IBM Security QRadar
バージョン 7.2.6

ハードウェア・ガイド

IBM

注記

本書および本書で紹介する製品を使用する前に、 53 ページの『特記事項』に記載されている情報をお読みください。

本装置は、高調波電流規格 JIS C 61000-3-2 に適合しています。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.6 および以降のリリースに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar
Version 7.2.6
Hardware Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

このガイドについて

IBM® Security QRadar® SIEM ハードウェア・ガイドには、QRadar アプライアンスの説明、図、および仕様が記載されています。

対象読者

このガイドは、ネットワーク・セキュリティーの調査と管理を担当するすべての QRadar SIEM ユーザーを対象としています。このガイドは、QRadar SIEM へのアクセス権限とご使用の企業ネットワークとネットワーキング・テクノロジーに関する知識をお持ちの方を想定して記述されています。

技術資料

詳細な技術資料、技術情報、およびリリース情報にアクセスする方法については、Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用やアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意:

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security

QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar M3 アプライアンスの概要

IBM Security QRadar に関する情報を参照して、ハードウェアとライセンスの要件を把握してください。

以下に、機能、およびライセンスの制限を含め、QRadar アプライアンスの概要を示します。

QRadar QFlow Collector 1201

IBM Security QRadar QFlow Collector 1201 (MTM 4378-QC1) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1201 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1201 のハードウェア情報および要件については、以下の表を参照してください。

表 1. QRadar QFlow Collector 1201

説明	値
ネットワーク・トラフィック	200 Mbps
インターフェース	6 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの管理インターフェース
メモリー	6 GB
ストレージ	146 GB
電源機構	二重予備 460 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	QRadar QFlow Collector 1201

QRadar QFlow Collector 1202

IBM Security QRadar QFlow Collector 1202 (MTM 4378-QC2) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1202 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1202 のハードウェア情報および要件については、以下の表を参照してください。

表 2. QRadar QFlow Collector 1202

説明	値
ネットワーク・トラフィック	2 Gbps
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	6 GB
ストレージ	146 GB
電源機構	二重予備 460W AC
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	QRadar QFlow Collector 1202 NT4E-STD Napatech ネットワーク・アダプター

QRadar QFlow Collector 1301

IBM Security QRadar QFlow Collector 1301 (MTM 4378-QD1) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1301 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1301 のハードウェア情報および要件については、以下の表を参照してください。

表 3. QRadar QFlow Collector 1301

説明	値
ネットワーク・トラフィック	2 Gbps
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	6 GB
ストレージ	146 GB
電源機構	二重予備 460 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	QRadar QFlow Collector 1301 NT4E-STD Napatech ネットワーク・アダプター

QRadar QFlow Collector 1310

IBM Security QRadar QFlow Collector 1310、-SR (MTM 4378-QSR) または -LR (MTM 4378-QLR) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1310 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1310 のハードウェア情報および要件については、以下の表を参照してください。

表 4. QRadar QFlow Collector 1310

説明	値
ネットワーク・トラフィック	3 GBps
インターフェース	2 つの 10 Gbps の XFP 1 つのシステム管理イーサネット・コネクター
メモリー	8 GB
ストレージ	300 GB
電源機構	二重予備 460 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	QRadar QFlow Collector 1310 NT20E Napatech ネットワーク・アダプター

QRadar Event Collector 1501

IBM Security QRadar Event Collector 1501 (MTM 4378-Q21) アプライアンスは、専用イベント・コレクターです。デフォルトでは、専用イベント・コレクターは、さまざまなログ・ソースからイベントを収集、解析し、これらのイベントをイベント・プロセッサーに継続的に転送します。 QRadar Event Collector 1501 アプライアンスは、イベントを一時的に保管し、保管したイベントだけをスケジュールに従って転送するように構成できます。専用イベント・コレクターは、イベントを処理しません。また、オンボード・イベント・プロセッサーは組み込まれていません。

QRadar Event Collector 1501 のハードウェア情報および要件については、以下の表を参照してください。

表 5. QRadar Event Collector 1501

説明	値
イベント/秒	2500 EPS
ログ・ソース	750
インターフェース	6 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース

表 5. QRadar Event Collector 1501 (続き)

説明	値
メモリー	24 GB
ストレージ	1.3 TB 専用ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	QRadar Event Collector 1501

QRadar Event Processor 1605

IBM Security QRadar Event Processor 1605 (MTM 4379-Q05) アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar デプロイメントをスケーリングできる専用イベント・プロセッサーです。 QRadar Event Processor 1605 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Event Processor 1605 は分散イベント・プロセッサー・アプライアンスであり、QRadar 3105 (コンソール) または QRadar 3124 (コンソール) アプライアンスに接続する必要があります。

QRadar Event Processor 1605 のハードウェア情報および要件については、以下の表を参照してください。

表 6. QRadar Event Processor 1605

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	最大 20,000 EPS
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	48 GB
ストレージ	6.2 TB 以上の専用イベント・ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター、イベント・プロセッサー

QRadar Event Processor 1624

IBM Security QRadar Event Processor 1624 (MTM 4379-Q24) アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar デプロイメントをスケーリングするための専用イベント・プロセッサーです。QRadar Event Processor 1624 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Event Processor 1624 は分散イベント・プロセッサー・アプライアンスであり、IBM Security QRadar 3124 (コンソール) (MTM 4379-Q24) Console アプライアンスに接続する必要があります。

QRadar Event Processor 1624 のハードウェア情報および要件については、以下の表を参照してください。

表 7. QRadar Event Processor 1624 イベント・プロセッサーの概要

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	最大 20,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	64 GB
ストレージ	16 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar Event Processor 1624 イベント・プロセッサー・プログラム

QRadar Flow Processor 1705

IBM Security QRadar Flow Processor 1705 (MTM 4379-Q05) アプライアンスは、より高い FPM レートを管理するように QRadar デプロイメントをスケーリングできるフロー・プロセッサーです。QRadar Flow Processor 1705 には、オンボード・フロー・プロセッサーおよびフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1705 のハードウェア情報および要件については、以下の表を参照してください。

表 8. QRadar Flow Processor 1705

説明	値
基本ライセンス	100,000 FPM
アップグレード後のライセンス	最大 600,000 FPM

表 8. QRadar Flow Processor 1705 (続き)

説明	値
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	48 GB
ストレージ	6.2 TB 以上の専用フロー・ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar Flow Processor 1705

QRadar Flow Processor 1724

IBM Security QRadar Flow Processor 1724 (MTM 4379-Q24) アプライアンスは、より高い FPM レートを管理するように QRadar デプロイメントをスケーリングできるフロー・プロセッサーです。QRadar Flow Processor 1724 には、オンボード・フロー・プロセッサーおよびフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1724 のハードウェア情報および要件については、以下の表を参照してください。

表 9. QRadar Flow Processor 1724

説明	値
基本ライセンス	100,000 FPM
アップグレード後のライセンス	最大 1,200,000 FPM
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	64 GB
ストレージ	16 TB 以上の専用フロー・ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar Flow Processor 1724

QRadar 1805

IBM Security QRadar 1805 (MTM 4379-Q05) アプライアンスは、イベント・プロセッサーとフロー・プロセッサーを結合したものであり、より多くのイベントおよびフローを管理するように QRadar デプロイメントをスケーリングできます。 QRadar 1805 には、オンボード・イベント・プロセッサー、オンボード・フロー・プロセッサー、およびイベントとフロー用の内部ストレージが組み込まれています。

QRadar 1805 のハードウェア情報および要件については、以下の表を参照してください。

表 10. QRadar 1805 の概要

説明	値
基本ライセンス	1,000 EPS 25,000 FPM、750 件のログ・ソース
アップグレード後のライセンス	最大 2,500 または 5,000 EPS。 最大 50,000、100,000、または 200,000 FPM
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	48 GB
ストレージ	6.2 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar 1805

QRadar 2100

IBM Security QRadar 2100 (MTM 4378-Q21) アプライアンスは、Network Behavioral Anomaly Detection (NBAD) と Security Information and Event Management (SIEM) が結合されたオールインワン・システムであり、ネットワークで発生する脅威を正確に特定し、適切な優先順位付けを行います。

QRadar 2100 のハードウェア情報および要件については、以下の表を参照してください。

表 11. QRadar 2100 の概要

説明	値
基本ライセンス	1,000 EPS 25,000 FPM
アップグレード後のライセンス	50,000 FPM

表 11. QRadar 2100 の概要 (続き)

説明	値
インターフェース	6 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	24 GB
ストレージ	1.3 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	イベント・コレクター、イベント・プロセッサー、1 つの QRadar QFlow Collector (最大 50 Mbps をサポート)

追加の QRadar QFlow Collector は、別売りとなります。

QRadar 3105 (All-in-One)

IBM Security QRadar 3105 (ベース) (MTM 4379-Q05) アプライアンスは、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができる、オールインワンの QRadar システムです。

QRadar Log Manager 3105 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 12. QRadar Log Manager 3105 (All-in-One)

説明	値
基本ライセンス	1,000 EPS 25,000 FPM
アップグレード後のライセンス	最大 5,000 EPS 最大 200,000 FPM
ログ・ソース	750
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T 管理インターフェース
メモリー	48 GB
ストレージ	6.5 TB
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	内部イベント・ストレージ (6.5 TB 以上) を備えたイベント・コレクターおよびイベント・プロセッサー

QRadar 3105 (All-in-One) アプライアンスでは、レイヤー 7 のネットワーク・アクティビティーをモニターするための外部 QRadar QFlow コレクター が必要です。

QRadar 3105 (コンソール)

QRadar 3105 (All-in-One) の容量を把握し、拡張します。

ライセンス・ベースのアップグレード・オプションを超えて QRadar 3105 (All-in-One) の容量を拡張するには、IBM Security QRadar 3105 (コンソール) (MTM 4379-Q05) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 22 ページの『QRadar Event Processor 1605』
- 24 ページの『QRadar Flow Processor 1705』
- 26 ページの『QRadar 1805』

QRadar 3105 (コンソール) アプライアンスを使用して、イベント・プロセッサーとフロー・プロセッサーの分散デプロイメントを管理することにより、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができます。

QRadar 3124 (All-in-One)

IBM Security QRadar 3124 (ベース) (MTM 4379-Q24) アプライアンスは、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができる、オールインワンの QRadar システムです。

QRadar 3124 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 13. QRadar 3124 (All-in-One)

説明	値
基本ライセンス	1000 EPS 25,000 FPM
アップグレード後のライセンス	最大 5000 EPS 最大 200,000 FPM
ログ・ソース	750
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	64 GB
ストレージ	16 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ

表 13. QRadar 3124 (All-in-One) (続き)

説明	値
組み込まれているコンポーネント	イベント・コレクターおよびイベント・プロセッサー

QRadar 3124 (All-in-One) では、レイヤー 7 のネットワーク・アクティビティーをモニターするための外部 QRadar QFlow Collector が必要です。

QRadar 3124 (コンソール)

IBM Security QRadar 3124 (コンソール) (MTM 4379-Q24) の拡張オプションを把握します。

ライセンス・ベースのアップグレード・オプションを超えて IBM Security QRadar 3124 (ベース) (MTM 4379-Q24) アプライアンスの容量を拡張するには、QRadar 3124 (コンソール) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 5 ページの『QRadar Event Processor 1624』
- 6 ページの『QRadar Flow Processor 1724』

QRadar 3124 (コンソール) アプライアンスを使用して、イベント・プロセッサーとフロー・プロセッサーの分散デプロイメントを管理することにより、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができます。

QRadar Log Manager 1605

IBM Security QRadar Log Manager 1605 (MTM 4379-Q05) アプライアンスは分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3124 コンソール アプライアンスに接続する必要があります。

QRadar Log Manager 1605 は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3105 コンソール アプライアンスに接続する必要があります。

QRadar Log Manager 1605 のハードウェア情報および要件については、以下の表を参照してください。

表 14. QRadar Log Manager 1605

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	最大 20,000 EPS

表 14. QRadar Log Manager 1605 (続き)

説明	値
インターフェース	4 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	48 GB
ストレージ	6.5 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター、イベント・プロセッサー

QRadar Log Manager 1624

IBM Security QRadar Log Manager 1624 (MTM 4379-Q24) アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar Log Manager デプロイメントをスケーリングするための専用イベント・プロセッサーです。QRadar Log Manager 1624 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Log Manager 1624 は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3124 コンソール アプライアンスに接続する必要があります。

QRadar Log Manager 1624 のハードウェア情報および要件については、以下の表を参照してください。

表 15. QRadar Log Manager 1624

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	最大 20,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	64 GB
ストレージ	16 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター、イベント・プロセッサー

QRadar Log Manager 2100

IBM Security QRadar Log Manager 2100 (MTM 4378-Q21) アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管できるオールインワン・システムです。

QRadar Log Manager 2100 のハードウェア情報および要件については、以下の表を参照してください。

表 16. QRadar Log Manager 2100 の概要

説明	値
基本ライセンス	500 EPS
ライセンスのアップグレード	最大 1000 EPS
ログ・ソース	750
インターフェース	6 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	24 GB
ストレージ	1.3 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 28 インチ x 幅 17.3 インチ x 高さ 1.69 インチ
組み込まれているコンポーネント	イベント・コレクター、イベント・プロセッサー

QRadar Log Manager 2100 には、外部フロー収集が組み込まれています。

追加の QRadar QFlow Collector は、別売りとなります。

QRadar Log Manager 3105 (All-in-One)

IBM Security QRadar Log Manager 3105 (ベース) (MTM 4379-Q05) アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管するために使用できるオールインワン・システムです。

QRadar Log Manager 3105 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 17. QRadar Log Manager 3105 (All-in-One) の概要

説明	値
基本ライセンス	500 EPS
アップグレード後のライセンス	最大 1000 EPS

表 17. QRadar Log Manager 3105 (All-in-One) の概要 (続き)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	48 GB
ストレージ	6.2 TB
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクターおよびイベント・プロセッサー

ライセンスをアップグレードすると、QRadar Log Manager 3105 (All-in-One) を QRadar 3105 (All-in-One) にマイグレーションできます。詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

QRadar Log Manager 3105 コンソール

ライセンス・ベースのアップグレード・オプションを超えて QRadar Log Manager (All-in-One) アプライアンスの容量を拡張するには、IBM Security QRadar Log Manager 3105 (コンソール) (MTM 4379-Q05) アプライアンスにアップグレードします。QRadar Log Manager 1605 アプライアンスまたは IBM Security QRadar Log Manager 1624 (MTM 4379-Q24) アプライアンスを 1 つ以上追加する必要もあります。

QRadar Log Manager 3105 コンソール アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。ライセンスを QRadar Log Manager 3105 コンソール から IBM Security QRadar 3105 (コンソール) (MTM 4379-Q05) にアップグレードできます。

QRadar Log Manager 3124 (All-in-One)

IBM Security QRadar Log Manager 3124 (ベース) (MTM 4379-Q24) アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管するために使用できるオールインワン・システムです。

QRadar Log Manager 3124 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 18. QRadar Log Manager 3124 (All-in-One)

説明	値
基本ライセンス	1000 EPS
アップグレード後のライセンス	最大 5000 EPS
ログ・ソース	750

表 18. QRadar Log Manager 3124 (All-in-One) (続き)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	64 GB
ストレージ	16 TB 以上
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクターおよびイベント・プロセッサー

ライセンスをアップグレードすると、QRadar Log Manager 3124 (All-in-One) アプライアンスを QRadar 3124 (All-in-One) にマイグレーションできます。QRadar Log Manager から QRadar SIEM へのマイグレーションについて詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

QRadar Log Manager 3124 コンソール

IBM Security QRadar Log Manager 3124 (コンソール) (MTM 4379-Q24) アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。QRadar Log Manager 3124 コンソール を拡張し、アップグレードします。

ライセンス・ベースのアップグレード・オプションを超えて QRadar Log Manager 3124 (All-in-One) アプライアンスの容量を拡張するには、QRadar Log Manager 3124 コンソール アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 10 ページの『QRadar Log Manager 1605』
- 11 ページの『QRadar Log Manager 1624』

ライセンスをアップグレードすると、QRadar Log Manager 3124 コンソール アプライアンスを QRadar 3124 (コンソール) にマイグレーションできます。詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

QRadar Log Manager 3124 コンソール アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。

QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager アプライアンスにより、ネットワークの脆弱性に関するスキャンと報告が行われます。 QRadar Vulnerability Manager には、QRadar SIEM と完全に統合された脆弱性管理ワークフローが用意されており、ソフトウェア・オプション、アプライアンス、および仮想アプライアンスとして使用できます。

QRadar Vulnerability Manager は、以下の機能を提供します。

- ネットワーク内外、ネットワーク・インフラストラクチャー、サーバーおよびエンドポイントをスキャンし、不正な構成、弱い設定、パッチが適用されていない製品、その他の重要な弱点を検出します。
- ネットワーク使用状況、脅威環境、セキュリティー構成情報、バーチャル・パッチ、およびパッチの可用性を使用することで、脆弱性管理の実際のコンテキストを把握することができるため、効率的な修復プロセスを推進します。
- 外部システムからのすべての脆弱性情報を統合し、単一のビューを提供します。
- QRadar アセット・プロファイル・データベースとの完全な統合により、インテリジェント・イベント・ドリブン・スキャンを提供します。
- 無制限の QRadar Vulnerability Manager 自動検出スキャン
- DMZ スキャンでのホスト・スキャナーの使用

QRadar Vulnerability Manager アプライアンスでは、以下がサポートされます。

表 19. QRadar Vulnerability Manager の概要

説明	値
基本ライセンス	255 のアセット
アップグレード後のライセンス	最大 32、768 のアセット
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース システム管理イーサネット・コネクター
メモリー	48 GB
ストレージ	6.5 TB 専用ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar Vulnerability Manager

QRadar Risk Manager

IBM Security QRadar アプライアンスには、完全に統合されたリスク管理、脆弱性の優先順位付け、および IBM Security QRadar プラットフォームに統合される自動構成ソリューションが用意されています。 QRadar Log Manager により、QRadar SIEM の緊密に統合された機能が使用可能になります。これらの機能により、インシデント管理、ログとネットワーク・アクティビティーの検索、脅威の可視化、およびレポートの機能が強化されます。

QRadar Risk Manager のハードウェア情報および要件については、以下の表を参照してください。

表 20. QRadar Risk Manager (次の表)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つのシステム管理イーサネット・コネクター
メモリー	48 GB
ストレージ	6.5 TB 専用ストレージ
電源機構	二重予備 675 W AC 電源
寸法	奥行き 29.5 インチ x 幅 19.2 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	QRadar Risk Manager

第 2 章 QRadar M4 アプライアンスの概要

IBM Security QRadar に関する情報を参照して、ハードウェアとライセンスの要件を把握してください。

以下に、機能、およびライセンスの制限を含め、QRadar アプライアンスの概要を示します。

QRadar QFlow Collector 1201

IBM Security QRadar QFlow Collector 1201 (MTM 4380-Q2C) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1201 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1201 のハードウェア情報および要件については、以下の表を参照してください。

表 21. QRadar QFlow Collector 1201

説明	値
ネットワーク・トラフィック	1 Gbps
インターフェース	5 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 2 つの 10 Gbps SFP + ポート 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース
メモリー	16 GB、4 x 4GB 1600 MHz RDIMM
ストレージ	2 x 2.5 インチ 600 GB 10 K rpm SAS、合計 600 MB (Raid 1)
電源機構	二重予備 550 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ
組み込まれているコンポーネント	QRadar QFlow Collector

QRadar QFlow Collector 1202

IBM Security QRadar QFlow Collector 1202 (MTM 4380-Q3C) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1202 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1202 のハードウェア情報および要件については、以下の表を参照してください。

表 22. QRadar QFlow Collector 1202

説明	値
ネットワーク・トラフィック	3 Gbps
インターフェース	Napatech ネットワーク・アダプター (4 つの 1 Gbps 10/100/1000 Base-T ネットワーク・インターフェースを提供) 2 つの 10 Gbps SFP + ポート 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース
メモリー	16 GB、4 x 4GB 1600 MHz RDIMM
ストレージ	2 x 2.5 インチ 600 GB 10 K rpm SAS、合計 600 MB (Raid 1)
電源機構	二重予備 550 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ
組み込まれているコンポーネント	QRadar QFlow Collector NT4E-STD Napatech ネットワーク・アダプター

QRadar QFlow Collector 1301

IBM Security QRadar QFlow Collector 1301 (MTM 4380-Q4C) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1301 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1301 のハードウェア情報および要件については、以下の表を参照してください。

表 23. QRadar QFlow Collector 1301

説明	値
ネットワーク・トラフィック	3 Gbps
インターフェース	Napatech ネットワーク・アダプター (4 つの 1 Gbps 1000 Base SX マルチモード・ファイバー・ネットワーク・モニター・インターフェースを提供) 2 つの 10 Gbps SFP + ポート 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース
メモリー	16 GB、4 x 4GB 1600 MHz RDIMM
ストレージ	2 x 2.5 インチ 600 GB 10 K rpm SAS、合計 600 MB (Raid 1)
電源機構	二重予備 550 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ

表 23. QRadar QFlow Collector 1301 (続き)

説明	値
組み込まれているコンポーネント	QRadar QFlow Collector NT4E-STD Napatech ネットワーク・アダプター

QRadar QFlow Collector 1310

IBM Security QRadar QFlow Collector 1310 (MTM 4380-Q5C) アプライアンスは、分散デプロイメント向けの大容量かつ拡張が容易なレイヤー 7 アプリケーション・データ収集機能を提供します。QRadar QFlow Collector 1310 では、外部のフロー・ベースのデータ・ソースもサポートされています。

QRadar QFlow Collector 1310 のハードウェア情報および要件については、以下の表を参照してください。

表 24. QRadar QFlow Collector 1310

説明	値
ネットワーク・トラフィック	7.5 Gbps
インターフェース	ファイバー用 Napatech ネットワーク・アダプターにより、2 つの 10 Gbps SFP + ネットワーク・モニター・インターフェースを提供 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース
メモリー	16 GB、4 x 4GB 1600 MHz RDIMM
ストレージ	2 x 2.5 インチ 600 GB 10 K rpm SAS、合計 600 MB (Raid 1)
電源機構	二重予備 550 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ
組み込まれているコンポーネント	QRadar QFlow Collector NT20E2 Napatech ネットワーク・アダプター

QRadar 1400 Data Node

IBM Security QRadar 1400 Data Node (MTM 4380-Q1E) アプライアンスは、QRadar デプロイメントに対して拡張が容易なデータ・ストレージ・ソリューションを提供します。QRadar 1400 Data Node によって、デプロイメントのデータ保存機能が拡張されるとともに、全体的な照会性能が向上します。

QRadar 1400 Data Node のハードウェア情報および要件については、以下の表を参照してください。

表 25. QRadar 1400 Data Node (XX05 アプライアンスで使用する場合)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	ストレージ: 9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	QRadar データ・ノード アプライアンス

表 26. QRadar 1400 Data Node (XX28 アプライアンスで使用する場合)

説明	値
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	40 TB 以上の専用イベント・ストレージ: 12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、40 TB 使用可能 (RAID 6)
電源機構	二重予備 900 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	QRadar データ・ノード アプライアンス

QRadar 1400-C Data Node

IBM Security QRadar 1400-C Data Node FIPS 準拠アプライアンスは、QRadar デプロイメントに対して拡張が容易なデータ・ストレージ・ソリューションを提供します。QRadar 1400-C Data Node によって、デプロイメントのデータ保存機能が拡張されるとともに、全体的な照会性能が向上します。

QRadar 1400-C Data Node のハードウェア情報および要件については、以下の表を参照してください。

表 27. QRadar 1400-C Data Node の仕様

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	40,000 EPS
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	データ・ノード

QRadar Event Collector 1501

IBM Security QRadar Event Collector 1501 (MTM 4380-Q2C) アプライアンスは、専用イベント・コレクターです。デフォルトでは、専用イベント・コレクターは、さまざまなログ・ソースからイベントを収集、解析し、これらのイベントをイベント・プロセッサーに継続的に転送します。 QRadar Event Collector 1501 アプライアンスは、イベントを一時的に保管し、保管したイベントだけをスケジュールに従って転送するように構成できます。専用イベント・コレクターは、イベントを処理しません。また、オンボード・イベント・プロセッサーは組み込まれていません。

QRadar Event Collector 1501 のハードウェア情報および要件については、以下の表を参照してください。

表 28. QRadar Event Collector 1501 の仕様

説明	値
イベント/秒	15,000 EPS
ネットワーク・トラフィック	1 Gbps
インターフェース	5 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 2 つの 10 Gbps SFP + ポート 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース

表 28. QRadar Event Collector 1501 の仕様 (続き)

説明	値
メモリー	16 GB、4 x 4GB 1600 MHz RDIMM
ストレージ	2 x 2.5 インチ 600 GB 10 K rpm SAS、合計 600 MB (Raid 1)
電源機構	二重予備 550 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ
組み込まれているコンポーネント	イベント・コレクター

QRadar Event Processor 1605

IBM Security QRadar Event Processor 1605 (MTM 4380-Q1E) アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar デプロイメントをスケーリングできる専用イベント・プロセッサーです。 QRadar Event Processor 1605 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Event Processor 1605 は分散イベント・プロセッサー・アプライアンスであり、IBM Security QRadar 3105 (コンソール) または QRadar 3128 (コンソール) アプライアンスに接続する必要があります。

QRadar Event Processor 1605 のハードウェア情報および要件については、以下の表を参照してください。

表 29. QRadar Event Processor 1605

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	20,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	メモリー: 64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	ストレージ: 9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Event Processor 1628

IBM Security QRadar Event Processor 1628 (MTM 4380-Q2E) アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar デプロイメントをスケーリングするための専用イベント・プロセッサーです。QRadar Event Processor 1628 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Event Processor 1628 は分散イベント・プロセッサー・アプライアンスであり、QRadar 3128 (コンソール) アプライアンスに接続する必要があります。

QRadar Event Processor 1628 のハードウェア情報および要件については、以下の表を参照してください。

表 30. QRadar Event Processor 1628 イベント・プロセッサーの概要

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	40,000 EPS
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 900 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

IBM Security QRadar Event Processor 1628-C

IBM Security QRadar Event Processor 1628-C FIPS 準拠アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar デプロイメントをスケーリングするための専用イベント・プロセッサーです。IBM Security QRadar Event Processor 1628-C アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

IBM Security QRadar Event Processor 1628-C は分散イベント・プロセッサー・アプライアンスであり、QRadar 3128-C (コンソール) Console アプライアンスに物理的に接続する必要があります。

IBM Security QRadar Event Processor 1628-C のハードウェア情報および要件については、以下の表を参照してください。

表 31. IBM Security QRadar Event Processor 1628-C FIPS 準拠イベント・プロセッサーの仕様

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	40,000 EPS
インターフェース	1 つの 2 ポート Emulex 8Gb FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

QRadar Flow Processor 1705

IBM Security QRadar Flow Processor 1705 (MTM 4380-Q1E) アプライアンスは、より高い FPM レートを管理するように QRadar デプロイメントをスケーリングできるフロー・プロセッサーです。QRadar Flow Processor 1705 には、オンボード・フロー・プロセッサーおよびフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1705 のハードウェア情報および要件については、以下の表を参照してください。

表 32. QRadar Flow Processor 1705

説明	値
基本ライセンス	100,000 FPM
アップグレード後のライセンス	600,000 FPM (トラフィック・タイプによる)

表 32. QRadar Flow Processor 1705 (続き)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	フロー・プロセッサー

QRadar Flow Processor 1728

IBM Security QRadar Flow Processor 1728 (MTM 4380-Q2E) アプライアンスは、より高い FPM レートを管理するように QRadar デプロイメントをスケーリングできるフロー・プロセッサーです。QRadar Flow Processor 1728 には、オンボード・フロー・プロセッサーおよびフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1728 のハードウェア情報および要件については、以下の表を参照してください。

表 33. QRadar Flow Processor 1728 の概要

説明	値
基本ライセンス	100,000 FPM
アップグレード後のライセンス	1,200,000 FPM
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 900 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ

表 33. QRadar Flow Processor 1728 の概要 (続き)

説明	値
組み込まれているコンポーネント	フロー・プロセッサー

QRadar Flow Processor 1728-C

IBM Security QRadar Flow Processor 1728-C FIPS 準拠アプライアンスは、より高いフロー/秒 (FPM) レートを管理するように QRadar デプロイメントをスケーリングできるフロー・プロセッサーです。QRadar Flow Processor 1728-C アプライアンスには、オンボード・フロー・プロセッサーおよびフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1728-C のハードウェア情報および要件については、以下の表を参照してください。

表 34. FIPS 準拠 QRadar Flow Processor 1728-C

説明	値
基本ライセンス	100,000 FPM
アップグレード後のライセンス	1,200,000 FPM
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	フロー・プロセッサー

QRadar 1805

QRadar 1805 (MTM 4380-Q1E) アプライアンスは、イベント・プロセッサーとフロー・プロセッサーを結合したものであり、より多くのイベントおよびフローを管理するように QRadar デプロイメントをスケーリングできます。 QRadar 1805 には、オンボード・イベント・プロセッサー、オンボード・フロー・プロセッサー、およびイベントとフロー用の内部ストレージが組み込まれています。

QRadar 1805 のハードウェア情報および要件については、以下の表を参照してください。

表 35. QRadar 1805 の概要

説明	値
基本ライセンス	25,000 FPM 1,000 EPS
アップグレード後のライセンス	200,000 FPM 5,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・プロセッサー フロー・プロセッサー

QRadar Flow Processor 1828

IBM Security QRadar Flow Processor 1828 (MTM 4380-Q2E) アプライアンスは、イベント・プロセッサーとフロー・プロセッサーを結合したものであり、より多くのイベントおよびフローを管理するように QRadar デプロイメントをスケーリングできます。QRadar Flow Processor 1828 には、オンボード・イベント・プロセッサー、オンボード・フロー・プロセッサー、およびイベントとフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1828 のハードウェア情報および要件については、以下の表を参照してください。

表 36. QRadar Flow Processor 1828 の概要

説明	値
基本ライセンス	25,000 FPM, 1000 EPS
アップグレード後のライセンス	300,000 FPM 15,000 EPS

表 36. QRadar Flow Processor 1828 の概要 (続き)

説明	値
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 900 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	フロー・プロセッサー

QRadar Flow Processor 1828-C

IBM Security QRadar Flow Processor 1828-C FIPS 準拠アプライアンスは、イベント・プロセッサーとフロー・プロセッサーを結合したものであり、より多くのイベントおよびフローを管理するように QRadar デプロイメントをスケーリングできます。QRadar Flow Processor 1828-C には、オンボード・イベント・プロセッサー、オンボード・フロー・プロセッサー、およびイベントとフロー用の内部ストレージが組み込まれています。

QRadar Flow Processor 1828-C のハードウェア情報および要件については、以下の表を参照してください。

表 37. QRadar Flow Processor 1828-C FIPS 準拠フロー・プロセッサーの仕様

説明	値
基本ライセンス	25,000 FPM, 1000 EPS
アップグレード後のライセンス	300,000 FPM 15,000 EPS
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM

表 37. QRadar Flow Processor 1828-C FIPS 準拠フロー・プロセッサーの仕様 (続き)

説明	値
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	フロー・プロセッサー

QRadar 2100

IBM Security QRadar 2100 (MTM 4380-Q1C) アプライアンスは、Network Behavioral Anomaly Detection (NBAD) と Security Information and Event Management (SIEM) が結合されたオールインワン・システムであり、ネットワークで発生する脅威を正確に特定し、適切な優先順位付けを行います。

QRadar 2100 のハードウェア情報および要件については、以下の表を参照してください。

表 38. QRadar 2100 の概要

説明	値
基本ライセンス	25,000 FPM 1000 EPS
アップグレード後のライセンス	50,000 FPM
インターフェース	3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	32 GB、4 x 8GB 1600 MHz RDIMM
ストレージ	6 x 2.5 インチ 500 GB 7.2K rpm SATA、合計 3 TB、1.5 TB 使用可能 (RAID 10)
電源機構	二重予備 750 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム 1 つの QRadar QFlow Collector

追加の QRadar QFlow Collector は、別売りとなります。

QRadar 3105 (All-in-One)

IBM Security QRadar 3105 (All-in-One) (MTM 4380-Q1E) アプライアンスは、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができる、オールインワンの QRadar システムです。

QRadar 3105 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 39. QRadar 3105 (All-in-One) の概要

説明	値
基本ライセンス	25,000 FPM 1000 EPS
アップグレード後のライセンス	200,000 FPM 5,000 EPS
ネットワーク・オブジェクト	1000
ログ・ソース	750
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベントおよびフロー処理用のイベント・プロセッサー イベントおよびフロー用の内部ストレージ

QRadar 3105 (All-in-One) アプライアンスでは、レイヤー 7 のネットワーク・アクティビティーをモニターするための外部 QRadar QFlow コレクター が必要です。

QRadar 3105 (コンソール)

QRadar 3105 (All-in-One) の容量を把握し、拡張します。

ライセンス・ベースのアップグレード・オプションを超えて QRadar 3105 (All-in-One) の容量を拡張するには、IBM Security QRadar 3105 (コンソール) (MTM 4380-Q1E) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805

QRadar 3105 (コンソール) アプライアンスを使用して、イベント・プロセッサーとフロー・プロセッサーの分散デプロイメントを管理することにより、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができます。

QRadar 3128 (All-in-One)

IBM Security QRadar 3128 (All-in-One) (MTM 4380-Q2E) アプライアンスは、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができる、オールインワンの QRadar システムです。

QRadar 3128 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 40. QRadar 3128 (All-in-One)

説明	値
基本ライセンス	25,000 FPM 1000 EPS
アップグレード後のライセンス	300,000 FPM 15,000 EPS
ネットワーク・オブジェクト	最大 1,000 (ライセンスによる)
ログ・ソース	750 (ライセンス・オプションを使用してデバイスを追加する)
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 900 W AC
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベントおよびフロー処理用のイベント・プロセッサー イベントおよびフロー用の内部ストレージ

QRadar 3128 (All-in-One) では、レイヤー 7 のネットワーク・アクティビティーをモニターするための外部 QRadar QFlow コレクター が必要です。

QRadar 3128-C (All-in-One)

IBM Security QRadar 3128-C (All-in-One) FIPS 準拠アプライアンスは、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができる、オールインワンの QRadar システムです。

QRadar 3128-C (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 41. QRadar 3128-C (All-in-One) の仕様

説明	値
基本ライセンス	25,000 FPM 1000 EPS
アップグレード後のライセンス	300,000 FPM 15,000 EPS
ネットワーク・オブジェクト	最大 1,000 (ライセンスによる)
ログ・ソース	750 (ライセンス・オプションを使用してデバイスを追加する)
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー イベントおよびフロー用の内部ストレージ

QRadar 3128-C (All-in-One) では、レイヤー 7 のネットワーク・アクティビティーをモニターするための外部 QRadar QFlow コレクター が必要です。

QRadar 3128 (Console)

IBM Security QRadar の拡張オプションを把握します。

ライセンス・ベースのアップグレード・オプションを超えて QRadar3128 (All-in-One) アプライアンスの容量を拡張するには、QRadar 3128 (Console) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 23 ページの『QRadar Event Processor 1628』
- 25 ページの『QRadar Flow Processor 1728』
- 27 ページの『QRadar Flow Processor 1828』

QRadar 3128 (Console) アプライアンスを使用して、イベント・プロセッサーとフロー・プロセッサーの分散デプロイメントを管理することにより、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができます。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar 3128-C (Console)

QRadar 3128-C (Console) FIPS 準拠アプライアンスを使用して、イベント・プロセッサーとフロー・プロセッサーの分散デプロイメントを管理することにより、ネットワーク動作のプロファイルを作成し、ネットワーク・セキュリティーの脅威を特定することができます。

ライセンス・ベースのアップグレード・オプションを超えて IBM Security QRadar 3128-C (All-in-One) FIPS 準拠アプライアンスの容量を拡大するには、QRadar 3128-C (Console) アプライアンスと FIPS 準拠のフローおよびイベント・プロセッサー・アプライアンスにアップグレードします。例えば、以下のアプライアンスを 1 つ以上追加します。

- 23 ページの『IBM Security QRadar Event Processor 1628-C』
- 26 ページの『QRadar Flow Processor 1728-C』
- 28 ページの『QRadar Flow Processor 1828-C』

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、47 ページの『QRadar xx28-C アプライアンス』を参照してください。

QRadar Log Manager 1605

IBM Security QRadar Log Manager 1605 は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3128 Console アプライアンスに接続する必要があります。

QRadar Log Manager 1605 は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3105 アプライアンスに接続する必要があります。

QRadar Log Manager 1605 のハードウェア情報および要件については、以下の表を参照してください。

表 42. QRadar Log Manager 1605

説明	値
基本ライセンス	2,500 EPS
アップグレード後のライセンス	20,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Log Manager 1628

IBM Security QRadar Log Manager 1628 アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar Log Manager デプロイメントをスケーリングするための専用イベント・プロセッサーです。QRadar Log Manager 1628 アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Log Manager 1628 は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3105 アプライアンスに接続する必要があります。

QRadar Log Manager 1628 のハードウェア情報および要件については、以下の表を参照してください。

表 43. QRadar Log Manager 1628

説明	値
基本ライセンス	20,000 EPS
アップグレード後のライセンス	40,000 EPS

表 43. QRadar Log Manager 1628 (続き)

説明	値
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 900 W AC
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Log Manager 1628-C

IBM Security QRadar Log Manager 1628-C FIPS 準拠アプライアンスは、より高いイベント/秒 (EPS) レートを管理するように QRadar Log Manager デプロイメントをスケーリングするための専用イベント・プロセッサーです。QRadar Log Manager 1628-C アプライアンスには、オンボード・イベント・コレクター、イベント・プロセッサー、およびイベント用の内部ストレージが組み込まれています。

QRadar Log Manager 1628-C は分散イベント・プロセッサー・アプライアンスであり、QRadar Log Manager 3105 アプライアンスに接続する必要があります。

QRadar Log Manager 1628-C のハードウェア情報および要件については、以下の表を参照してください。

表 44. QRadar Log Manager 1628-C FIPS 準拠の仕様

説明	値
基本ライセンス	20,000 EPS
アップグレード後のライセンス	40,000 EPS

表 44. QRadar Log Manager 1628-C FIPS 準拠の仕様 (続き)

説明	値
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、 47 ページの『QRadar xx28-C アプライアンス』を参照してください。

QRadar Log Manager 2100

IBM Security QRadar Log Manager 2100 アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管できるオールインワン・システムです。

IBM Security QRadar Log Manager 2100 のハードウェア情報および要件については、以下の表を参照してください。

表 45. IBM Security QRadar Log Manager 2100 の概要

説明	値
基本ライセンス	1000 EPS
ログ・ソース	750
インターフェース	3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	32 GB、4 x 8GB 1600 MHz RDIMM
ストレージ	6 x 2.5 インチ 500 GB 7.2K rpm SATA、合計 3 TB、1.5 TB 使用可能 (RAID 10)
電源機構	二重予備 750 W AC
寸法	奥行き 28.9 インチ x 幅 16.9 インチ x 高さ 1.7 インチ

表 45. IBM Security QRadar Log Manager 2100 の概要 (続き)

説明	値
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム

IBM Security QRadar Log Manager 2100 には、外部フロー収集が組み込まれています。

追加の QRadar QFlow Collector は、別売りとなります。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『M4 QRadar 2100、QRadar Event Collector 1501、およびすべての QRadar Flow Processor のアプライアンス』を参照してください。

QRadar Log Manager 3105 (All-in-One)

IBM Security QRadar Log Manager 3105 (All-in-One) アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管するために使用できるオールインワン・システムです。

QRadar Log Manager 3105 のハードウェア情報および要件については、以下の表を参照してください。

表 46. QRadar Log Manager 3105 の概要

説明	値
基本ライセンス	25,000 FPM 1000 EPS
アップグレード後のライセンス	200,000 FPM 5,000 EPS
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント処理用のイベント・プロセッサー イベント用の内部ストレージ

ライセンスをアップグレードすると、QRadar Log Manager 3105 (All-in-One) を QRadar 3105 (All-in-One) にマイグレーションできます。詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Log Manager 3105 Console

ライセンス・ベースのアップグレード・オプションを超えて QRadar Log Manager (All-in-One) アプライアンスの容量を拡張するには、QRadar Log Manager 3105 (Console) アプライアンスにアップグレードします。QRadar Log Manager 1605 アプライアンスまたは QRadar Log Manager 1628 アプライアンスを 1 つ以上追加する必要もあります。

QRadar Log Manager 3105 (Console) アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。ライセンスを QRadar Log Manager 3105 から QRadar 3105 にアップグレードできます。

QRadar Log Manager 3128 (All-in-One)

IBM Security QRadar Log Manager 3128 (All-in-One) アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管するために使用できるオールインワン・システムです。

QRadar Log Manager 3128 (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 47. QRadar Log Manager 3128 (All-in-One)

説明	値
基本ライセンス	1,000 EPS
アップグレード後のライセンス	15,000 EPS
ネットワーク・オブジェクト	最大 1,000 (ライセンスによる)
ログ・ソース	750 (ライセンス・オプションを使用してデバイスを追加する)
インターフェース	1 つの 2 ポート Emulex 8Gb FC 2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)

表 47. QRadar Log Manager 3128 (All-in-One) (続き)

説明	値
電源機構	二重予備 900 W AC
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム イベント用の内部ストレージ

ライセンスをアップグレードすると、QRadar Log Manager 3128 (All-in-One) アプライアンスを QRadar 3128 (All-in-One) にマイグレーションできます。QRadar Log Manager から QRadar SIEM へのマイグレーションについて詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Log Manager 3128-C (All-in-One)

IBM Security QRadar Log Manager 3128-C (All-in-One) FIPS 準拠アプライアンスは、さまざまなネットワーク・デバイスからのイベントを管理および保管するのに使用できるオールインワン・システムです。

QRadar Log Manager 3128-C (All-in-One) のハードウェア情報および要件については、以下の表を参照してください。

表 48. QRadar Log Manager 3128-C (All-in-One) FIPS 準拠の仕様

説明	値
基本ライセンス	1,000 EPS
アップグレード後のライセンス	15,000 EPS
ネットワーク・オブジェクト	最大 1,000 (ライセンスによる)
ログ・ソース	750 (ライセンス・オプションを使用してデバイスを追加する)
インターフェース	1 つの 2 ポート Emulex 8 Gbps FC 3 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合リモート・システム管理インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x16 GB 2133 MT/s DDR4 RDIMM
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 48 TB、うち 40 TB が使用可能 (Raid 6)

表 48. QRadar Log Manager 3128-C (All-in-One) FIPS 準拠の仕様 (続き)

説明	値
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	イベント・コレクター イベント・プロセッサー・プログラム イベント用の内部ストレージ

ライセンスをアップグレードすると、QRadar Log Manager 3128-C (All-in-One) アプライアンスを QRadar 3128-C (All-in-One) にマイグレーションできます。QRadar Log Manager から QRadar SIEM へのマイグレーションについて詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、47 ページの『QRadar xx28-C アプライアンス』を参照してください。

QRadar Log Manager 3128 (Console)

IBM Security QRadar Log Manager 3128 (Console) アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。QRadar Log Manager 3128 (Console) を拡張し、アップグレードします。

ライセンス・ベースのアップグレード・オプションを超えて QRadar Log Manager 3128 (All-in-One) アプライアンスの容量を拡張するには、QRadar Log Manager 3128 (Console) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 33 ページの『QRadar Log Manager 1605』
- 34 ページの『QRadar Log Manager 1628』

ライセンスをアップグレードすると、QRadar Log Manager 3128 (Console) アプライアンスを QRadar Log Manager 3128 (Console) にマイグレーションできます。詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

QRadar Log Manager 3128 (Console) アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Log Manager 3128-C (Console)

IBM Security QRadar Log Manager 3128-C (Console) FIPS 準拠アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。QRadar Log Manager 3128-C (Console) を拡張し、アップグレードします。

ライセンス・ベースのアップグレード・オプションを超えて QRadar Log Manager 3128-C (All-in-One) アプライアンスの容量を拡張するには、QRadar Log Manager 3128-C (Console) アプライアンスにアップグレードし、以下のアプライアンスを 1 つ以上追加します。

- 23 ページの『QRadar Event Processor 1628』

ライセンスをアップグレードすると、QRadar Log Manager 3128-C (Console) アプライアンスを QRadar Log Manager 3128-C (Console) にマイグレーションできます。詳しくは、「*Migrating QRadar Log Manager to QRadar SIEM Technical Note*」を参照してください。

QRadar Log Manager 3128-C (Console) アプライアンスは、イベント・プロセッサーの分散デプロイメントを管理して、イベントを収集および処理します。

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、47 ページの『QRadar xx28-C アプライアンス』を参照してください。

QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager アプライアンスにより、ネットワークの脆弱性に関するスキャンと報告が行われます。 QRadar Vulnerability Manager には、QRadar SIEM と完全に統合された脆弱性管理ワークフローが用意されており、ソフトウェア・オプション、アプライアンス、および仮想アプライアンスとして使用できます。

QRadar Vulnerability Manager は、以下の機能を提供します。

- ネットワーク内外、ネットワーク・インフラストラクチャー、サーバーおよびエンドポイントをスキャンし、不正な構成、弱い設定、パッチが適用されていない製品、その他の重要な弱点を検出します。
- ネットワーク使用状況、脅威環境、セキュリティー構成情報、バーチャル・パッチ、およびパッチの可用性を使用することで、脆弱性管理の実際のコンテキストを把握することができるため、効率的な修復プロセスを推進します。
- 外部システムからのすべての脆弱性情報を統合し、単一のビューを提供します。
- QRadar アセット・プロファイル・データベースとの完全な統合により、インテリジェント・イベント・ドリブン・スキャンを提供します。
- 無制限の QRadar Vulnerability Manager 自動検出スキャン
- DMZ スキャンでのホスト・スキャナーの使用

QRadar Vulnerability Manager アプライアンスでは、以下がサポートされます。

表 49. QRadar Vulnerability Manager の概要

説明	値
基本ライセンス	255 のアセット
アップグレード後のライセンス	32,768
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	QRadar Vulnerability Manager

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Risk Manager

IBM Security QRadar アプライアンスには、完全に統合されたリスク管理、脆弱性の優先順位付け、および IBM Security QRadar プラットフォームに統合される自動構成ソリューションが用意されています。 QRadar Log Manager により、QRadar SIEM の緊密に統合された機能が使用可能になります。これらの機能により、インシデント管理、ログとネットワーク・アクティビティーの検索、脅威の可視化、およびレポートの機能が強化されます。

QRadar Risk Manager のハードウェア情報および要件については、以下の表を参照してください。

表 50. QRadar Risk Manager (次の表)

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T QRadar SIEM 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM

表 50. QRadar Risk Manager (次の表) (続き)

説明	値
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750 W AC
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ
組み込まれているコンポーネント	QRadar Risk Manager

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Incident Forensics

IBM Security QRadar Incident Forensics を使用して、アタッカーの可能性がある人物のアクションを再トレースしたり、悪意のあるネットワーク・セキュリティー・インシデントと疑われるものに対して、詳細な Forensics 調査を行ったりします。QRadar Incident Forensics により、セキュリティー・チームがオフェンス・レコードの調査に要する時間が短縮されます。また、ネットワーク・セキュリティー・ブリーチを修復して、再発を防ぐのに役立ちます。

QRadar Incident Forensics では、ハードウェアが QRadar XX28 アプライアンスと共有されます。 XX28 アプライアンスについて詳しくは、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

QRadar Packet Capture

IBM Security QRadar Incident Forensics には、他にデプロイされているネットワーク・パケット・キャプチャー (PCAP) デバイスがない場合に、QRadar Incident Forensics で使用するデータを保管および管理するためのオプションの IBM Security QRadar Packet Capture アプライアンスが用意されています。任意の数のアプライアンスを、ネットワークまたはサブネットワークにタップとしてインストールし、未加工のパケット・データを収集できます。

QRadar Packet Capture のハードウェア情報および要件については、以下の表を参照してください。

表 51. QRadar Packet Capture の概要

説明	値
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/100 Base-T IBM Security QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 4 つの 10 Gbps SFP + ポート
メモリー	128 GB、8 x 16 GB 1866 MHz RDIMM8

表 51. QRadar Packet Capture の概要 (続き)

説明	値
ストレージ	12 x 3.5 インチ 4 TB SAS 7.2 K rpm、合計 41 TB、うち 32 TB が使用可能 (Raid 5)
電源機構	二重予備 900 W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.6 インチ x 高さ 3.4 インチ
組み込まれているコンポーネント	フロー・プロセッサー

このアプライアンスのフロント・パネルおよびバック・パネルの図および情報については、46 ページの『QRadar M4 のコンソール、プロセッサー、およびデータ・ノード』を参照してください。

第 3 章 アプライアンスの図

アプライアンスのバック・パネルとフロント・パネルの図と説明を示します。以下の図は、IBM Security QRadar アプライアンスを示しています。使用するシステムは、購入したアプライアンスのバージョンによって異なる可能性があります。

統合管理モジュール

すべてのアプライアンス・タイプのバック・パネルで、統合管理モジュール (IMM) を使用してシリアル・コネクターとイーサネット・コネクターを管理できます。IMM は、イーサネット・ポートを IBM Security QRadar 管理インターフェースと共有するように構成できますが、IMM を専用モードで構成すると、アプライアンスの再始動時に IMM 接続が失われるリスクを低減できます。 IMM を構成するには、IBM スプラッシュ画面が表示されたら F1 キーを押してシステム BIOS 設定にアクセスする必要があります。 IMM の構成方法について詳しくは、アプライアンスに付属の CD に収録されている「*統合管理モジュール・ユーザーズ・ガイド*」を参照してください。

M3 QRadar 2100、QRadar Event Collector 1501、およびすべての QRadar Flow Processor のアプライアンス

アプライアンスのフロント・パネルとバック・パネルの機能に関する情報を参照して、接続と機能が適切であることを確認してください。

- IBM Security QRadar QFlow Collector 1201 (MTM 4378-QC1)
- IBM Security QRadar QFlow Collector 1202 (MTM 4378-QC2)
- IBM Security QRadar QFlow Collector 1301 (MTM 4378-QD1)
- IBM Security QRadar QFlow Collector 1310-SR (MTM 4378-QSR), -LR (MTM 4378-QLR)
- IBM Security QRadar Event Collector 1501 (MTM 4378-Q21)
- IBM Security QRadar 2100 (MTM 4378-Q21)

フロント・パネルとバック・パネルの図を含め、QRadar M3 2100、QRadar Event Collector 1501、およびすべての QRadar Flow Processor のアプライアンスについて詳しくは、IBM System x3550 M3 (http://www.redbooks.ibm.com/abstracts/tips0804.html?Open) を参照してください。

QRadar M3 のコンソールおよびプロセッサー

アプライアンスのフロント・パネルとバック・パネルの機能に関する情報を参照して、接続と機能が適切であることを確認してください。

- IBM Security QRadar Event Processor 1605 (MTM 4379-Q05)
- IBM Security QRadar Event Processor 1624 (MTM 4379-Q24)
- IBM Security QRadar Flow Processor 1705 (MTM 4379-Q05)

- IBM Security QRadar Flow Processor 1724 (MTM 4379-Q24)
- IBM Security QRadar 1805 (MTM 4379-Q05)
- IBM Security QRadar 3105 (ベース) (MTM 4379-Q05)
- IBM Security QRadar 3105 (コンソール) (MTM 4379-Q05)
- IBM Security QRadar 3124 (ベース) (MTM 4379-Q24)
- IBM Security QRadar 3124 (コンソール) (MTM 4379-Q24)
- IBM Security QRadar Log Manager 1605 (MTM 4379-Q05)
- IBM Security QRadar Log Manager 1624 (MTM 4379-Q24)
- IBM Security QRadar Log Manager 3105 (ベース) (MTM 4379-Q05)
- IBM Security QRadar Log Manager 3105 (コンソール) (MTM 4379-Q05)
- IBM Security QRadar Log Manager 3124 (ベース) (MTM 4379-Q24)
- IBM Security QRadar Log Manager 3124 (コンソール) (MTM 4379-Q24)
- 14 ページの『QRadar Vulnerability Manager』
- 15 ページの『QRadar Risk Manager』

フロント・パネルとバック・パネルの図を含め、IBM Security QRadar M3 のコンソール、プロセッサー、およびデータ・ノードについて詳しくは、IBM System x3630 M3 (http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/tips0807.html) を参照してください。

M4 QRadar 2100、QRadar Event Collector 1501、およびすべての QRadar Flow Processor のアプライアンス

アプライアンスのフロント・パネルとバック・パネルの機能に関する情報を参照して、接続と機能が適切であることを確認してください。

- 29 ページの『QRadar 2100』 (4380-Q1C)。
- 17 ページの『QRadar QFlow Collector 1202』 (4380-Q3C)。
- 18 ページの『QRadar QFlow Collector 1301』 (4380-Q4C)。
- 19 ページの『QRadar QFlow Collector 1310』 (4380-Q5C)。
- 21 ページの『QRadar Event Collector 1501』、 17 ページの『QRadar QFlow Collector 1201』 (4380-Q2C)。
- 36 ページの『QRadar Log Manager 2100』 (4380-Q1C)。

フロント・パネルとバック・パネルの図を含め、QRadar M4 2100、QRadar Event Collector 1501、およびすべての QRadar Flow Processor のアプライアンスについて詳しくは、IBM System X3550 M4 (http://publib-b.boulder.ibm.com/abstracts/tips0851.html?Open) を参照してください。

QRadar M4 のコンソール、プロセッサー、およびデータ・ノード

アプライアンスのフロント・パネルとバック・パネルの機能に関する情報を参照して、接続と機能が適切であることを確認してください。

- 19 ページの『QRadar 1400 Data Node』 (4380-Q1E)。
- 22 ページの『QRadar Event Processor 1605』 (4380-Q1E)。

- 23 ページの『QRadar Event Processor 1628』 (4380-Q2E)。
- 24 ページの『QRadar Flow Processor 1705』 (4380-Q1E)。
- 25 ページの『QRadar Flow Processor 1728』 (4380-Q2E)。
- 30 ページの『QRadar 3105 (All-in-One)』 (4380-Q1E)。
- 30 ページの『QRadar 3105 (コンソール)』 (4380-Q1E)。
- 31 ページの『QRadar 3128 (All-in-One)』 (4380-Q2E)。
- 32 ページの『QRadar 3128 (Console)』 (4380-Q2E)。
- 33 ページの『QRadar Log Manager 1605』 (4380-Q1E)。
- 34 ページの『QRadar Log Manager 1628』 (4380-Q2E)。
- 37 ページの『QRadar Log Manager 3105 (All-in-One)』 (4380-Q1E)。
- 38 ページの『QRadar Log Manager 3105 Console』 (4380-Q1E)。
- 38 ページの『QRadar Log Manager 3128 (All-in-One)』 (4380-Q2E)。
- 40 ページの『QRadar Log Manager 3128 (Console)』 (4380-Q2E)。
- 41 ページの『QRadar Vulnerability Manager』 (4380-Q1E)。
- 42 ページの『QRadar Risk Manager』 (4380-Q1E)。

フロント・パネルとバック・パネルの図を含め、IBM Security QRadar M4 のコンソール、プロセッサー、およびデータ・ノードについて詳しくは、IBM System X3650 M4 BD (http://www.redbooks.ibm.com/abstracts/tips1102.html?Open) を参照してください。

QRadar xx28-C アプライアンス

アプライアンスのフロント・パネルとバック・パネルの機能に関する情報を参照して、接続と機能が適切であることを確認してください。

IBM Security QRadar xx28-C アプライアンスの製造元は Dell で、以下のアプライアンスに対して使用できます。

- QRadar
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Incident Forensics
- QRadar Packet Capture (QRadar Packet Capture Data Node を含む)。

QRadar xx28-C アプライアンスを FIPS 準拠で使用することもできます。

重要: xx28-C アプライアンスを FIPS 準拠にするには、QRadar のリリースが FIPS に準拠している必要があり、ご使用のアプライアンスに必須の物理的セキュリティーが備わっていなければなりません。物理的セキュリティーについて詳しくは、「*IBM Security QRadar Version 7.2.4 FIPS 140-2 Installation Guide*」を参照してください。 QRadar Incident Forensics と QRadar Packet Capture は、FIPS 準拠ではありません。

- 20 ページの『QRadar 1400-C Data Node』
- 23 ページの『IBM Security QRadar Event Processor 1628-C』
- 26 ページの『QRadar Flow Processor 1728-C』

- 28 ページの『QRadar Flow Processor 1828-C』
- 32 ページの『QRadar 3128-C (All-in-One)』
- 33 ページの『QRadar 3128-C (Console)』
- 35 ページの『QRadar Log Manager 1628-C』
- 39 ページの『QRadar Log Manager 3128-C (All-in-One)』
- 41 ページの『QRadar Log Manager 3128-C (Console)』

フロント・パネルのインディケーターと機能

IBM Security QRadar FIPS 準拠アプライアンスのフロント・パネルの図と説明を参照して、ハードウェアの機能を把握してください。

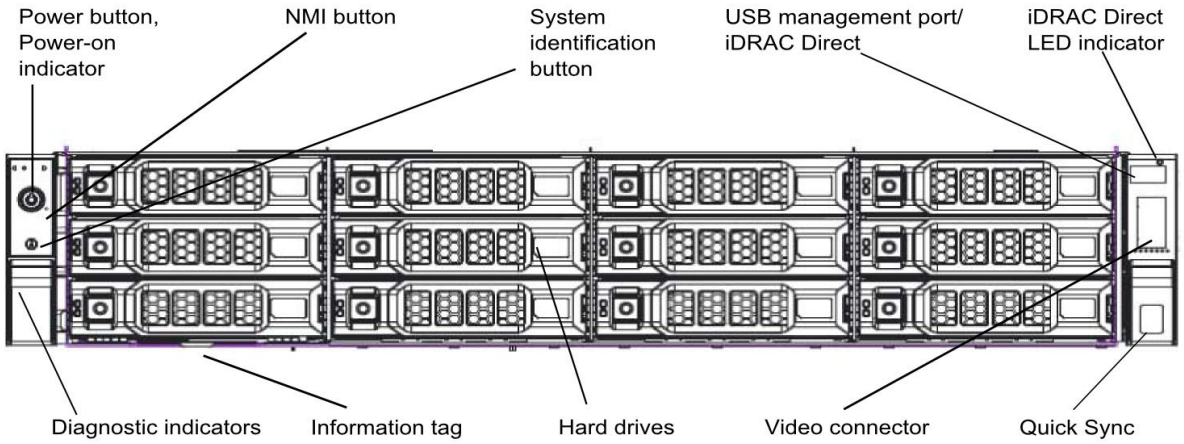

図 1. FIPS アプライアンスのフロント・パネル

表 52. IBM Security QRadar FIPS アプライアンスのフロント・パネルの機能

機能	説明
診断インディケーター	診断インディケーターは、エラー状況を表示します。

表 52. IBM Security QRadar FIPS アプライアンスのフロント・パネルの機能 (続き)

機能	説明
システム ID ボタン	フロント・パネルとバック・パネルにあるこの ID ボタンを使用して、ラック内の特定のシステムを見つけることができます。これらのボタンのいずれかを押すと、次にいずれかのボタンを押すまで、バック・パネルのシステム状況インディケーターが点滅します。押すと、システム ID のオンとオフが切り替わります。 POST 中にシステムが応答を停止した場合は、システム ID ボタンを押したまま 5 秒を経過すると、BIOS 進行モードになります。 iDRAC をリセットする (F2 iDRAC セットアップで無効になっていない場合) には、このボタンを 15 秒より長く押し続けてください。
電源オン・インディケーター、電源ボタン	電源オン・インディケーターは、システムの電源がオンになっているときに点灯します。電源ボタンはシステムへの電源機構の出力を制御します。 **注:** ACPI 準拠のオペレーティング・システムでは、電源ボタンを使用してシステムをオフにすると、システムが正常にシャットダウンしてからシステムへの電源がオフになります。
NMI ボタン	特定のオペレーティング・システムを実行しているときのソフトウェア・エラーおよびデバイス・ドライバー・エラーのトラブルシューティングに使用します。このボタンを押すにはペーパー・クリップの先端を使用します。 このボタンは、資格を有するサポート担当者またはオペレーティング・システムの資料により指示された場合にのみ使用してください。
情報タグ	スライドアウト・ラベル・パネルに、サービス・タグ、NIC、MAC アドレスなどのシステム情報が記録されています。
ハード・ディスク	3.5 インチ・ホット・スワップ対応ハード・ディスク (12 台まで)。
USB 管理ポート/iDRAC Direct	USB デバイスをシステムに接続したり、iDRAC Direct 機能へのアクセスを可能にします。USB 管理ポートは USB 2.0 準拠です。

表 52. IBM Security QRadar FIPS アプライアンスのフロント・パネルの機能 (続き)

機能	説明
iDRAC Direct LED インディケーター	このインディケーターには、エラー状況が表示されます。
ビデオ・コネクター	VGA ディスプレイをシステムに接続します。
Quick Sync (オプション)	Quick Sync 対応システムを示します。Quick Sync 機能はオプションであり、Quick Sync ベゼルが必要です。この機能を使用すると、モバイル・デバイスを使用してシステムを管理できます。この機能により、ハードウェアとファームウェアのインベントリー情報やシステムのさまざまなレベルでの診断とエラーの情報が集約され、これらの情報をシステムのトラブルシューティングに使用できます。

バック・パネルのインディケーターと機能

IBM Security QRadar FIPS 準拠アプライアンスのバック・パネルの図と説明を参照して、ハードウェアの機能を把握してください。

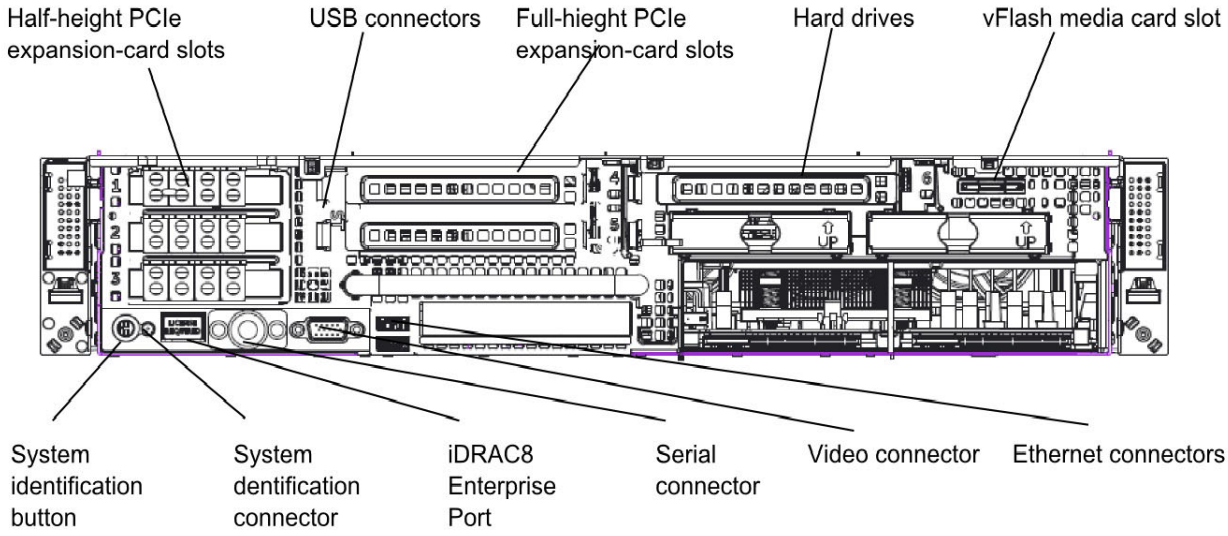

図 2. FIPS アプライアンスのバック・パネル

表 53. IBM Security QRadar コア・アプライアンスのバック・パネルの機能

機能	説明
システム ID ボタン	フロント・パネルとバック・パネルにあるこの ID ボタンを使用して、ラック内の特定のシステムを見つけることができます。 押すと、システム ID のオンとオフが切り替わります。 POST 中にシステムが応答を停止した場合は、システム ID ボタンを押したまま 5 秒を経過すると、BIOS 進行モードになります。 iDRAC をリセットする (F2 iDRAC セットアップで無効になっていない場合) には、このボタンを 15 秒より長く押し続けてください。
システム ID コネクター	オプションのケーブル管理アームを介して、オプションのシステム状況インディケーター・アセンブリーを接続します。
iDRAC8 Enterprise ポート	専用の管理ポート。
ハーフハイト PCIe 拡張カード・スロット	ハーフハイト PCI Express 拡張カードを 3 枚まで接続します。
シリアル・コネクター	シリアル・デバイスをシステムに接続します。
ビデオ・コネクター	VGA ディスプレイをシステムに接続します。
USB コネクター	USB デバイスをシステムに接続します。ポートは USB 3.0 準拠です。
フルハイト PCIe 拡張カード・スロット	フルハイト PCI Express 拡張カードを 4 枚まで接続します。
イーサネット・コネクター	統合 10/100/1000 Mbps NIC コネクター
電源装置ユニット	AC 495 W、750 W、1100 W、または DC 750 W、1100 W
vFlash メディア・カード・スロット	vFlash メディア・カードのホルダー。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

この用語集には、[製品名] のソフトウェアおよび製品で使用する用語と定義を記載します。

この用語集では、以下の相互参照を使用しています。

- 「*...を参照*」という表現は、非優先用語の場合は優先用語を参照し、略語の場合は正式な用語を参照するように促すための表現です。
- 「*...も参照*」という表現は、関連する用語や対比的な用語を参照するように促すための表現です。

この用語集に記載されていない用語と定義については、IBM Terminology Web サイト (新しいウィンドウで開きます) を参照してください。

『A』 『B』 58 ページの『C』 58 ページの『D』 59 ページの『E』 59 ページの『F』 59 ページの『G』 59 ページの『H』 60 ページの『I』 60 ページの『K』 60 ページの『L』 61 ページの『M』 61 ページの『N』 61 ページの『O』 62 ページの『P』 62 ページの『Q』 62 ページの『R』 63 ページの『S』 64 ページの『T』 64 ページの『V』 64 ページの『W』

A

アキュムレーター (accumulator)
特定の演算の 1 つのオペランドを格納するためのレジスター。このオペランドは、その演算の結果によって置き換えられる。

アクティブ・システム (active system)
高可用性 (HA) クラスターにおいて、すべてのサービスが稼働しているシステム。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))
ローカル・エリア・ネットワーク内で IP アドレスをネットワーク・アダプター・アドレスに動的にマップするプロトコル。

管理共有 (administrative share)
管理特権のないユーザーに非表示になっているネットワーク・リソース。管理共有により、管理者はネットワーク・システム上のすべてのリソースにアクセスできる。

アノマリ (anomaly)
予期されるネットワークの動作からの逸脱。

アプリケーション・シグニチャー (application signature)
パケット・ペイロードの検証によって取得された一連の固有の特性。特定のアプリケーションを識別するために使用される。

ARP 「アドレス解決プロトコル (Address Resolution Protocol)」を参照。

ARP リダイレクト (ARP Redirect)
ネットワーク上に問題が存在する場合に、その問題をホストに通知するための ARP 方式。

ASN 「自律システム番号 (autonomous system number)」を参照。

アセット (asset)
稼働環境にデプロイされているか、デプロイされる予定の管理可能オブジェクト。

自律システム番号 (ASN) (autonomous system number (ASN))
TCP/IP において、IP アドレスの割り当てを行う同じ中央認証局によって自律システムに割り当てられる番号。自律システム番号を自動ルーティング・アルゴリズムで使用すると、自律システムを識別することができる。

B

動作 (behavior)
特定の操作やイベントについて、その結果を含めた監視可能な影響。

結合インターフェース (bonded interface)
「リンク集約 (link aggregation)」を参照。

バースト (burst)
ライセンス交付を受けたフローやイベント

の速度制限を超えるような、着信イベントまたはフローの突然で急激な増加。

C

CIDR 「クラスレス・ドメイン間ルーティング (Classless Inter-Domain Routing)」を参照。

クラスレス・ドメイン間ルーティング (CIDR) (Classless Inter-Domain Routing (CIDR))
クラス C のインターネット・プロトコル (IP) アドレスを追加するための方式。このアドレスはインターネット・サービス・プロバイダー (ISP) に提供され、そのプロバイダーのユーザーによって使用される。CIDR アドレスによってルーティング・テーブルのサイズが削減されるため、組織内でより多くの IP アドレスを使用できるようになる。

クライアント (client)
サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。

クラスター仮想 IP アドレス (Cluster virtual IP address)
プライマリー・ホストまたはセカンダリー・ホストと HA クラスターとの間で共有される IP アドレス。

統合間隔 (coalescing interval)
イベントがバンドルされる間隔。イベントのバンドルは 10 秒間隔で実行され、現在のいずれの統合イベントにも一致しない最初のイベントから開始される。統合間隔の間に、一致する最初の 3 つのイベントがバンドルされ、イベント・プロセッサーに送信される。

共通脆弱性評価システム (CVSS) (Common Vulnerability Scoring System (CVSS))
脆弱性の重大度を測定するための評価システム

コンソール (console)
オペレーターがシステム操作の制御と監視を行うためのディスプレイ装置。

コンテンツ・キャプチャー (content capture)
構成可能なペイロード量を取得し、そのデータをフロー・ログに格納するプロセス。

資格情報 (credential)
ユーザーまたはプロセスに対して特定のアクセス権を付与する情報のセット。

信頼性 (credibility)
イベントやオフェンスの保全性を判別するために使用される 0 から 10 までの数値による評価。複数のソースが同じイベントまたはオフェンスを報告すると、信頼性が高くなる。

CVSS 「共通脆弱性評価システム (Common Vulnerability Scoring System)」を参照。

D

データベース・リーフ・オブジェクト (database leaf object)
データベース階層内の終端のオブジェクトまたはノード。

データ・ポイント (datapoint)
特定の時点におけるメトリックの計算値。

デバイス・サポート・モジュール (DSM) (Device Support Module (DSM))
複数のログ・ソースから受信したイベントを解析し、出力として表示可能な標準分類形式に変換する構成ファイル。

DHCP 「動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)」を参照。

DNS 「ドメイン・ネーム・システム (Domain Name System)」を参照。

ドメイン・ネーム・システム (DNS) (Domain Name System (DNS))
ドメイン名を IP アドレスにマップする分散データベース・システム。

DSM 「デバイス・サポート・モジュール (Device Support Module)」を参照。

重複フロー (duplicate flow)
異なる複数のフロー・ソースから受信した、同じデータ伝送の複数のインスタンス。

動的ホスト構成プロトコル (DHCP) (Dynamic Host Configuration Protocol (DHCP))
構成情報を一元的に管理するために使用される通信プロトコル。例えば DHCP は、

ネットワーク内のコンピューターに対して自動的に IP アドレスを割り当てる。

E

暗号化 (encryption)
コンピューター・セキュリティーにおいて、元のデータを取得できないように判読不能な形式にデータを変換するプロセス。暗号化解除プロセスを使用しない限り、元のデータを取得することはできない。

エンドポイント (endpoint)
環境内の API またはサービスのアドレス。API は、エンドポイントを公開し、同時に他のサービスのエンドポイントを呼び出す。

外部スキャン・アプライアンス (external scanning appliance)
ネットワーク内のアセットに関する脆弱性情報を収集するためにネットワークに接続されているマシン。

F

フォールス・ポジティブ (false positive)
ポジティブ (サイトが攻撃に対して脆弱であることを示す) として分類されるが、実際のユーザーの判断はネガティブ (脆弱ではない) となるテスト結果。

フロー (flow)
対話時にリンク経由で通過するデータの 1 回の伝送。

フロー・ログ (flow log)
フロー・レコードの集合。

フロー・ソース (flow sources)
フローの取得元。管理対象ホストにインストールされているハードウェアからフローが発生している場合、フロー・ソースは内部フローとして分類され、フローがフロー・コレクターに送信される場合は、外部フローとして分類される。

転送宛先 (forwarding destination)
正規化された生データをログ・ソースとフロー・ソースから受信する 1 つ以上のベンダー・システム。

FQDN 「完全修飾ドメイン名 (fully qualified domain name)」を参照。

FQNN 「完全修飾ネットワーク名 (fully qualified network name)」を参照。

完全修飾ドメイン名 (FQDN) (fully qualified domain name (FQDN))
インターネット通信において、ドメイン名のサブネームをすべて含むホスト・システム名。完全修飾ドメイン名の例としては、rchland.vnet.ibm.com などがある。

完全修飾ネットワーク名 (FQNN) (fully qualified network name (FQNN))
ネットワーク階層において、すべての部門を含むオブジェクトの名前。完全修飾ネットワーク名の例としては、CompanyA.Department.Marketing などがある。

G

ゲートウェイ (gateway)
ネットワーク体系が異なるネットワークやシステムの接続に使用されるデバイスまたはプログラム。

H

HA 「高可用性 (high availability)」を参照。

HA クラスター (HA cluster)
1 台のプライマリー・サーバーと 1 台のセカンダリー・サーバーで構成される高可用性構成。

ハッシュ・ベース・メッセージ認証コード (HMAC) (Hash-Based Message Authentication Code (HMAC))
暗号ハッシュ機能と秘密鍵を使用する暗号コード。

高可用性 (HA) (high availability (HA))
特定のノードまたはデーモンで障害が発生した場合に、ワークロードをクラスター内の他のノードに再配分できるように再構成されるクラスター化システムに関連する構成。

HMAC
「ハッシュ・ベース・メッセージ認証コード (Hash-Based Message Authentication Code)」を参照。

ホスト・コンテキスト (host context)
コンポーネントをモニターし、各コンポーネントが正常に機能していることを確認するサービス。

I

ICMP 「Internet Control Message Protocol」を参照。

ID (identity)
人、組織、場所、項目を表す、データ・ソースの属性の集合。

IDS 「侵入検知システム (intrusion detection system)」を参照。

Internet Control Message Protocol (ICMP)
データグラムのエラーを報告するなどの目的で送信元ホストと通信する際に、ゲートウェイが使用するインターネット・プロトコル。

インターネット・プロトコル (IP) (Internet Protocol (IP))
ネットワークまたは相互接続ネットワーク経由でデータを送信するプロトコル。このプロトコルは、上位のプロトコル層と物理ネットワークとの間の中継役として機能する。「伝送制御プロトコル (Transmission Control Protocol)」も参照。

インターネット・サービス・プロバイダー (ISP) (Internet Service Provider (ISP))
インターネットへのアクセスを提供する組織。

侵入検知システム (IDS) (intrusion detection system (IDS))
ネットワークやホスト・システムの一部であるモニター対象リソース上での侵入の試みや実際の侵入を検出するソフトウェア。

侵入防止システム (IPS) (intrusion prevention system (IPS))
潜在的な悪意を持つアクティビティーを拒否するシステム。拒否の手段としては、フィルター処理、トラッキング、速度制限の設定などがある。

IP 「インターネット・プロトコル (Internet Protocol)」を参照。

IP マルチキャスト (IP multicast)
単一のマルチキャスト・グループを構成する一連のシステムに対するインターネット・プロトコル (IP) データグラムの伝送。

IPS 「侵入防止システム (intrusion prevention system)」を参照。

ISP 「インターネット・サービス・プロバイダー (Internet service provider)」を参照。

K

鍵ファイル (key file)
コンピューター・セキュリティーにおいて、公開鍵、秘密鍵、トラステッド・ルート、および証明書を含むファイル。

L

L2L 「ローカルからローカル」を参照。

L2R 「ローカルからリモート」を参照。

LAN ローカル・エリア・ネットワーク (Local Area Network) を参照してください。

LDAP 「Lightweight Directory Access Protocol」を参照。

リーフ (leaf)
ツリーにおいて、子を持たないエントリーまたはノード。

Lightweight Directory Access Protocol (LDAP)
TCP/IP を使用して、X.500 モデルをサポートするディレクトリーへのアクセスを提供し、より複雑な X.500 Directory Access Protocol (DAP) のリソース要件には制約されないオープン・プロトコル。例えば、LDAP を使用して、インターネット・ディレクトリーまたはイントラネット・ディレクトリーで個人や組織などのリソースを検索することができる。

リンク集約 (link aggregation)
ケーブルやポートなどの物理ネットワーク・インターフェース・カードの、単一の論理ネットワーク・インターフェースへのグループ化。リンク集約は、帯域幅およびネットワーク可用性を増大させるために使用される。

ライブ・スキャン (live scan)
セッション名に基づいてスキャン結果からレポート・データを生成する脆弱性スキャン。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN))
限定された領域内 (単一のビルやキャンパスなど) の複数のデバイスを接続するネットワーク。このネットワークを、さらに大きなネットワークに接続することができる。

ローカルからローカル (L2L) (Local To Local (L2L))
あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィックに関連する構成。

ローカルからリモート (L2R) (Local To Remote (L2R))
あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィックに関連する構成。

ログ・ソース (log source)
イベント・ログの発生元となるセキュリティー装置またはネットワーク装置。

ログ・ソース拡張 (log source extension)
イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイル。

M

判定機能 (magistrate)
定義されているカスタム・ルールに対してネットワーク・トラフィックとセキュリティー・イベントを分析する内部コンポーネント。

マグニチュード (magnitude)
特定のオフェンスの相対的な重要性の尺度。マグニチュードは、関連性、重大度、信頼性から算出された重みを持つ値である。

N

NAT
「ネットワーク・アドレス変換 (network address translation)」を参照。

NetFlow
ネットワーク・トラフィックのフロー・データをモニターする Cisco ネットワーク・プロトコル。 NetFlow データには、クライアントとサーバーの情報、使用されるポート、ネットワークに接続されているスイッチとルーターを通過するバイト数とパケット数が含まれている。このデータは NetFlow コレクターに送信され、NetFlow コレクターがデータの分析を行う。

ネットワーク・アドレス変換 (network address translation) (NAT)
ファイアウォールにおいて、セキュアなインターネット・プロトコル (IP) アドレスを外部の登録済みアドレスに変換すること。これにより、外部ネットワークとの通信が可能になり、ファイアウォール内部で使用される IP アドレスはマスクされる。

ネットワーク階層 (network hierarchy)
ネットワーク・オブジェクトの階層コレクションであるコンテナーの一種。

ネットワーク層 (network layer)
OSI アーキテクチャーにおいて、予測可能なサービス品質を持つ複数のオープン・システム間でパスを確立するためのサービスを提供する層。

ネットワーク・オブジェクト (network object)
ネットワーク階層の構成要素。

O

オフェンス (offense)
モニターされる条件への応答として送信されたメッセージまたは生成されたイベント。例えば、オフェンスは、ポリシー違反があったかどうか、ネットワークが攻撃されているかどうかなどの情報を提供する。

オフサイト・ソース (offsite source)
正規化されたデータをイベント・コレクターに転送する、プライマリー・サイトから離れた場所に存在するデバイス。

オフサイト・ターゲット (offsite target)
イベント・コレクターからイベント・フローまたはデータ・フローを受信する、プライマリー・サイトから離れた場所に存在するデバイス。

オープン・ソース脆弱性データベース (OSVDB) (Open Source Vulnerability Database (OSVDB))
ネットワーク・セキュリティー・コミュニティーがネットワーク・セキュリティー・コミュニティーのために作成した、ネットワーク・セキュリティーの脆弱性に関する技術情報を提供するオープン・ソース・データベース。

オープン・システム間相互接続 (OSI) (open systems interconnection (OSI))
国際標準化機構 (ISO) の標準に準拠した、情報交換のためのオープン・システムの相互接続。

OSI 「オープン・システム間相互接続 (OSI) (open systems interconnection)」を参照。

OSVDB
「オープン・ソース脆弱性データベース (Open Source Vulnerability Database)」を参照。

P

解析順序 (parsing order)
共通の IP アドレスまたはホスト名を共有するログ・ソースに対して、ユーザーが重要度の順序を定義できるログ・ソース定義。

ペイロード・データ (payload data)
IP フローに含まれるアプリケーション・データ。ただし、ヘッダーと管理情報は除く。

プライマリー HA ホスト (primary HA host)
HA クラスターに接続されるメイン・コンピューター。

プロトコル (protocol)
通信ネットワーク内の複数のデバイス間またはシステム間におけるデータの通信と転送を制御する一連のルール。

Q

QID マップ (QID Map)
それぞれの固有イベントを特定し、そのイベントを下位カテゴリーと上位カテゴリーにマップして、イベントの相関方法と編成方法を決定する分類法。

R

R2L 「リモートからローカル」を参照。

R2R 「リモートからリモート」を参照。

recon 「スキャン行為 (reconnaissance)」を参照。

スキャン行為 (reconnaissance (recon))
ネットワーク・リソースの ID に関連する情報を収集する方式。ネットワーク・スキャンやその他の技法を使用してネットワーク・リソース・イベントのリストがコンパイルされ、それらに重大度レベルが割り当てられる。

リファレンス・マップ (reference map)
キーから値 (例: ユーザー名からグローバル ID) への直接マッピングのデータ・レコード。

マップのリファレンス・マップ (reference map of maps) 2 つのキーが多くの値にマップされるデータ・レコード。例えば、アプリケーションの合計バイト数から送信元 IP へのマッピング。

セットのリファレンス・マップ (reference map of sets) 1 つのキーが多くの値にマップされるデータ・レコード。例えば、特権ユーザーのリストからホストへのマッピング。

リファレンス・セット (reference set)
ネットワーク上のイベントまたはフローから派生した単一エレメントのリスト。例えば、IP アドレスのリストやユーザー名のリスト。

リファレンス・テーブル (reference table)
データ・レコードが、割り当てられている

タイプを持つキーを他のキーにマップし、次に単一の値にマップするテーブル。

最新表示タイマー (refresh timer)
一定の間隔で、手動または自動でトリガーされる内部デバイス。このデバイスにより、現在のネットワーク・アクティビティー・データが更新される。

関連性 (relevance)
ネットワーク上のイベント、カテゴリー、オフェンスの相対的な影響の尺度。

リモートからローカル (R2L) (Remote To Local (R2L)) リモート・ネットワークからローカル・ネットワークへの外部トラフィック。

リモートからリモート (R2R) (Remote To Remote (R2R)) リモート・ネットワークから別のリモート・ネットワークへの外部トラフィック。

レポート (report)
照会管理において、照会の実行結果にフォームを適用したフォーマット済みデータ。

レポート間隔 (report interval)
構成可能な時間間隔。この間隔の最後に、イベント・プロセッサー・プログラムは、取得したすべてのイベント・データとフロー・データをコンソールに送信する。

ルーティング・ルール (routing rule)
イベント・データによって基準が満たされた場合に、条件の集合とその結果として発生するルーティングが実行される条件。

ルール (rule)
コンピューター・システムが関係を識別し、それに応じて、自動化された応答を実行できるようにする一連の条件ステートメント。

S

スキャナー (scanner)
Web アプリケーション内でソフトウェアの脆弱性を検索する、自動化されたセキュリティー・プログラム。

セカンダリー HA ホスト (secondary HA host)
HA クラスターに接続されるスタンバイ・コンピューター。プライマリー HA ホストで障害が発生した場合は、セカンダリー HA ホストがプライマリー HA ホストの処理を引き継ぐ。

重大度 (severity)
ソースが宛先に及ぼす相対的な脅威の尺度。

Simple Network Management Protocol (SNMP)
複雑なネットワーク内のシステムとデバイスをモニターするための一連のプロトコル。管理対象デバイスに関する情報は、管理情報ベース (MIB) で定義されて保管される。

SNMP 「Simple Network Management Protocol」を参照。

SOAP 非集中型の分散環境で情報を交換するための XML ベースの軽量プロトコル。SOAP を使用して、インターネット経由で情報を照会して情報を返し、サービスを呼び出すことができる。

スタンバイ・システム (standby system)
アクティブなシステムで障害が発生した場合に、自動的にアクティブになるシステム。ディスクの複製が有効になっている場合、スタンバイ・システムはアクティブなシステムからデータを複製する。

サブネット (subnet)
「サブネットワーク (subnetwork)」を参照。

サブネット・マスク (subnet mask)
インターネット・サブネットワークで、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットの識別に使用される 32 ビットのマスク。

サブネットワーク (サブネット) (subnetwork (subnet))
相互に接続された、より小さな独立したサブグループに分割されているネットワーク。

サブ検索 (sub-search)
完了した検索結果セット内での検索照会の実行を可能にする機能。

スーパーフロー (superflow)
ストレージの制約を削減することによって

処理能力を向上させるために、類似するプロパティーを持つ複数のフローから構成される単一のフロー。

システム・ビュー (system view)
システムを構成するプライマリー・ホストと管理対象ホストの視覚的な表現。

T

TCP 「伝送制御プロトコル (Transmission Control Protocol)」を参照。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP))
インターネットで使用される通信プロトコル。また、インターネットワーク・プロトコル用の Internet Engineering Task Force (IETF) 標準に準拠するネットワークでも使用される。TCP は、パケット交換通信ネットワークと、パケット交換通信ネットワークの相互接続システムにおいて、信頼できるホスト間プロトコルを提供する。「インターネット・プロトコル (Internet Protocol)」も参照。

トラストストア・ファイル (truststore file)
トラステッド・エンティティーの公開鍵が入っている鍵データベース・ファイル。

V

違反 (violation)
企業のポリシーをバイパスする行為、または企業のポリシーに違反する行為。

脆弱性 (vulnerability)
オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

WHOIS サーバー (whois server)
ドメイン名や IP アドレスの割り振りなど、登録されているインターネット・リソースに関する情報の取得に使用されるサーバー。