セキュリティのこれからを考える

SQL サーバやアプリケーションサーバ導入におけるマルウェア対策の注意点

Hirotaka Mieda (Microsoft MVP for Windows Desktop Experience)

自己紹介

Hirotaka Mieda (hm_hiroppy@hotmail.com)

Microsoft MVP for Windows Desktop Experience (Oct. 2003 –)

活動領域

MS ニュースグループ、答えてねっと、オフライン講師など

昔アセンブラ、過去に C/C++/VB/VBA/VBS、今は C#

お金になることが基本的に好きです
半面、人助けは好きなようでコミュニティ活動大好きです

過去には英語の翻訳/通訳をしてました

TREND MICRO

Trend Micro 東京本社勤務 (2001-2007 は福岡営業所)

Agenda

1. 知っているようで知らない！？ マルウェアとは？
2. 最近のセキュリティ環境を取り巻くマルウェア状況
3. アプリケーションサーバ構築時におけるマルウェア対策はどうあるべきか？
4. SQL サーバ導入において特に注意するべきマルウェア対策は？
5. まとめ

Agenda

1. 知っているようで知らない！？ マルウェアとは？
2. 最近のセキュリティ環境を取り巻くマルウェア状況
3. アプリケーションサーバ構築時におけるマルウェア対策はどうあるべきか？
4. SQL サーバ導入において特に注意するべきマルウェア対策は？
5. まとめ

マルウェアをおさらいしよう

- 不正な動作を行うことが目的で作成されたプログラムを総称してマルウェアと呼ぶ
  - ウイルス
  - スパイウェア
  - (アドウェア)
- マルウェアを利用した攻撃行為には様々なものがある
  - 多重ウイルス感染によるシステム負荷増大
  - ウイルス感染動作によるネットワーク負荷増大
  - 迷惑メール発信行為への加担
  - スパイウェアによる情報漏えい
  - DoS / DDoS 攻撃への加担
  - 詐欺行為などに遭遇する危険性

正しく説明出来ますか？

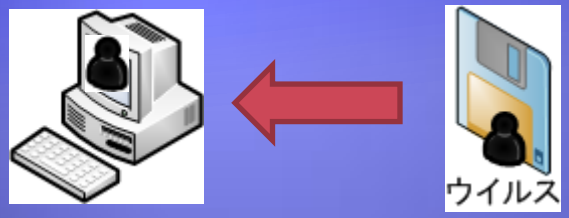
- 狭義では他の正常なファイルに感染し、感染/潜伏/発病のサイクルを持つものをウイルスと呼ぶ
- 広義では不正な動作を行うプログラムのうち、自己拡散を行うものをウイルスと呼ぶ
  - 1984 年にカリフォルニア大学の Frederick Cohen 博士が自然界に存在するウイルスに倣い、コンピュータウイルスと命名
  - 特徴としてはオフライン媒体/ファイル共有/インターネットメール/脆弱性攻撃などを通じて [自己拡散] を行う
  - システム破壊型からジョーク的動作まで、方式は多岐に渡る
  - いずれも基本的に自己顕示欲、愉快犯の域を出ないことが多い
    - 例: Netsky 発生時における拡散合戦など
      - ちなみに Netsky の作者は 2004 年 5 月に逮捕されてます

ウイルスの種類って？

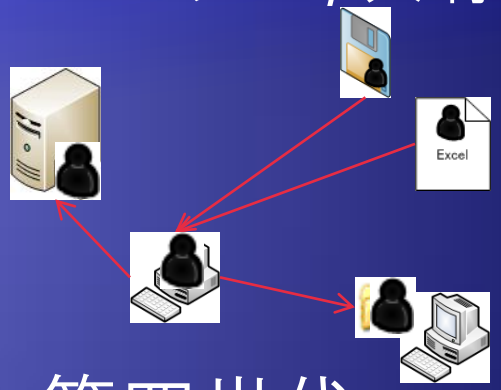
- システム領域感染型
- ファイル感染型
  - 上書き感染型 / 追記感染型
- ワーム型
  - ファイル共有拡散型
  - メール拡散型
- トロイの木馬型 (バックドア型)
- マクロウイルス型
- スクリプトウイルス型
- ネットワーク感染型 (ネットワークウイルス)
- 複合感染型
- (ダウンローダ型)

世代別ウイルス変遷

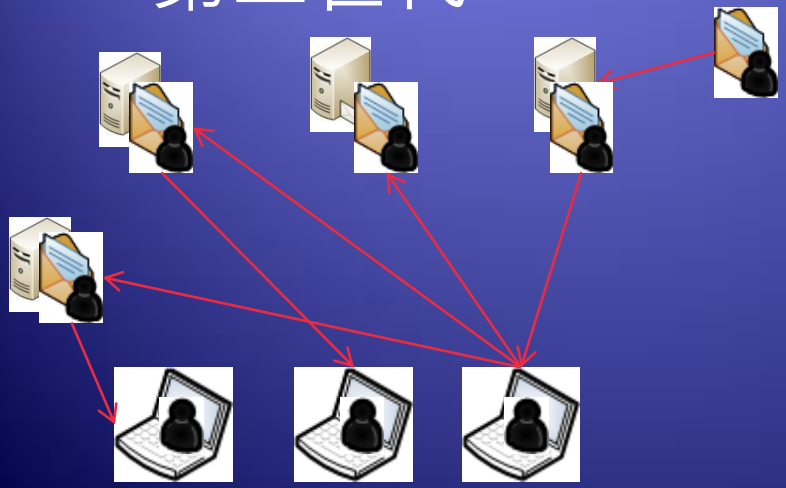
- 第一世代
  - オフライン媒体経由



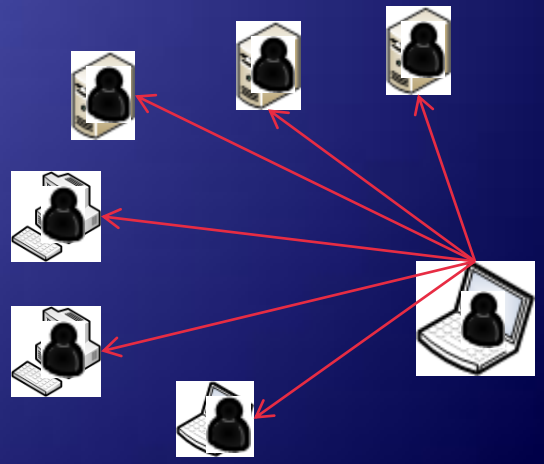
- 第二世代
  - マクロ / 共有フォルダ



- 第三世代



- 第四世代



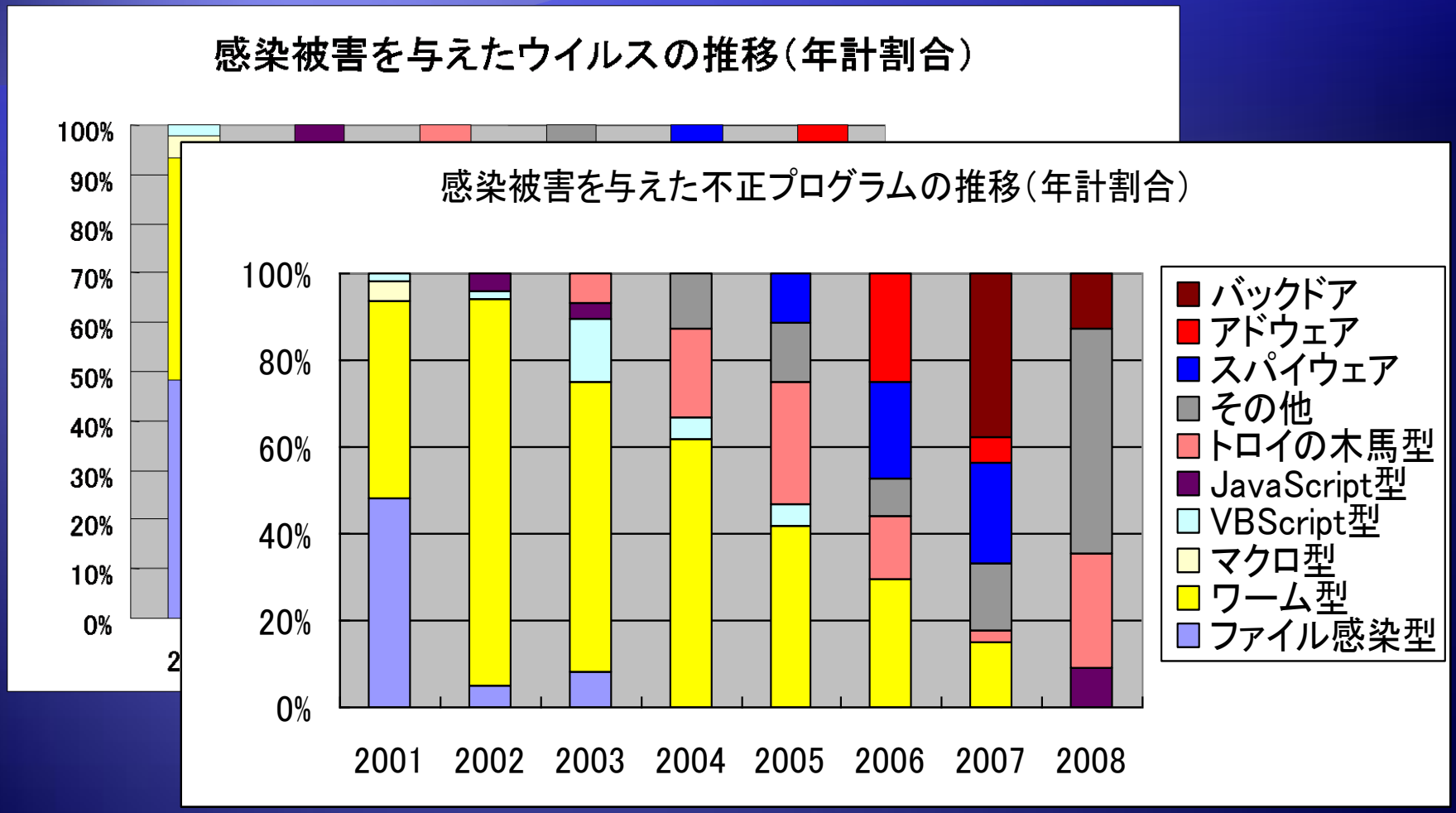
スパイウェアの登場

- 不正に情報を取得することを目的とするプログラム
- 基本的に自己拡散をしない
- スパイウェアの種類
  - ユーザの同意を得ずに情報収集するものすべて
  - (Tracking Cookie)
  - キーロガー
    - キー入力を監視してキーインの結果を取得、送信
    - SSL サイトへのアクセスは意味を為さない
  - Rootkit (ルートキット) タイプ
    - OS カーネル付近で動作して自身の存在を隠す
    - 有名な会社がやらかしたことでも有名

Agenda

1. 知っているようで知らない！？マルウェアとは？
2. 最近のセキュリティ環境を取り巻くマルウェア状況
3. アプリケーションサーバ構築時におけるマルウェア対策はどうあるべきか？
4. SQL サーバ導入において特に注意するべきマルウェア対策は？
5. まとめ

マルウェアの発生傾向



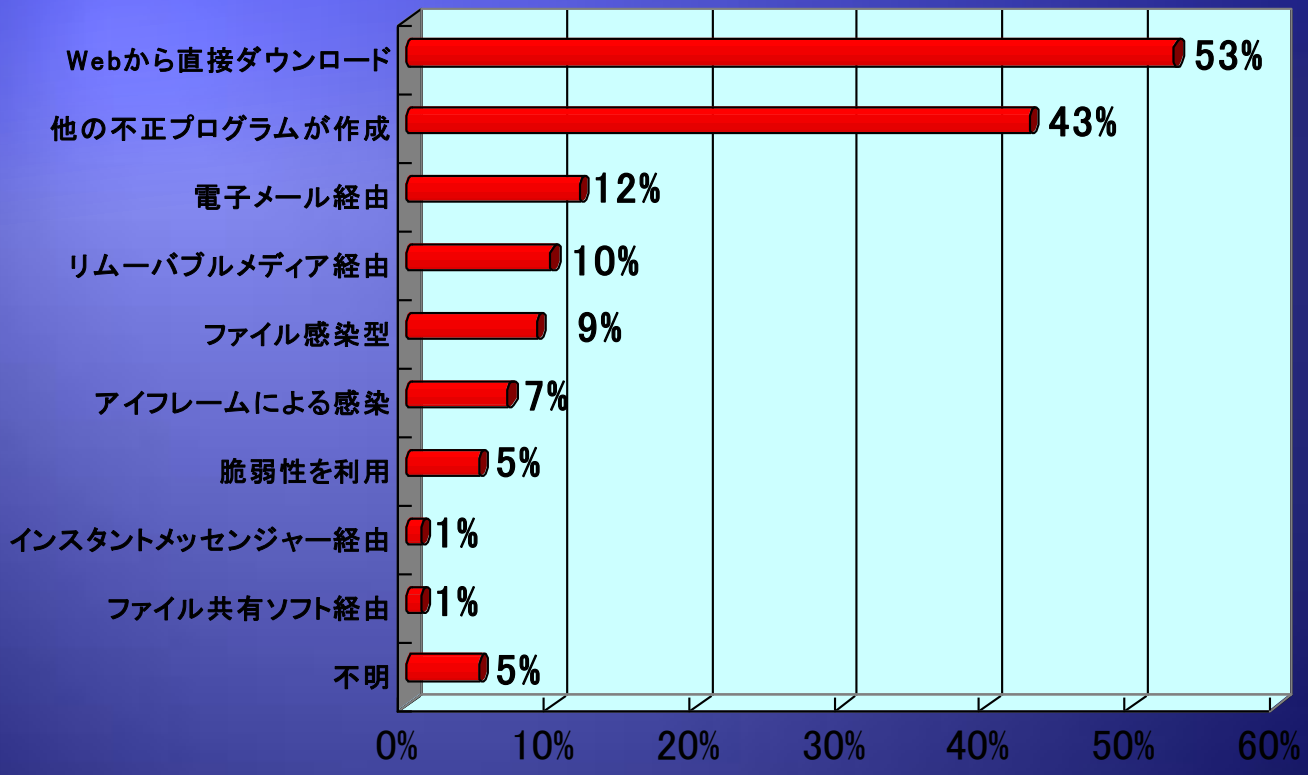
本データは、トレンドマイクロの日本サポートセンターへの問い合わせを元に集計しています。
各年の数値は、「ウイルス感染被害レポート」および「インターネット脅威レポート」で不正プログラム感染報告数上位10種の不正プログラムを種別の件数でまとめたものです。

発生しているマルウェアの数

2007年: 約5,500,000件

５３％・・・？

＜ウイルストラッキングセンター上位100種の不正プログラムにおける感染経路の割合＞



※このグラフは、2008年1月1日から11月25日の期間においてトレンドマイクロのウイルストラッキングセンターで全世界で感染数上位100種の不正プログラムを対象に感染経路を調査したデータです。
※ウイルストラッキングセンターのデータは、トレンドマイクロのオンラインスキャンでの検出や「Trend Micro Control Manager」で感染報告を送信した情報に基いて算出されます。
※複数の感染経路を持つものについては、感染経路1つにつき1カウントしています。

Agenda

1. 知っているようで知らない！？マルウェアとは？
2. 最近のセキュリティ環境を取り巻くマルウェア状況
3. アプリケーションサーバ構築時におけるマルウェア対策はどうあるべきか？
4. SQL サーバ導入において特に注意するべきマルウェア対策は？
5. まとめ

アンチマルウェアとデータ形式

- マルウェアは単体で EXE か COM 形式であるか、既存の EXE や COM 形式に感染
- スクリプト型 (VBS / JS など) もある
- つまりは実行可能なものに感染する
- アンチマルウェア製品は基本的にファイルをチェックする → 独自形式はわからない
- ！OS そのもののマルウェア対策は必須！

対応しないデータ形式での注意点

- 感染の可能性を検討しよう
  - マルウェアに関する知識が必要
  - OS 全般に渡る基礎知識
- どのような対策が可能かを検討しよう
  - OS レベルでのマルウェア対策
  - データ経路上でのマルウェア対策
- マルウェア対策によるパフォーマンス問題
  - 場合によっては致命的な問題になるケース
  - 検索除外で対応する必要性の考慮
- ローカルファイルが対策ソフトによって削除
  - アプリケーションによっては誤動作の可能性

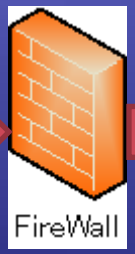
SQL サーバーは感染するか？

- SQL サーバーの稼動する OS は感染する
- SQL サーバーの脆弱性をついて感染の可能性
  - 例: SQL Slammer
    - SQL サーバーの脆弱性を攻撃
    - メモリ上でダイレクトアクション
    - 脆弱性への対策 → マルウェア対策とは分けて考慮
- データは感染するのか？？
  - バイナリデータを格納するケースで注意が必要
  - 純粋なテキスト形式以外のデータでも注意

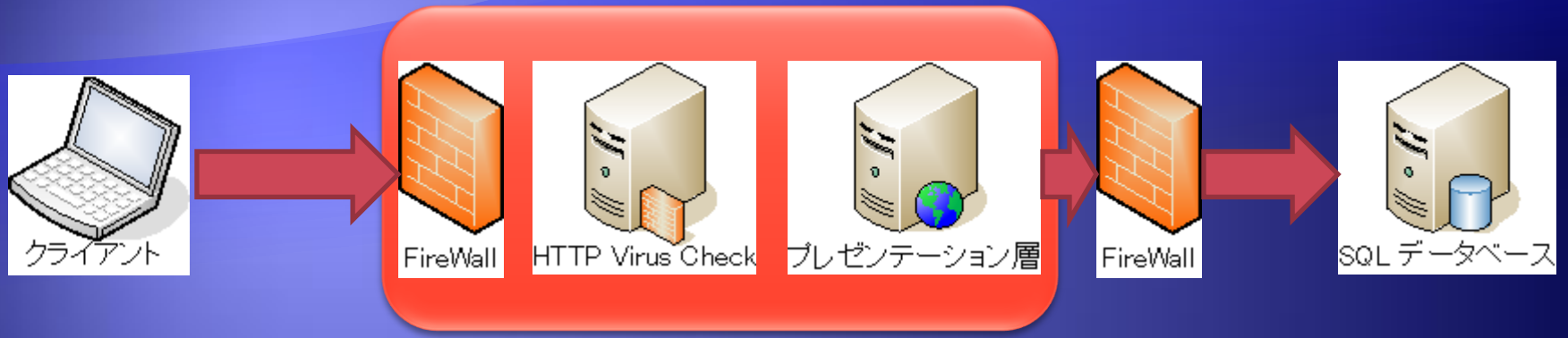
必要ならデータを保護しよう

専用のツールなどを利用して
直接ファイルのアップロード
/ダウンロード

OS 自体の対策では
データは保護されない



ではどうするべきなのか？



プレゼンテーション層の前で
HTTP SCAN などを用いて
危険をシャットアウト！

フローを変える事で
ダウンロードも安全に

起こりがちな問題点

- OS に導入したマルウェア対策製品の設定が不適切でアプリケーションや SQL サーバのパフォーマンスに致命的なダメージ
- OS に導入したマルウェア対策製品だけで十分と思い込み、思わぬ落とし穴に遭遇
- マルウェアに対する理解不足から思わぬ誤判定
  - OS の挙動を変更する VBS を動的に作成して実行

Agenda

1. 知っているようで知らない！？マルウェアとは？
2. 最近のセキュリティ環境を取り巻くマルウェア状況
3. アプリケーションサーバ構築時におけるマルウェア対策はどうあるべきか？
4. SQL サーバ導入において特に注意するべきマルウェア対策は？
5. まとめ

固有アプリケーションやSQL環境での注意点

- SQLデータベース内やアプリケーション固有のデータは中身を直接チェック出来ません
- SQLインジェクションへの対策やリモートからのセキュリティ侵害への対応は多く語られていますが･･･
- SQLに格納されるデータそのものの安全性を考慮するということまで懸念しているケースはまだまだ少ないのが現状です

質問コーナー