従業員・情報システム担当者
経営陣に聞いた
情報漏洩の実態調査

デジタルアーツ株式会社

調査概要

調査対象： 勤務先で日常的に「パソコン」「スマートフォン」「タブレット端末」のいずれかを利用している20歳以上の男女

調査期間： 2014年8月27日（水）～28日（木）

調査方法： インターネット調査

有効回答数： 1,648サンプル

（経営陣:309サンプル／情報システム担当者:309サンプル／従業員:1,030サンプル）

実施機関： 株式会社マクロミル

調査概要： 従業員、情シス担当者、経営陣のそれぞれの層におけるデータの持ち出しや情報漏洩の実態、対策状況、意識についてを把握する。

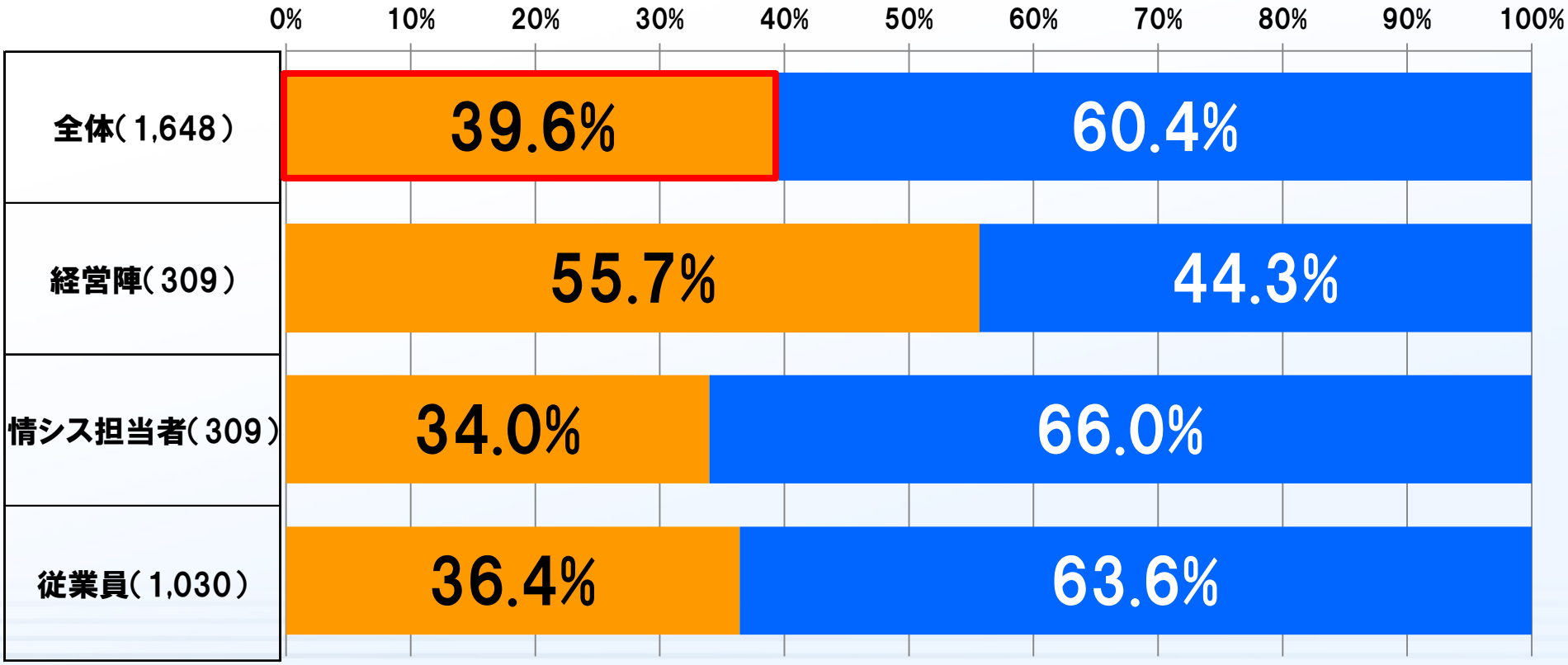
勤務先の資料・データの持ち出し経験

勤務先の資料・データの持ち出し経験

- 全体の39.6%が持ち出しの経験あり。

※回答者　n=1,648
（経営陣：309／情シス担当：309／従業員：1,030）

SA



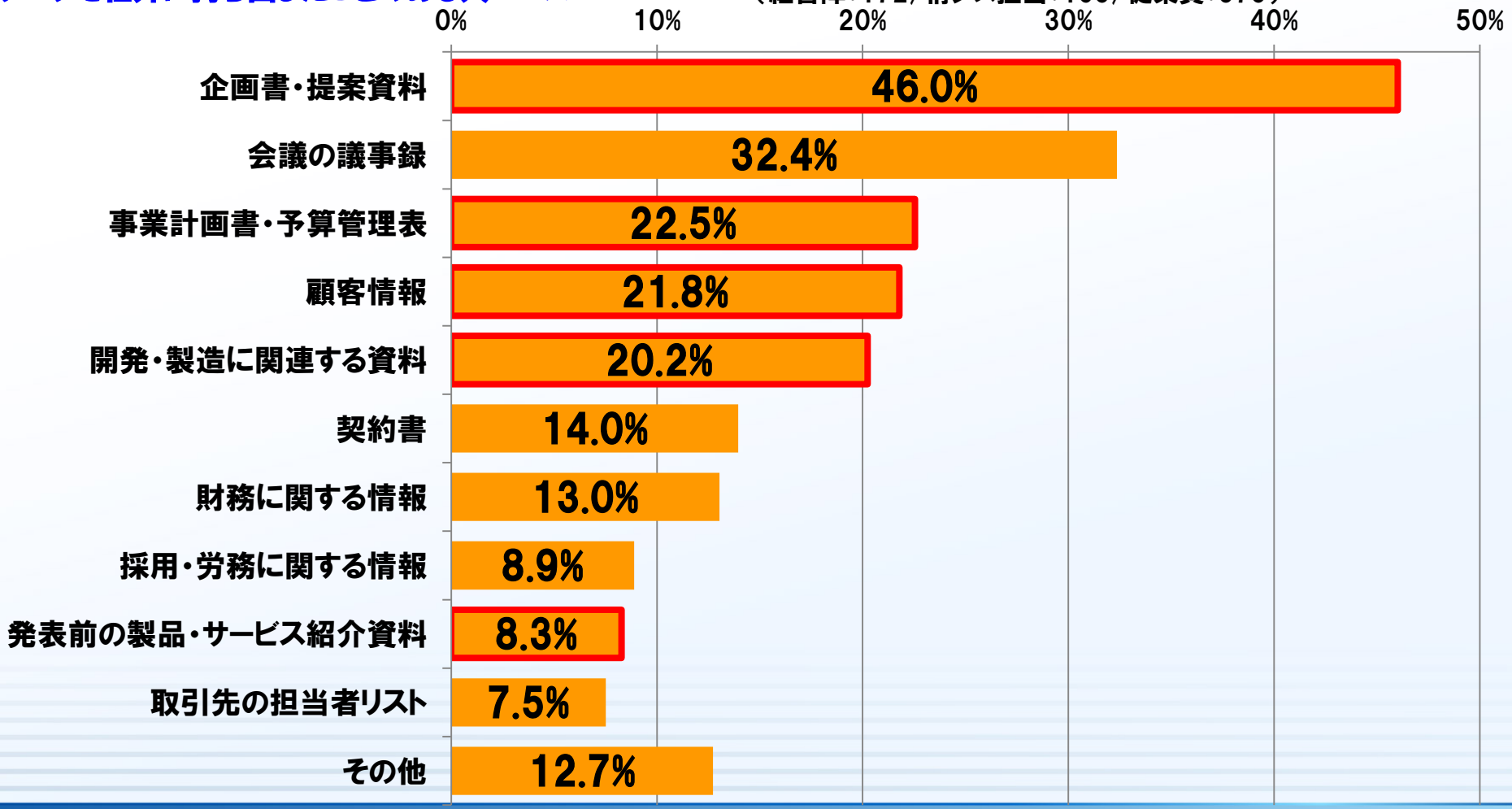
持ち出した勤務先の資料・データの種類

- 「企画書・提案資料」の持ち出しが最も多く46.0%。
- 「事業計画書・予算管理表」22.5%、「顧客情報」21.8%、「開発・製造に関する資料」20.2%の人が持ち出した経験がある。

データを社外に持ち出したことのある人ベース

※回答者　n=652
（経営陣：172/情シス担当：105/従業員：375）

MA

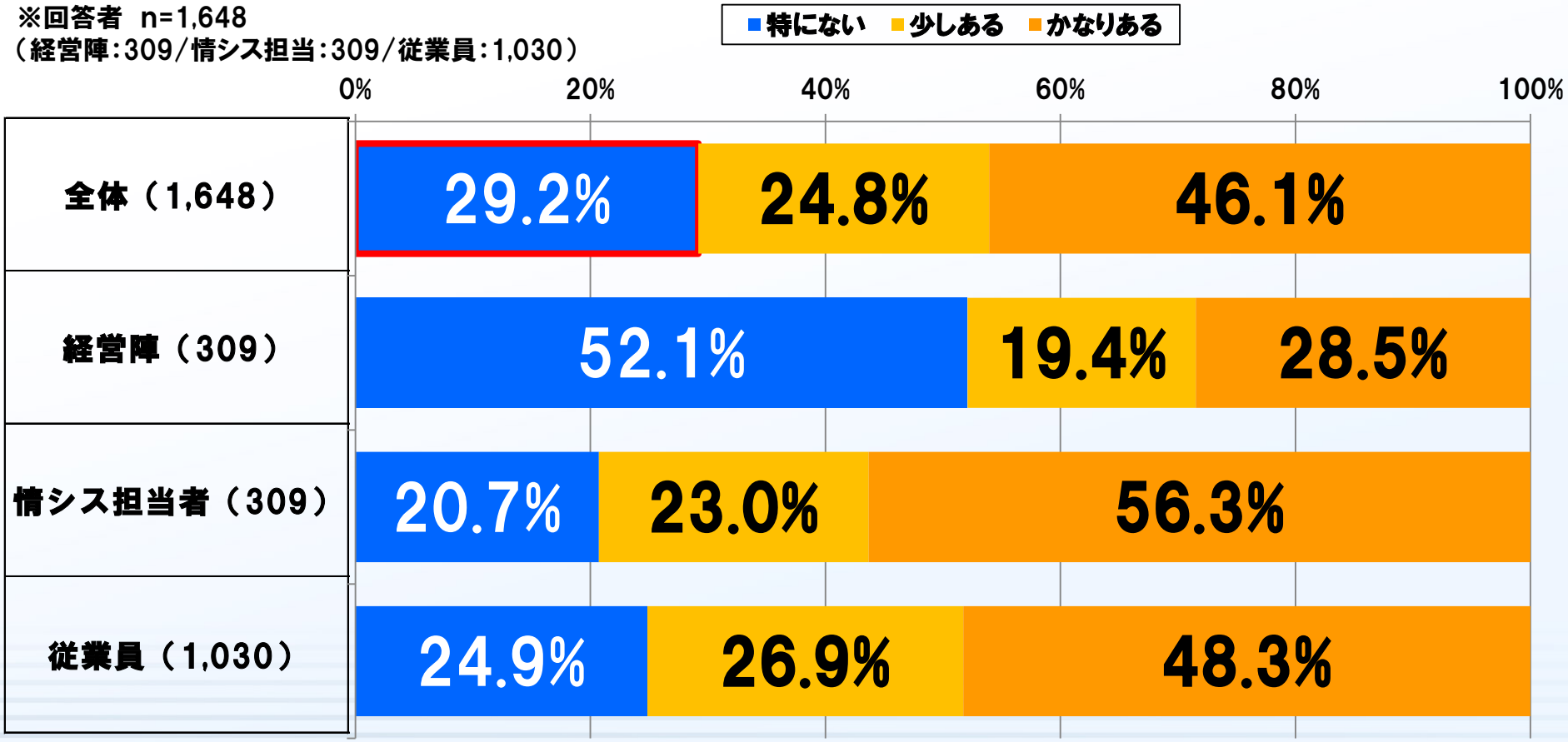


勤務先の資料・データの持ち出しに対する罪悪感

- 全体の29.2%が「特にない」と回答。

SA

※回答者　n=1,648
（経営陣：309/情シス担当：309/従業員：1,030）



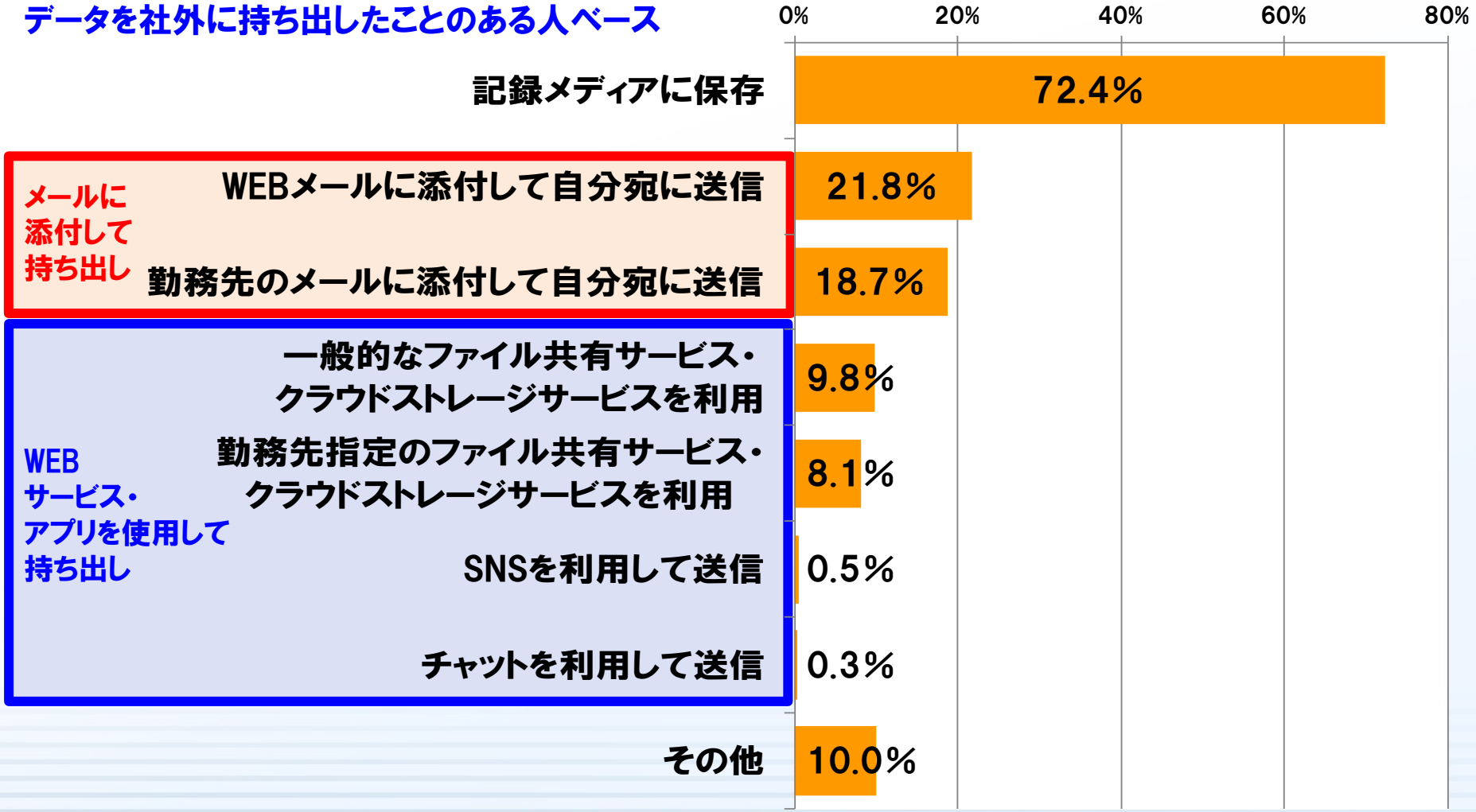
勤務先の資料・データの持ち出し方法

■持ち出し方法は「記録メディアに保存」が最も多く72.4%。

※回答者　n=652
（経営陣：172/情シス担当：105/従業員：375）

MA

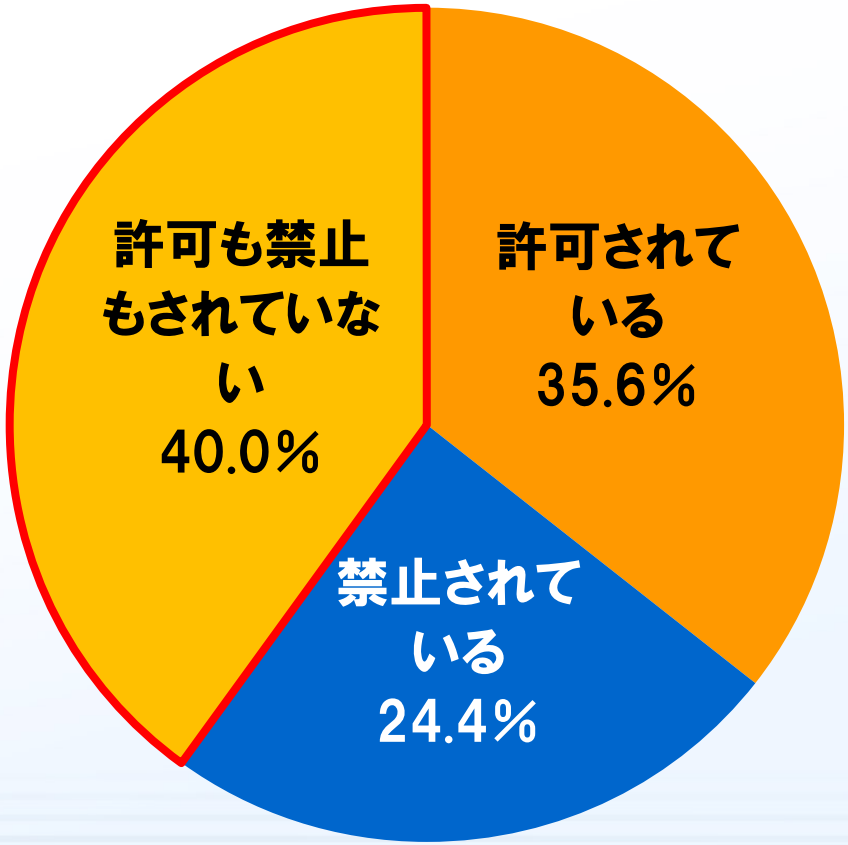
データを社外に持ち出したことのある人ベース



個人端末の仕事での利用許可状況

- 「許可も禁止もされていない」が最も多く、40.0%。
- 「許可されている」従業員は35.6%。「禁止されている」従業員は24.4%。

※回答者　従業員：1,030

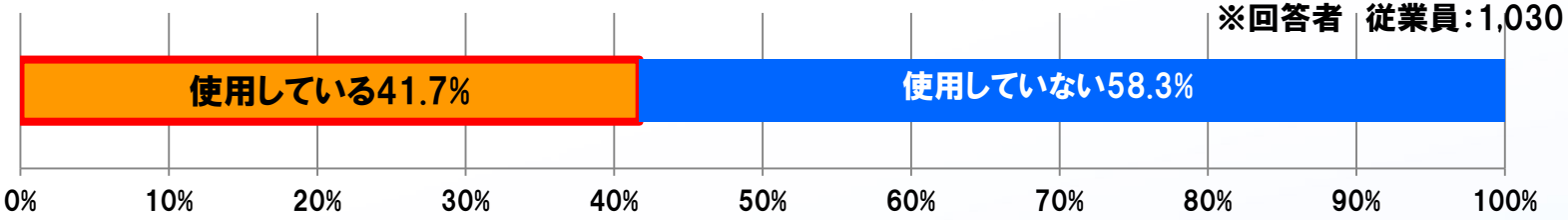


個人端末で業務情報をやり取りするサービス・アプリ

- 個人端末を業務で利用している従業員は41.7％。そのうち58.6%がWEBサービスやアプリを使い、業務情報のやり取りをしている。

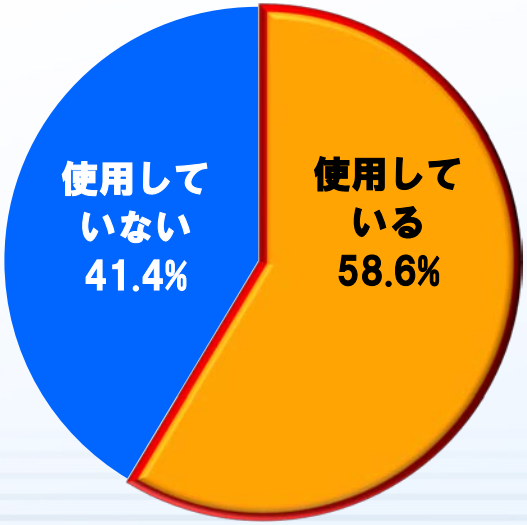
個人端末の業務での利用状況

※回答者　従業員：1,030



WEBサービス・アプリの使用状況

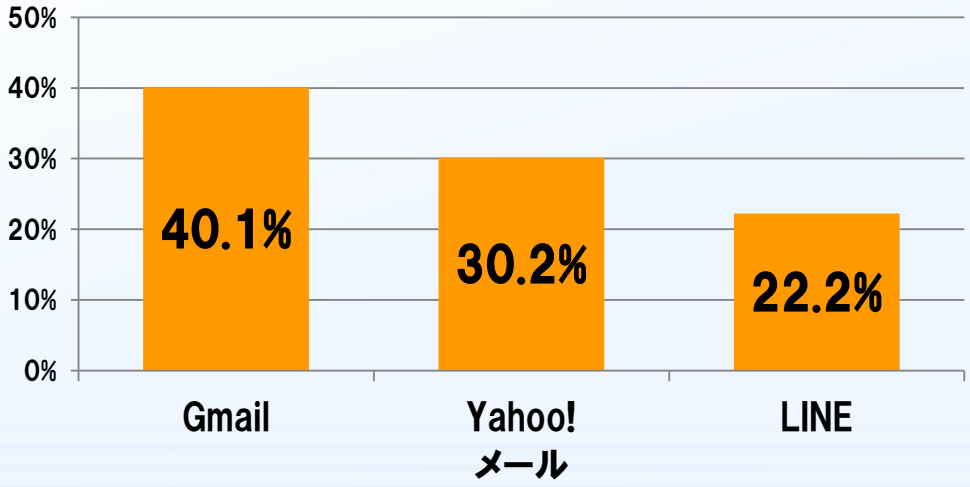
※回答者　従業員：430



仕事での個人端末使用者ベース

業務情報のやり取りに使用するWEBサービス・アプリ

※回答者　従業員：252

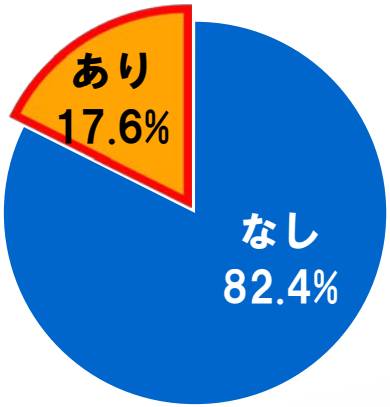


個人端末を業務で使用し、
尚且つWEBサービス・アプリを使用する人ベース

情報漏洩被害にあった経験

実際に情報漏洩被害にあった経験

※回答者　n=618
（経営陣:309/情シス担当:309）

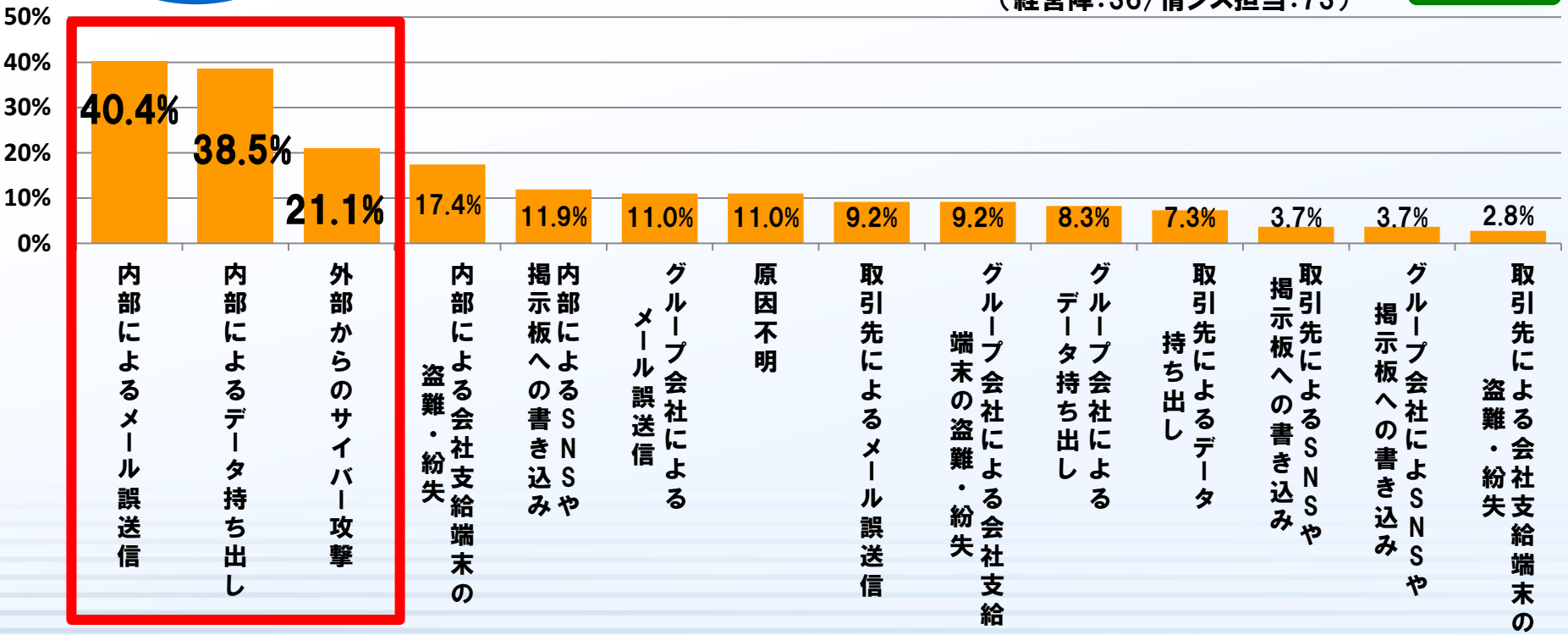


- 情報漏洩被害は17.6%経験あり。
- その内訳は、「内部によるメール誤送信」が40.4%、「内部によるデータ持ち出し」が38.5%、と内部からの情報漏洩が上位2つを占めている。
- 「外部からのサイバー攻撃」は21.1%。

情報漏洩被害にあったことのある人ベース

※回答者　n=109
（経営陣:36/情シス担当:73）

MA



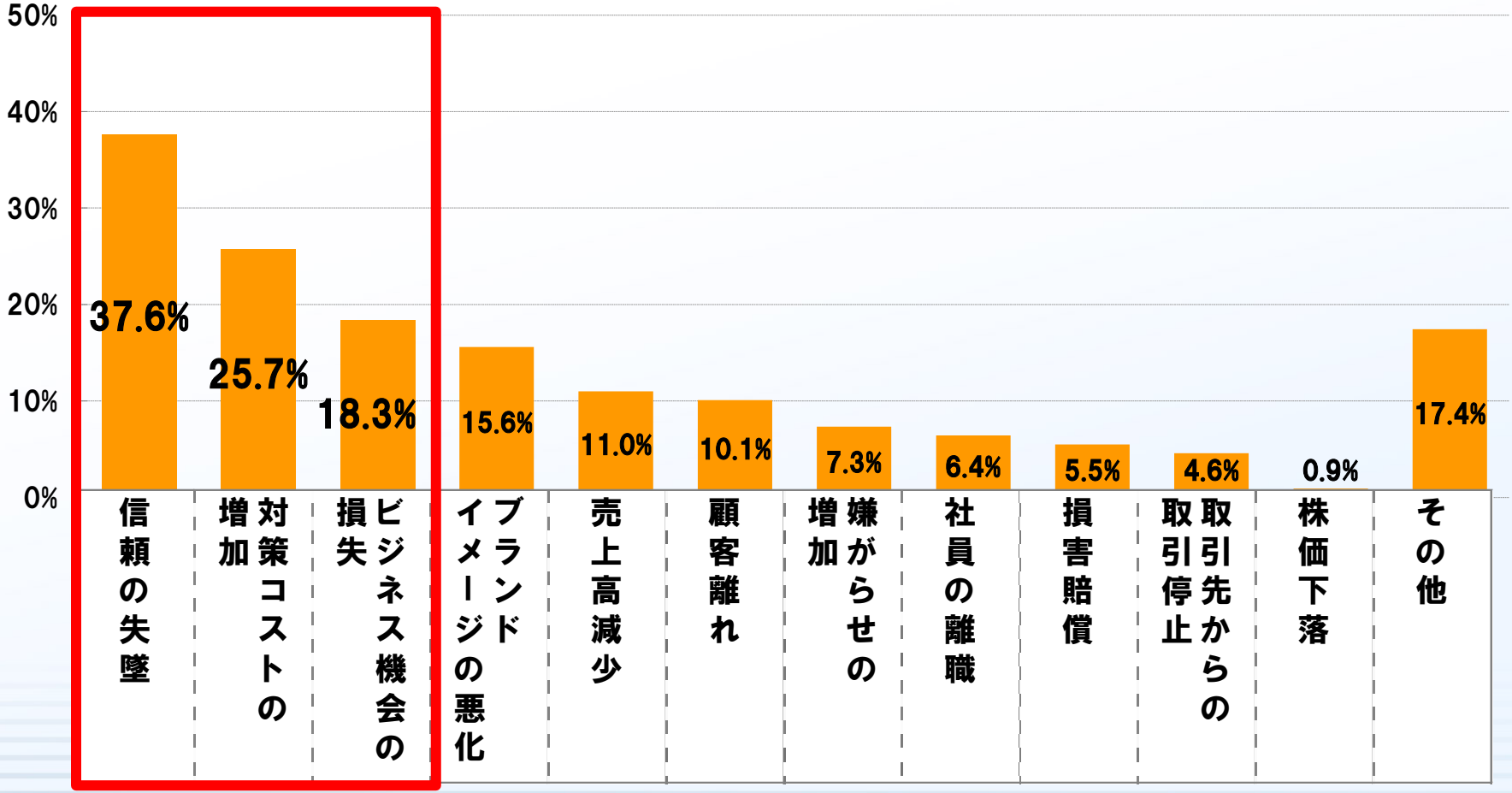
情報漏洩被害が経営に与えた悪影響

- 「信頼の失墜」が最も多く37.6%。次いで「対策コストの増加」が25.7%、「ビジネス機会の損失」が18.3%。

MA

情報漏洩被害にあったことのある人ベース

※回答者　n=109
（経営陣：36/情シス担当：73）



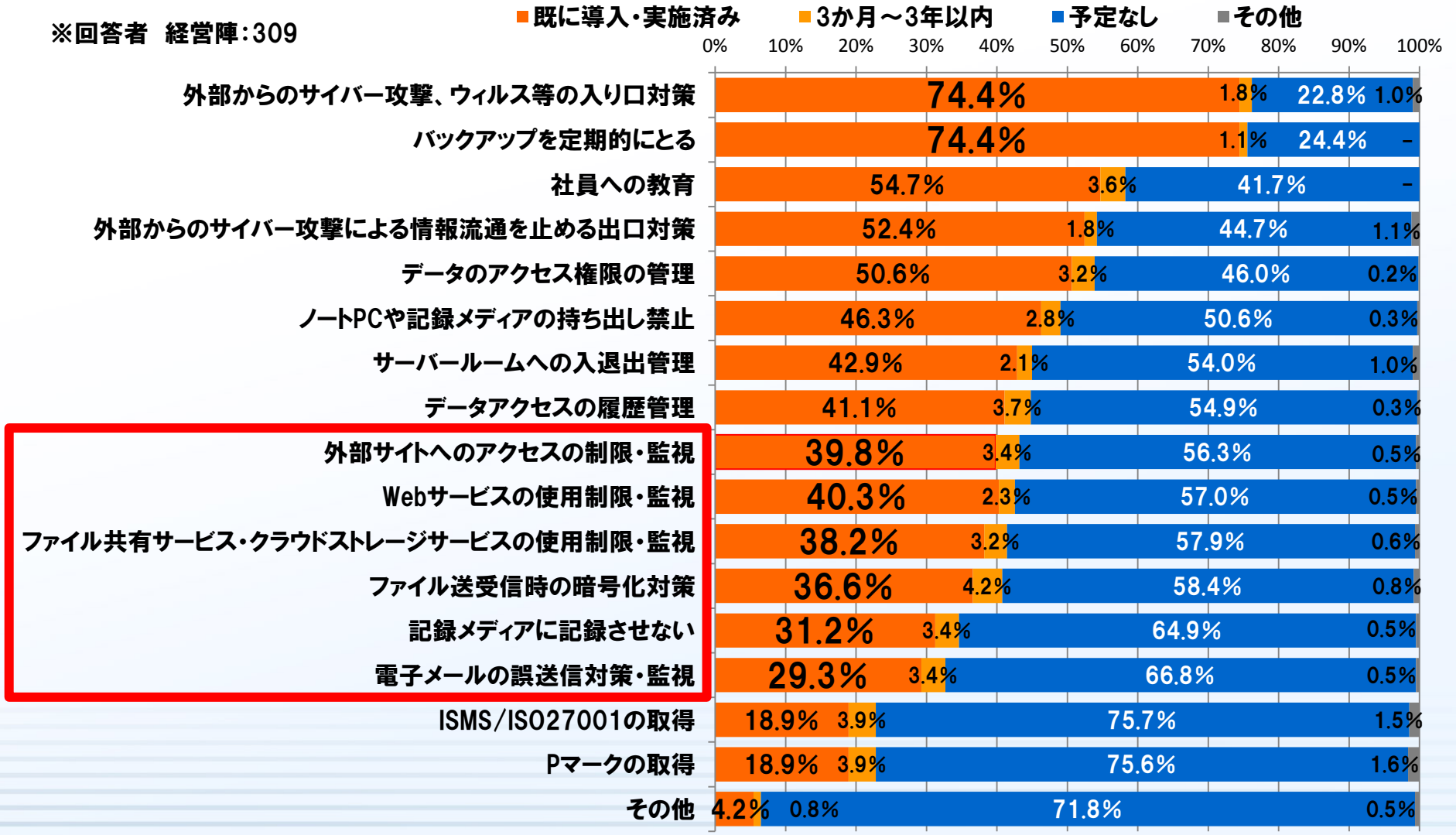
実際に行っている対策と
情報漏洩リスクに対する意識

どのような情報漏洩対策を導入しているか

- 「外部からのサイバー攻撃」、「バックアップを定期的にとる」が最も多く74.4%。
- 内部漏洩に有効な対策を導入している企業は全体的に低い結果となった。

MA

※回答者　経営陣：309

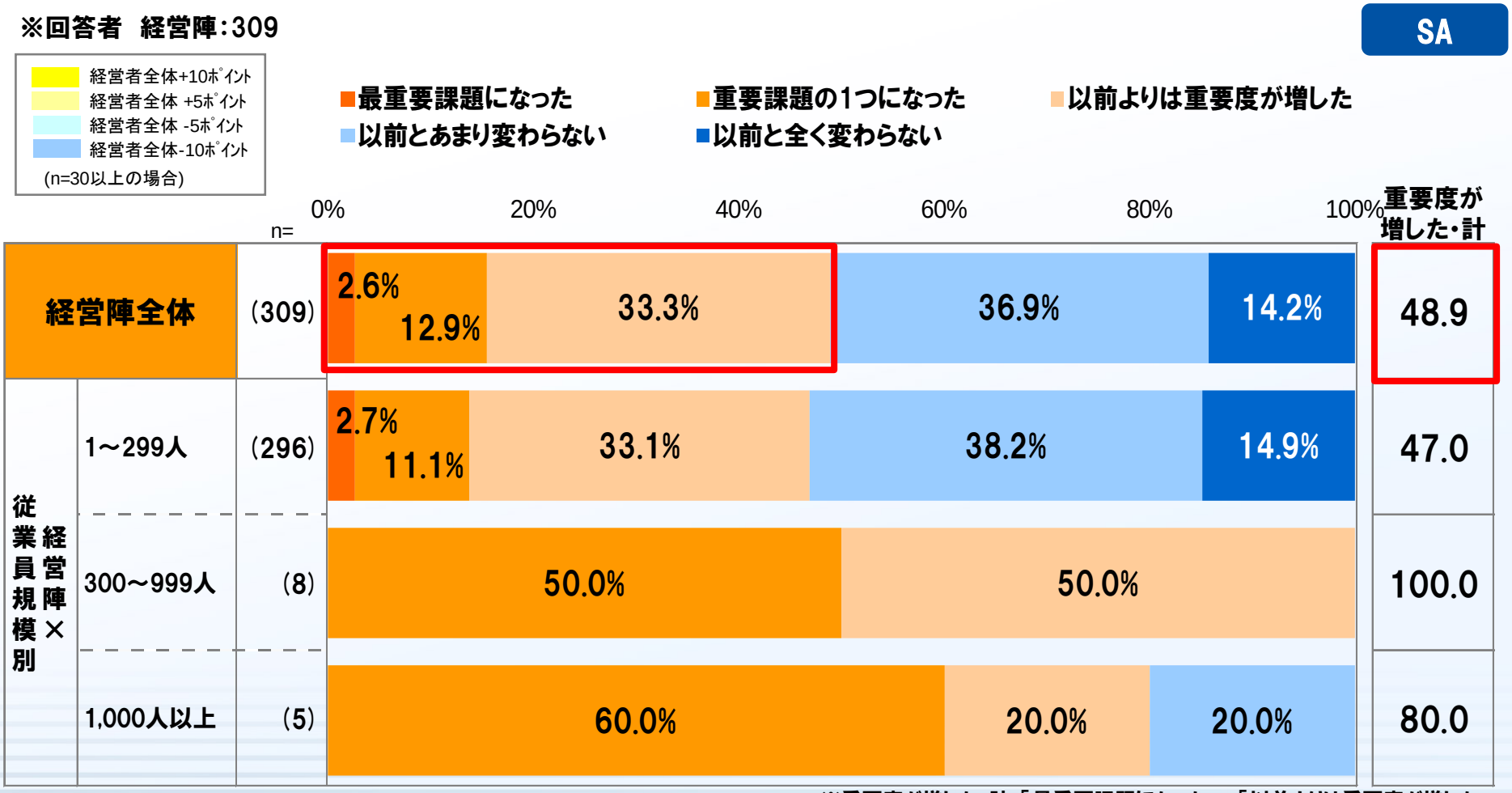


情報漏洩対策の重要度の変化（大手企業事件前と比較）

- 全体の48.9%が「重要度が増した」と回答。
- 参考数値として、従業員数300人以上の会社の経営陣は、80%以上が「重要度が増した」と回答。

※回答者　経営陣：309

SA



※重要度が増した・計：「最重要課題になった」～「以前よりは重要度が増した」

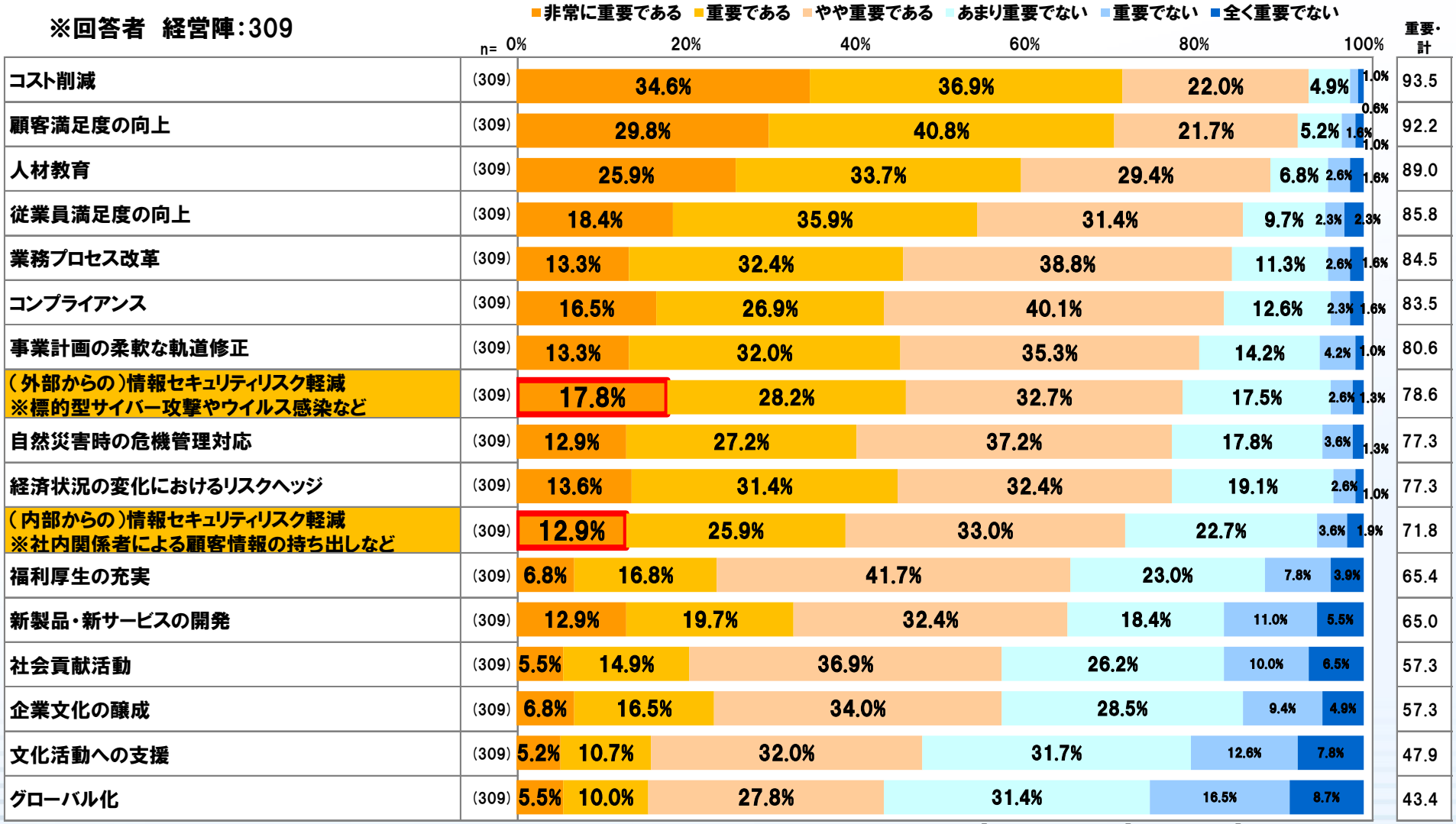
経営課題における情報セキュリティの重要度

DigitalArts

SA

情報セキュリティリスクの軽減は「外部からの攻撃」が17.8%、「内部からの漏洩」が12.9%。と低くなっている。

※回答者　経営陣：309



※重要・計：「非常に重要である」～「重要である」 ※「重要・計」のスコアで降順にソート

IT投資全体の中で情報漏洩対策への投資率

- 従業員規模299人以下の企業の経営陣で情報漏洩対策に「投資している」のは42.6%しかいない。57.4%が「投資していない」と回答。
- それに対して、従業員規模300人以上の企業の経営陣100%が「投資している」と回答した。（参考数値）

※回答者　経営陣：309

SA

情報漏洩対策に投資している経営陣の割合

100%	42.6%
従業員規模　300人以上の企業の経営陣	従業員規模　299人以下の企業の経営陣

今回の調査結果のポイント

- 勤務先の資料・データの持ち出し経験が39.6%。
  勤務先の資料・データを持ち出すことへの罪悪感は「特にない」が29.2%。
  ⇒　全体的に情報漏洩に対する意識の低さが伺える。

- 企業における情報漏洩被害で経験ありと回答したのが17.6%。
  被害内容の内訳は、「内部によるメール誤送信」が40.4%。
  「内部によるデータ持ち出し」が38.5%。
  ⇒　外部対策より、内部からの情報漏洩対策が重要。

- 情報漏洩対策について、「重要度が増した」と回答した経営陣は48.9%。
  しかし、他の経営課題と比較すると、「外部からの攻撃対策」は17.8%。
  「内部からの漏洩」は12.9%と低い傾向。
  また、IT投資の中で情報漏洩対策に「投資していない」と回答したのが57.4%。
  ⇒　日本企業の経営課題において、情報漏洩対策がまだ重要視されていない。