T13: 不正プログラム対策と侵入検知、防御技術

二木真明 (住商情報システム)
渡辺勝弘 (理化学研究所)

コンピュータウイルスと対策 ～その変遷と最近の動向～

Internet Week 2005
T13: 不正プログラム対策と侵入検知、防御技術

二木真明 (住商情報システム)

今なぜ「ウイルス対策」なのか

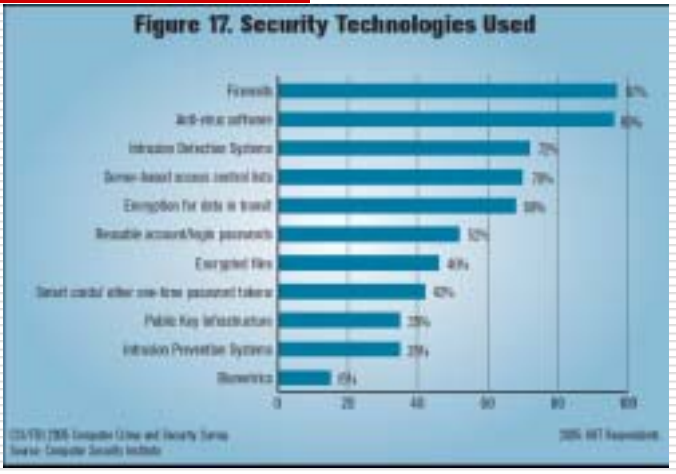
- ウイルス（不正プログラム）の変化
  - 新種、亜種の激増
  - 感染、拡大方法の多様化と拡大速度の向上
  - ウイルスを作る目的の変化
- 既存ウイルス対策の問題点
  - パターン更新がおいつかない対策ソフト
  - 不審なメールを開いてしまうユーザ
  - 一般に広く流布しないウイルスへの無力さ

CSI/FBI Survey 2005

アンチウイルスソフトの導入率は非常に高い

米国 CSI / FBI 共同コンピュータ犯罪とセキュリティについての調査２００５年版より

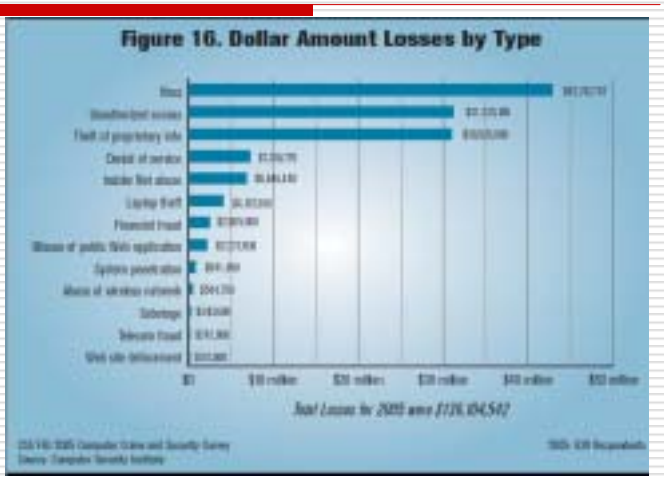
http://www.gocsi.com/



CSI/FBI Survey 2005

しかし、突出するコンピュータウイルスと不正アクセス被害・・・・・

対策は常識化したのに、なぜ？？？



なくならない被害、みつけられない被害

- 新種ウイルス感染被害はどこの組織でも・・・・
- ウイルス開発キット・・・・
- 「ボット」の蔓延
- ウイルス配布目的のWeb改ざん
- Card Systems 社事件の教訓
- あなたの組織も狙われている！？

敵を知って対策をたてよう

- ウイルス（不正プログラム）を知ろう
- これまでの「ウイルス対策」とその問題点を知ろう
- 新たな脅威＝今ある危機を知ろう
- どのような対策技術があるかを知ろう

そして、自分たちに合った対策を考えよう

コンピュータウイルスの歴史

- コンセプトは1970年代に既に存在
  - SF小説などに登場（Tape Worm…）
- 1980年代前半：研究の存在
  - 自己複製型プログラムの研究や実証実験
- 1980年代後半：基本的な技術の確立
  - 1986年 Brain Virus
  - 1987年 Morris Worm （Internet Worm）
- 1990年代：PC、インターネット普及に伴い一般化
  - マクロウイルス（非バイナリウイルス）の登場
  - メール媒介、感染型ウイルスの登場

コンピュータウイルス伝搬方法の変遷

- 1980年代～90年代前半
  - 主にオフラインメディアによる感染（FDなど）
  - 感染拡大はゆっくり、感染対象は選択的
- 1990年代後半
  - インターネット普及に伴い、電子メールやソフトウエアのダウンロードを介した感染が増加
  - 感染拡大は「人間の活動の速度」レベル、対象の無差別化
- 2000年代
  - 脆弱性を攻撃して自動侵入、拡散するものが登場（再来）
  - 伝搬・感染方法の複合化
  - 感染拡大は「コンピュータの速度」、無差別化が拡大する一方で選択的（特定目的）なものも増加（二極分化）

コンピュータウイルスって何？

- 一般の定義（マスコミ等の用法）
  - 「不正（悪性）プログラム」の総称としての使い方
  - ワーム、トロイの木馬・・・などもすべて含まれる
- 本来の（技術的な意味での）定義
  - 既存のプログラム（コード）に自分自身を組み込むことで、それらの実行時に自分自身の複製や他への感染、特定の作業の実行するような自己複製プログラム

不正（悪性）プログラムの分類

- 感染方法による分類
  - ウイルス
    - バイナリコードで記述されているか、インタープリタ言語（マクロ／スクリプト言語）で記述されているかを問わないが、既存のコードに改変を加え、自分自身を組み込むことにより感染する不正プログラム
  - ワーム
    - バイナリ、マクロを問わず、他のプログラムに依存せず単独でコンピュータシステム上で動作する不正プログラム
  - トロイの木馬
    - 他の目的のプログラムを装ってユーザにインストールさせ、表面上の機能に隠れて不正な処理を実行する不正プログラム

不正（悪性）プログラムの分類

- コードの形式による分類
  - バイナリ型
    - 感染段階では、コンピュータの機械コード（バイナリ）として存在し、ＣＰＵ上で直接コードが実行されるもの
    - 元々の記述言語は問わない。コンパイルされた結果として存在するもの
    - ＣＰＵ種別依存、ＯＳ依存あり
  - マクロ型
    - それ自体がなんらかのインタープリタ処理系で実行される高級言語（マクロ、スクリプト）で記述されたもの
    - 実行時、プラットホーム上に実行系が存在する必要がある
    - CPU依存がない（但し、OS、実行環境への依存はありうる）

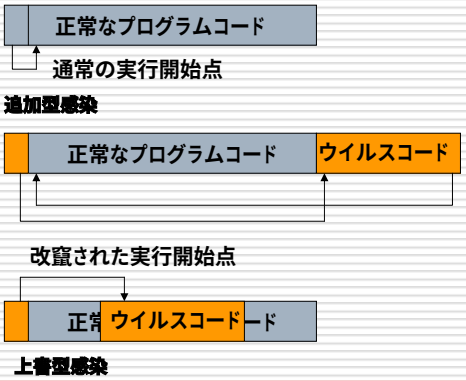
不正（悪性）プログラムの分類

- 拡散・侵入方法による分類
  - 電子メール媒介型
    - 感染した環境内に存在するアドレスデータなどを探して利用し、自分自身の複製を電子メールで送信するようなもの
  - 攻撃侵入型
    - ネットワーク上で脆弱性を持つコンピュータを探索し攻撃、侵入して自分の複製を送り込むもの
    - その他、一般に不正な侵入に使用される手法を使って侵入し、自分の複製を送り込むもの
  - Web媒介型
    - Webサイトに混入された不正スクリプトなどから拡散するもの
  - ファイル媒介型
    - 外部メディア、共有その他によるファイル受け渡しとその実行により拡散するもの

不正（悪性）プログラムの分類

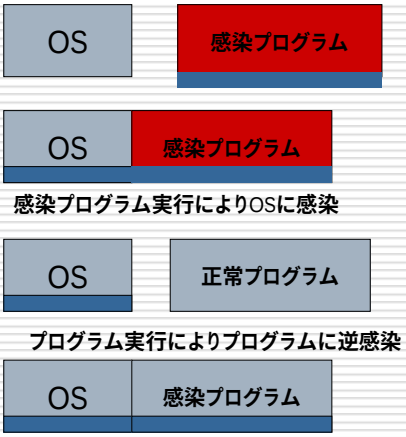
- 発症行動による分類
  - 破壊行動型
    - 感染したコンピュータの動作、操作を妨害、環境やデータを破壊するもの
  - バックドア型
    - 感染したコンピュータに本来の認証を回避して接続、操作出来るような仕組みを組み込んでしまうもの
  - DDoS型
    - ネットワークを経由して特定のサイトに対してサービス妨害を仕掛けるもの
  - 情報漏洩型（スパイウエア）
    - 感染したコンピュータ内のデータ（情報）を収集し、外部に持ち出すもの

ウイルスはいかに感染するか



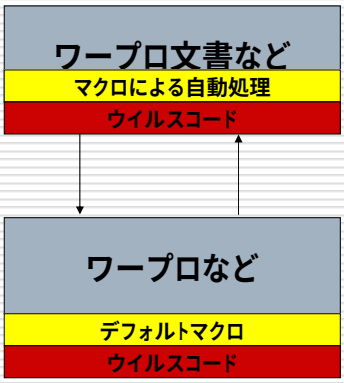
- バイナリウイルス
  - 実行形式ファイルに自分をコピーする。この場合、正常なコードを破壊しないタイプ（修復可能）と、破壊するタイプ（修復不可能）の二通りがある。
  - 実行開始点を操作して最初にウイルスのコードが実行されるように改竄
  - ウイルスコードが実行されると次の感染行動や不正操作を実行

バイナリウイルスの感染



- バイナリウイルス
  - OSのモジュールような常駐プログラムに感染
  - 常駐プログラムによって他の実行プログラムに媒介される

マクロウイルスの感染



- マクロウイルス
  - 文書などの自動処理機能を悪用
  - 文書を開くと自動実行され、ワープロなどが持つデフォルトマクロに感染
  - ワープロで作成・編集した文書に感染

メール拡散型ウイルスが引き起こす問題

- メールアドレス（個人情報）の漏洩
  - アドレス帳や、ＰＣ内のあらゆるファイルに含まれるメールアドレスが危険にさらされる
    - 宛先として利用されるだけでなく、送信者の詐称にも使われるため、第三者にメールアドレスがばらまかれる可能性がある→ＳＰＡＭ業者に捕捉されてしまう可能性も・・・
- 取引関係を推測できる
  - 大量感染があった組織から送られて来たメールの詐称された送信者アドレスから推測可能

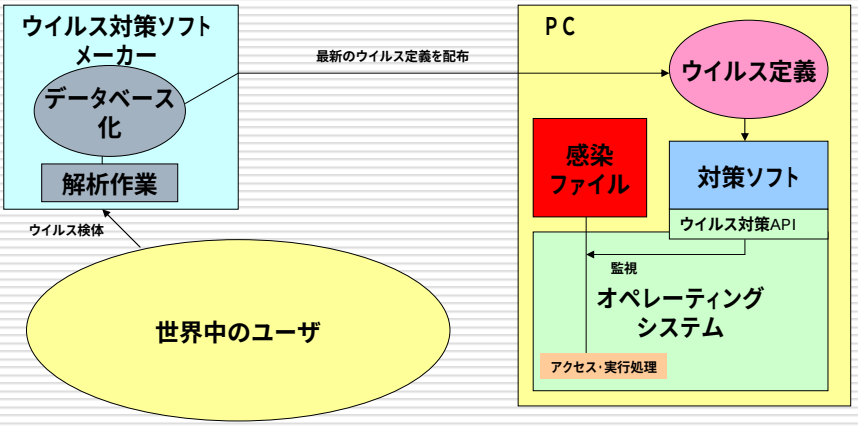
これまでのウイルス対策

- ウイルス対策ソフトウエアの歴史
  - 1987年、はじめてのAnti Virusソフトウエアが開発される
  - 1990年代前半、Windows PCの普及に伴い徐々に浸透
  - 電子メール拡散型ウイルスの登場で、一気に普及し、ウイルス対策は一大産業に成長

これまでのウイルス対策

- ウイルス対策ソフトウエアのしくみ
  - 初期の対策ソフトウエア
    - 手動で実行
    - 比較的単純なパターンマッチでウイルス感染ファイルを発見
  - 現在の対策ソフトウエア
    - 常駐型でリアルタイムにファイル操作、プログラム実行などを監視
    - 複雑な（状態をもつ）パターンマッチ
    - 未知ウイルスに（ある程度）対応できるパターンレスのウイルス発見機能
    - ウイルスの駆除、復旧機能（但し、限定的）

ウイルス対策ソフトウエアの動き



未知ウイルス発見機能の例

- ヒューリスティック機能
  - 一般的な不正プログラムの特徴を細かく分類し、複数の特徴を調べた結果を総合して、ウイルスかどうかを判断する機能
- ハッシュ検証
  - ウイルスによるファイル改ざんをチェックする方法。既知のファイルのハッシュ値と実際の値を比較して改ざんをチェック。(HIDS／IPSでも用いられる方法)

未知ウイルス検出機能の例

- コード検証
  - ウイルスと疑われる実行コードの処理を解析してウイルスかどうかを判断する。場合によってはサンドボックス内で実行して検証することもある。
- API呼び出しのチェック
  - たとえば実行形式ファイルを対象としたファイル操作APIやメール操作、ネットワーク操作APIなどの呼び出しをチェックする。(HIPSでも使われる手法)

未知ウイルス発見機能の弱点

- ヒューリスティックは確率的 (誤認、見落としが発生する可能性)
- ハッシュ検証はファイル改ざんが生じる場合のみ検出可能
- コード検証は負荷が重く、限定的 (一部の形式のウイルスのみにしか使えない)
- API監視も、すべての呼び出しパターンを網羅することが困難
- これらの組み合わせで確度を上げても、見落としは少なからず発生する。
- ウイルス対策ソフトウエアは市販品である。

さらに対策ソフトを悩ませる問題

- 新種、亜種の加速度的な増加
  - ウイルス定義の肥大化と処理負荷の増大
  - ウイルス定義更新作業負荷の増大と遅延の発生
- ウイルスの拡大速度の劇的な向上
  - ネットワークワームはもはや拡大に人手を介さない
  - 電子メール文化とメールによる感染頻度の激増
  - 数時間程度のウイルス定義配布遅れが致命的に

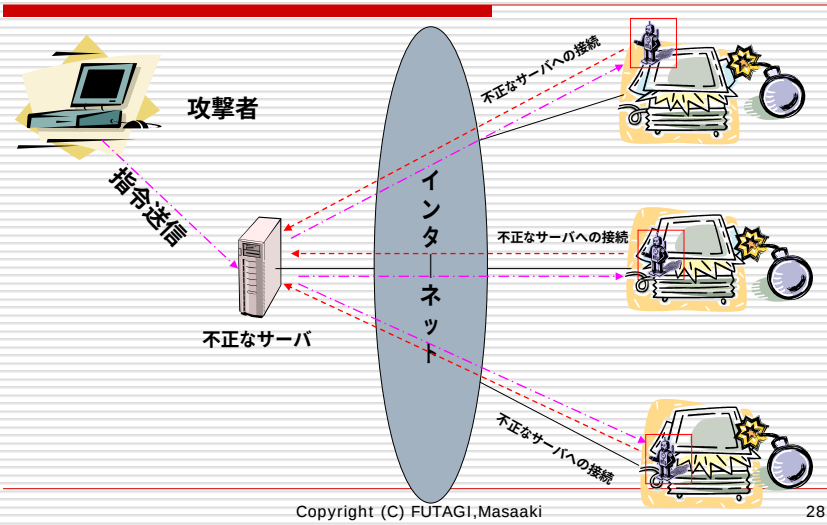
そして・・・・

- 特定目的、ターゲットを持ったウイルス（不正プログラム）の増加
  - 感染を広げない・・・　→検体入手が困難
  - 目立った活動をしない・・・　→感染に気づかない
  - たとえば特定の情報を盗む・・・　→被害は深刻
  - 目的達成後に消滅・・・　→感染の事実すら闇に
- ウイルス対策ソフトウエアは必要だが不十分
  - さらなる感染防止策が必要
  - 万一の感染をどう発見し、駆除するか・・が重要に

新たな脅威・・・「ボット」

- ウイルスやワームの形で侵入
- ボットネット（外部の悪意あるサーバ）に接続して指令を待つ
- 指令を受けて一斉に行動を起こす
  - 特定サイトへのDDoS攻撃
  - 他の不正プログラムのダウンロードと感染
  - 自分自身のアップグレード
  - ・・・・
- 一旦侵入されると「なんでもあり」

ボットの動き



ボット対策の難しさ

- 開発キットの流通と亜種の激増
- ウイルス対策ソフトは無力
  - ウイルス定義配布がおいつかない問題
  - 感染してしまった場合、定義更新で本体は駆除できても、感染～駆除までの間に何をされたかわからず、完全復旧の保証なし→ＯＳから再インストールするのが安全
- 通信規制の難しさ
  - IRCは止められても、httpを止めるのは困難

これからの不正プログラム対策

- 感染防止策の強化
  - 複数メーカーのウイルス対策ソフトウエアを利用
    - メールサーバやファイルサーバとクライアントＰＣでの使い分け
  - デスクトップファイアウォール、HIPS等の利用
  - 脆弱性対策の強化
    - パッチマネジメントツールの導入
    - 不正接続ＰＣ対策
    - クライアントＰＣへの定期的脆弱性検査

HIPS／デスクトップF/Wの利用

- HIPSの一般的な機能
  - ネットワークからの既知の攻撃監視
  - サービスへのアクセス制限
  - アプリケーションの挙動監視とポリシー違反の阻止
    - スタック保護（バッファオーバフロー防止）
    - API呼び出し監視、規定外の操作のブロック
    - ネットワーク活動の監視と制限
    - 許可外アプリケーションの起動阻止
  - ファイル保護
    - 特定のファイルに対する変更、削除の検出、防止など

HIPSは企業で本当に使える‥のか‥‥

- 集中管理とリアルタイムな監視が必要
  - HIPSを止めたり妨害したりする不正プログラムの存在
  - ポリシー違反や不審な挙動にはすぐ対処が必要
- なによりも、「ポリシー」がないと使えない
  - 何が異常な動きなのかを判断するためには、「正常」（ベースライン）を定義する必要がある（＝ポリシーが必要）

パッチマネジメントはワーム対策として充分か？

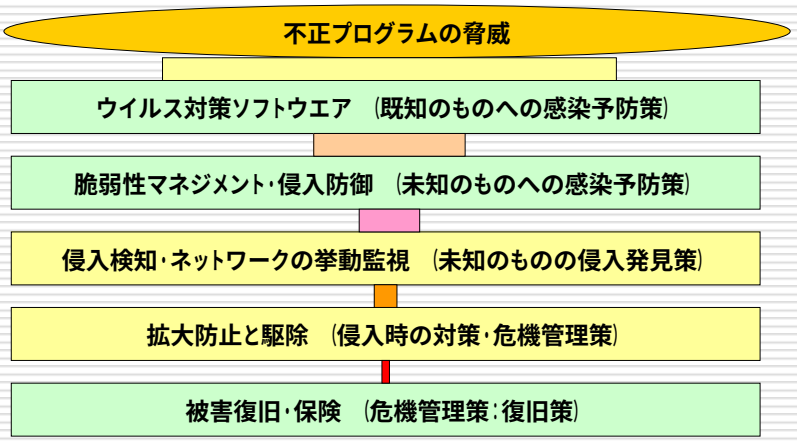
不

- 流布が目的の不正プログラムには有効だが
  - 一般的な、既知の脆弱性を利用したものはＯＫ
- ゼロ･デイ脆弱性の可能性
  - 可能性は低いが、特定組織を狙う場合は使われる可能性もある。リスクは非常に高くなる。
- ミスコンフィグレーションも狙われる
  - たとえば、Administrator アカウントにパスワードがかかっていなかったり、単純な辞書攻撃に耐えられないパスワードだったり･･･

結局、感染リスクはゼロにできない

- それでも感染する不正プログラムはより深刻
  - 特定組織を狙い撃ちにするもの
  - 情報窃取、業務妨害など、何者かの利益や金銭を目的とした「犯罪」行為の道具として使われる
- 万一の感染を発見する方法が必要
  - 通信監視
  - ＰＣ等の活動監視

“In depth”な不正プログラム対策



このセッションのテーマ

- 不正プログラムの侵入をどう発見し、どう対処するか・・・（できるのか？？）
  - 侵入検知・防御技術の現状　（渡辺さん）
  - 不正プログラム検知の実際　（渡辺さん）
  - リアルタイム監視による不正プログラム発見と対応　（二木）
  - 質疑応答