## 構成

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
|  | |

| 説明 | 参考情報 |
| --- | --- |
| NetWitness Endpointと構成に必要なタスクの概要を理解します。 | 『*Endpoint構成ガイド*』の「Netwitness Endpointの概要」と「Endpoint Serverの構成」 |
| エージェントのグループとポリシーを確認します。 | 『*Endpoint構成ガイド*』の「エンドポイント ソース」トピック |
| RSA Liveアカウントをセットアップし、Endpoint用のESAコンテンツとアプリケーション ルールが使用可能であることを確認します。<br>**注**：RSA Liveのファイル レピュテーション サービスは、自動的に有効になります。 | *Liveサービス管理ガイド* |
| RBAC(ロール ベースのアクセス制御)を構成します。 | 『システム セキュリティとユーザ管理ガイド』の「*ロールの権限*」 |
| データ保存ポリシーを構成します。 | 『*Endpoint構成ガイド*』「データ保存の構成」 |
| 非アクティブなエージェントを管理します。 | 『*Endpoint構成ガイド*』の「非アクティブなエージェントの管理」 |

## 調査

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
|  | |
| 調査の仕組みを理解します。 | 『*NetWitness Investigateユーザ ガイド*』の「NetWitness Investigateの仕組み」 |
| [調査]ビューを構成します。 | 『NetWitness Investigateユーザ ガイド』の「NetWitnessの[調査]ビューと環境設定*の構成*」 |
| さまざまな[調査]ビューで調査を開始します。 | 『NetWitness Investigateユーザ ガイド』の*「調査の開始」* |
| ファイルおよびホストの調査に関するベスト プラクティスを確認し、[調査]ビューをセットアップします。 | 『*Netwitness Endpointユーザ ガイド*』の「ファイルの調査」および「ホストの調査」の「ベスト プラクティス」セクション |
| ファイルを調査します。 | 『*Netwitness Endpointユーザ ガイド*』の「ファイルの調査」 |
| ホストを調査します。 | 『*Netwitness Endpointユーザ ガイド*』の「ホストの調査」 |

| 説明 | 参考情報 |
| --- | --- |
| プロセスを調査します。 | 『*Netwitness Endpointユーザ ガイド*』の「ホストの調査」 |
| ダウンロードしたファイルを分析します。 | 『*Netwitness Endpointユーザ ガイド*』の「ダウンロードされたファイルの分析」 |
| ファイルのステータスを変更して修正します。 | 『*Netwitness Endpointユーザ ガイド*』の「ファイル ステータスの変更または改善」 |
| イベントを分析します。 | 『*Netwitness Endpointユーザ ガイド*』の「イベントの分析」<br>『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでのRAWデータとメタデータの分析」、「[ナビゲート]ビューでのメタデータの調査」、「[イベント]ビューでのRAWイベントの分析」 |

## 対応およびレポート

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
|  | |
| Endpointインシデントに対応します。 | 『*NetWitness Respondユーザ ガイド*』 |
| Endpointデータに関連するレポートを表示します。 | 『*レポート ユーザ ガイド*』 |

## メンテナンス

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
|  | |
| 稼働状態を監視します。 | 『システム メンテナンス ガイド』 |

## レガシーNetWitness Endpointの統合

次のタスクは、任意の順序で実行できます。

| 説明 | 参考情報 |
| --- | --- |
| |  |
| NetWitness Endpoint 4.4.xメタデータを NetWitness Platformで構成します。 | 『*Endpoint構成ガイド*』の「Netwitness Endpoint 4.4.0.2以降とNetwitness Platformの統合」トピック |
| NetWitness Endpoint 4.4.xとNetWitness Platformの運用の統合を構成します。 | 『*RSA NetWitness Endpoint統合ガイド*』 |