報道発表

平成 24 年 4 月 25 日
内閣官房情報セキュリティセンター（NISC）

PDF ファイルの改ざんによるサイバー攻撃への対策について

1　背景

広く文書の交換に利用されている PDF (※) 形式の文書（以下「PDF ファイル」と呼ぶ。）にコンピュータウイルスが仕込まれ、ファイルを閲覧した際に端末がウイルスに感染してしまう事例が内外で報告されています。このコンピュータウイルスは、PDF ファイルの閲覧や編集を行うソフトウェア（以下「PDF ソフト」と呼ぶ。）の脆弱性を悪用したものです。この被害を防ぐために、PDF ソフトを更新して常に最新の状態に保つことや、PDF ソフトのセキュリティ設定を適切に設定したりすることが重要となっています。

2　政府機関における取組

2.1　PDF ソフトの更新

平成 24 年 4 月 11 日に、米国アドビシステムズ社より、同社が提供する PDF ソフト Adobe Reader 及び Adobe Acrobat の既知の脆弱性（JVNTA12-101B）に対処するための修正版ソフトウェアが公開されました。これを受け、同日付で、NISC から各府省庁に以下の通り注意喚起を行いました。

○　Adobe Reader 及び Adobe Acrobat における修正版ソフトウェアの公開に関する情報の提供
○　各府省庁において、システムに関する影響を検討の上、速やかに修正版ソフトウェアをインストールする指示

2.2　電子署名の確認

多くの政府機関においても、PDF ファイルを用いて、文書の交換や資料の公表が行われています。この公表されている真正な PDF ファイルを改ざんし、コンピュータウイルスを仕込んで、政府機関になりすまして不正な PDF ファイルがメールに添付されて送りつけられたり、ウェブサイトに掲載されたりして出回ることが懸念されます。このため、PDF ファイルに電子署名を付与して、改ざんが行われていないことを証明することが望ましいと考えます。政府機関においては、電子署名に政府認証基盤（GPKI）

を用いた証明書を利用していますが、これまで GPKI を用いた電子署名が真正なものであるか否かを確認するためには、利用者が個別に GPKI のサイトにアクセスし、GPKI 認証局の自己署名証明書を PDF ソフトにインストールするなどの事前設定の必要がありました。

この度、平成 24 年 4 月 21 日より、Adobe Reader 及び Adobe Acrobat において、GPKI 認証局の自己署名証明書の自動配信が開始されました。これにより、政府機関が GPKI を用いて電子署名を付与した PDF ファイルは、同ソフトウェアで閲覧すると、PDF ファイルの入手方法によらず、PDF ファイルの発行者が政府機関であること、及び改ざんされていないことが自動的に確認できるようになりました(†)。

3　PDF ファイル閲覧時の推奨事項

悪意のある PDF ファイルによる被害を防ぐため、PDF ファイルの閲覧を行う際には、以下の対策を実施されることを推奨します。

- ○　使用している PDF ソフトを常に最新の状態に保つこと。
- ○　PDF ファイルに電子署名が付与されている場合には、PDF ファイルの発行者が信用できるものであること及び改ざんが行われていないことを、PDF ソフトの表示により確認すること。
- ○　PDF ソフトを利用する端末にはセキュリティ関連ソフト（ウイルス対策ソフト）を導入すること。

4　今後の取組

NISC においては、引き続き、PDF ソフトのセキュリティ向上に係る取組等を推進し、情報セキュリティの向上に努めてまいります。

(※) PDF : ISO 32000-1 (Portable Document Format)として国際標準化されている電子文書フォーマット。

(†) Adobe Reader 及び Adobe Acrobat における証明書の自動更新確認は 30 日おきとなっているため、最長で平成 24 年 5 月 20 日（自動配信開始日の 30 日後）までは新たな自己署名証明書が自動的にインストールされない場合があります。（手動でこれを行うことも可能です。）

【本報道発表に関する問い合わせ先】
内閣官房情報セキュリティセンター
内閣参事官　木本裕司
電話 03-3581-3959（センター代表）