セキュリティに関するリファレンス情報

セキュリティ アドバイザリと注意事項は、Product Security Incident Response Team（PSIRT）からのその他の情報と一緒に、『http://www.cisco.com/go/psirt』に掲載されています。

ベスト プラクティス

Cisco ルータにおけるセキュリティの向上

このドキュメントは、ネットワーク管理者がセキュリティを強化するためにルータ（特に境界ルータ）上の変更を考慮すべき一部のシスコの構成時の設定に関する非公式の資料です。このドキュメントでは、IP ネットワークのほぼ全般に適用できる基本的な「ボイラープレート」設定項目と、不測の事態を招くいくつかの要注意項目を取り上げています。

Cisco IOS のパスワード暗号化情報

シスコ コンフィギュレーション ファイル内のユーザ パスワード（およびその他のパスワード）を復号化するためのプログラムが、シスコ以外の情報源から公開されています。このプログラムでは、enable secret コマンドで設定されたパスワードは復号化できません。このプログラムを原因とする予想外の懸念がシスコのお客様の間に広がっていることから、シスコのパスワード暗号化を利用している方の多くが、仕様以上のセキュリティを期待しているのではないかと考えました。このドキュメントでは、Ciscoパスワード暗号化の背後にあるセキュリティモデルと、その暗号化のセキュリティ制限について説明します

シスコの SAFE の設計

SAFE は、企業が e-ビジネスに安全に取り組めるようにする、総合的なセキュリティ設計です。SAFE では、ネットワークの成長と変更に伴って、セキュリティの設計、実装、および管理を容易に行えるモジュラ方式を採用し、Cisco Architecture for Voice, Video and Integrated Data（AVVID）上に構築されたネットワークを強化します。

攻撃を防御、トラッキング、緩和するための戦略

シスコ ルータによるパケット フラッディングの特性把握とトレーシング

> Denial of Service（DoS; サービス拒絶）攻撃は、インターネットで一般的な攻撃です。このような攻撃に対する最初のステップは、攻撃の種類を正確に見分けることです。一般的に使用される DoS 攻撃の多くは、高帯域幅のパケット フラッドや、その他の反復的なパケット ストリームによるものです。この文書では、これらの攻撃とトレース方法について、詳細に説明しています。

Nimda ウィルスに対抗する戦略

この項目では、Nimda ウィルスに対抗するためのテクニカル ティップスと、影響を軽減するための推奨事項を包括的に一覧しています。

Code Red ワームに対抗する戦略

この項目では、Code Red ワームに対抗するためのテクニカル ティップスと、影響を軽減するための推奨事項を包括的に一覧しています。

分散型サービス拒絶（DDoS）攻撃を防ぐ対策

このホワイトペーパーでは、潜在的なDDoS攻撃の発生方法と、それに対する防御にCisco IOSソフトウェアを使用するための推奨方法について技術的に説明します。

UDP 診断ポート サービス拒否攻撃に対する防御戦略

このホワイトペーパーでは、潜在的なUDP診断ポート攻撃の発生方法と、それに対する防御にCisco IOSソフトウェアを使用するための推奨方法について技術的に説明します。

TCP SYN サービス拒否攻撃に対する防御戦略

この White Paper では、潜在的な TCP SYN の攻撃がどのように発生するかについての技術的側面を説明し、Cisco IOS ソフトウェアを使用してこの攻撃を防御する推奨手法を説明します。

The Latest in Denial of Service Attacks:"Smurfing" Description and Information to Minimize Effects
注：上記のリンクは、シスコシステムズの管理外にある外部サイトを参照しています。

「smurf」攻撃に関する詳細な情報を提供し、シスコのルータと、これらの攻撃の影響を軽減する方法に焦点を当てます。一部の情報は一般的なもので、組織の特定のベンダーに関連するものではありません。ただし、これはシスコルータに焦点を当てて書かれています。このドキュメントは、「smurf」攻撃が他のベンダーの機器に及ぼす影響を確認するものではありません。ただし、さまざまなベンダーに関する情報が含まれています。

その他のリソース

Cisco 製品のセキュリティ上の問題への対応

この文書では、不具合情報と、問題が発生したときの対応手順について説明しています。特に、セキュリティ攻撃にさらされているときや、攻撃の可能性がある思われるとき、使用しているシスコ製品にセキュリティ上の問題があると思われるとき、シスコ製品に関する技術的なセキュリティ情報を入手したいとき、あるいはシスコ製品に関する公表済みのセキュリティ問題について質問がある場合などに行うことを説明しています。また、セキュリティに関する問題を処理する際の Cisco Product Security Incident Response Team（PSIRT）の役割についても説明しています。
