Cybercrime Investigation Body Of Knowledge

ファンダメンタルトレーニングコース（2日間）

コース概要

日々進化が著しいサイバー犯罪の捜査、調査に際して、法執行機関、民間のCSIRTが、それぞれの立場で正しく、組織的に事件に対応することを目的とし、共通のフレームワークに立脚して必要な知識とその本質を理解できる研修コースです。この研修を受講することで、サイバー犯罪に関連する様々な領域について、その概要を効果的に学ぶことができるようになります。

コース内容

CIBOK 第1・2章　サイバー犯罪とその捜査, サイバー犯罪の種類

- サイバー犯罪の定義
- サイバー犯罪者・犯罪組織のプロファイルとその背景

CIBOK 第3・4章 サイバー犯罪のアーティファクト、犯罪のスコープ

- サイバー犯罪のIoC（Indicator of Compromise)と内部・外部の犯行遺物
- サイバー犯罪の特性とその影響範囲

CIBOK 第5・6章 証拠の情報源・証拠の収集方法

- 証拠の情報源
- 証拠の収集手段

CIBOK 第7章 証拠分析の方法

- 証拠分析フレームワーク

CIBOK 第8章 最終処理

- サイバー事件の「最終処理」とは
- 最終処理に必要な組織、コミュニケーション、ツール、手続き

CIBOK 第9章 サイバー犯罪情報の共有

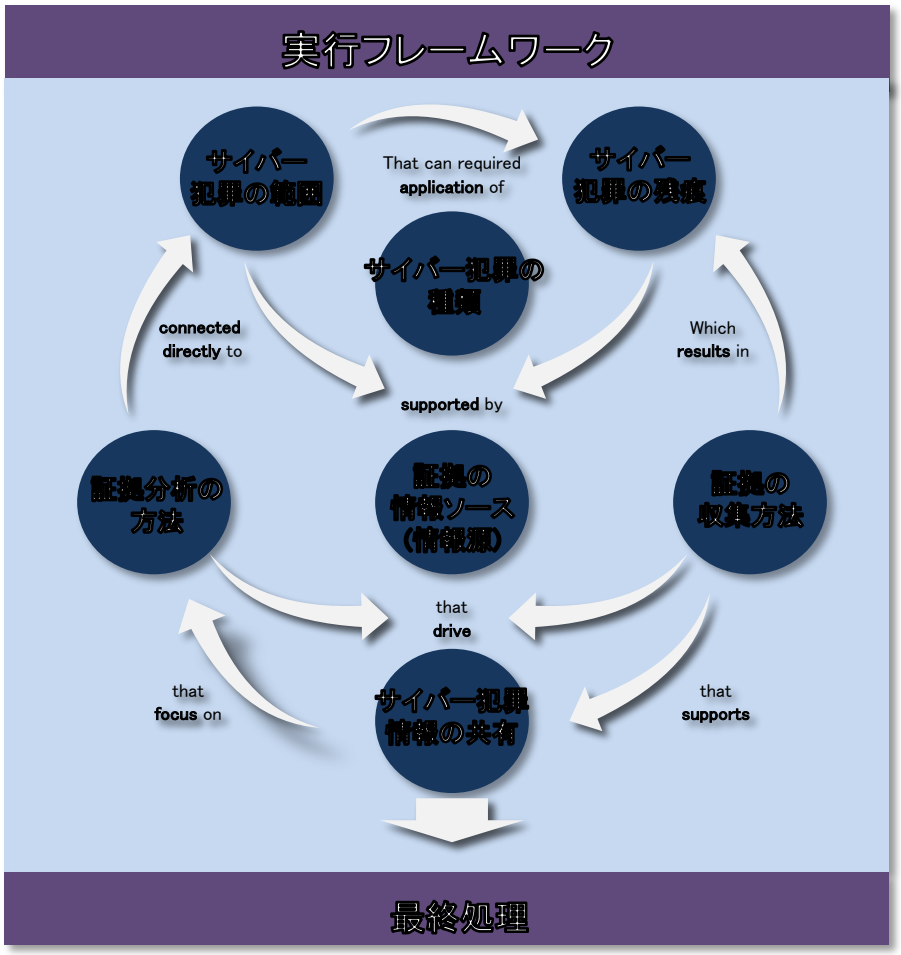
- サイバー犯罪の情報共有とは
- 情報共有方法と法的留意事項

学習目標

- 捜査官・調査官がサイバー犯罪の対処に必要な知識領域を理解することができる。
- 受講者自らの知識とのギャップを把握し、継続的かつ効果的な学習計画を立案できる。
- 所属する組織におけるサイバー犯罪及びサイバー空間の捜査能力の査定、再評価、及び改善指示が実施できる。
- 法執行機関と被害者となる組織の適切な連携のあり方を理解し、現行プロセスの改善計画を立案できる。

Cybercrime Investigation Body Of Knowledge
ファンダメンタルトレーニングコース（2日間）

本コースで扱うフレームワーク



本フレームワークは、捜査員・調査員がサイバー犯罪の正しい処理を行う上で必要になる8つの要素とその関係性を示します。各要素を理解することで、サイバー犯罪捜査の過程で必要となる知識領域とその本質を効果的に習得できます。

対象者

- サイバー関連部門における捜査員・調査員
- 法執行機関における捜査官・調査官

前提条件

- Windowsの基本操作が出来る方、あるいは同等の知識をお持ちの方。
- Windowsの基本操作が出来る方、あるいは同等の知識をお持ちの方。
- このコースでは詳細な技術知識は必要ではありませんが、ネットワークおよび情報セキュリティについての基礎知識を持たれている事をお勧めします。

お問い合わせ先：一般社団法人 サイバー犯罪捜査・調査ナレッジフォーラム secretariat@cibok.org