

ワーム「Blaster/Welchia」の統計情報

情報基盤センターネットワーク運用掛

<https://doi.org/10.15017/1470668>

出版情報：九州大学情報基盤センター広報：学内共同利用版. 3 (3), pp.115-125, 2003-11. 九州大学
情報基盤センター
バージョン：
権利関係：



ワーム「Blaster/Welchia」の統計情報

情報基盤センター ネットワーク運用掛

1 はじめに

8月12日に発見されたワーム「Blaster」は Windows 2000/2003 Server/NT 4.0/XP に存在するセキュリティホール MS03-026 を利用して感染を広げます。セキュリティホールに対して修正パッチが適用されていない Windows OS は攻撃を受け感染し、自らが攻撃者となり他のシステムに対して感染活動を開始します。

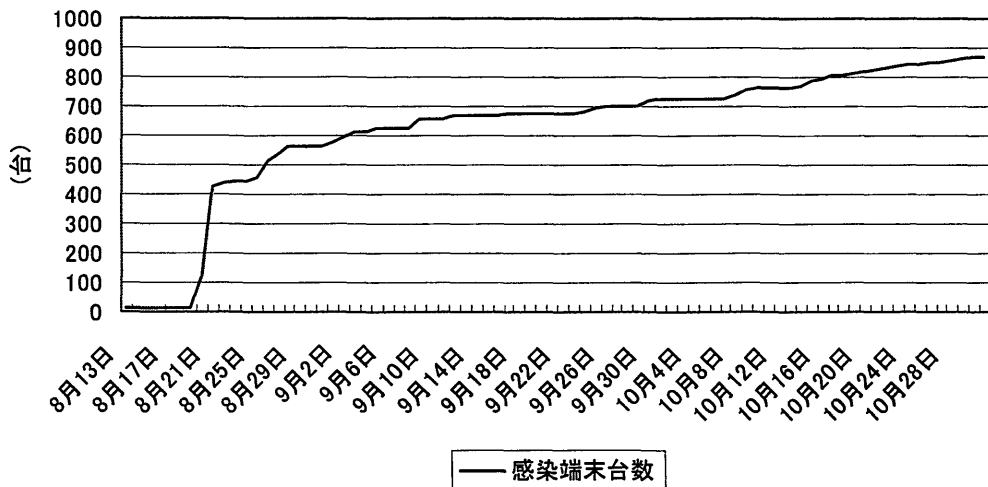
新たに8月18日に発見されたワーム「Welchia」は「Blaster」同様セキュリティホール MS03-026 の脆弱性を利用します。またセキュリティホール MS03-007 も利用しようとしています。このワームは ICMP エコーまたは PING を送信することによって、現在動作中のコンピュータを探して感染するため、このワームの動作中は ICMP トラフィックが増大するのが特徴です。

ワームに感染してしまった場合には、マイクロソフト社が提供する修正プログラム適用サービスである Windows Update 等の手段によりセキュリティホールを修正した後、各ワクチンベンダーから無償配布されている修復用ツールでワームを駆除する方法が有効です。詳しくは本誌の「Blaster ワームの概要とその対策」をご覧ください。

2 学内での感染状況

平成 15 年 10 月 31 日までに学内で「Blaster」または「Welchia」の少なくともどちらかに感染が確認されたホスト数は 868 台となっています。

Blaster/Welchia 感染ホスト数の推移



3 各支線毎の「Blaster/Welchia」感染端末台数と5回以上監視装置のログに載った端末台数（ログは1日区切り）

（平成15年10月31日現在）

サブネット	感染台数	5回以上ログに載った台数	敷設場所
7	6		情報基盤センター
11	45		情報基盤センター(教育用システム)
12	56	1	情報基盤センター教育用システム分室(経済学部)
13	61		情報基盤センター教育用システム分室(130番教室)
15	14	1	医学部附属統合教育研究実習センター、専門大学院研究棟 情報基盤センター教育用システム分室(医学部)
16	12	1	大学院システム情報科学研究院(情報工学) 大学院システム情報科学府(情報工学) 工学部電気情報工学科
20	6		大学院システム情報科学研究院 (電子デバイス工学・電気電子システム工学) 大学院システム情報科学府 (電子デバイス工学・電気電子システム工学) 工学部電気情報工学科
21	5		大学院システム情報科学研究院 (電子デバイス工学・電気電子システム工学) 大学院システム情報科学府 (電子デバイス工学・電気電子システム工学) 工学部電気情報工学科
22	10		大学院システム情報科学研究院(情報工学) 大学院システム情報科学府(情報工学) 工学部電気情報工学科
23	70		情報基盤センター教育用システム分室(136番教室)
25	1		新1号館、課外活動施設、六本松地区21世紀交流プラザ 附属図書館六本松分館
28	6		4号館、新4号館
33	2	1	大学院システム情報科学研究院(情報工学) 大学院システム情報科学府(情報工学)

サブネット	感染台数	5 回以上ログに載った台数	敷設場所
34	3		大学院システム情報科学研究院(情報理学)
			大学院システム情報科学府(情報理学)
37	3		大学院システム情報科学研究院附属超伝導科学研究センター
			電力実験室
38	2		大学院システム情報科学研究院、大学院システム情報科学府
			工学部電気情報工学科、システム情報講義棟
50	2		六本松本館4F～6F
52	3		基礎研究B棟1F～2F、基礎研究C棟
53	3		基礎研究A棟2F
54	3		基礎研究A棟3F
55	11		臨床研究棟A棟1F～2F
56	12		臨床研究棟A棟5F～6F
57	7		臨床研究棟B棟1F～2F
58	4	1	臨床研究棟B棟3F～4F
120	5		大橋キャンパス
121	2		大橋キャンパス
128	6		中央図書館(Fast Ethernet)
130	2		箱崎理系地区 21 世紀交流プラザ(事務局)
131	1		国際交流会館(情報サロン)
132	1		学際教育研究交流棟(リセウム悠遠)
134	6	1	大学院工学研究院(建設デザイン)
			大学院工学府(建設システム工学)
135	8		大学院工学研究院(航空宇宙工学)
			大学院工学府(航空宇宙工学)
			工学部機械航空工学科(航空宇宙工学)
136	13		大学院工学研究院(海洋システム工学)
			大学院工学府(海洋システム工学)
			工学部地球環境工学科(船舶海洋システム工学)
137	11		大学院工学研究院(航空宇宙工学)
			大学院工学府(航空宇宙工学)
			工学部機械航空工学科(航空宇宙工学)
138	1		大学院工学研究院(応用化学)、大学院工学府(材料物性工学)
			工学部物質科学工学科(応用化学・機能物質化学)

サブネット	感染台数	5回以上ログに載った台数	敷設場所
139	12		大学院工学研究院(化学工学)
			大学院工学府(化学システム工学)
			工学部物質科学工学科(化学プロセス・生命工学)
140	11	1	先導物質化学研究所
141	4	2	知能機械実験室、高速流実験室、機械工学科実験室
143	1	1	大学院工学研究院(エネルギー量子工学)
144	7	1	大学院人間環境学研究院(都市・建築学)、工学部建築学科
			大学院人間環境学府(都市共生デザイン／空間システム)
145	10	1	大学院工学研究院(知能機械システム)
			大学院工学府(知能機械システム)
			工学部機械航空工学科(機械工学)
146	8	2	大学院工学研究院(知能機械システム)
			大学院工学府(知能機械システム)
			工学部機械航空工学科(機械工学)
147	14		大学院工学研究院(機械科学)、大学院工学府(機械科学工学)
			工学部機械航空工学科(機械工学)、工学部材料強弱学教室
148	4		生協本部・倉庫
149	4		大学院工学研究院(材料工学)
			大学院工学府(物質プロセス工学)
			工学部物質科学工学科(材料科学工学)、超高压電子顕微鏡室
152	6		大学院工学研究院(地球資源システム工学)
			大学院工学府(地球資源システム工学)
			工学部地球環境工学科(資源工学)
153	7		大学院工学研究院(エネルギー量子工学)
			大学院工学府(エネルギー量子工学)
			工学部エネルギー科学科(エネルギー科学)
154	7		ベンチャー・ビジネス・ラボラトリー
155	4		工学研究科共同研究棟
157	3		産学連携棟(C&C)
158	1		大学院数理学研究院大学院数理学府
			理学部数学科、(工学部本館)
159	2		総合研究博物館、記念講堂
162	2		宙空環境研究センター

サブネット	感染台数	5 回以上 ログに載 った台数	敷設場所
163	2		アイソトープ総合センター(箱崎地区実験室)
165	1		大学院数理学研究院、大学院数理学府 理学部数学科、(理学部本館・3号館・4号館)
166	3		大学院理学研究院(地球惑星科学) 大学院理学府(地球惑星科学)、理学部地球惑星科学科
167	3		大学院理学研究院(化学) 大学院理学府(分子科学・凝縮系科学)、理学部化学科
170	2		理学部等事務部、学生交流プラザⅢ
172	1	1	人工分子集合組織体研究棟
175	6	1	先端科学技術共同研究センター4F～6F
178	10		応用力学研究所本館棟1F・2F・4F・5F 応用力学研究所3F計算機室、材料実験棟1 材料実験棟2、流体工学実験棟、深海機器力学実験棟 地球大気動態シミュレーション実験棟
179	4		応用力学研究所本館棟3F・5F・6F、海洋力学実験棟 大気力学実験棟、海洋環境実験棟、大型計測機器格納庫 応用力学研究所附属力学シミュレーション研究センター
180	14		先導物質化学研究所(中央棟・北棟) エネルギー変換研究棟、光高温実験棟
181	1	1	先導物質化学研究所(南棟)、総理工A棟、NMR解析棟
182	4		健康科学センター
183	23		総理工D棟、高速流動実験棟
188	11	2	総理工G棟
191	2		先導物質化学研究所(中央棟・北棟)、超音速ターボ実験室
192	3		先端科学技術共同研究センター1F～3F
197	14	1	農学部4号館、熱帯農学研究センター、実験研究センター
198	14		農学部7号館、干拓水槽上屋、生物機能制御学実験室 森林圏環境資源科学実験室
200	14	3	農学部5号館
201	15	7	農学部1号館、給水センター(工営掛)
202	19	4	留学生センター(国際ホール・分室を含む)、韓国研究センター 箱崎理系地区 21 世紀交流プラザⅡ(事務局)
203	19	2	農学部2号館

サブネット	感染台数	5 回以上 ログに載 った台数	敷設場所
204	1	1	農学部防音講義室、箱崎理系地区 21 世紀交流プラザⅡ(農)
207	6		農学部3号館1F～3F
208	5		医学部附属病院外来西側
210	4	1	医学部附属病院中央・東病棟
211	11	2	医学部附属病院検査部・手術部・西病棟
212	4	1	(新)医学部附属病院診療棟・病棟
213	8	1	基礎研究B棟3F～4F
216	8	1	医療技術短期大学部2・体育館
217	3		生体防御医学研究所
218	1		生体防御医学研究所(本館・別館・プレハブ研究棟)
			専門大学院研究棟
220	4	1	基礎研究A棟1F
221	11		附属図書館医学分館
222	7	4	臨床研究棟A棟3F～4F
223	6	1	特高変電所(電気掛)、給水センター
			同窓会館・外国人研究員等宿泊施設
			事務棟(医学部・医学部附属病院)、ボイラー棟(機械掛)
			工営掛事務室、医学部附属病院中央診療棟(中央監視室)
224	4	1	臨床研究A・B共通棟
225	7	2	臨床研究棟B棟5F～6F
226	5	1	薬学部1号館、薬学部1号館管理棟
227	2		薬学部2号館
229	9	1	歯学部臨床研究棟
233	7		生体防御医学研究所附属遺伝情報実験センター
234	1	1	健康科学センター・医学部臓器機能医学専攻・生活協同組合
235	10	3	歯学部本館・研究棟、歯学部プレハブ研究棟
236	3		コラボ・ステーション(歯・薬・医)
238	4		コラボ・ステーションⅡ
241	5	2	大学院人文科学研究院、大学院人文科学府、文学部
			(文・教育)研究棟、(文・教・人環)研究棟
242	8	1	大学院法学研究院・法学府、法学部、(法・経)演習棟
			(法・経)研究棟、箱崎文系地区 21 世紀交流プラザ(法)

サブネット	感染台数	5 回以上 ログに載 った台数	敷設場所
243	8		大学院人間環境学研究院(教育学)
			大学院人間環境学府(発達・社会システム)
			教育学部、(文・教)研究棟、(文・教育・人環)研究棟
244	7		大学院人間環境学研究院(人間科学)、(文・教・人環)研究棟
			大学院人間環境学府(人間共生システム・行動システム)
			認知心理学実験室、(文・教)研究棟
			大学院人間環境学府附属発達臨床心理センター
245	6		法文系事務、箱崎文系地区 21 世紀交流プラザ(事務局)
			文系講義棟、学生控室、大講義室、中講義室
			文系図書室(文・教・法・経)

4 ワーム「Blaster/Welchia」の感染が警告されていない支線

セグメント	敷設場所
1	情報基盤センター
5	情報基盤センター(情報サロン・高速検索システム)、高原農業実験実習場
6	情報基盤センター(旧:総合情報伝達システム運用センター) 国際交流会館(1F事務室)
8	情報基盤センターサービス2(GbE)
9	情報基盤センターサービス1(FDDI)
10	情報基盤センター(研究部・情報支援技術部)
14	情報基盤センター教育用システム分室(農学部)
17	大学院システム情報科学研究院(情報工学)、大学院システム情報科学府(情報工学) 工学部電気情報工学科
18	大学院システム情報科学研究院(知能システム学) 大学院システム情報科学府(知能システム学) 工学部電気情報工学科
24	大学院システム情報科学研究院(情報理学)、大学院システム情報科学府(情報理学) 工学部電気情報工学科
26	大学院数理学研究院、大学院理学府、理学部数学科 六本松3号館3F、4号館3F、本館2Fの一部
29	六本松2号館、3号館
30	六本松本館、1号館、比較社会文化研究科棟
31	六本松1号館3F
32	大学院システム情報科学研究院(知能システム学) 大学院システム情報科学府(知能システム学)
35	大学院システム情報科学研究院(知能システム学) 大学院システム情報科学府(知能システム学)
36	大学院システム情報科学研究院(電気電子システム工学) 大学院システム情報科学府(電気電子システム)、工学部電気情報工学科
39	大学院システム情報科学研究院、大学院システム情報科学府 工学部電気情報工学科
40～47	セキュリティ強化ネットワーク(事務用)
48	農学部6号館、農林生物物理研究棟、大学院農学研究院附属生物的防除研究施設 健康科学センター箱崎分室

セグメント	敷設場所
49	情報基盤センター、六本松分室等
51	六本松本館、1号館、2号館、3号館、4号館
129	中央図書館(FDDI)
133	保存図書館
142	大学院工学研究院(建設デザイン)、大学院工学府(都市環境システム工学) 工学部地球環境工学科(建設都市工学・水工)、西部地区自然災害資料センター
150	大学院工学研究院(応用化学)、大学院工学府(物質創造工学) 工学部物質科学工学科(応用化学・分子システム工学)
151	大学院システム情報科学研究院(電子デバイス工学・電気電子システム工学) 大学院システム情報科学府(電子デバイス工学・電気電子システム工学) 工学部電気情報工学科
156	工学部等事務部
160	理学部原子核実験室、理学部原子核実験室(HEPNET)
161	大学院理学研究院(生物科学)、大学院理学府(生物学科)、理学部生物学科
168	大学院理学研究院附属地震火山観測研究センター
164	大学院理学研究院(物理学)、大学院理学府(基礎粒子系科学・凝縮系科学) 理学部物理学
169	システム生命科学府棟
171	大学院理学研究院附属地震火山観測研究センター(箱崎)
173	大学院理学研究院(生物科学)、大学院理学府(生物学科)、理学部生物学科
174	コラボ特殊実験棟
176	総合理工学府等事務部、(共通管理棟)、(福利厚生施設)
177	応用力学研究所附属炉心理工学研究センター、(トライアム実験棟)
184	総理工C棟
185	総理工F棟
186	総理工H棟
187	中央分析センター
189	応用力学研究所本館棟1F・2F・4F・5F、応用力学研究所3F計算機室 材料実験棟1、材料実験棟2、流体工学実験棟、深海機器力学実験棟 地球大気動態シュミレーション実験棟
190	応用力学研究所附属力学シュミレーション研究センター
193	応用力学研究所6F
194	総理工 C棟～E棟(講義室)

セグメント	敷設場所
195	電離気体実験施設、マイクロ波計測実験棟
199	留学生センター2F～4F
205	農学部附属演習林
206	農学部附属農場
209	大学院医学研究院・医学系学府附属動物実験施設
214	医学部血液検査室、アイソトープ総合センター(病院地区実験室)、RI総合学生実習室
215	医療技術短期大学部1
228	薬学部研究棟
230	医学部附属病院医療情報部、(新)医学部附属病院診療棟・病棟
231	歯学部附属病院(外来棟・東棟)、歯学部臨床研究棟
232	薬学部1号館、薬学部1号館管理棟
237	生体防御医学研究所附属遺伝情報実験センター
240	大学院経済学研究院・経済学府、経済学部、(法・経)演習棟
246	中央体育館、課外活動共用施設、研修センター、就職情報室 国際交流会館(情報サロン)

5 Windows Update について

Windows Update とは Windows 98/2000/XP で採用されている、コンピュータを最新の状態に保つようにする Windows のオンラインの拡張機能のことです。マイクロソフト社が提供している Windows 及び同社提供のインターネット関連ソフトのセキュリティホール修正パッチや最新の追加機能を一覧し、必要なものをその場でインストールできる仕組みになっています。Windows Update を利用するには

URL: <http://windowsupdate.microsoft.com>

を指定する方法の他に、「スタート」ボタンや Internet Explorer のリンクバーから

「Windows Update」をクリックすることで「Microsoft Windows Update」というサイトに接続できます。サイトに接続後、コンピュータの現在の状況を確認するために「更新をスキャンする」をクリックすると、利用可能な更新項目を検索し始めます。しばらくすると「お使いのコンピュータ用の重要な更新が*個見つかりました。」と表示されます。必要な更新を、自己判断でダウンロード・インストールしてください。ダウンロード・インストールは、ウィザードに従って最後まで進むと、自動的に始まり完了します。

Windows Update を定期的に行うことで Windows をセキュリティの高い、最新の状態に保つことが出来ます。特にセキュリティに関する修正は非常に重要で、Windows などの脆弱性を狙ったウイルスなどからコンピュータを保護することができます。Windows

Update をまったく行わないままネットワークに接続していた場合、ワームに攻撃されたり、情報が漏洩したり、外部からハッキングを受けたりする危険性が高くなります。そのため Windows Up date Web サイトをこまめにチェックすることが望ましいです。

6 まとめ

ワーム「Blaster/Welchia」が発見されて三ヶ月以上経過しましたが依然として新規感染が後を絶えないのが現状です。ワームに感染した端末を放置した場合、同一支線内で新規感染が続く傾向にあります。ワーム感染後に適切な処置が施されず放置されている端末が存在する支線では、支線内の他の端末にセキュリティパッチを確実に適用しないと被害を広げる結果となります。

教育用システムでは、全ての端末が一つの共通設定の OS であるため、セキュリティパッチを適用していない場合は、全ての端末がワームに感染するため被害数が多くなっています。

サーバなどで NAT 機能を利用されている場合には、プライベートネットワーク内に感染端末がある場合でも、監視装置にはサーバの IP アドレスしかヒットしないので本当にワームに感染した端末を発見するのは困難になります。各支線で数台連続警告を受けている端末の中には NAT 機能を提供しているものが含まれていると思われます。

情報サロンなどでワームに感染したパソコンをネットワークに繋ぐ場合、監視装置には DHCP 機能によって配布される IP アドレスがヒットするのでワーム感染端末特定が困難になる傾向があります。

爆発的にネットワーク内で増殖するワームですが、ワームの感染が確認されていない優秀な支線も数多くあります。それらの支線では、日頃から Windows Update 等で脆弱性への対応、またはファイアウォール等で特定のポートを使用した通信を遮断するなどのワーム対策が万全にされていると思われます。

これからもワーム「Blaster/Welchia」の亜種や、新型のウイルスが登場することが考えられます。今回のワーム感染結果を教訓として、今後のウイルス対策を役立ててみては如何でしょうか。