Cybercrime Investigation Body of Knowledge

# トレーニングコースの紹介

## サイバー犯罪調査・捜査を目的とした知識の習得およびスキル開発トレーニング

サイバー犯罪捜査知識体系 (CIBOK) では、サイバー犯罪捜査で実行すべき活動を 8 つの知識領域に分類しています。
本トレーニングは、法執行機関や企業のセキュリティ担当者がサイバー犯罪調査に際して必要とされる、サイバー犯罪をどのように認識、対応、調査・捜査するかといった知識、スキル、技術の概要を習得するために設計されています。

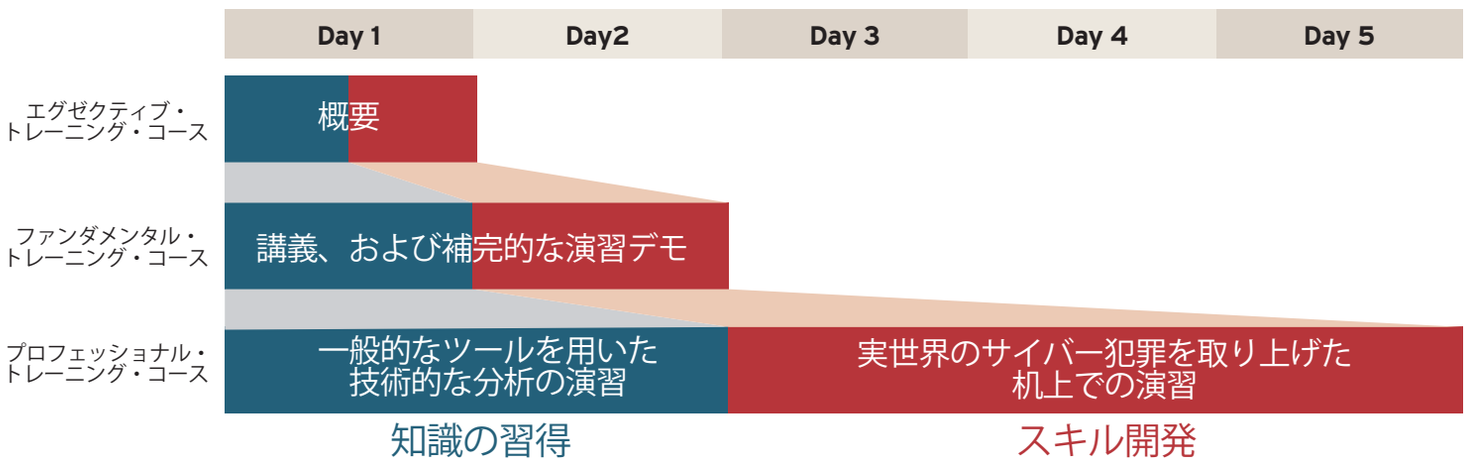
**▶本コースの受講対象者**

- 法執行機関の捜査官や検察官、または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の評価や軽減措置に責任を有する、企業におけるサイバーセキュリティ担当者や管理者。
- 上記捜査官や検察官、担当者を有する組織の CIO、CISO および経営管理者。

## 本トレーニングコースを受講するメリット

- 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（コモン・センス・アプローチ）の習得が可能。
- 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など、すでに体系化されているその他の実務慣行をサイバー犯罪捜査活動で活用する際の位置づけを理解することが可能。
- サイバー犯罪捜査において実践すべき内容を 8 つの知識領域で具体的に理解可能。
- 8 つの知識領域に関する項目については、詳細を理解するための豊富な参考文献を紹介。
- トレーニングカリキュラム開発および、サイバー犯罪捜査業務に携わる個人の知識とスキルを客観的に理解できるようになる。

## 本トレーニングのレベルと期間



Cybercrime Investigation Body of Knowledge

# トレーニングコースの紹介

## エグゼクティブ・トレーニング・コース

### 知識とスキルに関するハイレベルの紹介：5 時間

| | |
|---|---|
| CIBOK の紹介<br>サイバー犯罪とその調査<br>サイバー犯罪の分類<br>サイバー犯罪の犯行遺物<br>サイバー犯罪のスコープ<br>証拠の情報源<br>証拠収集の手段<br>証拠分析の方法<br>インシデントの解決<br>サイバー犯罪に関する情報共有<br>マネジメント・フレームワーク | 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の評価および軽減措置に責任を有する業務実施に際して必要な知識の概要を紹介。<br>Q&A を含む。 |


## ファンダメンタル・トレーニング・コース

### Day 1：知識の習得

| | |
|---|---|
| CIBOK の 5 つの目的<br>CIBOK とは？<br>サイバー犯罪の捜査とは？<br>サイバー犯罪捜査における課題とは？<br>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？ | ▶裁判に際しての配慮事項、および個人情報の取り扱いに関する国家間の違いに配慮した情報共有を含む。 |

### Day 2：スキルの開発

| | |
|---|---|
| サイバー犯罪における「証拠」と「犯行遺物」とは？<br>証拠の情報源とは？<br>証拠収集の手段とは？<br>証拠を捜査または裁判で利用する際の注意点とは？<br>サイバー犯罪の証拠分析の手段とは？<br>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？<br>サイバー犯罪に関する情報を共有する際の注意点とは？<br>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？<br>サイバー犯罪捜査官の育成のために利用可能なツールやトレーニングとは？ | ▶サイバー犯罪の分析を目的とした、異常な活動からのサイバー犯罪の認識（および判別）。証拠収集の手段および証拠の取り扱い方法。<br>▶一般的な専門ツールを活用した、効果的な証拠収集、取り扱い、および分析の手段。<br>▶参加者による議論を引き出すことを目的とし、技術的なデモも実施。 |

## プロフェッショナル・トレーニング・コース

### Day 1-2：知識の習得

| | |
|---|---|
| CIBOK の 5 つの目的<br>CIBOK とは？<br>サイバー犯罪の捜査とは？<br>サイバー犯罪捜査における課題とは？<br>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？ | ▶小売業 /POS での情報漏えい<br>▶IT 業界 / 政府での個人情報の窃盗<br>▶医療 / 政府でのデータ窃盗<br>▶銀行 ATM/ 支払ネットワークでの窃盗<br>▶SNS での ID 窃盗および詐欺 |

### Day 3-5：スキルの開発

| | |
|---|---|
| サイバー犯罪における「証拠」と「犯行遺物」とは？<br>証拠の情報源とは？<br>証拠収集の手段とは？<br>証拠を捜査または裁判で利用する際の注意点とは？<br>サイバー犯罪の証拠分析の手段とは？<br>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？<br>サイバー犯罪に関する情報を共有する際の注意点とは？<br>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？ | ▶サイバー犯罪の分析を目的とした、異常な活動からのサイバー犯罪の認識（および判別）。証拠収集の手段および証拠の取り扱い方法。<br>▶一般的な専門ツールを活用した、効果的な証拠収集、取り扱い、および分析の手段。<br>▶演習や事例を含む、技術的なデモ。 |

www.cibok.org
トレーニングの詳細・お申込みのお問い合わせはこちらまで：secretariat@cibok.org