JC3
Japan Cybercrime Control Center

JC3
公式ブック

ランサムウェア攻撃に対する捜査ハンドブック

一般財団法人日本サイバー犯罪対策センター 編著

立花書房

JC3
Japan Cybercrime Control Center

JC3
公式ブック

ランサムウェア攻撃に対する捜査ハンドブック

一般財団法人日本サイバー犯罪対策センター 編著

立花書房

目次

Chapter

1 本書について

1.1 本書の対象者

本書の主な対象者は、次のとおりである。

- ランサムウェア攻撃発生時に現場臨場を行う捜査員
- 現場臨場する捜査員を指揮する捜査幹部

1.2 本書作成の目的

1.2.1 攻撃者の検挙、被害回復

本書を作成した第一の目的は、警察によるランサムウェア攻撃者の検挙と被害法人の被害回復に貢献することである。

本書を参考に、警察が迅速・的確な捜査を行うことで、攻撃者の特定につながることはもちろん、暗号化されたファイルを復号するための情報を入手することなどにより、被害者の被害回復に寄与することも期待できる。

1.2.2 現場臨場時間の短縮、確実な資料収集

本書を作成した第二の目的は、捜査員の現場臨場を行う時間の短縮と、確実な資料収集を行うことである。

ランサムウェア攻撃の捜査が困難である要因の一つとして、攻撃者特定につながる資料や犯行疎明資料の収集が難しい点が挙げられる。

メモリ等の揮発性情報が消失する前に現場臨場できなかったり、フォレンジックツールの準備不足等で、必要な資料収集ができなかったりするためである。

これらの問題を解決するために、認知から現場臨場までの時間短縮、現場での確実な資料収集に役立つ情報を盛り込んだ。

1.2.3 初動対応の道しるべ

本書を作成した第三の目的は、ランサムウェア攻撃の発生時に現場臨場する捜査員へ道を示すことである。

初めてランサムウェア攻撃の現場に臨場する捜査員は、「必要な体制が整っているのか」、「資機材は足りているのか」、「選択した資料収集方法・手続は最善なのか」、「捜査項目に漏れはないのか」等の様々な疑問や不安を抱くのではないだろうか。

本書は、ランサムウェア攻撃発生時の現場臨場に立ち向かう捜査員が、これら疑問や不安を抱かずに、目の前の捜査に集中できるようになることを目指して作成された。

1.3 本書の作成方法

内容の偏りを避けるため、ランサムウェア攻撃に関する多くの情報を収集し、それら情報を分析・集約し、次の手順で作成した。

① ランサムウェア攻撃、インシデントレスポンス、デジタル・フォレンジック等に係る参考文献を収集

② 収集した参考文献の中から「ランサムウェア攻撃に対する捜査」に役立つと認めた情報を抽出・整理

1.4 本書の特徴

本書の特徴は、次のとおりである。

- ランサムウェア攻撃の捜査に役立つ情報を記載
- 理論や技術よりも行動（どう考えて何をするか）を重視
- 攻撃者の特定、犯行状況の疎明、罪名の適用を見据えた資料収集方法を記載

1.5 本書が対象とするランサムウェア攻撃

ランサムウェア攻撃には、いたずら目的でファイルを暗号化するものから金銭を要求するものまで、様々な種類が存在する。

本書では、現在主流となっている次のランサムウェア攻撃を主な対象としている。

- 人手によるランサムウェア攻撃
- 二重恐喝で金銭を要求するもの
- 主にWindows環境を攻撃対象とするもの

1.6 本書の使い方

本書は、読めばランサムウェア攻撃事案発生前の準備が可能なハンドブックとして、また、事案発生時に現場に持参する捜査員のためのハンドブックとしても使用できるように作成している。

言うまでもなく、警察が取り扱う事案は、発生時期、被害者、攻撃者、手口等によって異なり、全く同じ捜査手法・手続をそのまま適用できるものは存在しない。

当然、ランサムウェア攻撃の事案についても同じことが言え、本書どおりに捜査を進めるだけで、攻撃者の検挙にたどり着くような事件は存在しないと思われる。

しかし、本書の内容を踏まえて捜査に臨めば、現場での柔軟な対応ができるはずである。

なお、本書では、一部非公式のWebサイトやツール（フリーソフト）も紹介しているが、公判を見据えた証拠収集の観点から、同Webサイトやツールから収集した情報が、どの程度の証拠価値を持つのかを個別事件ごとに検討する必要があることに留意されたい。

1.7 動作環境

本書内には、フォレンジックツールを使用して、メモリダンプやディスクイメージを収集する手順、攻撃者の侵入経路や情報漏洩の有無を捜査する手順等を画面キャプチャ付きで掲載しているパートがあるが、これらはWindows 10 Pro（64ビット）環境で実行したものである。

被害法人の環境が異なる場合、本書の手順どおりに進まない場合があるので注意していただきたい。

Chapter

2 ランサムウェア攻撃

ランサムウェア攻撃の捜査に当たり、最低限必要な知識は次のとおりである。

2.1 ランサムウェア

ランサムとは「身代金」のことであり、ランサムウェアとはランサムとソフトウェアを組み合わせた造語である。

ランサムウェアは、感染すると端末（パソコン、サーバ）に保存されているファイルを暗号化して使用できない状態にした上で、そのファイルを元に戻す（復号する）ための身代金（金銭や暗号資産等）を要求する攻撃に使用されるマルウェア（不正プログラム）の一種である。

2.2 ランサムウェア攻撃

攻撃者によるランサムウェアを用いた一連の犯行を「ランサムウェア攻撃」という。

ランサムウェア攻撃は、攻撃グループや攻撃者によって、侵入方法やランサムウェア実行までの過程が大きく異なるため、捜査員はこれを念頭に置いて捜査すべきと考えられる。

2.3 人手によるランサムウェア攻撃

現在主流のランサムウェア攻撃は「人手によるランサムウェア攻撃」と呼ばれている。

攻撃者自身がパソコンに向かってキーボードを打ち、様々なツールや攻

撃手法を駆使して、遠隔地にある法人のネットワークへ侵入し、ネットワーク・端末の調査、侵害範囲の拡大（横展開）、情報流出、ランサムウェア感染（ファイル暗号化）等を敢行する。

このように、攻撃者自身が手を動かすことによって一連の犯行を実行するため、人手によるランサムウェア攻撃と呼ばれている。

人の手を介するということは、攻撃者が何らかのミスを犯す可能性があるということであり、それが攻撃者検挙に向けた突破口になる可能性がある。

2.4 ランサムウェア攻撃の分業化

人手によるランサムウェア攻撃は、ランサムウェアの開発、識別符号（ID、パスワード）等の収集、被害法人のネットワークへの侵入等の単位で分業化が進んでいる。

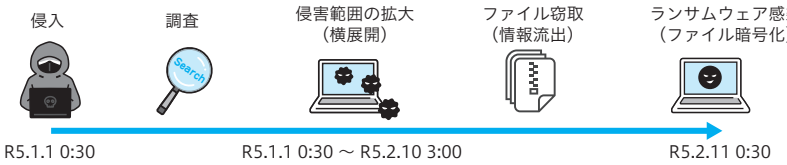
したがって、捜査を進める中で、当然のように複数地域のIPアドレスが登場するほか、単独犯か複数犯かの見極めも必要になる。

2.5 長期間にわたる一連の攻撃

人手によるランサムウェア攻撃は、侵入、調査、横展開、情報流出、ファイル暗号化といった複数の段階を踏むため、長期間（数時間、数日間、数か月間）にわたって敢行される。

よって、ランサムウェア攻撃に対する捜査は、被害法人が認知した時点、つまりファイルが暗号化された「点」だけに注目するのではなく、侵入から感染までの一連の流れ、つまり、「線」に着目すべきである。

■ 侵入から感染までの期間に係るイメージ図



※　侵入から感染までの期間（数時間、数日間、数か月間）は事案によって異なる

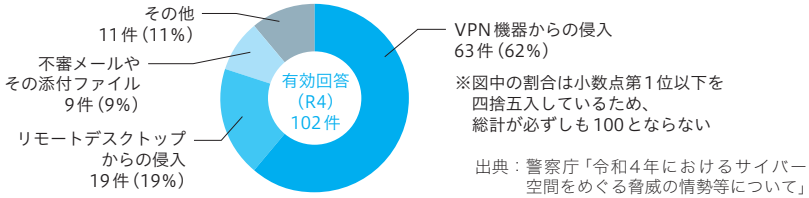
現状では、最初の侵入者がランサムウェアに感染させるわけではなく、侵入者がダークウェブ上で侵入に成功したアカウント情報を販売し、それを購入又は入手した別の攻撃者が被害法人に侵入してランサムウェアに感染させるケースも散見されるため、注意が必要である。

2.6 侵入経路

ランサムウェア攻撃の攻撃者が使う主な侵入経路には、VPN機器、リモートデスクトップ、メールなどがある。

また、攻撃者は複数回にわたって侵入している可能性が高く、その度に侵入経路が異なる可能性もある。

■ 侵入経路



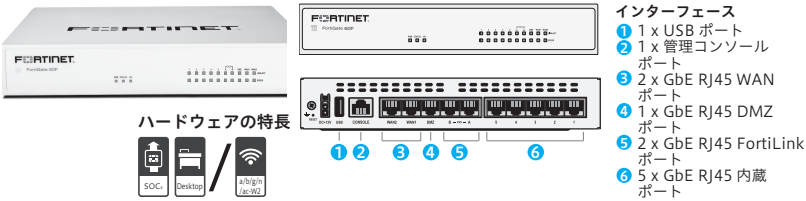
出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

VPN機器のイメージ

実際に現場に臨場する捜査員においてもVPN機器を目にする機会は少ないと思われる。

例えば、「FortiGate 60F」や「YAMAHA RTX5000」の場合、一般的なスイッチングハブに似た形・大きさをしている。

■ FortiGate 60F / FortiWiFi 60F



出典：FortiGate製品（https://www.fortinet.com/jp/products/next-generation-firewall）

■ YAMAHA RTX5000

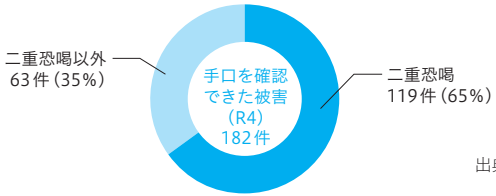
出典：ヤマハネットワーク製品（https://network.yamaha.com/support/download/tool）

2.7 二重恐喝

「二重恐喝」とは、ランサムウェアによって暗号化されたファイルを復号するための身代金要求に加え、暗号化する前にデータを窃取（攻撃者端末にコピー、ストレージサービスへアップロード等）しておき、対価を支払わなければ、データをインターネット上に公開すると脅すという、いわば二重に恐喝する攻撃方法である。

警察庁の調査によると、令和4年におけるランサムウェア被害の手口別報告件数のうち、手口が判明しているもののうち65％が二重恐喝となっている。

■ ランサムウェア被害の手口別報告件数



出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

2.8 ランサムノート

ランサムウェア感染端末に保存されている恐喝文を記載した壁紙や文書ファイルを「ランサムノート」と呼ぶ。

ランサムノートには、身代金の支払い方法、暗号化ファイルの復号方法、リークサイトのURL等が記載されている。

■ LockBit 2.0のランサムノート（壁紙）

出典：BlackBerry Blog（https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm）

■ LockBit 2.0のランサムノート（文書ファイル）

Restore-My-Files.txt

```
1  LockBit 2.0 Ransomware
2
3  Your data are stolen and encrypted
4  The data will be published on TOR website
   http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and
   https://bigblog.at if you do not pay the ransom
5  You can contact us and decrypt one file for free on these TOR sites
6  http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllygmiyhvanjj352jayid.onion
7  http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
8  OR
9  https://decoding.at
10
11 Decryption ID: 586A97038216AC6BF076FC47B7F227E3
```

出典：BlackBerry Blog（https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm）

2.9 リークサイト

攻撃者が被害法人から窃取したファイルを公開するためのサイトを、「リークサイト」と呼ぶ。

被害法人が一定期間を経過しても金銭等を支払わない場合や交渉に失敗した場合、実際にリークサイトにファイルが公開されることがある。

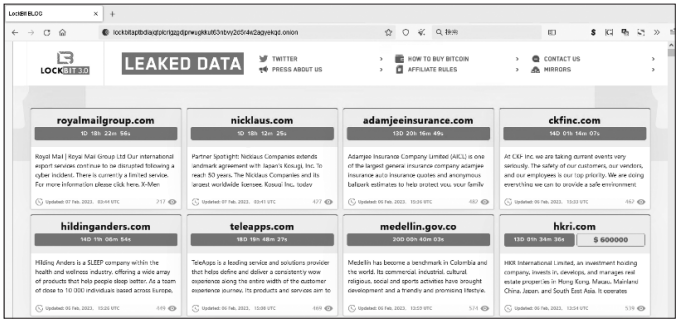
リークサイトがダークウェブの一種であるTorネットワークで公開され

ている場合、Microsoft EdgeやGoogle Chrome等の一般的なブラウザでは閲覧できないため、「Tor Browser」を使用して閲覧する。

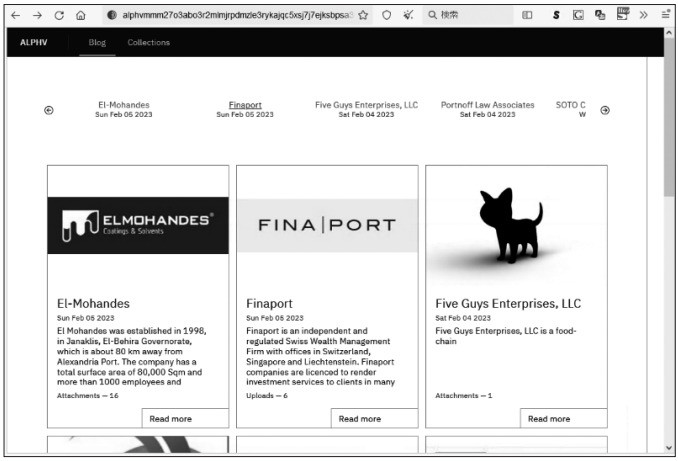
リークサイトのURLのトップレベルドメインが「.onion」であれば、Torネットワークのサイトである。

■ 代表的なリークサイト

リークサイト	URL
LockBit 3.0 （Torネットワーク）	http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion

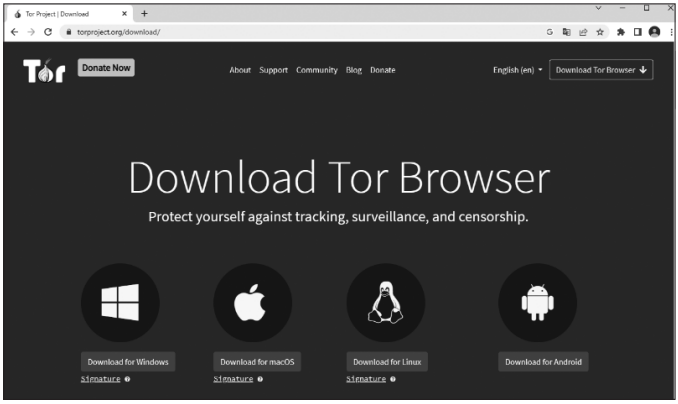


リークサイト	URL
ALPHV （Torネットワーク）	http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/



■ ダークウェブ閲覧ソフト

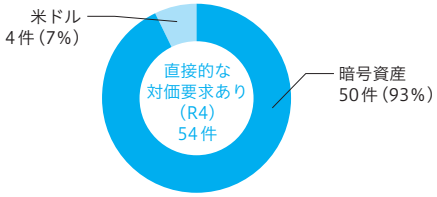
ツール名	URL
Tor Browser	https://www.torproject.org/



2.10 身代金の支払い方法

警察庁の調査によると、令和4年におけるランサムウェア被害のうち、直接的な対価の要求が確認できたものの金銭（身代金）の支払い方法は、93%が暗号資産によるものとなっている。

■ 要求された対価支払い方法別報告件数



出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

2.11 特徴的な拡張子、アイコン

ランサムウェアにファイルを暗号化された場合、拡張子やアイコンが特徴的なものに変更される場合がある。

JC3公式ブック
ランサムウェア攻撃に対する捜査ハンドブック

令和６年３月１日　第１刷発行

編　著　一般財団法人日本サイバー犯罪対策センター
発行者　橘　茂雄
発行所　立花書房
東京都千代田区神田小川町 3-28-2
電話　03-3291-1561（代表）
FAX　03-3233-2871
https://tachibanashobo.co.jp
組　版　BUCH⁺
印　刷
製　本　倉敷印刷