〈ソリューション〉

# ウィルス検疫VLANソリューション

## Virus Quarantine VLAN Solution

福田光司* 中田浩章* 下河浩樹** 田中伸佳*
Koji Fukuda Hiroaki Nakada Hiroki Shimokawa Nobuyoshi Tanaka

### 要　旨

SQLSlammerやBlaster，Nachiなどの凶悪化するウイルスの脅威を背景に，2003年末あたりから，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」という水際でのウイルス対策技術への注目度が高まっています。NECは，いち早くこの技術の製品化に取り組み，他社にない様々な特徴を盛り込んだ「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 V3.0」に組み込み，製品化を実現しました。本稿では，「PC検疫システム」の概要と特徴を説明します。

“Quarantine,” the new antivirus technology, has been attracting attentions increasingly due to the recent emergence of brutal worms such as SQLSlammer, Blaster and Nachi. 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 V3.0,” which has various unique features which other vendors do not have. This paper describes an outline and features of “PC Quarantine System.”

### 1. まえがき

2000年のCodeRedワームによってもたらされた甚大な被害や省庁ホームページ改ざんなどのインシデントにより，日本の企業へのウイルス対策ソフトやファイアウォールの導入は急速に進んでおり，現在ではどちらも90%以上の導入率といわれています。しかし，ウイルスの被害は2003年度は3025億円（IPA調べ）といわれており，沈静化の気配はありません。

NECでは，総合サイバーアタック対策製品CapsSuite[1)]で，企業のIT資産のセキュリティレベルを底上げするソリューションを提供していますが，セキュリティマネジメント強化による対策だけでは，企業内へのウイルスの侵入を根絶することは困難です。CapsSuiteのベースであるNEC社内システムCAPSで管理されている，NEC内へのウイルス持ち込みパターンを分析した結果，モバイルパソコンからの持ち込みがほとんどであることが判明しました（図1）。

このような，一度セキュリティレベルの管理を離れたPCからのウイルス持ち込みを防御するには，基幹ネットワーク接続時に，一度セキュリティレベルをチェックした上で基幹ネットワークに接続する仕組みが必要です。この仕組みを「検疫」と呼んでいます（「自己防衛ネットワーク」といっているメーカーもあります）。

### 2. PC検疫システムの特徴

これまで，ネットワーク機器ベンダやアンチウイルスソフトベンダが「検疫」に該当する機能を提供してきましたが，NECでは，「検疫ネットワーク」という独自の概念を採用しています。またその実装にいくつかの異なるインフラを利用して，ユーザの利用環境に合わせた導入が可能なようにしています。ここでは，NECの検疫ネットワークの考え方と特徴を説明します。

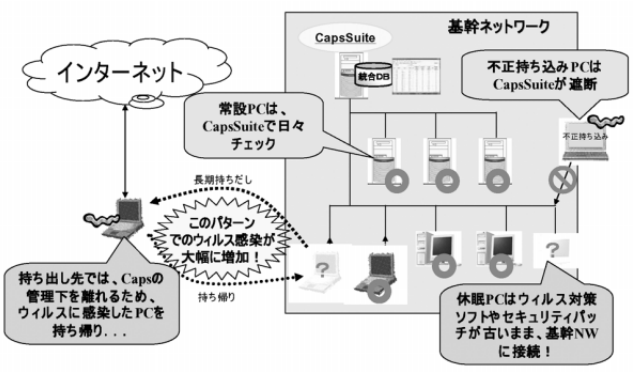


**図1　最近のウイルス感染のパターン**
**Fig.1　Recent virus infection pattern.**

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

＊＊ 第二コンピュータソフトウェア事業部
2nd Computers Software Division

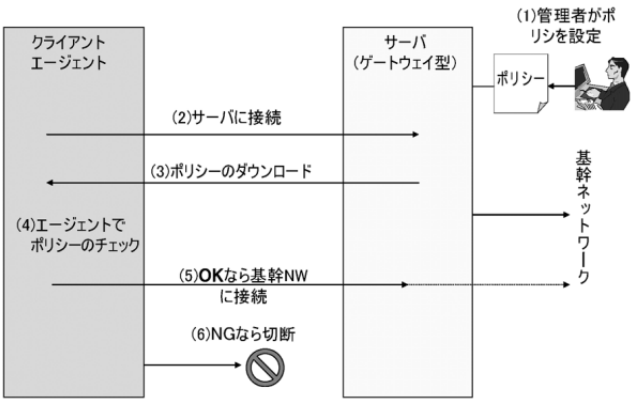


**図2　一般的な検疫の実装イメージ**
**Fig.2　Implementation image of general quarantine.**

2.1　一般的な検疫の実装

一般的な検疫システムの実装は図2のようになっています。

チェック可能なポリシーとしては，ウイルス対策ソフトのバージョンが中心ですが，製品によっては起動されているプロセスや，DLLのバージョン，レジストリ値などがチェックできるものもあります。このような実装は，VPN装置やSSL-VPN装置に多く見られますが，以下のような弱点があります。

・防御対象は外部からの接続が中心になる
・切断されるため社内のウイルス対策ソフトの配信やパッチ配布システムが利用できない
・サーバ側のポリシー設定が複雑

2.2　NECの実装 ～検疫ネットワーク～

NECの「PC検疫システム」では，検疫ネットワークという検疫用のネットワークを基幹ネットワークとは別に用意し，切断ではなくネットワークを振り分けることにより検疫された状態でのパッチやウイルス対策ソフトの配布の問題を解決しています（図3）。

検疫ネットワークを構築するためには，ネットワークを切り替えるためのインフラが必要になります。NECでは，

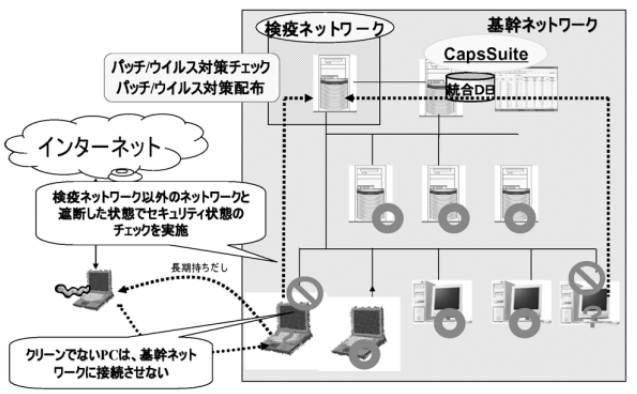


**図3　検疫ネットワークのイメージ図**
**Fig.3　Image of quarantine network.**

以下の3つの方式で検疫ネットワークを実現しています。

(1) 認証VLAN（IP8800）・認証DHCP
(2) クライアントファイアウォール
(3) サーバファイアウォール

各方式の概要や特徴は第3章で述べます。

2.3　その他の特徴

NECの「PC検疫システム」には，検疫ネットワーク以外に以下の特徴があります。

・総合サイバーアタック対策ソフト「CapsSuite」との連携により，セキュリティレベルを計数管理した上での検疫の実現
・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

## 3. 各方式の概要と特徴

本章では，NECが提供する3つの方式に関して，概要と特徴を説明します。NECが3種類の方式を提供している理由は以下の2点です。

・構築するネットワークの要件に合わせて方式を選択可能にする
・検疫する対象，導入コストにより方式を選択可能にする

3.1　認証VLAN方式

認証VLAN方式では，検疫ネットワークと基幹ネットワークの切り替えに認証VLANを利用します。認証VLAN装置としてはUNIVERGEシリーズのIP8800を利用します（図4）。

認証VLAN型検疫の動作フローは図5の通りです。

① クライアントがネットワークログイン時にDHCP認証（ID/パスワード）を実行。
② VitalQIP（認証DHCPサーバ）でDHCP認証を実行。
③ DHCP認証成功後，VLANaccessによって，CapsSuite検疫連携オプションサーバ機能に，クライアントのパッチ状態の問い合わせを実行（統合DBの内容が参照される）。

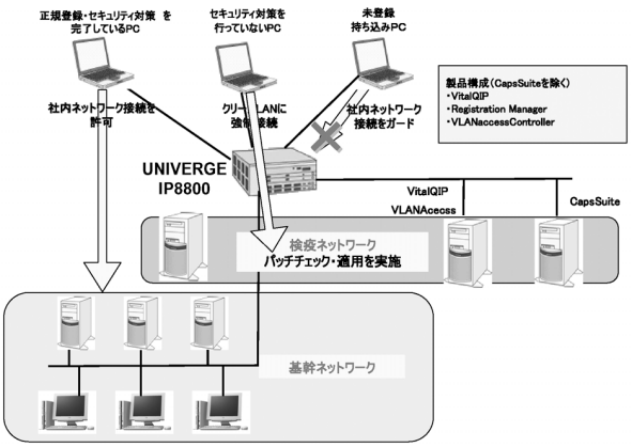


**図4　認証VLAN型検疫システムのイメージ図**
**Fig.4　Image of authentication VLAN quarantine system.**

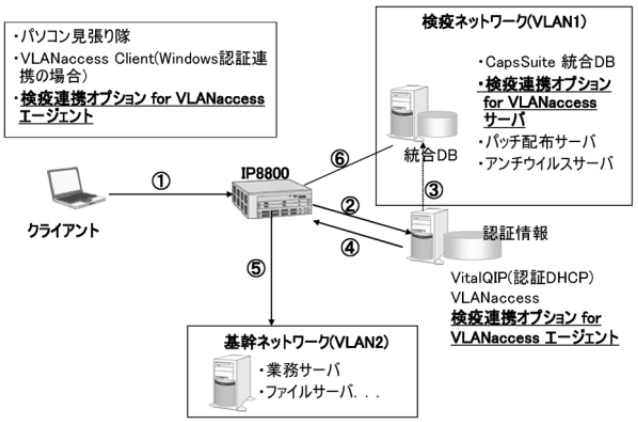


**図5　認証VLAN型検疫システムの動作フロー図**
**Fig.5　Operation flow of authentication VLAN quarantine system.**

④ VLANaccessでは，パッチが最新でない場合VLAN1（検疫ネットワーク）に振り分けられるようにIP8800を設定。最新の場合，VLAN2に振り分けられるようIP8800を設定。

⑤ ④でVLAN2に振り返られた場合，そのまま基幹ネットワークに接続される。

⑥ ④でVLAN1に振り分けられた場合，検疫ネットワークで，再度パッチのチェック－必要なパッチのダウンロード－パッチの適用－再起動を行う。パッチが最新になると，統合DBがリアルタイムで更新され，次のログインで，基幹ネットワークに接続できるようになる。

以上のように，本システムで検疫を実行すると，パッチが最新になるまで，検疫ネットワークにしか入れなくなります。CapsSuiteへの新しいパッチの登録で常に検疫されるようになると，エンドユーザへの負担が大きいため，検疫が開始されるタイミングを変更可能にしています。以下のようなタイミングでの検疫開始を推奨しています。

・パッチ登録後，一定期間が経過（Ex. 1週間）
・ぜい弱性を利用するウイルスの出現時

また，CapsSuiteの統合DBや検疫サーバ障害時や，パッチが掛けられないサーバは基幹ネットワークに接続できなくなるため，以下のような耐障害機能と運用機能を備えています。

・サーバの2重化機能
・検疫の停止機能
・特定マシンへの検疫免除機能

本方式は，スィッチとしてUNIVERGE IP8800が必要ですが，CISCOなどほかのスィッチと組み合わせることも可能です。この場合，下記の制約がつきます。

・スイッチがセカンダリアドレッシング（1つのポートに複数のIPアドレス割り当てを行う機能）を有すること。
・認証VLANとしては使用できない（認証DHCPのみ）こと。

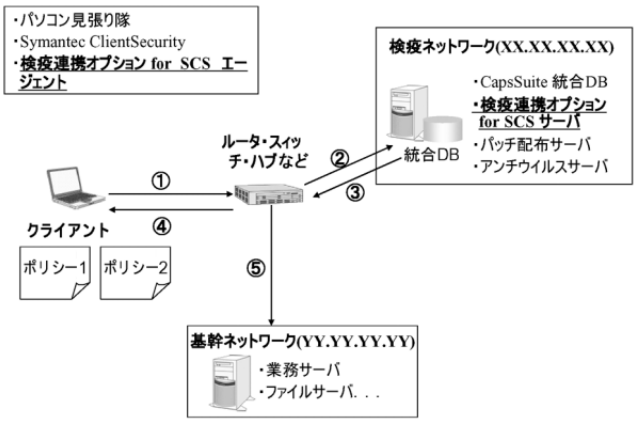


**図6　クライアントファイアウォール方式の動作フロー図**
**Fig.6　Operation flow of client firewall quarantine system.**

3.2　クライアントファイアウォール方式

クライアントファイアウォール方式では，検疫ネットワークと基幹ネットワークの切り替えをクライアントファイアウォールのポリシーを自動切り替えすることにより，物理ネットワークには依存せずに実現します（図6）。

① クライアント起動時に，クライアントエージェントはクライアントファイアウォール（Symantec ClientSecurity：SCS）のポリシーをポリシー1に設定する。ポリシー1はSCSのアクセス可能アウトバウンドポリシーを検疫ネットワーク（XX.XX.XX.XX）に限定する（この状態では，検疫ネットワーク以外にはアクセスできない）。

② クライアントエージェントは，①の状態でサーバエージェントに接続し，クライアントのセキュリティ状態を問い合わせる。

③ サーバエージェントは，CapsSuiteの統合DBの状態をチェックし，クライアントに返却する。

④ クライアントエージェントは，③の結果が最新であれば，ポリシーをポリシー2に切り替える。ポリシー2はSCSのアクセス許可のアウトバウンドのポリシーを基幹ネットワーク（YY.YY.YY.YY）に拡大したポリシーである。③の結果が最新でない場合，①の状態でパッチの適用を行い，再度チェックすると最新の状態になりポリシー2に自動的に切り替わる。

⑤ SCSがポリシー2に切り替わると基幹ネットワークにアクセス可能になる。

以上のように，クライアントファイアウォール方式では，(1) ネットワークの特別な変更なしに，仮想的に検疫ネットワークを構築することが可能，(2) 接続に依存しないため，イントラネットへの接続でも外部からの接続（VPN，ダイヤルアップなど）でも検疫を実行できる，(3) クライアントファイアウォールによりクライアントパソコンのウイルス耐性が向上する，という特徴があります。ただし，ファイアウォールソフトはSymantec社のSCSに限定されます。

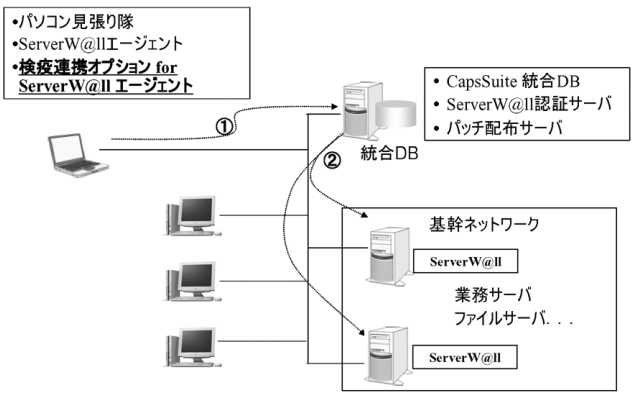


**図7　サーバファイアウォール型検疫システムの動作フロー図**
**Fig.7　Operation flow of server firewall type quarantine system.**

3.3　サーバファイアウォール方式

サーバファイアウォール方式は，今までの方式と異なり，保護対象のサーバにすべてファイアウォール（ServerW@ll）を入れ，検疫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（図7）。

① サーバを利用したいユーザはServerW@llクライアントエージェントにより，ServerW@ll認証サーバにチェックインする。

② ServerW@ll認証サーバでは，クライアントエージェントから送られた情報をチェックし，最新状態であれば業務サーバなどのServerW@llのインバウンドポリシーを制御してクライアントからのアクセスを可能にする。

このように，サーバファイアウォール型検疫は，(1) ネットワークに依存しない，(2) サーバにファイアウォールを入れるため，パッチを適用できないサーバのウイルス耐性が向上する，(3) 他の方式に比べて安価に構築できる，という特徴があります。ただし，クライアントは保護されない，方式上規模の上限が100サーバ/5,000クライアント程度，という制限があります。

## 4. むすび

社会のユビキタス化への流れに乗って，ますますモバイルパソコンの需要が高まり，そのセキュリティレベルの維持がサイバーアタック対策の重要な要素になっていくことが考えられます。NECでは，今後もUNIVERGE製品を活用した，無線LANシステムでの検疫やIEEE 802.1X認証環境での検疫，またサイバーアタック対策に留まらず，情報漏えい対策の施されていないパソコンの検疫など，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。

## 参考文献

1) 森野ほか；「サイバーアタック対策　統合管理ソフトウェア「CapsSuite」」，NEC技報，Vol.56，No.12，pp.23～27，2003-12.
2) Internet Technology 2004 Vol.2（日経システム構築 特別編集）
3) 日経コンピュータ 2004.6.23

## 筆者紹介

Koji Fukuda
**福田　光司**　1982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。

Hiroaki Nakada
**中田　浩章**　2000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主任。

Hiroki Shimokawa
**下河　浩樹**　1987年，NEC入社。現在，コンピュータソフトウェア事業本部第二コンピュータソフトウェア事業部主任。

Nobuyoshi Tanaka
**田中　伸佳**　1984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シニアマネージャー。