RISK SOLUTIONS REPORT

2015年
Winter
VOL.10

企業における情報漏洩の現状と対策
—漏洩リスク低減のための情報資産管理—

銀泉株式会社
GINSEN RISK SOLUTIONS 銀泉リスクソリューションズ株式会社

企業における情報漏洩の現状と対策

－漏洩リスク低減のための情報資産管理－

はじめに

企業における情報資産の管理のあり方が、企業価値の維持や向上のための重要な要素になりつつあります。直近では、大手半導体メーカーの業務提携先の技術者による最先端の技術情報漏洩や、大手通信教育会社の顧客情報漏洩などが発生しています。最先端の技術情報が漏洩した場合は競争力の低下を招き、また顧客から預かった情報を流出した場合は損害賠償をはじめとする直接的な損失に加え、長年にわたり築き上げた信用やブランドが一瞬にして失墜し、企業経営に大きな影響を与える重大な事態となる可能性もあります。

これらの営業秘密漏洩事件により、改めて自社の情報管理の状況を見直した企業も多かったのではないでしょうか。

そこで、本レポートでは、営業秘密漏洩の現状及び情報管理の進め方に関する基本的な考え方について検討してみたいと思います。

第１章では、不正競争防止法における営業秘密の要件を述べるとともに、退職者や委託先企業の従業員等の人を通じた営業秘密の流出が大きな問題になっていることを踏まえ、経済産業省の「人材を通じた技術流出に関する調査研究報告書」により営業秘密の漏洩の状況について確認します。

第２章では、直近の技術情報漏洩事例および顧客情報漏洩事例により、事案の背景と情報管理対策の課題について考えてみます。

第３章では、具体的な営業秘密漏洩対策について、組織的管理・人的管理・物理的管理・技術的管理に分けて検討します。

企業の競争力や信用に大きな影響を与える情報漏洩対策は、企業の経営課題の一つであるといえます。本レポートが、情報管理におけるリスクマネジメントの何らかのヒントとなり、更なる対策のきっかけとなれば幸いです。

第1章　企業における営業秘密漏洩の現状

第１章では、企業における情報漏洩の現状について説明します。まず不正競争防止法における「営業秘密」とは何かについて確認し、経済産業省が2012年に行った調査結果「人材を通じた技術流出に関する調査研究報告書（以下、「報告書」）」及び「同報告書別冊（以下、「アンケート調査結果」）」[1]により営業秘密漏洩の実態について確認します。

１．情報セキュリティにおける情報漏洩

営業秘密漏洩について説明する前に、情報セキュリティにおける営業秘密漏洩の位置付けについて確認しておきます。

一般に情報セキュリティ事故には、システム停止、コンピュータウィルス感染、不正アクセスなどがありますが、経営に大きな影響を与えるのは、やはり営業秘密の漏洩です。

情報セキュリティとは、狭い意味では、電子的な手段を利用した情報のやり取りに関する安全性や信頼性の確保のことを言うこともあります。しかし、情報セキュリティマネジメントシステムに関する用語及び定義について規定した規格 JISQ27000によると、企業の情報システムを取り巻くさまざまな脅威から、情報資産を機密性・完全性・可用性（三大要素）の確保を行いつつ、正常に維持することであると定義されており、「電子的」な範囲に限られているわけではありません。

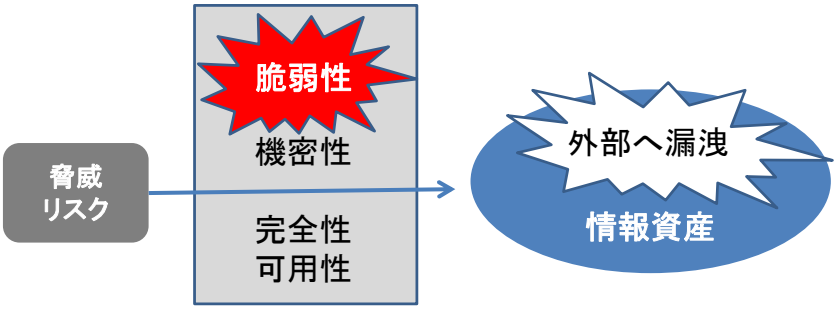
> ①　機密性：その情報にアクセスすることが認められた者だけが、その情報にアクセスすることができる状態を確保すること、認可されていない者には情報を非公開にして使用させないこと
> ②　完全性：その情報が破壊や改ざん又は消去されないで完全な状態を確保すること
> ③　可用性：その情報にアクセスすることを認められた者が、必要な時に速やかにその情報や資産にアクセスできる状態を確保すること

機密性：Confidentiality 、完全性：Integrity、可用性： Availability は、その頭文字を取って、情報のＣＩＡと呼ばれます。したがって、情報セキュリティとは情報のＣＩＡを維持することであると言い換えることもできます。守るべき対象は「情報セキュリティ目的に影響を与える情報と情報処理施設に関連する資産」であり、それらの侵害、情報漏洩を防ぐことにより、企業経営を守ることが情報セキュリティであるといえます。

本レポートのテーマである情報漏洩問題は、情報セキュリティの三大要素のうち「機密性」に関わる問題であるといえます。

[1] 信用調査会社の企業データベースから抽出した企業１万社（製造業・非製造業）に対して2012年に調査を実施し、3,011 社から回答があった。（回収率30.1%）

図表1-1　情報セキュリティ　イメージ



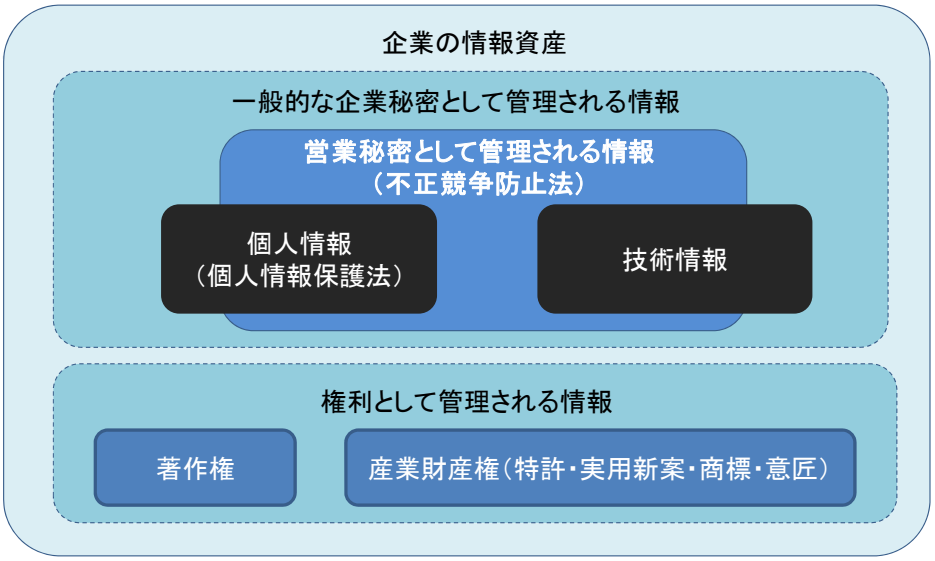
２．営業秘密とは何か

（１）企業の情報資産

企業経営にとって役立つさまざまな要素や能力のことを「経営資源」と呼びます。情報は、ヒト、モノ、カネと並び四大経営資源と呼ばれています。知識社会の進展に伴い、無形資産である情報資産が重要視されるようになってきているからです。これら情報資産は、顧客から預かった情報（個人情報、営業情報、購買情報、生産情報など）、顧客に提供する予定の情報（作成中の設計書、開発中のプログラムなど）、会社固有の情報（技術情報、顧客情報、経営情報、財務情報、営業ノウハウ、取引情報、人事情報など）とその内容は多岐にわたります。

また、これら企業の保有する情報資産を、その管理方法によって整理したものが図表1-2です。

図表1-2　企業の情報資産



このうち、著作権と産業財産権は権利化され公開されていますが、他は非公開です。競争の激しい半導体産業などは、特許を公開すると、その特許を迂回する形で類似品を製造される恐れがあります。そのため、敢えて特許を取得せず、非公開の営業秘密として管理するケースも増えてきています。

（２）営業秘密の三要件

次に、情報資産のうち、不正競争防止法における「営業秘密」とは何かについて確認します。

日本の不正競争防止法は、民法の特別法として、「営業秘密」に該当する情報を不正に取得、開示または使用する行為を「不正競争」の一類型と定め、このような行為の差止請求権や営業秘密が記載された資料等の廃棄請求権及び損害賠償請求権を定めています。

不正競争防止法第2条第6項は、営業秘密を「秘密として管理されている〔①秘密管理性〕生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報〔②有用性〕であって、公然と知られていないもの〔③非公知性〕をいう。」と定義しており、同法に基づく保護を受けるためには、この三つの要件全てを満たすことが必要となります。不正競争防止法に基づく「営業秘密管理指針」には、次のように説明されています。

① 秘密管理性（秘密として管理されていること）

秘密管理性が認められるためには、事業者が主観的に秘密として管理しているだけでは不十分であり、客観的にみて秘密として管理されていると認識できる状態にあることが必要です。これまでの裁判例では、①当該情報にアクセスできる者を制限する（アクセス制限）とともに、②同情報にアクセスした者にそれが秘密であることを認識できるようにしていること（客観的認識可能性）が必要とされています。裁判例では、事業規模、業種、情報の性質、侵害態様等を踏まえ、秘密管理の合理性が総合的に判断されています。

② 有用性（事業活動に有用な情報であること）

有用性についても、保有者の主観によって決められるものではなく、客観的に有用である必要があります。この有用性とは、競争優位性の源泉となる場合を含め、そもそも当該情報が事業活動に使用されたり、または使用されることによって費用の節約、経営効率の改善等に役立ったりするものであることを意味し（事業への活用性）、裁判例では、「財やサービスの生産、販売、研究開発に役立つなど事業活動にとって有用なもの」であることが必要とされます。直接ビジネスに活用されている情報に限らず、間接的な（潜在的な）価値がある場合も含み、例えば、いわゆるネガティブ・インフォメーション（ある方法を試みてその方法が役立たないという失敗の知識・情報）にも有用性は認められます。

現在の事業に活用できる情報だけなく、将来（近未来も遠い未来も含む。）の事業に活用できる情報にも有用性が認められ得ます。

③ 非公知性

非公知性が認められるためには、当該情報が刊行物に記載されていないなど、保有者の管理下以外では一般に入手できない状態にあることが必要です。

具体的には、書物、学会発表等から容易に引き出せることが証明できる情報は、非公知情報とは言えません。

他方、人数の多少にかかわらず、当該情報を知っている者に守秘義務が課されていれば、非公知情報といえます。さらに、同じ情報を保有している者が複数存在する場合であっても、各自が秘密にしているなどの事情で当該情報が業界で一般に知られていない場合には、非公

知情報であると考えられます。

（３）営業秘密保護要件の見直し動向

営業秘密漏洩の訴訟となった場合、これら３つの要件の中でも、特に、①秘密管理性が争点となる事例が多くなっています。例えば、「秘」という印を付けた情報でも、社内の誰でも閲覧や入手ができる状態を放置していた場合、「秘」という表示に対応した扱いをしていないため、営業秘密として保護されない可能性があります。また、情報について単にパスワードを用いて管理するだけでは秘密管理が不足していると判断されることもあります。したがって、企業にとって極めて重要な内部情報が漏洩しており、その情報についてある程度の秘密管理がなされている場合であっても、必ずしもその情報が不正競争防止法の下で保護されるとは限りません。これでは、これまで投資してきた資金や関係者の努力が無駄になってしまいます。

このような状況を鑑みて、不正競争防止法で「営業秘密」として認められるための要件について、現在、経済産業省 産業構造審議会 知的財産分科会 営業秘密の保護・活用に関する小委員会で議論が進められています。2014年10月31日に開催された第2回委員会資料によると、従業員が秘密であると認識できる程度に客観的に管理がされていれば、営業秘密とみなす考えが提示されており、営業秘密の要件が緩和される可能性があります。

不正競争防止法の営業秘密と認められれば、その営業秘密が不正利用等された場合に差止請求や損害賠償請求などの法的措置を採ることが可能となります。

また、併せて、不正競争防止法の見直し作業も進められています。日本では、営業秘密が不正に流出した場合、アメリカや韓国などの知的財産保護法制と比べて刑事罰に問える範囲が狭いこと等が情報を狙われやすい要因になっているとして、産業界から規制の強化を求める声が出ていました。11月27日に開催された第3回委員会資料によると、罰則の強化に加え、営業秘密を盗もうとした未遂の場合でも刑事罰に問えるようにすることや、被害を受けた企業の告訴が無くても起訴できるようにする非親告罪化、被害を受けた企業が民事の損害賠償訴訟を起こす際の立証責任の緩和などが改正案に盛り込まれる予定です。

３．営業秘密漏洩の現状

（１）営業秘密漏洩の状況

2014年には内部不正による営業秘密の漏洩事件が相次ぎました。報道された主な事件は、図表1-3のとおりです。これら公開されている事件は氷山の一角にすぎず、裁判に至らないものや社内や当事者間で処理された事件は多数存在すると思われます。また、情報の流出自体を企業が認識・把握していないケースも少なくないと思われます。

以下、実際に営業秘密の漏洩についてどのような状況なのか、経済産業省の調査結果により概観してみます。（各設問項目は複数回答式なので、合計値は100％になりません。）

図表1-4によると、全体のうち13.5%[2]の企業が、過去5年間で、人を通じた何らかの営業秘密の漏洩が「あった」と回答しています。

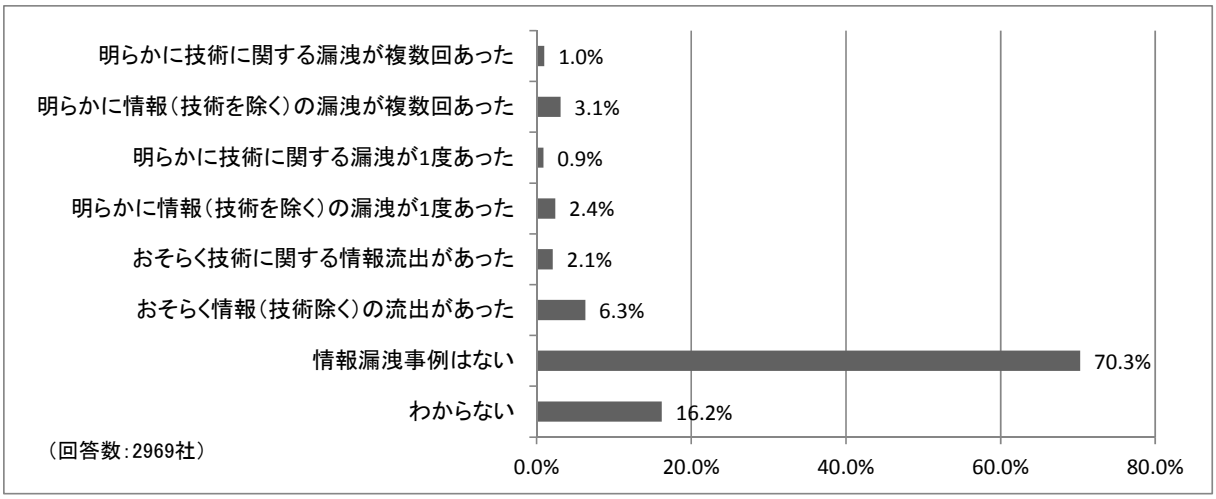
[2] 100％から「情報漏洩はない70.3％」及び「わからない16.2％」を差し引いた数値。

図表1-3 2014年に報道された主な営業秘密漏洩事件

報道月	事件の概要	不正行為者	動機
2014年2月	A銀行のATMの保守管理業務を受託しているB社の元社員が、ATMの取引データから顧客のカード情報を不正に取得し、偽造キャッシュカードを作成・所持した容疑で逮捕された。	委託先社員（技術者）	金銭の取得
2014年3月	C社の業務提携先であるD社の元社員が、C社の機密情報を不正に持ち出し、転職先の韓国E社に提供したとして、不正競争防止法違反の容疑で逮捕された。	業務提携先の退職者（技術者）	処遇（給与等）の不満
2014年5月	F社の元社員が退職する直前、同社のサーバーにアクセスし、販売計画など営業上の秘密を不正に得ていたとして不正競争防止法違反の疑いで逮捕された。	退職者	金銭の取得（容疑否認）
2014年5月	国立国会図書館のネットワークシステム保守管理の委託を受けているG社の社員が、システムにアクセスできる権限を悪用して国会図書館が発注していた入札情報などを不正に入手し、営業担当の社員に送付していた。	委託先社員（ｼｽﾃﾑｴﾝｼﾞﾆｱ）	受注活動を有利にするため
2014年7月	H 社の顧客データベースを保守管理するグループ会社の業務委託先の元社員が、大量の顧客情報を流出させたとして不正競争防止法違反の疑いで逮捕された。	委託先社員（ｼｽﾃﾑｴﾝｼﾞﾆｱ）	金銭の取得

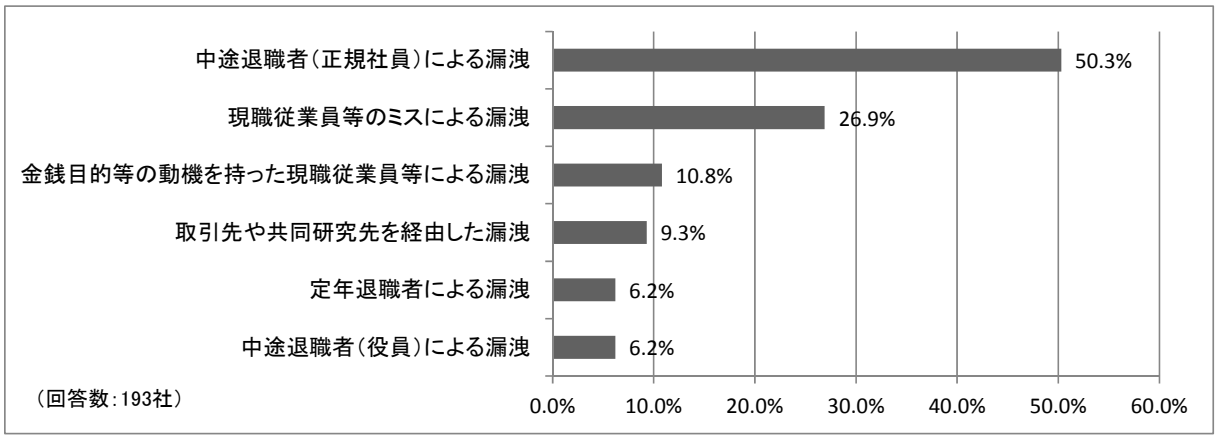
（出所）情報処理推進機構（IPA）資料を一部編集

図表1-4 過去5年間での人を通じた営業秘密の漏洩状況



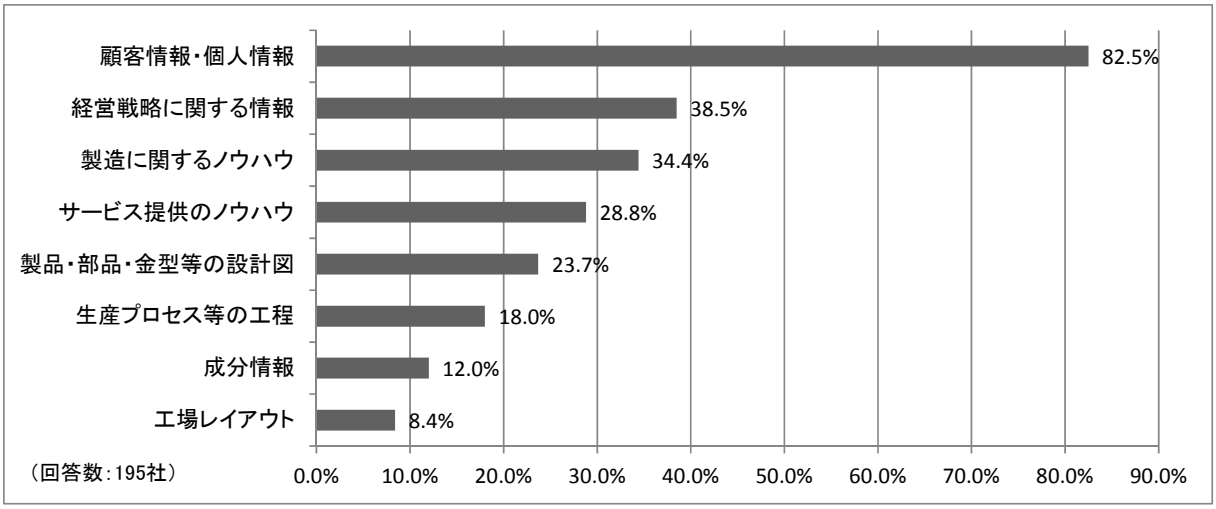
（出所）経済産業省「人材を通じた技術流出に関する調査研究報告書 別冊」より作成（以下、図表1-8まで同じ）

図表1-5 営業秘密の漏洩者



営業秘密の漏洩者は、「中途退職者（正規社員）」が50.3%と最も多くなっており、同様に退職した関係者では「定年退職者」「中途退職者（役員）」がそれぞれ6.2%となっています。およそ6割が退職者からの情報漏洩となっています。また、「金銭目的等の動機を持った現役従業員等による漏洩」が10.8%発生しており、これらを合計した内部者からの漏洩は、7割を超えます（図表1-5参照）。また、人を通じて漏洩した営業秘密の内容としては、「顧客情報・個人情報」が82.5%と最も多く、「経営戦略に関する情報」が38.5%、「製造に関するノウハウ」が34.4%と続いています（図表1-6参照）。

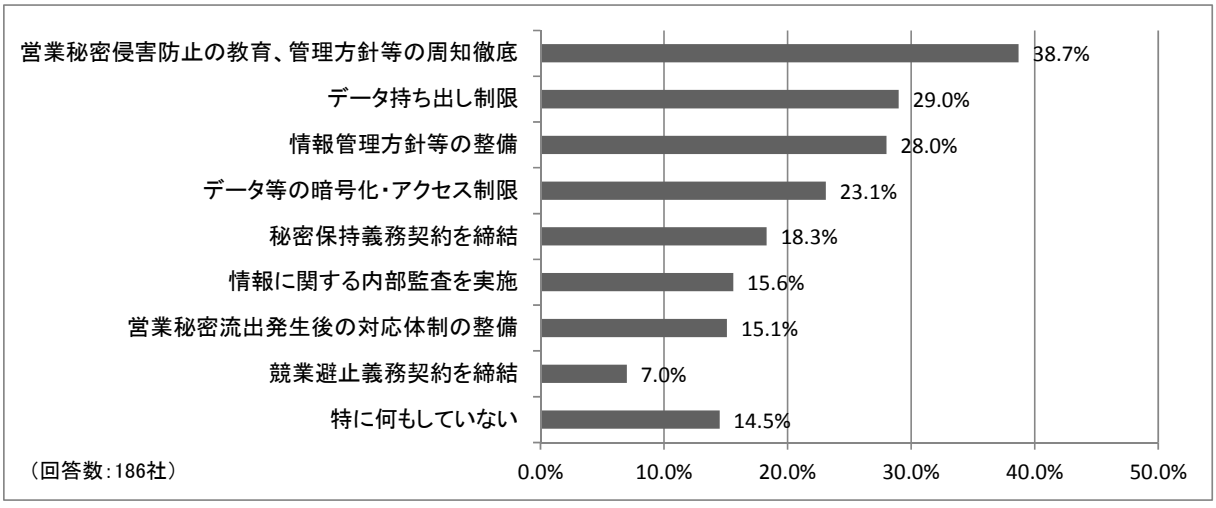
図表1-6 人を通じて流出した情報の種類



（２）営業秘密漏洩後の対策

営業秘密の漏洩が生じた後に、その再発を防止する対策として強化または新たに導入した対策に関しては、「データ等の持ち出し制限を行った」、「データの暗号化・アクセス制限を行った」との回答を合計すると52.1%と最も多くなり、「営業秘密侵害防止の教育、管理方針等の周知徹底を行った」が38.7%、「情報の管理方針等を整備した」が28.0%であり、規程や契約関係については、「秘密保持契約を締結するようになった」が18.3%、「競業避止契約を締結するようになった」が7.0%となっています（図表1-7参照）。

図表1-7 営業秘密漏洩後の再発防止策

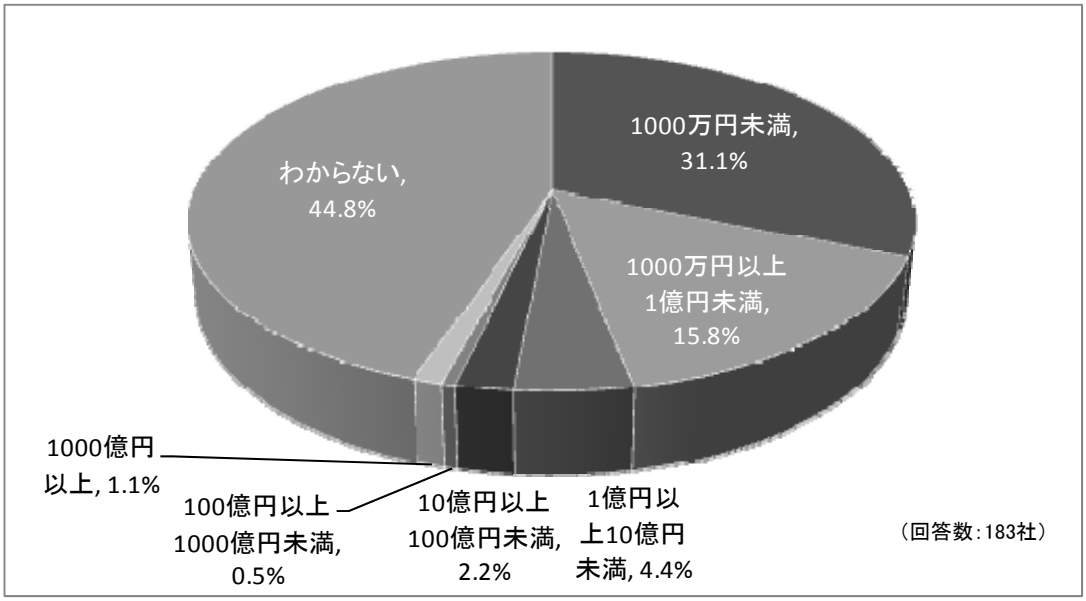


４．営業秘密漏洩による経済的損害

不正競争防止法第5条第2項には、賠償請求における損害の額については、侵害した者がその行為によって受けた利益の額を侵害された者が受けた損害の額と推定されると規定しています。しかしながら、営業秘密漏洩と損害額の因果関係を明確にするのは容易ではありません。

アンケート調査結果を見ても、営業秘密漏洩の損害額は、「わからない」が44.8%を占めています。一方で、100億円以上の損害額を推定している企業も少数（1.6%）ではありますが存在します。以下、技術情報と顧客情報のそれぞれの漏洩のケースにおける経済的損害について見てみます。

図表1-8　人を通じた営業秘密の漏洩による損害



（１）技術情報漏洩による経済的損害

図表1-9は、近年の主な技術漏洩事例とその後の漏洩先企業及び漏洩者への対応をまとめたものです。この表から分かるとおり、技術情報が漏洩しても、漏洩先の企業を相手に民事損害賠償請求を起こすケースは多くありません。

図表1-9　直近の技術情報漏洩事件とその後の対応

年（起訴時期等）	漏洩した技術情報	流出先	漏洩先企業・漏洩者への対応
2012年	工作機械（旋盤）の図面情報	企業への流出なし	・漏洩者→刑事訴訟（一審判決：懲役2年、執行猶予4年、罰金50万円）
2012年	方向性電磁鋼板技術	韓国企業	・漏洩先企業→民事訴訟（約1,000億円の賠償請求中）
2012年	自動車用エンジン部品等を製造するプレス機の設計図	中国企業	・漏洩者→刑事告訴（懲役2年、執行猶予3年、罰金100万円）
2014年	NAND 型フラッシュメモリーの製造技術	韓国企業	・漏洩先企業→民事訴訟（約1,091億円の賠償請求⇒330億円で和解し協業） ・漏洩者→刑事告訴（公判中）
2014年	自動車の販売計画等	国内企業	・漏洩者→刑事告訴（処分留保）

（出所）経済産業省資料より作成

これは、訴訟を提起した場合、営業秘密の侵害についての立証責任は原告にあり、裁判に長い時間と労力が掛かることが想定されるからです。また、一旦、訴訟を提起しても、和解により訴訟を取り下げたり、更に漏洩先企業と協業するケースもあります。半導体製造技術のような技術変化の激しい事業環境下におけるグローバル市場での競争を考えた場合、消耗的な訴訟にこだわるより、ある程度の和解金を受領して、協力を通じて技術競争力を確保することが企業の利益となると判断されるケースもあるからです。

（２）顧客情報漏洩による経済的損害

次に、顧客情報を漏洩した場合の経済的損害について見てみます。顧客情報の漏洩が起こってしまった場合の、企業の責任について確認しておきます。個人情報保護法は、個人の権利や利益を保護するために、個人情報を取り扱う事業者に対し適切な取扱いを求めた法律であり、行政上の責任を定めたものです。情報漏洩による損害賠償責任は民法の規定によります。顧客情報を漏洩した場合、漏洩した情報の本人[3]に対し、民法上の不法行為として損害賠償責任を負います。漏洩による被害がある場合はもちろん、被害が無くても漏洩したという事実により慰謝料などの損害賠償責任を負います。

実際には、訴訟にまで持ち込まれるケースは多くなく、大半の事案が、補償金の代わりとして商品券等のお詫びの金品を配布するという自主的な対応を行うことで終わっています。これは、被害者が訴訟に持ち込む前に企業側の誠意を示すことで顧客からの信頼を回復するという目的もあり、その支払いの有無、金額の多寡は、各企業の判断に委ねられています。しかしながら、このような商品券等の配布は、被害者への損害賠償請求権自体を消滅させるものではありません。

顧客情報の漏洩事故による損害賠償額等（慰謝料・補償金等を含む）についての事例を見てみると、一人あたり500円から数万円程度まで幅広く存在しています。個人の機微な情報（あまり他人に知られたくはない情報）の場合や、顧客リストとして価値があり、勧誘電話が掛かってくるなどの被害が発生している場合などは、高額となるケースもあります。

顧客情報の漏洩等のケースでは、一人ひとりについての損害賠償額等はそれほど大きくならないものの、電子データの場合、一度に大量の顧客情報が漏洩することも少なくなく、トータルでは大きな損害賠償額になってしまいます。仮に100万人の顧客情報が漏洩し、一人当たり500円のお詫びをする場合、それだけで5億円の費用となります。

1999年に発覚した自治体の住民基本台帳データの漏洩事件に係る判決は、個人情報漏洩に関する損害賠償支払い命令が出た判決としては初めてのもので、その後の裁判やお詫びの金品の水準に大きな影響を与えたとされています。当該自治体の乳幼児健診システムの開発を担当していた民間のシステム会社のアルバイト社員が、住民基本台帳データを不正にコピーして持ち出し、名簿業者に売却した事件です。漏洩したデータは、個人の住基番号・住所・氏名・性別・生年月日・世帯主・続柄等でした。最高裁まで争った結果、損害賠償額は、慰謝料10,000円、弁護士費用5,000円と認定されました。実際に訴訟を起こした提訴者は3人であったため賠償額は45,000円と少額ですが、現在では、当時と比べて市民の権利意識も高くなっており、仮に漏洩した22万人の0.1%が訴訟に参加すれば、220人となり、損害賠償額は、990万円となります。1%であれば、1億円近い

[3] 個人情報保護法では、例えば、「Ａさんの個人情報」について、Ａさんのことをその情報の「本人」と呼ぶ。

賠償額となります。

また、昨今ではお詫びの金品の水準は500円が一つの目安となっていますが、証券や保険など一般の業種より社会的責任が強く求められる業種においては、一人当たり10,000円の商品券を配布するなど、金額水準が高くなっています。

図表1-9 顧客情報漏洩・流出事件の損害賠償額・お詫びの金品

年	業種	概要	漏洩人数	1人当たり 損害賠償額/お詫びの金品
1998年	大学	講演参加者名簿を警察に提供	約1,400人	慰謝料5,000円 ※1
1999年	自治体	住民基本台帳データ流出	約22万人	慰謝料10,000円 弁護士費用5,000円 ※2
2000年	エステサロン	顧客情報流出	約5万人	慰謝料30,000円 弁護士費用5,000円 ※3
2003年	コンビニエンスストア	カード会員情報流出	約56万人	5,000円（商品券）
2003年	コンビニエンスストア	カード会員情報流出	約18万人	1,000円（クオカード）
2004年	インターネットプロバイダ	会員情報流出	約650万人	500円（商品券）
2004年	同上	同上	約650万人	各社慰謝料4,500円 ※4 （本件は漏洩した企業が2社あった）
2004年	カード	顧客情報流出	約48万人	500円（商品券）
2005年	アミューズメント施設	年間パスポート個人情報流出	約12万人	500円（商品券）
2009年	証券	顧客情報流出	約5万人	10,000円（商品券）
2009年	保険	顧客情報流出	約1万8000人	10,000円（商品券）
2013年	小売	不正アクセスによりカード情報流出	約1万2000人	1,000円（クオカード）
2014年	通信教育	顧客情報流出	約2,895万人	500円（電子マネー/図書カード/寄付）

※1 最高裁 平成15年9月12日判決
※2 最高裁 平成14年7月11日判決
※3 東京高裁 平成19年8月28日判決
※4 最高裁 平成19年12月14日判決
（出所）各種情報をもとに当社作成

（２）モデルによる想定損害賠償額

これらの賠償金やお詫びの金品の金額水準の計算にルールがあるわけではありませんが、日本ネットワークセキュリティ協会（ＪＮＳＡ）では、独自の想定損害額算出モデルである「ＪＯモデル（JNSA Damage Operation Model for Individual Information Leak）」を発表しています。

図表1-10 2012年 個人情報漏洩インシデント 概要データ[4]

漏洩人数	972万65人
インシデント件数	2,357件
想定損害賠償総額	2,132億6,405万円
一件あたりの漏洩人数	4245人
一件あたりの平均想定損害賠償額	9,313万円
一人あたりの平均想定損害賠償額	4万4,628円

（出所）日本ネットワークセキュリティ協会
「2012年情報セキュリティインシデントに関する調査報告書～個人情報漏洩編～」

このモデルに基づいた、2012年の個人情報漏洩インシデント[5]における被漏洩者一人あたりの平均想定損害賠償額は、44,628円となっています（図表1-10参照）。これ以外にも、原因調査費用、弁護士費用、謝罪広告費用なども必要になります。

また、情報漏洩対策が不十分であるために、情報漏洩事故を引き起こしてしまった場合には、直接的な経済的損失に加えて、企業としての信用・イメージをも損ない、ブランド価値を毀損してしまう可能性があります。情報漏洩対策は、単に重要な情報の流出、紛失を防ぐためだけでなく、企業のリスクマネジメントにおける大きな課題であるといえます。

[4] 「一件あたりの漏洩人数」及び「一件あたりの平均想定損害賠償額」は被害者数が不明のインシデント67件を除外して算出している。また、「一人あたりの平均想定損害賠償額」はインシデントごとに一人あたりの想定損害賠償額を推定し、その後、全てのインシデントの一人あたりの想定損害賠償額を用いて平均額を算出しているため、想定損害賠償総額を単純に漏洩人数で割った値とは一致しない。

[5] インシデントとは、情報セキュリティ分野では、情報管理やシステム運用に関して保安上の脅威となる現象や事案のことを指す。具体的には、ウィルス感染や不正アクセス、情報漏洩、メール誤送信などが含まれる。

■ＪＯモデルによる損害賠償額の計算

日本ネットワークセキュリティ協会（JNSA）では、個人情報漏洩における損害賠償について、過去の情報漏洩事件・事故の分析・プライバシー権や名誉棄損の判例分析等に基づき、独自の想定損害額算出モデルである「JOモデル（JNSA Damage Operation Model for Individual Information Leak）」を発表しています。本モデルによる損害賠償額の算出式は以下のとおりです。

損害賠償額＝漏洩個人情報価値　×　社会的責任　×　事後対応評価

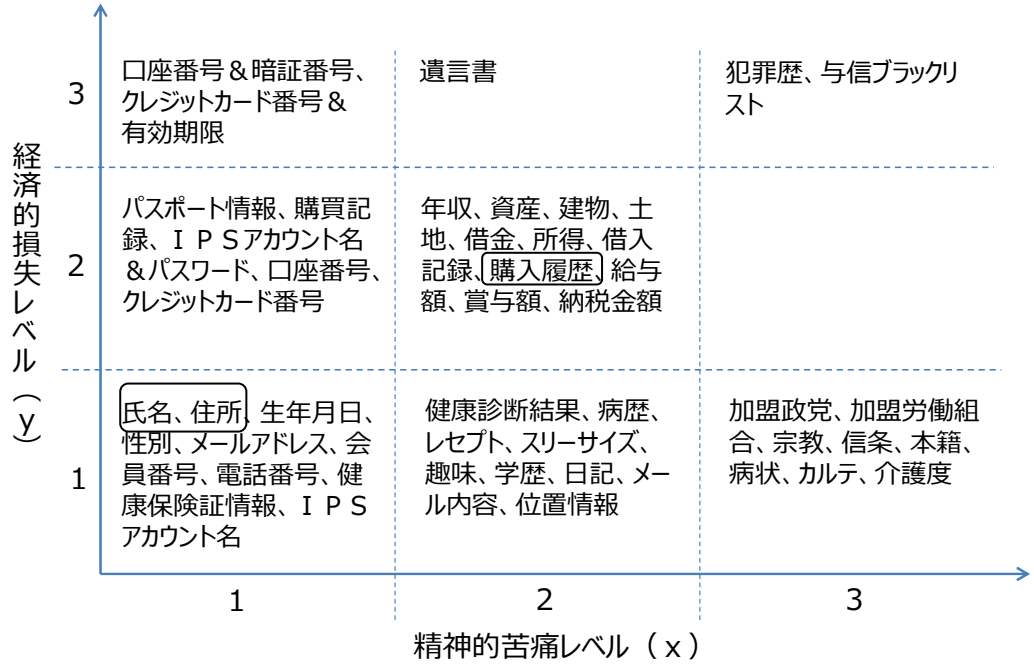
ここで、漏洩個人情報価値＝基礎情報価値×機微情報度×本人特定容易度　とすると

＝基礎情報価値　[500円]
×機微情報度　[$10^{x-1}+5^{y-1}$]
×本人特定容易度　[6、3、1]
×社会的責任度　[2、1]
×事後対応評価　[2、1]

x＝漏洩した情報の精神的苦痛レベルの最大値
y＝漏洩した情報の経済的損失レベルの最大値

漏洩した情報に対して、経済的な損失レベルと精神的苦痛レベルの 2 つの軸で評価を行います。

●機微情報度（抜粋）



●本人特定容易度

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所・電話番号」が含まれること。	3
特定困難。上記以外	1

●社会的責任度

判定基準	社会的責任度
一般より高い：適正な取り扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）及び、知名度の高い大企業、公的機関。	2
一　般　的：その他一般的な企業及び団体、組織。	1

●事後対応評価

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

適切な対応行動例	不適切な対応行動例
すばやい対応、被害状況の把握、インシデントの公表、状況の逐次公開、被害者に対する謝罪、クレーム窓口の設置、漏洩情報の回収、顧客に対する補償、原因の追究、セキュリティ対策の改善	指摘されても放置したまま、対応が遅い、繰り返し発生、対策を施したが有効でない、虚偽報告

【損害賠償額計算例】

・一般企業において、氏名、住所、購入履歴のあるデータが漏洩した場合の賠償額

１人あたりの賠償額　＝　500　[基礎情報額]
×$10^{2-1}+5^{2-1}$ [購入履歴の機微情報度：ｘ＝2、ｙ＝2]
×6　[本人特定容易度]
×1　[社会的責任度：一般企業]
×1　[事後対応適切]
＝45,000円

機微情報度は、
住所、氏名は、ｘ＝1、ｙ＝1ですが、
購入履歴は、ｘ＝2、ｙ＝2なので、
大きい数値である、ｘ＝2、ｙ＝2　を採用

・漏洩件数：10,000人とすると
45,000円×10,000人＝4億5,000万円

※実際には、個人情報を漏洩された全員が訴訟に参加するわけではありません。
正式なデータがあるわけではありませんが、訴訟参加率は、0.1～5%程度でシミュレーションされることが多いようです。

第2章　営業秘密漏洩に関する事例

第２章では、直近に発生した営業秘密漏洩事例により情報管理上の課題及び企業に求められる対策について考察します。

１．技術情報漏洩の事例

■大手半導体メーカーの業務提携先の元技術者が最新の研究データを持ち出しライバル企業に提供した事例

大手電機メーカーT社の開発拠点の工場において、業務提携先である半導体メーカーS社の元技術者が、2008年1～5月にT社の「NAND型」フラッシュメモリーに関する最新の研究データを記録媒体（USBメモリ）に不正にコピーし、同年7月以降、転職先の韓国の半導体大手メーカーH社にデータを提供した事件。

NAND型はT社の主力商品で、研究データは社内でアクセスが制限されるなどした「営業秘密」だった。元技術者はアクセス権限が与えられていたが、コピーしたり、退職後に秘密を漏洩したりすることを禁止されていた。

警視庁は2014年3月13日に不正競争防止法違反で元技術者を逮捕（2014年4月3日東京地検が起訴）した。報道によると、元技術者は「転職を有利にするため、優秀な研究者に見えるようにデータを利用した」と供述しているという。転職先では役員級の待遇を受けており、データ提供の見返りだったとみられる。なお、元技術者はS社で2007年に降格処分を受けており、周囲には待遇への不満を漏らしていたという。

また、T社は、同日、H社と元技術者に対し、「H社は不正入手を知りながらデータを利用して製品を製造販売し、損害を与えた」とし、約1,091億円の損害賠償請求と入手データの破棄などを求める民事損害賠償を起こしている。2014年11月12日の第1回口頭弁論では、H社は「何が営業秘密かが具体的に特定されていない」などと反論している。

（出所）各種報道資料より作成

（１）管理上の課題

本件事例は、技術情報の漏洩のため、第三者委員会等による調査報告書が公表されているわけではありませんので、事案の詳細な部分については不明ですが、以下のような点が管理上の課題として指摘できます。

①　記録媒体の持込

元技術者は、ＵＳＢメモリで技術情報を持ち出していますが、基本的な技術的管理として、許可したＵＳＢメモリ以外はアクセスが出来ないようにしたり、データを暗号化するなど、ごく基礎的なセキュリティ対策を行うだけでも、ある程度防ぐことができたのではないかと思われます。まずは、基本的な技術対策を確実に実施する必要があります。

② 営業秘密の特定と適切な管理

口頭弁論で、データ供与を受けた被告のH社が「何が営業秘密かが具体的に特定されていない」と反論しています。営業秘密として保護されるためには、「営業秘密管理指針」で求められている営業秘密の三要件を満たす必要がありますが、本事例に限らず「秘密管理性」については、 企業情報の漏洩防止対策として、どの程度の管理を行えば良いのか分からない、といった産業界からの意見がありました。そのため、第１章でも触れたように、営業秘密の要件に関する見直しの議論が始まっています。

これまでの裁判例によれば、営業秘密が漏洩した場合、被害者側の当該秘密が他の情報から区分できていたかが問題となっています。例えば電子データの場合、頻繁なパスワード変更や閲覧後のデータ削除など厳格な管理が必要とされてきましたが、要件の見直しが行われれば、従業員が「秘密として管理しようとする企業意思」を容易に認識できるような管理をしておけば、営業秘密として保護対象として認められるようになる見込みです。

③ 提携先企業の従業員等の管理

事件を起こした元技術者は、業務提携先Ｓ社の従業員であり、技術情報を持つＴ社とは直接雇用関係があるわけではありません。業務提携は、外部の専門的な知識や外部のノウハウを有効に活用できますが、社外の従業員等に技術情報を開示することになるため、情報漏洩の機会は増えます。

まず、双方の事業者間で秘密保持契約を締結することが必要ですが、事業者間で締結された秘密保持契約は、開示先の企業が、実際に技術情報を使用する自社の従業員等との間で秘密保持契約を締結しなければ、実効性が担保できないことに留意する必要があります。本事例でいうと、Ｔ社とＳ社間で秘密保持契約を締結することはもちろん、Ｓ社と元技術者との秘密保持契約の写しを徴求するなどの措置も必要でしょう。また別途、Ｓ社における秘密管理体制の確認を行うなどの措置が必要でしょう。

④ 労務管理・労務環境

最近は、海外企業への技術情報の漏洩が多くなっています。報道によると、元技術者は、Ｓ社から降格処分を受けており、待遇が悪化したり職を失ったりした技術者たちが、日本の高い技術を欲しがっている海外企業から高い報酬を提示されて転職する例が増えています。韓国や中国企業は半導体に限らず、日本の技術者の引き抜きや再雇用に積極的です。

営業秘密である技術情報を不正に持ち出したりすれば、不正競争防止法違反となり刑事罰や民事損害賠償請求を受けますが、技術者が長年の経験から得た頭の中にある「ノウハウ」を転職先で生かすことまでは止めることができません。本事例のような海外への情報流出を防ぐには、技術者が長く働き続けられるような職場環境・人事的処遇制度を整備する必要があります。

（２） Ｔ社の対応上評価できる点

今回、不正競争防止法に従って、刑事告訴、民事損害賠償を請求していますので、今後は、流出した情報が営業秘密に該当するのか、すなわち営業秘密として適切に管理されていたかが争点になります。

現在の不正競争防止法では、企業の営業秘密が漏洩して民事損害賠償になった場合、争点となる営業秘密の侵害についての立証責任は原告にあり、立証が極めて困難ですが、不正競争行為に対して法的措置を講じたことは評価できると考えられます。 不正の「やり得」を許さない断固とした対応を示すことは、大きな防衛策といえます。

なお、現在議論されている不正競争防止法改正案では、営業秘密の侵害に関する立証責任を被告側に課すことが検討されています。これは、営業秘密侵害の証拠は被告側企業の内部領域に偏在しているため、原告側としては情報収集が難しく立証が極めて困難であり、公平性を欠くとの産業界からの意見に対応したものです。

２．顧客情報漏洩の事例

■大手通信教育会社の業務委託先システムエンジニアによる顧客情報漏洩の事例

通信教育大手B社のシステム開発・運用を行っているS社の業務委託先のシステムエンジニアにより、顧客情報が私物のスマートフォンにコピーされて持ち出され、名簿業者に売却された事件。流出した顧客情報は、2,895万件に及ぶ大規模なもので、流出した情報は、通信教育サービスの顧客情報であり、子供や保護者の氏名、住所、電話番号、性別、生年月日などである。成績やクレジットカード番号などは含まれていなかった。

2014年6月に、B社の顧客宛てに、B社にしか登録していない情報により他社からダイレクトメールが届いたことから、問合せが急増し、B社が社内調査を行った結果、データベースの顧客情報が外部に持ち出されたことが発覚した。B社は、警察に対する相談を開始し、同年7月15 日には、警視庁に対して、本件個人情報漏洩についての刑事告訴を行い、同月17 日、警視庁は、不正競争防止法違反の容疑で、B社 のシステム開発・運用を行っているグループ会社S社の業務委託先で顧客情報データベースの保守メンテナンスを行っていたシステムエンジニアを逮捕した。

B社は、同年9月中旬に、顧客情報が漏洩したとみられる顧客に対し、お詫びとして「500円の図書券等」の進呈を決定した。

（出所）各種報道資料・B社「個人情報漏えい事故調査委員会による調査報告について」より作成

（１）管理上の課題

①　システム上の問題点

Ｂ社の事故調査委員会の調査報告書を見ると、Ｂ社では、一般的に考えられるよう安全管理措置は講じていました。しかし、幾つかのシステム上の問題点により、不正行為を防ぐことができませんでした。報告書では、次の５点を指摘しています。

1）アラートシステム[6]の不備

アラート（警告）の対象範囲が、明確に定められておらず、不正行為が行われた当時、今回の行為が対象として設定されていなかったため、システムが機能しませんでした。

[6] 報告書では、クライアントＰＣとサーバーとの間の通信量が一定の閾値を超えた場合、データーベース管理の担当部門長に対しメールで警告が送信される仕組みを「アラートシステム」と呼んでいます。

2）データの書出し制御設定の不備

書出し制御システムのバージョンアップの際に、特定の新機種のスマートフォンを含む一部の外部メディアへの書出しについて、書出し制御機能が機能しない状態が生じたため、クライアントＰＣ内に保存したデータを個人所有のスマートフォンに書き出すことが可能となりました。

3）アクセス権限の管理の不備

付与済みのアクセス権限の見直しが定期的に行われていない状況も多く見受けられました。

4）データベース内の情報管理

データベース内の個人情報は、主としてマーケティング分析のために使用されており、必要にして十分な程度までの個人情報の抽象化及び属性化は行われていませんでした。

5）アクセス・通信ログのモニタリングの不備

クライアントＰＣからデータベースへのアクセスについて、自動的にアクセスログ及び通信ログを取得していましたが、意図的な不正行為を想定してログを定期的にモニタリングすることはしていませんでした。

これら報告書で指摘されているシステム上の問題点は、一見、技術的に適切な管理措置が講じられているように見えても、実際には何らかの不備があったり、正しく運用されていない可能性を示唆しています。僅かな隙を突いて、不正行為は行われます。

②　組織体制・企業風土に関する問題点

また、報告書では、不正行為の原因となった組織体制及び企業風土に関しても以下のとおり指摘しています。

1）組織体制の問題点

・情報セキュリティのグループ全体の統括責任者が明確に定められていなかった。
・情報セキュリティについてグループ全体で統括的管理を行う部署が存在しなかった。
・組織再編の結果、従前行われていた業務が再編後の組織に承継されていなかった。
・組織間で責任・権限の所在が不明確になる場合があった。
・グループにおいて、個人情報管理の責任部門が不明確であった。
・内部の不正行為による情報漏洩を防止するための高度な監査は行われていなかった。

2）役職員の意識及びコーポレート・カルチャー

・グループにおいて、情報セキュリティに多くの予算及びリソースを投入し、また、役職員の教育・研修にも相当程度行ってきたことから、情報セキュリティについて相当なレベルにあると認識していた。
・社内の人間が悪意を持って大量の個人情報を持ち出すことはあり得ないという意識を持っていた。

③　業務委託先の管理に関する問題点

・業務委託先の担当者について、二次委託先、三次委託先等のどの委託先に所属する従業員かという契約上の位置付け等について把握することなく、本件データベースに保存された個人

情報等に広範囲にアクセスする権限を付与していた。
・業務担当者による不正行為を想定した十分な行動監視体制が整っていなかった。

これらの問題点は、従業員等及び委託先の管理を行う場合、実際の企業内の運用状況や企業活動の変化、企業風土等により問題が表面化する可能性があることを示唆しています。B社の場合、システム上の問題が全く無かったわけではありませんが、一般的に考えられる技術的な安全措置や従業員等への教育・研修は行われていました。報告書の指摘で注目したいのは、企業風土に関する「社内の人間が悪意を持って大量の個人情報を持ち出すことはあり得ないという意識を持っていた」という指摘です。企業規模が拡大するにつれて業務別の分社化やM&Aによる他社の買収などカルチャーの異なる従業員等がグループ内に入ってきます。また業務委託先も増えていきます。組織は常に変化していきます。これらの変化に合わせて、外部の専門家等の活用や定期的な監査により、管理体制を常に改善し続けることが必要であるといえます。

（２）Ｂ社の対応上評価できる点

顧客からの問合せに迅速に対応した点は、高く評価できるといえます。警視庁もB社からの被害相談からわずか10日の異例のスピードで、システムエンジニアを逮捕しました。この背景には、子供の個人情報が大量に流出するという社会的反響の大きさを考慮し、問題の早期収束を図ったものと思われます。

３．事例から考える営業秘密管理の問題点

以上、直近に発生した２つの情報漏洩事例について見てみました。この２つの事例を見る限り、まず、適切な技術的な対応を行い、その上で人的対応を行う必要があると考えます。情報漏洩に対する取り組みは、残念ながら「性善説」では成り立ちません。そのため、社内規程や管理体制等の整備が必要です。

管理体制を整備しても、それだけで営業秘密が適切に保護されるわけではありません。管理を行なうのは役員および従業員である「人」です。営業秘密を守るのも、漏洩するのも「人」が行う行為です。報道される情報漏洩事件のほとんどが、自社や委託先の従業員等による故意または単純ミスによる漏洩（持ち出し）であることからも、人的な安全管理は非常に大切です。したがって、技術的な対策のみならず、職場環境の整備も併せて行うことが情報漏洩対策にとって重要であるといえます。

第3章　営業秘密漏洩の対策

１．営業秘密管理の視点とプロセス

社内の秘密情報を営業秘密として法的な保護を受ける場合は、第１章で述べた秘密管理性、有用性、非公知性の三要件を満たすことが必要です。但し、その実現には、それぞれの組織の実態や実情を踏まえ、漏洩リスク、管理コスト、業務効率のバランスを考慮した合理的な管理が必要です。まずは、現在適用している社内のセキュリティ施策や内部統制プロセスを再確認した上で、適切な管理方法を検討しく必要があります。

営業秘密管理には、図3-1に示したように４つの安全管理措置があります。すなわち、「組織的管理」「人的管理」「物理的管理」「技術的管理」です。

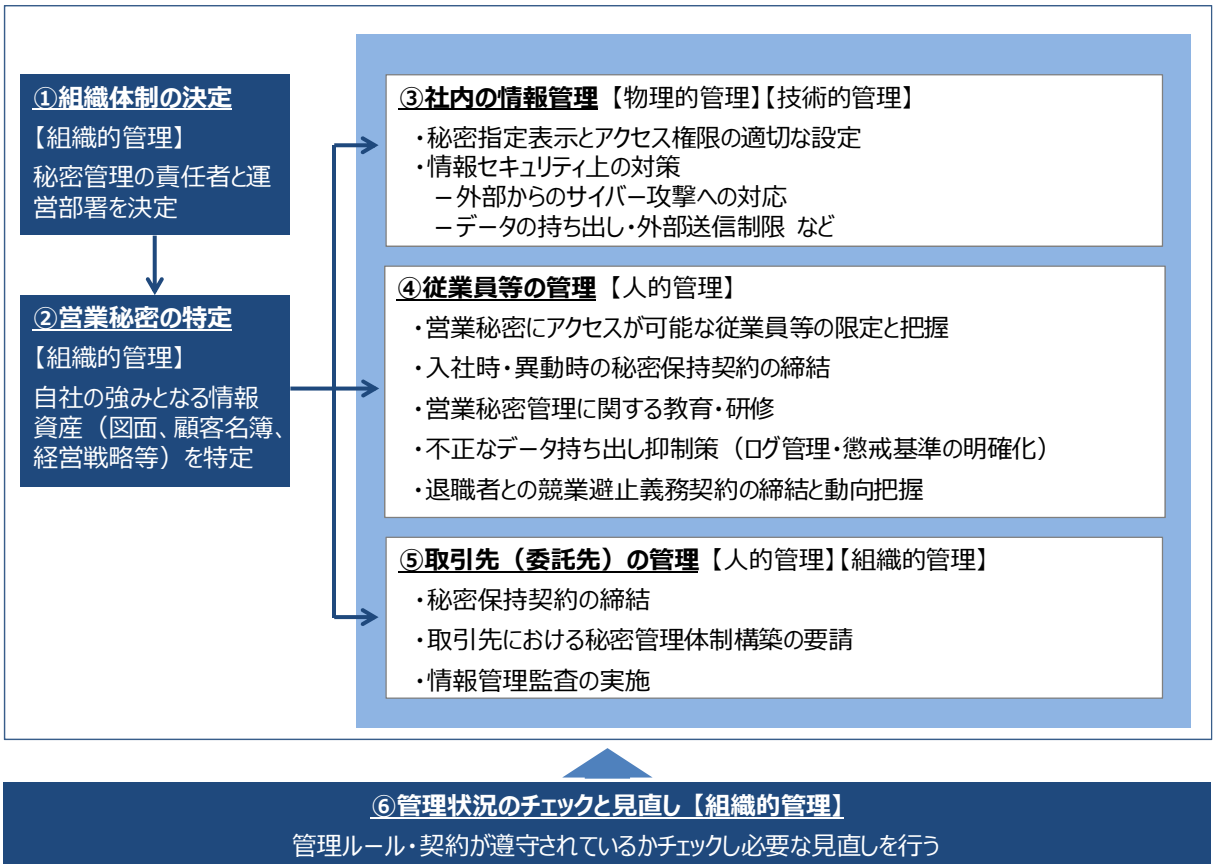
図表 3-1　営業秘密漏洩対策の 4 つの安全管理措置

安全管理措置	内容
(1)組織的管理: 体制をつくり、ルールをつくる	・情報資産の洗い出しとリスク分析・管理方針の策定・運用・改定 ・ルールの文書化(就業規則の整備・営業秘密管理規程の制定・操作マニュアル)と定期的な見直し ・管理方針の実施状況のモニタリング（内部監査、相談窓口の設置など） ・体制の構築と維持　など
(2)人的管理: ルールを従業員等に遵守させる	・就業規則で情報保護義務や罰則など定める ・営業秘密とその管理に関する定期的な従業員教育・研修の実施 ・委託先の情報セキュリティ評価や秘密保持契約の締結 ・秘密保持契約の締結、競業避止義務契約の締結 ・派遣社員・転入退出者の管理　など
(3)物理的管理: ルールの具体化を物理的側面で実現	・営業秘密及び区分の表示 ・情報機器の持出し管理 ・持ち出し・複製の制限、廃棄管理 ・重要度の高い情報の施錠管理 ・施設立入り制限や、入退室(館)管理　など
(4)技術的管理: ルールの具体化を技術的側面で実現	・ウイルス対策やハードディスクの暗号化 ・ネットワークファイアウォールの適切な管理 ・外部からの不正アクセス対策 ・アクセス権の設定 ・アクセスログの取得と定期的な確認　など

まずは、管理体制を作り、自社の強みとなる技術、ノウハウ、営業資料等の社内の情報資産を棚卸した上で、営業秘密としての管理対象を特定します。

次に、営業秘密を他の情報と区分し、情報にアクセスした者が営業秘密であると認識するために必要な措置、及び権限の無い者がアクセスできないような措置、委託先の管理等を検討します。これを図にしたものが、図表3-2です。以下、具体的な管理内容についてご説明します。

図表 3-2 営業秘密管理の全体像



（出所）経済産業省資料を一部修正

２．営業秘密管理のポイント

（１）組織体制の決定

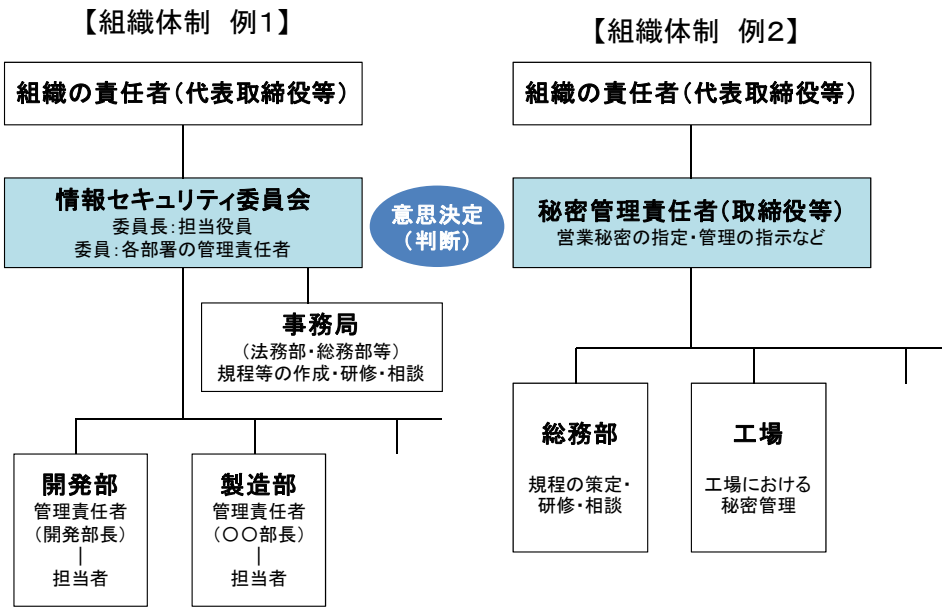
まず最初に行うことは、秘密管理について意思決定・判断する組織や責任者とその管理体制を決定します。図表3-3は、具体的な組織体制の例です。

例1では、「情報セキュリティ委員会」を設置した例です。できれば「情報セキュリティ委員会」の設置が望ましいといえます。なぜなら、経営陣がリーダーシップをとって情報セキュリティ対策のＰＤＣＡを回すためには、経営陣が報告を受け、経営判断を行う会議体が必要だからです。また、定期的に経営陣と現場が情報セキュリティに関する意思疎通を行うためにも有効です。もっとも、企業規模に応じて、簡素な組織を維持したいのであれば、経営会議のような既存の会議に、定期的に情報セキュリティに関する議案を付議することで代替しても良いでしょう。

委員会を設置しない場合は、例2のように秘密管理責任者を任命します。専任者を置くことが困難な場合は、兼務でもかまいません。ただし、秘密管理責任者としての役割が果たせるように仕

事を配分・調整することは、情報セキュリティ対策の形骸化を防ぐために必要です。

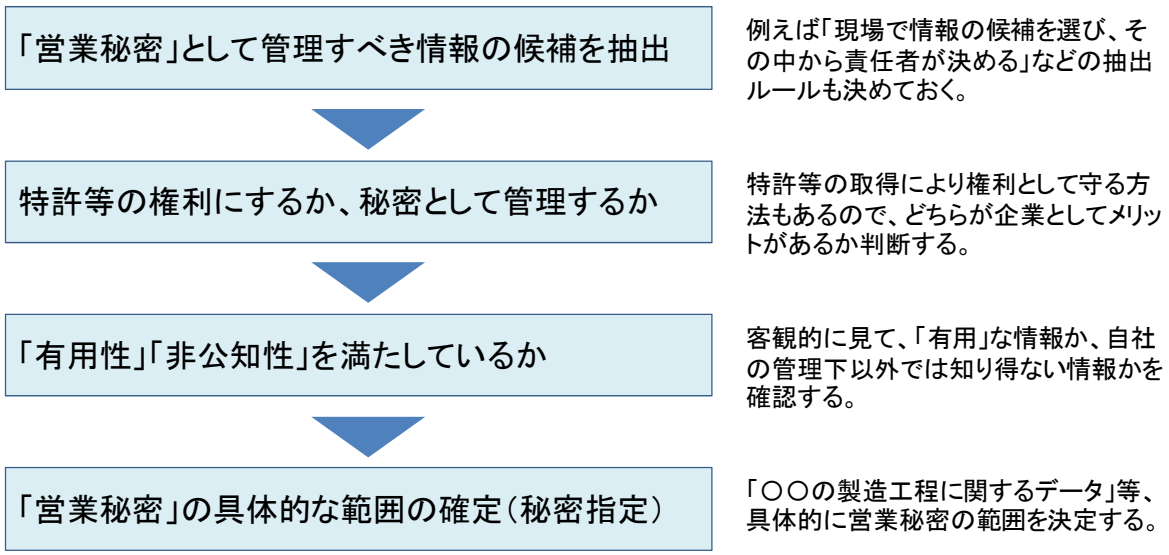
図表3-3 営業秘密管理の組織体制



(2) 営業秘密の特定

次のステップとして営業秘密候補を抽出し、そのうち「営業秘密」とするものを確定します。

図表3-4 営業秘密の抽出・指定



(出所)経済産業省資料を一部修正

企業が保有している情報資産について、どこにあり、誰が管理してどのような状況で取り扱われているかを、情報資産の洗い出しによって明確にします。洗い出しを行うには、各部署の理解と同意を得たうえで協力してもらう必要があります。

情報資産の量は膨大ですので、大まかにグループ化することによって作業の効率化が図れます。

グループ化は、次のような基準が考えられます。

図表3-5 グループ化の基準

区分	具体的な基準
所在	自社の機密情報、他社から預かった機密情報 など
情報のタイプ	個人情報、技術情報、財務情報、経営戦略 など
価値や属性	用途、保管場所、保管期間 など
機器や装置	顧客管理のデータベースサーバー、会計処理用のサーバー
情報のライフサイクル	生成、利用、保存、廃棄

洗い出した情報資産は、分類し、格付け（レベル付け）を行います。情報資産の格付けは、一般的に、機密性、完全性、可用性の３つの観点から分類していきます。情報漏洩に関連がある機密性の評価については、情報が許可されていない者に漏れてしまった場合にどのような影響があるかを考慮します。図表3-6は、機密性についての格付けの例です。

図表3-6 情報資産の機密性の格付けの例

格付け	格付けの概要	レベル	レベルの概要
4	情報が許可の無い者に漏洩した場合、業務への影響は深刻かつ甚大である。	極秘	特定の決められた関係者のみに開示または提供し、情報の複製は禁止または不可。
3	情報が許可の無い者に漏洩した場合、業務への影響は大きい。	秘密	特定の部門にのみ、開示または提供する。
2	情報が許可の無い者に漏洩しても、業務への影響は少ない。	社外秘	企業内でのみ開示または提供。
1	情報が許可の無い者に漏洩しても、業務への影響は無い。	公開	第三者にも開示または提供。

以上のような情報資産の格付けを行い、「営業秘密」として指定する情報資産を抽出していきます。図表3-7は、営業秘密の類型です。

図表3-7 営業秘密の類型

情報資産分類	情報資産分類に該当する主な情報の例
経営戦略に関する情報資産	経営計画、目標、戦略、新規事業計画、M&A 計画 など
顧客に関する情報資産	顧客情報、顧客ニーズ など
営業に関する情報資産	販売協力情報、営業ターゲット情報、セールス・マーケティングノウハウ、仕入価格情報、仕入先情報 など
技術に関する情報資産	共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウ など
管理（人事・経理等）に関する情報資産	社内システム情報（ID・パスワード）、システム構築情報、セキュリティ情報、人事評価データ など
その他の情報資産	上記以外の情報資産

（出所）経済産業省資料を一部修正

実際に営業秘密として指定する際には、例えば「顧客情報」ではなく、「○○顧客データベースに記載された情報」「○○顧客台帳にファイリングされている情報」など、より具体的に指定する必要があります。ある程度の具体性が無いと、管理が必要（あるいはアクセス権の無い者が触れてはいけない）な営業秘密が何なのかが、従業員等が認識できないからです。

また、技術情報等の場合、「権利」にするか、「秘密」として保存するかを検討する必要があります。「特許化」する技術等は特許法で守られ、「秘匿化」する営業秘密は不正競争防止法で守られることになります。それぞれのメリット・デメリットは図表3-8のとおりです。

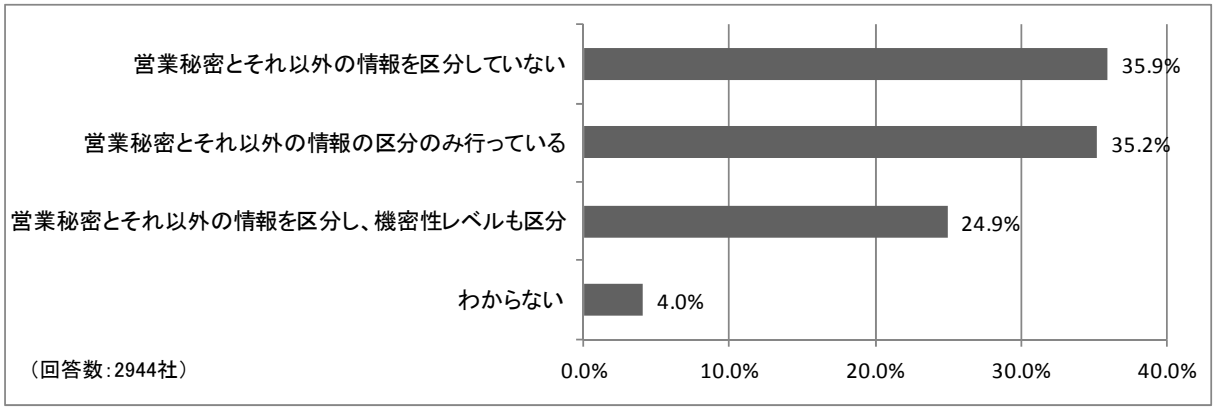
図表3-8 「特許化」と「秘匿化」のメリット・デメリット

	特許化	秘匿化
メリット	・事前の審査を通じて権利の内容が明確になる。 ・登録等を通じて権利の存否が明確になる。 ・一定期間、譲渡可能な排他的独占権を取得できる。	・保護期間の制限もなく、差別化を図れる。 ・自社の事業戦略の方向性が公開されない。 ・失敗した実験のデータ等の特許になじまないノウハウも保護できる。
デメリット	・出願内容の公開が前提であるため、開発動向を知られたり、周辺特許を取得される可能性がある。 ・保護期間が満了したら、誰でも使用可能。	・他社の独自開発やリバースエンジニアリングにより、独占できなくなる可能性がある。 ・適切な管理をしていないと法律による保護を受けることができない。

（出所）経済産業省資料を一部修正

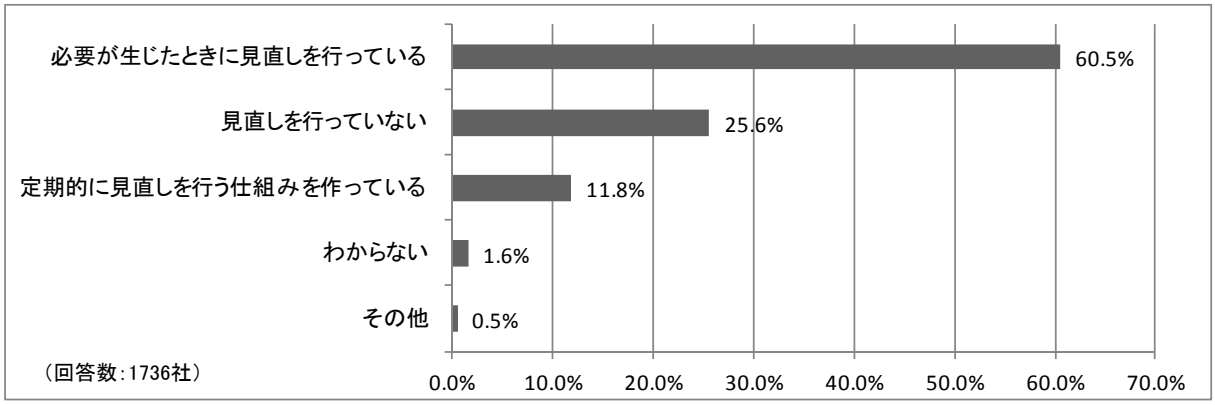
ここで、経済産業省の調査結果により、営業秘密の管理状況について確認しておきます。営業秘密とそれ以外の情報とを区分しているかという質問に対し、35.9%が「営業秘密とそれ以外の情報とを区分していない」と回答しています（図表3-9参照）。約3分の1の企業は、情報資産の区分さえも行っていないという状況です。

図表3-9 営業秘密の区分状況



（出所）経済産業省「人材を通じた技術流出に関する調査研究報告書　別冊」より作成（図表3-10も同じ）

図表3-10 営業秘密の格付け基準の見直し状況



営業秘密とそれ以外の情報の区分を行っていると回答した企業に対して、営業秘密の格付け基準に関する見直しの状況について質問したところ、「必要性が生じたときに見直しを行っている」と回答した企業の割合が60.5%と最も高くなっています（図表3-10参照）。

実際には、営業秘密管理の基本である営業秘密の区分や格付け基準の定期的な見直しを適切に行っている企業は、多くないことが分かります。

（３）社内の情報管理

物理的管理、技術的管理により、営業秘密を保護します。物理的管理とは、入退館（室）の管理、情報資産の盗難防止等の措置のことであり、技術的管理とは、情報資産及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等の技術的な措置のことです。

図表3-11 「物理的管理」・「技術的管理」の具体例

【物理的管理】

情報資産の保管	・責任者が施錠管理 ・専用スペースに分別保管し、無断で開けることのないように周知
「秘密」の表示	・従業員等が秘密であることを容易に認識できるように「秘」などの表示
持ち出し・複製	・持ち出し・複製・複写は原則禁止とし、必要に応じて責任者の許可制とする ・持ち出し時は注意を払う（手元から離さない・鍵付き鞄を使用等）
回収・廃棄	・持ち出した資料等は回収し、私物の記録媒体に複製していないか確認 ・廃棄時は、復元不可能な状態にする
施設等の管理	・（出入口等に）「部外者立入禁止」の表示 ・アクセス権限の無い者は入室制限 ・入退出記録の作成（氏名と入退出時間の記録）
持ち込み禁止	・私物のパソコン・スマートフォン・UBSメモリ等の持ち込み禁止

【技術的管理】

ルールの設定	・PCやサーバー等の使用ルールを決定し、従業員等に周知 －パスワード取扱いルール、社内ネットワークへの個人PCへの接続禁止、データ持出（送信・アップロード等）不可の措置、サーバー以外への保管の禁止
外部からの侵入に対する防御	・ファイアーウォール※・ウィルス対策ソフトの導入 ※ある特定のコンピュータネットワークとその外部との通信を制御し、内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア（あるいはそのソフトウェアを搭載したハードウェア） ・営業秘密を管理しているPCは、ネットワークに接続しない
アクセス制限	・ID・パスワードの設定（使い回し、共有をしない） ・フォルダ、ドライブ等の閲覧制限（誰もが見られるようにしない）
データの消去	・営業秘密を保管していたPC、サーバー等を廃棄・譲渡等する場合は、物理的破壊やソフト等によるデータの完全消去を行う
管理者	・信頼できる者をシステムの管理者に任命 ・従業員等が退職した場合は、パスワードの変更とID等の削除を確実に行う

以下、幾つかのポイントについて補足説明します。

① 持ち出しや持ち込みの管理

情報漏洩の大きな原因となるのが、持ち出しや持ち込み管理の不徹底です。マニュアル等に明確に持ち込み禁止が規定されているにもかかわらず、私物のノートパソコンや記録媒体の持ち込みをチェックしていない例は少なくありません。また、オフィス内での録画や録音に対しても、原則禁止とすべきです。特に、スマートフォンは、記録媒体にもなりデジタルカメラ機能や録音機能があるため、これも持ち込み禁止とするべきです。高度なセキュリティエリアにおいては、鞄や大きな袋なども持ち込み禁止とすべきです。

昨今では、委託業者の社員が情報を不正に持ち出す例が多くなっています。委託業者の社員がサーバールームで保守作業を行う場合は、担当者の氏名や持ち込む書類及び機器などを事前に申請させて、作業中は担当者を１人にさせないなどの配慮も必要でしょう。そして、作業終了後には、作業内容の記録を提出させ、入室時の物品の持ち込みと持ち出しの突合をすることが望ましいと言えます。

② 紙媒体の管理

2014 年に消費者庁が発表した「平成 25 年 個人情報の保護に関する法律の施行状況の概要」によると、漏洩した情報の形態では、電子媒体のみが約 45.9%、紙媒体のみが約 52.2%と紙媒体の方が未だに多いことが分かります。

また、漏洩した情報に対する暗号化等の情報保護措置の有無についてみると、紙媒体のみの漏洩については、約94%の事案において情報保護措置がとられていませんでした。したがって、紙媒体の管理は、重要であるといえます。紙媒体は、業種や会社規模にかかわらず利用されている

ため、情報が流出する可能性も多くなります。また、技術的な保護措置も掛けにくいので留意が必要です。

図表3-12 漏洩の形態と保護措置の有無

	電子媒体のみ		紙媒体のみ		電子媒体と紙媒体		不明		合計
	件数	割合	件数	割合	件数	割合	件数	割合	
措置有（全部保護）	49	13.4%	3	0.8%	0	0.0%	2	0.5%	
措置有（一部保護）	16	4.4%	5	1.4%	3	0.8%			
措置無し	87	23.8%	180	49.2%	1	0.3%			
措置不明	16	4.4%	3	0.8%	1	0.3%			
合計	168	45.9%	191	52.2%	5	1.4%	2	0.5%	366

（出所）消費者庁「平成25年 個人情報の保護に関する法律の施行状況の概要」

紙媒体も電子媒体と同様に、ラベリングし、台帳などによって管理する必要があります。保管に関しても同様で、文書の重要度や機密性のレベルにより格納場所や保管の手順を定めた上で施錠管理を行います。持ち出しや閲覧の際は、記録を残すようにします。

会議や打合せで出席者に配布する文書については、その重要度や機密性のレベルに応じて回収することが望ましいといえますが、状況により回収が困難な場合もあります。部外秘などの文書については、配布した文書が適切に管理されているか、不要になった場合は適切に廃棄されているかを追跡管理できることが望ましいといえます。

また、紙媒体は、電子媒体と異なり、情報を直接見ることができるので、不要となった紙媒体は、所定のルールに則り、速やかに廃棄処分するべきです。

③ 技術的保護措置の重要性

従業員等が社内業務システムを利用する場合、情報漏洩対策のポイントは、論理的に必要最小限のアクセスコントロールを設計し、それをシステムに実装し、アクセスログをきちんと取得し点検することです。最近の情報漏洩の特徴として、内部不正、すなわちアクセス権限のある者からの情報漏洩が増えているということがありますが、これに関連して独立行政法人情報処理推進機構（ＩＰＡ）の興味深い調査がありますので紹介します（図表3-13参照）。内部不正への気持ちが低下する対策を社員と経営者・管理者に質問したところ、社員が上位に挙げた回答と、経営者・管理者の回答に大きなギャップがあり、経営者・管理者が講じる対策が必ずしも効果的に機能しない可能性があるとのことです。

この調査の上位項目を見ると、例えば、「一定数以上の顧客情報のダウンロードがあった場合は、直ちに管理者または上司に自動的にアラートメールを送信するという仕組みの構築」なども、内部不正による情報漏洩に対する有効な抑止力として、検討に値すると思われます。

2014年に発生した大手通信教育企業の顧客情報漏洩事件でも、「アラートシステムの不備」が指摘されています。

図表3-13 内部不正への気持ちが低下する対策

社員の回答結果			経営者、管理者の回答結果	
順位	割合*1	対策内容	順位	割合*2
1位	54.2%	社内システムの操作の証拠が残る	19位	0.0%
2位	37.5%	顧客情報など重要な情報にアクセスした人が監視される（アクセスログの監視等含む）	5位	7.3%
3位	36.2%	これまでに同僚が行ったルール違反が発覚し、処罰されたことがある	10位	2.7%
4位	31.6%	社内システムにログインするためのIDやパスワードの管理を徹底する	3位	11.8%
5位	31.4%	顧客情報などの重要な情報を持ち出した場合の罰則規定を強化する	10位	2.7%

*1:内部不正への気持ちが低下すると回答した回答者の割合（社員n=3,000、経営者・管理者n=110）
*2:効果が見込める対策と回答した回答者の割合

（出所）情報処理推進機構（IPA）「組織内部者の不正行為によるインシデント調査報告書」

（４）従業員等の管理

① ルールの文書化と従業員等への周知

組織体制、対象となる営業秘密、物理的管理・技術的管理など、これまで決定してきたルール等を規程（文書）としてまとめます。規程化にあたっては、特に定まった形式があるわけではありませんが、「営業秘密管理指針」の参考資料として公表されている「営業秘密管理規程」「営業秘密管理基準」などが参考になります。

営業秘密管理規程は、営業秘密の機密性のレベル、レベルに応じたアクセス制限、閲覧や配布などの許可、使用目的の設定、秘密保持期間の設定といった情報管理責任と、アクセス権限を与えられた者だけにアクセスを許可するための情報セキュリティ管理責任の両方について、権限の範囲と責任者を定めます。

ルールの文書化（規程化）が出来たら、それを従業員等へ周知を図り、理解と実行を求めます。例えば、オフィス内での掲示のみなど、従業員等が気付かない可能性があるような方法では十分に周知を行ったとはいえません。情報漏洩を起こさないような教育・研修を全ての従業員等に徹底することが、経営者の責任であるといえます。

② 秘密保持契約の締結

昨今の営業秘密漏洩のパターンとして、内部不正が多くなっていることから、人的管理、すなわち労務管理の視点は重要です。そこで、事前の抑制策の一つとして、従業員等と秘密保持契約を締結しておくことが考えられます。損害賠償条項や差止請求条項を記載した法的に有効な契約を締結しておけば、保護の対象となる秘密情報が営業秘密の要件を欠いてしまって、不正競争防止法による保護がなされない場合でも、秘密保持契約を根拠として、民法上の債務不履行に基づく損害賠償請求のほか、差止請求権を行使することも可能となると考えられます。

秘密保持契約の対象となる秘密事項に関しては、「在職中に知りえた情報全般」というように一般的・包括的に定めている企業が大半を占めています。これは、入社時に秘密保持契約を締結する企業が多いことと関係があります。秘密保持契約の対象となる情報が具体的に特定されていないからといって、契約の有効性が直ちに失われるわけではありませんが、契約の解釈や有効性をめぐって紛争が生じるリスクを軽減するためには、契約の対象となる秘密事項を具体的に特定した上で、秘密保持義務が退職後もなお存続することを契約条項に明記することが望ましいといえます。

また、他の企業に勤務していた者を中途採用する場合には留意すべきことがあります。不正競争防止法では、営業秘密を取得する際、不正開示行為であること、または不正開示行為が介在していることについて悪意もしくは重過失で営業秘密を取得する行為、当該営業秘密を使用または開示する行為を不正競争としています（不正競争防止法2条1項8号）。これは、他の企業に勤務していた従業員等が営業秘密を不正に取得していることを知っていた場合、もしくは重大な過失によって知らなかった場合も該当します。中途採用者は、以前勤務していた企業との間で、秘密保持契約や競業避止契約に基づく義務を負っている可能性があり、他の企業の営業秘密を開示した場合、これら契約に基づく差止請求を受ける可能性もあります。

③　競業避止契約の締結

在職中の競業避止義務については、一般的に就業規則に規定され、労働契約の付随義務と考えられます。退職者等を通じた営業秘密の流出を防止するためには、秘密保持義務の他、競合企業への転職や従業員等の転職勧誘を禁止する競業避止義務契約を締結する方法があります。しかし、退職後の競業避止義務は、退職した役員や従業員の行動の把握が困難である等、運用上の問題もあります。また、広範な内容の競業避止契約を締結してしまうと、職業選択の自由を制限することとなり契約自体が無効とされる可能性が高くなります。

経済産業省「人材を通じた技術流出に関する調査研究報告書」では、直近10年間の裁判例について分析し、競業避止義務契約が有効と判断される基準に関して、次のようにまとめています。

●競業避止義務契約締結に際して最初に考慮すべきポイント：

- **企業側に営業秘密等の守るべき利益が存在する。**
- **上記守るべき利益に関係していた業務を行っていた従業員等特定の者が対象。**

●競業避止義務契約の有効性が認められる可能性が高い規定のポイント：

- **競業避止義務期間が１年以内となっている。**
- **禁止行為の範囲につき、業務内容や職種等によって限定を行っている。**
- **代償措置（高額な賃金など「みなし代償措置」といえるものを含む）が設定されている。**

●有効性が認められない可能性が高い規定のポイント：

- **業務内容等から競業避止義務が必要ない従業員等と契約している。**
- **職業選択の自由を阻害するような広汎な地理的制限をかけている。**
- **競業避止義務期間が２年超となっている。**
- **禁止行為の範囲が、一般的・抽象的な文言となっている。**
- **代償措置が設定されていない。**

●労働法との関係におけるポイント：

- 就業規則に規定する場合については、個別契約による場合がある旨を規定しておく。
- 当該就業規則について、入社時の「就業規則を遵守します」等といった誓約書を通じて従業員等の包括同意を得るとともに、十分な周知を行う。

④　職場環境に起因する不正行為への対策

営業秘密の漏洩者は、圧倒的に中途退職者によるものが多いわけですが、現職の従業員からの漏洩も発生しています。これらは「処遇（給与等）の不満」などのように職場環境に起因するものと考えられます。職場環境における危険要因と独立行政法人情報処理推進機構（ＩＰＡ）が策定している「内部不正防止ガイドライン」による対応策は以下のとおりです。

図表3-14 職場環境に起因する不正行為への対策

危険要因	項目	内部不正防止ガイドライン参照箇所
人事評価に納得しておらず、不満がある	公平な人事評価	(24)公平な人事評価の整備 (25)適正な労働環境及びコミュニケーションの推進 (26)職場環境におけるマネジメント
ある従業員が、特定の業務を長期間担当している	適正な労働環境	
特定の従業員の業務量が過大になっている		
業務の悩みを誰にも相談できない、孤立している	良好なコミュニケーション	
単独作業が多い		

(出所)情報処理推進機構(IPA)資料

各項目の具体的な内容としては、

●公平な人事評価

・公平で客観的な人事評価を整備し、従業員が評価内容を理解、納得できるよう、評価結果を説明する機会を設ける。

・適切な人員配置及び配置転換をする。

●適正な労働環境

・業務量や勤務時間を適正化する。

・特定の従業員の業務負荷が極端に高い状況を是正する。

●良好なコミュニケーション

・相談しやすい環境を整備し、業務の支援や上司や同僚との良好なコミュニケーションがとれる職場環境づくりを推進する。

などが、指摘されています。

秘密保持契約や競業避止契約を締結しても、職場に不満を持った従業員等を止めることはできません。従業員等の管理では、秘密保持契約や競業避止義務契約締結と併せて、職場環境の改善も営業秘密漏洩対策として重要であるといえます。

（５）取引先（委託先）の管理

取引先に自社の営業秘密を開示する場合には、開示する前に相手方企業に秘密保持義務を含む契約を締結します。営業秘密の秘密管理性及び非公知性を確保するために、相手方企業に対して、秘密を適正に保護する体制の構築を求めることも必要です。情報の開示を受けた企業は、自社情報との間でコンタミネーション（情報の混入）が生じないよう管理を行わければなりません。

また、営業活動に使う顧客情報等は、データベースの管理やダイレクトメールの発送等を外部業者に委託することが少なくありませんが、これについては、個人情報保護法第22条で、委託先業者の適切な管理を行うことが求められています。

更に「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（以下「経済産業省ガイドライン」）では、「委託先の選定」「委託契約の締結」「委託先における個人データ取扱状況の把握」の３つの視点で必要かつ適切な監督を行うよう求めています（図表3-15）。「経済産業省ガイドライン」は、昨今の顧客情報漏洩事件の多発を受けて、2014年12月12日に外部委託先への監督強化や社内の安全管理体制の強化を目的として改正が行われています。

図表3-15 経済産業省ガイドラインによる委託先監督の視点

視点	概要
委託先の選定	・委託先の安全管理措置が、少なくとも個人情報保護法第20条で求められる安全措置と同等であることを確認するため、「組織的」「人的」「物理的」「技術的」の各安全措置の項目が委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、適切に評価する。
委託契約の締結	・契約内容に、個人データの取扱いに関する安全管理措置として、委託元、委託先双方が同意した内容とともに、個人データの取扱い状況を合理的に把握することを盛り込む。
委託先における個人データ取扱状況の把握	・委託された個人データの取扱状況を把握するために、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託先の内容等の見直しを検討することを含め、適切に評価する。

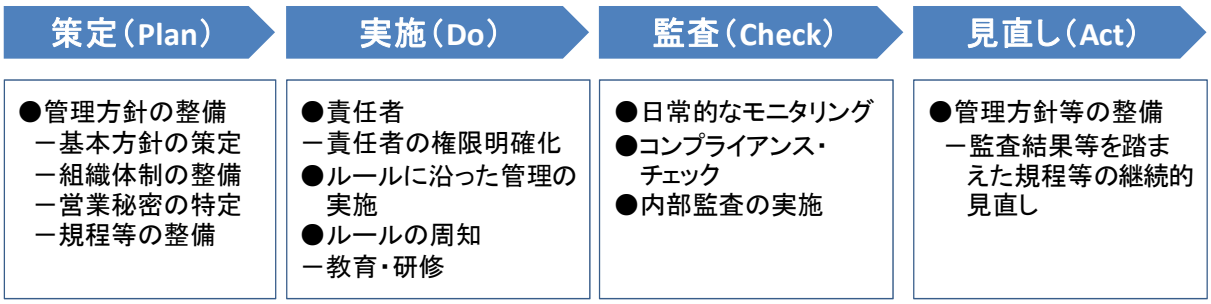
（出所）経済産業省ガイドラインより作成

なお、委託元が委託先に「必要かつ適切な監督」を行っておらず、委託先が適切とは言えない取扱いを行い、何らかの問題が生じたときは、委託元が責めを負うことになるので注意が必要です。

（６）管理状況のチェックと見直し

以上、営業秘密管理の考え方について説明してきました。どんな管理ルールや契約を施しても、それが遵守されていることの確認がなされなければ、実効性はありません。図表3-2をＰＤＣＡサイクルで再構成すると、図表3-16のようになります。

図表 3-16　営業秘密管理におけるPDCAサイクル



（出所）経済産業省資料を一部修正

３．リスクファイナンス

相応の対策を講じている企業においても、情報漏洩が発生しているのが現実です。情報漏洩リスクも、他のリスクと同様に、リスクを低減することはできても完全にゼロにすることはできません。そのため、何らかのリスクファイナンスを検討することは必要です。

リスクファイナンスとは、リスク対応を実施するコスト及び関連するコストに見合う資金を準備することです。積立金や準備金などの名目で必要な費用を内部留保する方法と、保険を利用することにより損失負担を外部に移転する方法があります。リスクの発生確率は高くないが、発生時の損失が大きい場合には、リスクファイナンスとして保険を利用することが有効です。情報セキュリティ対策においては、万一の場合に備えて、情報セキュリティ保険や情報漏洩賠償責任保険の付保を検討することも必要です。

図表3-17　情報漏洩賠償責任保険で支払われる保険金の種類（例）

損害	保険金の種類	内容
賠償損害	損害賠償金	法律上の損害賠償責任にもとづき被害者等に支払う賠償金
	争訟費用	争訟について支出した争訟費用、弁護士費用等
	求償権保全費用	他人から損害の賠償を受けることができる場合の権利保全手続きに要した費用
費用損害	法律相談費用	個人情報漏洩のために、法律事務所、弁護士に支払う相談費用
	事故対応費用	個人情報漏洩の直接の結果として、事故対応のために被る損害（通信費用、対応のための人件費、原因調査費用等）
	広告宣伝活動費用	個人情報漏洩に起因するブランドイメージ回復等のための広告宣伝活動に要した費用
	コンサルティング費用	個人情報漏洩の事実の確認・調査または個人情報回収等のために外部コンサルタントに委託した費用
	見舞金・見舞品費用	個人情報を漏洩された本人に対し、謝罪のために支払う見舞金、送付する見舞品にかかる費用

（注）補償の対象となる損害は、保険商品により異なります。

情報漏洩が発生した場合は、取引先や顧客の信用を失い、企業のブランドを毀損する可能性がありますが、これらの「信用」は保険ではカバーできません。したがって、あくまでも適切な情報漏洩対策を行った上で、万一の場合の財務的な損失を保険でカバーするという位置付けで検討します。

保険の対象となる情報は、「個人情報」と「法人情報[7]」です。媒体は、電子データでも紙データでも対象になります。

また、対象となる保険事故としては、外部からの攻撃（不正アクセスやウィルス）、過失（外出先での紛失）、盗難（外出先でのパソコンの盗難）、内部不正（情報の持ち出し）などです。支払われる損害は、大きく「賠償損害」と「費用損害」に分けられます（図表3-17参照）。

４．ＩＳＭＳ適合性評価制度

情報漏洩対策含む情報セキュリティ対策が簡単に進まない理由の一つは、企業によって、業種、社会的責任度、守るべき情報資産の内容、これまで講じてきた対策の積み重ねなどの状況が千差万別であり、どの企業にも一律に当てはまる処方箋が無い点にあります。

したがって、各企業は自ら、自社の現状に照らして、最も費用対効果の高い情報セキュリティ対策を検討していく必要があります。

企業等の組織において情報管理をするための適切な仕組み（情報セキュリティマネジメントシステム：Information Security Management System（ＩＳＭＳ））を認証する制度としてＩＳＭＳ適合性評価制度（ＩＳＭＳ認証）があります。ＩＳＭＳを構築する際の国際規格としてISO/IEC27001及び同27002 が発行されており、それに基づく日本語訳であるJISQ27001及び同27002があります。

ＩＳＭＳ認証では、企業の情報セキュリティ体制がJISQ27001及び同27002に沿って確立および運用されているかどうかが審査されます。すなわち、ＩＳＭＳ認証の取得によって、「組織的管理」「人的管理」「物理的管理」「技術的管理」の４つの視点から総合的な情報セキュリティ対策に取り組むことになります。結果として、情報セキュリティ管理体制のさらなる改善や社内組織の体質強化に繋がるだけでなく、顧客や取引先に対して情報セキュリティに関する信頼性を確保し、顧客満足度の向上や企業競争の優位性の獲得などにより、企業価値の向上に繋がります。

[7] ここでいう「法人情報」は、不正競争防止法でいう「営業秘密」から「個人情報」に該当する情報を除いたものをいう。

おわりに

昨今の営業秘密の漏洩は、もともと情報に容易にアクセスすることが可能であった者の内部不正によるものが増えています。これは、企業の内部でいかに技術的・物理的管理を尽くしても、外部への漏洩を完全に防ぐことは不可能であるといえます。まず、企業内のどこに機密情報が所在しているかを特定し、その保護状況が十分かどうかを評価し、営業秘密管理指針や国際規格などを参考に必要な対策を検討していかなければなりません。営業秘密を守るのも、漏洩するのも「人」が行う行為です。技術的・物理的な対策のみならず、人的管理は情報セキュリティ対策にとって非常に重要であるといえます。

また、漏洩が起きてしまった場合に、いかに実効性のある法的措置を採ることができるかという観点から、事前に適切な対策を講じておくことが重要です。そして、営業秘密の漏洩が疑われる場合には、事実関係の解明に努め、断固とした対応を行う必要があります。

情報セキュリティ管理体制の構築は「コスト」ではなく、ビジネスチャンスを生かし企業の信用力やブランドを上げるための「投資」と考えられます。可能な対策から実施し、企業全体の情報セキュリティレベルを高めていく継続的な取り組みが望まれます。

【本レポートに関するお問合せ先】
銀泉リスクソリューションズ株式会社　　リスクマネジメント部
102-0074　東京都千代田区九段南3-9-14
Tel : 03-5226-2212　　Fax : 03-5226-2884　　http://www.ginsen-risk.com/

■参考文献

・経済産業省

「平成25年度情報処理実態調査　結果分析等報告書」（2014年）

http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h25jyojitsu.html

「営業秘密管理指針」（2013年）

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf

「人材を通じた技術流出に関する調査研究報告書」（2013年）

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/houkokusho130319.pdf

（同報告書別冊）アンケート結果

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf

産業構造審議会 知的財産分科会 営業秘密の保護・活用に関する小委員会　資料（2014年）

http://www.meti.go.jp/committee/gizi_1/33.html

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（2014年）

http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf

・独立行政法人　情報処理推進機構（IPA）

「組織内部者の不正行為によるインシデント調査報告書」（2012年）

http://www.ipa.go.jp/files/000014169.pdf

「組織における内部不正防止ガイドライン」（2013年）

http://www.ipa.go.jp/files/000041054.pdf

「内部不正の現状について ～国内外の内部不正の動向～」（2014.8.26 企業の内部不正防止に関する緊急セミナー資料）

http://www.ipa.go.jp/files/000041262.pdf

・肥塚直人『「技術流出」リスクへの実務対応』（2014年）中央経済社

・消費者庁（2014）「平成25年度 個人情報の保護に関する法律施行状況の概要」
http://www.caa.go.jp/planning/kojin/pdf/25-sekou.pdf

・帝国データバンク（2014年）「営業秘密に関する企業の意識調査」
https://www.tdb.co.jp/report/watching/press/p140904.html

・日本規格協会（2014年）『JISQ27002　情報セキュリティ管理策の実践のための規範』

・一般財団法人　日本情報経済社会推進協会（JIPDEC）（2014年）『ISMS ユーザーズガイド』

・特定非営利活動法人　　日本ネットワークセキュリティ協会（2014年）
「2012年　情報セキュリティインシデントに関する調査報告書　～個人情報漏洩編～」
http://www.jnsa.org/result/incident/data/2012incident_survey_ver12.pdf

・羽田卓郎・山崎 哲（2014年）『ISO/IEC27001情報セキュリティマネジメントシステム（ISMS）構築・運用の実践』日科技連

・ISO/IEC 編著・JIPDEC 監訳（2011年）『わかりやすい情報セキュリティマネジメントシステム ISO/IEC27001実践ガイド』日本規格協会

・Ｂ社（2014年）「個人情報漏えい事故調査委員会による調査報告について」

Risk Solutions Report バックナンバーのご紹介

■季刊レポート

・Vol.1　2012年 Autumn
『米国における賠償責任の動向－PL（製造物責任）訴訟と雇用慣行賠償責任訴訟－』

・Vol.2　2013年 Winter
『アジア諸国のPL（製造物責任）法制整備の動向－各国PL法制の概要と特徴について－』

・Vol.3　2013年 Spring
『2012年度 Monthly Report 総集編（No.1‐No.8）』

・Vol.4　2013年 Summer
『メンタルヘルスに対応した企業のリスクマネジメント－休職制度の見直しとGLTDの導入－』

・Vol.5　2013年 Autumn
『2013年度 Monthly Report 上期総集編（No.9‐No.14）』

・Vol.6　2014年 Winter
『欧州諸国のPL（製造物責任）法制度と製品安全性規制の動向－主要国の制度概要と特徴について－』

・Vol.7　2014年 Spring
『2013年度 Monthly Report 下期総集編（No.15‐No.20）』

・Vol.8　2014年 Summer
『企業におけるリスクファイナンス手法－代替的リスク移転手法（ART）の種類と活用事例－』

・Vol.9　2014年 Autumn
『2014年度 Monthly Report 上期総集編（No.21‐No.26）』

■月刊レポート

・No.1（2012.08.16）「リスクマネジメントとしての企業のパワー・ハラスメント対策」
・No.2（2012.09.20）「会社法制の見直しに関する要綱案について」
・No.3（2012.10.24）「経営戦略実現のための等級制度のあり方」
・No.4（2012.11.27）「南海トラフ巨大地震の想定被害と被害軽減策」
・No.5（2012.12.17）「労働災害における使用者賠償責任リスク」
・No.6（2013.01.22）「2011年タイ大洪水のその後－復興と日系企業の動向－」
・No.7（2013.02.22）「マイカー通勤におけるリスクと企業責任」
・No.8（2013.03.18）「ＣＳＲ報告書に見る事業継続の取組み」
・No.9（2013.04.19）「従業員のソーシャルメディア利用における企業のリスク」
・No.10（2013.05.20）「南海トラフ巨大地震の被害想定と帰宅困難者対策」
・No.11（2013.06.17）「高まる洪水リスクと企業がとるべき対策」
・No.12（2013.07.19）「海外進出企業に求められる感染症対策」
・No.13（2013.08.20）「国際カルテル摘発事例の増加とグローバル企業の対応策」
・No.14（2013.09.17）「６５歳雇用時代の人事処遇制度の考え方」
・No.15（2013.10.21）「イベント開催における主催者のリスクと安全対策」
・No.16（2013.11.20）「リスクの本質とリスクファイナンスへの取組」

・No.17（2013.12.25）「化学プラントの爆発・火災事故とその法的責任」
・No.18（2014.01.24）「中国における日系企業の人材の現地化」
・No.19（2014.02.20）「安全性向上のための運輸安全マネジメント制度への取組み」
・No.20（2014.03.17）「食品表示問題から考える『食のブランド』について」
・No.21（2014.04.07）「スマートデバイスの業務利用における企業のリスク対策」
・No.22（2014.05.07）「労働災害におけるヒューマン・エラーとその対策」
・No.23（2014.06.05）「『消費者裁判手続き特例法』の概要と企業の対応について」
・No.24（2014.07.07）「高齢者介護施設における事故防止のためのリスクマネジメント」
・No.25（2014.08.07）「事業継続マネジメントにおける実践的なＢＣＰ訓練の実施方法」
・No.26（2014.09.05）「減災のための緊急地震速報の利活用ポイント」
・No.27（2014.10.07）「新たな食品リスクと食品事業者に求められる対応」
・No.28（2014.11.07）「人事評価制度の目標管理を成功に導くマネジメントシステムの考え方」
・No.29（2014.12.05）「土壌汚染に係る企業のリスクについて」

以　上

銀泉株式会社　概要

■設立　　昭和２９年５月（１９５４年）

■資本金　　３億7000万円

■代表者　　代表取締役社長　勝川 恒平

■社員数　　７００名

■事業内容　□ 保険代理店事業

＊ 損害保険代理店事業（取扱保険会社23社）
＊ 生命保険代理店事業（取扱保険会社19社）

□ 不動産事業

＊ ビルディング事業（首都圏・関西圏を中心に30棟の賃貸ビルを保有）
＊ 駐車場事業　（“GS Park”を約700ヶ所、20,000台の駐車場を運営）
＊ 不動産コンサルティング事業（有効活用コンサルティング）

■事業所　　本　　社　541-0043　大阪市中央区高麗橋4丁目6番12号
TEL　06-6202-2511　FAX　06-6202-6370
東京本社　102-0074　東京都千代田区九段南3丁目9番15号
TEL　03-5226-2203　FAX　03-5226-2905
名古屋支店/京都法人営業部/神戸支店/姫路法人営業部/広島支店/福岡支店

■主要株主　三井住友銀行、三井住友カード、アサヒグループホールディングス、京阪神ビルディング、サノヤス・ライド、日建設計、MS＆AD インシュアランスグループ、大和証券グループ本社、三井住友信託銀行グループ

■ﾎｰﾑﾍﾟｰｼﾞ　**https://www.ginsen-gr.co.jp**

銀泉リスクソリューションズ株式会社　概要

■設立　　平成９年６月（１９９７年）

■資本金　　１億円　（銀泉㈱100%出資）

■代表者　　代表取締役社長　久保出 俊博

■社員数　　４０名

■事業内容　＊ 保険ブローカー（仲立人）業務
＊ 最適保険プログラムの構築支援
＊ グローバル最適保険プログラムの構築支援
＊ リスクマネジメント・人事労務コンサルティング

■事業所　　本　　社　102-0074　東京都千代田区九段南3丁目9番14号
TEL　03-5226-2212　FAX　03-5226-2609
大阪本社　541-0043　大阪市中央区高麗橋4丁目6番14号
TEL　06-6205-6221　FAX　06-6205-6236

■ﾎｰﾑﾍﾟｰｼﾞ　**http://www.ginsen-risk.com**

Risk Solutions Report　Vol.10　　2015年1月1日発行
銀泉リスクソリューションズ株式会社　Risk Solutions Report 編集委員会 事務局
TEL：03-5226-2212（代表）　FAX：03-5226-2884

銀泉株式会社
東京 TEL.03-5226-2203　大阪 TEL.06-6202-2511
URL: https://www.ginsen-gr.co.jp

GINSEN RISK SOLUTIONS 銀泉リスクソリューションズ株式会社
東京 TEL.03-5226-2212　大阪 TEL.06-6205-6221
URL: http://www.ginsen-risk.com