

マイクロソフト Windows の脆弱性を狙ったワームの発生に関する注意喚起

(その2)

～ 18 日月曜日の朝に要注意～

平成 15 年 8 月 16 日

経済産業省

Microsoft Windows^(注1)の脆弱性(MS03-026)を利用したワーム(通称:Blaster(ブラスター)ワーム)^(注2)の被害拡大防止のため、経済産業省は、以下の「四カ条」(別紙「企業ユーザにおける Blaster(ブラスター)ワーム対策 四カ条」)を、情報サービス産業協会(JISA)に対して、協会の会員を通じ、ユーザ企業への注意喚起として徹底させるよう要請しました。あわせて、広く一般ユーザの方におかれても、十分ご注意くださいますようお願いいたします。

企業ユーザにおける Blaster(ブラスター)ワーム対策 四カ条

～ 18日月曜日朝に要注意～

【ユーザへのお願い】

- (1) コンピュータの電源はシステム担当者の指示を得てから投入する

【企業のシステム担当者へのお願い】

- (2) すべてのユーザに感染の危険性を事前に知らせる
- (3) ワームの侵入・拡大を防ぐようネットワークを設定する
- (4) ワームの駆除と感染予防を行う

また、個人ユーザの方におかれましても、以下の「三カ条」にご留意いただき、対策を徹底していただきますようお願いいたします。

個人ユーザにおける Blaster(ブラスター)ワーム対策 三カ条

- (1) このワームに感染しているかどうかを確認する
- (2) 感染している場合は、ワクチンソフト(駆除ソフト)を入手してワームを駆除するとともに、マイクロソフト社が配布する修正プログラムを利用して脆弱性(欠陥)を埋める
- (3) 感染していない場合は、マイクロソフト社のソフト(OS)を最新のバージョンにアップデートする

詳細は、情報処理振興事業協会セキュリティセンター(IPA/ISEC)の、以下のページを参照してください。

<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>

Blaster ワームの感染被害等の状況は、8月16日午後4時現在、

- 特に個人ユーザにおける感染被害が引き続き拡大(下記参考参照)し、TCP135 番ポートに対するアクセスは、高水準のまま増減を繰り返しているとの観測データがあるものの、
- IPA 及び JPCERT コーディネーションセンターからの報告によると、ネットワーク全体について、トラフィックに著しい過負荷の発生等は見られない

という状況です。

一方で、8月18日(月)は、多くの企業においてお盆明けの仕事開始日となることから、ここ数日に比べて、多くのコンピュータが起動されることが予想され、その際、Blaster ワームに感染していたり、脆弱性対策がなされていないコンピュータがあると、被害の拡大を引き起こす危険があると考えられます。

したがって、経済産業省としては、

- (1) 引き続き、個人ユーザを中心とした 感染の防止と 感染駆除の徹底の対策を行うとともに、
- (2) 企業ユーザ(企業に勤める個人及びシステム担当者)に対して、18日月曜日に向けての対策を徹底するよう呼びかけることとしたものです。

(参考) 8月16日午後4時までの感染被害等の状況

(1)情報処理振興事業協会(IPA)セキュリティセンターへの届出・相談件数

累計 1,570件

8/13	200件	累計	200件
8/14	400件	累計	600件
8/15	600件	累計	1,200件
8/16	370件	累計	1,570件 (午後4時まで)

(2)当省への届出・相談件数

累計 720件

8/14	100件	累計	100件
8/15	440件	累計	540件
8/16	180件	累計	720件 (午後4時まで)

(3)その他ネット等の状況

IPAセキュリティセンター及びJPCERTコーディネーションセンターからの報告によると、以下のような状況(本日午後4時現在)。

ネットワークのトラフィックに特に過負荷の発生等は見られない。

IPA観測システムによるポート135へのアクセス状況は、以下の通りです。

- ・8/12 本ワームによるアクセス増加の兆
- ・8/13 通常比較400～500%程度のアクセス数を検知
- ・8/14 一時的にアクセス数が通常時の200%程度まで低減
- ・8/15 通常時の500～600%に増加
- ・8/16 大きな増減なく推移。(午前9時)

やや減少傾向だが、収束に向かっているとは言えない。(午後 1 時)
増減を繰り返し、引き続き高水準で推移(午後 4 時)

【 問い合わせ先 】

経済産業省 商務情報政策局 情報セキュリティ政策室

担当 : 山崎、若畑、赤松

E-Mail: it-security@meti.go.jp

電話 : 03 - 3501 - 0397 (直通)

FAX: 03 - 3501 - 6639

(注1)対象となるのは、以下の Microsoft Windows オペレーティングシステム(OS)を搭載しているコンピュータ。

Microsoft Windows NT Server4.0

Microsoft Windows NT Server4.0, Terminal Server Edition

Microsoft Windows NT Workstation4.0

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows Server 2003

(注2)「ワーム」とは、コンピュータウイルスの一種で、自己増殖を繰り返す性質を持つもの。したがって、「ワーム」が、あるコンピュータに感染すると、自動的に他のコンピュータへの感染を試みるため、感染を食い止めないと、ねずみ算式に被害が拡大してしまう。

なお、この Microsoft Windows の脆弱性 (MS03-026) は、既に発見され、修正プログラムが配布されているもの。「Windows RPC インタフェースの脆弱性への注意喚起」(http://www.meti.go.jp/policy/netsecurity/win_rpc.html) 参照。

企業ユーザにおける Blaster(ブラスター)ワーム対策 四カ条

別紙

～ 18日月曜日朝に要注意～

2003.8.16 経済産業省

8月18日(月)は、多くの企業においてお盆明けの仕事開始日となることから、ここ数日に比べて、多くのコンピュータが起動されることが予想されます。その際、Blaster ワームに感染していたり、脆弱性対策がなされていないコンピュータがありますと、被害の拡大を引き起こす危険があります。このような事態を回避するため、企業のユーザ及びシステム担当者は、細心の注意を払っていただけますようお願いいたします。

【ユーザへのお願い】

(1) コンピュータの電源はシステム担当者の指示を得てから投入する

- ・感染したコンピュータが1台でも社内ネットワークにつながっていると、他にも被害が拡大する可能性があります。
- ・全てのコンピュータ(個人の持ち込みPCも含みます)については、電源投入前にシステム担当者の指示を受け、必要な対策をとって下さい。

【感染の可能性があるコンピュータ】

Windows XP、Windows 2000、Windows NT Server4.0、Windows NT Server4.0 Terminal Server Edition、Windows Server2003 のいずれかの OS を搭載していて、Microsoft Windows の脆弱性(MS03-026)への対策がとられていないコンピュータ。普段持ち歩いているモバイル PC や長期出張や離職等の理由により、半ば放置されているコンピュータにも注意。

【企業のシステム担当者へのお願い】

(2) すべてのユーザに感染の危険性を事前に知らせる

- ・社員等が出社した時点で把握できる場所(掲示板、各PCのモニタなど)に、上記の「ユーザへのお願い」を提示する。

(3) ワームの侵入・拡大を防ぐようネットワークを設定する

- ・社内ネットワークとインターネットの境界に設置したファイアウォールやルータの設定で、TCP135番ポート、UDP135番ポート、TCP4444番ポート、UDP69番ポートへのアクセスを許可しない。

(4) ワームの駆除と感染予防を行う

- ・社内ネットワーク内に感染の可能性があるコンピュータが存在する場合には、そのコンピュータのユーザに対し、電源投入前にネットワークケーブルを外すよう指示する。
- ・未だ感染していないコンピュータを含め全てのコンピュータで、情報処理振興事業協会(IPA)のホームページ(<http://www.ipa.go.jp/security/>)を参照に、脆弱性への修正対策を行う。
- ・既に感染したコンピュータについて、上記ホームページ等を参考に、Blasterワームを駆除する。