

# サプライチェーンにおける委託元企業／委託先企業の 営業秘密保護／内部不正防止の要点とグッドプラクティス

～IPA「内部不正防止対策・体制整備等に関する中小企業等の状況調査」の成果から～

2024年7月29日

株式会社NTTデータ経営研究所 エグゼクティブスペシャリスト 三笠 武則  
(営業秘密保護推進研究会 事務局長)



## 情報漏えい／内部不正インシデントの一般的な傾向 ～事例調査より

- 2020年4月以降の秘密情報漏えい／内部不正、サイバー攻撃、システム障害事案の調査結果： 257件

## 1. 情報漏えい／内部不正インシデントの一般的な傾向（1）

報道されている個人情報漏えい事案の、数の多さは圧倒的である。

個人情報漏えい事案

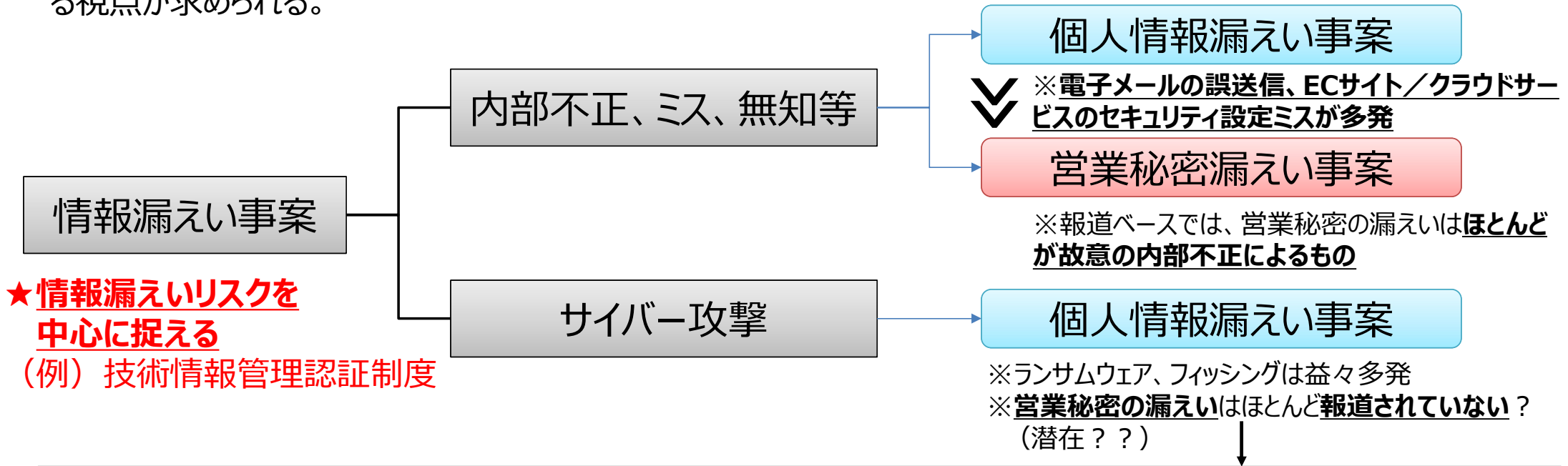


営業秘密漏えい事案

※報道されていない事案も多いと推察

# 1. 情報漏えい／内部不正インシデントの一般的な傾向（1）

「サイバーセキュリティ」だけでなく、「情報漏えい」を中心に据えて、事業リスクを評価することも必要。  
秘密情報漏えいの主因を、①内で起こる「内部不正、ミス、無知等」と、②外から来る「サイバー攻撃」に分類する視点が求められる。



(ご参考) 警察庁、NISCのパブリック・アトリビューション（2023/9/27発表）によると：  
中国を背景とするサイバー攻撃グループであるBlackTechが、2010年頃より日本を含む東アジア、米国の米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的に情報窃取を目的とするサイバー攻撃を行っていることを確認しているとのこと。

(出典) [https://www.nisc.go.jp/pdf/press/20230927NISC\\_press.pdf](https://www.nisc.go.jp/pdf/press/20230927NISC_press.pdf)

(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 1. 情報漏えい／内部不正インシデントの一般的な傾向（2）

### <得られた示唆>

サプライチェーンで営業秘密等の漏えいを発生させないためには：

- 💡 内部不正事案の多くは、情報漏えいを伴う

内部不正を起こさせないことが重要！

- 💡 営業秘密の漏えいは、内部不正によるものが看過しえないほど多くを占める

- 💡 営業秘密漏えいの発生は、企業規模によらない。 ➡ サプライヤー対策も重要

## 重視すべき2つの新しい着眼点

## 2. 重視すべき2つの新しい着眼点（1）

昨年度のIPA実態調査結果から、秘密情報漏えい／内部不正防止の充実に向けて、新しい2つの着眼点が重要であることが浮き彫りになってきている。これらの着眼点を具備することで、企業の取組が各段にレベルアップする。

### 秘密情報漏えい防止において 営業秘密を（最）優先

- 営業秘密の特定、格付け、表示の実効性を高める対策  
特定のための基準等：82.1% vs 11.1%  
格付けのための基準等：46.4% vs 9.3%  
格付け表示のルール等：30.4% vs 0.9%
- 格付け表示等により営業秘密等と認知できるか：  
60.4% vs 4.6%
- 秘密情報の不自然な取扱いや社外への不正な漏えいを見かけた際の適切な行動リテラシー構築：  
80.0% vs 1.9%

### 内部不正防止は サイバーセキュリティとは別建て

- 内部不正防止に特有の対策  
職場環境の改善：72.5% vs 38.3%  
雇用開始／終了時の誓約書：65.4% vs 43.1%  
人的ミスへの十分な注意喚起：61.3% vs 39.0%  
ITシステムアクセス等のログの定期的確認：  
47.7% vs 21.4%  
ログ取得の周知による抑止力発揮：21.3% vs 6.4%  
内部不正の罰則を定め周知徹底：30.6% vs 13.5%  
不必要な秘密情報を取引先に渡さないリテラシー構築  
39.7% vs 24.2%

数字は

「営業秘密を個人情報以上に重視」vs「営業秘密をあまり重視していない」

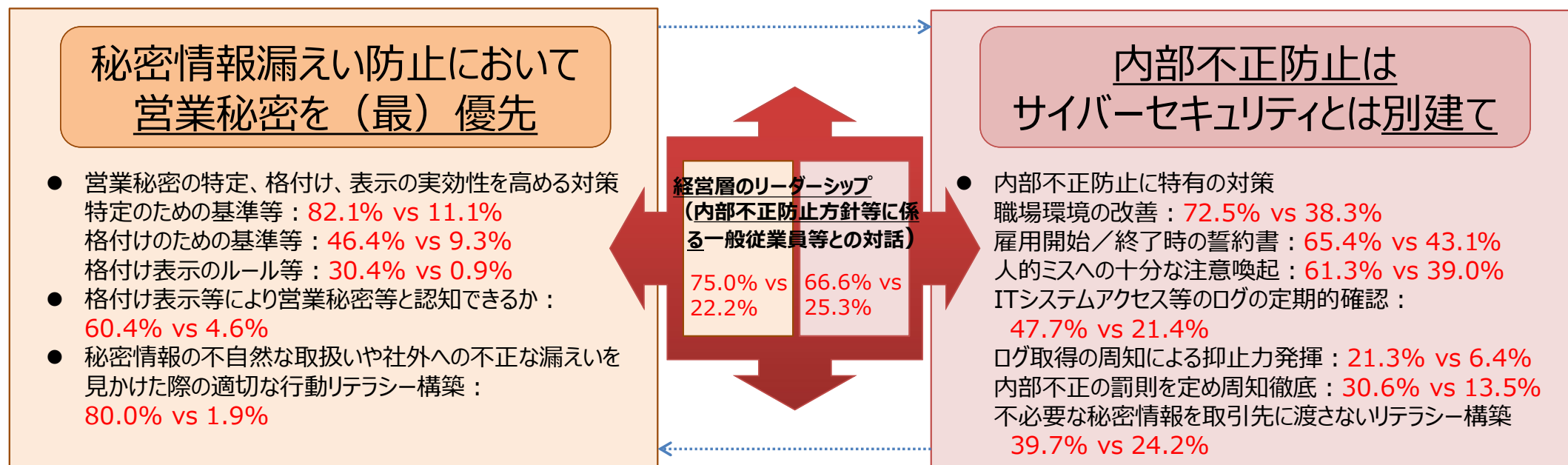
数字（%）は

「内部不正防止を意識的に別建て」vs「内部不正防止を分けていない等」

（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 2. 重視すべき2つの新しい着眼点（2）

秘密情報漏えい／内部不正防止に係る経営層のリーダーシップ向上と、新しい2つの着眼点を具備することは深く関わっており、相乗効果を生み出すことを期待できる。



数字は  
「営業秘密を個人情報以上に重視」vs「営業秘密をあまり重視していない」

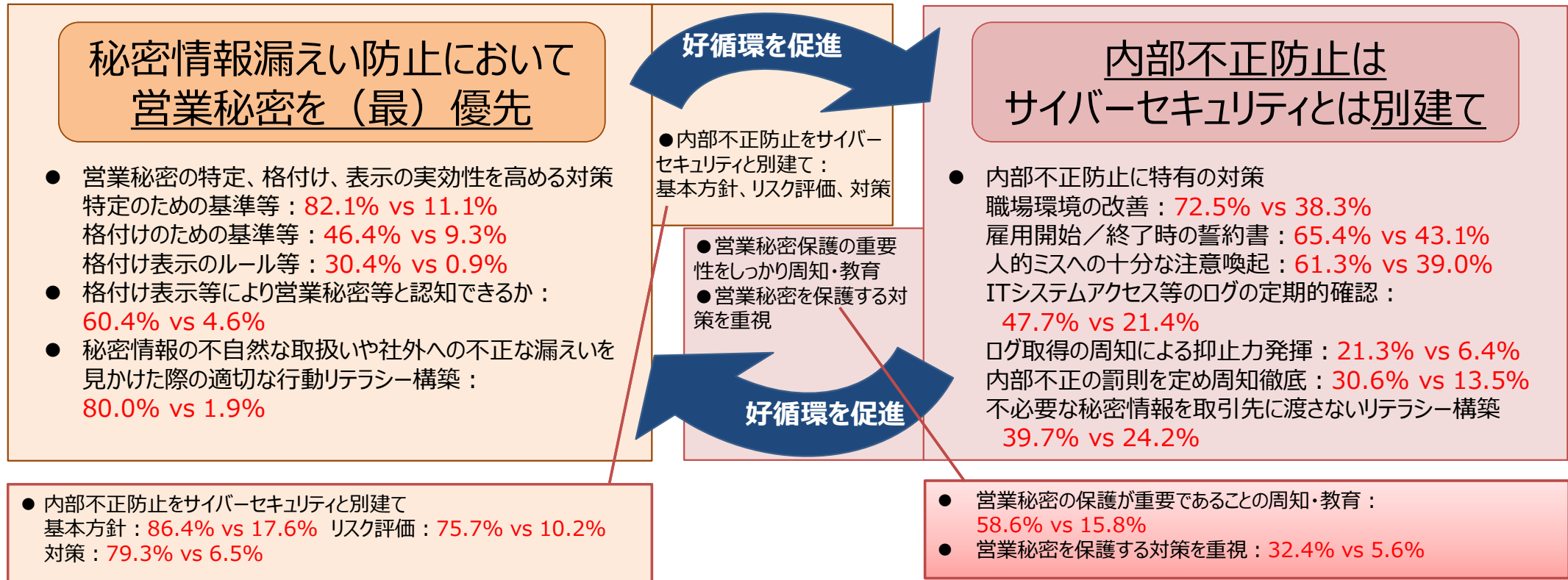
数字（％）は  
「内部不正防止を意識的に別建て」vs「内部不正防止を分けていない等」

（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>



## 2. 重視すべき2つの新しい着眼点（3）

新しい2つの着眼点は相互に良い影響を及ぼし合い、秘密情報漏えい／内部不正防止の取組のレベルアップを促進していると考えられる。



（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

数字は

「営業秘密を個人情報以上に重視」vs「営業秘密をあまり重視していない」

数字（%）は

「内部不正防止を意識的に別建て」vs「内部不正防止を分けていない等」

## 2. 重視すべき2つの新しい着眼点（4）

サプライチェーン管理強化の観点からは、新しい2つの着眼点に対し、委託元の大企業とサプライヤー企業が同程度の成熟レベルにあることが望ましいが、実際にはサプライヤーはかなり遅れている。この差を縮めることに重点を置いて、サプライヤー強化に取り組むことが望ましいが、中小企業の限られた人員・リソースが制約になりうることに留意が必要。

秘密情報漏えい防止において  
営業秘密を（最）優先

28.3%～40.2% vs 12.6%～20.4%

1,000人以上の大企業 100人以下の中小企業

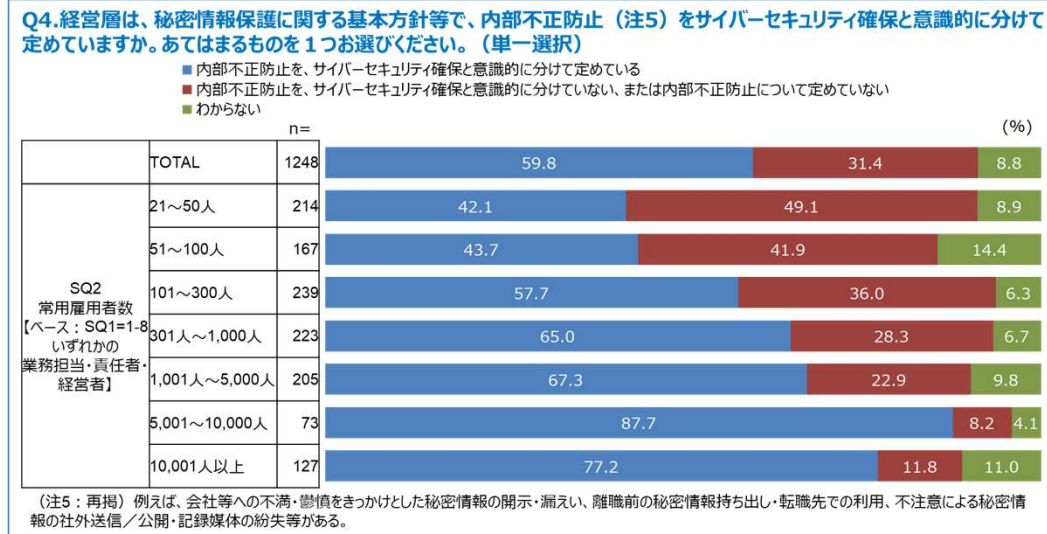
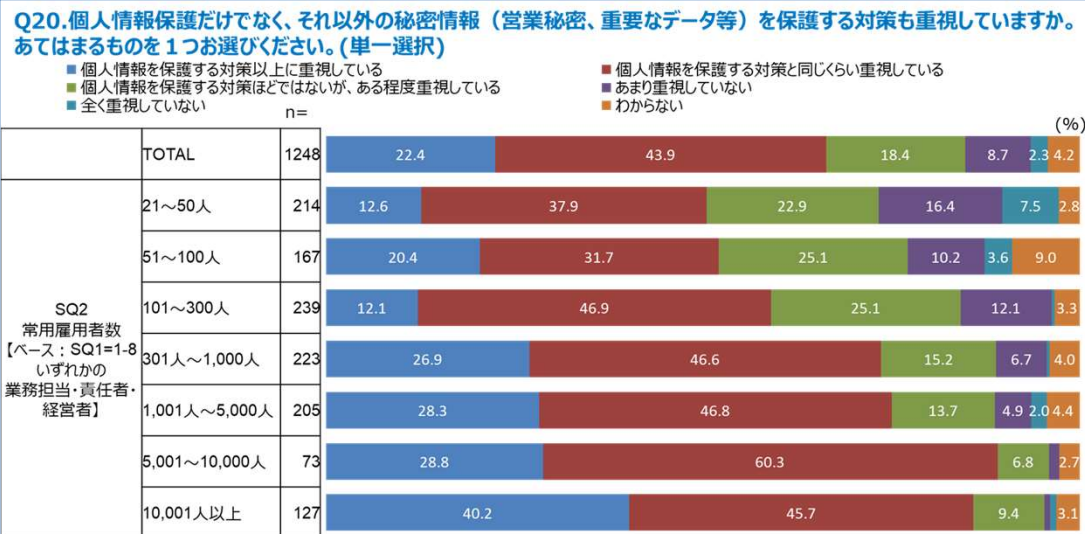
サプライヤーに営業秘密管理を新たに導入する等が効果的

サプライヤーの人員・リソースが課題

内部不正防止は  
サイバーセキュリティとは別建て

67.3%～87.7% vs 42.1%～43.7%

1,000人以上の大企業 100人以下の中小企業



（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

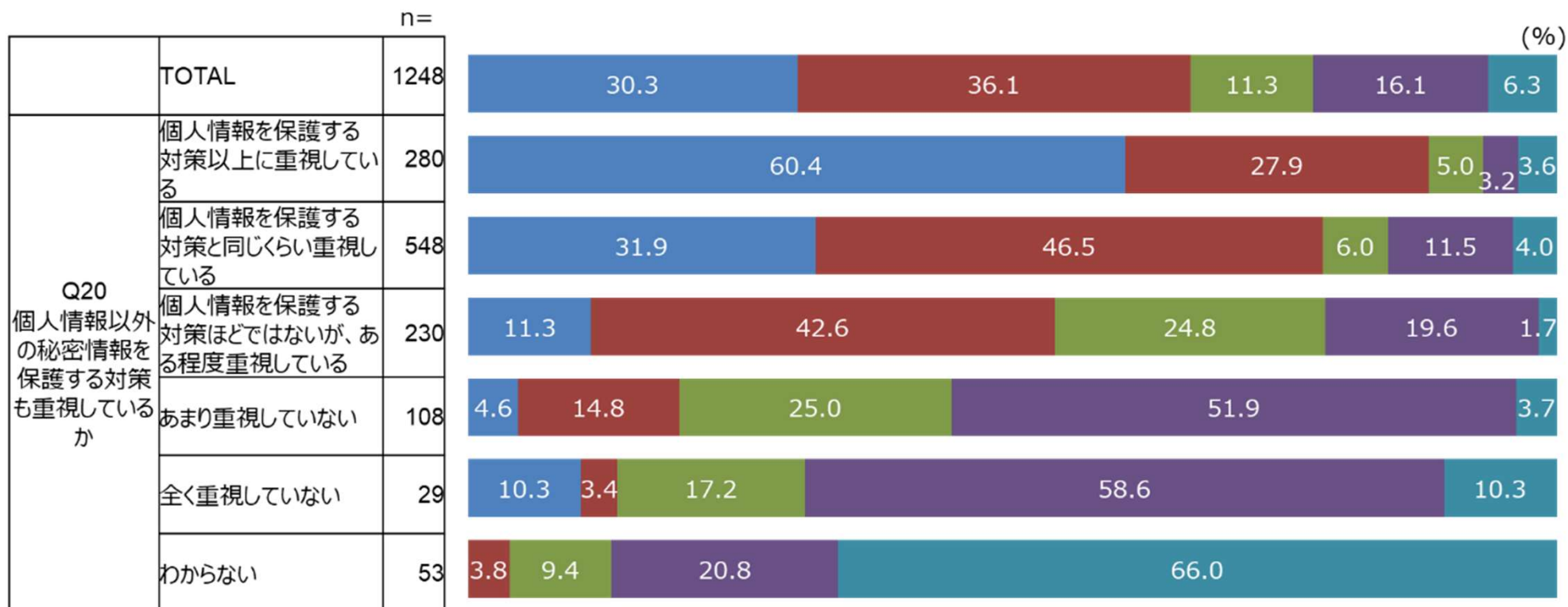
**Q7.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。（複数選択）**

(%)

|                                           |                               |      | 個人情報<br>以外の秘<br>密情報<br>（営業秘<br>密、重要<br>なデータ<br>等）を特<br>定するた<br>めの具体<br>的な基準<br>や、この基<br>準の全社<br>運用を求<br>める共通<br>ルール等<br>を定めて<br>いる | 個人情報<br>以外の秘<br>密情報を<br>格付けす<br>るための<br>基準や、<br>この基準<br>の全社運<br>用を求め<br>る共通ル<br>ール等を<br>定めてい<br>る | 個人情報<br>以外の秘<br>密情報を<br>特定また<br>は格付け<br>する基準<br>を適用し<br>やすいよ<br>うに例を<br>示してい<br>る | 格付けが<br>漏れなく<br>実行され<br>るための<br>仕組みを<br>設け、継<br>続的な改<br>善を図っ<br>ている | 格付けを<br>わかりやす<br>く表示す<br>るための<br>ルールを<br>定めてい<br>る | 格付け表<br>示がない<br>（不明瞭<br>な場合を<br>含む）社<br>内情報の<br>取扱いに<br>ついても<br>ルールを<br>定めてい<br>る | 重要な秘<br>密情報を<br>取り扱う<br>プロジェクト<br>に参加する<br>条件として、<br>「保護対象<br>とする重要<br>な秘密の<br>範囲を明<br>確にした上<br>で、上述し<br>た基準や<br>ルールの順<br>守・徹底を<br>あらためて<br>誓約するこ<br>と」を求め<br>るルールを<br>定めている | 定期的に<br>基準や<br>ルールを<br>順守して<br>いるかを<br>確認して<br>いる（定<br>期的なセ<br>ルフチェッ<br>クを含む） | 何も実施<br>していない | 上記以外 | わからない |
|-------------------------------------------|-------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|---------------|------|-------|
|                                           | TOTAL                         | 1248 | 55.4                                                                                                                               | 33.3                                                                                              | 27.9                                                                              | 18.3                                                                | 18.0                                               | 15.4                                                                              | 17.4                                                                                                                                                                         | 37.4                                                                          | 11.9          | 0.4  | 4.7   |
| Q20<br>個人情報以外の秘密情<br>報を保護する対策も重視<br>しているか | 個人情報を保護する対策以上に重視している          | 280  | 82.1                                                                                                                               | 46.4                                                                                              | 42.1                                                                              | 28.2                                                                | 30.4                                               | 23.9                                                                              | 30.4                                                                                                                                                                         | 46.4                                                                          | 1.1           | 0.4  | 2.1   |
|                                           | 個人情報を保護する対策と同じくらい重視している       | 548  | 66.4                                                                                                                               | 39.1                                                                                              | 31.0                                                                              | 21.9                                                                | 19.5                                               | 14.4                                                                              | 19.0                                                                                                                                                                         | 45.3                                                                          | 6.6           | 0.2  | 1.1   |
|                                           | 個人情報を保護する対策ほどではないが、ある程度重視している | 230  | 33.0                                                                                                                               | 25.7                                                                                              | 21.3                                                                              | 11.3                                                                | 13.9                                               | 12.6                                                                              | 10.0                                                                                                                                                                         | 28.7                                                                          | 14.3          | 0.9  | 2.6   |
|                                           | あまり重視していない                    | 108  | 11.1                                                                                                                               | 9.3                                                                                               | 4.6                                                                               | 1.9                                                                 | 0.9                                                | 13.9                                                                              | 4.6                                                                                                                                                                          | 13.9                                                                          | 48.1          | 0.0  | 4.6   |
|                                           | 全く重視していない                     | 29   | 10.3                                                                                                                               | 6.9                                                                                               | 3.4                                                                               | 0.0                                                                 | 0.0                                                | 3.4                                                                               | 0.0                                                                                                                                                                          | 10.3                                                                          | 69.0          | 3.4  | 0.0   |
|                                           | わからない                         | 53   | 11.3                                                                                                                               | 1.9                                                                                               | 9.4                                                                               | 1.9                                                                 | 0.0                                                | 1.9                                                                               | 0.0                                                                                                                                                                          | 9.4                                                                           | 9.4           | 0.0  | 67.9  |

**Q8.従業員は、自部署・他部署の情報に関わらず、個人情報以外の秘密情報に触れた際に、格付けの表示等によってほぼ漏れなく秘密情報であることを認知できますか。あてはまるものを1つお選びください。（単一選択）**

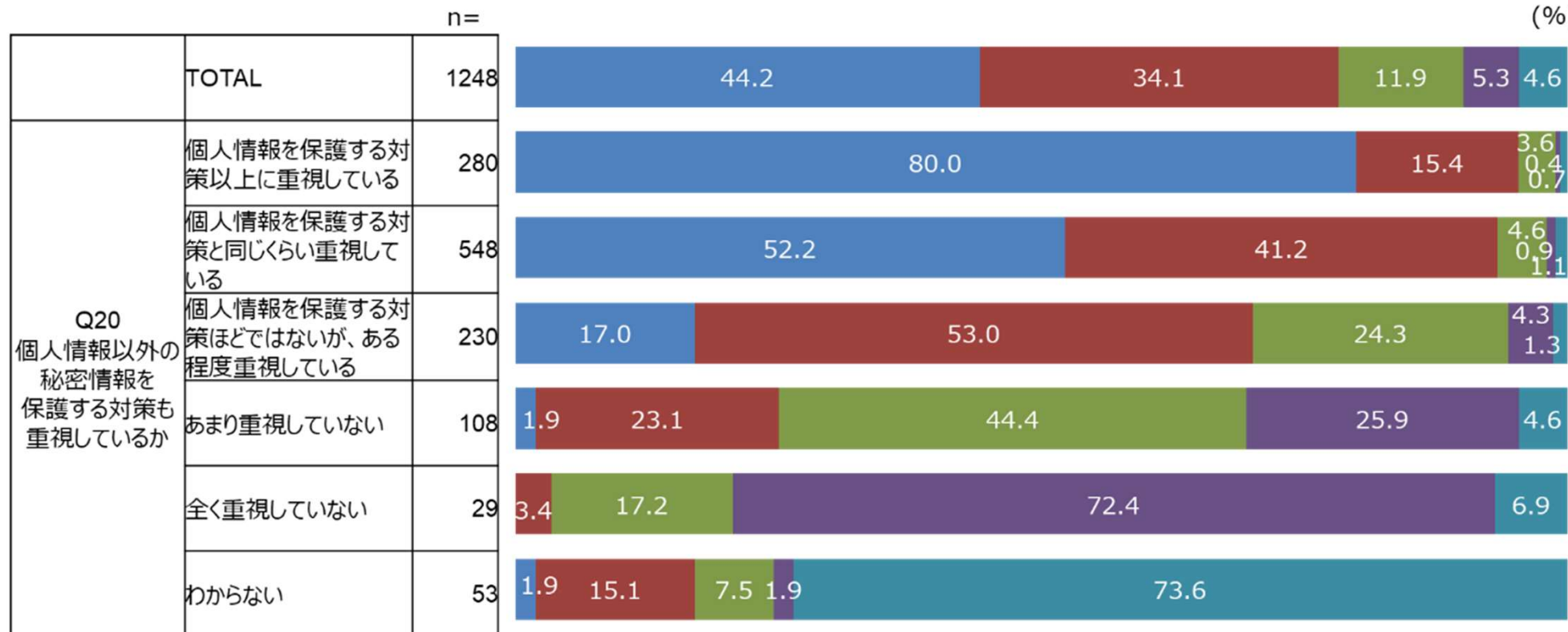
■ ほぼ漏れなく認知できる    ■ ときどき認知できないことがある    ■ ほとんど認知できない    ■ そもそも格付けが表示されていない    ■ わからない





**Q16.秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際の適切な行動について、社員教育等で組織全体に周知・徹底していますか。あてはまるものを1つお選びください。(単一選択)**

■ 定期的に周知・徹底している    ■ 必要に応じて一部を周知している    ■ ほとんど周知していない    ■ 全く周知していない    ■ わからない (%)

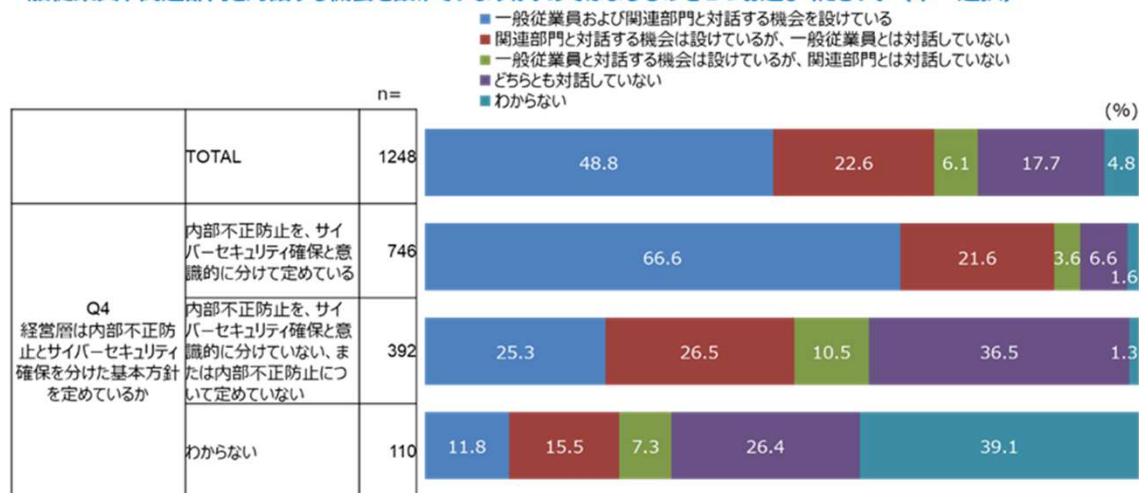


**Q22.以下に列挙した「秘密情報の漏えいに繋がる内部不正の防止」に特有の対策のうち、貴社で実際に実施しているものはどれですか。あてはまるものをすべてお選びください。（複数選択）**

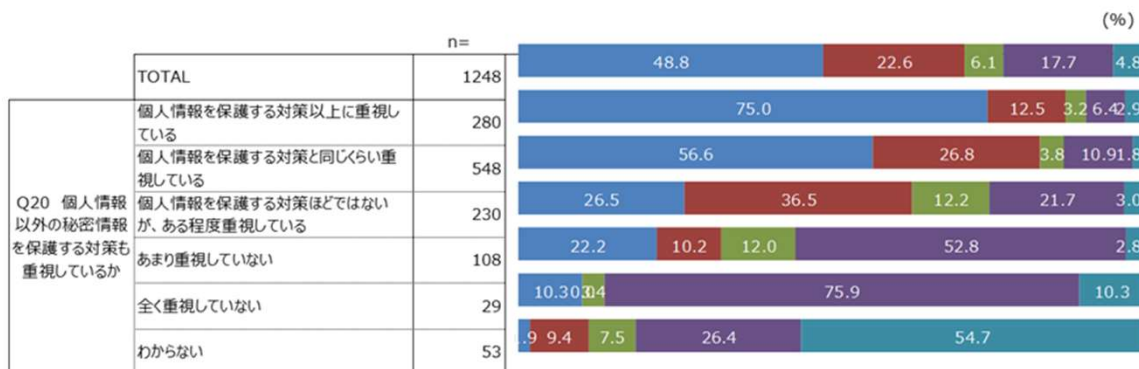
（％）

|                                              |                                                     |      | 1. 秘密情報の不正な開示・漏えいに繋がるように、会社等への不満・鬱憤を蓄積させない職場環境（過度の超過勤務がない、公平に評価されるハラスメント行為がない、良好なコミュニケーションが確保されている等）を整備している | 2. 就業規則に従業員の秘密保持義務を明記し、雇用開始時、及び雇用終了時に秘密保持義務に関する契約または誓約書の提出を求めている | 3. 重要な秘密情報を取り扱うプロジェクトへの参加／離任にあたり、秘密保持義務に関する誓約書を提出することを義務付けている | 4. 人的ミス（電子メールの誤送信、PC/USBメモリの紛失セキュリティ設定ミス等）への十分な注意を指示・徹底している | 5. 社内システム等の操作の異常や不正の可能性（深夜や休日の操作大量のファイルダウンロードなど）を、ログに基づいて定期的に確認している | 6. 中途退職を予定している従業員については、過去に遡って5.のログ確認を実施している | 7. 5.や6.の対策実施を従業員に周知し、不正の抑止力として役立てている | 8. 秘密情報の漏えいに繋がる内部不正に対する罰則を定めて、社員教育等で従業員に周知・徹底している | 9. テレワークやクラウドサービスで取り扱うことができる秘密情報を制限するための基準を設け、社員教育等で従業員に周知・徹底している | 10. 必要な秘密情報を取引先等に渡さないように、社員教育等で従業員に周知・徹底している | 11. 秘密情報の漏えいに繋がる内部不正の防止対策は実施していない | 12. わからない |
|----------------------------------------------|-----------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------|---------------------------------------|---------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------|-----------------------------------|-----------|
|                                              | TOTAL                                               | 1248 | 57.6                                                                                                        | 54.4                                                             | 25.6                                                          | 50.5                                                        | 36.2                                                                | 17.0                                        | 14.9                                  | 23.2                                              | 33.7                                                              | 32.4                                         | 6.8                               | 6.1       |
| Q4<br>経営層は内部不正防止とサイバーセキュリティ確保を分けた基本方針を定めているか | 内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている                   | 746  | 72.5                                                                                                        | 65.4                                                             | 32.6                                                          | 61.3                                                        | 47.7                                                                | 24.7                                        | 21.3                                  | 30.6                                              | 47.5                                                              | 39.7                                         | 1.1                               | 1.3       |
|                                              | 内部不正防止を、サイバーセキュリティ確保と意識的に分けていない、または内部不正防止について定めていない | 392  | 38.3                                                                                                        | 43.1                                                             | 16.3                                                          | 39.0                                                        | 21.4                                                                | 6.1                                         | 6.4                                   | 13.5                                              | 15.1                                                              | 24.2                                         | 16.8                              | 4.1       |
|                                              | わからない                                               | 110  | 25.5                                                                                                        | 20.0                                                             | 11.8                                                          | 18.2                                                        | 10.9                                                                | 3.6                                         | 1.8                                   | 7.3                                               | 6.4                                                               | 11.8                                         | 10.0                              | 45.5      |

Q3. 経営層は、「秘密情報の漏えいに繋がる内部不正」(注5)への対応方針等について、一般従業員や関連部門と対話する機会を設けていますか。あてはまるものを1つお選びください。(単一選択)

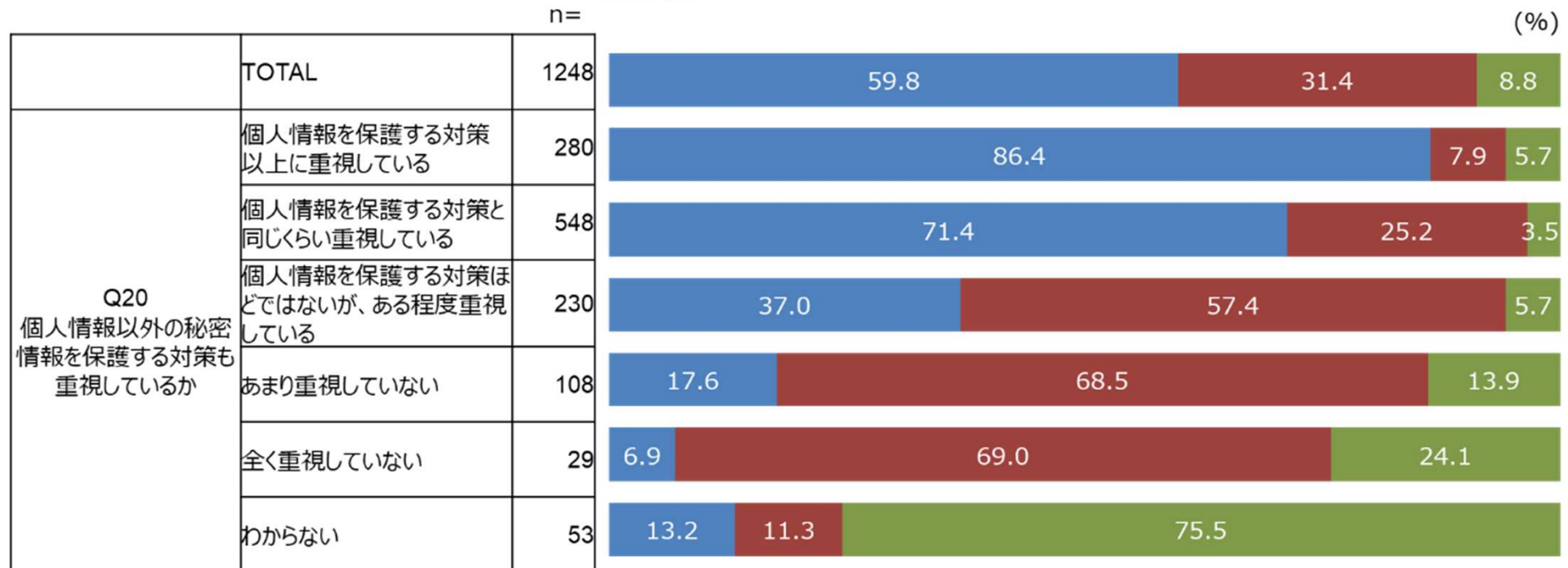


(注5) 例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。



#### Q4.経営層は、秘密情報保護に関する基本方針等で、内部不正防止（注5）をサイバーセキュリティ確保と意識的に分けて定めていますか。あてはまるものを1つお選びください。（単一選択）

- 内部不正防止を、サイバーセキュリティ確保と意識的に分けて定めている
- 内部不正防止を、サイバーセキュリティ確保と意識的に分けていない、または内部不正防止について定めていない
- わからない

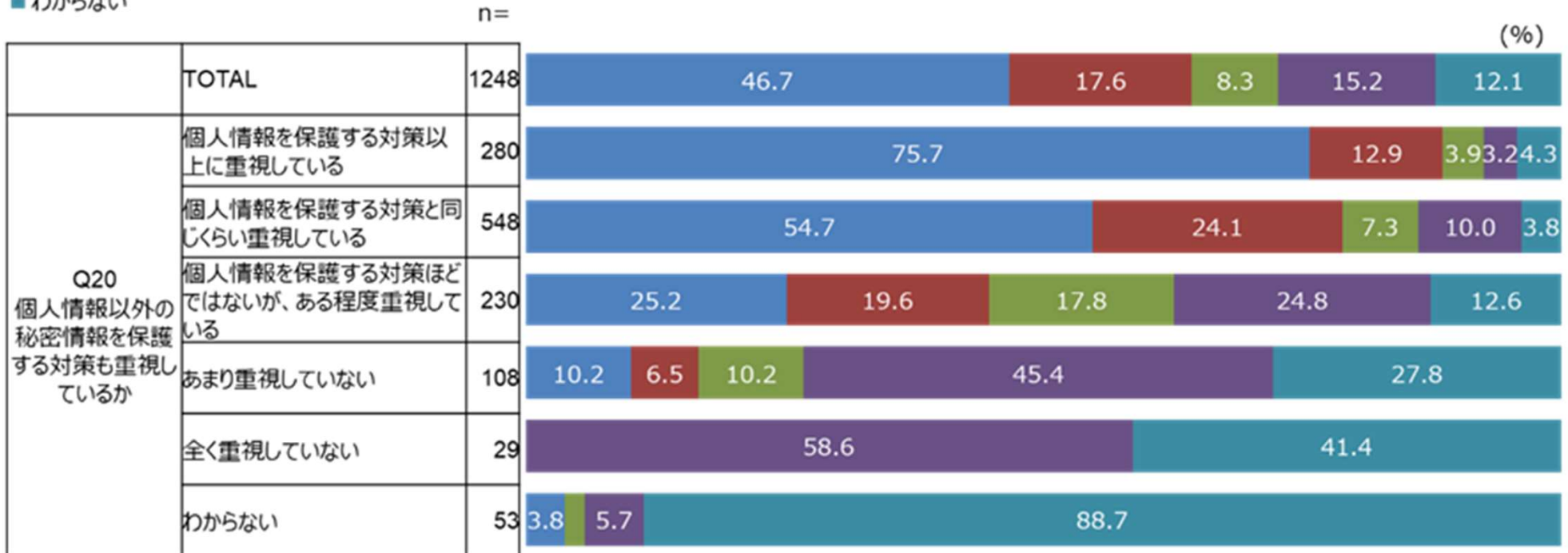


（注5：再掲）例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。



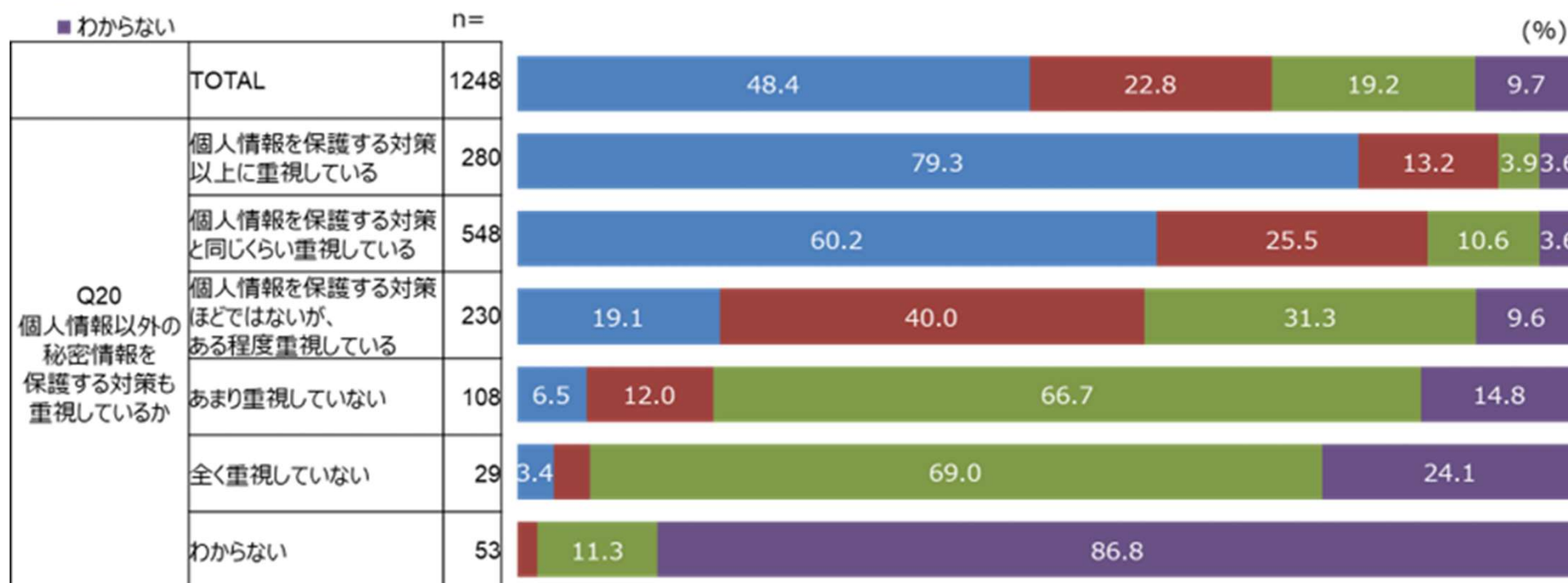
### Q21.「秘密情報の漏えいに繋がる内部不正（注5）リスク」を、「サイバー攻撃リスク」や「会計不正・ハラスメント等のリスク」と意識的に分けて評価していますか。あてはまるものを1つお選びください。（単一選択）

- 「サイバー攻撃リスク」や「会計不正・ハラスメント等のリスク」と意識的に分けて評価している
- 「サイバー攻撃リスク」とは分けて評価しているが、「会計不正・ハラスメント等のリスク」とは一緒に評価している
- 「会計不正・ハラスメント等のリスク」とは分けて評価しているが、「サイバー攻撃リスク」とは一緒に評価している
- 「サイバー攻撃リスク」と「会計不正・ハラスメント等のリスク」を評価するのみであり、「秘密情報の漏えいに繋がる内部不正リスク」をわざわざ切り出して評価することはない
- わからない



**Q23. 上述した「秘密情報の漏えいに繋がる内部不正の防止対策」を「サイバー攻撃対策」や「会計不正・ハラスメント等の対策」と意識的に使い分けていますか。あてはまるものを1つお選びください。(単一選択)**

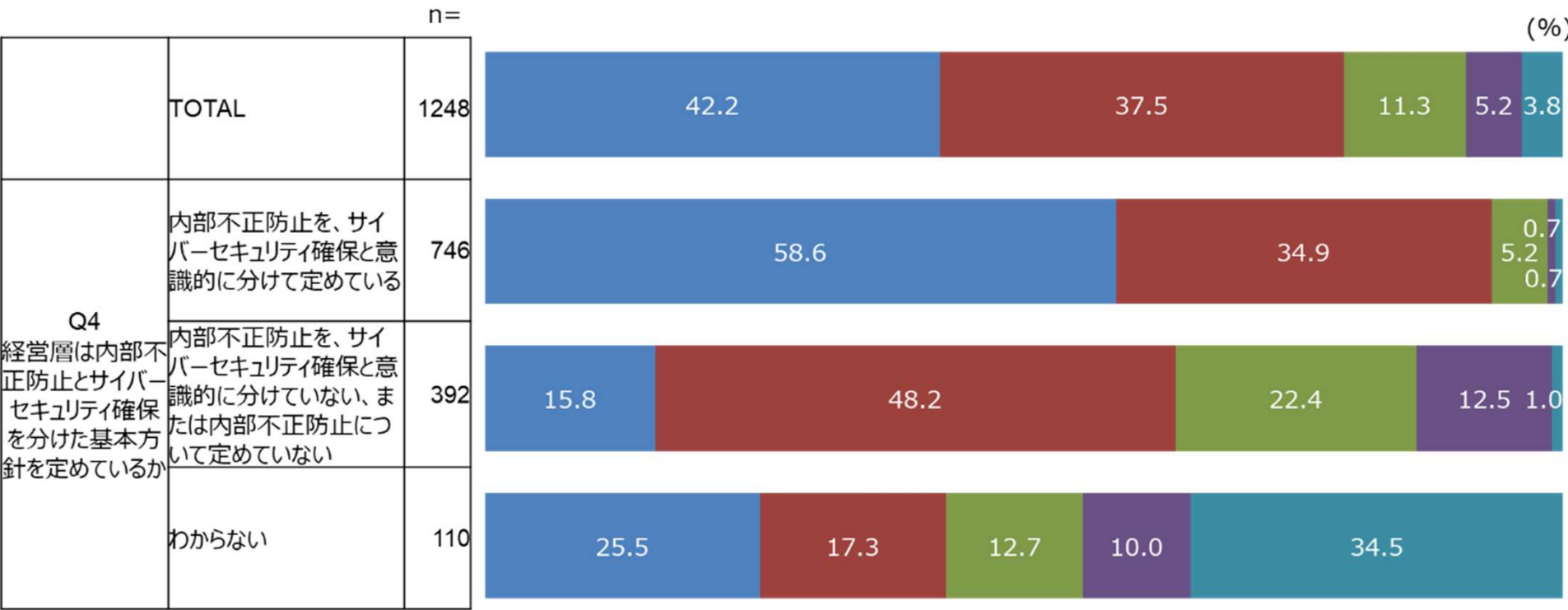
- 経営層が指示した基本方針に基づいて対策を意識的に使い分けており、定期的に経営層にその有効性を報告している
- 「サイバー攻撃対策」または「会計不正・ハラスメント等の対策」を実施する現場部門の裁量で対策を使い分けているが、経営層はその使い分けを把握していない
- 対策の意識的な使い分けは行っていない、または「秘密情報の漏えいに繋がる内部不正の防止対策」は実施していない
- わからない



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

Q14.貴社では、個人情報以外の秘密情報（営業秘密、重要なデータ等）の保護が、個人情報保護と同じように重要であることを周知・教育していますか。あてはまるものを1つお選びください。(単一選択)

■ 定期的にしっかりと周知・教育している ■ 必要に応じて時々周知・教育している ■ ほとんど周知・教育していない ■ 全く周知・教育していない ■ わからない



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

Q20.個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策も重視していますか。  
あてはまるものを1つお選びください。(単一選択)

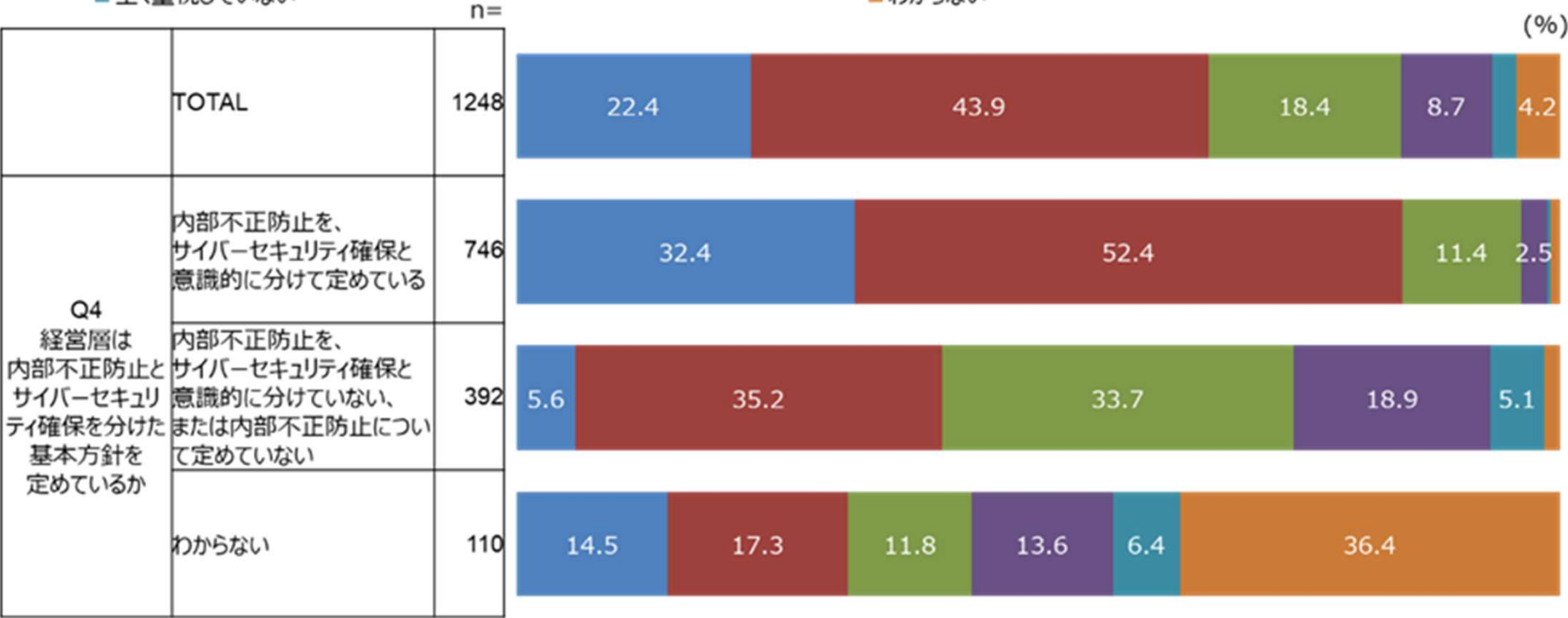
- 個人情報を保護する対策以上に重視している

■ 個人情報を保護する対策ほどではないが、ある程度重視している

■ 全く重視していない
- 個人情報を保護する対策と同じくらい重視している

■ あまり重視していない

■ わからない



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

凡例：サプライヤーを選ぶ際に有効な着眼点を示す😊

実態調査結果から分かる  
サプライチェーン管理における  
秘密情報漏えい／内部不正防止のポイント



## 3-1 経営課題の改善

**中小企業では**、経営者と従業員の距離が近く、**経営者次第**で秘密情報漏えい／内部不正の防止の取組が大きく変わってくる。

- サプライヤーの秘密情報漏えい／内部不正防止を考える上では、この問題に関する**経営者のアウェアネス、経営方針およびリーダーシップ**を見る（**経営者に直接確認**する）ことが良い指標になる。
  - 営業秘密管理、技術情報管理への取組状況を確認
  - 経営者から従業員への意識付け、方針の周知徹底などを確認



## 3-1 経営課題の改善

### 【経営者のアウェアネスを高める】

大企業との比較から、中小企業では秘密情報漏えい／内部不正防止に対する経営者のアウェアネスを高める必要があると考えて、改善策の実施状況を調査した。

- **実態調査結果では**、秘密情報漏えい／内部不正リスクに対する経営層の認識は、中小企業が全般に低くはあるものの、思ったほどの差はなかった。但し、取引先やクラウドサービスからの漏えいについては差が大きく、**サプライチェーンに対する中小企業の経営者のリスク認識は危惧される状況**であると示唆された。
- **インタビュー調査で**、秘密情報漏えい／内部不正防止の取組が**優れた複数の中小企業の実態を把握**したが、その**高い充実度・意欲**と、低調なアンケート調査結果との大きな違いに**強い印象を受けた**。

| 改善策に関わる好事例                                                                                                                                                                                         | 改善策を補う示唆                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• 業界の流れを意識し、技術情報管理の認証取得に取り組んだことが良い契機となった。</li><li>• 秘密情報との関りが深い事業を展開しているため自社でもしっかり取り組むことが必須だった。</li><li>• 悪意の有無に関わらず、人為的な秘密情報漏えいのリスクが高いと考えて経営している。</li></ul> | <ul style="list-style-type: none"><li>• 中小企業では経営層が高い意識を持って率先し牽引すれば会社全体の取組状況をがらりと変えられる可能性を持っている。</li><li>• 経営層が秘密情報の漏えいや内部不正防止について全社にしっかりと自分の経営方針を話していくことが望ましい。</li><li>• 中小企業では、営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。</li></ul> |

## 3-1 経営課題の改善

### 【経営者のアウェアネスを高める】

中小企業では、**経営者次第で**秘密情報漏えい／内部不正の防止の**取組が大きく変わってくる**にも関わらず、当該主題にほとんど関心がない経営者が多い点が一番の問題点。しかし、**経営者には学びを得るための実践的な機会も存在**している。

### ＜経営者が「秘密情報漏えい／内部不正の防止」の重要さを学ぶ機会（例）＞

- 業界団体による**業界全体での意識付け**（日本金型工業会の取組など）
- **情報管理認証の取得**（技術情報管理認証、ISMSなど）、ITコーディネータ等の外部専門家による支援 😊
- **営業秘密管理を社内に導入することに着手**、中小企業向けの知財戦略アドバイザーの活用 😊
- 痛い目に遭って経験する／他社の事例から学ぶ 等

**Q2.経営層や、秘密情報保護を統括する組織等の責任者は、秘密情報の漏えいに関するどのようなリスクが高いと認識していると思いますか。あてはまるものをすべてお選びください。（複数選択）**

(%)

|                                                             |               |      | (過度の<br>超過勤務、<br>不公平な<br>評価、ハラ<br>スメント等<br>に対して)<br>不満を蓄積<br>した従業員<br>による<br>秘密情報<br>の漏えい | 産業スパ<br>イによる<br>秘密情報<br>の漏えい | 中途退職<br>者による<br>秘密情報<br>の漏えい | 電子メー<br>ルの<br>誤送信、<br>PCや<br>USBメモ<br>リの紛失等<br>の人的ミス<br>による<br>秘密情報<br>の漏えい | クラウド<br>サービス<br>からの<br>秘密情報<br>の漏えい | 国内の<br>取引先<br>または<br>国内子会<br>社からの<br>秘密情報<br>の漏えい | 海外の<br>取引先<br>または<br>海外子会<br>社からの<br>秘密情報<br>の漏えい | テレワーク<br>による<br>秘密情報<br>の漏えい | サイバー攻<br>撃による<br>秘密情報<br>の漏えい | 秘密情報<br>の漏えい<br>や、それに<br>関する<br>内部不正<br>に関する<br>リスクを<br>あまり重視<br>していない | わからない |
|-------------------------------------------------------------|---------------|------|-------------------------------------------------------------------------------------------|------------------------------|------------------------------|-----------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------|---------------------------------------------------|------------------------------|-------------------------------|------------------------------------------------------------------------|-------|
|                                                             | TOTAL         | 1248 | 42.2                                                                                      | 17.2                         | 50.0                         | 59.1                                                                        | 32.7                                | 29.3                                              | 19.2                                              | 33.3                         | 50.6                          | 4.8                                                                    | 5.0   |
| SQ2<br>常用雇用者数<br>【ベース：SQ1=1-8<br>いずれかの業務担<br>当・責任者・経営<br>者】 | 21～50人        | 214  | 35.0                                                                                      | 9.3                          | 54.7                         | 49.5                                                                        | 21.0                                | 17.8                                              | 7.5                                               | 24.3                         | 39.7                          | 8.4                                                                    | 5.1   |
|                                                             | 51～100人       | 167  | 42.5                                                                                      | 11.4                         | 46.1                         | 61.1                                                                        | 27.5                                | 23.4                                              | 7.8                                               | 29.3                         | 49.7                          | 4.8                                                                    | 7.2   |
|                                                             | 101～300人      | 239  | 40.2                                                                                      | 9.6                          | 44.4                         | 56.1                                                                        | 25.9                                | 20.5                                              | 8.8                                               | 25.1                         | 46.0                          | 5.9                                                                    | 5.0   |
|                                                             | 301人～1,000人   | 223  | 39.9                                                                                      | 20.6                         | 52.0                         | 61.9                                                                        | 38.1                                | 31.8                                              | 19.7                                              | 39.0                         | 52.9                          | 4.0                                                                    | 3.1   |
|                                                             | 1,001人～5,000人 | 205  | 50.2                                                                                      | 17.6                         | 48.8                         | 62.0                                                                        | 38.5                                | 34.6                                              | 26.3                                              | 39.0                         | 55.1                          | 2.9                                                                    | 4.9   |
|                                                             | 5,001～10,000人 | 73   | 49.3                                                                                      | 38.4                         | 57.5                         | 72.6                                                                        | 39.7                                | 52.1                                              | 39.7                                              | 43.8                         | 67.1                          | 0.0                                                                    | 0.0   |
|                                                             | 10,001人以上     | 127  | 44.9                                                                                      | 33.9                         | 52.0                         | 61.4                                                                        | 48.8                                | 47.2                                              | 48.8                                              | 43.3                         | 57.5                          | 3.9                                                                    | 7.9   |

 (出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 3-1 経営課題の改善

### 【経営者がリーダーシップを発揮する】

大企業との比較から、中小企業では経営者と従業員の距離が近い。このため、社員が集まる機会等で経営者が全従業員に、秘密情報漏えい／内部不正防止に対する経営方針、判断、経験・ノウハウ等を直接伝えるのが良いと考えて、改善策の実施状況を調査した。

- **実態調査結果では、企業規模が小さくなるほど、経営層による一般従業員・関連部門との対話への取組度合いが弱くなっており、こうした対話への取組が奏功した場合の効果が大きく期待できる中小企業の強みを活かしていないことがわかった。**
- **インタビュー調査では、経営者が直接、従業員に向けて日常的にリスク認識、基本方針等を伝えること（中小企業ならではのリーダーシップ発揮）の効果が確かめられた。また有識者からは、埋めるべきギャップは中小企業の方が小さく、動き始めれば目標レベルへの到達が早いこと（小回りの利く機動力）を念頭に、経営者が何をどの程度重視しているかを、想いやこだわりを込めて従業員に率直に伝える😊のが良いという示唆が得られた。**

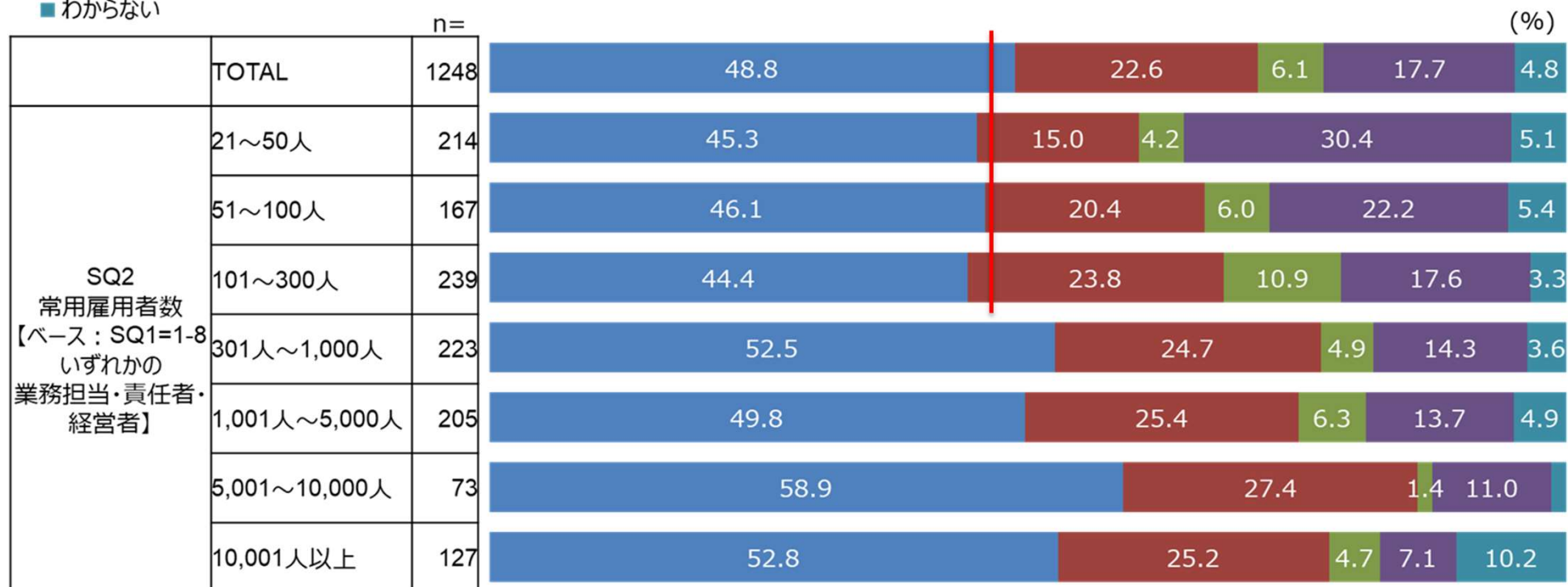
| 改善策に関わる好事例                                                                                                                                                                                                                                                                                                                                      | 改善策を補う示唆                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>・ 経営者が自ら基本方針を全社に周知・徹底している。</li><li>・ 定期的にも日常的にも経営者が社員に語ることで意識付け・啓発に効果を上げている。</li><li>・ 漏えいが自社の信頼失墜に直結することを強く認識して全社に周知・啓発している。</li><li>・ 秘密情報漏えい／内部不正防止の取組が特に進んでいる中小企業では、情報漏えい／内部不正防止に関する基本方針を情報セキュリティポリシーとは完全に別建てで定めている。</li><li>・ ISMS、プライバシーポリシー、技術情報管理等の認証取得が、中小企業の経営者が基本方針を定める契機となって取組が進んだ。</li></ul> | <ul style="list-style-type: none"><li>・ 従業員と直接コミュニケーションを取って趣旨をしっかりと伝えることで、ある程度リスクに対応できる。</li><li>・ 中小企業の取組強化に向けては、経営者が戦略を語り、コミットメントや指示に自身の想いやこだわりを込め、日々語ることが重要である。</li><li>・ 経営層が何をどの程度重視しているかを率直に伝えることで、従業員がこれを評価して行動することを期待できる。</li><li>・ 埋めるべきギャップは大企業より中小企業の方が小さいので、ひとたび良い方向に動き始めると、目標レベルに素早く到達できる。</li><li>・ 中小企業の規模やリソースを考慮すると、秘密情報漏えい／内部不正防止とサイバーセキュリティを敢えて分けて取り組む必要はない。</li></ul> |

（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>



**Q3. 経営層は、「秘密情報の漏えいに繋がる内部不正」(注5) への対応方針等について、一般従業員や関連部門と対話する機会を設けていますか。あてはまるものを1つお選びください。(単一選択)**

- 一般従業員および関連部門と対話する機会を設けている
- 一般従業員と対話する機会を設けているが、関連部門とは対話していない
- 関連部門と対話する機会を設けているが、一般従業員とは対話していない
- どちらとも対話していない
- わからない



(注5：再掲) 例えば、会社等への不満・鬱憤をきっかけとした秘密情報の開示・漏えい、離職前の秘密情報持ち出し・転職先での利用、不注意による秘密情報の社外送信／公開・記録媒体の紛失等がある。

(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 3-2 重要な秘密の特定と取扱いの改善

### 1. 委託元企業の皆様：委託する側として、まずはセルフチェックしてみよう。

- 「極秘」「社外秘」の情報資産の特定漏れがあるかも知れません。
- 「極秘」と「社外秘」、「社外秘」と「一般情報」の区分にブレがあるかも知れません。
- 「極秘」「社外秘」の区分表示に漏れがあるかも知れません。また、取引先に開示する資料に自社の秘密であることを明記できていますか。

INPIT よくあるご相談：営業秘密のQ&A（中小企業向け）から抜粋  
あらかじめ自社の強みとなる情報資産を把握して、分類して区分ごとに取扱いの基準を定めておきましょう。 …

- (1) 「どんなことがあっても他社に伝えない情報」（極秘）
- (2) 「秘密保持契約を交わせば他社に伝えてもよい情報」（社外秘）
- (3) 「通常の営業活動で他社（顧客、発注者等）に伝えても良い情報」（一般情報）

また、資料を開示するのであれば、必要最小限としたうえ、資料等に自社の秘密であることを明記、…

2. 一般論としては、サプライヤー企業では、機微な技術情報の漏えい防止や内部不正防止は十分ではないという前提に立って考えるべき。一方で、これが当てはまらない優れたサプライヤーはおり、インタビュー調査で変革の契機となった好事例が2つ判明した。



## 3-2 重要な秘密の特定と取扱いの改善

秘密情報漏えい／内部不正防止を進める上で基盤となるのが、何が守るべき秘密であるかということを確認にし、従業員自身がそれを認知し、適切に行動できる環境を作ることだと考え、その具体化となる、①秘密の特定および格付けルール策定や表示の徹底、②格付け表示等による秘密情報の認知向上の実施状況を調査した。

■ 実態調査結果から、企業規模に拠らず、実施状況が十分とは言えないことが判明。**大企業であっても安心せず、サプライヤーに委託する側として**、自社の現状をまずセルフチェックしておくが良い。

- 営業秘密等を**漏れなく特定**するための基準とその全社運用ルールを定めているか？ **55.4%が実施**
- **格付け**のための基準とその全社運用ルールを定めているか？ **33.3%が実施**
- 格付けをわかりやすく**表示**するためのルールを定めているか？ **18.0%が実施**
- 格付け等の**表示によってほぼ漏れなく**秘密情報であることを**認知**できるか？ **30.3%が可能**

■ インタビュー調査では、情報資産管理（特に台帳管理）が**各従業員の秘密保護への貢献を可視化**するため、**満足感とやる気の醸成を期待できる**という示唆が得られた。

| 改善策に関わる好事例                                                                               | 改善策を補う示唆                                                                                                                                                                          |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ・ <b>技術・事業・営業・取引等のノウハウについても、特定すべき重要な営業秘密として、価値を決めることが必要</b> で、大企業ではこの問題意識を持つ担当者が育ってきている。 | ・ 知らないうちに競合他社に持ち出されるくらいならば営業秘密をきちんと明確化しておこうという動機付けをするのがよい。<br>・ 会社にとって有用な営業秘密をリストアップし、 <b>自分たちがやっている仕事はその保護に貢献していることが可視化されると</b> 、会社の重要な仕事に <b>貢献しているという認識と満足感が浸透</b> することを期待できる。 |

（出典）2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 3-2 重要な秘密の特定と取扱いの改善

中小企業における ①秘密の特定および格付けルール策定や表示の徹底、②格付け表示等による秘密情報の認知向上の実施状況は、大企業と比べると、かなり差があるのが実状。

### ■ 実態調査結果：従業員千人以上の大企業と100人以下の中小企業間の格差の現状

| 望ましい取組                                | 大企業の実施状況<br>(従業員数千人以上) | 中小企業の実施状況<br>(従業員数100人以下) |
|---------------------------------------|------------------------|---------------------------|
| 営業秘密等を漏れなく特定するための基準とその全社運用ルールを定めているか？ | 63.9%～75.6%            | <b>32.2%～44.9%</b>        |
| 格付けのための基準とその全社運用ルールを定めているか？           | 35.1%～44.9%            | <b>15.4%～22.8%</b>        |
| 格付けをわかりやすく表示するためのルールを定めているか？          | 17.6%～37.8%            | <b>7.9%～10.8%</b>         |
| 格付け等の表示によってほぼ漏れなく秘密情報であることを認知できるか？    | 35.1%～50.7%            | <b>21.5%～22.2%</b>        |

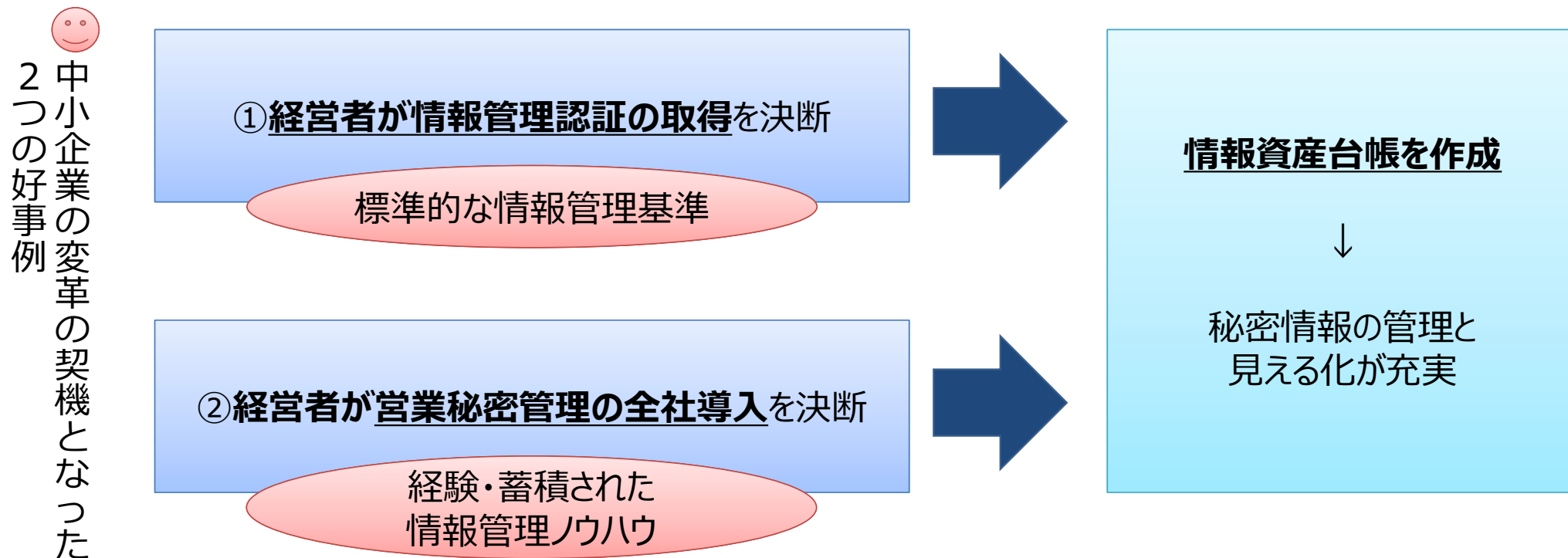
### ■ インタビュー調査では、**経営者が自ら**事業リスクを**判断**し、秘密情報の特定・格付けを**リード**し、情報管理認証の取得や営業秘密管理の導入を**決断**し、情報資産台帳を**作成した**ことで、傑出した中小企業に成長できた**好事例**を見いだせた。

| 改善策に関わる好事例                                                                                                                                                                                                                                                                                                                                                                                 | 改善策を補う示唆                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っている。</li><li>経営者が情報セキュリティや技術情報管理の認証取得を決断し、これに取り組んだことが契機となつて、営業秘密等の特定、格付け、表示に関する体制整備が進んだ。</li><li>認証制度が要求する管理基準に従い、秘密情報を管理できる情報資産台帳を作成している。</li><li>認証制度に沿って特定した情報資産については、情報の保存場所や保存期間、データ消去の方法やリスクの大きさ、格付けを台帳管理している。</li><li>情報資産を保存する共有フォルダ等の場所を格付けに沿って切り分け、かつ、適切なアクセス制御・記録を合わせることで、格付け・表示・アクセス管理を一体に実施している。</li></ul> | <ul style="list-style-type: none"><li>中小企業では、<b>営業秘密を社内できちんと保護する体制を構築することで、秘密情報漏えい／内部不正防止にも好ましい効果が生じる。</b></li><li>経営者の負担を避けるため、部下を育成し、権限移譲を考えることも必要である。</li></ul> |

(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

## 3-2 重要な秘密の特定と取扱いの改善

中小企業の秘密情報保護／内部不正防止の充実に向けて、経営者が標準／ノウハウに準拠した情報管理の導入に自ら取り組むことは重要。標準的な基準に従うことで、情報資産台帳の作成が不可欠になり、秘密情報の管理と見える化の充実が導かれる。委託元企業はサプライヤーの選択にあたり、経営者がこうした取組にどのようにコミットしているかを、経営者から直接聞き取って評価😊すると良い。



**Q7.個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けの実効性を高めるために、組織全体でどのような取組を実施していますか。あてはまるものをすべてお選びください。（複数選択）**

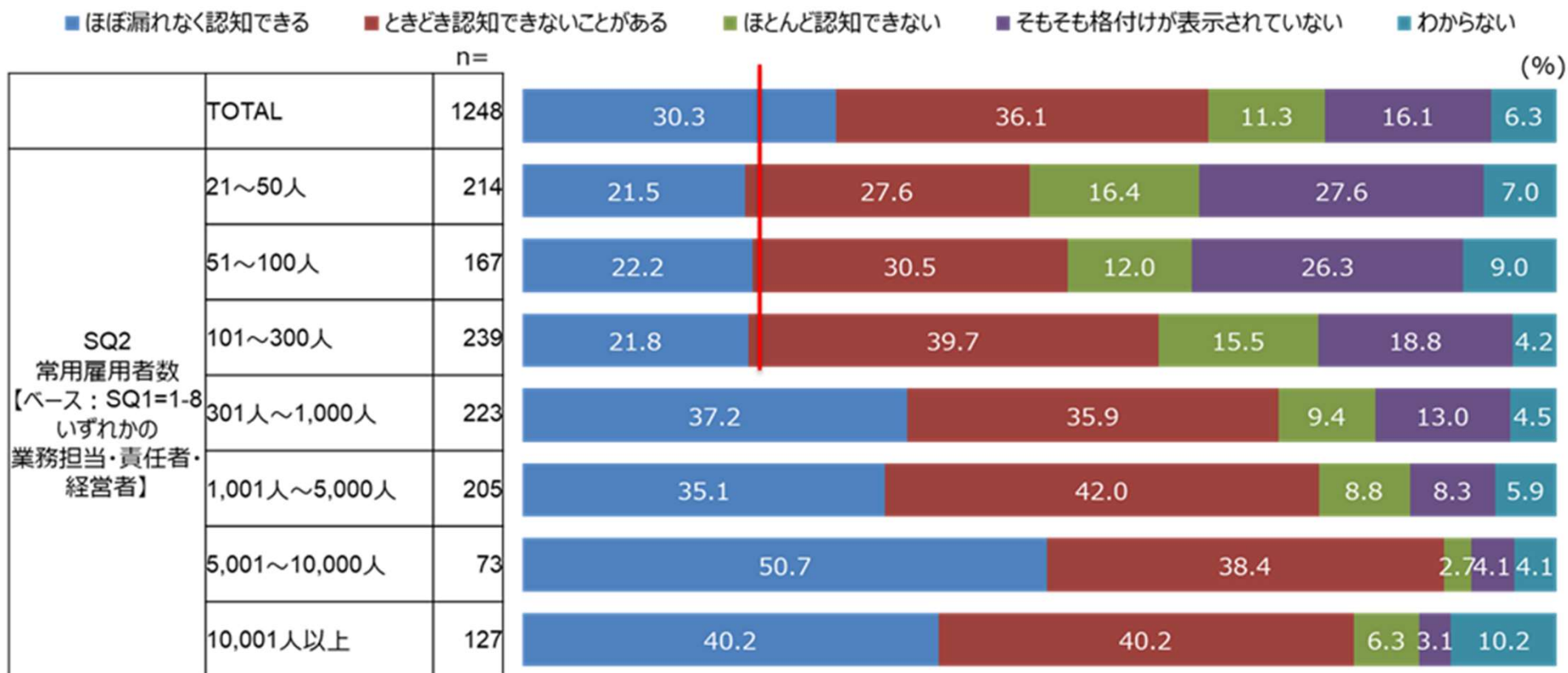
（%）

|                                                             |               | n=   | 個人情報<br>以外の<br>秘密情報<br>（営業秘密、<br>重要なデータ<br>等）を特定<br>するための具<br>体的な基準<br>や、この基準の<br>全社運用を<br>求める共通<br>ルール等を<br>定めている | 個人情報<br>以外の<br>秘密情報を<br>格付けする<br>ための基準や<br>この基準の<br>全社運用を<br>求める共通<br>ルール等を<br>定めている | 個人情報<br>以外の<br>秘密情報を<br>特定または<br>格付けする<br>基準を適用<br>しやすいよう<br>例を示してい<br>る | 格付けが<br>漏れなく<br>実行される<br>ための仕組み<br>を設け、<br>継続的な<br>改善を<br>図っている | 格付けを<br>わかりやすく<br>表示するた<br>めのルールを<br>定めている | 格付け表示<br>がない<br>（不明瞭な<br>場合を含<br>む）<br>社内情報の<br>取扱いに<br>ついても<br>ルールを<br>定めている | 重要な秘密<br>情報を取り扱<br>うプロジェクト<br>に参加する条<br>件として、「保<br>護対象とする<br>重要な秘密<br>の範囲を明<br>確にした上で、<br>上述した基<br>準やルールの<br>順守・徹底を<br>あらためて誓<br>約すること」を<br>求めるルール<br>を定めている | 定期的に、<br>基準やルール<br>を順守して<br>いるかを<br>確認している<br>（定期的な<br>セルフチェック<br>を含む） | 何も実施して<br>いない | 上記以外 | わからない |
|-------------------------------------------------------------|---------------|------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|---------------|------|-------|
|                                                             | TOTAL         | 1248 | 55.4                                                                                                               | 33.3                                                                                 | 27.9                                                                     | 18.3                                                            | 18.0                                       | 15.4                                                                          | 17.4                                                                                                                                                         | 37.4                                                                   | 11.9          | 0.4  | 4.7   |
| SQ2<br>常用雇用者数<br>【ベース：<br>SQ1=1-8いづれ<br>かの業務担当・<br>責任者・経営者】 | 21～50人        | 214  | 32.2                                                                                                               | 15.4                                                                                 | 16.4                                                                     | 7.5                                                             | 7.9                                        | 8.9                                                                           | 7.0                                                                                                                                                          | 24.8                                                                   | 29.4          | 0.0  | 5.6   |
|                                                             | 51～100人       | 167  | 44.9                                                                                                               | 22.8                                                                                 | 19.2                                                                     | 11.4                                                            | 10.8                                       | 13.8                                                                          | 12.6                                                                                                                                                         | 28.1                                                                   | 19.2          | 1.2  | 7.8   |
|                                                             | 101～300人      | 239  | 50.6                                                                                                               | 34.3                                                                                 | 24.7                                                                     | 13.4                                                            | 12.1                                       | 12.1                                                                          | 14.2                                                                                                                                                         | 30.1                                                                   | 11.7          | 0.4  | 3.3   |
|                                                             | 301人～1,000人   | 223  | 64.6                                                                                                               | 29.6                                                                                 | 29.1                                                                     | 17.9                                                            | 22.4                                       | 15.7                                                                          | 17.5                                                                                                                                                         | 47.5                                                                   | 7.2           | 0.0  | 4.0   |
|                                                             | 1,001人～5,000人 | 205  | 63.9                                                                                                               | 39.0                                                                                 | 35.1                                                                     | 23.9                                                            | 17.6                                       | 15.1                                                                          | 19.0                                                                                                                                                         | 40.5                                                                   | 3.9           | 0.0  | 4.9   |
|                                                             | 5,001～10,000人 | 73   | 75.3                                                                                                               | 56.2                                                                                 | 38.4                                                                     | 35.6                                                            | 37.0                                       | 21.9                                                                          | 35.6                                                                                                                                                         | 54.8                                                                   | 0.0           | 2.7  | 1.4   |
|                                                             | 10,001人以上     | 127  | 75.6                                                                                                               | 59.8                                                                                 | 44.9                                                                     | 36.2                                                            | 37.8                                       | 30.7                                                                          | 33.9                                                                                                                                                         | 52.0                                                                   | 1.6           | 0.0  | 4.7   |



(参考スライド)

**Q8.従業員は、自部署・他部署の情報に関わらず、個人情報以外の秘密情報に触れた際に、格付けの表示等によってほぼ漏れなく秘密情報であることを認知できますか。あてはまるものを1つお選びください。(単一選択)**



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>



### 3-3 全社でのリテラシー構築に関する課題の改善

**中小企業では、一般的傾向として、営業秘密等の漏えいが事業に及ぼすリスクの大きさを認識し、格付け・表示に基づく情報管理の必要性を理解し、不自然な取扱いや不正な漏えいを管理責任者等に報告するリテラシーが十分ではない。**また、従業員がこれらについて学ぶ機会も不足しており、他社で発生した参考事例の情報収集も難しい。

他方で、経営者が自ら営業秘密等の管理にコミットし、従業員のリテラシー教育にも注力している中小企業の中には、優れた好事例を多く実践して、全社でのリテラシー構築に成功している企業が見られた。 

■ サプライヤーの秘密情報漏えい／内部不正防止に関するリテラシーを量る上では、次のような好事例に着目すると良い :

- 経営者は事業リスクを従業員に語って聞かせているか
- 経営者が参考事例等の情報収集に直接関与し、従業員に事例からの気づきを与えているか
- 経営者は、全社に情報管理を定着させる意志を明示し、従業員に日頃から必要な取組、社内ルール等を説明しているか
- 経営者が、秘密情報の特定・格付けの判断を自ら行っている、または判断に直接関与しているか 等

### 3-3 全社でのリテラシー構築に関する課題の改善

中小企業における秘密情報保護／内部不正防止のリテラシー構築に関しては、営業秘密等の保護の重要性と格付け・表示による標準的な情報管理の必要性を従業員に浸透させることが必要だと考え、これらに関するリテラシー教育の実施状況を調査した。

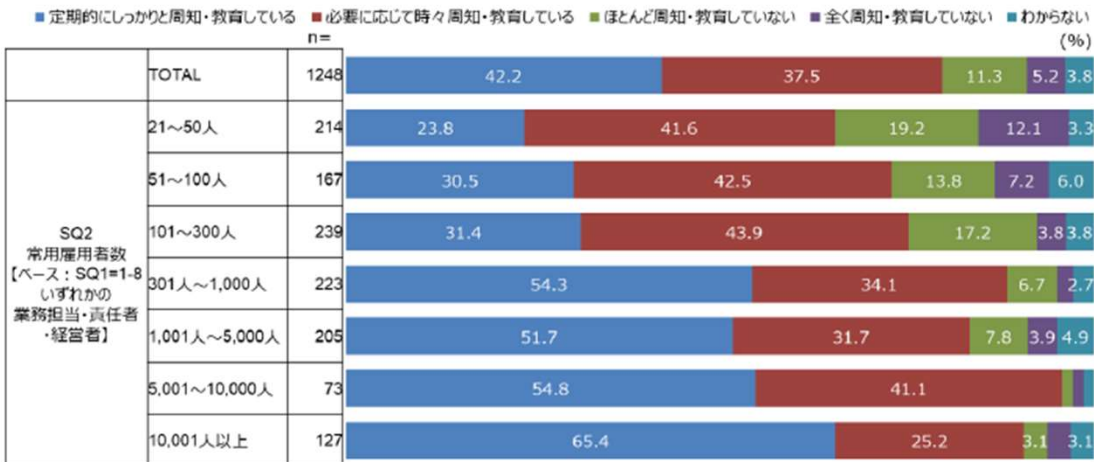
- 実態調査結果から、中小企業では営業秘密等の保護の重要性、格付け・表示による標準的な情報管理の必要性に関する教育が顕著に遅れている傾向が見られた。サプライヤーに営業秘密等を共有する際には、秘密保持契約の締結に加えて、委託元の営業秘密等であることの表示を義務付ける等が有効と考えられる。

| 望ましい取組                              | 大企業の実施状況<br>(従業員数千人以上) | 中小企業の実施状況<br>(従業員数100人以下) |
|-------------------------------------|------------------------|---------------------------|
| 営業秘密等の重要性を従業員に周知・教育しているか？           | 51.7%～65.4%            | <b>23.8%～30.5%</b>        |
| 営業秘密等の特定／格付けに係る全社基準を従業員に周知・徹底しているか？ | 50.7%～67.7%            | <b>29.4%～32.3%</b>        |

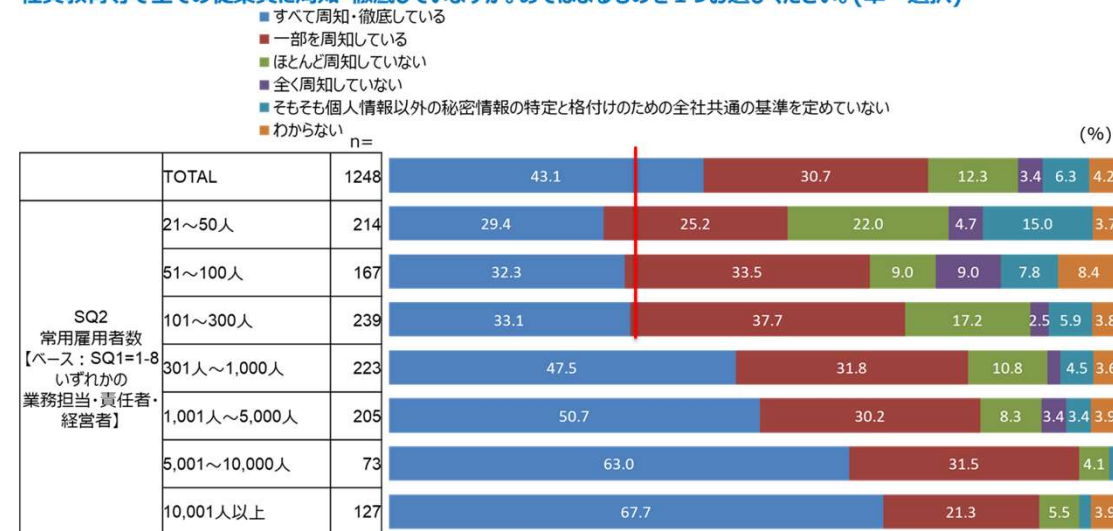
- インタビュー調査では、経営者が自ら事業リスクの判断や秘密情報の特定・格付けを行っているという好事例が見られた。また、経営者が情報管理認証の取得を決断することで、認証が求める管理基準に従って情報資産台帳の作成が進むため、従業員が秘密情報保護に貢献していることを実感できるようになると期待される。

## (参考スライド)

**Q14. 貴社では、個人情報以外の秘密情報（営業秘密、重要なデータ等）の保護が、個人情報保護と同じように重要であることを周知・教育していますか。あてはまるものを1つお選びください。（単一選択）**



**Q15. 個人情報以外の秘密情報（営業秘密、重要なデータ等）の特定と格付けのための全社共通の基準を、社員教育等で全ての従業員に周知・徹底していますか。あてはまるものを1つお選びください。（単一選択）**



### 3-3 全社でのリテラシー構築に関する課題の改善

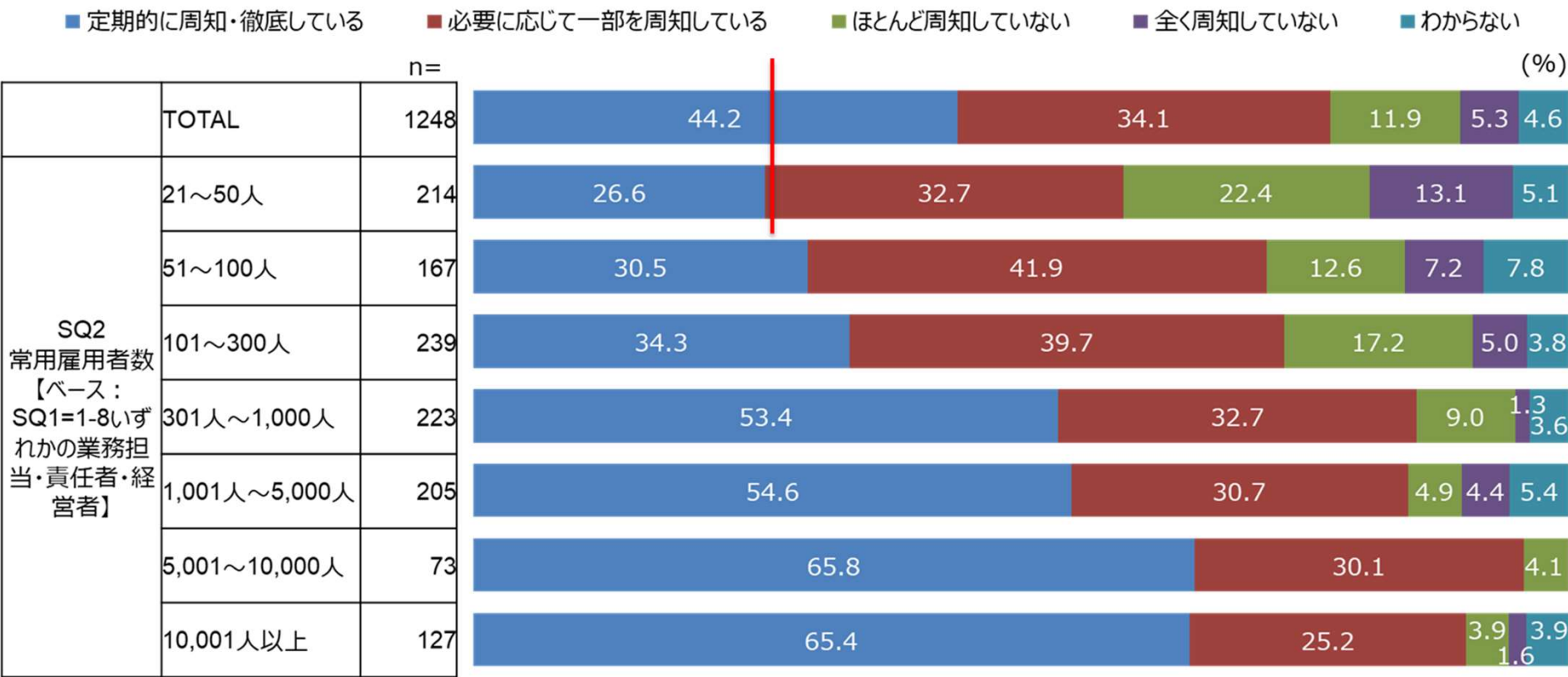
中小企業において、**発生した秘密情報漏えい／内部不正に管理責任者／経営者が早く気付くことが必要**と考え、これらを目撃した際の適切な行動に関するリテラシー教育の実施状況を調査した。

- 実態調査結果から、中小企業では秘密情報の不自然な取扱いや不正な漏えいを目撃した際の報告の必要性が社内に広く浸透していないことが懸念される。サプライヤーに営業秘密等を共有する際には、**不正や漏えいが発生した際のサプライチェーン全体での即応方針を定め**、サプライヤーに求めておくが良い。

| 望ましい取組                                          | 大企業の実施状況<br>(従業員数千人以上) | 中小企業の実施状況<br>(従業員数100人以下) |
|-------------------------------------------------|------------------------|---------------------------|
| 秘密情報の不自然な取扱いや不正な漏えいを目撃した際の報告について従業員に周知・徹底しているか？ | 54.6%～65.8%            | <b>26.6%～30.5%</b>        |

- インタビュー調査では、有識者から「中小企業には**営業秘密の秘密管理性の確保が自己防衛及びビジネス拡大に不可欠であることを大企業以上に認識してもらうことが望ましい**」という助言があった。

Q16. 秘密情報が不自然に取り扱われていることや、社外への不正な漏えいを目撃した際の適切な行動について、社員教育等で組織全体に周知・徹底していますか。あてはまるものを1つお選びください。(単一選択)



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>



## 3-4 対策実施に関する課題の改善

中小企業においても、**営業秘密等を保護する対策を講じることが重要**と考え、これをどの程度重視しているかの現状を調査した。

- 実態調査結果から、営業秘密等の保護対策をあまり重視していない中小企業は多く、企業規模が小さいほどその傾向が強まることが分かった。**サプライヤーに営業秘密等を共有する際には**、秘密保持契約の締結に加えて、**委託元の営業秘密等として厳しく管理**することを求める等が有効と考えられる。

| 望ましい取組                          | 大企業の実施状況<br>(従業員数千人以上) | 中小企業の実施状況<br>(従業員数100人以下) |
|---------------------------------|------------------------|---------------------------|
| 個人情報保護だけでなく、営業秘密保護等の対策も重視しているか？ | 75.1%～85.9%            | <b>50.5%～52.1%</b>        |

- インタビュー調査では、有識者から「営業秘密管理の導入が秘密情報保護だけでなく、内部不正防止のための対策向上にも役立つ」という示唆が得られた。サプライチェーン管理においては、**サプライヤーが全社に営業秘密管理の導入を進めているかを確認**することも有益である。

| 改善策に関わる好事例                                                                                                                                                                                                        | 改善策を補う示唆                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>・ 経営者のリーダーシップの下で、採用・退職・プロジェクト異動等の際に、都度必要な秘密保持義務契約を締結している。</li><li>・ 社長の意識づけに従い、プロジェクトごとに情報資産を定義しており、これに基づいて秘密情報を識別できるようにしている。これを活用し、秘密保持義務契約の対象となる秘密情報を具体的に示している。</li></ul> | <ul style="list-style-type: none"><li>・ <b>営業秘密を管理するための体制、何が秘密なのかをきちんと資産管理すること等から着手し、これを社内に浸透させていく過程で、自然に内部不正防止・営業秘密保護・サイバーセキュリティの全ての質が向上する。</b></li><li>・ 退職時の秘密保持義務契約において、対象とする秘密情報の範囲を具体的に示すことが重要である。</li><li>・ <b>入社時の契約書／誓約書で、「退職時にも契約する／誓約書を出す」という条項を書いておくことが有効である。</b></li></ul> |

(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

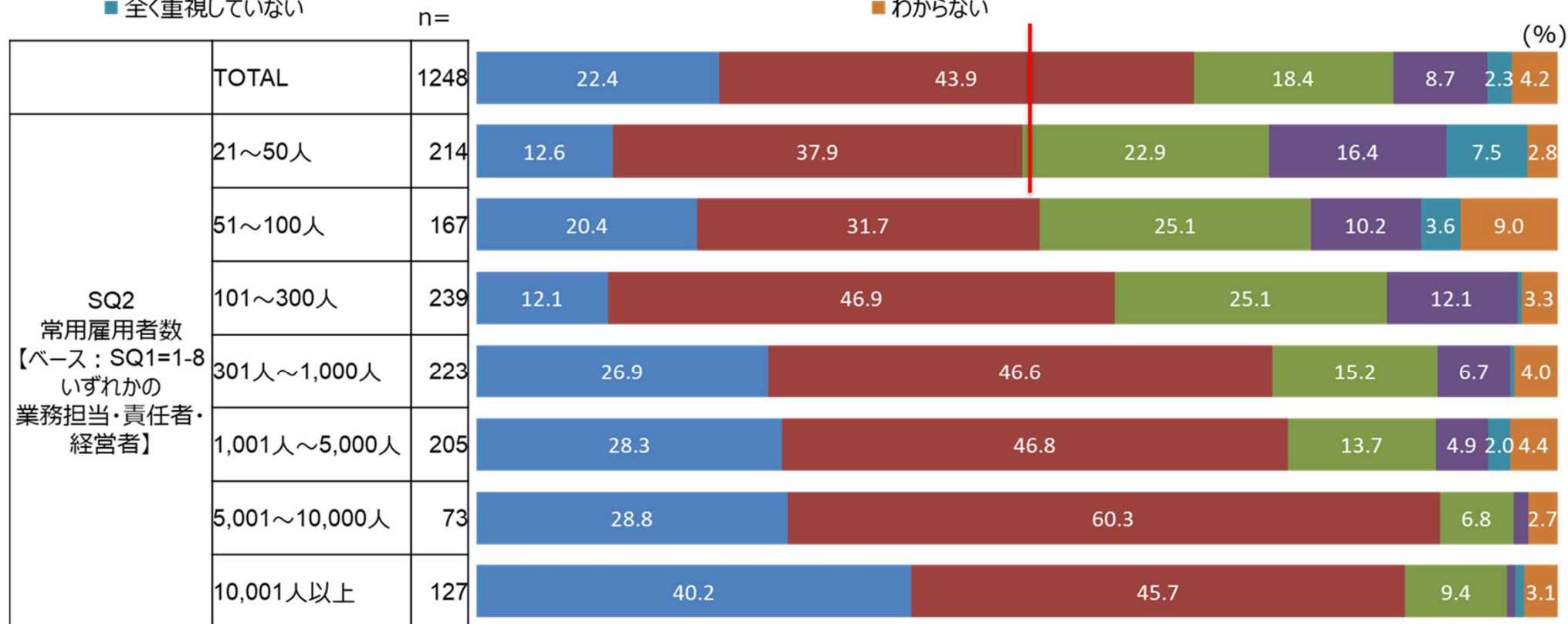
### **【最小限の内部不正対策付加】**

- インタビュー調査において、有識者から「中小企業では他社の事例等に基づいて意識の高い経営層がリスクを判断できれば、秘密情報漏えいや内部不正のリスク評価をある程度代替できる」と言うご指摘があった。
- 中小企業の中には、サイバーセキュリティ対策で手いっぱい、秘密情報漏えい／内部不正防止までは手が回らないと考える企業が多いものと推察される。一方で、取組が進む先進的な中小企業からは、「ISMSや技術情報管理の認証のスコップが両方をカバーしているため、秘密情報漏えい防止に向けた内部不正防止対策とサイバーセキュリティ対策を、同一の取組の一環として実施している」という回答が得られている。
- 上記の調査結果を踏まえると、サイバーセキュリティ対策でカバーできない秘密情報漏えい／内部不正防止特有のリスクと対策を特定する力を有していれば、中小企業の限られた人員・リソースであっても、秘密情報漏えい／内部不正防止に効率的・効果的に対応できるものと期待できる。委託元企業がこうした観点からサプライヤーの経営者と対話することも一案と言える。😊

**Q20.個人情報保護だけでなく、それ以外の秘密情報（営業秘密、重要なデータ等）を保護する対策も重視していますか。  
あてはまるものを1つお選びください。(単一選択)**

- 個人情報保護する対策以上に重視している
- 個人情報保護する対策ほどではないが、ある程度重視している
- 全く重視していない

- 個人情報保護する対策と同じくらい重視している
- あまり重視していない
- わからない



(出典) 2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書 および概要説明資料 <https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html>

本資料の内容についてのお問い合わせは下記までお願いします。

株式会社NTTデータ経営研究所 エグゼクティブスペシャリスト  
営業秘密保護推進研究会 事務局長 三笠 武則

(e-mail) [mikasat@nttdata-strategy.com](mailto:mikasat@nttdata-strategy.com)