

[04_01]九州大学情報基盤センター広報 : 学内共同 利用版表紙奥付等

<https://hdl.handle.net/2324/1470669>

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. 4 (1), 2004-03. 九州大学情報基盤センター
バージョン :
権利関係 :

学内ウイルス・セキュリティ被害状況

情報基盤センターネットワーク運用掛
2003年8月～2003年11月

1. ウイルス感染系 (2003年8月～2003年11月)

ウイルス感染系	8月	9月	10月	11月
Blaster または Welchia	563	207	165	86
Sobig.F	3	3		
Slammer	1	1		
Nimda	1			
Microsoft SQL 関連のワームに感染	1			
Klez		1		
Swen			1	
UDP port 137 番(NetBIOS)へパケット送出			1	
WOMANIZ.Bの亜種に感染				1
メールを大量に送信するウイルスに感染				1
月別総数	569	212	167	88

2. セキュリティ被害、不正利用系 (2003年8月～2003年11月)

セキュリティ被害、不正利用系	8月	9月	10月	11月
https ポート(443)に対する大量の攻撃パケットを検出	1			
Open SSL の脆弱性を利用して侵入される	1			
spam メール送信	1			
apache mod ssl (Open SSL) の脆弱性を突かれて不正侵入される		1		
書き込み可能な anonymous ftp server を運用		1		
TCP (smtp) 25 ポートにパケットを送出される		1		
大量の SMTP 接続を観測			12	
月別総数	3	3	12	0

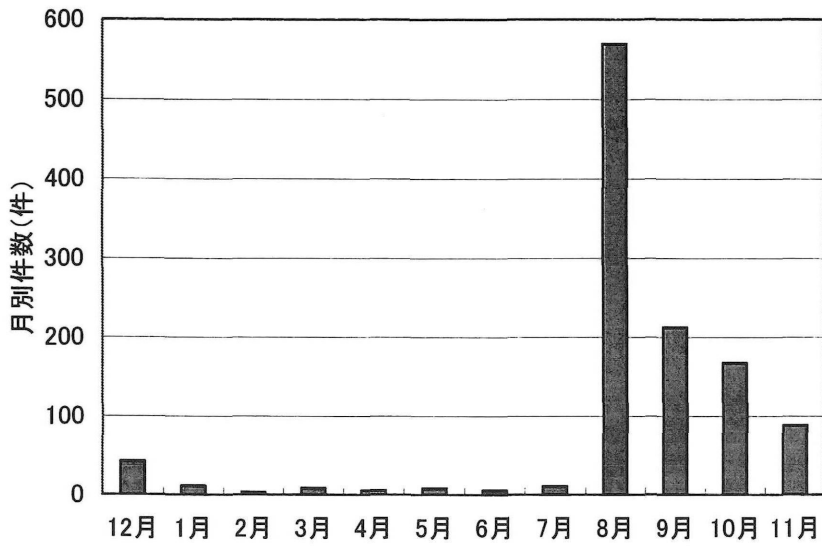
3. 全体的な傾向

8月に発生した Blaster と Welchia は一部の支線を除き爆発的に感染拡大したが、月を追うごとに感染数は減少している。

10月の「大量の SMTP 接続」は不正侵入を受けた1台の端末からのスパムメールを複数の PC がリレーしたことにより起こっている。

メールの添付ファイルを実行することによって活動を開始するタイプのウイルスが数種類確認できる。

4. ウイルス感染数の推移 (2002年12月～2003年11月)



5. セキュリティ被害、不正利用件数の推移 (2002年12月～2003年11月)

