

平成 21 年 4 月 28 日

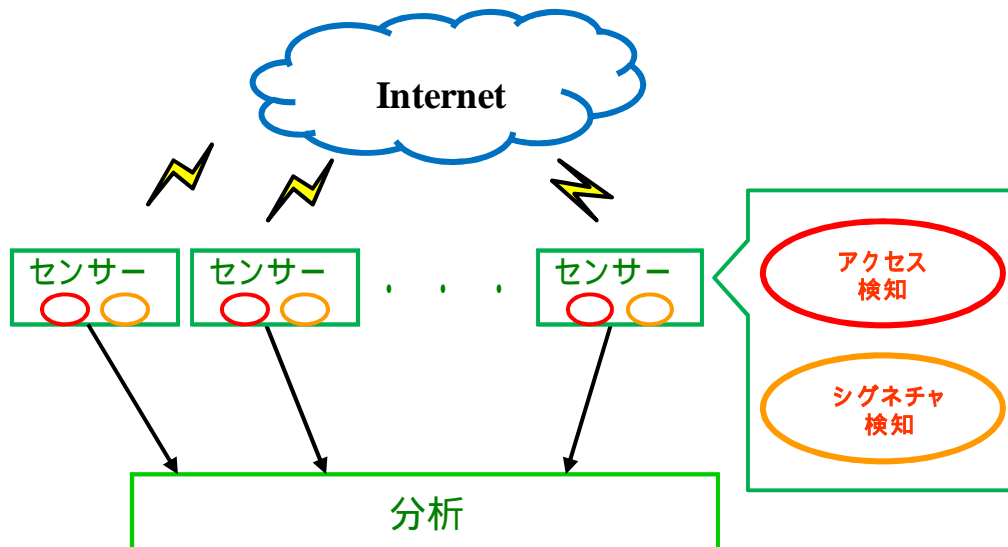
我が国におけるインターネット治安情勢

(平成 21 年 3 月期)

- ・平成 21 年 3 月から新システムによる観測開始
- ・センサーに対する総アクセス件数はやや減少
～ 445/TCP に対するアクセスが一時的に減少～
- ・シグネチャを用いた不正侵入等の検知状況
～ 中国からのアクセスが大半を占める～

1 警察庁のインターネット定点観測

警察庁サイバーフォースセンター(CFC)では、インターネット定点観測システムを更新し、平成 21 年 3 月から、新システムの運用を開始している。新システムでは、旧システムと同様に、全国の警察施設のインターネット接続点にセンサーを設置し、インターネット上の通信状況を観測している。



新しいセンサーは、以下の 2 点を重点的に観測している。

インターネットからセンサーへのアクセス

(旧システムでのファイアウォールによる集計に相当)

シグネチャを用いた不正侵入等の検知

(旧システムでの不正侵入検知システムによる集計に相当)

あらかじめ登録しておいた攻撃や侵入の挙動パターン

シグネチャ数については、大幅に増加し、より詳細な観測が可能となった。平成 21 年 3 月 31 日現在、シグネチャは 2,809 種類登録されており、随時更新している。代表的なシグネチャと分類については、以下に示すとおりである。

代表的なシグネチャと分類(新システム)

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

旧システム同様に、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、UDP を利用している UDP spam や Worm 系の検知が、大きな割合を占めている。

本レポートでは、インターネットからセンサーへのアクセスについては、センサーに到達するパケットを集計している。ICMP パケットについては、タイプごとに集計し、以下スラッシュの前にタイプを付けて表す。(例 8/ICMP は Echo Request を表す。)

2 概説

今期におけるセンサーに対するアクセス件数は、一日・1IP 当たり 390.2 件で、前期と比較して - 11.2 件 (- 2.8%) 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 2967/TCP の順であった。

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。前期と比較して、台湾及び韓国の 445/TCP に対するアクセスが減少した影響で、前期 6 位のロシアが今期 4 位となった。

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 29.5 件であった。

攻撃手法別では、UDP spam、Worm、Scan、DNS 及び DoS の順であった。攻撃手法別の上位 3 位までで大半を占めている。

発信元国 / 地域別において、上位 5 国は中国、米国、韓国、台湾及び日本の順であった。中国が全体の 84.9% と高い割合を占めている。

3 インターネット定点観測

3.1 センサーに対するアクセス

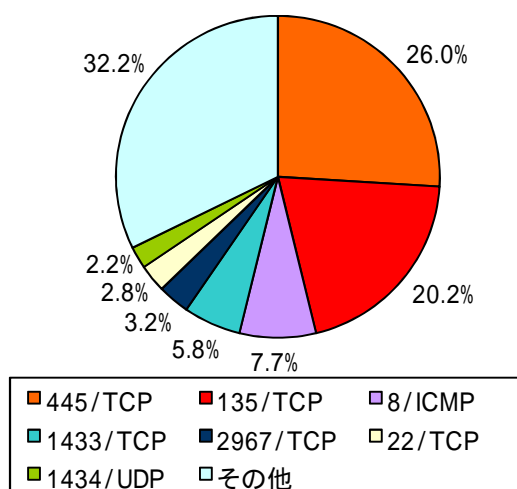
(1) 宛先ポート別概要

今期における上位5ポートは以下のとおりである。前期と比較して、445/TCP に対するアクセスがやや減少し、2967/TCP に対するアクセスが減少に転じた。

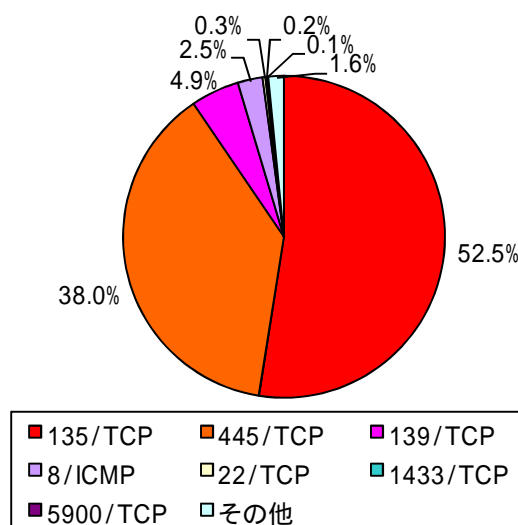
今期順位	ポート	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)
1位	445/TCP	101.33 件	- 10.4% (- 11.77 件)
2位	135/TCP	78.85 件	- 15.0% (- 13.92 件)
3位	8/ICMP	29.92 件	- 6.7% (- 2.15 件)
4位	1433/TCP	22.54 件	+ 6.0% (+ 1.27 件)
5位	2967/TCP	12.34 件	- 21.2% (- 3.32 件)

(2) 宛先ポート別比率

発信元/全世界



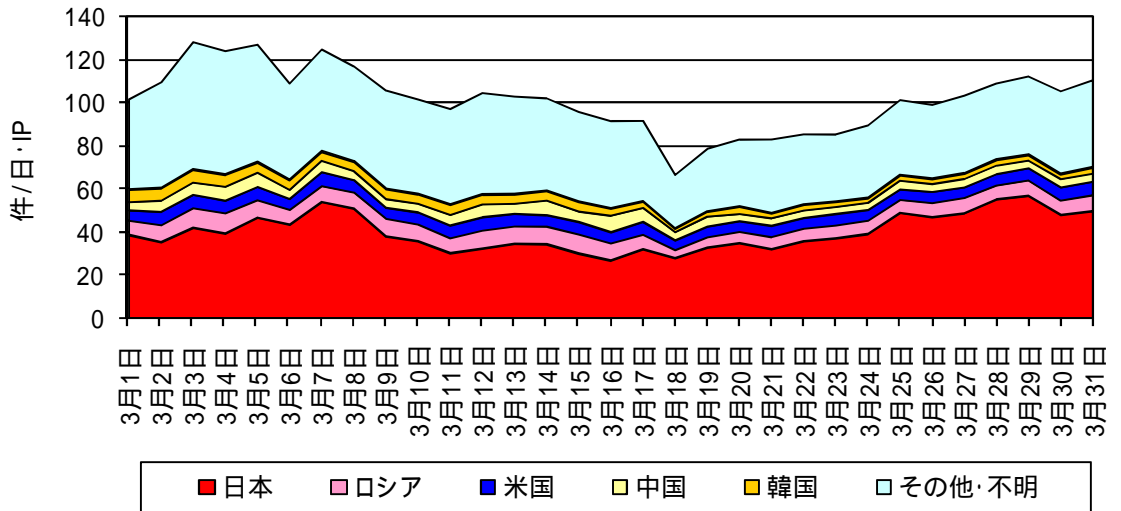
発信元/日本



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) 宛先ポート別推移(上位5ポート)

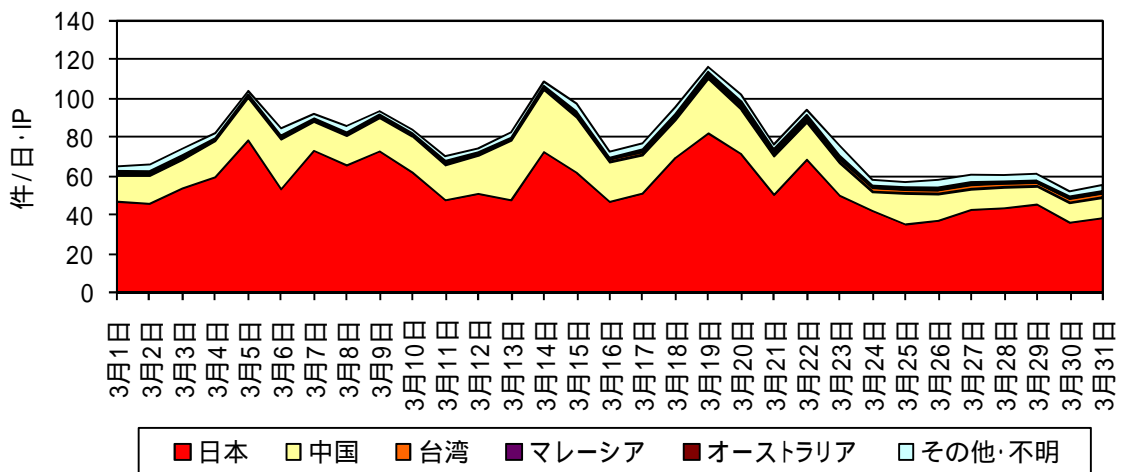
445/TCP



前期と比較して、日本国内からのアクセスは増加したものの、今期中旬に大部分の国からのアクセスが一時的に減少した影響で、全体としてやや減少となった。

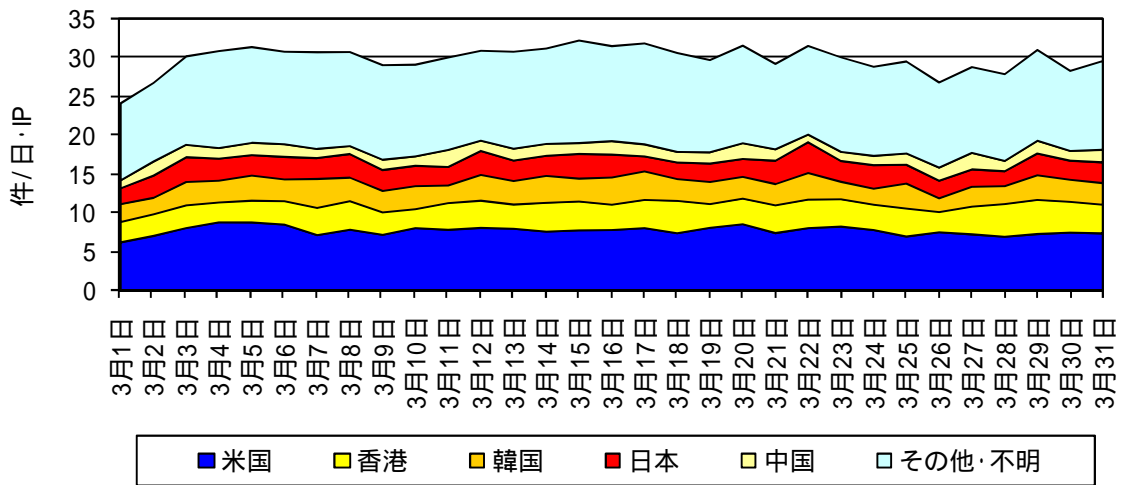
このポートは、Microsoft Windows 製品の Server サービスで使用されているもので、脆弱性 (MS08-067) を悪用した攻撃の可能性がある。

135/TCP



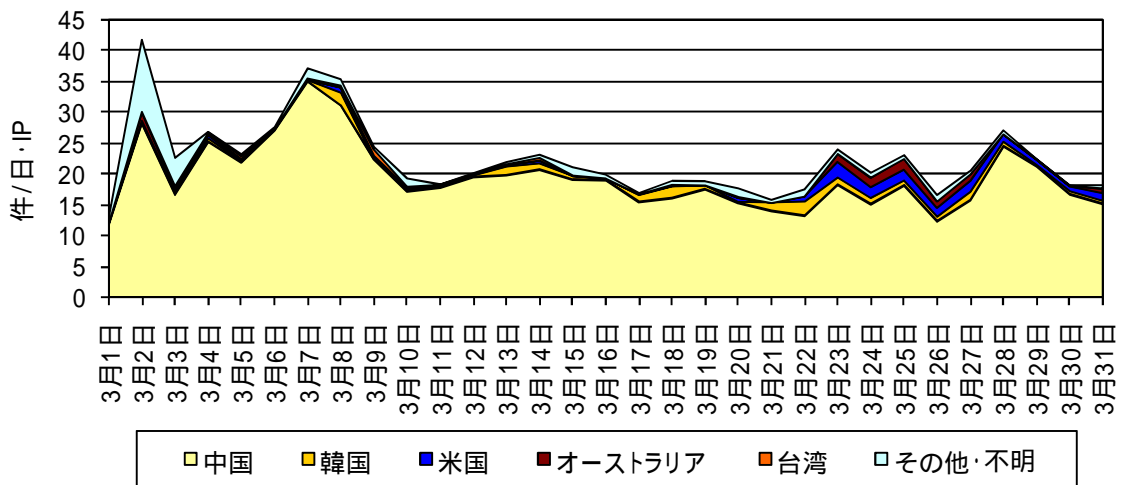
前期後半からの減少傾向が今期も見られ、全体としてやや減少となった。

8/ICMP



今期は、全体として横ばいで推移した。

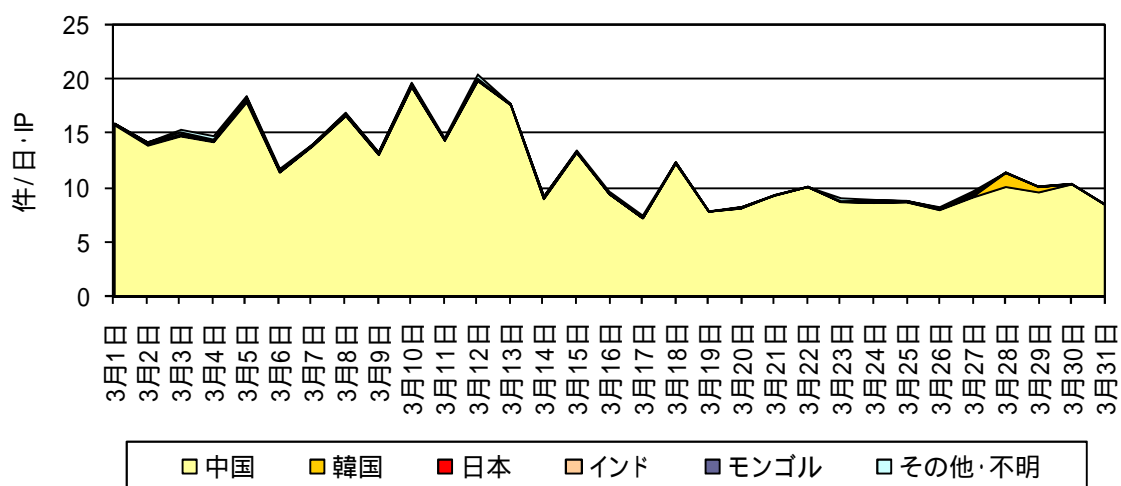
1433/TCP



大半を占める中国からのアクセス件数が横ばいであったため、全体としても横ばいで推移した。

1433/TCP は、Microsoft SQL Server が使用するポートであり、この製品の脆弱性を悪用した攻撃の可能性がある。

2967/TCP



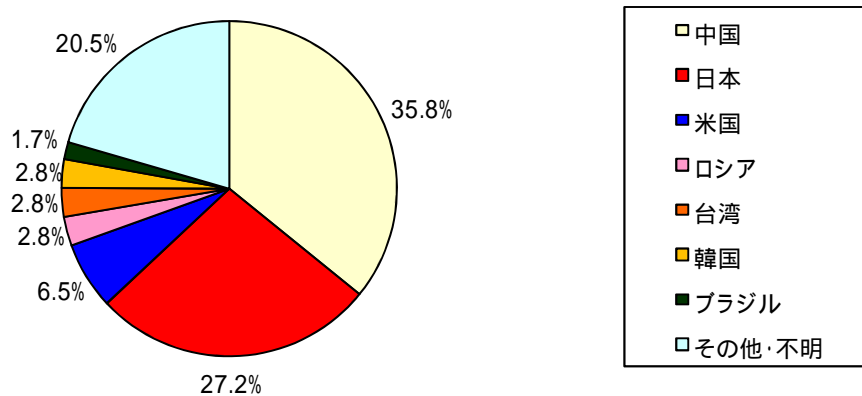
大半を占める中国からのアクセスが、3月14日頃から減少したことから、全体としても減少した。

(5) 発信元国 / 地域別概要

今期における上位5位までの発信元国 / 地域は以下のとおりである。前期4位の韓国が今期は6位となった。これは、445/TCP に対するアクセスが減少した影響である。

今期順位	国/地域	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)
1位	中国	139.84 件	- 2.3% (- 3.31 件)
2位	日本	106.07 件	+ 0.7% (+ 0.76 件)
3位	米国	25.24 件	+ 4.6% (+ 1.12 件)
4位	ロシア	10.95 件	+ 1.3% (+ 0.14 件)
5位	台湾	10.48 件	- 14.3% (- 1.81 件)

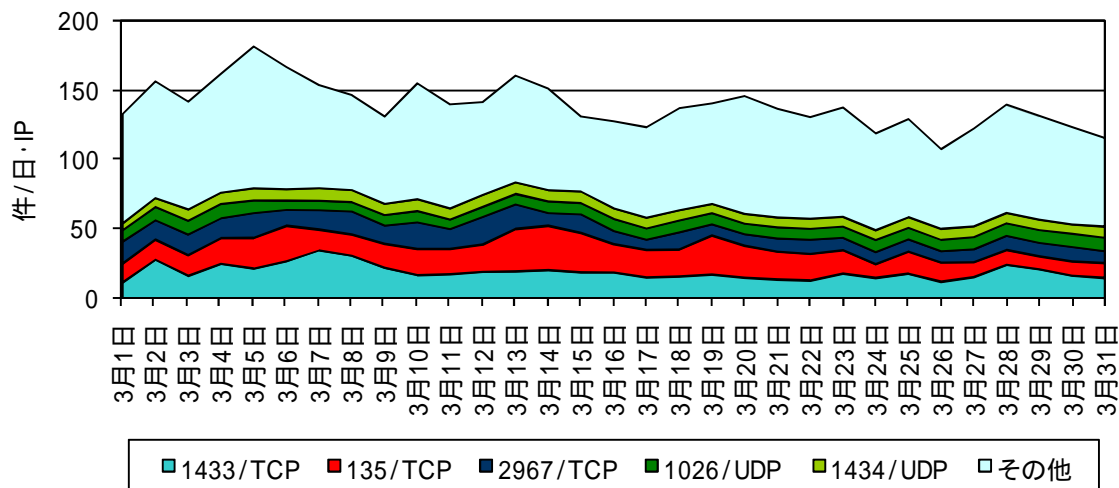
(6) 発信元国 / 地域別比率



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。

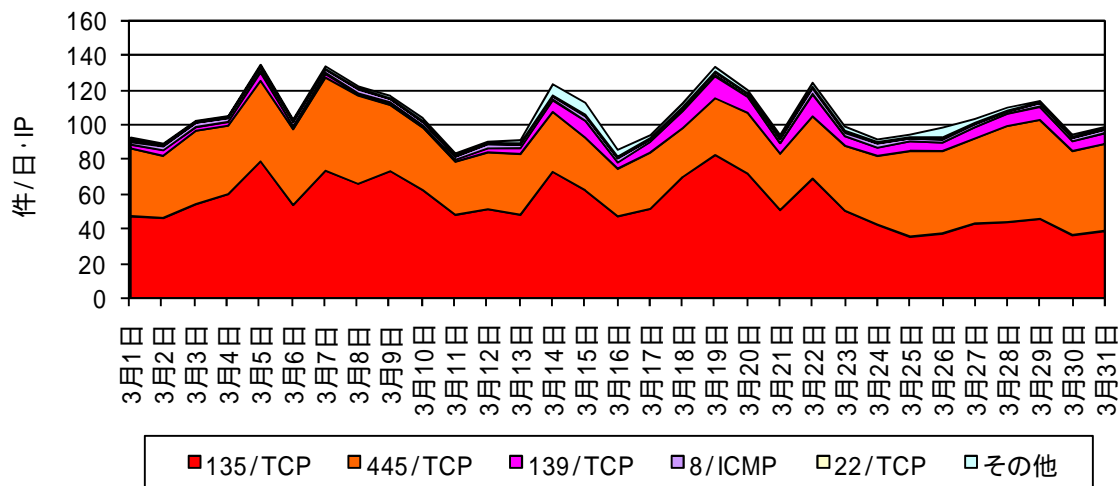
(7) 発信元国 / 地域別推移(上位 5 か国)

中国



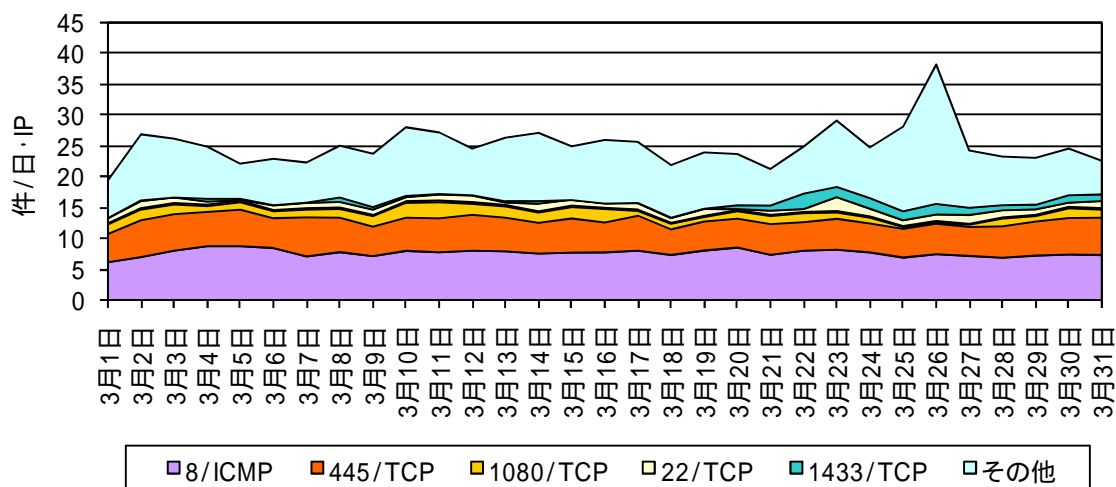
全体としては横ばいで推移した。1433/TCP 及び 2967/TCP に対するアクセスは、その大半が中国からのものである。

日本



前期後半からの減少傾向が続いている 135/TCP に対するアクセスは減少したが、445/TCP に対するアクセスが増加したため、全体としては横ばいとなった。

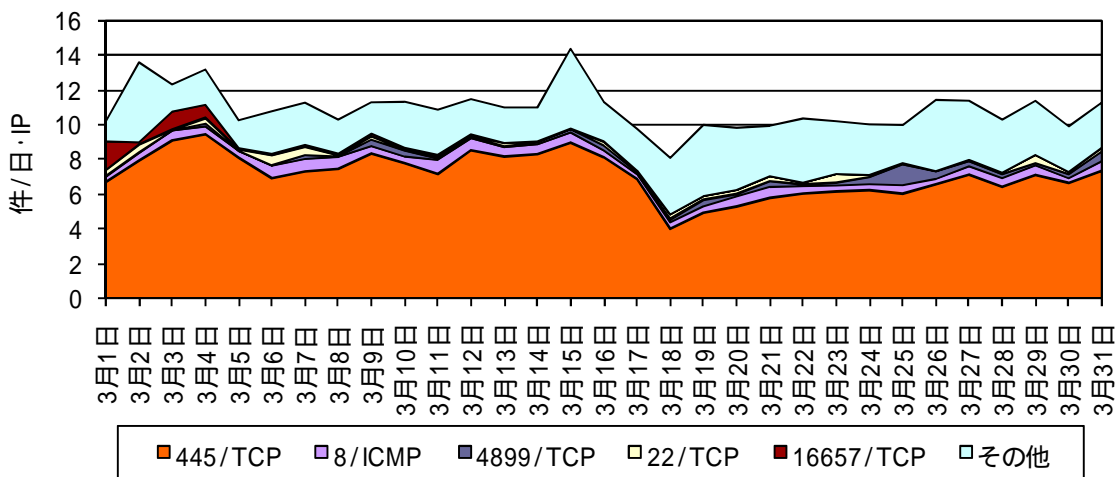
米国



米国からのアクセスは、全体として横ばいであった。

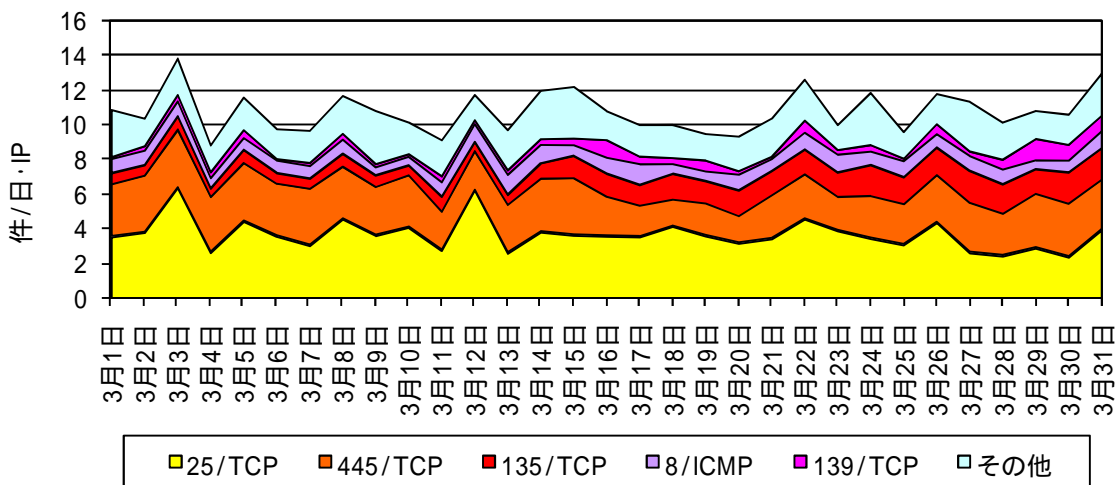
26日の「その他」に分類されているアクセス増加は、複数のポートに対する散発的なアクセスによるものである。

ロシア

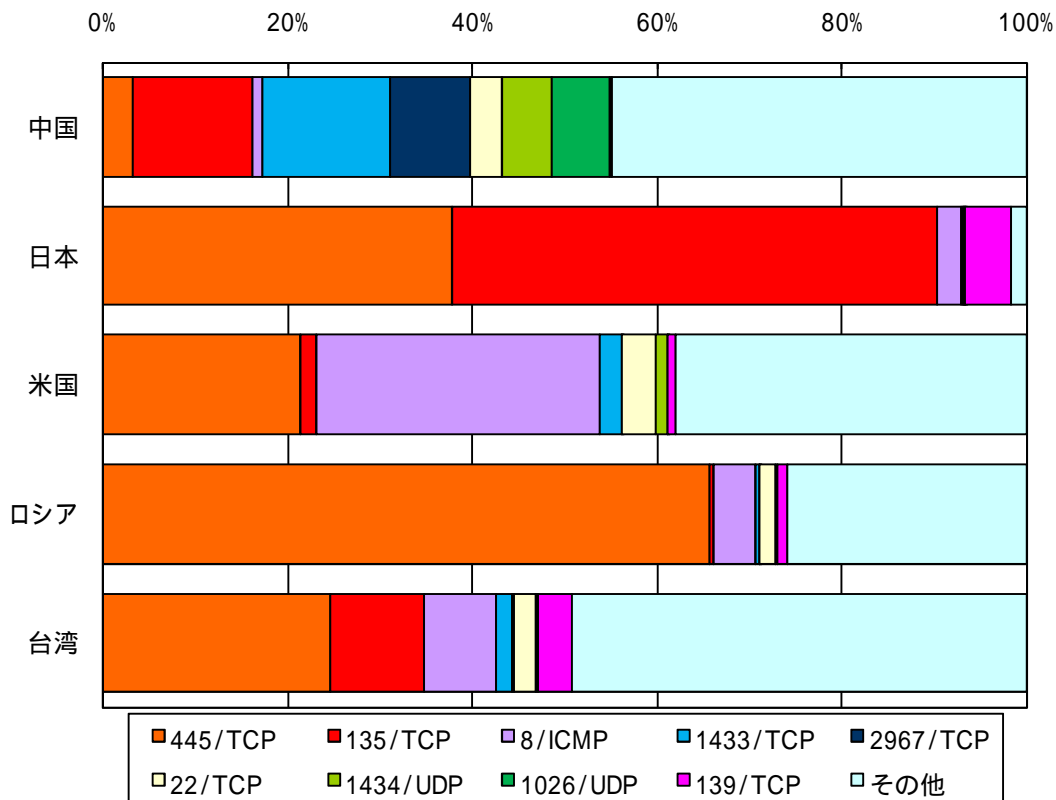


全体としては横ばいで推移した。445/TCP に対するアクセスは、3月中旬に一時的に減少したが、その後は増加傾向となった。この445/TCP に対するアクセスが3月中旬に一時的に減少する傾向は、多くの国で確認できる。

台湾

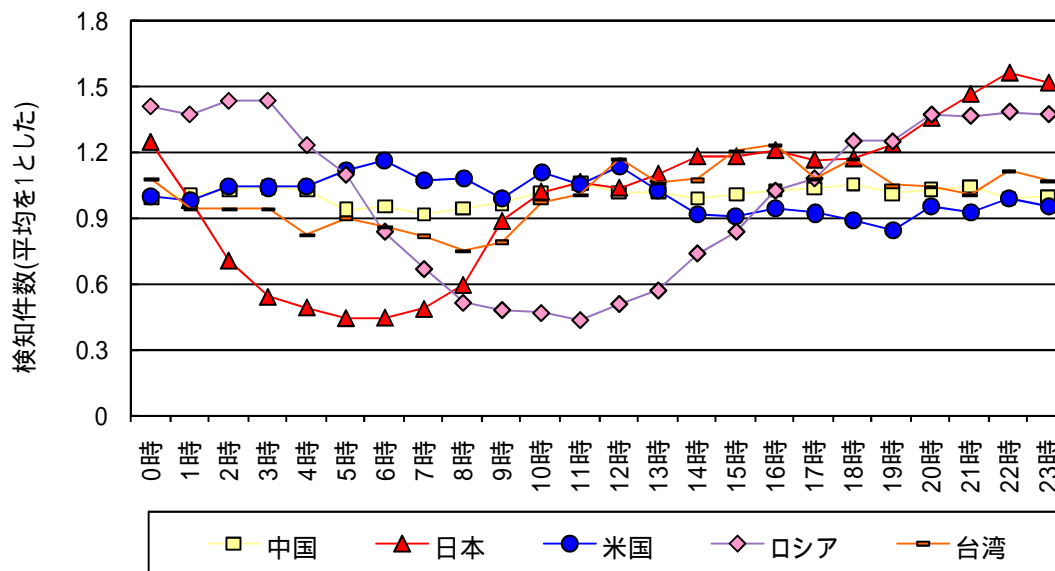


(8) 上位国/地域の宛先ポート別比率

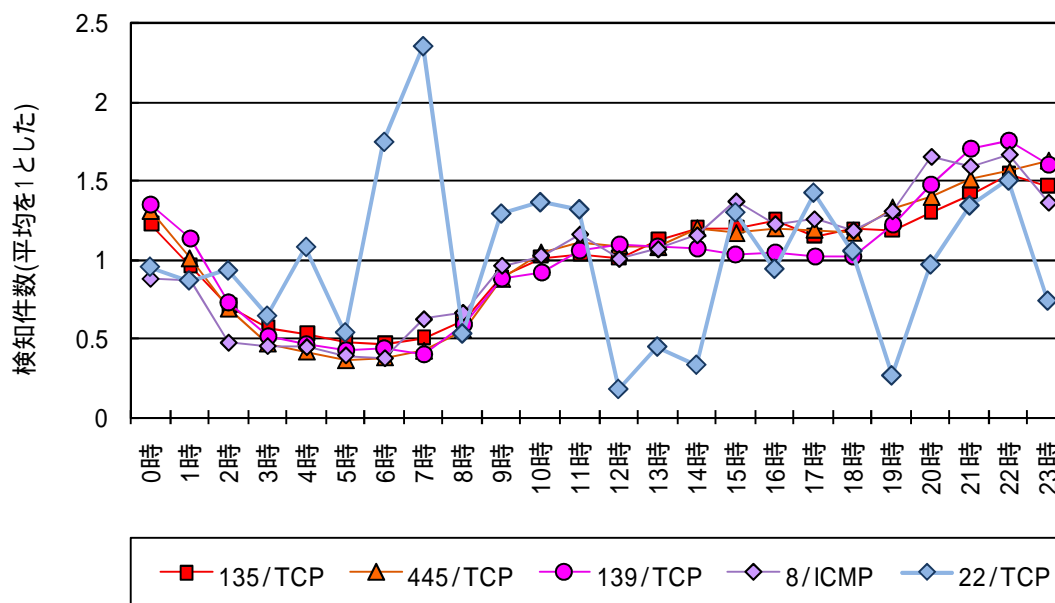


(9) 時間帯推移

上位5 各国



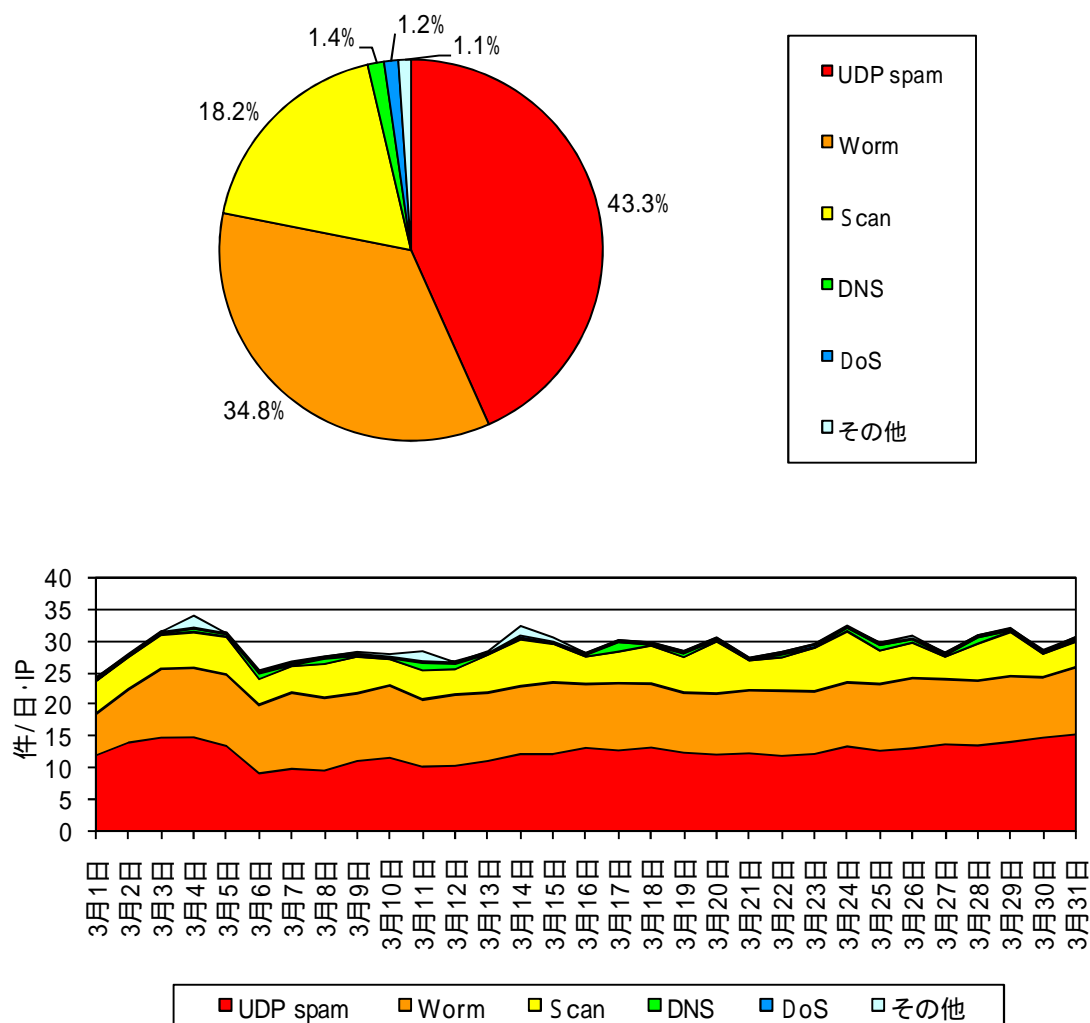
上位5 ポート(国内)



3.2 シグネチャを用いた不正侵入等の検知

平成 21 年 3 月より新システムによる観測を開始しており、シグネチャ数が大幅に増加し、より詳細な観測が可能になっている。

(1) 攻撃手法別

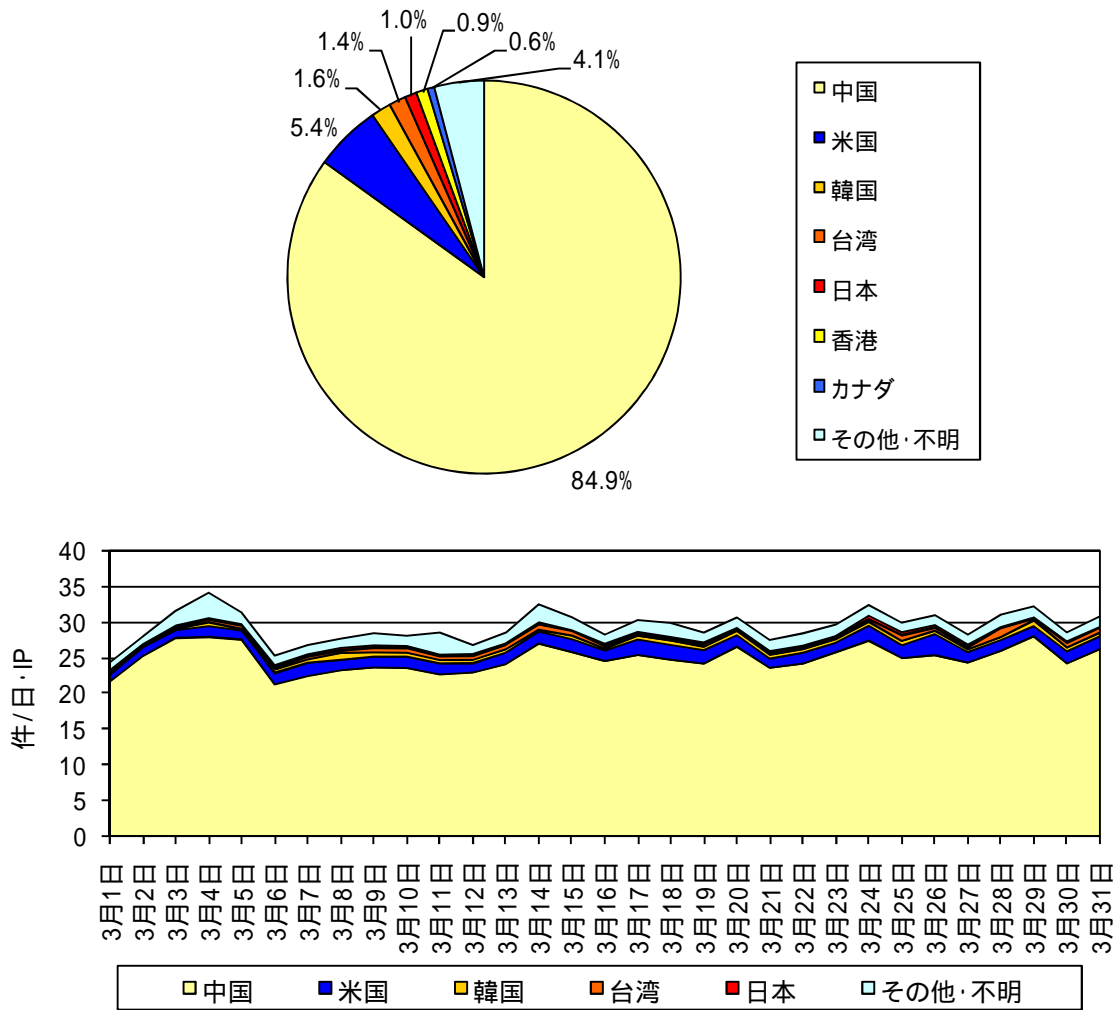


3 月期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 29.5 件であった。

攻撃手法別では、UDP spam、Worm、Scan、DNS 及び DoS の順であった。攻撃手法別の上位 3 位までが大半を占めており、それぞれ一日・1IP 当たり 12.8 件、10.3 件及び 5.4 件であった。

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。

(2) 発信元国 / 地域別

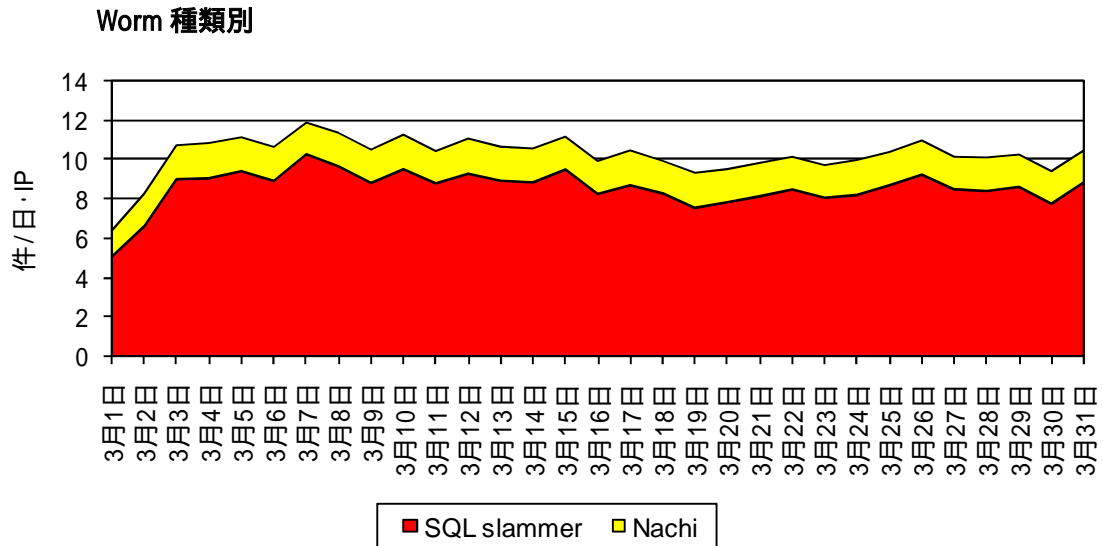


発信元(国/地域)別の上位5か国までの傾向は、中国、米国、韓国、台湾及び日本の順であった。中国を発信元とする攻撃手法別の検知状況は、UDP spam、Worm がそれぞれ 50.1%、30.5%を占め、米国を発信元とする攻撃手法別の検知状況は、Worm が72.7%を占めている。3月期においては、特異な変動は見られなかった。

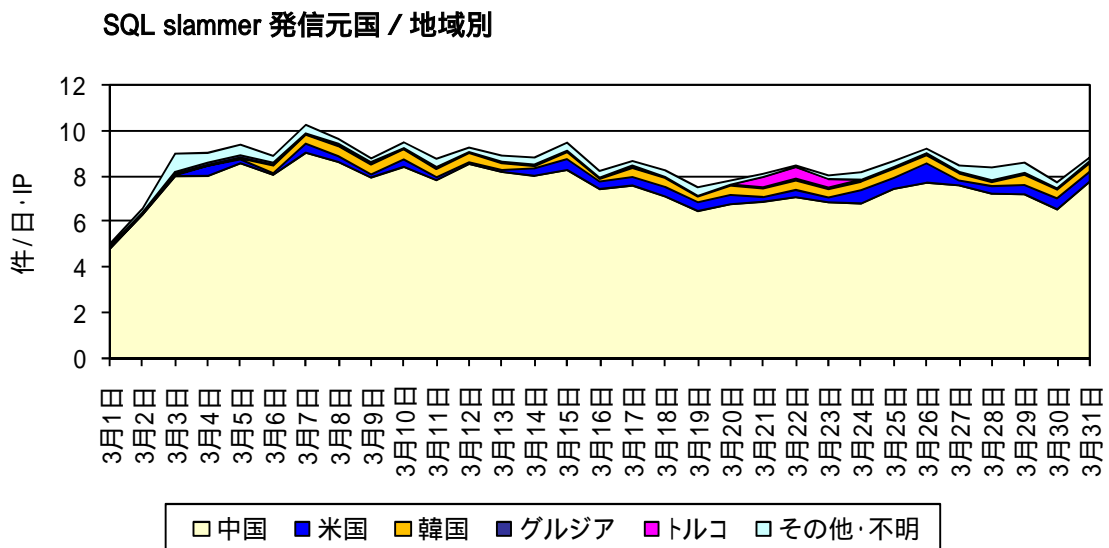
当データは、小数点第二位で四捨五入しているため、合計が100%にならないことがある。

(3) Worm の検知状況

新システムによる観測においても攻撃手法別では、Worm が大部分を占めている。Worm の検知件数は、依然として高い水準で検知しており、インターネットの脅威として活発な状況である。そこで、今期の Worm 検知状況について調査を行った。

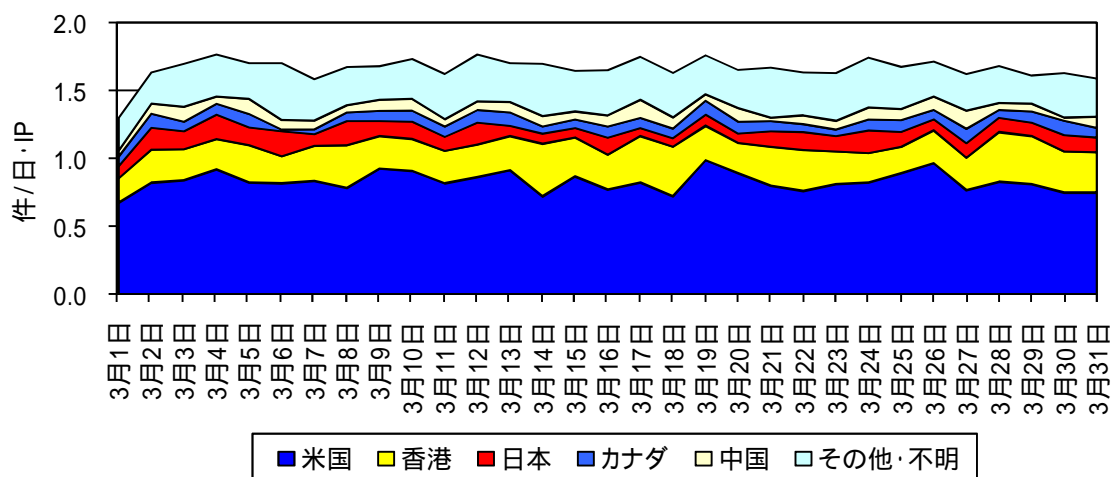


3月期のシグネチャを用いた不正侵入等の検知におけるWormの検知件数は、一日・1IP当たり10.27件であった。検知したWormの種類については、SQL slammer、Nachiの2種類を検知しており、それぞれ一日・1IP当たり8.59件、1.67件となっている。



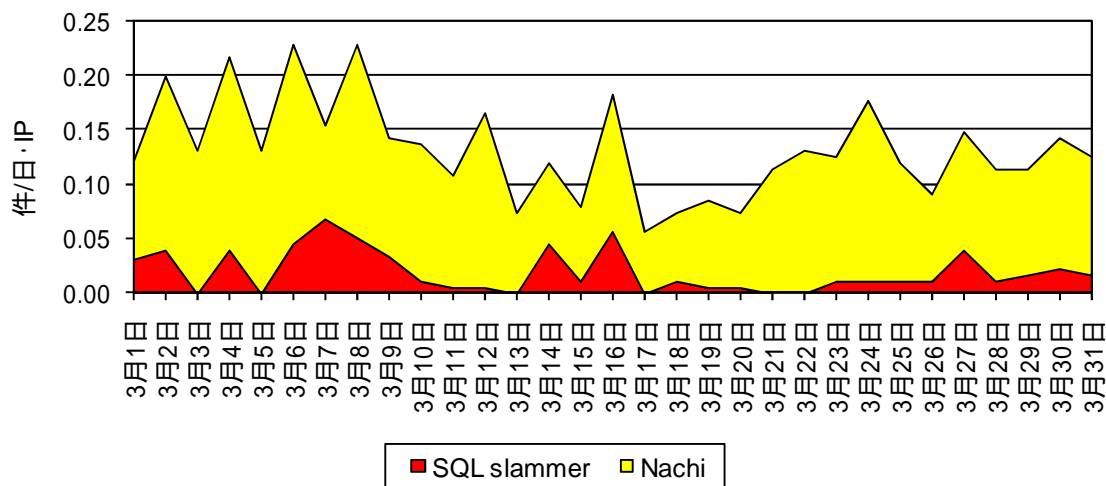
SQL slammerの発信元(国/地域)別の傾向は、中国が大半(88.0%)を占めている。旧システムで観測していた2月期においても、中国が大半を占めていた。

Nachi 発信元国 / 地域別



Nachi 発信元の発信元(国/地域)別の傾向は、米国、香港及び日本で多くを占めており、それぞれ 50.2%、16.1%及び 6.8%であった。3 月期の期間においては特異な変動は見られなかった。Nachi は、2003 年に猛威をふるった Welchia ワームの亜種であり、全体の検知に占める Nachi の検知件数は、少ない。

Worm 種類別(日本国内)



日本国内を発信元とする Worm 種類別の検知件数は、一日・1IP 当たり 0.13 件であった。検知した Worm の種類については、SQL slammer、Nachi の 2 種類を検知しており、それぞれ一日・1IP 当たり 0.02 件、0.11 件であった。

全世界からの検知状況と異なり、日本国内を発信元とする SQL slammer は比較的少ない。

Worm 等の脅威対策

警察庁の定点観測システムでの Worm の検知は、SQL slammer、Nachi の 2 種類を検知しているが、これは定点観測システムのネットワークには、サーバ等の攻撃対象となる可能性のある機器が一切接続されていないため、UDP を利用するネットワーク型 Worm のみ検知しているためである。2 種類以外にも、多数の Worm がインターネット上には存在しておりインターネットの脅威となっている。

今期に検知した 2 種類の Worm は、2003 年に確認されているものであるが、依然として高い水準で検知している状況であり、インターネットの脅威として活発な状況である。この理由としてこれらの Worm は感染速度が速いことに加え、セキュリティパッチを適用していないコンピュータが未だに多く存在することが考えられる。

このことから、インターネットに接続するコンピュータには Worm 等の脅威に対応できるように以下のような措置を講じることが重要である。

- OS やアプリケーションの更新プログラムを適切に運用する
- ウイルス対策ソフトを適切に運用する
- ファイアウォールソフトを適切に運用する
- メール の 添付ファイルやメール中のリンク先を不用意に閲覧しない

4 @police (Topics) 掲載事項

@police において3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
●	インターネット治安情勢更新(平成 21 年 2 月報を追加)(3/26)
重要	アドビシステムズ社の Acrobat Reader と Acrobat のセキュリティ修正プログラムについて(3/19)更新
重要	ジャストシステム社ワープロソフトー太郎の脆弱性について(3/16)
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 (MS09-006,007,008)(3/11)
●	インターネット定点観測の更新情報(3/2)