【第 269 回 監査実務研究会】

●日時：2022 年 12 月 23 日(金)14：00～17：00 Zoom 形式で開催

●テーマ 情報セキュリティと監査役監査 ～個人情報保護と営業秘密管理～

：近年個人情報保護法の改正等に伴い、個人情報を含めた情報セキュリティの重要性がより一層増しています。

一方で、個人情報を含めた重要情報に関する事故も依然として発生しており、営業秘密に関する事件も引き続き発生しております。

今回は、個人情報保護や営業秘密管理を含めた、近年の情報セキュリティ規制の動向、及び情報セキュリティに関わる監査役監査のポイントについて考察を行いたいと思います。

●問題提起者：㈱ピカパカ 常勤監査役 室 雅章

●コーディネータ：キオクシアホールディングス㈱ 常勤監査役 森田 功

●本日の説明の流れ

1. はじめに
   （1）自己紹介
   （2）弊社概要
   （3）本日お話ししたいこと
2. 情報セキュリティの動向
   （1）情報セキュリティに関する近年の法整備の動向
   （2）情報セキュリティに関する近年の動向
   （3）情報セキュリティインシデントに関する傾向
3. 個人情報保護監査
   （1）個人情報保護に関わる規制の動向
   （2）個人情報漏えい事件例
   （3）個人情報流出に関する会社が負うリスク
   （4）個人情報保護に関するポイント考察
   （5）個人情報保護に関する監査における監査役の姿勢
4. 営業秘密管理監査
   （1）営業秘密保護に関わる規制の動向
   （2）営業秘密に関する事件例

（３）営業秘密流出に関する会社が負うリスク
（４）営業秘密管理に関するポイント考察
（５）営業秘密管理に関する監査における監査役の姿勢
5. 情報セキュリティ監査まとめ
（１）企業における情報セキュリティ全般に関する課題の考察
（２）情報セキュリティ全般に関する監査全体のポイント考察

参考資料

1. はじめに

（1）自己紹介

●氏名：室　雅章

●生年月日・出身地：1989 年 12 月 30 日・大阪府出身

●出身大学：2013 年 3 月　京都大学法学部卒業

●現職：株式会社ピカパカ　常勤監査役

●経歴：現在が 3 社目

①2013 年～　新日本工機㈱　販売業務部

②2014 年～　デジタルデータソリューション㈱　経営管理部

（2016 年～2017 年で同社の常勤監査役）

主に法務担当、内部監査担当

情報セキュリティ認証関連外部審査担当、コンプライアンス研修担当

（資料作成及び講師）も担いました。

③2021 年～　㈱ピカパカ（同年 8 月　常勤監査役就任）

④㈳監査懇話会会員（2022 年 6 月～　監査実務研究会運営委員）

（2）弊社概要

●会社名：株式会社ピカパカ

●設立：2018 年 12 月

●資本金：231,950 千円

●拠点数：13 拠点（本社、衛生検査所、クイック検査センター11 か所）

●主な事業内容：

①福利厚生事業（法人出張サポートサービスの提供）

②ヘルスケア事業（医療機関向けの DX 支援サービスの提供、**PCR 検査センターの運営**）

●決算月／株主総会時期：8 月決算、11 月株主総会

●主な許認可：

①第一種旅行業

②衛生検査所（東京都港区）

③プライバシーマーク（2022 年 12 月認証）

（3）本日お話ししたいこと

●情報セキュリティ全般に関わる動向（法改正・事件を含む）

●個人情報保護に関する監査役監査のポイントの考察

●営業秘密管理に関する監査役監査のポイントの考察

●情報セキュリティ全般に関する監査役監査のポイント全般の考察

2.情報セキュリティの動向

（1）情報セキュリティに関する近年の法整備の動向

●日本では特に2003年に個人情報保護法が制定されて以降、急速に法整備が加速した。

時期	内容
1980年	プライバシー保護と個人データの国際流通についてのガイドライン（OECDプライバシーガイドライン）の勧告 **・OECD8原則（収集制限、データ内容、目的明確化、利用制限、安全保護措置、公開、個人参加、責任）** →この原則を適用した上で個人情報保護法が後に制定される。
1993年5月	現行の**不正競争防止法**が公布（旧不正競争防止法の全面改訂） ・不正競争の類型の整理・拡充および損害額推定規定の設置など
1995年	EUデータ保護指令が発効される。 ・2018年にEU一般データ保護規則（GDPR）が発効されるまで効力を有した。
1999年8月	**不正アクセス行為の禁止等に関する法律**（以下「**不正アクセス禁止法**」という。）が公布 ・罰対象は故意犯であり、過失犯は対象外。また、未遂犯も対象外。
2003年5月	**個人情報の保護に関する法律**（以下「**個人情報保護法**」という。）が公布 ・2005年4月に全面施行
2005年6月	不正競争防止法が改正 ・営業秘密の刑事的保護の強化（情報窃盗に関する規定などの追加）
2012年3月	不正アクセス禁止法が改正 ・他人の識別符号を不正に取得する行為、他人の識別符号を不正に保管する行為、識別符号の入力を不正に要求する行為などの禁止が追加
2013年5月	**行政手続における特定の個人を識別するための番号の利用等に関する法律**（**マイナンバー法**）が公布 ・2015年10月から施行
2015年2月	アメリカにおいて消費者プライバシー権利章典（法案）（※未成立）が公開される。 ・従来、個人データの保護に関する包括的な法律が存在しなかったアメリカにおいて、初めて包括的な法律の動きが出た。
2015年7月	不正競争防止法が改正 ・営業秘密の侵害の未遂、国外での営業秘密の取得も処罰対象に追加

時期	内容
2015 年 9 月	個人情報保護法が改正（2017 年施行） ・**「５０００件要件[1]」の撤廃**、要配慮個人情報[2]の新設、個人データの消去努力義務、外国にある第三者への提供の制限など
2016 年 4 月	**EU 一般データ保護規則（GDPR）**が採択される。 ・2018 年 5 月に発効される。
2017 年 1 月	中華人民共和国サイバーセキュリティ法が施行 ・個人情報保護のみだけでなく、オンライン上の情報の保護を目的とした法律。ただし、政府や公的機関は対象外。
2020 年 1 月	カリフォルニア州 消費者プライバシー法（CCPA）が適用開始される。 ・個人情報に関する消費者の権利が保護されており、他の州も同様に規制が強くなるかどうかが注目される。
2020 年 6 月	個人情報保護法が改正（2022 年 4 月施行） ・漏えい時の報告義務の強化、本人の権利保護の強化、仮名加工情報の創設など
2021 年 11 月	中華人民共和国個人情報保護法が施行 ・GDPR が「市民のプライバシーを守ること」が主目的であるのに対し、中国の個人情報保護法は「国家安全」が主目的と見られる。

（２）情報セキュリティに関する近年の動向

●特に 2020 年のコロナ禍以降、テレワークの実施や情報セキュリティに関する報道などの影響で、セキュリティ意識の高まりが見受けられる。

●一方で、特に中小企業では、業務用のモバイル端末（ノートパソコンやスマートフォン）が支給されていないケースも多く、個人所有のモバイル端末を業務で使用しているケースも多い。

●個人所有のモバイル端末を業務で使用している人のうち約 60%は週 1 回以上個人所有のモバイル端末を業務のために利用しており、さらにそのうち半数以上、つまり全体の約 30%は週 3 回以上利用している。また、個人所有のモバイル端末を業務で利用している人のうち約 35%以上は勤務先から許可無くモバイル端末を業務で利用している。

---

[1] 改正前は、「個人情報取扱事業者」は「体系的に整理された個人情報（個人データ）を５０００件以上保有する企業」と定義されていたため、保有する個人情報が５０００件以上ではない事業者は、個人情報保護法の規制が及ばなかったが、このような例外が撤廃されることとなり、**個人情報を取り扱うすべての事業者に個人情報保護法の規制が及ぶこととなった**。（個人情報保護法第１６条２項）

[2] 「本人に対する不当な差別・偏見その他の不利益が生じないように、取扱いについて特に配慮を要する一定の個人情報」のことであり、人種、信条、病歴（身体障害や精神障害等を含む）、犯罪歴、犯罪被害歴、健康診断等の結果などが該当する。（個人情報保護法第 2 条 3 項）要配慮個人情報を取得する場合、原則として本人の同意が必要となる他、オプトアウト方式による要配慮個人情報の第三者提供は禁止されている。（個人情報保護法第 20 条 2 項及び同法第 27 条 2 項）

●在宅勤務に関しても、勤務先に許可なく在宅勤務を実施した人が約 10%にのぼるという調査結果があり、また、在宅勤務を実施した際に、契約書、請求書、各種帳簿書類、提案書、企画書、会議資料だけでなく、顧客情報を勤務先から持ち出したという調査結果がある。

●クラウドサービスについては、会社から指定されたクラウドサービスの利用が全体の 30%程度に留まる一方、個人契約のクラウドサービスを業務に利用している人も 25%が超えている。

●セキュリティ研修に関しては、実際の受講者のうち 80%以上は「有益であった」と回答しているにも関わらず、情報セキュリティ研修の実施企業の割合は 30%強に留まっている。

（３）情報セキュリティインシデントに関する傾向

●近年では「ウイルス感染・不正アクセス」が原因の情報漏えいが増加している。

①特に 2019 年から件数が急増している。

→ランサムウェア[3]、Emotet[4]などのコンピュータウイルス、2020 年以降のコロナ禍の影響によるリモートワークの増加などが影響していると考えられる。

（※対象は上場企業及びその子会社）

[3]ランサム（身代金）を要求するコンピュータウイルス。メールやウェブサイトからサーバーなどに侵入して勝手に暗号化して鍵をかけてしまい、解除するために金銭などを要求する。

[4] 不正なメールに添付されるなどして、パソコン等のデバイス上で電子ファイルを開封すると感染するウイルス。このウイルスに感染するとメールアドレス、パスワード等の情報が抜き取られ、他者にも攻撃を仕掛けられる。不明なメールアカウントからのマクロ付きの電子ファイル添付のメールは特に要注意。

②特に上場企業及びその子会社に関しては「サプライチェーン攻撃[5]」の影響も考えられる。

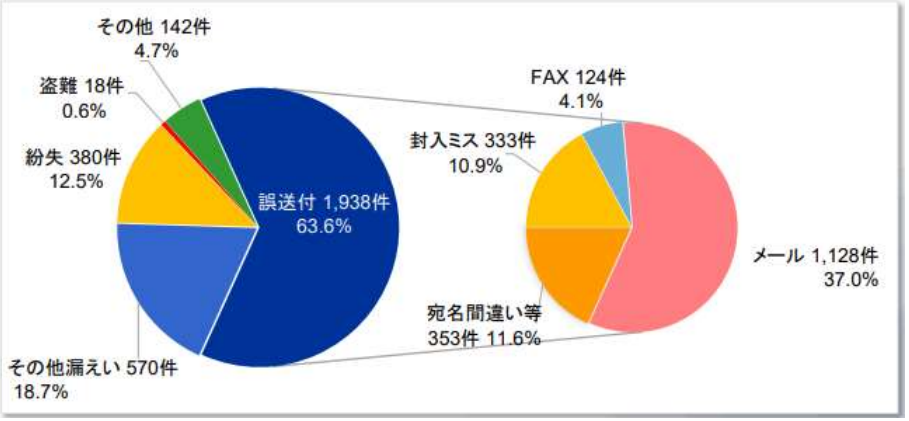
→中小企業だからといってサイバー攻撃を狙われないとは限らない。会社同士やソフトウェアのつながりで引き起こされるため、取り扱うソフトウェアやインターネット関連サービスが多いほど、サプライチェーン攻撃のリスクが高くなる。

●中小企業を含めると、「誤送付」が原因の情報漏えいが依然として多い。

①メールの誤送信が圧倒的に多く、特にコロナ禍以降件数が増加している。電子メールだけでなく、メッセージアプリ・SNS など「新たなコミュニケーションツール」における誤送信も増加している。

→コロナ禍においてリモートワークの増加に伴い、電子メールやメッセージアプリ・SNS などによる連絡、電子ファイル送信が増加していることが影響していると思われる。

②郵送時の場合、宛名間違いや封入ミスが依然として一定程度発生している。



（※日本情報経済社会推進協会及びプライバシーマーク審査機関に報告された個人情報の取扱いにおける事故）

●不正な情報の持ち出し（メール送付を含む）が原因の場合、事件化しやすい。

①営業秘密流出に関しては、不正な情報の持ち出しが原因となる事件が多い。（ソフトバンク 5G 営業秘密流出事件、はま寿司営業秘密流出事件等）

②自社だけでなく、委託先や派遣社員等が不正な情報の持ち出しを行い、情報流出が発生することをある。（ベネッセでの個人情報流出事件、神奈川県における HDD 転売・情報流出事件等）

[5] セキュリティが甘い取引先や関連企業に不正アクセスし、ターゲット（大手企業）の機密情報や個人情報を盗む攻撃。

3.個人情報保護監査

（1）個人情報保護に関わる規制の動向

●2010 年代において、情報流出事故の増加やマイナンバー法の施行などを背景に 2015 年に個人情報保護法が制定以降初めて改正され、特に個人情報保護法が適用される事業者の範囲が拡大するなど規制が強化された。また、関連するガイドラインの制定も進んだ。

●海外においては、アメリカは従来から個人データの保護に関する包括的な法律が存在しなかったが、州単位で規制が強化されたり、包括的な法律制定の動きが出たりと、徐々に個人情報保護の動きが強くなっている。一方、欧州では GDPR が 2018 年から適用され、最も厳しいルールとなっている。中国ではアメリカへの対抗から、昨年個人情報保護法が施行された。

●個人情報は事業運営や経営管理における根幹情報となっていることから、個人情報保護法だけでなく、金融商品取引法、特定商取引法など他の法規範にも影響を及ぼす。

●個人情報保護法施行（2005 年）以降、個人情報保護に関する関心の高まりからプライバシーマーク[6]の認証企業が急増し、2022 年 12 月現在 17,000 社を超えている。ただし、プライバシーマーク認証企業においても個人情報流出事故は発生しており、中にはプライバシーマーク認証が取り消しになった事例も発生している。(ベネッセコーポレーション、リクルートキャリアなど)

（2）個人情報漏えい事件例

時期	法人名	流出件数	原因	内容・影響
2006 年	富士ゼロックスシステムサービス	400 万件	元協力会社社員による不正コピー及び不正持ち出し	流出したデータを使い富士ゼロックスシステムサービスを恐喝未遂。
2007 年	アメリカンファミリー生命（アフラック）	20 万件	パソコンの盗難	保険業界で当時過去最大規模の個人情報漏洩事故。
2010 年	サミーネットワークス	173 万件	オンラインゲームサイトへの不正アクセス	複数回、外部からの不正アクセスの痕跡を確認。

[6] 個人情報の保護体制に対する第三者認証制度。個人情報保護体制の基準への適合性を評価し、一般財団法人日本情報経済社会推進協会（JIPDEC）が使用を許諾する。取得には審査機関による適合認証が必要となるため、プライバシーマークの認証を得て表示することにより、個人情報の取扱い体制への一定の信頼を得るものと言える。特に 2010 年代以降、官公庁など公的機関の入札資格にプライバシーマーク（あるいは ISMS、ISO 27001）の取得を要件とするものが増えている。

時期	法人名	流出件数	原因	内容・影響
2011 年	ソニーグループ	1 億 261 万件 （グループ全体）	主に不正アクセス	PlayStation のネットワークサービスへの不正アクセスを皮切りに、ハッカー集団による不正アクセスなどの攻撃を受けた。
2014 年	ベネッセコーポレーション	2900 万件	委託先従業員による不正持ち出し	2015 年 3 月期に上場以降初の赤字決算、翌期も赤字決算。
2015 年	日本年金機構	125 万件	不正アクセス	流出が確定した加入者に関しては基礎年金番号の変更が行われ、少なくとも 8 億円の経費が発生。
2016 年	サンナチュラルズ	6159 万件	不正アクセス	クレジットカード情報のほか、住所や電話番号、メールアドレスなどが流出。
2018 年	日本経済新聞	38 万件	元社員による不正持ち出し	2012 年 10 月に元社員が社用パソコンを持ち出しし、私物のパソコンにデータ移行。6 年後に日本経済新聞が元社員を刑事告訴。
2019 年	神奈川県	54 テラバイト （54,000 ギガバイト）	再委託先従業員による不正持ち出し	県からハードディスクの廃棄を委託された企業の再委託先の従業員がハードディスクを不正に持ち出し、ネットオークションで転売。
2020 年	PayPay	最大 2,007 万件	不正アクセス	加盟店など約 260 万店舗の営業情報などが流出。従業員やパートナー企業に関する情報も流出。
2021 年	T モバイル（米国）	5000 万件	不正アクセス	パスワードの強制変更措置を実施。

（3）個人情報流出に関する会社が負うリスク

●金銭的損失：顧客・取引先への賠償、対策費用（ex. ベネッセでの個人情報流出事件、日本年金機構）

●社会的評価の低価、顧客の喪失、売上の減少、事業の存続の危機（ex. 神奈川県における HDD 転売・情報流出事件）
●システム停止等による業務の停滞（特にサイバー攻撃、ウイルス感染による場合）
●従業員のモラル低下、職場環境の悪化、人材の流出
●刑事罰：罰金、懲役刑等

（4）個人情報保護に関するポイント考察
●企業規模、事業内容に応じた個人情報保護方針の策定
→企業として保護対象とする個人情報及び利用目的を明確化することが重要。
●情報セキュリティを推進するための責任者と担当者を定め、必要な予算を確保する。
→実際に発生した際の金銭的損失＞情報セキュリティのための費用
「情報セキュリティのための費用は企業を守るための投資」という意識が何よりも重要。
自社のリソースだけで賄いきれない場合、外部サービスの導入を検討する。
●企業規模、事業内容に応じた対策の検討と実行
→流出を防止すべき情報、及びその情報に関連する業務を整理し、必要な対策を規程やマニュアルとして文書化する。
文書化することで従業員も対策を実行しやすくなり、取引先に対しても説明をしやすくなる。
対策がルール通り実施されているかどうかを月次や四半期で報告させ、実効性を検証する。また内部監査によって検証も行う。
特に対策を検討、実行すべき内容は以下のとおりである。
①コンピュータウイルス対策（セキュリティソフト、無線 LAN、ファイヤウォール、OS のアップデート等）
②個人情報の不要な持ち出し・持ち込みを防止するためのルール策定、運用及びモニタリング
③個人情報の安易な放置・廃棄の防止のためのルール策定・運用の徹底
④個人情報への無許可のアクセス、口外の防止のためのルール策定・運用（アクセス権限等）
⑤誤送信、誤送付を防止するための宛先確認の徹底
⑥信頼性の低いメールやサイトにアクセスしないためのルールの策定・運用の徹底
●ルールや対策の適宜な見直し
→基本方針やルール、対策に関して、企業規模、事業内容、顧客からの要望等を踏まえて、基本方針、ルール、対策を適宜に見直す。
●緊急時の体制、復旧のための体制の整備
→緊急時の連絡先、連絡フロー、復旧手順などを整備し、緊急時を想定した訓練を実施する。

対応の遅れが致命的となるため、緊急時発生には隠ぺいすることなく速やかに報告させることを徹底し、報告を受けた後に第三者への報告や原因分析を即時に実行できる体制を整備する。

●外部委託や外部サービスの利用の際のセキュリティ事項の確認

→委託先で情報漏えいが発生した場合、委託元も責任を問われる。

委託先にも同等の責任を課し、セキュリティ対策の実施に関して、契約書等により明確に合意を得る必要がある。

外部サービスを利用する場合、情報セキュリティに関して規約や約款に明記されているかどうかを検証する。

●情報セキュリティに関する情報収集

→IT 技術の進化が早いことから、法規範等の改正や実施すべき対策の変化が著しく変化する。

独立行政法人情報処理推進機構や内閣サイバーセキュリティセンターなどの公的機関が情報セキュリティに関する最新動向を発信している。

●役職員、委託先等への情報セキュリティルールの周知

→最新動向、事例を紹介しながら、ルールや対策について定期的に周知を行う。また新入社員に対する周知も重要。

●情報セキュリティに関する誓約書の締結

→入社時だけでなく退職時に関しても誓約書を締結する。副業を認める場合、副業先への情報流出も対象となる。

●新規事業、新サービスの開始時において取り扱う個人情報の内容、利用目的、取得方法等の取り決め

→個人情報保護規範だけでなく、倫理面や信義則という点でも問題が無いかどうか。（ex. 内定辞退予測サービス「リクナビ問題」[7]）

（５）個人情報保護に関する監査における監査役の姿勢

前提として、上記（４）のポイントに関する取組状況を、内部統制システムに係る「損失の危険を管理する体制」の整備運用の確認のために、内部監査部門と連携して監査を実施するべきであるが、監査役としては代表取締役を含む取締役及び執行役員等に対し、「個人情報保護に関する取組＝企業を守るための投資」という考えのもと、以下の事項を働き掛けていくことが重要と考えます。

●個人情報保護方針、社内規程、マニュアルに関する整備、及び企業規模や業態に合った内容の見直しを促す。

●個人情報流出対策に関して検証を行い、企業規模や業態に合った対策の実施を促す。

●緊急時における報告体制、復旧のための体制の整備を促す。

●最新の個人情報保護規制に関する情報収集及び社内への継続的な周知を促す。

---

[7] 2019 年 8 月、就活サイト「リクナビ」を運営する株式会社リクルートキャリアが、就活生の内定辞退率を本人の同意なしに予測し、有償で 38 社に提供していたことが報じられた。同月に個人情報保護委員会から勧告・指導を受け、同年 9 月には厚生労働省から行政指導を受けた。また、個人情報保護法に抵触する新たな事実が確認されたことで、同年 12 月に再び、個人情報保護委員会から勧告・指導を受けた。

●外部との取引の際の個人情報保護に関する取り決めの策定、及び取引先への継続的なチェックの実施を促す。

●役職員による個人情報の意図的漏えいに対する対策の整備を促す。

●新規事業、新サービスの開始時における個人情報の取扱いのルール策定、及び倫理面や信義則という点でも問題が無いかどうか検証することを促す。

4. 営業秘密管理監査

（1）営業秘密保護に関わる規制の動向

●1993 年の現行の不正競争防止法の制定以降、2005 年、2015 年に大きな改正がなされている。

●海外の企業への営業秘密の不正流出の事件を契機に、2015 年には営業秘密の侵害の未遂、国外での営業秘密の取得も処罰対象に追加されるなど、営業秘密の流出に関する規制は強化されている。

●一方で、特に退職時前後の営業秘密の不正流出が後を絶たず、個人情報の漏えいと違い、営業秘密の不正流出の立証に時間を要するため、事件化するまでに時間を要してしまう。

●営業秘密とみなされるための３要件は「秘密管理性[8]」、「有用性[9]」、「非公知性[10]」である。（不正競争防止法第 2 条 6 項）

●このうち、一番焦点となる要件は「秘密管理性」である。秘密管理性が認められるためには、主観的に秘密として管理しているだけではなく、客観的にみて秘密として管理されていると認識できる状態にあることが必要とされている。裁判例では、

A. 情報にアクセスできる者が制限されていること（「アクセス制限」。例えば、社員以外の者はアクセスできないような措置がとられているなど）、

B. その情報にアクセスした者にそれが営業秘密であることを認識できるようにしていること（「認識可能性」。例えば、書類に「部外秘」と記載されているなど）、

が必要とされている。ただし、両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、「アクセス制限」は、「認識可能性」を担保する一つの手段であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる（「認識可能性」を満たす）場合に、十分なアクセス制限がないことを根拠に秘密管理性が否定されることはない。もっとも、従業員等がある情報について秘密情報であると現実に認識していれば、営業秘密保有企業による秘密管理措置が全く必要ではないということではなく、何らの秘密管理措置がなされていない場合には秘密管理性要件は満たさないと考えられる。

●必要な秘密管理措置の程度としては、「営業秘密情報と一般情報（営業秘密ではない情報）が合理的に区分されていること」、「営業秘密であることを明らかにする措置」が挙げられる。「合理的に区分されていること」に関しては、営業秘密情報へのアクセス権限の制限や書庫にファイル別、箱別で保管されるなど、企業の規模、業態等に即した媒体の通常の管理方法に即して、営業秘密である情報を含む（一般情報と混在することもありうる。）のか、一般情報のみで構成されるものであるか否かを従業員が判別できればよいとされ、紙の１枚１枚、電子ファイルの１ファイル毎に営業秘密であるか一般情報であるかの

---

[8] 秘密として管理されていること。

[9] 有用な営業上又は技術上の情報であること。有用性が認められるためには、当該情報自体が客観的に事業活動に活用されていたり、利用されたりすることによって、経費の節約、経営効率の改善等に役立つものであることが必要となります。例えば、製造技術や実験データ、顧客リストなどは有用性が認められる情報といえるでしょう。ただし、犯罪の手口など反社会的な情報については、秘密として法的保護の対象とはならず有用性は認められません。

[10] 公然と知られていないこと。非公知性が認められるためには、その情報が保有者の管理下以外では、一般に入手できないことが必要です。例えば、刊行物や特許公報に記載されていたり、学会発表等で公開されたりしている情報については、非公知性は認められません。

表示等を求めるものではない。また、秘密管理措置の具体的な内容・程度は、当該営業秘密に接する従業員の多寡、業態、従業員の職務、情報の性質、執務室の状況その他の事情によって当然に異なるものであり、例えば、営業秘密に合法的かつ現実的に接しうる従業員が少数である場合において、状況によっては当該従業員間で口頭により「秘密情報であること」の確認をしている等の措置で足りる場合もあり得る。

●合理的区分に加えて必要となる秘密管理措置としては、主として、媒体の選択や当該媒体への表示、当該媒体に接触する者の限定、ないし、営業秘密たる情報の種類・類型のリスト化、秘密保持契約（あるいは誓約書）などにおいて守秘義務を明らかにする等が想定される。要するに、秘密管理措置の対象者たる従業員において当該情報が秘密であって、一般情報とは取扱いが異なるべきという規範意識が生じる程度の取組であることがポイントとなる。

（2）営業秘密に関する事件例

時期	法人名	内容・影響
2012 年	ヤマザキマザック	同社の営業担当従業員（中国人）が営業秘密（製品図面）を売却目的で取得（本社のサーバーコンピューターにアクセスし、ハードディスクに複製した）。知人を介して売却先を探す。 ・営業秘密を行為者が使用または開示をしなくても、その前段の「複製を作成すること」等の方法で「営業秘密を領得した」段階で刑事罰を科す、という不正競争防止法第 21 条 1 項 3 号が適用された。
2012 年	新日本製鐵（現日本製鉄）	同社の元社員が方向性電磁鋼板の製造技術を韓国の大手製鉄会社のポスコに提供していた。 ・当時の新日鉄住金がポスコに損害賠償請求の訴訟を提起したが、2015 年 9 月、当時の新日鉄住金がポスコから 300 億円の支払いを受けることで和解し、訴訟は取り下げられた。同社の元社員とも和解が成立した。
2014 年	東芝	当時の同社の提携先の元技術者が韓国企業であるＳＫハイニックスに営業秘密（ＮＡＮＤ型フラッシュメモリの製造技術）を漏えいした（不正に記録媒体に複製して持ち出した）。 ・東芝がＳＫハイニックスに損害賠償請求の訴訟を提起したが、2014 年 12 月、東芝がＳＫハイニックスから 331 億円の支払いを受けることで和解した。提携先の元技術者には懲役 5 年が科せられた。
2015 年	エディオン・上新電機	エディオンの元部長が転職先の上新電機に営業秘密（リフォームに関する商品仕入れ原価や粗利のデータ等）を漏えいした（遠隔操作ソフトをパソコンに仕込み、退職後にパソコン操作で情報を取得していた）。 ・エディオンの元部長と上新電機に損害賠償 1,800 万円の支払いが命じられ、エディオンの元部長には執行猶予付きの有罪判決となった。
2016 年	日本ペイント・菊水化学工業	日本ペイントの元執行役員が菊水化学へ転職する際に、日本ペイントの営業秘密を持ち出し、菊水化学で開示・使用した。

時期	法人名	内容・影響
		・日本ペイントの元執行役員には執行猶予付きの有罪判決となった。
2016 年	NEXCO 中日本	同社の業務委託先の従業員が、同社が発注した 2 件の工事の設計金額に関する情報を特定の工事会社に漏えいし、この工事会社が当該 2 件の工事を落札した。 ・業務委託先の従業員には罰金 100 万円の略式命令が下った。
2016 年	DMG 森精機	同社子会社の従業員が、同社の取引先への機械納入時期といった顧客管理データにアクセスし、約 300 社分の情報を印刷し、不正に持ち出した。
2019 年	アシックス	同社の元社員（同社のシューズに関する品質や性能データへのアクセス権有り）が競合他社へ転職する際に、同社のシューズに関する品質や性能データなど約 36,000 ファイルを持ち出し（社用メールから私用メールに転送）。
2020 年	ソフトバンク	同社の元従業員が基地局の情報を社内サーバーから不正に入手し、ロシアの元外交官に流出させた。 ・元従業員は、執行猶予付きの有罪判決を受けた。ロシア元外交官は書類送検されたが不起訴となった。
2020 年	野村証券	同社の元従業員が法人顧客情報を転職先へ漏えいした。 ・同社と転職先に対して、金融庁から金融商品取引法に基づく報告徴求命令が発出された。
2020 年	積水化学	同社の元従業員がスマートフォンの液晶技術に関する情報を不正に中国企業に漏洩した。 ・SNS を通じて中国企業が元従業員に接触した。元従業員は、執行猶予付きの有罪判決を受けた。
2021 年	ソフトバンク・楽天モバイル	ソフトバンクの元従業員が、社外から自身のパソコンで会社のサーバーにアクセスし、5G に関する営業秘密を不正に入手し、転職先の楽天モバイルに漏えいした。 ・ソフトバンクは元従業員と楽天モバイルに 10 億円の損害賠償請求を提訴した。（漏えいから 1 年 4 か月後）
2021 年	はま寿司・カッパ・クリエイト	カッパ・クリエイトの代表取締役社長（当時）が、はま寿司の営業秘密（売上データ等）を不正に取得し、カッパ・クリエイトの事業活動に使用した疑い。 ・営業秘密の閲覧権限を持つ元部下に依頼し、メール等で受け取っていたいたとみられる。競合企業の営業秘密を侵害したとして、上場企業の現職社長が逮捕されるのは異例。

（3）営業秘密流出に関する会社が負うリスク

●金銭的損失：顧客・取引先への賠償（顧客情報流出の場合）、

●社会的評価の低価
●技術情報やノウハウの流出
●顧客の流出
●民事罰：損害賠償
●刑事罰：罰金、懲役刑等

（4）営業秘密管理に関するポイント考察
●営業秘密保護に関するルール策定
→社外秘、社内秘とする情報の定義、保管・管理方法
●営業秘密にアクセスできる者の制限
→「業務上、その情報をどうしても知っていないといけないのは誰か」という観点から、「どの情報に誰がアクセスできる」ようにするかを決定する。
そのうえでアクセス権限の付与設定を行い、アクセス出来る者を制限する。部署異動や退職時におけるアクセス権限の見直しを適時に行うことも重要。
アクセス制限の方法は企業規模、業態、使用するシステム等によって種々存在する。
●紙ベースの営業秘密情報の管理
→施錠付き書庫、ロッカーでの保管、「社外秘」、「社内秘」等の表示、閲覧の際の管理簿への記帳など
●営業秘密の漏えい禁止の明文化
→就業規則、役員規程等に記載しておくのがベスト。
●入社時、退職時における秘密保持、競業避止に関する契約の締結
→誓約書に署名、捺印をさせて提出させる。
特に退職時に営業秘密の不正持ち出しが発生するため、名刺やファイルを回収し、パソコンも返還の上、アクセス履歴やメール履歴等を確認する。

（5）営業秘密管理に関する監査における監査役の姿勢
前提として、上記（4）のポイントに関する取組状況を、内部統制システムに係る「損失の危険を管理する体制」の整備運用の確認のために、内部監査部門と連携して監査を実施するべきであるが、監査役としては代表取締役を含む取締役及び執行役員等に対し、「営業秘密保護に関する取組＝企業の継続的成長を実現させるための投資」という考えのもと、以下の事項を働き掛けていくことが重要と考えます。
●流出すべきでない営業秘密の確定及び保管・管理方法の検討を促す。
●営業秘密へのアクセス権限の適宜の見直しを促す。

●役職員による営業秘密の意図的漏えいに対する対策の整備を促す。

5. 情報セキュリティ監査まとめ

（1）企業における情報セキュリティ全般に関する課題の考察

IT 技術の進展、インシデント事例等により、個人情報や営業秘密といった重要情報が流出することに関する問題意識は高まっている。しかし、

●そもそも何から対策を講じるべきか分からない。

●対策を講じたいがコストを多大に投じたくない。

●役職員の間でセキュリティに関する意識の差が大きい。

●社内ルールを策定したが、策定後一度も改訂されず、実態との乖離が発生している。

●情報セキュリティを担当する人員、ノウハウ、スキルが不足している。

●法規制の変化のキャッチアップが難しい。

（2）情報セキュリティ全般に関する監査全体のポイント考察

●情報通信に関する技術やサービスの進歩は今後も続く傾向が予想される。（5G、電子契約、会計システムのクラウド化、キャッシュレス社会など）

●情報セキュリティに関しても、ウイルス対策ソフトに加えて、現在では様々なサービス（ペネトレーションテスト、SOC サービスなど）がリリースされている。

●一方で、サイバー攻撃の手口も巧妙化しており、また依然として人的リスク（誤送信、紛失、不正な持ち出し）も残っている。

●情報セキュリティに関する対策は今後も強化が要請される一方で、自社の規模、業態、取り扱っている情報、リソースを踏まえて適切なルール策定、対策実施が求められる。

こうした中で、情報セキュリティを維持し、個人情報や営業秘密の流出を防止するためには、**情報セキュリティに関するルールを自社の規模、リソースに合わせて適切に策定した上で、物理的対策[11]・技術的対策[12]・人的対策[13]を、自社の規模、業態、取り扱っている情報、リソースを踏まえてバランス良く実施す**

---

[11] システムやデータ、ネットワークなどのセキュリティリスクに対して、ハードウェアやソフトウェアから対応する対策である。技術的なセキュリティリスクは「ウイルス対策」や「不正アクセス」「データ保護」など分野が多岐にわたるため、何に対する対策なのか明確化することが大切である。
また、技術は日ごとに進歩しているため、随時、対策の見直し・更新を行っていくことが必要になる。
具体的には、「ウイルスや不正アクセスへの対策としてのツールやシステムの導入・設定」、「アクセス制限や、データの利活用・OS のアップロードなどに関するルールの明確化」が挙げられる。

[12] 不法侵入や破壊、紛失や災害などのセキュリティリスクに対応するための対策である。
具体的には、「監視カメラ、警備員、スマートロックや生体認証などの設置・導入」、「入退室や来社の記録取得」、「火災や地震への対策」が挙げられる。

[13] 従業者のミスや不正など、人によるセキュリティリスクに対応するための対策である。

ることが重要である。監査役としては「情報セキュリティ対策＝企業を守り、継続的成長を実現させるための投資」と「企業規模、業態に合わせた効率的かつ実効的な対策」を両立させるため、代表取締役を含む取締役及び執行役員等に対し、**ルール策定や対策の実施を促しつつ、策定されたルールや対策の適正性を検証し、より良い内容へのアップデートを促すという姿勢**が今後求められる。

具体的には、「役職員への研修」、「ルールやマニュアルの整備」が挙げられる。

第269回監査実務研究会出典一覧

①「個人情報保護法、１０年ぶりの改正！」
新日本法規出版株式会社　2015年11月18日　森山裕紀子氏
https://www.sn-hoki.co.jp/articles/article090500/
②「個人情報の保護に関する法律等の一部を改正する法律について」
個人情報保護委員会　2021年4月27日
https://www.soumu.go.jp/main_content/000747671.pdf
③情報セキュリティ意識に関する実態調査レポート2021～コロナ禍で高まる「シャドーIT」の情報セキュリティリスク～
キャノンマーケティングジャパン株式会社　2021年7月8日
https://eset-info.canon-its.jp/malware_info/special/detail/210708.html
④「2021年 上場企業の情報漏えいの半数はサイバー攻撃 ～ 東京商工リサーチ 調査」
株式会社イード　2022年1月21日　ScanNetSecurity
https://scan.netsecurity.ne.jp/article/2022/01/21/46986.html#:~:text=%E5%90%8C%E8%AA%BF%E6%9F%BB%E3%81%AB%E3%82%88%E3%82%8B%E3%81%A8%E3%80%81202
1,%E3%82%92%E8%A8%98%E9%8C%B2%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%80%82
⑤「国内におけるインシデント報告傾向を見てみる」
日本電気株式会社　2022年7月29日　NECセキュリティブログ　郡義弘氏
https://jpn.nec.com/cybersecurity/blog/220729/index.html
⑥2021年度「個人情報の取扱いにおける事故報告集計結果」
日本情報経済社会推進協会（JIPDEC）プライバシーマーク推進センター　2022年10月7日
https://privacymark.jp/system/reference/pdf/2021JikoHoukoku_221007.pdf
⑦第250回 監査実務研究会 報告「DX 、サイバーセキュリティへの監査役の対応」
監査懇話会　2021年7月19日　小川重光氏
https://kansakonwakai.com/course/audit-practical-work-
group/%e7%9b%a3%e6%9f%bb%e5%ae%9f%e5%8b%99%e7%a0%94%e7%a9%b6%e4%bc%9a%e3%81%ae%e5%ae%9f%e7%b8%be%ef%bc%882021%e5%b9%b4%e5%ba%a6%ef%bc%89/

⑧「【知っておくべき】サプライチェーン攻撃とは？手口や対策法解説！」
株式会社ベルテクノス　Office110
https://office110.jp/security/knowledge/cyber-attack/supply-chain-attacks
⑨「世界の個人情報保護法を比べてみた！GDPR・CCPA・PDPA など一挙紹介」
株式会社 Acompany　2022 年 6 月 15 日　プライバシーテック研究所
https://acompany.tech/privacytechlab/global-personal-information-protection-law-gdpr-ccpa-pdpa/
⑩「個人情報漏洩事件・被害事例一覧」
株式会社セキュアオンライン　サイバーセキュリティ.com
https://cybersecurity-jp.com/leakage-of-personal-information
⑪「中小企業の情報セキュリティ対策ガイドライン（第 3 版）」
独立行政法人情報処理推進機構　2021 年 3 月 10 日
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
⑫「【企業向け】情報漏洩対策の完全ガイド｜情報漏洩で重要な 2 つの視点」
NTT 東日本　2022 年 7 月 6 日　クラソル
https://business.ntt-east.co.jp/content/cloudsolution/column-283.html#section-2
⑬内定辞退予測サービス「リクナビ問題」は何が問題だった？プライバシー保護の観点から考察
株式会社 Acompany　2022 年 5 月 20 日　プライバシーテック研究所
https://acompany.tech/privacytechlab/rikunabi-privacy-protection-what-is-the-problem-2019/#:~:text=%E3%81%BF%E3%82%88%E3%81%86%E3%81%A8%E6%80%9D%E3%81%86%E3%80%82-,%E3%83%AA%E3%82%AF%E3%83%8A%E3%83%93%E4%BA%8B%E4%BB%B6%E3%81%AE%E6%A6%82%E8%A6%81,%E8%A1%8C%E6%94%BF%E6%8C%87%E5%B0%8E%E3%82%92%E5%8F%97%E3%81%91%E3%81%9F%E3%80%82
⑭「営業秘密管理指針」
経済産業省　2019 年 1 月 23 日
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf
⑮「不正競争防止法における営業秘密の保護」
近江法律事務所　2014 年 7 月　中小企業の法律相談
https://www.oumilaw.jp/kouza/105.html#:~:text=%E4%B8%8D%E6%AD%A3%E3%81%AE%E5%88%A9%E7%9B%8A%E3%82%92%E5%BE%97%E3%82%8B%E7%9B%AE%E7%9A%84%E5%8F%88%E3%81%AF%E5%96%B6%E6%A5%AD%E7%A7%98%E5%AF%86%E3%81%AE,1%E5%8F%B7%EF%BD%9E7%E5%8F%B7%EF%BC%89%E3%80%82

⑯「過去の営業秘密流出事件」
特許と営業秘密と知財戦略～営業秘密ラボ～　2022 年 4 月 11 日最終更新　弁理士　石本貴幸氏
https://www.xn--zdkzaz18wncfj5sshx.com/p/blog-page_29.html
⑰「社員による営業秘密の持ち出し、何が問題？必要な対策を解説」
MIKATA 株式会社　2021 年 4 月 8 日　オフィスのミカタ
https://officenomikata.jp/coverage/12143/#:~:text=%E5%96%B6%E6%A5%AD%E7%A7%98%E5%AF%86%E3%81%AE%E6%8C%81%E3%81%A1%E5%87%BA%E3%81%97%E3%81%AB%E3%82%88%E3%82%8A,%E3%81%99%E3%82%8B%E5%8F%AF%E8%83%BD%E6%80%A7%E3%81%8C%E3%81%82%E3%82%8B%E3%80%82
⑱「金融分野におけるサイバーセキュリティ対策について」　　金融庁
https://www.fsa.go.jp/policy/cybersecurity/index.html
⑲「技術的・物理的・人的対策とは？」
株式会社 LRM　2021 年 2 月 23 日　「現役コンサルタントが解説　ISMS 徹底解説ブログ」　石濱雄基氏
https://www.lrm.jp/iso27001/blog/security/8321/