共通基準 EAL4 評価済み Cisco 適応型セキュリティ アプライアンス Version 7.0(6) のインストレーションおよびコンフィギュレーション

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

March 2007

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

OL-12987-01-J

目次

このマニュアルは、共通基準 Evaluation Assurance Level 4（EAL4; 評価保証レベル 4）によって認定された Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) をインストールして設定する方法について説明します。

このマニュアルでは、「セキュリティ アプライアンス」および「適応型セキュリティ アプライアンス」という語は、特に明記していない限り Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) のすべてのモデルに適用されます。

（注） このマニュアルに記載されている情報に従わないと、適応型セキュリティ　アプライアンスが評価に準拠しなくなります。また、セキュアでなくなる可能性があります。

このマニュアルには、次の項があります。

概要

このマニュアルは、Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) のマニュアルに対する追補です。セキュリティ アプライアンスを設定する間に、このマニュアルをお読みください。

シスコの製品マニュアルには、次のものがあります。

- リリース ノート
  - *Cisco PIX Security Appliance Release Notes*
  - *Cisco ASA 5500 Series Release Notes*
- クイック スタート ガイド
  - *Cisco PIX 515E Security Appliance Quick Start Guide*
  - *Cisco ASA 5500 Quick Start Guide*
- ハードウェア インストレーション ガイド
  - *Cisco PIX Security Appliance Hardware Installation Guide*
  - *Cisco ASA 5500 Hardware Installation Guide*
- 適合認定および安全性に関する情報ガイド
  - *Cisco PIX Security Appliance Regulatory Compliance and Safety Information*
  - *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- コマンドライン コンフィギュレーション ガイド
  - *Cisco Security Appliance Command Line Configuration Guide*
- コマンド リファレンス ガイド
  - *Cisco Security Appliance Command Reference*
- システム ログ メッセージ ガイド
  - *Cisco Security Appliance System Log Messages*

セキュリティ アプライアンスのマニュアルは、CD-ROM でも、印刷物としても、オンライン（HTML 形式と PDF 形式の両方）でも入手できます。このマニュアルは、2005 年 8 月版の CD-ROM ベースのマニュアルと併せてお読みください。

対象読者

このマニュアルは、Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) ソフトウェアを設定する管理者を対象としています。また、読者がネットワークとその用語に精通していること、信頼されている人物であること、インターネットとその関連用語およびアプリケーションを使用するための訓練を受けていることを前提としています。

サポートされているハードウェアおよびソフトウェアのバージョン

表 1 および表 2 に示しているハードウェアの組み合せだけが、セキュリティ アプライアンス 7.0(6) の EAL4 評価に準拠しています。指定されていないハードウェアを使用すると、セキュアなコンフィギュレーションが無効になります。同様に、Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) 以外のソフトウェア バージョンを使用すると、セキュアなコンフィギュレーションが無効になります。

表 1　　認定済み PIX Firewall でサポートされているハードウェア

モデル	オプションのハードウェア モジュール	インターフェイスの最大数
PIX 515[1] /515E[1]	PIX-1FE PIX-4FE	6
PIX 525[1]	PIX-1FE PIX-4FE PIX-1GE-66	8
PIX 535[1]	PIX-1FE PIX-4FE PIX-1GE-66	10

1. これらのモデルは、AC 電源または DC 電源を装備できます。

表 2　　認定済み Cisco ASA 5500 シリーズ セキュリティ アプライアンスでサポートされているハードウェア

モデル	オプションのハードウェア モジュール	インターフェイスの最大数
ASA 5510	4GE SSM	9
ASA 5520	4GE SSM	9
ASA 5540	4GE SSM	9

この評価に含まれている PIX Firewall Syslog Service（PFSS）のバージョンは 5.1(3) です。

セキュリティに関する情報

次の各項では、『*Regulatory Compliance and Safety Information*』の補足として、共通基準で認定された適応型セキュリティ アプライアンス用の追加のセキュリティ情報を提供します。

組織のセキュリティ ポリシー

セキュリティ アプライアンスが、組織のセキュリティ ポリシーに従って配送、インストール、管理、および稼働されていることを確認してください。セキュリティ ポリシーの定義方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

セキュリティの実装に関する注意事項

次の各項では、セキュリティ アプライアンスを安全に管理するために必要な、実装に関する注意事項について説明します。

認定されたコンフィギュレーション

セキュリティ アプライアンス ソフトウェア Version 7.0(6) だけを使用します。評価済みコンフィギュレーションの実装には、表 1 および表 2 に示しているハードウェア バージョンの組み合せだけを使用できます。ソフトウェアを別のバージョンに変更すると、特定のハードウェア プラットフォームの評価済みステータスが無効になります。

共通基準で認定された適応型セキュリティ アプライアンス 7.0(6) は、次の機能をサポートしていません。

- カットスルー プロキシ
- Routing Information Protocol（RIP; ルーティング情報プロトコル）
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
- Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）サーバ
- Virtual Private Network（VPN; バーチャル プライベート ネットワーク）

セキュリティ アプライアンスのその他すべてのハードウェア機能およびソフトウェア機能は、このマニュアルに従って設定、稼働、および管理する限り、評価済みの製品コンフィギュレーションに含まれます。

Cisco PIX セキュリティ アプライアンス Version 7.0(6) および Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.0(6) の評価対象は、監査サーバとしての機能を Windows 2000 コンピュータまたは Windows XP コンピュータに依存します。Windows 2000 または Windows XP は、EAL 4 評価済みコンフィギュレーションで設定され、この評価をサポートします。Microsoft Windows 2000 または Windows XP の評価済みコンフィギュレーションに関するマニュアルは、次のリンクから参照できます。

Windows 2000 のマニュアル

- Windows 2000 Common Criteria Evaluated Configuration User's Guide：
  http://www.microsoft.com/technet/security/prodtech/Windows2000/w2kccug/default.mspx
- Windows 2000 Common Criteria Evaluated Configuration Administrator's Guide：
  http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/default.mspx
- Windows 2000 Common Criteria Security Configuration Guide：
  http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccscg/default.mspx

Windows XP のマニュアル

- Windows XP Common Criteria Evaluated Configuration User's Guide：
  http://download.microsoft.com/download/d/3/0/d304ab38-567c-4fad-a368-a3661ca1a16d/wxp_common_criteria_user_guide.zip
- Windows XP Common Criteria Evaluated Configuration Administrator's Guide：
  http://download.microsoft.com/download/e/8/9/e897a1ee-0273-4694-b155-ad02f7b2b4d5/wxp_common_criteria_admin_guide.zip
- Windows XP Common Criteria Security Configuration Guide：
  http://download.microsoft.com/download/5/3/b/53b53a3e-39d5-4d30-86f2-146aa2c7be45/wxp_common_criteria_configuration_guide.zip

セキュリティ アプライアンスのコンフィギュレーションを定期的に確認して、次のようなことが発生してもコンフィギュレーションが引き続き組織のセキュリティ ポリシーに適合することを保証する必要があります。

- セキュリティ アプライアンスのコンフィギュレーションの変更
- 組織のセキュリティ ポリシーの変更
- 非信頼ネットワークからの脅威の変化
- セキュリティ アプライアンスの管理スタッフや操作スタッフの変更、またはセキュリティ アプライアンスの物理的な環境の変化

物理的なセキュリティ

セキュリティ アプライアンスは、信頼されている管理者だけがアクセスできる物理的にセキュアな環境に配置する必要があります。侵入者がセキュリティ アプライアンスに物理的にアクセスすると、セキュリティ アプライアンスのセキュアなコンフィギュレーションが損なわれる可能性があります。同様に、セキュリティ アプライアンスのシステム ログ メッセージの格納および管理に使用する監査サーバは、物理的に保護し、適切な識別 / 認証メカニズムを適用して、信頼されている管理者だけがアクセスできるようにする必要があります。

オペレーション モード

ファイアウォール

製品のファイアウォール コンポーネントには、Audit Trail Full、ルーテッド、透過という 3 つのオペレーション モードがあります。認可された管理者は、ルーテッド モードまたは透過モードで動作するようにセキュリティ アプライアンスを設定できます。これらのモードのどちらでも、1 つのコンテキストまたは複数のコンテキストとして動作するようにセキュリティ アプライアンスを設定できます。マルチコンテキストを選択した場合は、すべてのコンテキストがルーテッドまたは透過のいずれかとして動作する必要があります。両方の混合は許可されていません。詳細については、『*Cisco Security Appliance Command Line Configuration Guide, Version 7.0*』の「Security Context Overview」の項を参照してください。

ルーテッド モード

これは、セキュリティ アプライアンスに設定されているデフォルトのモードです。外部ネットワークでセキュリティ アプライアンスの IP アドレスを参照できます。このモードでは、この製品にネットワーク アドレス変換を設定できます。

透過モード

透過モードの場合、セキュリティ アプライアンスの IP アドレスは、外部ネットワークには見えません。送信されるトラフィックは、その最終的な宛先にアドレス指定される必要があります。このモードでは、ネットワーク アドレス変換を設定できません。片方のモードでしか使用できないコマンドもあるため、モードが変更されると、セキュリティ アプライアンスは、以前に設定されていたモードをクリアします。ルーテッド モードと透過モードのどちらでも、トラフィック フローを許可するにはアクセス リストを設定する必要があります。

Audit Trail Full モード

デフォルトでは、監査サーバがいっぱいまたは使用不能になった場合、ネットワーク インターフェイスに到着するトラフィックはセキュリティ アプライアンスを通過できません。監査サーバがいっぱいまたは使用不能であるときにトラフィックがアプライアンスを通過したことを、認可された管理者が検出した場合は、「logging no permit-hostdown」コマンドを使用して Audit Trail Full モードを再度アクティブ化する必要があります。この方法をとらないと、監査可能イベントが、監査証跡に記録されずに発生する可能性があります。

監査サーバ

監査サーバには、PFSS Active および Log Searching という 2 つのオペレーション モードがあります。これら 2 つのモードは互いに分離されており、両方を同時に実行することも、一度に 1 つだけをアクティブにすることもできます。

PFSS Active モード

このモードでは、PIX Firewall Syslog Server アプリケーションが監査サーバ上で動作し、ファイアウォール コンポーネントから監査イベントの詳細が転送されるのを待ちます。アプリケーションは、ファイアウォール コンポーネントからの TCP 接続をリスンし、転送された監査イベントの詳細を、監査サーバのオペレーティング システムが保持しているファイルに記録します。アプリケーションが動作していない場合は、監査イベントの詳細が記録されません。監査可能イベントが、通知されずに発生する可能性があります（上記の「Audit Trail Full モード」を参照してください）。

Log Searching モード

このモードでは、検索 / ソート アプリケーションが監査サーバ上で動作し、認可された管理者によって使用されて監査イベントの詳細を表示します。このアプリケーションは、適切な権限を持つユーザ（特に、認可された監査サーバ管理者）が起動および停止できる標準的な実行ファイルです。アプリケーションが起動されていない場合または停止されている場合は、アプリケーションで監査イベントの詳細を表示できません。監査サーバのオペレーティング システムによって保持されている、監査イベントの詳細を含むファイルは、検索 / ソート アプリケーションで変更できません。

潜在的な非セキュア コンフィギュレーション（誤用）

コミットされていない変更

セキュリティ アプライアンスは、保存されているスタートアップ コンフィギュレーションをロードし、そのコンフィギュレーションを自動的に実行コンフィギュレーションにコピーします。ユーザは、自分のニーズに合せて実行コンフィギュレーションを設定した場合、その実行コンフィギュレーションを保存するか、またはアップデートしたコンフィギュレーションをスタートアップ コンフィギュレーションに保存します。実行コンフィギュレーションは揮発性メモリに保持されるため、動作上の理由や動作エラーでセキュリティ アプライアンスがリロードされる場合、保存されていない変更内容があると、その変更内容が失われます。

デフォルトのフロー ポリシー

インストール時に、デフォルトで、セキュリティ アプライアンスにデフォルトの DHCP アドレス プールが設定されます。発信インターフェイスは、外部から内部へのデータ フローをすべて拒否します。管理者はこれを認識し、ユーザがセキュリティ アプライアンスの使用を許可される前に、組織にとって適切なポリシーが導入されコミットされていることを確認する必要があります。トラフィックがセキュリティ アプライアンスを通過できるようにするには、アクセス リストを設定する必要があります。プロトコル、送信元と宛先の IP アドレスまたはネットワーク、およびオプションで送信元ポートおよび宛先ポートに、特定の許可規則または拒否規則を適用する必要があります。

監査のコンフィギュレーション

タイムスタンピングをイネーブルにするために、ファイアウォール管理者は「logging timestamp」コマンドを入力する必要があります。コマンド「write memory」を使用してこのコマンドをコミットすると、このコマンドがデフォルトとして残ります。

デフォルトでは、監査イベントが UDP でリモート Syslog サーバに転送されます。監査イベントが確実にリモート Syslog サーバに転送されるようにするには、TCP オプションを使用する必要があります。これを行うには、「logging host <ip-address> tcp/<port-number>」コマンドを使用します。

管理アクセス

管理者がセキュリティ アプライアンスの管理に使用できる方法は、次の 2 つだけです。

- セキュリティ アプライアンスに直接接続されているシリアル インターフェイスを使用する。
- SSH アクセスを使用する。

サーバとプロキシ

セキュリティ アプライアンスの出荷時に完全なセキュリティを確保するため、当初はすべてのプロキシおよびサーバへの着信アクセスがディセーブルになっています。インストール後、各サービスを明示的に許可し、セキュリティ ポリシーに必要なサービスをイネーブルにする必要があります。ログ ファイルのメッセージを表示するには、**show logging** コマンドまたはセキュリティ アプライアンス Syslog サーバを使用します。セキュリティ アプライアンスの設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。認定では、指定されたサービスが許可され、他のすべてのサービスが拒否される、完全に制御された環境が要求されています。

ロギングとメッセージ

ログ ファイルのモニタリング アクティビティは、ネットワーク セキュリティの重要な側面であり、定期的に実行する必要があります。ログ ファイルをモニタリングすることで、セキュリティ違反や将来セキュリティ違反につながる可能性のあるイベントを検出した場合に、タイムリーに適切な対応策を取ることができます。ログ ファイルのメッセージを表示するには、**show logging** コマンドまたはセキュリティ アプライアンス Syslog サーバを使用します。メッセージの送信、およびアーカイブについては、『*Cisco Security Appliance System Log Messages*』を参照してください。

アクセス リスト

access-list コマンドは、ファーストマッチ ベースで動作します。そのため、アクセス リストに追加される最後の規則は、最後にチェックされる規則です。最後の規則は規則解析の残りの部分に影響を及ぼす可能性があるため、管理者は、設定中に初期規則を入力するときに、最後の規則に注意する必要があります。

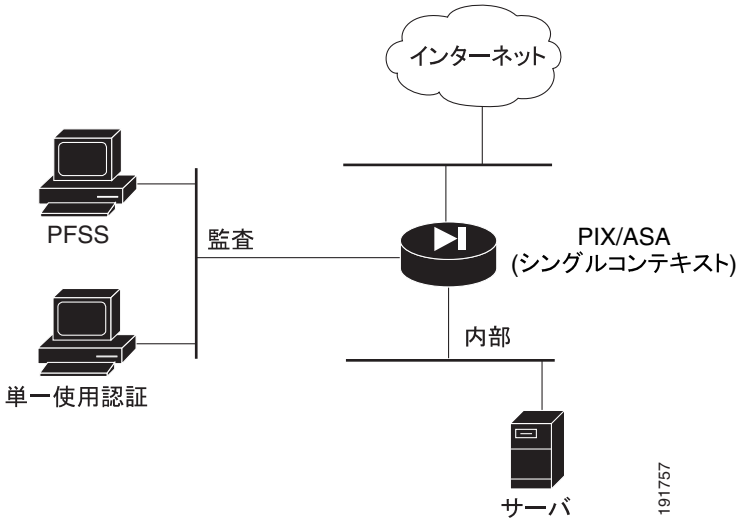
信頼ネットワークと非信頼ネットワーク

セキュリティ アプライアンスは、ネットワークをインターネットまたは別のネットワークから分離するために使用できます。信頼ネットワークは、通常、内部ネットワークです。非信頼ネットワークは、インターネットの場合も他のネットワークの場合もあります。そのため、セキュリティ アプライアンスが内部ネットワークとすべての外部ネットワークの間の唯一のネットワーク接続として機能するように、セキュリティ アプライアンスを設定する必要があります。セキュリティ アプライアンスは、規則が定義されていないすべての情報フローを拒否します。セキュリティ実装は、あるネットワークから別のネットワークへのトラフィック制御に基づきます。また、セキュリティ実装は、セキュリティ ポリシーをサポートする必要があります。

PFSS は、ファイアウォールにシステム監査ストアを提供する Windows Syslog サービスです。PFSS には、ファイアウォールが動作しているモードに応じて、ファイアウォールとの通信用の設定が必要となります。

ファイアウォールがシングルコンテキスト モードで動作している場合、PFSS サーバには通信用の独自の定義済みインターフェイスが必要となります。このインターフェイス上で Syslog TCP を介してメッセージを監査サーバに記録するように、このインスタンスの「logging host」コマンドを設定します。

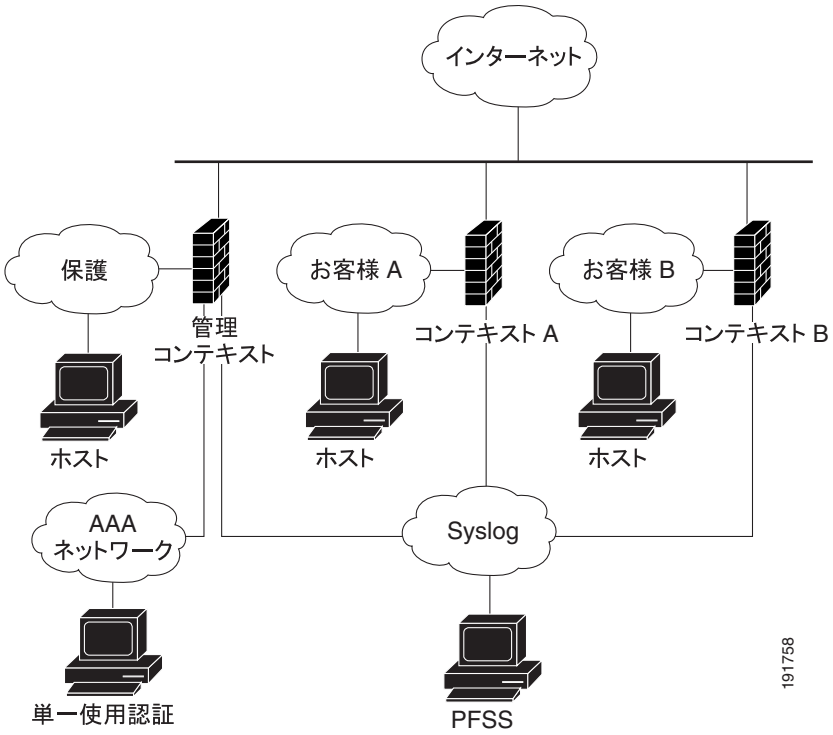
図 1　　シングルコンテキスト



ファイアウォールがマルチコンテキスト モードで動作している場合は、各コンテキストが監査サーバおよびコンフィギュレーション設定と通信するように定義し、ポリシーで特別に許可されている以外のトラフィックを受信しないように監査サーバを保護する必要があります。

ファイアウォールが透過モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。この場合もルート文を設定することはできますが、セキュリティ アプライアンスから発信されたトラフィックだけに適用されます。たとえば、Syslog サーバがリモート ネットワークにある場合は、セキュリティ アプライアンスがそのサブネットに到達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。

図 2　　マルチコンテキスト



（注） 監査サーバの適切な保護を実現するため、PFSS サーバを信頼ネットワーク上に配置し、PFSS への TCP Syslog データだけ許可するアクセスコントロール リストをファイアウォールに適用する必要があります。

この例では、PFSS サーバが IP アドレス 1.2.3.4 で設定され、ファイアウォールがシステム ログを 3.4.5.6 から送信しています。マルチコンテキストが使用されている場合は、アクセス リストに行を追加する必要があります。

```
hostname(config)# access-list INSIDE extended permit tcp host 3.4.5.6
host 1.2.3.4 eq 1470
hostname(config)# access-group INSIDE in interface inside
```

（注） ファイアウォールが、直接接続されているスイッチに対するレイヤ 2 攻撃によってバイパスされないようにするには、ファイアウォールに接続されている各ネットワーク間で別個の物理スイッチを使用する必要があります。

表 3　デフォルト コンフィギュレーションでは、トラフィック タイプは内部から外部へのトラフィックに関するデフォルト ポリシーに従う

トラフィック タイプ	シングル ルーテッド モード	マルチ ルーテッド モード	シングル透過モード	マルチ透過モード
スプーフィングされたトラフィック	No（RPF がイネーブル）	No（RPF がイネーブル）	No（ARP 検査がイネーブル）	No（ARP 検査がイネーブル）
イーサネット	Yes	Yes	Yes	Yes
ARP	No（ルータ ホップ）	No（ルータ ホップ）	Yes	Yes
CTIQBE	Yes	Yes	Yes	Yes
DNS	Yes	Yes	Yes	Yes
エコー	Yes	Yes	Yes	Yes
Finger	Yes	Yes	Yes	Yes
H.323	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes
ICMP	Yes	Yes	Yes	Yes
TCP	Yes	Yes	Yes	Yes
UDP	Yes	Yes	Yes	Yes
FTP	Yes	Yes	Yes	Yes
GTP	Yes	Yes	Yes	Yes
HTTP	Yes	Yes	Yes	Yes
ILS	Yes	Yes	Yes	Yes
MGCP	Yes	Yes	Yes	Yes
POP3	Yes	Yes	Yes	Yes
RSH	Yes	Yes	Yes	Yes
RTSP	Yes	Yes	Yes	Yes
Skinny	Yes	Yes	Yes	Yes
SIP	Yes	Yes	Yes	Yes
ESMTP	Yes	Yes	Yes	Yes
SunRPC	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes
XDMCP	Yes	Yes	Yes	Yes
トレースルート	Yes	Yes	Yes	Yes
STP	No	No	Yes	Yes
その他すべてのトラフィック	Yes	Yes	Yes	Yes

表 4　デフォルト コンフィギュレーションでは、トラフィック タイプは外部から内部へのトラフィックに関するデフォルト ポリシーに従う

トラフィック タイプ	シングル ルーテッド モード	マルチ ルーテッド モード	シングル透過モード	マルチ透過モード
スプーフィングされたトラフィック	No（RPF がイネーブル）	No（RPF がイネーブル）	No（ARP 検査がイネーブル）	No（ARP 検査がイネーブル）
イーサネット	No	No	Yes	Yes
ARP	No（ルータ ホップ）	No（ルータ ホップ）	No	No
CTIQBE	No	No	No	No
DNS	No	No	No	No
エコー	No	No	No	No
Finger	No	No	No	No
H.323	No	No	No	No
IP	No	No	No	No
ICMP	No	No	No	No
TCP	No	No	No	No
UDP	No	No	No	No
FTP	No	No	No	No
GTP	No	No	No	No
HTTP	No	No	No	No
ILS	No	No	No	No
MGCP	No	No	No	No
POP3	No	No	No	No
RSH	No	No	No	No
RTSP	No	No	No	No
Skinny	No	No	No	No
SIP	No	No	No	No
ESMTP	No	No	No	No
SunRPC	No	No	No	No
Telnet	No	No	No	No
TFTP	No	No	No	No
XDMCP	No	No	No	No
トレースルート	No	No	No	No
STP	No	No	Yes（ACL によって拒否できる）	Yes（ACL によって拒否できる）
その他すべてのトラフィック	No	No	No	No

パブリック アクセス サーバ

パブリック アクセス サーバをホストする計画がある場合は、パブリック アクセス サーバをセキュリティ アプライアンスに対してどの位置に配置するかを決定する必要があります。セキュリティ アプライアンスの外部にあるネットワークにサーバを配置すると、サーバが攻撃に対して無防備なままになります。サーバを内部ネットワークに配置する場合は、アクセスを許可するようにセキュリティ アプライアンスを設定する必要があります。

FTP の使用

リモート サーバ上のファイルを取得したり、リモート サーバ上にファイルを置いたりする場合は、File Transfer Protocol（FTP; ファイル転送プロトコル）を使用します。ネットワークを介した接続のように、コンソールを使用してリモート サーバにアクセスするには、Telnet を使用します。共通基準のセキュリティ ターゲットでは、セキュリティ アプライアンスを通過する Telnet トラフィックおよび FTP トラフィックは、通過前に認証を受ける必要があります。Telnet および FTP を認証するようセキュリティ アプライアンスを正しく設定する方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Authentication for Network Access」の項を参照してください。

モニタリングとメンテナンス

セキュリティ アプライアンス ソフトウェアには、セキュリティ アプライアンスを監視するためのいくつかの方法（ログからメッセージまで）が用意されています。

- セキュリティ アプライアンスのパフォーマンスと、発生する可能性のあるセキュリティ問題の両方を監視する方法を認識しておきます。
- バックアップを計画します。ハードウェアまたはソフトウェアの問題が発生した場合は、セキュリティ アプライアンスのコンフィギュレーションを復元する必要が生じることがあります。
- セキュリティ アプライアンスのコンフィギュレーションを定期的に確認して、次のようなことが発生してもコンフィギュレーションが組織のセキュリティ目標を達成することを保証する必要があります。
  - セキュリティ アプライアンスのコンフィギュレーションの変更
  - セキュリティ目標の変更
  - 外部ネットワークからの脅威の変化

管理ロール

認定されたコンフィギュレーションには、評価済みコンフィギュレーション用の 2 つの管理ロールが含まれています。

表 5　評価済みコンフィギュレーション内の管理ロール

ロール名	説明
Authorized Firewall Administrator	ファイアウォールの「イネーブル」パスワードを知っている管理者。特権アクセスは、個々のログイン後にイネーブル パスワードを入力するときの特権レベルによって定義されます。
Authorized Audit Administrator	ログインして、PFSS アプリケーションによって記録された情報を確認するユーザに割り当てられるロール。

監査コンポーネントの要件

セキュリティ アプライアンスは、監査データを格納するために Windows サーバと対話します。Windows サーバは Windows 2000 Service Pack 4 または Windows XP Service Pack 2 を実行している必要があります。監査マシンは、適切な監査レコードを管理者に提供し、格納されている監査レコードを不正な削除から保護し、監査レコードに対する変更を検出します。セキュリティ アプライアンスから提供される監査レコードを定期的に確認し、必要に応じて対応策を取って適応型セキュリティ アプライアンスのセキュリティを確保するのは、管理者の責任です。監査マシンおよび監査レコードの場所には、管理者だけがアクセスできるようにする必要があります。

パスワードの複雑性

パスワードの長さは、8 ～ 16 文字にする必要があります。管理者がパスワードの最小長を強制する必要があります。パスワードに使用できる文字は、次のとおりです。

- アルファベット 26 文字の大文字（A ～ Z）
- アルファベット 26 文字の小文字（a ～ z）
- 10 個の数字（0 ～ 9）
- !"#$%&'()*+,-./:;<@[\`{|=>?]^_}~

これが、パスワードの作成に使用できる 94 文字すべてです。空白文字は使用できません。

この項に示すパスワード ガイダンスは、ユーザ パスワードの作成と管理に適用されます。ユーザは、パスワードを作成または変更するときに、次の要件が満たされていることを確認する必要があります。

1. 次のようなパスワードであること
   - 8 ～ 16 文字
   - 大文字と小文字のアルファベット文字を含む
   - 数字を少なくとも 1 つ含む
2. 次のものを含まないパスワードであること
   - 誕生日
   - 名前（親、家族、配偶者、ペット、好きなスポーツ選手）
   - スポーツ チーム
   - 町、市、または国

IT 環境での AAA サーバと認証ポリシー

この認定済みコンフィギュレーションで指定されている AAA サーバは、環境内に含まれています。管理者は、インストール中に AAA サーバで次のことが可能であることを確認する必要があります。

- 各ユーザのアトリビュート（ID、ユーザと管理者アカウントの関連付け、およびパスワード）の保持
- ファイアウォール管理者が、リモートでファイアウォールにアクセスする前に、単一使用認証メカニズムで認証を受けること
- ユーザが、ファイアウォールを通過する FTP または Telnet を使用するときに、単一使用認証メカニズムで認証を受けること
- 認可された管理者がローカル　コンソールを使用してファイアウォールまたはルータのコンソールに直接アクセスする場合に、再使用可能なパスワードを使用できること
- セキュリティ アプライアンス上のコンソール接続および「enable」に、再使用可能なパスワードを使用できること

セキュリティ ターゲットの IT 環境の項では、管理者がガイダンスに従うことが要求されています。そのガイダンスとは、認定されたコンフィギュレーションを管理するために各要求で必要となる認証タイプに関するガイダンスです。

ソフトウェア バージョンの確認

セキュリティ アプライアンス装置のソフトウェア バージョンを確認するには、**show version** コマンドを使用します。

インストールに関する注意事項

セキュリティ アプライアンスをインストールする前に、『*Cisco ASA 5500 Hardware Installation Guide*』を読んでください。

ハードウェアとソフトウェア イメージの確認

次の手順を実行して、配送中にセキュリティ アプライアンスのソフトウェアおよびハードウェアに不正な変更が加えられていないことを確認します。

ステップ 1 セキュリティ アプライアンスを開梱する前に、配達された装置を梱包している物理的なパッケージを調べます。段ボールの外箱にシスコシステムズのロゴとモチーフが印刷されていることを確認します。印刷されていない場合は、装置の納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）にお問い合せください。

ステップ 2 パッケージを封印しているテープを調べて、パッケージが明らかに開封されたり、封印し直されたりしていないことを確認します。パッケージが封印し直されているような場合は、装置の納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）にお問い合せください。

ステップ 3 段ボールの外箱に、シスコシステムズの白い改ざん防止用バーコード ラベルが貼られていることを確認します。貼られていない場合は、装置の納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）にお問い合せください。このラベルには、シスコの製品番号、シリアル番号、およびボックスの中身に関するその他の情報が記載されています。

ステップ 4 出荷書類に記載されているセキュリティ アプライアンスのシリアル番号に注意します。外箱の白いラベルに記載されているシリアル番号が、セキュリティ アプライアンスのそのシリアル番号です。出荷書類に記載されているシリアル番号が、装置の納品伝票（別途郵送）に記載されているシリアル番号と一致することを確認します。一致しない場合は、装置の納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）にお問い合せください。

ステップ 5 予定されていた装置納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）からボックスが実際に出荷されたことを確認します。これを行うには、ボックスを配達した宅配業者と、納入業者が出荷に使用した宅配業者が一致すること、および受け取った送り状の番号が配送時に使用された番号と一致することを、納入業者に確認します。また、出荷されたアイテムのシリアル番号が、配達されたアイテムのシリアル番号と一致することも確認します。この確認作業は、実際の装置配送に関与しなかったメカニズム（たとえば、電話やファックス、その他のオンライン追跡サービスなど）で行う必要があります。

ステップ 6 セキュリティ アプライアンスを開梱したら、装置を調べます。装置本体に表示されているシリアル番号が、出荷書類および納品伝票に記載されているシリアル番号と一致することを確認します。一致しない場合は、装置の納入業者（シスコシステムズ、あるいは認可されているシスコの代理店またはパートナー）にお問い合せください。

ステップ 7 共通基準の評価済みソフトウェア イメージを入手するには、次の 3 つの方法があります。

- 共通基準の評価済みソフトウェア イメージ ファイルを Cisco.com から、信頼できるコンピュータ システムにダウンロードします。このサイトにアクセスするには、登録ユーザとしてログインする必要があります。ソフトウェア イメージは、Cisco.com の URL http://www.cisco.com/kobayashi/sw-center/ から入手できます。

- セキュリティ アプライアンスに同梱の CD に、現在のソフトウェア イメージがすべて含まれています。この CD で、共通基準の評価済みソフトウェア イメージ Version 7.0(6) を入手できます。
- お客様は、Cisco.com で、現在のすべてのソフトウェア イメージを含む CD を注文できます。これは、有料のオプションです。

ステップ 8 706-k8.bin or pix 706.bin ファイルをダウンロードします。

ステップ 9 ファイルをダウンロードしたら、MD5 ユーティリティを使用して、ダウンロードしたファイルの MD5 ハッシュを計算し、イメージの MD5 ハッシュ（後述）と比較して、ファイルが改ざんされていないことを確認します。MD5 ハッシュが一致しない場合は、Cisco TAC にお問い合せください。どちらのファイルの MD5 も 27164a0652cc4fe86fe35370f98fe733 です。

ステップ 10 Web からダウンロードしたイメージをフラッシュにコピーするには、次のコマンドを入力します。

a. **copy tftp:/1.2.3.4/**asa706-k8.bin **disk0:**
b. boot system **disk0:/**cdisk.bin
c. **write memory**
d. **reload**

ステップ 11『*Cisco Security Appliance Command Line Configuration Guide*』の「Getting Started」の章の説明に従って、セキュリティ アプライアンスを起動します。セキュリティ アプライアンスがイメージを正しくロードし、内部のセルフチェックを完了することを確認します。プロンプトで、次のように **show version** コマンドを入力します。バージョンが 7.0(6) であることを確認します。セキュリティ アプライアンスのイメージのロードに失敗した場合、またはセキュリティ アプライアンスのバージョンが 7.0(6) でない場合は、Cisco TAC にお問い合せください。

次に、「**show version**」コマンドの出力例を示します。セキュリティ アプライアンスのバージョンが表示されています。

```
hostname# show version
Cisco ASA Software Version 7.0(6)
PIX (7.0.1.0) #28: Mon XXX 23 15:37:25 EDT 2005
ASA up 21 mins 44 secs
Hardware: ASA5530-K8, 2048 MB RAM, CPU Pentium 4 Celeron 2500 MHz
Internal ATA Compact Flash, 489MB
Slot 1: ATA Compact Flash, 244MB
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
Encryption hardware device: Cisco ASA-55x0 on-board accelerator (revision 0x0)
Boot microcode: CNlite-MC-Boot-Cisco-1.2
SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
IPSec microcode: CNlite-MC-IPSECm-MAIN-2.01
0: Ext: GigabitEthernet0/0: media index 0: irq 9
1: Ext: GigabitEthernet0/1: media index 1: irq 9
2: Ext: GigabitEthernet0/2: media index 2: irq 9
3: Ext: GigabitEthernet0/3: media index 3: irq 9
4: Ext: Management0/0: media index 0: irq 11
5: Int: No HWIDB: media index 4: irq 11
6: Int: Control0/0: media index 1: irq 5
License Features for this Platform:
Maximum Physical Interfaces: Unlimited
Maximum VLANs: 50
Inside Hosts: Unlimited
Failover: Enabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Security Contexts: 20
GTP/GPRS: Disabled
VPN Peers: 5000
Serial Number: P3000000002
Running Activation Key: 0x881ed361 0x447555a8 0xac73bc44 0xb3f0f888 0x8e26f18b
Configuration register is 0x11
Configuration last modified by enable_15 at 15:55:27.399 UTC Mon XXX 23 2005
```

コンフィギュレーションに関する注意事項

ここでは、次の項目について説明します。

コンフィギュレーションの保存

セキュリティ アプライアンスのコンフィギュレーションに変更を加える場合は、頻繁に **write memory** コマンドを使用する必要があります。コミットされていない変更がある場合にセキュリティ アプライアンスがリブートして動作を再開すると、コミットされていない変更が失われ、セキュリティ アプライアンスは最後に保存されたコンフィギュレーションに戻ります。

established コマンドの使用

認定されたセキュリティ アプライアンスでは、管理者が **established** コマンドを使用しないことが推奨されています。このコマンドを誤って使用すると、外部ユーザに内部システムに対するアクセス権を意図していたよりも多く与えてしまう可能性があります。そのため、このコマンドの使用は推奨されていません。詳細については、次の Web サイトにアクセスして参照してください。

http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/products_security_advisory09186a008009429 3.shtml

タイムスタンプのイネーブル化

デフォルトでは、どの監査レコードにも、イベントの発生時にシステム クロックから生成される日時が刻印されません。認定されたセキュリティ アプライアンスでは、タイムスタンプ オプションをイネーブルにする必要があります。監査イベントのタイムスタンプをイネーブルにするには、**logging timestamp** コマンドを使用します。タイムスタンプ オプションをデフォルトとして残すには、**write memory** コマンドを使用して、このオプションをスタートアップ コンフィギュレーションに保存します。

信頼性の高いロギングのイネーブル化

デフォルトでは、監査イベントは UDP でリモート Syslog サーバに転送されます。認定されたセキュリティ アプライアンスでは、監査イベントを TCP で転送する必要があります。TCP オプションを設定するには、**logging host** interface *ip_address* **tcp**/*port_number* コマンドを使用します。TCP ロギングが設定されていると、ログ メッセージをリモート ホストに転送できない場合、認定されたセキュリティ アプライアンス経由の新しいセッションが拒否されます。

TCP ロギング機能を促進するには、セキュアな Windows サーバ上に適応型セキュリティ アプライアンスを設定する必要があります。ロギング機能を取得して設定する方法の詳細については、「セキュリティ アプライアンス Syslog サーバの使用」を参照してください。

システム ログ

『*Cisco Security Appliance System Log Messages*』に、セキュリティ アプライアンスのシステム ログの詳細が記載されています。認定されたセキュリティ アプライアンスでは、次の各項がサポートされていません。

- セキュリティ アプライアンスのシステム ログ
  - Receiving SNMP Requests
  - Sending SNMP Traps
- 他のリモート管理ツールおよびモニタリング ツール
  - ASDM
  - Cisco Secure Policy Manager
  - SNMP Traps

（注） 認定されたセキュリティ アプライアンスでは、Telnet がサポートされていません。Telnet は、デフォルトでディセーブルになっています。

サーバの設定

ACS サーバをインストールする必要があります。Cisco Secure ACS のインストールについては、http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/install/inst02.htm#wp980695 にあるマニュアルを参照してください。

セキュリティ アプライアンスでの認証の設定

サーバ グループを作成し、そのグループに AAA サーバを追加し、プロトコルを設定して、SSH に認証を追加するには、次の手順を実行します。

（注） 評価済みのコンフィギュレーションには、セキュリティ プロトコル TACACS+ および RADIUS だけが含まれています。aaa-server で、他のプロトコル オプションを選択しないでください。TACACS+ と RADIUS はどちらも、サーバに対する認証でパスワードを要求します。管理者は、RADIUS または TACACS+ のパスワードを作成する場合、このマニュアルのガイダンスに従う必要があります。

ステップ 1 サーバ グループ名とプロトコルを指定します。これを行うには、次のコマンドを入力します。

```
hostname(config)# aaa-server server_group protocol {radius | tacacs+}
```

たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバ グループを作成する必要があります。

最大 15 のシングルモード サーバ グループまたは 4 つのマルチモード サーバ グループを指定できます。各サーバ グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

aaa-server protocol コマンドを入力する場合は、グループ モードに移行します。

ステップ 2 ネットワーク上の各 AAA サーバについて、次の手順を実行します。

サーバを、所属する AAA サーバ グループを含めて、指定します。これを行うには、次のコマンドを入力します。

```
hostname(config)# aaa-server server_group (interface_name) host server_ip password
```

aaa-server host コマンドを入力する場合、ホスト モードに移行します。

AAA サーバとグループの設定後、次のコマンドを使用して認証を設定します。

```
hostname(config)# aaa authentication enable console [server-tag | LOCAL]
```

セキュリティ アプライアンスは、管理目的でセキュリティ アプライアンスへの SSH 接続を許可します。セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。評価済みのコンフィギュレーションにおける SSH セッションは、ローカル パスワード データベースではなく、単一使用パスワード ソリューションを使用して認証される必要があります。

```
hostname(config)# aaa authentication ssh console [server-tag]
```

（注） イネーブル認証では、ローカル ユーザ データベースまたはリモート AAA サーバのいずれかを使用でき、再使用可能なパスワードが許可されています。SSH 認証では、単一使用認証用に設定されているリモート AAA サーバを使用する必要があります。認証方式「none」の使用は許可されていません。

（注） 現時点では、セキュリティ プロトコル TACACS+ および RADIUS だけがサポートされています。

SSH の設定については、『*Cisco Security Appliance Command Line Configuration Guide, Version 7.0*』の「Allowing SSH Access」の項を参照してください。

（注） デフォルトでは、SSH バージョン 1 と SSH バージョン 2 の両方が許可されますが、必ずバージョン 2 を選択してください。バージョン番号を指定するには、hostname(config)# ssh version version_number コマンドを入力します。

（注） SSH セッションの確立後、管理者は「>」プロンプトで enable コマンドではなく「login」と入力してから、ローカル データベース アカウントとパスワードでログインする必要があります。この方法により、すべての監査イベントがそのローカル ユーザに帰属します。

AAA を使用するファイアウォールに対するコンソール アクセスの設定（オプション）

AAA を使用するファイアウォールに対するコンソール アクセスはオプションですが、評価済みのコンフィギュレーションでは不要です。

システム管理者の認証とコマンド認可をイネーブルにする方法については、『*Cisco Security Appliance Command Line Configuration Guide 7.0*』の「AAA for System Administrators」の項を参照してください。

セキュリティ アプライアンス上のユーザ名

認定されたコンフィギュレーションでは、ユーザ名が定義され、定義済みのロールを各個人に分割するために使用されます。ユーザ名は、スーパーバイザ モジュールからローカル セッションで、認定されたコンフィギュレーションに対して身元を明らかにするために使用されます。ユーザにパスワードと特権レベルを割り当てるには、**username** コマンドを使用します。特権レベルの範囲は 0（最低）～ 15 です。一般に、システム管理者は最高の特権レベルを持ちます。

username *name* {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

（注） 評価済みのコンフィギュレーションでは、レベル 15 のユーザだけが必須です。

次の例では、ユーザ名は testuser です。

```
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

評価済みのコンフィギュレーションがマルチコンテキスト モードで動作している場合、ユーザ名は、その作成元の 1 つのコンテキストだけで使用できます。

コマンド構文の詳細については、『*Cisco Security Appliance Command Reference, Version 7.0*』を参照してください。

（注） 評価コンフィギュレーションでは、ローカル認証は SSH 認証のオプションではありません。また、管理者が認証オプションに none という値を単独で使用しないことが推奨されています。「none」という値を単独で使用すると、パスワードを入力する必要がなくなります。

Telnet および FTP の AAA の設定

カットスルー プロキシを使用する Telnet および FTP の AAA を設定するには、まず AAA サーバ グループと認証の設定を行う必要があります。これらの設定が有効になった後、aaa authentication include {telnet, ftp} コマンドを使用して、Telnet および FTP の認証をイネーブルにします。

（注） 非標準のポートで FTP サーバおよび Telnet サーバを実行すると、そのフローが RADIUS および TACACS+ の認証を要求しません。これは、評価済みのコンフィギュレーションでは許可されていません。

```
hostname(config)# aaa-server aaasrvgrp protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server aaasrvgrp host 10.30.1.20
hostname(config-aaa-server-host)# authentication-port 1645
hostname (config-aaa-server-host)# timeout 10
hostname (config-aaa-server-host)# retry-interval 2
hostname (config-aaa-server-host)# exit
hostname (config)# aaa authentication include telnet outside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include ftp outside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include telnet inside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include ftp inside 0 0 0 0 aaasrvgrp
```

マルチユーザ マシンからの別個のセッションが既存の認証要求にピギーバックできないようにするには、認証のタイムアウトを 0 に設定して、認証データがキャッシングされないようにします。

```
hostname (config)# timeout uauth 0:00:00
```

フェールオーバーの設定

（注） フェールオーバーを使用する場合は、2 つのファイアウォール装置間で使用される認証パスワードを必ず設定してください。コマンドは「failover key {secret | hex key}」です。キーとして使用されるパスワードが、このマニュアルの「パスワードの複雑性」のガイダンスに従っていることを確認してください。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide, Version 7.0*』の「Configuring Failover」の章を参照してください。

ICMP 検査

ICMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。**inspect icmp** コマンドは、PFSS 監査サーバに障害が発生した場合に、ICMP トラフィックがファイアウォールを通過しないようにするために必要です。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

ARP 検査

ARP 検査エンジンを設定するには、グローバル コンフィギュレーション モードで arp-inspection コマンドを使用します。ARP 検査は、ファイアウォール コンテキストが透過モードで動作しているときにトラフィックの IP スプーフィングを防止するために必要です。

ARP 検査のコンフィギュレーションを完了するには、管理者が、ファイアウォール コンテキストによって保護されるホストごとにスタティック ARP エントリを作成する必要があります。

```
hostname(config)# arp inside 1.2.3.4 0050.abcd.1234
hostname(config)# arp-inspection outside enable
hostname(config)# arp-inspection inside enable
```

Unicast RPF

Unicast RPF をイネーブルにするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。Unicast RPF は、コンテキストがルーティング モードで動作している場合にだけ適用できます。

```
hostname(config)# ip verify reverse-path interface outside
hostname(config)# ip verify reverse-path interface inside
```

STP と透過モード

透過モードの場合、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）はデフォルトでファイアウォールを通過します。このトラフィックをブロックするアクセス リストを作成することにより、製品のこのデフォルト動作を抑制できます。

```
hostname(config)# access-list layer2 ethertype deny bpdu
```

同じセキュリティのトラフィック

評価済みのコンフィギュレーションでは、「same-security-traffic」コマンドは許可されていません。このコマンドがイネーブルであると、現在のセキュリティ ポリシーに関係なく、同じセキュリティ レベルのインターフェイス間をトラフィックが通過できます。「same-security-traffic」がイネーブルである場合は、include を使用して設定された AAA 文はすべてバイパスされます。

セキュリティ アプライアンス Syslog サーバの使用

セキュリティ アプライアンス Syslog サーバ（このマニュアルでは PFSS とも呼ばれる）を使用すると、Windows システムから Syslog メッセージを表示できます。Windows システムが装備されていると、セキュリティ アプライアンス Syslog サーバの使用により、信頼性という追加の利点が得られます。この信頼性は、TCP イベント メッセージの受信、タイムスタンプ付きのメッセージの受信、およびサーバがアップしているかダウンしているかをセキュリティ アプライアンスから監視する機能によって得られます。セキュリティ アプライアンス Syslog サーバは、Cisco.com から無料で入手できます。セキュリティ アプライアンス Syslog サーバのインストール手順については、『*Installation Guide for the Cisco Secure PIX Firewall, Version 5.2*』を参照してください。

セキュリティ アプライアンスは、セキュリティ アプライアンス Syslog サーバ（監査サーバとも呼ばれる）に TCP で Syslog メッセージを送信する必要があります。セキュリティ アプライアンス Syslog サーバのシステム ディスクがいっぱいになると、セキュリティ アプライアンスは新しい接続をすべて停止します。

ディスク スペースを使い果たす可能性を最低限に抑えるため、必ずセキュリティ アプライアンス Syslog サーバのログ ファイルを定期的にバックアップしてください。

セキュリティ アプライアンス Syslog サーバを使用する方法の詳細については、このマニュアルの「セキュリティ アプライアンスのシステム ログ メッセージの検索に使用するシステム ログ メッセージ検索機能の設定」の項を参照してください。

（注） 監査レコードを相関させることができるように、ファイアウォールと Windows サーバの間で時刻を同期させてください。

ここでは、次の項目について説明します。

- セキュリティ アプライアンス Syslog サーバの設定（P.25）
- Windows システムでの Syslog サーバ パラメータの変更（P.27）
- セキュリティ アプライアンス Syslog サーバのディスク満杯状態からの回復（P.28）

セキュリティ アプライアンス Syslog サーバの設定

Syslog サーバを使用するようにセキュリティ アプライアンスを設定するには、次の手順を実行します。

ステップ 1 評価済みのコンフィギュレーションでは、セキュリティ アプライアンスと PFSS 監査サービスの間の通信に許可されているプロトコルは TCP だけです。

```
logging host interface ip_address tcp/port_number
```

interface にはサーバが存在するインターフェイスを、*IP-address* にはホストの IP アドレスを、*port-number* には TCP ポート（デフォルト値の 1468 以外の場合）を指定します。**show logging** コマンドを使用して、ディスプレイで「disabled」キーワードを検索することにより、Syslog サーバのディスク満杯状態のためにセキュリティ アプライアンスのトラフィックがディセーブルになっていないかどうかを確認できます。

サーバに対して UDP または TCP の 1 つのコマンド文だけが許可されています。後続のコマンド文は以前のコマンド文を上書きします。コンフィギュレーション内の **logging host** コマンド文を表示するには、**write terminal** コマンドを使用します。コンフィギュレーションで、UDP プロトコルは「17」と表示され、TCP は「6」と表示されます。

ステップ 2 さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するロギング リストを作成します。作成するリストでは、イベント 106023、109001 ～ 109014、109021、109023 ～ 109028、111008、111009、113001、113003、113006、113007、160000 ～ 169999、106014、199002、302013、302014、302020、302021、609001、609002、199001、199005、199006、201008、502101 ～ 502103、605004、605005、および 611101 ～ 611104 が必ずログに記録されるようにする必要があります。グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。

```
logging list name {level level [class event_class] | message start_id[-end_id]}
hostname(config)# logging list CC-config message 106023
hostname(config)# logging list CC-config message 109001-109014
hostname(config)# logging list CC-config message 109021
hostname(config)# logging list CC-config message 109023-109028
hostname(config)# logging list CC-config message 111008-111009
hostname(config)# logging list CC-config message 113001
hostname(config)# logging list CC-config message 113003
hostname(config)# logging list CC-config message 113006-113007
hostname(config)# logging list CC-config message 199001
hostname(config)# logging list CC-config message 199005-199006
hostname(config)# logging list CC-config message 201008
hostname(config)# logging list CC-config message 502101-502103
hostname(config)# logging list CC-config message 605004-605005
hostname(config)# logging list CC-config message 611101-611104
hostname(config)# logging list CC-config message 160000-169999
hostname(config)# logging list CC-config message 106014
hostname(config)# logging list CC-config message 199002
hostname(config)# logging list CC-config message 302013
hostname(config)# logging list CC-config message 302014
hostname(config)# logging list CC-config message 302020
hostname(config)# logging list CC-config message 302021
hostname(config)# logging list CC-config message 609001
hostname(config)# logging list CC-config message 609002
```

ステップ 3 グローバル コンフィギュレーション モードで **logging trap** コマンドを使用して、セキュリティ アプライアンスが Syslog サーバに送信する Syslog メッセージを指定します。このときに、ステップ 2 で作成したロギング リストを使用します。

```
logging trap [logging_list | level]
hostname (config)# logging trap CC-config
```

初期セットアップ中およびテスト中は debugging レベルを使用することをお勧めします。その後、実稼動環境で使用するためにレベルを debugging から errors に設定してください。

ステップ 4 必要に応じて、**logging facility** コマンドをデフォルトの 20 以外の値に設定します。ほとんどの UNIX システムでは、メッセージがファシリティ 20 に到着すると想定しています。ファシリティ 20 では、local4 受信メカニズムでメッセージが受信されます。

ステップ 5 **logging enable** コマンドで、メッセージの送信を開始します。メッセージの送信をディセーブルにするには、**no logging enable** コマンドを使用します。

ある特定のメッセージの Syslog サーバへの送信を停止する場合は、**no logging** *message syslog_id* コマンドを使用します。*syslog_id* には、Syslog メッセージ ID を指定します。

ステップ 6 タイムスタンプ付きのメッセージを Syslog サーバに送信する必要があります。**clock set** コマンドを使用してセキュリティ アプライアンスのシステム クロックを設定し、**logging timestamp** コマンドを使用してタイムスタンピングをイネーブルにします。次に例を示します。

```
clock set 14:25:00 oct 1 2005
logging timestamp
```

この例では、クロックが現在の時刻 2005 年 10 月 1 日午後 2:25 に設定され、タイムスタンピングがイネーブルにされています。

ステップ 7 グローバル コンフィギュレーション モードで **no logging permit-hostdown** コマンドを使用して、Syslog サーバがダウンしたときまたは使用不能になったときにトラフィックを通過させないようにします。デフォルトでは、TCP 接続を使用する Syslog サーバへのロギングをイネーブルにした場合、何らかの理由で Syslog サーバが使用不能になると、ファイアウォールは新しいネットワーク アクセス セッションを許可しません。「no logging permit-hostdown」は、PIX/ASA のデフォルトの動作です。このコマンドが適用されている場合、このコマンドはコンフィギュレーション ファイルに表示されません。

```
hostname(config)# no logging permit-hostdown
```

コマンド構文の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

Windows システムでの Syslog サーバ パラメータの変更

Windows システムで Syslog サーバのパラメータを変更するには、**Start > Settings > Control Panel > Services** を選択します。

Syslog サーバのパラメータ値はすべて、sass.log ファイルを調べることで確認できます。このファイルは、Syslog サーバによって Syslog サーバのログ ファイルと同じディレクトリに作成されます。

Syslog サーバは、インストール直後に起動します。Services コントロール パネルを使用して、新しいパラメータの入力、サービスの一時停止とその後の再開、サービスの停止と開始を行うことができます。

次のうち、1 つまたは複数のパラメータを選択します。

- d%_disk_full：Windows システム ディスクの使用率が何パーセントになると、Syslog サーバがセキュリティ アプライアンスに送信を停止させるか。これは、1 ～ 100 の範囲の整数値です。デフォルトは 90 です。
- t tcp_port：Windows システムが TCP Syslog メッセージのリスンに使用するポート。デフォルトは 1468 です。別のポートを指定する場合は、1024 ～ 65535 の範囲である必要があります。
- u udp_port：Windows システムが UDP Syslog メッセージのリスンに使用するポート。デフォルトは 514 です。別のポートを指定する場合は、1024 ～ 65535 の範囲である必要があります。
- e disk_empty_watch_timer：ディスク パーティションがまだ空いているかどうかを Syslog サーバが調べる間隔（秒単位）。デフォルトは 5 秒です。0 より大きい任意の数字を指定できます。
- f disk_full_watch_timer：ディスク パーティションがまだいっぱいであるかどうかを Syslog サーバが調べる間隔（秒単位）。デフォルトは 3 秒です。0 より大きい任意の数字を指定できます。

次の手順を実行して、%_disk_full を 35% に、disk-full タイマーを 10 秒に設定します。

注意 レジストリが編集されない限り（「syslogd」の「ImagePath」を変更）、これらのパラメータは一度だけ適用されます。

ステップ 1 PIX Firewall Syslog Service のサービス プロパティを表示します。

ステップ 2 サービスを停止します。

ステップ 3 変更するパラメータを入力し（**-d 35 -f 10**）、サービスを開始して、**OK** をクリックします。

（注） 上記の例では、サーバの現在のインスタンスの設定だけが影響を受けます。サービスのレジストリ値がアップデートされた場合に限り、変更が永続的になります。

（注） Syslog サーバは、512 文字よりも長い Syslog メッセージを切り捨てます。

セキュリティ アプライアンス Syslog サーバのディスク満杯状態からの回復

TCP で Syslog メッセージを送信する場合、Windows ディスクがいっぱいになって、セキュリティ アプライアンス装置がトラフィックを停止することがあります。Windows ファイル システムがいっぱいになると、Windows システムはビープ音を鳴らします。Syslog サーバは、その TCP リスン ソケットを閉じることで、セキュリティ アプライアンス装置からのすべての TCP 接続をディセーブルにします。

セキュリティ アプライアンスは、Syslog サーバへの再接続を 5 回試行します。そのリトライ中、セキュリティ アプライアンスを介した新しい接続をすべて停止します。このような場合は、すべてのログ ファイルを別のディスクに、またはネットワークを介して、バックアップする必要があります（Syslog サーバがメッセージを受信している間、ログ ファイルはローカル ディスク上に存在する必要があります）。

ディスク満杯状態から回復するには、次の手順を実行します。

ステップ 1 Windows システム上のファイルをバックアップします。

ステップ 2 セキュリティ アプライアンスで、**show logging** コマンドを使用して Syslog がディセーブルであることを確認します。Syslog サーバが接続をディセーブルにしている場合、ディスプレイに「disable」キーワードが表示されます。

ステップ 3 **no logging host** コマンドを使用して、Syslog サーバへのロギングをディセーブルにします。

```
no logging host dmz1 10.1.1.2
```

ステップ 4 **logging host** コマンドを使用して、ロギングを再起動します。

```
logging host dmz1 10.1.1.2 tcp/1468
```

ステップ 5 **show logging** コマンドを使用して、サーバがイネーブルになっていることを確認します。「disabled」キーワードが表示されていない必要があります。

セキュリティ アプライアンスのシステム ログ メッセージの検索に使用するシステム ログ メッセージ検索機能の設定

システム ログ メッセージは、日時、Syslog ID、および送信元と宛先の IP アドレスによって検索したりソートしたりできます。また、Advanced Option 機能を使用すると、ポート番号、サービス、およびインターフェイス名に基づいてシステム ログ メッセージを検索することもできます。この項の手順を使用する前に、必ずセキュリティ アプライアンス Syslog サーバをインストールしてください。セキュリティ アプライアンス Syslog サーバをインストールする方法の詳細については、次の URL にアクセスして参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a008021d772.html#wp3514

ここでは、次の項目について説明します。

セキュリティ アプライアンスのシステム ログ メッセージ検索画面の設定

この項では、セキュリティ アプライアンスのシステム ログ メッセージ検索画面の概要を示します。

セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションにアクセスするには、次の手順を実行します。

ステップ 1 デスクトップで PFSS Search.exe ショートカット アイコンをクリックします。セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションが開き、メイン ウィンドウが表示されます。

ステップ 2 View メニューで、**Select Column** を選択します。Select Columns ダイアログボックスが表示されます。

ステップ 3 このダイアログボックスで、適切なチェックボックスをオンにして、右側のウィンドウ ペインに選択したオプションのカラムを表示します。項目を昇順または降順でソートするには、任意のカラム ヘッダーをクリックします。

日時に基づくシステム ログ メッセージの検索

特定の日時に基づいてシステム ログ メッセージを検索するように設定できます。1 つの日付または時刻を指定することも、日時範囲を指定することもできます。

特定の日時に基づいてシステム ログ メッセージを検索するように設定するには、次の手順を実行します。

ステップ 1 デスクトップで **PFSS Search.exe** ショートカット アイコンをクリックします。セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションが開き、メイン ウィンドウが表示されます。

ステップ 2 **Date** チェックボックスをオンにし、**Between** フィールドおよび **And** フィールドのドロップダウンリストを使用して、1 つの日付または日付範囲を入力します。

ステップ 3 **Time** チェックボックスをオンにし、**Between** フィールドおよび **And** フィールドのドロップダウンリストを使用して、特定の時刻または時刻範囲を入力します。

ステップ 4 **Search Now** をクリックします。

システム ログ メッセージ ID に基づくシステム ログ メッセージの検索

特定のシステム ログ メッセージ ID に基づいてシステム ログ メッセージを検索できます。

特定のシステム ログ メッセージ ID に基づいてシステム ログ メッセージを検索するように設定するには、次の手順を実行します。

ステップ 1 デスクトップで **PFSS Search.exe** ショートカット アイコンをクリックします。セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションが開き、メイン ウィンドウが表示されます。

ステップ 2 Syslog ID フィールドに、検索するシステム ログ メッセージの ID を入力します。

ステップ 3 **Search Now** をクリックします。

IP アドレスに基づくシステム ログ メッセージの検索

特定の送信元 IP アドレスから特定の宛先アドレスへのシステム ログ メッセージを検索できます。検索する 1 つの IP アドレスまたはアドレス範囲を指定できます。

特定の送信元 IP アドレスから特定の宛先アドレスへのシステム ログ メッセージを検索するには、次の手順を実行します。

ステップ 1 デスクトップで **PFSS Search.exe** ショートカット アイコンをクリックします。セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションが開き、メイン ウィンドウが表示されます。

ステップ 2 **IP Address** をクリックします。左側の表示ペインに IP Address ダイアログボックスが開きます（IP Address の各フィールドを表示するために、スクロールする必要が生じることがあります）。

ステップ 3 検索基準として 1 つの IP アドレスを指定するには：

a. Source IP Address From フィールドに、1 つの IP アドレスを入力します。

b. Destination IP Address From フィールドに、同じ IP アドレスを入力します。

ステップ 4 検索基準として IP アドレスの範囲を指定するには：

a. Source IP Address From フィールドに、IP アドレス範囲の最小値を入力します。

b. Source IP Address To フィールドに、IP アドレス範囲の最大値を入力します。

c. Destination IP Address From フィールドに、IP アドレス範囲の最小値を入力します。

d. Destination IP Address To フィールドに、IP アドレス範囲の最大値を入力します。

ステップ 5 **Search Now** をクリックします。

Windows 監査イベントの検索

Event Viewer を使用して監査レコードを表示する方法については、『*Windows 2000 EAL 4 Administrator Guidance*』の「Audit Management」の項を参照してください。

Advanced Option 機能によるシステム ログ メッセージの検索

Advanced Option 機能を使用してシステム ログ メッセージを検索するように設定できます。Advanced Option 機能を使用すると、ポート番号、サービス、およびインターフェイス名に基づいてシステム ログ メッセージを検索できます。検索基準として 1 つのポートを指定することも、ポート範囲を指定することもできます。

Advanced Option 機能を使用してシステム ログ メッセージを検索するには、次の手順を実行します。

ステップ 1 デスクトップで **PFSS Search.exe** ショートカット アイコンをクリックします。セキュリティ アプライアンスのシステム ログ メッセージ検索アプリケーションが開き、メイン ウィンドウが表示されます。

ステップ 2 **Advanced Options** をクリックします。左側の表示ペインに Advanced Options ダイアログボックスが開きます（Advanced Options の各フィールドを表示するために、左側のペインをスクロールする必要が生じることがあります）。

ステップ 3 検索基準として 1 つのポートを指定するには、Port No フィールドに 1 つのポート番号を入力します。

ステップ 4 検索基準としてポートの範囲を指定するには：

a. 左側の Port No フィールド（— で区切られている）に、ポート範囲の最小値を入力します。

b. 右側の Port No フィールドに、ポート範囲の最大値を入力します。

c. **Search Now** をクリックします。

ステップ 5 検索基準としてサービス名を指定するには：

a. Services フィールドにサービス名を入力します。

b. **Search Now** をクリックします。

ステップ 6 検索基準としてインターフェイス名を指定するには：

a. Interface Name フィールドに、インターフェイス名を入力します。

b. **Search Now** をクリックします。

PIX Firewall Syslog Server（PFSS）に関するガイダンス

インストール手順

PFSS をインストールするには、次の手順を実行します。

ステップ 1 実行ファイル **pfss<ver>.exe**（<ver> は PFSS のバージョン番号）をダブルクリックします。

ステップ 2 **Yes** をクリックします。セットアップが起動します。

ステップ 3 Welcome ウィンドウで、**Next** をクリックします。ログ ファイルの宛先ディレクトリを選択すると、ログ ファイルの格納先となるファイル システムが NTFS であるかどうかが確認されます。NTFS でない場合は、セットアップが終了します。NTFS である場合は、セットアップが続行します。このサービスがすでにインストールされていることが検出された場合は、すでにインストールされているサービスをアンインストールするかどうか尋ねられます。

ステップ 4 プログラムの格納先とログ ファイルの宛先フォルダを選択した後、TCP Syslog サーバおよび UDP Syslog サーバのポート番号を選択する必要があります。デフォルト値は次のとおりです。

TCP PORT = 1470

UDP PORT = 514

（注） 1024 より大きく 65536 より小さいポート番号を入力する必要があります。

ステップ 5 最後のウィンドウでは、% Disk Full、Disk Empty Watch、および Disk Full Watch の値を入力するように求められます。次の説明を参照してください。

% Disk Full : ディスク使用率が何パーセントになったときに、Syslog サーバを停止させるか（デフォルトは 90%）。

Disk Empty Watch ：ディスクがまだ空いているときに、ディスクがいっぱいになっていないかどうかをディスク モニタに確認させる間隔（秒数。デフォルトは 5 秒です）。

Disk Full Watch : ディスクがまだいっぱいであるときに、ディスクが空いていないかどうかをディスク モニタに確認させる間隔（秒数。デフォルトは 3 秒です）。

ステップ 6 これで、セットアップが完了し、サービスが開始されます。サービスを停止または一時停止するには、コントロール パネルに移動して、**Services** をクリックします。PIX Firewall Syslog Server を探し、目的のサービスのボタンをクリックします。

ステップ 7 パラメータ（% Disk Full など）を変更するには、サービス パネルに移動して、目的のパラメータを入力します。

-d <% Disk Full >

-t <TCP PORT >

-u <UDP PORT>

-e <Disk Empty Watch >

-f <Disk Full Watch >

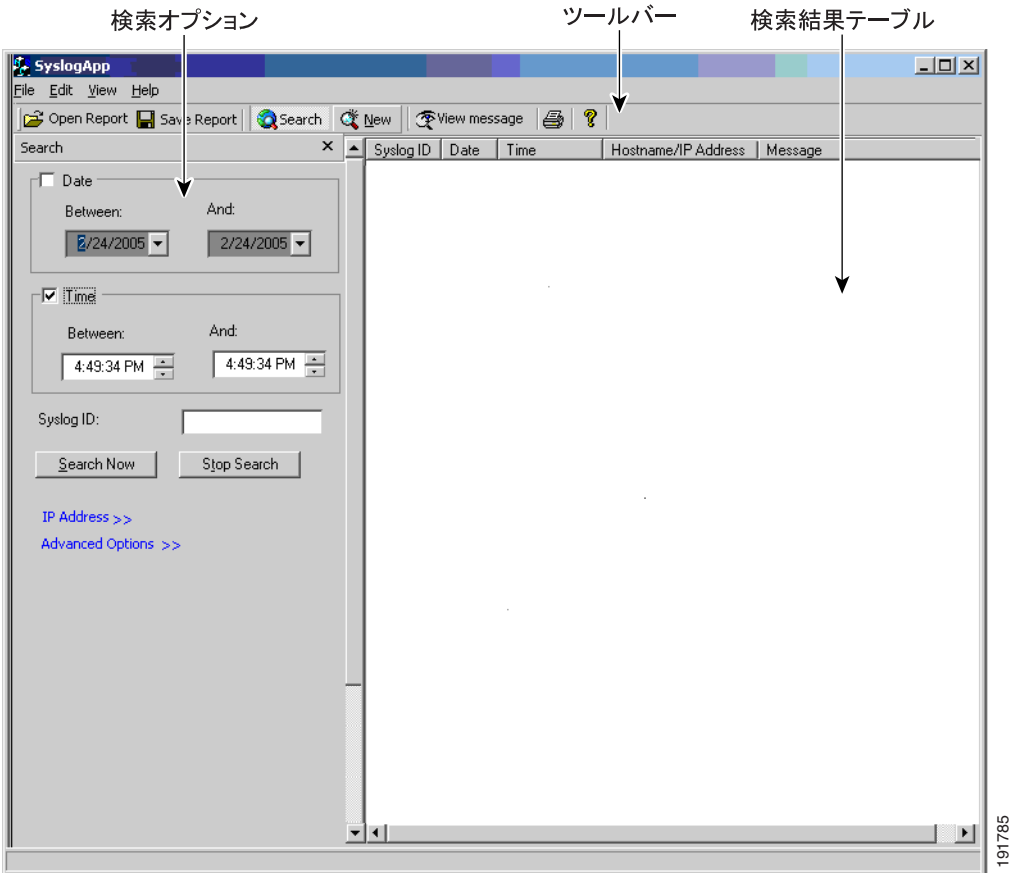
たとえば、% Disk Full を %35 に、TCP PORT を 1470 に設定するには、**-d 35 t 1470** と入力します。

使用方法

PFSS は、実行アプリケーションにバンドルされており、格納されているシステム ログ メッセージ レコードの検索とソートを行います。このアプリケーションのショートカットは、デスクトップと、既存の PFSS プログラム フォルダに作成されます。この検索 / ソート アプリケーションからログ ファイルに変更を加えることはできません。

PFSS 検索 / ソート アプリケーションを起動するには、デスクトップまたはプログラム フォルダにあるショートカットをクリックします。初期画面は、次の 3 つの部分に分かれています。

- ツールバー
- 検索オプション
- 検索結果テーブル



ツールバーのボタン

ツールバーには、次のボタンが用意されています。

- Open Report
- Save Report
- Search
- New
- View message
- Print

Open Report をクリックすると、すでに格納されているレポート ファイルを表示できます。

Save Report をクリックすると、次の 2 つの形式のいずれかで検索結果を保存できます。

- *.PFSS
- *.txt

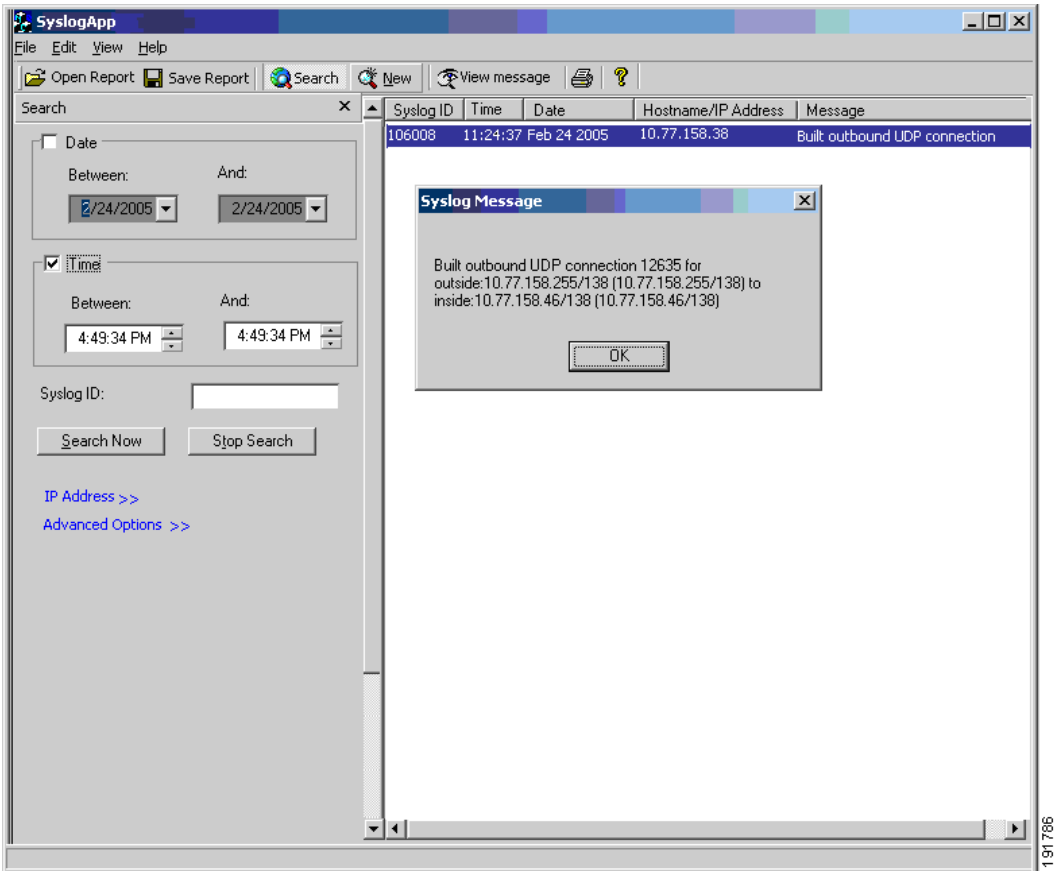
.PFSS 形式では、フィールド間にデリミタ（$）が存在します。このアプリケーションからこのファイルを開くと、検索結果テーブルにメッセージが表示されます。

*.txt 形式の場合、格納されたシステム ログ メッセージ情報はテキスト ビューアに表示されます。

Search をクリックすると、検索オプション ペインを開くまたは閉じることができます。検索ペインは、**View > Search** を選択してイネーブルにすることもできます。

New をクリックすると、既存の検索値をクリアし、検索フィールドをデフォルト値に設定できます。**Edit > New Search** を選択して、新しい検索を実行することもできます。

メッセージを選択して **View message** をクリックすると、検索テーブルにメッセージを表示できます。行をダブルクリックして、システム ログ メッセージを表示することもできます。次の図を参照してください。



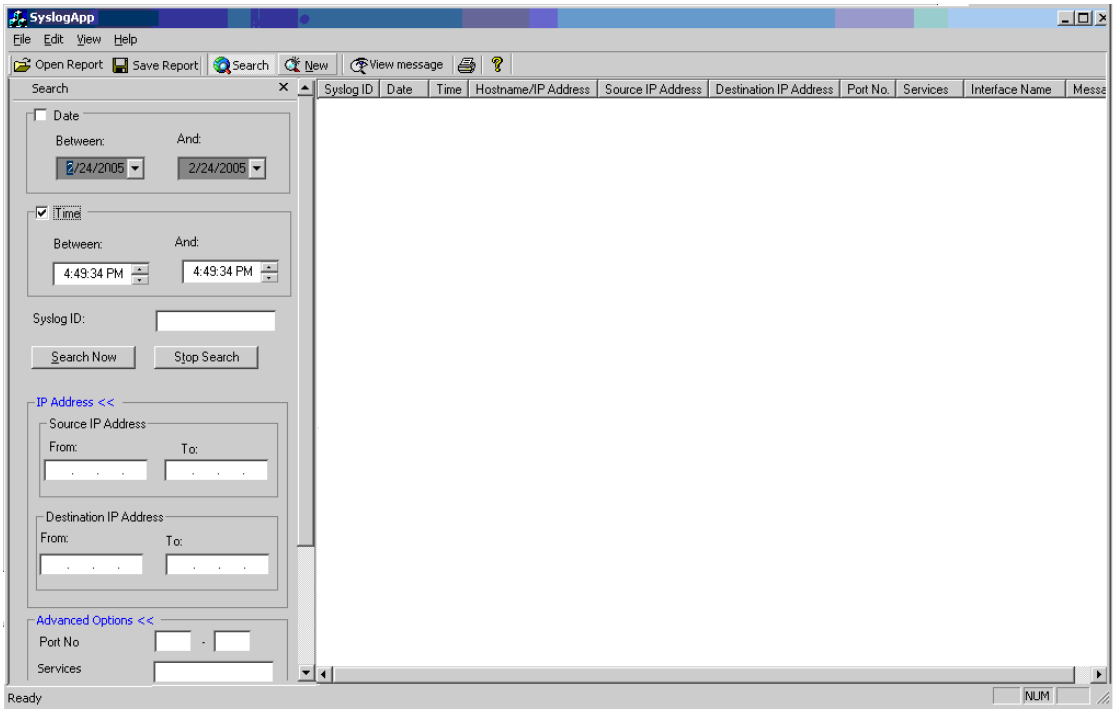
検索ペインのフィールド

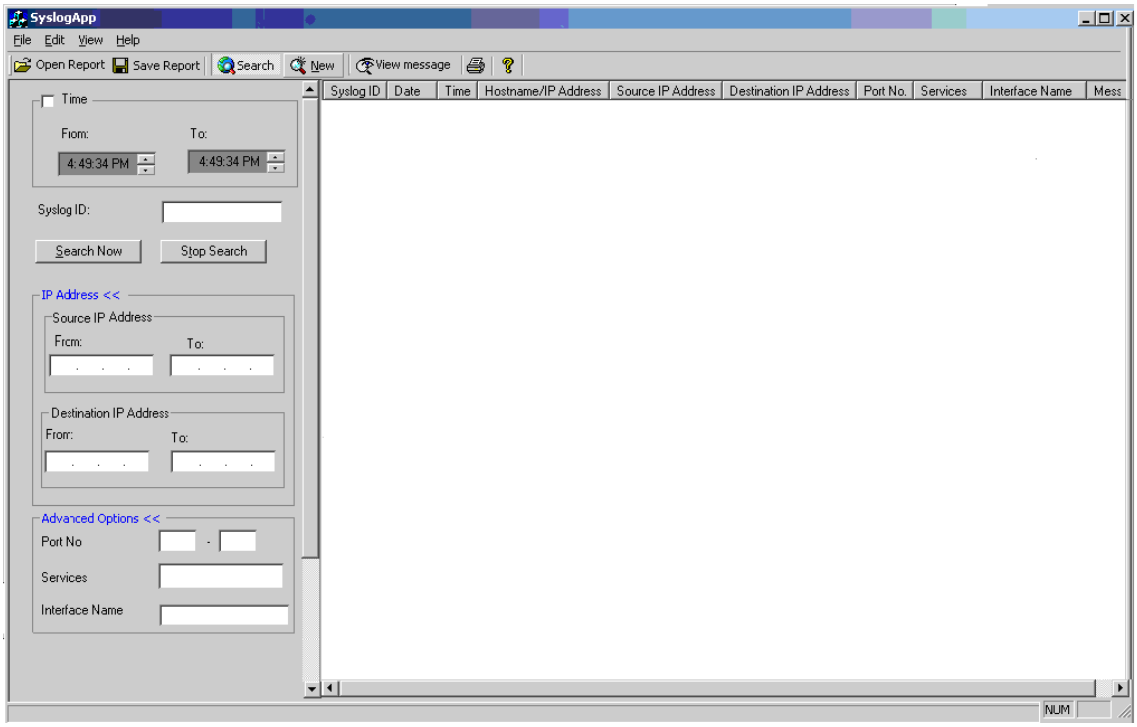
検索ペインには、選択可能な次のオプションが表示されます。

- Date
- Time
- Syslog ID
- IP Address
- Advanced Options

範囲を選択できる Date フィールドと Time フィールド、および Syslog ID フィールドは、最もよく使用されます。これらのオプションは、デフォルトでイネーブルになっています。他の 2 つのフィールドは、デフォルトでディセーブルになっています。

検索ペインで **IP Address** または **Advanced Options** をクリックすると、送信元 IP アドレスと宛先 IP アドレス、またはサービスとポートをイネーブルまたはディセーブルにすることができます。次の各図は、検索オプションの完全なビューを示しています。


SyslogApp
File Edit View Help
Open Report
Save Report
Search
New
View message
Search
Date
Between:
And:
2/24/2005
2/24/2005
Time
Between:
And:
4:49:34 PM
4:49:34 PM
Syslog ID:
Search Now
Stop Search
IP Address <<
Source IP Address
From:
To:
Destination IP Address
From:
To:
Advanced Options <<
Port No
Services
Syslog ID
Date
Time
Hostname/IP Address
Source IP Address
Destination IP Address
Port No.
Services
Interface Name
Ready
NUM
191787


SyslogApp
File Edit View Help
Open Report
Save Report
Search
New
View message
Time
From:
To:
4:49:34 PM
4:49:34 PM
Syslog ID:
Search Now
Stop Search
IP Address <<
Source IP Address
From:
To:
Destination IP Address
From:
To:
Advanced Options <<
Port No
Services
Interface Name
Syslog ID
Date
Time
Hostname/IP Address
Source IP Address
Destination IP Address
Port No.
Services
Interface Name
NUM
191788

検索結果

検索結果ペインには、検索条件を満たすシステム ログ メッセージが表示されます。次の情報が表示されます。

- Syslog ID
- Date
- Time
- Hostname/IP Address
- Message

さらに、**View > Select Column** を選択して、検索結果の次のカラムを選択できます。オプションのカラムは次のとおりです。

- Source IP Address
- Destination IP Address
- Services
- Port
- Interface Name

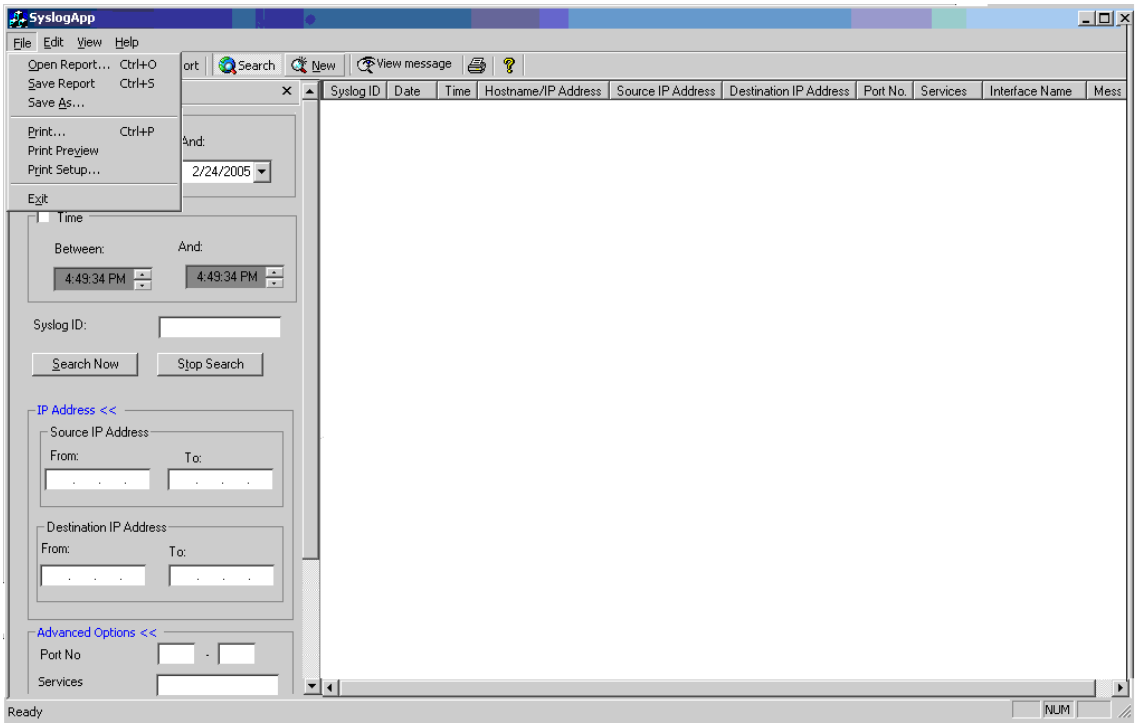
カラム ヘッダーをクリックして、カラムをソートできます。たとえば、Syslog ID でソートするには、検索結果ペインで **Syslog ID** カラム ヘッダーをクリックします。

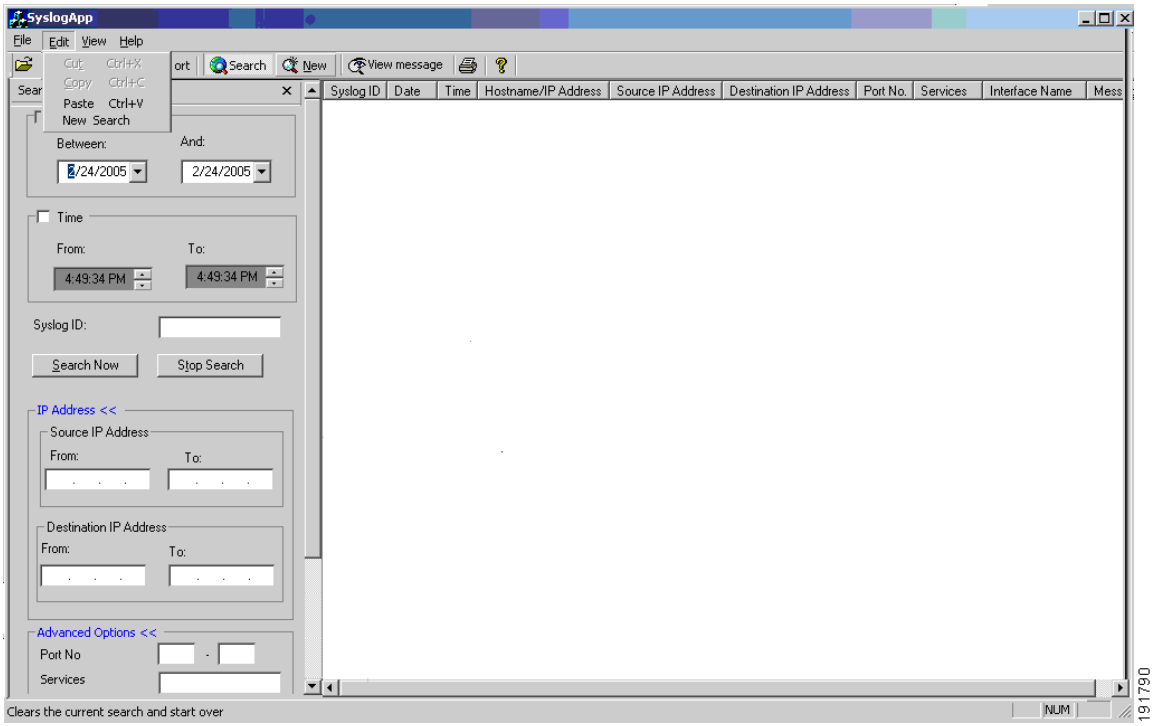
検索 / ソートのメニュー

File メニューでは、検索結果レポートを開く、保存する、および印刷することができます。

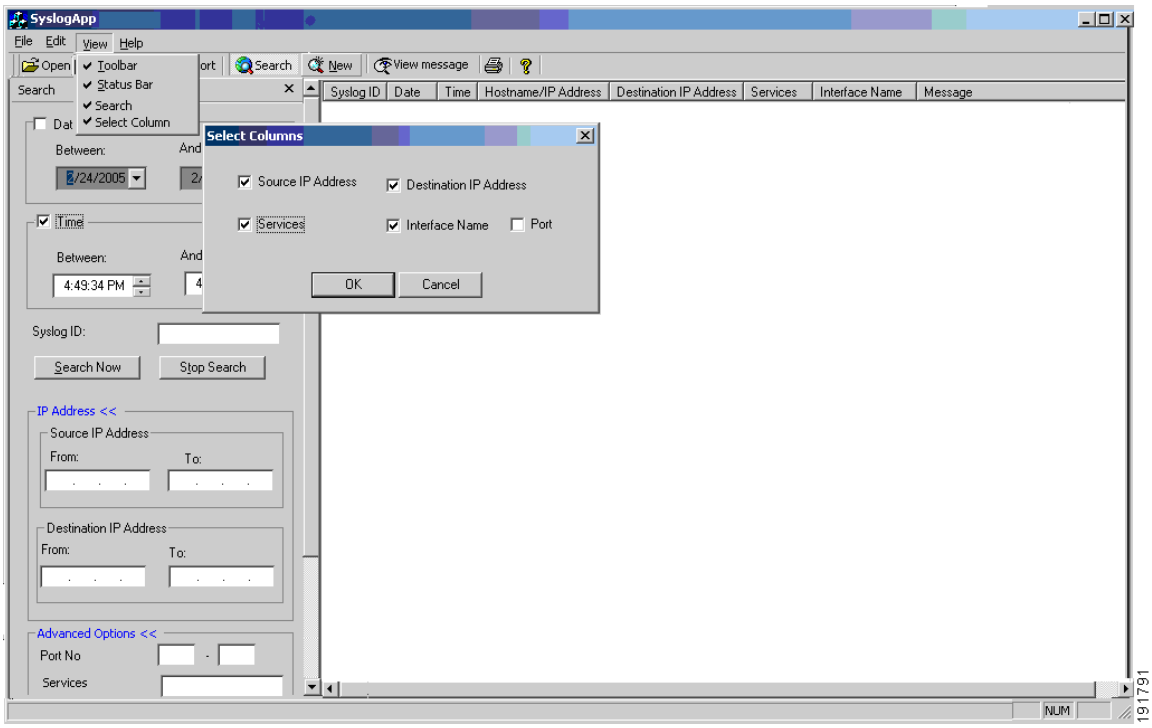
Edit メニューでは、テキストを切り取る、コピーする、および貼り付けることができます。

New Search をクリックすると、現在の検索フィールドをクリアできます。





View メニューでは、ツールバー、ステータス バー、検索、およびカラム選択をアクティブにすることができます。Select Columns オプションは、検索結果のカスタマイズに使用します。検索結果のすべてのオプションをカスタマイズできるわけではありません。システム ID、日付、時刻、ホスト名 /IP アドレス、およびシステム ログ メッセージの各フィールドは、必ず表示されます。Select Columns を選択して、送信元 IP アドレス、宛先 IP アドレス、ポート、サービス、およびインターフェイス名の各フィールドをイネーブルまたはディセーブルにすることができます。次の図を参照してください。



PIX Firewall Syslog Server 5.1(2) のリリース ノート

- PFSS は、現在、Windows 2000 Service Pack 3、Windows NT 4.0 Service Pack 6、および Windows XP Professional Service Pack 1 でサポートされています。
- PFSS のインストールおよびアンインストールには、管理特権を持つアカウントが必要です（CSCdz04526）。非管理特権でこのような操作を試行すると、システムが不安定な状態になることがあります。
- PFSS アプリケーションは、FAT ファイル システムまたは NTFS ファイル システムにインストールできます。ただし、ログ ファイルのディレクトリは、ローカルの NTFS ファイル システム上に存在する必要があります。インストール中に、ログ ファイルを FAT ファイル システムに保存しようとすると、警告が出され、インストール プログラムが終了します。FAT ファイル システムを NTFS に変換するには、DOS プロンプトから変換プログラムを使用します。

PIX Firewall Syslog Server 5.1(1) のリリース ノート

5.1(1) では、バグ CSCdp45416 に基づいて、PFSS に 2 つの変更が加えられています。

- PFSS が、ログ ファイル名を変更するときに、ファイルの作成日ではなく変更日を使用するようになりました。
- バックアップ ディレクトリがログ ファイル ディレクトリ内に作成されるようになりました。バックアップ ディレクトリには、名前変更後の <day>.mmddyy ファイルが存在します。

セキュリティ アプライアンスの MD5 ハッシュ値

MD5 ファイル検証機能を使用すると、シャーシに格納されている適応型セキュリティ アプライアンスのイメージの MD5 ハッシュを生成し、Cisco.com に掲載されている値と比較して、シャーシ上のイメージが破損していないことを確認できます。

Cisco.com のソフトウェア センターからシステム イメージの MD5 値を入手できます。また、イメージ ファイルの転送後に、次のコマンドを入力してチェックできます。

[**message-digest-key** *key_id* **md5** *key*]

このコマンドは、Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。

MD5 値の不一致は、イメージが破損していることを意味します。

技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここには、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。
本書とあわせてご利用ください。

Cisco.com 日本語サイト
http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

シスコシステムズマニュアルセンター
http://www2.hipri.com/cisco/

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合せください。

シスコシステムズ合同会社
〒 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
0120-933-122（通話料無料）、03-6670-2992（携帯電話、PHS）
電話受付時間 ： 平日 10:00 ～ 12:00、13:00 ～ 17:00

OL-12987-01-J