

平成 30 年 9 月 28 日

平成 30 年 7 月 期 観 測 資 料

1 観測結果概要

平成 30 年 7 月 期 (以下「今期」という。)に、インターネットとの接続点に設置したセンサーにおいて検知したアクセス件数は、一日・1IP アドレス当たり 2,907.3 件で、平成 30 年 6 月 期 (以下「前期」という。)と比較して 149.5 件 (5.4%) 増加しました。また、発信元 IP アドレス数は、一日当たり 46,956.8 個で、前期と比較して 836.4 個 (1.8%) 減少しました。

不正侵入等の行為 (以下「不正侵入等」という。)のシグネチャを用いた検知件数は、一日・1IP アドレス当たり 552.0 件で、前期と比較して 57.5 件 (9.4%) 減少しました。また、発信元 IP アドレス数は、一日当たり 4,120.7 個で、前期と比較して 995.6 個 (19.5%) 減少しました。

DoS 攻撃被害検知件数は、一日当たり 5,592.0 件で、前期と比較して 13,606.3 件 (70.9%) 減少しました。また、発信元 IP アドレス数は、一日当たり 402.0 個で、前期と比較して 9.0 個 (2.2%) 減少しました。

2 センサーにおけるアクセス検知の観測結果

2-1 宛先ポート別アクセス検知件数

表 2-1 宛先ポート別検知件数(今期順位)

今期 順位	前期 順位	ポート	今期件数 ⁱ	前期比 ⁱ
1位	1位	23/TCP	411.61件	+9.0% (+33.87件)
2位	2位	445/TCP	215.86件	+7.0% (+14.14件)
3位	4位	22/TCP	90.46件	+12.7% (+10.19件)
4位	3位	80/TCP	80.40件	-58.4% (-112.66件)
5位	7位	53/UDP	80.04件	+65.8% (+31.76件)

表 2-2 宛先ポート別検知件数(増加順位)

増加 順位	ポート	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	23/TCP	411.61件	+9.0% (+33.87件)	1位	1位
2位	5555/TCP	51.19件	+193.0% (+33.72件)	9位	19位
3位	53/UDP	80.04件	+65.8% (+31.76件)	5位	7位
4位	53413/UDP	37.90件	+98.1% (+18.76件)	11位	18位
5位	81/TCP	50.38件	+44.0% (+15.40件)	10位	10位

表 2-3 宛先ポート別検知件数(減少順位)

減少 順位	ポート	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	80/TCP	80.40件	-58.4% (-112.66件)	4位	3位
2位	6379/TCP	5.78件	-72.7% (-15.39件)	38位	16位
3位	8000/TCP	12.18件	-53.9% (-14.25件)	24位	12位
4位	8545/TCP	33.49件	-26.3% (-11.95件)	13位	8位
5位	5038/TCP	3.33件	-56.0% (-4.24件)	55位	29位

ⁱ 一日・1IPアドレス当たり。

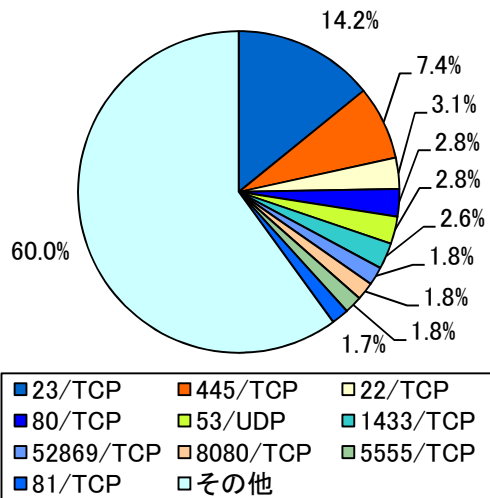


図 2-1 宛先ポート別比率(全て) ⁱ

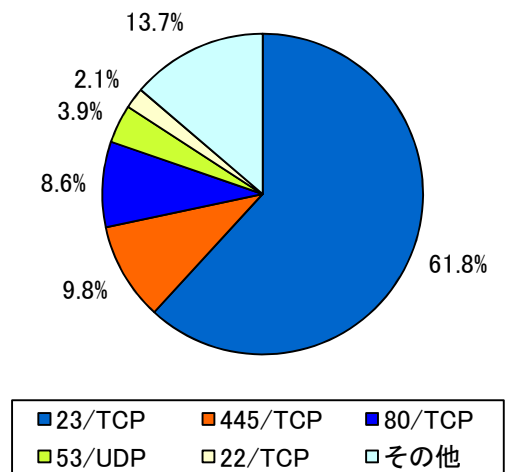


図 2-2 宛先ポート別比率(日本国内)

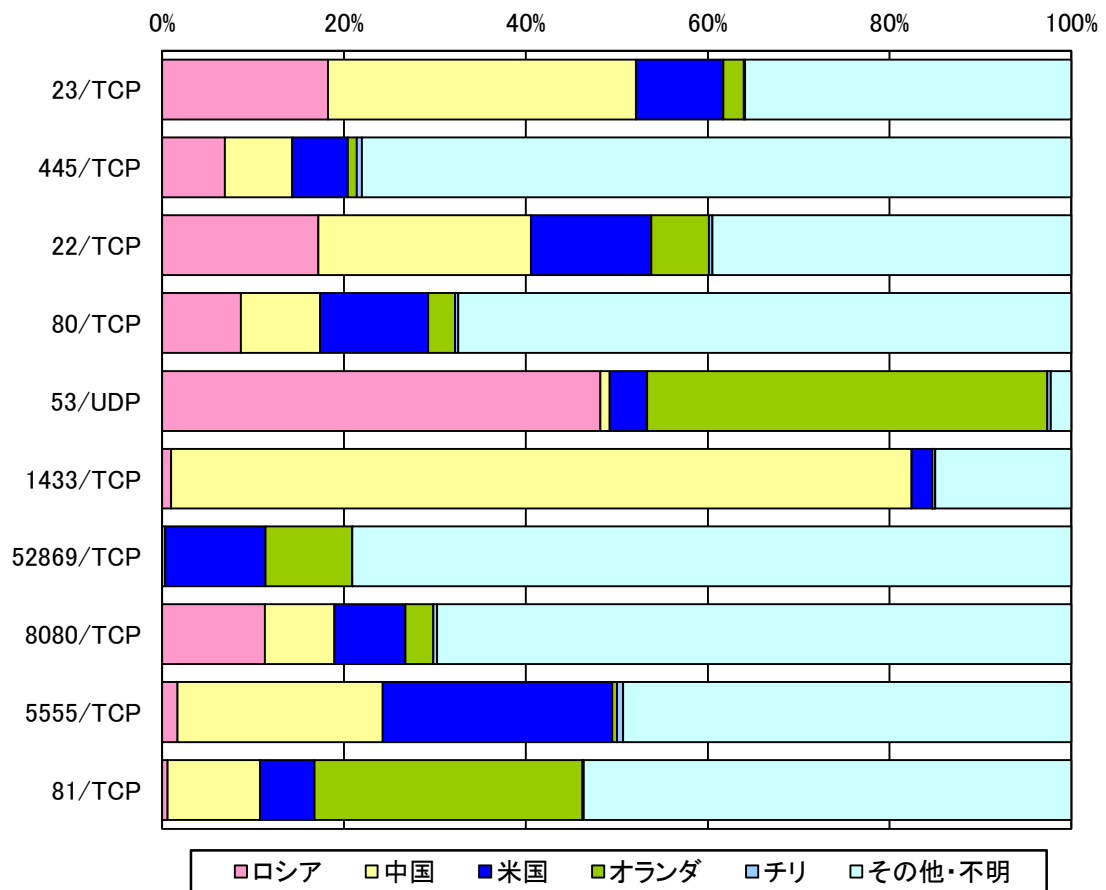


図 2-3 宛先ポート別上位の発信元国・地域別比率 ⁱⁱ

ⁱ 当データは、小数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ります。以降の円グラフも同様です。

ⁱⁱ 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

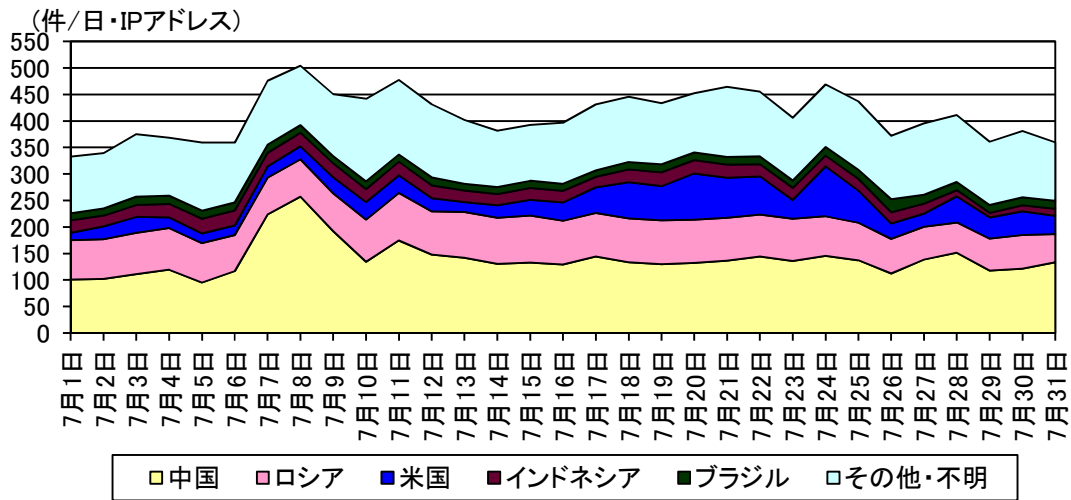


図 2-4 センサーのポート 23/TCP における検知件数の推移

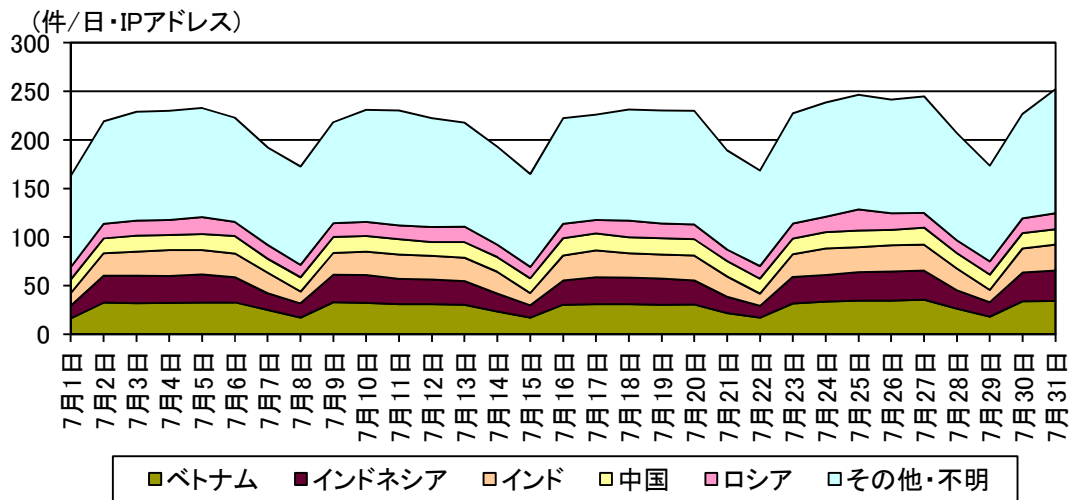


図 2-5 センサーのポート 445/TCP における検知件数の推移

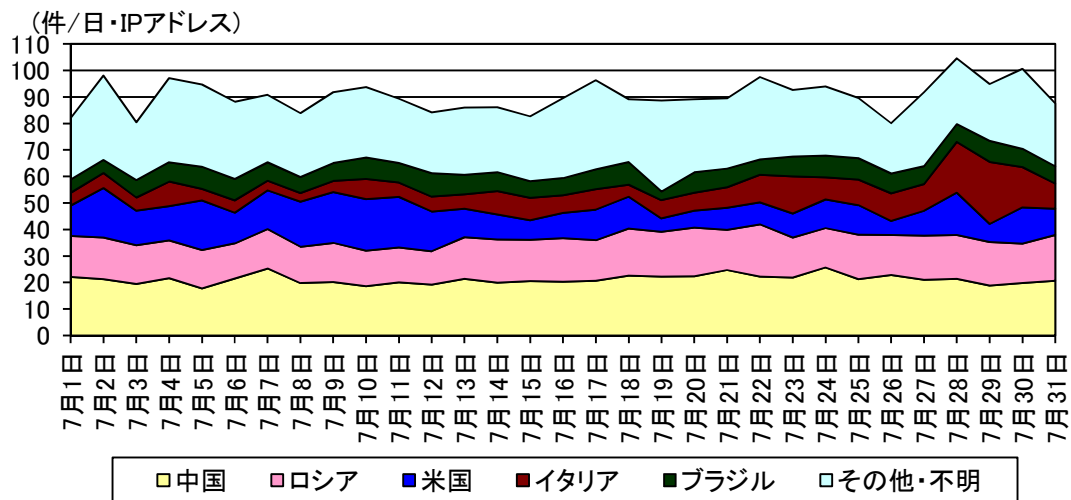


図 2-6 センサーのポート 22/TCP における検知件数の推移

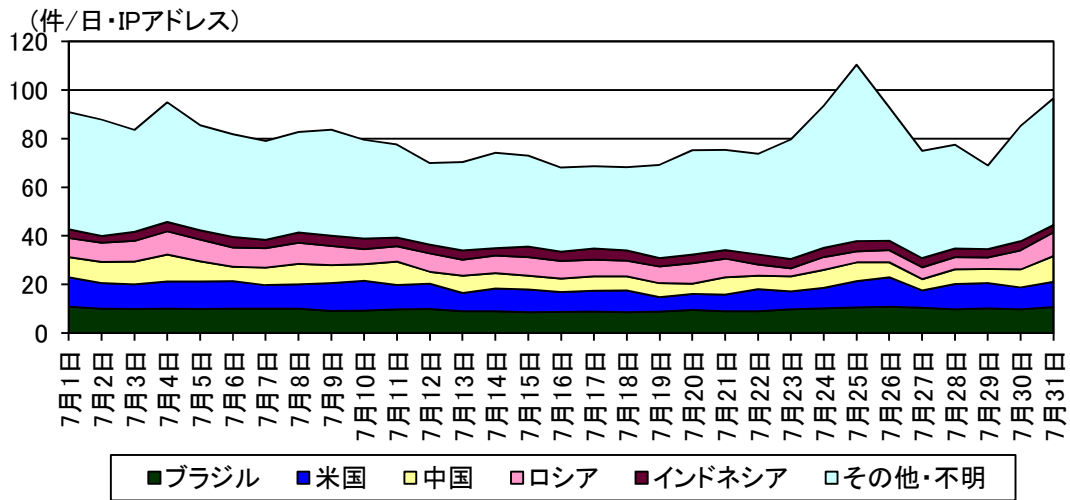


図 2-7 センサーのポート 80/TCP における検知件数の推移

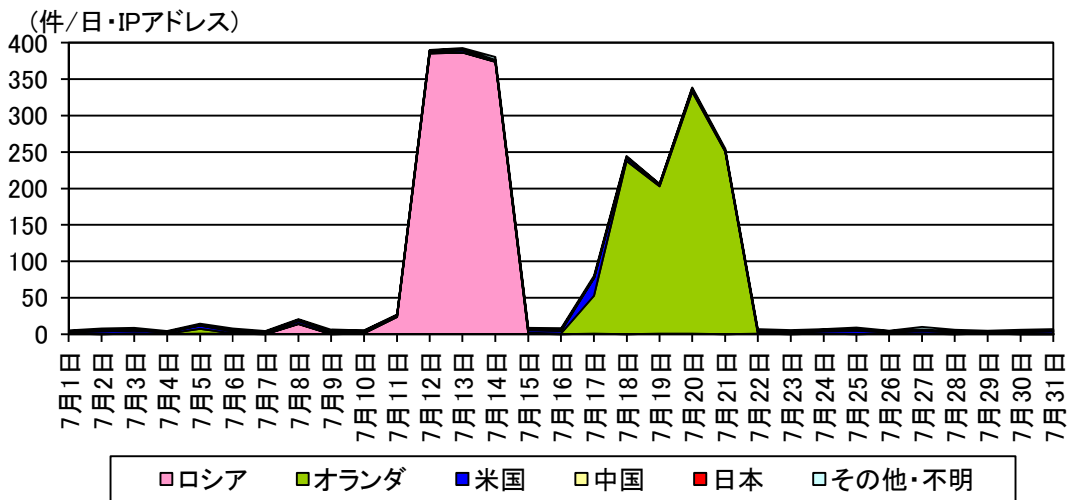


図 2-8 センサーのポート 53/UDP における検知件数の推移

2-2 発信元国・地域別アクセス検知件数

表 2-4 発信元国・地域別検知件数(今期順位)

今期 順位	前期 順位	国・地域	今期件数 ⁱ	前期比 ⁱ
1位	1位	ロシア	689.92 件	+50.5% (+231.48 件)
2位	2位	中国	440.29 件	+4.3% (+18.08 件)
3位	3位	米国	316.73 件	-6.5% (-21.86 件)
4位	4位	オランダ	274.10 件	+25.3% (+55.41 件)
5位	6位	チリ	134.31 件	-17.5% (-28.56 件)

表 2-5 発信元国・地域別検知件数(増加順位)

増加 順位	国・地域	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	ロシア	689.92 件	+50.5% (+231.48 件)	1位	1位
2位	オランダ	274.10 件	+25.3% (+55.41 件)	4位	4位
3位	ブルガリア	62.19 件	+372.6% (+49.03 件)	9位	31位
4位	中国	440.29 件	+4.3% (+18.08 件)	2位	2位
5位	イタリア	78.60 件	+24.5% (+15.49 件)	7位	9位

表 2-6 発信元国・地域別検知件数(減少順位)

減少 順位	国・地域	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	英国	70.09 件	-57.9% (-96.45 件)	8位	5位
2位	チリ	134.31 件	-17.5% (-28.56 件)	5位	6位
3位	米国	316.73 件	-6.5% (-21.86 件)	3位	3位
4位	メキシコ	8.31 件	-71.8% (-21.13 件)	36位	16位
5位	ブラジル	56.16 件	-16.2% (-10.83 件)	11位	8位

ⁱ 一日・1IP アドレス当たり。

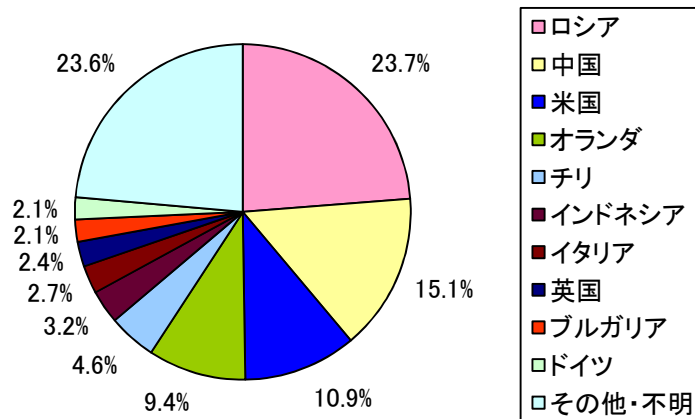


図 2-9 発信元国・地域別比率

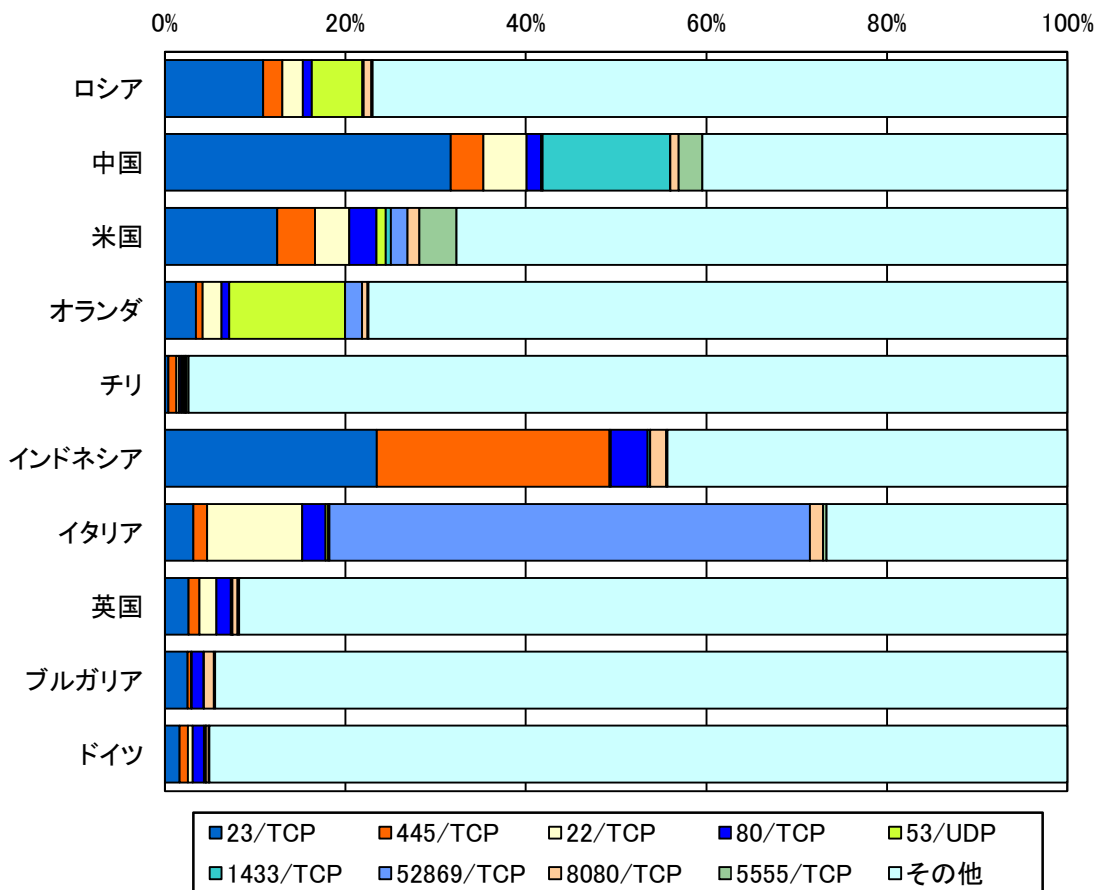


図 2-10 発信元国・地域別上位の宛先ポート別比率

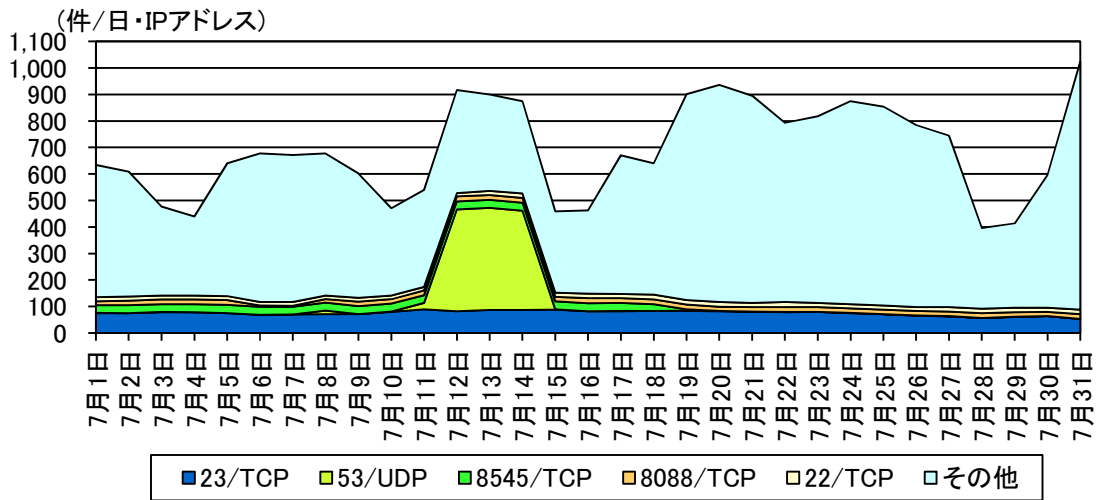


図 2-11 ロシアからの検知件数の推移

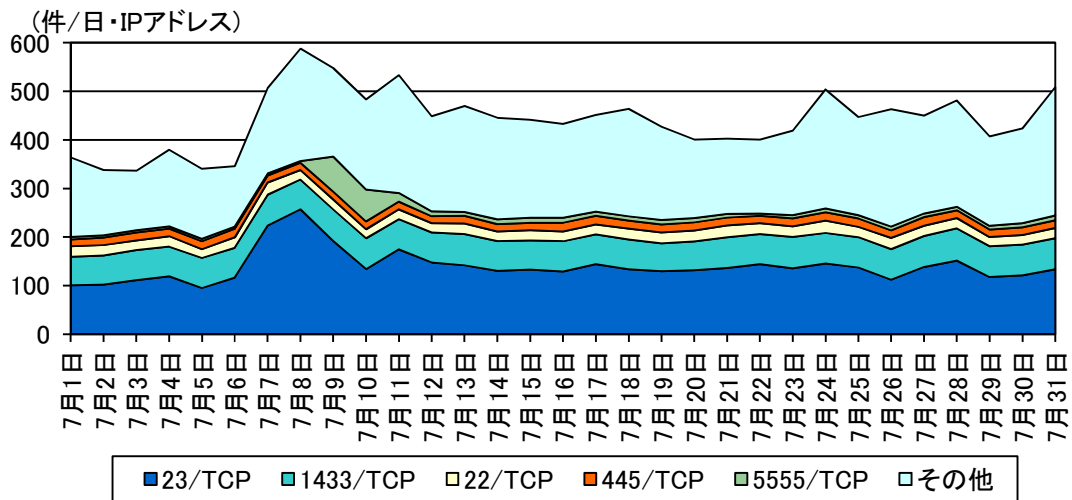


図 2-12 中国からの検知件数の推移

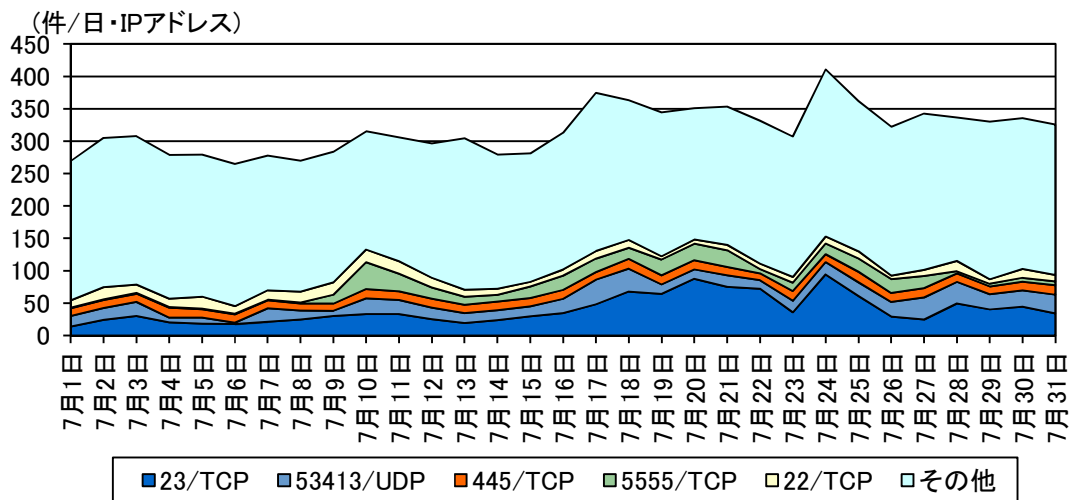


図 2-13 米国からの検知件数の推移

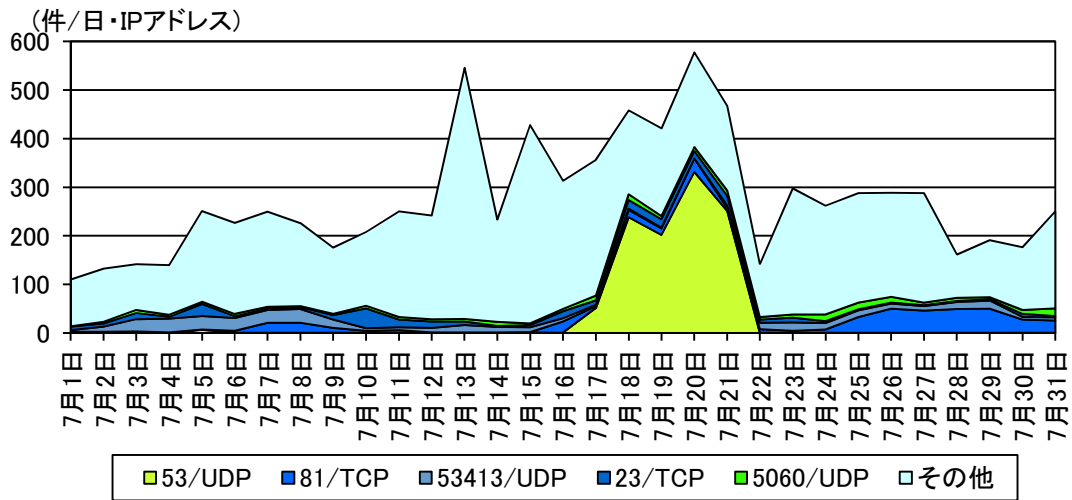


図 2-14 オランダからの検知件数の推移

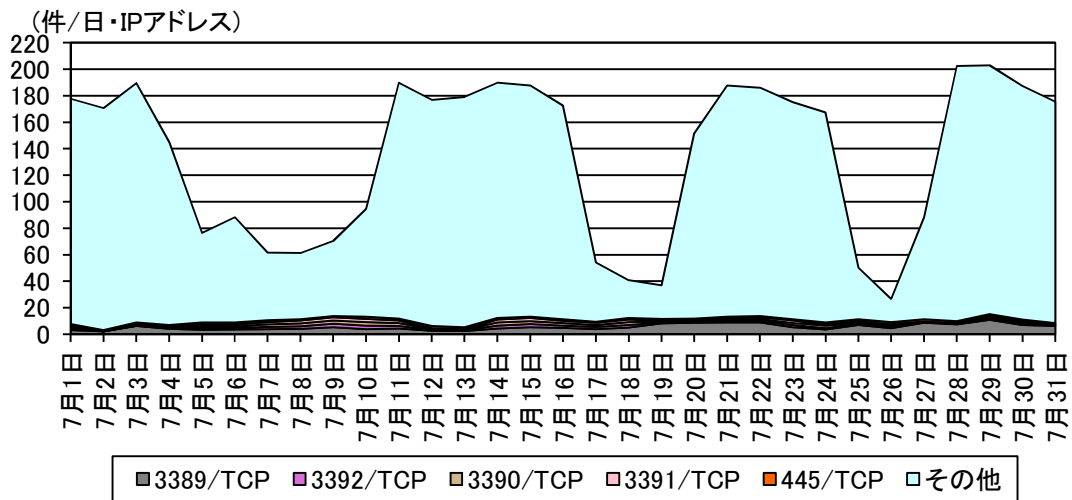


図 2-15 チリからの検知件数の推移

3 不正侵入等の観測結果

3-1 攻撃手法別アクセス検知件数

表 3-1 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 ⁱ	前期比 ⁱ	増加 順位	減少 順位
1位	1位	Scan	468.24 件	-11.3% (-59.48 件)		1位
2位	2位	VoIP	34.47 件	+23.8% (+6.62 件)	1位	
3位	4位	Scan(Password)	17.20 件	+5.9% (+0.96 件)	2位	
4位	3位	ICMP	16.28 件	-18.9% (-3.80 件)		2位
5位	5位	DNS	10.18 件	-9.2% (-1.03 件)		3位

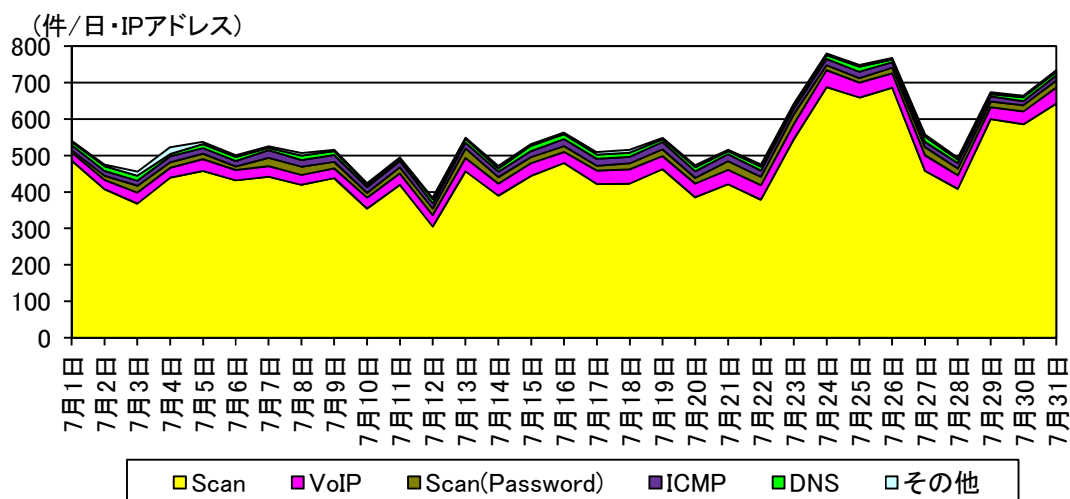


図 3-1 不正侵入等の攻撃手法別検知件数の推移

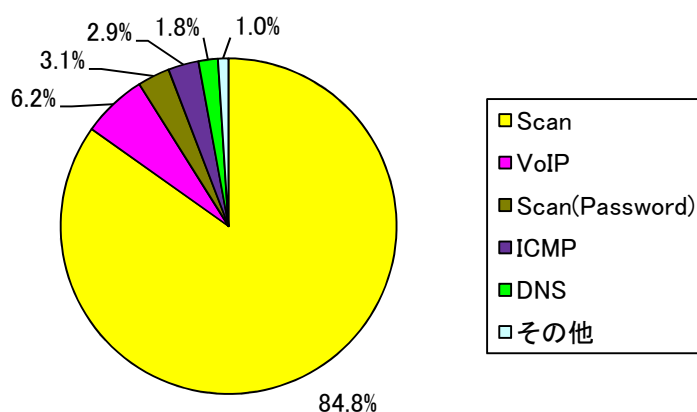


図 3-2 不正侵入等の攻撃手法別検知比率

ⁱ 一日・1IPアドレス当たり。

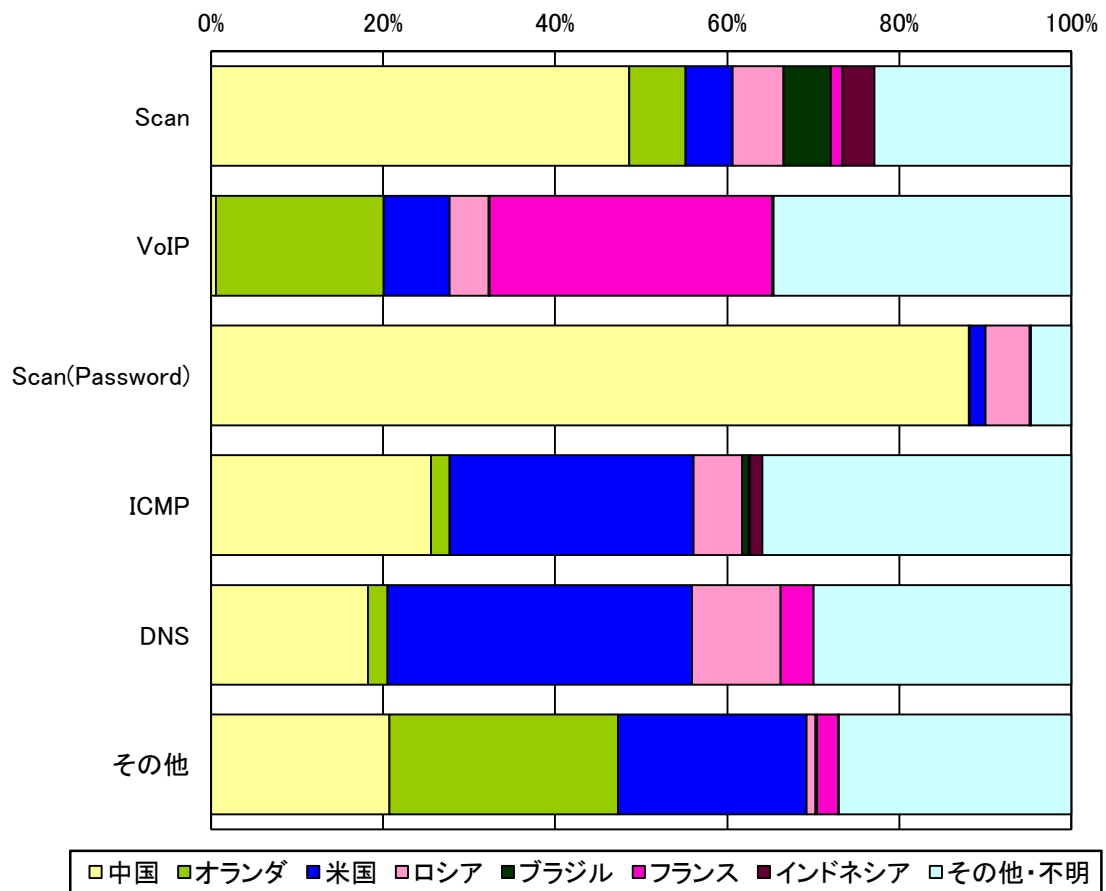


図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 発信元国・地域別アクセス検知件数

表 3-2 不正侵入等の発信元国・地域別検知件数(今期順位)

今期 順位	前期 順位	国・地域	今期件数 ⁱ	前期比 ⁱ
1位	1位	中国	250.18 件	+21.8% (+44.85 件)
2位	3位	オランダ	39.50 件	-40.0% (-26.30 件)
3位	2位	米国	37.86 件	-50.6% (-38.81 件)
4位	4位	ロシア	32.29 件	-5.1% (-1.73 件)
5位	5位	ブラジル	26.08 件	-13.3% (-4.01 件)

表 3-3 不正侵入等の発信元国・地域別検知件数(増加順位)

増加 順位	国・地域	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	中国	250.18 件	+21.8% (+44.85 件)	1位	1位
2位	フランス	18.12 件	+49.8% (+6.03 件)	6位	9位
3位	エジプト	1.06 件	+269.2% (+0.77 件)	37位	61位
4位	イラン	5.77 件	+13.9% (+0.70 件)	13位	19位
5位	モルドバ	0.97 件	+120.8% (+0.53 件)	38位	50位

表 3-4 不正侵入等の発信元国・地域別検知件数(減少順位)

減少 順位	国・地域	今期件数 ⁱ	前期比 ⁱ	今期 順位	前期 順位
1位	米国	37.86 件	-50.6% (-38.81 件)	3位	2位
2位	オランダ	39.50 件	-40.0% (-26.30 件)	2位	3位
3位	ウクライナ	5.48 件	-64.4% (-9.90 件)	14位	7位
4位	メキシコ	0.69 件	-92.1% (-7.98 件)	41位	13位
5位	ブラジル	26.08 件	-13.3% (-4.01 件)	5位	5位

ⁱ 一日・1IPアドレス当たり。

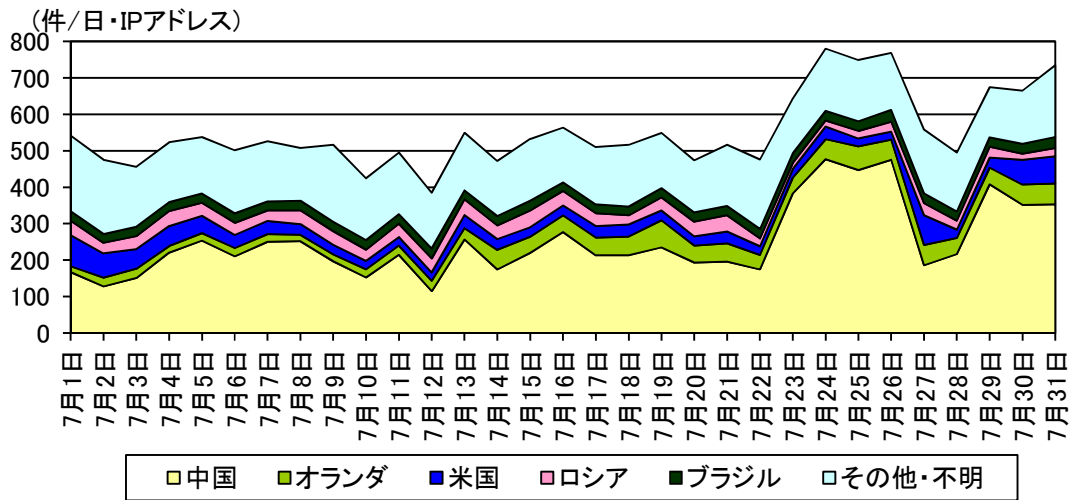


図 3-4 不正侵入等の発信元国・地域別検知件数の推移

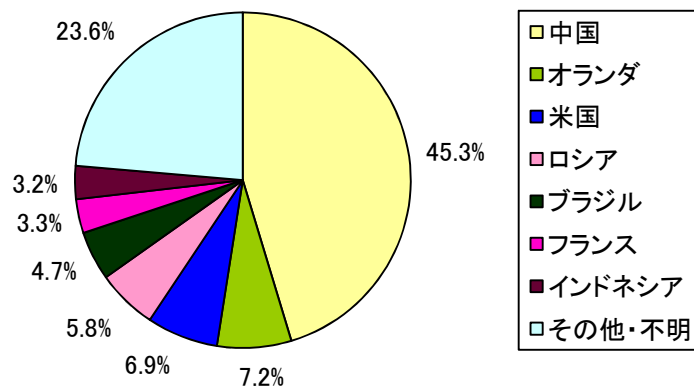


図 3-5 不正侵入等の発信元国・地域別検知比率

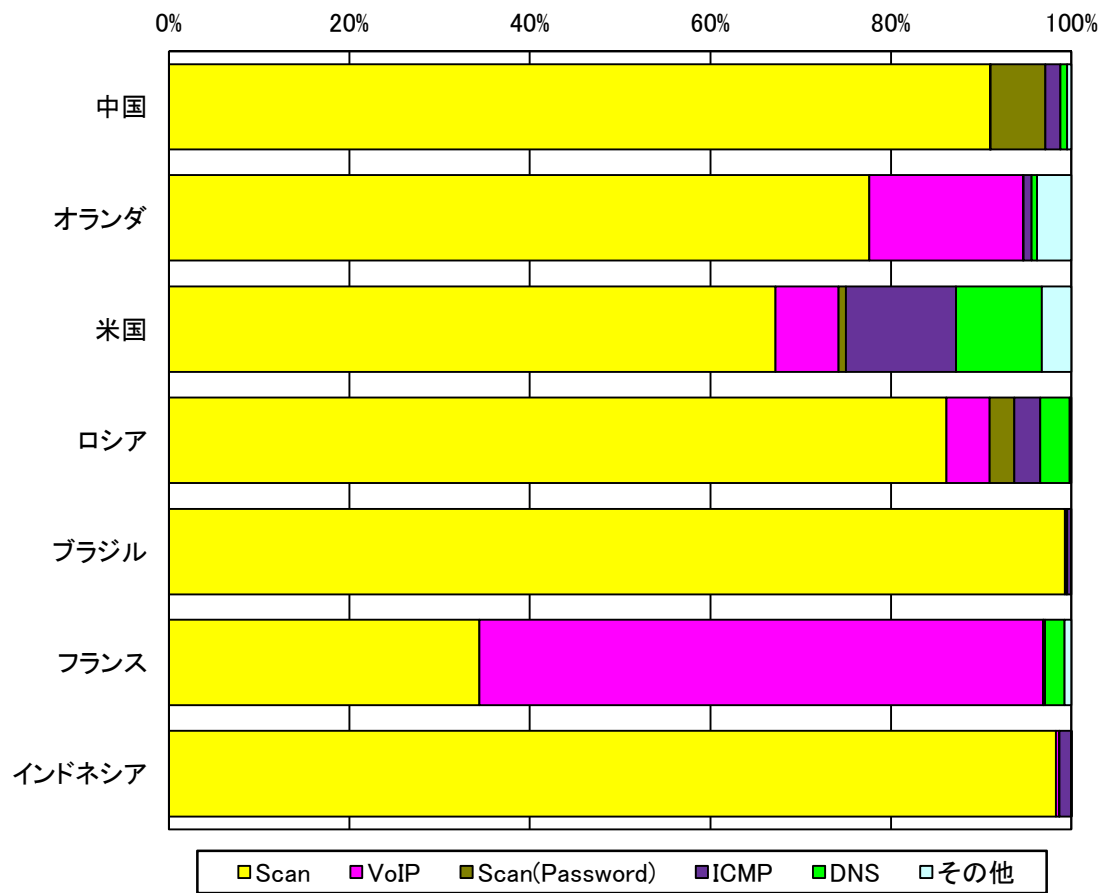


図 3-6 不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

4 DoS 攻撃被害の観測結果

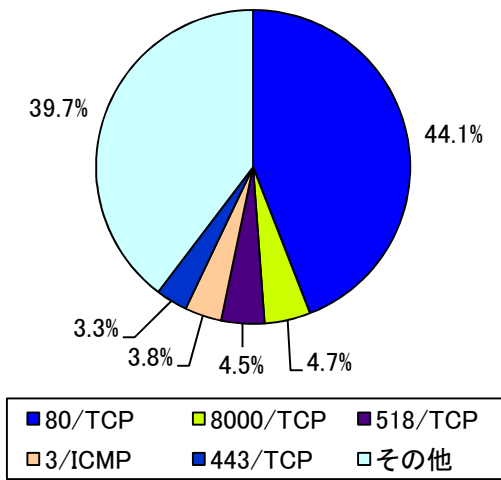


図 4-1 跳ね返りパケット発信元ポート別比率

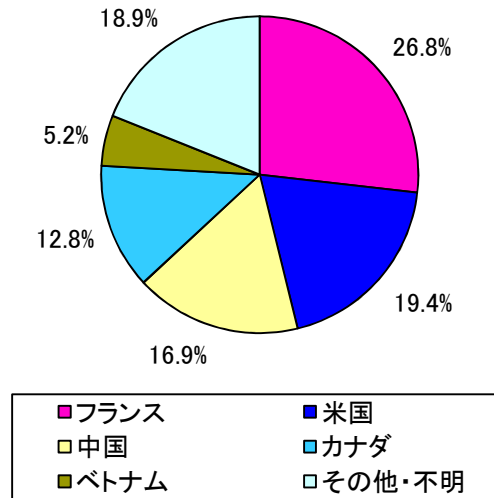


図 4-2 跳ね返りパケット発信元国・地域別比率

5 観測方法等

警察庁では、インターネット接続点に設置したセンサーにおいて検知したアクセス情報等を集約・分析した結果を観測結果として公表しています。その方法については、次のとおりです。

5-1 パケットの表記

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

5-2 パケットの分類

センサーにおいて検知したパケットの分類は、表 5-1 に示す分類に従って集計しています。DoS 攻撃被害観測では、SYN/ACK 及び RST/ACK パケットに加えて、ICMP Echo Reply (以下「0/ICMP」という。)、ICMP Destination Unreachable (以下「3/ICMP」という。) 及び ICMP Time Exceeded (以下「11/ICMP」という。)を集計対象としています。

表 5-1 パケットの分類

章	集計対象	
2 センサーにおけるアクセス検知の観測結果	センサーにおいて検知したアクセス	● TCP SYN パケット ● UDP による問い合わせパケット等 ● 8/ICMP
	目的が不明なパケット	● その他
4 DoS 攻撃被害の観測結果	SYN flood 攻撃による跳ね返りパケット	● TCP SYN/ACK ● TCP RST/ACK
	PING flood 攻撃による跳ね返りパケット	● 0/ICMP
	各種の flood 攻撃による跳ね返りパケット	● 3/ICMP ● 11/ICMP

5-3 不正侵入等の検知

検知された各シグネチャは、表 5-2 に示す分類に従って集約・分析しています。

また、各センサーには、攻撃対象となる可能性のあるサーバ等の機器は一切接続していません。

表 5-2 シグネチャによる検知の分類

分類	説明
DNS	DNS に対するスキャン活動や不正なクエリ等の検知
DoS	DoS 攻撃の可能性のあるパケットの検知
ICMP	ICMP パケットの検知
Scan	インターネット上の各種サービスに対するスキャン活動の検知
Scan (P2P)	スキャン活動のうち、P2P に対する活動の検知
Scan (Password)	スキャン活動のうち、各種サービスの ID・パスワード等に対する活動の検知
UDP spam	UDP を使用したポップアップメッセージ等の検知
VoIP	VoIP に対するスキャン活動等の検知
Worm	インターネットを通じて拡散するワームの検知
Others	上記の分類に含まれないもの