IPA Technical Watch

IPA Better Life with IT

ランサムウェアの脅威と対策

～ランサムウェアによる被害を低減するために～

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目次

はじめに

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ある。感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいる。特に 2015 年以降、パソコンに保存されているファイルを暗号化し、復号（暗号化されたデータを元の状態に戻すこと）のための金銭を要求するランサムウェアが多く確認されている。IPA の情報セキュリティ安心相談窓口でも 2015 年 4 月にこのランサムウェアに関する相談が急増した。このランサムウェアの厄介なところは、感染した際の被害の大きさが暗号化されたファイルの重要度に依存する点である。暗号化されたファイルの復元は困難であるため、暗号化されたファイルによっては企業存続に致命的なダメージを与える可能性があり、早期復旧のためには金銭要求に応じざるを得ない状況に陥ることが考えられる。そのため、ランサムウェアに感染しないための対策が重要であるものの、万が一ランサムウェアに感染したことでファイルを暗号化されてしまった場合のリスクを想定し、被害を低減させるための環境づくりも重要となる。

本書では、現在主流となっているファイルを暗号化して復号するために金銭を要求するランサムウェアに関する、一般的な脅威と対策をまとめている。ランサムウェアに感染しないため、また感染した場合でも被害を最小限に留めるために、必要となるセキュリティ対策の手引きとして参照してほしい。

本書の対象読者

本書の主な対象読書は、以下の方々を想定している。

・パソコンでインターネットを用いて、ウェブサイト閲覧やメールを利用する方。
（個人のパソコン利用者および企業のパソコン利用者）
・企業内のウイルス対策を検討しているシステム管理者の方

1. ランサムウェアの脅威

IPA の情報セキュリティ安心相談窓口へ寄せられたランサムウェアに関する相談情報などを基に、ランサムウェアの基本的な動作概要や種別、被害内容についての概要を述べる。

1.1. ランサムウェアのタイプ

ランサムウェアはパソコンに特定の制限をかけて、その制限解除と引き換えに金銭を要求する不正プログラムである。制限をかける対象によって大別すると、パソコンに保存しているファイルを暗号化する「ファイル暗号化型」と、パソコンの操作ができないようにロックをかける「端末ロック型」の２種類がある。

表 1-1-1. ランサムウェアのタイプ

No.	ランサムウェアのタイプ	制限をかける対象
1	ファイル暗号化型	画像、文書、データ等のファイル[1]
2	端末ロック型	端末の特定のソフトウェア （OS など）

いずれのタイプのランサムウェアもパソコンに制限をかけた後、パソコン上に制限解除と引き換えに金銭を要求する（支払い方法を説明する）画面を表示する。画面の表示方法は、テキストやブラウザ画面（HTML）、画像など、ファイル形式やメッセージの内容は様々なものが確認されている。

1.2. ランサムウェアの種別

ランサムウェアは同じタイプであっても様々なものが存在する。IPA の情報セキュリティ安心相談窓口に寄せられた相談で確認できた、主要なランサムウェアについてその名称やタイプについて以下に紹介する。また、当該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につけられる拡張子の例と、金銭を要求する画面に用いられる言語が日本語に対応しているかについても合わせて記載する。

[1] ランサムウェアに暗号化されてしまうファイルは特定の拡張子をもったファイル。どの拡張子をもったファイルが暗号化されてしまうかについては、各々のランサムウェアの仕様に依存する。

表 1-2-1. ランサムウェアの種別抜粋

No.	相談初出時期	名称	タイプ	ファイル拡張子	日本語対応
1	2015 年 4 月	Crypt0L0cker	ファイル暗号化型	.encrypted	○
2	2015 年 12 月	CryptoWall	ファイル暗号化型	ランダム文字列	×
3	2015 年 12 月	TeslaCrypt	ファイル暗号化型	.vvv	×
4	2016 年 2 月	Locky	ファイル暗号化型	.locky	○
5	2016 年 3 月	Android 端末のランサムウェア	端末ロック型	-	○
6	2016 年 6 月	Zepto	ファイル暗号化型	.zepto	○

1.3. ランサムウェアによるファイル暗号化

現在、主流となっているランサムウェアはファイル暗号化型である。ファイル暗号化型のランサムウェアが、ファイルを暗号化するまでの基本的な動作の流れを次に示す。

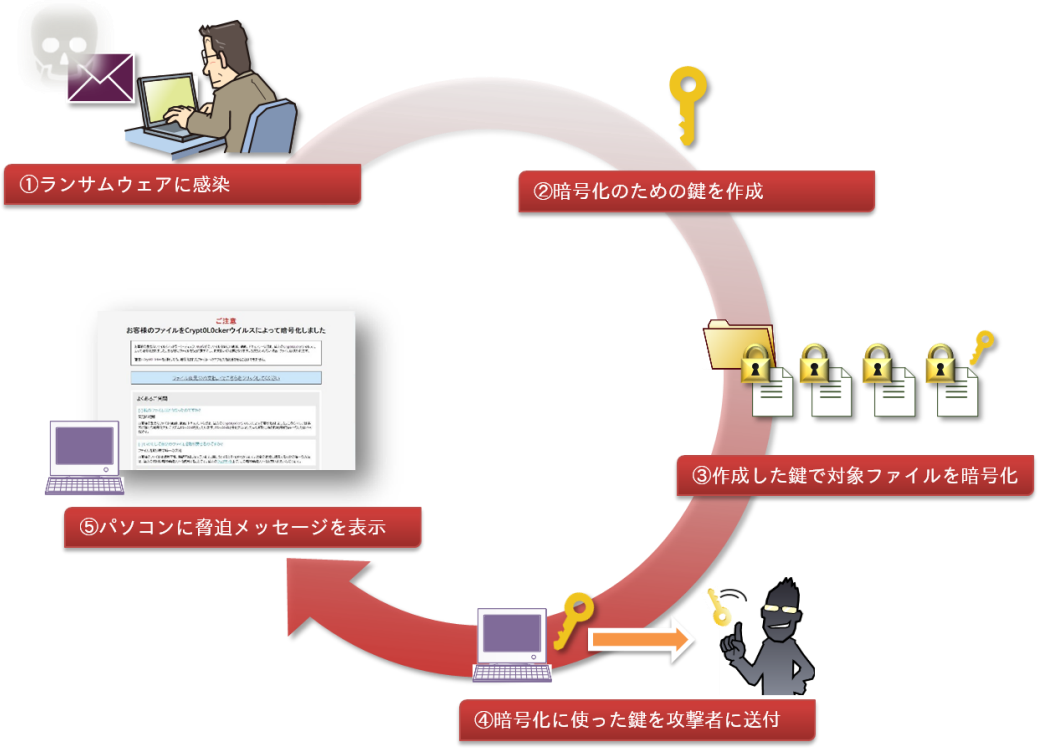

図 1-3-1：ランサムウェアのファイル暗号化の動作概要

① パソコンがランサムウェアに感染させられる

② パソコン上でファイル暗号化用の鍵が作成される

③ ②のファイル暗号化用の鍵でファイルが暗号化される

④ ②のファイル暗号化用の鍵が攻撃者に送付される

⑤ パソコンの画面に金銭支払いを要求する画面が表示される

1.4. ファイル暗号化型のランサムウェア感染時の影響範囲

ファイル暗号化型のランサムウェアに感染した場合、端末ロック型と異なり当該パソコンだけでなく、同一ネットワーク上のファイルサーバや接続している記録媒体などにもその影響が及ぶ場合がある。具体的には、感染したパソコンが（その際、ログインしているユーザの権限で）アクセス可能な場所にあるファイルに影響が及ぶ可能性がある。

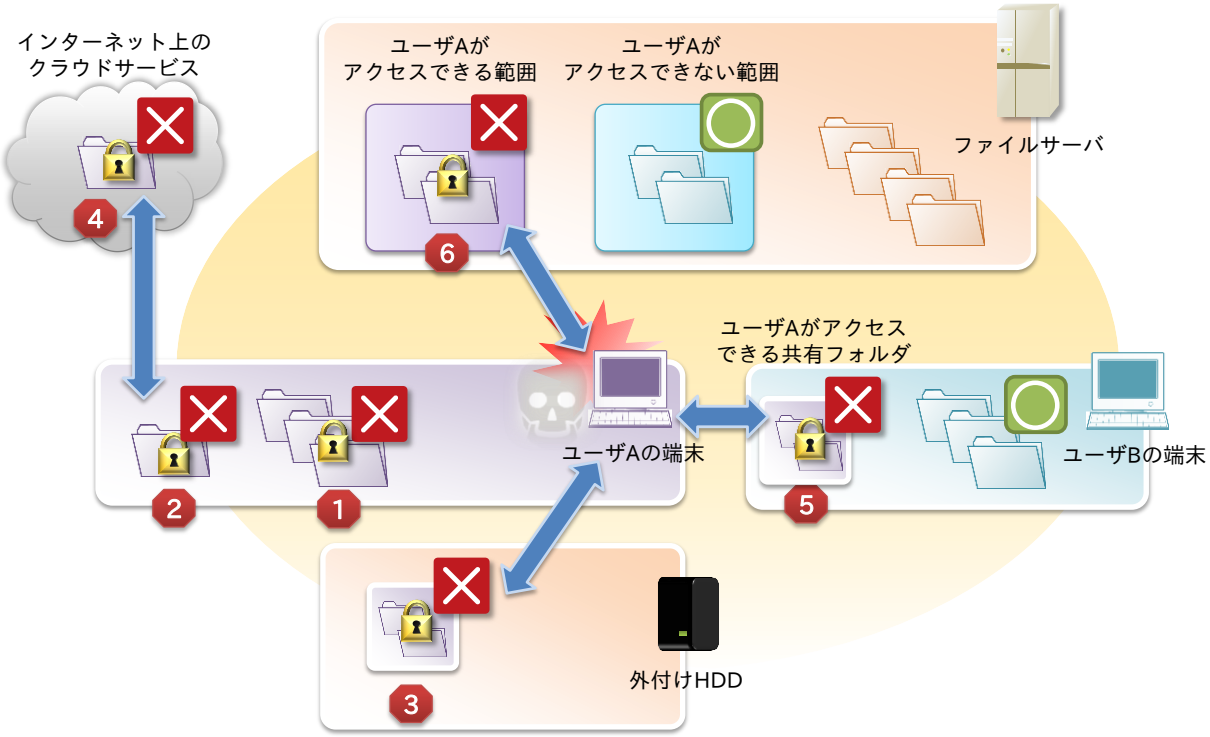

図 1-4-1：ファイル暗号化型のランサムウェア感染時の影響範囲

① 感染端末内に保存されているファイル

② 感染端末内のクラウドと同期するフォルダ内のファイル（①に含まれる）

③ 感染端末に接続されている外付け HDD 内に保存されているファイル

④ ②を同期することによるクラウド内のファイル（上書き）

⑤ 他の端末上の感染端末（ユーザ A）と共有しているフォルダ内のファイル

⑥ ファイルサーバ上で感染端末（ユーザ A）がアクセスできる（書き込み権限がある）領域に保存されているファイル

このように、ファイル暗号化型のランサムウェアに感染したパソコンの環境によっては、被害は当該パソコンだけに留まらない。そのため、組織内のパソコン 1 台だけが感染した場合であっても、ファイルサーバ上のファイルも暗号化されてしまうことで、組織の運営に致命的な影響を与えることも考えられる。

1.5. 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他の不正プログラム同様、主にメールに添付されたファイルを開くことによる感染と特定の条件下でウェブサイトを閲覧したことによる感染とがある。

■メールに添付されたファイルを開くことによる感染

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。

■特定の条件下でウェブサイトを閲覧したことによる感染

脆弱性があるソフトウェアがインストールされたパソコンから、ランサムウェアの感染を狙って改ざんされたウェブサイトにアクセスするとドライブ・バイ・ダウンロード攻撃によって感染する。また、ウェブサイトではなく、ウェブサイトに掲載されている広告が攻撃者によって細工されている場合もある。

2. IPA に寄せられたランサムウェアの感染事例

IPA の情報セキュリティ安心相談窓口へのランサムウェアに関する相談が、2016 年 1 月に 11 件、2 月に 17 件寄せられていたが、3 月には 96 件と急増した。この時期に多く感染が確認されたランサムウェアは「Locky」である。

2.1. ランサムウェア Locky の感染事例

2016 年 3 月に IPA に寄せられたランサムウェアに関する相談の多くは、「受信したメールの添付ファイルを開いてしまったことでファイルが暗号化された」というものであった。状況を確認すると、パソコン内のファイルが暗号化されて開けない状態となり、ファイルの拡張子が「.locky」に変更されていた。そしてパソコンの画面上に、ランサムウェアによって金銭を要求する画面が表示されていた。

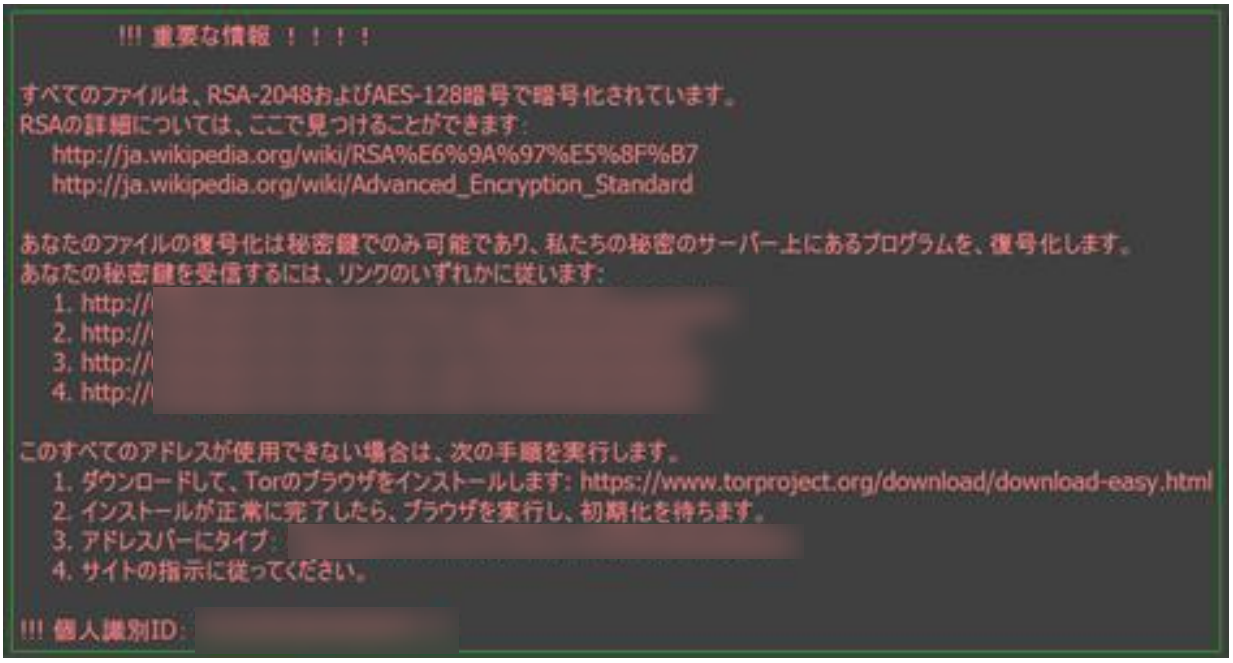

図 2-1-1：Locky の金銭要求画面

同時期にランサムウェア感染が目的と考えられる「ばらまき型メール[2]」の相談と情報提供も寄せられたことから、ばらまき型メールによって「Locky」が不特定多数にばらまかれたものと考えられる。

[2] 【注意喚起】ランサムウェア感染を狙った攻撃に注意
https://www.ipa.go.jp/security/topics/alert280413.html

3. ファイル暗号化型ランサムウェアへの対策

ここでは、ファイル暗号化型のランサムウェアの被害を防止または軽減させるための主な対策について紹介する。紹介する対策はすべて実施すれば良いというものではなく、普段利用しているパソコンの環境によって想定されるリスクが異なるため、実施する対策のメリット、デメリットなども考慮した上で、適切な対策を選択、実施する必要がある。

3.1. ランサムウェアに感染しないための対策

ランサムウェアはその他のウイルス同様で不正プログラムの一種である。そのため、ランサムウェアに感染しないために以下の対策が有効である。

■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する。

■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する。

■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ウイルスに感染する可能性がある。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メール、文面の意味が分からないメールなどは、安易に開かないことが重要である。

最近では、メール送信者情報として実在する企業を騙ったり、メール本文も当該企業が送信するメールを模倣したりするケースが多く確認されており、不特定多数の人物にメールを開かせる手口が巧妙になっている[3]。メールの添付ファイルを開くことは極力避け、どうしても開く必要がある場合は、万が一ウイルスに感染しても影響がない環境を用意した上で開くことが望ましい。

[3] 「ウイルス感染を目的としたばらまき型メールに引き続き警戒を」
https://www.ipa.go.jp/security/txt/2015/12outline.html

3.2. ランサムウェアの感染に備えた対策

ランサムウェアに感染しないための対策を実施していても、100%被害を防げるとは限らない。そのため、万が一ランサムウェアに感染してしまった場合でも、その被害を最小限に留める準備をしておくことも重要である。

特に現在主流となっているファイル暗号化型のランサムウェアに感染した場合、暗号化されたファイルの復号は困難である。そのため、失った場合の影響が大きい（重要な）ファイルについては、バックアップを取得しておく必要がある。バックアップを取得しておけば、万が一ランサムウェアに感染してファイルが暗号化されてしまっても、バックアップしたファイルからリストアすることが可能となる。

図 3-2-1：重要なデータはバックアップを

なお、バックアップをいつ、どのような方法で取得するかは、対象ファイルの更新頻度やバックアップに使用する装置・媒体の特性に応じて検討する必要がある。特に企業においてはシステム環境が複雑になることが多いため、１．４で記載した影響範囲を元にリスク分析を行い、環境に適したバックアップ方式や頻度、管理方法などを検討してほしい。

3.3. バックアップに使用する装置・媒体

バックアップ対象となるファイルの特性に応じた、使用するバックアップ装置・媒体の例を表 3-3-1 に示す。

表 3-3-1：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

3.4. バックアップにおける留意事項

ランサムウェアの影響は感染端末（ユーザ）のアクセス可能な場所に及ぶため、バックアップ装置・媒体として外付け HDD や USB メモリなどを端末に常時接続していると、バックアップしたファイルも暗号化の対象となる。そのため、以下のような点に留意する必要がある。

■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

外付け HDD や USB メモリは、パソコンに接続していない状態であればランサムウェアの影響は及ばないため、バックアップ時のみ接続することが望まれる。なお、光学メディアなど一度データを書き込んだ後はその書き換えができないタイプの媒体であれば、パソコンに接続していても（メディアが挿入された状態でも）問題はない。

■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

バックアップに使用する装置・媒体をバックアップ時のみパソコンと接続するようにしていても、バックアップ中にランサムウェアに感染しないとも限らない。そのため、複数の装置・媒体でバックアップを取得しておくことやバックアップ中はそれ以外の操作を行わないといった対策も望まれる。なお、複数のバックアップ装置・媒体でバックアップを取得しておくと、ランサムウェアに限らずバックアップ装置・媒体の故障や不具合などが発生した場合にも対応が可能となる。

■バックアップ方式の妥当性を定期的に確認する

ファイルのバックアップを取得したとしても、有事の際にそのバックアップからリストアできなければ意味がない。また、ランサムウェアのファイル暗号化の機能・仕様なども変化しうる可能性があるため、問題なくリストアができるか、現状のバックアップ方式でリスクに耐えることができるかなどを定期的に確認、検討することも重要である。

おわりに

本書では、IPA の安心相談窓口に寄せられたランサムウェアの相談などから、現在主流となっているファイル暗号化型のランサムウェアについて概要や対策を解説した。

ファイル暗号化型のランサムウェアによる被害の影響度は暗号化されてしまうファイルの重要度に依存するため、場合によっては要求された金額を支払う方が、総被害額が少なくなるといったケースも想定される。このあたりが、ランサムウェアが流行している背景の一端であると考えられる。

ウイルス対策を実施していても、ランサムウェアの感染を 100%防ぐことは難しい。しかし、重要なファイルは適切にバックアップを取得、管理しておくことで、万が一のランサムウェアによる被害の影響度を低減できる。また、バックアップの取得はランサムウェアによる被害に限らず、意図しないハードウェア故障や不具合、システム障害などの予期せぬトラブルによりファイルが消失してしまった際の対策にもなる。

本書が、個人および企業において、より安全なパソコンの利用やシステム環境の構築・運用を行う上での一助となることを願う。

付録

IPA の情報セキュリティ安心相談窓口に寄せられた相談の中には、Android 端末で動作する端末ロック型のランサムウェアの被害も確認されている。その概要を以下に紹介する。

Android 端末のランサムウェアの被害事例

このランサムウェアは端末ロック型であり、具体的な症状としては Android 端末上に以下のような画面が表示されて通常の操作ができなくなる。この解除のために金銭の支払い（実際には iTunes カードのコード）を要求するというものである。

図 4-1-1：Android 端末のランサムウェアで表示されるロック画面（出典）愛知県警察「Android 版スマートフォン用身代金要求型ウイルス（ランサムウェア）について[4]」を元に IPA が抜粋

復旧方法

Android 端末では、ランサムウェアはアプリとして端末にインストールされる。そのため、当該アプリを端末からアンインストールすることで復旧することが可能である。ただし、端末がロ

[4] 「Android 版スマートフォン用身代金要求型ウイルス（ランサムウェア）について」
http://www.pref.aichi.jp/police/anzen/cyber/1news/documents/capture_1.pdf

ックされているため、通常はアプリのアンインストールの操作ができない状態となっている。これについては端末をセーフモード[5]で起動できれば、操作可能な状態で起動することができる。セーフモードでの起動可否・方法やアプリのアンインストール操作方法の詳細は、利用している端末によって異なる。愛知県警察のウェブサイト上にて当該アプリのアンインストール方法の例が公開[6]されているので、参考にしてほしい。ここで挙げられている例では当該ランサムウェアは「System Update」という名称に偽装されてインストールされている。万が一アンインストールすべきアプリの判断が難しい場合は、端末を初期化することでも復旧できる。

[5] セーフモード：端末診断用の起動モード。最小限のアプリのみの状態で端末が起動する。

[6] 「Android 版ランサムウェアのアンインストール手法」
http://www.pref.aichi.jp/police/anzen/cyber/1news/documents/uninstall_1.pdf

IPA テクニカルウォッチ

「ランサムウェアの脅威と対策」

～ランサムウェアによる被害を低減するために～

[発　　行]　2017 年 1 月 23 日
[著作・制作]　独立行政法人情報処理推進機構 技術本部 セキュリティセンター
[執　筆　者]　黒谷 欣史　野澤 裕一