第 16-01-345 号
2016 年 1 月 5 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 ランサムウェア感染被害に備えて定期的なバックアップを 」
～ 組織における感染は組織全体に被害を及ぼす可能性も ～

IPA では、2015 年 4 月に日本語で表示されるランサムウェアの相談が増えたことから、その後の被害増加を懸念し、同年 6 月の呼びかけ※1において注意を促しました。6 月、7 月に安心相談窓口に寄せられた相談は 20 件前後ありましたが、その後しばらく沈静化していました。

しかし 10 月最終週以降、再び相談件数が増加傾向にあります（図 1）。この相談増加の要因には、10 月に確認されたウイルス感染を目的としたウェブサイトの改ざん※2や、12 月に確認されたランサムウェア感染を目的としたメールのばら撒き※3があると考えられます。

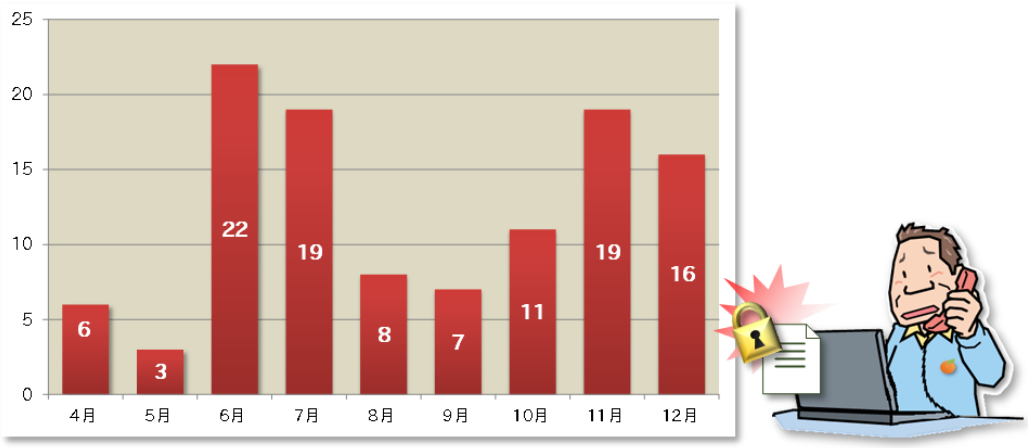

図 1：ランサムウェアに関する相談件数の推移

寄せられた相談によると、感染経路や感染後に暗号化されるファイルの特徴に違いはありますが、**ファイルが開けなくなってしまうという被害は共通**でした。特に、組織内の端末が感染してしまった場合は、被害が感染した端末のみではなく組織全体に及ぶ懸念があり、業務遂行に大きな影響を与える可能性があります。個人、組織を問わず、ランサムウェアの対策として、**定期的なバックアップ取得は必須**と言えます。

今月の呼びかけでは IPA に寄せられたランサムウェアに関する相談事例を基に、その感染経路と対策について紹介します。

---

[1] 2015 年 6 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！ 」
https://www.ipa.go.jp/security/txt/2015/06outline.html
[2] トレンドマイクロ：ランサムウェア拡散を狙う Web 改ざん、国内サイト 70 件以上で被害を確認
http://blog.trendmicro.co.jp/archives/12434
[3] 日本 IBM:ランサムウェア CryptoWall への感染を狙った攻撃を 11 月下旬から連日確認
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ransomware_20151208

（1） ランサムウェアの感染経路

ランサムウェアの感染経路は一般的なウイルスと同様、主にメールからの感染とウェブサイトからの感染があり、以下のようなケースが考えられます。

■メールからの感染

・メール本文中の URL にアクセスすることで感染

メール本文中に記載されている URL のウェブサイトが、ランサムウェアに感染するように細工されていて、ソフトウェアに脆弱性がある状態でこの URL にアクセスしてしまうことで、ドライブ・バイ・ダウンロード攻撃によってランサムウェアに感染する。

・メールの添付ファイルを開くことで感染

メールにランサムウェアに感染するように細工されたファイルが添付されていて、ソフトウェアの脆弱性有無に関わらず、このファイルを開いてしまうことで感染する。

IPA で確認したランサムウェアの感染を狙ったメールは、請求書の確認を促すような英語の文面で、zip ファイルが添付されていました。この zip ファイルには、ランサムウェアをダウンロードするように細工されたファイルが含まれていて、この細工されたファイルを開いてしまうとランサムウェアに感染するというものでした。

■ウェブサイトからの感染

・改ざんされた正規のウェブサイトや細工された不正広告を閲覧することで感染

ソフトウェアに脆弱性がある状態で、ランサムウェアに感染するように改ざんされた正規のウェブサイトや細工された不正広告を閲覧してしまうことで、ドライブ・バイ・ダウンロード攻撃によってランサムウェアに感染する。

・ウェブサイトからダウンロードしたファイルを開くことで感染

ダウンロードしたファイルがランサムウェアに感染するように細工されていて、ソフトウェアの脆弱性有無に関わらず、このファイルを開いてしまうことで感染する。

IPA に寄せられた相談にも、正規のウェブサイトにアクセスしただけでランサムウェアに感染したという事例がありました。確認したところ、当該ウェブサイトが改ざんされていたことがわかりました。

（2） ランサムウェアへの対策

ランサムウェアの被害は、ファイルが暗号化され開けなくなってしまうことです。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、重要なファイルについては暗号化されてしまった場合でも復元できるよう、**定期的にバックアップを取得してください。**

図 2.重要なデータは定期的にバックアップを

■バックアップに使用する装置・媒体

バックアップに使用する装置・媒体は各々特徴がありますので、バックアップ対象となるファイルに応じて使い分けることをお奨めします。例を以下に示します。

表 1. バックアップするファイル別の保存先例

No.	バックアップするファイル	バックアップに使用する装置・媒体
1	基本的に加工や編集が発生しないファイル 例・写真ファイル ・音楽ファイル　など	光学メディア（DVD-R、BD-R など）
2	基本的に加工や編集が発生するファイル 例・ドキュメントファイル　など	USB メモリ、メモリーカード、 外付け HDD

■バックアップにおける留意事項

・バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する
・バックアップに使用する装置・媒体は複数用意し、バックアップする
・バックアップから正常に復元できることを定期的に確認する

IPA に寄せられた相談に、「パソコンに接続していた外付け HDD のファイルも暗号化された」、「ネットワーク上のファイルサーバに保存していたファイルも暗号化された」という事例がありました。ランサムウェアに感染したパソコンと接続したままになっていたことで、パソコン以外に保存されていたファイルも暗号化されてしまったためと考えられます。このため、**バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続することが重要です。**

また、パソコンに接続している時にバックアップに使用する装置・媒体が暗号化されてしまう可能性もあります。複数の装置・媒体でバックアップしておくことで、万が一どれかが暗号化されても、それ以外のものを使って復元することができます。なお、バックアップに使用する複数の装置・媒体は、パソコンに同時に接続しないことが重要です。

バックアップの取得以外では、以下の対策を実施してください。ランサムウェア以外のウイルス対策としても有効です。

■OS およびソフトウェアを常に最新の状態に保つ

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、脆弱性を解消することで感染リスクを低減します。

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※4」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ます。

■セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ

セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つことで、ランサムウェアへの感染リスクを低減します。

■メールや SNS のファイルや URL に注意する

メールや SNS の添付ファイルを開くことや、本文中の URL をクリックすることでランサムウェアに感染する可能性があります。

受信したメールは送信者、添付ファイル、文面等に十分に注意を払い、**心当たりのないメールや英文など文面の意味が分からないメールの添付ファイルは安易に開かないほうが賢明です。**

■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

[4] 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