

## 「一太郎シリーズ」におけるセキュリティ上の弱点(脆弱性)の注意喚起

IPA(独立行政法人情報処理推進機構、理事長:西垣 浩司)は、「一太郎シリーズ」におけるセキュリティ上の弱点(脆弱性)に関する注意喚起を、2009年4月7日に公表しました。

( URL: [http://www.ipa.go.jp/security/vuln/documents/2009/200904\\_ichitaro.html](http://www.ipa.go.jp/security/vuln/documents/2009/200904_ichitaro.html) )

これは、「一太郎シリーズ」の利用者が、ウェブブラウザやメール経由で細工された文書ファイルを開覧した場合に、任意のコードが実行されてしまうというものです。

悪用されると、コンピュータ上でユーザの意図しないプログラムの実行や、ファイルの削除、ウイルスやボットなどの悪意あるツールがインストールされるなど、コンピュータが悪意あるユーザによって制御される可能性があります。

対策方法は「ベンダが提供する対策済みバージョンに更新する」ことです。

### 1. 概要

株式会社ジャストシステムが提供する「一太郎シリーズ」は、日本語ワープロソフトです。「一太郎シリーズ」は、文章を作成するソフトウェアの一つとして、日本国内で広く利用されています。

「一太郎シリーズ」には、文書ファイルを読みこむ際に、バッファオーバーフローというセキュリティ上の弱点(脆弱性)があります。この弱点が悪用されると、「一太郎シリーズ」がインストールされたコンピュータ上で、任意のコードが実行されてしまう可能性があります。

脆弱性による影響が大きいことと、「一太郎シリーズ」の普及状況により、この影響を受ける利用者が国内に広く存在すると判断し、注意喚起を行いました。

詳細は、次の URL を参照して下さい。

<http://www.justsystems.com/jp/info/js09002.html>

最新情報は、次の URL を参照下さい。

<http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-000018.html>

本脆弱性情報は、情報セキュリティ早期警戒パートナーシップに基づき、2009年2月12日に以下の報告者からIPAが届出を受け、JPCERT/CC(有限責任中間法人 JPCERT コーディネーションセンター)が製品開発者と調整を行ない、2009年4月7日に公表したものです。

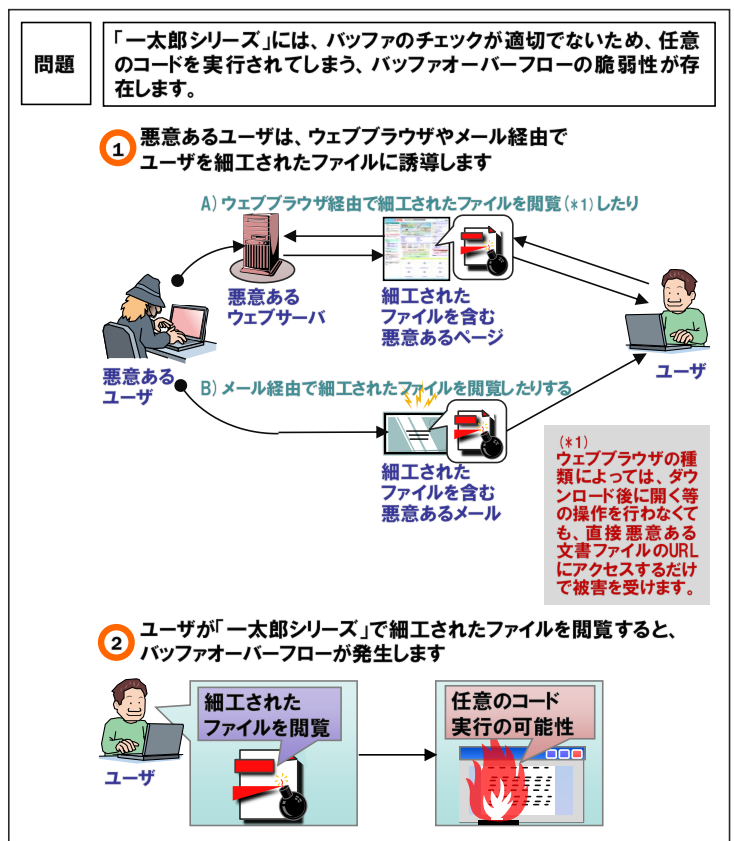
報告者: (株)フォティンフォティ技術研究所  
鶴飼 裕司 氏

### 2. 脆弱性による影響

「一太郎シリーズ」の利用者が、ウェブブラウザやメール経由で細工された文書ファイルを開覧した場合に、システムが破壊されたり、ウイルスやボットに感染させられたりする可能性があります。

**特に、ウェブブラウザでの閲覧の場合、ウェブブラウザの種類や設定によっては、ダウンロード後に開く等の操作を行わなくても、悪意ある URL にアクセスするだけで被害を受けてしまう可能性があります。**

結果として、コンピュータが悪意あるユーザによって制御される可能性があります。



### 3. 対策方法

対策方法は「ベンダが提供する対策済みバージョンに更新する」ことです。

### 4. 本脆弱性の深刻度<sup>1</sup>

#### (1) 評価結果

本脆弱性の深刻度 (CVSS <sup>2</sup> 基本値の範囲)	<input type="checkbox"/> レベルⅠ(注意) (0.0～3.9)	<input checked="" type="checkbox"/> レベルⅡ(警告) (4.0～6.9)	<input type="checkbox"/> レベルⅢ(危険) (7.0～10.0)
本脆弱性の CVSS 基本値		6.8	

#### (2) CVSS 基本値の評価内容

AV: 攻撃元区分	<input type="checkbox"/> ローカル	<input type="checkbox"/> 隣接	<input checked="" type="checkbox"/> ネットワーク
AC: 攻撃条件の複雑さ	<input type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input type="checkbox"/> 低
Au: 攻撃前の認証要否	<input type="checkbox"/> 複数	<input type="checkbox"/> 単一	<input checked="" type="checkbox"/> 不要
C: 機密性への影響	<input type="checkbox"/> なし	<input checked="" type="checkbox"/> 部分的	<input type="checkbox"/> 全面的
I: 完全性への影響	<input type="checkbox"/> なし	<input checked="" type="checkbox"/> 部分的	<input type="checkbox"/> 全面的
A: 可用性への影響	<input type="checkbox"/> なし	<input checked="" type="checkbox"/> 部分的	<input type="checkbox"/> 全面的

■ : 選択した評価結果

AV: Access Vector, AC: Access Complexity, Au: Authentication, C: Confidentiality Impact, I: Integrity Impact, A: Availability Impact

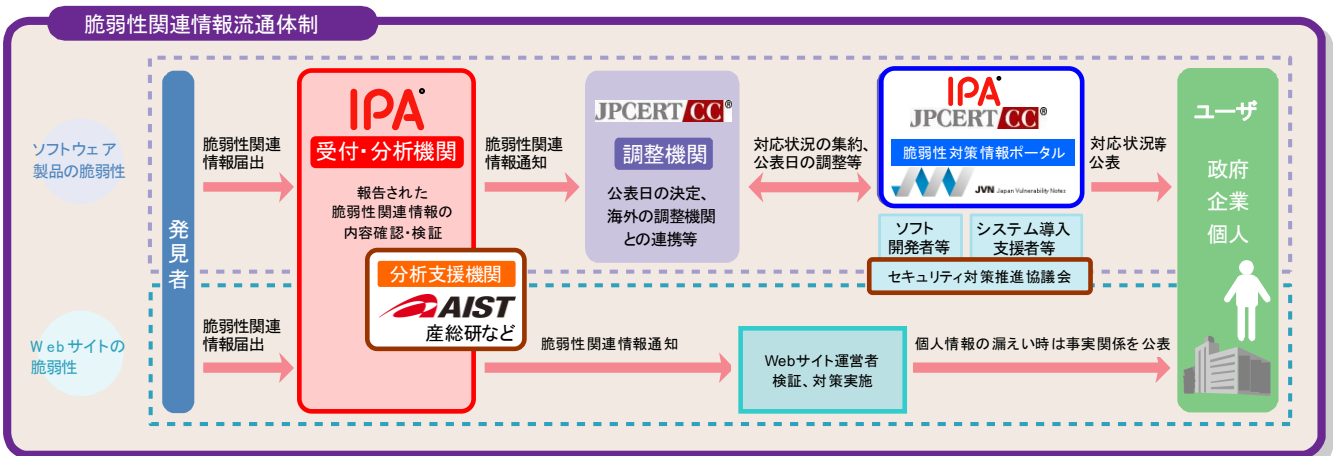
### 5. 本脆弱性の CWE<sup>3</sup>分類

本脆弱性の CWE 分類は、「バッファエラー (CWE-119)」です。

### 6. 参考情報

#### (1) 「情報セキュリティ早期警戒パートナーシップ」について

ソフトウェア製品及びウェブサイトの脆弱性対策を促進し、コンピュータウイルスやコンピュータ不正アクセス等によって、不特定多数のコンピュータ(パソコン)に対して引き起こされる被害を予防するため、経済産業省の告示に基づき、官民の連携体制「情報セキュリティ早期警戒パートナーシップ」を整備し運用しています。



※JPCERT/CC: 有限責任中間法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

<sup>1</sup> 脆弱性の深刻度評価の新バージョン CVSS v2 への移行について。 <http://www.ipa.go.jp/security/vuln/SeverityLevel2.html>

<sup>2</sup> Common Vulnerability Scoring System. 共通脆弱性評価システム。 <http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html>

<sup>3</sup> Common Weakness Enumeration. 共通脆弱性タイプ一覧。 <http://www.ipa.go.jp/security/vuln/CWE.html>

■ 本件に関するお問い合わせ先  
 IPA 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](mailto:vuln-inq@ipa.go.jp)  
 ■ 報道関係からのお問い合わせ先  
 IPA 戦略企画部広報グループ 横山/大海  
 Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: [pr-inq@ipa.go.jp](mailto:pr-inq@ipa.go.jp)