

検疫ソフトウェア iNetSec Inspection Center

Security Inspection Software iNetSec Inspection Center

平松幸司 *
Koji Hiramatsu

濱野登志邦 *
Toshikuni Hamano

高橋政孝 *
Masataka Takahashi

* プロダクト本部 ソフトウェアプロダクト事業部 第二開発部

検疫ソフトウェアはネットワーク機器と連携して、ネットワーク接続を試みるクライアント PC のセキュリティパッチやウイルス対策ソフトのパターンファイルが適切か検査し、不適切な場合はネットワーク的に隔離する。これにより、持ち込み PC やモバイル PC、利用者の運用に任されていた社内 PC のセキュリティ運用を徹底させ、ウイルス感染・機密情報漏洩の脅威から社内ネットワークを守る。

Security inspection software works with network equipment to inspect the effectiveness of anti-virus software pattern files or security patches in client PCs when they attempt to connect to the network. If those files and patches are found to be ineffective, it will isolate the client PC by redirecting it to the patch server. The use of this software will make it possible to ensure PC security when used in connection with PCs brought in from external sources, mobile PCs, and office PCs which users have been free to use until now. It will also protect the office network against threats posed by virus infection and the leak of confidential information.

1 まえがき

個人情報漏洩の脅威拡大、持ち込み PC によるウイルス被害の拡大により、社内ネットワークセキュリティ対策のニーズが高まっている。当社はこの要望に対応し「PFU 検疫ネットワークシステム」を 2004 年 7 月に発売し、2004 年 12 月には機能強化を行っている。

「PFU 検疫ネットワークシステム」¹⁾は、検疫ソフトウェア「iNetSec Inspection Center」、米国 Top Layer Networks, Inc.社製ネットワーク認証機器「Secure Controller」、各社 IEEE802.1X 認証 VLAN スイッチ（以降、802.1X 認証 VLAN）を用いて、システムインテグレーションサービス、運用サービスを提供している。

本稿では、当社が独自開発した検疫ソフトウェア「iNetSec Inspection Center」を中心に「PFU 検疫ネットワークシステム」の開発のねらいと特長、今後の取り組みなどを紹介する。

2 開発の背景とねらい

2.1 開発の背景

後を絶たない個人情報漏洩事件は社会問題になっており、対策の一つとして社内ネットワークレベルでの対応が必要とされている。一方、2003 年夏に「Blaster」ウイルスが日本で猛威を振るったのは記憶に新しいところである。ほとんどの企業はインターネットとの接続口からのウイルス侵入を防止するウイルスウォール等を導入済みにも係わらず被害が拡大した。その理由は、社内ネットワークのクライアント PC（モバイル PC や持ち込み PC など）が感染源であったためである。

この頃、このような被害・脅威への対応策の相談があり、当社でも調査に着手した。この調査段階において、当社がゴールドセールspartner^{注1)}になっており、

注1) トップレイヤーの1次代理店として認定技術者を多数擁し、製品およびソリューションの提案・販売・インテグレーションおよび保守を行う販売パートナー。

ネットワーク接続ユーザーの認証とアクセス制御を実現できる米国 Top Layer Networks, Inc.社製ネットワーク認証機器「Secure Controller」と連携した「検疫ネットワーク」というコンセプトおよび仮説の確立に至り、マーケティング活動を展開することになった。

2.2 本システムのねらい

既存のお客様やパートナー様へのヒアリング活動を通じて、貴重な意見・ご要望を収集することができた。このような顧客要望分析結果や仮説検証から、次のニーズ（課題）を抽出した。

- 1) ソフトウェア導入を徹底できない管理外のクライアント PC からネットワークを守りたい
- 2) クライアント PC 利用者（被検疫対象）の運用負荷を極力少なくしたい
- 3) 検疫ネットワークシステムの運用管理負担・コストを極力少なくしたい
- 4) ネットワークエッジ（PC 単位）での認証・検疫により強固なセキュリティ環境を構築したい
- 5) 企業が設定運用しているセキュリティポリシーを満たしているか検査したい

この課題を商品仕様・品質目標として実現するために、検疫ソフトウェアを新規開発することにした。

3 本システムの概要

一般的に、検疫ネットワークとはクライアント PC をネットワークへ接続する際に Windows^{注2)}OS のセキュリティパッチとウイルス対策ソフトウェアのパターンファイルが適切かを検査し、セキュリティレベルが低いクライアント PC のネットワーク接続を許さない仕組みを持つネットワークのことを指す。

2004 年から今年にかけて様々なベンダが各社各様の方式で検疫ネットワーク商品を市場に出してきているが、ここで、市場に出ている代表的な検疫の方式について表 - 1 に示す。

「PFU 検疫ネットワークシステム」はこの中の“認証スイッチ方式”と“802.1X 認証 VLAN 方式”での検疫ネットワークを提供している。この両方式において検疫ソフトウェア「iNetSec Inspection Center」はセキュリティポリシーの運用管理機能やクライアントの

検査機能等を提供しており、方式が混在しているシステムにおいても一元管理が可能である。検疫の大まかな流れを図 - 1 に示す。

以降では、ネットワーク構成から見た特徴を紹介し、検疫ソフトウェア「iNetSec Inspection Center」の詳細は次章で紹介する。

表 - 1 検疫の方式

方式	メリット	デメリット
認証スイッチ方式	既存ネットワークに容易に追加導入でき、機器の入れ替えが不要。またネットワークリソースへのアクセスコントロールが可能。	通信で認証スイッチを通過しない PC は検疫されない。
802.1X 認証 VLAN 方式	クライアントの接続ポート単位で検疫が可能。	末端のスイッチを 802.1X 対応に置き換える必要があり導入費が高価。
Personal Fire Wall 方式	検疫目的以外のクライアントセキュリティ機能が充実。	クライアントあたりの導入費が高価。
DHCP 方式	コスト的に安価。	IP アドレスの設計の見直しが必要で、固定 IP アドレスでの運用は不可。
セキュリティ専用装置方式	コスト的に安価。	利用が特定のウイルス対策ソフトウェアとの組み合わせに限定。

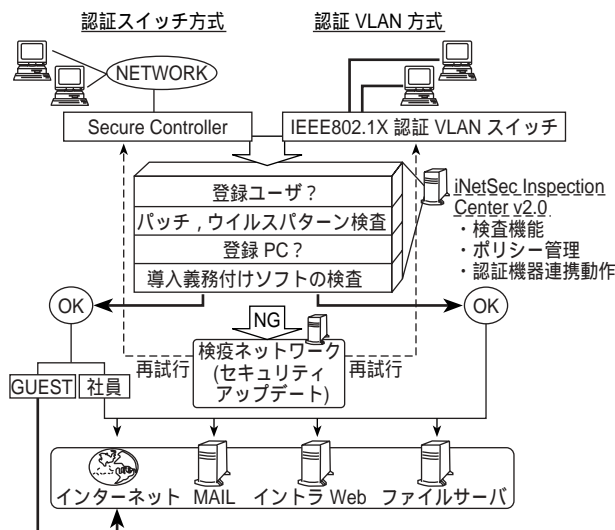


図 1 検疫の流れ (Fig. 1-Inspection flow)

注 2) Windows, ActiveX は、米国 Microsoft Corporation の米国およびその他の国における登録商標である。

3.1 ネットワーク構成

「PFU 検疫ネットワークシステム」は、利用シーンを大きく三つのモデルに集約し、顧客の業務やネットワーク運用によって特有のニーズをカバーしている。ここで、それぞれのモデルのネットワーク構成とそのモデルの特徴について述べる。

(1) フロアモデル/エッジモデル

企業内や大学構内など、組織的にネットワークが構築されている環境に適したモデル(図-2参照)。社員には専用の検疫クライアントソフトウェアを導入してネットワークの末端で検疫を実施する。派遣社員などクライアントソフトウェアを導入していないPCは、インストール型の検疫クライアントソフトウェア(Webアプリケーション)によりインストールを強いることなく検疫を実施。しかもネットワークへのアクセスコントロールを実施することが可能。

(2) センター保護モデル

データセンターのサーバ群の手前に認証スイッチを配置し、サーバ群をセキュリティの脅威から守るモデル(図-3参照)。利用者認証によりアクセス可能なサーバをユーザー毎に限定できる。

(3) リモートアクセス/VPNモデル

WAN 経由でのアクセスポイントで検疫を実施するモデル(図-4参照)。不特定多数の利用者のPCや、相対的にセキュリティが低くなりがちな自宅PCおよびモバイルPCから社内のイントラネットワークを守る。

4 検疫ソフトウェア

4.1 特長

検疫ソフトウェア「iNetSec Inspection Center」は、検疫・認証サーバソフトウェアと検疫クライアント

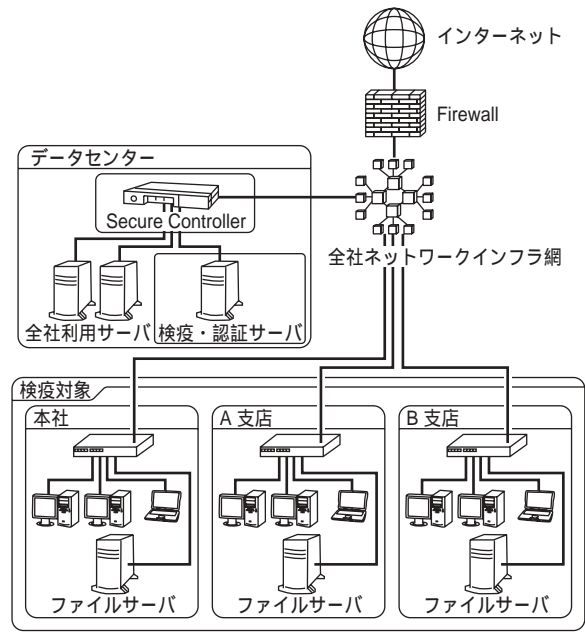


図-3 センター保護モデル
(Fig.3-Center protection model)

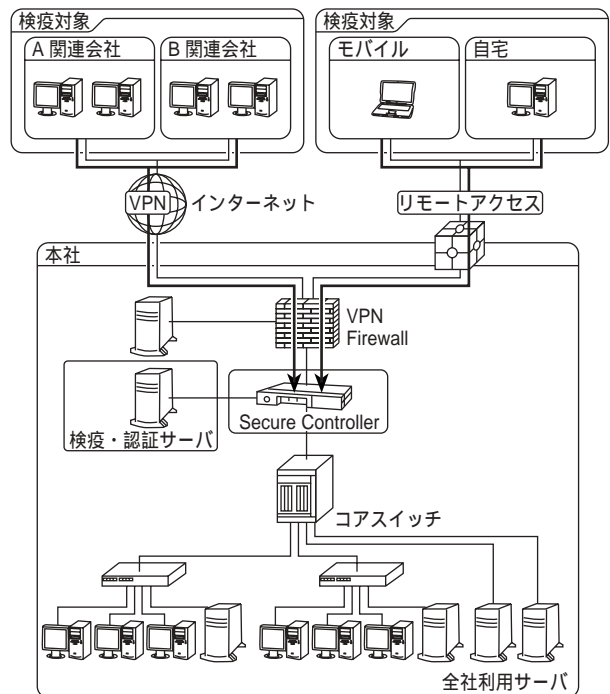


図-4 リモートアクセス/VPNモデルネットワーク構成
(Fig.4-Remote access/VPN model network configuration)

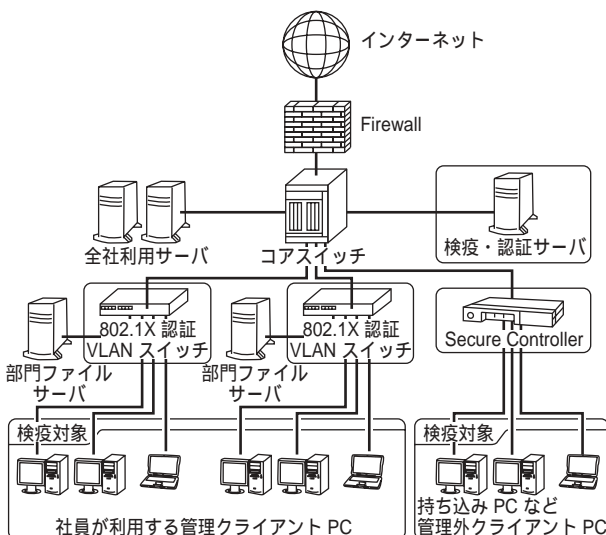


図-2 フロアモデル/エッジモデルネットワーク構成
(Fig.2-Floor model/edge model network configuration)

ソフトウェアで構成され、クライアントの検疫結果に応じてネットワーク機器を制御し、検疫ネットワークを実現する。

「iNetSec Inspection Center」には、一般的な検疫要件である Windows OS のセキュリティパッチとウイルス対策ソフトウェアのパターンファイルの検査以外に、顧客ニーズ（課題）に応えるため以下の特長を持たせた。

(1) インストールレス型クライアントソフトウェア

管理徹底できないクライアント PC を確実に検疫するためクライアント PC に専用ソフトウェアの事前導入が不要なインストールレス型クライアントソフトウェア（web アプリケーション）を提供。

(2) 検疫性能 10 秒前後を実現

クライアント PC 利用者に検疫の運用負荷を感じさせないよう、ネットワーク接続時の検疫に要する時間の最少化を目指し 10 秒前後を実現。

(3) 運用管理負担を軽減する検疫辞書配付サービス提供

検疫する項目や内容、すなわちセキュリティパッチやウイルスパターンの情報を検疫辞書として配付するサービスを提供しており、運用管理者はシンプルで分かり易い管理画面で項目選択するだけで検疫ポリシーを設定できる。図 - 5 注3) は検疫ポリシーの内、セキュリティパッチの設定画面例である。これにより、検疫ネットワークシステムの運用管理負担・コストを少なくする。

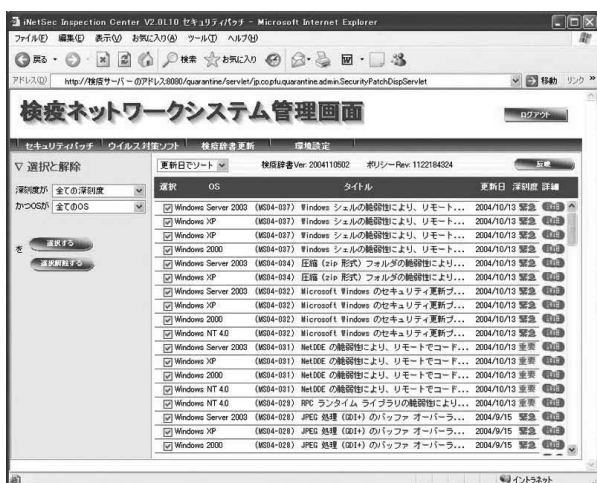


図 - 5 検疫ポリシー設定画面例 (Fig.5-Inspection policy settings window example)

注3) Microsoft Corporation のガイドラインに従って画面写真を使用している。

(4) 二つの検疫方式をサポート・運用を一元管理

ネットワークエッジ（PC 単位）で認証・検疫を行い強固なセキュリティ環境を構築できる 802.1X 認証 VLAN 方式と、ネットワーク構成を変更せずに導入できる認証スイッチ方式の双方のネットワーク機器をサポートし、1 台の検疫・認証サーバで両方式を一元管理する。

(5) 多様なセキュリティポリシーに対応

企業セキュリティポリシーに応じた検査を可能とすべく、以下の検査項目を持つ。

- a) 資産管理台帳との連携機能により、管理外（未登録）PC か否かを検査する
- b) 導入を義務付けているソフトウェアの導入状況を検査する

4.2 開発の取り組み

急速に生まれつつあった検疫ネットワークの市場に製品を投入するにあたって、スピードをもって開発すると共に次の取り組みを実施した。

(1) プロトタイプによるマーケティングの実施

プロトタイプを開発してデモを行い、より具体的な顧客要件のヒアリングを実施し、製品仕様へ反映。また、要件ヒアリングによって機能を絞り込み、短期間での開発を実現した。

(2) 方式の異なるネットワーク機器のサポート

方式の異なるネットワーク機器を迅速にサポートすること、またあとからサーバ本体に制御ロジックを追加することを可能にするために、各機器の制御ロジックモジュールはプラグインにより機能拡張するアーキテクチャを開発した。

(3) 検査項目の拡充

新しい検疫・認証の検査内容を市場ニーズに応じて後から容易に追加導入可能にするため、検疫・認証の制御ロジックモジュールはプラグインにより機能拡張するアーキテクチャを開発した。

(4) 802.1X 認証 VLAN 方式の実現

LAN 接続するユーザーを認証するための標準プロトコルである IEEE 802.1X²⁾ と組み合わせて検疫ネットワークを実現する製品も多い。他社の 802.1X 認証 VLAN 方式の大半が、まずは検疫のための隔離されたネットワークへ IP 接続し、検疫が OK だったときに VLAN を切り替える方式を採用しているなか、iNetSec Inspection Center は検疫が完了するまで IP 接続を行わない方式を開発。これにより、セキュリ

ティが低いクライアント PC に検査サーバを晒すリスクを限りなく減少させた。

(5) 検査性能

ネットワーク接続時の検査時間を品質目標の一つとして拘り、徹底したクライアント PC 検査の高速化、ネットワーク通信データの最小化などにより、検査性能 10 秒前後を実現した。

5 隔離誘導方式

5.1 認証スイッチ方式

認証機能を持つ「Secure Controller」を用いてスイッチを通過する通信の前に利用者認証および検査を行う。顧客要望に応じて二通りの検査システムを構築できる仕組みを提供している。

一つ目は、インストールレス型の検査システムで、Web ページを表示する直前に認証ページに遷移させ認証および検査処理を実行する。ActiveX^{注2)}を利用するため導入コストが削減できる。

二つ目は、インストール型の検査ネットワークシステムで、Windows ログインと同時に認証、検査処理を行うことができるため、Windows 認証と検査認証の両方入力することが不要となる。

図 - 6 に認証スイッチ方式 (インストールレス型) の処理手順を示す。

① 認証リダイレクト

クライアント PC が業務サーバ (業務に利用する Web サーバ) にアクセスする際に未認証であれば

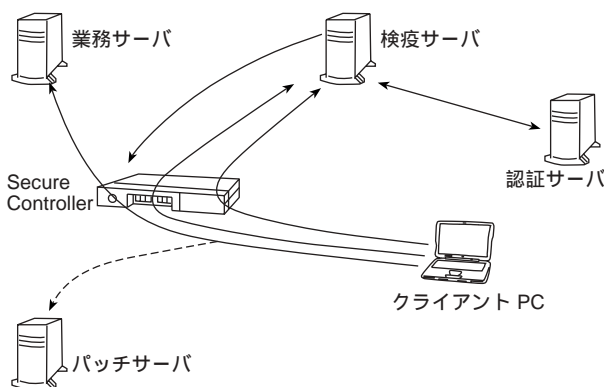


図 - 6 認証スイッチ方式の処理手順
(Fig.6-Authentication switch method procedure)

注 2) Windows, ActiveX は、米国 Microsoft Corporation の米国およびその他の国における登録商標である。

ば検査サーバの認証ページにリダイレクトされる。認証ページでクライアント PC に ActiveX がダウンロードされる。

② 認証

ActiveX は検査サーバ経由で認証サーバに対し、クライアント PC 利用者のユーザー認証を行う。ユーザー認証エラーになった場合は、業務サーバへのアクセスを遮断する。

③ 検査

ActiveX は検査サーバと通信して検査処理を行う。

④ 切り替え

検査の結果、OK であれば検査サーバはクライアント PC が業務サーバと通信できるように接続を切り替える。NG であればパッチサーバと通信できるように接続を切り替える。

⑤ 接続

検査 OK のときクライアント PC は業務サーバに接続される。NG のときはパッチサーバに接続され、最新セキュリティパッチの適用、ウイルスパターンファイルの更新を行う。

5.2 認証 VLAN 方式による検査

IEEE 802.1X 認証のシーケンス中に検査も行うことが当社製品の特長となっている。他社製品では一度検査 VLAN に接続後、セキュリティ検証を行って業務 VLAN に接続されることが多い。この仕組みでは検査 VLAN にはセキュリティの高いクライアントとセキュリティの低いクライアントが混在することになりウイルスの脅威にさらされてしまう。当社の検査ネットワークシステムでは検査完了まで IP レベルの通信を許可しない仕組みで検査 VLAN にセキュリティレベルの低いクライアントと混在することなくセキュリティの高いシステムを構築することができる。

図 - 7 に認証 VLAN 方式の処理手順を示す。

① 認証

802.1X 認証 VLAN スイッチ経由 iNetSec Inspection Center 認証サーバでユーザー認証を行う。

② 検査

認証の延長で検査処理を行う。検査処理中は IP 通信が行えない状況を維持する。

③ VLAN 切り替え

認証、検査の結果に合わせて次の 3 通りの切り替

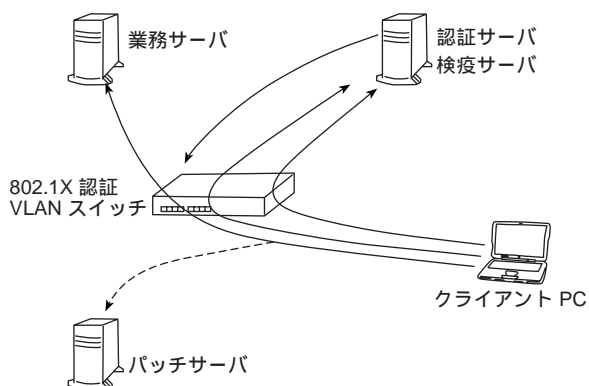


図 - 7 認証 VLAN 方式の処理手順
(Fig.7-Authentication VLAN method procedure)

えを行う。

- a) 認証 NG の場合
通信切断 (もしくはデフォルト VLAN に切り替え)
- b) 認証 OK, 検疫 NG の場合
検疫 VLAN へ切り替える。
- c) 認証 OK, 検疫 OK の場合
業務 VLAN へ切り替える。

④ 接続

検疫 OK のとき、クライアント PC は業務サーバに接続される。NG のときはパッチサーバに接続され、最新セキュリティパッチの適用、ウイルスパターンファイルの更新を行う。

6 適用例

本章では代表的な適用例として PC 資産管理ツールとの連携システムを紹介する。

企業内で利用されている PC の情報 (ハードウェア

設備, 利用ソフトウェア) を正しく把握し, PC 資産を適正に運用管理するため「PC 資産管理ツール」を導入する企業が増えている。この場合, 各 PC への「PC 資産管理ツール」エージェント導入を徹底することが必要条件となり, 逆にエージェント未導入な PC は無許可 PC として排除しなければならない。

「PFU 検疫ネットワークシステム」を適用することで, エージェント導入の徹底や無許可 PC の接続拒否を実現でき, PC 資産の運用管理を徹底することができる。

7 むすび

多くの企業では, セキュリティポリシーなどを規定し社員が遵守することで企業のセキュリティ維持を図っている。しかしながら, セキュリティポリシーを遵守しているつもりで真面目な社員が本人の知らぬ間にセキュリティ問題の起因になってしまうケースが多い。また, 社員はセキュリティポリシーを遵守しているはずという性善説に基づく対策を危惧させる事件も発生し始めている。

企業には, 業務効率を落とすことなく, 真面目な社員が問題を起してしまうリスクを軽減するとともに, 性善説から一歩踏み込んだ対策が必要とされている。

対策は, 環境, 運用, システムなど様々な観点から必要になるが, 当社では「セキュリティ脅威からお客様ネットワークを守る」ことを IT 情報システム面から支援していきたいと考えており, iNetSec Inspection Center およびその関連商品の拡充を図っていく。

参考文献

- 1) PFU 検疫ネットワークシステム紹介ホームページ
<http://www.pfu.fujitsu.com/solution/keneki/>
- 2) 北井：無線 LAN 環境のユーザ認証ソフト Safeauthor, *PFU Tech. Rev.*, 14,2, pp.25-34 (2003)。