

# SAFE による Code-Red 攻撃の緩和

## 概要

この文書では、最近発生した Code-Red 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。これには、侵入検知やパケットフィルタリングといったセキュリティ技術だけではなく、VLAN (バーチャルLAN) のセグメンテーション、パケット分類、およびコンテンツサービスも含まれます。これに加え、この文書では、セキュリティ上のベストプラクティスとセキュアなネットワーク設計を組み合わせることで、Code-Red や他の攻撃を緩和する SAFE ブループリントの仕組みについても解説します。最後に参考資料として、これらの技術において、Code-Red の被害を軽減するための検証済みの構成設定を記載します。

## Code-Red ワームの発生と進化

### Code-Red の背景

2001年7月19日木曜、約13時間のうちに少なくとも359,104台のホストが Code-Red による被害を受けました。CAIDA (Cooperative Association for Internet Data Analysis) によるこの統計は、Code-Red ワームの被害がいかに大きいか、いかに感染力が強いかを物語ります。よくご存じない方のために簡単に説明すると、ワームとは、コンピュータソフトウェアの欠陥を利用して自己増殖する能力を持つコードのことです。Code-Red ワームの場合は、Microsoft Internet Information Server (IIS) パージョン4および5の、リモートからの不正利用が可能な脆弱性を突いています。ワームはホストに対し、IIS の一部である Microsoft Index Server 内のバッファを溢れさせる (オーバーフロー) URL を送りつけます。ワームはこのバッファオーバーフローを利用することで、任意のコードを実行

できます。Code-Red は感染したコンピュータのメモリ内に自分自身をコピーし、さらに別のホストへ感染を試みます。

このワームには、2つのバージョンが確認されています。1つ目のワームは、このワームを最初に分析したチームである eEye Digital Security によって「CRv1」と命名されています。これは、標的とする IP アドレスのランダムな生成過程に欠陥があります。7月15日に一般環境での実際の感染が初めて公表された CRv1 は、決まった一定のシードを利用する乱数ジェネレータを使用して、攻撃対象の新規 IP アドレスを取得していました。同じシードを使うということは、同一マシン群が何度も繰り返し攻撃対象となり、ワームの感染範囲が限定されることを意味します。そのため、CRv1 は感染を広げたものの、その速度と影響力は深刻なものではありませんでした。次に、7月19日午前、CRv2 が発見されました。CRv2 は CRv1 とほぼ同じですが、ターゲット IP アドレスの取得に使用する乱数ジェネレータが改良されています。また、一時的に Web サイトを書き換える機能も削除されています。CRv2 は、強力な自己増殖能力を発揮しました。このような短期間で 359,104 台ものホスト感染は、このタイプの攻撃の感染力の強さを表します。CAIDA によると、ピーク時の CRv2 は毎分 2,000 台のホストを新規に感染させていたということです。

Code-Red II (CRv2 との混同に注意) は、Security Focus ARIS 分析チームによって初めて一般に報告されました。同チームがこのワームのコピーを eEye の分析チームに送付したところ、eEye 分析チームはこれを分解し、その結果を発表しました。Code-Red II を CRv1 および CRv2 と比較すると、完全にメモリから実行され、同じくバッファオーバーフローを利用し、自己増殖のために複数スレッドを作成する点だけが類似しています。Code-Red は英語システムに対して大きな被害を及ぼしましたが、Code-Red II は中国語システムに対して他よりも大きな被害を及ぼします。



## Code-Red CRv1 および CRv2 の機能

Code-Red CRv1およびCRv2の機能はほぼ同じです。いずれも、最初に99個のスレッドを作成して、他のシステムへの感染活動を行います。CRv1は100番目のスレッドを使用して、対象システムが英語システムかどうかを調べます。英語システムの場合、このスレッドは一定期間休眠します。これにより、感染システムは、注意を喚起するような多くの影響を出さずにワームを蔓延させます。2、3時間ののち、感染したWebサイトは次のようなメッセージに一時的に置き換わります。

"Welcome to http://www.worm.com!, Hacked By Chinese!"

実際には、ポート80への接続をインターセプトすることによって、このメッセージが表示されます。ファイルを改ざんするわけではありません。CRv2はWebサイトの表示妨害を行いませんが、英語システムに感染した場合は、100番目のスレッドによって無害なりダイレクトを行います。CRv1またはCRv2は「c:\notworm」というファイルを見つけると、活動を中止します。このファイルが見つからない場合は、日付が1～19日であれば感染活動を行い、20～28日であればホワイトハウスのWebサイト（現在は新規アドレスへ移動）に対し、DDoS攻撃（分散型サービス拒否攻撃）を行います。28日～月末であれば活動を中止しますが、また次の月初からこのサイクルを繰り返します。DDoS攻撃は、複数の感染システムを使用してターゲットに大量のパケットを送りつけ、このターゲットホストが正規のサービスを提供できないようにするものです。CRv1のDDoSでは、ホワイトハウスの旧IPアドレス(198.137.240.91)がハードコードされていましたが、CRv2はwww.whitehouse.govを名前解決してIPアドレスを割り出すようになっています。

## Code-Red II の機能

Code-Red IIは、Code-Redと一部の機能は似ていますが、まったく異なるワームです。マシンに感染したCode-Red IIは、中国語以外のシステムでは300のスレッド、中国語システムでは600のスレッドを生成します。ワームはこの期間、中国語以外のシステムでは1日間、中国語システムでは2日間に渡り、他のシステムに感染します。この待機期間が過ぎると、ワームはシステムを再起動し、ファイルシステムの保護機能を無効にします。

Code-Red IIはCRv1やCRv2とは異なり、Windows 2000だけに影響を与えます。攻撃に使用されたオフセットは、Windows NTシステム上では機能しません。Code-Red IIは、次のターゲットの選択においても、まったく異なるアルゴリズムを使用します。自身のIPアドレスの上位2オクテットを共有するシステムは、攻撃を受ける可能性が高くなります。しかし、最上位オクテットだけが同一のシステム、あるいは完全にランダムなIPアドレスであっても、攻撃を受ける可能性があります。Code-Red IIによって内部的に感染した企業の数があるかに多いのは、こうした手法によるものです。自社のWebサーバ自身が企業内部のWebサーバを攻撃することを想定したフィルタの設置は、行われてい

なかったためです。さらに、Code-Red IIはいくつかのバックドアを残します。1つは、cmd.exeのコピーを2つの異なるディレクトリ内に作成し、root.exeと名前変更するためのものです。このコピーを使用すれば、サーバ上で任意のコマンドを実行できます。また、WebサーバのCおよびDドライブに対する仮想マウントも作成します。これにより、root.exeファイルが削除されても、攻撃者はCまたはDドライブ上のcmd.exeにアクセスできます。

## ネットワークとそのホストに対する影響

DDoS攻撃は、攻撃対象のWebサイトだけではなく、感染ホストのローカルネットワークにも被害を及ぼします。1つのネットワーク内の感染Webサイト数によっては、DDoS攻撃による負荷の量はローカルネットワーク障害にもつながります。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。

## Code-Red 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

Code-Redおよびその変種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。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。Microsoft製品およびシスコ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.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.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。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Code-Redの変種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。



## セキュリティ技術

このセクションでは、シスコ製品が提供する、Code-Red 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。最初に、優先事項であるセキュリティ技術について解説します。以降のセクションでは、攻撃緩和機能を実現するその他の技術についても解説します。こうした技術は、セキュリティ技術が利用できない一部のネットワークに対する暫定措置として使用できます。これらの核技術に対する詳細、またはCode-Red対策の設定については、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

Code-Redおよびその変種の場合、HIDSはインデックスサービスを無効にすることで、IISの安全を確保します。また、一元管理を行うモニタコンソールに対し、不正利用の試みをインターセプトしたことを伝えるアラームを送ります。

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。Code-Red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り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。

ネットワーク上で遮断機能を有効にすることを検討する場合は、この機能を利用するための特別な注意事項を考慮する必要があります。これには、SAFEの技術資料で詳細を確認してください。CRv1およびCRv2は1つのパケット内に攻撃機能を仕込んでいるため、NIDSではこの攻撃を防止できません。ただし、CRv1およびCRv2攻撃がネットワーク上に広がると、アラームを発生して視覚的に注意を促します。Code-Red IIは複数のパケットを使用するため、NIDSはCode-Red IIからの攻撃であれば、TCPリセットの使用によって高い確率でこれを防止できます。NIDSの詳細については、<http://www.cisco.com/go/ids> を参照してください。

### アクセス制御

ステートフル ファイアウォールは、Code-Red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ます。第1に、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要求に回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アウォールは、サーバに対して許可する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。Code-Redの場合は、こうした制限により、不正利用を試みる外部からの接続を防止できます。

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。Code-Redに関しては、少して



も不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、最新パッチを当てべきです。このようにインGRESSフィルタリングは、ユーザシステムを標的とした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。Code-Red 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向けて DDoS 攻撃が行われることはありません。この機能を実装することで、インターネットリンクに過剰な負荷を送り、内部または外部への正規のトラフィックを阻害する DDoS 攻撃も防止できます。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GRESS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 ホワイトペーパー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 Code-Red 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で実現し、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。

## Code Red の被害を緩和するその他のシスコネットワーク技術

### ネットワーク識別型アプリケーション認識 (NBAR)

ネットワーク識別型アプリケーション認識 (Network-Based Application Recognition ; NBAR) は、Cisco IOS® Software に含まれる分類エンジンです。URL や MIME ( Multipurpose Internet Mail Extensions ) タイプからの HTTP 識別のほか、動的なポート割り当てを利用するプロトコルなど、幅広い種類のアプリケーションレベルプロトコルを認識できます。NBAR によってトラフィックが分類されると、トラフィックの各分類クラスに対し、適切な QoS ( Quality of Service ) ポリシーが適用されます。NBAR は CRv1 および CRv2 からの URL 要求であれば認識しますが、Code-Red II からの URL 要求は認識できません。これは、Code-Red II が複数のパケットを使用して GET 要求を拡散するのに対し、現在の NBAR では最初のパケットしか検査できないためです。NIDS と異なり、NBAR は CRv1 および CRv2 トラフィックを瞬時に分類し、サーバに到達する前にこれを破棄することができます。NBAR は、内部または外部への両方向に使用することで、Code-Red の被害を緩和できます。

NBAR に関する詳細は、以下の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm>

### コンテンツエンジンおよびコンテンツアクセラレータ

コンテンツ認識デバイスは、通常は Webサーバなどのコンテンツエンジンによって実行される機能の一部を、高速ネットワークアプライアンスに割り当てて負荷を軽減する方法によって、コンテンツ配信を行います。こうしたデバイスはコンテンツの要求側と提供側の接続を仲介するので、接続の確立を変更できます。こうしたデバイスを使用すると、ユニークな HTTP 要求に基づいて Code-Red の侵入を検出し、Webサーバに到達する前にこれを破棄できます。この機能を実現するには、内部の遮断 / 許可リストを使用する方法と、Websense と統合する方法の 2 つがあります。内部の遮断 / 許可リストを使用する方法では、内部の遮断 / 許可機能を使用して、指定の URL リストを明示的に遮断または許可します。これには、許可または遮断すべき URL のリストを表すテキストファイルを管理者がアップロードします。リスト内の URL は、URL の先頭文字列から部分一致を探す方法で照合されます。シスコでは、この技術の中～高速で使用することはお勧めしません。CE ( Content Engine ) に負荷がかかりすぎると、WCCP ( Web Cache Control Protocol ) はバイパスモードに切り替わり、パフォーマンス条件が解決するまでフィルタリングを中止してしまうためです。

CE に関する詳細は、以下の URL を参照してください。

[http://www.cisco.com/warp/public/779/largeent/learn/technologies/content\\_networking](http://www.cisco.com/warp/public/779/largeent/learn/technologies/content_networking)



## シンクホールルータ

シンクホールルータを設定すると、NIDSが利用できない場合に、ネットワーク環境から感染システムを検出しやすくなります。これには、IANA (Internet Assigned Numbers Authority) によってまだ割り当てられておらず、Code-Redが意図せず利用する可能性のあるアドレスを使用します。シンクホールルータは、これらのネットワークをローカルに限定して広告します。このため、これらのネットワークへ向かうパケットは、すべてシンクホールルータにルーティングされます。シンクホールルータはこうしたパケットを受信すると、ログを記録した上で破棄します。このログの結果、感染ホストのリストが得られます。

シンクホールルータの機能的な構成設定方法に関する詳細は、以下のURLを参照してください。

<http://www.cisco.com/public/cons/isp/security/>

## SAFE ブループリント

SAFEブループリントは、これまでに述べたすべてのセキュリティ技術を使用して、Code-Redの被害を緩和します。したがって、SAFEブループリントは「Code-Redセーフ(耐Code-Red)」となっています。SAFEブループリントでは、インGRESSおよびイーGRESS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ヤウォールは、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Code-Red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、Code-Red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Code-Redから守ることは、最初の一步にすぎません。Code-Red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、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、Code-Red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対策のための設計または実装上の変更がいったい必要なかった点です。IISの不正利用およびCode-Redの検出に必要となったのは、NIDSシグネチャの定期的な更新のみでした。Code-Redや、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お勧めできません。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。

## 設定についての情報

このセクションでは、本文書で取り上げた技術のうち、SAFEの一部として攻撃緩和機能のテストを行わなかったいくつかの技術、または後から設定変更が必要となった技術の設定例を示します。HIDSについては、その攻撃緩和機能がそのまま利用でき、稼働システム内に実装する以外は特に追加設定を必要としないため、ここでは触れていません。

### NIDS 攻撃シグネチャ

以下のシグネチャは、SAFEブループリントの多数のモジュール内のNIDSシステム (Cisco Secure IDS 4210 Sensor、Cisco Secure IDS 4230 Sensor、Intrusion Detection System Module) に追加されたものです。

#### インデックスサーバへの不正アクセス

文字列 :

```
"[Gg][Ee][Tt].*.[Ii][Dd][Aa][x00-\x7f]+[x80-\xff]"
```

出現回数 : 1

ポート : 80

Webサーバが他のTCPポート (ポート8080など) から受信している場合は、各ポート番号に対して独自の文字列一致を設定する必要があります。

推奨するアラーム重大度レベル :



- High (Cisco Secure Policy Manager [CSPM])
- 5 (UNIX Director)

Code-Red ワームのバッファオーバーフローによるインデックスサーバアクセス

文字列：

```
"[/]default[.]ida[?][a-zA-Z0-9]+%u"
```

この文字列には、空白スペースが含まれないことに注意してください。

出現回数：1

ポート：80

Webサーバが他のTCPポート（ポート8080など）からも受信している場合は、各ポート番号に対して独自の文字列一致を設定する必要があります。

推奨するアラーム重大度レベル：

- High (CSPM)
- 5 (UNIX Director)

NBAR マーキング

これらの構成には、Cisco 7206 VXRが使用されました。以下に、3種類のパケット破棄手法を示します。テストの結果、NBARポリシーによるCPU稼働率への影響が最も低かったことは注目に値します。以下のコマンドはCode-Redトラフィックを分類し、最初のDSCP (Differential-Services-Control-Point)値でマークします。

```
class-map match-any http-hacks
match protocol http url "*default.ida*"
policy-map mark-inbound-http-hacks
class http-hacks
set ip dscp 1
interface FastEthernet 2/0
service-policy input mark-inbound-http-hacks
interface ATM 4/0
service-policy input mark-inbound-http-hacks
```

ACLブロックとログ機能を使ったNBARマーキング（オプション）

以下のコマンドは、DSCPマーキングを使用して、デバイスから外部へ向かおうとするパケットを拒否し、その過程をログに記録します。ACL（アクセス制御リスト）を有効にする場合は、ルータに過剰なパケット負荷を与えないように特に注意が必要です。

```
access-list 105 deny ip any any dscp 1 log
```

```
access-list 105 permit ip any any
```

```
interface ATM 4/0
```

```
ip access-group 105 out
```

```
interface FastEthernet 2/0
```

```
ip access-group 105 out
```

ポリシールートをNull 0とするNBARマーキング

以下のコマンドは、DSCPマーキングとポリシールーティングの組み合わせによってパケットを破棄します。

```
access-list 106 permit ip any any dscp 1
```

```
route-map null_policy_route 10
```

```
match ip address 106
```

```
set interface Null 0
```

```
interface ATM 4/0
```

```
ip policy route-map null_policy_route
```

```
interface FastEthernet 2/0
```

```
ip policy route-map null_policy_route
```

NBARポリシーの設定によるパケット破棄

以下のコマンドは、NBARポリシーの設定によってパケットを破棄します。

```
policy-map drop-inbound-http-hacks
```

```
class http-hacks
```

```
police 100000000 50000 50000 conform-action drop
exceed-action drop
```

```
exit
```

```
interface ATM 4/0
```

```
service-policy input drop-inbound-http-hacks
```

```
interface FastEthernet 2/0
```

```
service-policy input drop-inbound-http-hacks
```

## コンテンツエンジン (透過モード)

以下のコマンドは、正規表現との照合によってCode-Redシグネチャを検索する遮断ルールを設定して、該当パケットを破棄します。この機能は、CE-550およびCE-590コンテンツエンジンを使用してテスト済みです。

```
!CE blocking filter rule
```

```
rule block url-regex ^http://.*/default\..ida$
```

## 関連情報へのリンク

シスコシステムズによるCode-Red対策と必要なパッチ(英語):

<http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml>

MicrosoftによるCode-Red対策と必要なパッチ(英語):

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp>

Cisco Technical Assistance Center (TAC) による、Code-Red対策のための技術的なヒント(英語):

[http://www.cisco.com/warp/public/63/codered\\_index.shtml](http://www.cisco.com/warp/public/63/codered_index.shtml)

eEyeによるCode-Red関連文書(英語):

<http://www.eeye.com/html/Research/Advisories/AL20010717.html>

<http://www.eeye.com/html/Research/Papers/DS20010802.html>

IISの脆弱性およびNIDSシグネチャIDの解説(英語):

[http://www.cisco.com/go/csec. Search for ID 3394.](http://www.cisco.com/go/csec.Search%20for%20ID%203394)

Computer Emergency Response Team (CERT) によるCode-Red関連情報(英語):

<http://www.cert.org/advisories/CA-2001-19.html>

<http://www.cert.org/advisories/CA-2001-23.html>

SAFEブループリントに関する情報(英語):  
[www.cisco.com/go/safe](http://www.cisco.com/go/safe)

シスコの製品およびサービスへのリンク(英語):

NIDS: <http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz>

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およびセキュリティコンサルティングに関する情報(英語):

<http://www.cisco.com/go/security>

<http://www.cisco.com/go/securityconsulting>

Cisco PIX® Firewall :

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

コンテンツネットワーク機器であるコンテンツエンジン/コンテンツサービススイッチ(CE/CSS)に関する情報:

<http://www.cisco.com/jp/product/product/scale/index.html>

Websenseコンテンツフィルタリングサーバ(英語):

[http://www.cisco.com/warp/public/779/largeent/partner/esap/profiles/websense\\_entv3.html](http://www.cisco.com/warp/public/779/largeent/partner/esap/profiles/websense_entv3.html)

