2008 年 12 月 24 日

# MS08-067 のセキュリティホールを衝く WORM_DOWNAD ファミリによる被害が広まっています

**現在、「WORM_DOWNAD」（ダウンアド）と呼ばれるネットワーク型ウイルスの感染被害が広まっています。このワームは Windows 製品のセキュリティホールを利用して感染します。**
**トレンドマイクロでは、多層防御（Defense In Depth）の思想に基づき、様々な層でのソリューションを提供しています。**
**ここでは、「WORM_DOWNAD」の概要とその対策手法について紹介します。**

## ■収束傾向にある今も、潜伏PCからの予期せぬ再発が

2008 年 11 月 25 日に日本国内で初報告され、局地的に組織内での大規模感染（アウトブーイク）が報告されているネットワーク型ウイルス「WORM_DOWNAD（ダウンアド、別名：「W32.Downadup」または「Win32/Conficker.A」）ファミリ」。同ウイルスは Windows OS が抱えるセキュリティホールを衝くことで能動的な攻撃を試みるネットワーク型ウイルスです。

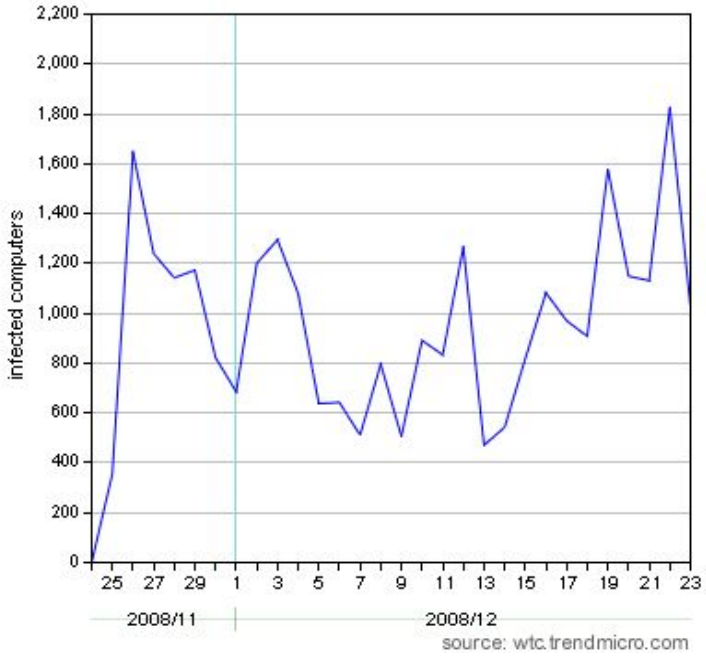


図 1 WORM_DOWNAD.A 感染状況（2008/12/23 時点）



トレンドマイクロ株式会社

セキュリティホールが未修正な環境によってはその感染により、予期せぬ再起動が繰り返し発生、正規プロセス（*svchost.exe -k netsvcs*）により起動されたサービスが一斉に停止する、意図せぬ TCP 445 通信による帯域圧迫などの症状が報告されています。
その一方で、攻撃者の意図通り攻撃が成立した場合、何ら表層的な症状は現れず、深く静かに攻撃が進行している場合もあります。
このため、ウイルスの特徴を理解し、各層において最適な対策を施していくことが重要です。

## ■予見された脅威、日本国内での報告に至るまで

「WORM_DOWNAD」は「Server サービスのセキュリティホールにより、リモートでコードが実行される（MS08-067：CVE-2008-4250）」のセキュリティホールを狙い、脆弱なコンピュータを探し出すとウイルスを送り込み侵入してくることが大きな特徴です。
同セキュリティホールは 10 月 24 日にマイクロソフト社より、セキュリティ更新プログラムが公開されています。同社アドバイザリ[1]では最大深刻度「緊急」、悪用可能性指標「1：安定した悪用コードの可能性」との指標とともに 2 週間前に限定的な攻撃が確認されていることを発表しています。
同日トレンドマイクロでは同セキュリティホールを衝く「WORM_GIMMIV.A」の感染報告をアメリカ、オランダなど複数の国より寄せられていることを発表しています。「WORM_GIMMIV.A」はウェブサイトへ接続し、「TSPY_GIMMIV」をダウンロードすることが確認されています。また、サーバの設置場所は、その IP アドレスから日本国内のレンタルサーバであることが特定され、リージョナルトレンドラボより、該当レンタルサーバ業者へ連絡を行い、10 月 24 日 15:44 にウェブサイトの閉鎖をご連絡いただいています。
限定的な攻撃は続きます。11 月 2 日には新たなウイルス「TROJ_DUCKY.M」、「TROJ_DUCKY.O」が報告されています。また、11 月 4 日には「WORM_KERBOT.A」が報告されるとともに、JPCERT コーディネーションセンター（JPCERT/CC）によれば、TCP 445 番ポートに対する、日本国内および中国からのスキャンが 10 月 30 日深夜より増加していることが発表[2]されています。
また、トレンドマイクロでは中国語ユーザインタフェースを持つ MS08-067 を衝く攻撃ツールの流通について 11 月 6 日に発表しています。
11 月 21 日にスペインのセキュリティ組織より、IntelliTrap 機能[3]で「PAK_Generic.001」[4]（後に「WORM_DOWNAD」ファミリの名称割り当て）として検出された検体が報告されています。
11 月 25 日早朝、日本国内企業より、「WORM_DOWNAD」ファミリによる攻撃被害報告を入電いたしました。

---

[1]マイクロソフト セキュリティ情報 MS08-067 - 緊急 ：Server サービスの脆弱性により、リモートでコードが実行される (958644)
http://www.microsoft.com/japan/technet/security/bulletin/MS08-067.mspx
[2] JPCERT/CC：TCP 445 番ポートへのスキャン増加に関する注意喚起
http://www.jpcert.or.jp/at/2008/at080019.txt
[3] 製品 Q&A：IntelliTrap 機能：自動実行型の圧縮ファイル(パッカー)により難読化されたウイルスに対するヒューリスティック（ルールベース方式）検出機能
http://esupport.trendmicro.co.jp/supportjp/viewxml.do?ContentID=JP-2060755
[4] ウイルス情報「PAK_Generic.001」
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PAK_GENERIC.001



トレンドマイクロ株式会社

| 報告日 | 概要 |
|---|---|
| 2008-10-24 | マイクロソフト社より Windows OS の Server Service に関するセキュリティホールアドバイザリ、MS08-067 セキュリティ更新プログラムが公開 |
| 2008-10-24 | セキュリティホールを衝くウイルス「WORM_GIMMIV.A」を確認 |
| 2008-10-25 | 「Metasploit」（セキュリティ研究者向けの攻撃コード開発および検証ツール）向けに MS08-067 の攻撃コードがリリース<br>攻撃コード公開サイトにて先の「Metasploit」とは異なる別の攻撃コードがリリース |
| 2008-11-02 | セキュリティホールを衝くウイルス「TROJ_DUCKY.M」、「TROJ_DUCKY.O」を確認 |
| 2008-11-04 | JPCERT/CC より、TCP 445 番ポートに対する、日本国内および中国からのスキャンが 10 月 30 日深夜より増加していることが発表 |
| 2008-11-04 | セキュリティホールを衝くウイルス「WORM_KERBOT.A」を確認 |
| 2008-11-06 | 中国語圏の攻撃者に向けた攻撃ツールのリリースを確認 |
| 2008-11-21 | スペインセキュリティ組織より、IntelliTrap 機能による「PAK_Generic.001」（後に「WORM_DOWNAD」ファミリの名称割り当て）検体が報告 |
| 2008-11-25 | 日本国内企業より、「WORM_DOWNAD」ファミリによる攻撃被害報告を入電 |

**表 2 MS08-067 セキュリティホールを衝く攻撃の時系列変化**

## ■二段構成での拡散を行う、「WORM_DOWNAD」

ここでは、「WORM_DOWNAD.A」の詳細な振る舞いについて解説していきます。
同ウイルスは、セキュリティホールを衝く振る舞いと感染コンピュータを HTTP (Web) サーバへと変換する振る舞いで拡散能力を高める戦略を採っています。
同ウイルスも他のウイルスと同様に、スパムメール (迷惑メール) の添付ファイル、悪意のある Web サイト、利用者自身の手によるインストールなどにより、初期の侵入に至った可能性が考えられます。
このほかに、ネットワークを介した拡散行為、ワーム (拡散) 活動に特徴があります。
ワーム活動の一つ目として、「Windows Server Service RPC」のセキュリティホールを衝いた侵入が挙げられます。セキュリティホールを衝いた侵入は、同ウイルスが細工された不正な RPC (Remote Procedure Call) リクエストを、感染対象コンピュータの TCP 445 ポートへ送信されることで行われます。このとき、対象コンピュータが MS08-067 のセキュリティホールを抱えている場合、ペイロード (発病機能) が発症し、シェルコード (悪意ある行為を行うコード) が動作します。なお、ウイルスは感染対象コンピュータを探索するために、攻撃元となるコンピュータのネットワークアドレスを起点として、アドレスに対し数値を一つずつ加算していくことを特定しています。

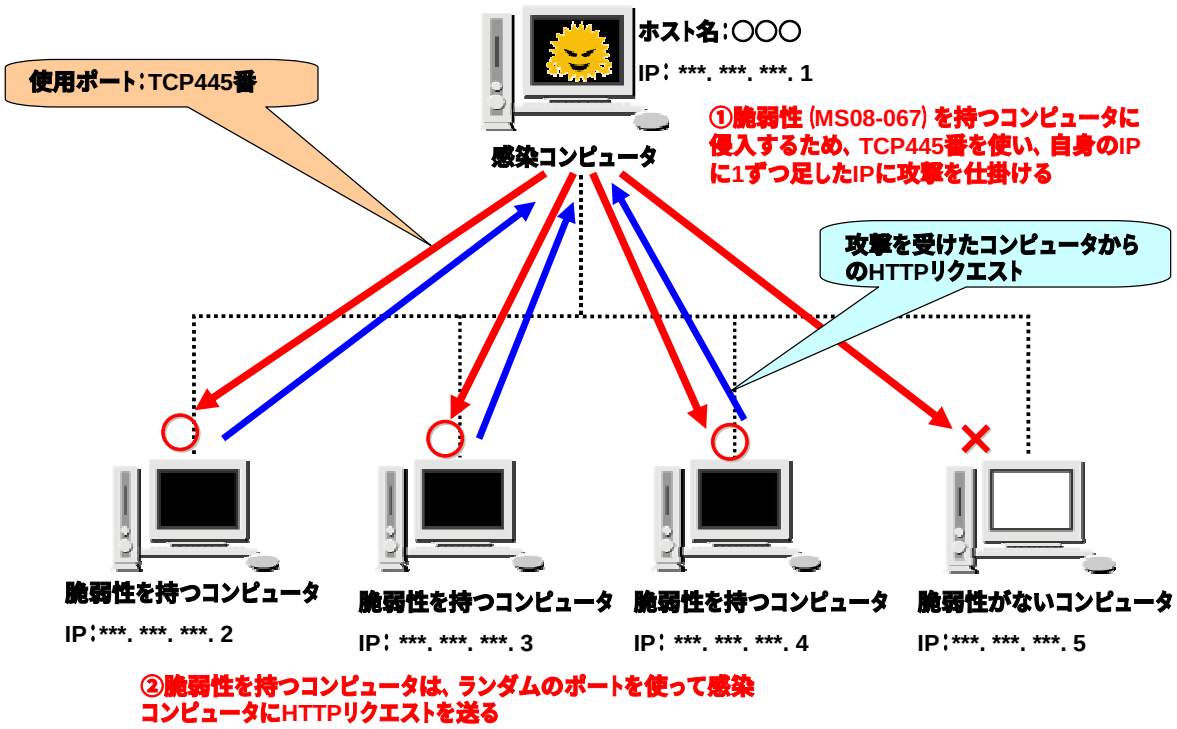


図 2「WORM_DOWNAD.A」による「Windows Server Service RPC」の脆弱性を衝いた侵入

ワーム活動の二つ目はシェルコードの起動により行われます。シェルコードの起動により感染対象コンピュータは HTTP サーバへと変換が行われます。これは、感染源である攻撃元も既に HTTP サーバ化されていることを意味しています。シェルコードは感染対象コンピュータの HTTP サーバ変換と同時に、攻撃元に対する HTTP リクエストの発行が行われます。感染源では、感染対象コンピュータからの HTTP リクエストに対し、「WORM_DOWNAD.A」のコピーである「x」と名付けられた DLL ファイルを HTTP レスポンスとして返答を行います。なお、HTTP レスポンス返答時のヘッダにおいて、「Content-Type: image/jpeg」と指定されています。これは、実行ファイルの通信をコンテンツフィルタリング製品により禁じられているような環境に対する回避策であると推定されます。

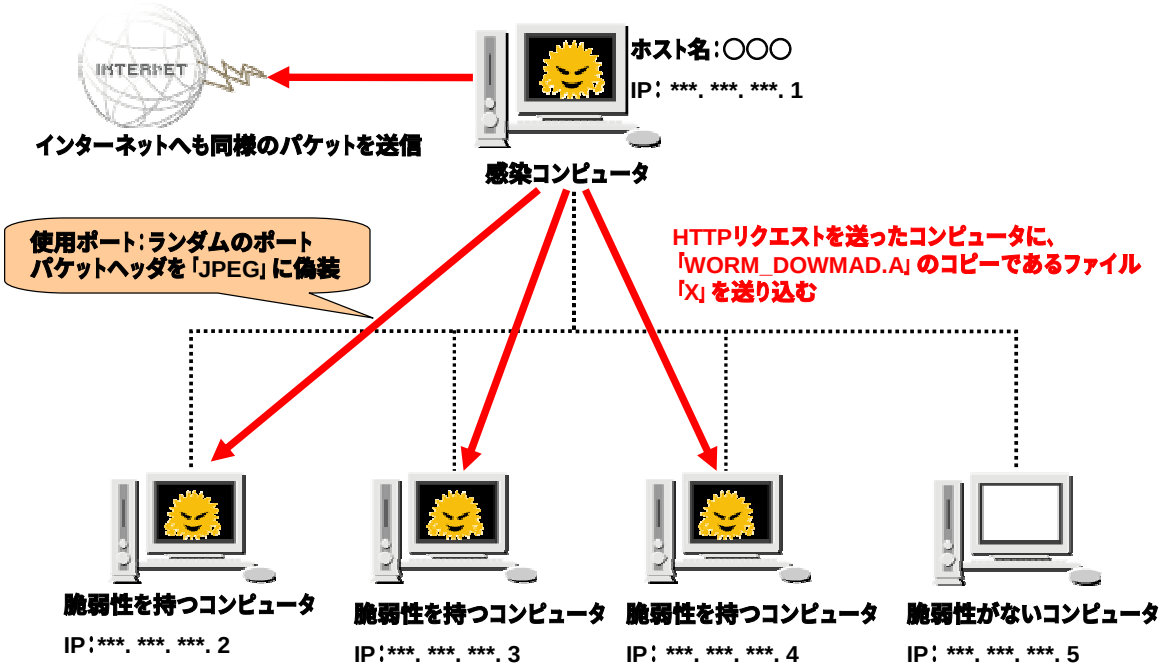


**図 3 シェルコード起動により感染対象コンピュータを HTTP サーバ変換**

ウイルスはワーム活動を閉じられたネットワークのみならず、インターネットへと広げていく為に正規のインターネットサービスの悪用を行っています。まず HTTP サーバとなるランダムなポートを開き、インターネット上に発信します。これにより、インターネットを介しての自由なアクセスが可能になります。ウイルスは、コンピュータの外部 IP アドレスを取得し、そのコンピュータがインターネットへ直に接続しているかを確認します。これは、ウイルスが感染対象コンピュータのインターネット接続能力を測定していることを意味しています。感染対象コンピュータのインターネット接続を外部 IP アドレスの有無で確かめます。さらにその設定された IP アドレスが、イーサネットかモデムドライバかどうも確かめます。このインターネット接続能力測定において、ウイルスは、正規インターネットサービスを利用します。正規インターネットサービスを利用することで、取得した感染対象コンピュータの IP アドレスが有効かどうか、またローカル IP アドレスでないかどうかをチェックします。また、ウイルスは、外部 IP アドレスが、コンピュータ上で設定された IP アドレスと同じものであるかどうかもチェックします。

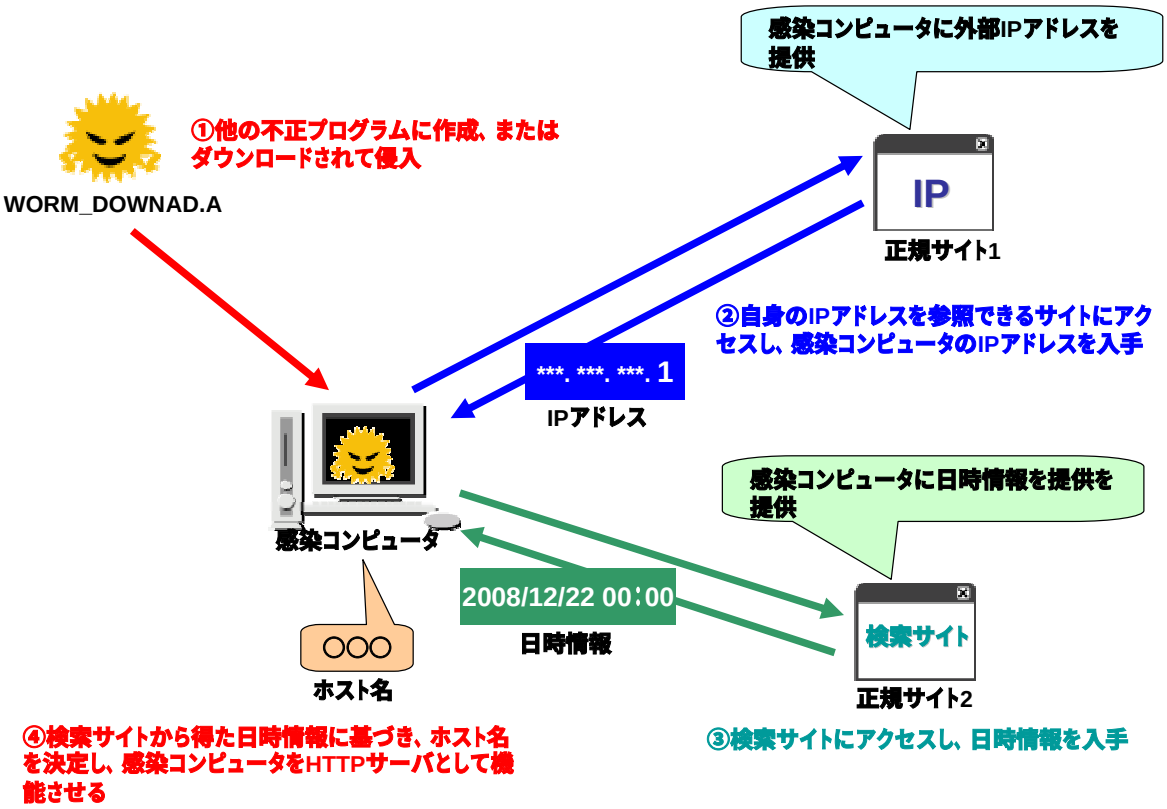


図 4 正規インターネットサービスを悪用、インターネットへのアクセスを実現

ウイルスが変換した感染対象コンピュータの HTTP サーバにはランダムなポートが設定されています。このため、ランダムなポートがオンラインで利用可能かどうかをチェックする際、ユニバーサルプラグアンドプレイ（UPnP）の仕組みである SSDP（Simple Service Discover Protocol）リクエストを介して応答可能な HTTP サーバの通知が行われます。
拡散機能の他に、新たな脅威を不正な Web サイトを介して呼び込もうとするダウンローダ機能も組み込まれています。攻撃者は不正な Web サイトに様々なウイルスを仕掛けることによって、第二、第三の攻撃を計画していた可能性も考えられます。

## ■ウイルス拡散に至った要因

組織から寄せられる被害報告を分析することにより、「WORM_DOWNAD」ファミリが拡散に至った要因が明らかとなってきています。

セキュリティ更新プログラムの公開から「WORM_DOWNAD」の拡散まで約 1 ヶ月の猶予がありました。しかしながら、多くの組織ではセキュリティ更新プログラム適用に至っていませんでした。これには、いくつかの要因が挙げられます。利用者に委ねる形でのセキュリティ更新プログラム適用計画が進められており、利用者側での作業が実施されなかったケース。または、管理者による強制的なセキュリティ更新プログラム適用計画が進行していたが、検証作業が間に合わず、その日を迎えてしまったケースなどが挙げられます。特に「MS08-067」に関しては、セキュリティ更新プログラムの適用にあたって、コンピュータの再起動を要するため、高い可用性を求められるシステムで運用されている場合、直ちに適用することが困難であった背景も挙げられます。

一部組織では、セキュリティ更新プログラム未適用のリスクをファイアウォール（含む、IDS：Intrusion Prevention Service、不正侵入防御システム）で補完する取り組みが行われていました。組織とネットワークとの境界となる箇所に攻撃の始点である細工された不正な RPC リクエストをブロックする機構を設置しておくことで、リスクに対する有効な補完機能を提供するに至っています。

リスク補完機構を設置している企業においても、意外な盲点により侵入に至ったケースが報告されています。ノート PC にてモバイルカード経由でのインターネット接続を実施した際にウイルス侵入を許し、同ノート PC を組織内ネットワークに再接続時に、組織内での拡散に至ったケースです。

多くの組織では、一部従業員に対しモバイルカードを貸与している場合があります。このため、従業員はノート PC によるモバイル接続を許可された PC、ネットワークでの利用であると理解しています。しかし実情は、モバイルカードにより割り振られる IP アドレスはグローバルアドレスであることが多く、管理されていないネットワークに接続している状態と同一です。

いくら強固な城壁や門番を組織の境界に立たせていたとしても、内部の危険性に対しても目を光らせねば情報セキュリティが抱える課題をクリアしていくことは困難であると言えそうです。



トレンドマイクロ株式会社

## ■多層防御思想に基づくトレンドマイクロの検出技術

トレンドマイクロでは多層防御の思想に基づき、「WORM_DOWNAD」ファミリ検出対応ウイルスパターンファイルのみならず、感染防止策から感染コンピュータの駆除策まで提供しています。

| トレンドマイクロ製品によるセキュリティホール緩和策 | | | |
|---|---|---|---|
| リリース日時 | ソリューション | バージョン | 効果 |
| N/A | 不正変更の監視 | N/A | 「WORM_DOWNAD」ファミリが行うシステム改変を検知<br>ウイルスバスター 2009/2008 にて実装 |
| 2008-08-26 | インテリトラップパターンファイル | 109 | 「WORM_DOWNAD.A」不正である可能性がある、Win32 圧縮ツールで圧縮された実行可能形式（PE 形式）ファイルとして「PAK_Generic.001」の名称で検知 |
| 2008-10-27 16:56 | ネットワークウイルスパターンファイル | 10269 | 不正な通信を「MS08-067_Server_Service_Remote_Execution_Exploit」の検出名にて検知<br>ActiveUpdate（自動更新）サーバより配信 |
| 2008-10-30 17:41 | セキュリティ診断パターンファイル | 091 | [セキュリティ診断]機能により、MS08-067：セキュリティ更新プログラムの適用状況を確認可能<br>ActiveUpdate（自動更新）サーバより配信 |
| 2008-11-25 12:56 | ウイルスパターンファイル | 5.673.00 | 「TROJ_AGENT.AKX」（後に「WORM_DOWNAD.A」に改称）の検出に対応<br>ActiveUpdate（自動更新）サーバより配信 |
| 2008-11-25 15:40 | Web レピュテーション | N/A | 「WORM_DOWNAD.A」が接続するサイトを「Disease_Vector」として検知<br>トレンドマイクロ Web レピュテーションサーバへ直ちに反映 |
| 2008-11-26 10:29 | WORM_DOWNAD 専用駆除ツール[5] | バージョン 1.0 | 「WORM_DOWNAD.A」が実施したレジストリ改変（正規のプロセスにウイルスを埋め込む記述）を削除します。再起動により、メモリ上に残る「WORM_DOWNAD.A」プロセスを駆除<br>「WORM_DOWNAD 駆除ツール」配布サイトの開設 |
| 2008-11-26 14:03 | ダメージクリーンナップテンプレート | 992 | 「WORM_DOWNAD.A」によるシステム改変を復旧<br>ActiveUpdate（自動更新）サーバより配信 |
| 2008-11-27 11:16 | ウイルスパターンファイル | 5.677.00 | 「WORM_DOWNAD.A」（「TROJ_AGENT.AKX」からの改称を実施）<br>ActiveUpdate（自動更新）サーバより配信 |

**表 2 トレンドマイクロ製品によるセキュリティホールの緩和策**

[5] WORM_DOWNAD 駆除ツール配布サイト
http://jp.trendmicro.com/jp/threat/extermination_tool/downad/

## ■最良の対策はセキュリティ更新プログラムの適用

セキュリティホールを衝く攻撃において、最良の対策はセキュリティ更新プログラムの適用です。今回対処となっている「MS08-067」の適用はもちろん、導入している機器やソフトウェアについて、セキュリティ更新プログラムが公開されていないかどうか確認することが重要です。
また、直ちにセキュリティ更新プログラムの適用が困難な環境においては、有効なリスク低減策の有無について確認すべきです。
ウイルスバスターをはじめとする総合セキュリティ対策製品の利用においては、最新版のウイルスパターンファイルの利用はもちろん、最新の脅威に対する対策を含む最新バージョンの利用と最新版ウイルス検索エンジンの利用が推奨されます。
また、モバイル接続を行うノート PC 利用者に対しては社内利用時よりも強固な利用指針を提示するとともに、組織ネットワークへ再接続を許可する際には、独立した検疫ネットワークを用意するなどの対策を検討することも有効です。

- 最新のセキュリティ更新プログラムが適用されていることを確認する
- 許容するリスクを把握し、低減策の有無を確認/適用する
- 最新バージョンの総合セキュリティ対策製品を利用し、アップデートを怠らない
- モバイル接続の危険性を示し、利用者に対しては強固な指針を提示する
- 持ち出しノート PC の再接続の際には独立したネットワークでの検疫を推奨する



トレンドマイクロ株式会社