平成26年度　経済産業省委託調査

営業秘密管理の実態に関する調査研究

報告書

平成２７年３月

三菱UFJリサーチ&コンサルティング

（空白）

■目次

序. 1
Ⅰ. 秘密情報管理に対する関心の高まり 3
Ⅱ. 日本企業における秘密情報管理の実態と課題 6
１. 秘密情報管理に対する考え方 6
（１）秘密情報管理に対する考え方 6
（２）秘密情報管理の社内における位置づけ 7
２. 秘密情報管理に係る体制 10
（１）組織体制の実態 10
（２）関連規程の整備実態 15
（３）情報区分の考え方 17
３. 物理的な管理 21
（１）情報システムの管理 21
（２）情報機器の管理 24
（３）紙媒体の管理 27
（４）施設の管理 30
４. 労務管理 34
（１）従業員の採用 34
（２）従業員との契約締結 34
（３）従業員に対するエンフォースメント 36
（４）研修・人材育成 38
（５）退職者に対するフォロー 40
（６）その他 44
５. 取引先管理 45
（１）パートナー企業との契約 45
（２）パートナー企業の選定と調査・監査の実施 46
（３）パートナー企業の管理 47
６. グローバル拠点の管理（日本企業の場合） 49
７. 中小企業における実態 50
（１）秘密情報管理に対する考え方 50
（２）秘密情報管理に係る体制 51
（３）物理的な管理 52
（４）労務管理 53
（５）取引先管理 54
（６）グローバル拠点の管理 55
Ⅲ. 米国企業における秘密情報管理の実態 57
１. 米国企業における秘密情報管理の考え方 57

（１）米国企業における秘密情報管理の捉え方 57
（２）秘密情報管理の社内における位置づけ 58
２．　秘密情報管理に係る体制 61
（１）組織体制の実態 61
（２）関連規程の整備実態 62
（３）情報区分の考え方 65
３．物理的な管理 68
（１）情報システムの管理 68
（２）情報機器の管理 71
（３）紙媒体の管理 72
（４）施設の管理 74
４．労務管理 76
（１）従業員の採用 76
（２）従業員との契約締結 77
（３）従業員に対するエンフォースメント 78
（４）研修・人材育成 80
（５）退職者に対するフォロー 82
５．取引先管理 84
（１）パートナー企業との契約 84
（２）パートナー企業の選定と調査・監査の実施 84
（３）パートナー企業の管理 85
６．グローバル拠点の管理 87
Ⅳ．諸外国における秘密情報管理の実態 88
１．ドイツ企業の実態 88
（１）ドイツ企業における秘密情報管理の捉え方 88
（２）秘密情報管理に係る体制 89
（３）物理的な管理 89
（４）労務管理 90
（５）取引先管理 92
（６）グローバル拠点の管理 93
２．中国の実態 94
（１）中国企業における秘密情報管理の捉え方 94
（２）秘密情報管理に係る体制 94
（３）物理的な管理 95
（４）労務管理 96
（５）取引先管理 97
（６）グローバル拠点の管理 97
Ⅴ．情報漏えいに係る事後対応 98

１．情報漏えい事例 98
（１）国内における事例 98
（２）海外における事例 100
２．国内企業における事後対応の実態 102
（１）検知の仕組み 102
（２）内部監査、社内調査による検知 105
（３）事後対応の実態 105
３．海外企業における事後対応の実態 107
（１）検知の仕組み 107
（２）内部監査、社内調査による検知 109
（３）事後対応の実態 110
Ⅵ. 秘密情報管理のポイント 111
１．秘密情報管理に係る体制 111
２．物理的な管理 113
３．労務管理 115
４．取引先管理 117
５．グローバル拠点の管理 117
６．情報漏えいに係る事後対応 118

序.

本調査研究は、経済産業省における営業秘密管理指針見直しに関連した検討の基礎資料とすべく、国内外の最新の情報漏えい手口や、情報管理に関するグッドプラクティス及びベストプラクティス、情報漏えい後の迅速な検知・証拠確保方法のグッドプラクティス及びベストプラクティスなどを明らかにすることを目的として実施したものである。本調査研究の開始後に、従前の営業秘密管理指針の内、不正競争防止法の法解釈などのガイドラインに係る部分が 2015 年 1 月 28 日に公表された営業秘密管理指針として全部改訂され、本調査研究報告書作成時点では、別途「営業秘密管理マニュアル（仮称)」の策定に向けた検討が行われており、本調査研究によって整理されたグッドプラクティス及びベストプラクティスが今後策定される「営業秘密管理マニュアル（仮称)」や経済産業省における関連施策検討の一助となれば幸いである。

なお本調査研究報告書は、本調査研究事業において実施した国内外の文献調査及びヒアリング調査の結果を取りまとめたものである。ヒアリング調査については、下記の通り多数の企業及び有識者にご協力を頂いたが、特に個社の事情については当該企業の秘密情報であることから、本調査報告書上は匿名としている。個社名、ご担当者名は掲載できないが、ご多忙な中、本調査研究にご協力頂いた各位にはこの場を借りて謝意を申し上げたい。

海外企業及び海外有識者のヒアリング調査については、スクワイヤ外国法共同事業法律事務所の井口加奈子パートナー弁護士と、オリック・ヘリントン・アンド・サトクリフ LLP の矢倉信介パートナー弁護士の協力をそれぞれに頂いて実施した。本調査研究テーマの性質上、特に海外企業に対するヒアリング調査は容易ではなかったが、両先生には大変なご尽力を頂いた。

【ヒアリング調査の実施状況】

国内大企業（製造業）	業種のバランスを意識しつつ、国内のリーディングカンパニーの中から選定。	12 社
国内大企業（非製造業）	業種のバランスを意識しつつ、国内のリーディングカンパニーの中から選定。	3 社
国内中小企業（製造業）	経済産業省からご推薦頂いた中小企業を対象とした。	4 社
国内有識者（有識者）	本テーマについて国内外の事情に精通する弁護士、フォレンジック会社有識者、大手情報ベンダー有識者。	4 者
米国企業（製造業）	業種のバランスを意識しつつ、米国のリーディングカンパニーの中から選定した。	11 社
米国企業（非製造業）	業種のバランスを意識しつつ、米国のリーディングカンパニーの中から選定した。	2 社
米国有識者（有識者）	本テーマについて米国の事情に精通する弁護士。	4 者
ドイツ企業（製造業）	ドイツの大規模製造業。	1 社

ドイツ有識者（有識者）	本テーマについてドイツの事情に精通する弁護士。	1 者
中国企業（製造業）	中国の大規模製造業。	1 社
中国企業（非製造業）	中国の非製造業。	1 社
中国有識者（有識者）	本テーマについて中国の事情に精通する弁護士。	1 者
合計		45 者

最後に、本調査研究報告書における用語法についてであるが、「営業秘密」という用語については日本であれば不正競争防止法上の定義に該当する場合、海外調査であれば各国の法令などにおいて定義されている「営業秘密」を指す場合にのみ使用している。また、「秘密情報」とは、ヒアリング調査などに対応頂いた企業において秘密として管理の対象とすべき情報全般を呼んでおり、「営業秘密」を包含する概念として用いている。

Ⅰ．秘密情報管理に対する関心の高まり

相次ぐ大企業における情報漏えいや技術流出が大きく報道される中、営業秘密管理に対する企業や社会の関心は大いに高まっている。情報漏えいや技術流出自体はそれほど新しい問題とは言えないが、近年は海外への情報漏えいや技術流出が顕在化していることや、国内における事案であっても個人情報など、一般国民の関心の高い情報漏えいも相次いでいることが、世の中の関心を高めていることは間違いないであろう。

表 1：国内における主な情報漏えいの事案

時期 （問題が公となった時期など）	事案の概要
2007 年	デンソーの元社員が、同社の図面データなどを大量にダウンロードして無断で持ち出し、私有の記録媒体に複製したとされている事案。
2012 年	新日鐵住金の元技術者が、退職後に韓国の大学に招聘された際にポスコに対して新日鐵住金の製造技術情報を漏えいさせていたとされる事案。
2012 年	ヨシツカ精機の元社員が、中国企業と提携していた企業の社員と共謀し不正の利益を得る目的で同社の図面データを漏えいさせていたとされる事案。
2012 年	ヤマザキマザックの元社員が退職を申し出た後に、不正の利益を得る目的で同社の図面情報などを含む大量のデータを複製したとされている事案。
2014 年	東芝の提携先であるサンディスクの元技術者が、東芝の研究データを不正に複製し、韓国 SK ハイニックスに転職した際に当該データを漏えいさせていたとされる事案。
2014 年	日産自動車の元社員が、同社の新車販売計画などを含む大量のデータを、いすゞ自動車への転職前に不正に複製したとされている事案。
2014 年	ベネッセコーポレーションのシステム運用を行っているグループ会社の業務委託先の元社員が、大量の顧客情報を不正に持ち出し、利益を得る目的で名簿業者に売却したとされている事案。

（参照：各社プレスリリース及び各種報道資料より作成）

この点、平成 24 年度に経済産業省が実施したアンケート調査[1]によれば、過去５年間で

[1] 経済産業省（委託先：三菱 UFJ リサーチ&コンサルティング株式会社）「平成 24 年度経済産業省委託調査　人を通じた技術流出に関する調査研究報告書（別冊）」（2014 年 3 月）。

の何らかの営業秘密の漏えい事例があったと回答している企業は 13.5%[2]となっている。当該調査では規模別にも集計が行われているが、従業員規模 3001 人以上の大企業に限ってみると 39.9%[3]の企業が明らかに又はおそらく漏えいありと回答しており、情報漏えいないし技術流出が企業にとっても身近な問題であることがうかがえる。このように秘密情報管理に対する関心が高まっているのは、日本だけでなく、欧米の主要国においても同様の傾向がある。例えば、米国でも情報漏えいや技術流出事件は頻発しており、例えば以下のような著名な事例が知られている。

表 2：米国における主な情報漏えいの事案

時期（問題が公となった時期など）	事案の概要
2005 年	General Motors の元技術者が、自身と夫が運営する中国企業の利益のために、ハイブリッド車技術などの情報を不正に持ち出したとされている事案。
2010 年	Valspar Corporation の元化学者が競合企業への転職前に同社の技術データなどを含む内部資料を私有の USB に複製したとされている事案。
2011 年	Motorola の元技術者が、中国軍向けの通信技術を開発する企業の利益のために、非常に重要な通信技術の情報などを不正に持ち出したとされる事案。
2011 年	Ford Motor Company の元技術者が競合企業へ転職するに際して、同社の設計情報などを含む大量の内部資料を不正に私有の記録媒体に複製して持ち出したとされている事案。

（参照：White House, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 及び各種報道資料より作成）

2013 年２月には、関係政府機関と連名でホワイトハウスから「営業秘密侵害を低減するための米国政府戦略（ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS）」と題する方針を公表し、国をあげて情報漏えいないし技術流出に取り組む姿勢を明らかにしたことからも、連邦政府も高い関心を示していることがうかがえる。

また米国における本件テーマの関心の高さをうかがわせる報道や各種レポートが多数見られるが、例えば米国の非営利団体である CREATe.org が公表しているレポート「Trade

[2] 経済産業省・前掲注 1、50 頁。
[3] 経済産業省・前掲注 1、143 頁。

Secret Theft: Managing the Growing Threat in Supply Chains」[4]では上記のような情報漏えいや技術流出事件の経済的なインパクトについて紹介が行われていたり、CREATe.org がPricewaterhouseCoopers LLP（PWC）と連名で公表している「Economic Impact of Trade Secret Theft」[5]において不数の代替手法を総合的に考慮し、米国における営業秘密侵害の経済的損失を GDP の１％～３％と試算した結果を公表するなど、情報漏えいないし技術流出の量的な影響度についての議論も盛んとなってきていることもうかがえる。

[4] CREATe, Trade Secret Theft: Managing the Growing Threat in Supply Chains. 日本語版「営業秘密の窃盗 サプライチェーンにおいて増大する脅威を管理する」も公表されている。
[5] CREATe/PWC, Economic Impact of Trade Secret Theft (2014). 日本語版「営業秘密の窃取がもたらす経済的影響」も公表されている。

Ⅱ．日本企業における秘密情報管理の実態と課題

日本企業における秘密情報管理の実態について、本調査研究で実施した国内企業に対するヒアリング調査の結果を中心に、整理を行った。

１．秘密情報管理に対する考え方

（１）秘密情報管理に対する考え方

秘密情報管理の重要性に対する認識の程度や秘密情報管理の位置づけなどは、以下のとおり、各社によって様々である。

意識の高い企業においては、これを経営レベルの問題と捉え、独自の考え方で整理しているプラクティスが見られた。例えば、製造業では従前から安全管理や品質管理といった観点からコンプライアンス[6]を重視した経営が行われているが、今回実施したヒアリング調査においてもコンプライアンスの観点から情報漏えいはあってはならず、秘密情報管理の必要性を強く認識しているというプラクティスが見られた。

一方、非製造業では秘密情報を含む会社情報を「資産」と捉え、これを適切にマネジメントしていくことで、経営目標を実現する手段として秘密情報管理を捉えているプラクティスや、より直接的に、情報漏えい対策を企業の責任のみと捉えるのではなく、顧客満足度を高めるための手段（サービスの一部）と捉えているといったプラクティスが見られた。

また、顧客から高度な秘密情報管理を具体的に求められている企業においては、むしろ自社の秘密情報管理レベルの高さや情報漏えい対策を積極的な PR 材料としているというプラクティスも見られた。

【秘密情報管理に対する企業内での考え方（ヒアリング調査結果)】

- 当社の基本的なスタンスとして、安全管理と法令遵守の徹底を重視しており、情報漏えいについてもこうした観点からあってはならないことであると認識している。他社との比較分析をした訳ではないが、秘密情報管理に対する社長を含む経営層の意識は極めて高い。特に社会的な影響があるものについては、対外的な公表も含め記者会見を 24 時間以内に実施できることをルールとしており、過去にあった事故についても、事実確認を含め迅速に情報収集し、必要に応じ対外公表することになっている。（製造業）
- 秘密情報管理ないし情報セキュリティについては､単なる情報漏えい対策として位置づけず、情報セキュリティマネジメントとして捉えており、情報資産取り扱いの側面から、「業務改善活動」として位置づけている。とくに、経営層が問題を認識する事が大前提であり、マネジメントの問題であることを理解することが重要となる｡経営者にこの認識を持たせる事は、

6 コンプライアンスとは、法令や社会的な規範などを遵守した活動のことを指す。

秘密情報管理ないし情報セキュリティの第一歩であると言える。（非製造業）

- 秘密情報管理ないし情報セキュリティは業務推進を阻害するものであると認識されていたが、当社では自社のミッション・ビジョンを下支えするものであり、経営視点での取組が必要であると認識している。（非製造業）
- 情報セキュリティという表現を用いた場合、「セキュリティ」という言葉が守りをイメージさせるが、本来は業務改善の要になる重要な役割を担うもので、結果として売上・利益の源泉になるという事を全社的に周知させていく必要がある。（非製造業）
- 「企業の社会的責任の遂行」という考え方ではなく、顧客満足度の向上を目指していく事が求められる（顧客に迷惑を掛けない秘密情報管理という発想から、顧客満足度を高める秘密情報管理という発想への転換が必要）。（非製造業）
- 重要な取引先情報を取り扱う当社のような業種においては、ISO などの第三者認証を取り、認証機関などによる外部審査を受けていることは業界標準的な取組となっている。そのため、ある程度の秘密情報管理ないし情報セキュリティは出来て当たり前となっている。それでも近年は情報漏えいに対する懸念から、秘密情報管理実態について顧客から詳細に説明するよう求められることが増えており、顧客に安心してもらえる仕組みを構築していることが営業上も重要となっている。当業界の中堅企業の中には、あえて第三者認証を取得せずに独自に構築している秘密情報管理体制がISO などのフレームよりも厳格であることをアピールする手法も目立っている。（非製造業）

（２）秘密情報管理の社内における位置づけ

秘密情報管理の仕組みについて、社内におけるマネジメントシステム[7]の一部と捉え、PDCA[8]を意識した運用体制の構築や、マネジメントシステムに係る第三者認証を活用して社内体制の整備や継続的な運用を行っているというプラクティスも見られた。国内企業が活用している第三者認証は、個人情報保護に係るプライバシーマーク[9]と情報セキュリティに係る情報セキュリティマネジメントシステム（Information Security Management System：

7 ここでマネジメントシステムとは、経営目的を実現するためのマネジメントを実践していくための制度や体制といった仕組み全般のことを指す。

8 PDCA とは、基本的なマネジメントサイクルとして認識されている、Plan（計画）、Do（実行）、Check（評価）、Act（改善）のプロセスのことである。このプロセスを繰り返すことで、業務の継続的な改善を行っていくことが意図されている。

9 プライバシーマーク制度を運用している一般財団法人日本情報経済社会推進協会（JIPDEC）によれば、「プライバシーマーク制度は、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者などを認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です。」と定義されている。

＜http://privacymark.jp/privacy_mark/about/outline_and_purpose.html＞

ISMS）[10]などが知られているが、ヒアリング調査の中でもこれらを活用している企業があった。標準化されたこれらのスキーム[11]を活用することで、秘密情報管理体制の高度化や対外的な説明が容易となるというメリットはあると思われる。しかし、ヒアリング調査では、当初プライバシーマークを取得したものの、当該企業における管理体制高度化の取組と適合せず、他のスキームを採用することを検討しているといったプラクティスもあった。

標準化されたスキームは有用であるが、各社の実情に合わせて活用していくことが重要であり、あくまで秘密情報管理を高度化するための手段の１つとして捉える事が重要であると考えられる。

【秘密情報管理の社内における位置づけ（ヒアリング調査結果)】

- 秘密情報管理についても、各種施策に実効性を持たせるための IT を導入しつつ、それぞれについてPDCAサイクルを回しながら施策を実施することで徐々に管理の仕組みを発展させている。(製造業)
- 第三者認証としては、プライバシーマークと ISMS を取得している。取得の背景は、当社グループの中核企業が導入の大号令を出した事が始まりであるが、現在、中核企業はプライバシーマークを返上している（製造業を担う中核企業においては、個人情報と言っても従業員情報が主となるため第三者認証を対外的には取得する必要性が低かったため）他、ISMS もシステム部門でしか取得していない。現在、取引先からも第三者認証を求められることも増えており、当社としては業務推進上も第三者認証を取得・維持することは重要視されている。第三者認証に関する課題は２つあり、１つ目は M&A によりグループ化された会社に同様のルールを適用する事が困難である事、２つ目は維持に係る業務負担が大きく事務局の負担が大きくなる事である。なお、多くの企業が属人的な繋がりでマネジメントを行うなか、当社が組織的に対応出来ている理由は、ISMS が業務上必要とされ、その徹底が出来ていたからだと想定される。(非製造業)
- プライバシーマークは一度導入したものの、当社の管理体制高度化実現に向けた取組に適合しにくい点が見られたため、現状は導入を中止し、代替として ISO27001 の導入を検討中である。(製造業)
- 情報システムの信頼性や安全性などについてのシステム監査を受けた際に、「社会的な説明責任を果たしていない」と指摘された。具体的には ISO や ISMS などの評価尺度に即した整理が必要というものであった。経営層は ISO について懐疑的ではあったが、技術部門と情報システム部門の部門認証にて認証を 2015 年中に受ける準備を進めている。(製造業)
- セキュリティ・ポリシーにおける施策の区分は情報セキュリティマネジメントに関する国際規格である ISO27001 に準拠している。(製造業)
- ISMS に関しては、事業所単位で導入をしていため、当該事業所内に事務局を設置して対応しているが、事務局への情報提供やスケジュール管理など後方支援を本社部門であるマネジ

[10] ISMS は、情報管理に係る規格ではなく、情報セキュリティに係る規格であり、ISO/IEC27001、JISQ27001 が認証基準となっている。

[11] スキームとは、体系的に整理された仕組みや手段のことである。

メント推進部が行っている。（非製造業）

２．秘密情報管理に係る体制

（１）組織体制の実態

ヒアリング調査の結果、一定の規模以上の大企業では、経営者のコミットメント[12]の下で秘密情報管理に係る方針策定や体制整備を行うことを組織制度として担保するため、経営者をメンバーとする委員会組織を設置するというプラクティスが見られた。どのような委員会組織に秘密情報管理を所管させるかについては企業によって異なる（なお、今回実施したヒアリング調査の中では「情報セキュリティ委員会」を設置し、これが秘密情報管理を所管している例が少なくとも、国内大企業 15 社中 3 社において見られた)。いずれの企業においても委員会組織においては、役員がリーダーシップを取ることが予定されているものの、それほど頻繁に開催するものではなく、実務レベルでは委員会組織よりも下位の会議体を設置して、関連規程の整備や組織の運用を行っていた。委員会組織においてリーダーシップを取る役員としては、明示的にチーフ・セキュリティ・オフィサー（CSO）、チーフ・インフォメーション・オフィサー（CIO）を設置しているプラクティスが見られた他、情報セキュリティ施策を統括する部門長を取締役並みの権限を付与した執行役員としているプラクティスも見られた。

【秘密情報管理に係る組織体制（ヒアリング調査結果)】

- 常設の委員会としては、「コンプライアンス推進委員会」「リスク管理委員会」「情報セキュリティ委員会」があり、そのほかにも必要に応じて随時開催されるものもある。「コンプライアンス推進委員会」「リスク管理委員会」は取締役会メンバーが参加するもので年に 1 回開催され、別途実務レベルでの事務局会議が年に 2 回開催される。「情報セキュリティ委員会」は規程の起案などの実務寄りの委員会であり、前者の各部門から出席者が集まるもので年に 2 回開催される。(製造業)
- 仕組みとしては、独立した委員会組織である情報セキュリティ委員会を年 2 回程度開催し、大きな方針を確認している（委員長は法務担当役員)。この下部組織として、部長級職員による情報委員会という会議（委員長は法務部長）を毎月という頻度で開催し、ガイドラインの運用を含め具体的な情報漏えい対策などについて討議、情報共有を行っている。(製造業)
- チーフ・セキュリティ・オフィサー（CSO）とチーフ・インフォメーション・オフィサー（CIO）を共同議長とする情報セキュリティ委員会のもとに、部門ごとの情報管理責任者の合議体を設置し、横串を通したガバナンスを実施している。部門ごとの責任者は各部門の管理部の部長である場合が多い。上記の委員会による横断的な管理は、国外の拠点でも地域別に実施される。地域の拠点ごとに CSO が配置される。（製造業）
- 当社で発生した技術情報流出事件以降、社内の体制を見直し、経営層とのコミュニケーショ

[12] コミットメントとは、経営学などの領域においては、達成すべきゴールを示し、このゴール達成に向けて責任を持つという意味で用いられる。ここでは経営者が、秘密情報管理体制を整備するということについて、責任を持って取組むという意味で用いている。

ンを取りつつ制度や仕組みの導入を進めてきた。当社の経営本部の情報セキュリティ施策を兼務統括する部門の執行役員兼部長を設置しており、経営トップから、取締役と同等の権限と発言権を付与され、社内体制などの見直しにあたってきた。(製造業)

また今回ヒアリング調査を実施した中では、CSR[13]委員会ないしリスクマネジメント委員会と呼ばれる委員会組織を設置し、秘密情報管理もその所管事項の１つとしている企業も、上記情報セキュリティ委員会を設置している３社とは別途、３社見られた。

【秘密情報管理よりも大きな概念を所管する委員会組織を設置している例(ヒアリング調査結果)】

- 全社的には役員で構成される CSR・リスクマネジメント委員会が上位に存在し、CSR、コンプライアンス、内部統制などに関連する事項を所管している。以前は情報セキュリティ委員会を別途設けていたが、現在は前記委員会との重複感から、より実務的ないし推進に比重を置いた情報セキュリティ部会を開催している。(製造業)
- 副社長を委員長として四半期ごとに開催されるリスクマネジメント委員会が、秘密情報管理についても所管している。現在、プロジェクト組織として、秘密情報管理に係る小委員会を設置し、対策を検討している。(製造業)
- 情報セキュリティ、コンプライアンス、環境保全やその他 CSR 分野を統括する CSR 委員会を組成し、全社の最高レベルの委員会の１つとして位置付けている(トップマネジメント層と当社主要子会社社長で構成される)。(非製造業)

国内大企業 15 社の中で、経営者が参画する委員会組織で検討された方針に沿って実際の秘密情報管理体制や各種の施策を担うため、下位の会議体を設置している例と各部門に推進担当者を設置している例が見られた。前者については、社内横断的に CSR 推進部門、知的財産部門、情報システム部門の担当者を参加させているプラクティスと、人事部門、セキュリティ企画部門、情報システム部門、総務部門の担当者を参加させているプラクティスが見られた(情報システム部門が横断的な管理を実施)。また、知的財産部門が秘密情報管理について所管部となっているプラクティスや、全社的なリスクマネジメント部門や CSR 部門、マネジメントシステム全般を所管する部門を設置している企業で、当該部門が秘密情報管理について所管をしているというプラクティスも見られた。

【秘密情報管理を推進する体制の例(ヒアリング調査結果)】

- 情報セキュリティ部会は、CSR 推進部門、知的財産部門、情報システム部門の課長級担当者が参加する会議で、部門横断的なテーマである情報セキュリティに取り組むため、毎月会議を開催している(目的から言えば、今後は人事部部門や営業企画部門などもメンバーに入れ

[13] CSR とは、Corporate Social Responsibility の略称であり、企業の社会的な責任全般を指す。実務上は、企業の社会的責任として様々な利害関係者に対して実施する「活動」を指すことも多い。

ていく必要がある)。部会メンバーの情報セキュリティ推進に係るコミット率は明示的に定められておらず、現場の運用によっているのが現状となっている。(製造業)

- リスクマネジメント部長を統括責任者として、各部署のトップを責任者とする横断的な管理体制を構築している。リスクマネジメント部門、法務部門、人事部門、総務部門から、リスク・コンプライアンス委員会を組成し、各部署からの報告を収集し、対策に反映している。(製造業)
- 秘密情報管理は、人的管理、労務的管理、IT 的管理、施設管理という 4 つの管理を行っており、それぞれ、人事部門、セキュリティ企画部門、情報システム部門、総務部門が所管している。こうした複数の部門と連携については、情報システム部門がイニシアチブをとって横断管理している。(非製造業)
- 知的財産部門が営業秘密管理の中心的役割を担っている。技術情報の管理は知的財産部門の中核的業務のひとつと位置づけられており、全社における技術情報の共有と管理のバランスをとる機能を果たしている。(製造業)
- 当社ではリーガルセクションと内部統制セクションが秘密情報管理に関連する業務を所管している。リーガルセクションは、契約の他、紛争・訴訟などを中心に担当しているが、当社では様々な社外の取引先の情報を取得・共有することも少なくないことから、契約を含む法的なフレームも秘密情報管理上は重要な要素となる。内部統制セクションは、個人情報管理を含めたコンプライアンス全般を所管している。(非製造業)
- CSR 部が秘密情報管理の仕組みについても所管しているが、全社的なガバナンス体制のもとで、ガバナンスや管理意識を全社的に浸透させる役割を担っており、基準などを設定して、各部と連携・行動している。
- マネジメント推進部が社内の内部管理体制強化を担当しており、具体的には環境に関する事項、内部統制関係、ISO や社会からの要望などに対応するための管理体制の構築を行っている。マネジメント推進部が発足したのは比較的最近であり、それまでは情報管理といえば「個人情報管理」という意識が強かったが、近年の情報セキュリティに関する社会的関心の高まりを受けて、社内の情報資産の管理、顧客情報の管理なども管理するという社内意識が高まってきたため、マネジメント推進部という情報管理と担当する部署が設置された。(非製造業)

この点、以前は IT 部門に秘密情報管理を所管させていたものの、全社的に牽制機能を発揮できなかった反省から、現在はコンプライアンス部門に所管させているという企業もあった。IT 部門が直ちに秘密情報管理を所管する部門として不向きという訳ではないが、秘密情報管理を全社横断的な取組としていこうとすれば、それに適した役割と権限が担当部門・担当部署に与えられていることが必用となることは当該企業の反省からもうかがえる。

【秘密情報管理体制の失敗例(ヒアリング調査結果)】

- 全体的な情報セキュリティの管理は、以前は IT 部門が担当していたがうまく牽制機能が働かなかったこともあり、今はコンプライアンス部門が担当している。(製造業)

その他、秘密情報管理に特化した委員会組織を研究拠点毎に設置しているプラクティスが見られた。また会社全体のマネジメントシステムの推進を担当させる部署に秘密情報管理の役割を与えているプラクティスや、100 名程度の組織単位ごとに秘密情報管理の推進役を設置しているプラクティスも見られた。この推進役は、兼務者であり、実際に秘密情報管理の推進に投入している時間は稼働時間の 10 分の１程度であるものの、責任を持って推進を行う担当者がいることで運用上は大きなプラスとなっているとの評価も聞かれた。

【研究拠点や一定の組織単位毎に秘密情報管理の推進役を設置している例（ヒアリング調査結果）】

- 当社の特徴として、各研究所・研究室の単位で、トレードシークレット委員会と個人情報委員会という現場の会議を設置している点が指摘できる。全社的なガイドライン自体は 20 頁程度のボリュームのもので、具体的な運用は各部門に任せ、各部門が実情に合わせて、責任をもってローカルルールを整備し、情報委員会及び事務局となっている法務部門がこれを検証するという仕組みとなっている。そのため、研究拠点間の異動があった場合には運用が異なるため、新しい研究拠点における運用について別途説明をする時間を確保している。（製造業）
- 秘密情報管理に係る各部門の管理者はライン長が務めている他、秘密情報管理に係る推進役を置いている点が特徴的である。この推進役には当社特有の人材呼称をつけており、所管業務改善を恒常的に検討する人材と定義している。100 名程度の組織に１名～２名程度の課長級従業員を推進役として指名している。実際に推進役として情報セキュリティにコミットするのは業務量の１割程度であると思うが、具体的なミッションを持った推進役を置くことで、運用面に大きなプラスとなっている。（非製造業）

ヒアリング調査において、技術流出防止に力点を置いている企業においては、知的財産部門が重要な役割を果たしている場合が見られた。例えば、学会発表も含め従業員が技術情報を含む何らかの情報発信を行う場合の事前審査や、技術情報の管理を主たるミッションとした会社横断的なチームを設置しているというプラクティスが見られた。

【知的財産部門が秘密情報管理上重要な役割を果たしている例（ヒアリング調査結果）】

- 学会や講演会、工場見学なども含め、技術情報を何らかの形で公開する場合は必ず知的財産部門が開示審査を行い、公開の可否を決定する（工場見学であっても、一種の情報開示・技術協力であると規定上定義されている）。（製造業）
- 知的財産部門のみで対応していると、秘密情報管理に係る活動が恒常的になると硬直化するリスクもあるので、プロジェクト的対応も行っている。具体的には技術情報管理タスクフォースを部門横断で設置している。同タスクフォースは技術系の常務役員クラスをヘッドとして関係部門が一体となった諸策の総点検をミッションとしている。（製造業）

ヒアリング調査の中では、秘密情報管理を所管している部門が、情報漏えいないし技術流出リスクに係るアセスメント（評価）を実施しているというプラクティスが見られた。１社においては、技術情報の価値を多面的に評価し、自社にとっての重要度に応じた秘密情報管理を行っているというプラクティスを実践している。なお、情報漏えいないし技術流出リスクを含めたリスクに係るアセスメントとは、リスクマネジメントにおける基本動作であり、自社の抱えているリスクを特定した上で、リスクが顕在化した場合の影響度ないし経済的な損失額などを算定し、当該リスクを評価するプロセス[14]のことであり、これによってリスクの程度に応じた合理的なリスク対策が可能となる。

【リスクアセスメントを前提とした秘密情報管理を行っている例（ヒアリング調査結果）】

- 当社の CSR 部は秘密情報管理も所管しているが、全社的なリスクアセスメントを実施しており、情報漏えいないし技術流出に係るリスクについてもアセスメントの対象となっている。洗い出された項目のうち、事業継続に影響を与えると考えられる項目は重点的にチェックし、リスクマネジメントに活かしている。（製造業）
- 会社が保有している技術情報を最大限活用するため、情報が特定の時点で持つ価値に応じて戦略的に管理の方法を変えている。具体的には、個別の技術情報について、技術的価値、経済的価値、法的価値という 3 軸で評価し、技術的価値と経済的価値に応じて管理の度合いを変えるということを行っている。例えば、技術として競合市場で抜きん出ており、自社事業にもたらす付加価値が極めて大きいコアの先端技術であれば、営業秘密として取扱い、ブラックボックス化するが、徐々に競合他社のキャッチアップが進んでいき、技術水準が横並びに近づくと、特許化してライセンス契約による協業を進めるといったパターンがある。特に昨今では、すべての技術情報を囲い込むのではなく、他業種も含めた他社との技術協力を通じたオープンイノベーションで市場を広げていくことも重要であるという認識に立ち、全社のオープン&クローズ戦略を作る役割を知的財産部門が担っている。（製造業）

今回のヒアリングの中で１社からしか明示的な回答がなかったが、秘密情報管理に関わる各部門の責任者や、推進役となる担当者については、定期的に交代させることで当該部門全体の意識向上させる効果を期待しているというプラクティスもあった。

【秘密情報管理に関わる部門責任者などの交代を意識的に行っている例（ヒアリング調査結果）】

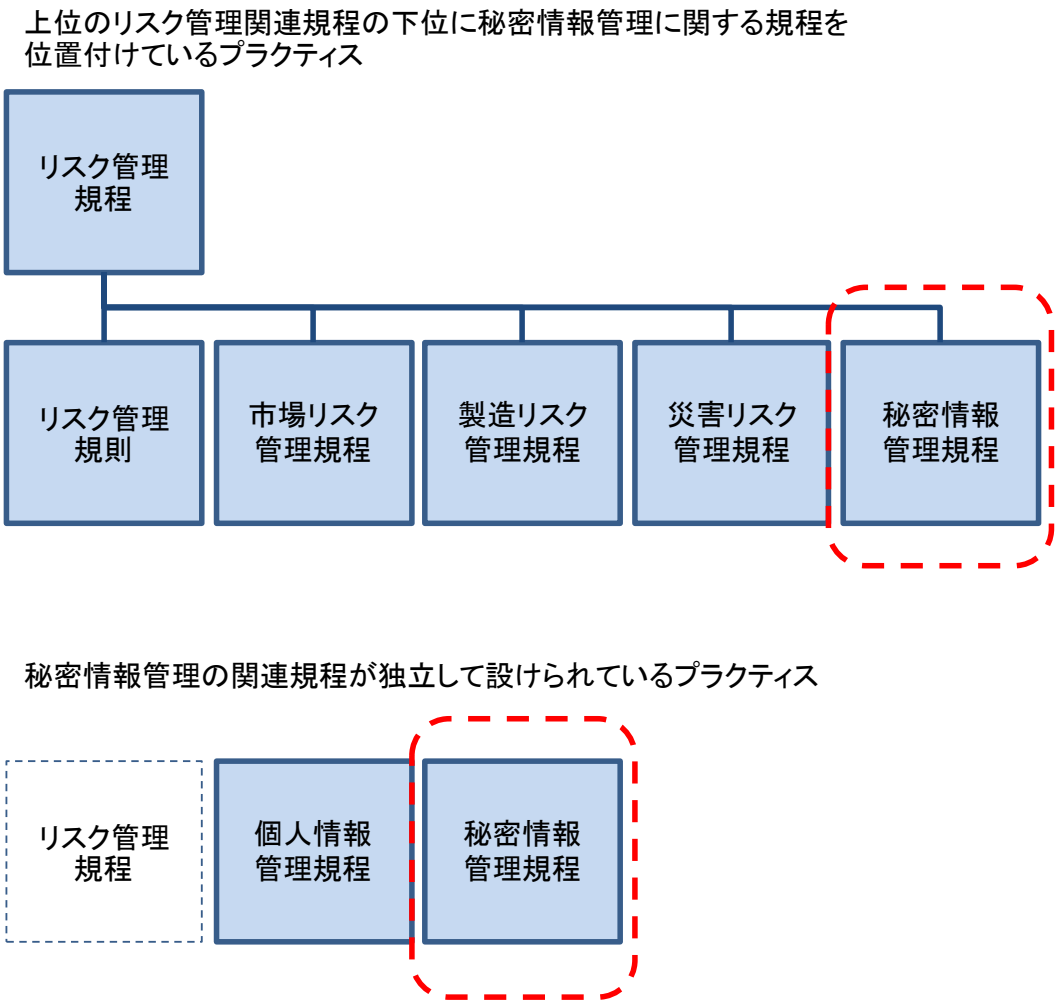
- 意識徹底のために情報セキュリティ管理者を定期的に交代させる事で部門への定着化を図っている。（非製造業）

14 リスクアセスメントとは、リスクマネジメントに係る ISO 規格である ISO31000 によれば、「リスク特定、リスク分析、及びリスク評価のプロセス全体」を指す。リスクマネジメント規格活用検討会『ISO31000：2009　リスクマネジメント 解説と適用ガイド』（日本規格協会、2010 年）36 頁参照。

（２）関連規程の整備実態

平成 24 年度に経済産業省が実施したアンケート調査によれば、営業秘密の漏えいを未然に防ぐための管理方針を策定している企業は 63.8%（301 人以上の製造業が 82.9%、301 人以上の非製造業が 74.8%）[15]となっており、秘密情報管理に係る関連規程の整備は多くの企業において進められている所である。今回実施したヒアリング調査によれば、リスク管理関連規程の下位に秘密情報管理に関する規程を位置付けているプラクティスと、秘密情報管理の関連規程が独立して設けられているプラクティスとが見られた。

図 1：秘密情報管理の関連規程の位置づけ例



（出所）肥塚直人『「技術流出」リスクへの実務対応』（中央経済社）102－103 頁を参考に作成

【秘密情報管理の関連規程の位置づけ（ヒアリング調査結果）】

・　規程類については、最上位にリスク管理規程があり、その下に情報セキュリティ関連の規程

[15] 経済産業省・前掲注 1、8－9 頁。

がある。情報セキュリティ規程については、米国・欧州と同じ項目レベルで概要を示したガイドライン（２～３頁の資料）を定めている（その他の国は独立性が高く各国ごとに定めたものを使用している)。(製造業)

- 規程上は、内部統制とリスクマネジメントは一体的な規程体系になっているが、情報セキュリティについては別途、情報セキュリティに係る基本規程とその細則となる対策基準の２つの規程を設けている。また個別に情報システム部門、人事部門、知的財産部門などが細則を設けている場合がある。(製造業)
- 情報漏えいは、リスクマネジメントの対象としては整理されておらず、情報取扱規程もリスクマネジメント規程とはリンクしていない。(製造業)
- もともと情報管理方針は策定されていたが、全社体系としての整備は直近で整備を行った。情報管理と個人情報管理は参照している規程が異なっているため、体系としてはそれぞれ別個の規程としている。その他の情報管理に関する規程としては、情報漏えいや不正、環境問題（工場からの汚染水流出など）が発生した際の対応をまとめた危機管理マニュアルがある。危機管理マニュアルは以前から整備されており、危機管理の定義としては経営に直接かかわるかどうかで決めている。(非製造業)

企業によって、どの程度の内容を規程でルール化しているかは異なるが、具体的な細則についても規程の階層を多重階層にしつつ、下位の階層に属する規程においては詳細な取扱いルールを定めているプラクティスが見られた。また近年注目されているソーシャル・ネットワーキング・サービス（social networking service。以下、SNS）やクラウドといったネットワークや、スマートフォンなどの端末を通じた情報漏えいに対応して、関連規程に規定の追加を行っているプラクティスも見られた。

【関連規程の細則例（ヒアリング調査結果)】

- 営業秘密管理指針も参考にしながら、社内の秘密管理規程を整備してきたが、現在の規程体系は 4 層構造となっている。最上位の規程は、会社情報に関する管理規程であり、定義規程や情報管理区分などの概略を定めている。(製造業)
- 周知するルールの策定にあたっては、細かく書くと 100 ページを超えてしまうため、どのようにメリハリをつけていくかは今後の検討課題と考えている（現状、実際のルールは 100 ページを超えるものになっている)。例えば、外勤と内勤とで留意すべきポイントは異なるはずであり、タイプに応じてアピールすべきルールが異なるものと思われる。また、R&D 情報や新商品情報は対外厳秘の営業秘密であるが、ルールの中で明確にメリハリをつけた重みづけができていない。グループ会社共通で「営業秘密管理方針」と、９章で構成される「機密管理規程」を制定した。営業秘密管理方針は、ルール策定と継続的な改善、適切な管理・運用、厳格な措置といったポリシーを記述しており、詳細は営業秘密管理規程に定めている。規程レベルで定めている事項は、営業秘密管理区分、部門の役割、従業員の義務、情報取り扱い、社外への情報持出手続き、コンプライアンス、人材派遣・業務請負時の機密取り扱いなどと

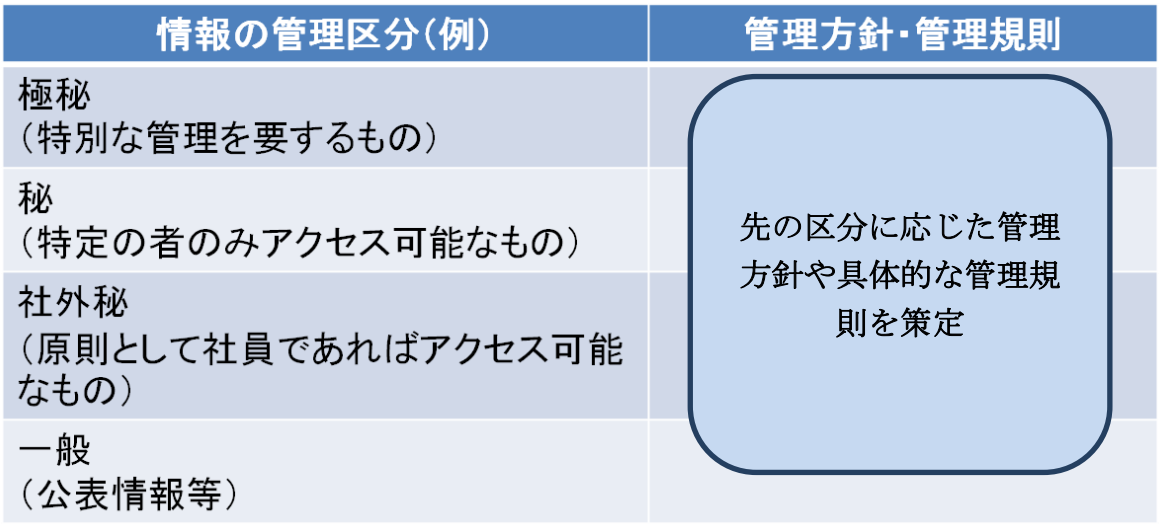
なっている。（非製造業）
- 細則である対策基準には、人的管理、物的管理、情報システムなど、幅広く必要な規則が定められている。（製造業）
- ホールディングスとしての情報セキュリティ体系としては、最上位に「グループセキュリティ規則」があり、その下に「システム細則」「ルール」がある。さらに、「ルール」に紐づく形で、「情報セキュリティ向上のために」というタイトルで、ルールの周知徹底を図るための自己学習用テキストが用意されている。（製造業）
- 情報セキュリティの規程で最近追加したものには、ソーシャルメディア、クラウド、スマートフォンなどのガイドラインがある。（製造業）

（３）情報区分の考え方

ヒアリング調査では、関連規程の中で情報区分を定め、区分に応じた秘密情報管理を行うというプラクティスが複数の企業において見られた。

ヒアリング調査では３区分ないし４区分程度に情報を区分しているプラクティスが見られた。例えば４区分の典型的な例としては、図２のように、特別な管理を要するもの（例えば取締役会・経営会議資料のような高度な経営に関する資料など）、特定の者のみアクセスを可能としている情報、社員であればアクセス可能な情報（例えば社員用のポータルサイトに掲載している社内規程や社内書式、社内報など）、公表情報などの一般情報といった区分を採用している企業があった。

図 2：情報区分の例



（出所）ヒアリング調査を基に作成

【情報区分の考え方（ヒアリング調査結果)】

- 20 年程前、秘密情報の管理に関するガイドラインを策定し、厳秘、秘、社外秘といった３区分を設け、それぞれ区分に応じた管理を定めている。ガイドラインは法務部門の所管であり、法改正や営業秘密管理指針の改訂などに対応して度々改訂されている。個人情報については別途のガイドラインを設けている。(製造業)
- 情報は４つの区分に分類し、部外秘以上の情報について特に厳格な管理を行っている。部外秘以上の情報の管理については秘密管理性を意識しているが、有用性などの要件も含めて営業秘密に該当するかどうかについてはリンクさせていない。(製造業)
- 書類については、「秘密」「重要」「取扱注意」「一般」の４つに区分し、「秘密」「重要」については機密扱い、「取扱注意」については社内のみ、「一般」については公開可としている。（製造業）
- 書類については、「極秘」「秘」「それ以外」の３つに区分して管理されている。「極秘」「秘」の開示可能範囲などの細かな定義は部署によって異なる。「極秘」「秘」の書類については施錠管理を徹底しており、机上放置はルール違反となる。(製造業)
- 現状では、「厳秘」と「機密」に分けた管理を行っている。「厳秘」についてはアクセス制限がかけられ、規程上、コピーや持ち出しにも機関長や組織長の許可が必要なことになっているが、守られてはいないのが実態である。「機密」は組織内で共有可能だが、管理は行っている情報のことである。今後、「機密」の下位に「社外秘」という区分を新しく設け、管理はしないが積極的に社外に出すことはしない情報として扱っていく予定である。(製造業)
- 情報資産台帳を作成のうえ、社内の機密情報は４段階に区分されて管理されている。各区分にどのような情報が属するかは、地域別に定義される。(製造業)

またヒアリングを行った企業の中には、運用によっては管理対象となる情報が膨大となってしまう秘密情報の区分に工夫を行っている企業もあった。例えば、秘密情報が当該資料単体で価値を持つものと、当該資料単体では価値を持たないものとで区分を行い、前者については管理のレベルを高め､法的なエンフォースメント[16]まで意識していると思われる運用を行っているプラクティスも見られた。

【法的なエンフォースメントを意識した情報区分を設定している例（ヒアリング調査結果)】

- 当社の営業秘密ガイドブックには、情報の管理区分なども定められている。具体的には、極秘、秘、一般機密（社外秘）という区分を設けているが、「秘」の情報は、各種計画や図面など、当該資料単体で秘密情報として価値を持ちうるもの（区分 A）と、秘密情報であることは間違いないが、当該資料単体では価値を持ち得ないもの（区分 B）に分解され、区分 A に該当する場合には台帳管理（毎年棚卸しを実施）を行い、所在や当該秘密情報の管理者など

[16] エンフォースメントとは、法令などに代表されるルールを執行することである。典型的には、訴訟手続を利用したり、訴訟外紛争解決手段（例えば調停制度や仲裁制度など）を活用して、自らの権利を実現していく活動がこれに当たる。

を把握・管理している。現場で区分Aの情報と区分Bの情報を直ぐに判別できるよう、区分Aの情報はファイル名やファイルのヘッダーに当該区分情報であることを表記することを義務付けているが、特段の表示が無い場合には区分Bに分類されるということになっている。恐らく定義上は区分Aの情報も区分Bの情報も営業秘密の要件を満たすと思われるが、実際にエンフォースできるかと言えば、区分Aの情報のような管理と証跡が無ければ難しいのではないかと感じている。(製造業)

受注型の生産を行っている企業では、顧客情報を特に厳格に管理しており、受託している案件の性質に応じても情報区分を設けているというプラクティスが見られた。

【受託案件の性質によって情報区分を設定している例（ヒアリング調査結果)】

- 全社的には顧客情報の情報管理を最も厳格に捉えており、受託しているプロジェクトの顧客や性質に応じてプロジェクト自体に３つのセキュリティ区分を設けている。自社の開発情報が漏えいした場合のダメージよりも、顧客情報漏えいによるレピュテーションや営業上のデメリットの方が深刻であることから、顧客情報の管理が優先されている状況である。(製造業)
- 現業部門では事業部単位のガイドラインを持っている。協力会社には契約上厳格な秘密保持義務を負わせているが、秘密情報の共有は最小限度となるようにしている（基本的に現場に秘密情報があるという状態にはならないような管理の仕方)。(製造業)

さらに、機密性が高い顧客データを扱う場合には、当該データにアクセス可能な従業員の名簿を作成しているプラクティスも見られた。当該企業においては、必要に応じて社員の調査なども実施し、当該秘密情報を欲しがるような事情や勤務状況などに不安・不審な点がないかといった点を確認していることが特徴的であった。

【機密性が高い顧客データにアクセス可能な従業員名簿を作成している例（ヒアリング調査結果)】

- 機密性が高い顧客データを扱う際は社員の名簿の作成をしており、必要に応じて社員の調査も行う。調査に際しては、当該秘密情報を欲しがる事情が無いか、過去の勤務状況などに不安・不審な点が無いかなどを調査している。(非製造業)

また、情報区分と区分に応じた運用を行う上で情報の特性に応じた管理が必要となることから、同じポリシー（なお、ここでポリシーとは、個々の規程間で相対的に上位にある方針・基本規程レベルの規程を意味する）で管理することの難しさや、従前は異なるポリシーを持っていた企業が経営統合された場合の難しさを指摘する声も聞かれた。

【情報区分を設定する際のむずかしさ（ヒアリング調査結果)】

- 情報管理といっても、個人情報、技術情報、その他の経営情報ではそれぞれに特性が異なり、一括して同じ方針で管理はできない。技術情報の場合、社内外の様々な組織や個人と共有し、活用していく必要があるため、取扱いに対してあまりに厳重な制約を課すことは適切ではない。情報の活用と保護とのバランスをとることが課題である。(製造業)
- 経営統合もあり、全社横断的な情報区分ルールは整備出来ていない。部門によって扱われる秘密情報は極めて多様であり、基本的には各部門の判断で業務上扱われる情報はほぼ全てが秘密情報に該当するという整理となっている。ファイルへのパスワード設定やアクセス制御はある程度行えているが、紙媒体資料の施錠管理や秘密情報であることの表示などは必ずしも徹底できていない。(非製造業)

３．物理的な管理

（１）情報システムの管理

情報漏えいや技術流出対策の観点から積極的行われている対策として、まず外部に対する誤送信などを予防する観点から、メールを暗号化する、誤送信防止ソフトウェアを活用するといったプラクティスが見られた。また、Web サイト上に情報を記載することは故意、過失を問わず、情報漏えいの懸念があることから、書き込みについて警告を出すソフトウェアや、危険な Web サイトのスクリーニングなどを実施しているプラクティスも見られた。

【外部に対する誤送信防止などの取組（ヒアリング調査結果)】

- 情報システム関係のセキュリティは、メールの暗号化、PDF ポリシーなどを導入するも、ハードディスクドライブ内のチェックや持ち出し管理などの対応はこれからである。部門によっては、上記暗号化メールに加えて、誤送信防止のために CC に上司を入れないと送信できないソフトウェアを導入している（部門ごとに運用は任せている)。(非製造業)
- メールの誤送信対策として、社外へのメールに対するアラートを出し、また、メールアドレスのオートコンプリート機能を無効化するアプリケーションを導入している。ウェブへの書き込みについてもアラートを飛ばすサービスを導入している。危険ページの閲覧については、別システムでスクリーニングをかけている。(製造業)

情報へのアクセス制御は、秘密情報に対してアクセスの必要が無い者によるアクセスを遮断する手段としても、当該情報がアクセス制御されている情報であること、つまり秘密情報として管理されていること（秘密管理意思）を従業員などに認識させる手段としても重要である（「営業秘密管理指針（平成 27 年 1 月 28 日全部改訂版)」 5 頁注記 5 参照)。様々な工夫をしながら、情報区分に応じた秘密情報管理ルールに従って、アクセス権を設定し、アクセス制御を実施しているプラクティスが見られた。

【情報へのアクセス制御の取組（ヒアリング調査結果)】

- 情報閲覧範囲の設定、紙媒体の場合は施錠管理などが基本である。なお、アクセス制御の対象となる秘密情報が掲載されている紙媒体は施錠管理を徹底している。電子データはアクセス制限が基本だが、パソコン上にはデータ保存をさせず、パソコン（全てノートタイプ）は帰宅時、キャビネに施錠して帰ることになっている。(非製造業)
- ネットワークアクセスについて、セキュリティ管理にツールを活用した効率化を進めている。投資としては大規模なものとなるが、発注先の見直しや競合提案させることでコストを一定額に抑えることができたことからツール導入を決定した。(製造業)
- 秘密情報を含む電子情報（ファイル）は、特定のアクセス制御されたフォルダに保存することになっている。特殊な文書管理システムが入っているかどうかまでは分からないが、当社

用にカスタムされたファイル保存の仕組みとなっており、フォルダ毎に開示範囲を変更できるようになっている。(製造業)
- ファイルサーバについては、アクセス権を厳格に設定して管理している。ファイルサーバに格納されているファイルについては、アクセス権があれば出力することはできる。(製造業)
- システム上でも、秘密レベルの高い情報はアクセスログを監視したり、プリンタから出力できなくしたりするなどの措置を講じている。(製造業)
- 個人情報としては、もちろん取引先などの情報もあるが、様々な懸賞などで集める個人情報が膨大にある。以前行われた経営統合前は、各社で許諾の範囲が様々であったが、経営統合後は統一的な管理運用が行われている。 全て ID 管理され、メルマガの配信の他、懸賞の送付漏れが無いかといった確認もできるよう、物流システムともリンクさせている。(非製造業)
- 研究拠点間を超えたアクセスを認めている他、詳細な企画やデータなども開示して行われる研究報告会などには、どこの研究拠点に所属していても参加できるようにしている他、販売・営業サイドの人間も参加が可能となっている。(製造業)

秘密情報管理に限ったことではないが、秘密情報管理と関連付けて必要な情報のバックアップや管理を行っているプラクティスが見られた。すなわち、下記のヒアリング調査結果にもあるように、保管すべきデータと削除すべきデータを峻別するだけでも、保有している情報が秘密情報として継続的に管理、保有していくことが必要なものであるのか、比較的短期間で削除することが可能な相対的に秘密性及び重要性の低い情報であるのかといった、判断を定期的に行うことに繋がる。そのためこうした文書管理と秘密情報管理は、管理という観点から、親和性のある取組であることから、一体的に検討を行うことも効率の観点から検討に値するものと思われる。

【秘密情報管理の一環として情報のバックアップをしている例（ヒアリング調査結果)】

- 技術情報に関しては常時バックアップをとっているが、量が膨大で、維持管理にも費用がかかるため、毎月不要なものについてはファイルサーバ上から削除せざるを得ない。そのため、実質的に各部署別個で保管するという管理体制をとっている。各部署で所持しているハードディスクドライブなどは施錠管理している。残念ながら、ファイルの種類に応じた保管期限などの管理は体系的に行えておらず、個別判断となっている。(製造業)

アクセス制御をより高度化し、単に情報にアクセスすることの可否をコントロールするだけでなく、印刷の可否などまで含めて管理が可能な文書管理システムや、決裁管理機能が付加された文書管理システムを導入して対応しているというプラクティスも見られた。

【文書管理システムを活用している例（ヒアリング調査結果)】

- 導入している文書管理システムには特定の秘密情報を管理する際、アクセスの範囲なども入

力し、システム上アクセス制御が行えるようになっている。またこれに付随して、契約書などを含む秘密情報の印刷に関する権限なども設定されるようになっており、誰もが自由に印刷できる状態ではない。なお、複合事務機については、コピーを取る際に ID 管理と印刷履歴が管理できる機械を導入しているが、導入状況は統合前の各社によってバラツキがあったため、統一的な導入・運用は検討途上である。（非製造業）

- 上述の区分別に情報管理を行うための文書管理システムが既に導入されているが、決裁・稟議目的のみに使っているのが現状であり、本来の目的に沿った運用はこれから開始しようとしているところである。（製造業）
- 情報管理システムとしては、大手情報ベンダーのソリューションを全社レベルで導入しており、コピーや印刷などの様々な制限をかけられる機能が装備されているが、あまり利用されていないのが現状である。社員が海外で重要な情報を紛失したことがきっかけで導入したものである。（製造業）

社外からのサイバー攻撃によって情報漏えいや技術流出が発生することも重大な懸念事項である。そこで社外からのサイバー攻撃に対する取組をグループ企業全体で取り組んでいるプラクティスや、これまでの取組が不十分であったとして近時、全社的なマネジメント部門が管理を行うこととなったというプラクティスが見られた。

【サイバー攻撃に対する取組（ヒアリング調査結果）】

- サイバー攻撃の対応策について、グループ全体で標準化を進めている。具体的には、多数の関連会社の間で、メーラーの統一や OS ソフトへの防護策の統一を行っている。（製造業）
- 外部からからの不正アクセスや攻撃に対する施策は情報システム部で以前から導入・管理されていたが、内部からの攻撃、不正に対しては管理が十分ではなかった。そこでマネジメント推進部が新しく管理することとなった。（非製造業）

また、業務の性質上、SNS の利用を禁止できない企業においては、SNS の活用状況の管理に課題を抱えているというプラクティスもあった。

【SNS 活用に係る管理についての取組例（ヒアリング調査結果）】

- SNS は業務の性質上活用せざるを得ず、禁止は出来ない。私用端末の場合、物理的にチェックが及ばず、管理は出来ているとは言えない。部門毎の会議で社内セミナーをまめに開催するなど、リテラシー向上には取り組んでいるが、ガイドラインなどは未整備の状況である。サーバへのアクセスや外部とのメールのやり取りもある程度モニタリングされており、異常があればアラートが送られてくる。（非製造業）

（2）情報機器の管理

情報機器の管理については、会社所有のものでシステム的に管理された機器のみ利用を認め、私有の機器については利用を禁止している企業が、今回のヒアリング調査においてもこうした運用が散見された。USB などの記録メディアは、容易に大量のデータを保存することが可能な上、小型で持ち出しが容易であることから、情報の受け渡しには便利であるものの、紛失リスクがある他、悪意のある情報の持ち出しに用いられる懸念もあることから、各社では厳格な取扱いが見られた。

【私有機器の利用禁止に係る取組（ヒアリング調査結果)】

- パソコンや USB（アクセスのためのパスワード付き）などのデバイスは全て会社所有のもののみ利用（ルール上は私有パソコンや私有デバイスの利用は一切禁止)。社外の端末などを接続すれば検知できる仕組みを導入している。ただ、これも事件以降に対応したこと。副次的なメリットとして、資産管理が徹底され、IT 投資の圧縮にも繋がるものとなっている（余分な端末が判明するなど)。(製造業)
- パソコンや USB などのデバイスは全て会社所有のもののみ利用可能となっており、ルール上は私有パソコンや私有デバイスの利用は一切禁止されている。 物理的に接続することまでは遮断していないが、 接続すれば会社所有物以外のパソコンやデバイスであることが直ぐに検知できる仕組みとなっている。(製造業)
- USB などの記録メディアは会社貸与のもののみ利用が認められており、台帳管理されている。(非製造業)
- USB などの原則利用禁止などを徹底している。(製造業)

私有の情報機器の使用を厳格に禁止し、社内ネットワークへのアクセスを遮断しているプラクティスが見られたが、ヒアリング調査に回答頂いた企業においても私有の情報機器の利用を一切禁止することは容易ではなく検討途上にあるというプラクティスがあった。

【私有機器の利用禁止徹底の難しさについての指摘（ヒアリング調査結果)】

- 私有の情報端末の使用はルール上禁止されている。私用パソコンなどでは会社のネットワークには入ることはできないものの、社有パソコンに私有スマートフォンを接続して充電など行われているのが実態であり、監視もされておらず、現状を問題視している。(製造業)
- 私有のスマートフォンやタブレットパソコンも同様に使用を認めていない。(製造業)
- 私有の USB の使用はモニタリングされているが、実際に注意を払ってチェックされているのは退職予定者などの要注意対象のみとなっている。(製造業)

社有の情報機器についても、厳格な運用を行っている企業が多いが、例えば、データの複

製、持ち出しを予防する観点から、社用の情報機器に書き込みできるパソコンを物理上的に限定し、各自のデスクなどではデータ書き込みをできないように物理的に制限を行うといったプラクティスが見られた。また、社用の情報機器への書き込み自体に事前申請を必要としているプラクティスも見られた。

【データの複製、持ち出しを予防する取組（ヒアリング調査結果)】

- 情報システム関係についてはある程度全社的に対応している部分があり、書き込みできるパソコンを限定している。(製造業)
- 社内のパソコンは外部媒体に書き込みができない設定にしており、書き込みができるパソコンは特定された場所にのみ設置している。書き込みをする際は事前申請が必要。(非製造業)

社有、私有を問わずノート型パソコンは社外への持ち出しが容易であることから、持ち出しについても制限を行うプラクティスや、申請を必要としているプラクティスが見られた。もっとも、業務の性質上、一律にノート型パソコンの持ち出しを禁止すれば、業務効率を大きく損なうという側面があることは否めないため、情報の暗号化及びローカルドライブへの情報保存の禁止をルール上徹底していることを前提として、持ち出し自体の全面的な禁止を緩和しているプラクティスも見られた。

【ノート型パソコンの管理に係る取組（ヒアリング調査結果)】

- 申請をすればノートパソコンは会社所有のものを貸与し、持ち出すことが可能であるが、長期間特定の個人の下に置くことはできず､用が済んだら返却することとなっている｡(製造業)
- 会社パソコンの持ち出しには申請が必要である。(非製造業)
- ルールを変えた例として､「パソコン持ち出しルール」が挙げられる。以前は、飲酒の可能性がある外出に際してのパソコン持ち出し自体を禁止していたが、営業サイドから実務上の不都合を指摘する声が相次ぎ、パソコンのローカルドライブに情報を保存しないというルールが徹底されていることを前提として、これを緩和した例がある（システム面でのセキュリティ機能の高まり（ハードディスクドライブ暗号化など）も、ルール緩和という対応の背景として指摘出来る)。(非製造業)

また、ヒアリング調査の中でも、近年、ノートパソコンなどの活用場面が増えたことなどから、シンクライアント[17]と呼ばれる方式が注目されるようになり、既に導入している企業や

[17] シンクライアント（Thin Client）とは、利用者の情報機器で行う処理や保存する情報を最小限にして、処理の大半をサーバ側で行う方式のことである。これによって、従業員が利用するパソコンなどの情報機器に保存する、秘密情報を含む情報が最小化されることから、情報機器の盗難・紛失、従業員などの不正による情報漏えいないし技術流出リスクを軽減することが期待されている。

導入を検討している企業が見られた。

【シンクライアント方式に対する注目（ヒアリング調査結果)】

- シンクライアント対応させるサーバ集約やバックアップ機能の拡充などを今後も進めていく。(製造業)
- 社外に持ち出すパソコンはシンクライアント端末の利用を義務付けている。(製造業)
- 社用パソコンについては最近シンクライアント対応としたため、ローカルにデータを落とせないようになっている。シンクライアント化する前は、個々人に情報検索ソフトを実行してもらうことで、ローカルのデータの有無の自己チェックをしてもらっていた。(製造業)
- なお、現時点でシンクライアントの導入はしていないが、導入可否も含め引き続き社内で検討をしていく。(シンクライアント導入の障壁は、グループ全体を当社の IT 本部が統括している事による膨大な予算と対応リソースの確保である。)(非製造業)

小型で携帯が容易な USB などの記録メディアについては、故意でなくても紛失や盗難による情報漏えいの懸念もあることから、意識的に管理を行っているプラクティスが比較的多数見られた。記録メディアについては、そもそも原則禁止としているプラクティスや、個別に許可を得た従業員や部署のみが利用できるような運用を行っているプラクティスも見られた。また、記録メディアを登録制とした上で現物確認(登録済み記録メディアの存在を目視する)をする、記録メディアにバーコードタグを付けて個体管理を行う、記録メディアへの書き込みを物理的に制限するといったプラクティスも見られた。

【USB などの記録メディア管理に係る取組（ヒアリング調査結果)】

- USB などの原則利用禁止などを定めている。(製造業)
- USB などの可搬媒体の使用も、事前に登録され、許可されたものを除いて禁止されている。登録されたもの以外が会社のパソコンに接続されるとアラートが出るようになっている。(製造業)
- USB などの記録メディアは全て登録制となっている。(製造業)
- USB の使用は、限られた従業員のみが行える。今後も、書き込み権限を持つ従業員数を減らそうとしている。以前幹部社員による情報漏えい事件が発生しており、ルールが厳格化された。(製造業)
- 顧客からデータを USB でもらうことが多いため、USB の利用を制限することが非常に難しい。USB を使用する部署を特定し、符番された USB のみが使用できるように設定している。(非製造業)
- パソコンや USB などの情報機器類は年に 2 回、現物確認を行い、紛失が無いか確認する他、確認を通じて管理意識を高めている。
- USB については、必要に応じて会社で管理しているものを貸し出すルールになっているため、ルール上は私有の USB を使用してはいけないことになっている。但し、私有 USB の使

用を検知できる仕組みは導入しておらず、対策すべき課題であると考えている。（製造業）
- USB については個人には使用を禁止しており、モバイルも厳重に管理している。（製造業）
- USB は読み込みのみで書き込みができないようにしている。（非製造業）
- 顧客からのデータは電送が増えているものの、USB で渡されることが依然として多い。その際は営業や工場が一度は受け取ることになる。そこからの出荷や入荷の際に紛失が起きないようにバーコードタグをつけて紛失が起きないように管理している。（非製造業）

また、大容量ファイルを送受信するために提供されているストレージサービスの中には情報セキュリティの脆弱性に起因する情報漏えいに対する懸念から、指定されたサービス以外の利用を禁止しているというプラクティスが見られた。もっとも、物理的に指定以外のサービスへのアクセスを遮断しているわけではなく、運用が徹底されることが前提となっているとのことであった。

【ストレージサービス利用管理に係る取組（ヒアリング調査結果)】

- 大容量ファイルのやりとりには、外部ストレージサービスの使用が推奨されている。使用するサービスは指定されているが、それ以外のサービスを使うことも物理的に制限はされていない。（製造業）
- 大容量ファイルなどを送信する際は、専用のストレージサービスを利用させており、一般のサービスを利用することは禁止している（専用サービス以外への接続遮断まではしていない)。（製造業）
- インターネット上への書き込みはそもそもできないように制限している。（製造業）

情報機器の紛失や盗難についても、必ず報告をさせ、担当部門が情報を集約し、全社的にフィードバックを行うといったプラクティスが見られた。

【紛失や盗難時の対応例（ヒアリング調査結果)】

- 社内で事務ミスなどによる漏えいや機器紛失（未遂含む）があれば、委員会事務局の法務部門で情報を集約して、トレードシークレット委員会などを通じて全社にフィードバックを行っている。こうした仕組みで現状、大きな問題は発生していないが、管理レベルが揃っていないことについては課題意識も持っている。（製造業）

（3）紙媒体の管理

秘密情報が紙媒体で存在している場合には、紙媒体自体の管理が必要となるとして、関連

規程上、電子媒体と紙媒体を別体系で管理しているプラクティスも見られた。例えば、外勤職員が秘密情報の区分として相手に開示することが出来ない書類を誤って開示してしまったり、異なる相手に他者の秘密情報を開示してしまうといった人的な過失による情報漏えいを懸念し、書類の性質によって明示的な色分けを行うといった工夫をしているプラクティスも見られた。また、社内においても、開示範囲を明確化し、機密性の高い情報が掲載されている紙媒体を当該情報に接する必要の無い者が不用意にアクセスしないような工夫をしているプラクティスも見られた。

【紙媒体の管理に係る取組（ヒアリング調査結果）】

- 情報セキュリティ規程において、電子媒体と紙媒体ではそれぞれ個別の体系で管理している。（製造業）
- 特に外勤の社員が扱う書類については、明示的に色で分類したマークを付けて、持ち出しの可否、相手に渡すことの可否がわかるようにしている。上述の分類はイントラネットにガイドラインを掲載しており、各分類の文書例などを公開している。現場レベルでの書類の分類は、現場のマネージャーの判断に委ねられており、実際は厳密に運用することが難しいケースもあるため、まずは分類をすることを習慣づけることから始め、徐々に制度をあげていくことが有用であると考えている。（製造業）
- 2007 年以降、全ての社内資料に開示範囲を記載する運用を徹底した事で、意識が低い社員にも認識してもらう事ができた。（ルールを作るだけでは徹底は難しく、社員に負担にならないような運用上の工夫をする事が肝要）なお、2007 年より前の書類・データについては、それぞれ想定される最高区分の管理区分を設定し、フォルダへの格納、施錠管理などを行っている（当該フォルダから取り出す場合には改めて区分や開示範囲を表示することを求めている）。（非製造業）

管理対象となっている紙媒体については秘密情報であることの表示や台帳管理を行い、所在の確認などを把握するといったプラクティスも見られた。また、不正競争防止法が定める営業秘密として法的な保護を受けることを前提とした管理を行っているプラクティスも見られた。なお、今後は 2015 年 1 月に改訂された営業秘密管理指針（平成 27 年 1 月 28 日全部改訂版）[18]も参考にしつつ、営業秘密の保護要件などを検討することが肝要である。

【管理対象となる紙媒体についての扱い（ヒアリング調査結果）】

- 情報についてはエクセルで作成した台帳を用いて管理しており、台帳に記入する際に管理レ

18 改訂された営業秘密管理指針は、営業秘密が不正競争防止法によって法的保護を受けるために必要となる水準を示すものである。従前の営業秘密管理指針には、情報管理に関するベストプラクティス及び普及啓発的事項を含んでいたが、全部改訂によって不正競争防止法の解釈に係る部分のみが整理されることになった。よって、法的保護を睨んだ管理を行う場合には、全部改訂された営業秘密管理指針を参考に、不正競争防止法の保護要件を満たす管理を行うことが必要となる。（http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf）

ベルを設定している。（非製造業）

- 秘密情報であることの表示や台帳管理（個別の文書単位ではなく、文書のジャンル単位で管理）、コピーを当初の関係者以外に配布する場合（配布を受けた者も関係者となる）の管理などを徹底している。コピーも研究発表会などの場面で使用される資料は全て通し番号を振り、回収もしている。（製造業）
- 不正競争防止法の保護を受けるために営業秘密として管理することは、管理レベルとしては高いレベルが必要であると認識しており、関係者限りの情報全てをこの水準で管理することは難しいとの判断から、特に法的保護を必要とする情報のみ「要法対応情報」として、個別管理を行っている。対象となる情報について管理表を記入し、台帳管理されている。もっとも、実際の運用としては、この要法対応情報とされている情報は、本当に経営レベルの極秘情報や国プロなどの中でも特に機密性の高い案件で扱う情報のみであり、限定的な使われ方となっている。要法対応情報は、資料のコピーも制限され、コピー履歴も全て残すなど、厳重な管理を行う。現物の管理自体は現場部門が行うが、管理台帳は知的財産部門が管理している。（製造業）

秘密情報が記載された紙媒体については、複製をどのように制御・制限するか、破棄をどのように徹底させるかといった問題が生じる。ヒアリング調査の中では、印刷ルールを定めたり、機密情報の破棄を明示的に一般情報の破棄と区別しているプラクティスが見られた。

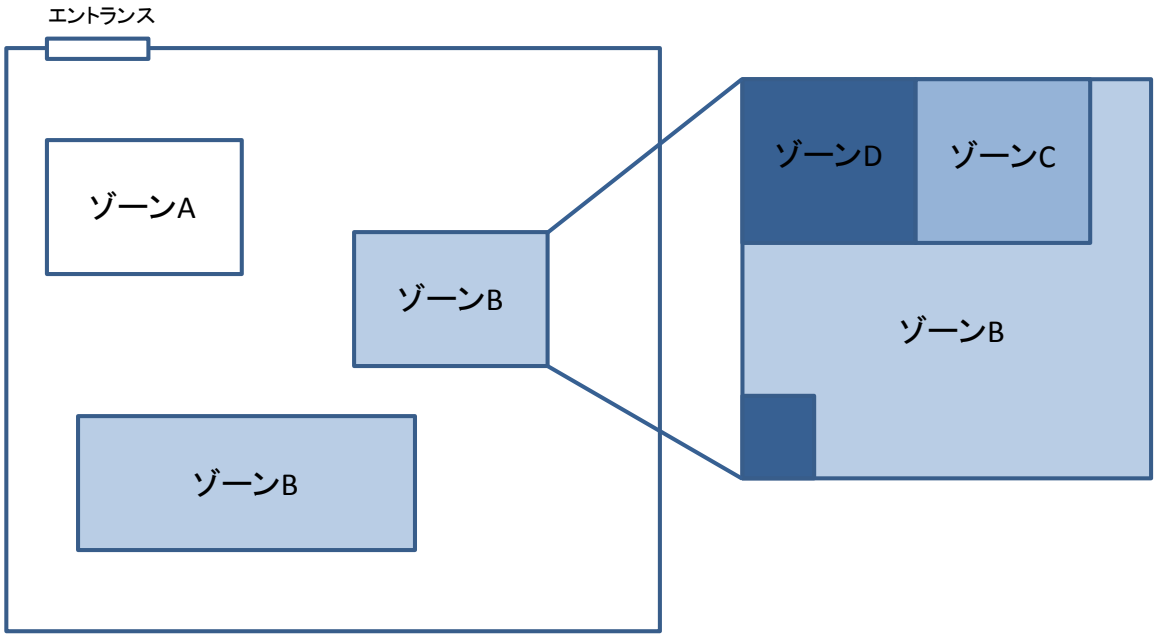
【紙媒体の複製や破棄についての扱い（ヒアリング調査結果）】

- 紙の書類の廃棄については、一般情報用のゴミ箱と機密情報のゴミ箱とを分けて管理している。（製造業）
- 印刷に関するルールは整備されているものの、紙媒体の破棄ルールまでは整備出来ていない。（非製造業）

（４）施設の管理

施設の管理には、不正の意図を持った外部者を秘密情報に物理的にアクセスさせないという目的がある。加えて、アクセス制限の手段としてゾーニング[19]を行うことで、秘密情報を取り扱うエリアから権限のない者を遮断するという効果を得ることができ、アクセス制限目的も加味した施設管理が行われている場合も多かった。

図 3：ゾーニングの例



ゾーンA	社外のものが立ち入れるエリア	（例）展示スペース、応接・会議スペース
ゾーンB	従業員のみが立ち入れるエリア	（例）一般執務室
ゾーンC	従業員の中でも特定の部署に所属する者のみが立ち入れるエリア	（例）経営企画部門、研究所等執務室
ゾーンD	個別に入室を許可された従業員のみが立ち入れるエリア	（例）極秘プロジェクトルーム、文書保管室

（出所）ヒアリング調査を基に作成

ヒアリング調査においても、外部者を執務エリアに入れないというゾーニングだけでなく、社内においても権限に応じた入退室管理を行っているプラクティスが見られた。また、ゾーニングを行う手段として、電子錠と ID カードないし生態認証などが一般的には知られているところ、行動を監視することで不正を予防するという見地から、動線やレイアウトの工夫を行っているプラクティスが見られた。同様に、特に機密性の高い情報を取り扱う企業の例では、社内に監視カメラを導入している他、従業員が１人にならないような業務オペレーション上の工夫も行っているプラクティスも見られた。

19 ゾーニングとは、空間を用途や機能に応じて区分し、配置などを決めることを指す。

【ゾーニングに係る取組例（ヒアリング調査結果)】

- 執務スペースのゾーニングは行っており、社外の人間は特定の会議室スペースなどしか立ち入れない。社内の人間でも例えばアクセス権の無い社員であれば研究所に入れないといった区分は行っている。また動線も以前よりは改善しており、いわゆる裏道は無くなり、必ず守衛所を通らなければ入れない動線になっているなど、工夫されている。(製造業)
- ビルへの入館カードに対しては、入館する者の属性に応じて数段階に分けた制限をかけており、フロアや部屋によって入室可否を管理している。(製造業)
- 機密情報を扱う部署の社員に対しては入退室管理やログ管理も行っており、アクセス権限のない社員がアクセスした際はアラートが鳴るように設定している。(非製造業)
- 「予算が不足」「人的リソースが不足」、を理由に取組を躊躇する会社もあるが、予算をかけずとも出来る工夫はあるはずであり、その工夫を真剣に考える土壌を社内で醸成する事が大切である。例えばグループ会社にも小規模な会社では IC カードによる入退館管理を行っている会社もあるが、複数あった出入口や動線を１つにすることで外部者がフロアに入ればだれもが直ぐに気づけるようにレイアウトを工夫するといったことも行っている。(非製造業)
- 顧客の秘密情報を取り扱う拠点では極力社員が一人にならないように、原則として食事を全員一緒に取らせるなどの工夫をしている。またシステムアクセスについては情報システム部が管理しているが、業務は監視カメラを導入しているが全社的に可視化できていないのが現状である。(非製造業)

厳格にゾーニングを行っている企業では、４段階や５段階のゾーンに区分し、それぞれのゾーンのレベルに応じた管理を行うというプラクティスも見られた。管理レベルの高いゾーンへの入退管理は、来訪者にカメラなどの持ち込みを禁止したり、アクセス可能な従業員に対して情報機器や鞄の持ち込みを禁止しているプラクティスも見られた。

【ゾーニングを厳格に行っている企業の例（ヒアリング調査結果)】

- １番管理の厳しい領域は個人情報や特に重要な顧客情報を保管している保管室である。住所、氏名などの一般的な個人情報を扱う部署が 2 番目に管理の厳しい領域となっている。この部署の執務エリアへの入室に際して指紋認証などまでは導入していないが、監視カメラを導入しており、ゾーニング自体は最高ランクと同様にしている。個人情報や特に重要な顧客情報を必要とする工場が 3 番目のランクとなり、私物の持ち込み禁止や保管場所・作業場所へのパーティション設置などにより関係者の特定を実施している。4 番目が一般的なオフィスエリアとなり、オフィスカードがあれば社員は全員が入室可能となっている。5 番目の領域は訪問客が入室可能な打合せエリアである。(非製造業)
- ランクは固定されているわけではない。顧客から預かる情報の内、特に機密性の高いものについては管理対象者を絞り込み、パーティションで区切るなど管理を強化している一方、頻繁に情報が更新される相対的に機密性が低いものについてはそこまで高いレベルの管理を行っていない。(非製造業)

- 工場はゾーニングを行っており、A ゾーンから D ゾーンに分類している。工場訪問者については、カメラは持ち込み禁止、携帯カメラについてはレンズにシールを張っている。(製造業)
- 工場にはロッカーを設置しており、社員のパソコンやカメラ、携帯電話、鞄などはロッカーに預けたうえで勤務エリアに入室することを義務付けている。(非製造業)

また、秘密情報に限ったことではないが、不正に取得したいと思わせるもの（経済価値を有する有体物を含め）の存在を極力伏せるという企業もヒアリングの中で見られた。例えば、特殊な製品を製造する工場や高度な機密情報を含む顧客情報を扱う工場などの所在地も積極的には公表していないといったプラクティスが見られた。

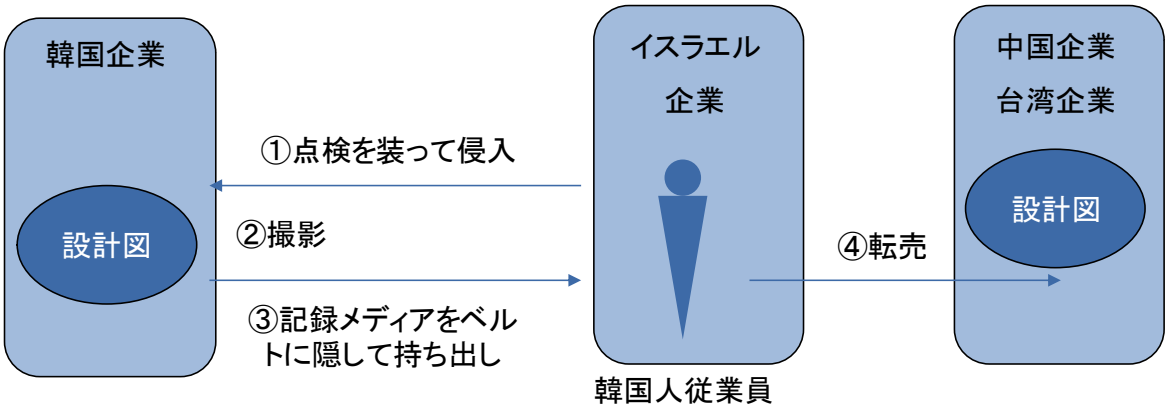
【秘密情報の所在を明らかにしないというプラクティス（ヒアリング調査結果）】

- 物理的保護を強化する意図としては、「情報セキュリティ」の観点もあるが、「ターゲットとなる有体物や情報の所在」を隠すためのものであると言える。ターゲットとなる有体物や情報の所在を明らかにすると攻撃の対象になる可能性がある。(製造業)
- 工場の名前や場所についても公開しておらず、また工場では企業名を外に表示しないようにしている。(製造業)
- 発送に使う段ボールにも企業名は記載していない。(製造業)

施設自体の管理とは異なるが、施設に入室する従業員にはポケットのない作業着を着用させたり、外部者を入出させる際もポケットのない作業着の着用を求めたりしているというプラクティスも見られた。

なお、国内ではなく韓国における事例ではあるが、比較的近年においても、イスラエル企業の韓国人従業員が、韓国企業に点検を装って侵入し、設計図などを撮影し、記録メディアに保管した上で当該記録メディアをベルトに隠して持ち出し、中国企業及び台湾企業にこれを転売したという事例が報道などでも知られている。

図 4：韓国企業における記録メディア持ち出しの事案



（出所）肥塚直人「『技術流出』リスクへの実務対応」（中央経済社、2014 年）29 頁。

【着用する衣服にも秘密情報管理の観点から工夫をしているプラクティス（ヒアリング調査結果）】

・　作業着に関してもポケットのないものを着用させている。スーツで訪問してくる外部の方にも着替えて頂いている。（非製造業）

４．労務管理

（１）従業員の採用

従業員を採用する際、バックグラウンドチェック[20]まで実施しているプラクティスが１社見られた他、前職で営業秘密とされた秘密情報を持ち込まないことについて契約書または誓約書を取っているプラクティスが２社見られた。

【従業員採用時の取組（ヒアリング調査結果）】

- 中途採用で他社から転職してくる者に対しては、入社時に、バックグラウンドチェックのうえ、前職で知った営業秘密を使わないことを義務付ける契約を結ぶ。ただし、個人に蓄積されて残っている情報やノウハウは管理しきれないため、契約書の文面における内容の特定は、人材流動を妨げない程度におさえている。（製造業）
- 他社から転職してきた者に対しては、入社時に他社の機密情報を持ちこんでいない旨の誓約書を取るようにはしているが、一定期間類似業務には関わらせないといった措置までは取っていない。（製造業）
- 会社が身辺調査をするわけではなく、あくまでも自己申告制になっている。当社への転職を希望してくる者が前職において従事していた研究開発プロジェクトの内容について、当該希望者の特許出願状況を調査し、同人がどのような秘密情報に携わった可能性があるのか調査するといったことまでは行えていない。（非製造業）
- 新規採用者が前職の営業秘密を持ち込んだり利用したりしているかについてのチェックまでは行っていない。（製造業）

（２）従業員との契約締結

平成 24 年度に経済産業省が実施したアンケート調査によれば、就業規則以外に従業員と秘密保持契約を締結している企業は 55.5%（301 人以上の製造業が 70.5%、301 人以上の非製造業が 70.2%）[21]、競業避止契約を締結している企業は 14.3%（301 人以上の製造業が 28.8%、301 人以上の非製造業が 14.8%）[22]となっている。

本調査研究で実施したヒアリング調査によれば、入社時のみならず、退職時にも従業員と秘密保持契約書または誓約書を取り交わすプラクティスが複数見られた。また退職時の競業避止契約または誓約書の取り交わしについては、今回ヒアリング調査を実施した限りにおいては１社で確認されたに留まった。

---

[20] バックグラウンドチェックとは、過去の経歴を調査することである。一般的には経歴書などを確認することが多いが、経歴書確認内容を証明する書類や客観的な証明が難しい場合には記載内容が正しいことについての誓約書を取るなどの調査が行われることが多い。

[21] 経済産業省・前掲注 1、11 頁。

[22] 経済産業省・前掲注 1、22 頁。

【従業員との契約締結に係る取組（ヒアリング調査結果）】

- 入社時に秘密保持契約を締結する。（製造業）
- 誓約書は入社時・退職時に取り交わしているが、人事異動で部署がわかった際も誓約書の内容を変えるということはしていない（非製造業）
- 入社時と退職時に秘密保持の誓約書は取っているが、退職時の競業避止に係る誓約書は取っていない。（製造業）
- 誓約書は入社時・退職時に取り交わしている。退職した社員の転職先についての調査は行っていない。当該 OB の名前が聞かれなくなった場合に、海外企業を指導しているケースは少なからずあると理解している。（製造業）
- 退職時には秘密保持誓約書を取っている。誓約書は研究者用とその他用と大雑把には２種類あり、研究者用の誓約書であれば研究テーマなども具体的に秘密保持義務の内容として記載される（その他にも出向者用などいくつかの派成版がある）。なお競業避止条項は入れていない。（製造業）
- 人事部からも、情報セキュリティに係る行動規範について従業員に都度通知が行われる。特に、入社時と退職前には秘密保持義務の誓約書がとられ、違反時の懲戒基準、罰則規定についても通告がなされる。秘密の範囲は特に指定されないが、当社の情報区分において秘密情報と定義されている機密についてはすべて対象となる。（製造業）
- 退職者とは秘密保持契約を締結するが、一律のひな型を用いており、個人毎に秘密保持義務の対象となる秘密情報を個別に特定はしていない。（製造業）
- 従業員に対する秘密保持は、基本的には就業規則などに依っている。退職者については別途誓約書を取っており、秘密保持及び競業避止を定めている。内容についてはある程度、判例などを研究して作成しているが、訴訟戦略的なことまでは踏まえられていない。（製造業）

入社時及び退職時のみならず、重要なプロジェクト参加時や R&D 部門（研究開発部門）配属時に別途の秘密保持契約書ないし誓約書の取り交わしを行うというプラクティスも２社で見られた他、重要会議などにおいては、参加者から都度誓約書を取っているというプラクティスも２社において見られた。

【入社時及び退職時以外にも契約書ないし誓約書を取り交わす例（ヒアリング調査結果）】

- 入社時に秘密保持契約を締結するほか、重要なプロジェクトへの参加時には再度、具体的に秘密内容を特定した個別の秘密保持契約を結ぶ。(製造業)
- 秘密保持に係る誓約書は入社時には全員から取っている。また中途で R&D 部門などに配属される者についても誓約書を取っている。（製造業）
- 新薬の開発に関する情報などの企業にとって非常に機微な情報を扱う、経営上の重要な会議やグローバル会議では必ず参加者から秘密保持の誓約書を取るようにしている。（製造業）
- 新しい技術や材料について検討する「新市場勉強会」には、情報保護に関する誓約書にサイ

ンとしてからでないと参加できないこととしている。なお当勉強会は議事録も公開していない。（製造業）

今回のヒアリング調査の中では、上記の場合を除いて、部門によって労務管理に運用上の差異を設けているプラクティスは見受けられなかった。

【その他従業員との契約締結に係る事項（ヒアリング調査結果）】

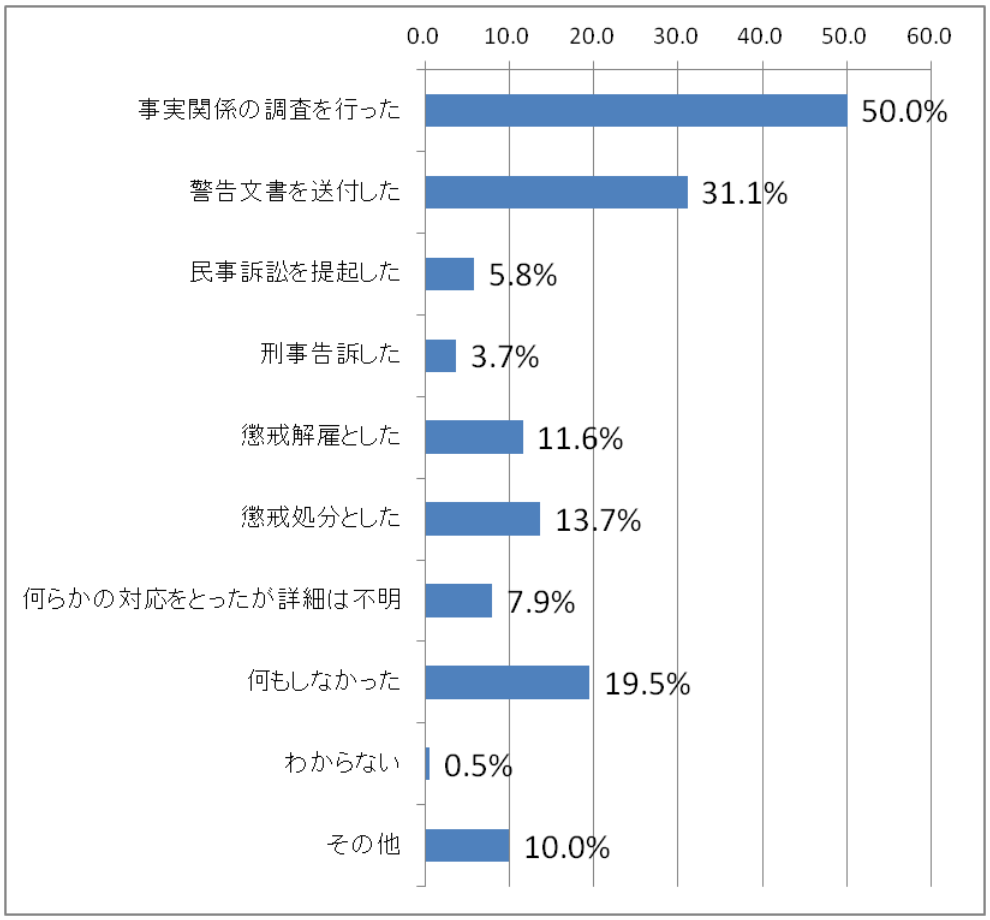
- 情報管理に関する誓約書は以前から導入しており、特段変更をしておらず、全社員同じ誓約書になっている。（製造業）
- R&D 部門だけでなく、営業職なども研修プログラムや誓約書の運用は同じとなっている。（製造業）

（3）従業員に対するエンフォースメント

一般に日本企業は、従業員ないし元従業員に対して積極的な対応を行わない傾向があり、経済産業省が実施した過年度の調査においてもこうした傾向は明確に現れている。具体的には、営業秘密の侵害行為者・企業に対して半数しか調査を実施しておらず、警告文書を送付した企業が 31.1%、民事訴訟を提起した企業が 5.8%、懲戒解雇とした企業が 11.6%となっている[23]。

[23] 経済産業省・前掲注 1、57 頁。

表 3：営業秘密の侵害行為の行為者・企業に対する対応



（出所）経済産業省（委託先：三菱 UFJ リサーチ&コンサルティング株式会社）「人材を通じた技術流出に関する調査研究報告書（別冊）」（2013 年 3 月）57 頁。

本調査で実施したヒアリング調査においても、エンフォースメントに係るプラクティスはほとんど聞かれなかった。例えば、情報機器の紛失の程度により懲戒処分としている例も見られた。また、エンフォースメントについて現状は積極的であるとは言えないものの、悪意のある場合においては、抑止の観点からもエンフォースメントを強化していく必要があると認識している企業も 1 社見られた。

【エンフォースメントの実態（ヒアリング調査結果）】

- 懲戒処分は他社比で厳しいと言えるか分からないが、時々処分例がある。実際に情報機器の紛失で懲戒処分となった例もある。（製造業）
- 悪意をもった漏えいに関しては、今後抑止力を強くしていく必要があると認識している。（製造業）
- 危機管理委員会に報告された事項は得意先関係であれば営業部、社員の懲罰に関することは人事部、社会に報告する必要がある場合は広報部、社内に周知させる際はマネジメント推進部へと報告される。（非製造業）

- 情報漏えいにつながるようなオペレーショナルミスや、社内ルール違反について、懲戒の対象となるような重大なものは別として、通常の人事評価に影響を与えるような仕組みはない。（非製造業）

（4）研修・人材育成

秘密情報管理に関連した研修を実施している企業では、集合研修だけではなく、e-learning を活用しているプラクティスが散見された。e-learning については、受講結果をテスト形式などで確認し、理解が不十分であった従業員に対しては追加的な勉強をさせるといったプラクティスも見られた。また、e-learning について、理解度テストで 100 点を取ることをルール上は求めながらも、受講率の向上を課題として受講を昇格要件化することなどを含めた検討を行っているプラクティスも見られた。

【研修実施の取組（e-learning の活用実態）（ヒアリング調査結果）】

- 情報セキュリティに関する従業員の教育を実施している。e-learning や集合研修などの形態で、情報セキュリティについてのさまざまな内容の研修プログラムがさまざまなタイミングで実施される。（製造業）
- 現在、教育機会を年２回確保している。１～1.5 時間程度をあてているが、e-learning などを利用してフォローアップや理解度を計測していくことが必要だと感じている。受講や理解度を高めることについて、何らかのインセンティブを考えていくことも必要と感じている（が、現状、委員会の議題には至っていない）。（製造業）
- 年に１回、情報管理に関するテストを e-learning で受講するよう周知している。（非製造業）
- e-learning なども活用し定着を図っている。（製造業）
- e-learning は頻繁に行っており、２～３カ月に１回程度は行っている。（製造業）
- 不正競争防止法の遵守について e-learning などの形式で研修を実施し、啓発をはかっている。(製造業)
- 随時 e-learning などの形式で研修を実施し、啓発をはかっている。（製造業）
- テスト結果をみると知識問題は正答率が高いが、社内ルールに関しては誤答が目立っている。（非製造業）
- 正答できなかった社員には社内ポータルで勉強してもらうようにお願いしている。（非製造業）
- 情報セキュリティ全般について e-learning が実施されている。（製造業）
- 研修内容はメニュー化されており、各社を訪問して実施するタイプのものや、イントラネットで配信するものがある。（製造業）
- e-learning やテストで合格点を取ることはルール化されているものの、実施しない社員もいる。昇格の条件にするなど何かしらのインセンティブをつけなければならないと考えている。（非製造業）

研修の受講対象としては、正社員に限定せず、派遣社員や社内に常駐する業務提携先の従業員なども対象としているプラクティスの他、管理者を対象とした研修と全従業員を対象とした研修というように階層別の研修を実施しているプラクティスも見られた。

【研修受講対象者についての考え方（ヒアリング調査結果）】

- 情報管理意識向上のための教育・研修については、以前は正社員のみが対象だったが、現在は派遣社員、常駐している他社社員も受講を義務付けている。（非製造業）
- 研修は管理者向けと全従業員を対象としたものと二段階で実施している。（製造業）
- 管理職などに対する研修には知的財産部門が講師となって実施する研修も多いが、契約や知的財産の部分はかなり重点的に行っている。（製造業）

研修などにおいて意識されている事項としては、リテラシー[24]向上の重要性があげられる。ヒアリング調査では、複数の企業においてこうしたプラクティスが見られた他、特に海外赴任者など、特定の従業員に対して別途の研修を行っているプラクティスが見られた。

【基本的なリテラシー向上に向けた取組（ヒアリング調査結果）】

- 社員のリテラシー向上は、情報漏えい対策として極めて重要である。（非製造業）
- 当社でも情報漏えいないし技術流出が発生したことはあるが、そうした事態を踏まえて社内で実施している情報管理施策についても、さらに周知と意識付けをはかる目的で新たな定期的研修を実施予定である。(製造業)
- 当社の人事ローテーション上、R&D 部門出身者が様々な部門で活躍しており、経営層・上級管理職などにも R&D 出身者が多い。R&D 部門を経験する中で、秘密情報に係るリテラシーを高め、結果としてリテラシーの高い人がマネジメントを担っている。（製造業）
- 社員教育に関しては人事部が新入社員教育と役職者教育を実施している。（製造業）
- 現職者に対して、OB であっても外部者であり、不用意に情報を開示しないよう意識付けを行っている。（製造業）
- 情報管理に対する教育を根づかせるためには上長の意識が必要。教育により上長の意識を変えても、人事異動で当上司が変わってしまった場合、また教育をやり直さなければならない。この点について解決策を検討する必要がある。今後も他社の情報管理事例や導入方法を参考として体制強化に努めたい。（非製造業）
- 特に海外赴任者に対しては、情報の無断持ち出しをしないよう、別枠で研修を実施する。（製造業）

[24] リテラシーとは、物事の趣旨を理解し、適正な行動ができる能力のことである。

研修の他、秘密情報管理の観点から重要となるメッセージの従業員に対する発信や、危機感を持ってもらうための情報提供などを積極的に検討ないし実施しているというプラクティスも見られた。

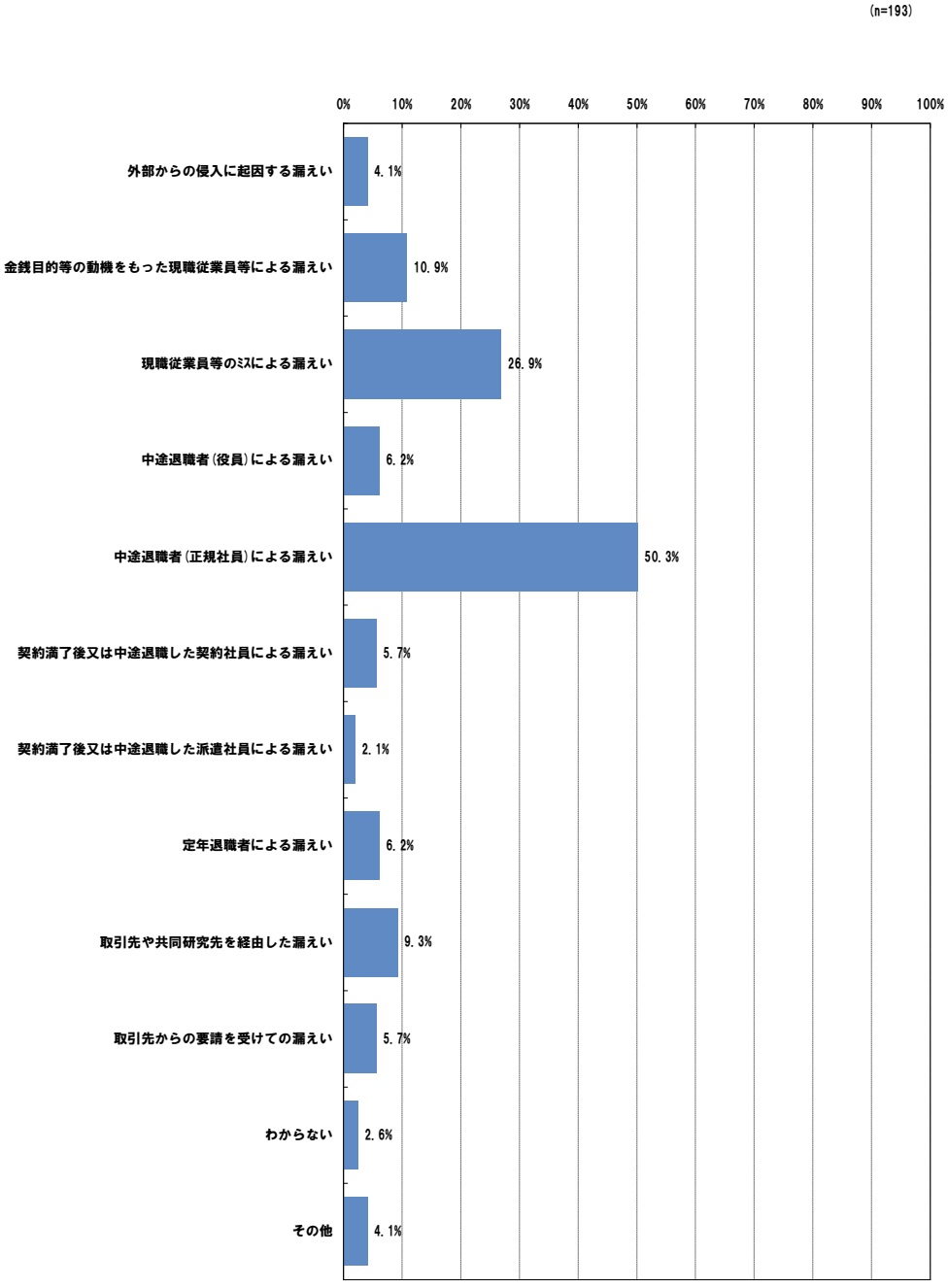
【社内への情報発信に係る取組（ヒアリング調査結果）】

- ビジュアルなガイドブックの作成も検討中である。社内でリスクが顕在化した事例を載せるのがわかりやすいと考えている。（製造業）
- 研修内容はメニュー化されており、各社を訪問して実施するタイプのものや、イントラネットで配信するものがある。（製造業）
- 加えて定期的に「情報セキュリティ通信」を発行し、他社事例や旬のトピックなどを共有している。また、社用車の車上あらしや携帯電話の紛失、置引、飲酒に関する事故などの 実際に発生した事故の共有も行っている。（製造業）

（５）退職者に対するフォロー

平成 24 年度に経済産業省が実施した調査によれば、過去５年間で営業秘密の漏えい事例が明らかにあったと回答した企業においては、退職者が営業秘密の漏えい者となっているケースが多いことが明らかとなっている（表４参照）。

表 4：営業秘密の漏えい者の種別



（注） 過去 5 年間で営業秘密の漏えい事例が明らかにあったと回答した企業のみ回答。複数回答式の設問のため、各選択肢の割合の合計は 100%にならない。

（出所）経済産業省（委託先：三菱 UFJ リサーチ&コンサルティング株式会社）「人材を通じた技術流出に関する調査研究報告書（別冊）」（2013 年 3 月）53 頁。

今回のヒアリング調査の結果、退職者に対して秘密保持契約書にサインさせることが比較的広く行われていた。また、競業避止義務契約を締結するプラクティスも見られた。

【秘密保持契約や競業避止契約に係る実態（ヒアリング調査結果）】

- 社員には退職の際、秘密情報保護の誓約書を書かせている。（製造業）
- 退職者については全社レベルで全ての退職者について誓約書を取っているが、事業本部 単位で流出した場合のリスクが高い情報に接している者が退職する場合には、人事部門に相談することなく、事業本部の判断で全社共通の誓約書の他に具体的な秘密情報を特定し、競業避止条項を付加した確認書を取っている。（製造業）
- 契約上、競業避止義務も負わせている。競業避止期間は１年程度だが、特段代償措置を含む有効性要件まで精査出来ておらず、どちらかと言うと現状では心理的効果に留まるという認識である。（非製造業）
- 社員には退職の際、秘密情報保護の誓約書を書かせている。（製造業）
- 優秀な人材に関しては当然説得を試みるが、それでも退職したいとなった場合、個別に競合避止契約を結んでいる。（製造業）
- 退職時の対応については、現状では秘密保持を取っている程度である。退職者の ID は即座に抹消するようにしている。（製造業）
- 競業避止契約、秘密保持契約などについても面談時に説明の上、押印を求めている。（非製造業）
- 退職時に秘密保持契約を締結する。特に重要技術の研究開発に関わった技術者に関しては、秘密内容を特定した契約を結ぶ。（製造業）

退職者が秘密情報を持ち出す可能性があることから、秘密情報管理の観点からも転職先の把握や、秘密保持義務や競業避止義務の存在を強く認識させることを目的とした面談を実施するというプラクティスが見られた。

【退職予定者面談の実態（ヒアリング調査結果）】

- 転職先の把握については、人事部が退職予定者については全員に対して面談を行っており、必ず把握を試みるようにしている。（非製造業）
- OB 組織が発達しており、定期的に会合があるので、その場を活用しながら緩やかに近況を把握している。競業避止義務契約の締結や厳格な追跡などは行わない。それよりも文書や図面を通じた流出リスク管理のほうが優先度は高いので、退職時には個別に面談を実施し、「ついつい」持ち出してしまうことを予防している。（製造業）

なお、ヒアリング調査に回答頂いた企業の中には、大学教員や自社 OB などが顧問として研究部門に在籍しているものの、一般の研究職に比べて十分な秘密情報管理が行えていないことを問題視しているというプラクティスもあった。

【研究部門などにおける顧問活用の課題（ヒアリング調査結果)】

・　研究部門には、顧問などの非正規職員（大学教員や当社 OB など）が在籍しているが、機密情報の管理については基本的に信頼関係に任せている部分があり、コントロールが難しいと感じている。(製造業)

また、退職者による不正な情報の持ち出しに対して、退職金の不支給措置[25]を含む厳しいエンフォースメントを実施しているというプラクティスも見られた。

【退職金不支給について（ヒアリング調査結果)】

・　退職者が不正な情報持ち出しをしたことが発覚した場合、退職金の不支給措置がとられる。情報を漏えいしなくても、持ち出しただけで罰則の対象となる。罰則の程度は、情報の内容によって異なる。(製造業)

[25] 退職金などの減額や不支給が常に認められる訳ではないが、事前に退職金などの減額や不支給に係るルールを定めておくなど労働法上の要件を満たしていること、退職者に背信性があること（全額不支給とすることについては、減額の場合と比較してより高度な背信性が必要であるとされている）などの要件を満たしていれば法的には認められる可能性が高い。この点については、平成 24 年度に経済産業省が実施した調査で詳細に検討が行われており、経済産業省（委託先：三菱 UFJ リサーチ＆コンサルティング株式会社)「平成 24 年度経済産業省委託調査　人を通じた技術流出に関する調査研究報告書」（2014 年 3 月）29 頁以下が参考になる。

（6）その他

従業員などが処遇や与えられている業務自体に不満を持っている場合、これがきっかけとなって不正を行う可能性が無いとは言えない。そこで、従業員満足度調査（ES 調査）の結果から従業員の不満などを分析し、不正の兆候の検知に役立てているというプラクティスも見られた他、不満を持つ従業員などによるインターネットの書き込みなども調査の対象としているというプラクティスもあった。

【その他労務管理上の取組（ヒアリング調査結果)】

- 3 年前から従業員満足度（ES）調査を実施している。ES 調査では自由記載項目があり、そこで社員の不満や疑問などを収集し、不正の兆候発見している。会社に不満を持つ人物からの漏えいリスクは相対的に高いため、ISO 導入により、PDCA の流れを体系的に実施できる体制を構築すべきだろう。(製造業)
- インターネットへの書き込みも含めて、当社に不満を持っている従業員や不正の兆候の有無についても調査を実施している。(製造業)

５．取引先管理

（1）パートナー企業との契約

ヒアリング調査において、パートナー企業との各種契約において、秘密情報ないし営業秘密の取り扱いについて明確な定めを設けるというプラクティスが定着しつつあり、秘密保持条項について厳格な運用を行っているという声があった。また、共同研究先や生産委託先には技術的に秘密性の高い情報を開示することが多いことから、契約書を取り交わすこと自体や契約書の内容についての重要性を指摘する声があった。

【パートナー企業との契約に係る実態（ヒアリング調査結果)】

- 営業機密に関しては、共同開発契約、販売契約など、各契約書の条項においても定めており、契約の観点からも厳格に運用している。(製造業))
- R&D 部門は外部との協働も多く、適切な内容の契約を締結することは重要である。(製造業)
- 共同研究や生産委託などで技術情報に接触する可能性がある協業先とは、個別に契約を結んで管理する。また、協業先の従業員とも秘密時保持契約を締結する。逆に、協業先の営業秘密を不当に使用してしまうリスクを回避するため、業務の中で接触したり、見たりするものの使用を許す秘密不開示契約を締結する場合もある。(製造業)

研究開発部門において、契約に特化した研修を行い、自社の秘密情報を守るという観点のみならず、他社に対する秘密保持義務に違反しないような情報の取り扱いについて啓発を行っているというプラクティスも見られた。

【研究開発部門における契約研修実施の取組（ヒアリング調査結果)】

- 契約については、契約専門の研修を行っており、日本知的財産協会（JIPA）などで行われている契約関連の研修と比べても踏み込んだ研修を実施している。研修では秘密情報について、自社の情報だけでなく、他社の秘密情報について意識的に区別して取扱いの考え方について研修を行っている。(製造業)

秘密保持契約については相手に対して秘密保持義務を課す手段として認識されるが、一般的に秘密保持義務は相互に負うため、自社も相手から課された秘密保持義務に違反するリスクを負うことになる。特に秘密保持契約を締結する相手方が多岐にわたり、様々な部門において独自に契約を締結すると、秘密保持義務を負っているという認識をしていない従業員が知らず知らずのうちに秘密保持義務違反を犯してしまう可能性がある。こうしたリスクを軽減する観点から、契約管理システムを構築・導入しているプラクティスが見られた。

また、様々な取引関係者に対して重層的な契約関係が発生する企業で、契約管理自体の必

要性から契約管理のシステムを導入しているところ、管理項目の１つとして秘密保持義務を扱っているというプラクティスもあった。

【契約管理システムの活用実態（ヒアリング調査結果）】

- 秘密保持契約（Non-disclosure agreement：NDA）の当事者、守秘義務を負っている情報の内容などについて契約管理システムを導入してシステム管理を行っている。（製造業）
- 大手システムベンダーが提供している契約管理データベース（database ：DB）を用いて、契約の相手先となる取引先の契約管理を行っている。この契約管理 DB には秘密保持条項などについても入力されており、どのような取引先に対してどのような秘密保持義務を負っているのかといった点についても把握ができ、例えば子会社同士で一方が追っている秘密保持義務を他方が知らずに義務違反を犯してしまうようなことが無いようにしている。（製造業）

大学と行う共同研究につき、原則的には技術的な観点から秘匿性の高い秘密情報を共有しなくてもよいテーマを中心に行いつつ、特殊性の高い研究で秘匿性の高い秘密情報を共有せざるを得ないテーマにおいては特別な管理を行うというプラクティスも見られた。

【大学との共同研究実施の考え方（ヒアリング調査結果）】

- 大学との共同研究では、基本的にはオープンになっても深刻な問題とならない情報のみを共有して進めている。ただし、特定の大学と行っている特殊な研究に関しては厳重な情報管理を前提に共同研究を実施している。（製造業）

（２）パートナー企業の選定と調査・監査の実施

ヒアリング調査において、パートナー企業を選定する際、秘密情報管理という観点から、秘密情報の預託を行いうる企業であるかどうかについて調査を行うことが多いことがわかった。情報管理の状況やプライバシーマークや ISMS などの第三者認証の有無を含めて確認しているというプラクティスが見られた。また事前の調査は実施しているもの、契約後に監査をすることまでは行えていないという声もあった一方で、契約後も契約上の義務に係る履行状況を監査しているというプラクティスも見られた。

【パートナー企業の選定と調査・監査の実施（ヒアリング調査結果）】

- 外部委託先のチェックについては、情報管理の状況やプライバシーマークの有無などを中心に確認している。基本的には、契約の開始時などに先方から情報管理の状況などについて申告してもらっているが、契約締結後も半年に１回程度は申告内容が正しいかどうかの確認を行っている。（製造業）
- 個人情報を外部委託する場合、預託前に訪問して情報セキュリティ体制について調査を行い、

事後に定期的な監査も実施している。プライバシーマークやISMSを取得している事業者の場合、特段の事情が無ければ取引前調査のみで済ませているが、そうでない事業者の場合、事後の監査も定期的に行っている。外部に委託する際は、一定のセキュリティを担保できるかどうかを事前に確認するようにしている。また、委託先から再委託という形で別の機関が関与する場合もあるが、その場合も同等レベルの事前確認をしている。(製造業)

- 外部委託先の管理は、事前の与信審査が中心であり、契約上秘密保持義務や一定の管理を要求しているものの、契約後のモニタリングは出来ている訳ではない。(非製造業)
- 協業先の秘密をむやみに受け取らないよう、事業フェーズが進んでもモニタリングを実施する。具体的には、他社に提出する秘密保持契約書はすべて報告させ、不正な使用をしてしまわないよう管理する。(製造業)

一般的な委託契約と、秘密情報を預託する可能性がある共同研究契約では異なる管理プロセスを設けているというプラクティスも見られた。また、中には事務作業に係る一般的な業務委託において個人情報を預託する場合以外は、秘密情報を基本的には外部の企業と共有しないというプラクティスも見られた。

【取引の性質に応じた管理の取組（ヒアリング調査結果)】

- 外注契約と技術契約（共同研究契約など）とで管理プロセスが異なる。基本的には、いずれの場合にも情報セキュリティなどについて確認書を取り、NDAを結ぶことになる。確認書のレベル感はプロジェクトの区分に応じて異なるものを用いている。外注契約の場合、確認書を記入頂き、当社側で確認するという形になるが、技術契約の場合、確認書を相互に交わし、お互いの情報セキュリティなどについて確認を行っている。(製造業)
- 基本的には個人情報の預託先を除いては、機密情報は外部には出さずに社内のみでの管理となっている。(製造業)

（3）パートナー企業の管理

パートナー企業と秘密情報の受け渡しを行う場合には、授受記録をつけた上で、受け渡しを行った秘密情報について台帳管理を行っているというプラクティスが見られた。

【情報授受に係る管理の実態（ヒアリング調査結果)】

- 取引先との情報の受け渡しが発生する際は、社内で書類を管理する際と同じ分類で授受記録を取るようにしている。授受記録のフォーマットは整備されているが、これに限らず電子的に証跡があれば代用可としている。授受記録の保管期限は特に定めていない。(製造業)
- 取引先と受け渡しを行った情報については、エクセルで台帳管理を行っている。管理している項目は、内容、保管場所、機密区分、提供先、管理責任者、入手先などである。但し、こ

れらのファイルが本当に台帳に記載されているフォルダに格納されているかどうかまでは確認できていない。(製造業)

また、ヒアリング調査の中では、取引先における秘密情報管理レベルの向上が課題であるとする声も聞かれた。

【取引先の秘密情報管理レベル向上に向けた取組（ヒアリング調査結果)】

- 当社と取引がある中小企業の底上げが不可欠である。そのためには、情報セキュリティマネジメントが業務改善の要である事を徹底的に理解させる必要があり、当社も取引先に対し積極的に啓蒙活動を行っていく必要がある。(非製造業)
- 関連会社に対する情報セキュリティの説明会でも、インシデント発生時に同じ対応を取ってもらえるよう説明を行っている。また、訴訟を含めた事後対応を容易にするための証跡収集や当局の協力を効率的に得るためのノウハウもグループで共有していこうとしている。(製造業)

６．グローバル拠点の管理（日本企業の場合）

海外に複数の拠点、支店や関連会社を持つ経営は、大企業だけでなく中小・中堅企業にとっても身近なものとなっている半面、現地特有の事情などもあることから、グローバル拠点における秘密情報管理については、各社ともに試行錯誤している実態が分かった。

ヒアリング調査の中では、海外拠点にも日本本社と同一の秘密情報管理に係る規程を採用させているが、図面の管理や人的な管理については海外拠点においてより踏み込んだ管理を行っているというプラクティスや、グローバルに展開する関連会社に対して適用するセキュリティ・ポリシーを説明し、これを理解してもらうために、敢えてセキュリティ・ポリシーには国際規格を用いているというプラクティスも見られた。また、定期的に関係部門による連携会議を開催し、世界各所での情報共有を図っているプラクティスも見られた。

【グローバル拠点の管理実態（ヒアリング調査結果）】

- 中国に生産拠点を持っており、日本と同一の規程を採用している。しかし運用上は、それ以上の管理を指示している。特に、図面の管理について徹底している。デザインについてはいたちごっこになるため、人的な管理に注力している。信賞必罰の基準を明確にして、秘密を守ることのインセンティブが働くよう工夫している。責任を持って取り組むこととその成果に対するメリットを明確にしている。（製造業）
- グローバルに展開する関連会社（資本関係のある企業）にも同じセキュリティ・ポリシーは適用されるが、国際規格を用いることで説明が容易になり、協力も求めやすくなっている。複雑な自社仕様ではなく敢えて標準化されたフォーマットを活用している。（製造業）
- 年２回グループ全体で営業機密の事務局連絡会を開催しており、その際に、グル―プグローバルで情報の共有を行っている。（非製造業）
- グローバルでの管理の徹底にあたり、最も重要な事は現地のカルチャーの違いを理解する事である。（非製造業）
- グループ本社や、傘下の別のグループ会社では、情報セキュリティに対する考え方そのものが異なるため、サーバ上のアクセス制限やUSBの使用禁止が受け入れられないことが多い。海外は訴訟社会なので、不正が発覚した際は厳罰を科す、という前提のもと、緩やかな規制がかけられているようである。（製造業）
- 現在は海外支店を保有しているため、今後は上海に続き、米国、タイ、フィリピンにおける管理を徹底していく必要がある。なお、グループ化したばかりの拠点での管理の徹底はこれからだが、他の海外支店は人数も少ないので運用でカバーしていきたい。（非製造業）
- 現地法人の監査（輸出・輸入など）については強く必要性を感じているが、現在ルールを検討中である。（非製造業）

７．中小企業における実態

本調査研究では、中小企業における秘密情報管理の実態についても把握すべく、国内中小企業に対するヒアリング調査を実施した。

中小企業においても、限られた経営資源を有効に活用しつつ、適切な秘密情報管理を行っている企業も存在する。広く中小企業にとって参考となると思われるプラクティスを【特徴的な取組】として、以下整理する。

（1）秘密情報管理に対する考え方

ヒアリング調査の結果、秘密情報の存在や秘密情報が漏えいすることのリスクは概ね理解されていても、秘密情報管理については組織的な対応には至っておらず、各担当者個人の裁量的な管理に任されているケースも少なくないのが実態であることが分かった。

他方、特徴的な取組として、オープン＆クローズ戦略を意識しつつ、ノウハウとして秘匿すべきものについて意識的な秘密情報管理を行っている中小企業のプラクティスが見られた。当該中小企業においては、製造仕様書などの形で文書化が可能なノウハウについては文書化を行った上で、経済産業省が策定している営業秘密管理指針を参考に、営業秘密として管理を行っている。

【秘密情報管理に対する考え方（ヒアリング調査結果）】

- 自社内もしくは外部委託先に仕様書などの重要な秘密情報は存在しているが、現在は明示的な管理はなされていない。公開可能な情報なのか、社外秘の情報なのかも個々人の裁量に任されているのが実態であり、情報区分もルール化されていない（製造業）。
- 社内の部署は「営業」「業務」「製造」に大別でき、原則、業務部と製造部の書類については、社内の数字や製造ノウハウが記載されているものがあるため、持ち出し禁止としている。もっとも書類上にその旨が明記されているわけではない（製造業）。
- 権利化ではなくノウハウとして管理している技術もある。知財管理についても出願行為を先使用の公証資料として扱うなど、戦略的な管理を行っている。しかしノウハウに係る管理については、ファイリング方法も重要なものについて丸秘マークを付けている程度で、今後より精緻な制度に切り替えていきたいと考えている（製造業）。

【特徴的な取組】

- 製造・加工プロセス、薬品配合比率、配合方法、不純物の除去方法などのノウハウが品質競争力の源泉となっている。これは基本的に開示すべきではないとの考えから、権利化を行っておらず、営業秘密として管理を行っている（知的財産権については商標権などの取得はしている）。こうした営業秘密の多くは、製造仕様書などの形である程度は文書化されており、当該文書は管理の対象となっている。もっとも文書に落とせない技能的なノウハウもまた少

なくない（製造業）。
- 取引先の大企業から契約上、秘密保持義務を課されているが、具体的な秘密保持のための管理方法や管理水準まで細かく指示を受けている訳ではない。そこで、当社として秘密保持義務に違反しないよう、不正競争防止法改正の報道をきっかけに、営業秘密管理の重要性を改めて認識し、経済産業省の Web サイトに掲載されている資料や、営業秘密管理指針を参考に体制整備を行った（製造業）。

（２）秘密情報管理に係る体制

経営者が中心となって秘密情報管理体制を運用しているプラクティスが散見された。中には、経営者自らが秘密情報管理担当者を選任して社内に配置し秘密管理体制の浸透に努めているプラクティスも見られたが、他方で、秘密情報管理担当者の存在と役割が社内で十分に理解されているとは言えず、秘密情報管理体制自体が社内に浸透している訳ではない企業も見られた。

他方、特徴的な取組として、取引先の大企業が毎年セキュリティ監査を実施していることを受けて、監査時に当該取引先に説明可能なレベルの秘密情報管理体制を構築しているというプラクティスや、第三者認証を上手に活用しながら秘密情報管理についても適切なマネジメントシステムを構築しているというプラクティスも見られた。

【秘密情報管理に係る体制の実態（ヒアリング調査結果）】

- 情報管理担当者は任命しているがマニュアルを作成するなどした明示的な管理は行っていない。社員が 80 名程度であるため、それなりに全社員に対して目が届く規模感であり、お互いの信頼関係を前提にした運用を行っている。（製造業）
- 情報管理の責任者は社長が担当しており、パソコンに対するパスワード設定の遵守など、ルールを定めているものもあるが、事細かなルール作りはしていない。本社・工場を含めて 3 拠点あるが、社長が各拠点に顔を出していることと、社員数が 3 拠点合計で 26 名と少数であるため、しっかりと目は行き届いていると思っている。（製造業）
- 経営面（財務面）や人事面に関する情報や顧客情報、図面情報、単価情報、情報セキュリティに関する情報などを重要度の高い情報として位置づけている。ただし、厳密な階層を設け総合的に管理しているまでには至っていない。ファイリング方法も重要なものについて丸秘マークを付けて、社内の秘密情報は施錠のできるキャビネット内に保管するほか、鍵も一部の社員（社長および幹部社員）が使用できるように制限している。（製造業）
- 管理体制上の責任者は社長をトップに各部門の部門長が当該部門における営業秘密管理の責任者となっている。営業秘密管理規程を整備し、管理すべき情報と取扱について社内にルールとして徹底をしている。（製造業）

【特徴的な取組】

- 顧客（大企業）との安全管理に関する取り決めに対応しており、先方から毎年セキュリティ監査が入るため、先方の様式に沿って、社内の秘密情報の管理責任者などを明確にするほか、当該情報にアクセスできる社員も制限をかける（社長、役員など８名）など、情報が拡散しないよう管理している。（製造業）
- 研究開発や製造部門では部門長の判断で、営業秘密管理規程を策定した際に読み合わせを実施し、内容の理解も促している。この点、当社は ISO9001、ISO14001 を取得しており、ISO に準拠したマネジメントシステムとして、新しいルールを周知し、周知記録を証跡として取るという行動を自然に行ったに過ぎない。その意味においては ISO をベースとしたマネジメントシステムはある程度定着していると思われる。（製造業）

（３）物理的な管理

物理的な管理については、パソコンや USB などの情報機器の取り扱いについてルールを設けたり、電子媒体へのアクセス制御などを実践している企業も見られた。

加えて、特徴的な取組として、情報システム全般について社長自らが主導的に構築し、情報システム上のセキュリティについても社長自らが決定しているというプラクティスが見られた。アクセス権の設定、変更といった重要な処理も、社長が行っているため、経営者の知らない所で重要な秘密情報が従業員の誰からでも閲覧可能な状態にならないような運用が行われており、組織の規模に応じて適切な物理的な管理を行っているプラクティスとして参考になる。

【物理的な管理に係る取組（ヒアリング調査結果）】

- 紙媒体の秘密情報については、秘密情報などの明示はしておらず、秘密情報を保管するための施錠可能な棚があるので、原則そこに保管するルールにはなっている程度である。どのような情報が記載された紙媒体が施錠管理対象なのかの定義・台帳管理までには至っていない。電子媒体の秘密情報については、個人情報が記載されたものだけはパスワードをかけて管理しているが、仕様書などを含めたその他の資料については特段の管理をしていない。パソコンの持ち出しや USB の利用については原則禁止としている。（製造業）
- 紙媒体の秘密情報は、決められた場所への保管、FAX などの禁止をルール化している。施錠管理は徹底出来ているとは言い難いが、施設セキュリティ自体は入口の施錠や入り口や通路のカメラ監視なども含め、ある程度厳重におこなっている。（製造業）
- 紙媒体の秘密情報については、全ての文書についてルールを決めて施錠管理するような体制にはなっていないが、作業マニュアルについては工場で施錠管理されており、施錠の鍵も工場長だけが管理できるようにしている。作業マニュアル以外の紙媒体については、秘密表示の記載や台帳管理などもなされていない。電子媒体の秘密情報については、アクセス制御やパスワード付与を含めて、情報管理に関するルールはほとんどないのが現状である。USB の利用については原則禁止としている。（製造業）

・ 紙媒体の管理について、ファイリング方法に一定のルールを設けている。例えば重要なものについて丸秘マークを付けて、社内の秘密情報は施錠のできるキャビネット内に保管する他、鍵も一部の社員（社長および幹部社員）が使用できるように制限している。電子媒体などの管理について重要度の高い情報（経営に関わる情報や、人事や給与に関わるもの）については、フォルダへのアクセス制御、ファイルへのパスワード設定を行っている（社長であってもパスワードがないと開けない)。暗号化などのソフトウェア導入までは行っていない。情報セキュリティ規程は未整備である。事業継続計画（Business continuity planning : BCP）の観点で整理している事項はあるが、情報セキュリティ規程については今後策定していきたい。ただし、どこまで精緻に準備すべきか判断が難しいと感じている。（製造業）

【特徴的な取組】

・ 当社では情報システムを社長自らが責任を持って構築しており、社長が実質的な担当者となっている。アクセス権変更権限は社長しか持っていないので、アクセス権を変更する場合には社長に依頼する必要があるため、不必要にアクセス権が拡大することはない。社長自身は情報システムを通じた漏えい対策の重要性を十分に理解しており、費用対効果を考えつつも必要なシステム投資は行っている。（製造業）

（4）労務管理

労務管理に関連して、秘密保持契約書または誓約書によって従業員に対して秘密保持義務を明示的に課すというプラクティスは、中小企業においても実施されている例が見られた。また、秘密保持義務のみならず競業避止義務を含んだ契約書または誓約書を退職者との間で取り交わしている例が複数の中小企業において見られた。

加えて、特徴的な取組として、Ａ４一枚ほどの比較的詳細な業務日誌の記載を全従業員に求め、従業員相互にも回覧する他、上司は部下の業務日誌に、社長や副社長は全員の業務日誌に毎日目を通すことで、従業員の心理的な変化や不正の予兆などを未然に把握し、事前の対応を行っているというプラクティスも見られた。当該中小企業では、それほど規模も大きくないことから社長や副社長が全従業員の業務日誌を見ることが可能であることに加え、古くから業務日誌を運用してきたため、結果として、業務日誌を秘密情報管理という観点からも有効に利用できているようであった。

【労務管理に係る取組（ヒアリング調査結果)】

・ 社内ネットワーク上で、ウイルス検出のソフトは導入している一方で、社員の不正を検知・モニタリングするような仕組みはない。従業員には入社時および退社時に秘密保持誓約書にサインさせているが、秘密情報を事細かに指定しているわけではないので、実際にどこまで効力があるのかは分からない。（製造業）
・ 秘密保持誓約書には退職後の秘密保持条項に加えて、在職中に取得した秘密情報の返還規定

なども含まれている他、競業避止義務規定も盛り込まれている（期間は２年間）。過去に従業員が過失で機密文書を社外に置き忘れてきてしまったことがある。その際、当該文書の印刷・コピー記録から持ち出した従業員を特定し、本来持ち出しが禁止されている文書を持ちだしたことについては注意を行った。（製造業）

- 社内ネットワーク上で、社員の不正を検知する目的でモニタリングするようなことは実施していない。従業員には入社時に秘密保持誓約書にサインさせている。入社時にサインさせている誓約書で退社時もカバーしているつもりであり、退社時に改めて誓約書にサインをさせることはしていない。現状の誓約書で、実際にどこまで秘密情報保持の義務をカバーできているのかは不明なところである。（製造業）
- 社員に対する秘密保持誓約書や退社時の競業避止誓約書は提出してもらっている。運用を開始して間もないため、全社員が対象となっていない部分は課題であると認識している。転職する同業他社も国内にはないため、社員に蓄積された技術的なノウハウが流出する点は、現時点は懸念材料となっていない。退社後のモニタリングも未実施となっている。（製造業）
- 従業員には秘密保持誓約書にサインさせている。入社時誓約書はかなり前から運用していたが、退職時の誓約書は 2010 年に営業秘密管理規程を整備した際に導入した。内容については顧問弁護士に相談し、ひな型を提供してもらい、これを微調整して運用している。社内ネットワーク上の監視ソフトは導入しており、社外メールやサーバアクセスは記録を取っている。全てを見ている訳ではないが、不審な点があれば調査出来る。退職予定者が出た際には、社長が直接不審な点が無いかチェックを行ったこともある。（製造業）

【特徴的な取組】

- 秘密保持契約の当事者、守秘義務を負っている情報の内容などについて契約管理システムを導入してシステム管理を行っている。（製造業）
- 社長を含む全役職員は毎日業務日報を書いている。業務日報はプリントアウトされ回覧しており、副社長は全員分を必ず毎日読んでいる他、社長もほとんど全てに目を通している。また部門長も当該部門の従業員の日報は毎日読んでいる。これは創業当時からやっているが、社内の情報共有を促進すると同時に、従業員自身や業務上の異常に直ぐに気づくことが出来るというメリットがある。いつもと様子の違う従業員の変化もすぐに分かるため、声掛けをするなどして状況も把握できる。この取組は、社内には情報をオープンにしつつ、社外秘情報は漏えいさせないというプラクティスを支えるものだと思われる。（製造業）

（５）取引先管理

ヒアリング調査の結果、取引先との契約書に、秘密保持条項を盛り込むことは比較的実施されていたが、多くの中小企業が長年の信頼関係を重視している中、最低限度の対応に留まっている例が多かった。特に、長年の信頼関係を壊したくないという意識から、秘密情報管理について取引先に対して踏み込んだ調査や依頼を行えていないことが多かった。

他方、特徴的な取組としては、ISO を取得している中小企業におけるプラクティスとして、ISO の要求事項に従い、取引の相手方に対して必要な調査や監査を実施しているという企業もあった。

【取引先管理に係る取組（ヒアリング調査結果)】

- 外部委託先は長い付き合いの会社が多く、その会社の中で適切に秘密情報が管理されているかどうかを調査したことはない。懇意にしている委託先ばかりなので、急に情報管理体制の調査をした場合に、「疑っている」というようなニュアンスで受け取られてしまうことに懸念があるため、国からの要請や法的な求めでない限りはやりにくい部分はある。一方で、中国の企業に廉価版の製品の製造を委託するケースがあるのだが、その際にはしっかり契約書の中でカバーするようにはしている。(製造業)
- 外部委託先は３社あり、競合他社に対して情報を開示しないことなどを求める秘密保持契約書を締結しているが、当該会社の中でどのような情報管理が行われているかまでは調査していない。これまでに外部委託先から情報が漏れたことがないということもあるが、あまり細かい調査を依頼するのは取引上躊躇してしまう面もあり、担当者個人を信用するしかないと思っている。(製造業)
- 取引先を通じた情報漏えい、技術流出の対策について、機密性の高い情報を集中管理することで対応している。下請企業などに対して必要に応じて守秘義務誓約書を出してもらうようにしている。(製造業)
- 外部委託先は創業当時からの取引先に絞っているが、営業秘密管理体制のレベル感には多少のムラがある（営業秘密管理規程をもっているのは３社中、１社である)。しかし全ての会社が ISO は取得しており、当社が機密情報である明示して提供した情報はそれなりに管理してくれている。(製造業)

【特徴的な取組】

ISO の規程に沿って定期的に監査を実施し、情報管理体制をチェックしている。(製造業)

（６）グローバル拠点の管理

ヒアリング調査の結果、海外に子会社を持っている中小企業では、現地の実状に応じた秘密情報の管理を進め、国内とは異なるルールを設けている例があった。

また、特徴的な取組として、輸出入に際して情報漏えいを防止する観点から、自社で通関手続を行い、相手国の税関職員とも情報開示を最小限の範囲とするための交渉を行うなど、秘密情報の漏えい防止に取り組んでいるプラクティスも見られた。

【グローバル拠点管理の取組（ヒアリング調査結果)】

- タイにも独立資本による子会社を設置しており、日本国内よりも水準の高い安全管理を行っ

ている（守衛を立たせているなど)。海外の方が高水準である理由は、現地の水準に合わせるため。国内では「性善説」で対応できる部分が、海外では通用しない。(製造業)

・ 中国に卸子会社を持っているが、基本的に模倣品が出現してもダメージの少ない、古いタイプの製品のみを扱わせている。多くの製品は日本で製造し、輸出することになるが（輸出が6割を占める)、近年化学品規制が周辺国では厳しくなっており、税関において配合されている物質の構成を正確に開示することが求められるようになっており、営業秘密の漏えいが危惧されている。(製造業)

【特徴的な取組】

・ 商社経由で税関に書類を出すと、商社に対しても配合されている物質の構成を伝える必要が生じ、情報漏えいリスクが高いことから、通関は全て自社で行っている。相手国税関職員次第ではあるが、自社にとっての営業秘密であり、秘密を厳守するように明示しながら相手の要求に対応している。不正アクセスがあれば、最後の砦はパスワードとなるので、この点も徹底するように呼びかけてはいる。(製造業)

Ⅲ．米国企業における秘密情報管理の実態

米国における有識者に対するヒアリングから、米国においても情報漏えいや技術流出の問題は、この数年間で急速に注目されるようになったテーマであり、「どこの会社においても、現在実施している対策には改善の余地があると認識している」という声が聞かれた。米国企業においても試行錯誤しながら本テーマに取り組んでいるというのが実態であると分かった。

試行錯誤の結果到達したプラクティスの数々は、日本において試行錯誤する企業にとっても大いに参考となる。

１．米国企業における秘密情報管理の考え方

（１）米国企業における秘密情報管理の捉え方

有識者ヒアリングの結果、米国企業における「秘密情報管理は、リスクマネジメントの一環として行われていることが多い」との指摘が得られた。すなわち、米国では、秘密情報管理ないし情報セキュリティを、全社的な内部統制のフレームワーク又はリスクマネジメントのフレームワークの一部として位置づけているというプラクティスが業種や規模を問わず行われているとのことである。

【秘密情報管理に対する企業内での考え方（ヒアリング調査結果）】

- 秘密情報管理は、リスクマネジメントの一環として行われていることが多い。所管部としては、法務部門などが所管している会社が多いようだが、これは会社によって異なる。（有識者）
- 情報漏えい対策に係るマネジメントは内部統制ないしリスクマネジメントの仕組みに組み込まれている。（製造業）
- 情報セキュリティは内部管理体制の一部である。（製造業）
- 秘密情報管理については、内部統制ないしリスクマネジメントの仕組みの中にビルトインされている。（非製造業）
- 情報セキュリティ対策は、リスクマネジメントの仕組みにビルトインされており、情報漏えいないし技術漏えいは非常に重要なリスク類型であると考えている。（非製造業）
- 内部統制ないし全社的なリスクマネジメントの仕組みの中に、会社の仕組みとして情報漏えい、技術流出対策が組み込まれているとは言えない。（製造業）
- 情報漏えい、技術流出は、内部統制ないしリスクマネジメントの仕組みにビルトインされている。事実、情報セキュリティのフレームワークは、リスクマネジメントシステムの一環である。（製造業）
- リスクマネジメントは、潜在的なリスクを発見し、リスクが顕在化する前に訴訟の準備をすることもその視野に含まれている。（製造業）
- 情報漏えいの対策は、リスクマネジメントシステムに組み込まれている。会社の方針や行動

について、リスクアセスメント及びリスクマネジメントの観点からレビューを行う際、情報漏えいリスクについては、当社の財務上のリスクエクスポージャー[26]を含めたリスク全体を対象とし、これらエクスポージャーを管理、監視する仕組み、プロセスを見直している。（非製造業）

日本企業においては、プライバシーマークや ISMS といった第三者認証機関が存在するマネジメントシステムを参考としたリスクマネジメント体制を構築している企業が多く見られるが、米国においては必ずしもこうした国際標準が参照されている訳ではないことが有識者から指摘された。

【リスクマネジメントのフレームに対する考え方（ヒアリング調査結果）】

- 情報漏えい対策は、リスクマネジメントの一環であることは認識されている。例えばリスクマネジメントないし内部統制のフレームについては、ISO31000（リスクマネジメント）や ISO27001（情報セキュリティ）といった国際標準も整備されているが、米国ではこれらのフレームが参照されることはそれほど一般的ではない。例えば COSO[27]の ERM フレーム[28]も含め、全社リスク管理についての汎用モデルは他にも多く存在し、普及しているため、ISO ばかりに目が行く訳ではない。（有識者）

（２）秘密情報管理の社内における位置づけ

複数の米国企業のアンケート回答から、情報漏えいリスクについては、経営者の認識も含めて基本的に高いリスク類型であると認識されていることがうかがえた。もっとも、リスク類型として特別視されている訳ではないようであり、他の様々なリスクと一体的に考えているプラクティスが散見された。

【情報漏えいリスクの位置づけ（ヒアリング調査結果）】

- 経営陣は情報漏えいリスクに対して高い意識を持っている。（製造業）
- 情報漏えいリスクは、市場リスクなどと同等のリスクと位置付けている。（製造業）
- 情報漏えいリスクは、高いリスクのある類型として取り扱われている。（製造業）

[26] リスクマネジメント用語であり、リスクファクターが顕在化した場合における、当該リスクファクターのリスク感応度（具体的にどの程度の経済的な損失が発生しうるかなど）を指す。
[27] 米国のトレッドウェイ委員会支援組織委員会（The Committee of Sponsoring Organizations of the Treadway Commission）の略称。
[28] COSO は、内部統制（Internal Control）の標準的なフレームとなっている全社的なリスクマネジメント（Enterprise Risk Management）のフレームを示している。

- 経営陣は、情報漏えいないし技術漏えいについて、他のリスク類型と並ぶ重大なリスクであると捉えている。特に顧客情報の漏えいを気にしている。（非製造業）
- 情報漏えいは、従業員の安全配慮や企業倫理と同等の問題として認識されている。（製造業）
- 経営者の認識は高いと思われるが、個人情報保護に対する意識の方が高いリスクとして認識されている感がある。（製造業）
- 情報漏えいは、オペレーションの停止、あるいは、市場での利点を失うことに繋がることから重大な関心事である。（製造業）
- 経営陣は、情報漏えい、技術流出リスクを強く認識しているが、米国においてこうしたリスクが顕在化したことはこれまでのところない。（製造業）
- 技術流出も懸念はあるが、販売価格情報の方が技術情報それ自体より、この業界では貴重である。そのような情報が漏えいした場合、同社は、著しい損害を生じることになると予想している。（製造業）
- 技術系企業において技術流出リスクの重要性は高い。（有識者）
- 経営者は情報漏えい、技術流出について、重大なリスクであると認識している。（有識者）
- 経営陣は情報漏えいリスクを他のリスクカテゴリと比べて特段重大なリスクとして認識している訳ではない。経営陣が秘密情報の不正流用に対する保護を重視する一方、実際、会社が秘密情報の不正利用によるデータ漏えいにあった場合、これらの問題が世間の注目を浴びることが一般的に考えられる。（有識者）
- 情報漏えいリスクが他のリスクと比べて特に高いリスクであると考えている訳ではない。（非製造業）

また、有識者から、近年は人を通じた情報漏えいないし技術流出が米国でも問題となっており、人事部門が秘密情報管理のトピックにコミットしている企業が増えているとのコメントも得られた。人を通じた情報漏えいないし技術流出に係る課題を会社の経営上の課題として認識しやすくしている可能性として、米国における人事部門長は、上級執行役であることが一般的であることが示唆された。

【情報漏洩対策への人事部のコミット（ヒアリング調査結果）】

- 特に人事部が大きくコミットして取り組んでいる企業が多い。近年では、従業員や元・従業員を介した漏えいが大きなインパクトを持っている。アクセス権などをいくらシステム上で制限しても、アクセス権を持っている人間が秘密を漏えいさせることは防ぎようがなく、漏えいが発生しにくい人事制度上の環境整備や、入社時、退職時の面接によるフォローなど、人事部の所掌業務として実施されている。当然、法務部や情報セキュリティ部門とも緊密な連携がとられている。（有識者）
- 人事部のヘッドは上級役員であることが多く、取締役会や執行役員会のメンバーとなっていることも多く、企業のトップマネジメントとも直結していることが多いため、全社の経営上の課題として認識もされやすくなる。例えば、退職者に対して人事との面接を実施し

（Executive interview）、退職後の秘密情報漏えい防止のための心構えなどを伝えることを制度化している企業も多い。（有識者）

２． 秘密情報管理に係る体制

（１）組織体制の実態

ヒアリング調査によると、米国企業においては、秘密情報管理ないし情報セキュリティを、全社的な内部統制のフレームワーク又はリスクマネジメントのフレームワークの一部として位置づけている例が多く見られることからも、経営マターとされていることが多いと考えられる。今回実施したヒアリング調査の中では、秘密情報管理をコンプライアンスの領域で捉えていることを示唆する複数の有識者からのコメントが得られた。

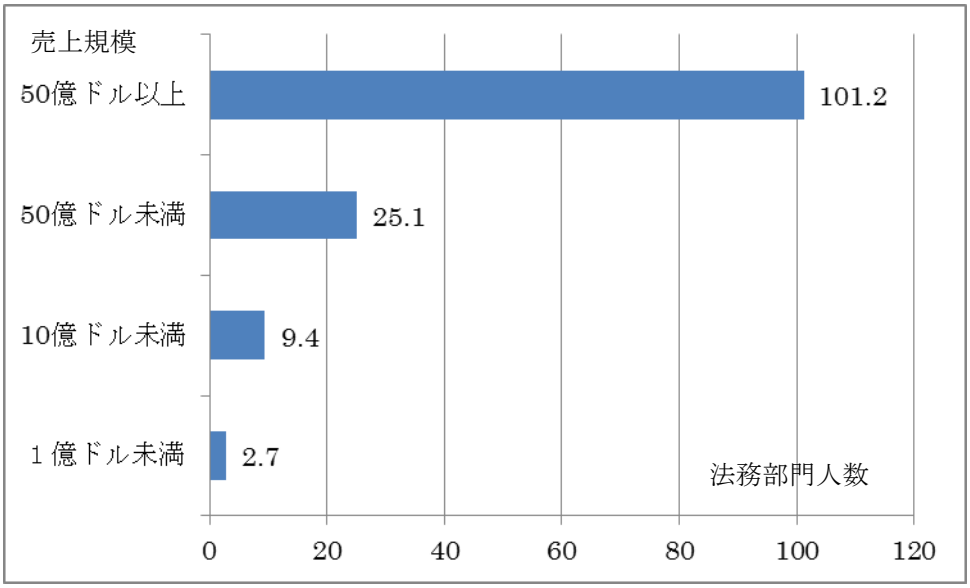
【秘密情報管理に係る組織体制（ヒアリング調査結果）】

- 米国では秘密情報はコンプライアンスの観点からどのようにマネジメントするかという上位概念の下で管理されるケースが多く、そのような場合は顧客へ提供する価値に対する意識や品質管理、リスク管理といった観点との親和性も高くなり、俯瞰的なマネジメントが可能となる。（有識者）
- 情報漏えい、技術流出については、一義的には法務部門長が責任を負う。（製造業）
- 多くの場合、コンプライアンス部門のトップは取締役会に報告する責任を持つチーフ・コンプライアンス・オフィサーが務める。（有識者）
- 法務部門には経験豊富な弁護士を置いている。日本企業の法務部門には弁護士が配置されておらず、日本企業の法務部門と法律問題で協議する際に難しい場面に直面したことがある。（製造業）
- ヘルスケアサービス提供事業者の大半は、情報セキュリティ責任者と個人情報保護管理責任者を配置している。事業者によるが、当該責任者はチーフ・コンプライアンス・オフィサーや CEO から直接の指示を受けて行動する。（有識者）

一般論として、訴訟社会である米国においては、コンプライアンス部門ないし法務部門の位置づけが日本におけるそれよりも高いと言える。例えば、表５のとおり、米国において実施された法務部門の実態調査（サンプル企業は 70 社）によれば、年間売上が 50 億ドルを超える企業の法務部門は平均で 101.2 名の人員規模であり、そのうち 49.2 名が社内弁護士とのことである[29]。有識者ヒアリングによれば、法務部門のトップは上級執行役員が担っているケースが多く、当該上級執行役員は取締役会メンバーとなっていることも少なくないなど、経営レベルの目線をもって役割を果たしていることが多いとのことであった。

[29] ALM Legal Intelligence, Law Department Metrics Benchmarking Survey 2013 (Sponsored by LexisNexis) 参照。

表 5：米国企業の売上規模別に見た法務部門人員数



（出所）ALM Legal Intelligence, Law Department Metrics Benchmarking Survey 2013 (Sponsored by LexisNexis)掲載データより作成

また、CEO や COO の指示で情報システム部門のトップ（Chief Information Officer：CIO）が情報漏えい、技術流出対策全般について管理責任を負っているケースや、製造業における技術情報については、技術部門のトップ（Chief Technical Officer：CTO）が管理責任を負っているプラクティスも見られた。

【秘密情報管理責任者の設置例（ヒアリング調査結果）】

・ 情報漏えい、技術流出対策について、CEO は COO や CIO に権限を委譲し、管理させるのが一般的である。（有識者）
・ 技術情報は、最高技術責任者（CTO）が管理責任を負っている。（製造業）

（２）関連規程の整備実態

関連規程の整備状況については、社外コンサルタントなども活用しながら、経営層を巻き込んで上位のリスク管理ポリシーを策定することが比較的広く行われているとの有識者のコメントがあった。また、全社的な行動規範を策定し、その中に秘密情報管理に関連する規定も入れ込み、年１回という頻度で行動規範を見直しているというプラクティスも見られた。

【関連規程の整備（ヒアリング調査結果）】

・ リスク管理ポリシーについても米国では、外部のコンサルタントなども活用しながら独自に策

定することが少なくない。ポリシー策定段階で経営層や関係者を巻き込んで、秘密情報漏えい対策の意義や重要性を浸透させていくということもある。（有識者）
- 業務行動規範という、業務上遵守すべき行動規範の中に、情報の適切管理のための項目も定められている。この文書は、業界の状況やICT環境の変化を踏まえて、内容が毎年更新される。（非製造業）

また、どのようなレベルの規程を定めることが一般的であるかについて、有識者からは、次のような8類型程度のポリシーや規則を定めることが多いというコメントが得られた。

【秘密情報管理の関連規程の一般的な整理例（ヒアリング調査結果）】

- 一般的な秘密情報管理に係る規程に定められる事項を分類すると、（1）認可事項を管理するポリシーや規則の策定、秘密事項にアクセス権がある労働者の監督、（2）秘密情報へのアクセス権を規制するポリシーや規則の策定、（3）秘密情報へのアクセス権の終了を規制するポリシーや規則の策定、(4)セキュリティ意識と教育を管理するポリシーや規則の策定、(5)セキュリティ・インシデントレポートを管理するポリシーや規則の策定、（6）偶発事故や緊急対応を規制するポリシーや規則の策定、（7）定期的な評価を管理するポリシーや規則の策定、(8) データの第三者提供に関して規制するポリシーや手順の策定、などに整理できる。（有識者）

情報システムに関連した規程については、例えば、以下のような事項についてまで規程の中で明確に定めているといったプラクティスも見られた。

【情報システム関連規程の例（ヒアリング調査結果）】

- 従業員個人所有の電子機器持ち込みについての適切な規制、適切なクラウドポリシーの策定・実施、コアとなる知的財産権の特定、ログイン情報の継続的監視、リモートアクセスの制限、退職とともにアカウントを即時削除することなどを定めている。（製造業）

近年、日本企業においても問題意識が高まっているSNSの利用について、ヒアリング調査の結果、SNS利用についての指針を策定し、行動監視を行っている米国企業のプラクティスも見られた。

一方、グローバルな米国企業ながらSNSについては特段ルールや監視を行っていないというプラクティスも見られた。もっとも、従業員は不正や情報漏えいの事実があれば即解雇されるという認識を持っており、厳格なエンフォースメントを前提とした運用となっているようである。

【SNS 利用に対する管理の例（ヒアリング調査結果）】

・　近年では従業員による SNS の利用について指針を管理し、行動を監視する専門のチームが設置されている。（非製造業）
・　SNS の使用に関する内規はなく、監視も行われていない。どこに出張しているか、といった情報は営業上機微情報にあたるが、そのような情報を流出させたことが発覚した場合に解雇されうるリスクを従業員は認識している。（製造業）

また、多数の事業部を有する企業において、事業部門や地域による差異を許容し、敢えて全社統一的な規程体系を設けていないというプラクティスも見られた。

【部署や地域に応じた規程の設置例（ヒアリング調査結果）】

・　具体的な規程については、部署ごとに、対応する事業領域や地域に応じた規程を作って運用している。製品やサービスの性格によって必要な保護レベルも変わり、また、地域別で法体系も異なるので、情報管理について全社で一貫した基準は設定できない。（非製造業）

（3）情報区分の考え方

有識者に対するヒアリングによると、情報区分に応じた管理というのは、米国においても比較的広く行われているとのことであるが、米国企業に対するヒアリング調査においても、複数の米国企業において情報区分を前提とした管理を行っているプラクティスが見られた。

【情報区分の考え方（ヒアリング調査結果)】

- 情報の内容によってラベリングも実施している。(製造業)
- 文書管理規定の中で、作成者が文書保存時に作成者自身が情報の重要度に応じた秘密分類を施すことを要求し、当該ルールを適切に遵守させることで、上記の情報の保護分類を漏れ無く行うプロセスを導入している。(製造業)
- 情報の重要性に基づいた秘密管理を行っている。顧客情報の管理については、高い顧客からの信頼を前提に事業が成り立っているため、特に注意深く取り扱っている。(非製造業)
- 秘密情報区分は行われている。基本的には法務部門が区分を決定するが、部門によって独自にこれを設定する場合がある。秘密情報は区分毎にそれぞれ異なる取扱がなされる。(製造業)
- 情報の性質による区分は行っている。(非製造業)
- 情報の重要度に応じて秘密情報を区分することは一般的である。(有識者)
- Restricted/Confidential/Internal/Public の 4 段階に分かれており、Restricted/Confidential 情報は、原則として持ち出し禁止としている。また上位区分の情報を取り扱う媒体は Locked storage に保管され、アクセスキーなどは必要な人のみにしか与えられない。またこれら秘密情報を外部とやりとりする際には暗号化を施し、VPN[30]経由で送付させている。(製造業)

一般的な情報区分の考え方に加えて、情報漏えいの企業業績などに対する影響度といった観点から秘密情報の管理区分を設定しているプラクティスも見られた。これは情報漏えいリスクのアセスメント（評価）を前提としており、相対的に高度な管理が行われているプラクティスと言える。

【漏えいの影響度に応じて情報区分を設定している例（ヒアリング調査結果)】

- 秘密情報に関わる関係者及び情報漏えいの影響度によって秘密情報の管理区分を設定している。秘密情報の区分は、情報の重要度だけで区分、判断される訳ではなく、どのような影響を及ぼす可能性があるか、誰が当該情報の最新情報を共有する必要があるのかといった点を考慮する必要がある。(製造業)

[30] Virtual Private Network の略称。通信の暗号化や通信制御によって、仮想的な専用回線を提供するものである。

一方、秘密情報については特段の区分を行わず、全て高いレベルでの管理を行っているというヒアリング調査の回答も見られた。この場合、個々の秘密情報の内容には目が届いていない可能性が高いことから、情報漏えいリスクのアセスメントについても実施できていない可能性が高い。

【秘密情報の重要度などに応じた区分を設定していない例（ヒアリング調査結果）】

- 秘密情報は、重要度の高いレベルに分類される。ひとたび機密として分類された情報は、直ちに重要レベルに置かれる。秘密情報の重要度に応じた区分は行っておらず、全ての秘密情報についての重要性や取扱手順は、同じレベルとなっている。（非製造業）
- 全ての秘密情報が高度な機密として管理されており、管理レベルに特段の違いを設けていない。（製造業）

情報の区分について現場の個別判断を尊重し、これに委ねているというヒアリング調査への回答も見られた他、秘密情報の管理区分を設けていないというヒアリング調査への回答も見られた。

【秘密情報区分の取り決めが存在しない例（ヒアリング調査結果）】

- 秘密／機密情報の定型化された区分はない。いかなる秘密区分指定も個別に行われる。（製造業）
- 情報区分によって管理は異なる。基本的には社内で管理が行われるが、中には第三者的な機関によって管理される情報もある。（非製造業）
- 一般に食品業界では、秘密情報の重要性によって情報区分を行っていない。もっとも、自分の顧客企業の場合、情報セキュリティルールというよりも、１つでも機密情報が含まれていれば当該文書全体について厳重な管理を行うという行動を取る。（有識者）
- 情報の重要性に基づいた秘密情報区分は特段設けていない。（製造業）

秘密情報区分や秘密情報管理の仕組みにおいて、法的意味においての「営業秘密（trade secrets）」を意識的に取り扱っているかどうかについてもヒアリングの中で質問を行ったところ、企業秘密の１類型として取り扱うプラクティスと、秘密情報は原則として営業秘密として定義し、管理、保護の対象としているというプラクティスが見られた。

【営業秘密の位置づけ（ヒアリング調査結果）】

- 営業秘密は、会社や業界全体に影響を与えうるもので、企業秘密の１つと位置付けている。（非製造業）
- 営業秘密は、企業秘密の一類型として取り扱っている。（非製造業）
- 営業秘密も企業秘密の一類型と捉えられている。（製造業）

・　秘密情報は営業秘密と定義しており、保護されるべき対象であると認識している。（製造業） ・　営業秘密もまた秘密情報の１つとして区分されることが多い。（有識者）

ヒアリング調査の結果、新製品に係る情報を厳重に取り扱うため、意識的な情報アクセス制御を行い、新製品開発の総責任者が情報の開示範囲を一元的に管理するというプラクティスが見られた。

【新製品情報に係る管理の例（ヒアリング調査結果）】

・　新製品・サービスのリリースに関する情報は特に厳重に管理する。（非製造業） ・　新製品情報の事前流出防止が極めて重視されていることは、規程などに明示されているわけではないが、会社全体の価値として共有されている。（非製造業） ・　新製品の開発の際は、開発の総責任者が情報共有人員の範囲（disclosed members）を決める。発売が発表されるまで、その範囲内の人間しか製品の情報を知りえず、PR 部門や修理・カスタマーサービス担当の部門でさえ直前まで新製品に関して通知されることはない。こうした極端にモジュール化した体制では、R&D における部門間のシナジーは発生しにくいかもしれないが、結果的に情報管理は容易になっているといえる。（非製造業）

３．物理的な管理

（１）情報システムの管理

米国における有識者に対して行ったヒアリングによれば、米国企業では何らかの文書管理ソリューション（ECM）[31]を導入している企業が多く、その理由として民事訴訟における Discovery 制度対策という側面と IT リテラシーの側面があることが指摘された。

主要な情報ベンダーが提供する文書管理ソリューションには、①詳細なアクセス権設定機能と、②監査レポート出力機能があり、情報セキュリティの観点からも有用性の高さが指摘された。アクセス権の設定（①）を用いると、個々のドキュメントに対して様々な権限を設定することが可能となり、例えば、ダウンロード可／不可、参照可／不可、印刷可／不可といった細かいレベルでの権限設定が可能となる。また、監査レポートの出力（②）とは、誰が・いつ・どのドキュメントに・どんな操作を行ったのか、という記録を任意の形式でレポーティングすることが可能となる機能である。例えば、関係のない部署の社員が特定のファイルに頻繁にアクセスしているなどの情報についてのレポーティングが可能となる。情報漏えいの未然検知や事後調査に力を発揮する可能性があるとのことであった。

【文書管理システムの導入例（ヒアリング調査結果)】

- 欧米では当たり前のように ECM が導入されており、文書がファイルサーバで管理されることが少なくなっているのに対して、日本では中小企業での導入状況はごく少数であり、上場企業でも４～５割程度で、いまだにファイルサーバ管理が主流になっている。（有識者）
- ECM 導入状況に関する日本と欧米との差は、IT リテラシーへの意識の差が大きく影響していると思われる。セキュリティに限らず、ビジネスプロセス・リエンジニアリング（BPR）なども含めて全般的に日本の企業への IT への意識は低い。（有識者）
- 米国の大企業では､文書管理のために大規模な ICT システムを導入することが一般的であり、これは秘密情報管理の上でもアドバンテージになっている。特に漏えいの発見に役立つことが多い。（有識者）
- 文書管理システムの導入が進んでいるのは、米国が訴訟社会であることによる。法的措置を取る際の膨大な要求事項に対応するため、日頃から文書の取り扱いについてログやエビデンスを体系的かつ訴訟を意識して集めておく必要があるためである。（有識者）
- Discovery 制度が営業秘密を厳格に管理することのインセンティブとなっていることは間違いない。（有識者）

また、情報システムの管理についてヒアリング調査で尋ねたところ、回答はアクセス権制御に関する回答が中心であり、アクセス権の設定に際しては、当該秘密情報に真にアクセス

[31] 情報ベンダーが提供している文書管理システムは、一般に Enterprise Content Management（ECM）などと呼ばれており、日本においても多数の導入例が見られる。

が必要な者に限定をして権限を付与しているというコメントも複数社から得られた。

【アクセス制限の設定例（ヒアリング調査結果）】

- 従業員の情報アクセスは統制されており、許可された情報のみにアクセスできる。秘密情報は、権限を付与されたメンバーだけでシェアされ（経営陣、ディレクターといったレベルで権限が区別される）、それ以外のメンバーには閲覧出来なように設定されている。（非製造業）
- 高度な重要性を有すると判断されるものについては、徹底した一元管理が図られ、そもそも本社から出さない（門外不出化）ものとされ、場合によっては、外部インターネット環境から隔離させ、ネットワーク経由の不正侵入を未然に防ぐ措置が講じられている。（製造業）
- 情報の部分的開示を徹底している。ある生産設備に従事する従業員について、全工程についての秘密情報へのアクセスを与えないようにしている。（製造業）
- 従業員のグループ毎に適切なアクセス権の設定を行う。（製造業）
- 公開されていない情報はすべて機密情報として扱われ、プロジェクト実施上必要最低限の人数にしか共有されない。（製造業）
- 情報へのアクセスは、必要最低限のことを知る範囲に制限しており、不必要な情報へのアクセスは認めていない。（製造業）
- 情報セキュリティ上、アクセス制限が重要となる。また秘密情報を使用する従業員を監視出来るように、法務部門などに必要な機能を持たせることも重要である。（製造業）
- アクセス制限の方法は、ID カード、指紋認証 ID、レティーナ ID（網膜スキャン認証）などがあるが、多くの企業でレティーナ ID を使い始めている。（有識者）

ヒアリング調査への回答及び有識者へのヒアリングの結果、アクセスログを取っていないという企業は今回見られなかったが、アクセスログのモニタリングについては、実施している企業と実施していない企業があった。また、年 1 回の情報管理に係る研修において、アクセスログを取っていることを従業員に積極的に伝えているというプラクティスも見られた。

【アクセスログの取り扱い例（ヒアリング調査結果）】

- 秘密情報へのアクセス記録は全て履歴を残している。重要文書のファイルが開かれる際、自動的にデータとアクセス時間が記録される。（非製造業）
- 文書全般について、アクセス、ファイルの転送、編集については記録を取っている。（非製造業）
- 暗号化の他、情報へのアクセス記録のモニタリングや情報源に対するトラッキングを行っている。またメールアカウントのパスワード変更などは定期的に行っている。（非製造業）
- アクセス及び編集ログを取っており、アクセスログを取っていることを含め、情報管理について年に 1 回程度研修会を実施している。（製造業）
- アクセスログなどのサンプリング調査は通常は実施していない。当社においては情報を窃取されることよりも、会社製品自体の盗難の方が懸念されている。（製造業）

少し特殊なプラクティスとして、チームメンバー同士の専用コミュニケーションツールの利用を義務付け、コミュニケーション参加者を制限することで漏えい対策としている例が見られた。

【専用コミュニケーションツールの導入例（ヒアリング調査結果)】

・　システム上の漏えい対策として、電子メールなどの使用制限、文書データへのアクセス制限のほか、チームメンバー同士の専用のコミュニケーションツールの利用が義務付けられる場合もある。(非製造業)

また、社外からのサイバー攻撃に対応する専門家や専門部署を設置しているというプラクティスも見られた他、必要に応じてフォレンジックを行うというプラクティスも見られた。

【サイバー攻撃に対する取組（ヒアリング調査結果)】

・　自社内に IT セキュリティ専門家の配置している。また専門家の中には、元 FBI などの官公庁出身者や軍隊／警察出身者も積極的に雇用し、有事の際に迅速に対応できる体制を構築している。(製造業)
・　一般的な社内情報システム部門に加え、外部からのサイバー攻撃に専従的に対応する専門部署が置かれており、脅威の兆候があればアラートを全社に発する機能を担っている。また、インシデント発生時にはフォレンジックも行う。(非製造業)

フォレンジックとは、もともと刑事及び民事手続における証拠収集を指す言葉であったが、電子化が進んだ結果、電子的に保存されている膨大な情報の中から証拠となるものを一定のアルゴリズムを用いて検出する調査手法を指すようになった。米国における訴訟手続（民事においては特に discovery 段階）で頻繁行われる他、不正調査手段としても認知されている。この点、有識者によれば、フォレンジックによって、例えばメールの使用状況、データ消去履歴、削除データ復元、外部機器の接続履歴、インターネットや Web メールの利用履歴、パスワード解析、ソフトウェアインストール履歴、ソフトウェア実行履歴、パソコンの起動履歴、ファイルへのアクセス履歴などが調査可能となり、フォレンジック会社は discovery 制度を前提とした証拠収集・保全や社内調査の一部を請け負っているとのことであった[32]。

[32] 日本でサービスを提供しているフォレンジック会社も複数存在する。米国における訴訟対応に限らず、国内訴訟対応や不正調査を目的として活用されるケースも増えている。

（2）情報機器の管理

情報機器の管理については、日本と特段異なる米国企業独自と言えそうなプラクティスは見当たらなかったが、調査の結果、情報の暗号化や情報機器運用のルール化が意識的に行われていることが分かった。

【情報および情報機器の取り扱い（ヒアリング調査結果）】

- 顧客のパスワードは暗号化して管理する。（非製造業）
- 顧客の支払い処理の暗号化およびロックをすることは徹底させている。また当然、クレジットカード情報を保存（記憶）させないようにしている。（非製造業）
- モバイル端末の取り扱いについては、特段のルールを設定している。（製造業）
- 秘密情報を含む電子媒体は暗号化されている。（製造業）
- ソースコードは安全な収納場所に収納される。（製造業）
- 月１回の頻度でパスワードを更新し、四半期ごとにセキュリティシステムを定期的に検査する。（非製造業）
- 安全が確保されたネットワークに限りログイン出来る。またパソコンなどにはソフトウェアをまめにアップデートすることになっている。（非製造業）
- 秘密情報をネットワークに繋がっていないパソコンでのみ閲覧可能としているケースもある。（有識者）

上記のとおり、日本企業においても USB などの記録メディアの取り扱いについては意識的に行っている企業が散見されたところ、米国でも記録メディアの取り扱いについては特に留意しているプラクティスが見られた。

【記録メディアの取り扱い（ヒアリング調査結果）】

- 記録メディアの管理について、ポリシーを文書で明確化した上、全ての記録メディアを会社で管理している。また記録メディアの利用については全てログを取っており、記録メディアとサーバとの情報のやり取りに不審な点が無いかについても月に１回程度の頻度で監視を行っている。（有識者）

有識者によれば、米国でも個人所有の情報機器の活用が注目されているが、これが可能なのは高度な情報システム上のセキュリティ対策が取れている企業に限られるのが実態であるとのことであった。

【私有機器の利用に係る取組（ヒアリング調査結果）】

- 最近のトレンドとしては、BYOD（Bring Your Own Device）が注目されているが、これは

個人の IT 機器を業務に持ち込むものであるため、そもそもセキュリティ対策が十分になされている前提であることが肝要である。（有識者）
- BYOD によるコスト削減効果を期待する企業もない訳ではないが、端末側のセキュリティ設定、利用するソフトウェアなどをコントロールすることができず、情報漏えい対策や紛失・盗難時の対応が複雑化する。また個人所有の端末を管理する場合には、通信内容などを把握、調査するにしてもプライバシーとの両立が問題となる。（有識者）

（3）紙媒体の管理

紙媒体の管理方法について、ヒアリング調査の回答が得られた。独自のフォーマットを用いて管理しているプラクティス、紙媒体で管理される秘密情報については、極めて限られた人間のみが鍵を持つキャビネットへ保管し、当該情報には法務部門長の許可が無ければアクセス出来ないような運用を行っている例があった。

【紙媒体の管理（ヒアリング調査結果）】

- 紙媒体の資料については、当社のフォーマットで保管される。（製造業）
- 紙媒体の機密情報及び契約書は、全て副社長と法務部門長のみがキーを持つキャビネットに保管しており、その他の者がアクセス出来ないようにしている。また当該情報にアクセスが必要な者は法務部門長の許可が必要となる。（製造業）

秘密情報として管理される紙媒体について、紙媒体の管理が適切であれば、紙媒体は電子的な複製リスクやネットワーク上の拡散リスクが低いことから、あえて電子的なコピーやデータを持たないという運用を行っているプラクティスや、紙媒体を保管するエリアにカメラなどの持ち込みを制限するなど、厳格なゾーニングを行っているプラクティスが見られた。

【紙媒体管理に係る取組例（ヒアリング調査結果）】

- 当該紙媒体については電子的なコピーやデータベースが存在しない。（製造業）
- 紙媒体を保管している場所に、カメラなどを持ち込むことは禁止されており、ビジターの入室は認めていない。（製造業）

これに対して、紙媒体で存在する秘密を全て電子化し、文書管理システムによって所在の把握や管理を行っているプラクティスも見られた。また、有識者からは、電子化された情報についての対策は進んできているが、紙媒体の情報についての漏えいリスクは低減できていないとして、紙媒体のみでの管理を問題視する指摘も聞かれた。

【紙媒体の電子管理および漏えいリスク（ヒアリング調査結果)】

・　紙媒体で存在する企業秘密（例えば契約書、各種証跡、図面など）についても、全て電子化を行った上で、全社的な文書管理システムによって所在の把握や管理が行える状態にある。紙媒体原本についても施錠キャビネや入出制限のされた書庫への保存が徹底され、台帳などによって所在の把握や管理が行える状態を確保している。（有識者）
・　ヘルスケアサービス提供事業者は電子データに関する情報漏えいを検知するシステムを持っているが、紙媒体の情報についての情報漏えいリスクは低減されていない（リスクが高いと思慮している)。（有識者）

（4）施設の管理

ヒアリング調査の結果、従業員の役職や秘密情報を取り扱う部署などへの立ち入りの必要性なども踏まえたゾーニングを行っている企業が散見された。

特徴的な例として、時間帯によって入退室可能なエリアを変えることで業務時間中の負担を軽減しているプラクティスや、R&D 部門を他の部門から明確に区分した上、R&D 部門の中でもセクション別にゾーニングを行っているといったプラクティスも見られた。

ID カードなどによる入退館管理自体には、不審者の侵入を防ぐという物理的な施設セキュリティ手段としての意味ももちろんあるが、当該 ID カード所持者が「アクセス」できる施設領域を制限する手段であり、秘密情報へのアクセス制御手段としても認識されている。

【ゾーニングに係る取組例（ヒアリング調査結果)】

- 部署別のフロアへの入退室はセキュリティカードで制限されている。ミーティングの必要性などから、管理部門の人間であれば他部署に入出できるが、勤務時間外になれば違う部署に入れなくなるなど、時間帯によっても異なる管理が行われている。(製造業)
- 時間帯問わず、R&D 部署のフロアには他部署のセキュリティカードでは入れない。また、R&D 部署の中でも、セクション別に入退室が管理されており、行き来はできない。(製造業)
- ゾーニングを行っており、部外者立入禁止フロアが設定されている。(製造業)
- 従業員に対しては、契約による管理やゾーニング、システム上のアクセス権制限などの対策といった管理施策を一通り講じている。管理のレベルには部署や従業員の職種に応じた違いがある。(非製造業)
- 物理的なアクセス制限（施錠による入退室管理によるゾーニング、文書の厳格な閲覧制限など）を実施している。(非製造業)
- 重要な書類や顧客情報を扱っている部署には監視カメラも導入している。(非製造業)
- オフィスでの工夫としては、ID カードによる入退室管理、秘密情報に配慮した個室形態の会議室の確保・利用、セキュリティ講習会への出席などである。(非製造業)
- オフィスへの入退室に際しては、ID カードによるアクセス管理を行っている。(非製造業)
- 施設管理やオフィスレイアウトは情報セキュリティ上重要な要素である。(有識者)
- 企業秘密の中でも特に漏えいした場合のリスクが高いものについては特定の施設領域でしか扱うことができず（ゾーニングを実施)、当該領域では、廊下も含めた監視カメラの設置、ID カードなどによるアクセスの厳格な制限（入室できる人を最小化)、当該領域内からの外部との通信の禁止を徹底している。(有識者)
- ID カードによる入退館管理は標準的に実施されている。(有識者)

オフィスレイアウト（机の配置や動線の取り方、パソコン画面の設置方法など）において、情報漏えいなど不正を防止する観点を取り入れているかについては、死角ができないようなレイアウトを設計し、情報セキュリティにも配慮しているプラクティスが見られた。一方で、

特段の工夫はしていないというプラクティスも見られた。

【オフィスレイアウトに係る工夫例（ヒアリング調査結果)】

・　オフィスエリアは施錠管理されている。特定の場所への入退室についてアクセス制限がなされているが、フロアレイアウトを設計する際には情報セキュリティを必ずしも意識している訳ではない。(製造業)
・　オフィスレイアウトについては、死角が出来ないようにレイアウトされており、情報セキュリティに配慮したフロアプランとなっている。(製造業)
・　特にオフィスレイアウト上の工夫はしていない。(非製造業)
・　自分の知る限り、秘密情報漏えい対策の観点からオフィスレイアウトを工夫している例はない。(有識者)
・　小規模な事業所であるため、フロアレイアウトが見渡せるため、不正を働きにくい。(製造業)

４．労務管理

（１）従業員の採用

米国における有識者によれば、米国では従業員の雇用に際して、犯罪歴・逮捕歴の確認を含む身元確認を行うことが一般的とのことであり、実際、ヒアリング調査に回答を得た複数の企業において身元確認のプラクティスが確認された。もっとも、米国においても、雇用における差別的な取扱いについては厳格な規制に服しており、連邦政府には Equal Employment Opportunity Commission (EEOC)と呼ばれる規制当局が存在している[33]。この点、差別的取扱いとは別に、身上調査を行うこと自体については連邦レベルでは禁止されていないが、州レベルでは、犯罪歴・逮捕歴に係る質問を採用時に尋ねることなどを制限する立法例が近年散見される点には留意を要する。また、雇用に際し犯罪歴・逮捕歴などを含む身上調査を採用時の判断材料とする場合には、その旨を対象者に伝え、文書をもって対象者に身上調査の了解を得ることが必要であるとされている[34]。

また、ヒアリング調査に協力頂いた企業の中には、競合他社からの採用を控えるというポリシーを採用している企業も見られた。

【従業員採用時の取組（ヒアリング調査結果)】

- 新入社員に対しては、身元確認が義務付けられている。(製造業)
- バックグラウンドチェックを可能な限り実施（プライバシー関連法に反しない範囲）している。(製造業)
- 地元の警察による犯罪歴の確認を採用前に要求している。入社時には、身元確認と与信チェックを受ける。自身の場合、身元確認、与信チェックの他、3 つの照会文書を求められた。(非製造業)
- リファレンスと犯罪歴の確認（スクリーニング）は、雇用前に必ず実施している。(非製造業)
- 新しく入社する者については、身元確認や身元照会を行う。(有識者)
- 新人研修と退職者面接は、情報、現社員および元社員に関する従業員の権利と責任を取り扱う。(製造業)
- 入社時には身元確認を行っているが、退職者についてはそれほど厳密なことは行っていない。(製造業)
- 新たに入社する従業員の身元調査結果と元雇用主のリファレンスは、採用時に常に考慮される。例えば、仕事の適正だけで見れば完璧であっても、経理担当者に、過去不払いを起こした経験のある者を採用することはない。(製造業)
- 原則として競合他社からの採用は控えるというポリシーを採用している。(製造業)

[33] EEOC は、2012 年に Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964 という Enforcement Guidance を公表している。(http://www.eeoc.gov/laws/guidance/subject.cfm#retaliation)

[34] Federal Trade Commission（FTC）消費者向け情報サイト参照。
(http://www.consumer.ftc.gov/articles/0157-employment-background-checks)

（2）従業員との契約締結

ヒアリング調査の結果、新しく入社する従業員に対して、個別の秘密保持契約書や誓約書への署名を求めるプラクティスが多かった。中には、一律の秘密保持契約書ではなく、配属される部署によってそれぞれの内容の秘密保持契約書を締結している例も見られた。

【従業員との契約締結に係る取組（ヒアリング調査結果）】

- 全ての従業員は、秘密保持契約書にサインをしている。これによって従業員は義務の内容について認識をする。当社では全ての従業員が秘密保持義務に違反することが、解雇に繋がることを理解している。（製造業）
- 入社時に秘密保持契約を締結するが、秘密の範囲や内容は入社時点では特定されない。（製造業）
- 入社時には秘密保持契約を締結する。もっとも秘密保持条項は、競業避止や勧誘禁止規定なども含む契約に包含されている。（製造業）
- 従業員には NDA を締結させている。顧客情報にアクセスするときや顧客の会社と契約するときには、従業員は契約書にサインすることを求められる。（製造業）
- 全ての従業員という訳ではなく、商品部や経理部など特定の部署に配属される従業員と別途の NDA を締結している。経営陣については、職責とリンクした NDA がある訳ではないが、この点については改善を検討している。（製造業）

前職において課された秘密保持義務に違反していないことなどについても誓約書を徴求しているプラクティスも見られた。また、競業避止契約を入社時から求めるというプラクティスもあるようである。

【前職での秘密保持義務の確認や競業避止契約を求める例（ヒアリング調査結果）】

- 新入社員は秘密保持契約書にサインすることが求められる他、元雇用主に対して転職自体がいかなる秘密保持契約によっても禁止されていないこと、元雇用主の下での秘密情報を一切持っていないこと、持ち込まないことを約束させられる。（有識者）
- 発明譲渡契約や競業避止契約にもサインが求められる。（有識者）
- ほとんどのヘルスケア事業の組織では、雇用契約以外に NDA にサインさせることは一般的ではない。ハイレベルな戦略上の情報が個人によって保持される場合を除き、競合避止義務が個人に課されることも稀である。（有識者）
- 経営陣は、秘密保持義務を含む利益相反禁止誓約書に署名することが求められる。（有識者）

特定のプロジェクトに参加する従業員に対して、プロジェクト参加時に別途、秘密保持契約書や誓約書への署名を求めるケースも少なくなかった。また、当該企業において重要となる秘密情報に接することになるプロジェクトメンバーの意識を常に高くしておくために、特定のプロジェクトに参加した後も、定期的な研修を課している例も見られた。その他、従業員に対して「知らなくて良いことは教えない」という考え方を採用し、不必要な情報には触れさせないようなマネジメントを行っているプラクティスも見られた。

【プロジェクト参加時に秘密保持契約を締結する例（ヒアリング調査結果)】

- 高い秘密管理レベルを求められるプロジェクト参加者は、参加前に秘密保持契約を締結する。（製造業）
- 従業員は、利益相反、新規顧客および退職に関連した、新しいプロジェクトに加わる前に、非開示のステートメント（陳述書）にサインする必要がある。またプロジェクトに参加した後も、定期的に研修を実施している。(非製造業)
- Need to know の原則に基づき、プロジェクト遂行上触れることになる情報はすべて秘密として扱うことを求められる。ただし、プロジェクトに入る際も個別に誓約書をとることはしない。(製造業)
- 作業開始前に、従業員は NDA に署名する。(製造業)
- 会社の秘密情報や知的財産にアクセス可能な従業員に対して専有情報契約及び発明譲渡契約の締結を求めることが通常である。（有識者）
- どのような場合であれ、原則として秘密情報に接触する人数は最小化するようなマネジメントがなされるが、情報管理の厳格さは、事業に進捗段階に応じても濃淡をつける。例えば、ある製品を開発するプロジェクトにおいて、R&D の段階では、技術情報に触れる人数は極めて限定され、従業員や共同開発企業と個別に契約を締結することで管理される。製品が市場投入に近づき、営業準備やマーケティングの段階になると製品情報に触れる人間の数が増えるので、アクセス権のコントロールや個別の契約といった方法の効果は薄くなる。また、製品に付随するサービスやアプリケーションを開発する際には、第三者のベンダーと共同してプロジェクトを進めることになる。さらに、リリース直前には外部のモニターからのプレビューを取り入れることも行う。こうした段階でも、秘密保持契約は締結される一方で、契約において特定されている以上に厳格な情報管理行動が望まれる。そこで、社外も含めた秘密情報管理文化の醸成が重要になる。(非製造業)

（3）従業員に対するエンフォースメント

ヒアリング調査においても見られたように秘密保持義務に違反する行為はもちろん、社内規程から逸脱した行為が続けば米国企業は厳しい態度で臨むのが一般的であり、ヒアリング調査で回答を得られた企業においても悪意による秘密保持義務違反があれば即解雇に相当するという運用が行われている企業もあった。従業員による法的な義務違反に対して、訴訟提

起を行うことも躊躇わないという姿勢も明確である企業が多かった。

また、警告を行う場合についても、警告を発するだけでなく、警告を受けた従業員に対して特別な研修やカウンセリングを行うというプラクティスも見られた。単に警告を行うよりも改善を促す効果が期待される取組であると考えられる。その他、従業員同士による相互監視を１つの手段として取り入れているというプラクティスも見られた。

【エンフォースメントの実態（ヒアリング調査結果)】

- 監視活動の結果、警告が複数回に及べば、当該従業員は解雇される可能性もある（程度は考慮される）。なお、警告を受けた従業員は、機密書類の扱い方について研修を受けなければならない。（製造業）
- 違反の程度によって適切な制裁措置を取る。（製造業）
- 情報漏えいに関与した従業員に対しては降格といった処分の他、必要があれば訴訟提起も行っている。（非製造業）
- 雇用期間中に秘密保持義務違反があった場合、当社は当該違反者に対して法的措置を講じるために法的助言を求める権利がある。（非製造業）
- 会社は契約上の権利を有しており、必要に応じてこれを行使する。軽率な過失による行動について警告が与えられることがあるが、悪意のある違反については即座に解雇の対象となる。（有識者）
- 従業員は秘密情報の漏えいなどによって解雇されることがある。また情報漏えいによる損害の程度に応じて、訴訟費用の負担を求める場合がある。（非製造業）
- 秘密保持義務に違反した従業員は、刑事的な処分の対象となる。多くのヘルスケア関連企業においては、情報セキュリティ・ポリシーおよび規則の違反に対して先進的な懲戒処分プロセスがある。一般に情報セキュリティ・ポリシーは、規則違反の性質によっては解雇となることが明らかにされている。（有識者）
- 情報漏えいを行った従業員に対しては、解雇、報酬減額がなされる。（有識者）
- 行動が故意で継続した場合、カウンセリングや教育を実施、必要に応じて雇用契約を解除する。（製造業）
- 雇用契約ないし社内ルールに違反すれば、懲戒の対象となり得る。（製造業）
- 情報漏えいに従業員が関われば、会社として必要な警告を発したり、当該従業員を解雇することもある。（製造業）
- 情報漏えいを未然に防ぐ観点から、全従業員に対して秘密情報を厳格に保持することを義務付けている。当社では従業員が相互監視を行っており、故意または過失で情報漏えいをしていることを発見すれば、雇用契約終了事由ともなる。日本においては懲戒としての解雇のハードルが高いと聞いているが、情報漏えいに対しては会社を守るために厳しく対応していくことが必要である。信頼出来る人間を雇用し、信頼を失うような行動をした従業員は解雇するということが、会社は情報漏えいやその他の不正から守ることに繋がると考えている。その意味でエンフォースメントは厳格にしており、違反者に対しては厳しい制裁措置を講じている。具体的には、深刻な問題があれば降格などの中途半場な措置ではなく、解雇という措

置を講じており、基準は明確にしている。情報漏えいを予防（拡大予防）に非協力的な従業員に対して民事訴訟を提起する割合は２割程度である。（製造業）
・ 機密情報を流出させれば即解雇されるというリスクは広く認識されており、従業員の多くは注意深く行動していると思われる。実際にミスによる解雇事例はあるようだが、情報流出による解雇事例が全社でシステマティックに共有されているわけではない。（製造業）

（４）研修・人材育成

様々な秘密情報管理の前提として、研修を通じて情報漏えいが会社にとって致命的な損害をもたらすものであることを従業員に理解させているという企業もあった。また、同様に、秘密情報管理の重要性を継続的に啓発していくことが重要であるとして、年４回のワークショップで情報漏えいの影響や対策について従業員が討議する機会を設けているというプラクティスも見られた。

【研修実施の取組（ヒアリング調査結果）】

・ 諸施策の中でも、特に研修による意識啓発は、有効かつ重要であると認識している。動機は様々であれ、秘密情報の情報漏えいが会社にとって致命的な損害をもたらすことが理解できれば、適切な行動をするようになるという前提に立っている。（非製造業）
・ 当社は顧客の秘密情報を取り扱うため、継続的に機密保持の重要性を喚起して行くことが重要である。情報漏えいがあった場合に、どのような影響が出るのか、意図しない情報漏えいを防ぐ方法に関するワークショップを年４回実施している。（非製造業）
・ 情報セキュリティに掛かる研修は参加を義務付けている。プロジェクトによっては、当該プロジェクト特有のセキュリティ研修を実施している。（製造業）

しかしながら、秘密情報管理という観点からの意識的に研修を行えておらず、注意喚起に留まっている企業も見られた。また、様々な社内研修などの場面で、秘密情報管理について取り扱うなどの工夫を行っている例が散見された。その他、情報セキュリティチームを対象とした研修プログラムを設けているというプラクティス、正規社員以外のスタッフも研修に参加させているというプラクティス、部門によってプログラムの内容を変えているというプラクティスもあった。

【秘密情報に係る注意喚起や研修の具体例（ヒアリング調査結果）】

・ ルールの遵守状況に関するアンケートや幹部からの注意喚起が定期的に行われている。（製造業）
・ 情報セキュリティなどを主目的とした研修プログラムはない。従業員に対して秘密保持義務の内容について注意喚起をしている程度に留まっている。（製造業）

- 年に１～２回ビデオによる研修プログラムの受講が義務付けられており、そのうち３割程度は情報セキュリティに関わる内容である。内容はグローバルで統一されており、日本用にローカライズされているわけではない。実際に視聴しているかログが記録されており、受講しなかった場合は上司に報告が行く。（製造業）
- 社内の関連規程に関する研修はオンライン上で毎年１回実施され、全役職員に受講の義務がある。（非製造業）
- 企業秘密を取り扱う人は、取扱手順について教育を受ける。またコンプライアンスを確保するためにフォローアップを行っている。（製造業）
- 従業員に与えられた情報へのアクセス権の適切な運用についてプロジェクト/プログラムマネジャーは従業員を教育する。（製造業）
- 機密書類の取り扱いについて、年１回の研修会（参加義務あり）でも取り扱った上で、公共スペースでの会話について監視を行っている。こうした監視情報はセキュリティ部門に報告される。また情報システム上も監視が行われている。（製造業）
- 従業員への研修では、秘密情報アクセスや情報の取り扱い、パスワードのアップデート、情報漏えいによる影響などに関して、常に、注意喚起をしている。（非製造業）
- 部門や役職に応じた異なる内容の訓練、教育も受けている。（非製造業）
- 情報セキュリティチームも、それぞれのトレーニングプログラムに沿って教育・訓練を受ける。（非製造業）
- 本来、定期的に機密保持の重要性や義務について従業員の注意を喚起させる定期的な研修が行われることが望ましいが、多くの企業において実現出来ていない。（有識者）
- 情報の取り扱いについて、定期的な講習会＆ワークショップを実施している。また第三者からの情報セキュリティ対策としての社内指示書（Security company instructions）を出してもらっている。（非製造業）
- 従業員は採用時に研修を受けるが、雇用後も毎年プライバシー啓発プログラムを受講する。また正規の従業員に限らず、ボランティアや学生も研修に参加することが必要である。（有識者）
- 研修については役職に応じて実施しているのではなく、部門によって違いを設けている。人事部門による研修で、情報保護に関するものは年に６回程度まで実施することがある。情報漏えいというよりは独占禁止法対策として、競合他社との交流制限や秘密情報を有する営業部門に対する管理徹底は研修で取り上げられている。また部長級以上は全社的な情報保護についても研修を受ける。（製造業）

また、新入社員（中途採用含め）研修において、情報セキュリティについても重要なテーマと位置づけ、まとまった時間を割いたプログラムを策定しているという企業も見られた。

【新規雇用者に対する研修（ヒアリング調査結果)】

・　新規雇用者は入社時に 2 日間集中的に研修を受講するが、うち 2 時間を割いて、当社における情報管理の重要性とカルチャーを徹底的に学習させる。（非製造業）

（5）退職者に対するフォロー

退職者に対する秘密保持契約や競業避止義務契約については、有識者によれば、「米国においては競業避止契約の有効性が、比較的広く認められており、カリフォルニア州のように法令によって競業避止契約の禁止されている地域などを除けば、実務上も頻繁に用いられている」と指摘されている。

【秘密保持契約や競業避止契約に係る実態（ヒアリング調査結果)】

・　退職者に対しては、通常、秘密保持契約を締結させている。(製造業)
・　離職後、従業員から情報漏えいに対する責任があることを明示した契約にサインをもらい同意を得ている。(非製造業)
・　離職者に対しては、競業避止条項又は秘密保持条項を含む契約を締結する。(非製造業)
・　従業員の退職時、その者のポジションによっては競業避止義務契約にサインを求める。営業部門の場合、競合他社に転職する際にはこの義務を負わせている。この場合、当該営業部門の人間が転職した先に対しても、当該義務の内容を通知している。競業するかどうかについてはしばしば争いとなるが、裁判所は割と早く答えを出す。(製造業)
・　米国においては競業避止契約の有効性が、比較的広く認められており、カリフォルニア州のように法令によって競業避止契約の禁止されている地域などを除けば、実務上も頻繁に用いられている。(有識者)

退職予定者には面談を実施し、秘密保持義務や競業避止義務を含む法的義務などについて必要な注意喚起を実施したり、会社所有の備品と合わせて情報についても返却を求めるといったプラクティスが見られた。

【退職予定者への対応（ヒアリング調査結果)】

・　退職予定者には上位職が個別に面接を実施する。この面接では、の秘密情報の防止を予防するというより、業務の中で知りえた第三者企業の秘密を転職先で流出させたり不正に使用したりすることを予防することに主眼が置かれる。(非製造業)
・　退職予定者については、退職者面接や会社所有の備品や情報などの返還を求める。また退職時には秘密保持契約上の義務について、注意喚起を行う。(有識者)
・　退職面接は必ず実施し、情報の返却を求める。(製造業)
・　面接の際の情報（顔色も含む）は、不正調査を開始するかどうかを判断する上で極めて重要

なプロセスである。(製造業)
- 退職従業員が負担する義務について明確に説明し、遵守を求め、その誓約内容についてサインを取得するよう務めている。(製造業)
- 退社する従業員に、退職者面接で法的な義務を注意喚起しているが、会社は、元従業員を監視はしない。(製造業)
- 退職者に対して秘密保持義務についての注意喚起は行っているが、新しい雇用主に対して何らかの注意喚起や警告は行っておらず、転職後の事後フォローも行われていない。(製造業)
- 離職者に対しては、秘密保持義務について注意喚起が行われる。また可能な限り、新しい雇用主に対して当該従業員の秘密保持義務について通知を行う。(有識者)

また、人事部が退職予定者に対する社内情報へのアクセス権について責任を持ち、退職予定者に対する社内情報へのアクセス権に係る独自のガイドラインを策定しているプラクティスや、離職者に対して離職後も監視を行い、新しい雇用主に対してもコンタクトを取るというプラクティスも見られた。

【退職予定者のアクセス権制御や退職後の監視に係る取組（ヒアリング調査結果)】

- 退職予定者に対する情報アクセス権の制限などについては人事部門が管轄し、独自のガイドラインに従って実施される。(非製造業)
- 離職者に対しては、離職後も監視を行う。さらに、彼らの新しい雇用主とコンタクトをとり、秘密保持などの制限を通知する。業界内の仕事で情報漏えいなどの違反を発見した場合、訴訟を提起する前に警告状を送るのが通常である。(製造業)
- 場合によっては転職先企業に対し、アラートを送付する。(製造業)
- 例えばソフトウェア業界の労働市場は（一般に考えられているよりも）小さなコミュニティであり、転職者の動向に関する情報共有はしやすい。したがって、転職者による競合他社に対する情報漏えいの事案が発生すれば、それは業界全体に比較的容易に知られうるため、社会的な抑止効果がある。(非製造業)

５．取引先管理

（1）パートナー企業との契約

ヒアリング調査の結果、単純な業務のアウトソーシング先から、共同研究先や製造委託先まで、様々なパートナー企業と協働することが不可欠となる中、パートナー企業を通じた情報漏えいないし技術流出に対する懸念が高いため、一般に契約上、取引の相手方に秘密保持義務を負わせるといったプラクティスが米国企業でも、浸透していることが分かった。

【パートナー企業との契約に係る実態（ヒアリング調査結果)】

- 非常に多くのベンダーと共同研究や製造委託を行っている。共同研究先や委託先とは、秘密保持契約を締結するほか、セキュリティ体制を必ず現地でチェックすることになっている。（製造業）
- 取引先が契約に違反すれば、セキュリティ部門に報告される。（製造業）
- 取引先との間でも秘密保持契約が締結される。各社は、秘密保持の対象となる情報の特定や当該情報の受取人の制限といった点に留意する。すなわち、会社が秘密保持契約を前提に受け取る情報が、秘密保持の対象となるかどうかの確認を厳格に行い、秘密保持義務違反を起こさないように当該情報を安全に管理する。（有識者）
- NDA は取引上必要である。特に重要な情報を特定し、これに印をつけ、当該情報へのアクセスを制限するといったこともされている。（有識者）
- 取引先（ディーラー）との契約には NDA が含まれている。特に重要なのは未発売の製品について、下見の権利を与えており、未発売製品に係る情報漏えいを懸念しているからである。（製造業）
- 取引先や顧客と秘密情報を共有することが必要な場合、厳格な秘密保持義務を課さなければ情報を共有することはない。相手を信頼できない場合には、情報は共有されない。（製造業）
- 情報の開示範囲は狭くして草案するようにしている。いずれにしても秘密保持義務を負った者は、違反に対して法的な責任を負うことになる。（製造業）

（2）パートナー企業の選定と調査・監査の実施

パートナー企業に対して秘密保持契約上の義務を遵守させるための措置を行っているプラクティスが見られた他、必要に応じて相手企業に対する調査・監査も実施するなど、積極的な行動によって秘密保持義務の確実な履行を確保しているプラクティスも見られた。

【パートナー企業の選定と調査・監査の実施（ヒアリング調査結果)】

- 協業に先立っては、必ず業務仕様書（Request For Proposal：RFP）を作成し、候補となる企業の情報セキュリティレベルを評価したうえで、選定を行う。（非製造業）

- 契約条項の整備のみならず、当該契約条項の執行、警告、訴訟対応を含め、徹底化が図られている。（有識者）
- 取引先に係る契約書は、文書管理システムによって管理・保管されることが一般的で、契約終了日と合わせて遵守状況が監視される。（有識者）
- 秘密保持契約上の義務履行を確認するため、秘密情報の授受記録も重要である。（有識者）
- 取引先が秘密保持義務を遵守しているかどうかについては抜き取り検査を行っている。（製造業）
- プライバシー保護の観点から、顧客と企業秘密を共有しないようにしている。 自社のネットワーク上で疑わしい兆候があればこれを明確にして、情報マネジメントチームに更なる調査を行うよう、要請を行う。（非製造業）

（3）パートナー企業の管理

原則として社外の事業者と秘密情報を共有しないというポリシーを前提にし、外部委託先などからの情報漏えいに対して根強い警戒感を持つ米国企業が見られた。

【パートナー企業との情報共有の考え方（ヒアリング調査結果）】

- 取引先とは原則として秘密情報を共有しない。（非製造業）
- 技術的なセンシティブ情報は、社外で共有されないよう徹底している。（製造業）

他方で、ヒアリング調査の結果、複数の米国企業が提携をしながら技術開発や商品開発を行うという中、パートナー企業の意識向上に努めているプラクティスも見られた。また、IT系企業などにおいては特に、小規模事業者も含めて無数のベンダーと取引を行うことが通常であるため、取引先に対して相互に秘密情報管理に関するリテラシー向上に取り組んでいる例も見られた。

【パートナー企業の秘密情報管理に関するリテラシー向上に係る取組（ヒアリング調査結果）】

- 協業が決定した後も、パートナー企業とは継続的に対話と教育を続け、情報管理についての規範を共有していこうとしている。（非製造業）
- 無数のベンダーと協業しているので、情報管理カルチャーの共有は極めて重要である。オープンソースとネットワーク化の時代にあって、協業者同士がお互いの秘密情報を尊重しあうカルチャーは業界で共通のものになりつつあると認識している。（非製造業）
- 大企業と連携する場合は、フォーマルで詳細な契約書を取り交わすことになるが、現在の協業先にはタートアップの中小企業や個人でも多いため、同レベルの情報管理対策の実施や体制構築を要求するのは現実的ではない。（非製造業）

また、共同研究など、プロジェクトベースで情報共有が必要な場合に、暗号化するわけではないものの特殊なデータ形式の特別なソフトウェアを用いたデータの共有を行ったり、外部送信を不可とするといったプラクティスも見られた。

【特別なソフトウェアを活用した情報共有例（ヒアリング調査結果）】

・　プロジェクトにおいて複数の企業間で情報を共有する必要がある場合（例えばCADデータの共有）、データをそのまま共有すると秘密情報管理として問題がある。そこで、CADデータの閲覧については、特別のソフトウェアを使用するものとし、閲覧以外にダウンロードや電子メールでの外部送信ができないような措置をとっている。（製造業）

なお、自社も取引先の秘密情報を受け取る場合もあることから、パートナー企業に対する権利侵害や情報漏えいがないように特に注意を払っているという企業姿勢も見られた。

【パートナー企業から受け取った情報の管理（ヒアリング調査結果）】

・　自分たちがパートナー企業に提供する情報を守るだけでなく、先方から秘密情報を受け取ることも多いため、パートナー企業に対する特許侵害や秘密情報の間接流出には特に注意を払っている。（非製造業）

６．グローバル拠点の管理

グローバル拠点の管理について、今回実施したヒアリング調査の範囲では、日本企業と大きく異なるようなプラクティスは見られなかったが、グローバルで統一化された規程を用いる際、もっとも秘密情報漏えいの懸念がある地域を基準としたポリシーとするといったプラクティスが見られた。各国の事情を踏まえた統一的なポリシー策定にはコストが掛かるものの、必要コストとみなされている、という企業の声が聞かれた。なお、現地法人の法務部門や監査部門に比較的重要な役割を担わせ、米国本社との定期的なミーティングにおいて潜在的なリスクの所在と対応方針などについて検討を行わせているといったプラクティスも見られた。

【グローバル拠点の管理実態（ヒアリング調査結果)】

- 対象国ごとに異なるポリシーを策定するのではなく、対象国如何を問わず「統一化された」秘密情報保護ポリシーを策定し、実施している。その際、重視されるのが、当該企業の活動対象国の中で最も情報漏洩が発生し易い地域を特定し、当該地域の特徴を十分に考慮した統一ポリシーを策定するというプロセスである。アジア圏で言えば、例えば中国が秘密情報の漏えいについて問題視されるべき地域として認識されている。問題が大きい国におけるリスク回避に資するポリシーを策定、実施することで、全体としての秘密情報漏えいのリスクを軽減させるという方針である。(製造業)。
- 統一化されたポリシーを策定する前提としては、関連国の法制度、判例、ガイドライン等を十分に検証するよう努められている。そのような裏付け作業そのものは時間と費用のかかるものであるが、秘密情報管理のための合理的なコストとして認識している。
- 海外拠点に対しても同じルールを適用する。(非製造業)
- 本社から子会社に秘密情報を展開する際には、本社と同などの管理が求められている。(製造業)
- 現地法人では法務部門が監査部門として立ち回っている。週次又は月次のミーティングで関連会社の社長たちと潜在的なリスクや対応について話をしている。(製造業)
- グローバル規定が定められているが、各国において固有の情報セキュリティ規則がある。(製造業)
- 秘密情報の取り扱いは国によって異なるので、地元でのカウンセリングを前提に見直しが行われる。(有識者)

Ⅳ．諸外国における秘密情報管理の実態

ここでは、ドイツ企業及び中国企業の実態について、現地有識者に対するヒアリング及びドイツ企業に対するヒアリング結果も踏まえ、参考となるプラクティスを整理した。

１．ドイツ企業の実態

（１）ドイツ企業における秘密情報管理の捉え方

現地有識者によれば、ドイツにおいても、秘密情報管理の重要性に対する認識が近年高まっているところ[35]、秘密情報管理の仕組みは、リスクマネジメントの一部として捉える企業と、リスクマネジメントとは独立した情報セキュリティという枠組みでフレームワークを構築しているプラクティスが見られた。経営者の認識としては、情報漏えい、技術流出のリスクを重大なリスクとして捉えているが、これを全社的なリスクマネジメントの中で独立したリスク類型とせず、コンプライアンスリスクの１つと捉えている側面もあるようであり、同様の認識は企業においても見られた。

【秘密情報管理に対する考え方（ヒアリング調査結果)】

- 技術流出は、とても重要なトピックで、不正なデータ収集及びドイツ国内においてアメリカ国家安全保障局（National Security Agency：NSA）がスパイ活動を行っていたことに係る報道などを受けて、ドイツにおける問題意識は高まっている。（有識者）
- 情報セキュリティのフレームワークは、多くの場合、品質管理に係るマネジメントシステムの一部ではなく、リスクマネジメントの一部もしくは独立したフレームワークとなっている。（有識者）
- 情報漏えい、技術流出に係るリスクマネジメントは、内部統制ないし全社的なリスクマネジメントのフレームにビルトインされている。（有識者）
- 経営陣は他のリスク類型と比較して、情報漏えい、技術流出リスクを重大なリスクであると認識している。経営陣は法令遵守と同じレベル感で捉えており、事が起これば一大事であると考えている。（有識者）
- 情報セキュリティ自体はコンプライアンスの１つという位置づけで考えている。（製造業）

35 ドイツ企業だけでなく、EU 加盟各国企業 537 社から回答を得た調査において、10 年前に比べて営業秘密侵害のリスクが高まっていると考えている企業が 38.1%に上ることが示されている。European Commission, Study on Trade Secrets and Confidential Business Information in the Internal　Market (Final Study), April 2013.）参照。

（２）秘密情報管理に係る体制

秘密情報管理に係る体制について、現地有識者によれば、IT 部門、知的財産部門、法務部門の他、チーフ・リスク・オフィサー（CRO）が設置されている場合には、CRO の助言に基づいて取締役会などが方針及び体制について決定するというプラクティスが多いとのことであった。

【秘密情報管理に係る体制の実態（ヒアリング調査結果)】

・　秘密情報管理区分を含む秘密情報管理に係るルール、基準に係る重要な決定は、IT 部門、知的財産部門、法務部門、又は CRO などが存在する場合には CRO からの助言に基づいて、取締役会が決定する。(有識者)
・　情報の重要性に基づいた秘密管理区分は一般的に行われている。また秘密情報は、営業秘密として位置づけられていることが通常である。(有識者)

（３）物理的な管理

現地有識者によれば、ドイツにおいても、アクセス権の設定が秘密情報管理上、重要な意義を有していることが指摘された。

【物理的な管理に対する考え方（ヒアリング調査結果)】

・　一般論として、知る必要がある情報に限定したアクセス権の設定、NDA の締結、営業秘密に関する企業のガイドライン策定といった対策が特に重要となる（有識者）

ヒアリングに対応頂いたドイツ企業では、ドイツにおけるグローバル本社の IT 部門が世界各国拠点の IT 部門を統括し、情報システムや情報機器についても全て本社のポリシーやルールに従い、本社から指示が出されるという仕組みを採用していた。当該企業では、こうした運用が徹底されており、印刷機で紙媒体を出力する場合、社員証などで出力者の ID が確認され、当該 ID 記録も全て本社で一元的な管理が行われているとのことであった。

【情報機器や記録メディアの利用に係る取組（ヒアリング調査結果)】

・　情報システムや情報通信端末については、IT 部門の所管で詳細は分からないが、IT 部門はグローバル本社直轄のチームとなっており、基本的にはすべてグローバル本社のポリシーやルール、個別の指示に従っている。(製造業)
・　USB などの利用を物理的に不可能としている訳ではないが、アクセス制御により、仮に持ち出されてもインパクトの小さい情報にしかアクセスできないような仕組みとなっており、リスクは軽減されている。(製造業)

・　紙媒体をコピーする際も、コピー機に社員証などで社員 ID を読みとらせてからでないと印刷ができず、印刷をしたという記録は全てグローバル本社で一元的に管理、分析される。（製造業）

現地有識者によれば、ドイツ企業においては、オフィスレイアウトについても、情報セキュリティを考慮に入れる場合が多いとのことである。アンケート回答のあったドイツ企業においても、特に研究開発部門を中心に厳格なゾーニングが行われていた。

【ゾーニングに係る取組（ヒアリング調査結果）】

・　オフィスレイアウトについては、情報セキュリティを考慮に入れる場合が多い。特に大半の会社では従業員の場所的なアクセスについて、カード式の電子キーで入退室できるエリアを制限している。（有識者） ・　グローバル本社では研究開発部門などを中心に厳格な管理が行われている。例えば試作段階のプロジェクトを担う研究拠点は厳格なゾーニングがなされ、最小限の関係者しか入れない。管理上、立ち入りが必要な場合には詳細な申請・手続を経て許可を受けなければならない。製品を製造する段階、販売する段階と進むにつれて、関係者が増えて行くことになる。（製造業）

（4）労務管理

ヒアリング調査に対応頂いた企業では、採用時のバックグラウンドチェックを行っているものの、米国企業が自主的に行っているような犯罪歴の調査まで実施してはいないとのことであった。

【従業員採用時の取組（ヒアリング調査結果）】

・　採用時のバックグラウンドチェックは行っているが、犯罪歴の調査などまで行うかどうかについては社内でも議論がある（現在は未実施）。必要であるという意見もあるが、やはり国によって人権侵害が問題となる場合もあり、難しい問題である。（製造業）

また、ヒアリング調査によれば、入社時や退社時の秘密保持契約や競業避止契約の締結については、ドイツ企業においても比較的広く行われているようである。もっとも、競業避止契約の有効性が認められるためには、相当の経済的対価が必要となるとのことであった。

【従業員との契約締結に係る取組（ヒアリング調査結果）】

・　入社時、退社時には秘密保持に係る誓約書を取っている。（製造業）

- 主な対策は、従業員との雇用契約上の秘密保持条項、あるいは個別の秘密保持契約となる。（製造業）
- 部長など、一定の幹部職員については退職時に競業避止条項を入れている。もっとも代償措置についてはそれほど厳密に考えて運用されていない。（製造業）
- 退職時には会社に帰属する情報の返還を求めるが、例えば名刺も会社に帰属するもので、返却の必要があるものだと伝えている。名刺の数合わせまではしていないが、あまりに返却枚数が少ないということであれば、人事部門から確認を入れているようである。（製造業）
- 秘密情報については、雇用関係終了後も秘密保持契約によって保護される。しかし、一般的なノウハウやスキルについては、どのような契約を締結しても法的保護をすることは難しい。（有識者）
- 雇用契約終了後の競業避止義務については、両者の合意があれば課すことができる。しかし、その場合、当該従業員が競業避止義務賦課に対して、相当額の対価を支払わなければならず、これが支払われていない場合、当該契約は無効となる。（有識者）

現地有識者によれば、具体的な情報漏えいなど、秘密保持義務に違反するような不正行為に対しては警告を行い、必要に応じて法的な措置も取るというのがドイツにおけるエンフォースメントの実態であるとの指摘があった。また、程度によっては解雇に至るケースもあるが、減給といった雇用契約上のエンフォースメント手段を講じることはあまり一般的ではないとの指摘もあった。

【エンフォースメントの実態（ヒアリング調査結果）】

- 具体的な不正行為が発生しない限り、予防的に元従業員又は新しい雇用主に警告を出すことは稀である。（有識者）
- 営業秘密が、新しい雇用主の下で、秘密保持義務や競業避止義務に違反して営業秘密が利用され場合、元従業員と新しい雇用主に対して法的措置を取ることができる。具体的には差止請求、保全処分、損害賠償請求及び刑事的な制裁措置を求めることができる。（有識者）
- 現従業員による不正に対しては、比較的軽い事案であれば文書などによる警告ないし訓告程度のサンクションとなり、中度・重度の事案であれば雇用契約の解除に至る場合もある。減給というのはあまり一般的な制裁措置ではないものの、従業員の同意があれば課すことができる。給与はあくまで実績に対する報酬であり、ルールを遵守させるためのインセンティブではない。（有識者）
- 内部告発プログラムについて、ドイツでは明確な証拠が存在しない場合、他の従業員の不正の疑いを報告する義務の存在を認めることに裁判所はかなり躊躇する傾向にある。（有識者）

ヒアリング調査によれば、ドイツ企業においても研修の重要性は認識されているようであり、情報セキュリティに関する研修はほとんどの会社で実施されているとの指摘もあった。

【研修実施の取組（ヒアリング調査結果）】

- 入社時には Web トレーニングを実施している。コンテンツは基本的に現地語で作成している。（製造業）
- 従業員に対する情報セキュリティ研修はほとんど全ての会社で行われている。（有識者）
- 研修１つとっても管理者研修の中で、「unhappy」な人を事前に把握し、フォローするといったことも、情報管理の側面からも意識的に行うといったことは気づきになるのではないか。（製造業）

ヒアリング調査によれば、退職予定者について、情報システム上のアクセスを制限したり、自宅待機を命じるといったプラクティスが見られた。

【退職予定者への対応（ヒアリング調査結果）】

- 同業他社に転職する人については、翌日からパソコンのアクセスを遮断したり、自宅待機を命じることもある。（製造業）

（５）取引先管理

ヒアリング調査によれば、取引先管理については、秘密保持契約を締結することを前提に、契約終了後における情報の返却や破棄の重要性が指摘された。また、秘密情報の返却や破棄に係る契約違反に対しても損害賠償を求める場合があるとのことであった。

【パートナー企業との契約に係る実態（ヒアリング調査結果）】

- 取引先との関係では、契約終了後における情報の返却・破棄条項を NDA に含めることが重要となる。ドイツ法の下ではこうした条項の違反に対して損害賠償を求めることができる。明示的な合意があれば損害賠償額を予定することも出来るが、それほど一般的ではない。（有識者）
- また取引先に対して秘密情報を明確にするため、ラベリングを行うことも重要である。（有識者）
- 重要な取引との関係では特殊な電子メールのエンコードを設定することも重要な対策である。（有識者）

ヒアリング調査によれば、訴訟に際して証拠として有効かどうかを意識して、取引先とのやり取りに基づいて発生する各種証跡を、作成、管理しているというプラクティスが見られた。

【パートナー企業とのやり取りの証跡管理（ヒアリング調査結果）】

・　関係証跡は、争いになった場合、証拠として有効かどうかという観点を意識して作成している。この点は、契約書や誓約書の文言も同様である。（製造業）

（６）グローバル拠点の管理

ヒアリング調査の結果、グローバル拠点の管理に関連して、グループ各社に情報漏えいないし技術流出に係るリスクアセスメント（リスクが顕在化した場合に想定される経済的損失額も含む）を実施させた上、ドイツにあるグローバル本社において、本当にグループ全体の業績に影響を与えるような損害が発生しうる情報資産のみを管理するというプラクティスが見られた。

【グローバル拠点の管理実態（ヒアリング調査結果）】

・グローバル本社のある EU でも個人情報保護規制は厳しいが、データプライバシー対応ということで近年になってグローバルなミニマムスタンダードを策定した所であり、むしろ日本法人の方が少し進んでいたのではないかと思われる。（製造業） ・情報セキュリティのクライテリアもグローバルなものとは別途、ローカルでの影響を関上げて検討されている。グローバル本社から半年毎に情報漏えいリスクのある情報資産のたな卸しを指示されているが、数 10 億ユーロ程度の損害が発生し得るものという定義なので数件しかない。グローバル本社としてのリスクマネジメントとしては、インパクトの小さいものは現地法人のマネジメントに任せるということで合理的だと思うが、現地法人としては信頼に関わる部分なので、より厳格に考えている。（製造業）

２．中国の実態

（１）中国企業における秘密情報管理の捉え方

中国の秘密情報管理実務に詳しい有識者によれば、中国においても秘密情報管理自体はリスクマネジメントシステムの一部として見なされているとのことであった。また、情報漏えいないし技術流出リスクは、オペレーショナルリスク[36]やリーガルリスク[37]と同等のリスクと捉えられているようであるとのことであった。

【秘密情報管理の位置づけ（ヒアリング調査結果）】

・　秘密情報管理のフレームワークは、リスクマネジメントシステムの一部として見なされている。（有識者）
・　一般的に、情報漏えいないし技術流出リスクは、オペレーショナルリスクと同じカテゴリのリスクと認識されている。（有識者）
・　情報漏えいないし技術流出リスクは、コンプライアンスリスク、訴訟リスク、その他法務・税務上のリスクなどと同等のリスクと捉えられている。（有識者）

有識者によれば、国有企業の経営者は、秘密情報の漏えいが国家秘密[38]漏えいとされ、刑事的にも国家秘密漏えい事件として告発されるリスクを認識しているとのことであった。

【秘密情報に対する考え方（ヒアリング調査結果）】

・　国有企業では、秘密情報の漏えいが国家秘密の漏えいにつながる場合もあり、刑事的にも厳しい措置が取られる場合があることも経営者はリスクとして認識されている。（有識者）

（２）秘密情報管理に係る体制

有識者によれば、中国企業においても秘密情報区分がなされ、区分に応じたアクセス権設定は行われているとのことであった。もっとも、必ずしも、秘密情報区分について統一的なルールを設けられている訳ではないとの指摘もあった。

【秘密情報管理に係る体制（ヒアリング調査結果）】

・　包括的な秘密情報管理が行われている。社内の情報は複数のレベルに区分され、アクセス承

36 オペレーショナルリスクとは、業務オペレーション（事務処理など）上発生するリスクを指す。
37 リーガルリスクとは、法務活動に起因する法的な責任が発生するリスクを指す。
38 中国における営業秘密は不正競争防止法によって保護されるが、国家機密については国家秘密保護法によって保護されている。

認された特定の者がそれぞれの管理レベルに区分されている情報にアクセスできるようになっている。（有識者）
- 国有企業の場合、特定の情報を国家機密として区分することが可能である。（有識者）
- 期初に秘密情報管理の対象となる技術情報の種類を明らかにさせている。（製造業）
- 情報を区分するための統一的なルールは存在していない場合も少なくない。情報の性質に応じて、CEO や他のトップマネジメント層が決定する可能性がある。例えば技術情報は技術部門で管理されており、CTO などが情報を分類する権限を持っている。業務執行上の情報であれば、CEO やジェネラルマネージャーによって区分される。（有識者）

なお、有識者によれば、中国企業では、チーフ・リスク・オフィサーなどの役職者が配置されていることは一般的なプラクティスとはなっていないとのことであった。

【CRO 配置の実態（ヒアリング調査結果）】

- チーフ・リスク・オフィサー（CRO）は、知る限り配置されている企業を知らない。（有識者）

また、ヒアリング調査に協力頂いた中国企業では、事前に管理者及び知的財産部門が社内情報の対外公表をチェックする仕組みを設けているプラクティスが見られた。

【情報公開に際したチェック体制例（ヒアリング調査結果）】

- 外部（社内も含む）での発表、交流に関して、内容を事前に管理者、知財部門によって、チェックする体制となっている。（製造業）

（3）物理的な管理

有識者によれば、秘密情報区分に応じたアクセス権設定などが行われている他、ゾーニングを実施している企業も少なくないとのことであった。また、技術流出の観点から、サンプルや関連備品の破棄を徹底しているといったプラクティスや、秘密情報の管理に文書管理システムを活用していると思われるプラクティスも見られた。

【秘密情報の物理的な管理例（ヒアリング調査結果）】

- 機密情報を取り扱うネットワークと一般のネットワークを区別させること及び混合できないようなファイアウォール[39]を設けている。（製造業）

[39] ここでファイアウォールとは、ネットワークに対するアクセス権限のないアクセスを遮断する

- サンプルや関連備品の破棄を徹底し、一括管理を行っている。（製造業）
- パソコンなどの情報機器管理の強化、監視カメラの設置、作業日記管理の徹底化などの対応を行っている（非製造業）
- 秘密情報に関する分類は、従業員が企業秘密や他（コピーするために必要な承認のレベル、FAX、企業秘密などが含まれる書類の電子メール）へのアクセス権の範囲を決定することができる。（有識者）
- 情報区分に応じたセキュリティ保護対策が実施される。一般的に情報システム上、限られたアクセス権者のみ特定の情報にアクセスできるように設定される。（有識者）
- 情報区分によって、アクセス権の承認権者は異なる。仮に全ての情報を機密として扱うのであれば、CEO とジェネラルマネージャーのみがアクセス承認権限を有することになる。（有識者）
- 秘密情報が掲載されている文書の保管について、金庫（セーフティーボックス）が割り当てられている。（有識者）
- 文書のタイトルは、システム上管理され、承認者は秘密情報を含む文書の所在や媒体を管理することができる。（有識者）
- オフィスレイアウトなどを秘密情報管理の観点から工夫している例は知らない。（有識者）
- 秘密情報を保管している特別なエリアに入るためには特別な ID カードによるアクセス承認が必要となっている。こうしたエリアは、CCTV をはじめ、他の監視装置が備えられている。（有識者）
- 特定のエリアには情報通信端末を持ちこませないようにしている。（製造業）

（4）労務管理

有識者によれば、入社時、退職時の秘密保持契約書の締結は広く行われているとのことであった。

【新規雇用者および退職者への対応例（ヒアリング調査結果)】

- 異動、退職時に、外部弁護士の立ち会いのもとで、秘密保持契約を結ぶ。(製造業)
- 入社時には、個別の秘密保持契約の締結を求めている。（有識者）
- 秘密保持条項は就業規則に記載することも可能である。（有識者）
- 秘密保持規定については研修においても取り上げられる。（有識者）
- 上級管理職や秘密情報にアクセスを認める技術者などについては個別の秘密保持契約を締結する。（有識者）
- 退職時にも、雇用関係終了後も秘密保持義務が存続し、義務違反から生じる責任を負うことを同意書の形で確認している。（有識者）
- 秘密保持契約などには高額な違約金を定めている。（非製造業）

仕組みの意味である。

・　懲戒処分としては、警告、給与／ボーナス削減、昇進の機会の損失、解雇などがある。解雇に至るには決定的な秘密保持義務違反が無ければならず、頻繁に実施されている訳ではない。（有識者） ・　コンプライアンス研修に係るプログラムでは、秘密保持義務に必ず触れている。（有識者） ・　競業避止契約を締結するには、法令によって経済的な補償が必要となる。（有識者）

（5）取引先管理

有識者によれば、取引先との秘密保持契約の締結は行われているものの、秘密保持義務履行に係るエンフォースメントまでは行えていない企業が多いとのことであった。

【パートナー企業との契約に係る実態（ヒアリング調査結果)】

・　取引に係る契約書上、秘密保持条項は盛り込まれるが、取引先に対して秘密情報管理監査までは実施していない。（有識者） ・　契約上、秘密保持義務違反に対して違約金を定めておくこともある。（有識者） ・　受け渡しをする秘密情報には、機密指定の表示を行い、通信時には暗号化などの対応を行う。（有識者）

（6）グローバル拠点の管理

有識者によれば、中国のグローバル企業においても各国統一のルールを設けていることが多いとのことであった。

【グローバル拠点の管理実態（ヒアリング調査結果)】

・　グローバル企業は、現地の法律を意識した修正を加えつつも、グローバル統一ルールを基本としている。（有識者）

Ⅴ．情報漏えいに係る事後対応

１．情報漏えい事例

（１）国内における事例

東芝（半導体メーカー、売上高：約 6 兆 5,000 億円（連結）、約 3 兆 3,000 億円（単独））

2014 年３月に、同社が有する営業秘密を不正に取得・使用しているとして、韓国の SK ハイニックス社に対して不正競争防止法に基づく損害賠償を求める民事訴訟を提起した事案である。

漏えい者は、東芝の提携先であるサンディスクの技術者として 2008 年に東芝の四日市工場内で共同開発していた際に、東芝の NAND 型フラッシュメモリーに関わる研究データを不正にコピーし、同年に SK ハイニックスに転職した際に当該データを持ち出したとされている。

営業秘密である当該研究データが漏えいした疑いが生じ、東芝が調査を進める中で不正の事実が発覚したため、SK ハイニックスに対して約 1,000 億円の損害賠償を求める訴訟を提起した。

その後、2014 年 12 月に SK ハイニックスから東芝に対して約 278 百万米ドルの和解金を支払うことで民事については和解に合意している。また、東芝は漏えい者を刑事告訴し、2015 年３月に東京地裁において懲役５年、罰金 300 万円（求刑懲役６年、罰金 300 万円）が言い渡されている。

新日鐵住金（製鉄メーカー、売上高：約 5 兆 5,000 億円）

2012 年４月に、同社が有する営業秘密を不正に取得・使用しているとして、韓国ポスコ社およびその日本法人に対して不正競争防止法に基づく約 1,000 億円の損害賠償請求および当該営業秘密を使用した製品の製造・販売などの差止めを求める民事訴訟を提起した事案である。また、不正取得・使用に加担したとして同社の元社員に対しても不正競争防止法に基づく損害賠償を求める民事訴訟を提起した。

漏えい者は新日鐵住金の元技術者であり、1990 年代半ばに同社を退職した後、ポスコと関係がある韓国の大学に客員教授として招聘された際に、新日鐵住金が有する方向性電磁鋼板の製造技術をポスコに対して不正に漏えいしていたとされている。

当該営業秘密の漏えいは、ポスコの元社員が中国宝鋼集団に同技術を漏えいしたとして刑事告訴された際に、当該技術がポスコの技術ではなく元々は新日鐵住金の技術であるとの主張がなされたことで発覚したものである。

ヤマザキマザック（工作機械メーカー、売上高非公開）

2012 年３月に、同社のサーバにアクセスし営業秘密情報を不正に複製したとして、同社の元社員が不正競争防止法違反容疑で逮捕された事案である。

漏えい者は中国籍の同社の元社員であり、不正に取得した２万件以上ともされる図面などの情報を中国のメーカーに売却して利益を得る目的があったとされている。また、同容疑者が 2012 年３月に退職を申し出た後に大量の図面情報などがサーバからダウンロードされたことが確認されている。

2014 年８月、名古屋地裁において同容疑者に対して懲役２年、執行猶予４年、罰金 50 万円の判決が言い渡された。

ベネッセコーポレーション（教育・出版業、売上高：約 4,700 億円（ベネッセ HD））

2014 年７月に、同社の顧客情報を社外に漏えいさせたとして、同社のシステム開発・運用を行っているグループ会社の業務委託先の元社員が逮捕された事案である。

漏えい者は、不正の利益を得る目的で、データベースからクライアントパソコンに当該顧客情報を保存し、ケーブル経由で私有のスマートフォンに転送・保存した上、名簿業者に売却していたとされ、流出した個人情報は約 4,858 万人分、延べ約 2 億 1,639 万件と推計されている。

当該顧客情報の漏えいについては、2014 年６月より同社の顧客宛に他社からのダイレクトメールなどが頻発していたことを受けて調査した結果、顧客情報が保存されているデータベースへのアクセス権を有する者が期間中複数回にわたりデータベースにアクセスしていたログが確認されたことから判明したものである。

日産自動車（自動車製造・販売、売上高：約 10 兆 4800 億円（連結））

2014 年５月に、同社の営業秘密情報を不正に持ち出したとして、不正競争防止法違反容疑で同社の元社員が逮捕された事案である。

漏えい者は同社の商品企画部門も元社員であり、2013 年８月のいすゞ自動車への転職前の 7 月に、日産のパソコンを用いて日産本社のサーバから新型車の販売計画などを含む約 5 千件のデータをダウンロードし、自宅で私有パソコンなどに複製していたとされている。

日産における内部調査で、退職前に大量のファイルをコピーしていた疑いがあることが判明したものであり、2014 年５月の逮捕後の６月に処分保留で釈放されていたが、同年 10 月に不正競争防止法違反の罪で在宅起訴となっている。

デンソー（自動車部品製造、売上高：約 4 兆円（連結）、約 2 兆 5,000 億円（単独））

2007 年３月に、同社の最高レベルの機密データを持ち出したとして、横領容疑で同社の元社員が逮捕された事案である。

漏えい者は中国籍の同社の元技術者であり、2006 年 10 月～2006 年 12 月にかけて、漏えい者が所属していた部署を含む一部の部署のみがアクセスできるデータベースから、大量の図面データなどを同社が貸与しているノートパソコンにダウンロードし、自宅に持ち帰った上で外付けのハードディスクなどに複製したとされている。

2007 年２月に同社のコンピューター上に漏えい者のアクセスログが残っていたことをきっかけとして事件が発覚したものである。しかし、発覚後の操作時にはパソコンには外付けのハードディスクなどにデータを複製した痕跡は見られたものの、すでにパソコンからはデータは消去されており、また外部記録媒体の多くは破壊されていた。

その後、2007 年４月に漏えい者は処分保留で釈放されている。

ヨシツカ精機（プレス機械製造、売上高非公開）

2012 年６月、同社の図面データなどを不正に持ち出したとして、同社の元社員およびその共犯者１名が不正競争防止法違反容疑で逮捕・刑事告訴された事案である。

漏えい者である同社の元社員は、2009 年 11 月に共謀者である中国企業Ａ社と提携していた企業Ｂ社の社員からの依頼で、約 258 の同社の図面データを複製したとされている。漏えい者は 2009 年 12 月に退職した後に、共謀者に対して図面データを渡し、共謀者は同データを 2010 年１月に中国企業Ａ社に対して送付したとされている。

中国企業Ａ社に図面データ郵送した共謀者は中国企業Ａ社から 500 万円を受け取り、漏えい者も 100 万円程度を受け取っていたとされる。

2012 年９月、横浜地裁において、両者とも懲役２年、執行猶予３年、罰金 100 万円が言い渡された。

（２）海外における事例

General Motors (GM) （米国、自動車製造・販売、売上高約 1,554 億ドル）

2012 年 11 月、同社の営業秘密情報を不正に持ち出したとして、同社の元技術者およびその夫に有罪判決が出された事案である。

漏えい者である同社の元技術者は､ハイブリッド車技術のグループに所属していたが､2005 年に退職契約を提示された数日後に営業秘密情報を含む 16,000 以上のファイルを外部記録媒体に複製したとされている。また、不正に持ち出した情報の価値は 4,000 万ドル以上になるとも推計されている。

不正に持ち出した情報は、漏えい者とその夫が共同で保有・運営しており、GM の競合にあたる中国企業 Millennium Technology International Inc. (MTI) の利益のために使用されたとされている。

Motorola（米国、通信機器、売上高約 12 億ドル）

2012 年 8 月、同社の営業秘密情報を不正に持ち出したとして、同社の元技術者に対して懲役 4 年が言い渡された事案である。

漏えい者である同社の元技術者は、病気休暇を取得していた 2006 年～2007 年に中国に帰国し、中国軍向けの通信技術を開発する Sun Kaisens 社で中国軍向けのプロジェクトに従事していた。その後、Motorola に復帰した際に社内でセキュリティのかかったネットワーク上に保有されている多くの重要な技術情報を入手し、復帰から数日後にその情報を中国に持ち出そうとしたとされている。持ち出そうとされていた情報の中には、Motorola が数年間に 400 万ドルもの資金を費やして開発した iDEN と呼ばれる通信技術の情報も含まれていた。

漏えい者が中国への出国を画策していた際に、空港で米国当局が呼び止めて手荷物を検査した結果、Motorola の大量の技術情報資料と中国軍の資料が発見されたものである。

Valspar Corporation（米国、塗料製造、売上高約 41 億ドル）

2010 年 10 月、同社の営業秘密を不正に持ち出したとして、同社の元化学者に対して懲役 15 カ月が言い渡された事案である。

漏えい者である同社の元化学者は、2006 年より同社の建築塗装グループの技術部長として研究開発に従事していたが、2009 年に同社の競合にあたる日本ペイント（中国・上海）に転職する前の 2008 年～2009 年にかけて、同社の化学式などの技術資料や売上・コストに関するデータを含む内部資料をダウンロードし、私有の USB に複製したとされている。これらの情報は、2,000 万ドル以上に相当する情報であるとされている。

Ford Motor Company（米国、自動車製造・販売、売上高約 1,469 億ドル）

2010 年 10 月、同社の営業秘密を不正に持ち出したとして、同社の元技術者が起訴された事案である。

漏えい者である同社の元技術者は、1997 年～2007 年まで同社での製品開発に従事しており、この間に営業秘密にアクセスしていたとされている。2006 年に米国企業の中国支社へ転職する際に約 4,000 もの重要な書類を私有の外付記録媒体に複製して持ち出し、2008 年には同社と直接の競合関係にある中国に自動車会社で働き出している。

2009 年に漏えい者が米国に来た際に空港で逮捕されており、所持していたパソコンの中には同社の設計図面などが保存されており、漏えい者がその情報にアクセスしていたことも確認されている。

被害額は推定で 5,000 万ドル以上とされており、また漏えい者に対しては約 70 カ月の懲役が言い渡されている。

２．国内企業における事後対応の実態

（１）検知の仕組み

ヒアリング調査の結果、権限の無い者が特定のファイルやフォルダなどに対してアクセスを試みることや、外部との電子メールのやり取り、情報機器への情報のコピーなどを、情報システム上検知できる仕組みを作っているプラクティスが見られた。一方で、社有の業務用情報機器に私有情報機器を接続した場合などの検知や、情報機器にデータを保管することを禁止していながらも、物理的なデータのコピーまでは制限できておらず、データ保管を検知する仕組みを構築できていないという企業もあった。

【検知に係る取組の実態（ヒアリング調査結果）】

- サーバへのアクセスや外部とのメールのやり取りなどもある程度モニタリングされており、異常があればアラートが送られてくる。またアクセスログなども相当長期にわたって保存してあり、事後的な調査が可能となっている。（製造業）
- アクセスログを記録するなど、漏えい発生後に追跡調査はできる体制になっているが、事前発見を目的とした経常的なモニタリングは行っていない。（製造業）
- 業務用端末へのアプリケーションのインストールは検知できる仕組みになっている。（製造業）
- メールのモニタリングなどを受けており、ルールで定めている秘密情報が外部に発信されていれば直ぐに検知される。また情報サイトやインターネットサービスプロバイダー（ISP）が提供するメールサービスなどへの発信や不審点があるメールなどもチェックの対象とされているようである。（製造業）
- パソコンに私有端末を接続した際のリアルタイムでの検知はできていない。（製造業）
- 業務用ノートパソコンのローカルにデータを落とすことは、ルール上は禁止されているが、現状では保存が可能であり、検知もできていないので今後の課題であると考えている。（製造業）
- 不正な情報の持ち出しについては、システム上のログとアクセス権の管理によって制御・監視している。ログは部署別に監視させる体制を導入し、問題が発見された場合に報告させるようにしている。全社のログを監視するのは量的に困難であるだけでなく、現場の方が問題点を把握・評価しやすいことも理由である。（情報セキュリティに関して相互にベンチマークしている国内グローバル企業でも、システム上のログは部門の責任で管理している）（製造業）
- アクセスログなどは取っており、また外部からダウンロードされるファイルなどもチェックしている。また紛失や誤送信などの過失による情報漏えいについては報告ルールなどを徹底し、事態の把握と問題を最小化するような管理を行っている。一方、悪意による情報漏えいを未然に検知するという意図でパトロール的なことをしているかというと十分に行えていない。（製造業）

ヒアリング調査の結果、実際に退職予定者や上司が必要と認める従業員について積極的にアクセスログの監視を行い、不正の未然防止に取り組んでいるプラクティスが見られた。

【退職予定者に対する監視例（ヒアリング調査結果）】

- 入館カードで出入のログは取れているが、この情報は現状では勤怠チェックなどの総務的な観点でしか活用されていない。例えば、休日に関係のない部屋に頻繁に出入りしているというような不正検知や、要注意の人物に対して重点的に監視するというような運用は全くなされていない。（製造業）
- 退職の申し出が無い職員についても、転職する可能性があると上司が判断すれば、ログやメールなどの重点監視対象としており、部門を問わず定期的に現場から監視対象に加えて欲しいという申告がある。（製造業）
- 私有の USB の使用はモニタリングされているが、実際に注意を払ってチェックされているのは転職が決まっている社員などの要注意対象のみである。（製造業）

SNS などを通じた情報漏えいに対する懸念から、業務用の携帯端末への SNS アプリケーションのダウンロードを検知できる仕組みを導入しているプラクティスが見られた。また、業務推進に係る必要性から私有端末の利用自体を禁止していない企業におけるプラクティスとして、SNS 上で不正な情報発信が行われていないかといった Web パトロールを実施しているというプラクティスも見られた。

【SNS 利用に係る検知の仕組み例（ヒアリング調査結果）】

- ソーシャルメディアについては、顧客とのコミュニケーションツールになっているという実態もあるのが事実だが、私的に利用していたとしてもその個人の所属する会社名がわかってしまうのでリスクであると認識している。業務用携帯に SNS アプリケーションをインストールした際には警告が出る仕組みにしているが、私有の端末であくまでも私的に利用している部分は管理できない。また、業法上の広告宣伝に対する規制があり、業法に違反するような行為があると大きなリスクになるため、外部に委託してソーシャルメディア上での不適切な発言がないかをサイバーパトロールしてもらっている（”会社名” + “XXX（不適切な内容）”などで検出）。不適切な発言で、明らかな違反行為が見つかった場合は懲戒処分になる場合もあり、過去に２例発生している。現状で行っている対策は、そのような事例を共有することによる啓発が挙げられる。（製造業）
- クラウドの利用は、主に製品の安全性情報の管理目的である。安全性情報はグローバルで一元管理することが求められているが、多くの個人情報が含まれたデータであり、パブリッククラウドでの管理はリスクがあるため、プライベートクラウドを利用している。（製造業）

情報システム上不正のおそれまたは不正があった場合には直ちに対応を検討する部門にレポーティングする仕組みを構築しているプラクティスが見られた。また、情報機器の紛失を含む事故について 24 時間以内に報告を上げる仕組み徹底しているというプラクティスも見られた。

【不正や紛失などに係る事後対応例（ヒアリング調査結果)】

- 情報セキュリティ関係のトラブル、不正などがあった場合には直ちにレポートを上げることになっている。事態発生から 24 時間以内に上長にレポートを提出し、上長から内部統制セクションに報告、内部統制部門が必要に応じて情報システム部門などと協議しながら対応を検討するという仕組みになっている。異動、転籍、退職予定者については、情報システム部門で社外メールやサーバアクセス状況などについてパトロールに行ったり、データの移動や消去などがないようにバックアップも取っている。(非製造業)
- USB 紛失といった事故はやはり年間数件程度は発生している。こうした現場で発生する事故も全て 24 時間以内に報告させることを徹底している。(製造業)

ヒアリング調査の結果、不正のおそれまたは不正があった場合に適切なレポートを上げさせる仕組みを構築する際、現場部門においてできれば事態を顕在化させたくないという意識が働く場合が少なくないことから、漏れなく報告をさせる風土ないし組織文化を醸成することの重要性を指摘する声も聞かれた。また、上がってくるレポートについては、分析を行い、対応策の検討や改善に活用したり、従業員の意識向上のために周知を行うなどの対応をしているプラクティスも見られた。

【インシデント報告の風土作りや事例分析の取組（ヒアリング調査結果)】

- インシデント発生時の報告ルートとプロセスは関連会社も含めてグループに周知されているが、本社からの注意の対象になるのではないかといった懸念から、関連会社からインシデント報告が発生時に上がってくるケースは実際には少ない。しかしインシデントには即時に対応する必要があるため、何かが起きたらまずは報告をするものであるという風土作りが重要であると認識している。そのため、本社の役員にインシデントに対する非難をしない習慣づけをするほか、インシデント報告をしなかった場合は罰則の対象としている。(製造業)
- 報告された個別のインシデント事例を分析し、対応策の考案と改善に活用しているほか、各事例と実施された処罰については様々な方法で社内に通知し、抑止効果を狙っている。(製造業)

（2）内部監査、社内調査による検知

監査部門が行う内部監査の一環として、秘密情報管理に係る監査が行われているというプラクティスが見られた。一方、内部監査部門とは異なる専門部署による監査を実施しているプラクティスも見られた。

【秘密情報管理に係る監査例（ヒアリング調査結果）】

- 内部監査は監査部門が行っているが事業部門や事業所が多岐にわたることから、１つの事業部門・事業所から見れば数年に１回程度となっており、日常的には部門長などが管理している。もっともセルフチェックが十分にできているかというとまだ課題も多い。情報システム部門による監査もあるが、基本的に監査部門の監査とセットで行われるため、現場から見れば監査は数年に１回となる。（製造業）
- 内部監査部は内部統制監査の一環として業務監査を実施しているのに対して、マネジメント推進部は規格ものの監査を実施している。具体的にはプライバシーマークとの関連で個人情報管理に関する監査を実施したり、環境 ISO との関係で、環境マネジメントなどに関する監査を実施している監査結果・課題に対する提言は情報セキュリティ担当役員と社長に報告している。各部署には部内推進者（基本的には管理職）が在籍しており、担当者と共に監査を実施している。内部監査部とは情報交換やチェック項目の確認などを行っているが一緒に行動することはない。（非製造業）

また、一般的に不正が行われやすい休日のアクセスログや入退室ログなどを不審な点が無いかという観点から毎週調査するプラクティスも見られた。

【休日のログの調査に係る取組（ヒアリング調査結果）】

- 休日は人がいなくなるため、不正が行われやすいと思われるため、毎週、休日明けの朝に全社的にチェックしている。不審な行動が発見された場合は、危機管理委員会（危機管理マニュアルを策定した委員会）に報告。（非製造業）

（3）事後対応の実態

ヒアリング調査の結果、事後対応について、特にエンフォースメントという観点から見ると必ずしも積極的ではない企業も見られた。他方で、退職者について不正な情報持ち出しが発覚した場合、退職金の不支給措置を取るといったプラクティスも見られた。

【事後対応の実態（ヒアリング調査結果）】

- 個別に法的手段を取らざるを得ないケースが発生した場合の対応は全社の法務セクションに

移管されるため、事業本部で対応することはない。(製造業)
- 現在、退職者による情報持ち出しの予防および事前発見に力を入れている。退職願の提出が行われた翌日から過去ログの追跡が開始され、会社パソコンの持ち出しと、会社パソコンからのインターネット接続が全面的に禁止される。(製造業)
- 退職者が不正な情報持ち出しをしたことが発覚した場合、退職金の不支給措置がとられる。情報を漏えいしなくても、持ち出しただけで罰則の対象となる。罰則の程度は、情報の内容によって異なる。(製造業)

また、秘密情報管理の観点から従業員の行動について、部門別の評価に反映させる仕組みを導入し、部門それぞれが所属従業員の秘密情報関連規定の遵守などを徹底させるインセンティブを持たせているというプラクティスも見られた。

【評価への反映に係る取組（ヒアリング調査結果)】

- 2012 年度までは情報セキュリティ行動についての個人の自己評価に任せていたが、2013 年度より部門別の評価を行うようになった。(製造業)
- インシデントの報告件数は部門別に集計され、全社で共有される。(製造業)

過去、実際に情報漏えい事件が発生した企業においては、迅速に警察当局にも捜査依頼を行い、必要な法的措置を講じたというプラクティスも見られた。その際、必要な証跡を蓄積できていたことが迅速な対応に繋がったという指摘もあった。

【法的な措置を実施した例（ヒアリング調査結果)】

- 事件が発覚した際に、速やかに警察当局に捜査を依頼して、法的な措置を取ることとした。サーバアクセスなどのデータを蓄積できていたことで、証拠をそろえることができ、迅速な対応を取ることができた点は当局からも評価をいただいた。(製造業)

３．海外企業における事後対応の実態

（１）検知の仕組み

従業員の不正の端緒となりそうな行動がないか、情報システム上の監視を行っているプラクティスが見られた。また、実際に情報漏えいが発生した場合には全社的にシステムをシャットダウンする仕組みを構築しているプラクティスが見られた。

【検知に係る取組の実態（ヒアリング調査結果)】

- セキュリティ部門は、閲覧可能な領域にどのような情報があるか、コンピューターにログインしたまま退席していないかといった点についても、ランダムに監視を行っている。（製造業）
- リスクアセスメントに関連して、定期的にデータベースのチェックを行っている。（非製造業）
- 不正アクセスに対しては、システム的な監視が行われる。（有識者）
- 情報漏えい対策システムについてはメリハリをつけている。（製造業）
- 企業秘密を取り扱う従業員全てのアクセスログや外部とのメールのやり取りについてサンプル調査を悉皆的に実施し、懸念事項が発覚した場合には関係者に対する調査や勧告を即時に実施している。勧告自体は当該従業員の評価に影響を与える他、必要に応じて懲戒手続が取られる場合もある。(有識者)
- 第三者による不正侵入防止ソフトウェアが多くの技術系企業で利用されている。（有識者）
- 情報漏えいが検知された場合、会社のシステムがロックダウンする。ロックダウンを解除するには役員の承認が必要となる。（非製造業）
- 懸念が強い違反が見つかった場合には、システム全体のシャットダウン、および、特定のアカウントに対し一時的にアクセスを切断することを決定することが出来る。この場合も、サードパーティマネジメントチーム、セキュリティリサーチチームは、更なる調査を継続する。（非製造業）
- 重要な情報が漏えいした場合に、一般的なシステムのシャットダウン方法につい全従業員が訓練を受けている。(非製造業)
- 部署において不審な点があれば情報セキュリティを担うデータマネジメントチームに報告し、システム上のモニタリングを実施してもらう。（非製造業）
- 不審な行動を見つける際に、使いやすい監査の特徴を含む情報管理システムを活用している。（製造業）

また、今回のヒアリング調査においても有識者から、情報システム上の不正の事前の検知については、外部のフォレンジック会社を活用することも増えており、次のような指摘が得られている。

【フォレンジック会社の活用例（ヒアリング調査結果）】

- フォレンジック会社は、不審なアクセスやメールの送受信について、会社に自動的に警告を行うという不正防止のためのセキュリティシステムを提供している。こうしたシステムは、潜在的な不正も含め不適切な行動を識別することが可能であり、情報漏えいの潜在的な行動を検知することで、損害を最小化することが可能である。（有識者）
- フォレンジック会社によるアラートシステムは、恐らく 50%～75%の違反を発見することができると思われる。（有識者）
- 現従業員に疑わしい行為があった場合に備え、進入防止セキュリティシステムを社内コンピューターに設定するため、外部のコンピューターフォレンジック会社を利用する。最良の事例は、社内で状況に対処することを試みるより、フォレンジック会社のようなエキスパートに頼ることであると個人的には考えている。（有識者）
- フォレンジック会社によって情報がどのように漏えいしたか、アクセスしたかについては特定され、こうした事実は犯罪捜査や民事訴訟における証拠として日常的に活用されている。（有識者）

ヒアリング調査に対応頂いた企業の中には、ハッキング行為があった場合にフォレンジック会社を活用し、不正を検知・調査させるといったプラクティスが見られた。

【ハッキング行為発覚時のフォレンジック会社の活用（ヒアリング調査結果）】

- ハッキング行為があった状況を仮定した場合、フォレンジック社をすぐ利用するだろう。また、状況によっては、外部法律顧問も利用することもある。（製造業）

情報漏えい自体についてほぼ 100%検知できるとするヒアリング調査回答もあった。他方、相当のレベルで不正検知の仕組みを導入していると思われる企業においても、少なくともヒアリング調査に対応頂いた担当者の見解としては、どの程度検知できているか確信が持てないとする不安の声も聞かれた。

【情報漏えいの検知（ヒアリング調査結果）】

- 情報漏えいは、ほぼ 100%検知できる。発見が遅れるケースはあり得るが、当社のセキュリティチームは損害を軽減するために、徹底的な調査とバックアップ対応が可能である。（非製造業）
- 不正の検知について現状の仕組みでどの程度検知出来ているのかについては、確信が持てない。（非製造業）
- 情報漏えいについて、どの程度検知出来ているかについては、正直分からない。（製造業）

（2）内部監査、社内調査による検知

ヒアリング調査によれば、米国においても内部監査は一般的に実施されており、定期的な監査が行われている。顧客情報を大量に管理している企業においては四半期毎に監査を実施しているというプラクティスも見られた。また、潜在的なリスクを把握する観点から外部の調査会社を活用してリスクアセスメントを実施しているプラクティスも見られた。

【内部監査の実施例（ヒアリング調査結果）】

- 法務部門などが内部調査を行っている。噂や周辺情報から調査が開始されることもある。（製造業）
- 調査のトリガーとしては、前述の退職時面接における退職従業員の態度や、IT システムの不自然な利用（ログから判明）、他の従業員からの告発などがある。（製造業）
- 監査は定期的に行われており、IT 部門及び情報セキュリティ部門が半年毎に監査を実施している。アクセス記録などもこの監査時にはチェックしている。（非製造業）
- リスク管理及び情報管理部門が顧客情報管理について四半期毎に監査を実施している。（非製造業）
- 第三者監査や第三者モニタリングソフトウェア（第三者の行為を監視する）がしばしば利用される。（有識者）
- 監査自体は内部統制監査部門が対応している。（製造業）
- 監査は、取締役会決議された監査委員会規定に基づいて行われる。監査は、経営陣、内部監査部門、独立監査人によって定期的に行われる。（非製造業）
- 内部監査について、関係部門が定期的に行うが、情報漏えい、技術流出について責任を持つ法務部門自身は定期的な監査を独自には行っていない。（製造業）
- 情報漏えいなどの回避に役立つ対策として内部監査を行っており、経営陣は、何が起っているか、また、外部から入った情報などに関する監視を怠らない。そして我が社を保護するため潜在的な危険に対して必要な対策を取ります。また潜在的な危険を調査するために何度か外部の調査会社を活用したこともある。（製造業）

内部通報制度を秘密情報管理の一部として理解しているプラクティスもあった。当該企業においては、内部通報窓口の運用における通報者の保護に配慮しつつ、従業員相互の監視を重要な秘密情報管理手段として位置付けるというプラクティスが実践されていた。

【秘密情報管理としての内部通報制度（ヒアリング調査結果）】

- 通報者を守るため、匿名で報告ができるコンプライアンスホットラインを設けている他、電子メールにおいても個人を特定できないように報告ができる仕組みを導入している。被通報者による報復訴訟も米国では一般的に行われているため、通報者保護には特に配慮するようにしている。当社の対策が十分であるとは考えていないが、従業員が相互に監視する仕組み

によって 90%以上の確率で情報漏えいを検知できると考えている。（製造業）

（3）事後対応の実態

ヒアリング調査を実施した範囲では、情報漏えいないし技術流出が発生した場合の対応については、訴訟手続における秘匿特権[40]を確保する観点から、外部弁護士を関与させるといったプラクティスや、経営者がリーダーシップを発揮しつつ、法的措置を含めて厳しい態度で臨んでいくというプラクティスが見られた。

【事後対応の実態（ヒアリング調査結果）】

- 即座に不正調査チームを組織し、秘匿特権確保の観点から、外部弁護士の関与を原則とする。（製造業）
- 情報漏えいが発覚した場合の法的対応については、経営陣が意思決定を行う。（非製造業）
- 経営陣の責任としては、情報漏えいがあった場合に適切にメディア対応をする、事件による影響を最小化することである。更に必要な資源（ソフトウェア含む）を確保し、セキュリティマネジメントチームを全面的に支援することが必要である。（非製造業）
- 情報漏えいがあった場合、経営者が会社のイメージや顧客の不満解消についてリーダーシップを取る。（非製造業）
- 不正と思われる行為があった場合、FBI に報告するとともに、IT セキュリティ部門や当該データの管理者に報告し調査を行う。（非製造業）
- 事後調査に対応するため、従業員を解雇した場合も 6 ヶ月間は情報を保管する。（非製造業）

[40] 弁護士と依頼者間の秘匿特権（attorney-client privilege）のことであり、弁護士が依頼者とやり取りした秘密情報について訴訟手続などにおいて開示を拒否するコモン・ロー上権利のことである。米国においては、当該秘匿特権を行使できる秘密情報について民事訴訟における discovery の対象外となるなど、訴訟戦術上、重要な意義を有している。社内弁護士であっても、法的助言については秘匿特権の対象となるが、業務執行上のやり取りについては秘匿特権の対象とならないことから、社外弁護士を活用するというプラクティスがしばしば見受けられる。

Ⅵ. 秘密情報管理のポイント

本調査研究で実施したプラクティス調査の結果、改めて「正解」と呼ぶべきモデルないしスキームがある訳ではないことが確認された。

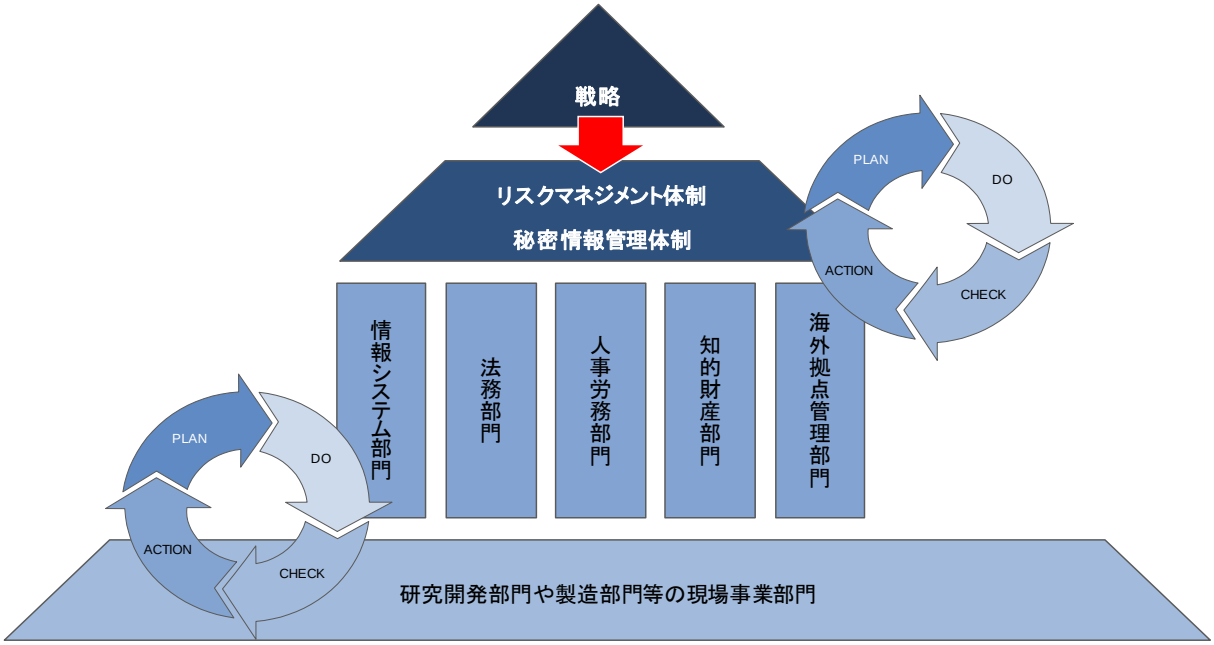
各企業のプラクティスには秘密情報管理に取り組む際に参考とすべきエッセンスが多数含まれている。ここでは、秘密情報管理のあり方を検討する際の参考となるよう、そのエッセンスを整理し、秘密情報管理を実践する際のポイントを示したが、あくまでプラクティスであり、各社の実情に合わせて最適な秘密情報管理体制を検討いただきたい。

１．秘密情報管理に係る体制

日本だけでなく海外においても、情報漏えいないし技術流出は重大なリスクの１つと捉えられており、全社的なリスクマネジメントの一環として捉えることが適切である。また情報漏えいないし技術流出リスクを軽減・最小化するために秘密情報管理を行おうとした場合、全社的な秘密情報管理体制の構築、物理的な管理、労務管理、取引先管理、グローバル拠点の管理といったように、様々な切り口からマネジメントと具体的な対策を行っていく必要があり、ベストプラクティス的な企業においてはこれらが相互に連携しながら取り組んでいることが改めて確認された。

この事を図式化すると、例えば以下のようなイメージとなる。すなわち、リスクマネジメントとは、企業の目的を実現するための経営手段の１つであり、目的実現に向けたリスクを最小化するマネジメントのことである。そのため、リスクマネジメントを担うリスク管理体制は、企業戦略に応じて最適な仕組みとすべきであり、必然的に全社横断的なものとなる。秘密情報管理については、情報システム部門、法務部門、人事労務部門、知的財産部門、海外拠点管理部門などのコーポレート部門、研究開発部門や製造部門といった事業部門が、全社的な秘密情報管理に係る方針や体制に基づいて、それぞれに PDCA サイクルを回しながら運用を徹底させていくことが肝要となる。

図 5：全社的なリスクマネジメントとしての秘密情報管理の位置づけ



（出所）三菱 UFJ リサーチ＆コンサルティング作成

上記のような秘密情報管理に係る体制を構築する上では、経営者が全社的なリスクマネジメントの観点から方針策定にコミットした上で、当該方針を実現するための体制及び規程の整備を行うことが重要となる。その際、社内の各種機能部門や事業部門を横断的にマネジメントする仕組みが必要となることから、この意味でも経営者のリーダーシップが求められる。また実際に施策を実施していくことをミッションとした推進役の設置が必要となるが、日本では既存の機能部門（例えば情報システム、法務、人事、知財など）の代表者が参加する会議体などにその機能を担わせつつ、事務局となる部署に企画調整機能を担わせたり、各事業部門に推進役を置くケースが散見された。

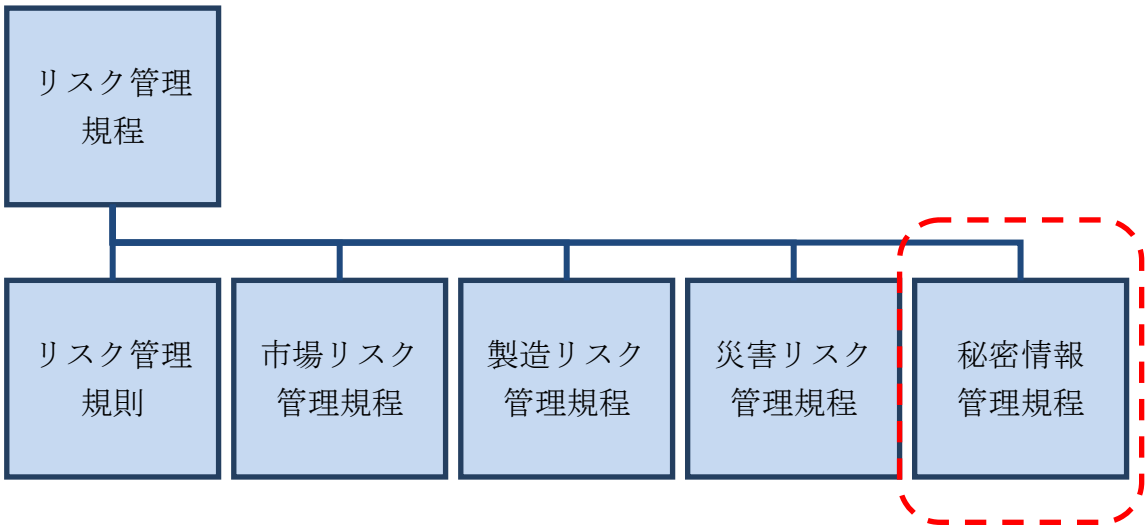
これに対して米国などでは、必ずしも組織横断的な委員会などを設置している訳ではないが、秘密情報管理について責任を持つ者（例えば法務部門長やチーフ・リスク・オフィサーなど）が取締役会メンバーであったり、上級執行役であることが一般的であったりすることが、秘密情報管理に必要な権限を持ち、経営目線でのマネジメント実施を可能にしているものと考えられる。米国では、経営に係る業務執行と監督がコーポレート・ガバナンスの仕組みとして分離されており、一般に独立取締役の比率が高い取締役会が監督機能を担い、業務執行は執行役が担っている（上級執行役は取締役を兼務し、取締役会メンバーとなることが少なくないが、CEO、COO、CFO など限られたメンバーに限られる）。業務執行を担う執行役は、株主総会で選任され、会社から委任契約の形で経営を任されている立場にあり、株主に対して法的な責任も負っている（執行役による業務執行の結果発生した会社の損害などについては株主代表訴訟の対象となる）ことから、個々の執行役の期待役割に対して必要な権限が付与されていることに加え、株主や独立取締役を中心とした取締役会によるガバナンス

が働いているといった事情も、こうした背景には存在している。日本企業と米国企業との間には、コーポレート・ガバナンス上の差異などがあることは間違いないが、米国などのプラクティスからも秘密情報管理に係る体制を考える上で、秘密情報管理について責任をもって取り組む組織ないし者に対して、業務執行上の重要事項として業務執行のトップである CEO などから必要な権限と仕組みを提供することが重要であるということが示唆されている。

日本企業の中でも委員会設置会社方式のガバナンス体制としている企業もあれば、秘密情報管理についてリーダーシップを発揮すべき担当役員などを指名して対応させているプラクティスが見られたように、米国のプラクティスも参考としつつ秘密情報管理体制を構築する方法もある。一方で、特定の組織や者に権限を集中させたり、社内横断的な取組に課題があるような場合には、委員会組織などを活用した横断的な会議組織やバーチャル組織を活用し、様々な関連部門を巻き込むことで、合意形成に力点を置いた日本企業において多く見られたプラクティスも大いに参考になるものと考えられる。

以上からすると、関連規程の整備や情報区分の考え方についても、全社的なリスクマネジメントの仕組みとリンクしていることが望ましい。関連規程の整備について言えば、日本企業及び米国などの企業においても散見されたように、リスク管理関連規程体系の中に秘密情報管理に係る規程を組み込んでいるというプラクティスの方が望ましい規程体系のあり方であると考えられる。

図 6：秘密情報管理規程のあり方の例



（出所）肥塚直人『「技術流出」リスクへの実務対応』（中央経済社）102 頁を参考に作成

２．物理的な管理

物理的な管理については、日本企業だけでなく海外企業においても、秘密情報管理を行う上で情報システム上のアクセス制御や情報機器についての管理が必要不可欠であるという認

識はほぼ共通して持っていることがうかがえるが、その程度感については一様ではなく、各社の実情に合わせた取組が行われているのが実態である。

ヒアリング調査を通じて得られたプラクティスから言える範囲の整理とはなるが、少なくとも、秘密情報についてのアクセス権を設定し、電子媒体で保有されている秘密情報へのアクセス制御や、紙媒体の保管管理などについては一般的に行われていると言えそうである。また情報機器、特にノート型パソコンや記録メディアなどの紛失・盗難による情報漏えい、技術流出についてもリスクファクターとして広く認識されており、これら情報機器については何らかの個体管理が行われている。

一方、日本企業に限らず、海外企業においても、一般的に実施されているとまでは言えないものの、物理的な管理手段として参考となるプラクティスを整理すると次のようなものがある。

【情報システムの管理】

- 電子メール誤送信防止ツールの活用
- Web サイトへの書き込みについて警告を発信するツールの活用
- 文書管理システムの活用
- サイバー攻撃に対する組織的な対応
- 特に秘密性の高い情報を扱う部門における専用のコミュニケーションツールの活用

【情報機器の管理】

- ノート型パソコンや USB などの記録メディア利用の制限及び管理
- ストレージサービスの利用制限及び管理

【紙媒体の管理】

- 外勤職員による誤配布防止の取組（書類に情報区分などを目立つように色分けしつつ表示するなど）
- 開示範囲の明示（閲覧が許される者の範囲を書類に明記するなど）
- 紙媒体で保管される秘密情報についての台帳管理
- 印刷・複製の制限及び管理
- 破棄ルールの明確化と徹底（溶解、シュレッダー処理など）
- 紙媒体を極力排除し、紙媒体で管理される秘密情報閲覧を制限（閲覧に法務部門長の許可を求めるなど）

【施設の管理】

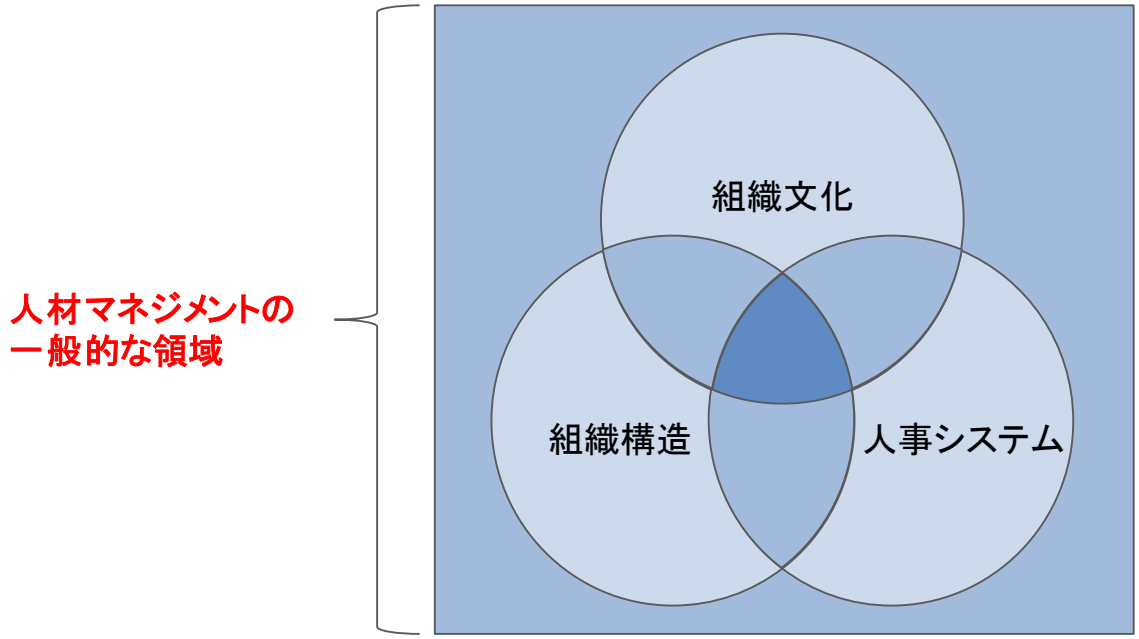
- 従業員でも職務や所属によって不必要な執務領域への侵入を制限する
- 時間帯によってゾーニング設定を変更する
- オフィスレイアウトを工夫し、死角をなくす
- 秘密情報の所在自体の秘匿

３．労務管理

既に紹介したように経済産業省が平成 24 年度に実施した調査においても「人を通じた」が情報漏えいないし技術流出が典型的な流出経路であることが示唆されていることからも、労務管理が秘密情報管理上も重要となることは間違いない。この点、米国などのプラクティスからも、同様の趣旨で労務管理の重要性が認識され、人事部門が秘密情報管理にコミットするケースが増えていることも本調査研究を通じて明らかとなった。

ヒアリング調査の中でも米国などでは人事部門のトップが上級執行役や取締役会メンバーとなっていることが多く、経営目線で対応を行うことができるという指摘もあったが、米国ではそもそも人事部門を人材マネジメント（Human Resource Management：HRM）部門と呼ぶことが多い。元来、HRM は、組織文化、組織構造、人事システムなどの領域を指す概念であり、人のマネジメントを通じて、企業の目的を実現するという意識が高いこともこうした背景にあるものと考えられる。

図 7：人材マネジメントの領域



（出所）三菱 UFJ リサーチ＆コンサルティング作成

ここで組織文化とは、人材マネジメントの３つの領域の中で最も抽象的な概念を取り扱う領域であり、定義についても様々なものがあるが、経営理念や価値観が定着し、当該経営理

念や価値観を行動規範として、従業員などが行動できることが重要な要素となる[41]。米国企業に対するヒアリング調査の中でも、「漏れなく報告をさせる風土ないし組織文化を醸成することの重要性」を指摘する声があったことは印象的であるが、日本企業においてもコンプライアンス実現のために組織文化が重要であることは比較的認識されている所であるが、秘密情報管理についても組織文化の促進が有効かつ必要であるものと考えられる。

組織構造については、本調査報告書では秘密情報管理体制という観点から取り扱っていることから、ここでは人事システム的な内容を含める形で労務管理という項目で整理を行っている。この点、従業員との秘密保持契約の締結について、今回ヒアリング調査を実施した範囲では、広く実施されていることが改めて確認された他、競業避止契約についても必要に応じてこれを活用するというプラクティスが散見された。また研修や人材育成の重要性についても今回ヒアリング調査を実施した範囲ではほぼ共通の認識となっていたと考えられるが、具体的な研修ないし人材育成プログラムについては試行錯誤しているのが実態となっている。

日本企業に限らず、海外企業においても、一般的に実施されているとまでは言えないものの、労務的な管理手段として参考となるプラクティスを整理すると次のようなものがある。

【従業員の採用】

・　バックグラウンドチェックを実施する。

【従業員との契約締結】

・　入社時、退社時のみならず、重要なプロジェクト参加時や R&D 部門配属時にも別途の秘密保持契約などを締結する。 ・　部門の性質に応じて、契約内容をカスタマイズした契約書を用いる。

【従業員に対するエンフォースメント】

・　懲戒処分の手続を明確化し、必要に応じて懲戒を行う。 ・　必要に応じて刑事及び民事訴訟の提起を行う。 ・　懲戒や法的措置の前に、警告を実施した場合、研修やカウンセリングの受講を義務付ける。

【研修・人材育成】

・　正社員以外の職員も研修の対象とする。 ・　リテラシー向上のための情報発信などを併せて行う。 ・　秘密情報を取り扱うプロジェクトや部署などに応じた研修を行う。

41 例えば、トム・ピーターズ＝ロバート・ウォータマン（大前研一訳）『エクセレント・カンパニー』（英治出版社、2003 年）44 頁、スティーブン P. ロビンス＝デービット A. ディチェンゾ＝メアリー・コールター（高木晴夫監訳）『マネジメント入門』（ダイヤモンド社、2014 年）51 頁、エドガー・H・シャイン（梅津祐良＝横山哲夫訳）『組織文化とリーダーシップ第 4 版』（白桃書房、2012 年）21 頁などの定義も参照。

・　年に複数回、ワークショップを実施し、意識変革を促す。

【退職者に対するフォロー】

・　転職先の把握と面談を実施する。 ・　備品と合わせて情報の返却を徹底する。 ・　退職予定者に対するアクセス権の制限やモニタリングを実施する。

４．取引先管理

取引先からの情報漏えいないし技術流出についても、日本企業であるか海外企業であるかを問わず懸念しており、パートナー企業管理の重要性については広く認識されていることが確認された。取引先との契約において、秘密保持条項を盛り込むというプラクティスは広く行われているが、パートナー企業の選定と調査・監査の実施まで行えているかについては企業によって温度差が見られた他、パートナー企業の管理についても温度差が見られた。

一方、日本企業に限らず、海外企業においても、一般的に実施されているとまでは言えないものの、取引先管理手段として参考となるプラクティスを整理すると次のようなものがある。

・　取引先の選定について適切な選定プロセスを設け、必要な事前調査を行う。 ・　必要に応じて相手企業における秘密情報管理体制について調査・監査を実施する。 ・　パートナー企業にも自社と同様の秘密情報管理体制を構築してもらえるよう、必要な支援を行う。

５．グローバル拠点の管理

国内外問わず、また企業の大小問わず、企業活動のグローバル化が進展する中、グローバル拠点の管理は重要なテーマの１つである。本調査研究において実施したヒアリング調査の中では、基本的に全世界統一のポリシーを策定し、ある程度当該地域の法令や制度などに応じてポリシーの現地化を行っているというのが実態である。

日本企業に限らず、海外企業においても、一般的に実施されているとまでは言えないものの、取引先管理手段として参考となるプラクティスを整理すると次のようなものがある。

・　グローバルで統一化されたポリシーを用いる際、もっとも秘密情報漏えいの懸念がある地域を基準としたポリシーとする。 ・　現地法人においては、法務部門や監査部門に比較的重要な役割を担わせ、定期的なミーティングにおいて潜在的なリスクの所在と対応方針などについて検討を行わせる。

６．情報漏えいに係る事後対応

日本だけでなく、海外においても情報漏えいないし技術流出事件は頻発しており、重大な問題であると認識されている。情報漏えいに係る事後対応の状況を見ていくと、不正を検知する仕組み、不正ないし不正の疑いが検知された場合に実態を正確に調査し、必要があればエンフォースメントを行っていけるよう必要な証拠を確保しておくことが重要であることが、本調査研究におけるヒアリングからも示唆されている。

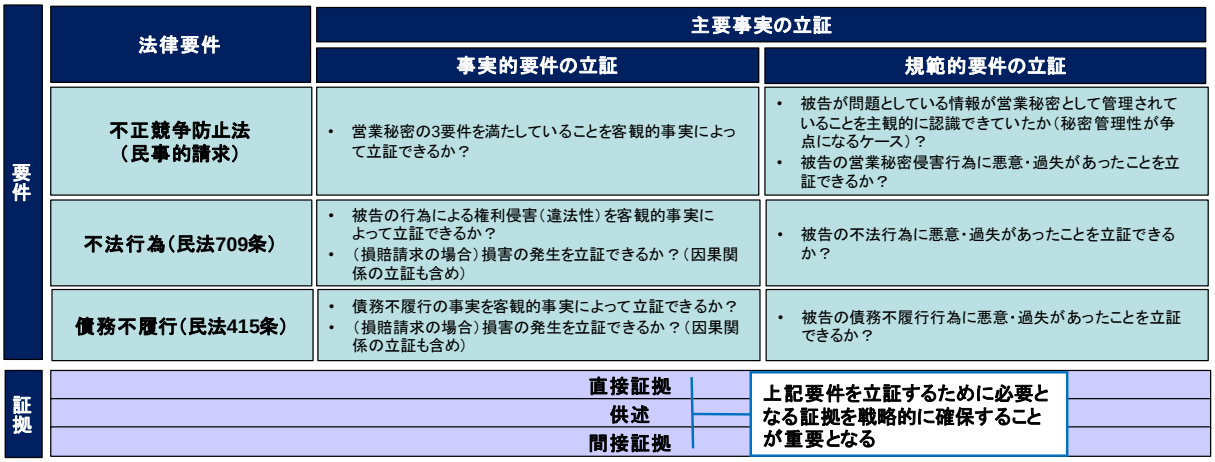
検知の仕組みとしては、情報システム上のアクセスログ（ファイルへのアクセスや外部との電子メールのやり取りなど）や、ヒアリング調査に回答頂いた企業の一部に見られたように、ゾーニング上のエリアアクセスログ（入退室ログなど）を１つの端緒として活用すべく、定期的なモニタリングを実施したり、退職予定者や特に重要な秘密情報に接する可能性がある者について重点的なモニタリングを行ったりすることは検討に値する。

内部監査についても社内ルールを徹底させる手段であると同時に、不正の端緒を検知する効果も期待できる。多くの企業では内部統制監査の一環として、又は内部統制監査と同時に秘密情報管理体制についての監査を実施しているようである。また必要に応じて社内調査を実施することがあるが、米国などの企業ではフォレンジック会社などの活用も進んでいるようであり、調査手法の１つとして参考となる。

事後対応として、従業員に対する懲戒処分や、従業員や元従業員、第三者に対して訴訟提起をするといった場合には、訴訟上有効と思われる証拠を迅速に収集することが重要となる。米国企業では訴訟対策を意識した文書管理が行われているプラクティスも散見された他、証拠収集にもフォレンジック会社を活用するプラクティスが見られた所である。日本企業においては、米国企業に比べると訴訟に直面する場面が少ないことなどから、この点についての意識や文書管理は若干遅れているようにも見受けられるが、秘密情報管理がリスクマネジメントの一環であることを惹起すれば、リスクが顕在化した場合に重大な影響を及ぼすような秘密情報についてはメリハリをつけた上で十分な事前準備を行っておくことが肝要であろう。

事前準備を行う際、費用対効果はもちろんであるが、関係しそうな情報を全て保存していくのではなく、例えば訴訟になった場合にどのような立証が必要となるのかといった観点から、必要とされる証拠を定義し、優先順位をつけて管理を行っていくことも重要となると考えられる。また米国など海外での訴訟リスクも高い企業においては、当該国における訴訟制度も視野に入れた管理が行えることが望ましいと考えられる。

図 8：訴訟において立証が必要となる事項と証拠



（出所）三菱 UFJ リサーチ＆コンサルティング作成

（様式２）

二次利用不可リスト

営業秘密管理の実態に関する調査研究　報告書

平成２６年度産業経済研究委託事業

三菱UFJリサーチ＆コンサルティング株式会社

頁	図表番号	タイトル
3	表１	国内における主な情報漏えいの事案
4	表２	米国における主な情報漏えいの事案
15	図１	秘密情報管理の関連規程の位置づけ例
17	図２	情報区分の例
30	図３	ゾーニングの例
33	図４	韓国企業における記録メディア持ち出しの事案
37	表３	営業秘密の侵害行為の行為者・企業に対する対応
41	表４	営業秘密の漏えい者の種別
62	表５	米国企業の売上規模別に見た法務部門人員数
112	図５	全社的なリスクマネジメントとしての秘密情報管理の位置づけ
113	図６	秘密情報管理規程のあり方の例
115	図７	人材マネジメントの領域
119	図８	訴訟において立証が必要となる事項と証拠