CHAPTER 5

# ファイアウォール モードの設定

この章では、ファイアウォール モードの設定方法、および各ファイアウォール モードでファイアウォールがどのように機能するかについて説明します。マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

FWSM（またはマルチモードでの各コンテキスト）は、2 種類のファイアウォール モードのいずれかで動作可能です。

- ルーテッド モード
- 透過モード

ルーテッド モードの場合、FWSM はネットワーク上のルータ ホップとみなされます。接続されたネットワーク間で NAT を実行できます。また、OSPF またはパッシブ RIP（シングルコンテキスト モード限定）を使用できます。ルーテッド モードは、異なるサブネット上にある複数のインターフェイスをサポートします。一定の制限のもとに、コンテキスト間でインターフェイスを共有できます。

透過モードの場合、FWSM は「ワイヤの凹凸」、すなわち「ステルス ファイアウォール」のように動作し、ルータ ホップにはなりません。FWSM は内部および外部インターフェイス上の同一ネットワークに接続します。マルチコンテキスト モードを使用しない場合、またはコンテキストを最大限に使用する場合は、ブリッジ グループと呼ばれるインターフェイスの複数のペアを作成できます。各ブリッジ グループは別々のネットワークに接続します。ダイナミック ルーティング プロトコルや NAT は使用しません。ただし、ルーテッド モードと同様、透過モードでも、自動的に通過を許可される Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを除くすべてのトラフィックが FWSM を通過できるようにするためのアクセス リストが必要です。透過モードでは、ルーテッド モードでブロックされる特定のタイプのトラフィックをアクセス リストで許可できます。サポート対象外のルーティング プロトコルなどが該当します。透過モードの場合、任意で EtherType アクセス リストを使用して、IP 以外のトラフィックを通過させることができます。

（注） ブリッジ グループはそれぞれ管理 IP アドレスが必要です。FWSM はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。管理用 IP アドレスは、接続先ネットワークと同じサブネット上になければなりません。

この章で説明する内容は、次のとおりです。

# ルーテッド モードの概要



## IP ルーティング サポート

FWSM は、接続されたネットワーク間でルータとして動作します。各インターフェイスには、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードの場合、ルーテッド ファイアウォールは OSPF および RIP（パッシブ モード）をサポートします。マルチコンテキスト モードがサポートするのは、スタティック ルートだけです。広範なルーティング ニーズに対応するには、FWSM に依存するのではなく、アップストリームおよびダウンストリーム ルータの高度なルーティング機能を使用することを推奨します。

## NAT

Network Address Translation（NAT; ネットワーク アドレス変換）は、パケットの実アドレスを宛先ネットワーク上でルーティング可能なマップ アドレスに置き換えます。デフォルトでは NAT は必要ありません。セキュリティの高いインターフェイス上のホストがセキュリティの低いインターフェイス（外部）と通信するときに NAT の使用を要求する NAT ポリシーを適用する場合、NAT 制御をイネーブルにできます（**nat-control** コマンドを参照）。

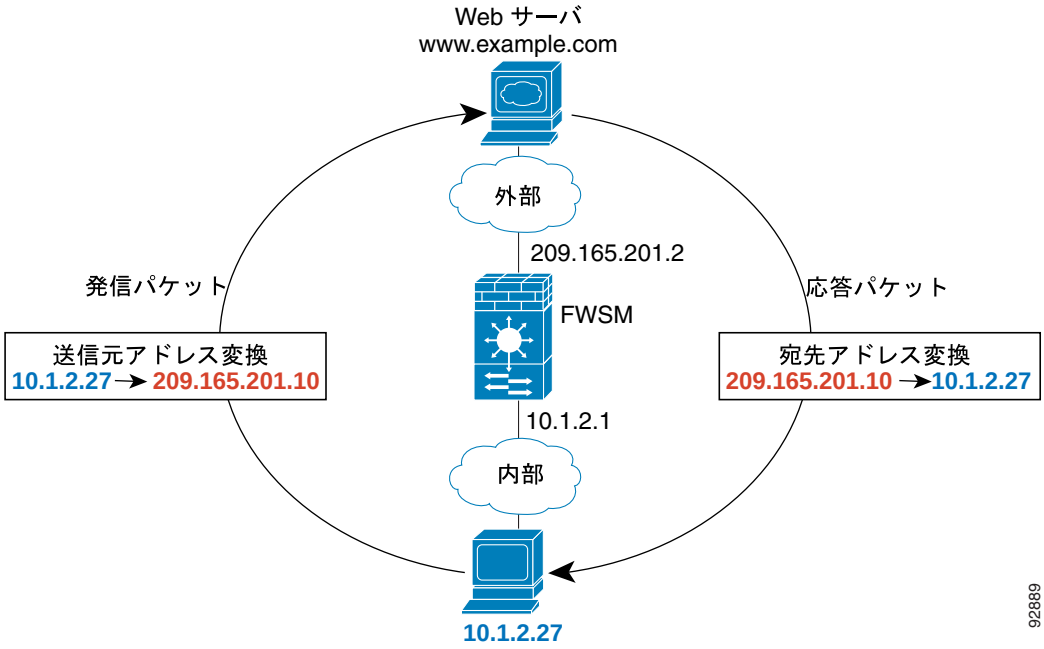
（注）　Version 3.1 以前のソフトウェア リリースでは、NAT 制御はデフォルト動作となっていました。FWSM を旧バージョンからアップグレードした場合は、コンフィギュレーションに **nat-control** コマンドが自動的に追加され、予期された動作が保持されます。

NAT の利点の一部は、次のとおりです。

- 内部ネットワーク上でプライベート アドレスを使用できます。プライベート アドレスはインターネット上でルーティングできません。
- NAT は他のネットワークに対してローカル アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- NAT は IP アドレスのオーバーラップをサポートすることによって、IP ルーティングに伴う問題を解決します。

図 5-1 に、内部にプライベート ネットワークのある、NAT の一般的な使用例を示します。内部ユーザがインターネット上の Web サーバにパケットを送信すると、そのパケットのローカルな送信元アドレスがルーティング可能なグローバル アドレスに変更されます。応答時、Web サーバはグローバル アドレスに応答を送り、FWSM がパケットを受信します。FWSM はさらに、グローバル アドレスをローカル アドレスに変換してからユーザに送ります。

図 5-1　NAT の例




## ルーテッド ファイアウォール モードで FWSM を通過するデータ

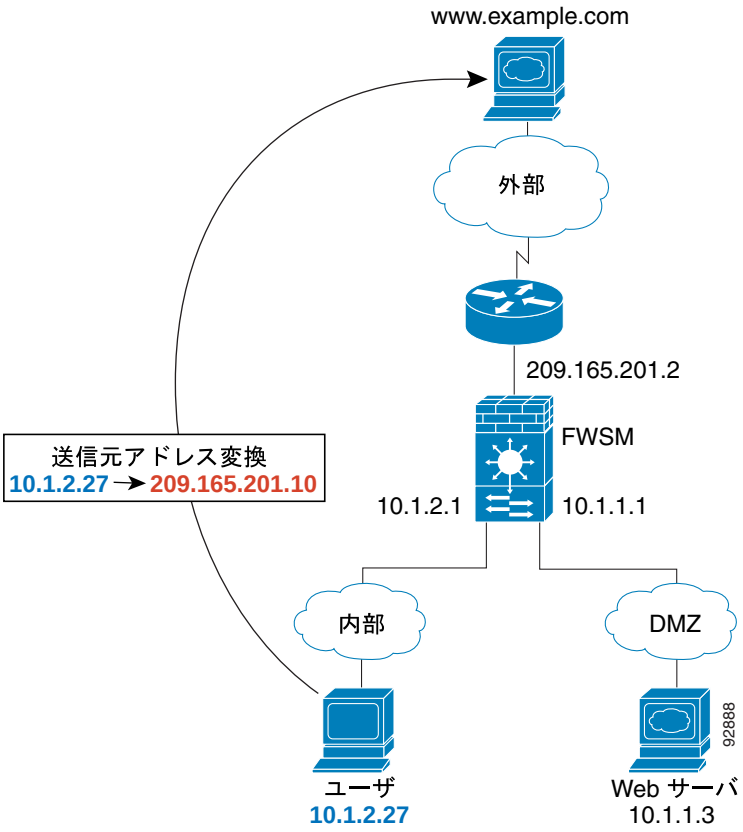
ここでは、ルーテッド ファイアウォール モードにおいて、データが FWSM をどのように通過するかについて説明します。内容は次のとおりです。

- 内部ユーザによる Web サーバ アクセス（p.5-4）
- 外部ユーザによる DMZ 上の Web サーバ アクセス（p.5-5）
- 内部ユーザによる DMZ 上の Web サーバ アクセス（p.5-6）
- 外部ユーザによる内部ホストへのアクセス試行（p.5-6）
- DMZ ユーザによる内部ホストへのアクセス試行（p.5-8）

## 内部ユーザによる Web サーバ アクセス

図 5-2 に、内部ユーザが外部の Web サーバにアクセスする例を示します。

**図 5-2　内部から外部**




データが FWSM を通過する順序は、次のとおりです（図 5-2 を参照）。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

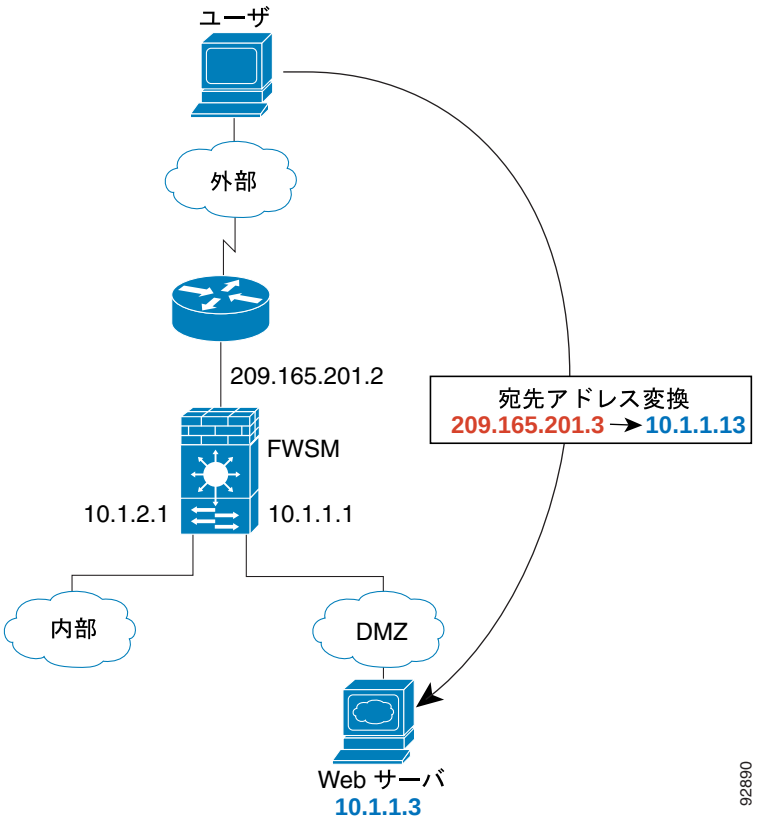
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、インターフェイスは固有です。www.example.com の IP アドレスはコンテキストでアドレス変換が行われません。
3. FWSM は、ローカル送信元アドレス（10.1.2.27）をグローバル アドレス 209.165.201.10 に変換します。このグローバル アドレスは外部インターフェイスのサブネット上にあります。

   グローバル アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. FWSM はさらに、セッションが確立されたことを記録して、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットは FWSM を通過します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。FWSM は NAT を実行し、グローバル宛先アドレスをローカル ユーザ アドレス 10.1.2.27 に変換します。
6. FWSM が内部ユーザにパケットを転送します。

## 外部ユーザによる DMZ 上の Web サーバ アクセス

図 5-3 に、外部ユーザが DMZ 上の Web サーバにアクセスする例を示します。

**図 5-3　外部から DMZ**




データが FWSM を通過する順序は、次のとおりです（図 5-3 を参照）。

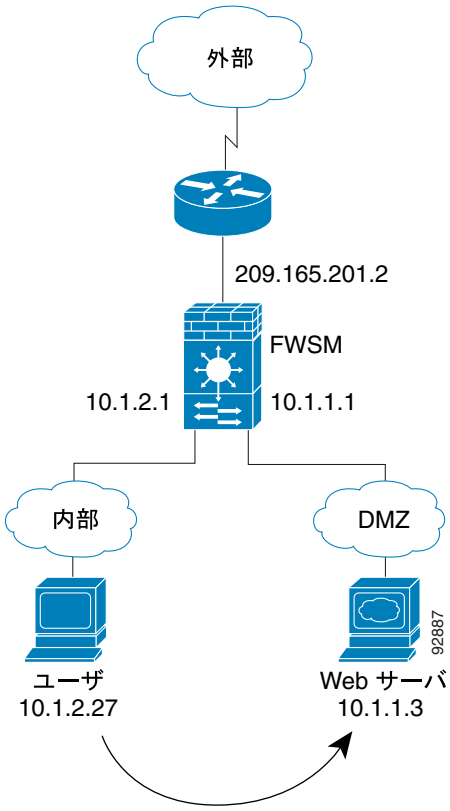
1. 外部ネットワーク上のユーザがグローバル宛先アドレス 209.165.201.3 を使用して、DMZ 上の Web サーバに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、分類機能はサーバ アドレス変換によって、DMZ 上の Web サーバのアドレスが特定のコンテキストに属することを「認識」します。
3. FWSM は宛先アドレスをローカル アドレス 10.1.1.3 に変換します。
4. FWSM はさらに、高速パスにセッション エントリを追加し、DMZ インターフェイスからパケットを転送します。
5. DMZ 上の Web サーバが要求に応答すると、パケットは FWSM を通過します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。FWSM は NAT を実行し、ローカル送信元アドレスを 209.165.201.3 に変換します。
6. FWSM が外部ユーザにパケットを転送します。

## 内部ユーザによる DMZ 上の Web サーバ アクセス

図 5-4 に、内部ユーザが DMZ 上の Web サーバにアクセスする例を示します。

**図 5-4　内部から DMZ**




データが FWSM を通過する順序は、次のとおりです（図 5-4 を参照）。

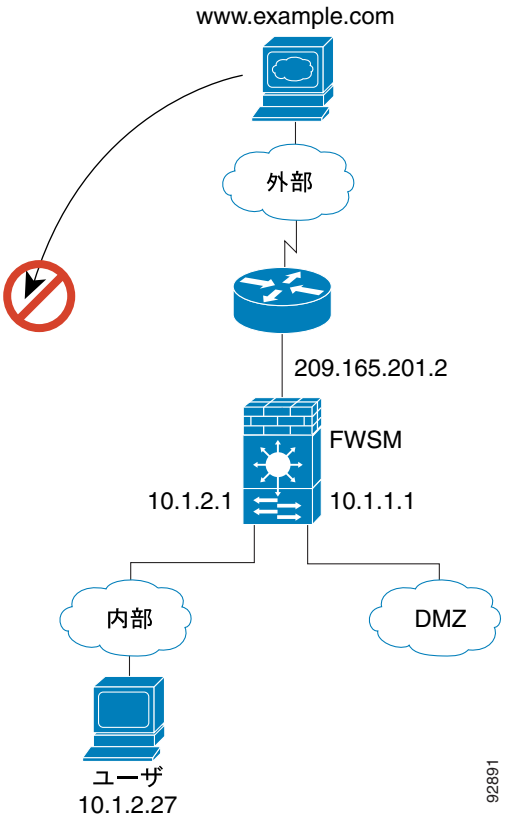
1. 内部ネットワーク上のユーザが宛先アドレス 10.1.1.3 を使用して、DMZ の Web サーバに Web ページを要求します。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、インターフェイスは固有です。Web サーバの IP アドレスはアドレス変換が行われません。
3. FWSM はさらに、セッションが確立されたことを記録して、DMZ のインターフェイスからパケットを転送します。
4. DMZ の Web サーバが要求に応答すると、パケットは高速パスを通過します。したがって、パケットは新しい接続に伴うさまざまな検査をバイパスできます。
5. FWSM が内部ユーザにパケットを転送します。

## 外部ユーザによる内部ホストへのアクセス試行

図 5-5 に、外部ユーザから内部ネットワークにアクセスを試みる例を示します。

**図 5-5　外部から内部**




データが FWSM を通過する順序は、次のとおりです（図 5-5 を参照）。

1. 外部ネットワーク上のユーザが内部ホストにアクセスしようとしています（ホストにルーティング可能な IP アドレスが与えられているものとします）。

   内部ネットワークでプライベート アドレスを使用している場合、NAT を実行しないかぎり、外部ユーザが内部ネットワークにアクセスすることはできません。外部ユーザは既存の NAT セッションを使用することによって、内部ユーザへのアクセスを試みる可能性があります。

2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に基づいて、そのパケットが許可されるかどうかを検証します。

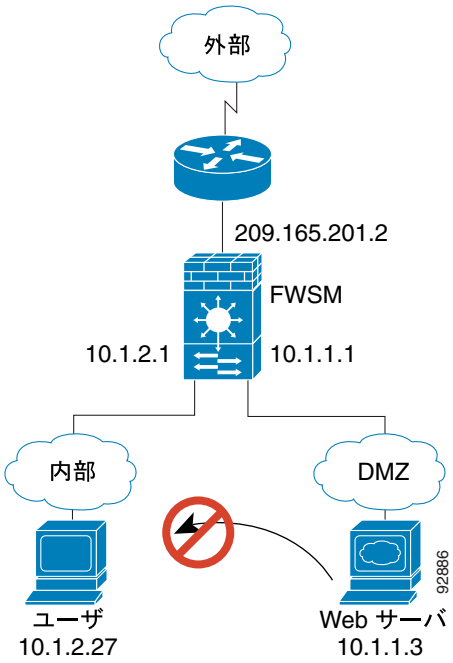
3. パケットが拒否され、FWSM がパケットを廃棄して、接続試行を記録します。

   外部ユーザが内部ネットワークの攻撃を試みている場合、FWSM はさまざまなテクノロジーを駆使し、確立済みのセッションに対してパケットが有効かどうかを判別します。

## DMZ ユーザによる内部ホストへのアクセス試行

図 5-6 に、DMZ 上のユーザから内部ネットワークにアクセスを試みる例を示します。

**図 5-6　DMZ から内部**




データが FWSM を通過する順序は、次のとおりです（図 5-6 を参照）。

1. DMZ　ネットワーク上のユーザが内部ホストにアクセスしようとしています。DMZ　ではインターネット上のトラフィックをルーティングする必要がないため、プライベート アドレッシング スキームはルーティングを阻止しません。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に基づいて、そのパケットが許可されるかどうかを検証します。
3. パケットが拒否され、FWSM がパケットを廃棄して、接続試行を記録します。

# 透過モードの概要

ここでは、透過ファイアウォール モードについて説明します。内容は次のとおりです。



## 透過ファイアウォールの機能

従来のファイアウォールはルーティングされるホップであり、ファイアウォールが保護しているサブネットの 1 つに接続するホストに対して、デフォルト ゲートウェイとして動作します。一方、透過ファイアウォールは、「ワイヤの凹凸」すなわち「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続先装置へのルータ ホップとはみなされません。FWSM は内部および外部インターフェイス上の同一ネットワークに接続します。

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、ブリッジ グループと呼ばれる最大 8 つのペアのインターフェイスを設定できます。各ブリッジ グループは別々のネットワークに接続します。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。ブリッジング機能はブリッジ グループごとに別々ですが、他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループのセキュリティ コンテキストを使用します。

透過ファイアウォールはルーティング対象のホップではないので、既存のネットワークに容易に導入できます。IP 再アドレッシングは不要です。複雑なルーティング パターンのトラブルシューティングや NAT 設定が不要なので、メンテナンスが容易です。

透過モードはブリッジとして動作しますが、IP トラフィックなどのレイヤ 3 トラフィックは、拡張アクセス リストで明示的に許可されていないかぎり、FWSM を通過できません。アクセス リストなしに透過ファイアウォールを通過できるトラフィックは、ARP トラフィックだけです。ARP トラフィックは、ARP インスペクションで制御できます。

ルーテッド モードでは、アクセス リストで許可されていても、一部のトラフィック タイプは FWSM を通過できません。ただし、透過ファイアウォールの場合は、拡張アクセス リスト（IP トラフィックの場合）または EtherType アクセス リスト（IP 以外のトラフィックの場合）のどちらかを使用することによって、あらゆるトラフィックを通過させることができます。

**（注）** 透過モードの場合、CDP パケット、または 0x600 以上の有効な EtherType を持たないパケットはすべて FWSM を通過できません。たとえば、IS-IS パケットは通過できません。BPDU に対しては例外が設定されています。

たとえば、透過ファイアウォールをまたいでルーティング プロトコルの隣接関係を確立できます。拡張アクセス リストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを通過させることができます。同様に、HSRP または VRRP などのプロトコルも FWSM を通過できます。特定のトラフィックを許可する処理については、表 10-2（p.10-8）を参照してください。

EtherType アクセス リストを使用することによって、IP 以外のトラフィック（AppleTalk、IPX、BPDU、MPLS など）を通過させるように設定できます。

透過ファイアウォールで直接サポートされていない機能については、アップストリーム ルータおよびダウンストリーム ルータが機能をサポートできるように、トラフィックの通過を許可できます。たとえば、拡張アクセス リストを使用して、DHCP トラフィック（サポート対象外の DHCP リレー機能の代わりに）または IP/TV によって作成されたマルチキャスト トラフィックの通過を許可できます。

FWSM が透過モードで稼働している場合、パケットの発信インターフェイスはルート検索ではなく、MAC アドレス検索を実行することによって判別されます。ルート ステートメントも設定できますが、適用されるのは FWSM を起点とするトラフィックだけです。たとえば、Syslog サーバがリモート ネットワークに配置されている場合、FWSM がそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

## ネットワークでの透過ファイアウォールの使用例

図 5-7 に、外部デバイスが内部デバイスと同一サブネット上にある、標準的な透過ファイアウォール ネットワークを示します。内部ルータと内部ホストは、見かけ上、外部ルータに直接接続されています。

**図 5-7　透過ファイアウォール ネットワーク**

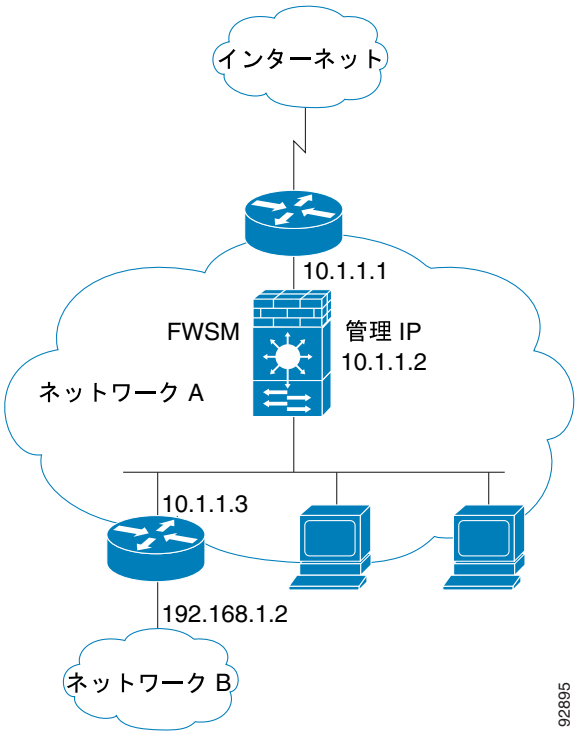
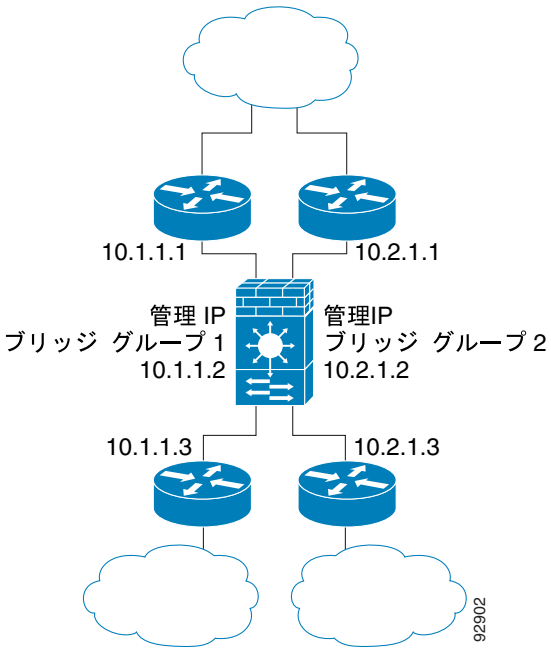


図 5-8 に、2 つのブリッジ グループを持つ、FWSM に接続されている 2 つのネットワークを示します。

**図 5-8　2 つのブリッジ グループを持つ透過ファイアウォール ネットワーク**




## 透過ファイアウォールの注意事項

透過ファイアウォール ネットワークを計画するときの注意事項は、次のとおりです。

- 各ブリッジ グループに管理 IP アドレスが必要です。

  各インターフェイスに IP アドレスが必要なルーテッド モードとは異なり、透過ファイアウォールではブリッジ グループ全体に 1 つの IP アドレスが割り当てられています。FWSM はシステム メッセージ、AAA 通信など、FWSM が発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。

  管理用 IP アドレスは、接続先ネットワークと同じサブネット上になければなりません。管理 IP サブネットの詳細については、「IP アドレスのブリッジ グループへの割り当て」（p.6-7）を参照してください。
- 各ブリッジ グループは、内部インターフェイスと外部インターフェイスだけを使用します。
- 直接接続された各ネットワークは、同一サブネット上になければなりません。
- ブリッジ グループの管理用 IP アドレスを接続されたデバイスのデフォルト ゲートウェイとして指定しないでください。デバイスには、FWSM の反対側にあるルータをデフォルト ゲートウェイとして指定する必要があります。
- 管理トラフィックの戻りパスを指定するために必要な、透過ファイアウォールのデフォルト ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにのみ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別するスタティック ルートを指定する必要があります。

- マルチコンテキスト モードの場合、コンテキストごとに異なるインターフェイスを使用する必要があります。複数のコンテキスト間で同じインターフェイスを共有することはできません。
- マルチコンテキスト モードの場合、各コンテキストは一般に異なるサブネットを使用します。オーバーラップするサブネットを使用することはできますが、ルーティングの見地から重複サブネットを可能にするようにルータと NAT を設定したネットワーク トポロジーが必要です。
- 拡張アクセス リストを使用して、IP トラフィックなどのレイヤ 3 トラフィックが FWSM を通過できるようにしなければなりません。

  任意で EtherType アクセス リストを使用することによって、IP 以外のトラフィックを通過させることもできます。

## 透過モードでサポートされていない機能

透過モードでは、次の機能はサポートされていません。

- NAT

  NAT はアップストリーム ルータで実行します。
- ダイナミック ルーティング プロトコル

  ただし、FWSM を発信元とするトラフィックのスタティック ルートを追加できます。拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルが FWSM を通過できるようにすることもできます。
- ブリッジ グループ IP アドレスの IPv6。ただし、EtherType アクセス リストを使用して IPv6 EtherType を通過させることはできます。
- DHCP リレー

  透過ファイアウォールは DHCP サーバとして機能することはできますが、DHCP リレー コマンドはサポートしません。拡張アクセス リストを使用して DHCP トラフィックを通過させることができるため、DHCP リレーは必要ありません。
- マルチキャスト

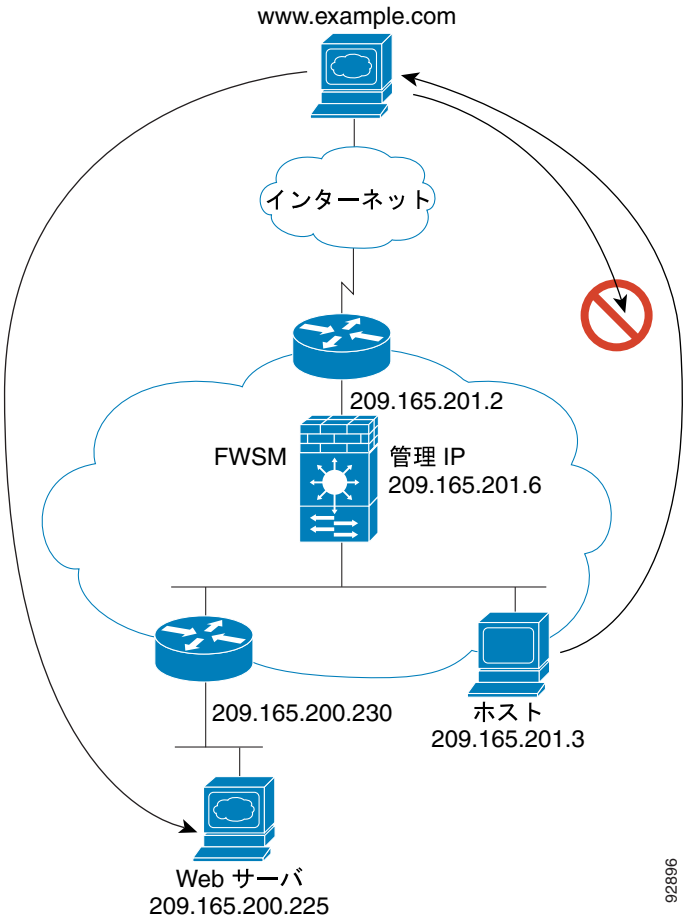
  ただし、拡張アクセス リストで許可することで、マルチキャスト トラフィックが FWSM を通過できるようにすることはできます。
- 管理用リモート アクセス VPN

  管理のためにサイト間 VPN を使用できます。

## 透過ファイアウォールを通過するデータ

図 5-9 に、内部ネットワークにパブリック Web サーバが配置されている状況で、透過ファイアウォールを使用する一般的な宅装例を示します。FWSM には、内部ユーザがインターネット リソースにアクセスできるようにするアクセス リストが 1 つ設定されています。さらに、もう 1 つのアクセス リストで、外部ユーザが内部ネットワーク上の Web サーバに限ってアクセスできるようにしています。

**図 5-9　一般的な透過ファイアウォールのデータ パス**



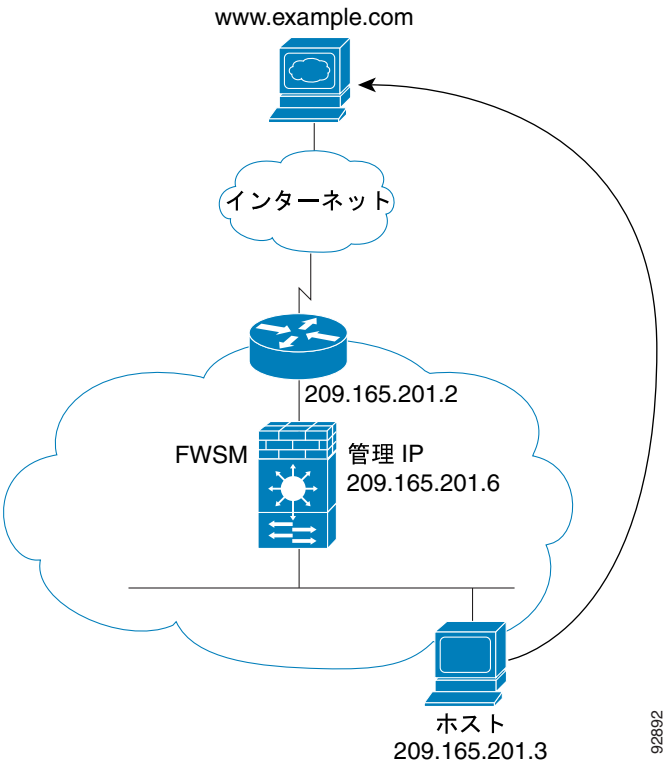

ここでは、データが FWSM をどのように通過するかについて説明します。内容は次のとおりです。

- 内部ユーザによる Web サーバ アクセス（p.5-14）
- 外部ユーザによる内部ネットワーク上の Web サーバ アクセス（p.5-15）
- 外部ユーザによる内部ホストへのアクセス試行（p.5-16）

## 内部ユーザによる Web サーバ アクセス

図 5-10 に、内部ユーザが外部の Web サーバにアクセスする例を示します。

**図 5-10　内部から外部**




データが FWSM を通過する順序は、次のとおりです（図 5-10 を参照）。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

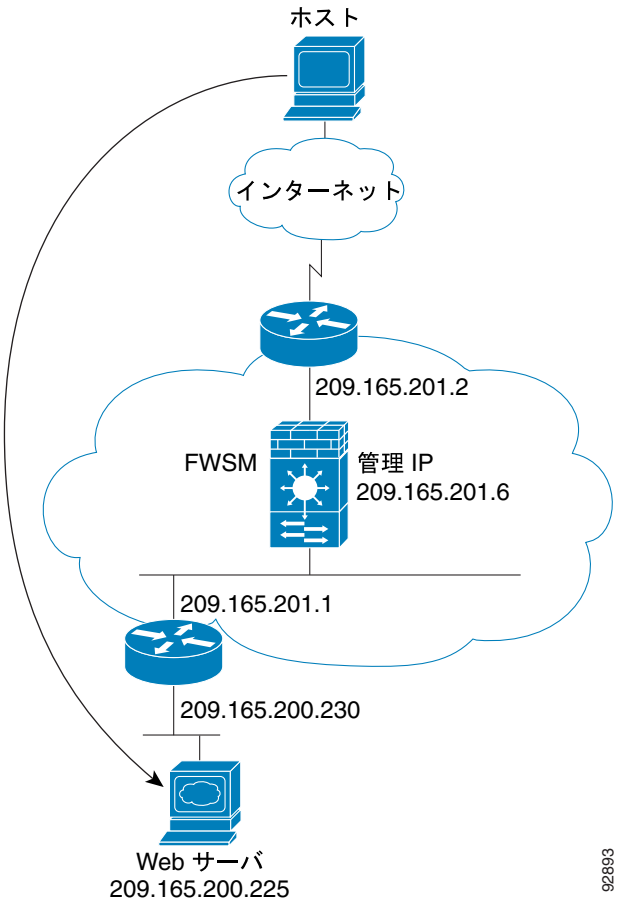
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. FWSM がセッションの確立を記録します。
4. 宛先 MAC アドレスが MAC アドレス テーブルに含まれている場合、FWSM は外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.186.201.2 です。

   宛先 MAC アドレスが FWSM のテーブルに含まれていない場合、FWSM は ARP 要求を送信し、ping を実行することによって、MAC アドレスを突き止めようとします。最初のパケットは廃棄されます。
5. Web サーバが要求に応答すると、FWSM は必要に応じて Web サーバ MAC アドレスを MAC アドレス テーブルに追加します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。
6. FWSM が内部ユーザにパケットを転送します。

## 外部ユーザによる内部ネットワーク上の Web サーバ アクセス

図 5-11 に、外部ユーザが内部の Web サーバにアクセスする例を示します。

**図 5-11　外部から内部**




データが FWSM を通過する順序は、次のとおりです（図 5-11 を参照）。

1. 外部ネットワーク上のユーザが内部の Web サーバに Web ページを要求します。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

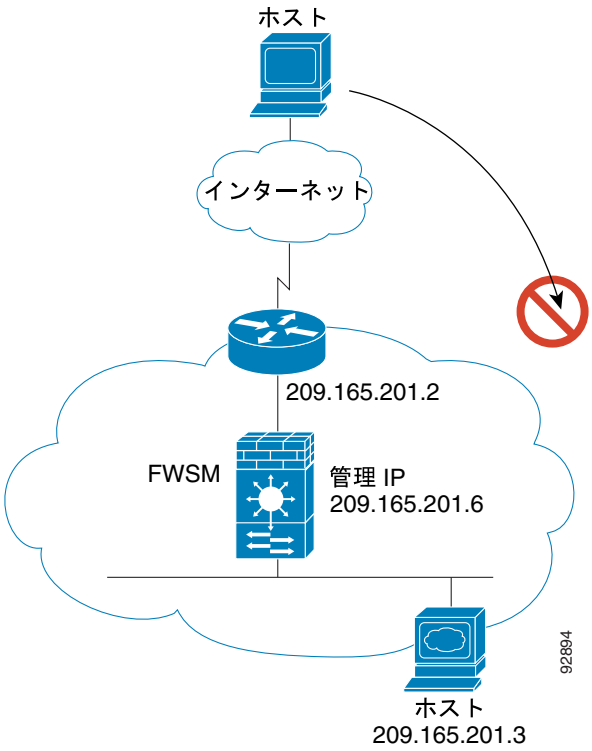
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. FWSM がセッションの確立を記録します。
4. 宛先 MAC アドレスが MAC アドレス テーブルに含まれている場合、FWSM は内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータのアドレス 209.186.201.1 です。

   宛先 MAC アドレスが FWSM のテーブルに含まれていない場合、FWSM は ARP 要求を送信し、ping を実行することによって、MAC アドレスを突き止めようとします。最初のパケットは廃棄されます。
5. Web サーバが要求に応答すると、FWSM は必要に応じて Web サーバ MAC アドレスを MAC アドレス テーブルに追加します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。
6. FWSM が外部ユーザにパケットを転送します。

## 外部ユーザによる内部ホストへのアクセス試行

図 5-12 に、外部ユーザから内部ネットワーク上のホストにアクセスを試みる例を示します。

**図 5-12　外部から内部**




データが FWSM を通過する順序は、次のとおりです（図 5-12 を参照）。

1. 外部ネットワーク上のユーザが内部ホストにアクセスしようとしています。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. パケットが拒否され、FWSM がパケットを廃棄します。
4. 外部ユーザが内部ネットワークの攻撃を試みている場合、FWSM はさまざまなテクノロジーを駆使し、確立済みのセッションに対してパケットが有効かどうかを判別します。

# 透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定

ルーテッド ファイアウォール モード（デフォルト）または透過ファイアウォール モードで動作するように、各コンテキストを設定できます。

モードを変更すると、FWSM によってコンフィギュレーションが消去されます。両方のモードでサポートされるコマンドは少ないからです。入力済みのコンフィギュレーションがすでにある場合は、必ず、モードを変更する前にコンフィギュレーションのバックアップを行ってください。新しいコンフィギュレーションを作成するときに、このバックアップを参照できます。

**firewall transparent** コマンドでモードを変更するテキスト コンフィギュレーションを FWSM にダウンロードする場合は、必ず、コンフィギュレーションの先頭にこのコマンドを指定してください。FWSM はコマンドを読み取るとただちにモードを変更し、そのあとでダウンロードされたコンフィギュレーションの残りを読み取ります。コンフィギュレーションの後ろの方にこのコマンドが指定されていると、FWSM はコンフィギュレーションのそこまでの行をすべて消去します。

- モードを透過的に設定するには、各コンテキストに次のコマンドを入力します。

  ```
  hostname(config)# firewall transparent
  ```

- モードをルーテッドに設定するには、各コンテキストに次のコマンドを入力します。

  ```
  hostname(config)# no firewall transparent
  ```