概要ガイド

Sentinel 7.0.1

March 2012

保証と著作権

NetIQ コーポレーション (“NetIQ”) は、本書の内容または本書を利用した結果について、いかなる保証または表明も行っておりません。また、本書の商品性、および特定の用途への適合性について、いかなる表明または黙示的保証も否認します。また、NetIQ は、本書を改訂し、その内容をいつでも変更する権利を留保します。NetIQ は、このような改訂または変更に関し、いかなる個人または事業体に通知する義務を負いません。

NetIQ は、すべてのソフトウェアについて、いかなる表明または保証も行っていません。また、ソフトウェアの商品性、または特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。NetIQ は、NetIQ 製ソフトウェアの一部または全部を変更する権利を常に留保します。NetIQ は、このような変更に関し、いかなる個人または事業体に通知する義務を負いません。

本契約の下で提供される製品または技術情報はすべて、米国の輸出管理規定およびその他の国の輸出関連法規の制限を受けます。お客様は、すべての輸出規制を遵守して、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。NetIQ は、お客様が必要な輸出承認を取得しないことについては、いなかる責任も負わないものとします。

Copyright (c) 2012 Novell, Inc. All rights reserved. 本ドキュメントの一部または全体を無断で複写転載することは、その形態を問わず禁じます。

サードパーティの商標は、それぞれの所有者に属します。

詳細については、NetIQ までお問い合わせください。お問い合わせ先は次のとおりです。

1233 West Loop South, Houston, Texas 77027
U.S.A.
www.netiq.com

目次

このガイドについて 5

1 Sentinel 製品の概要 7

1.1 セキュリティが重要な理由 . . . 7
1.2 IT 環境のセキュリティ保護の課題 . . . 7
1.3 Sentinel が提供するソリューション . . . 9

2 Sentinel の動作原理 11

2.1 イベントソース . . . 13
2.2 Sentinel イベント . . . 15
2.2.1 マッピングサービス . . . 15
2.2.2 マップのストリーミング . . . 16
2.2.3 エクスプロイト検出 (マッピングサービス) . . . 16
2.3 コネクタ . . . 16
2.4 コレクタ . . . 16
2.5 コレクタマネージャ . . . 17
2.6 通信バス . . . 17
2.6.1 メッセージバス . . . 17
2.6.2 チャネル . . . 18
2.7 Sentinel データストレージ . . . 19
2.8 フィルタ . . . 19
2.9 相関 . . . 20
2.10 セキュリティインテリジェンス . . . 20
2.11 iTRAC . . . 20
2.12 レポート . . . 21
2.13 イベント分析 . . . 21

このガイドについて

このガイドでは、WorkloadIQ 製品である Sentinel の概要を説明します。

対象者

このガイドは、情報セキュリティの専門家向けです。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用してください。

マニュアルの更新

『*Sentinel 7.0.1 概要ガイド*』の最新バージョンについては、NetIQ Sentinel マニュアルの Web サイト (http://www.novell.com/documentation/sentinel70) を参照してください。

その他のマニュアル

Sentinel テクニカルマニュアルは、次の分冊から構成されています。

- Sentinel クイックスタートガイド (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel インストールガイド (http://www.novell.com/documentation/sentinel70/s70_install/data/bookinfo.html)
- Sentinel 管理ガイド (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel ユーザガイド (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel リンク概要ガイド (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Sentinel 内部監査イベント (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Sentinel SDK サイトには、ご自分のプラグインを構築するための情報が提供されています。

Novell および NetIQ へのお問い合わせ

Sentinel は現在 NetIQ 製品ですが、Novell では引き続き製品サポートをしています。

- Novell Web サイト (http://www.novell.com)
- NetIQ Web サイト (http://www.netiq.com)

- 技術サポート (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- セルフサポート (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- パッチダウンロードサイト (http://download.novell.com/index.jsp)
- Sentinel コミュニティサポートフォーラム (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TID (http://support.novell.com/products/sentinel)
- Sentinel プラグイン Web サイト (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **電子メールお知らせリスト** Sentinel プラグイン Web サイトから登録してください。

セールスサポートへのお問い合わせ

商品、価格、機能についてのご質問は、ローカルパートナーへご連絡ください。ローカルパートナーとの連絡が取れない場合、セールスサポートチームへご連絡ください。

各国共通 : NetIQ 会社所在地 (http://www.netiq.com/about_netiq/officelocations.asp)

米国およびカナダ : 888-323-6768

電子メール : info@netiq.com

Web サイト : www.netiq.com

1 Sentinel 製品の概要

Sentinel は、セキュリティ情報とイベント管理のソリューションおよびコンプライアンスモニタリングソリューションです。Sentinel は、最も複雑な IT 環境を自動的にモニタリングし、IT 環境を保護するのに必要なセキュリティを提供します。

- 7 ページのセクション 1.1「セキュリティが重要な理由」
- 7 ページのセクション 1.2「IT 環境のセキュリティ保護の課題」
- 9 ページのセクション 1.3「Sentinel が提供するソリューション」

1.1 セキュリティが重要な理由

セキュリティは、コストを抑制し顧客の信頼を確保するため、今日の世界では会社にとって最大の関心事でなければなりません。レコードを流出すると各レコードにつき平均 200 ドルの損害が生じます。たった 1 回の侵害による 20 ～ 30 万レコードの流失でビジネスに重大な結果がもたらされます。

もし会社が攻撃されると、次の損失を被る可能性があります。

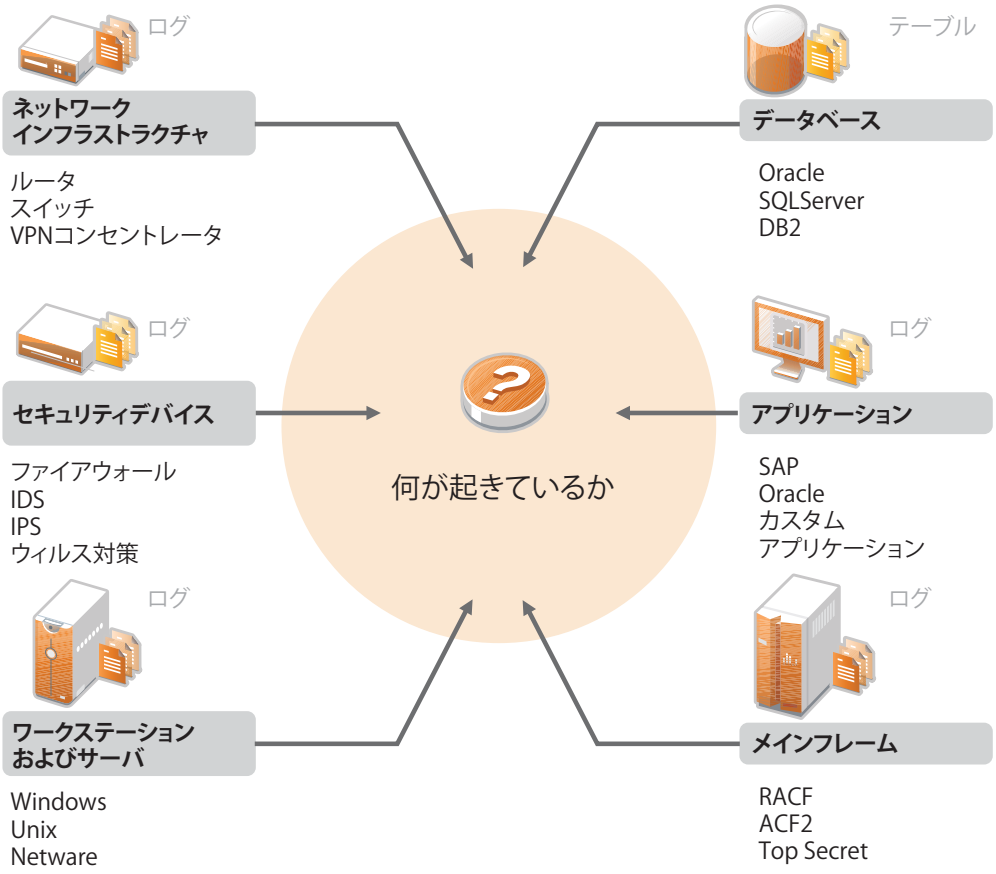
- 訴訟費用
- 調査費用と法廷費用
- 監査の増加
- 罰金と刑罰
- 顧客との間の信頼関係を失ったことによる隠れたコスト
- 信頼関係損失による顧客減少

これは、IT 環境をセキュリティ保護する重要性を示しています。今日の世界では、インターネットの使用、さらにはクラウド技術の使用の増加によって、内部関係者と部外者との間の境目があいまいになってきています。

1.2 IT 環境のセキュリティ保護の課題

IT 環境のセキュリティ保護は、環境が複雑であるため、困難です。多数の異なるアプリケーション、データベース、メインフレーム、ワークステーション、およびサーバがあり、それらすべてに発生しているイベントのログがあります。さらには、セキュリティデバイスとネットワークインフラストラクチャデバイスがあり、それらすべてに IT 環境で発生したことについてのログが含まれています。

図 1-1　環境で発生していること



困難をもたらす原因は次のとおりです。

- IT 環境に数多くのデバイスがある
- ログの形式が異なる
- ログがサイロ式に格納されている
- ログで生成される情報量
- すべてのログを手動で解析しなければ、誰が何を実行したか特定できない

有用な情報を得るためには、以下の機能が必要となります。

- データを収集する
- データを集約する
- 異なるデータを簡単に比較可能なイベントに正規化する
- イベントを標準規制に対応付けする
- データを分析する
- 複数のシステム間のイベントを比較し、セキュリティの問題があるかどうかを判断する
- データが基準を外れているときに通知を送信する

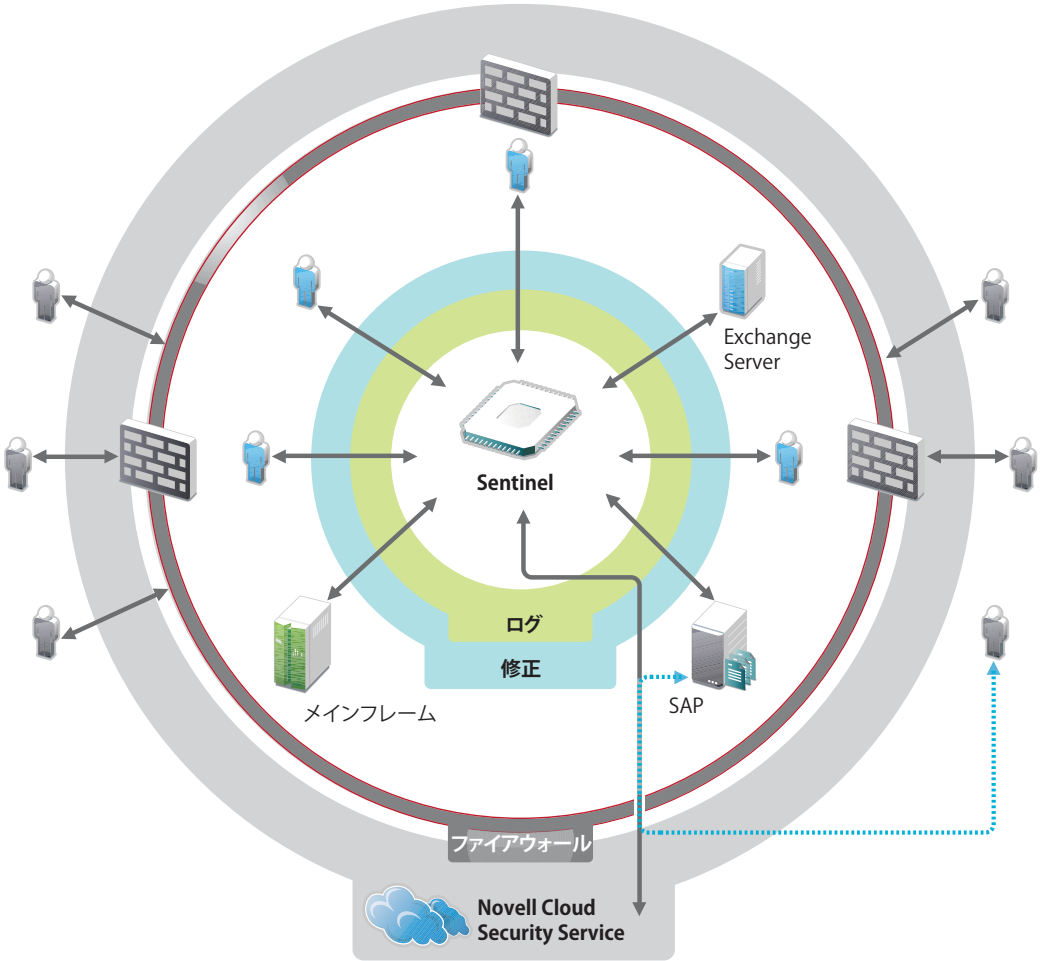
- ビジネスポリシーに従って通知に対する行動をとる
- コンプライアンスの証明のためにレポートを生成する

IT 環境をセキュリティ保護するうえでの課題を理解したら、ユーザのために、またユーザから企業をセキュリティ保護する方法を特定する必要があります。これは、ユーザを犯罪者として扱ったり、ユーザが生産的でなくなるような負荷を与えたりせずに行う必要があります。Sentinel がソリューションを提供します。

1.3 Sentinel が提供するソリューション

Sentinel は企業のセキュリティの中枢神経系として動作します。アプリケーション、データベース、サーバ、ストレージ、セキュリティデバイスなどのインフラストラクチャ全体からデータを取り込みます。データを分析して相関させ、データに自動または手動で対処できるようにします。

図 1-2 *Sentinel が提供するソリューション*



その結果、特定の時点で IT 環境に生じている重大事を判断することができ、リソースに対する操作とそれを行っている人物を結び付けることができます。これにより、ユーザの操作を特定し、コントロールを効果的に監視できます。その人物が内部者であるかに関係なく、行われる操作をすべて結びつけて、損害が発生する前に本当に危険な操作を明らかにすることができます。

Sentinel では、以下のコスト効率の高い方法でこれを実行します。

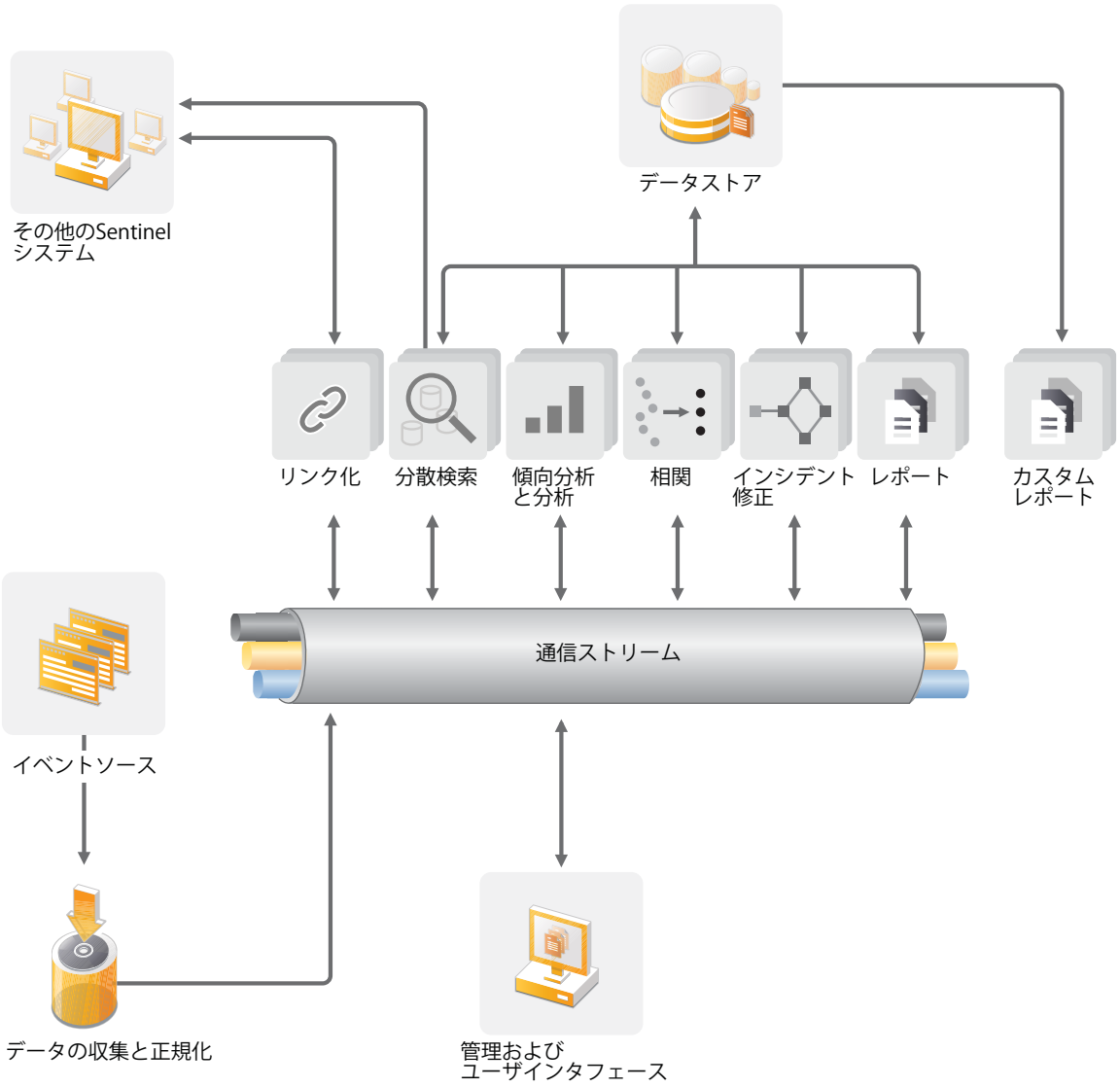
- 単一のソリューションを使用して、複数の規制にまたがる IT コントロールに対処する
- ネットワーク環境で行われるはずのことと実際に行われていることの間にある知識のギャップを埋める
- 組織でセキュリティコントロールに関する文書化、監視、報告を行っていることを監査担当者および監督機関に実証する
- すぐに使えるコンプライアンスモニタリングおよびレポーティングプログラムを提供する
- 組織のコンプライアンスプログラムおよびセキュリティプログラムの有効性を継続的に評価するために必要な可視性とコントロールを得る

Sentinel では、ログの収集、分析、およびレポーティングプロセスが自動化されるので、IT コントロールが効果的に脅威の検出と監査要件をサポートします。Sentinel では、セキュリティイベント、コンプライアンスイベント、IT コントロールの自動モニタリングが提供されているため、セキュリティ違反またはコンプライアンス違反イベントが発生した場合に、即座に対処することができます。また、Sentinel では、環境に関するサマリ情報を簡単に収集できるため、セキュリティに対する全般的な方針を重要な利害関係者に伝達できます。

2 Sentinel の動作原理

Sentinel では、IT 環境全体のセキュリティ情報とイベントを継続的に管理することで、完全なモニタリングソリューションを提供します。次の図は、Sentinel がどのように動作するのかを示しています。

図 2-1 *Sentinel の動作原理*



Sentinel は以下のように動作します。

- IT 環境におけるすべての異なるイベントソースからログ、イベント、およびセキュリティ情報を収集する
- 収集したログ、イベント、およびセキュリティ情報を共通の形式に正規化する
- 正規化された情報を、1 秒あたり数千のメッセージパケットを移動できるメッセージバスに追加する
- スケーラビリティのためにメッセージバスを介してすべてのSentinelコンポーネントと通信する

この時点で、各 Sentinel コンポーネントがメッセージバスにアクセスし、Sentinel は以下の機能を実行します。

- 柔軟でカスタマイズ可能なデータ保持ポリシーを使用して、ファイルベースのデータストアにイベントを格納します。
- Sentinel Log Manager、Sentinel、Sentinel Rapid Deployment などの複数の Sentinel システムを階層的にリンクする機能を提供します。
- ローカルの Sentinel サーバはもとより、世界中に分散している Sentinel サーバでもイベントを検索できる機能を提供します。
- 統計分析を実行してベースラインを定義し、次にベースラインと発生中の事象を比較し、未知の問題が発生していないかどうかを判断します。
- 指定された期間の類似または比較可能なイベントのセットを相関させて、パターンを特定します。
- 対応管理および追跡を効率的に行うため、イベントをインシデントにまとめます。
- リアルタイムおよび履歴イベントに基づいて機能をレポートします。

以降のセクションでは、Sentinel のコンポーネントについて詳しく説明しています。

- 13 ページのセクション 2.1「イベントソース」
- 15 ページのセクション 2.2「Sentinel イベント」
- 16 ページのセクション 2.3「コネクタ」
- 16 ページのセクション 2.4「コレクタ」
- 17 ページのセクション 2.5「コレクタマネージャ」
- 17 ページのセクション 2.6「通信バス」
- 19 ページのセクション 2.7「Sentinel データストレージ」
- 19 ページのセクション 2.8「フィルタ」
- 20 ページのセクション 2.9「相関」
- 20 ページのセクション 2.10「セキュリティインテリジェンス」
- 20 ページのセクション 2.11「iTRAC」
- 21 ページのセクション 2.12「レポート」
- 21 ページのセクション 2.13「イベント分析」

2.1 イベントソース

Sentinel では、IT 環境における多数の異なるソースからセキュリティ情報とイベントを収集します。このようなソースはイベントソースと呼ばれます。イベントソースはネットワーク上に存在する各種アイテムであったりします。

次の図は、Sentinel が情報を収集できる各イベントソースの一部について示しています。

セキュリティの境界 : お使いの環境向けのセキュリティパラメータを作成するために使用するデバイスおよびソフトウェア。

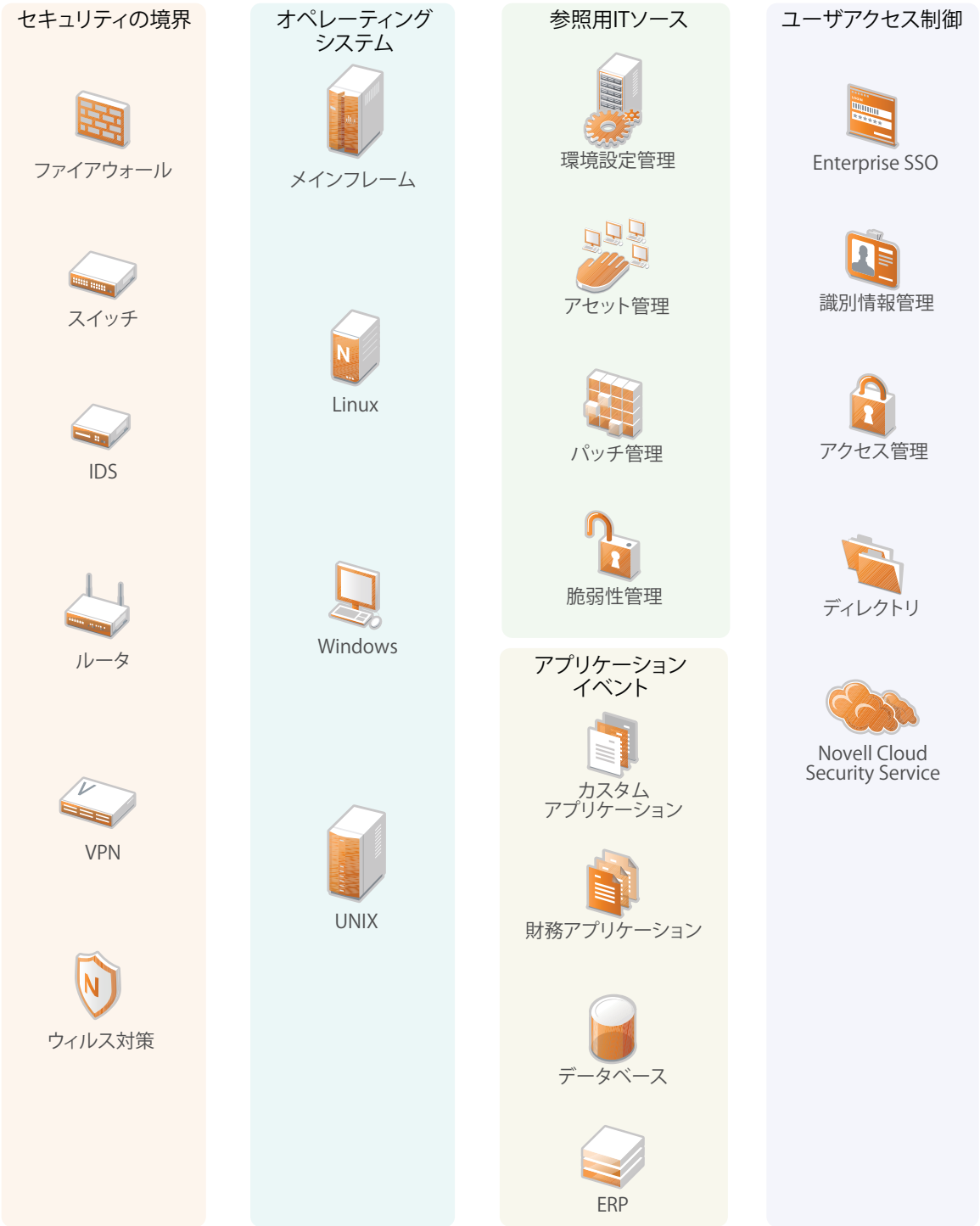
オペレーティングシステム : ネットワークで稼動中の各オペレーティングシステムからのイベント。

参照用 IT ソース : アセット、パッチ、環境設定、および脆弱性を維持および追跡するのに使用するソフトウェア。

アプリケーションイベント : ネットワーク内にインストールされているアプリケーションから生成されるイベント。

ユーザアクセス制御 : ユーザによる会社のリソースへのアクセスを許可するアプリケーションまたはデバイスから生成されるイベント。

図 2-2　イベントソース


セキュリティの境界
ファイアウォール
スイッチ
IDS
ルータ
VPN
ウィルス対策
オペレーティング システム
メインフレーム
Linux
Windows
UNIX
参照用ITソース
環境設定管理
アセット管理
パッチ管理
脆弱性管理
アプリケーション イベント
カスタム アプリケーション
財務アプリケーション
データベース
ERP
ユーザアクセス制御
Enterprise SSO
識別情報管理
アクセス管理
ディレクトリ
Novell Cloud Security Service

2.2 Sentinel イベント

Sentinel は、デバイスから情報を受信し、この情報をイベントと呼ばれる構造に正規化し、そのイベントを分類してから処理用に送信します。イベントに分類情報 (Taxonomy) を追加することで、異なった形でイベントをレポートするシステム間でのイベントの比較をより簡単に行えます。例として、認証の失敗などが挙げられます。イベントは、リアルタイム表示、相関エンジン、ダッシュボード、およびバックエンドサーバによって処理されます。

イベントは 200 を超えるフィールドで構成されます。イベントフィールドの種類と目的はさまざまです。重大度、重大性、宛先 IP、宛先ポートなど、定義済みのフィールドがいくつかあります。構成可能なフィールドが 2 種類あります。予約済みフィールドは、将来の拡張のために Sentinel が内部で使用します。顧客フィールドは、顧客が拡張に使用します。

フィールドの目的は、名前を変更することで再設定できます。フィールドのソースは、外部 (デバイスまたは対応するコレクタによって明示的に設定されます)、または参照の場合があります。参照フィールドの値は、マッピングサービスを使用して 1 つ以上の他のフィールドに応じて計算されます。たとえば、イベントの宛先 IP として指定されているアセットを含む建物の建物コードになるようフィールドを定義できます。たとえば、イベントの宛先 IP を使用する顧客定義マップを使用してマッピングサービスによってフィールドを計算することができます。

- 15 ページのセクション 2.2.1「マッピングサービス」
- 16 ページのセクション 2.2.2「マップのストリーミング」
- 16 ページのセクション 2.2.3「エクスプロイト検出 (マッピングサービス)」

2.2.1 マッピングサービス

マッピングサービスにより、システム全体にビジネス関連データを伝達する高度なメカニズムが使用できるようになります。このデータによってイベントは参照情報で充実したものとなるため、アナリストは、より適切な決定、より有用なレポートの作成、考え抜かれた相関ルールの作成を行うことができます。

ソースデバイスからの着信イベントにホストと識別情報の詳細などの情報を追加するマップを使用することで、イベントデータを充実させることができます。この追加情報は、高度な相関とレポーティングに使用できます。システムは複数の組み込みマップとユーザ定義のカスタムマップをサポートしています。

Sentinel で定義されるマップは 2 つの方法で格納されます。

- 組み込みマップは、データベースに格納され、コレクタコードで API を使用して更新され、マッピングサービスに自動的にエクスポートされます。
- カスタムマップは、CSV ファイルとして格納され、ファイルシステム上またはマップデータの環境設定 UI を使用して更新され、マッピングサービスによってロードされます。

いずれの場合も、CSV ファイルは中核となる Sentinel サーバに保存されますが、マップへの変更は、各コレクタマネージャに分散され、ローカルに適用されます。この分散処理で、マッピング動作によるメインサーバのオーバーロードを防止できます。

2.2.2 マップのストリーミング

マップサービスにはダイナミック更新モデルが採用されており、ある場所から別の場所にマップをストリーミングして、ダイナミックメモリ内に大きなスタティックマップが蓄積されるのを回避します。このストリーミング機能は、システム上の一時的な負荷に関係なく、予測されるデータ移動を着実かつ迅速に行う必要がある Sentinel などのミッションクリティカルなリアルタイムシステムで特に重要です。

2.2.3 エクスプロイト検出 (マッピングサービス)

Sentinel は、イベントデータ署名と脆弱性スキャナデータを相互参照する機能を提供します。攻撃により脆弱なシステムが悪用されそうになると直ちに、自動的にユーザに対し通知が送信されます。これは次のような機能によって実現できます。

- アドバイザのフィード
- 侵入検出
- 脆弱性スキャン
- ファイアウォール

アドバイザは、イベントデータ署名と脆弱性スキャナデータとの相互参照を提供します。アドバイザのフィードには、脆弱性と脅威、さらにイベント署名と脆弱性プラグインの正規化に関する情報が含まれます。アドバイザの詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』の「「Configuring Advisor （アドバイザの設定）」」を参照してください。

2.3 コネクタ

コネクタにより、イベントソースから Sentinel システムへの接続が提供されます。syslog、データベーステーブルからの読み込みのための JDBC、Windows イベントログからの読み込みのための WMI など、イベントを取得するための業界標準のプロトコルを使用することで、コネクタは以下の機能を提供します。

- イベントソースからコレクタへの生イベントデータの転送。
- 接続固有のフィルタリング。
- 接続エラー処理。

2.4 コレクタ

コレクタは、コネクタから情報を収集して正規化します。コレクタは Javascript で記述されており、以下に関するロジックを定義します。

- 生データをコネクタから受信する。
- データを解析および正規化する。
- 反復可能なロジックをデータに適用する。
- デバイス固有のデータを Sentinel 固有のデータに変換する。

- イベントの形式設定を行う。
- 正規化、解析、および形式設定を行ったデータをコレクタマネージャに渡す。

2.5 コレクタマネージャ

コレクタマネージャは、データコレクションを管理し、システムステータスメッセージを監視し、必要に応じてイベントフィルタリングを実行します。コレクタマネージャの主要な機能は以下のとおりです。

- イベントを変換する
- マッピングサービスによってイベントにビジネスとの関連性を追加する
- イベントのグローバルフィルタリングを実行する
- イベントをルーティングする
- リアルタイム、脆弱性、アセット、または非リアルタイムデータを特定する
- ヘルスメッセージを Sentinel サーバに送信する

2.6 通信バス

通信バスアーキテクチャは、メモリ内処理と分散コンピューティングの利点を組み合わせた、標準ベースのサービス指向アーキテクチャ (SOA) を使用して構築されています。通信バスは iSCALE と呼ばれ、大量のデータを取り扱える専用のメッセージバスです。

- 17 ページのセクション 2.6.1「メッセージバス」
- 18 ページのセクション 2.6.2「チャネル」

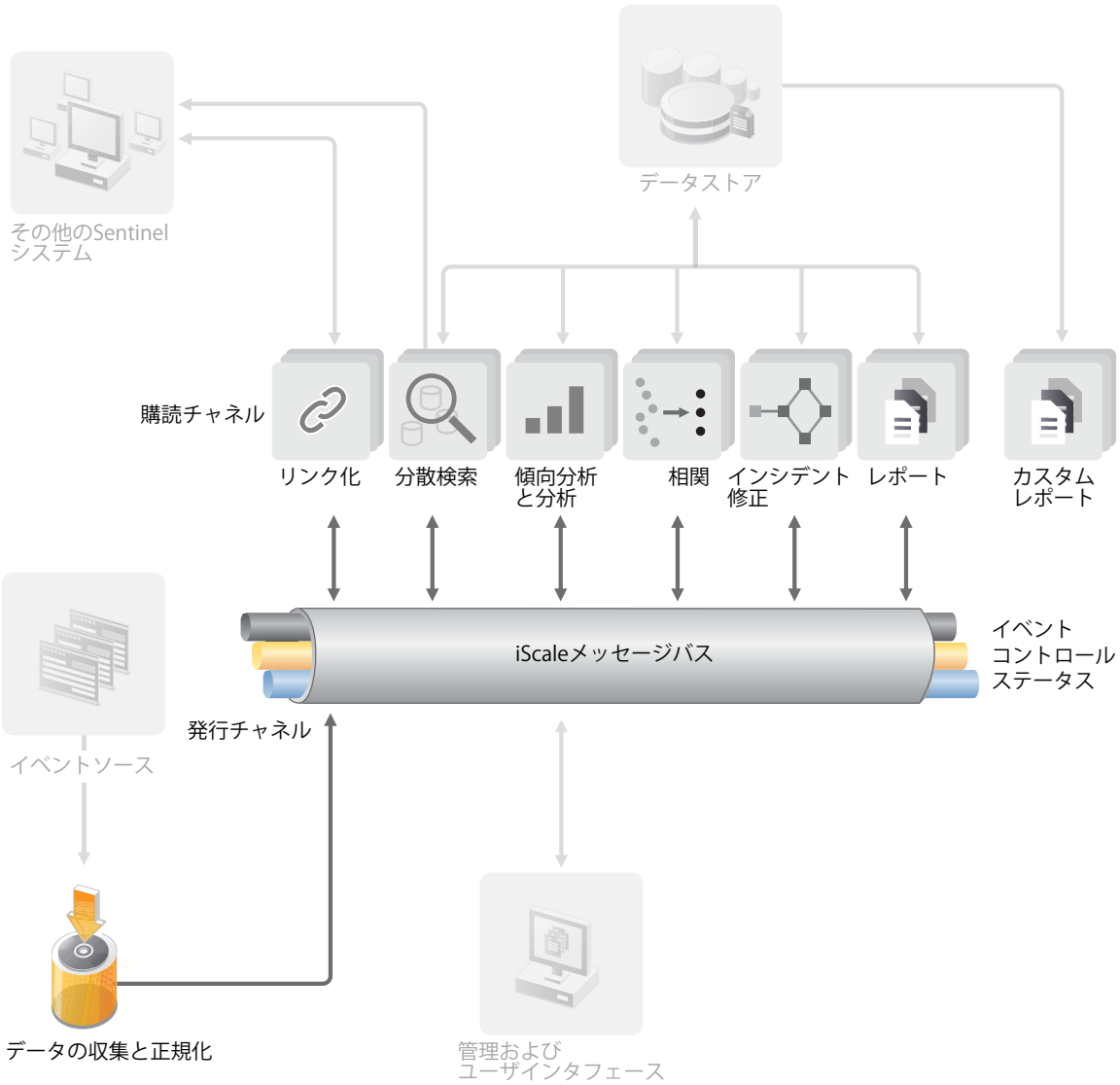
2.6.1 メッセージバス

iSCALE メッセージバスにより、個々のコンポーネントの独立したスケーリングが可能になると同時に、外部アプリケーションとの標準ベースの統合が可能になります。スケーラビリティにとって重要なのは、他の分散ソフトウェアと異なり、互いに直接通信する 2 つのピアコンポーネントがないという点です。すべてのコンポーネントは、1 秒あたり数千のメッセージパケットを移動できるメッセージバスを介して通信します。

メッセージバスの固有の機能を活用することで、スループットの高い通信チャネルが、システムの各コンポーネント間のデータスループット率を最大化し、高いスループット率を維持することができます。イベントは、ネットワークまたはコレクションポイントのエッジからシステムのハブへ安全かつ効率的に配信するために通信中は圧縮され暗号化されます。システムのハブでは、リアルタイム分析が実行されます。

iSCALE メッセージバスは、通信の信頼性をプラットフォームのセキュリティおよびパフォーマンス面以上に強化するさまざまなキューサービスを使用します。さまざまな一時および永続キューを使用して、システムは比類ない信頼性と耐障害性を提供します。たとえば、送信中の重要なメッセージは、通信パスの障害に備えて (キューに入れることによって) 保存されます。キューに入れられたメッセージは、システムが障害状態から回復した後で宛先に配信されます。

図 2-3　iSCALE メッセージバス



2.6.2　チャネル

iSCALE プラットフォームは、ワークロードに基づくシステム全体でのコンポーネントの独立したスケーリングを可能にする、データ駆動型またはイベント駆動型のモデルを使用します。サイトにより、デバイス数が多くてもイベントボリュームが小さかったり、逆にデバイス数が少なくてもイベントボリュームが非常に大きかったりと、顧客の環境はそれぞれ異なりますが、このプラットフォームにより柔軟な展開モデルを実現することができます。イベントの密度 (コレクションポイントから通信中のイベント集約およびイベント多重化のパターン) は場合によって異なり、メッセージバスでは多様なワークロードの一貫したスケーリングが可能です。

iSCALE は独立した多重チャネル環境を利用します。これにより、実質的に競合がなくなり、イベントの並列処理を推進できます。これらのチャネルおよびサブチャネルは、イベントデータのトランスポートに役立つだけでなく、さまざまな負荷状況でシステムのスケーリングおよび負荷分散を

行うための細かなプロセス制御を提供します。メインイベントチャネルに加え、コントロールチャネル、ステータスチャネルなどの独立したサービスチャネルを使用することで、イベント駆動型アーキテクチャのコスト効率に優れた高度なスケーリングが可能になります。

2.7 Sentinel データストレージ

Sentinel には、収集したデータを格納する複数のオプションがあります。Sentinel はデフォルトでは、2 つの独立した、同類のデータストリーム (イベントデータと生データ) をコレクタマネージャから受信します。このデータは、Sentinel サーバのローカルファイルシステムに格納されます。

ネットワーク上のストレージロケーションにデータを格納するように、Sentinel を設定することができます。また、データ同期ポリシーを使用して外部データベースにイベントデータを格納するように、Sentinel を設定することもできます。詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』の「「Configuring Data Storage (データストレージの設定)」」を参照してください。

2.8 フィルタ

Sentinel のフィルタを使用すると、イベント検索をカスタマイズしてデータのオーバーロードを防ぐことができます。この機能により、簡単なものから複雑なものまで検索クエリを構築できるフィルタビルダが提供されます。検索クエリをフィルタとして保存し、必要に応じて再使用できるので、毎回手動でクエリを指定するのではなく、フィルタを選択して検索を実行できます。

次のような Sentinel 機能を使用または設定しているときに、フィルタを再使用できます。

- セキュリティインテリジェンスダッシュボードの作成。

  詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Creating Dashboards （ダッシュボードの作成）」」を参照してください。

- アクティブビューのリアルタイムイベント表示。

  詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Viewing Events (イベントの表示)」」を参照してください。

- データ保持ポリシーの設定。

  詳細については『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』の「「Configuring Data Retention Policies (データ保持ポリシーの設定)」」を参照してください。

- データ同期の設定。

  詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』の「「Configuring Data Synchronization (データ同期の設定)」」を参照してください。

- 相関ルールのテスト。

  詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Correlating Event Data (イベントデータの相関)」」を参照してください。

Sentinel はデフォルトで、フィルタのリストを提供します。また、独自のフィルタも作成できます。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Configuring Filters (フィルタの設定)」」を参照してください。

2.9 相関

1 件のイベントはささいに思えるかもしれませんが、他のイベントと組み合わさると潜在的な問題について警告する場合があります。Sentinel では、ユーザが作成したルールを使用してこのようなイベントを相関させ、相関エンジンに展開し、適切な対策を講じて、問題を緩和することができます。

相関関係により、受信するイベントストリームの分析を自動化し、特定のパターンを発見できるため、セキュリティイベント管理のインテリジェンスが高まります。相関関係により、重大な脅威や複雑な攻撃パターンを識別するルールを定義できることで、イベントに優先順位をつけるとともに、効果的なインシデント管理と対応が可能になります。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Correlating Event Data (イベントデータの相関)」」を参照してください。

2.10 セキュリティインテリジェンス

Sentinel の相関機能では、セキュリティ、コンプライアンス、またはその他の理由による既知のパターンの動作に対する機能が提供されます。セキュリティインテリジェンス機能では、通常の動作から外れた、悪意のある動作である可能性があるが、既知のパターンとは一致しない動作を検索します。

Sentinel のセキュリティインテリジェンス機能では、時系列データの統計分析を採用しており、自動化された統計エンジンまたは手動解釈用の統計データの視覚表示によって、分析者が逸脱 (アノマリー) を識別および分析することができます。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Analyzing Trends in Data (データの傾向の分析)」」を参照してください。

2.11 iTRAC

iTRAC ワークフローは、企業のインシデント対応プロセスの自動化および追跡を行うための、シンプルで柔軟性のあるソリューションを提供するように設計されています。iTRAC では Sentinel の内部インシデントシステムを活用し、相関ルールまたは手動識別による識別から解決に至るまで、セキュリティやシステム上の問題を追跡できます。

ワークフローは、手動ステップと自動ステップを使用して構築できます。分岐、時間ベースのエスカレーション、およびローカル変数などの高度な機能がサポートされています。外部のスクリプトおよびプラグインとの統合により、サード パーティシステムとの柔軟な対話が可能になります。包括的なレポーティングにより、管理者はインシデント応答プロセスを理解し、微調整することができます。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Configuring iTRAC Workflows (iTRAC ワークフローの設定)」」を参照してください。

2.12 レポート

Sentinel は、収集したデータでレポートを実行する機能を提供します。Sentinel には、一般的なものからデバイス固有のもの (SUSE Linux など) まで、各種のカスタマイズ可能なレポートが事前にパッケージ化されています。一部のレポートでは、ユーザが柔軟に結果で表示するカラムを指定できます。

ユーザはレポートを実行したり、スケジュールしたり、PDF レポートを電子メールで送信したりすることができます。また、任意のレポートを検索として実行し、検索条件を絞ったり結果に対応したりするなど、あらゆる検索と同じように結果を利用することができます。異なる地域に分散している Sentinel サーバでレポートを実行することもできます。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の「「Reporting (レポート)」」を参照してください。

2.13 イベント分析

Sentinel では、重大なイベントデータを簡単に検索して分析できる強力なツールのセットが提供されています。システムは特定の種類の分析に合わせて、効率が最大限になるように調整、最適化され、1 つの種類の分析から別の分析にシームレスで簡単に移行できる方法が提供されています。

Sentinel でのイベントの調査は、ほぼリアルタイムのアクティブビューで開始する場合がよくあります。さらに高度なツールも使用できますが、アクティブビューではフィルタされたイベントストリームがサマリチャートと一緒に表示されるため、イベントの傾向とイベントデータのシンプルでおおまかな分析や、特定のイベントの識別の使用できます。時間の経過と共に、相関からの出力など、特定のクラスのデータに対して調整されたフィルタを構築します。アクティブビューは、運用とセキュリティに関する全般的な方針を示すダッシュボードとして使用できます。

さらにインタラクティブ検索を使用して、より詳細なイベントの分析を実行できます。これにより、特定のユーザや特定のシステムによる動作など、特定のクエリに関連するデータをすばやく簡単に検索して見つけることができます。イベントデータをクリックしたり、左側の絞り込みウィンドウを使用すると、簡単に目的のイベントに焦点を絞ることができます。

多数のイベントを分析する場合、Sentinel のレポーティング機能ではイベントのレイアウトに対するカスタムコントロールが提供されているため、より多くのデータを表示できます。Sentinel では検索インタフェースで構築されたインタラクティブ検索をレポーティングテンプレートに移動できるため、この移行が簡単です。そのため、多数のイベントにより適した形式で同じデータを表示するレポートを即座に作成できます。

Sentinel にはこの目的のためのテンプレートが多数含まれています。一部のテンプレートは、認証データやユーザ作成など、特定の種類の情報を表示するように調整されています。また、一部のテンプレートは汎用的なテンプレートで、レポートのグループと列をインタラクティブにカスタマイズできます。

時間の経過と共に、共通して使用するフィルタとレポートを開発して、ワークフローをより簡単にできます。Sentinel では、この情報の保存と、組織内のユーザへの配布が完全にサポートされています。詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』を参照してください。