企業における営業秘密管理に関する実態調査 2020

調査実施報告書

令和3年　3月

独立行政法人情報処理推進機構

（実施：みずほ情報総研株式会社）

IPA Information-technology Promotion Agency, Japan

目　次

1 はじめに

1.1 背景及び目的

企業の技術情報や顧客情報等、営業上重要な情報である営業秘密の漏えいが後を絶たず、近年、大型の訴訟事例や海外からの営業秘密侵害事案の例も発生している。営業秘密の活用は企業の競争力の強化に重要な役割を果たす一方、ひとたび営業秘密が漏えいすると、事業に深刻な影響を及ぼすことから、その保護は喫緊の課題である。

営業秘密の保護については、第四次産業革命を背景に、ビッグデータ等の解析技術の進展等を踏まえ、不正競争防止法[1]第 5 条の 2 の「技術上の秘密」として「情報の評価又は分析の方法」を対象とすること、「技術上の秘密を使用したことが明らかな行為」として「情報の評価又は分析の方法を使用して評価し、又は分析する役務の提供」を対象とすること等を規定した不正競争防止法施行令が 2018 年 11 月 1 日に施行[2]された。また、クラウド管理等、情報の管理形態の多様化等を踏まえた営業秘密管理指針の改訂[3]が 2019 年 1 月 23 日に行われる等、政府による環境整備が進められている。

このような背景を受け、企業に対し、営業秘密の保護強化に向けた、情報セキュリティ対策等の実施を促す必要がある。

独立行政法人情報処理推進機構（以下「IPA」という。）では、企業における営業秘密の漏えいの発生状況や被害状況、漏えい対策や事後対応等の実態を明らかにし、営業秘密漏えいを防ぐために有用な対策等を分析するとともに、その情報を広範に提供することで、営業秘密の保護強化に資することを目的として、「企業における営業秘密管理に関する実態調査 2020」（以下「本調査」という。）をみずほ情報総研株式会社への委託により実施した。

なお、営業秘密管理に関する調査として、2016 年度に IPA が「企業における営業秘密管理に関する実態調査[4]」（以下「2016 年度調査」という。）を実施しているが、本調査は、2016 年度調査も参考にしながら、社会的変化を踏まえ、最新動向を反映した情報の提供を目指したものである。

---

[1] 平成五年法律第四十七号

[2] 経済産業省：「不正競争防止法第十八条第二項第三号の外国公務員等で政令で定める者を定める政令の一部を改正する政令」が閣議決定されました
https://www.meti.go.jp/press/2018/09/20180904001/20180904001.html

[3] 経済産業省：営業秘密管理指針（最終改訂：平成 31 年 1 月 23 日）
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

[4] IPA：企業における営業秘密管理に関する実態調査
https://www.ipa.go.jp/security/fy28/reports/ts_kanri/index.html

1.2 実施内容

本調査において実施した内容は次の通りである。

1.2.1 文献及び裁判例調査

企業における営業秘密の漏えいや保護対策に関連した最新の動向や裁判例について、それぞれ以下の調査を実施した。

(1) 文献調査

営業秘密漏えい及び保護対策に関連する国内や海外のレポート等計 21 文献についての調査を実施した。これらの文献調査により、営業秘密漏えいの発生状況や営業秘密保護対策に関する最新の動向を整理すると共に、アンケートの調査項目とすべき事項の検討における参考とした。

(2) 裁判例調査

2016 年以降に判決が示された裁判例のうち、営業秘密性が争点となったものを中心に 22 例の事例を収集し、秘密情報の保護対策の実施状況が判決に及ぼす影響について整理ならびに考察を行った。

1.2.2 アンケート調査

国内企業 16,000 社を対象に、書面による調査票を郵送にて送付・回収する形式にて、アンケート調査を実施した。本調査における企業の属性（業種、従業員数）毎の最低回収数は次表の通りであり、それぞれ所定の最低回収数以上の回収を実現した。

表 1.2-1　本調査で実施するアンケート調査における業種別・従業員別の最低回収数

	製造業	非製造業
従業員 301 名以上	300 社以上	400 社以上
従業員 300 名以下	300 社以上	400 社以上

1.2.3 インタビュー調査

営業秘密漏えいや管理の実態、法的な観点から実施すべき対策等を把握するため、以下のインタビュー調査を実施した。なお、新型コロナウイルスの感染状況を踏まえ、いずれもオンラインインタビューによる調査にて実施した。

(1) 企業へのインタビュー

営業秘密の漏えいや管理に関する実態についてより詳細を把握するため、アンケート調査においてインタビュー調査への対応が可能と回答した国内企業 5 社に対して、インタビュー調査を実施した。実施に際しては、アンケート調査の深掘りを中心として、各社における情報管理において重点を置いている事項や課題と考えている事項についての把握を行った。

(2) 法律の専門家へのインタビュー

法的な観点から、営業秘密漏えいの実態及び企業で実施すべき対策を把握するため、法律の専門家 2 人に対して、インタビュー調査を実施した。

1.3 略称について

本報告書で用いる略称は、それぞれ次の意味を示すものとする。

AI	人工知能
BYOD	Bring your own device（私物機器の業務利用）
CAD	コンピュータ支援設計
CC	Carbon Copy（並列配布する宛先）
CASB	Cloud Access Security Broker
CSR	企業の社会的責任
DVD	Digital Versatile Disc
DTSA	米国　連邦営業秘密保護法
DX	デジタルトランスフォーメーション
EEA	米国　連邦経済スパイ法
Emotet	エモテット（コンピュータウイルスの一種）
Excel	Microsoft Excel
EU	欧州連合
ESG	環境・社会・ガバナンス（持続可能な成長を目指すための 3 要素）
FAX	ファクシミリ
FBI	米国　連邦捜査局
ID	識別番号
IPA	独立行政法人情報処理推進機構
ISMS	情報セキュリティマネジメントシステム
IT	情報技術
ITC	国際貿易委員会
JNSA	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
JPCERT/CC	一般社団法人 JPCERT コーディネーションセンター
OJT	オン ザ ジョブ トレーニング
OS	オペレーティングシステム
PDCA	Plan Do Check Action サイクル
PC	パーソナルコンピュータ
SaaS	Software as a Service
SIEM	Security Information and Event Management
SNS	ソーシャル ネットワーキング サービス
UTSA	米国　統一営業秘密法
URL	Uniform Resource Locator
USB	ユニバーサル シリアル バス
VPN	バーチャルプライベートネットワーク
Web	ウェブ
Word	Microsoft Word

2 実態調査の概要

本章では、本調査において実施した調査項目毎の調査設計と結果について説明する。

2.1 調査仮説の設定

調査の実施に先立ち、アンケート調査の設計に資することを目的として、現在の国内企業における営業秘密管理の実態に関して調査仮説を設定した。具体的な内容を次に示す。

2.1.1 前回からの変化

2016 年度調査の時点からの変化に関して示した仮説は、以下に示す(1)～(4)の通りである。

(1) 内部不正対策は進展したか？

① 秘密保持に関する誓約書の徴求や就業規則の見直しを行う企業が増加

営業秘密漏えいに関する報道等を受けて、内部不正による情報持ち出し抑制のため、誓約書の徴求や就業規則の見直しを行った企業が増加することが見込まれる。

② 内部不正を原因とする情報漏えいインシデントの発生は微減

技術的対策と組織的対策の組み合わせが普及し、内部不正を原因とするインシデントの発生傾向は微減となることが見込まれる。

③ クラウドサービス上の秘密情報の不正利用対策は進展していない

クラウドサービスで秘密情報を共有している場合の不正利用対策については、対策の認知度が低いこともあって導入が進んでいる企業は少ないと見込まれる。

(2) 中小企業における情報管理対策は進展したか？

① 情報漏えいの生じた企業の比率はやや増加

情報漏えいの生じた企業の比率は、対策が進む一方で企業におけるデジタル活用の進展の勢いには及ばず、2016 年度調査と比べてやや増加していると見込まれる。

② 情報漏えいの発生頻度は中小規模企業よりも大規模企業において高い

2016 年度調査と同様、大手と中小で比較すると、大手企業における発生数が多くなるものと思われる。これは中小企業ではそもそも漏えいに気づく企業が少ないことによる。

③ 連携先やサプライチェーンを通じた情報漏えいが増加

情報漏えいの原因は、2016 年度調査に引き続き過失によるものが最多であるが、連携活動の活発化等の影響で連携先やサプライチェーンを通じたものが増えると見込まれる。

④ 漏えいする情報の種類は引き続き顧客情報・個人情報が最多

流出した情報は 2016 年度調査に引き続き顧客情報・個人情報に関するものが最多である一

方で、技術情報の事例も増えると見込まれる。

⑤ 営業秘密のレベル別管理を行っている企業は増えていない

営業秘密をその他の情報と何らかの形で区分している企業は多いと見込まれるが、そのうちレベル毎の格付けまで行っている例は依然として限られるものと想定される。

⑥ 企業内でルールが適切に運用されているとは限らない

営業秘密を扱う企業において、情報の格付けがルールとして定められていても、実運用でそれが適切に運用されているとは限らない。

(3) 情報管理に関する強化のきっかけはあったか？

① 情報管理強化のきっかけは取引先からの要求が最多

企業における情報管理の強化のきっかけは「取引先からの要求」が最多であり、「自社でのインシデント（未遂を含む）」、「他社のインシデント」が続くものと想定される。それがなければ情報管理の強化に取り組まれることはない。

(4) 「秘密情報の保護ハンドブック」を活用している企業では、同ハンドブックに対して追加的なニーズが潜在的にあるのではないか？

① 現行ハンドブックに記載のない対策の情報提供ニーズ

「情報管理に関する特権の悪用防止対策」や「秘密情報の不正利用検知技術」など、現行のハンドブックに具体的な対策の記載はないが、企業で今後必要となる対策に関する情報提供ニーズが示される可能性がある。

2.1.2 法改正の影響

2018 年における改正不正競争防止法の施行を踏まえ、このような法改正が企業における営業秘密管理に及ぼした影響に関して、次のような仮説を設定した。

(1) 不正競争防止法改正の効果はあったか？

① 一部の企業が限定提供データとして保護することを前提とする契約ひな型等を整備

AI やビッグデータを扱う企業の一部が、限定提供データとして保護することを前提に、規定や手続等を整備していることが考えられる。

② 限定提供データを対象とした不正競争行為を認める裁判例の出現

改正後十分な時間を経ていないこともあり実際に出現する可能性は小さいものの、限定提供データの要件を満たす営業情報に対する不正競争行為を認める裁判例が出現する可能性がある。

③ 技術的制限手段の効果を妨げる不正競争行為を認める裁判例の出現

②と同様、改正後十分な時間を経ていないこともあり実際に出現する可能性は小さいものの、技術的制限手段の効果を妨げることを目的とした代行サービスを不正競争行為とする裁判例が

出現する可能性がある。

(2) 営業秘密に関する訴訟・判決に変化は見られるか？

① 秘密管理性の認定に係るアクセス制御方法の有効性判断に関して新たな裁判例が出現

近年のアクセス制御に関する技術の発展や対応製品・サービスの増加を踏まえて、そうしたアクセス制御の実施状況を考慮した判決が新たに示される可能性がある。

② 非公知性の認定に係る情報の管理方法に関する判断を含む新たな裁判例が出現

企業における情報の管理方法に応じて、営業秘密の非公知性に関して判決で新たな判断が示される可能性がある。

③ 欧米の営業秘密保護に係る判例が国内にも影響

グローバルで事業展開を行っている企業での取組や営業秘密に関する海外とのトラブル等を通じて、米国及び欧州で 2016 年に施行された営業秘密に関する法規制の影響が示される可能性がある。

2.1.3 ニューノーマル環境での営業秘密管理状況等

2020 年における新型コロナウイルスの蔓延及びそれに伴う同 4 月の緊急事態宣言等が企業における営業秘密管理にどのような影響を及ぼしたかに関して、次のような仮説を設定した。

(1) ウィズコロナ、ポストコロナで課題や対策は変化しているか？

① 国内企業のうち 2～3 割程度がコロナ禍で情報管理のルール見直しを実施

非常事態宣言を踏まえて情報管理のルールの見直しを行ったところは 2～3 割と見込まれ、以前から対応済みの企業が 2 割、今回暫定ないし例外の扱いを定めた企業が 3 割として、計 7～8 割の企業で何らかの対策が講じられたと想定される。

② テレワークの導入で営業秘密該当性が損なわれる可能性の認知が進んでいない

テレワークが急速に浸透する中で、営業秘密該当性を満たさない環境で営業秘密データが扱われる結果、営業秘密に対する法的救済が機能しない状況が生じている恐れがあるが、それが企業で認識されていない。

③ テレワークの導入を通じて企業におけるペーパーレス化が進展

企業におけるテレワーク導入を通じて、企業におけるペーパーレス化が進展。ただし電子データへのアクセス制御とセットで管理している企業は少ない。

④ クラウドを通じた秘密情報の共有が進む一方、その不正利用対策は不十分

クラウドサービスを用いた社内外での秘密情報の共有が進んでいると見込まれる。一方でクラウドを通じた不正なデータ流出が生じた場合の証跡確保、責任の明確化等の対策を講じている企業はわずかと想定される。

2.2 アンケート調査

2.2.1 調査設計

本調査の実施に先立ち、2.1 項に示した調査仮説を踏まえ、調査票の設計において考慮した事項は次の通りである。

(1) 調査項目数の抑制

2016 年度調査は 60 項目の構成にて実施された。この結果、2012 年度に実施された類似調査（39 問構成）において回収率が 30.1%であったものが、2016 年度調査では 18.1%に低下している。この背景として、アンケート調査の調査項目数が 39 問から 60 問へと約 1.5 倍になったことで、回答に要する負担を嫌って回答しない企業が増えたこと推察される。こうした実態を踏まえ、本調査においては調査項目を 40 項目程度に抑制することを目標に実施することとした。さらに 2.2 項にて示した調査仮説のうち、ニューノーマル環境の影響に係る調査項目については新たに追加の必要があることから、2016 年度調査において尋ねた項目のうち、本調査で継続的な把握が困難となるものが生じることは避けられない。そこで、本調査における調査対象から除外する項目の選定にあたっては、2016 年度調査における調査項目のうち、経年による変化が生じにくいと見込まれるものを優先して選ぶこととし、具体的には以下の調査項目を除外することとした。

- 情報の区分や格付けの見直しの実施状況、頻度
- 企業における営業秘密管理に関する問題の位置づけ
- ノウハウの管理や活用に関して実施している取組
- ノウハウのライセンス化や形式知化の状況
- オープンイノベーションに関する企業としての方針
- 経営資源としてのデータの位置付けに関する状況
- 退職者、取引先、外部者に対して実施している特有の対策
- 転職者が以前所属していた企業等の営業秘密に触れてしまうことを防ぐための対策
- 外部の研究者等によって開示された営業秘密を侵害してしまうことを防ぐための対策
- 対策の有効性に関する自己評価
- 政府機関等による営業秘密に関する情報提供に関して希望する内容

また、以下に示す調査項目については 2016 年度調査において複数の調査項目で尋ねていたものを集約することで、調査項目数の抑制と経年変化の把握の両立に努めることとした。なおこの結果、2016 年度調査での回答者数が異なる調査項目を集約したものについて、経年変化に関するグラフ上での集計母数と比率との対応関係が 2016 年度調査結果では不正確になっているものがある。それらのグラフでは、2016 年度調査結果の数値については参考値として参照することが適切である。

- 秘密情報の保護対策のうち、アクセス制御に関するものの導入状況
- 秘密情報の保護対策のうち、持ち出しの制御に関するものの導入状況
- 秘密情報の保護対策のうち、漏えいしにくい環境作りに関するものの導入状況

(2) 新型コロナウイルスの蔓延が調査に及ぼす影響の考慮

調査設計を行った 2020 年 8 月から 9 月の時点で、調査実施時期となる同年 10 月～11 月にお

ける新型コロナウイルスの影響として、次のような状況が想定された。

- 一部の業種において事業への負の影響が深刻であり、調査時点で休廃業となっている企業が一定比率存在する可能性がある。
- 在宅・テレワーク勤務の影響により、組織内でのやりとりにこれまでよりも時間を要することで、期限内の回答が困難となる企業が増える可能性がある。

こうした状況を踏まえ、本調査においては以下の対応をとることとした。

- 回答率の低下を前提に、アンケート送付数を増加させる。
- 回答期間として、企業内での担当者への回付、回収等に必要な日数を加味する。

2.2.2 アンケート調査票送付先リストの作成

アンケート調査票の送付数と送付先は次の要領にて実施した。

(1) 企業データベースの選定

企業信用調査を実施する会社の企業情報データベースとして、本調査では株式会社東京商工リサーチの提供する「TSR 企業情報ファイル」を利用した。同社のデータベースは属性の種類により費用が異なるが、本調査では本項(3)に示す業種・規模に応じた構成の選定に必要十分な属性として、「283byte」（所在値、従業員数、資本金、業種コード等を含む）を選定した。

(2) アンケート調査票の送付数の決定

本調査では、1.2.2 項に示す「業種別・従業員別の最低回収数」に示された条件を満たす有効回答数 1,400 件の回収を行う必要がある。2016 年度調査によれば、12,000 社への郵送により下表に示す回収実績が得られている（有効回答 2,175 件、回収率 18.1%。なお同表には業種または従業員数を回答しなかった 24 社が含まれない）。

表 2.2-1　2016 年度調査における回収実績

	製造業	非製造業
従業員 301 名以上	449 社	599 社
従業員 300 名以下	433 社	670 社

2.3.1 項に示したように、本調査では調査項目数を 43 項目に抑制し、調査票のページ数も 16 ページから 12 ページに削減したことで、回収率の向上を期待し得る。しかしながら、前述の通り新型コロナウイルスが社会に及ぼしている影響は依然として無視できるものではなく、特に従業員数 300 名以下の中堅・中小企業において、小売業、運輸業、飲食・観光等のサービス業をはじめとして事業継続に深刻な影響を与えており、回答対応が困難な企業も多いと推察される。そこで、企業の従業員数に応じて次のように異なる回答率を推定し、従業員 300 名以下の企業への送付数を増やすことで、合計 16,000 社に回答を依頼することにより、十分な回収数の確保を実現することとした。

表 2.2-2　企業の従業員数毎の回収率推定に基づく送付数

従業員数	回収率の推定 (A)	送付数 (B)	回収見込み数（A×B）	
1～100 名	5%	4,293 社	214 社	計 761 社
101～300 名	10%	5,470 社	547 社	
301 名以上	12%	6,237 社	748 社	
合計	－	16,000 社	1,509 社	

(3) 従業員数及び業種毎の送付数の割り付け

2016 年度調査における回答企業の従業員数に基づく規模別の構成は次図の通りである。

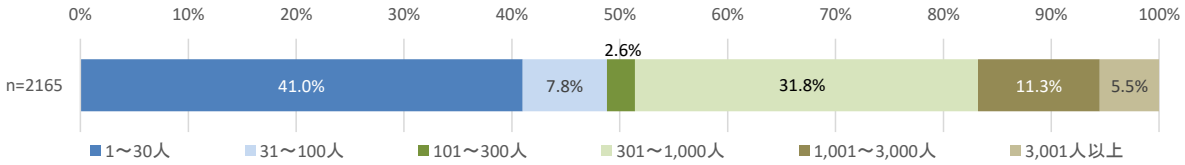

図 2.2-1　2016 年度調査における回答企業の規模別構成

規模毎の企業数は従業員数と反比例の関係にあるが、上図では 101～300 名までと 301～1,000 名の規模のところで比率が大きく異なっている。これは、「従業員 300 名以下」と「従業員 301 名以上」の 2 つの集合でそれぞれランダムに抽出したことによるものであるが、実態の反映の観点からすればややアンバランスな傾向となっている。また、従業員数 30 名以下の企業で全回答の 4 割を超えているのは、実際の企業数の反映という点では問題ないが、こうした小規模・零細企業では一般に実施可能な営業秘密保護対策が限定されることから、本調査の趣旨を踏まえると、中規模以上の企業の構成比率をより高めることが望ましい。

そこで、本調査では従業員数をより細かく区分して割り付けを行うこととし、(2)で定めた送付総数について、(1)で選定した企業データベースにおける業種毎の企業登録数を参考にランダム抽出と割り付けを実施した結果、送付リストにおける企業の構成は次表の通りとなった。この際、製造業については従業員 300 名以下、301 名以上それぞれについて 300 社以上の回収が求められていることから、これを考慮した割り付けを行っている。

表 2.2-3　従業員数・業種毎の割り付け状況

業種 (TSR 企業情報ファイルの分類)	従業員数毎の企業数							合計	構成比率
	1～4 名	5～30 名	31～100 名	101～300 名	301～1,000 名	1,001～3,000 名	3,001 名以上		
農林業	2	4	5	1	2	0	0	14	0.1%
漁業	2	4	4	1	0	0	0	11	0.1%
鉱業、採石業、砂利採取業	2	4	4	1	1	0	0	12	0.1%
建設業	9	32	195	229	109	26	5	605	3.8%
製造業	67	226	1,493	2,273	1,960	488	176	6,683	41.8%
電気・ガス・熱供給・水道業	2	7	39	34	17	15	13	127	0.8%
情報通信業	9	32	212	434	308	105	27	1,127	7.0%
運輸業、郵便業	9	29	219	422	307	83	24	1,093	6.8%
卸売業、小売業	18	63	410	719	619	107	32	1,968	12.3%
金融業、保険業	9	31	207	359	101	57	15	779	4.9%
不動産業、物品賃貸業	5	20	130	152	67	15	7	396	2.5%
学術研究、専門・技術サービス業	5	18	121	174	153	39	4	514	3.2%
宿泊業、飲食サービス業	5	19	100	120	136	31	7	418	2.6%
生活関連サービス業、娯楽業	5	18	99	114	56	16	3	311	1.9%
教育、学習支援業	3	10	53	60	21	2	0	149	0.9%
医療、福祉	7	23	129	146	118	12	2	437	2.7%
複合サービス業	2	7	37	51	96	17	3	213	1.3%
サービス業(他に分類されないもの)	5	16	107	180	648	143	44	1,143	7.1%
合計	166	563	3,564	5,470	4,719	1,156	362	16,000	
構成比率	1.0%	3.5%	22.3%	34.2%	29.5%	7.2%	2.3%		

2.2.3 実施及び調査票回収の状況

(1) アンケート調査票の発送

例年、12 月は企業活動の繁忙期であり、アンケート回答期限を 12 月に設定するのは適切でないことから、本調査におけるアンケート調査の回答期限は 2020 年 11 月 27 日に設定した。

さらに 2.3.1 項にて示した通り、新型コロナウイルスの影響で在宅もしくはテレワーク形態での勤務を行う企業が多いと予想され、企業内での回答対応に通常よりも時間を要すると見込まれることから、回答期間として約 1 ヶ月を設定し、2020 年 10 月 26 日に郵送にてアンケート調査票の発送を行った。

(2) 調査票回収の状況

① 企業規模に基づく回答状況の分析

前述の通り、新型コロナウイルスの影響で大幅な回答率の低下が懸念されたが、実際の回答数は下表の通り有効回答数 2,175 件（無効回答 3 件を除いた件数）、回答率 13.6%であり、中小企業における大幅な回答率の低下は生じず、むしろ従業員 301 名以上の大企業において回答率が伸び悩む結果となった。なお、製造業において、従業員 1,001～3,000 名のグループと 3,001 名以上のグループとで回答率に著しい差が生じているが、これは用語定義における従業員の定義として、「自社内の実習生、派遣労働者、委託先従業員であって自社内で勤務する者を含める」ことを求めていることから、TSR 企業情報ファイルにおいて従業員 1,001～3,000 名とされている企業において、これらの人数を含めて従業員 3,001 名以上として回答しているケースが存在することによるものと推察される。実際に、製造業の従業員 1,001 名以上を 1 つの区分として回答率を算出すると 11.9%となり、妥当な結果となる。

表 2.2-4　業種毎の回答率

従業員数	製造業（企業数）			非製造業（企業数）		
	送付数	回収数	回答率	送付数	回収数	回答率
1～4 名	67	10	14.9%	99	22	22.2%
5～30 名	226	41	18.1%	337	56	16.6%
31～100 名	1,493	196	13.1%	2,071	300	14.5%
101～300 名	2,273	336	14.8%	3,197	443	13.9%
301～1,000 名	1,960	225	11.5%	2,759	323	11.7%
1,001～3,000 名	488	40	8.2%	668	95	14.2%
3,001 名以上	176	39	22.2%	186	38	20.4%
300 名以下合計	4,059	583	14.4%	5,704	785	14.4%
301 名以上合計	2,624	304	11.6%	3,613	438	12.6%
総合計	6,683	887	13.3%	9,317	1,277	13.7%
全業種総合計				16,000	2,164	13.5%
合計（企業規模未回答の企業を含む）				16,000	2,175	13.6%

② 業種に基づく回答状況の分析

業種毎の回答率を整理した結果を次表に示す。この結果を見ると、事業活動において新型コロナウイルスの影響が深刻とされる宿泊業、飲食サービス業において、平均をやや下回りながらも比較的堅調な回答率が得られている。このような傾向が示される原因として、本調査の実施用に TSR 企業情報ファイルを調達したのが 2020 年 10 月であり、同時期までに休廃業した企業がリストに含まれていなかったことが影響している可能性がある。

なお、従業員数毎の回答数については、表 2.2-3 に示す通り、業種によってサンプル数がわずか 1～5 件の場合もあり、統計的な傾向を分析することに用いるのは適切ではない。ただし、こうしたいわば国内でも事業者数が極めて少ない業種における実態についてのサンプルの回収ができているという点でみると、貴重なデータが得られているといえる。

表 2.2-5　従業員数・業種毎の回答率

業種	従業員数毎の回答率							業種全体の回答率
	1～4名	5～30名	31～100名	101～300名	301～1,000名	1,001～3,000名	3,001名以上	
農林業	0.0%	0.0%	60.0%	100.0%	100.0%	－	－	42.9%
漁業	0.0%	50.0%	75.0%	0.0%	－	－	－	54.5%
鉱業、採石業、砂利採取業	0.0%	50.0%	75.0%	0.0%	0.0%	－	－	41.7%
建設業	22.2%	25.0%	24.1%	16.2%	13.8%	38.5%	20.0%	19.8%
製造業	14.9%	18.1%	12.9%	14.7%	11.4%	8.2%	22.2%	13.2%
電気・ガス・熱供給・水道業	50.0%	14.3%	20.5%	26.5%	11.8%	20.0%	30.8%	22.0%
情報通信業	11.1%	3.1%	14.6%	14.3%	9.7%	9.5%	3.7%	12.1%
運輸業、郵便業	22.2%	6.9%	11.9%	13.5%	9.4%	7.2%	33.3%	11.9%
卸売業、小売業	27.8%	11.1%	12.2%	9.6%	10.5%	14.0%	28.1%	11.2%
金融業、保険業	22.2%	19.4%	16.4%	16.4%	36.6%	17.5%	46.7%	19.9%
不動産業、物品賃貸業	40.0%	10.0%	10.0%	9.2%	13.4%	0.0%	0.0%	10.1%
学術研究、専門・技術サービス業	60.0%	33.3%	10.7%	14.9%	15.7%	7.7%	0.0%	14.6%
宿泊業、飲食サービス業	40.0%	15.8%	6.0%	15.0%	7.4%	29.0%	42.9%	12.2%
生活関連サービス業、娯楽業	0.0%	5.6%	11.1%	10.5%	5.4%	18.8%	33.3%	10.0%
教育、学習支援業	0.0%	20.0%	18.9%	11.7%	23.8%	0.0%	－	16.1%
医療、福祉	0.0%	26.1%	14.7%	16.4%	16.1%	8.3%	0.0%	15.8%
サービス業(他に分類されないもの)	28.6%	30.4%	13.9%	20.3%	9.5%	15.0%	8.5%	12.9%

2.2.4 調査結果概要

アンケート調査の結果をもとに、単純集計及び検討の観点に応じたクロス集計の結果に基づく分析結果を示す。なお、個別の説明のない限り、帯グラフで示している結果は単一選択形式の質問、棒グラフで示している結果は複数選択形式の質問でそれぞれ尋ねた結果である。また、当該質問に無回答の場合は集計から除外しており、集計母数にも含めていない。

2.2.4.1 回答企業属性

(1) 回答企業の業種構成

今回の回答企業の業種構成を以下に示す。製造業については②にその細区分を示す。

① 全体構成

2016 年度調査と比較して、建設業、小売業の比率が低下し、他に分類されないサービス業の比率が増加している。

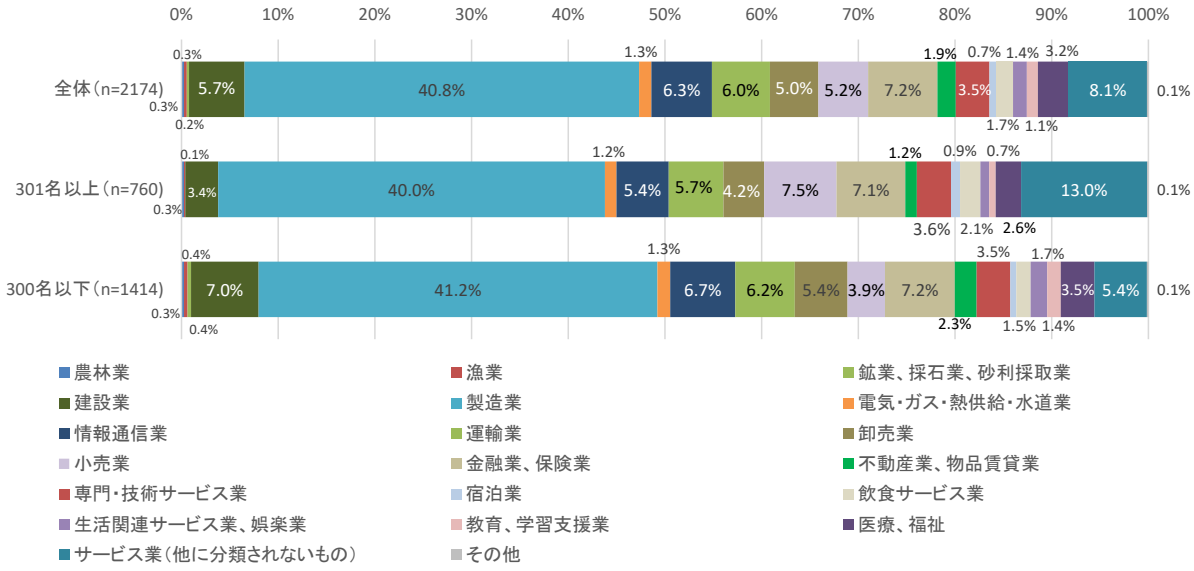

図 2.2-2 回答企業の業種構成（全体）

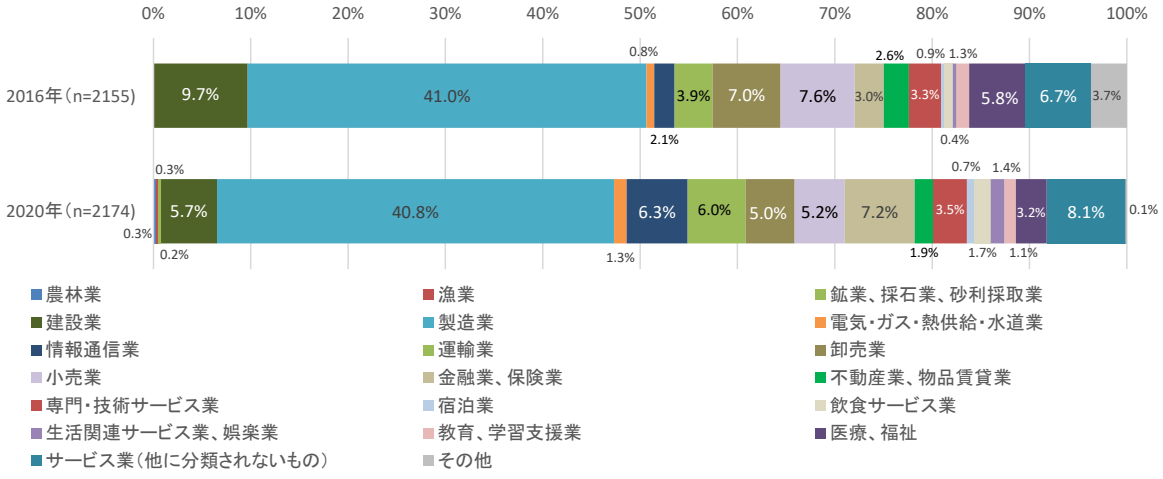

図 2.2-3 回答企業の業種構成（全体の経年比較）

② 製造業における細区分

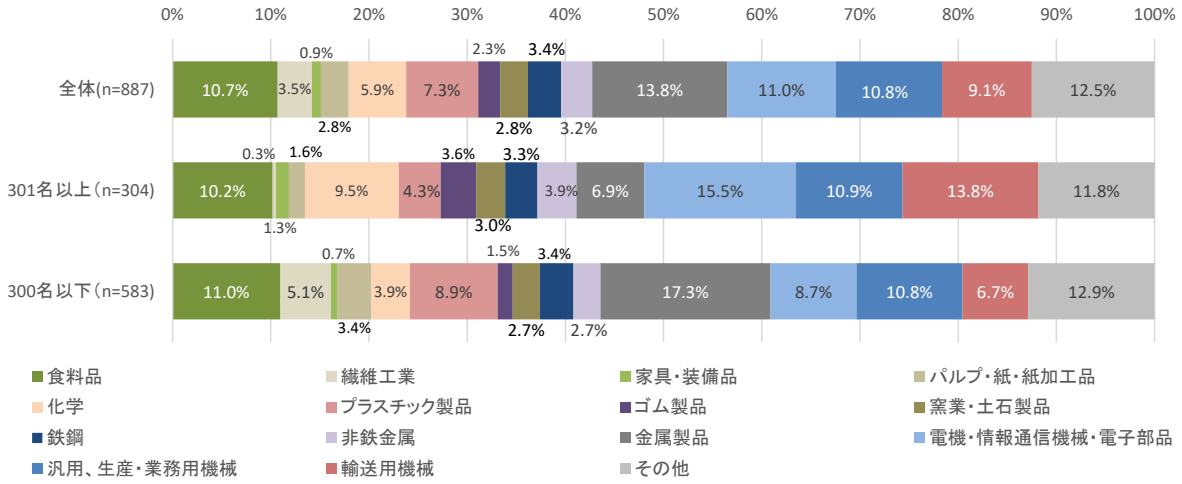

図 2.2-4　回答企業の業種構成（製造業における細区分）

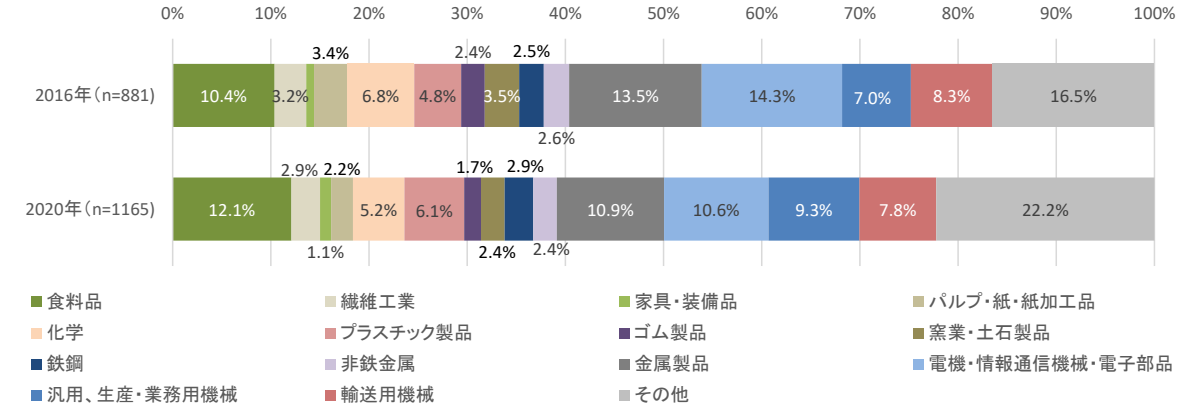

図 2.2-5　回答企業の業種構成（製造業における細区分の経年比較）

(2) 回答企業の規模構成

① 従業員数

今回の回答企業の従業員数に基づく規模構成は次の通りである。製造業とそれ以外とで構成比の差はほとんどない。

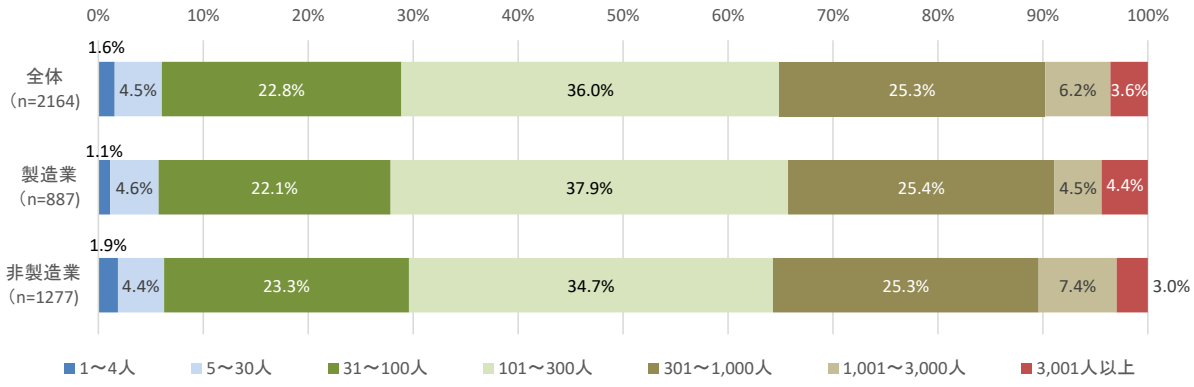

図 2.2-6　回答企業の規模構成（従業員数）

一方、2016 年調査と比較すると、構成比に大きな違いがあることがわかる。これは、2.2.2(3)における検討を反映した割付を行ったことによるものである。

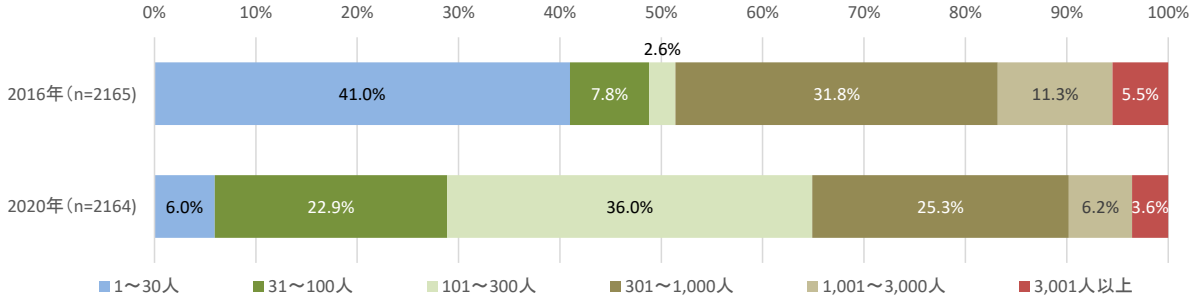

図 2.2-7　回答企業の規模構成（従業員数の経年比較）

② 資本金

今回の回答企業の資本金に基づく規模構成は次の通りである。「その他」には資本金の扱いがない法人を含む。

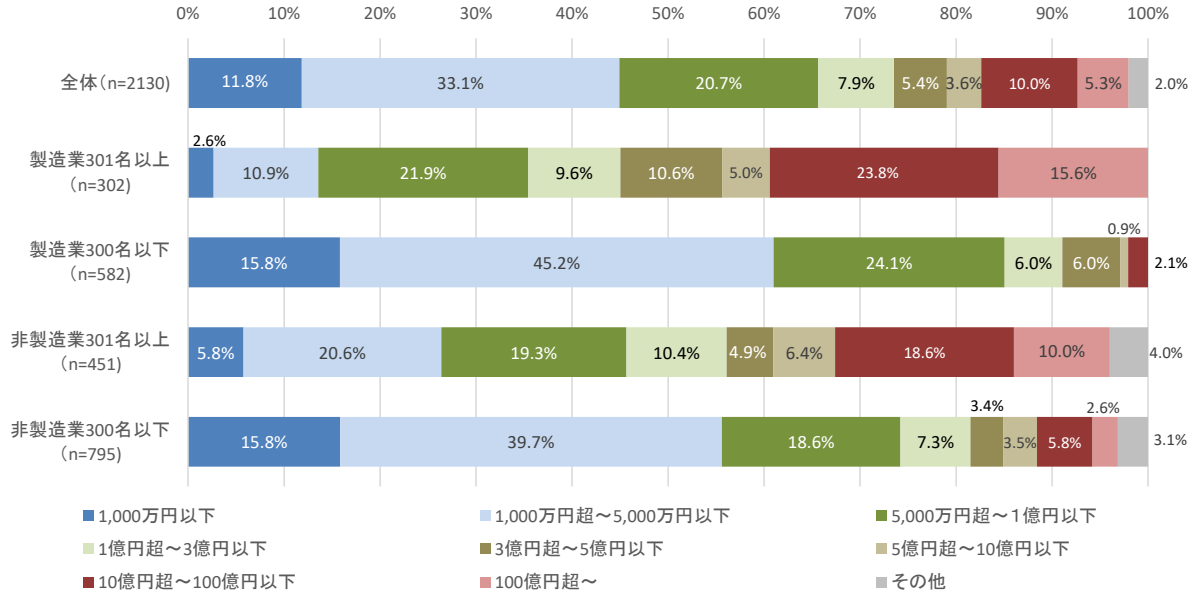

図 2.2-8　回答企業の規模構成（資本金）

③ 売上高

今回の回答企業の資本金に基づく規模構成は次の通りである。売上を有しない法人については、無記入により回答母数に含まれない場合と、「10 億円以下」として回答する場合の両方が含まれる。

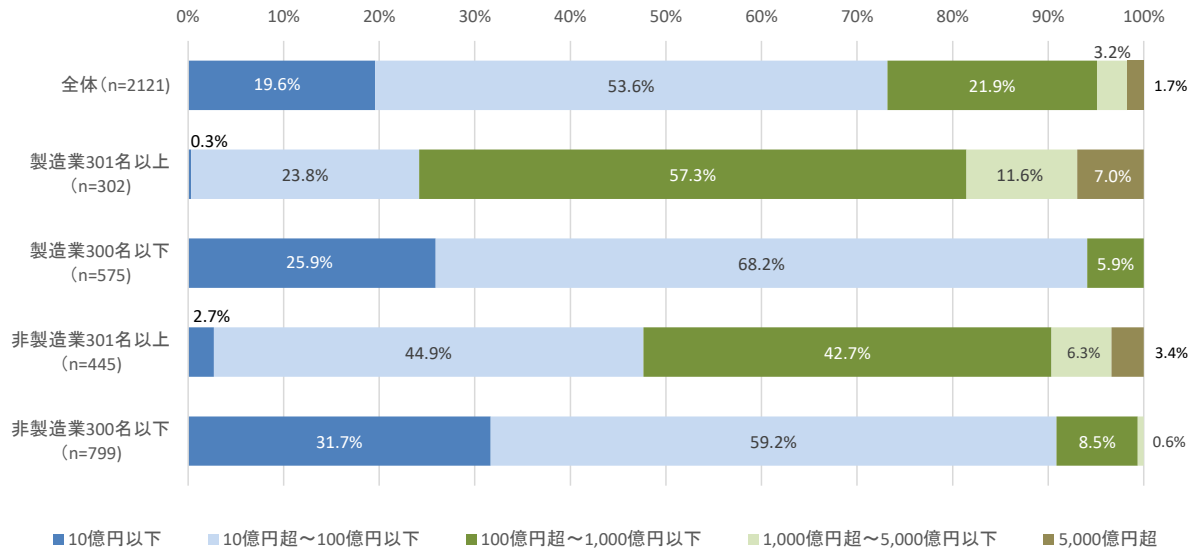

図 2.2-9　回答企業の規模構成（売上高）

2.2.4.2　営業秘密の漏えい実態

(1)　営業秘密漏えいの発生状況

過去５年以内における営業秘密漏えい事例の有無について尋ねた結果を示す。「情報漏えいの事例はない」の意味は、回答企業において営業秘密漏えいが発生していないことではなく、アンケートの回答者（リスク管理部署、情報管理担当部署、サイバーセキュリティ担当部署等）が漏えいの発生を把握していないことを表すものである。2016 年度調査との比較についての考察は、3.1 項にて行う。

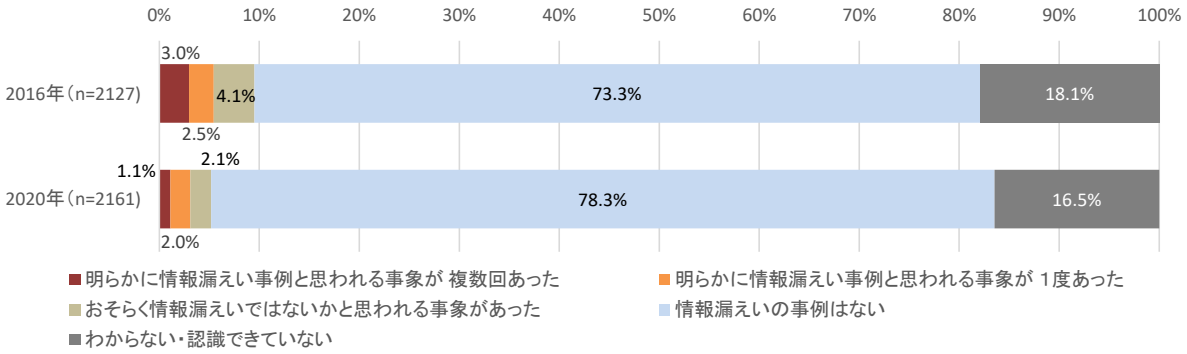

図 2.2-10　営業秘密漏えいの発生状況（経年比較）

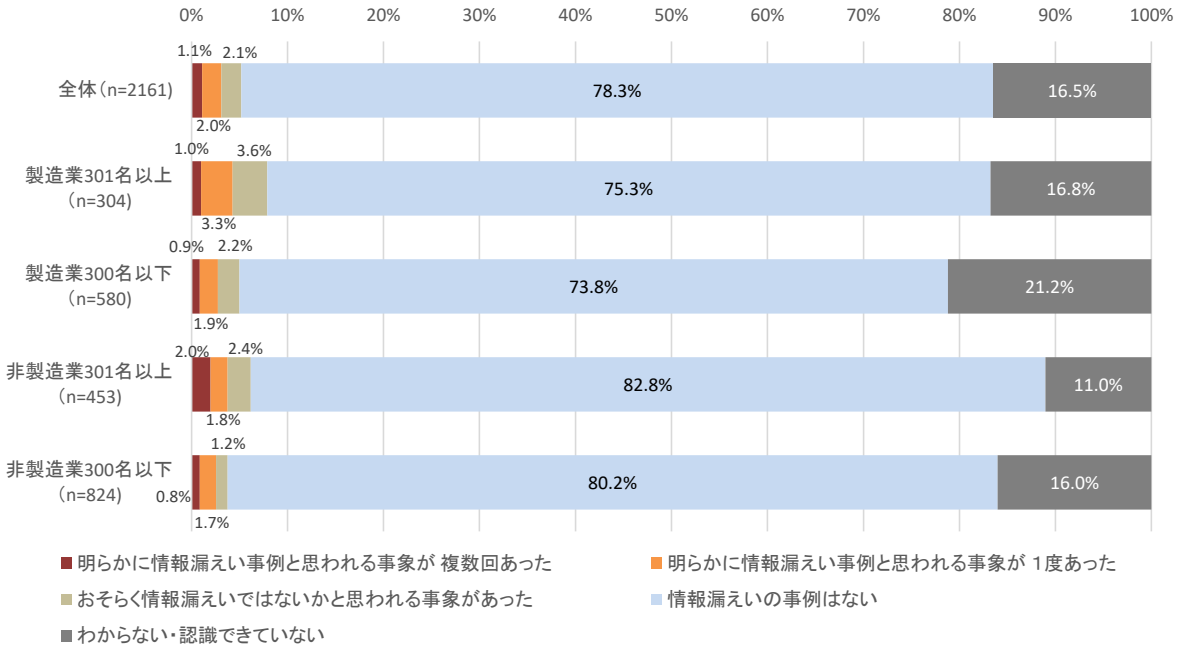

図 2.2-11　営業秘密漏えいの発生状況（業種・規模別４区分によるクロス集計）

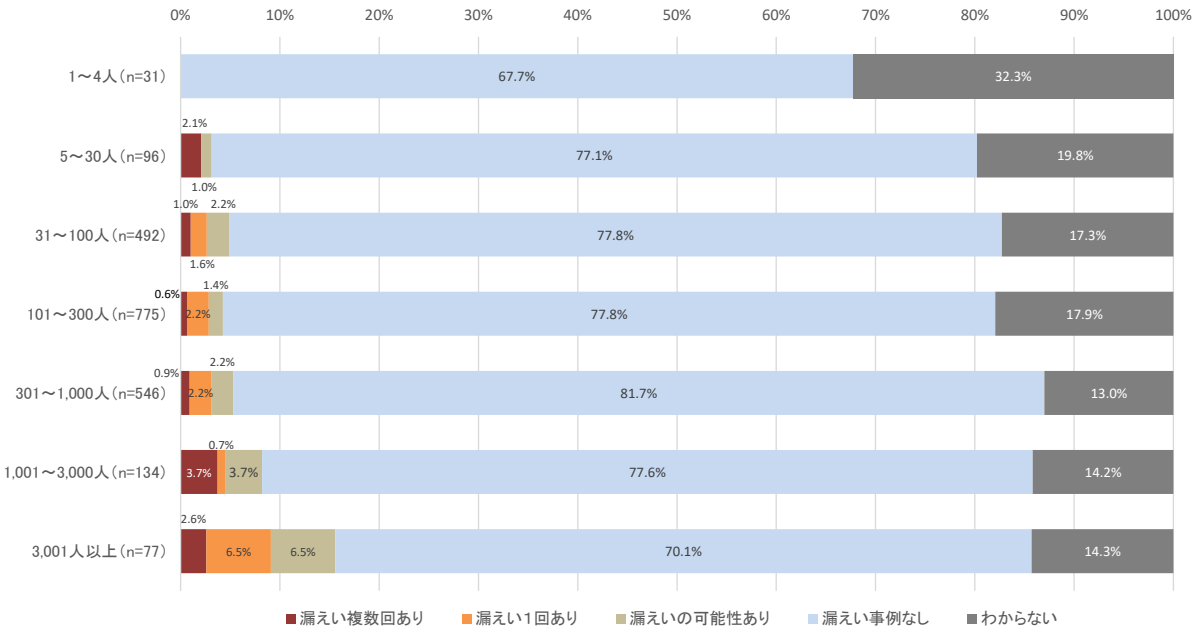

図 2.2-12　営業秘密漏えいの発生状況（規模別クロス集計）

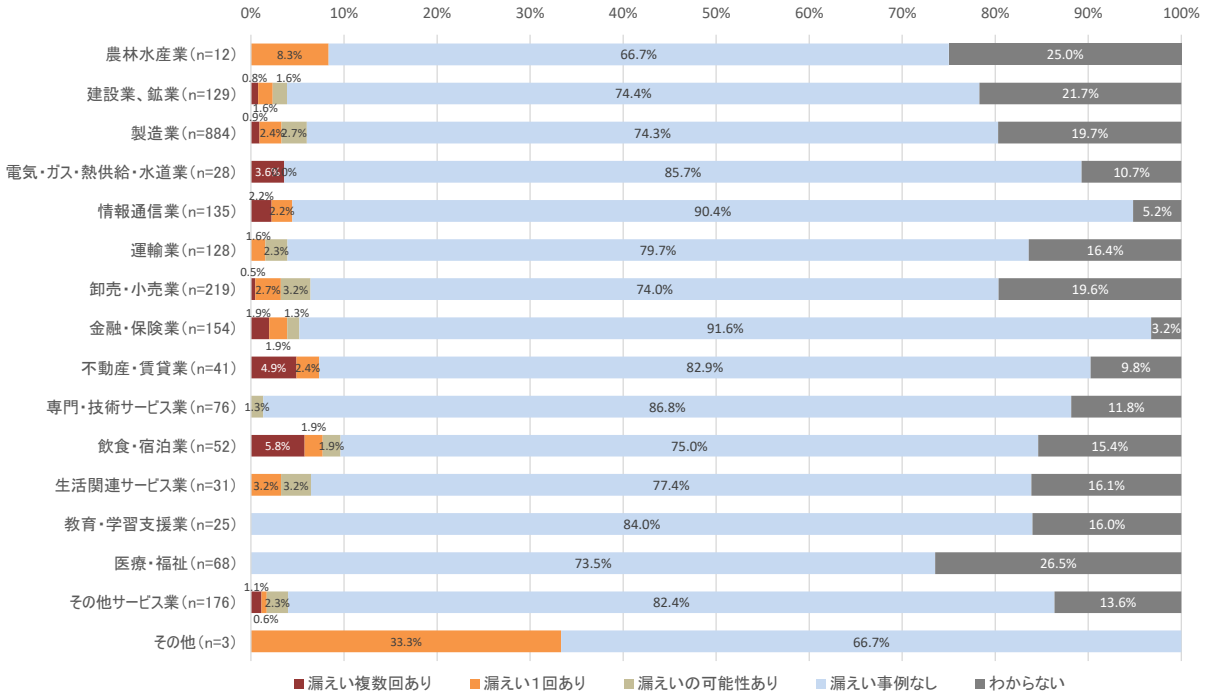

図 2.2-13　営業秘密漏えいの発生状況（業種別クロス集計）

(2)　漏えいした営業秘密の内容と重要性

漏えいした情報が具体的にどのような内容であったかと、その情報が自社の事業においてどの程度重要な情報であったかについて尋ねた結果を示す。なんらかの情報漏えいがあったとされた企業から漏えい項目の内容とその情報の重要性を得た。2016 年度調査においては、①～⑦の項目ごとに有無のみ尋ねているため図 2.2-14 では異なるグラフ形式にて表現している。

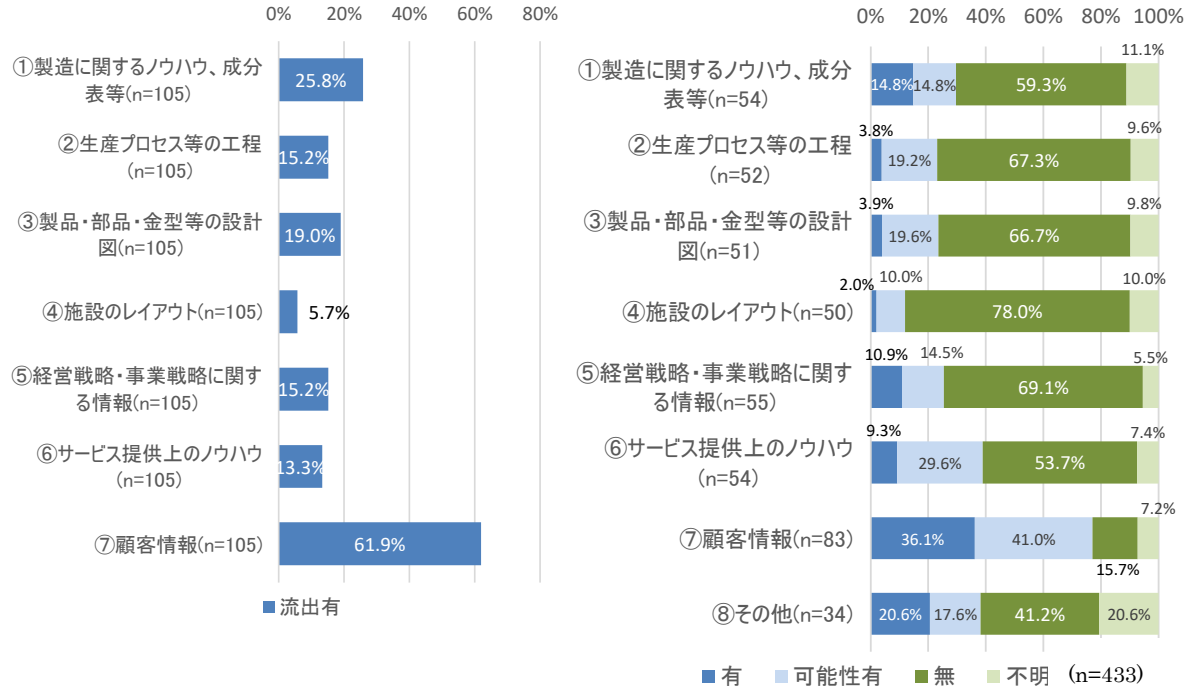

図 2.2-14　漏えいした営業秘密の内容（左図：2016 年、右図：2020 年）

2020 年度調査では、各項目で漏えい（可能性含み）ありと回答された内容の重要性も得ているが、一部「不明」からの回答もあり、図 2.2-14 から予測される母数より多くなっている。

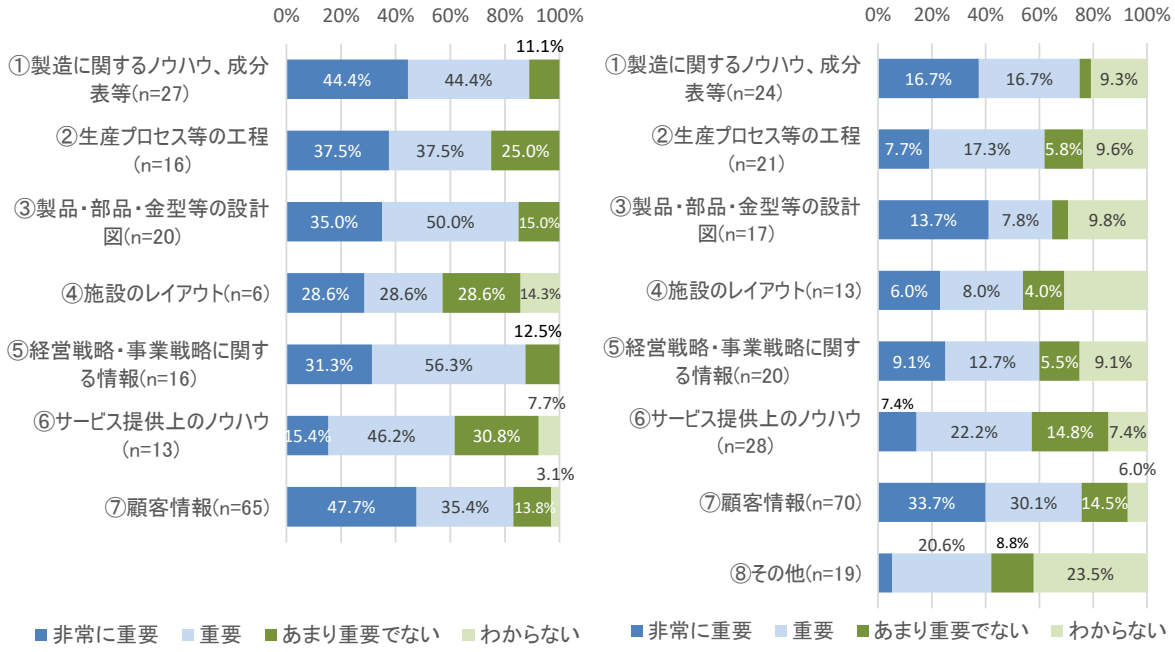

図 2.2-15　漏えいした営業秘密の重要性（左図：2016 年、右図：2020 年）

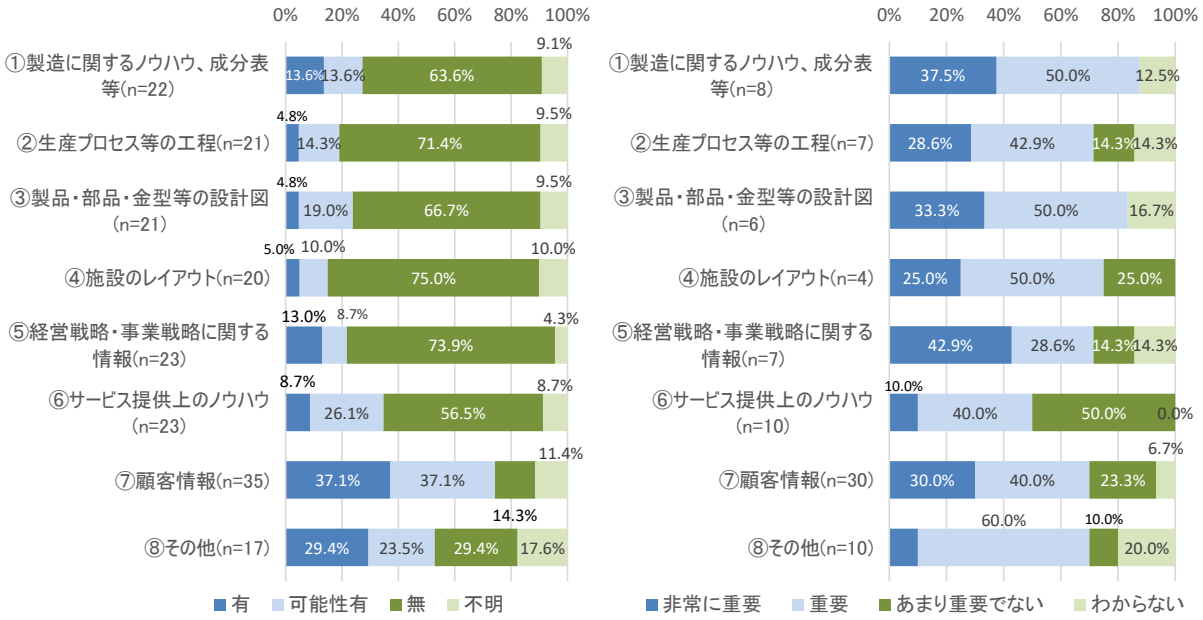

図 2.2-16　左図：営業秘密の内容と漏えい可能性（大規模企業：2020 年）
右図：漏えいした営業秘密の重要性（大規模企業：2020 年）
※大規模企業：人数 301 名以上、中小規模企業：人数 300 名以下

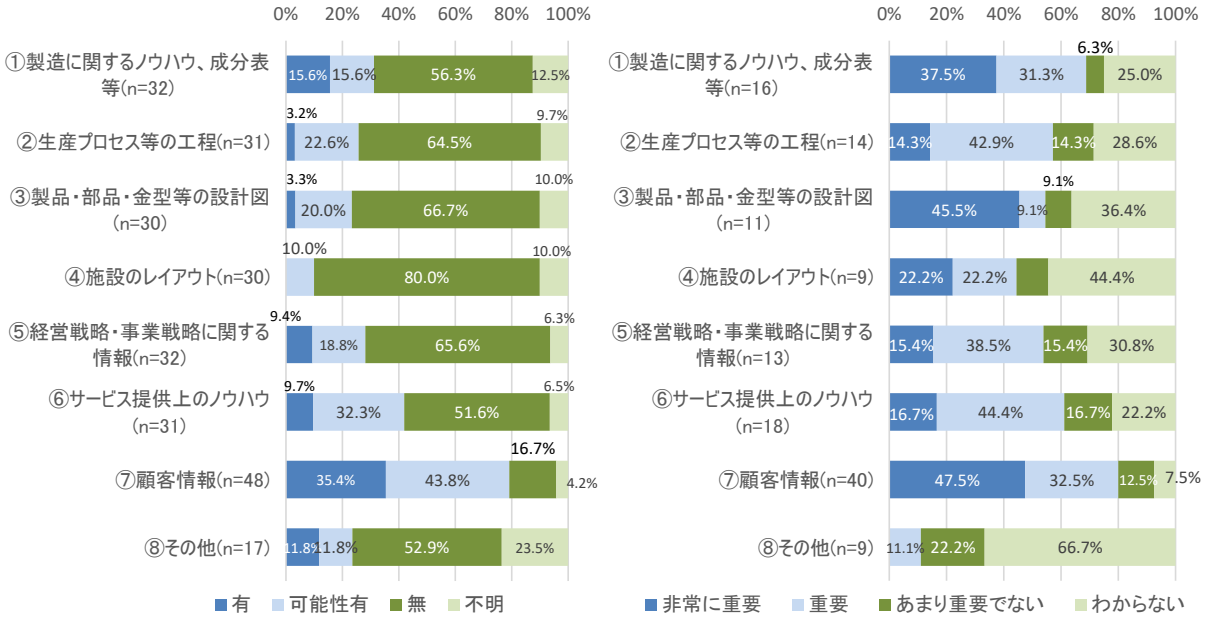

図 2.2-17　左図：営業秘密の内容と漏えい可能性（中小規模企業：2020 年）

右図：漏えいした営業秘密の重要性（中小規模企業：2020 年）

※大規模企業：人数 301 名以上、中小規模企業：人数 300 名以下

(3) 漏えい事例の認識方法

どのようなことから漏えい事例を認識したかについて尋ねた結果を示す。2016 年度調査と本調査とで選択肢の構成を変更していることから、経年比較には注意が必要である。

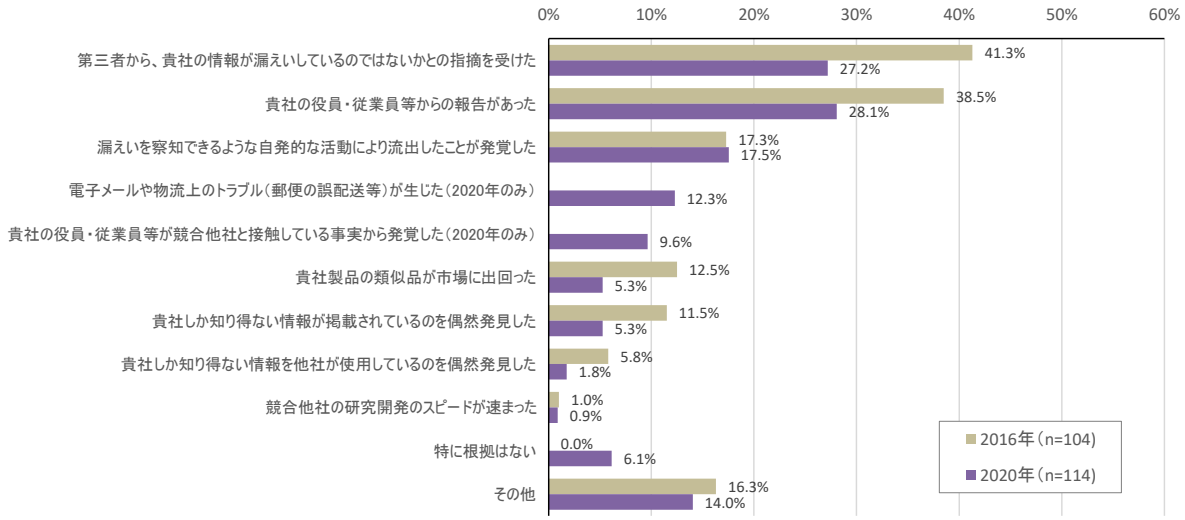

図 2.2-18　漏えい事例の認識方法（経年比較）

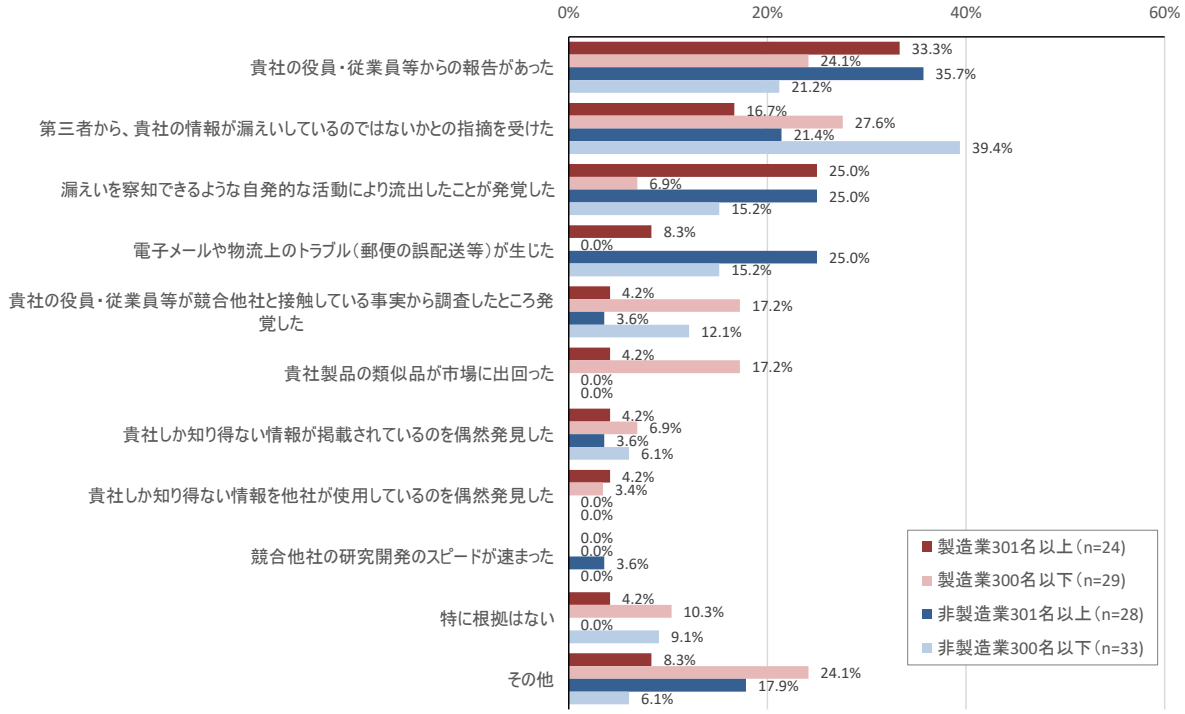

図 2.2-19　漏えい事例の認識方法（業種・規模別４区分によるクロス集計）

(4) 事実確認や証拠収集のために対応した内容

漏えい事例の認識後、事実確認・証拠収集のためにどのような対応をしたかについて尋ねた結果を示す。結果的に何もしなかった場合でも、その理由について尋ねているが、選択肢として設けた３つの理由（実施すべき内容がわからない、余裕がない、費用が確保できない）のいずれに

も該当する企業が複数社存在することがわかる。

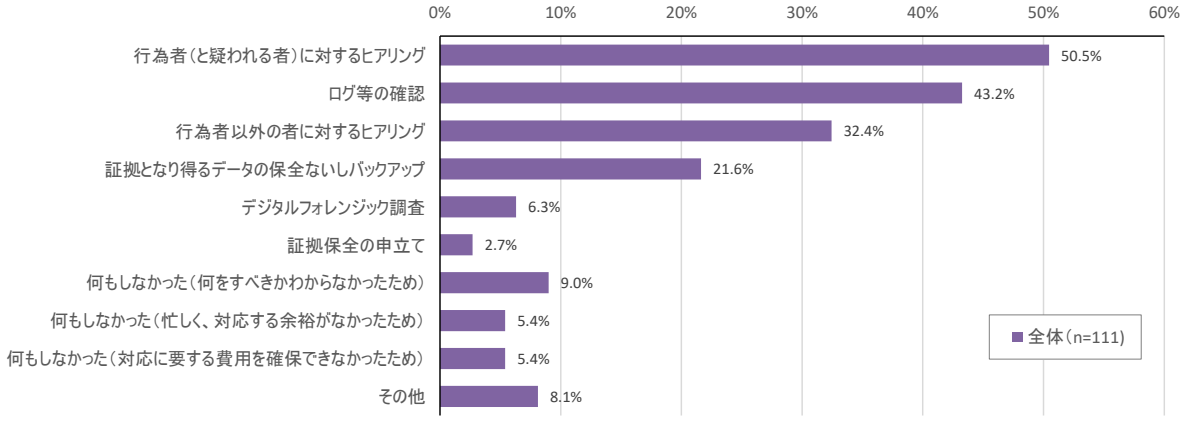

図 2.2-20　事実確認や証拠収集のために対応した内容

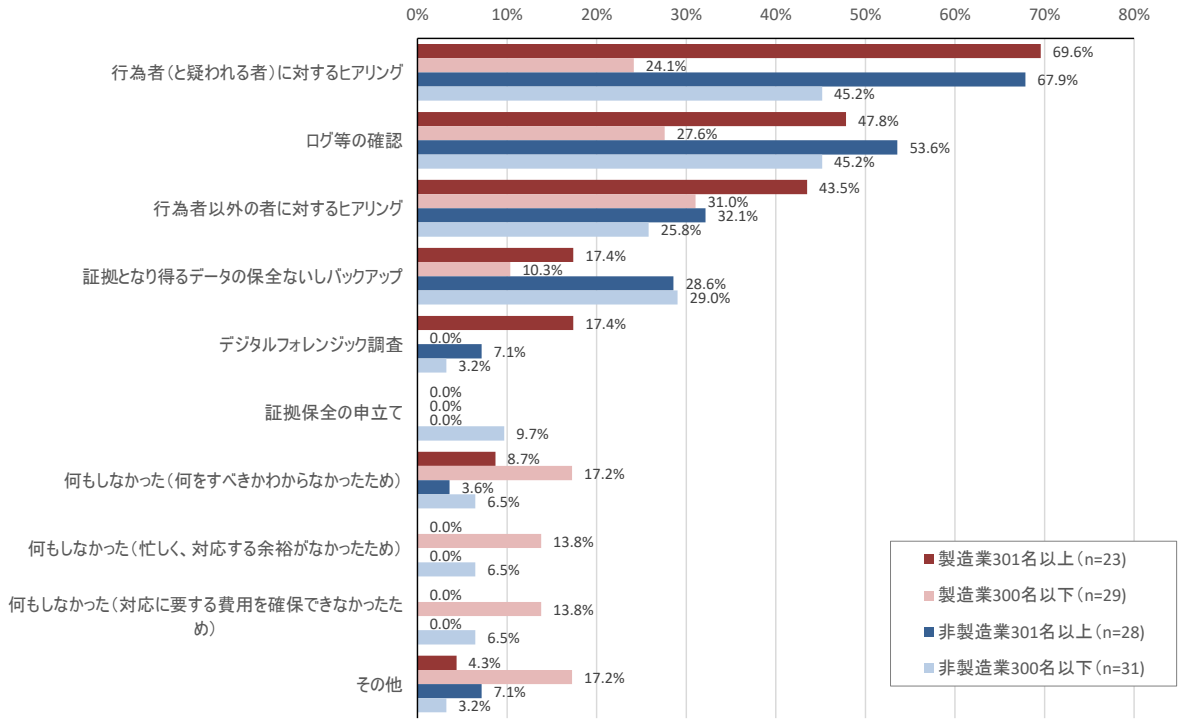

図 2.2-21　事実確認や証拠収集のために対応した内容（業種・規模別4区分によるクロス集計）

(5)　営業秘密の漏えい先

営業秘密がどこに漏えいしたかについて尋ねた結果を示す。外国の競合他社の国名としては「中国」、その他の回答には「取引先」「仕入先」「顧客」「退職者の転職先」「サイバー犯罪組織」等が挙げられている。

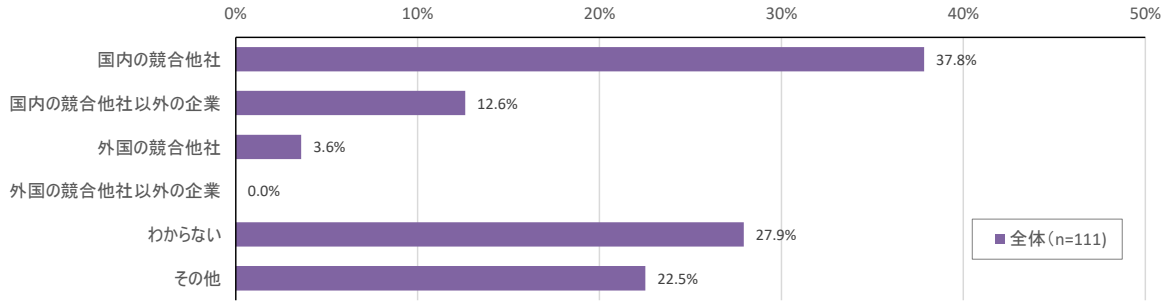

図 2.2-22　営業秘密の漏えい先

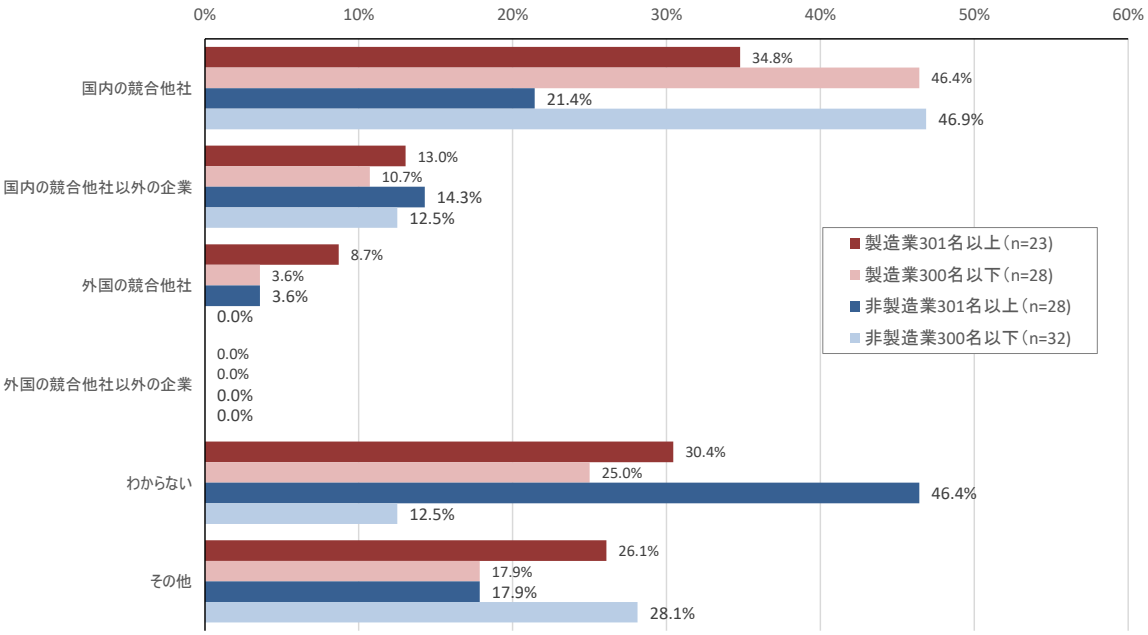

図 2.2-23　営業秘密の漏えい先（業種・規模別４区分によるクロス集計）

(6)　営業秘密漏えいによる推定損害額

営業秘密の漏えいによって、どの程度の損害が生じたかについて尋ねた結果を示す。なお、グラフに示されている通り、「1000 万円以下」が多く、他の区分の選択が少なくなっていることから、将来同様の調査を実施する場合は、「1,000 万円未満」[5]を細分化して尋ねることが考えられる。このとき、さらに新たな選択肢として「実質的な損害無し」を設けることも考えられるが、(4)で分析した事実確認や証拠収集に要した費用も損害に相当するものであり、質問文でその旨を説明すべきであろう。

[5] 現在の調査票において、損害額がちょうど 1,000 万円の場合に２つの選択肢に該当してしまっているため修正することが望ましい。

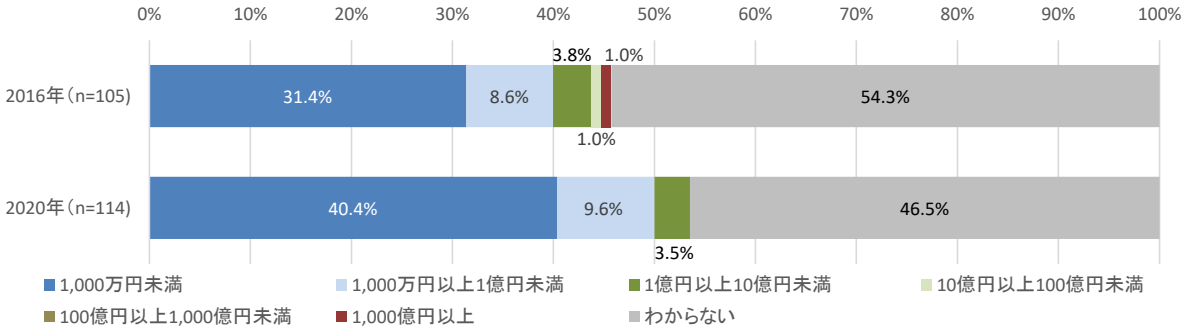

図 2.2-24　営業秘密漏えいによる推定損害額（経年比較）

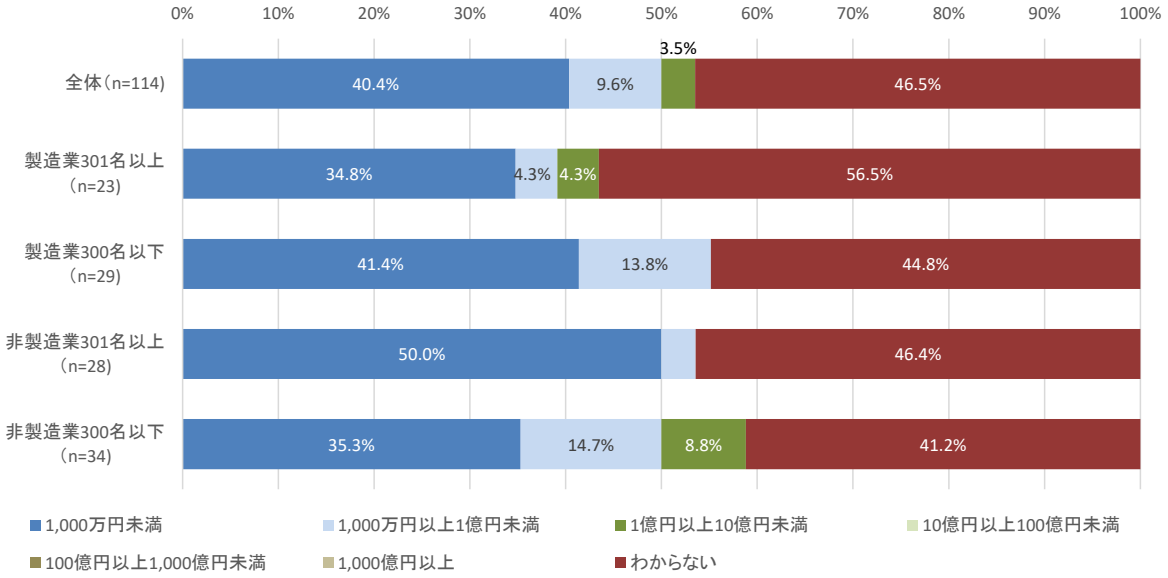

図 2.2-25　営業秘密漏えいによる推定損害額（業種・規模別 4 区分によるクロス集計）

(7)　営業秘密の漏えいルート

どのようなルートで、営業秘密の漏えい事例が発生したかについて尋ねた結果を示す。2016 年度調査と一部選択肢を変更し、従業員の誤操作やルール不徹底に起因するものを識別できるようにしているが、傾向は概ね共通といえる。

中途退職者による漏えいを防ぐ手段としては、アクセスログを取得していることを周知するとともに、漏えい発生後に違反を問うなどの対策が中心となり、技術的に防ぐことが難しいことから、状況の改善が簡単でないことを示している結果と言える。

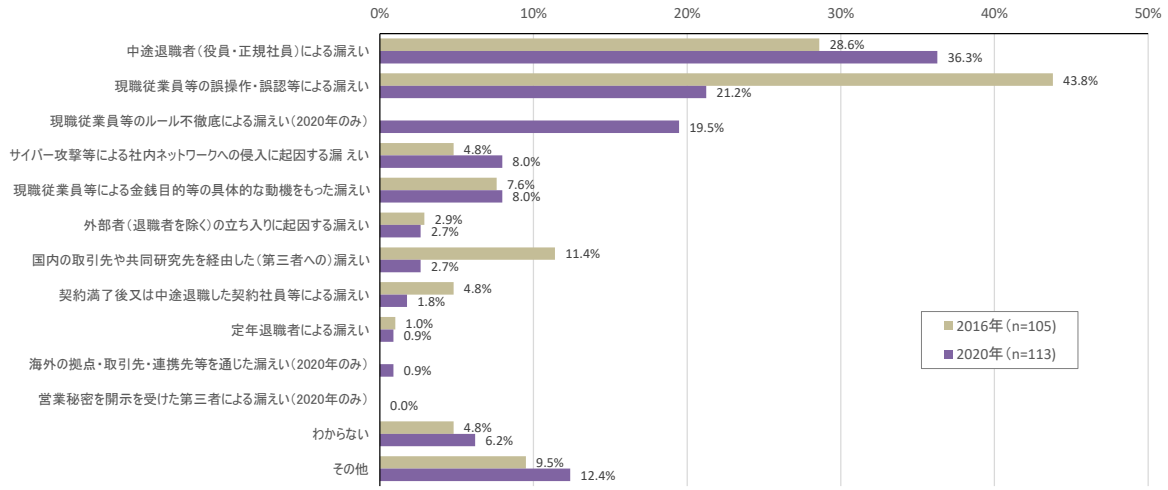

図 2.2-26　営業秘密の漏えいルート（経年比較）

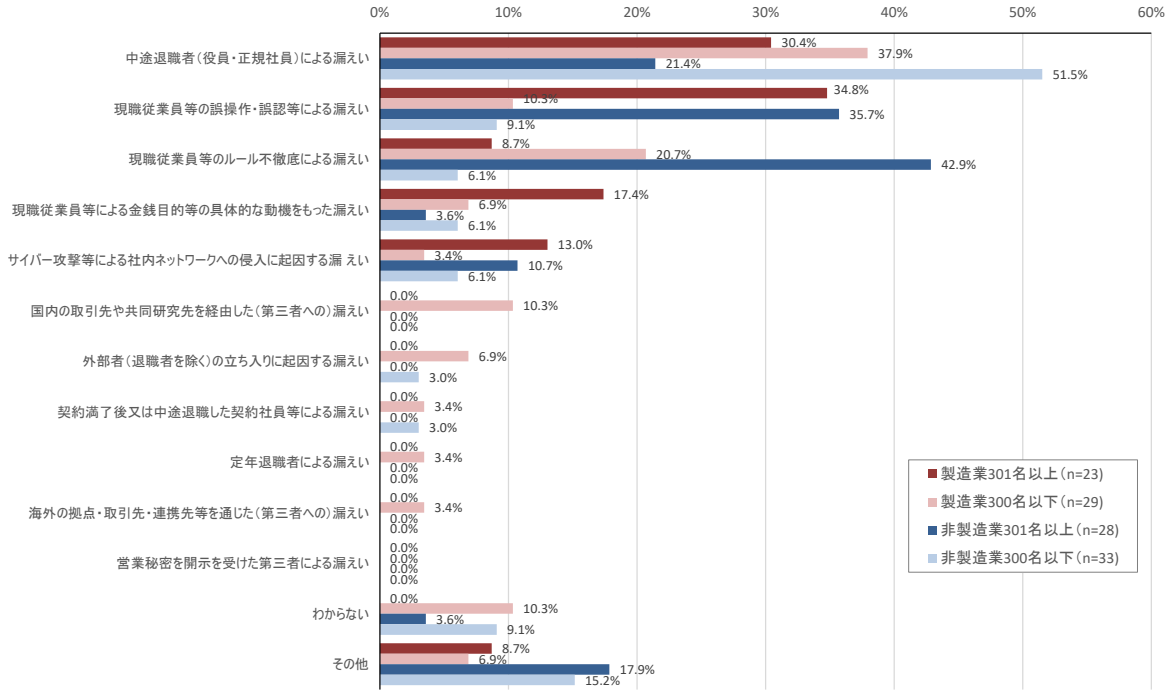

図 2.2-27　営業秘密の漏えいルート（業種・規模別４区分によるクロス集計）

(8)　営業秘密の侵害行為を行った行為者・企業への対応

営業秘密の侵害行為を行った行為者・企業に対してどのような対応をとったかについて尋ねた結果を示す。

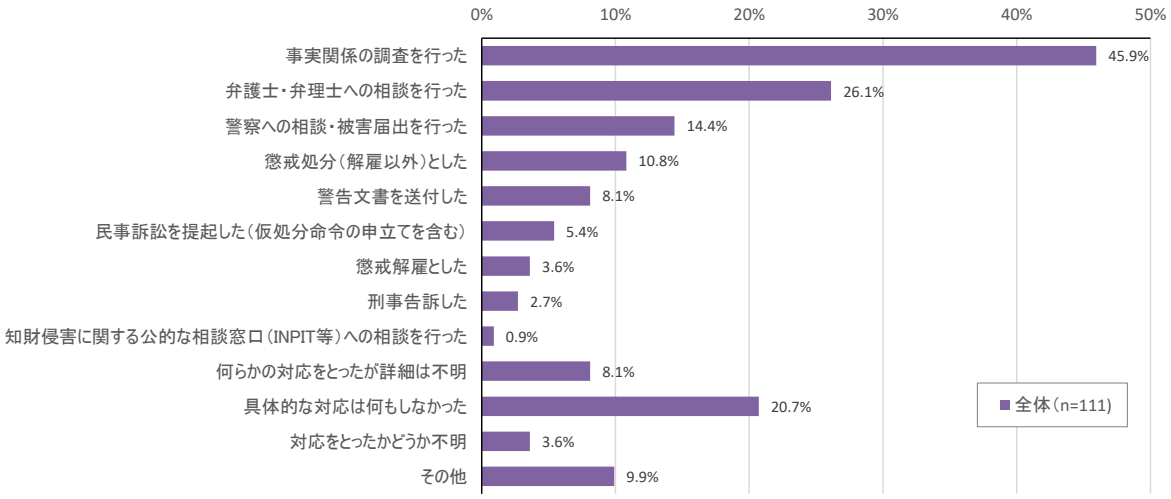

図 2.2-28　営業秘密の侵害行為を行った行為者・企業への対応

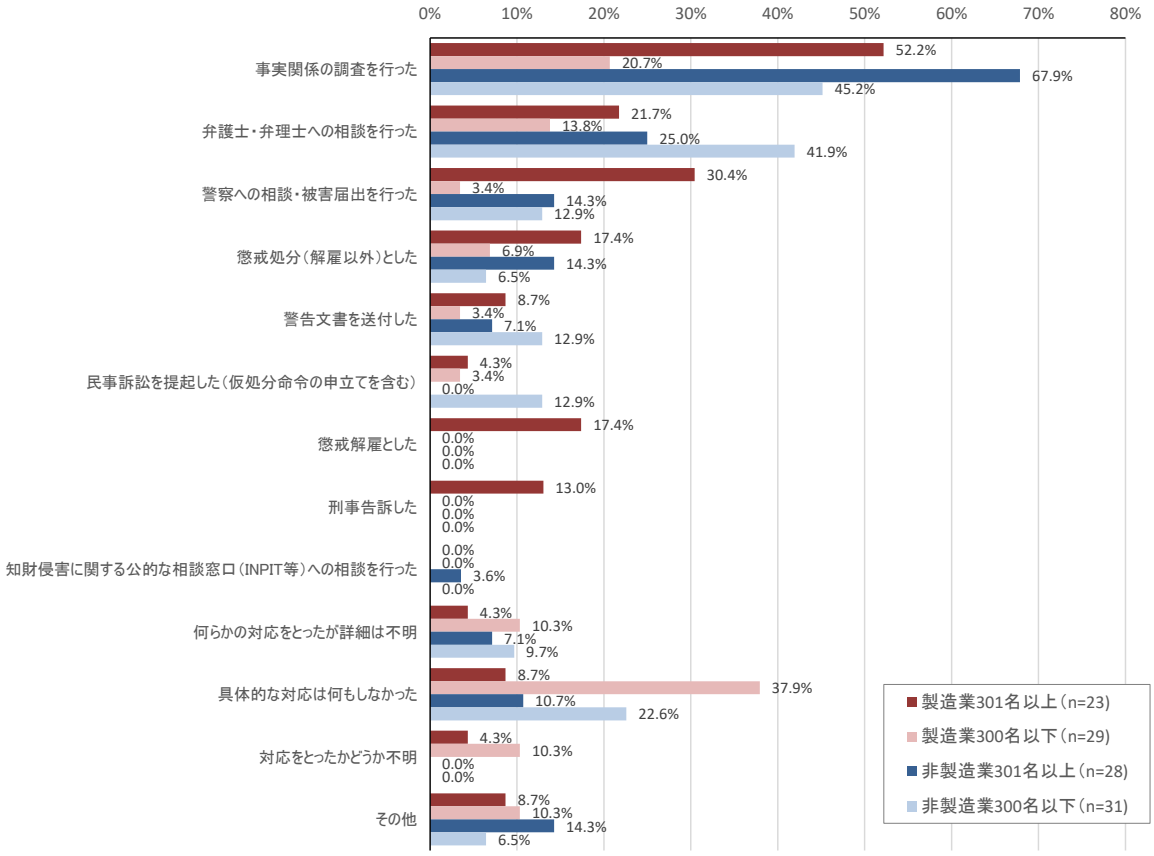

図 2.2-29　営業秘密の侵害行為を行った行為者・企業への対応（業種・規模別4区分によるクロス集計）

(9)　営業秘密の漏えいが起こっていない要因

本項目は(8)までとは逆に、(1)において「情報漏えいの事例はない」と回答している企業のみを対象に、営業秘密情報の漏えいが起こっていない要因について尋ねたものである。複数の要因が作用していることが見込まれ、複数選択形式で尋ねることで影響の大きな要因が見いだされにく

くなることへの懸念から、最大３項目までの選択とした。

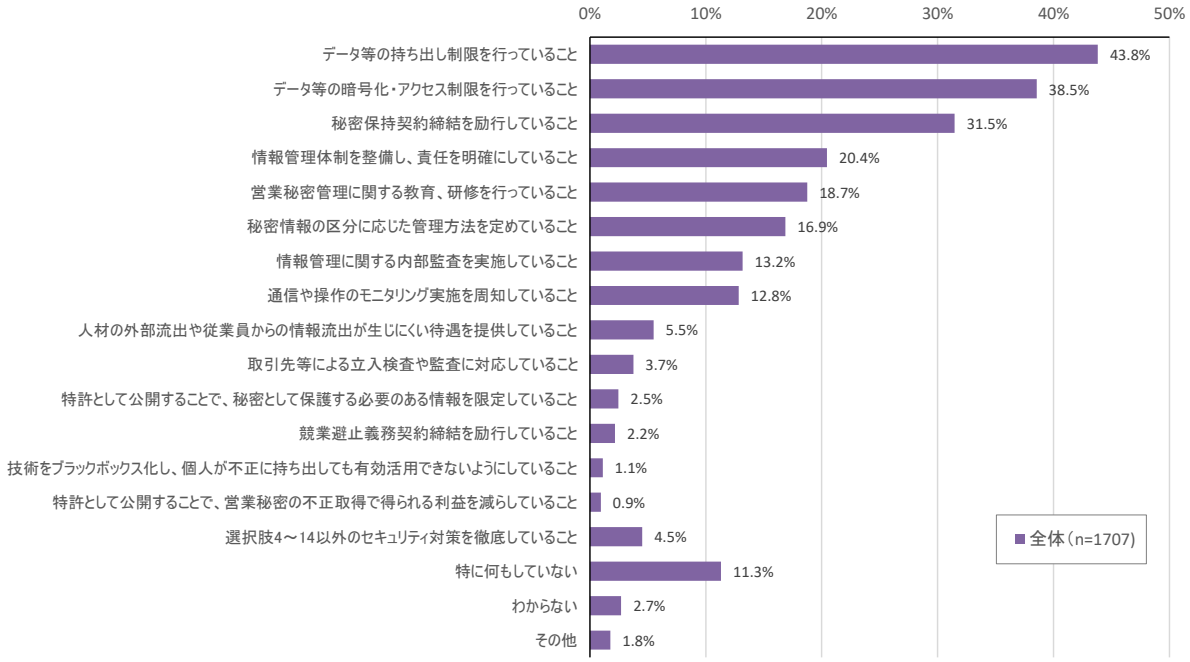

図 2.2-30　営業秘密の漏えいが起こっていない要因

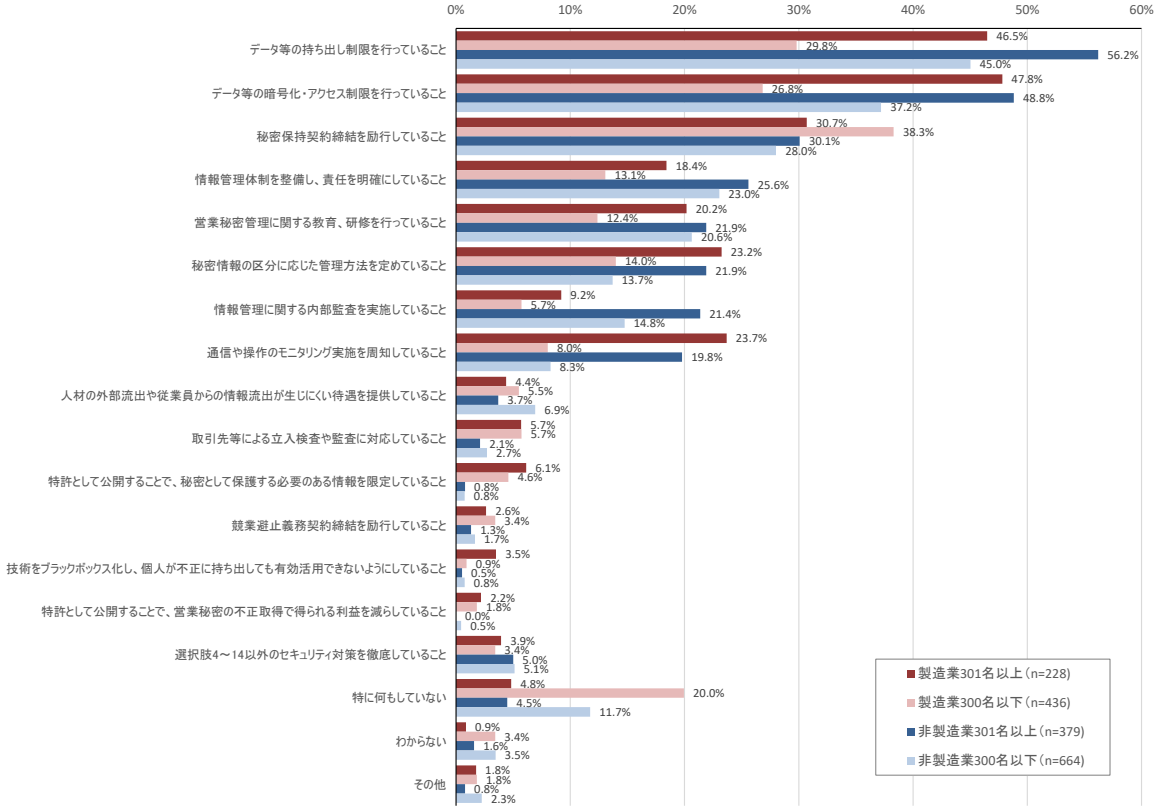

図 2.2-31　営業秘密の漏えいが起こっていない要因（業種・規模別４区分によるクロス集計）

(10) 営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているもの

本項目はすべての企業に尋ねている。(9)と同様、多くの脅威が該当する場合が多いと見込まれ、複数選択形式で尋ねることで影響の大きな脅威が見いだされにくくなることへの懸念から、最大３項目までの選択とした。

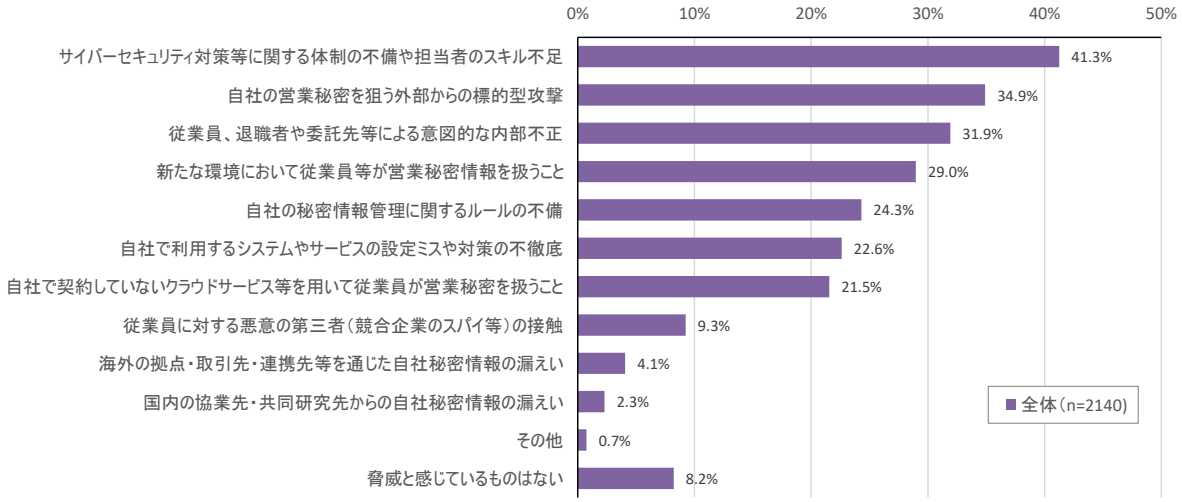

図 2.2-32　営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているもの

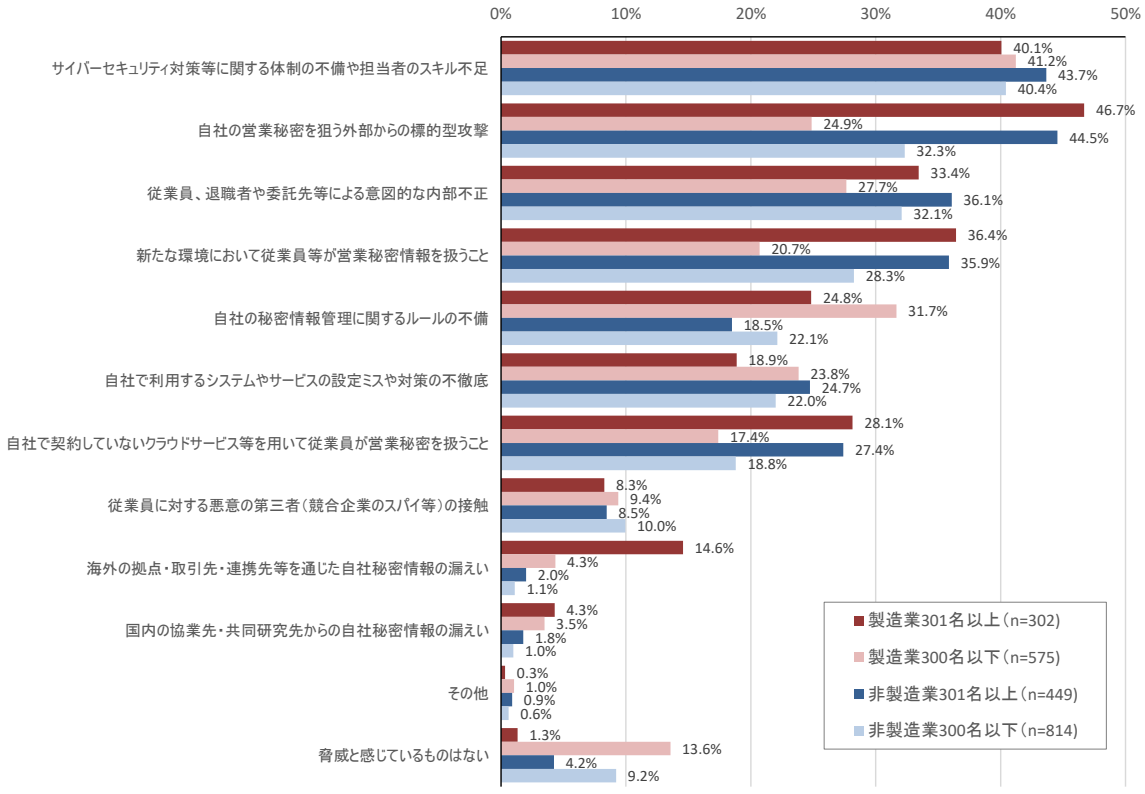

図 2.2-33　営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているもの
（業種・規模別４区分によるクロス集計）

2.2.4.3　営業秘密として扱う情報の考え方

(1)　営業秘密の区分管理状況

自社で保有する情報について、営業秘密とそれ以外の情報とを区分しているか、及び営業秘密

をその秘密性のレベルに応じて格付けしているかについて尋ねた結果を示す。

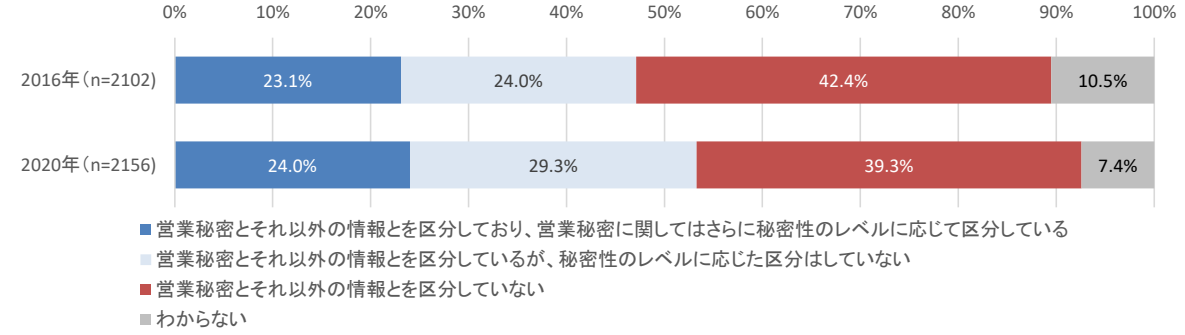

図 2.2-34　営業秘密の区分管理状況（経年比較）

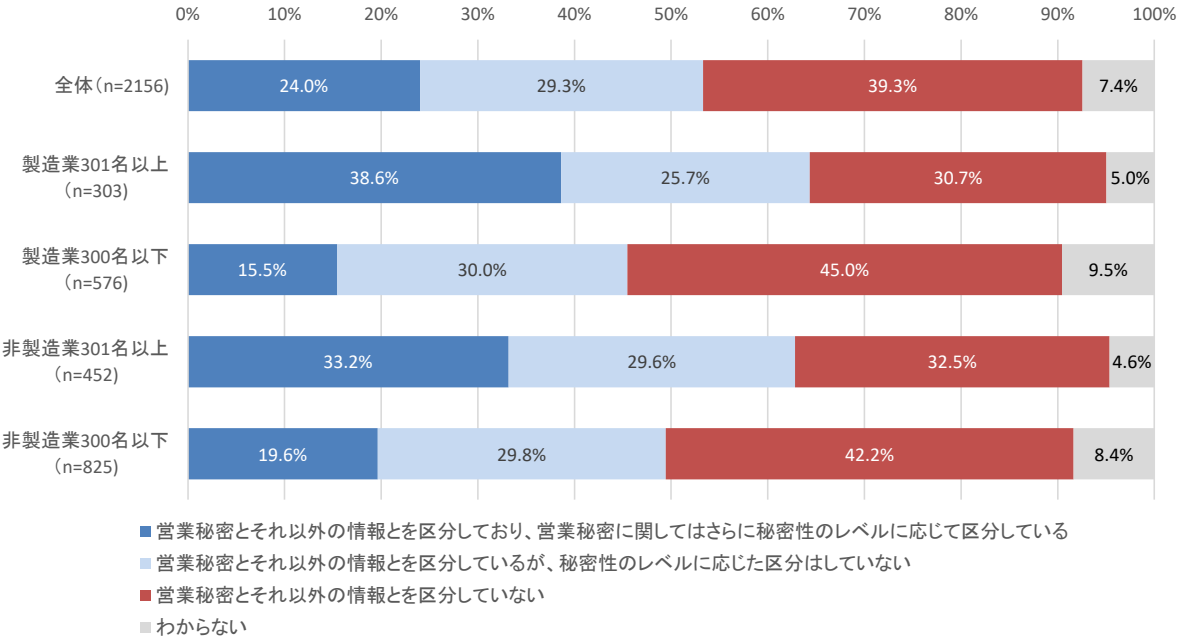

図 2.2-35　営業秘密の区分管理状況（業種・規模別４区分によるクロス集計）

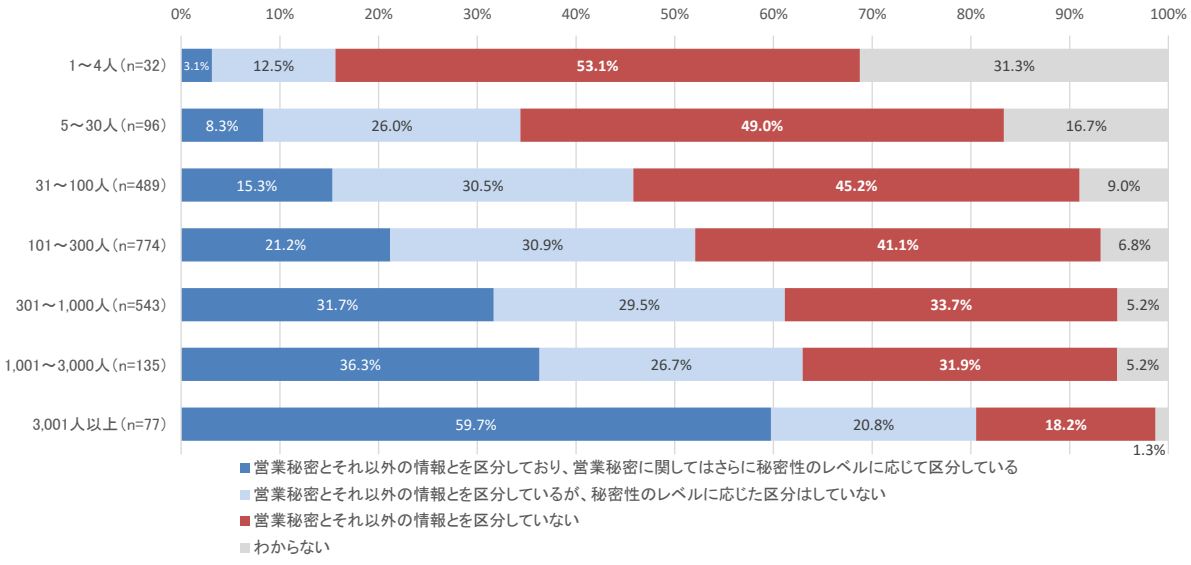

図 2.2-36　営業秘密の区分管理状況（規模別クロス集計）

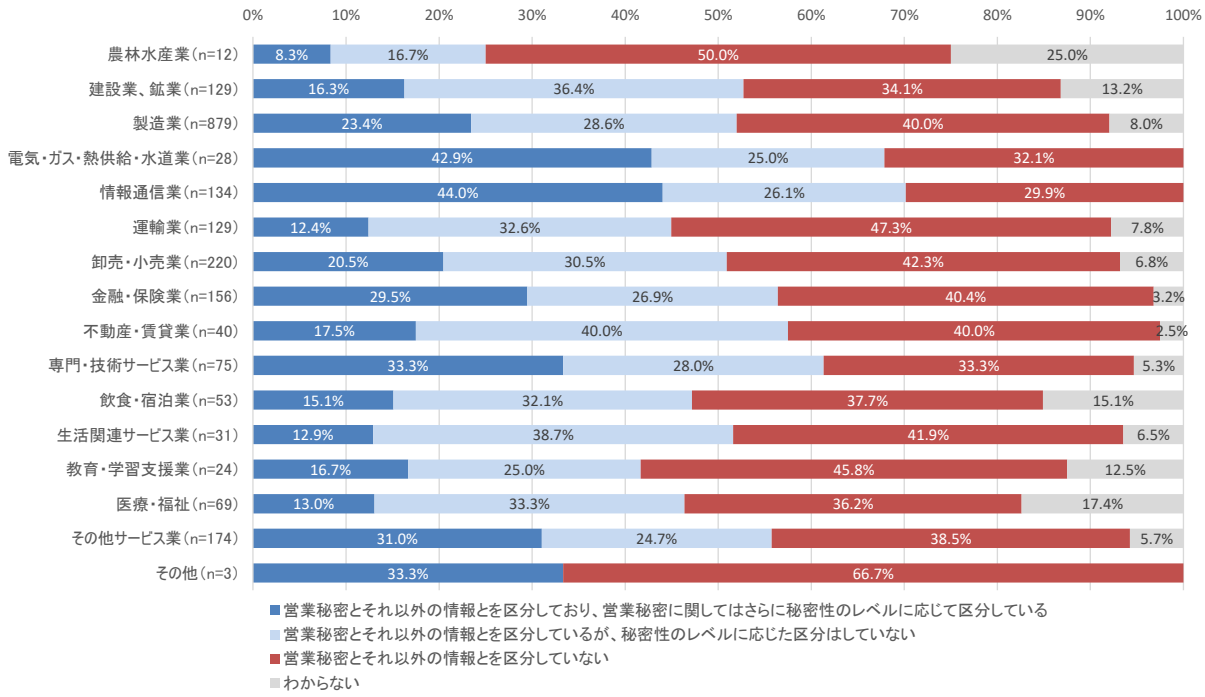

図 2.2-37　営業秘密の区分管理状況（業種別クロス集計）

(2)　営業秘密管理の運用実態

自社で保有する営業秘密について、社内規程として定められた管理ルールがどの程度厳密に運用されているかについて尋ねた結果を示す。2016 年度調査とは選択肢を変更しており、回答はそれに基づき詳細になされていることから、単純な比較が難しいことに注意が必要である。

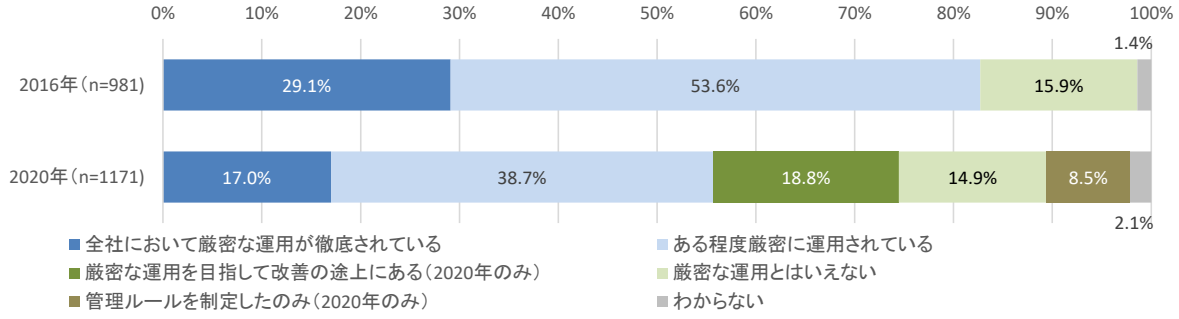

図 2.2-38　営業秘密管理の運用実態（経年比較）

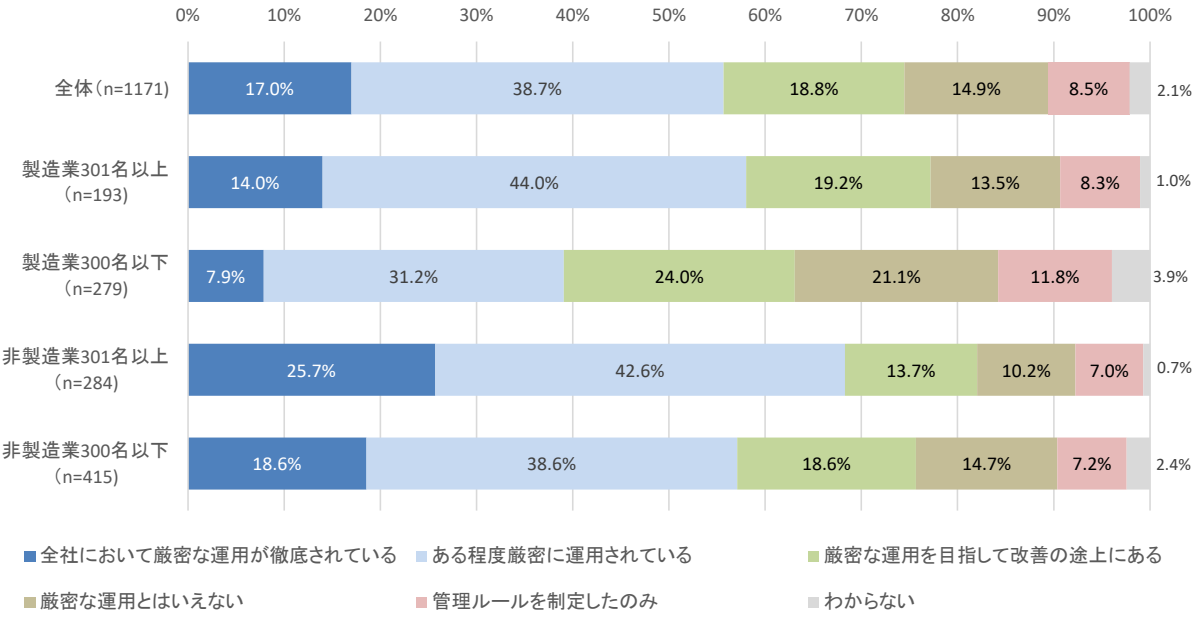

図 2.2-39　営業秘密管理の運用実態（業種・規模別４区分によるクロス集計）

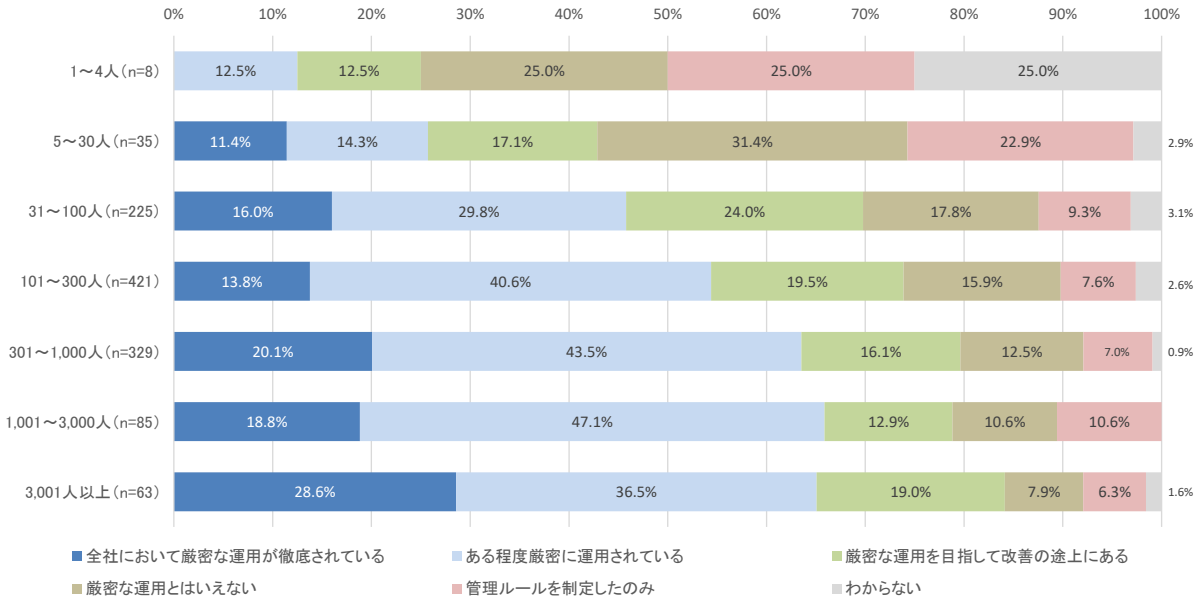

図 2.2-40　営業秘密管理の運用実態（規模別クロス集計）

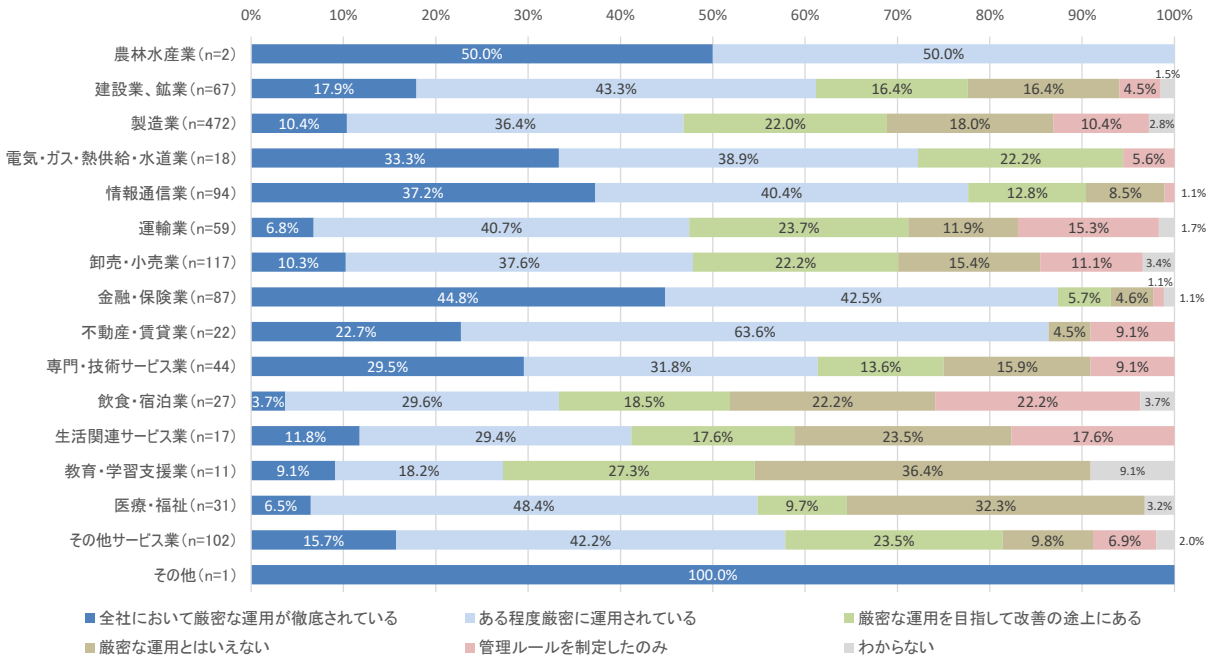

図 2.2-41　営業秘密管理の運用実態（業種別クロス集計）

(3) 実態営業秘密の保護対策実践上の課題

営業秘密情報の保護対策を実践する上で課題と感じる事項について尋ねた結果を示す。

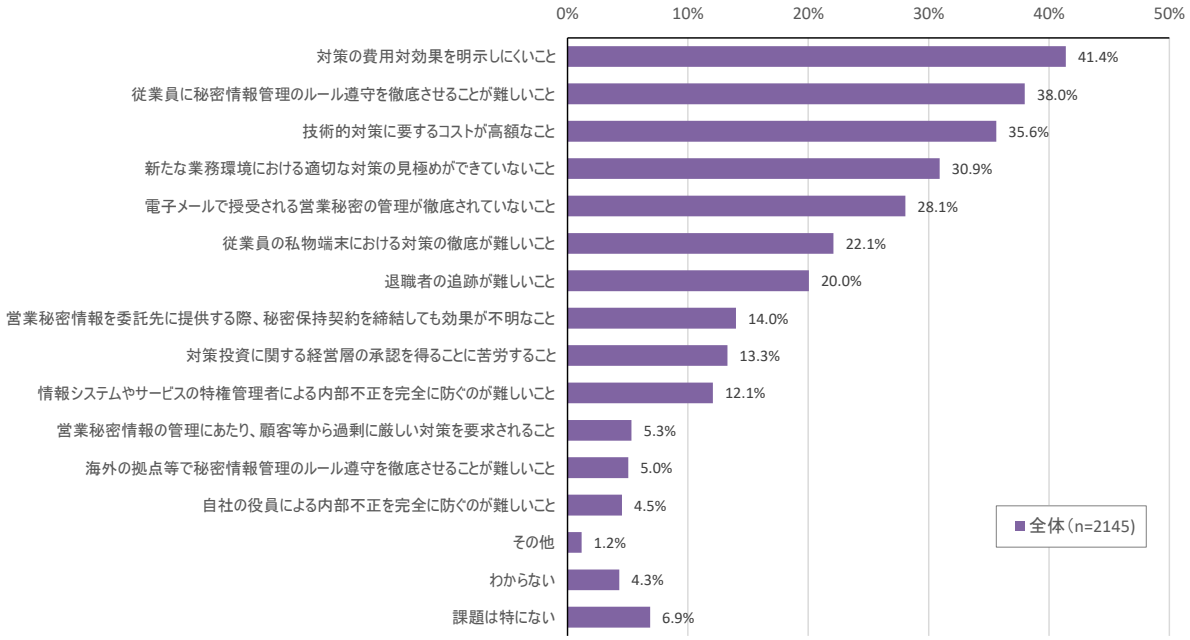

図 2.2-42　営業秘密の保護対策実践上の課題

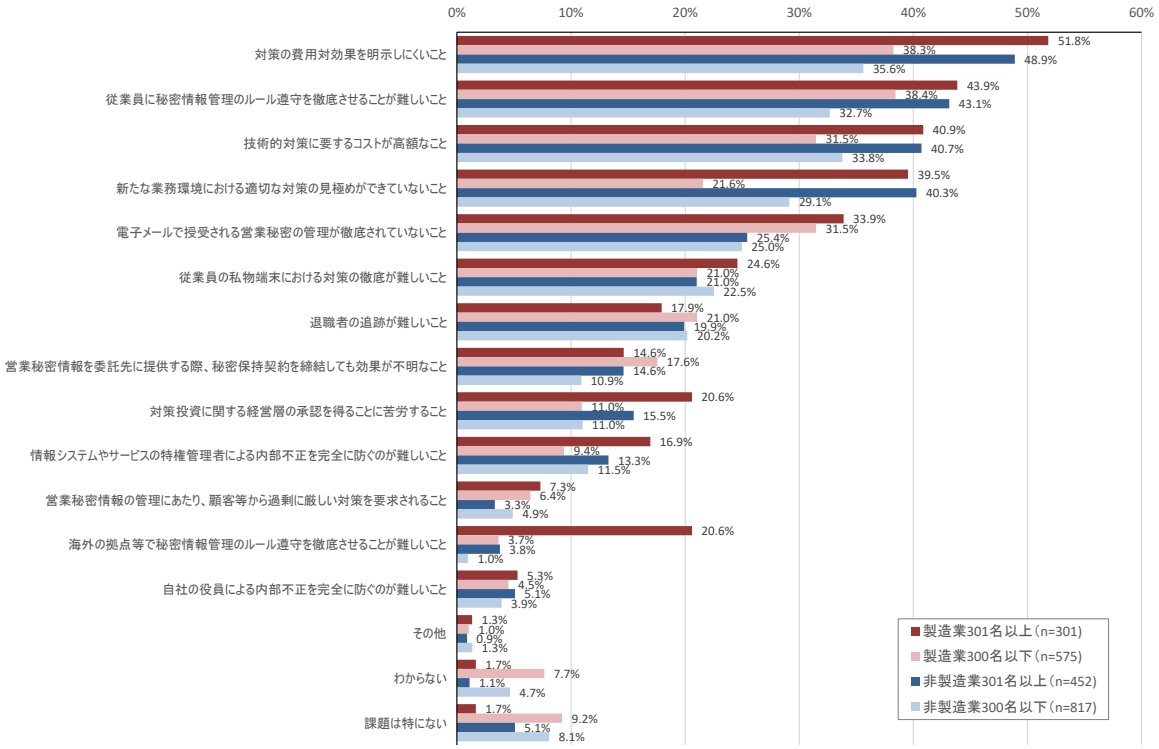

図 2.2-43　営業秘密の保護対策実践上の課題（業種・規模別４区分によるクロス集計）

(4) 限定提供データに相当する情報の保有状況

調査仮説を踏まえ、営業秘密及び限定提供データの保有状況について尋ねた結果を示す。このとき、「両方とも保有していない」企業が多いのは、「営業秘密」を不正競争防止法の用語ととらえず、「営業活動のための情報」と解釈した企業が多いためであり、「両方を保有」の比率以外の活用には慎重を要するものと考えられる。

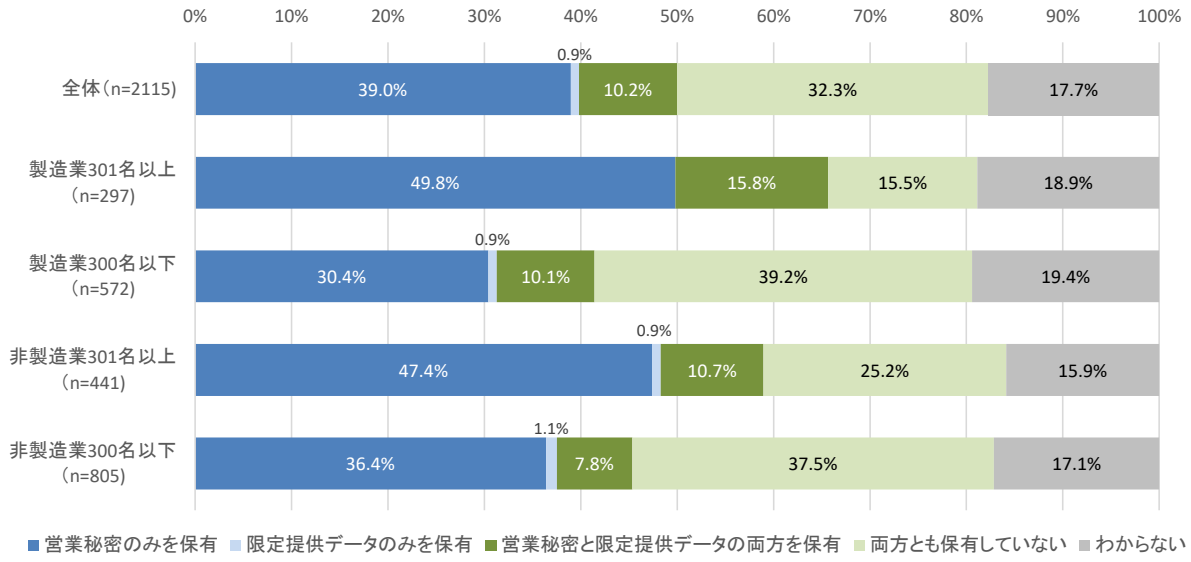

図 2.2-44　限定提供データに相当する情報の保有状況（業種・規模別4区分によるクロス集計）

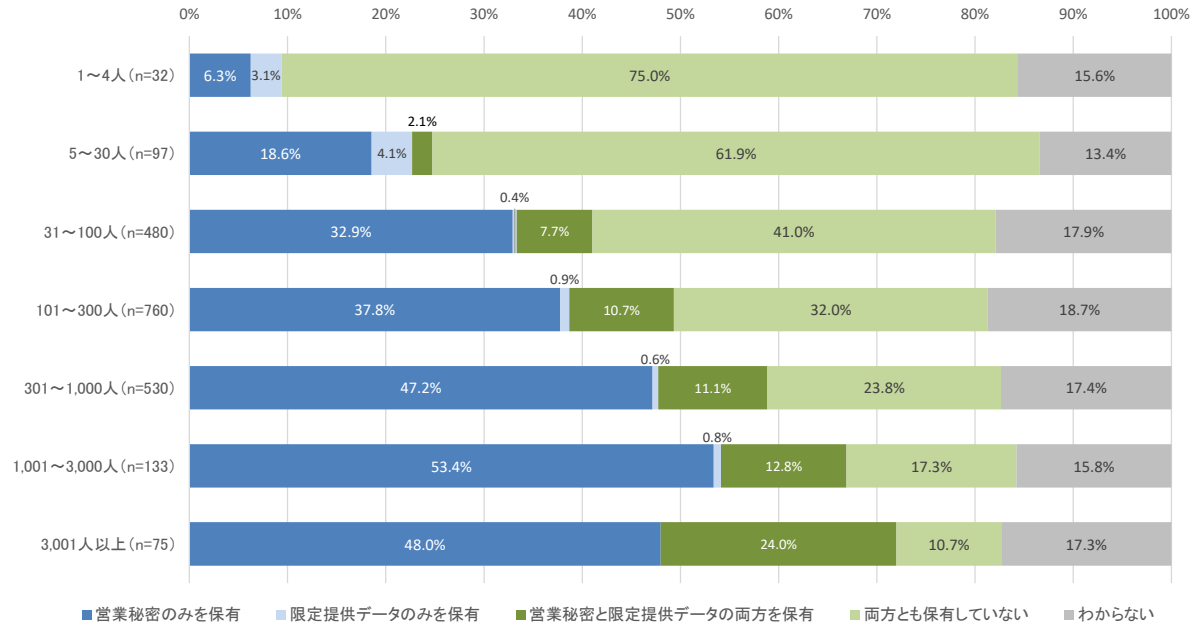

図 2.2-45　限定提供データに相当する情報の保有状況（規模別クロス集計）

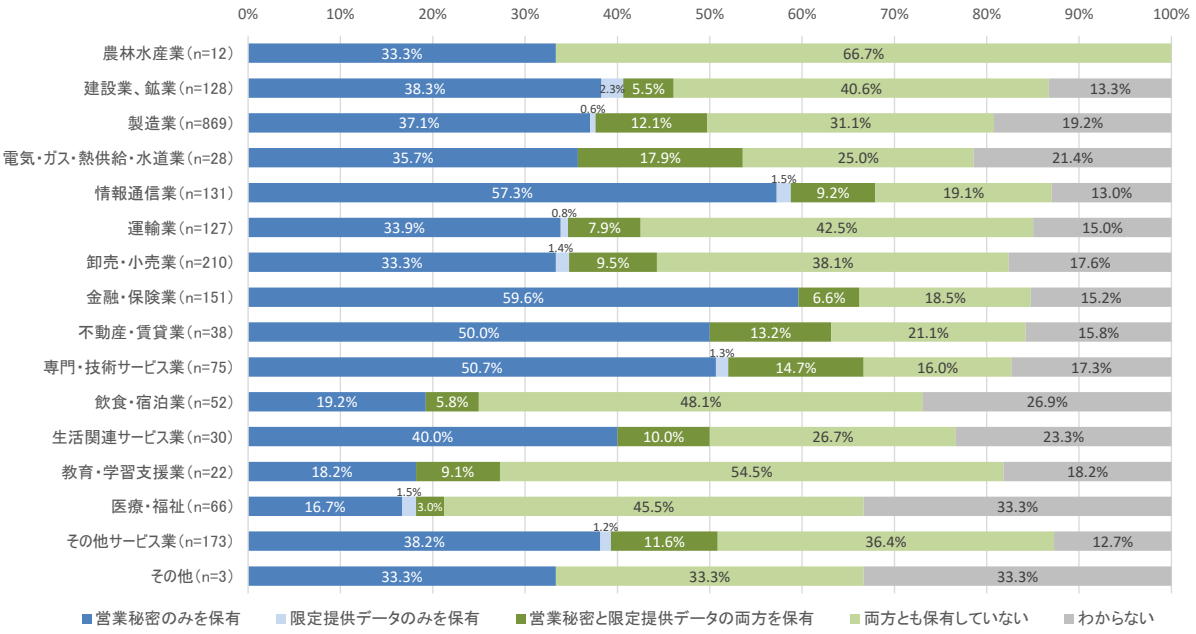

図 2.2-46　限定提供データに相当する情報の保有状況（業種別クロス集計）

(5)　限定提供データを考慮した管理の実施状況

前問で限定提供データを保有していると回答した企業に対し、限定提供データに相当するデータについて、不正競争防止法が定める限定提供データの要件を意識した管理を行っているかについて尋ねた結果を示す。

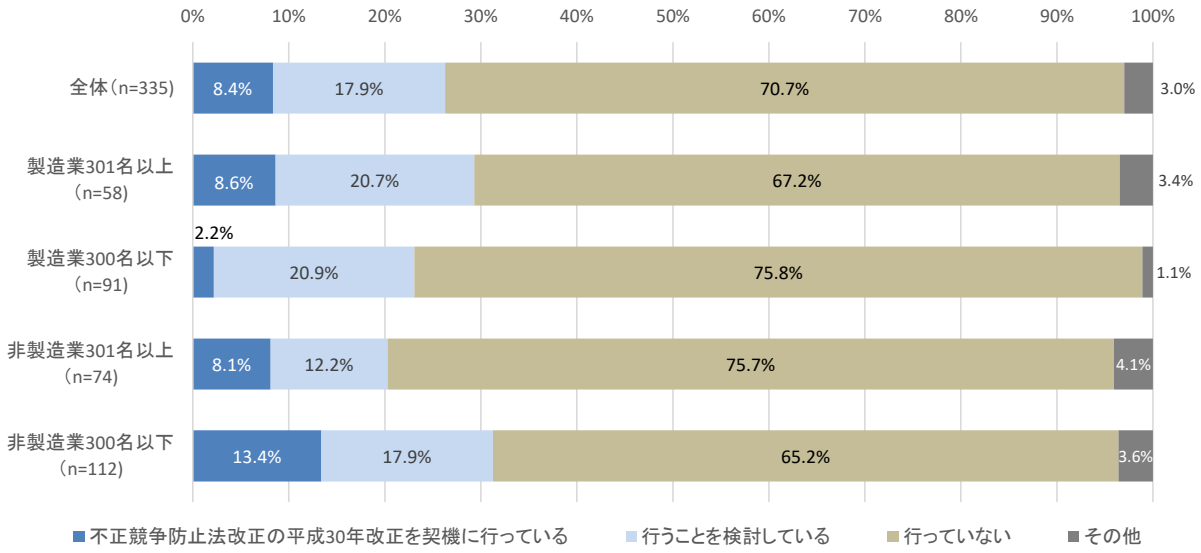

図 2.2-47　限定提供データを考慮した管理の実施状況（業種・規模別4区分によるクロス集計）

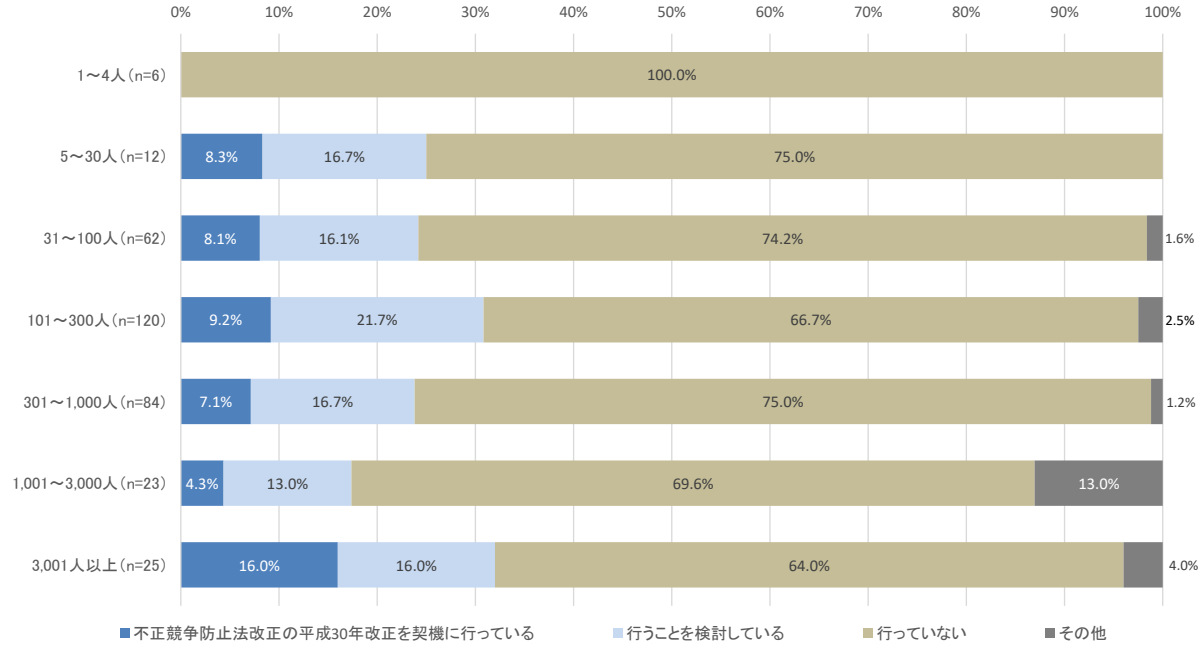

図 2.2-48　限定提供データを考慮した管理の実施状況（規模別クロス集計）

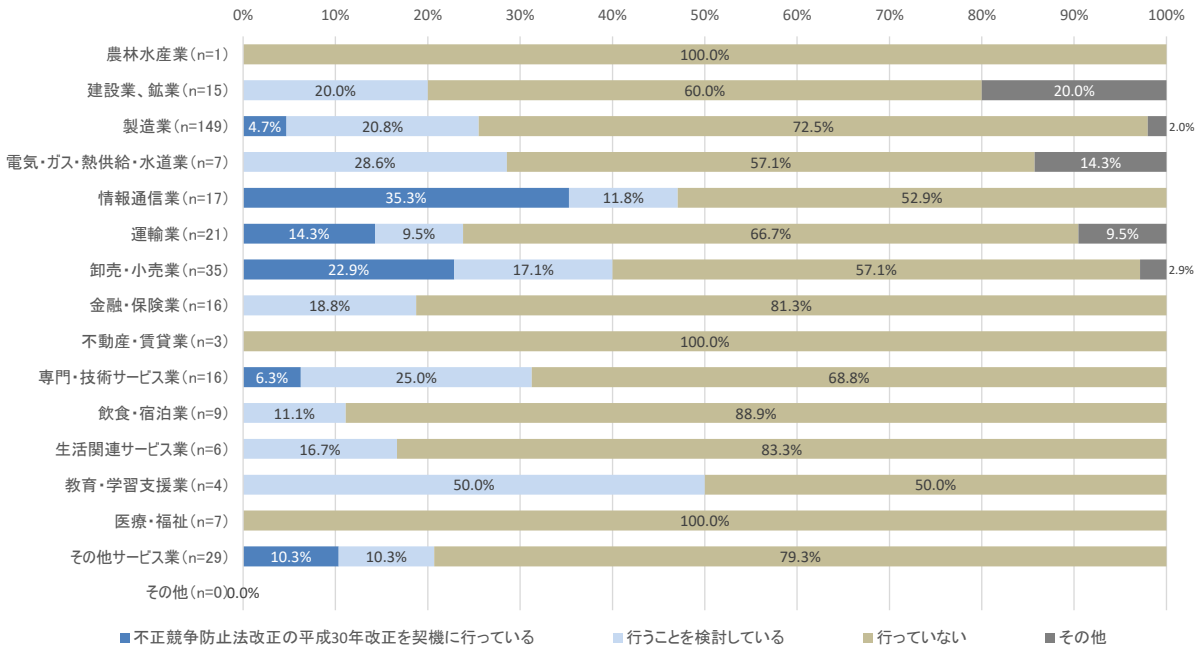

図 2.2-49　限定提供データを考慮した管理の実施状況（業種別クロス集計）

(6) 限定提供データの管理を目的として実施している対策

前問で「不正競争防止法の平成 30 年改正を契機に行っている」と回答した企業に対し、実施している対策について尋ねた結果を示す。さらに、本項目にて「限定提供データを対象とする規定等を整備」及び「限定提供データの扱いに関する契約ひな型を策定」と回答した企業に対し、策定した規程や契約ひな形の具体的内容について尋ねたところ、直接的に関わる回答は少なかったものの、「抵触しそうな画像の例を作成して営業時の判断を容易にする」等の回答が得られた。

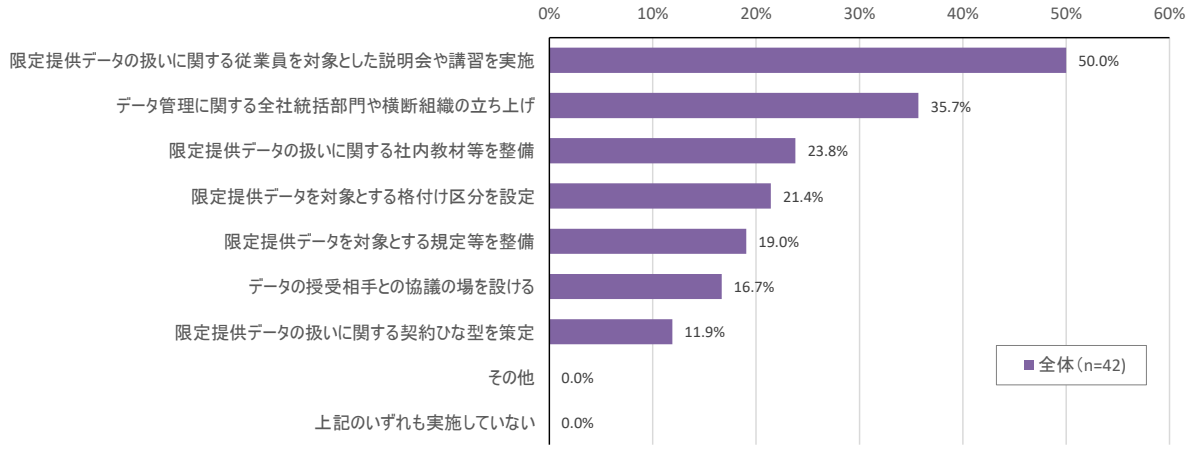

図 2.2-50　限定提供データの管理を目的として実施している対策

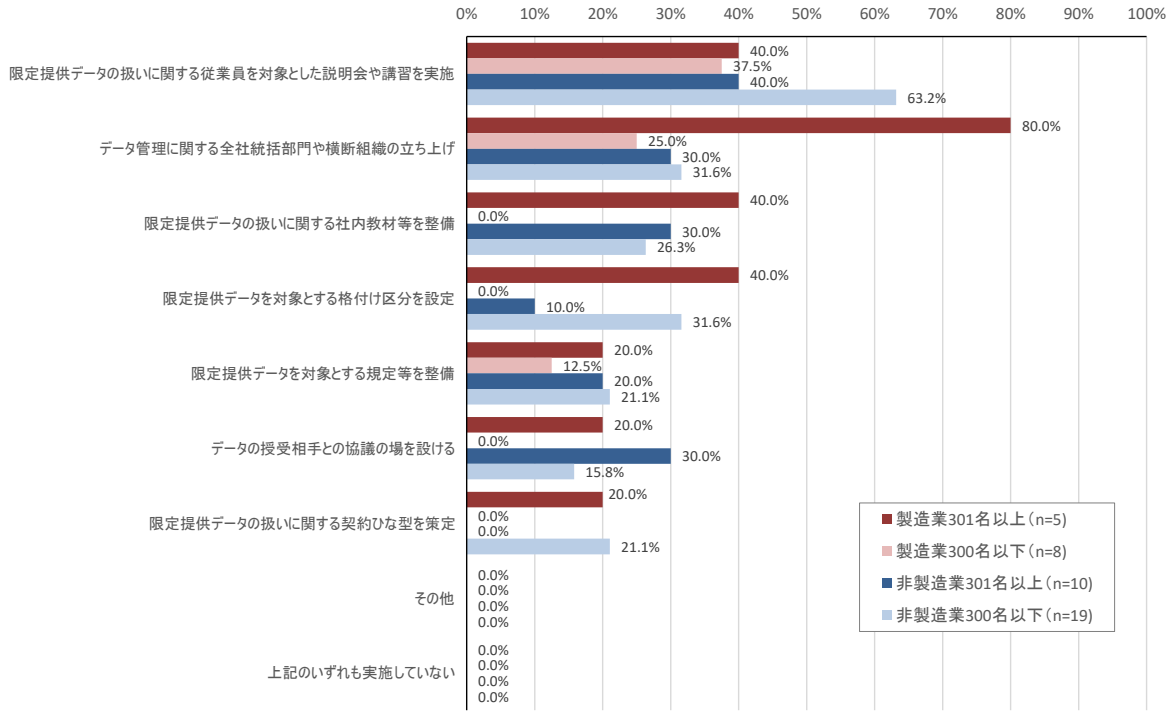

図 2.2-51　限定提供データの管理を目的として実施している対策（業種・規模別4区分によるクロス集計）

2.2.4.4　営業秘密の漏えい対策の状況

(1)　営業秘密の漏えいに気付くことができるような対策の実施状況

サーバーのアクセスログ確認やメールのモニタリング等、営業秘密の漏えいに気付くことができるような対策が実施されているかどうかについて尋ねた結果を示す。2016 年度調査と比較して、対策の実施率そのものは 50.2%から 57.8%に増加する一方で、従業員への周知を行っている比率が低下しているが、この理由として企業における IT 機器の利用において一般にセキュリティ対策としてモニタリングが行われることがコンセンサスとして受け入れられていると考えて、積極的に周知を行わない企業が増えたことが考えられる。

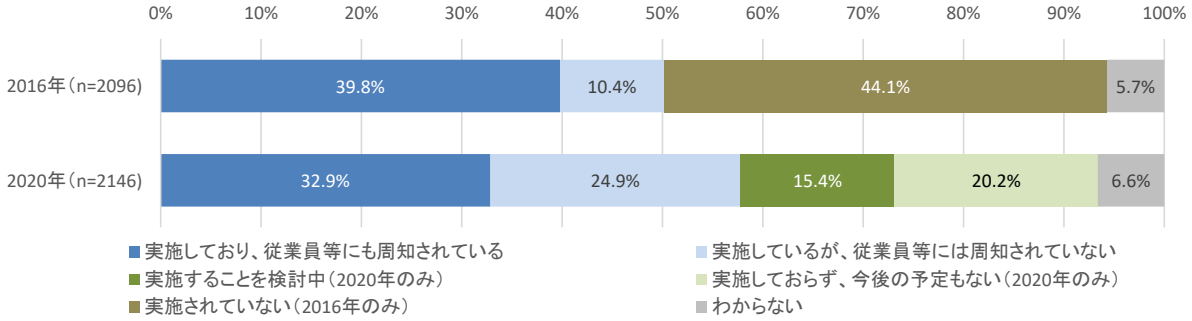

図 2.2-52　営業秘密の漏えいに気付くことができるような対策の実施状況（経年比較）

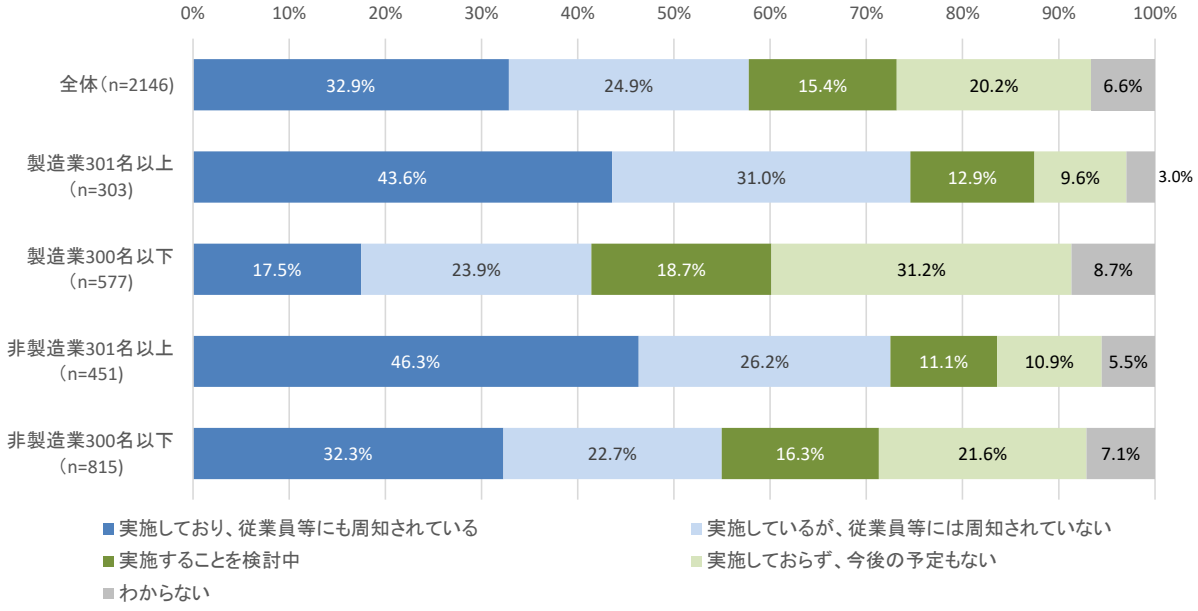

図 2.2-53　営業秘密の漏えいに気付くことができるような対策の実施状況
（業種・規模別４区分によるクロス集計）

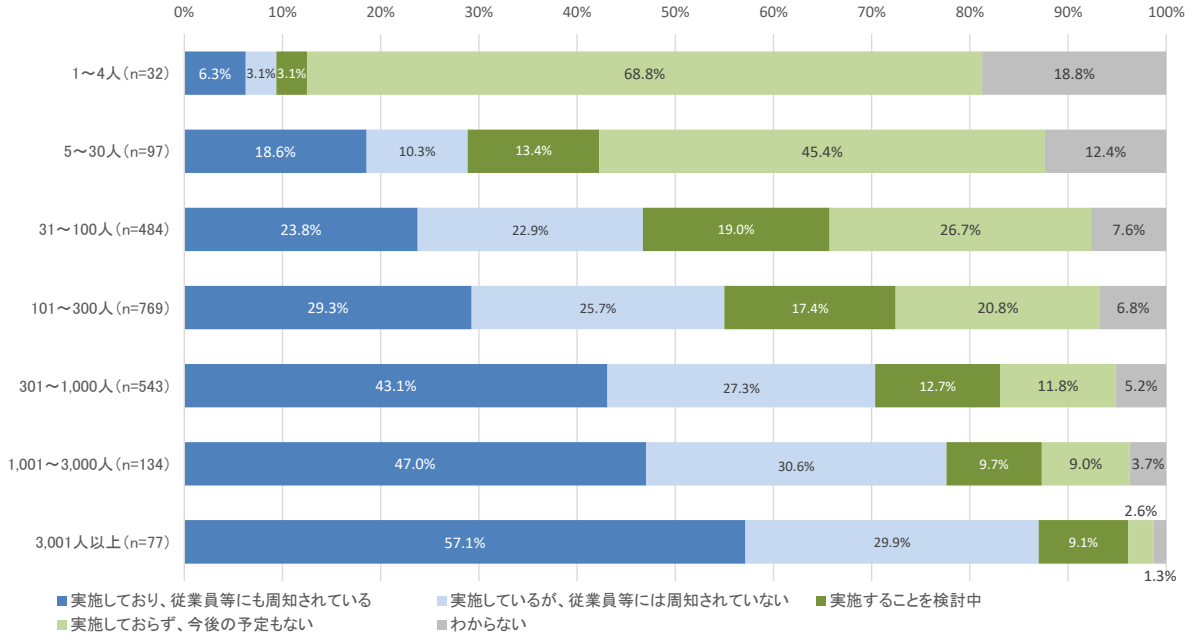

図 2.2-54　営業秘密の漏えいに気付くことができるような対策の実施状況（規模別クロス集計）

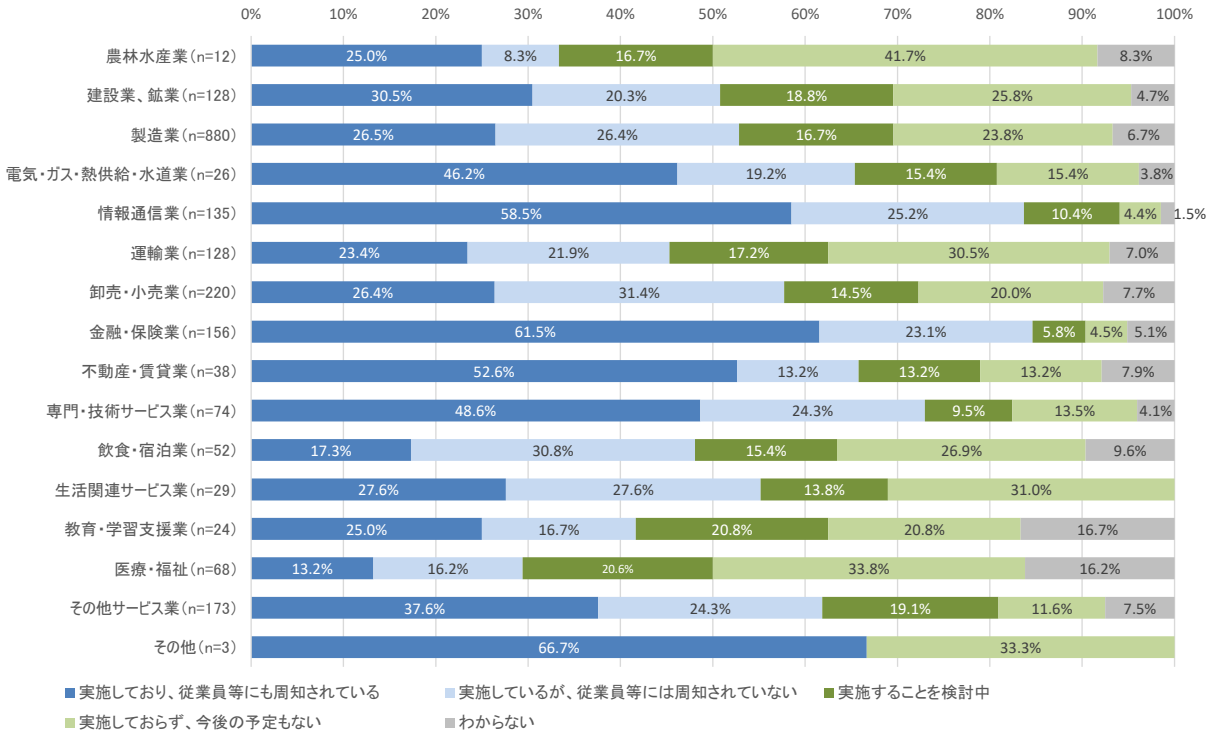

図 2.2-55　営業秘密の漏えいに気付くことができるような対策の実施状況（業種別クロス集計）

(2) 営業秘密情報への不正なアクセスを防ぐための対策の実施状況

営業秘密情報（紙と電子媒体の両方）への不正なアクセスを防ぐための対策として、実施しているものについて尋ねた結果を示す。なお、本調査ではさらに選択した対策のうち、最も有効と考えるものについて、単一選択式で回答を求めており、その結果も併せて示している（後述の(3)(4)も同様）。アンチウイルスソフト導入やファイアウォール等の導入などの基礎的な対策は伸びが見られる一方、「電子ファイルへのパスワード設定」が 2016 年度と比較して比率が低下しているのは、より高度なアクセス制限方式に移行している可能性、「分離して保管」「入室制限」等については第４章で論じるようにテレワーク等では機能しないことを意識して回答している可能性がそれぞれ想定される。

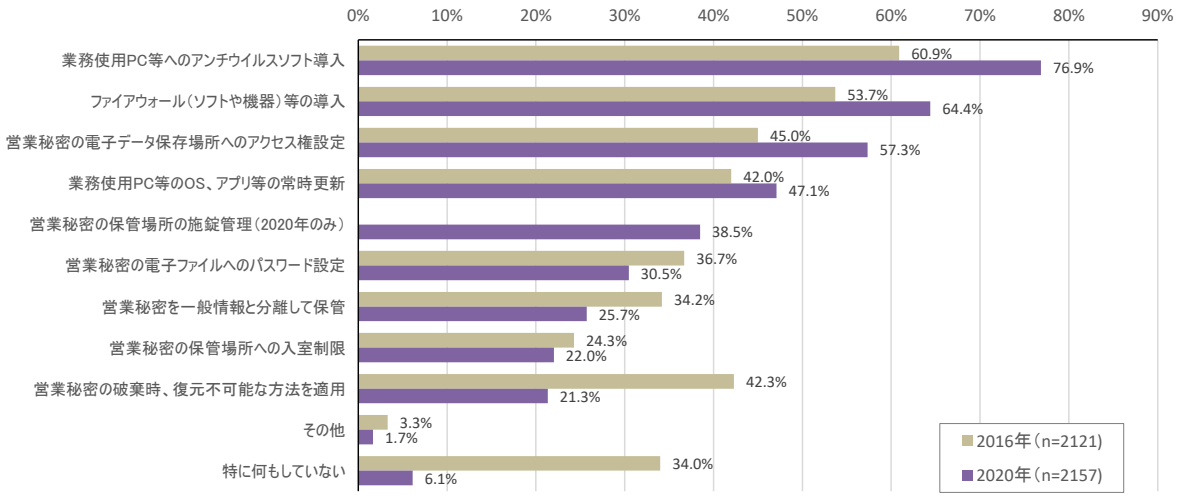

図 2.2-56　営業秘密情報への不正なアクセスを防ぐための対策の実施状況（経年比較）

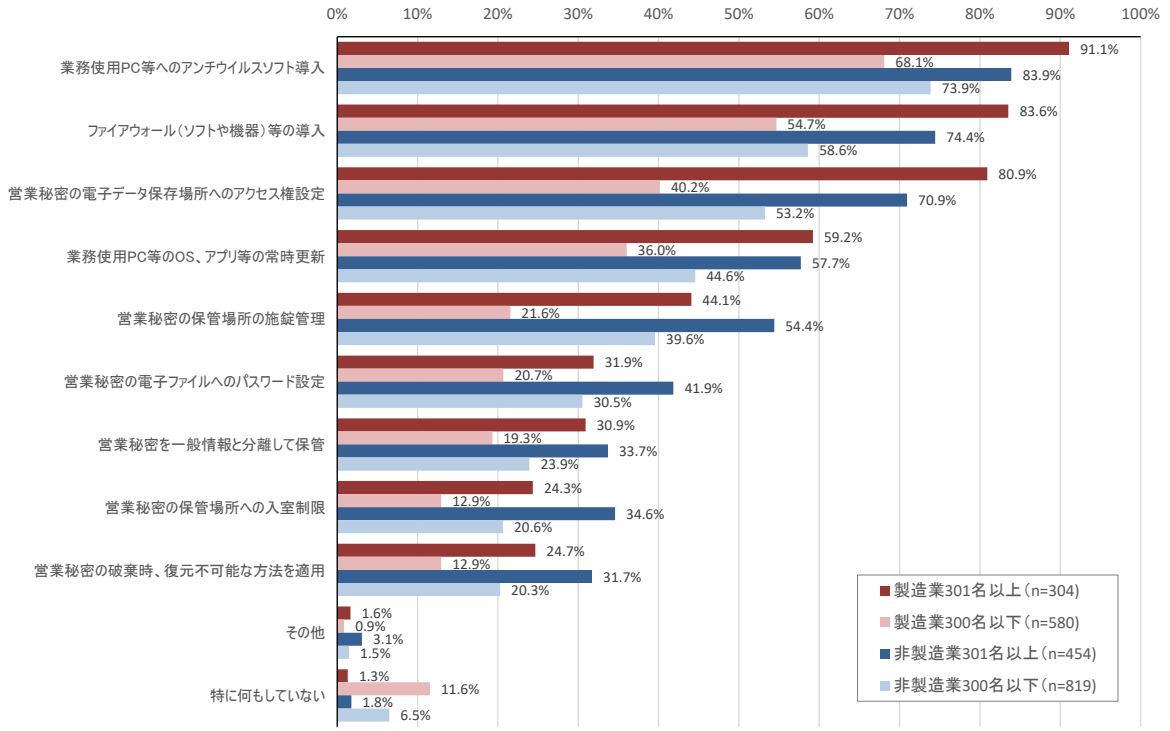

図 2.2-57　営業秘密情報への不正なアクセスを防ぐための対策の実施状況
（業種・規模別４区分によるクロス集計）

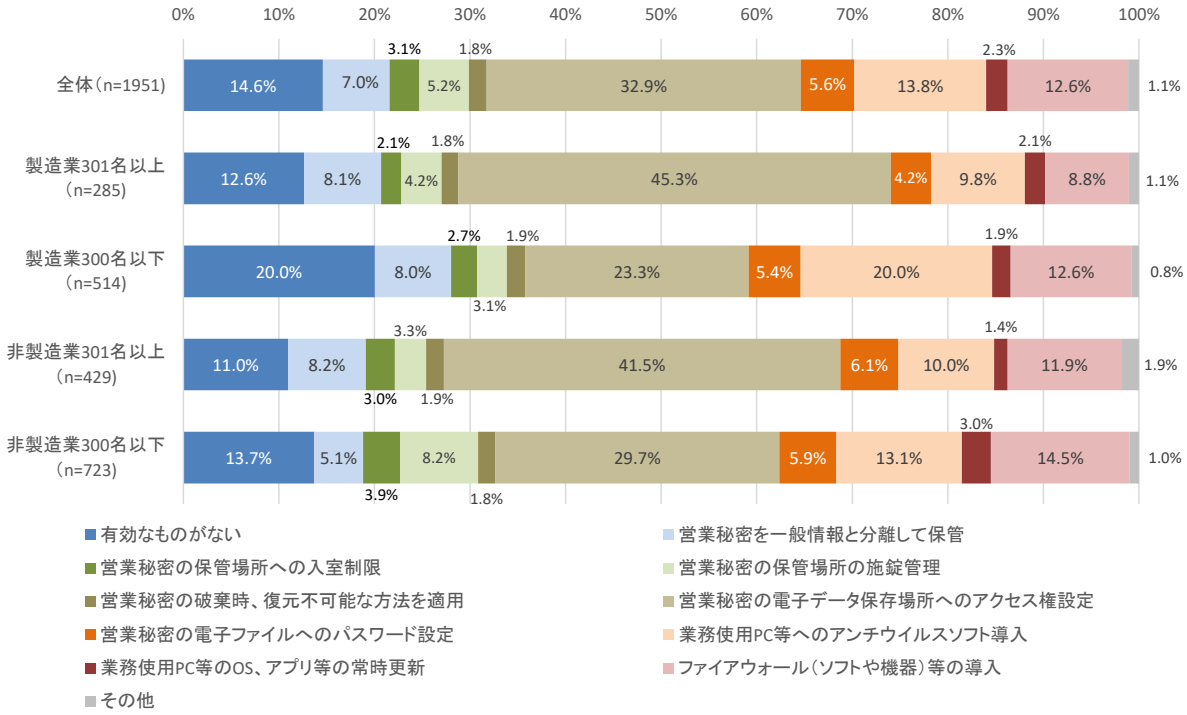

図 2.2-58　営業秘密情報への不正なアクセスを防ぐための対策の実施状況
（実施している対策のうち最も有効と考えるもの）

(3) 営業秘密情報の社外への不正な持出を防ぐための対策の実施状況

営業秘密情報の社外への不正な持出を防ぐための対策として、実施しているものについて尋ねた結果を示す。「特に何もしていない」が大幅に減少したのは、何らかの対策を講じる企業が増えたことを示すものである。「電子メールに添付できるファイルの制限」が減少したのは、添付ファイルに代わってセキュアなストレージを経由するファイルの受け渡しを行う企業が増えたことの影響が考えられる。

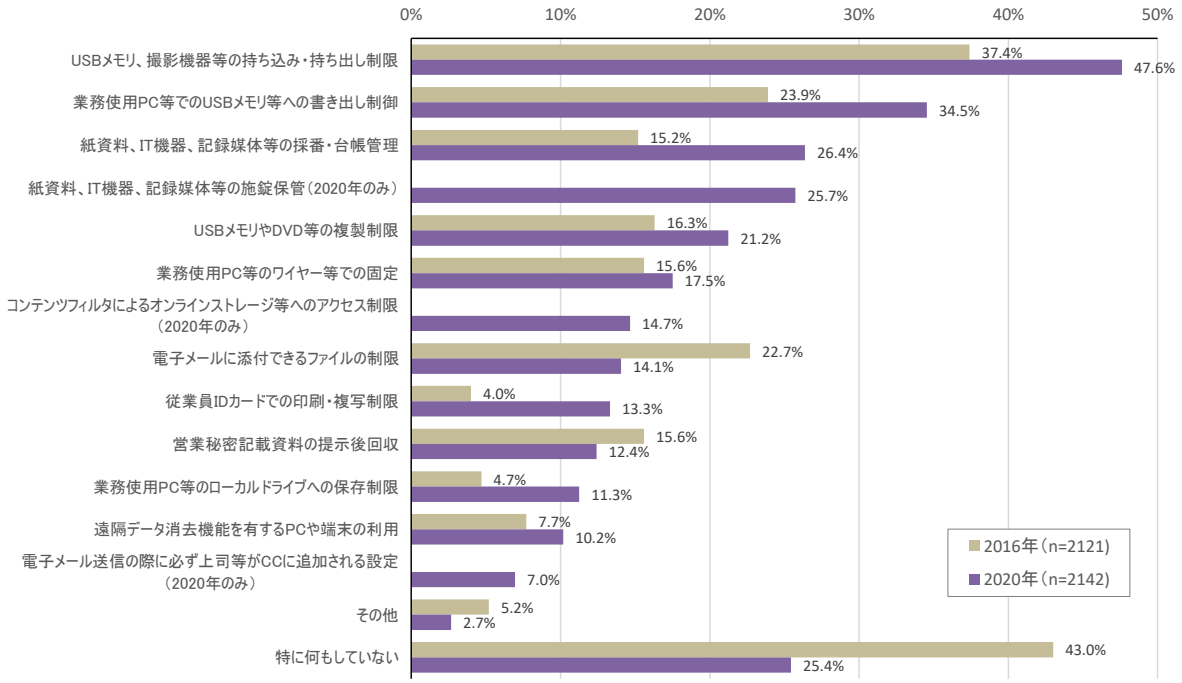

図 2.2-59　営業秘密情報の社外への不正な持出を防ぐための対策の実施状況（経年比較）

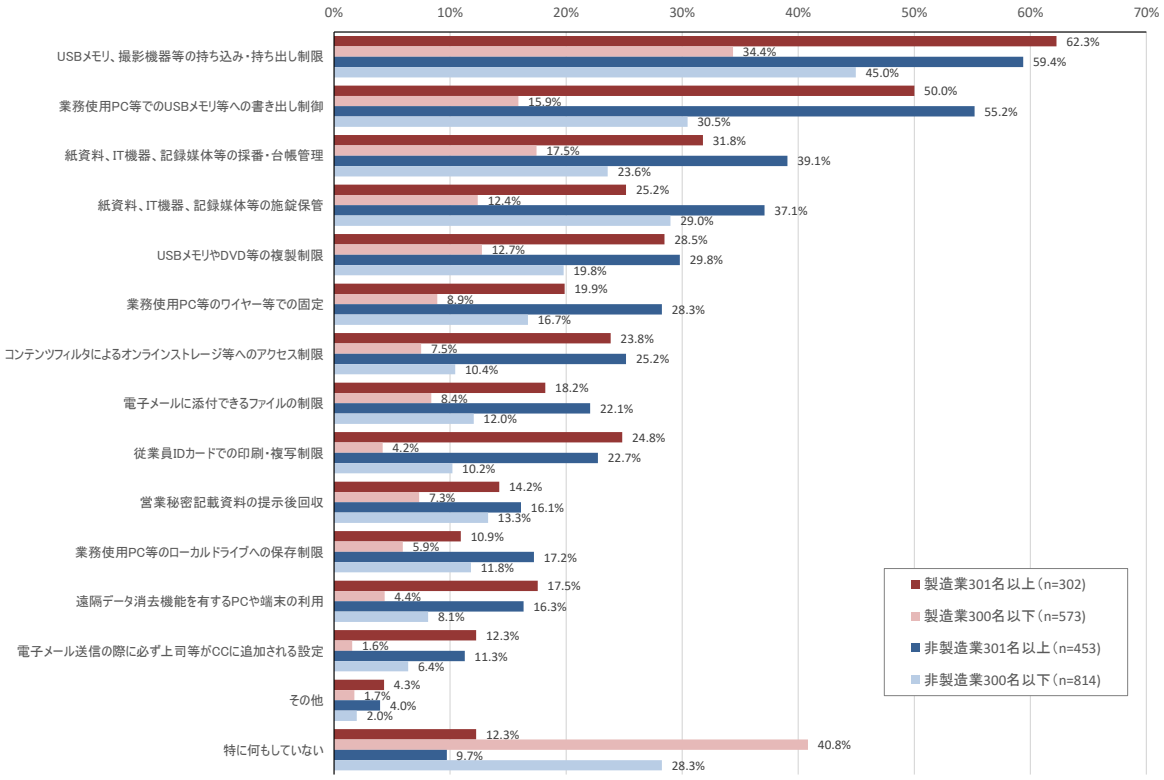

図 2.2-60　営業秘密情報の社外への不正な持出を防ぐための対策の実施状況
（業種・規模別４区分によるクロス集計）

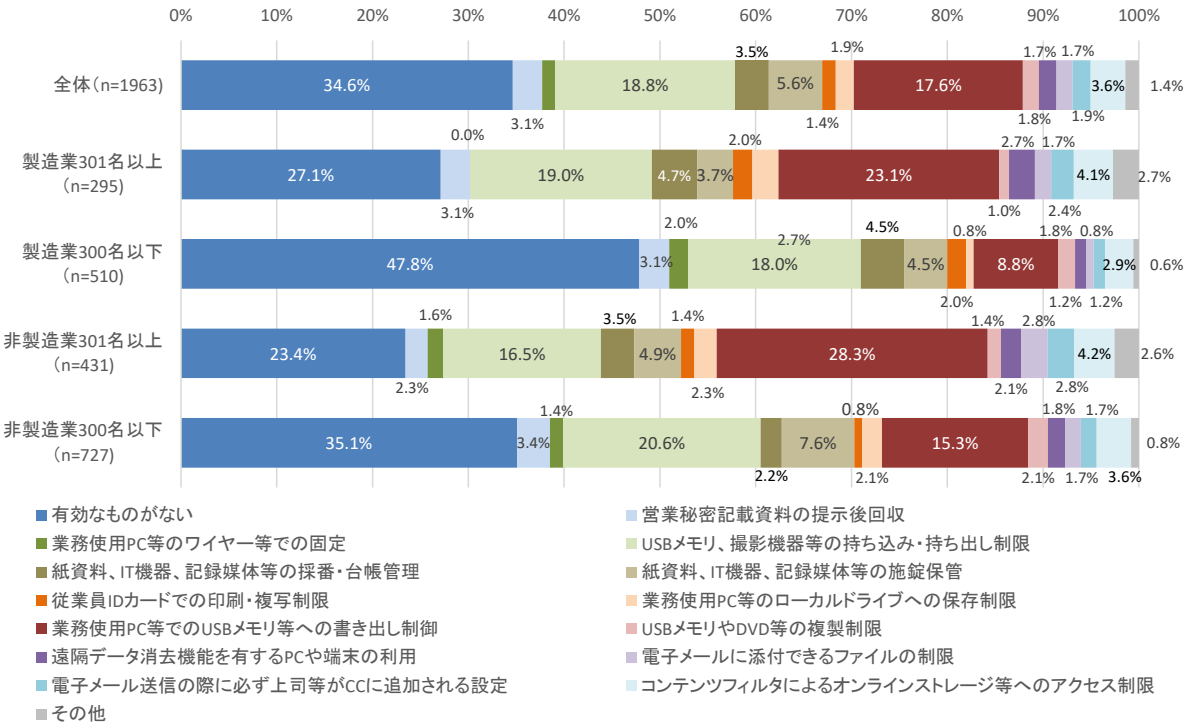

図 2.2-61　営業秘密情報の社外への不正な持出を防ぐための対策の実施状況
（実施している対策のうち最も有効と考えるもの）

(4) 営業秘密情報の漏えいを生じさせにくい環境をつくるための対策の実施状況

営業秘密の漏えいを生じさせにくい環境をつくるための対策として、実施しているものについて尋ねた結果を示す。(3)と同様、「特に何もしていない」が大きく減少している。なお、「情報システムのログの記録・保管と周知」については後述の 3.2 項において別途考察する。

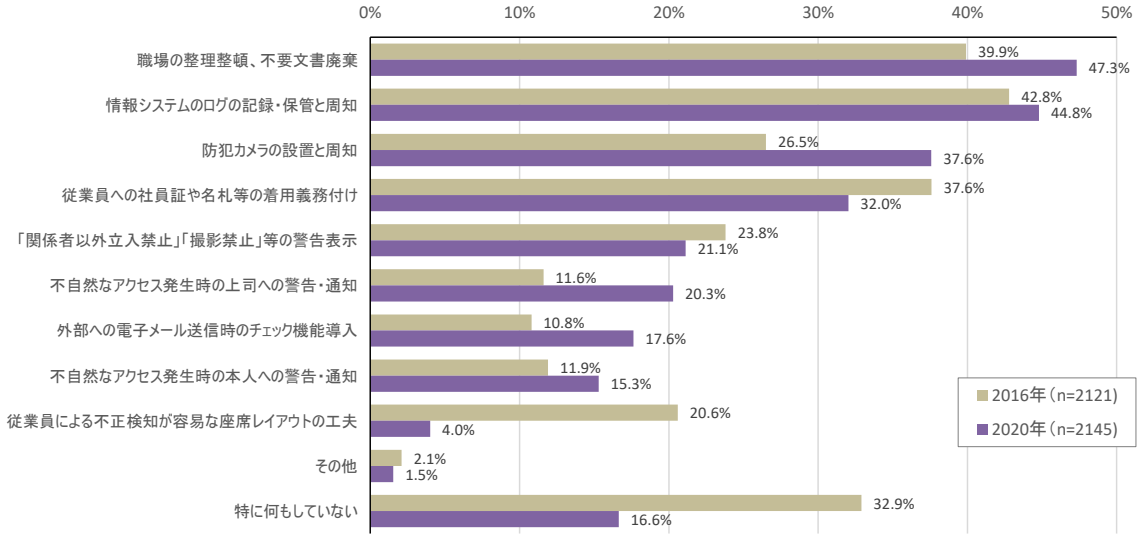

図 2.2-62　営業秘密情報の漏えいを生じさせにくい環境をつくるための対策の実施状況（経年比較）

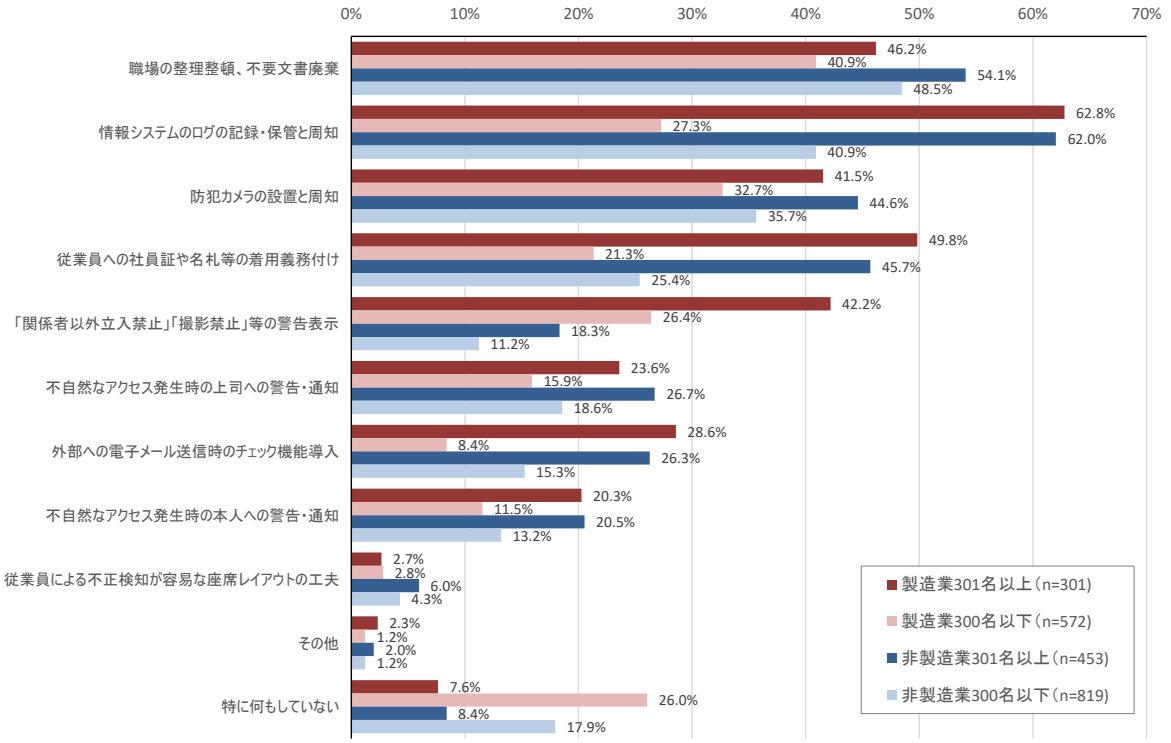

図 2.2-63　営業秘密情報の漏えいを生じさせにくい環境をつくるための対策の実施状況
（業種・規模別 4 区分によるクロス集計）

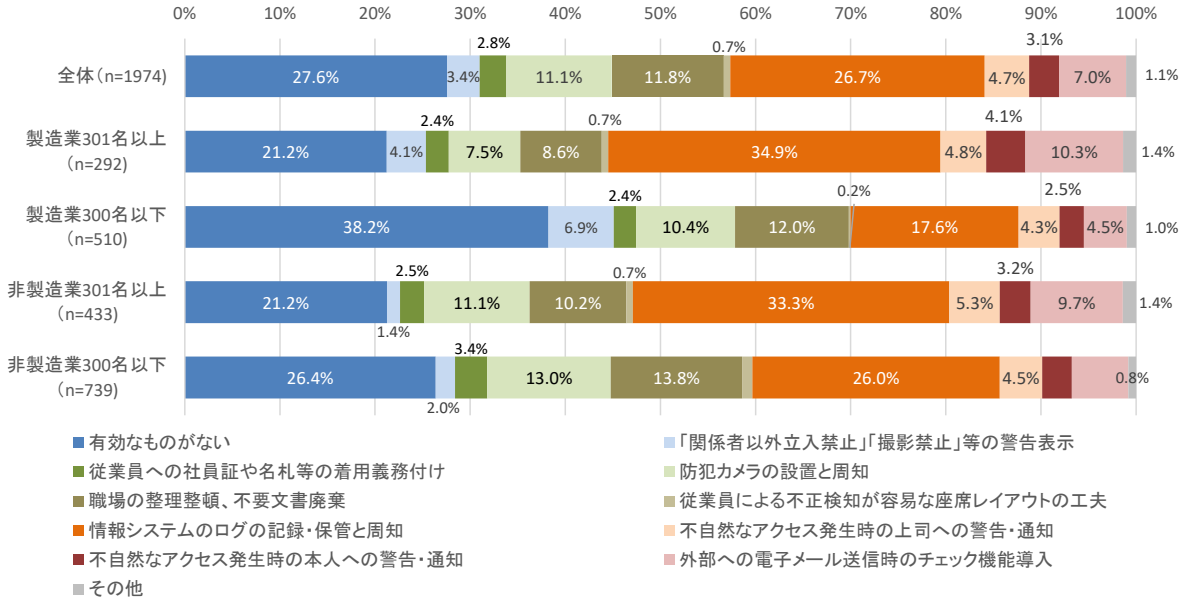

図 2.2-64　営業秘密情報の漏えいを生じさせにくい環境をつくるための対策の実施状況
（実施している対策のうち最も有効と考えるもの）

(5)　役員・従業員を対象とする秘密保持契約の締結状況

就業規則以外に役員・従業員と秘密保持契約（それに準じるような誓約書を含む）を締結しているかどうか、締結している場合はその秘密保持期間を含めて尋ねた結果を示す。2016 年度調査と比較すると、役員・従業員とも「期間の定め無し」を中心に締結している企業が増加傾向にあることがわかる。

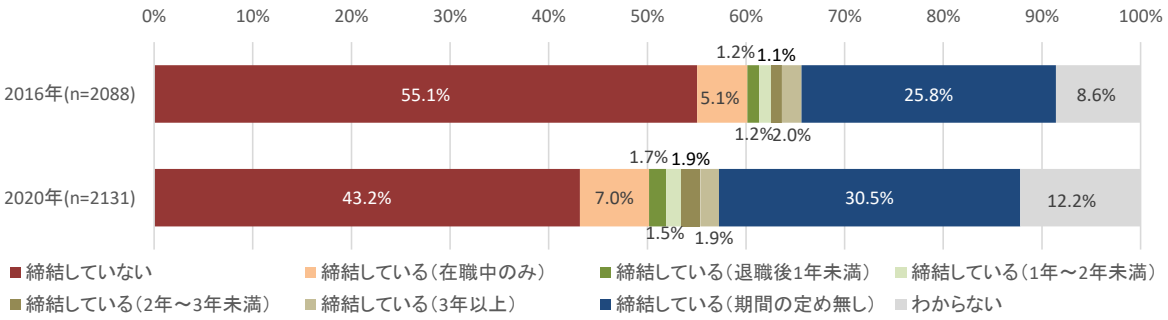

図 2.2-65　役員を対象とする秘密保持契約の締結状況（経年比較）

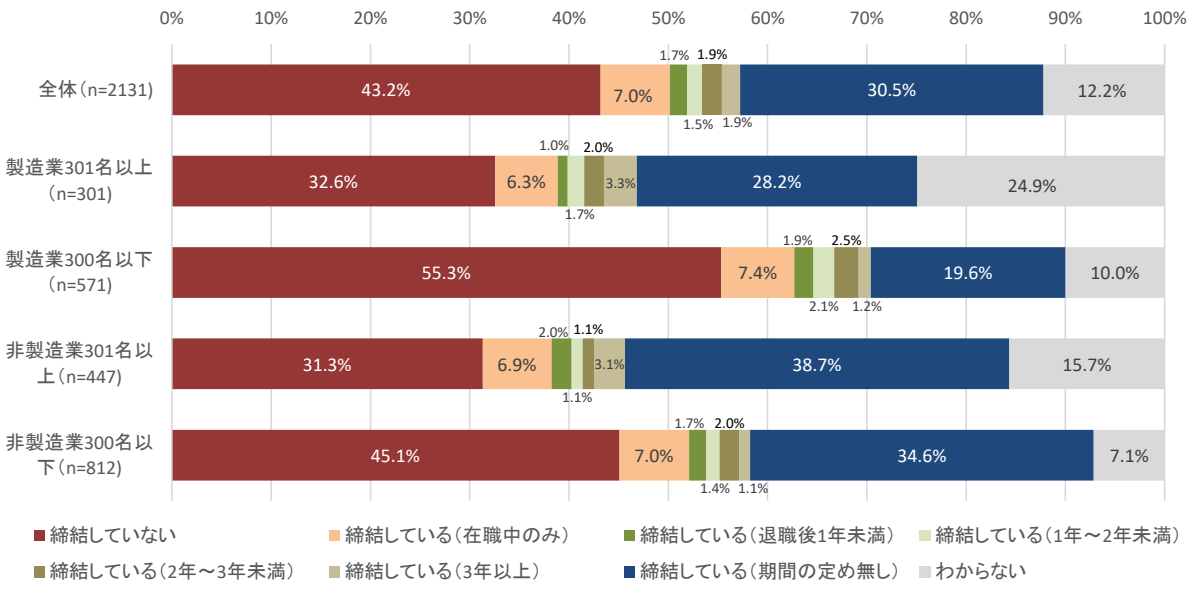

図 2.2-66　役員を対象とする秘密保持契約の締結状況（業種・規模別4区分によるクロス集計）

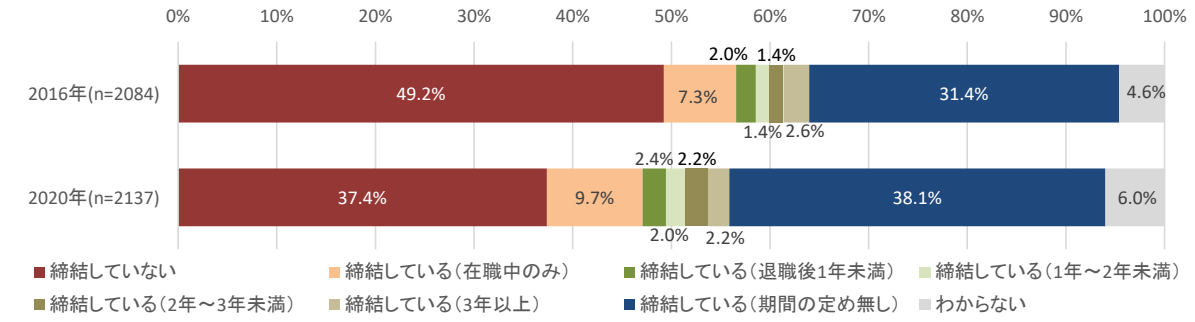

図 2.2-67　従業員を対象とする秘密保持契約の締結状況（経年比較）

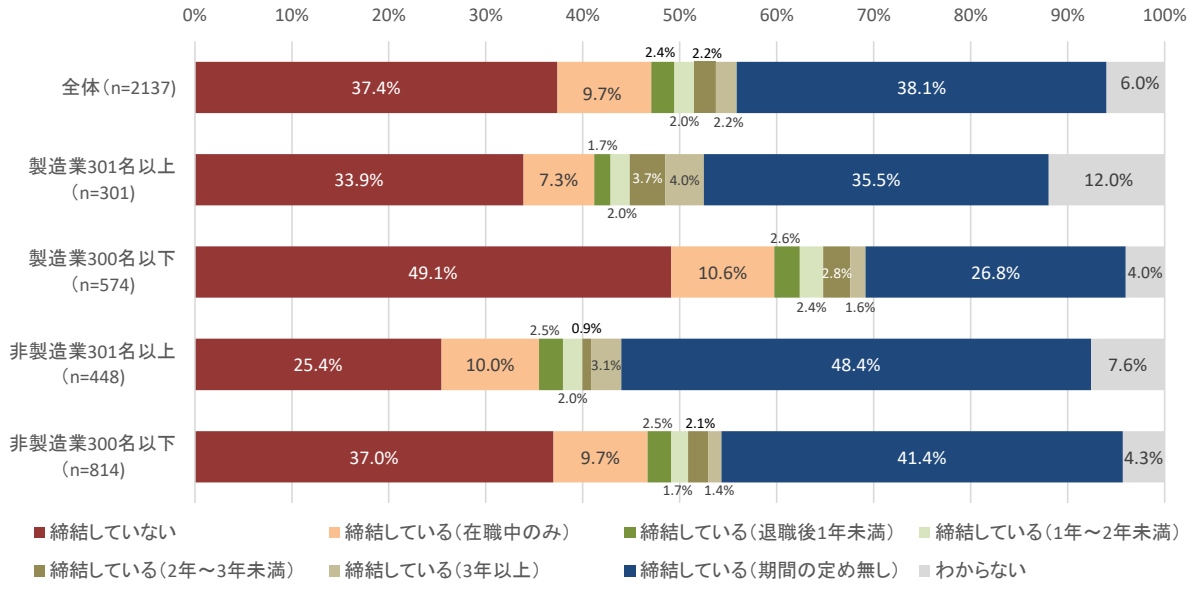

図 2.2-68　従業員を対象とする秘密保持契約の締結状況（業種・規模別4区分によるクロス集計）

(6) 役員・従業員を対象とする秘密保持契約を締結しない理由

前問で「締結していない」と回答した企業に対し、その理由について尋ねた結果を示す。

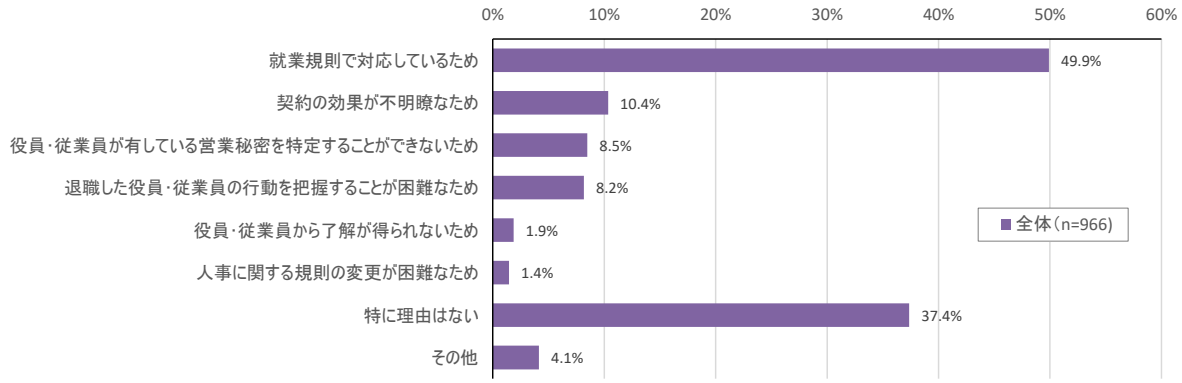

図 2.2-69　役員・従業員を対象とする秘密保持契約を締結しない理由

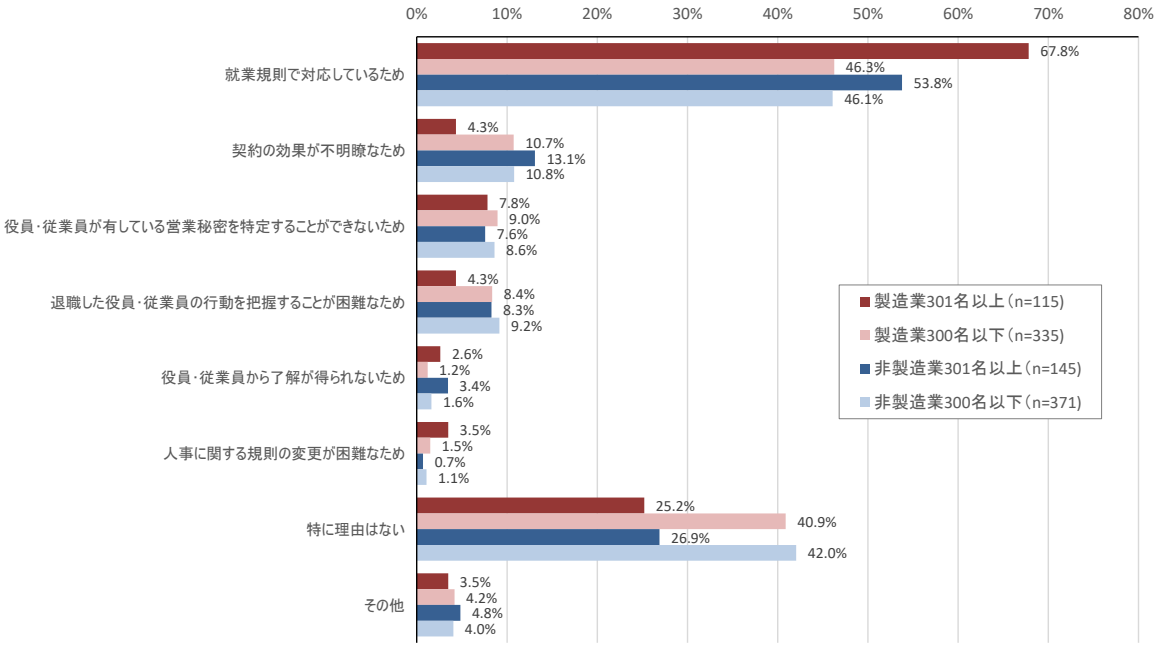

図 2.2-70　役員・従業員を対象とする秘密保持契約を締結しない理由
（業種・規模別４区分によるクロス集計）

(7) 役員・従業員を対象とする競業避止義務契約の締結状況

役員・従業員との競業避止義務契約（それに準じるような誓約書を含む）を締結しているかどうか、締結している場合はその期間も併せて尋ねた結果を示す。(5)と同様、役員・従業員とも「期間の定め無し」を中心に締結している企業が増加傾向にあることがわかる。

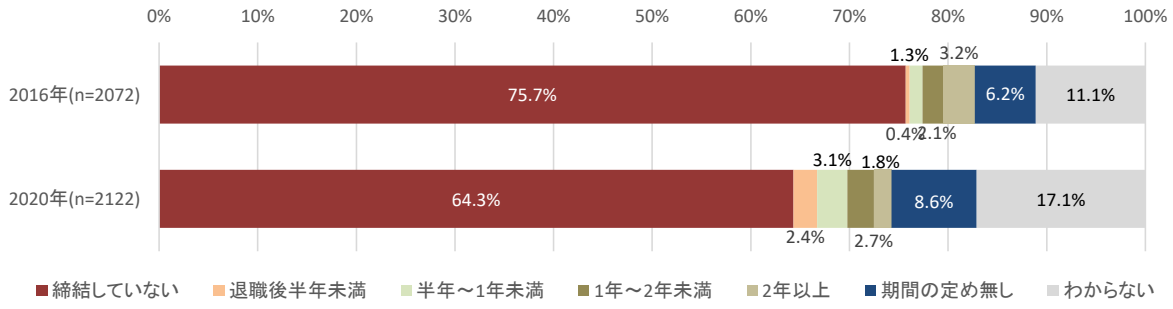

図 2.2-71　役員を対象とする競業避止義務契約の締結状況（経年比較）

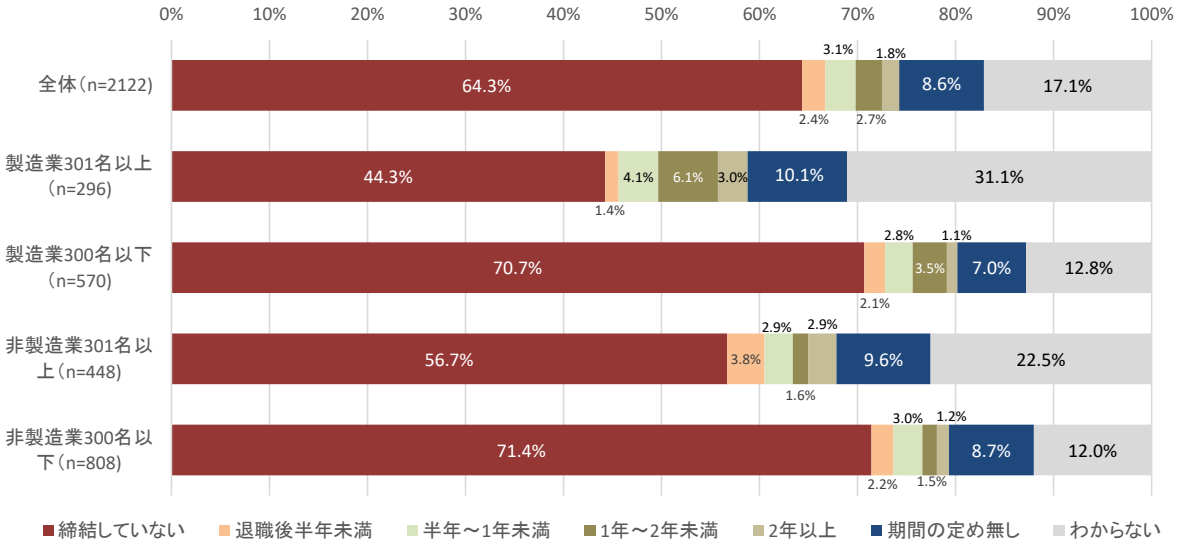

図 2.2-72　役員を対象とする競業避止義務契約の締結状況（業種・規模別4区分によるクロス集計）

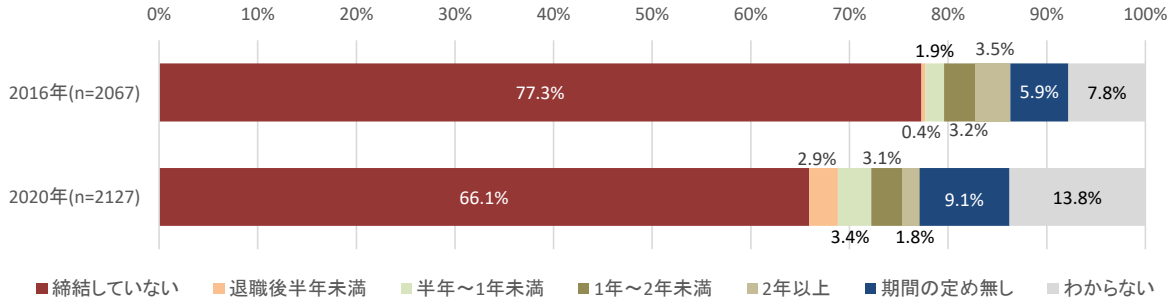

図 2.2-73　従業員を対象とする競業避止義務契約の締結状況（経年比較）

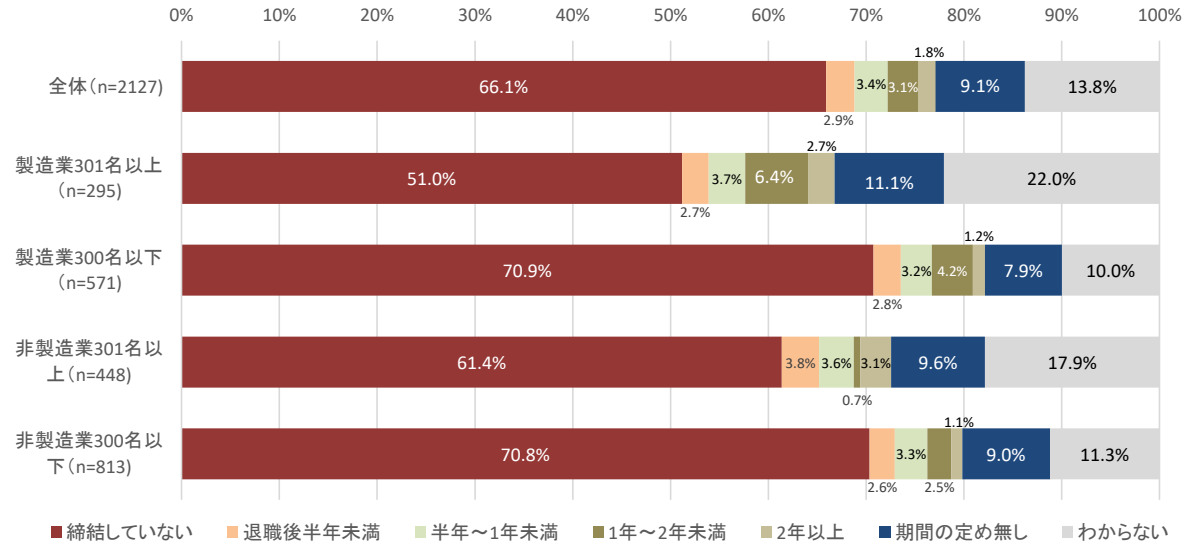

図 2.2-74　従業員を対象とする競業避止義務契約の締結状況（業種・規模別4区分によるクロス集計）

(8) 役員・従業員を対象とする競業避止義務契約で取り決めている内容

前問で「締結している」と回答した企業に対し、役員・従業員との競業避止義務契約（それに準じるような誓約書を含む）の中では、競業避止の期間以外に、どのような内容を取り決めているかについて尋ねた結果を示す。

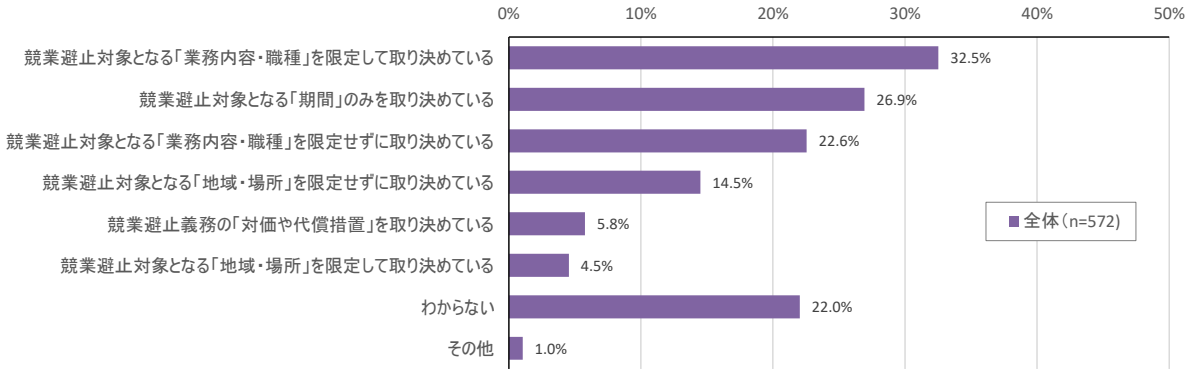

図 2.2-75　役員・従業員を対象とする競業避止義務契約で取り決めている内容

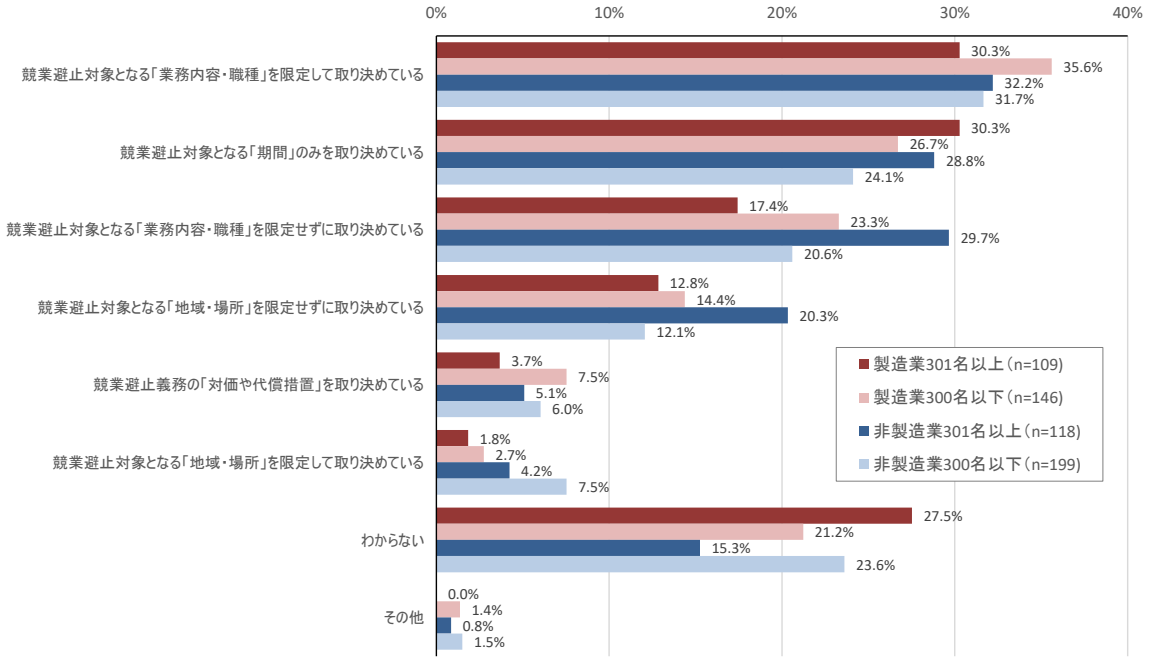

図 2.2-76　役員・従業員を対象とする競業避止義務契約で取り決めている内容
（業種・規模別４区分によるクロス集計）

(9)　競業避止義務契約に違反した役員・従業員への対応内容

(8)と同様の対象企業に対し、競業避止義務に違反した役員・従業員に対して実施した対応について尋ねた結果を示す。わずかではあるが訴訟に至った企業による回答が含まれている。

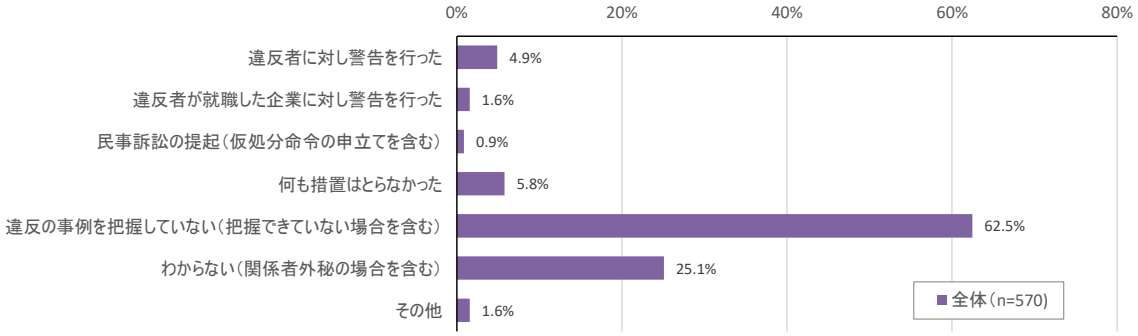

図 2.2-77　競業避止義務契約に違反した役員・従業員への対応内容

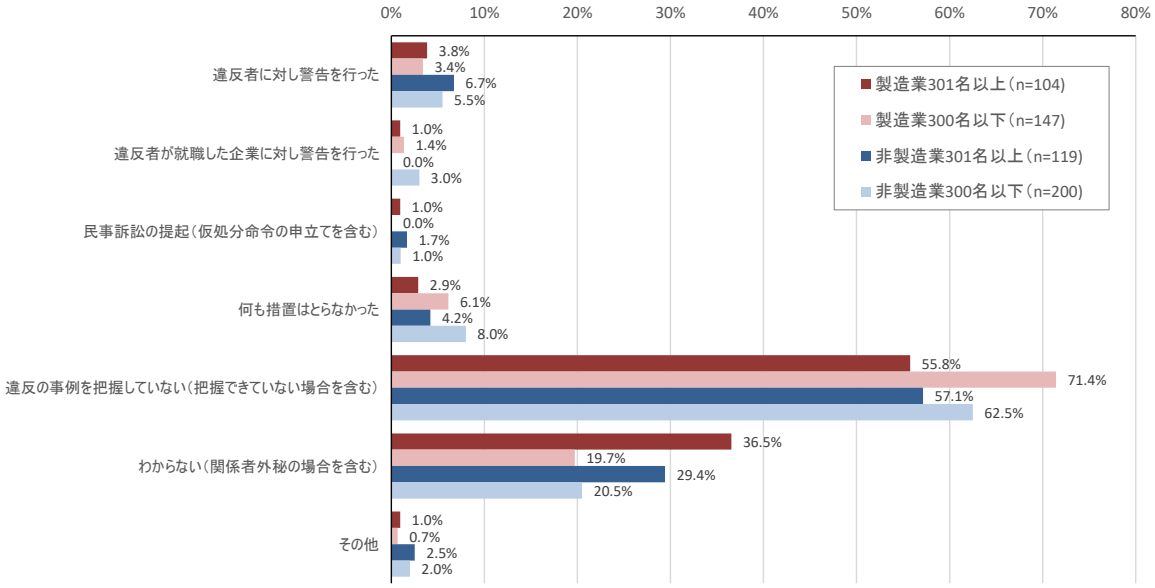

図 2.2-78　競業避止義務契約に違反した役員・従業員への対応内容
（業種・規模別４区分によるクロス集計）

(10) サプライチェーンにおける営業秘密の管理実態の把握に関する状況

子会社、関連会社、取引先など、貴社事業のサプライチェーンにおける営業秘密の管理状況について、どこまで把握しているかについて尋ねた結果を示す。

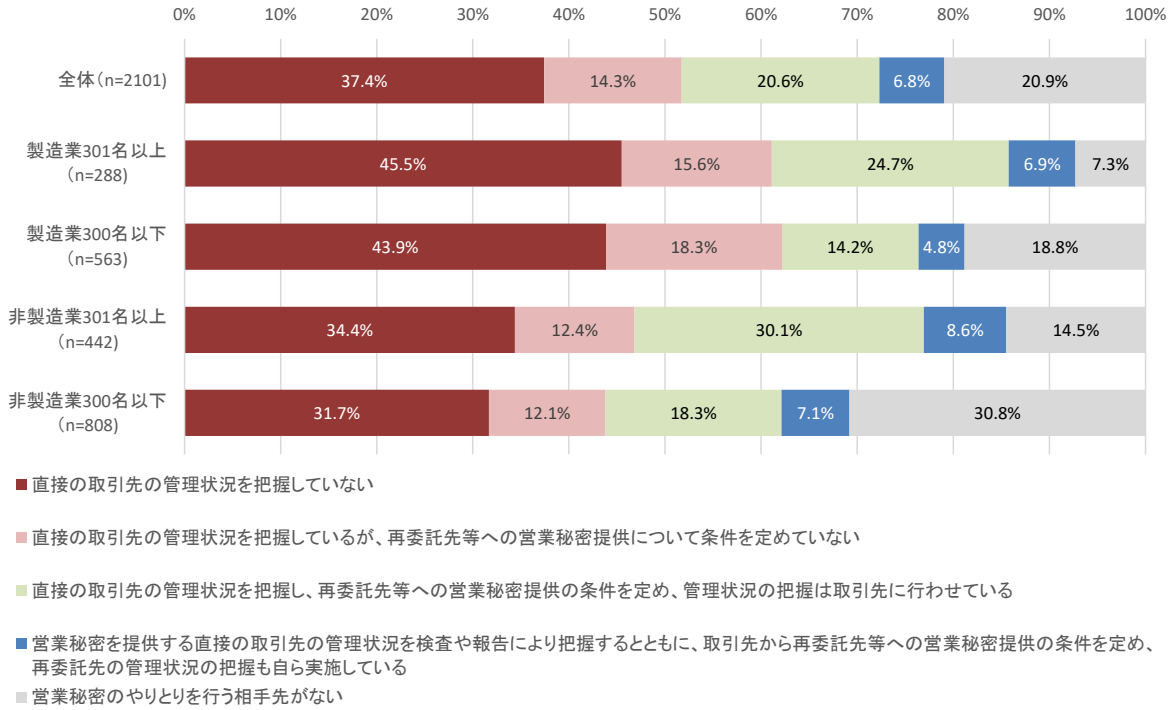

図 2.2-79　サプライチェーンにおける営業秘密の管理実態の把握に関する状況
（業種・規模別４区分によるクロス集計）

選択肢の内容が大きく異なるが、2016 年における類似設問では次のような傾向が示されている。

把握していない比率が少ないように見えるが、判断する対象が子会社・関連会社に限定され、対象がない比率がその分多い結果であると考えることができる。

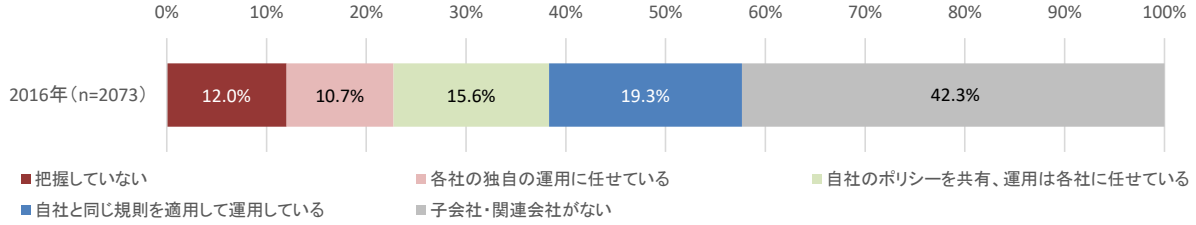

図 2.2-80　子会社・関連会社における営業秘密の管理状況（2016 年）

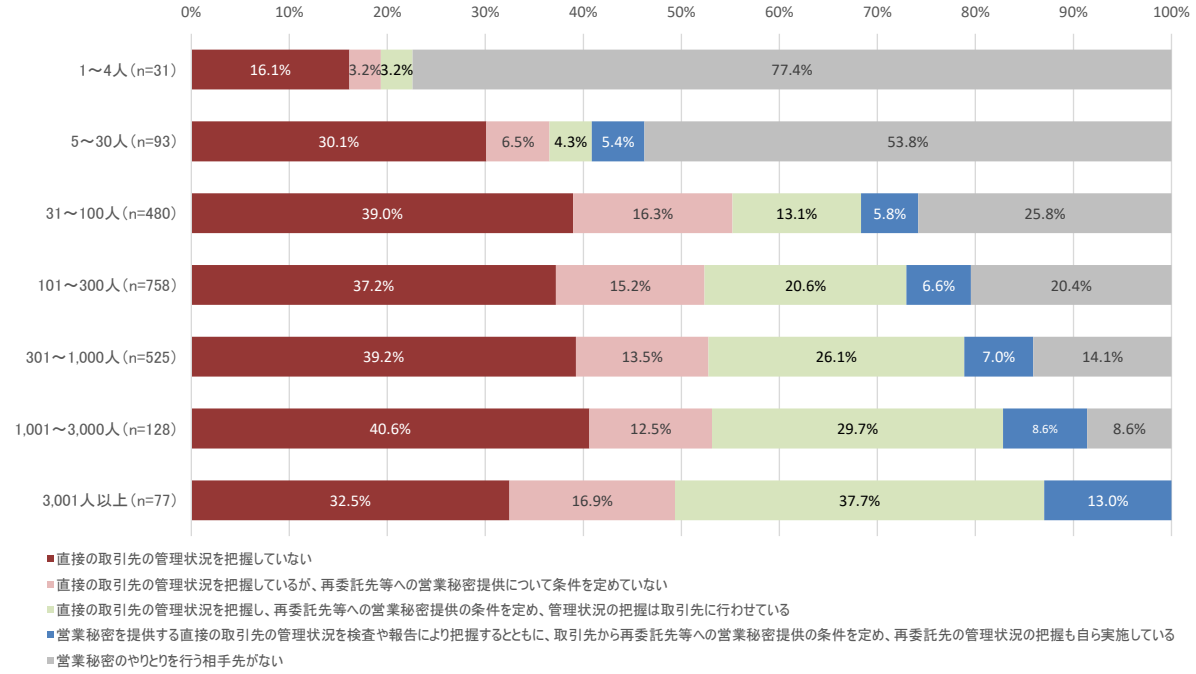

図 2.2-81　サプライチェーンにおける営業秘密の管理実態の把握に関する状況（規模別クロス集計）

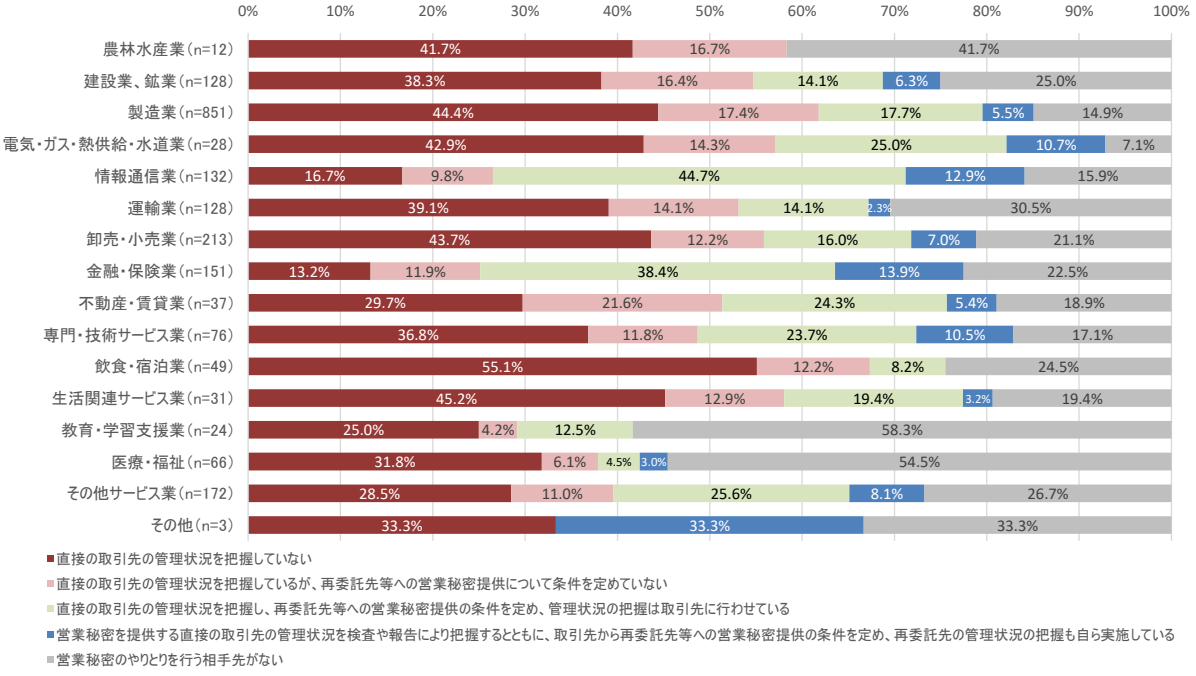

図 2.2-82　サプライチェーンにおける営業秘密の管理実態の把握に関する状況（業種別クロス集計）

(11) クラウドサービスを用いた営業秘密の共有状況

企業としてクラウドサービスを使って社外との営業秘密の共有を行っているかについて尋ねた結果を示す。

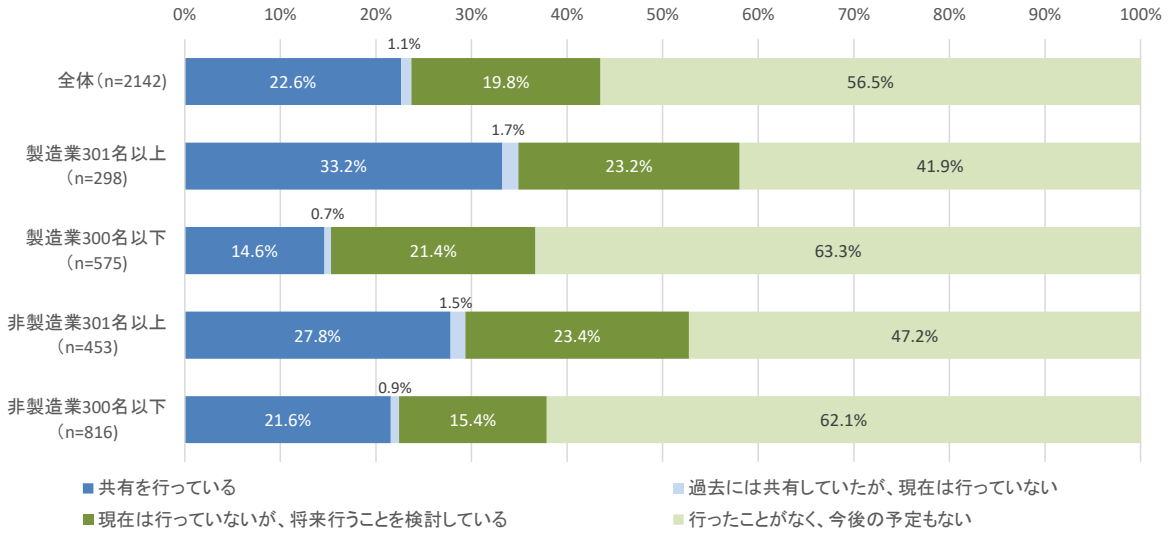

図 2.2-83　クラウドサービスを用いた営業秘密の共有状況（業種・規模別4区分によるクロス集計）

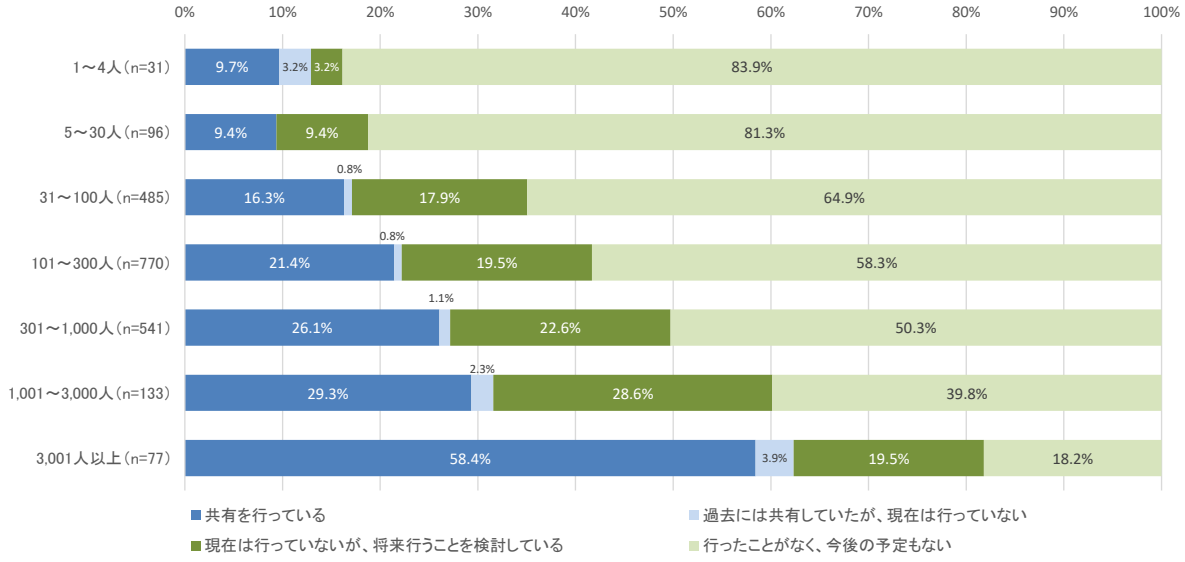

図 2.2-84　クラウドサービスを用いた営業秘密の共有状況（規模別クロス集計）

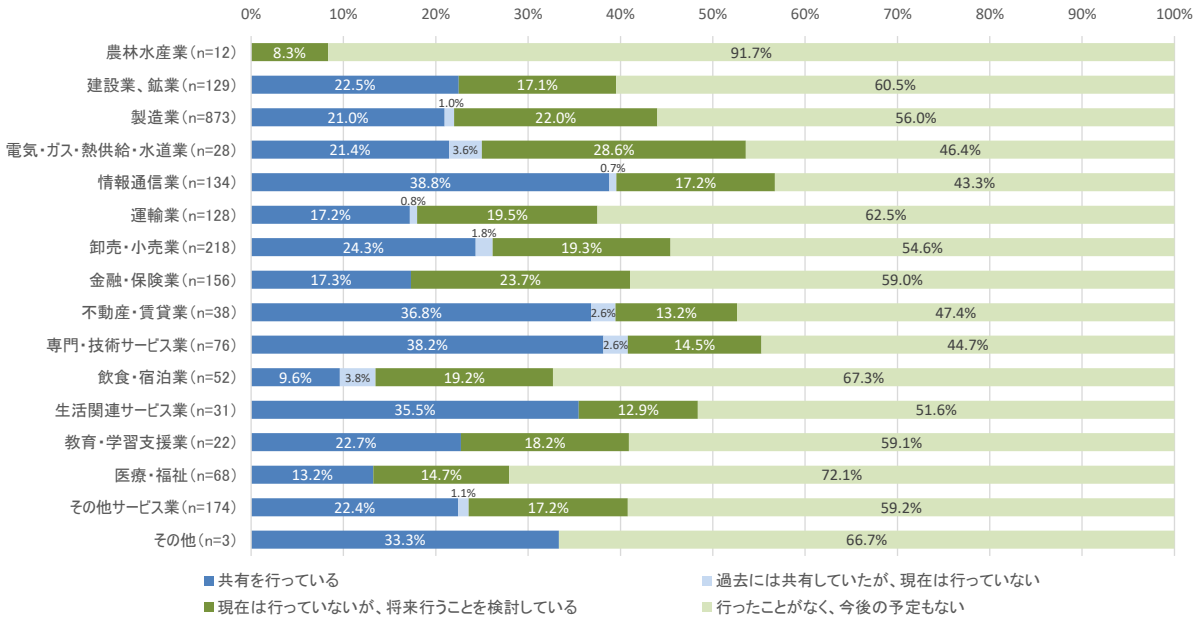

図 2.2-85　クラウドサービスを用いた営業秘密の共有状況（業種別クロス集計）

(12) クラウドサービスにおける営業秘密の不正利用防止のために実施している対策

クラウドサービスにおける営業秘密に関する不正使用リスクを想定した対策として、実施しているものについて尋ねた結果を示す。

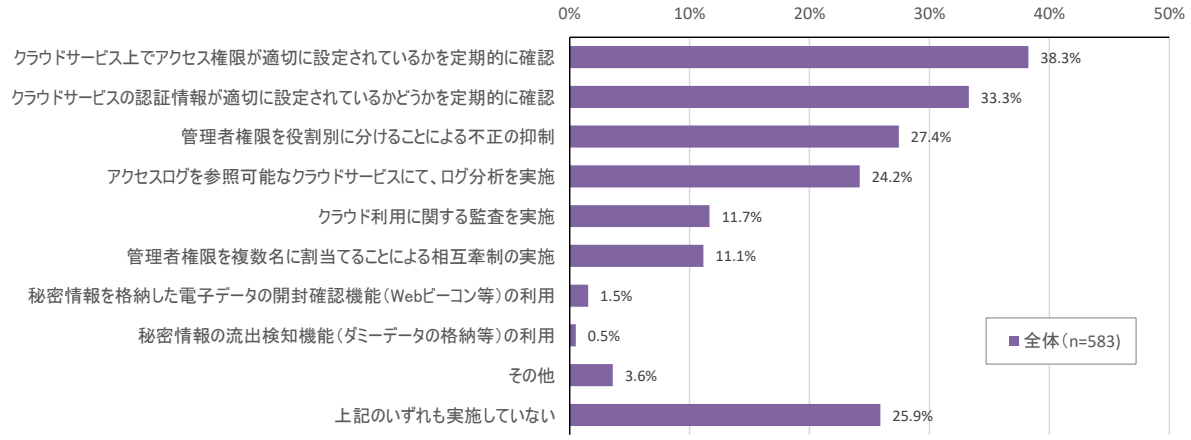

図 2.2-86　クラウドサービスにおける営業秘密の不正利用防止のために実施している対策

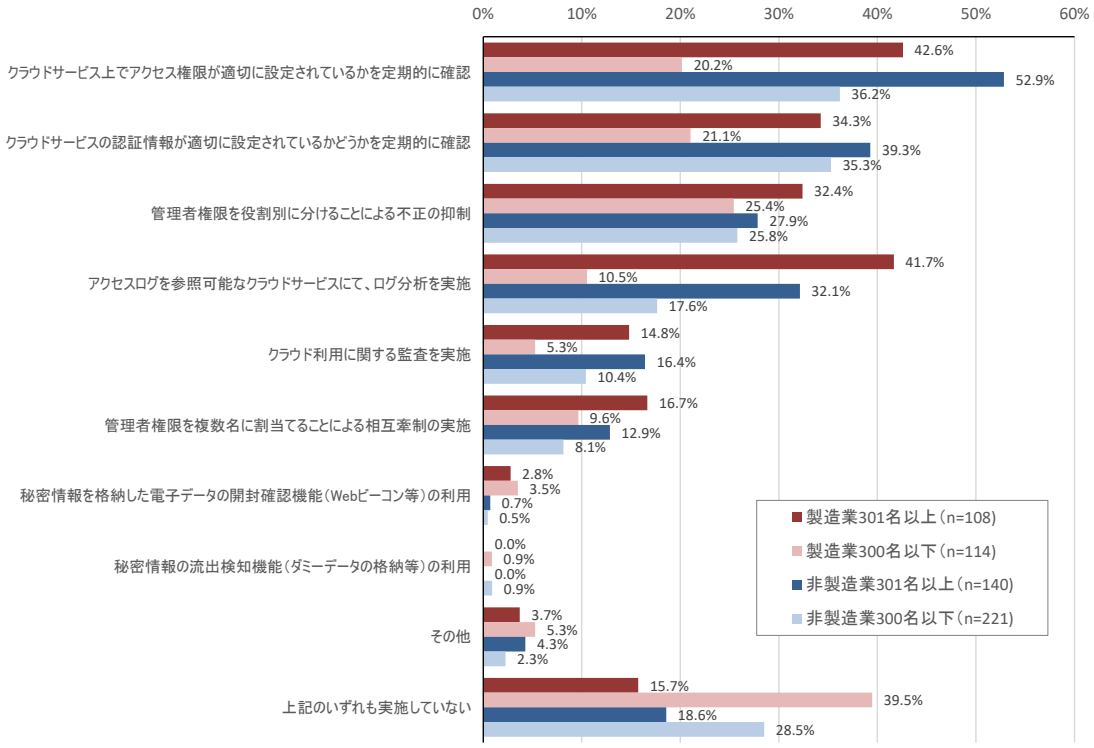

図 2.2-87　クラウドサービスにおける営業秘密の不正利用防止のために実施している対策
（業種・規模別４区分によるクロス集計）

(13) シャドークラウドが生じることを防止する対策の実施状況

本項目では、シャドークラウドを「貴社のセキュリティ担当者が把握していない、個人や部署が勝手に利用しているようなクラウドサービス」と定義した上で、その防止対策の実施状況について尋ねた結果を示す。

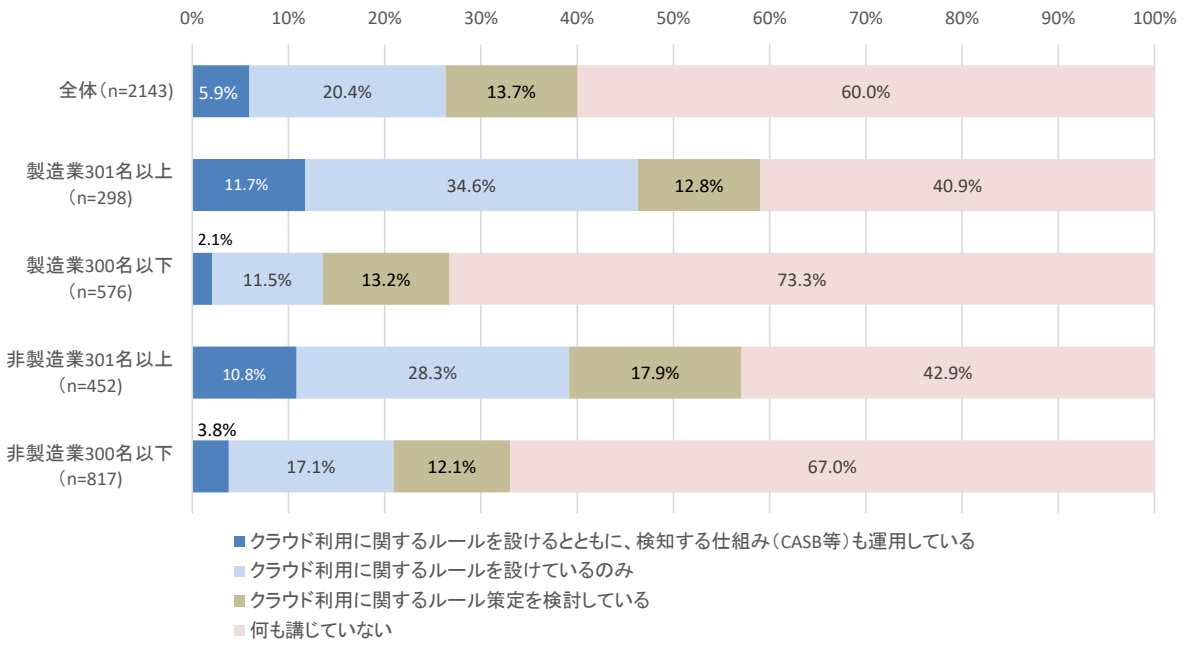

図 2.2-88　シャドークラウドが生じることを防止する対策の実施状況
（業種・規模別４区分によるクロス集計）

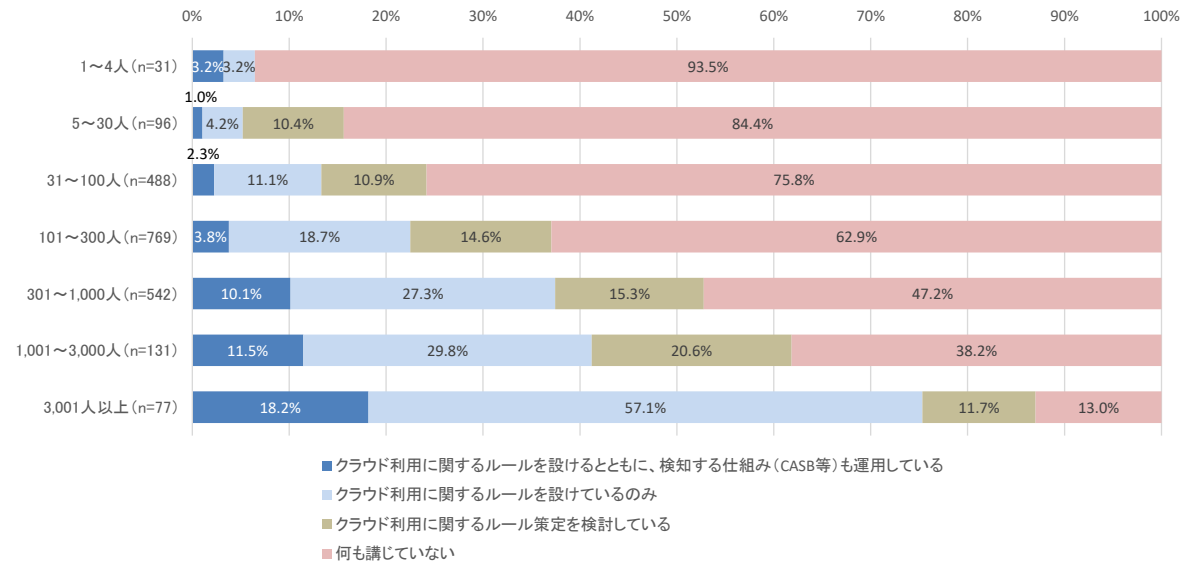

図 2.2-89　シャドークラウドが生じることを防止する対策の実施状況（規模別クロス集計）

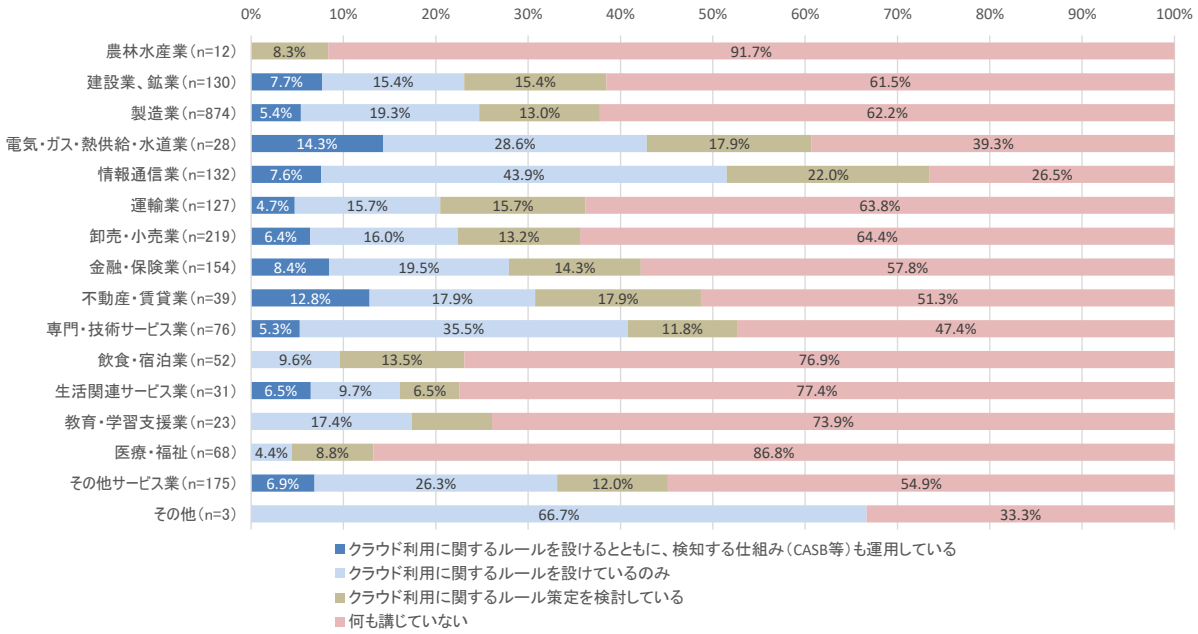

図 2.2-90　シャドークラウドが生じることを防止する対策の実施状況（業種別クロス集計）

(14) 秘密情報の漏えい時の組織体制

秘密情報の漏えい時における貴社の組織体制について尋ねた結果を示す。なお、2016 年度調査では通常時と漏えい時の２通りについて回答を求めているが、本調査では総設問数の削減の観点から漏えい時に限定して尋ねている。経年比較により、体制を定めていない企業が顕著に減少する傾向が示されていることがわかる。

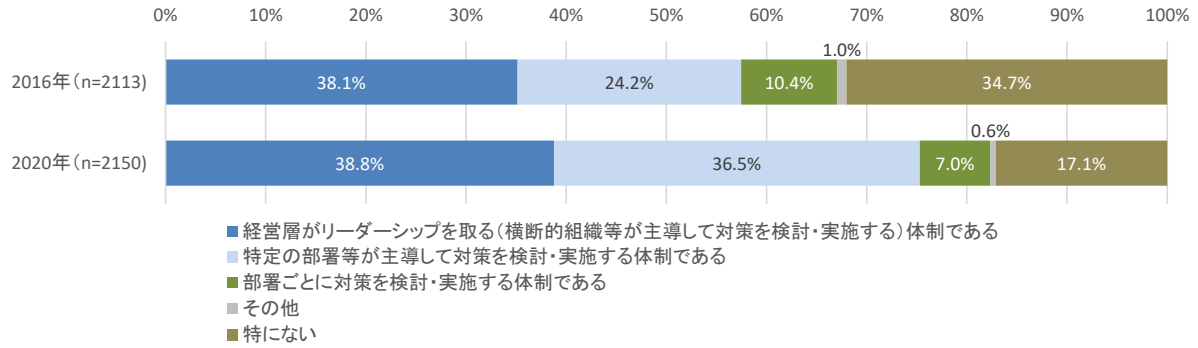

図 2.2-91　秘密情報の漏えい時の組織体制（経年比較）

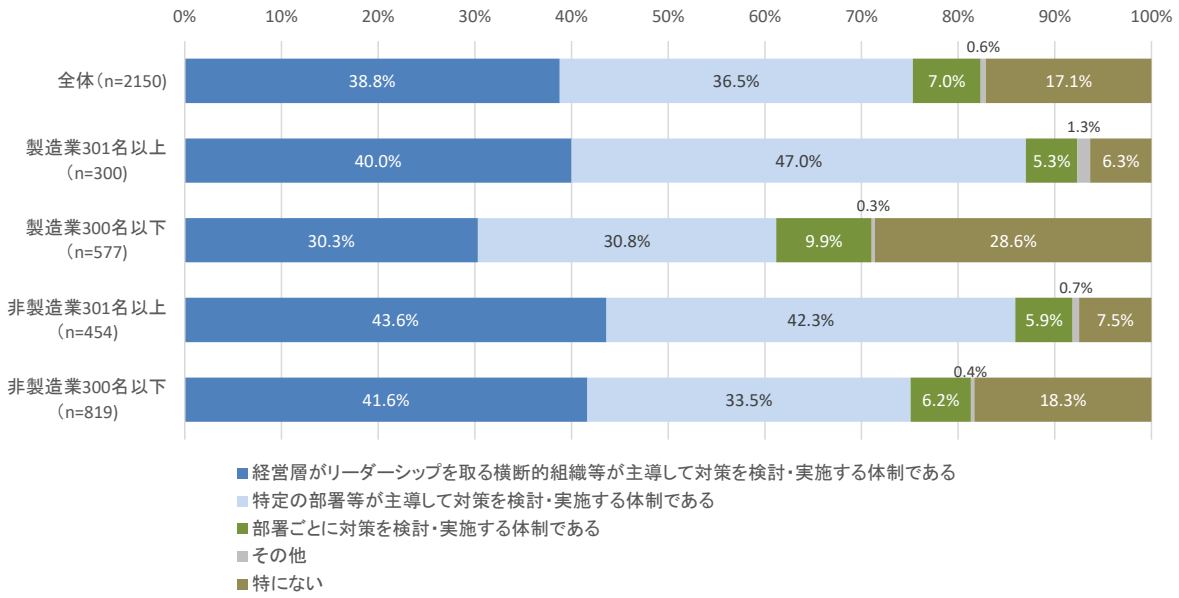

図 2.2-92　秘密情報の漏えい時の組織体制（業種・規模別４区分によるクロス集計）

(15) 秘密情報漏えい時の対応を主導する部署・担当

自社において秘密情報の漏えい時に対応を主導する部署・担当について尋ねた結果を示す。本項については企業の業種・業態・規模・業務内容等に応じて適切な方法を選択すればよく、特定の望ましい選択肢が存在するわけではない。

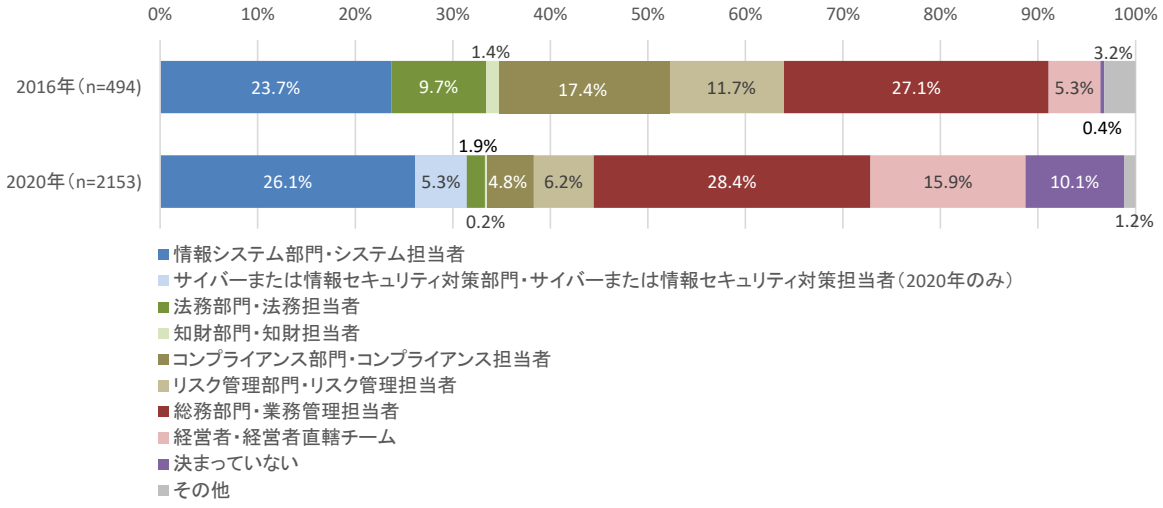

図 2.2-93　秘密情報漏えい時の対応を主導する部署・担当（経年比較）

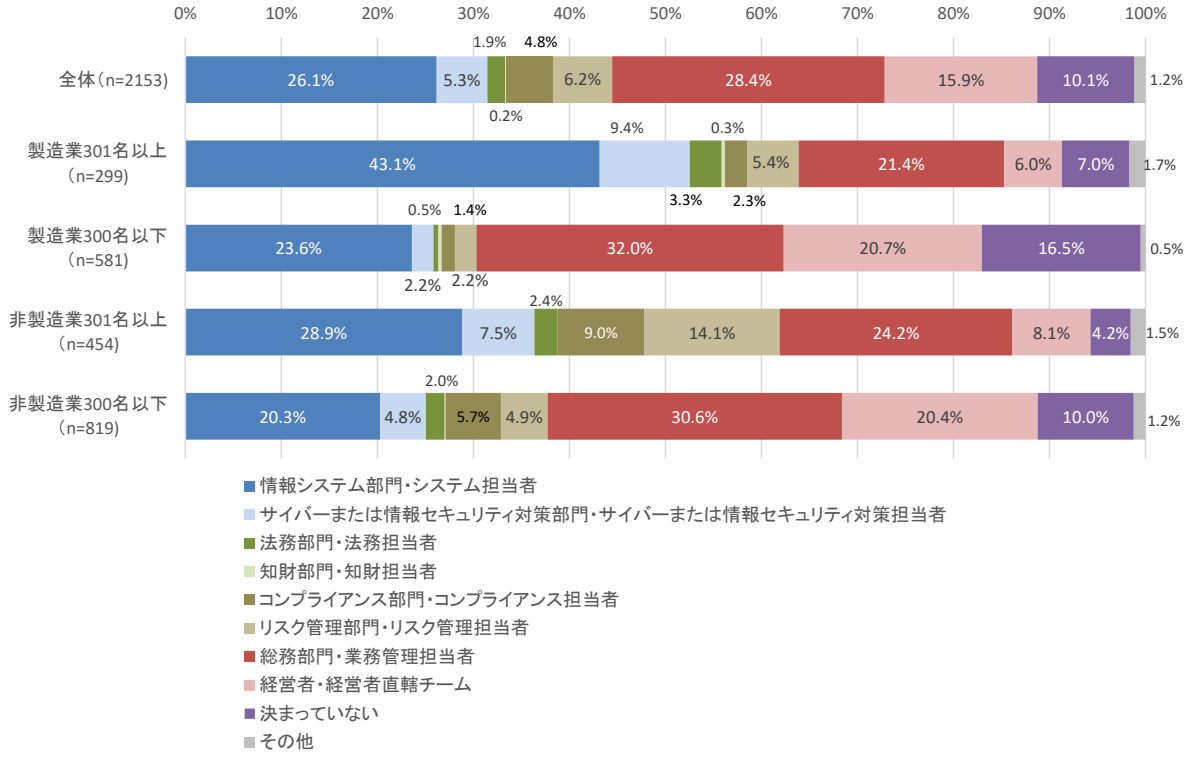

図 2.2-94　秘密情報漏えい時の対応を主導する部署・担当（業種・規模別4区分によるクロス集計）

(16) 過去５年間での情報管理に関する規程・手続等の見直し内容

過去 5 年以内に自社で扱う情報の管理に関する規程や手続・様式、教育啓発等について、どのような見直しを行ったのかを尋ねた結果を示す。2016 年度調査では単一選択形式で尋ねているので直接の比較は困難であるが、「見直しを行っていない」比率はほぼ同じであることから、大きな変化は生じていないと考えられる。

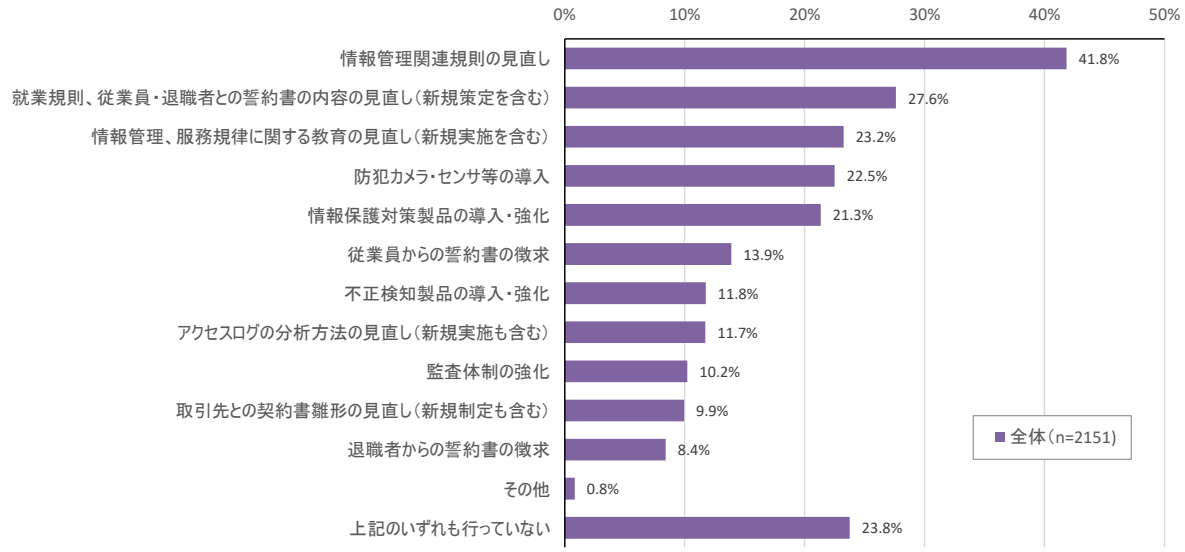

図 2.2-95　過去５年間での情報管理に関する規程・手続等の見直し内容

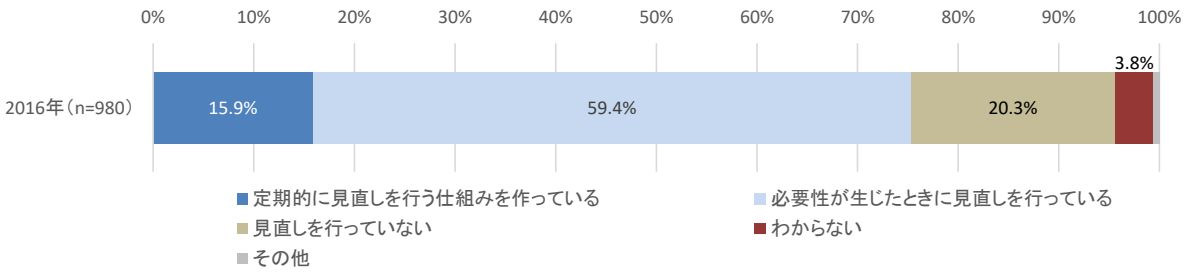

図 2.2-96　情報区分や格付け基準の見直し状況（2016 年）

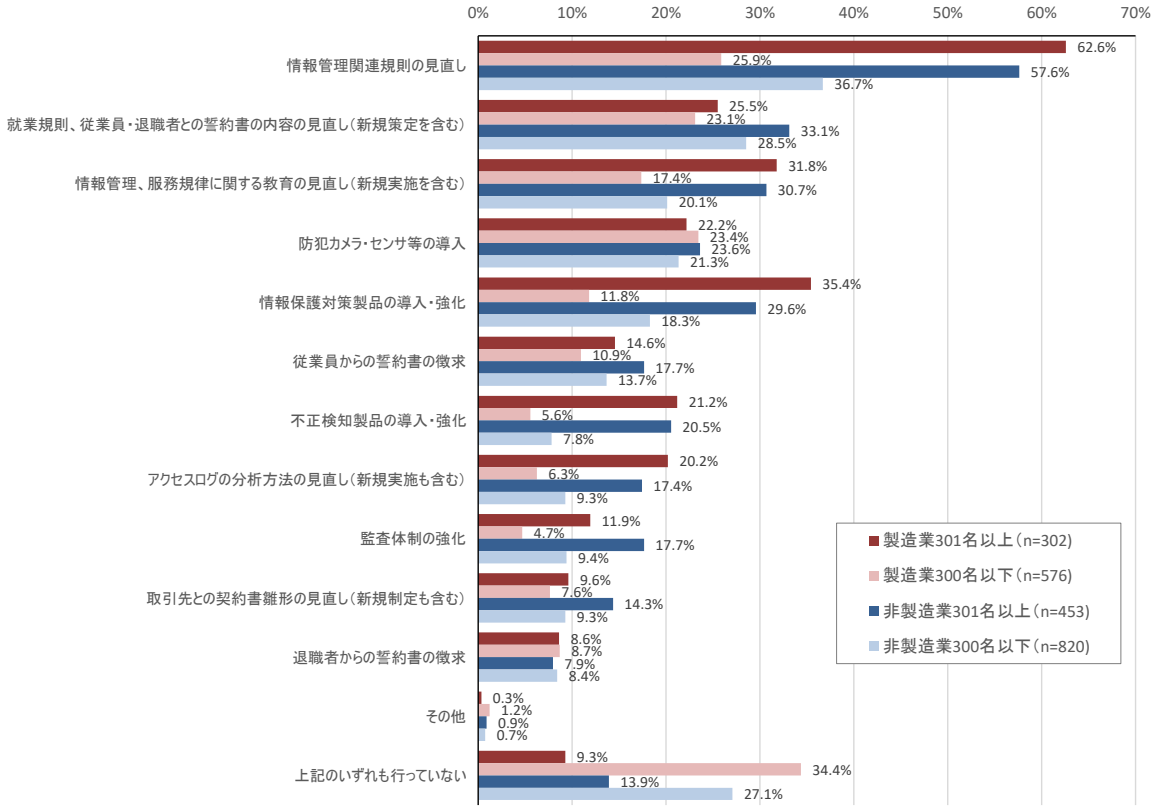

図 2.2-97　過去５年間での情報管理に関する規程・手続等の見直し内容
（業種・規模別４区分によるクロス集計）

(17) 情報管理に関する規程・手続等の見直しを行った目的や動機

前問で何らかの見直しを行ったと回答した企業を対象に、見直しを行った目的や動機について尋ねた結果を示す。「経営層の指示」「働き方の変化」「社内からの提案・働きかけ」が主たるきっかけとなっており、調査仮説で示した「取引先からの要請」を選んでいる企業は少ない。こうした傾向の背景についての考察を、後述の 3.1 項にて行う。なお、中小規模企業において、「経営層からの指示」がさらに多い傾向が示されているが、アンケート調査票における回答者情報によれば小規模・零細企業においては経営層が自らアンケートに回答している例が多く見られることから、こうした事情が結果に反映している可能性がある。

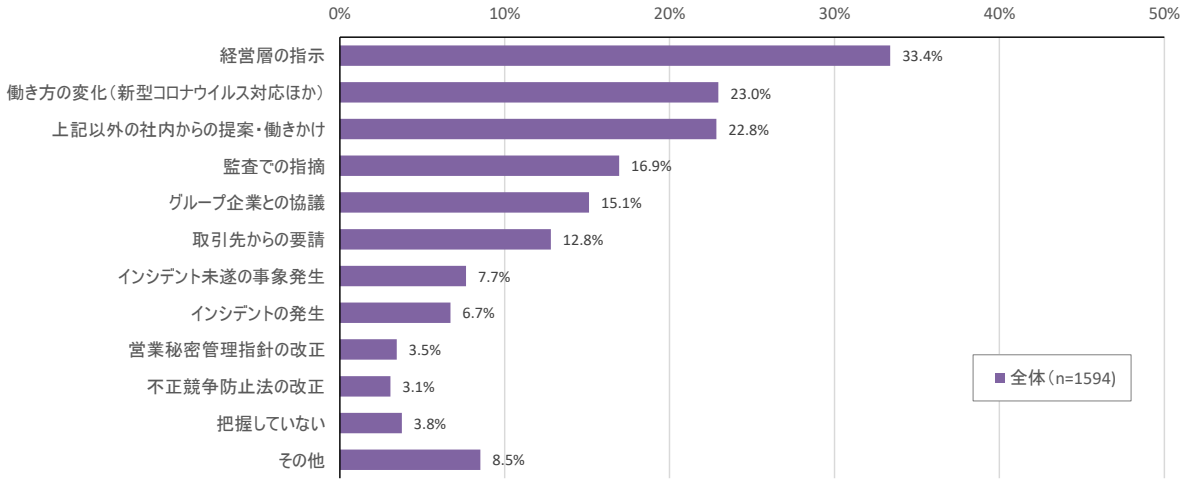

図 2.2-98　情報管理に関する規程・手続等の見直しを行った目的や動機

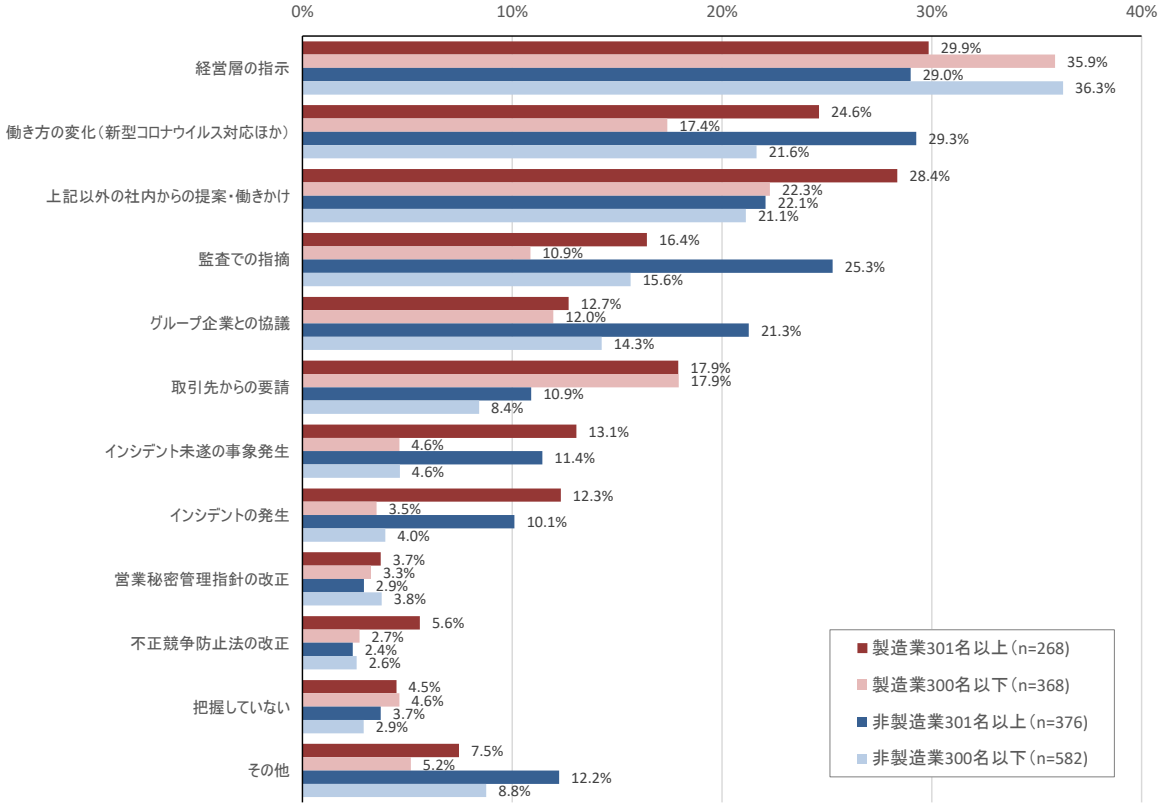

図 2.2-99　情報管理に関する規程・手続等の見直しを行った目的や動機
（業種・規模別４区分によるクロス集計）

(18) データの格付けや取扱の見直しを行った際に目標をどこに置いたか

営業秘密を含むデータの格付けや取扱いについて、過去５年間で見直しを行っている場合には、その目標をどこに置いたかについて尋ねた結果を示す。調査結果のうち、業種別クロス集計において情報通信業で突出した傾向が示されているが、これは情報通信業にて取得の多い ISMS 認証の影響である。

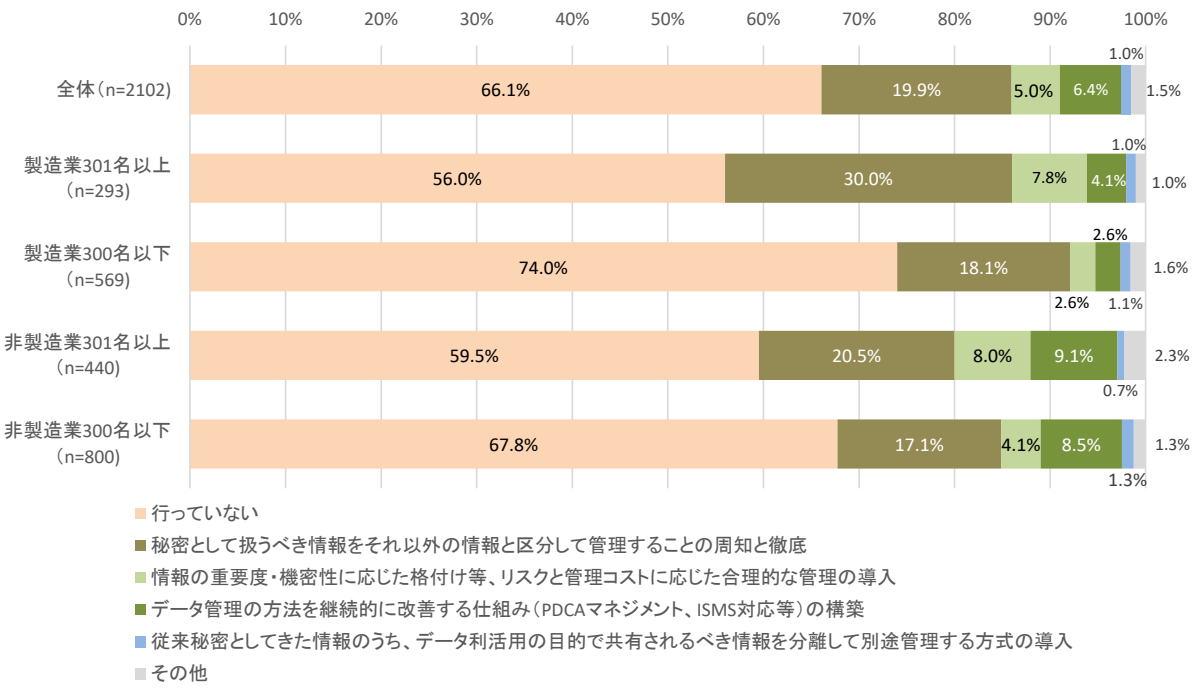

図 2.2-100　データの格付けや取扱の見直しを行った際に目標をどこに置いたか（業種・規模別４区分によるクロス集計）

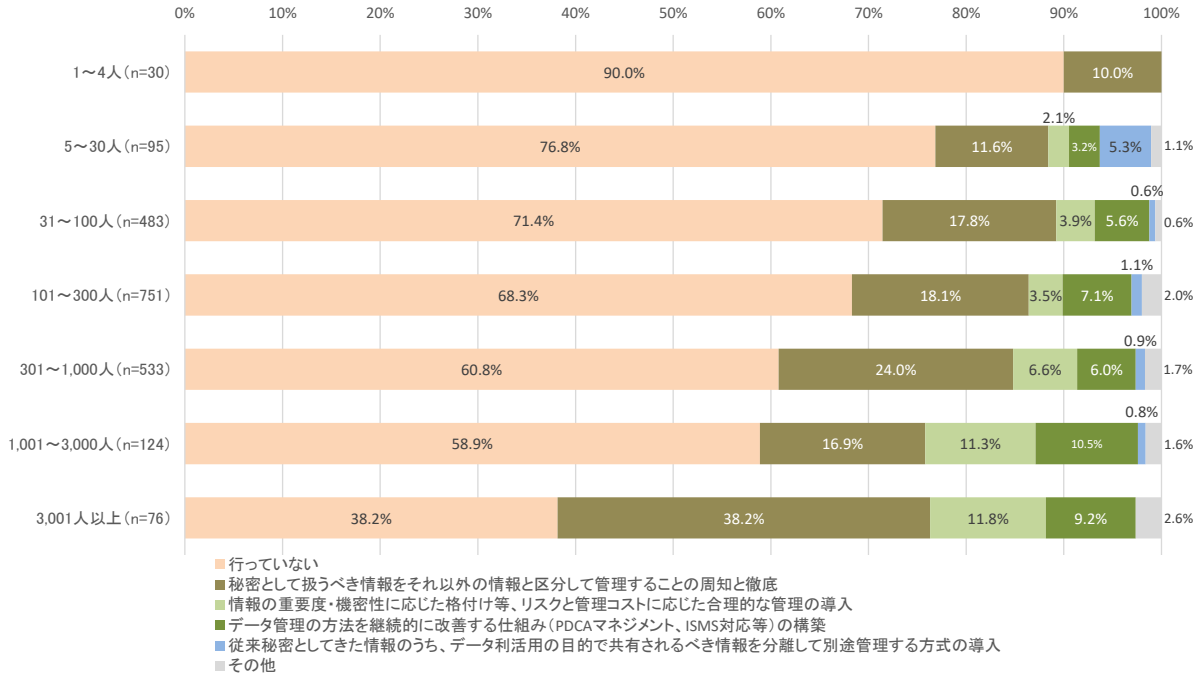

図 2.2-101　データの格付けや取扱の見直しを行った際に目標をどこに置いたか（規模別クロス集計）

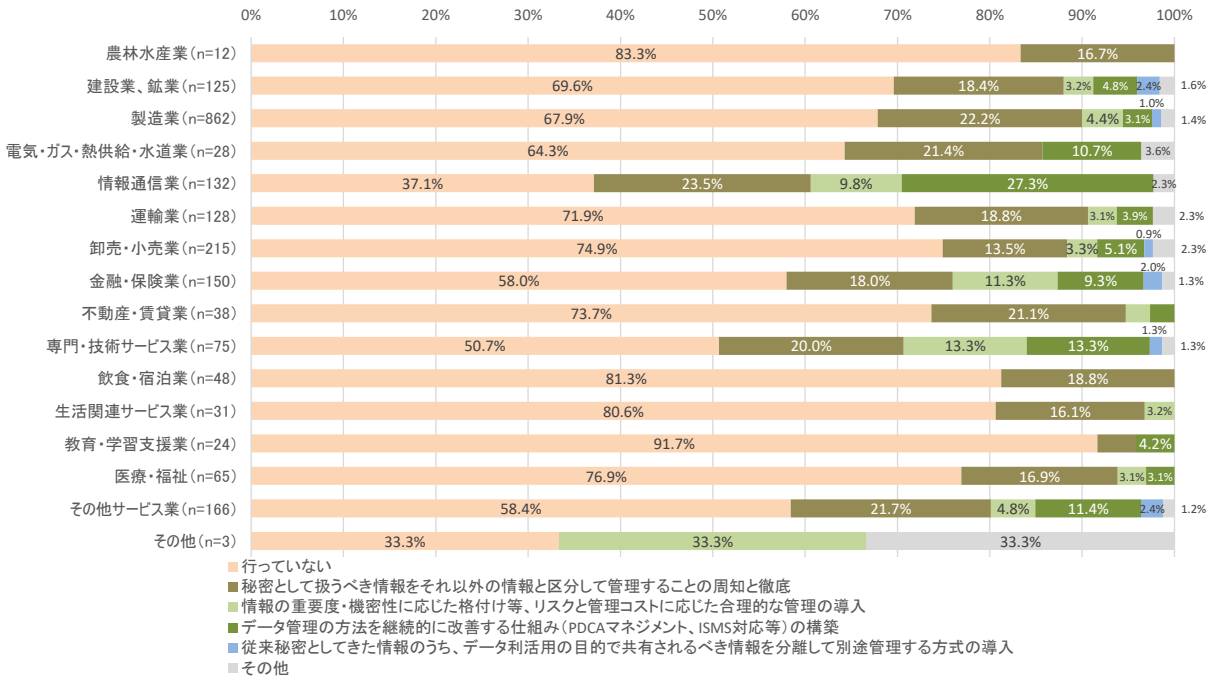

図 2.2-102　データの格付けや取扱の見直しを行った際に目標をどこに置いたか（業種別クロス集計）

2.2.4.5　ウィズコロナ・ポストコロナ環境における営業秘密管理の考え方

(1)　テレワーク（在宅勤務等）の実施状況

2020 年以降の新型コロナウイルス蔓延とそれに伴う非常事態宣言発令に伴い、テレワーク（在宅勤務等）の働き方を実施したかどうかについて尋ねた結果を示す。本項は情報管理やセキュリティ対策と直接関連するものではない。

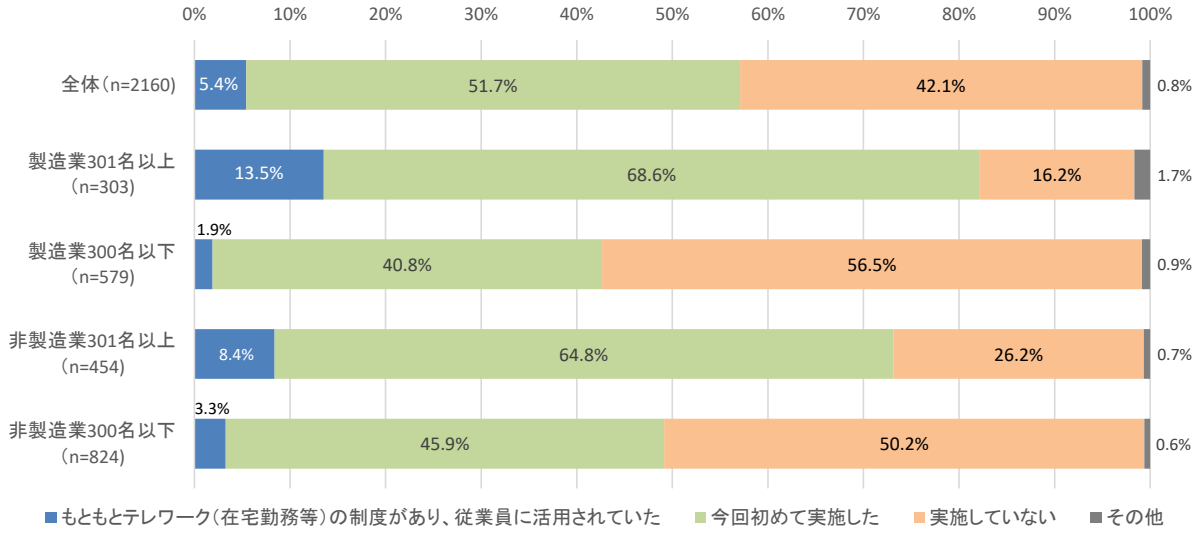

図 2.2-103　テレワーク（在宅勤務等）の実施状況（業種・規模別 4 区分によるクロス集計）

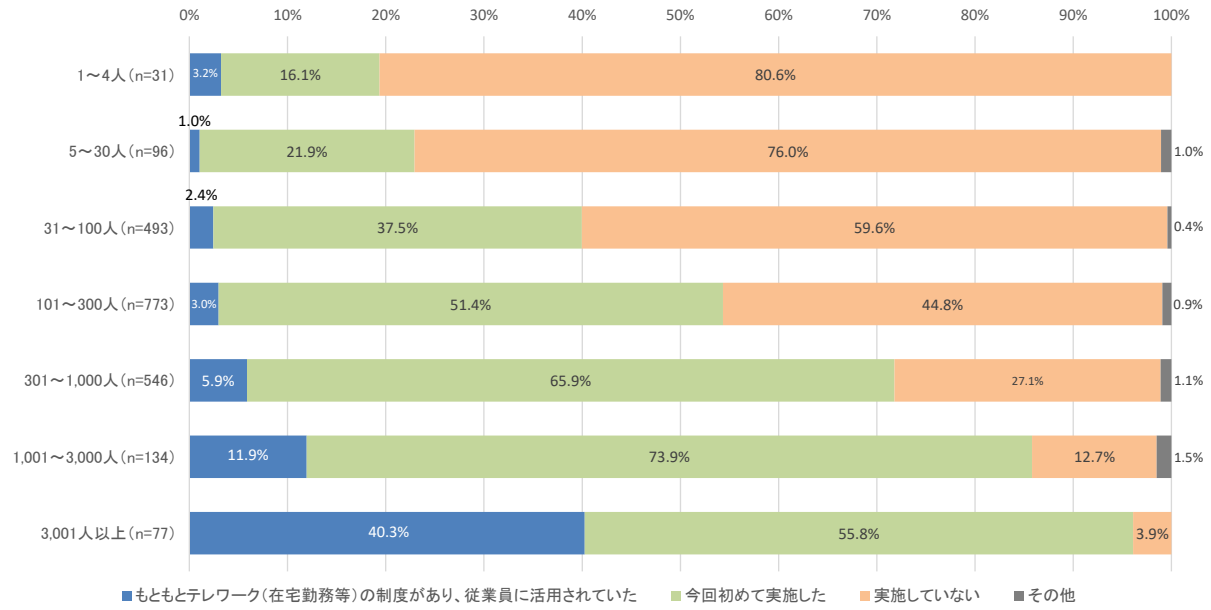

図 2.2-104　テレワーク（在宅勤務等）の実施状況（規模別クロス集計）

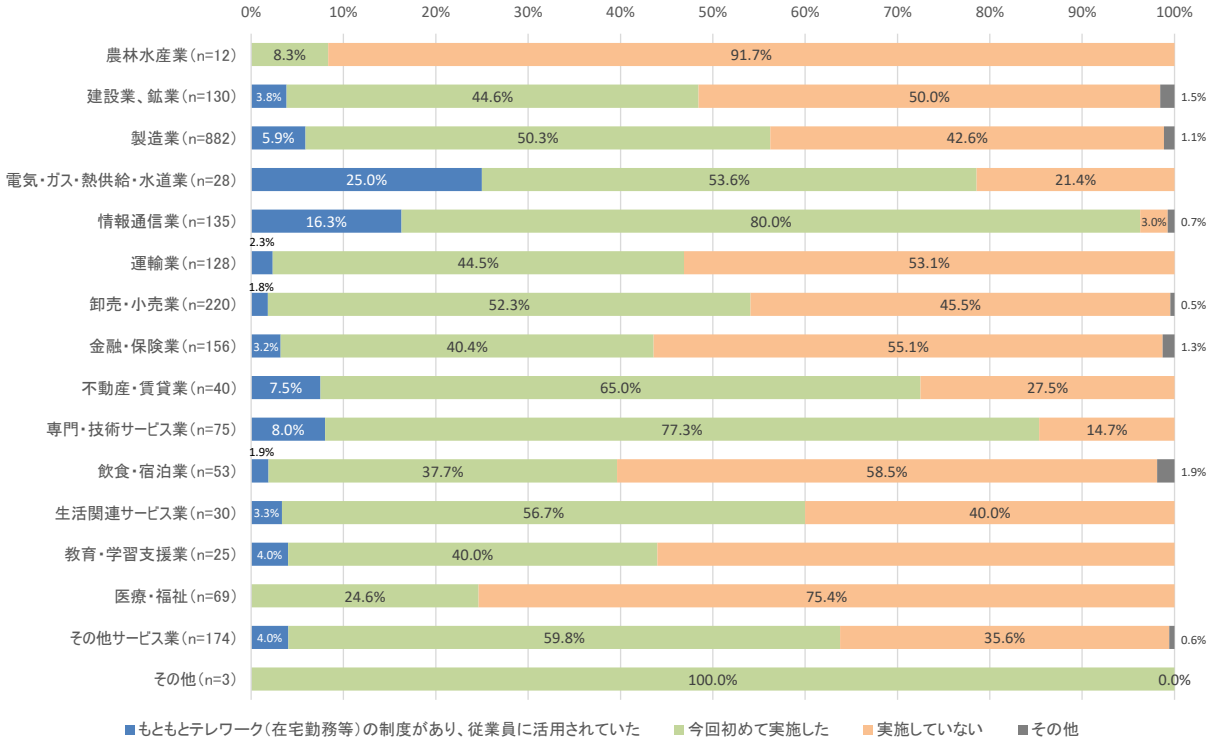

図 2.2-105　テレワーク（在宅勤務等）の実施状況（業種別クロス集計）

(2)　テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況

前問でテレワーク等を実施していると回答した企業に対し、テレワーク等の環境で営業秘密を扱う場合の対策として、職場向けとは別にルール等を定めたかどうかを尋ねた結果を示す。

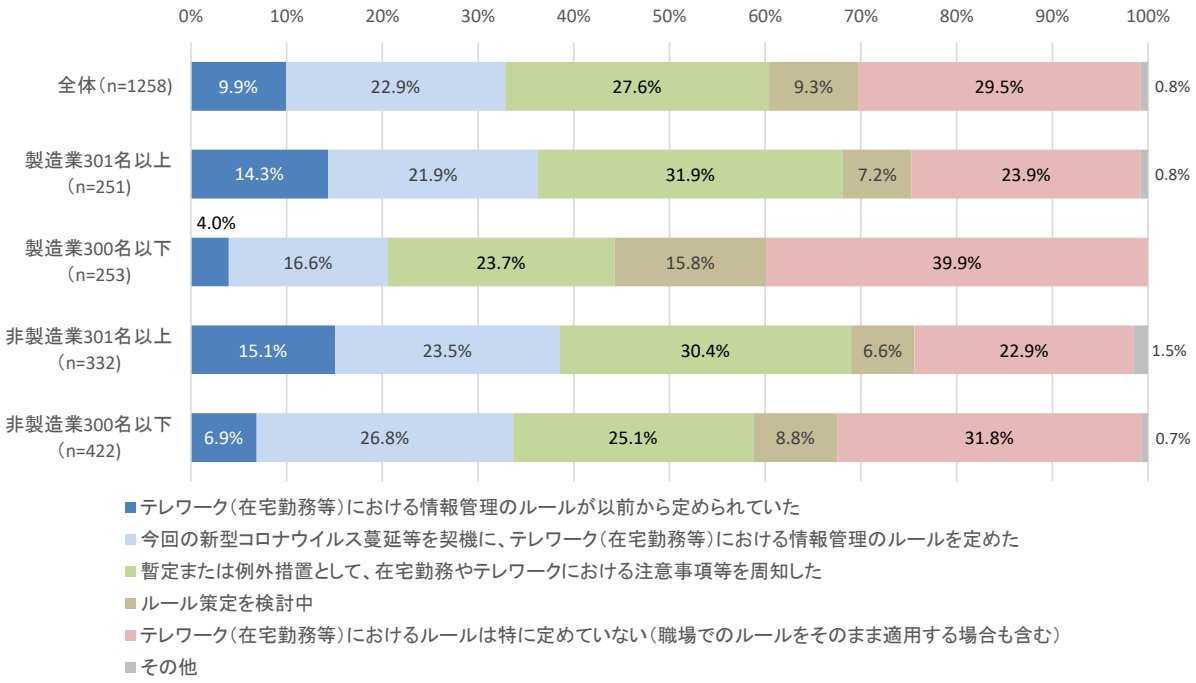

図 2.2-106　テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況
（業種・規模別４区分によるクロス集計）

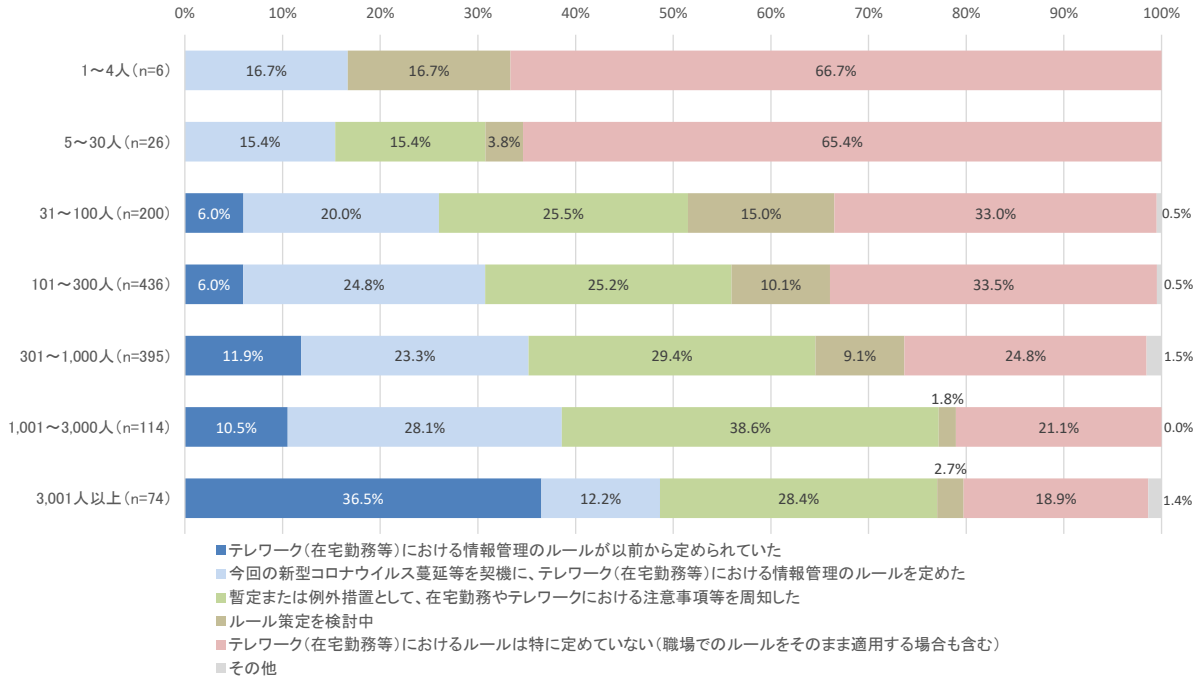

図 2.2-107　テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況
（規模別クロス集計）

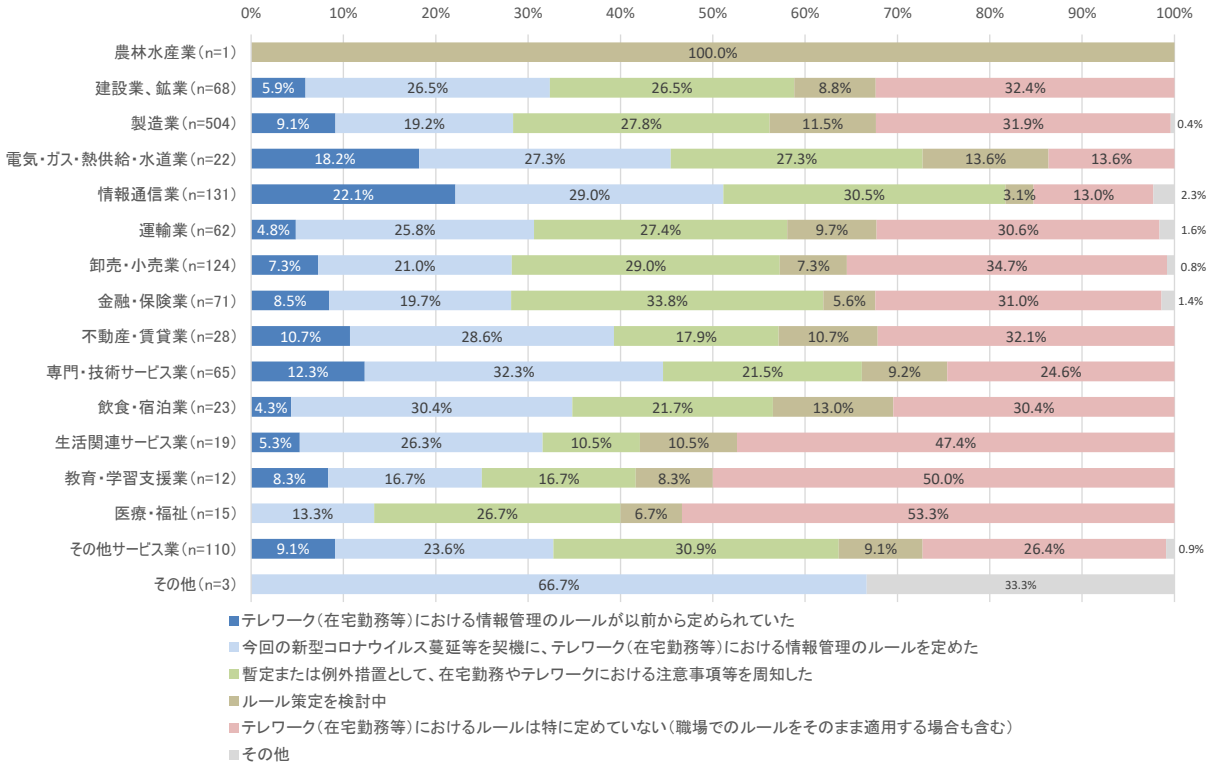

図 2.2-108　テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況（業種別クロス集計）

(3) テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の具体的内容

① 目的別対策の導入状況

前問でテレワーク等に関して何らかのルール等を整備していると回答した企業に対し、テレワーク等の環境で営業秘密を扱う場合のルールの具体的内容について尋ねた結果を示す。

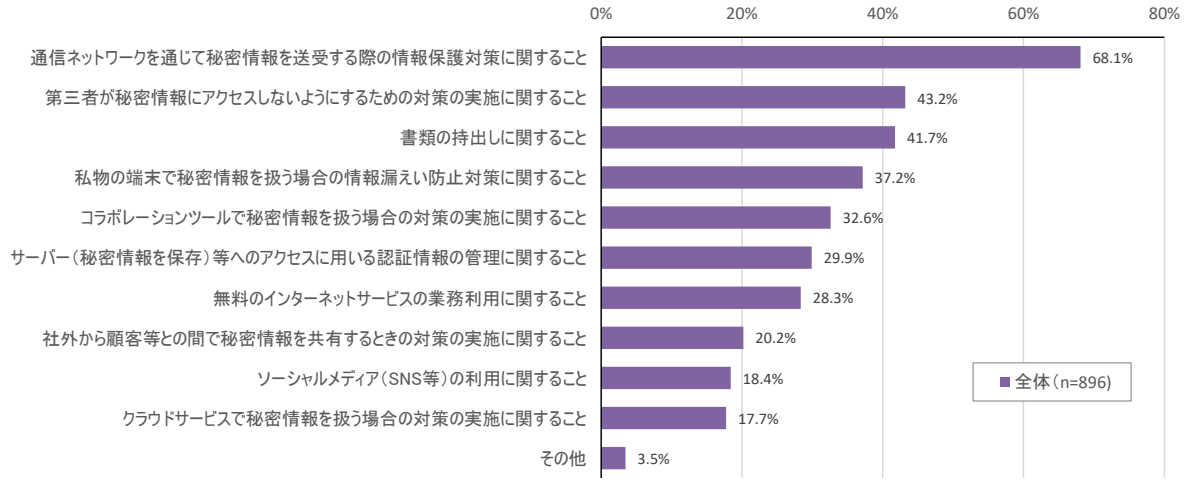

図 2.2-109　テレワーク（在宅勤務等）で営業秘密を扱う場合の目的別対策の導入状況

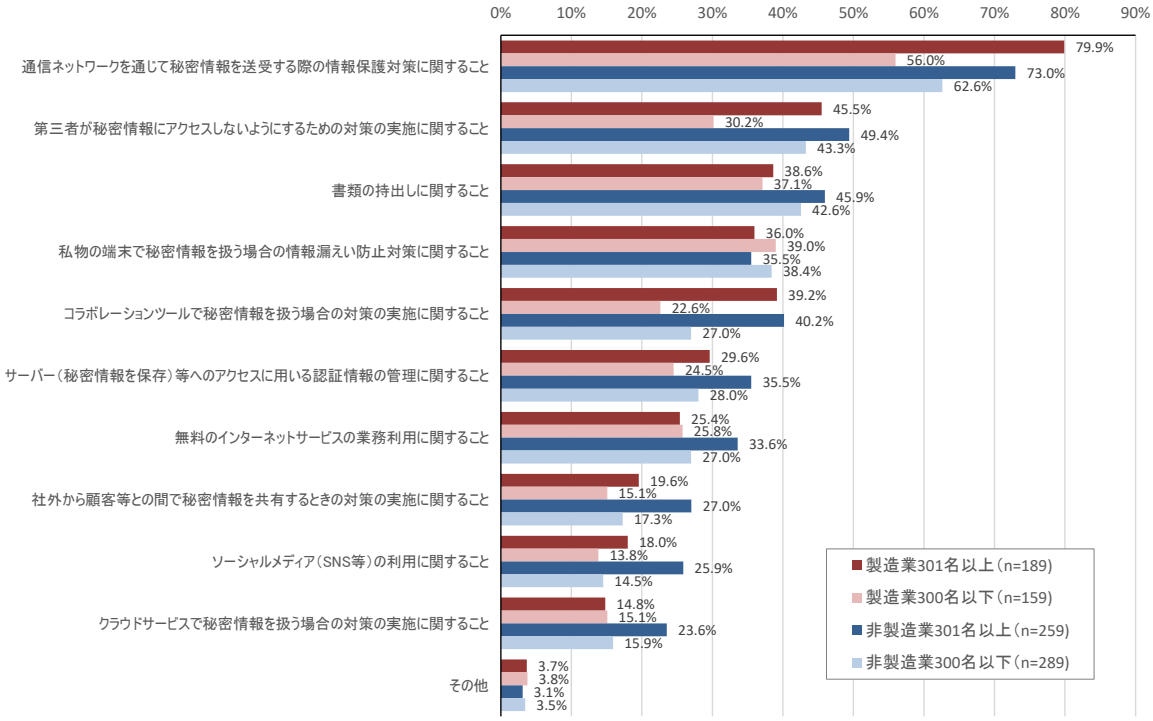

図 2.2-110　テレワーク（在宅勤務等）で営業秘密を扱う場合の目的別対策の導入状況
（業種・規模別４区分によるクロス集計）

② 具体的ルールの回答例

具体的なルールとして、次のようなものが回答されている。

- テレワーク環境からの接続は VPN 経由
- ローカル環境へのデータ保存の禁止又は制限
- 私物端末の利用禁止
- テレワークに用いる私物端末の許可制
- 私物端末を用いたテレワークで利用可能な業務の制限
- リモートデスクトップ（シンクライアント）によるアクセスに限定
- 公共 Wi-Fi の利用制限
- 利用可能なネットワークの限定
- テレワークを行う場所を自宅に限定
- テレワークが可能な場所の限定又は制限
- 企業が支給する PC の持出に係る誓約書の徴求
- 同居する家族からの営業秘密の保護、情報管理への協力依頼
- 自宅等でビデオ会議を行う場合の音声経由での情報漏えい防止策
- 画面ののぞき見防止策
- SNS の利用制限
- 自宅プリンタの利用制限
- 書類の持ち出し禁止または制限

- シャドークラウドの利用禁止
- クラウドサービス利用の許可制
- ２段階認証の必須化
- 認証情報の適切な管理
- PC 等貸与機器の紛失時のルール
- アクセス履歴のモニタリング
- テレワーク環境での ISMS ルールの遵守
- 総務省「テレワークセキュリティガイドライン」に基づくルール策定

(4) テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識

テレワーク等の実践を通じて、営業秘密漏えいのリスクは増大していると考えるかどうかについて尋ねた結果を示す。このとき、自社で定めた対策が遵守されていることを前提としている。

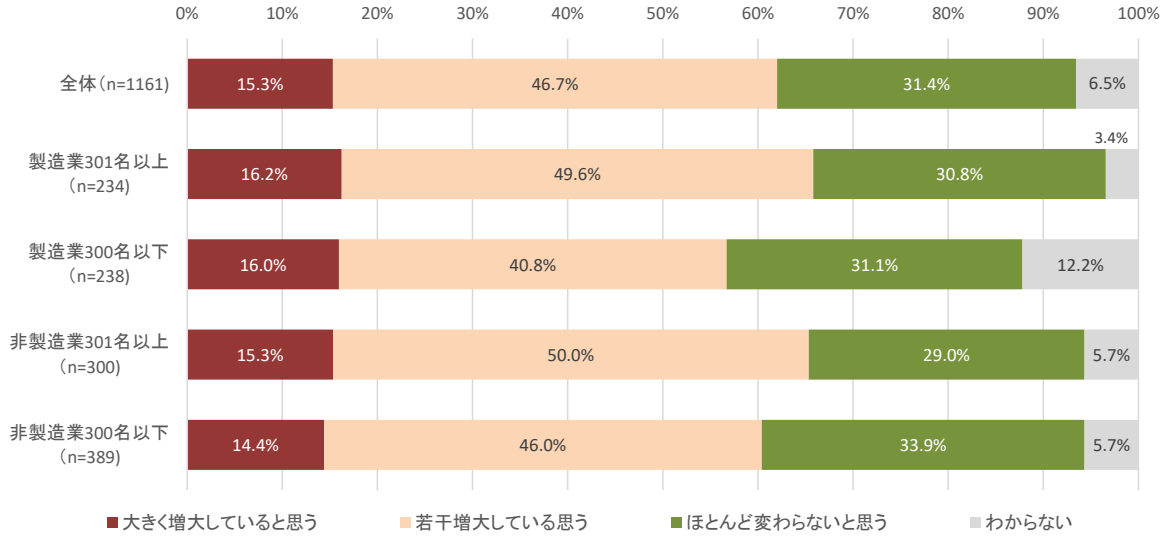

図 2.2-111　テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識（業種・規模別４区分によるクロス集計）

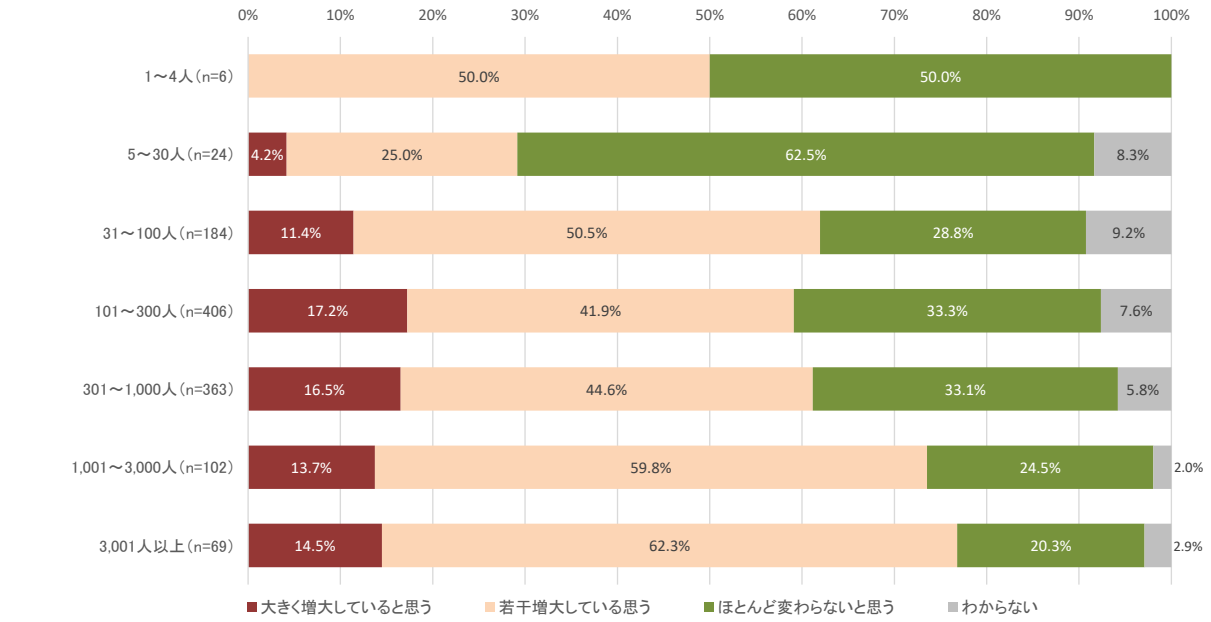

図 2.2-112　テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識（規模別クロス集計）

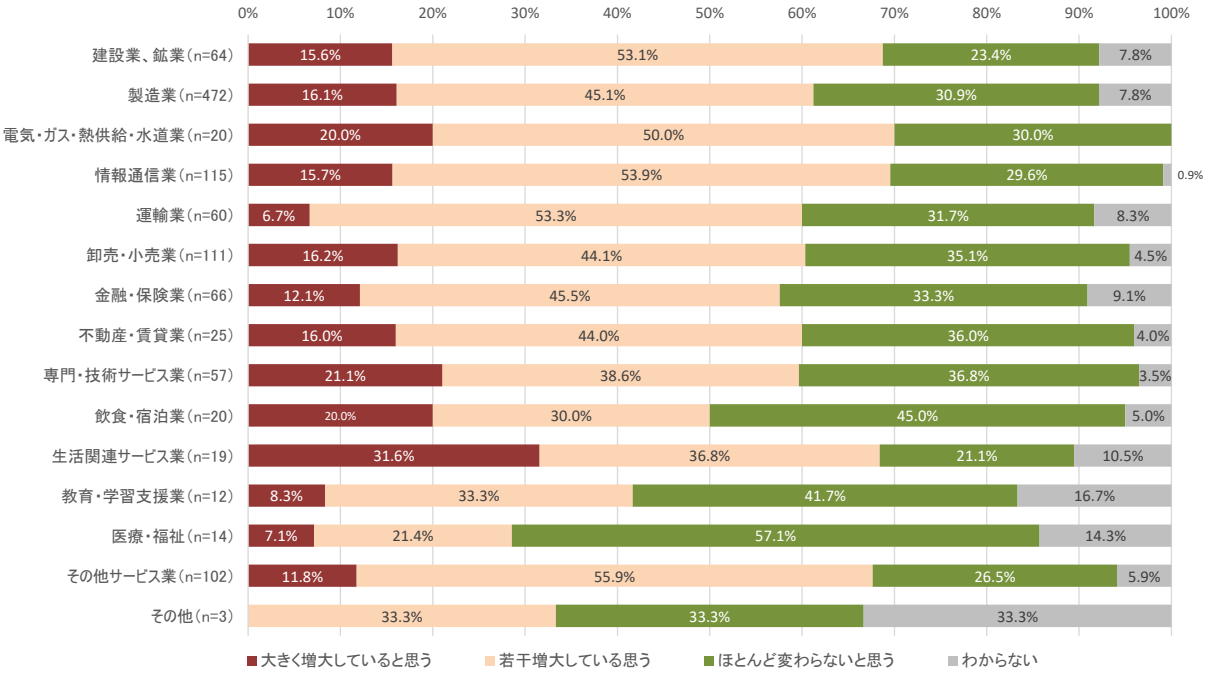

図 2.2-113　テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識（業種別クロス集計）

(5)　営業秘密管理の観点から今後必要と考える取組

ウィズコロナ・ポストコロナ等の自社をとりまく環境変化を踏まえ、営業秘密管理の観点から今後どのような取組が必要と考えているかについて尋ねた結果を示す。

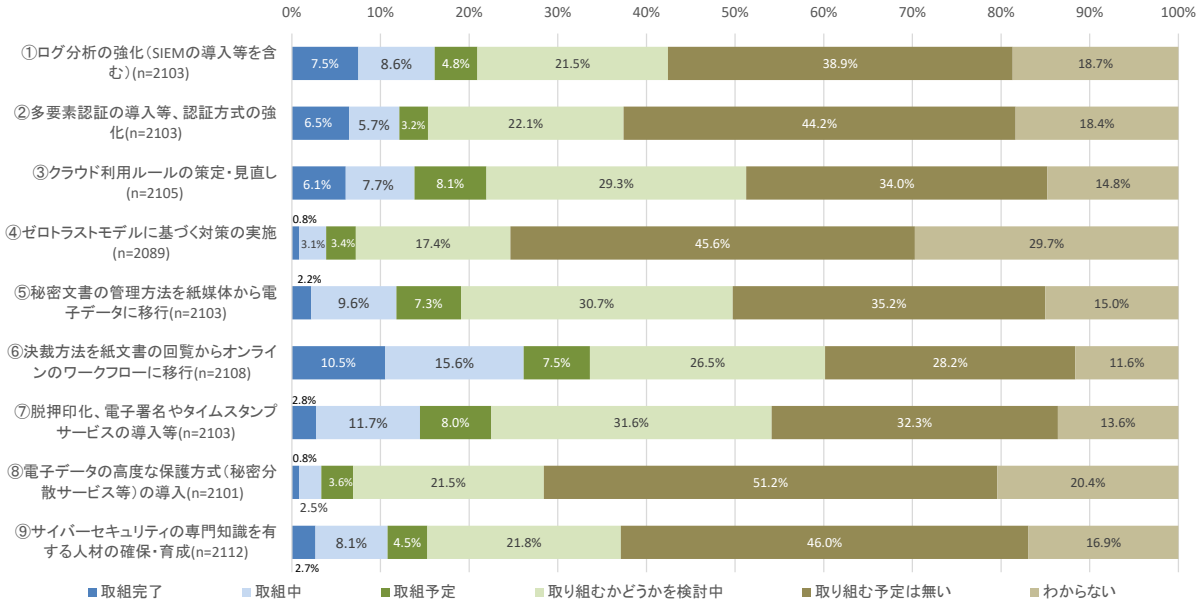

図 2.2-114　営業秘密管理の観点から今後必要と考える取組（全体）

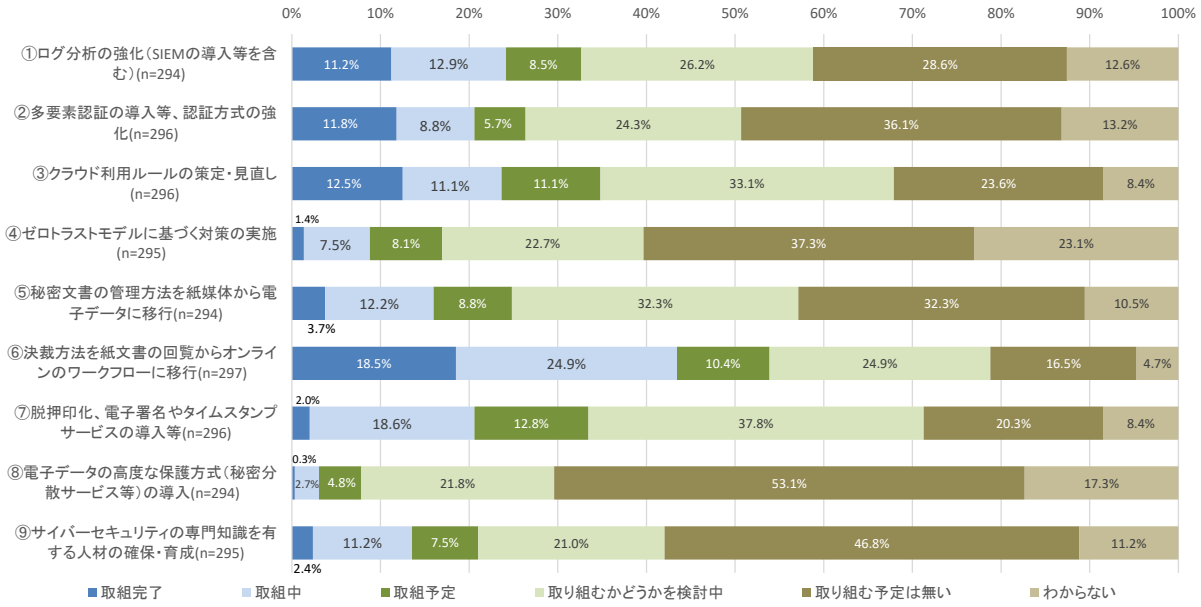

図 2.2-115　営業秘密管理の観点から今後必要と考える取組（大規模製造業）

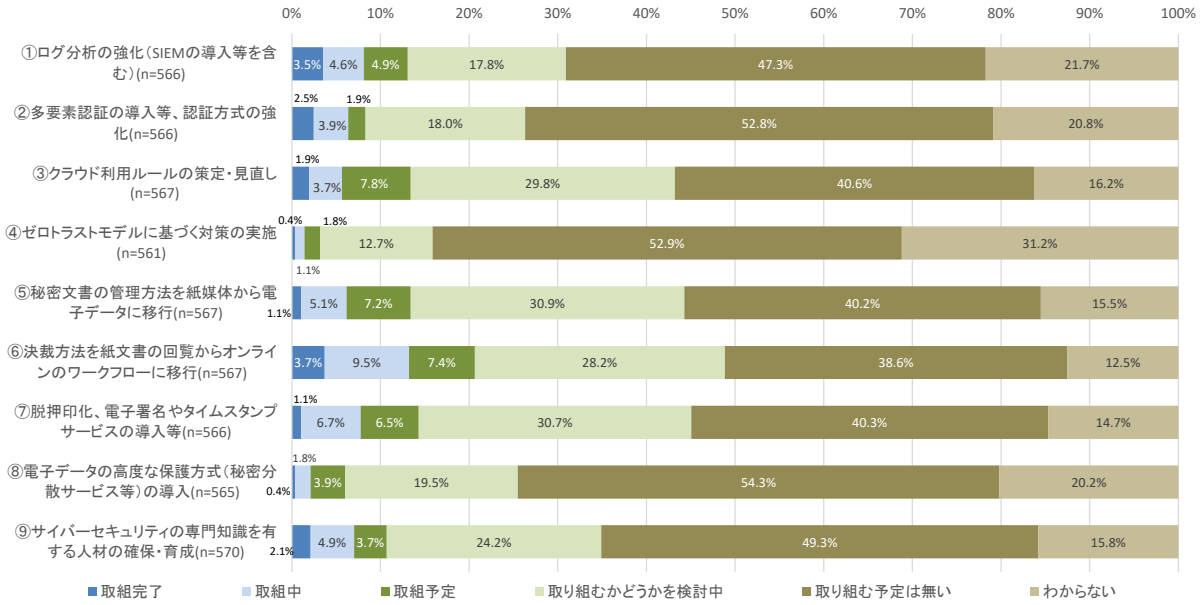

図 2.2-116　営業秘密管理の観点から今後必要と考える取組（中小規模製造業）

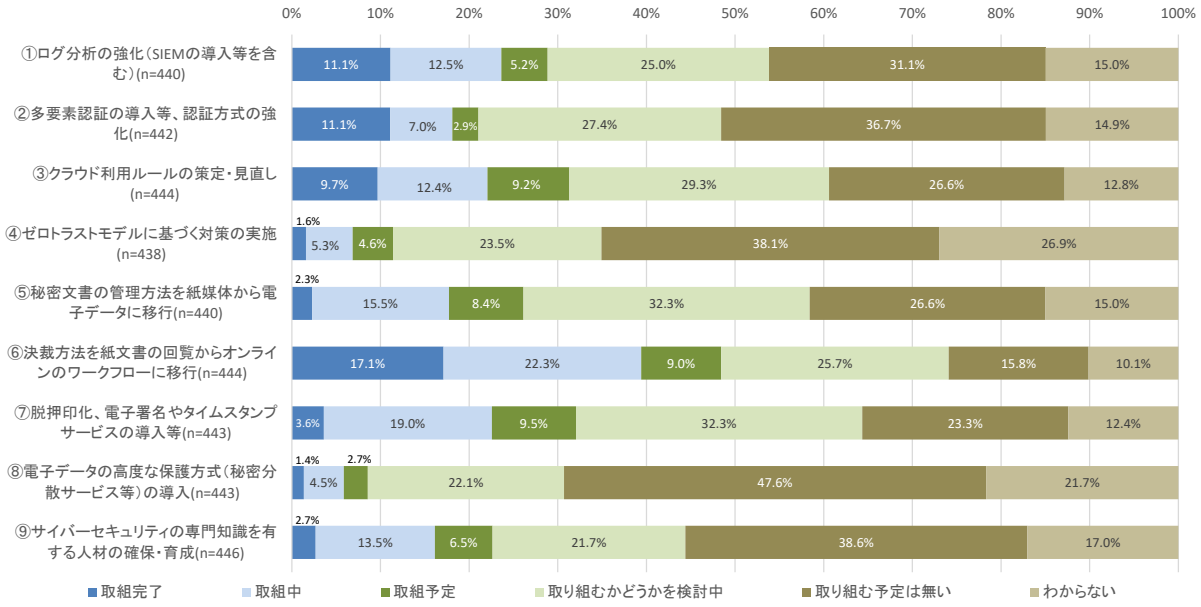

図 2.2-117　営業秘密管理の観点から今後必要と考える取組（大規模非製造業）

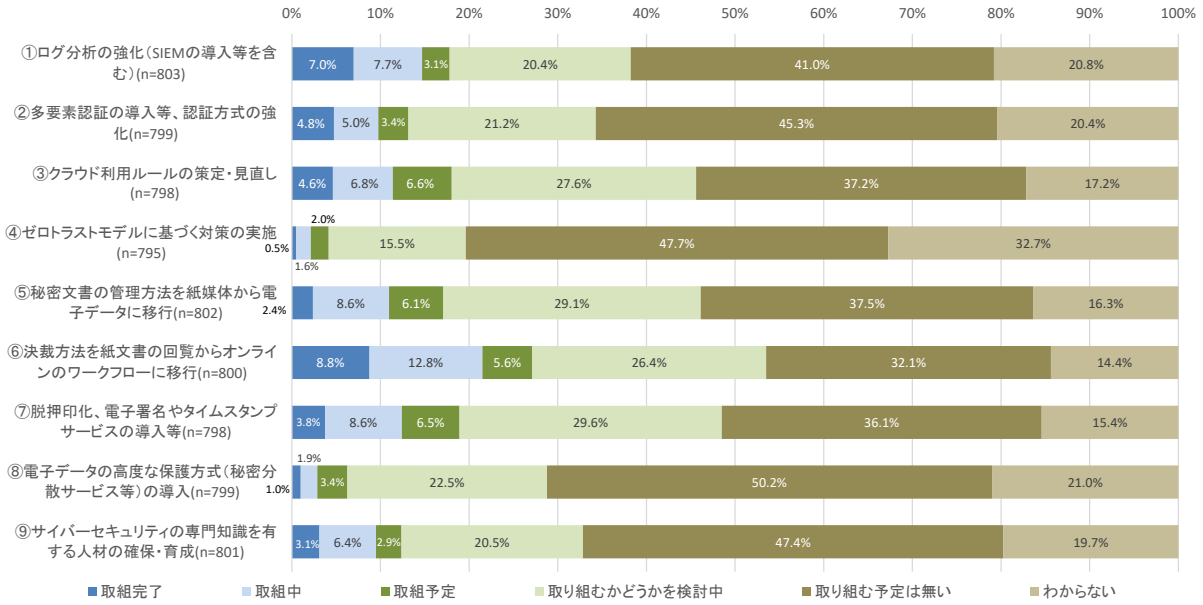

図 2.2-118　営業秘密管理の観点から今後必要と考える取組（中小規模非製造業）

2.2.4.6　その他の質問

(1)　「秘密情報の保護ハンドブック」の認知及び活用状況

経済産業省が 2016 年に公表した「秘密情報の保護ハンドブック」について、自社の対策における参考として利用した経験について尋ねた結果を示す。2016 年度調査と比較すると、ハンドブックに関する認知度はほとんど向上していないながら、活用経験のある企業は着実に増加している。

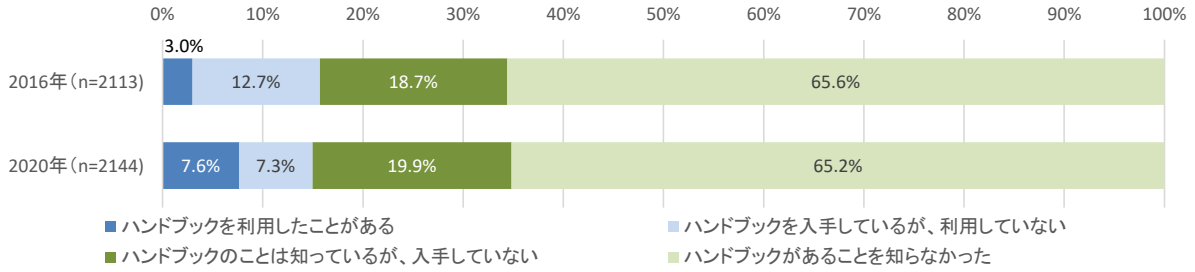

図 2.2-119　「秘密情報の保護ハンドブック」の認知及び活用状況（経年比較）

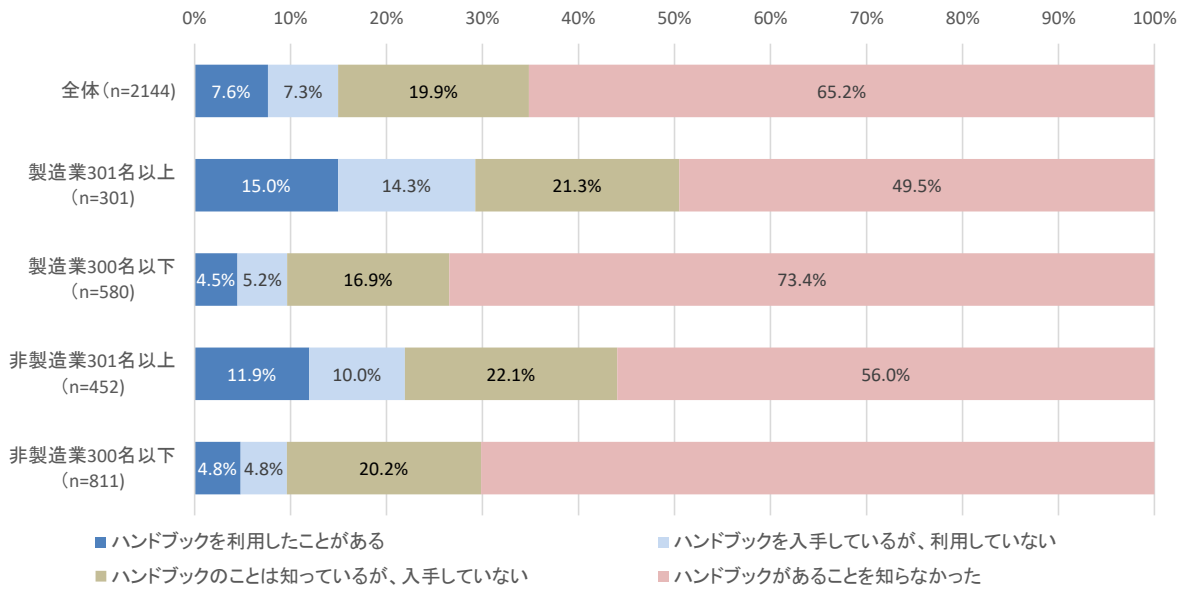

図 2.2-120　「秘密情報の保護ハンドブック」の認知及び活用状況
（業種・規模別４区分によるクロス集計）

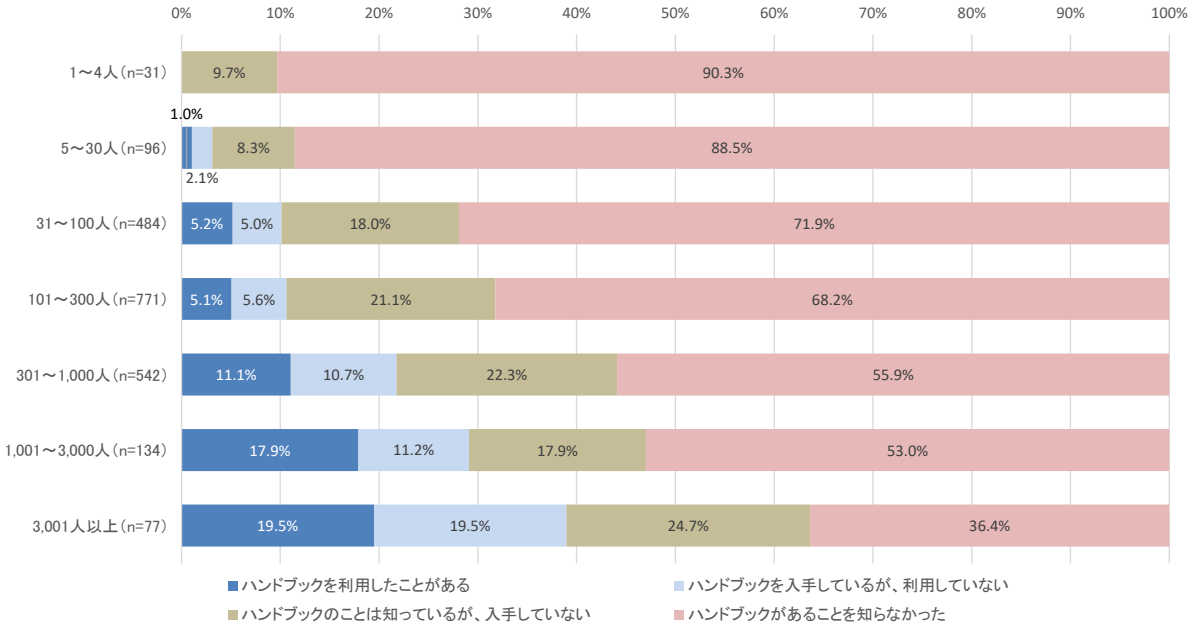

図 2.2-121　「秘密情報の保護ハンドブック」の認知及び活用状況
（規模別クロス集計）

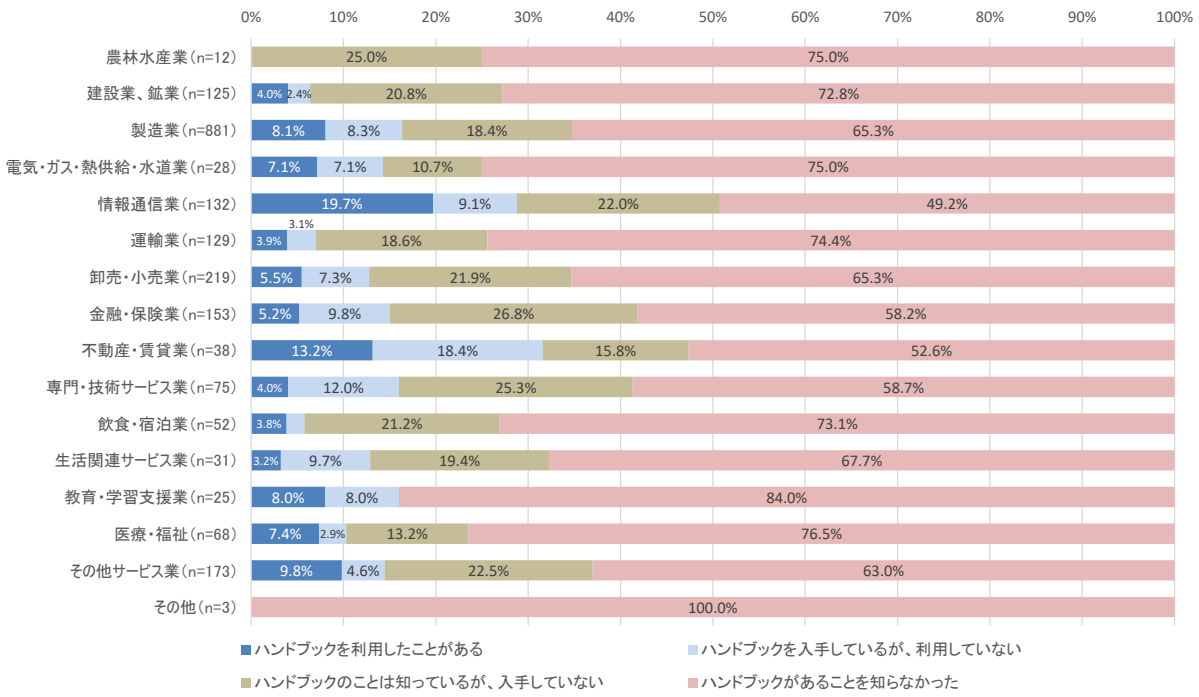

図 2.2-122　「秘密情報の保護ハンドブック」の認知及び活用状況
（業種別クロス集計）

(2)　「秘密情報の保護ハンドブック」の今後の改訂で実施して欲しい内容

前問で「ハンドブックを利用したことがある」と回答した企業に対し、今後の改訂で実施してほしいと考える内容について尋ねた結果を示す。

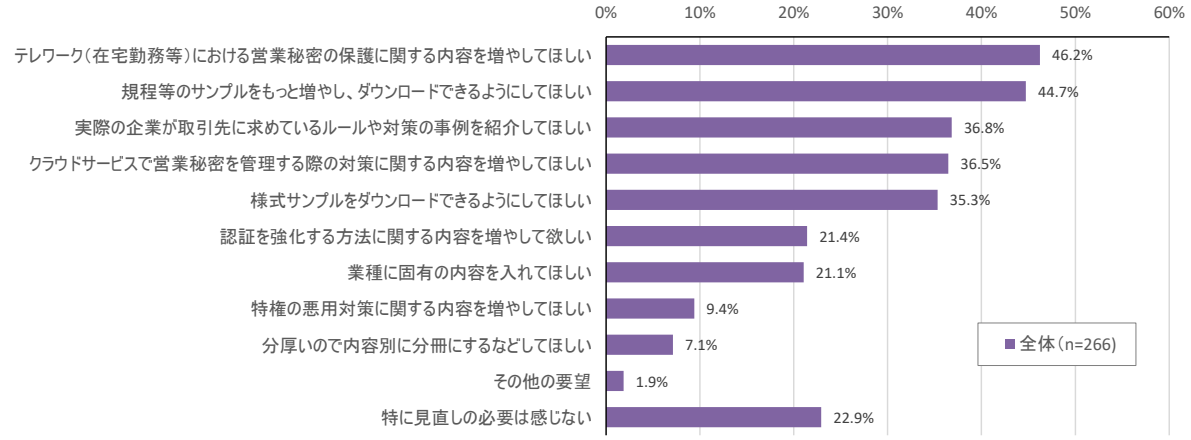

図 2.2-123　「秘密情報の保護ハンドブック」の今後の改訂で実施して欲しい内容

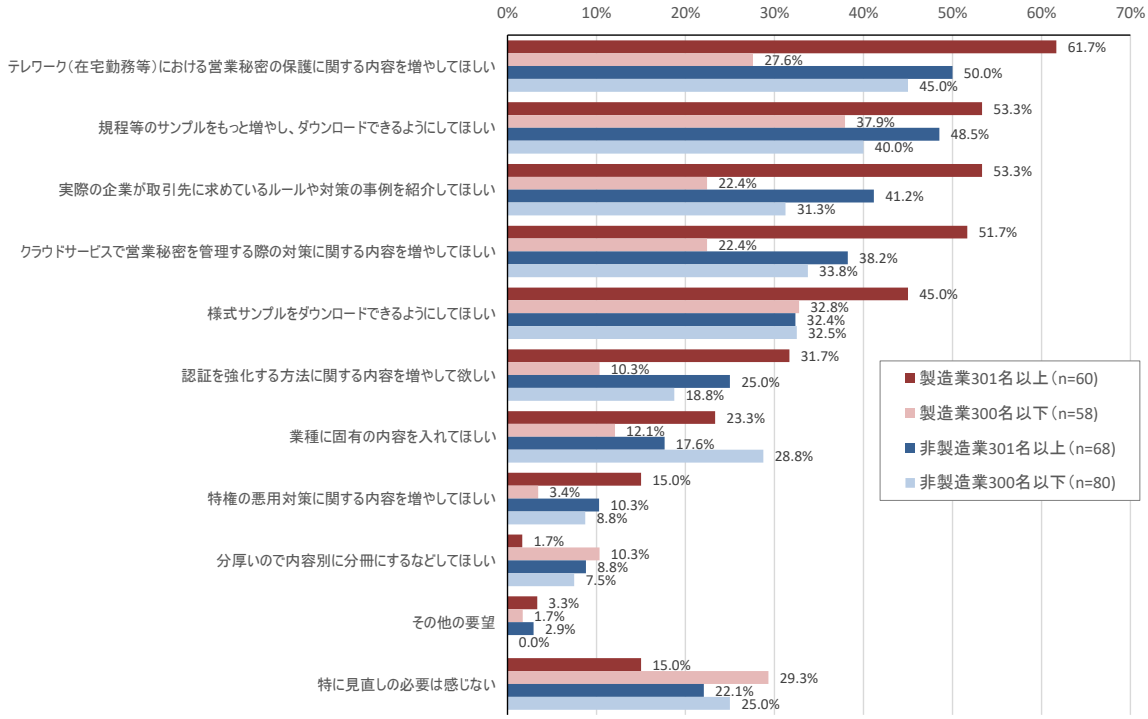

図 2.2-124　「秘密情報の保護ハンドブック」の今後の改訂で実施して欲しい内容
（業種・規模別４区分によるクロス集計）

(3) その他のご意見、ご要望等

自由回答形式にて、意見・要望を尋ねた。このうち、今回は紙媒体の調査票を郵送にて送付・回収する方法に限定して実施したことから、オンラインで回答できるようにしてほしいとの要望が多数示されている。そのほか回答例の一部を以下に示す。

- 最初は回答するのが面倒だと思ったが、答えているうちに分からないことが出てきて調べることで勉強になりました。今後は協力していきたいと思います。
- 規模が小さい会社なので基本的には信頼をベースでやりたいと思っているが、お客様の事を考えると何かしらの策を考えないといけないと今回のアンケートで気付きました。ありがとうございました。
- 今回、シャドークラウドという言葉を初めて知りました。
- 現在まで秘密情報は特定の人間しか関っておらず、あまり意識してこなかったので、今後は、人員が増えるに従って考えていかなければならないと思った。
- 対策の必要性を感じましたので、今後検討していきます。
- 質問によって対策の打つ手が少ないことに気づかされました。他、特にございません。
- 「秘密情報の保護ハンドブック」を活用させていただきます。
- 是非ハンドブックを参考にしたいと思います。
- 情報セキュリティの啓発や地域にて研修会開催を希望
- 指針、方針説明会（Web）実施してほしい。
- テレワーク、クラウド利用に関する秘密情報管理の対策を増やしてもらいたい

- 昨今なりすましメール、マルウェア Emotet の感染事例が急増しており、その対策について何か情報あれば伺いたいところです。
- トピックス、最新の情報を提供願いたい。
- セミナーがあれば参加したい
- シン・テレワークシステムを活用しております。大変助かっております。
- テレワークやモバイルワークの利用が増え、情報へのアクセスがあたりまえとなり、情報セキュリティの３要素が可用性＞機密性＞完全性というバランスになり、個人情報保護や情報セキュリティよりも生命・財産の保護が大切なのもわかるが、軽んじられている気がしてならない。
- ICT の進展により、情報セキュリティに対する脅威が増大する中で、情報セキュリティ確保のための人材確保やシステム導入が困難な状況となっている。よって、これら企業の指導・サポートが望まれる。
- セキュリティ保護の重要性は認識しているが、どこまで取組めば良いのか判断ができない。
- 問 41 のハンドブックを入手し、自社のセキュリティに活用したいと思います
- どこまでやるべきかの判断は難しい

2.2.5 情報管理に関する成熟度に基づく分析

2.2.5.1 「情報管理に関する成熟度」の定義

営業秘密を含む秘密情報の管理においては、管理体制や規程・手続等の整備、対策の検討・導入・運用、実践状況の確認と見直し等の一連の取組が適切に組み合わされて実施される必要がある。そこで、これらの取組について尋ねている複数の質問をもとに「情報管理に関する成熟度」を下図のように定義し、この成熟度の値をもとにこれまで示した質問についてのクロス集計を行うことで、企業における営業秘密管理の実態と成熟度の関係について分析した。

下表における点数付けの根拠は次の通りである。

- 国内企業の平均的な取組状況と比較して、優れた段階に位置付けられる対策を実施：2 点
- 前項には達しないものの、一定の効果のある対策を実施：1 点
- 「わからない」もしくは中立的な選択肢の場合：0 点
- 情報管理に関する個別の取組が実施されていない：-1 点
- 情報管理に関する基本的な取組が実施されていない：-2 点

成熟度判定に用いた質問

質問内容	選択肢	点数
2.2.4.3 (1) 営業秘密の区分管理状況	レベル区分している	2
	秘密かどうかのみ区分	1
	わからない	0
	区分なし	-2
2.2.4.3 (2) 営業秘密管理の運用実態	厳密な運用を徹底、ある程度厳密	2
	改善の途上	1
	厳密とは言えない、ルールのみ	0
	わからない	0
2.2.4.4 (10) サプライチェーンにおける営業秘密管理把握状況	把握していない	-1
	相手がいない	0
	把握のみ	1
	把握＋再委託時の条件提示	2
	再委託先も管理	3
2.2.4.4 (14) 秘密情報漏えい時の組織体制	経営層のリーダーシップ、特定部署主導	2
	部署毎	1
	その他、特にない	0
2.2.4.4 (18) 格付けや取扱の見直しの目標	見直しを行っていない	-1
	区分管理の徹底	1
	合理的管理、継続改善、分離管理	2

総和

成熟度別企業数

合計	区分	企業数
5以上	成熟度高	702
0～4	成熟度中	841
-1以下	成熟度低	631

図 2.2-125 本調査における「情報管理に関する成熟度」の定義

2.2.5.2 「情報管理に関する成熟度」に基づく比較分析

(1) 業種との関係

次図に、回答企業の業種別に成熟度の構成比を整理した結果を示す。全業種の中で最も成熟度高の比率が高いのは情報通信業、逆に低いのが農林水産業と教育・学習支援業である。

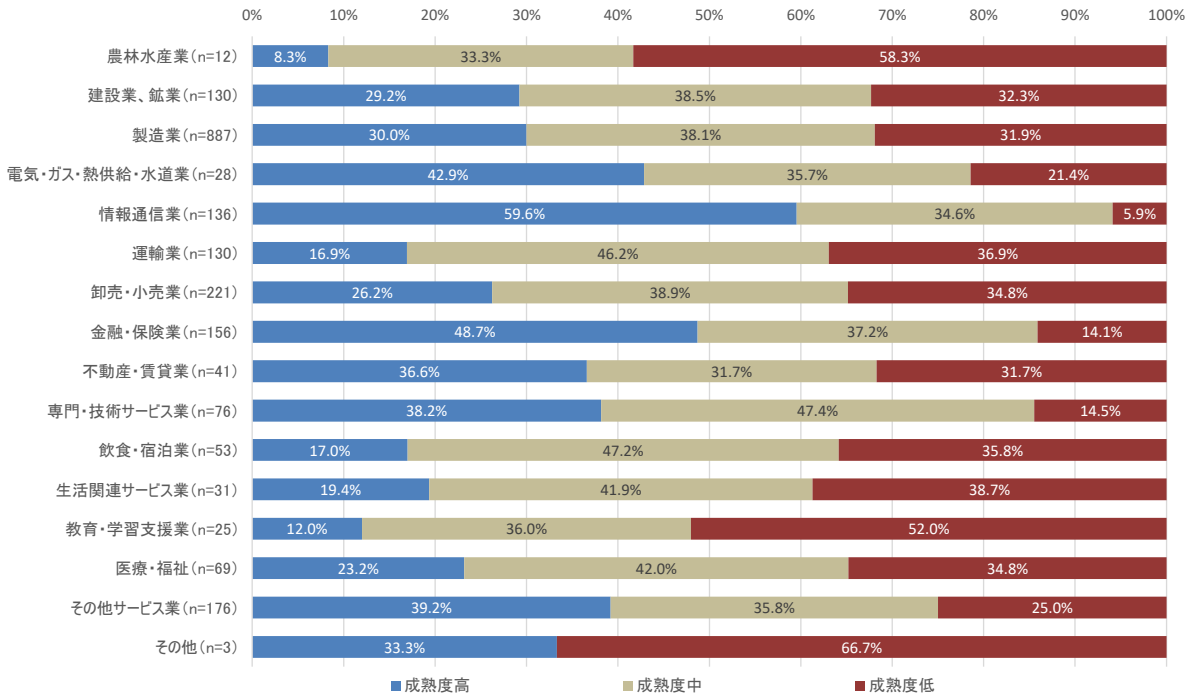

図 2.2-126　情報管理に関する成熟度と業種との関係

(2) 企業規模との関係

次図に、回答企業の従業員数ベースの企業規模と成熟度の関係を整理した結果を示す。情報管理に関する成熟度と企業規模は完全な正相関の関係にあるが、零細を除く中小規模企業でも一定比率で成熟度高の企業があり、超大手の企業でもわずかながら成熟度低の企業があることがわかる。

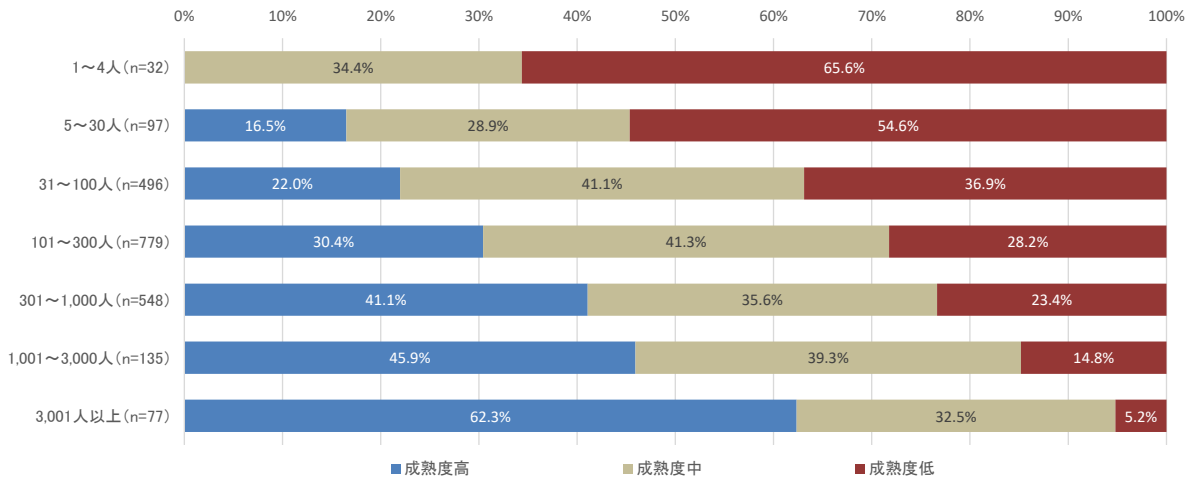

図 2.2-127　情報管理に関する成熟度と企業規模との関係

(3) 営業秘密漏えいの発生状況

次図に、営業秘密漏えいの発生状況に関する成熟度に基づくクロス集計結果を示す。漏えい事例の発生比率は情報管理に関する成熟度と相関しないが、「わからない」の比率から、成熟度が高

くなるほど漏えいの有無等の実態を把握できていることが推察される。

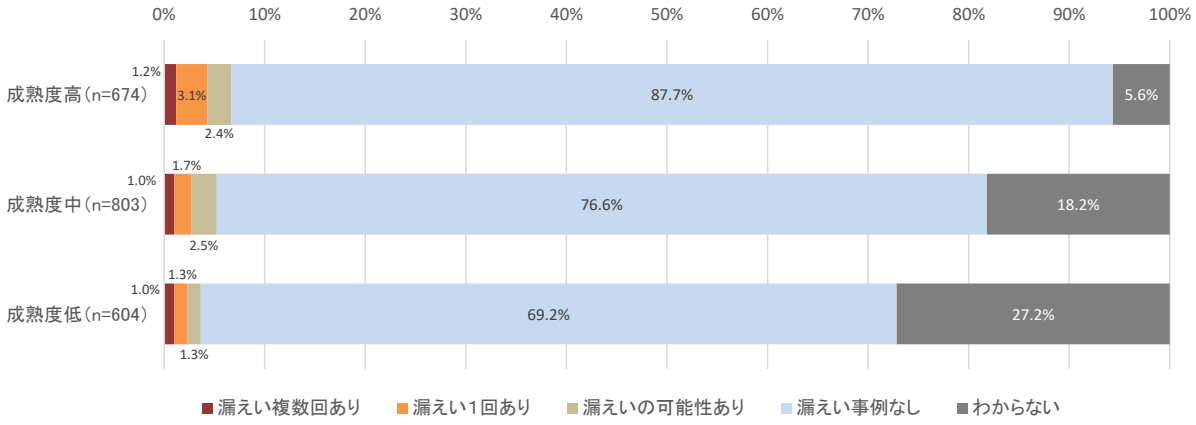

図 2.2-128　営業秘密漏えいの発生状況（成熟度別クロス集計）

(4) 対策が必要と考えている脅威

次図に、企業において対策が必要と考えている脅威に関する成熟度に基づくクロス集計結果を示す。このとき、情報管理に関する成熟度毎に重視している脅威が異なることが注目される。成熟度高の企業の場合は「外部からの標的型攻撃」「新たな環境において営業秘密を扱うこと」など未知の要素を含む脅威に関するもの、成熟度中の企業の場合は「体制不備やスキル不足」など現在改善しようと考えている内容、そして成熟度低の企業の場合は「ルールの不備」などそもそも情報管理を行うための体制や仕組みが未整備であることによるものも上位に位置付けられており、情報管理に関する組織としての成熟度をそのまま反映した結果となっている。

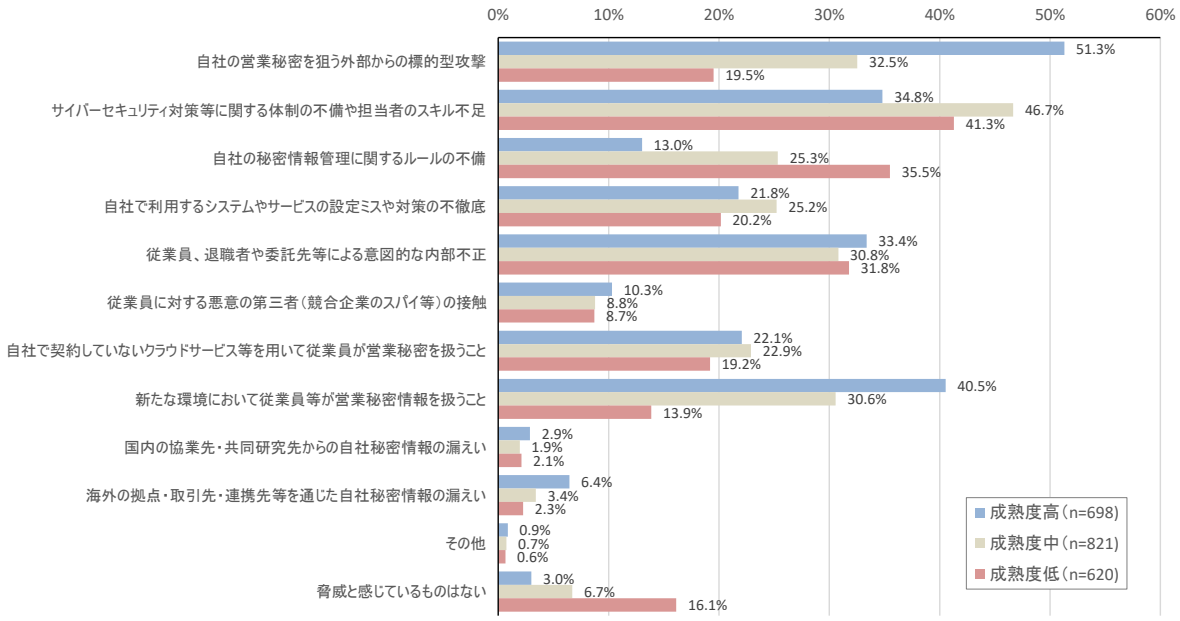

図 2.2-129　営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているもの（成熟度別クロス集計）

(5) 対策実践における課題

次図に、企業における対策実践における課題に関する成熟度に基づくクロス集計結果を示す。(4)と同様に、情報管理に関する成熟度の定義を反映した結果となっている。成熟度高の企業においては「対策コストが高額なこと」や「新たな業務環境における適切な対策の見極めができない」等、対策を実施した上での課題が選択されているのに対し、成熟度低の企業においては「従業員にルール遵守を徹底させることが難しい」といった対策に着手した時点で直面している課題が多く選択されている。

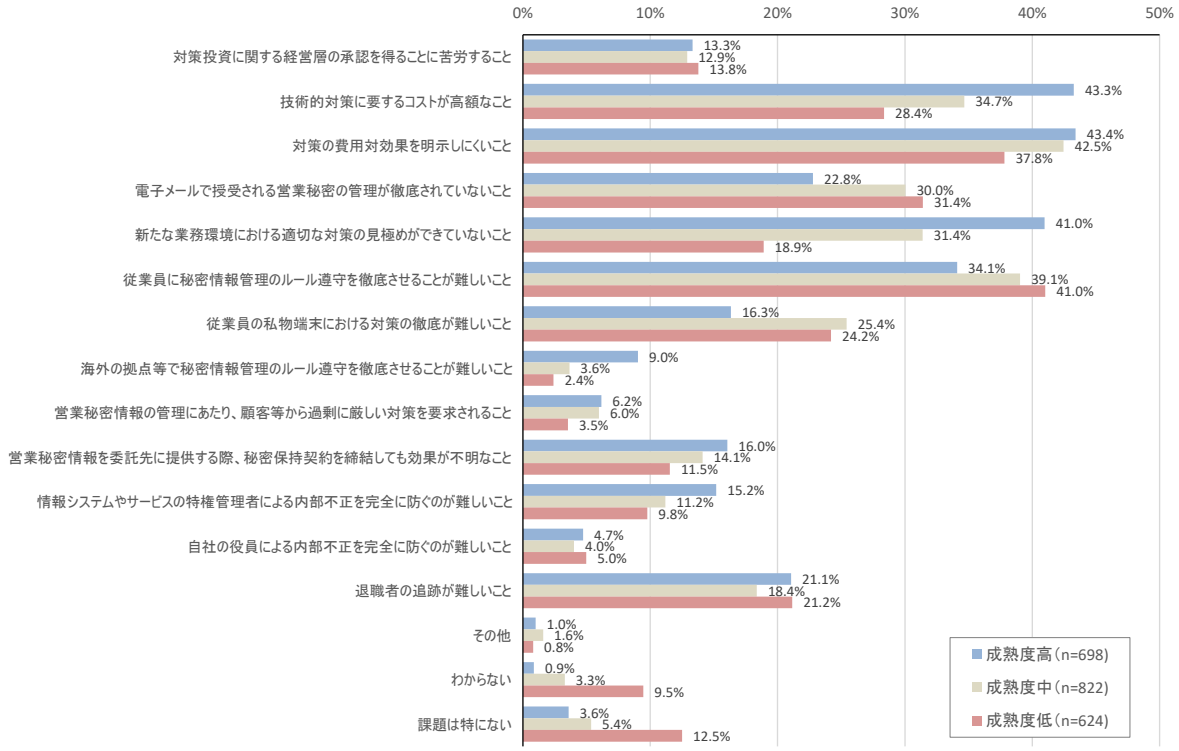

図 2.2-130　営業秘密の保護対策実践上の課題（成熟度別クロス集計）

(6) クラウドサービスを用いた営業秘密の共有状況

次図に、クラウドサービスを用いた営業秘密の共有状況に関する成熟度に基づくクロス集計結果を示す。本項はセキュリティ対策を問うものではないが、情報管理に関する成熟度が高い企業ほど、情報共有を積極的に行っていることがわかる。

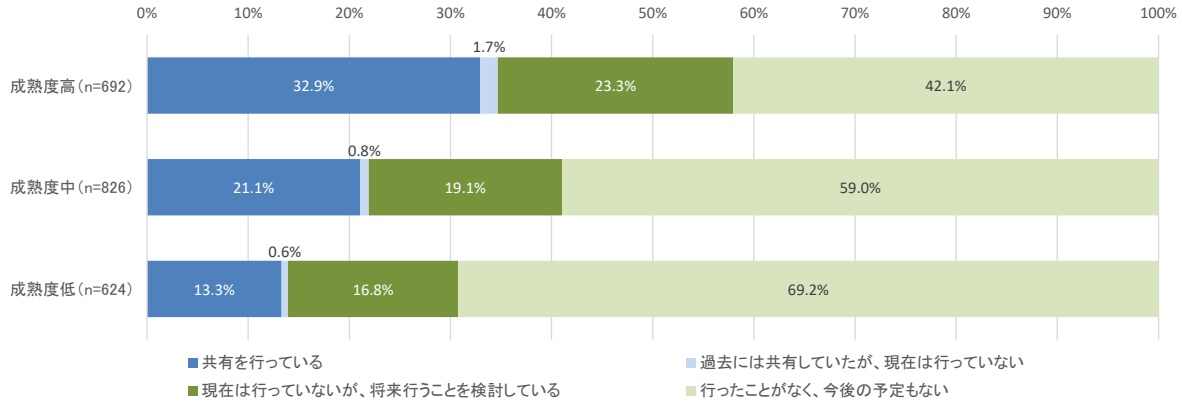

図 2.2-131　クラウドサービスを用いた営業秘密の共有状況（成熟度別クロス集計）

(7) クラウドサービスにおける営業秘密の不正利用防止のために実施している対策

次図に、クラウドサービスにおける営業秘密の不正利用防止のために実施している対策に関する成熟度に基づくクロス集計結果を示す。選択肢として挙げている対策のうち、高度なものほど成熟度による相違が拡大する傾向にあることがわかる。

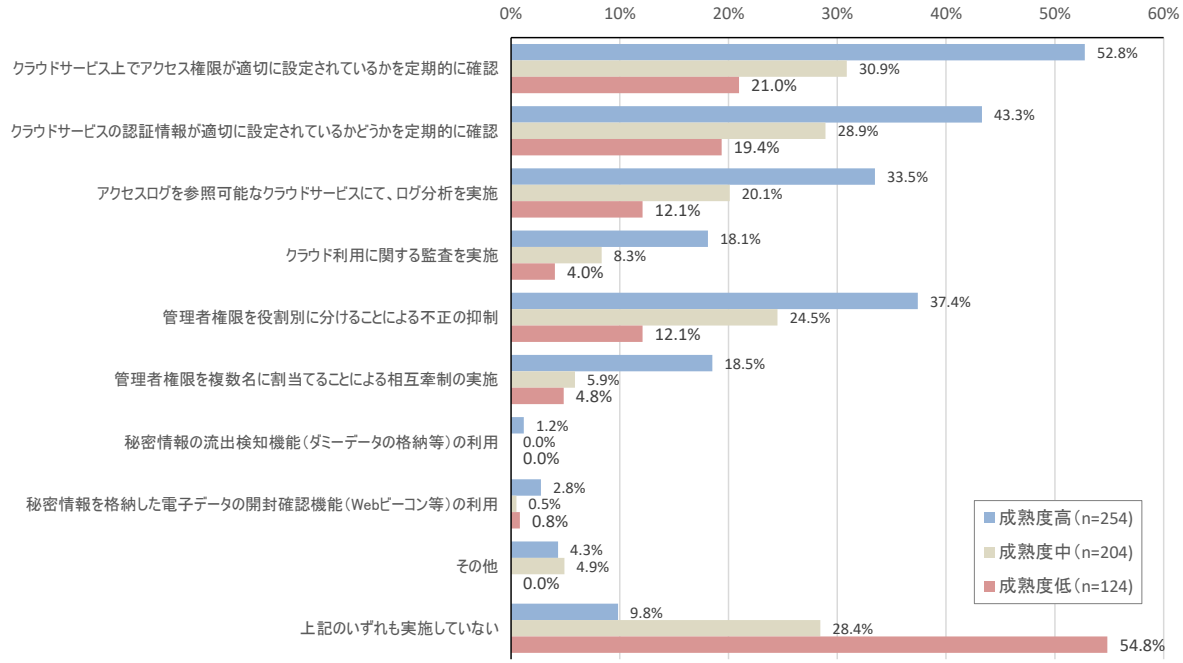

図 2.2-132　クラウドサービスにおける営業秘密の不正利用防止のために実施している対策（成熟度別クロス集計）

(8) シャドークラウドが生じることを防止する対策の実施状況

次図に、シャドークラウドが生じることを防止する対策の実施状況に関する成熟度に基づくクロス集計結果を示す。本項で扱うシャドークラウド対策の実施状況についても、情報管理に関する成熟度と完全な正相関の関係にあることがわかる。

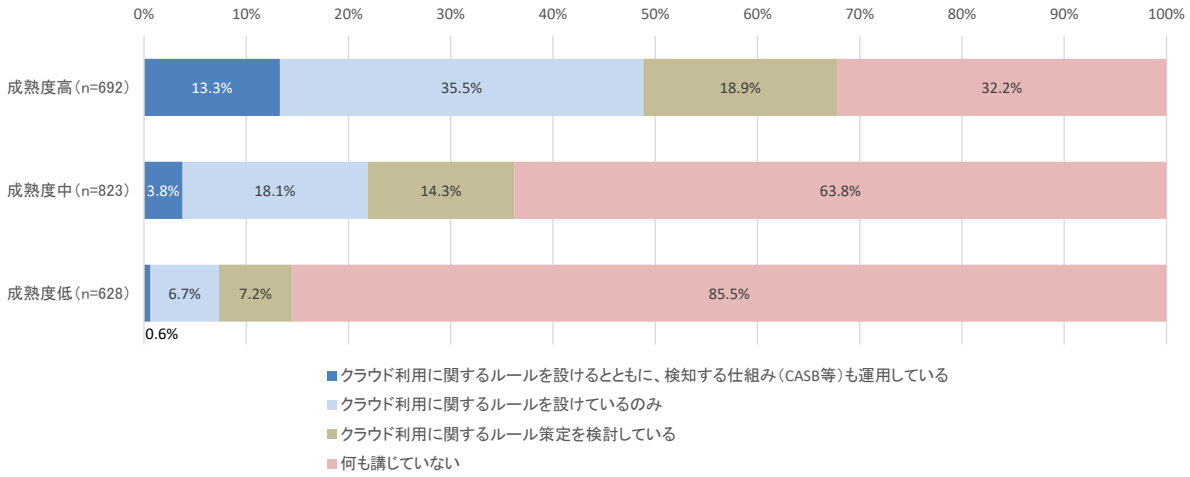

図 2.2-133　シャドークラウドが生じることを防止する対策の実施状況（成熟度別クロス集計）

(9) 情報管理に関する規程・手続等の見直しを行った目的や動機

次図に、情報管理に関する規程・手続等の見直しを行った目的や動機に関する成熟度に基づくクロス集計結果を示す。「経営層の指示」は成熟度に関わらず最も多く選択されている。一方で、成熟度が中ないし低の企業では、「社内からの提案・働きかけ」が相対的に多く選択されており、現場からのボトムアップでの提案を通じて対策が実施されているケースが多いことが推察される。

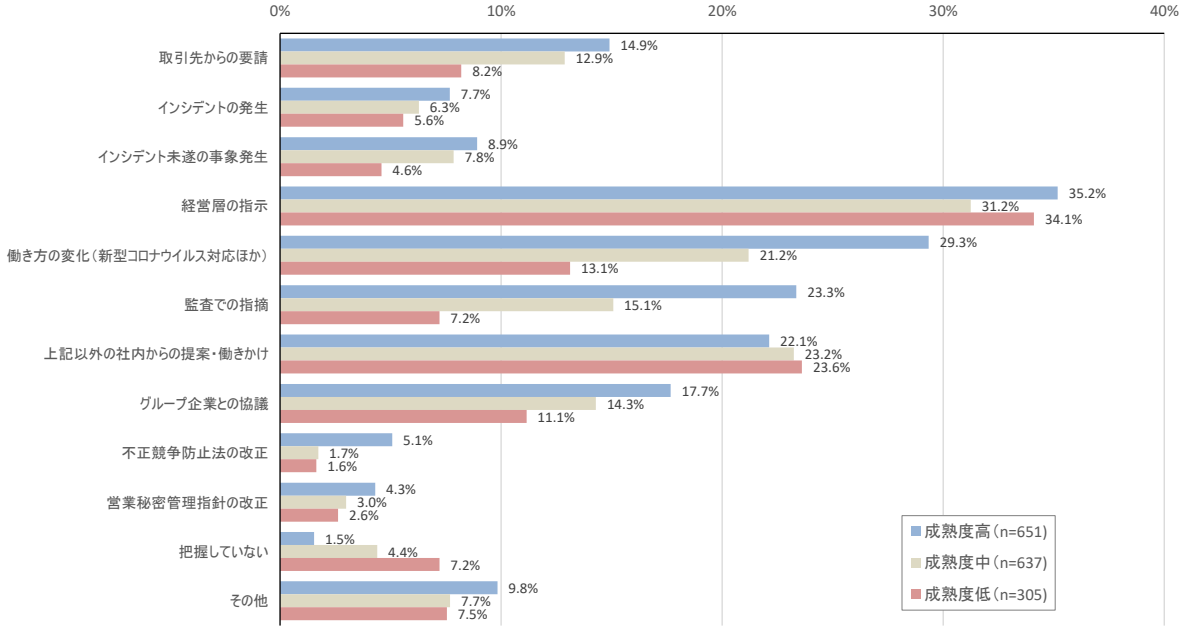

図 2.2-134　情報管理に関する規程・手続等の見直しを行った目的や動機（成熟度別クロス集計）

(10) テレワーク（在宅勤務等）の実施状況

次図に、テレワーク等の実施状況に関する成熟度に基づくクロス集計結果を示す。本項はセキュリティ対策を問うものではないが、(6)と同様、成熟度高の企業ほどテレワークを推進していることがわかる。

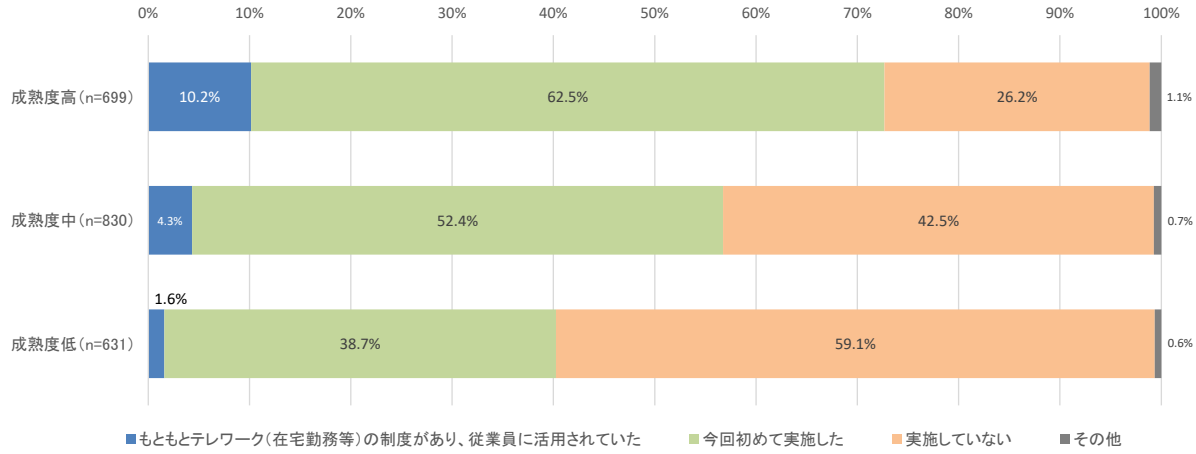

図 2.2-135　テレワーク（在宅勤務等）の実施状況（成熟度別クロス集計）

(11) テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況

次図に、テレワーク等で営業秘密を扱う場合のルール等の整備状況に関する成熟度に基づくクロス集計結果を示す。成熟度が高いほど、テレワーク等に対応したルールの整備が行われる傾向が示されている。

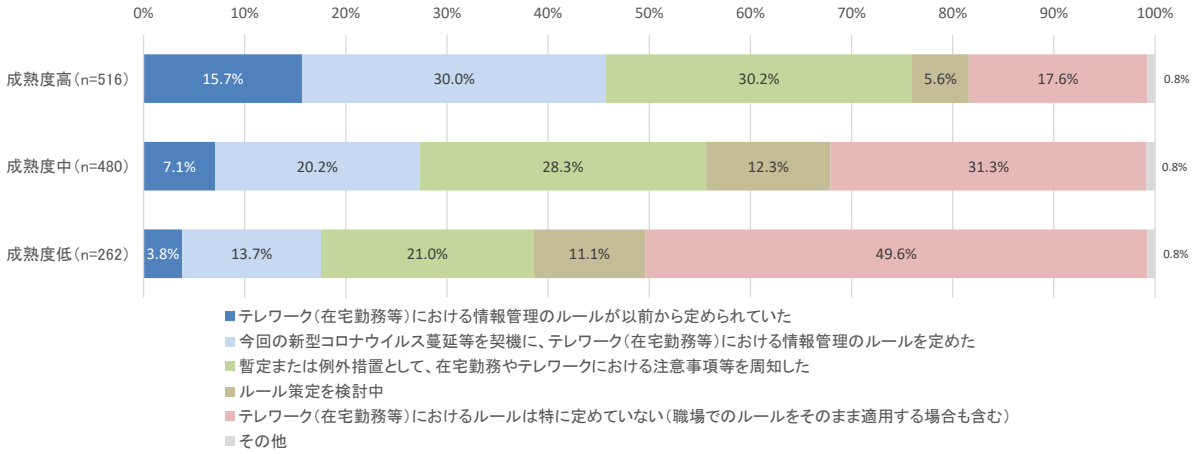

図 2.2-136　テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の整備状況
（成熟度別クロス集計）

(12) テレワーク（在宅勤務等）で営業秘密を扱う場合のルール等の具体的内容

次図に、テレワーク等で営業秘密を扱う場合のルール等の具体的内容に関する成熟度に基づくクロス集計結果を示す。本項は他の項目と比較すると、相対的に成熟度の違いによる影響が小さい。しかしながら成熟度高の企業ほど、各選択肢に関するルールの策定が行われる傾向にあることがわかる。

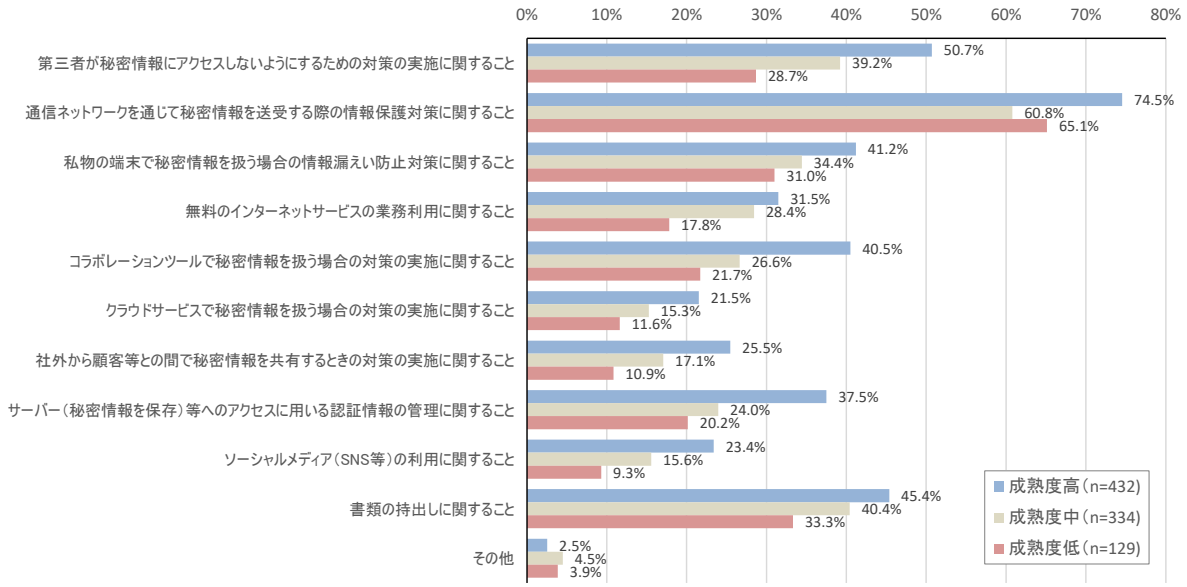

図 2.2-137　テレワーク（在宅勤務等）で営業秘密を扱う場合の目的別対策の導入状況
（成熟度別クロス集計）

(13) テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識

次図に、テレワーク等の実践を通じた営業秘密漏えいリスク増大についての認識に関する成熟度に基づくクロス集計結果を示す。成熟度が高いほど、「若干増大」が多く、「変わらない」が少ない傾向が示されている。これは、成熟度の高い企業において、テレワークによる漏えいリスクの増大があることを把握した上で、許容可能なリスクとして受容している企業が多いことを反映している可能性がある。

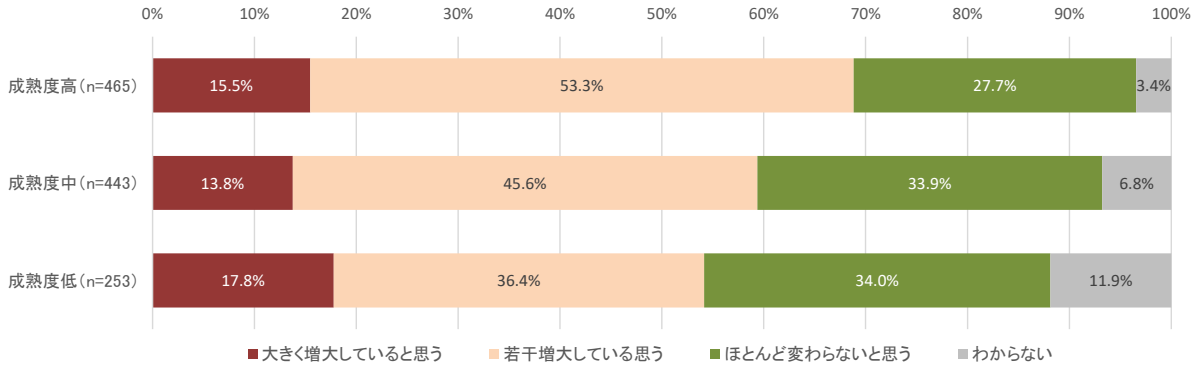

図 2.2-138　テレワーク（在宅勤務等）の実践を通じた営業秘密漏えいリスク増大についての認識（成熟度別クロス集計）

(14) 「秘密情報の保護ハンドブック」の認知及び活用状況

次図に、「秘密情報の保護ハンドブック」の認知及び活用状況に関する成熟度に基づくクロス集計結果を示す。本項についても、情報管理に関する成熟度と、「秘密情報の保護ハンドブック」の認知及び活用状況とが正相関の関係にあることがわかる。これは、成熟度が高い企業ほど、同ハンドブックを含む自社の対策を検討する際に参考となる情報の収集及び活用に積極的であることを示すものと考えられる。

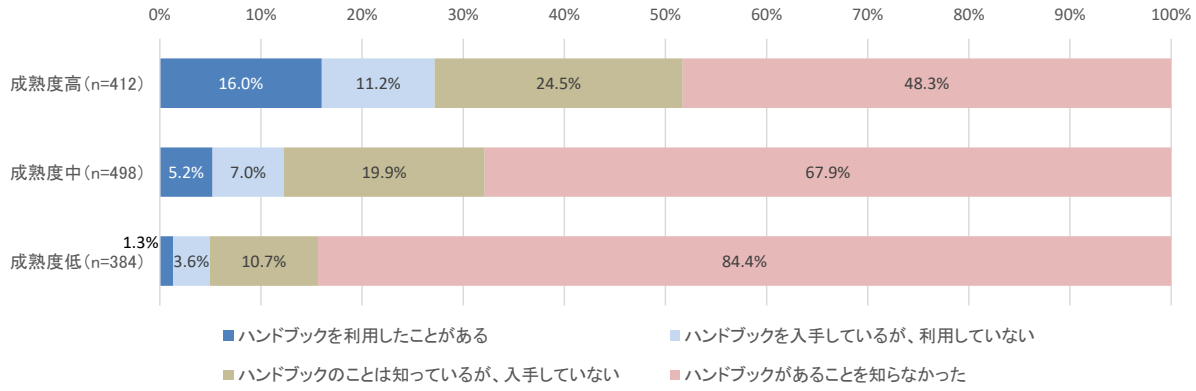

図 2.2-139　「秘密情報の保護ハンドブック」の認知及び活用状況（成熟度別クロス集計）

2.2.5.3 「情報管理に関する成熟度」に基づく考察

以上の分析結果をもとに、情報管理に成熟度から次のような傾向が読み取ることができる。

- 情報管理に関する成熟度と企業規模（従業員数ベース）は完全な正相関の関係にあるが、零細を除く中小規模企業でも一定比率で成熟度高の企業がある一方、超大手の企業でもわずかながら成熟度低の企業があり、「大規模企業なら一定の情報管理はできている」と判断することは適切ではない。
- 成熟度が中または低の企業においては、本来実現されているべき情報管理のための体制の構築やルール整備、従業員への周知等ができていないことが、まず優先的に解決すべき課題になっていることが観察される。こうした状況の結果、リスクが見通せないことでテレワークの推進に踏み込めていない実態に繋がっている可能性がある。
- 成熟度高の企業は、新しい IT の活用形態であるテレワークやクラウドサービスを積極的に活用しているが、これは適切な情報管理ができていることが、新しい情報管理の形態に取り組むための基盤として機能していることを示唆するものである。よって、営業秘密保護を含む情報管理対策の推進は、DX に代表される新たな IT 利活用を通じて企業競争力を高める効果につながることが期待される。

2.2.6 実施結果総括

以上の分析をもとに、アンケート調査結果をまとめると次のようになる。

(1) 営業秘密管理に関する全体的な傾向

次のような傾向が観察される。

- 2016 年度調査と比較して、情報漏えいに関するインシデントは回答者における認識状況に基づくデータをもとに判断すると減少傾向にある。サイバー攻撃の巧妙化により回答者に認識されていないことで減少している可能性はあるものの、対策の導入状況で改善が見られることから、総合的に判断すると情報漏えいインシデントの予防・抑止効果が高まったことの成果と考えることができそうである。
- 企業規模と対策状況は概ね正相関の関係にある。しかしながら、大規模企業であればどこでも対策ができているわけではない。
- 業種間での比較では、情報通信業及び電力・ガス・熱供給・水道業において対策が進む一方、教育・学習支援業や医療・福祉分野において対策導入が不十分な傾向が調査全体を通じて示されている。ただし、これらの傾向はこれまで情報管理やサイバーセキュリティ対策に関して論じられていた内容に反するものではない。
- テレワークにおける秘密情報管理に関しては、対策を積極的に行っている企業とそうでない企業の差が顕著である。

(2) 調査仮説の検証結果

2.1 項に示した調査仮説について、アンケート調査を通じて想定に反する結果が示されたものとして以下が挙げられる。

- 内部不正に起因する情報漏えいインシデントの件数は減少せず、最多の要因となっている。
- 情報漏えいインシデント全体でみた発生件数は減少
- 連携先やサプライチェーンを通じた情報漏えいは増加せず
- 情報管理のきっかけは「取引先からの要請」ではなく、「経営層の指示」が最多

(3) 注目すべき傾向

アンケート調査において、最も注目されるのは、上述のように情報管理に関する規程等の見直しを行ったきっかけとして、「経営層の指示」が最多となったことである。情報管理やサイバーセキュリティ対策は IT ガバナンスの一環として経営層がトップダウンで指示すべきものであり、経済産業省や IPA では『サイバーセキュリティ経営ガイドライン』の公表等を通じてその啓発に努めてきたことを踏まえると、この傾向は望ましいものと言える。また今回のアンケート調査の場合、調査に先だってコロナ禍に伴う緊急事態宣言が発令され、多くの企業において働き方を緊急に見直す必要が生じたことから、こうした緊急対応を実現するために、トップダウンでの指示がなされた可能性も考えられる。

2.3 インタビュー調査

2.3.1 調査先選定方針

以下の方針にて調査対象となる企業及び有識者の選定を行った。

(1) 企業

アンケート回答企業においてインタビュー調査への対応が可能と回答した企業のうち、製造業及び非製造業の双方を含む、インタビュー実施時期（2020 年 12 月～2021 年 1 月）における対応が可能であった以下の 5 社にご協力いただいた。

- 製造業（家具・装備品）
- 製造業（非鉄金属）
- 製造業（輸送用機械）
- 医療福祉系サービス業
- コンシューマー系サービス業

インタビュー調査項目については、アンケート調査への回答内容に関する深掘りを中心に、それぞれの企業における営業秘密管理の取組状況と直面している課題について尋ねた。

(2) 有識者

不正競争防止法ならびに企業における営業秘密管理に関して豊富な知見と実績を有する 2 名の弁護士に対し、アンケート調査結果から読み取れる企業における営業秘密管理の実態、近年の事件や裁判例から見た企業における営業秘密管理における課題、本調査を通じて企業に対して伝えるべき内容等について尋ねた。

2.3.2 調査結果概要

(1) 企業における情報管理の実態

① 企業における情報管理関連のインシデント発生の実態

- 電子メールの添付ファイルによる誤送信があったことを踏まえ、対策としてクラウドサービス上にアップロードしたファイルの URL を送付するようにすることで、誤りに気付いたときに削除できるようにした。（製造業）
- 外部からの Word 添付ファイルを通じた Emotet の感染があった。インシデントが発生したのは以前から社内で相対的にセキュリティ意識が低いと感じていた部署においてであり、再発防止策として社内で勉強会を開催した。まずはこうした意識の低い部署の底上げが重要と考えている。（医療福祉系サービス業）

② 秘密情報の区分管理の実態

- 「極秘」「社外秘」「一般」の 3 種類に区分し、従業員がそれを認識できるようにしている。（医療福祉系サービス業）
- 現場の従業員が本来秘密として管理すべき情報とそれ以外の情報を混在させて扱っているのを管理部門がやめさせることができない。そこで区分の代替策として、秘密情報を含むデータの操作を監視しているが、電子データのみが対象であり、紙媒体上の情報の保護は難しい。（製造業）

- 保護すべき秘密情報であると認識している人と認識していない人との差が大きい。(製造業)
- 営業秘密の区分管理の必要性は認識しているが、業務の多様性に対応しようとするとなかなか手を付けられない。(コンシューマー系サービス業)
- 商用ディレクトリサービスを用いてアクセス制御に取り組んでいるが、階層構造が複雑化しており管理上の負担が大きい。(コンシューマー系サービス業)
- 商用ディレクトリサービスを用いてシステムの利用者を限定しているが、社内人事異動への対応は、年２回程度、２名の担当者でなんとか対応している。(コンシューマー系サービス業)
- 商用ディレクトリサービスにおいて現場部門の希望するアクセス権限設定を実装しようとすると、過剰に複雑になりがちである。そこで、アクセス権限設定の管理を事業部門に委ね、IT 管理部門では事業部門が棚卸しした結果を確認するようにすることで、管理負荷が IT 管理部門に集中するのを回避している。棚卸しの頻度は年１回である。(製造業)
- 機微情報を扱う部門については、インターネット接続を止めることを検討している。(医療福祉系サービス業)
- 多くの企業が、ISMS でいう情報のアセスメントの段階で行き詰まっている。アセスメントというから網羅的かつ徹底してやらなければならない難しい活動という印象を与えるが、部門毎に漏れてはならない情報が何かを聞けばよいだけのはず。ISMS に対する企業の誤解である。(有識者)

③ 企業における情報管理体制の実態

- 情報管理やセキュリティ対策の担当部署は社内のリスク管理部署とは別に設置されている。担当者のスキル育成は OJT 主体で実施している。(製造業)
- IT ベンダーと現場部署との橋渡しをすることが、情報システム部門の重要な役割と認識している。(コンシューマー系サービス業)
- 一部の業務分野に限定して ISMS 認証を取得しており、当該分野の営業情報管理はその管理策に基づいて実施している。(医療福祉系サービス業)
- 経営層による情報管理に関する理解は２～３年前と比較するとかなり改善されてきたと感じており、予算もつけてもらいやすくなっている。外部からの圧力よりも、社内での働きかけの影響が大きいと考えている。(医療福祉系サービス業)
- 業界他社の導入状況等の他社比較は予算確保上有効。業界団体や日本経団連の公表しているガイドブック等に示されているサイバーセキュリティに関する考え方を経営陣にインプットしている。(製造業)
- 海外拠点の情報システムは現地で調達しており、そのシステムのアクセスログの監視は現地拠点で実施している。適切な運用がなされているかどうかは監査で確認するが、サンプリングとヒアリングが主体であり、実効的に機能しているかどうかに不安はある。(製造業)
- 企業内の規程管理担当者は、2021 年 4 月に迫っている同一賃金関連の人事規程の改訂に追われ、テレワーク対策の規程整備まで手が回っていない可能性が高い。結果的に規程改訂をせずになし崩しでテレワークを実施しているところも多いのではないか。(有識者)

④ 企業における情報保護対策の実態

- 境界防御対策として、振る舞い検知型のファイアウォールやフィルタリングサービスを導入している。（製造業）
- 明らかに業務に不要なウェブサイトにアクセスした場合、強制的にブラウザが終了して警告が表示されるようにしている。（製造業）
- 内部不正対策として、秘密情報へのアクセスログを保存しており、不正に持ち出そうとしても露見することを従業員に周知している（製造業）
- 内部不正対策として端末での不正検知機能を提供する製品を導入し、端末を監視していることを社内に周知もしている。（医療福祉系サービス業）
- アクセスログの分析は、社内の２名の担当者が行っている。AI 技術を利用することで管理負担を減らせるような製品があるのは認知しているが、高価であり導入は難しいと感じる。（医療福祉系サービス業）
- 費用のかからない対策を優先して実施している。（コンシューマー系サービス業）
- データの処理を外部委託することはあり、委託先が他の企業に再委託する可能性もあり得る。ただしその場合の情報漏えい防止対策等は委託先に委ねている。（医療福祉系サービス業）
- 年１回セキュリティ勉強会を実施している。（医療福祉系サービス業）
- 今後は認証系の強化（ゼロトラストモデルの導入を含む）を検討している。（製造業）
- 今後実施したいと考えている対策はいくつかあるが、リソースの制約もあってすぐには取り組めない。（製造業）
- ISMS 認証を取得することまでは考えていないが、ISMS の考え方の導入に取り組んでいる。（製造業）
- 取引先から情報管理対策の実施状況を問われることはある。現状で第三者認証等の制度は利用していないが、取引先毎に独自形式でエビデンスを提出することは負荷がかかることであり、業界で統一的な方法が定まると、サプライヤーの立場からは有り難い。（製造業）
- 最近は CSR やコンプライアンスに関して取引先から求められるアンケートの中に、情報セキュリティ対策に関する項目がある。（製造業）
- 現在、多くの企業では外部からの攻撃についてはある程度対策されている一方、フィッシングや脆弱性で内部から漏えいすることが増えている。絶対安全を確保できるセキュリティはないが、世間並みの対策を行うことが重要。（有識者）
- ログファイルを取得していても、そこから不審な通信を検出するなどしているのは全体の３分の１程度なのではないか。ログファイルのサイズの大きさを考えれば、異常な振る舞いを自動的に検知する仕組みの導入は最低限必要。（有識者）
- 内部不正対策としては、「不正を行おうとしてもできない」ようにすることが重要。できてしまったことを咎めても、相手に言い逃れの余地を与えてしまう。可用性の関係で触れさせないことが困難でも、セキュリティ心理学の知見を活用し、「アクセスすると通知が来る」ことで抑止効果を生むといった仕組みを用意すべき。（有識者）
- 企業の実情を踏まえると、Excel ワークシートで営業秘密のリストを管理するといった方法は現実的ではない。初年度は実施するかもしれないが、継続的に機能するかどうかは不

安である。実態との棚卸しができていないケースも多い。（有識者）

⑤ 企業における情報管理に関するリスクと課題認識

- 標的型電子メールが絶えず届いている。自社のみならず、子会社や取引先で感染すると自社にも影響が及ぶことから、対策しようと考えている。（製造業）
- 海外の特定の地域にデータが保存されるクラウドサービスは利用したくないとの上層部の意向により、クラウドサービスの内容によって、可否の判断が分かれる。また、取引先がデータの授受方法としてクラウドサービスを指定した場合に利用することはある。その場合も、都度許可申請を必要としている。（製造業）
- 対策ツール等の費用が高いとは思わないが、まとまった対策を導入しようとすると金額が嵩む印象を受ける。被害額と発生頻度の組合せで考えると、単純に投資としては見合わない。（製造業）
- IT 管理部署が普通と考える対策が、事業部門の立場になると難しい、負担が大きいと感じられていることはあると思う。（製造業）
- 担当部署により、情報の取扱いに対する意識の差が大きい一方、意識の低い人の底上げの対策ができていない。（コンシューマー系サービス業）
- 従業員に対してサイバーセキュリティ教育を必修として実施しても、理解できていない、そもそも話を聞いていないことも多く、十分に効果を発揮しているとはいえない。（製造業）
- 子会社や孫会社との間で、自社の環境を通じた情報の共有を行っている。これらの子会社等の中には情報システムの管理部署や担当者がいないところもあり、今後は子会社等のセキュリティ対策の確保にも取り組む必要があると社内で議論している。（製造業）
- サイバーセキュリティのスキルが高い人材を採用したいと考えているが、東京から離れた地域では当該人材は少なく、採用は困難と感じている。（コンシューマー系サービス業）
- 情報管理のリスクは考えればきりがないところがあり、セキュリティ対策もいくら費用があっても足りないということになりがち。（医療福祉系サービス業）
- 内部犯行よりも、業務遂行上の過失や無意識で漏えいにつながるインシデントが起こることを懸念している。また、過失等が生じた場合にその旨の報告が遅くなることも問題である。これらの問題については、改善は可能だが完全な防止は困難に思える。（医療福祉系サービス業）
- 将来的な業務の省力化・無人化の実現に向け、情報管理の重要性は今後ますます高まると考えている。経営層もそれを認識しており、方向性が決まれば必要なコストを投じて進めていくことができるのではないかと考えている。（コンシューマー系サービス業）
- 企業は、情報管理において、営業秘密や技術情報の保護と、個人情報の保護の２本柱の間での調整に困っている。前者については、誰が情報のラベリングをするかの問題がある。秘密管理性要件を満たす上でラベリングが欠かせない一方で、法務や知財の担当部署では現場の実態把握ができず、どうハンドリングすべきかの判断が後回しになっている。現場での担当者の悩みは切実なのではないか。後者については、個人情報といっても顧客情報、従業員情報などバリエーションが多く、保護規程の策定が難しい。（有識者）
- 「秘密情報と認識できなかった」という言い逃れを避けるためには、アクセス制御をしっ

かりかける、秘密情報にマル秘マークの透かしを入れる等の対策を行うしかない。牽制のためには、操作が見られていることを認識させることが重要。ログを取得し、適切に監査していることを伝える必要がある。（有識者）

⑥ 情報管理やセキュリティ対策に関する情報源

- IPA や経済産業省が公表している文書を参照している。（製造業）
- IPA のサイバーセキュリティ対策に関するスライド等のマテリアルは有り難い。一方で読み物は社内で展開してもなかなか読んでもらえない。（製造業）
- IPA や JPCERT/CC からの電子メールを受信し、脅威に関する注意情報があれば社内にグループウェアへの掲示等を行うことで注意喚起している。ただし十分伝わっているかといえば確証はない。（医療福祉系サービス業）
- セキュリティに関する情報源としては、IPA やセキュリティ製品ベンダーからの電子メールや、開催するセミナー、セキュリティ関連の展示会等を利用している。（医療福祉系サービス業）
- 情報管理やセキュリティ対策に関して、同業種や近隣の企業等と情報交換を行う機会はなく、自ら情報収集をする必要がある。（医療福祉系サービス業）

(2) 情報管理に関する近年の注目事項

① DX（デジタルトランスフォーメーション）推進における情報管理対策

- これまでの情報システム（クライアント・サーバー型）はサーバー室のデータを守ればよかった。DX ではデータがクラウドを含めて広範囲に散らばることになり、情報管理が難しくなった。ある意味、サーバー上で情報を集中管理できるようになる以前の状況に戻ったようにも感じる。（コンシューマー系サービス業）
- 業務毎に適切な情報管理の方法を考えるために、現場に 1 週間ほど通い、業務における情報の流れを把握した上で対策方法を提案することを繰り返している。設備やサービスの種類毎に異なる専門用語が用いられ、それぞれの専門業者とのやりとりにも苦労する。（コンシューマー系サービス業）
- 「デジタル化で情報の統合」といったことが謳われるが、実際には職人肌の人材が共通化を拒むなどして、受け入れられないことも多い。（コンシューマー系サービス業）

② 企業における「限定提供データ」への対応状況

- 現状では他企業等とのコラボレーション等において、限定提供データの要件を考慮した契約等は行っていないが、経営層がデータ活用の重要性を認識しており、今後は弁護士のアドバイス等の法的な理論武装をした上で活用することはあり得る。（コンシューマー系サービス業）
- アンケート結果において、「中小規模の非製造業」で不正競争防止法改正に合わせた規程見直しを行った比率が高いのは、AI 向けの学習データを扱う情報通信系のスタートアップ企業等がデータを提供する企業との連携にあたり、適切なデータの保護が可能な規程の策定を要求されていると考えてよい。（有識者）

- 企業からの相談を受けている経験から、限定提供データを意識した管理をしている企業が回答企業の 8%もあるのは高すぎる印象。ただし知財関連の部署で回答しているとすれば、こうした結果になるのかもしれない。（有識者）

③ クラウドサービスでの秘密情報の共有時の対策

- クラウド型のオフィスアプリケーションが備える認証機能やアクセス制御機能を活用している。（製造業）
- 無料クラウドストレージや業務に無関係と思しき延べ 500 程度のサイトにアクセスしても、ブラウザが強制的に終了するなどしてアクセスできないようにしている。（製造業）
- 無料クラウドストレージのような 400 種類程度のクラウドサービスを無許可で使用しても、ブラウザが強制的に終了するなどしてアクセスできないようにしている。（製造業）
- クラウドサービスの保守は自社要員で行っており、対応上不明な点が生じた場合にのみ、当該システムを開発したベンダーに確認している。用途はグループウェア等に限定されており、クラウドサービスで障害が発生した場合には止めても業務上の支障は少ない。（医療福祉系サービス業）
- 従業員が勝手に無料のクラウドサービスを利用し、そこで業務上の情報を扱うことについて、特に規制等は行っていない。（医療福祉系サービス業、コンシューマー系サービス業）
- 素人がサーバーを管理することに比べれば、クラウドサービスを利用するほうがよい。ただし、どのようなクラウドでもよいわけではなく、絶対に守るべきものはそれなりの費用がかかるサービスを選定すべき。（有識者）
- 適切なエンタープライズ契約で利用しないと、障害時のリストアなどのサービスが受けられない可能性がある。ログ監査ができるものや、世代管理が可能なものを選定するなど、IPA からクラウドサービスが提供する機能の推奨を行うべきかもしれない。（有識者）

④ 脱印鑑、ペーパーレス化等の取組状況

- オフィス移転を契機に、オフィスをフリーアドレス化するとともに、クラウドベースの電子ワークフロー・決裁システムを導入した。これに合わせて一般の従業員の端末をシンクライアント化したため、秘密情報は従業員端末には残らないようになっている。ただしシンクライアントがネットワーク帯域を消費するため、使い勝手についての不満が生じており、改善方法を検討している。（製造業）
- 社外との契約書などで印鑑を用いることはあるが、それ以外はすべて電子化されている。印鑑のように代理で押印するといった運用は組み込んでおらず、権限者がリモートからでも承認する仕組みである。（製造業）
- オンラインワークフローを導入済みであり、役職者による承認プロセス等はテレワークで実施可能である。（製造業）
- IT 管理部門はペーパーレス化を実施したいと考えているが、現場事業部門の理解が前提であり、現状では事業部門では電子化を歓迎していないため進んでいない。（製造業）

⑤ テレワーク等の環境における営業秘密管理の状況

- 従業員の端末をシンクライアント化していたことが、緊急事態宣言の際にも活用できた。シンクライアント利用者に対しては、緊急事態宣言に伴う手続関連の見直しは、在宅勤務を事前申請制としていたことをなくした程度である。一方でデザイン関連業務など通常の PC を使わざるを得ない従業員もいたので、これらの機器を在宅勤務でも利用できるようにするために暫定的な対策を設けるとともに、注意喚起を図る必要があった。全体で見ると、テレワーク形態に移行したことでセキュリティを緩めている部分はない。（製造業）
- VPN のセッション数が足りなくなり、追加した。（製造業）
- 紙媒体の持ち帰りは極力避けるように求めている。（製造業）
- テレワークで実施可能な業務を制限している。資金決済などリスクの観点から不可としているものと、CAD のようにパフォーマンスの観点でできないものがある。（製造業）
- PC は社内ネットワーク内で利用することを前提としており、出張などの一時的な持ち出しのみを想定した対策しかできていない。そのため、今の対策だけで社外に持ち出している状況では、対策の十分性に不安がある。現状では実施すべき対策が十分ではないと考えていることから、テレワークにおける情報管理リスクは高いと認識している。（製造業）
- 現在通常の PC を用いて実施している業務については、セキュリティ機能を強化した PC に移行させることを検討している。（製造業）
- テレワーク環境は「シン・テレワークシステム」で構築した。（製造業）
- 子会社の中には緊急事態宣言の中でやや強引にテレワークを開始したところもある。テレワーク時のセキュリティ対策に関するガイドレベルの文書を提供している。（製造業）
- 自社の業務の多くが、職場の設備を用いる必要があるものであるため、テレワークにおいては機微な情報を扱うことがなく、実施可能な従業員も限定されている。よってテレワーク導入により情報管理上のリスクはほとんど変化していない。（医療福祉系サービス業）
- 私物利用は認めず、テレワークでの業務が必要な従業員に PC を配布したため、対策費用がかさむこととなった。（コンシューマー系サービス業）
- アンケート結果については、宿泊業・飲食業などテレワークの対象外企業が含まれており、その影響を考慮する必要がある。（有識者）
- BYOD がなし崩しで許可され、規定されていない場合が多いはず。（有識者）
- テレワーク環境はオフィス環境よりも監視が緩いという印象を従業員に与えると、不正に関する心理的ハードルが下がり、誘惑にかられる可能性が高まる。この対策に関して簡単な答えはないが、操作やデータの内容に応じて警告画面の色が変わるなどの警告を工夫すべきかもしれない。（有識者）
- プライバシー保護型カメラの自宅設置を求めるのはハードルが高い。大企業でも就業規則で従業員の個人情報の扱いは規定していないところが多いが、設置するのであれば規程等で映像の扱いを明確にすることが最低限求められる。労働組合との協議も必要。金融機関ではインサイダー対策で実施しているところもあるかもしれない。また、リアルタイムに監視をするか、何か起きたときのみ事後的に確認するかでも変わってくる。（有識者）
- IPA が NTT 東日本等との連携のもとで提供した「シン・テレワークシステム」について、報告書でも紹介すると良い。（有識者）

⑥ 境界防御型モデルからゼロトラストモデルへの移行の取組状況

- SaaS ベースのゼロトラストモデルへの移行に取り組んでいる。以前よりも運用コストは増えることになるが、経営層には情報管理の対象箇所を集約できることによる管理コストの圧縮が可能と説明して理解を得ている。（製造業）

(3) 「ニューノーマル」等の変化が営業秘密管理に及ぼす影響

- テレワークはコロナ禍以外にも、今後の老々介護の増大など社会の変化や、大規模災害におけるサプライチェーンの障害などの場面でも必要になることが見込まれる。そのためニューノーマルとしてそうしたニーズの増大に応じて、セキュリティの重視が欠かせなくなる。（有識者）
- 境界防御をドアロックなどで実現していた場合、ネットワーク接続が前提の現状では不十分となるため、その対策が必要。（有識者）

(4) 今後公的機関が取り組むべき施策

- サイバーセキュリティ対策や情報管理に関する５分程度の動画があると社内で活用しやすいので、ぜひ取り組んでいただきたい。（製造業）
- 外からの攻撃を防ぐための対策の全体的な見直しが必要と考えているが、その見直しに応じた情報セキュリティ関連の規約類を整備する人的リソースが社内に不足している。ついては参考にできるような規約類のサンプルを公開してもらえるとありがたい。（製造業）
- セミナー開催場所が東京に偏っている印象がある。オンラインでもよいので東京近郊以外からも参加できるような機会を増やして欲しい。（医療福祉系サービス業）
- 「秘密情報の保護ハンドブック」改訂に際しては、「入門」相当の最初の手順として、人事や営業の各部署で漏えいすると問題になる情報のトップ３をそれぞれ出してもらうところから始めるといった記載をすべき。「0 か 100 か」ではなく、まず 1 を目指す。「アセスメント」や「洗い出し」という表現も使うべきではない。（有識者）
- 企業におけるログにおける不審なアクセス等の自動検知に要する費用の支援をしてはどうか。（有識者）
- IPA が公表している各種コンテンツや、総務省のテレワークセキュリティガイドライン等で提供している情報管理のための様式の雛形等は積極的に紹介すべき。（有識者）
- 営業秘密管理は知財や労働法と密接に関連するので、これらをまとめて紹介するようなセミナーがあるとよい。（有識者）

2.3.3 実施結果総括

インタビュー調査を通じて得られた知見のうち、以降の考察において重要な意味をもつものを以下に示す。

(1) 企業インタビュー

- テレワーク等の実施に伴うリスクの高低を企業がどのようにとらえるかは、その企業がテレワークにおいてどのような業務を認めるかに大きく依存することが確認された。必ずしも十分な対策が講じられていなくても、重要な情報を扱わない範囲のみでテレワークが実施されている場合、テレワークによるリスクの増大はほとんどないとみなされることがあり得る。
- 情報管理における区分管理の阻害要因として、企業より次のような事例が挙げられた。
  - 業務形態が多様であり、それぞれの業務に適した情報管理ルールを作って守らせようとしても、管理側の手が回らない。
  - 現場では管理すべき秘密情報が管理不要の情報と混在して扱われているため、秘密情報のみを取り出して管理することは現実的でない。

(2) 有識者インタビュー

- 営業秘密の適切な管理の実現に向けて、多くの企業が社内情報のアセスメントや洗い出し、棚卸し等の段階で行き詰まっている実態を踏まえ、部門毎に漏れてはならない情報が何かを把握した上で、異論と無理が出ないところから開始すべきとの指摘が得られた。

2.4 文献調査

直近（概ね 5 年以内）において不正競争防止法及び企業における営業秘密保護に関して、当該分野の関係機関、専門家及び研究者等により示された様々な見解や解説について、アンケート調査における調査項目の検討を目的として調査した結果を、当該文献の記載内容をもとに整理する。

2.4.1 営業秘密漏えいの発生状況

文献 1	
文献表題	2018 年情報セキュリティインシデントに関する調査結果（速報版）
公表媒体	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（JNSA）ウェブサイト https://www.jnsa.org/result/search.html
著者	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（JNSA）調査研究部会
発行者	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（JNSA）
公表時期	2019 年 6 月

企業等の事業活動を通じた個人情報の漏えいインシデントの実態について、報道等の情報をもとに 2008 年 1 月 1 日から同年 12 月 31 日までの 1 年間あたりの漏えい件数と漏えいした個人情報の数、損害賠償額の総額について集計したもの。2017 年と比較して、漏えい件数が 386 件から 443 件に増加し、それに伴い漏えい人数も 8%増の 561 万 3,797 人、1 件あたりの平均想定損害賠償額は 16.3%増の 6 億 3,767 万円に増加するなど、漏えい被害は依然として増加傾向にあることが示されている。これを踏まえ、アンケート調査の設計にあたっては、被害や対策状況が 2016 年調査から改善されていないことを前提に選択肢等の設計を行うこととした。

なお、JNSA では 2019 年以降の情報セキュリティインシデントに関する調査結果を公表していない。

2.4.2 営業秘密認定に関する裁判例の動向

文献 2	
文献表題	営業秘密の不正利用行為の規律に関する課題と展望
公表媒体	知的財産法政策学研究 Vol.47 https://www.juris.hokudai.ac.jp/riilp/journals/
著者	田村　善之
発行者	北海道大学
公表時期	2015 年 11 月

過去に公表された「営業秘密管理指針」において、過去の裁判例における「判決理由」と「傍論」との区別が十分でなく、秘密管理性が認められるための要件に関する解説内容が不適切であった旨を指摘している。さらに、我が国の裁判例における秘密管理性の考え方の変遷[6]を次の 3 期に分けて分析している。

- 草創期から 2000 年代初頭まで（緩和期）：情報の管理を一部欠いている場合でも秘密管理性を肯定した裁判例が頻出。

[6] このほか、著者が参加した座談会において、同様の解説を行っている。
小泉直樹、清水節、田村善之、長澤健一、三村量一：『座談会：営業秘密をめぐる現状と課題』（Jurist, No. 1469, 2014 年 7 月）

- 2000 年代初頭から 2000 年代中盤まで（厳格期）：以前であれば秘密管理性が肯定されるような状況においても、客観的に認識しうるような秘密管理がなされていないとみなされる場合は秘密管理性が否定される裁判例が主流を占める。
- 2000 年代終盤から現在（揺戻期）：秘密として管理していることが認識可能であったかどうかが秘密管理性の判断基準となる裁判例が増加。

また、現行の営業秘密管理指針については、本文献の筆者と共通の考え方に基づいた記述となっており問題ないとしながらも、秘密管理が争点になる裁判例の多くが内部者による不正取得によるものであり、厳密に秘密管理しても紛争を防ぎ得ないことから、秘密管理性に厳格さを求めるメリットはあまりなく、保護すべき利益が背後にあるような営業秘密について、より使い勝手のよい法理とするために、秘密管理、特定立証、営業差止に関して柔軟に考えていくべきと主張している。

文献 3	
文献表題	営業秘密の保護
公表媒体	知的財産法政策学研究 Vol.47 （オンラインでは非公表）
著者	髙部　眞規子
発行者	北海道大学
公表時期	2015 年 11 月

営業秘密の保護に関する論点として、以下の①～③について紹介している。

① 実体法上の問題点

2015 年の時点で、秘密管理性に関する最高裁判断はなされていない。下級審での裁判例は営業秘密の管理状況に限らず、行為の悪質性や侵害行為の有無等を含めて、保護すべき事案かどうかを考慮した上で秘密管理性を総合的に判断していると考えられることから、「社外秘表示があったかどうか」といった個別要素を取り出して判断の妥当性を論じることは適切ではないとしている。

② 訴訟手続き上の問題点

営業秘密の侵害等を理由とする差止請求訴訟等において、原告が営業上の利益の侵害等を主張立証する際に提出する証拠には営業上又は技術上の秘密情報が含まれることから、提出に伴い営業秘密が公知となり、秘密管理性の要件を欠くことになってしまうのを避ける必要がある。制度として定められている「訴訟記録の閲覧制限」「秘密保持命令」「公開停止」等を活用するだけでなく、運用面でも「非公開の弁論準備手続期日での審理」、「陳述書の活用」等を考慮すべきとしている。

③ 最高裁判所による裁判例

営業秘密保護に関連する最高裁の裁判例として、競業避止義務に係る特約がない場合の競合行為が不法行為に該当するかが争われた事案（最一小判平成 22・3・25 民集 64 巻 2 号 562 頁）と、海外の裁判所で言い渡された損害賠償及び差し止めに関する日本国内での執行を求める事案（最一小判平成 26・4・24 民集 68 巻 4 号 329 頁）を紹介している。前者では競合行為における不当性の有無と協業行為による営業阻害の程度が判断要素となっていること、後者は属地主義の原則によるものとされる特許権等の産業財産権と異なり、生命・身体・名誉・信用等、世界中で普遍

的な権利として保護を受けるべきものとして扱われていることをそれぞれ特徴として指摘している。

文献 4	
文献表題	営業秘密における有用性と非公知性について
公表媒体	月刊パテント Vol.70, No.4 https://system.jpaa.or.jp/patent
著者	石本　貴幸
発行者	日本弁理士会
公表時期	2017 年 4 月

営業秘密の３要件のうち、有用性と非公知性については未だ判断基準が定まっていないことを踏まえ、過去の裁判例をもとに判断の妥当性について論じている。

有用性に関しては、経営情報の場合は情報の羅列に過ぎず、分類がなされていない情報や、第三者が容易に入手可能な情報の場合に営業秘密としての有用性が否定される傾向が明確であるのに対し、技術情報の場合は効果が客観的に確認されるべきことや、公知技術よりも特段の優れた作用効果を求める裁判例（例：大阪地裁平成 20 年 11 月 4 日判決（発熱セメント体事件)、大阪地裁平成 28 年 7 月 21 日判決（錫合金組成事件)）があることを指摘した上で、有用性の判定に関してこのような要件を求めることは、具体的な数値等を秘匿して作成された技術文書が不正に持ち出され使用された場合に、差止請求や損害賠償請求が認められにくくなるなどの影響をもたらすと主張している。

非公知性に関しては、インターネット上のサイト等で公開されている住所等の情報を集めた程度の情報には非公知性がないとの判断が示されている一方で、リバースエンジニアリングによって得られる情報の非公知性に関して、過去の裁判例（大阪地裁平成 15 年 2 月 27 日判決（セラミックコンデンサー事件)）から推察される、「専門家により、多額の費用をかけ、長期間にわたって分析することが必要と推認されるもの」という基準は、求められる専門性や高額かどうかに曖昧性を伴うことから適切とはいえないとしている。

以上のまとめとして、企業が望まない形で情報が持ち出されたことが明確である場合には、その企業を保護するためにも、情報の有用性及び非公知性の要件認定を緩和すべきと主張している。

文献 5	
文献表題	技術情報に係る営業秘密に対する秘密管理性の認定について
公表媒体	月刊パテント Vol.71, No.5 https://system.jpaa.or.jp/patent
著者	石本　貴幸
発行者	日本弁理士会
公表時期	2018 年 5 月

営業秘密の３要件のうち、最も訴訟等で問題となりやすい秘密管理性について、これまでの裁判例のうち、秘密管理しているとの明示がなかったにも関わらず秘密管理性が認められた事例、秘密管理性が認められなかったもののうち特徴的な事例として、以下の裁判例を紹介している。

① 秘密であることの明示がないにも関わらず秘密管理性が認められた事例

- 大阪地裁平成 15 年 2 月 27 日判決（セラミックコンデンサー事件）：秘密情報を格納したコンピュータの隔離、バックアップ操作権限を有する担当者の限定、バックアップ媒体の施錠保管等の対策と企業規模を勘案して秘密管理性を認定
- 東京地裁平成 22 年 4 月 28 日判決（生産菌製造ノウハウ事件）：種菌の施錠可能な冷凍庫への保管、保管場所へ入出可能な従業員の限定、保管場所の常時施錠、監視カメラの設置、持ち出し時の在庫管理等の管理状況をもとに秘密管理性を認定
- 大阪地裁平成 25 年 7 月 16 日判決（Full Function ソフトウェア事件）：秘密保持契約を前提とした開示、顧客に非開示のパスワードを用いた開発環境の起動制御、ソースコードを開示しない販売形態等の実態をもとに秘密管理性を認定
- 東京地裁平成 29 年 2 月 9 日判決（婦人靴木型事件）：従業員への機密保持に関する誓約書の徴求、木型の厳重保管、通常時の従業員の取扱不可等の状況をもとに秘密管理性を認定

② 秘密管理性が認められなかった事例

- 知財高裁平成 27 年 5 月 27 日判決（金型技術情報事件）：秘密保持契約を締結せず、業界内での一般的理解のみでは秘密管理性の成立を認めず
- 知財高裁平成 28 年 4 月 27 日判決（接触角計算プログラム事件）：ソフトウェアの営業担当者向けハンドブックに秘密である旨の記載があったものの、公知の原理に基づくアルゴリズムであり、当該ハンドブックにパラメータを公開している旨が明示されていたことで、情報の使用態様により秘密管理性を否定
- 東京地裁平成 29 年 7 月 12 日判決（光配向装置事件）：営業秘密とされた文書が、秘密である旨の記載がある一方で、通常の営業活動の中で取得することが不自然ではないと判断され、秘密管理性を否定
- 東京地裁平成 27 年 8 月 27 日判決（二重打刻鍵事件）：原告が訴状別紙として提出した営業秘密目録について閲覧等制限の申立てを行わなかったことで、約 10 ヶ月にわたり鍵情報が何人も自由に閲覧できる状態に置かれていたことで、営業秘密性があることが認められず

以上の事例をもとに、秘密管理性が認められるためには、必ずしも「秘密であることの表示」が求められるわけではなく、「アクセスした者が当該情報が営業秘密であることを認識できる態様」で管理されていればよいながら、秘密管理措置を行っていたことを示す多くの主張立証が必要と見込まれる。このため、営業秘密に相当する情報に対して複数の秘密管理措置を講ずるとともに、その秘密管理措置を毀損しないように当該情報の取扱いに努める必要があると結論づけている。

文献 6	
文献表題	営業秘密の有用性と非公知性について－錫合金組成事件－
公表媒体	知的財産法政策学研究 Vol.52 https://www.juris.hokudai.ac.jp/riilp/journals/
著者	陳　珂羽
発行者	北海道大学
公表時期	2018 年 11 月

大阪地裁平成 28.7.21 平成 26（ワ）11151・平成 25（ワ）13167（錫合金組成事件）の判決について、営業秘密に関する有用性及び非公知性の否定に至った背景について考察している。これ

によれば、有用性の否定は原告の主張する営業秘密情報が公知の技術の中で特定の数値や条件を特定したに止まることから、公知技術の中の条件の組合せの事例として、追加的な効果がないことによるものである。一方、非公知性の否定については、市販されている製品を分析することで成分元素と構成割合を把握することが可能であることが根拠とされており、原告が主張した専門知識や技術の必要性は同業者であれば容易であるとの判断により否定されており、これまでの裁判例から外れるものではないと結論づけている。

文献 7	
文献表題	プログラムの営業秘密性に対する裁判所の判断
公表媒体	月刊パテント Vol.72, No.7 https://system.jpaa.or.jp/patent
著者	石本　貴幸
発行者	日本弁理士会
公表時期	2019 年 7 月

コンピュータソフトウェアを営業秘密として管理する場合に留意すべき事項として、ソースコードとアルゴリズムに分けて検討する必要性と、営業秘密侵害とともに著作権侵害が提起されることが多いという特徴について、これまでの裁判例をもとに次の各点について論考している。

① ソースコードの営業秘密性に関する裁判所の判断傾向

一般に、商用ソフトウェアにおいてはコンパイルした実行形式のみを配布したり、ソースコードを顧客の稼働環境に納品しても開示しない措置をとったりすることが多い実態を踏まえ、ソースコードを秘密管理性が高い技術情報との前提にその営業秘密性を判断する傾向が強い。

② 技術的に特徴のないソースコードの非公知性

公知の複数のコードが組み合わされたソースコードであっても、全体として公知でなければ営業秘密としての非公知性は認められると考えられる。

③ 営業秘密性が否定されたアルゴリズムに基づく場合のソースコードの営業秘密性

アルゴリズムに営業秘密性が認められない場合でも、ソースコードが適切に秘密管理等されていたのであれば、当該ソースコードの営業秘密性は認められ得る。

④ 営業秘密と認定されたソースコードの不正使用に関する該当性

技術的特徴のないソースコードから想起される技術思想を参考にする場合、ソースコードの不正使用と判断されない可能性が高いが、不自然に類似・共通する箇所が存在する場合、不正使用が認められる可能性がある。

⑤ 著作権侵害との関係

営業秘密侵害における不正使用の範囲は、著作権侵害の複製又は翻案の範囲よりも広い概念であると考えられ、それぞれ個別に判断すべきである。

⑥ アルゴリズムの営業秘密性

アルゴリズムを営業秘密とした場合の不正使用の範囲は、ソースコードの不正使用の範囲よりも広い概念であることが示唆されるが、これまでアルゴリズムが営業秘密として認められた裁判例は見つかっていない。

文献 8	
文献表題	営業秘密の刑事上の保護といくつかの問題について
公表媒体	工業所有権法学会年報第 43 号 有償刊行物（ISBN 978-4-641-49954-6）
著者	平野　惠稔
発行者	有斐閣
公表時期	2020 年 5 月

情報社会の進展に伴い営業秘密の事業上の重要性が高まる中、民事上の営業秘密の保護のみでは不十分であるとして、不正競争防止法の平成 15 年改正において営業秘密侵害罪が刑事罰の対象となった。一方で刑事的執行は当初ほとんどみられなかったが、平成 23 年改正法の施行以降、コンスタントに判決が出るようになっている。こうした中で、営業秘密の刑事的保護における論点として、以下の点を挙げている。

① 領得行為

平成 21 年改正で営業秘密不正領得罪が新設されたことで、何をもって営業秘密という情報そのものを「領得」したとするかの定義が求められており、「営業秘密について自らが保有者となる意思を有して行為すること」と「保有者として営業秘密を処分・利用できるようになること」の２点を満たすことをもって示すことが可能としている。

② 図利加害目的

図利加害目的は、これまで「不正の競争の目的」とされていたものが、競争関係の存在を前提としない加害目的や、外国政府を利する目的にも適用可能とするため、平成 21 年改正にて改められたものである。第三者の利益を図る目的が含まれ、営業秘密の保有者本人の利益を図る目的や正当な報道や内部告発等の目的が含まれないことに異論が生じない一方で、財産上の利益・損害以外の利益・損害が含まれるかどうかや、正当な目的と図利加害目的が混在する場合の総合判断などは争点となり得ることもあって、健全な事実認定がされた事例の集積が望まれるとしている。

③ 秘密管理

刑事と民事とで、秘密管理の要件を別異に解することはないが、刑事事件では秘密管理性の要件を充足する為に検察側で合理的な疑いを入れない程度の立証が必要であることから、営業秘密性の認定に際して確たる証拠がない場合に、民事と刑事とで判断が異なる結果となることがあり得るとしている。

2.4.3 営業秘密保護対策に関する最新の動向

文献 9	
文献表題	企業における秘密管理の実務について－コカ・コーラ社における営業秘密の保護を中心に－
公表媒体	知的財産法政策学研究 Vol.47 （オンラインでは非公表）
著者	足立　勝
発行者	北海道大学
公表時期	2015 年 11 月

コカ・コーラ社における営業秘密保護に関するプラクティスとして、いくつもの皮で芯に相当する営業秘密をしっかり守ろうとすることから、社内で「オニオンモデル」と呼ばれる考え方を

以下の３種類のアプローチを通じて実践していることを紹介している。

① 物理的アプローチ

物理的なアクセスのコントロールや守秘義務契約等を通じて、本当に知る必要がある人のみが営業秘密を知る仕組みとする。

② 技術的なアプローチ

調達と製造を分離し、製造プロセスをコードで管理することで、自らの担当分以外の具体的な作業がわからないような工夫を行う。

③ 組織的なアプローチ

対外的な告知を行う場合、組織内の特定の役職者の了解を得る必要がある。

文献 10	
文献表題	富士通の情報管理について
公表媒体	知的財産法政策学研究 Vol.47 https://www.juris.hokudai.ac.jp/riilp/journals/
著者	西田　雅俊
発行者	北海道大学
公表時期	2015 年 11 月

国内企業における情報管理の取組事例として、富士通株式会社における情報管理について以下の内容について紹介している。

① 情報の分類方法

自社で扱う情報を以下のように４種類に分類し、さらに個人情報については社内外を問わず別途法令やプライバシーマークに準拠して適切に保護するためのポリシーを適用している。

- 公開情報（カタログ、マニュアル、自社ウェブサイト内容等）
- 社外秘情報（関係社外秘情報以外の社内情報：社内ルール、社内報等）
- 関係社外秘情報（関係者以外に開示できない情報：顧客リスト、技術情報等）
- 他社秘密情報（顧客預かり情報、他社からライセンスを受けた技術情報等）

② 情報管理に関する規定等

情報管理規程により、秘密である旨の表示を行う、関係者以外がアクセスできないようにする、廃棄時はシュレッダーや焼却処理等のように情報の扱いを規定。さらに部門毎の運用細則を定め、年１回の監査実施を遵守している。

③ 情報を扱う要員の管理

情報管理に関する e ラーニング講座による教育を実施するとともに、情報管理ハンドブックを提供。退職時の情報持ち出しに関するログ確認や外部記憶媒体の使用制限等を実施。

④ 情報管理における課題

海外における合弁事業を通じた技術提供・技術移転を通じた情報の不正な流出を防ぐための秘密保持契約の締結、重要技術のブラックボックス化、現地での教育・情報管理体制の徹底、オープンイノベーション時代における情報の提供と保護のバランス等が課題としている。

文献 11	
文献表題	技術情報を営業秘密化して記録する場合の注意点 ―タイムスタンプを利用して営業秘密を保護する場合の注意点―
公表媒体	月刊パテント Vol.70, No.3 https://system.jpaa.or.jp/patent
著者	北村光司（平成 27 年度不正競争防止法委員会委員長）ほか
発行者	日本弁理士会
公表時期	2017 年 3 月

平成 27 年度不正競争防止法委員会第 2 小委員会第 2 グループにおいて検討された、タイムスタンプを利用して技術情報等の営業秘密を記録することの効果と実施上の注意点について紹介するものである。

① タイムスタンプを利用して営業秘密を記録することの効果（抜粋）

- 発明者（創作者）や技術内容等を特定可能とすることで、共同発明者による抜け駆け的な特許出願の抑止や、発明者等からの情報漏えいを防止する効果が期待できる。
- 権利者情報を特定可能とすることで、原告適格を容易に証明したり、技術の財産的価値を高めたりする効果が期待できる。
- 中小企業においては、複数の特許出願を行うことが困難な場合や、特許が取得できても訴訟による権利行使等が費用的な問題から困難な場合がある。このような場合に技術情報にタイムスタンプ等を付与して、技術上の営業秘密として保護することにより、特許出願よりも少ない費用で自社での実施を確保する方法として利用することができる。

② 実施上の注意点（抜粋）

- 平成 29 年から提供開始されたタイムスタンプ保管サービスでは、保管されるのはタイムスタンプトークン（ハッシュ値）のみであり、営業秘密文書自体は自己管理する必要がある。自己管理している営業秘密文書を誤って改変したり、紛失したりしてしまうと証明が不可能となる。
- 発明に関する技術情報をすべて使用者等に帰属する技術上の営業秘密としてしまうと、不正競争防止法上、発明者は技術の移転について民事上、刑事上の責任を負わされ、意図しない紛争に巻き込まれるリスクが高まるほか、特許を受ける権利を実質的に移転することができなくなるなど、発明者の権利が奪われる恐れもある。
- 営業秘密に係る電子データは、サイバー攻撃による被害を受けないように適切な対策を講じて管理する必要がある。
- タイムスタンプを利用して営業秘密化した情報について、不正競争防止法上の保護を求めた裁判例はほとんどないことから、先使用権に関する判例等を研究して、証拠化した書面の有効性を判断せざるを得ない。

文献 12	
文献表題	インフォメーション・ガバナンス 企業が扱う情報管理のすべて 顧客情報から社内情報まで
公表媒体	書籍（ISBN 978-4-492-53400-7）
著者	ベーカー&マッケンジー法律事務所ほか
発行者	東洋経済新報社
公表時期	2018 年 6 月

企業における情報管理の制度設計や諸規程の整備に資することを目的とする書籍である。導入において日本企業における情報管理の問題点として、情報管理の概念に対する認識不十分とそれに基づく投資の不足、有事のみならず平時の適切なマネジメントを考慮した統一的な管理体制やシステム化の欠如、及び複数の法律が複雑に適用される可能性への非対応等を挙げ、その対応方法を以下の観点から整理している。

- 統一的アプローチの利点
- 個人情報保護のための情報マネジメント
- 営業秘密を管理するための情報マネジメント
- ディスカバリー制度と情報の一元管理
- インサイダー取引を防止する為の情報管理
- 各個別法に対応する為の統一的な情報管理手法
- 現在の情報マネジメントとセキュリティの関係
- 日本企業に求められる企業情報マネジメント
- 構築が急務となる企業情報システム

このうち、本報告書との関係が深い営業秘密管理に関しては、訴訟等で営業秘密として認められるための３要件のうち秘密管理性の確保に焦点を置き、これまでの裁判例で秘密管理性が肯定・否定された例について整理した上で、「秘密情報の保護ハンドブック」にて示されている営業秘密管理のステップを紹介している。

文献 13	
文献表題	スタートアップと営業秘密～将来のオープン&クローズ戦略に備えて～
公表媒体	月刊パテント Vol.72, No.1 https://system.jpaa.or.jp/patent
著者	平野隆之（平成 29 年度関東支部中小企業・ベンチャー支援委員会委員長）
発行者	日本弁理士会
公表時期	2019 年 1 月

オープン＆クローズ戦略を実践するには、製品に利用する技術に関する特許とノウハウを組み合わせることで保護がしやすくなり、戦略の幅も広がるメリットがある。一方で起業間もないスタートアップ企業にとって、技術の特許出願およびノウハウ営業秘密としての保護のいずれも、多忙や人手不足により容易ではない場合が多い。そこで本文献では、スタートアップ企業に対する知財の啓発を行う一環としての営業秘密管理をどのように説明するのがよいかについて、秘密管理性に焦点を当て、以下のような説明方法の例を挙げている。

- 営業秘密に係る不正行為であると裁判所が認めると、不正競争防止法に基づき営業秘密の使用差し止めや、営業秘密の不正使用により生じた製品の廃棄、賠償金の支払い等を要求が可能となるといった、スタートアップ企業が実際に直面するフェーズでの説明が有効。
- どのような行為が不正競争に該当するかは、最近の複数の事件を例に挙げて説明する。どのような営業秘密が、どのように漏えいしたか等の話題は法律論よりも関心を示してもらいやすい。
- 企業が実施する秘密管理措置が秘密管理性の要件を満たすには、「経済合理的な秘密管理措置」が実際に行われ、従業員や取引業者の「認識可能性が確保」されていたかがポイントになる。どのような措置を施せばよいのかに関しては、必要最低限の水準が「営業秘密管理指針」に、高度な対策に関しては「秘密情報の保護ハンドブック」にそれぞれ記載されている。
- スタートアップ企業も大企業と同じ秘密管理措置を行うことが要求されるのではない。どのような秘密管理措置が秘密管理性の要件を満たすかは裁判所が最終的に判断するものであって、実際の裁判では企業規模や情報の性質を考慮して個別に判断がなされている。

さらに、スタートアップ企業を対象とする秘密管理措置に関するアンケート調査を実施し、11社から回答を得ている。これによると、情報漏えいを気にかけているか、ログイン時のパスワードを設定しているかの 2 点については全社が Yes と回答しているのに対し、情報漏えいに関する社員教育を実施している企業は 1 社もなく、「関係者以外立入禁止」や「撮影禁止」等の掲示をしている企業は 1 社のみ、投資家と秘密保持契約を結んでから詳細な説明をしている企業も半数未満といった結果が得られている。

文献 14	
文献表題	3 訂版 社内諸規程作成・見直しマニュアル
公表媒体	書籍（ISBN 978-4-539-72663-1）
著者	岩﨑　仁弥（著）　TMI 総合法律事務所（監修）
発行者	日本法令
公表時期	2019 年 5 月

就業規則ほか社内向けの諸規程について、現行の諸法令解釈に基づくモデル規程とその記載内容に関する解説を付加し、読者がモデル規程をカスタマイズして自社にあった社内規程を策定することに資することを目的とした書籍である。営業秘密管理に関連するモデル規程として、以下の事例が紹介されている。

- 就業規則
- 文書管理規程
- 営業秘密等管理規程
- 個人情報取扱規程（特定個人情報以外）
- 特定個人情報（マイナンバー）等取扱規程
- モバイル PC・スマートフォン取扱基本規程
- モバイル PC 取扱マニュアル

2.4.4 海外における営業秘密保護の動向

文献 16	
文献表題	DEFEND TRADE SECRETS ACT OF 2016 （2016 年米国連邦民事トレードシークレット保護法）
公表媒体	合衆国議会ウェブサイト https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf
著者	合衆国議会
発行者	合衆国政府印刷局
公表時期	2016 年 5 月

文献 19 に示されているように、営業秘密を取り巻く環境の変化、ならびに既存の統一営業秘密法（UTSA）に基づく各州法や連邦経済スパイ法（EEA）のみでは対応に限界があるとの認識を受け、2016 年に施行された米国の連邦法であり、次の各条から構成される。

- 第 1 条　Short title.（略称）
- 第 2 条　Federal jurisdiction for theft of trade secrets.（営業秘密の窃取に対する連邦の司法管轄権）
- 第 3 条　Trade secret theft enforcement.（営業秘密の窃取に係る法執行）
- 第 4 条　Report on theft of trade secrets occurring abroad.（海外で発生した営業秘密の窃取に関する報告）
- 第 5 条　Sense of congress.（議会の認識事項）
- 第 6 条　Best practices.（ベストプラクティス）
- 第 7 条　Immunity from liability for confidential disclosure of a trade secret to the government or in a court filing.（政府に対する又は裁判所提出書類における営業秘密の開示行為に関する免責）

文献 15	
文献表題	DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure （営業秘密保護指令）
公表媒体	EU ウェブサイト https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943
著者	欧州連合（EU）
発行者	欧州連合（EU）
公表時期	2016 年 6 月

米国と同様、営業秘密の不正利用行為の拡大及び情報通信技術の発展によるそのようなリスクリスクの増大を受け、企業による知的創造及び革新的なノウハウの保護の 1 つの形態である営業秘密について、これまで EU の法的枠組みで十分な保護がなされていなかったのを踏まえて制定されたものであり、次の各条から構成される。

① 第 1 章：Subject matter and scope（対象事項及び適用範囲）

- 第 1 条：Subject matter and scope（対象事項及び適用範囲）
- 第 2 条：Definitions（定義）

② 第 2 章：Acquisition, use and disclosure of trade secrets（営業秘密の取得、使用及び開示）

- 第 3 条：Lawful acquisition, use and disclosure of trade secrets（営業秘密の適法な取得、

使用及び開示）

- 第 4 条 : Unlawful acquisition, use and disclosure of trade secrets（営業秘密の違法な取得、使用及び開示）
- 第 5 章：Exceptions（例外）

③ 第 3 章：Measures, procedures and remedies（措置、訴訟手続及び司法救済）

＜第 1 節：General Provisions（一般規定）＞

- 第 6 条：General obligation（一般的な義務）
- 第 7 条：Proportionality and abuse of process（比例性及び訴訟手続の濫用）
- 第 8 章：Limitation period（制限期間）
- 第 9 章：Preservation of confidentiality of trade secrets in the course of legal proceedings（訴訟手続の過程における営業秘密の秘密性の保持）

＜第 2 節：Provisional and precautionary measures（暫定及び予防措置）＞

- 第 10 章：Provisional and precautionary measures（暫定及び予防措置）
- 第 11 章：Conditions of application and safeguards（適用要件及び安全性確保措置）

＜第 3 節：Measures resulting from a decision on the merits of the case（事件の本案に関する判断から生ずる措置）＞

- 第 12 章：Injunctions and corrective measures（差止命令及び是正措置）
- 第 13 章：Conditions of application, safeguards and alternative measures（適用要件、案税確保措置及び代替措置）
- 第 14 章：Damages（損害賠償）
- 第 15 章：Publication of judicial decisions（裁判所による判断の公表）

④ 第 4 章：Sanctions, reporting and final provisions（制裁、報告及び最終条項）

- 第 16 条 : Sanctions for non-compliance with this Directive（本指令の不遵守に対する制裁）
- 第 17 条：Exchange of information and correspondents（情報交換及び連絡官）
- 第 18 条：Reports（報告書）
- 第 19 条：Transposition（国内法化）
- 第 20 条：Entry into force（発効）
- 第 21 条：Address（発出）

文献 17	
文献表題	米国における営業秘密保護の現状について
公表媒体	月刊パテント Vol.70, No.9 https://system.jpaa.or.jp/patent
著者	向山　純子（平成 28 年度不正競争防止法委員会第 1 小委員会米国グループ副委員長）ほか
発行者	日本弁理士会
公表時期	2017 年 9 月

平成 28 年度不正競争防止法委員会第 1 委員会米国グループにおいて、「米国での営業秘密保護の動向の調査・研究」に関して検討した結果を示している。これによれば、米国における営業秘密保護に関しては、以下の各点に留意する必要がある。

● 対象となる裁判所は連邦裁判所か州裁判所か
● 基づいている法律は連邦法か州法か
● 救済手段は損害賠償のみか、差止請求も対象とするか
● 陪審制度の適用があるか

さらに、具体的に適用される保護方法として、次の 5 種類を紹介している。

① 統一営業秘密法（UTSA）による保護

営業秘密に関して全米的に統一された保護を与えることを目的として制定されたモデル法であり、不正競争行為に不正な使用、不正な開示に加えて不正な取得行為を含む。救済手段としては、差止め、損害賠償請求（現実損害及び逸失利益）、不当利得返還請求及び合理的なロイヤリティ、さらに故意・悪意の場合は補填的損害賠償の 2 倍までの懲罰的損害賠償及び弁護士費用の賠償を認めている。

② 連邦経済スパイ法（EEA）による保護

営業秘密の不正取得に関して民事規制のみでは十分でないとの観点から、刑事面を規律するために制定された連邦法である。外国政府による、又は外国政府に便益を与えるための経済スパイによる営業秘密の不正取得等のほか、民間の個人・企業による営業秘密の不正取得等が対象に含まれる。EEA による保護においてはおとり捜査の手法が積極的に採用されており、救済手段としては、罰金、懲役、それらの併科、違反から得られた財産の没収が含まれる。

③ 連邦営業秘密保護法（DTSA）による保護

文献 16 に示す連邦法であり、これまで民事上では州法によってのみ保護されていた営業秘密が連邦法によっても保護されることになった点に特色がある。DTSA 特有の制度として、営業秘密の頒布等を防ぐため一方当事者の申立てに基づいて財産の差押命令を裁判所が明示できることが挙げられる。さらに、従業員の転職に対する保護規定を有している点も特色となっている。このほか州法ではディスカバリーの前に盗まれた営業秘密の特定が必要であるのに対し、DTSA ではその必要がなく、営業秘密の保護を求めやすくしている。

④ 国際貿易委員会（ITC）による保護

ITC は米国貿易法を取り扱う連邦準司法政府機関であり、1930 年関税法第 337 条に基づく調査の対象として営業秘密の不正取得等を扱っている。ITC は損害賠償を認める権限を有さない一方で、排除命令又は停止命令の形式による差止命令を認める権限を有する。

⑤ 契約による保護

米国においては、秘密保持義務契約及び競業避止義務契約を締結することにより営業秘密を保護することが一般的に行われていることにも留意する必要がある。

以上の営業秘密に関する保護体制が布かれていることを確認した上で、第 1 委員会米国グループにおいては実際に生じうる事例に関連した情報提供を行うことを目的として、15 項目の質問を作成した。その回答は次項である文献 18 に示されている。

文献 18	
文献表題	日本企業の米国子会社における営業秘密の保護に関する実務的考察
公表媒体	月刊パテント Vol.70, No.9 https://system.jpaa.or.jp/patent
著者	荒木　源徳（モリソン・フォースターLLP パートナー）ほか
発行者	日本弁理士会
公表時期	2017 年 9 月

文献 17「米国における営業秘密保護の現状について」において提起された、平成 28 年度日本弁理士会不正競争防止法委員会第一委員会米国グループによる 15 件の質問に対して、米国法律事務所に所属する弁護士２名による回答を記載している。

① 米国子会社が保有する営業秘密の保護の方法

米国法では、営業秘密として法的保護を受けるために、当該営業秘密の秘密性（非公知性）を保護するための合理的な努力が行われる必要があることから、従業員を雇用する場合、守秘義務及び開示許容要件を明確にした雇用契約書を締結するとともに、これを補完する手段として、営業秘密に関する管理方針・手続を制定する場合が通例である。また従業員が退職する場合、会社の営業秘密に関する方針に従う旨の署名、証拠保全等を行う。

② 米国子会社が営業秘密侵害で訴えられないために必要な措置

他社を退職した従業員を採用する場合、前の会社の営業秘密を持ち込まないことを誓約させることが重要。米国子会社又は日本親会社が他社とライセンス契約の締結ないし交渉を行う場合、営業秘密の保護の観点からその範囲を特定した上で、開示される営業秘密の使用態様や保護の方法等について、具体的かつ明確に定めた秘密保持契約を締結し、遵守することが必要。また営業秘密に該当するソースコード等を含むソフトウェアの開示が求められる場合は、エスクロー制度を活用して保護を図ることも考えられる。

③ 米国子会社が他社に対して営業秘密侵害の訴えを提起する場合

日本企業の米国子会社が他社を営業秘密侵害で提訴する場合、連邦法である営業秘密保護法（DTSA）と州の営業秘密保護法又は不法行為法のいずれに基づく請求をすべきかについて、具体的事案との関係で検討する必要がある。財産差押手続が認められているのは DTSA のみである。またニューヨーク州等の営業秘密法では、従業員に対して転職先で転職前の会社の営業秘密を開示する結果になることが不可避的である業務に従事することを禁止することが可能、カリフォルニア州では意図的な不正取得に対する懲罰的賠償として３倍賠償を認めることがある等、州毎の相違についても考慮する必要がある。

④ 日本親会社への米国裁判管轄権の波及を防ぐための方法

日本親会社が米国子会社を有しているという事情のみでは裁判管轄は認められないが、日本親会社が米国子会社に対して過度の支配を行い、米国子会社が法人としての独立を維持していない場合、又は米国子会社における会社手続が遵守されていない場合には、日本親会社に裁判管轄が及ぶことがある。こうしたリスクを最小限にするには、親会社の米国との接触を最小限にする必要がある。日本親会社が米国子会社との間で、他社の営業秘密にアクセスできるように取引していたと認められる場合は、十分な接触があったとして日本親会社に裁判管轄が及ぶ可能性がある。

⑤ 中国、韓国、台湾企業を米国裁判所で訴えることについて

米国での訴訟はディスカバリー対策に費やす時間及び労力が人材であることから、日本での訴訟とは桁違いの法律費用が必要となることもあって、米国外での訴訟で利用する情報を得るために米国で訴訟提起することは余り行われない。案件の重大性、証拠の重要性などと合わせて慎重に判断する必要がある。

文献 19	
文献表題	アメリカにおける営業秘密の保護(1) －連邦営業秘密防衛法（DTSA）の運用実態と日本の営業秘密訴訟との比較－
公表媒体	知的財産法政策学研究 Vol.53 https://www.juris.hokudai.ac.jp/riilp/journals/
著者	山根　崇邦（同志社大学教授）
発行者	北海道大学
公表時期	2019 年 3 月

米国法制の国際的な影響力及び州法と比較した把握の容易性の観点から連邦営業秘密防衛法（DTSA）に着目し、その制定背景と運用実態、日本における営業秘密訴訟との比較を行った論考の冒頭部分である。

① DTSA の制定背景

DTSA 制定の背景として、以下の各点に示されるように、営業秘密を取り巻く環境変化に既存の法制では十分に対応できないと判断されたことがあるとしている。ゆえに DTSA は「不正利用の州際化に対応するためのアクセス機会の確保（営業秘密訴訟に係る連邦管轄権の創設）」、ならびに「不正利用の国際化及び不正利用のデジタル化に伴う証拠破壊の容易化に対応するための迅速な救済措置の拡充（一方的差押制度の創設）」に最大の意義があるとされる。

- 営業秘密の環境の変化：立法資料より、次の 3 点が認識されていたとされる。
  - 営業秘密の窃取の増加：サイバー攻撃等を通じた営業秘密の窃取が拡大し、雇用の喪失、起業家のイノベーション意欲の減少等、年間 4,800 億ドルの損失を生じている。
  - 不正利用のデジタル化：デジタルデータの拡散を通じて、これまでとは異なる管理方法が求められるようになっている。
  - 不正利用の州際化・国際化：営業秘密の窃取が 1 つの州内にとどまることはまれであり、別の州に持ち出されるケースが増えているほか、営業秘密を窃取した者の国外逃亡を防ぐための迅速な対応が求められている。
- 既存の法制による対応の限界：営業秘密の窃取被害への対応のための既存の 2 つ選択肢（連邦経済スパイ法、州営業秘密法）には、それぞれ次のような限界があったとされる。
  - 連邦経済スパイ法の限界：法律の規定内容よりも、FBI や司法省が捜査及び訴追に統一ことができる資源に限界があることから、損害賠償額が 10 万ドルを超える事例に限られるなど運用上の制約がある。
  - 州営業秘密法の限界：急増する営業秘密の窃取事例において、窃取された営業秘密が 1 つの州のみにとどまることは希であり、別の州に持ち出されたり、複数の州で使用されたりすることで、ディスカバリーや文書送達を効率的に命じることができない等、対応に苦慮することが多くなっている。同様に国際化への対応能力にも限界があるほか、不正利用のデジタル化に伴う証拠の隠蔽や破壊の容易化への対応にも限界がある。

② DTSA の規定内容とその運用実態

営業秘密訴訟に関するこれまでの調査研究及び著者自身による調査結果をもとに、DTSA の運用実態と日本国内での法運用の実態との比較として、次の結果を示している。

- DTSA 施行の影響
  - DTSA 施行後、連邦地方裁判所に提起される営業秘密訴訟の件数は 30%以上増加。
  - DTSA 訴訟の多い裁判地としては、シカゴ、サンフランシスコ及びシリコンバレー、ロサンゼルス、ニューヨーク、フィラデルフィア等が挙げられている。
  - DTSA 訴訟の被告としては（元）従業員に対するものが全体の 62%、退職従業員の新雇用主を対象とするものもが 40%（従業員と共同で訴追対象となる場合が多い）、ビジネスパートナーに対するものが 34%と続いている。
- DTSA で保護対象となる営業秘密
  - DTSA によって保護される営業秘密の保護要件は、「保有者がその情報の秘密性を保持するために合理的な措置を講じていること」、「当該情報がその開示や使用から経済価値を得ることのできる他の者に一般的に知られておらず、かつその者が正当な手段によっては容易に確認することができないこと」及び「それによって当該情報が現実にまたは潜在的に独立した経済的価値を有すること」の 3 点とされ、日本における保護要件との間で差異はない。
  - 一方で、日米の営業秘密訴訟における営業秘密要件に基づく請求棄却率や請求棄却事例における棄却理由の分布を比較すると、両国で大きな差異が見られる。この原因として、2000 年代に入ったあたりから 2009 年頃まで、日本国内で秘密管理要件が厳格に判断されていたことの影響が大きいとしている。

文献 20	
文献表題	アメリカにおける営業秘密の保護(2) －連邦営業秘密防衛法（DTSA）の運用実態と日本の営業秘密訴訟との比較－
公表媒体	知的財産法政策学研究 Vol.55 https://www.juris.hokudai.ac.jp/riilp/journals/
著者	山根　崇邦（同志社大学教授）
発行者	北海道大学
公表時期	2020 年 3 月

文献 19 から続く DTSA に関する論考の続編である。本項以降の論考については、本調査の実施時点で公表されていない。

② DTSA の規定内容とその運用実態（続き）

- DTSA で規制対象となる営業秘密の不正利用行為
  - DTSA では、これまでの統一営業秘密法（UTSA）における不正利用の類型に合わせる形で、不正利用を取得行為と開示・使用行為の 2 つに大別して規定している。一方、日本では主に一次行為者の行為か転得者の行為かという観点から類型を規定しており、規律範囲に差異が存在する。
  - DTSA 訴訟における不正利用肯定例のうち、7 割以上が不正取得の事案である。さらにその 9 割近いケースでは営業秘密の保有者に対し秘密保持義務を負っている者が不正取得の

行為者として認定されている。これは、米国では使用者が従業員と秘密保持契約を交わすことが一般的であり、同契約の中で機密情報の目的外複製・保存の禁止や退職時の返還・消去を義務づける場合が多いことが影響しており、将来競合他社で使用する目的で営業秘密をダウンロードする行為が、正当なアクセス権限を有していても不正取得に該当するとされる裁判例も示されている。

- 不正使用・開示に係る規律の運用実態に関しては、日米で大きな差異は見られない。

文献 21	
文献表題	営業秘密の保護の国際的側面に関する覚書
公表媒体	特許研究 No.69 https://www.inpit.go.jp/jinzai/study/
著者	鈴木　將文
発行者	独立行政法人工業所有権情報・研修館（INPIT）
公表時期	2020 年 3 月

我が国の不正競争防止法並びに米国と EU の制度を素材として、最近の営業秘密保護制度と越境的行為の関係について、国外犯や営業秘密侵害品の流通規整に関する規定を対象に検討した内容をまとめたものである。

我が国の不正競争防止法に関しては、2 条 1 項 10 号における営業秘密侵害品の範囲に関する認定が容易ではなく、越境的な行為の場合に行為者にとって予見可能性が低い問題がより深刻になることが懸念されるとしている。また刑事罰については日本国内において事業を行う営業秘密保有者の営業秘密に係る国外の行為が罰せられる点に議論の余地がある点、水際措置において専ら行政府の判断に委ねられる中で、営業秘密侵害品の輸出入について侵害品該当性判断の難しさや、秘密の保持手続の不完全性が問題を生じさせる懸念についても指摘している。

一方、米国の経済スパイ法及び営業秘密の民事的保護を図る法律（DTSA）の対象となる永劫秘密は州際通商及び国際通商向けの商品・役務に関係する営業秘密とされ、我が国の不正競争防止法 2 条 1 項 10 号の定める営業秘密侵害品の流通に係る規定を設けていない。DTSA が外国の行為に適用されるかは議論の最中であり、関税法 337 条に基づく国際貿易委員会（ITC）による排除命令には予見可能性に欠ける問題があるとする。また EU が 2016 年に制定した営業秘密保護指令に関しては、我が国と営業秘密侵害品の範囲が異なるほか、主観的要件がより緩やかであり、刑事罰や水際措置の規定がない等の相違点を指摘している。

以上の検討をもとに、営業秘密侵害品に関する規整については、対象行為の要件に不明確な点が多く見られることから、その制度・運用については慎重な検討を要すると結論づけている。

2.4.5 文献調査結果から判読される事項

前述の文献を整理・検討した結果、次のような傾向が判読されることから、裁判例の分析及びアンケート調査結果の分析の際に留意して実施することとした。

- 裁判例における営業秘密性、特に秘密管理性の認定に関して、調査対象の文献での論考の範囲内では過去 5 年間程度での変化を指摘するものは見られない。
- 中小企業等が原告となっている民事訴訟において、秘密管理性に関して「営業秘密管理指針」や「秘密情報の保護ハンドブック」等において示されている秘密管理措置等の要件を満たしていない場合（例：秘密である旨の表示なし）でも、営業秘密として認定される例がある。
- 裁判所は、営業秘密として保護すべき事案かどうかを営業秘密情報の管理状況に限らず、行為の悪質性や侵害行為の有無等を含めて判断しており、「社外秘表示があったかどうか」といった個別要素のみを取り出して判断の妥当性を論じることは適切ではない。
- 米国及び EU において、2016 年にそれぞれ営業秘密保護のための法整備がなされており、国内でも 2015 年及び 2018 年に不正競争防止法の改定が行われている等、国際的に調和のとれた営業秘密の保護の実現に向けた取組が進められているが、現状において、国毎での営業秘密の保護ならびに不正競争行為の規制に関する扱いには相違がある。

2.5 裁判例調査

2016 年調査以降の不正競争防止法における営業秘密管理性が争点となった裁判例について調査及び分析を行った結果を示す。

2.5.1 裁判例選定方針

本調査で分析対象とする裁判例は、2016 年（平成 28 年）8 月 24 日以降に確定したもののうち、営業秘密性の 3 要件（秘密管理性、有用性、非公知性）の扱いが争点となったものについて、以下の条件のもとで収集を試みた。しかしながら、このうち(4)を満たすものについては調査した範囲内で該当するものが存在しなかったため、分析対象には含まれない。

(1) 刑事・民事の双方を対象とする。
(2) 結果的に営業秘密と認められなかった例も含む。
(3) 民事事件において原告の属性は問わない。すなわち、営業秘密情報の作成者ないし所有者以外を原告とする場合も含む。
(4) 次の要件を満たすものは可能な限り網羅するように努めることとする。
  - 2018 年（平成 30 年）11 月 29 日（改正不正競争防止法施行日）以降に、技術的制限手段の有効性が争点となったもの
  - 2019 年（令和元年）7 月 1 日（改正不正競争防止法施行日）以降に、「限定提供データ」の扱いが争点となったもの
  - 2019 年（平成 31 年）1 月 23 日（営業秘密管理指針改訂版の公表日）以降に、同指針の記載内容に関する争点を含むもの

なお、民事事件において、不正競争行為を理由とする差止請求や損害賠償請求を行う訴訟は多数見られるものの、この中には従業員の競合他社への転職ないし起業、競合企業による類似製品・サービスの提供等で不利益を被った原告が、実際には営業秘密情報の不正使用に起因する事件ではないにも関わらず、不正競争防止法を適用するために秘密情報である旨を主張するものが含まれる。このような裁判例では、原告において事業に用いる情報を秘密として管理しようとする実態が伴わないことから、判決において秘密管理性や非公知性を明確に否定される傾向が見受けられる。そこで、本調査における裁判例の選定にあたっては、原告において営業秘密として管理しようとする意図が示されているものを中心に抽出することとした。

2.5.2 裁判例に関する調査結果一覧

調査対象とした裁判例の一覧を次表に示す。なお表内に記載した各種の記号の示す意味は、表末に示した通りである。

表 2.5-1　調査対象とした裁判例の一覧

No.	裁判所 判決日	民事／刑事	情報の種類	原告企業規模	秘密管理性の確保のための対策実施に関する認定有無							「認識」の表現	競業避止義務の有効性	営業秘密性の構成要件			営業秘密該当性	備考
					アクセス制限	施錠管理	パスワード設定	秘密区分表示	就業規則	研修	誓約書等			秘密管理性	有用性	非公知性		
1	大阪地裁 H29.1.12	民	営	?	○	○	○	－	－	○	○	－	－	○	○	○	○	
2	東京地裁 H29.2.9	民	技	小	○	○	－	○	○	－	○	B	○	○	○	○	○	※1
3	大阪地裁 H29.10.19	民	技	中	○	－	－	△	○	－	○	B	－	○	○	○	○	
4	大阪高裁 H30.5.11	民	技	中	○	－	－	△	－	－	○	B	○	○	○	○	○	※2
5	大阪地裁 H30.3.5	民	営	小	×	－	－	－	○	－	○	B	○	○	○	○	○	※3
6	大阪地裁 H30.3.15	民	営	?	○	○	○	－	－	－	○	B	○	○	○	○	○	
7	大阪地裁 H30.3.15	民	技	小	×	－	－	－	○	－	－	B	－	×	－	－	×	
8	大阪高裁 H31.2.14	民	技	小	△	－	－	×	－	－	－	B	－	×	－	－	×	※4
9	知財高裁 H30.3.26	民	技	小	○	－	○	○	○	○	－	B	－	○	○	○	○	※5
10	大阪地裁 H30.4.24	民	技	小	×	－	－	－	－	－	－	－	－	×	－	－	×	※6
11	東京地裁 H30.9.27	民	技	?	－	－	－	×	－	－	－	B	－	×	－	－	×	
12	東京地裁 H30.11.29	民	技	－	－	－	－	－	－	－	－	B	－	○	○	○	○	※7
13	大阪地裁 H30.12.6	民	技	小	×	－	×	－	○	－	－	B	－	×	－	－	×	
14	東京地裁 H31.1.18	民	営	?	○ ×	－	○ －	－	○ －	○ －	○ －	B	－	○ ×	○ －	○ －	○ ×	※8
15	東京地裁 H31.3.19	民	技	中	×	－	－	－	－	－	△	－	△	×	－	×	×	※9
16	東京地裁 H31.4.24	民	技	大	○	－	－	－	○	○	○	B	－	○	○	○	○	※10
17	知財高裁 R1.8.7	民	技	?	×	×	－	△	○	－	○	B	－	×	－	－	×	
18	大阪地裁 R2.10.1	民	営	大	△	－	○	－	○	○	○	B	－	△	△	△	△	※11
19	東京地裁 R2.11.17	民	営	?	×	×	－	×	○	－	○	B	－	×	－	－	×	
20	東京高裁 H29.3.21	刑	営	－	○	×	×	×	○	○	○	A	－	○	○	○	○	※12
21	東京高裁 H30.3.20	刑	技	－	－	－	－	－	－	－	－	B	－	○	－	－	－	※13
22	名古屋地裁 R1.6.6	刑	技	－	○	×	×	○	○	－	○	－	－	－	－	－	－	※14

＜表中記号の凡例＞

刑事／民事	刑＝刑事事件、民＝民事事件

情報の種類	営＝営業情報に相当する営業秘密、技＝技術情報に相当する営業秘密
原告企業規模（民事のみ）	大＝大規模企業（従業員 301 名以上）、中＝中規模企業（従業員 51～300 名）、小＝小規模企業（従業員 50 名以下）、？＝不明
秘密管理性の確保のための対策実施に関する認定有無	○＝有効と認定されたもの、△＝一部有効と認定されたもの ×＝有効と認定されなかったもの、－＝判断がなされていないもの
競業避止義務の有効性	
「認識」の表現	営業秘密管理指針における「秘密管理性」に関する総説の内容を原告が意識している可能性を考慮し、原告による秘密管理性の主張における「認識」という表現の有無で以下のように分類：A＝「容易に認識」という表現があるもの、 B＝「認識」という表現があるもの、－＝いずれの表現もないもの
営業秘密性の構成要件	○＝肯定、△＝一部肯定、×＝肯定されず、－＝判断がなされていない
営業秘密該当性	

※1　文献調査における文献 5 において、「婦人靴木型事件」と称されている事件。当該業界内で木型が事業の生命線ともいうべき重要な価値を有することが認識されるとともに、本件オリジナル木型と同様の設計情報が化体されたマスター木型が厳重に管理され、こうした木型に関する秘密情報を通常従業員が取り扱えないようにしていたことから、従業員は原告の秘密情報であると認識していたと判断されている。

※2　裁判例 No.3 の事件の控訴審であり、控訴棄却とされている。

※3　原告における顧客情報へのアクセス制限の程度は明らかになっていないが、原告は小規模企業であり、営業所内でアクセス制限が設けられていないとしても、それをもって対外的にも秘密でない扱いがされていたとはいえないとして、他の就業規則や誓約書徴求等の状況と合わせて秘密管理性が肯定されている。

※4　裁判例 No.7 の事件の控訴審であり、控訴棄却とされている。

※5　文献調査における文献 7 において、「ケーブルテレビ関連機器事件」と称されている事件。プログラムの営業秘密性に関する裁判所の判断例として検討対象となっている。原告は原審において著作権侵害に基づく差止、廃棄及び損害賠償を求めていたが、控訴にあたって著作権に基づく訴えを取り下げた。判決において、PC ソースコードについては、営業秘密該当性を肯定した上で、ソースコード中に非実行化された記載等、控訴人製品において意味をもたない記載がある等の事実をもとに不正な開示と認定し、使用差止と損害賠償請求について原判決変更・一部認容したのに対し、マイコンソースコード、回路図データ、部品リストデータ、基板データについては不正使用があったとは認められず、控訴棄却された。

※6　文献調査における文献 13 にて秘密管理性が否定された事例として紹介されている事件。原告において製造販売している生春巻きの製造方法の営業秘密該当性が争点となったが、第三者の出入り管理は食品衛生管理のための管理と変わらず、被告が営業秘密を入手した手段は原告代表者による口頭での説明を通してとしか考えられないということで秘密管理性を否定され、全部棄却。

※7　文献調査における文献 7 において、「字幕制作ソフトウェア事件」と称されている事件。プログラムの営業秘密性に関する裁判所の判断例として検討対象となっている。原告は当初著作権侵害で提訴したが控訴の後、棄却で確定した後、本訴訟を提起した結果、差止及び損害賠償請求について一部認容の判決を得た。

※8　争点となった営業秘密のうち、原告が運用する顧客情報管理システムで管理されていた顧客情報については営業秘密該当性が肯定されたが、被告に提供された顧客の連絡先が記載されたメモについては、メモに記載された内容が検証困難であったこともあって営業秘密該当性が否定された。

※9　原告が被告の一部に対して課していた退職後 3 年間の競合関係に立つ事業者への転職を禁止する誓約書について、競業避止義務を課すことに対する代替措置も講じられていないことから、公序良俗に反するとして無効とされた。

※10 新日鐵住金（当時）の元社員による、株式會社ポスコ（POSCO）への技術情報流出事件の民事訴訟。

※11 原告の主張する営業秘密情報のうち、パッケージリフォーム商品を購入した顧客に対し、守秘義務を課すことなく公布している書面等、一部の情報を除いて営業秘密該当性を肯定。

※12 文献調査における文献 8 において、「ベネッセ顧客情報流出事件」と称されている事件の控訴審。営業秘密該当性は肯定されたが、被害が拡大したことの一因として、顧客情報の管理主体における対応の不備があり、落ち度は大きく、ひとえに被告の責めに帰するのは相当でないとの判断がなされたことで、原判決破棄、一審よりも減刑の判決となった。

※13 文献調査における文献 8 において、「日産自動車商品企画情報事件」と称されている事件の控訴審。勤務先会社のサーバーに保存されていたデータファイルを同業他社への転職直前に自らのハードディスクに複製した行為に対し、被告が記念写真の取得が目的と主張するも、自動車の商品企画等に関するものが大半を占めていることから、「不正の利益を得る目的」と認定した第一審判決を支持。上告でも覆らず確定。

※14 文献調査における文献 8 において、「超硬工具メーカーマニュアルデータ事件」と称されている事件。営業秘密の区分管理、就業規則等における漏えい禁止等の措置をもとに秘密管理性を肯定。

2.5.3 調査結果より観察される事項

前ページに示した裁判例の抽出及び分析の作業を通じて、次のような傾向が明らかとなった。

- 文献調査における 2.5 項で示した通り、「営業秘密管理指針」等で示されている秘密管理措置が必ずしも適切に講じられていないとみなされる場合でも、裁判例 No.5 のように小規模企業であることを考慮して秘密管理性が肯定されている事例が見られる。裁判例 No.12 においては、争点が原告の保有するソースコードの不正使用有無に置かれ、ソースコードの営業秘密性を被告側が争点としなかったこともあり、秘密管理措置に関する裁判所の判断が示されないまま原告の主張する営業秘密該当性が肯定されている。このような事例を含め、営業秘密該当性に関する判断において、2016 年 8 月以前の傾向と異なる要素は見当たらない。
- 裁判例 No.9 と裁判例 No.12 はソフトウェアのソースコードを営業秘密として扱い、その不正な使用を不正競争行為として訴えた事件である。両者とも当初著作権違反で提訴していたものが棄却ないし取り下げを経て不正競争行為差止請求を行ったものであり、いずれも原告の主張が一部認められ、差止及び損害賠償を命じる判決が示されている。この結果より、文献調査における文献 7 における論考の通り、営業秘密侵害における不正使用の範囲は、著作権侵害における複製又は翻案の範囲よりも広い概念であることがわかる。著作権法では、プログラムの著作権は 15 条などにより一般の文学などより広い範囲が保護対象となっているが、営業秘密の場合は不正使用の概念をさらに広く捉えていると解釈される。
- 本調査では、営業秘密管理指針の「秘密管理性」において「従業員が当該秘密管理意思を容易に認識できる必要がある」との総説を原告が意識している可能性を考慮し、原告による秘密管理性の主張に「容易に認識」ないし「認識」の表現があるかどうかの分析を行った。この結果、調査対象裁判例のうち、「容易に認識」の表現があったものは 1 事例（刑事事件）にとどまったが、「認識」については 8 割弱の事例に含まれることが確認された。ただし、「秘密であることを認識」という表現は営業秘密管理指針に限らず一般的に用いられていることから、今回の傾向をもって原告の多くが営業秘密管理指針を意識していると結論づけることは難しいと思われる。
- 営業秘密性の構成要件のうち、有用性については一般に事業で用いられる情報であれば有用であることを否定されることは少ないとされるが、裁判例 No.18 における 1 種類の情報のみ、「名称を見ても，それがいかなる意味において現在又は将来の経済活動に役立てることができるものであるか，およそ判然としない」ことから「事業活動に有用なものであるとはいえない」とされ、有用性を否定されることで秘密管理性等の考慮に及ぶことなしに営業秘密該当性を否定される結果が示されている。

2.5.4 分析結果総括

以上の分析をもとに、調査結果は次のように総括される。

- 秘密情報該当性に関して、2016 年度調査において実施された裁判例についての分析結果と比較して、異なる傾向は示されておらず、新たな方向性を示すような裁判例も現れていない。
- 秘密管理性の判断においては、安全管理措置のほか、企業規模等を含めた総合的な判断がなされており、すべての企業に対して同レベルの情報管理対策が求められているわけではない。
- 2018 年改正の不正競争防止法において新たに盛り込まれた技術的制限手段に関する不正競

争行為の有効性、及び限定提供データの扱いが争点となった判決はいずれも調査対象とすることができなかった。特に、限定提供データを対象とする事項の施行（2019 年 7 月 1 日）から 2 年に満たないこともあり、引き続き注視する必要がある。

3 調査結果についての考察

3.1 仮説の検証

2.1 項において示した仮説について、調査結果をもとに検証を行う。各項目の小見出しは 2.1 項で設定した仮説のタイトルであるため、本調査結果を説明するものではないことに留意されたい。

3.1.1 前回からの変化

(1) 内部不正対策は進展したか？

① 秘密保持に関する誓約書の徴求や就業規則の見直しを行う企業が増加

アンケート結果の図 2.2-65 及び図 2.2-67（47-48 ページ）に示すように、役員を対象とする秘密保持契約を締結している企業は 36.4%から 44.6%（8.2%増）、従業員とは 46.1%から 56.6%（10.5%増）といずれも増加している。図 2.2-98（63 ページ）で情報管理に関する規程・手続等の見直しを行った動機として経営層の指示が高いことを踏まえると、仮説の通り営業秘密漏えいに関する報道等を受けて、経営層が内部不正による情報持ち出し等の被害抑制のため、秘密保持契約の締結等の対策を講じる企業が増えたものと考えられる。

② 内部不正を原因とする情報漏えいインシデントの発生は微減

アンケート調査結果の図 2.2-26（28 ページ）に示されているように、退職者による秘密情報持ち出しは 2020 年においても主たる要因となっており、減少傾向にはない結果から、内部不正による情報漏えいが微減しているのではないかとの仮説は成立しなかった。一方で、図 2.2-59（44 ページ）や図 2.2-62（46 ページ）に示すように情報の不正な持出を防ぐための対策や漏えいを生じさせにくい環境をつくるための対策のような、内部不正の検知技術の導入は進んでいるが、これはこのように内部不正インシデントが引き続き重視すべき脅威と認識されていることの表れと考えられる。

③ クラウドサービス上の秘密情報の不正利用対策は進展していない

アンケート調査結果の図 2.2-86（56 ページ）に示すように、企業が契約するクラウドサービスにおける情報漏えい防止対策は内部不正を意図するよりも、アクセス権限の設定ミスやサイバー攻撃に備えたものが中心となっており、不正利用対策が進展していないのは仮説の通りである。一方で、従業員が勝手に無料のクラウドサービスを利用し、データをアップロードすることで不正な持ち出しを実現するようなシャドークラウドについては、図 2.2-88（58 ページ）のように大規模企業に関して言えば半数近い企業において何らかの対策が進んでおり、クラウドサービスを用いた不正利用の脅威が企業において認識されていることがわかる。

(2) 中小企業における情報管理対策は進展したか？

① 情報漏えいの生じた企業の比率はやや増加

アンケート調査結果の図 2.2-10（19 ページ）に示すように、情報漏えいインシデントが発生した（可能性を含む）と回答した企業は 2016 年度調査における比率よりも 4 割程度減少し、

仮説を否定する結果となった。しかしながら、図 2.2-7（18 ページ）のように、企業規模の構成比でみると 2016 年調査では零細・小規模事業者の比率が多く、本調査は中規模企業の比率が多いという相違があるため、この母集団の相違がこの結果に影響している可能性がある。もっとも、零細・小規模企業では適切なサイバーセキュリティ対策を実施している企業の比率が少ないためサイバー攻撃の被害を受けやすく、中規模以上の企業ではアクセスログの分析などを通じてインシデントの検知能力が高いことで零細・小規模企業よりも巧妙なサイバー攻撃に気づきやすいという両面の特徴があり、総合的に考慮すると情報漏えいの発生が減少傾向にあることは確かであると考えられる。

② 情報漏えいの発生頻度は中小規模企業よりも大規模企業において高い

アンケート調査結果の図 2.2-12（20 ページ）に示す通り、仮説通りの結果が得られた。同図における「わからない」の比率の比較からも、大規模企業のほうが情報漏えいインシデントの検知能力が高いと推定される。一方で、内部不正を通じた情報漏えいインシデントは具体的な被害発生の事実そのものを通じて把握されることが多く、こうしたインシデントについては企業規模による相違は小さいと考えられる。

③ 連携先やサプライチェーンを通じた情報漏えいが増加

アンケート調査結果の図 2.2-26（28 ページ）に示すように、2016 年度調査において取引先や共同研究先からの漏えいは全体の 11.4%を占め、主要な要因の 1 つと位置付けられていたが、本調査では当該選択肢への回答は 2.7%にとどまり、仮説とは反対に大幅な減少の傾向がみられた。この背景としては、(1)①と同様に企業間でセキュリティリスクを認識して秘密保持契約を締結し、互いに遵守する企業が増えた可能性が考えられる。

④ 漏えいする情報の種類は引き続き顧客情報・個人情報が最多

アンケート調査結果の図 2.2-14（21 ページ）に示すように、本調査においても仮説の通り顧客情報の漏えい事例が最多となっている。アンケート上での回答方法が変更となっているため単純な比較はできないが、漏えいした情報全体に占める顧客情報の比率は減少している。

⑤ 営業秘密のレベル別管理を行っている企業は増えていない

アンケート調査結果の図 2.2-34（32 ページ）に示すように、2016 年度調査と比較して営業秘密のレベル別管理を行っている企業は 23.1%から 24.0%へと若干増加している。とはいえ顕著な増加とはいえず、おおむね横ばい傾向にあるといえる。この背景と対策については、重要な論点であると考えられるため第 4 章にて詳述する。

⑥ 企業内でルールが適切に運用されているとは限らない

アンケート調査結果の図 2.2-38（33 ページ）に示すように、営業秘密管理に関して「厳密な運用の徹底」「ある程度厳密に運用」以外の選択肢を選んだ回答者が 4 割程度存在しており、仮説を概ね裏付ける結果が得られている。なお、同図での経年比較については、本調査で選択肢を増やしたことでその影響を受けていることが見込まれるため、単純な比較はできない。

(3) 情報管理に関する強化のきっかけはあったか？

① 情報管理強化のきっかけは取引先からの要求が最多

アンケート調査結果の図 2.2-98（63 ページ）に示すように、企業における情報管理の見直しのきっかけは「経営層の指示」が最多であり、仮説で最多とした「取引先からの要求」は 6 位、「インシデント未遂」が 7 位となるなど、仮説と大きく異なる結果となった。この背景として次のような要因が影響していることが考えられるが、企業インタビュー調査ではこれを裏付ける情報を得ることはできなかった。

- 経済産業省や IPA で普及促進を図っている『サイバーセキュリティ経営ガイドライン』による啓発効果
- 経営層が参加する活動（商工会議所、商工会等）による啓発効果
- 営業秘密の不正利用に係る事件報道等に接した経営層によるリスクの認知

(4) 「秘密情報の保護ハンドブック」を活用している企業では、同ハンドブックに対して追加的なニーズが潜在的にあるのではないか？

① 現行ハンドブックに記載のない対策に関する紹介へのニーズ出来

アンケート調査結果の図 2.2-123（76 ページ）に示すように、以下の 2 例についての要望が最多となっている。

- テレワーク等における営業秘密保護：これまでの考え方では対応できない情報漏えいリスク等についての情報提供が求められていると考えられる。
- 規程等のサンプルの提供：インタビュー調査において、情報管理のルール等の策定が負担との意見が示されており、このような策定作業の負荷を軽減するための情報提供が求められていると考えられる

このほかの要望としては、「企業における取組事例の紹介」「クラウドにおける情報管理対策」など、上述と同様に実務に直結した情報提供を求める意見が多くなっている。

3.1.2 法改正の影響

(1) 不正競争防止法改正の効果はあったか？

① 一部の企業が限定提供データとして保護することを前提とする契約ひな型等を整備

アンケート調査結果の図 2.2-47（38 ページ）に示すように、少数ながら「限定提供データ」に対応した規程を整備する企業が現れている。このグラフで特徴的なのは、製造業では大規模企業のほうが中小規模企業よりも限定提供データに対応した管理を行っている比率が高いのに対し、非製造業ではその逆で中小規模企業において限定提供データに対応した管理を行っている比率が高いことである。この原因を精査するため、対象を中小規模企業に限定し、業種別のクロス集計を行った結果を次ページ図に示す。同図を見ると、「情報通信業」「運輸業」「卸売・小売業」において限定提供データに対応した管理を行っている比率が高く、「情報通信業」では半数にも及んでいることがわかる。

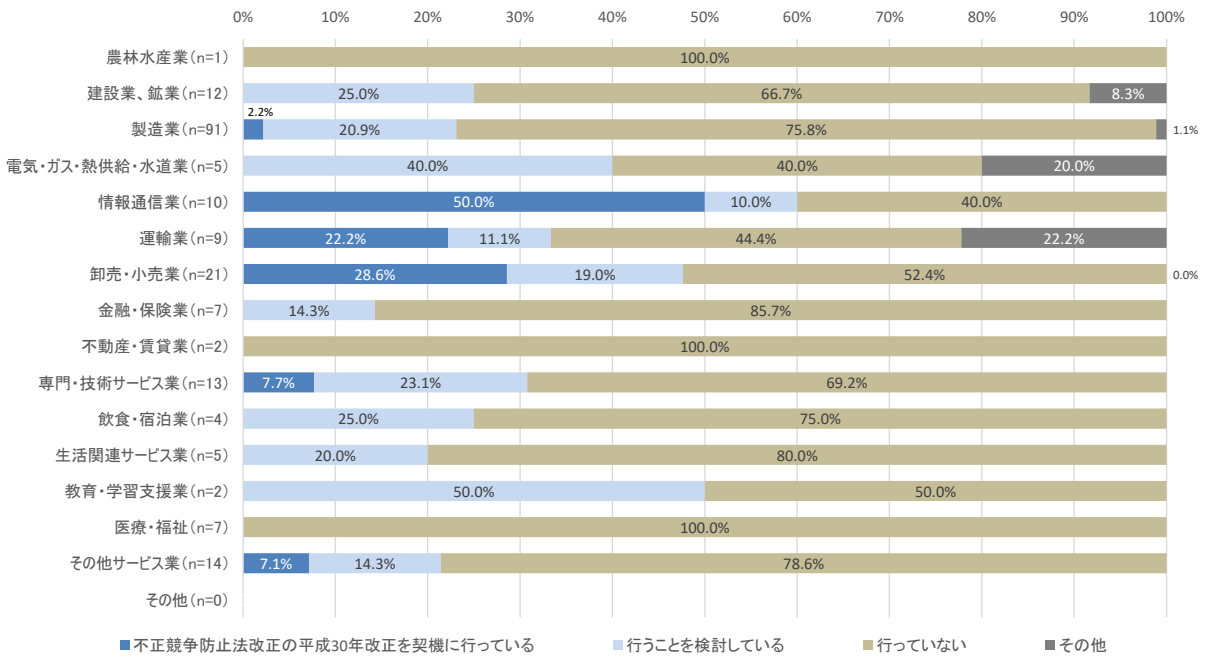

図 3.1-1　限定提供データを考慮した管理の実施状況（中小規模事業者に限定した業種別クロス集計）

このような結果が得られる背景として、次の２つの要因が想定される。

- AI 学習データを扱うスタートアップ企業等が、データ提供元企業との契約に際して適切な管理を保証する規程や手続の整備を求められている可能性
- いわゆる下請企業が、発注元企業からの要請のもとで、発注元企業と同等の規程や手続を整備している可能性

一方、限定提供データの管理を目的として実施している対策としては、図 2.2-50（39 ページ）に示すように従業員を対象とした説明会や講習の開催が多く、仮説で想定した契約ひな型等の策定を行っている企業はわずかであった。

なお、有識者へのインタビューにおいて、図 2.2-47 に示す結果は実際に相談を受けている状況と比較して多いとの指摘があった。この背景としては、次のような可能性が考えられる。

- 前述のように企業が取引先や発注元からの要請のままに、弁護士等に相談することなく対応する規程等を整備しているため、対応状況が顕在化していない可能性
- 企業の知財部門で対応しており、法務部門で扱っていない可能性
- 不正競争防止法の定める限定提供データでなく、字義から「相手を限定して提供するデータ」のことと解釈して回答が行われている可能性

② 限定提供データを対象とした不正競争行為を認める裁判例の出現

仮説においても実際に出現する可能性は小さいとしていたが、裁判例調査の結果、調査範囲内において限定提供データの要件を満たす営業情報に対する不正競争行為を認める裁判例は存在しなかった。

③ 技術的制限手段の効果を妨げる不正競争行為を認める裁判例の出現

②と同様、技術的制限手段の効果を妨げることを目的とした代行サービスを不正競争行為とする裁判例は調査範囲内において存在しなかった。

(2) 営業秘密に関する訴訟・判決に変化は見られるか？

① 秘密管理性の認定に係るアクセス制御方法の有効性判断に関して新たな裁判例が出現

裁判例調査の結果、仮説で想定したようなアクセス制御方法の有効性判断に関して新たな裁判例は出現しておらず、直近５年間の裁判例における営業秘密該当性に関する判断は、それまでの傾向と変わっていないことが確認された。また、新たなアクセス制御技術に基づく製品・サービスによって保護されている営業秘密についての判断もなされていない。

② 非公知性の認定に係る情報の管理方法に関する判断を含む新たな裁判例が出現

①と同様、営業秘密の非公知性に関して新たな判断を示すような裁判例は出現していない。

③ 欧米の営業秘密保護に係る判例が国内にも影響

調査対象とした裁判例において、欧米における営業秘密に関する法制度や海外裁判所の判断について言及するものは存在しなかった。

3.1.3 ニューノーマル環境での営業秘密管理状況等

(1) ウィズコロナ、ポストコロナで課題や対策は変化しているか？

① 国内企業のうち 2～3 割程度がコロナ禍で情報管理のルール見直しを実施

アンケート調査結果の図 2.2-106（67 ページ）に示すように、回答企業の２割がコロナ禍をきっかけとしてテレワーク等における情報管理のルールを定め、３割弱が暫定または例外措置としてテレワークにおける注意事項を周知している。仮説では以前から対応済みの企業が 2 割、今回暫定ないし例外の扱いを定めた企業が 3 割と想定したことを踏まえると、想定よりはやや少なめであるものの、概ね仮説に近い形で情報管理に関するルールの見直しが実施されていることが確認された。

② テレワークの導入で営業秘密該当性が損なわれる可能性の認知が進んでいない

インタビュー調査を含めて、本項目を直接検証することが可能な調査を実施するには至らなかったが、アンケート調査結果の図 2.2-109（68 ページ）に示すように、テレワークにおける営業秘密の取扱いに対応した対策として、最も多く選択されているのが「ネットワーク上での情報保護対策」であり、次いで「第三者が秘密情報にアクセスしないようにする対策」となった。これらの対策は適切に実施されない場合に営業秘密の外部への漏えいにつながる恐れがあるものであり、実施されているという事実からの推察として、テレワークの導入で営業秘密該当性が損なわれる可能性の認知は企業において一定程度なされているとみなすことが可能と考えられる。

③ テレワークの導入を通じて企業におけるペーパーレス化が進展

アンケート調査結果の図 2.2-114（72 ページ）の⑤に示すように、ペーパーレス化については他の対策と比較して進展しているとはいえない。しかしながら、同図ではテレワーク実施におけるペーパーレス化について尋ねているわけではなく、インタビュー調査においては複数の企業から、テレワーク時には紙媒体の営業秘密の持ち出しを禁じているとの回答を得ており、仮説で想定している状況は概ね実現しているものと考えられる。

④ クラウドを通じた秘密情報の共有が進む一方、その不正利用対策は不十分

アンケート調査結果の図 2.2-83（55 ページ）に示すように、全体で２割程度の企業はクラウドサービスを用いて情報共有を行っていることがわかる。さらに、図 2.2-84 によれば、企業規模が大きくなるほどクラウドサービスの活用度が高い傾向にあることから、今後は中小規模企業にも普及していくことが見込まれる。

一方、クラウドサービスを通じた不正なデータ流出に備えた対策については、図 2.2-86 によれば不正操作の証跡確保に相当する「ログ分析の実施」を実施している企業は共有を行っている企業の 24%にとどまるなど、仮説の通り十分な対策が講じられているとはいえないものの、対策の必要性を意識している企業は一定の比率で存在していることが確認された。

3.2 企業における営業秘密管理に関する課題

これまでの分析・調査結果をもとに、企業における営業秘密管理の現状に関する課題について分析・考察する。

(1) 企業による現状認識

はじめに、アンケートに回答した企業が営業秘密情報の管理に関してどのように認識しているかについて分析する。

① 脅威と感じられている事項

アンケート調査結果の図 2.2-32（31 ページ）に示すように、回答者全体で見ると自社における「体制の不備や担当者のスキル不足」が最多である。ただし、情報管理に関する成熟度別に見ると、2.2.5.2(4)に示したように、成熟度高の企業の場合は「外部からの標的型攻撃」「新たな環境において営業秘密を扱うこと」など未知の要素を含む脅威に関するもの、成熟度低の企業の場合は「ルールの不備」など、そもそも情報管理を行うための体制や仕組みが未整備であることが上位に位置付けられており、成熟度中及び低に相当する企業においては、新たな脅威にどう対応するかよりも、既知の脅威に対応するための体制や仕組みができていないことそのものが、情報管理上の脅威となっていることがわかる。

② 企業が課題と認識している事項

アンケート調査結果の図 2.2-42（35 ページ）に示すように、回答者全体でみると「対策の費用対効果を明示しにくい」「従業員にルールを徹底されることが難しい」「対策に要するコストが高額」等、管理上直面する様々な課題が挙げられている。①と同様、情報管理に関する成熟度毎に分析すると、図 2.2-130（82 ページ）に示すように、成熟度高の企業においては外部要因や対策コストに関すること、成熟度中低の企業においては従業員へのルール遵守徹底などが相対的に重い課題として認識されており、回答企業において、営業秘密管理の観点で本来やるべきことができていないことが課題として自覚されていることがわかる。

(2) 企業における対策実施状況から示唆される課題

上述のとおり、営業秘密情報の漏えいを防ぐための体制の構築や対策の実施が十分にできていないことは、情報管理に関する成熟度が中や低の企業における課題となっている。企業における営業秘密の侵害行為に対する法的救済の観点からは、これとは別に、営業秘密に対する不正アクセス等の行為が行われたことの証拠を確保することも重要である。具体的には、秘密情報に対するアクセスログの記録及び保管がこれに相当する。図 2.2-62（46 ページ）のグラフのうち、「情報システムのログの記録・保管と周知」のみについて企業規模別のクロス集計を行った結果を次ページに示す。これによれば、ログの記録等の実施率は企業規模と正相関の関係にあり、零細企業においてはまったく実施されていない一方、従業員数 3,001 人以上の企業においては、8 割を超える実施率となっている。

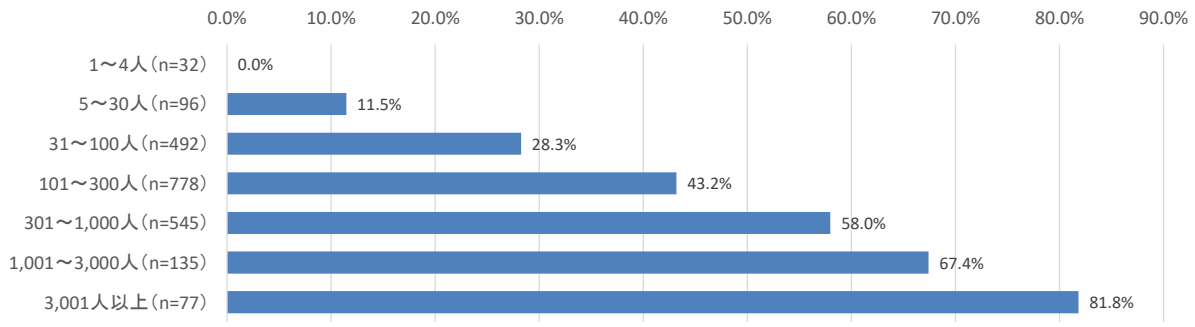

図 3.2-1 「情報システムのログの記録・保管と周知」の実施率

この例は、多くの中小規模企業において、適切な営業秘密管理を実現するために必要となる取組が十分に行われていないことを示すものであるが、同時に従業員 3,001 人以上の大規模企業であっても、2 割弱の企業はログの記録を行っておらず、不正競争行為に対する適切な法的救済を受けられない恐れがあるという課題の存在を示唆している。

(3) テレワーク等の新たな働き方の実施に伴うリスク認識

アンケート調査結果の図 2.2-111（70 ページ）に示すように、テレワーク等の実践を通じて営業秘密漏えいリスクが増大しているかどうかについてテレワークを実施している企業を対象に訪ねた結果、リスクが大きく増大すると認識している回答者が 15.3%、若干増大すると認識している回答者が 46.7%、ほとんど変わらないと認識している回答者が 31.4%との結果が得られている。このようなリスク認識に差が生じる背景として、調査の結果、次のような要因があることが明らかとなった。

① テレワーク等の環境で厳重に保護すべき情報を扱っていない

企業インタビューにおいて、リスクがほとんど変わらないと回答した企業に対してその理由を尋ねたところ、テレワーク等の環境では厳重に保護すべき営業秘密を扱うことを認めておらず、仮に情報漏えいが生じても被害が大きくならないことが挙げられた。この場合、業務の遂行に専用の設備を必要とし、テレワーク等の環境で実施可能な業務が限られることが背景にある。このような考え方をとることで、テレワーク等の働き方を導入することによる営業秘密漏えいのリスクの増大や、対策に要するコストを抑制することが可能となるが、反面テレワーク等を実施することによる効果も限定されてしまう。現実にテレワーク等の働き方を全面的に導入することが困難な業種や事業形態の企業は多く、こうした企業で限定的にテレワークを行う場合は、このようにテレワークで取扱可能な情報を限定してしまうことも対策の一案といえる。

② テレワーク等の安全確保のために実施すべき対策ができていない

一方、リスクが大きく増大していると回答した企業におけるその理由を推察する手段として、図 2.2-42（35 ページ）に示した営業秘密情報の保護対策を実践する上で課題と感じる事項について、テレワークのリスク認識をもとにクロス集計した結果を次ページの図 3.2-2 に示す。

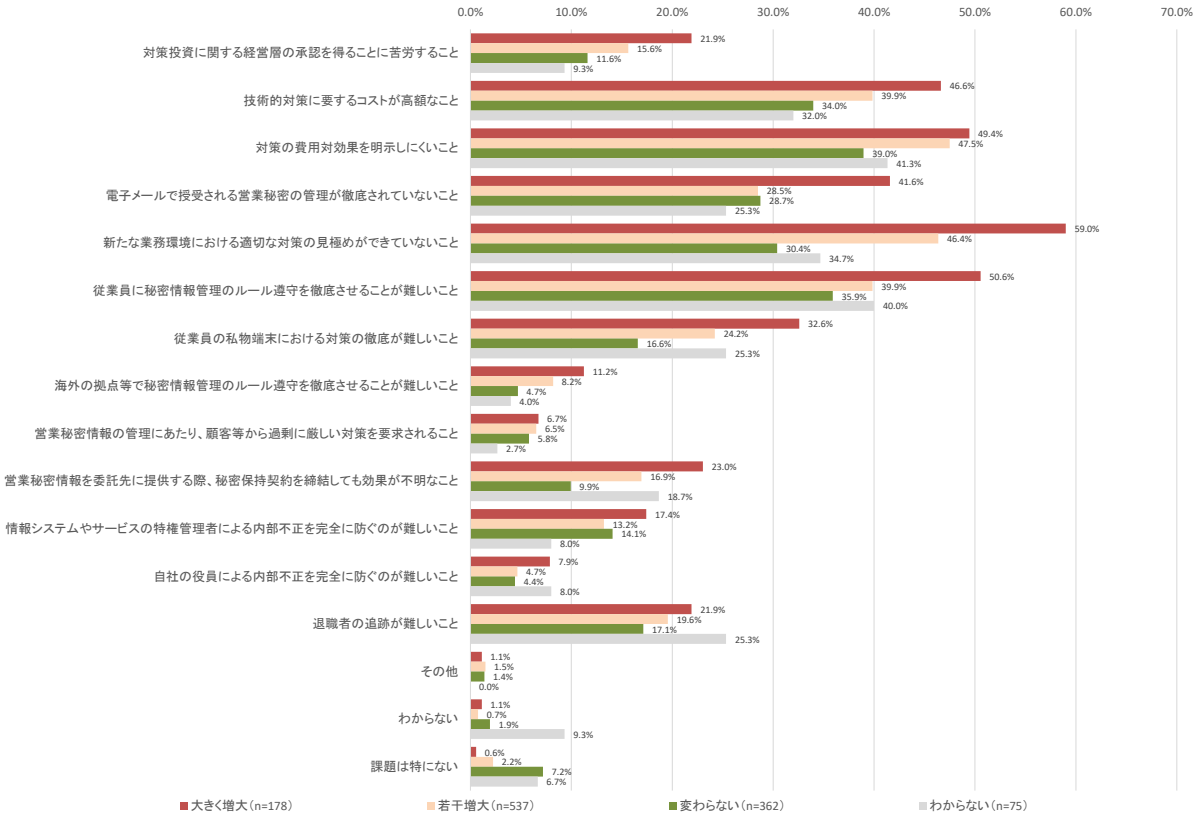

図 3.2-2　営業秘密の保護対策実践上の課題（テレワークのリスク認識別クロス集計）

同図によれば、テレワークで「リスクが大きく増大している」と回答している群が、それ以外の群と比較して突出して懸念している項目として、次の課題があることがわかる。

- 対策投資に関する経営層の承認を得ることに苦労すること
- 技術的対策に要するコストが高額なこと
- 電子メールで授受される営業秘密の管理が徹底されていないこと
- 新たな業務環境における適切な対策の見極めができていないこと
- 従業員に秘密情報管理のルールを遵守させることが難しいこと
- 従業員の私物端末における対策の徹底が難しいこと

これらの課題は、回答者から見て「対策が必要と思っているが、実際には対応できていない」ものであり、これらが改善されないままテレワークを実施していることから、テレワークのリスクは著しく大きいと感じられていることが考えられる。

こうした傾向から示唆されるのは、緊急事態宣言の発令等に伴って急遽テレワーク等の働き方を導入した企業において、テレワーク等の業務形態に応じた情報管理対策が講じられないまま運用が継続されている可能性である。リスクが大きく増大すると認識している回答者の比率である 15.3%は、こうした状態にある企業がどの程度存在するかの推定にあたって参考にできるデータであると考えられる。

4 実態を踏まえた企業向け啓発の方向性

本章では、前章の考察を踏まえ、今後企業が取り組むべき適切な営業秘密管理の考え方について説明する。

4.1 ニューノーマル環境における営業秘密保護の考え方

ニューノーマル環境において企業における働き方が変化する中で、企業が営業秘密を適切に管理・活用するために意識し、対策するために考慮すべき事項を示す。

4.1.1 「見切り発車」状態からの脱却の必要性

本報告書のとりまとめの時点（2021 年 1 月）において、新型コロナウイルスが今後の社会にどのような影響を及ぼしていくのかの予測は困難であるが、有識者インタビューより、今後の老々介護の増大など社会の変化や、大規模災害におけるサプライチェーンの障害への対処などの目的で、テレワーク等を用いた新たな働き方が常態化していくことが指摘されている。この結果、いわゆる「デスクワーク」の形で処理される業務は、今後業種や業態に関わらず、テレワークでも実施され得る状況になっていくことが見込まれる。

一方、アンケート調査結果の図 2.2-106（67 ページ）に示されているように、2020 年にテレワーク等を実施した企業のうち、テレワーク等に対応した規程等を整備済みの企業は全体の 3 割程度にとどまる。約 3 割弱の企業が暫定または例外措置として運用を行い、残りの企業は検討中若しくは対応の予定が無い。この結果に示されているように、国内の多くの企業において、緊急事態宣言発令を受け、事業継続の観点から機密性よりも可用性を重視する形で、「見切り発車」的にテレワーク等の働き方が導入されたことが想定される。これは緊急避難的な措置としてはやむを得ない面があるが、企業の施設内のみで営業秘密を扱うことを前提としたこれまでの手続や対策のうち、テレワーク等の環境においては有効でなくなるものが生じることから、緊急避難的な状況を永続させることには大きな危険が伴う。例として、秘密情報を限られた者しか入室できない建物や部屋に保存したり、秘密情報の管理責任者が管理する鍵で施錠されたキャビネットに保管したりするような対策や、秘密文書を綴じたバインダーへのマル秘表示等については、電子データ化された営業秘密を取り扱うことが前提のテレワーク環境においては機能しないことから、これらに代わる対策を検討しなければならない。2021 年 1 月までにこのような状況に起因するような大規模な情報漏えい等のインシデントは報告されていないものの、今後も同じ状況が続くことは限らない。

4.1.2 テレワーク等の環境における秘密管理措置の考え方

テレワーク等に対応した営業秘密管理に関する規程や手続の整備にあたっては、次に示す２つの観点から検討する必要がある。

- **被害発生防止の観点**：サイバー攻撃等で不正に秘密情報を窃取しようとする外部からの攻撃者や、内部不正により秘密情報を持ち出そうとする者、さらには役員・従業員の過失やシステムの誤動作などの脅威による、秘密情報の漏えいをどのように実効的に防ぐか
- **法的救済の観点**：何者かの不正競争行為によって上述のような秘密情報の漏えいが生じた場

合、行為者に対して秘密情報の利用に関する差し止め請求や損害賠償請求を行えるようにするために、裁判所が営業秘密該当性を認定するに足る管理の実態をどのように担保するか

以下ではこの２点について、本調査の結果をもとに考慮すべき視点を示す。

(1) テレワーク等の環境における情報漏えい被害防止

テレワーク等におけるサイバーセキュリティ対策及び秘密情報管理については、公的機関より様々な資料[7]が公表されており、これらの資料を参考に業種や業務内容、扱う情報の特徴に応じて適切な対策を検討することが求められる。本調査の調査結果をもとに、情報漏えいの原因別に考慮すべき事項を示す。

① 外部からのサイバー攻撃等への対応

アンケート調査結果の図 2.2-32（31 ページ）に示されているように、「自社の営業秘密を狙う外部からの標的型攻撃」は回答者において２番目に多く選択されている脅威である。オフィスで業務を遂行中に不審な電子メールを受信した場合、電子メールにおけるリンク先を参照したり、添付ファイルを開封したりする前に周囲の同僚や上司に相談するなどにより、攻撃による被害を未然に防ぐ機会があるのに対し、テレワーク等の環境では気軽に相談できる相手がいないこともあって、オフィス環境よりも標的型攻撃やフィッシング詐欺等の被害が生じやすいとされる。さらにテレワーク等による働き方は事務職の者に対してより多く採用される傾向にあるため、テレワーク等の環境においては営業秘密の中でも技術情報より営業情報がより多く扱われることになる。テレワーク等におけるサイバーセキュリティ対策の検討にあたっては、こうした傾向を考慮することが望まれる。

また、サイバーセキュリティ対策製品やサービスを開発・提供している企業においてもサイバー攻撃によるインシデントの発生が報じられるなど、サイバー攻撃は適切な対策を講じても完全に防ぐことが困難なリスクである。そのような状況において、施錠されたキャビネット等に格納する紙媒体の形で管理していた秘密情報をテレワーク等で利用するために電子データ化した場合、適切な保護対策を講じたとしてもサイバー攻撃による情報漏えいリスクが生じるのは確かである。一方で、現状では紙媒体の営業秘密を作成する際に手書きで作成されることは稀であり、通常は何らかのネットワークに接続された IT 機器上で作成することを考えると、営業秘密を電子データで管理することそのものが情報漏えいリスクを著しく増大させるとは限らない。

このように、テレワーク環境での業務遂行に伴うサイバー攻撃の影響を適切に評価することは必ずしも容易ではないが、保護すべき営業秘密の利用実態、情報漏えいが生じた場合の被害の大きさ等を勘案した上で、テレワーク等で取り扱う事を認める情報の種類と、対策方法につ

[7] 一例として、内閣サイバーセキュリティセンター『テレワーク実施者の方へ』
https://www.nisc.go.jp/security-site/telework/index.html
総務省『テレワークにおけるセキュリティ確保』
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
経済産業省『テレワーク時における秘密情報管理のポイント』
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf
IPA『テレワークを行う際のセキュリティ上の注意事項』
https://www.ipa.go.jp/security/announce/telework.html

いて検討する必要がある。

② 従業員や関係者による内部不正への対応

アンケート調査結果の図 2.2-26（28 ページ）に示されているように、情報漏えいに関するインシデントが発生している企業において、その主たる要因とされるのが中途退職者による秘密情報の持ち出しである。テレワーク等の場合、上司や同僚の目に触れることなく秘密情報にアクセスできることはリスク要因となる。一方で、秘密情報が電子データ化されていることで秘密情報へのアクセスログを自動的に取得する仕組みを構築できることから、アクセスに用いる ID の詐称や不正利用がない限りという条件[8]は付くものの、内部不正行為のエビデンスを電子的に取得できるという点で、テレワーク等環境のほうが内部不正を検知しやすいともいえる。さらに、このようにアクセスログを通じて不正が露見することを従業員等に周知することにより、「不正をしても見合わない」ことを理解してもらうことで、内部不正の抑止効果を期待することができる。インタビュー調査の対象企業においても、営業秘密の保護対策として実際にこのような取組を行っていることが確認されている。それでも、秘密情報にアクセスするための正当な権限をもつ担当者が、業務目的でのアクセスと区別できない形で参照した上で不正に持ち出すような場合は、退職直前に不自然な大量のアクセス等を行わない限り、アクセスログ上で不正かどうかの判断は困難であり、アクセスログを利用した不正検知の限界は存在する。

③ 業務上の過失や誤操作への対応

企業において情報漏えいが生じた場合の損害が大きな営業秘密を電子メールや FAX 等で送信する場合、誤送付防止の観点から宛先が正しいかどうかを複数名で確認するなどの手続が定められていることがある。このような手続はオフィス環境で営業秘密を扱うことを前提としており、テレワーク等の環境で同じことをしようとしても簡単ではない。そこで、テレワーク勤務者が外部に営業秘密を送信する場合、組織内の別のメンバー（上司、同僚等）により宛先が正しいことを確認するプロセスを追加することで、同等の安全性を担保することが考えられる。このように、テレワークで行う業務における従業員の過失や誤操作による情報漏えいを防ぐための対策について、テレワーク等の環境で実施可能な代替策の検討を行うことが望まれる。

また、テレワーク等の利用時に限定されるものではないが、クラウドサービスを用いて秘密情報の共有を行う場合に、そのアクセス権限の設定ミスにより、インターネットから閲覧可能な状態となることで情報漏えいが生じるインシデントはこれまでに多数発生している。アンケート調査の図 2.2-86（56 ページ）に示す通り、アクセス権限の定期的な確認はクラウドサービス利用における対策として最も多く実施されているものであり、クラウドサービスを利用する場合は怠りなく実施する必要がある。

(2) 営業秘密該当性を満たすための秘密管理措置の考え方

不正競争防止法による法的救済を可能とするには、対象となる営業秘密について、「営業秘密管

[8] 厳密には、内部不正行為者がログファイルを改ざんして証拠を抹消する可能性を考慮し、これを防ぐ対策も実施する必要がある。

理指針」が示す秘密管理性、有用性、非公知性の３条件で構成される営業秘密該当性を満たす必要がある。2.4 項の文献調査及び 2.5 項の裁判例調査で示した通り、裁判所における営業秘密該当性は秘密として管理すべき情報の管理状況から機械的に判断されるものではないが、「営業秘密管理指針」に示されている秘密管理措置の例示に相当する対策を講じることがひとつの目安となる。テレワーク等の環境における秘密管理措置について、アクセス制限と秘密情報であることの認識可能性の２つの観点に基づく考え方を以下に示す。

① 現実的なアクセス制限の実施

アクセス制限の基本的な考え方は、参照する必要のある者にアクセスを許可し、不要なものには許可しないことであり、これは"Need-to-know"の原則として知られている。一般に、アクセス制限を厳格に実施しようとすると、業務を行う体制やプロジェクトの変化毎に頻繁に変更する必要があり、その結果としてアクセス制限に係る運用負荷が膨大となる。そこで現実には同一部署の全メンバーに同一の権限を適用するなど、やや緩めの運用を行ったり、細かい設定変更に関しては現場部署に一定の管理権限を与えて管理を委ねたりすることで管理負担を減らしていることがインタビュー調査結果において示されている。その一方で、アクセス制限のルールはあるものの完全に形骸化し、実際には誰でも秘密情報にアクセスできるような場合には、秘密管理性があったと認めない裁判例も存在しており、合理的な範囲でアクセス制限を設定し、持続的にその機能を維持するような運用を行うことを心がける必要がある。

テレワーク等の環境の場合、秘密情報へのアクセスに先だって適切な利用者認証を行い、アクセス権限を有する者かどうかを識別する仕組みを用いて業務を行うのであれば、オフィス環境で業務を行うのと同等のアクセス制限が有効なケースが多いと考えられる。ただし、テレワーク環境への紙媒体による秘密情報の持ち出しを許可する場合は、運用次第では紙媒体の施錠保管ルールが形骸化する恐れがあることから、持ち出しの必要性について慎重に検討すべきである。

② 秘密情報であることの認識可能性の確保

従業員等による営業秘密情報の持ち出しを不正競争行為とする訴訟において、情報を持ち出した時点で当該従業員がその情報が秘密であると認識できていなかったことが推定される場合、裁判所によって秘密管理性が否定されることが多い。テレワーク等の環境では、従来のオフィス環境における、営業秘密の保管場所への「関係者以外立入禁止」表示や営業秘密を綴じたバインダーへの「マル秘」表示などが機能しなくなることから、従業員が容易に秘密であると認識可能な代替方法を用意する必要がある。具体例として、営業秘密を保存するフォルダーをそれ以外の情報から区分し、フォルダー名に秘密であることがわかる記号等を含めることをルール化することが挙げられる。反面、このような方法は、秘密情報を外部に不正に売却しようと考える内部不正行為者に対し、価値の高い情報の場所を示すことになる弊害もあることから、①に示したアクセス制限との適切な組合せで実施することが欠かせない。

なお、アンケート調査結果の図 2.2-62（46 ページ）において、営業秘密情報の漏えいを生じさせにくい環境をつくるための対策に関する選択肢のうち、2016 年調査と比較してほとんどの項目の実施率が増える中で、「社員証等の着用義務づけ」「立入禁止等の警告表示」及び「不正

検知が容易な座席レイアウトの工夫」の３項目のみ実施率が減少する傾向が示されているのは、上述したようなテレワーク等の環境でこうした対策が機能しないことを回答企業が意識し、代替案に重点を置くようになったことの現れと考えられる。

4.2 秘密情報の区分管理の更なる普及に向けて

(1) 国内企業における営業秘密の区分管理に関する現状と課題

3.2 項で考察したとおり、今回の調査結果において依然として営業秘密の区分管理をせず、他の情報と共通で運用している企業が全体の約４割、大規模企業においても約３割にわたって存在することが明らかとなった。今回実施したアンケート調査の回答率は 13.6%であるが、回答した企業には情報管理への関心が高い企業が多いと想定されることから、実際の国内企業において秘密情報を区分管理している企業の比率はさらに下がるものと考えられる。区分管理を推進する際の阻害要因として、企業及び有識者へのインタビュー調査では次のような事項が挙げられている。

- 現場業務が多様なため、それぞれに対応したルールを策定しようとしても手が回らない
- 現場がこれまでの情報管理のやり方を変えようとしない
- 情報管理に先だって社内情報のアセスメントや洗い出し、棚卸し等をしようとしても、現実的なリソースの範囲でやっていると終わらず、その先のフェーズに進めない

営業秘密の区分管理をしない状況でも、組織の IT インフラに対して一定のサイバーセキュリティ対策を講じることで情報の漏えいを防ぐことは可能であり、社内の情報に対して外部からのアクセスを制限する措置等も一定の措置に相当しうるが、営業秘密の不正利用の脅威に対して不正競争防止法による救済措置を適用可能とすることを考えた場合、4.1②に示した秘密情報であることの認識可能性に関しては不十分であり、区分管理をしないままでは営業秘密該当性が認定されない恐れがある。

(2) 無理なく区分管理を開始するためのプラクティス

前項に示したような阻害要因を抱える企業において、無理なく営業秘密の区分管理を開始するためのプラクティスとして、有識者インタビューを通じて次のような提案が示された。

① 異論と無理が出ないところから開始する

阻害要因に示されている通り、これまで区分管理ができなかった理由として、「現場の反対」や「リソース不足」の影響が大きいことから、まずはこれらが障害にならない範囲から開始することが適切である。具体的には、１部署あたり３種類程度の、誰もが秘密として管理することに異論のない情報のみを管理対象とすることが考えられる。例としては次のような営業秘密が挙げられる。

- 人事評価情報
- 非公表の事業戦略、交渉経過
- 特定の担当者以外参照する必要のない、企業競争力の観点で重要な技術情報

もっとも、こうした情報はこれまで「存在すること自体が非公表」として扱われていたものが多く、これらのみを管理対象としていわば存在を可視化してしまうことへの抵抗感も生じることが予想される。しかしながら、今後テレワーク等の環境でこれらの情報を扱うことを想定

する場合、区分管理等の規定を設けぬまま場当たり的な保護のもとで情報を取り扱うことは、漏えい事故を生じさせる原因となりやすく、適切なルールを定めた上で管理すべきである。

② 管理負荷の小さいプラットフォームで管理する

営業秘密等、保護する必要のある情報の管理において、多くの企業では表計算アプリケーションのワークシート等を用いた情報管理台帳を用いた情報の持ち出し等の制御を行っている。しかしながら、このような方法に対しては台帳の管理負荷が大きいとの指摘もあり、実際の情報へのアクセスとは別に台帳対応を行う場合には形骸化の懸念もある。そこで、これから営業秘密の区分管理を行おうとする場合、商用で提供されている文書管理ソリューションや、クラウド型のオフィスアプリケーションのように、あらかじめ文書管理機能やアクセス制限機能を備えた文書管理用のプラットフォームを用いることが考えられる。このようなプラットフォームの場合、営業秘密等の保護対象データにアクセスするためには、プラットフォームが提供する認証や申請・承認等の手続を経る必要があるため、台帳の内容が実態と乖離するような問題が生じにくい利点もある。欠点はプラットフォーム導入コストを必要とすることであり、これを避けるために冒頭に示したワークシートによる管理を選択することもあり得るが、コストと効率を天秤にかけ、組織として合理的な管理の方法について検討することが望ましい。

4.3 情報管理の成熟度と新たな IT 環境の活用状況との関係

2.2.5 項で検討したように、情報管理に関する成熟度と、テレワークやクラウドサービス等の新しい IT 技術の活用状況との間には、明確な正相関の関係が示されている。これは、適切な情報管理の仕組みを構築し、運用できている企業ほど、適切なサイバーセキュリティ対策を実施しているという当然予測される傾向にとどまらず、企業の事業展開の上で有用となり得る新しい IT 環境の活用が可能となり、企業としての競争力を高めることを示唆するものである。このとき、活用可能となる新しい IT 環境としては次のようなものが想定される。

(1) DX（デジタルトランスフォーメーション）の実現に関するもの

DX が進展する中で、企業における IT 活用は従来型の情報システム部門主導から現場事業部門主導へと変化することが見込まれる。このような中で、情報管理に関する成熟度が低い状態、すなわち区分管理なし、改善の取組なしといった状態で現場事業部門において秘密情報を扱おうとしても、合理的な保護ができず混乱が生ずる恐れがある。DX 推進に先だって、各部署で扱う情報の特徴に応じた管理の体制や手続を整備することが求められる。

さらに、AI（人工知能）の効果的な活用にあたって必要となる機械学習用のデータについても、データの提供側事業者と利用側事業者との間で今後限定提供データの要件に基づいた保護や取扱の規定が求められることが増えるものと見込まれる。アンケート調査結果の図 2.2-49（39 ページ）においてもこうした傾向が一部業種等で示されており、限定提供データの三要件を満たすようなデータの保管や共有の方法について、自社の事業内容や事業戦略に応じた検討が望まれる。

(2) ニューノーマルでの事業展開に関するもの

本報告書ではテレワーク等による新しい働き方における情報管理の考え方について論じているが、ニューノーマル社会においては、テレワーク等以外にも、行政分野のデジタル化、ヘルスケア分野でのデータ活用、運輸分野における自動化から農作物や食料品等まで、IT のさらなる利活用を前提とした変化が生じていくことが見込まれる。このような環境変化の中で企業の競争力を高めるために、企業内で適切な情報管理のための体制と制度を整備しておくことは欠かせない。

さらに、社会における新たな動きについて速いスピードでの変化が見込まれることから、こうした変化に対応するための手続等の見直しをタイムリーに行えるような体制とすることも考慮する必要がある。

5 おわりに

これまで示したように、本調査では 2020 年における国内企業での営業秘密管理の実態を把握することを目的として、アンケート調査を中心とする各種調査を実施した。本調査の実施に先立って新型コロナウイルス蔓延、これに対応する緊急事態宣言の発令に伴い企業に対してテレワークの推奨が行われ、企業における働き方が変化することで、業務で取り扱う情報管理の方法についても多くの変化が見られたことから、調査設計にあたってはテレワーク環境での営業秘密管理の実態についても把握できるように配慮している。アンケート調査結果を踏まえ、実際に企業で情報管理に取り組んでおられる担当者から実務の実態を、不正競争防止法に高度な知見を有する弁護士から専門的知見に基づくご意見をそれぞれインタビュー調査にて把握した上で、企業を対象とした今後の啓発の方向性として、ニューノーマル環境における営業秘密保護の考え方等についてとりまとめた。コロナ禍の中実施したアンケート調査では目標を大きく上回る企業から貴重なご回答をいただけたことで、業種別のクロス集計分析等において統計としての精度を高めることが可能となった。この場を借りて、繁忙にも関わらずアンケート調査にご協力いただいた企業の皆様に心より御礼を申し上げたい。

今後、同様の調査を実施する場合、現状では次のような状況が明らかでないことから、これらの状況についての仮説を設定した上で調査することが考えられる。

- 限定提供データを対象とする保護対策は、これまでの営業秘密情報とどのように異なるのか
- ニューノーマル環境での業務遂行を続ける中で、対策の傾向はどのように変化したのか
- 企業の評価の視点として、ESG（環境・社会・ガバナンス）が注目される中で、企業は自社で扱う情報についてどのような方針で管理するのか

今回アンケート調査にご協力いただかなかった企業においても、図 2.2-125（79 ページ）に示す算出方法をもとに成熟度の算出を行うことで、企業規模別、業種別のほか、情報管理に関する成熟度別のクロス集計結果の各種グラフにおける自社のポジションを把握することが可能となる。企業をとりまく環境が大きくかつ目まぐるしく変化する中、自社の営業秘密を保護しつつ、新たな IT 技術を活用するためにどのような対策を行うべきかの検討に、本調査結果を参考としていただければ幸いである。

変更履歴

日付	内容
2023 年 10 月 24 日	P56 「(12) クラウドサービスにおける営業秘密の不正利用防止のために実施している対策」における説明文を変更。