

ふくしまPITネットワーク No.48

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

同業他社に転職の元社員が秘密情報持出!!

令和3年1月、国内情報通信会社に勤務していた同社元社員が、同業他社に転職する際、勤務していた会社から秘密情報を社外に持ち出したとして、不正競争防止法違反容疑で逮捕されました。

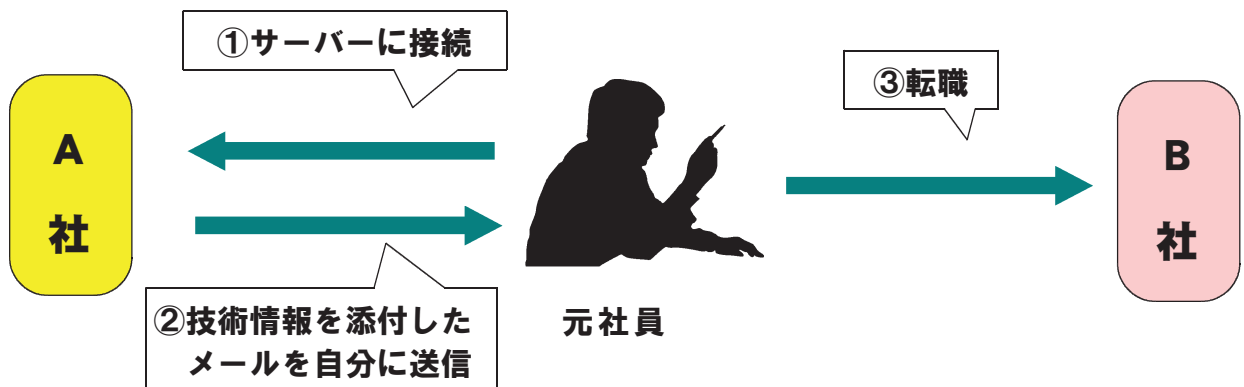
事件の概要

今回の事件は、自宅のパソコンから会社のサーバーにアクセスし、営業秘密である技術情報のファイルをメールに添付して自分に送信するなどし、不正に営業秘密を持ち出したとされています。

元社員は、10年以上勤務した会社から同業他社へ転職する際、営業秘密を持ち出したとみられており、退職を申告し、転職するまでの1か月間でサーバーに約30回アクセスして、約170点のファイルを持ち出したとされています。

持ち出された営業秘密の情報は、転職先の会社のサーバーや業務用のパソコンに保存されていたようです。

【イメージ図】



御存じのとおり、企業が保有する技術情報は、企業の大切な財産です。技術情報が流出してしまうことは、企業の財産が流出していることとなります。また、流出事案が発生してしまうと企業の信用も失墜してしまうおそれも生じてきます。

今回の事件は、国内企業から国内企業への持出でしたが、海外企業への持出だと国内企業としての損失だけでなく、軍用技術等への転用の可能性も否定できないので、注意が必要です。



※ 新聞等の報道を基に作成しています。

ふくしまPITネットワーク No.49

ふくしま技術情報不正流出防止ネットワーク

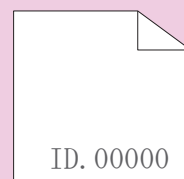
Fukushima Prevention Network for Illegal Leakage of Technological Information

情報漏えい対策（視認性の確保に資する対策）

事後的に検知されやすい状況を作り出す対策

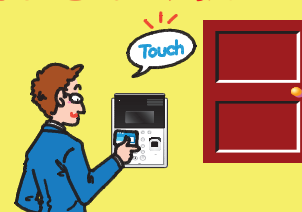
○ 印刷者の氏名等の「透かし」が印字される設定の導入

秘密情報が記載された電子データを印刷した場合に、強制的に印刷者の氏名やIDの「透かし」が印字されるように設定することで、印刷物の外観から、誰が印刷したものがすぐ分かるようになります。



○ 秘密情報の保管区域等への入退室の記録・保存とその周知

秘密情報が記録された媒体等を分離保管している区域への入退室について記録する（台帳管理、ICカードや生体認証等）とともに、その旨を社内に周知します。



職場の出勤や退社時間を記録にすることも一つの方法です。

○ 秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査

内部監査等を実施する際に、秘密情報の管理が適切に実施されているかを監査するとともに、資料の不足・欠損、不審な情報システムログ等の情報漏えい行為につながり得る兆候がないかを監査するとともに、監査が実施されている旨を社内に周知します。



監査の実施は、従業員等の秘密情報の取扱い方法等に関する認識を高めることにもつながります。



※ 平成28年2月経済産業省策定「秘密情報の保護ハンドブック～企業価値向上に向けて～」から抜粋

ふくしまPITネットワーク No.50

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



～ 産業スパイの手口 ～ FBIがドラマ作成!!

YouTubeで
視聴可能!

日本語字幕付き!!

- ・ 皆様の会社の技術や情報はこの様にして盗まれている可能性が!
- ・ 企業トップの皆様が気をつけていても、技術、情報は流出します!
- ・ 経団連加盟企業経営者の皆様にも紹介されています!

ドラマは、1本約30分の短編です!

↓↓ こちらのワードで **YouTube** 検索!! ↓↓

【 FBI The Company man 】

【 FBI The Nevernight connection 】

何かお気づきのことがありましたら、お気軽にお近くの警察署までご相談ください。

