内部統制時代の検疫ネットワーク

安留 良夫・安達 智雄・吉田 享之

要　旨

内部統制を図る上での1つの課題であるセキュリティポリシの遵守を実現する手段の1つとして、検疫ネットワークの重要性が高まっています。検疫ネットワークを実現するには複数の検疫方式が現存しているため、システムの導入に当たっては検疫方式の選定が重要です。本稿では、検疫機能の動向、各検疫方式の特徴とシステム導入の際の検討ポイントを述べ、NECの取り組みについて紹介します。

キーワード

●検疫ネットワーク　●セキュリティポリシ　●セキュリティ対策　●内部統制
●検疫方式　● NAC　● NAP　●エージェントレス方式

1. はじめに

2005年4月の個人情報保護法の施行により、企業のセキュリティ対策は情報漏えい対策をキーワードに進んできました。そして、2006年6月の日本SOX法成立により内部統制へとセキュリティの適用必須範囲は拡大しています。従来からのウイルス・ワームによる発見報告数は減少傾向に向かっていますが、被害額が減少しているわけではありません[1]。特に最近の傾向として凶悪化、感染力UP、セキュリティホールの悪用が進み、ウイルス発生から2ヵ月余りで70種類以上もの亜種が登場しています[2]。

ネットワークを防衛する従来の対策は、外部からの攻撃に対応するファイアウォールの導入でした。しかし大きな被害をもたらしたMS Blasterの感染経路は、25%が持ち込みPCからとされており[3]、ファイアウォールでは持ち込まれたPCからの攻撃には対応できませんでした。また、近年の情報漏えいは、PCが発生源になることが多く、Antinnyに代表される個人情報を暴露するウイルスの報道も後を絶ちません。

今後は、イントラネットに接続されるPCを発生源とするウイルス・ワームの脅威からネットワークや情報を守ることがより重要となります。本稿ではPCを発生源とする脅威にネットワークから対策を講じる検疫ネットワークについて述べます。

2. セキュリティ対策における検疫機能とは

2.1 PC検疫の重要性

(1) 従来の対策

従来のネットワークのセキュリティ対策は、外部ネットワークからの侵入と攻撃を防ぐファイアウォール・IDS(侵入検知システム)が中心でした。しかし、これらの対策は人手を経由してイントラネットへ持ち込まれたPCから発生する攻撃を阻止することはできません。このため、内部に持ち込まれてしまうことが避けられない脅威への対策が課題として残っています。

(2) PCの構成管理

イントラネットに不正に持ち込まれた脅威による被害を受けないためには、接続を検知した未登録PCをネットワークから遮断する方式や、PCの構成を管理しセキュリティ状態をチェックする方式が利用されています。後者は、PCへのパッチの適用や企業のセキュリティポリシに基づいたPC運用を実現します。

社内のすべてのPCにパッチを適用し社内規定に従ったポリシで運用を行うことはセキュリティ対策として非常に効果があるため[4]、NECでは2002年からサイバー攻撃防御システム(Cyber Attack Protection System:CAPS)を全社に適用し、すべてのPCを管理しています。

一方で、近年はパッチの公開からそのセキュリティホールを突くウイルスの発生までの間隔が狭まっており、パッチの逐次適用を確実に実施する必要が高まっています。

(3) PCの検疫

最新パッチの適用に対するタイムラグという弱点を克服し、さらに運用コストを削減するソリューションの1つにPCを検疫するという解があります。検疫を実施すると、PCの脆弱性の発見・パッチの即時適用・適用率向上・社内ポリシの適用など、組織内に統一したセキュリティポリシを強制することができます。この強制力により、セキュリティポリシの遵守状態を素早く全社均一に保つという、統制を実現できます。

2.2 検疫ネットワークシステム

検疫をすべてのPCに対して、ネットワークから効率的に行うのが検疫ネットワークシステムです。

(1) 検疫ネットワークシステムとは

検疫ネットワークシステムを導入すると、セキュリティポリシに適合したPCだけが基幹ネットワークを利用できます。また、適合しないPCを基幹ネットワークとは別に用意された検疫ネットワークに隔離し、セキュリティポリシを満たすための治療を行います。

(2) 検疫機能の4要素

検疫ネットワークシステムは、検査(監査)・隔離・治療・復帰の4つの要素で構成されます。**図1**では、各要素の概要についてまとめています。

①検査(監査)

PCのセキュリティポリシの遵守状況を確認します。一般的にはPC内に検疫機能用のエージェントソフトを導入し、チェック結果を検疫ポリシサーバへ送信します。事前にエージェントソフトウェアの導入が不要なエージェントレス方式もあり、エージェント利用を強制できないユーザのPCに対しても検疫を実行できます。

②隔離

セキュリティポリシに不適合と判断されたPCを検疫ネットワークに隔離します。隔離には、検疫ネットワークシステムと連携する装置の特徴から、複数の検疫方式があります。

③治療

隔離されたPCを、セキュリティポリシに適合させます。セキュリティパッチ適用やウイルスワクチン定義ファイルの更新、Winnyなどの使用禁止されているソフトウェアのアンインストールを自動・手動で行います。セキュリティポリシに準じた治療を行うため、検疫ネットワークシステムはパッチ配布製品やウイルス対策製品と連携します。

④復帰

隔離要因の治療が済んだPCを基幹ネットワークへ接続させます。一般には①検査に含める場合もありますが、再監査の結果に基づく基幹ネットワークへの復帰の簡易さが検疫の運用性に与える影響が大きいため、本稿では独立した要素として扱います。

(3) 検疫方式

この項では検疫の代表的な方式を5つにまとめます。**図2**は、隔離ポイントを含めた検疫ネットワークシステムの構成図を示しています。ここでは主に各方式での隔離と復帰の流れを説明します。

①認証VLAN方式

VLAN対応のネットワークスイッチを使い、VLANによるセグ

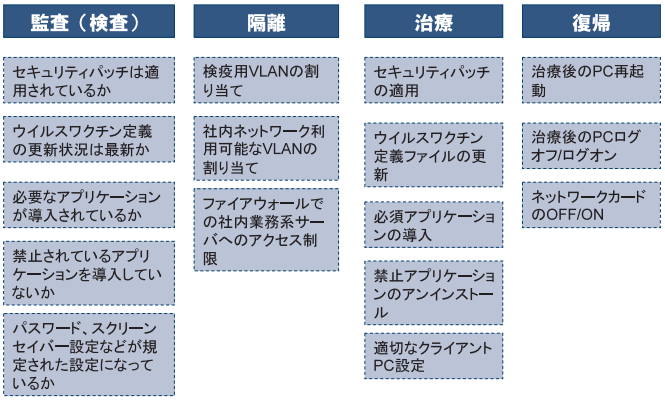

図1　検疫ネットワークシステムの要素

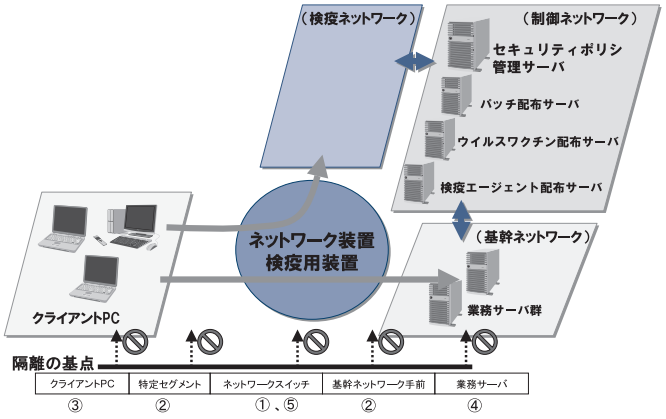

図2　検疫ネットワーク構成図

メントで検疫ネットワークと基幹ネットワークを分離します。ネットワーク接続時のIEEE802.1X認証やDHCP認証のタイミングで、ポリシ監査適合であれば基幹ネットワークへのVLANを割り当て、不適合であれば検疫ネットワークへのVLANを割り当てます。隔離されたPCは、治療され、再監査の結果ポリシ管理サーバへ適合情報を通知し、再認証のタイミングで基幹ネットワークのVLANを割り当てられます。再監査と再認証の際にユーザに行わせる操作をどれだけ減らせるかが課題として挙げられます。

②ゲートウェイ(GW)型ファイアウォール方式

PCと基幹ネットワーク間に設置するGWで隔離を行います。GW設置場所により、特定セグメントのみの検疫も可能です。ファイアウォールなどのGWのフィルタ操作で制御するため、固定IPアドレスでの利用環境に適しています。

隔離されたPCは、治療され、再監査が行われた時点で隔離を解除するため復帰時のユーザ操作はありません。

③クライアントファイアウォール方式

PCにインストールされているクライアントファイアウォールのフィルタ制御で検疫ネットワークへの接続を強制します。この方式もファイアウォールのフィルタ操作制御になるため、復帰時のユーザ操作はありません。

この方式では、クライアントファイアウォールなどのエージェントソフトが導入されていないと、PCの制御ができないため、PCのアプリケーション構成管理の徹底が必要です。

④サーバファイアウォール方式

業務サーバ上に専用ファイアウォールを導入することにより、業務サーバ自身でフィルタ制御を行います。ファイアウォールのフィルタ制御になるため、復帰時のユーザ操作はありません。監査適合になったPCのみ業務サーバへの接続を許可します。この方式では業務サーバ以外のネットワークへのアクセスは可能となるため、特定サーバのみを守りたいというニーズに適します。

⑤リモートアクセス方式

社外から社内へリモートアクセスする時に経由するスイッチで制御を行います。リモートアクセスのアクセス制御と監査を連携させて検疫ネットワークへの接続を強制します。他の方式と異なり、社外からアクセスする場合と社内からアクセスする場合でそれぞれのポリシが用意されるため、隔離する先も別にすることが求められる場合があります。この場合には、検疫の判断にもそれぞれ異なる管理が必要です。

(4) 検疫ネットワーク導入の効果

検疫ネットワークシステムを導入することで運用部門は以下の問題を解決できます。

- 持ち込まれるPCが検疫ネットワークに隔離されるため、PCにワームが入っていても、ワームの蔓延を阻止できる(リスク低減)
- セキュリティポリシが遵守されていないPCが隔離されるため、脆弱なPCがワームに感染するなどイントラネットを混乱させる事態を阻止できる(リスク低減)
- 検疫ネットワークへの隔離が自動的に行われ、このときにリスクのあるPC台数を掌握することができるので、管理工数を減らすことができる(運用コスト削減)
- 強制力を伴うため、セキュリティポリシの遵守を全社に浸透させることができる(統制力強化)

また利用するユーザにとっては以下の効果があります。

- 誤ってイントラネットに危険なPCを持ち込み、問題を起こして責任を問われるリスクを低減できる
- 常に最新のセキュリティレベルで社内ネットワークにPCを接続できるため、安心して業務に専念できる。

このように、運用部門、利用者ともに安心できる仕組みであり、ネットワーク全体でのセキュリティレベルが維持可能になります。

2.3 検疫にかかわる新しい動向

検疫ネットワークシステムは、2003年後半から注目され始めていました。シスコシステムズやマイクロソフトといった大手ベンダの検疫機能の実装に向けた提唱やアライアンスも活発化し、市場としても着実な増加が予測されています[5]。

2.4 標準化動向

検疫ネットワークを実現する鍵になるセキュリティポリシ管理サーバと隔離装置(ネットワークスイッチ等)の連携方法について標準仕様として3方式が提唱されています。

(1) NAC (Network Admission Control)

シスコシステムズが提唱している自己防衛型ネットワーク構想です。PCの検査で不適合を見つけると、ネットワークデバイスでアクセス制限を掛けます。ネットワークに接続される端末のセキュリティを既存のネットワーク機器で確保する、シスコ主導の業界アライアンスをベースとしたセキュ

リティソリューションです。3層(ネットワークレイヤ)でのネットワーク制御(NAC L3-IP方式)、2層(データリンクレイヤ)での制御(NAC L2-IP方式)、IEEE802.1X認証を加えた方式(NAC L2-802.1X方式)の3つの制御方式が用意されています。シスコルータをベースに広く使われていく可能性があります[6]。

(2) NAP (Network Access Protection)

マイクロソフト社の次期サーバOSとなるWindows Server "Longhorn" に組み込まれるポリシ強制プラットフォームです。NAP により、オペレーティング システムとウイルス対策の更新ポリシを設定し、PCがポリシに準拠していることを証明できるまで、そのPCによるネットワークへのアクセスを制限します。今後、Windowsサーバ環境において標準で使われるため、広く使われる可能性があります[7]。

(3) TNC (Trusted Network Connect)

安全なコンピュータプラットフォームの実現に向けた標準仕様の開発、普及を目的とした業界団体、Trusted Computing Group(TCG)が公開したセキュリティ仕様です。ベンダ主導のNACやNAPに対し、オープンな標準であることを強みとしています。あらゆるサードパーティに仕様が開かれており、特定の製品に縛られることなく、検疫の仕組みを実現できるため、多くの通信装置ベンダ、PCセキュリティベンダに支持されることが予想できます[8]。

3. 検疫ネットワーク導入のポイント

検疫ネットワークを導入するとき、検疫の方式と既存ネットワークとの関係を考慮すると利便性とセキュリティのバランスの取れたシステムを構築できます。費用対効果も踏まえて以下に導入のポイントをまとめます。

3.1 何を守るか?

検疫方式ごとに、隔離手段・隔離ポイントが異なります。そのため、検疫ネットワークで守りたい範囲を明確にしておく必要があります。「特定のサーバを守りたいのか」、「データセンタのような特定のネットワークを守りたいのか」、「イントラネット全体を守りたいのか」などを明確にします。

また、基幹ネットワークとは違い、検疫ネットワークにはウイルス・ワームが侵入する可能性が残るので、その際のリスク分析と対策検討が必要です。影響が及ぶ範囲を「PCのみにするのか」、「ユーザが接続するセグメント内にとどめるのか」などを明確にすることが検疫方式・製品選定に役立ちます。

3.2 どう隔離するか?

守りたい範囲を明確化した次は、隔離先の検討を行います。隔離する方式を、認証VLANとするか、フィルタリングによるアクセス制御とするかを検討します。次に検疫ネットワークの設計が課題となります。たとえば治療に用いるパッチ配布サーバ群を、運用コストと安全性のバランスとともに検討し、「ポリシ管理サーバと同じセグメントに1つ配置するのか」、「検疫・基幹それぞれ別のネットワーク上に配置するのか」を選定します。

3.3 部分導入・段階導入

外部PCが持ち込まれる可能性の高い職場やモバイルPCを標準利用している営業部門といった、特定のネットワークに対してだけに検疫ネットワークを導入することも可能で、導入コストを抑えリスクを低減させるための現実的な解となります。その際には、今後の拡張を考え、様々な検疫方式に対応した製品を選択することも重要です。導入する特定のネットワークごとに適した検疫方式を一元管理すれば運用コストを削減できます。

この際、既存のネットワークとの適合を十分に考慮する必要があります。たとえば、認証VLAN方式によるネットワーク認証と連携させる場合、VLAN対応装置が使われていないと、装置を購入する分だけコスト高となる傾向があります。しかし、無線LANなどで認証ネットワークが導入されていれば比較的安価に導入できます。

3.4 運用

検疫ネットワークシステムを導入したとき、毎朝一斉にPCを隔離するような運用は現実的でありません。隔離によりユーザの業務が停止するため、利便性、業務の遂行、問合せ対応、パッチやポリシ適用で起こるサーバ負荷の集中、ネットワーク負荷などを適切に制御する仕組みと運用設計が必要です。パッチの適用を例に挙げると、「毎日ネットワークに接続してパッチを適切に当てているユーザは、隔離されることなく業務を遂行できる」が実現できることが必要です。また、常時起動しているPCの定期的な監査や、長期持ち出しPCの隔離

も自動的に行われることが必要です。ユーザ利便性を損なわない運用設計には、ポリシ管理製品の選定が重要になります。

4. NECの検疫ソリューション

NECでは2004年8月から検疫製品(CapsSuite検疫連携オプション)を提供してきました。検疫方式のバリエーションも拡大しており、現在では主要な検疫方式を網羅しています。また、認証VLAN方式を使用し、社内で大規模実証実験を行い、検疫ネットワークの効果と実運用上での課題の確認を行いました。本稿で述べた課題事項を機能・運用の両側面から検討し、実証実験の結果をフィードバックした製品として、「CapsSuite/PC検疫システム」を2006年9月に製品化しています。

5. おわりに

検疫ネットワークについて、仕組みや技術動向、NECの取り組みについて述べました。NECでは、2007年度から検疫ネットワークの段階的な社内展開を検討しています。検疫ネットワークは、管理者・利用者の双方にメリットがあり、安心できるネットワークを維持できると考えます。今後は、NECが提唱する協調型セキュリティの一要素を担うInfoCage Networkシリーズの主要製品として、先進的なソリューションを市場に投入していく予定です。

＊ 本稿に記載されている会社名、製品名は各社の商標または登録商標です。

参考文献

1) 「企業における情報セキュリティ事象被害額調査」および「国内におけるコンピュータウイルス被害状況調査」、2005年、独立行政法人 情報処理推進機構(IPA)
http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html

2) コンピュータウイルス・不正アクセスの届出状況[11月分]について、独立行政法人 情報処理推進機構(IPA)
http://www.ipa.go.jp/security/txt/2006/12outline.html

3) W32/MSBlaster および W32/Welchi ウイルス被害に関する企業アンケート調査の結果について、情報処理振興事業会 (IPA/ISEC)
http://www.meti.go.jp/policy/netsecurity/Blaster_Survey.pdf

4) 岡崎久、「情報セキュリティ技術大全」、2002年、日経BP社

5) 「2006ネットワークセキュリティビジネス調査総覧」、p.214、2006年、富士キメラ総研

6) Network Admission Control シスコシステムズ
http://www.cisco.com/japanese/warp/public/3/jp/solution/netsol/security/nac/index.shtml

7) Windows 2003 Server ネットワークアクセス保護
http://www.microsoft.com/japan/windowsserver2003/technologies/networking/nap/default.mspx

8) Trusted Computing Group
https://www.trustedcomputinggroup.org/groups/network/

執筆者プロフィール

安留 良夫
システムソフトウェア事業本部
第一システムソフトウェア事業部

安達 智雄
システムソフトウェア事業本部
第一システムソフトウェア事業部
マネージャー

吉田 享之
システムソフトウェア事業本部
第一システムソフトウェア事業部
マネージャー