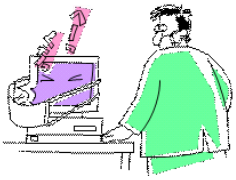
ふくしまPITネットワーク　No.60

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for Illegal Leakage of Technological Information

標的型サイバー攻撃、不審メールにご注意ください!

メールのURLリンクから悪意あるファイルをダウンロードさせる



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てくる。
- 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リンクの記載されたメールが送られたり、資料・原稿等が添付ファイルとして送付されたりする。

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
  ※　内閣太郎〈naikaku.taro@example.com〉等
- 〈詐称対象の人物名〉@〈著名なフリーメールのドメイン〉
  ※ yahoo.co.jp gmail.com outlook,jp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【〇〇〇〇〇〇〇】
- 【ご出講依頼】〇〇〇〇〇〇勉強会　　※〇には実在する組織名が入る

怪しいと思ったら・・・

ログインアラートの受信

- アラートメールを受信し、身に覚えのないログインが成功していた場合は、急いでパスワードを変更してください。
- 一方、ログインアラートを装ったフィッシングメールが確認されているので、パスワードを入力する際には、URLをよく確認してください。

ウイルス対策ソフトのスキャン

- ウイルス対策ソフトを最新の状態にして、フルスキャンを実施してください。
- ウイルス対策ソフトが検知した際は、検知画面を保存（スクリーンショット、スマートフォン等で撮影）し、検知名（マルウェア名）や検知場所（フォルダ・ファイル名）の記録をお願いします。

パスワードの変更

- 漏洩や不正利用の疑いがあれば、至急、パスワードを変更してください。
- パソコンがマルウェアに感染している場合、パスワードを変更しても攻撃者が入手できる可能性があるので、マルウェアに感染していないかも確認する必要があります。

転送設定の確認

- メールの転送設定がされていないか確認してください。
- 転送設定がされている場合には、その状況を保存（スクリーンショット、スマートフォン等で撮影）し、設定が変更された状況の記録をお願いします。