第 15-09-334 号
2015 年 6 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 パソコン内のファイルを人質にとるランサムウェアに注意！ 」
～ メッセージが流暢な日本語になるなど国内流行の懸念 ～

2015 年 4 月に、IPA の情報セキュリティ安心相談窓口に「パソコンに『暗号化しました』というメッセージが表示されて、ファイルが開けなくなった」という相談の件数が増えました。相談内容からランサムウェアの被害と推測されます。

ランサムウェアとは、ファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラムの総称です。IPA に寄せられたランサムウェアに感染したという相談は、2011 年 7 月が初めてでした。その後もランサムウェアに関する相談はありましたが、2014 年 12 月に初めて日本語でメッセージが表示される種類のランサムウェアの相談が 1 件[※1]寄せられました。2015 年 4 月にはさらに異なる種類のランサムウェアの相談が 6 件[※2]あり、すべてが日本語でメッセージが表示される種類のものでした（図 1）。また、そのうち 1 件は初めて企業から寄せられた感染被害の相談でした。

直近で確認されているランサムウェアは支払い方法がビットコインのみのため、現状日本国内で金銭面での被害は大きくないと考えられますが、今後は支払い方法を日本向けに工夫するなどの可能性は否定できません。

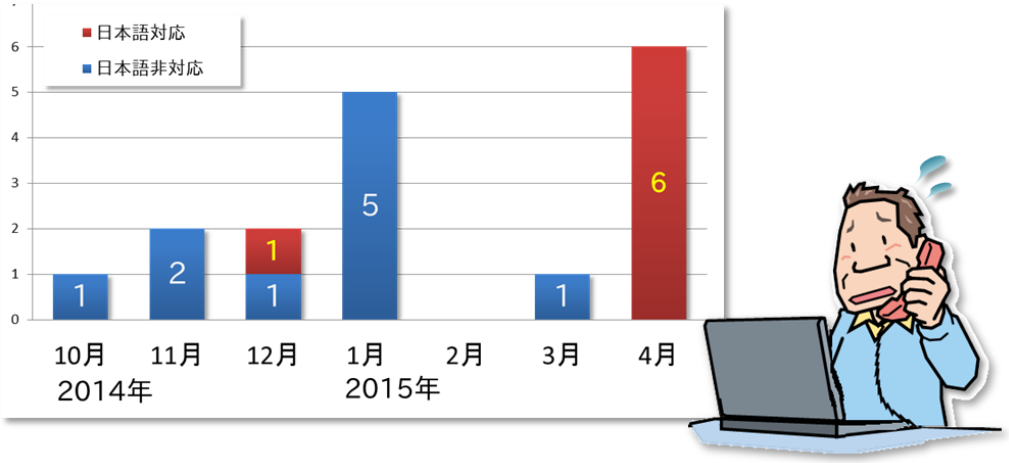

図 1：ランサムウェアに関する相談件数の推移

[1] コンピュータウイルス・不正アクセスの届出状況および相談状況 [2014 年年間] 3-2. 相談事例
https://www.ipa.go.jp/security/txt/2015/2014outline.html#section3
[2] トレンドマイクロ：日本語対応した Crypto ランサムウェアを国内で確認
http://blog.trendmicro.co.jp/archives/11378

IPA が 2014 年 10 月に実施した意識調査[※3]において、ランサムウェアを知っている人は約 2 割という結果が出ています。被害防止の観点から早急に周知を図りたいと考え、今月の呼びかけではこのランサムウェアについて、その手口と対策を紹介します。

（1） ランサムウェアとは

ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。パソコンに保存されている特定のファイル（オフィスドキュメントや圧縮ファイル、音楽、画像など）に**勝手に暗号化処理を行い、読みとれない状態にしてしまう不正プログラムで、ファイルを暗号化した後にそのファイルの復元と引き換えに金銭を要求する**ような文面が表示されます。この現象が、あたかもファイルが身代金を要求するための人質の様であることからランサムウェアと呼ばれます（図 2）。

要求される金額は様々ですが、数万円程度の額に相当するビットコインの支払いを要求されるケースが多いようです。なお、ファイルを暗号化されてしまった後は、ランサムウェア自体を駆除してもファイルを復元することはできません。また、要求された金額を支払ったところで元に戻せる保証もありませんので、感染してしまうとパソコン内の重要なファイルを失ってしまうことになり、影響度の大きい不正プログラムと言えます。

図 2：ファイルを暗号化した後に表示されるメッセージ

ランサムウェアの感染経路は、一般的なウイルスの感染経路と同様です。メール内の URL をクリックしたり、攻撃者が用意したウェブサイトを閲覧したりすることで感染[※4]します。

冒頭の相談の事例では、特にメールの添付ファイルを開いたり、URL をクリックしたりという自覚が利用者になく、怪しいとは思えないブログを閲覧した後で金銭を要求するメッセージが表示されたとのことでした。このことから、パソコンにインストールされているソフトウェアの脆弱性を

---

[3] 2015 年 2 月 17 日発表「2014 年度 情報セキュリティの脅威に対する意識調査」
P31 情報セキュリティに関する攻撃・脅威等の認知
https://www.ipa.go.jp/security/fy26/reports/ishiki/index.html

[4] 2010 年 12 月の呼びかけ
「ウェブサイトを閲覧しただけでウイルスに感染させられる“ドライブ･バイ･ダウンロード”攻撃に注意しましょう！」
https://www.ipa.go.jp/security/txt/2010/12outline.html#5

悪用し、**ウェブサイトにアクセスしただけでウイルスに感染するドライブ・バイ・ダウンロード**[※5]による被害と、IPA では推測しています。

（2） ランサムウェアへの対策

ランサムウェアによって暗号化されてしまったファイルの復元は困難なことから、予防がとても重要です。ランサムウェアの感染対策として、以下を実施してください。

■セキュリティソフトを導入する
セキュリティソフトを導入し、定義ファイルを最新に保つことで、ランサムウェアの感染リスクを低減させることができます。

■OS および利用ソフトウェアを最新の状態にする
OS およびソフトウェアのバージョンを常に最新の状態に保ち、脆弱性をなくすことでドライブ・バイ・ダウンロードによる感染リスクを低減します。

■重要なファイルを定期的にバックアップする
基本的にはランサムウェアによって暗号化されたファイルは復元できません。そのため、重要なファイルについては、定期的にバックアップする必要があります。

IPA ではパソコンにインストールされているソフトウェアが最新の状態であるか、どのようにアップデートを行えば良いのかが確認できるツール「MyJVN バージョンチェッカ[※6]」を提供しています。これを活用して使用しているソフトウェアのバージョン管理の実施を推奨しています。

また、冒頭で紹介した意識調査では、“定期的にバックアップをしている人は約 5 割”で、半数の人は定期的にバックアップを取っていない、という結果が出ています。バックアップはランサムウェアへの対策としてだけでなく、パソコンが突然故障してしまった場合の備えにもなります。

バックアップの方法には、Windows のバックアップ機能を利用する、同一フォルダで管理して定期的に外部媒体やクラウドサービスへコピーするなどがあります。万が一の場合に備えて定期的にバックアップをとることを推奨します。

もしランサムウェアと疑われる症状が確認されたなど、パソコンのウイルス感染に関しての相談は安心相談窓口[※7]に連絡してください。

■お問い合わせ先
情報セキュリティ安心相談窓口
Tel: 03-5978-7509　Fax: 03-5978-7518
E-mail: anshin@ipa.go.jp
技術本部セキュリティセンター 加賀谷／野澤

[5] ドライブ・バイ・ダウンロード： OS や Java や Flash などのソフトウェアの脆弱性を悪用して、ウェブサイトにアクセスした際に不正プログラムをパソコンにダウンロードさせてウイルスに感染させてしまう攻撃です。
[6] MyJVN 一般利用者の方へ MyJVN バージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/personal.html
[7] IPA　情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html