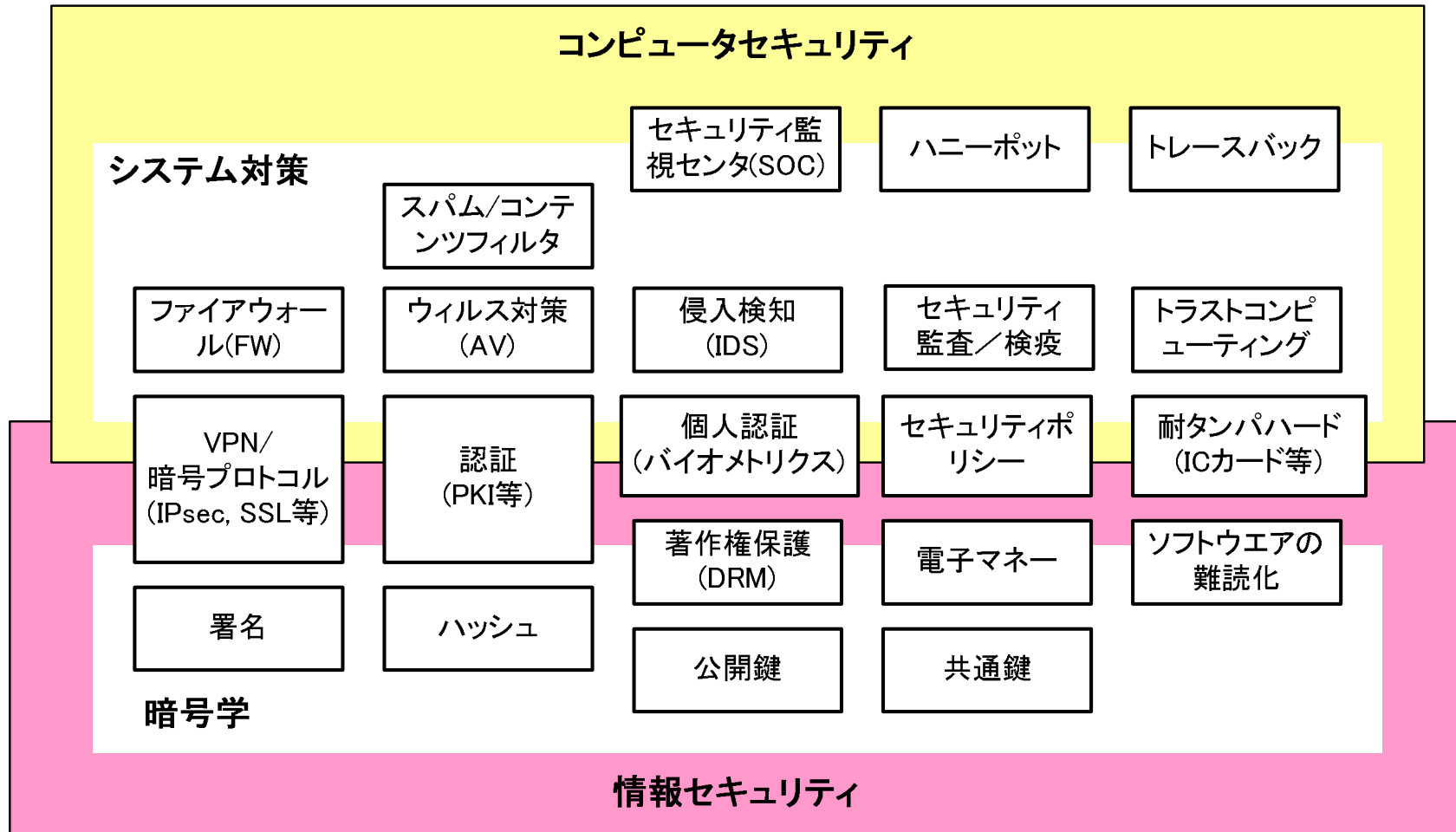


テレコム九州情報ランナー

ハッキングの手口とセキュリティ対策
～基礎編～

2010年12月16日
KDDI研究所 竹森 敬祐

セキュリティの全体像



注)セキュリティの全てのテーマを包含しきれていない。

目次

九州テレコム
振興センター

【ハッキングの手口】

- パスワード攻撃
- 踏み台
- 攻撃ツールの入手
- ホームページ改ざん
- フィッシング
- 情報漏洩
- ウィルス感染
- ボットネット

【セキュリティ対策】

- ファイアウォール(FW)
- アンチウイルス(AV)
- スпам／コンテンツフィルタ
- 侵入検知システム(IDS)
- セキュリティ監査
- セキュリティ監視センター(SOC)
- ハニーポット

パスワード攻撃

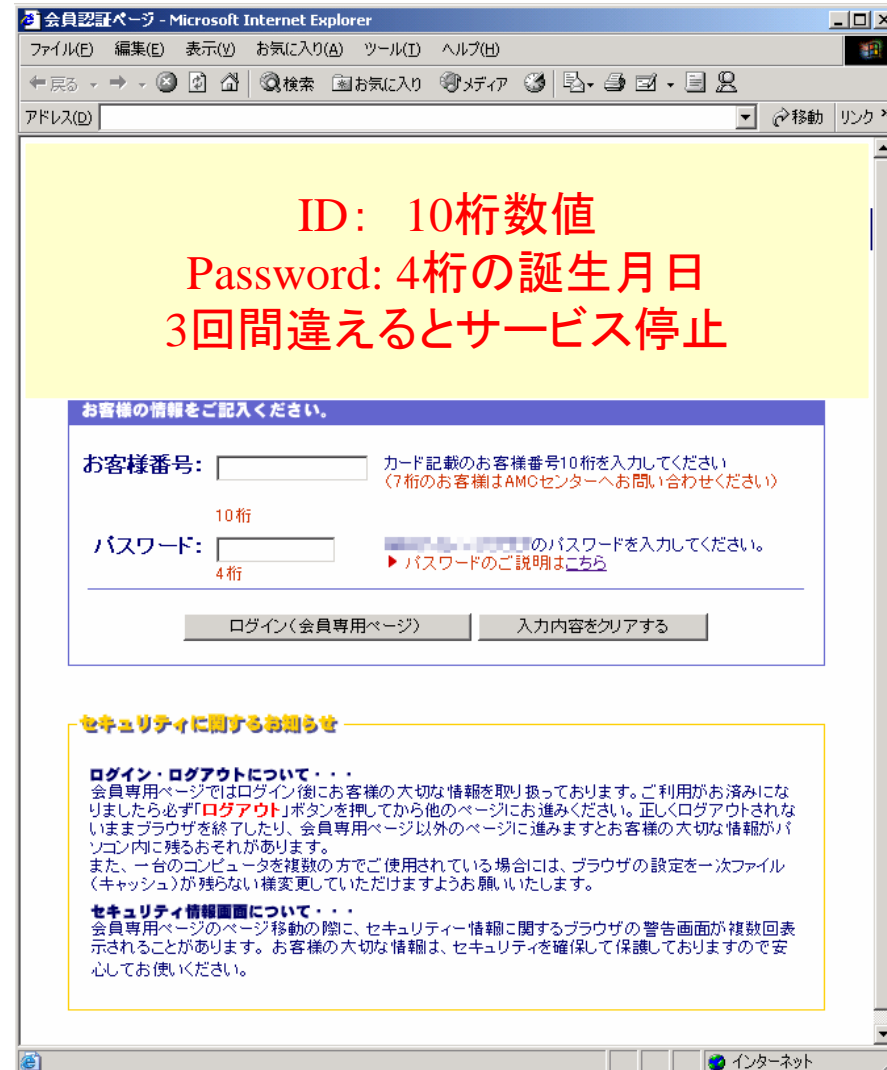
■ パスワード攻撃(辞書攻撃)

◆ 全てのパスワードを試す攻撃

- ⇒ ユーザID: 10桁程度の数値
パスワード: 4桁数値(誕生日)
でユーザ管理しているサイトに対してパスワードは固定してユーザIDをインクリメントさせることで、一致するユーザを探し当てることができる。

■ サービス停止攻撃(DoS攻撃)

- ⇒ 上記のサイトに対して3回ずつパスワードを誤りながらユーザIDをインクリメントすると、ログインできなくなる。

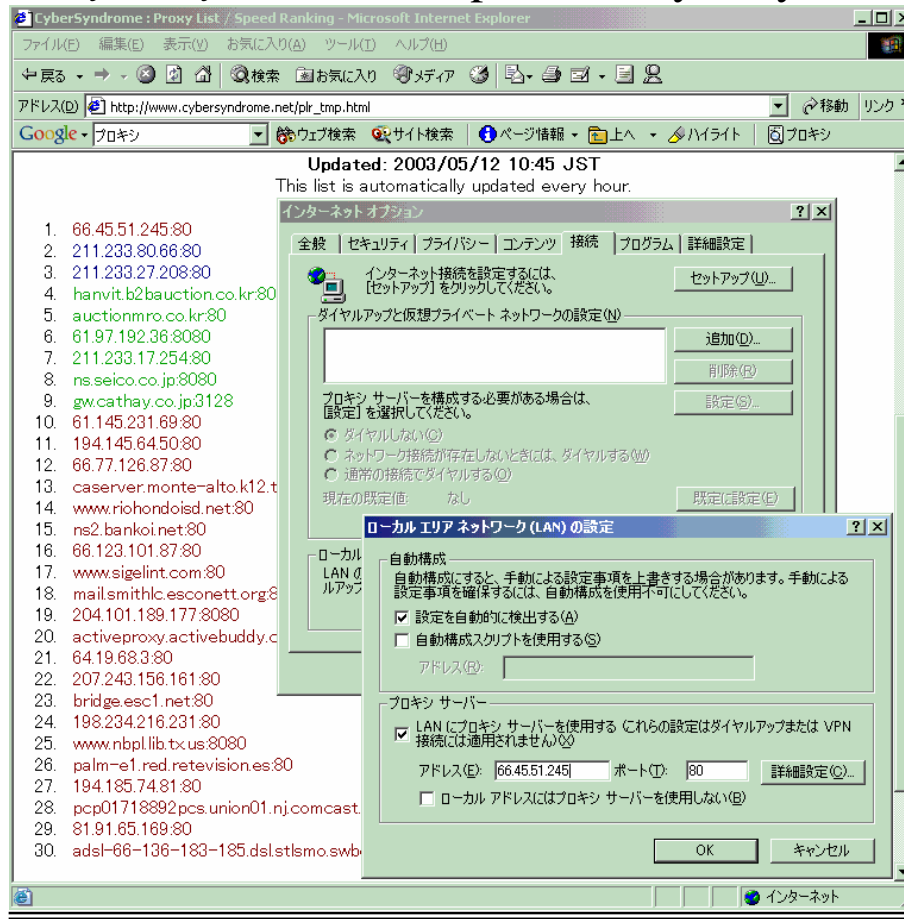


踏み台

■ プロキシ経由による踏み台攻撃

◆ 他人のプロキシサーバを経由すると身元IPアドレスを通信先に対して隠すことができる。

■ CyberSyndrome (http://www.cybersyndrome.net)



■ 脆弱プロキシの自動探索

◆ 設定の甘いプロキシが公開されている。

■ IEへのプロキシ設定

⇒ ツール

⇒ インターネットオプション

⇒ 接続

⇒ LANの設定

⇒ プロキシサーバ

左記サイトに公開されているIPやドメイン名を入力すれば、踏み台として利用できる。

攻撃ツールの入手

■ 攻撃ツールの公開

rootkit.com - Microsoft Internet Explorer

http://www.rootkit.com/

REGISTER

login:
password:

ROOTKIT

Share Your Old Stuff, Keep Your Good Stuff Sunday January 14th

main menu
home
forums Show me new threads!
bookmarks
post article
view blogs
vault
you must be level 2 to upload files to your vault
downloads
you must be logged to access downloads
search the site

projects:
Hacker Defender
This is the Hacker Defender rootkit for Windows. This is more of a 'blackhat' tool than a training

ROOTKITS

ROOTKITS, Subverting the Windows Kernel
By: Greg Hoglund and Jamie Butler

Rootkits are powerful tools to compromise computer systems *without detection*. Learn why virus scanners and desktop firewalls are not enough. Learn how attackers can get in and stay in for years, without detection.

Detours within Windows kernel

By: izik

I had to do an inline function hooking (aka. Detouring) to accomplish some task. When I've started looking around for example in rootkits source codes, it turns out no rootkit is actually using this method. It's makes sense in a way since it's much easier to hook functions within service tables when trying to intercept calls from applications to the kernel, but as far as intercepting functions within the same module (driver) it won't work. Since I couldn't find anything, I have then decided to write my own detouring driver, now I am publishing it for educational purpose only ☺

KREMBO is a Windows driver which detours nt!RtlRandom (for no particular reason, just as a proof of concept). It's well commented and includes debug prints. I have successfully compiled it with Windows DDK 3790.1830. The zip includes in it, both the source code and an already compiled (in checked environment) driver.

KREMBO (zip)

read comments (19) / write comment

recent comments:

Google 辞書をバックグラウンドでダウンロードしています

Packet Knights - Microsoft Internet Explorer

http://www.pkcrew.org/index.php

Packet Knights Tools

www.pkcrew.org

News Tools Docs Advisories About Us Members Contacts Links

Tool	Author	Description
MAC-gyver A-team	the rECIdjVO	HEAT implementations
FingerPrintFucker (fixed!)	CyRaX & FuSyS	FingerPrintFucker is an lkm for linux that changes the tcp/ip stack in order to emulate other os'es against tcp/ip fingerprinting. The package contains the lkm and a parser for the nmap file that let you choose directly the os you want. (Of course, it doesn't work with all the os'es :). This is a new version that fixes a remot denial of service. The module still has some problems. Don't use it on servers!
Slapcrack	Techno[]	SlapCrack is a configurable cracker for linux. It gets the basic options, as host, port, from the command line and it is configurable through a script
Hijacking Suite 0.1b	CyRaX	hjsuite is a collection of programs for hijacking. It contains a library for hijacking, an irc hijacker, an httpd server overhijacking and others.
FingerPrintFucker FreeBSD	cthulhu	Porting of FingerPrintFucker for freebsd
lbk	cthulhu	Local backdoor in a kld (for FreeBSD 4.0 that gives a root shell by putting a password in the TERM environment.
Route Fakker	CyRaX	This (stupid) program adds hop in the result when someone traceroute you.
Key Hole	Asynchro & cthulhu	Key Hole is a linux administration tool that permits an admin to firewall even the ports he needs to

Graphics by Mr Moon

ページが表示されました

ホームページの改ざん

■ 日本の改ざん状況の報告 (http://izumino.jp/Security/def_jp.html)

- ◆ 2000年：多数のWebページが一斉に改ざん
- ◆ 2005年：某所のWebページが繰り返し改ざん
- ◆ 2010年：Gumblarウイルスによる改ざん多発

■ 2002年度総務省調査

- ◆ 改ざん被害を受けた企業は4.7%、検知対策システムの導入済企業は3.3%、導入検討企業は16.6%である。

Web改ざんの発生状況と対策状況

(総務省2002年度調査 http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf)

被害と対策	民間企業	地方 公共団体	病院	大学	その他研 究機関
改ざん被害	4.7%	8.1%	0.0%	21.3%	6.7%
改ざん検知 導入済み	3.3%	3.5%	0.9%	4.6%	5.7%
改ざん検知 導入予定	16.6%	11.0%	11.0%	18.3%	11.4%

■ 携帯サイトの改ざん

- ◆ 携帯電話用サイトも改ざんされている。



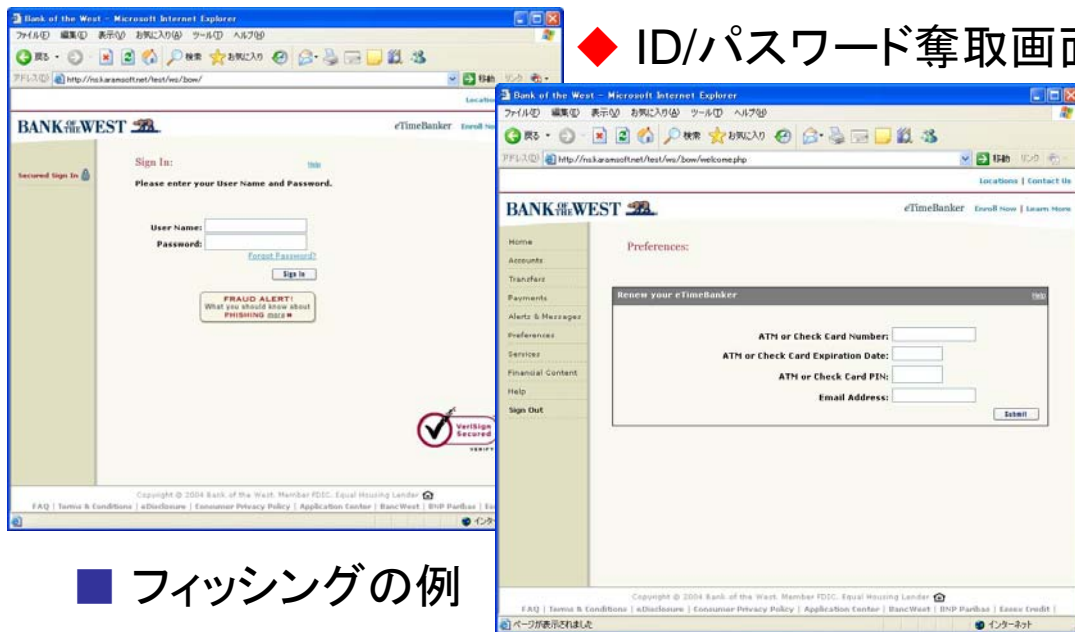
携帯専用サイトの改ざん例

フィッシング

■ フィッシングとは

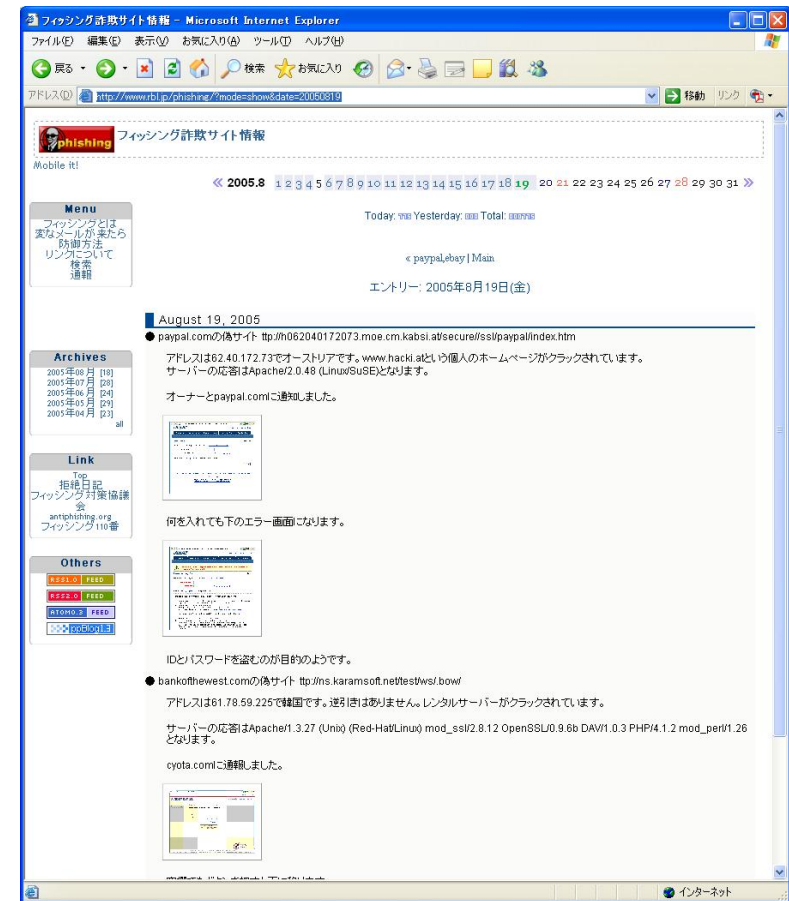
- ◆ 本物サイトに似せたサイトを作り、メールで利用者を誘き寄せ、クレジットカード等の情報を盗み取る行為。
- ◆ セキュリティの甘いWebサーバを踏み台にして、奥深いディレクトリに偽のページを設置する。

◆ 偽のログイン画面



■ フィッシングの例

◆ ID/パスワード奪取画面



■ フィッシング情報公開サイト
<http://www.rbl.jp/phishing/>

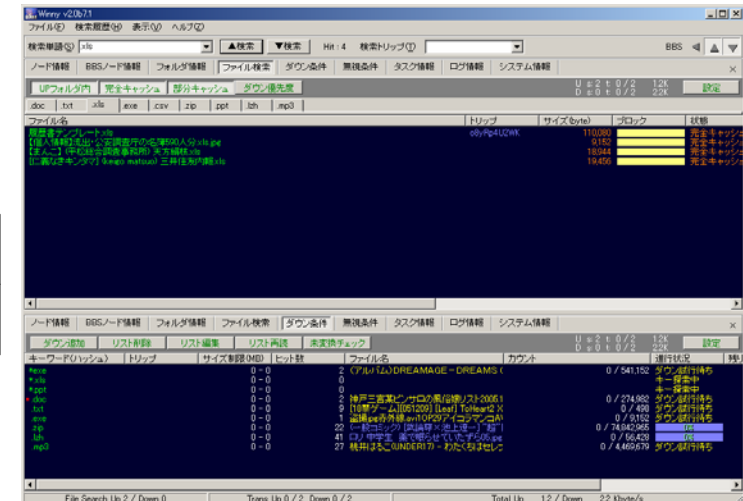
情報漏洩 ～Winnyの脅威～

Winnyでのファイル収集

- ◆ jpg、lzh、xls、doc、rar、zip、exe、txtを指定する。

2006年4月3日17:00-18:00の結果

拡張子	jpg	lzh	xls	doc	rar	zip	exe	txt	合計
ファイル数	11	16	46	2	11	3	1	51	141



収集したファイル数と情報漏洩数

- ◆ 拡張子がxlsに注目(計46件)
情報漏洩数=19件(41%)
例) 送信メールがエクセルファイルに出力。
高校クラスの成績表。
- ◆ jpgファイルの中にはデスクトップのスクリーンショットも多数流出している。
- ◆ docの中には各種仕様書なども流出。

種類	件数(計46)
非個人情報	27件
個人属性のみ	3件
氏名リスト+属性	5件
氏名リスト+住所	11件

ウイルス感染 ～Winnyの脅威～

■ 収集したファイル数とウイルス数

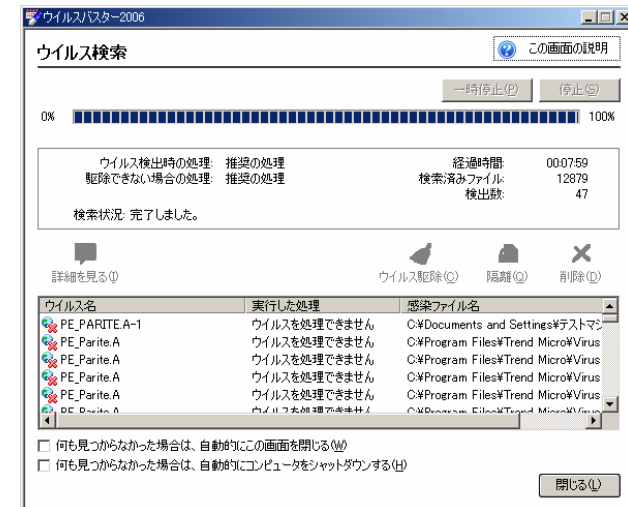
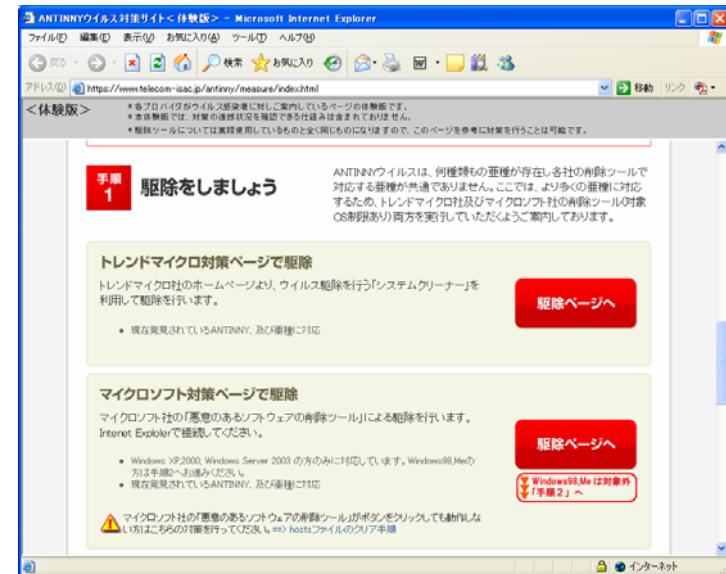
- ◆ レンドマイクロのウィルスバスター2006
- ◆ マイクロソフトの悪意のツール駆除

<https://www.telecom-isac.jp/antinnny/measure/index.html>

表 収集した合計141件のファイルで調査

ツール	検知数 ／141
トレンドマイクロ ウィルスバスター2006	37
マイクロソフト 悪意のツール駆除	3種類

ウイルス含有率 = 37件 / 141件 = 26%



ウィルス感染

■ 未知ウィルスの実態調査

◆ Telecom-ISAC Japanによるボットウィルスの調査

Table. Counts and Varieties of Collected Computer Viruses.

	Counts of Collected Computer Viruses	Varieties of Collected Computer Viruses
Total	150,290	19,259
Known Computer Viruses	130,586 (87%)	2,984 (15%)
Unknown Computer Viruses	19,709 (13%)	16,267 (85%)

【References】

- ◆ Telecom-ISAC Japan
<https://www.telecom-isac.jp/>
- ◆ T. Sudo and K. Fujiwara, "The evaluation of the botnet analysis system based on the virtual internet environment," CSS2006, pp.513-158, October, 2006.(NTT Communications Inc.)

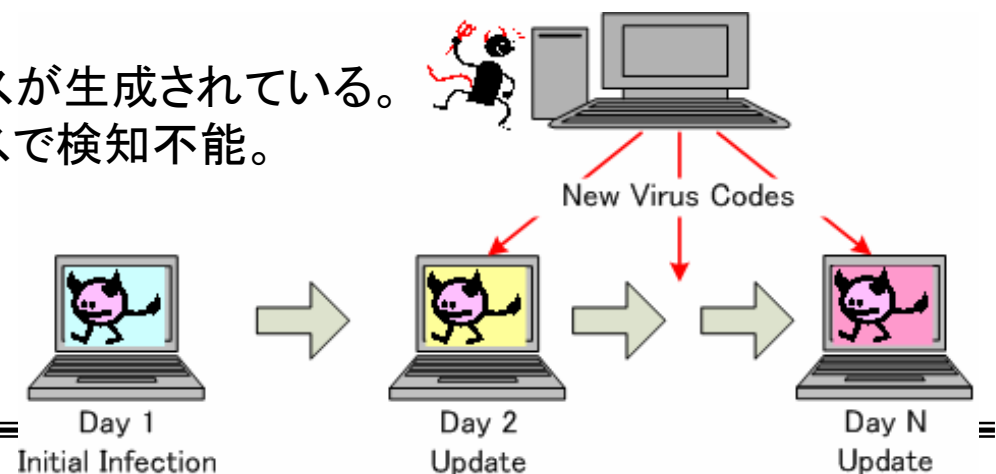
◆ We investigated on February to May, 2006.

(ISAC: Information Sharing and Analysis Center)

◆ Monitoring points were located on the Japanese internet service providers.

■ ウィルスコードのアップデート

- ◆ 1日あたり150種類以上のボットウィルスが生成されている。
- ◆ 次々とアップデートされ、アンチウイルスで検知不能。
- ◆ アップデートサイトが次々変化。



ボットネット

■ ボットネットとは

- ◆ ホストを制御するエージェントが組み込まれた複数のPCを配下に持ち、指令者からの指示に従いSPAMメールやDDoS攻撃を仕掛ける攻撃ネットワークのこと。
- ◆ スпам送信業者や嫌がらせ業者など、裏社会にて時間貸しビジネスが成り立っている。

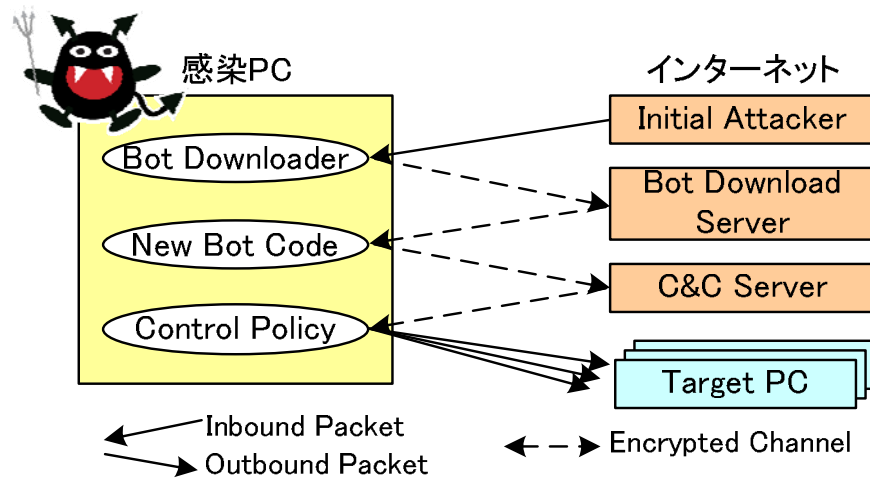


図 ボット(感染PC)の通信特性

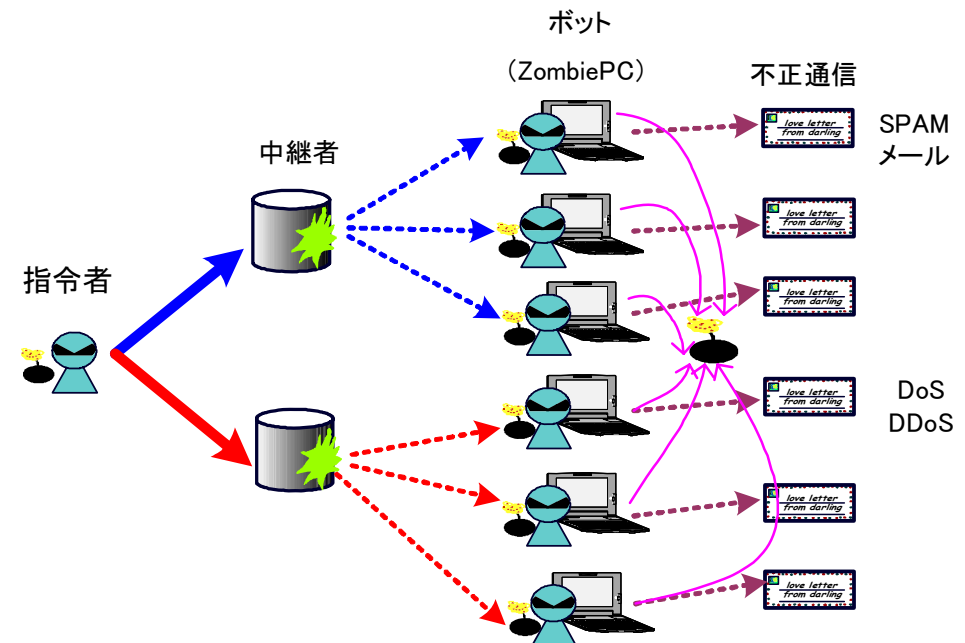


図 ボットネット

目次

九州テレコム
振興センター

【ハッキングの手口】

- パスワード攻撃
- 踏み台
- 攻撃ツールの入手
- ホームページ改ざん
- フィッシング
- 情報漏洩
- ウィルス感染
- ボットネット

【セキュリティ対策】

- ファイアウォール(FW)
- アンチウイルス(AV)
- スпам／コンテンツフィルタ
- 侵入検知システム(IDS)
- セキュリティ監査
- セキュリティ監視センター(SOC)
- ハニーポット

ファイアウォール (FW)

■ FW (Firewall) とは

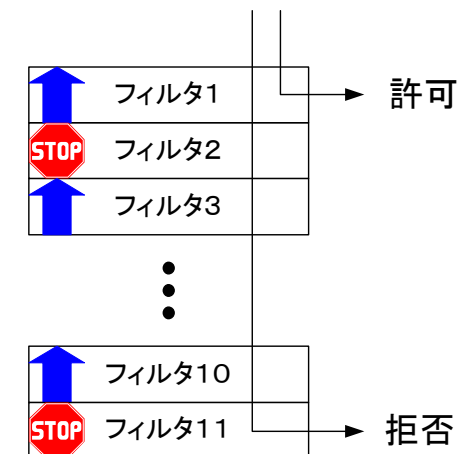
- ◆ ネットワークの出入り口において、パケットの通過と棄却を制御する。

■ 分類

- ◆ 一般的なFW: インターネット (WAN)、公開用ネットワーク (DMZ)、内部ネットワーク (LAN) 間の接続ルールを、通信サービス (Destination Port) ごとに規定する。
- ◆ アプリケーションFW: アプリケーションへの攻撃の有無を検査する。

表 アプリケーションFWのルール設定例

Source IP	Destination IP	Destination Port	許可/拒否
192.168.0.1	ALL	HTTP, POP	許可
LAN	DMZ	ALL	許可
● ● ●			
WAN	LAN	ALL	拒否



パケット毎に、上から順にルールとマッチング ⇒

アンチウイルス (AV)

■ AV (Anti Virus) とマルウェア

- ◆ ファイルを解析して、悪意のソフトウェア(マルウェア)を検知する。
- ◆ マルウェアを上位概念に、様々な呼ばれ方がある。
 - ⇒ ウイルス: 感染するソフトウェア
 - ⇒ ワーム: ネットワークを介して感染するソフトウェア
 - ⇒ トロイの木馬: 正しいソフトウェアのフリをしてユーザによる発見を逃れるソフトウェア
 - ⇒ ボット: 外部からの指示を受けて活動する悪意のエージェント
 - ⇒ Rootkit: APIをフックして応答を偽る。lsやpsコマンドを改ざんしてOS自体を騙す。

■ 課題

- ◆ 感染時に変化する(Polymorphic)ウイルスや、暗号化するウイルスの検知が難しい。
- ◆ 外部サーバから新たなコードをダウンロードして更新するボットの検知が難しい。

■ 解析手法

- ◆ パターンマッチング: 既知のウイルスコードをパターンDB化してファイルを検査する。
- ◆ 挙動解析: ウイルスを擬似的に動作させて、不審なコードの実行を検査する。

■ 駆除

- ◆ 不正なファイル／挿入コード／設定変更などを、正常な状態に戻すこと。

スパム／コンテンツフィルタ

■ スパム／コンテンツフィルタとは

- ◆ 迷惑(スパム)メールや、有害サイト、フィッシングサイトなどを、アプリケーションレベルで除去するシステム。

■ ネットワーク型スパム対策

- ◆ OP25B (Outbound Port 25 Block) : プロバイダドメインから発信されるメールは、認められたSMTPサーバからのみ許可する。ボットからのスパムメール送信を境界FWにて棄却。
- ◆ SPF (Sender Policy Framework) : ドメインの正規SMTPサーバをホワイトリスト化する。
- ◆ PoP before SMTP / SMTP AUTH : 認証されたクライアントからのみメール送信を認める。

■ ホスト型スパム対策

- ◆ ベイズフィルタ: スパムメールに出現する単語を学習して、正規とスパムを判定する。

■ 有害サイト対策

- ◆ IP/ドメインのブラックリストを用いる場合や、出現単語や画像から、有害性を判定する。

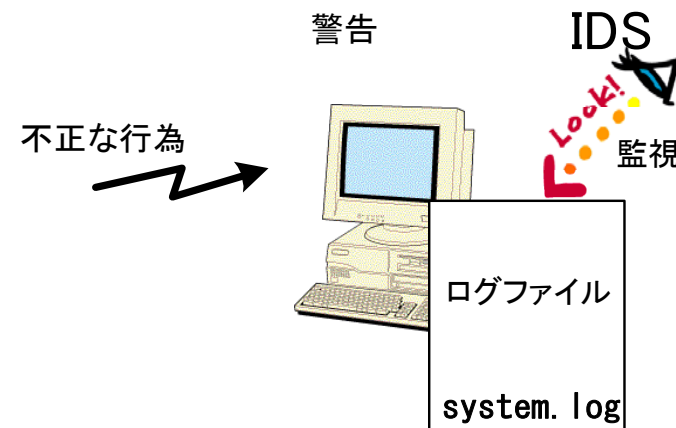
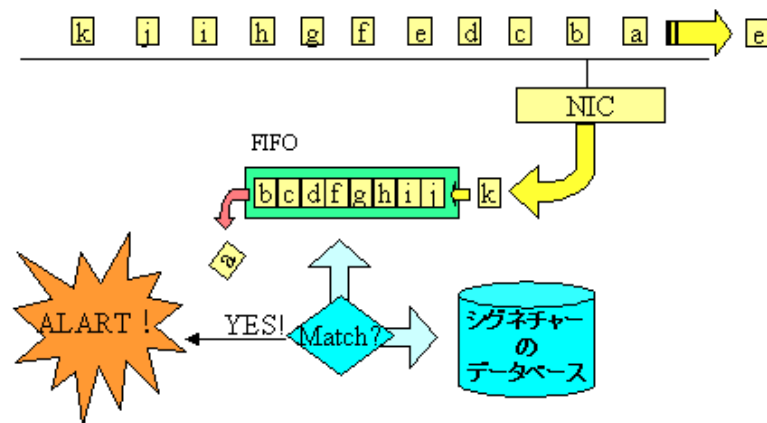
■ フィッシング対策

- ◆ IP/ドメインのブラックリストを用いる場合や、ドメインの生成日時から、偽サイトを判定する。
-
-

侵入検知システム (IDS)

■ IDS (Intrusion Detection System) とは

- ◆ パケットやログファイルに、攻撃に見られる特徴(シグネチャ)の有無を検査して、アラームを出力する。
- ◆ 特に、不正なパケットをオンラインで拒否するツールをIPS (IDS & Prevention) と呼ぶ。



■ ネットワーク型IDS

- ◆ ネットワークを流れるパケットを監視して、攻撃コード(シグネチャ)の有無を検査する。

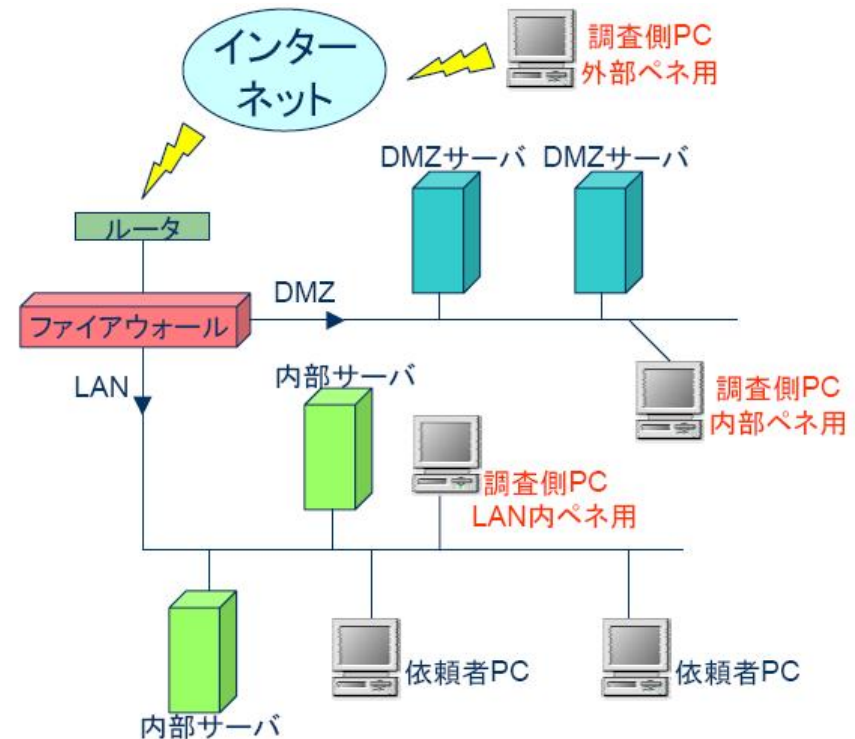
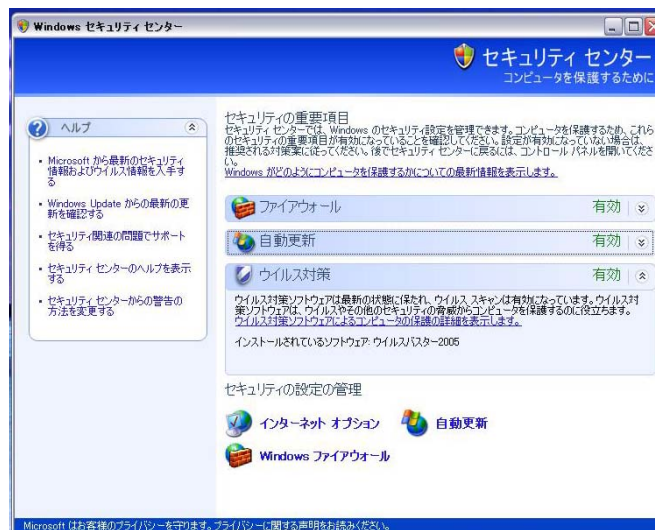
■ ホスト型IDS

- ◆ システムのログファイルを検査して、侵入の記録の有無を検査する。

セキュリティ監査

■ セキュリティ監査とは

- ◆ FW・AV状態の確認、セキュリティパッチの適用などを検査して、問題があれば、対策するシステムのこと。



■ ホスト監査

- ◆ OSやアプリケーションのバージョンやパッチ状態を検査
- ◆ 最新状態はセンタ局(NW側)で管理

■ ネットワーク監査

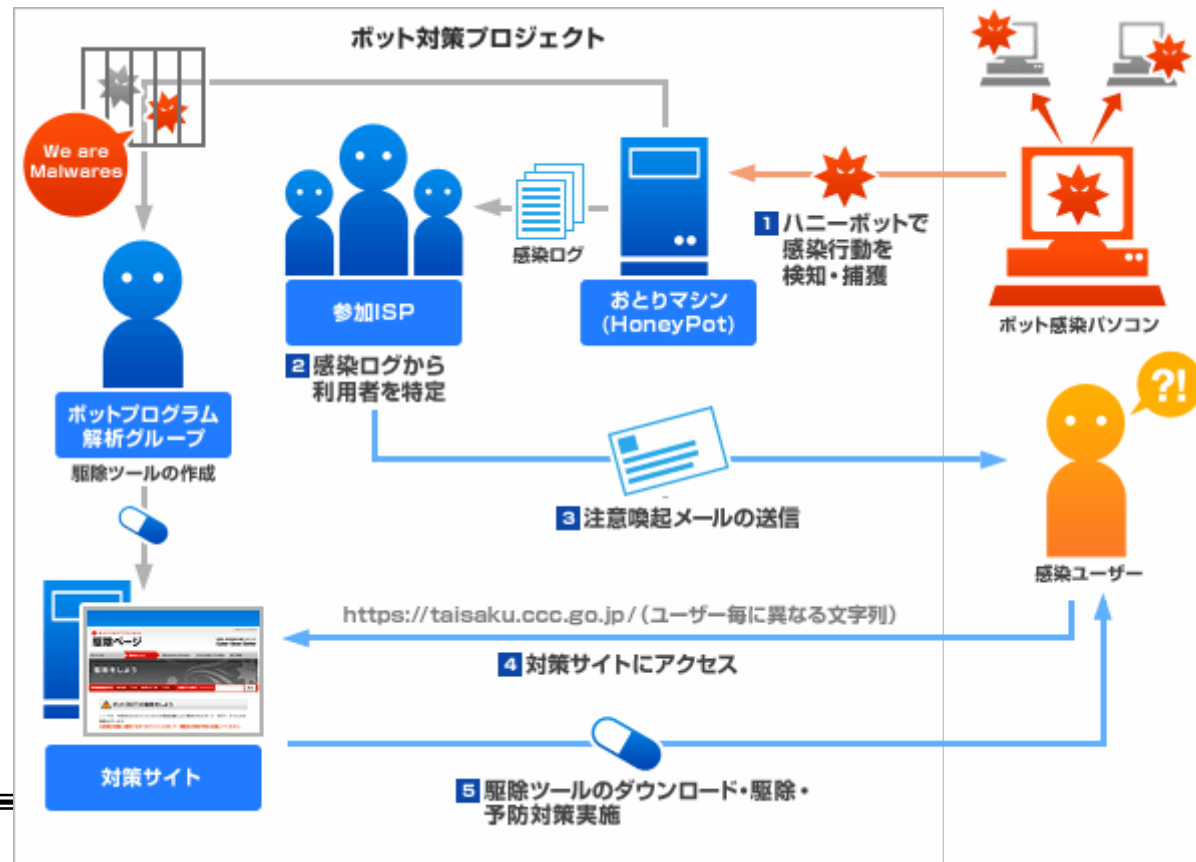
- ◆ 擬似攻撃(ペネトレーション)試験を行い、侵入の可否を検証

セキュリティ監視センター（SOC） ～サイバークリーンセンター（CCC）の取り組み～

九州テレコム
振興センター

- サイバークリーンセンターとは（<https://www.ccc.go.jp/ccc/index.html>）
 - インターネットにおける脅威となっているボット特徴を解析し、ユーザのPCからボットを駆除するために必要な情報をユーザに提供
 - ISP（インターネットサービスプロバイダ）の協力によって、ボットに感染しているユーザに対し、ボットの駆除や再感染防止を促す

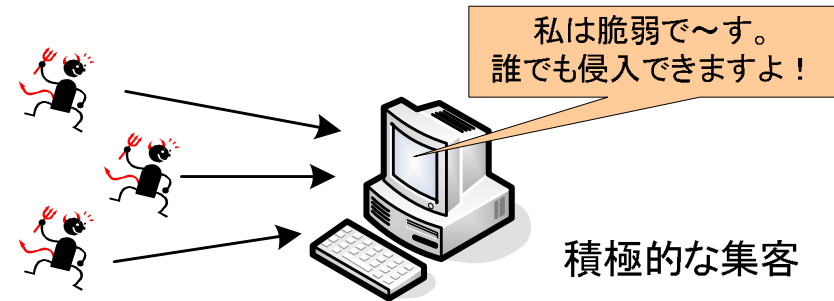
- 注意喚起の流れ
(CCCホーム
ページより引用)



ハニーポット

■ ハニーポットとは

- ◆ わざと脆弱性を持たせたPCに侵入者を誘い込み、攻撃手法や活動の様子を収集する。



■ 分類

- ◆ 低対話型: 架空のOS・アプリケーションをエミュレートして、侵入初期の情報を収集する。
⇒ Nepenthes (<http://www.honeynet.org/tools/index.html>) ツールは、Linux上でWindowsの脆弱性をエミュレートして、侵入初期の活動やウイルスコードを収集する。ウイルスへの感染はしない。
- ◆ 高対話型: 本物のOS・アプリケーションを用いて、侵入のシナリオを詳細に収集する。
⇒ 仮想マシンモニタなどのゲストOSに侵入させて、ウイルス感染、データ改ざん・漏洩など、本当に被害を受けてみる。情報収集後は、ゲストOSをリセットすると簡単に元に戻る。

