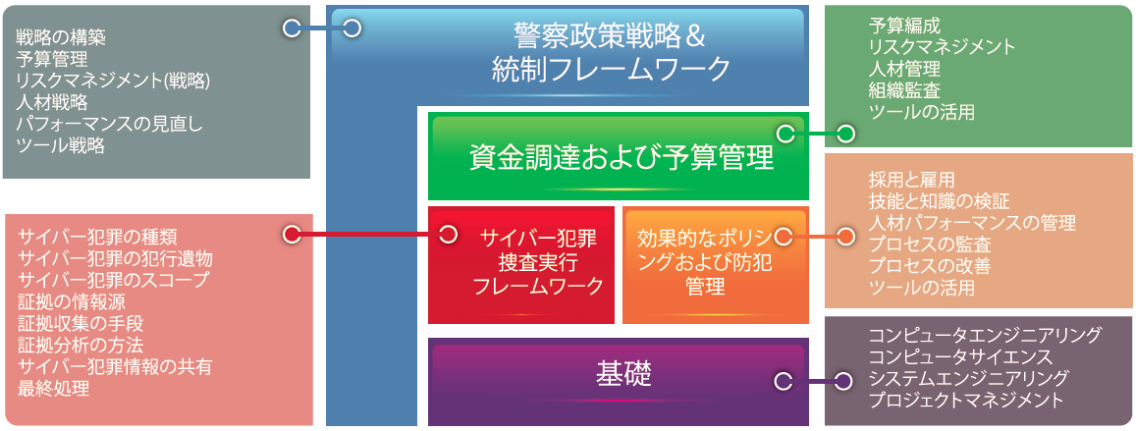
プロフェッショナル・トレーニング・コース

- Cybercrime Investigation Body of Knowledge -

(第 1 版©)



概要

インターネットの利用が拡大するにつれ、コミュニケーション、システム制御、情報共有が急速に促進されてきました。このメリットは、社会や商業活動の成長を促し、情報サービスへのほぼリアルタイムでのアクセスを可能にする大きな機会を生み出しました。

この成長は、その反面として、同様のサービスのメリットを悪用し、窃盗、詐欺、脅迫といった従来の犯罪を、革新的な方法を用いることで、より広範囲そして大規模に行おうとする犯罪者の台頭を引き起こしています。またこれまでのような、一匹狼の犯罪者が自身の能力を誇示することを目的とし、個人的なメリットを追求する犯罪行為は、今日、組織的な犯罪活動にとって代わられてきています。

これらのような犯罪活動は、従来の調査手法では追いつかないほどのスピードで、かつ匿名性をもって行われています。このような課題に対抗することを目的に、法執行機関の捜査官や検察官、企業のインシデント・レスポンスの担当者、リスク・マネジメントにかかわる経営層のコラボレーションによって、(犯罪に対抗するための)捜査や反応に関する法執行機関と企業の認識やアプローチを統一させる「シーボック(CIBOK：Cybercrime Investigation Body of Knowledge)が生み出されました。

プロフェッショナル・トレーニング・コース

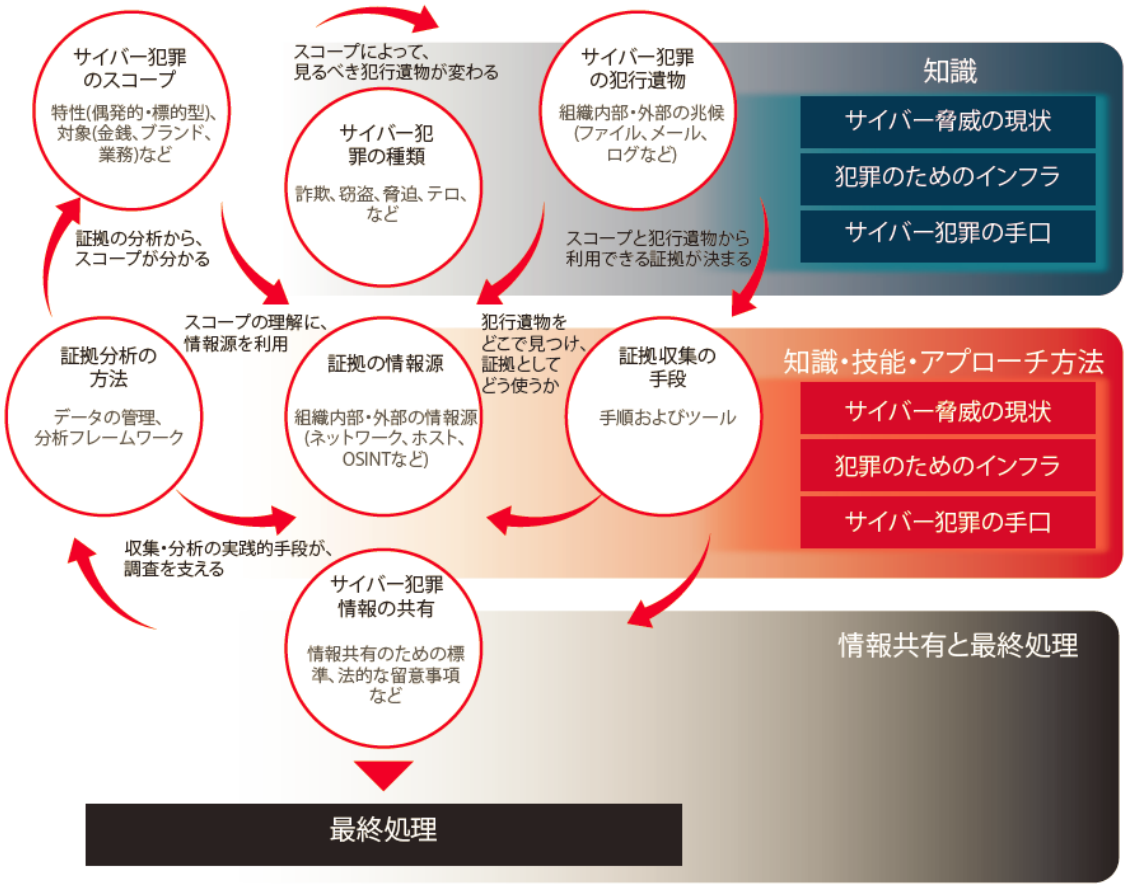
- Cybercrime Investigation Body of Knowledge -

(第 1 版©)

目的

CIBOK では、どのようにサイバー犯罪を特定し、適切に反応するかを理解するために、法執行機関の捜査官や企業のセキュリティ担当者が必要とされる知識、能力、技術の概要を、以下の目的に沿って提供します：

1. 各国の法律に依ることのない全世界で一貫したサイバー犯罪に関する心得（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、特徴づけして示すこと
4. サイバー犯罪捜査知識体系に対して、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



プロフェッショナル・トレーニング・コース

- Cybercrime Investigation Body of Knowledge -

(第 1 版©)

本コースに含まれるトピック：

この 5 日間コースでは、インタラクティブな実習を交え、以下のトピックの詳細を提供します：

- CIBOK の紹介
- サイバー犯罪とその調査
- サイバー犯罪の分類
- サイバー犯罪の犯行遺物(Artifact)
- サイバー犯罪のスコープ
- サイバー犯罪に関連するリスクおよびコンプライアンス
- 証拠の情報源
- 証拠収集の手段
- 証拠分析の方法
- インシデントの解決
- サイバー犯罪に関する情報共有
- マネジメント・フレームワーク

このコースの対象となる受講者

このコースは、法執行機関の捜査官、検察官、またはサイバー犯罪に関するリスクおよびコンプライアンスの評価や軽減措置に責任を有する、企業における監査実施者、インシデント対応担当者向けの、導入コースとして設計されています。

このコース受講者への配布物

受講時にはシーボックの第 1 版、コースマニュアル、参考資料を配布します。

講師について

シェーン・シュック博士（*Shane Shook , Ph.D.*）は、セキュリティやセキュリティの問題への対応に従事し、政府や企業の問題に、広く 30 年余りの経験を有しています。博士は、金融サービス、医療、小売、サービス業、交通、自動車、エンターテイメント企業や政府といったシステムに対する凶悪な侵害事案に対して、フォレンジックによる分析を主導、専門家としての意見を提供するとともに、国家の活動、市民生活および商業活動に関するさまざまな議論に関しても、専門家としての提言をおこなう経験を有しています。また現在博士は、新興のセキュリティ技術企業の顧問としても活躍しています。

プロフェッショナル・トレーニング・コース

- Cybercrime Investigation Body of Knowledge -

(第 1 版©)

トピック	トレーニングによる効果
1-2 日目：知識の習得 • CIBOK の 5 つの目的 • CIBOK とは？ - 攻撃対象としての技術 - 攻撃道具としての技術 - 攻撃から目をそらす手段としての技術 • サイバー犯罪の捜査とは？ - With evidence of data/other loss - Without evidence of loss • サイバー犯罪調査における課題とは？ - 管轄権と裁判が行われる場所 - 人権とプライバシー • サイバー犯罪捜査のための能力開発として必要なスキル、知識、経験は何か？	サイバー犯罪の認識、調査に従事するに際して、実例を介して、サイバー犯罪の種類、スコープ、犯行遺物およびアプローチを理解することができるようになる。 司法上の注意点、国際的なプライバシーの壁を意識した情報共有を含む。 ケース例： - 小売業/POS での情報漏えい - IT 業界/政府での個人情報の窃盗 - 医療/政府でのデータ窃盗 - 銀行 ATM/支払ネットワークでの窃盗 - Securities Fraud - SNS/サービスでの窃盗および詐欺

一般にサイバー犯罪の種別に関する組織内関係者による理解を促進することを目的としてはいるものの、サイバー犯罪のスコープやコミュニケーションの方法、組織上層部が必ず行わなくてはいけない意思決定を知るうえで、知識の習得は依然捜査官、分析官にとって重要な基盤となるものです。

主要な捜査官や部門管理者に加えて、組織上層部の関係者にもこのトレーニングに参加することをお勧めします。またサイバー犯罪に関する戦略的な予防、発見、捜査に、自身の業務がどのように関連するかを理化するためにも、捜査官や分析官の皆様にも、このトレーニングに参加することをお勧めします。

知識習得を目的としたこのトレーニングの最後には、実世界のサイバー犯罪に関連した、机上での演習が含まれます。

プロフェッショナル・トレーニング・コース

- Cybercrime Investigation Body of Knowledge -

(第 1 版©)

トピック	トレーニングの効果
3 日目-5 日目：スキルの開発 • サイバー犯罪における「証拠」と「犯行遺物」は？ • 証拠の情報源とは？ • 証拠収集の手段とは？ • 証拠を捜査または裁判で利用する際の注意点とは？ • サイバー犯罪の証拠分析の手段とは？ • サイバー犯罪を事前に発見、防止するために利用可能な情報源とは？ • サイバー犯罪に関する情報を共有する際の注意点とは？ • サイバー犯罪捜査のために組織に求められる最低条件とは？ • サイバー犯罪捜査のための人員を育成するために、どのようなツールやトレーニングが利用可能か？	サイバー犯罪捜査を実施するに際して、実践的な要件を理解することができるようになる。 異常な活動から、サイバー犯罪を認識(および判別)し、分析のための証拠収集と取り扱いができるようになる よく利用される専門家向けのツールを利用した、効率的な収集、処理、分析手法も含む。 ディスカッションを目的として、関連する実習(および実例)を踏まえた技術的なデモンストレーション。

スキル開発のためのトレーニングでは、参加者の皆様に、サイバー犯罪捜査を行う際に証拠の情報源について考慮すべき点を提供することを目的としています。ここでいう情報源には、脅威に関する知識、業界や法執行機関の持つ知識、インターネット上の有償またオープンソースの情報、ダークウェブやディープウェブに関する議論といったものが含まれます。その他の情報源としては、セキュリティ調査による検体、ネットワーク、ファイル、OS、メモリから収集された証拠も含まれます。証拠収集のための手段、処理、分析についても、適切な文書化、保管・管理に重点を置いて解説されています。

技術に特化している、していないにかかわらず、サイバー犯罪の捜査官および部門管理者の方には、このトレーニングに参加し、スキル、ならびにサイバー犯罪捜査の機能、人員配置の件について理解することをお勧めします。

スキル習得のためのこのトレーニングには、技術的な分析の演習が含まれています。