

サイバーコネクトSHIG@

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

学術関係者・シンクタンク研究員等を標的としたサイバー攻撃

近年、日本国内の学術関係者、シンクタンク研究員、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やりとりする中で、不正なプログラム（マルウェア）を実行させ、その人物がやりとりするメールやパソコン内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。



講演依頼、取材依頼等を騙り、URLリンクから悪意のあるファイルをダウンロードさせる。

- ・ 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きます。
- ・ 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リンクが記載されたメール、または資料・原稿等が添付されたメールが送信され、ここからファイルをダウンロードするとウイルスに感染してしまいます。



●●様
お世話になっております。●●●●●●の▲▲▲▲▲▲と申します。私ども●●●●●●の主催する勉強会（非公開）につきまして、先生のご都合を内々にお伺いしたく、ご連絡させていただきました。
…
（具体的な依頼内容）
…
何かご不明な点等ございましたら、何なりとお知らせください。どうぞよろしくお願い申し上げます。
▲▲▲▲▲▲ ●●●●●●
…
（詐称人物の偽の連絡先）



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。
- 【ご出演依頼】●●●●●●勉強会研究会へのゲスト参加のお願い【●●●●●●】

※ ●には実在する組織名等が入ります。



皆様
平素は大変お世話になっております。先日、■新聞に標記の拙稿が掲載されました。ご興味がありましたら、電子版を送付いたします。
<署名>

怪しいと思ったら・・・

別の手法での送信名義人への確認



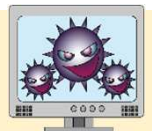
- ◇ 送信元として知人の名が記載されたメールであっても、少しでも内容に不審な点を感じた場合は、当該メールへの返信以外の方法で送信者に内容の確認を行ってください。

アクセス履歴、転送設定の確認



- ◇ アラートメールを受信した場合は、アクセス履歴を確認し、身に覚えのないログインが成功していた場合は、至急パスワードを変更してください。
- ◇ その際、当該ログインアラートメールが偽のものである可能性があるため、メール内のリンクはクリックせず、ブラウザから直接WEBメールサービスにログインしてください。
- ◇ メール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、スマホで撮影など）し、設定が変更された状況を記録しておいてください。

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。
- ◇ ウイルスを検知した際は、検知画面を保存（スクリーンショット、スマホで撮影など）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。
- ◇ もし可能であれば、検知したマルウェアは削除せず、隔離した状態で、警察へご連絡ください。

メールパスワードの変更



- ◇ 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、変更後のパスワードも攻撃者に漏洩する可能性があるため、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。

詳細は、警察庁ウェブサイト「報道発表資料」をご確認ください。
引用：https://www.npa.go.jp/news/release/2022/20221130001.html

サイバー攻撃、不審メールの受信等があった場合は、警察への通報をお願いします。

「サイバーセキュリティ情報SHIG@」フィッシングによるインターネットバンキングの不正送金に注意してください。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表）