CHAPTER 12

ネットワーク スキャンの設定

（注） **Nessus ベースのネットワーク スキャン機能は、UNIX オペレーティング システムベースのクライアント マシンを経由して Cisco NAC アプライアンス ネットワークにアクセスするユーザにのみ適用されます。Cisco NAC Agent は、Nessus ベースのネットワーク スキャンをサポートしていません。**

この章では、Cisco NAC アプライアンスのネットワーク スキャンの設定方法について説明します。次の内容について説明します。

概要

Cisco NAC アプライアンスのネットワーク スキャナは、セキュリティの脆弱性の検査に Nessus プラグインを使用しています。Cisco NAC アプライアンスでは、スキャン結果に対する即座の自動対応を設定できます。たとえば、脆弱性が発見された場合、そのユーザに対し、通知、ネットワークからのブロック、または Quarantine（検疫）ロールへの割り当てを実行できます。

セキュリティ関連ソフトウェアのオープン ソース プロジェクトである Nessus（http://www.nessus.org）は、ネットワークの特定の脆弱性テスト用に設計したプラグインを提供しています。特定のワームの存在をリモートから検出するプラグインだけでなく、ピアツーピアのソフトウェア アクティビティまたは Web サーバを検出するためのプラグインもあります。Nessus プラグインの説明は次のとおりです。

> *Nessus プラグインは、一般的なウイルス スキャナ アプリケーションのウイルス シグニチャときわめて類似しています。各プラグインは、特定の脆弱性をテストするように作成されています。これには、実際に脆弱性を利用するように設計されたものもあれば、単に既知の脆弱なソフトウェア*

バージョンかどうかをテストするだけのものもあります。プラグインはほとんどの言語で作成できますが、通常は、Nessus Attack Scripting Language（NASL）で作成されます。NASL は Nessus 独自の言語であり、特に脆弱性テスト開発用に設計されたものです。各プラグインは、既知の特定の脆弱性、または業界の最良の方法、またはその両方をテストできるように設計されます。NASL プラグインは通常、対象に特定のコードを送信し、保存されている脆弱性の値と結果を比較する方法でテストを実行します。

— Anderson, Harry 著『Introduction to Nessus』（2003/10/28）
http://www.securityfocus.com/infocus/1741(2004/10/29)

（注）　Cisco NAC アプライアンスでは、Nessus プラグインの起動のみをサポートし、Nessus プラグイン自体はサポートしません。

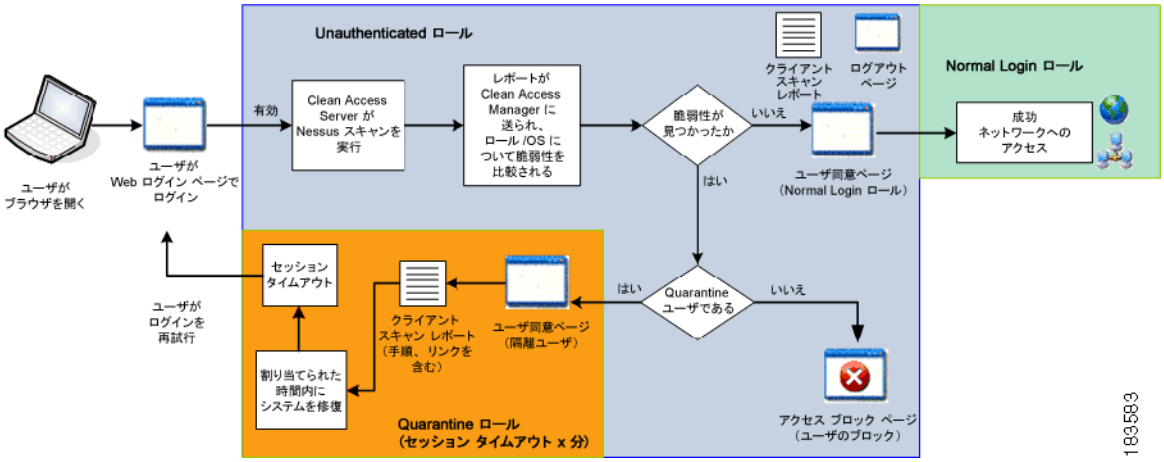
Cisco NAC アプライアンスでは、標準的なほとんどの Nessus プラグインを使用できます。また、プラグインをカスタマイズしたり、NASL を使用して独自のプラグインを作成することもできます。NASL を使用したプラグインの作成方法については、Nessus Web サイトを参照してください。

スキャンが実行されると、選択したプラグインに従ってネットワーク スキャナがクライアント システムをスキャンし、スキャン結果の標準レポートを生成して、Clean Access Manager に提出します。ネットワーク スキャン レポートには、そのプラグインによってセキュリティ ホールの有無、警告、またはシステム情報が示されます（Nessus プラグインの設計に従ってです）。Clean Access Manager は、設定されている脆弱性定義とプラグインの結果を比較して、レポートを解釈します。脆弱性として設定されている結果とレポートの結果が一致すれば、[Monitoring] > [Event Logs] > [View Logs] にそのイベントが記録されます。そのほかに設定できるオプションは、次のとおりです。

- ユーザにスキャン結果を表示する。
- ネットワークからユーザをブロックする。
- そのユーザを Quarantine ロールにして、クライアント システムが修正されるまで、アクセスを制限する。
- 脆弱性についてユーザに警告する（ユーザ同意ページを使用）。

図 12-1 は、Web ログインを通じたユーザ認証時の全般的なネットワーク スキャンのクライアント評価プロセスを示しています。あるユーザ ロールに対して、Agent とネットワーク スキャンが両方イネーブルに設定されている場合には、ユーザは図 10-1（P.10-2）のプロセス後に、図 12-1 のネットワーク スキャンに進みます。この場合、Agent ダイアログにユーザ情報が表示されます（適用できる場合）。

図 12-1　　ネットワーク スキャンのクライアント評価



ネットワーク スキャンの設定手順

次の各項で、ネットワーク スキャンの設定に必要な手順を説明します。

ステップ 1　「Quarantine ロールの設定」（P.12-6）
ステップ 2　「Clean Access Manager のリポジトリへの Nessus プラグインのロード」（P.12-6）
ステップ 3　「[General Setup] ページでの設定」（P.12-9）
ステップ 4　「プラグインの適用」（P.12-10）
ステップ 5　「プラグイン オプションの設定」（P.12-13）
ステップ 6　「脆弱性の処理の設定」（P.12-14）
ステップ 7　「スキャンのテスト」（P.12-16）
ステップ 8　「ユーザ同意ページのカスタマイズ」（P.12-20）
ステップ 9　「スキャン レポートの表示」（P.12-18）

ユーザ ページの概要

ログインと Nessus スキャンのプロセス中にユーザに表示される Web ページ、および Web 管理コンソールで設定するリストについて、表 12-1 に概要を示します。

表 12-1　ユーザ ページの概要

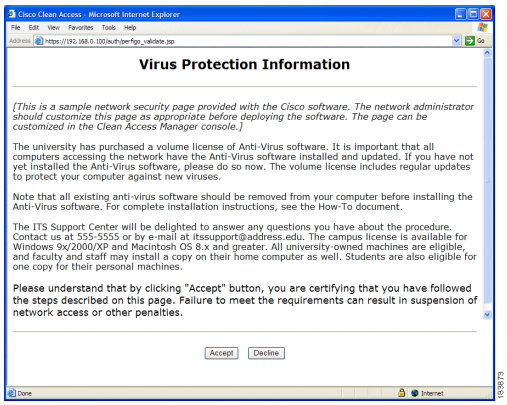
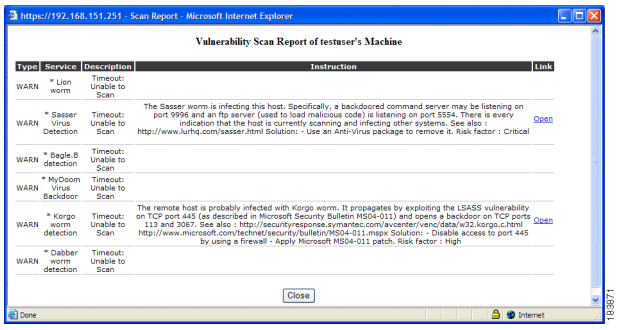
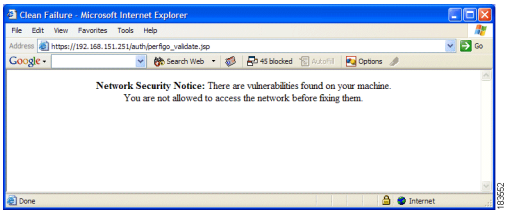
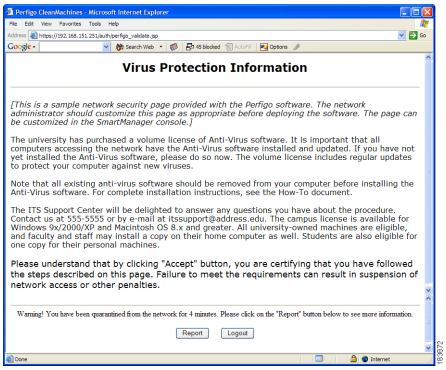
ページ	設定場所	目的
Web ログイン/ネットワーク スキャナ ユーザ ページ		
ネットワーク スキャン ユーザ同意ページ	イネーブルに設定： [Device Management] > [Clean Access] > [General Setup] > [Web Login] 設定ページ： [Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [User Agreement] 「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。	このページをイネーブルに設定すると、Web ログイン ユーザに対して、認証およびネットワーク スキャン合格後にこのページが表示されます。ネットワークにアクセスするためには、ユーザは [Accept] ボタンをクリックしなければなりません。 
脆弱性スキャン レポート	イネーブルに設定： [Device Management] > [Clean Access] > [General Setup] > [Web Login] 設定ページ： [Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [Vulnerabilities] 「脆弱性の処理の設定」（P.12-14）を参照してください。	イネーブルに設定すると、ネットワーク スキャンによって脆弱性が発見された場合、Web ログイン ユーザに、このクライアント レポートが表示されます。ログアウト ページにも、このレポートへのリンクが表示されます。管理者は、[Device Management] > [Clean Access] > [Network Scanner] > [Reports] から、このクライアント レポートの管理バージョンを表示できます。ネットワーク スキャンで脆弱性が発見された Agent ユーザに対して、Agent ダイアログの一部としてこの情報が表示されます。レポートは次のように表示されます。 

表 12-1　ユーザ ページの概要 （続き）

ページ	設定場所	目的
アクセス ブロック ページ	[Device Management] > [Clean Access] > [General Setup] > [Web Login] 「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。	イネーブルに設定すると、ネットワーク スキャンによってクライアント システムに脆弱性が発見され、ネットワークからブロックされる場合に、Web ログイン ユーザに対してこのページが表示されます。 
ユーザ同意ページ：隔離ユーザ、オリジナル ロール	イネーブルに設定： [Device Management] > [Clean Access] > [General Setup] > [Web Login] 設定ページ： [Network Scanner] > [Scan Setup] > [User Agreement] [Normal Login] ロールを選択します。 「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。	イネーブルに設定すると、ネットワーク スキャンによってクライアント システムに脆弱性が発見されて隔離される場合に、Web ログイン ユーザに対してこのページが表示されます。  このページには、Normal Login ロール用のユーザ同意ページと同じ [Information Page Message (or URL)] コンテンツ（「Virus Protection Information」）が表示されます。ただし、[Acknowledgment Instructions] にはオリジナル ロールのセッション タイムアウトがハードコードされていて、さらに、ボタン ラベルは、「**Report**」および「**Logout**」にハードコードされています。
ユーザ同意ページ： **隔離ユーザ、Quarantine ロール**	イネーブルに設定：[Device Management] > [Clean Access] > [General Setup] > [Web Login] 設定ページ：[Network Scanner] > [Scan Setup] > [User Agreement] 該当する [Quarantine] ロールを選択します。 「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。	イネーブルに設定すると、ネットワーク スキャンによってクライアント システムに脆弱性が発見されて隔離される場合に、Web ログイン ユーザに対してこのページが表示されます。 このページでは、Quarantine ロール専用のユーザ同意ページを指定できます（上述の Normal Login ロール用の Quarantine 版ユーザ同意ページを使用するのではありません）。[Acknowledgment Instructions] には Quarantine ロール用のセッション タイムアウトがハードコードされ、またボタン ラベルも「**Report**」および「**Logout**」にハードコードされています。

ロール別にユーザを特定のページまたは URL（Cisco NAC アプライアンス外の）にリダイレクトする場合の詳細については、「ローカル ユーザ アカウントの作成」（P.6-15）を参照してください。

Cisco NAC アプライアンスの設定に関するその他の情報については、「[General Setup] ページでの設定」（P.12-9）を参照してください。

エージェント条件の設定に関する詳細は、「Agent ベースのポスチャ評価の設定」（P.9-41）を参照してください。

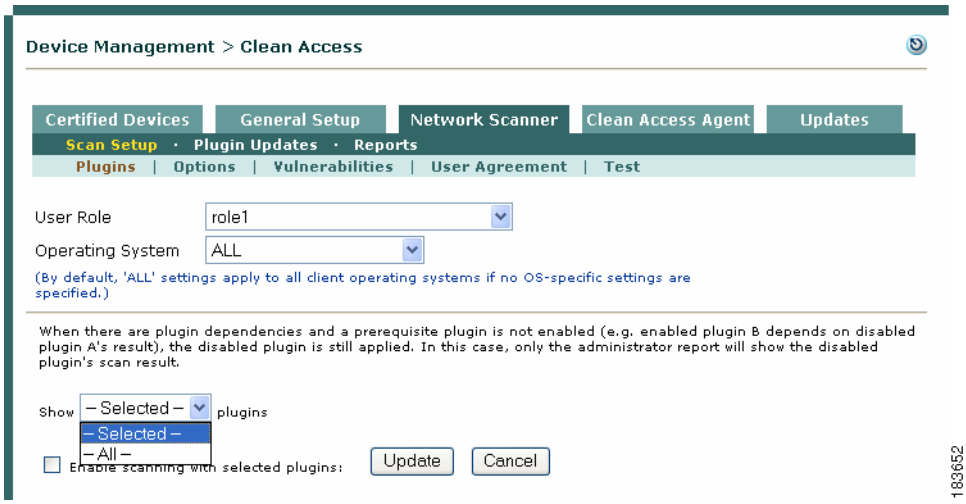
Quarantine ロールの設定

詳細については、「ネットワーク スキャン Quarantine ロールの設定」（P.8-24）を参照してください。

Clean Access Manager のリポジトリへの Nessus プラグインのロード

Clean Access Manager の最初のインストール時には、Nessus スキャン プラグイン リポジトリは空の状態です（図 12-2）。このリポジトリ内のプラグインは、[Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [Plugins] で表示されます。Nessus Web サイトからダウンロードしたプラグイン（連結された **plugins.tar.gz** ファイルまたは個々の .nasl ファイル）は、Clean Access Manager のプラグイン リポジトリに手動でロードできます。また、自分で作成した .nasl プラグインをロードすることもできます。

図 12-2　[Network Scanner] の [Plugins] ページ



（注）　Tenable のライセンス要件に制約されるため、シスコはテスト済みの Nessus プラグインまたは自動化したプラグイン アップデートを、有効なリリース 3.3.6/3.4.1 である Cisco NAC アプライアンスに組み込みできません。しかし、お客さまは Nessus プラグインを選択して手動でダウンロードできます。サイトは http://www.nessus.org です。
Nessus プラグインのフィードに関する詳細は、http://www.nessus.org/plugins/index.php?view=feed を参照してください。
手動でアップロードしたプラグインの簡便なデバッグ方法については、「ログの表示」（P.12-17）を参照してください。

（注）　ほとんどの Nessus 2.2 プラグインは Clean Access Manager でサポートされておりアップロードできます。Nessus 2.2 を入手するには、http://www.nessus.org/plugins/index.php?view=register から登録する必要があります。登録後、無償のプラグインをダウンロードできます。Nessus バージョン 2.2.7 の NASL_LEVEL 値は、3004 未満です。Cisco NAC アプライアンスは、NASL_LEVEL が 3004 以上であることを要求される Nessus プラグインをサポートしません。現在、Cisco NAC アプライアンスは Nessus バージョン 3.0 以降のプラグインをサポートしていません。

追加するプラグインに従属するプラグインがある場合は、それらのプラグインもロードする必要があります。ロードしない場合、プラグインは適用されません。プラグインをカスタマイズする場合は、Nessus アップデート セットのプラグインで上書きされないようにするため、プラグインに固有の名前を付けることを推奨します。

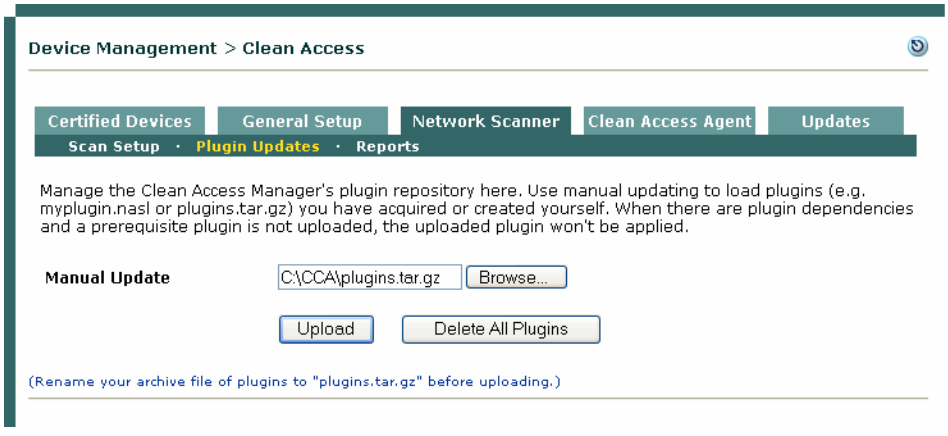
プラグインの説明は、[Scan Setup] サブメニューの [Plugins] フォームに表示されます（図 12-4 (P.12-8)）。プラグインの説明をカスタマイズして、管理コンソール ユーザがプラグイン セット内の他のプラグインから区別できるようにすることもできます。

ロードしたプラグインは、Clean Access Manager のリポジトリから実際にスキャンを実行する Clean Access Server に自動的に発行されます。CAM は、Clean Access Server 内のプラグイン セットのバージョンが CAM 内のバージョンと異なっている場合、CAS の起動時にプラグイン セットを CAS に配布します。

プラグインのアップロード

1. [Device Management] > [Clean Access] > [Network Scanner] > [Plugin Updates] の順に進みます。

図 12-3　[Plugin Updates] 画面

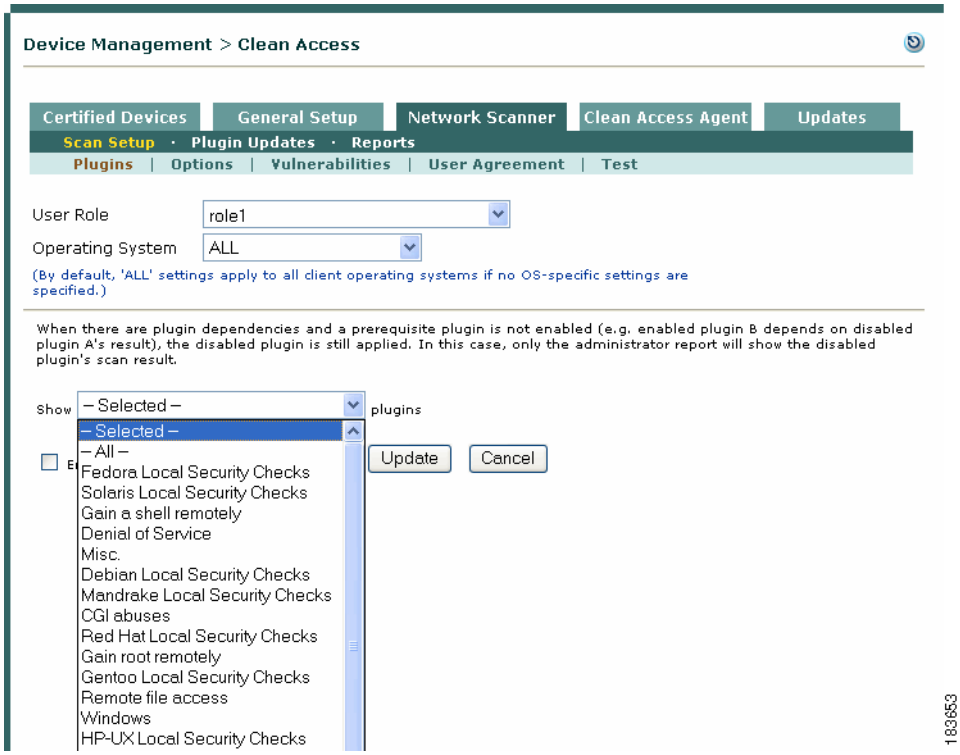


2. 使用中のコンピュータでアクセス可能なロケーションにプラグイン ファイルがあれば、[Manual Update] フィールドの横にある [Browse] ボタンをクリックし、プラグイン アーカイブ ファイル（**plugins.tar.gz**）または個々のプラグイン ファイル（**myplugin.nasl**）を探します。

（注）　アップロードされている Nessus プラグイン アーカイブのファイル名は、**plugins.tar.gz** でなければなりません。ほとんどの Nessus 2.2 プラグインがサポートされています。Nessus バージョン 2.2.7 の NASL_LEVEL 値は、3004 未満です。Cisco NAC アプライアンスは、NASL_LEVEL が 3004 以上であることを要求される Nessus プラグインをサポートしません。現在、ベンダー ライセンス上の制約から、Cisco NAC アプライアンスは Nessus バージョン 3 プラグインをサポートしていません。

3. [Upload] をクリックします。
4. リポジトリにロードされているプラグインのリストは、[Network Scanner] > [Scan Setup] > [Plugins] に表示されます（図 12-4）。

図 12-4　アップロード後の [Plugins] ページ



（注）　[Plugins] ページのデフォルト表示は [Selected] です。そのユーザ ロールに対して、Nessus プラグインの確認と更新がまだ実行されていなければ、デフォルト（Selected Plugins）では、プラグインは表示されません。アップロードしたプラグインを表示するには、[Show...Plugins] のドロップダウンから、その他の表示（「All」、「Backdoors」など）のうち 1 つを選択する必要があります。

5. [Upload] をクリックしてもすぐにプラグインが表示されない場合は、[Delete All Plugins] をクリックしてから、再度アップロードを実行してください。
6. プラグインを適用し、次の項の説明に従ってプラグインのパラメータを設定します。
   - 「プラグインの適用」（P.12-10）
   - 「脆弱性の処理の設定」（P.12-14）

（注）　プラグインに依存関係があり、前提となるプラグインがアップロードされていない場合は、プラグインをアップロードしても表示されません。

プラグインの削除

1. [Device Management] > [Clean Access] > [Network Scanner] > [Plugin Updates] の順に進みます。
2. リポジトリからすべてのプラグインを削除する場合は、[Delete All Plugins] ボタンをクリックします。[Network Scanner] > [Scan Setup] > [Plugins] ページに、プラグインが表示されなくなります。

[General Setup] ページでの設定

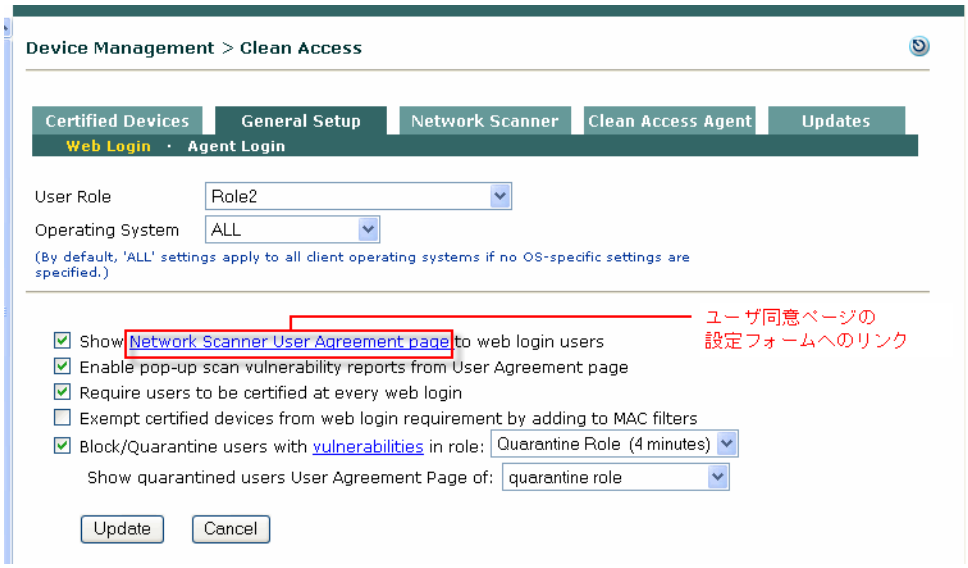
スキャン プラグインをロードしたら、ユーザ ロール別および OS 別にスキャンを設定できます。作業をはじめる前に、ご使用の環境に適したユーザ ロールが作成されていることを確認してください。

[General Setup] ページには、一般的な設定オプションがあり、ユーザ同意ページとスキャン レポートのどちらを表示するか、脆弱性が発見された場合にクライアントをブロックするか、隔離するかなど、ネットワーク スキャンに関する事項をユーザ ロール別および OS 別に設定できます。

ネットワーク スキャン ユーザ ページのオプションの設定手順

1. [Device Management] > [Clean Access] > [General Setup] > [Web Login] に移動します。

図 12-5　[General Setup] - [Web Login]



2. [User Role] のドロップダウンからスキャンを設定するロールを選択します。

3. 同様に、[Operating System] のドロップダウンから、その設定を適用する OS を選択します。設定は、あらゆるバージョンの OS プラットフォーム（WINDOWS_ALL など）に適用することも、また特定の OS バージョン（WINDOWS_XP）に適用することもできます。ALL の設定がクライアント システムに適用されるのは、そのユーザの OS の特定バージョンに対する設定がない場合です。

   特定のバージョンに設定を適用する場合は、OS を選択して、ALL 設定のチェックボックスをオフにします（たとえば、[Use 'ALL' settings for the WINDOWS OS family if no version-specific settings are specified] の選択を解除します）。

4. 次のネットワーク スキャン オプションをイネーブルにします。
   - Show Network Scanner User Agreement page to web login users
   - Enable pop-up scan vulnerability reports from User Agreement page
   - [Require users to be certified at every web login]：このオプションをイネーブルにすると、ログインのたびにクライアントに対してネットワーク スキャンが行われます（ディセーブルにすると、クライアントに対するスキャンは初回のログイン時だけになります）。
   - [Exempt certified devices from web login requirement by adding to MAC filters]：（任意）このオプションをイネーブルにすると、ネットワーク スキャン要件を満たしているユーザは、デバイス フィルタ リストにそれらのユーザのマシンの MAC アドレスを追加することで、Web ログインを完全にバイパスできます。
   - [Block/Quarantine users with vulnerabilities in role]：次のいずれかを選択します。

     ユーザを隔離する Quarantine ロールを選択する。

     ユーザをネットワークからブロックし、表示されるブロックされたアクセス ページの内容を変更する場合は、Block Access を選択する。

5. 完了したら、[Update] をクリックして、ユーザ ロールへの変更を保存します。

詳細については、「クライアント ログインの概要」（P.1-7）および「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。

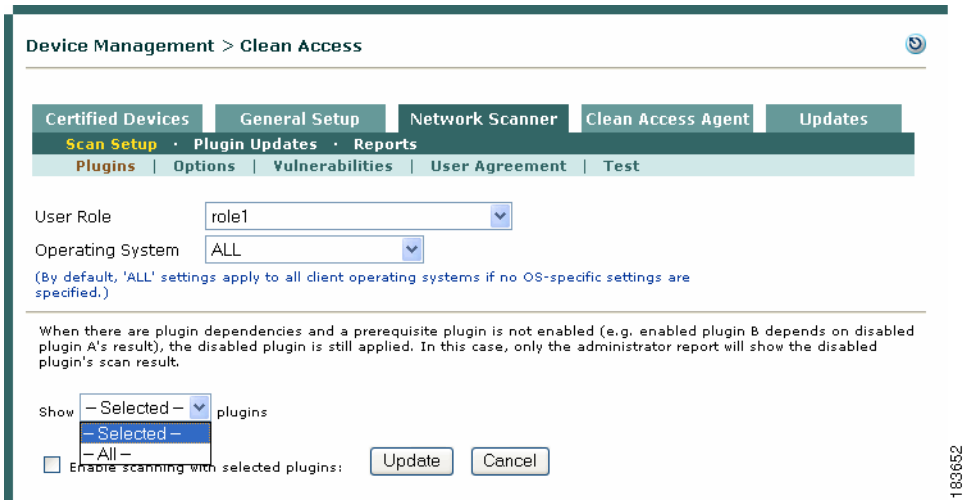
プラグインの適用

クライアントの脆弱性の判断に使用される Nessus プラグインを、[Plugins] ページから選択します。ユーザ ロールと OS を選択し、スキャンに加えるプラグインを選択します。

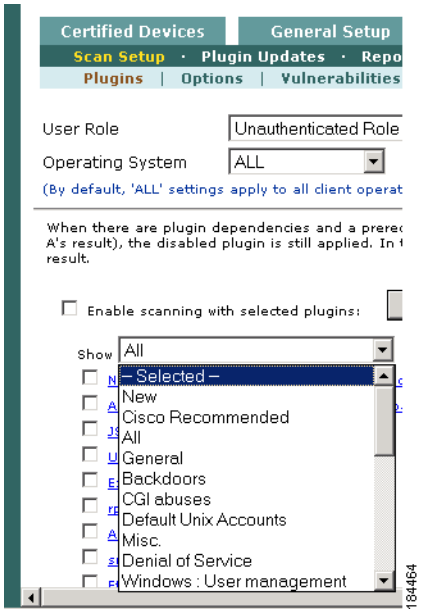
スキャン プラグインの適用手順

1. [Network Scanner] > [Scan Setup] > [Plugins] の順に進みます。

図 12-6　Plugins



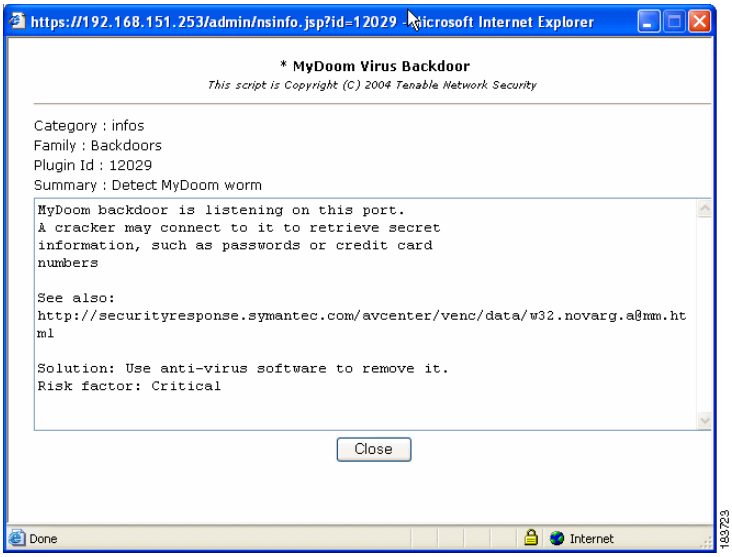
2. このフォームで、[User Role] と [Operating System] を選択し、[Enable scanning with Selected Plugins] チェックボックスをオンにします。
3. リポジトリに多くのプラグインがある場合、次の方法で、プラグイン リストからプラグイン ファミリを選択することにより、一度に表示されるプラグインを絞ることができます。
   - [All] を選択すると、リポジトリ内のすべてのプラグインが表示されます。
   - [- Selected-] を選択すると、そのロールに対して選択し、イネーブルにしたプラグインだけが表示されます。



（注）　Nessus プラグイン ページ（[Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [Plugins]）のデフォルトのビューは [Selected] です。そのユーザ ロールに対して、Nessus プラグインの確認と更新がまだ実行されていなければ、デフォルト（Selected Plugins）では、プラグインは表示されません。プラグインを選択するには、管理者が [Show...Plugins] のドロップダウンから、その他の表示（「All」、「Backdoors」など）のいずれかを選択する必要があります。

4. 詳細情報を見る場合は、プラグイン名をクリックします。各プラグインの情報ダイアログが表示されます（図 12-7）。

図 12-7　Nessus プラグインの説明



5. そのロールのスキャンに加える各プラグインのチェックボックスをオンにします。

（注）　そのプラグインがリポジトリ内の他のプラグインに従属している場合、これらのプラグインも自動的にイネーブルになります。

6. 完了したら、[Update] をクリックします。これによって、選択されたプラグインが [Vulnerabilities] ページに移動し、クライアント システムで脆弱性が発見された場合にどのように処理するかを設定できるようになります。

プラグインに設定可能なパラメータがある場合は、[Options] フォームを使用して、次の手順で設定できます。設定可能なパラメータがなければ、「脆弱性の処理の設定」（P.12-14）に進みます。

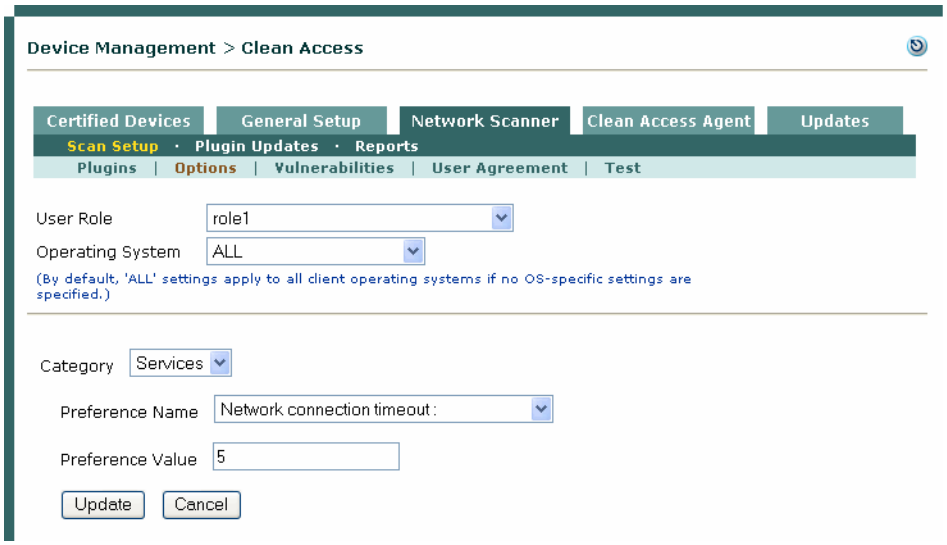
プラグイン オプションの設定

入力パラメータをサポートしているプラグインの場合は、[Options] フォームでパラメータを設定できます。作業を開始する前に、「プラグインの適用」（P.12-10）で説明したように、プラグインが [Plugins] フォームでイネーブルに設定されている必要があります。

プラグイン オプションの設定手順

1. [Network Scanner] タブで [Scan Setup] サブメニュー リンクをクリックして、[Options] フォームを開きます。
2. 適切なロールと OS を選択し、設定するプラグインを [Plugin] リストから選択します。リストには、イネーブルに設定されているすべてのプラグインが表示されます。
3. プラグインに設定するオプションをオプション リストから選択します。設定可能なオプションを選択すると、そのオプションに応じて、[Category]、[Preference Name]、および [Preference Value] のドロップダウンまたはテキストボックスが表示されます。設定できないパラメータの場合、「Not supported」というメッセージが表示されます。

図 12-8　　Options



4. ドロップダウン メニューから、[Category] と [Preference Name] を選択し、[Preference Value]（該当する場合）を入力して、[Update] をクリックします。設定するパラメータごとに [Update] をクリックする必要があります。

（注）　ホスト レジストリ検査には、Agent を使用することを推奨します。Nessus Windows レジストリ検査を使用するためには、検査対象となるすべてのマシン上に、レジストリへのアクセス権を持つ共有アカウントが必要です。これは [Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [Options] | [Category]: [Login configurations] | [Preference Name]: [SMB account/domain/password] で設定できます。Nessus 2.2 Windows レジストリ検査（資格情報を要求）についての詳細は、http://www.nessus.org/documentation/nessus_credential_checks.pdf を参照してください。

脆弱性の処理の設定

スキャンの対象外の脆弱性がユーザ システム上にある場合、そのユーザに対して、ネットワークからのブロック、隔離、または脆弱性に関する警告を行います。

ネットワーク スキャン レポートは、ユーザのログイン試行ごとに、[Device Management] > [Clean Access] > [Network Scanner] > [Reports] に表示されます。クライアント スキャン レポートをイネーブルにするには、[Device Management] > [Clean Access] > [General Setup] から、[Enable pop-up scan vulnerability reports from User Agreement page] オプションを選択します。

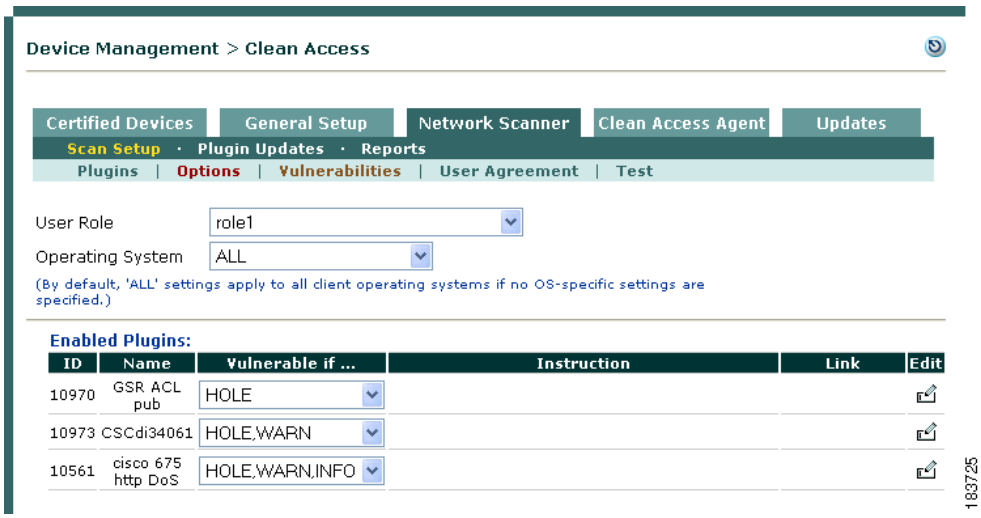
クライアント スキャン レポートをイネーブルにすると、脆弱性が発見された場合、ユーザに通知するためレポートがポップアップ ウィンドウに表示されます。このクライアント レポートはスキャン レポートの一部であり、脆弱性の結果およびユーザがその脆弱性を修復できるようにする手順または URL リンクだけが表示されます。ユーザのシステムでブラウザのポップアップがブロックされている場合は、ログアウト ページの [Scan Report] リンクをクリックすると、レポートを表示できます。脆弱性ごとにユーザに表示される警告テキストは、次の手順で設定できます。

通常、問題が発見されなければ、プラグインは結果を返しません。したがって、クライアントがネットワーク スキャンを受けて、脆弱性が発見されなければ、スキャン レポートは表示されません。

脆弱性処理の設定手順

1. [Network Scanner] > [Scan Setup] > [Vulnerabilities] フォームを開きます。
2. [User Role] と [Operating System] を選択します。選択したプラグインは、ユーザ ロールと OS の組み合わせに対して適用されます。そのロールのすべての OS に対して同じプラグイン集合が表示されます。ただし、どのプラグインを脆弱と判断するかは OS ごとにカスタマイズできます。

図 12-9　Vulnerabilities



3. イネーブルに設定されているプラグイン（[Plugins] メニューですでにイネーブルにされているプラグイン）について、次を選択します。

   [ID]：スキャン レポートにリストされるプラグインの番号。

   [Name]：プラグインの名前。

[Vulnerable if]：これらのドロップダウン オプションでは、プラグインのスキャン結果を Clean Access Manager がどのように解釈するかを設定します。クライアントのスキャンが実行され、返されたプラグイン結果が脆弱性の設定と一致していた場合、そのクライアントは Quarantine ロールを割り当てられます（またはブロックされます）。脆弱性をトリガーし、ユーザを Quarantine ロールに割り当てる結果レベルの高低を調節できます。

1. [NEVER]：プラグインについてのレポートを無視します。[HOLE]、[WARN]、[INFO] の結果がレポートに表示されても、このプラグインは脆弱であるとして処理されることも、ユーザが Quarantine ロールに割り当てられることもありません。
2. [HOLE]：プラグインの結果が [HOLE] の場合、クライアントには脆弱性があり、Quarantine ロールが割り当てられます。レポートの [WARN] または [INFO] という結果はこのプラグインの脆弱性とは見なされません。ほとんどの場合、管理者は脆弱性の設定として [HOLE] を選択する必要があります。[HOLE] を選択すると、プラグインによって他のタイプの情報が報告されても無視されます。
3. [HOLE, WARN]（タイムアウト）：この設定の意味は次のとおりです。

   プラグインの結果が [HOLE] なら脆弱と判断し、クライアントは Quarantine ロールになります。

   プラグインの結果が [WARN] の場合、脆弱と判断し、クライアントは Quarantine ロールになります。[WARN] という結果は、プラグインのスキャンが（パーソナル ファイアウォールまたはその他のソフトウェアによって）タイムアウトになり、そのマシン上でスキャンを実行できなかったという意味になります。脆弱性として [WARN] を選択すると、ファイアウォールがイネーブルになっているクライアントはすべて隔離されます。ただし、この設定は、スキャン結果が既知のものでなかった場合にクライアントを隔離する予防手段としても利用できます。

   レポートの結果が [INFO] の場合、このプラグインは脆弱とは判断しません。
4. [HOLE, WARN, INFO]：この設定の意味は次のとおりです。

   プラグインの結果が [HOLE] の場合、クライアントには脆弱性があり、Quarantine ロールが割り当てられます。

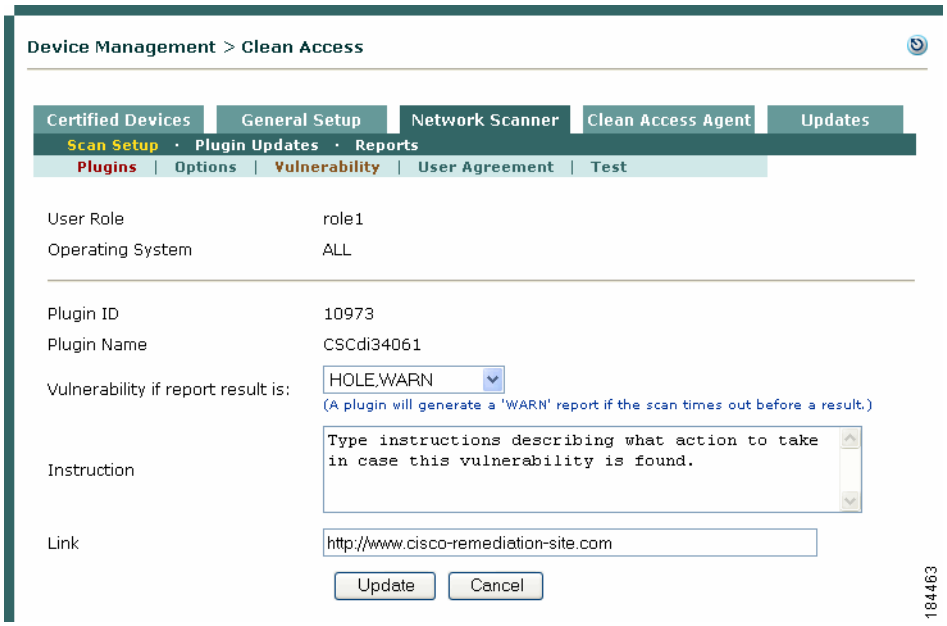
   プラグインの結果が [WARN] の場合、脆弱と判断し、クライアントは Quarantine ロールになります。[WARN] という結果は、通常、クライアントでファイアウォールがイネーブルになっていることを示します。

   レポートの結果が [INFO] の場合、脆弱と判断し、クライアントは Quarantine ロールになります。[INFO] の結果は、ポートで稼動しているサービス（Windows など）やそのマシンの NetBIOS 情報などのステータス情報を示します。このレベルの脆弱性を選択すると、ステータス情報が戻るすべてのクライアントが隔離されます。

（注） このプラグインが [INFO] の結果を返さない場合（[HOLE] または [WARN] の結果もない場合）、クライアントは隔離されません。

5. プラグインの設定を変更するには、設定するプラグインの横にある [Edit] ボタンをクリックします。
6. [Edit Vulnerabilities] フォームが表示されます。

図 12-10　Edit Vulnerability



7. [Vulnerability if report result is:] オプション メニューでは、このプラグインで報告され、ユーザに Quarantine ロールを割り当てる脆弱性のレベルを変更できます。
8. [Instruction] テキスト フィールドには、このプラグインが脆弱性を発見した場合にユーザに表示されるポップアップ ウィンドウの通知メッセージを入力します。
9. [Link] フィールドには、システムを修正するためにユーザがアクセスできる URL を入力します。この URL はスキャン レポートにリンクとして表示されます。Quarantine ロールのトラフィック ポリシーで、その URL へのユーザ HTTP アクセスが許可されていることを確認してください。
10. 完了したら、[Update] をクリックします。

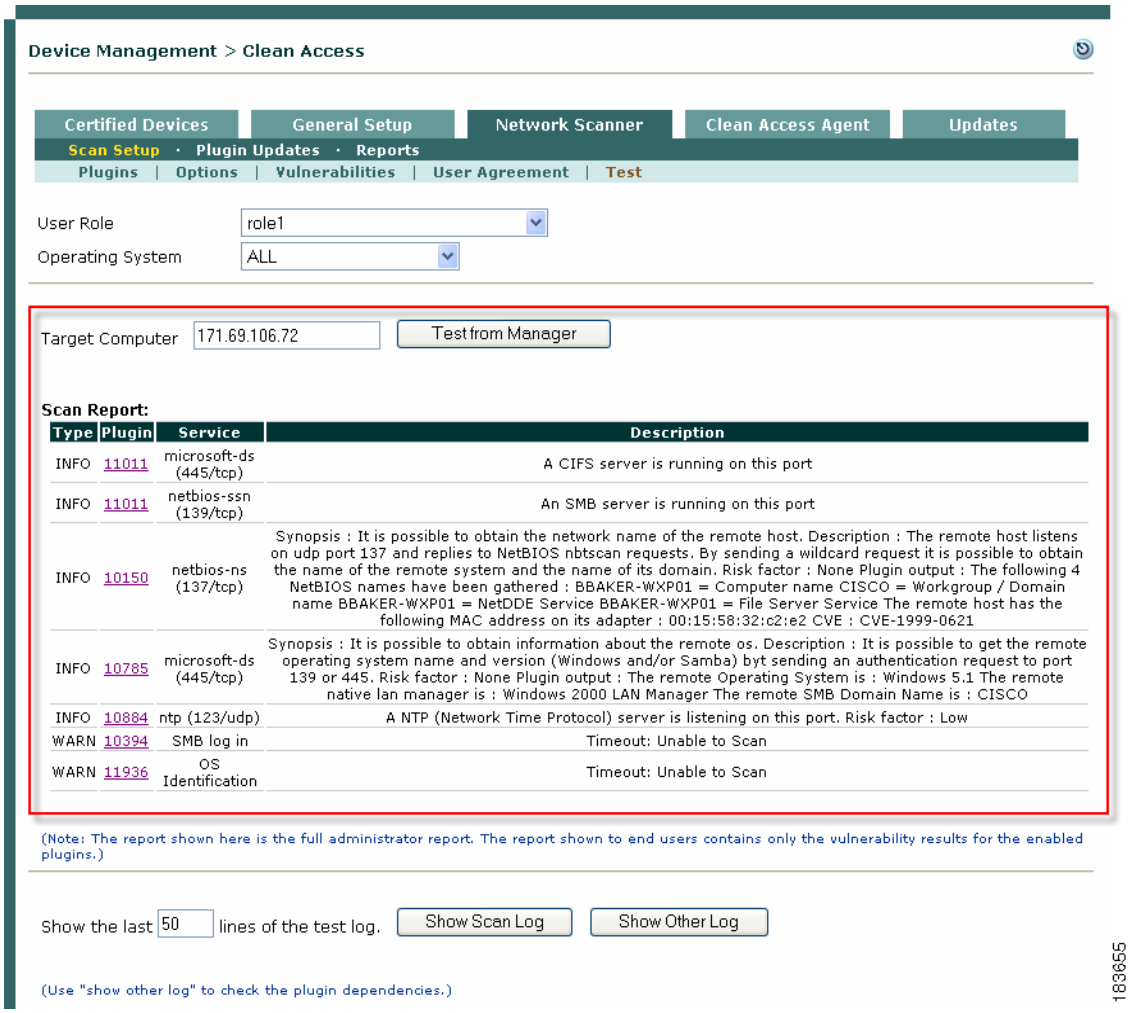
スキャンのテスト

Test フォームを使用すると、スキャンの設定を試せます。どのマシンでもスキャンの対象にできます。テストのために、対象クライアントによって想定されるユーザ ロールを指定することもできます。この種のテストでは、Clean Access Manager に保存されているスキャン プラグインのコピーに対して実際にテストが実行されます。実稼動環境では、Clean Access Server は Clean Access Manager から自動的にスキャン プラグインのコピーを取得し、スキャンを実行します。

テスト スキャンの実行手順

1. [Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [Test] の順に進みます。
2. ユーザ テストを行うユーザ ロールと OS を [User Role] と [Operating System] のドロップダウンから選択します。
3. [Target Computer] フィールドに、スキャン対象のマシンの IP アドレスを入力します（デフォルトでは現在のマシンのアドレスが表示されます）。
4. [Test] をクリックします。ページの下部にスキャン結果が表示されます。

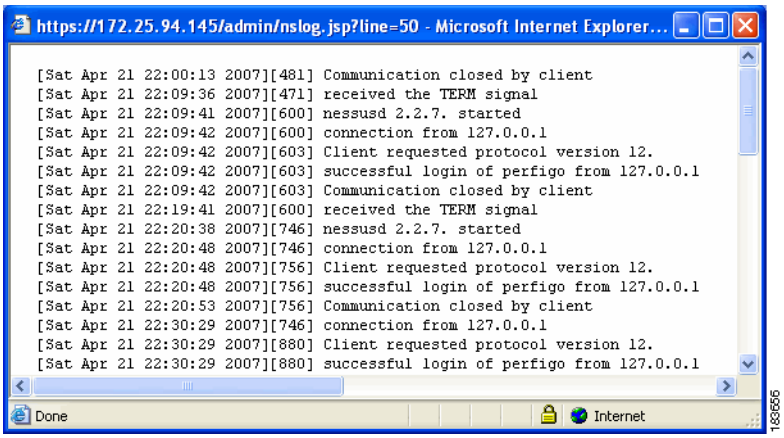
図 12-11　ネットワーク スキャンの [Test] ページ



ログの表示

[Device Management] > [Network Scanner] > [Scan Setup] > [Test] ページの [Show Scan Log] ボタンをクリックすると、テスト対象のコンピュータのデバッグ ログ（図 12-12）が表示されます（表示元は /var/nessus/logs/nessusd.messages）。ログには実行されたプラグイン、実行結果、省略されたプラグインとその理由（依存関係、タイムアウトなど）が示されています。スキャン結果が期待どおりでなかった場合、管理者はこのログから原因を調べることができます。

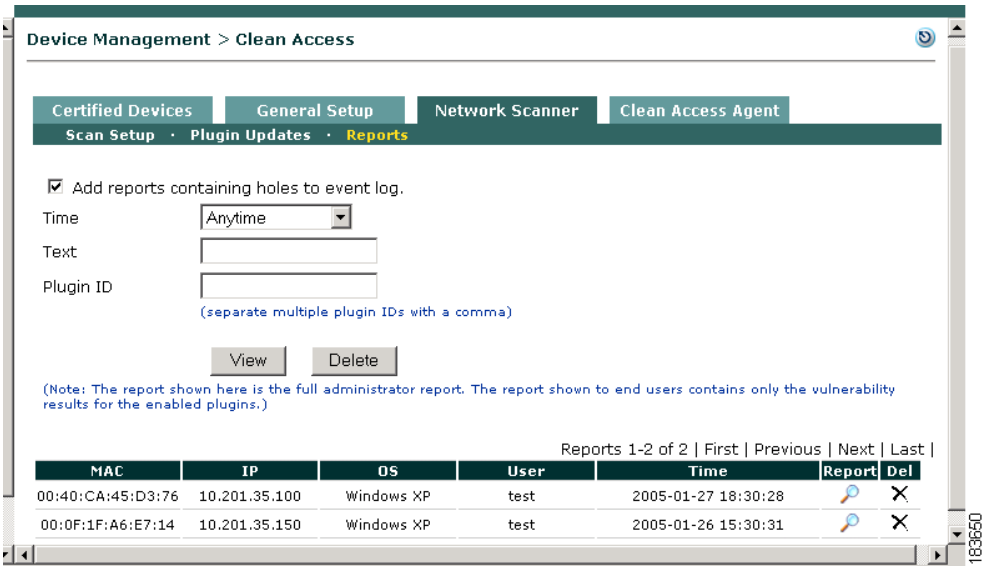
図 12-12　ネットワーク スキャンの [Show Log] ページ



スキャン レポートの表示

ネットワーク スキャンをイネーブルにすると、[Device Management] > [Clean Access] > [Network Scanner] > [Reports] から、個々のスキャン レポートを表示できます。ここで表示されるレポートは、管理者用の詳細なレポートです（図 12-14）。エンド ユーザに表示されるレポートの内容は、イネーブルに設定されているプラグインの脆弱性の通知だけです（ユーザはログアウト ページの [Scan Report] リンクをクリックすることにより、該当するバージョンのスキャン レポートにアクセスできます）。

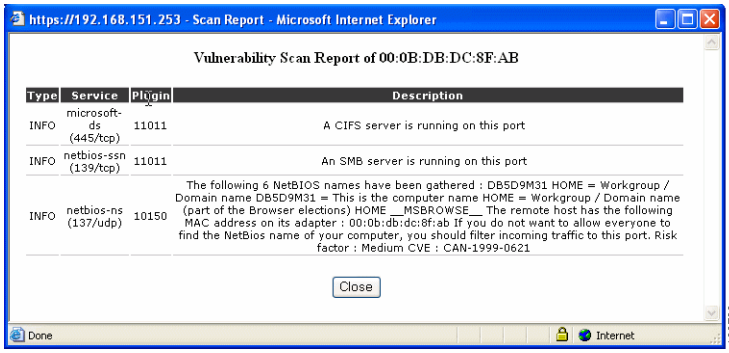
図 12-13　[Network Scanner] の [Reports] 画面



- すべてのレポートを表示するには、[Time] のドロップダウン メニューから [Anytime] を選択します。
- 選択したレポートだけを表示するには、異なる [Time] を選択するか、または検索 [Text] または [Plugin ID] を入力して、[View] をクリックします。[User Defined] タイム インターバルを選択した場合は、最初のテキスト ボックスに「開始」年月日と時刻（例：2006-03-22 13:10:00）、2 番目のテキスト ボックスに「終了」年月日と時刻（例：2006-03-23 11:25:00）を入力して、[View] をクリックします。

- 選択した基準に従って表示されているレポートを削除する場合は、[Delete] をクリックします。
- [Report] アイコンをクリックすると、図 12-15 のような詳細なスキャン レポートが表示されます。

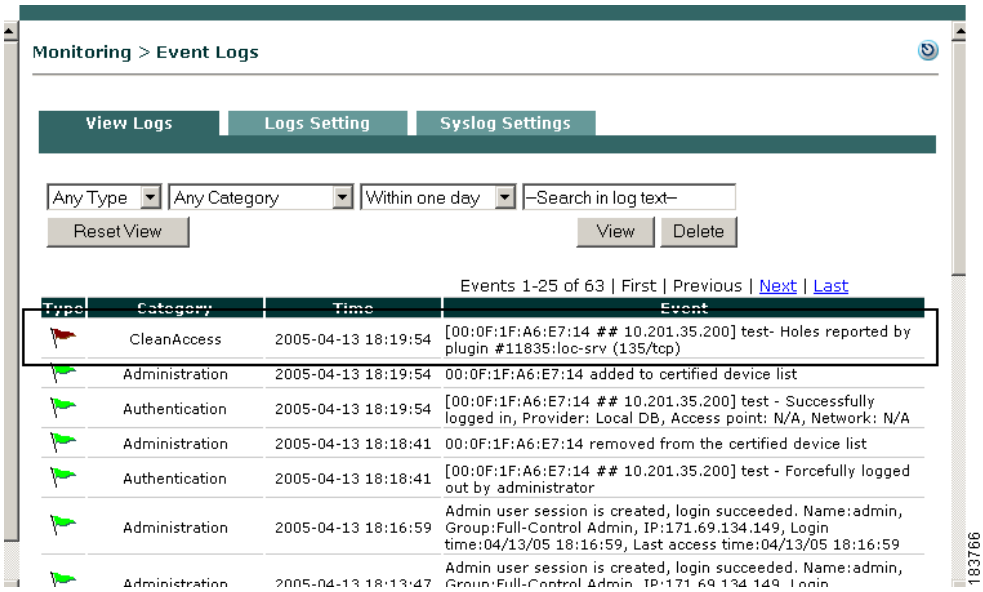
図 12-14　ネットワーク スキャナ管理者レポートの例



（注）プラグイン間に依存関係がある場合、たとえば、プラグイン B がイネーブルに設定され、プラグイン A のスキャン結果がプラグイン B の前提条件となっている場合、プラグイン A がイネーブルに設定されているかどうかに関係なく、ネットワーク スキャナは自動的にプラグイン A を適用します。ただし、プラグイン A は明示的にイネーブルには設定されていないので、プラグイン A から報告されるスキャン結果は管理者レポートにだけ表示されます。

- イベント ログ（[Monitoring] > [Event Logs] > [View Logs]）にレポートを追加するには、[Add reports containing holes to event log] オプションを選択します。図 12-15 のような CleanAccess カテゴリ レポートが生成されます。

図 12-15　CleanAccess ネットワーク スキャン イベント ログ



ユーザ同意ページのカスタマイズ

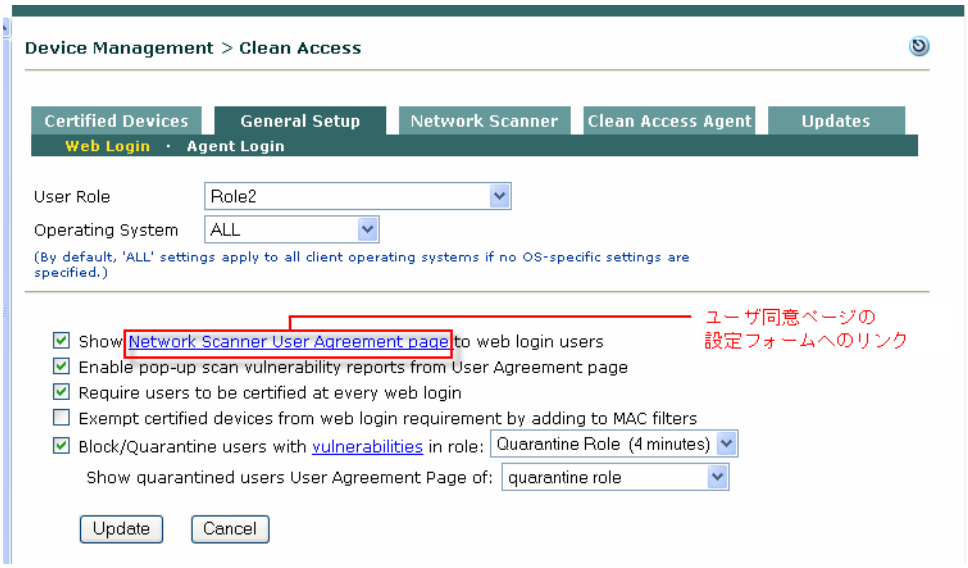
ユーザ同意ページ（「ウイルス対策ページ」）を Web ログイン ユーザに対してイネーブルにすると、ログインおよびネットワーク スキャンの通過後に、ネットワーク使用ポリシー情報、ウイルスに関する警告、ソフトウェア パッチやアップデートへのリンクのいずれかまたは全部をユーザに通知できます。

ユーザ同意ページは、未認証のユーザに対してだけ表示されます。ユーザ デバイスが Certified Devices List に登録された後は、そのデバイスが Certified Devices List から消去されるまで、ユーザ同意ページは表示されません。**Certified Devices List** は、デバイスにログインした最初のユーザだけを記録し、この方法で、どのユーザがログイン時にユーザ同意ページで同意したかを追跡します。ログインのたびにユーザに対してユーザ同意ページページが表示されるようにするには、[General Setup] ページの該当するロール/OS に対して [Require users to be certified at every web login] オプションをイネーブルにします。

このページは、2 箇所で設定します。

- ページの対象（あるユーザ ロールのユーザにこのページを表示するかどうか）は、[Device Management] > [Clean Access] > [General Setup]（図 12-16）で設定します。

図 12-16　[General Setup] タブ



- ユーザ ロールごとのページ内容は、[Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [User Agreement Page]（図 12-17）で設定します。

図 12-17　ユーザ同意ページの内容設定フォーム

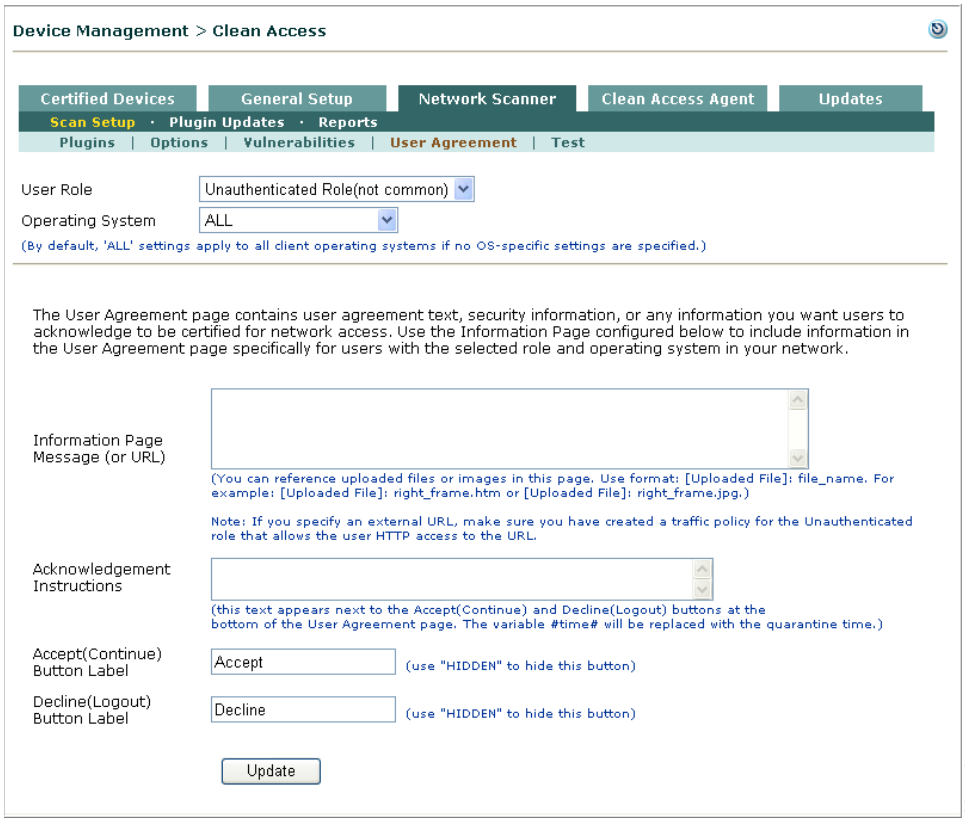
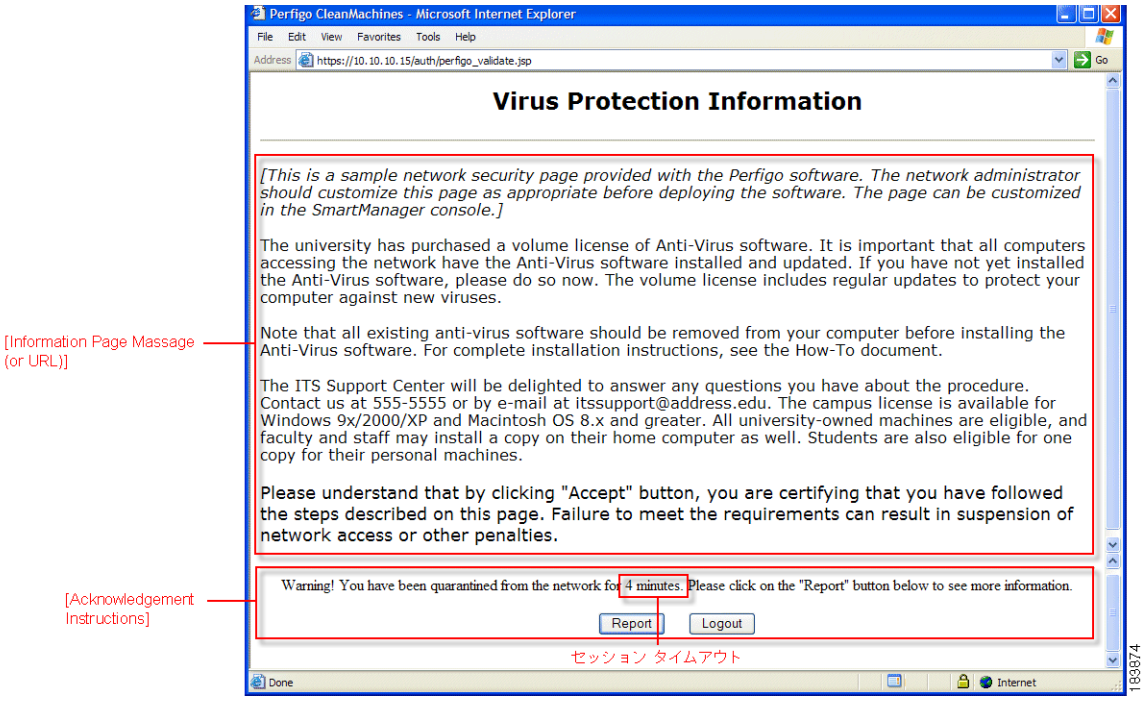


図 12-18 は、エンド ユーザに表示されるデフォルト生成ページを示しています。ユーザ同意ページは、ポップアップではなく HTML フレームベースのページで、次に示すコンポーネントで構成されています。

- **Information Page Message (or URL)** コンポーネント：指定するページ内容
- **Acknowledgement Instructions** フレーム コンポーネント：同意を確認するためのテキストやボタン（Accept、Decline）

（注）　Quarantine ロール ページでは、「Report」と「Logout」を読み取るためにボタンがハードコードされています。

図 12-18　ユーザ同意ページ（Quarantine ロールの例）



（注）　図 12-18 に示されているページ内容（「ウイルス対策情報」）は、ユーザ同意ページに他の通知メッセージや URL が指定されなかった場合にエンド ユーザに表示されるデフォルトのページ内容です。このデフォルトのページ内容は、設定フォームの **Information Page Message (or URL)** テキスト領域には表示されないので注意してください。

設定フォーム（図 12-17）では、Web ログイン ユーザ用に次のタイプのページを設定できます。

- ネットワーク スキャンでシステムに脆弱性が発見されなかった場合、ユーザには Normal Login ロール用に設定されたユーザ同意ページ（[Accept] および [Decline] のボタン）が表示されます。
- Web ログイン後のネットワーク スキャンでクライアント システムに脆弱性が発見された場合
  - ユーザには Quarantine ロールが割り当てられ、Quarantine ロール用のユーザ同意ページ（[Report] および [Logout] ボタン）が表示されます。
  - ユーザには Quarantine ロールが割り当てられますが、Normal Login ロールのユーザ同意ページ（[Report] および [Logout] ボタン）が表示されます。

作業をはじめる前に、**Information Page Message (or URL)** コンポーネントに使用する HTML ページを作成します。Cisco NAC アプライアンスは、特定のロールまたは OS のユーザに特定の通知ページを表示します。カスタマイズされたページは、Cisco NAC アプライアンスの要素にアクセス可能な Web サーバ上に置かなければなりません。

ユーザ同意ページの設定が完了したら、トラフィック ポリシーを作成して、そのロールのユーザに、そのページの Web リソースへのアクセス権を与えなければなりません。ロールには、CAM のポート 80 へのアクセス権があります。詳細については、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

ユーザ同意ページのカスタマイズ手順

1. [Device Management] > [Clean Access] > [Network Scanner] > [Scan Setup] > [User Agreement Page] の順に進みます。図 12-17 のように、ユーザ同意ページの設定フォームが表示されます。

2. [User Role] と [Operating System] のドロップダウンで、そのページを適用するユーザ ロールと OS を選択します。Clean Access Manager は、ログイン時にユーザのシステムの OS を判断し、その OS に指定されているページを表示します。Quarantine ロールを選択した場合は、[Acknowledgement Instructions] とボタンのフィールドがディセーブルになります。
3. ユーザ同意ページの [Information Page Message (or URL)] フィールドに表示するページの HTML コンテンツまたは URL を入力します。CAM または CAS にアップロードしたファイルを使用する場合は、次の方法でファイルを参照できます。
   a. ***URL を入力する***：（表示する 1 つの Web ページについて）

      外部 URL の場合は、**http://www.webpage.com** 形式を使用します。

      CAM 上の URL の場合は、次の形式を使用します。

      ```
      [Uploaded File]:file_name.htm
      ```

      イメージの場合は、次の形式を使用します。

      ```
      [Uploaded File]:file_name.jpg
      ```

（注）　外部 URL または CAM の URL を入力する場合は、その外部サーバまたは CAM へのユーザ HTTP アクセスだけを許可する Unauthenticated ロールのトラフィック ポリシーが作成されていることを確認してください。

   b. ***HTML を入力する***：（ロゴと HTML リンクなど、リソース ファイルの組み合わせを追加する場合）

      HTML コンテンツを直接テキストフィールドに入力します。

      HTML コンテンツの一部としてアップロードされているリソース ファイルを参照する場合は、次の形式を使用します。

      アップロードされた HTML ファイルへのリンクを参照する場合は、次の形式を使用します。

      ```
      <a href="file_name.html"> file_name.html </a>
      ```

      画像ファイル（JPEG ファイルなど）を参照する場合は、次のように入力します。

      ```
      <img src="file_name.jpg">
      ```

   詳細については、「リソース ファイルのアップロード」（P.5-13）を参照してください。
4. [Acknowledgement Instructions] フィールドには、必要に応じて、[Accept] と [Decline] のボタンの上部に表示するテキストを入力します。
5. [Accept] と [Decline] のボタンに表示するラベルをそれぞれのフィールドに入力します。
6. [Save] ボタンをクリックして、変更を保存します。

これで、ネットワークにログインするユーザには、変更後のユーザ同意ページが生成されます。

（注）　Web ユーザ ログイン ページの詳細については、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。トラフィック ポリシーの詳細については、「Agent Temporary および Quarantine ロールのポリシーの設定」（P.8-21）を参照してください。