

「文書閲覧ソフトウェアの古い脆弱性を狙った標的型攻撃」についての調査結果の公開
～「2009年度 脆弱性を利用した新たなる脅威の分析による調査 最終報告書」～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、「情報窃取を目的として特定の組織に送られる不審なメール（標的型攻撃）」の実態把握と対策促進のための調査レポートとして「脆弱性を狙った脅威の分析と対策について Vol.4」、「2009年度 脆弱性を利用した新たなる脅威の分析による調査 最終報告書」を2010年7月29日（木）から、IPAのウェブサイトで公開しました。
URL：<http://www.ipa.go.jp/security/vuln/report/newthreat201007.html>

近年、特定の組織を対象として、メールの送付元を知人や取引先企業等に詐称してウイルスを送付する「標的型攻撃」が発生しています。IPA セキュリティセンターでは、それら攻撃への対策促進のため、「脆弱性を狙った脅威の分析と対策について」を定期的に公開しています。今回、2010年3月に発生した標的型攻撃を解析し、その結果概要を「脆弱性を狙った脅威の分析と対策について Vol.4」として公開しました。また、2009年12月に発生した標的型攻撃の解析結果概要（Vol.3¹）の内容と合わせ、2009年度版最終報告書を作成し、公開しました。

Vol.4で解析した「標的型攻撃メール」の特徴は以下の通りです。

- 受信者に心当たりのない個人名
- フリーメールのアドレス
- 受信者が業務用で加入しているメーリングリスト
- 当時話題になっていたニュースを連想させる件名
- 受信者に添付ファイルを開くよう仕向ける文章
- 実在の団体名
- フリーメールのアドレス
- 本文と関連がありそうな名前のDOCファイル。実態はマルウェア²。



図1. 標的型攻撃メール(メーラー：Outlook2000)

標的型攻撃を解析した結果、Vol.4で紹介している標的型攻撃は、Microsoft Wordの脆弱性を利用しており、この脆弱性は攻撃から4年前に発見されたものであることが分かりました。また、この脆弱性とVol.3の標的型攻撃において利用された脆弱性の比較を行いました。その結果を表1に示します。

¹ 「脆弱性を狙った脅威の分析と対策について Vol.3」

<http://www.ipa.go.jp/security/vuln/report/newthreat201006.html>

² Malicious Software：悪意あるプログラム。ユーザの望まない悪さをするプログラムのこと。

表 1.利用された脆弱性の比較

	Vol.3(2010年6月公開)	Vol.4(2010年7月公開)
利用された脆弱性	CVE-2009-4324 (JVND-2009-002451)	CVE-2006-2492 (JVND-2006-000296)
脆弱性を利用されたソフトウェア	Adobe Reader	Microsoft Word
脆弱性の発見日	2009/12/16	2006/5/19
パッチの発行日	2010/1/12	2006/6/14
標的型攻撃メールの受信日	2009/12/25	2010/3/18

Vol.3 の標的型攻撃は、攻撃時点ではまだパッチが発行されていないゼロデイ攻撃でした。これに対して、Vol.4 の標的型攻撃では約 4 年前に発見された脆弱性が利用されており、この点で 2 件の標的型攻撃は対照的です。定期的なバージョンアップを実施していないユーザが一定数存在することは、攻撃者を含めて広く知られており、そのため、発見から 4 年が経過した古い脆弱性でも依然として攻撃に利用されています。パソコンの利用者は、基本的なセキュリティ対策であるバージョンアップを確実に実施する必要があります。また、ゼロデイ攻撃にも対応するため、Vol.3 で紹介したような更新プログラムが存在しない脆弱性への対策も併用することが望ましいと言えます。

上述のとおり、攻撃には古い脆弱性が利用されることもありますので、定期的なバージョンアップを行い、現在までに発行されたパッチは全て適用してマルウェアへの感染を防ぐことが必要です。Microsoft 製品のバージョンチェックには Microsoft Update³を使用してください。Adobe Reader 等 9 つの製品のバージョンチェックには、MyJVN バージョンチェッカ⁴を使用することが可能です。

最終報告書では、Vol.3 と Vol.4 の標的型攻撃について、それぞれに用いられたマルウェアの動作やソーシャルエンジニアリング⁵手法等の詳細を記述し、2009 年度に発生した標的型攻撃への対策をまとめています。

標的型攻撃は特定の組織を標的にするため情報が表面化し難く、被害に気付きにくい攻撃です。IPA では、本調査報告書の事例のような「不審メール」の情報収集、および予防・対処方法等の情報提供を目的とした「不審メール 110 番」⁶相談窓口を設置しています。

IPA では今後も、標的型攻撃について調査・分析を実施し、標的型攻撃に対する知識の普及、対策の促進のため、「脆弱性を狙った新たな脅威の分析と対策について」として定期的に対策を発表していきます。

「脆弱性を狙った脅威の分析と対策について Vol.4」(全 8 ページ)は、次の URL よりダウンロードの上、ご参照ください。

URL : <http://www.ipa.go.jp/security/vuln/report/newthreat201007.html>

「2009 年度版最終報告書」(全 54 ページ)は、次の URL よりダウンロードの上、ご参照下さい。

URL : <http://www.ipa.go.jp/security/vuln/report/newthreatreport2009.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 小林 / 中野 / 長谷川
 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
 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

³ Microsoft Update
<http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ja>

⁴ MyJVN バージョンチェッカ
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

⁵ 話術や盗み聞き・盗み見等を利用し、人間の心理・行動の隙を突くことで情報を不正に取得する手段の総称。

⁶ 不審メール 110 番
<http://www.ipa.go.jp/security/virus/fushin110.html>