

ランサムウェアの脅威動向および被害実態調査報告書

1.0 版

一般社団法人 JPCERT コーディネーションセンター
2018 年 7 月 30 日

はじめに	3
1. ランサムウェアの脅威	5
1.1. ランサムウェアとは	5
1.2. ランサムウェアの感染経路.....	5
1.3. 攻撃手口の変化と国内への影響.....	8
1.3.1. 身元を明かさず身代金を受け取るためのサービスの普及	9
1.3.2. 高度化するランサムウェアの攻撃手口	10
1.3.3. 言語の壁を超えたランサムウェア	11
1.4. 攻撃ベクトルの変化	12
2. ランサムウェア被害実態調査	13
2.1. 調査概要.....	13
2.2. 結果概要.....	13
2.3. 組織の規模	14
2.4. インシデント発生状況.....	14
2.5. ランサムウェアの被害状況.....	15
2.5.1. ランサムウェアの被害件数	15
2.5.2. 感染したランサムウェアの種別、感染時期	16
2.5.3. 被害者の属性	17
2.5.4. ランサムウェアの感染原因	17
2.5.5. ランサムウェアの被害にあった際の影響、被害にあった機器	18
2.5.6. 被害にあった際の対処法.....	19
2.5.7. 感染時に攻撃者から要求された金額.....	20
2.5.8. 通常の業務稼働が復旧するまでにかかった時間	21
2.6. 予防対策の実施状況	22
2.6.1. サイバーセキュリティおよびランサムウェアに関する意識啓発、トレーニング	22
2.6.2. 予防措置	23
2.6.3. 懸念されるインシデント.....	23
2.7. 「No More Ransom」プロジェクトについて.....	24
3. 調査結果に対する考察	25
おわりに	29
付録 A. ランサムウェアの種類一覧	30

はじめに

ランサムウェアの起源は 1989 年に遡るが、数多くの種類のランサムウェアが出現するようになったのは 2012 年前後からである。そして近年では、脅迫文の多言語化、攻撃者が匿名のまま身代金を回収するためのサービスや技術の普及、攻撃に関連する活動の分業化とそれに伴う専門性の深化などを背景に、ランサムウェアの脅威が世界各地に広まっている。特に 2015 年以降は、海外で確認された各種ランサムウェアが、ほぼ同時期に日本国内でも確認されるようになっており、国内においても感染リスクが高まっている。

ランサムウェアの感染経路が、スパムメールや改ざんされた Web サイトであることは従来からよく知られており、そうした感染事例は依然として多い。しかし 2017 年には、「WannaCry (WannaCrypt)」のような自己伝染機能を持つランサムウェアが出現し、世界各地で急速に感染を拡大させるなど、感染手口が多様化していると言える。さらに、ランサムウェアを用いてターゲットのシステムを破壊する事例や、標的型攻撃の痕跡調査をかく乱するために用いるなどの特殊な事例も確認されており、ランサムウェアを用いた攻撃の意図が拡大し、新たな脅威となっている。国内において、このような新たなタイプのランサムウェアの確認された被害はまだ多くないが、これまでのランサムウェアに対する予防対策や事後の措置に加え、今後は感染経路や原因を追究できる体制や仕組みを整える必要があると考えられる。

こうした問題意識から、ランサムウェアの感染経路や感染リスクが拡大している背景、脅威動向の変遷について公開情報をもとに調査し、その結果を踏まえて、国内の法人組織の被害実態を明らかにするためのランサムウェアに関するアンケート調査を実施した。

本報告書は次の 3 つの部分から構成されている。

第 1 章では、インターネット上に公開されている情報をもとにした、ランサムウェアの感染経路や国内における感染リスク拡大の背景、脅威動向などについての調査結果を述べる。

第 2 章では、国内の重要インフラ関連の組織に対して行ったランサムウェアの被害実態に関するアンケート調査の集計結果を、質問項目ごとに掲げる。

第 3 章では、アンケート調査結果から見られた傾向の分析や考察、さらには、感染を予防するための対策や、感染時の被害を最小化するための対策について述べる。

また、「付録 A」には、国内でも特に影響が確認された、もしくは世界的に注目されたランサムウェアの種類について、脅威概要や復号ツールの有無などの情報を一覧形式にまとめた。

本報告書が、国内の法人組織におけるランサムウェアの被害実態を理解するための一助となり、対策を推進する手引きとして活用されることを願いたい。

本書の想定読者

本報告書は、次のような方々を主な読者として想定している。

- ・個人および法人組織で、パソコンを用いて Web 閲覧やメールを使用するユーザ
- ・法人組織のシステム管理者

改訂履歴

版数	発行日	改訂内容
第1版	2018年7月30日	初版発行

1. ランサムウェアの脅威

1.1. ランサムウェアとは

ランサムウェアはマルウェアの一種であり、ランサムウェアに感染したコンピュータシステムは、動作が妨害される、あるいはデータが暗号化されて使用できない状態になる。ランサムウェアの「ランサム」という言葉は身代金を意味しており、被害者に脅迫文が送り付けられ、「データやシステムを元に戻して欲しければ金を出せ」と要求する。

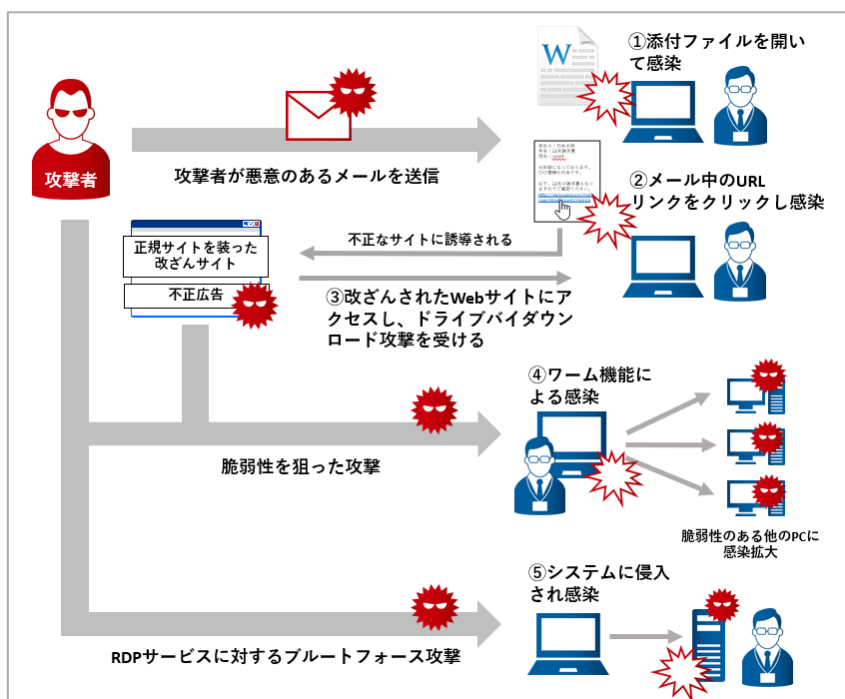
ランサムウェアは、ファイルを暗号化する「ファイル暗号化型」と、デバイスの操作ができないようにロックをかける「デバイスロック型」の2種類に大別できる。以前は伝染性がないとされていたが、最近では「WannaCry (WannaCrypt)」に見られるように、隣接する他のデバイスやシステムに感染を拡大するものもある。「NotPetya」に見られるように、システムを破壊し元の状態には戻せないようにするものもある。

ランサムウェアの要求に応じて身代金を支払ったとしても、被害にあったデータやシステムが元通りになる保証はない。すなわち、身代金を取られた上に、データやシステム機能も失ったままの二重の被害となる可能性もある。

1.2. ランサムウェアの感染経路

ランサムウェアに感染するシナリオとして、次のようなケースがある。

- ① 攻撃者から送り付けられたメールの添付ファイルを開く
- ② 攻撃者から送り付けられたメール本文中に記載されている URL リンクをクリックする
- ③ 改ざんされた Web サイトにアクセスしてドライブバイダウンロード攻撃を受ける
- ④ 脆弱性などを悪用する自己伝染機能をもったランサムウェアに感染する
- ⑤ リモートデスクトップ機能を通じて侵入され感染させられる



[図 1-1 ランサムウェアの感染経路の例]

ランサムウェアへの感染を防ぐためには、[図 1-1] に示すような感染経路やその背景を理解することが重要である。スパムメールや 익스프로イトキットを介する典型的な感染経路以外にも、広告を悪用したマルバタイジングや脆弱性を悪用する手口など様々な感染経路がある。次に、それぞれの感染経路を詳細に説明する。

— スパムメール

ランサムウェアを拡散するために用いられている最も一般的な手法はスパムメールである。かつて、ランサムウェアの拡散は日本でも主に英語メールによってなされ、不特定多数を狙う世界的なばらまき型のスパムメールが、日本国内にも届いたケースが多かった。しかし、2016年4月の「Ransom_CRYPTSHED」の事例¹以降、日本語のスパムメールも確認されるようになり、攻撃者が意図的に日本を標的とし始めた変化がみられた。スパムメールには、不正なマクロが仕込まれた Microsoft の文書ファイル(拡張子は.doc)が添付されているケースが多かったが、2016年10月頃からは、Windows Script Files (WSF) 形式のファイルを添付したケース等、攻撃の手口の変化が確認されている²。

— 익스프로イトキット

ランサムウェアを拡散する手法のもう一つの典型的な例が 익스프로イトキットの利用である。 익스프로イトキットには、Adobe Flash Player、Internet Explorer (IE)、Adobe Acrobat、Adobe Reader などの様々な脆弱性を悪用するコードが含まれている。攻撃者は、アンダーグラウンドマーケット等で攻撃用 Web サイトを購入またはレンタルし、そこに 익스프로イトキットを設置する。Web サイトを改ざんして、そこを介して攻撃用サイトにアクセスするようユーザを誘導し、ユーザの端末でマルウェアを含む不正なコードを実行させようとする。2015年以降の攻撃において最も頻繁に見られる 익스프로イトキットとして「Angler Exploit Kit (Angler EK)」が知られており、2015年に検出された 익스프로イトキットによる攻撃全体のうち 57.25%が Angler EK によるものとされている³。Angler EK は、国内でも流行した CryptoWall や CryptXXX、TeslaCrypt などのランサムウェアファミリの流布に使用されていたことが確認されたが、ロシアでサイバー犯罪者が逮捕された 2016年6月以降は、Angler EK の活動が沈静化した。その後「Nuclear Exploit Kit (Nuclear EK)」や「Magnitude Exploit Kit (Magnitude EK)」などを用いたランサムウェアの拡散が報告されたが、いずれの 익스프로イトキットを用いた活動も 2017年初めには鈍化したことが確認されている⁴。

— マルバタイジング (不正広告)

익스프로イトキットを仕掛けた攻撃用 Web サイトへと誘導する方法は、メール本文に仕掛けられた URL リンクだけではない。広告会社などを通じて細工した広告を出す、または広告サーバに侵入して広告に細工する等の方法によって、オンライン広告を掲載している Web サイトを訪問したユーザをマルウ

¹ 「あなたは新しい請求書 ~ を持っています」日本語メールでのランサムウェア拡散を確認
<http://blog.trendmicro.co.jp/archives/13198>

² Surge of email attacks using malicious WSF attachments
<https://www.symantec.com/connect/blogs/surge-email-attacks-using-malicious-wsf-attachments>

³ 2016年を振り返る：相次ぐ主流 익스프로イトキットの活動停止、減少傾向は続くか
<http://blog.trendmicro.co.jp/archives/14468>

⁴ 2016年を振り返る：相次ぐ主流 익스프로イトキットの活動停止、減少傾向は続くか
<http://blog.trendmicro.co.jp/archives/14468>

エアに感染させる「マルバタイジング⁵」という手口も確認されている。2017年6月には、「Mole」というランサムウェアに感染させるマルバタイジングキャンペーン「AdGholas」の攻撃による被害が海外で確認されており、日本への影響も報告されている。マルバタイジングによる攻撃の場合には、Webサイトを訪問しただけで、それ以上のアクションを何もしなくても、 익스프로イトキット（「AdGholas」の場合には「Astrum Exploit Kit（Astrum EK）」）が仕掛けられた攻撃用Webサイトに誘導され、感染にまで至ってしまう。

一 リモートデスクトッププロトコル（RDP）経由のブルートフォース攻撃

外出先などからパソコンを操作したり、保守業者やシステム管理者による遠隔からの保守を受けたりするためにRDPを有効化している場合がある。攻撃者はこのRDPサービスに対し、あらゆるIDとパスワードを試す「ブルートフォース攻撃（総当たり攻撃）」を実行し、システムへの侵入を試み、システムへのログイン成功後、ランサムウェアを感染させる手口が確認されている。同手口を使用した感染の事例として、2017年2月にはランサムウェア「CRYSIS⁶」が、同年11月にはランサムウェア「LockCrypt⁷」が確認されている。

ダークウェブ・ディープウェブ上のアンダーグラウンドマーケットでは、世界中の脆弱なRDPサーバの認証情報が35,000件以上売られていることが2017年10月に報告されており⁸、攻撃者は認証情報を購入することで、より効率的に標的をランサムウェアに感染させることができるようになっていると考えられる。

一 自己伝染機能をもつランサムウェア

2017年には自己伝染機能をもつマルウェアが登場し、大きな話題となった。2017年5月に世界中で感染が確認された「WannaCry」は、Windows SMB v1の脆弱性「CVE-2017-0144 (MS17-010)」を悪用し、他の脆弱なWindowsシステムに感染を広げるワーム機能を持ったランサムウェアであったことから、短期間に広い範囲で感染が拡大したと言われている⁹。その被害は、わずか数日で、150カ国以上にわたる約30万台のPCが感染するという前例にない被害規模となり、日本においても、大手製造事業者や地方自治体などが感染被害にあったことが報じられた。今年に入ってから、引き続き感染が確認されている。また、同年6月にウクライナや欧州を中心に感染が広まった「NotPetya」や、10月にロシアおよび東欧の各国で広まった「BadRabbit」についても、初期感染の経路は異なるが、感染拡大方法の一つとしてSMBv1の脆弱性が利用されていたことが確認されている。

⁵ AdGholas Malvertising Campaign Using Astrum EK to Deliver Mole Ransomware
<https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware>

⁶ RDP 経由のブルートフォース攻撃を確認、暗号化型ランサムウェア「CRYSIS」を拡散
<http://blog.trendmicro.co.jp/archives/14451>

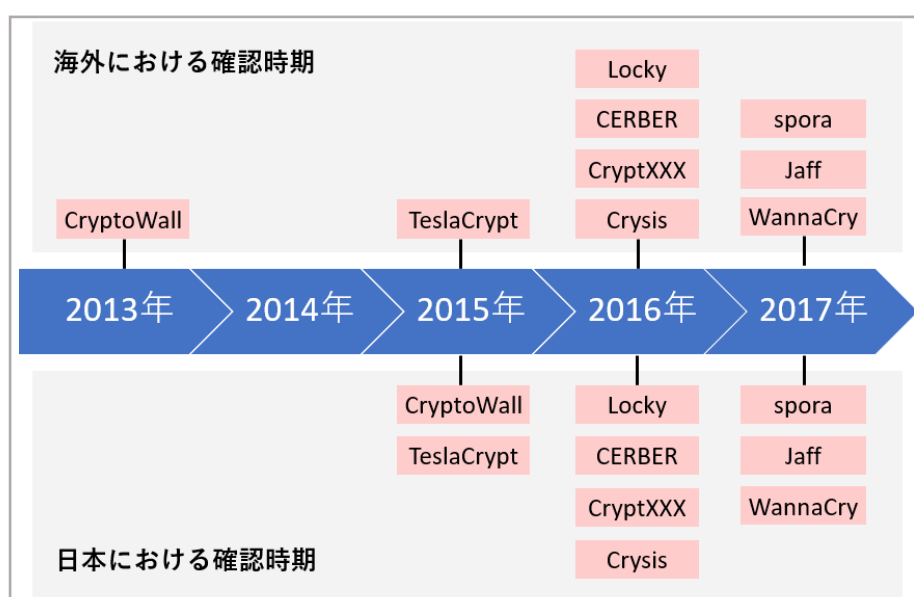
⁷ LockCrypt Ransomware Spreading via RDP Brute-Force Attacks
<https://www.alienvault.com/blogs/labs-research/lockcrypt-ransomware-spreading-via-rdp-brute-force-attacks>

⁸ “Ultimate Anonymity Services” Shop Offers Cybercriminals International RDP
<https://www.flashpoint-intel.com/blog/uas-shop-international-rdp-servers/>

⁹ ランサムウェアの多様化が生んだ「WannaCry」
<https://www.trendmicro.com/content/dam/trendmicro/global/ja/security-intelligence/research-reports/sr/sr-2017h1/2017h1sr0921.pdf>

1.3. 攻撃手口の変化と国内への影響

ランサムウェアの感染報告は、以前は海外のものがほとんどだった。法執行機関や警察を騙った「ポリスランサム」が海外で話題になり始めた 2011 年頃には、脅迫文が日本語に対応していなかったことや、身代金の支払い手段が、Ukash などの日本では利用されていない電子決済システムであったこともあり、「対岸の火事」と見られていた。また、2013 年に登場した「CryptoLocker」の場合には、感染被害の約 3 分の 2 (64%) が米国、次いで英国 (11%)、カナダ (6%)¹⁰とされ、日本国内への影響は確認されなかった。しかし、2014 年以降、この状況が徐々に変化し、日本国内においてもランサムウェアが確認されるようになってきた。[図 1-2] は、海外でランサムウェアが確認された時期と、日本で確認された時期を、インターネット上の公開情報をもとに調査し、両者の対比をまとめた結果である。調査対象としたのは、世界的に注目され国内でも影響が確認された 2013 年以降に登場した 9 種類のマルウェアである。



[図 1-2 各ランサムウェアによる影響が海外と日本国内で確認された時期]

この図からランサムウェアの現状について次の事実が確認できる。

- 2016 年前後からランサムウェアの種類が急増した
- 日本でマルウェアの影響が見られるようになったのは 2015 年以降である
- 2016 年以降は世界各地で確認されたのと同じ時期に日本でも確認されている

上記のようなランサムウェアによる被害状況の変化をもたらしたと考えられる背景を次に述べる。

¹⁰ Defending Against CryptoLocker

<http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-cryptolocker/>

1.3.1. 身元を明かさず身代金を受け取るためのサービスの普及

攻撃者は犯罪を行う上で、身元を隠すためにあらゆる最新技術を用いて匿名化をしており、そのために様々な手法やツールを用いている。従来は、司法当局による捜査の手が届かないように犯罪を行うことが難しかったが、昨今では身代金の集金と被害者との通信について、匿名性の高いツールが利用できるようになった。その中でも代表的なものが「仮想通貨」と「匿名通信システム」の採用である。

— 仮想通貨

ビットコインなどの仮想通貨は、取引するために利用するウォレットの登録に実名のような個人情報を必要とせず、高い匿名性を保った取引ができる。身代金をビットコインで指定された場合、その送金先から攻撃者を特定することが困難である。仮想通貨による身代金送金の要求が初めて確認されたランサムウェアが「CryptoWall¹¹」である。「CryptoWall」に感染すると表示される脅迫画面で、500US ドル（日本円で約 5 万円）相当の金額を仮想通貨ビットコイン（単位 BTC）で支払うよう要求され、支払いが遅れた場合、2 倍の 1,000US ドルへ身代金の金額を引き上げると脅される。「CryptoWall」に起因して支払われた身代金の総額の推定額は 3 億 2500 万ドル（約 400 億円：2015 年 11 月 20 日時点）¹² に達しており、金銭被害として甚大になっている。

「CryptoWall」の例のように、ビットコインなどの仮想通貨を取引に利用することで莫大な利益を得た攻撃者は、ビットコインによる身代金の支払いを要求するランサムウェアの開発を本格化させたと考えられる。そして、昨今では多くのランサムウェアがビットコインによる支払いを要求する仕組みになっている。

— 匿名通信システム

ランサムウェアにおける匿名通信システム「The Onion Router（以下、Tor と記す）」の利用が初めて確認されたのは、2015 年 2 月に出現した「CTB-Locker（Curve Tor Bitcoin Locker の略）¹³」である。Tor が利用されると、捜査機関等がマルウェア検体等を分析しても、それをもとに C&C サーバを特定することが困難で、差し押さえや犯罪活動の追跡が難しくなる。

CryptoWall 3.0¹⁴の場合には、Tor の Web サイトを表示して直接支払いを要求するか、もしくは Tor ブラウザ経由で支払いページにアクセスする方法が記された脅迫状を「メモ帳」で表示する。

¹¹ CryptoWall and HELP_DECRYPT Ransomware Information Guide and FAQ

<https://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information#CryptoWall>

¹² 被害額 3 億 2500 万ドル（約 400 億円）の CryptoWall ランサムウェアの調査結果レポートを共同で発表

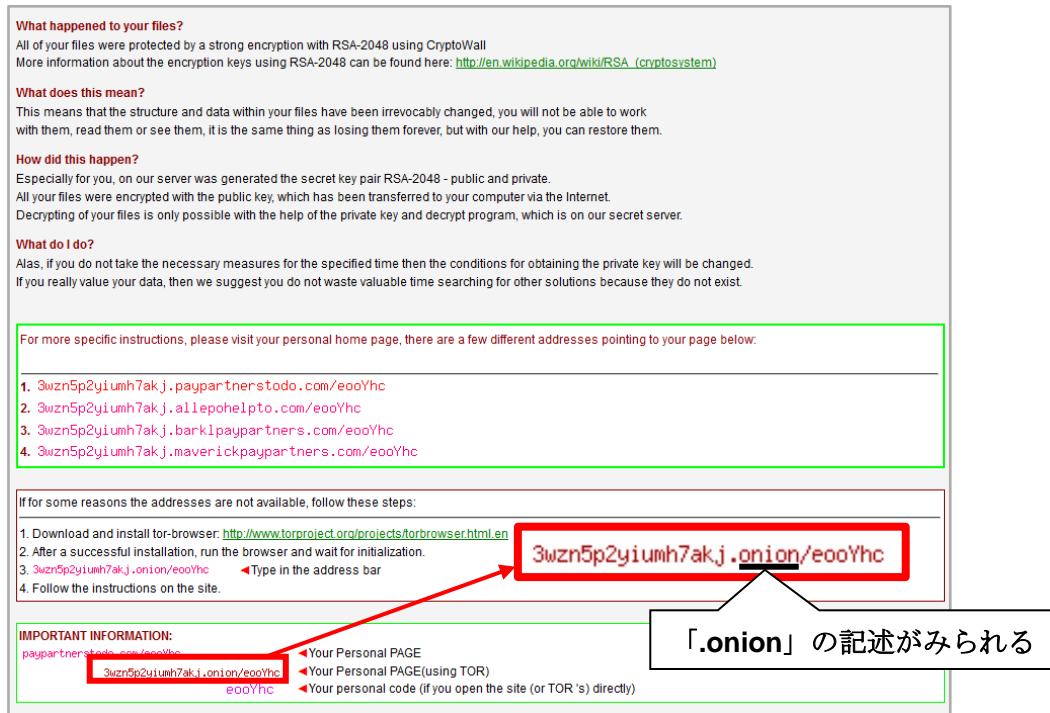
<http://blogs.mcafee.jp/32500400cryptow-a0cb>

¹³ CTB-Locker（Onion ランサムウェア）の亜種が現れる

<https://blog.kaspersky.co.jp/new-version-ctb-locker/6729/>

¹⁴ 情報窃取型不正プログラムと連携するランサムウェア「Cryptowall 3.0」

<http://blog.trendmicro.co.jp/archives/11149>



[図 1-3 Tor ブラウザ経由で支払いページにアクセスする方法が記された脅迫状]

一方、感染したユーザに合成音声で身代金の支払いを促す機能を持つ「CERBER」は、当初は英語の音声のみであったが、後のバージョンでは、被害者に言語を選択させるために、Tor ブラウザ経由でリンクをクリックするよう誘導する仕組みが追加され、日本語も選択できることが確認されている¹⁵。

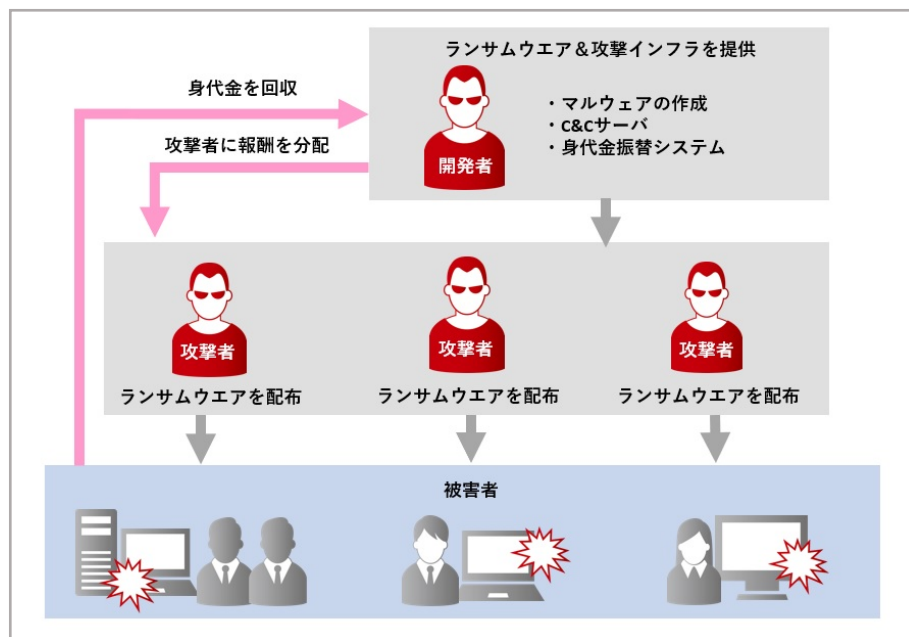
1.3.2. 高度化するランサムウェアの攻撃手口

2つ目の背景として、ランサムウェアに係る攻撃者側業務の分業化とそれに伴う専門化がある。従来はランサムウェアの開発者が自身で攻撃を行い、収益を得ていたが、ファイル暗号化型ランサムウェアが台頭した2013年頃からランサムウェアの需要が高まるとともに、ダークウェブ・ディープウェブ上で RaaS (Ransomware-as-a-Service) と呼ばれるサービスが確認されるようになった。

RaaS とは、ランサムウェアの開発者が、ランサムウェアの作成や管理などを行うためのインフラを、サイバー攻撃者向けに提供するサービスのことである。このサービスにより、ランサムウェアの開発者は、自身の代わりにランサムウェアを拡散してくれる協力者を得て、広い範囲に感染を拡大させ、より多くの収益を見込むことができるようになった。また、サイバー攻撃者はランサムウェアの開発技術や知識を持たずとも、RaaS を活用することによりランサムウェアの配布を行うだけで、開発者が回収した身代金の一部を成功報酬として得ることができる。実際に2015年から2016年にかけて、ランサムウェアのファミリー数を比較してみると、2016年上半期だけでも2015年の全体の2.7倍¹⁶に達しており、大幅に増えていることが分かった。

¹⁵ “話す” 暗号化型ランサムウェア「CERBER」、ロシアのアンダーグラウンド市場で販売
<http://blog.trendmicro.co.jp/archives/12987>

¹⁶ ランサムウェア取引のビジネスモデル「サービスとしてのランサムウェア」
<https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/190/ransomwareasaservice->



[図 1-4 RaaS の仕組みの例]

また、RaaSを活用したランサムウェアの一例として「CERBER」が挙げられる。「CERBER」のキャンペーンによる収益は、2016年7月だけで19万5,000ドルに上り、そのうち開発者の取り分は約7万8,000ドルであったという調査結果がある¹⁷。残りの利益は、各キャンペーンでの感染件数や身代金支払額に応じてランサムウェアを配布した攻撃者に分配されたと考えられている。その他、2016年3月頃に確認されている「Petya」もRaaSとしてダークウェブ上で提供されていたことが確認されている¹⁸。

1.3.3. 言語の壁を超えたランサムウェア

3つ目の背景として、ランサムウェアに伴う脅迫文の多言語化がある。ランサムウェアに感染した際に表示される脅迫文は、以前は英語で書かれたものが多かったが、昨今では様々な言語で表示されるものが存在することが確認されている。2016年に確認された「Locky」は、日本語を含む多言語に対応した脅迫文を表示させることで知られており、日本や米国、オーストラリア、ドイツ、イギリスなど世界中で拡散が確認された。また、同年にロシアのアンダーグラウンド市場で確認された「CERBER」は、日本語を含む12か国語に対応しており、日本を含む世界各地で拡散活動が確認されている。さらに、2017年に世界的に感染が確認された「WannaCry」に関しては28言語に対応している。

これらの例から、多言語化が定着しているとともに、攻撃の手口が変化していることが分かる。利益を上げようとする攻撃者は、攻撃対象をグローバルに広げるために、ランサムウェアを高機能化するとともに、多言語対応する仕組みを最初からランサムウェアに装備するようになっている。そのため、今後はグ

ransomware-operators-find-ways-to-bring-in-business

¹⁷ Ransomware-as-a-Service 「Cerber」の詳細分析
<http://www.checkpoint.co.jp/threat-cloud/2016/08/cerberrring.html>

¹⁸ Petya is being sold as a ransomware as a service offering on the darknet
<https://siliconangle.com/blog/2017/06/27/headline-grabbing-petya-sold-darknet-ransomware-service-offering/>

グローバルに起きている脅威をいち早く検知し、国内においても迅速に対策へつなげることが求められる。

1.4. 攻撃ベクトルの変化

ランサムウェアを用いた攻撃は、これまでは単に金銭の窃取を目的としたものであった。しかし、昨今その攻撃意図に変化がみられており、ターゲットのシステムを破壊するものや、標的型攻撃の痕跡調査をかく乱させるためにランサムウェアを用いたとみられる特殊な事例が確認されている。日本国内で確認されている事例はまだ少ないが、今後このような攻撃が増えていく可能性があり、これまでの単なるランサムウェアに対する予防対策や事後の措置だけでなく、感染経路や原因を追究できる体制や仕組みを整える必要があると考えられる。ここでは、2つの事例について紹介する。

— システム破壊

2017年6月にウクライナと欧州を中心に大規模な攻撃が確認された「NotPetya」は、その被害が甚大であったことから、当時被害が確認されていなかった日本国内においても注意が呼びかけられた。本攻撃で最初に狙われたウクライナでは、チェルノブイリの放射線モニタシステムや地下鉄などのインフラ、電力会社、銀行などの重要インフラに大きな混乱が生じた。その後、欧州へと攻撃が拡大し、多くの企業で感染被害が発生した。「NotPetya」はランサムウェアのように身代金を要求する脅迫画面を表示するが、システム破壊型のマルウェアであり、社会インフラの破壊と混乱を招くことが目的であったと考えられ、新たな脅威となっている。

— 標的型攻撃の痕跡調査のかく乱

ランサムウェアの最近の動向として、もう一つ注目したいのは、標的型攻撃などで攻撃者による侵入の痕跡を隠蔽するためにランサムウェアを使用する新たな事例が確認されたことである。例えば、日本企業への標的型攻撃で使用されていたと考えられているランサムウェア「ONI」は、長期間の侵入の痕跡を消去する目的で使用されていた可能性があることがセキュリティベンダの調査により明らかになっている¹⁹。この調査によると、「ONI」に感染する前の数か月間において標的型攻撃の被害に既に遭っていることが確認されており、攻撃の最終段階に、システム破壊型のマルウェアを使用することで、攻撃者の活動痕跡の追跡を困難にさせていたと考えられる。このように、ランサムウェアの使用用途も多様化しており、単なる金銭を狙った攻撃にとどまらないケースがあるため、それらも考慮して調査を行う必要がある。

¹⁹ NIGHT OF THE DEVIL: RANSOMWARE OR WIPER? A LOOK INTO TARGETED ATTACKS IN JAPAN USING MBR-ONI
<https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan>

2. ランサムウェア被害実態調査

第一章でまとめたランサムウェアの脅威動向を踏まえ、国内組織に協力いただいて、国内における被害実態を把握するためのアンケート調査を実施した。本章には、その集計結果を掲載し、次章で調査結果に対する考察を試みる。本アンケート調査結果を、国内の被害状況や対策傾向の理解と組織における予防策の検討の参考資料として活用いただきたいと考えている。また、調査から得られた発見を、JPCERT/CC がサポーティングパートナーとして参加している No More Ransom の国内における活動や今後提供するサービスの向上に役立てたいと考えている。

2.1. 調査概要

本調査では、ランサムウェアの被害実態を把握することを目的として、国内の重要インフラなどの組織に対し、アンケート調査を実施した。アンケート調査の概要は次のとおりである。

調査方法	アンケート調査
調査対象	国内の重要インフラなどの組織
調査期間	2017年9月19日～2017年10月17日
回答組織数	184組織
調査目的	各組織におけるランサムウェアの被害実態や対策などについて状況を把握するために実施

2.2. 結果概要

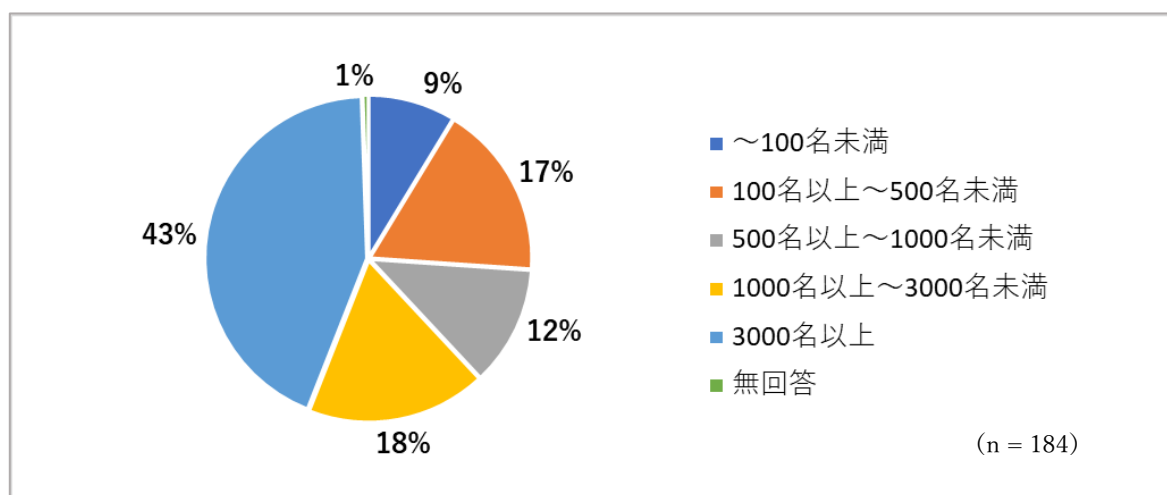
調査を通じて次のことが明らかになった。各項目について掘り下げた議論は「3. 調査結果に対する考察」で行う。

- － ヒアリングの結果、**87%**の組織がサイバーセキュリティ対策の啓発の一環としてランサムウェアへの対策も含んだトレーニングを行っていた。
 - 身代金の支払いは**97%**の組織が行っていない。
 - 感染事例の多くは「Locky (52%)」、「TeslaCrypt (20%)」、「WannaCry (17%)」であった。
- － 感染経路は「Eメールの添付ファイル (66%)」、次いで「ウェブサイトまたはウェブアプリケーション (41%)」であった。
- － 感染してから通常業務が復旧するまでに**36%**の組織が「1週間未満」の時間を要した。
 - 被害状況としては、「データが暗号化された (89%)」、「業務端末が使用不可になった (56%)」などが多かった。
- － 感染予防策として一般的なセキュリティ対策と同様に「アンチウイルスソフトウェア」「ファイアウォール」の導入が行われており、また、クラウドもしくはオンプレミスによる定期的なバックアップの導入の実施が多く行われていた。
 - 既にサイバー保険へ加入している組織は**21%**、検討中が**17%**だった。

2.3. 組織の規模

アンケートの質問項目 1.業種「Q1-1. あなたが所属する企業、組織の業種をお答えください」の集計結果は、非公開としている。

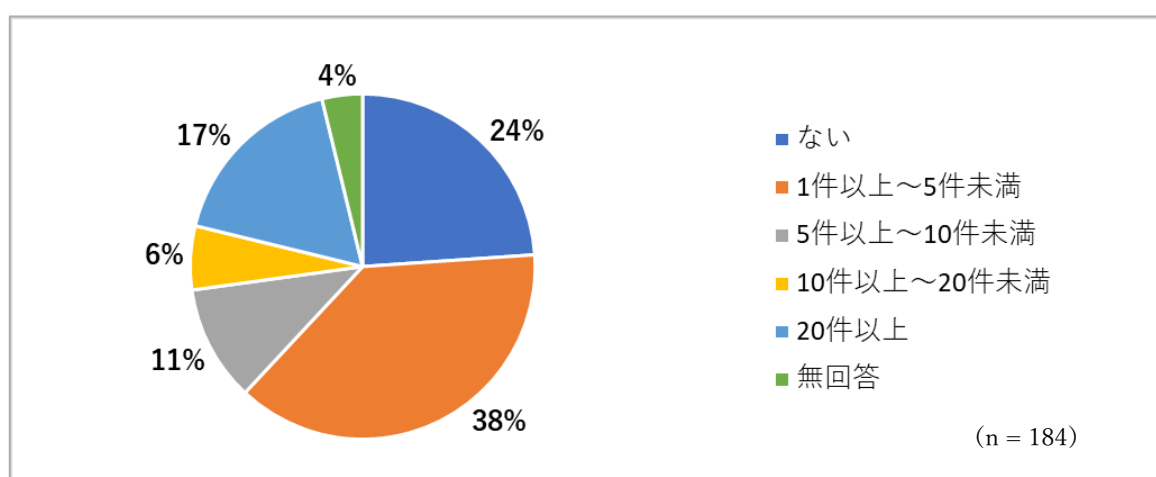
Q1-2. あなたが所属する企業、組織の規模をお答えください。



[図 2-1 回答組織の規模]

2.4. インシデント発生状況

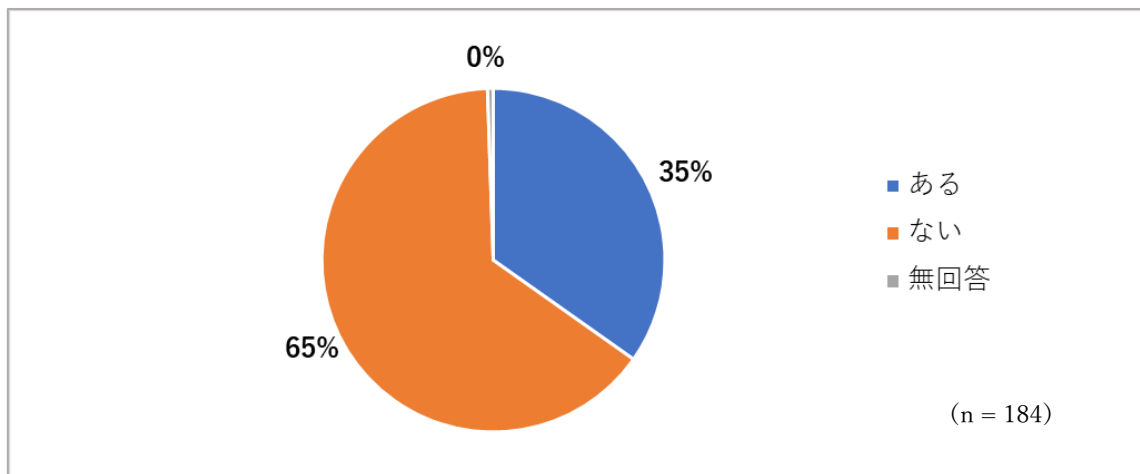
Q2-1. 過去 3 年間でセキュリティインシデントが発生したことはありますか？ある場合、何件発生していますか？



[図 2-2 過去 3 年間のセキュリティインシデント発生有無および件数]

2.5. ランサムウェアの被害状況

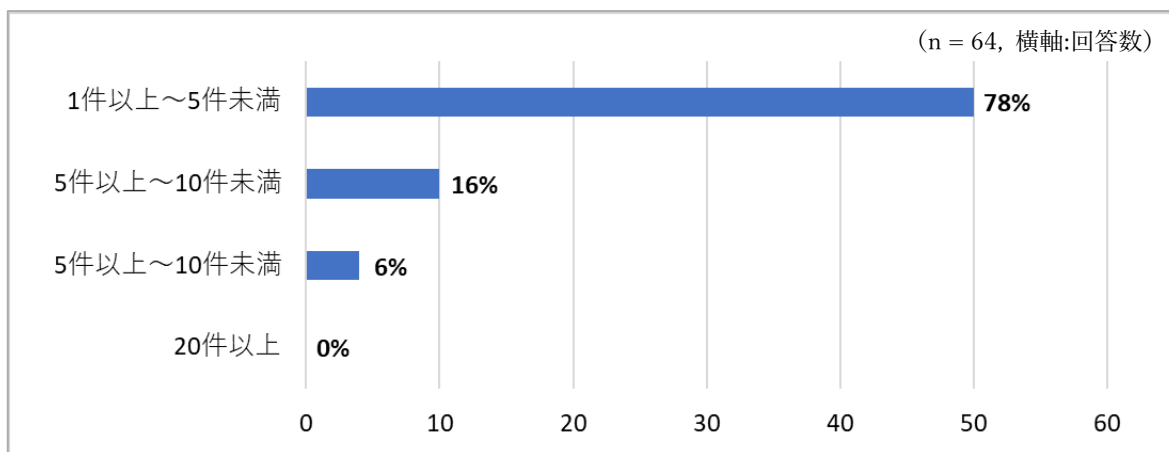
Q2-2. ランサムウェアの被害にあったことはありますか？（「ある」→アンケート項目「Q3-1」に進む、「ない」→「Q4-1。」に進む）



[図 2-3 ランサムウェアの感染被害の有無]

2.5.1. ランサムウェアの被害件数

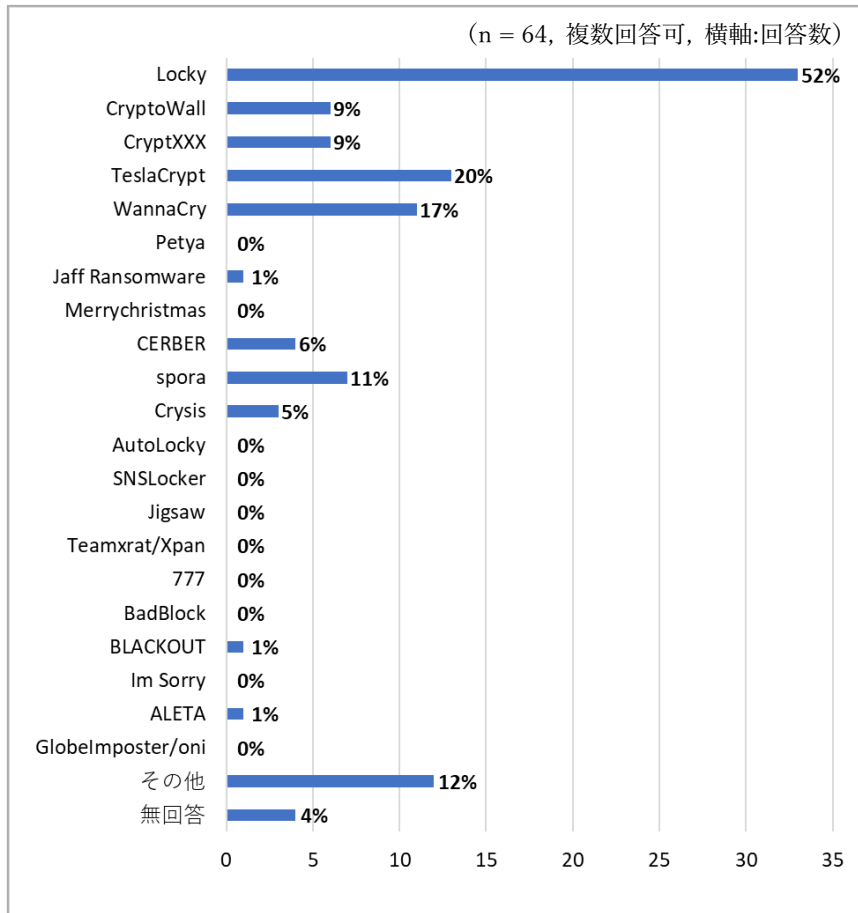
Q3-1. ランサムウェアの被害は何件発生していますか？



[図 2-4 ランサムウェアの被害件数]

2.5.2. 感染したランサムウェアの種別、感染時期

Q3-2. 被害にあったランサムウェアの種別と感染を確認した時期はいつ頃ですか？



[図 2-5 被害にあったランサムウェアの種別]

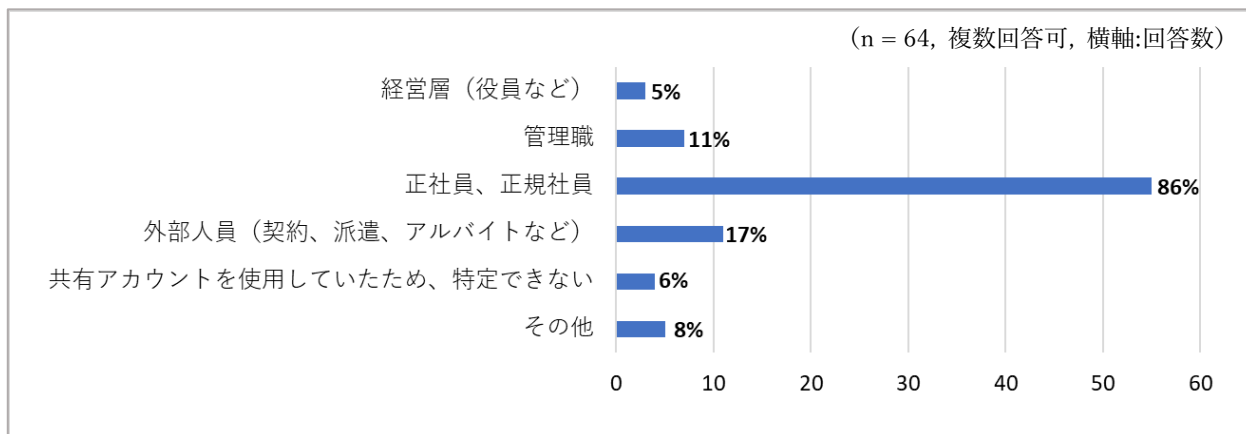
種別	2015年					2016年												2017年								
	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9
Locky																										
CryptoWall																										
CryptXXX																										
TeslaCrypt																										
WannaCry																										
CERBER																										
spora																										
Crysis																										
BLACKOUT																										
ALETA																										

1.赤色：感染時期 2.Jaff Ransomware：感染時期不明のため除く

[図 2-6 ランサムウェアに感染した時期]

2.5.3. 被害者の属性

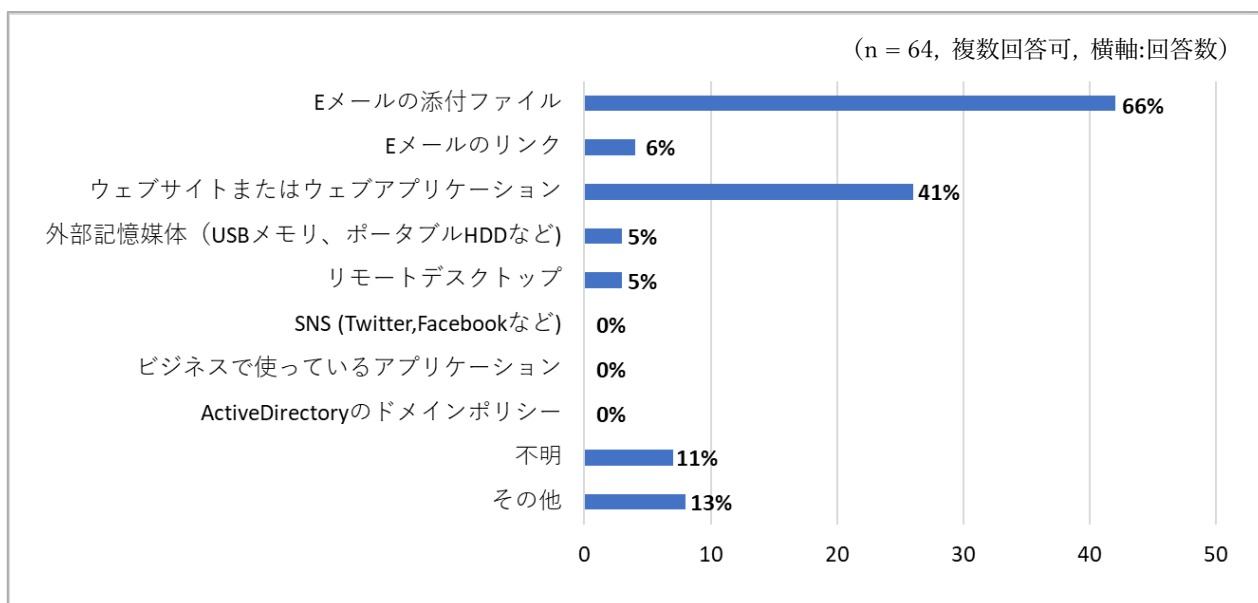
Q3-3. 被害者は誰ですか？



[図 2-7 被害者の属性]

2.5.4. ランサムウェアの感染原因

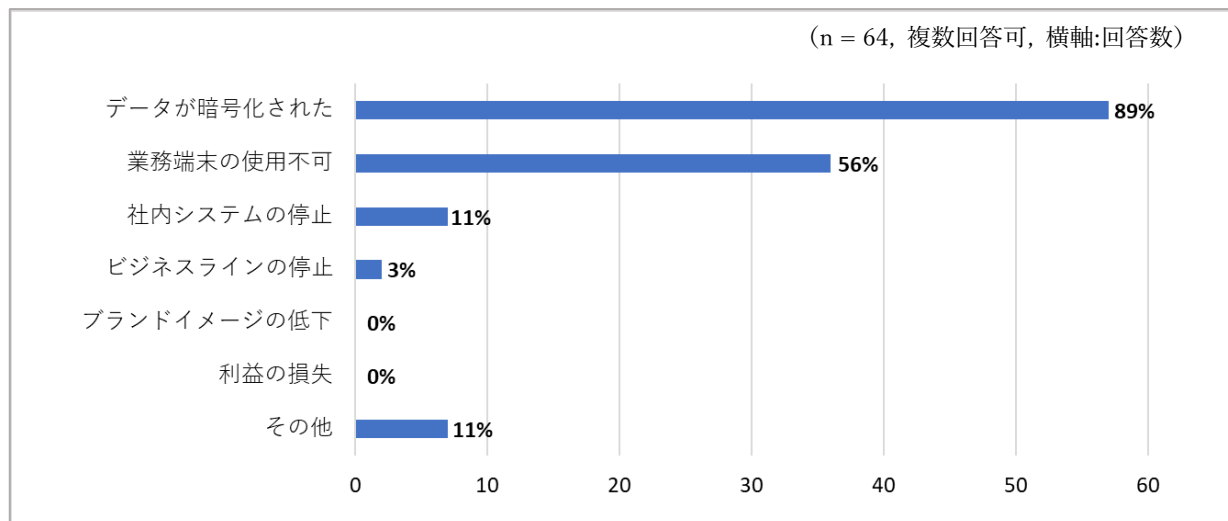
Q3-4. 感染原因は何ですか？



[図 2-8 感染原因]

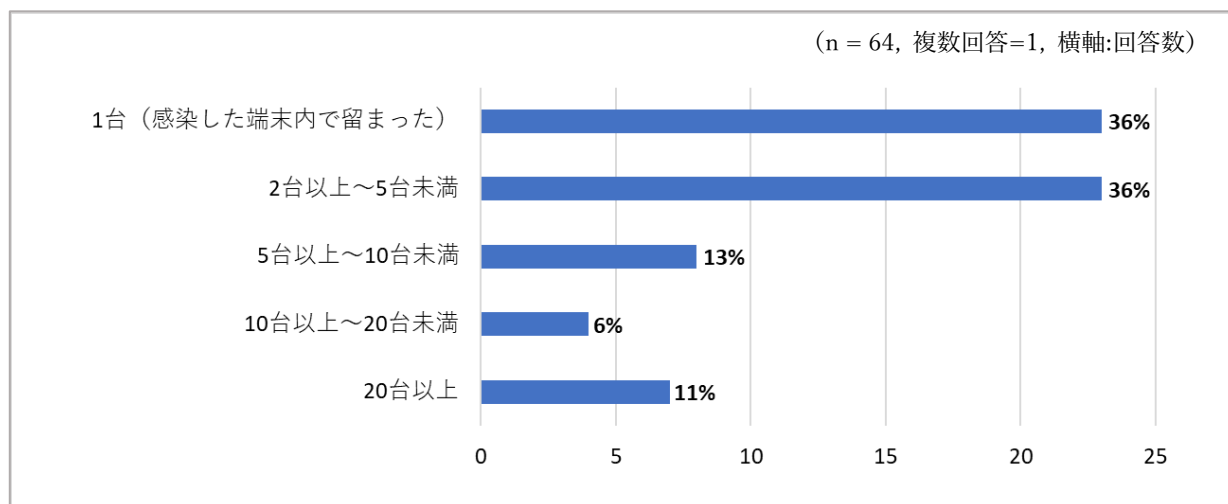
2.5.5. ランサムウェアの被害にあった際の影響、被害にあった機器

Q3-5. 被害にあった際にはどのような影響がありましたか？



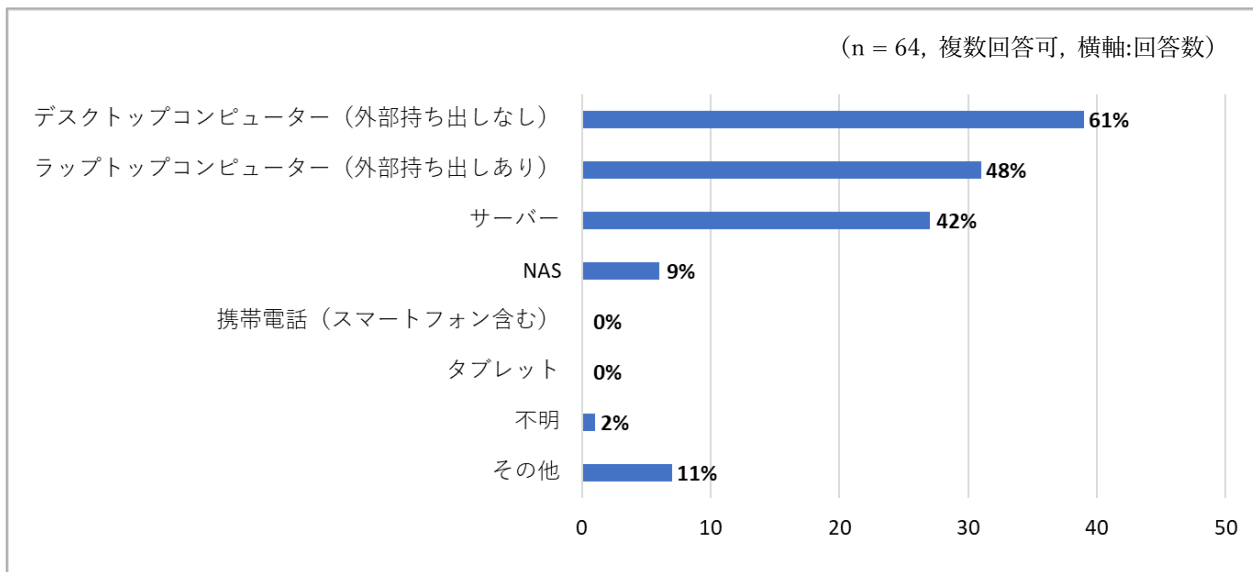
[図 2-9 被害にあった際の影響]

Q3-6. 影響があった機器数は何台ですか？



[図 2-10 被害にあった機器の数]

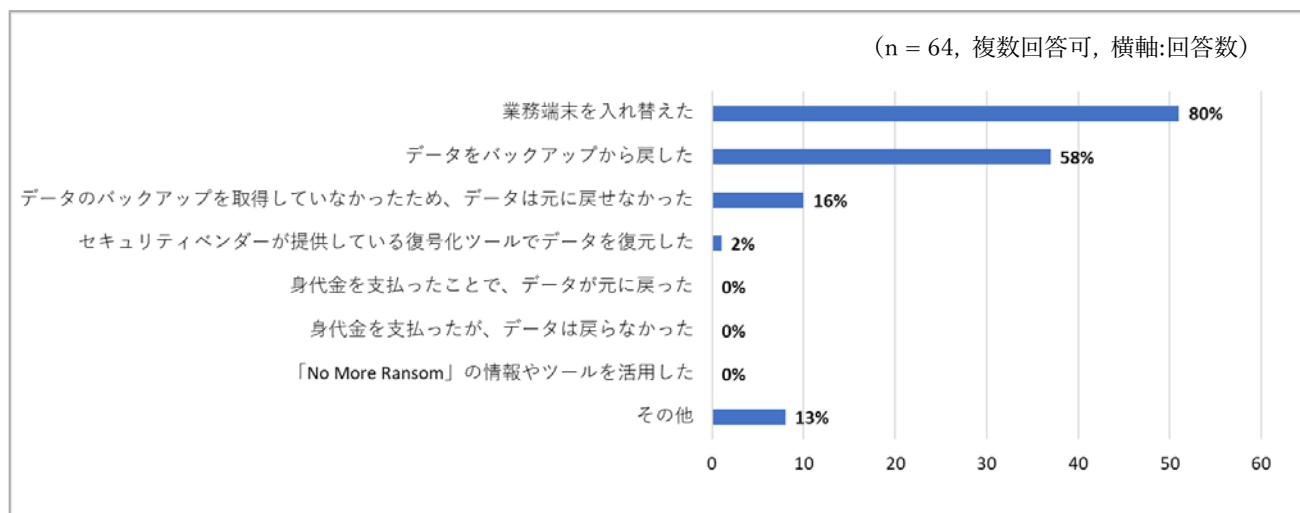
Q3-7. 影響を受けた端末の種別をお答えください。



[図 2-11 影響を受けた端末の種別]

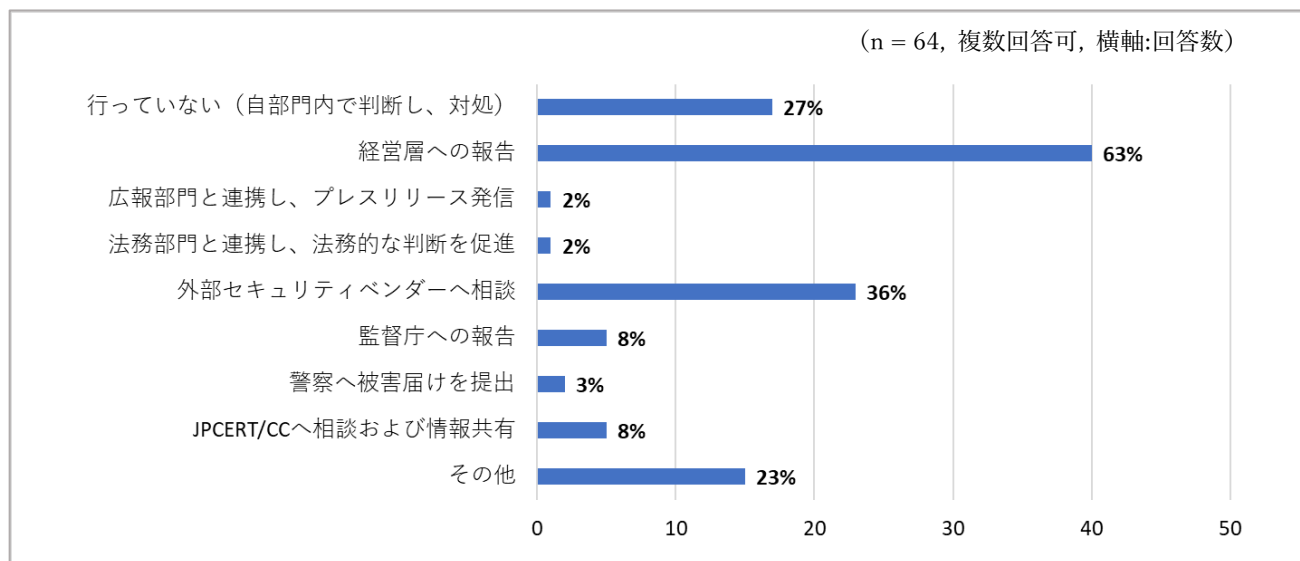
2.5.6. 被害にあった際の対処法

Q3-8. 被害にあった際、どのように対処しましたか？



[図 2-12 被害にあった際の対処法]

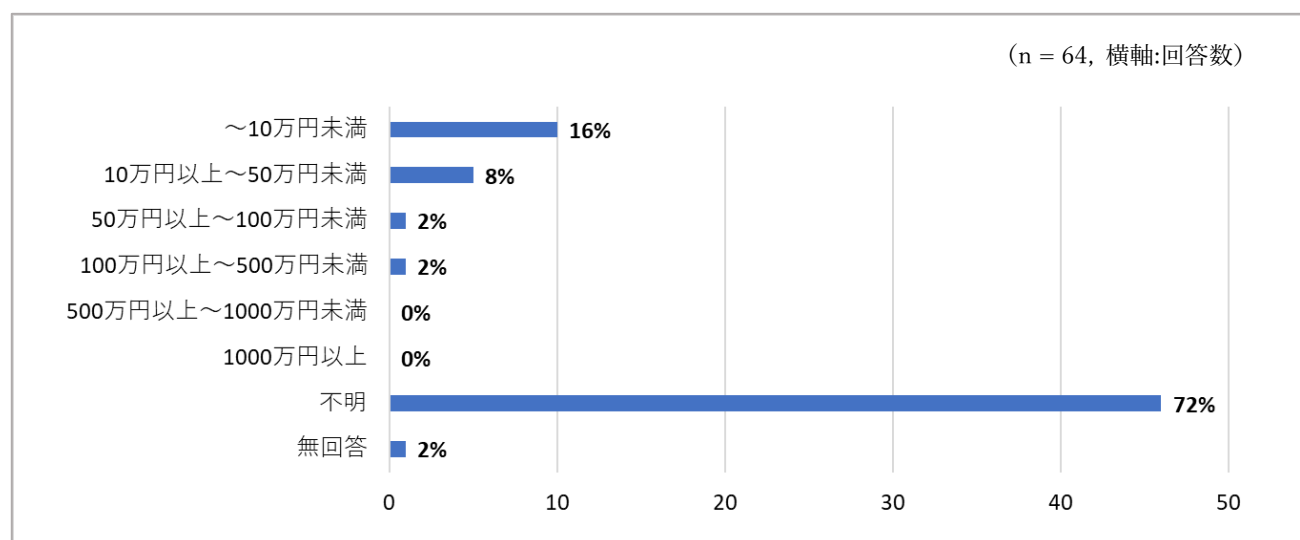
Q3-9. 被害にあった際、解決に向けて他部署・他組織と連携を行いましたか？



[図 2-13 被害にあった際の他部署・他組織との連携]

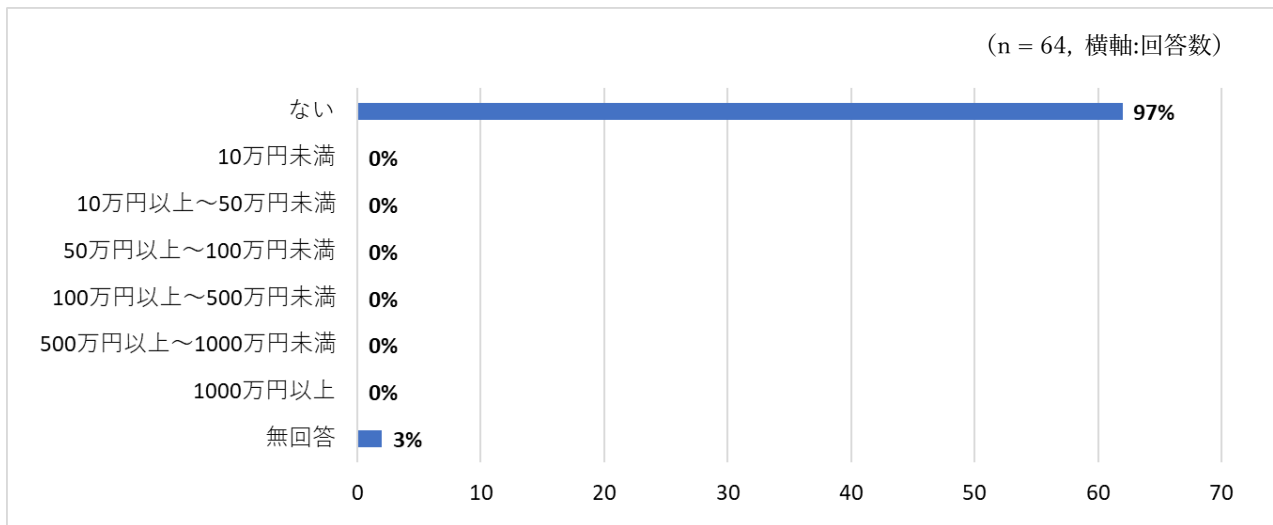
2.5.7. 感染時に攻撃者から要求された金額

Q3-10. 感染時に、攻撃者から要求された金額はおよそいくらですか？ (複数回感染した場合は、合計の金額を選択して下さい)



[図 2-14 感染時に、攻撃者から要求された金額]

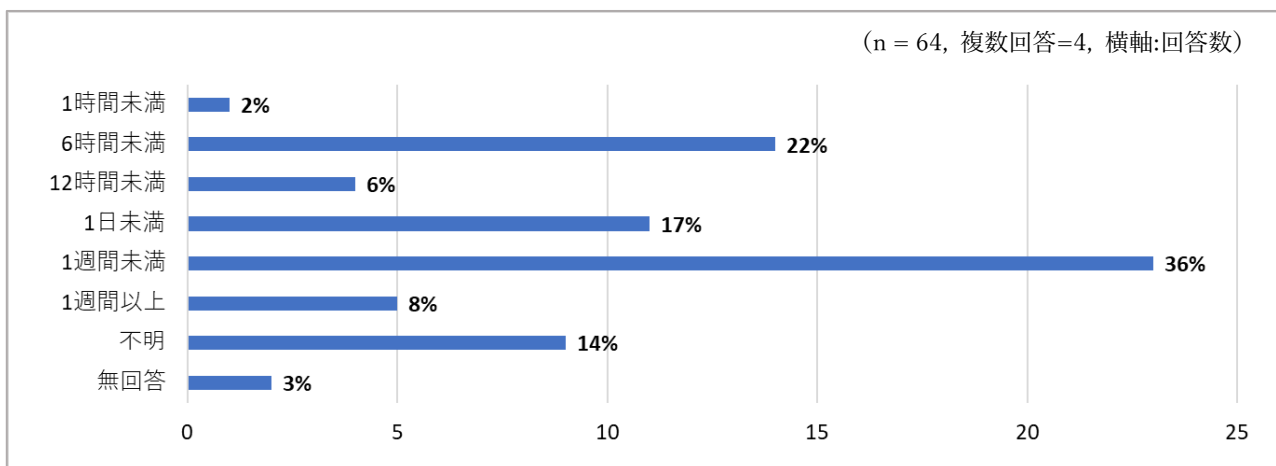
Q3-11. 暗号化されたデータの復旧のために、犯人に身代金を支払ったことがありますか？ある場合、いくら支払いましたか？（複数回ある場合、合計金額をお選びください）



[図 2-15 犯人への身代金支払いの有無およびその金額]

2.5.8. 通常の業務稼働が復旧するまでにかかった時間

Q3-12. ランサムウェアに感染してから、通常の業務稼働が復旧するまでにかかった時間はどのくらいですか？

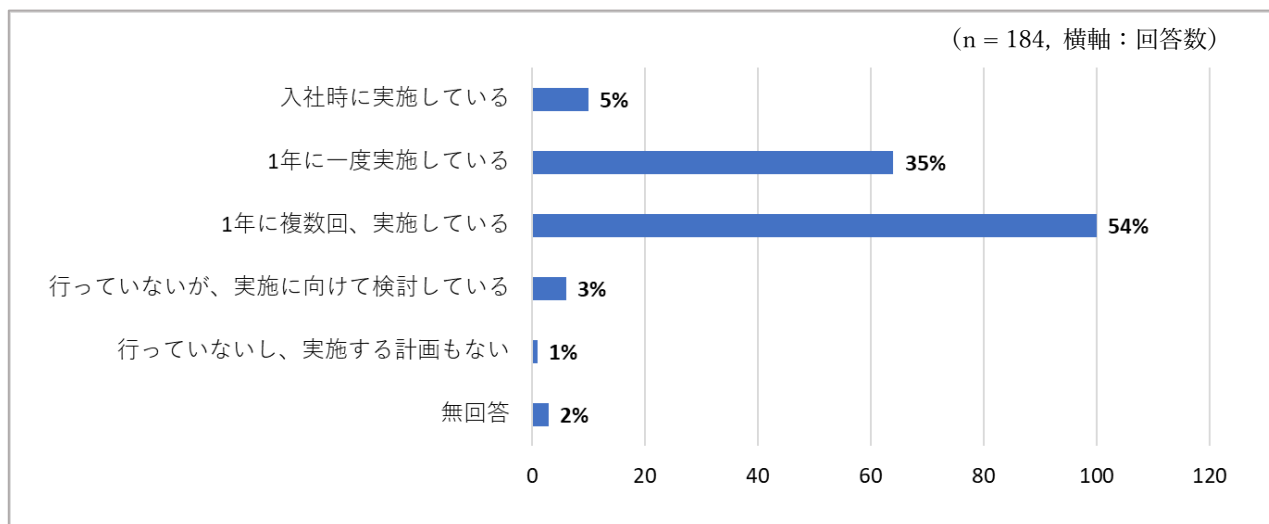


[図 2-16 業務稼働が復旧するまでにかかった時間]

2.6. 予防対策の実施状況

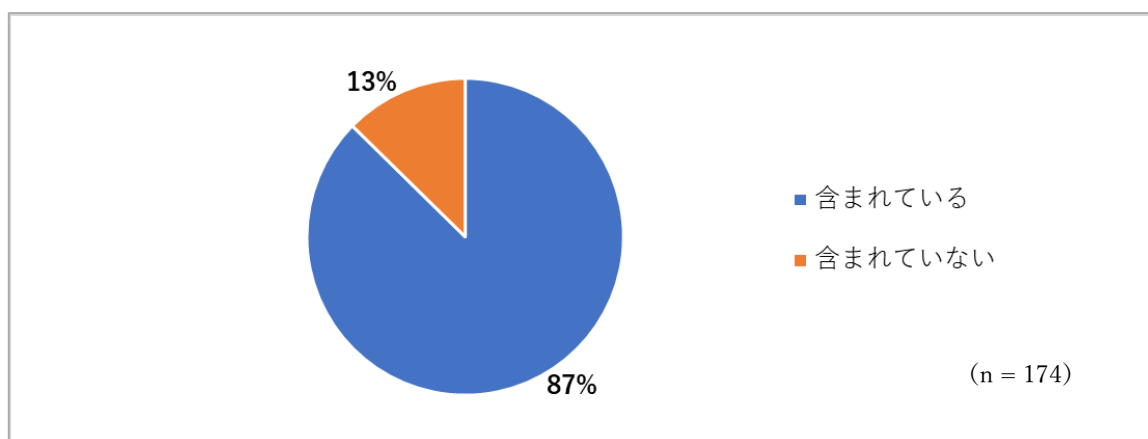
2.6.1. サイバーセキュリティおよびランサムウェアに関する意識啓発、トレーニング

Q4-1. 自組織内でサイバーセキュリティに関する意識啓発やトレーニングを行っていますか？（「実施している」→「Q4-2」に進む、「実施していない」→「Q4-3」に進む）



[図 2-17 自組織内でサイバーセキュリティに関する意識啓発、トレーニングを実施しているか]

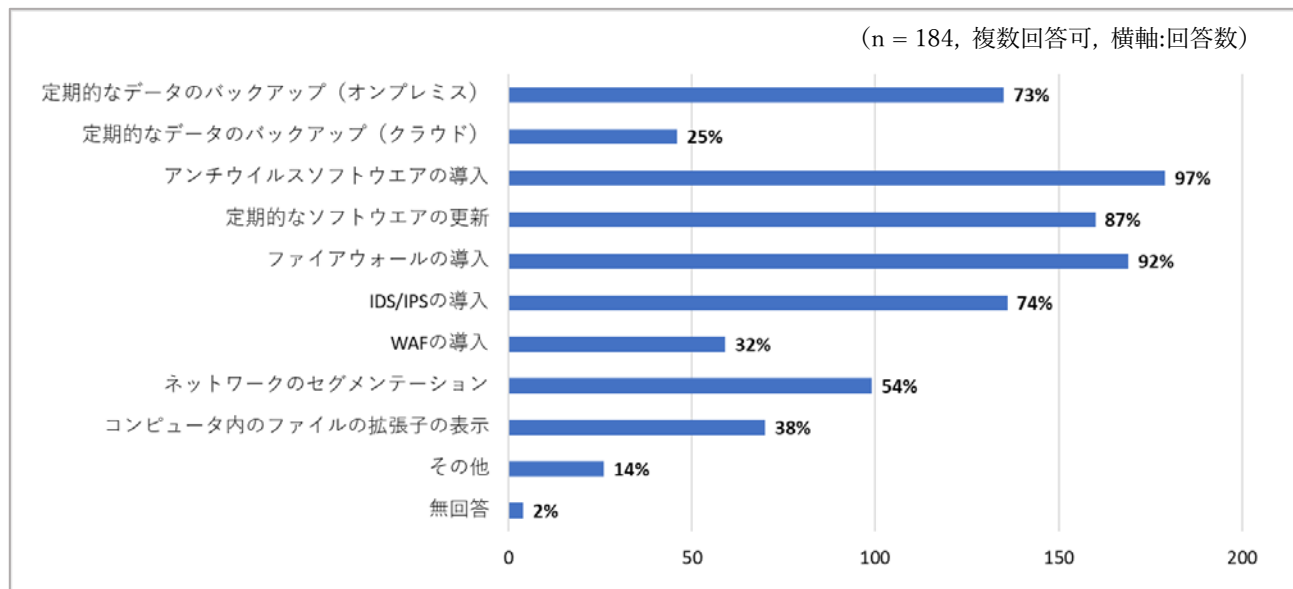
Q4-2. 意識啓発やトレーニングには、ランサムウェアに関する内容は含まれていますか？



[図 2-18 意識啓発やトレーニングに、ランサムウェアに関する内容が含まれているか]

2.6.2. 予防措置

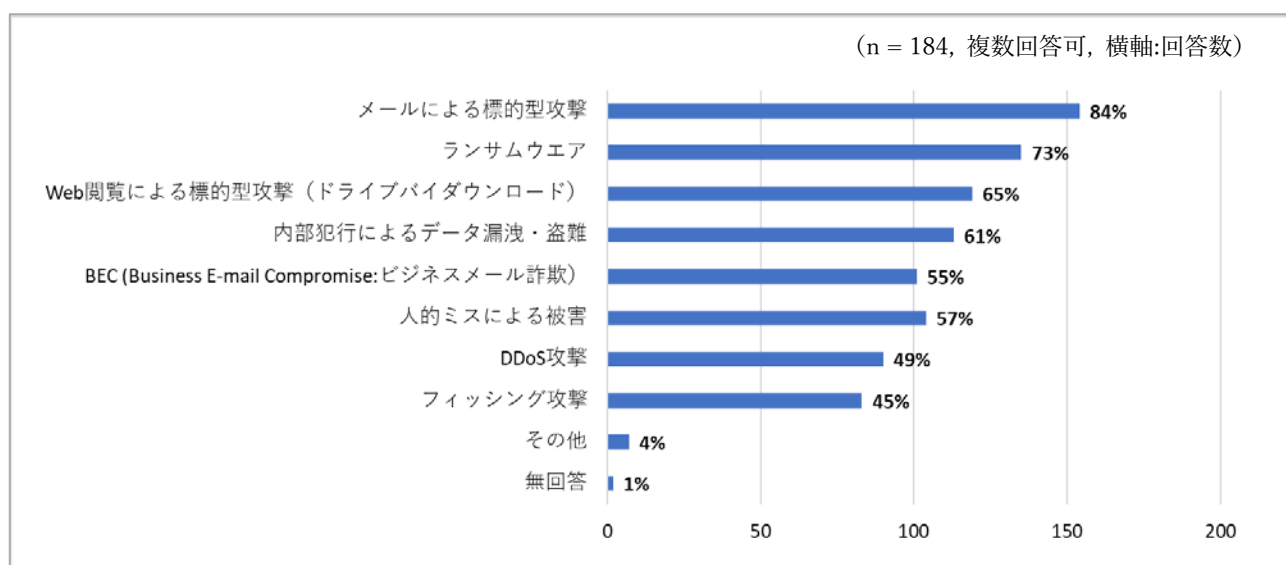
Q4-3. ランサムウェアの予防措置としてとっている対策はありますか？



[図 2-19 ランサムウェア予防措置としての対策内容]

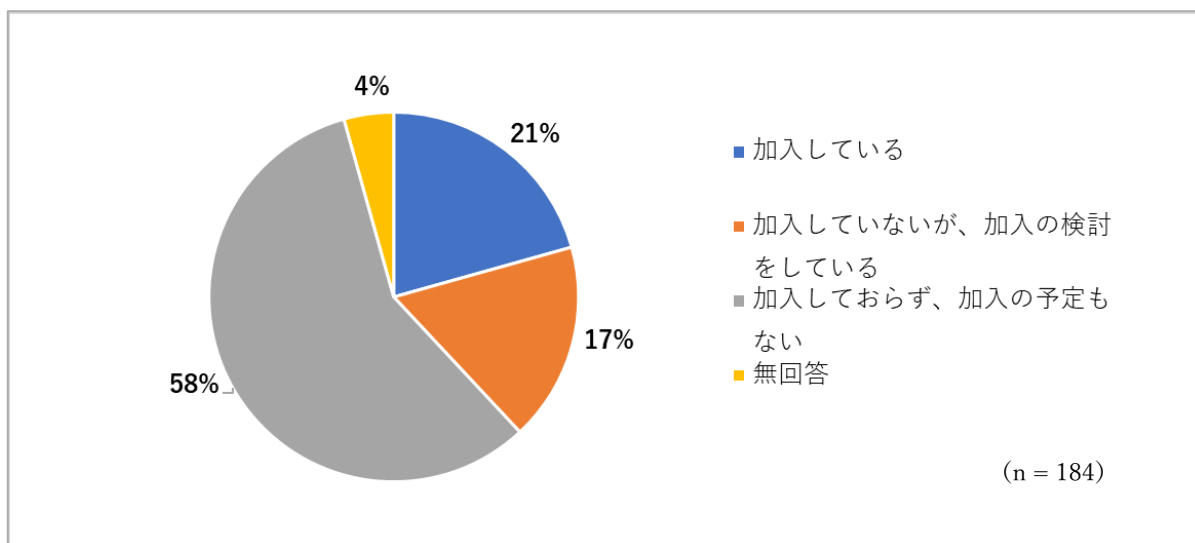
2.6.3. 懸念されるインシデント

Q4-4. 今後、懸念されるセキュリティインシデントは何ですか？



[図 2-20 今後懸念されるセキュリティインシデント]

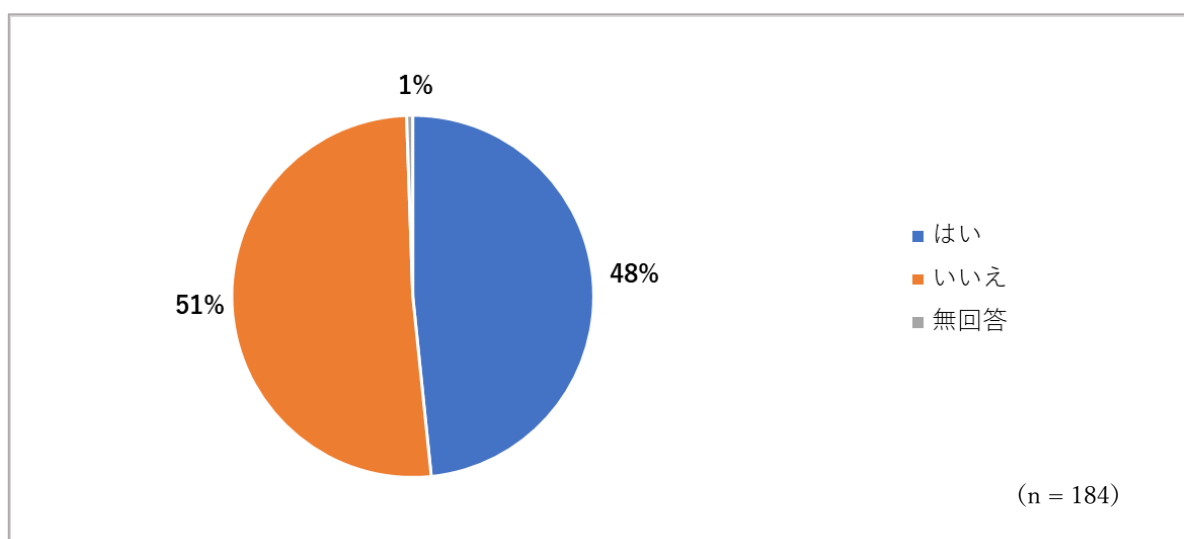
Q4-5. サイバー保険へ加入していますか？



[図 2-21 サイバー保険への加入有無]

2.7. 「No More Ransom」プロジェクトについて

Q5-1. JPCERT/CC は、ランサムウェアの被害低減を目指す国際的なプロジェクト「No More Ransom」(<https://www.nomoreransom.org/ja/index.html>) の活動に賛同しています。このプロジェクトを知っていますか？



[図 2-22 「No More Ransom」プロジェクトを知っているか]

3. 調査結果に対する考察

本章では、ランサムウェア被害実態調査について考察し、推奨する対策を述べる。

■サイバーセキュリティやランサムウェアの脅威に対する意識は比較的高い

— 87%の組織がランサムウェアに関するトレーニングを実施

多くの組織がランサムウェアを含めたサイバーセキュリティ対策に対する意識を持っており、意識啓発やセキュリティトレーニングを実施している（2.6.1. 図 2-17）と回答していた。また、「ランサムウェアについてのトレーニングを含む」と回答した組織は 87%に達していた（2.6.1. 図 2-18）。

— ほぼ全ての組織がランサムウェアに感染しても身代金を支払っていない

ランサムウェアに感染したことが「ある」と回答した組織のほとんどが、犯人への身代金支払いの有無および金額の設問で「身代金を支払わなかった（97%）」（2.5.7. 図 2-15）と回答していた。身代金を支払った場合でも、データが元に戻る保証はなく、また、攻撃者の要求がエスカレートすることや、再度、攻撃のターゲットにされる可能性も考えられる。感染時には冷静に対処を行い、バックアップからの復旧の可能性など状況に応じた対応が必要となる。

— 今後懸念されるインシデントは「メールによる標的型攻撃」、次いで「ランサムウェア」

今後懸念されるインシデント（2.6.3. 図 2-20）は、「メールによる標的型攻撃（84%）」が最も多く、次いで「ランサムウェア（73%）」という結果となっているが、ほとんどのインシデントについても半数以上の組織が選択しており、インシデントに対する関心が高いと言える。

■感染したことが「ある」組織は 35%、トレーニングを行っていても感染を防ぎきるのは難しい

35%の組織がランサムウェアに感染した経験がある（2.5. 図 2-3）ことから、トレーニングなどを通してサイバーセキュリティ対策を行っていても、完全に防ぐことは難しい実態があることが分かった。ランサムウェアを用いた攻撃を含め、サイバー攻撃の手法や手口は日々変化しており、実態に合わせて予防策やトレーニング内容の見直しを行っていくことも重要である。

■「Locky」や「TeslaCrypt」, 「WannaCry」の感染率が高い傾向

ランサムウェアに感染したことが「ある」と回答した組織のうち、最も多くの対象組織が感染を報告したランサムウェア（2.5.2. 図 2-5）は「Locky（52%）」であった。「Locky」は、2016年2月に海外や日本国内での感染事例が確認されており、日本語を含む多言語の脅迫文を表示させることで知られている。感染経路は「ばらまき型メール」だった。請求書を装ったメールに文書ファイルが添付されており、これを開くと文書内のマクロが実行され、ランサムウェア本体がダウンロードされる仕組みになっていた。次に多くの組織が感染していたマルウェアは「TeslaCrypt（20%）」である。これは「vvv ウイルス」とも呼ばれ、2015年12月に海外や日本国内でその存在が確認された。

このランサムウェアは、ゲームユーザを標的としており、セーブされたゲームファイルや環境設定ファイル、ゲームアイテムなどのデータを暗号化し、身代金を要求する。「TeslaCrypt」の脅迫文は英語のみであり、特に日本を標的にしたものではないと考えられるが、英語がわからない場合は Google 翻訳を使うようすすめる文言が脅迫文の冒頭に書かれており、英語圏以外もの国も標的にしている可能性も考えられる。ばらまき型メール経由と脆弱性攻撃サイト経由の 2 種類の感染経路が確認されており、国内においてもこれらの伝染経路で広まったと考えられる。

3 番目の「WannaCry (17%)」については、2017 年 5 月 12 日より世界 150 か国で感染が確認されており、短期間のうちに広い範囲で感染被害が発生した。その理由としては、「WannaCry」がこれまでのランサムウェアと異なりワーム機能を持ったランサムウェアであったことと、あらゆるネットワークに対してランダムに攻撃パケットを送出して伝染する機能をもっていたことが挙げられる。日本国内でも感染事例が確認されており、脅迫文は日本語を含む多言語に対応している。

■感染原因として最も多いのは「E メールへの添付ファイル」「ウェブサイトまたはウェブアプリケーション」

ランサムウェアの感染原因 (2.5.4. 図 2-8) として、最も多かったのが「E メールへの添付ファイル (66%)」であった。攻撃者はメールや SNS など様々な手段を使って感染させようと試みるため、そのことを常に念頭に置き、添付ファイルやリンクには細心の注意を払うことが必要である。特に、送信者やメールの内容に心当たりがない場合や文面に不自然な点がある場合は当事者および関係者への電話など別ルートでの事実確認を怠らないようにすることをおすすめする。

また、「ウェブサイトまたはウェブアプリケーション (41%)」が次に多い感染原因となっている。今回の調査結果 (2.6.2. 図 2-19) では「定期的なソフトウェアの更新」を行っているという回答した組織が 87% あり、概ね適切な対策が行われているようではあるが、「WannaCry」が感染拡大した時のように、OS やアプリケーション・ソフトウェアに脆弱性があると、感染のリスクが高まってしまうため十分に注意する必要がある。ソフトウェアの自動更新を有効にすることや組織内のパッチマネジメントを徹底することで、OS やアプリケーション・ソフトウェアを最新の状態にし、脆弱性の修正と感染リスクの低減を行ってほしい。

■感染後の主な影響は、「データが暗号化された」「業務端末が使用不可になった」

ランサムウェアに感染した際の影響 (2.5.5. 図 2-9) については、典型的なランサムウェアの被害である「データが暗号化された (89%)」または「業務端末が使用不可になった (56%)」と回答した組織が多かった。また、被害の対処法 (2.5.6. 図 2-12) では、「データのバックアップを取得していなかったため、データは元に戻せなかった (16%)」と回答している組織もある。一旦、ファイルが暗号化されてしまうと復号できない可能性もあるため、そのような結果を想定した事前の対策が重要であることを改めて認識しておきたい。その一方で、ランサムウェアによっては後述する No More Ransom プロジェクトなどで復号ツールが提供されていることもあるため、そちらも活用してみることをお勧めする。

例えば、「データのバックアップをとっておく」、「予備の端末を用意しておく」といった準備をしておくことで、万が一ランサムウェアに感染した場合でも、早期の復旧が可能となる。また、バックアップ自体が暗号化されてしまうという事態も想定し、定期的なバックアップや世代管理だけでなく、オリジナルとは別のネットワークにバックアップデータを保管することを推奨する。その際、クラウドストレージや

外付けハードディスクなどを活用し、複数の場所にバックアップを取っておくことも、有効な対策になる。

万が一感染してしまった場合には、感染した端末をネットワークにつないだままにすると他の端末への感染拡大を引き起こしてしまう可能性がある。そうならないために、有線接続であれば LAN ケーブルを端末から外す、無線接続であれば、Wi-fi をオフにすることで、ネットワークから切り離すことも重要である。また、感染した端末に外部ストレージを接続していたり、ネットワーク内で感染した端末が見つかったりした場合は、外部ストレージも暗号化の対象になってしまうことがあるため、同様に端末から切り離すようにすることが重要である。

■感染してから通常業務が復旧するまでにかかった時間は「1 週間未満」が 36%

ランサムウェアに感染してから、通常の業務稼働が復旧するまでにかかった時間（2.5.8. 図 2-16）については、「1 週間未満」と回答した組織が 36%と最も多かった。復旧までに時間がかかると、業務停止などの影響も考えられ、それに伴うコストなども軽視できない。また、今回の調査では、ランサムウェアに感染した際の影響（2.5.5. 図 2-9）について、「社内システムの停止（11%）」「ビジネスラインの停止（3%）」という深刻な影響を受けた組織もあり、万が一の状況を考慮し、復旧を早めるための対策を検討しておくことは経営目線からも重要である。

■「アンチウイルスソフトウェア」「ファイアウォール」の導入が予防対策の上位に

今回の調査では、現在行っているランサムウェアの予防措置（2.6.2. 図 2-19）として、ほとんどの組織が「アンチウイルスソフトウェアの導入（97%）」を行っていることが分かったが、こうしたセキュリティソフトを導入するだけでなく、最新の定義ファイルに更新することも重要であることを改めて伝えたい。新たな脅威に対してもできるだけ対応できる状態を保てば、感染するリスクを低減させることができる。

次に多い「ファイアウォールの導入（92%）」についても、ファイアウォールやメールフィルタを適切に設定することで、不審な通信を制限することができる。また、スパムメールフィルタの活用やメール送信ドメインの検証を行い、不審なメールを着弾させないようにすることも有効な対策の一つである。

「コンピュータ内のファイルの拡張子の表示」を行っている組織が 38%と想定よりも少なかったが、ファイル拡張子の表示もランサムウェアの感染を防ぐために有効な対策の一つである。メールに添付されて送られてきたファイルが不審なファイルか否かを区別しやすくするためにも、拡張子が表示されるようにしておき、「exe」「vbs」「scr」などのプログラムを実行させる拡張子のファイルには触らないようにすることが肝心である。また、それ以外の一見無害な拡張子のファイルであっても危険が潜んでいることがあるため、注意が必要である。このような基本的な対策についても周知を図るため、事例を用いたトレーニングなどの実施を勧めたい。

■既にサイバー保険へ加入している組織は 21%、検討中が 17%

サイバー保険について（2.6.3. 図 2-21）は、21%の組織が既に加入しており、17%が加入を検討しているという結果となった。4 割近くの組織がサイバー保険に加入している、または加入を検討している状況から、サイバー保険がサイバー攻撃への備えの一つとして位置づけられてきていることが窺えた。

■ 「No More Ransom」プロジェクトの認知度の向上が課題

「No More Ransom」プロジェクトについて（2.7. 図 2-22）「知っている」と回答した組織は 48%で、半数以上の組織が認識していないことが分かった。同プロジェクトでは各種ランサムウェアの復号ツールの提供を行っているが、今回の調査で初めて知ったという意見も寄せられている。同プロジェクトを有益な活動にするため、認知度の向上が課題であることが分かった。

また、「No More Ransom」プロジェクトやランサムウェアに関する情報提供について寄せられた意見から、次のような情報が求められていることが分かった。

- 感染経路や攻撃の手口、分析結果
- 感染を防御するための対策
- 感染した場合の対策、復号ツールの提供
- 新たなランサムウェアの情報提供
- ベンダや関連組織と連携した情報提供、情報の集約
- 教育用資料の提供

なお、「No More Ransom」プロジェクトの Web サイトでは、セキュリティベンダから提供されているさまざまな復号ツールが紹介されており、本ツールを使用することで復号できるケースもあるため、ぜひ活用してみることをお勧めする。

The No More Ransom（日本語版）復号ツール

<https://www.nomoreransom.org/ja/decryption-tools.html>

JPCERT/CC は、サポーターメンバとして、同プロジェクトに参加しており、海外メンバと連携し、同プロジェクトで提供されるコンテンツやサービスの日本語化などを行っている。国内においては、独立行政法人情報処理推進機構（IPA）や一般財団法人日本サイバークリミナル対策センター（JC3）と協働して国内におけるランサムウェアの対策に取り組んでいる他、同プロジェクトに関する相談を受け付けている。

早期警戒グループ

TEL: 03-3518-4600 メール : ww-info@jpcert.or.jp

おわりに

第一章で述べたように、ランサムウェアの拡散手法や脅迫方法が年々変化を遂げている。その被害は個人だけでなく、法人にも及んでおり、ビジネスに深刻な影響を与えるケースも増えている。さらに、単に身代金を目的としたものだけでなく、標的型攻撃の痕跡調査をかく乱するためにランサムウェアを使用するものも出てきており、今後は特定の組織を狙ったランサムウェア攻撃が起きる可能性も予想される。このようなランサムウェアを用いた攻撃手法の多様化や、新たな脅威に対応していくためには、企業も多層的な対策をとっていく必要があると考えられる。また、感染経路や原因を追究できる体制や仕組みを整える必要性について検討することも大切である。

第二章と第三章では、感染原因として「Eメールの添付ファイル」や「ウェブサイトまたはウェブアプリケーション」が多く、組織内でランサムウェアの予防措置や教育を行っていても、感染被害を完全に防ぐことは難しい現状を述べた。完全には防げなくても、ランサムウェアの感染リスクを低減するための事前の対策と、感染した場合に迅速に対処するための事後の対策を検討し準備しておくことは重要である。組織内での教育を徹底する他、ランサムウェアの脅威情報や新たな復号ツールなどの情報をタイムリーに取得し活用するなど、多層的な対策によりランサムウェア被害の低減ができると考えられる。

一方で、今回のアンケート調査を通じて寄せられた意見の中には、ランサムウェアの感染経路や攻撃手口、対策などについて、各ベンダや関連機関と連携し、迅速かつまとまった情報発信を求める声も聞かれた。今後の課題としては、情報をタイムリーかつユーザに届くように発信し、啓発活動を推進していくことが必要だと考えている。

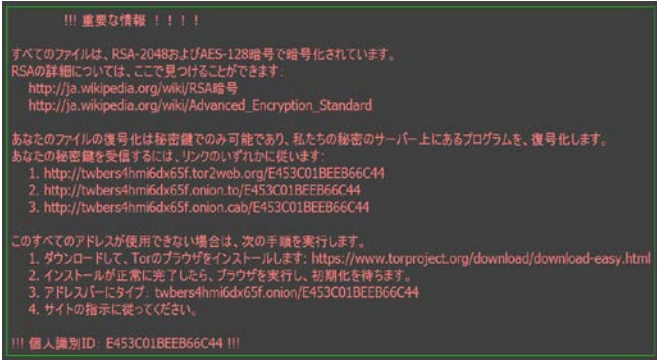
「No More Ransom」プロジェクトの一員としての活動や、国内組織との情報連携を通じて、ランサムウェアによる被害を低減できるよう今後も努力していくとともに、本報告書が、組織が対策を講じる際の参考となるよう願っている。

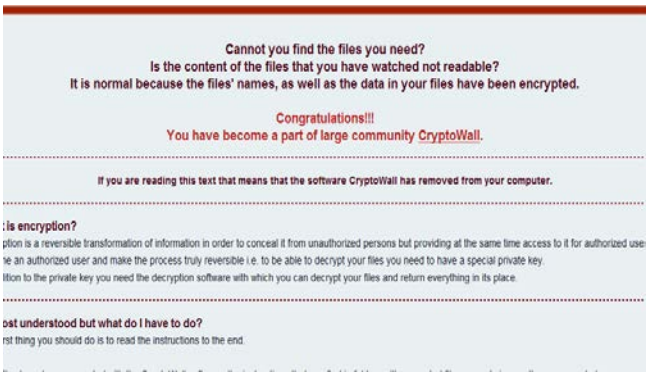
付録 A. ランサムウェアの種類一覧

国内でも特に影響が確認された、もしくは世界的に注目されたランサムウェアの種類について、脅威概要や復号ツールの有無などの情報を一覧形式にまとめた。

[凡例]

ランサムウェアの名称	
ファイル拡張子:ランサムウェアの感染により、暗号化されたファイルの拡張子例	[感染した際に表示される脅迫画面の例]
タイプ:ファイル暗号化型/端末暗号化型	
日本語表示:日本語の脅迫文表示の有無	
NMR での復号ツールの提供:あり/なし	
拡散に使用されるエクスプロイトキット: Neutrino Exploit Kit、Rig Exploit Kit など拡散に使用されたエクスプロイトキットの名称	
概要:公開情報からまとめた各種ランサムウェアのおおよその確認時期、拡散地域、感染経路、身代金要求額など。	

Locky	
ファイル拡張子：「.locky」	
タイプ：ファイル暗号化型	
日本語表示：あり	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット： Neutrino Exploit Kit、Rig Exploit Kit、 Nuclear Exploit Kit、Sundown Exploit Kit、 Hunter Exploit Kit、Bizarro Sundown Exploit Kit	
概要：2016年に、米国や、オーストラリア、ドイツ、イギリスなど世界中で拡散が確認され、日本においても同時期に感染が急増した。国内で感染が拡大した主な理由として、同ランサムウェアが多言語対応型であり、脅迫文が日本語で記載されていたことが挙げられる。「Locky」の拡散経路として、Word 文書ファイルを添付したスパムメールが確認されており、このファイルを開くと、マクロや JavaScript が実行されて「Locky」をダウンロードする。暗号化されたファイルの拡張子を「.locky」に変更するランサムウェアとして知られており、身代金として 0.5 ビットコイン（当時 2 万 4 千円前後）を要求される。	

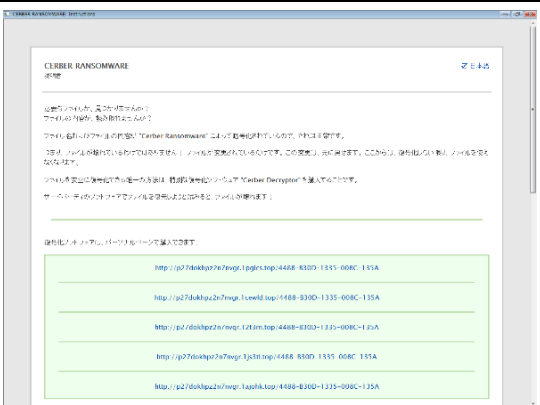
CryptoWall	
ファイル拡張子：ランダムな文字列	
タイプ：ファイル暗号化型	
日本語表示：なし	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット： Angler Exploit Kit、Neutrino Exploit Kit、 Magnitude Exploit Kit	
概要：CryptoWall は、2013 年末頃に海外で存在が確認されたマルウェアで、CryptoLocker を模倣した亜種。日本国内においては 2015 年末頃から感染が確認され始めた。C&C 通信は Tor 匿名ネットワークを介して行っていることで知られており、 익스プロイトキット、マルバタイジング、フィッシング・キャンペーン経由で広く配布される。また、ビットコインによる身代金の支払いを要求した最初のマルウェアでもある。マカフィーによると、2015 年 2 月から 4 月の 2 カ月の調査期間における、ビットコインをドル換算した場合の平均的な価値を基に取引金額を計算した結果、CryptoWall に起因して支払われた身代金の総額の推定額は 3 億 2500 万米ドル(約 400 億円相当) に達しており、金銭被害という面で甚大な被害を及ぼしたランサムウェアのひとつである。同ランサムウェアに感染すると、ファイルの拡張子がランダムな文字列に変更されることとして知られている。	

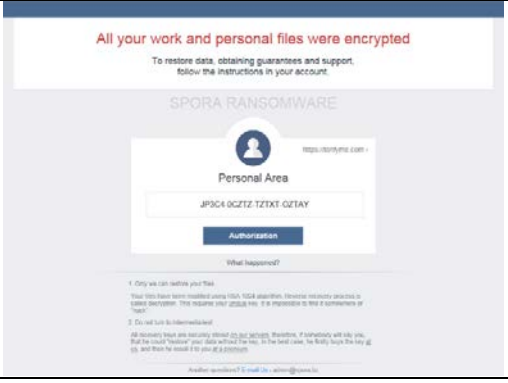
TeslaCrypt	
ファイル拡張子：「.vvv」	<p style="text-align: center;">NOT YOUR LANGUAGE? USE Google Translate</p> <p>What happened to your files? All of your files were protected by a strong encryption with RSA4096 More information about the encryption RSA4096 can be found https://en.wikipedia.org/wiki/RSA_(cryptosystem)</p> <p>What does this mean? This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them</p> <p>How did this happen? Especially for you, on our SERVER was generated the secret key All your files were encrypted with the public key, which has been transferred to your computer via the Internet. Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!</p> <p>What do I do? Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.</p> <p style="border: 1px solid green; padding: 2px;">For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:</p> <ol style="list-style-type: none"> 1 - http://K54ndfku456ngkwsdger.walymac.com/FAB771FAEE0968E 2 - http://ps4dtdgjehejhrhsasqrgzrsatubommarwp.at/FAB771FAEE0968E 3 - http://hftgd74nfbajdcnklrweefotal.materdumst.com/FAB771FAEE0968E
タイプ：ファイル暗号化型	
日本語表示：なし	
NMR での復号ツールの提供：あり	
拡散に使用される 익스プロイトキット： Angler Exploit Kit、Neutrino Exploit Kit、 Nuclear Exploit Kit	
<p>概要：TeslaCrypt は、2015 年初め頃に海外で先行して話題になり、国内においては同年の年末頃に被害が確認された。Angler などの 익스プロイトキット経由で拡散する。初期の TeslaCrypt のターゲットは、ビデオゲームのコミュニティと考えられており、一般的なファイル（文書、画像、データベースファイル等）以外に、ゲーム用のファイルを暗号化することが特徴となっている。暗号化されたファイルの拡張子を主に「.vvv」に変更するランサムウェアとして知られている。また、TeslaCrypt の作者は、一連の活動を謝罪し、回復キーをリリースしている。</p>	


CryptXXX	
ファイル拡張子：「.5桁の英数字」「.crypt1」「.crypt」「.cryptz」など	<p style="text-align: center;">NOT YOUR LANGUAGE? USE https://translate.google.com</p> <p>What happened to your files ? All of your files were protected by a strong encryption with RSA4096 More information about the encryption keys using RSA4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)</p> <p>How did this happen ? !!! Specially for your PC was generated personal RSA4096 Key, both public and private. !!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet. !!! Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our Secret Server</p> <p>What do I do ? So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW!, and restore If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment</p> <p>Your personal ID: CD27199B449C</p> <p>For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:</p> <ol style="list-style-type: none"> 1 - http://ekmkd756hn5aqdft.onion.io 2 - http://ekmkd756hn5aqdft.onion.cab 3 - http://ekmkd756hn5aqdft.onion.cny
タイプ：ファイル暗号化型、端末ロック型	
日本語対応：なし	
NMR での復号ツールの提供：あり	
拡散に使用される 익스プロイトキット： Angler Exploit Kit、Neutrino Exploit Kit	
<p>概要：CryptXXX は、日本を含む世界各地で活発に活動を行っていたランサムウェアの一つで、2016 年に感染活動が多く確認されるようになった。ランサムウェア TeslaCrypt の活動停止と入れ替わるようにして登場し、TeslaCrypt と同様に不正広告や改ざんされた Web サイト等を通じて拡散する。感染すると、PC 内のファイルの拡張子が「.crypt」へ変更され、復元のための身代金として 500 ドル相当のビットコインを要求する。ファイルの暗号化だけでなく画面ロックを行う機能を備えた亜種も発見されている。</p>	

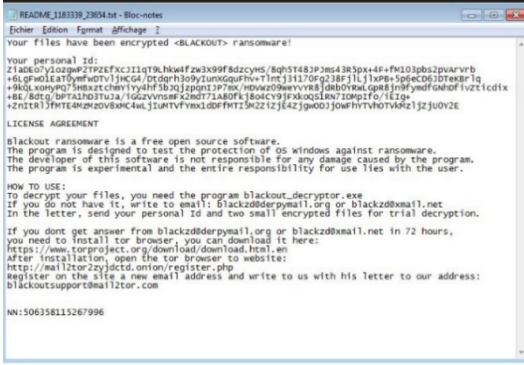
WannaCry (WannaCrypt)	
ファイル拡張子：「.WCRY」「.WNCRY」「.WNCRYT」	
タイプ：ファイル暗号化型	
日本語対応：あり	
NMR での復号ツールの提供：なし	
拡散に使用されるエクスプロイトキット：なし	
<p>概要：WannaCry は、2017 年 5 月に世界中で感染が確認され、欧州、米国、日本を含むアジアなど世界各地の政府機関、病院、企業などに史上前例のない大規模な影響を及ぼしたランサムウェア。適切なアップデートが行われていない Windows OS の脆弱性を利用し、全世界 150 カ国にわたり感染を広めた。WannaCry の最大の特徴は、ワームのようにネットワーク経由で侵入し、拡散する点である。感染すると、感染端末ならびにネットワーク共有上のファイルを暗号化し、身代金として 300 米ドル相当のビットコインを支払うように要求する。感染後の画面に表示される脅迫画面が、日本語を含む 28 種類の言語に対応していることも特徴の一つ。</p>	

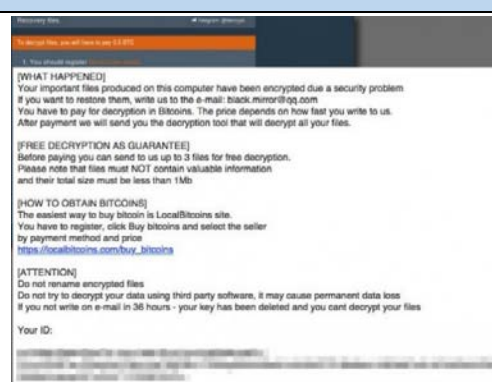
Jaff Ransomware	
ファイル拡張子：「.jaff」「.sVn」	
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：あり	
拡散に使用されるエクスプロイトキット：なし	
<p>概要：Jaff は 2017 年 5 月頃に Jaff に感染させるためのスパムメールが世界中で大量に出回った。このスパムメールは「Invoice」の件名で届き、請求書に見せかけた PDF ファイルが添付されている。感染すると、英語のメッセージが表示され、ファイルを暗号化して拡張子を「.jaff」に変更する。一方、日本およびアジア地域において、Jaff の亜種が添付されたスパムメールが 2017 年 6 月初め頃に大量に拡散された。このスパムメールは、プリンタや複合機からの通知などを装う内容で、感染すると英語のメッセージが表示され、ファイルを暗号化して、拡張子を「.sVn」に変更する。さらに約 18 万円相当のビットコインを支払うように要求する。</p>	

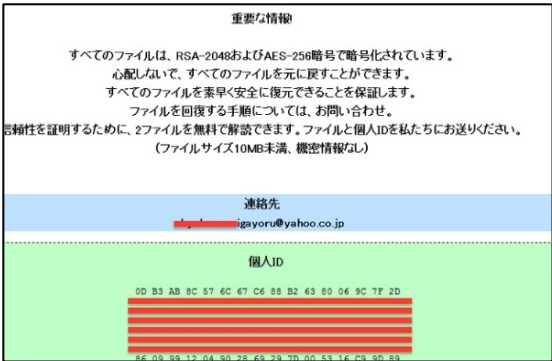
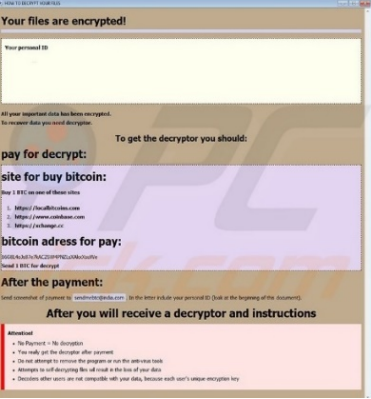
CERBER	
ファイル拡張子：「.cerber」	
タイプ：ファイル暗号化型	
日本語対応：あり	
復号ツール：あり	
拡散に使用される 익스プロイトキット： Magnitude Exploit Kit、Rig Exploit Kit、 Nuetrino Exploit Kit	
<p>概要：CERBER は、2016 年に初めてロシアのアンダーグラウンド市場で確認され、その後日本を含む世界各地で活発な活動を行っているランサムウェアである。史上初の音声を再生し脅迫する機能を備えたランサムウェアとして知られている。また、次々と新しい機能を追加していることも特徴の一つで、クラウドサービスやマルバタイジング（不正広告）、Windows スクリプトファイル、各種 익스プロイトキットなど、多種多様な拡散機能を取り入れ、時とともに変化してきた。感染経路については、全てのバージョンにおいて、スパムメールが利用されている。CERBER の表示画面は、英語、中国語、フランス語、日本語など多数の言語に対応している。身代金として 1.24 ビットコイン（当時 5 万 8 千円相当）の支払いを要求し、その後 7 日間で 2.48 ビットコイン（11 万 7 千円相当）にまで要求額を引き上げる。</p>	

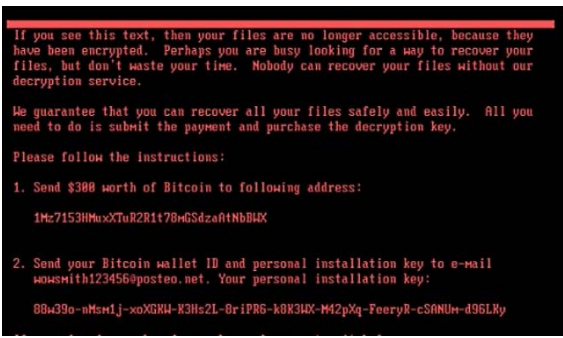
Spora	
ファイル拡張子：拡張子に変更なし	
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット： なし	
<p>概要：Spora は、2017 年 1 月に確認され、2 月中旬頃からロシアを中心に感染被害が急増した。英語圏や日本国内でもごく少数であるが、感染被害が確認されている。Spora は、Web ブラウザ上で「使用文字フォントがインストールされていないため表示が乱れている」という旨の偽のメッセージを表示し、フォントのインストールに見せかけてランサムウェア本体をインストールするという特徴がある。感染後のファイル名は特に変化しない。また全てのファイルが暗号化される訳ではなく、特定の拡張子のファイル、またはフォルダ毎に複数のファイルが暗号化される傾向にある。復元範囲が選べるようにメニューを用意していたり、攻撃者に連絡が取れるチャット機能を用意していたりと、金銭の支払いを促す仕組みが充実している点も特徴の一つ。完全に復元するには、140US ドル相当のビットコインを要求される。</p>	


Crysis	
ファイル拡張子：拡張子に変更なし	 <p>The screenshot shows a ransomware message window with a yellow padlock icon. The text reads: 'All your files have been encrypted! All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail webnafia@asias.com. Write this ID in the title of your message: F20105F8. You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.' Below this, there are sections for 'Free decryption as guarantee' and 'How to obtain Bitcoins'.</p>
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：あり	
拡散に使用されるエクスプロイトキット：なし	
<p>概要：Crysis は、2016 年初め頃にその存在が初めて確認され、5 月末頃から日本を含む世界各地で活発な感染活動が確認された。メールやソーシャルネットワークの広告といった、さまざまな経路を使って拡散する。感染すると、ファイルが暗号化され、画面上の E メールアドレス宛に連絡し、ビットコインで身代金の支払いをするよう要求する画面が表示される。ファイルの拡張子は変化しない。</p>	

BLACKOUT	
ファイル拡張子：拡張子に変更なし	 <p>The screenshot shows a text file named 'README_118133R_23054.txt - Bloc-notes'. The text reads: 'Your files have been encrypted <BLACKOUT> ransomware! your personal id: 21ade07y2ozgw27p2zfxccj11q19khw4fz3k99f8dzynd...'. It includes a 'LICENSE AGREEMENT' section and a 'HOW TO USE' section with instructions on how to contact the developer for decryption.</p>
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：なし	
拡散に使用されるエクスプロイトキット：なし	
<p>概要：BLACKOUT は、2017 年 7 月に海外において感染が確認された。主にスパムメールやメールの添付ファイルを介して拡散したと考えられている。感染すると、ファイル名をランダムな文字を含む名前に変更する。BLACKOUT には、身代金の要求メッセージを含むテキストファイルを作成し、既存のすべてのフォルダに配置するという特徴がある。身代金要求メッセージでは、被害者にファイルを暗号化したことを通知し、BLACKOUT の開発者に電子メールで連絡をしてデータを復元するように促す。身代金として、500 ドル～1500 ドル相当のビットコインを要求する。</p>	

ALETA	
ファイル拡張子：「.aleta」	
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット：なし	
<p>概要：ALETA は、2017 年 7 月に海外で初めて確認された。感染経路としては、リモートデスクトッププロトコル（RDP）を使用してシステムに侵入すると考えられている。感染すると、データが暗号化され、ファイルの名前に「E メールアドレス」が、拡張子に「.aleta」が付加される。また、感染した PC の各フォルダに HTA ファイルを配置する。この HTA ファイルには、ファイルを暗号化したことや、ファイルを復元するために、攻撃者に連絡をして身代金を支払うように書かれており、被害者からの報告によると、身代金として 2 ビットコイン（5000US ドル相当）を提示される。</p>	

Globelmposter・Oni ランサムウェア	
ファイル拡張子： 「.cypt」「.pscrypt」「.oni」	
タイプ：ファイル暗号化型	
日本語対応：あり	
NMR での復号ツールの提供：あり	
拡散に使用されるエクスプロイトキット： Rig Exploit Kit	
<p>概要：Globelmposter は、2017 年 5 月頃から欧州等で被害が発生しており、比較的新しいランサムウェアであることが推測されている。元々は Globe と呼ばれるマルウェアを起源としており、感染するとファイルが暗号化され、ファイル名に「.cypt」や「.pscrypt」といった拡張子を付けて HTML ファイルベースの脅迫文を表示する。WannaCry や EternalRocks、Petya-Like など悪用された ShadowBrokers のエクスプロイトツールが使用されたケースもあるため、APT 攻撃グループとの関連性も疑われている。</p> <p>日本国内においては、2017 年 6 月に Globelmposter の亜種である「.oni」という拡張子を付加する Oni ランサムウェアが確認された。暗号化された各フォルダには「!!!README!!!.html」という html ファイルが生成され、日本語の脅迫文と復号のための指示が表示される。現時点で感染経路は明らかになっていないが、Web またはメールなどの経路から、他のエクスプロイトやマルウェアなどを介して感染すると考えられている。</p>	

Petya 亜種 (NotPetya)	
ファイル拡張子：なし	 <p>The screenshot shows a ransomware message with the following text: "If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service. We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key. Please follow the instructions: 1. Send \$300 worth of Bitcoin to following address: 1Mz7153HMuxXTuR2R1t7BwG5dzaftNbB4X 2. Send your Bitcoin wallet ID and personal installation key to e-mail w4wsM1th123456@posteo.net. Your personal installation key: 8Bw39o-nMsh1j-xoXGRH-R3Hs2L-8riPR6-k8K34X-M42pXq-FeeryR-c50NUh-d96Lky"</p>
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット：Sundown Exploit Kit	
<p>概要：ランサムウェア Petya の存在は、2016 年に既に確認されていたが、2017 年 6 月から Petya の亜種 (NotPetya) による感染被害が、ウクライナ、ロシア、欧州などで多数確認されたことで再び話題になった。Petya は、PC 上のファイルだけでなく、マスターブートレコード (MBR) も暗号化する点が特徴となっている。Petya の亜種では、Windows SMBv1 の脆弱性を悪用して感染を拡大させる仕組みなどが付加されており、暗号化されたファイルの拡張子に変更を加えることはない。また、データを元に戻すことが非常に難しいことでも知られている。感染すると、身代金として 300 米ドル相当のビットコインを要求される。</p>	

Bad Rabbit	
ファイル拡張子：変更なし	 <p>The screenshot shows a ransomware message with the following text: "Oops! Your files have been encrypted. If you see this text, your files are no longer accessible. You might have been looking for a way to recover your files. Don't waste your time. No one will be able to recover them without our decryption service. We guarantee that you can recover all your files safely. All you need to do is submit the payment and get the decryption password. Visit our web service at [redacted] Your personal installation key#1: [redacted] If you have already got the password, please enter it below. Password#1: -"</p>
タイプ：ファイル暗号化型	
日本語対応：なし	
NMR での復号ツールの提供：なし	
拡散に使用される 익스プロイトキット：なし	
<p>概要：Bad Rabbit は、2017 年 10 月にロシアやウクライナなどの地域を中心として、世界各地で感染が確認されたランサムウェアである。主な標的となったウクライナでは、鉄道や空港などの交通機関、報道機関をはじめとする多くの重要インフラが影響を受け、システムが停止するなどの被害があった。感染経路としては、偽の Flash インストーラを装って感染を広げており、ロシアの正規ニュース・サイトでポップアップ・ウィンドウが表示され、そこから攻撃サイトに誘導されて、ランサムウェアのドロッパー (実行可能ファイル) がダウンロードされるというケースが確認されている。また、感染拡大方法の一つとして SMBv1 の脆弱性が利用されていたことも確認されている。Bad Rabbit に感染すると、コンピュータのファイルが暗号化され、カウントダウンタイマーが表示された、Tor ネットワーク経由で支払い用のページに誘導される。攻撃者はファイルを復号する見返りに、40 時間前後の制限時間内に 0.05 ビットコイン (約 285US ドル) を支払うよう要求する。タイマーがゼロになるまでに身代金を支払わなかった場合、身代金額は引き上げられる。</p>	