

添付資料

経営リスクとしてのサイバーセキュリティ
—アンケート調査から読み解く企業の現状と監査役等の着眼点—
アンケート調査 集計結果

実施期間：2026年5月21日（木）から同年6月10日（水）

対象：当協会の法人会員 7,775 社（2026年5月現在）

実施形式：インターネット上のアンケートフォームにて一社一回答

総回答社数：1,528 社（回答率 19.7%）

※割合（%）は回答数を集計母数で除した数値（小数点以下第2位四捨五入）を表示しているため、合計数値が 100.0%にならない場合もある。

※「複数選択可」の質問でも、「全体」の回答率は 100.0%と表示しているが、各選択肢の回答率の合計は 100.0%にならない。

※上場区分別・資本金区分別の集計表および自由記述回答の抜粋版は、日本監査役協会ホームページに別掲資料として掲載。

【1.サイバーセキュリティリスク管理体制に対する監査役等の向き合い方】

■(1)取締役会の状況■

Q1. 監査役等からみて、取締役会等（経営会議等も含む。以下同様）におけるサイバーセキュリティをめぐる報告や議論はどのような状況ですか。最も近いものを1つ選択してください。（1つ選択）	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4（スタンダード、グロース、その他上場）	5. 非上場	500億円以上
全 体	1527 100.0	419 100.0	380 100.0	728 100.0	103 100.0
1. 特段の定例報告はなく、経営課題としての議論はない	175 11.5	30 7.2	47 12.4	98 13.5	4 3.9
2. インシデント発生時または必要に応じて報告・議論されるが、個別のシステムトラブル対応等が中心である	492 32.2	98 23.4	157 41.3	237 32.6	9 8.7
3. インシデント件数や主要施策の進捗が定期的に報告・議論されている	372 24.4	117 27.9	82 21.6	173 23.8	25 24.3
4. 3に加え、事業戦略・リスクマネジメントの一環として、KPIやリスク評価を踏まえて議論されている	315 20.6	123 29.4	51 13.4	141 19.4	47 45.6
5. 4に加え、中長期戦略や投資判断と連動し、取締役会等が主体的に関与している	111 7.3	40 9.5	23 6.1	48 6.6	15 14.6
6. その他（自由記述）	62 4.1	11 2.6	20 5.3	31 4.3	3 2.9

Q2. 監査役等からみて、直近1年間におけるサイバーセキュリティをめぐる経営陣の意識に変化や進展はみられますか。最も近いものを1つ選択してください。（1つ選択）	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4（スタンダード、グロース、その他上場）	5. 非上場	500億円以上
全 体	1524 100.0	419 100.0	379 100.0	726 100.0	103 100.0
1. 以前から重要な経営リスクとして認識しており、高い危機感を持っている	590 38.7	184 43.9	112 29.6	294 40.5	65 63.1
2. 経営リスクとして以前より危機感を持つようになった	760 49.9	218 52.0	216 57.0	326 44.9	35 34.0
3. 危機感や意識は低く、変化はあまりみられない	136 8.9	15 3.6	41 10.8	80 11.0	3 2.9
4. 以前からあまり関心がなく、変化はあまりみられない	15 1.0	－ －	5 1.3	10 1.4	－ －
5. その他（自由記述）	23 1.5	2 0.5	5 1.3	16 2.2	－ －

Q3. 直近1年間において、サイバーセキュリティをめぐる対策に関して、取締役会等の議論で進展したこと、それを踏まえて実行された施策（予定を含む）はありますか。（自由記述）

Q4. 監査役等は、サイバーセキュリティについて意見を述べたことがありますか。当てはまるものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1514 100.0	416 100.0	375 100.0	723 100.0	101 100.0
1. 取締役会等で意見を述べた	376 24.8	134 32.2	105 28.0	137 18.9	28 27.7
2. 経営陣に意見を述べた	564 37.3	129 31.0	125 33.3	310 42.9	36 35.6
3. 取締役会で意見し、経営陣にも別途、意見を述べた	168 11.1	67 16.1	44 11.7	57 7.9	21 20.8
4. 意見を述べたことはない	327 21.6	69 16.6	81 21.6	177 24.5	9 8.9
5. その他(自由記述)	79 5.2	17 4.1	20 5.3	42 5.8	7 6.9

■(2)サイバーセキュリティリスク管理体制■

Q5. 貴社では、サイバーセキュリティ対策について誰が最終的な責任者になっていますか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1526 100.0	418 100.0	380 100.0	728 100.0	103 100.0
1. 代表取締役	634 41.5	146 34.9	171 45.0	317 43.5	27 26.2
2. CISO、CIOなど	230 15.1	93 22.2	29 7.6	108 14.8	52 50.5
3. 1・2以外の取締役、執行役(員)	445 29.2	134 32.1	119 31.3	192 26.4	17 16.5
4. サイバーセキュリティリスク管理・統括組織の長(1～3以外)	148 9.7	32 7.7	44 11.6	72 9.9	5 4.9
5. その他(自由記述)	30 2.0	8 1.9	4 1.1	18 2.5	2 1.9
6. 特にない	39 2.6	5 1.2	13 3.4	21 2.9	— —

Q5. 責任者への確認事項、責任者からの報告内容など。(自由記述)

Q6. 貴社には、サイバーセキュリティリスクを管理・統括している組織がありますか。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1525 100.0	419 100.0	380 100.0	726 100.0	104 100.0
1. サイバーセキュリティリスク管理の専門組織はない	147 9.6	16 3.8	42 11.1	89 12.3	— —
2. 専門組織はないが部分的にある、または他の部門が兼務している	673 44.1	155 37.0	205 53.9	313 43.1	20 19.2
3. サイバーセキュリティリスク管理の専門組織を設けている	306 20.1	118 28.2	50 13.2	138 19.0	46 44.2
4. 全社リスク管理組織の中にサイバーセキュリティも組み込まれている	450 29.5	153 36.5	107 28.2	190 26.2	49 47.1
5. サイバーセキュリティリスク管理の専門組織がグループ全体(および委託先も含めた広範囲)のリスク管理・統括を行っている	203 13.3	84 20.0	29 7.6	90 12.4	39 37.5
6. サイバーインシデントに対応可能な専門チーム(CSIRTなど)を設けている	216 14.2	109 26.0	21 5.5	86 11.8	54 51.9
7. その他(自由記述)	82 5.4	17 4.1	22 5.8	43 5.9	4 3.8

Q6. 当該組織への確認事項など、監査役等の関わり方。(自由記述)

Q7. 監査役等からみて、サイバーセキュリティに関する対応方針の社内への周知はどのような状況ですか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1524 100.0	418 100.0	379 100.0	727 100.0	104 100.0
1. 従業員には周知されていない	83 5.4	8 1.9	24 6.3	51 7.0	1 1.0
2. 一部の従業員へ周知されている	110 7.2	19 4.5	48 12.7	43 5.9	1 1.0
3. 全従業員向けに周知されている	361 23.7	71 17.0	120 31.7	170 23.4	7 6.7
4. 3に加え、定期的な教育・訓練により理解度が確認されている	592 38.8	196 46.9	119 31.4	277 38.1	49 47.1
5. 4に加え、従業員の行動・意識が確認され、違反や是正状況がモニタリングされている	344 22.6	114 27.3	60 15.8	170 23.4	44 42.3
6. その他(自由記述)	34 2.2	10 2.4	8 2.1	16 2.2	2 1.9

Q8. 監査役等からみて、貴社のサイバーセキュリティリスク管理体制の構築・運用はどのような状況ですか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1525 100.0	419 100.0	380 100.0	726 100.0	104 100.0
1. 部門ごとに個別に対応しており、全社的な体制はない	72 4.7	7 1.7	26 6.8	39 5.4	— —
2. 基本方針や規程はあるが、統括機能や責任分担は不明確である	209 13.7	39 9.3	79 20.8	91 12.5	2 1.9
3. 基本方針や規程があり、責任部門・責任者を定め、全社的な体制を構築している	627 41.1	164 39.1	178 46.8	285 39.3	27 26.0
4. 3に加え、グループ会社を含めた統括体制があり、定期的に見直し・改善されている	354 23.2	125 29.8	59 15.5	170 23.4	36 34.6
5. 4に加え、経営・監査の連携によりモニタリングされ、体制の有効性が継続的に検証されている	216 14.2	76 18.1	24 6.3	116 16.0	39 37.5
6. その他(自由記述)	47 3.1	8 1.9	14 3.7	25 3.4	— —

Q9-1. 監査役等からみて、サイバーセキュリティのリスク評価の実施はどのような状況ですか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1523 100.0	419 100.0	379 100.0	725 100.0	103 100.0
1. 体系的なリスク評価は実施されていない	268 17.6	36 8.6	92 24.3	140 19.3	3 2.9
2. 技術部門を中心に、脆弱性等の評価は一部実施されている	367 24.1	83 19.8	107 28.2	177 24.4	8 7.8
3. 事業への影響を考慮したリスク評価が定期的に実施されている	357 23.4	105 25.1	99 26.1	153 21.1	23 22.3
4. 3に加え、リスク対応計画と連動し、経営層へ報告されている	389 25.5	143 34.1	57 15.0	189 26.1	50 48.5
5. 4に加え、リスク評価結果が投資判断・戦略見直しに活用されている	111 7.3	45 10.7	16 4.2	50 6.9	19 18.4
6. その他(自由記述)	31 2.0	7 1.7	8 2.1	16 2.2	— —

Q9-2. 監査役等は、サイバーセキュリティのリスク評価の結果をどのように確認していますか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1521 100.0	418 100.0	380 100.0	723 100.0	104 100.0
1. 監査役等は特に確認していない	200 13.1	36 8.6	62 16.3	102 14.1	2 1.9
2. 報告内容を確認している	623 41.0	163 39.0	173 45.5	287 39.7	22 21.2
3. 2に加え、リスク評価プロセスや結果を確認している	295 19.4	91 21.8	72 18.9	132 18.3	34 32.7
4. 3に加え、課題や改善点をフォローアップしている	227 14.9	76 18.2	39 10.3	112 15.5	29 27.9
5. 4に加え、他社事例や外部の情報・知見も踏まえ、経営層へ確認している	129 8.5	41 9.8	20 5.3	68 9.4	17 16.3
6. その他(自由記述)	47 3.1	11 2.6	14 3.7	22 3.0	— —

Q10-1. 監査役等からみて、貴社のサイバーセキュリティ対策の全体像は、どのような状況ですか。最も近いと思われるものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1523 100.0	418 100.0	379 100.0	726 100.0	104 100.0
1. 初期段階: 場当たりの最低限の対策のみで、全体像は把握されていない	56 3.7	3 0.7	23 6.1	30 4.1	1 1.0
2. 基礎段階: セキュリティの基本的対策が実施されている	379 24.9	76 18.2	117 30.9	186 25.6	4 3.8
3. 標準化: セキュリティ対策が全社的に標準化され運用されている	654 42.9	184 44.0	178 47.0	292 40.2	29 27.9
4. 高度化: 第三者評価や改善点の分析・検証により、対策を継続的に高度化している	301 19.8	106 25.4	43 11.3	152 20.9	47 45.2
5. 最適化: 新技術の導入などにより対策の自動化・先進化に取り組んでいる	110 7.2	44 10.5	14 3.7	52 7.2	22 21.2
6. その他(自由記述)	23 1.5	5 1.2	4 1.1	14 1.9	1 1.0

Q10-2. 監査役等は、サイバーセキュリティ対策の整備・運用状況をどのように確認していますか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1527 100.0	419 100.0	380 100.0	728 100.0	104 100.0
1. 監査役等は特に確認していない	143 9.4	25 6.0	46 12.1	72 9.9	1 1.0
2. 報告内容を確認している	713 46.7	186 44.4	194 51.1	333 45.7	28 26.9
3. 2に加え、セキュリティ対策プロセスや結果を確認している	288 18.9	92 22.0	69 18.2	127 17.4	26 25.0
4. 3に加え、課題や改善点をフォローアップしている	222 14.5	76 18.1	37 9.7	109 15.0	32 30.8
5. 4に加え、他社事例や外部の情報・知見も踏まえ、経営層へ確認している	120 7.9	35 8.4	19 5.0	66 9.1	17 16.3
6. その他(自由記述)	41 2.7	5 1.2	15 3.9	21 2.9	— —

Q11. 監査役等からみて、グループ会社におけるサイバーセキュリティの管理・統制はどのような状況ですか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	857 100.0	398 100.0	284 100.0	175 100.0	85 100.0
1. 自社以外の状況は把握されていない	153 17.9	40 10.1	63 22.2	50 28.6	2 2.4
2. 重要なグループ会社に関し、状況確認が行われている	192 22.4	77 19.3	67 23.6	48 27.4	6 7.1
3. グループ会社全体にセキュリティの基本方針や報告ルールなどを展開している	261 30.5	121 30.4	96 33.8	44 25.1	15 17.6
4. 3に加え、グループ会社のセキュリティリスクやその対策状況を評価している	142 16.6	95 23.9	32 11.3	15 8.6	35 41.2
5. 4に加え、インシデント対応・演習を含め、グループ会社を一体的に管理している	81 9.5	56 14.1	14 4.9	11 6.3	26 30.6
6. その他(自由記述)	28 3.3	9 2.3	12 4.2	7 4.0	1 1.2

Q11. 監査役等からみて、グループ会社におけるサイバーセキュリティの管理・統制はどのような状況ですか。(グループ会社数別)(1つ選択)	F5-2. グループ会社の総数				
	1. 1～5社	2. 6～10社	3. 11～50社	4. 51～100社	5. 101社以上
全 体	350 100.0	155 100.0	241 100.0	51 100.0	60 100.0
1. 自社以外の状況は把握されていない	107 30.6	24 15.5	21 8.7	1 2.0	0 0.0
2. 重要なグループ会社に関り、状況確認が行われている	74 21.1	48 31.0	58 24.1	10 19.6	2 3.3
3. グループ会社全体にセキュリティの基本方針や報告ルールなどを展開している	107 30.6	47 30.3	85 35.3	11 21.6	11 18.3
4. 3に加え、グループ会社のセキュリティリスクやその対策状況を評価している	26 7.4	21 13.5	48 19.9	21 41.2	26 43.3
5. 4に加え、インシデント対応・演習を含め、グループ会社を一体的に管理している	18 5.1	11 7.1	25 10.4	7 13.7	20 33.3
6. その他(自由記述)	18 5.1	4 2.6	4 1.7	1 2.0	1 1.7

■(3)サイバーインシデント発生時の緊急対応体制の整備■

Q12. 貴社では、サイバーインシデント(特にランサムウェア攻撃)を想定した事業継続計画(BCP)が策定されていますか。最も近いものを選択して下さい。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1513 100.0	414 100.0	375 100.0	724 100.0	102 100.0
1. 策定していない	340 22.5	41 9.9	108 28.8	191 26.4	5 4.9
2. 策定中、検討中	518 34.2	159 38.4	147 39.2	212 29.3	21 20.6
3. サイバーインシデントのBCPを策定している	247 16.3	81 19.6	59 15.7	107 14.8	23 22.5
4. 既存のBCPにサイバーインシデントも含まれている	322 21.3	108 26.1	52 13.9	162 22.4	41 40.2
5. 事業継続力強化計画にサイバーインシデントも含まれている	59 3.9	19 4.6	6 1.6	34 4.7	8 7.8
6. その他(自由記述)	27 1.8	6 1.4	3 0.8	18 2.5	4 3.9

Q13-1. 監査役等からみて、サイバーインシデントを想定した事業継続計画(BCP)の運用はどのような状況ですか。最も近いものを選択して下さい。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	626 100.0	207 100.0	117 100.0	302 100.0	72 100.0
1. 文書上は整備しているが、訓練は行っていない	175 28.0	47 22.7	47 40.2	81 26.8	6 8.3
2. 定期的に訓練を実施している	161 25.7	46 22.2	29 24.8	86 28.5	15 20.8
3. 2に加え、訓練結果を踏まえ、BCPを見直している	127 20.3	53 25.6	23 19.7	51 16.9	16 22.2
4. 3に加え、実際のインシデント・他社事例も反映して見直している	102 16.3	35 16.9	10 8.5	57 18.9	19 26.4
5. 4に加え、サプライチェーンでのインシデント発生やその影響も考慮し、見直している	50 8.0	23 11.1	6 5.1	21 7.0	14 19.4
6. その他(自由記述)	11 1.8	3 1.4	2 1.7	6 2.0	2 2.8

Q13-2. サイバーセキュリティの事業継続計画(BCP)の見直しの頻度はどの程度ですか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	625 100.0	207 100.0	117 100.0	301 100.0	72 100.0
1. 見直しはされていない	41 6.6	11 5.3	12 10.3	18 6.0	3 4.2
2. 年に1回程度	363 58.1	121 58.5	68 58.1	174 57.8	45 62.5
3. 数年に1回程度	114 18.2	40 19.3	15 12.8	59 19.6	10 13.9
4. インシデントやリスクが発生したとき	79 12.6	30 14.5	18 15.4	31 10.3	11 15.3
5. その他(自由記述)	28 4.5	5 2.4	4 3.4	19 6.3	3 4.2

Q13-3. サイバーインシデントを想定した事業継続計画(BCP)の策定や運用状況について、監査役等が関与していることはありますか。(自由記述)

Q14. 貴社で実施されているサイバーインシデント発生時の緊急対応の訓練などについて、当てはまるものを選択したうえ、監査役等からみた課題などについてご記入ください。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1510 100.0	414 100.0	374 100.0	722 100.0	103 100.0
1. 役職員向けの標的型攻撃メール訓練、フィッシング訓練	1031 68.3	331 80.0	196 52.4	504 69.8	93 90.3
2. サイバーセキュリティについての研修、eラーニングなど	1133 75.0	337 81.4	241 64.4	555 76.9	98 95.1
3. 技術演習(ログ分析、マルウェア解析、フォレンジック演習など)	171 11.3	81 19.6	22 5.9	68 9.4	36 35.0
4. 組織横断型演習(経営層・広報・法務なども参加)	217 14.4	86 20.8	20 5.3	111 15.4	33 32.0
5. 復旧演習、バックアップデータの復元訓練	182 12.1	66 15.9	32 8.6	84 11.6	28 27.2
6. ペネトレーションテスト(第三者による侵入テスト)	210 13.9	92 22.2	23 6.1	95 13.2	42 40.8
7. レッドチーム演習(攻撃者視点による組織全体での実践演習)	40 2.6	17 4.1	1 0.3	22 3.0	14 13.6
8. その他(自由記述)	34 2.3	11 2.7	5 1.3	18 2.5	3 2.9
9. 特に実施していない	157 10.4	22 5.3	70 18.7	65 9.0	1 1.0

Q14. 監査役等からみた課題など。(自由記述)

Q15. 貴社では、社内外にサイバーインシデントを報告・公表するルートやタイミングなどが定められていますか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1508 100.0	412 100.0	373 100.0	723 100.0	103 100.0
1. 特段の方針等はない	277 18.4	55 13.3	85 22.8	137 18.9	6 5.8
2. インシデント発生の都度、報告・公表する	587 38.9	157 38.1	171 45.8	259 35.8	19 18.4
3. 社内外の共有・報告先や公表すべき時期・内容等が規程化されている	219 14.5	63 15.3	45 12.1	111 15.4	22 21.4
4. 3に加え、規程が社内に周知され、関係者間で確認されている	270 17.9	85 20.6	50 13.4	135 18.7	32 31.1
5. 4に加え、規程が訓練で確認されるなど運用されている、見直しされている	103 6.8	37 9.0	14 3.8	52 7.2	20 19.4
6. その他(自由記述)	52 3.4	15 3.6	8 2.1	29 4.0	4 3.9

■(4) サプライチェーン全体でのセキュリティ対策■

Q16-1. 監査役等として、委託先等のサプライチェーンのサイバーセキュリティ体制や対策などについて、どのようにアプローチしていますか。当てはまるものを選択してください。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1497 100.0	410 100.0	374 100.0	713 100.0	104 100.0
1. 監査役等は確認していない、報告を受けていない	575 38.4	136 33.2	152 40.6	287 40.3	17 16.3
2. 委託先の管理・統括部門に確認する	207 13.8	52 12.7	46 12.3	109 15.3	16 15.4
3. サイバーセキュリティを管理・統括している部門、責任者に確認する	614 41.0	184 44.9	143 38.2	287 40.3	66 63.5
4. 内部監査部門に確認する	336 22.4	113 27.6	77 20.6	146 20.5	34 32.7
5. 取締役会等(経営会議等も含む)におけるサイバーセキュリティをめぐる報告や議論で確認する	344 23.0	122 29.8	66 17.6	156 21.9	52 50.0
6. サイバーセキュリティの外部専門家に確認する	15 1.0	4 1.0	4 1.1	7 1.0	1 1.0
7. 監査役等が直接現場部門に確認する、契約内容を確認する	38 2.5	8 2.0	10 2.7	20 2.8	2 1.9
8. その他(自由記述)	27 1.8	6 1.5	5 1.3	16 2.2	1 1.0

Q16-2. 監査役等が、委託先等のサプライチェーンのサイバーセキュリティ体制や対策などに関して、気掛かりな点、課題または工夫している事項などを記載してください。(自由記述)

【2.サイバーセキュリティへの監査役等の活動】

Q17-1. 監査計画の中にサイバーセキュリティを入れていますか。最も近いものを選択してください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1498 100.0	411 100.0	374 100.0	713 100.0	104 100.0
1. 数年前から監査計画に入れて実施している	275 18.4	93 22.6	55 14.7	127 17.8	48 46.2
2. 1,2年前から監査計画に入れて実施している	230 15.4	70 17.0	48 12.8	112 15.7	21 20.2
3. 監査計画には入れていないが、監査を実施する(予定も含む)	451 30.1	119 29.0	127 34.0	205 28.8	19 18.3
4. 過去年度に監査したため、当年度は(重点的には)実施しない	21 1.4	5 1.2	5 1.3	11 1.5	— —
5. 以前から特に監査対象にはしていない	398 26.6	90 21.9	118 31.6	190 26.6	9 8.7
6. その他(自由記述)	123 8.2	34 8.3	21 5.6	68 9.5	7 6.7

Q17-2. サイバーセキュリティを重点監査項目にしていますか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1071 100.0	313 100.0	248 100.0	510 100.0	95 100.0
1. 重点監査項目である(重点監査項目であったことがある)	518 48.4	187 59.7	105 42.3	226 44.3	71 74.7
2. 重点監査項目にしていない	553 51.6	126 40.3	143 57.7	284 55.7	24 25.3

Q18-1. サイバーセキュリティについて、監査役等は基本的にどのようにアプローチしていますか。主な対象について選択してください。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1095 100.0	320 100.0	253 100.0	522 100.0	95 100.0
1. 経営陣への確認、対話	498 45.5	129 40.3	101 39.9	268 51.3	53 55.8
2. 取締役会等(経営会議等も含む)の報告や議論	543 49.6	189 59.1	121 47.8	233 44.6	66 69.5
3. サイバーセキュリティ対策の責任者への確認	687 62.7	221 69.1	147 58.1	319 61.1	70 73.7
4. サイバーセキュリティリスク管理・統括組織への確認、報告の受領、会議への参加など	627 57.3	217 67.8	100 39.5	310 59.4	83 87.4
5. 内部監査部門からの報告、確認、監査の指示や依頼	533 48.7	185 57.8	117 46.2	231 44.3	65 68.4
6. サイバーセキュリティの外部専門組織への確認	31 2.8	13 4.1	5 2.0	13 2.5	3 3.2
7. 監査役等自身が直接確認する	87 7.9	30 9.4	18 7.1	39 7.5	7 7.4
8. その他(自由記述)	16 1.5	3 0.9	1 0.4	12 2.3	1 1.1

Q18-2. 監査役会(監査等委員会、監査委員会または監事会等)では、サイバーセキュリティについて議論をしていますか。その内容についてご記入ください。(自由記述)

Q18-3. サイバーセキュリティの監査について、内部監査部門との連携がありますか。その内容についてご記入ください。(自由記述)

Q19-1. 今後、サイバーセキュリティについて監査計画に入れる予定はありますか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	394 100.0	89 100.0	116 100.0	189 100.0	9 100.0
1. ある	224 56.9	51 57.3	71 61.2	102 54.0	5 55.6
2. ない	170 43.1	38 42.7	45 38.8	87 46.0	4 44.4

Q19-2. 監査計画に入れていない理由について。(自由記述)

Q20. 監査役等が参考にしているサイバーセキュリティのガイドラインなどがありますか。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1193 100.0	315 100.0	306 100.0	572 100.0	84 100.0
1. サイバーセキュリティ経営ガイドライン(経済産業省)	683 57.3	224 71.1	181 59.2	278 48.6	57 67.9
2. NISTサイバーセキュリティフレームワーク(NIST)	122 10.2	52 16.5	12 3.9	58 10.1	23 27.4
3. 中小企業の情報セキュリティ対策ガイドライン(IPA)	239 20.0	38 12.1	74 24.2	127 22.2	5 6.0
4. ISO/IEC27000シリーズ	143 12.0	31 9.8	45 14.7	67 11.7	5 6.0
5. サプライチェーン強化に向けたセキュリティ対策評価制度(案)(SCS評価制度)	63 5.3	21 6.7	19 6.2	23 4.0	5 6.0
6. その他(自由記述)	317 26.6	63 20.0	70 22.9	184 32.2	21 25.0

Q20. 情報収集や学習の内容について。(自由記述)

Q21. 監査役等からみて、貴社におけるサイバーセキュリティをめぐる課題はどのようなものがありますか。(複数選択可)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1486 100.0	405 100.0	372 100.0	709 100.0	102 100.0
1. 経営陣の意識、経営リスクとしての認識	556 37.4	140 34.6	151 40.6	265 37.4	21 20.6
2. 取締役会等(経営会議等も含む)におけるサイバーセキュリティの報告や議論の状況	444 29.9	128 31.6	120 32.3	196 27.6	17 16.7
3. サイバーセキュリティの管理・統括部門、責任者	422 28.4	101 24.9	117 31.5	204 28.8	17 16.7
4. 現場部門、従業員の教育、研修	632 42.5	152 37.5	164 44.1	316 44.6	37 36.3
5. サイバーセキュリティ監査(内部監査部門の監査、IT部門等の監査、外部専門組織の監査など)	512 34.5	151 37.3	124 33.3	237 33.4	27 26.5
6. サイバーセキュリティを担当する人材の育成、人材獲得	750 50.5	227 56.0	171 46.0	352 49.6	72 70.6
7. サイバーセキュリティの外部専門組織との提携	248 16.7	70 17.3	60 16.1	118 16.6	17 16.7
8. サイバーセキュリティの対策の予算・費用、保険	353 23.8	100 24.7	90 24.2	163 23.0	26 25.5
9. サイバーインシデントを想定した緊急対応計画、体制、訓練	629 42.3	188 46.4	159 42.7	282 39.8	46 45.1
10. グループ会社のリスク評価、セキュリティ対策等	543 36.5	238 58.8	121 32.5	184 26.0	66 64.7
11. 委託先等のサプライチェーンのリスク評価、セキュリティ対策等	568 38.2	194 47.9	121 32.5	253 35.7	63 61.8
12. その他(自由記述)	23 1.5	8 2.0	4 1.1	11 1.6	2 2.0
13. 特にない	24 1.6	4 1.0	4 1.1	16 2.3	1 1.0

Q21. 課題の内容、監査役等の対応、工夫など。(自由記述)

【3.サイバーインシデント発生後の対応】

Q22. 貴社では、事業に一定程度の影響を与えたサイバー攻撃(不正アクセス等)が発生したことがありますか。サイバー攻撃により、重要業務の停止や大幅遅延、個人情報等の漏えいの懸念、外部通報・公表・当局への報告の検討、多額の損失や復旧費用などが生じた場合を指します。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1490 100.0	409 100.0	372 100.0	709 100.0	104 100.0
1. ある	277 18.6	129 31.5	48 12.9	100 14.1	38 36.5
2. ない	1213 81.4	280 68.5	324 87.1	609 85.9	66 63.5

Q23. 当該インシデントの主な原因は何でしたか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	270 100.0	126 100.0	46 100.0	98 100.0	38 100.0
1. マルウェア攻撃(ランサムウェア、ウイルス、ワーム、トロイの木馬 等)	203 75.2	105 83.3	34 73.9	64 65.3	33 86.8
2. フィッシング	31 11.5	10 7.9	5 10.9	16 16.3	3 7.9
3. サービス拒否(DoS/DDoS)攻撃	11 4.1	3 2.4	1 2.2	7 7.1	1 2.6
4. その他(自由記述)	25 9.3	8 6.3	6 13.0	11 11.2	1 2.6

Q24. 当該インシデントが発生した会社はどこに該当しますか。例えばランサムウェアの場合、最初に侵入された会社をご回答ください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	271 100.0	126 100.0	46 100.0	99 100.0	38 100.0
1. 自社(自社が親会社の場合も含む)	106 39.1	27 21.4	28 60.9	51 51.5	5 13.2
2. 親会社	4 1.5	1 0.8	1 2.2	2 2.0	— —
3. 国内グループ会社	42 15.5	26 20.6	6 13.0	10 10.1	8 21.1
4. 海外グループ会社	99 36.5	70 55.6	7 15.2	22 22.2	24 63.2
5. 委託先などのサプライチェーン	20 7.4	2 1.6	4 8.7	14 14.1	1 2.6

Q25. 監査役等は、当該インシデントの第一報をどのタイミングで把握しましたか。会社がサイバーインシデントの発生を把握してから、監査役等が第一報を受けるまでの間をご回答ください。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	270 100.0	125 100.0	46 100.0	99 100.0	37 100.0
1. 発生当日～1日後	129 47.8	51 40.8	26 56.5	52 52.5	18 48.6
2. 2～3日後	58 21.5	33 26.4	11 23.9	14 14.1	5 13.5
3. 1週間以内	45 16.7	24 19.2	4 8.7	17 17.2	8 21.6
4. 2週間以内	12 4.4	6 4.8	2 4.3	4 4.0	2 5.4
5. 1か月以内	7 2.6	4 3.2	2 4.3	1 1.0	2 5.4
6. 1か月超	2 0.7	2 1.6	— —	— —	1 2.7

7. 不明、その他	17 6.3	5 4.0	1 2.2	11 11.1	1 2.7
-----------	-----------	----------	----------	------------	----------

Q26. 監査役等は、当該インシデントの第一報を誰から受けましたか。(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	271 100.0	127 100.0	46 100.0	98 100.0	38 100.0
1. サイバーセキュリティ対策の責任者	64 23.6	32 25.2	11 23.9	21 21.4	6 15.8
2. サイバーセキュリティを管理・統括している部門	128 47.2	51 40.2	27 58.7	50 51.0	13 34.2
3. 内部監査部門	13 4.8	6 4.7	1 2.2	6 6.1	1 2.6
4. 現場部門	25 9.2	13 10.2	3 6.5	9 9.2	7 18.4
5. 子会社(グループ会社)の監査役	5 1.8	4 3.1	1 2.2	－ －	1 2.6
6. その他(自由記述)	36 13.3	21 16.5	3 6.5	12 12.2	10 26.3

Q27. 当該インシデントの発覚から復旧までに、どの程度の期間がかかりましたか。(1つ選択) 製造やサービスなどが再開され、通常の業務運営にほぼ戻った状態までの間をご回答ください。	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	267 100.0	125 100.0	46 100.0	96 100.0	36 100.0
1. 1か月以内	156 58.4	68 54.4	28 60.9	60 62.5	17 47.2
2. 2か月以内	31 11.6	18 14.4	6 13.0	7 7.3	5 13.9
3. 3か月以内	23 8.6	12 9.6	5 10.9	6 6.3	5 13.9
4. 半年以内	30 11.2	15 12.0	5 10.9	10 10.4	5 13.9
5. 1年以内	6 2.2	5 4.0	－ －	1 1.0	2 5.6
6. 1年超	1 0.4	－ －	－ －	1 1.0	－ －
7. 不明、その他	20 7.5	7 5.6	2 4.3	11 11.5	2 5.6

Q28. 監査役等からみて、インシデントの発生から復旧までの執行側の対応にどのような課題がみられましたか。(自由記述)

Q29. 復旧後、サイバーセキュリティリスク管理体制などについて見直された事項はありましたか。(自由記述)

Q30. 監査役等は、インシデントの対策本部等にどのように関わっていましたか。また、インシデントを通して、監査役等の監査活動にどのような変化がありましたか。(自由記述)

【回答会社の属性】

F1. 機関設計(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. 監査役(会)設置会社	1123 73.5	217 51.7	224 58.9	682 93.7	58 55.8
2. 監査等委員会設置会社	365 23.9	182 43.3	154 40.5	29 4.0	28 26.9
3. 指名委員会等設置会社	24 1.6	21 5.0	2 0.5	1 0.1	17 16.3
4. 監事設置法人	16 1.0	-	-	16 2.2	1 1.0

F2. 上場区分(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. プライム市場	420 27.5	420 100.0	-	-	76 73.1
2. スタンダード市場	259 17.0	-	259 68.2	-	-
3. グロース市場	81 5.3	-	81 21.3	-	-
4. その他上場	40 2.6	-	40 10.5	-	-
5. 非上場	728 47.6	-	-	728 100.0	28 26.9

F3. 資本金区分(1つ選択)	全 体	F2. 上場区分			F3. 資本金区分
		1. プライム市場	2・3・4(スタンダード、グロース、その他上場)	5. 非上場	500億円以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. 1億円未満	218 14.3	6 1.4	38 10.0	174 23.9	-
2. 1億円以上5億円未満	321 21.0	10 2.4	79 20.8	232 31.9	-
3. 5億円以上10億円未満	153 10.0	15 3.6	70 18.4	68 9.3	-
4. 10億円以上30億円未満	257 16.8	52 12.4	116 30.5	89 12.2	-

5. 30億円以上50億円未満	127 8.3	41 9.8	45 11.8	41 5.6	— —
6. 50億円以上100億円未満	133 8.7	84 20.0	23 6.1	26 3.6	— —
7. 100億円以上500億円未満	205 13.4	136 32.4	9 2.4	60 8.2	— —
8. 500億円以上	104 6.8	76 18.1	— —	28 3.8	104 100.0
9. なし(監事設置法人)	10 0.7	— —	— —	10 1.4	— —

F4-1. 業種区分(1つ選択)	全 体	F2. 上場区分			F3. 資本金 区分
		1. プライ ム市場	2・3・4(ス タダー ド、グロー ス、その他 上場)	5. 非上 場	500億円 以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. 製造業	550 36.0	228 54.3	152 40.0	170 23.4	46 44.2
2. 非製造業	978 64.0	192 45.7	228 60.0	558 76.6	58 55.8

F4-2. 業種分類(1つ選択)	全 体	F2. 上場区分			F3. 資本金 区分
		1. プライ ム市場	2・3・4(ス タダー ド、グロー ス、その他 上場)	5. 非上 場	500億円 以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. 農業・林業・漁業・鉱業	15 1.0	7 1.7	2 0.5	6 0.8	1 1.0
2. 建設業	74 4.8	20 4.8	18 4.7	36 4.9	1 1.0
3. 製造業	477 31.2	212 50.5	128 33.7	137 18.8	42 40.4
4. 電気・ガス・熱供給・水道業	41 2.7	14 3.3	2 0.5	25 3.4	8 7.7
5. 情報通信業	178 11.6	27 6.4	54 14.2	97 13.3	3 2.9
6. 運輸業	56 3.7	16 3.8	6 1.6	34 4.7	12 11.5
7. 卸売業・小売業	197 12.9	50 11.9	70 18.4	77 10.6	4 3.8
8. 金融業・保険業	128 8.4	30 7.1	7 1.8	91 12.5	24 23.1
9. 不動産業・物品賃貸業	69 4.5	10 2.4	15 3.9	44 6.0	3 2.9
10. 学術研究・専門・技術サービス業	25 1.6	2 0.5	5 1.3	18 2.5	— —
11. 宿泊業・飲食サービス業	17 1.1	4 1.0	6 1.6	7 1.0	— —
12. 生活関連サービス業・娯楽業	12 0.8	1 0.2	3 0.8	8 1.1	— —

13. 教育・学習支援業	7 0.5	－ －	3 0.8	4 0.5	－ －
14. 医療・福祉	23 1.5	2 0.5	9 2.4	12 1.6	－ －
15. 複合サービス事業(郵便・農協・生協・協同組合など)	7 0.5	－ －	－ －	7 1.0	1 1.0
16. その他サービス業	154 10.1	22 5.2	41 10.8	91 12.5	4 3.8
17. その他	48 3.1	3 0.7	11 2.9	34 4.7	1 1.0

F5-1. 貴社のグループにおける位置付け(1つ選択)	全 体	F2. 上場区分			F3. 資本金 区分
		1. プライ ム市場	2・3・4(ス タンダー ド、グロ ース、その他 上場)	5. 非上 場	500億円 以上
全 体	1528 100.0	420 100.0	380 100.0	728 100.0	104 100.0
1. 最終親会社である	861 56.3	399 95.0	285 75.0	177 24.3	85 81.7
2. 子会社である	489 32.0	14 3.3	33 8.7	442 60.7	18 17.3
3. 親会社・子会社はない	178 11.6	7 1.7	62 16.3	109 15.0	1 1.0

F5-2. グループ会社の総数(1つ選択)	全 体	F2. 上場区分			F3. 資本金 区分
		1. プライ ム市場	2・3・4(ス タンダー ド、グロ ース、その他 上場)	5. 非上 場	500億円 以上
全 体	861 100.0	399 100.0	285 100.0	177 100.0	85 100.0
1. 1～5社	352 40.9	59 14.8	178 62.5	115 65.0	8 9.4
2. 6～10社	156 18.1	64 16.0	63 22.1	29 16.4	4 4.7
3. 11～50社	241 28.0	171 42.9	42 14.7	28 15.8	15 17.6
4. 51～100社	51 5.9	46 11.5	2 0.7	3 1.7	13 15.3
5. 101社以上	61 7.1	59 14.8	－ －	2 1.1	45 52.9