

# ランサムウェア攻撃について

## ～ ランサムウェア攻撃の脅威とは ～

従業員向けコース ー No.2

## 導入



パソコン(サーバー含む)やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、復旧に金銭を支払うよう脅迫する**ランサムウェア**と呼ばれるウイルスへの感染被害が、大企業や中小企業に関係なく確認されています。

## 用語解説

### ●ランサムウェア (ransomeware)

**マルウェア**の一種で、パスワードでシステムをロックしたり、ファイルやフォルダを暗号化するなどしてコンピュータを利用できない状態（人質）にして、もとの状態に戻すことと引き換えに金銭（身代金）を要求する不正プログラム。

### ●マルウェア (malware)

コンピュータウイルス、スパイウェア、ボットなどの不正プログラムの総称。これらの不正プログラムは、使用者や管理者の意図に反して、コンピュータに入り込み、悪意のある行為を行うことから、このように呼ばれる。マルウェア (malware) は“Malicious Software”（悪意のソフトウェア）を短縮した造語。

#### 【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

## 導入

ランサムウェアに感染すると、パソコンやスマートフォンのファイルを暗号化されたり、画面ロック等されファイルを開けなくなったり、パソコンやスマートフォンを利用できなくなってしまう。また、暗号化されたファイルが顧客情報や業務で使用している共有ファイル等、企業にとって重要な情報であった場合は、業務の遂行に大きな支障がでることも考えられます。

## 導入



パソコンの脆弱性を悪用したり、メールの添付ファイルやメール本文中のリンクを開かせることで感染させたりと、従業員一人ひとりが気をつけないと、こんなことになりかねません・・・。



**事例**

さてと、午後も仕事仕事と・・・。

広瀬洋子 【株式会社シックハック／総務部社員】

## 事例

あっ！  
そういえば午前中に届いたメールを読まなきゃ。

午前中は忙しくてメール読めてなかったから・・・。

## 事例

あれれ？こんな時にソフトウェアの更新かぁ・・・。

先月もメールきてたけどやったかしら？  
まあ気がついた時に更新しておかないと忘れちゃうからな。



事例

あれ？  
今ので更新されたのかな？

・・・たぶん大丈夫でしょ、さあ仕事の続きをしょ。

事例

え！あれ！？  
なにこの画面！！？

 **警告！** ATTENTION!  
Your files have been encrypted!  
あなたのデータは暗号化されました。  
お金を支払ってください。

Q: ファイルは回復できますか？  
ファイルを修復したい場合は3万円の支払いが必要です。制限時間が過ぎるとデータは永遠に失われますのでお急ぎください！

お支払いはこちらから

数分後

**事例**

なにになに！？

広瀬さん！どうしたの！？





## 事例

これ見てください！  
急に”暗号化しました”、”お金を払え”、っていう  
画面が現れて！

なにこれ！？

ん？これはもしかしてランサムウェアに感染したんじゃ…  
とりあえずネットワークの線を抜くぞ。  
他の人も感染していないか確認してくれ！



事例

ランサムウェア…って何ですか？



やはりそうだね、  
ここの所に『ファイルを元に戻したいのならお金を払え』って書いてある。


事例

ファイルを元に？お金を払え？？  
何ですかそれ！？

うん、ファイルを使えない様に入質として預かったから、  
元にもどきたいなら身代金を払って脅迫してるんだ。  
広瀬さんのパソコン内にあるファイルは、  
ランサムウェアによってほとんどが暗号化されて使えないはずさ。

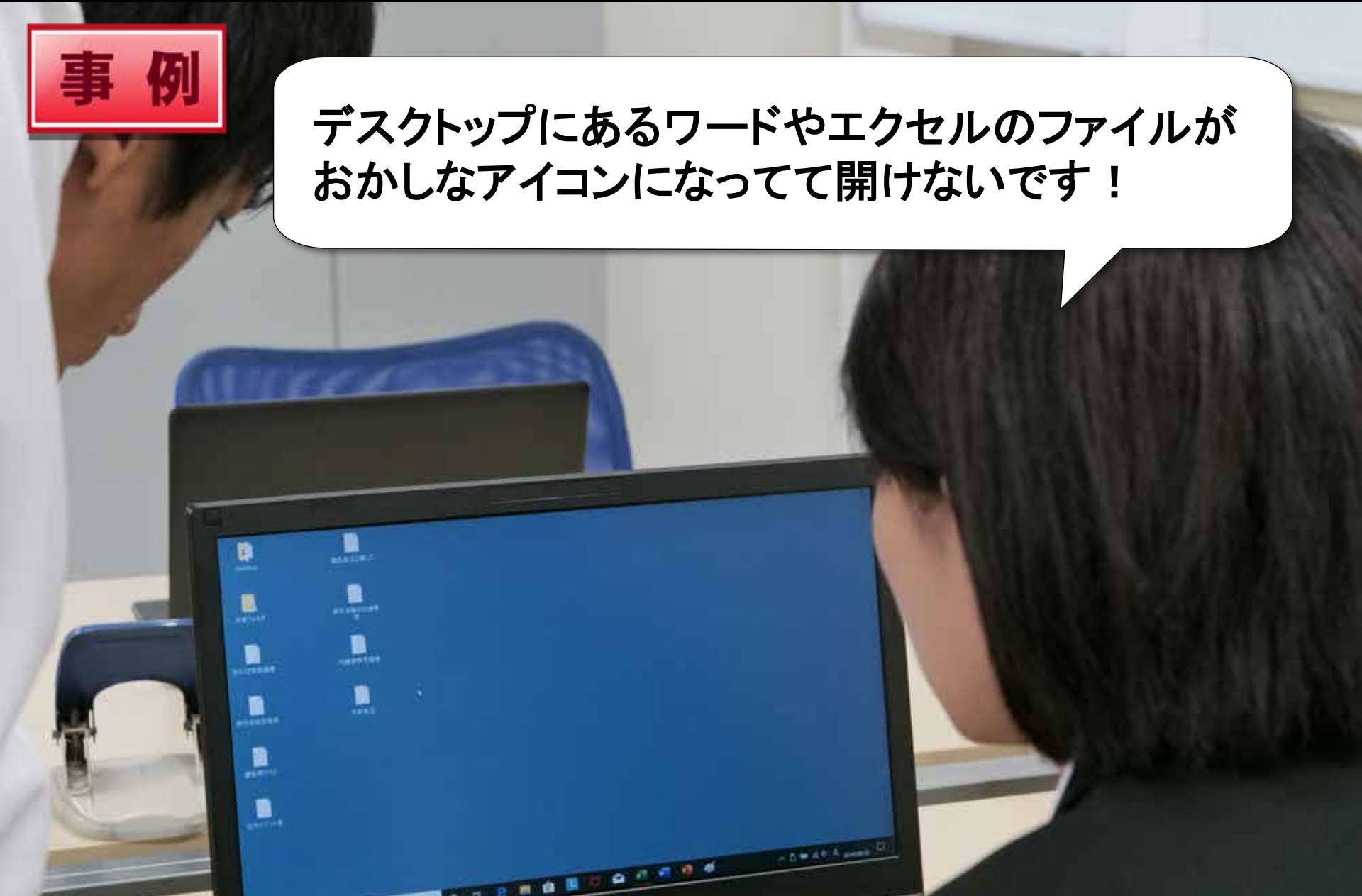
事例

あー！

A woman with short dark hair, wearing a black business suit over a white shirt, is shown from the chest up. She has a shocked expression on her face, with wide eyes and an open mouth. She is holding a black folder or tablet in front of her. A large, white, jagged speech bubble is superimposed over the lower left of the image, containing the text 'あー！' (Aa!). The background is a plain, light-colored wall.

**事例**

デスクトップにあるワードやエクセルのファイルがおかしなアイコンになって開けないです！





**事例**

だろうな・・・何か怪しいメールの添付ファイルか、  
本文中のリンク先URLをクリックしなかったか？

怪しいのなんて・・・  
ソフトウェアの更新のお知らせメールが届いていたので、  
それならさっきクリックしましたよ・・・。

事例

おそらくそれが原因だな・・・、  
ひょっとして先月のソフトウェアの更新もやってなかったんじゃないか？

はい・・・なので今度は早くやろうと・・・。

やっぱり、  
それで脆弱性が解消されていないから、  
今回のランサムウェアに感染したって訳か。

**事例**

**あー！**

**今度は何だ！？**

**事例**

共有フォルダ内にあるワードやエクセルのファイルがおかしいアイコンになってて見られなくなってます！





**事 例**

広瀬さんも共有フォルダ使っているよね？

はい、  
フォルダ内のファイルを  
参考に使っていますので。

それなら共有フォルダ内のファイルも暗号化されてしまったようだね。

事例

えー！？  
そうしたら他の人にも迷惑が・・・。

共有フォルダ内のファイルは、  
毎日バックアップを取って別サーバーに保管しているから大丈夫だ。  
広瀬さんのパソコンは初期化するしかないが。

**事例**

そうですか、ああよかった・・・。

自分のパソコン内にあるファイルは仕方ないとしても、  
他の人にまで迷惑はかけられないですから。



**事例**

でもさっきの画面に書いてあった様に、  
『お金を払え』ばデータを元に戻してくれるんですか？

戻してくれるかはわからないけど、  
こんなことをやるヤツの言うことなんか信じられないだろ？



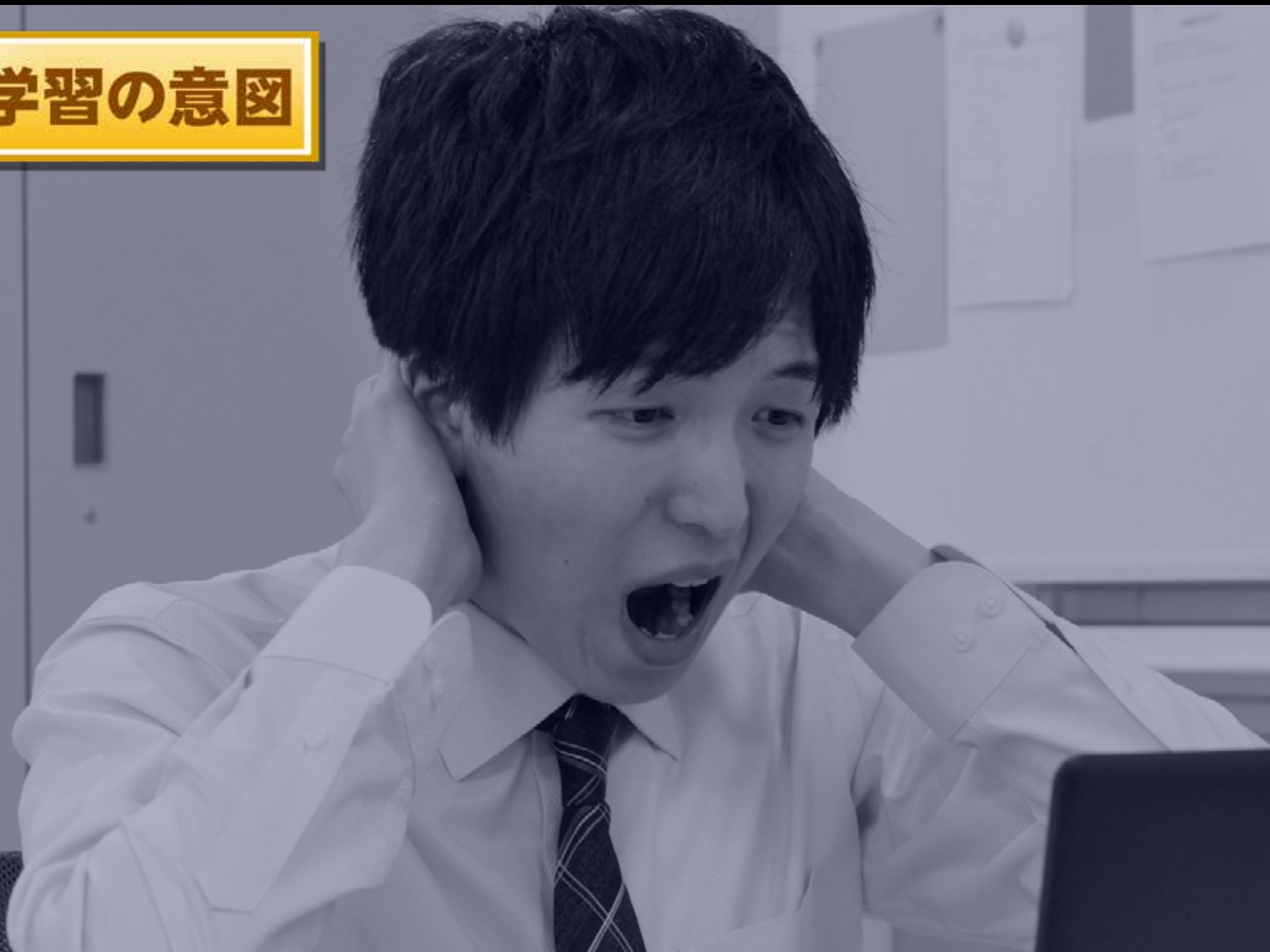
**事例**

それもそうですね。

そういうことだ。



## 学習の意図



**ランサムウェア**は、感染したパソコンだけではなくパソコンに接続している外部記憶媒体や、ネットワークで接続されているサーバー内のファイルまで暗号化してしまいます。また**ランサムウェア**の種類によっては、感染したパソコンの画面をロックしてしまい、まったく利用できなくしてしまうものもあります。

## 用語解説

### ●ランサムウェア (ransomeware)

**マルウェア**の一種で、パスワードでシステムをロックしたり、ファイルやフォルダを暗号化するなどしてコンピュータを利用できない状態（人質）にして、もとの状態に戻すことと引き換えに金銭（身代金）を要求する不正プログラム。

### ●マルウェア (malware)

コンピュータウイルス、スパイウェア、ボットなどの不正プログラムの総称。これらの不正プログラムは、使用者や管理者の意図に反して、コンピュータに入り込み、悪意のある行為を行うことから、このように呼ばれる。マルウェア (malware) は“Malicious Software”（悪意のソフトウェア）を短縮した造語。

#### 【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

## 学習の意図



感染しないことが一番良いのですが、もし感染してしまった場合は、すぐに復旧できる様、データのバックアップをしておくことが重要です。決して身代金を払う行為だけは行わないことです。



## 学習の意図

「ランサムウェア攻撃」について、以下を学習しましょう。

1. ランサムウェアの感染に備え、  
重要なデータのバックアップを他の記録媒体に保存する。

## 正しい対処法



感染しないための基本的な対策として、受信メールやウェブサイトの十分な確認、添付ファイルや本文内のリンク先URLを安易にクリックしない、セキュリティソフトの使用、サポートの切れたOSやソフトウェアの利用停止、使用しているOSやソフトウェアの脆弱性の解消、などが挙げられます。

## 正しい対処法



また、共有サーバーのアクセス権の最小化(必要最小限のアクセス権の設定)や、外部記憶媒体は使用する時だけ接続し、使わない時は接続しておかない、などによる対策で、被害の拡大を防ぐことに繋がります。

## 正しい対処法



その上で、**ランサムウェア**に感染してしまった場合を考慮し、重要なデータのバックアップを他の記録媒体に保存しておきましょう。また、保存したバックアップのデータから、正常に復旧できるか確認しておくことも重要になります。



## 用語解説

### ●ランサムウェア (ransomeware)

**マルウェア**の一種で、パスワードでシステムをロックしたり、ファイルやフォルダを暗号化するなどしてコンピュータを利用できない状態（人質）にして、もとの状態に戻すことと引き換えに金銭（身代金）を要求する不正プログラム。

### ●マルウェア (malware)

コンピュータウイルス、スパイウェア、ボットなどの不正プログラムの総称。これらの不正プログラムは、使用者や管理者の意図に反して、コンピュータに入り込み、悪意のある行為を行うことから、このように呼ばれる。マルウェア (malware) は“Malicious Software”（悪意のソフトウェア）を短縮した造語。

#### 【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

## 確認テスト 問題

### No.2 ランサムウェア攻撃について ～ランサムウェア攻撃の脅威とは～

#### Q1

攻撃者が他人のPCにランサムウェアを感染させる狙いはどれか。

(出典: 令和元年度秋期 ITパスポート試験 公開問題 問98)

#### 選択肢

- |  |                                      |
|--|--------------------------------------|
|  | 1. PC内の個人情報ネットワーク経由で入手する。            |
|  | 2. PC内のファイルを使用不能にし、解除と引換えに金銭を得る。     |
|  | 3. PCのキーボードで入力された文字列を、ネットワーク経由で入手する。 |
|  | 4. PCへの動作指示をネットワーク経由で送り、PCを不正に操作する。  |

次のページで正解と  
解説を確認しましょう

## 確認テスト 正解と解説

### Q1

攻撃者が他人のPCにランサムウェアを感染させる狙いはどれか。

(出典:令和元年度秋期 ITパスポート試験 公開問題 問98)

正解	選択肢
	1. PC内の個人情報ネットワーク経由で入手する。
●	2. PC内のファイルを使用不能にし、解除と引換えに金銭を得る。
	3. PCのキーボードで入力された文字列を、ネットワーク経由で入手する。
	4. PCへの動作指示をネットワーク経由で送り、PCを不正に操作する。

### 【解説】

出典:令和元年度秋期 ITパスポート試験 公開問題 問98

## 確認テスト 問題

### No.2 ランサムウェア攻撃について ～ランサムウェア攻撃の脅威とは～

#### Q2

職場のPCを使用していたところ、ウイルス対策ソフトでウイルスを検出した旨のメッセージが表示された。このPCで直ちに行うべきこととして、適切なものはどれか。

(出典：平成29年度秋期 ITパスポート試験 公開問題 問94)

#### 選択肢

- |  |                    |
|--|--------------------|
|  | 1. PCの再起動          |
|  | 2. 電子メールによる職場内への通知 |
|  | 3. ネットワークからの切断     |
|  | 4. ファイルのバックアップ     |

次のページで正解と  
解説を確認しましょう



## 確認テスト 正解と解説

### Q2

職場のPCを使用していたところ、ウイルス対策ソフトでウイルスを検出した旨のメッセージが表示された。このPCで直ちに行うべきこととして、適切なものはどれか。

(出典：平成29年度秋期 ITパスポート試験 公開問題 問94)

正解	選択肢
	1. PCの再起動
	2. 電子メールによる職場内への通知
●	3. ネットワークからの切断
	4. ファイルのバックアップ

### 【解説】

出典：平成29年度秋期 ITパスポート試験 公開問題 問94