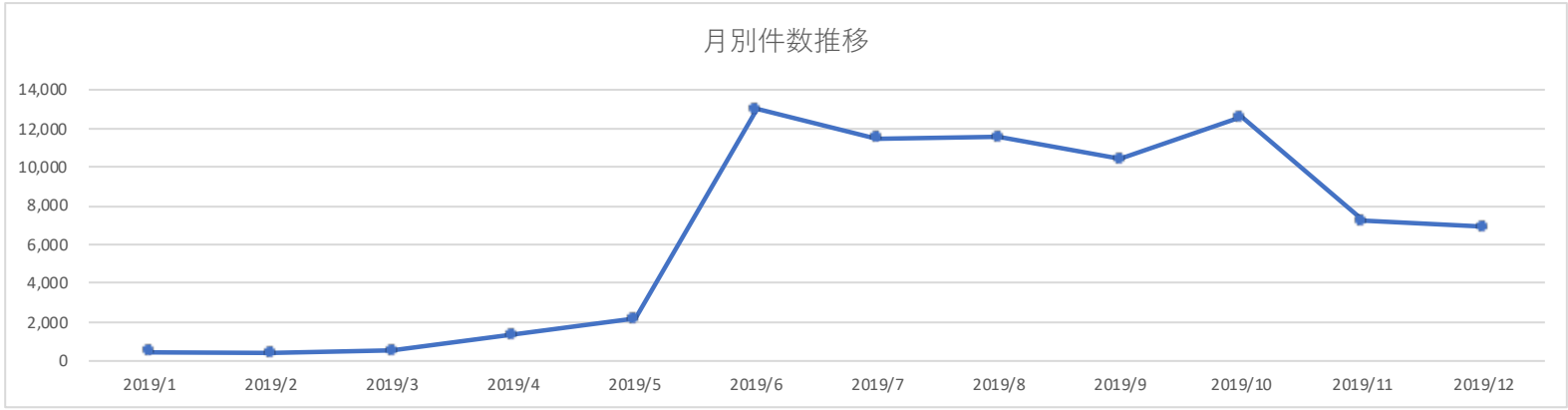
◆SiteGuard Lite 攻撃傾向分析

分析日	2020/1/11
分析期間	2019/1/1 ～ 2019/12/31
対象サイト	www.websec-room.com

◆サマリー

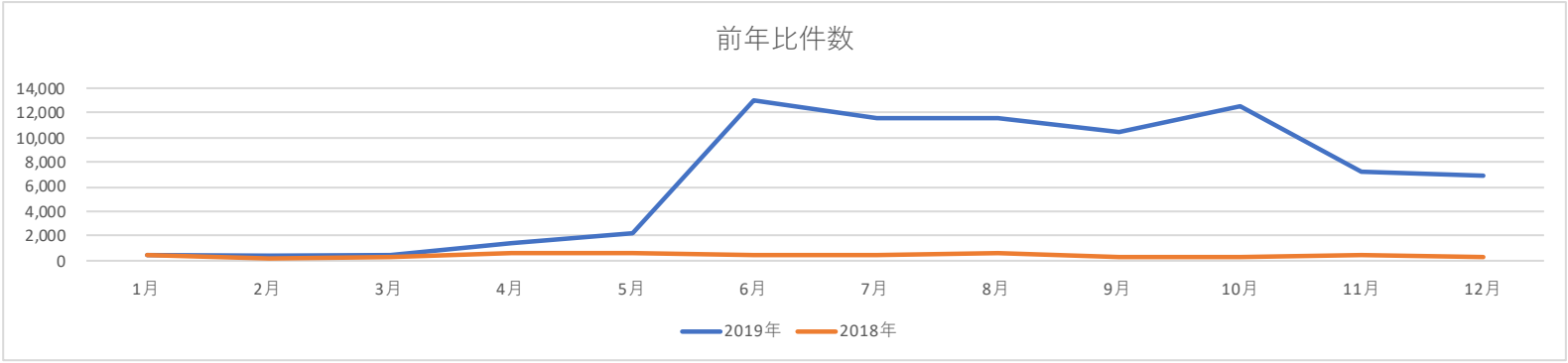
攻撃件数は、1月は約400件で始まったが、4, 5月で上昇を始め、6月には1万件を超えて推移している。
個人サイトへの攻撃件数としてはかなり多い印象。また、前年よりもはるかに攻撃件数が増加している。
攻撃の種類は前半は「SQLインジェクション」が最多で、後半は「OSコマンドインジェクション」の攻撃が最多に変わったがサイト乗っ取りが狙いか。
「クロスサイトスクリプティング」も継続して検出されている。
トピック件数では、phpとjoomuraへの攻撃が継続して検知されている。最新バージョンへのアップデートを推奨。
攻撃元は中国が圧倒的に多い。IPアドレスも分散していたので組織的な攻撃だと推測している。
現状では、WAF(Web Application Firewall) を導入しないでサイト運営は相当リスクが高い。WAFの導入を強く推奨。

◆月別件数推移



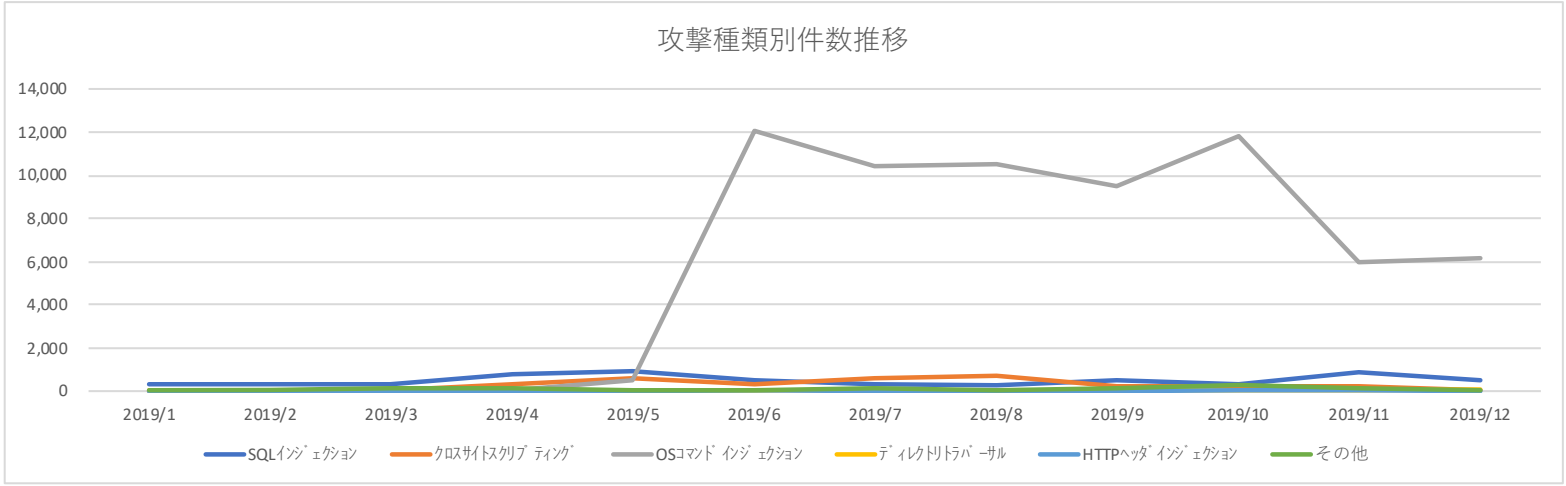
	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12
月別件数	463	414	521	1,370	2,175	13,012	11,491	11,545	10,418	12,599	7,214	6,906

◆前年比件数



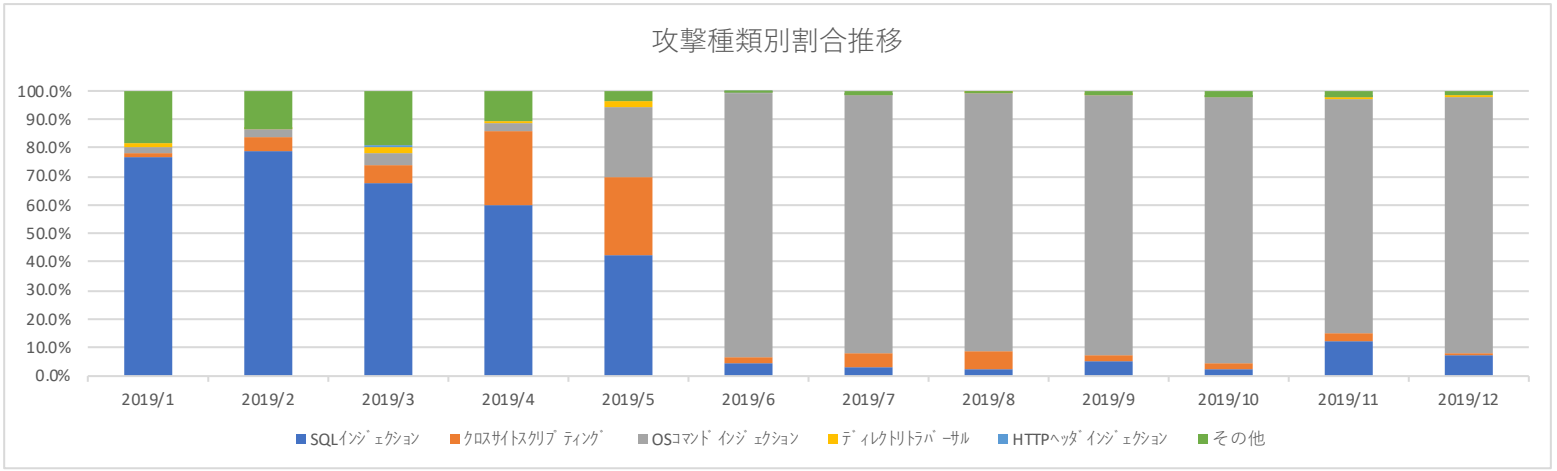
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
2018年	449	186	227	545	571	420	396	620	268	335	453	323
2019年	463	414	521	1,370	2,175	13,012	11,491	11,545	10,418	12,599	7,214	6,906

◆攻撃種類別件数推移



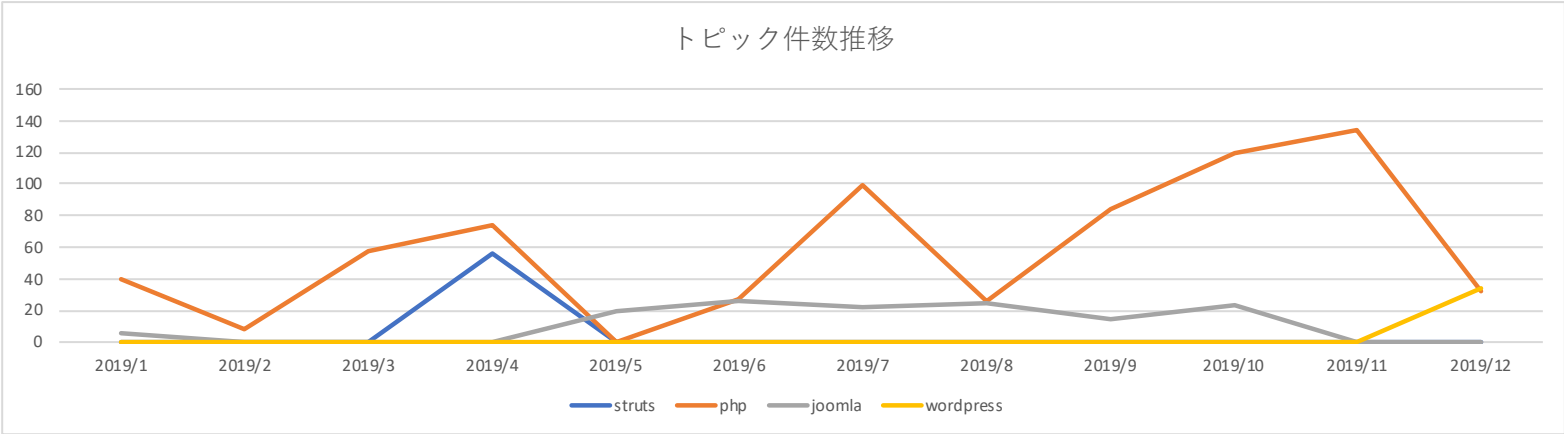
	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12
SQLｲﾝｼﾞｪｸｼｮﾝ	354	326	351	824	924	549	340	272	544	287	873	530
ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞ	7	20	33	355	597	321	552	711	232	245	190	40
OSｺﾏﾝﾄﾞｲﾝｼﾞｪｸｼｮﾝ	10	13	23	35	538	12,059	10,444	10,482	9,497	11,777	5,929	6,182
ﾃﾞｨﾚｸﾄﾘﾄﾗﾊﾞｰｻﾙ	6	1	13	8	35	7	18	4	6	4	41	75
HTTPﾍｯﾀﾞｲﾝｼﾞｪｸｼｮﾝ	0	0	3	0	0	2	3	0	0	1	2	0
その他	86	54	98	148	81	74	134	76	139	285	179	79
合計	463	414	521	1,370	2,175	13,012	11,491	11,545	10,418	12,599	7,214	6,906

◆攻撃種類別割合推移



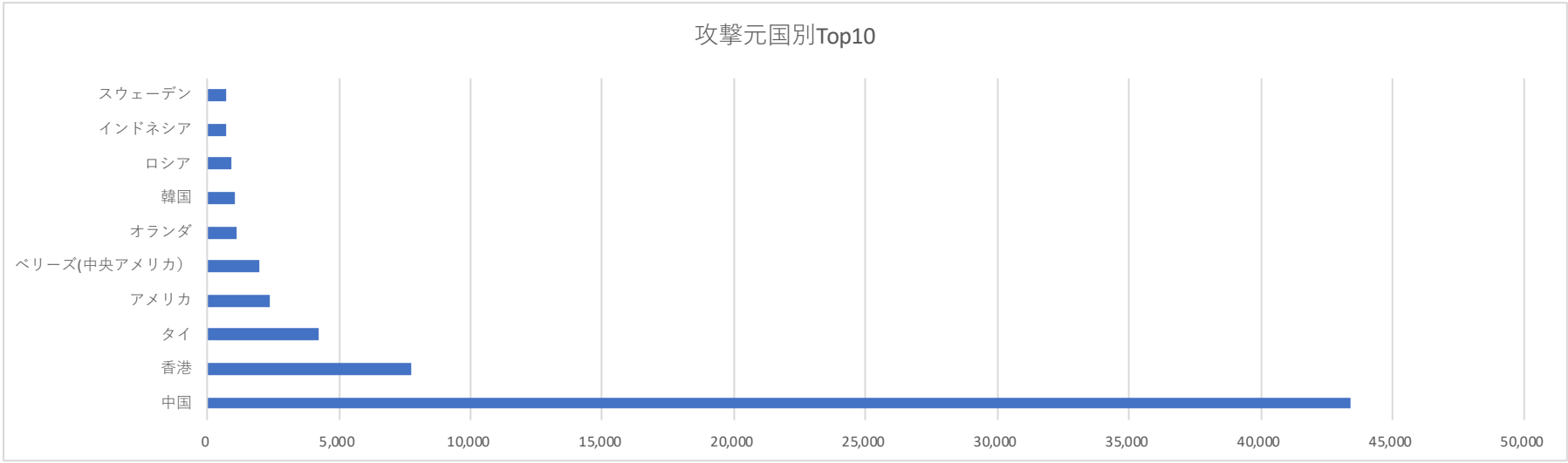
	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12
SQLｲﾝｼﾞｪｸｼｮﾝ	76.5%	78.7%	67.4%	60.1%	42.5%	4.2%	3.0%	2.4%	5.2%	2.3%	12.1%	7.7%
ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞ	1.5%	4.8%	6.3%	25.9%	27.4%	2.5%	4.8%	6.2%	2.2%	1.9%	2.6%	0.6%
OSｺﾏﾝﾄﾞｲﾝｼﾞｪｸｼｮﾝ	2.2%	3.1%	4.4%	2.6%	24.7%	92.7%	90.9%	90.8%	91.2%	93.5%	82.2%	89.5%
ﾃﾞｨﾚｸﾄﾘﾄﾗﾊﾞｰｻﾙ	1.3%	0.2%	2.5%	0.6%	1.6%	0.1%	0.2%	0.0%	0.1%	0.0%	0.6%	1.1%
HTTPﾍｯﾀﾞｲﾝｼﾞｪｸｼｮﾝ	0.0%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
その他	18.6%	13.0%	18.8%	10.8%	3.7%	0.6%	1.2%	0.7%	1.3%	2.3%	2.5%	1.1%
合計	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

◆トピック件数推移



	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12
struts	0	0	0	56	0	0	0	0	0	0	0	0
php	40	8	58	74	0	27	99	26	84	120	134	32
joomla	5	0	0	0	20	26	22	25	15	23	0	0
wordpress	0	0	0	0	0	0	0	0	0	0	0	34

◆攻撃元IPアドレス国別分析



No.	国	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12	合計
1	中国	2	15	14	565	860	7,262	7,891	9,178	5,652	6,494	2,671	2,804	43,408
2	香港			4		22	576	600	620	628	2,591	1,336	1,347	7,724
3	タイ						1,109	584	621	632	653	658		4,257
4	アメリカ	12	50	20	21	13			44	1,271	118	117	684	2,350
5	ベリーズ(中央アメリカ)		217	217	217	217		217	217	217		434		1,953
6	オランダ		4		24	217				217	217	217	217	1,113
7	韓国					508	540							1,048
8	ロシア	217	3		9								674	903
9	インドネシア											69	676	745
10	スウェーデン	2				47					653			702

◆攻撃元IPアドレス国別分析（続き）

No.	国	2019/1	2019/2	2019/3	2019/4	2019/5	2019/6	2019/7	2019/8	2019/9	2019/10	2019/11	2019/12	合計
11	ドイツ	3	4	6		10					662			685
12	マケドニア											673		673
13	インド									45	623			668
14	シンガポール	2		6				601					53	662
15	ベトナム	4								632				636
16	マレーシア									632				632
17	トルコ							601						601
18	アルゼンチン								601					601
19	台湾											557		557
20	セルビア						546							546
21	メキシコ						540							540
22	スペイン			12			478							490
23	パナマ				217								217	434
24	チリ							433						433
25	オーストラリア			6		70				33		33		142
26	フランス	10		18	68								45	141
27	ウクライナ					6						40	58	104
28	ルーマニア				4							77	11	92
29	イギリス			16						55				71
30	日本	10	17			10								37
ー	その他	22	4	21	26	17								90