

平成 21 年 12 月 25 日

我が国におけるインターネット治安情勢

(平成 21 年 11 月期)

- ・SMB の脆弱性を狙ったスキャン活動の可能性
～ 日本国内からの 139/TCP へのアクセスが増加～
- ・Conficker ワームの活動が継続

1 概説

今期のセンサーに対するアクセス件数は、一日・1IP 当たり 367.2 件で、前期と比較して - 12.1 件 (- 3.2%)とやや減少した。検知した発信元 IP アドレス数は一日当たり平均 13,431.3 個で、前期と比較して + 93.9 個 (+ 0.7%)と横ばいであった。

アクセス件数の上位 5 ポートは、445/TCP、135/TCP、ICMP Echo Request(以降、「8/ICMP」と表記する。)、1433/TCP 及び 22/TCP の順であった。

最もアクセス件数が多い445/TCPは、一日・1IP当たり164.6件で、前期と比較して - 13.0 件 (- 7.3%)と、やや減少した。これは、日本国内における一部の IP アドレスからのアクセスが減少したためと思われる。ただし、445/TCP に対するアクセスは、マイクロソフト社のセキュリティ情報 (MS08-067) で公表された脆弱性を悪用する Conficker ワームが多くを占めていると考えられる。Conficker ワームのアクセスは依然として多く観測され、引き続き感染活動は活発である。

アクセス件数の上位 5 か国は、中国、日本、米国、ロシア及び台湾の順であった。

今期は 11 月 13 日から 14 日にかけて、中国から 6919/TCP を発信元ポートとする、大量の跳ね返りパケットを検知した。何者かがオンラインゲームサービスの妨害を目的として、中国のサーバに DoS 攻撃を行ったものとみられる。

日本国内では、11 月 21 日に 139/TCP に対するアクセスが増加し、現在までアクセスが続いている。家庭で使用しているコンピュータがウイルスに感染し、スキャン活動を行っている可能性がある。また、このアクセスは、11 月 14 日にマイクロソフト社から公表された、WindowsOS で使用される SMB (Server Message Block) の脆弱性¹との関連が疑われる。

今期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 11.7 件で、前期と比較して + 0.8 件 (+ 7.1%)と横ばいであった。また、検知した発信元 IP アドレス数の 1 日当たりの平均は 354.1 個で、前期と比較して + 38.7 個 (+ 12.3%)とやや増加している。

¹ 「SMB の脆弱性により、サービス拒否が起こる」(マイクロソフト社)
<http://www.microsoft.com/japan/technet/security/advisory/977544.mspx>

2 インターネット定点観測 センサーに対するアクセス

今期は WindowsOS で使用される SMB の脆弱性を狙ったと見られる日本からの 139/TCP へのアクセス増加や、Conficker ワームの活動が引き続き活発であることが特徴である。今期のセンサーに対するアクセス件数及び発信元 IP アドレス数に大きな変化はなかった。アクセス件数は一日・1IP 当たり 367.2 件で、前期と比較して - 12.1 件 (- 3.2%)、IP アドレス数は一日当たり平均 13,431.3 個で、前期と比較して + 93.9 個 (+ 0.7%) であった。

2-1 宛先ポート別

ワームやボットの感染活動に利用される、445/TCP、135/TCP 及び 8/ICMP に対するアクセスが、前期に引き続き上位を占めている。(図 2-1、表 2-1)

今期 1 位の 445/TCP に対するアクセスは、前期と比較して、やや減少した。これは、日本国内の一部の IP アドレスからのアクセスが減少したためである。しかしながら、445/TCP に対するアクセスのうち、多くを占めるとされる Conficker ワームによるものに減少は見られない。Conficker ワームは、ネットワーク経由のほか、リムーバブルディスク経由で感染を拡大させることも可能であり、感染力の強さをうかがうことができる。

今期 2 位の 135/TCP に対するアクセスには大きな変化はなかった。135/TCP に対するアクセスの 67.2% を日本国内が占めている。日本国内からのアクセスは、前期と比較して、アクセス数に大きな変化はなかったが、発信元 IP アドレス数は 22.8% 減少した。これは、以前から活動していた複数のコンピュータが、スキャン活動を停止した可能性が考えられる。

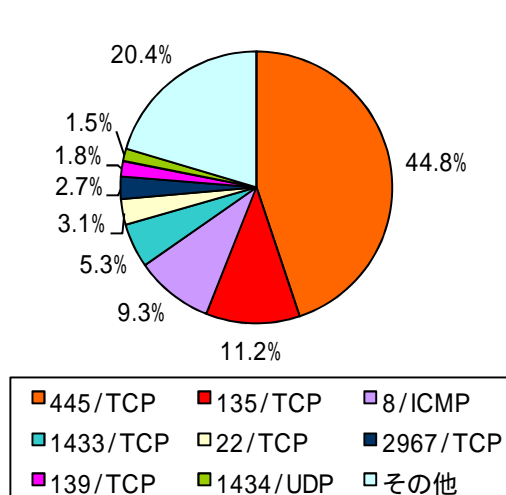


図 2-1 世界の宛先ポート比率¹

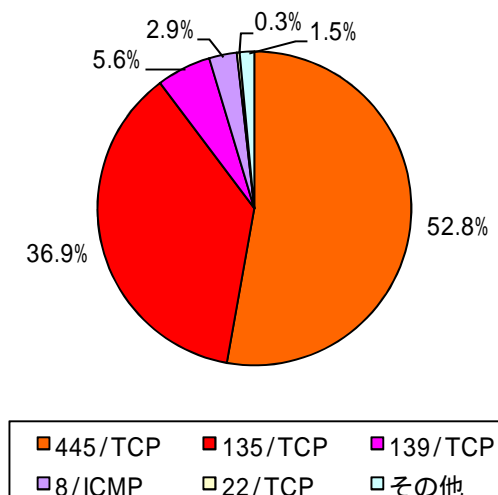


図 2-2 日本の宛先ポート比率¹

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

表 2-1 宛先ポート別検知件数

| 今期 順位 | 前期 順位 | ポート | 今期件数 (一日・1IP 当たり) | 前期比 (一日・1IP 当たり) | 増加 順位 | 減少 順位 |
|----------|----------|----------|----------------------|----------------------|----------|----------|
| 1位 | 1位 | 445/TCP | 164.60 件 | - 7.3% (- 13.02 件) | | 1位 |
| 2位 | 2位 | 135/TCP | 41.00 件 | - 3.3% (- 1.40 件) | | 2位 |
| 3位 | 3位 | 8/ICMP | 34.21 件 | + 17.6% (+ 5.13 件) | 1位 | |
| 4位 | 4位 | 1433/TCP | 19.30 件 | + 6.9% (+ 1.24 件) | | |
| 5位 | 5位 | 22/TCP | 11.23 件 | + 13.7% (+ 1.36 件) | 5位 | |
| 6位 | 6位 | 2967/TCP | 9.81 件 | + 42.3% (+ 2.92 件) | 4位 | |
| 7位 | 10位 | 139/TCP | 6.70 件 | + 104.6% (+ 3.42 件) | 2位 | |
| ... | | | ... | | | |
| 9位 | 18位 | 1521/TCP | 4.99 件 | + 195.0% (+ 3.30 件) | 3位 | |
| ... | | | ... | | | |
| 16位 | 13位 | 23/TCP | 1.67 件 | - 24.2% (- 0.53 件) | | 5位 |
| ... | | | ... | | | |
| 23位 | 16位 | 1024/TCP | 0.82 件 | - 58.2% (- 1.15 件) | | 3位 |
| 24位 | 17位 | 3072/TCP | 0.82 件 | - 56.2% (- 1.06 件) | | 4位 |

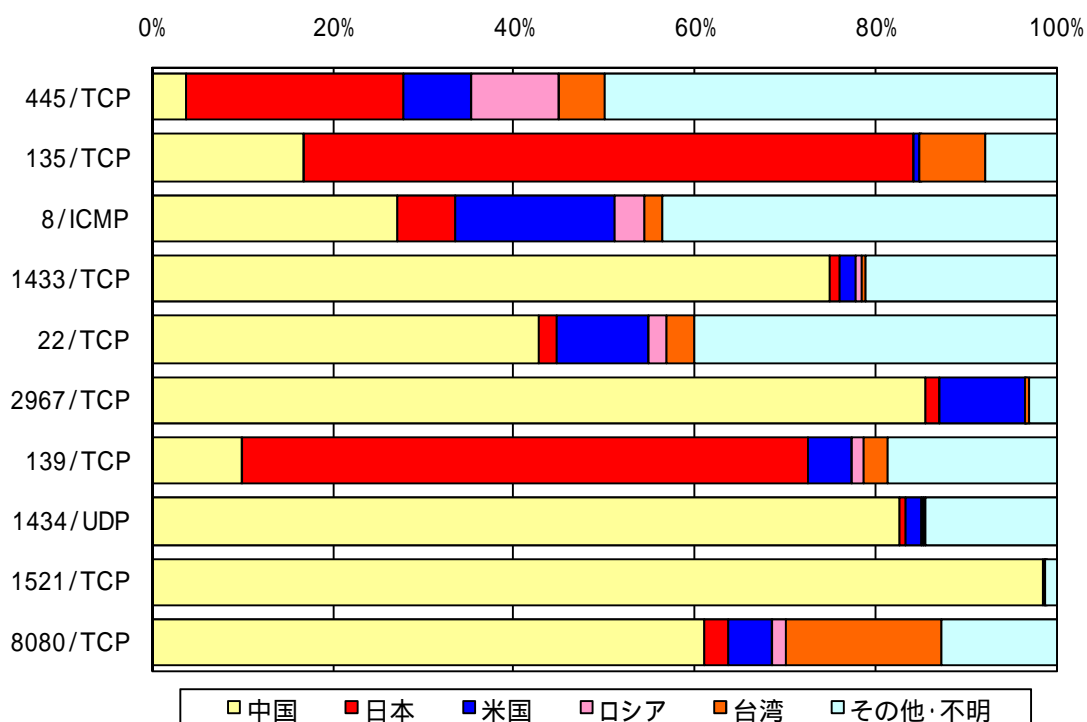


図 2-3 宛先ポートの国・地域別比率

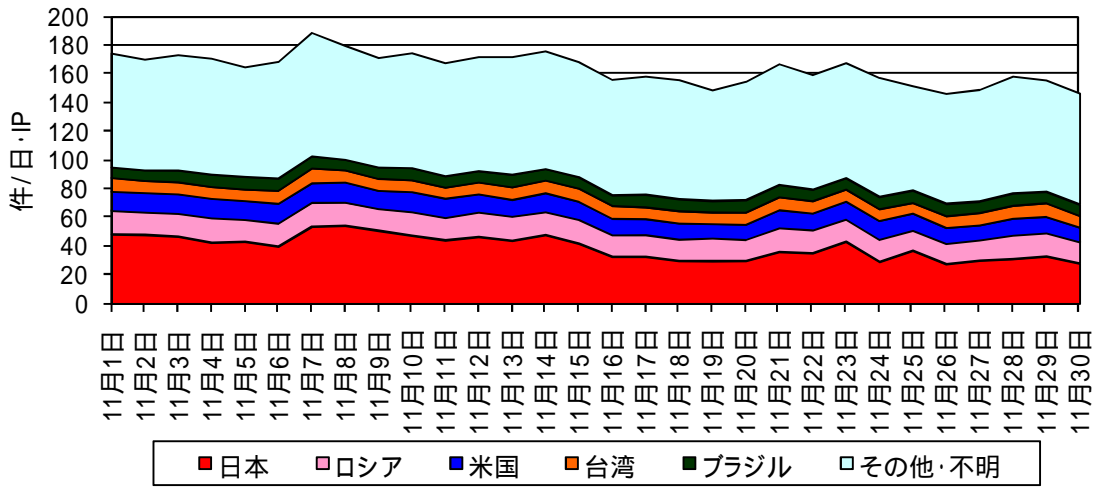


図 2-4 宛先ポート 445/TCP に対するアクセスの推移

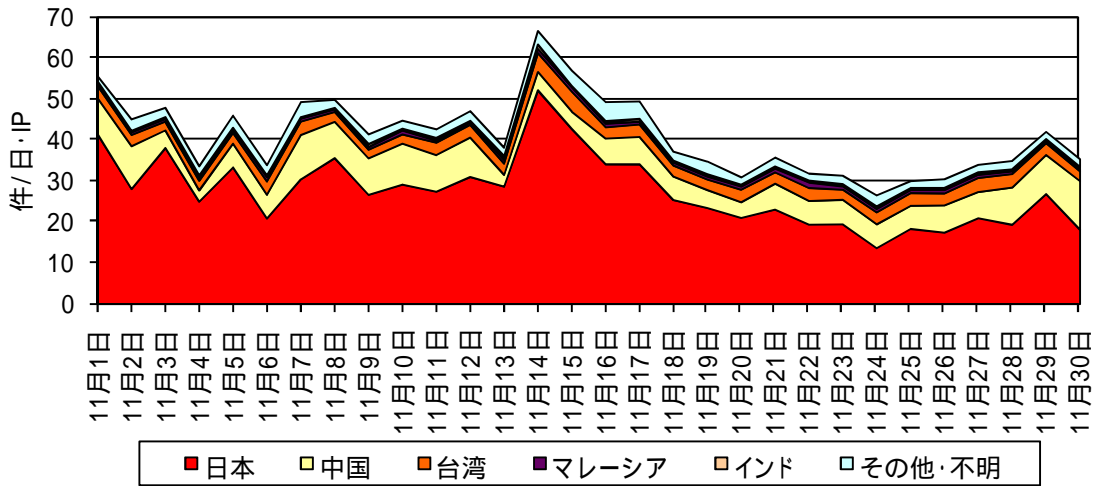


図 2-5 宛先ポート 135/TCP に対するアクセスの推移

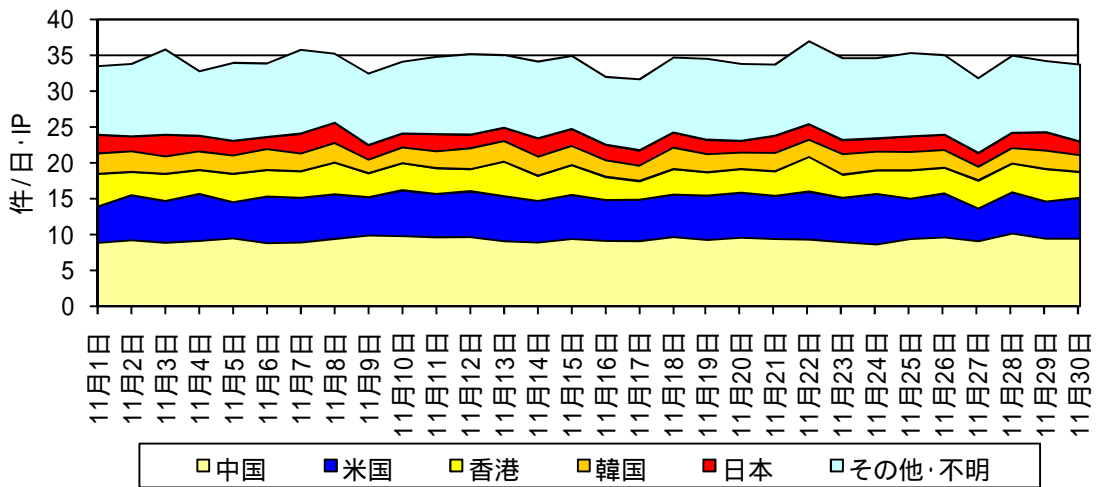


図 2-6 8/ICMP のアクセスの推移

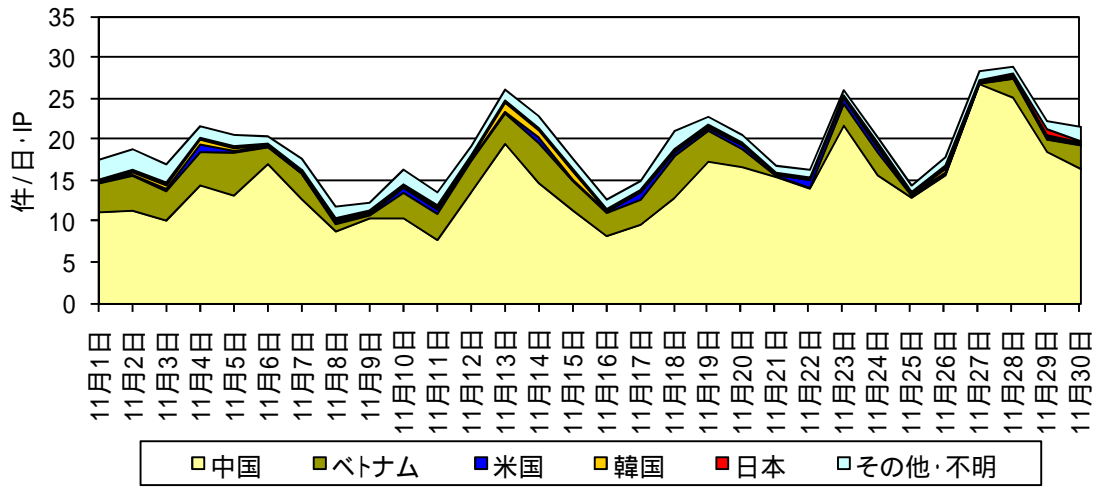


図 2-7 宛先ポート 1433/TCP に対するアクセスの推移

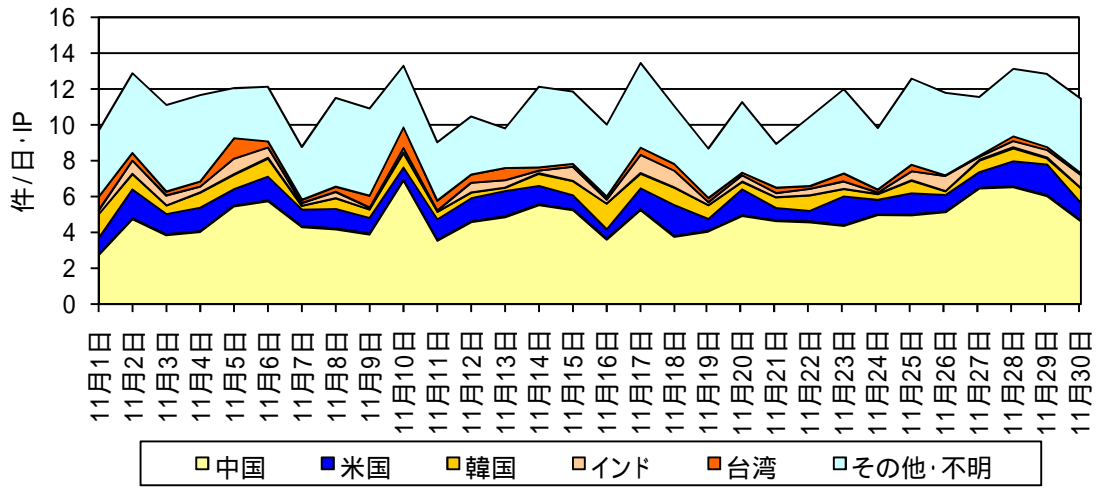


図 2-8 宛先ポート 22/TCP に対するアクセスの推移

2-2 発信元国・地域別

中国の特定のIPアドレスから、11月13日から14日にかけて、6919/TCPを発信元ポートとする、大量の跳ね返りパケットを検知した。(図 2-11 では「その他」に分類される。) 6919/TCP は、オンラインゲームで使用されているポートであり、何者かがオンラインゲームサービスの妨害を目的として、中国のサーバに対して DoS 攻撃を行ったものとみられる。中国からは、今期に限らず、跳ね返りパケットを多く検知している。

また、中国の特定の1IPアドレスから、8/ICMP に対する定期的なアクセスを7月30日から検知している。このアクセスは、10月7日に一旦停止したが、10月27日から再度検知が続いている。この一連のアクセスの目的は判明していない。

今期2位の日本国内からのアクセスは、前期と比較して、やや減少した。これは、日本国内における複数のIPアドレスからの445/TCPに対するアクセスが減少したことが、主な要因である。ただし、445/TCPに対するアクセスの多くがConfickerワームであると考えられ、Confickerワームのアクセスは依然として多く観測されている。引き続き日本国内のConfickerワームの感染活動は活発であると言える。

11月21日以降、日本国内から139/TCPに対するアクセスが見られる。これは、午後に増加し、未明から明け方にかけて減少していることから、家庭で使用されているコンピュータがウイルスに感染し、スキャン活動を行っている可能性が考えられる。11月14日にマイクロソフト社から公表された、WindowsOSで使用されるSMBの脆弱性¹との関連が疑われる。

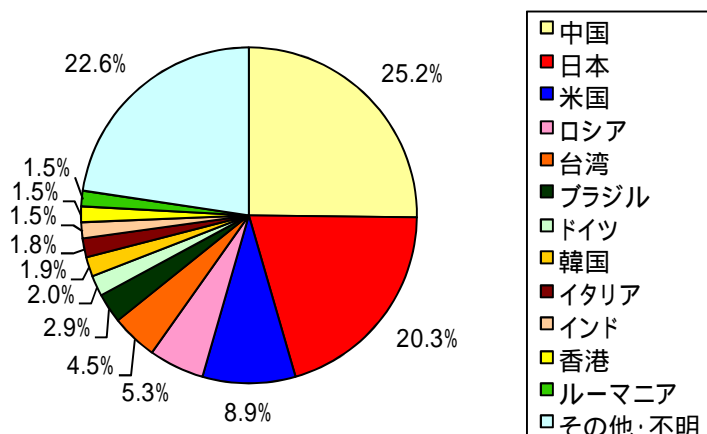


図 2-9 発信元国・地域別比率²

¹ 「SMBの脆弱性により、サービス拒否が起こる」(マイクロソフト社)
<http://www.microsoft.com/japan/technet/security/advisory/977544.mspx>

² 当データは、小数点第二位で四捨五入しているため、合計が100%にならないことがある。

表 2-2 発信元国・地域別検知件数

| 今期 順位 | 前期 順位 | 国・地域 | 今期件数 (一日・1IP 当たり) | 前期比 (一日・1IP 当たり) | 増加 順位 | 減少 順位 |
|----------|----------|-------|----------------------|---------------------|----------|----------|
| 1 位 | 1 位 | 中国 | 92.47 件 | + 2.8% (+ 2.53 件) | 1 位 | |
| 2 位 | 2 位 | 日本 | 74.71 件 | - 16.0% (- 14.20 件) | | 1 位 |
| 3 位 | 3 位 | 米国 | 32.77 件 | + 2.6% (+ 0.83 件) | 4 位 | |
| 4 位 | 4 位 | ロシア | 19.60 件 | + 6.3% (+ 1.16 件) | 3 位 | |
| 5 位 | 5 位 | 台湾 | 16.34 件 | - 4.8% (- 0.83 件) | | 4 位 |
| ... | | | ... | | | |
| 7 位 | 8 位 | ドイツ | 7.31 件 | - 8.2% (- 0.66 件) | | 5 位 |
| 8 位 | 7 位 | 韓国 | 6.90 件 | - 14.8% (- 1.20 件) | | 3 位 |
| ... | | | ... | | | |
| 13 位 | 15 位 | カナダ | 5.20 件 | + 16.9% (+ 0.75 件) | 5 位 | |
| ... | | | ... | | | |
| 17 位 | 26 位 | ベトナム | 3.53 件 | + 104.8% (+ 1.81 件) | 2 位 | |
| ... | | | ... | | | |
| 25 位 | 9 位 | フィリピン | 1.81 件 | - 74.7% (- 5.34 件) | | 2 位 |

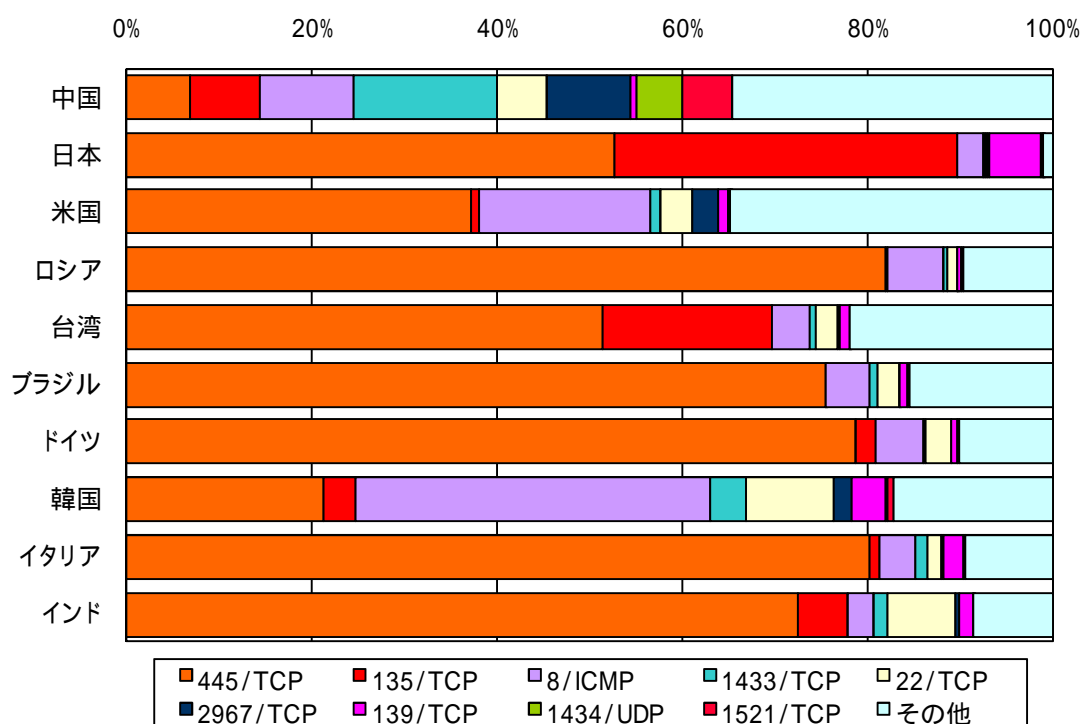


図 2-10 発信元国・地域別上位のポート別比率

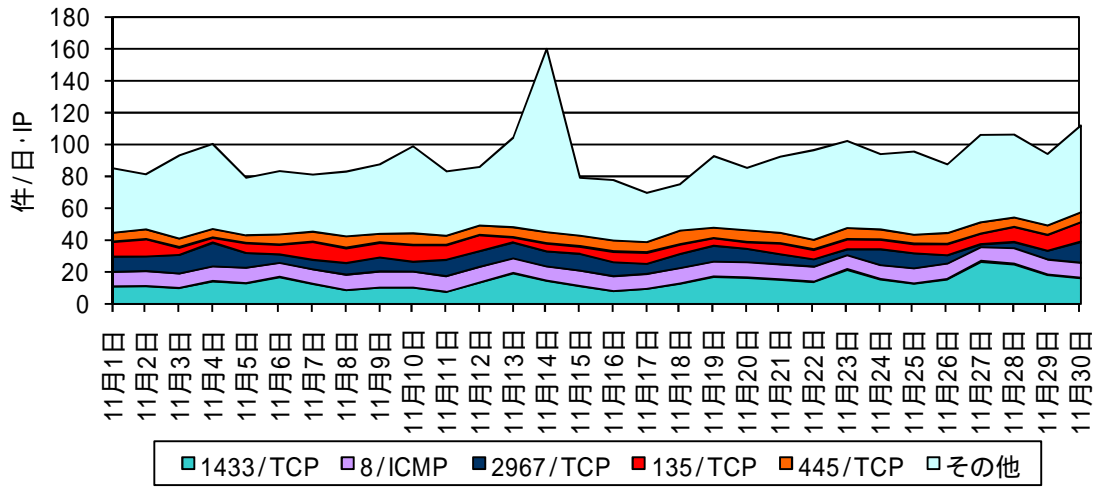


図 2-11 中国からのアクセスの推移

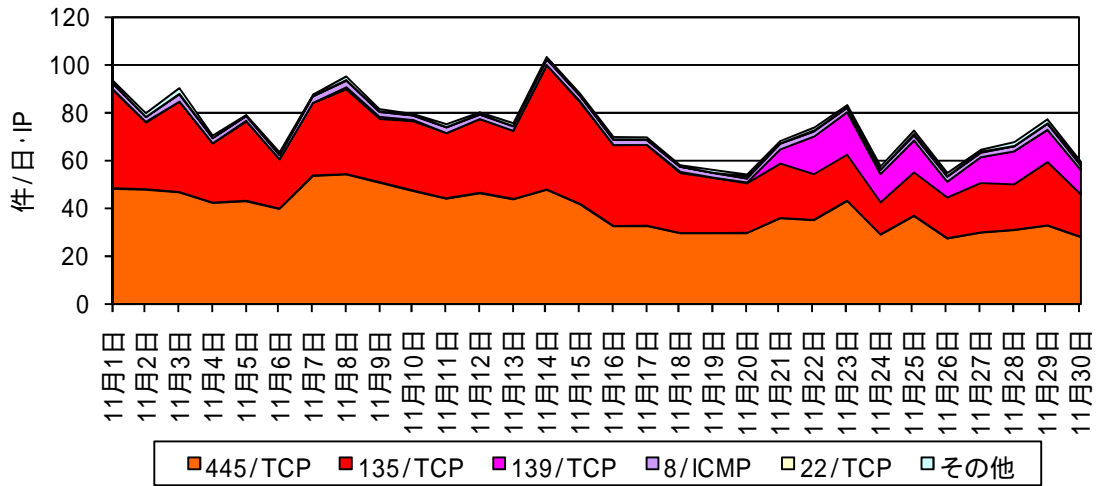


図 2-12 日本からのアクセスの推移

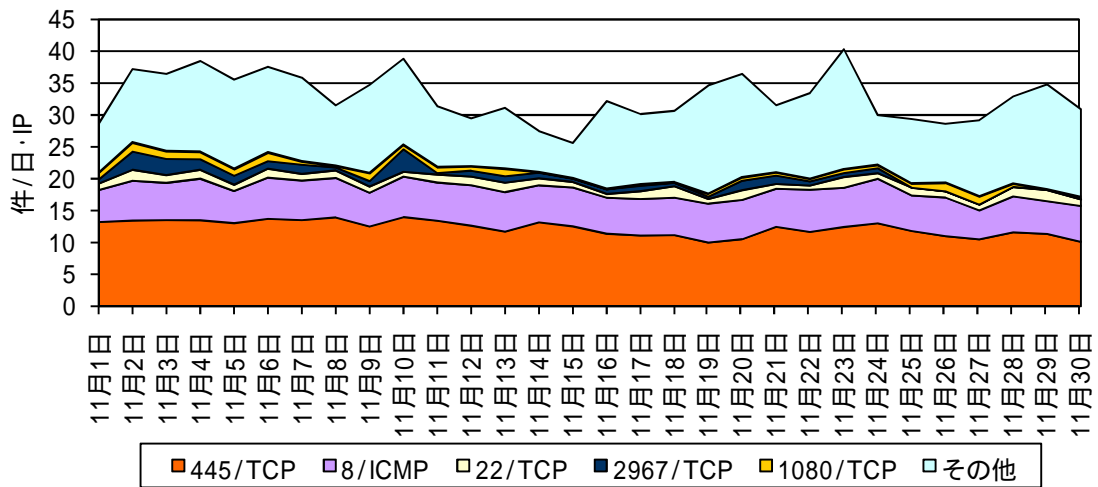


図 2-13 米国からのアクセスの推移

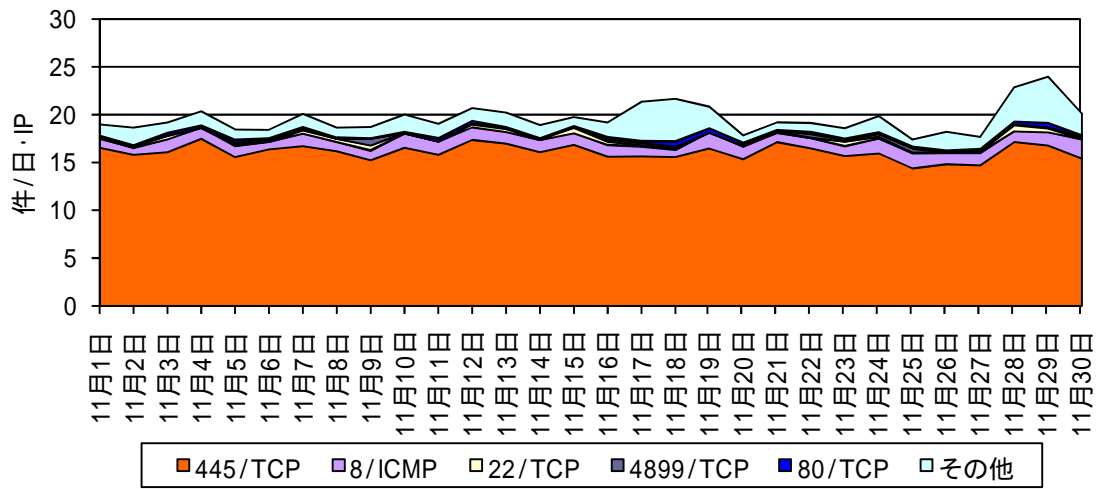


図 2-14 ロシアからのアクセスの推移

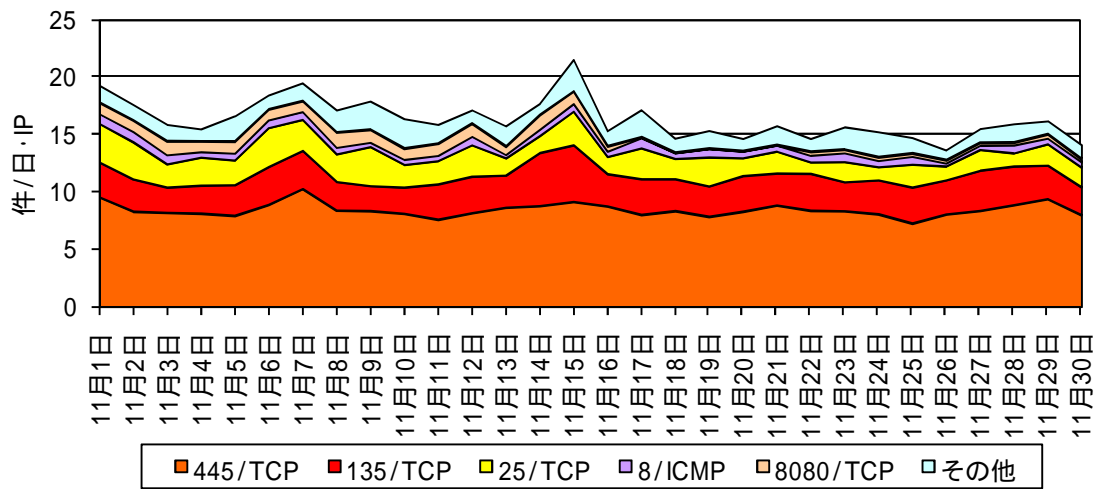


図 2-15 台湾からのアクセスの推移

3 インターネット定点観測 シグネチャを用いた不正侵入等の検知

今期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 11.7 件で、前期と比較して +0.8 件 (+7.1%) と横ばいであった。また、検知した発信元 IP アドレス数の 1 日当たりの平均は 354.1 個で、前期と比較して +38.7 個 (+12.3%) とやや増加した。

3-1 攻撃手法別

今期のシグネチャを用いた不正侵入等の検知件数は、攻撃手法別では Worm、Scan、DNS の順であり、Worm と Scan で約 9 割を占めている。(図 3-3)

シグネチャ分類の「Worm」の検知件数は、一日・1IP 当たり 6.9 件で、前期と比較して +0.7 件 (+11.0%) とやや増加した。(表 3-1) また、「Worm」を検知した発信元 IP アドレス数の 1 日当たりの平均は 259.4 個であり、前期と比較して +7.7 個 (+3.0%) とやや増加した。

「Worm」の検知件数と IP アドレス数を時間別に見ると、24 時間ほぼ一定数であり、人間の生活リズムの影響は見られない。このため、サーバなどの常時起動している機器が感染していると推測される。(図 3-2)

なお、「Worm」として検知したものの大部分は SQL Slammer 及び Nachi であった。

「Scan」の検知件数は、一日・1IP 当たり 4.0 件で、前期と比較して -0.3 件 (-6.9%) と横ばいであった。(表 3-1) また、「Scan」を検知した発信元 IP アドレス数の 1 日当たりの平均は 36.6 個であり、前期と比較して +2.1 個 (+6.1%) と横ばいであった。

11 月 24 日に、インターネット電話などで用いられるプロトコルである SIP (図 3-1 では「その他」に分類される。)を検知した。これは、通常の通信では使用されないパケットであり、特定のネットワークの複数のコンピュータから、不特定多数の IP 電話機に無差別に発信を行っていた可能性がある。(図 3-1)

表 3-1 シグネチャを用いた不正侵入等の攻撃手法別検知件数

| 今期 順位 | 前期 順位 | 攻撃手法 | 今期 件数 | 前期比 | 今期 増加順位 | 今期 減少順位 |
|----------|----------|------|----------|------------------|------------|------------|
| 1 位 | 1 位 | Worm | 6.88 件 | +11.0% (+0.68 件) | 1 位 | |
| 2 位 | 2 位 | Scan | 3.98 件 | -6.9% (-0.30 件) | | 1 位 |
| 3 位 | 3 位 | DNS | 0.05 件 | -4.5% (-0.00 件) | | 2 位 |

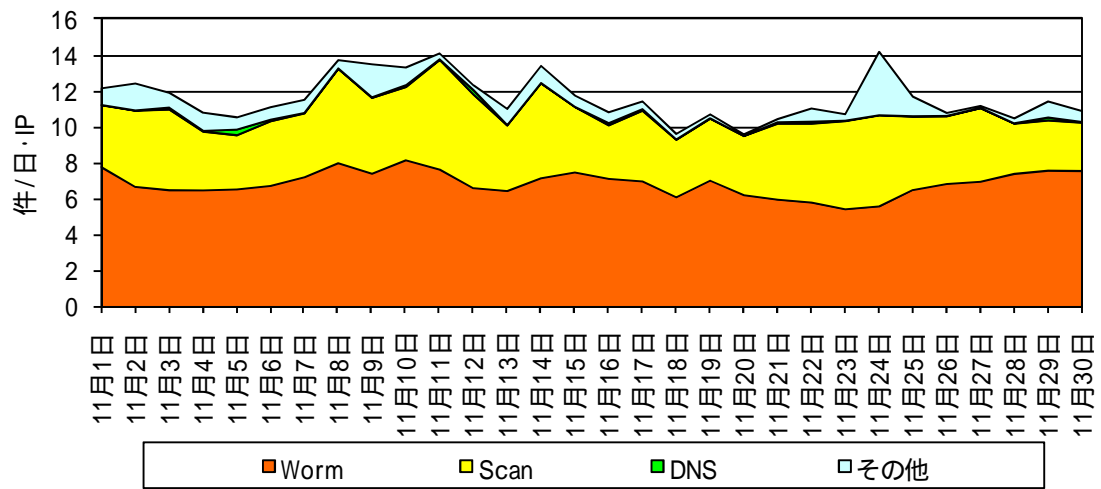


図 3-1 シグネチャを用いた不正侵入等の攻撃手法別検知推移

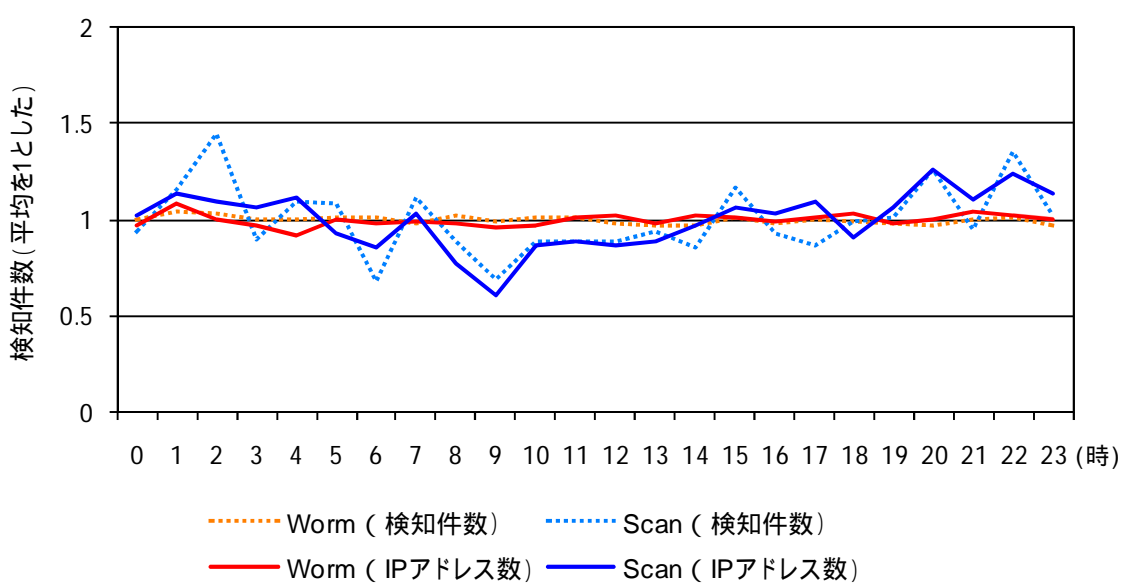


図 3-2 Worm 及び Scan の時間帯別検知件数

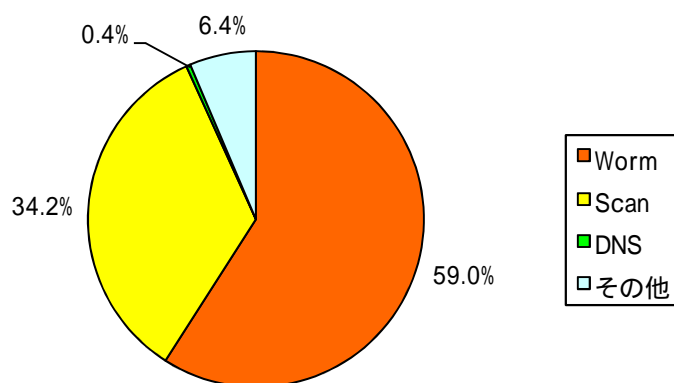


図 3-3 シグネチャを用いた不正侵入等の攻撃手法別検知比率¹

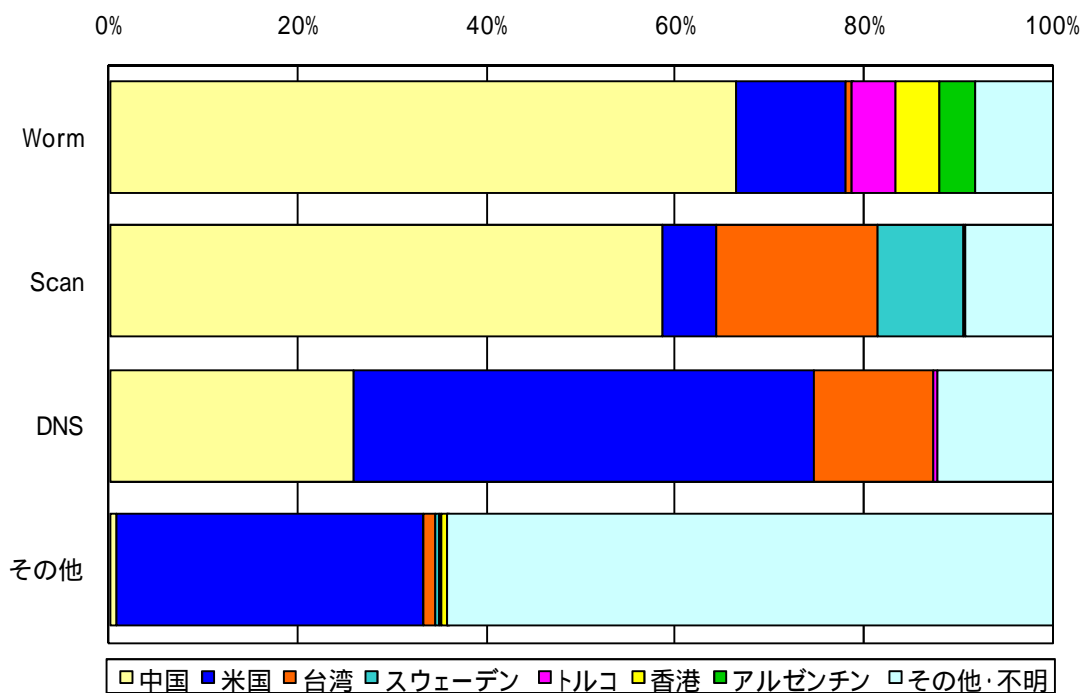


図 3-4 シグネチャを用いた不正侵入等の攻撃手法の国・地域別比率

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

3-2 発信元国・地域別

中国を発信元とする SQL Slammer ワームの検知状況は、一日・1IP 当たり 4.6 件で、前期と比較して +0.6 件 (+15.1%) とやや増加した。SQL Slammer ワームは、複数の発信元から継続的に検知しており、管理が不十分なサーバが依然として多数中国に存在すると考えられる。

台湾を発信元とする検知件数は、一日・1IP 当たり 0.7 件で、前期と比較して -0.6 件 (-46.8%) と減少した。これは、9月26日から検知していたプロキシサーバへのスキャンが、11月17日に一度停止したためである。このスキャンは、複数のコンピュータを使用していると思われる、11月22日以降に規模を縮小してスキャンを再開している。

前期と同様に、トルコの特定の IP アドレスを発信元とする SQL Slammer ワームを継続して検知している。

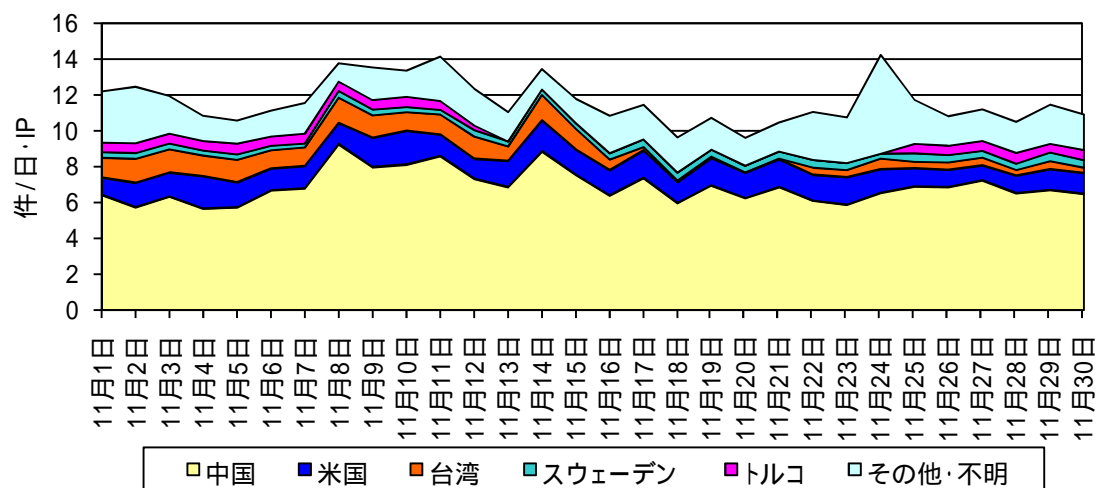


図 3-5 シグネチャを用いた不正侵入等の発信元国・地域別検知推移

表 3-2 シグネチャを用いた不正侵入等の発信元国・地域別検知件数

| 今期 順位 | 前期 順位 | 国/地域 | 今期 件数 | 前期比 | 今期 増加順位 | 今期 減少順位 |
|----------|----------|---------|----------|-------------------------|------------|------------|
| 1位 | 1位 | 中国 | 6.91件 | +13.4% (+0.82件) | 1位 | |
| 2位 | 3位 | 米国 | 1.30件 | +11.7% (+0.14件) | 4位 | |
| 3位 | 2位 | 台湾 | 0.74件 | -44.9% (-0.60件) | | 1位 |
| 4位 | 5位 | スウェーデン | 0.37件 | +15.2% (+0.05件) | | |
| 5位 | 4位 | トルコ | 0.32件 | -20.5% (-0.08件) | | 2位 |
| ... | | | ... | | | |
| 7位 | 9位 | アルゼンチン | 0.27件 | +159.1% (+0.17件) | 3位 | |
| 8位 | 38位 | オランダ | 0.21件 | - ¹ (+0.20件) | 2位 | |
| 9位 | 7位 | 日本 | 0.19件 | -18.8% (-0.04件) | | 3位 |
| ... | | | ... | | | |
| 16位 | 59位 | ベトナム | 0.05件 | - ¹ (+0.05件) | 5位 | |
| ... | | | ... | | | |
| 35位 | 21位 | ポーランド | 0.01件 | -54.6% (-0.01件) | | 5位 |
| ... | | | ... | | | |
| 64位 | 18位 | ルクセンブルク | 0.00件 | -95.4% (-0.02件) | | 4位 |

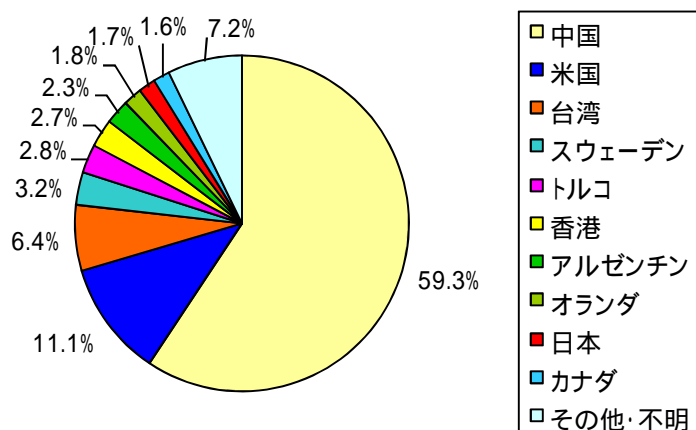


図 3-6 シグネチャを用いた不正侵入等の発信元国・地域別検知比率²

¹ 前期の検知件数が少なかったため、前期比率は記載していない。

² 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

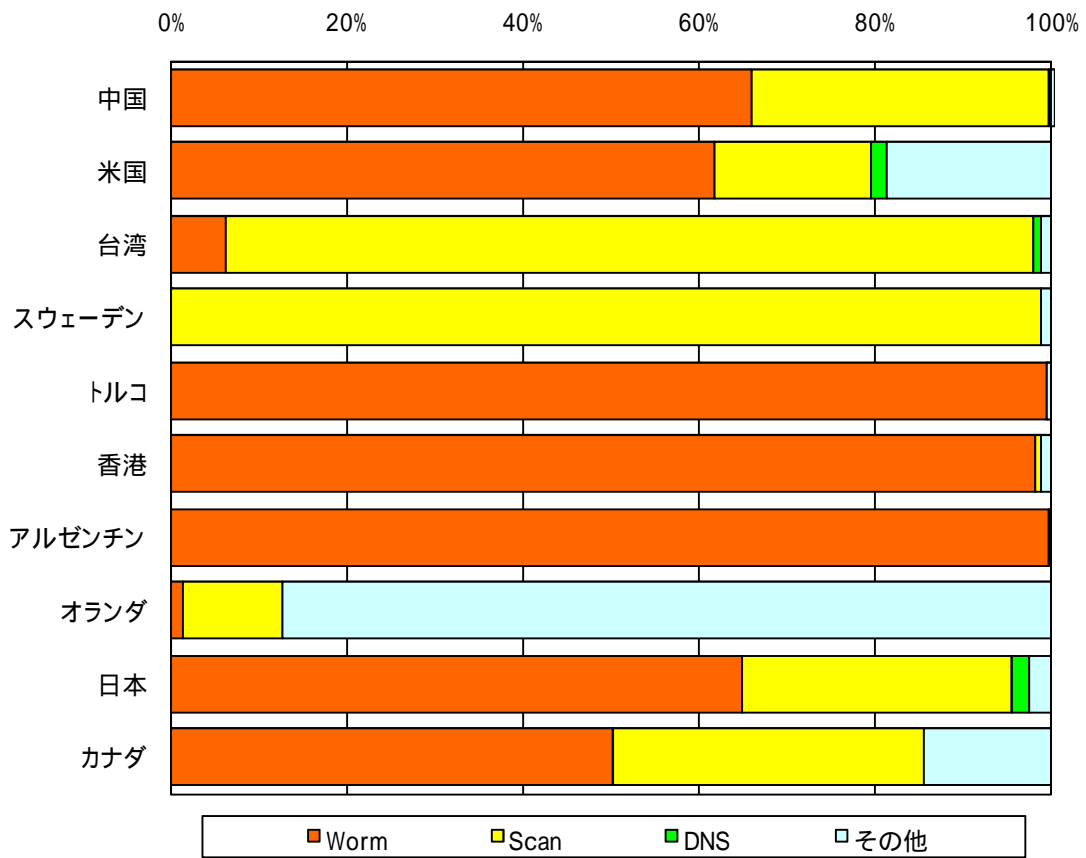


図 3-7 シグネチャを用いた不正侵入等の発信元国・地域別上位のシグネチャ別比率

4 @police (Topics)掲載事項

@police において、11月期に掲載した主なものは、次のとおりである。

| 分類 | 掲 載 事 項 |
|----|---|
| 重要 | マイクロソフト社のセキュリティ修正プログラムについて (MS09-045,046,047,048,049)(11/11)更新 |
| 重要 | マイクロソフト社のセキュリティ修正プログラムについて (MS09-063,064,065,066,067,068)(11/11) |
| ● | インターネット治安情勢更新(平成 21 年度第 2 四半期報を追加)(11/18) |

5 集計方法

5-1 センサーに対するアクセス

TCP 及び UDP はポートごとに集計し、以下ではスラッシュの前にポート番号を付けて表す。(例 135/TCP は TCP の 135 番ポートを表す。) ICMP パケットについては、タイプごとに集計し、以下ではスラッシュの前にタイプ番号を付けて表す。(例 8/ICMP は ICMP Echo Request を表す。)

5-2 シグネチャを用いた不正侵入等の検知

各センサーの不正侵入検知装置には、平成 21 年 11 月 30 日現在、シグネチャは 2,992 種類が登録されている。検知された各シグネチャは、表 5-1 に示す分類に従って集計している。

また、シグネチャを用いた不正侵入等の検知を行うセンサーには、サーバ等の攻撃対象となる可能性のある機器を一切接続していない。そのため、セッションの確立を必要としない、UDP を利用する Worm や Scan 系の検知が、大きな割合を占めている。

表 5-1 グラフに表示される分類と代表的なシグネチャ

| 分類 | 代表的なシグネチャ |
|----------|---|
| Worm | SQL Slammer, Nachi, Dabber |
| Scan | Sweep of a subnet for active hosts, Proxy port probe, Port scan, TCP ACK ping |
| UDP spam | MSRPC Popup Message |
| DoS | Smurf denial of service, ICMP Echo Reply without Echo |
| DNS | DNS request made for all records, DNS port probe, RR denial of service |
| Others | Traceroute, ISAKMP Vendor ID, SIP message detected |