

Cisco Security Monitoring, Analysis and Response System 4.2.x/5.2x

Cisco® Security Monitoring, Analysis and Response System (CS-MARS)は、ネットワークに導入されたセキュリティ対策を有効に利用し、これらを制御するアプライアンスです。シスコのセキュリティ管理ライフサイクルの主要なコンポーネントである CS-MARS は、セキュリティおよびネットワークの管理部門が、セキュリティ脅威を識別および管理し、これに対応するための機能を強化します。CS-MARS を使用すると、既存のネットワークおよびセキュリティへの投資を活用しながら、問題となる要素の識別、切り離し、的確な排除が可能となります。また、このシステムは組織のセキュリティ ポリシーに従った適切な運用を支援します。

セキュリティ管理者およびネットワーク管理者は、次のようなさまざまな問題に直面しています。

- 膨大な量のセキュリティおよびネットワークの情報
- 攻撃や障害の識別、優先順位付け、および対応のための機能不足
- 攻撃の高度化と高速化、および復旧コストの増加
- セキュリティ ポリシーの遵守と監査要件への対応
- セキュリティ スタッフおよび予算の制約

CS-MARS は、次のような機能によって、これらの問題を解決します。

- ネットワーク インテリジェンスを統合し、ネットワーク異常やセキュリティ イベントの相関分析を実施
- 確認されたインシデントを視覚化し、調査を自動化
- 既存のネットワークおよびセキュリティのインフラストラクチャを活用して攻撃を軽減
- システム、ネットワーク、およびセキュリティの動作を監視して、セキュリティ ポリシーへの準拠をサポート
- 最小限の総所有コスト (TCO) で簡単に導入および運用できる、スケーラブルなアプライアンスを提供

CS-MARS は、未処理のネットワーク データおよびセキュリティに関する一次データを解析し、必要な対策に直結する情報に変換することで、適切にセキュリティ インシデントを排除するとともに、セキュリティ ポリシーの遵守を可能にします。また、CS-MARS では操作性に優れたユーザ インターフェイスを提供しており、オペレータはインフラストラクチャにすでに導入されているネットワーク デバイスとセキュリティ デバイスを利用しながら、脅威を優先順位付けし、これに対する一元処理、検出、対応、および報告を行うことができます。

防御におけるジレンマ

情報セキュリティの実装は、インターネットとの境界での保護を目的とするものから始まり、プライベートネットワーク内部への導入を含む、より複雑な防御モデルへと発展してきました。このモデルでは、複数のセキュリティ対策をインフラストラクチャ全体に階層的に配置して、脆弱性と攻撃に対処します。攻撃の頻度の増加、多様化、高速化のために、ネットワーク内部や境界といった概念にとらわれない、このようなモデルが不可欠となっています。

ネットワーク アクセス ポイントおよびシステムに対しては、脆弱性を利用しようとする者から、日に数千回ものアクセスが試行されています。最新の複合型の攻撃では、組織の外部および内部から不正なシステム アクセスや制御を行うために、複数の不正な攻撃方法が使用されています。ワーム、Day Zero 攻撃、ウイルス、トロイの木馬、スパイウェア、および攻撃ツールの急増により、きわめて堅固に防御されたインフラストラクチャですら攻撃の対象になり、対応時間の不足、ダウンタイム、多額の復旧コストなどが発生しています。

ネットワーク上に設置された各種のセキュリティ コンポーネントは、異常検出、脅威への対応、フォレンジクスに必要なデータを含むイベント ログやアラート機能を提供しています。しかし、こういったイベント ログやアラートの総数が急増した結果、オペレータは膨大な量の警告、アラーム、ログ ファイル、およびフォールス ポジティブを識別し、効率的に利用しなければならなくなっています(ただし、これらの情報を解析し理解するだけの時間とリソースがある場合に限りです)。また、セキュリティ ポリシーを維持するためには、データ プライバシーの保護、運用セキュリティの改善、および監査プロセスの保守も必要です。

高度なセキュリティ情報管理および脅威の軽減

セキュリティ情報およびイベント管理製品は、脅威を測定して管理できるようにすることを目的としているため、論理上はこれらの問題を軽減するものと考えられます。これらの製品によってオペレータは、セキュリティ イベントとログの集約、限定された相関とクエリーによるこれらのデータの分析、および個別のイベントに関するアラームとレポートの生成を一元的に実行できます。

第一世代および第二世代のセキュリティ情報およびイベント管理製品の多くは、ネットワーク インテリジェンスやパフォーマンスが十分ではなく、相関性のあるイベントの正確な識別と検証、攻撃経路の特定、脅威の根本的な除去、またはイベント負荷の高い環境での継続的な動作には対応できませんでした。このようなセキュリティの問題と管理の欠如に対処するため、シスコシステムズではスケーラブルな企業向け脅威軽減対策アプライアンス ファミリーを提供しています。CS-MARS は、導入と運用が簡単で、コスト効率に優れたセキュリティ脅威の制御および封じ込めソリューションを提供することにより、ネットワークおよびセキュリティ インフラストラクチャへの投資を補完します。CS-MARS は、ハイ パフォーマンスでスケーラブルな脅威軽減対策アプライアンス ファミリーです。ネットワーク インテリジェンス、ContextCorrelation™ 機能、SureVector™ 分析、および AutoMitigate™ 機能を統合することで、企業がネットワーク攻撃を迅速に識別、管理、および排除し、組織のセキュリティを遵守するとともに、導入されているネットワーク デバイスの有効な利用とセキュリティ対策の強化を実現します。

CS-MARS は、シスコの高性能セキュリティ管理スイートである Cisco Security Manager と緊密な連携が可能です。この統合化により、Cisco Security Manager からのイベントをトリガーにして、トラフィックに伴うSyslog メッセージと、Cisco Security Manager 上で定義されたファイアウォールおよび IPS ポリシーとをマッピングできます。ポリシー ルックアップによって高速なラウンドトリップ分析が可能になり、IPS とファイアウォール設定に関連するネットワークの問題、ポリシー設定エラーのトラブルシューティングを行うことができます。さらに、定義済みポリシーの微調整も可能となります。

機能と利点

ネットワークのインテリジェントなイベント集約と高速処理

CS-MARS は、ネットワーク トポロジを理解し、ルータ、スイッチ、およびファイアウォールといった機器の設定情報を認識し、さらにネットワーク トラフィックの傾向を把握することによって、ネットワークをインテリジェントに管理します。システムに組み込まれたネットワーク検出機能により、デバ

イス設定と現在のセキュリティ ポリシーを含むトポロジ マップが作成され、これによってネットワーク上でのパケット フローのモデル化が可能になります。CS-MARS はインラインでは動作せず、また既存のソフトウェア エージェントをほとんど使用しないので、ネットワークまたはシステム パフォーマンスへの影響はわずかです。

CS-MARS は、一般的な各種ネットワーク デバイス(ルータ、スイッチなど)、セキュリティ デバイスとアプリケーション(ファイアウォール、侵入検知システム [IDS]、脆弱性スキャナ、ウイルス対策アプリケーションなど)、ホスト(Windows、Solaris、Linux Syslog など)、アプリケーション(データベース、Web サーバ、認証サーバなど)、およびネットワーク トラフィック(Cisco NetFlow など)から、ログやイベントを収集します。

Cisco ContextCorrelation

CS-MARS の ContextCorrelation 機能は、イベントおよびデータを受信したときに、トポロジ、検出されたデバイス設定、(Network Address Translation [NAT; ネットワーク アドレス変換] 境界を越えて)同じ送信元と宛先のアプリケーションかどうかに基づいて正規化して分析します。一致するイベントは、リアルタイムでセッションにグループ化されます。システム定義およびユーザ定義の相関ルールは、複数のセッションに適用され、インシデントとして識別されます。CS-MARS は、シスコによって随時更新される定義済みルールを導入して出荷されます。これらの定義済みルールによって、複合型の攻撃シナリオ、Day Zero 攻撃、およびワームの大半を識別できます。ユーザ定義のカスタム ルールは、グラフィカルなルール フレームワークを使って簡単に作成できます。ContextCorrelation は、未処理のイベント データを大幅に削減し、対応の優先順位付けを容易にして、導入されたセキュリティ対策の効果を最大限に引き出します。

セキュリティ関連情報のハイ パフォーマンスな集約と統合

CS-MARS は、数百万もの未処理のイベントをキャプチャし、新たなデータ削減機能によりインシデントを効率的に分類して、この情報をアーカイブ用に圧縮します。この大量のセキュリティ イベントを管理するには、安全で安定した集中型のプラットフォームが必要です。CS-MARS アプライアンスは、強固なセキュリティを備え、非常に大量なイベント トラフィック(1 秒間に 15,000 を超えるイベントまたは 300,000 を超える Cisco NetFlow イベント)を受信できるように最適化されています。このハイパフォーマンスな相関分析は、インライン処理ロジックおよびシステムに組み込まれたハイパフォーマンス データベース システムを利用することで実現されています。データベース機能およびチューニングを、ユーザが意識することはありません。内部にストレージを搭載し、NFS (Network File System)セカンダリ ストレージ デバイスへの履歴データの継続的なアーカイブと圧縮に対応することにより、CS-MARS は、信頼性の高いセキュリティ ログ/イベント集約ソリューションとして機能します。

インシデントの視覚化と軽減機能

CS-MARS を使用すると、脅威の識別、調査、検証、および軽減のプロセスを高速化および簡素化することができます。セキュリティ スタッフは、解決と復旧に多くの時間を必要とする膨大なイベントに頻繁に直面しています。CS-MARS は、強力な対話形式のセキュリティ管理ダッシュボードを提供します。オペレータ GUI でリアルタイムのホットスポット、インシデント、攻撃経路、および詳細な調査情報で構成されるトポロジ マップを表示することにより、インシデントの詳細情報を明らかにして、被害をもたらす恐れのある脅威を迅速に検証できるようにします。

Cisco SureVector 分析プロセスは、類似したイベント セッションを処理し、エンドポイントの MAC アドレスに至るまでの攻撃経路全体を評価して、脅威が効力を持っているか、または対処が行われているかを判断します。この自動プロセスは、ファイアウォールや IPS(侵入防御システム)など

のデバイス ログの分析、サード パーティが提供する脆弱性評価データの分析、およびフォールス ポジティブを排除する CS-MARS のエンドポイント スキャンによって実行されます。ユーザは、システムを迅速かつきめ細かく調整し、フォールス ポジティブをさらに削減できます。

セキュリティ プログラムの目標は、システムをオンライン状態に維持しながら適切に機能させることです。これは、セキュリティの破綻を防ぎ、インシデントを抑制して、復旧を容易にするために重要な意味を持ちます。CS-MARS を使用することで、オペレータは、問題の原因になっているシステム MAC アドレスなど、攻撃に含まれるすべてのコンポーネントを迅速に把握できます。Cisco AutoMitigate 機能は、攻撃への対処が可能なデバイスと攻撃経路を識別し、ユーザが脅威を軽減するために使用できる適切なコマンドを自動的に提供します。これによって、攻撃を迅速かつ正確に防止または抑制できます。

リアルタイムの調査とレポート

CS-MARS は、これまでのセキュリティ ワークフローを合理化する使いやすい分析フレームワークを備え、インシデントの自動分類、調査、エスカレーション、通知、および注釈機能を提供することで、通常業務だけでなく特殊な監査要求などにも対応しています。CS-MARS は、過去のイベントを分析するために、攻撃をグラフィカルに再現し、保存されているイベント データを取り出します。また、リアルタイムおよび後日のデータ マイニングに対応するために、アドホック クエリーをフルサポートしています。

CS-MARS は、あらかじめ定義されたさまざまなレポート作成機能を備えているため、運用要件を満たし、法令を順守するために役立てることができます。対応する法令には、Sarbanes-Oxley (SOX; 米国企業改革法)、Gramm-Leach Bliley Act (GLBA; 米国金融制度改革法)、Health Insurance Portability and Accountability Act (HIPAA; 医療保険の相互運用性と説明責任に関する法律)、米国の Federal Information Security Management Act (FISMA; 連邦情報セキュリティ管理法)、EU の Revised Basel Capital Framework (Basel II) などがあります。CS-MARS は、レポート ジェネレータによって 100 を超える標準レポートを微修正したり、ユーザごとのニーズに応じたカスタム レポートの新規作成を行ったりすることができます。たとえば、実行計画および復旧計画、インシデントおよびネットワーク アクティビティ、セキュリティ状況および監査、さらには部門レポートなどを、データ形式、トレンド形式、グラフ形式などで作成できます。バッチおよび E メールでのレポートもサポートされています。

Network Admission Control (NAC) のサポート

CS-MARS では、レイヤ 2 スイッチと Cisco Secure Access Control Server (ACS) の両方からの 802.1X 認証イベントの解析、標準化、関連付け、およびレポートを実行します。レイヤ 3 ルータおよび Cisco VPN 3000 シリーズ コンセントレータについても、Extensible Authentication Protocol (EAP) を使用して同様の処理を行います。これにより、スイッチ、Cisco Secure ACS、検証対象のエンドポイント、および Active Directory または Network Information Service (NIS) などの外部認証ソース間の接続チェーンを調べて、デバイス認証方法のトラブルシューティングを実行することができます。また、CS-MARS では、NAC (Network Admission Control) フェーズ 1 とフェーズ 2 パラメータに関する一括レポートを作成できます。このレポートには、デバイス認証およびポスチャ認証に失敗した理由が詳細に示されます。レポート内容には、以下のような情報が含まれます。

- ユーザ レポート
- ユーザの詳細情報
- エンドポイントの詳細情報
- 実行されなかったエンドポイント レポート

- エンドポイント ステータス クエリーの障害レポート
- アプリケーション ポスチャトークン配布レポート
- エンドポイント違反およびユーザによる違反の各上位 10 件分のレポート
- エンドポイント別復旧時間レポート

迅速な導入とスケーラブルな管理

CS-MARS は、TCP/IP ネットワーク上に配置され、標準の安全なプロトコルまたはベンダー固有のプロトコルを介して、導入されたネットワークおよびセキュリティ デバイスとの間でイベントやアラート情報を送受信し、安全なセッションを確立します。CS-MARS のインストールと導入には、ハードウェア、オペレーティング システム パッチ、ライセンス、または長期にわたるプロフェッショナル サービス契約の追加は必要ありません。CS-MARS アプライアンスを送信先とするようにログのソースとなるデバイスを設定し、Web ベースの GUI を介してネットワークとソースを定義するだけです。既存の syslog-ng サーバまたは Kiwi Syslog サーバからメッセージを転送すると、CS-MARS を迅速に導入できます。この機能によって、CS-MARS を運用中のネットワークに組み込む際に必要となる、多くのネットワークおよびデバイス変更作業が不要になります。

CS-MARS は、ロールベースの管理および認証をサポートする安全な Web ベース インターフェイスを使用して集中的に管理できます。オプションのグローバル コントローラ アプライアンスは、拡張したセキュリティ管理を一元化して、企業全体を 1 つのビューで表示し、アクセス権限、設定、更新、カスタム ルール、およびレポート テンプレートを提供します。また、高速のクエリーおよびローカル処理されるレポートにより、複雑な調査を統合します。

ローカルの CS-MARS アプライアンスが企業全体に対してクエリーとルールを実行すると、その結果が収集されて、システムのグローバル コントローラによる迅速かつ集中的な分析が行われます。このスケーラブルなアーキテクチャにより、分散処理とストレージ機能が拡張されます。その結果、地理的に広範囲に分散した大規模組織の要件に対応する、費用対効果の高い導入と優れた管理が可能になります。

CS-MARS の技術仕様

バージョン情報

4.2.x リリースは、引き続き MARS-20R、MARS-20、MARS-50、MARS-100e、MARS-100、MARS-200、MARS-GCm、MARS-GC アプライアンスをサポートします。5.2.x リリースは、新しいアプライアンス モデルである MARS-110R、MARS-110、MARS-210、MARS-GC2 の機能をサポートします。2 つのリリース間の主な機能は同等です。アプライアンスの違いにより、いくつかの機能の実装については若干の差異が生じる可能性があります。開発チームは同等の機能を並行してサポートしていくよう努力しています。詳しくは、リリース Q&A を参照してください。

CS-MARS では、多様なネットワークの規模や導入目的に対応するため、さまざまなパフォーマンス特性と価格の製品ファミリーを用意しています (表 1)。

表 1 CS-MARS 製品

シスコ製品番号(ローカルコントローラモデル)	イベント/秒 ¹	NetFlowフロー/秒	ストレージ	ラックユニット	電力
CS-MARS 20R (CS-MARS-20R-K9)	50	1500	120 GB(非 RAID)	1 RU × 16 インチ	300 W、120/240 V 自動切り替え
CS-MARS 20 (CS-MARS-20-K9)	500	15,000	120 GB(非 RAID)	1 RU × 16 インチ	300 W、120/240 V 自動切り替え
CS-MARS 50 (CS-MARS-50-K9)	1000	30,000	240 GB RAID 0	1 RU × 25.6 インチ	300 W、120/240 V 自動切り替え
CS-MARS 100e (CS-MARS-100E-K9)	3000	75,000	750 GB RAID 10 ホットスワップ可能	3 RU × 25.6 インチ	500 W デュアル冗 長、120/240 V 自動 切り替え
CS-MARS 100 (CS-MARS-100-K9)	5000	150,000	750 GB RAID 10 ホットスワップ可能	3 RU × 25.6 インチ	500 W デュアル冗 長、120/240 V 自動 切り替え
CS-MARS 200 (CS-MARS-200-K9)	10,000	300,000	1 TB RAID 10 ホッ トスワップ可能	4 RU × 25.6 インチ	500 W デュアル冗 長、120/240 V 自動 切り替え
CS-MARS 110R (CS-MARS-110R-K9)	4,500	75,000	1,500 GB RAID 10 ホットスワップ可能	2 RU × 奥行 27 3/4 インチ × 高さ 3.44 イ ンチ × 幅 19 インチ	2 × 750 W デュア ル冗長、120/240 V 自動切り替え
CS-MARS 110 (CS-MARS-110-K9)	7,500	150,000	1,500 GB RAID 10 ホットスワップ可能	2 RU × 奥行 27 3/4 インチ × 高さ 3.44 イ ンチ × 幅 19 インチ	2 × 750 W デュア ル冗長、120/240 V 自動切り替え
CS-MARS 210 (CS-MARS-210-K9)	15,000	300,000	2,000 GB RAID 10 ホットスワップ可能	2 RU × 奥行 27 3/4 インチ × 高さ 3.44 イ ンチ × 幅 19 インチ	2 × 750 W デュア ル冗長、120/240 V 自動切り替え

1 イベント/秒: 動的な相関分析とすべての機能が有効な場合の 1 秒あたりのイベントの最大処理数

シスコ製品番号(グローバルコントローラモデル)		分散モニタリング			
	サポートされるモデル	最大接続数	ストレージ	ラックユニット	電力
CS-MARS GCm (CS-MARS-GCm-K9)	CS-MARS 20R/20/50	5	1 TB RAID 10 ホットスワップ可能	4 RU × 奥行 25.6 インチ × 幅 19 インチ	2 × 500 W デュア ル冗長、120/240 V 自動切り替え
CS-MARS GC (CS-MARS-GC-K9)	CS-MARS 20R/20/50/100/ 100e/200	現在は制限なし	1 TB RAID 10 ホットスワップ可能	4 RU × 25.6 イ ンチ	500 W デュアル冗 長、120/240 V 自動 切り替え
CS-MARS GC2 (CS-MARS-GC2-K9)	CS-MARS 110/110R/210	現在は制限なし	2 TB RAID 10 ホットスワップ可能	2 RU × 奥行 27 3/4 インチ × 高さ 3.44 イ ンチ × 幅 19 インチ	2 × 750 W デュア ル冗長、120/240 V 自動切り替え

動的なセッションベースの相関分析

- Cisco NetFlow を含むネットワークベースの異常検出
- ふるまいベースおよびルールベースのイベント相関分析
- 包括的な組み込みルールおよびユーザ定義ルール
- NAT 処理への自動対応

トポロジの検出

- レイヤ 3 および レイヤ 2 ルータ、スイッチ、ファイアウォール
- ネットワーク IDS: ブレードおよびアプライアンス
- 手動による検出および定期的な検出
- Secure Shell (SSH)、SNMP、Telnet、およびデバイス固有の通信

脆弱性の分析

- インシデントによってトリガーされるネットワーク ベースおよびホスト ベースのフィンガープリント
- スイッチ、ルータ、ファイアウォール、および NAT 構成の分析
- 自動脆弱性スキャナ データ キャプチャ
- 自動およびユーザ調整によるフォールス ポジティブの分析

インシデントの分析と対応

- ロール ベースのセキュリティ イベント管理ダッシュボード
- 完全なルール コンテキストを使用したセッションベースのイベント統合
- 詳細な調査による攻撃経路のグラフィカルな視覚化
- エンドポイント MAC ID を使用した攻撃経路のデバイス プロファイル
- グラフィカルで詳細な連続攻撃パターンの表示
- インシデントの詳細: ルール、未処理イベント、Common Vulnerabilities and Exposure (CVE)、および軽減オプション
- 迅速なインシデント調査とフォールス ポジティブの判断
- カスタム ルールとキーワード解析をサポートする GUI によるルール定義
- ユーザベースの「作業」リストを使用したインシデントのエスカレーション
- 通知: E メール、ポケットベル、Syslog、SNMP
- XML (Extensible Markup Language) イベント通知による既存のチケット システムおよびワークフロー システムへの統合

クエリーとレポート

- 遅延の少ないリアルタイムのイベント クエリー
- さまざまなデフォルトのクエリーとカスタマイズ クエリーをサポートする GUI
- 150 を超える標準のレポート: 管理、運用、および規制 (米国内の規制に対応)
- 操作性に優れたレポート生成機能による、カスタム レポートの作成
- HTML および CSV 形式のエクスポートをサポートするデータ形式、グラフ形式、およびトレンド形式のレポート
- リアルタイム、バッチ、テンプレート、および E メール フォワーディング レポート システム
- 特定のインシデントにおける情報に効果的にドリル ダウンするための使いやすいクエリー構造の構築

管理性

- Web インターフェイス (HTTPS): 定義済みの権限に基づくロールベースの管理
- 複数の CS-MARS をグローバル コントローラ によって階層的に管理
- 検証済みの自動更新: デバイスのサポート、新しいルール、および機能
- オフライン NFS ストレージへの素データとインシデント アーカイブを圧縮して継続的に保存

サポートされるデバイス

- ネットワーク: Cisco IOS ソフトウェア、Cisco Catalyst® OS、Cisco NetFlow、および Extreme Extremeware
- ファイアウォール/VPN: Cisco ASA Software、Cisco PIX® セキュリティ アプライアンス、Cisco IOS ファイアウォール、Cisco FWSM (Firewall Services Module)、Cisco VPN 3000 コンセントレータ、Checkpoint Firewall-1 NG および VPN-1 バージョン、NetScreen ファイアウォール、および Nokia Firewall Intrusion Detection、Cisco IDS、Cisco IDS モジュール、Cisco IOS IPS、Enterasys Dragon NIDS、ISS RealSecure Network Sensor、Snort NIDS、McAfee Intrushield NIDS、NetScreen IDP、OS、および Symantec ManHunt
- 脆弱性の評価: eEye REM、Qualys QualysGuard、および FoundStone FoundScan
- ホスト セキュリティ: Cisco Security Agent、McAfee Enterecept、および ISS RealSecure Host Sensor
- ウイルス対策ソフトウェア: Symantec Antivirus、Cisco ICS (Incident Control System)、Trend Micro Outbreak Prevention Service (OPS)、Network Associates VirusScan、および McAfee ePO
- 認証サーバ: Cisco Secure ACS
- ホスト ログ: Windows NT、2000、および 2003 (エージェントおよびエージェントレス)、Solaris、および Linux
- アプリケーション: Web サーバ (Internet Information Server、iPlanet、および Apache)、Oracle 監査ログ、および Network Appliance NetCache
- アプリケーション Syslog を集約およびサポートするための汎用的なデバイス サポート
- カスタム ログ解析機能による追加的なカスタム デバイスのサポート

CS-MARS ではデバイスのサポートを今後も一層充実させていきます。サポート対象のバージョンなどについての最新情報は、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html

その他のハードウェア仕様

- 19 インチ ラックマウント アプライアンス、UL、VCCI、CE、FCC Part 15 承認
- セキュリティが強化された OS: サービスを制限したファイアウォールを設置
- 10/100/1000 MB イーサネット インターフェイス × 2
- リカバリ メディア付き DVD-ROM

発注情報

表 2 に、CS-MARS の発注情報を示します。

表 2 CS-MARS の発注情報

製品名 ²	製品番号
CS-MARS 20R、最大 50 イベント/秒および 1500 NetFlow フロー/秒	CS-MARS-20R-K9
CS-MARS 20、最大 500 イベント/秒および 15,000 NetFlow フロー/秒	CS-MARS-20-K9
CS-MARS 50、最大 1000 イベント/秒および 30,000 NetFlow フロー/秒	CS-MARS-50-K9
CS-MARS 100e、最大 3000 イベント/秒および 75,000 NetFlow フロー/秒	CS-MARS-100E-K9
CS-MARS 100、最大 5000 イベント/秒および 150,000 NetFlow フロー/秒	CS-MARS-100-K9

製品名 ²	製品番号
CS-MARS 200、最大 10,000 イベント/秒および 300,000 NetFlow フロー/秒	CS-MARS-200-K9
CS-MARS 110R、最大 4,500 イベント/秒および 75,000 NetFlow フロー/秒	CS-MARS-110R-K9
CS-MARS 110R から CS-MARS 110 へのアップグレード	CSMARS-110-LIC-K9=
CS-MARS 110、最大 7,500 イベント/秒および 150,000 NetFlow フロー/秒	CS-MARS-110-K9
CS-MARS 210、最大 15,000 イベント/秒および 300,000 NetFlow フロー/秒	CS-MARS-210-K9
CS-MARS GCm、最大 5 台のローカル コントローラ モデル 20 または 50 の分散モニタリング	CS-MARS-GCM-K9
CS-MARS GC、任意の台数の全ローカル コントローラ モデルの分散モニタリング	CS-MARS-GC-K9
CS-MARS GC2、任意の台数の全ローカル コントローラ モデルの分散モニタリング	CS-MARS-GC2-K9

2 その他の製品仕様は表 1 を参照してください。

サービスおよびサポート

シスコは、お客様がそのネットワーク サービスを最大限に活用するため、各種サービス プログラムを用意しています。これらのサービスは、スタッフ、プロセス、ツールをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワーク インテリジェンスの強化や事業拡張を進めていただくためにシスコのサービスを是非お役立てください。サービスについての詳細は、以下の URL を参照してください。

テクニカル サポート サービス

<http://www.cisco.com/jp/go/tac/>

サービス プログラム

<http://www.cisco.com/jp/services/>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先