

## IPA におけるインターネット定点観測について

### はじめに

インターネット定点観測(TALOT2)に関するプレスリリースの月次レポートが発信され始めて2年が経ちました。そこで、特集記事ということで、インターネット定点観測について開発の背景および経緯について、さらに、一般のインターネット利用者の皆さんに何に注意して欲しいかを、順を追って解説します。

### 1. コンピュータウイルスおよび不正アクセスの脅威

コンピュータウイルスは 1980 年代後半から登場したと言われています。

- ブートセクタ感染型ウイルス(\*1)(80 年代後半～90 年代前半)
- ファイル感染型ウイルス(\*2)(80 年代後半～)
- マクロ感染型ウイルス(\*3)(90 年代半ば～)
- トロイの木馬型ウイルス(\*4)(90 年代～)
- ネットワーク感染型ウイルス(\*5)(01 年～)

特に、ネットワークから感染するタイプのコンピュータウイルスの出現は、コンピュータ利用者(ネットワーク利用者)にとっては、意識せずに感染させられる可能性が高まったということ、脅威が大きくなっていると言えます。

なお、ネットワークからの不正アクセスと言う意味では、90 年代半ばから、いわゆるコンピュータのぜい弱性を狙ったアクセスが行われるようになっていました。

- 1996 年の年末から 1997 年の年始にかけては、休暇中で管理が不十分であったメールサーバ、ニュースサーバ(sendmail,inn)のぜい弱性が標的
- 1997 年には、NCSA(\*6)の古いバージョンの Web サーバに最初から付属している phf(\*7)という cgi のサンプルプログラム(cgi-bin/phf)のぜい弱性が標的
- 1998 年以降、メール不正中継(\*8)、ポートスキャン(\*9)が発生しています
- 2000 年に BIND(\*10)のぜい弱性が標的

- **Solaris/Sadmind**

2001 年 5 月には sadmind/IIS などのワームによる自動的な攻撃により大きな被害を出しました。このウイルスは、SolarisOS 上で動作するウイルスで、セキュリティホール(ぜい弱性)を悪用して感染を広げました。セキュリティホールのあるシステムに侵入すると、自分自身をコピーし、外部からリモートアクセスができるように設定を変更しました。次に、インターネット上のぜい弱性のあるマイクロソフト社の Internet Information Services (IIS)サーバを検索し、発見すると、そのマシンの Web ページを改ざんしました。

ワーム sadmind/IIS による Web 改ざんインシデントの対策について  
<http://www.ipa.go.jp/security/ciadr/200105sadmindiis.html>

- **W32/CodeRed**

2001 年 7 月には W32/CodeRed が発生しました。このウイルスは、マイクロソフト社の IIS(Internet Information Services) のぜい弱性を利用して感染を拡げるワームでした。セ

セキュリティホールのあるシステムに侵入すると、メモリ上で動作し、英語版の場合は、Webを改ざんしました。次に、インターネット上のぜい弱性のあるIISサーバを検索し、発見するとそのマシンに侵入しました。さらに、バックドアプログラムをインストールする亜種も発見されています。

■ 「Code Red ワームに関する情報」- 新種の Code Red II に注意を -

<http://www.ipa.go.jp/security/ciadr/vul/20010727codered.html>

● W32/SQLSlammer

マイクロソフト社の SQL Server 2000 のぜい弱性を攻略する新種ワームが、2003年1月25日に発見され、その伝搬が急激に拡大しました。2003年1月25日から、本ワームの影響と思われるトラフィックの急増とシステムが繋がりにくくなる現象が、世界各地で報告されていました。IPA/ISECでも、1月25日14:30頃から、1434/udpの急激なトラフィック増加を観測しました。

■ 新種ワーム「W32/SQLSlammer ワーム」に関する情報

<http://www.ipa.go.jp/security/ciadr/vul/20030126ms-sql-worm.html>

● W32/MSBlaster

2003年8月に発生したこのワームは、TCP 135番ポートを通じて、「RPC インターフェースのバッファオーバーランによりコードが実行される(MS03-026)」という Microsoft Windows のぜい弱性を攻略し、msblast.exe という名のファイルをダウンロードし、実行を試みました。このワームが実行されると、レジストリに msblast.exe を登録し、パソコン起動時にワームが実行されるように変更しました。また、任意に感染対象のコンピュータを検索し、感染拡大を試みました。さらに、感染したコンピュータの日付が 2003年8月16日になると windowsupdate.com に対してサービス妨害攻撃(DoS)(\*11)をしかけました。

■ 「W32/MSBlaster」ワームに関する情報

<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>

● W32/Welchia

W32/MSBlasterと同じく2003年8月に発生したこのワームは、ランダムなIPアドレスに対して Ping(\*12)を発信し、応答があったIPアドレスの 135/TCP に接続しました。

その際、「RPC インターフェースのバッファオーバーランによりコードが実行される(MS03-026)」、「Windows コンポーネントの未チェックのバッファにより Web サーバが侵害される(MS03-007)」という Microsoft Windows のぜい弱性を攻略し、システムフォルダに dllhost.exe、svchost.exe という名のファイルをダウンロードし、実行を試みました。

その後、感染対象のコンピュータをランダムに検索し、感染拡大を試みました。また、言語環境が英語、中国語、韓国語の場合には、上記(MS03-026)の修正プログラムをマイクロソフト社のサイトからダウンロードし、インストールしました。これにより、ぜい弱性の一つは解消されました(日本語環境では修正プログラムのインストールは行われませんでした)。さらに、感染したシステムの日付が 2004年になると活動を停止しました。

■ 「W32/Welchia」ワームに関する情報

<http://www.ipa.go.jp/security/topics/newvirus/welchi.html>

● W32/Sasser

2004年5月に発生したこのワームは、TCP 445番ポートを通じて、「Microsoft Windows のセキュリティ修正プログラム(MS04-011)」という Microsoft Windows のぜい弱性を攻略し、avserve.exe という名のファイルをダウンロードし、実行を試みました。

このワームが実行されると、レジストリを操作し、パソコン起動時にワームが実行される

ように改変しました。また、任意に感染対象のコンピュータを検索し、感染拡大を試みました。

さらに、攻撃対象のコンピュータをリモートコントロール可能な状態にしました。

■ 新種ワーム「W32/Sasser」に関する情報

<http://www.ipa.go.jp/security/topics/newvirus/sasser.html>

● ポット/ポットネットワークの脅威

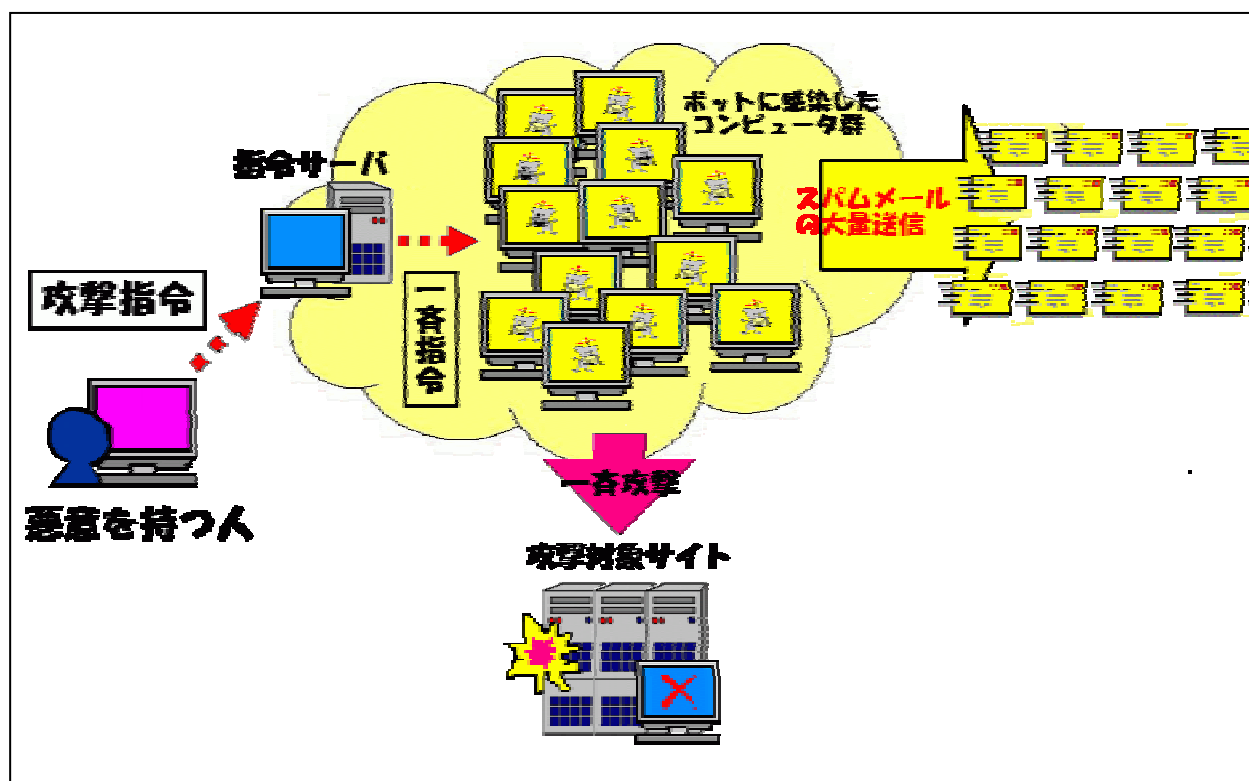
いままでに挙げた各種のワームの発生と同じ時期(2003 年半ばごろから)に、ポットと呼ばれるウイルス(トロイの木馬やワームに分類される)が発生しています。

ポットに感染すると、バックドアが埋め込まれ、リモートから操作可能な攻撃ツール(複数の脆弱性を狙い感染活動を行うプログラムコードやDoS攻撃(\*11)を行うプログラムコード)も埋め込まれます。

このようなポットに感染したコンピュータをゾンビと呼ぶ人もいます。ゾンビ化されたコンピュータが連携(場合によっては数万台が連携)することで、ゾンビネットワーク(ポットネットワーク)が構成され、これらのネットワークが悪用されると

- ・ 多量のスパムメール(\*13)の発信
- ・ 特定サイトに対する DDoS 攻撃(\*11)

が行われる危険性が指摘されています。



【図 1.1 ポットネットワークの脅威】

## 2 . インターネット定点観測

このような状況の変化の中、前述のマイクロソフト社の SQL Server 2000 の脆弱性を攻略する W32/SQLSlammer ワームの影響と思われるトラフィック(1434/udp ポートへのアクセス)の急増を、IPA/ISEC でも、2003 年 1 月 25 日 14:30 頃から観測していました。この観測データ

をもとに、発信した情報が

■ 新種ワーム「W32/SQLSlammer ワーム」に関する情報

<http://www.ipa.go.jp/security/ciadr/vul/20030126ms-sql-worm.html>

でした。

この情報発信を契機として、インターネット(ネットワーク)上を流れる不正なアクセスについて、リアルタイムに観測できないかと言うことで誕生したのが、IPA/ISEC のインターネット定点観測システムです。当初は、前述の W32/SQLSlammer ワームの影響と思われるアクセスを観測した環境で動作していました(TALOT1)。しかしながら、この環境はインターネット上では限定されたアドレス環境であったため、インターネット上で固定されたアドレス(IPアドレス)を持たない環境での観測を実施するために、2004年6月以降、公表する観測データはTALOT2でのものに移行しました(TALOT2システムは2004年6月より本稼働)。

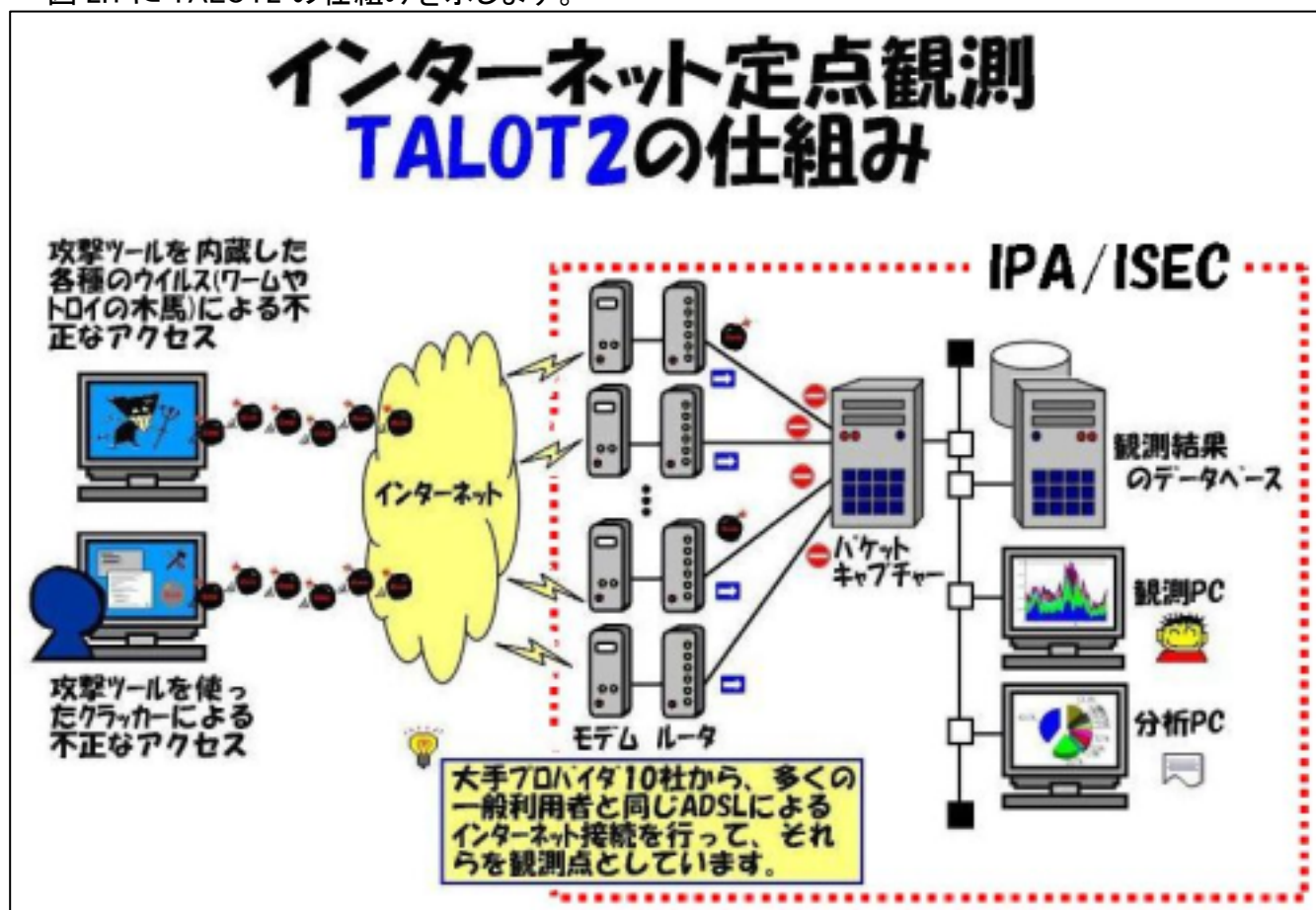
■ インターネット定点観測システムが新しくなります！！

<http://www.ipa.go.jp/about/press/pdf/040511Press.pdf>

TALOT2 の動作環境(観測データの収集環境)は、一般のインターネット利用者がインターネットサービスプロバイダ(ISP)経由で取得する環境と同じで、10個のインターネット接続環境をもとに作りました。ご存知のように、一般的な接続環境においては、接続のリフレッシュを行うたびに、IPアドレスが変更されるものであり、TALOT2においても特定の接続環境(IPアドレス)に依存しない観測を行えるものとなりました。

10個の接続環境は、それぞれ国内の大手ISPと一般的な契約で取得したものであり、これらの大手ISPから接続している一般の利用者は、接続人口の80%を超える利用者と同じ環境であると考えています。

図 2.1 に TALOT2 の仕組みを示します。



【図 2.1 TALOT2 の仕組み】

前述の W32/MSBlaster や W32/Welchia に関する IPA からの情報発信においても、インターネット定点観測で観測した観測データが利用されています。

■ 「W32/MSBlaster」ワームに関する情報

<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>

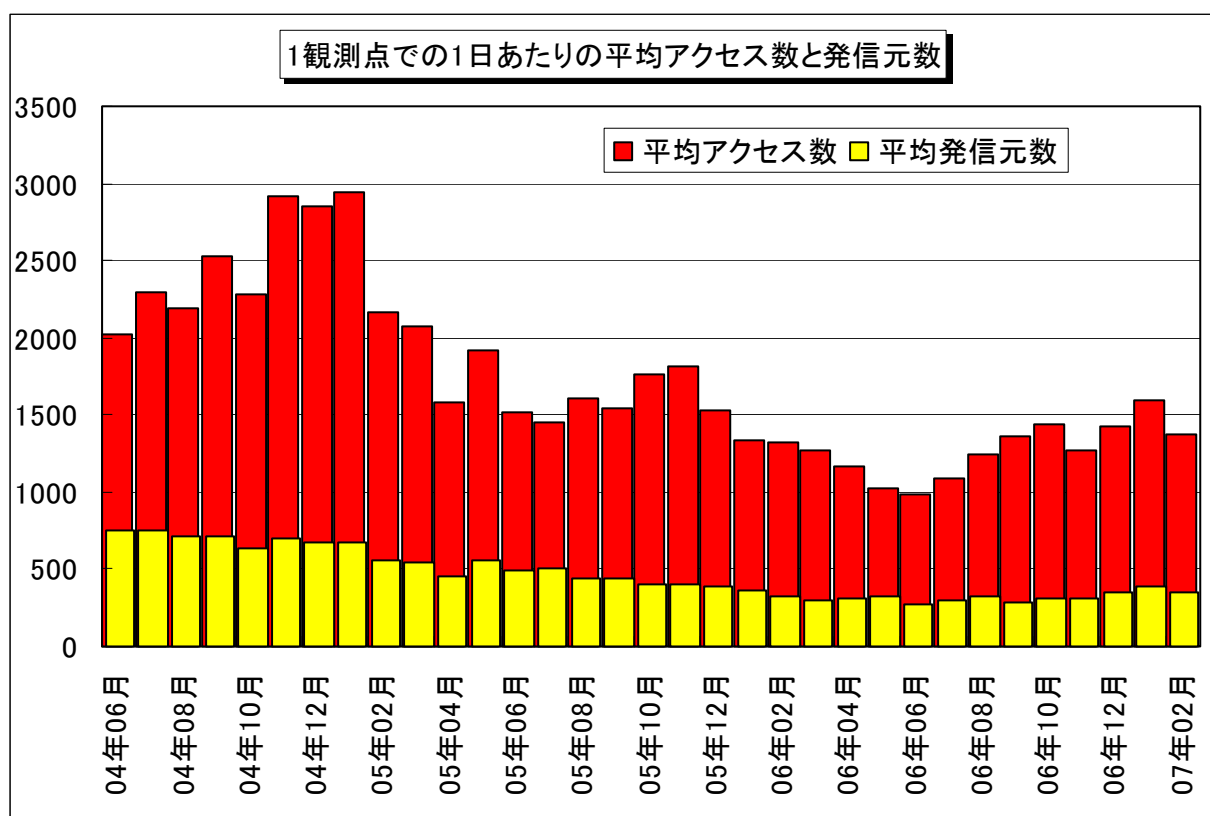
■ 「W32/Welchia」ワームに関する情報

<http://www.ipa.go.jp/security/topics/newvirus/welchi.html>

ただし、2004 年 5 月に発生した W32/Sasser については、Sasser による不正なアクセスが顕著なかたちで観測されなかったため、公表資料中で観測データは利用できませんでした。

インターネット観測システムが TALOT1 から TALOT2 に移行してから、観測データを定期的に公表することとなり、2005 年 1 月の観測データから月次のプレスリリース情報の一部として、毎月情報公開しています。

2005 年 2 月の観測データからは、一般のインターネット利用者への脅威の指針として、1 日あたりどれくらいの期待しないアクセスが発生しているかを示すようになりました。図 2.2 は、いままで TALOT2 で観測したデータの総まとめです。



【図 2.2 1 観測点での 1 日あたりの平均アクセス数と発信元数】

インターネット定点観測の目的は、

- インターネットから一方的にやって来るパケット(特にポートスキャン(\*9))を観測・分析する
- インシデント発生時は、IPA セキュリティセンターの緊急対策情報の発行を行うか否かの判断材料とする
- 実際の観測に基づく分析結果から適切な対策情報の提供が行えるようにする
- 実際に被害が起こった場合には、その被害の影響範囲や規模等の情報提供も行えるようにする

であり、実際に、

- 時系列のアクセス数および発信元 IP 数の変化を観測
  - ・ 特定ポートへのアクセス数の急増あるいは発信元 IP 数の急増を検知:ワームの出現を検知
  - ・ 特定ポートからのアクセス数の急増あるいは発信元 IP 数の急増を検知:ワームの出現あるいは SYN Flood 攻撃(\*16)による DoS 攻撃(\*11)先を検知
- 特定アクセスの発信地域別アクセス数の変化を観測
  - ・ ワーム等の地域別感染活動および収束(対応)状況を把握する
  - ・ ワーム等の発生地域(どこで生まれたか)の分析を行う
- アクセスを発信元 IP ごとに集計して観測
  - ・ アクセスパターンの決まっているボット系のアクセスを判別する

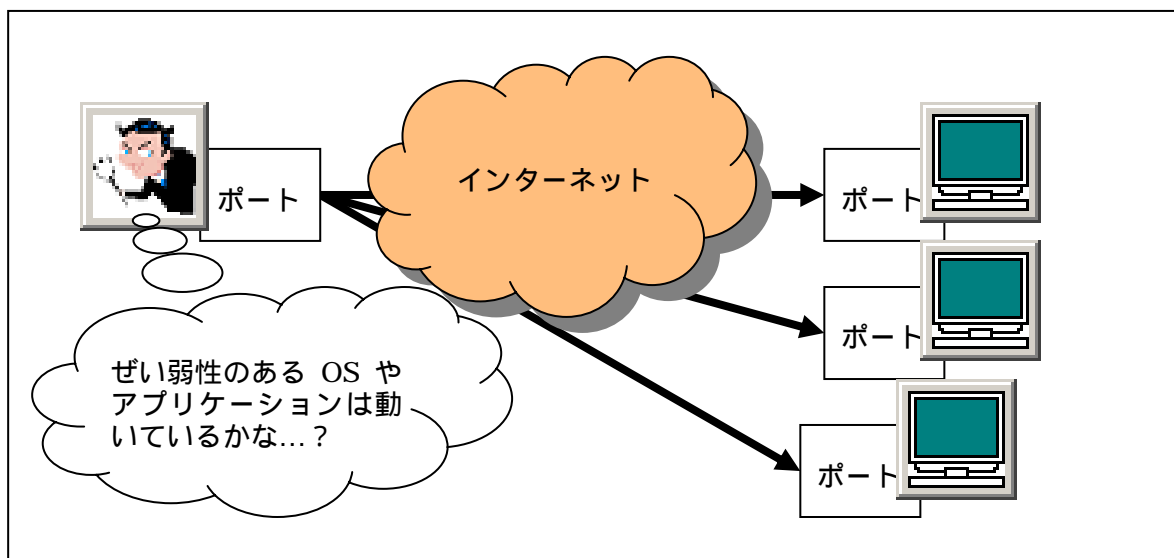
を実施しています。

### 3 . インターネットからの期待しないアクセス

インターネットに接続しますと、悪意のある無しに関わらず何らかのアクセスが必ずやってきます。一般的に、インターネット利用者のコンピュータでは、自分から発信したアクセスに対して、インターネットから返信のかたちでアクセスがあるのが普通です。期待しないアクセスとは、自分からのアクセスではなく、一方的にインターネットからくるアクセスのことです。期待しないアクセスは通常、攻撃ツール(プログラム)を利用して自動的に行われますので、個人、法人などに関係なく無差別に、ランダムな IP アドレスに向けて、頻繁に行われます。インターネットに接続している限り、このようなアクセスを受ける可能性があります。

特に多いのが、攻撃・侵入(不正アクセス)の前段階として、標的のコンピュータの各ポートにおけるサービスの状態を調査するポートスキャン(\*9)と呼ばれるアクセスです。

特に、最近ではボットが蔓延しているため、毎日複数回、何らかのアクセスが来る可能性があります。



インターネットからの期待しないアクセスは、特定のプロバイダに加入していると多いとか少ないとか言うことではなく、先に述べたように、プロバイダから割り振られた IP アドレスに対して、無差別に、ランダムに、頻繁に行われています。

これらのアクセスが狙う(宛先)ポートが開いていない状態であれば、これらのアクセスによるトラブルや被害は起こりません。つまり、コンピュータの利用者にとって不要なサービスを停止しておく(\*14)ことで、不要なポートを閉じることができます。また、パーソナルファイアウォール

(\*15)やOSに付属しているファイアウォール機能で、これらのアクセスを遮断しているのであれば、同様に、トラブルや被害は起こりません。

また、ファイアウォール機能等を利用していない環境でも、利用者 ID やパスワードの設定や管理が十分であり、コンピュータ上のぜい弱性の解消(例えば Windows Update の定期的な適用)が行われていれば、これらのアクセスからのトラブル防止を行うことができます。

インターネットの利用者の皆さんには、状況をご理解いただき、適切な対策を講じていただきたいと思います。

一般のインターネット利用者の皆さんには、以下に示す Web サイトあるいは資料を参考に、ご自身のコンピュータおよびコンピュータ内の個人情報を守るために方法を身につけていただきたいと思います。

■ 個人の方向け情報サイト(IPA セキュリティセンター)

<http://www.ipa.go.jp/security/personal/>

■ 他人事じゃない CHECK PC !

<http://www.checkpc.go.jp/>

『ITが国民生活・社会経済活動に深く浸透していく中で、インターネットの利用者がコンピュータウイルスへの感染、不正アクセス、フィッシング等の被害に遭遇する危険性は高まっています。このような状況を踏まえまして、経済産業省では、1月22日から3月末までの間、テレビCM、新聞広告、専用ホームページ等を通じて国民に情報セキュリティ対策の重要性を訴える「CHECKPC！」キャンペーンを実施します。』

経済産業省 2007年1月22日 News Release より引用

□ 「『CHECK PC ! 』キャンペーン」の開始について

<http://www.meti.go.jp/press/20070122003/check-pc.p.r.pdf>

■ サイバークリーンセンター

<https://www.ccc.go.jp/>

『サイバークリーンセンターは、インターネットにおける脅威となっているボット(「ボットとは」を参照してください)の特徴を解析するとともに、ユーザのコンピュータ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する活動を行っています。また、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プロジェクトの中核を担っています。』

「総務省・経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター」のサイトより引用

■ 対策のしおり(IPA セキュリティセンター)

- ウイルス対策、スパイウェア対策、ボット対策、不正アクセス対策、情報漏えい対策 -

<http://www.ipa.go.jp/security/antivirus/shiori.html>

## 4 . TALOT2 における観測情報の報告

以下に、TALOT2 における観測状況の報告一覧を示します。

□ 2005 年 1 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0502.pdf>

IPAプレスリリースにおいて、インターネット定点観測の報告を開始しました。

□ 2005 年 2 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0503.pdf>

インターネットからの脅威を防ぐもの・・・と言うことで、『ルータ』についてのコラムを掲載しました。

□ 2005 年 3 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0504.pdf>

もうひとつの定点観測・・・と言うことで、『ウイルスメールの定点観測』について、IPA でのメールサーバでのウイルス検査結果の定点観測についてのコラムを掲載しました。

□ 2005 年 4 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0505.pdf>

一方的なアクセスの曜日別統計と時間帯別統計を行いました。曜日別統計については統計分析する意味があまりなかったようです。

□ 2005 年 5 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0506.pdf>

一時的な 445/tcp ポートへのアクセス急増を検知しましたが、原因は不明としました。今になって考えると W32/Sasser によるものである可能性が高いようです。さらに、リモートアクセスツールである SSH(Secure Shell)を狙った 22/tcp ポートへのパスワードクラッキングアクセスについても掲載しました。

□ 2005 年 6 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0507.pdf>

VERITAS 社の Backup Exec にある複数のぜい弱性を狙ったと思われる 10000/tcp ポートへのアクセスを検知し、アプリケーションへのパッチ適用を呼びかけました。また、ボットについて解説しました。

□ 2005 年 7 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0508.pdf>

Microsoft SQL Server を狙っていると思われる 1433/tcp ポートへのアクセス急増を検知し、サーバ等の初期設定を見直すように警告しました。また、Windows の Messenger 機能(Microsoft Windows Messenger service)を悪用した 1026/udp および 1027/udp ポートへのアクセスを解析し、セキュリティ警告を謳ったポップアップメッセージに注意するよう警告しました。

□ 2005 年 8 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0509.pdf>

『どこからどんなアクセスが発生しているか』について、2005 年 8 月のアクセスの発信元

地域別のアクセス種類(宛先ポート別)を分析しました。

□ 2005 年 9 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0510.pdf>

中国(中華人民共和国)方面からの、特定発信元の特定ポートからのアクセス数急増を観測し、SYN Flood 攻撃(\*16)による DoS 攻撃(\*11)が発生したことを検知しました。

□ 2005 年 10 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0511.pdf>

Windows の Messenger 機能(Microsoft Windows Messenger service)を悪用したアクセスが増加したことに対して、警告を行いました。

□ 2005 年 11 月の観測状況について

<http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0512.pdf>

2005 年 10 月の Windows の Messenger 機能(Microsoft Windows Messenger service)を悪用したアクセスがさらに増加したことに対して、Messenger service の停止方法を含めた再度の警告を行いました。また、リモート接続ツール SSH(Secure Shell)を利用するサーバに対してパスワードクラッキング攻撃を多数観測したため、これらの利用者に対する警告も行いました。

□ 2005 年 12 月の観測状況について

<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0601.pdf>

Windows の脆弱性(MS05-051)を狙った Dasher ワームのアクセスが観測されたので、このワームに関する警告を行いました。さらに、2005 年 8 月と同様に、アクセスの発信元地域別のアクセス種類(宛先ポート別)を分析しました。

□ 2006 年 1 月の観測状況について

<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0602.pdf>

コンピュータのぜい弱性を狙ったアクセスや OS に付属するサービスを悪用したアクセスに対応するために、IPA 対策のしおりシリーズを参考にして、不正アクセス対策を行うよう呼びかけました。

□ 2006 年 2 月の観測状況について

<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0603.pdf>

統計情報からは除外している特定観測点への冗長なアクセス(P2P ファイル交換関連のアクセス)が多く観測されたため、これらのアクセスについて分析しました。

□ 2006 年 3 月の観測状況について

<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0604.pdf>

SSH(Secure Shell)を狙ったアクセスおよび DoS 攻撃(\*11)の痕跡アクセスについて特記しました。

□ 2006 年 4 月の観測状況について

<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0605.pdf>

2006 年 3 月に引き続き、SSH(Secure Shell)を狙ったアクセスおよび DoS 攻撃(\*11)の痕跡アクセスについて特記しました。

- 2006年5月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0606.pdf>  
RealVNCのぜい弱性を狙ったものと思われる5900/tcpポートへのアクセスが観測されたため、警告を含めた情報を発信しました。
- 2006年6月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0607.pdf>  
2006年5月に引き続き、RealVNCのぜい弱性を狙ったものと思われる5900/tcpポートへのアクセスが継続観測されたため、さらなる警告を行いました。また、SSHを狙ったアクセスについても再度警告を行いました。
- 2006年7月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0608.pdf>  
2006年6月に引き続き、RealVNCのぜい弱性を狙ったアクセスと、SSHを狙ったアクセスについて警告を行いました。
- 2006年8月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0609.pdf>  
新しいWindowsのぜい弱性(MS06-040)を狙ったと思われる139/tcpポートへのアクセスが観測されたため、このぜい弱性に関する警告を行いました。
- 2006年9月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0610.pdf>  
2006年8月に警告した139/tcpポートへのアクセスについて経過報告を行いました。
- 2006年10月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0611.pdf>  
2006年2月と同様に、統計情報からは除外している特定観測点への冗長なアクセス(P2Pファイル交換関連のアクセス)が多く観測されたため、これらのアクセスについて分析しました。
- 2006年11月の観測状況について  
<http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0612.pdf>  
2006年2月と同様に、統計情報からは除外している特定観測点への冗長なアクセス(P2Pファイル交換関連のアクセス)が多く観測されたため、これらのアクセスについて分析しました。
- 2006年12月の観測状況について  
<http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0701.pdf>  
Ping(ICMP)(\*12)アクセスが増加傾向のため、注意喚起を行いました。さらに、Symantec社のセキュリティ対策ソフトのぜい弱性を狙ったと思われるアクセス(2967/tcpポートへのアクセス)が観測されたため、注意喚起を行いました。
- 2007年1月の観測状況について  
<http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0702.pdf>  
総務省・経済産業省 連携プロジェクトであるサイバークリーンセンターがスタートしたので、ボット対策に関する情報発信を行いました。また、Ping(ICMP)(\*12)アクセスおよび

Symantec 社のセキュリティ対策ソフトのぜい弱性を狙ったと思われるアクセス(2967/tcp ポートへのアクセス)について継続報告を行いました。

□ 2007 年 2 月の観測状況について

<http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0703.pdf>

Ping(ICMP)(\*12)アクセスおよび Symantec 社のセキュリティ対策ソフトのぜい弱性を狙ったと思われるアクセス(2967/tcp ポートへのアクセス)について継続報告を行いました。さらに、中国(中華人民共和国)方面から一時的に増加した 139/tcp ポートへのアクセスについて報告しました。

## 5 . 用語解説

以下に、本文中にある用語について解説します。

### (\*1) ブートセクタ感染型ウイルス

ブートセクタ感染型ウイルスとは、システム領域感染型ウイルスとも呼ばれ、ディスクのブートセクタやパーティション領域に感染し、コンピュータシステムの起動時に活動を開始するウイルスです。ブートセクタ/パーティション領域感染型とも呼ばれています。

例えば、感染したフロッピーディスクをセットしたままコンピュータを再起動し、フロッピーディスクのブートセクタを読み込んでしまうと、ウイルスが実行され、そのコンピュータのハードディスクに感染してしまいます。

### (\*2) ファイル感染型ウイルス

アプリケーションプログラムのファイルや、オペレーティングシステムを構成するシステムファイル、データファイルなど、ファイルを感染対象とするウイルスの総称。どんなファイルを狙うかによって、実行ファイル型やマクロ型などに細分化できます。

### (\*3) マクロ感染型ウイルス

ファイル感染型ウイルスの一種で、マクロ命令(スクリプト)を使用できるデータファイルのマクロ命令部分に感染するものを、特にマクロ感染型ウイルスと呼びます。感染したデータファイルを開いて、マクロ命令部分が動作すると発病します。

### (\*4) トロイの木馬型ウイルス

トロイの木馬型ウイルス(プログラム)は、有益なプログラムのふりをしてユーザの知らない間に不正な行為を行うウイルスです

最近話題のスパイウェアやボットも、当初はこのトロイの木馬型ウイルス(プログラム)に分類されていました。

### (\*5) ネットワーク感染型ウイルス

ネットワークに接続しているだけで、感染するウイルスで、トロイの木馬型ウイルス(プログラム)が利用者の意図に反してダウンロードされたり、特定の Web サイトを閲覧しただけでダウンロードさせられたりするものです。さらに、同じネットワークに接続している他のコンピュータへも感染活動を行います。

### (\*6) NCSA: National Center for Supercomputing Applications

米国立スーパーコンピュータ応用研究所のこと。グラフィカルな Web ブラウザ、NCSA <http://www.nslc.org/Mosaic/> を開発しました。

### (\*7) phf

phfとは、NCSA httpd や Apache に添付されていた CGI(Common Gateway Interface) のスクリプト(サンプルプログラム)です。しかしながら httpd を起動しているユーザ権限にて悪意あるコマンドの実行を許可してしまうぜい弱性を持っていました。

### (\*8) メール不正中継

電子メールの悪用の手段。例えば、sendmail プログラムのぜい弱性を悪用して、無関係なサイトへの電子メールの不正な中継を行わせること。

### (\*9) ポートスキャン

攻撃・侵入の前段階として、標的のコンピュータの各ポートにおけるサービスの状態を調査すること。

ポート(port)とは、IP アドレス(コンピュータ)毎のコンピュータ内の各種サービスの窓口のことです。ポートは 0 から 65535 までの数字が使われるためポート番号とも呼ばれます。

### (\*10) BIND

DNS サーバソフトウェアで、フリーソフトウェアとして世界的に利用されています。BIND は、カリフォルニア大学バークレー校で開発されました。

### (\*11) サービス妨害攻撃(DoS)/DDoS 攻撃

DoS 攻撃(Denial of Service attack) : サービス妨害攻撃。コンピュータ資源やネットワーク資源を利用できない状態に陥れる攻撃のことです。

DDoS 攻撃(Distributed Denial of Service attack) : 分散型サービス妨害攻撃。DoS 攻撃の攻撃元が複数で、標的とされるコンピュータに大きい負荷を与える攻撃のことです。

### (\*12) Ping(ICMP)

インターネットやイントラネットなどの TCP/IP ネットワーク上で、特定の IP アドレスを割り振られた機器が接続されているか診断するプログラム。診断する機器の IP アドレスを指定すると、ICMP(Internet Control Message Protocol: IP のエラーメッセージや制御メッセージを転送するプロトコル)を使って通常 32 バイト程度のデータを送信し、相手の機器から返信があるかどうか、返信がある場合はどのくらい時間がかかっているか、などの診断結果を得ることができます。

```
C:¥>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:¥>
```

【ping コマンドの実行例】

### (\*13) スпамメール

スパムメールとは、無差別に送られてくるダイレクトメールなどの広告メールことを言います。国内では、出会い系の勧誘メールや、アダルトサイトへの勧誘メールなどが多く見受けられ、ワンクリック詐欺や、フィッシングなどを目的にしたメールも多いようです。

### (\*14) 不要なサービスの停止

一般の利用者には少し難しい話かも知れませんが、自分が実行させようとしているソフトウェアについて十分に理解し、興味本位でのフリープログラムのインストールや利用は避けたほうが無難であるということです。特に、インターネットへのアクセスをとまなうソフトウェアの場合は、ソフトウェアの技術的な処理論理やアクセス先の確認が重要で、信頼できるソフトウェアかどうかの判断も必要となります。

### (\*15) パーソナルファイアウォール(personal firewall)

エンドユーザが使用するパーソナルコンピュータ上で、インターネットからの不正なアクセスやワームによる攻撃を防ぐために導入するソフトウェアです。

### (\*16) SYN Flood 攻撃

DoS 攻撃(\*11)の1つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット(3 ウェイ・ハンドシェーク(\*17)での接続確立の最初に送られるパケット)を大量に送りつけ、確立途中状態の接続を大量作成することで、過負荷を与えるものです。

### (\*17) 3 ウェイ・ハンドシェーク

TCP(Transmission Control Protocol)で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下に A と B の通信確立の手順を示します

- ①A から B へ SYN パケットの送信
- ②B から A へ ACK+SYN パケットの送信
- ③A から B へ ACK パケットの送信

これで、AB 双方の通信が確立されます。

#### お問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター  
宮本 / 内山 / 加賀谷

Tel:03-5978-7527 Fax:03-5978-7518

E-mail:isec-info@ipa.go.jp