
# アプライアンスの概要

この章では、Cisco Security Monitoring, Analysis, and Response System（MARS）のコンポーネントを定義し、各種アプライアンス モデルの前面パネルおよび背面パネルについて説明します。この章で説明する内容は、次のとおりです。

# システムの概要

Cisco Security MARS は、Security Threat Mitigation（STM; セキュリティ脅威軽減）システムです。ネットワーク上の装置からのレポートに基づいて、ネットワーク動作に関する広範囲の情報を提供します。レポーティング デバイスからの生イベントを処理し、各種装置間でセッショナイズ[1] し、一致検査ルール（システムおよびユーザ定義）を評価し、フォールス ポジティブを識別し、図、表、クエリー、レポート、ルールを使用して情報を統合します。

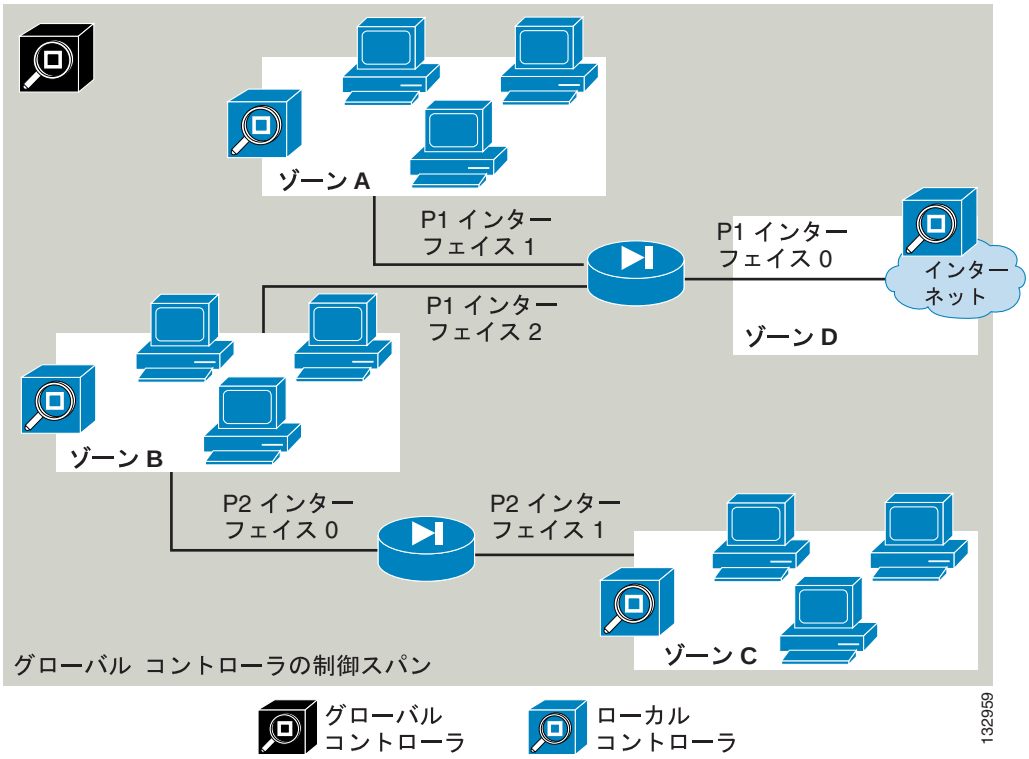
MARS は、次の機能により、生産性向上を支援します。

- 手動でのレビューを必要とする生データの量を減少
- ネットワーク セキュリティ方針の進行状態を表示
- 悪意のある動作のホット スポットを識別
- 不要なトラフィックをネットワークからブロック

MARS システムは、ネットワークのレポーティング デバイスに関して提供される情報量に基づいて、明確に異なるレベルで動作します。最も基本的なレベルでは、MARS は syslog サーバとして動作します。レポーティング デバイスの情報を追加すると、MARS は生データのセッショナイズを開始します。さらに追加のレポーティング デバイスを設定し、より詳細なレポート機能をイネーブルにすると、ネットワークのより包括的なビューが提供され、そこから特定の MAC アドレスなどを迅速に絞り込むことができます。

図 1-1 に、システムのコンポーネントと相互関係を示す、MARS の配置例を示します。

**図 1-1　Global Controller、Local Controller、およびレポート / 脅威軽減デバイスの関係**




1. セッショナイズとは、単一セッションまたは通信の一部として、開始、本文、および終了のパケットを判別するために、報告されたネットワーク データ、ログ、およびイベントを関連付けて高レベルの解析を行うことを意味します。

Cisco Security MARS システムは、次のコンポーネントで構成されます。



## ローカル コントローラ

Local Controller は、5 つのモデル — MARS 20、MARS 50、MARS 100、MARS 100e、および MARS 200 を使用できる MARS アプライアンスです。各モデルは、レポーティング デバイスからのイベントの処理機能および保存容量が異なり、実ネットワークのサイズおよびトラフィック量に基づいて、最適なモデルを選択できます。

Local Controller は、ファイアウォール、ルータ、侵入検知 / 防止システム、脆弱性査定システムなどのレポーティング デバイスからデータを受信し、抽出します。これらのデバイスから取得したデータ、およびデータの統合レベルに基づいて、MARS は検出された攻撃に対して推奨する脅威軽減ルールを提示し、状況によっては、攻撃の対象となったネットワーク装置である脅威軽減デバイスにこれらのルールを適用し、影響を受けたホストへのネットワーク アクセスを制限します。

Local Controller は、モニタ対象のレポーティング デバイスから受信するデータに基づいて、ネットワーク動作に関する情報を要約します。

Local Controller は、次の機能を実行します。

- すべての生イベントの収集
- 各種デバイス間でのイベントのセッショナイズ
- 特定の事象に対する検査ルールの適用
- フォールス ポジティブの判別
- 図、表、クエリー、レポート、および通知による統合情報の配信
- 非アクティブなレポーティング デバイスの検出
- モニタ対象の Cisco IPS 5.x アプライアンスにより報告された攻撃に基づく、IOS/IPS Distributed Threat Mitigation（DTM）シグニチャ セットの抽出
- IOS/IPS デバイスが最新のシグニチャ セットをダウンロードできる、IOS/IPS DTM シグニチャのレポジトリとして動作

## グローバル コントローラ

多数のLocal Controllerを配置する場合には、複数のLocal Controllerの情報を要約するGlobal Controllerを配置できます。この方法で Global Controller を使用することにより、管理作業を増やさずにネットワークのモニタリングを拡張できます。Global Controller は、新しいデバイス タイプ、検査ルール、およびクエリーを定義する単一ユーザ インターフェイスを提供し、Local Controller を一元管理できます。この管理には、管理アカウントの定義、およびリモート Local Controller の分散アップグレードの実行が含まれます。Global Controller には、MARS GCm および MARS GC の 2 つのモデルがあります。

## MARS HTML インターフェイス

MARS HTML インターフェイスは、クライアント コンピュータ上で動作します。Local Controller および Global Controller の両方に共通する多数の機能を備えた HTML インターフェイスは、タブ付き、ハイパーリンク付きのブラウザ ベースのユーザ インターフェイスです。HTML インターフェイスは、ネットワーク上の MARS アプライアンスにアクセスできる任意のコンピュータからアクセスできます。クライアント要件の詳細については、Web ブラウザ クライアントの要件（p.3-10）を参照してください。

HTML インターフェイスでは、コマンドラインでサポートされないすべての機能を含め、ほとんどの管理機能を実行できます。このマニュアルには、HTML インターフェイスを使用したアプライアンスの初期設定の手順が含まれていますが、対応する HTML インターフェイスの詳細は、次のマニュアルを参照してください。

- 『*User Guide for Cisco Security MARS Local Controller Version 4.1.x*』
- 『*User Guide for Cisco Security MARS Global Controller Version 4.1.x*』

## レポーティング デバイスと脅威軽減デバイス

MARS システムを階層的に見ると、Global Controller が Local Controller をモニタし、Local Controller が 1 つまたは複数のレポーティング デバイスをモニタします。*レポーティング デバイス*は、ルータのトラフィック フローをはじめ、脆弱性査定システムから得られる潜在的な攻撃対象コンフィギュレーションまで、ネットワークに関するデータを MARS に提供します。

トラフィック フローを拒否できるレポーティング デバイスを、*脅威軽減デバイス*と呼びます（スイッチなど）。MARS は、2 つの形式で脅威軽減をサポートします。

- サポート対象のレイヤ 3 装置（OSI ネットワーク モデルに基づく）の場合、MARS は、検出された進行中の攻撃を停止できるように、推奨デバイスおよびコマンド セットを提供します。この情報を使用して、攻撃を手動でブロックできます。
- サポート対象のレイヤ 2 装置の場合、MARS は、検出された進行中の攻撃を停止するためのデバイスとコマンド セットを推奨し、管理者のためにコンフィギュレーションの変更方法を提供します。

レポーティング デバイスおよび脅威軽減デバイスの設定方法は、進行中の攻撃を検出する MARS の機能に大きく影響します。これらのデバイスの設定方法の詳細については、次のマニュアルを参照してください。

- 『*User Guide for Cisco Security MARS Local Controller Version 4.1.x*』
- 『*User Guide for Cisco Security MARS Global Controller Version 4.1.x*』

サポート対象のレポーティング デバイスおよび脅威軽減デバイスの完全なリストは、次の資料を参照してください。

- 『*Supported Devices for Cisco Security MARS Local Controller Version 4.x*』

# ハードウェアの概要

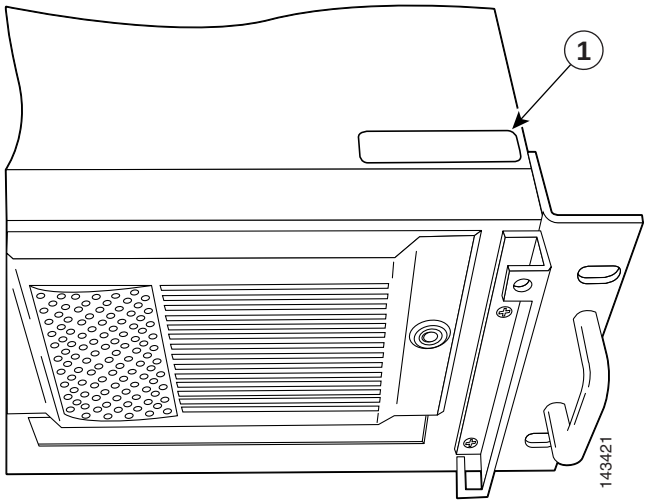
ここでは、各種の MARS アプライアンス モデルの前面パネルと背面パネル、および統合コンポーネントについて説明します。



## ライセンス キーの位置

MARS アプライアンス モデルはいずれも、シャーシ上の同じ場所にライセンス キー ステッカーが貼付されています。また、製品に付属の Recovery DVD のケースにも記載されています。図 1-2 に、ライセンス キー ステッカーの位置を示します。

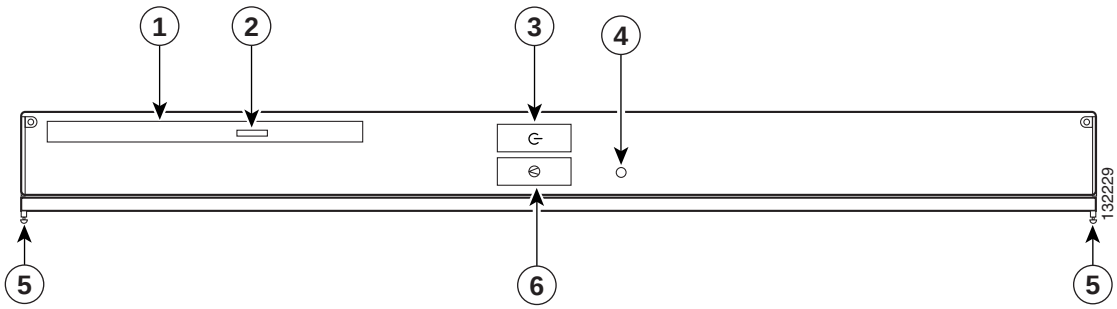
**図 1-2　ライセンス キーの位置**



# MARS 20

## 前面パネルの機能

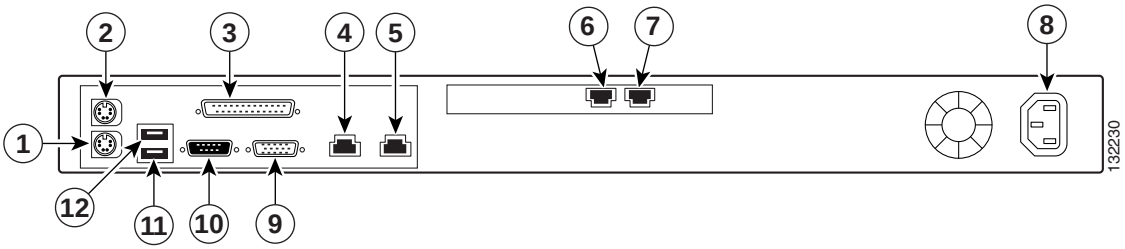
**図 1-3　MARS20 の前面パネル**




| エレメント | 説明 |
|---|---|
| 1 | DVD ドライブ |
| 2 | DVD イジェクト ボタン |
| 3 | 電源スイッチ |
| 4 | 電源インジケータ ライト |
| 5 | 前面パネル リリース ネジ |
| 6 | 再起動ボタン |

## 背面パネルの機能

**図 1-4　MARS20 の背面パネル**




| エレメント | 説明 |
|---|---|
| 1 | PS/2 キーボード ポート |
| 2 | PS/2 マウス ポート |
| 3 | パラレル ポート（非サポート） |
| 4 | eth0、Ethernet 0 ポート |
| 5 | eth1、Ethernet 1 ポート |
| 6 | RJ-11 ラインイン ポート |
| 7 | 電話ポート（ライン アウト） |
| 8 | パワー ソケット |

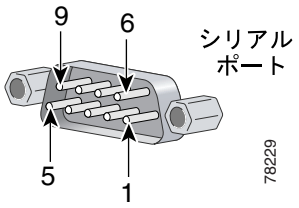
| エレメント | 説明 |
|---|---|
| 9 | シリアル ポート |
| 10 | VGA ポート |
| 11 | USB 0 ポート（非サポート） |
| 12 | USB 1 ポート（非サポート） |

## シリアル ポート

アプライアンスの背面パネル上の統合シリアル ポートは、9 ピン D サブミニチュア コネクタを使用します。

ハードウェアを再設定する場合には、シリアル ポート コネクタのピン番号および信号に関する情報が必要になることがあります。図 1-5 に、シリアル ポート コネクタのピン番号、ピン割り当て、およびインターフェイス信号を示します（ピン番号は、図に示すように、右下から左上の順序で対応しています)。

**図 1-5　シリアル ポート コネクタのピン番号**




| ピン | 信号 | I/O | 定義 |
|---|---|---|---|
| **1** | DCD | 入力 | データ キャリア検知 |
| **2** | SIN | 入力 | シリアル入力 |
| **3** | SOUT | 出力 | シリアル出力 |
| **4** | DTR | 出力 | データ端末動作可能 |
| **5** | GND | 適用外 | 信号アース |
| **6** | DSR | 入力 | データ セット レディ |
| **7** | RTS | 出力 | 送信要求 |
| **8** | CTS | 入力 | 送信可 |
| **9** | RI | 入力 | リング インジケータ |
| **シェル** | 適用外 | 適用外 | シャーシ アース |

## ラインイン ポート

MARS アプライアンスには、SMS およびページャ アラート用の V.90 モデムが組み込まれています。このモデムは、付属のケーブルとラインイン ポート（標準 RJ-11 ポート）を使用して壁面ジャックに接続します。

## 電話ポート

モデムを壁面の電話ジャックに接続した場合、MARS アプライアンスの電話ポートに電話線を接続できます。電話ポートは、標準 RJ-11 ポートです。

## VGA ポート

標準 VGA ポートを使用してアプライアンスにモニタを接続すると、コンソール ログを表示したり、コマンドラインを使用できます。ただし、これらの機能を使用するには、MARS アプライアンスにキーボードを接続する必要があります。

## パラレル ポート

使用しません。

## キーボード ポート

PS/2 キーボード接続用です。MARS アプライアンスに、キーボードを直接接続できます。このポートにキーボードを接続し、VGA ポートにモニタを接続すると、アプライアンスのコンソール ログおよびコマンドライン インターフェイスにアクセスできます。

## マウス ポート

使用しません。

## USB ポート（0 および 1）

使用しません。

## イーサネット コネクタ（eth0 および eth1）

システムには、2 つの 10/100/1000 Mbps 自動感知イーサネット コネクタが統合されています。MARS アプライアンスでは、両方のイーサネット コネクタを使用できます。各イーサネット コネクタは、ネットワーク拡張カードのすべての機能を提供し、10BASE-T、100BASE-TX、および 1000BASE-TX イーサネット標準をサポートしています。

各 NIC は、ネットワークの速度およびデュプレックス モードを検出するように設定します。

MARS アプライアンスは、eth0 に割り当てられた IP アドレス宛てのネットワーク トラフィックをモニタします。eth0 コネクタは、**gateway** コマンドが適用されるポートです。したがって、eth0 は、レポーティング デバイスがアクセスできるネットワークに接続する必要があります。eth1 コネクタは通常、管理者に高速 GUI（グラフィカル ユーザ インターフェイス）応答を提供する帯域外管理ネットワーク用に使用されます。eth1 を使用するには、インターフェイスの宛先ネットワークへのスタティック ルートを定義する必要があります。

## ネットワーク ケーブルの要件

**警告**　**感電を防ぐため、Safety Extra-Low Voltage（SELV; 安全特別低電圧）回路を、Telephone Network Voltage（TNV; 電話網電圧）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が含まれています。一部の LAN ポートおよび WAN ポートは、いずれも RJ-45 コネクタを使用します。ケーブルを接続するときは十分に注意してください。**

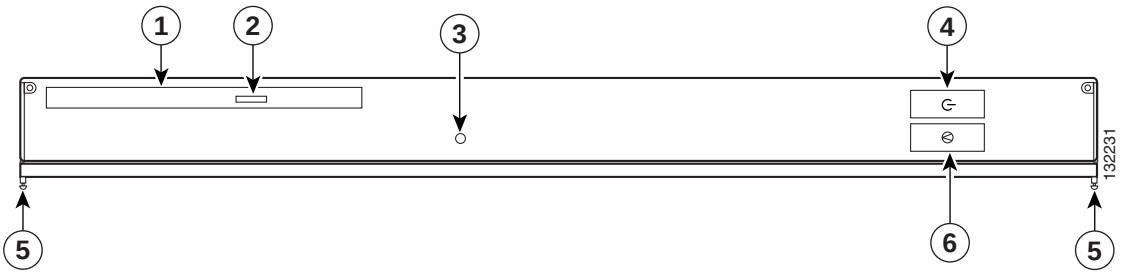
イーサネット コネクタは、標準 RJ-45 対応プラグの付いた Unshielded Twisted Pair（UTP; シールドなしツイスト ペア）イーサネット ケーブルを接続するように設計されています。UTP ケーブルの一端をイーサネット コネクタに接続し、プラグを確実に固定します。ケーブルの他端は、ネットワーク構成に応じて、ハブまたは他の装置の RJ-45 ポートに接続します。10BASE-T、100BASE-TX、1000BASE-TX ネットワークには、ケーブル接続に関して次の制約があります。

- 10BASE-T ネットワークの場合、カテゴリ 3 以上のケーブルおよびコネクタを使用します。
- 100BASE-TX および 1000BASE-TX ネットワークの場合、カテゴリ 5 以上のケーブルおよびコネクタを使用します。
- ケーブルの最大長は、328 フィート（100 m）です。

# MARS 50

## 前面パネルの機能

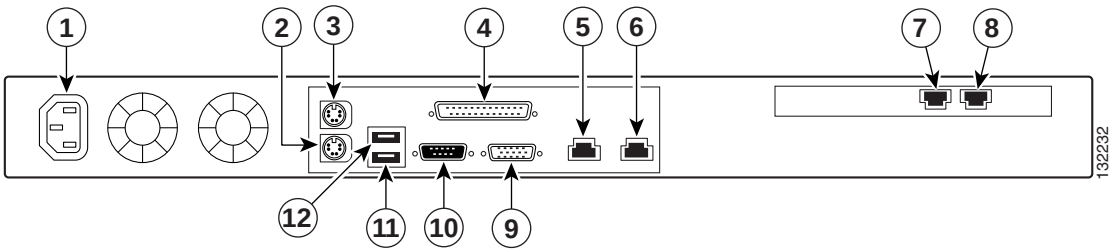
**図 1-6　MARS50 の前面パネル**




| エレメント | 説明 |
|---|---|
| 1 | DVD ドライブ |
| 2 | DVD イジェクト ボタン |
| 3 | 電源インジケータ ライト |
| 4 | 電源スイッチ |
| 5 | 前面パネル リリース ネジ |
| 6 | 再起動ボタン |

## 背面パネルの機能

**図 1-7　MARS50 の背面パネル**

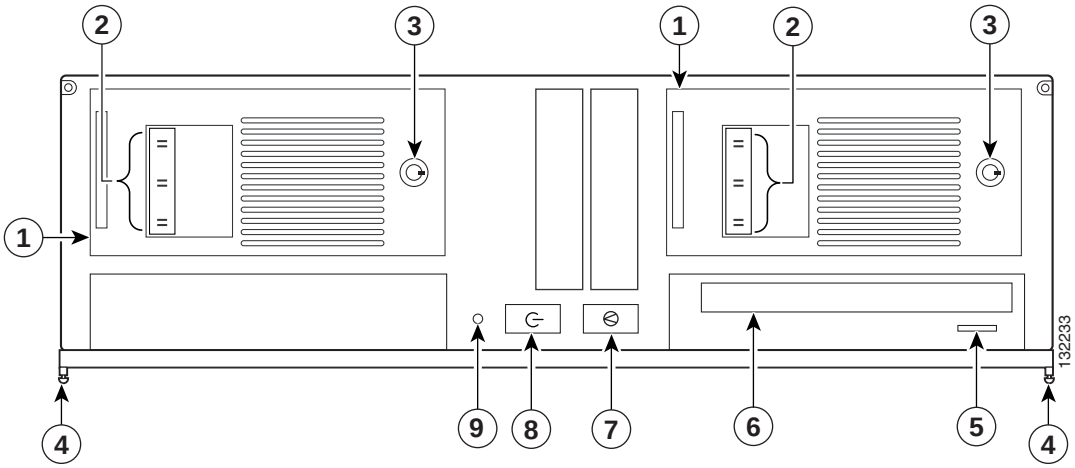



| エレメント | 説明 |
|---|---|
| 1 | パワー ソケット |
| 2 | PS/2 キーボード ポート |
| 3 | PS/2 マウス ポート |
| 4 | パラレル ポート（非サポート） |
| 5 | eth0、Ethernet 0 ポート |
| 6 | eth1、Ethernet 1 ポート |
| 7 | RJ-11 ラインイン ポート |
| 8 | 電話ポート（ライン アウト） |
| 9 | シリアル ポート |
| 10 | VGA ポート |
| 11 | USB 0 ポート（非サポート） |
| 12 | USB 1 ポート（非サポート） |

# MARS100 および MARS100e

## 前面パネルの機能

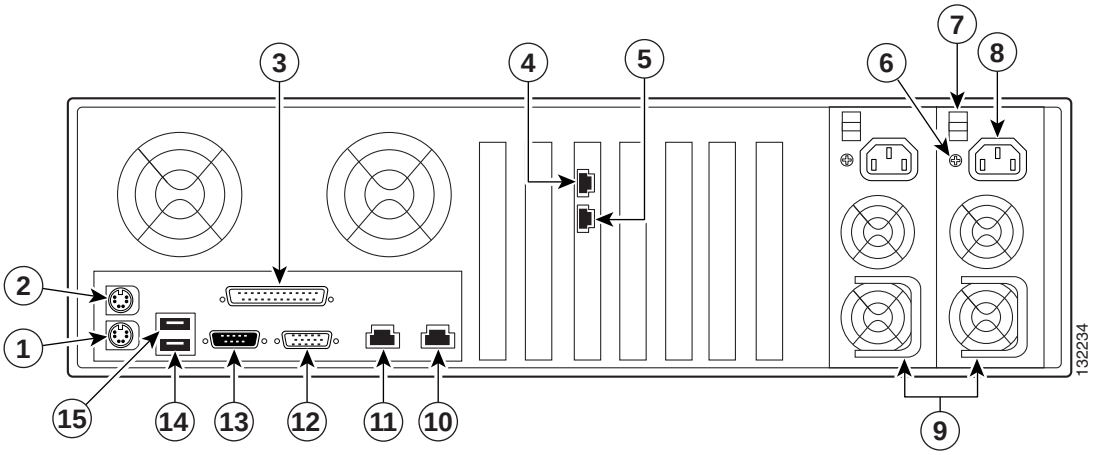
**図 1-8　MARS100 および MARS100e の前面パネル**




| エレメント | 説明 |
|---|---|
| 1 | ドライブ 1 ～ 3 |
| 2 | ドライブ ステータス ライト |
| 3 | ドライブ ベイ ドア ロック |
| 4 | 前面パネル リリース ネジ |
| 5 | DVD イジェクト ボタン |
| 6 | DVD ドライブ |
| 7 | 再起動ボタン |
| 8 | 電源スイッチ |
| 9 | 電源インジケータ ライト |

## 背面パネルの機能

**図 1-9　MARS100 および MARS100e の背面パネル**

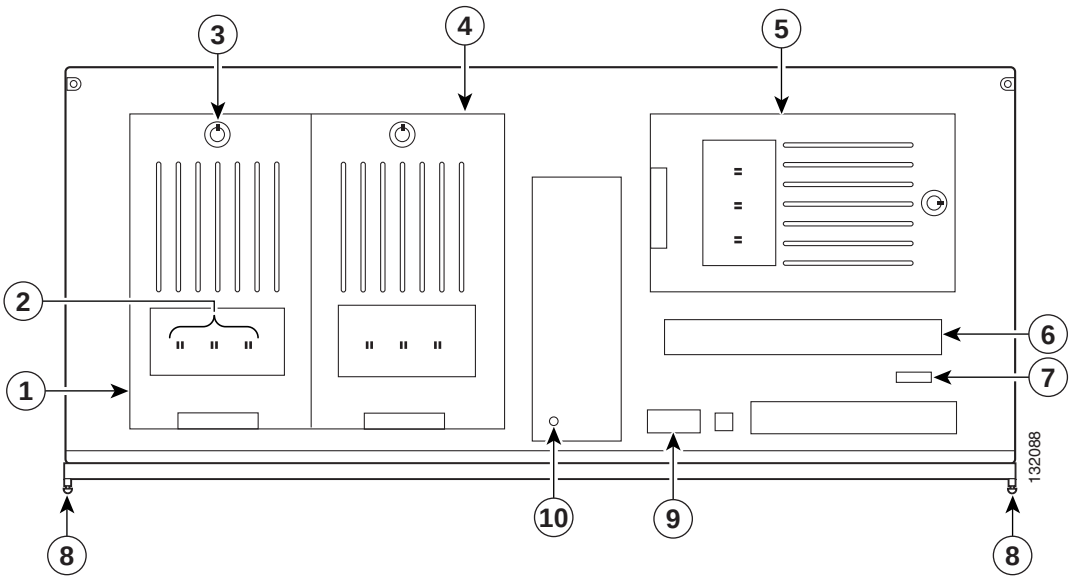



| エレメント | 説明 |
|---|---|
| 1 | PS/2 キーボード ポート |
| 2 | PS/2 マウス ポート |
| 3 | パラレル ポート（非サポート） |
| 4 | 電話ポート（ライン アウト） |
| 5 | RJ-11 ラインイン ポート |
| 6 | 電源装置リリース ネジ |
| 7 | 電源装置リリース レバー |
| 8 | パワー ソケット |
| 9 | 電源装置ハンドル |
| 10 | eth1、Ethernet 1 ポート |
| 11 | eth0、Ethernet 0 ポート |
| 12 | シリアル ポート |
| 13 | VGA ポート |
| 14 | USB 0 ポート（非サポート） |
| 15 | USB 1 ポート（非サポート） |

# MARS 200、MARS GCm および MARS GC

## 前面パネルの機能

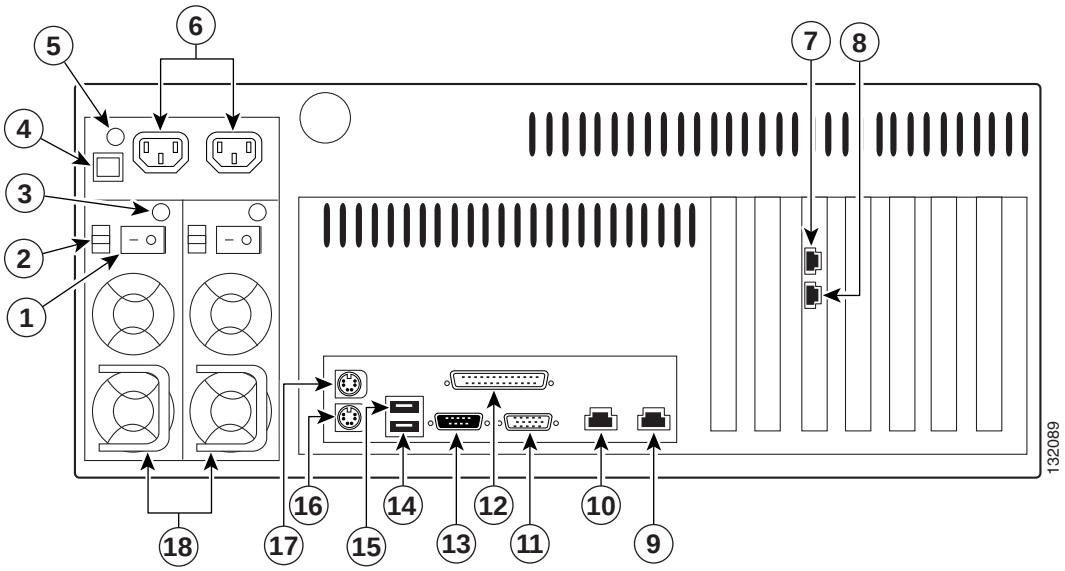
**図 1-10　MARS 200、MARS GCm または MARS GC の前面パネル**




| エレメント | 説明 |
|---|---|
| 1 | ドライブ 1 ～ 3 |
| 2 | ドライブ ステータス ライト |
| 3 | ドライブ ベイ ドア ロック |
| 4 | ドライブ 4 ～ 6 |
| 5 | ドライブ 7 ～ 9 |
| 6 | DVD ドライブ |
| 7 | DVD イジェクト ボタン |
| 8 | 前面パネル リリース ネジ |
| 9 | 電源スイッチ |
| 10 | 電源インジケータ ライト |

## 背面パネルの機能

**図 1-11　MARS 200、MARS GCm または MARS GC の背面パネル**




| エレメント | 説明 |
|---|---|
| 1 | 電源装置スイッチ |
| 2 | 電源装置リリース レバー |
| 3 | 電源装置ライト |
| 4 | 電源装置リセット ボタン |
| 5 | 電源インジケータ ライト |
| 6 | パワー ソケット |
| 7 | 電話ポート（ライン アウト） |
| 8 | RJ-11 ラインイン ポート |
| 9 | eth1、Ethernet 1 ポート |
| 10 | eth0、Ethernet 0 ポート |
| 11 | シリアル ポート |
| 12 | パラレル ポート（非サポート） |
| 13 | VGA ポート |
| 14 | USB 0 ポート（非サポート） |
| 15 | USB 1 ポート（非サポート） |
| 16 | PS/2 キーボード ポート |
| 17 | PS/2 マウス ポート |
| 18 | 電源装置ハンドル |