立花書房 最新刊 令和６年３月刊行

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。

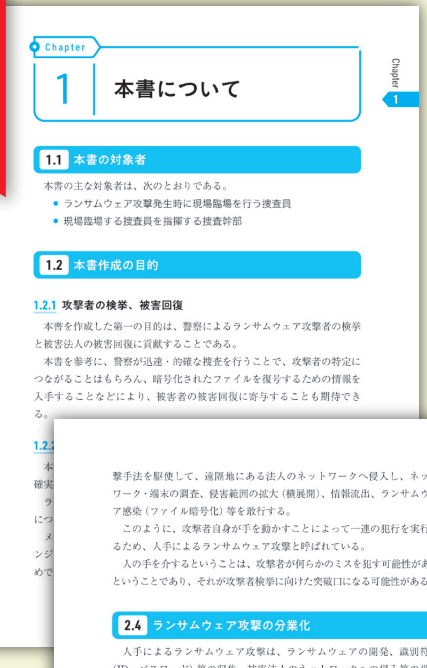
わかりやすい解説と２色カラーの図表で現場対応をイメージできる！

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

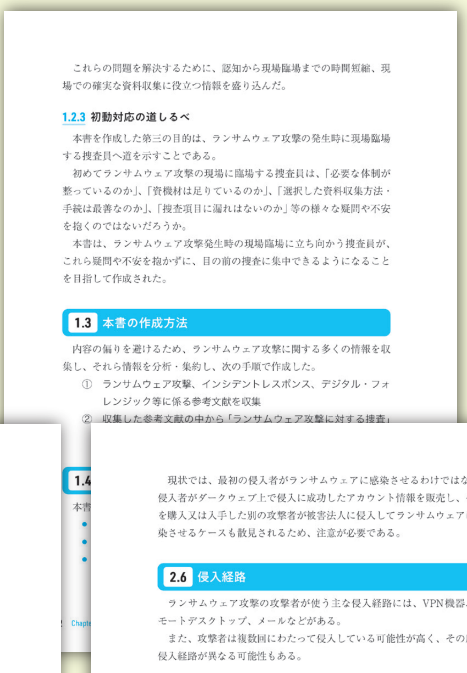
本書の主な対象者は、次のとおりである。
- ランサムウェア攻撃発生時に現場臨場を行う捜査員
- 現場臨場する捜査員を指揮する捜査幹部

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。


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。

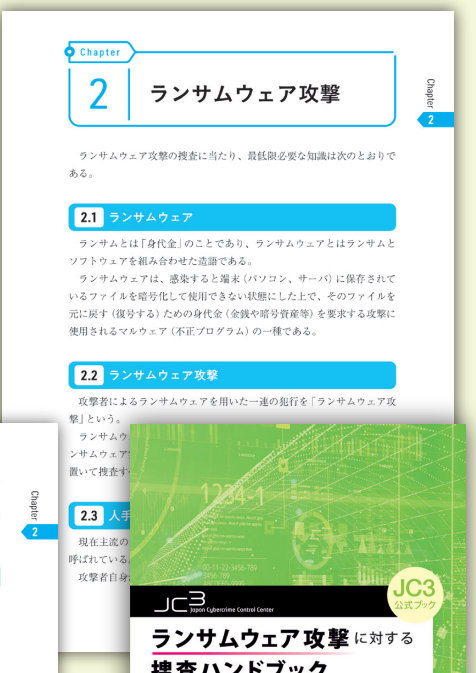
本書は、ランサムウェア攻撃発生時の現場臨場に立ち向かう捜査員が、これら疑問や不安を抱かずに、目の前の捜査に集中できるようになることを目指して作成された。

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」


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。

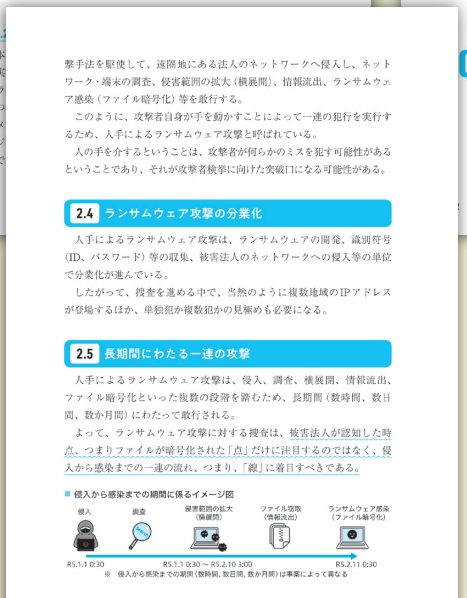
2.1 ランサムウェア

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。


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。

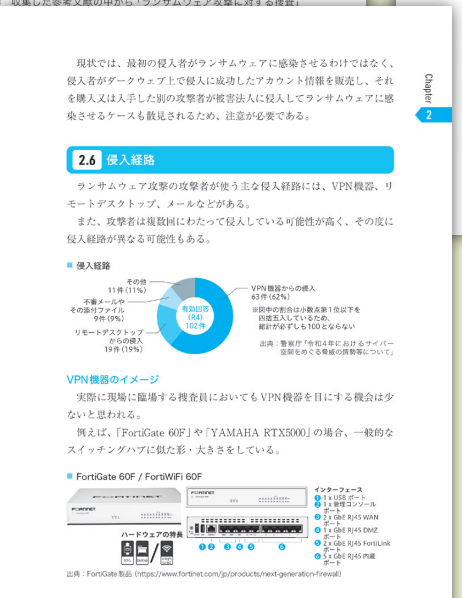
2.5 長期間にわたる一連の攻撃

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

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）

目次裏面参照▶▶▶

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

目　次（抜粋）

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
	署・隊・課

貴社の個人情報の取扱いに同意の上、申し込みます。

ご担当者名 （TEL： ）

備 考 欄

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