# はしがき

本書は、教育システムデジタルブックサービス「HONTATE」でデジタル書籍として発売している「サイバー論文集」について、紙書籍を手元において学習したいという多くのご要望をいただき、このたび、増補版として発行したものです。

本書では最新の法改正やサイバー情勢に合わせて内容を増補するとともに、理解を助けるイラスト等を追加しました。簡潔にまとめた答案例に加えて一問一答を収録し、昇任試験の対策だけでなく知識の整理、確認にも活用できる内容となっています。

巧妙・複雑化するサイバー犯罪は、ますます重要な課題の一つとなっており、最近の昇任試験ではサイバー警察科目の設置が検討されたり、全国的にサイバー犯罪等対処能力検定の取得に力を入れたりするなど、若手からベテランまで、サイバーに関する幅広い知識と理解が求められています。本書が、昇任試験対策はもちろん、検定試験対策や日々の実務に役立つ一冊となれば幸いです。

令和８年８月

株式会社　教育システム

代表取締役社長　松﨑　基子

# CONTENTS

## 生活安全

### 論文問題



### 確認一問一答

## 警　　備

### 論文問題

## 12 不正アクセス事犯の捜査要領について述べなさい。

## 不正アクセス事犯の捜査要領

### 1 利用権者からの事情聴取

不正アクセスされた状況等について聴取する。

### 2 アクセス管理者の特定

不正アクセスされたウェブサイトのURL等からアクセス管理者を特定する。

### 3 ログイン記録の照会・精査

⑴ アクセス管理者に対し、ログイン記録を照会する。

⑵ ログイン記録のIPアドレスからWHOIS検索を利用してプロバイダを特定する。利用権者が利用しているプロバイダ以外からログインされたものは不正アクセスとなる。

⑶ ログインが失敗している場合は、不正アクセス行為に該当しない。

### 4 プロバイダに対する差押え等

プロバイダに対する差押え等を実施し、契約者情報を入手する。

### 5 基礎捜査

プロバイダから差し押さえた契約者情報を基に、契約者の身辺捜査等の基礎捜査により、被疑者を絞り込む。

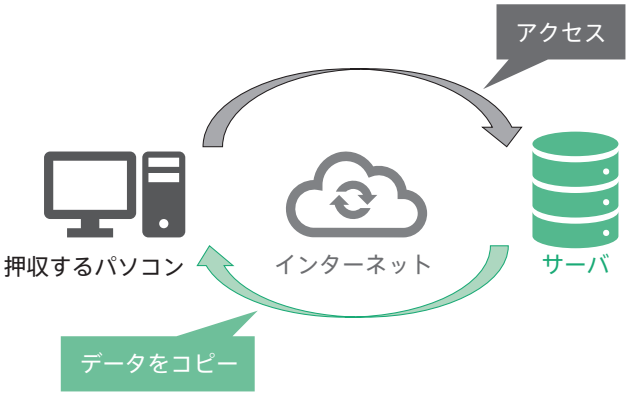
## 6　被疑者の居宅等の捜索・差押え

被疑者の居宅等の捜索・差押えを実施し、パソコン、電磁的記録媒体、周辺機器のみならず、犯行の手口や動機を裏付ける関連書籍等を差し押さえる。

### Step Up

#### リモートアクセスによる差押え

リモートアクセスによる差押えとは、捜索・差押え実施時に、外部サーバ等に差し押さえるべきデータがある場合、捜索場所にある差し押さえるべきパソコン等からネットワークを介して、当該外部サーバ等に接続し、データを複写して差し押さえる処分である（刑訴法218条２項）。



# 確認一問一答

## 1 サイバー攻撃の意義と特徴

(1) サイバー攻撃とは、サイバー事案と重大サイバー事案の総称をいう。

(2) サイバー攻撃には、攻撃の被害が潜在化する傾向があるなどの特徴がある。

## 2 サイバーテロとサイバーエスピオナージ

(3) サイバーテロとは、情報通信技術を用いた諜報活動のことをいう。

(4) サイバーエスピオナージとは、重要インフラの基幹システムに対する電子的攻撃、又は重大な障害で電子的攻撃による可能性が高いものをいう。

(1) × (2) ○ (3) × (4) ×

## 3 サイバー攻撃の主な手法

(5) DDoS攻撃とは、特定の組織や個人を標的とし、不正プログラムを添付したメールを送信して感染させる手法である。

(6) SQLインジェクション攻撃とは、SQLというプログラム言語を用いて、企業等が管理するデータベースを外部から不正に操作する手法である。

## 4 サイバーキルチェーン

(7) サイバーキルチェーンとは、攻撃者が標的を決定し、実際に攻撃して目的を達成するまでの行動を5つのフェーズに分類したものである。

(8) サイバーキルチェーンにより攻撃者の行動パターンを知ることができ、各フェーズで対策を立てることが可能になる。



(5)× (6)○ (7)× (8)○