

## セキュリティ Q&amp;A

# 企業を狙い始めたランサムウェアに どう対処すれば良いのか

## 回答サマリー

### 基本的なセキュリティ対策とバックアップで対抗

ランサムウェアとは、感染したパソコンを利用できなくするマルウェアです。感染すると、正常な状態に戻すことを引き替えに金銭を支払うよう要求されます。日本国内で感染報告が相次いでおり、重要なデータを失う可能性があるため、対策が急務となっています。マルウェアの感染対策や脆弱性解消といった基本的な対策、さらにデータの定期的なバックアップなどの対策が重要です。





## 回答詳細

### 企業の情報資産を脅かす暗号化型ランサムウェア、 海外では「身代金」を支払った事例も

ランサムウェア (Ransomware) は、感染したパソコンの利用を阻害したり、データを利用できなくするマルウェアです。感染すると画面上に、「正常な状態に戻すには、金銭『 (=身代金 (Ransom)) 』を支払う必要がある」などと表示し、脅迫するのが特徴です。

ランサムウェアには、大きく分けて2種類あります。画面をロックしてしまい、操作をできなくする「画面ロック型」と、ファイルやハードディスクを勝手に暗号化し、使用できなくする「暗号化型」です。いずれも復旧の交換条件として金銭が要求されます。特に「暗号化型」は、自力で暗号を解読することは困難であることが多く、被害に遭うと重要なデータを失うリスクがあります。

### 主なランサムウェアのタイプ

	画面ロック型	暗号化型		
タイプ	 端末の画面をロックし、 操作をできなくする	 データを暗号化して使用できなくする		
対象	画面操作 	内蔵ドライブ (HDD など) 	外付けドライブ (USB メモリー など) 	ネットワーク上の共有ドライブ 
データの復旧の	比較的容易	自力によるデータ復旧は 困難であることが多い		

**セキュリティ Q&A 企業を狙い始めたランサムウェアにどう対処すれば良いのか**

2016年に入り、国内でもランサムウェアによる被害が増加傾向にあります。情報処理推進機構(IPA)に寄せられた相談件数は、2016年1月に11件でしたが、3月には96件へと急増しました。相談の多くは、「暗号化型」に関するものです。主な感染経路は請求書などを装ったメールの添付ファイルですが、改ざんされたWebサイト経由で感染する場合があります。

被害が公表されることは少ないですが、海外ではまれに公表するケースもあります。例えば、アメリカの病院ではシステムがランサムウェアに感染しました。またカナダの大学が被害に遭ったケースもあります。苦渋の選択を迫られるなか、いずれも「身代金」を支払いました。

## 定期的なバックアップデータさえあれば、 身代金を支払わずに済むことも

「暗号化型」ランサムウェアに狙われるのは、内蔵ドライブのデータだけとは限りません。外付けドライブやネットワーク経由でファイルサーバー上のファイルを暗号化するなど、法人や組織を狙ったと見られる攻撃も発生しています。

またパソコンだけでなく、スマートフォンを対象としたランサムウェアが登場しています。今後、こうした脅威がIoTへ波及することへ懸念の声も出ています。

重要なシステムやデータが「人質」に取られるリスクは高まりつつあるといえます。ランサムウェアの感染を防ぐには、まず、セキュリティ対策ソフトを導入して定義ファイルを最新の状態に保つようにしましょう。また、OSとアプリケーションに脆弱性があると、それが感染の原因にもなりかねません。OSとアプリケーションも常に最新状態にアップデートして、脆弱性を解消しておくことが大切です。あわせて、メールの添付ファイルを安易に開かないなど、セキュリティの基本的な事前対策が求められます。

こうした事前対策にとどまらず、万が一感染した場合に備えて、普段からデータを定期的にバックアップしておくことも重要です。ただし、ファイルサーバーを狙うケースもあるため、データのバックアップは隔離された環境へ行うなど対策が必要となります。

万が一、ランサムウェアに感染した場合は、IPAの情報セキュリティ安心相談窓口やセキュリティベンダーなど、専門機関や専門家に相談することをおすすめします。身代金を支払わずに復号できるツールなどをセキュリティベンダーが独自に開発し、提供している場合もあります。

重要な情報資産を人質にとるランサムウェアは今や多くの企業にとっての脅威の一つになりつつあります。その感染を防ぐには、まずは、ここで示したようなセキュリティの基本的な事前対策を確実に実践することが大切です。