

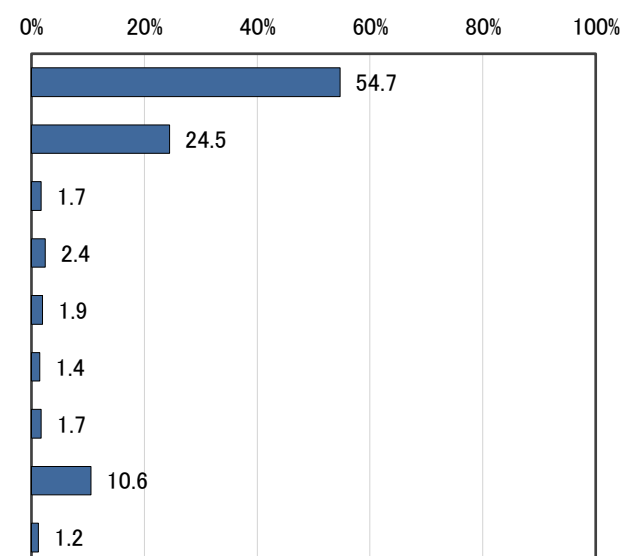
ITシステム・サービスの業務委託に関する調査 委託元調査 単純集計結果

回答組織数 = 417

回答事例数 = 365

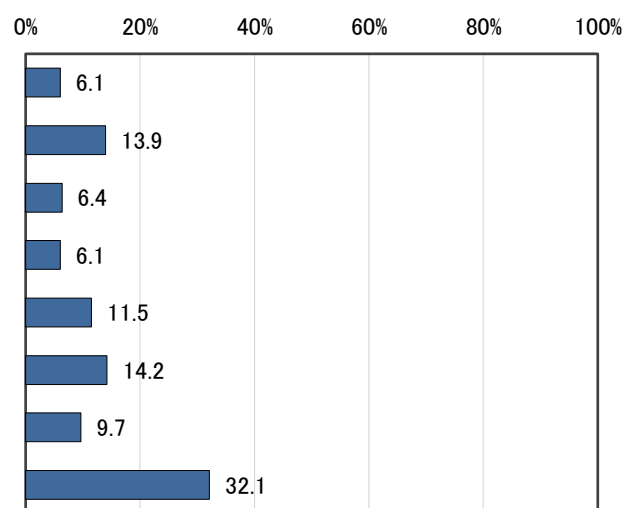
S1 貴社の主な業種をお選びください。（ひとつだけ）

選択肢	%	N
1 製造業	54.7	228
2 卸売業、小売業	24.5	102
3 不動産業、物品賃貸業	1.7	7
4 学術研究、専門・技術サービス業	2.4	10
5 宿泊業、飲食サービス業	1.9	8
6 生活関連サービス業、娯楽業	1.4	6
7 複合サービス事業	1.7	7
8 サービス業（3～7に分類されないもの）	10.6	44
9 その他	1.2	5
計	100	417



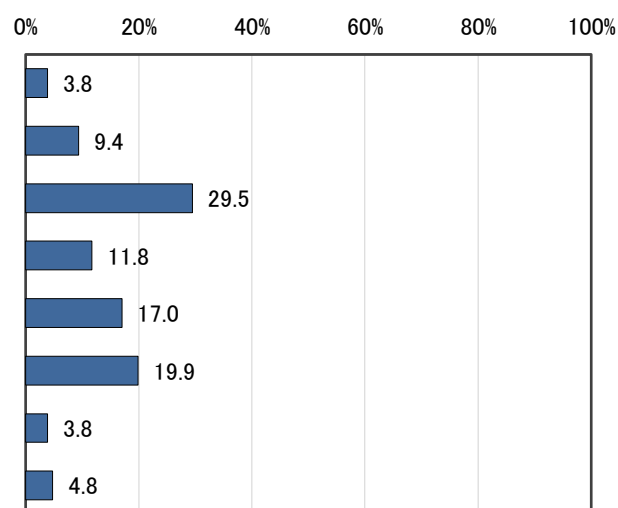
S1 -1（S1で「製造業」または「卸売業、小売業」と回答した場合）貴社の事業のうち、最も売上高の高い分野をお選びください。（ひとつだけ）

選択肢	%	N
1 繊維・衣服	6.1	20
2 飲食料品	13.9	46
3 建築材料、鉱物・金属材料	6.4	21
4 印刷・印刷関連製品	6.1	20
5 化学製品	11.5	38
6 電気機械器具、情報通信機械器具	14.2	47
7 輸送用機械器具	9.7	32
8 その他の製品	32.1	106
計	100	330



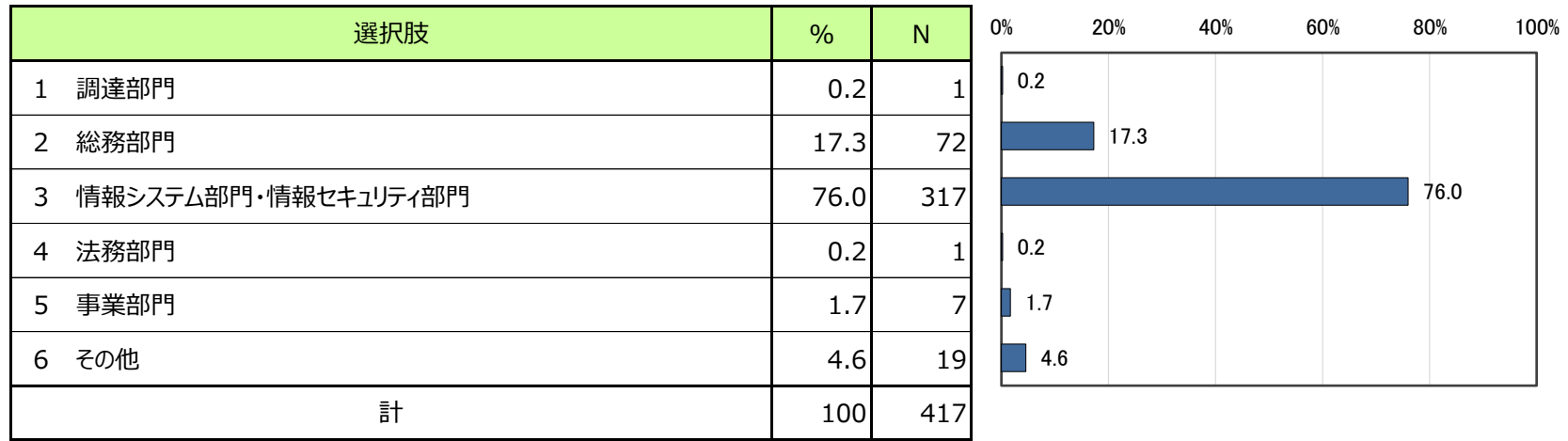
S2 貴社の総従業員数（正社員、準社員等を含む）をお選びください。（ひとつだけ）

選択肢	%	N
1 ～50名	3.8	16
2 51名～100名	9.4	39
3 101名～300名	29.5	123
4 301名～500名	11.8	49
5 501名～1,000名	17.0	71
6 1,001名～5,000名	19.9	83
7 5,001名～10,000名	3.8	16
8 10,001名以上	4.8	20
計	100	417

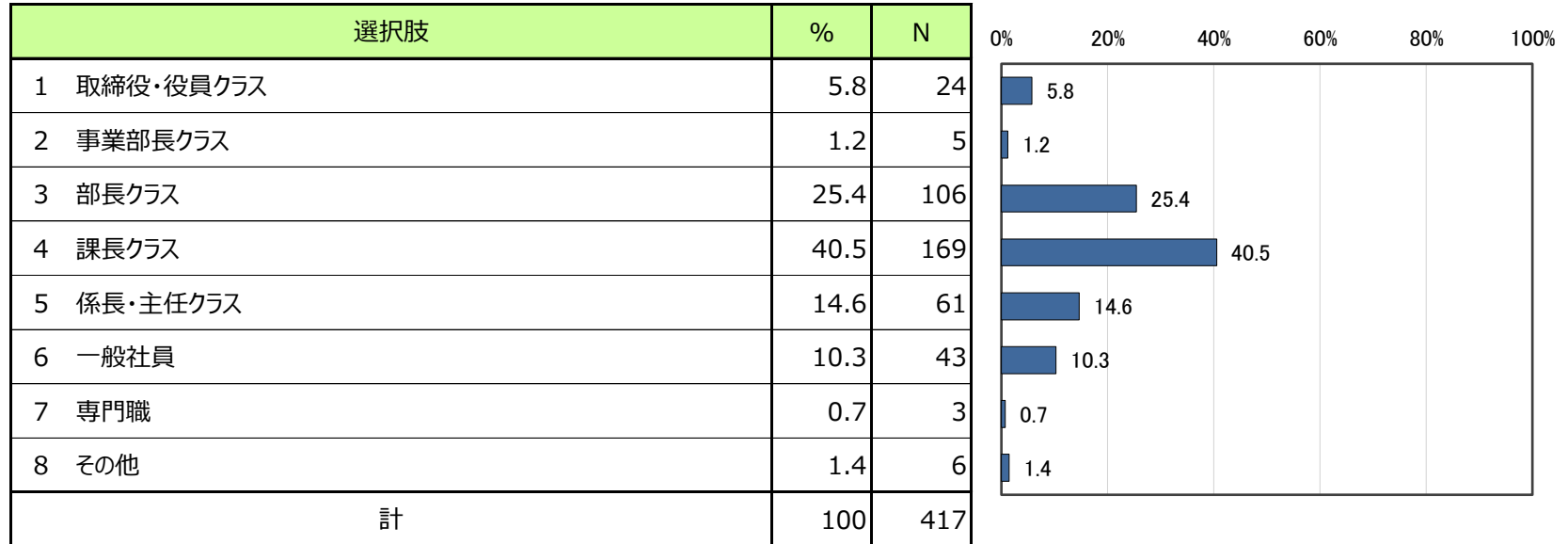


付録3-1 アンケート調査 単純集計結果（委託元調査）

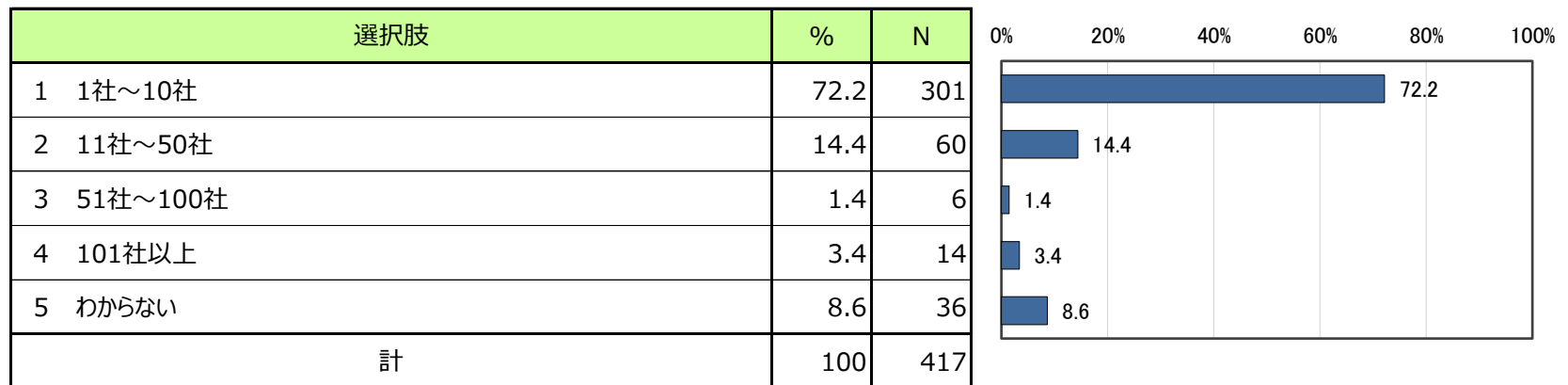
S3 ご回答者の所属部門をお選びください。複数の部門で回答された場合は、主に回答された部門をお選びください。（ひとつだけ）



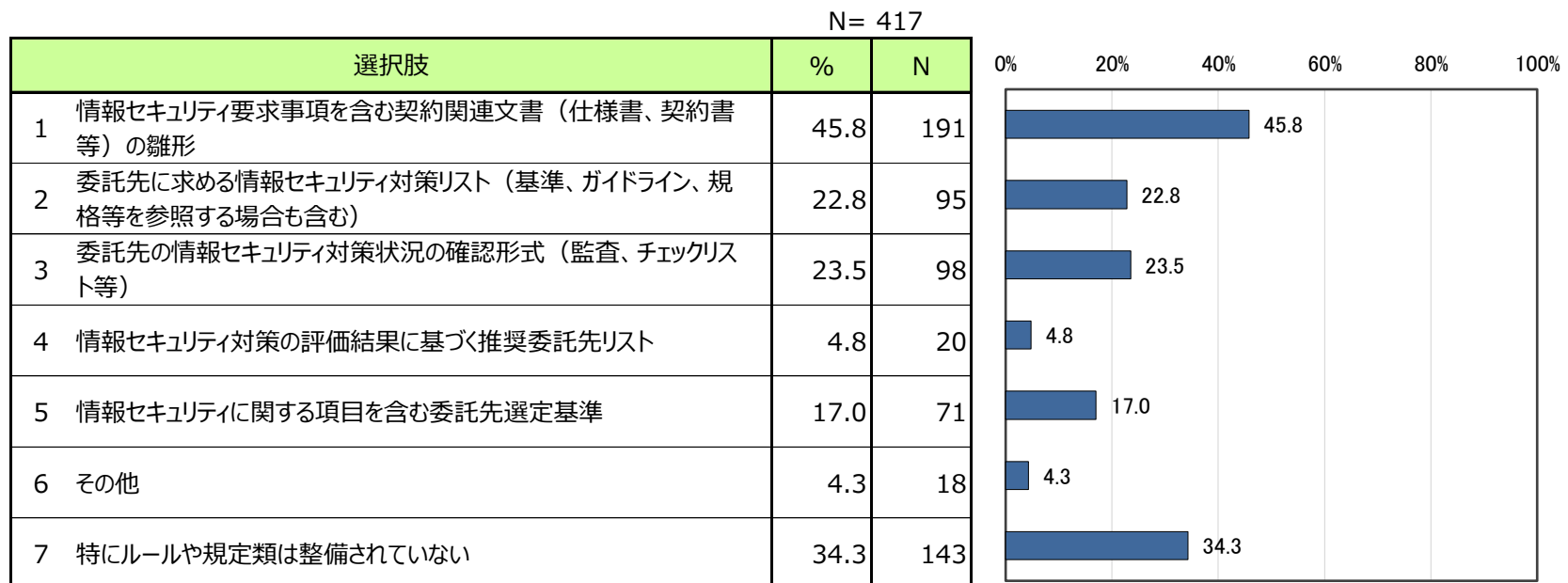
S4 ご回答者の役職をお選びください。（ひとつだけ）



問1 貴社において、昨年度（2017年度）、直接取引のあった委託先の社数をお選びください。（ひとつだけ）

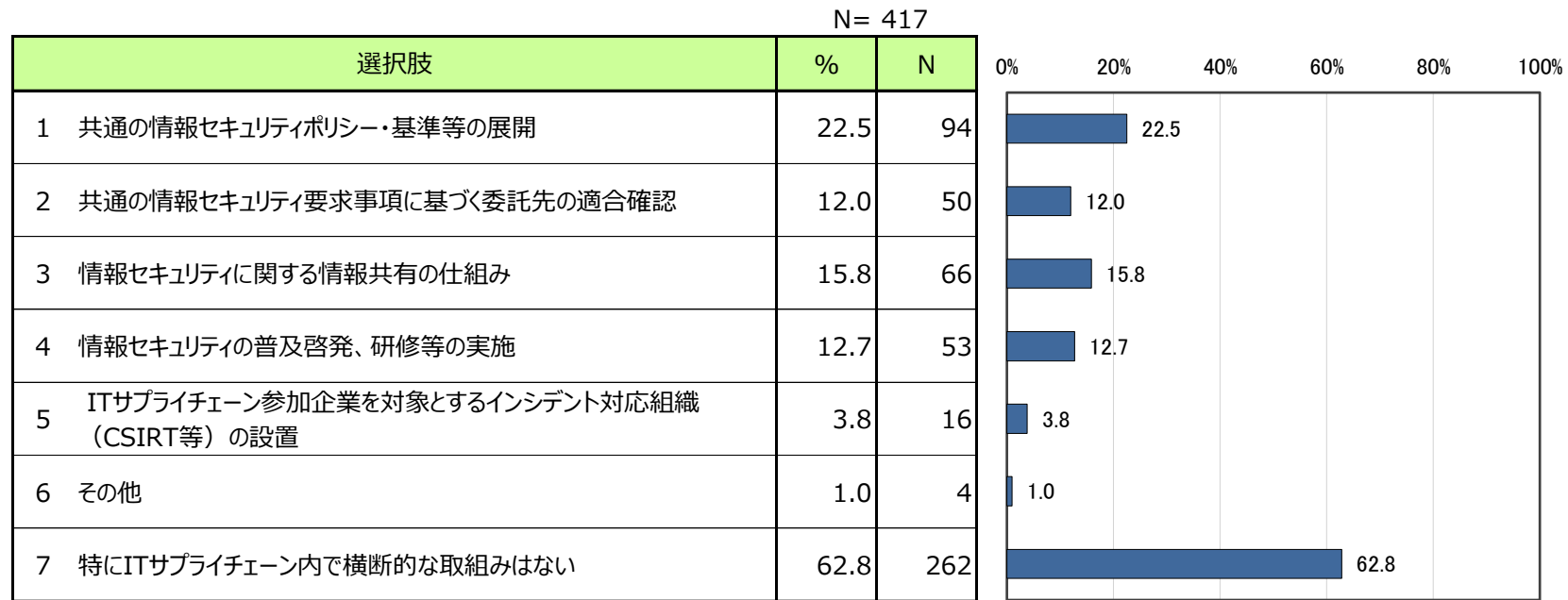


問2 情報セキュリティに関する委託先管理に関し、貴社では、どのような社内ルール・規定類を整備されていますか。当てはまるものを全てお選びください。（いくつでも）

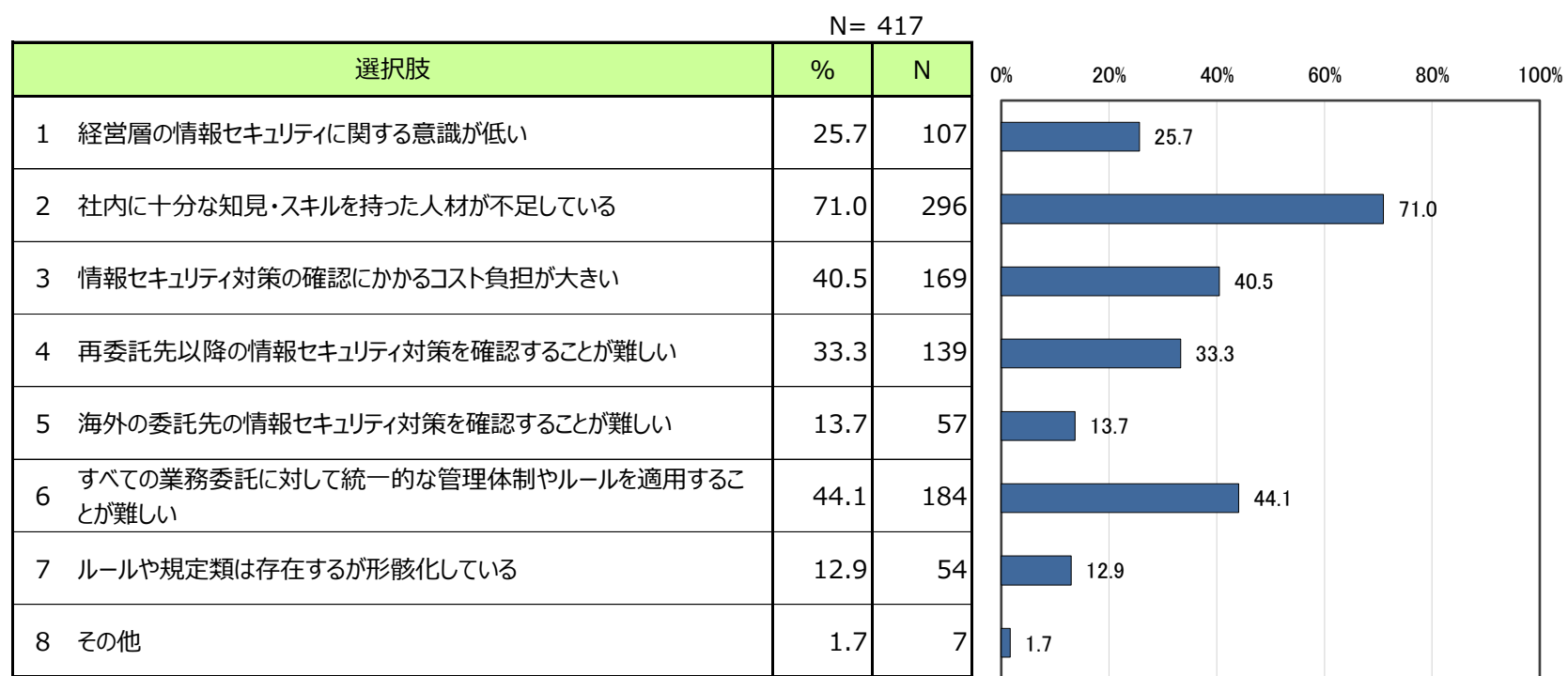


付録3-1 アンケート調査 単純集計結果（委託元調査）

問3 貴社が参加するITサプライチェーン内で横断的な情報セキュリティ対策はありますか。当てはまるものを全てお選びください。（いくつでも）



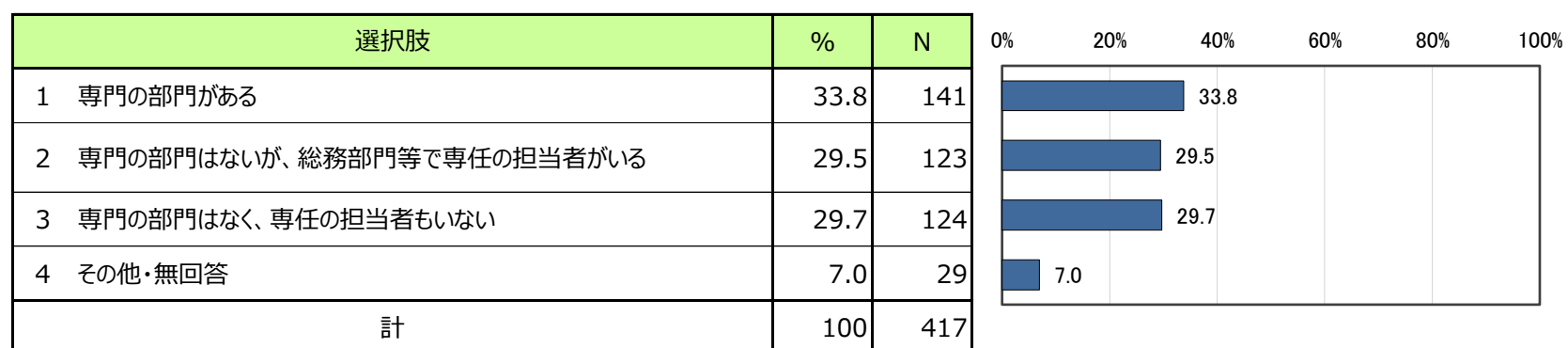
問4 情報セキュリティに関する委託先管理において、どのような点が課題だと考えますか。特に課題と考えるものを最大3 つまでお選びください。



問5 問2 で「1 情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形」を選んだ方にお伺いします。契約関連文書に記載する情報セキュリティ要求事項の変更は認められていますか。（ひとつだけ）



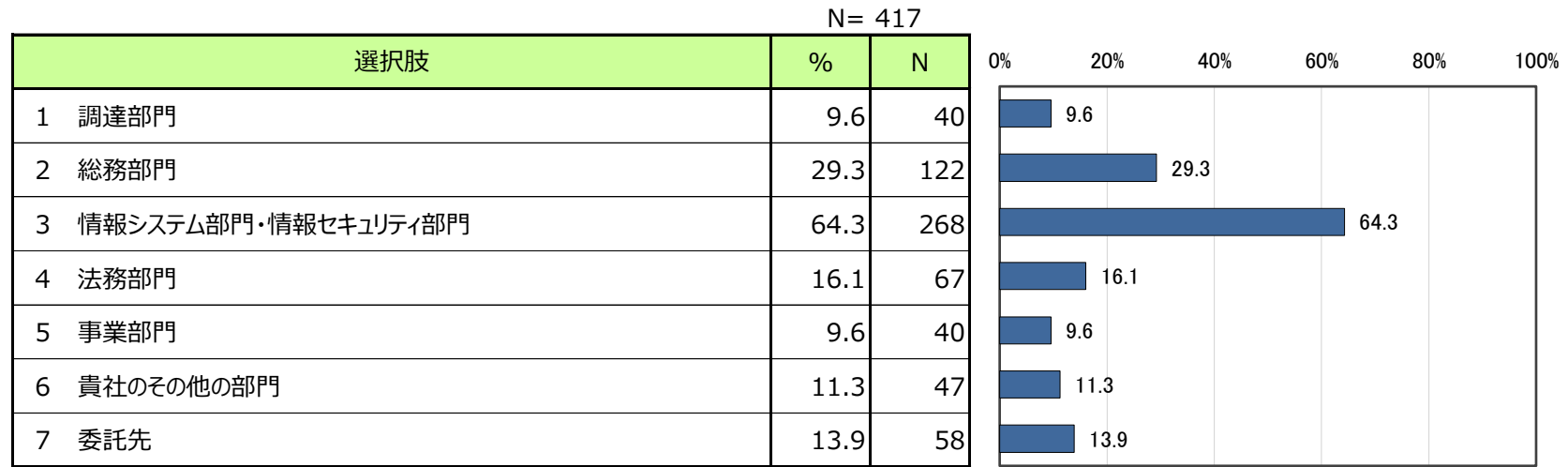
問6 貴社では、業務委託ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けていますか。（ひとつだけ）



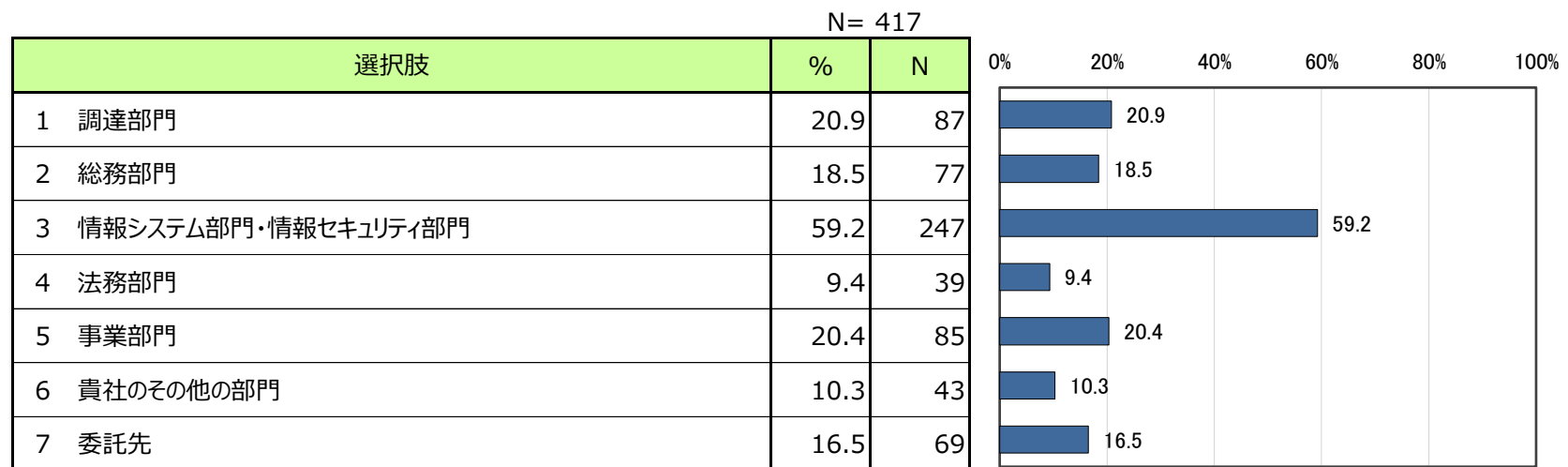
付録3-1 アンケート調査 単純集計結果（委託元調査）

問7 業務委託における情報セキュリティ要求事項の明確化について、役割ごとに所管（関与）する部門をお選びください。1つの役割に対して複数の部門が関与する場合は、関与する部門全てをお選びください。（それぞれいくつでも）

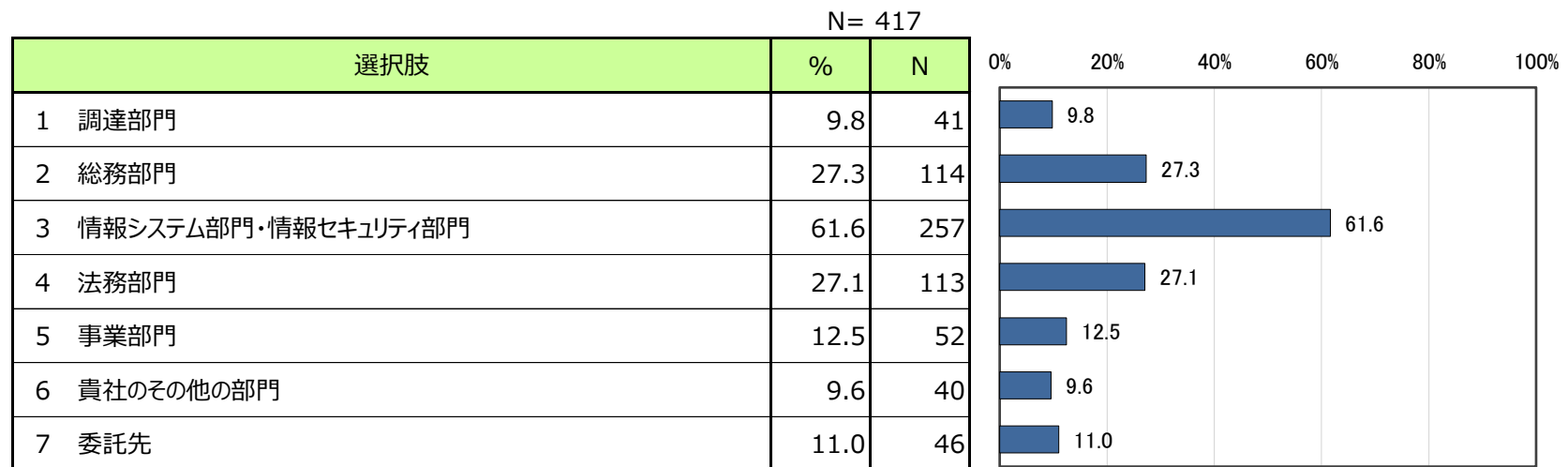
a. 記載項目や手順等ルールを決める



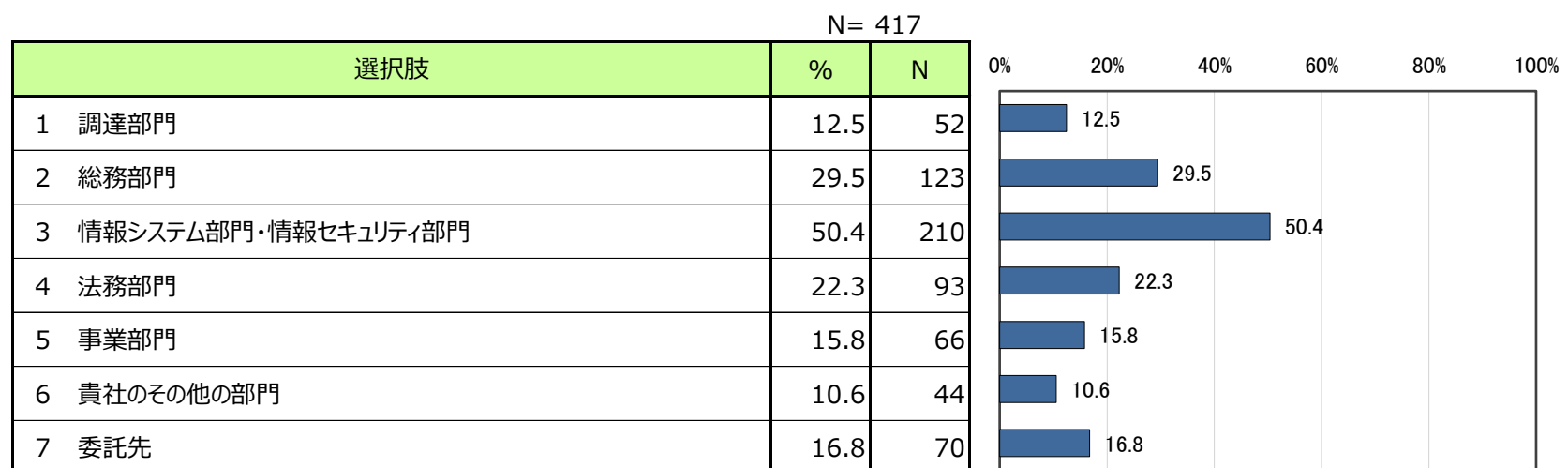
b. 委託先と内容を調整する



c. 要求事項の内容が妥当か確認する

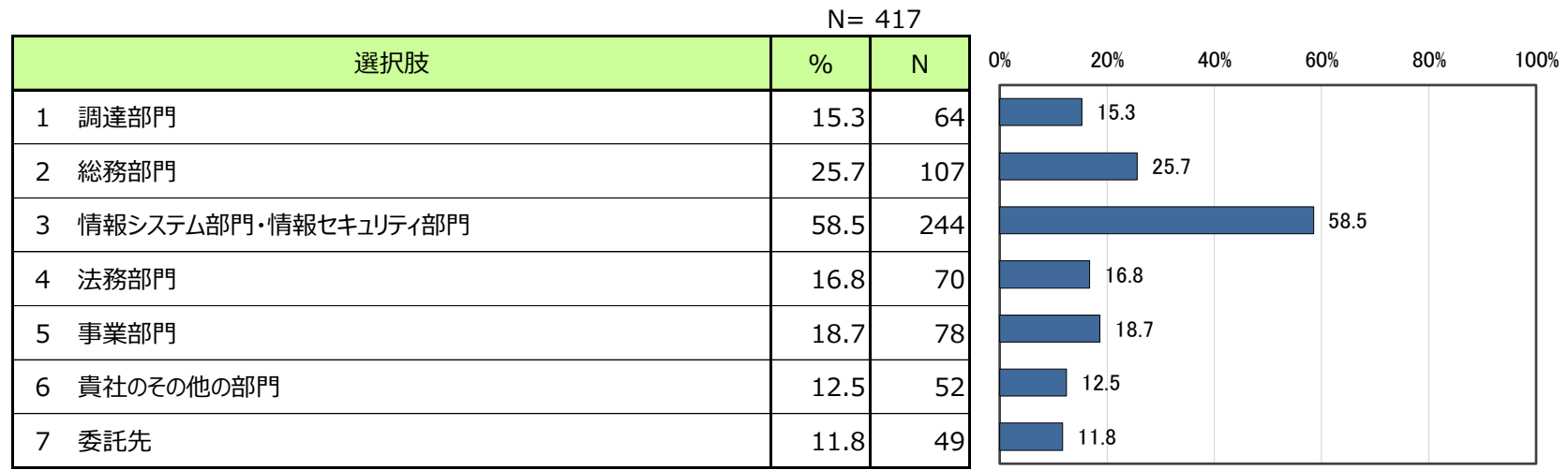


d. 要求事項を契約関連文書（仕様書、契約書等）に記載する



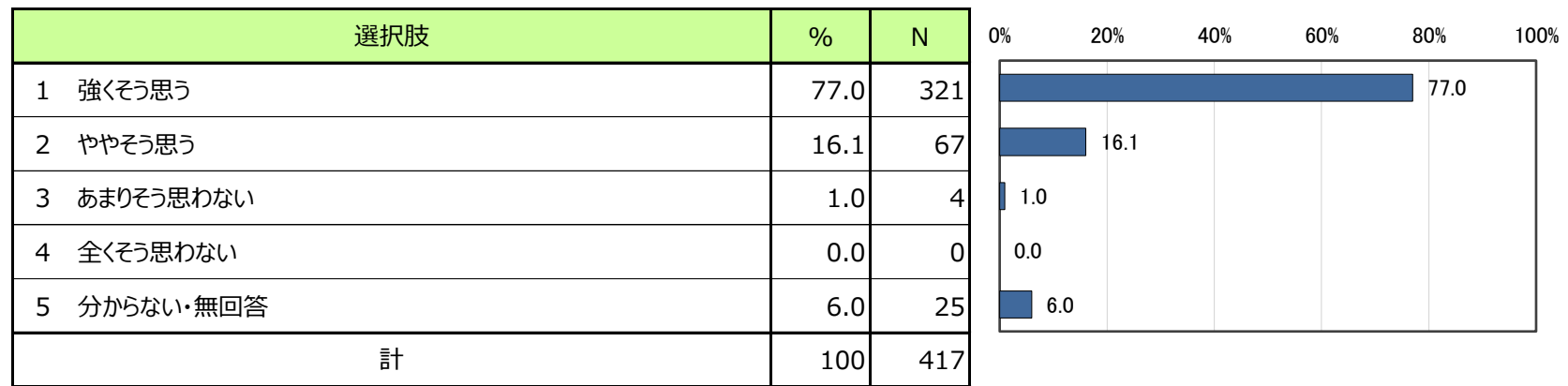
付録3-1 アンケート調査 単純集計結果（委託元調査）

e. 要求通りになっていることを確認する

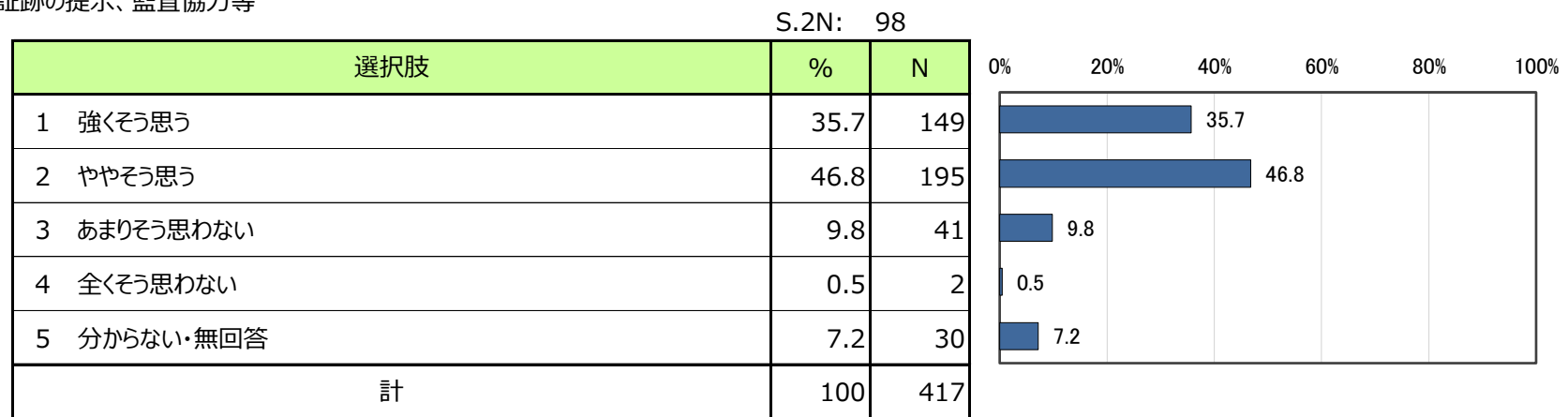


問8 以下の情報セキュリティ要求事項に関し、業務委託契約において、委託先の責任を明確にしたいと思う度合について、当てはまるものをお選びください。（それぞれひとつずつ）

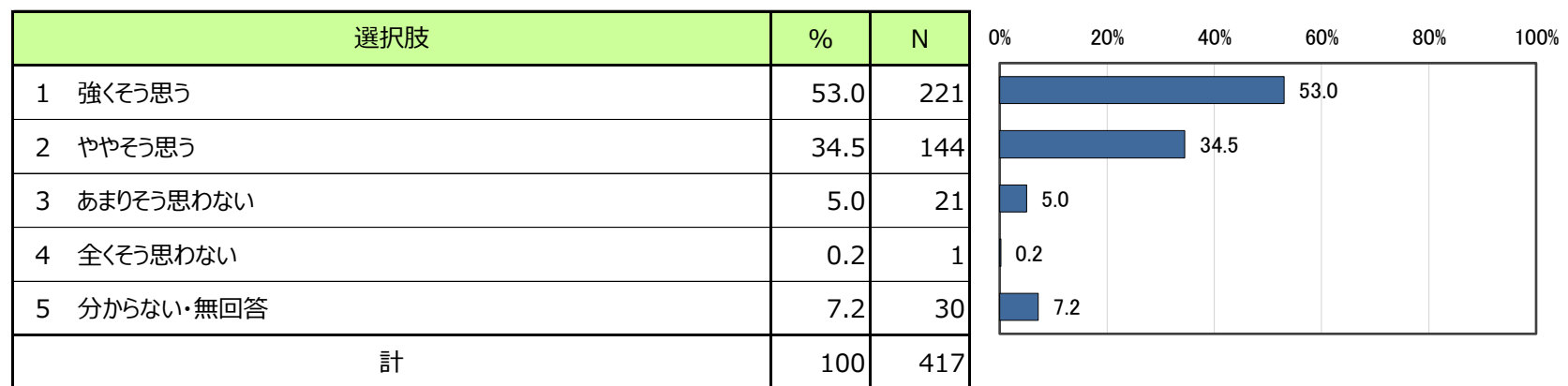
a. 秘密保持



b. 証跡の提示、監査協力等



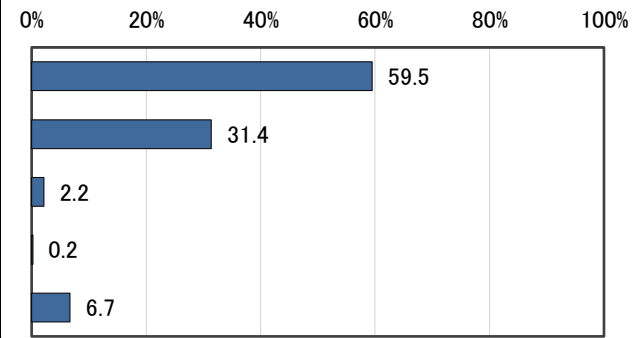
c. 情報セキュリティに関する契約内容に違反した場合の措置



付録3-1 アンケート調査 単純集計結果（委託元調査）

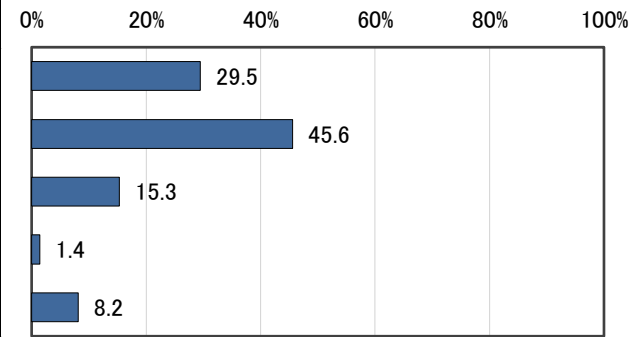
d. インシデントが発生した場合の対応

選択肢	%	N
1 強く思う	59.5	248
2 やや思う	31.4	131
3 あまり思わない	2.2	9
4 全く思わない	0.2	1
5 分からない・無回答	6.7	28
計	100	417



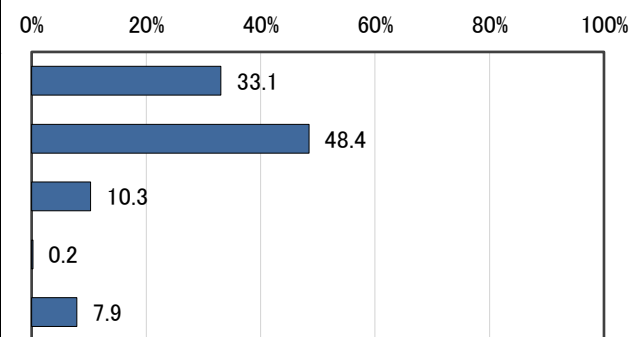
e. 可用性（稼働率の水準、目標復旧時間等）

選択肢	%	N
1 強く思う	29.5	123
2 やや思う	45.6	190
3 あまり思わない	15.3	64
4 全く思わない	1.4	6
5 分からない・無回答	8.2	34
計	100	417



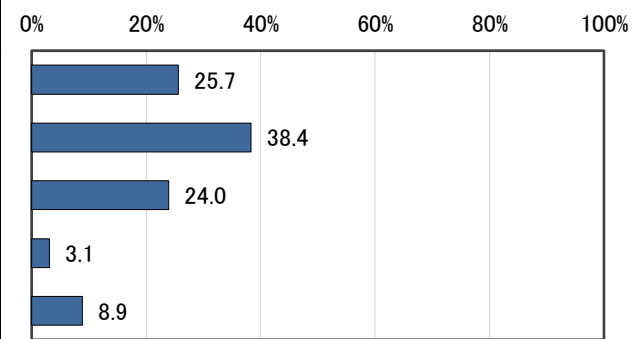
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応

選択肢	%	N
1 強く思う	33.1	138
2 やや思う	48.4	202
3 あまり思わない	10.3	43
4 全く思わない	0.2	1
5 分からない・無回答	7.9	33
計	100	417



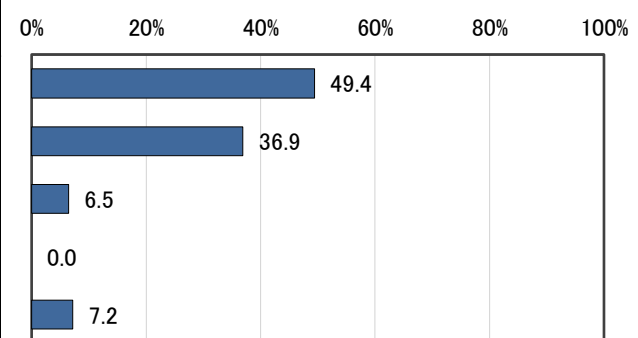
g 再委託の禁止または制限

選択肢	%	N
1 強く思う	25.7	107
2 やや思う	38.4	160
3 あまり思わない	24.0	100
4 全く思わない	3.1	13
5 分からない・無回答	8.9	37
計	100	417



h 契約終了後の情報資産の扱い（返却、消去、廃棄等）

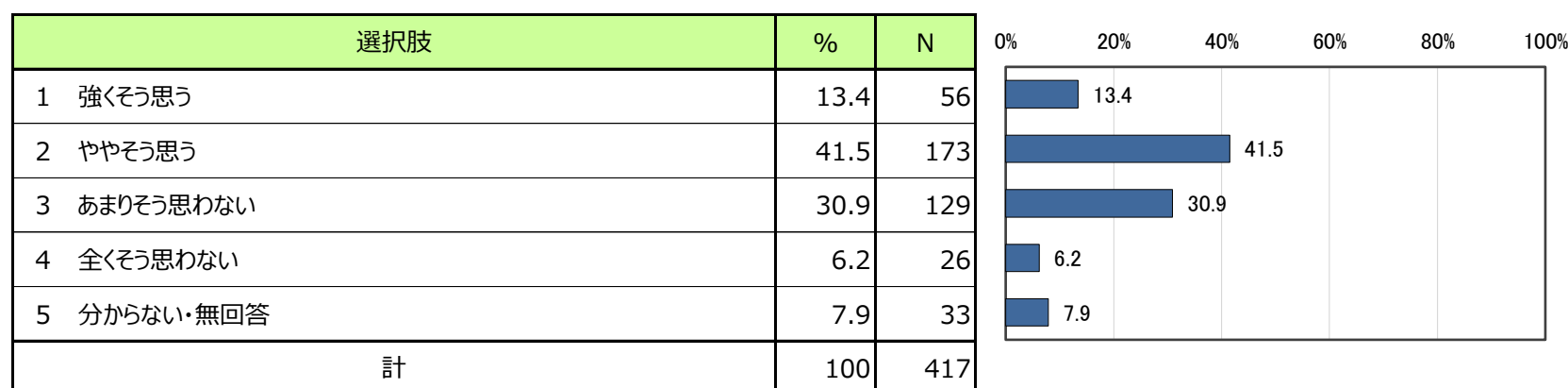
選択肢	%	N
1 強く思う	49.4	206
2 やや思う	36.9	154
3 あまり思わない	6.5	27
4 全く思わない	0.0	0
5 分からない・無回答	7.2	30
計	100	417



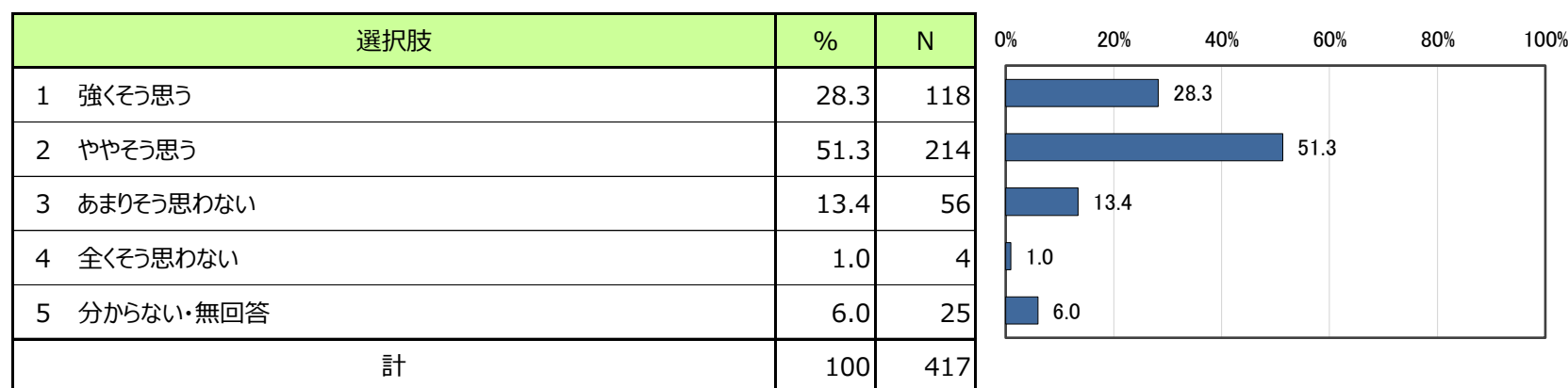
付録3-1 アンケート調査 単純集計結果（委託元調査）

問9 業務委託契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）が明確にならない理由は何だと思えますか。以下の項目について、理由としての当てはまりの度合いをお選びください。（それぞれひとつずつ）

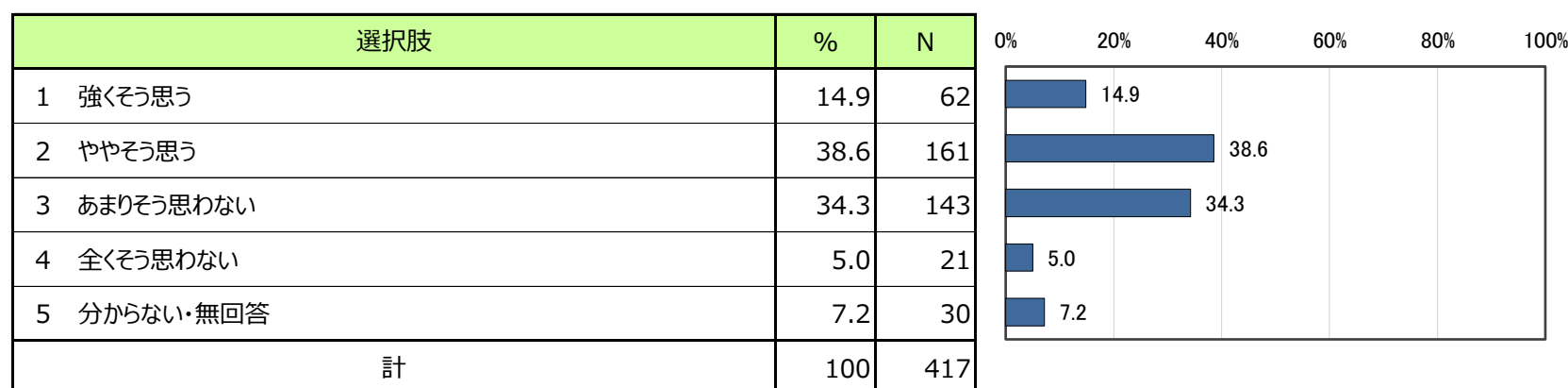
a. 自組織の契約関連文書（仕様書、契約書等）の雛形に情報セキュリティ要求事項の記載がないため、何を決めたらいいかわからない



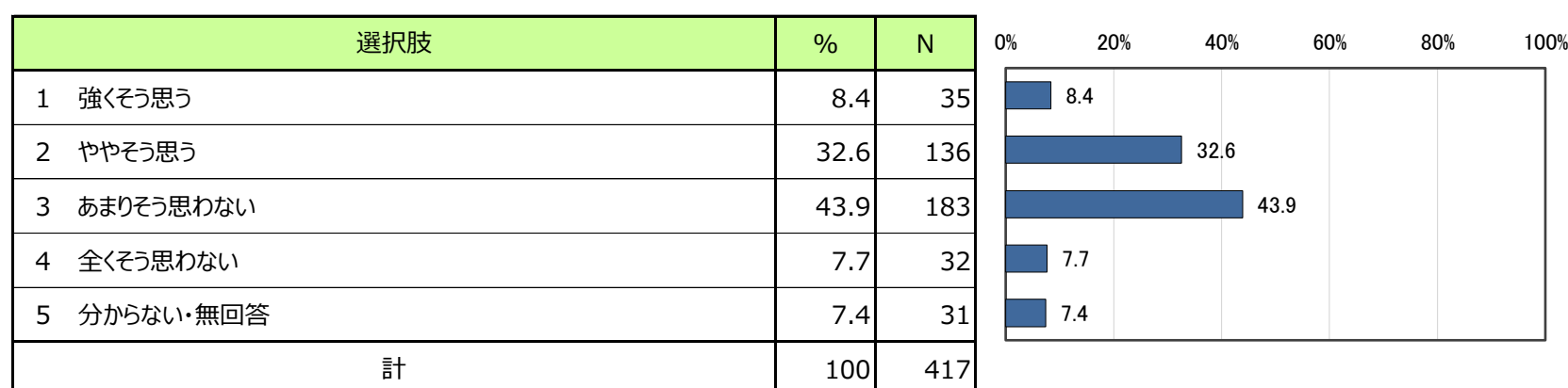
b. 情報セキュリティに関する自組織内の専門知識・スキルが不足している



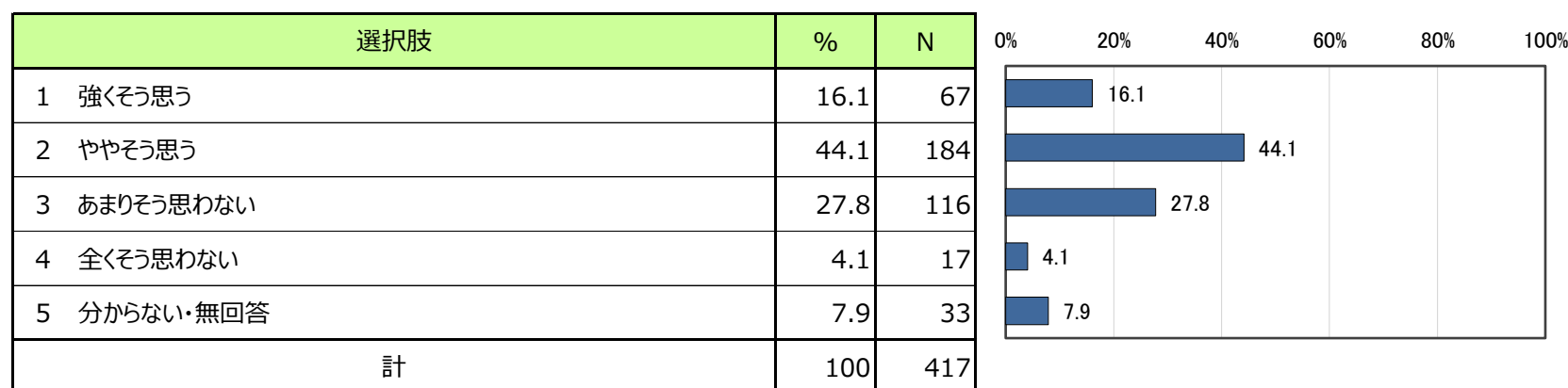
c. 責任範囲を明確にすることで、見積りに反映され、コスト増となる



d. 責任範囲を明確にすることで、自組織内の関係者の心理的負担が増える



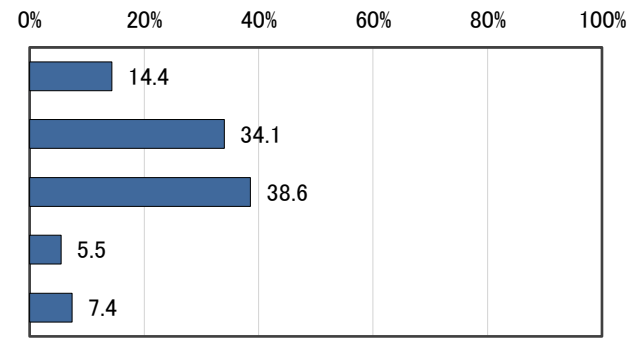
e. 責任範囲を明確にするための作業、調整に時間がかかり契約締結が遅くなる（利用者の不満増大、機会損失の恐れがある）



付録3-1 アンケート調査 単純集計結果（委託元調査）

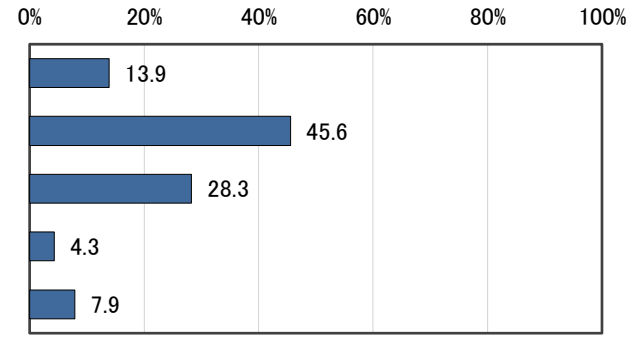
f. 責任範囲を明確にすることで、仕様書等に記述されている以外の対応が期待できなくなる

選択肢	%	N
1 強くそう思う	14.4	60
2 ややそう思う	34.1	142
3 あまりそう思わない	38.6	161
4 全くそう思わない	5.5	23
5 分からない・無回答	7.4	31
計	100	417



g 同じ業者と継続して契約している業務が多く、責任範囲を見直す機会がない

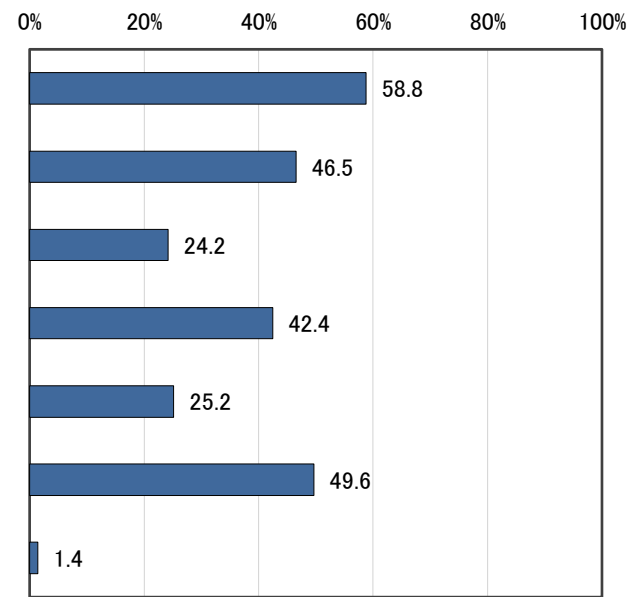
選択肢	%	N
1 強くそう思う	13.9	58
2 ややそう思う	45.6	190
3 あまりそう思わない	28.3	118
4 全くそう思わない	4.3	18
5 分からない・無回答	7.9	33
計	100	417



問10 業務委託契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）を明確にするためには、どのようなことが有効だと考えていますか。当てはまるものを全てお選びください。（いくつでも）

N= 417

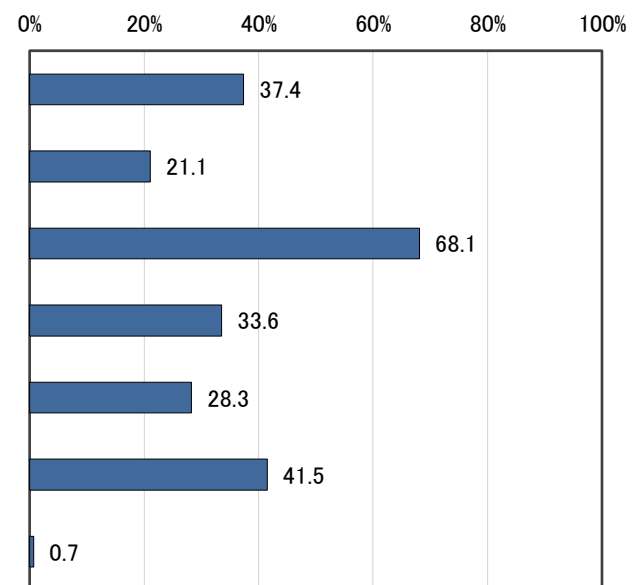
選択肢	%	N
1 契約関連文書（仕様書、契約書等）の雛形の見直し	58.8	245
2 委託先と協力して行うリスクアセスメント	46.5	194
3 調達担当者向けの情報セキュリティに関するセミナー・教育の実施	24.2	101
4 情報セキュリティに関する委託元と委託先の責任範囲が明確でなかったことで起こったトラブルの事例集	42.4	177
5 国による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関する法律の整備	25.2	105
6 国や業界による情報セキュリティに関する委託元と委託先の責任範囲の取り決め方法に関するガイドラインの整備	49.6	207
7 その他	1.4	6



問11 業務委託契約における情報セキュリティに関する責任範囲の明確化について、どのような点が課題だと考えますか。特に課題と考えるものを最大3つまでお選びください。

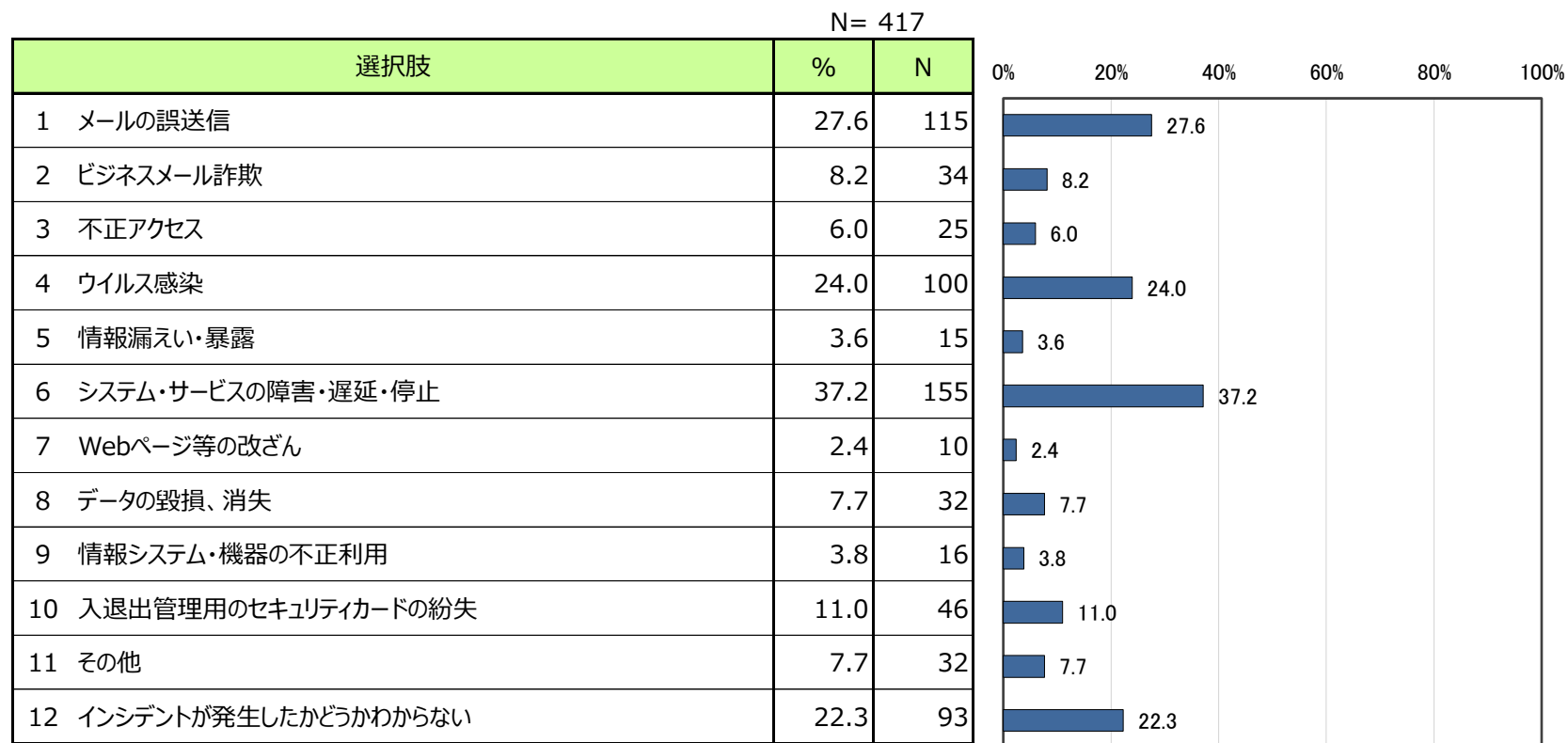
N= 417

選択肢	%	N
1 社内で統一された契約関連文書（仕様書、契約書等）の雛形がない	37.4	156
2 経営層の情報セキュリティに関する意識が低い	21.1	88
3 社内に十分な知見・スキルを持った人材が不足している	68.1	284
4 事業部門の担当者が契約書等の内容を知らずに作業を進めている	33.6	140
5 IoTやAI等の新技術を利用する場合は、責任範囲の考え方について業界指針や判例がない	28.3	118
6 すべての業務委託に対して統一的な管理体制やルールを適用することが難しい	41.5	173
7 その他	0.7	3



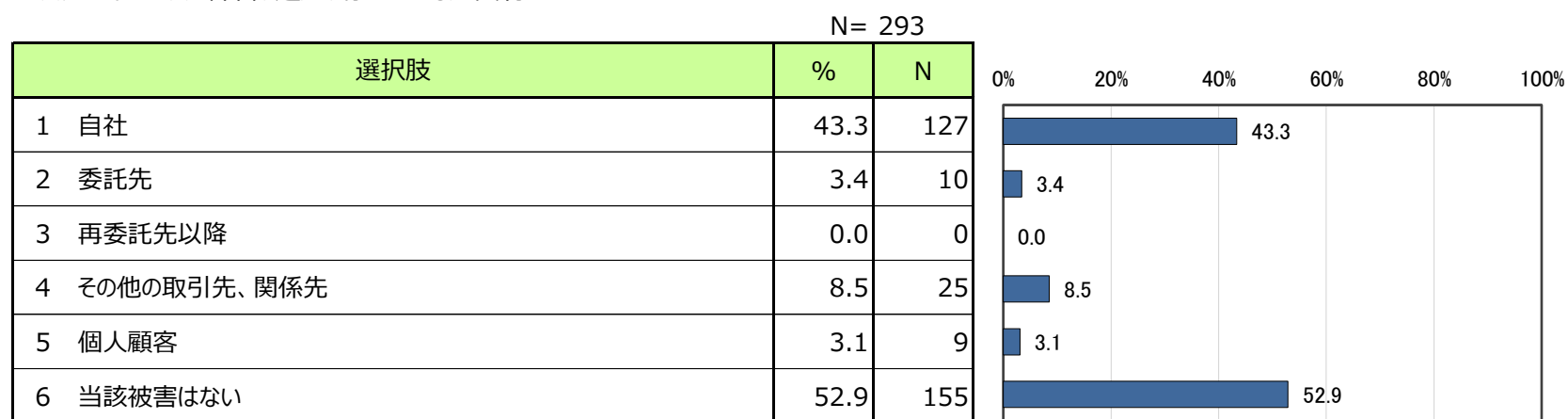
付録3-1 アンケート調査 単純集計結果（委託元調査）

問12 過去3年間の業務委託において、以下のような事象が発生したことがありますか。当てはまるものを全てお選びください。（いくつでも）

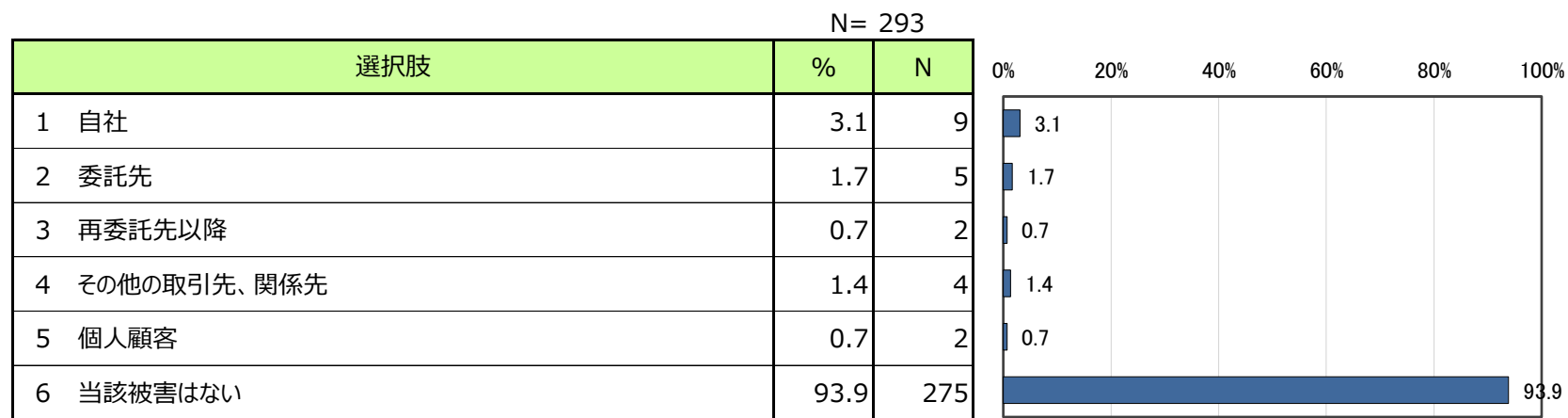


問12-1（問12でいずれかの事象が発生したと回答した場合）発生した事象によって生じた被害の内容と、被害の影響が及んだ範囲（組織・個人）について、当てはまるものを全てお選びください。（それぞれいくつでも）

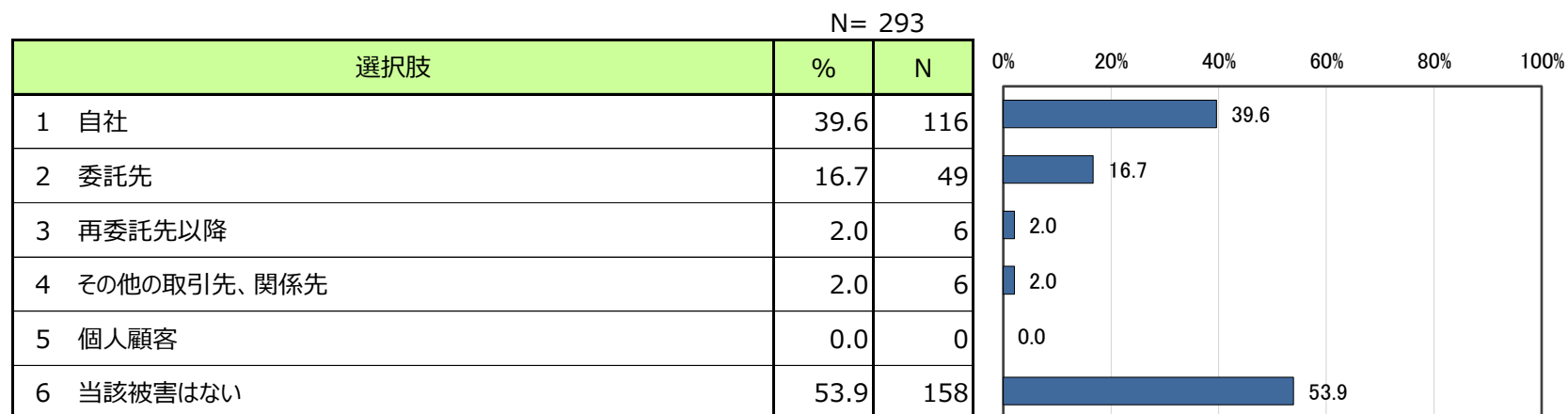
a. ITシステム・サービスの障害、遅延、停止による逸失利益



b. 個人顧客への賠償や法人取引先への補償負担

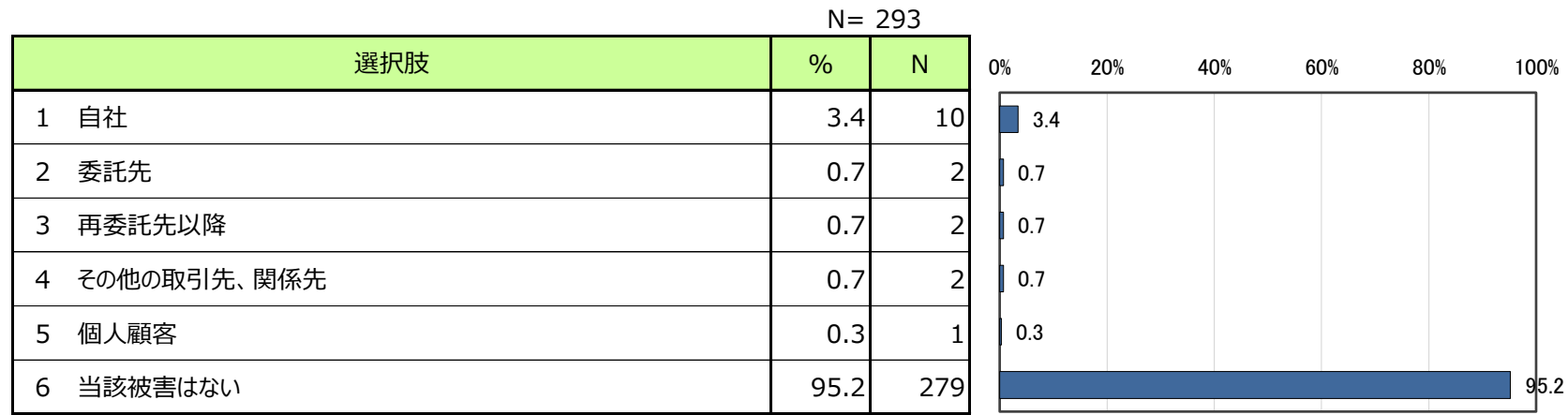


c. 原因調査・復旧にかかわる人件費等の経費負担

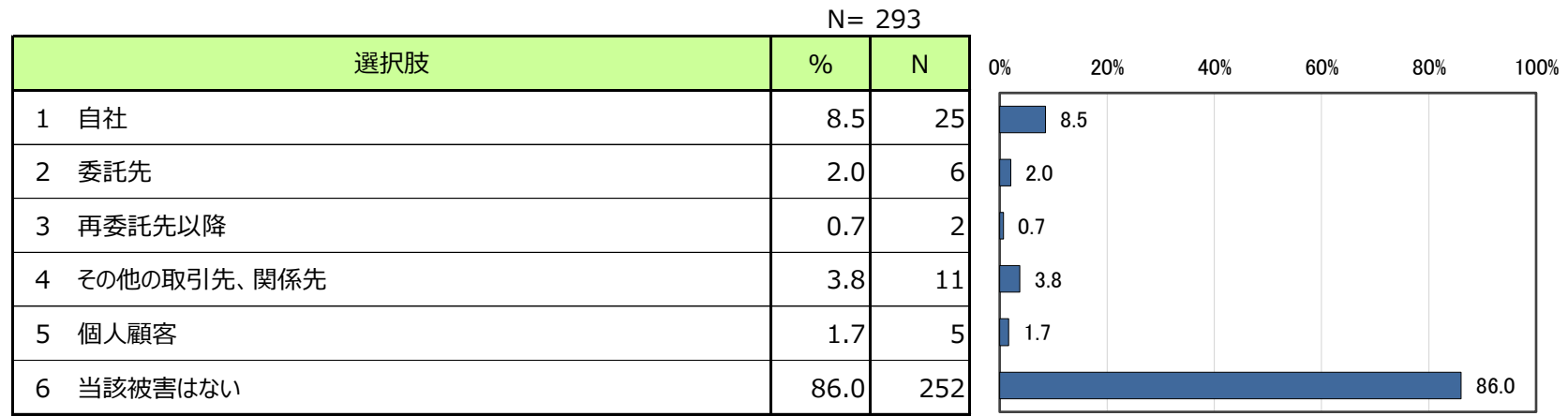


付録3-1 アンケート調査 単純集計結果（委託元調査）

d. 裁判、調停等にかかる人件費等の経費負担

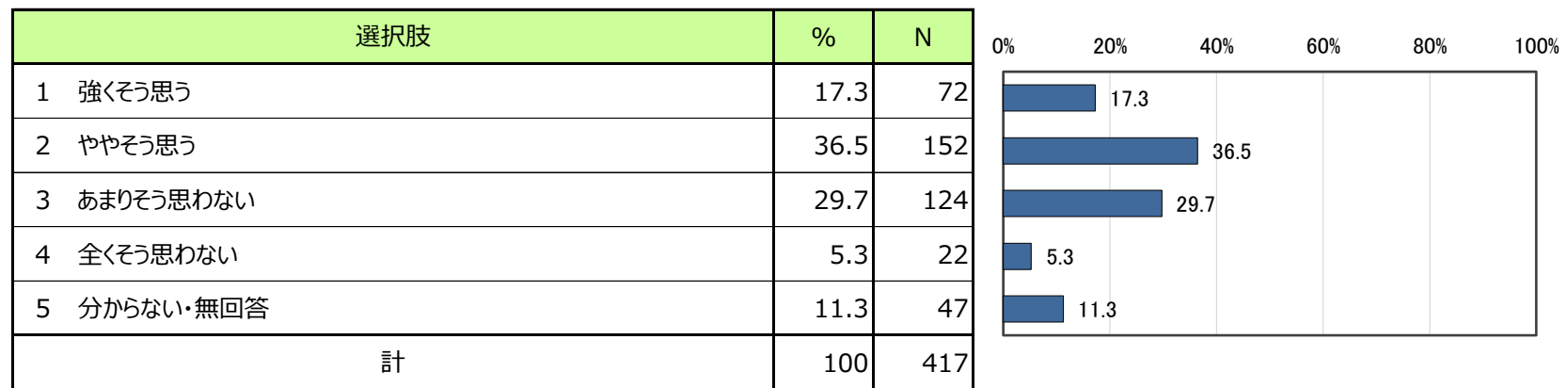


e. 個人顧客や法人取引先に対する信頼の失墜

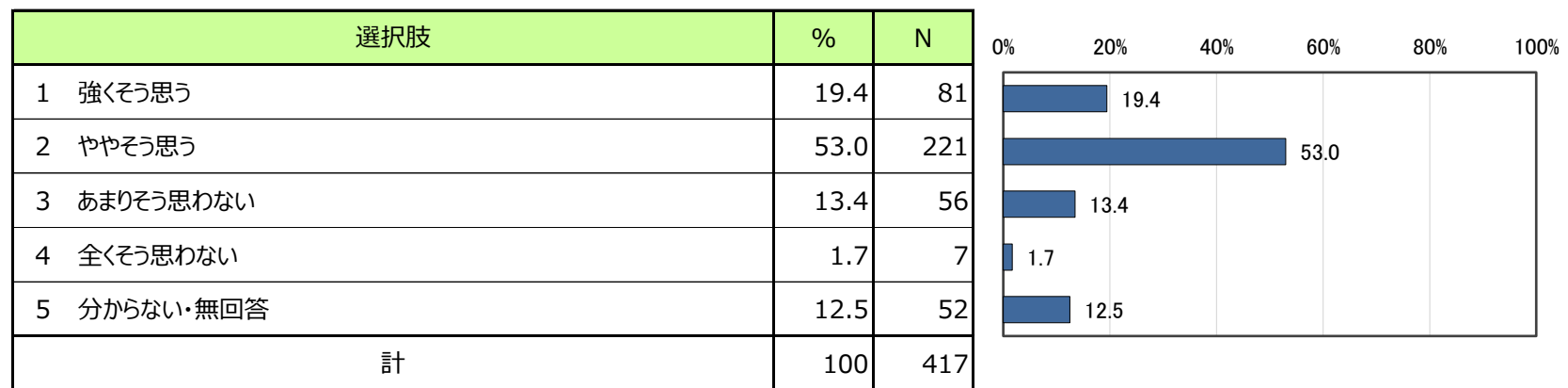


問13 納品後（契約期間外）のITシステムの情報セキュリティに関する未知の脆弱性（契約期間内に明らかでなかったもの）への対応について、どのように考えますか。以下の項目について、当てはまるものをお選びください。（それぞれひとつずつ）

a. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ



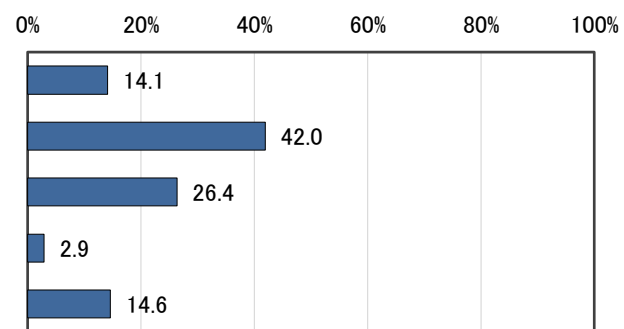
b. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ



付録3-1 アンケート調査 単純集計結果（委託元調査）

c. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ

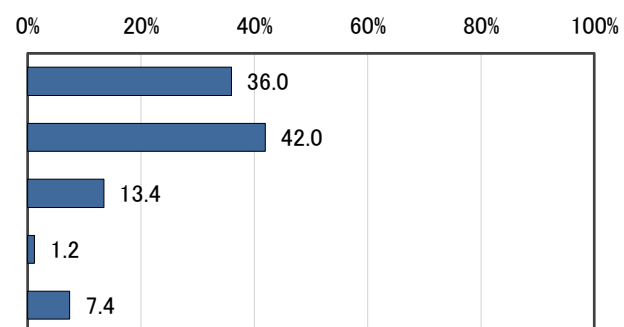
選択肢	%	N
1 強く思う	14.1	59
2 やや思う	42.0	175
3 あまりそう思わない	26.4	110
4 全くそう思わない	2.9	12
5 分からない・無回答	14.6	61
計	100	417



問14 以下の情報セキュリティに関する事項について、懸念の度合いをお答えください。（それぞれひとつずつ）

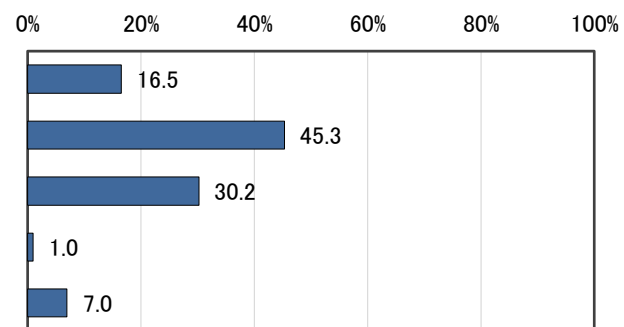
a. 顧客情報や業務情報（機密情報等）が盗まれる（流出する）

選択肢	%	N
1 非常に懸念している	36.0	150
2 ある程度懸念している	42.0	175
3 あまり懸念していない	13.4	56
4 全く懸念していない	1.2	5
5 分からない・無回答	7.4	31
計	100	417



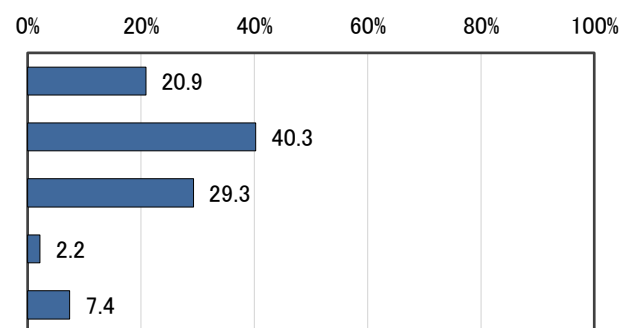
b. Webサイトや業務サーバの内容が改ざんされる

選択肢	%	N
1 非常に懸念している	16.5	69
2 ある程度懸念している	45.3	189
3 あまり懸念していない	30.2	126
4 全く懸念していない	1.0	4
5 分からない・無回答	7.0	29
計	100	417



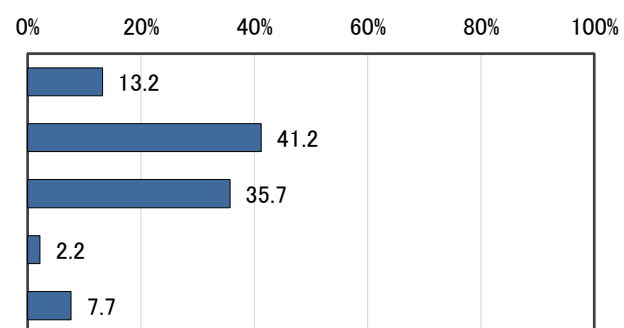
c. WebサイトやIoT機器が乗っ取られサイバー攻撃に悪用される

選択肢	%	N
1 非常に懸念している	20.9	87
2 ある程度懸念している	40.3	168
3 あまり懸念していない	29.3	122
4 全く懸念していない	2.2	9
5 分からない・無回答	7.4	31
計	100	417



d. サイバー攻撃によってWebサイトの負荷が高まり利用できなくなる

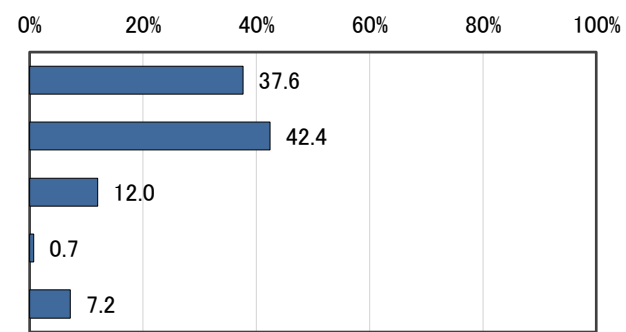
選択肢	%	N
1 非常に懸念している	13.2	55
2 ある程度懸念している	41.2	172
3 あまり懸念していない	35.7	149
4 全く懸念していない	2.2	9
5 分からない・無回答	7.7	32
計	100	417



付録3-1 アンケート調査 単純集計結果（委託元調査）

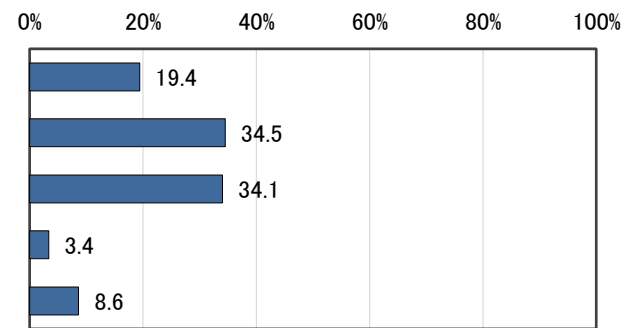
e. 業務サーバ、Webサーバがウイルスに感染する

選択肢	%	N
1 非常に懸念している	37.6	157
2 ある程度懸念している	42.4	177
3 あまり懸念していない	12.0	50
4 全く懸念していない	0.7	3
5 分からない・無回答	7.2	30
計	100	417



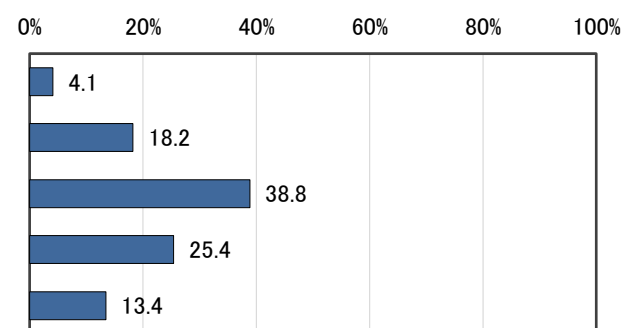
f. マスメディアで騒がれたりインターネット上で風評被害が広がる

選択肢	%	N
1 非常に懸念している	19.4	81
2 ある程度懸念している	34.5	144
3 あまり懸念していない	34.1	142
4 全く懸念していない	3.4	14
5 分からない・無回答	8.6	36
計	100	417



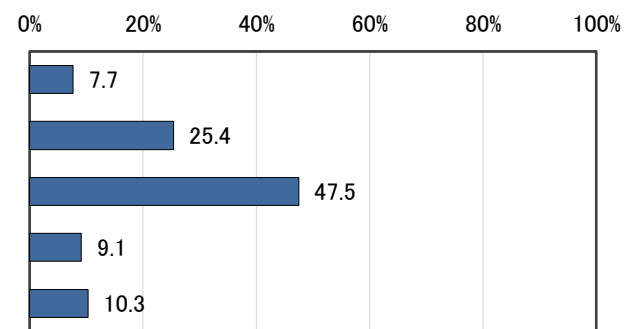
g クラウドサービスのサーバが海外にある

選択肢	%	N
1 非常に懸念している	4.1	17
2 ある程度懸念している	18.2	76
3 あまり懸念していない	38.8	162
4 全く懸念していない	25.4	106
5 分からない・無回答	13.4	56
計	100	417



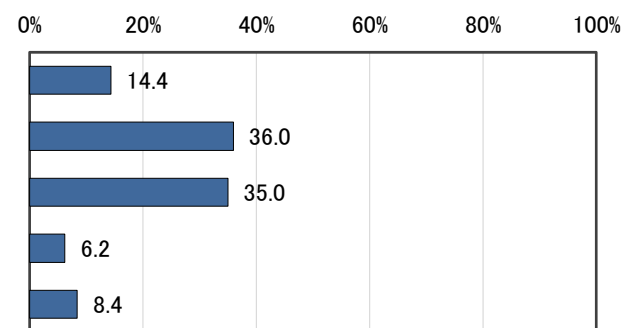
h 委託先で不正なプログラムや機能が埋め込まれる

選択肢	%	N
1 非常に懸念している	7.7	32
2 ある程度懸念している	25.4	106
3 あまり懸念していない	47.5	198
4 全く懸念していない	9.1	38
5 分からない・無回答	10.3	43
計	100	417



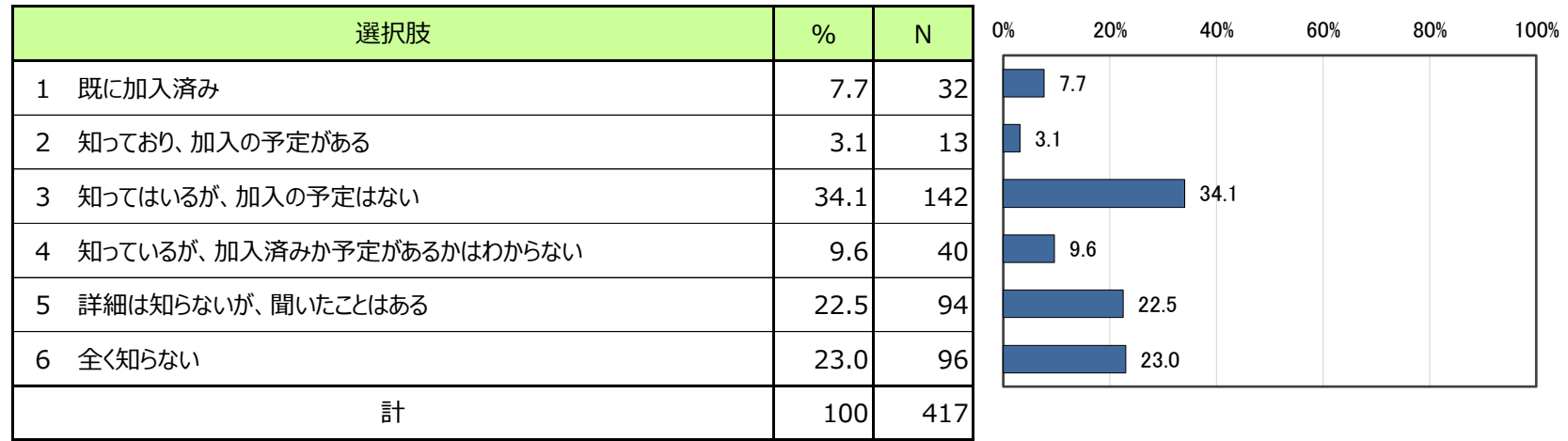
i 取引先の脆弱性が原因で自社内に侵入される

選択肢	%	N
1 非常に懸念している	14.4	60
2 ある程度懸念している	36.0	150
3 あまり懸念していない	35.0	146
4 全く懸念していない	6.2	26
5 分からない・無回答	8.4	35
計	100	417

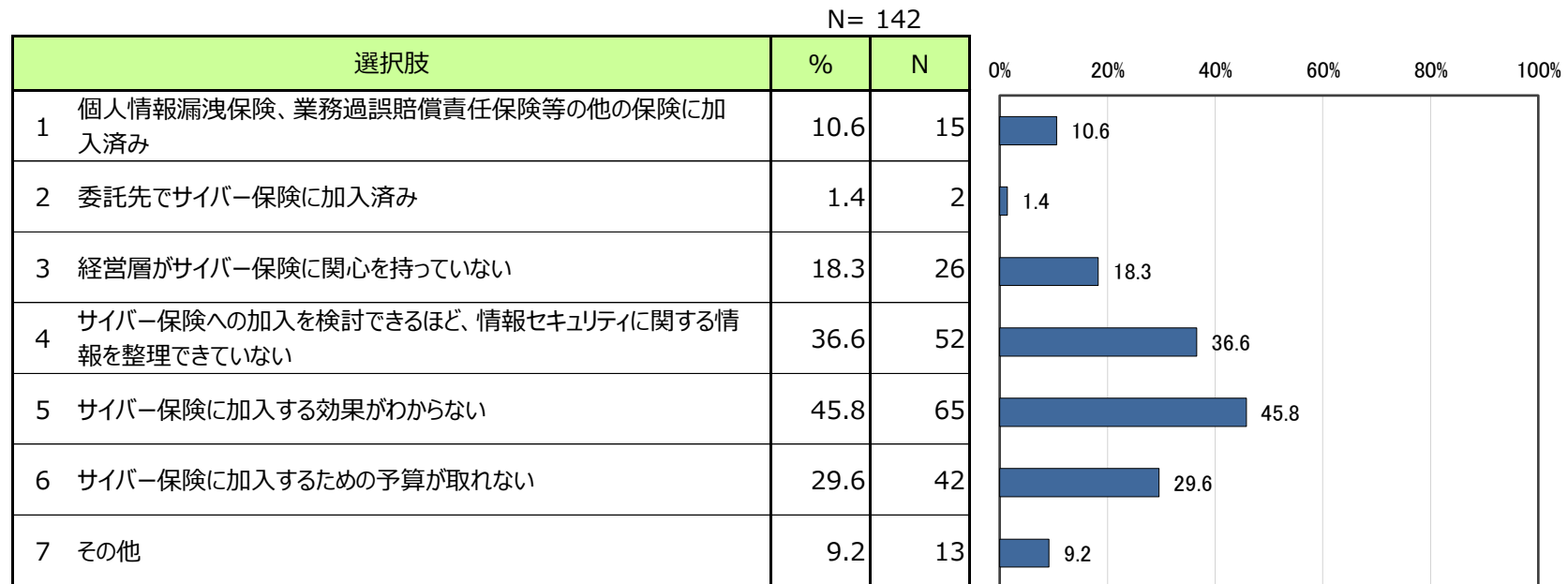


付録3-1 アンケート調査 単純集計結果（委託元調査）

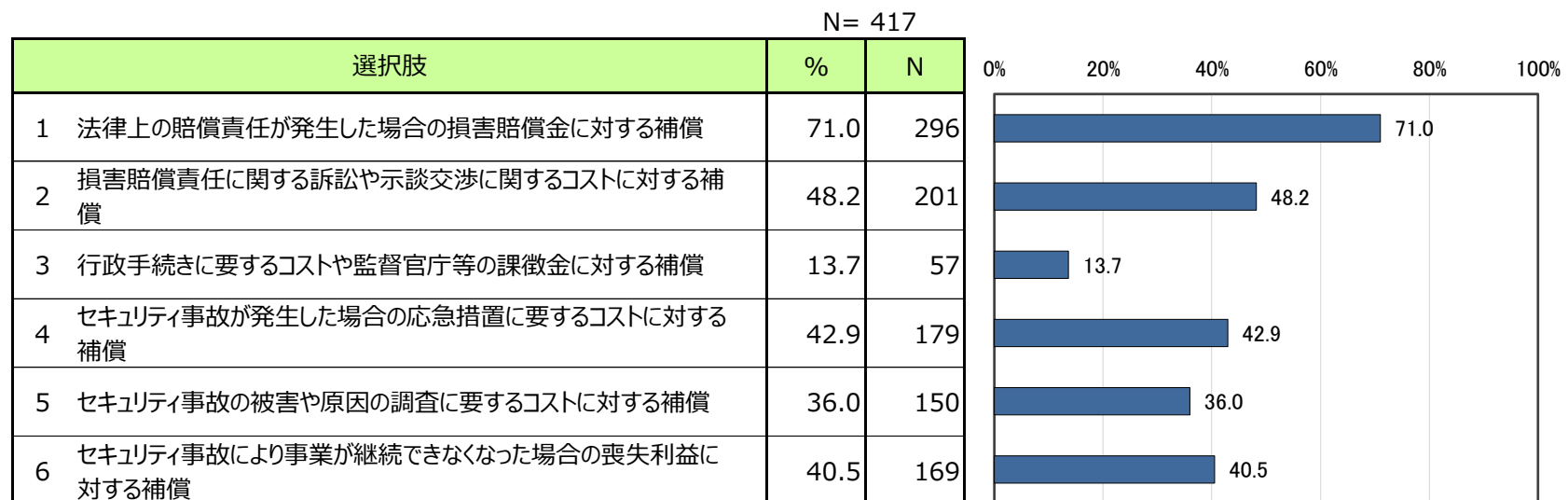
問15 情報セキュリティのリスク低減（移転）策のひとつにサイバー保険がありますが、サイバー保険をご存じですか。当てはまるものをお選びください。（ひとつだけ）



問15 -1（問15で「知ってはいるが、加入の予定はない」と回答した場合）加入の予定がない理由について、当てはまるものを全てお選びください。（いくつでも）

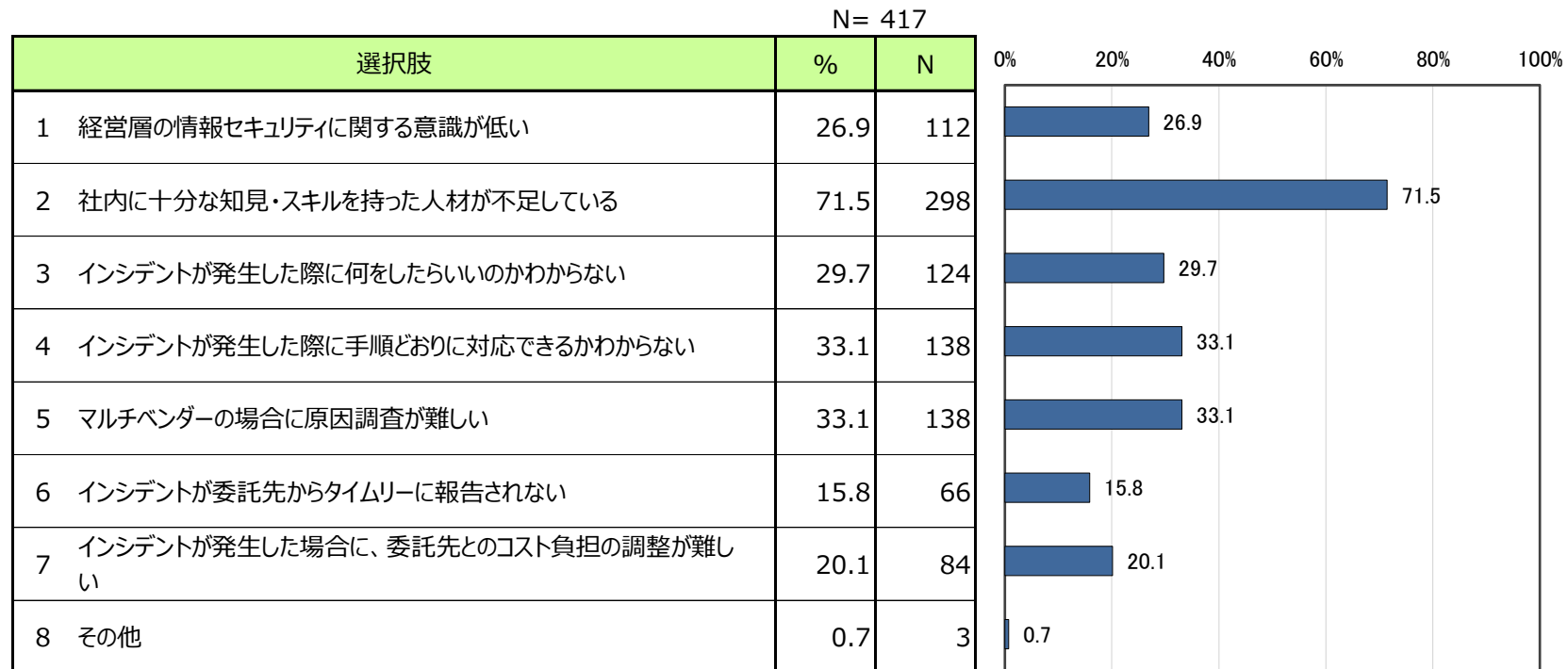


問16 以下にサイバー保険の代表的な補償内容をあげています。これらの補償内容のうち、どれが魅力的であると考えますか。特に魅力的であると考えるものを最大3つまでお選びください。

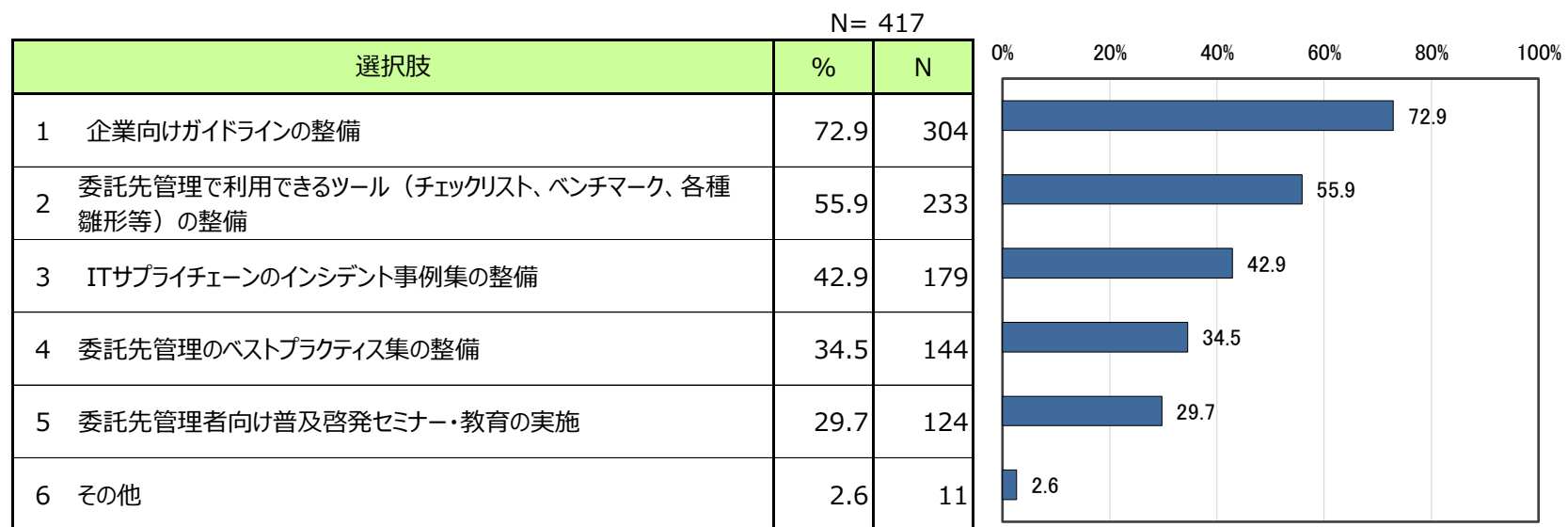


付録3-1 アンケート調査 単純集計結果（委託元調査）

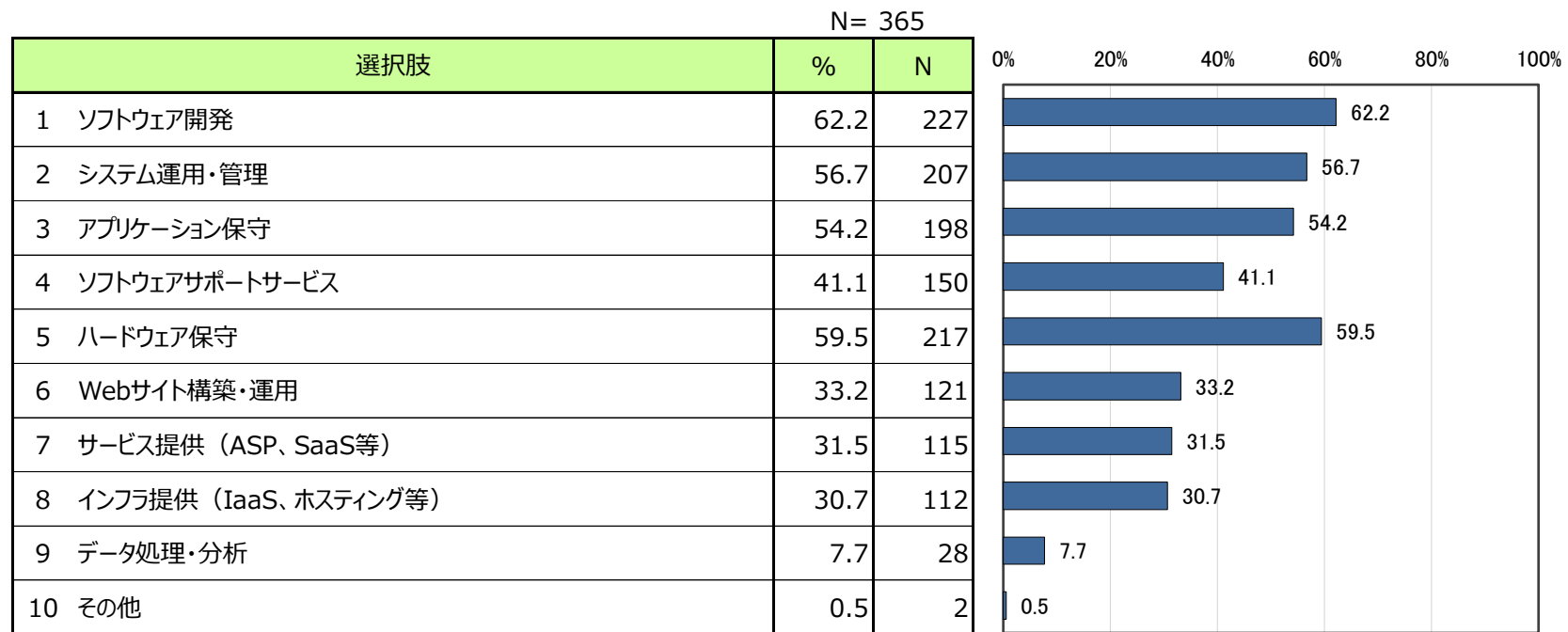
問17 インシデント対応やリスク対応において、どのような点が課題と考えますか。特に課題と考えるものを最大3つまでお選び下さい



問18 ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに求める施策はありますか。施策として期待するものを全てお選びください。（いくつでも）

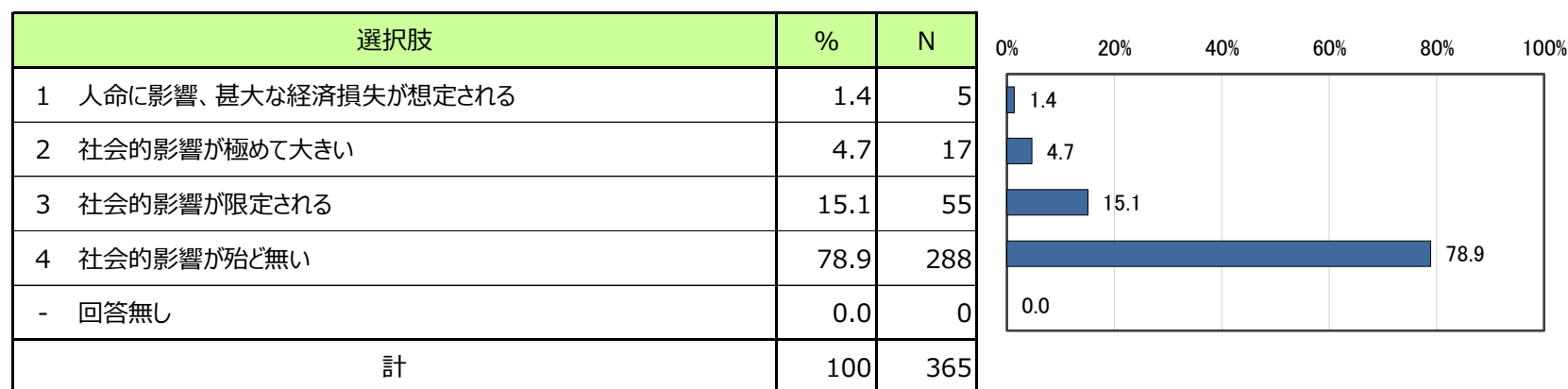


問19 当該事例に含まれるITシステム・サービスについて当てはまるものを全てお選びください。（いくつでも）

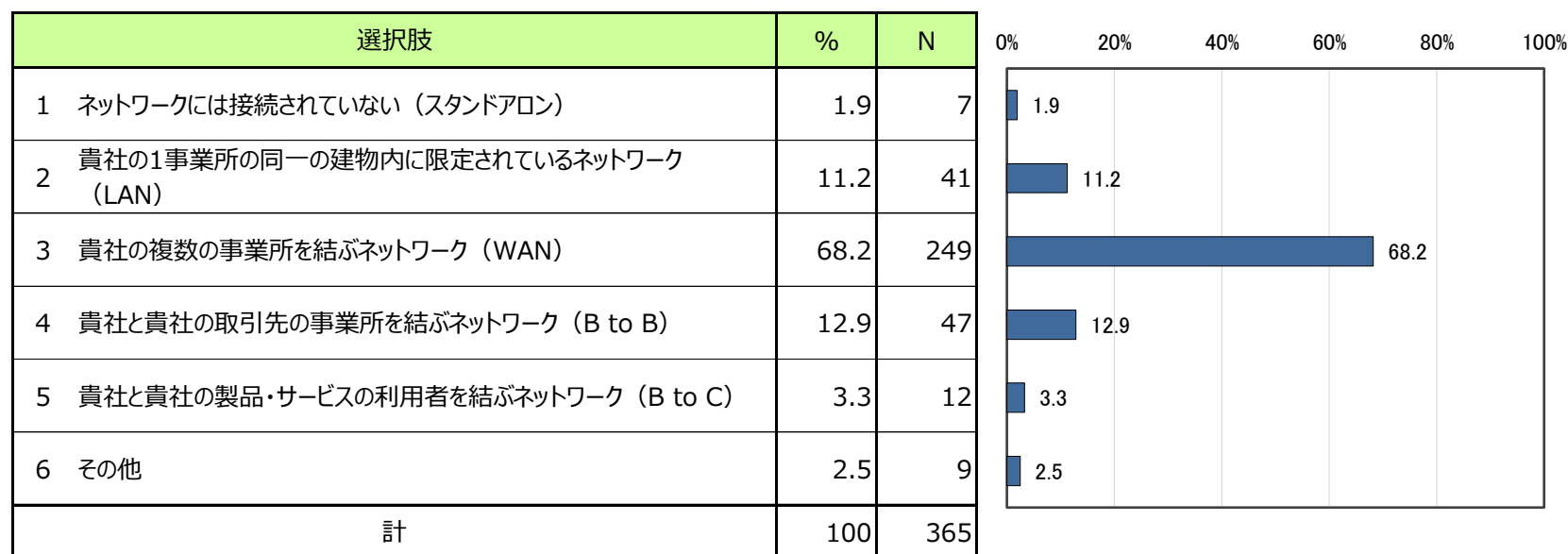


付録3-1 アンケート調査 単純集計結果（委託元調査）

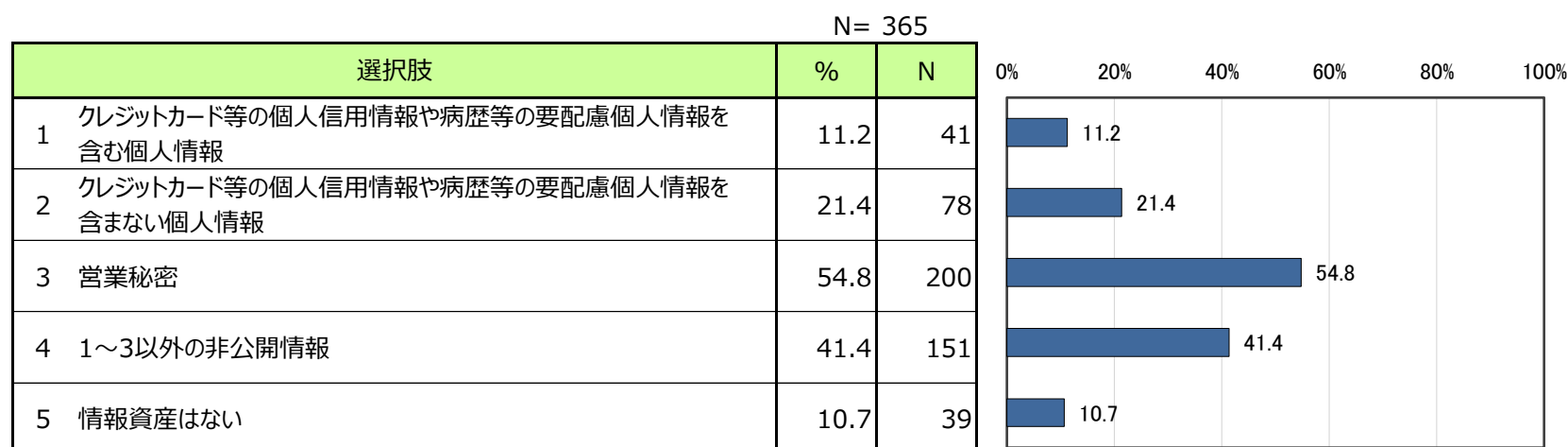
問20 当該事例のITシステム・サービスの障害発生時の社会的影響度について、当てはまるものをお選びください。（ひとつだけ）



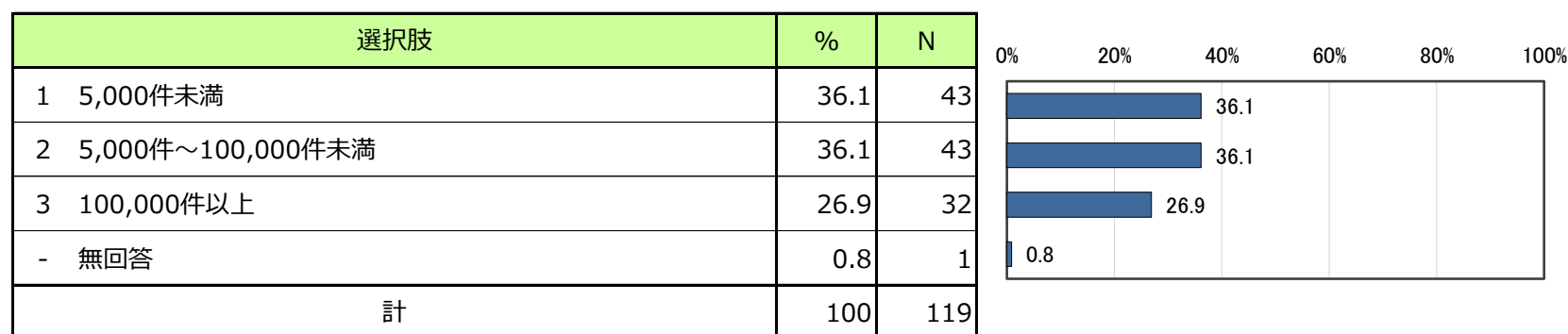
問21 当該事例のITシステム・サービスのネットワークの範囲について、当てはまるものをお選びください。（ひとつだけ）



問22 当該事例のITシステム・サービスで扱う情報資産について、当てはまるものを全てお選びください。（いくつでも）



問22-1（問22で「個人情報が含まれている」と回答した場合）個人情報のデータ件数について、当てはまるものをお選びください。（ひとつだけ）

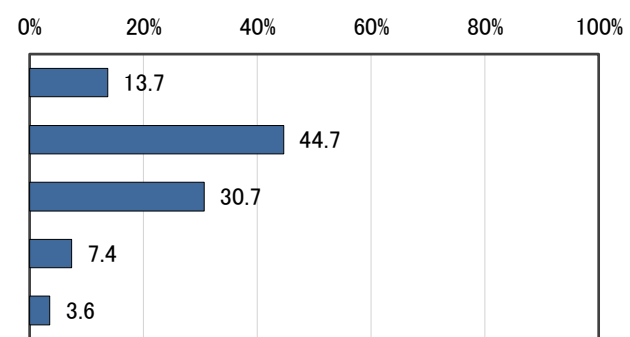


付録3-1 アンケート調査 単純集計結果（委託元調査）

問23 当該事例の業務委託で扱う情報資産に関して、契約の際に情報セキュリティ上のリスクをどの程懸念しましたか。それぞれの脅威に対する懸念の度合いとして当てはまるものをお選びください。（それぞれひとつずつ）

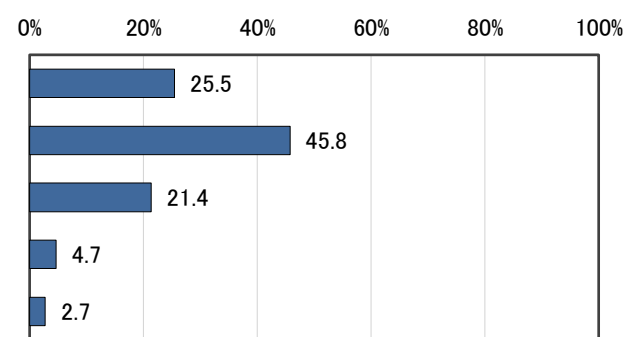
a. 内部不正

選択肢	%	N
1 非常に懸念した	13.7	50
2 ある程度懸念した	44.7	163
3 あまり懸念しなかった	30.7	112
4 全く懸念しなかった	7.4	27
5 分からない・無回答	3.6	13
計	100	365



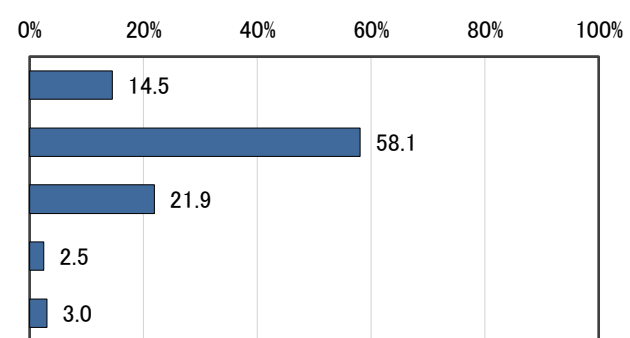
b. 外部攻撃（ウイルス感染や不正アクセス等）

選択肢	%	N
1 非常に懸念した	25.5	93
2 ある程度懸念した	45.8	167
3 あまり懸念しなかった	21.4	78
4 全く懸念しなかった	4.7	17
5 分からない・無回答	2.7	10
計	100	365



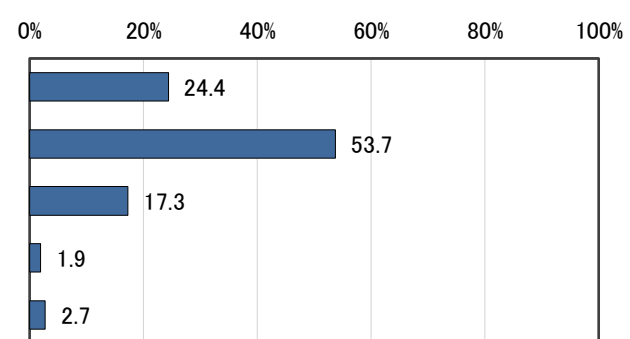
c. 人的ミス(誤操作等)

選択肢	%	N
1 非常に懸念した	14.5	53
2 ある程度懸念した	58.1	212
3 あまり懸念しなかった	21.9	80
4 全く懸念しなかった	2.5	9
5 分からない・無回答	3.0	11
計	100	365



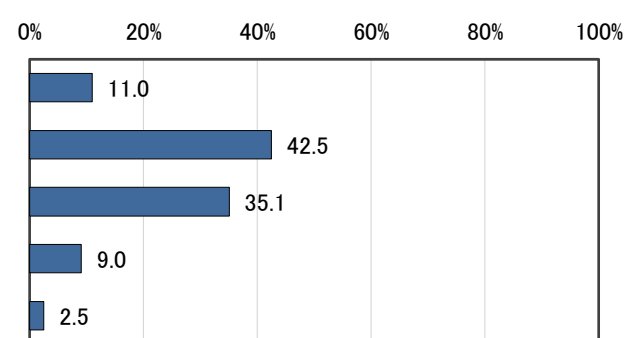
d. システム障害、停止

選択肢	%	N
1 非常に懸念した	24.4	89
2 ある程度懸念した	53.7	196
3 あまり懸念しなかった	17.3	63
4 全く懸念しなかった	1.9	7
5 分からない・無回答	2.7	10
計	100	365



e. 災害

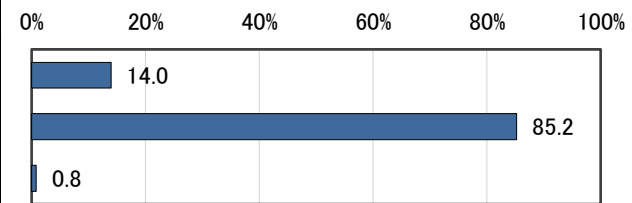
選択肢	%	N
1 非常に懸念した	11.0	40
2 ある程度懸念した	42.5	155
3 あまり懸念しなかった	35.1	128
4 全く懸念しなかった	9.0	33
5 分からない・無回答	2.5	9
計	100	365



付録3-1 アンケート調査 単純集計結果（委託元調査）

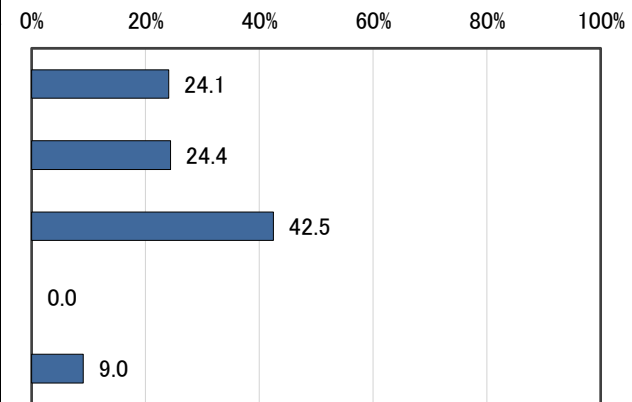
問24 当該事例の委託先は、貴社と資本関係のある系列企業・グループ企業ですか。（ひとつだけ）

選択肢	%	N
1 系列企業・グループ企業	14.0	51
2 系列企業・グループ企業以外	85.2	311
- 無回答	0.8	3
計	100	365



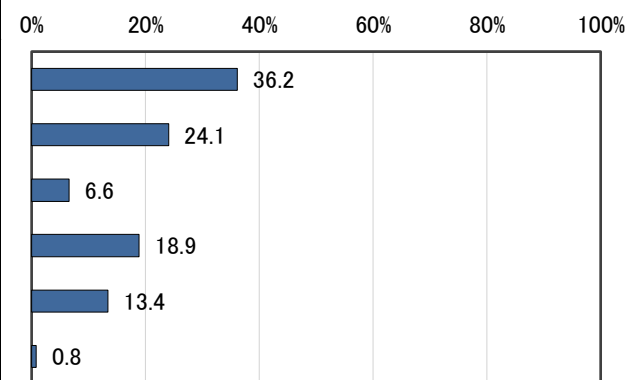
問25 当該事例の委託先はどのようにして決定しましたか。（ひとつだけ）

選択肢	%	N
1 1社にのみ見積りを徴収して決定	24.1	88
2 2社以上から見積りのみを徴収して決定	24.4	89
3 2社以上から業務提案と見積りを徴収して技術力等を勘案して決定	42.5	155
4 一般公募による入札で決定	0.0	0
5 その他・無回答	9.0	33
計	100	365



問26 委託先には再委託先がありますか。また、再々委託先等の有無を把握していますか。（ひとつだけ）

選択肢	%	N
1 再委託先はない	36.2	132
2 再委託先はあり、再々委託先はない	24.1	88
3 再委託先はあり、再々委託先以降もある	6.6	24
4 再委託先はあるが、再々委託先があるかどうか分からない	18.9	69
5 再委託先等があるかどうか分からない	13.4	49
- 無回答	0.8	3
計	100	365

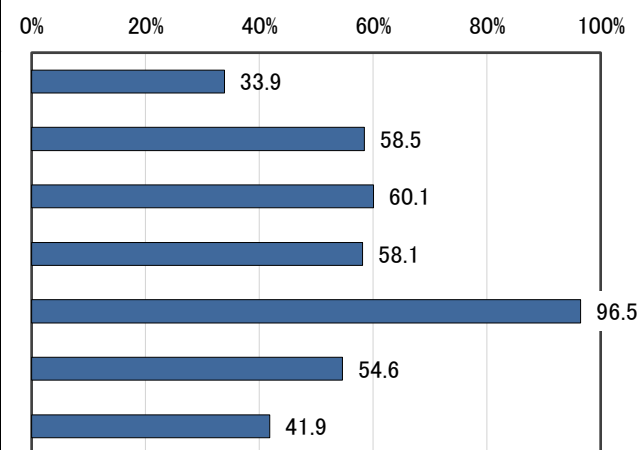


問27 以下の情報セキュリティに係る要求事項について、当該事例の契約関連文書（仕様書、契約書等）にどのように記載されているか、選択肢の番号でご回答ください。

1. 使用した契約関連文書

N= 313

契約関連文書	%	N
1 約款	33.9	106
2 委託先の提案書	58.5	183
3 仕様書	60.1	188
4 委託先の見積書	58.1	182
5 契約書	96.5	302
6 覚書	54.6	171
7 その他（SLA等）	41.9	131



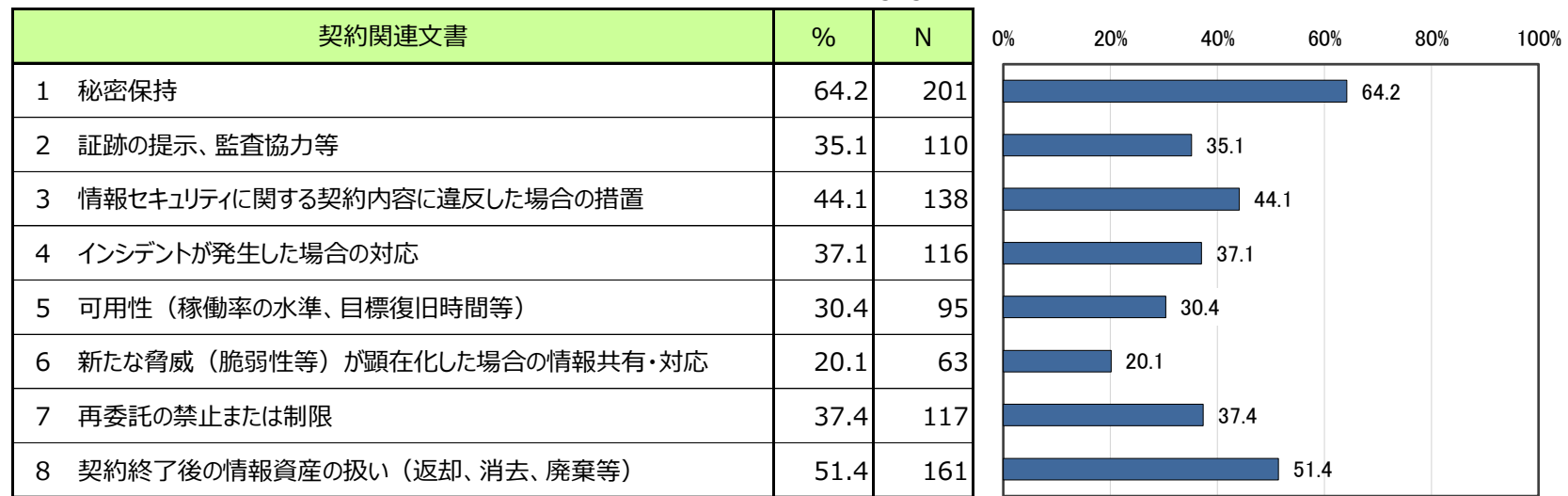
※責任範囲の明示の有無について回答のなかった53件を集計から除いている

付録3-1 アンケート調査 単純集計結果（委託元調査）

2. 契約関連文書に記載されているセキュリティ要求事項（文書は問わない）

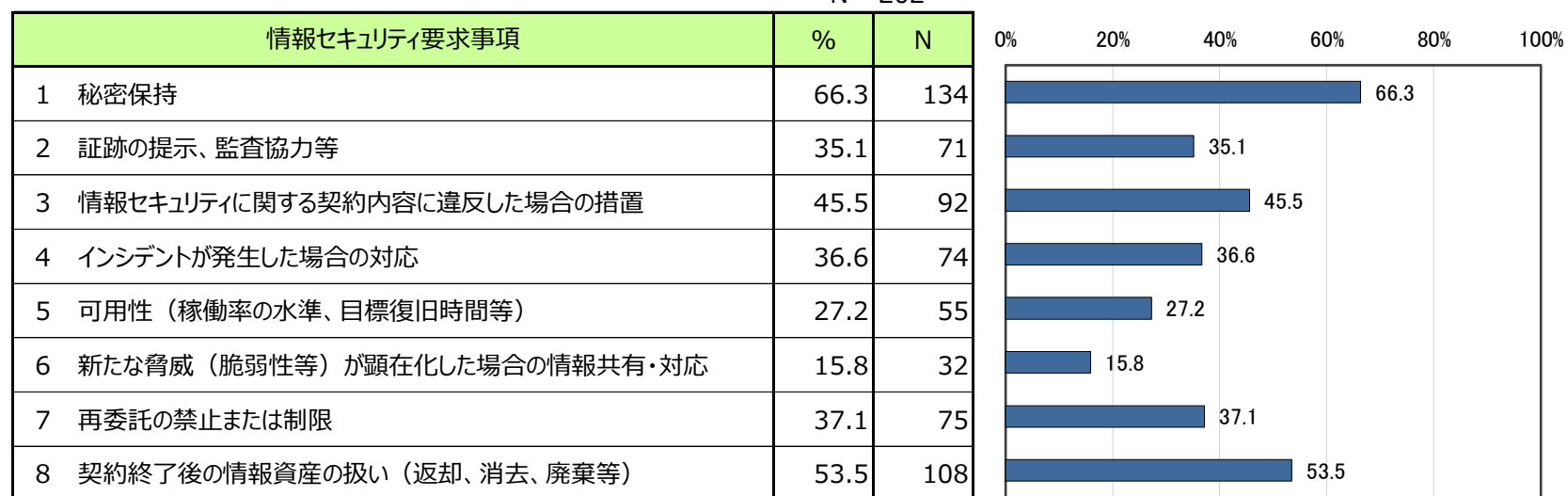
<全体>

N= 313



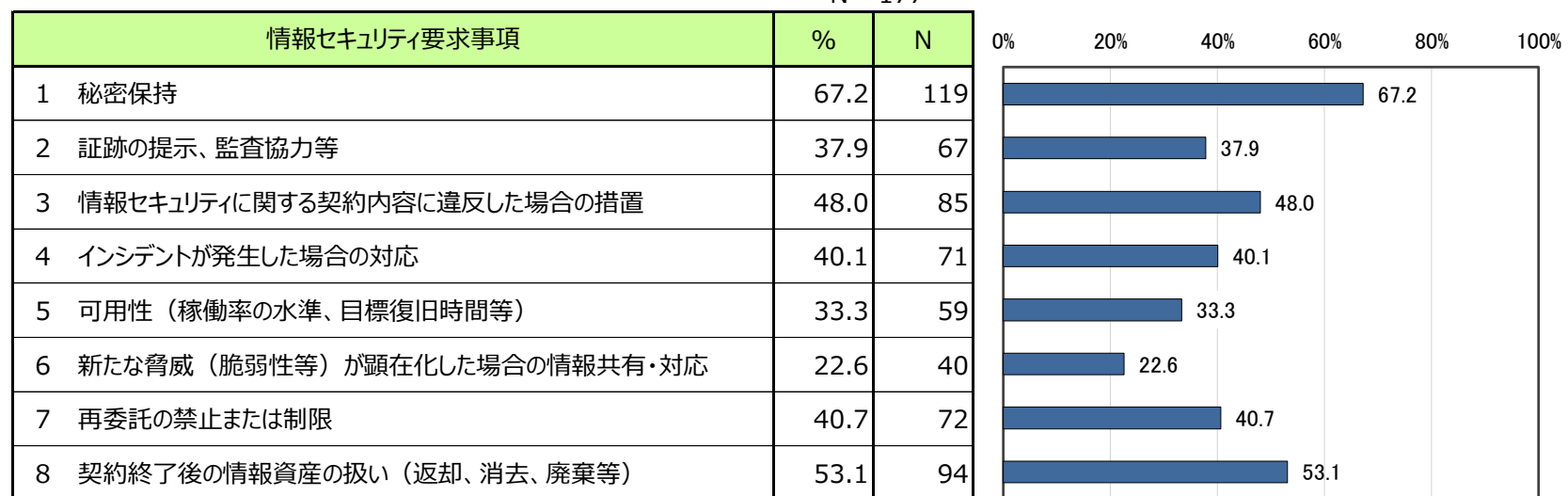
a. ソフトウェア開発を含む事例

N= 202



b. システム運用・管理を含む事例

N= 177



c. アプリケーション保守を含む事例

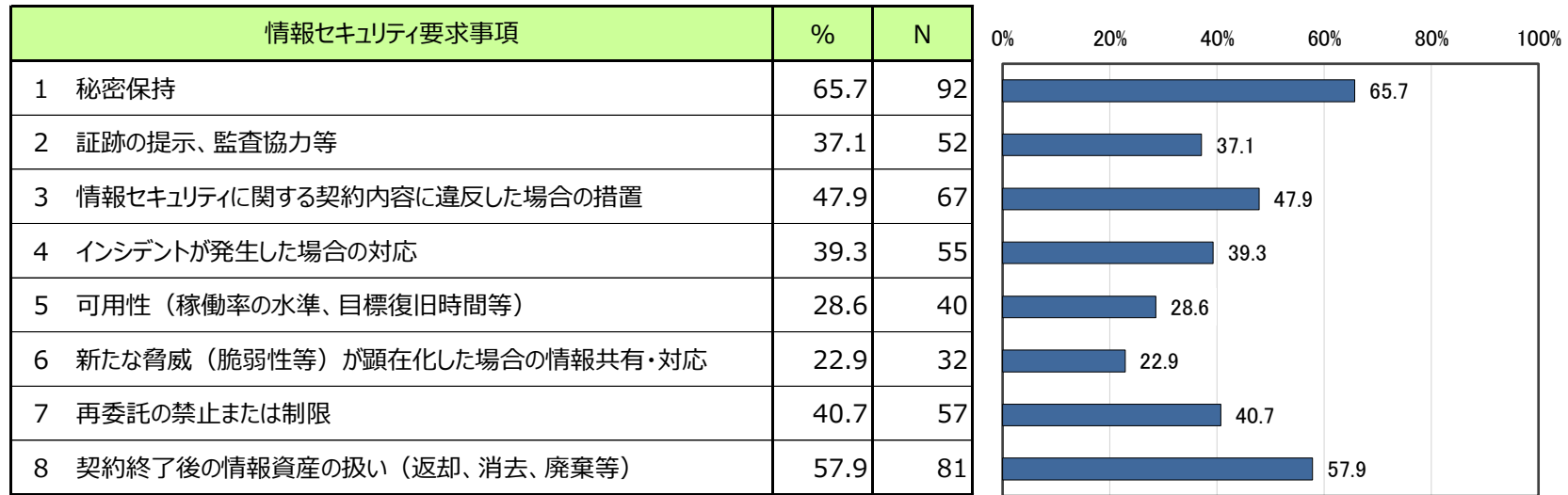
N= 178



付録3-1 アンケート調査 単純集計結果（委託元調査）

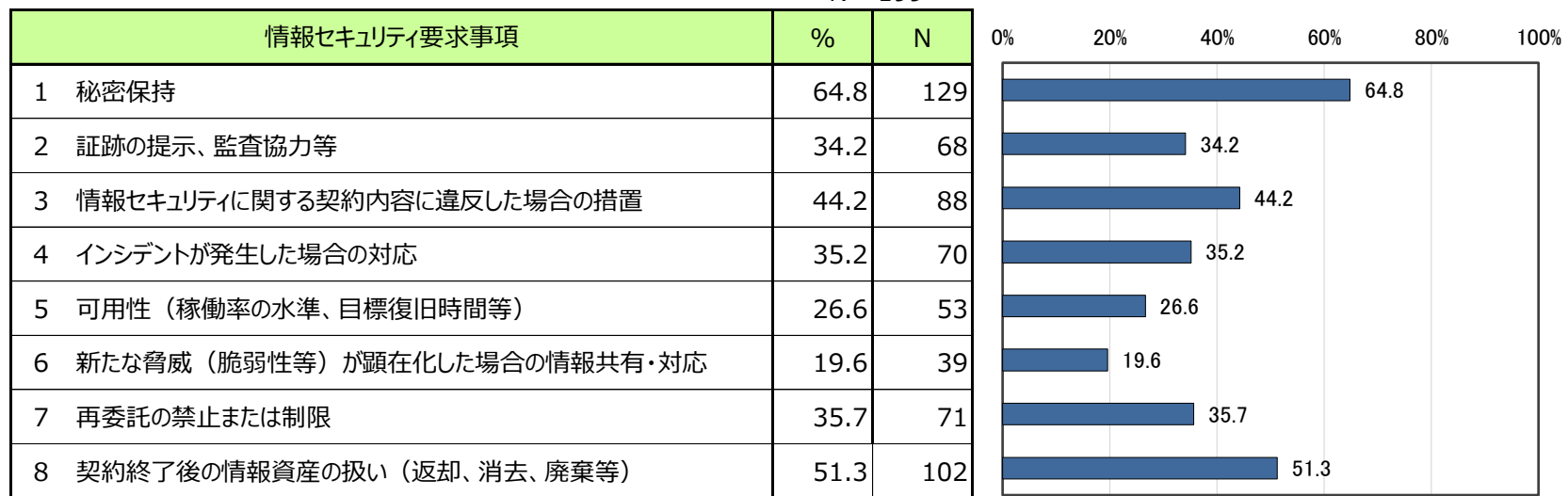
d.ソフトウェアサポートサービスを含む事例

N= 140



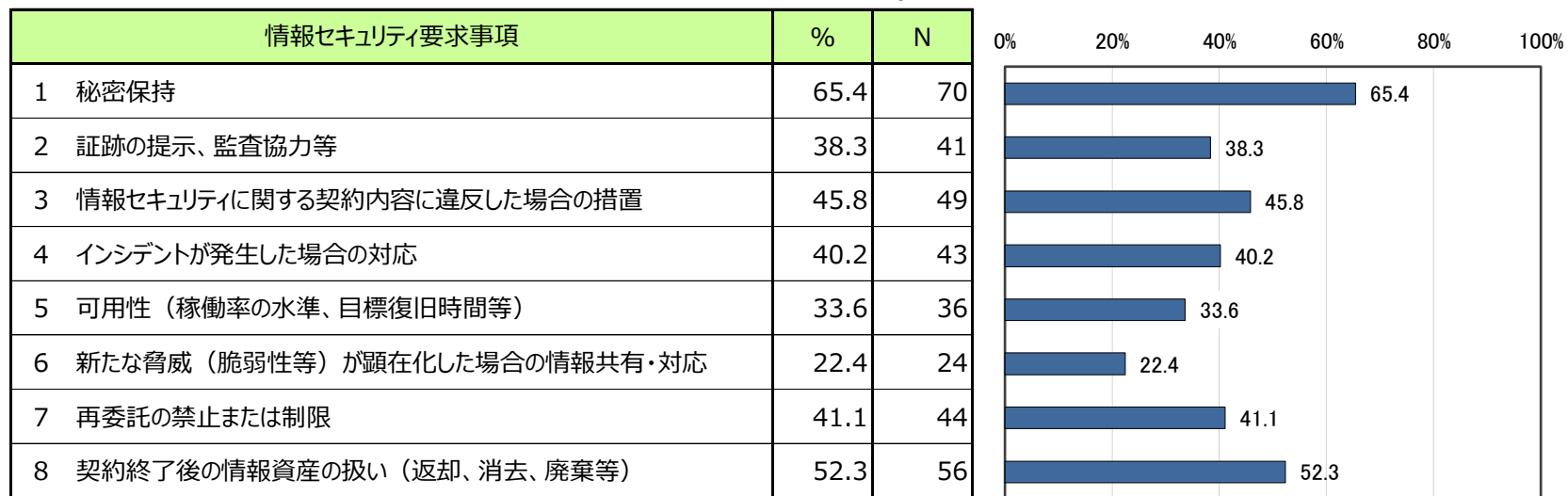
e.ハードウェア保守を含む事例

N= 199



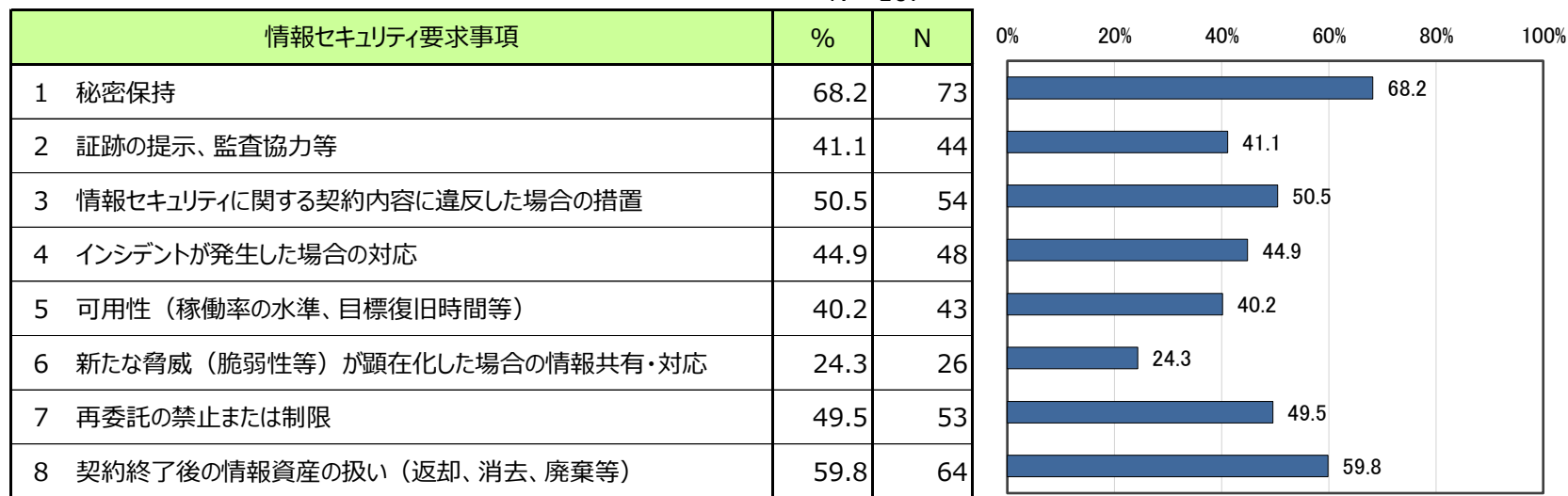
f.Webサイト構築・運用を含む事例

N= 107



g.サービス提供（ASP、SaaS等）を含む事例

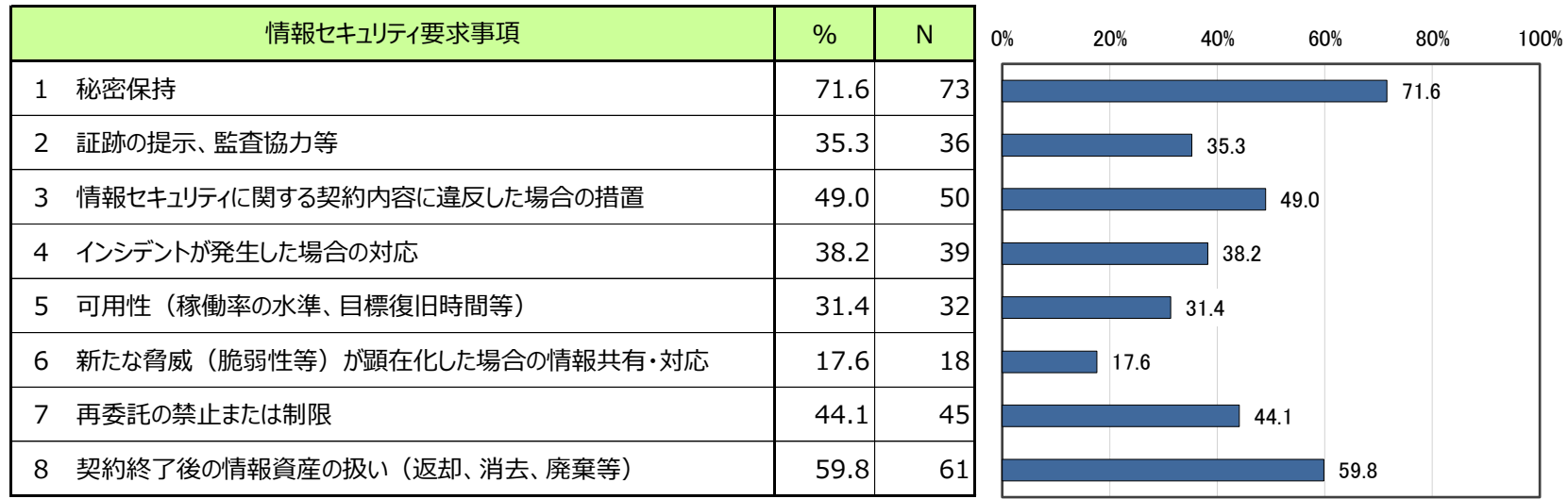
N= 107



付録3-1 アンケート調査 単純集計結果（委託元調査）

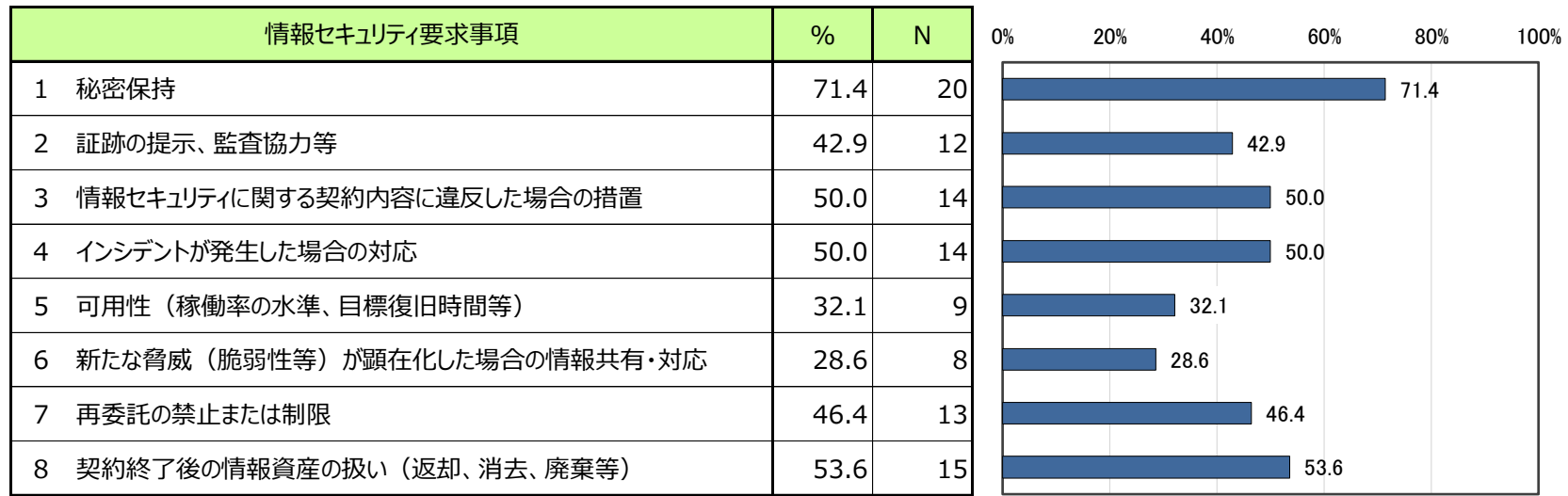
h.インフラ提供（IaaS、ホスティング等）を含む事例

N= 102



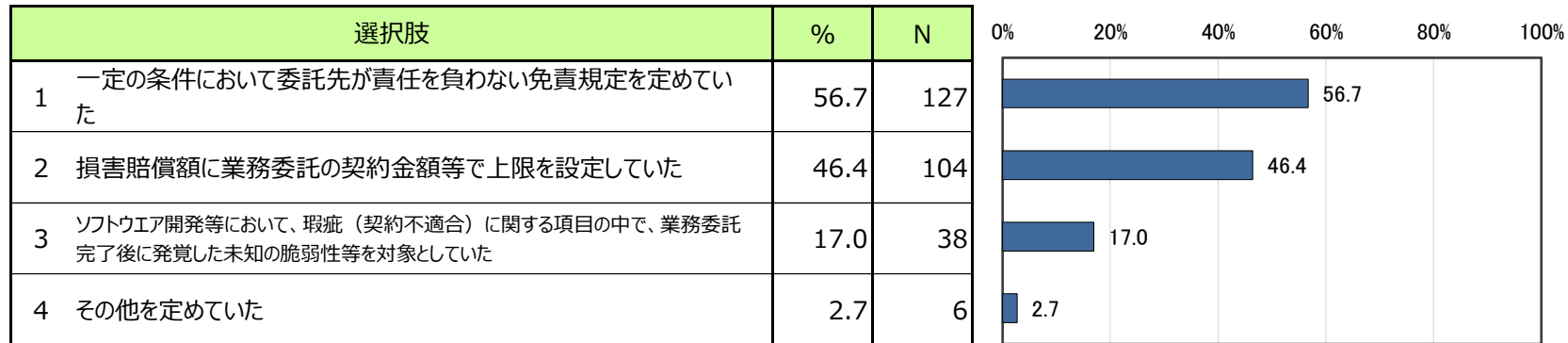
i.データ処理・分析を含む事例

N= 28

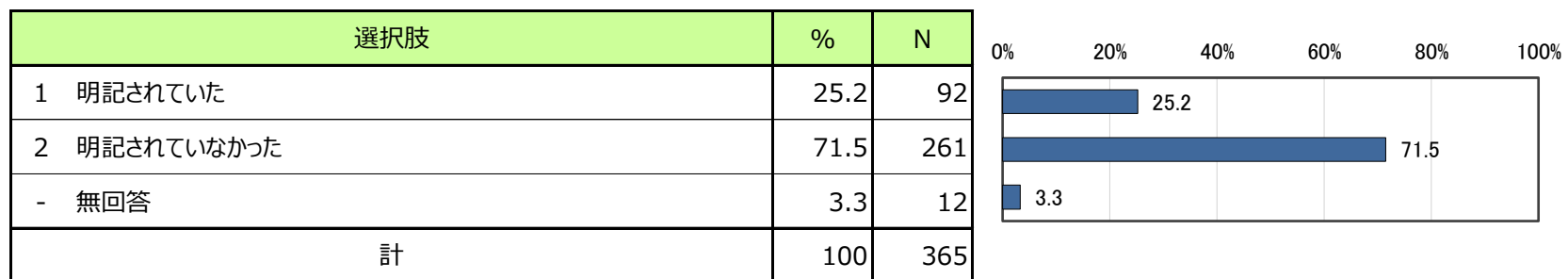


問27-1（問27でいずれかで「責任範囲が明記されていた」と回答した場合）情報セキュリティに関する委託先の責任範囲についてどのように明示されていましたか。当てはまるものを全てお選びください。（いくつでも）

N= 224

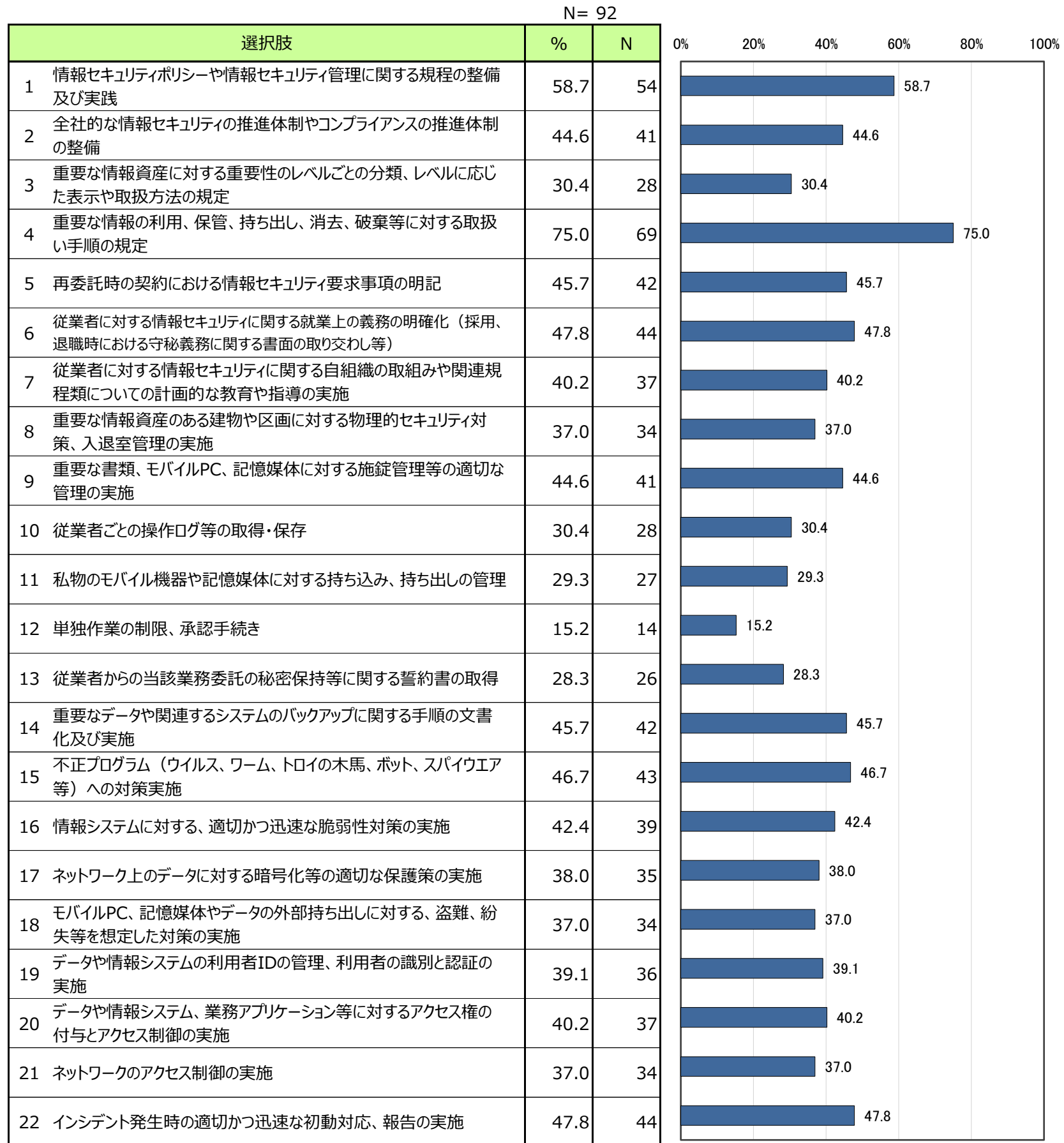


問28 当該事例の契約関連文書（仕様書、契約書等）では、委託先が実施すべき組織的な情報セキュリティ対策が明記されていましたか。（ひとつだけ）

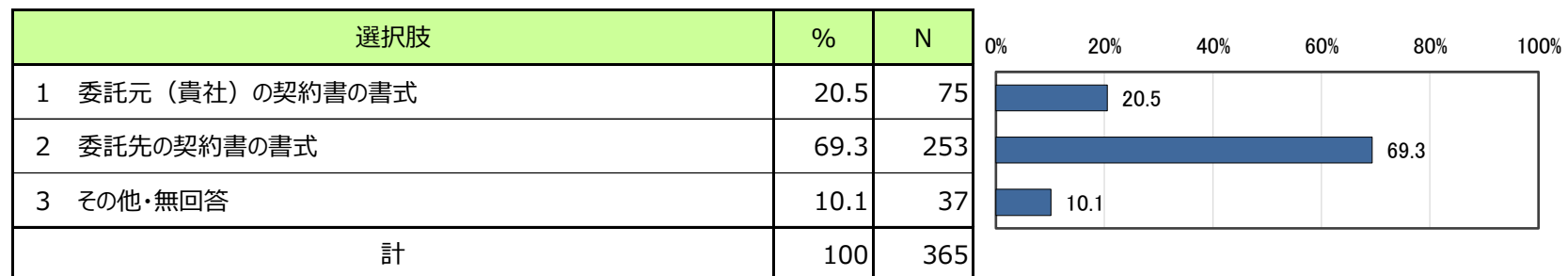


付録3-1 アンケート調査 単純集計結果（委託元調査）

問28-1（問28で「明記されていた」と回答した場合）委託先が実施すべき組織的な情報セキュリティ対策として明記されていたものを全てお選びください。（いくつでも）



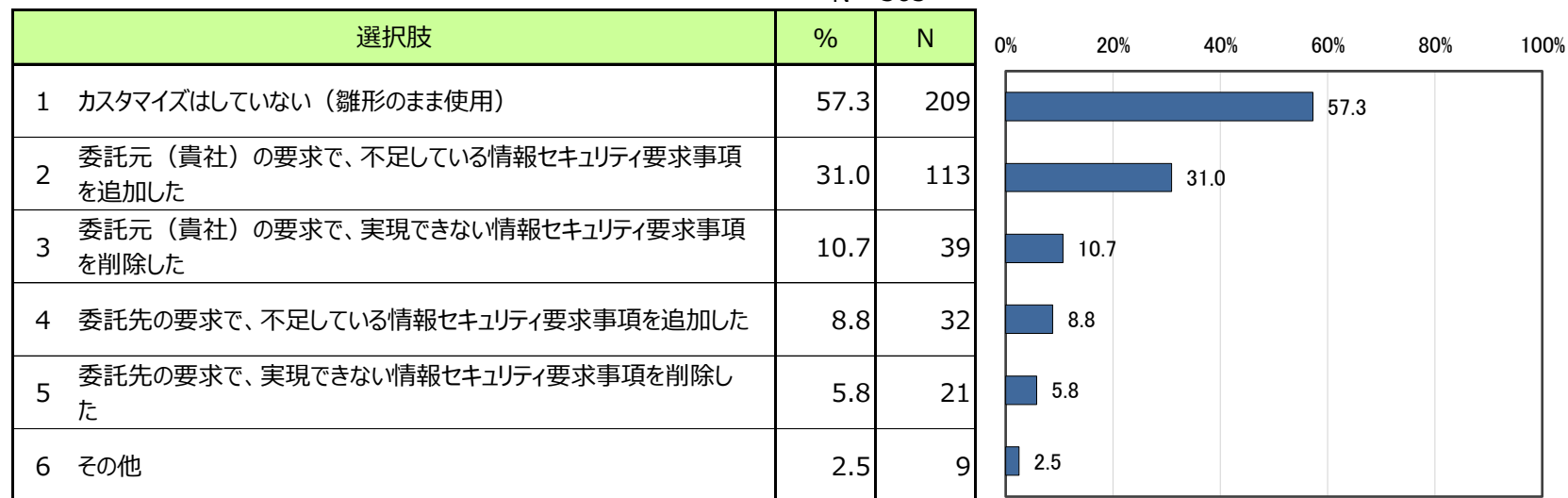
問29 当該事例において使用した契約書の書式は委託元のものですか、委託先のものですか。当てはまるものをお選びください。（ひとつだけ）



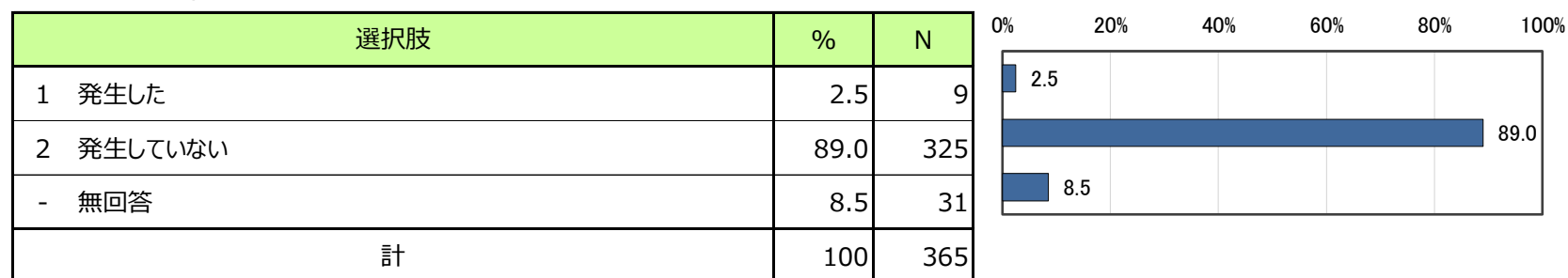
付録3-1 アンケート調査 単純集計結果（委託元調査）

問30 当該事例において使用した契約書の書式は、対象業務の情報セキュリティ要求事項に合わせて、情報セキュリティに関する項目を追加したり、内容を修正したりするカスタマイズを行いましたか。当てはまるものをお選びください。（いくつでも）

N= 365



問31 当該事例において、業務委託契約における情報セキュリティ要求項目に関し、委託先との間で何らかのトラブルが発生したことがありますか。当てはまるものをお選びください。（ひとつだけ）

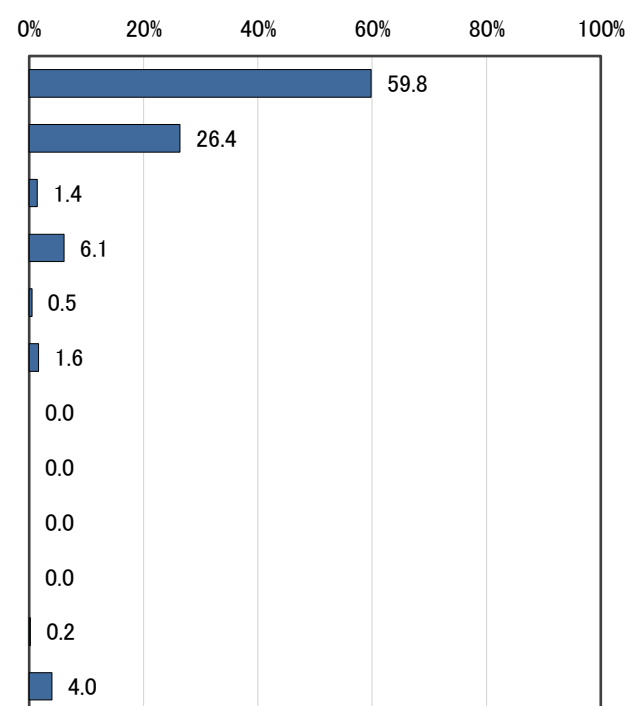


ITシステム・サービスの業務委託に関する調査 委託先調査 単純集計結果

回答組織数 = 428
回答事例数 = 407

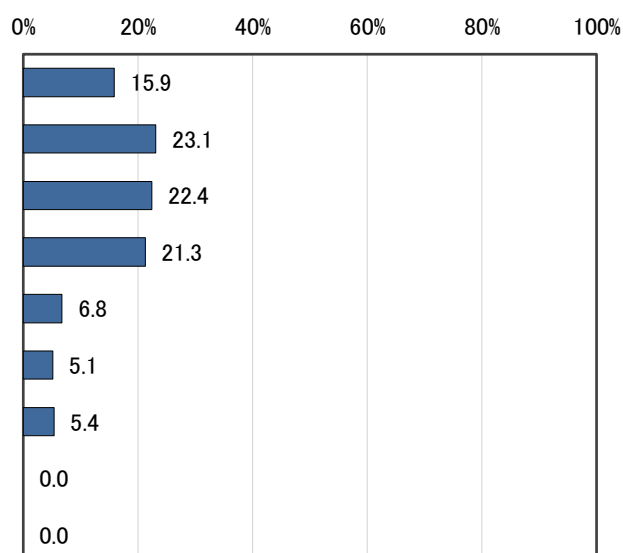
S1 貴社の主な業種をお選びください。（ひとつだけ）

選択肢	%	N
1 ソフトウェア業	59.8	256
2 情報処理サービス業	26.4	113
3 情報提供サービス業	1.4	6
4 その他の情報サービス業	6.1	26
5 国内・国際電気通信業	0.5	2
6 電気通信に付帯するサービス業	1.6	7
7 民生用電気機械器具製造業	0.0	0
8 電子計算機・同付属装置製造業	0.0	0
9 工業計器製造業	0.0	0
10 発電機・電動機・その他の回転電気機械製造業	0.0	0
11 電気機械製造業	0.2	1
12 その他	4.0	17
計	100	428



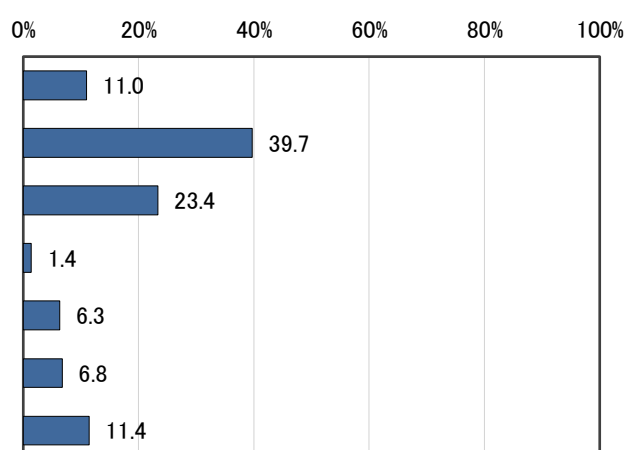
S2 貴社の総従業員数（正社員、準社員等を含む）をお選びください。（ひとつだけ）

選択肢	%	N
1 ~20名	15.9	68
2 21名~50名	23.1	99
3 51名~100名	22.4	96
4 101名~300名	21.3	91
5 301名~500名	6.8	29
6 501名~1,000名	5.1	22
7 1,001名~5,000名	5.4	23
8 5,001名~10,000名	0.0	0
9 10,001名以上	0.0	0
計	100	428



S3 ご回答者の所属部門をお選びください。複数の部門で回答された場合は、主に回答された部門をお選びください。（ひとつだけ）

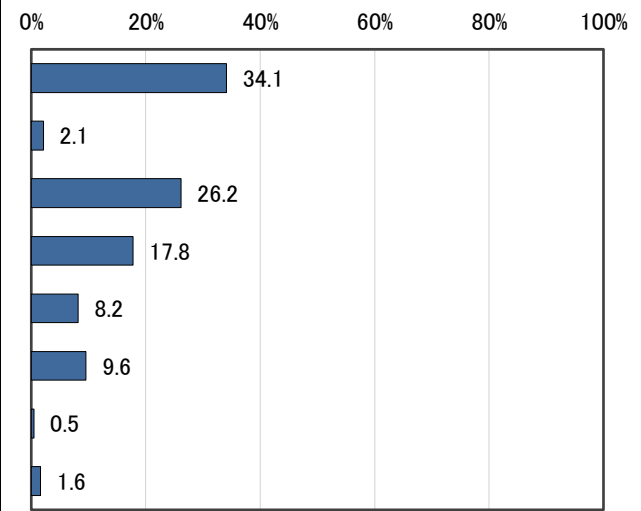
選択肢	%	N
1 営業部門	11.0	47
2 総務部門	39.7	170
3 情報システム部門・情報セキュリティ部門	23.4	100
4 法務部門	1.4	6
5 事業部門	6.3	27
6 品質・リスク管理部門	6.8	29
7 その他	11.4	49
計	100	428



付録3-2 アンケート調査 単純集計結果（委託先調査）

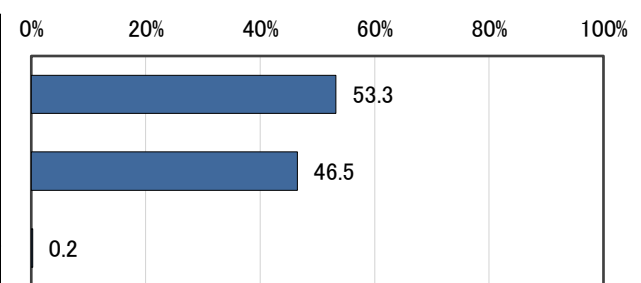
S4 ご回答者の役職をお選びください。（ひとつだけ）

選択肢	%	N
1 取締役・役員クラス	34.1	146
2 事業部長クラス	2.1	9
3 部長クラス	26.2	112
4 課長クラス	17.8	76
5 係長・主任クラス	8.2	35
6 一般社員	9.6	41
7 専門職	0.5	2
8 その他	1.6	7
計	100	428



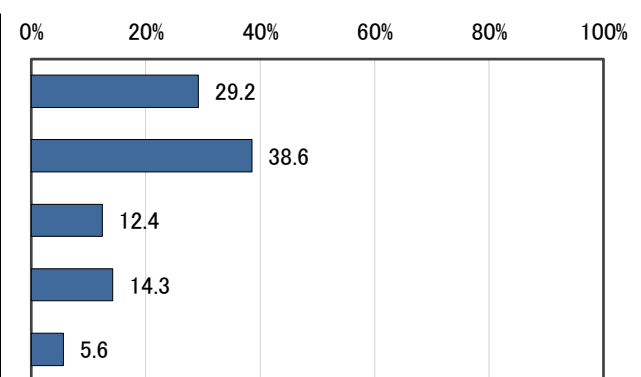
S5 ITシステム・サービスの取引において、貴社の位置付けとして主要なものをお選びください。（ひとつだけ）

選択肢	%	N
1 元請け（プライムベンダー）	53.3	228
2 二次請け以降	46.5	199
- 無回答	0.2	1
計	100	428



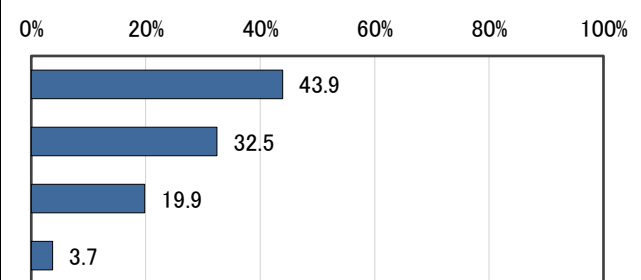
S6 貴社において、昨年度（2017年度）、直接取引のあった委託元の社数をお選びください（ひとつだけ）

選択肢	%	N
1 1社～10社	29.2	125
2 11社～50社	38.6	165
3 51社～100社	12.4	53
4 101社以上	14.3	61
5 わからない・無回答	5.6	24
計	100	428



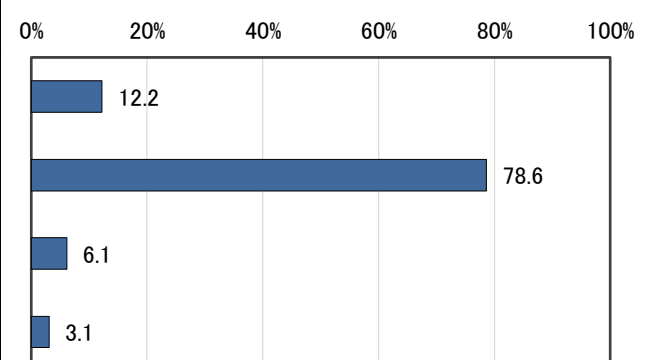
問1 貴社には、情報セキュリティ要求事項を含んだ契約書の雛形がありますか。当てはまるものをお選びください。（ひとつだけ）

選択肢	%	N
1 サービスの種類に係わらない統一の雛型がある	43.9	188
2 サービスの種類に応じた複数の雛型がある	32.5	139
3 雛型はなく、過去の契約書を流用する等して都度作成している	19.9	85
4 その他	3.7	16
計	100	428



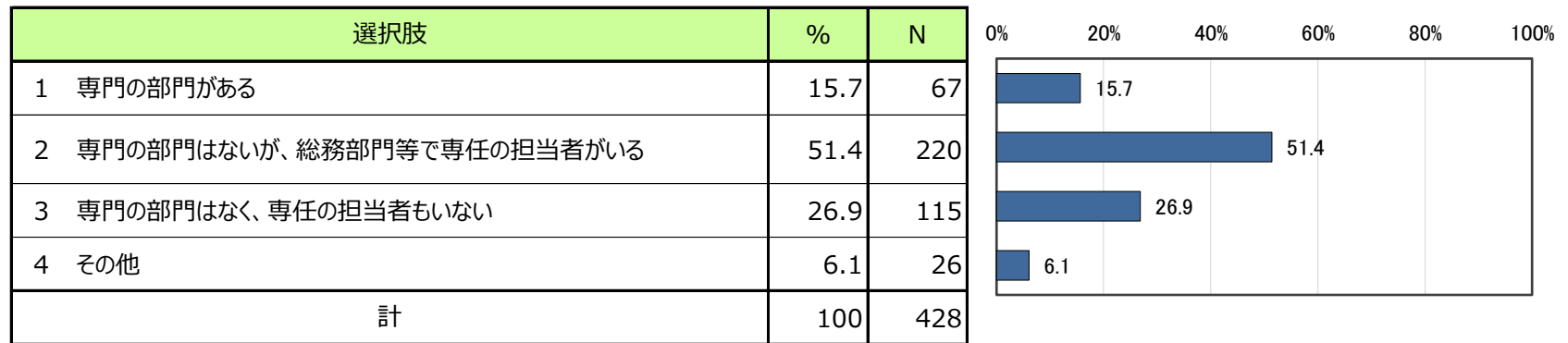
問1-1（問1で1または2の「雛型がある」を選んだ場合）契約書に記載する情報セキュリティ要求事項の変更は認められていますか。（ひとつだけ）

選択肢	%	N
1 情報セキュリティ要求事項の内容は変更できない	12.2	40
2 管理者（法務部門や総務部門の担当者等）からの承認が得られれば、情報セキュリティ要求事項の内容は変更できる	78.6	257
3 情報セキュリティ要求事項の内容は、営業担当者等の委託元との窓口の判断だけで変更できる	6.1	20
4 その他・無回答	3.1	10
計	100	327



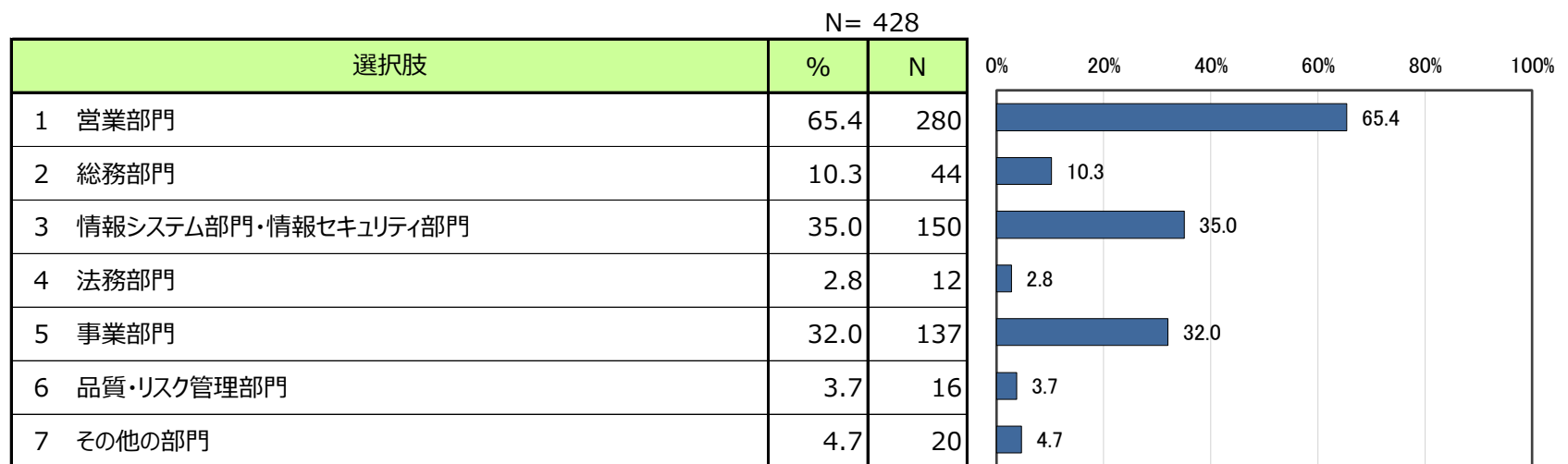
付録3-2 アンケート調査 単純集計結果（委託先調査）

問2 貴社では、受託業務ごとに契約関連文書（契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けていますか。（ひとつだけ）

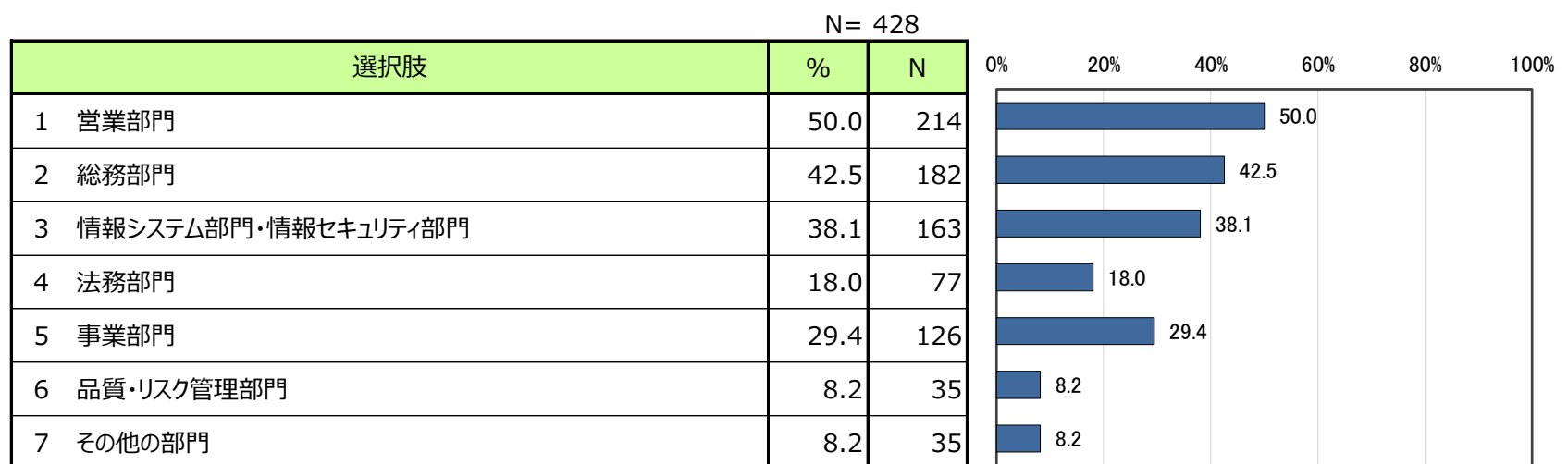


問3 受託業務における情報セキュリティ対策について、役割ごとに所管（関与）する部門をお選びください。1つの役割に対して複数の部門が関与する場合は、関与する部門全てをお選びください。（それぞれいくつでも）

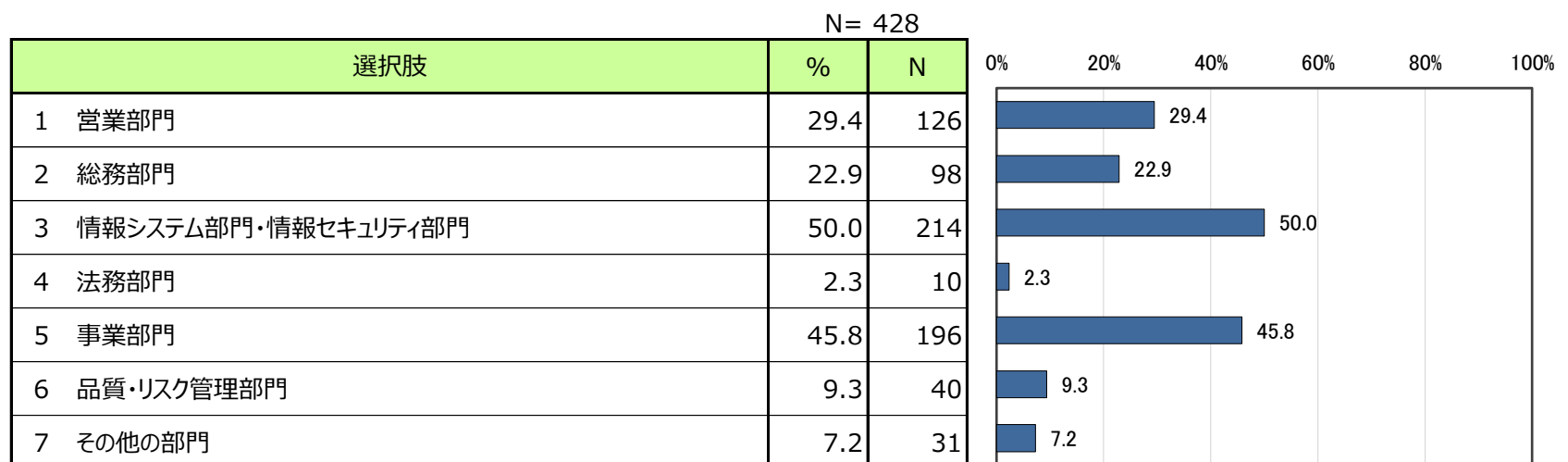
a. 提案時の情報セキュリティ対策の説明



b. 情報管理・情報セキュリティに関する契約内容確認

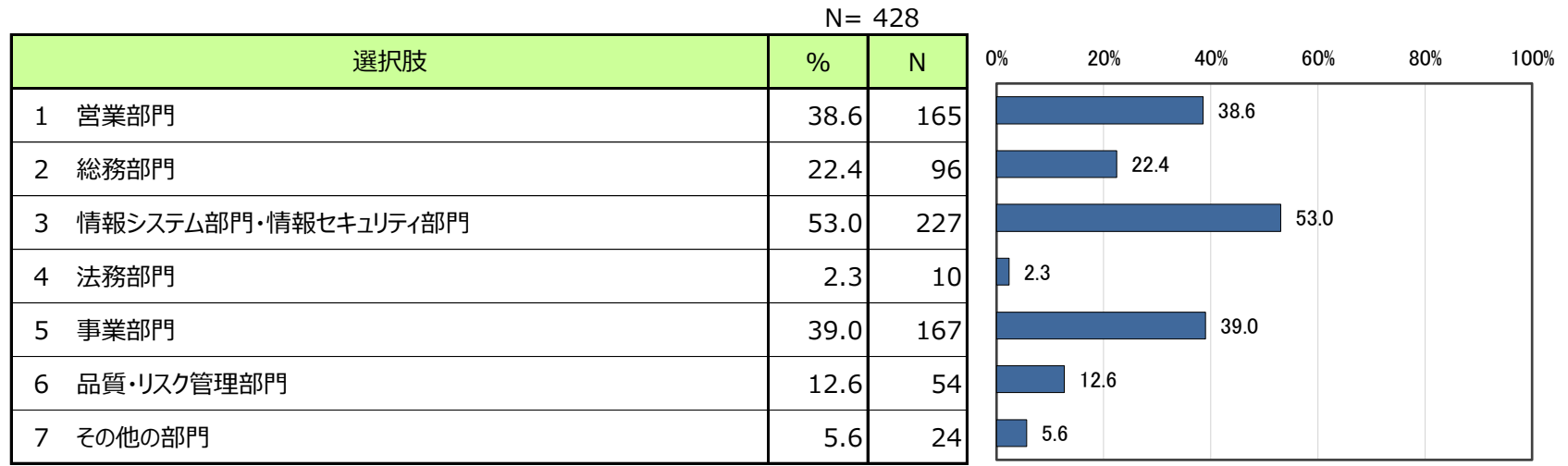


c. 受託業務で扱う情報資産の厳格な管理（授受から廃棄等の一連のプロセス）

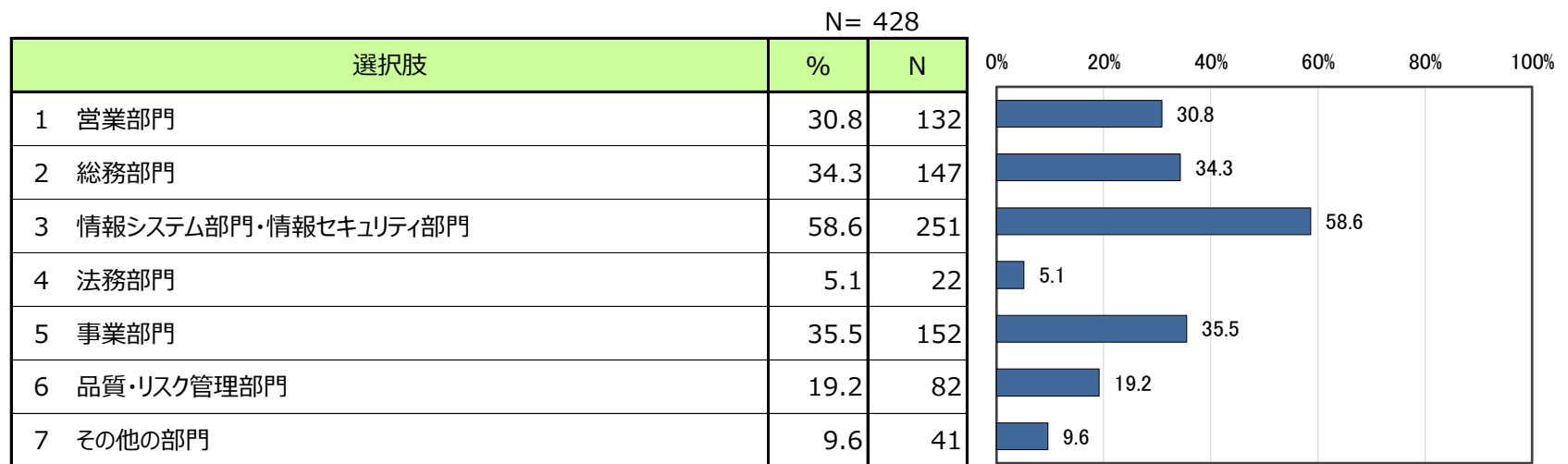


付録3-2 アンケート調査 単純集計結果（委託先調査）

d. 委託元による情報セキュリティ対策の実施状況の確認への対応

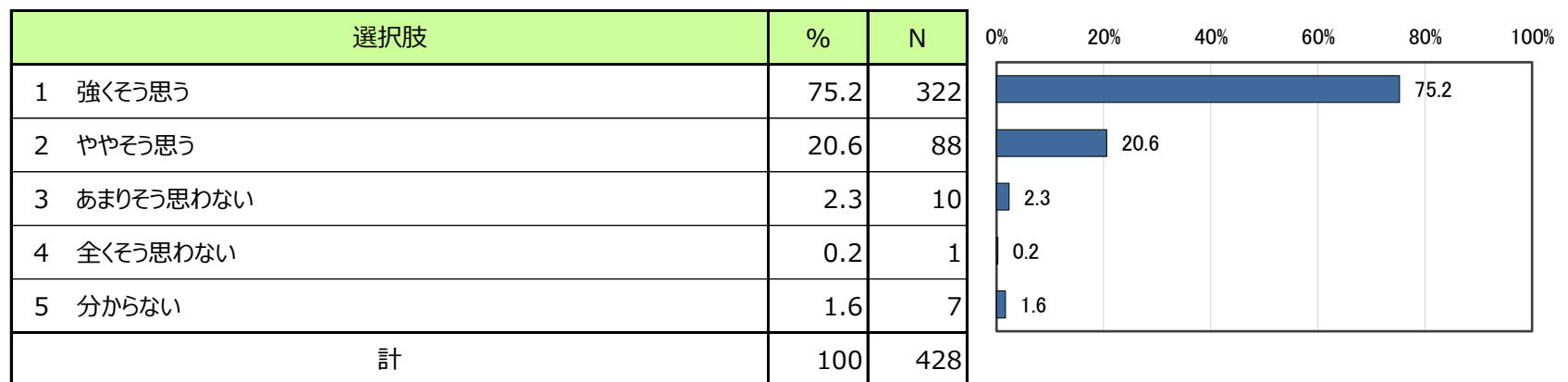


e. インシデントに対する対応体制の整備

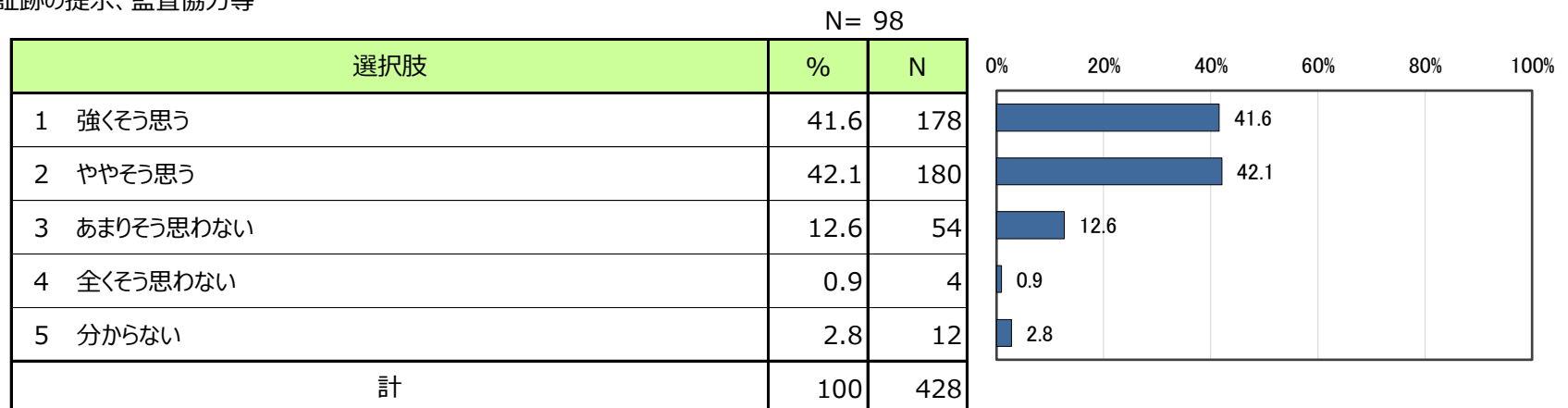


問4 以下の情報セキュリティ要求事項に関し、受託業務の契約において、委託先（貴社）の責任を明確にしたいと思う度合いについて、当てはまるものをお選びください。（それぞれひとつずつ）

a. 秘密保持



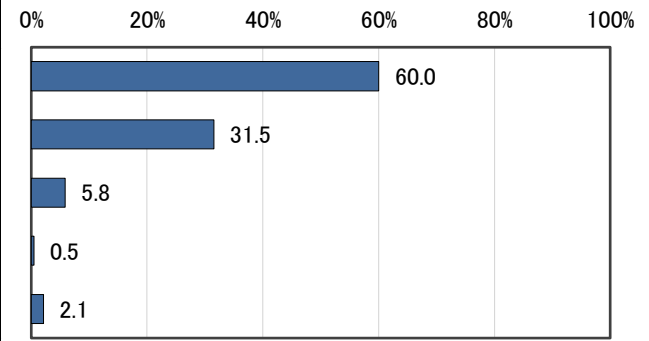
b. 証跡の提示、監査協力等



付録3-2 アンケート調査 単純集計結果（委託先調査）

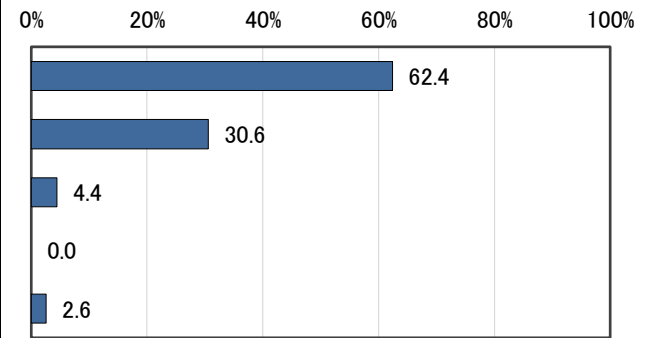
c. 情報セキュリティに関する契約内容に違反した場合の措置

選択肢	%	N
1 強く思う	60.0	257
2 やや思う	31.5	135
3 あまりそう思わない	5.8	25
4 全くそう思わない	0.5	2
5 分からない	2.1	9
計	100	428



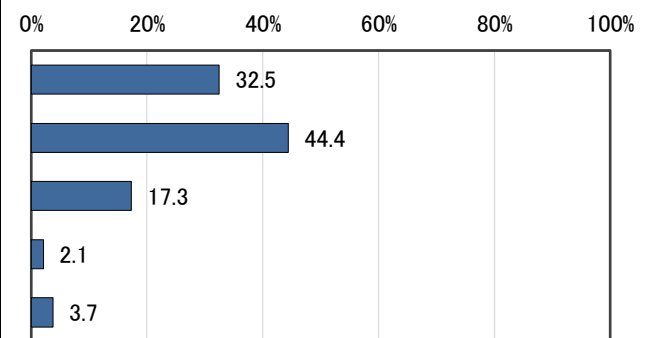
d. インシデントが発生した場合の対応

選択肢	%	N
1 強く思う	62.4	267
2 やや思う	30.6	131
3 あまりそう思わない	4.4	19
4 全くそう思わない	0.0	0
5 分からない	2.6	11
計	100	428



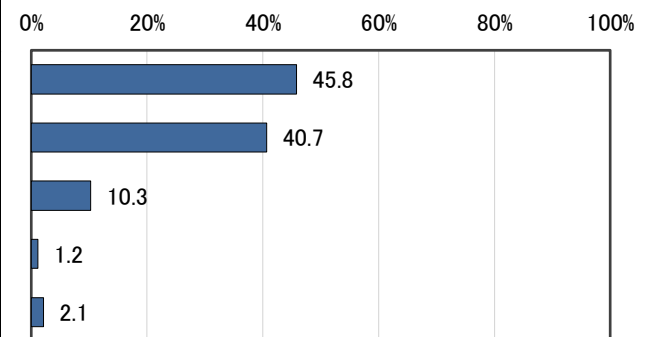
e. 可用性（稼働率の水準、目標復旧時間等）

選択肢	%	N
1 強く思う	32.5	139
2 やや思う	44.4	190
3 あまりそう思わない	17.3	74
4 全くそう思わない	2.1	9
5 分からない	3.7	16
計	100	428



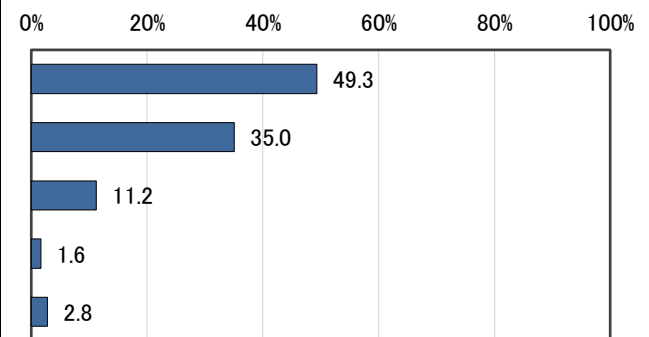
f. 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応

選択肢	%	N
1 強く思う	45.8	196
2 やや思う	40.7	174
3 あまりそう思わない	10.3	44
4 全くそう思わない	1.2	5
5 分からない	2.1	9
計	100	428



g 再委託の禁止または制限

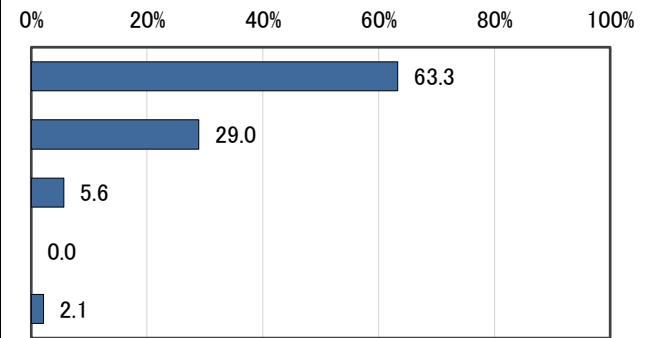
選択肢	%	N
1 強く思う	49.3	211
2 やや思う	35.0	150
3 あまりそう思わない	11.2	48
4 全くそう思わない	1.6	7
5 分からない	2.8	12
計	100	428



付録3-2 アンケート調査 単純集計結果（委託先調査）

h 契約終了後の情報資産の扱い（返却、消去、廃棄等）

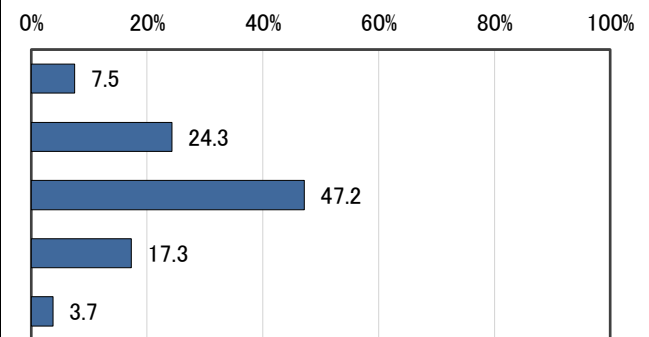
選択肢	%	N
1 強く思う	63.3	271
2 やや思う	29.0	124
3 あまり思わない	5.6	24
4 全く思わない	0.0	0
5 分からない	2.1	9
計	100	428



問5 受託業務の契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）が明確にならない理由は何だと思いますか。以下の項目について、理由としての当てはまりの度合いをお選びください。（それぞれひとつずつ）

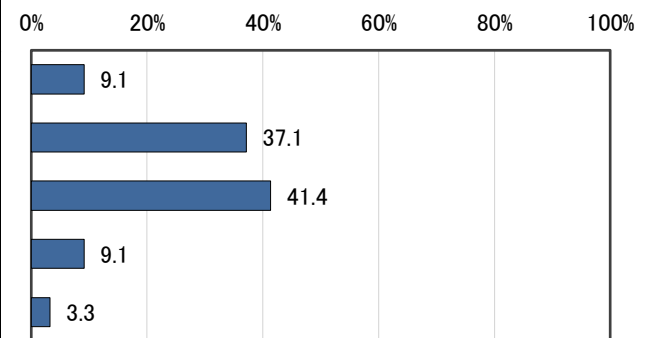
a. 自組織の契約関連文書（契約書等）の雛形に情報セキュリティ要求事項の記載がないため、何を決めたらいいのかわからない

選択肢	%	N
1 強く思う	7.5	32
2 やや思う	24.3	104
3 あまり思わない	47.2	202
4 全く思わない	17.3	74
5 分からない	3.7	16
計	100	428



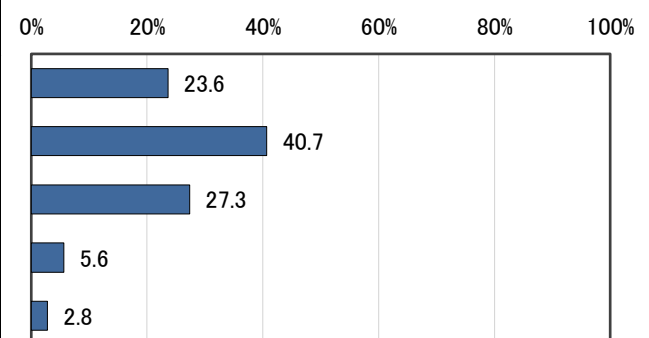
b. 委託元の情報セキュリティに関する専門知識・スキルが不足している

選択肢	%	N
1 強く思う	9.1	39
2 やや思う	37.1	159
3 あまり思わない	41.4	177
4 全く思わない	9.1	39
5 分からない	3.3	14
計	100	428



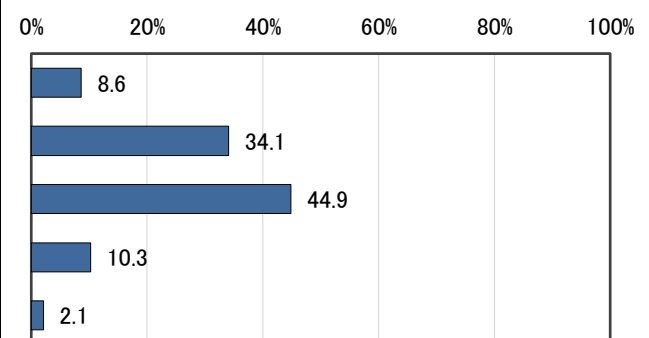
c. 責任範囲を明確にすることで、見積りに反映せざるを得ないが、委託元にはコスト増を受け入れてもらえない

選択肢	%	N
1 強く思う	23.6	101
2 やや思う	40.7	174
3 あまり思わない	27.3	117
4 全く思わない	5.6	24
5 分からない	2.8	12
計	100	428



d. 責任範囲を明確にすることで、自組織内の関係者の心理的負担が増える

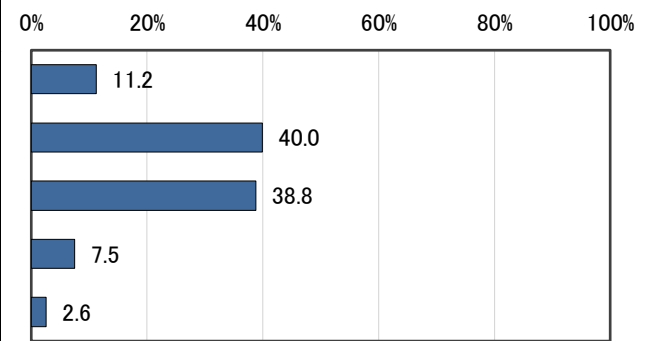
選択肢	%	N
1 強く思う	8.6	37
2 やや思う	34.1	146
3 あまり思わない	44.9	192
4 全く思わない	10.3	44
5 分からない・無回答	2.1	9
計	100	428



付録3-2 アンケート調査 単純集計結果（委託先調査）

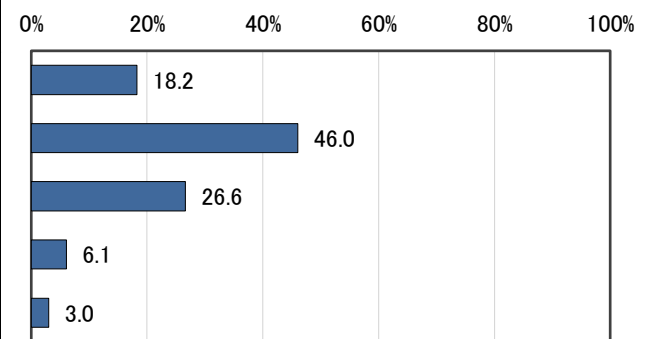
e. 責任範囲を明確にすることで、調整に時間がかかり契約が遅くなる（工期圧迫、機会損失等）

選択肢	%	N
1 強く思う	11.2	48
2 やや思う	40.0	171
3 あまり思わない	38.8	166
4 全く思わない	7.5	32
5 分からない	2.6	11
計	100	428



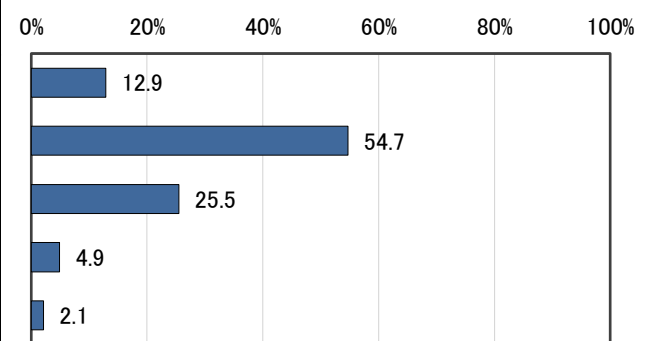
f. 契約時点では業務要件自体が未確定であることが多く、情報セキュリティ要求事項のみを明確にすることができない。

選択肢	%	N
1 強く思う	18.2	78
2 やや思う	46.0	197
3 あまり思わない	26.6	114
4 全く思わない	6.1	26
5 分からない	3.0	13
計	100	428



g. 同じ顧客と継続して契約している業務が多く、責任範囲を見直す機会がない

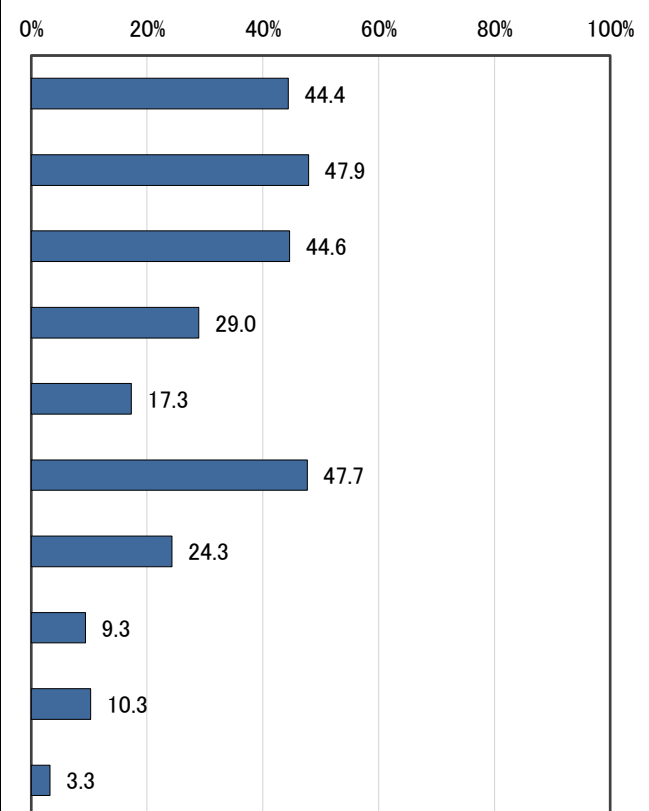
選択肢	%	N
1 強く思う	12.9	55
2 やや思う	54.7	234
3 あまり思わない	25.5	109
4 全く思わない	4.9	21
5 分からない	2.1	9
計	100	428



問6 受託業務の契約にあたり、情報セキュリティ要求事項に関して、委託元と委託先の責任範囲に曖昧さが残る場合に、貴社独自に取られている対策はありますか。（いくつでも）

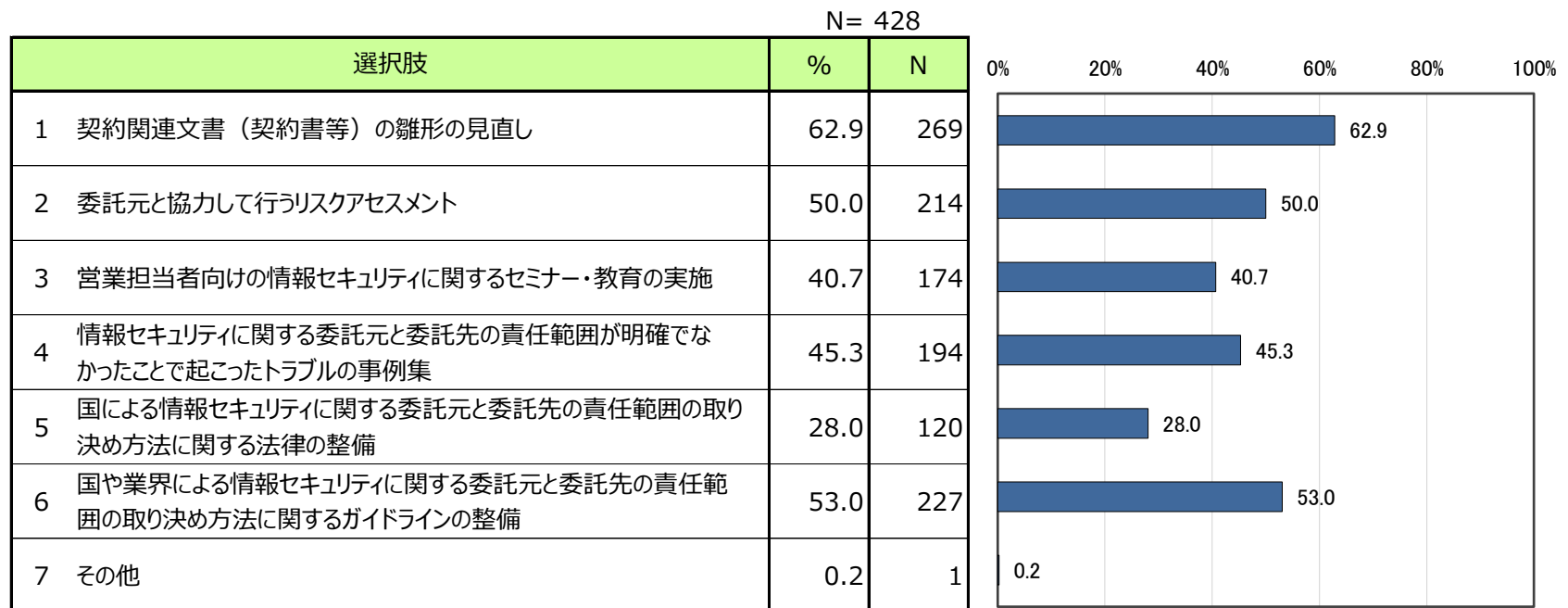
N= 428

選択肢	%	N
1 当該受託業務についてのリスクアセスメントを行い、想定されるリスクを洗い出す	44.4	190
2 委託元の提示する条件で受注してよいか、社内で第三者部門や上位責任者が参加する審査を行う	47.9	205
3 請負契約ではなく準委任契約や多段階契約等、責任が限定的になるように契約の方法を変える	44.6	191
4 委託元との情報セキュリティに関する意見交換の場を設定する	29.0	124
5 サイバー保険への加入により、いざという時の経済的影響を最小限にする	17.3	74
6 委託元との協議内容をできるだけ詳細に文書に記録して残すようにする	47.7	204
7 サイバー攻撃や脆弱性の最新情報入手し、当該受託業務への影響がないかを監視する	24.3	104
8 委託元と事例の共有や合同訓練等インシデントに備えた準備を行う	9.3	40
9 他部署や他社からの支援体制を構築しておく	10.3	44
10 その他	3.3	14

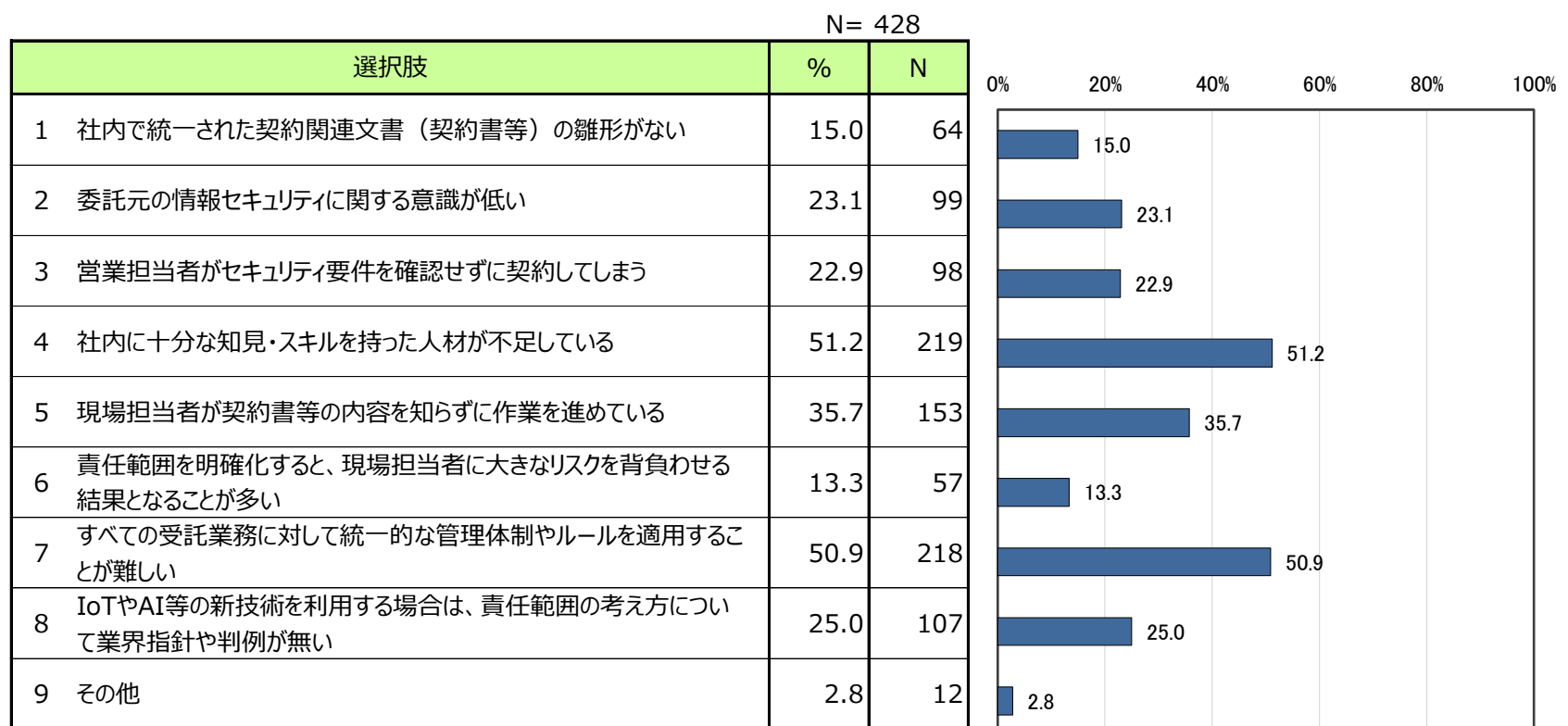


付録3-2 アンケート調査 単純集計結果（委託先調査）

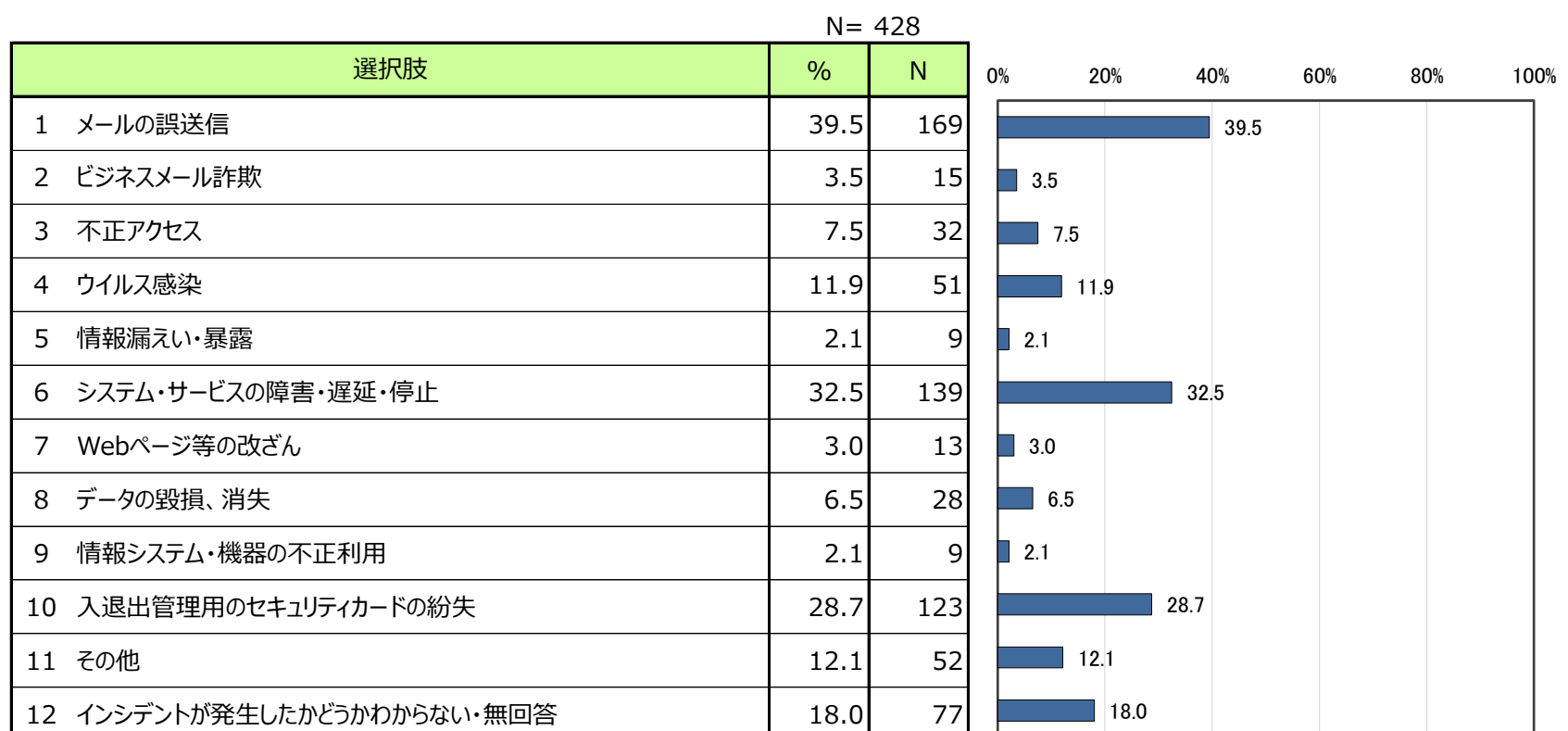
問7 受託業務の契約において、情報セキュリティに関する委託元と委託先の責任範囲（責任分界点）を明確にするためには、どのようなことが有効だと考えていますか。当てはまるものを全てお選びください。（いくつでも）



問8 受託業務の契約における情報セキュリティに関する責任範囲の明確化について、どのような点が課題だと考えますか。特に課題と考えるものを最大3つまでお選びください。



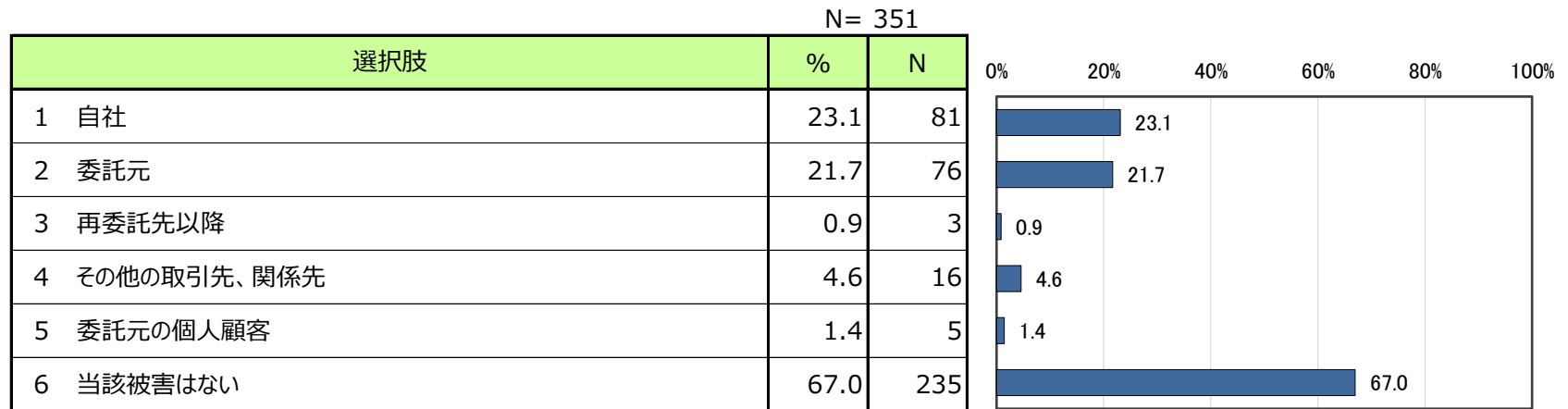
問9 過去3年間の受託業務において、以下のような事象が発生したことがありますか。当てはまるものを全てお選びください。（いくつでも）



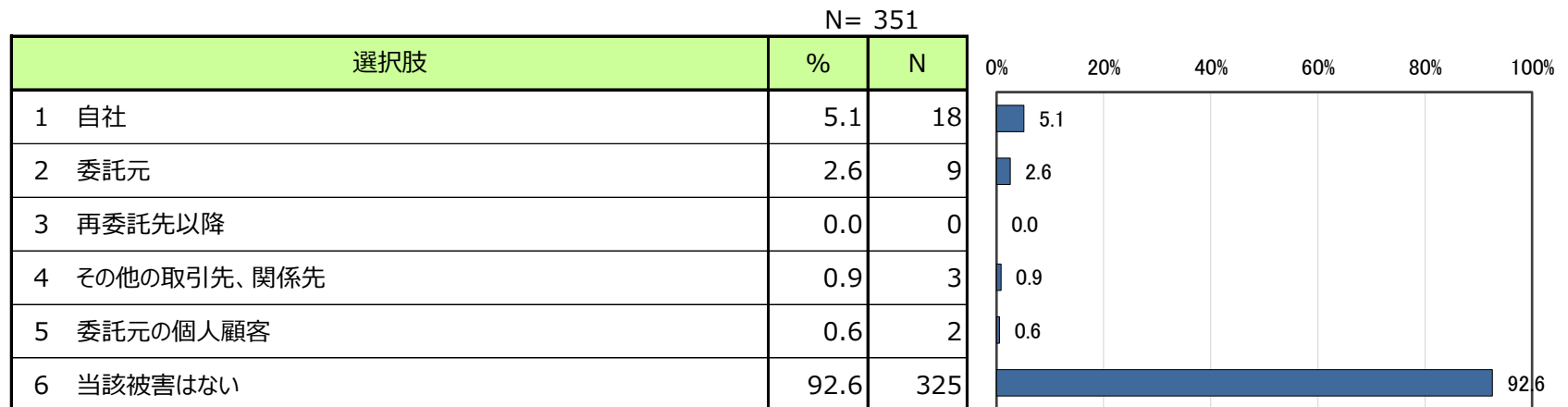
付録3-2 アンケート調査 単純集計結果（委託先調査）

問9-1（問9でいずれかの事象が発生したと回答した場合）発生した事象によって生じた被害の内容と、被害の影響が及んだ範囲（組織・個人）について、当てはまるものを全てお選びください。（それぞれいくつでも）

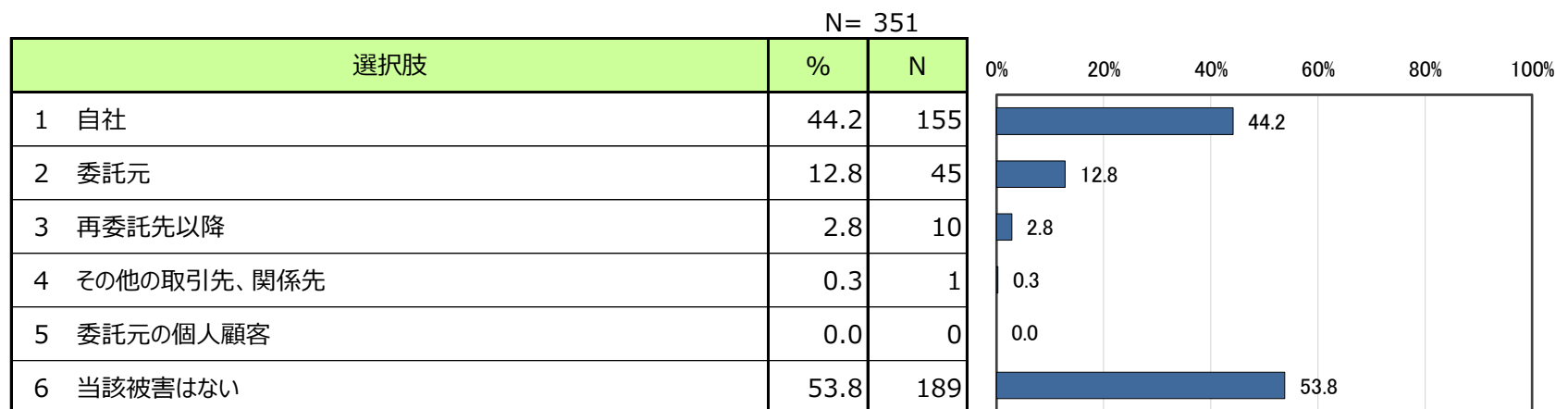
a. ITシステム・サービスの障害、遅延、停止による逸失利益



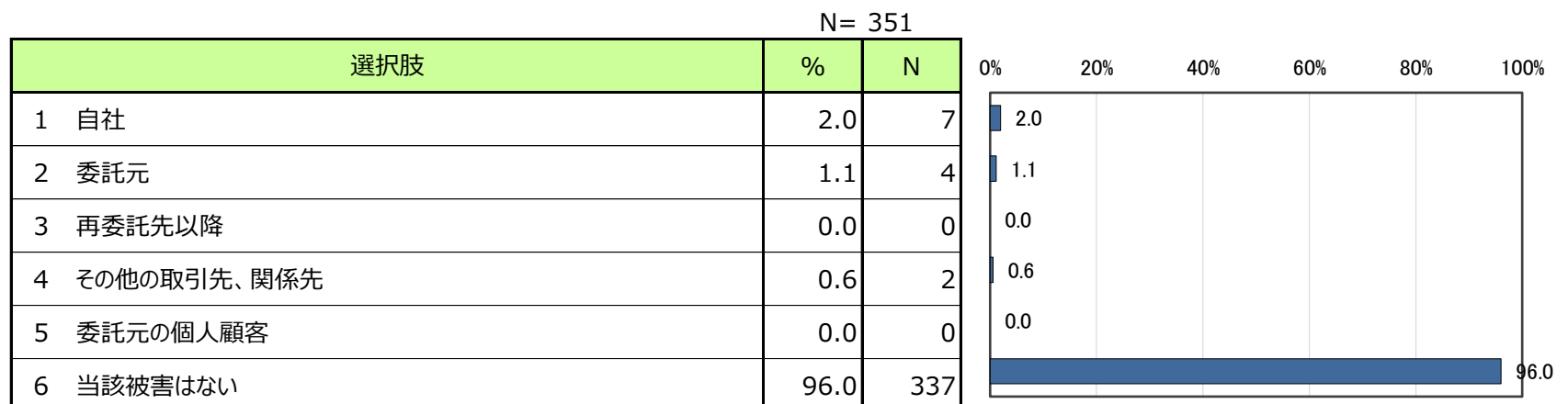
b. 個人顧客への賠償や法人取引先への補償負担



c. 原因調査・復旧にかかわる人件費等の経費負担



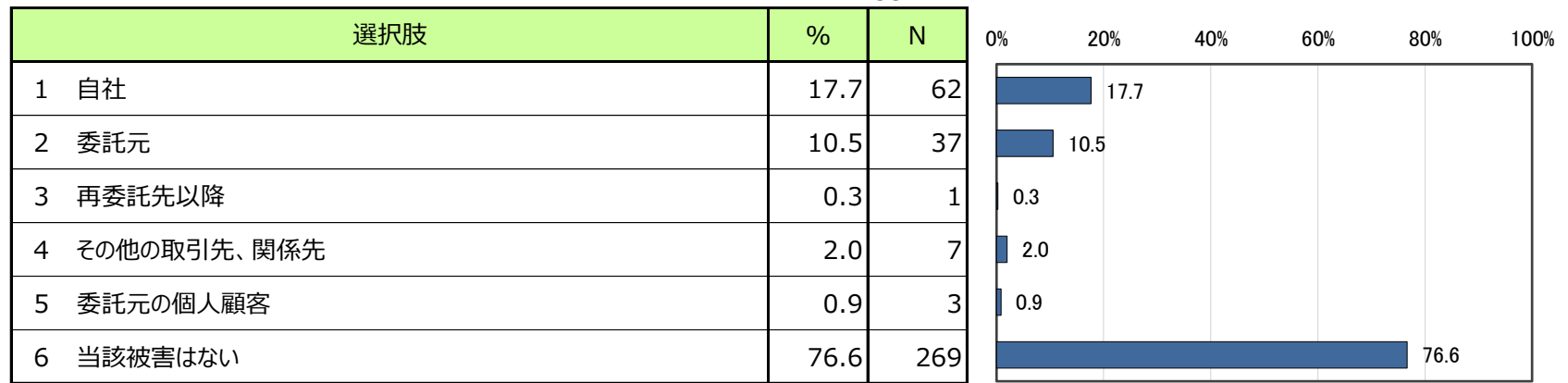
d. 裁判、調停等にかかわる人件費等の経費負担



付録3-2 アンケート調査 単純集計結果（委託先調査）

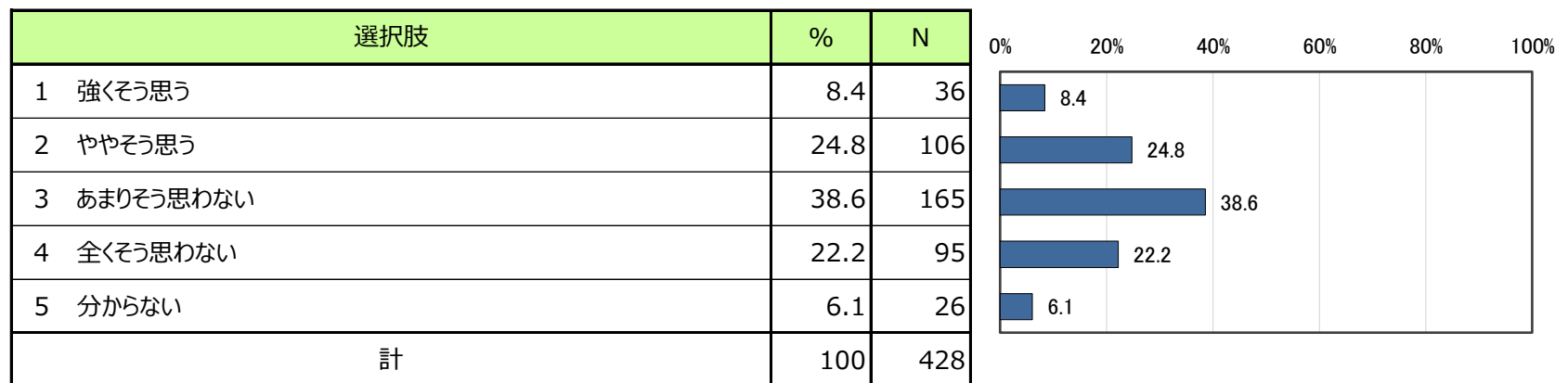
e. 個人顧客や法人取引先に対する信頼の失墜

N= 351

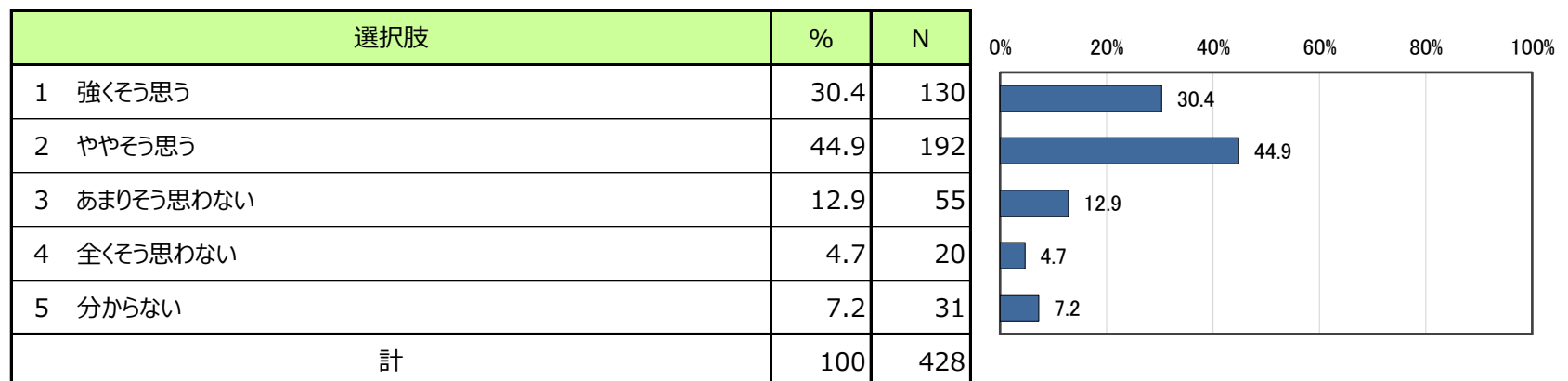


問10 納品後（契約期間外）のITシステムの情報セキュリティに関する未知の脆弱性（契約期間内に明らかでなかったもの）への対応について、どのように考えますか。以下の項目について、当てはまるものをお選びください。（それぞれひとつずつ）

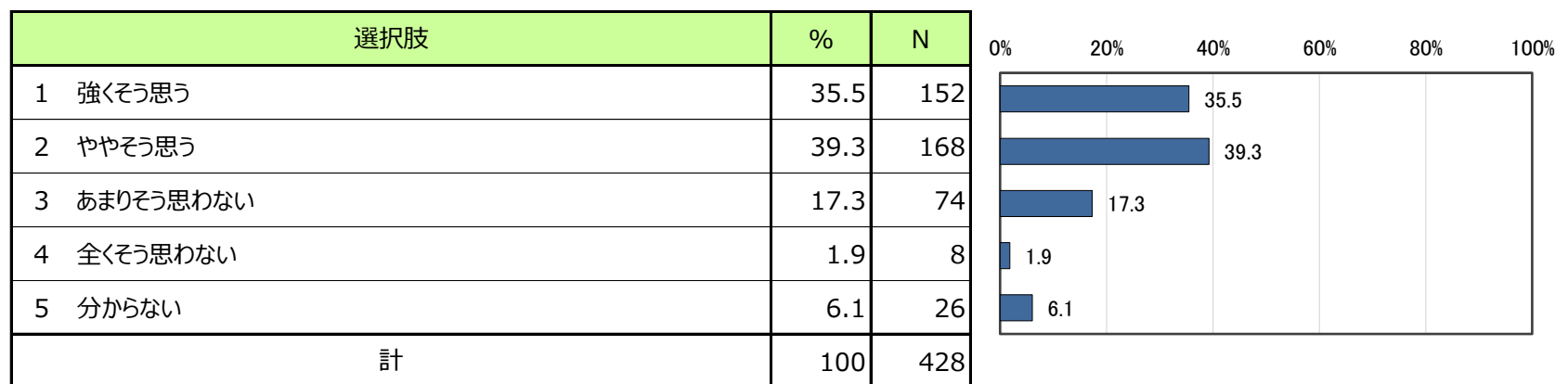
a. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託先（貴社）が責任を持つべきだ



b. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ



c. 納品後のITシステムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ

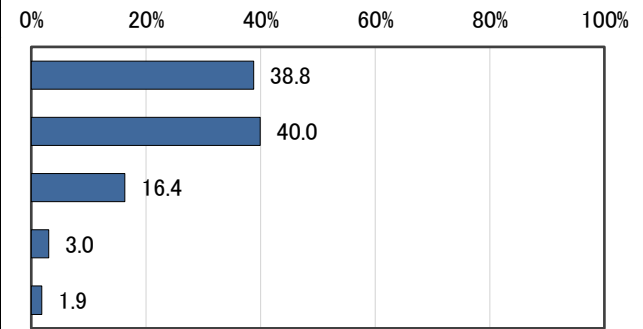


付録3-2 アンケート調査 単純集計結果（委託先調査）

問11 以下の情報セキュリティに関する事項について、懸念の度合いをお答えください。（それぞれひとつずつ）

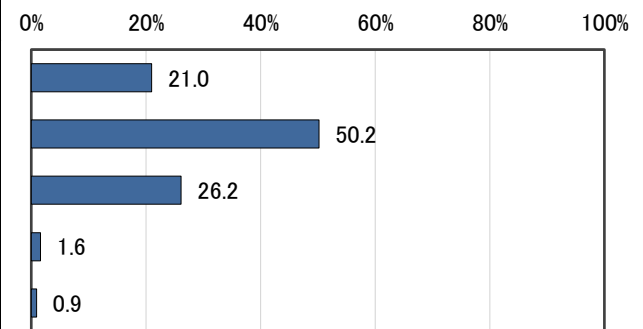
a. 顧客情報や業務情報（機密情報等）が盗まれる（流出する）

選択肢	%	N
1 非常に懸念している	38.8	166
2 ある程度懸念している	40.0	171
3 あまり懸念していない	16.4	70
4 全く懸念していない	3.0	13
5 分からない	1.9	8
計	100	428



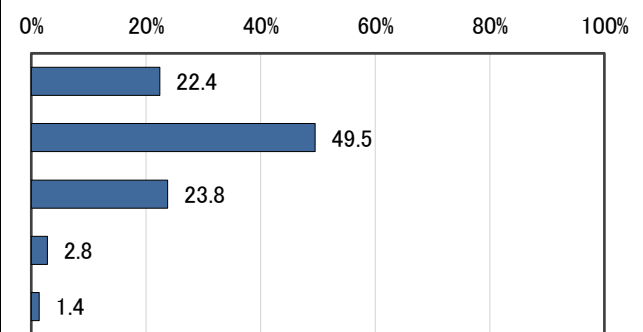
b. Webサイトや業務サーバの内容が改ざんされる

選択肢	%	N
1 非常に懸念している	21.0	90
2 ある程度懸念している	50.2	215
3 あまり懸念していない	26.2	112
4 全く懸念していない	1.6	7
5 分からない	0.9	4
計	100	428



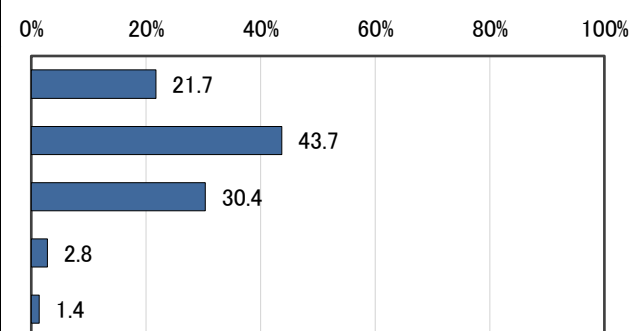
c. WebサイトやIoT機器が乗っ取られサイバー攻撃に悪用される

選択肢	%	N
1 非常に懸念している	22.4	96
2 ある程度懸念している	49.5	212
3 あまり懸念していない	23.8	102
4 全く懸念していない	2.8	12
5 分からない	1.4	6
計	100	428



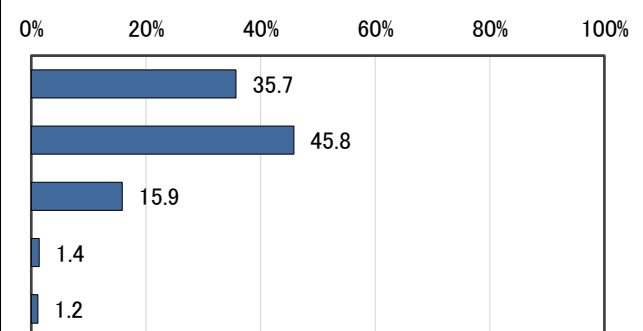
d. サイバー攻撃によってWebサイトの負荷が高まり利用できなくなる

選択肢	%	N
1 非常に懸念している	21.7	93
2 ある程度懸念している	43.7	187
3 あまり懸念していない	30.4	130
4 全く懸念していない	2.8	12
5 分からない	1.4	6
計	100	428



e. 業務サーバ、Webサーバがウイルスに感染する

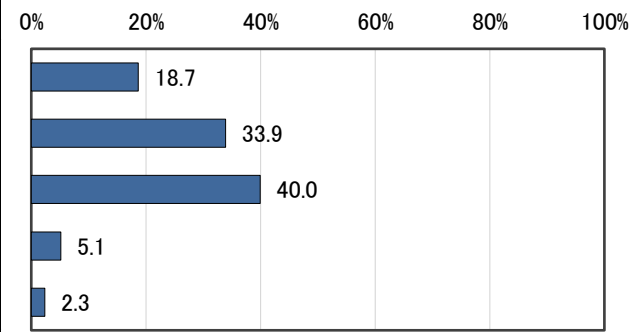
選択肢	%	N
1 非常に懸念している	35.7	153
2 ある程度懸念している	45.8	196
3 あまり懸念していない	15.9	68
4 全く懸念していない	1.4	6
5 分からない	1.2	5
計	100	428



付録3-2 アンケート調査 単純集計結果（委託先調査）

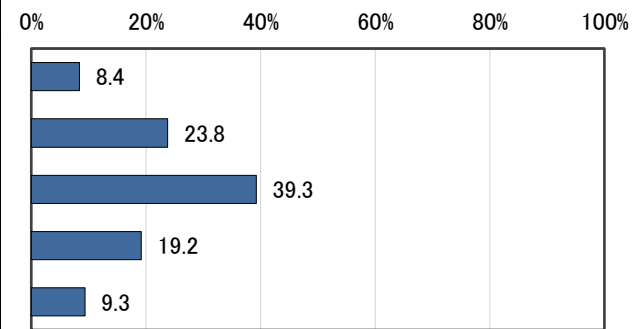
f. マスメディアで騒がれたりインターネット上で風評被害が広がる

選択肢	%	N
1 非常に懸念している	18.7	80
2 ある程度懸念している	33.9	145
3 あまり懸念していない	40.0	171
4 全く懸念していない	5.1	22
5 分からない	2.3	10
計	100	428



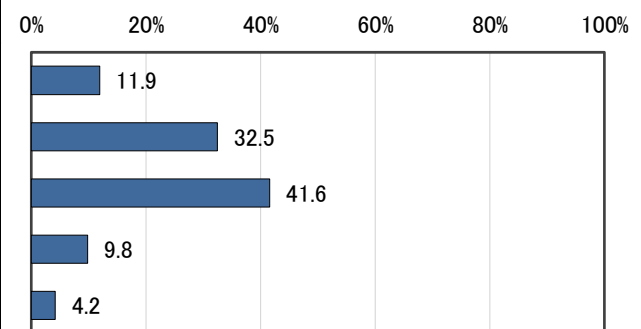
g. クラウドサービスのサーバが海外にある

選択肢	%	N
1 非常に懸念している	8.4	36
2 ある程度懸念している	23.8	102
3 あまり懸念していない	39.3	168
4 全く懸念していない	19.2	82
5 分からない	9.3	40
計	100	428



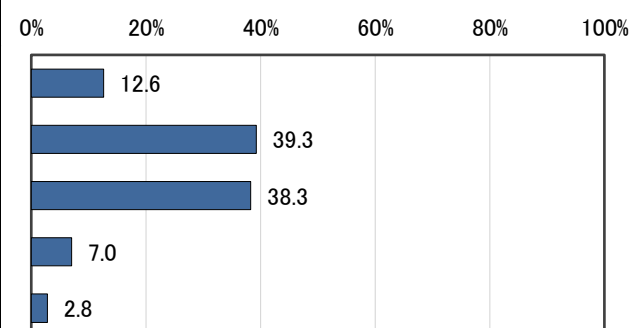
h. 再委託先で不正なプログラムや機能が埋め込まれる

選択肢	%	N
1 非常に懸念している	11.9	51
2 ある程度懸念している	32.5	139
3 あまり懸念していない	41.6	178
4 全く懸念していない	9.8	42
5 分からない	4.2	18
計	100	428



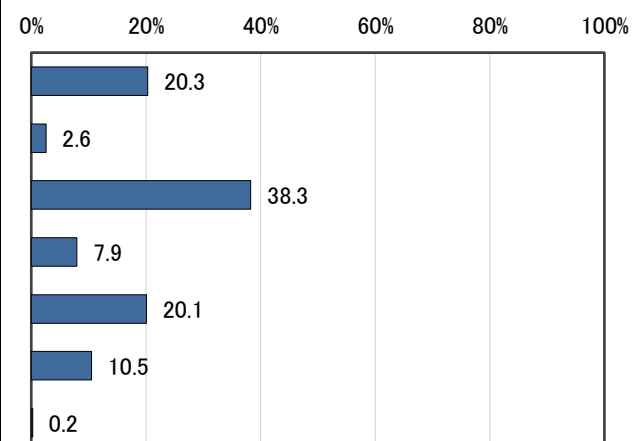
i. 取引先の脆弱性が原因で自社内に侵入される

選択肢	%	N
1 非常に懸念している	12.6	54
2 ある程度懸念している	39.3	168
3 あまり懸念していない	38.3	164
4 全く懸念していない	7.0	30
5 分からない	2.8	12
計	100	428



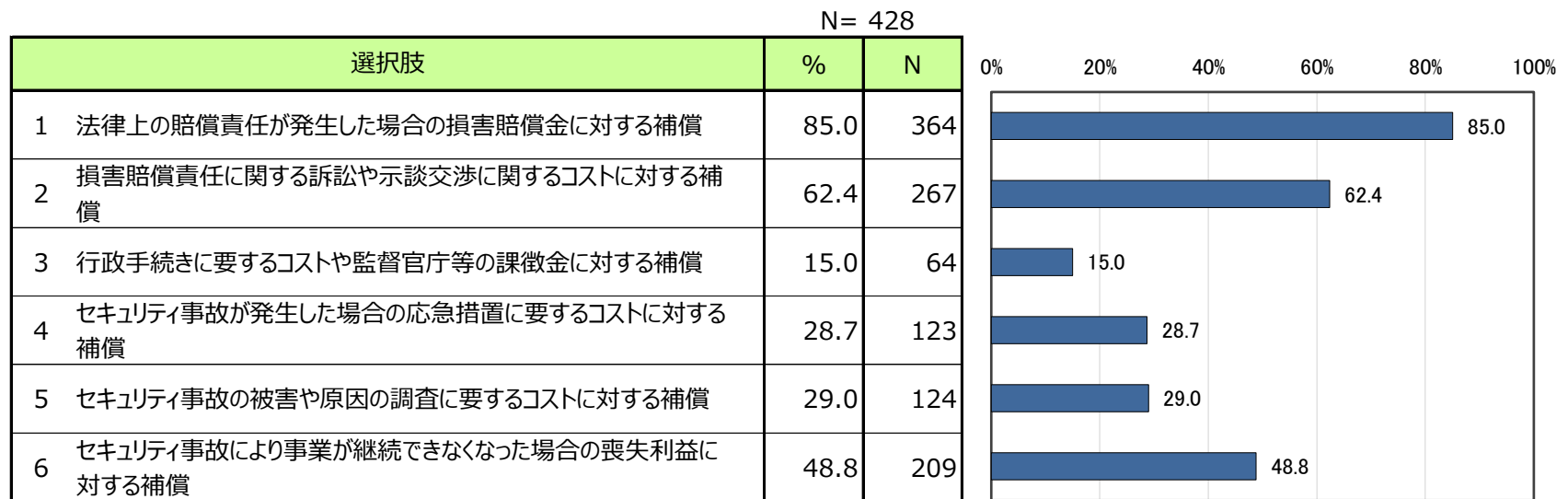
問12 情報セキュリティのリスク低減（移転）策のひとつにサイバー保険がありますが、サイバー保険をご存じですか。当てはまるものをお選びください。（ひとつだけ）

選択肢	%	N
1 既に参加済み	20.3	87
2 知っており、加入の予定がある	2.6	11
3 知っているが、加入の予定はない	38.3	164
4 知っているが、加入済みか予定があるかはわからない	7.9	34
5 詳細は知らないが、聞いたことはある	20.1	86
6 全く知らない	10.5	45
- 無回答	0.2	1
計	100	428

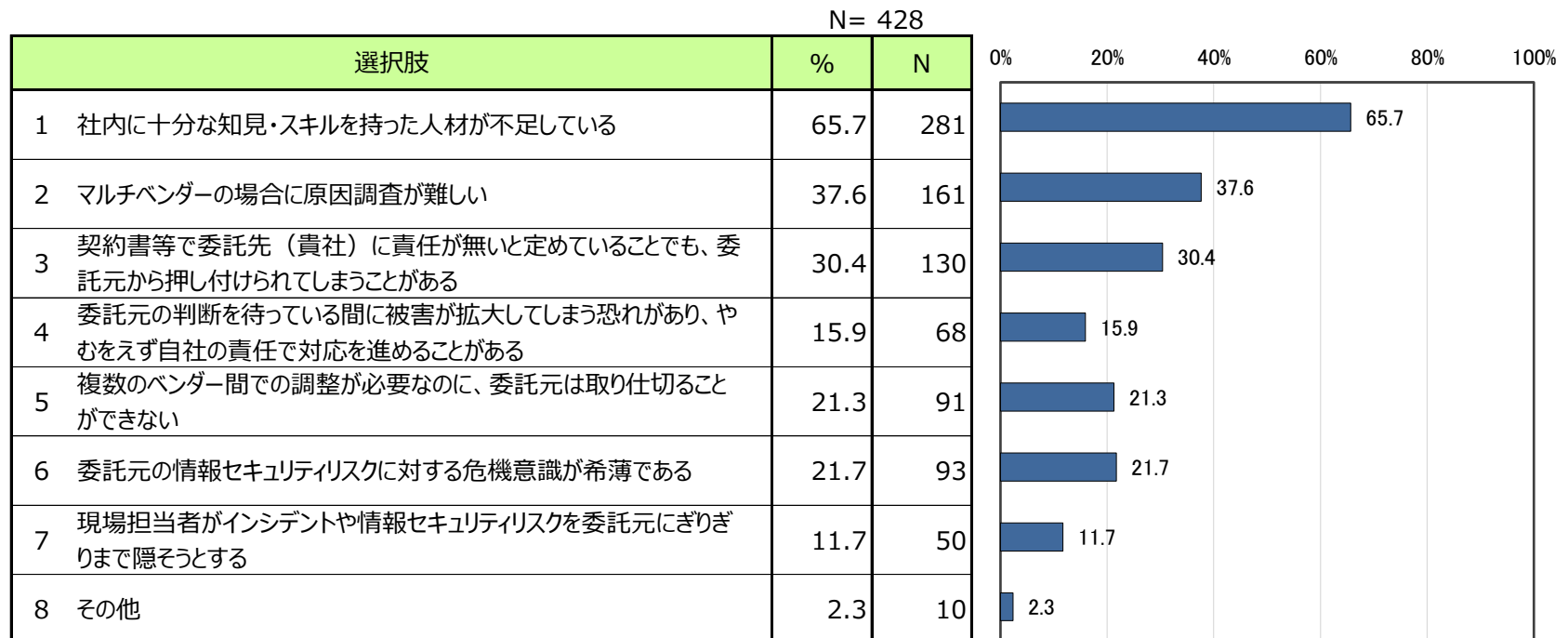


付録3-2 アンケート調査 単純集計結果（委託先調査）

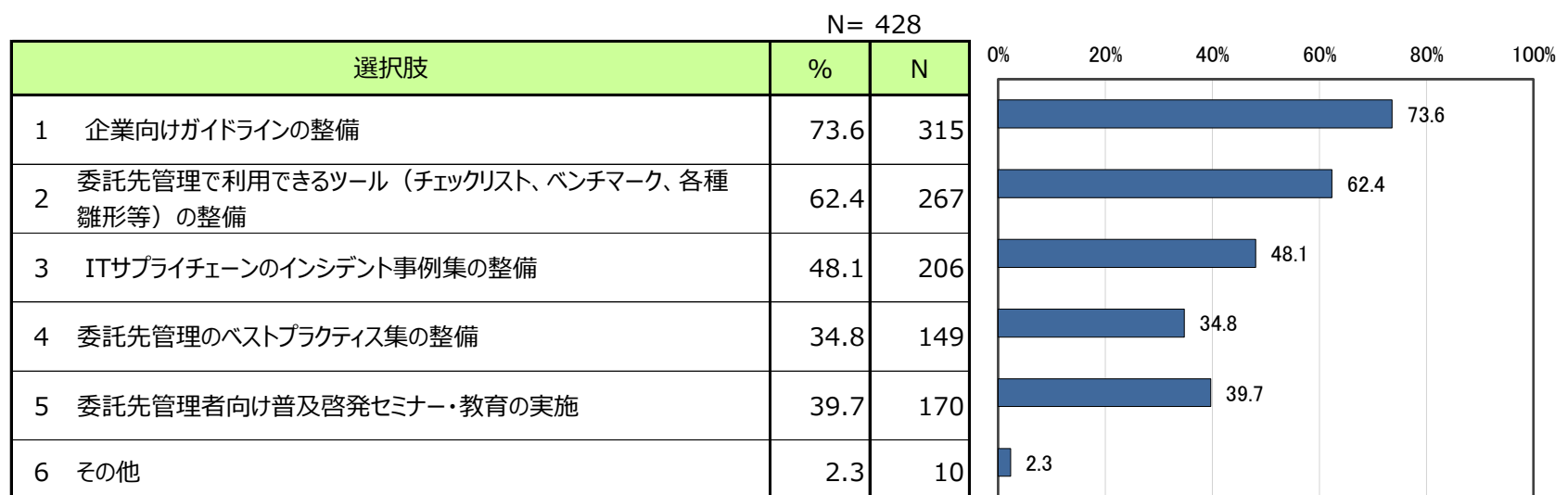
問13 以下にサイバー保険の代表的な補償内容をあげています。これらの補償内容のうち、どれが魅力的であると考えますか。特に魅力的であると考えるものを最大3つまでお選びください。



問14 インシデント対応やリスク対応において、どのような点が課題と考えますか。特に課題と考えるものを最大3つまでお選び下さい。



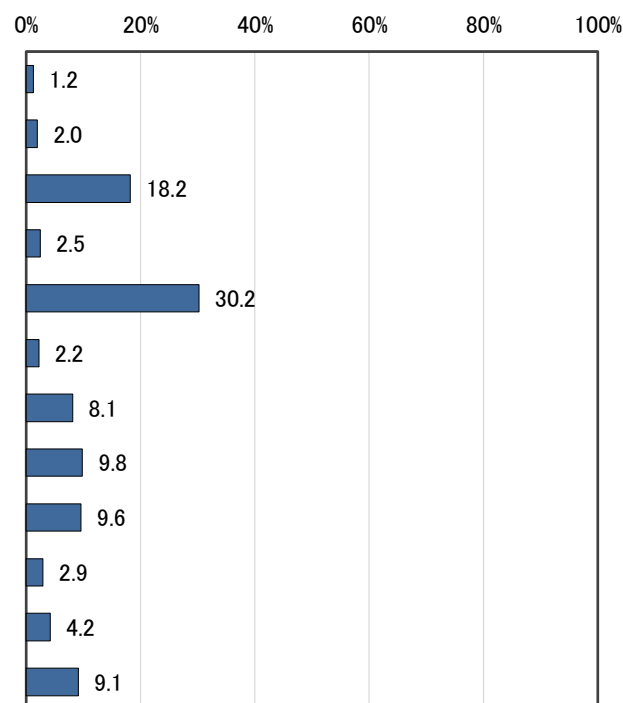
問15 ITサプライチェーンにおける情報セキュリティの向上のため、国、IPAに求める施策はありますか。施策として期待するものを全てお選びください。（いくつでも）



付録3-2 アンケート調査 単純集計結果（委託先調査）

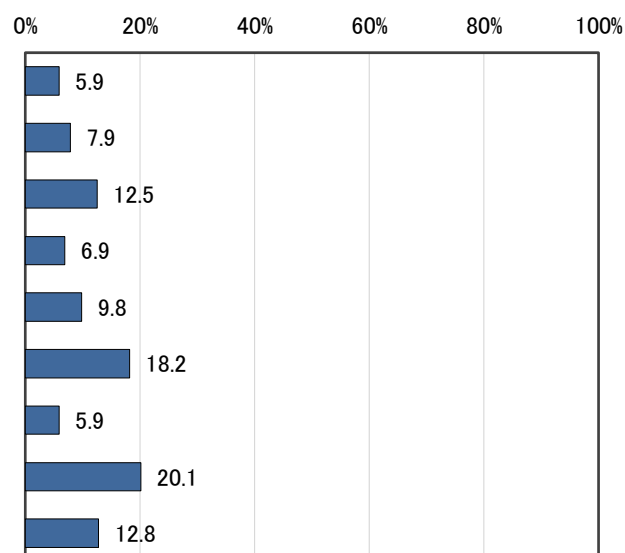
問16 当該事例の委託元の業種をお選びください。（ひとつだけ）

選択肢	%	N
1 農林漁業・同協同組合、鉱業	1.2	5
2 建設業	2.0	8
3 製造業	18.2	74
4 電気・ガス・熱供給・水道業	2.5	10
5 情報通信業	30.2	123
6 運輸業、郵便業	2.2	9
7 卸売業、小売業	8.1	33
8 金融業、保険業	9.8	40
9 その他のサービス業	9.6	39
10 教育、学習支援業	2.9	12
11 医療、福祉	4.2	17
12 その他	9.1	37
計	100	407



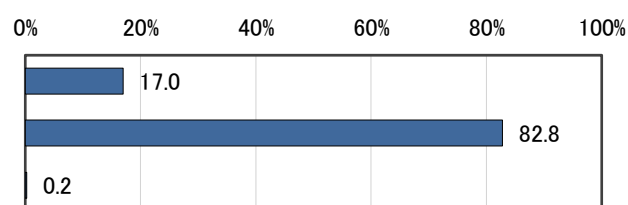
問17 委託元の企業規模（総従業員数）をお選びください。（ひとつだけ）

選択肢	%	N
1 ~50名	5.9	24
2 51名~100名	7.9	32
3 101名~300名	12.5	51
4 301名~500名	6.9	28
5 501名~1,000名	9.8	40
6 1,001名~5,000名	18.2	74
7 5,001名~10,000名	5.9	24
8 10,001名以上	20.1	82
9 わからない	12.8	52
計	100	407



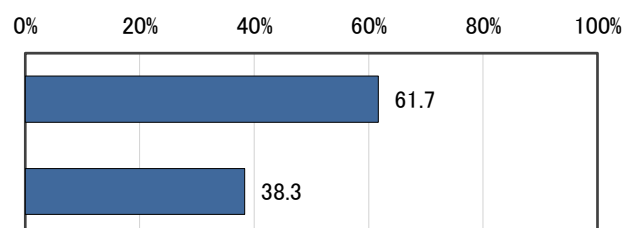
問18 当該事例の委託元は、貴社と資本関係のある系列企業・グループ企業ですか。（ひとつだけ）

選択肢	%	N
1 系列企業・グループ企業	17.0	69
2 系列企業・グループ企業以外	82.8	337
- 無回答	0.2	1
計	100	407



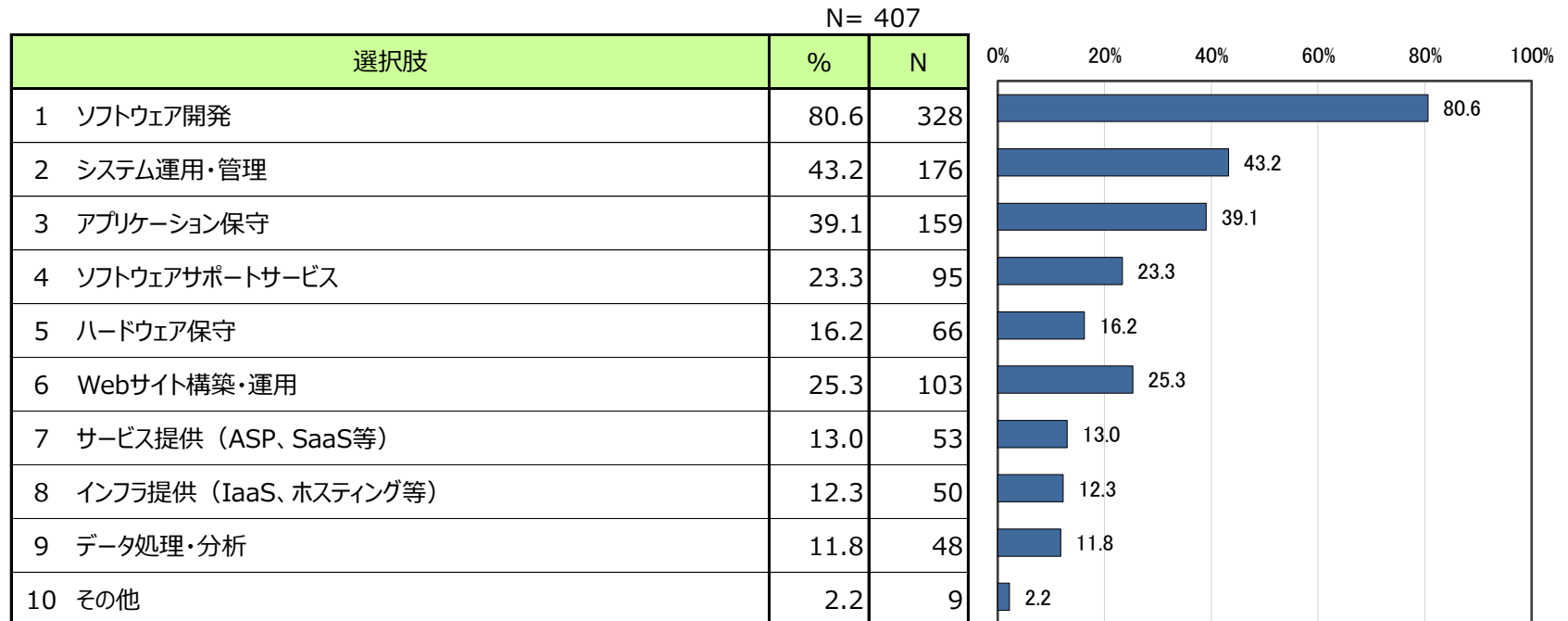
問19 当該事例のITサプライチェーンにおける、貴社の位置付けをお選びください。（ひとつだけ）

選択肢	%	N
1 元請け（プライムベンダー）	61.7	251
2 二次請け以降	38.3	156
計	100	407

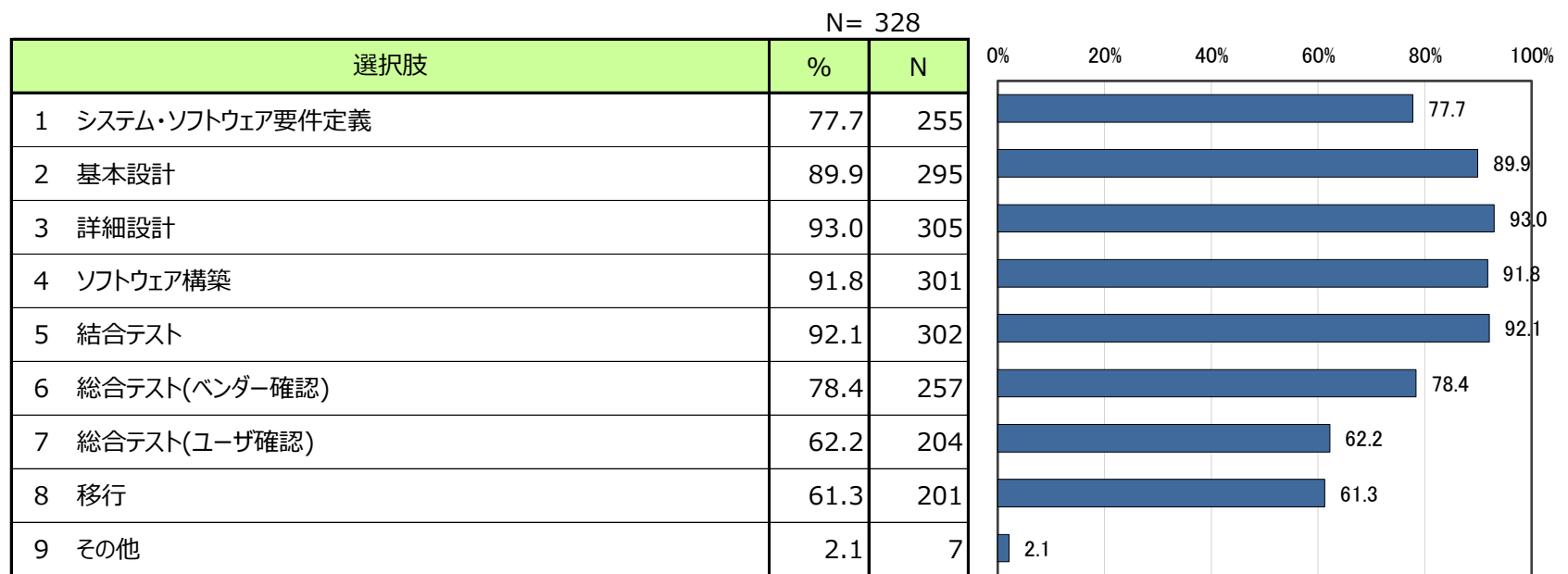


付録3-2 アンケート調査 単純集計結果（委託先調査）

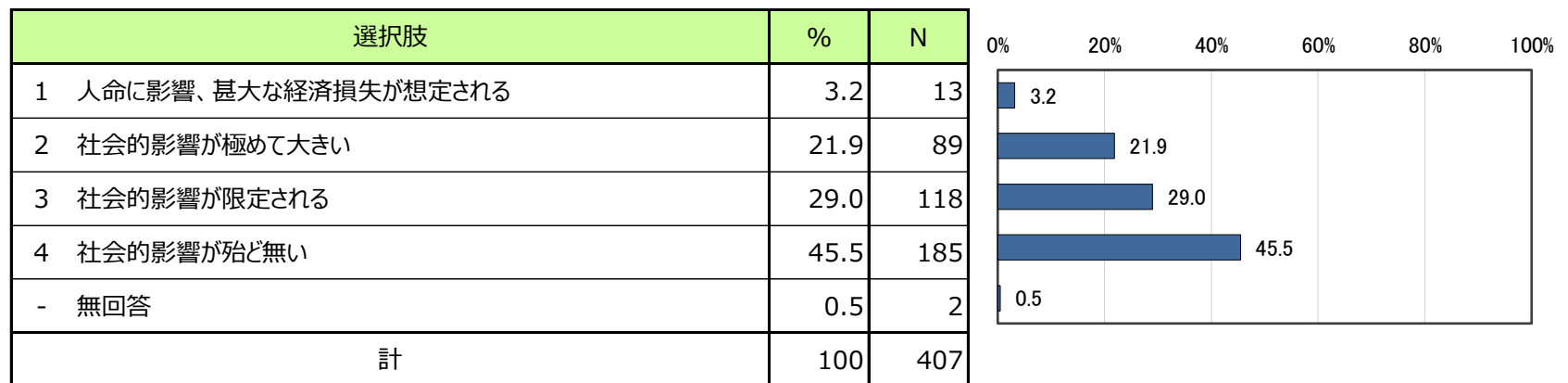
問20 当該事例に含まれるITシステム・サービスについて当てはまるものを全てお選びください。（いくつでも）



問20-1（問20で「ソフトウェア開発」を選んだ場合）委託された開発工程について、当てはまるものを全てお選びください。（いくつでも）

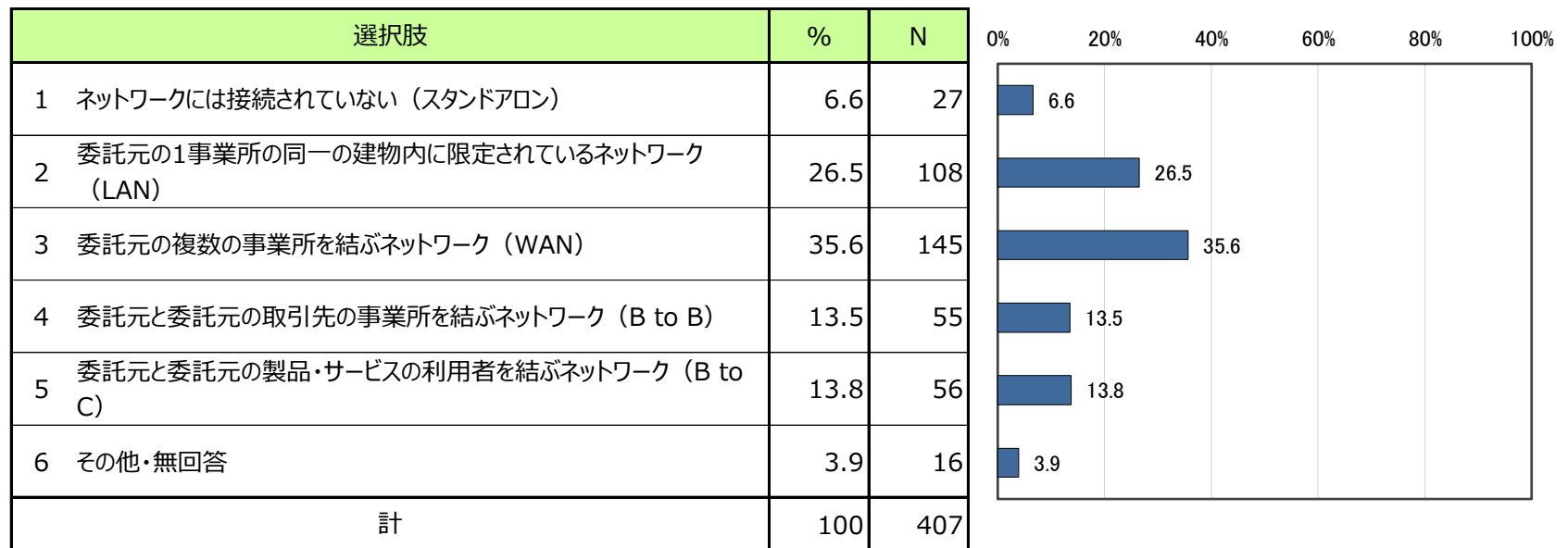


問21 当該事例のITシステム・サービスの障害発生時の社会的影響度について、当てはまるものをお選びください。（ひとつだけ）

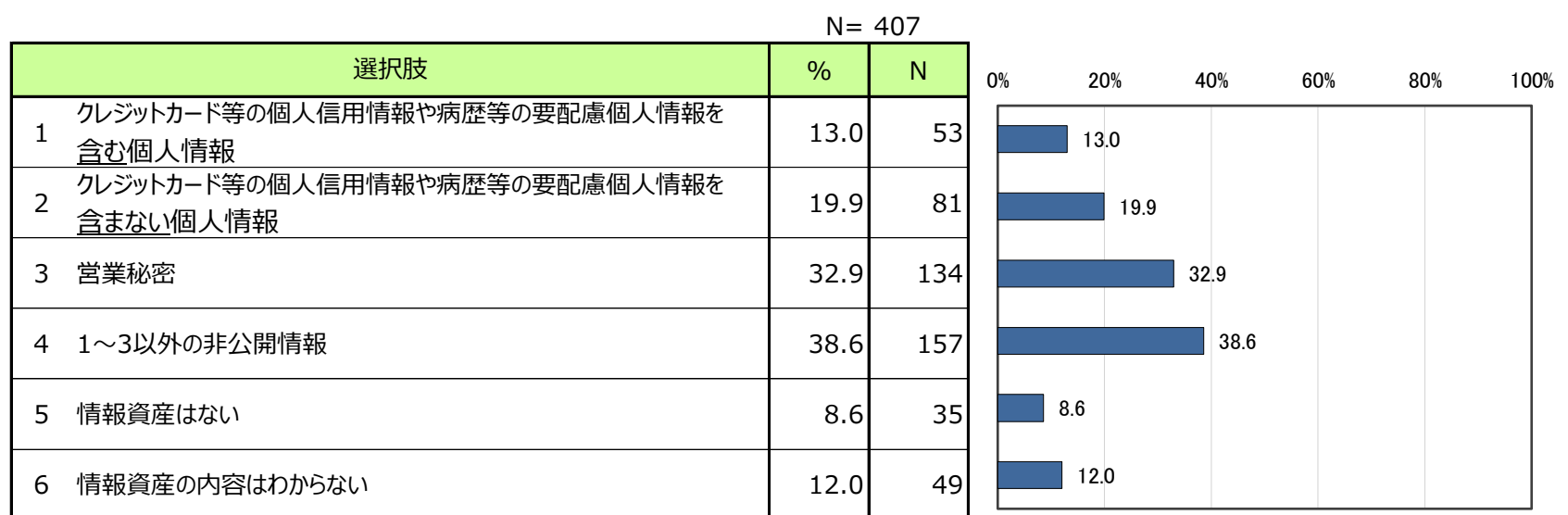


付録3-2 アンケート調査 単純集計結果（委託先調査）

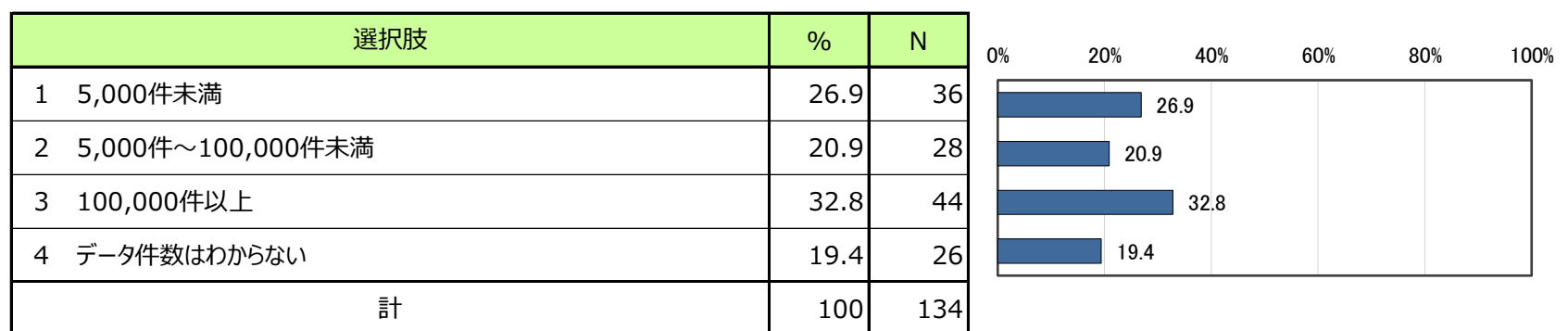
問22 当該事例のITシステム・サービスのネットワークの範囲について、当てはまるものをお選びください。（ひとつだけ）



問23 当該事例のITシステム・サービスで扱う情報資産について、当てはまるものを全てお選びください。（いくつでも）

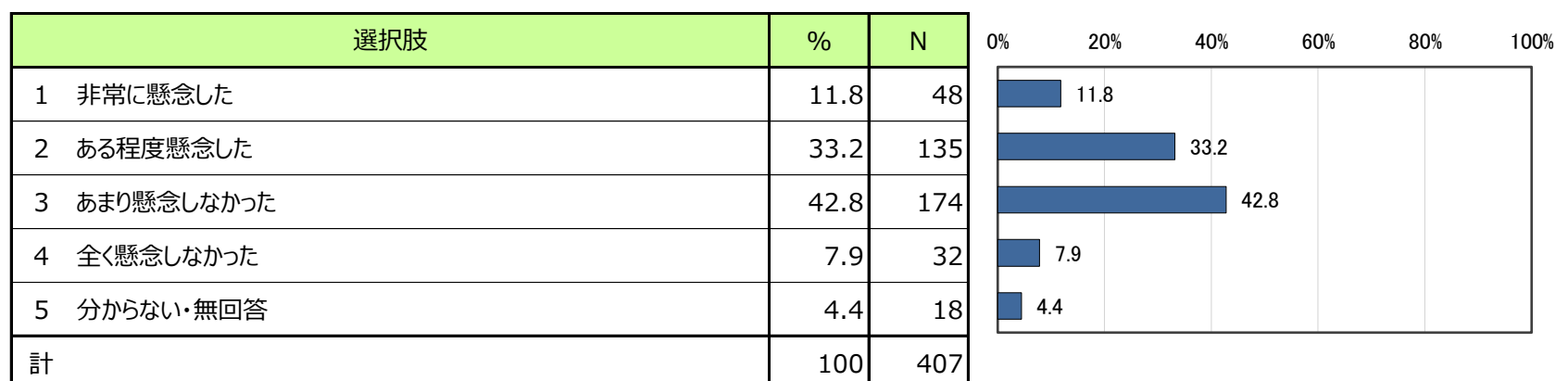


問23-1（問23で「個人情報が含まれている」と回答した場合）個人情報のデータ件数について、当てはまるものをお選びください。（ひとつだけ）



問24 当該事例の業務委託で扱う情報資産に関して、契約の際に情報セキュリティ上のリスクをどの程懸念しましたか。それぞれの脅威に対する懸念の度合いとして当てはまるものをお選びください。（それぞれひとつずつ）

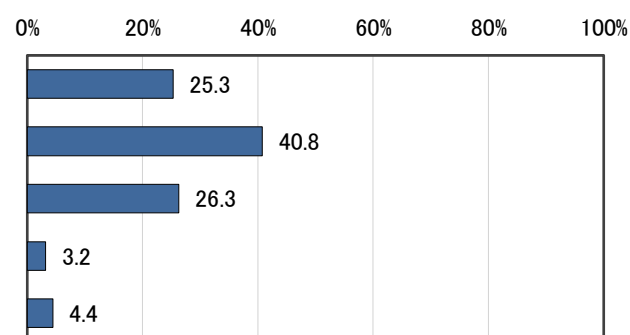
a. 内部不正



付録3-2 アンケート調査 単純集計結果（委託先調査）

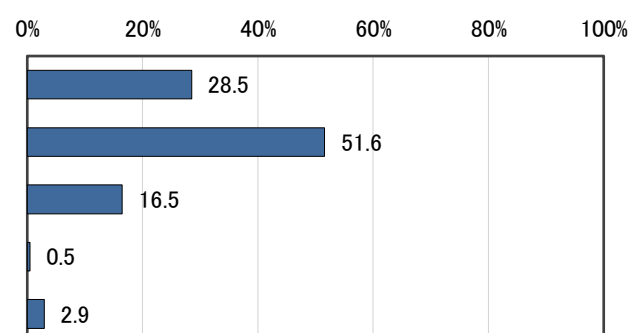
b. 外部攻撃（ウイルス感染や不正アクセス等）

選択肢	%	N
1 非常に懸念した	25.3	103
2 ある程度懸念した	40.8	166
3 あまり懸念しなかった	26.3	107
4 全く懸念しなかった	3.2	13
5 分からない・無回答	4.4	18
計	100	407



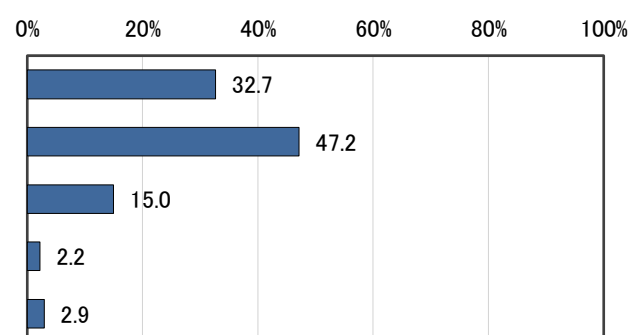
c. 人的ミス(誤操作等)

選択肢	%	N
1 非常に懸念した	28.5	116
2 ある程度懸念した	51.6	210
3 あまり懸念しなかった	16.5	67
4 全く懸念しなかった	0.5	2
5 分からない・無回答	2.9	12
計	100	407



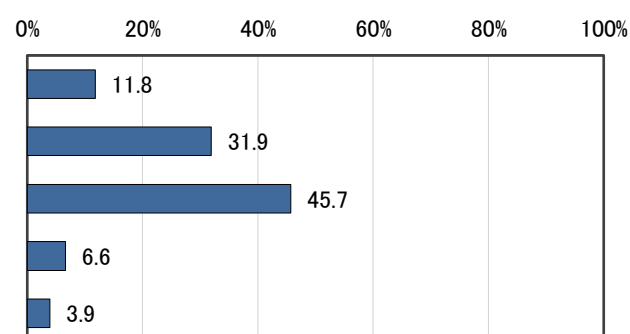
d. システム障害、停止

選択肢	%	N
1 非常に懸念した	32.7	133
2 ある程度懸念した	47.2	192
3 あまり懸念しなかった	15.0	61
4 全く懸念しなかった	2.2	9
5 分からない・無回答	2.9	12
計	100	407



e. 災害

選択肢	%	N
1 非常に懸念した	11.8	48
2 ある程度懸念した	31.9	130
3 あまり懸念しなかった	45.7	186
4 全く懸念しなかった	6.6	27
5 分からない・無回答	3.9	16
計	100	407



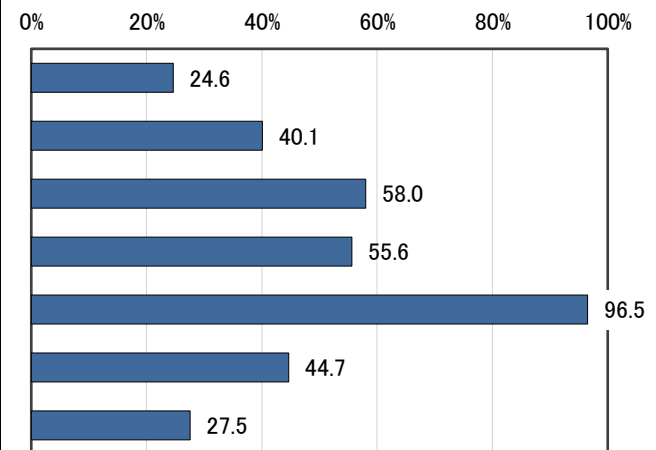
付録3-2 アンケート調査 単純集計結果（委託先調査）

問25 以下の情報セキュリティに係る要求事項について、当該事例の契約関連文書（仕様書、契約書等）にどのように記載されているか、選択肢の番号でご回答ください。

1. 使用した契約関連文書（情報セキュリティ要求事項は問わない）

N = 374

契約関連文書	%	N
1 約款	24.6	92
2 提案書	40.1	150
3 委託元の仕様書	58.0	217
4 貴社の見積書	55.6	208
5 契約書	96.5	361
6 覚書	44.7	167
7 その他（SLA等）	27.5	103



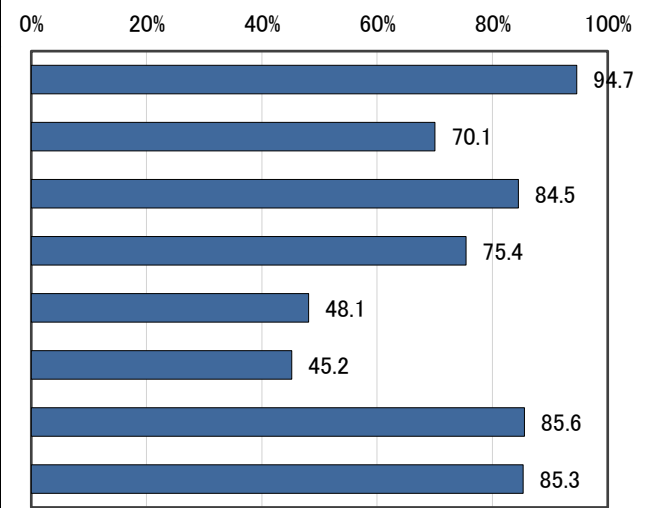
※責任範囲の明示の有無について回答のなかった33件を集計から除外している

2. 契約関連文書に記載されている情報セキュリティ要求事項（文書は問わない）

<全体>

N = 374

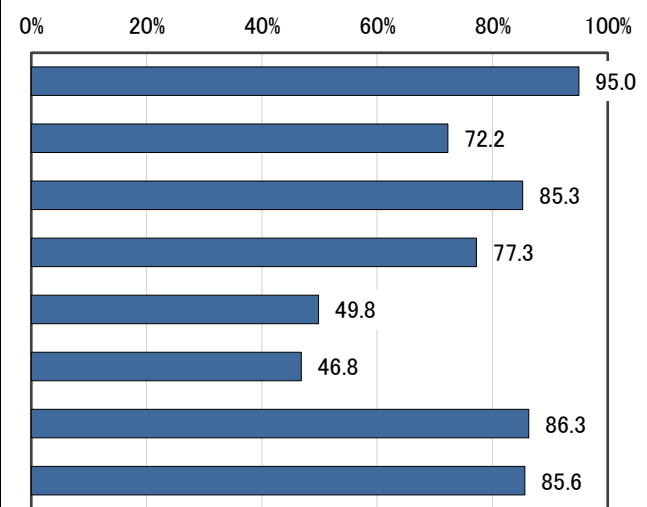
情報セキュリティ要求事項	%	N
1 秘密保持	94.7	354
2 証跡の提示、監査協力等	70.1	262
3 情報セキュリティに関する契約内容に違反した場合の措置	84.5	316
4 インシデントが発生した場合の対応	75.4	282
5 可用性（稼働率の水準、目標復旧時間等）	48.1	180
6 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応	45.2	169
7 再委託の禁止または制限	85.6	320
8 契約終了後の情報資産の扱い（返却、消去、廃棄等）	85.3	319



a. ソフトウェア開発を含む事例

N = 299

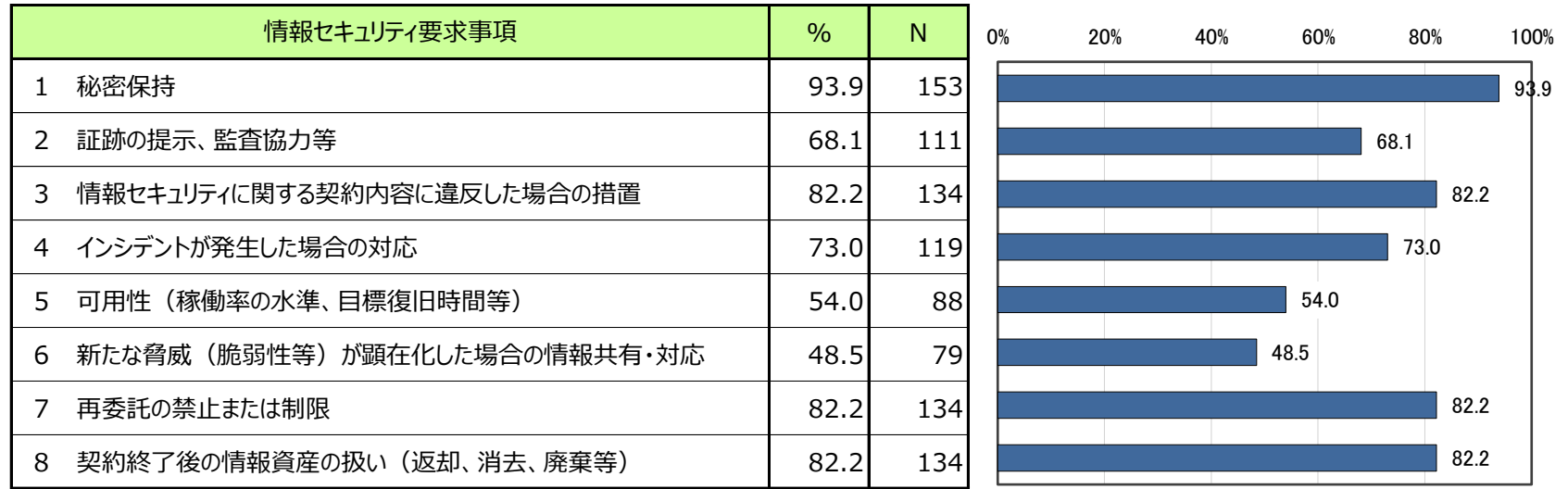
情報セキュリティ要求事項	%	N
1 秘密保持	95.0	284
2 証跡の提示、監査協力等	72.2	216
3 情報セキュリティに関する契約内容に違反した場合の措置	85.3	255
4 インシデントが発生した場合の対応	77.3	231
5 可用性（稼働率の水準、目標復旧時間等）	49.8	149
6 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応	46.8	140
7 再委託の禁止または制限	86.3	258
8 契約終了後の情報資産の扱い（返却、消去、廃棄等）	85.6	256



付録3-2 アンケート調査 単純集計結果（委託先調査）

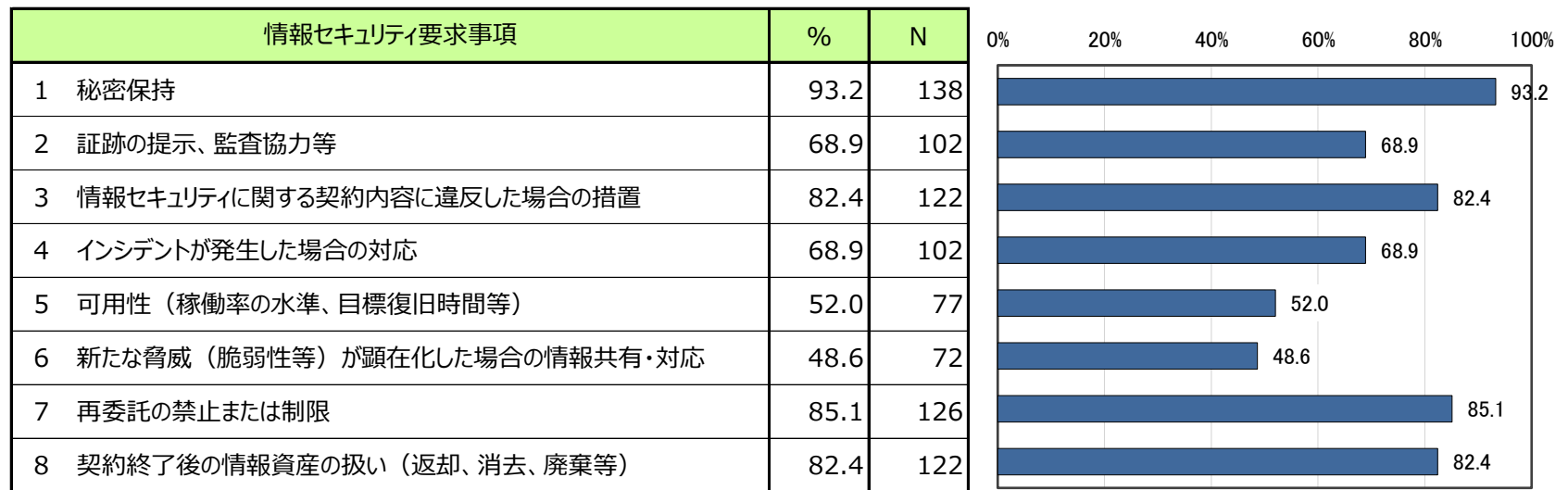
b. システム運用・管理を含む事例

N = 163



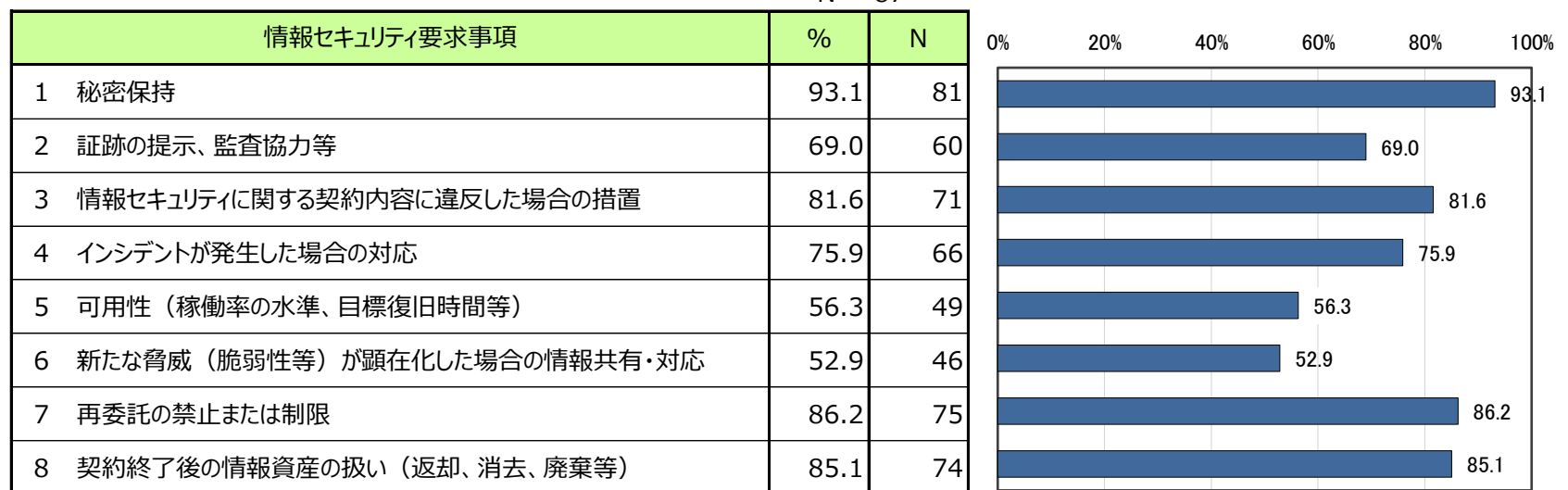
c. アプリケーション保守を含む事例

N = 148



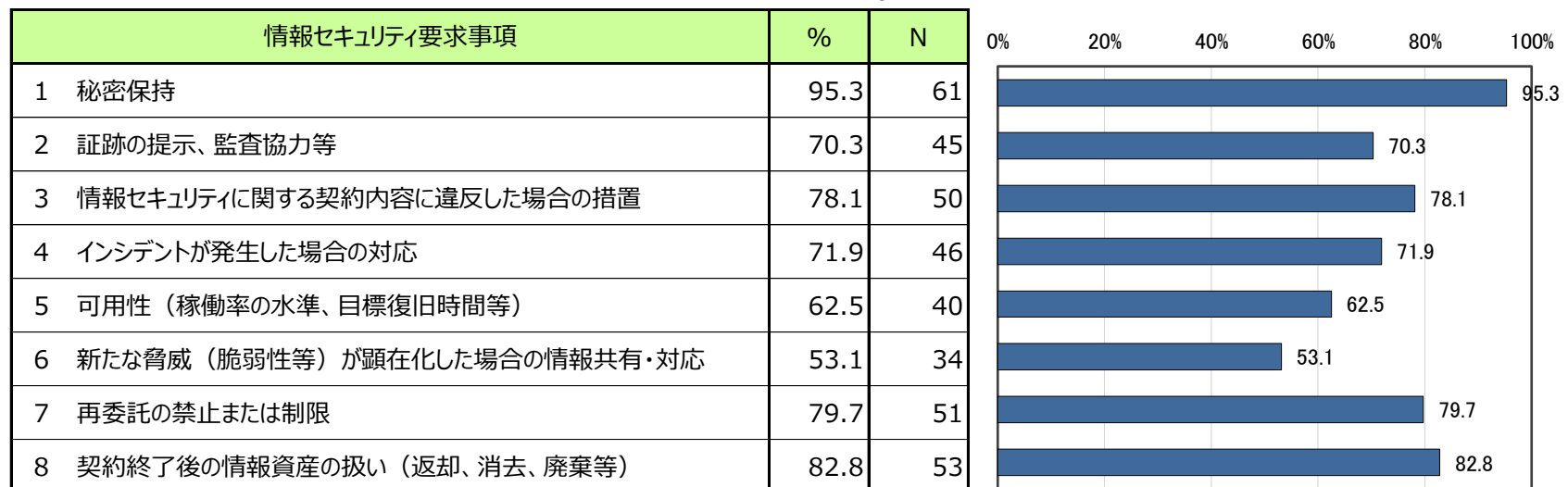
d. ソフトウェアサポートサービスを含む事例

N = 87



e. ハードウェア保守を含む事例

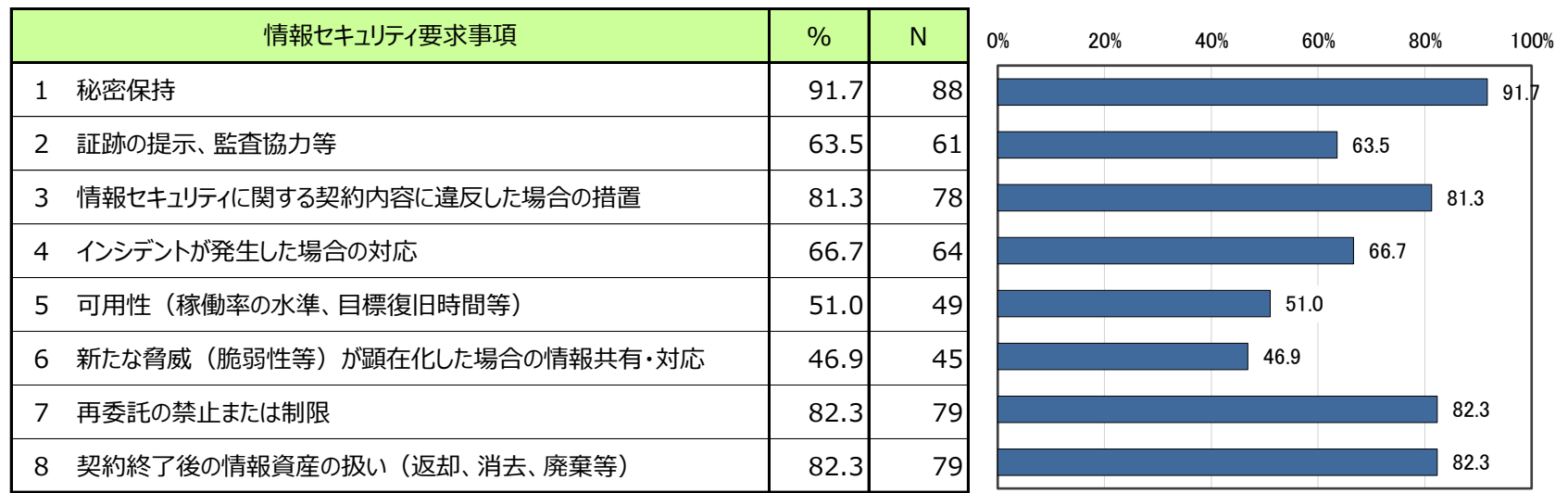
N = 64



付録3-2 アンケート調査 単純集計結果（委託先調査）

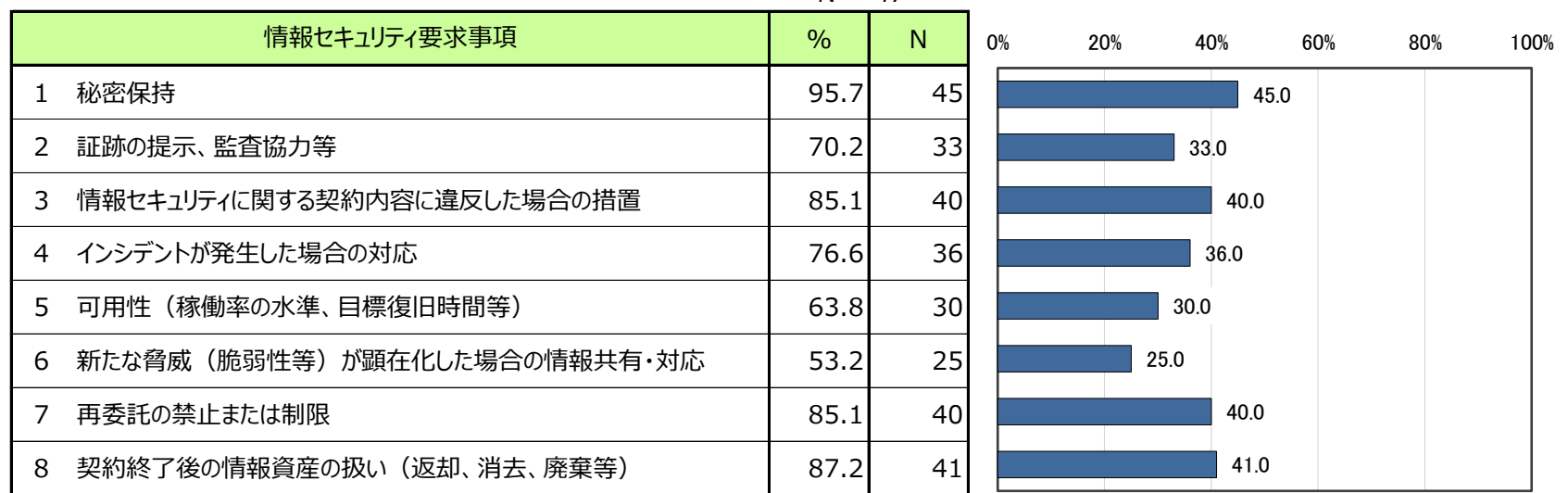
f. Webサイト構築・運用を含む事例

N = 96



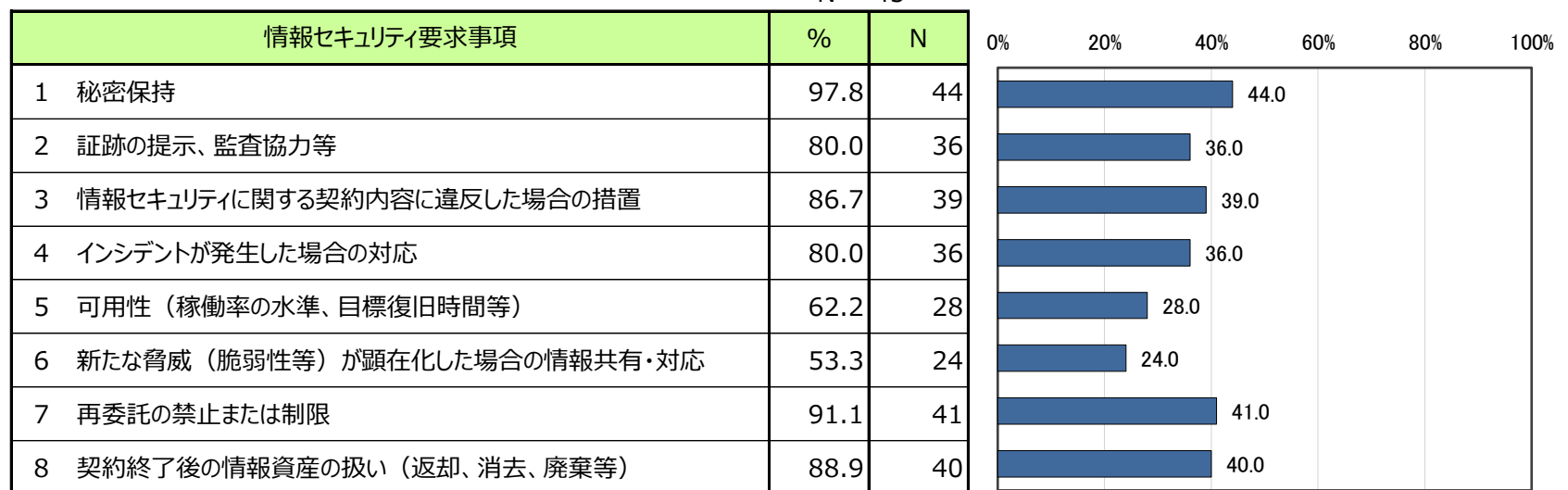
g. サービス提供（ASP.SaaS等）を含む事例

N = 47



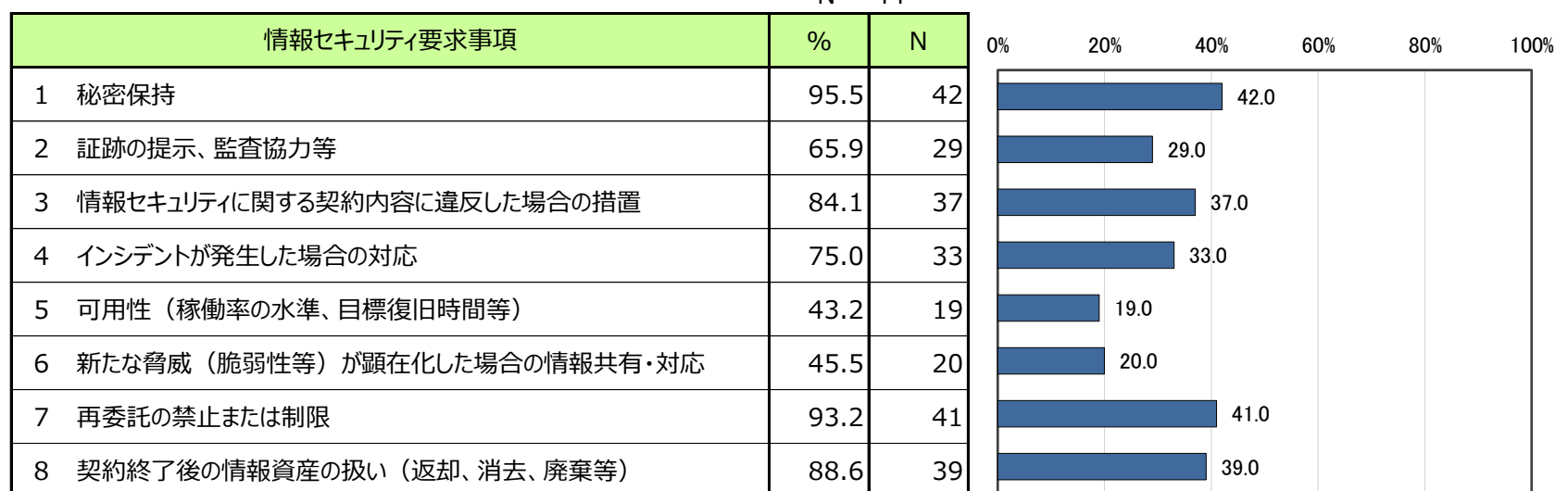
h. インフラ提供（IaaS、ホスティング等）を含む事例

N = 45



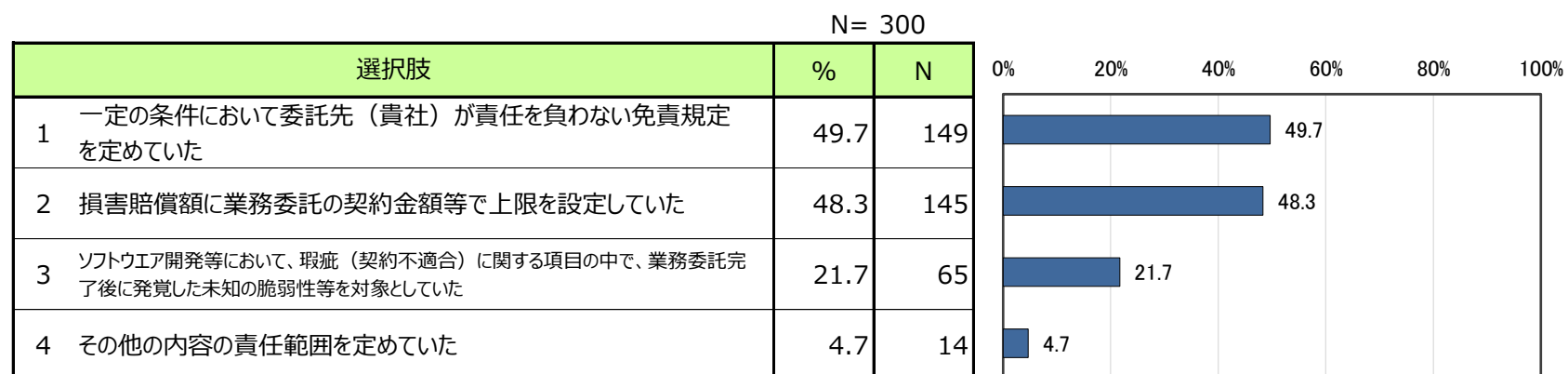
i. データ処理・分析を含む事例

N = 44

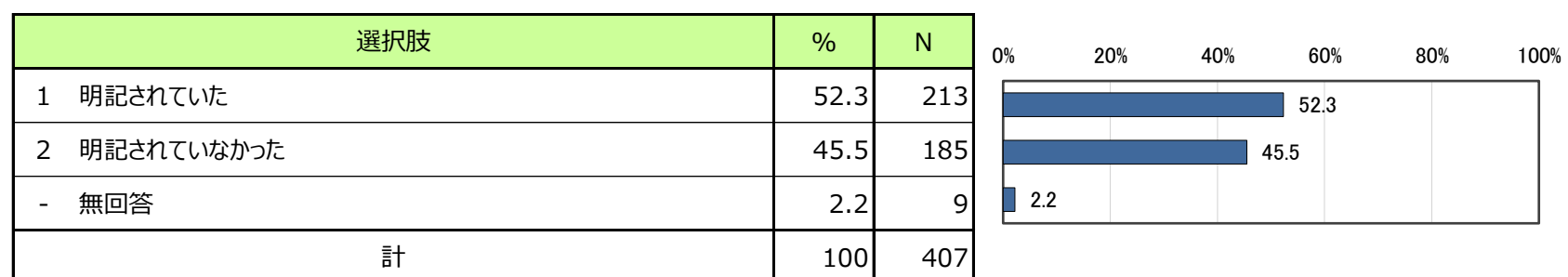


付録3-2 アンケート調査 単純集計結果（委託先調査）

問25-1（問25でいずれかで「責任範囲が明記されていた」と回答した場合）情報セキュリティに関する委託先（貴社）の責任範囲についてどのように明示されていましたか。当てはまるものを全てお選びください。（いくつでも）

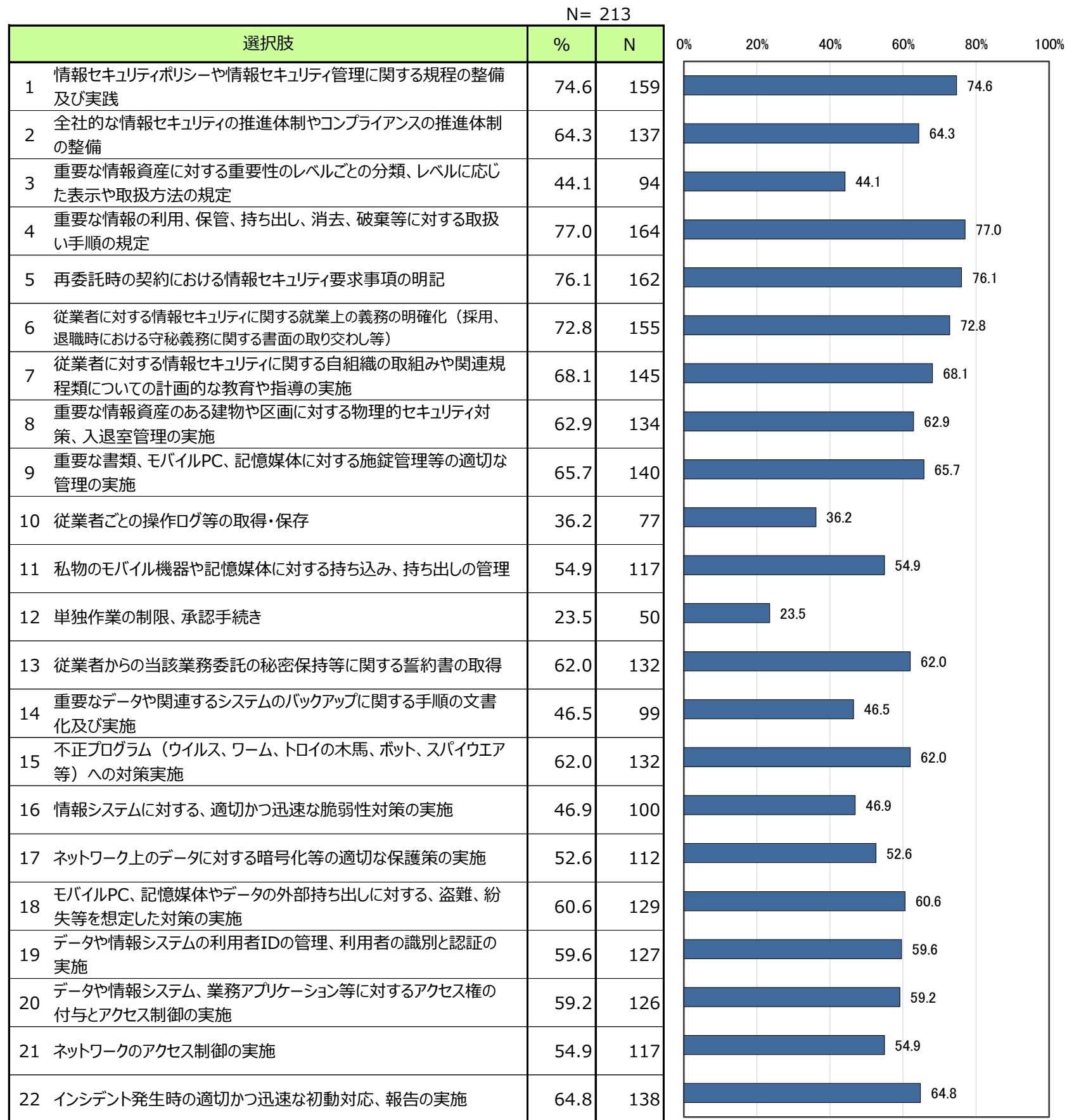


問26 当該事例の契約関連文書（仕様書、契約書等）では、委託先（貴社）が実施すべき組織的な情報セキュリティ対策が明記されていましたか。（ひとつだけ）

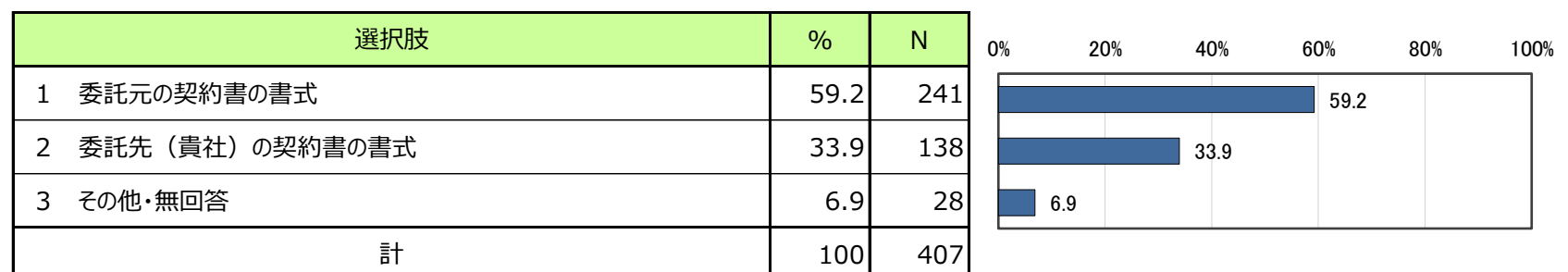


付録3-2 アンケート調査 単純集計結果（委託先調査）

問26-1（問26で「明記されていた」と回答した場合）委託先（貴社）が実施すべき組織的な情報セキュリティ対策として明記されていたものを全てお選びください。（いくつでも）

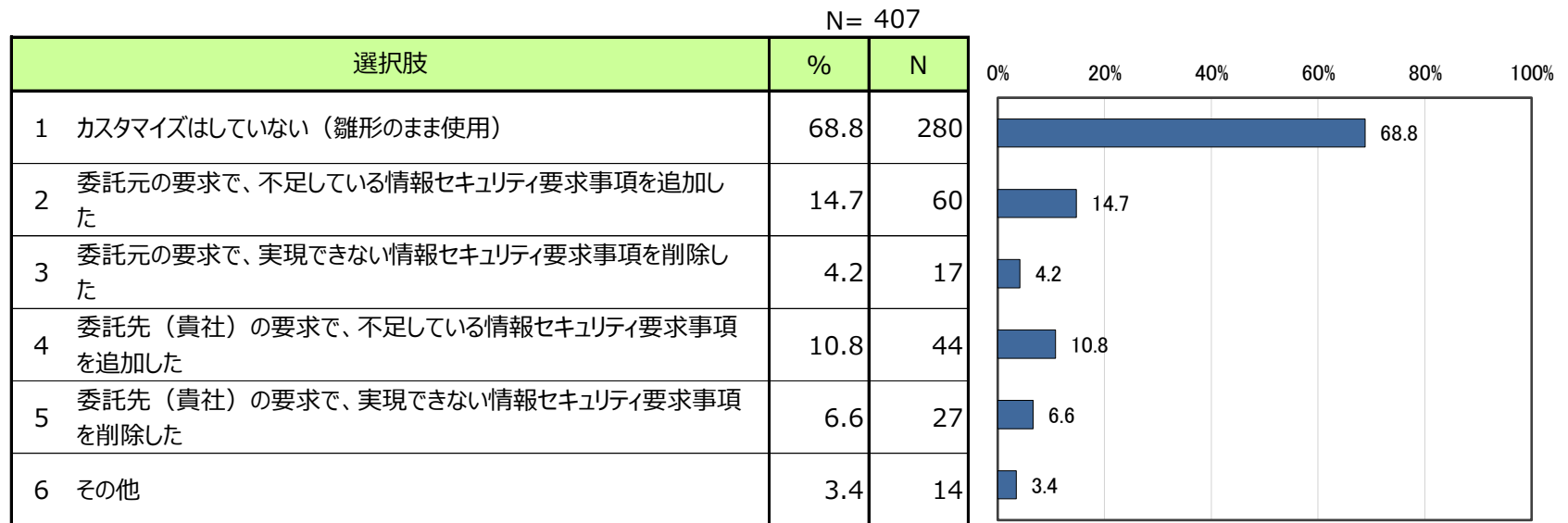


問27 当該事例において使用した契約書の書式は委託元のものですか、委託先のものですか。当てはまるものをお選びください。（ひとつだけ）



付録3-2 アンケート調査 単純集計結果（委託先調査）

問28 当該事例において使用した契約書の書式は、対象業務の情報セキュリティ要求事項に合わせて、情報セキュリティに関する項目を追加したり、内容を修正したりするカスタマイズを行いましたか。当てはまるものをお選びください。（いくつでも）



問29 当該事例において、受託業務の契約における情報セキュリティ要求項目に関し、委託元との間で何らかのトラブルが発生したことがありますか。当てはまるものをお選びください。（ひとつだけ）

