

検疫ネットワークソフトウェア iNetSec Inspection Center V3.0

Quarantine Network Software iNetSec Inspection Center V3.0

伊藤泰成 *
Yasunari Itoh

今福宏壮 *
Kousou Imafuku

吉岡直人 *
Naoto Yoshioka

濱野登志邦 *
Toshikuni Hamano

北井彦久 **
Hikohisa Kitai

* 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

** プロダクト本部 アプライアンス事業部 第一開発部

企業における情報セキュリティ対策の必要性の認識は高まっているものの、ウイルス対策ソフトウェアやファイアウォール等の導入が中心で、セキュリティポリシー策定や監査といったマネジメント面での対策は進んでいない。

検疫ネットワークは、社内ネットワークに接続するパソコンからのウイルスやワーム感染を防止する仕組みとして関心が集まったが、最近の市場動向および市場動向を踏まえた iNetSec Inspection Center の取り組みについて説明する。

While information security measures are becoming an increasingly urgent priority for most organizations, management response in terms of security policies and audits, has not kept pace, save for the piecemeal introduction of antivirus software and firewalls.

In light of this, quarantine networks are attracting interest as more stringent measures to protect internal PC networks from virus and worm infections. This paper discusses the recent market trends and our approach in developing iNetSec Inspection Center based on that trend.

1 まえがき

検疫ネットワークシステムは、社内ネットワークに接続するパソコンからのウイルスやワーム感染を防止する仕組みとして関心が集まったが、最近では単にウイルスやワーム感染防止だけではなく、学校・企業におけるセキュリティポリシーの維持・徹底を支援する仕組みとして関心を集めている。セキュリティポリシーについては、機能（ログインパスワード設定チェックなどセキュリティ監査機能など）、隔離方法（検疫 NG でも隔離しないなど）など業種によって多様なニーズが出てきている。

またネットワーク制御方式として市場から非常に関心の高い Cisco Systems 社の NAC^{注1)}に対応した製

品も出始めている。

本稿では、検疫ネットワークシステムの市場動向および市場動向を踏まえた検疫ソフトウェア「iNetSec Inspection Center」^{※1)}のねらいと特長、今後の取り組みなどを紹介する。

2 検疫ネットワークの市場動向

当社が 2004 年 7 月に「PFU 検疫ネットワークシステム」の販売を開始してからの、検疫ネットワークの市場環境変化について述べる。

図 - 1 は、日経 BP 社の発行する各雑誌に掲載された「検疫ネットワーク」に言及した記事数を 4 半期ごとに集計^{注2)}したものである。

2004 年に急激に立ち上がった検疫ネットワークへ

注 1) Cisco Systems NAC

NAC (Network Admission Control) ソリューションは、ネットワークに接続するデバイスがネットワークセキュリティポリシーに適合しているか確認することで、ネットワークアクセスを制御する仕組みで、米国 Cisco Systems が主導するマルチパートナープログラムである。

注 2) 「検疫ネットワーク」という文字列を日経 BP 社発行雑誌記事より全文検索し、ヒットした記事の数 (2006 年 2 月 20 日現在)。当社調べ。

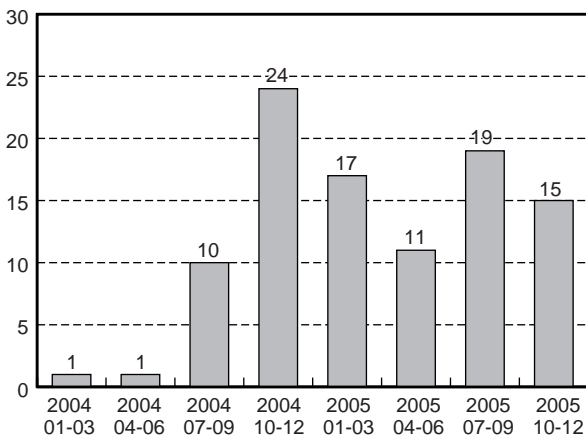


図 1 「検疫ネットワーク」記事掲載数
(Fig.1-Number of articles concerning " quarantine networks ")

の関心は 2004 年下期にいったんピークに達している。当時の検疫ネットワークへの期待は、Blaster 等のウイルスの進入を水際で阻止するというウイルス対策の面が比較的強調されていた。

当社製品^{※2)}も 2004 年 7 月の初版出荷、2004 年 12 月の機能強化とこの関心の高まりの中で多くの導入をいただいた。実際に導入を検討されているお客さまや、導入し運用を開始したお客さまとの会話から得たその後の市場環境の変化としては以下があげられる。

(1) 情報漏えいリスクのクローズアップ

個人情報保護法の施行ともあいまって、企業内の情報システムへのニーズが多少の運用性を犠牲にしても安全性を高めるニーズが現れてきた。

管理されたクライアントに管理されたソフトウェアのみを搭載し、管理外のクライアントは検査するまでもなく接続を拒否する、というような運用も一般的になってきた。

(2) セキュリティ知識の向上ニーズ

大学など、管理外のクライアントを接続・運用させざるを得ない環境では、隔離はしないまでも、クライアント検査を実行して、セキュリティ知識を高めるための警告や猶予期間等を求められるようになった。

(3) より多様なネットワークへの適用

当社で従来提供してきた認証スイッチ方式、802.1x 方式に加えて、より安価な機器や既設の設備を利用した方式へのニーズが高まってきた。

このように、検疫ネットワークに期待される機能は一樣ではなく、隔離・検査・対処等の機能ごとに、より多様なポリシーを求められるように変化してきた。これも検疫ネットワークがより一般的に受け入れられてきた

ことを示すと考えられる。広がってきたニーズに対して、よりきめ細かいセキュリティポリシーの遵守を、より少ないコストで運用できることが、検疫ネットワークシステムに求められている。

3 エンハンスの狙い

2004 年 7 月の iNetSec Inspection Center V1.0 の販売開始から V2.0 にかけては、下記のように検疫システムとしての基本機能を中心に提供してきた。

(1) セキュリティ対策の徹底

Windows^{※3)} OS のセキュリティパッチ、ウイルス対策ソフトのパターンファイルが適切かをチェックし、セキュリティレベルの低いクライアント PC を業務ネットワークに接続させない。

(2) 不正接続防止

社内で管理されていない持込み PC をネットワーク接続させない。

(3) 容易な導入

インストールレスクライアントの提供、既存ネットワークの変更が不要な認証ゲートウェイ方式の採用

(4) ネットワークエッジ (PC 単位) での検疫

IEEE 802.1x 認証 VLAN スイッチを利用し、TCP/IP 通信が可能となる前に検疫を実施。よりセキュリティの高い検疫が可能。

このような基本機能の充実が市場に評価され、2006 年 3 月末時点で累計数万クライアントの販売に至っている。

Version 2.0 までも非常に好評を頂いていたが、既存のお客さまやパートナー様へのヒアリング活動を通じて、更なるニーズ (課題) を抽出した。

(1) セキュリティポリシー維持徹底

個人情報保護法対策として、各種セキュリティソフトウェアの導入やスクリーンセーバーパスワード設定などを指導しているが、導入後の遵守状況が把握できない。導入後の遵守状況を把握したい。

(2) 管理者の負荷軽減

検疫辞書配付サービス (メール送付) により、管理者の負荷はかなり軽減されているが、毎日の辞書更新が大変。

注 3) Windows 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) Cisco Systems の NAC への対応

Cisco Systems 社製の機器だけで構成されているフロアでは NAC で検査を行いたい。

これらの課題及び市場動向を踏まえ、V3.0 の開発を行うことにした。

3.1 検査項目の拡充

V2.0 までのセキュリティパッチ適用状況、ウイルスパターン更新状況、義務付けソフトウェアの導入状況などの検査に加え、パーソナルファイアウォールの設定状況、ウイルス対策ソフトウェアのリアルタイムスキャン設定状況、Windows 及びスクリーンセーバーのパスワード設定状況を検査する機能を提供する。また、ユーザーが独自の検査項目を追加できるように任意のレジストリやファイルパス名の検査機能を提供する。

これまで目視などで確認していた、これら検査項目の拡充により、セキュリティポリシーの維持コストを大幅削減するとともにセキュリティポリシーを徹底することが可能となる。

3.2 運用性改善

「PFU 検査ネットワークシステム」では、専任のサーベスタッフにより検査辞書を作成し、システム運用管理者向けのメール配信サービスとして「検査辞書配信サービス^{注4)}」を提供してきた。しかし、メールによる配信では、毎日の辞書更新と PC セキュリティポリシーをサーバ上で手動設定する必要があり、運用管理者の負荷となっていた。V3.0 では、検査辞書の自動更新、PC セキュリティポリシーの自動設定機能を提供することにより、検査ネットワークシステムの自動運転を可能とした。

また、検査状況などの統計データをレポートする機能や検査結果が不適切な場合でも警告表示のみ行い隔離しない猶予期間を設ける「警告モード」を提供することにより、システム運用管理者への問合せを減らすとともに、一般利用者の業務効率を下げることなく導入や運用が可能となる。

注4) 検査辞書配信サービス

検査ソフトウェアでは検査辞書（セキュリティパッチ、ウイルスパターンの情報）により、企業セキュリティポリシーに応じた検査ポリシーを設定できる。検査辞書配信サービスは、常に最新の検査辞書を運用管理者に提供している。

3.3 ネットワーク利用性拡大

従来の米国 Top Layer Networks, Inc. 社製ネットワーク認証機器「Secure Controller」による認証ゲートウェイ方式、各社スイッチを使った IEEE802.1x 認証 VLAN 方式に加え、米国 Cisco Systems の NAC Phase2 方式に対応することで、企業内のネットワーク環境に応じた最適なシステム構築が可能となる。iNetSec Inspection Center を利用することで、これら 3 方式の混在環境でも、シームレスに管理や運用が可能となる。

4 検査項目の拡充

多様化された企業ネットワークのセキュリティマネジメントニーズに応えるため、今回のエンハンスでは従来の「Windows OS のセキュリティパッチ適用検査」、「ウイルス対策ソフトウェアの導入およびパターンファイルの適用検査」、そして「必須ソフトウェアの導入検査」の検査項目に加え、以下の検査項目をサポートして検査項目の拡充を行い、よりニーズに即したセキュリティマネジメントの実現を図った。

(1) スクリーンセーバーパスワード設定検査

情報漏えい対策の第一歩として、パソコンから離れたときに第三者に不正利用されたり画面を覗かれたりすることを防ぐために、スクリーンセーバーをパスワードでロックする運用を徹底する必要がある。スクリーンセーバーパスワードの設定状況およびスクリーンセーバー起動までの待ち時間の検査により、情報漏えいを防止する意識を高めることを図った。

(2) Windows ログオンパスワード設定検査

セキュリティ対策の基本である Windows ログオンパスワードの設定状況の検査をサポートした。セキュリティに対する意識が低いパソコン利用者は往々にしてログイン名とパスワードを同一にしがちであるが、Windows ログオンパスワード設定検査ではログイン名がパスワードと同一かどうか、および自動ログオン設定が有効になっていないかどうかを検査し、パスワード設定に対する意識を高め、注意を払うように徹底することを図った。

(3) パーソナルファイアウォール設定検査

Windows XP SP2 以降で標準装備された Microsoft Windows ファイアウォール機能、あるいは導入されているウイルス対策ソフトウェアが持つパーソナルファイアウォール機能を有効にしているかどうか

を検査し、パーソナルファイアウォールの運用を徹底することを図った。

(4) ウイルス対策ソフトウェアのリアルタイムスキャン設定検査

ウイルス対策ソフトウェアを導入してパターンファイルを更新していても、実際にパソコンのウイルススキャンを実行していないと、いざウイルスが侵入したときに防ぎようがない。リアルタイムスキャン機能を有効にする設定を徹底させることにより、より強固なウイルス対策の実現を図った。

5 運用性の改善

運用管理者およびパソコン利用者の運用コストを最小化（ゼロアドミニストレーション）すると共に、セキュリティマネジメントのPDCAサイクルの運用をより効率よく実施することを目的に、今回のエンハンスでは以下の機能強化を実施した。なお、セキュリティマネジメントのPDCAサイクルを図-2に示す。

(1) 辞書自動ダウンロード機能

従来より、高い知識を要するセキュリティパッチやウイルスパターンの検査内容を検疫辞書として配付するサービスを提供しているが、運用管理者は配付された辞書をシステムに取り込む、日々の業務が必要であった。今回、独自に辞書ダウンロードセンターを立ち上げて更新された辞書を自動的にダウンロードしてシステムに反映する機能を実装し、運用管理者の辞書に対する運用負担を軽減した。また、辞書ダウンロードセンターとの通信はSSLによる暗号化通信、センターの認証で辞書の改竄を防止している。

(2) ポリシーの自動設定機能

ゼロアドミニストレーションを目的とした機能の二つ目として、検疫ポリシーを自動的に設定する機能を実装した。セキュリティパッチなどの辞書が更新されて、

新しい検査対象のパッチが増えた場合に新規増加分のパッチを検疫対象とするか否かの検疫ポリシーを予め設定されたセキュリティポリシーに従って自動的に設定する。また、よりスムーズに検疫ネットワークの運用が行えるように、検疫対象とするまでの期間も設定できるようにした。例えば、辞書が更新された3日後から、新規検査対象のパッチを自動的に検査対象にする、という運用が可能である。

(3) 検疫 NG 時警告通知機能

一般的に、運用管理者が新しいセキュリティポリシーを適用した場合や Microsoft 社から Windows OS のセキュリティパッチが公開された場合は、パソコン利用者がそのセキュリティポリシーに対応するまでに1~2日の猶予期間が必要となる。また、資源配付ソフトウェアを利用してセキュリティパッチを配付している環境でも、末端のパソコンまでパッチが行き渡るまでにやはり1~2日を要する。特に出張者が多い職場環境であれば、これが3~4日かかる場合も常である。そこで、今回のエンハンスでは検疫 NG 時の警告通知機能をサポートした。この機能を用いれば、検疫 NG 時にはパソコン利用者にセキュリティに問題がある旨を通知してセキュリティの更新を促すが、いきなり隔離するのではなく、業務ネットワークへ接続する猶予期間を設けることができる。また、ポリシーの自動設定機能と組み合わせることで、セキュリティパッチが Microsoft 社から公開された翌日から警告での猶予期間運用を行い、5日経過した時点で検疫+隔離の対象とするといった運用が自動で実施できる。

(4) 検疫 NG 時の自動対処実行機能

パソコン利用者のゼロアドミニストレーションを目的に、検疫 NG 時の自動対処実行機能をサポートした。この機能は、クライアントで検疫 NG が検出されたときに、セキュリティ更新用のコマンドをクライアントで実行する機能である。この機能を用いれば、検疫 NG になったときに自動的に WSUS (Windows Server Update Services) のパッチ適用コマンドを起動し、検疫 NG の要因となった不足パッチを自動適用したり、ウイルス対策ソフトウェアのパターンファイルダウンロード機能を実行し、自動的にパターンファイルを更新するなどのセキュリティ対策をパソコン利用者の運用負担をかけずに実施できる。

(5) レポート機能

iNetSec Inspection Center V3.0 では、4種類のレポートを用意した。

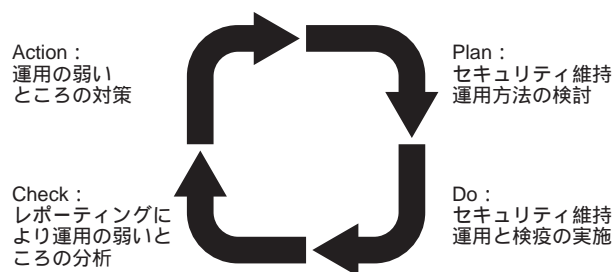


図 2 セキュリティマネジメントのPDCAサイクル (Fig.2-PDCA cycle of security management)

1) 接続クライアント数集計

指定期間内に接続したクライアント数の推移を確認する。クライアント数はユニークな数で集計して、指定期間内では同一クライアントを1クライアントとしてカウントする。

2) クライアント別セキュリティ情報報告

クライアント毎に指定期間内の検疫結果情報を集計する。このレポートでクライアント毎、更には部門毎のセキュリティレベルを把握して、セキュリティマネージメントの実施状況の分析を支援する。

3) 検疫 NG 要因別セキュリティ情報報告

指定期間内で、検疫 NG になった要因別にクライアント数を集計する。このレポートでセキュリティ監査項目毎の検疫 NG の多さ、少なさを把握して、セキュリティ対策の運用が弱い部分を見出すことができる。

4) 時系列検疫状況報告

接続クライアントの検疫・認証状況を時系列に閲覧できる。

今回サポートしたレポート機能 (PDCA の Check) を元に運用上の弱点を分析し、改善していくことで、セキュリティマネージメントの PDCA サイクルを低コスト、かつ容易に運営していくことが出来るようになった (図 - 2 参照)。

(6) クライアントアップデート機能

iNetSec Inspection Center V3.0 L10 からは、クライアントモジュールの自動アップデート機能をサポートした。この機能により、検疫クライアントのマイナーエンハンスやバージョンアップを実施したクライアントがリリースされたときに、パソコン利用者の負担なく、クライアントの更新が可能である。

6 多様なネットワーク環境に柔軟に対応

iNetSec Inspection Center は、マルチベンダーサポートを特長として、当初から様々なネットワーク機器や検疫方式に対応してきたが、今回のエンハンスでは高いニーズがある米 Cisco Systems, Inc. 社の NAC Phase2 方式をサポートした。NAC Phase2 方式では従来の NAC Phase1 でサポートされていた、ルータでの検疫および VPN 装置での検疫に加え、802.1X 認証 VLAN スイッチでの検疫をサポートする。従来の検疫方式に加えて Cisco NAC 方式をサポートするこ

とにより、ほぼあらゆるネットワークモデルでの検疫に柔軟に対応できる。

NAC 方式の検疫では、Cisco 社の CTA (Cisco Trust Agent) と iNetSec Inspection Center 検疫クライアントをクライアント PC にインストールし、NAC 対応ネットワーク機器を通して Cisco ACS (Access Control Server) と通信して検疫を実施する。サーバ側では Cisco ACS が iNetSec Inspection Center 検疫サーバを呼び出して、検疫結果の通知を受け、その結果に応じて Cisco NAC 対応ネットワーク機器の制御を行う。

Cisco NAC 方式の構成を図 - 3 に示す。

7 適用例

セキュリティポリシーの維持・徹底を支援する適用例として、ウィルスやワーム感染防止以外の適用例を 2 例示す。

- 1) セキュリティレベル検査・警告表示
- 2) 不正接続パソコン排除

7.1 セキュリティレベル検査・警告表示

セキュリティレベルの監査を実施したい場合、検疫ソフトウェアのみで監査する適用例を示す。

利用シーンとしては、学内または社内ポータルサイ

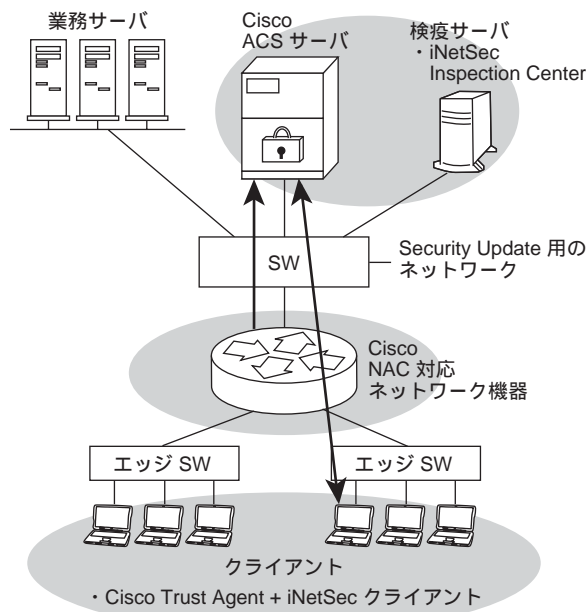


図 3 Cisco NAC 方式の構成 (Fig.3-Configuration of Cisco NAC method)

トアクセス時に検査ソフトウェアで PC のセキュリティ状態を自動チェックする例である。

(1) 導入効果

ネットワーク機器と連携しないため、検査 NG でもネットワークから隔離されないが、セキュリティポリシーの維持・徹底とセキュリティレベルの監査コストの削減が図れる。また初期導入コストの削減が可能。

(2) 運用

- 1) 学内または社内ポータルサイトを検査サーバのサイトにする。
- 2) ポータルサイトアクセス時に PC のセキュリティの状態をチェックする。
- 3) 各パソコンのチェック結果をロギングする。
- 4) チェック結果が OK の場合は、学内または社内ポータルサイトを表示する。
- 5) チェック結果が NG の場合は、ネットワーク接続を拒否しないが、警告メッセージをパソコン上に表示し、セキュリティ対策ページ等へ誘導する。

(3) システム概要

図 - 4 にセキュリティレベル検査・警告表示システムの構成例を示す。

7.2 不正接続パソコン排除

(1) 概要

社内ネットワークに管理対象外のパソコンを接続させたくない場合の適用例を示す。

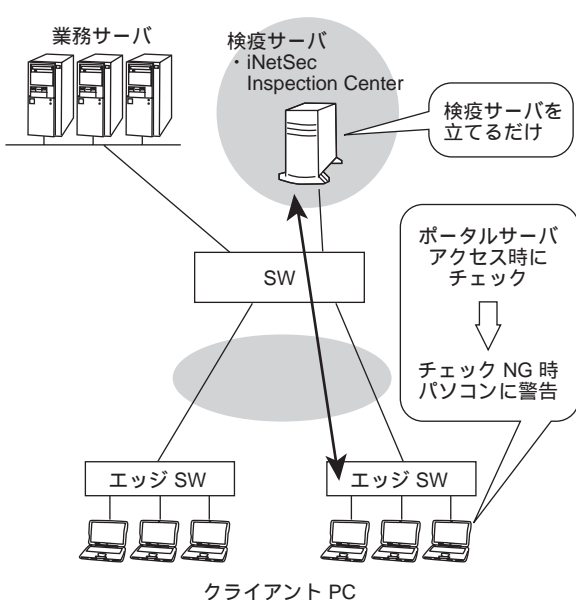


図 4 セキュリティレベル検査・警告表示システム構成例
(Fig.4-Example configuration of a security level check/warning display system)

管理対象かどうかは、MAC アドレスが登録されているかどうかで判断し、管理対象外の PC アクセス時には、ネットワークから隔離する。

(2) 導入効果

社内ネットワークへの不正侵入、持ち込みパソコンの排除が図れる。

(3) 運用

- 1) ポータルサイトアクセス時（業務ネットワークアクセス時）に登録済みパソコンかどうか自動チェックする。
- 2) 管理対象外のパソコンの場合、ネットワークへの接続を拒否する。

システム運用にあたっては、以下の考慮をすることで運用コストの削減ができる。

- 1) 資産管理ツールとの連携で管理対象パソコンかを判断することにより運用コスト削減が図れる。
- 2) 協力会社の出入りが頻繁な企業は、その都度 MAC アドレスを登録する必要があり、運用管理負荷が高い。協力会社員が業務ネットワークに接続する場合、あらかじめ登録済みの LAN カード（PCMCIA / USB など）を借り受け、ネットワーク接続を行うことで、運用管理負荷軽減が図れる。

(4) システム概要

図 - 5 に不正接続パソコンを排除するシステムの構成例を示す。

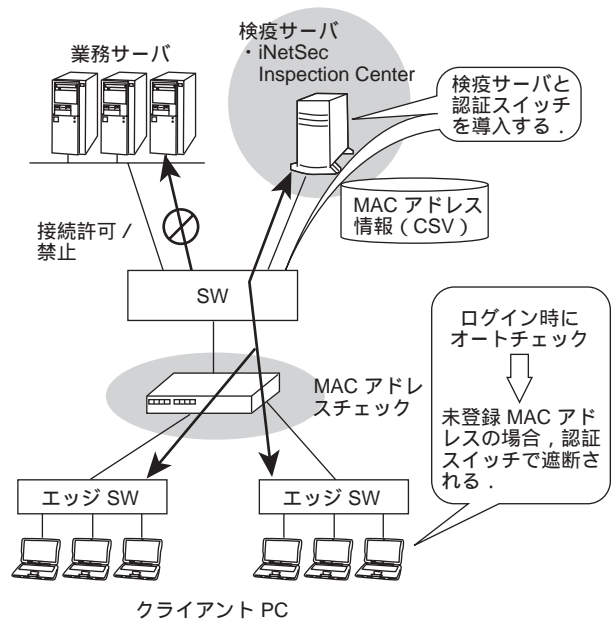


図 5 不正接続パソコン排除システム構成例
(Fig.5-Example configuration of a system to reject unauthorized connections from PCs)

8 むすび

個人情報保護法などへの対応として、多くの企業がセキュリティポリシーを策定し、ディスク暗号化ソフトウェアなど個々のポリシー実現のためのツールを導入している。しかしながら、導入後に必要なソフトウェアが導入されているかなどのチェックと対策（PDCA サイクルにおける CA）を入手に頼っていて、企業内セキュリティポリシーの維持徹底に多大な工数をかけている場合が多いと推測される。

iNetSec Inspection Center では、企業におけるセキュリティポリシーの維持と徹底を、システム管理者

や一般利用者の負荷とならないよう支援していきたいと考えている。

また、当社では IT 技術を通し「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

- 参 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/>
- 参 2) 平松，濱野，高橋：検疫ソフトウェア iNetSec Inspection Center，*PFU Tech.Rev.*，16,1,pp.29-34（2005）。