

平成 20 年 5 月 13 日

我が国におけるインターネット治安情勢について

(平成 20 年 4 月期)

- ・ファイアウォールに対するアクセスは減少傾向
～中国、日本及び台湾からのアクセスが減少～
～1026/UDP 及び 1027/UDP ポートに対するアクセスが増加～
- ・不正侵入検知システムにおける不正なアクセスは増加傾向

1 概説

平成 20 年 4 月期におけるファイアウォール^{*}に対するアクセス件数は、一日・1IP 当たり約 181.0 件で、平成 20 年 3 月期と比較して約-5.5 件 (約-3.0%) と減少した。

上位 5 位までのポート別順位は、135/TCP、ICMP (Echo Request)、1026/UDP、1027/UDP 及び 1433/TCP の順であり、3 月期と比較して 135/TCP 及び 1433/TCP ポートに対するアクセスが減少し、その他のポートに対するアクセスは増加した。

4 月期におけるアクセス件数の上位 5 か国は 3 月期と同様で、中国、日本、米国、台湾及び韓国であり、中国、日本及び台湾からのアクセス件数は減少した。

4 月期の不正侵入検知システム^{*}における不正なアクセスの検知件数は、一日・1IP 当たり約 10.3 件で、3 月期と比較して約+2.0 件 (約+23.9%) であった。攻撃手法別においては、第 1 位の Worm (SQL Slammer ワーム)、第 2 位の Scan と共に増加している。発信元国/地域別において上位 5 か国は 3 月期と順位は変わらないが、エストニアとスペインの検知件数が増加した。

^{*}ファイアウォール及び不正侵入検知システムについては、「4 集計対象」を参照のこと。

2 インターネット定点観測

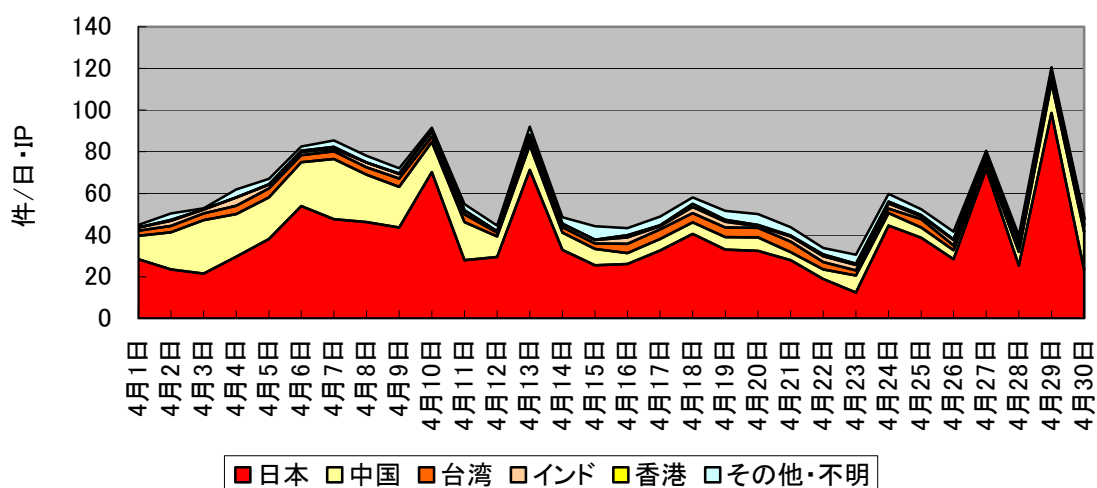
2.1 ファイアウォールに対するアクセス分析

(1) 宛先ポート別推移(上位 5 ポート、積み上げ)

4 月期における上位 5 ポートは以下のとおりである。上位 2 ポートの順位に変動はない。3 月期に 3 位であった 1433/TCP に対するアクセスが減少し、1026/UDP 及び 1027/UDP に対するアクセスが増加したため、5 位となった。

4 月期順位	ポート	前月比 (一日・1IP 当たり)	3 月期順位
1 位	135/TCP	約-11.9% (約-8.00 件)	1 位
2 位	ICMP (Echo Request)	約+2.2% (約+0.66 件)	2 位
3 位	1026/UDP	約+6.7% (約+0.99 件)	4 位
4 位	1027/UDP	約+10.5% (約+1.35 件)	5 位
5 位	1433/TCP	約-6.1% (約-0.92 件)	3 位

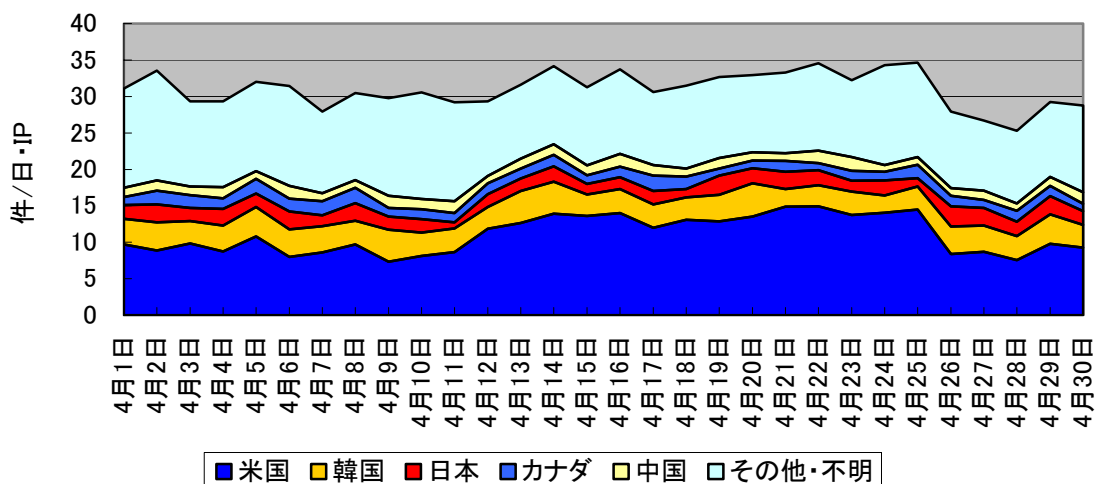
■ 135/TCP



4 月期において 10 日、13 日、27 日及び 29 日に見られるアクセスの増加は、日本国内の特定のネットワークからのアクセスによるものであり、ボット又はワームによる影響と考えられる。

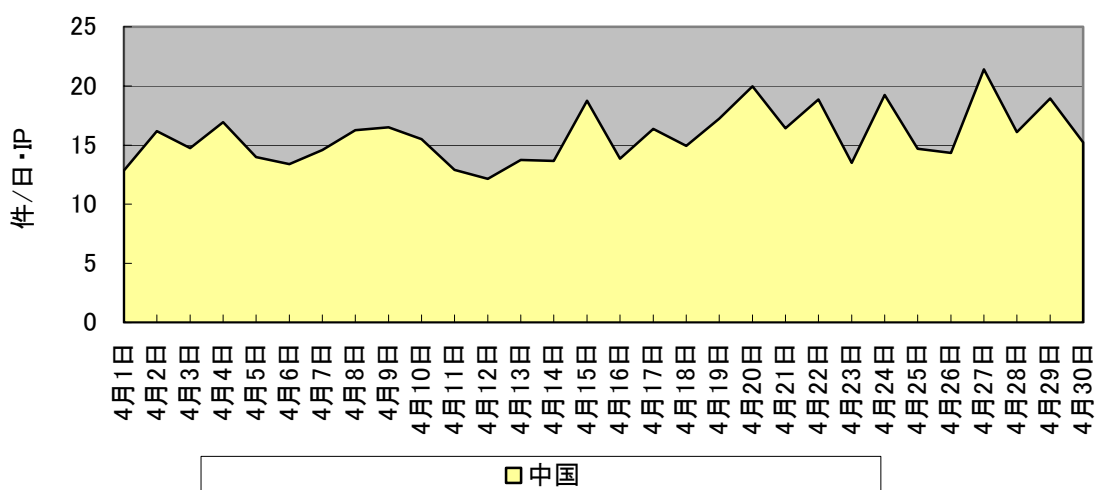
3 月期と比較して、上位を占める国からのアクセスが減少したため、全体としても減少傾向となった。

■ ICMP(Echo Request)



3月期と比較して、上位を占める国において、米国を除いた国からのアクセスは減少したものの、大部分を占める米国からのアクセスが増加したことから、全体としても増加傾向となった。

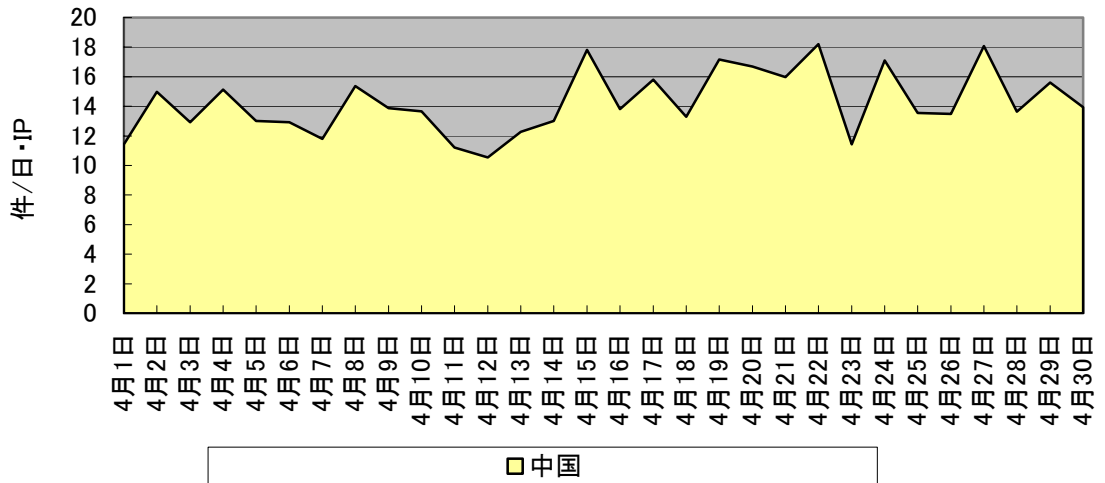
■ 1026/UDP



1026/UDP に対するアクセスの多くは Windows の Messenger サービスに対するスパムであり、受信したコンピュータにおいて、商品の購入を促す広告等の表示を目的としたものであった。

4月期から、すべてのアクセスが中国からのものとなり、3月期と比較して増加傾向となった。

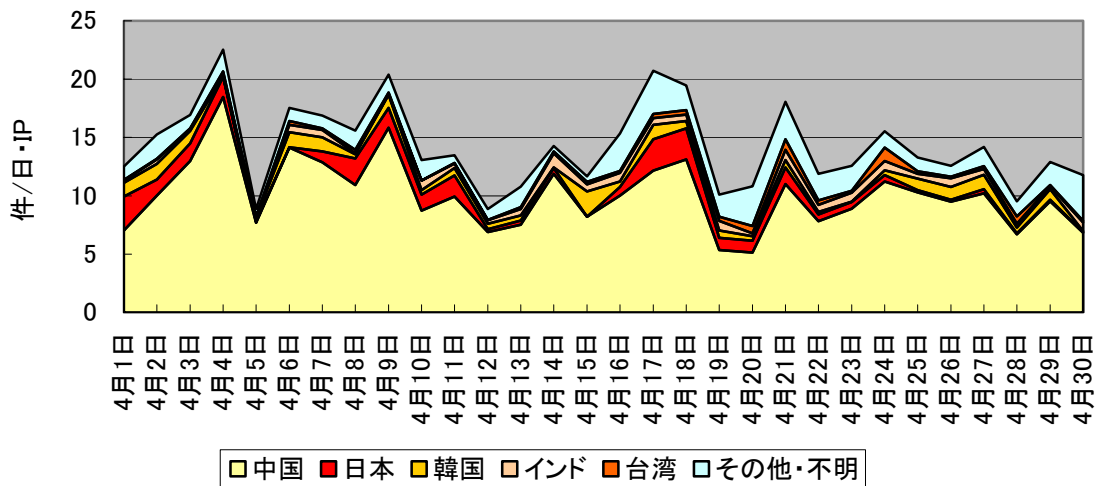
■ 1027/UDP



1026/UDP に対するアクセスと同様に、1027/UDP に対するアクセスの多くも、Windows の Messenger サービスに対するスパムであり、受信したコンピュータにおいて、商品の購入を促す広告等の表示を目的としたものであった。

1026/UDP に対するアクセスと同様に、すべて中国からのアクセスであり、3 月期と比較して増加傾向となった。

■ 1433/TCP

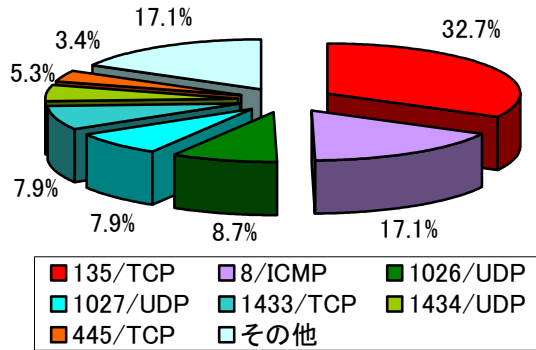


3 月期と比較して、中国以外からのアクセスが増加したものの、大部分を占める中国からのアクセス数が減少したことから、全体としても減少した。

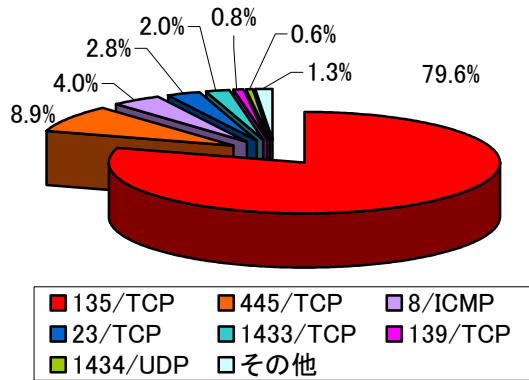
このポートは Microsoft SQL Server で使用されているもので、このソフトウェアの脆弱性を突くウイルス等によるアクセスと推測される。

(2) 宛先ポート別比率

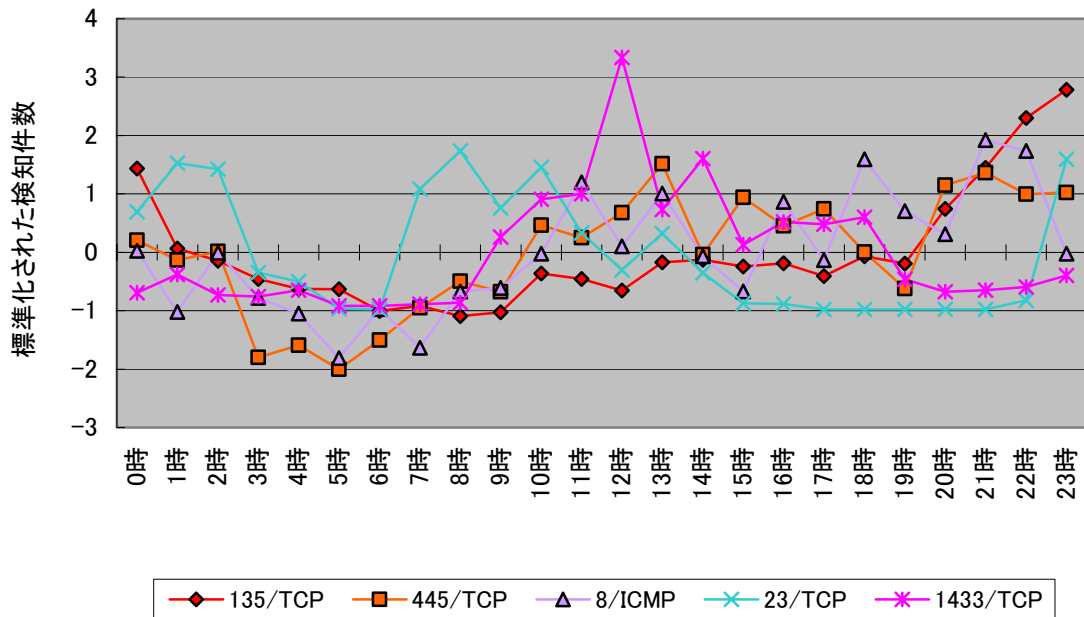
■ 発信元/全世界



■ 発信元/日本



(3) 国内の時間帯推移(上位 5 ポート)



注) 件数は、宛先ポートごとに次の式により標準化した。

$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

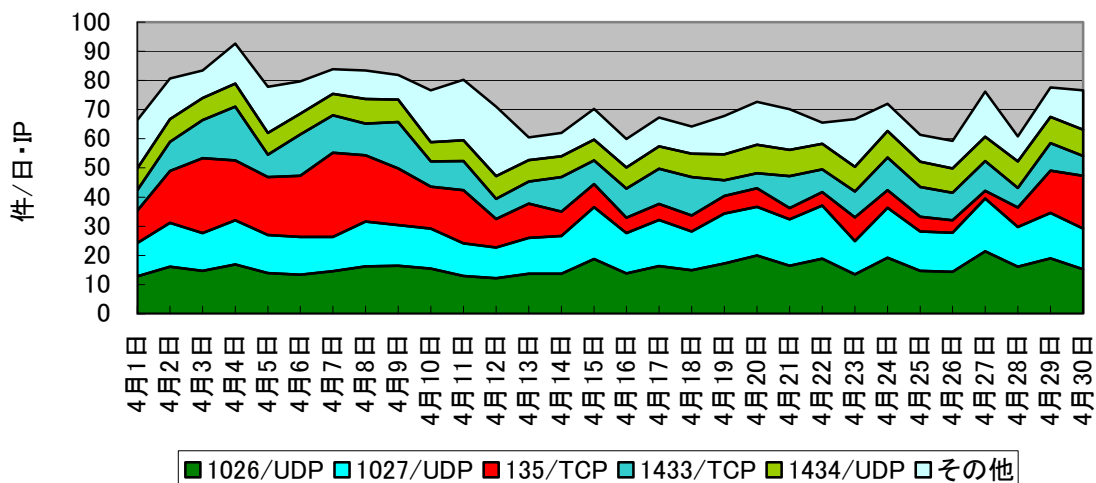
(4) 発信元国／地域別推移(上位 5 か国、積み上げ)

4 月期と 3 月期における上位 5 位までの発信元国／地域は以下のとおりである。
3 月期と比較して、国毎に増減のばらつきはあるものの、順位に変動はない。

一日・1IP 当たりのアクセス件数について、3 月期との増減比較を前月比の欄に示す。

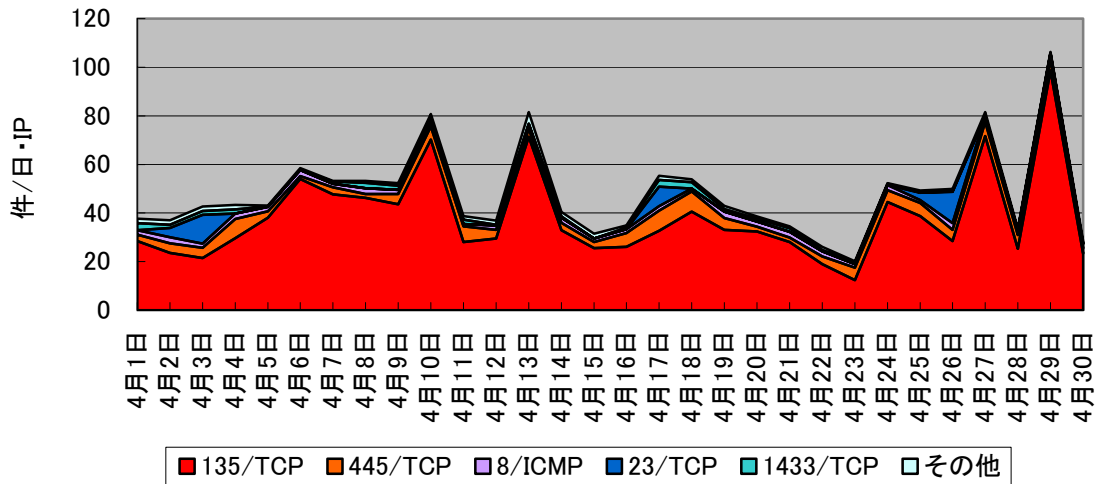
4 月期順位	国 名	前月比 (一日・1IP 当たり)	3 月期順位
1 位	中 国	約-5.5% (約-4.20 件)	1 位
2 位	日 本	約-0.6% (約-0.30 件)	2 位
3 位	米 国	約+16.5% (約+2.18 件)	3 位
4 位	台 湾	約-10.9% (約-0.99 件)	4 位
5 位	韓 国	約+0.1% (約 0.00 件)	5 位

■ 中国



3 月期と比較して、1026/UDP、1027/UDP 及び 1434/UDP ポートに対するアクセスが増加したものの、135/TCP 及び 1433/TCP ポートに対するアクセスが減少したことから、全体としては減少傾向となった。

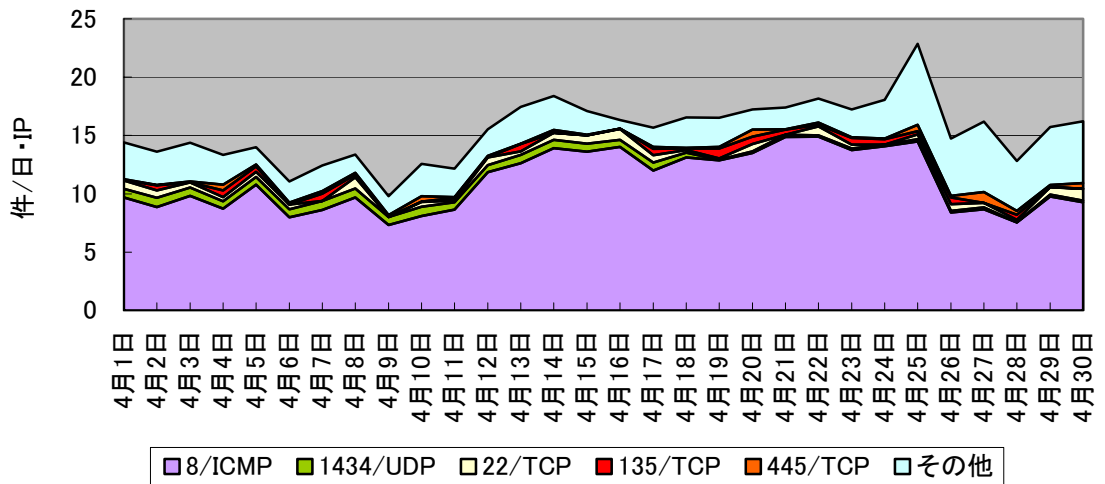
■ 日本



3月期と比較して、大部分を占める 135/TCP ポートに対するアクセスが減少したことから、全体としても減少傾向となった。

23/TCP ポートに対するアクセスが増加しているが、このポートは TELNET サービスで使用されているものであり、不正なアクセスの試みと推測される。

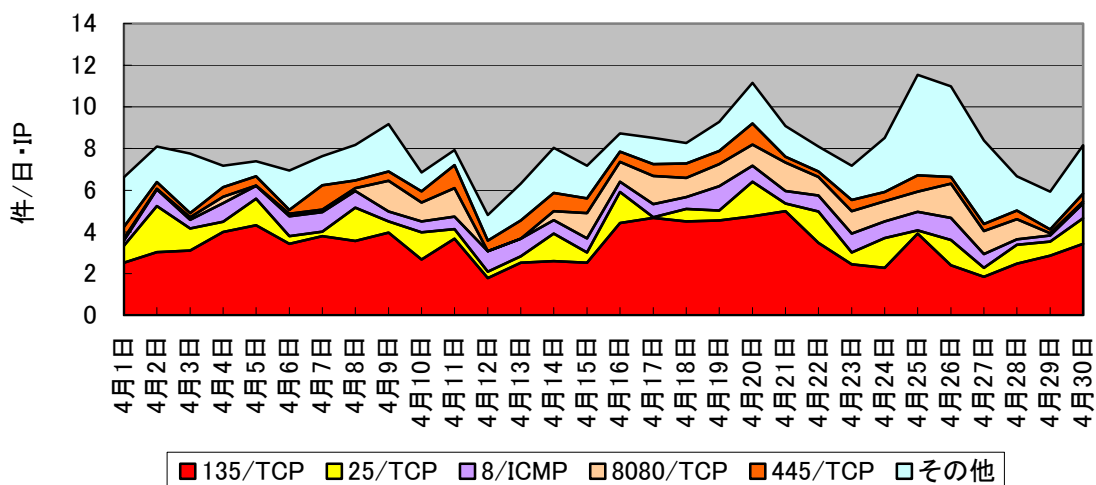
■ 米国



3月期と比較して、1434/UDP及び135/TCPポートに対するアクセスは減少したものの、大部分を占める8/ICMPポートに対するアクセスが増加したことから、全体としても増加傾向となった。

なお、25日からアクセスが増加しているその他のポートは、特定のネットワークからのものであった。

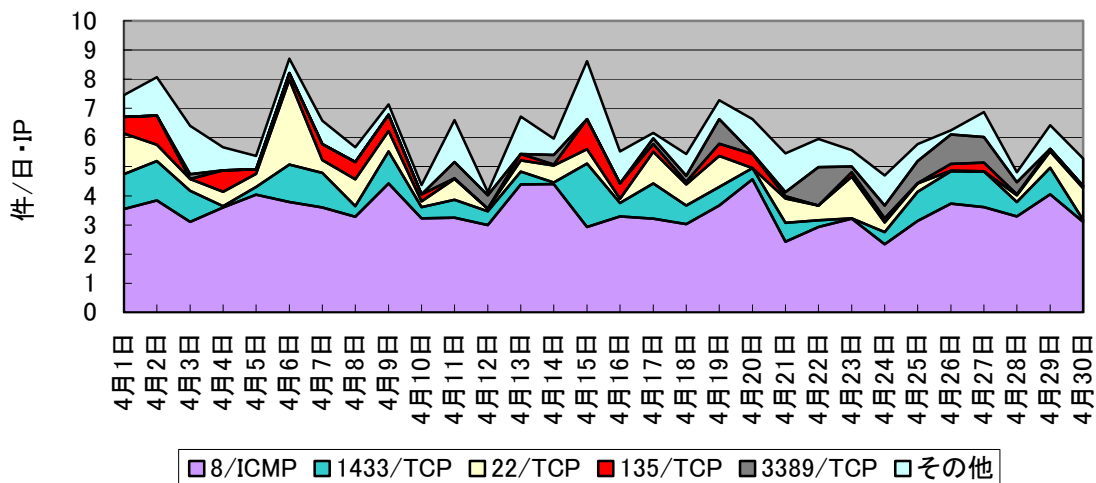
■ 台湾



3月期と比較して、大部分を占める135/TCPポートに対するアクセスが減少したことから、全体としても減少傾向となった。

なお、25日から27日までの間アクセスが増加しているその他のポートは、特定のネットワークからのものであった。

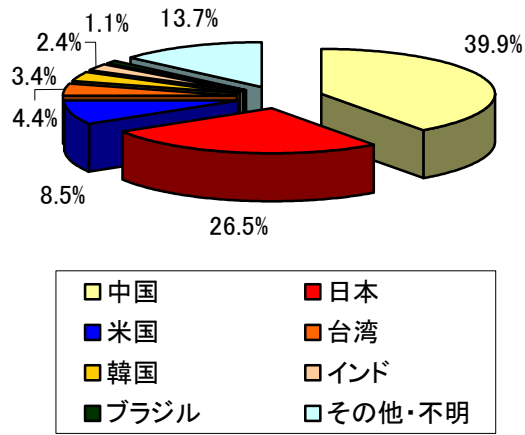
■ 韓国



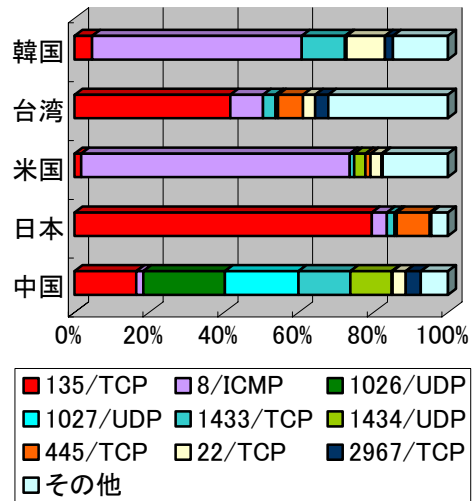
3月期と比較して、8/ICMP及び22/TCPポートに対するアクセスが減少し、1433/TCP、135/TCP及び3389/TCPに対するアクセスが増加したため、全体としては横ばいとなった。

3389/TCPポートに対するアクセスが増加しているが、このポートはWindowsのリモートデスクトップ等で使用されているものであり、不正なアクセスの試みと推測される。

(5) 国／地域別比率

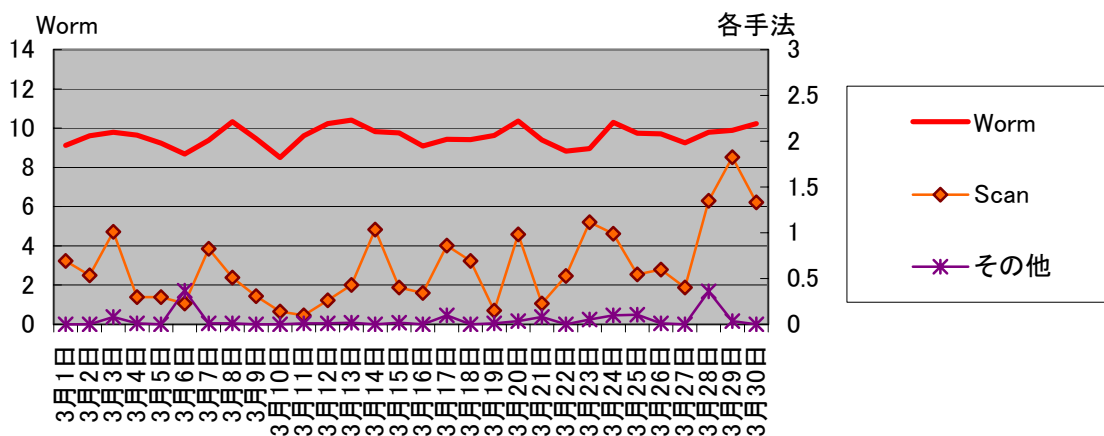


(6) 上位国／地域の宛先ポート別比率



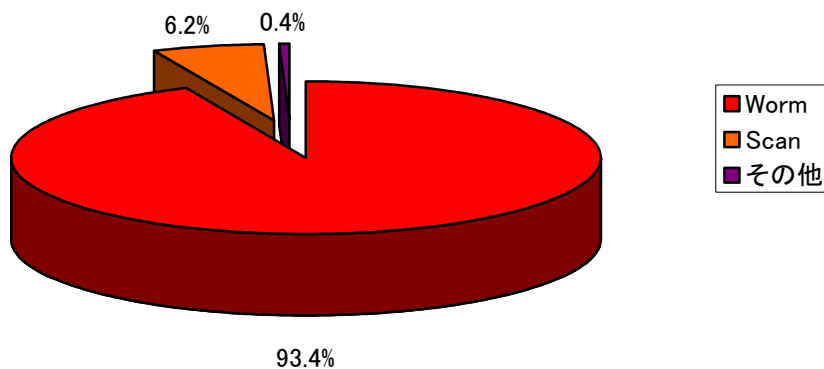
2.2 不正侵入検知システムにおける不正なアクセスの検知分析

(1) 攻撃手法別推移



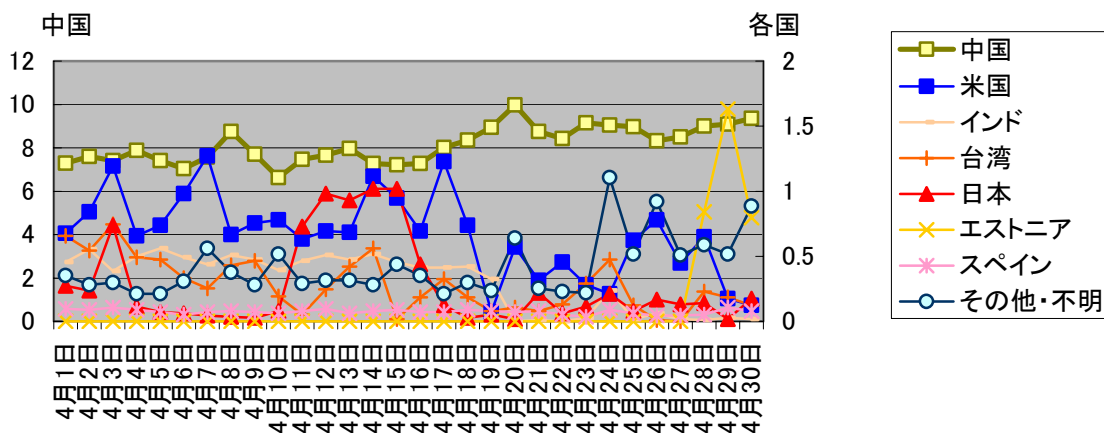
第1位のWorm (SQL Slammer ワーム) は、一日・1IP当たりの検知件数が約9.6件で、3月期と比較して約+1.7件 (約+21.9%) と増加した。第2位のScanは、一日・1IP当たりの検知件数が約0.63件で、3月期と比較して約+0.23件 (約+58.1%) と増加した。

(2) 攻撃手法別比率



3月期と同様にWormが大半を占めているが、Scanが増加傾向となった。

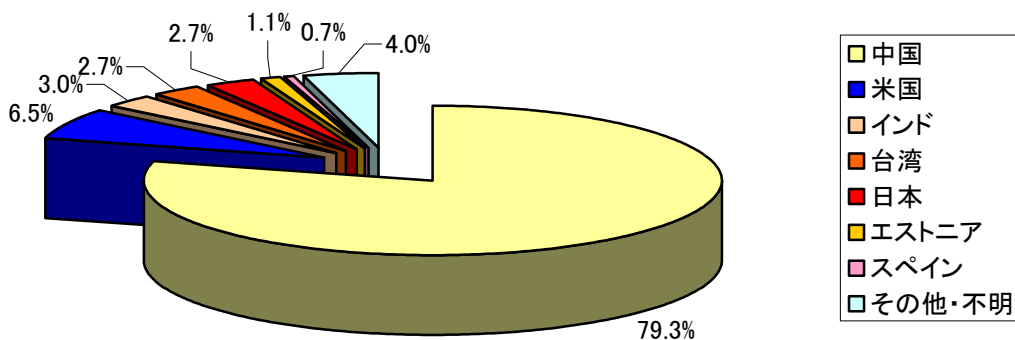
(3) 発信元国／地域別推移



3月期と比較してインドを除く上位の国からの検知件数が増加したため、全体としては増加傾向となった。

なお、11日から15日までの間、日本国内からのアクセスが増加しているが、特定のネットワークからのWormによるものであった。また、29日のエストニアからのアクセスは、特定のネットワークからのScanが多数を占めている。




(4) 発信元国／地域別比率



3月期に引き続き、発信元が中国であるものを最も多く検知している。その内訳は、Worm (SQL Slammer ワーム) が大多数を占めている。

3 @police (Topics) 掲載事項

@police において4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
	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 (MS08-018, 019, 020, 021, 022, 023, 024, 025) (4/25) 更新
●	インターネット治安情勢更新(平成 19 年度第 4 四半期報を追加) (4/23)
●	脆弱性情報の発表日の修正についてのお知らせ(4/22)
	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 (MS08-014, 015, 016, 017) (4/21) 更新
●	インターネット治安情勢更新(平成 20 年 3 月報を追加) (4/18)
	Flash Player の脆弱性について(4/9)

4 集計対象

■ ファイアウォール

定点観測で集計対象としているファイアウォールは、すべての incoming のパケットを破棄する設定となっている。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ない。

なお、ICMP パケットに関しては、タイプごと※に集計している。

■ 不正侵入検知システム

各拠点の不正侵入検知装置には、平成 20 年 4 月 30 日現在、381 種類のシグネチャが登録されている。検知された各シグネチャは、次に示す分類に従って集計している。グラフには、分類における上位 2 つとそれ以外 (Others) の件数がプロットされる。

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
Backdoor	SubSeven, IP Unknown Protocol, BackOrifice, NetBus
DDoS	TFN Probe
DNS	DNS HINFO decode, DNS Length Overflow Attack, DNS named iquery attempt, named version attempt
DoS	SYN Flood, UDP Flood, Stick Attack, Land
ICMP	Superscan Echo, redirect host, redirect net, Ping Flooding
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
Worm	SQL Slammer
Others	Traceroute 検出, Connection Closed MSG from Port 80, IP Duplicate, IP Fragmentation 等を含み上位 4 つを除くもの

・シグネチャは随時更新している。

※ グラフの凡例においては、スラッシュの前にタイプを付け加えている。