マルウェア

ネットワークと情報セキュリティ3

菊池　浩明

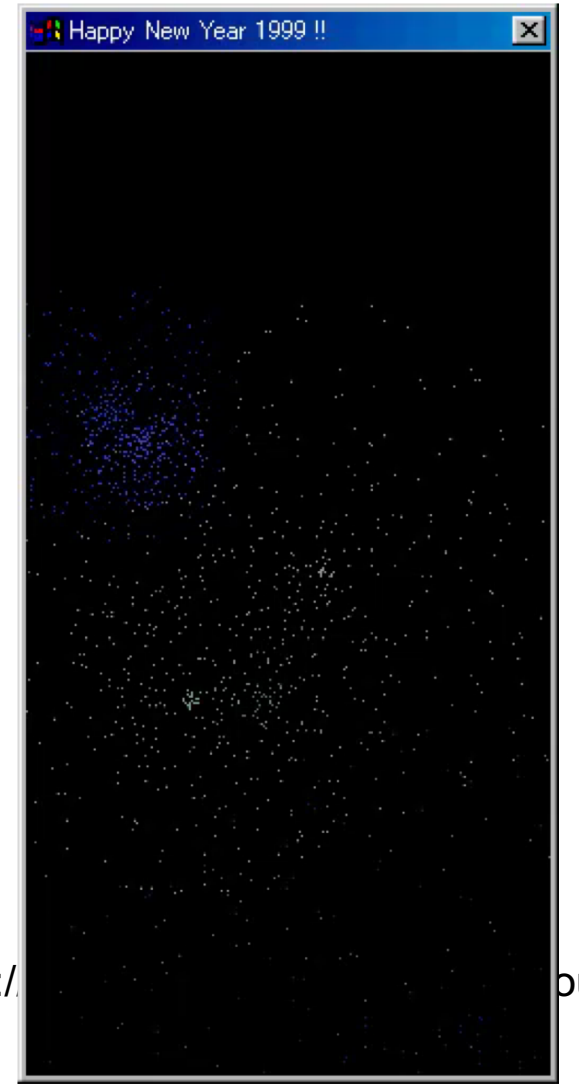
CONTENTS

- コンピュータウィルス
- 不正アクセス
  - ファイヤウォール
  - IDS

1. マルウェアの脅威

コンピュータウィルス図鑑

- TROJ_SKA
  - 通称：Happy99
  - 花火が表示されている間に，自分自身の複製を作る．
  - メールを送るたびに，HAPPY99.exeを添付



http:/ outline

MS Blaster

- W32.Blaster.worm
  - 2003/7/17 MS, Windows 2000/XP (95/98/Meは大丈夫) RPCの脆弱性発表
  - 8/12　19万台感染
  - TCP 135 によるネットワークからの侵入（Worm）
  - 修正セキュリティパッチ
  - 8/29 米，作者（18歳）逮捕

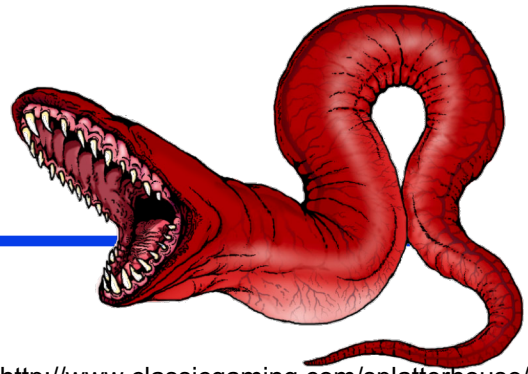
発病画面（シャットダウンを繰り返す）

マルウェア

- 定義
  - 次の機能を(一つ以上)持つ悪意を持つ (Malicious) プログラム(software)

1. 伝染 （自己伝染機能）
   プログラムやデータの一部を書き換える
   自分自身の複製を作る(感染）
   感染先を探す．他へコピーする
2. 潜伏
   感染していることを隠す．ログを消す
3. 発病
   » 「いいこと」をする
   » 1. 花火，2. メモリ浪費，3. 機密漏洩，4. ファイル削除

ワーム [伝染機能]



http://www.classicgaming.com/splatterhouse/worm.jpg

- 定義
  - 自立して自己増殖が可能なウィルス （伝染機能）
  - 「ミミズなどの虫，寄生虫」
  - “Internet Worm” （1988年）
    - sendmailのbuffer overflow
    - 全米6,000台（全体の10%)
    - CERT/CC (コンピュータ緊急対応センター）が設立
  - W32.Nimda.A@mm （2001年）
    - Windows IISの脆弱性
    - ローカルファイルのhtmlから抽出したアドレスへ送信
    - ファイル共有から感染

トロイの木馬 [潜伏]

http://www.intellectualconservative.com/article2506.html

- 定義
  - 感染機能を持たないウィルス （潜伏機能）
  - 有用なプログラムの振る舞いを真似る
  - ギリシャ神話トロイ軍との戦い
  - login
    - » ユーザID, Passwdのプロンプト．正規の処理呼び出し．
    - » 裏側でPasswdを送付．
  - AIDS情報入門 (1988)
    - » AIDSに関する質問と診断
    - » 90回起動後に全てのファイルを暗号化．復号の為にはパナマの口座へ送金を指示
  - Back Olifice

スパイウェア [発病]

- 不正を行うプログラム
  - ウィルス，ワーム，トロイの木馬
  - ロガー (logger)
    - » キーボードでの
      全ての入力をログ
    - » 実行されていても
      気がつかない

SpyEye

- 銀行をターゲットとした攻撃
- 偽のポップアップメッセージを提示
  - Man-in-the-browser

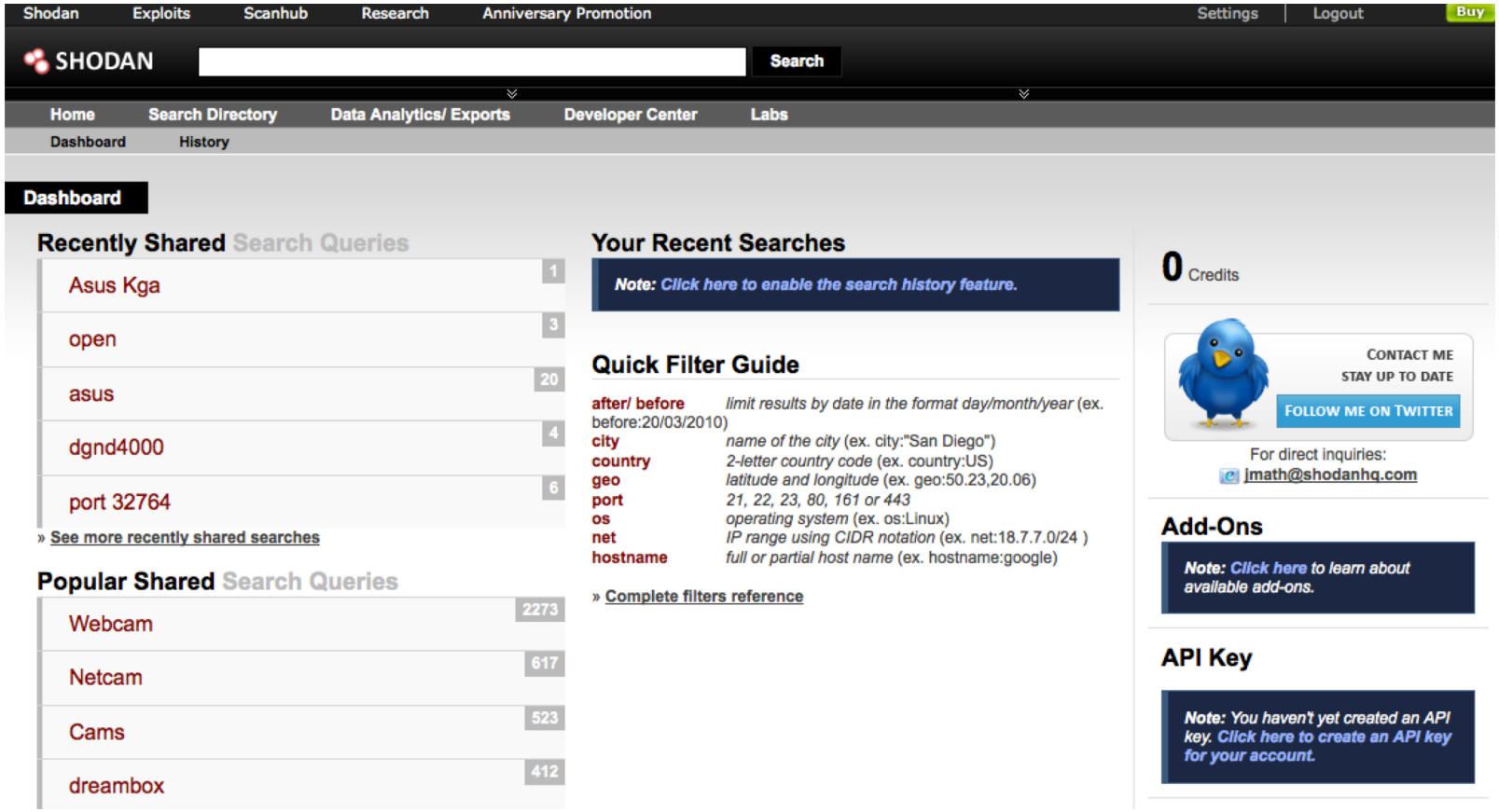
偽の情報入力画面例（三菱東京UFJ銀行の情報から引用）
http://itpro.nikkeibp.co.jp/article/NEWS/20121030/433523

What is “Mirai”

- Mirai botnet
  - composed primarily of embedded and IoT devices, took the Internet by storm in late 2016 when it overwhelmed several high-profile targets with massive distributed denial-of-service (DDoS) attacks
  - an unprecedented 623 Gbps DDoS attack on Sep. 21, 2016.

Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera
pass	Axis IP Camera	admin	IPX-DDK Network Camera
888888	Dahua DVR	system	IQinVision Cameras
666666	Dahua DVR	meinsm	Mobotix Network Camera
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers
666666	Dahua IP Camera	1111111	Samsung IP Camera
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router
cat1029	HiSilicon IP Camera	supervisor	VideoIQ
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera
klv123	HiSilicon IP Camera		

SHODAN (脆弱デバイス検索エンジン



制御システムを狙うマルウェア

- Stuxnet (2010)
  - イランの核燃料再処理プラントPLC
- Havex (2014)
- BlackEnergy (2015)
  - 変電所管理SCADAソフトの脆弱性
    - » 監視を停止，ファイル消去，コールセンターに禍荷電
  - 2015年12月，ウクライナ西部を6時間に渡り大規模停電，40万人が影響

Stuxnet

- 2010年，イランの原子力発電所を対象としたマルウェア
  - サイバーセキュリティ
  - Closed なネットワークでも，USBメモリーを介して感染

イランの原子力施設

http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html

BadUSB

- USBデバイスの脆弱性(?)
  - Black Hat USA 2014
  - 見た目はメモリだが，
    自動入力盗聴機能を
    持つキーボードデバイス
  - 2GB, $55.99

ハードウェアキーロガー
KeyGrabber Wi-Fi Premium

https://www.keelog.com/wifi_hardware_keylogger.html

攻撃者の変化 (IPA「2013年10大脅威」より抜粋)

	2001年	2004年	2009年
背景	不正アクセス禁止法(2001)	個人情報保護法(2005)	国家安全保障
マルウェア	Nimda (2001), Code Red (2001)	P2P (2005), スパイウェア (2005)	米国DDos(2009), Stuxnet (2010)
目的	いたずら	金銭目的	国家安全

マルウェアの命名規則

- 発見者が命名
  - Nimda　　**Admin**istrator の反対
  - SirCum　　プログラム名
  - Klez　　暗号鍵の一部
  - codeRed　　炭酸飲料「マウンテンデュー」
  - soBig　　架空アドレス big@boss.com
  - Worm_MSBlaster.D = Nachi = Welchia

わざと「ださい」名前を付ける

http://hotwired.goo.ne.jp/news/news/culture/story/20030910206.html

誰が何のために作っているのか

- 2000/5/12
  - “I LOVE YOU”
  - マニラのコンピューター学校の男子学生(23)
  - フィリピン国家捜査局(NBI)の家宅捜索

http://www.sankei.co.jp/databox/nw/

攻撃者の変化 (IPA「2013年10大脅威」より抜粋)

	2001年	2004年	2009年
背景	不正アクセス禁止法(2001)	個人情報保護法 (2005)	国家安全保障
マルウェア	Nimda (2001), Code Red (2001)	P2P (2005), スパイウェア (2005)	米国 DDos(2009), Stuxnet (2010)
目的	いたずら	金銭目的	国家安全

2. マルウェアのしくみ

どうやって感染するか？

- 不用意に未知の「感染」プログラムを実行
  - メディア（FD, USB）から起動する
  - メール添付ファイルを開く（マクロウィルス, Melissa）
  - ウェブページを開く（Nimda)
  - 何もしない?! (ワーム，ネットワークから侵入）
  - Winny (危険性を顧みず，ついインストール）

バッファオーバーフロー

- バグのあるプログラム

buf.c

```
1  main(){
2       char a[10] = "", b[10] = "";
3          gets(b);
4          printf("a = %s¥n", a);
5          printf("b = %s¥n", b);
6  }
```

※gets(char *b) : キーボードから
文字をbへ読み込む
セキュリティホール

- 正しい入力

```
./buf
HELLO
a =
b = HELLO
```

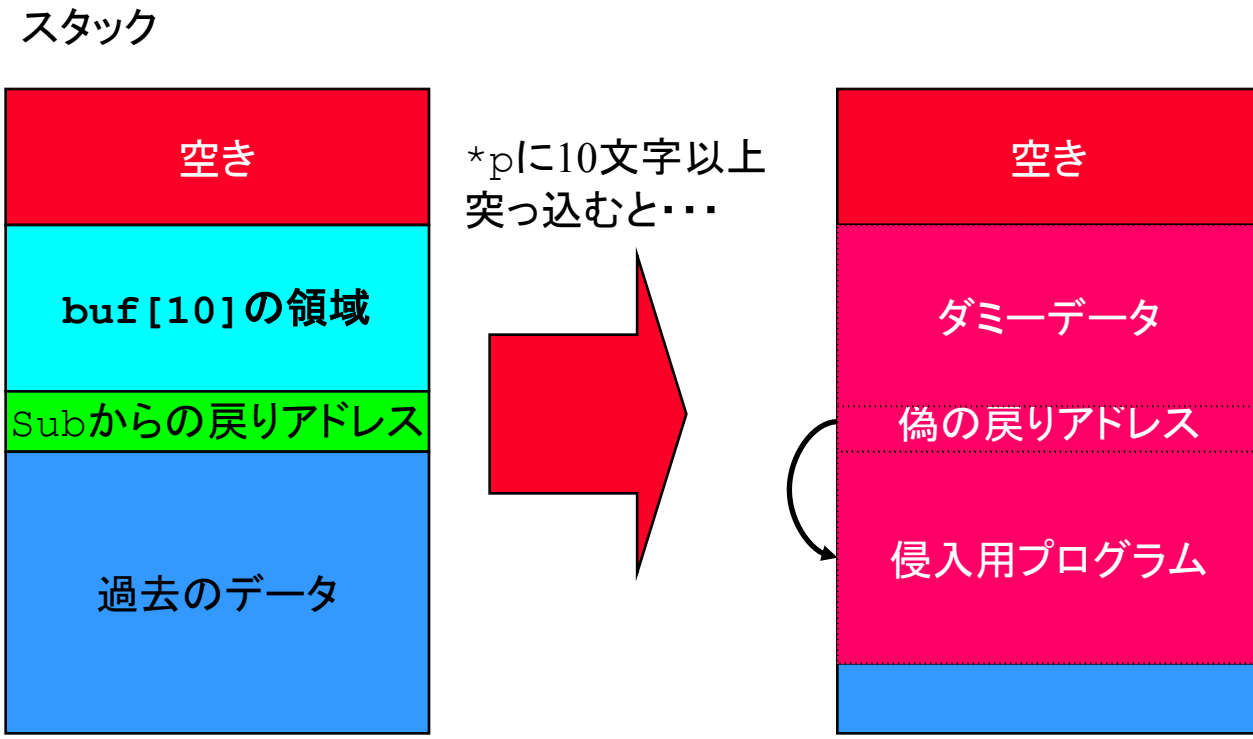
- 不正な入力

```
./buf
HELLO123456789
A = 89 入力されてない!!
B = HELLO123456789
```

スタックオーバーフロー

- C言語の文字列データは「NULLで終わる」以外のルールがないことを利用してバッファ領域を破壊

```
void sub()
{
   char buf[10];
   …
   strcpy(buf,p);
   …
   return;
}
```



アセンブラと機械語

- アセンブラ(CASL)
- 機械語(COMET)

ニモニック（命令）　オペランド

```
PGM    START BEGIN
BEGIN  LD    GR0,A
       LAD   GR1,A
       LD    GR2,0,GR1
       LAD   GR3,0,GR1
       RET
A      DC    #27
B      DC    #1D
C      DS    1
       END
```

記号アドレス

アセンブラ命令

アセンブル →

逆アセンブル ←

"バイナリ"

アドレス	データ
0000	1000 0009
0002	1210 0009
0004	1021 0000
0006	1231 0000
0008	8100
0009	0027
000A	001D
000B	0000

例) 総和を求める

```
0000 PGM      START  BEGIN
0000 BEGIN    LAD     GR0,0
0002          LAD     GR1,0
0004 LOOP     ADDA    GR0,A,GR1
0006          ADDA    GR1,ONE
0008          CPA     GR1,COUNT
000A          JMI     LOOP
000C          ST      GR0,B
000E          RET
```

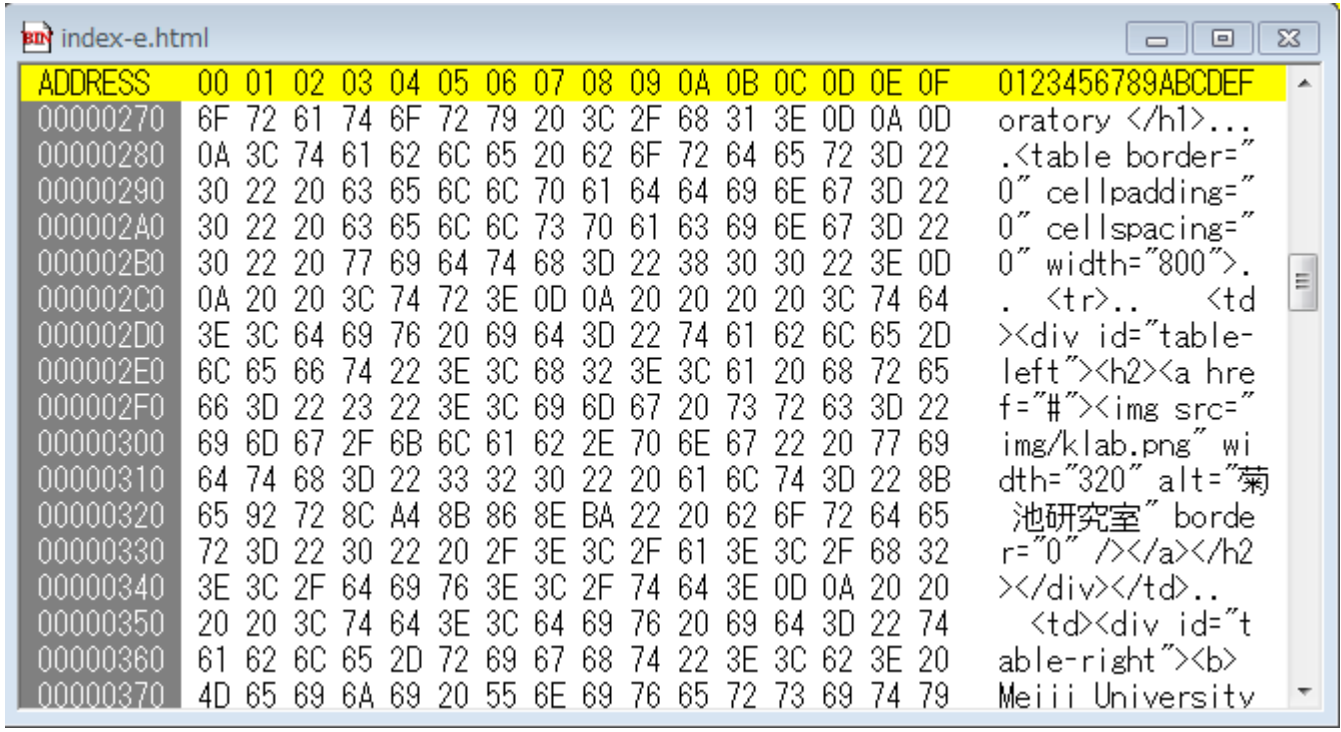
(Java)

```
GR0=0;
for(GR1=0;
    GR1 – Count <0;
    ++GR1){
    GR0 = GR0 +A[GR1];
}
B[0] = GR0;
```

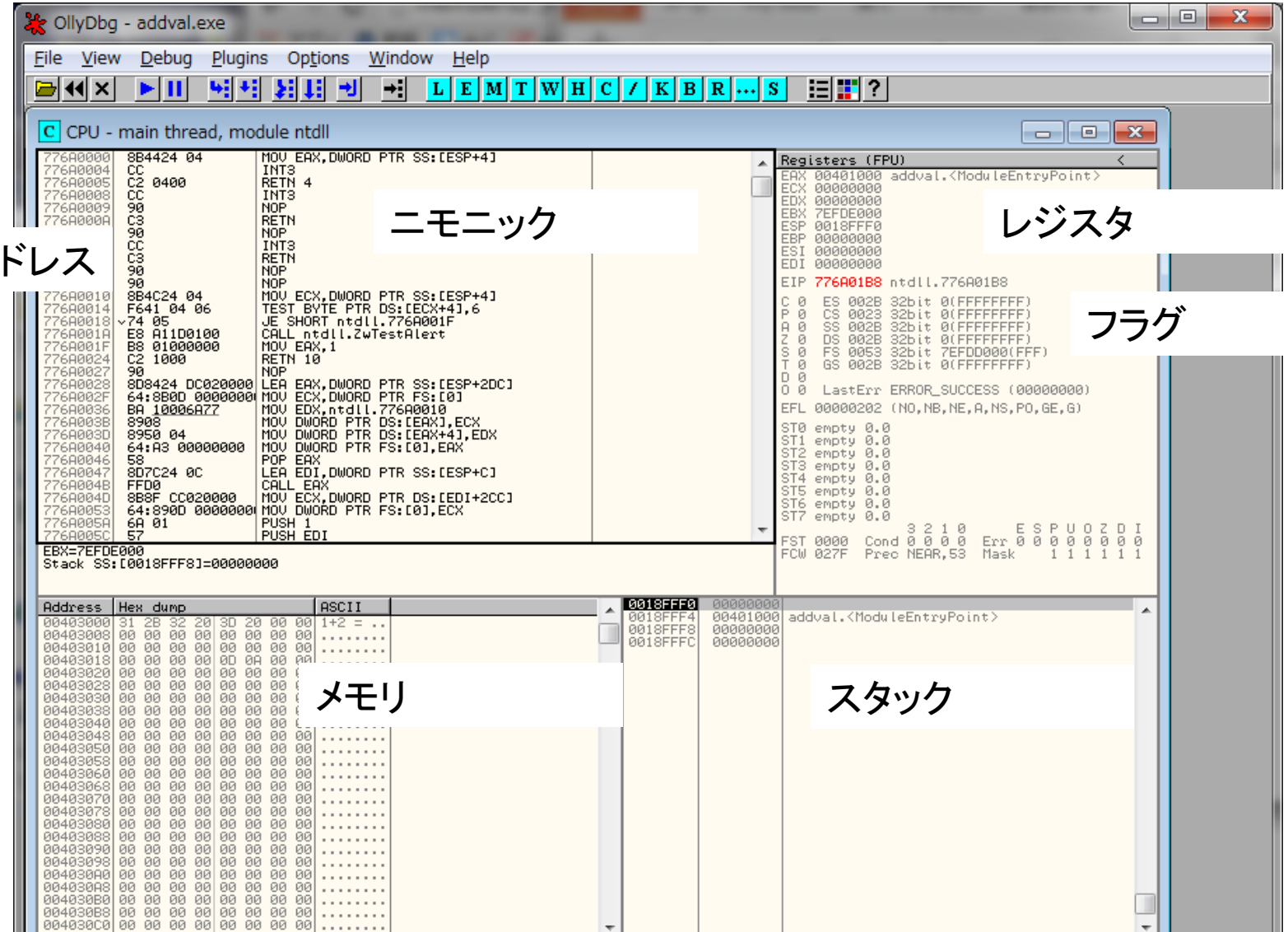
メモリーダンプ

- Stirling（バイナリエディター）

```
<table border="0"
cellpadding="0"
width="800">
  <tr>
  <td><div id="table-
left"><h2><a
href="#"><img
src="img/klab.png"
width="320" alt="菊池研
究室" border="0"
/></a></h2></div></td>
```

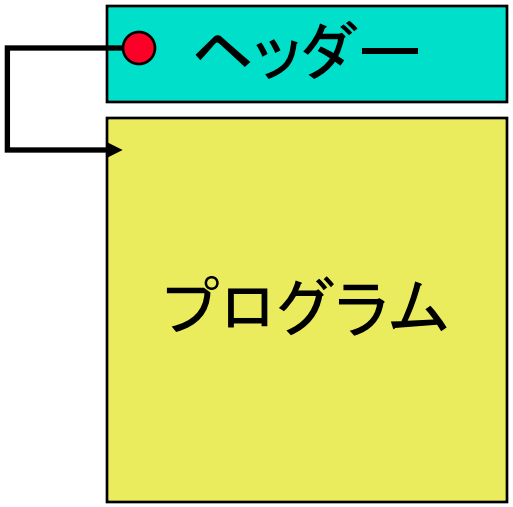


逆アセンブラー OllyDbg



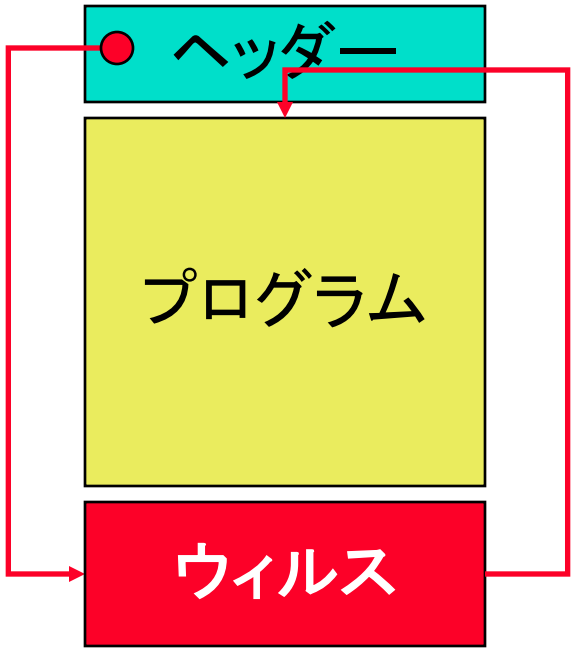
感染の原理

- 実行型プログラム



  - COM, EXE形式

- 感染後

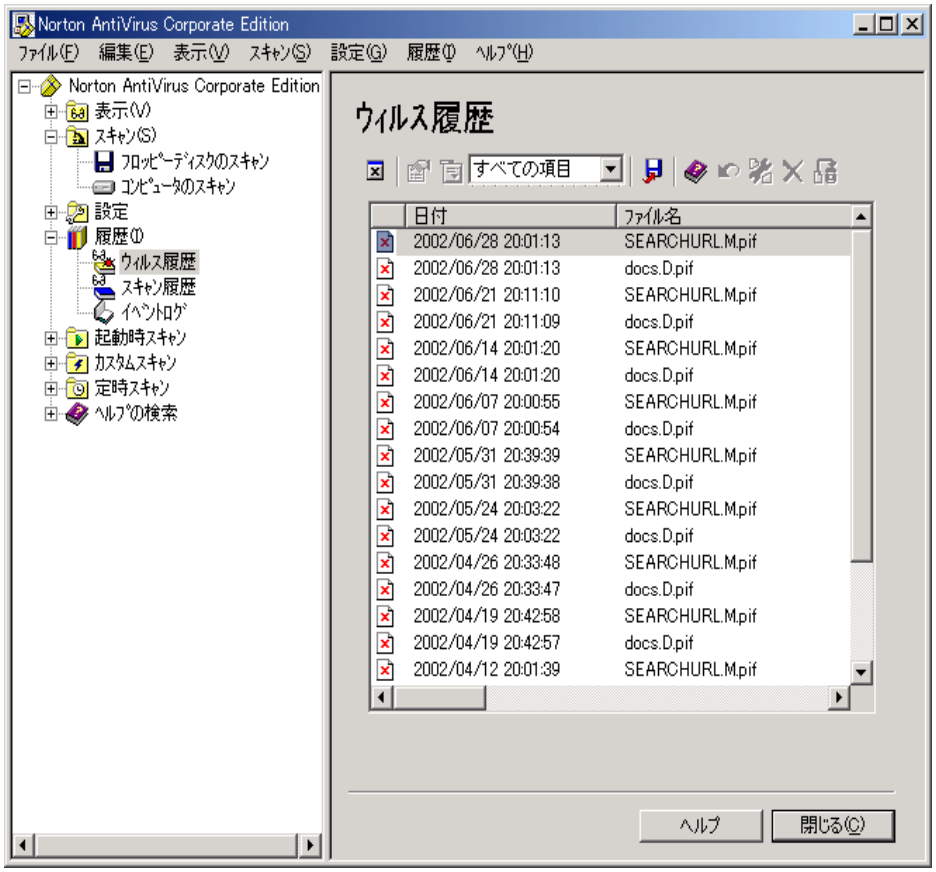


  - プログラムは動き続ける

3. マルウェア対策

1. アンチウィルスソフト

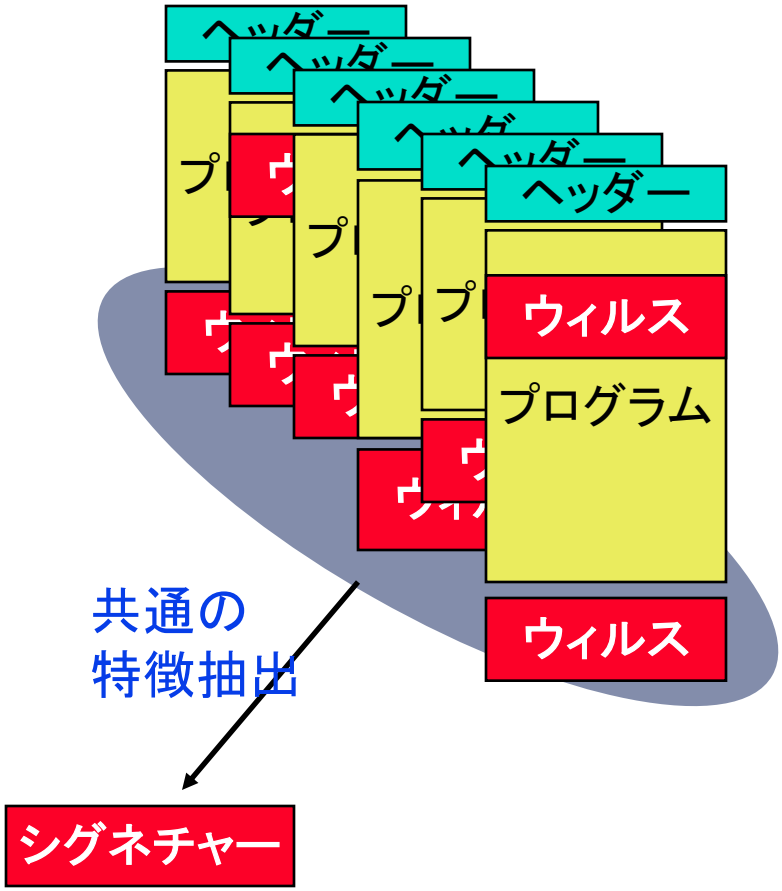
- 通称「ワクチン」
  - 常時起動
  - 定期的に検査
  - ファイル
  - メール



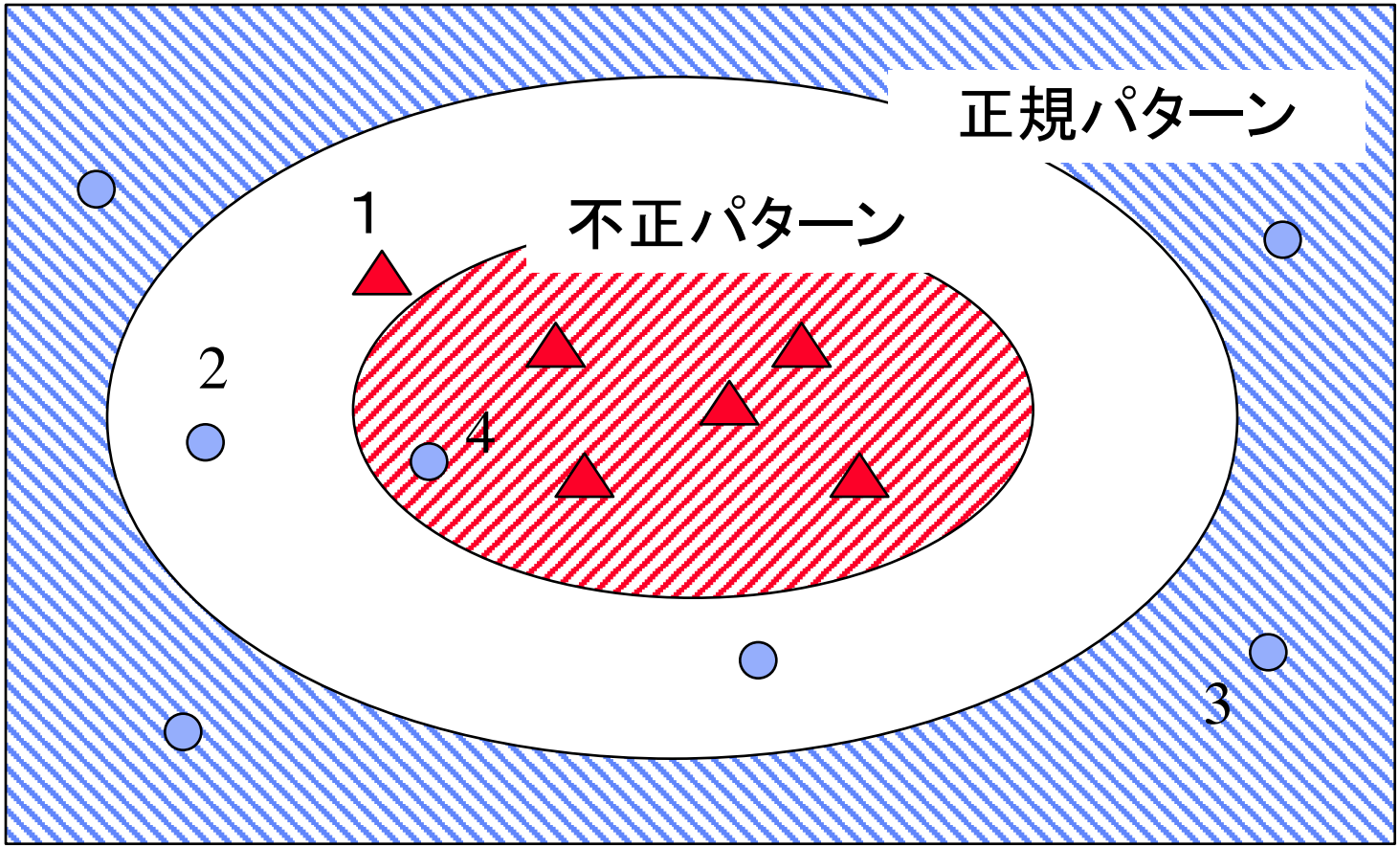
Norton AntiVirus 7.51

シグネチャー

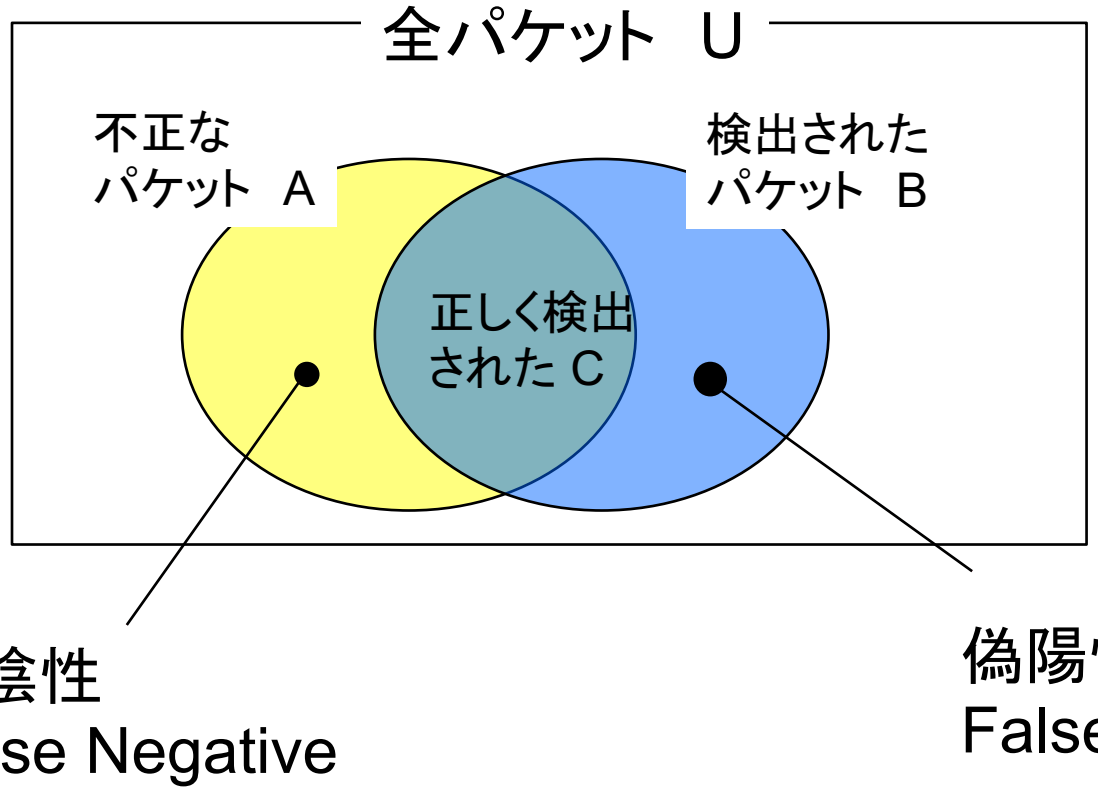
- パターンデータベース
  = シグネチャー
  - サイズ小さく
  - 変種への適応
  - 誤認識低く
  - (2-3MBのサイズで3-5万種のウィルス対応）
  - 更新し続ける必要性



異常検出



検出誤り


全パケット U
不正な
パケット A
検出された
パケット B
正しく検出
された C
偽陰性
False Negative
偽陽性
False Positive

検出誤り

sip	dip	sp	dp	通過
NetA	NetA	any	80	pass
NetA	NetA	any	53	pass
NetA	NetB	any	80	pass
NetA	NetB	any	53	**drop**
NetB	NetA	any	80	pass
NetB	NetA	any	53	pass
NetB	NetB	any	80	**pass**
NetB	NetB	any	53	drop

- ルール.
  - deny all
  - allow sip=NetA
  - allow dip=NetA

真 / 検出	許可	拒否
許可	5	**1 (FN)**
拒否	**1 (FP)**	1

静的解析と動的解析

	静的解析	動的解析
方法	バイナリを逆アセンブルして不正プログラムの内容を解析する	対象プログラムを安全な環境で実行して，振舞いを観測する
長所	正確にプログラムの再現をすることが出来る.	高速に振舞いを検知できる. 機械的に自動化処理.
短所	解析に専門知識が必要で時間がかかる.	マルウェアが観測されていることを検知して，不正の再現を停止してしまう.
例	逆アセンブラ―，メモリーダンプ	仮想環境，サンドボックス

DEP (Data Execution Prevention)によるデータ保護

IPA セキュアプログラミング講座 C言語編　図10-7

2. 不正アクセス禁止法

- 不正アクセスの禁止(3条)
  - 識別符号(IDとパスワード)を入力することで利用できるようになっているコンピュータに，ネットワークを通じてアクセスし，利用できる状態にしてしまう(セキュリティホールを利用すること)行為.
  - 1年以下の懲役または50万円以下の罰金
- 不正アクセスを助長する行為(4条)
  - 他人のパスワード販売, 掲示
  - 30万円以下の罰金
- 管理者の義務(5条), 警察への協力(6条)

「不正アクセス」はどれか？

1. 教授に頼まれて教授のIDでメールした
2. sendmail のセキュリティホールをつついた（侵入はしなかった）
3. イントラネットでパスワードを推測して課長になりすました
4. ふられた腹いせに彼女のIDとパスワードをウェブ掲示板にただで出した
5. 計算センタに忍び込んでコンソールから成績を改ざんした

3. サイバー演習

- 総務省「実践的サイバー防御演習(CYDER)」
  - 2013年より3回
  - 2015年度，全8回，計101組織(応募345)，275名，
  - 12のマイルストーン
    - » 事象発見，通報，収集，証拠保全
    - » 可否判断
    - » 原因推定，復旧，再発防止
- セプター
  - 官公庁　25，
  - 地方自治体　32，
  - 金融　27
  - 独法　6

http://biz.nikkan.co.jp/news/nkx0220151027a

標的型攻撃演習

- 訓練サービス (GSX)
  - 訓練メールの送信
  - クリック率のレポートと教育

http://www.gsx.co.jp/informationsecurity/attackmailtraining.html

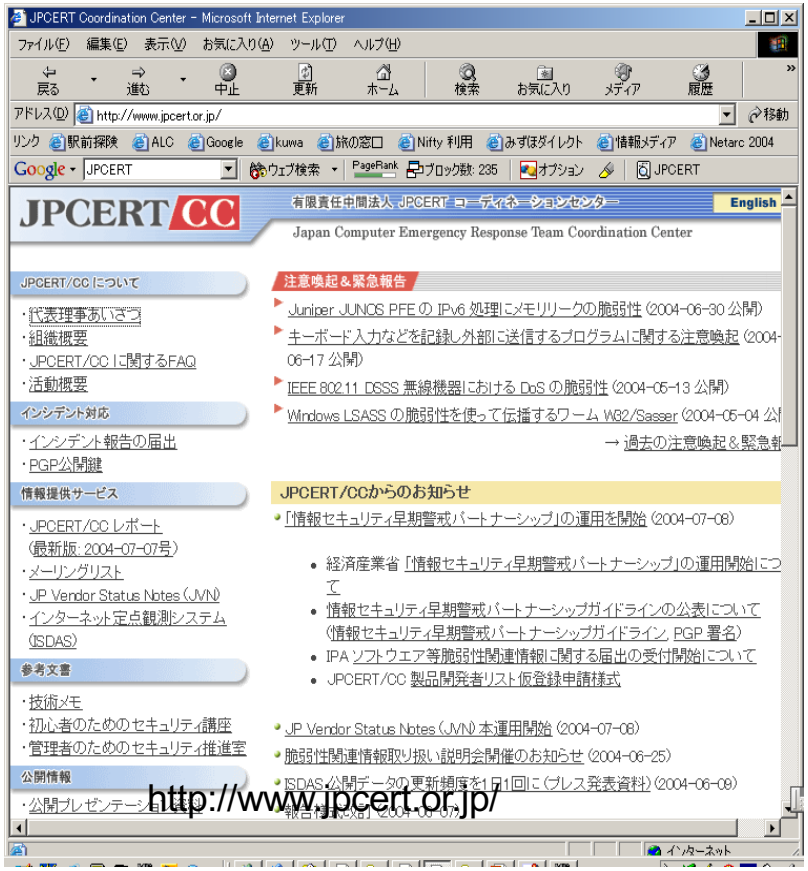
4. CSIRT

- computer security incident response team (CSIRT)
  - 1988 CERT
  1. SOC(Security Operations Center) 検出
  2. Incident Response Team 対応
  3. Forensic investigators 保全
  4. Engineering team

インシデント対応組織

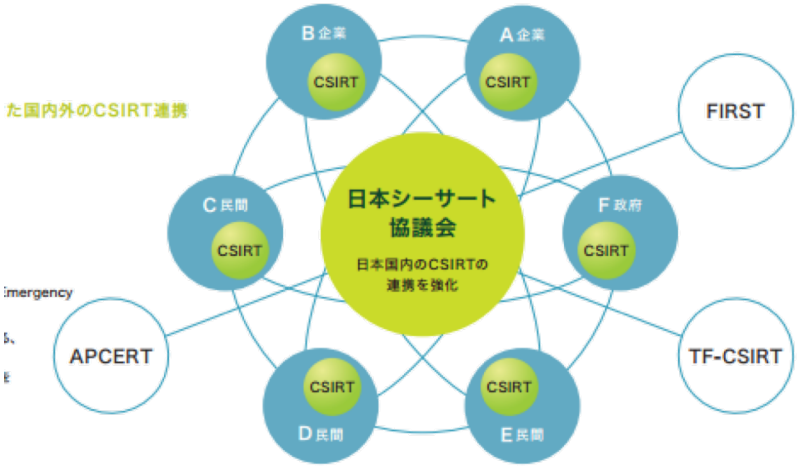
- JPCERT (Japan Computer Emergency Response Team)
  - インシデント(事件）の対応
  - 関連組織の連携
  - インシデントの報告
  - 他の組織(CERT/CC，IPAセキュリティセンタ)との連携

- 法的対応も担う
  （不正アクセス禁止法など）



日本シーサート協議会 NCA

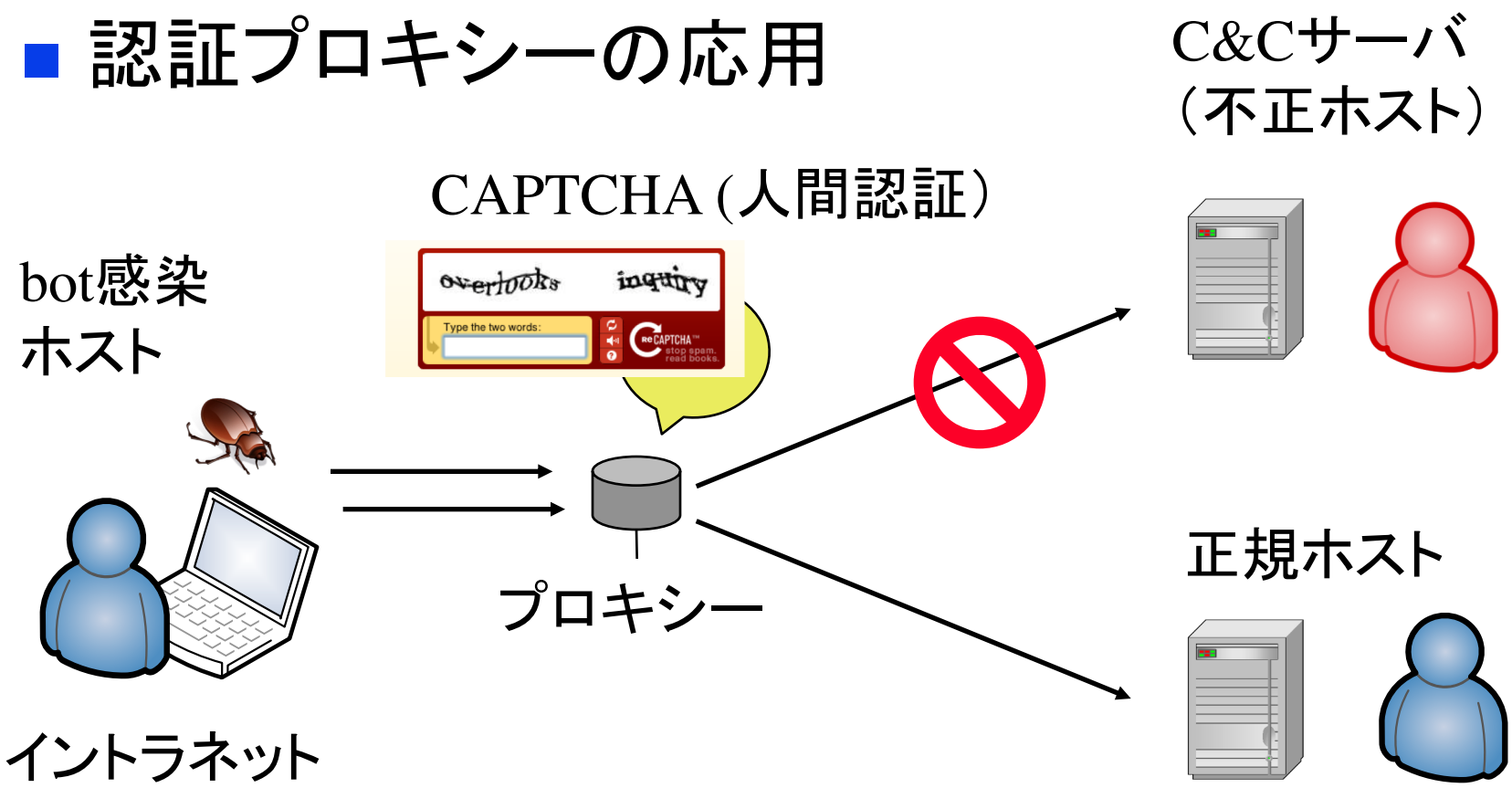
- 2007年設立
  - JPCERT/CC事務局
  - 会員間情報共有
  - ワーキングループ
  - 年次会合
- 106組織
  （waiting 90組織）



http://www.nca.gr.jp/

5. 出口対策

- 認証プロキシーの応用



まとめ

- マルウェアは（　　）という意味のmalicious なsoftwareから来ている．ウィルスの定義とされる（　　），（　　），（　　）の3つのどれかを有する．
- 不正行為の目的は，従来のいたずらから，（　　）や国家安全に移行してきている．
- 有効なポートをランダムに検査する（　　），不正なデータを送信して管理領域を書き換える（　　）などの攻撃手法がある．