

平成20年上半期におけるインターネット治安情勢について

【インターネット定点観測システム等での観測結果】

インターネットに接続したコンピュータに対する無差別なサイバー攻撃は、前期に比較してほぼ横ばいで、依然として高水準にとどまっています。ワームの活動と思われる攻撃やボットの活動も継続して続いています。攻撃手法には変化がみられ、SYN flood 攻撃が増加しました。Windows の Messenger サービスを悪用する手口も確認される等、攻撃手法が多様化しています。

1 はじめに

警察庁では、国民生活又は社会経済活動に重大な影響を及ぼすおそれのある情報システムに対する犯罪を未然に防止し、あるいは被害の拡大防止を図るために必要となる情報を収集する手段のひとつとして、全国の警察施設のインターネット接続点におけるアクセス情報等を観測・分析し、情報セキュリティの向上に資する情報の提供等を実施しています。

本資料は、サーバの管理者を中心としたインターネット利用者のセキュリティ対策の参考としていただくため、平成20年1月から6月までの上半期に警察庁がインターネットを直接観測することにより把握した情報を取りまとめ公表するものです。

2 定点観測の結果

全国の警察施設のインターネット接続点¹に設置してあるファイアウォール²と侵入検知装置³の記録を全般的に分析したものを以下で紹介します。

2.1 全般的なアクセス状況：無差別な攻撃は依然高水準を維持

今期は、前年同期と比較するとアクセス件数は減少しましたが、前期との比較ではほぼ横ばいの推移となりました。サーバ、パソコン一台（1IP）あたり平均して約7分50秒に1回のアクセスが観測されており、無差別なサイバー攻撃は、依然として高水準を維持しています。

今期、ファイアウォールに対する総アクセス件数は、1IPあたり約33,500件で、前年同期比較では約33%減少していましたが、前期との比較ではほぼ横ばいで推移しました。また、警察庁で侵入検知装置を利用して検知したワーム等の活動は、1IPあたり約1,800件で、前年同期比較では約14%減少しており、前期と比較して約5%減少しました。

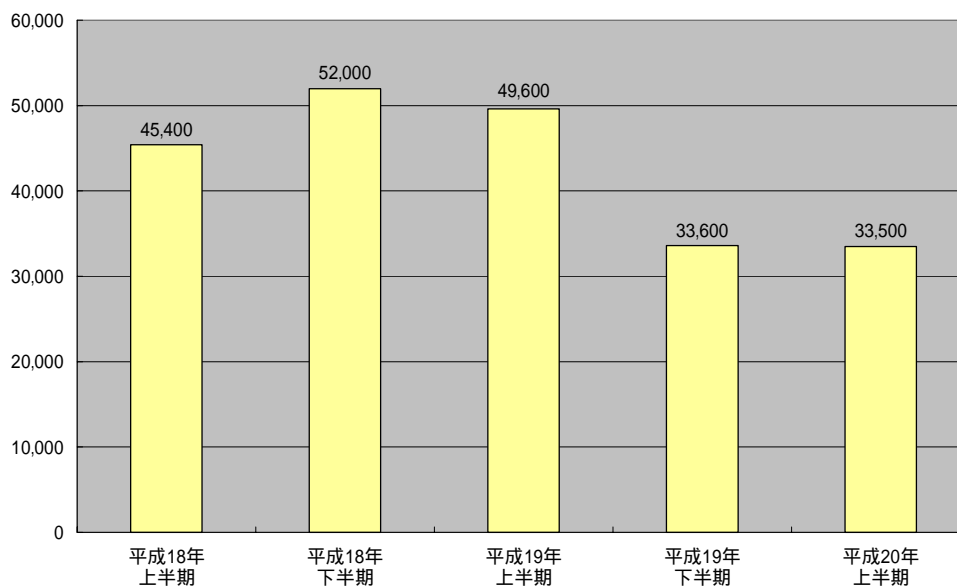


図 2-1 ファイアウォールへの1IPあたりの総アクセス件数の推移

¹ 日本国内の拠点の1IPあたりの観測記録をもとに分析しています。

² 集計は、incomingのトラフィックのみ対象とし、outgoingのトラフィックは対象としていません。

³ 平成20年6月30日現在、381種類のシグネチャが登録されています。

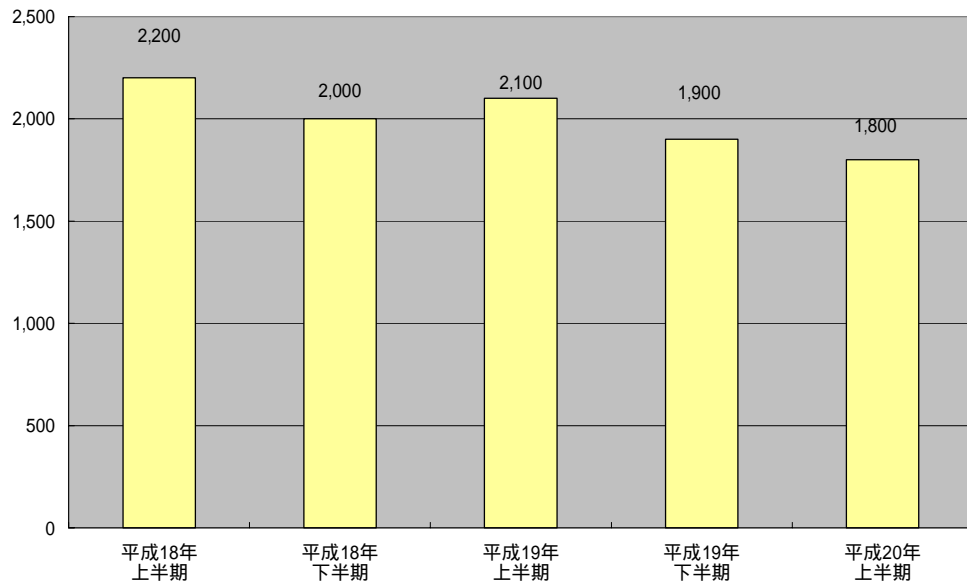


図 2-2 侵入検知装置での 1IP あたりのアラートの総検知数の推移

2.2 宛先ポート別の推移

ファイアウォールに対するアクセスは、1026/udp、1027/udp へのアクセスが大幅に増大し、1026/udp は、1日・1IP あたり 18.5 件で前期と比較して約 127% 増加し、1027/udp は、1日・1IP あたり 17.0 件で約 363%増加しました。なお 1026/udp 及び 1027/udp は Windows の Messenger サービスを利用したスパムの通信に利用されることが多いものです。

また、これまで上位を占めてきた 445/tcp へのアクセスは、1日・1IP あたり 5.4 件で前期と比較して約 44%減少しました。

| | 平成18年 上半期 | 平成18年 下半期 | 平成19年 上半期 | 平成19年 下半期 | 平成20年 上半期 |
|--------------------|--------------|--------------|--------------|--------------|--------------|
| 135/tcp | 78.8 | 94.1 | 82.3 | 57.9 | 58.7 |
| ICMP(Echo Request) | 21.6 | 34.6 | 65.0 | 39.2 | 29.8 |
| 1026/udp | 7.6 | 13.7 | 14.7 | 8.2 | 18.5 |
| 1027/udp | 2.5 | 5.5 | 9.5 | 3.7 | 17.0 |
| 1433/tcp | 15.6 | 11.8 | 7.1 | 8.4 | 11.7 |
| 1434/tcp | 11.1 | 10.1 | 10.1 | 8.7 | 9.3 |
| 22/tcp | 5.9 | 6.1 | 7.1 | 5.2 | 6.2 |
| 445/tcp | 47.0 | 51.0 | 25.8 | 9.8 | 5.4 |
| 2967/tcp | 0.0 | 1.1 | 8.7 | 4.2 | 3.3 |
| 4899/tcp | 8.5 | 5.8 | 4.7 | 4.1 | 3.2 |

表 2-1 宛先ポート別の1日・1IPあたりのアクセス件数の推移

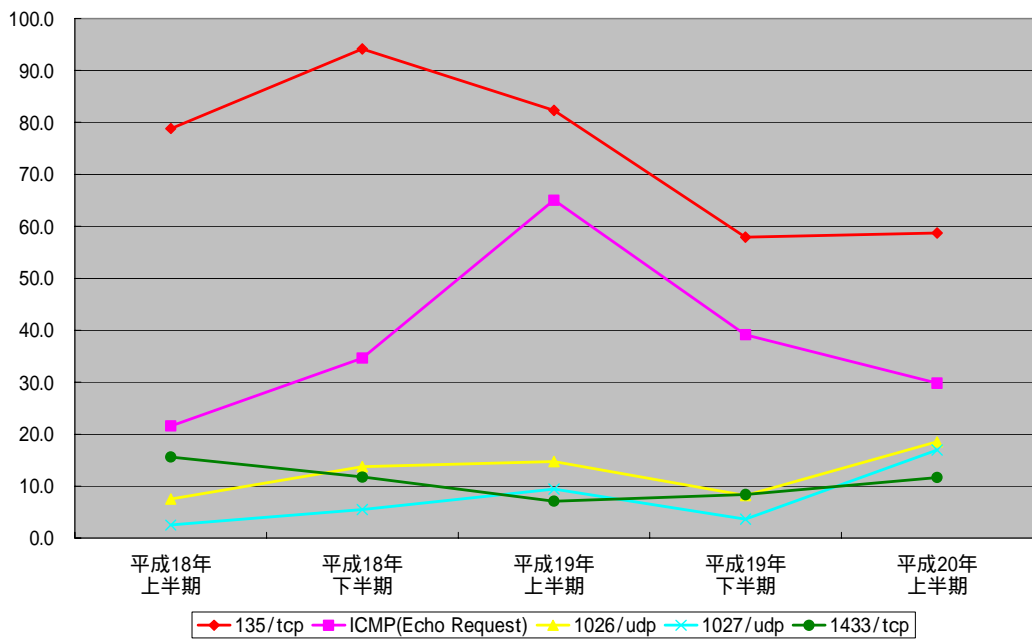


図 2-3 宛先ポート別の1日・1IPあたりのアクセス件数の推移(1位から5位)

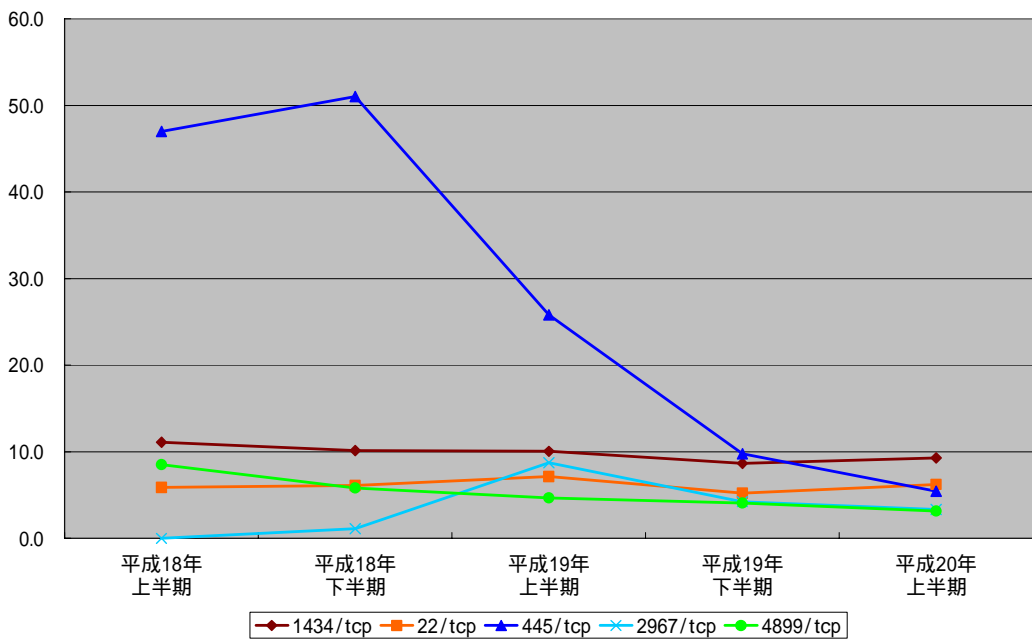


図 2-4 宛先ポート別の1日・1IPあたりのアクセス件数の推移(6位から10位)

2.3 発信元（国／地域）別の推移

ファイアウォールへのアクセス件数が多い発信元の国／地域は、平成19年の下半期を境に、日本と中国の順位が入れ替わっています。前期と比較すると、中国からのアクセスが1日・1IPあたり78.8件で約63%増加し、日本国内からのアクセスが1日・1IPあたり44.0件で約6%減少しました。

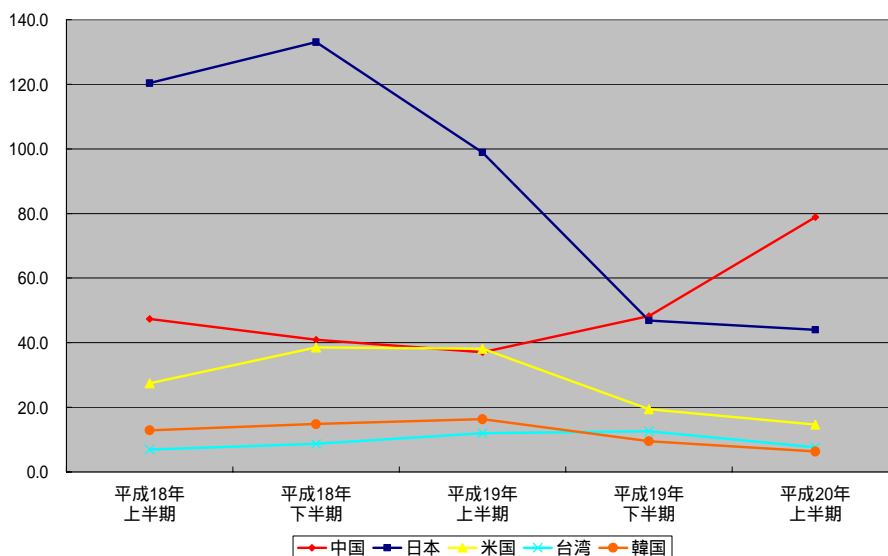


図 2-5 発信元(国/地域)別の1日・1IPあたりのアクセス件数の推移
(1位から5位)

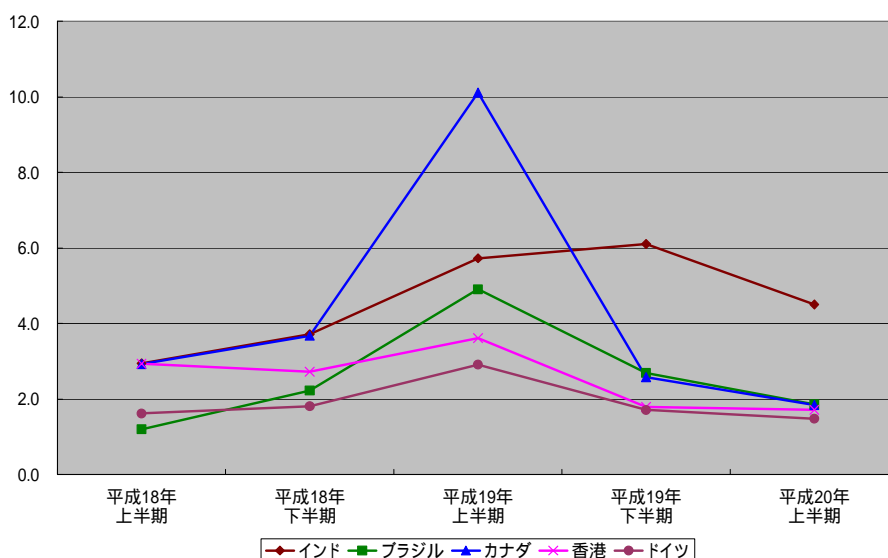


図 2-6 発信元(国/地域)別の1日・1IPあたりのアクセス件数の推移
(6位から10位)

| | 平成18年 上半期 | 平成18年 下半期 | 平成19年 上半期 | 平成19年 下半期 | 平成20年 上半期 |
|------|--------------|--------------|--------------|--------------|--------------|
| 中国 | 47.3 | 41.0 | 37.1 | 48.2 | 78.8 |
| 日本 | 120.4 | 133.1 | 98.9 | 46.9 | 44.0 |
| 米国 | 27.5 | 38.5 | 38.2 | 19.4 | 14.7 |
| 台湾 | 6.9 | 8.7 | 12.0 | 12.6 | 7.6 |
| 韓国 | 12.9 | 14.8 | 16.3 | 9.5 | 6.3 |
| インド | 2.9 | 3.7 | 5.7 | 6.1 | 4.5 |
| ブラジル | 1.2 | 2.2 | 4.9 | 2.7 | 1.9 |
| カナダ | 2.9 | 3.7 | 10.1 | 2.6 | 1.8 |
| 香港 | 2.9 | 2.7 | 3.6 | 1.8 | 1.7 |
| ドイツ | 1.6 | 1.8 | 2.9 | 1.7 | 1.5 |

表 2-2 発信元(国/地域)別の1日・1IPあたりのアクセス件数の推移

2.4 攻撃手法別の推移

侵入検知装置を利用して検知したアラート⁴の件数を前期と比較すると、「Worm」が1日・1IPあたり約9件で、前期と同数ですが、全体の約94%を占めていました。「Scan」は、1日・1IPあたり約0.52件で約55%減少しました。なお「その他」は、1日・1IPあたり約0.04件で約60%減少し、その多くは「Traceroute」が占めていました。

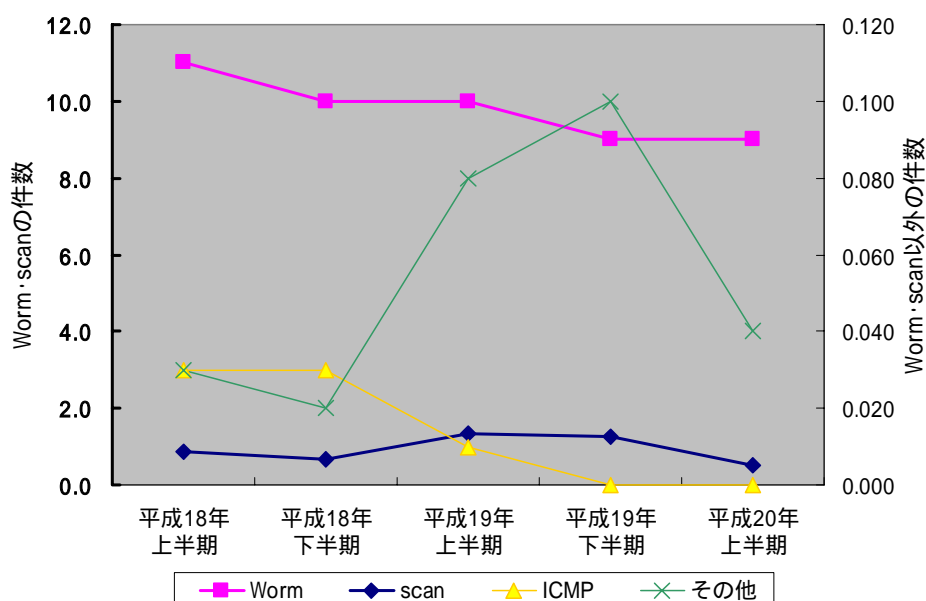


図 2-7 攻撃手法別の1日・1IPあたりのアラート件数

| | 平成18年 上半期 | 平成18年 下半期 | 平成19年 上半期 | 平成19年 下半期 | 平成20年 上半期 |
|------|--------------|--------------|--------------|--------------|--------------|
| Worm | 11 | 10 | 10 | 9 | 9 |
| Scan | 0.88 | 0.65 | 1.33 | 1.25 | 0.52 |
| ICMP | 0.03 | 0.03 | 0.01 | 0 | 0 |
| その他 | 0.03 | 0.02 | 0.08 | 0.1 | 0.04 |

表 2-3 攻撃手法別の1日・1IPあたりのアラート件数

⁴ 侵入検知装置で検知された各シグネチャは、以下のとおりに分類しています。

Worm : SQL Slammer

Scan : Proxy attempt, Port sweep, SYN FIN scan, FIN scan, NMAP TCP, NMAP XMAS, NMAP Fingerprint, Portscan Detection Attack, Window size of 55808(SYN) TCP Packet

ICMP : Superscan Echo, redirect host, redirect net, Ping Flooding

2.5 サーバコンピュータに対する DoS 攻撃 (SYN flood 攻撃)

ファイアウォールに送信された SYN/ACK パケットを分析することにより、DoS 攻撃の一手法である SYN flood 攻撃の兆候について観測を行ったところ、SYN flood 攻撃の総検知件数は 1IP あたり約 2,274 件で、前期と比較して約 141%増加しました。

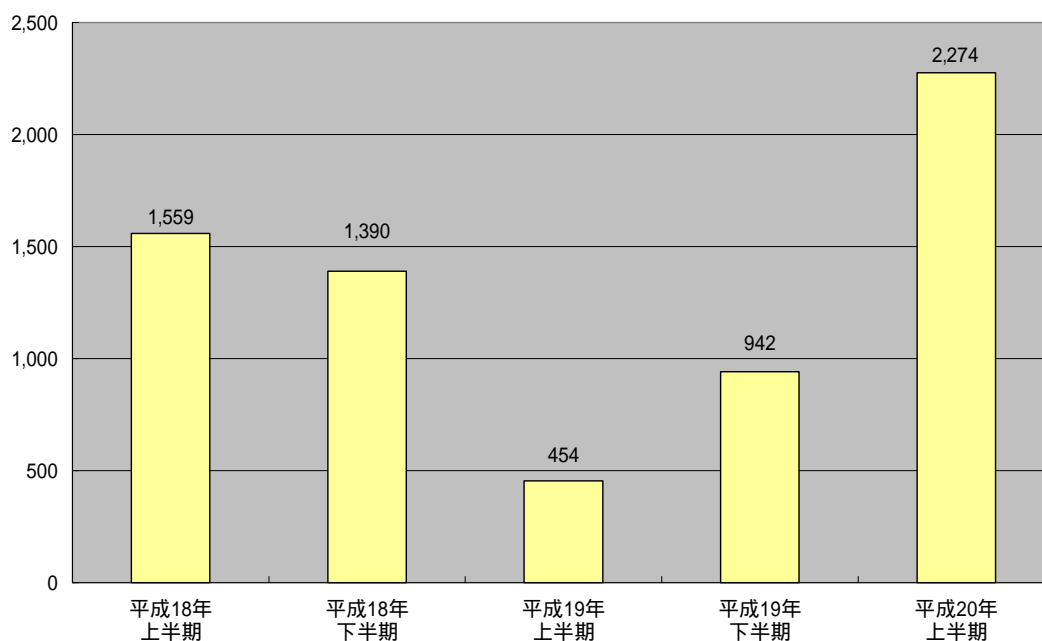


図 2-8 DoS 攻撃(SYN flood 攻撃)の 1IP あたりの推移

2.6 国内からの攻撃

今期、侵入検知装置を利用して検知したワーム等の活動について全世界からのものと日本国内からのものを比較すると、全世界のコンピュータからのものは約 1,800 件で、前期と比較して約 5%減少しました。日本国内のコンピュータからのものは約 34 件で、前期と比較して約 11%減少しました。また、ファイアウォールへの全世界のコンピュータからのアクセス件数は約 33,500 件で、前期と比較してほぼ横ばいで推移していました。日本国内のコンピュータからのアクセス件数は約 8,000 件で、前期と比較して約 7%減少しました。日本国内からの攻撃の減少率は、全世界の攻撃の減少率よりも高くなっていました。

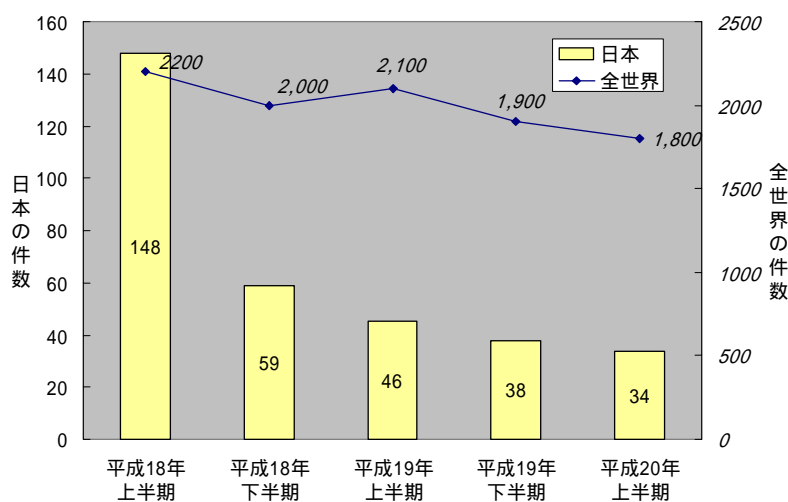


図 2-9 侵入検知装置への 1IP あたりの総アラート件数の推移

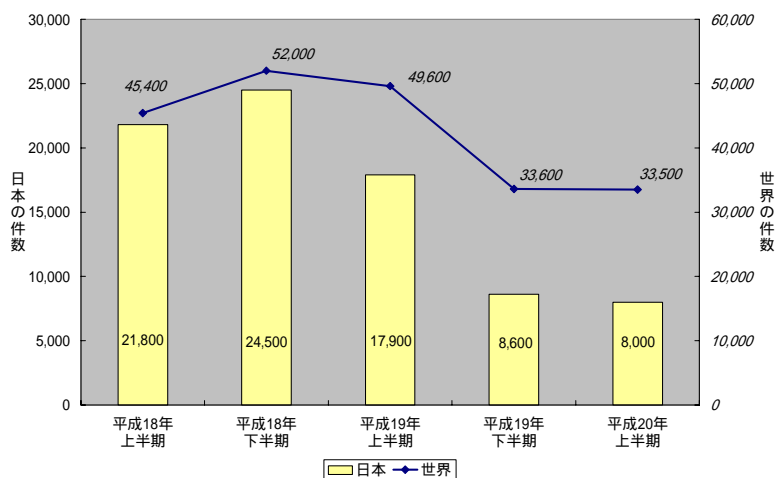


図 2-10 ファイアウォールへの 1IP あたりの総アクセス件数

3 ボットネット観測の結果

ボットは不正プログラム的一种で、プログラムの脆弱性を悪用するなどしてコンピュータに感染し、コンピュータが遠隔操作できる状態になったことを攻撃者に伝えて命令を待ちます。攻撃者はボットに感染した多数のコンピュータを一斉に操作できるようにネットワーク化した「ボットネット」を構築し、サイバー攻撃等を行うための道具として利用しています。ボットは DoS 攻撃、迷惑メールの大量送信のほか、個人情報等の窃取、フィッシング詐欺などにも利用可能であり、国のインフラ、経済の脅威になりつつあります。

3.1 ボットネット観測件数の推移

今期、警察庁で観測したボットネットは 247 個で、前期の 305 個に比べ約 19% 減少しました。そのうち今期に新たに把握したものが 104 個あり、前期から継続して存在しているものが 143 個、今期に観測できなくなったものが 162 個ありました。

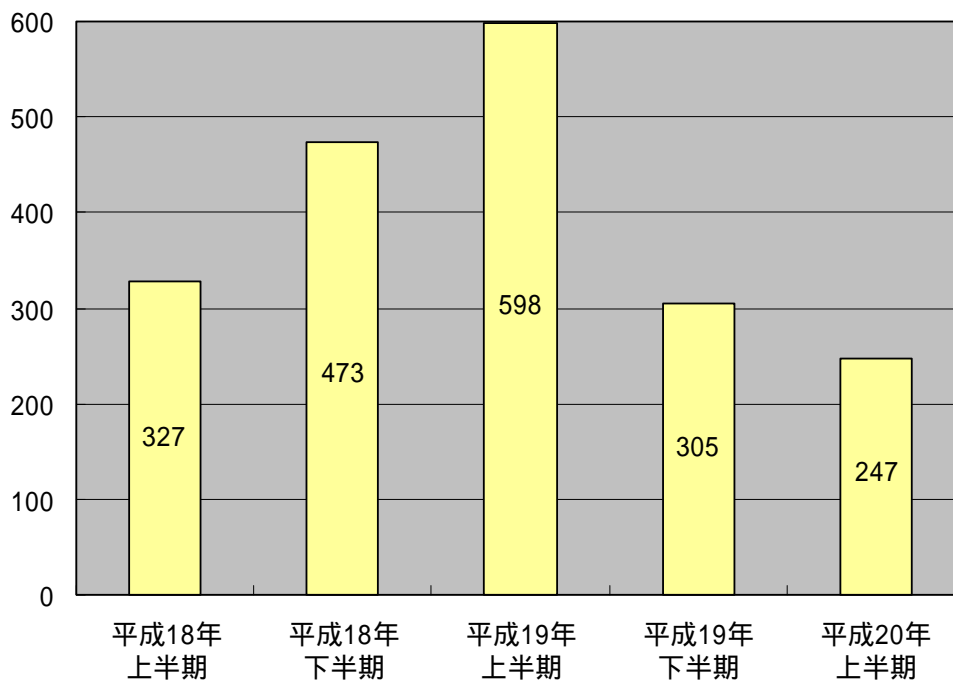


図 3-1 ボットネット認知数の推移

3.2 ボット観測件数の推移

今期、警察庁で観測したボットネットを構成するボットに感染したコンピュータは296,423台で、前期の392,949台と比べ約25%減少しました。このうち日本に所在すると考えられるコンピュータは11,998台に上り、前期の14,960台と比べ約20%減少しました。今期観測した最も大きなボットネットは、約12万台のボットから構成され、通信プロトコルとしてIRC、通信ポートは7000番を使用していました。日本に所在するIRCサーバを利用していた最も大きなボットネットは、約6,800台のボットから構成されており、通信プロトコルとしてIRC、通信ポートは80番を使用していました。一般にHTTPプロトコルとしてよく使われている通信ポート80番が、IRCプロトコルを利用したボットネットの通信手段となっていました。

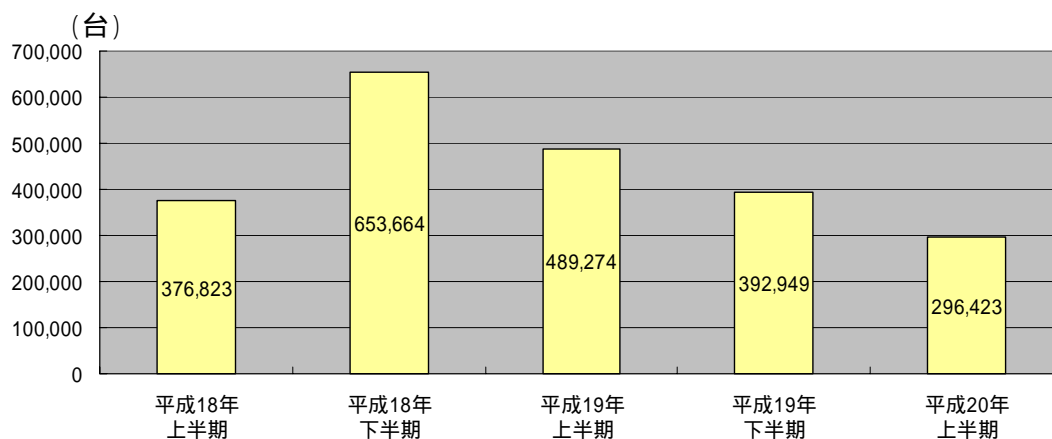


図 3-2 ボット認知数の推移

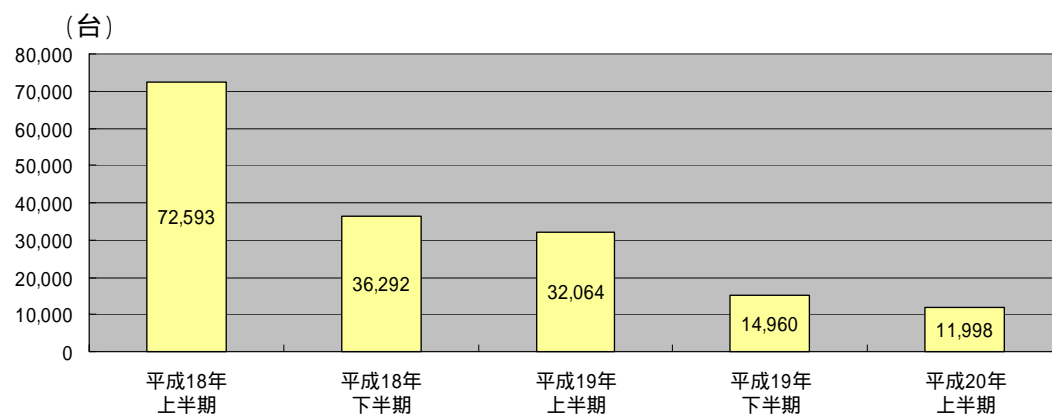


図 3-3 ボット認知数の推移(日本)

4 DNS サーバの現状調査

DNS(Domain Name System)は、コンピュータのホスト名と IP アドレスを対応付けるサービスであり、インターネットの基幹システムの一つです。DNS の各種サーバソフトウェアには、過去にさまざまな脆弱性やサイバー攻撃の踏み台として利用される可能性（外部からの再帰的な問い合わせの許可）などが報告されています。

そこで、DNS サーバの現状を把握するために、2008 年 4 月 1 日～2008 年 5 月 31 日の間、日本国内の主要な重要インフラ事業者等⁵のサイトで使用されている DNS サーバ 2,022 台を対象に調査を実施した結果、次のことが判明しました。

調査対象の約半数が外部からの再帰的な問い合わせを許可

BIND のバージョン情報の問い合わせに対する回答の分類毎に、外部からの再帰的な問い合わせを許可している割合が異なる

4.1 再帰的な問い合わせによるサイバー攻撃に利用される可能性

「再帰的な問い合わせ」とは、DNS サーバの機能の一つで、利用者のコンピュータから、ホスト名に対応する IP アドレスを知りたい等の問い合わせを受けた DNS サーバが、他の DNS サーバに対して問い合わせを行い、得られた情報を利用者のコンピュータに回答する機能です。外部からの再帰的な問い合わせが可能な場合、DDoS 攻撃の踏み台⁶にされる可能性があります。

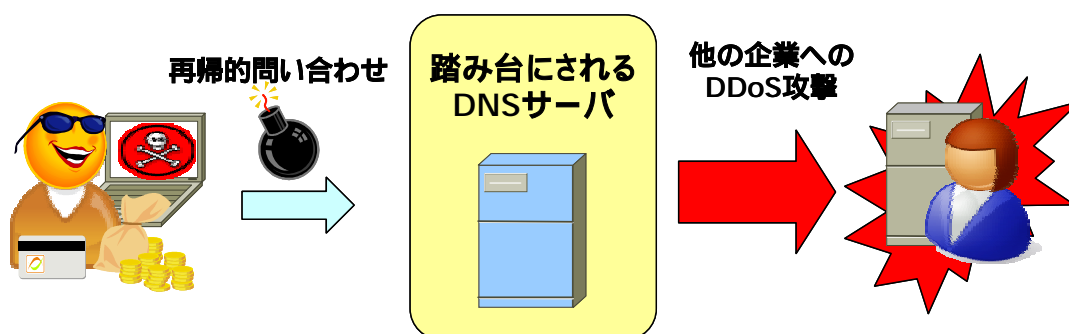


図 4-1 DNS の再帰的な問い合わせを悪用した攻撃の例

⁵ 警察庁では、「情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流」の 10 分野の基幹システムを管理又は運用する事業者等を重要インフラ事業者等としています。

⁶ 「DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について」をご参照ください。
http://www.cyberpolice.go.jp/server/rd_env/pdf/20060711_DNS-DDoS.pdf

4.2 DNS サーバの調査

(1) 外部からの再帰的な問い合わせに関する調査

外部からの再帰的な問い合わせを許可している DNS サーバは、49%で調査対象の約半数を占めました。

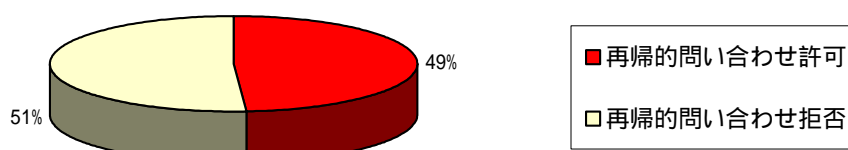


図 4-2 外部からの再帰的な問い合わせが可能な DNS サーバの割合

(2) サーバソフトウェアとバージョン情報調査

DNS サーバに対しバージョン情報の問い合わせを行ったところ、BIND8 と回答したサーバは 6%、BIND9 と回答したサーバは 23%、その他の文字列を回答するサーバは 45%でした。BIND のバージョン情報の問い合わせに対して回答しないサーバは 26%でした。

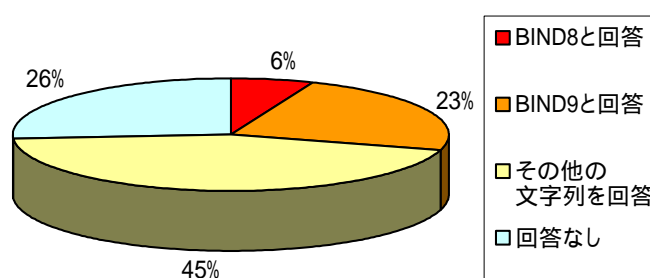


図 4-3 BIND のバージョン情報問い合わせに対する回答

(3) バージョン情報の問い合わせ結果と外部からの再帰的な問い合わせの許可との関係

再帰的な問い合わせの可否をバージョン情報の問い合わせに対する応答の別に分類しました。外部からの再帰的な問い合わせを許可するものは、BIND8と回答したものは80%、BIND9と回答したものは68%、その他の文字列を回答したものは55%でした。BINDのバージョン情報の問い合わせに対して回答をしなかったものは13%でした。外部からの再帰的な問い合わせを許可している割合は、BIND8と回答したものが最も高く、回答しないものが最も低いという傾向が見られました。

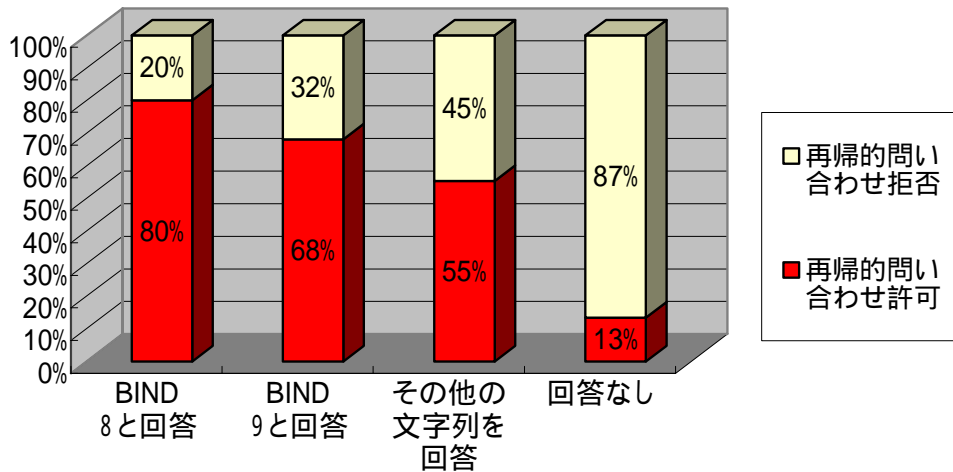


図 4-4 バージョン情報取得状況と再帰的な問い合わせの可否の割合

5 Messenger スパムの情勢について

Messenger スпамとは、マイクロソフト社の OS である Windows 上で動作する Messenger サービス⁷を利用したスパムです。

警察庁のインターネット定点観測では、2004 年から継続的に Messenger スпамを検知していますが(図 5-2 のとおり)、2007 年 12 月頃から検知件数が増加しています。

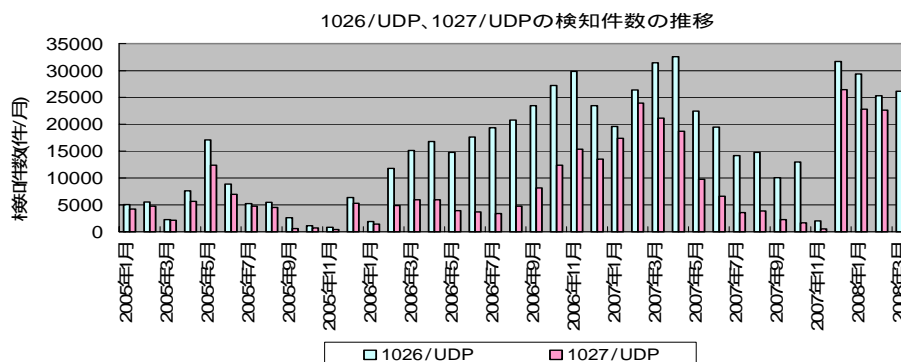


図 5-1 2005 年 1 月から 2008 年 3 月の観測状況

そこで、現状を調査した結果、次のことが判明しました。

ユーザをだまし、悪意のあるソフトウェアをインストールさせようとする Messenger スпамが存在

Messenger スпамの受信頻度は、最も多いときで 5 分に 1 回

1026/UDP 及び 1027/UDP 以外のポートへのアクセスを行う Messenger スпамが存在

5.1 Messenger サービスと Messenger スпам

Messenger サービスとは、マイクロソフト社の Windows 上で動作するサービスの一つで、ネットワーク経由で簡単なメッセージをやり取りすることができます。一方で、この Messenger サービスの機能を利用してコンピュータの画面上に迷惑メッセージを表示させる Messenger スпамが存在します。

警察庁で観測した代表的な Messenger スпамは、「Windows に深刻なシステムエラーが発生した。エラーを修復するためには、www. .com からプログラムをダウンロードして実行すること。この作業を行わない場合は、システム障害が発生する可能性がある。」と、英文で記述されたメッセージを表示す

⁷ ここで述べる Messenger サービスとは、Windows Messenger、MSN Messenger 等のインスタントメッセンジャーとは別のものです。

るものでした。

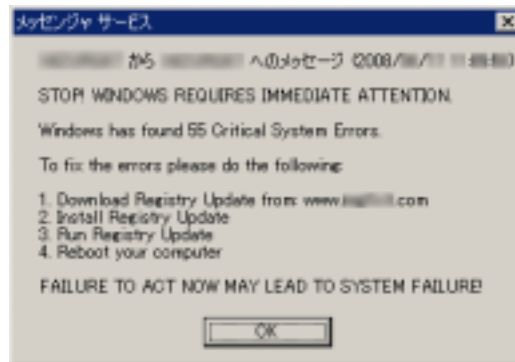


図 5-2 代表的な Messenger スパムの内容

5.2 Messenger スпамに記述された URL

観測した Messenger スпамには、メッセージ本文にホスト名（ドメイン名）が記述されているものがあり、内容は、記述されたホストにアクセスし、プログラムのダウンロードを促すメッセージでした。

そこで、これらのホストにアクセスしたところ、アクセスした時点では、Web ページが存在しないものが大半でしたが、Web ページにアクセスが可能であるホストが存在し、「OS のエラーを修復するプログラム」と称するソフトウェアをダウンロードできることが確認されました。

今回ダウンロードできたソフトウェアは、すべて、実行させると OS にセキュリティ上の問題がないにも関わらず、「OS に 件の問題が見つかりました。」等と虚偽のメッセージを表示し、セキュリティソフトと称するものを購入させようとする、悪意のあるソフトウェアでした。

5.3 Messenger スパムのアクセス状況

Messenger スпамが主に利用する 1026/UDP 及び 1027/UDP について調査したところ、Messenger スпамは、最も多いとき、5 分に 1 回の間隔で観測されました。

5.4 1026/UDP、1027/UDP 以外に対する Messenger スпам

Messenger スпамの観測状況を、送信先ポート別に調査したところ、1026/UDP 及び 1027/UDP が約 96% を占めました。一方で、同じく Messenger サービスで使用されている 135/UDP や、1024 番よりも大きな UDP の一時ポート等に対してアクセスを行う Messenger スпамの存在も確認されました。

6 警察庁で確認したその他の攻撃手法

警察庁では定点観測のほか、重要インフラ訪問、民間企業等からの情報提供等により、さまざまな攻撃の情報を収集しています。以下では、今期に警察庁で収集された情報の中から3つ紹介します。

(1)SQL インジェクションによるホームページの改ざん

企業等が構築した Web アプリケーションを攻撃対象とする SQL インジェクションによるものと思われるホームページの改ざんが確認されています。

SQL とは、データベースに対する命令等をプログラムするプログラム言語の一種です。SQL インジェクションとは、データベースを利用した Web アプリケーションに対しサービスを利用するための本来の入力以外に、SQL を悪用したコードを入力し、データベースを操作する攻撃です。この攻撃が成功すると個人や企業等の情報の漏えいや、ホームページの改ざんにより利用者を悪意のあるサイトへ誘導すること等が可能になります。

(2)標的型メール攻撃

企業等の組織や個人を直接の対象として悪意のあるソフトウェアを添付したメールを送り付ける標的型メール攻撃が確認されています。

無差別に大量のメールを送付するスパムメールと異なり、非常に巧妙に作られており、心当たりのある組織や知人を詐称したものがあります。不用意に添付されたファイルを開くと、コンピュータに悪意のあるソフトウェアが感染します。感染したコンピュータからは個人情報の漏えいや、他のコンピュータ等へのサイバー攻撃の踏み台等に利用される可能性があります。

(3)USB メモリ感染型ワーム

USB メモリ等を介して感染するワームが確認されています。

インターネット接続されていないコンピュータにも感染するため、企業等のインターネットに接続されていない内部ネットワークに接続されているコンピュータ等にも、感染した USB メモリ等を接続することで侵入することが可能です。

7 対策

インターネットを利用されている皆さんが自らの情報資産を守るためのみならず、ポットに代表されるような、意図せず攻撃者に加担してしまう類の脅威にも対応するためには、普段からセキュリティに関する情報について注意し、推奨されている対策を実施することが重要です。今期、観測されたサイバー攻撃の多くは、その対策を行うことで防いだり、被害を最小にしたりすることが可能になります。以下では、少なくとも対策として講じることが大変重要なものについて紹介します。

- 各ソフトウェアや機器のベンダからリリースされる脆弱性を修正するセキュリティ更新プログラムの適切な適用を行う
- ウイルス対策ソフトの適切な運用を行う
- 使用しているソフトウェアのバージョンの適切な更新を行う

また、企業等のサーバ管理者の皆さんが、情報資産に対する様々な被害を未然に防いだり、軽減したりするにあたって講じることが推奨されるものとして、上記対策に加えて、以下の対策も講じることが大変重要であると考えています。

- パーソナルコンピュータ、Web サーバ以外にも DNS サーバやルータ等の機器においても適正な設定の確認とセキュリティ更新プログラムの適切な適用を行う
- 証跡を定期的に確認し、異常を早期に発見・把握し適切な対策をとる

なお、各対策の実施に当たっては、事前に実施に伴う不具合の発生等を検証するために、ベンダから提供されているセキュリティ情報の確認を行うことも重要です。

警察庁セキュリティポータルサイト「@police」⁸では、一般のパソコンユーザの皆さんやシステム/ネットワーク管理者の皆さんがインターネットを安心して利用できるための情報を公開しています。

⁸ @police URL : <http://www.cyberpolice.go.jp/>

8 おわりに

今期の観測では、インターネットに接続されているコンピュータに対する無差別なサイバー攻撃は、依然として高い水準を維持していました。サーバに対する DoS 攻撃の一種である SYN flood 攻撃は、急激に増加しています。DoS 攻撃によく利用されるボットのプログラムは年々変化しており、より発見されにくくなってきていることも考えられますので注意が必要です。さらに、DNS サーバについての分析結果では、DoS 攻撃等に悪用可能な設定がされている DNS サーバが多数確認されました。また、宛先ポートの変化について、増加が確認された一部を分析した結果、Messenger スпамを悪用する等、サイバー攻撃の手口に新しいものが現れたことが確認できました。

そのほか、定点観測以外では、SQL インジェクションによるものと思われるホームページの改ざん、USB メモリを媒介して感染するワームや攻撃対象を特定の人物や組織に限定し、悪意のあるソフトウェアを添付してメールを送りつける標的型メール攻撃も確認されています。

これらのサイバー攻撃の多くは、コンピュータのソフトウェアの脆弱性や設定の不備等を悪用しています。このようなサイバー攻撃を防ぐために、インターネットを利用される皆さんは、脆弱性を修正するセキュリティ更新プログラムの適切な適用やウイルス対策ソフトの適切な運用、使用しているソフトウェアのバージョンの更新といった一般的なセキュリティ対策を講じることが大変重要です。企業等のサーバ管理者においては、上記一般的なセキュリティ対策に加えて、脆弱性等のセキュリティについて常に情報を収集し、必要なときは、パーソナルコンピュータや Web サーバのみならず、DNS サーバ、ルータ等の機器においても適正な設定やセキュリティ更新プログラムの適切な適用及びバージョンの更新が行われていることを確認し対策を実施することが非常に重要です。

また、サイバー攻撃の早期発見と対処のためには、証跡を定期的に確認し異常を発見し把握することが特に重要となります。

警察庁では、今後とも、様々な機会を捉えて、情報セキュリティ対策に資する情報を積極的に提供し、インターネット社会の安全・安心の確保に努めて参ります。