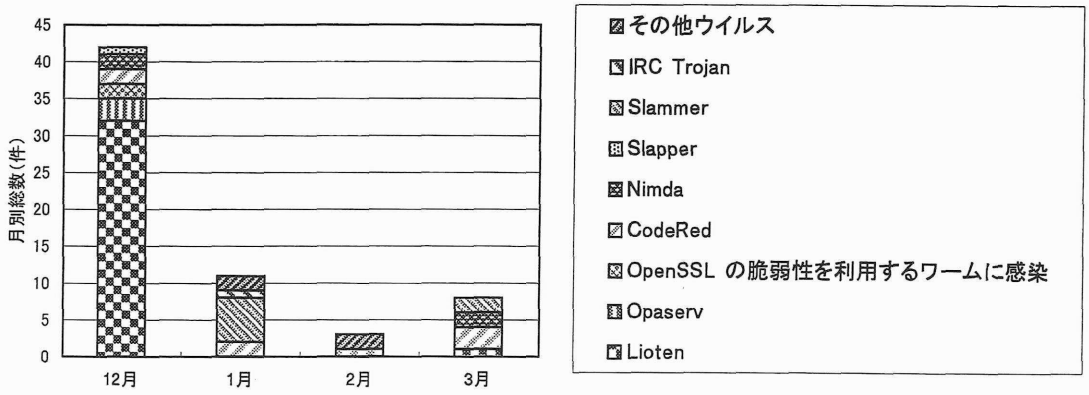
[03_02]九州大学情報基盤センター広報 : 学内共同利用版表紙奥付等

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 (2), 2003-07. 九州大学情報基盤センター
バージョン：
権利関係：

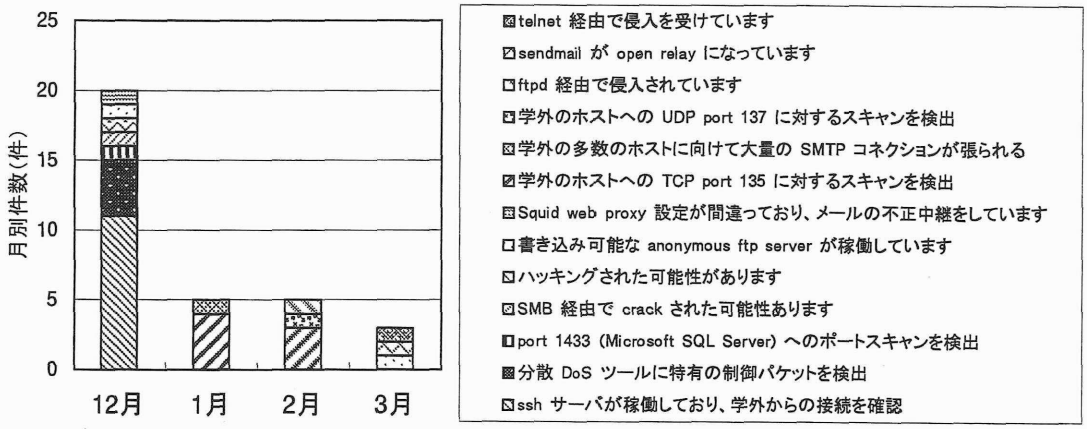
学内ウイルス・セキュリティ被害状況

情報基盤センターネットワーク運用掛

1. ウイルス感染系 (2002年12月～2003年3月)



2. セキュリティ被害、不正利用系 (2002年12月～2003年3月)



3. 全体的な傾向

1月25日午後に Microsoft SQL Server 2000 の脆弱性をねらうワーム "Slammer"に6台の端末が感染。"CodeRed"は毎月数件ほど感染報告がある。

12月に確認されたウイルス "Lioten"は、Windows NT/2000/XP においてパスワードを設定していない場合に感染するため、多数被害がでたと思われる。

1月2月は、port 135 へのスキャンが目立った。port 135 は Windows の リモート プロシージャ コール で使われるポートで、Windows 2000 SP3 に対して DoS を起こす脆弱性が知られているので、それを狙うウイルスに感染している可能性があります。

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
2002年12月～2003年3月

ウイルス感染系	12月	1月	2月	3月	4月
Lioten	32			1	
Opaserv	3				1
OpenSSL の脆弱性を利用するワームに感染	2				
CodeRed	2	2	1	3	2
Nimda	2			2	
Slapper	1				
Slammer		6		2	1
IRC Trojan		1			
BKDR_DELODER.A					1
その他ウイルス		2	2		
月別総数	42	11	3	8	5

セキュリティ被害、不正利用系	12月	1月	2月	3月	4月
ssh サーバが稼働しており、学外からの接続を確認	11				1
分散 DoS ツールに特有の制御パケットを検出	4				
port 1433 (Microsoft SQL Server) へのポートスキャンを検出	1				
SMB 経由で crack された可能性あります	1				
ハッキングされた可能性があります	1				
書き込み可能な anonymous ftp server が稼働しています	1			1	
Squid web proxy 設定が間違っており、メールの不正中継をしています	1				
学外のホストへの TCP port 135 に対するスキャンを検出		4	3		
学外の多数のホストに向けて大量の SMTP コネクションが張られる		1			
学外のホストへの UDP port 137 に対するスキャンを検出			1		
ftpd 経由で侵入されています			1		
sendmail が open relay になっています				1	
telnet 経由で侵入を受けています				1	
Solaris の /bin/login に存在する脆弱性を telnet 経由で突かれ侵入					2
非常に大量の攻撃パケットが学外に出力されています					1
Microsoft IIS の脆弱性を攻撃する通信が大量に送信されています					1
月別総数	20	5	5	3	5