



# サイバーセキュリティの置き薬

2022年  
第16号

## 標的型サイバー攻撃、不審メールにご注意ください！

国内の学術関係者や報道関係者等に対し、講演依頼や取材依頼等を装ったメールを送信し、そのやり取りの中で、不正なプログラム(コンピュータウイルス)を実行させ、メールやコンピュータ内のデータの窃取を試みるサイバー攻撃が多数確認されています。

### 特徴

- ・ 実在する**組織の社員・職員を騙り**、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られる。
- ・ その後、日程や内容の調整に関するメールのやり取りを通して、**資料や依頼内容と称したURLリンクの記載や添付ファイル**が送付される。



### 送信元メールアドレスの例

- ・ 表示名<見覚えのない不審なメールアドレス>
- ・ <詐称対象の人物名>@<詐称対象の組織略号>.com(.org)
- ・ <詐称対象の人物名>@<著名なフリーメールのドメイン>(yahoo、gmail等)

### 不審メールの件名の例

- ・ 【依頼】インタビュー取材をお願いします
- ・ 研究会へのゲスト参加のお願い【●●●●●●●●】抜粋
- ・ 【ご出講依頼】●●●●●●勉強会 ※●には実在する組織名等が入る

### 日頃のセキュリティ対策が重要です！

#### ● ウィルス対策ソフトの導入

定期的にフルスキャンを実施してください。定義ファイルを更新することにより、新たに出てきたマルウェアが検知できるようになります。

#### ● ログインアラートの設定

メールサービスやプロバイダによっては、Webメールのログイン時等に、通常と異なる状況(海外からのログイン等)が確認された際、アラートメールを送付する機能があります。活用・設定し、アラート時は注意しましょう。

#### ● 多要素認証の導入

複数の要素(記憶情報、所持情報、生体情報のうち2つ以上)を使用して認証することで、セキュリティ強化を図りましょう。

#### ● 複雑なパスワードの設定と使い回しの厳禁

パスワードは、大小英字、数字及び記号を混在させた複雑なものとし、使い回しはしないようにしましょう。



少しでも「変だな」と思った場合は、クリックすることなく、直接相手先に電話をかけて確認してください！

【参考】警察庁「標的型メール攻撃、不審メールにご注意ください！」

[https://www.npa.go.jp/cyber/pdf/R041130\\_cyber\\_alert\\_2.pdf](https://www.npa.go.jp/cyber/pdf/R041130_cyber_alert_2.pdf)

[https://www.npa.go.jp/cyber/pdf/R041130\\_cyber\\_alert\\_1.pdf](https://www.npa.go.jp/cyber/pdf/R041130_cyber_alert_1.pdf)

