JNSA
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

不正プログラム対策ガイドライン
不正プログラム調査WG

2004 年 1月18日

目次

1. はじめに
2. 不正プログラムの定義
3. 不正プログラムの分類
4. 不正プログラムの構造
5. 不正プログラム対策
    1. セキュリティルールの策定
    2. 専用ツールの導入

はじめに

- 不正プログラムの問題が深刻化
  - キーロガーによるパスワード漏洩
    - オンラインバンキング口座からの不正引出し
  - トロイの木馬による「無意識のうちの加害者」
    - DDOS攻撃の根源
    - 踏み台としての使用
  - 情報セキュリティ被害の過半数がウィルス感染などの不正プログラムに起因

    出展：「平成15年度不正アクセス対策の調査」警察庁

不正プログラムの定義

「個人またはシステム管理者の意図ところで、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」

通商産業省告示 第952号「コンピュータウイルス対策基準」
（「通産省」の表記は省庁改変前の通告のため）
「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」

総務省 「国民のための情報セキュリティサイト」

- 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（トロイのもくば）：
  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。

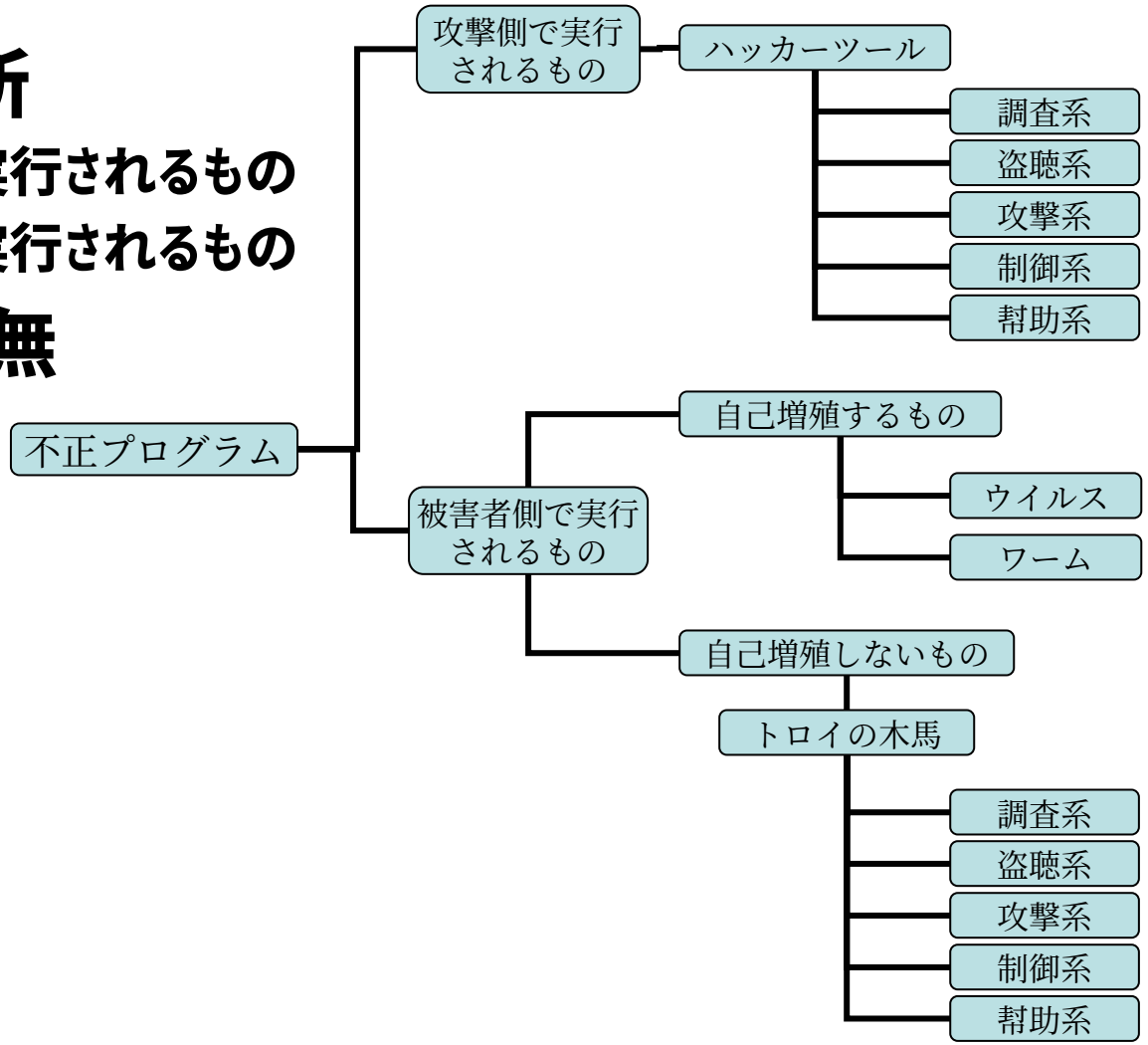
不正プログラムの定義

- 例外
  - 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

    (通常のアプリケーションで使用者に不利益な機能が隠れて動作する場合は除く)
  - 一般的にジョークプログラムと言われているもの
  - プログラムの瑕疵に起因するユーザの意図しない挙動

不正プログラムの分類 (1)

- **実行される場所**
  1. **攻撃者側で実行されるもの**
  2. **被害者側で実行されるもの**
- **自己増殖の有無**
- **機能別**
  1. **調査系**
  2. **盗聴系**
  3. **攻撃系**
  4. **制御系**
  5. **幇助系**



不正プログラムの分類 (2)

- 具体例
  - 被害者側で実行される、自己増殖しない、盗聴系、不正プログラム
    スパイウェア、キーロガー など

※最近は複合的な機能を持つものが主流になってきている。
「自己増殖＋盗聴＋制御」など

不正プログラムの構造(1)

「ウィルス・ワーム」

vs「ハッカーツール・トロイの木馬」

	原産地	活動の性質	被害期間	被害件数	1件当り被害額
ウィルス・ワーム	海外産	顕在的	一時的	多	比較的多
ハッカーツール・トロイの木馬	海外産 国内産	潜在的	長期的	少	比較的少

不正プログラムの構造 (2)

- ハッカーツール・トロイの木馬は両刃の剣

  例:

	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

不正プログラム対策 (1)

代表的な自衛策は2通り

1. セキュリティルールの策定
2. 専用ツールの導入

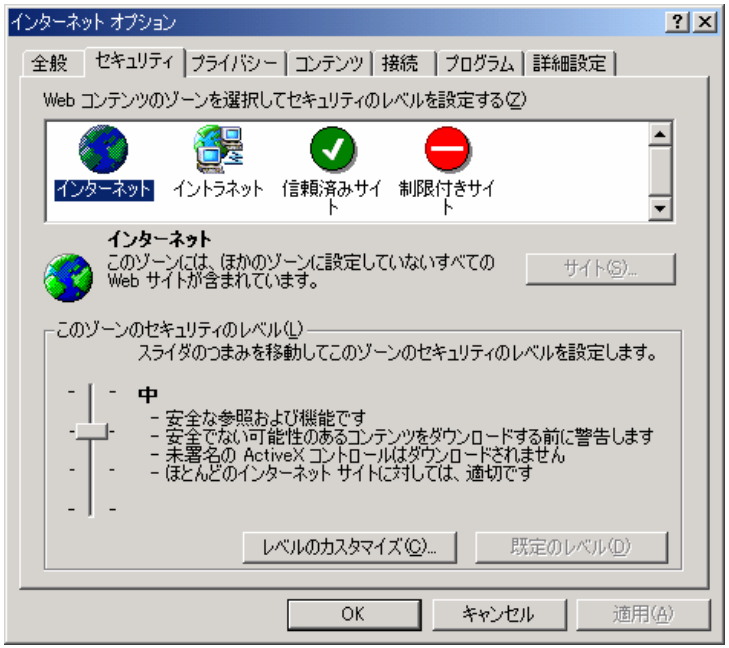
不正プログラム対策 (2)

- セキュリティルールの策定
  - 侵入経路毎の自衛策を策定し実行する
    1. Web閲覧時にスクリプトを悪用した侵入
    2. セキュリティホールを悪用した侵入
    3. スパイウェア･クッキーとして侵入
    4. HTML メールのスクリプトを悪用した侵入
    5. メール添付を悪用した侵入
    6. P2Pソフトウェアを悪用した侵入
    7. 直接システムに仕掛けられて侵入

不正プログラム対策 (3)

1. Web閲覧時にスクリプトを悪用した侵入への対策

- ブラウザのセキュリティ設定を強化
- 確認ダイアログが表示されたときには、本当に信用できるサイト以外では「受け入れない」を選択



不正プログラム対策 (4)

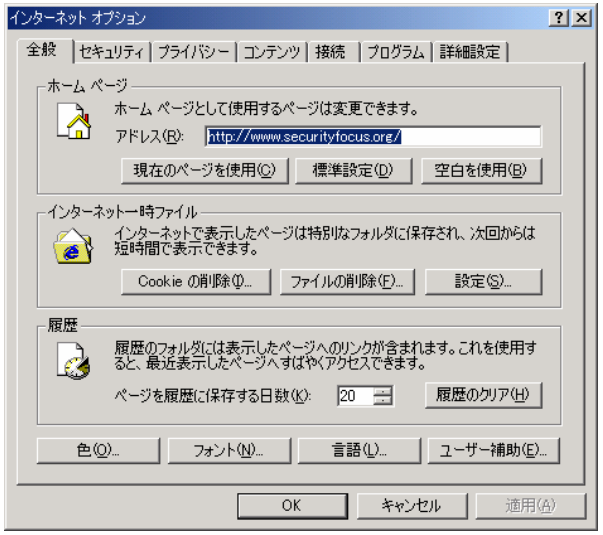
2．セキュリティホールを悪用した侵入への対策

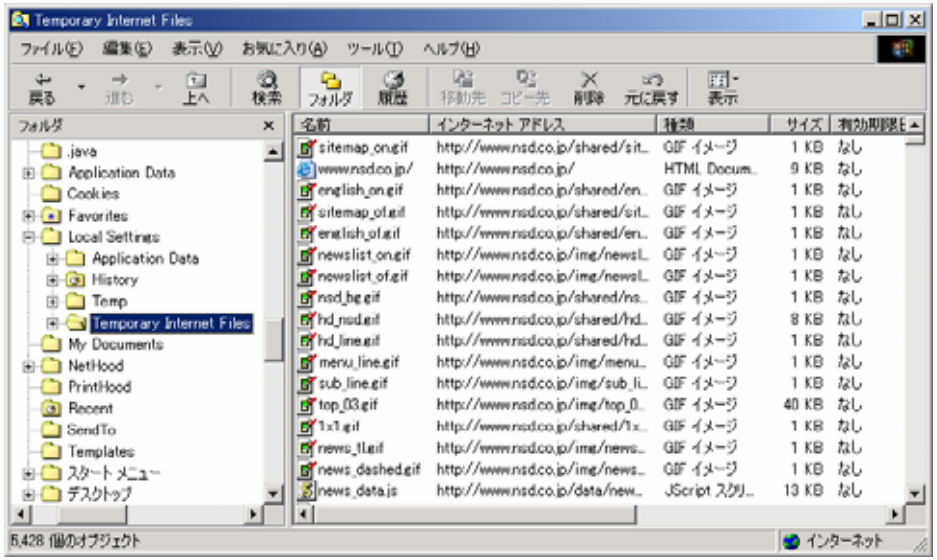
- 個人ユーザの場合は、脆弱情報が発表されたら速やかにプログラム更新を実施
- 組織の場合は、その組織のセキュリティ・ポリシーに従い行動する
- OSやアプリケーションの種類によっても一定の抑止効果が生まれるので、利便性との兼ね合いで検討する
  - ウイルスやハッカーツールやトロイの木馬は、多くの人が使用するOS やアプリケーションを攻撃対象とすることが多い

不正プログラム対策 (5)

3．スパイウェア･クッキーの対策

- 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･削除
- 定期的にテンポラリファイルを整理するツールの使用も有効

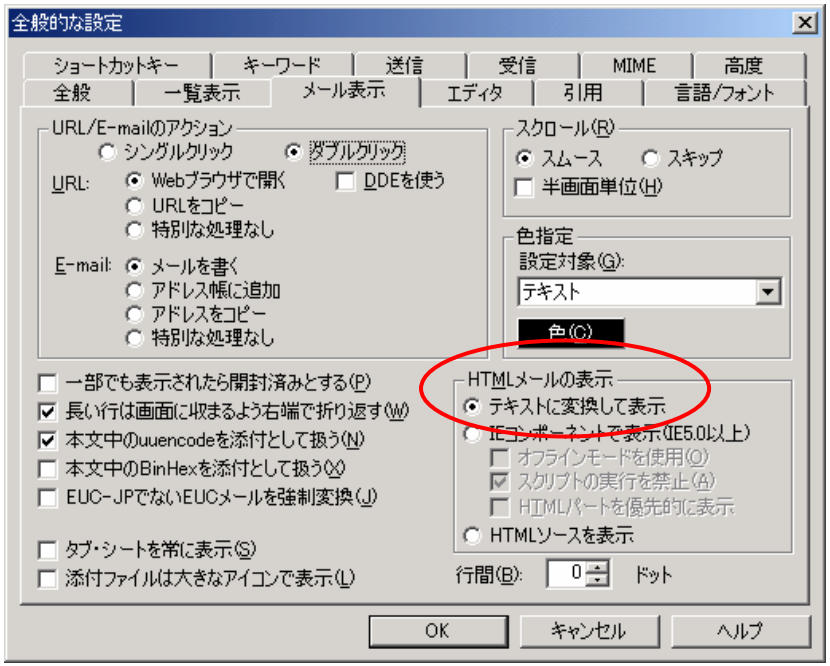




不正プログラム対策 (6)

4．HTML メールのスクリプトを悪用した侵入への対策

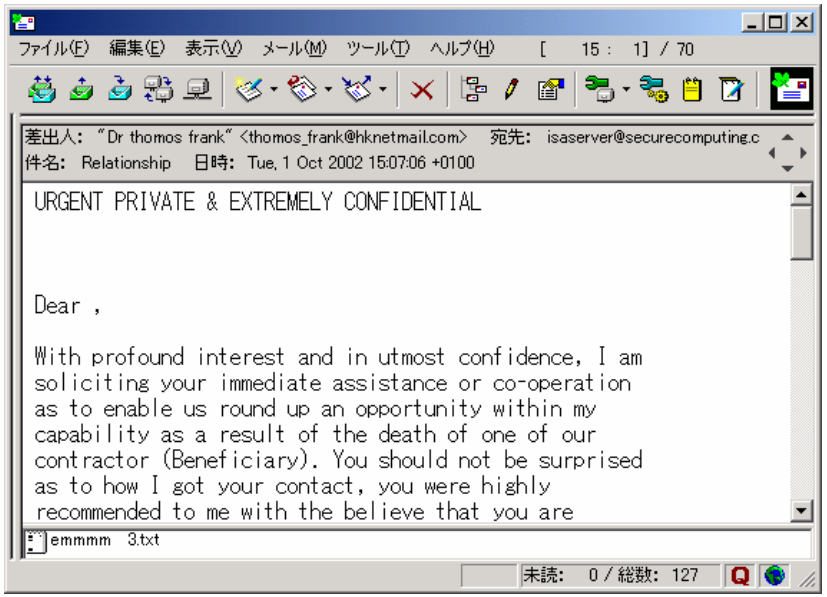
- まずテキスト形式で受信するようにメールシステムの設定
- スクリプトの自動実行機能をオフにする



不正プログラム対策 (7)

5．メール添付を悪用した侵入への対策

- 出所のはっきりとしないメールや添付ファイルを開かずに削除する
- 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



不正プログラム対策 (8)

6. P2Pソフトウェアを悪用した侵入への対策

※ 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ことがある

- 確認の取れないソフトウェアやファイルの取得を控える
- 確認の取れない相手先との通信も控える
- 原則として、実行形式のファイルは取得しない
  - 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いるので注意が必要。

不正プログラム対策 (9)

7. 直接システムに仕掛けられた場合の対策

※内部犯行によるケースが多い。

- 個人レベルの対策としてはシステム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
- 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

不正プログラム対策 (10)

- 専用ツールを導入する方法
  - ネットワーク等の環境別に適したツールを導入して防御
    ※複数の形態を組み合わせて使用する場合が多い
    1.基本事項
    2.スタンドアロン環境
    3.LANに接続された環境
    4.インターネットに接続されたLAN環境
    5.グループウェアが導入されたLAN環境

不正プログラム対策 (11)

JNSA

1. 基本事項

※「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。

→ 事前対策と事後対策の両方が必要

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する。
- 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る。
- 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する。

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する。
- 対象物によっては損害保険の加入も検討する。

不正プログラム対策 (12)

JNSA

2. スタンドアロン環境

- トロイの木馬／スパイウェア対策ソフトを導入する。
- クライアントにおける「ファイル／フォルダの共有」の管理を厳格化する。
- パーソナル・ファイアウォールを導入する。
- 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。
- 前記「侵入経路別の自衛策」を施す。

不正プログラム対策 (13)

JNSA

3. LANに接続された環境

- セグメント単位での内部ファイアウォールの導入
  - 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。
  - 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。
- サーバ・ホストベースIDSを導入する。
  - 不正プログラム検出ツールを導入する。
  - 適切なセキュリティホール対策を実施する。
  - ソリューションを導入する。
- 「ファイル／フォルダ」へのアクセス管理の確立
  - 各々のユーザ毎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有るものについてはログが残るように設定する。

不正プログラム対策 (14)

4. インターネットに接続されたLAN環境 (1)

- ネットワークファイアウォールの導入
  - 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。
- ゲートウェイ・ソリューションの導入
  - メールフィルタリング、URLフィルタリング、Anti-Virusなどの機能をゲートウェイにて提供するツールを導入する。
  - 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る。

	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	重くなる傾向有り
独立型	複雑になる	比較的軽減可

不正プログラム対策 (15)

4. インターネットに接続されたLAN環境 (2)

- ネットワークIDS の導入
  - 検知するだけで防ぐ機能は別物であることの認識が必要。
  - 動作がVLANやL2/L3スイッチに影響を受けるので、導入にあたってはネットワーク構成の再検討が必要。
- IPS (Intrusion Prevention System) の導入
  - 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･検証する必要が有る。
- MMC (Malicious Mobile Cord : JAVA、ActiveX、VisualBasicなどのスクリプト) による攻撃対策ツールの導入
  - 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が必要。

不正プログラム対策 (16)

5. グループウェアを使用している場合

– グループウェア・ソリューションの導入

- 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、専用のツールが必要となる。
- グループウェア導入の段階で、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。

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)

・成果物の取扱いについて

成果物の著作権、使用等の権利は、著者及びＪＮＳＡとの共有とします。引用した文章、図表についての著作権は各作成者にあります。この成果物の配布、複製、修正についきましては、JNSA**事務局までお問い合わせください。**