

【今月の呼びかけ】

「ファイル名に細工を施されたウイルスに注意！」
～見目でパソコン利用者をだます手口～

2011年9月、IPAにRLTrapというウイルスの大量の検出報告（約5万件）が寄せられました。このウイルスには、パソコン利用者がファイルの見在目（主に拡張子）を誤認し実行してしまうように、ファイル名に細工が施されています。このような手法は決して新しいものではなく、2006年頃には既に確認されていました。

ここでは、このような手法にだまされてウイルスに感染しないように、ファイル名偽装の手口を解説するとともに、ウイルス感染の被害を未然に防ぐための対策を紹介します。

(1) ファイル名偽装の手口

この手口は、Unicodeの制御文字を利用してファイル名の拡張子を偽装し、危険なファイルを安全な別の種類のファイルだと思わせます。Unicodeとは、世界中の言語を単一の文字コードで取り扱う目的で作られた規格のことです。制御文字とは、文字コードで定義される文字ですが画面には表示されず、プリンタや通信装置などを制御するために使われるものです。

ここで使われる制御文字はRLO（Right-to-Left Override）というものです。この制御文字は、ファイル名の文字の並びを「左→右」から、「右→左」に変更します。この機能は、日本語や英語に代表される、文字を左から右に読ませる言語とは逆に、右から左に読ませる言語（アラビア語など）を使用する際に用いられます。

RLOの使用例を簡単に説明します。ここに「ABCDEF.doc」という名前のファイルがあるとします。このファイル名の先頭の「A」の前にRLOを挿入します（RLO自体は目に見えません）。するとファイル名は拡張子も含めて文字の並びが右方向から左方向に変更され、ファイル名の見目が「cod.FEDCBA」に変わります（図1-1参照）。



図 1-1 : RLO の使用例の図

この機能を悪用することで、「exe」形式のファイルを「pdf」形式のファイルに偽装することが可能になります。

(2) 実際に使われたウイルスメール

IPAが確認したウイルスメールを紹介します。ウイルスはZIP形式で圧縮されて、図1-2のようなメールの添付ファイルとして送られていました。

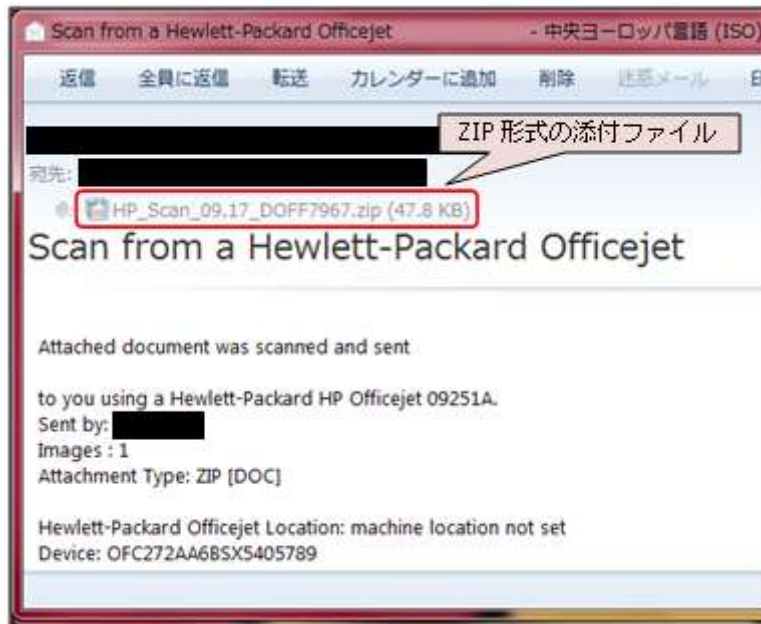


図 1-2 : 実際に使われたウイルスメールの本文

図 1-2 の添付ファイル(圧縮ファイル)を解凍すると、「HP_SCAN_FORM_N90952011__Collexe.pdf」というファイル名に偽装した「exe」形式のファイルが作成されます (図 1-3 参照)。

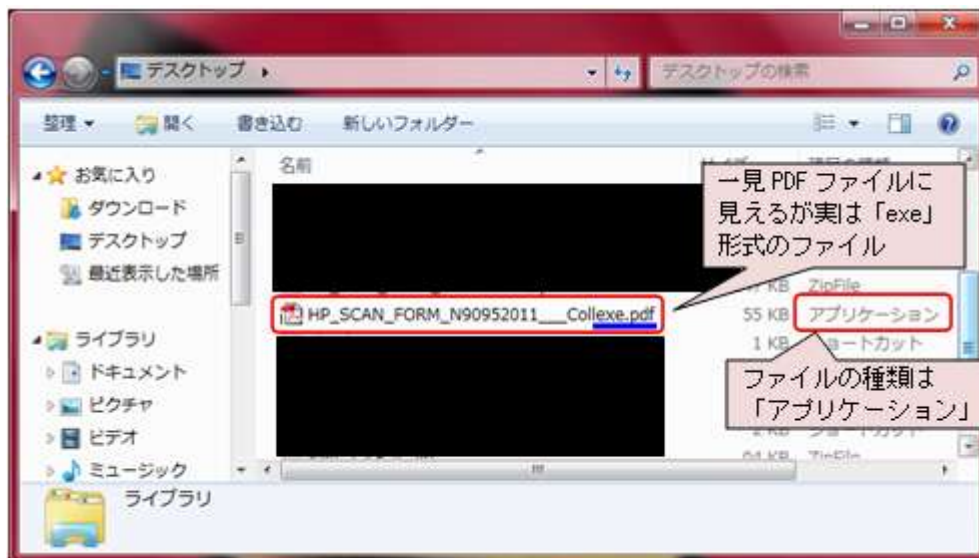


図 1-3 : ウイルスメールの添付ファイルの中のファイルの表示例

なお、圧縮・解凍ソフトによっては、中のファイルが意図したとおりに表示されない場合があります。図 1-4 は、その際の表示例です。

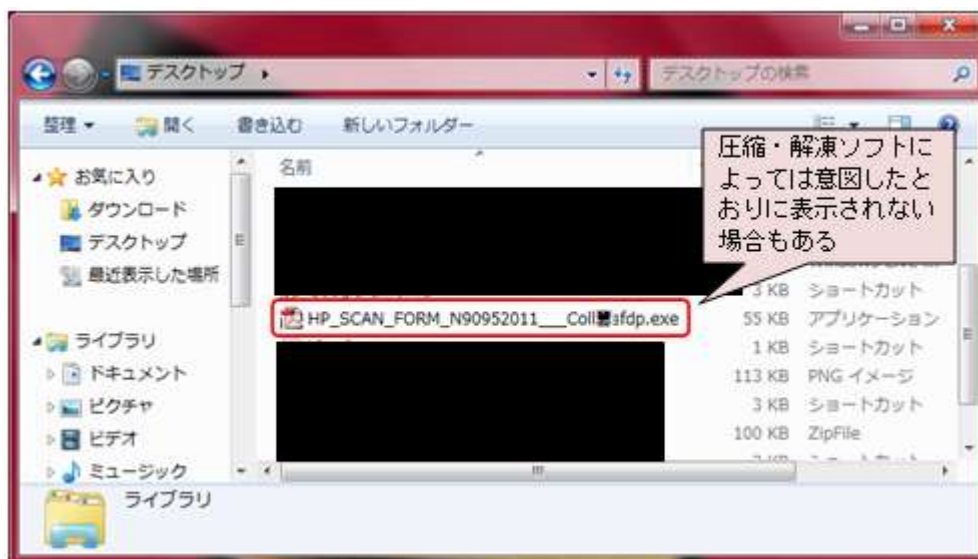


図 1-4：添付ファイルの中のファイルが意図したとおりに表示されなかった表示例

(3) RLTrap ウイルスの解析結果（ウイルスの動作概要）

IPA では RLTrap ウイルスの解析を行いました。解析の結果、このウイルスは Windows 7 環境でのみ動作し、感染すると以下の動作を行うことを確認しました。

- ・ロシアのあるウェブサイトと通信を試みます。ただし、解析を行った時点では既に当該サイトは存在しておらず、通信は行われませんでした。通信が行われた場合、別のウイルスをダウンロードして感染させる可能性があります。
- ・ウイルスは Windows の特定のフォルダに「csrss.exe」という名前で自身のコピーを作ります。
- ・ウイルスは一度実行すると、実行された自身のファイルを削除します。

(4) 対策

ウイルス感染の被害を未然に防ぐための対策としては、「ウイルス対策ソフトの活用」と「脆弱（ぜいじゃく）性対策」の二点が基本的な対策になりますので、必ず実施してください。

[i] ウイルス対策ソフトの活用

ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。ウイルス対策ソフトが導入済であればメール受信時や添付ファイル保存時、またはファイルを開く際にウイルスとして検出することができます。

[ii] 脆弱性対策

Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。一般的に利用者の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。

（ご参考）

MyJVN バージョンチェッカ（IPA）

<http://jvndb.jvn.jp/apis/myjvn/vccheck.html>

[iii] RLO を悪用するウイルスへの対策

上述した基本的な対策に加え、以下に示す対策を行うことで、今回のように Unicode 制御文字を悪用したウイルスの感染を未然に防ぐことができます。その手順を Windows 7 を例に解説します。

(手順 1)

スタートメニューの下部に「secpol.msc」と入力し、Enter キーを押す（図 1-5 参照）。なお、Windows XP の場合は、スタートメニューから「ファイル名を指定して実行 (R)」をクリックし、表示された画面の名前 (O) の欄に「secpol.msc」と入力し、Enter キーを押します。Windows Vista の場合は、Windows 7 の場合とほぼ同様です。

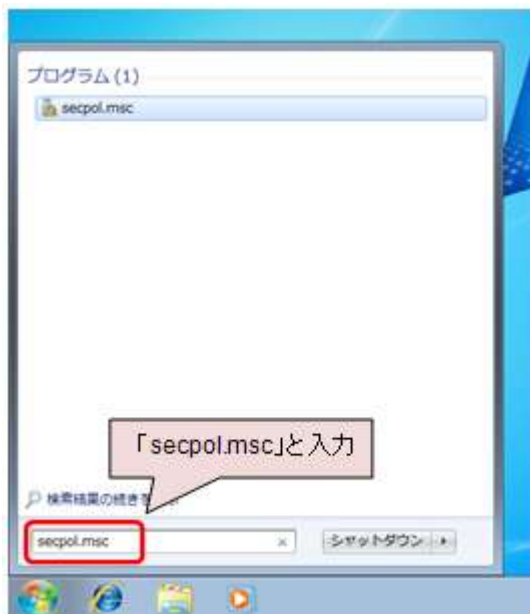


図 1-5 : RLO 対策手順 1

(手順 2)

ローカルセキュリティポリシーの画面が出たら、左部の「ソフトウェアの制限のポリシー」を右クリックし、表示されたメニューから「新しいソフトウェアの制限のポリシー (S)」をクリック（図 1-6 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

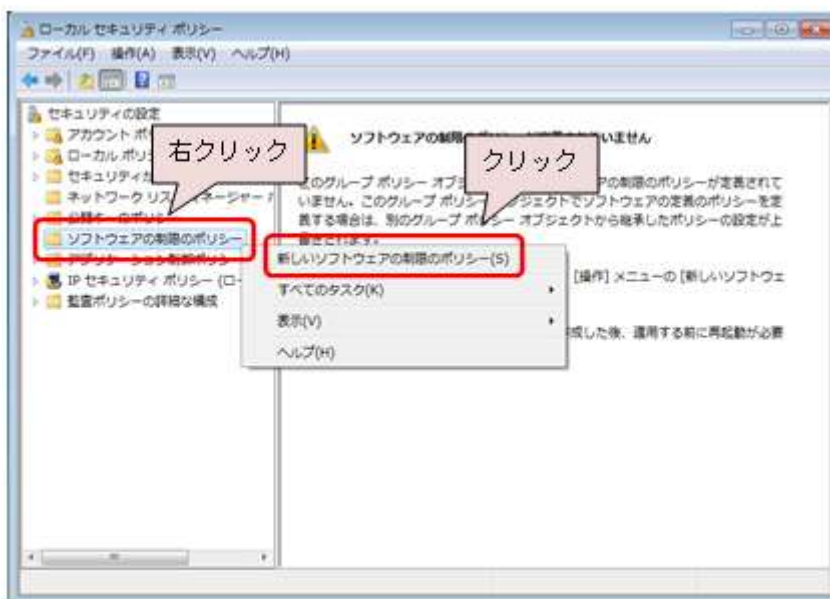


図 1-6 : RLO 対策手順 2

(手順 3)

ローカルセキュリティポリシーの画面の右部の「追加の規則」を右クリックし、表示されたメニューから「新しいパスの規則 (P) ...」をクリック（図 1-7 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

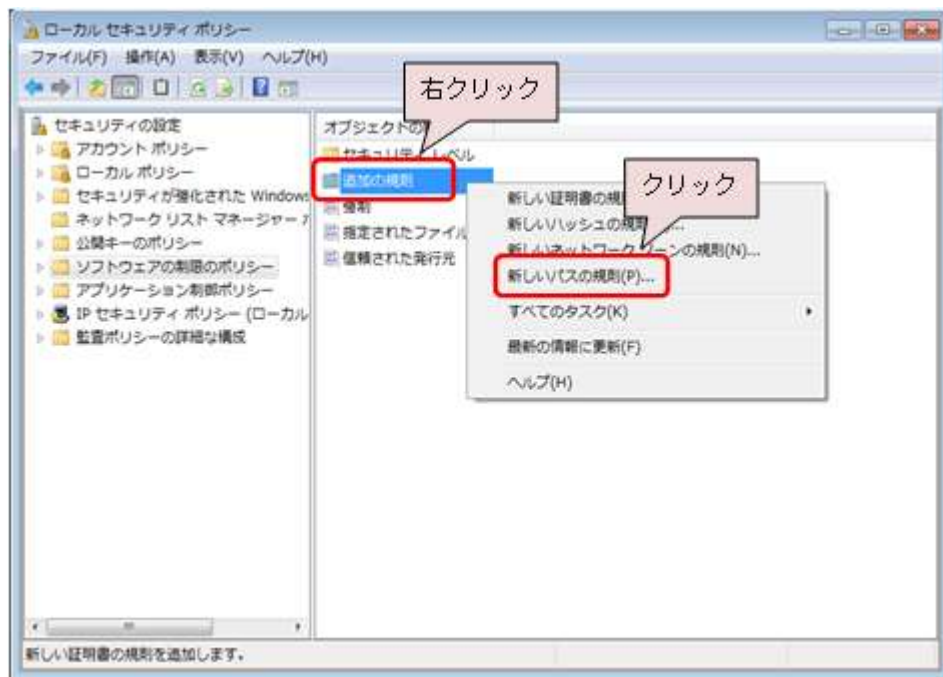


図 1-7 : RLO 対策手順 3

(手順 4)

「新しいパスの規則」の画面が出たら、パス (P) の欄に「**」(アスタリスク 2 つ) を入力し、「*」と「*」の間にカーソルを合わせ右クリックし、表示されたメニューから「Unicode 制御文字の挿入」→「RLO Start of right-to-left override」を選択します。(図 1-8 参照)。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

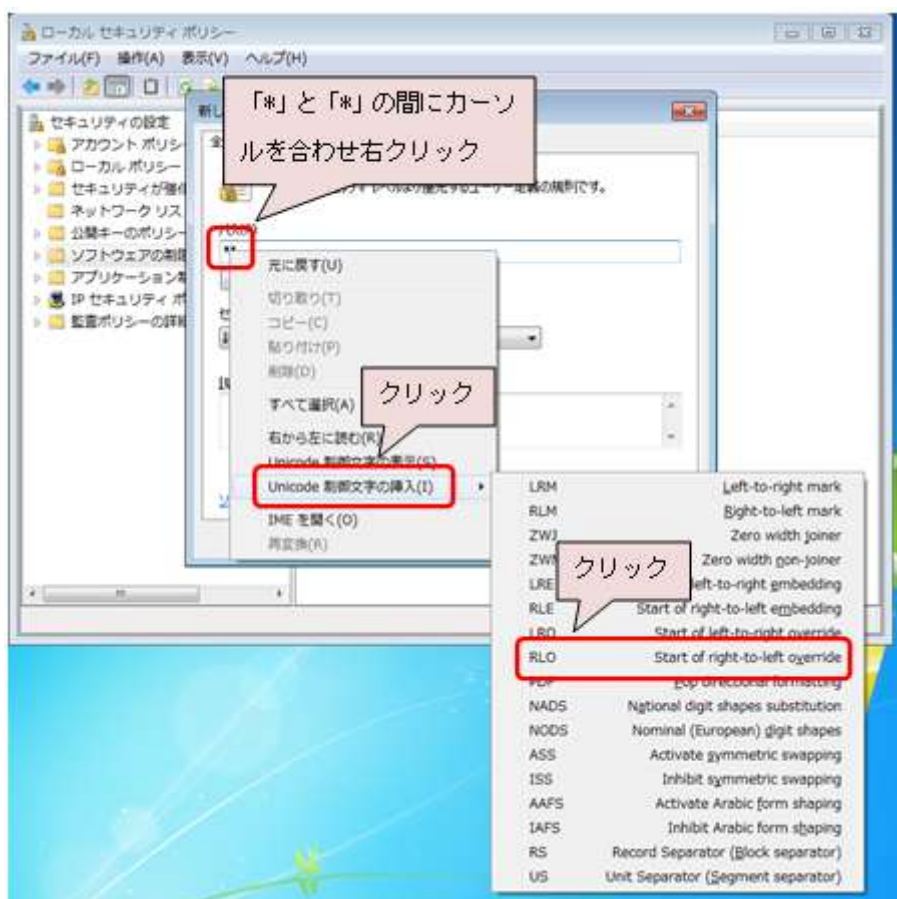


図 1-8 : RLO 対策手順 4

(手順 5)

セキュリティレベル (S) の欄が「許可しない」になっていることを確認して、OK ボタンをクリック (図 1-9 参照)。なお、Windows XP および、Windows Vista の場合もほぼ同様です。



図 1-9 : RLO 対策手順 5

(手順 6)

パソコンを再起動する。

上記対策を行うことで、RLO を使ってファイル名に細工が施されたファイルをクリックすると、図 1-10 のような警告メッセージが表示され、実行が制限されるようになります。

なお、この対策は組織のグループポリシーとして、組織内のパソコン全体を保護する場合でも有効です。

ここで紹介した対策は、文字を [右→左] の順番で読む言語を扱うパソコンには適用しないでください。

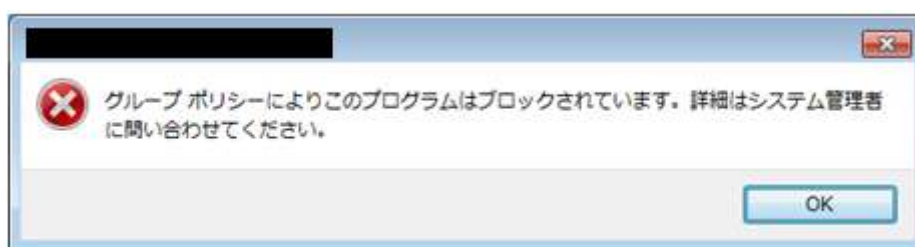


図 1-10 : RLO 対策を行った状態でファイル名に細工が施されたファイルをクリックした場合に表示される警告メッセージ例 (Windows 7 の場合)