JPCERT CC®

近時の情報セキュリティに関する脅威の動向

JPCERT コーディネーションセンター
早期警戒グループ　リーダ
中谷　昌幸

講演者は、

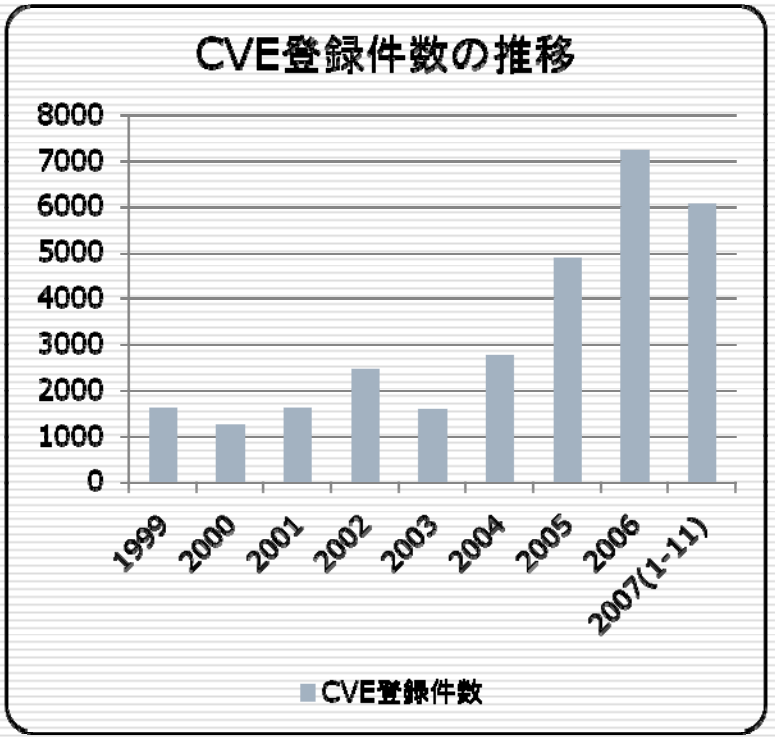
- JPCERT/CC の情報セキュリティアナリストです。
- 日頃、たくさんの情報を集めて、分析してます。
- やばい情報を見つけたら、注意喚起などの Alert を出します。
- 他に、インターネット定点観測システム(ISDAS)の保守、運用とか、各種調査の実施とか、いろいろやってます。

本日のトピック

- この一年の脅威について
  - 攻撃対象の変化
  - 金銭詐取を目的とした攻撃
- 対策は？

この一年の脅威について ー その1

- 今年も多くの脆弱性が検出、公開されました！
  - OS,オフィスアプリ,ブラウザ,ウイルス対策ソフト,ユーティリティ･･･ などなど
  - あらゆるカテゴリの製品で、脆弱性が発見された。
  - 中には非常に脅威度の高い脆弱性も。
- あまり大きく報道されないが、情報漏洩も引き続き多発している。



CVE:Common Vulnerabilities and Exposures

この一年の脅威について ー その2

- 攻撃が巧妙に！
  - あの手この手で感染を試みる『StormWorm』
    - 感染したPCはボットPCに！？
    - そして、さらなる攻撃に利用される。
  - 攻撃者のための管理ツールを含んだ攻撃ツール『Mpack』
  - 多種多様なスパムメール（doc,jpg(gif),PDF,Excel,mp3）
  - データなどを人質に金銭を詐取しようとするランサムウェア

この一年の脅威について

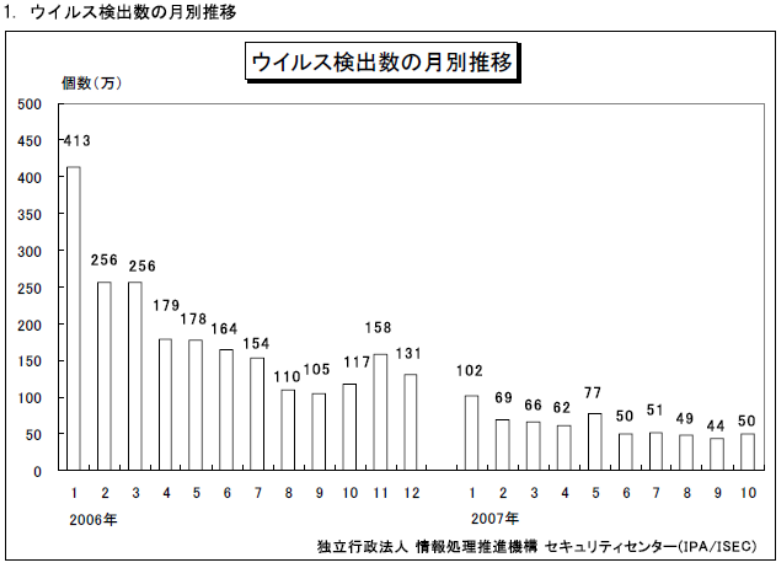
- 攻撃者は、
  1. 攻撃対象を『特定組織』に
  2. 攻撃目的を『金銭詐取』に

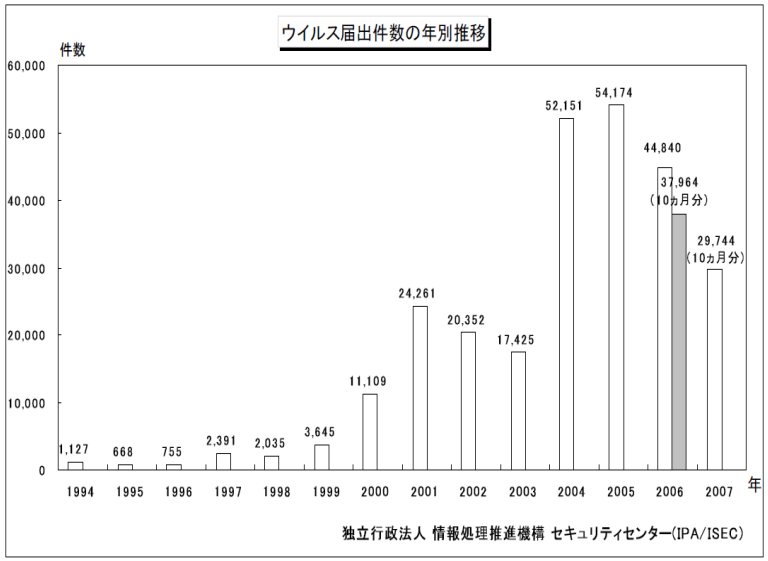
攻撃を仕掛ける！といった傾向に!?
（と、よく言われています・・・）

それって、日本でも？

攻撃対象の変化　－　日本の状況その1

- 不特定多数への感染を目的としていたウイルスから、「個人」、「組織」を対象に限定した範囲、時間（1日とか）に感染を試みるボットに変化している。
  - 実際に、IPA に届けられるウイルスも減少。

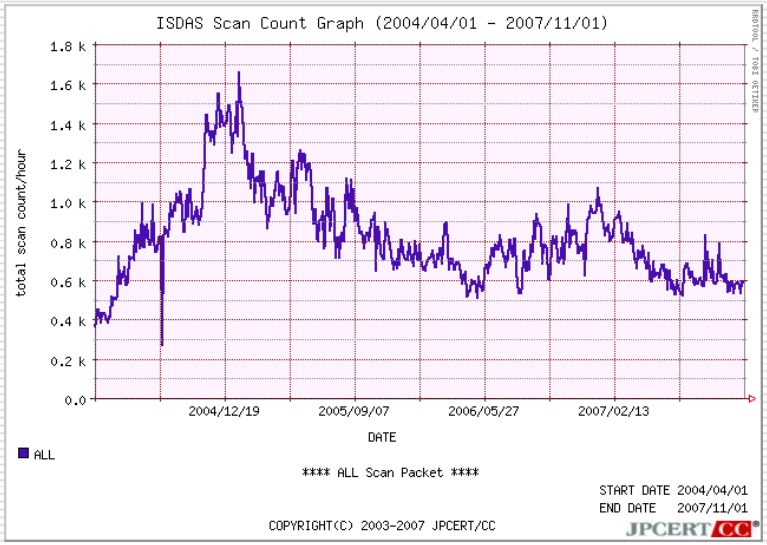


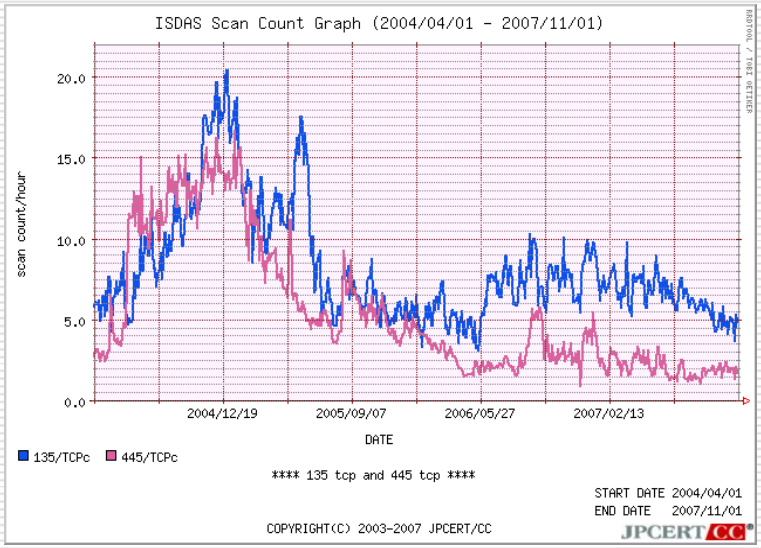


出典：情報処理推進機構 セキュリティセンター　コンピュータウイルス・不正アクセスの届出状況[10月分]について

攻撃対象の変化　－　日本の状況その2

- 定点観測システム（ISDAS）の観測データでも、無差別に送られてくる Scan パケットは、2005年頭をピークに減少。
  - 無差別に感染を広げるウイルスの減少が影響と思われる。





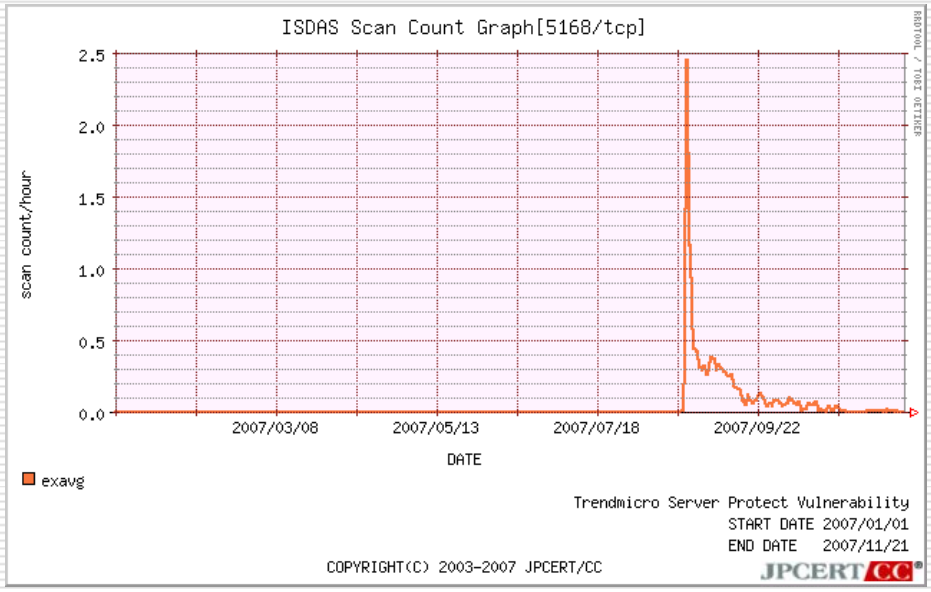
グラフ：定点観測システムISDAS観測データ

参考：TrendMicro ServerProtect の脆弱性を探索するScanの例

8/21 脆弱性に関するアドバイザリー公開
　　夕方から一部センサーで攻撃の予兆を観測
8/23 から攻撃が本格化。

- 脆弱性の情報が公開された2日後から攻撃が本格化したケース。

- 今でも悪用しやすい脆弱性があれば、ネットワーク経由での攻撃が行われる！



攻撃対象の変化　－　日本の状況その3

- 実際に特定組織あるいはグループに対してメールが送付されるケースが発生している。
  - 「小泉首相靖国参拝」
  - 「対日AD情報」(アンチダンピング)
  - 「不祥事への対応について」
  - 「知的財産権侵害実態調査(中国)結果データ」

  などなど

- 手口
  - 件名や送信者などを巧妙に細工されている
  - マルウェアが添付されているケース
    (未修正の脆弱性が悪用されることも。。。)

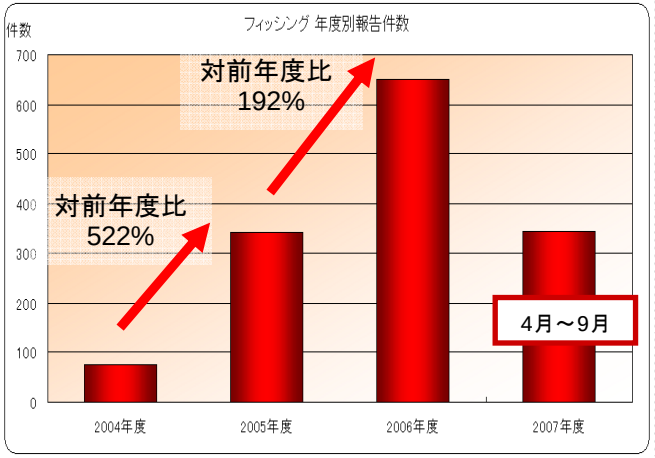
攻撃対象の変化　－　まとめ

- 「特定の組織を対象とした攻撃」ということが、海外ではよく言われていたが、

- 国内でも、実際に「限定された分野」や「特定の組織」を対象に攻撃が行われるようになってきたようだ！

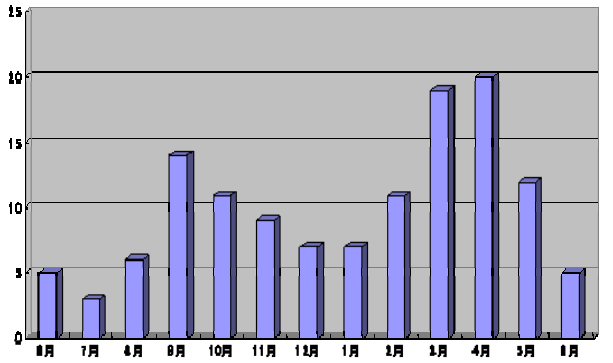
金銭詐取を目的とした攻撃 ー フィッシング

- JPCERT/CCへのフィッシング報告件数
  - 報告されるフィッシング（主に日本で立ち上げられたフィッシングサイト）の届出件数も右肩上がりで増加



出典；JPCERT/CC フィッシング統計

- フィッシング対策協議会4半期レポートでもフィッシング情報の届出が全体的に増加傾向に！



フィッシング情報の届出件数（2006年6月～2007年6月）

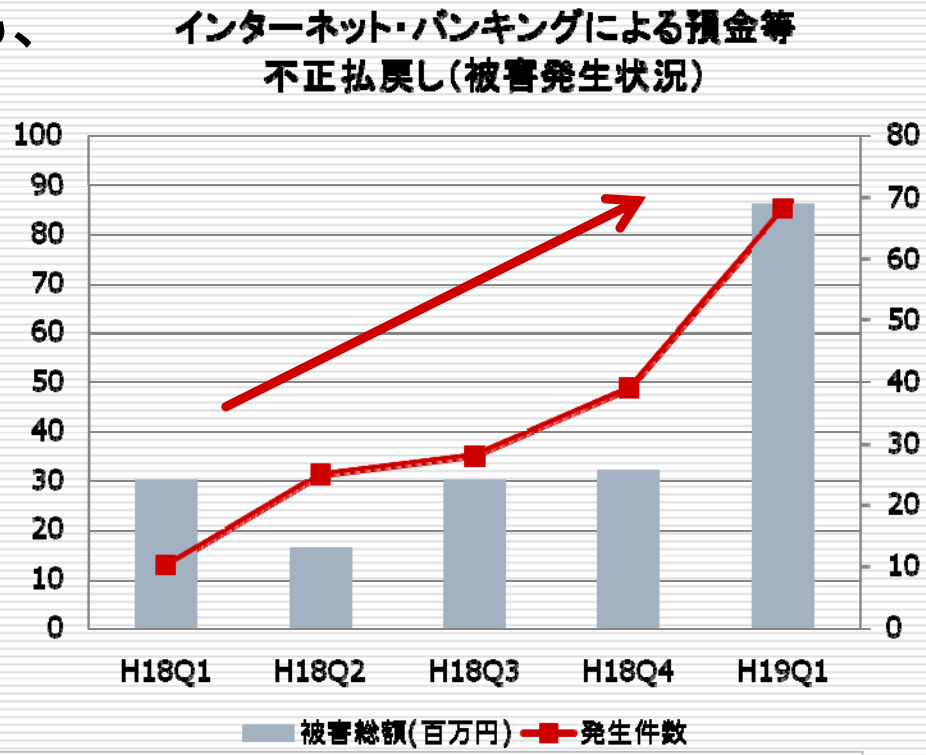
出典：フィッシング対策協議会4半期レポート2007年4-6月期

金銭詐取を目的とした攻撃 ー　偽セキュリティソフト

- 偽セキュリティソフトによる金銭的被害
  - IPA への不審なセキュリティソフトに関する相談も、2005年度から寄せられ初めて、2006年度には356件も。
    （ 07/11/8：日本経済新聞夕刊23面「駆除ソフト詐欺ご用心」より）
  - 国民生活センタ
    セキュリティソフトに関するトラブル
    http://www.kokusen.go.jp/soudan_now/data/sn-20071029.html
    - 偽セキュリティソフトに関する問い合わせも。

金銭詐取を目的とした攻撃
ー　インターネットバンキングにおける被害

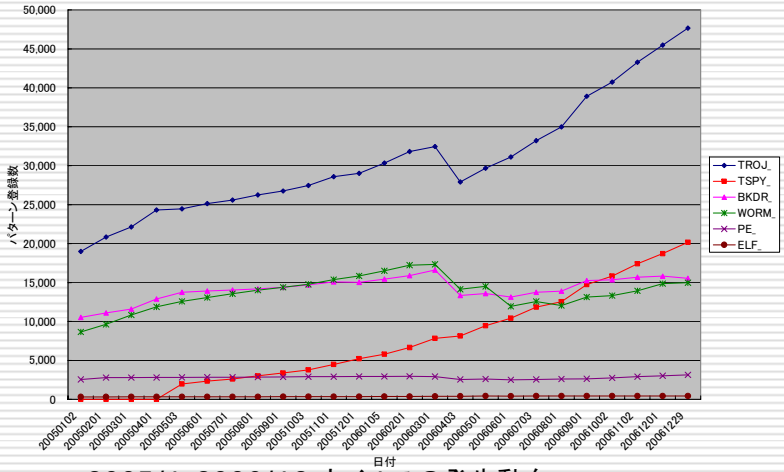
- 金融庁に報告のあったインターネットバンキングにおける被害発生状況でも、発生件数は確実に増えている。



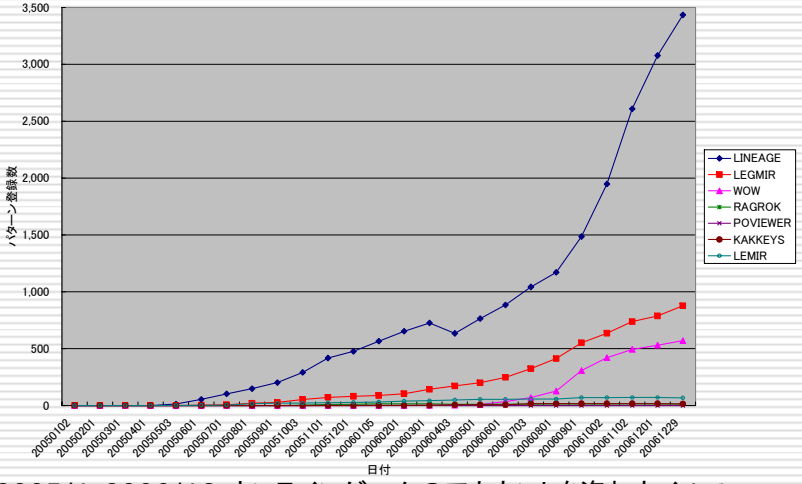
参考：金融庁 偽造キャッシュカード等による被害発生等の状況について

金銭詐取を目的とした攻撃 ー ウイルスタイプの変化

- 情報を盗み出すTROJやスパイウェアが増加
- さらにオンラインゲームのアカウント情報を盗むタイプの増加が著しい
  - RMT による現金化が目的？



2005/1-2006/12 ウイルスの発生動向



2005/1-2006/12 オンラインゲームのアカウントを盗むウイルス

出典：JPCERT/CC マルウェアの最近の傾向とウェブアプリケーションの脆弱性を狙うボットの実態

金銭詐取を目的とした攻撃　－　まとめ

- やはり国内でも「金銭詐取を目的とした攻撃」が増えているようだ！

対策は？

- 「特定の組織」に、「金銭を詐取する目的」で仕掛けられる攻撃に対応していくには、
  - 個人の対策だけではなく、
  - インシデントが発生したときに「組織的に対応できる力」が重要

- JPCERT/CCでは、
  「組織的に対応できる力」＝「組織内CSIRT」の構築を支援しています。

CSIRT については、NTT-CERT 杉浦さんの講演で！

お問い合わせ先

- JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/
- インシデント報告
  - Email：info@jpcert.or.jp

    PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73　57 EE 3C 2B 13 F0 48 B8
  - 報告様式

    http://www.jpcert.or.jp/form/

JPCERT CC®

ご清聴ありがとうございました