既存脆弱性情報を利用したクライアント向け脆弱性検査システムの提案と評価

藤堂 洋介 † 朝倉 康生 ‡ 森井 昌克 ‡

† 神戸大学工学部
657-8501 神戸市灘区六甲台町 1-1

todo@stu.kobe-u.ac.jp
‡ 神戸大学大学院工学研究科
657-8501 神戸市灘区六甲台町 1-1

yasakura@stu.kobe-u.ac.jp, mmorii@kobe-u.ac.jp

あらまし 本稿では Web 上に存在する既存脆弱性情報を利用した，クライアント向け脆弱性検査システムを提案する．提案システムは，Web 上に存在する脆弱性情報を監視し，新たな情報が出た際に自動でデータベースを作成する．よって，データベースを手動で作成するのに対し，システム運用者への負担が非常に小さくて済み，かつ最新の情報にも対応することが可能である．

A Proposal and Evaluation of the Vulnerability Scanner for Client Using Existing Vulnerability Information

Yosuke TODO † Yasuo ASAKURA ‡ Masakatu MORII ‡

†Faculty of Engineering, Kobe University
1-1 Rokkodai Nada-ku Kobe-shi Hyogo 657-8501 Japan

todo@stu.kobe-u.ac.jp
‡Graduate School of Engineering, Kobe University
1-1 Rokkodai Nada-ku Kobe-shi Hyogo 657-8501 Japan

yasakura@stu.kobe-u.ac.jp, mmorii@kobe-u.ac.jp

Abstract In this paper, we propose a vulnerability scanner for client using existing vulnerability databases. The proposed system observes vulnerability databases existing on the Internet and automatically updates our system's database. So it can reduce the system administrator's tasks compared with the manual updating system, and can keep the database latest.

1 まえがき

近年インターネットの普及により数多くのソフトウェアが生まれユーザに利用されている．しかし，ソフトウェアの脆弱性を利用した攻撃も非常に多くなっている．近年では Adobe Reader の脆弱性を利用してリモートからマルウェアなどを送り込むといった問題が報告されている [1].

こういった問題を防ぐため，各ソフトウェアメーカは脆弱性の存在するソフトウェアを使用しないよう警告する．しかし，多くのユーザはその警告を見落とし，自身のコンピュータに攻撃を受ける可能性を保有した状態にしている．

この問題の背景には，ユーザのコンピュータ

セキュリティに対する関心の低さがあげられる．多くのユーザはセキュリティ対策としてウィルススキャンソフトへの関心が高い．しかし脆弱性に対する関心は未だ低いままである．また，仮に脆弱性対策を施す意志があっても，脆弱性の存在するソフトウェアを使用していないか調べるのは非常に手間のかかる作業となる．よって，ユーザのインストールしているソフトウェアを一括で検査し，ソフトウェアに脆弱性が見つかった場合は対策を施すよう勧告するシステムを提案する．また，提案システムではユーザに脆弱性対策を施すよう勧めるため，脆弱性自体の詳細情報や重要度を明記する．このシステムによりユーザが攻撃を受ける可能性を軽減することができる．

2 既存システム

2.1 自動アップデートシステム

脆弱性対策の手法として最もユーザに使用されているシステムは，各ソフトウェア制作メーカが開発している自動アップデートシステムである．有名なものではマイクロソフトの自動更新[1]，Adobe Updater[2]，などがあげられる．これらのシステムはアップデート対象となるソフトウェアを入手した時点でインストールされる．よって，ユーザは意識せずに脆弱性対策を施すことができる．しかし，意識せず利用されているためユーザの脆弱性対策への関心を高める効果を期待できない．また，バグ修正や機能の追加などの脆弱性対策以外のアップデートも同様の形式で警告される．よって，ユーザに対してアップデートを行わないことがコンピュータのセキュリティ保持において，非常に危険であることを示せない．他にも脆弱性を解決するパッチが未開発の内に行われる攻撃であるゼロデイ攻撃への対策を取ることができない．

[1]Windows や Office と言ったマイクロソフト製品のアップデートを自動で実施するシステム

[2]Adobe Reader や Adobe Flash Player などの Adobe 製品に最新のバージョンがみつかった際警告を出すシステム

2.2 Secunia PSI

提案システムと同様に脆弱性を検知するソフトウェアも存在する．Secunia PSI はデンマークのセキュリティ専門会社の Secunia が開発している脆弱性検知システムである [2]．多くのソフトウェアに対応しているが，実際に脆弱性検知が可能なソフトウェアには偏りが存在する．例に，日本制のフリーソフトである圧縮解凍ソフト Lhaplus などの脆弱性検知を行うことができない．また，発見された脆弱性の詳細内容や危険度の記述が不十分である．ユーザの脆弱性対策への意識の低さの改善を求める上で，発見された脆弱性の内容や危険度を明記することは非常に重要である．

提案システムとの違いとして，検査に用いる脆弱性情報の作成手法の違いがあげられる．Secunia PSI は Secunia 自体が作成した脆弱性データベースを利用することで検査を行う．一方提案システムでは WEB 上に公開されている既存脆弱性データベースを用いる．これは検査に用いる脆弱性データベースの作成の高速化やシステム運用者への負担軽減につながる．また提案システムの手法を用いることで，様々な既存脆弱性データベースを利用した脆弱性検査が可能となる．次章から WEB 上で公開されている既存脆弱性データベースを用いて検査を行う手法を示す．

3 提案システム

3.1 システムの概要

提案システムはサーバクライアント方式のシステムであり，クライアントがサーバ上から最新の脆弱性データベースをダウンロードし，脆弱性検査を行うシステムである．第一に，既存脆弱性データベースから情報を取得し，サーバ上に新たな脆弱性データベースを構築する．本稿ではこのサーバ上に作成されるデータベースのことを，検査用データベースと定義する．また，提案システムが主に利用する既存脆弱性データベースは JVN iPedia[3]，スキャンネットセキュリティ [4]，マイクロソフトセキュリティ情報検索 [5] の三つの脆弱性データベースである．こ

のように複数の脆弱性データベースを利用することで，より正確に多様なソフトウェアの脆弱性検査を可能とする．第二に，サーバ上に作成された検査用データベースとクライアントの検査用データベースを同期させる．第三に，脆弱性検査に必要な情報をクライアントのパソコンから取得する．ただし，ここで言う情報とはクライアントの所有するソフトウェアのバージョンや適用されているマイクロソフト製品のパッチ情報を表す．第四に，クライアントの所有するソフトウェアのバージョンとデータベース上の脆弱性のあるソフトウェアのバージョンを比較する．提案システムは以上の流れで脆弱性検査を行う．

3.2 データベース構築プログラム

提案システムを実装するためには WEB ページである既存脆弱性データベースから，自動で情報を取得し検査用データベースを作成する必要がある．自動で検査用データベースを作成するには既存脆弱性データベースの HTML を解析し，必要な要素を抜き出す必要がある．例に JVN iPeida からの取得法を図 1 に示す．

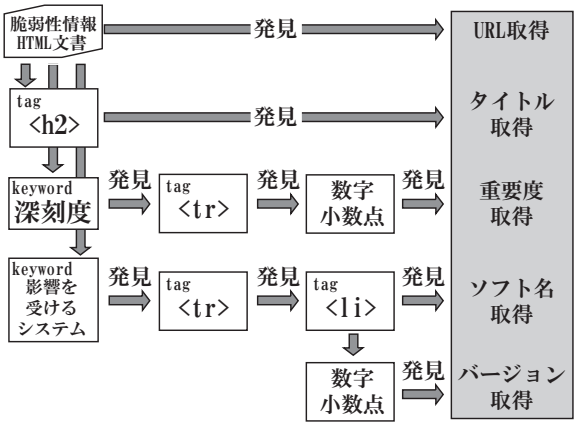

図 1: JVN iPedia からのデータベース取得法

脆弱性情報が記載されている HTML 文書を読み込み，図 1 に記載されているタグやキーワードを見つけ必要な情報を取得していく．li タグからはソフトウェア名とバージョン情報が取得できる．バージョン情報は通常数字と小数点で構成されるので，ソフトウェア名の後に出現する数字と小数点で構成される要素を抜き出すことで，バージョン情報を取得できる．この手法を用いることで，脆弱性データベースの HTML 構文の構造が大きく変更されない限り，自動でデータベースを構築できる．次にマイクロソフトセキュリティ情報検索での取得法を図 2 に示す．マイクロソフトセキュリティ情報検索は，HTML 構文の構造が全ての脆弱性情報で統一化されていない．よって構造の違いごとに固有の取得法を用いる必要がある．ここでは 2009 年の脆弱性情報に主に用いられている HTML 構文の構造での取得法を示す．

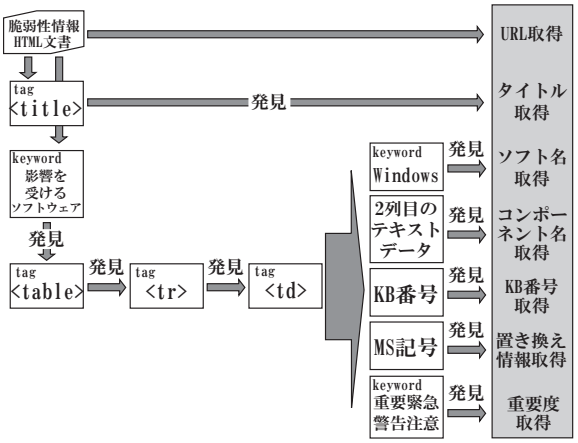

図 2: マイクロソフトセキュリティ情報検索からのデータベース取得法

マイクロソフトセキュリティ情報検索では脆弱性情報を表にまとめて公開している．よってキーワード後の表の各セルを取得し，必要な情報を取得していく．図 2 の KB 番号とはサポート技術情報 (KB) 番号 (以下 KB 番号と表記) と呼ばれ，パッチを特定できるセキュリティ情報に割り振られている番号である．この番号の記述方法は KB[六桁の数字] と決まっており tr タグ内から取得できる．また，MS 記号とはセキュリティ情報 MS で，脆弱性情報に個別に割り振られている記号である．記述方法は MS[年の下二桁]-[三桁の番号] と決まっており KB 番号と同様に tr タグ内から取得できる．マイクロソフトが提供するパッチの中には過去のパッチを内包したパッチが存在し，パッチを適用すると過去のパッチを適用する必要がなくなるものが存在する．このような置き換え可能かの情報はセキュリティ情報検索では MS 記号を用いて記載

されており，マイクロソフト製品の脆弱性検査には必要不可欠な情報である．

3.3 データベースの同期

クライアントは脆弱性検査に用いるための検査用データベースをサーバからダウンロードする必要がある．よって，クライアントは一定期間ごとにサーバ上のデータベースを確認し，自身のデータベースが古いものでないか検査する必要がある．データベースの同期を円滑に行うため，クライアントの所有するデータベースのハッシュ値[3]とサーバ上に存在するデータベースのハッシュ値の比較を行う．このハッシュ値が異なった時のみ，データベースをダウンロードすることとする．こうして，大きな容量のファイルを不必要にダウンロードすることを防ぐことができる．

3.4 バージョンの取得

ユーザが所有しているソフトウェアのバージョンの取得方法を示す．提案システムでは三つの取得方法を用いてバージョンを取得する．一般的にソフトウェアの実行ファイルまたはバイナリファイルには，バージョン情報が記載されている．このバージョンを抜き出すことで取得できる．しかし，取得したバージョン情報が既存脆弱性データベースのバージョン情報と明らかに異なる場合や，実行ファイルやバイナリファイルそのものが存在しない場合がある．よって，以上の手法では取得困難なものに対しては別の手法でバージョンを取得する必要がある．ソフトウェアの中には特定の引数を渡すとバージョンを出力するものがある．その出力を取得することでバージョンを取得できる．また，バージョン情報がレジストリ内に記載されているケースもあり，レジストリの値を取得することでバージョンを取得できる．

次に，ユーザのパソコンに適用されているマイクロソフト製品のパッチの適用を調査する手法を示す．レジストリ内には適用されているパッチの情報が保存されている．提案システムでは

[3]提案システムでは SHA-1 を用いてハッシュ値を計算している

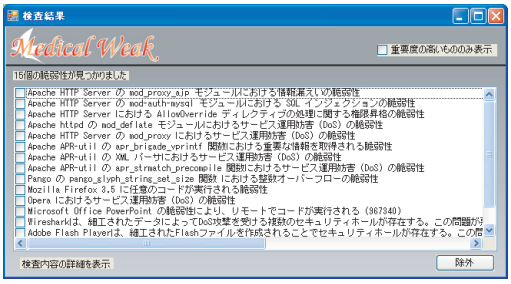

図 3: 検査結果の表示

レジストリから KB 番号を取得し検査に用いる．例として 2009 年 8 月 12 日に公開されたセキュリティ情報『MS09-038：Windows Media ファイル処理における脆弱性により、リモートでコードが実行される』[6] を見てみる．このセキュリティ情報の KB 番号は 971557 である．このパッチを適用している場合，レジストリキー

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Updates\Windows XP\SP4\KB971557
(Window XP SP3 の場合)
```

が存在し，この情報を取得することでパッチの適用の有無を検査できる．

3.5 バージョンの比較

3.4 で述べた手法で取得したソフトウェアのバージョンと検査用データベースに記載されている脆弱性の存在するバージョンを比較することで，バージョンアップ型に関しては脆弱性検査を行うことができる．次に，マイクロソフト製品に関しては **3.2** で述べたように，置き換え可能なパッチが存在する．置き換えられたパッチも含めて，KB 番号がレジストリ内に存在するかをもって，マイクロソフト製品に関しても脆弱性検査を行うことができる．もしここで，脆弱性の存在するバージョンを使用していた際は，ユーザに対してその脆弱性の危険度や詳細を明記した警告を促す．システムの画面の一部を図 3 に示す．

4 最新のニュースを利用した脆弱性ニュースリーダ

2.1 でも述べたように，近年被害が拡大している攻撃としてゼロデイ攻撃があげられる．脆

弱性データベースは脆弱性情報を収集し分かりやすくまとめるデータベースである．よって，脆弱性情報が報道されてすぐに脆弱性情報がアップされるとは限らないため，脆弱性データベースの確認だけではゼロデイ攻撃への対策には不十分である．よって，ユーザがゼロデイ攻撃を防ぐには，こまめにコンピュータセキュリティのニュースを見て，自身のコンピュータと関わりのあるニュースがないか確認を行い適切な対処を施す必要がある．しかし，膨大な情報から自身のコンピュータと関わりのある情報のみを取捨選択するのは困難であり，また手間もかかる．本稿ではゼロデイ攻撃への対応として，クライアントに関わりのある脆弱性ニュースを自動取得するシステムを提案する．

提案システムでは IT Media[7]，Internet Watch[8] の二つのサイトから，最新のニュースを取得する．この二つのサイトを用いるのは，多くのコンピュータ関連のニュースを報道しており，かつ脆弱性に関わるニュースも多数配信しているためである．

提案システムを実装するためには，このニュースの中身を調査し脆弱性に関わるニュースかを自動で検知する必要がある．また，どのソフトウェアに関わるニュースかを調査し，データベースに所持しておく必要がある．IT Media では各ニュースごとに，そのニュースの関連キーワードがまとめられている．よって，『脆弱性』というキーワードが関連キーワードに存在するかをもって判断できる．ソフトウェア名も同様にキーワードに含まれているので，キーワードにシステムで対応するソフトウェアが記載されているかで判断する．一方，Internnet Watch ではキーワードの類は存在しないため，ニュースのタイトルに『脆弱性』というキーワードが存在するかで判断する．脆弱性のニュースと判断されたものは本文を調査する．どのソフトウェアに関わるニュースなのかは，提案システムで対応するソフトウェア名が本文に記載されているかで判断する．

クライアントではインストールされているソフトウェアを検査し，上記で述べたデータベースと比較する．こうして，自動でクライアント

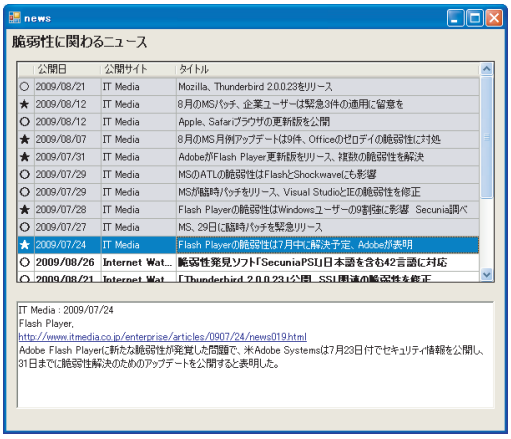

図 4: 最新ニュースの表示

のインストールしているソフトウェアに関するニュースのみを選択し表示できる．実際にシステムを用いてニュースを表示したものを図 4 に示す．また，ユーザがすぐに新しいニュースを確認できるよう，ニュースが新しく報道されると最新のニュースがポップアップされる．

5 評価

提案システムの有用性を示すため実際に脆弱性検知が可能か評価を行う．本稿では表 1 に記載されているソフトウェアを評価の対象とし，これらのソフトウェアを評価ソフトと定義する．評価ソフトは一般的なユーザの環境を再現する形をとり，原則同じ分類に属するソフトウェアを評価対象としない．また，Internet Explorer や Windows Media Player など，Windows に添付しているソフトウェアは Windows XP に含むこととする．

次に評価ソフトのバージョンに関して示す．本稿では 2009 年 6 月 1 日時点の最新バージョンと同年 7 月 15 日時点の最新バージョンの，二つのバージョンを 2009 年 9 月 2 日の検査用データベースをもって検査する．過去のバージョンで脆弱性検査を行うのは，最新バージョンでの脆弱性検査ではソフトウェアに脆弱性が存在せず，評価を行うことができないためである．本稿では評価ソフトのバージョンを評価バージョンと定義する．

最後に実際の評価手法に関して示す．提案システムが評価ソフトをインストールした環境の脆弱性を検知できるかで判断する．評価ソフト

表 1: 提案システムの評価

	2009 年 6 月 1 日の最新バージョン			2009 年 7 月 15 日の最新バージョン		
評価ソフト	評価バージョン	脆弱性	検知結果	評価バージョン	脆弱性	検知結果
Adobe Flash Player	10.0.22.87	有	○	10.0.22.87	有	○
Adobe Reader	9.1.1	有	○	9.1.2	有	○
Google デスクトップ	5.8.809.23506	無	○	5.8.809.23506	無	○
iTunes	8.1.1	有	○	8.2.0	無	○
JRE	6 Update 13	有	○	6 Update 13	有	○
Lhaplus	1.57	無	○	1.57	無	○
Office 2007 Professional	SP2	有	○	SP2	無	○
Mozilla Firefox	3.0.10	有	○	3.5	有	○
Mozilla Thunderbird	2.0.0.21	有	○	2.0.0.22	有	×
Quick Time Player	7.6.0	有	○	7.6.2	無	○
Windows Live Messenger	14.0.8064.206	無	○	14.0.8064.206	無	○
Windows XP	SP3	有	○	SP3	有	○

の評価バージョンに本来脆弱性が存在するかに関しては最新のニュース等を確認して判断し，表の『脆弱性』の欄に示す．また,『検知結果』の欄には提案システムで正しく検知できれば○，できなければ×を記す．

表 1 から分かるように，2009 年 6 月 1 日時点での最新バージョンでは，脆弱性が存在する場合はその脆弱性を検知できることが分かった．一方，2009 年 7 月 15 日時点での最新バージョンでは，Mozilla Thunderbird に関して脆弱性を検知できなかった．これは脆弱性自体はニュースやベンダの公式サイトで報道されているが，JVN iPedia やスキャンネットセキュリティでは脆弱性が公開されていないためである．また，**4** で提案したニュースリーダシステムを用いることで，Mozilla Thunderbird に関するニュースを読むことができた．

6 むすび

脆弱性対策はコンピュータセキュリティ保持において重要な役割を担うが，ユーザの脆弱性に対する意識は非常に低いと言える．本稿では既存脆弱性データベースを利用した脆弱性検査システムを提案，評価した．提案システムを用いて脆弱性対策を行う過程を自動化したことにより，脆弱性情報を見落とす問題や，個々の情報を確認する時間の削減につながる．また，脆弱性の詳細情報や重要度を明記することで，ユーザの脆弱性に対する関心を高める効果が期待できる．

参考文献

[1] IT Media “Adobe Reader に未解決の脆弱性、アップデートは準備中,” available at http://www.itmedia.co.jp/enterprise/articles/0904/29/news003.html

[2] Secunia PSI, available at http://secunia.com/vulnerability_scanning/personal/

[3] JVN iPedia, available at http://jvndb.jvn.jp/index.html

[4] Scan NetSecurity, available at https://www.netsecurity.ne.jp/

[5] Microsoft セキュリティ情報検索, available at http://www.microsoft.com/japan/technet/security/current.aspx

[6] マイクロソフト セキュリティ情報 MS09-038 - 緊急 : Windows Media ファイル処理における脆弱性により、リモートでコードが実行される (971557), available at http://www.microsoft.com/japan/technet/security/Bulletin/MS09-038.mspx

[7] IT Media, available at http://www.itmedia.co.jp/

[8] INTERNET Watch, available at http://internet.watch.impress.co.jp/