2W-4

接続端末セキュリティ度判定方法の提案

服部正尚† 辻秀一‡
東海大学大学院工学研究科† 東海大学電子情報学科‡

１．研究目的

近年の情報漏洩は80%以上が内部からの漏洩である。犯罪傾向の分析から、有権限者による端末直接接続犯罪の多発が判明している。[4]これに加え、Blaster ウイルスなどのＯＳのセキュリティホールを突いた攻撃が多発している。

本研究では、内部ネットワークに接続を試みる端末を仮想的なネットワークを用いて検疫を行なうシステムを提案する。

２．従来方式

検疫ネットワークとは、認可したユーザやクライアントのネットワーク接続を許可する認証ネットワークに加え、必要なセキュリティ対策のされてないクライアントを隔離、検疫（検査・治療）、再接続までを行なうネットワークである。

検疫ネットワークに隔離する方法として以下の例をあげる。

（1）ＤＨＣＰによる隔離

内部ネットワークに接続を試みた端末に対して検疫用のネットワークへの仮アドレスを渡し隔離・検疫を行なう。コンプライアンス検査に合格した端末に対して正規のアドレスを渡す。

（2）認証ＶＬＡＮによる隔離

内部ネットワークに接続を試みた端末に対してデフォルトでのＶＬＡＮに接続させ認証スイッチにてユーザ認証し検疫も行なう。コンプライアンス検査に合格した端末に対してＶＬＡＮ切り替えを行い内部ネットワークへ接続させる。

３．提案方式

検疫ネットワークを用いる上で既存のネットワークへの影響を最小限に抑えたい。検疫ネットワークを物理的な空間ではなく仮想的に構築することによって導入の際のコスト、アドレス設計の変更を最小限に抑える。

VMWare などのソフトを用いてひとつのサーバの中に仮想的にもうひとつの仮想ネットワークを構築する。内部ネットワークに接続を試みる端末を仮想ネットワークに強制的に接続しコンプライアンス検査を行なう。

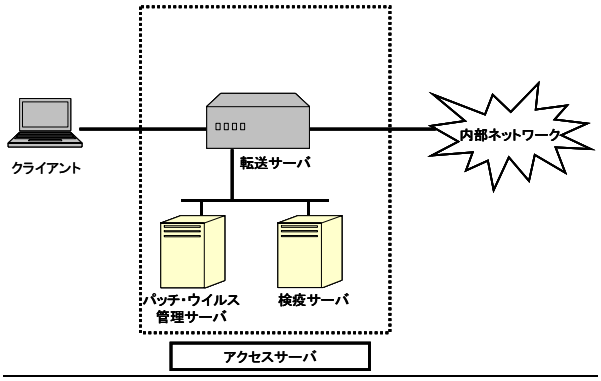

Fig.1:システム構成図

３．１：システム構成

本システムは転送サーバ、パッチ・ウイルス管理サーバ、検疫サーバの３つから構成される。

① 転送サーバ
内部ネットワークへの接続要求がきた場合
検疫サーバに強制的に接続させる。
検疫サーバからのコンプライアンス検査の結果を参照して内部ネットワークに接続を許可する。

② パッチ･ウイルス管理サーバ
コンプライアンス検査で用いるファイル類及び設定されたセキュリティポリシーなどが保存されている。

③ 検疫サーバ
パッチ・ウイルス管理サーバにあるデータを参照しコンプライアンス検査を行なう。
ユーザ認証を行う。
検査結果を転送サーバに送信する。

３．２：システムの基本動作

内部ネットワークに接続要求があると転送サーバに接続される。転送サーバは強制的に仮想ネットワーク内の検疫サーバに接続させコンプライアンス検査を行う。検査結果によって内部ネットワークにあるアプリケーション、サーバに接続を許可する。

３．２．１：転送サーバの動作

転送サーバに接続された後、強制的に仮想的な検疫サーバに接続させる。コンプライアンス検査の結果により内部ネットワークに接続する。不合格の場合は接続を拒否する。合格の場合はユーザの属性が持つすべてのアクセス権を得る。一部が不合格の場

The proposal of the method of deciding security level of the network terminal

† Masanao Hattori ‡ Hidekazu Tuji ‡
† Graduate School of Engineering, Tokai University
‡ School of Information Technology and Electronics, Tokai University

合はアクセスルールに即したアクセス権を得る。

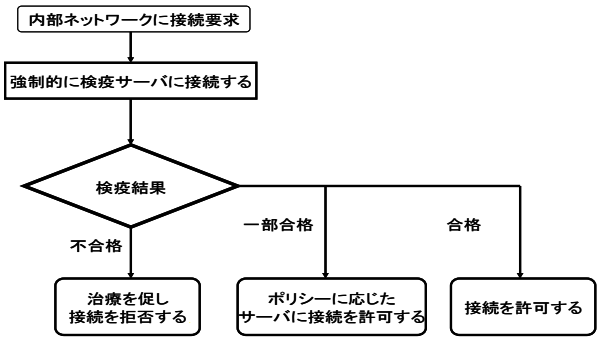

Fig.2:転送サーバの動作フロー

３．２．２：検疫サーバの動作

検疫サーバに接続されるとユーザ認証を行う。認証を通過した端末に対してコンプライアンス検査を行う。ウイルス対策ソフトの有無と定義ファイルの更新日時、端末のＯＳのサービスパックやパッチが最新であるか、ポリシーで定められていないポートが開いていないか、のチェックを行う。それぞれの検査項目の結果を元に内部ネットワークでの行動の制限を決めたアクセステーブルを作成し転送サーバに送信する。

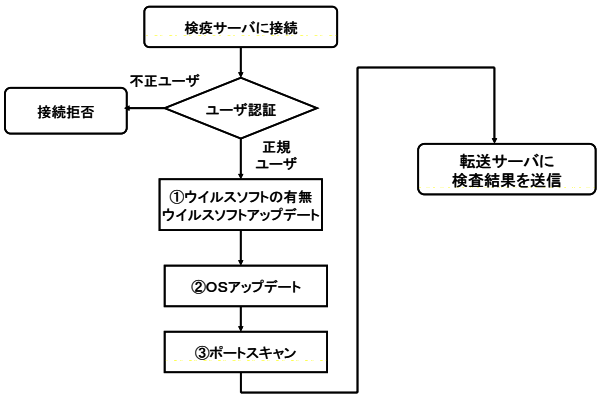

Fig.3:検疫サーバの動作フロー

３．３．３：パッチウイルス管理サーバの動作

コンプライアンス検査で使用する各ＯＳのパッチ、各ウイルスソフトの定義ファイル、を常に最新の状況を維持する。このサーバに保持してあるデータを参照してコンプライアンス検査を行う。

４．評価

本研究では検疫サーバ、転送サーバを作成し、仮想マシン内に構築し動作実験を行った。

転送サーバでは検疫サーバにて作成されたアクセステーブルを参照してアクセス制御を行えた。検疫サーバでは各コンプライアンス検査における項目に対して検査を行った。検疫にかかる時間を考慮するためにポートスキャン時にはすべてのポートではなく「telnet」「FTP」など攻撃対象になりやすいポートを対象にスキャンした。

hostname を参照にしてデータのやり取りを行うことによりアドレス環境の変更をせずに行うことが出来た。検疫サーバにおいて不具合が発生した場合、サーバのリセットが簡単に出来ることを確認した。

5. 考察

このシステムはコンプライアンス検査にすべて合格しなくても導入した際のアクセスポリシーによって使用できるアプリケーションやサーバを設定できる。これにより柔軟なアクセス制御が行える。

一方、このシステムでは一つのマシンに３つのサーバが処理を行うため負荷が高くなる。大規模なネットワーク環境の場合、負荷分散などの対策を行う必要がある。

6. 結論

本研究ではセキュアなアクセス管理を行うための検疫ネットワークシステムを提案した。これにより、ＩＰアドレス設計の大幅な見直しが必要なく検疫ネットワークに隔離できる。また、検疫項目の中にポートスキャンを行うことによりパッチ適用以前のワーム感染によるすり抜けを防止することが出来る。

今後、一度に大量の接続要求がある時の負荷実験や内部ネットワーク内に接続したあとの各端末のセキュリティ状況の監視、より詳細な検疫項目などを考えていく必要がある。

7. 参考文献

[1] 水野優良,辻秀一.仮想サーバを利用した安全なサーバシステムの提案. 情報処理学会第６６回全国大会, 4V-4:2004

[2] 中川秦宏, 須田宇宙, 浮貝雅裕, 三井田惇郎. VMware を利用したネットワーク管理者の試み. 情報処理学会第６５回全国大会, 2D-6:2003

[3]神園雅紀,白石善明,森井昌克.仮想環境を使った不正プロセスの監視による未知ウイルス検知システム.SCIS2004

[4] 服部正尚,柿崎淑郎,辻秀一.経路制御を用いた盗聴防止方式の提案.第６６回情報処理学会全国大会,6V-4,2004 年３月

[5]インテリジェントウェイブ
http://www.iwi.co.jp/index.html