INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

TCP/IPに係る既知の
脆弱性検証ツールバージョン 5.0 の開発

株式会社ラック　江口　慶、高坂　史彦、須田　堅一、芝原　潤一、吉永　昇

概要

TCP/IP に係る既知の脆弱性が多数公表されている。これらの脆弱性の中には、脆弱性と言えるのかどうか曖昧なものや、仕様上の問題で、対策が難しいものも含まれている。新しい TCP/IP の実装を作り込む場合には、このような既知の脆弱性を十分考慮する必要がある。また、新しい TCP/IP の実装に対して、これらの既知の脆弱性が存在しないかを検証するツールが必要である。

本プロジェクトでは、「TCP/IP に係る既知の脆弱性検証ツール V4.0」を基に機能拡張を実施した。これにより利用者を拡大させ、ソフトウェア開発者自身による更なる脆弱性対策を促進することを目的とした。

1.　背景

コンピュータ、機器に広く組み込まれている TCP/IP ソフトウェアに関して多数の脆弱性が公表されている。しかし、既知の脆弱性であっても対策を実装せず、そのまま放置するケースが少なくない。IPA では既知の脆弱性を検証するツールを開発/配布することで、開発者自身による開発段階からの脆弱性対策を促進してきた。

2.　目的

本プロジェクトでは「TCP/IP に係る既知の脆弱性検証ツール V4.0」について、これまでの運用実績とユーザからの要望などを踏まえて機能拡張を実施した。特に IPv6 環境での検証項目の追加とツールの利便性を向上させる機能拡張を実施した。これにより利用者を拡大させ、ソフトウェア開発者自身による更なる脆弱性対策を促進することを目的とした。

3.　概要

本プロジェクトでは「TCP/IP に係る既知の脆弱性検証ツール」を構成する脆弱性検証ツールと脆弱性確認ツールについて機能拡張を実施した。これらのツールは検証する脆弱性項目を選択し、利用者が開発したソフトウェアに選択した脆弱性項目が存在するか否かを判定するツールである。

利用者は、脆弱性検証ツール、脆弱性確認ツールを使用して、TCP/IP に係わる脆弱性が開発したソフトウェアに存在するか否かを調査し、脆弱性調査報告書を参照して脆弱性の内容や対策方法を知ることができる。

図 1、図 2 に脆弱性検証ツール、脆弱性確認ツールの利用イメージを示す。利用者

は、インストール CD から脆弱性検証ツール動作 PC に脆弱性検証ツールのプログラムをインストールし、GUI またはコマンドラインを操作することによって検証対象機器に脆弱性が存在するか否かを調査する。調査結果の詳細な内容は脆弱性報告書を参照して知ることができる。(図 1)

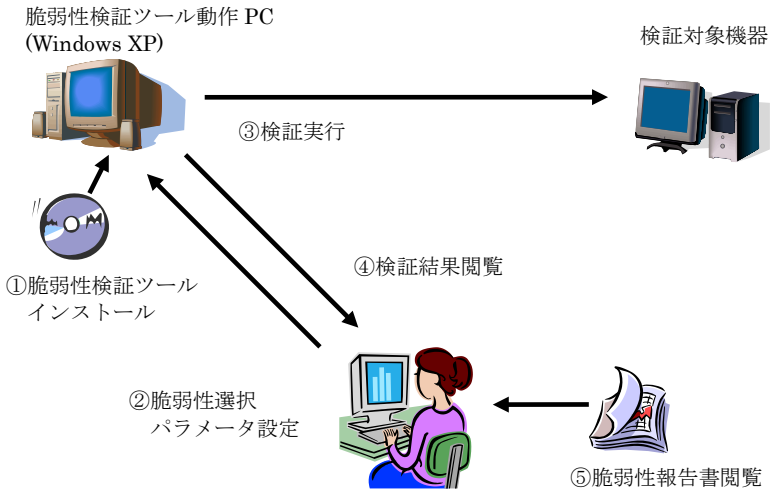

図 1

また、インストール CD から脆弱性確認ツール動作 PC に脆弱性確認ツールのプログラムをインストールし、GUI またはコマンドラインを操作することによって脆弱性検証ツールから送信されたパケットが検証対象機器を通過したか否かを確認することにより、検証対象機器に脆弱性が存在するか否かを調査する。(図 2)

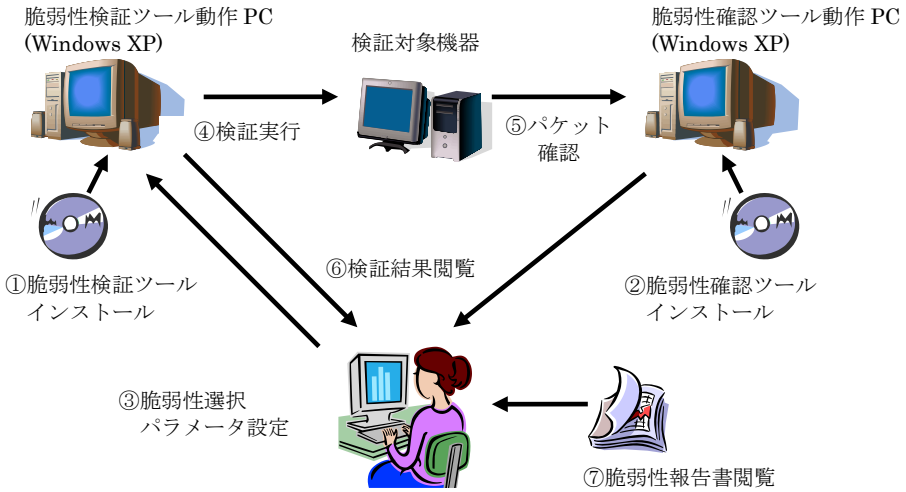

図 2

4. バージョン 5.0 で拡張した機能

バージョン 5.0 では、これまでの運用実績とユーザからの要望などを踏まえて以下の機能拡張を実施した。

(1) IPv6 環境での検証項目の拡張

バージョン 4.0 までは IPv6 環境での検証項目は 5 項目であったが、バージョン 5.0 では 9 項目を追加した。(表 1)

検証項目の追加によりバージョン 5.0 では IPv6 環境では 14 項目の検証が可能になった。

表 1

No	IPv4	IPv6	項目名
1	○	◎	TCP の初期シーケンス番号予測の問題
2	○	○	SYN パケットにサーバ資源が占有される問題 (SYN Flood Attack)
3	○	◎	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)
4	○	○	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)
5	○	○	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)
6	○	—	Out of Band(OOB)パケットにより、サービス不能状態に陥る問題
7	○	○	パケット再構築時にバッファが溢れる問題(Ping of death)
8	○	◎	ICMP Path MTU Discovery 機能を利用した通信遅延の問題
9	○	◎	ICMP リダイレクトによるサービス応答遅延の問題
10	○	◎	ICMP リダイレクトによる送信元詐称の問題
11	○	—	ICMP 始点制御メッセージによる通信遅延の問題
12	○	○	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)
13	○	◎	ICMP エラーにより TCP 接続が切断される問題
14	○	◎	ICMP Echo リクエストによる帯域枯渇の問題 (Ping flooding, Smurf Attack, Fraggle Attack)
15	○	◎	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)
16	○	—	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)
17	○	—	IP ヘッダオプションのデータ長が 0 のパケットの問題
18	—	◎	IPv6IPComp パケットの処理によるサービス不能状態に陥る問題
19	○	—	ARP テーブルが汚染される問題
20	○	—	ARP テーブルが不正なエントリで埋め尽くされる問題

○：V4.0 までに実装済み　　◎：V5.0 で追加実装

－：未実装

(2) パラメータのインポート/エクスポート

バージョン 4.0 までは毎回パラメータを手動で設定し直すため、同じパラメータを使った複数回の検証が困難だった。

バージョン 5.0 では以下のパラメータをインポート/エクスポートする機能拡張を実施した。

1. 検証対象機器の IP アドレス
2. 脆弱性項目のパラメータ

エクスポート機能により、検証対象機器の IP アドレスと脆弱性項目のパラメータを保存できる。形式は検証対象機器の IP アドレスはテキストファイル、脆弱性項目のパラメータは XML ファイルである。2 回目以降は、インポート機能により前述したファイルをそれぞれ読み込むことで、前回設定したパラメータを再利用できる。複数回の検証でもパラメータをインポートすれば、毎回手動で設定しなくても簡単に検証できる。

(3) 検証結果の出力

バージョン 4.0 までは検証結果が GUI 画面上にしか表示されないため、後から複数回の検証結果を比較するなど再利用が困難であった。

バージョン 5.0 では以下の検証結果を出力する機能拡張を実施した。

1. 脆弱性検証の結果
2. 詳細ログ

検証結果の出力機能により、脆弱性検証の結果と詳細ログを保存できる。形式は脆弱性検証の結果は CSV ファイル、詳細ログはテキストファイルである。

検証毎に保存することで、各検証結果を比較するなど再利用ができる。他にも過去の検証で設定したパラメータの確認、ツール起動中に不測の事態が発生した場合に原因の推測などができる。

(4) コマンドラインからの実行

バージョン 4.0 までは検証に必要なパラメータ設定や結果出力が全て GUI 操作であるため、ツールの自動化(バッチ処理)が困難であった。

バージョン 5.0 ではコマンドラインから実行する機能拡張を実施した。

コマンドラインで実行するためには、事前にユーザが手動で以下の３つのファイルを作成する必要がある。

1. 設定ファイル
2. パラメータファイル
3. IP アドレスファイル

３つのファイルを準備した後、コマンドラインから実行すると以下の３つのファイルを出力する。

1. 検証結果ファイル
2. 詳細ログファイル
3. エラーログファイル

コマンドラインからの実行機能により、自動実行(バッチ処理)ができる。バッチファイルにツールを実行するコマンドを記載し、このファイルをタスクスケジューラに登録すれば、指定した時間にツールを自動実行できる。他にも外部のソフトウェアから検証ツールを実行するなど検証方法に選択の幅ができる。

5. ツールの仕組み

(1) システム構成

「TCP/IP に係る既知の脆弱性検証ツール」は脆弱性検証ツールと脆弱性確認ツールで構成され、Windows XP Professional を搭載した IBM AT 互換機上で動作する。これらのツールは、各種指示を行うメインプログラムと、攻撃パケットを送信/受信する脆弱性検証モジュールの２つに分かれる。

(2) 機能

- 攻撃シミュレーション機能

20 の脆弱性検証モジュール(IPv4 に関しては 19、IPv6 に関しては 14 の脆弱性検証モジュール)により、当該脆弱性を突く攻撃パケットを送信する。

脆弱性検証モジュールは、今後、追加することが可能である。

- サービス監視機能

検証対象の機器に対して、任意の TCP ポートが接続可能かどうかを、検証中と検証終了後に定期的に監視し、脆弱性に対する効果の有無を調査することができる。接続不能な状態が指定した回数連続して発生すると、効果が有ったと判定する。ただし、脆弱性に対する効果の有無は、この機能だけでは判断できないが、判断に対する１つの材料として活用できる。

脆弱性に対する効果の確認方法については、取扱説明書に詳しく明記している。

(3) ユーザインターフェイス(検証ツール)

- 脆弱性項目選択

図 3 に『脆弱性項目選択』画面を示す。

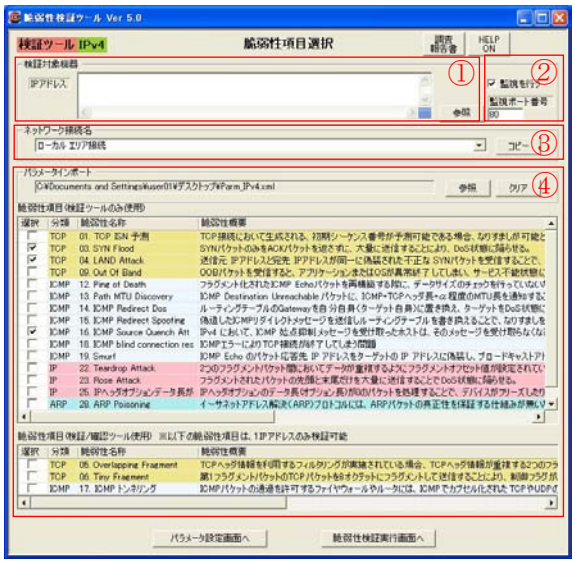

図 3

検証に必要な以下の項目を設定する。

① 検証対象機器の IP アドレス
   - [参照]ボタンから IP アドレスをインポートできる

② サービス監視機能の監視ポート番号

③ 使用するネットワーク接続名

④ 検証する脆弱性項目
   - [参照]ボタンからパラメータをインポートできる

また、[調査報告書]ボタンをクリックすると PDF 形式の TCP/IP に係る既知の脆弱性に関する調査報告書を表示する。

- パラメータ設定

図 4 に『パラメータ設定』画面を示す。

図 4

脆弱性項目毎に、攻撃パケットに関するパラメータとサービス監視に関するパラメータを入力する。これらのパラメータの設定方法については、取扱説明書にて詳しく明記している。

- 脆弱性検証実行

図 5 に『脆弱性検証実行』画面を示す。

図 5

選択した脆弱性項目が表示される。ここで[実行]ボタンをクリックすると検証を開始する。

また、実行前に[参照]ボタンよりログファイルの保存先を指定することで、テキスト形式の詳細ログを取得できる。

- 脆弱性検証確認

図 6 に『脆弱性検証確認』画面を示す。

図 6

検証状況と脆弱性判定が表示される。

検証状況では、表 2 に示す表示が行われる。

表 2

表示内容	説明
ー	まだ実行されていません。
検証中	検証を行っています。
監視中	サービスの監視を行っています。
検証エラー	攻撃パケットの送信処理において、エラーが発生しました。 ネットワークの接続を確認してください。また、送信間隔とパケット送信回数を調整して、再度検証を行ってください。
中止	[一時停止]ボタンをクリック後、検証が中止されました。
スキップ	脆弱性判定結果が有り、又は、検証エラーの場合、残りの脆弱性項目の検証をスキップし、次の対象機器の検証を開始します。
完了	検証と監視が終了しました

脆弱性判定では、表 3 に示す表示が行われる。

脆弱性判定は、単純なサービスポートの監視結果を見ているに過ぎない。実際の脆弱性の有無は、検証対象機器の状態を、検証者が確認する必要がある。確認方法については、取扱説明書にて詳しく解説している。

表 3

表示内容	説明
ー	まだ判定されていません。あるいは、サービス監視を行いませんでした。あるいは、検証がエラーとなりました。
無し	サービス監視で異常はありませんでした。
有り	サービス監視で異常の回数がしきい値に達しました。
有りの疑い	サービス監視で異常がありましたが、回数がしきい値に達しませんでした。

エクスポート機能により、各種データをファイルに出力できる。以下に示すボタンよりファイルの保存先を指定することで、各種データを取得できる。

① [結果出力]ボタン
- 脆弱性検証の結果を記載した CSV ファイルを出力する

② [IP アドレスエクスポート]ボタン
- 検証対象機器の IP アドレスを記載したテキストファイルを出力する。このファイルはインポート機能やコマンドラインからの実行機能で利用できる

③ [パラメータエクスポート]ボタン
- 脆弱性項目のパラメータを記載した XML ファイルを出力する。このファイルはインポート機能やコマンドラインからの実行機能で利用できる

● コマンドラインからの実行

コマンドラインを用いて検証を行うためには、事前に設定ファイルや利用するパラメータを準備する必要がある。以下に必要なファイルと準備する方法を示す。

① 設定ファイル
- ツール起動に必要な情報を記載した INI ファイル。ユーザが手動で作成する必要がある

② IP アドレスファイル
- 検証対象機器の IP アドレスを記載したテキストファイル。GUI からエクスポート機能により作成できる

③ パラメータファイル
- 脆弱性項目のパラメータを記載した XML ファイル。GUI からエクスポート機能により作成できる

３つのファイルを準備した後、コマンドラインから設定ファイルをパラメータに指定することで検証を実行できる。

検証終了後は検証結果として３つのファイルを出力する。

① 結果出力ファイル
- 脆弱性検証の結果を記載した CSV ファイル

② 詳細ログファイル
- 検証ツールと脆弱性検証モジュールの詳細ログを記載したテキストファイル

③ エラーログファイル
- 検証ツールと脆弱性検証モジュールのエラーメッセージを記載したテキストファイル

(4) ユーザインターフェイス(確認ツール)

- 脆弱性項目選択

図 7 に『脆弱性項目選択』画面を示す。

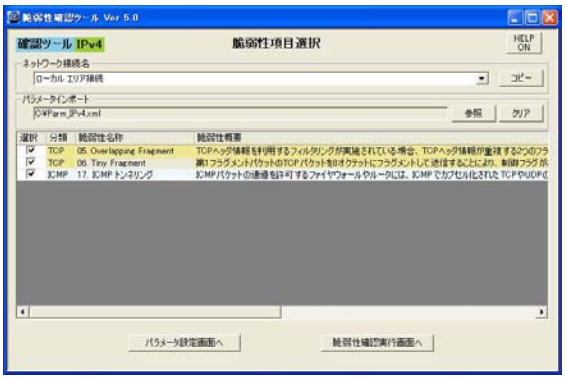

図 7

以下の項目を設定する。

① 使用するネットワーク接続名

② 脆弱性項目の選択
- ［参照］ボタンからパラメータをインポートできる

- パラメータ設定

図 8 に『パラメータ設定』画面を示す。

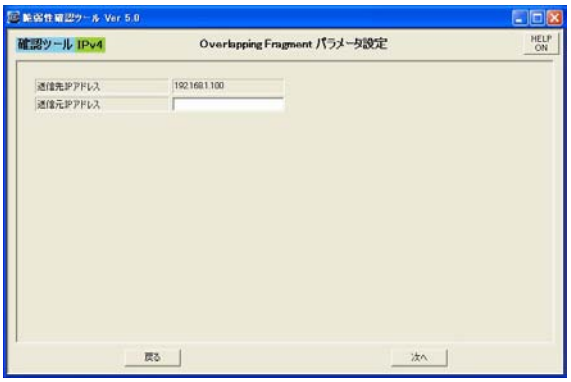

図 8

脆弱性項目毎に、攻撃パケットに関するパラメータを入力する。これらのパラメータの設定方法については、取扱説明書にて詳しく解説している。

- 脆弱性確認実行

図 9 に『脆弱性確認実行』画面を示す。

図 9

選択した脆弱性項目が表示される。ここで[実行]ボタンをクリックすると、検証を開始する。

また、実行前に[参照]ボタンよりログファイルの保存先を指定することで、テキスト形式の詳細ログを取得できる。

- 脆弱性確認

図 10 に『脆弱性確認』画面を示す。

図 10

脆弱性判定では、表 4 に示す表示が行われる。検証ツールから送信されたパケットを受信すると検証対象機器に脆弱性が存在すると判断し”有り”と表示される。

表 4

表示内容	説明
ー	まだパケットの到着が確認されていません
有り	パケットの到着が確認されました

エクスポート機能により、各種データをファイルに出力できる。以下に示すボタンよりファイルの保存先を指定することで、各種データを取得できる。

① [結果出力]ボタン
- 脆弱性検証の結果を CSV ファイルに出力する

② [パラメータエクスポート]ボタン
- 脆弱性項目のパラメータを XML ファイルに出力する。このファイルはインポート機能やコマンドラインからの実行機能で利用できる

- コマンドラインからの実行

コマンドラインを用いて検証を行うためには、事前に設定ファイルや利用するパラメータを準備する必要がある。以下に必要なファイルと準備する方法を示す。

① 設定ファイル
- ツール起動に必要な情報を記載した INI ファイル。ユーザが手動で作成する

② パラメータファイル
- 脆弱性項目のパラメータを記載した XML ファイル。GUI からエクスポート機能により作成できる

２つのファイルを準備した後、コマンドラインから設定ファイルをパラメータに指定

することで検証を実行できる。

検証終了後は検証結果として３つのファイルを出力する。

① 結果出力ファイル
- 脆弱性検証の結果を記載したCSV ファイル

② 詳細ログファイル
- 確認ツールと脆弱性検証モジュールの詳細ログを記載したテキストファイル

③ エラーログファイル
- 確認ツールと脆弱性検証モジュールのエラーメッセージを記載したテキストファイル

6. 今後の課題

TCP/IP に係る脆弱性を突く攻撃手法が新たにインターネット上に公開された場合などは検証項目を追加する必要がある。特に IPv6 の普及が進められていることから、IPv6 環境での脆弱性検証項目を充実させることが必要であると考える。

また、ツールの動作環境が Windows XP のみであるため、今後は Windows 7 への対応が必要であると考える。

－ 以上 －