2026 年 10 月 30 日

SOMPOリスクマネジメント

損保ジャパンＲＭレポート｜　293

コーポレートガバナンス・コード 2026 年改訂版から考えるこれからのリスクガバナンス

～ リスク情報を経営判断につなげるために ～

原　敬徳　Takanori Hara

取締役常務執行役員

首席コンサルタント

概要

2026 年 7 月に改訂されたコーポレートガバナンス・コードを、リスクマネジメントの視点から読み解く。コーポレートガバナンス・コード（2026 年改訂版）の原則 4-4 の解釈指針やパブリックコメントを踏まえ、取締役会、経営会議、内部監査、リスク管理部門の役割と、機関設計ごとのリスクガバナンス体制を整理する。さらに、取締役会の実効性評価、サステナビリティ、サイバーリスク、データガバナンス、AI 時代の判断責任と監督体制を取り上げ、リスク情報を経営判断や取締役会の監督にどう生かすかという観点から、これからのコーポレートガバナンスの在り方を考察する。

目次

概要 1
はじめに 2
1. CG コード 2026 年改訂版の概要と実務上の論点 2
　1.1. CG コード改訂の要点とリスクガバナンス上の主要論点 2
　1.2. パブリックコメントから読み解く 5 つの実務論点 4
2. 経営判断と監督を支えるリスクガバナンス体制 5
　2.1. リスクガバナンスを支える各機関・部門の役割 5
　2.2. 機関設計に応じたリスクガバナンスの特徴と留意点 5
　2.3. 取締役会の実効性評価を通じたリスクガバナンスの強化 7
3. 変化する経営課題とリスクガバナンスの実践 8
　3.1. サステナビリティ課題を経営判断につなげる 8
　3.2. サイバーリスクに備える経営判断とデータガバナンス 8
　3.3. AI 活用における経営の判断責任と監督体制 9
おわりに 11

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

はじめに

2026 年 7 月、コーポレートガバナンス・コードが 5 年ぶりに改訂された（以下、CG コード改訂版）[1]。今回の改訂では、各社が自社の状況に応じて、ガバナンスを実際に機能させているかが改めて問われている。加えて、これからのリスクマネジメントには、リスクを抑える「守り」だけでなく、必要なリスクを取りながら、成長や中長期的な企業価値の向上につなげていく役割も求められる。そのためには、リスクを洗い出して経営に報告するだけでなく、得られた情報を投資や資源配分、事業の継続・撤退などの経営判断に生かし、具体的な行動につなげなければいけない。

本レポートは、大きく三つのテーマで構成している。第一に、CG コード改訂版やパブリックコメントを踏まえ、リスクマネジメントに何が求められているのかを整理する。第二に、取締役会、経営会議、内部監査、取締役会事務局、リスク管理部門の役割や機関設計、取締役会の実効性評価を取り上げ、経営判断と監督を支えるリスクガバナンスの在り方を考える。第三に、サステナビリティ、サイバーセキュリティとデータガバナンス、AI ガバナンスを取り上げ、変化する経営課題にどう向き合うべきかを検討する。誰が判断し、誰が監督し、リスク情報をどのように経営判断につなげるのか。こうした観点から、これからのリスクガバナンスの在り方を考察したい。

1. CG コード 2026 年改訂版の概要と実務上の論点

1.1. CG コード改訂の要点とリスクガバナンス上の主要論点

今回の CG コード改訂版では、従来の補充原則が廃止・再整理され、コンプライ・オア・エクスプレインの対象は、より基本的な原則に絞られた。あわせて、各原則をどう理解し、実際の経営やガバナンスにどう生かすかを示す「解釈指針」が新たに設けられた。解釈指針そのものは、コンプライ・オア・エクスプレインの直接の対象ではないが、各原則を実際に機能させるための手引きと位置付けられている。

リスクマネジメントの観点から特に注目したいのが、原則 4-4 の解釈指針である。そこでは、内部統制や全社的なリスク管理には、リスクを抑えるだけでなく、経営陣が必要なリスクを取ることを支える役割もあるとされている。さらに、今回の改訂では、サイバーセキュリティ、サプライチェーンの途絶、技術情報の流出なども、リスク管理体制を整えるうえで考慮すべき事項として例示された。

こうした改訂からは、新たなリスクへの対応に加え、既存のリスク管理体制が経営判断を支える仕組みとして、実際に機能しているかを重視する考え方が読み取れる。この点を踏まえ、表 1 では、適切なリスクテイク、全社的リスク管理、取締役会機能の強化という 3 つの論点について、企業が見直すべき実務と、今後目指したい運用の方向性を整理した。

[1] 金融庁・株式会社東京証券取引所,「コーポレートガバナンス・コード（2026 年改訂版）」,（アクセス日：2026-10-19）, https://www.fsa.go.jp/news/r7/singi/20260721/01.pdf

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

表 1　CG コード改訂版を踏まえたリスクマネジメントの見直しの方向[2]

改訂の論点	見直したい実務の例	目指す運用	リスクマネジメントとしての意味
適切なリスクテイク	損失防止やリスク抑制に議論が偏る	成長機会とそれに伴うリスクを評価し、リスクを取る条件や対応策を検討する	リスクの抑制と適切なリスクテイクの両面から、経営判断を支える
全社的リスク管理	リスクの集計と報告で終わる	重要リスクの把握から対応状況、残存リスクの確認までをつなぎ、取締役会が管理体制の運用状況を監督する	全社的リスク管理を取締役会の重要な監督事項とする
取締役会機能の強化	報告や承認が中心で、戦略との関係まで十分に議論できない	経営戦略、経営資源の配分、重要リスクを関連付けて議論する	リスクを踏まえた戦略的判断と、その実行状況の監督につなげる

CG コード改訂版は、基本原則、原則、そしてそれらを実践するための解釈指針で構成されている。ここでは、その中からリスクマネジメントやガバナンス体制と特に関わりが深いと筆者が考える原則を取り上げる（表 2）。読者が各章の内容と CG コード改訂版の原則との関係を理解しやすいよう、主な原則の概要と、それぞれに関連する章を次表にまとめた。本文を読み進める際に、各章で取り上げる論点がどの原則と結び付いているのかを確認する手掛かりとして、活用していただきたい。

表 2　本レポートで取り上げる CG コード改訂版の主な原則の対比表[3]

原則	CG コードの概要と本レポートで取り上げた要旨	本レポートで扱う章
基本原則 4	• 取締役会が戦略の方向性を示し、経営陣が適切にリスクを取れる環境を整えることを求める原則。 • 本レポートでは、リスク管理を経営の挑戦を支える基盤として捉える。	1. 2.
原則 4-2	• 経営資源の配分が戦略・計画に照らして適切か、取締役会が継続的に検証することを求める原則。 • 本レポートでは、各機関・部門の役割分担や機関設計の違いに応じて、重要リスクへの対応を取締役会がどう検証するかを取り上げる。	2.
原則 4-4 と解釈指針	• 取締役会による内部統制や全社的リスク管理体制の整備を求め、解釈指針では内部監査部門の活用と運用状況の監督を示している。 • 本レポートでは、サイバーや AI に関する新たなリスクへの対応も含め、取締役会と内部監査がリスク管理体制の実効性をどう確かめるかを扱う。	1. 2. 3. おわりに
原則 4-5 と解釈指針	• サステナビリティ対応、人権尊重、自然災害などへの危機管理を求める原則。 • 本レポートでは、サステナビリティとリスクマネジメントの関係を整理する。	3.
原則 4-6 と解釈指針	• 監査役・監査役会が、独立した立場から株主への受託者責任を踏まえて判断し、取締役会や経営陣に積極的に意見を述べることを求める原則。 • 社外取締役との連携も重視される。	2.
原則 4-13 と解釈指針	• 取締役会全体の実効性を毎年評価し、その概要を開示することを求める原則。 • 本レポートでは、リスクガバナンスの観点を評価に取り入れる方法を検討する。	2.
原則 4-14 と解釈指針	• 解釈指針では、内部監査部門から取締役会や監査役会等への直接報告の仕組みや、取締役会の審議を支える事務局機能の強化を示している。	2.

[2] 金融庁・株式会社東京証券取引所「コーポレートガバナンス・コード（2026 年改訂版）」を基に当社作成
[3] 金融庁・株式会社東京証券取引所「コーポレートガバナンス・コード（2026 年改訂版）」を基に当社作成

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

1.2. パブリックコメントから読み解く 5 つの実務論点

今回の改訂案については、2026 年 4 月から 5 月にかけて事前に意見募集が行われ、147 の個人・団体から意見が寄せられた。金融庁と東京証券取引所は、その結果を「改訂案に対するご意見の概要及びそれに対する考え方」[4]（以下、パブリックコメント）として公表している。

ここでは、その中から、リスクマネジメントとガバナンスを考えるうえで、筆者が特に注目した 5 つの論点を取り上げる。選定にあたっては、リスクマネジメントを経営判断にどう結び付けるか、取締役会や経営陣にどのような役割が求められるかなど、企業実務との関わりを重視した。

以下では、寄せられた意見と、それに対する金融庁・東京証券取引所の考え方を、原文の趣旨を損なわない範囲で要約している。パブリックコメントは、条文だけでは読み取りにくい改訂の狙いや、実際の運用を考えるうえでの有用な手掛かりとなる。なお、正確な内容については、公表されている原文を参照していただきたい。

表 3　パブリックコメントにおける主要論点と筆者の着眼点[5]

意見 No.	掲載頁	論点	提出意見の概要	東京証券取引所の考え方（要旨）	筆者の着眼点
519	287 頁	「リスク最小化」と適切なリスクテイク	リスク管理を「リスクの最小化」と表現すると、過度なリスク回避を促し、適切なリスクテイクを妨げるのではないか。	「リスクの最小化」は過度なリスク回避を意味しない。全社的リスク管理や内部統制による適切なリスク管理は、経営陣のリスクテイクを支えるものである。	リスク管理では、案件を進める場合も、止める場合もある。取るべきリスクと避けるべきリスクを見極め、経営が根拠を持って判断できる状態をつくることが必要。
520	287 頁	「適切なリスク管理体制」の評価	適切なリスク管理体制を何によって判断するのか。共通の評価基準やプロセスを示すべきではないか。	コードは原則主義であり、一律の評価基準は定めない。取締役会が自社の重要リスクを認識し、体制の実効性を自主的に検証、改善することが重要である。	共通の正解がなくても評価はできる。重要リスクの伝達、資源配分、残存リスクの再評価が適切に行われているかを確認すべきである。
517	285 から 286 頁	取締役会と内部監査の関係	内部監査を取締役会の監督機能の代替手段として用いることで、その独立性や専門性が損なわれないよう、役割の違いを明確にすべきではないか。	内部監査は取締役会の監督責任を代替しない。取締役会自身が独立した立場で判断、関与するとともに、内部監査部門と連携する必要がある。	内部監査で「重大な問題なし」とされても、それだけで監督が十分とはいえない。取締役会は監査範囲や対象外領域、改善状況まで確認すべきである。
727	383 から 384 頁	取締役会事務局の機能強化	取締役会事務局の役割を強化すると、本来取締役会が負うべきガバナンス上の責任まで事務局に移ることにならないか。	意思決定主体は取締役会であり、事務局は議題設定、会議運営、情報提供などを通じて、その機能発揮を支援する役割を担う。	事務局の機能強化は資料作成の充実にとどまらない。重要リスクや残存リスク、未解決の論点など、取締役会が議論すべき事項を適切に提示する必要がある。
521	287 から 288 頁	サイバーリスク等の継続的な監視	サイバーリスクのように急速に変化するリスクについて、一時点の評価だけで十分なのか。継続的な監視が必要ではないか。	特定のリスクを取り巻く環境が変化した場合には、その変化に対する継続的なモニタリングや対応を行うべきである。	評価回数だけで実効性は決まらない。定期評価に加え、重要な前提の変化に応じて、リスクと経営判断を見直す仕組みが必要。

[4] 金融庁・株式会社東京証券取引所,「改訂案に対するご意見の概要及びそれに対する考え方」,（アクセス日：2026-10-19）,https://www.fsa.go.jp/news/r7/singi/20260721/06.pdf

[5] 金融庁・株式会社東京証券取引所「改訂案に対するご意見の概要及びそれに対する考え方」を基に当社作成

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

2. 経営判断と監督を支えるリスクガバナンス体制

2.1. リスクガバナンスを支える各機関・部門の役割

今回の CG コード改訂版では、ガバナンスの体制を整えるだけでなく、経営判断や取締役会の監督が実際に機能しているかが重視されている。原則 4-4 では、内部統制や全社的なリスク管理体制を整備することを取締役会の責務としている。また、その解釈指針では、サイバー攻撃やサプライチェーンの途絶、技術情報の流出などへの対応についても触れている。

こうした考え方を実務に落とし込むには、それぞれの部門や機能が担う役割を明確にする必要がある。事業部門は日常的にリスクを管理し、リスク管理部門はそれらを全社的に把握・評価する。経営会議は、社内の権限規程に応じて、重要リスクへの対応方針や経営資源の配分について審議・判断する。取締役会は、経営として引き受けているリスクと管理体制が適切に機能しているかを監督する。内部監査はその仕組みを独立した立場から評価し、取締役会事務局は、必要な情報が取締役会の審議につながるよう支える。大切なのは、こうした役割が個別に分断されることなく、リスク情報が経営判断から監督まで一連の流れとしてつながり、実際に機能することである。

表 4　リスクガバナンスの体制：機能・部門別の主な役割と留意点[6]

機能・部門	主な役割	リスク管理上の重要な論点	留意点
取締役会	重要リスクとリスク管理体制の運用状況を監督	経営が引き受けているリスクは適切か	個別対策の実行主体にならない
経営会議	重要リスクへの対応方針、資源配分の判断	何を実施し、何を受容するのか	「対応中」のまま判断を先送りしない
事業部門	事業遂行と日常的なリスク管理	自らの事業に伴うリスクを管理できているか	リスク管理部門に責任を転嫁しない
リスク管理部門	全社的な把握、評価、問題提起	経営が判断すべきリスクは何か	単なる集計・報告機能にしない
内部監査部門	リスク管理体制の独立的評価	内部統制の 3 ラインモデルについて、第一線、第二線のリスク管理は実際に機能しているか	自ら運営した仕組みを自ら保証しない
取締役会事務局	取締役会アジェンダ、情報提供、審議支援	取締役会で何を問うべきか	資料作成・会議運営だけに限定しない

2.2. 機関設計に応じたリスクガバナンスの特徴と留意点

東証「コーポレート・ガバナンス白書 2025」[7]（図 1）によると、東証上場会社の機関設計は、監査役会設置会社が 55.2%、監査等委員会設置会社が 42.3%、指名委員会等設置会社が 2.5%となっている。CG コード改訂版の基本原則 4 の解釈指針では、どの機関設計であっても、それぞれの機関が実質的に機能することが求められている。重要なのは組織の形そのものだけではなく、リスク情報がどのように共有され、誰が判断し、誰が監督しているのかである。こうした視点から、主要な機関設計ごとの特徴を見ていきたい。

[6] 金融庁・株式会社東京証券取引所「コーポレートガバナンス・コード（2026 年改訂版）」を基に当社作成
[7] 株式会社東京証券取引所,「コーポレート・ガバナンス白書 2025」より一部抜粋,（アクセス日：2026-10-19）, https://www.jpx.co.jp/equities/listing/cg/tvdivq0000008jb0-att/um3qrc000001noil.pdf

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

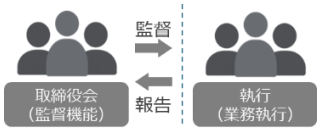
図 1　組織形態の採用比率の推移（東証上場会社）[7]

機関設計によって、取締役会、執行側、監査機関などが担う役割や、重要なリスク情報が共有される経路は異なる。以下では、三つの機関設計について、それぞれの特徴や強み、リスク管理上の課題を検討したい。

筆者も企業のガバナンス体制を確認する機会があるが、会議体の数や名称だけでは、ガバナンスが実際に機能しているかどうかは分からない。特に重視しているのは、経営陣や取締役会が判断するために必要なリスク情報が、途中で滞ることなく、関係する部門や担当者に適切に伝わっているかという点である。また、経営判断の前提となる状況が変化したとき、その変化が会議で適切に取り上げられ、必要に応じて判断を見直せる仕組みになっているかも確認している。

なお、以下は各機関設計の一般的な特徴を踏まえ、筆者がリスクガバナンスの観点から整理したものであり、実際の機能や課題は各社の運用によって異なる。

表 5　機関設計ごとのリスクマネジメントの特徴・ポイント・留意点[8]

項目	監査役会設置会社	監査等委員会設置会社	指名委員会等設置会社
基本的な特徴			
	独立した監査役による監査	監査等委員が取締役として議決に参加	監督と執行の役割分担を明確化
メリット	監査役による独立した現場情報収集	監査情報を取締役会の監督に活用しやすい	執行への権限委譲とモニタリングに適する
懸念点	監査役の指摘と取締役会監督の分断	監査等委員会、取締役会、内部監査の役割の分断	権限委譲後の重大リスクの情報不足
リスクマネジメント上のポイント	監査で把握した重大リスクを経営判断に活かす	内部監査と連携し重大リスクを監督につなぐ	委任範囲、リスクアペタイト、残存リスクの監督
取締役会事務局に求められる機能	監査役、社外取締役、執行側の情報連携	監査等委員会と取締役会の情報連携	執行と監督の情報非対称性を緩和

[8] e-Gov 法令検索,「会社法（平成 17 年法律第 86 号）」を参照し当社作成,（アクセス日：2026-10-19）, https://laws.e-gov.go.jp/law/417AC0000000086

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

2.3. 取締役会の実効性評価を通じたリスクガバナンスの強化

リスクガバナンスを強化するうえでは、取締役会の実効性評価を活用することも有効である。CG コード改訂版の原則 4-13 では、取締役会全体の実効性について毎年分析・評価を行い、その概要を開示することが求められている。今回の改訂を機に、重要リスクと経営戦略への影響を十分に把握できているか、適切なリスクテイクを監督できているか、新たなリスクについて必要な情報提供や議論が行われているかといった観点から、実効性評価の項目を見直すことも必要だ。

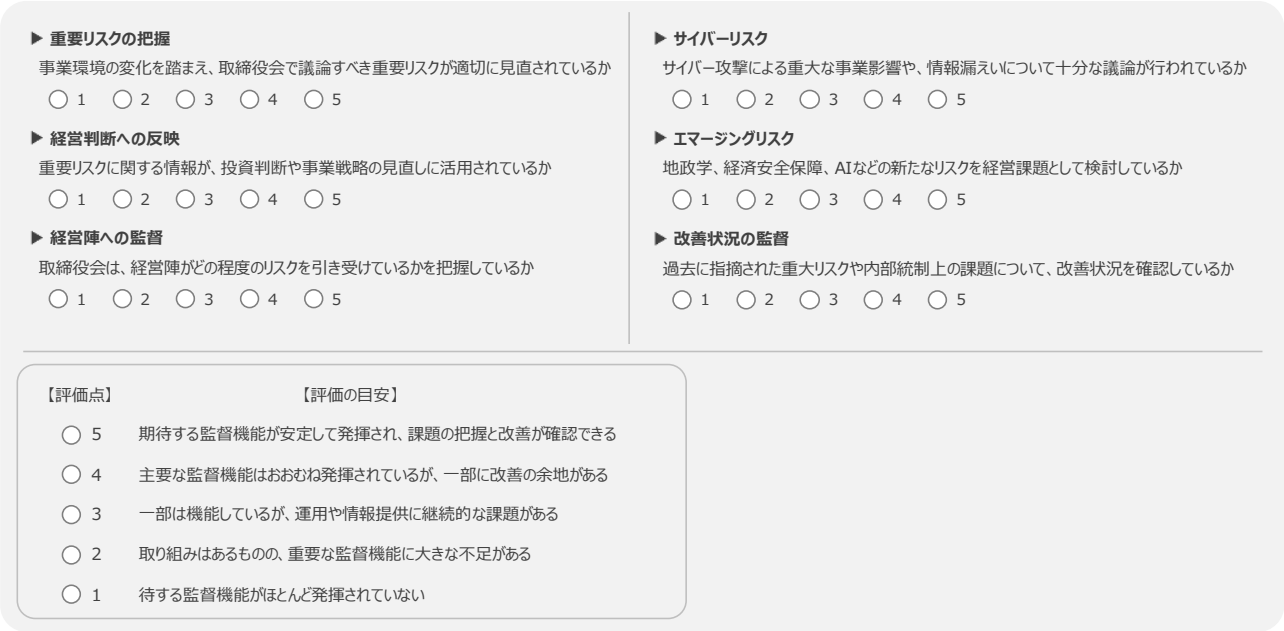


図 2　リスクガバナンスに関する実効性評価項目の一例[9]

筆者が支援先企業の取締役会の実効性評価を行う際には、こうした観点から評価している。5 段階評価などを用いることもあるが、点数の高低だけで判断することはない。前年と比べて評価がどう変化したのか、社内取締役と社外取締役の間で認識に違いがないかを確認し、議事録や実際の意思決定の記録とも照らし合わせながら評価している。

評価を通じて明らかになった課題は、翌年度の取締役会運営に反映させる必要がある。例えば、リスク情報の提供方法を見直す、審議事項や年間の審議計画を改めるといった対応である。そして翌年度の実効性評価で、こうした対応によって実際に改善が進んだかを確認する。このように、評価と改善を繰り返していくことが、取締役会のリスクガバナンスを真に実効的なものにすると考えている。

[9] 当社作成

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

3. 変化する経営課題とリスクガバナンスの実践

3.1. サステナビリティ課題を経営判断につなげる

ここでは、サステナビリティとガバナンスの関係について考えたい。筆者はクライアントから、「サステナビリティ委員会とリスクマネジメント委員会を統合すべきか」と相談を受けることがある。答えは企業によって異なるが、まず見るべきなのは委員会の形ではない。そこで何が議論され、その結果が経営会議や取締役会の判断にどうつながっているかである。

気候変動や人権、人的資本は、事業上のリスクであると同時に、成長や競争力にも関わる経営課題である。脱炭素投資であれば、排出削減量だけでなく、投資採算や規制動向、将来の競争力まで含めて判断する必要がある。人権上の懸念がある調達先についても、改善を働きかけるのか、取引関係を見直すのかという経営判断が求められる。

こうした課題を見る視点は、サステナビリティ部門とリスク管理部門で異なる。前者は気候変動や人権、人的資本などの観点から、後者は事業継続や財務影響、リスク許容度などの観点から評価するため、結論が分かれることもある。問題は、その違いではなく、なぜ評価が分かれたのかを整理しないまま、それぞれが別々に経営へ報告してしまうことである。まず事実や判断の前提をそろえ、評価が分かれた理由を明らかにしたうえで、経営会議が共通の情報を基に判断できる状態にしておく必要がある。

取締役会には、その経営判断を監督する役割がある。各委員会から報告を受けるだけでなく、経営陣がなぜその対応を選び、どのようなリスクを許容したのかまで確認する必要がある。今回の CG コード改訂を踏まえても、大切なのは委員会を統合するか分けるかという形式ではない。議論が経営判断につながり、その判断を取締役会が適切に監督できる仕組みになっているかである。

3.2. サイバーリスクに備える経営判断とデータガバナンス

サイバーリスクも、経営判断との関係が問われる重要な課題である。現在、企業や公共機関では、サイバー攻撃による情報漏えいや事業停止が相次いでいる。被害は個人情報や営業秘密の流出にとどまらない。基幹システムが停止すれば、製造、物流、販売、決済など、幅広い業務に影響が及ぶこともある。

CG コード改訂版の原則 4-4 の解釈指針でも、サイバーセキュリティリスクへの対応が明記された。その背景には、サイバー攻撃がサプライチェーンの途絶や技術情報の流出と同様に、事業継続や企業価値に大きな影響を与えるリスクとして捉えられていることがある。経営陣は、こうしたリスクを踏まえ、何を守り、どの事業を優先するのかを平時から考えておく必要がある。

【筆者の経験談】

筆者も企業の経営層やリスク管理担当者と議論する中で、当初はサイバー対策の話だったものが、最後には「どの事業を止めてはいけないのか」「情報が漏えいした場合、いつ顧客に説明するのか」「どこまで事業を継続するのか」といった経営判断の問題に行き着く場面を何度も経験してきた。

こうした判断を、事故が起きてから初めて議論するのでは遅い。経営陣は、漏えいすれば重大な影響を及ぼす情報や、停止すれば事業継続が難しくなるシステムを把握しておく必要がある。そのうえで、どの程度の事業停止まで許容するのかを、あらかじめ決めておくことが求められる。

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

サイバーリスクを考えるうえでは、情報をどう守るかだけでなく、そもそも何を保有するのかという視点も欠かせない。サイバー攻撃による大規模な個人情報漏えいが相次ぐ中、企業のデータガバナンスも、情報の保有そのものを見直す段階に来ている。企業はこれまで、不正アクセスや情報漏えいを防ぐ安全管理を中心に対策を重ねてきた。しかし、サイバー攻撃を完全に防ぐことは難しく、防御を強化し続けるだけでは、被害を抑えるにも限界がある。

個人情報についても同様である。氏名、年齢、住所、電話番号など、取得時には必要だった情報を、今も保有し続ける必要があるのか、改めて問い直す必要がある。個人情報保護法[10]も、個人データを利用する必要がなくなったときは、遅滞なく消去するよう努めることを定めている。もちろん、法令や事業上の理由で、一定期間の保有が必要な情報もある。だからこそ企業には、何を取得し、何を持たず、いつ手放すのかまで含めて判断することが求められる。

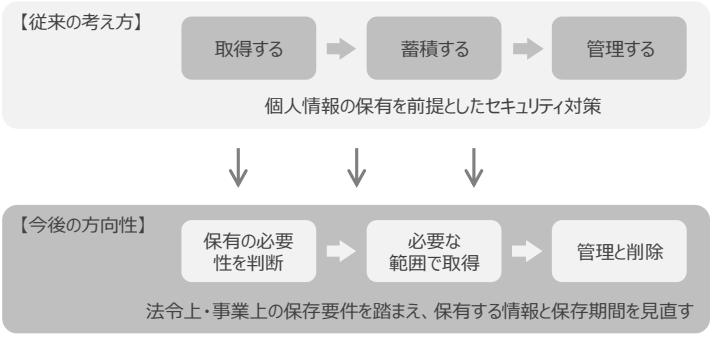


図 3　データガバナンスは保有の必要性まで見直す[11]

今後、個人情報の管理は、単に情報を安全に守るだけでは済まなくなるだろう。企業がどのような情報を保有し、それに伴うリスクをどこまで引き受けるのかという経営判断の問題であり、顧客との信頼関係や取締役会による監督にも関わってくる。相次ぐ情報漏えい事案を契機に、企業は情報を安全に管理するだけでなく、そもそも保有し続ける必要があるのかを見直すべきである。こうした考え方をデータガバナンスに取り入れ、情報を保有すること自体を経営課題として捉えていく必要がある。

3.3. AI 活用における経営の判断責任と監督体制

続いて、AI ガバナンスと経営の判断責任についても考えたい。AI が経営判断に深く関わるようになっても、最終的に判断し、その責任を引き受けるのは人である。ただし、判断の結果が悪かったからといって、直ちに法的責任を負うわけではない。個々の取締役の責任は、権限や情報収集の状況、判断に至る過程などによって異なる。

CG コード改訂版でも、取締役会による実効的な監督や適切な情報の確保が重視されている。AI を経営判断に利用する場合も、そのリスクを把握し、どこまで許容するのかを明確にしたうえで、経営陣が何を根拠に判断したのかを説明できることが求められる。そして、取締役会には、こうした判断とリスクへの対応を監督する役割がある。

[10] 個人情報の保護に関する法律（平成 15 年法律第 57 号）第 22 条「データ内容の正確性の確保等」, e-Gov 法令検索,（アクセス日：2026-10-19）, https://laws.e-gov.go.jp/law/415AC0000000057
[11] 当社作成

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

【想定事例】

例えば、ある企業が取締役会の審議を支援する生成 AI を導入し、投資案件について「見送るべき」との意見を示したとする。役員から判断の根拠を問われても、AI の説明をそのまま根拠にはできない。生成 AI が示す理由は、実際の処理過程を正確に反映しているとは限らず、学習データの出所を確認することも通常は難しいからだ。だからこそ、AI に入力した資料や参照データ、指示内容を記録し、役員が元の資料と照合できるようにしておく必要がある。AI の意見はあくまで参考情報であり、投資案件の採否は社内の権限規程に基づいて取締役会または経営陣が判断する。利用前に確認手順や判断者、誤りがあった場合の責任の所在を明確にしておくことが、AI ガバナンスの出発点となる。

経営陣がまず押さえておきたいのは、AI の性能や限界を理解したうえで、どのような判断に使い、その出力を誰が確認するのかを決めておくことである。誤りや想定外の出力が生じた場合に、誰が利用を止める権限を持つのかも明確にする必要がある。AI の技術を理解することと、経営として責任ある判断ができることは同じではない。

AI ガバナンスを IT 部門だけに担ってもらうことは難しい。NIST の「Artificial Intelligence Risk Management Framework」[12]でも、役割と責任、リスク許容度、継続的な監視を組織全体の方針や業務プロセスに組み込む考え方が示されている。経営陣、事業部門、IT 部門、リスク管理部門などが、それぞれの役割を持って関わることが前提となる。IPA の「DX 動向 2026」に掲載された 2025 年度調査では、AI の導入や利活用を主導する主体として「IT 部門の長」が 46.0%と最も高く、「経営層」が 32.1%、「現場の長」が 27.5%と続く。一方、CAIO（最高 AI 責任者）は 2.9%にとどまっている。

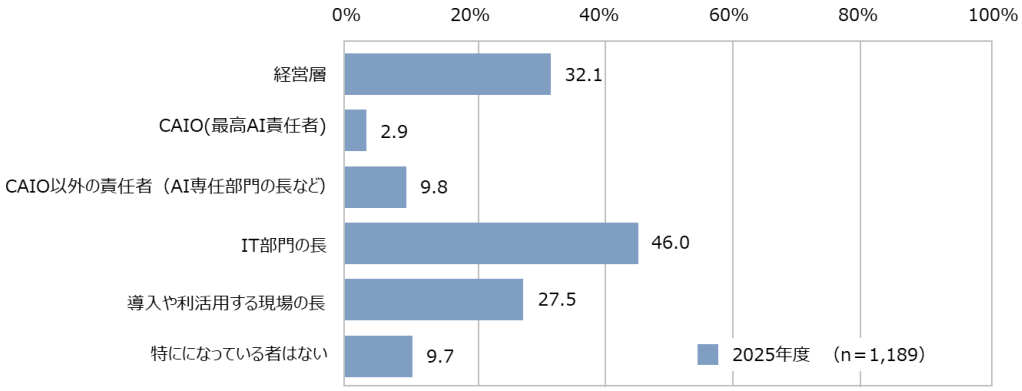


図 4　AI の導入・試行・検討企業における導入・利活用のリーダーシップ体制[13]

今後、AI の活用が広がれば、CAIO を置く企業も増える可能性がある。ただし、役職を設けるだけでは責任の所在は明確にならない。例えば、採用や与信、顧客対応で AI を使う場合、どの段階で人が確認し、誤った結果が出たときに誰が利用を止めるのかを決めておく必要がある。取締役会には、こうしたルールが整備され、実際に守られているかを監督する役割がある。AI に任せる範囲と、人が判断し責任を負う範囲を明確にすることが、AI ガバナンスの出発点となる。

[12] National Institute of Standards and Technology (NIST), “Artificial Intelligence Risk Management Framework”, 2023, (アクセス日：2026-10-19), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[13] 独立行政法人情報処理推進機構（IPA），「DX 動向 2026」より一部抜粋, (アクセス日：2026-10-19), https://www.ipa.go.jp/digital/chousa/dx-trend/rcu1hd0000017uk8-att/dx-trend-2026.pdf

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

おわりに

本レポートでは、CG コード改訂版が企業のリスクマネジメントに何を求めているのかを確認し、その要請を経営判断と取締役会の監督につなげるリスクガバナンスのあり方を考えてきた。サステナビリティ、サイバーセキュリティ、データガバナンス、AI といった新たな経営課題も取り上げた。

以前、ある会社の取締役会資料に掲載された重要リスクの一覧を見たことがある。5 年前と比べても、内容はほとんど変わっていなかった。その間、同社は海外拠点を新設し、新規事業にも進出していた。事業が変われば、依存する相手も、守るべきものも、引き受けるリスクも変わる。見るべきなのは、リスクの名称が変わったかどうかではない。経営環境や戦略の変化に応じて、評価の前提や対応方針、経営資源の配分まで見直されているかである。

筆者は、リスクマネジメントの価値は、減らしたリスクの数ではなく、経営の判断にどれだけ役立ったかで決まると考えている。何を守るのか。どこまでリスクを許容するのか。どの条件が変われば判断を見直すのか。取るべきリスクと抑えるべきリスクを見極め、成長機会との釣り合いを取る。そこにリスクガバナンスの役割がある。

そのためには、役割分担を明確にしておく必要がある。リスク管理部門が判断材料を整え、経営陣が判断し、取締役会がその判断とリスクテイクを監督する。内部監査は、この仕組みが機能しているかを独立した立場から確かめる。論点が複雑になるほど、誰が何を担い、どのように情報が伝わるのかが重要になる。

最後に確認しておきたい。「そのリスク情報を、経営はどの判断に、どう生かしたのか」。

CG コード改訂版への対応を、規程や報告書を整えるだけで終わらせてはならない。今回の改訂を、自社のリスクガバナンスが本当に経営に生かされているかを見つめ直す機会としてほしい。

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

【本レポートに関する注意事項】

1. 本レポートの位置付け
本レポートは、コーポレートガバナンス、内部統制、リスク管理等に関する一般的な情報および筆者の見解を示すものであり、個別企業の適法性やガバナンス、内部統制、リスク管理の有効性を保証するものではありません。また、法律、会計、税務その他の専門的助言を提供するものではありません。必要に応じて専門家にご相談ください。

2. 情報に関する留意事項
掲載情報は、作成時点で合理的な範囲において確認していますが、その正確性、完全性、最新性を保証するものではありません。法令、制度、ガイドライン等は、その後変更される場合があります。また、将来見通し、分析、評価、提言等は、作成時点の情報に基づくものであり、将来の結果を保証するものではありません。

3. 利用および責任に関する留意事項
本レポートは、お読みいただく方の検討や判断の参考としてご活用いただくことを目的としています。実際の意思決定にあたっては、個別の事情を踏まえてご判断ください。なお、本レポートの利用によって生じた結果について、当社および筆者は責任を負いかねますので、あらかじめご了承ください。

4. 生成 AI の利用について
本レポートの作成では、情報の整理、要約、文章表現の検討等の一部に生成 AI を利用しています。生成 AI の出力はそのまま使用せず、当社担当者が内容を確認し、必要な修正および検証を行ったうえで反映しています。

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.

筆者紹介

原　敬徳　Takanori Hara
取締役常務執行役員　首席コンサルタント
専門は、全社的リスクマネジメント、コーポレートガバナンス、内部統制など

ＳＯＭＰＯリスクマネジメントについて

ＳＯＭＰＯリスクマネジメント株式会社は、損害保険ジャパン株式会社を中核とするＳＯＭＰＯホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策等のソリューション・サービスを提供しています。

本レポートに関するお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
マーケティング戦略部　広報担当
〒163 - 6028 東京都新宿区西新宿 6-8-1
Email:10_srmpr@sompo-rc.co.jp

Copyright © 2026 Sompo Risk Management Inc. All rights reserved.