

SAFE による Nimda 攻撃の緩和

概要

この文書では、最近発生した Concept/Nimda (Nimda) ワーム/ウィルスと、このワームがネットワークおよびそのホストに及ぼす影響について解説します。現在シスコシステムズの製品には、このワームの有害な効果を緩和するための多数の技術が利用されています。こうした技術に加え、SAFEブループリントでは、セキュリティ上のベストプラクティス（最善の実践原則）とセキュアなネットワーク設計を組み合わせることによって、Nimdaのようなワーム/ウィルスまたは他の攻撃による被害を緩和します。この文書には、www.cisco.com/go/safeに掲載されている技術資料とほぼ同じ内容が含まれます。このことは、新たなワームが発生しても、中核的な緩和技術は変わらないという傾向を示しています。

Nimda の背景と機能

Nimda ワームは実際には複合型であり、ワームとウィルスの両方の性質を併せ持ちます。ワームもウィルスも、複数のシステムに感染を広げて増殖します。2つの違いは、ウィルスは自身を増殖させるために、何らかの形で人の手を借りなければならない点です。Nimda は、以下を媒介して増殖します。

- 電子メールの添付ファイル (ウィルス)
- ネットワーク共有 (ワーム)
- 感染した Web サイトの閲覧時に JavaScript を実行 (ウィルス)
- 他の侵入可能なホストをアクティブに検索中の感染ホスト (ワーム)
- Code-Red および sadmind/IIS ワームの作成したバックドアをアクティブに検索中の感染ホスト (ワーム)

Code-Red と異なり、Nimda は意図的な破壊能力をまだ示していません。その活動は現時点では自己増殖に限定されていますが、これは DoS (サービス拒否) 攻撃という副作用を伴います。

DoS 攻撃は、攻撃対象とするシステムだけでなく、感染ホストのローカルネットワークにまで被害を及ぼします。ネットワーク内の感染ホスト数によっては、これらの機器が生じさせる負荷により、ローカルネットワーク障害が発生しかねません。予想外の負荷によって回線が混雑したり機器に障害が生じるため、その被害はネットワーク速度が低下するだけの場合もあれば、ネットワークが使用不可能になってしまう場合もあります。多くの場合、すべての感染システム上のサービスは低速になり、サービスの正規利用も妨げられます。

Nimda の攻撃方法は、複数の手段によってシステムを攻撃および感染できるという点で、Code-Red よりも進化しています。しかも、その攻撃手段の一部は、インターネットコミュニティにとって極めて新しいものです。たとえば、電子メールクライアントによっては、ユーザが添付された感染ファイルを実行しなくても Nimda に感染します。また、Nimda はネットワーク上の共有ファイルに自身のコピーを送り込みます。これにより、プレビュー表示オプションが有効になっている Windows エクスプローラでこのファイルを開覧しようとするすべてのユーザは、ワームの実行プログラムをロードしてしまいます。Nimda はいったんシステムに感染すると、ローカルに保存されている HTML ファイルすべてに JavaScript を埋め込みます。この JavaScript は、この HTML ファイルを開覧するすべてのリモートシステムに対して、ユーザの手を借りることなくワームの実行プログラムをロードします。Nimda についての詳細情報は、<http://www.cert.org/advisories/CA-2001-26.html> を参照してください。



Nimda の被害を緩和するためのシスコの提案

脆弱性が認められる全システムにパッチを適用

Nimda による被害を防ぐ最も効果的な方法は、脆弱なすべてのシステムにパッチを当てることです。まずはこれが第1段階です。パッチの適用は、ローカルネットワーク内にある管理対象外になっているユーザシステムに対しては困難であり、VPN(仮想プライベートネットワーク)やRAS(リモートアクセスサーバ)経由でリモートにネットワーク接続しているシステムではさらに困難です。しかし、脆弱性を検出するセキュリティ検査ツールを使用すれば、悪用される可能性のあるデバイスの特定も容易になります。ローカルなワークステーションには、PCのブラウザおよび電子メールクライアントにもパッチが必要となる場合があります。Microsoft製品に対する感染被害の緩和については、下記のURLを参照してください。

- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp>

多くのベンダの製品は、リモート管理およびレポート作成のためのWebアクセスを実現するため、IISをインストールして使用しています。これらも、パッチを適用しない限り安全ではありません。Microsoft OutlookおよびOutlook Expressメールアプリケーションは、埋め込まれたMIMEタイプを自動実行してしまうという脆弱性を持つため、これにもパッチを当てる必要があります。同じく、不正利用を許すバージョンのMicrosoft Internet Explorerにもパッチが必要です。これらのアプリケーションにおいて脆弱性を持つバージョンについては、上記のURLを参照してください。適切なタイミングで全システムにパッチを適用することが不可能であれば、今すぐ、以下のセクションで述べる各技術の採用を検討してください。また、将来的にNimdaやその他の攻撃を総合的に防止するため、これらの技術をプロアクティブに導入することも考慮する必要があります。

Nimda対策の第2段階は、すべてのウイルススキャンソフトウェアを、最新のウイルスリストに更新することです。万が一すでに感染している場合を踏まえ、システムのウイルススキャンはローカルに実行することをお勧めします。最終段階は、パッチの適用やウイルススキャンが行われなかったデバイスがあれば、感染しているもの、または脆弱なものをネットワーク内で判別することです。この作業はネット

ワークスキャナで実行できることもありますが、基本的には侵入検知システム(Intrusion Detection System;IDS)が発したアラームを分析して行います。

セキュリティ技術

ここでは、シスコの各製品が提供する、Nimdaやその他の攻撃を緩和するための技術について解説します。これらの技術について、またはNimda対策用の設定方法についての詳細は、SAFEの技術資料(<http://www.cisco.com/jp/solution/ent/tech/security/safe.html>)を参照してください。

ホストベース侵入検知システム (HIDS)

ホストベース侵入検知システム(Host-Based Intrusion Detection System;HIDS)は、インストールされたホストに対する攻撃を検知します。具体的には、OSおよびアプリケーションコールのインターセプト、OSおよびアプリケーションの設定の安全化、受信するサービス要求の検証を行い、ローカルログファイルを分析して疑わしい動作の痕跡を調べます。操作モードには、モニタモード(アラームのみ)と実施モードの2つがあります。HIDSは、以下の多数のセキュリティ機能を実行します。

- 受信するHTTP(Hypertext Transfer Protocol)トラフィックを分析し、一般規則と既知の攻撃シグネチャを使用して、これが攻撃行為かどうかを判断
- HTTPサーバの動作を分析し、通常の運用モードを反映しているかどうかを判断
- バッファオーバーフローやバイナリ変更の防止といった、OSの一般的な保護

HIDSで保護したWebサーバの場合、ワームが感染させようとしても攻撃は失敗し、サーバは感染しません。HIDSはWebサーバをロックダウンすることで、このワームのような感染手法(Microsoft IISの脆弱性を突いた自己増殖)を遮断します。HIDSはディレクトリ横断(Directory Traversal)やリモートコードの実行による攻撃だけでなく、Webコンテンツの不正改ざんも防止することで、ワームが他のサーバに自身を拡散できるようにWebページを変更する機能を制限します。最後に、HIDSは攻撃シグネチャの検出により、HTTPおよびIISを悪用した感染からサーバを保護します。

HIDSは以下のルールにより、Nimdaの感染を防ぎます。

- IISディレクトリ横断
- IISディレクトリ横断およびコードの実行
- IISの二重16進エンコードによるディレクトリ横断

ただし、ウイルスの動作に類似した手動による感染行為、たとえば電子メールの添付ファイルのオープン、感染ファイルの手動実行、感染Webサイトの自主的な閲覧などは、HIDSによって遮断されないので注意が必要です。これらの行為による被害は、SAFEの包含するセキュリティ上のベストプラクティス(ウイルススキャンなど)、およびユーザベースの教育によって緩和できます。たとえば管理者は、実行中のWebサイトで電子メールアプリケーション



ンを実行したり、Webサイトを閲覧するべきではありません。また、公開サーバ上ではネットワーク共有ファイルを実行しないことも大切です。

HIDSの導入には、攻撃緩和に関して、システムへのパッチ適用のセクションで前述したものと同一問題が生じるように思われるかもしれません。しかし、HIDSクライアントの稼働システムへのインストールはパッチ適用よりはるかに簡単であり、運用上の影響も少なく、システムの中断や再起動が必要となる可能性も低くなります。現行の問題への対策としてHIDSをインストールするシステムを選ぶには、ネットワークセキュリティスキャナを使用して、Webサービスを実行しているシステムを識別します。Nimda以外にも将来的な攻撃を緩和するには、HIDSを重要なサーバ上にインストールすることを検討してください。

ネットワークベース侵入検知システム (NIDS)

ネットワークベース侵入検知システム(Network-Based Intrusion Detection System; NIDS)は、最初にネットワークレベルで攻撃を検出した上で、自ら修復アクションを実行するか、または管理者が何らかの措置を取れるように、管理システムに通知します。攻撃を検出するには、ネットワーク上のトラフィックフローからシグネチャの有無を調べます。NIDSは攻撃を検出すると、アラームを発生し、あらかじめ設定されたアクションを実行します。ここで可能なアクションは、ネットワーク遮断とTCPリセットの2つです。NIDSはデータパス上にはないため(NIDSはパケットをルーティングするのではなく、ネットワークを巡回しながらパケットのコピーを受信する)、攻撃時に最初のパケットをフィルタリングできません。次のパケットからは、「遮断(shunning)」と呼ばれる機能によってフィルタリングできます。これは、ネットワーク上流にあるアクセス制御デバイスを修正して、攻撃側システムのIPアドレスからのアクセスを今後いっさい禁止する機能です。TCPリセットは、受信デバイスからと見せかけて作成したリセットコマンドを攻撃側デバイスに送ることで、TCP接続を切断しようとする方法です。NIDSはNimdaワームの使用するさまざまなWebアプリケーション攻撃を識別し、影響を受けたホストおよび感染ホストの詳細情報を提供します。

不正侵入を検知すると、以下のCisco IDS Network Sensorアラームが発生します。

- WWW WinNT cmd.exeアクセス(シグニチャID:5081)
- IIS CGI二重デコード(シグニチャID:5124)
- WWW IISユニコード攻撃(シグニチャID:5114)
- IIS Dot Dot実行攻撃(シグニチャID:3215)
- IIS Dot Dotクラッシュ攻撃(シグニチャID:3216)

NIDS運用者は、Nimdaを名前で識別するアラームを目にすることはありません。代わりに、Nimdaがターゲットに感染しようとして違った種類の攻撃を試みる度に、これらのアラームが発生します。これらのアラームにより、感染済みホストの送信元アドレスが識別できるので、これらのホストをネットワークから切り離し、クリーンにした上でパッチを適用する必要があります。

ウィルススキャン

ウィルススキャンソフトウェアは、悪意のあるコードおよびウィルスによるホストへの攻撃を、リアルタイムで緩和します。Nimdaの場合、ウィルスは電子メール、Webサイトの閲覧、ファイル交換など、いくつもの経路を通じてシステムに侵入します。これらの経路は本質的に、それ自体がシステムへの複数の経路を持つものです。たとえばWebページは、追加機能を実現するために、リモートに使用可能なコードをActiveX、Java、およびJavaScriptといった手段で取り込むようになっています。しかし、こうした複数の仕組みがすべて、システム上で悪意のあるコードを実行するための侵入口となります。ほとんどの場合、ユーザはリモートコードの実行を許可するかどうかを尋ねられます。ユーザの教育が不十分だと、ほとんどのユーザがここでためらいもなく「はい」を選択してしまいます。さらに悪いことには、古いバージョンのWebブラウザの場合、ユーザに尋ねることもせずコードを自動的に実行します。ウィルススキャンを成功させるには、以下を定期的に行う必要があります。

- ホストのローカルファイルの定期スキャン
- ウィルスリスト/シグネチャの定期更新
- ホストスキャナの生成する警告の定期監視

この文書の最後に、ウィルススキャンソフトウェアを提供する弊社パートナーのリストを掲載しています。

アクセス制御

ステートフルファイヤウォールは、Nimdaの被害をプロアクティブに緩和するための多数のセキュリティ機能を備えています。まず、ステートフルインスペクションエンジンは適切なプロトコル準拠を検証することで、接続の試みを通常よりきめ細かなレベルで制御できます。このようなフィルタリングを使用すれば、Webサーバへの外部からの(インバウンド)接続を許可しながら、このサーバが外部への(アウトバウンド)接続を開始することを禁止して、ワームの自己増殖を制限できます。この手法は、DMZ(非武装セグメント)にWebサーバを配置する上で特に有効です。SAFEでも述べているように、Webサーバには通常、外部への接続を確立する機能、いわばWebサーフィン機能は不要です。ほとんどの場合、Webサーバには、外部から送られるWeb要求に応答する機能だけが必要とされます。第2に、ステートフルファイヤウォールは、サーバに対して外部からの接続数を制限する機能があり、これによってサーバが過剰な負荷を受けることを防止できます。Nimdaの場合、あらかじめ許可した最大数にアクセスが達した時点で、外部からの過剰な不正接続を遮断できます。

インGRESS(入口側)でのフィルタリングは通常、ネットワークの境界でアクセスを制御することで実現します。この機能は、一般公開されるべきではないホストおよびサービスに対するアクセスを遮断するために使用されます。たとえば、公開サービスの提供にアクティブに関与しているものでない限り、ホストまたはネットワーク機器に対しては外部からの接続要求を禁止することが、セキュリティ上のベストプラクティスです。Nimdaに関しては、少しでも



正利用の可能性があるユーザシステム、または非公開 Web サーバに対し、外部からの HTTP 接続を禁止できます。ただし、このフィルタリングを設定する際、公開 Web サーバまたは E-コマースサーバに対してはアクセスを許可する必要があります。理想的には、公開サーバは管理者による厳格な管理下に置き、最新パッチを当てるべきです。このようにイングレスフィルタリングは、ユーザシステムを標的とした Nimda の不正利用を事実上遮断します。

イーグレス(出口側)でのフィルタリングも同様に、ネットワークの境界でアクセスを制御することで実現します。この機能は、ローカルホストによるネットワーク外部へのアクセスを遮断します。ネットワーク内のほとんどのネットワーク機器や、内部環境だけにサービスを提供する Web サーバなど、外部へのインターネット接続を必要としないデバイスには、外部への接続の開始を許可するべきではありません。Nimda に関しては、外部へ向かうトラフィックはネットワーク境界でインターセプトおよび破棄されるため、あるデバイスが感染した場合でも、このデバイスから外部ネットワークに感染が広がることはありません。WAN の境界に加え、ネットワーク内の付加的な階層にイーグレスフィルタリングを実装すると、感染した公開 Web サーバ(Web ファームの場合はセグメント全体)から、境界でのイングレスフィルタリングによって保護されているプライベートの内部サーバにまで感染が広がることも防止できます。アクセス制御とフィルタリングに関する詳細は、SAFE の技術資料を参照してください。

プライベート VLAN

プライベート VLAN は、同一 VLAN 内の他のポートと通信できるポートを限定する機能です。これは通常、特定セグメント内のホストがそのデフォルトゲートウェイだけと通信し、ネットワーク内の他のホストとは通信できないようにするために実装します。たとえば、ある Web サーバが Nimda に感染した場合、このサーバは同一ネットワークセグメント内にあるものでも、同じ VLAN 内の他の Web サーバに感染を試みません。このアクセス制御は、ホストを隔離ポートまたはコミュニティポートのいずれかに割り当てることによって実現し、1 つの感染ホストからの影響を効果的に緩和できます。隔離ポートは、相手を選別しないポート(一般的にはルータ)だけと通信できます。コミュニティポートは、相手を選別しないポート、および同一コミュニティ内の他のポートと通信できます。

プライベート VLAN について詳しくは、<http://www.cisco.com/warp/public/473/90.shtml> を参照してください。

SAFE ブループリント

SAFE ブループリントは、Nimda の被害を緩和するための多くのセキュリティ技術を利用します。したがって、SAFE ブループリントは「Nimda セーフ(耐 Nimda)」となっています。SAFE ブループリントでは、イングレスおよびイーグレスフィルタリングをネットワーク境界だけでなく、ほぼすべての SAFE モジュール間に適用します。このフィルタリングにより、感染サーバから外部へのアクセ

ス、およびユーザシステムに対する外部からの感染攻撃を防止できます。ステートフルファイアウォールは、フィルタリングと共に、ユーザとサーバセグメントの両方を保護し、公開サーバに対しては DDoS 接続レートを制限します。NIDS は、すべての公開セグメントに配置して Nimda の侵入を検出するだけでなく、ネットワーク境界でのフィルタリングおよびステートフルインスペクションの背後にも配置し、ネットワーク境界で不正侵入が行われた形跡がないかどうかを検査します。HIDS はすべての公開サーバだけでなく、インターネットへのアクセスを行わない内部の重要サーバにも実装し、管理の及ばないユーザシステムへの感染を防ぎます。プライベート VLAN は公開サービスセグメントに設置し、ここで複数の公開サーバによって信用詐欺を防止します。

結論

この文書で解説した各技術は、Nimda とその変種による潜在的な被害だけでなく、ほぼあらゆる攻撃による被害を緩和します。セキュリティはインフラ全体で考慮することが重要であり、それは、これまでに述べた各技術が示すとおりです。ネットワークとそのリソースを Nimda から守ることは、最初の一步にすぎません。Nimda だけでなく、将来的な攻撃からもネットワークを防御できるように、セキュリティに関してはプロアクティブな対策を取ることが不可欠です。セキュリティポリシーを確立し、上記技術のいずれかを実装し、ネットワーク構成を社内で、または外部委託によって定期的に査定することで、ネットワークをセキュアにし、その安全性を保つことができます。

この文書では、シスコシステムズの提供する、セキュリティおよびネットワーク設計におけるベストプラクティスについての文書のごく一部を紹介しました。ネットワークの安全対策に関する詳細は、SAFE ブループリントの Web サイト(<http://www.cisco.com/jp/solution/ent/tech/security/safe.html>)を参照してください。どのような技術導入においても共通しますが、上述したいずれかの技術の採用を検討する際には、ご使用の機器が十分な CPU リソースを持つかどうかを確認してください。これらの機能を実装することで負荷が増加したとしても、Nimda の内部感染による負荷の方がはるかに大きいということにも注意が必要です。

特に注目すべきは、SAFE ブループリントが最初に公開されたのは 2000 年 10 月であるにもかかわらず、Code-Red や Nimda 対策のための設計または実装上の変更がいっさい必要なかった点です。新型の不正利用や攻撃の検出に必要なとなったのは、NIDS シグネチャとウィルスリストの定期的な更新のみでした。Nimda や Code-Red、その他大きな話題となったネットワーク不正利用が常に示すように、ネットワークセキュリティをリアクティブ(事後対策的)に設計するような方法は勧められません。優れたセキュリティポリシー判断に基づき、包括的なネットワークセキュリティ対策を講じることが、現在取り組んでいるリスクを組織内に周知させ、ほぼあらゆる潜在的な脅威を効果的に封じ込むための唯一の方法です。

関連情報へのリンク

CERTによるNimda関連情報 (英語):
<http://www.cert.org/advisories/CA-2001-26.html>

SAFEブループリント (英語):
<http://www.cisco.com/go/safe>

シスコによるCode-Red関連情報:
http://www.cisco.com/jp/solution/ent/tech/security/tech/scdam_wp.html

シスコの製品およびサービスに関するリンク

Cisco NIDSおよびHIDS (英語):
<http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml>

ウィルススキャン (英語):
http://www.cisco.com/cgi-bin/ecoa/displayProfile?PARTNER_ID=602
http://www.cisco.com/cgi-bin/ecoa/displayProfile?PARTNER_ID=1003

ネットワークスキャナ (英語):
<http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/index.shtml>

シスコのセキュリティ製品に関する一般情報

ネットワークセキュリティ (英語):
<http://www.cisco.com/go/security>

シスコのセキュリティコンサルティング (英語):
<http://www.cisco.com/go/securityconsulting>

Cisco PIX Firewall:
<http://www.cisco.com/jp/product/product/security/pix/>



シスコシステムズ株式会社

URL:<http://www.cisco.com/jp/>
問合せ URL:<http://www.cisco.com/jp/service/contactcenter/>
〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL:03-6655-4433

電話でのお問合せは、以下の時間帯で受付けております。
平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先