



# ランサムウェア攻撃に対する

# 捜査ハンドブック

JC3  
公式ブック

■ 一般財団法人日本サイバー犯罪対策センター 編著 ■ A5判 ■ 並製 ■ 226頁

定価 3,850 円 (本体 3,500 円 + 税 10%)

ISBN978-4-8037-4296-1 C3032

本書のポイント

## サイバー犯罪捜査員必読！ 第一線から贈る最適解の実務書。

サイバー犯罪捜査の第一線で活躍する実務家による、ランサムウェア攻撃捜査に当たる現場捜査員と捜査幹部に向けた最適解の実務書。

## わかりやすい解説と2色カラーの図表で現場対応をイメージできる！

想定される捜査上の問題点を洗い出し、重要なポイントにフォーカスして、図表・画像を用いて解説。この一冊で、ランサムウェア攻撃の基礎知識と捜査のポイントがわかる！

## 攻撃発生前の準備にも、発生時の現場対応にも役立つ！

理論や技術よりも行動を重視し、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掲載。ランサムウェア攻撃の事前対策にも捜査にも役立つ。

内容見本

### 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者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

捜査手法を駆使して、遠隔地に所在す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）を実行する。このように、攻撃者自身の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称されている。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

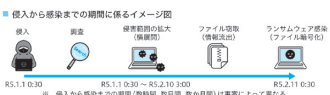
人手によるランサムウェア攻撃は、ランサムウェアの開発、識別符号（ID、パスワード）等の収集、被害法人のネットワークへの侵入等の単位で分業化が進んでいる。

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、単独犯が複数犯か見極める必要になる。

#### 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）にわたって実行される。

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、侵入から感染まで一連の流れ、つまり「線」に着目すべきである。



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」「証拠は足りているのか」「選択した資料収集方法・手続は最適なのか」「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掻かず、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

内容の幅りを避けるため、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。

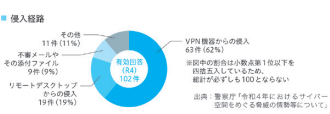
- ① ランサムウェア攻撃、インシデントレスポンス、デジタル・フォレンジック等に係る参考文献を収集
- ② 収集した参考文献の中から「ランサムウェア攻撃に対する捜査」

#### 1.4

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、侵入者がグループウェア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数見られるため、注意が必要である。

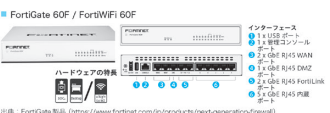
#### 2.6 侵入経路

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。



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。



### 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。

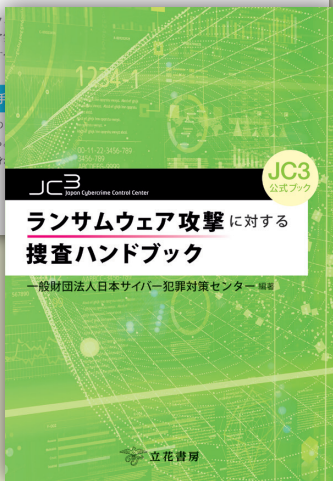
#### 2.2 ランサムウェア攻撃

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。

ランサムウェアをランサムウェアに置き、捜査員が捜査する。

#### 2.3 人手

現在主流の呼ばれている。攻撃者自身



目次裏面参照 ▶▶▶

## Chapter 1 本書について

- 1.1 本書の対象者
- 1.2 本書作成の目的
- 1.3 本書の作成方法
- 1.4 本書の特徴
- 1.5 本書が対象とするランサムウェア攻撃
- 1.6 本書の使い方
- 1.7 動作環境

## Chapter 2 ランサムウェア攻撃

- 2.1 ランサムウェア
- 2.2 ランサムウェア攻撃
- 2.3 人手によるランサムウェア攻撃
- 2.4 ランサムウェア攻撃の分業化
- 2.5 長期間にわたる一連の攻撃
- 2.6 侵入経路
- 2.7 二重恐喝
- 2.8 ランサムノート
- 2.9 リークサイト
- 2.10 身代金の支払い方法
- 2.11 特徴的な拡張子、アイコン
- 2.12 復号ツール配布サイト
- 2.13 ランサムウェア情報まとめサイト
- 2.14 ランサムウェア攻撃の手口の体系
- 2.15 ランサムウェア攻撃のイメージ
- 2.16 攻撃者がよく使うツール

## Chapter 3 捜査全般の留意事項

- 3.1 迅速な現場臨場、資料収集
- 3.2 資料収集の重要性
- 3.3 身代金の支払い
- 3.4 適用罪名
- 3.5 攻撃者特定に資する資料
- 3.6 被害状況（犯行状況）の疎明資料
- 3.7 ランサムウェア攻撃の現場における捜査の流れ

## Chapter 4 捜査体制の確保

- 4.1 捜査時の役割、指揮系統
- 4.2 役割の説明、成果物等
- 4.3 関係部署

## Chapter 5 平時における準備

- 5.1 ランサムウェア攻撃情報の収集
- 5.2 ジャンプバッグの整備

## Chapter 6 事案の認知

- 6.1 認知の流れ
- 6.2 被害法人の確認
- 6.3 被害法人への要請
- 6.4 自所属／本部への即報

## Chapter 7 緊急参集、現場臨場

- 7.1 緊急参集
- 7.2 現場臨場

## Chapter 8 事情聴取

- 8.1 事情聴取の流れ
- 8.2 関係者の把握
- 8.3 被害法人の状況を理解
- 8.4 被害法人に関する事項の聴取
- 8.5 被害状況に関する事項の聴取
- 8.6 設計書等の入手

## Chapter 9 状況把握

- 9.1 ランサムウェアに関する事項
- 9.2 攻撃者に関する事項
- 9.3 影響範囲に関する事項
- 9.4 対応状況に関する事項
- 9.5 調査状況に関する事項
- 9.6 復旧に関する事項

## Chapter 10 被害法人への助言

## Chapter 11 資料収集の考え方

- 11.1 資料収集する前の同意、調整等
- 11.2 資料収集の流れ
- 11.3 資料収集範囲の限定
- 11.4 保全端末の選定
- 11.5 優先順位付け
- 11.6 作業の記録
- 11.7 その他

## Chapter 12 ファスト・フォレンジック

- 12.1 ファスト・フォレンジックの意義
- 12.2 ファスト・フォレンジックの流れ
- 12.3 収集すべき資料
- 12.4 メモリ情報の収集
- 12.5 ディスクイメージの収集
- 12.6 端末情報の収集（CDIR-C）
- 12.7 解析

## Chapter 13 刑罰法令

- 13.1 刑法
- 13.2 不正アクセス行為の禁止等に関する法律

### 付録1 用語集

### 付録2 ランサムウェア攻撃者グループのリークサイト一覧

### 付録3 ランサムウェア攻撃者グループとツールの対比表

## Chapter 14 参考文献

- 14.1 書籍
- 14.2 Web 資料
- 14.3 Web ページ
- 14.4 Web 動画
- 14.5 その他資料

FAXでのご注文は、切りとらずにそのままご送信ください。FAX 03-3233-2871

申込書

\*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

申 込 部

ご所属名

庁・道・府・県

貴社の個人情報の取扱いに同意の上、申し込めます。

署・隊・課

ご担当者名

(TEL :

)

備考欄

個人情報の取扱いについて 株式会社立花書房 個人情報管理者 総務部長

**利用目的** お客様の個人情報は商品発送・サービス実施とご案内・お問合せへの回答に利用します。**第三者提供** 本人の同意がある場合又は法律に基づく場合を除き、第三者に提供しません。**委託** 利用目的の達成に必要な範囲内で取扱いの一部を委託することがございます。**開示請求・問合せ窓口** 本人からのお申し出により、個人情報の利用目的の通知・開示、内容の訂正・追加・削除、利用の停止又は消去、第三者への提供の停止・提供記録の開示に対応します。弊社窓口 (info@tachibanashobo.co.jp) までご連絡ください。**提供の任意性** 個人情報のご提供は任意ですが、必要な項目を頂けない場合、お申込みをお受けできない場合がございます。



立花書房

〒101-0052 東京都千代田区神田小川町3-28-2

TEL:03-3291-1561(代表) <https://tachibanashobo.co.jp>