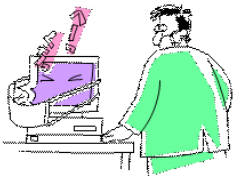
ふくしまPITネットワーク　No.60

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。

ふくしまPITネットワーク

令和５年
第１号

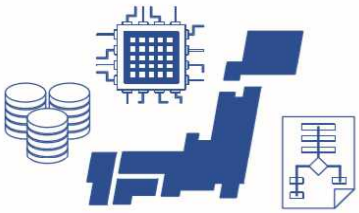
ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for Illegal Leakage of Technological Information

技術流出の防止に向けて

情勢～今、何が起きているのか

近年、地政学上のリスクがクローズアップされ、国際的な産業競争が激化



日本には、規模の大小を問わず、先端技術を保有する企業やアカデミアが多数存在

こうした技術を入手して自国産業を強化したり、軍事技術に転用したりしようとする外国から狙われるように

技術流出の防止は 経済安全保障上の課題

福島県の場合・・・
▼従前から高度な技術情報を持つ企業が多数存在
▼東日本大震災以降、復興事業として立ち上げられた各種国家プロジェクトに基づく高度先端技術の研究・集積の進行

⇒ 福島県も、決して他人事ではありません!!

事例～どのようにして起きるのか

外国から技術が狙われるリスクのパターンは、大きく3つに分類できます。

①サイバー攻撃

あらゆる産業でDX（デジタルトランスフォーメーション）が進むにつれ、サイバー攻撃や不正アクセスによって、直接的に情報を窃取される危険性が増大

②スパイ工作

サイバー上だけでなく、人を通じて情報を窃取されるリスクが存在

③経済・学術活動を通じた技術流出

合弁や企業の買収、共同研究など、合法な経済・学術活動を隠れ蓑にして、情報が狙われるリスクが存在

次号から、技術流出防止に向けた備えについて紹介していきます。

ふくしまPITネットワーク
令和５年
第 ２ 号

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

技術流出の防止に向けて

～ 最初にすべきこと（秘密情報の指定と管理） ～

STEP１＝保有する情報の把握・評価及び秘密情報の決定＝

① 企業が保有する情報の全体像の把握

✓ 紙、サーバーやPC内の電子データ

✓ 目に見えない形で存在する情報（従業員が業務の中で記憶した製造ノウハウなど）

② 保有する情報の評価（指標に基づく評価）

＜指標の例＞

- 経済的価値
- 情報管理の必要性・程度
- 漏えい時の被害（経済的損害、競争力や社会的信用の低下など）
- 競合他社から見た有用性
- 契約等で他社から預かった情報か否か

③ 秘密情報の決定

情報の評価の高低を基準に、保護に値するかどうか判断（想定される管理コスト、訴訟コストのほか、漏えいによって被るおそれのある損失など、総合的に判断）

STEP2＝秘密情報の分類＝

◎ 企業で取り扱う秘密情報の内容・性質やその評価の高低、利用態様、採用することが可能な管理措置等の事情に応じ、秘密情報の管理水準を分類していきます。

◎ 情報保護の観点と、日頃の業務で情報を使う場合の利便性の観点とのバランスをとることが重要です。

STEP3＝秘密情報の分類に応じた対策の選択＝

◎ 秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。

◎ 誰に対して対策を行うのか、どのような形で秘密情報が存在しているのか、漏えいの手口やその動機がどんなものかといった状況によって、効果的な対策は異なります。

◎ テレワークの有無などによっても判断が変わるので、企業に応じた対応をしましょう。