〈製品/ソフトウェア〉

IEEE802.1X型PC検疫システム

IEEE802.1X-type PC Quarantine System

石澤克之* 谷川智彦**
Katsushi Ishizawa Tomohiko Tanikawa

要　旨

情報漏えい問題，またコンピュータウイルス・ワーム問題などLAN環境における不正アクセスに起因する問題が多発していることもあり，セキュリティレベルの低いPCを基幹ネットワークに接続させない「検疫」のニーズが高まっています。NECはいち早くこの技術の製品化に取り組み，PC検疫システムを開発し，総合サイバーアタック対策製品「CapsSuite」に組み込んでいます。そして今回，LAN環境におけるユーザ認証の方式を定めた標準規格であるIEEE802.1Xに対応した，PC検疫システムを開発しました。本稿では，「IEEE802.1X型PC検疫システム」の概要と特徴を説明します。

Since the problems resulting from unlawful access in the LAN environment, such as an information leak problem and a computer virus worm problem, are occurring frequently, the needs of “quarantine” which does not connect PC with a low security level to a trunk-line data service network are increasing. This technology is designed to prevent insecure PC’s connection to the enterprise network on the borderline. NEC has worked on production of this technology early and recently started to ship “PC Quarantine System,” integrated with cyber attack protection system “CapsSuite,” which has various unique features which other vendors do not have. This paper gives an outline of “IEEE802.1X type PC Quarantine System” and describes its features.

1．まえがき

NECでは2004年の1月より，PC検疫システムについての情報発信を行っています。2004年度は様々なベンダーよりPC検疫システムの製品発表があり，PC検疫システムの認知度が飛躍的に上がった年でした。そして2005年に入り，本格的にPC検疫システム導入についての検討が行われるようになってきています。今やネットワーク更新の案件では，必ずといってよいほど要求書に検疫システム対応の記述がでている状況です。

PC検疫システムは，ネットワーク機器とセキュリティ関連のサーバ製品を連携させて実現するシステムであるため，その両面からのアプローチが必要になります。

2．CapsSuiteをベースとしたPC検疫システム

NECでは，総合サイバーアタック対策ソフトである「CapsSuite」をベースとしたPC検疫システムを提供しています。お客様のニーズに合わせたシステム構築を可能とするために，以下にある3つの方式を提供しています。

(1) 認証VLAN方式

基幹ネットワークと検疫ネットワークとの切り替えに，認証VLANを利用する方式です。認証VLANスイッチであるUNIVERGE IP8800/700シリーズを用いたネットワーク環境において，認証サーバ機能を提供するVLANaccessからCapsSuiteが保持するセキュリティ対策状況を参照することにより，PC検疫システムを構築します。

(2) クライアントファイアウォール方式

基幹ネットワークと検疫ネットワークとの切り替えに，クライアントファイアウォールを利用する方式です。Symantec ClientSecurityを用いた環境において，CapsSuiteが保持するセキュリティ対策状況を参照することにより，PC検疫システムを構築します。

(3) サーバファイアウォール方式

保護対象のサーバにファイアウォール（ServerW@ll）を入れることにより，検疫チェックに合格したもののみファイアウォールでアクセス許可を行う方式です。

このたび，上記方式に加え，LANでのユーザ認証の方式を定めた標準規格であるIEEE802.1Xに準拠したネットワーク環境において，PC検疫システムを構築する製品を開発しました。

2.1　CapsSuiteを用いたPC検疫システムの特徴

①　様々な方式での「PC検疫システム」の提供が可能

＊ ユビキタスソフトウェア事業部
Ubiquitous Software Division

＊＊ NECソフト静岡支社
NEC Soft, Ltd.

検疫システムを導入する場合，ユーザが構築するネットワークの要件，検疫する対象，導入するコストなどの要件は様々です。NECではそれぞれのユーザの利用環境に合わせて導入できるよう，いくつかの異なるインフラを利用した，様々な方式のPC検疫システムを提供しています。

② 「CapsSuite」との連携により，セキュリティレベルの係数管理をした上での検疫を実現可能

「CapsSuite」は，社内ネットワークに接続されたPCやパソコンのパッチ適用情報やハードウェア情報を自動的に確認し，クライアントPCに自動ポップアップでパッチの適用表示を行います。

③ CapsSuiteの「パッチ適用情報パッケージ」の利用により，運用者による複雑なポリシー作成が不要

一般的に適用すべきパッチを配布するためには，セキュリティホール情報の収集，緊急度の見極め，パッチの不具合確認，複雑な配布条件スクリプトの作成など，運用者にとって非常に手間暇かかる作業となります。

NECでは，NEC社内で実際に評価・適用したパッチ定義を社外向けに「パッチ適用情報パッケージ」として提供しています。このサービスを利用することにより，管理者の負担を大幅に軽減することが可能です。

2.2 IEEE802.1X認証について

IEEE802.1Xは，LAN環境でユーザ認証を行うための方式を定めた規格です。IEEE802.1Xは無線LANのセキュリティ問題の解決策として当初は注目されましたが，有線LAN環境でもIEEE802.1X対応のHUBなどを利用することにより，無線LAN環境と同様に認証を行うことができます。

IEEE802.1Xでは，認証方式にEAP認証を採用しているため，ユーザIDとパスワードによる認証や電子証明書による認証など，様々な認証方式に対応しています。

また，認証サーバとしてIEEE802.1X認証機能を有したRADIUSサーバが必要です。

IEEE802.1X認証は，レイヤ2（データリンク層）の認証といわれることもあります。その理由はIEEE802.1X認証がIP通信を使わずに行われるためです。

IEEE802.1X認証が成功した場合には，接続したネットワーク機器を超えた通信が可能になります。逆に，認証が失敗した場合には，接続したネットワーク機器を超えた通信は一切できません。**図1**にIEEE802.1Xのコンポーネントを示します。

2.3 IEEE802.1Xの付加機能について

前述のようにIEEE802.1Xの規約は，ネットワーク機器へのアクセスを制御する（OK or NG）ものです。IEEE802.1Xの規約で定めているのはここまでの機能であり，ユーザ認証VLANシステムで求められる，動的VLAN振り分け機能（ユーザ認証を行ったユーザIDに設定されているポリシーに従ったVLANへの接続を許可する機能）については規約に定められていません。そのため，動的VLAN振り分け機能については，各ベンダー固有の実装となっているのが現実です。IEEE802.1X環境においてPC検疫システムを構築する場合に，この動的VLAN振り分け機能が重要な役割を果たすことになります。

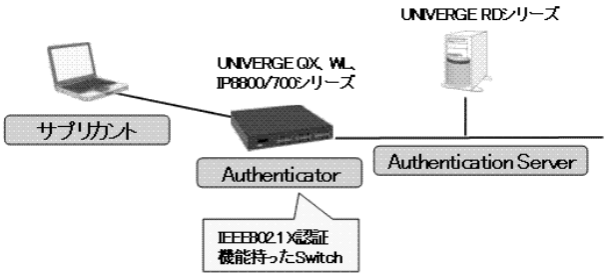

図1 IEEE802.1Xのコンポーネント
Fig.1 IEEE802.1X component.

IEEE802.1X認証をする場合，RADIUSサーバにユーザ認証を行うための情報（ユーザID，パスワード，証明書など）が必要です。さらに動的VLAN振り分け機能を使用するためには，ユーザIDと関連付けてその利用者が認証成功時に動的に割り振られるVLANをVLAN-IDで指定する必要があります。このVLAN-IDの指定は標準的なアトリビュートを使って設定します。

VLAN-IDはネットワーク機器側で設定されている値をそのまま指定します。1つのユーザIDに対して，このVLAN-IDは通常1つしか割り当てることができないため，利用者が端末を持ち歩き，様々なLAN環境で端末を接続して利用する場合には，ネットワーク機器側に設定するVLAN-IDの設定に工夫が必要になります。

3．IEEE802.1X型PC検疫システムの概要

IEEE802.1Xの基本的なシステム構成を**図2**に示します。認証を行う端末に実装されるサプリカント，IEEE802.1X認証対応のネットワーク機器に実装されるAuthenticator，AuthenticationサーバのRADIUSサーバです。RADIUSサーバではサプリカントから送られたユーザ認証情報をチェックし，その結果をAuthenticatorに返します。Authenticator

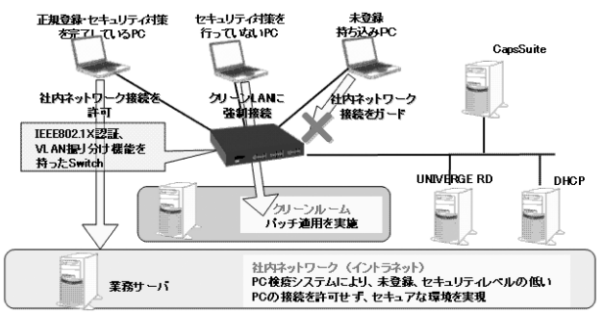

図2 IEEE802.1X型PC検疫システム
Fig.2 IEEE802.1X-type PC Quarantine System.

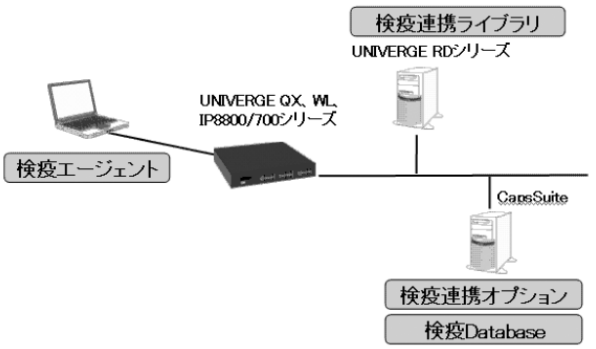

図3　PC検疫システムのための追加コンポーネント
Fig.3　Additional component for PC Quarantine System.

ではその結果に応じてネットワーク機器へのアクセスを制御します。

IEEE802.1X環境において，PC検疫システムを構築するには下記の機能が必要となります（**図3**）。

・検疫

ユーザ認証情報だけでなく，ネットワーク接続に使用する端末のセキュリティ対策状況を動的に判断する機能です。セキュリティ対策状況としては，セキュリティパッチの適用状況，アンチウイルスソフトのインストールの有無，アンチウイルスソフトのパターンファイルのバージョンチェックなどがあります。また，セキュリティ対策状況の判断項目，判断基準をポリシーと呼ぶことが多いです。

・隔離

接続する端末のセキュリティ対策状況に応じて，ネットワーク機器へのアクセスを制御する機能です。動的VLAN振り分け機能を用いることが多いです。ポリシーに合致しない端末についてアクセスを拒否することは簡単ですが，治療するための環境を提供する場合には，アクセスが制限された特別な環境に導く必要があります。

・治療

セキュリティ対策状況が万全ではないマシンを，万全な状況にすることを指します。セキュリティパッチの適用，アンチウイルスソフトのパターンファイルの更新などがそれにあたります。

NECでは，IEEE802.1X環境において，下記に説明するコンポーネントを開発することにより，適用性の広いPC検疫システムの構築を可能としました。

・UNIVERGE RD検疫連携ライブラリ

RADIUSサーバにおいて，EAP認証時にMACアドレスを拾い出し，そのMACアドレスをキーとして，CapsSuite検疫連携オプション機能に対してセキュリティ対策状況の問い合わせを行う機能です。UNIVERGE RDシリーズにこの機能を組み込みました。

・CapsSuite検疫連携オプション

UNIVERGE RDからのセキュリティ対策状況確認要求を受け付けます。そして，要求に含まれるMACアドレスをキーとして検疫Databaseを検索し，その結果を応答としてUNIVERGE検疫連携ライブラリに返します。

・検疫Database

接続するすべての端末のセキュリティ対策状況のチェック結果を保持するDatabaseです。MACアドレスをキーにして，セキュリティ対策状況を検索できるようになっています。

・検疫エージェント

ネットワークに接続する端末のセキュリティ対策状況を監視するモジュールです。セキュリティ対策が万全になったことを検知し，検疫Databaseの状態を更新する機能を持ちます。

CapsSuite検疫連携オプションと検疫Database，検疫エージェントについては，CapsSuiteをベースとした検疫システムの認証VLAN型や，クライアントファイアウォール型などの他の方式についても利用可能な，共通的なコンポーネントとなっており，各方式を混在して構成することも可能になっています。

3.1　PC検疫システムの利用イメージ

IEEE802.1X型PC検疫システムの動作概要と，利用イメージを説明します。

①　検疫ポリシーの設定

検疫対象とする条件（例：このセキュリティパッチが適用されていること）をポリシーとして，夜間バッチファイルに設定します。

②　全端末のセキュリティ対策状況の確認

全端末の検疫ポリシーの適合状況を調査するために，夜間バッチ処理を実行します。チェック結果は検疫Databaseに格納されます。

③　利用者によるIEEE802.1X認証

利用者は，ネットワークへのアクセスをするためにIEEE802.1X認証を行います。AuthenticationサーバであるUNIVERGE RDがIEEE802.1XのEAP認証要求を受けた場合，EAP認証チェックを先に行います。EAP認証が成功した場合には，EAP認証要求元のMACアドレスを取得し，CapsSuite検疫連携オプションに対して，MACアドレスを検索キーとしたセキュリティ対策状況の問い合わせを行います。CapsSuite検疫連携オプションでは，MACアドレスを検索キーとして検疫Databaseを参照し，該当端末のセキュリティ対策状況結果を獲得し，検疫連携ライブラリに応答を返します。検疫連携ライブラリにおいて応答を判別し，チェック結果がNGであった場合には，RADIUSサーバの設定で検疫ネットワーク用に割り振られているVLANのVLAN-IDを獲得し，EAP認証の結果とそのVLAN-IDをネットワーク機器に返送します。ネットワーク機器では，検疫ネットワークとして定義されたアクセスが制限されたVLANに動的に割り振りを行います。

④　検疫ネットワークにおける治療

検疫ネットワークに誘導された利用者は，そこで治療を

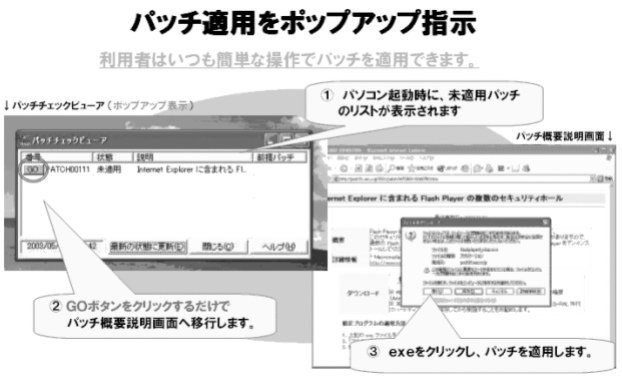

図4　パッチチェックビューアによる治療
Fig.4　Solution by Patch-Check-Viewer.

行います。検疫ネットワークは，治療を行うために必要なリソース（サーバなど）にのみアクセスが可能なように，ネットワーク機器でアクセスが制限されています。CapsSuite導入環境で治療をする場合には，パッチチェックビューアが利用者端末に表示されるため，その支持に従うだけで，適用すべきセキュリティパッチの適用が可能です（**図4**）。

⑤　基幹LANへのログオン

セキュリティパッチを適用すると，検疫エージェントが動作し，端末の状態を調査し，検疫Databaseにある該当端末の情報を更新します。端末利用者にはIEEE802.1Xの再認証を促す画面が表示され，利用者が再認証を行うとIEEE802.1X認証と検疫ポリシーチェックの両方が成功するため，ユーザIDに関連付けされたVLANに動的に割り振られます。その結果，利用者は基幹LANへのアクセスが可能になります。

3.2　IEEE802.1X型PC検疫システムの特徴

NECが今回開発したIEEE802.1X型PC検疫システムは，IEEE802.1Xの規格を拡張することなくPC検疫システムの構築を実現しています。そのため，サプリカントには各ベンダーからリリースされているIEEE802.1X認証に対応した製品が使用でき，また，AuthenticatorにはIEEE802.1X認証機能を有するスイッチを利用することができます。IEEE802.1X認証機能は現在発売されている各ベンダーのL3SW/L2SWでほぼ標準的に搭載されている機能です。そのため，適用可能な環境が非常に幅広いという大きな特徴を持っています。

また，検疫連携オプション機能については，汎用的な構造を実現しているため，NECが提供する数多くのPC検疫システム方式とノウハウにより，お客様がすでに持っている資産を有効活用してPC検疫システムを構築することも可能としています。

また，ネットワーク機器として，UNIVERGE IP8800/700シリーズ，SR，QXシリーズを使用した場合は，認証VLAN機能とIEEE802.1X機能の両方の機能を提供できるため，お客様環境に合わせて認証VLANとIEEE802.1Xを選択できるメリットがあります。

4．むすび

本稿では，UNIVERGE製品を活用したIEEE802.1X型PC検疫システムを紹介しました。本方式は今後社内システムへの展開も検討されており，よりいっそうお客様が利用しやすい，また運用管理者が運用しやすい製品にするための検討を継続していきます。

情報漏えい対策，不正接続対策のためにネットワークセキュリティを保つためのニーズはますます高まっているため，社会に貢献できる新しいソリューションを提案していきたいと考えています。

筆者紹介

Katsushi Ishizawa
石澤　克之　1990年，NEC入社。現在，システムソフトウェア事業本部ユビキタスソフトウェア事業部エンジニアリングマネージャー 。

Tomohiko Tanikawa
谷川　智彦　1987年，NECソフト入社。現在，NECソフト静岡支社第五SI部エンジニアリングマネージャー。