

不審メールの見分け方とその対策

1 見分け方

本来は送信者のアカウントとメールアドレスは一致していますが、なりすましが起きていると、例えば横浜太郎：〇〇@yokohama-cu.ac.jp が本来正しい送信者の場合に、〇〇@yokohama-cu.ac.jp でないアドレスが表示されています。

The screenshot shows an email client window with the following annotations:

- なりすまされている人のアカウント名** (Account name of the person impersonating): Points to the sender's name field.
- 実際に送受信したメール件名** (Actual email subject): Points to the subject line.
- XXXX@フリーメールアドレス** (XXXX@free email address): Points to the sender's email address, which is highlighted as suspicious.
- 攻撃者のアドレス** (Attacker's address): Points to the sender's email address.
- メール受信者名** (Email recipient name): Points to the recipient's name field.
- 本来は〇〇@yokohama-cu.ac.jp でなければならないが違っている** (Originally must be 〇〇@yokohama-cu.ac.jp but is different): Points to the sender's email address.
- 開いてはいけない添付ファイル** (Attachment file that should not be opened): Points to a Word document attachment.
- 感染したメールアドレス** (Infected email address): Points to the sender's email address.
- なりすましが起こっているメール** (Email where impersonation is occurring): Points to the sender's email address.
- 実際に受信したメール本文** (Actual received email body): Points to the main body of the email.
- 実際に受信したメールに含まれる履歴** (History included in the actual received email): Points to the header information.

The email header information is as follows:

From: メールアカウント名 [mailto:メールアドレス]
Sent: Monday, June 03, 2019 7:45 PM
To: メール受信者名 <受信者メールアドレス>
Subject: 実際に送受信したメール件名

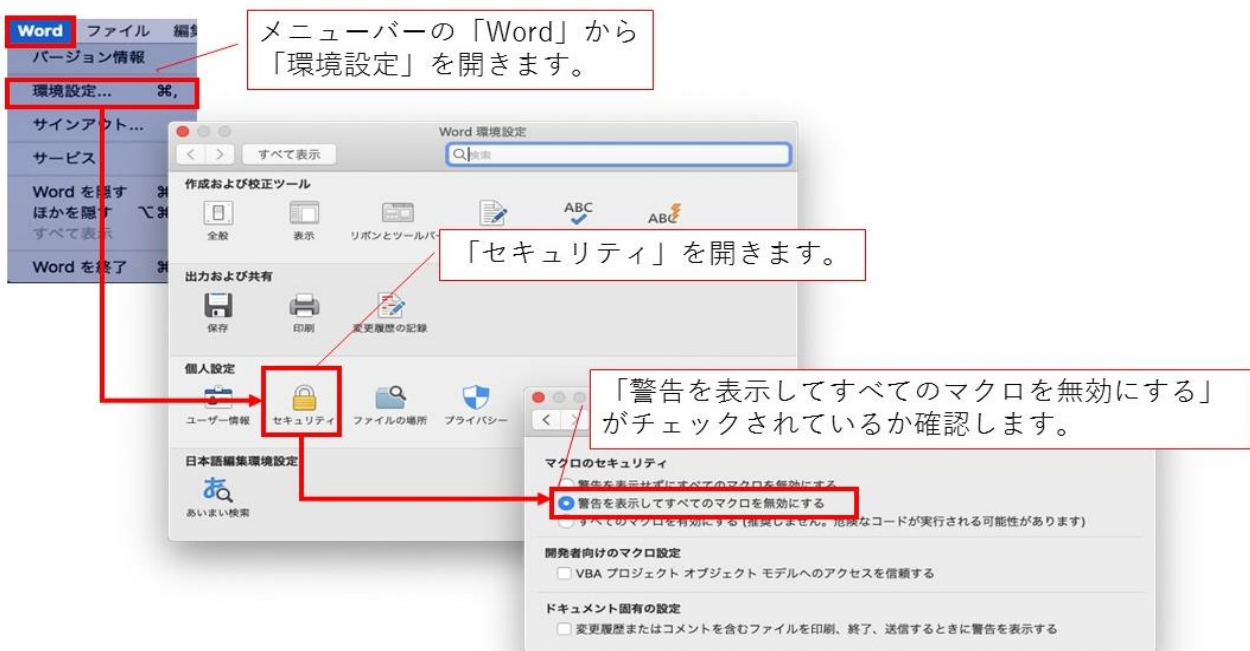
(次ページあり)

2 対策

- (1) Microsoft Word を立ち上げ、「ファイル」→「オプション」→(Word のオプション画面)「セキュリティセンター」→「セキュリティセンターの設定」の順にクリックすると以下の「マクロの設定」画面になります。



※macOSの場合



(2) マクロの設定画面で

二つ目 「警告を表示してすべてのマクロを無効にする (D)」 を選択します。
最後に、右下のOKをクリックします。