不正プログラム調査 WG　平成 15 年度成果物

不正プログラム対策ガイドライン

NPO　日本ネットワークセキュリティ協会
2003年度　不正プログラム調査ワーキンググループ
平成 16 年 3 月

目次

1

はじめに

最近、コンピュータウイルスやワーム以外に個人や企業に実害をもたらす不正プログラムによる問題がクローズアップされています。それらの不正プログラムには、知らないうちにシステムから個人情報を盗み取る「キーロガー」や「スパイウェア」、不正アクセスを行う目的で利用される「ハッカーツール」や「トロイの木馬」などの悪質なものが多くあります。

例えば、「キーロガー」がシステムに仕込まれると、キーボードの入力が筒抜けになったり、また「スパイウェア」が侵入するとシステムに登録している氏名や住所、メールアドレスなどの個人情報や、Web の閲覧履歴などが収集され、犯人にメールなどでその情報を送信されてしまいます。これを使用してパスワードが盗まれネットバンキングから大金が引き出される事件などがおきています。

平成 12 年より警察庁が毎年行っている「不正アクセス対策の調査」によると、情報セキュリティ被害の過半数がウイルス感染などの不正プログラムに起因しております。

また、「ハッカーツール」や「トロイの木馬」は不正アクセスを行うために犯人が利用するものなので一般ユーザには関係が無いと思われがちです。実はこれらのツールは企業ユーザはもちろん、個人ユーザのシステムに、知らない間に仕掛けられ不正アクセスに必要な情報を犯人に提供していたり、間接的に他のコンピュータに対して不正侵入や攻撃をすることで加害者となってしまうのです。このように他人のコンピュータを踏み台にすることは、犯人が自分の足跡を追跡されないようにするための常套手段なのです。

これらの不正プログラムが自分のシステムに仕掛けられている状態で、外部から組織内へ通信をしたり、組織内でネットワークに接続したらどうなるでしょう？ 組織に与える被害は、システムの停止、営業機会の喪失、訴訟問題、信用の失墜など計り知れないものがあります。

2 不正プログラムの定義

ここでは不正プログラムを「個人またはシステム管理者の意図しないところで、破壊、盗聴、侵入、迷惑、感染などの不正な動作をするプログラム」と定義します。

また、ネットワーク管理ツールなどで、正規の目的があり、使用者によっては不正な使用が可能であるものや、一般的にジョークプログラムと言われているものは、不正プログラムには含まないことにします。なお、プログラムの瑕疵に起因するユーザの意図しない動作も対象外とします。ただし、通常のアプリケーションであっても、使用者に不利益な機能が隠れて動作する場合は、その限りではありません。

経済産業省では、通商産業省告示 第 952 号「コンピュータウイルス対策基準」でウイルスを下記のように定義しています。「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の一つ以上有するもの 」としています。

- ■ 自己伝染機能
  自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能。
- ■ 潜伏機能
  発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能。
- ■ 発病機能
  プログラムやデータ等のファイルの破壊を行なったり、コンピュータに異常な動作をさせるなどの機能。

また、総務省の「国民のための情報セキュリティサイト」では、以下のようなセキュリティ用語解説をしています。

- ■ ウイルス
  他人のコンピュータシステムの破壊やいたずら目的で作られた特殊なプログラム。コンピュータウイルスとも呼ばれています。多くのウイルスが、感染活動のために、自分自身を複製する仕組みを持ち、ウイルスが埋め込まれた電子メールやホームページの閲覧を通して次々と増殖します。
- ■ トロイの木馬
  コンピュータの内部に潜伏して、外部からの不正侵入を助けたり、そのコンピュータの情報を外部に発信したりするタイプのウイルス。
- ■ ワーム
  ほかのファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルス。

3　不正プログラムの分類

ここでは不正プログラムを、攻撃者側で実行されるものと、被害者側で実行されるものに大別します。さらに、被害者側で実行されるものを、自己増殖する「コンピュータウイルス」や「コンピュータワーム」と、

自己増殖しない「トロイの木馬」に小分類しました。(図 3.1:参照)

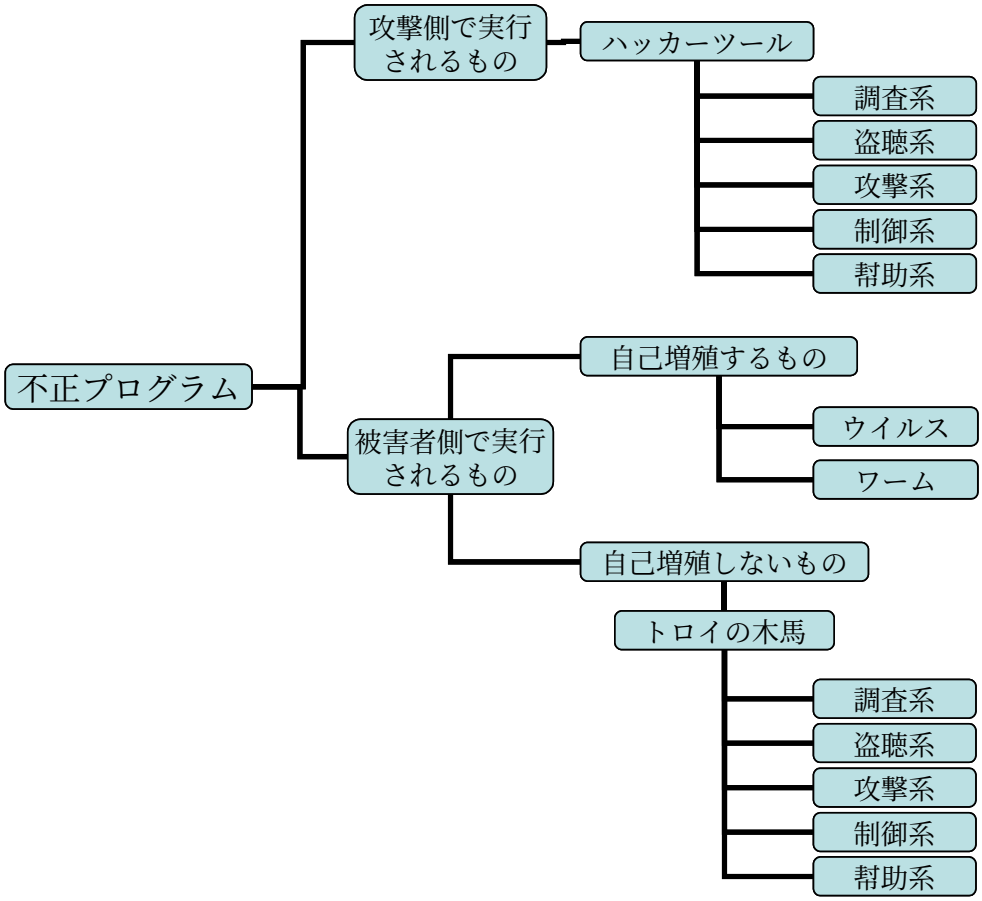

図 3.1　不正プログラムの分類

例えば、スパイウェアやキーロガーと呼ばれる不正プログラムは、ここではトロイの木馬の盗聴系に属します。最近ではコンピュータウイルスやワームであって発病症状としてトロイの木馬やハッカーツールなど複合的な機能を有するものも増加してきています。

4　不正プログラムの構造

ハッカーツールやトロイの木馬とウイルスやワームとの決定的な違いは、自己増殖するかどうかです。ウイルスは正常なプログラムやマクロ機能のあるデータファイルに取りつき感染します。また、ワームは自分自身をコピーし増殖します。一方、ハッカーツールやトロイの木馬は増殖をしない独立したアプリケーションである場合が多く、パソコンにインストールされます。

また、現在国内で確認されるウイルスやワームの多くは海外で作成されるもので、国内産のものはほとんどありません（過去に国内産もわずかながら確認されました）。一方、トロイの木馬やハッカーツールなどは、日本人作者のものも多く、インターネットなどで入手が容易です。

トロイの木馬は、盗聴・不正侵入・攻撃といった実被害が目的で、その性質上、姿を隠しているものが多いために発見が困難です。また、一度組み込まれると、継続的な機密情報の漏洩など、その被害は長期的かつ多大なものになります。一方、ウイルスやワームは個人がいたずら目的で配布する愉快犯的なものが多く、自己増殖する性質上、発見が簡単です。その被害数は他の脅威に比べると圧倒的に多いのですが、感染のみで実被害がない場合はそれほど大きなものになりません。仮に感染被害が大規模であっても、復旧のために数日ネットワークを止めた場合の復旧費用と、その間の営業機会の喪失といった一時的なものです。

表 4.1　ウイルス・ワームとトロイの木馬の違い

	原産地	見つけ易さ	被害期間	被害数	被害額
ウイルス、ワーム	海外産	簡単	短期的なもの	多大	少ない
トロイの木馬、ハッカーツール等	海外産＋日本産	困難	長期にわたる	少ない	多大

ウイルスはどんなコンピュータユーザにとっても有害なものですが、ハッカーツールやトロイの木馬は使う人や使い方によって、有益にも有害にもなりうるものです。例えば、スパイウェアの機能も通常のアプリケーションに含まれる場合があります。ユーザのシステム情報やエラー情報、機能やコンテンツの利用頻度などを集めて、機能修正や追加、ユーザサポートのための統計情報として利用している場合などです。

このような商用で利用されているスパイウェアは、ソフト導入時の「使用許諾条件」や Web ページの「プライバシー条項」などで、統計目的で個人情報を集めることを明記しており違法とはいえません。しかし、ソフトウェアのインストール時や、Web 閲覧時にそれらの注意書きを読まない人が多く、知らないうちにインストールしてしまうのが現状です。

また、キーロガーの場合、企業の管理者が商用のキーロガーを個人のパソコンに導入し社員の監視目的で使用する場合があります。同様に「パケットアナライザ」（ネットワーク上に流れるデータを監視できる）や「脆弱性検知ツール」（セキュリティホールを検出する）などのネットワーク管理ツールの多くが、使用する人によってはハッカーツールに簡単になってしまい両刃の剣といえます。

表 4.2　目的別各ツールの用途

	好意的な使用	悪意ある使用
スパイウェア	システムの稼動監視 ユーザサポート支援	重要情報の不正取得
キーロガー	ユーザの動向監視	パスワードの不正取得
パケットアナライザ	ネットワーク管理支援 トラブル対応	パスワードや重要なデータの 不正取得
脆弱性検知ツール	セキュリティレベルの管理	攻撃対象の選定

ところが、ハッカーツールやトロイの木馬の多くが既存のセキュリティツールで検出できないという問題点があります。例えば、ウイルス対策ソフトの場合、トロイの木馬を検出し駆除するための構造になっていないために網羅的な対応が困難です。それでも、明らかに危険なもの、話題性のあるもの、緊急性のあるものについては既にウイルス対策ソフトで対応していますが、管理ツールのような危険性を明確にできないツールについては性格上対応できないと思われます。

5　不正プログラム対策

5.1 セキュリティルールの策定

実害を組織や個人に与える不正プログラム、その自衛の策には、2 つの方法があります。まずは、WEB 閲覧やメールの閲覧などに関して、一定のセキュリティルールを自分で守ること。実際、ウイルス感染にせよトロイの木馬の侵入にせよ、非常に基本的なネット上のルールが守られていないがために起こっている場合が非常に多く、まずそのルールを知り、守ることは非常に大切です。

そして次に専用ツールの導入が考えられます。スパイウェアやキーロガーを検出･駆除できる専用対策ツールを利用することで、ウイルス対策ソフトなどの既存のセキュリティ技術の弱点を補完できます。

個人がツールなどを使わずに自衛をするにあたっては、不正プログラムがどこからやってくるかを知ることが必要でしょう。侵入経路別に説明すると以下のようになります。

5.1.1 Web 閲覧時にスクリプトを悪用した侵入への対策

Web サイトの閲覧時に ActiveX や Java、 Visual Basic などのスクリプトを悪用して侵入する場合があります。これらの対策としては、まずブラウザのセキュリティ設定を強化することが肝要です。さらに WEB 閲覧中に確認ダイアログが表示された場合は、本当に信用できるサイト以外では「受け入れない」を選択することが賢明です。

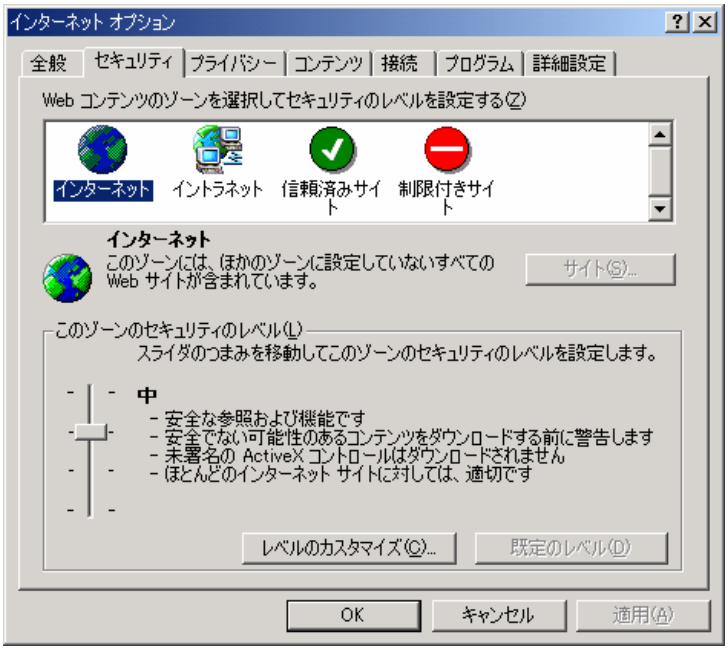

図 5.1.1　ブラウザのセキュリティレベル設定

5.1.2 セキュリティホールを悪用した侵入への対策

OS やブラウザ、メーラーなどのプログラムのセキュリティホールを悪用して侵入してくる場合があります。個人ユーザの場合は、脆弱情報が発表されたら速やかに Windows Update などのプログラム更新を実施することが賢明です。これを怠ったがために起きるハッカーツールやトロイの木馬の侵入は非常に多いものです。ただし、組織の場合は、その組織のセキュリティポリシーに従い行動することが求められます。

さらに、ウイルスやハッカーツールやトロイの木馬は、多くの人が使用する OS やアプリケーションを攻撃対象とすることが多いので、OS やアプリケーションの再検討も一定の抑止効果があります。

5.1.3 スパイウェア・クッキーの対策

情報収集を目的としたクッキー（スパイウェア・クッキー）として侵入する場合があります。これはブラウザの「インターネットオプション」を利用して、テンポラリファイルの中にあるクッキーや Web 閲覧履歴を定期的に整理したり削除することで被害を防ぐことができます。この場合、定期的にテンポラリファイルを整理するツールなどが利用できます。

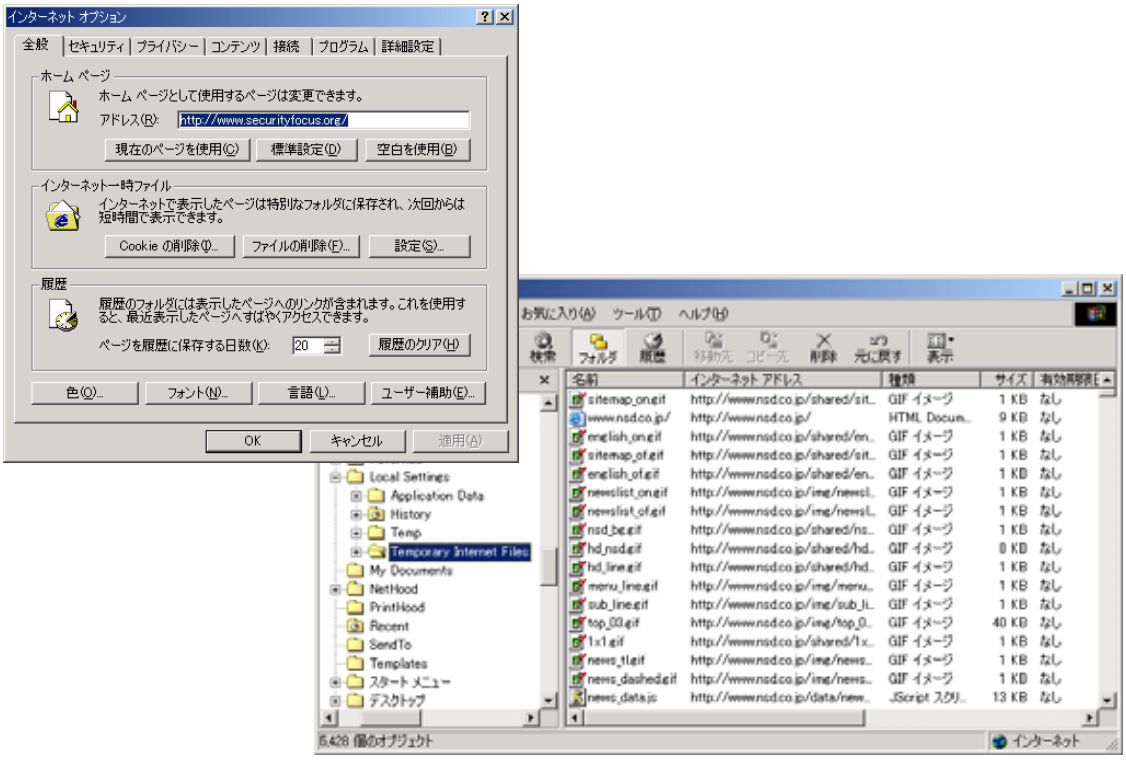

図 5.1.3　定期的にクッキーを整理

5.1.4 HTML メールのスクリプトを悪用した侵入への対策

Web と同じ HTML 形式のメールにスクリプトを忍ばせておいて侵入する場合があります。これは HTML 形式のメールは、閲覧するだけでスクリプトが実行されるので、感染や侵入の経路になってしまいます。これの対策には、まずテキスト形式で受信するようにメーラーの設定を変更し、さらにはスクリプトの自動実行機能をオフにすることが有効な対策といえます

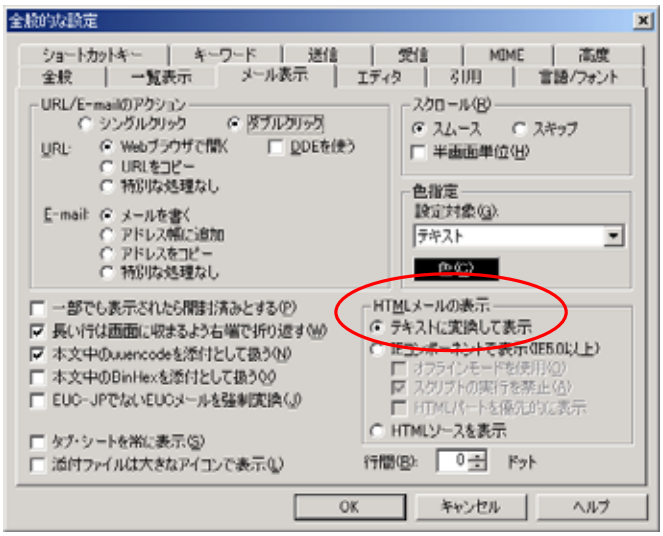

図 5.1.4　メールの受信形式設定

5.1.5 メール添付を悪用した侵入への対策

現在では危険性がかなり認知されてきているものとしてメールに添付して侵入する場合があります。出所のはっきりとしないメールや添付ファイルを、削除し、開かないことは有効な対策です。実行可能や添付ファイルや思い当たりのない相手からの添付ファイル付きのメールは、危険性が高いといえます。また、ターゲットになりやすい多くの人が使用するメールソフトを使用しないというのも有効な手段です。

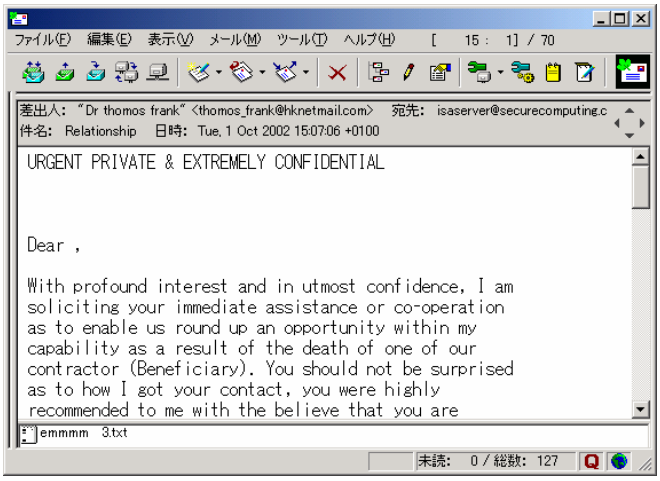

図 5.1.5 添付ファイルに注意

5.1.6 P2P ソフトウェアを悪用した侵入への対策

P2P ソフトウェアを使用して入手した第三者のファイルに不正プログラムが含まれている場合があります。P2P ソフトウェアを使用する場合は、確認の取れないソフトウェアやファイルの取得を控え、同時に、確認の取れない相手先との通信も控えるべきです。また、原則として、実行形式のファイルは取得しないようにした方が無難です。最近では、実行形式ファイルを JPEG 画像などのデータファイルに偽装する手法も報告されておりますので注意が必要です。

5.1.7 直接システムに仕掛けられた場合の対策

第三者が直接システムにハッカーツールやトロイの木馬を仕掛けて侵入する場合があります。個人レベルの対策としてはパソコンの起動時やスクリーンセーバのパスワードロックを設定することが有効な手段です。組織内の重要なシステムでは、サーバ・ルームの設置など物理セキュリティとの併用も有効です。

図 5.1.7　スクリーンセーバの設定

表 5.1 不正プログラム侵入経路別の対策

No.	侵入経路	対策
1	Web の閲覧時に ActiveX や Java などのスクリプトを悪用して侵入	ブラウザのセキュリティ設定を強化する
2	OS やプログラムのセキュリティホールを悪用して侵入	脆弱情報発表時に Windows Update などのプログラム更新を実施する
3	情報収集を目的としたクッキー（スパイウェア・クッキー）として侵入	定期的なクッキーや Web 閲覧履歴の整理と削除を実施する
4	Webと同じHTML形式のメールにスクリプトを忍ばせておいて侵入	メーラーの設定でHTML形式のメール受信とスクリプトの自動実行機能をオフにする
5	メールに添付して侵入	出所のはっきりとしない怪しいメールや添付ファイルは削除し、絶対に開かない
6	P2P ソフトウェアを悪用した侵入	確認の取れない相手とのやり取り、ファイルの取得を控える。実行形式のファイルは取得しない
7	第三者など他人が直接システムに仕掛けて侵入（内部犯罪）	パソコンの起動時やスクリーンセーバのパスワードロックを設定する
		サーバ・ルームの設置など物理セキュリティと併用する

5.2 専用ツールを導入する方法

組織においては、ツールを使用し対策を行うことが有効です。

SOHO でも大企業でも、扱っているデータの重要性や、ネットワークの論理は変わらないのですから、規模が異なるとはいえ、その考え方や仕組みは同一です。

組織向けの不正プログラム対策は、どのようなネットワーク接続がされているかによって対策も変わってきます。

以下はネットワーク接続および使用環境を考慮した対策です。

5.2.1 基本事項

使用環境に関わらず、共通的な対策事項として、先ず、「不正プログラム対策」をセキュリティポリシー及び行動基準の両方に盛り込んで実行することが挙げられます。これらの対策は、大きく分けて、事前対策と事後対策の **2** 種類に分類されます。

事前対策：

- 各種対策ツールでリアルタイム検査機能を有するものについては常に有効にして運用します。
- 各種対策ツールでデータベース更新が必要なものについては最新の状態での運用を心がけます。
- 規模によっては脆弱性監査ツールや資産管理ツールによる自動パッチ適用なども検討します。

事後対策：

- インシデント発生時の連絡体制と復旧手順を明確に策定し、定期的な訓練を実施します。
- 対象物によっては損害保険の加入も検討します。

5.2.2 スタンドアロン環境

スタンドアロン環境でシステムを使用している場合は、まずトロイの木馬やスパイウェア対策ソフトと、パーソナルファイアウォールを導入します。

システムの **OS** の機能を使用して対策をするのもよい方法です。たとえば、共有ファイルやフォルダの管理を厳格化する、マシンのブート時やスクリーンセーバのパスワードロックを有効化するなどが挙げられます。

5.2.3 LAN に接続された環境

LAN に接続された環境でシステムを使用している場合は、サーバ、クライアントに不正プログラム検出ツールを導入する必要があります。適切なセキュリティホール対策を実施するためのツールの導入や、ネットワークやホストベースの **IDS**（**Intrusion Detection System**：不正侵入検知システム）の導入などがあります。セグメント単位でのファイアウォールの導入も

挙げられます。できれば不正パケットフォーマットを検知できるものが望ましいでしょう。**Web** などのアプリケーションに特化したものも環境によっては有効です。

ファイルやフォルダへのアクセス管理の確立も必要です。各々のユーザごとに必要最小限のアクセス権限しか与えない、アクセス権限違反のロギング機能があるものについてはログが残るように設定するといった運用を心がけ、環境によっては専用ツールの導入も検討します。

5.2.4 インターネットに接続された LAN 環境

インターネットに接続された **LAN** 環境でシステムを使用している場合には、厳重なセキュリティ対策が必要です。まず、ネットワークファイアウォールの導入が必要です。不正なパケットフォーマットを検知できるものが望ましいでしょう。また、メールフィルタリング、**URL** フィルタリング、**Anti-Virus** などの昨日をゲートウェイにて提供するツールを使用した、ゲートウェイ・ソリューションの導入も検討してください。ネットワーク・ファイアウォールに連動して検査するタイプとプロキシーとして独立して検査するタイプがあります。下の表はゲートウェイソリューションの特徴の比較表です。

表 5.2.4 ゲートウェイソリューションのタイプ

	ネットワーク構成	機器への負荷
ファイアウォール連動型	簡素化できる	重くなる傾向あり
独立型	複雑になる	比較的軽減可

また、ネットワーク **IDS**、**IPS**（**Intrusion Prevention System**：不正侵入防御システム）の導入も検討するとよいでしょう。**IDS** は、検知するだけで防ぐ機能は別物であること、動作が **VLAN** や **L2/L3** スイッチに影響を受けるので、導入に当たってはネットワーク攻勢の再検討が必要なことに留意してください。**IPS** は、ネットワーク上に直列に接続されるので接続速度への影響を慎重に検討・検証する必要があります。

MMC（**Malicious Mobile Cord**：**JAVA**、**ActiveX**、**Visual Basic** などのスクリプト）による攻撃対策ツールの導入も必要ですが、効果が特定のアプリケーションや攻撃に限定されることが多いので、機能についての十分な検証と検討をするようにしてください。

5.2.5 グループウェアを使用している場合

グループウェアを使用している環境では、グループウェアは、独自のファイルシステムを使用しているため、製品に特化したソリューションの導入が必要です。導入の段階で、専用ツールの整備度合いを検討項目に入れておくことが望ましいでしょう。

以上

執筆者

■飯沼　正枝(Masae Iinuma)
日本ネットワークアソシエイツ株式会社
技術本部　教育部

■植山　達弥(Tatsuya Ueyama)
大興電子通信株式会社
ネットワークソリューション部　セキュリティシステム課

■奈良岡　健太(Kenta Naraoka)
株式会社ディアイティ
製品事業本部　セキュリティビジネスユニット

■西野　一行(Kazuyuki Nishino)
株式会社ニコンシステム
管理本部　企画部

■ピョー　ナィン　トォン(Pyo Naing Tun)
株式会社アークン
R&D事業本部

■米澤　一樹(Kazuki Yonezawa)
セキュアコンピューティングジャパン株式会社

■渡部　章(Akira Watanabe)
株式会社アークン

(敬称略、五十音順)