

## ウイルス解析報告書

ウイルス名	W32/SQLSlammer (W32.SQLExp.Worm, SQL_Overflow, WORM_SQL1434.A)
プログラム名及び容量 (添付ファイル名)	ファイルとして存在しない。また活動の過程で環境にファイルを書き込むこともしない。実行コードのサイズは376バイトである。
種別	ワーム (32ビットWindowsプログラム)
プログラム言語:	アセンブラ
発症環境	Microsoft SQL サーバー 2000が稼働し、セキュリティホールMS02-039のパッチが適用されていないサーバーマシン、または Microsoft Office 2000(Access2000)のSQL Server 2000 Desktop Engineがインストールされているマシン
発見日時	2003年1月25日未明 (日本時間で1月25日14時頃)
発見場所(発信地)	米国、イギリス、韓国その他(発信地は不明)
危険性	かなり高い。5段階で4ないし4.5。ワームの活動によりネットワークトラフィックが異常に増加し、通信が困難または不能になる可能性がある。
発症条件	Microsoft SQL サーバー 2000が稼働し、セキュリティホールMS02-039のパッチまたはサービスパック3が未適用 Microsoft Office 2000(Access2000)のSQL Server 2000 Desktop Engineがインストールされ、修正プログラムが未適用
ウイルスの活動、影響	このワームは脆弱性があるMicrosoft SQL サーバー 2000またはMicrosoft Desktop Engine 2000が動作しているマシンに感染する。 <a href="http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS02-039.asp">http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS02-039.asp</a>  感染したマシンは他のランダムに選んだマシンのポート1434を攻撃し、侵入・感染する。これを繰り返すことによって感染を拡大する。  ワームに感染すると大量の攻撃が行われるため、ネットワークが遮断される、または著しくアクセス速度が低下することがある。  ワームはメモリに存在し、ファイルとしての実体はない。  このワームに破壊的な発病ルーチン等は存在しない。
被害の規模	世界的規模でインターネットの通信速度が1月25日未明(GMT)より著しく低下し、これが終日続いた。正確な数値等は現時点では不明。(2003年1月27日)
亜種、変種の有無	現時点では確認されていない
ウイルス動作概要	ワームは実行されるとスタックを初期化する。 ワームはws2_32.dllとkernel32.dllをロードする。 ワームはkernel32.dllのGetTickCountのアドレスを取得して、GetTickCountを呼び出す。 ワームはGetTickCountで取得した時間を攻撃対象のIPアドレスの初期値とする。 ワームはws2_32.dllのsocketのアドレスを取得して、socketを呼び出してUDPでソケットを作成する。 ワームはws2_32.dllのsendtoのアドレスを取得する。 ワームは1つ前の攻撃対象のIPアドレスから次の攻撃対象のIPアドレスを演算によって求める。 ワームはsendtoを呼び出して攻撃対象のIPアドレスのポート1434に376バイトのワームを送信する。 ワームはIPアドレスを求める演算に戻って攻撃を繰り返す。
感染・発症防止方法	SQL Server 2000 Service Pack 3を適用していない場合はこれを適用する。 SQL Server 2000 Desktop Engine(MSDE2000)の場合は修正プログラムを適用する。
ウイルスの駆除方	< 確認 > パッチを適用していないMicrosoftのSQLサーバを動作させており、ネットワークが異常に遅いときには感染している可能性がある。 確認のためにはタスクマネージャー等でSERVER.EXEのCPU占有率を確認し、通常と比較して明らかに高ければいったんシャットダウンして再比較する。

法	< 駆除 > <a href="#">SQL Server 2000 Service Pack 3</a> を用意したのち、サーバーをいったんシャットダウンする。 再起動後、ネットワーク接続を解除した状態でサービスパックを適用する。
その他	報告書作成 : 2002年1月27日現在

W32/SQLSlammer フローチャート

