検疫システムの現状と標準とのギャップ
～悪意なき情報流失への対策～

東京エレクトロン株式会社
水本　真樹

組織のクライアントセキュリティ管理を取り巻く環境・制度が変わりつつある。ISMS、個人情報保護法によるクライアントPCの漏えい保護対策に対するニーズの高まり、日本版SOX法のITシステムへの影響など、今後も検討すべき点はある。
情報漏えい対策や企業のPCコンプライアンスを実現するために検疫ネットワークが注目されている。
実は検疫システムには標準が確立していない。各団体やベンダーから企業を中心とする組織に合うよう検疫ネットワーク標準が策定されつつあるというのが現状だ。
検疫ネットワークは、エンドユーザーの良識に任されがちなクライアントPCのセキュリティ対策をシステム側で管理するシステムだ。企業内ネットワークに接続しようとするクライアントPCに対して、ウイルス対策ソフトの起動の有無や定義ファイルのバージョン、パッチ適用の有無などのポリシーをチェックし、ここで「陽性」と判定されると接続を拒否。最新の定義ファイルをインストールするなどの「治療」を施してから、社内ネットワークへの接続を許す。
しかし実状は現段階の標準をベースとしたシステムでは要求にマッチしない場合が多い。どのような仕組みが必要とされるのか―検疫システムの構築経験を踏まえ考察する。

RSA Conference 2006

2006年2月、「RSA Conference 2006」がアメリカ サンノゼ カンファレンスセンターにて開催された。今回で記念すべき15周年を迎えるこのイベントは、情報セキュリティのプロフェッショナルをターゲットとしているセキュリティ技術をテーマとした世界最大のイベントだといえる。筆者が初めて参加したのは2001年の回だった。今回の寄稿にあたり当時の出張報告を読み直してみた。メインテーマはPKIで、当時のセキュリティ技術の中心。2001年はPKI元年と位置付けられてPKI関連のアプリケーションベンダーが数多く展示会に出展していた。

サンノゼ カンファレンスセンター（US）

ここ3年前から基調講演にマイクロソフト社のビル・ゲイツ氏が参加し始めたことが象徴的であるように、業界の動向が変わってきている。徐々にセキュリティ技術の中心がネットワーク・セキュリティ、エンドポイント、さらには企業のコンプライアンスを対象としてきている。

なお今回はシスコシステムズのジョン・チェンバース氏やサン・マイクロシステムのスコット・マクリーニー氏の皮肉たっぷりの講演、RSA暗号、Diffie-Hellman暗号など今日の暗号技術の考案者達によるパネルディスカッションなどあり非常に貴重だった。

この模様はWebキャストで閲覧可能なため、興味のある方は下記のURLにアクセスいただければと思う。
※ https://2006.rsaconference.com/us/conference/webcasts.aspx

さて、このConferenceでは17カテゴリの総計200クラスに及ぶEducational Trackが提供されている。4日間に及ぶこのセッションの中でも非常に多くテーマとして取り上げられていたのが企業のセキュリティ・ポリシーの遵守、とりわけ端末のセキュリティ管理とネットワーク接続制御だったと感じている。これらの核となるのが検疫ネットワークである。「Network Quarantine」や、「Endpoint Security」、単に「Network Access Control（NAC）」と分類されるものも同義と捉えて差し支えないと考えている。

後を絶たないウイルス感染による個人情報流出

さて、日本国内の情報漏えい事件に話を移す。つい先日も国家の機密情報を扱う組織から、私物パソコンに保存された秘密情報がウィルス感染によりネットワークに流出する、という事態が発生した。それ以外にも様々な組織で同様の事象が発生している。（次頁表参照）

各報道でさんざん取り上げられているはずのこういった事件。多くがファイル共有ソフト「Winny」のウイルス感染だと何かとニュースでも取り上げられるため、知っている方も多いだろう。特に本特集をご覧の方はセキュリティの知識としてもご存知だろう。ただ一般的な、ごく普通のパソコンユーザの場合はどうか。ピンとこない、というのが大半か、知人から「ゲームやソフト、音楽ファイルがダウンロードできるツールだ」として紹介されて軽い気持ちでインストールした結果、重大な事態を引き起こす可能性がある。「Antinny」やその亜種に感染した不運なユーザはマイドキュメント以下の重要な情報をWinnyネットワークに大放出して食い止められることのない個人情報流出被害が発生してしまうのだ。どこの組織でもセキュリティ規定策定や通達は行っているはずだ。つまりコンプライアンスのためのルールは存在しているのだが、往々にして遵守がなされない。すると事故も招きうるのだ。

別の側面だが国会では個人情報保護法改正案が提出されているようだ。個人情報を不正に漏らした企業の社員に対し「個人情報漏えい罪」を罰則規定として新設するというものである。成立かどうかは慎重に検討がなされるであろうが情勢は変化しつつある。

エンドポイントに必要とされる検査内容

組織には事故などの考えうるリスクに対し社会的責任を果たすための取り組みをどう行っているかを示すことが期待されている。情報漏えいが従業員への貸与端末や、ましてや個人の私用PCから発生しうるような取り組みでは、管理責任を問われても仕方がないであろう。検疫システムによる取り組みとしてWinnyをはじめとする不正なアプリケーションやプロセスの存在、固有のハードウェア情報による不正な端末の排除、ファイルの暗号化などの推奨設定を適切にチェックし未然にリスクを低減できることが必要とされる。

検疫と治療 ― 既存環境への適合

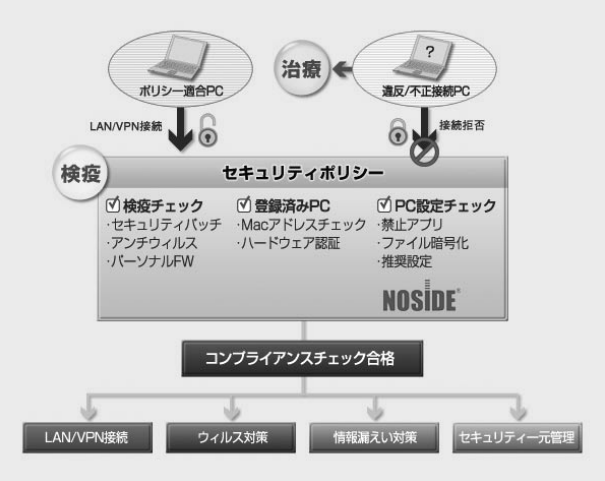
もちろんウイルス対策ソフトやOSパッチの適用状況のチェックも必須である。さらに不適合時の自動治療機能を提供すること、またシステムとして容易に日々更新されるパターンファイル番号やマイクロソフト社の月例パッチや累積パッチの変更・追加に追従できることが求められる。

この際、既存のウイルス対策ソフトの環境やパッ

最近の主なウイルス感染被害（報道発表記事より）

年月日	概要	詳細
2006/1	顧客情報が Winny に流出、私用 PC のウイルス感染が原因	コールセンタースタッフの私用 PC が Antinny に感染し、顧客情報を含む一部の業務ファイルが Winny 上に流出したことが明らかになった。
2005/12	再び Winny で情報流出、情報管理の徹底を指導	社員の個人所有 PC がウイルスに感染し、業務情報が Winny 上に流出したことを明らかにした。
2005/12	顧客情報、Winny で流出	同社社員が自宅で利用している PC が Winny に感染し、法人顧客の情報 82 件が流出したと発表した。
2005/12	取引先 104 件にウイルスメールを送信	一部顧客に対して、ウイルス「Netsky.P」を添付したメール 104 件を送信する事故が発生したと発表した。
2005/12	顧客リストが Winny に流出、私用 PC のウイルス感染で	同社が主催したイベントの案内送付先、286 社 528 名分の名刺情報が Winny ネットワークに流出したことを明らかにした。
2005/12	法人顧客情報などが Winny で流出、元社員の PC から	元社員の個人用 PC がウイルスに感染し、法人顧客と同社社員の情報、計 190 件が Winny ネットワークに流出した。
2005/12	顧客 7000 人にウイルス・メールを配信	同社のメール配信サービスに登録している顧客約 7000 人に対し、Worm_Netsky.P と呼ぶウイルスを添付したメールを配信した。
2005/12	PC のウイルス感染により生徒の個人情報を流出	生徒の個人情報が流出していることが判明したと発表した。原因は、パソコンのウイルス感染によるという。
2005/12	PC にウイルス感染、機密情報などが流出	自宅で使用している個人所有のパソコンへウイルスが感染し、業務上利用する暗証番号といった機密情報がインターネット上に流出したと発表した。
2005/12	私用 PC のウイルス感染で顧客情報が流出	職員の私用パソコンがウイルスに感染した事を原因とし、同社顧客情報 53 件がインターネット上に流出したと発表した。
2005/12	ウイルス感染で資料が流出	社員の私用パソコンがウイルスに感染し、技術資料などがインターネット上に流出したと発表した。
2005/11	ウイルス感染で Winny 上に個人情報を流出	社員が自宅で使用する私用パソコンにウイルスが感染し、顧客 2 名および社員 285 名の個人情報が Winny ネットワーク上へ流出したと発表した。
2005/11	設定ミスでユーザー 1518 人がワームに感染	会員向けに提供しているサービスのユーザーのうち、少なくとも 1518 名のパソコンが、同社のミスによってワーム型ウイルス「Sasser(サッサー)」に感染したことを明らかにした。さらに 2717 人のユーザーのパソコンに、ウイルスが感染を試みた形跡があったという。
2005/11	ショップが Winny で情報流出	ショップでユーザーの個人情報が流出したと発表した。スタッフが自宅で使用する個人所有の PC が Winny のウイルスに感染し、内部に保存していた情報が流出した。
2005/10	ウイルスで Winny 上に顧客情報が流出	県内の代理店において、Winny の感染により 4/4 ～ 9/29 の間、同店管理の 564 名分の顧客情報が Winny ネットワーク上に流出する事故が発生していたと発表した。
2005/9	ウイルス感染で Winny 上に顧客情報を流出	社員の個人パソコンがウイルスに感染し、137 件の顧客情報が記載されたリストが Winny ネットワーク上に流出したと発表した。
2005/9	また情報流出	個人パソコンが Winny に感染し、技術資料や出張手続きに関する書類が流出していたと発表した。
2005/9	ウイルス感染で Winny 上へ原発情報が流出	協力会社に所属する技術者のパソコンがウイルスに感染し、検査関連情報が Winny ネットワーク上に流出したと発表した。
2005/6	ウイルス感染により機密情報を流出	子会社の技術者が所有するパソコンがウイルスに感染し、同パソコンに保存されていた点検報告書などの機密情報が、Winny ネットワーク上に流出していた事実が、6 月 22 日に判明したと発表した。
2005/6	基地局情報が Winny で流出	管理する基地局情報が、Winny 経由で流出した。会社員が、情報を PC に入れて自宅に持ち帰り、Winny に感染したことが原因。
2005/5	メルマガ購読者にウイルスメールを大量転送	同社メールマガジン登録者 1 万 6233 人に対してウイルスメールを転送してしまったという事故が発生したことを発表した。今回転送されたウイルスは「NETSKY」の亜種などで、その対処法をサイトに掲載している。"
2005/5	PC のウイルス感染により一部の顧客にウイルスメールを送信	インターネット接続サービスにおいて、顧客対応用パソコンのウイルス「WORM_MYTOB.ED」への感染により、一部ユーザーへウイルスメールを配信したと発表した。
2005/4	ウイルス感染 PC から患者の個人情報が流出	かつて同院に在籍していた医師のパソコンから、2003 年 10 月 1 日から 2004 年 3 月 31 日の間に小児科に入院していた患者 63 名の個人情報が流出したと発表した。

チ管理システムとそのまま連携が取れることが好まれる。



検疫ネットワークの検査内容と機能概略図

検疫ネットワークの仕組みと必要性

ここで少し検疫ネットワークの話に戻す。「セキュリティの要件を満たしている端末だけネットワークに接続させる」―たったそれだけのことのようにも思えるが、インターネットを含むオープンなネットワークでは、この条件を満たすためのさまざまな仕組みが必要となる。

個人認証を例に取ると、LAN 接続認証、リモート VPN 接続やファイアウォール認証ログインなどの仕組みは、ユーザー名とパスワードなどを組み合わせ「本人しか知りえない情報を知っている」ことを「本人である」ということと関連付け、個人認証が得られたとして接続性を提供するという仕組みである。パスワードや個人を識別するための手法に十分な強度が確保できた場合には「本人である」ことは保証される。

このことと認証された本人が使用している「端末がセキュリティの要件を満たしているか」―特にウイルス対策ソフトや最新の OS アップデート、禁止アプリケーションの不使用や様々な推奨設定などの社内セキュリティ規定を怠りなく実施しているかというコンプライアンスの観点とは必ずしも一致しない。

こうした問題を解決するために検疫ネットワークソリューションの仕組みが今注目されている。これはネットワーク接続前に端末のセキュリティ要件をチェックし（検疫）、場合によっては接続制限を行い（隔離）、強制的にチェック項目を適用させて（治療）、さらに、認証が得られた場合に接続を許可する仕組みである。

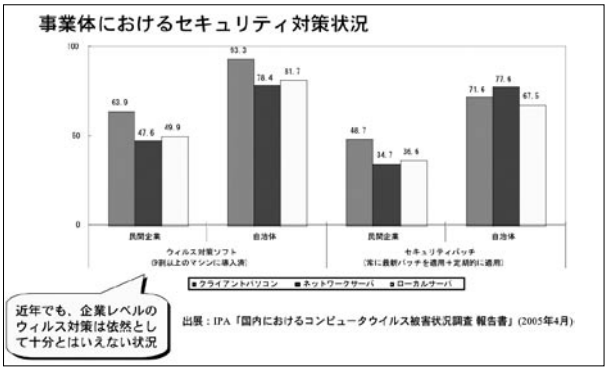
では企業のセキュリティ対策の実状は？

検疫システムの導入を検討している企業の一例を挙げる。提案や構築の経験から、ほぼ 3 パターンに分類される：

[大企業型]
大規模企業で、既に端末の標準化や体系的なパッチ管理、ウイルス対策や情報漏えい対策を行っている

[中企業型]
大～中規模な企業、もしくは教育機関などの組織で、システム管理部門の権限が弱くセキュリティ一元管理は行われていない

[管理外型]
管理外の端末、個人または各企業の端末が乗り入れるシステム



出展：IPA「国内におけるコンピュータウイルス被害状況調査 報告書」（2005 年 4 月）

細かく分析する。[大企業型] の場合は既に一元的に行われているセキュリティ対策の一環として導入を検討されるケースが多い。特長としては :

・Windows のパッチ適用・管理はコスト面から Windows 標準の Software Update Service（SUS）か Windows Server Update Service（WSUS） を採用
・標準端末化されていればパッチ管理とソフトウェア配布を兼ねるため専用のソリューションを採用
・大規模なほどエージェントの事前インストールは嫌われる
・同様に 802.1x は敷居が高い
・段階的に導入が可能な仕組みが好まれる
・ネットワーク機器の更改を要するスイッチベースの検疫は難しい
・シスコかマイクロソフトを待ちたいとは思う
・開発用など例外扱いの端末がある
・旧 OS の資産が結構存在している（Windows NT や 98 など）

[中企業型] の場合、管理者の方が苦慮しているケースが窺える :

・ウイルス対策ソフトはコーポレート版を導入済みだが、パッチ管理は個々のユーザの Windows Update 任せ
・資産管理やライセンス管理もシステム化されていない（管理者の調査による台帳管理）
・Active Directory 環境は存在していない、もしくは一部
・どうにかセキュリティ一元管理を行いたいと考えている

このように我々の知るセキュリティパッチ管理の実態と IPA での調査結果とほぼ一致していると考えられる。つまりまだ多くの組織ではルールを徹底する、というところまでたどり着いていないのだ。今後 PC コンプライアンスシステムとして検疫ネットワークが有効になるだろう。

検疫ネットワークの標準化動向

ここで、標準化動向にも触れておきたい。現在広く知られているものとして 3 つの標準化方式、およびその他の独自の実装が存在している。

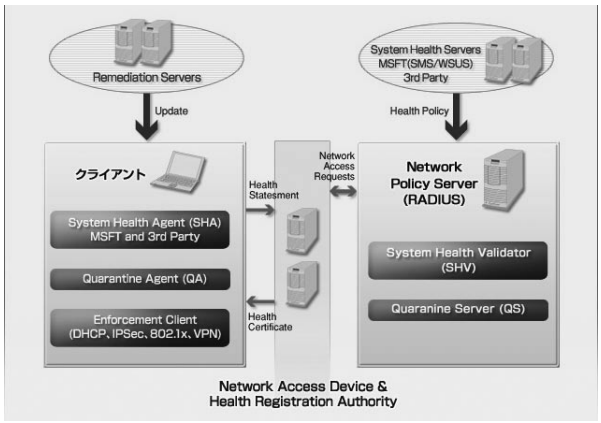
NAC（Network Admission Control）
シスコが提唱する、シスコのネットワーク製品をベースとしたエンドポイントセキュリティ管理のための標準規格。トレンドマイクロ、シマンテック、マカフィーをはじめとするベンダーが NAC パートナーとして参加。NAC Phase II で、スイッチベースの検疫システムに対応。

NAP（Network Access Protection）
マイクロソフトが提供予定のネットワーク検疫ソリューション。25 ベンダーの協業の元に、Longhorn Server で検疫ネットワーク対応機能を提供予定。2004/10/18 に NAC - NAP の互換性提供を発表。
Longhorn サーバと Vista クライアント間（ともにベータ中）で実現予定。

TNC（Trusted Network Connect）
米 Trusted Computing Group が 2005/5/3 に発表した、検疫ネットワークシステムに関するオープンな標準規格。HP、IBM、Sun、Symantec、Funk Software（現 Juniper Networks）等がメンバーとして参加

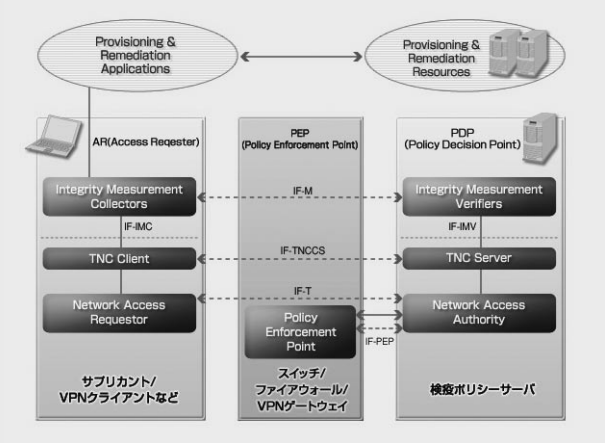
NAP に関して興味のある方は、今年リリース予定の Windows Vista バージョンと Longhorn サーバ（2007 年リリース予定）とを連携させた仕組みのベータ版テストが可能なはずである。様々な配置オプションやコンセプトなどを示したホワイトペーパーが公開されているので参考にしていただきたい。クライアントとネットワーク間の接続の制御方法として、802.1x

方式、DHCP 方式、VPN 方式、IPSec 方式などが存在する。この場合 Vista 標準のサプリカント機能、DHCP の場合は NAP に準拠した Longhorn などの DHCP サーバおよび DHCP クライアント機能と Network Policy Server（RADIUS）により、検疫時、ポリシー不適合時の制御を行う。この接続を治療に関しては Windows Server Update Services（WSUS）の機能を用いるか、サードパーティ性の検疫ポリシーサーバを連携させることになるだろう。



マイクロソフト Network Access Protection（NAP）概要

TNC は数十社からなるオープンな仕様であり、互換性や他の機能面で優れた設計思想を持っている。現在も TNC に準拠するいくつかの製品が実現されてきている。接続の制御を行うネットワーク機器やプロトコルを境界として、クライアント側の検査、接続制御層とサーバ側のポリシー検査、接続認証層を階層化しオープンなフレームワークを提供しているのが現段階のアーキテクチャだ。



Trusted Network Connect（TNC）概要

現段階で悪意あるユーザの悪意ある行動を防ぐ、というのは現実的に難しい。だが悪意なきユーザによる情報流出を水際で防ぐ可能性は検疫システムにより非常に高まる。現段階で導入が進んでいるもの、および既に稼働している検疫システムの多くは、下記のいずれかであろう。

1）パーソナルファイアウォールを中心としたシステム
2）認証 VLAN やゲートウェイを中心としたシステム
3）上記に DNS や DHCP、ホストスキャン、ARP や TCP リセットなどを組み合わせた方式

これらは前述の将来的な 3 つの標準と比較して、現時点の事実上の標準方式だといえる。ただこれらはユーザの操作に影響が及ぶことがあまり考慮されていない。例えば動作が重い、つながらない、余分な操作などがある。またこういった事実上の標準などによる分類だけでは図れない面がある。統一的な展開が図れない中規模な組織や、個人 PC や組織からみて管理外の機器が接続するシステムでは、導入時点でのハードルが多い。

悪意なき情報流出への対策として今後導入がより進むのは、導入や幅広い展開が容易なシステムになるだろう。