IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2008 年 2 月 6 日
独立行政法人 情報処理推進機構

「TCP/IP に係る既知の脆弱性検証ツール」を公開

～脆弱性の再発防止のため、TCP/IP 実装製品の開発者向けに無償貸出～

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、インターネットに接続する電子機器の情報セキュリティ対策を推進するため、インターネットの標準的な通信手順である TCP/IP(Transmission Control Protocol / Internet Protocol)を実装する製品の開発者向けに、TCP/IP に係る既知の脆弱性検証ツールを 2008 年 2 月 6 日（水）より公開しました。

コンピュータをはじめとしたインターネットに接続する電子機器には、TCP/IP ソフトウェアが組み込まれています。 近年では、情報家電や携帯端末などの組込み機器にも使われるようになり、TCP/IP ソフトウェアは広く利用されています。

TCP/IP を実装したソフトウェアは、これまで多くの脆弱性が発見、公表され、機器ごとに対策が施されてきました。しかし、こうした脆弱性を体系的に検証するツールが整備されてこなかったことから、新たに開発されるソフトウェアで、既に公表されている脆弱性の対策が実装されず、脆弱性が「再発」するケースが見受けられます。このような課題に対応するため、IPA では、TCP/IP 実装製品の開発者向けに「TCP/IP に係る既知の脆弱性検証ツール」を開発し、2008 年 2 月 6 日（水）より CD-ROM での貸出を開始しました。

■ツールの概要

本ツールは、2008 年 1 月 8 日に公開した「TCP/IP に係る既知の脆弱性に関する調査報告書（改訂第 3 版）」に記載している 23 項目の脆弱性のうち、18 項目の脆弱性を体系的に検証できるツールです（詳細「別紙」参照」。

図 1 に示すように、TCP/IP を実装する製品開発者は、本ツールを使用することにより、検証対象機器の脆弱性検証を自動実行し、脆弱性の有無を簡易判定できます。また、脆弱性の判断のための確認ガイドを参照することにより、脆弱性の有無の正確な判断ができます。

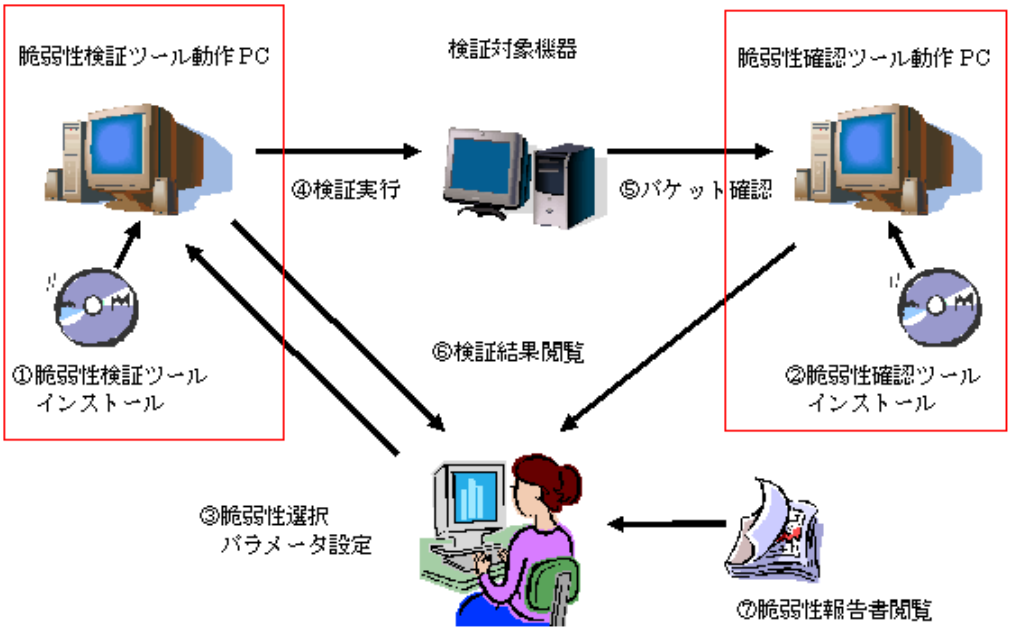

図 1．検証ツールの利用イメージ

■検証ツールの貸出方法

1. 貸出対象

原則として、次の条件を満たす開発者へ検証ツールを貸出します。

（1）TCP/IP を実装する日本国内の製品開発ベンダーで、法人格を持つ事業体であること。

（2）不正使用禁止の「利用許諾条件合意書」に合意していただくこと。

（3）場合によって、会社経歴書などの提出を求めることがあります。

2. 費用および期間

費用は無償です。貸出期間は 1 年間（更新可能）です。

3. 申込手順

（1）申込受付は電子メールにて行います。記載事項は以下のとおりです。

受付アドレスは、E-mail：vuln-inq@ipa.go.jp です。

・メールの件名：TCP/IP 脆弱性検証ツールの貸出の申込み

・記載事項：1. 申込者の所属法人名、所属部署名

2. 所属法人がウェブサイトを公開している場合はその URL

3. 申込者の氏名と読み仮名

4. 申込者の連絡先電子メールアドレス、連絡先電話番号

5. 本ツールで脆弱性検証を予定している対象機器の概要

（2）IPA より申込者の連絡先電子メールアドレスへ「利用許諾条件合意書」を返信します。

（3）申込者は「利用許諾条件合意書」に必要事項を記載の上 IPA に郵送。IPA は合意書を受領し記載事項確認後、「TCP/IP に係る既知の脆弱性検証ツール」を格納した CD-ROM を郵送します。

（参考）

・TCP/IP に係る既知の脆弱性に関する調査報告書（改訂第 3 版）2008 年 1 月公表
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター　山岸／渡辺
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503　Fax:03-5978-7510　E-mail: pr-inq@ipa.go.jp

別 紙

「TCP/IP に係る既知の脆弱性検証ツール」検証可能な脆弱性一覧

（「TCP/IP に係る既知の脆弱性に関する調査報告書（改訂第 3 版）」に記載している脆弱性 23 項目との対比）

＜TCP（ Transmission Control Protocol ）関連＞		
1.	○	TCP の初期シーケンス番号予測の問題
2.		TCP 接続の強制切断の問題
3.	◎	SYN パケットにサーバ資源が占有される問題（SYN Flood Attack）
4.	○	特別な SYN パケットによりカーネルがハングアップする問題（LAND Attack）
5.	◎	データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題（Overlapping Fragment Attack）
6.	○	十分に小さい分割パケットがフィルタリングをすり抜ける問題（Tiny Fragment Attack、Tiny Overlapping Fragment Attack）
7.		PAWS 機能の内部タイマを不正に更新することで、TCP 通信が強制的に切断される問題
8.		Optimistic TCP acknowledgements により、サービス不能状態に陥る問題
9.	○	Out of Band（OOB）パケットにより、サービス不能状態に陥る問題
＜ICMP（ Internet Control Message Protocol ）関連＞		
10.	○	パケット再構築時にバッファが溢れる問題 （Ping of death）
11.	○	ICMP Path MTU Discovery 機能を利用した通信遅延の問題
12.	○	ICMP リダイレクトによるサービス応答遅延の問題
13.	○	ICMP リダイレクトによる送信元詐称の問題
14.	○	ICMP 始点抑制メッセージによる通信遅延の問題
15.	○	ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題（ICMP トンネリング）
16.	○	ICMP エラーにより TCP 接続が切断される問題
17.	○	ICMP Echo リクエストによる帯域枯渇の問題（Ping flooding, Smurf Attack, Fraggle Attack）
＜IP（ Internet Protocol ）関連＞		
18.	○	フラグメントパケットの再構築時にシステムがクラッシュする問題（Teardrop Attack）
19.	○	パケット再構築によりメモリ資源が枯渇される問題（Rose Attack）
20.		IP 経路制御オプションが検査されていない問題（IP Source Routing 攻撃）
＜ARP（ Address Resolution Protocol ）関連＞		
21.	○	ARP テーブルが汚染される問題
22.	○	ARP テーブルが不正なエントリで埋め尽くされる問題
＜その他（ TCP/IP 全般 ）＞		
23.		通常でないパケットへの応答によって OS の種類が特定できる問題(TCP/IP Stack Fingerprinting)

（注） ○ ：IPv4(Internet Protocol Version 4)環境で検証が可能な項目

◎ ：IPv4、IPv6 環境での検証が可能な項目