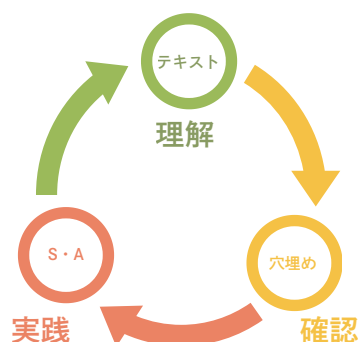


ゼロから始めるサイバー犯罪捜査テキスト —穴埋め&S・A問題—

昇任試験や検定で問われるサイバー犯罪捜査に関する知識等について、図表を交えながら基礎から解説

✓合格への3つのサイクル



- ◇テキスト編と問題編の2編で構成
- ◇問題編は、穴埋め問題とS・A問題を収録
- ◇「テキスト」「穴埋め」「S・A」のサイクルにより、効率的に合格力を養成できます。

✓テキスト編の特徴

サイバー犯罪捜査に関する知識等を簡潔にまとめているため、繰り返し目を通すことで知識の定着（インプット）が図れます。

✓問題編の特徴

◇穴埋め問題（計100問）

穴埋め問題は、文脈を手がかりに重要キーワードを思い出す学習ができ、記憶の検索力（アウトプット力）が鍛えられます。

◇S・A問題（計24問）

S・A問題は、実際の試験と同じ形式で問題を解く学習ができ、実践力の向上が図れます。

✓「昇任試験対策 サイバー論文集」との併用がおすすめ！

「サイバー論文集」と併せて学習することで、サイバー攻撃に関する知識等もカバーでき、得点力アップにつながります。

※本書は、ご購入いただいた日から2年間閲覧が可能です。

収録内容一覧

1.サイバー犯罪の概要

- 1 サイバー犯罪の種類
- 2 サイバー犯罪に該当する犯罪
- 3 サイバー犯罪の特徴

2.インターネットの基礎知識

- 1 インターネット
- 2 プロバイダ
- 3 IPアドレス
- 4 URL
- 5 ドメイン名
- 6 WHOIS検索

3.サイバー犯罪捜査の基本的な流れ

- 1 サイバー犯罪捜査の基本的な流れ
- 2 サイバー犯罪認知時の措置等
- 3 サイト管理者に対する照会
- 4 プロバイダの特定
- 5 プロバイダからの差押え
- 6 被疑者の特定
- 7 検索・差押え
- 8 リモートアクセスによる差押え

4.不正アクセス禁止法違反の捜査要領

- 1 相談受理要領
- 2 ログイン記録の照会
- 3 ログイン記録の解析
- 4 不正アクセスによるログインの特定
- 5 アクセス管理者からの聴取
- 6 所要の捜査

5.その他捜査要領

- 1 電子メール利用事件の捜査要領
- 2 SNS利用事件の捜査要領
- 3 外国の捜査機関に対する捜査共助の要請

6.証拠品の解析等

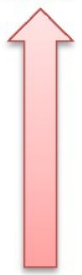
- 1 証拠品の保管・管理
- 2 電磁的記録媒体の解析
- 3 スマートフォンの解析

テキスト

4 メールヘッダの読み解き方

【メールヘッダの例（抜粋）】

宛先

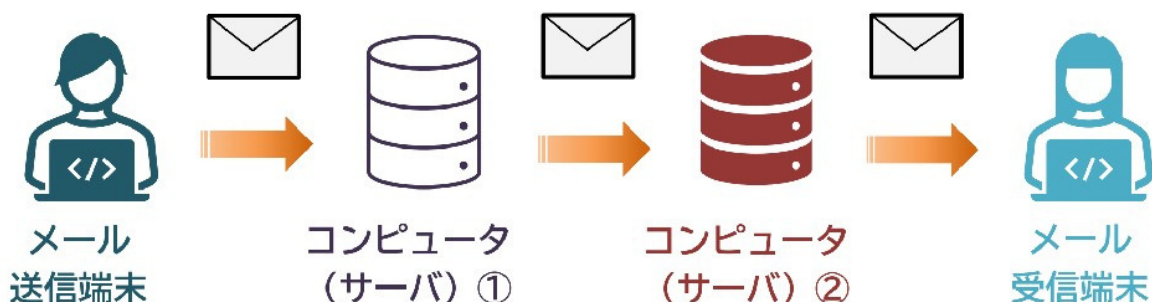


送信元

```
Received: from sample.ocn.ne.jp(sample.ocn.ne.jp[192.0.2.1])  
by example.biglobe.ne.jp(Postfix) with ESMTP id DAA08171  
for<hon@tate.com>;Mon, 12 May 2028 10:15:30 +0900(JST)  
Received: from aaa39(aaa39.ocn.ne.jp[210.130.202.103])  
by sample.ocn.ne.jp(Postfix) with ESMTP id DAA19039  
for<hon@tate.com>;Mon, 12 May 2028 10:15:29 +0900(JST)
```

メールは、通常、インターネット上で幾つかのコンピュータ（サーバ）を経由して宛先に届く。このため、メールヘッダの「Received」には、そのメールがどのコンピュータを経由して（転送されて）来たのかを示す情報が記載されている。

「Received」の情報は、メールが転送されるたびに追加されるため、一番下に記載されたものが送信元に関する情報である可能性が高いといえる。

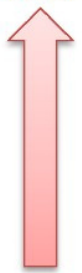


穴埋め問題

4 メールヘッダの読み解き方

【メールヘッダの例（抜粋）】

宛先

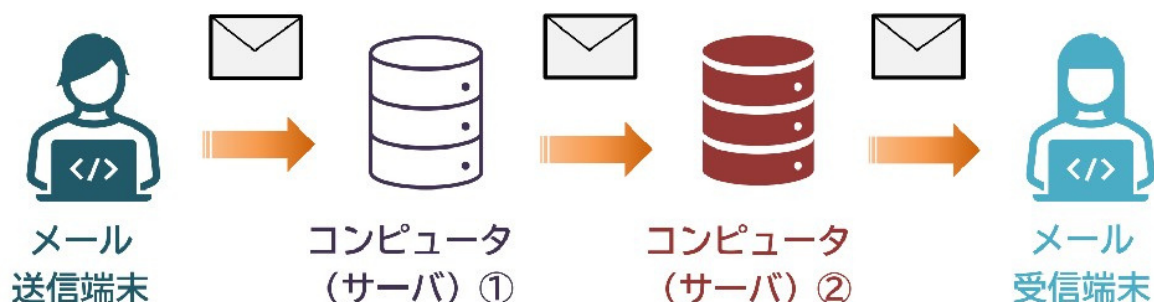


送信元

```
Received:from sample.ocn.ne.jp(sample.ocn.ne.jp[192.0.2.1])  
by example.biglobe.ne.jp(Postfix) with ESMTP id DAA08171  
for<hon@tate.com>;Mon, 12 May 2028 10:15:30 +0900(JST)  
Received:from aaa39(aaa39.ocn.ne.jp[210.130.202.103])  
by sample.ocn.ne.jp(Postfix) with ESMTP id DAA19039  
for<hon@tate.com>;Mon, 12 May 2028 10:15:29 +0900(JST)
```

メールは、通常、インターネット上で幾つかのコンピュータ（サーバ）を経由して宛先に届く。このため、メールヘッダの「【 ⑦ 】」には、そのメールがどのコンピュータを経由して（転送されて）来たのかを示す情報が記載されている。

「Received」の情報は、メールが転送されるたびに追加されるため、【 ⑧ 】に記載されたものが送信元に関する情報である可能性が高いといえる。



S・A 問題

2

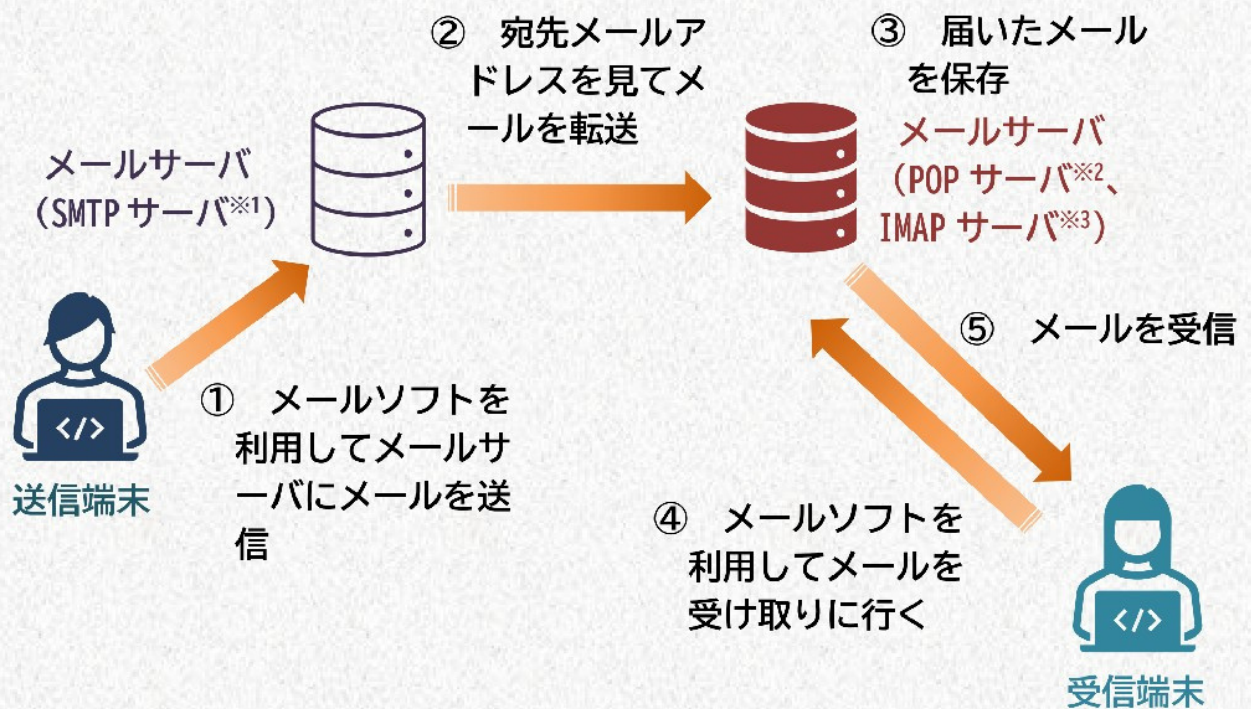
次は、メールヘッダについての記述であるが、誤りはどれか。

- (1) メールヘッダとは、メールが配送された経路や時間、経由したサーバ等のメールの詳細情報が記載されているものである。
- (2) メールヘッダに記載される情報としては、「From」「Received」「Date」等が挙げられる。
- (3) 「Return-Path」は、メール送信元へのリターンアドレスを表している。
- (4) 「Cc」は、同じメールを同時に送信する宛先メールアドレスを表している。
- (5) メールヘッダの確認方法は、メールソフトの種類やスマートフォンの機種等が異なっても同じである。

2 答え (5)

メールヘッダの確認方法は、**メールソフトの種類やスマートフォンの機種等によってそれぞれ異なる。**

【メールの仕組み】



※1 インターネット利用者が送信したメールを他のメールサーバに転送するサーバ。

※2 受信したメールをため込まず、全て利用者に渡すサーバ。

※3 受信したメールをサーバ上に保管したまま管理するサーバ。