プレスリリース
2017 年 9 月 28 日
独立行政法人情報処理推進機構

【注意喚起】Windows アプリケーションの利用における注意

～ダウンロード時のファイル保存先に注意を～

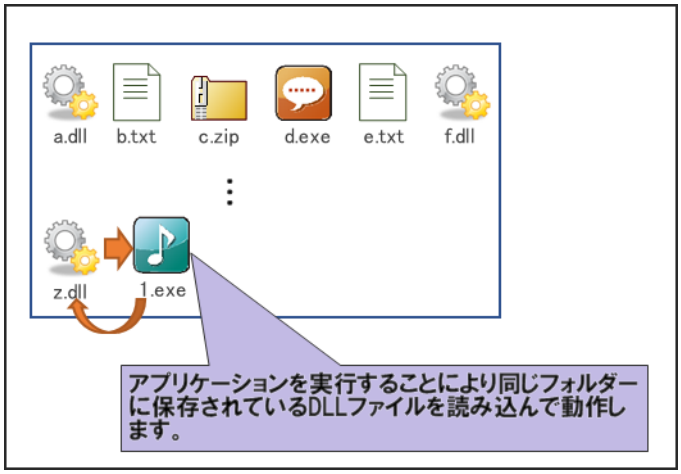
2017 年 4 月から 8 月末までに JVN（Japan Vulnerability Notes）にて公表された“DLL 読み込み”の脆弱性は 53 件で、それ以前（2017 年 1 月から 3 月：4 件）までと比べて急増しています。

この脆弱性は、Windows アプリケーション（以下、アプリケーション）に起因する問題です。広く普及している Windows ゆえ、この脆弱性が存在するアプリケーションは多く、JVN で公表されているものは、氷山の一角といえます。加えて、この脆弱性の場合、対象のアプリケーションが対策済みかどうか、利用者自身が確認するのは困難です。

そこで、利用者の自衛のため、回避策を示し、対策の実施を促す注意喚起を行います。なお、本脆弱性の悪用は困難であり、現在、悪用された事例は、IPA では確認していません。

■ “DLL 読み込み”の脆弱性とは？

Windows OS は、アプリケーションと同じフォルダーに格納されている DLL ファイル (*1) を、優先的に読み込む動作をします。



“DLL 読み込み”の脆弱性は、下記の前提条件が全て揃い、かつ DLL ファイルに悪意ある細工が施されていると、アプリケーション実行時に悪意ある任意のコードが実行されてしまう可能性があるものです。

- 悪用の可能性がある前提条件
  - ・アプリケーション実行時に、DLL ファイルを読み込んで動作するアプリケーションである。
  - ・アプリケーションと DLL ファイルが、ダウンロードフォルダー (*2) などの同じフォルダーに保存されている。

また、この脆弱性が該当するアプリケーションは一般的に広く普及していると考えられます。加えて、利用者には脆弱性が対策済みかの確認は困難です。よって、安全な環境下での利用が難しいのがこの脆弱性の特徴といえます。

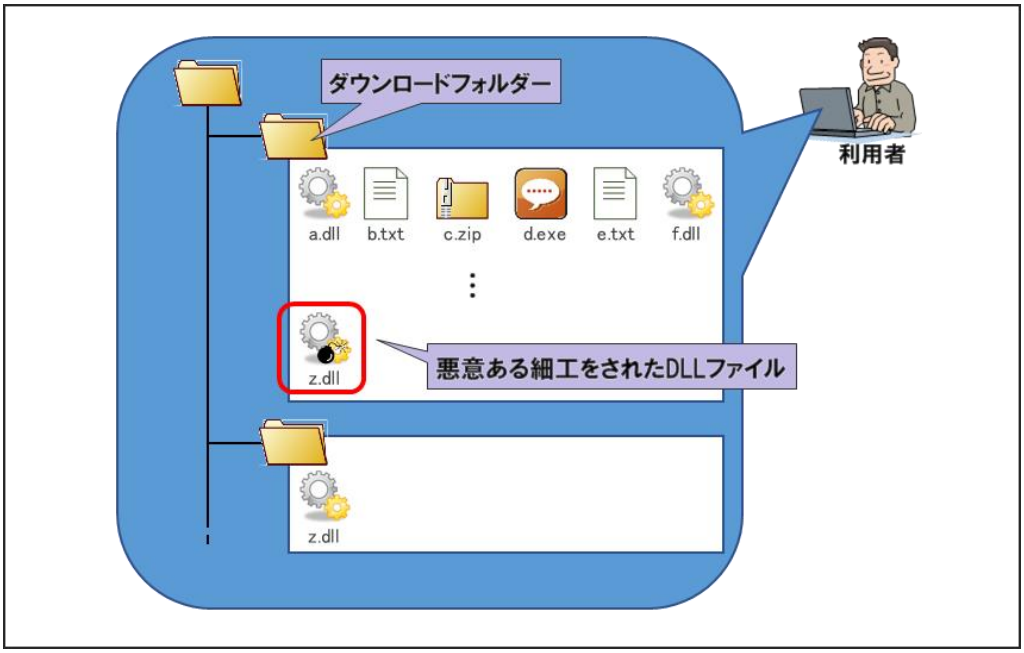
■ “DLL 読み込み”の脆弱性の悪用シナリオ（下記図）

(*1) DLL（Dynamic Link Library）：Windows アプリケーションで使用可能な、共通的な機能をアプリケーションとは別に提供しているもの。これによりアプリケーションに共通機能を保持しておく必要がない。

(*2) ブラウザの設定によることが一般的で、設定変更を行わなければダウンロードフォルダーに保存される。

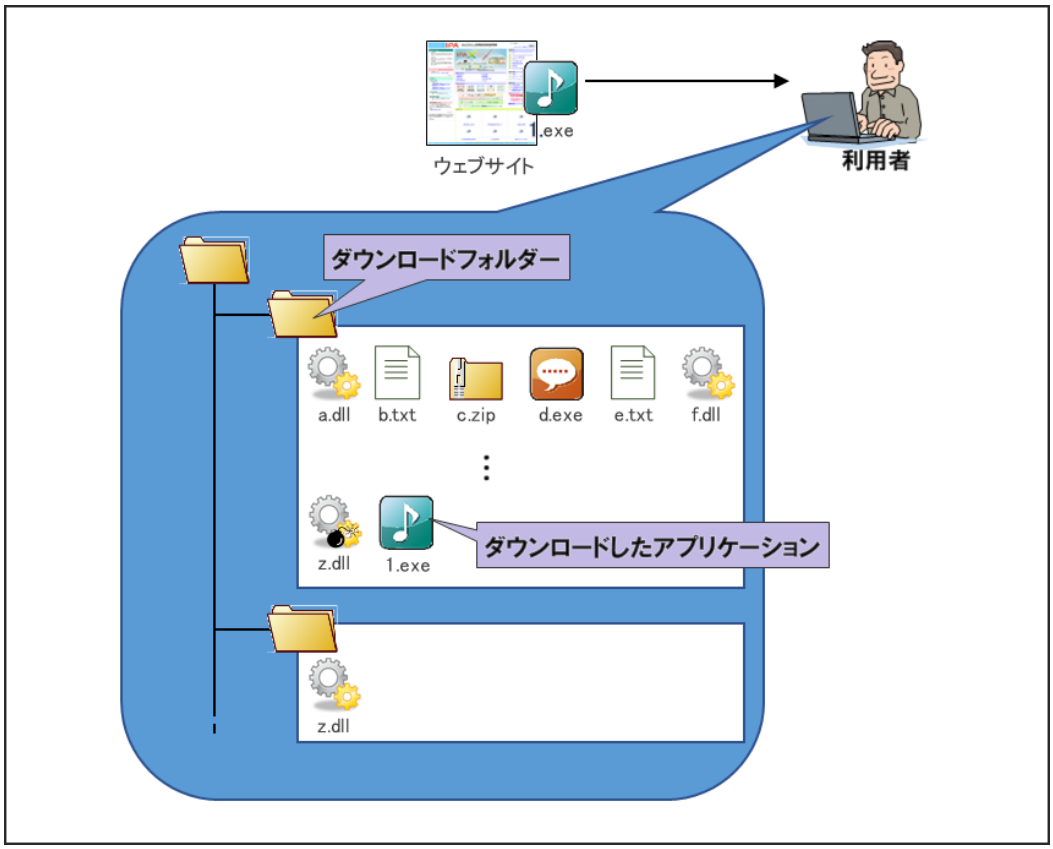
① よくあるダウンロードフォルダーの状況

過去にダウンロードしたファイルは、削除など定期的に整理を行っていなければ、ダウンロードフォルダーにそのまま残存しています。この状態では意図せずに悪意ある DLL ファイルがダウンロードされても、発見するのは困難です。



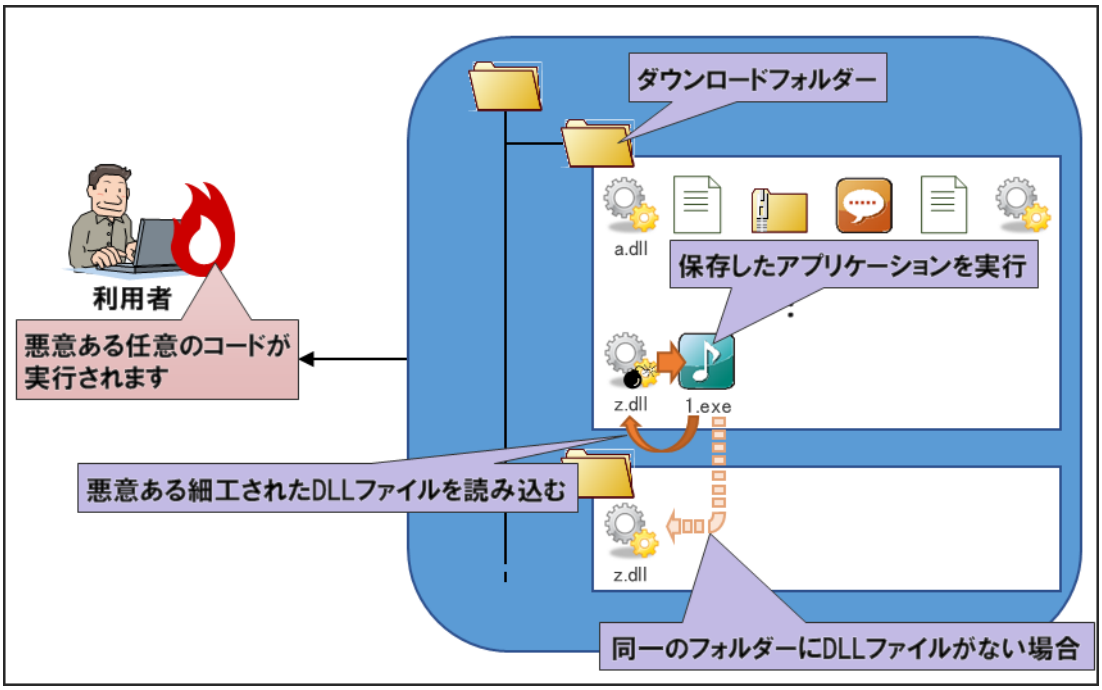
② アプリケーションのダウンロード

ウェブサイトからアプリケーションをダウンロードする際、初期設定ではダウンロードフォルダーに保存されます。



③ アプリケーションの実行

悪意ある DLL ファイルがダウンロードフォルダーに残存している状況下で、脆弱性があるアプリケーションを実行すると悪意ある DLL ファイルが読み込まれてしまいます。



■ 対象となるアプリケーションの種類

- インストーラー
  - アプリケーションを PC に導入するソフトウェア
- 自己解凍書庫
  - 圧縮されたプログラムやデータにそれ自体を解凍するためのプログラムが付加された実行可能形式のファイル
- ポータブルアプリケーション
  - インストーラーを使用することなく、実行可能なソフトウェア

■ 対策方法

以下のどちらかの対策を実施してください。

- ダウンロードフォルダーに保存しない。
  アプリケーションをダウンロードする場合は、新規にフォルダーを作成し、そのフォルダーに保存する。あるいは、ダウンロードフォルダーに保存されたファイルを、新規に作成したフォルダーへ移動する。
- フォルダー内を確認する。
  実行するアプリケーションに同梱されている「ReadMe」などのマニュアルに記載されているファイル構成などを確認し、フォルダー内に正規のファイル以外が保存されていないかを確認する。記載されていない不審なファイルがあれば削除する。

■ 参考情報

- JVNTA#91240916　Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題
  https://jvn.jp/ta/JVNTA91240916/index.html

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 田村／板橋
Tel: 03-5978-7527　Fax: 03-5978-7552　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 白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp