

ふくしまPITネットワーク No.54

ふくしま技術情報不正流出防止ネットワーク

令和3年上半期のサイバー空間の情勢

サイバー攻撃により情報が窃取される事案も引き続き多発しています。
事業者等に対して、業務に関連した精巧な内容の標的型メール攻撃が実行されています。

次のページに、実際に事業者等に送付された標的型メールについて例示しますので、参考にしてください。

事業者等の皆様は、標的型メールを受信した際の対応は御存じだと思いますが、標的型メールを受信した際の対応要領について、おさらいのため紹介します。

◆ 経営者層

● 組織としての体制の確立

- 迅速かつ継続的に対応できる組織内体制（CSIRT※）の構築
- 対策予算の確保と継続的な対策の実施
- セキュリティポリシーの策定

※ Computer Security Incident Response Teamの略。コンピューターセキュリティに関する事故対応チームのこと。

◆ 従業員、職員等

● 情報リテラシーの向上

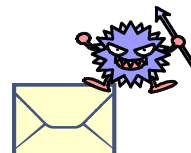
- セキュリティ教育の受講
 - ・ メールの添付ファイルやURLを安易に開かない
 - ・ Officeファイルのマクロを安易に有効化しない
 - ・ 被害を受けた際は迅速に連絡

○ 被害の予防（組織全体で実施）

情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）の実施

● 被害を受けた後の対応

- CSIRT等所定の連絡先への連絡



※ 独立行政法人情報処理推進機構 (IPA)
「情報セキュリティ10大脅威2021」より引用

【シンクタンクに対する標的型メール攻撃】

大学の研究者をかたり、「バイデン政権下の日米安保体制」と題して、不正プログラムが仕掛けられた添付ファイルを開くよう誘導する標的型メールがシンクタンクに送信された。

差出人:	██████████ <██████████>
送信日時:	2021年4月██████████
宛先:	██████████ co.jp
件名:	Re: ██████████ でございます。
添付ファイル:	バイデン政権下の日米安保体制.doc

██████████ 先生

こちらこそお世話になっており、ありがとうございます。
では、拙稿をご参考にお送りします。
未発表のものです。ただ自分の愚見を述べただけです。
ご笑覧ください。
██████████ ご紹介をいただき、有識者にご意見ご指導いただければ幸いです。

開封パスワードは ██████████ です。
どうぞよろしくお願いいたします。

██████████
██████████ 大学大学院 ██████████
〒██████████-██████████ ██████████
tel: ██████████ (内線 ██████████)

【半導体関連の製造業者に送信された不審なメール】

メールボックスのクォータ（割り当てられた容量）の更新と称して、リンク先からログインしてパスワード等を入力するよう誘導する不審なメールが半導体関連の製造業者に送付された。

差出人:	██████████ 支援チーム <██████████>
送信日時:	2021年2月5日 金曜日 0:45
宛先:	██████████ co.jp
件名:	メール見積もりを増やす

: ██████████ co.jp

メールボックスのサイズが 制限
クォータを超えないように、ログインしてクォータを更新してください

メールクォータの更新

*NOTE:メールクォータの更新の失敗
メールを送受信できなくなります

*これは自動化されたメッセージです返信しないでください**
よろしく、
メール管理者
この郵便物に ██████████ co.jp

【機械部品関連の製造業者に送信された不審なメール】

支払い依頼の確認と称して、リンク先から資料をダウンロードするよう誘導する不審なメールが機械部品関連の製造業者に送信された。

差出人:	██████████ <██████████>
送信日時:	2021年1月15日 金曜日 0:52
宛先:	██████████
件名:	Fwd: WIRE PAYMENT ORDER

Dear

please confirm payment order remitted on monday

ATTACHED_PDF_(DOWNLOAD_OPEN)

ふくしまPITネットワーク No.55

ふくしま技術情報不正流出防止ネットワーク

コンピューターウイルスEmotet (エモテット) の感染拡大が再び!!



Emotet (エモテット) とは？

マルウェアの一種で、メールに添付されたファイルを実行する等して感染します。

令和3年11月頃からEmotetによる攻撃再開が確認され、日本国内でも被害が増加しています。

メールは、「新型コロナウイルス」、「賞与支払届」等、受信者が興味・関心をひく内容とタイミングで送信されてきます。

Emotet

感染すると

情報窃取

+

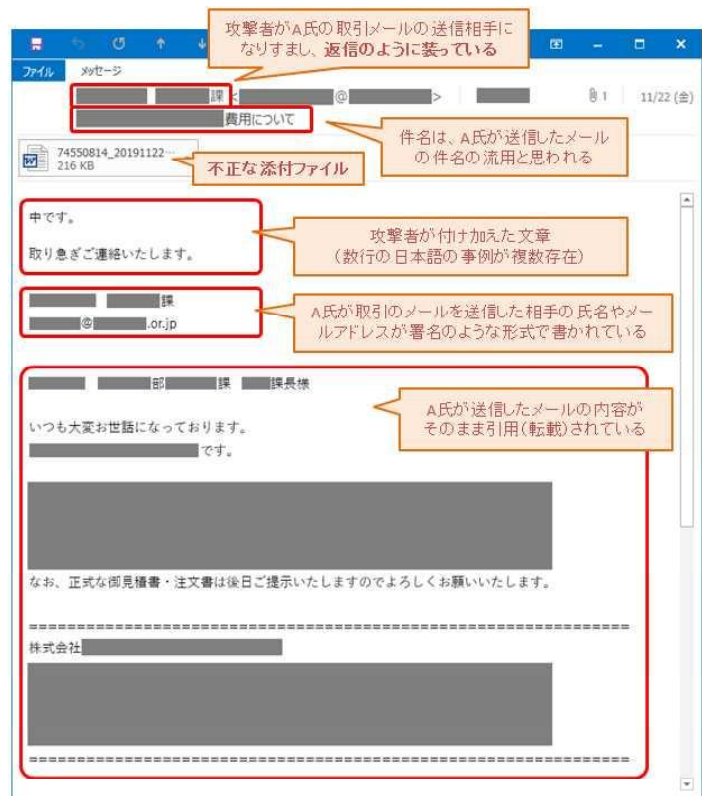
感染拡大



被害防止のチェックポイント！

1 なりすまし メールに注意！

- メールは、受信者が過去にメールをやり取りをしたことのある、
**実在の相手の氏名、
メールアドレス、
メールの内容等の一部**
を流用するなど、**実在の相手になりすました**内容となっている。
- 不自然な点があればメールを送ったかどうか**相手に直接確認**する。
- 過去のメールに対する返信メールとして送信される。
※ 次のページに続く



2 「コンテンツの有効化」ボタンを押さない！

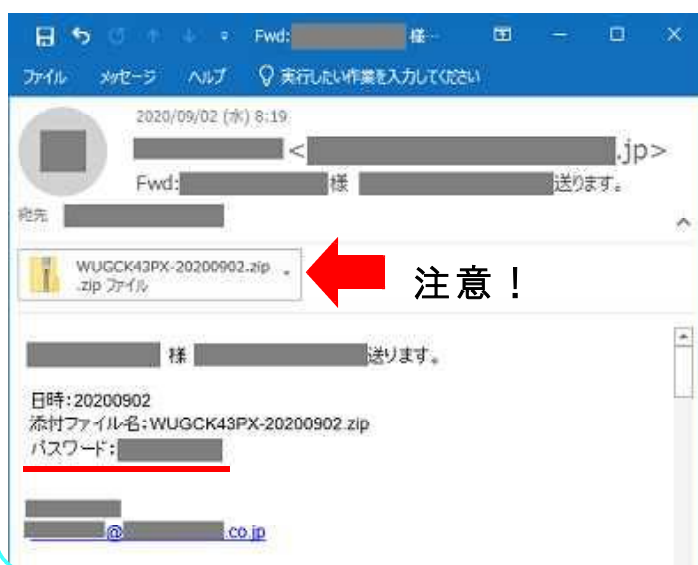
「コンテンツの有効化」ボタンをクリックすることで感染活動が開始されます。

注意！

このパソコン上で、文書ファイルに埋め込まれているマクロ(プログラム)等の実行を許可するという意味のボタン。このボタンをクリックすると、悪意のあるマクロが動作し、ウイルスに感染させられてしまう。



3 パスワード付きZIPファイルにも注意！



パスワード付きZIPファイルは、添付ファイルが暗号化されているため、セキュリティ製品の検知・検疫をすり抜けて受信者へ届く確率が高まります。

解凍したファイルを開き、
「コンテンツの有効化」
ボタンをクリックしない。

※ 独立行政法人情報処理推進機構(IPA)【「Emotet」と呼ばれるウイルスへの感染を狙うメールについて】より出典

経営者の皆様へ

令和3年10月に発足した岸田内閣において、経済安全保障大臣が新設されるなど、経済安全保障が注目されています。福島県警察本部外事課においては、企業等の会合等の際に経済安全保障に関する講話を行っておりますので、講話のご希望がありましたら、福島県警察本部外事課又は最寄りの警察署にご相談ください。

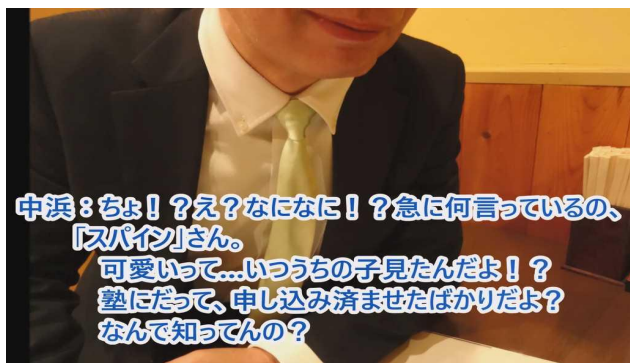


ふくしまPITネットワーク No.56

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

福島県警が独自に作成した 技術情報流出防止動画をYouTubeにアップ!!



福島県警察公式

検 索

福島県警察経済安全保障対策プロジェクトチームでは、社員教育等でご活用頂けるよう、実例を基に産業スパイの手口を分かりやすく動画にしました。産業スパイの外国人が、会社の開発部門社員に偶然を装って接近し、徐々に関係を深め、甘言や金品交付、脅迫を手段として会社の技術情報を提供させる一部始終を、実例を基に分かりやすく構成した動画です。

福島県警察公式Youtubeでは是非ご覧ください！

