参考資料４

秘密情報管理に関する各種ガイドライン等について

各章ごとに参考になるガイドライン等を紹介します。

【第２章　保有する情報の把握・評価、秘密情報の決定】

■知的財産の利用に関する独占禁止法上の指針（公正取引委員会）

http://www.jftc.go.jp/dk/guideline/unyoukijun/chitekizaisan.html

知的財産のうち技術に関するものを対象として、技術の利用に係る制限行為に対する独占禁止法の適用に関する考え方を包括的に明らかにした指針。本書第２章２－２「秘密情報の決定」における技術情報の活用方法を検討する際に参考になります。

■個人情報の保護に関する事業分野ごとのガイドライン一覧（個人情報保護委員会）

http://www.ppc.go.jp/files/pdf/personal_guideline_ministries.pdf

事業者が個人情報の保護に関する法律に基づき、個人情報の適切な取扱いの確保に関して行う活動を支援するため、事業分野ごとの具体的な指針が示されています。本書第２章２－２「秘密情報の決定」を検討する際に参考になります。

【第３章　秘密情報の分類、情報漏えい対策の選択及びそのルール化】

■情報セキュリティ関係

(1) 組織における内部不正防止ガイドライン

（独立行政法人情報処理推進機構（ＩＰＡ））

https://www.ipa.go.jp/security/fy24/reports/insider/

組織において、内部不正による情報セキュリティ事故を防止するためのガイドライン。第３章３－４「具体的な情報漏えい対策例」の情報システム関連の対策については、本ガイドラインも参考にしています。

(2) ＩＳＭＳ関係（JISQ27001、JISQ27002）

①JISQ27001、JISQ27002

情報セキュリティマネジメント（ISMS）は、組織のマネジメントとして情報の機密性、完全性、可用性を維持することを目的としており、JISQ27001 及び JISQ27002 は、ISMS を実施する際の要求事項等を定めたものです。情報セキュリティマネジメントの観点から情報漏えい対策を検討する場合や、取引先の漏えい対策の状況を確認する際に参考になります。

また、ISMS の認証を行う ISMS 適合性評価制度が運用されており、一般財団法人日本情報経済社会推進協会(JIPDEC)から認定された「認証機関」に申請す

ることで認証を受けることができます。

ISMS 適合性評価制度　（JIPDEC 情報システムマネジメントセンター）
http://www.isms.jipdec.or.jp/isms.html

②情報セキュリティ管理基準（経済産業省）、情報セキュリティ監査制度

JIS Q 27001 のほかに「情報セキュリティマネジメント実践のための規範（ベストプラクティス）」として、JIS Q 27002 が策定されています。これらに基づいて、マネジメント基準や技術基準など具体的な管理策をまとめた「情報セキュリティ管理基準」が経済産業省より公開されており、ISMS 認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織等幅広い利用者を想定して情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定。

情報セキュリティ監査制度、情報セキュリティ管理基準（経済産業省）
http://www.meti.go.jp/policy/netsecurity/index.html

(3) 情報セキュリティ対策のしおり（ＩＰＡ）

http://www.ipa.go.jp/security/antivirus/shiori.html

①ＩＰＡ対策のしおりシリーズ

一般のご家庭や企業・組織の方々を対象に、情報セキュリティ上の様々な脅威への対策をテーマ別（ウィルス対策、不正アクセス対策、情報漏えい対策、インターネット利用時の危険対策、標的型攻撃メール対策、暗号化による対策等）に分かり易く説明した小冊子シリーズ。情報セキュリティ上の対策を検討する際に参考になります。

②ＩＰＡセキュリティマネジメントのしおりシリーズ

情報セキュリティ対策を実施する企業・組織の経営者、管理者、従業者の方々を対象とした小冊子シリーズ。中小企業において情報セキュリティ対策を検討する場合、自社の対策状況のチェックや他社の対策状況と比較する際に参考になります。

【第４章　秘密情報の管理に係る社内体制のあり方】

■サイバーセキュリティ経営ガイドライン（経済産業省、ＩＰＡ）

http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

情報システムの専門部署を持ち、IT を利活用する企業の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」及び経営者が担当幹部に指示すべき「重要１０項目」をまとめたもの。秘密情報の管理に係る社内体制を検討する際に参考になります。

【第５章　他社の秘密情報に係る紛争への備え】

■先使用権制度の円滑な活用に向けて－戦略的なノウハウ管理のために－（特許庁）

https://www.jpo.go.jp/shiryou/s_sonota/senshiyouken.htm

先使用権制度の明確化と先使用権の立証手段の具体化を図り、先使用権制度がより円滑に活用されることを目的に、有識者による委員会での議論の結果を踏まえて、特許庁が作成し公表したもの。

第三章中の「証拠力を高めるための具体的な手法の紹介」では、公証制度、タイムスタンプが紹介されており、本書第５章５－１「自社情報の独自性の立証」を検討する際に参考になります。

【第６章　漏えい事案への対応】

■高度サイバー攻撃への対処におけるログの活用と分析方法

（一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））

https://www.jpcert.or.jp/research/apt-loganalysis.html

企業の情報セキュリティにおけるインシデントの対処に対して、情報漏えい事案の調査や、解析に資するログの活用と分析方法について解説したもの。情報漏えい事案に対応する調査分析方法等を検討する際に参考になります。

■CSIRT マテリアル（一般社団法人 JPCERT/CC）

http://www.jpcert.or.jp/csirt_material/

企業の情報セキュリティにおけるインシデントに対して迅速に対応する CSIRT(Computer Security Incident Response Team)=「コンピューターセキュリティインシデントに対応するチーム」の構築について解説したもの。情報漏えい事案に対応する組織構築を検討する際に参考になります。