MS&AD InterRisk Report

No.24-005

2024.04.01

ESG リスクトピックス ＜2024 年度第 1 号＞

本誌では、E（環境）・S（社会）・G（ガバナンス）に関する国内・海外の最近の重要なトピックスをお届けします。

今月のトピックス

＜気候変動＞

〇日米で GHG 排出量の開示義務化の動き強まる

（参考情報：2024 年 2 月 19 日付　金融庁 HP
https://www.fsa.go.jp/singi/singi_kinyu/sustainability_disclose_wg/shiryou/20240326/03.pdf
参考情報：2024 年 3 月 26 日付　金融庁 HP
https://www.fsa.go.jp/singi/singi_kinyu/soukai/siryou/20240219/1.pdf）

金融庁は 2 月 19 日に開催された金融審議会において、東証プライム企業を対象に、現在策定中のサステナビリティ基準委員会（SSBJ）の基準に沿って、有価証券報告書におけるサステナビリティ情報開示を義務化する方針を示した。SSBJ は、昨年 6 月に公表された国際サステナビリティ基準審議会*（ISSB）の基準を踏まえて、日本版の開示基準を策定中であり、2024 年 3 月までに公開草案を示し、2025 年 3 月までに最終化を予定している。

温室効果ガス（GHG）排出量の開示対象範囲は ISSB 基準を踏まえて、スコープ 1（直接排出）とスコープ 2（電力やその他エネルギーの使用による間接排出）だけでなく、スコープ 3（バリューチェーンからの排出）も対象となる見通しだが、一定の経過措置が設けられる可能性もある。

世界でも、GHG 排出量の開示義務化が進んでいる。米国証券取引委員会（SEC）は 3 月 6 日、気候関連開示規則を採択した**。本規則は、米国上場企業に気候関連リスクとリスク管理に関する情報開示を義務付けるもので、開示要求事項にはスコープ 1、2 の GHG 排出量が含まれる。一方、当初案には含まれていたスコープ 3 は、企業の算定コストの負担増などの批判を受けて、開示義務化の対象から外された。本規則は米国登録企業だけでなく、外国登録企業にも適用され、米国に上場している日系企業も対象となる。

また、EU では企業サステナビリティ報告指令（CSRD）が 1 月 1 日から適用開始となり***、欧州サステナビリティ報告基準（ESRS）に基づいて、スコープ 1、2、3 の開示が求められるようになった。CSRD では、EU 域内にグループ会社を持つ日系企業は開示対象となるため、適用要件を確認する必要がある。

世界各国で GHG 排出量の開示義務化が進んでおり、日本ではスコープ 3 も対象となる公算が高い。スコープ 3 を未算定の企業は、いよいよ取り組む必要がある。また現状では、企業が開示しているスコープ 3 は原単位法による推計値が大半で、かつ対象としているバリューチェーンのプロセスも企業ごとに異なる場合があり、比較可能性の観点から懸念が残る。企業側の算定コストとの兼ね合いにはなるが、より合理的な算定手法や仕組みの追求が期待される。

* 国際会計基準の策定機関を傘下に持つ IFRS 財団が、サステナビリティ情報開示の統一的なルールの作成を目的に 2021 年 11 月に設立。2023 年 6 月にサステナビリティ開示基準（S1）、気候基準（S2）の最終版を公表。

** 米国証券取引委員会（FACT SHEET The Enhancement and Standardization of Climate-Related Disclosures）https://www.sec.gov/files/33-11275-fact-sheet.pdf

*** 欧州委員会

https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

＜サステナビリティ情報開示＞

○金融庁がサステナビリティ情報の保証制度導入に向け WG 設置

（参考情報：2024 年 2 月 19 日付　金融庁 HP：https://www.fsa.go.jp/singi/singi_kinyu/soukai/siryou/20240219.html）

金融庁の金融審議会は 2 月 19 日、「サステナビリティ情報の開示と保証のあり方に関するワーキング・グループ」の設置を公表した。有価証券報告書でのサステナビリティ情報開示に、財務諸表と同様の第三者が「保証」する制度の導入を検討する。

3 月 26 日に第 1 回会合を開き、サステナビリティ情報の保証の担い手や保証基準・範囲・水準、制度整備などを議論する。

保証制度は、信頼性確保のため投資家から導入を望む声が上がっている。EU の欧州サステナビリティ報告基準（ESRS）や米証券取引委員会（SEC）気候関連開示規則では、保証が義務化されている。適用対象の企業は、中長期的に「限定的保証」から「合理的保証」への移行が必要だ。両者は、監査人などが対象情報の信頼度を表明する際の水準が異なり、後者の方が保証のレベルは高い。

国際会計士連盟（IFAC）の「The State of Play: Sustainability Disclosure and Assurance 2019-2022」によると、世界 22 カ国の企業約 1,400 社のうち 98%がサステナビリティ情報を報告しているが、何らかの保証を受けている企業は 69%に留まり、合理的保証を取得する企業は 10%に満たない。日本企業の場合、保証を取得する企業の 94%を限定的保証が占めている。

欧州や米国では、サステナビリティ情報の制度開示で保証の導入がスケジュールで示されている。こうした動きを受けて、国際監査・保証基準審議会（IAASB）が策定中の国際サステナビリティ保証基準「ISSA5000」が、24 年 9 月の最終化に向けて開発が進む。同基準は、先行するサステナビリティ開示基準（ISSB や ESRS など）への適用を目的にする。日本のサステナビリティ基準委員会（SSBJ）が開発中の基準にも適用可能な想定で、「保証」の内容を伺うことができる。

＜サステナビリティ情報開示＞

〇ISSB がサステナ開示基準の各国採用状況を調査、24 年上期めどに結果を公表へ

（参考情報：IFRS HP：https://www.ifrs.org/content/dam/ifrs/supporting-implementation/adoption-guide/preview-of-the-jurisdictional-adoption-guide.pdf ）

国際サステナビリティ基準審議会（ISSB）はこのほど、2023 年 6 月にリリースしたサステナビリティ開示の国際基準について、各国での採用状況を調査・一覧化したガイドを 24 年上期めどに公表すると発表した。

ガイド発行の主な趣旨は、①ISSB 基準採用を検討する各国の開示規制当局に、他国の採用状況など参考情報を提供する ②国を跨いで資金運用する機関投資家に対して、外国の投資先企業のサステナビリティ情報を把握したり、別の国の企業と比較したりする際に、各国の開示規制の特徴を把握する際の参考情報を提供すること。企業が他国に進出する際に、各国の開示基準の特性を把握する際にも役立ちそうだ。

＜調査の項目と内容＞

#	項目	内容
3.3.1	規制または法的地位	ISSB 基準の開示要件を導入するための法律/規制の導入状況
3.3.2	整合性の程度	ISSB 基準との整合性の程度
3.3.3	説明責任を負う事業体の範囲	説明責任を負う対象範囲が、上場企業や受託者の立場で資産を保有する「銀行、保険会社、投資信託など」のほか、SME（中小企業）なども含むか
3.3.4	事業体における説明責任の程度	第 1 層(プライム市場)と第 2 層（スタンダード市場)に対する要件の差異
3.3.5	開示の位置づけ	サステナビリティ情報の開示場所を「一般目的財務報告書」（日本の場合は有価証券報告書）の中に設けているか
3.3.6	報告主体	一般目的財務報告書と同一であるかどうか
3.3.7	二重報告	各国規制と ISSB 基準のいずれにも準拠する法律または規制を導入しているかどうか
3.3.8	発効日	ISSB 基準の発行日の設定状況
3.3.9	移行に伴う救済措置	ISSB 基準における以下の救済事項の、各国規制における導入状況とその範囲 ・ 「気候優先」報告(初年度に限り、気候関連のリスク・機会のみの情報開示可) ・ 報告のタイミング(初年度に限り、財務報告書公表後のサステナビリティ関連開示可) ・ GHG プロトコル(初年度に限り、各国において既に使用している測定方法を利用可) ・ GHG 排出量“スコープ 3”(初年度は開示不要)
3.3.10	管轄変更	各国規制における管轄区域の変更の有無
3.3.11	追加の開示要件	ISSB 基準と異なる要件の有無

日本を例にすると、ISSB 基準では「3.3.3 説明責任を負う事業体の範囲」「3.3.4 事業体における説明責任の程度」を「公開市場で証券が取引されている企業」としているのに対し、金融庁金融審議会は今月、「東証プライム上場企業」に限定する意向を示している。

ISSB 基準の各国での適用については、世界 130 以上の加盟国・地域の証券監督当局や証券取引所等で構成する証券監督者国際機構（IOSCO）が 23 年 7 月、「ISSB 基準は資本市場での利用目的に適合している」という強いメッセージを発信し、積極的な導入を訴え。一方で、機関投資家か

らは、国ごとの制度にわずかな違いがあり把握が困難、との異論がでていた。

ISSB は 24 年上期のガイド初版公表後も 3 年以内の更新を予定する。

＜国際動向＞

〇EU がグリーンウォッシュ禁止指令案を採択

（参考情報：2024 年 2 月 20 日付　European Commission HP
https://www.consilium.europa.eu/en/press/press-releases/2024/02/20/consumer-rights-final-approval-for-the-directive-to-empower-consumers-for-the-green-transition/）

2024 年 2 月 20 日、EU 理事会（閣僚理事会）はグリーンウォッシュを禁止するために、「グリーン・トランジションのための消費者権利の強化指令案」（以下、本指令案）を正式に採択した。グリーンウォッシュとは、英語で「ごまかす」「欠点を隠してよく見せる」という意味の「ホワイト・ウオッシュ（Whitewash）」と「環境に良い」という「Green」を組み合わせた造語で、実質を伴わない、または裏付けのない不明確な環境訴求のことを指す。グリーンウォッシュの問題は、消費者や投資家などが製品や企業を環境に配慮されたものと思い込み、適切な選択肢を選べず、結果的に環境問題が深刻化してしまう点にある。加えて、実際に環境に配慮している企業の努力が隠れてしまう可能性もある。欧州委員会が 2020 年に行った企業の環境訴求に関する調査によると、EU 域内に流通する 150 件の製品のうち、環境訴求の 53%は「あいまい／誤解を招く／根拠がない」、40%は「裏付ける根拠がない」という結果が出ている。

本指令案は、現行の不公正取引方法指令（UCPD:Unfair Commercial Practices Directive）と消費者権利指令（CRD:Consumer Rights Directive）などを改正するものである。改正により、消費者がより環境に優しい、あるいは循環型の製品やサービスを正しく選択できるようにすることを目的としている。企業が環境性能を不当に主張して誤解を招くような「グリーンウォッシュ」や、予測よりも長持ちしない製品に対する虚偽の主張などの不公正な慣行を取り締まることとなる。

指令案では、環境や社会への影響、耐久性、修理可能性などの製品の循環性について、誤解を与えてはならない製品の要素と規定している。環境訴求に関しては、測定可能な目標や達成期限などの現実的な実施計画を伴い、独立した第三者機関による定期的な検証を受けた、明確かつ客観的で検証可能なコミットメントがない場合は、誤解を招くマーケティング方法として使用を禁止する。原則禁止とするマーケティング方法は以下のとおりである。

・実証できない一般的な環境訴求の表示を用いたマーケティングを行うこと。
　例）「環境に優しい」「エコロジカル」「グリーン」「自然に優しい」「エネルギー効率が良い」「生分解性」「バイオベース」など
・製品や企業活動の一部にのみ該当する環境訴求をもって、製品や企業活動全体に関する環境訴求を行うこと。
・カーボン・オフセットのみに基づき、環境への悪影響が軽減されたなどと訴求すること。
・公共の機関から発行されているものや、EU 域内で承認された証明スキームに基づいているもの以外のサステナビリティ・ラベルを用いること。

実質を伴う環境訴求は、指令案の適用開始後も認められる。

また、製品の循環性に関する以下のマーケティング方法などを原則禁止とする。

・通常の使用条件下における耐用期間・強度など、製品の耐久性に関する虚偽の訴求をするこ

と。

・技術上の理由で必要となる時期よりも早い段階で消耗品の交換を促すこと。

・製品の製造元以外が提供する消耗品や部品を使用すると故障するなどの虚偽の訴求をすること。

・機能性向上のためだけのソフトウエアのアップデートを、必要なアップデートと提示すること。

欧州理事会は 2023 年 3 月、環境に配慮されていることを実証するための最低条件として、第三者機関による裏付けと認証が必要だとしている。これに違反した企業に対して、罰則として罰金や公的資金提供の一時的な除外などが含まれる予定となっている。

今後、EU 官報への掲載から 20 日後に施行され、加盟国による国内法化を経て、施行 30 か月後から適用が開始される。EU 加盟国での国内法が整備されれば、EU 市場で活動する日本企業もその適用を受けることとなる。

グリーンウォッシュ規制の進展は欧州に限ったものではない。米国では、米連邦取引委員会（FTC）がグリーンウォッシュ防止のためのガイドラインの見直しに着手している*。オーストラリア競争・消費者委員会（ACCC）は 2023 年 12 月、グリーンウォッシングから消費者を保護することを目的とした、罰則つきの新たな環境およびサステナビリティに関する訴求のガイダンスを発表した**。

日本では、現状はグリーンウォッシュに対処する法的な規制は確立していない。グリーンウォッシュに関する規制としては、ISO が定めた ISO14021（環境ラベル）規格や、環境省による「環境表示ガイドライン」、「不当景品類及び不当表示防止法」による優良誤認表示規制などがあるが、いずれも法的拘束力はない状況である。

しかし、2022 年には「生分解性」を謳っていたプラスチック製のカトラリー類やレジ袋などの表示が「優良誤認」にあたるとして、消費者庁が行政処分を行う事例が発生している。今後は日本でも環境配慮の表示については厳しく取り締まるようになることが予測される。

* https://www.ftc.gov/legal-library/browse/federal-register-notices/guides-use-environmental-marketing-claims-green-guides

** https://www.accc.gov.au/media-release/accc-releases-eight-principles-to-guide-businesses%E2%80%99-environmental-claims

＜気候変動＞

○環境省「ブルーカーボン」の吸収量を世界初算定、国連に報告へ

（参考情報：2024 年 2 月 19 日付　環境省
「我が国インベントリにおける藻場（海草・海藻）の算定方法について」
https://www.env.go.jp/content/000203001.pdf）

環境省は 2 月 28 日、「ブルーカーボン」による二酸化炭素（CO2）吸収量を世界で初めて算定し、その方法を公開した。4 月に温室効果ガスインベントリ（Greenhouse Gas Inventory）に反映させ、国連条約事務局に提出する。

ブルーカーボンとは、沿岸湿地のマングローブや潮汐湿地（沿岸洲や海岸砂丘による埋め立てで生じる湿地）、海草（アマモなど根・茎・葉が区別できる種子植物）・海藻（ワカメなど根・茎・葉の区別がはっきりしない種子植物）、藻場（海草や海藻が茂る場所）で吸収される炭素のこと。対して、陸上の植物が吸収した炭素はグリーンカーボンという。

ブルーカーボンは CO2 の吸収率（生きものが排出した量に対する吸収した量）が約 30%で、植物の約 12%と比較して高く、貯留期間も水中で安定的なため数十年から数千年と長い（植物は数十年～数百年）。日本は藻場やマングローブなどのブルーカーボンを見込める海域の面積が比較的広いことから、海草・海藻とそれらの藻場の両方を含めた吸収量の算定方法を検討していた。そして 2023 年、環境省温室効果ガス排出量算定方法検討会で算定方法が確定された。海草・海藻・藻場の吸収量の算定方法の提出は世界で初めて。

温室効果ガスインベントリは、自国が 1 年間に排出・吸収する温暖化効果ガスの量や計算方法等を取りまとめたデータのこと。気候変動枠組条約締約国は毎年 1 回、関連情報と併せて国連の条約事務局への提出が義務付けられている。

ブルーカーボンによるオフセットの枠組みも始まっている。カーボンオフセットとは、CO2 削減努力後にどうしても減らせない排出量を、他者の削減取り組みで創出され、第三者機関が認めた削減量をクレジットとして購入して相殺する仕組み。ブルーカーボンによるカーボンクレジット制度として、ジャパンブルーエコノミー技術研究会（JBE）が 20 年に「J ブルークレジット」の認定を始めた。公的な制度ではないものの、CO2 の譲渡総量は 21 年の 20 トンから、22 年は 3,733 トンに増えている。購入者は商船三井や住友商事、東京ガス、セブン - イレブン・ジャパンなど 100 社以上に上り、人気の高さが伺える。しかし、政府が 19 年に運営を開始した J-クレジットの 889 万トン（22 年）に比べると、まだ規模が小さい。また、購入者に比して創出者が少なく、価格の高騰や検証手続きの煩雑さなどの課題もあげられる。今後市場を拡大できるかがカギとなっている。

ブルーカーボンは、海に囲まれた日本の特性を生かしたカーボンニュートラルの取り組み。藻場や湿地、マングローブの再生のほか、空港や洋上風力などの人工物が新たな藻場となり豊かな漁場を創出できる。ブルーカーボンは気候変動の対策のみならず、生態系の保全や回復、漁業の振興などに同時に貢献できるため、企業にとって活用の可能性は大きい。

＜不正競争防止法＞

〇外国公務員に対する贈賄への対応強化に向けて外国公務員贈賄防止指針を改訂

（参考情報：2024 年 2 月 1 日付　経済産業省 HP
https://www.meti.go.jp/policy/external_economy/zouwai/pdf/GaikokukoumuinzouwaiBoushiShishin.pdf）

経済産業省は 2 月、外国公務員贈賄防止指針を改訂した。2023 年 6 月に不正競争防止法の一部が改正されたことに加え*、OECD からのスモール・ファシリテーション・ペイメント(SFP)**に係る解釈についての指摘を踏まえたもの。本改訂により、企業における外国公務員に対する贈賄防止体制の構築と運用のポイントや外国公務員贈賄の法解釈に関して、内容が拡充された。改訂された主な点は以下のとおりである。

・外国公務員贈賄罪にかかる法改正事項の反映
・スモール・ファシリテーション・ペイメント（SFP）に関する記載の修正
・海外子会社・支店の従業員による贈賄行為について、親会社（本社）に処罰が及ぶケースの明確化
・外国公務員贈賄防止体制の構築（特にリスクベース・アプローチ）に関する記載の充実

2024 年 4 月より改正不正競争防止法が施行される。企業においては、上記指針を参考にし、贈賄防止体制の見直しに活用されたい。また、あわせて、自社の贈賄リスク対策の現状を簡易チェックすることができ、対策の段階ごとに留意すべき事項が示された「外国公務員贈賄防止指針のてびき」***があるため、こちらも参照されたい。

* 外国公務員への贈賄に関しては、違反者への法定刑引き上げ、公訴時効期間の延長、処罰対象拡大（日本人ではない国外従業員等による贈賄行為も対象）等の罰則強化がなされた。

** 一義的な定義があるものではないが、例えば、通常の行政サービスに係る手続の円滑化のための少額の支払いとされることがある。

*** https://www.meti.go.jp/policy/external_economy/zouwai/pdf/zouwai_shishin_tebiki.pdf

＜内部通報制度＞

〇消費者庁が内部通報制度に関する意識調査の結果を公表

（参考情報：2024 年 2 月 29 日付　消費者庁 HP：
https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/research/assets/research_240229_0002.pdf）

消費者庁は 2 月 29 日、就労者 1 万人を対象に実施した「内部通報制度に関する意識調査」（以下、「本調査」）の結果を公表した。本調査は、公益通報者保護法が求める「内部通報制度*」の認知度や通報に対する意識を把握し、制度の普及や実効性向上に向けた施策の参考とすることを目的に 2023 年 11 月に実施された。本調査で明らかとなった主な結果は以下のとおり。

・ 内部通報制度について「よく知っている」または「ある程度知っている」と回答した割合は、約 39%だった。
・ 勤務先に内部通報受付窓口が「設置されていることを知っている」と回答した割合は、約 30%だった。

・ 内部通報制度を「よく知っている」と回答した人の 88%が、勤務先で重大な法令違反を知った場合に勤務先または行政機関等へ「相談・通報する」または「たぶん相談・通報する」と回答した（全体平均よりも約 30%ポイント高かった）。

・ 内部通報制度を「よく知っている」と回答した人は、勤務先の重大な法令違反を一番相談・通報しやすい先として「勤務先」を回答した割合は約 58%だった（全体平均は約 47%）。

・ 勤務先や行政機関等に重大な法令違反を「相談・通報する」または「たぶん相談・通報する」と回答し、かつ勤務先に内部通報受付窓口が「設置されていることを知っている」と回答した人のうち、約 76%が最初の通報先として「勤務先」を回答した。

・ 勤務先で重大な法令違反を知った場合に「たぶん相談・通報しない」または「絶対相談・通報しない」と回答した人のうち、理由として「誰に相談・通報したら良いか分からない」を選択した割合は、「たぶん相談・通報しない」と回答した人の約 32%、「絶対相談・通報しない」と回答した人の約 51%で、最も高かった。

本調査では、内部通報制度の理解度が高いほど通報意欲が高くなる傾向や、勤務先の通報窓口を認知している人ほど最初に勤務先へ通報する傾向があることがわかった。そのため、企業においては、内部通報制度を整備するだけでなく、従業員に対する制度の周知や理解促進に取り組むことが、企業内部の自浄作用を高めるとともに、社外告発による風評リスク等を低減することに繋がると推察できる。一方で、本調査からは、従業員の内部通報制度の理解度や通報窓口の認知度は十分とはいえないことも明らかになった。企業にとっては、自社の内部通報制度について、従業員に対する啓発活動をより一層強化していくことが課題といえるだろう。この点、本調査結果において、内部通報制度を「よく知っている」と回答した人の 75%が、制度を知ったきっかけとして、「勤務先・派遣先・従前の勤務先における研修・周知」と回答していることから、地道に、本制度の周知を図っていくことが企業には期待される。

＊ 本調査での「内部通報制度」とは、勤務先における法令違反行為について、勤務先自身が従業員から情報を受け付けて調査を行い、法令違反を是正する制度をいう

＜非財務情報開示＞

〇金融庁が有価証券報告書の「好事例集」を公表　開示充実のポイント解説

（参考情報：2023 年 12 月 27 日付　金融庁 HP　https://www.fsa.go.jp/news/r5/singi/20231227.html
2024 年 3 月 8 日付　金融庁 HP　https://www.fsa.go.jp/news/r5/singi/20240308.html）

金融庁は 3 月 8 日、企業の有価証券報告書の優れた開示を紹介する「記述情報の開示の好事例集 2023」を更新した。開示の充実化を促すため毎年作成しており、2023 年版は内閣府令の改正で新たに開示が求められるようになった「サステナビリティに関する考え方及び取組」をテーマに昨年 12 月に公表していた。今回の更新では、「コーポレート・ガバナンスの概要」などの分析を追加。投資家、アナリストらの意見をもとに選んだ好事例について高く評価したポイントを解説しており、開示の充実化を目指す企業が参考にしやすい構成となっている。

「サステナビリティに関する考え方及び取組」は、内閣府令で 4 つの枠組み（ガバナンス、戦略、リスク管理、指標及び目標）について開示することが求められている。好事例集では、各項目の記載前にサステナビリティ全般に関する説明や企業の全体戦略とサステナビリティとの関わりについて紹介することが、わかりやすい開示につながると指摘した。

開示項目別では、4 つの枠組みのうち、ガバナンスとリスク管理が特に重要とし、ガバナンス

においては、全般的なガバナンス体制と実効性に関する評価を開示することをポイントとして挙げた。また、リスク管理では、有価証券報告書で開示が求められている「事業等のリスク」だけでは情報が不足する可能性があるとし、リスクだけではなく、機会についても記載することが有用だとした。

「コーポレート・ガバナンスの概要」では、ガバナンスの実効性を訴求するポイントとして、取締役のスキルマトリクスや取締役会での議論の状況を開示すること、取締役会議長の視点からの説明を記載することなどを挙げている。

そのほか、「監査の状況」「株式の保有状況」「経営上の重要な契約等」の開示についても分析。企業の規模に着目し、中堅企業や中小企業の開示に関する好事例も紹介している。また、リソースに課題があり、十分な開示をできていない企業は、自社にとって特に重要な論点や、開示を通じて投資家に伝えたいことに焦点を当てて開示をすることや、現時点で開示できていない情報については今後の方針や方向性について記載することを推奨している。

近年、情報開示の重要性は高まっており、有価証券報告書の内容も開示の充実化を進める企業と従来の開示を続けている企業の二極化が顕著となっている。有価証券報告書を充実させることは、株主や投資家への説明責任を果たすだけでなく、新たな投資を呼び込むことにもつながる。好事例と自社の開示内容を比較し、より高いレベルの開示を志向する契機としてほしい。

＜サイバーセキュリティ＞

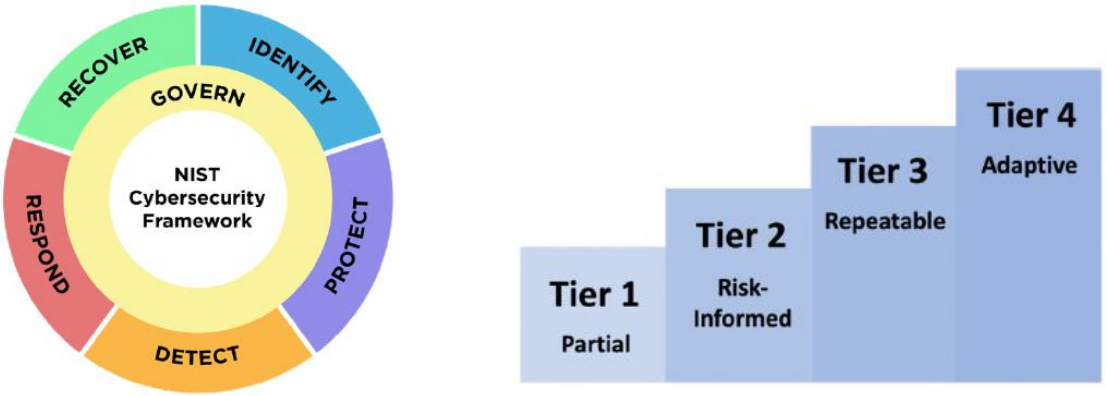
〇サイバー管理・対策の「共通言語」がアップデート「The NIST Cybersecurity Framework 2.0」が公開

（参考情報：2024 年 2 月 26 日　NIST
「NIST Releases Version 2.0 of Landmark Cybersecurity Framework」
https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework)

米国国立標準技術研究所（NIST）は 2024 年 2 月 26 日、「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1(以下、NIST CSF1.1)」の後継となる「The NIST Cybersecurity Framework (CSF) 2.0 (以下、NIST CSF2.0)」を公開した。

NIST CSF2.0 は 6 つのコア機能（CSF Core Functions）と、それぞれの機能で求められる管理策の実施状況を 4 段階で評価するティア（CSF Tiers）、自社のセキュリティ対策の現状と目指す姿を評価するプロファイル（CSF Organizational Profiles）を活用することで、企業・組織が網羅的にサイバーセキュリティ対策・管理の成熟度を評価できる。

＜NIST CSF2.0 の CSF Core Functions と CSF Tiers＞



出典： The NIST Cybersecurity Framework (CSF) 2.0

NIST CSF1.1 までは「重要インフラ向け（for Improving Critical Infrastructure）」であったものの、多くの企業・組織でサイバーセキュリティ管理・対策を推進する際の「共通言語」として活用されてきた。NIST CSF2.0 は公式に、小規模な学校や非営利団体から大規模な機関や企業に至るまで、サイバーセキュリティ対策の洗練度に関係なく、すべてのユーザー、業界、組織を対象に設計されている。

NIST CSF2.0 のポイントを 3 点紹介する。

1 点目はガバナンスとサプライチェーンセキュリティの重要性が強調された点である。NIST CSF2.0 より、従前のコア機能（「識別（Identify）」「防御（Protect）」「検知（Detect）」「対応（Respond）」「復旧（Recover）」）に「統治（Govern）」が追加された。「統治」はセキュリティ対策を円滑に進めるための推進役として期待されており、経営陣の積極的な関与と全社的なリスクマネジメント戦略を踏まえたサイバーセキュリティ対策の検討をより明確に要求している。また、サプライチェーン上の弱点を狙った攻撃が増加している背景を踏まえ、「統治」の機能において、サプライチェーンセキュリティに関する管理策が強化された。経営陣はサプライチェーンを含め、セキュリティリスクの状況や対策の目標を把握し、推進役としての役割が期待されている。

2 点目は 6 つのコア機能で求められる管理策を具体的に示した「Implementation Examples」が追加された点である。これまで、コア機能を達成する上で求められる管理策は、「Informative References」として、NIST SP800-53*、ISO27001 等の別ガイドラインの関連箇所が示され、それぞれのガイドラインを参照することで具体的な管理策の内容を確認できた。NIST CSF2.0 では、従前の「Informative References」に加えて、「Implementation Examples」としてフレームワーク自体に具体的な管理策の実施例が追加され、セキュリティ対策・管理の習熟度を評価する事業者にとって、より活用しやすくなった。

3 点目は NIST CSF2.0 の公開と合わせて、多くの「Quick Start Guides」が公開された点である。「Quick Start Guides」は企業のリスク管理者や小規模事業者の責任者、サプライチェーンセキュリティの強化を検討している事業者向けに、それぞれの目的や課題に合わせて NIST CSF2.0 を効果的に活用するための要点がまとめられた有益なガイドとなっている。その他、ティアやプロファイルの要点がまとめられたガイドも公開されているので、サイバーセキュリティ管理・対策を推進する際に参考にされたい。

NIST は、利用者からのフィードバックを踏まえながら、NIST CSF2.0 をより効果的に活用する

ため、リソースの継続的な拡充および更新を予定している。大幅にアップデートされたサイバーセキュリティ管理・対策の「共通言語」を確認の上、継続的なサイバーセキュリティ対策の強化を進めていただきたい。

* NIST が公開している米国政府機関が採用するセキュリティ管理策を指す。

＜サイバーセキュリティ＞

〇ENISA「サイバー危機管理のベストプラクティス集」を公開

（参考情報：2024 年 2 月 28 日付　ENISA ニュースリリース
「Geopolitics Accelerates Need For Stronger Cyber Crisis Management」
https://www.enisa.europa.eu/news/geopolitics-accelerates-need-for-stronger-cyber-crisis-management）

ENISA*は、2 月 28 日に「サイバー危機管理のベストプラクティス集」を公開した。EU においても地政学的な状況はサイバー脅威に大きな影響を与えており、加盟国間における「サイバー危機」の定義の相違が、国境を越えた大規模なサイバーセキュリティ事件・危機への協調的対応の課題となっている。2024 年 10 月には、EU 加盟国のサイバーセキュリティ対策のギャップを取り除き、全体のサイバーセキュリティのレベルを高めるための法的措置に関する指令「NIS2」が施行される。この研究は、EU サイバー危機連絡組織ネットワーク（EU-CyCLONe**）のために実施されたもので、NIS2 の求める要件を充足する助けとなる一連のベストプラクティスを提案、EU 加盟国間の異質なエコシステムをより強力な調和へ導くことを目的するものである。

本研究の本編ではサイバー危機シナリオの枠組みと状況を概説、「prevention（予防）」「preparedness（準備）」「response（対応）」「recovery（復旧）」4 段階のサイクルに分け、国家によるサイバー危機の定義採用からコミュニケーション戦略の策定、危機時の技術支援への民間セクターの関与の奨励に至るまで、各段階で発生する問題にオールハザードアプローチで言及した 16 のベストプラクティスを紹介している。

① 予防段階

No.	ベストプラクティスの概要
1	国境を越えることも考慮した「サイバー危機」の国内的定義の採用
2	国の公共部門に特化した情報セキュリティ基準の策定、定期的な見直し、更新
3	DDoS 緩和のような予防プログラムの策定を促進する国家イニシアチブの育成

② 準備段階

No.	ベストプラクティスの概要
4	ガバナンス構造の定義、具体的な能力の提供、クライシスコーディネーターの任命
5	迅速な行動を可能にするために、重要な資産に関する情報のマッピングと収集
6	危機発生時の瞬時に安全な通信手段の確立
7	サイバー危機への対応に関わる関係者間の明確な役割分担を定義
8	時間、優先度、関係者、攻撃の重大性などの要素を考慮し、サイバー危機対応計画を発動し、関係先へのエスカレーション基準の策定
9	危機発生時の調整と相互運用性を最適化するための方法論とリスク評価ツールの開発
10	複数年にわたるサイバー危機管理演習と訓練セッションのプログラムを通じて、サイバー危機に対応するための全体的な作戦計画をテスト
11	現在および将来、運用レベルでサイバー危機管理を担当するスタッフのための訓練セッションを設定

12	危機発生時における、情報連携が必要不可欠な団体へのメッセージの明確なフォーマット、関与する利害関係者、優先度レベルと時間的要因、使用するコミュニケーションチャネルを含めたコミュニケーション戦略の開発

③ 対応段階

No.	ベストプラクティスの概要
13	被害者に技術支援を提供するために、民間で認定された「信頼できるプロバイダー」の動員を奨励する
14	統一されたメッセージで、被害者の危機コミュニケーションを支援する

④ 復旧段階

No.	ベストプラクティスの概要
15	関連するステークホルダーと協議し、定期的な見直しと更新を行いながら、参照フレームワークで定義された事業再開計画（BRP）を策定し、実施する
16	サイバー危機管理のための行動計画を改善するための提言を作成する部署を設置

そのうえで、EU-CyCLONe に対する 5 つの提言を述べている。

提言	内容
1	モデル的なサイバー危機対応計画につなげるため、EU 全体のサイバー危機メカニズムを定義するための作業部会の設置
2	EU 加盟国全体で、プレーヤーと手順をテストするシミュレーション演習を開発する（能力を強化するだけでなく、加盟国間の信頼関係を構築する上でも重要）
3	サイバー危機発生時に、安全なコミュニケーション・プラットフォームの設置
4	各国のサイバー危機管理当局が、自国の重要情報システムマップを定期的に更新する（インシデント発生時の迅速な対応や、その影響の限定化、あるいは実施された防御行動の結果の防止にも貢献）
5	各国のサイバー危機管理当局が、メディアに対して危機対応の進捗状況を適時適切に提供できるための、メディアトレーニングの開催

* The European Union Agency for Cybersecurity の略称。EU 加盟国全体でセキュリティレベルの維持や向上の実現を目的とする機関。

** The European cyber crisis liaison organisation network の略称。EU 加盟国のサイバー危機管理当局の代表によって構成される、サイバー危機の活動と管理における加盟国当局間の協力を強化することを目的としたネットワーク。

以上

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランスグループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。本誌を編集している以下のグループでは、危機管理、サステナビリティ、ERM（全社的リスク管理）、サイバーリスク等に関するコンサルティング・セミナー等のサービスを提供しています。
弊社サービスに関するお問い合わせ・お申込み等は、下記のお問い合わせ先、または、お近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱　リスクコンサルティング本部
リスクマネジメント第三部
interrisk_csr@ms-ad-hd.com（危機管理・コンプライアンスグループ）
interrisk_erm@ms-ad-hd.com（統合リスクマネジメントグループ）
CyberRisk_irric@ms-ad-hd.com（危機管理・サイバーリスクグループ）
リスクマネジメント第五部
kankyo@ms-ad-hd.com（サステナビリティ第一グループ）
sustainability2@ms-ad-hd.com（サステナビリティ第二グループ）
https://www.irric.co.jp/

主な担当領域は以下のとおりです。

＜危機管理・コンプライアンスグループ＞
- ◆ 危機管理・海外危機管理
- ◆ コンプライアンス（法令遵守）
- ◆ 役員賠償責任（D&O）
- ◆ CS・苦情対応

＜統合リスクマネジメントグループ＞
- ◆ ERM（全社的リスク管理）
  - ・リスクマネジメント体制構築
  - ・企業リスク分析・評価（リスクアセスメント）

＜危機管理・サイバーリスクグループ＞
- ◆ 情報セキュリティ、サイバーリスク

＜サステナビリティ第一グループ＞
- ◆ 気候変動・TCFD支援
- ◆ 自然資本（原材料調達、グリーンレジリエンス、TNFD支援）

＜サステナビリティ第二グループ＞
- ◆ SDGs（持続可能な開発目標）推進支援
- ◆ 生物多様性（企業緑地）取り組み支援
- ◆ 「ビジネスと人権」取り組み支援
- ◆ サステナビリティ経営に関する体制構築・課題対応支援

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業のリスクマネジメント活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

MS&AD インターリスク総研は、2024 年 4 月、これまでのホームページを刷新し、リスクに強い組織づくりをサポートするプラットフォーム「RM NAVI（リスクマネジメント ナビ）」をリリースしました。
「RM NAVI」は、MS&AD インターリスク総研の知見をフル活用して、情報提供から実践までをトータルサポート。
コンサルタントの豊富な経験と、最先端のデジタルサービスで、リスクに強い組織づくりを支えます。
あなたに寄り添い、最適な答えへと導く、リスクマネジメントの羅針盤です。