ふくしまPITネットワーク

令和６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

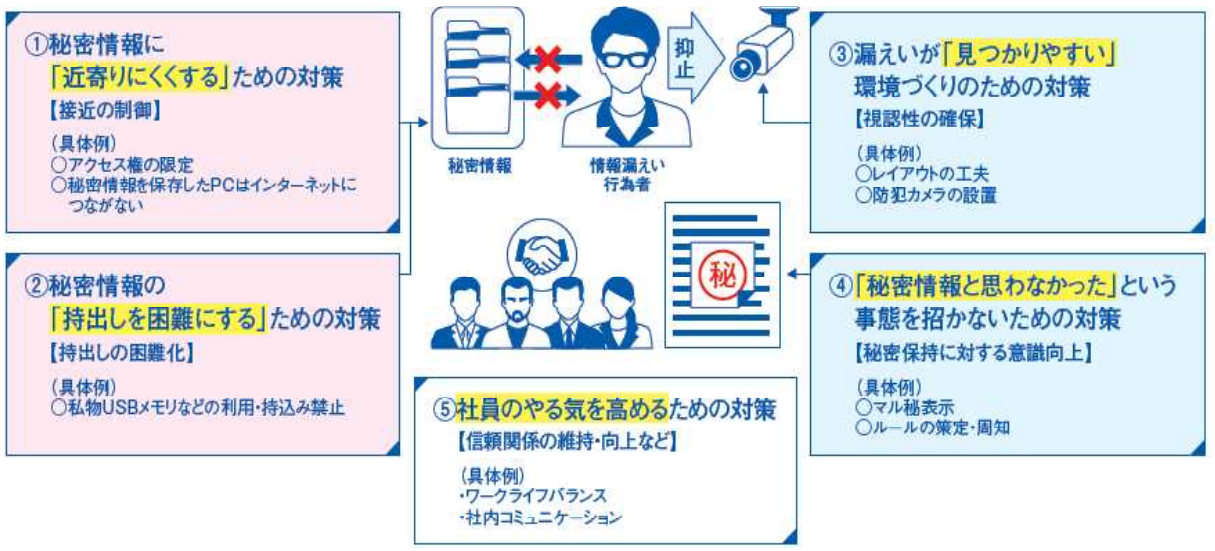
技術流出の防止に向けて

新年を迎え、いよいよ年度末が近づいてきました。

年度移行期は、退職や転勤などの人事異動の時期でもありますので、この時期を捉えて、自社の大切な技術情報等が流出しないよう、流出防止対策を見直されてはいかがでしょうか。

今回は、今一度、基本的な情報漏えいを防ぐための対策をご紹介していきます。

５つの漏えい対策



【出典:経済産業省「秘密情報の保護ハンドブック」】

情報漏えい対策は、誰に対して行うのか（従業員、退職者、取引先、外部者など）、どのような形で秘密情報が存在しているのか、などといった状況や事情に応じて、効果的・効率的な対策を講ずることが大切です。

例えば、退職・離職される方に対しては、

- ◆ 適切なタイミングでのアクセス権の制限
- ◆ 社内貸与の記録媒体、情報機器等の返却
- ◆ 秘密保持契約や競業避止義務契約の締結

など、必要に応じて対策をご検討ください。

詳細は、経済産業省「秘密情報の保護ハンドブック」をご参照ください。

ふくしまPITネットワーク

令和６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

営業秘密侵害事犯（不正競争防止法違反）について

今般、某県において、大手通信会社の子会社の元派遣社員が、多数の顧客情報を不正に持ち出して名簿業者に漏えいしたとして、不正競争防止法違反の疑いで逮捕されたことが伝えられています。本号では、不正競争防止法の営業秘密侵害についてご説明しますので、参考にしてください。

■ 営業秘密の侵害とは

窃取等の不正の手段によって営業秘密を取得し、自ら使用し、若しくは第三者に開示する行為等をいいます。

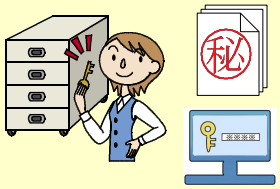
＜罰則＞

個人　10年以下の懲役若しくは2,000万円以下の罰金、又は併科

法人　５億円以下の罰金

※　海外使用等の場合～個人が3,000万円以下、法人が10億円以下。

■ 営業秘密として法律による保護を受けるための３つの要件



①　秘密管理性（秘密として管理されていること）

企業が情報を秘密として管理（アクセス制限や秘密である旨の表示、施錠管理等）し、情報を扱う従業員も秘密であることを認識できること。

②　有用性（有用な技術上又は営業上の情報であること）

生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であること。失敗した実験データといったネガティブ・インフォメーションにも有用性が認められ得る。

③　非公知性（公然と知られていないこと）

刊行物には記載されていないなど、保有者の管理下以外では、一般に入手できないこと。

■ 営業秘密保護のための秘密管理措置の例

◎ 適切なアクセス制限

営業秘密を従業員に示す場合、必要な範囲に必要な権限を付与し、アクセス権限を管理する。

◎ 合理的区分による管理

・　ファイルに「社外秘」等と明示する。

・　営業秘密と一般情報を同じファイルに保存しない。

◎ 各種規程の整備

・　規程等で企業が保有する営業秘密を具体的に定義する。

・　複製や社外持ち出しの禁止等を規定しておく。

◎ 従業員への指導教養

定期的な従業員への指導教養によって、各種規程や営業秘密の管理方法を認識させ、実行させる。

ふくしまPITネットワーク

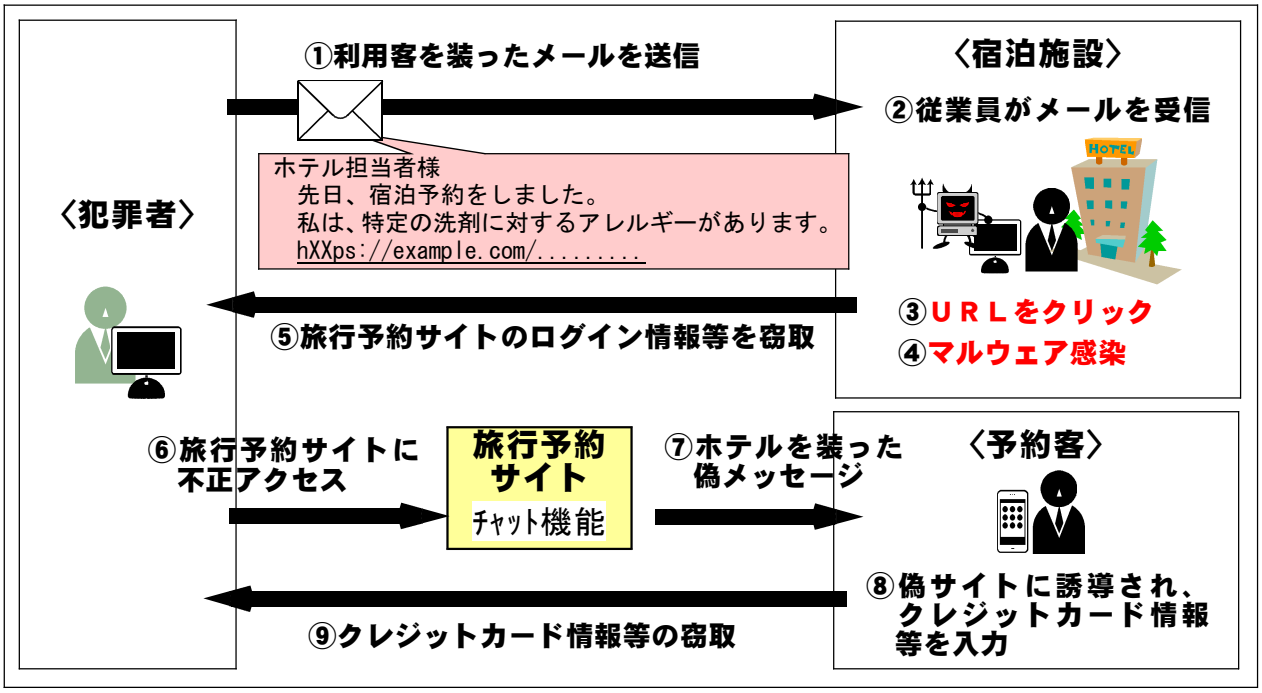
令和６年
第　３　号

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

メールのURLは要注意！

宿泊施設に対して、利用客を装い、ＵＲＬが記載されたメールが送り付けられる事案が発生しており、予約客の個人情報が窃取されるなどしています。概要は次のとおりです。

■　事案の概要



■　日頃からの備え

身に覚えのない不審なメールに記載されたＵＲＬや添付ファイルは、安易に開かないことはもちろんですが、日頃から

- 業務用端末と個人端末を混同しない（環境を混ぜない）。
- ＯＳやソフトウェア、ウイルス対策ソフトを常に最新の状態にする。
- 各種アカウントのパスワードは複雑なものに設定する。
- アカウントやパスワードをブラウザに保存しない。

などの備えをするのも効果的です。

メールに不審な点があれば、慌てずに、電子メール等とは別のルートで一度先方に確認するなどの対策も有効と考えられます。

サイバー空間をめぐる脅威は極めて深刻な情勢が続いており、機微な技術情報を保有する企業の場合、今回の事例のように、犯罪者が取引先を装ってメールを送り付け、技術情報の窃取を試みるなどの標的型サイバー攻撃も予想されます。

社内で脅威に対する認識を共有して社員教育に努めるなど、被害に遭わないよう注意しましょう。