～営業秘密漏えい防止のために～

近年増加傾向にある**「営業秘密の漏えい事案」を防ぐため**、当庁職員と当庁サイバーセキュリティアドバイザーの対談形式にて、お伝えします。

●警視庁サイバーセキュリティアドバイザーとは？

辻　伸弘（SBテクノロジー株式会社）

大阪府出身。

セキュリティ診断、ペネトレーションテスト等の専門家。

2022年より警視庁サイバーセキュリティアドバイザーとして警視庁職員に対し、最新のセキュリティ動向や技能を伝承中。

警視庁職員（以下、警と記載）：今回は、警視庁のサイバーセキュリティに関する外部顧問であるセキュリティアドバイザーの辻伸弘さんとともに、内部不正に関して気をつけて頂きたいことを話していきます。

辻伸弘氏（以下、辻と記載）：こんにちは！辻です！難しいと思われがちなサイバーセキュリティをできるだけ楽しく分かりやすくお伝えしていきたいと思います。今回は内部不正の中でも情報漏えいについて私見を述べますんで、最後までお付き合いください。

警：不正行為は、不正のトライアングル理論で提唱された「動機・機会・正当化」が揃うことで起こってしまうといわれています。

辻：「機会」は、持ち出し行為を容易とする状況・環境が存在すること、「正当化」は、持ち出し行為に対し、自らを納得させる身勝手な理由付けがあることですね。

警：過去の判例を踏まえた動機としては「転職先で使いたい」、「今後役に立つかもしれない」、「思い出のために」等が挙げられます。
これらを避けるために、企業は様々な対策を講じなければなりませんが、辻さんは持ち出し行為をする人についてどうお考えですか？

辻：持ち出す人って「どうせバレないって思っている」、「罪の意識が希薄」、「なにがなんでもやってやる！」の３パターンやと思うんですよ。このうち前の２つには抑止効果を働かせることができると思うんです。

警：では「どうせバレない！」と思っているパターンにはどうしたらいいとお考えですか？

辻：例えばパソコンにスマホを繋いで充電をはじめたことを検知できたらセキュリティ部門が直接電話かけて「今何かしました？」って伝えたらいいんですよ。そうすると実際に見られているという認知がされますし、場合によってはちゃんと見られているらしいということがクチコミで組織内に広まっていきます。しかも無料ですよ！

警：低コストで効果的な対策は導入しやすくて良いですね。では「罪の意識が希薄」というパターンへの対策も教えてください。

辻：罪の意識が希薄で甘く考えてる人に対しては、「仮に持ち出したら最大１０年の懲役・2,000万円以下の罰金！あとマジで訴えるから」ってセキュリティ教育の場できちんと伝えたらええと思うんですよ。あとは社員教育の場で「こんなログ(注ⅰ)取ってるから、アカンことしたらバレる！」って釘刺したりして、不正を許さない雰囲気作ることも大事ですね。

職場環境の整え方

警：不正を許さない雰囲気をどう醸成していくかという話になると、職場環境を整える必要がありますね。

辻：雑多に書類などが散らかったデスクで仕事をすると、人間どんどん緩みが生まれるんで、ほかした[注ii]資料かも分からんようになりますし、そのうち情報漏えいにつながるかもしれません。

警：職場環境を整理整頓して業務情報をきちんと判別できるようにするのはとても大事ですね。

辻：割れ窓理論って理論もありますから、「クリアデスク施策[注iii]」でオフィスをきれいにしたら、「ちゃんとせな！」って意識付けできますからね。

警：社員一人一人にクリアデスク を呼びかけることで、意図しない情報の漏えいを防止するのが重要ということですね。

辻：社内に「秘密情報の漏えいに注意」や「写真撮影禁止」等の掲示をしたり、執務室内や出入り口に防犯カメラを設置することも効果的ですね。

効果的な意識付け方法

警：効果的に意識付けさせる方法として、社員に対する定期的なセキュリティ教育を実施することって大事ですよね。

辻：教育の場では、直近の情報漏えいニュースを取り上げることや、自組織の規程を例示しながら繰り返し説明することで、問題をより身近に感じられるんで、自然と社員の意識も高まりますね。

警：教育と同時に、きちんと扱う情報を分類・明示することも重要で、秘密情報には「社外秘」「関係者外秘」等の表示を付して、一目で営業秘密だと分かるようにすることも必要ですね。

辻：要は、社員が日々の業務の中で「このファイルが大事なんや！」「これやったらアカンねんな！」って気づけるようにすることが大事なんですよ。
例えば、ファイルを自分のパソコンにコピーしたら「このファイルは機密情報です」みたいなポップアップ[注iv]を出したり、私物のＵＳＢメモリを挿入した際に「ＵＳＢメモリの使用は禁止です！」と警告メッセージを出したりすれば、ちゃんと業務の中でやったらアカンことが分かりますよね。

警：そうですね。不用意にやってしまった社員が居たとしても、「これダメなことなんだ！」と一目で分かりますね。

辻：あとは、ファイルを作成するときに大事なもんには「社外秘」表示など規定で決まっているものをしっかりつけようね、みたいな互いの声掛けも大事な対策やと思います。
そして、意識付けと同時に堅牢なシステム運用をすることも大事やと思いますね。

堅牢性を保つシステム作り どうすればよいのかな

警：堅牢なシステムというと、「Ｎｅｅｄ－ｔｏ-Ｋｎｏｗの原則（必要とする情報のみ知ること）」という考え方を基に社員毎の情報閲覧制限するため、必要最小限のアクセス権限を設定して、不要な情報に触れさせない環境を作ることが大事ですよね。

辻：それに加えてアクセス権限の設定変更できる人を限定し、変更時にはきちんと履歴を残しておくことも必要ですね。

警：その目的を教えてください。

辻：せっかく個人ごとのアクセス権限管理をしても、各々勝手に変えられたら元も子もないですからね。
業務上必要かどうかの妥当性も申請上げてもらって確認して、作業後もログをチェックする流れにすれば、勝手に権限変えられませんから、堅牢性高いシステム運用になりますよね。

警：社員毎のアクセス権限の制限だけでなく、私物ＰＣやスマホ等からの社内システムに対するアクセスを禁止することもきちんと設定することも忘れずに実施したいですね。
そして、設定をした後は、適切な頻度のアクセスであるかをモニタリングして「どの社員がどのような操作をしていたか」ということを振り返られるようにすることも重要ですね。

辻：今、挙がった社員の内部不正防止対策をするのって実はめっちゃお得で、社外の人間からの侵入にも効くんですよ。
例えば、社外からの乗っ取りがあったときでも、アクセス権限をちゃーんとしておけば、重要な情報に辿り着かれへんかもしれませんし、侵入された形跡をぱぱっと保全・分析して被害範囲も把握できるし、早期発見・原因特定・再発防止策の検討に使えるんですよね。
だから、内部不正対策って真摯に取り組めば取り組むほどお得なんやって意識してほしいですね。

社内規程・誓約書等の管理担当部署の方、聞いてください。

警：セキュリティというとどうしてもシステムの話になりがちですが、社内規程等に機密保持の要綱を入れることも重要だと思いますが、辻さんはどのようにお考えですか？

辻：規程って実はよく読むとふわっとした定義付けしているものが多いイメージなんで、なるべく列挙する方式にして、読む人ごとに認識が変わらないようにすることが、組織管理の面でも有効やと思います。

警：つまりなるべく具体的に例示する形が推奨されるということですね。
右上に企業における機密情報の定義について、推奨例をまとめてみたので、参考にしてみてください。

＜企業における機密情報の定義＞
（推奨例）

〇製品開発に関する技術資料（設計書、研究データ、論文等）

〇製造原価及び販売における価格決定等の貴社製品に関する情報（原価表、提携業者情報、資産管理表、稟議書、採算関連情報等）

〇その他、貴社が営業秘密と指定した情報

警：社内規程を定めるだけでは社員への理解を促しているとは言えませんので、定期的な教育の場を設けることや、社員が容易に確認可能であることが必要です。
また、情報の保持期間や対象部門を記載した情報資産管理台帳を作成・周知し、定期的に情報の棚卸しをすることも重要です。
さらに、実際の裁判例でも「機密情報の保持の必要性」を会社内に周知していたことで、被害企業が「営業秘密を適切に管理していた」と判断された事例があります。

辻：最近では、雇用契約時に「秘密情報を持ち出さないこと」のほかに「秘密情報を持ち込まないこと」を誓約させる企業が増えてきていますね。
自身の勤務先を守る意味でも「個人で情報は持たず、情報は持ち出さず、情報を持ち込ませず」ということを意識させるようにしましょう。

警：社内規程・誓約書等の管理担当部署の方々は是非とも参考にしていただければと思います。
次のページではよくある質問をまとめてみたので、最後まで読んでいただけると幸いです。

〔よくある質問集〕

Q１：会社が保有する情報は全部営業秘密として扱われるのですか？

警：会社が保有する情報が全て「営業秘密」とはなりませんので注意が必要です。
営業秘密として不正競争防止法上の保護を受けるためには「秘密管理性」「有用性」「非公知性」という要件を全て満たす必要があります。

辻：例えば飲み会の出欠表やら、特許情報として公開されてる情報はこの要件に当てはまらないから違うよねってことですね。

Q２：情報漏えい対策ってどういうことをすればいいんでしょうか？

警：経済産業省が発出している「情報漏えい対策一覧」に載っている対策を執ることがおすすめです。
一覧には端的に対策がまとまっているので、チェックシート代わりにも使うことができます。

辻：経済産業省のサイトって営業秘密関連の良い資料めちゃめちゃあるんやけど、その中でも「情報漏えい対策一覧（経済産業省ウェブサイト）」は必見！

Q３：実際に営業秘密漏えいが発覚した時はどう対応すればいいんでしょうか？

警：まずは持ち出し経路を特定し、持ち出し行為が証明できるログ等を保全することが大事ですよね。
その後、持ち出された情報の内容、機密性を確認し、一覧にまとめることも必要となります。
持ち出した者が社員であれば、該当社員に関する情報を集めておいてください。
持ち出しに使われたものが、貸与端末の場合は当該端末の電源を入れずに保全してください。
営業秘密漏洩の被害相談は、いまお話しした資料を準備し、事前連絡をした上で法人所在地を管轄する警察署に相談してください。

辻：ボクだったら、「絶対許しまへんでぇ！」って気持ちでありとあらゆるログを提出しますね。
いろんなログを横断的に見たら、「ほら、社外に持ってってるやないかーい！」ってちゃんと説明出来きますからね。
そのためには、適切にログ収集をしたうえで保全しておくこと、一般社員が改ざん出来ないようにしておくことっていう基本的なことをきちんとやっておくことも大事ですね。

●おわりに

警：ＩＰＡ(注v)によれば、情報セキュリティの脅威のうち、企業における情報漏えいが年々増加傾向にあり、どの企業でも発生する危険があるものだと注意喚起されています。
また、情報漏えいをした者は、刑事事件として取締りを受けることや、民事事件として高額な損害賠償を請求されることもあります。
さらに、ひとたび発生すれば企業のレピュテーションリスク(注vi)も甚大で経営に大きなダメージを与える可能性があることを意識してください。

辻：最近は度々「営業秘密の持ち出しで逮捕された」なんて記事もよく見ますからね、ほんと「許されへん犯罪や！」って気持ちを皆で持つことが大事やと思いますよ。

「情報の持ち出し」は身近に潜む犯罪ですが、みなさん一人一人の意識で発生を防ぐことができるということを覚えておいてください！

本文中注釈

注ⅰ パソコン等の起動、データ送受信、外部との通信記録等を時系列に記録した履歴。

注ⅱ 捨てるという意味の関西弁

注ⅲ 離席や退社時にデスク周りを整理整頓し、重要書類や記録媒体を放置させないための対策。

注ⅳ パソコン画面において自動的に別のウィンドウが最前面に起動する仕組み。

注ⅴ 独立行政法人　情報処理推進機構。経済産業省のIT政策実施機関。

注ⅵ 企業等のネガティブな評価が広まり、信用やブランド価値が低下することで損失を被るリスク。