CIBOK(Cybercrime Investigation Body of Knowledge)

サイバー犯罪捜査知識体系

Cybercrime Investigation Body of Knowledge

CIBOK(Cybercrime Investigation Body of Knowledge)は、サイバー犯罪捜査におけるナレッジに関するガイドです。CIBOKでは、サイバー犯罪捜査の実施に際して一般的に習得が必要な知識、技能、アプローチ方法、そして捜査に必要な組織構成などを、8つの知識領域に体系立てて分類し、紹介しています。

CIBOK(シーボック)の内容と活用メリット

- 各国の法律に依ることのない、全世界で一貫した
  サイバー犯罪捜査に関する心得(コモン・センス・アプローチ)を紹介

  ・捜査官からのヒアリングに基づいて特定された、実践的な需要を体系化
  ・世界各国の現場従事者が参加している開発プロセス(企画、執筆、レビュー)

- 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など、
  すでに体系化されている実務慣行をサイバー犯罪捜査で活用する際の位置づけを紹介

  ・サイバー犯罪捜査に必要な知識、技能、アプローチ方法を紹介
  ・さらに紹介した知識、技能、アプローチ方法を、サイバー犯罪捜査に当てはめて「分類」

- 実務で使われている知識、技能を職務に分類して紹介することで、
  トレーニングカリキュラム開発および、サイバー犯罪捜査にかかわる個人の知識とスキルの
  客観的な理解を後押し

  ・職位レベルごとに要求される「専門性」と「重要度」を定義
  ・磨くべき知識や技能を明確に紹介

CIBOKの8つの知識領域

- サイバー犯罪の種類
- サイバー犯罪の犯行遺物(Artifacts)
- サイバー犯罪のスコープ
- 証拠の情報源
- 証拠収集の手段
- 証拠分析の方法
- 最終処理
- サイバー犯罪情報の共有
- 管理フレームワーク

サイバー犯罪捜査におけるCIBOK活用例

全世界共通のサイバー犯罪捜査に関する心得

- サイバー犯罪における活動の「ステージ」に加えて、ディープウェブ、ダークウェブといった犯行遺物の情報源について、サイバー犯罪にかかわる組織全体で共通の認識をし、サイバー犯罪の証拠、犯罪の兆候を、組織全体で、効率的に収集する。

体系化されている実務慣行をサイバー犯罪捜査で活用

- 限られた資源で効率よくサイバー犯罪捜査を進めるために、「一層」、「調査」、証拠の「収集」による、トリアージ型の証拠収集を行う。

個人の知識とスキルの客観的な理解

- サイバー犯罪捜査における「説明責任(Judiciary)」の担当者には、サイバー犯罪の犯行遺物、スコープ、証拠の情報源、収集手段、分析方法についてそれほど高い知識は要求されないが、「知見収集(Intelligence)」、「調査(Investigation)」担当者は、ともに犯行遺物や証拠に関する高い知識が要求される。

CIBOK(Cybercrime Investigation Body of Knowledge)

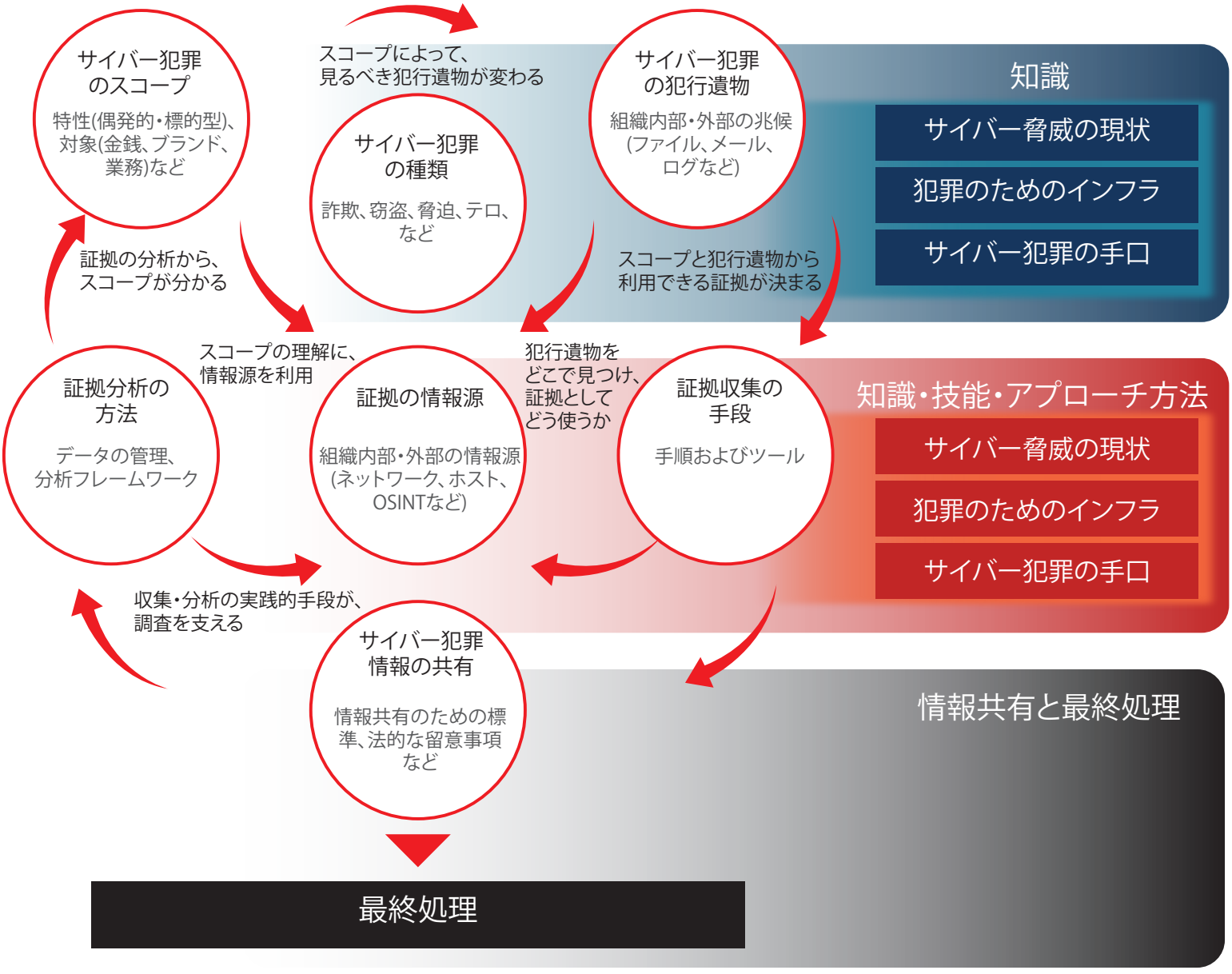
実行フレームワーク

サイバー犯罪捜査の実行フレームワークは、CIBOKの重要な一部を構成しています。

実行フレームワークでは、すでに体系化され、実績のある実務慣行や、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といった知識を、サイバー犯罪捜査に当てはめてサイバー犯罪捜査のプロセスに基づいて分類しています。

CIBOK(シーボック)の活用メリット

- 実行フレームワークは、サイバー犯罪の種類を判別することから始まる
- どの工程からも着手できる。
- 各工程の関連性を俯瞰できる。
- 他の工程からのフィードバックにより、自らの工程の見直しが柔軟にできる。



www.cibok.org
詳細・ご購入のお問い合わせはこちらまで: secretariat@cibok.org
Copyright © CIBOK Editorial Committee. All Rights Reserved.
記載内容は2017年7月現在のものです。
内容は予告なく変更になる場合がございます。