# Adobe Reader/Acrobat のゼロデイ脆弱性（CVE-2009-4324）

ＮＴＴ コミュニケーションズ株式会社
ＩＴ マネジメントサービス事業部
セキュリティオペレーションセンタ

2009 年 12 月 16 日

Ver. 1.0

# 1. 調査概要

2009 年 12 月 15 日に Adobe Reader / Acrobat の newplayer() 関数の脆弱性を悪用したゼロデイの攻撃コードが公開された。この脆弱性を突いて攻撃を行うとコンピュータを乗っ取る事が可能であり、12 月 16 日現在セキュリティアップデートが提供されておらず非常に危険であるため注意を喚起する。

本レポートでは、この脆弱性について検証を行った結果と考察を報告する。

# 2. 脆弱性の概要

2009 年 12 月 15 日に発見された Adobe Reader の脆弱性（CVE-2009-4324）では、受動的攻撃により悪意あるコードを含む PDF ファイルをクライアントに実行させる事により、実行したユーザの権限でコンピュータを乗っ取る事が可能となる。攻撃のイメージは以下の図の通りとなる。

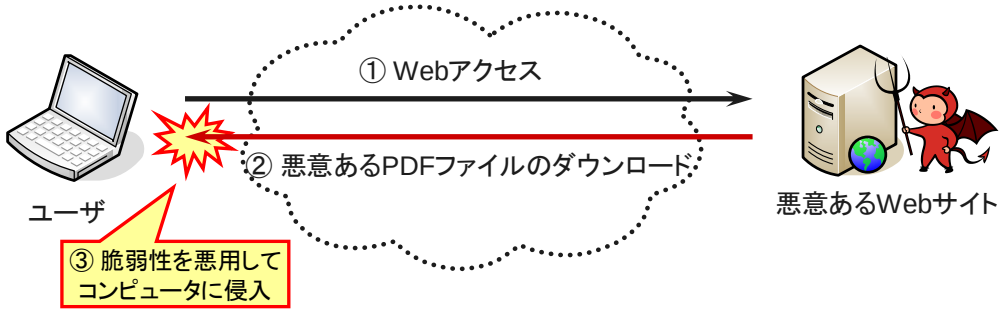



図 1　攻撃のイメージ

この脆弱性について、影響を受ける製品は以下の通りとなる。

- Adobe Reader 8
- Adobe Reader 9
- Adobe Acrobat Standard 8
- Adobe Acrobat Standard 9
- Adobe Acrobat Professional 8
- Adobe Acrobat Professional 9

# 3. 検証環境

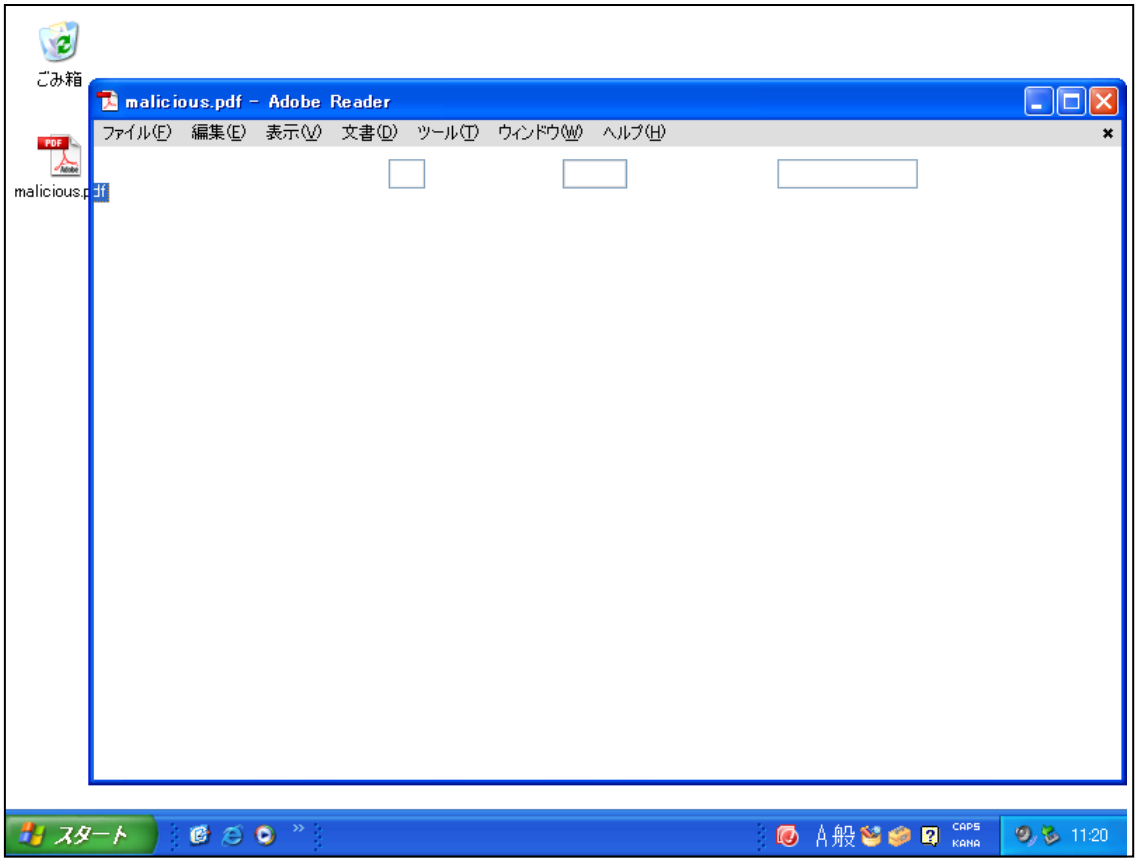
本レポートで使用した検証環境は以下の通りである。

- Windows XP SP3
- Adobe Acrobat 9.2.0

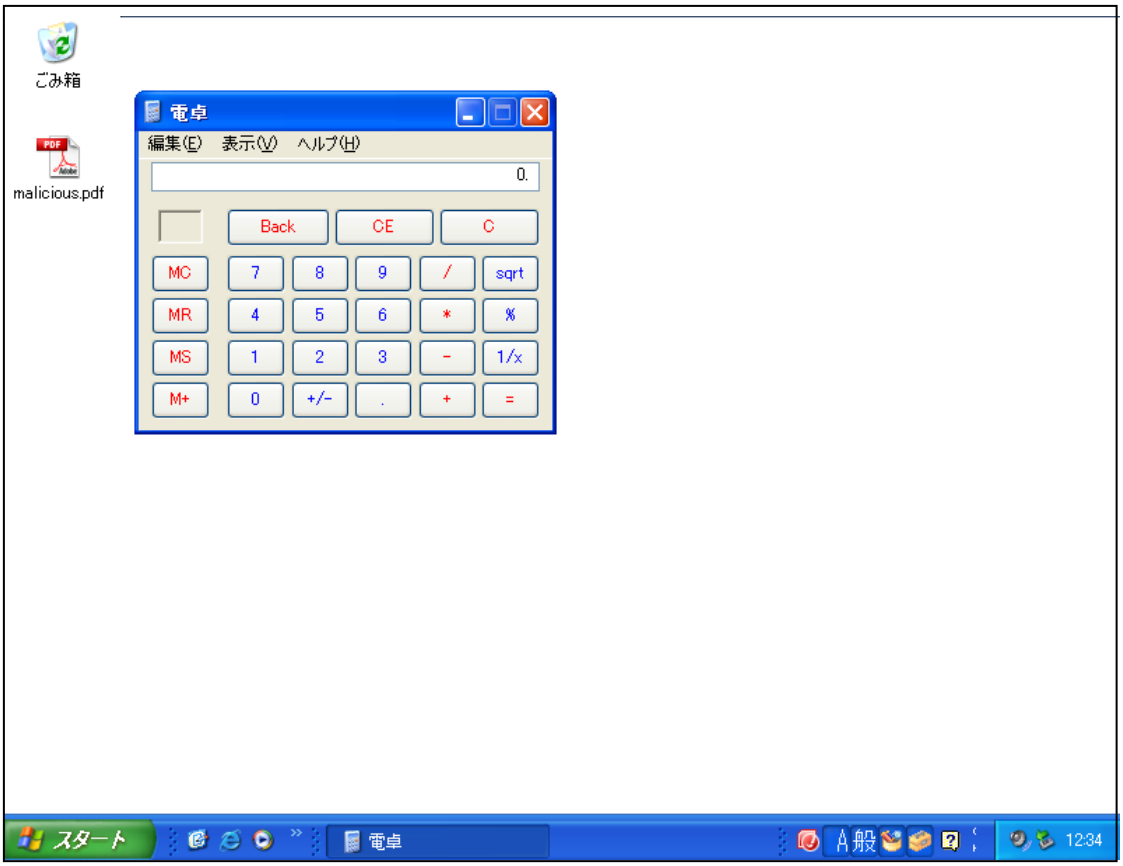
# 4. 攻撃コードの検証

攻撃コードの検証結果は以下の通りである。

1. 悪意ある PDF ファイル（malicious.pdf）を実行すると、Adobe Reader が起動します。



2. Adobe Reader が終了した後、PDF ファイルに埋め込まれた calc コマンドが実行され、電卓プログラムが起動します。



# 5. 本脆弱性の暫定対策

本脆弱性はゼロデイの脆弱性であり、12 月 16 日現在ではセキュリティアップデートは提供されておらず、非常に危険である。不用意に Adobe Reader / Acrobat を利用する事は避けるべきであるが、必要となった場合は以下の対策を行う事で暫定対策が可能となる。

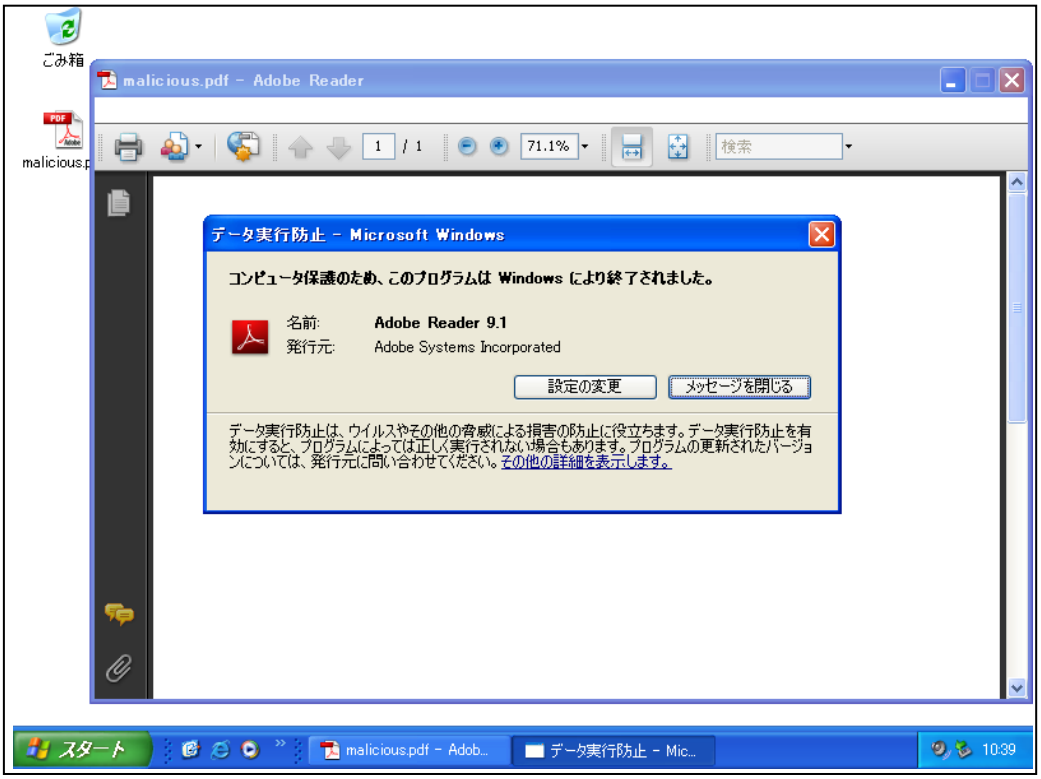
## 5.1. Adobe Reader / Acrobat の JavaScript を無効化する

Adobe Reader / Acrobat の JavaScript を無効化する事で対策が可能となる。設定方法については、以下の通りである。

1. Adobe Reader / Acrobat を起動する。
2. メニューバーから「編集」→「環境設定」をクリックする。
3. 「分類」の中で「JavaScript」を選択する。
4. 「Acrobat JavaScript を使用」のチェックを外す。
5. 「OK」ボタンを押す。

## 5.2. DEP を有効にする

Windows での DEP（データ実行防止）を有効にすると、以下のようにコードが実行される前にプログラムが強制終了する。



## 5.3. ウイルス対策ソフトを利用する

本脆弱性を狙った攻撃を検知するウイルス対策ソフトを利用する事で防御する。2009 年 12 月 16 日 17 時現在では以下のウイルス対策製品が対応している。


Virustotal は 疑わしいファイルを解析するサービスであり、ウイルス、ワーム、トロイの木馬およびアンチウイルスエンジンにより検出される全てのマルウェアを素早く簡単に検出します。詳細...

ファイル名 **malicious.pdf** 受理 **2009.12.16 08:38:23 (UTC)**
現在の状態: **完了**
結果: **5/41 (12.2%)**

定型書式　　結果を印刷

| アンチウイルス | バージョン | 更新日 | 結果 |
|---|---|---|---|
| a-squared | 4.5.0.43 | 2009.12.16 | - |
| AhnLab-V3 | 5.0.0.2 | 2009.12.16 | - |
| AntiVir | 7.9.1.108 | 2009.12.15 | - |
| Antiy-AVL | 2.0.3.7 | 2009.12.16 | - |
| Authentium | 5.2.0.5 | 2009.12.02 | - |
| Avast | 4.8.1351.0 | 2009.12.15 | - |
| AVG | 8.5.0.427 | 2009.12.15 | - |
| BitDefender | 7.2 | 2009.12.16 | Exploit.PDF-JS.Gen |
| CAT-QuickHeal | 10.00 | 2009.12.16 | - |
| ClamAV | 0.94.1 | 2009.12.16 | - |
| Comodo | 3260 | 2009.12.16 | - |
| DrWeb | 5.0.0.12182 | 2009.12.16 | - |
| eSafe | 7.0.17.0 | 2009.12.15 | - |
| eTrust-Vet | 35.1.7178 | 2009.12.16 | - |
| F-Prot | 4.5.1.85 | 2009.12.15 | - |
| F-Secure | 9.0.15370.0 | 2009.12.16 | Exploit.PDF-JS.Gen |
| Fortinet | 4.0.14.0 | 2009.12.16 | - |
| GData | 19 | 2009.12.16 | Exploit.PDF-JS.Gen |
| Ikarus | T3.1.1.77.0 | 2009.12.16 | - |
| Jiangmin | 13.0.900 | 2009.12.16 | - |
| K7AntiVirus | 7.10.920 | 2009.12.14 | - |
| Kaspersky | 7.0.0.125 | 2009.12.16 | - |
| McAfee | 5833 | 2009.12.15 | - |
| McAfee+Artemis | 5833 | 2009.12.15 | - |
| McAfee-GW-Edition | 6.8.5 | 2009.12.15 | - |
| Microsoft | 1.5302 | 2009.12.16 | - |
| NOD32 | 4691 | 2009.12.15 | - |
| Norman | 6.04.03 | 2009.12.15 | - |
| nProtect | 2009.1.8.0 | 2009.12.16 | - |
| Panda | 10.0.2.2 | 2009.12.15 | - |
| PCTools | 7.0.3.5 | 2009.12.16 | - |
| Prevx | 3.0 | 2009.12.16 | - |
| Rising | 22.26.02.04 | 2009.12.16 | - |
| Sophos | 4.48.0 | 2009.12.16 | Mal/PDFEx-D |
| Sunbelt | 3.2.1858.2 | 2009.12.16 | Exploit.PDF-JS.Gen (v) |
| Symantec | 1.4.4.12 | 2009.12.16 | - |
| TheHacker | 6.5.0.2.094 | 2009.12.15 | - |
| TrendMicro | 9.100.0.1001 | 2009.12.16 | - |
| VBA32 | 3.12.12.0 | 2009.12.16 | - |
| ViRobot | 2009.12.16.2091 | 2009.12.16 | - |
| VirusBuster | 5.0.21.0 | 2009.12.14 | - |

## 5.4. IPS、UTM を利用する

IPS や UTM などのセキュリティ機器を導入している場合、今回の脆弱性に対する攻撃を検知するシグネチャを有効にする。

・Snort
Sourcefire VRT Rules Update Date: 2009-12-15
http://www.snort.org/vrt/docs/ruleset_changelogs/2_8/changes-2009-12-15.html
シグネチャ名：Adobe Reader util.printd memory corruption attempt
Adobe Reader compressed util.printd memory corruption attempt

・Fortigate
FortiGuard Advisory (FGA-2009-47)
http://www.fortiguard.com/advisory/FGA-2009-47.html
シグネチャ名：Adobe.Reader.Javascript.0day

・Proventia
IBM Internet Security Systems Ahead of the threat
http://www.iss.net/threats/358.html
シグネチャ名：Adobe Acrobat and Acrobat Reader Remote Code Execution

# 6. まとめ

本脆弱性はゼロデイの脆弱性であり、比較的容易に攻撃コードを作成できることから非常に危険なものであるが、暫定対策をする事で影響を最小限に抑える事が可能なため、速やかに対策を行うべきである。また、Adobe Systems 社からのセキュリティアップデートに関する情報をチェックして定期的にアップデートを適用する事が望ましい。

## 7. 検証作業者

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター
　羽田　大樹

## 8. 参考

1. [Adobe] New Adobe Reader and Acrobat Vulnerability
http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html

2. [Adobe] Security Advisory for Adobe Reader and Acrobat
http://www.adobe.com/support/security/advisories/apsa09-07.html

3. [CVE] CVE-2009-4324
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324

4. [BID] Adobe Reader and Acrobat 'newplayer()' JavaScript Method Remote Code Execution Vulnerability
http://www.securityfocus.com/bid/37331

## 9. 履歴

- 2009 年 12 月 16 日 ：ver1.0 公開

## 10.　最新版の公開 URL

http://www.ntt.com/icto/security/data/soc.html#security_report

# 11. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター

e-mail: scan@ntt.com

以 上