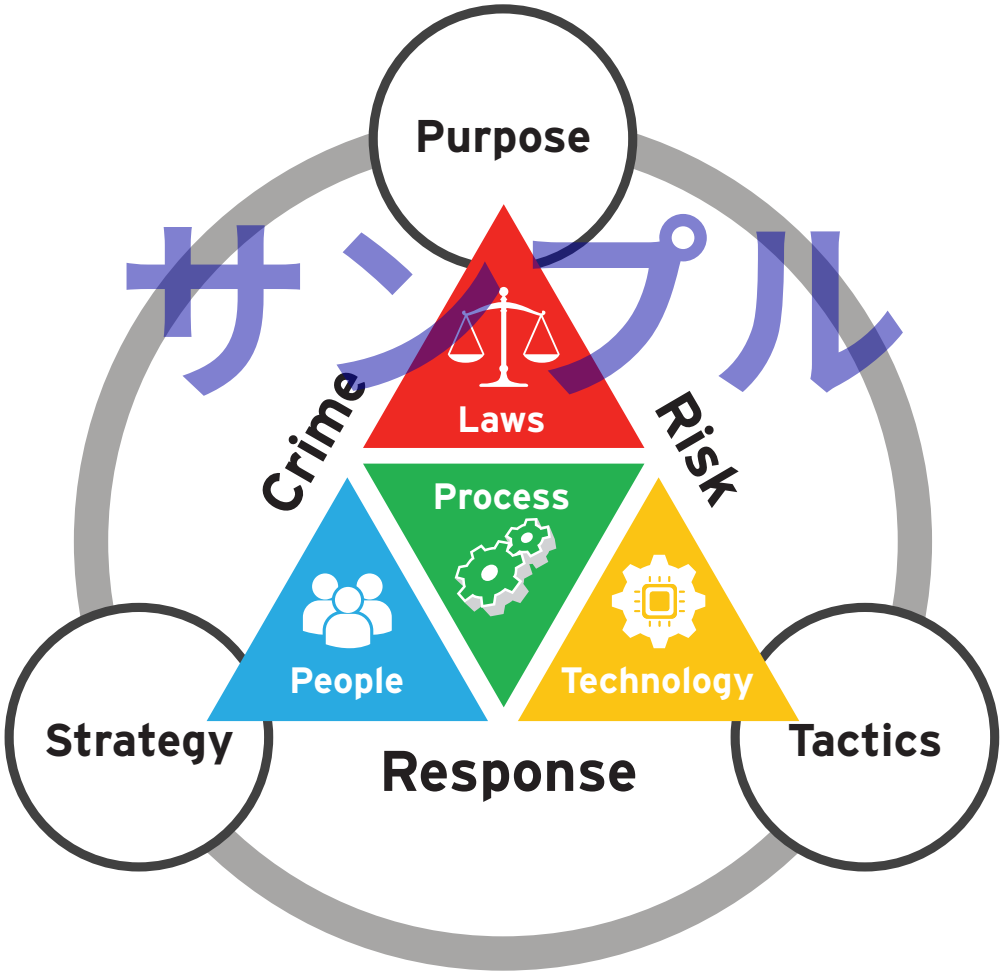
Cybercrime Investigation Body Of Knowledge

第1版

サンプル

A Guide to the

Cybercrime Investigation Body of Knowledge



All statements of fact, opinion, or analysis expressed are the authors' alone and do not necessarily reflect the official positions or views of the Department of Justice (DOJ) or any other U.S. government agency. Relevant chapters have been reviewed by DOJ to prevent the disclosure of classified or otherwise sensitive information.

The Publisher;
CIBOK Editorial Committee

Sponsored by Trend Micro Incorporated.
First printing, January 2017

執筆者

Executive Editor

Shane Shook (PhD) is a well-known veteran of information security and response engagements with nearly 30 years of experience spanning government and industry IT risk management issues. He has led forensic analysts and provided expert testimony in many of the most notorious breaches across most industry sectors. He has also served as expert witness in related (international and US) federal, civil and commercial disputes. He currently serves on the advisory boards of several emerging security technology companies. He is a contributing author and editor of several books and a frequent keynote or guest speaker.

Authors and Contributors

Judith H. Germano is the founding member of Germano Law LLC, a law firm specializing in advising companies on cybersecurity governance and data privacy issues. Ms. Germano is an Adjunct Professor at New York University (NYU) School of Law and a Senior Fellow at the New York University Center for Cybersecurity, where she leads NYU's task force of corporate executives and senior government officials focusing on emerging cybersecurity issues and solutions. Previously, Ms. Germano served as Chief of Economic Crimes at the U.S. Attorney's Office for the District of New Jersey, and was a federal prosecutor for 11 years. Before joining the U.S. Attorney's Office, she worked at the multinational law firm, Shearman & Sterling LLP, in New York City. Ms. Germano's publications include *Cybersecurity Partnerships: A New Era of Collaboration* and *After the Breach: Cybersecurity Liability Risk.*

Craig W. Sorum is a 25-year veteran of the Federal Bureau of Investigation (FBI) where he conducted and supervised hundreds of domestic and international cybercrime investigations while assigned to field offices in El Paso, TX, Washington, D.C., Cedar Rapids, IA and Minneapolis, MN. Craig received awards for significant cyber investigations as a field agent and was selected as a "Federal 100 Award" winner for top IT managers in government for his accomplishments as Chief of the FBI's Law Enforcement Online Unit at FBIHQ. Following the Bureau, Craig was employed as a Senior Manager of Information Security at a Fortune 500 defense and aerospace company where he was responsible for all cyber investigations and threat intelligence matters. Craig is currently working as a cyber security management consultant.

David Cowen is a Certified SANS Instructor, CISSP, and GIAC Certified Forensic Examiner. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sector. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series of books on digital forensics; Hacking Exposed Computer Forensics (1st-3rd editions), Infosec Pro Guide to

Computer Forensics, and the Anti Hacker Toolkit (Third Edition).

Patrick A. Westerhaus joined Wells Fargo in 2016 and is heading up a team in Enterprise Information Security (EIS), Cyber Threat Fusion Center (CTFC), working to consolidate and analyze data in an effort to develop an enterprise program to reduce cyber, fraud, and money laundering risk for the institution. Prior to joining Wells Fargo, Patrick was with KPMG in their fraud and forensic practice and he spent the last 12 years in the FBI reaching the level of Supervisory Special Agent in the Headquarters Cyber Division. During his tenure in the FBI Patrick led investigations into corporate/ government fraud, public corruption, counterterrorism, counterintelligence, cyber fraud/theft and his last position was at the NCIJTF's Virtual Currency Team. Patrick has a Bachelor of Business Administration in accounting from Gonzaga University, a Masters in Forensic Science in Security Management from The George Washington University, and a graduate certificate in International Security from Stanford. Patrick also is a CPA and he maintains CFE & CAMS certifications.

Chris Coulter is a forensic examiner and incident responder who has led engagements in government, industry, and individual computer crimes investigations. He is a patent holder (Digital forensic acquisition kit and methods of use thereof - United States US 13/019,796) for technology that he developed and delivered to the market to simplify the complex methods of evidence acquisition in forensic computer investigations. His experience includes corporate leadership in cyber security services and products, audit and investigations experience with PwC, Stroz Friedberg LLC, MIT Labs, and the IRS.

Eric Zimmerman is a senior director in Kroll's Cyber Security and Investigations practice. Eric has a tremendous depth and breadth of expertise in the cyber realm, spanning complex law enforcement investigations, computer forensics, expert witness testimony, computer systems design and application architecture. He has received numerous recognitions for his work, is an award-winning author and is a frequently sought-after instructor and presenter on cyber-related topics. Before joining Kroll, Eric was a Special Agent with the Federal Bureau of Investigation (FBI), specializing in investigating criminal and national security-related computer intrusions, crimes against children (production, distribution and possession of child pornography), intellectual property theft and related crimes.

Noriaki Hayashi is a Senior Researcher with Trend Micro Incorporated in Japan. He is a highly-skilled and certified administrator and systems engineer in several computing platforms and technologies. He has more than 17 years of systems management and security experience, including program and project management, security research, and threat response.

Luke Dembosky is a Partner in Debevoise & Plimpton's Cybersecurity & Data Privacy group and formerly served as Deputy Assistant Attorney General for National Security at the Justice Department's National Security Division. Over 14 years with DOJ, he has served in various roles, including as Deputy Chief for Litigation at DOJ's Computer Crime and Intellectual Property

Section. Mr. Dembosky has been a regular advisor to the leadership of the DOJ, FBI, Secret Service, National Security Council and other agencies regarding major cyber cases and related legal and policy issues. He participated in the negotiation of a 2013 cyber accord with Russia and the historic 5-point agreement signed by President Obama and President Xi Jinping of China in 2015, and has co-represented DOJ in cyber discussions at the United Nations. He was recently named Vice Chair of the ABA Public Contract Law Section, focusing on addressing technology risks to supply chain. Mr. Dembosky is also Co-Chair of the Information Sharing and Analysis Organization Governance Working Group leading the development of internal governance guidance for ISAOs as part of the White House initiative to establish cybersecurity threat sharing platforms across industry.

John Jolly is the Vice President of Customer Success at Syncurity. Prior to joining Syncurity John was the Vice President and General Manager of the Cyber Security Division at General Dynamics, where he had responsibility for a broad portfolio of products and services that included a commercial incident response practice. John holds an undergraduate degree in Computer Science with honors from the University of Maryland Baltimore County and a MBA in Finance with honors from the Wharton School at the University of Pennsylvania.

Philip Fodchuk leads Suncor's Enterprise wide Information Security Program. Within Suncor, Philip is responsible for maturing and enhancing the information security posture of the organization, and leads the cyber security incident response function. Previously, Philip was a Partner with Deloitte's Cyber Security practice within the Enterprise Risk Services group. In that role he served as a Global leader for Crisis Management for the Energy & Resources sector and was Deloitte's Canadian leader for Cyber Security Incident Response. Philip was a sworn police officer with the Royal Canadian Mounted Police (RCMP) and the Calgary Police Service where he worked with technological crime, cyber security and incident response matters. With 20 years of diverse experience, Philip is considered a subject matter expert in responding to, managing and developing strategies around cyber security, digital forensic, incident management and organizational crisis issues.

Ian (Iftach) Amit is a seasoned manager in the security and software industry with vast experience in a myriad areas of information security- from enterprise security, through retail, to end user software and large back-end systems. He is an Information Security expert with experience ranging from low level technical expertise and up to corporate security policy, regulatory compliance and strategy. Ian is a frequent BlackHat and DefCon speaker, and founding member of the PTES (Penetration Testing Execution Standard), IL-CERT, and the Tel-Aviv DEFCON group (DC9723).

書評家

A special thanks to the following individuals who reviewed the draft edition of the CIBOK. Each provided important feedback to assist the authors. The list of contributors and reviewers will expand over time as this CIBOK evolves.

Reviewers

Richard Nolan, Global Managing Director of Cyber Investigations, Citi

Nicholas Peach, Senior Vice President, Information Security Executive, Bank of America/Merrill Lynch

Ronald Ritchey, Managing Director, JPMorgan Chase & Co.

Michael Woodson, VP, State Street

G. Bobby Singh, CISO, TMX Group

Avner Ziv, CIO, Bank of Israel

John R. Riley, Division Chief (Cyber Division), US Department of Homeland Security

Goran Oparnica, Managing Director, INsig2

Benoit Piton, CISO, BNP Paribas France

Dr. Richard Schroth, Executive Director and Executive in Residence, the Kogod Cybersecurity Governance Center at American University

John Walton, Azure Security, Microsoft Corporation

Carmen Oveissi-Fields, Partner/Global CISO, Deloitte

Ron Gula, Founder Tenable Network Security

Michael J. Hershman, CEO, Fairfax Group / ICSS

CIBOK Organizing Committee

The CIBOK was conceived and organized by the following individuals who contributed their talents and efforts to produce this important work.

Executive Editor and Principal Author, Shane Shook

Executive Producer, Trend Micro Corporate Officer of Japan Region, Satoshi Shimizu

Executive Director, Proseed Corporation CEO, Hiroshi Nishino

Senior Coordinator, Trend Micro Incorporated Director, Masakazu Yasumoto

Contributing Author and Project Member, Trend Micro Incorporated Senior Researcher, Noriaki Hayashi

Style Editor and Project Controller, Trend Micro Incorporated Senior Specialist, Yuka Miyatake

Project Consultant, Proseed Corporation Senior Consultant, Tetsuri Sawada

CIBOK 目次

序 章

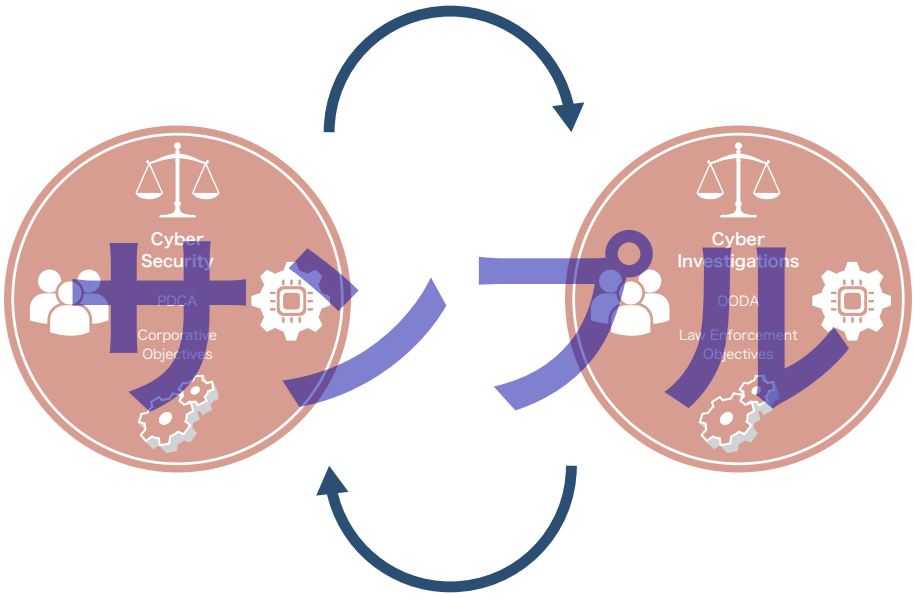
本書に対する序言

サンプル

本書の対象読者

本書は、以下を想定読者と考える。

- 犯罪捜査を行う警察組織または法執行機関（検察、裁判所）、類似する職務執行機関（捜査権または逮捕権など警察権が認められている機関）の職員、組織における不正を調査する職員、犯罪捜査に関する経験を有しているが、「サイバー犯罪」と言われても、何をすべきかよく分からない者
- 新たに組織内にサイバー犯罪捜査チームの組成を任命された責任者
- すでに犯罪捜査の実働組織をマネジメントした経験があり、今後、サイバー犯罪捜査部門の責任者としての任命が期待されている幹部候補生
- 短期的に高い効果を発揮することのできるサイバー犯罪捜査官をトレーニングするプログラムの研究・開発・指導を行う者



「CIBOK」の概念

なぜ「CIBOK」なのか

サイバーセキュリティとは、組織のリスクを特定し、軽減するための情報通信技術（IT）における機能である。

組織は「**オペレーショナルリスク**[1]」とその管理に関して、「**基本方針（Policy）**」、「**実施手順（Procedure）**」および「教育（Training）」を有している。そこに情報通信技術は、情報収集、処理、管理、定着、および保護の形で支援している。また、情報通信技術は享受者である下流の顧客に対し、サービ

1　内部プロセス・人・システムが不適切であること、もしくは機能しないこと、または外生的事象が生起することから生じる損失に係るリスク。バーゼル銀行監督委員会「自己資本の測定と基準に関する国際的統一化：改訂された枠組」より

スを提供し続ける上でのリスクを軽減する管理機能の役割も果たしている。これらの機能により、市場、株主、出資者に対する義務が果たされ、「**経営管理（Executive Management）**」を満たすことができる。

組織で使用される情報通信技術は、組織要件の高まりとともに、梃（Leverage）として「攻撃対象としての技術（Technology as a Tool）」を進化させてきた。時を同じくして、組織機能を破壊または混乱させるサイバー攻撃も発生している。

こうした現状において、「**最高情報処理責任者（CIO）**」は情報通信技術の支援を通して業務の継続性を確保する役割を果たすことで担当幹部として「役員会議室の椅子（Seat at the Boardroom Table）」を手中に収めた。そこには情報保護と情報インフラストラクチャに対するセキュリティも含まれる。そのCIOの役割を支えるため、「**最高情報セキュリティ責任者（CISO）**」の役職が新設された。CISOは必要となる資源の戦略的かつ戦術的な計画策定と管理の役割を担っている。

情報通信技術の急速な発展とそれに相関する脅威によって、特定のスキル、知識そして経験を満たすために求められる要件は定義された。脅威と関連要件はそれに対応する「マーケットインテリジェンス（Market Intelligence）」（公開情報または独自情報）が形成された。それは組織にとって新たなリスクともなり、現在もそのリスクは進化を続けている。

そこで組織では「**適時性捜査（Coincidental Investigative）**」や「**インテリジェンス（Intelligence）**」に対する要求が高まり、その支援者として新たな「**サイバー犯罪捜査官（Cybercrime Investigator）**」の役割に期待される。

「**サイバー犯罪捜査知識体系（Cybercrime Investigation Body of Knowledge: CIBOK）**」は、法執行機関のみならず、組織におけるリスク管理者、情報通信技術者を支えるために必要な背景、要件について記述することを意図している。

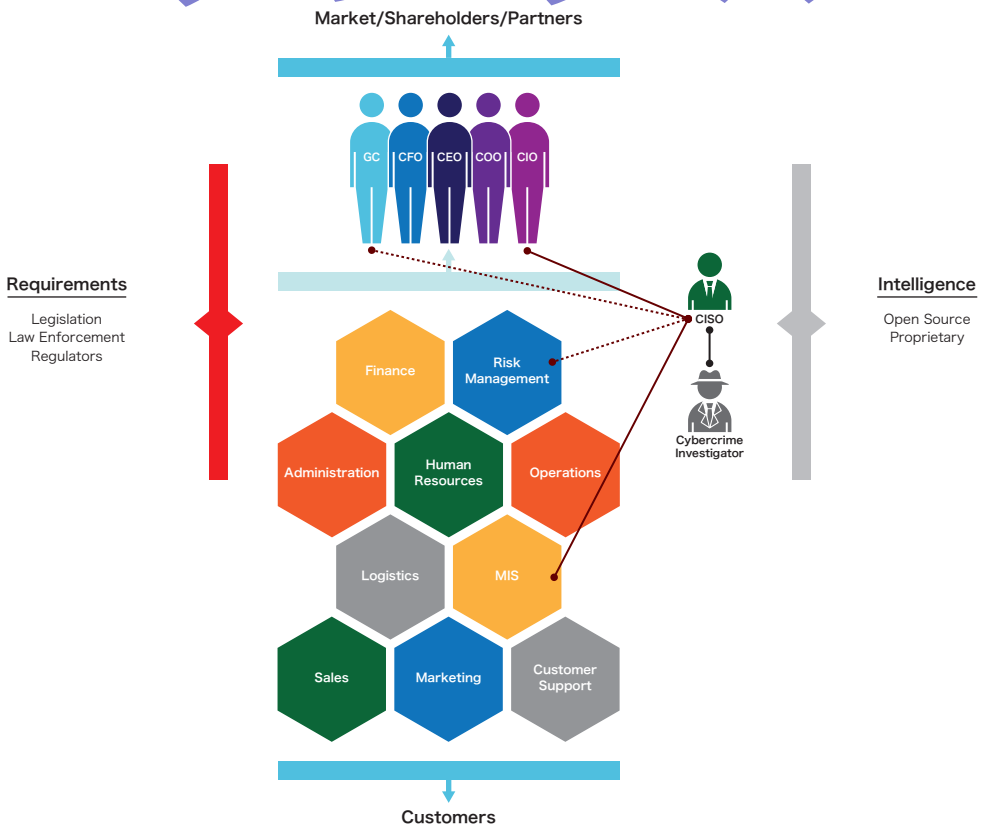


図 1. サイバー犯罪捜査フレームワーク

「CIBOK」の目的とは何か

本書の目的とは

「**サイバー犯罪捜査知識体系（Cybercrime Investigation Body of Knowledge: CIBOK）**」の目的は、力量を備えた、有能なサイバー犯罪捜査官が、その捜査活動において、実践している「**良い実務慣行（Good Practice）**」とはなにかを示すことにある。

サイバー犯罪捜査を実行する上で一般的に身についていなければならない知識、技能、姿勢について領域全体を体系的に分類・秩序立てを行い、「**階層構造（Taxonomy）**」を示すことで、それに含まれるトピックスを利用するためのアクセス手段を提供することにある。このため、各トピックに関する記述は、そのトピックに関して、読者が参照資料を首尾良く発見するために必要な範囲だけに限定する。知識体そのものは、本書のなかにあるのではなく、参照資料の中から見いだされるものである。

CIBOK を確立する 5 つの目的

本書は、次に示す 5 つの目的に従って確立されている。

1. 各国の法律に拠ることのない全世界で一貫したサイバー犯罪捜査に関する心得（Common Sense Approach）を普及・促進すること。
2. 他の体系化された実務慣行、プロジェクト管理、コンピュータサイエンス、デジタルフォレンジックスについて、サイバー犯罪捜査の範囲における位置づけを詳細に示すこと。
3. サイバー犯罪捜査において実践すべき内容を、特徴付けして示すこと。
4. サイバー犯罪捜査知識体に対して、トピックスを利用するための手段を提供すること。
5. トレーニングカリキュラム開発および、業務に携わる個人の知識とスキルが高い水準のレベルであることの保証に必要な基礎を提供すること。

これらの目的を達成するために、次の活動が行われている。

第 1 の目的（全世界で一貫したサイバー犯罪捜査に関する心得）を達成するため、本書は 3 か国から参加した 12 人の執筆者、およびレビュワーによる開発プロセスによって構築されている。

第 2 の目的（他の体系化された実務慣行とサイバー犯罪捜査の範囲における位置づけを詳細に示す）を達成するために、サイバー犯罪捜査における実行フレームワークとして取り入れなければならないと認識された資料（Materials）は、図 2 に列挙された 8 つの知識領域からなるサイバー犯罪捜査における実行フレームワークによって階層化されている。

第1章

サイバー犯罪とその捜査

サンプル

はじめに

犯罪は、常に社会の一要素として存在してきた。人間が罪を犯す理由はさまざまで、目的が1つではない場合もある。犯罪行為の影響は社会によって解釈され、合理的な処罰が科される。犯罪者はその行為を成し遂げるために道具を使う。サイバー犯罪の場合、その目的で使われるのはコンピュータである。企業がネットワークやインターネットにつながる以前は、侵入といえば、ハンマーやピックといった道具が使われたり、入館証や警報システムの暗証番号が盗まれて悪用されたりするか、窓ガラスが割られたりして起こるものであった。現在、企業への侵入に使われているのは、電子メールによるスピアフィッシング攻撃やウェブサービスに対するSQLインジェクション攻撃、ソーシャルエンジニアリング手法などである。何かを破壊して侵入するという意味では同じ犯罪であるが、その目的を果たすための道具が異なっている。いずれにしろ、罪を犯しているのはやはり人間である。

本章では、サイバー犯罪に関連する法理について触れ、それらの定義と捜査、起訴の方法をみていく。また、内部統制の問題や、捜査および起訴の方法に影響する管轄権に関する指標（および制限事項）についても触れる。さらに、専門家がそれぞれのプログラムや方針を調整し、応用可能なフレームワークを構築できるよう、組織機関および捜査機関の役割と責任について説明する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- 法廷や法令における「サイバー犯罪」の定義とは
- サイバー犯罪捜査を管轄するのはだれか
- サイバー犯罪捜査における「ベストプラクティス」とは

第2章

サイバー犯罪の種類

はじめに

かつて、活動家は組織活動に起因する不正や不公平に対し、社会的抗議活動やデモ活動として、責任者や決定者がいる施設の前でプラカードを掲げ、公の場で自らの主張を示すことが彼らの専売特許であった。今日、このような社会的抗議はソーシャルメディア上で展開されている。より悪質な例として標的組織が運営する Web サイトなどのマーケティング情報を改変する活動もみられる。これらのデモ活動に共通する目的は、顧客が企業の製品やサービスを利用することを妨げたり、従業員の業務遂行能力を低下させることであった。今日ではその手段として、システム消去やシステムを使用不能にするツールを用いることでサービス拒否攻撃や妨害行為を実現し、その目的を達成している。同様にかつての恐喝は、都合の悪い情報を使用したり、企業が依存している手段やサービスをコントロールすることで実行されていたが、今やそれもランサムウェアで容易に実行されるようになっている。(民間または政府による) 諜報活動は常に存在したが、今はリモートアクセスや傍受を可能にするバックドア型トロイの木馬でそれも容易に実行されている。

サイバーで容易に実行できるのは、どのような犯罪の「種類 (Type)」だろうか？　本章では、企業の妨害や敵対するブランドへの攻撃を容易に実現するために用いられたサイバーツールの使用方法から、犯罪行為者が (しばしばサイバーツールを使用して) 達成しようとしている実際の目的から、捜査官の目をはぐらかすために用いているサイバーツールの使用方法に至るまで、サイバー犯罪の進化について説明している。また、そのような目的や彼らを後押しする動機、犯罪者と犠牲者のプロファイル、サイバー犯罪者の特徴の特定に関する説明も行っている。

本章で示されている定義は、サイバー犯罪が映し出す脅威の種類を示すことで、監査および評価項目を決定する際、また防御および保護メカニズムを決定する際に、組織のポリシー策定者にとっての一助とすることが狙いである。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- 「サイバー犯罪」とは
- その目的や動機とは
- サイバー犯罪者のプロファイルとは
- サイバー犯罪者の組織構成とは
- サイバー犯罪者が保有するスキルや知識とは
- サイバー犯罪の進化経緯とは

第3章

サイバー犯罪の犯行遺物 (Artifacts)

サンプル

はじめに

犯罪は必ず証拠を残すものである。犯罪は単独の行為ではなく、いくつもの行為が積み重なって違法行為となる。したがって、捜査官や組織の管理職が犯罪者の手口である TTP（Tactics, Techniques and Procedures：戦術、技術および手順）を理解できれば、サイバー犯罪の計画や準備、管理から実行を反映する形跡や手掛かりをつかむことができる。計画された犯罪か否かにかかわらず、そのような形跡が犯罪の特性を識別するのに役立つことになる。これらの形跡は、一般的に「犯行遺物（Artifacts）」と呼ばれる。

本章では、活動のステージ（段階）を示す証拠として、また犯罪に関係のある活動の兆候または属性として評価可能なサイバー犯罪の犯行遺物について詳細に説明する。さらに、捜査官がこういった犯行遺物を発見するのに役立つ内外の情報源について説明し、加えて組織の意思決定者や管理職が包括的な監査や評価のプログラム、または防衛・防御システムおよび手順を構築するのを支援する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の兆候とは
- サイバー犯罪の犯行遺物と兆候の違いとは
- サイバー犯罪活動におけるステージ（段階）とは
- 捜査官が使用できるサイバー犯罪の犯行遺物の種類とは
- 捜査官がサイバー犯罪の犯行遺物と兆候を見つけられる場所はどこか

第4章

サイバー犯罪のスコープ

サンプル

はじめに

ある人物が銃撃を受けた。これは状況によっては犯罪かもしれないし、そうでないかもしれない。ある人物が意図的な銃撃を受けた。これでも犯罪でない可能性がある。その人物が撃たれた場所は戦場ではなく、住宅地であった。まだ、状況は明確でない。その人物は、デモに参加している群衆の中にいて、意図的な銃撃を受けた。もしかすると、発砲者には自己防衛といった正当な理由があっただろうか。撃たれた人物は、デモに参加している群衆に向かって演説していた。あるいは、犯罪かもしれない。撃たれたのは、マーティン・ルーサー・キングであった。いかなる犯罪も、行動と意図、その行為による影響によって定義される。犯罪の特性も同じ基準によって定義される。区別に使われるのは、基本的に犯罪の「スコープ」である。

上記のような犯罪は、撃たれた人物が戦場にいる兵士だった場合や、マーティン・ルーサー・キングではなく、デモに居合わせた人物だった場合には違うものになる。これは、単純に、犯罪行為の影響はスコープが幅広いからである。犯罪の脅威または（既遂の場合）結果は、犯罪の目的と達成手段によって変わる。

次のシナリオで、もっと一般的なサイバー犯罪を説明しよう。セキュリティシステムが警告を発し、あるビルにだれかが適切な暗証番号を使わずに侵入したことを知らせたとする。警察が対応に駆けつけ、ドアが開いているのを発見する。さらに調べてみると、窓ガラスの一枚が割られ、内側からドアが開けられたことが判明した。ビルに入ったすぐのところにホームレスが寝ているのを警察が見つける。同じシナリオで、今度はホームレスがいるホールから奥のオフィスルームで明かりがついているのに気付いたとする。1台のコンピュータは電源がオンになっていて（他のコンピュータはすべてがオフなので不審である）、コンピュータのデスクトップにあるフォルダの1つが開いている。「2016年の合併」という名前のファイルが選択された状態で「コピー完了」というダイアログボックスが画面に表示されている。ホームレスに対する尋問で、ホームレスが屋外の寒さから逃れて安全に寝られる場所を求めてビル内に入ってきたときには、すでにドアが開いていたことが分かる。

どれも人騒がせな犯罪に聞こえるかもしれないが、残念ながら、これらはサイバー空間のTTP（Tactics, Techniques and Procedures：戦術、技術および手順）によって遂行される代表的な犯罪の種類である。

殺人や社会転覆、不法侵入、知的財産窃盗、恐喝など、あらゆる種類の犯罪がサイバー技術で可能となる。しかしながら、これらの犯罪が及ぼす影響の決定的要素となるのは、最終的に、犯罪の実行と結果におけるスコープである。すでに使えなくなったボットネットサービスへの加入を試行させる無差別なコンピュータ感染は、サイバー犯罪者が企業内のコンピュータに感染を広げ、ボットネットの無人操作機に仕立て上げて利用する標的型コンピュータ感染とは、まったく別物である。後者はサイバー犯罪者が情報を盗む、企業の業績データを盗聴する、企業システムへのアクセスをボットネットの登録利用者に販売するといったことを行う。また、コンピュータをボットネットに組み込むためのコンピュータ侵入は、ボットネットに利用者として登録し、そこで得た非公開情報をもとにインサイダー取引を行おうとする不正トレーダーとは異なる。

本章では、サイバー犯罪を理解し評価する際の「スコープ」の概念について説明する。また、犯罪の特性、（TTPで実行する目標を達成するための）標的決定の目的、公共組織と民間組織における考え方の違いも説明する。さらに、捜査・調査を指揮するための統制基準と、防衛と予防に関連する方針やシステム、手続きを、組織が定める上で参考となる情報を提供する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪にはどのような「特性」があるか
- サイバー犯罪が標的とする組織機能にはどのようなものがあるか
- そのような機能に対するリスクは、官と民の組織でどのように異なるか

第5章

証拠の情報源

サンプル

はじめに

「第 3 章 サイバー犯罪の犯行遺物」では、サイバー犯罪活動におけるステージおよび TTP（Tactics, Techniques and Procedures：戦術、技術および手順）に関係する兆候に基づいて、サイバー犯罪の犯行遺物について考察した。すでに述べたように、犯罪では必ず証拠が残る。証拠によっては、一般に公開されている情報源に残るものもある。なぜなら、サイバー犯罪はインターネット上の共有サービスを使って実行されることが多く、分散型の行動（他者に雇われて実行する行動や、組織的犯罪集団による行動）であったり、さまざまな形で繰り返されたりすることが理由で、使った TTP が、情報を共有する捜査官と分析員に見えてしまうからである。それ以外の証拠は、システムや従業員、関連の活動ログなど、内部（被害者）の情報源からしか得られないものである。

本章では、捜査官がサイバー犯罪のスコープ、影響、および行動を理解するために利用できる内外の証拠の情報源について考察する。この情報は、組織の意思決定者および管理職が防衛と予防に関する方針やシステム、手続きを決定するための監査と評価の基準を設ける際の助けとなる。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪を識別する証拠の情報源にはどのようなものがあるか
- 証拠は組織内外のどこで見つけることができるか
- 証拠の情報源別に、内容、信頼性、および構造はどのように異なるのか

第6章

証拠収集の手段

サンプル

はじめに

捜査官が情報源から証拠を収集する手段は、被疑者の嫌疑が何であるのかと同じくらい、場合によってはそれよりも重要である。証拠の収集または取り扱いが不適切であったために起訴がうまくいかなかった例は数多い。同じく、過去に集められた証拠をもとに関連犯罪の起訴が行われる例も多い。どのような種類の証拠を（また、どの情報源から）使えるかは、サイバー犯罪の特性とスコープ、攻撃手口（TTPs :Tactics, Techniques and Procedures：戦術、技術および手順）によって決まる。

本章では、各種のサイバー犯罪の特性とスコープ、TTP に応じて自動および手作業で証拠を収集する手段を検証する。また、犯罪のスコープと影響によってはサイバー犯罪が後に他の犯罪に関係する、あるいは、司法上の要件が存在する可能性があるため、サイバー犯罪の種類ごとの要件に関連する具体的な違いを検討する。たとえば、対人の犯罪は業務妨害や知的財産の窃盗とは異なるため、そのような違いについても見ることにする。

本章では、そのような要件に応じて効果的な証拠収集の手段を作り上げるための参照フレームワークを捜査官向けに提示する。さらに、防衛と予防に関連する方針やシステム、手続きを、組織の管理職が定める上で参考となる情報を提供する。

本章には分析のためにコンピュータから証拠を収集する手段の説明が含まれているが、これらの作業は適格な捜査官が行うものとする。また、複数の手段とツールについて説明しているが、本章は「インシデント対応」ガイドではない。本章は、これまでに述べた証拠の情報源から犯行遺物を収集する際の手助けとなることを主眼としている。サイバーセキュリティとサイバー犯罪捜査のトピックスは相互に関連するが、本章は IT 活動と捜査、すなわち証拠収集の違いを理解する上で読者の役に立つはずである。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の証拠はどのように収集できるか
- サイバー犯罪の証拠はどのように収集すべきか
- 証拠の信頼性を確保するにはどのような手段または手順に従うべきか
- サイバー犯罪の種類によって、証拠や関連手段はどのように異なるか

第7章

証拠分析の方法

サンプル

はじめに

本章「証拠分析の方法」は、サイバー犯罪捜査官が、偶然の一致として証拠を取り扱うのではなく、特定の検査によって証拠を集約し、分析するための方法を扱っている。

サイバー犯罪捜査においては、データサイエンスに基づく分析のコントロールが必要である。それは、テスト、品質保証、そして結果の開示を含む、効果的な証拠分析フレームワークの要件として定義する必要がある。

この知識領域によって、サイバー犯罪捜査官が、組織に関連するリスクと脅威を特定するために、サイバー犯罪における「範囲（Scope）」、「ステージ（Stages）」、「種類（Types）」のそれぞれを切り離して検討することが可能となる。またそれらには、「プロファイル（Profile）」、例えば「脅威アクター（Threat Actors）」（企業や組織へ脅威を引き起こす犯罪者）やそれらによって引き起こされる「活動（Activity）」に関する影響分析も含んでいる。

本章では、サイバー犯罪捜査官へ、証拠分析の効果的な方法を開発するために必要となる基準のフレームワークを提供する。

それはまた、管理職に対しては、防衛と保護に関する「政策（Policies）」、「システム（System）」、「手続き（Procedures）」を定義するための支援となる。

この知識領域は、3つのトピックスに分類されている。「第5章 証拠の情報源」、「第6章 証拠収集の手段」と密接に関係している。

サイバー犯罪捜査官にとって、利用可能な情報ソースから適切な証拠収集が重要であるように、証拠分析はサイバー犯罪の範囲を評価する上で重要である。

通常、捜査には制約がある。そこで、評価された範囲に従って、技術および他のリソースについて割当を行うべきである。

このとき、証拠分析における効率性と有効性とは、サイバー犯罪捜査の適切な実行と将来阻止すべき敵との差分もしくは、同様の（もしくはより凶悪化していく）サイバー犯罪からの苦しみと将来に向け用意したサイバー防犯設備の効果との差分である。

以上の点から、本章は、サイバー犯罪捜査における他のすべての側面との関係を持っており、本書の他のすべてのサイバー犯罪捜査官知識領域とリンクしている。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- どのようにサイバー犯罪の証拠分析のために、証拠を集約、分析すべきか
- どのように効率的なデータ管理と分析フレームワークを定義すべきか
- どのように分析結果を入力し、サイバー犯罪の範囲を関連付けすべきか
- どのような解釈が「脅威（Threat）」、「活動（Activity）」「脅威アクター（Threat Actors）」、「活動（Activity）」に関する影響分析となるか

第8章

最終処理

サンプル

はじめに

サイバー犯罪に対する効果的な対応とは何かを考えるときは、「どうすれば」事件を最終処理できるかだけではなく、「だれが」最終処理に関与すべきなのか、「いつ、どの時点で」関与するのかを考慮する必要がある。サイバー犯罪の最終処理を行うには、技術と手続きの両面で、組織的な取り組みとして評価や調査、理解、改善にあたることが求められる。不正アクセスに遭ったシステムを単に取り替えただけでは、効果的な最終処理とはいえない。最終処理への道のりは、事件が発生しないうちから始まっている。すなわち、組織において守るべき情報資産は何なのか、組織がどのようなリスクに直面していて、自己防衛にどれだけの時間とリソースを割く必要があるのかを前もって評価しておく必要がある。また、サイバー犯罪から組織を守り、対応できる体制を強化するにはどのような計画とテストが必要かも把握しておかねばならない。その上で、啓発や予防、捜査などの手段を通じて「通常の業務」における活動も守ることになる。

本章では、サイバー犯罪の捜査と対応に関係する役職と任務、アクション（処置）、手続きについて解説する。また、サイバー犯罪のスコープや犯行遺物、発生源、証拠が、組織または管轄地の方針に従って事件を最終処理する際のプロセスとどのように関わってくるかも説明する。サイバー犯罪の種類は多様であり、それによって生じる影響もさまざまである。したがって、捜査や最終処理の手法もそれぞれに異なる。

本章では、ベストプラクティスに加え、多くの管轄地で責任に関連して考慮すべき点とされる事項を踏まえながら、サイバーインシデントへの対応および脆弱性の修正に関する枠組み案を捜査官向けに提案として示す。さらに、防衛と予防に関連する方針やシステム、手続きを、組織の管理職が定める上で参考となる情報を提供する。

なお、本章で解説する問題や処置の多くは、管轄地によって法および規制上の取り扱いが異なるので留意されたい。本章は法律的な助言の提示を目的としておらず、その用途で参考とすることはできない。むしろ、本章の目的は、サイバーインシデントへの対応を行う場合に、犯行の内容を現地の適用法に照らし合わせて考慮すべき法的事項や実務的事項の概要を示すことにある。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪の捜査と最終処理の機能はどのように組織すべきか
- サイバー捜査と最終処理の各段階においてどのようなコミュニケーション手段と権限を確立すべきか
- サイバー犯罪の捜査と最終処理の計画に関与すべき人物および関与のタイミングとは
- 最終処理のために整備すべきツール類、人員、および手順とは

第9章

サイバー犯罪情報の共有

サンプル

はじめに

サイバー犯罪が行われると、その活動の証拠は通常、意図的（ウェブサイトの改ざん、機密情報の開示）、または不注意（センサー、マルウェアバイナリ解析によって記録されたIPアドレス）のいずれかで残る。法の執行機関、または他の捜査機関が犯罪に最初に対応する際には、特に攻撃者が自分たちの痕跡を隠そうと高度な技法を用いている場合や、本来の活動がそれ以前に始まっている場合には、利用可能な当初情報は少ないと考えられる。整然としたインシデントレスポンス（IR: Incident Response）プロセスに従い、確実に分析過程の適切な管理を行い、これまでの章で触れてきたフォレンジックやIR手法を用いることで、付加情報や証拠が浮かび上がる。当該データには、攻撃者が使用した戦術（Tactics）、手法（Technique）、手順（Procedure）と併せて、原因の特定（犯罪に関わる個人、またはグループの特定）や動機の理解、解明に役立つ情報が含まれている場合がある。

その証拠は、今後の事案や分析・起訴の効率向上のために捜査官が経験を積むには役に立つ。今日の知識、スキル、リソース（インフラさえも）、そしてサイバー犯罪組織の「共有（シェアリング）」エコノミーが背景となっているため、1か所の犯罪現場で見つかった犯行遺物だけでは、サイバー犯罪者の特定、または効果的な起訴を可能にするには十分とは言えないようである。これが、情報共有がサイバー犯罪捜査において極めて重要であるとする1番の理由である。情報共有を行えば、対応できていた可能性のある初期活動段階での犯行遺物や検知指標を特定して、以降の犯罪を防ぐことができるかもしれない。特定の種類の犯罪は、プライバシーへの配慮や、起訴に向けた付加証拠検出に極めて重要な調査上の詳細であることから、共有できる情報の種類をやむを得ず制限する必要がある。つまり、サイバー犯罪の阻止に実際に役立つと言えども、情報がすべて共有できるわけではないということである。

本章では、サイバー犯罪の情報共有における手法、および関連する制限事項について触れている。特に、犯罪種類別の管轄地や分類の制限事項、開示担当の当局、および関連情報の共有について解説している。また、共有する情報の文書化や必要条件、および共有の時間軸や目的についてもガイダンスを示している。本章では、当該要件に基づいた情報共有のための参照フレームワークが記されている。さらに、本章は組織のマネージャにとっては、防御や保護における関連する方針、システム、そして手順の決定にも役立つようになっている。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪情報を共有する理由は何か
- サイバー犯罪情報を、内部および外部と共有する理由は何か
- どのような要件が、いつ共有する情報の種類を左右するか
- どの場所で、どのようにサイバー犯罪情報を共有すべきか

第10章

管理フレームワーク

サンプル

はじめに

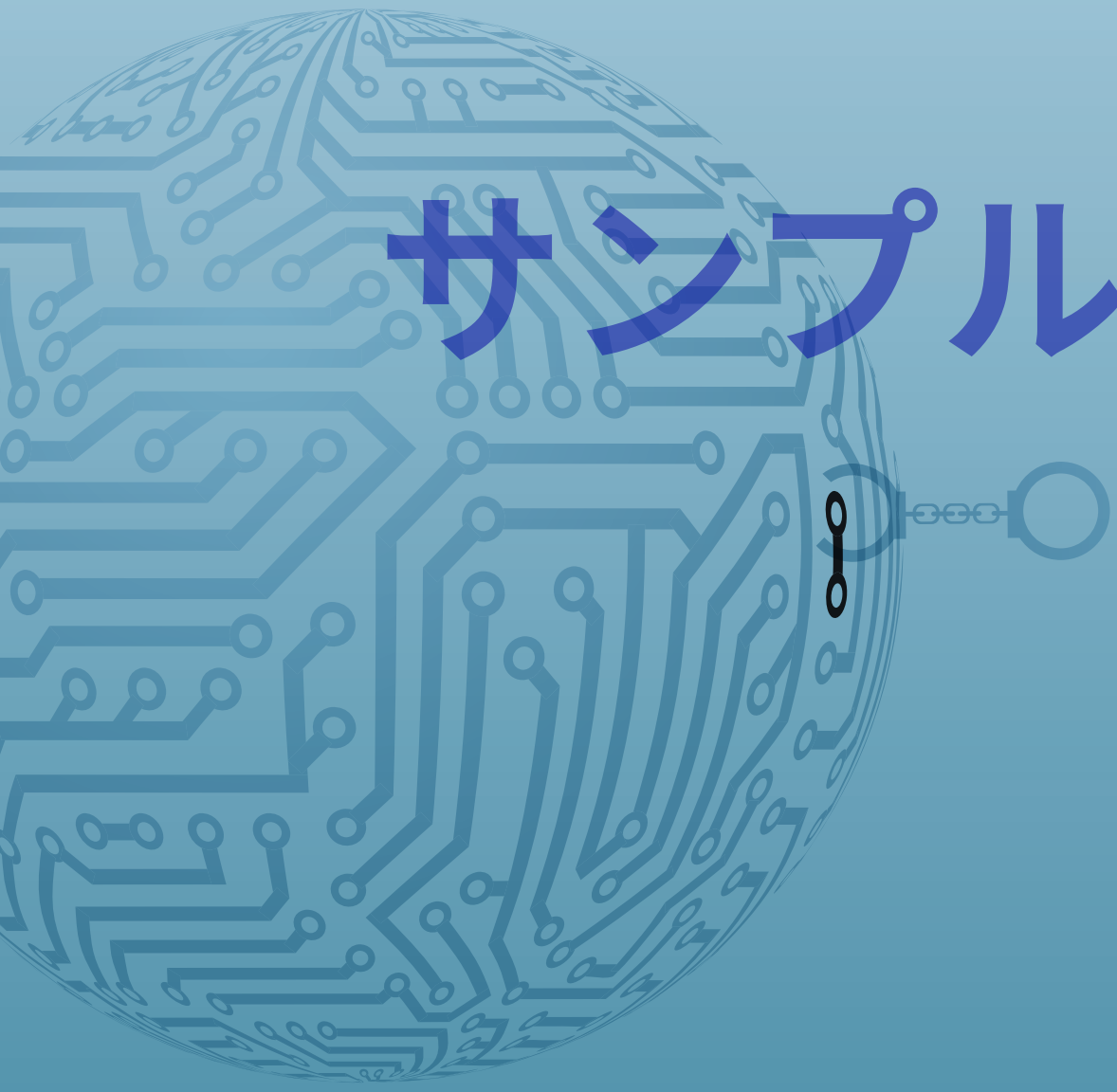
官民に関係なく、どのような組織であってもリソースには限りがあり、その中で各種機能とそれに関連する手続きを支えている。リソースは規模の効率と応用の範囲を考えて管理しなければならない。組織にとって、サイバー犯罪におけるインシデント対応や調査、最終処理は比較的新しい活動であって、これまでは（経理や総務、情報サービス、顧客サポートのように）一般的な機能として設置されていなかった。

本章では、サイバー犯罪捜査機能の管理フレームワークを構成、計画および実行するための構造と枠組みについて説明する。これまで、情報サービスは組織の各機能を支援するように拡大し、管理フレームワークは各種の手順やツールを発展させてきた。サイバーツールあるいはサイバー型攻撃手口を使った犯罪の登場は組織にとって新しい局面であるが、組織はこれに対応し、サイバー犯罪の調査や予防に取り組み、関連手続きやツールを定める必要がある。階層型およびマトリックス型の組織構造は、サイバー犯罪捜査の機能と人員によって実行される活動と対応させて説明する。

本章では、そのような要件に応じて効果的に証拠を収集する方法を作り上げるための参照フレームワークを捜査官向けに提示する。さらに、防衛と予防に関連する方針やシステム、手続きを、組織のマネージャー職が定める上で参考となる情報を提供する。

本章で解説する内容の習得により、読者は次の理解を得ることができる。

- サイバー犯罪捜査および最終処理の機能の目的は何か
- 本機能はどのように組織し、管理すべきか
- 本機能の戦略的な目標は何か
- 本機能のリソースにはどのような要件があるか（スタッフ、ツール、およびコミュニティ）
- 本機能のスタッフ割り当て、管理、指導 / 統制にはどのような技術的・経験的要件があるか
- 本機能（およびそのスタッフ）のパフォーマンスはどのように測定すべきか
- 組織をうまく機能させるには、どのような組織コミュニケーションと戦略的関与を、組織のどのチャネルに組み込むべきか
- サイバー犯罪捜査および最終処理の機能は組織のどの幹部機能の配下とすべきか



サンプル