ふくしまPITネットワーク　令和５年第３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

～ 対策①　サイバー攻撃への備え ～

「ふくしまPITネットワーク　令和５年第１号」では、技術情報の流出がどのようにして起きるのかについて、①サイバー攻撃、②スパイ工作、③経済・学術活動を通じた技術流出の３つの分類を紹介しました。そのうちの一つである「サイバー攻撃」への備えについてご紹介します。

3つの基本的対策

１　リスク低減のための措置

▼　**本人認証の強化**
- ✓パスワードが単純でないかの確認
- ✓アクセス権限の確認
- ✓多要素認証の利用
- ✓不要なアカウントの削除　など

▼　**IoT機器を含む情報資産の保有状況を把握**

特にＶＰＮ装置やゲートウェイなど、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラムなど）を迅速に適用する。

▼　**組織内への周知**
- ✓メールの添付ファイルを不用意に開かない
- ✓ＵＲＬを不用意にクリックしない
- ✓連絡・相談を迅速に行うこと　など

２　インシデントの早期検知

▼　サーバなどにおける各種ログを確認する。

▼　通信の監視・分析やアクセスコントロールを再点検する。

３　インシデント発生時の適切な対処・回復

▼　データ消失などに備えて、データのバックアップの実施及び復旧手順を確認する。

▼　インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制を準備する。

ふくしまPITネットワーク　令和５年 第４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

～ 対策②　スパイ工作への備え ～

こんなことはありませんでしたか？

- ✓個人のＳＮＳに、接点のない外国企業からメッセージが送られてきた
- ✓道端で、見知らぬ外国の人に声をかけられた
- ✓付き合いのある外国企業の人から「お礼」としてプレゼントやご馳走をされた
- ✓外国企業の人から、アクセス制限のある情報の提供をお願いされた

これらは、スパイが近づいてくるときのサインの一例です。スパイ工作から身を守るため、何に気を付ければいいでしょうか。

一人ひとりに守ってほしい3つのS

See　相手をよく見る

プライベートやSNSなど、普段のビジネスシーンとは異なる場面で出会った相手については、所属や連絡先などの情報を確認しましょう。

▼　悪意ある者が近づいてくるリスクは、誰にでもあります。

▼　あなたのことを調べた上で、偶然を装って近づき、食事に誘い出すなどして、情報を引き出そうとするケースもあります。

▼　相手の会話内容とプロフィールに矛盾がないか、相手の会社は実在するかなどもチェックポイントです。

Stop　立ち止まって考える

SNSなど、不特定多数の人の目に触れる場所に個人情報を記載する時は、立ち止まって慎重になりましょう。

▼　ＳＮＳは便利なツールですが、悪意ある者は、ターゲットの個人情報を調べ上げ、接近する際の口実や脅迫などに利用する可能性もあります。

相手からの贈り物には、一度立ち止まって慎重になりましょう。

▼　相手からのプレゼントやご馳走は、あなたを「断りづらい状況」に追い込み、後からあなたに情報提供を要求するきっかけとなる可能性があります。なぜ個人的に贈り物をするのか、その意味を冷静に考えましょう。

Share　共有する・相談する

ささいなことでも上司や同僚に共有・相談しましょう。不審に思うことがあれば、警察にも相談してください。

▼　悪意ある者は、ひそかにターゲットに狙いを定めます。
見知らぬ人からのコンタクトや不審な働き掛けがあった場合、相談することで冷静になり、共有することで周りの人がターゲットにされることも防げます。

▼　情報の提供を依頼された場合に、「これくらいの情報なら」「相手はいい人だから」と軽く考えると、大切な技術が流出してしまうだけでなく、あなたが法律違反に問われる可能性もあります。

ふくしまPITネットワーク

令和５年
第　５　号

ふくしま技術情報不正流出防止ネットワーク

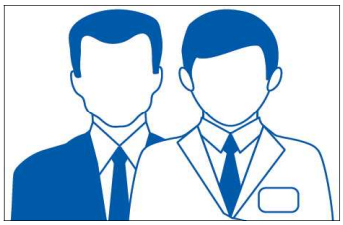
Fukushima　Prevention Network for　Illegal Leakage of　Technological Information

技術流出の防止に向けて

～ 対策③　経済・学術活動における備え ～

合弁企業の設立、共同研究の実施など、外国企業とのコラボレーションは、企業価値を高めるチャンスとなる一方で、意図・予測していなかった技術流出を招くリスクも秘めています。

こうしたリスクが、日本の安全保障にも影響を与えかねないといわれている昨今、企業やアカデミアは、何に気を付ければいいでしょうか。



企業やアカデミアに守ってほしい3つのS

See

相手・書類をよく見る

取引などの相手方となる外国企業をよく確認してください。

▼　外国企業との合弁や買収、共同研究を抑制することではなく、背景に存在するかもしれない技術流出のリスクを認識することが重要です。

▼　専門家により、相手方の実態をチェックすることも有効です。

技術流出のリスクを認識しましょう。

▼　契約書などの記載内容もよく確認してください。

▼　相手を信頼して確認を怠ると、“輸出管理条項”などの重要項目が、説明なく削除される可能性もあります。担当部署や専門家などによる確認も有効です。

Stop

立ち止まってリスクを把握する

外国への技術の提供につながる行為や活動については、一度立ち止まり、リスクを踏まえた検討を行ってください。

▼　外国企業から契約成立直前に機器の不備を指摘され、設計図の閲覧や機器の試作品の提供を要求されたというケースがありました。こうしたケースで相手側に渡してしまった機器などから技術が盗まれる可能性もあります。

▼　例えば、外国への進出や合弁企業の設立に伴うリスクだけではなく、外国からの撤退や合弁の解消などに伴うリスクもチェックポイントです。

▼　その国の法律や、リスクのある事例を確認するための業界内での情報交換も有効です。

Share

共有する・相談する

機微な技術の提供を含む取引については、関係部署などに情報共有・事前相談をしてください。

▼　取引の成立に向けて集中していると、輸出管理や営業秘密管理などがおろそかになり、対応を誤って関係法令に抵触してしまう可能性もあります。

不審な動向があれば関係機関や警察に相談してください。

▼　一度技術情報が流出してしまったら取り戻すことはできません。

▼　未然防止のためにも、外国への技術の提供をめぐって不審に感じることがあれば、関係機関や警察に相談してください。