システム監査学会 第37回研究大会

「BCP/BCMSと新システム監査制度」研究プロジェクト報告

「ＢＣＰと地政学リスク」

"BCP and Geopolitical risk with Systems Audits"

2023年6月16日

１．当研究プロジェクトの内容紹介①

「BCP/BCMSと新システム監査制度」研究プロジェクト

- 2018年度発足プロジェクト
- 主査：黒澤　兵夫
  メンバー：竹淵　広志（発表者）、水野　英治、
  牧野　博文
- 2020年2月以降、 開催頻度は１～２ヶ月に1回程度、所要時間は１回２時間程度で、 WEB会議/電子メールベースで活動

１．当研究プロジェクトの内容紹介②

【研究テーマ】

- 新システム監査制度（システム監査基準およびシステム管理基準）の発行に伴い、システム監査、監査制度の普及と啓蒙につとめる。
  また、新しい技術 IoT、AI、ビッグデータ等への適合性を調査・研究する。
- 上記の結果をBCP/BCMS関連の監査へ適用を図っていく予定。

２．テーマ選定理由①

（1）足元の環境

2022年2月24日のロシアによるウクライナ侵攻により、地政学リスクに対する注目が高まってきている。しかしながら、一般社団法人日本能率協会「日本企業の経営課題2022」の調査結果によれば、BCPについて地政学リスクに対しては9割が未策定となっている。

【出典】一般社団法人日本能率協会「日本企業の経営課題2022」
04 BCP（事業継続計画）の取り組み状況（pp.47-48）
https://www.jma.or.jp/img/pdf-report/keieikadai_2022_report.pdf

２．テーマ選定理由②

（2）新「システム管理基準」Ⅱ .9. 事業継続管理

Ⅱ.9.1 リスクアセスメント

情報システムに影響を与える重大事故、サイバー攻撃、災害、テロ等に対する対応策を具体化するため、影響範囲、業務の重要性及び緊急性を明確にし、復旧優先度を設定する。**その際には、必要に応じて、地政学的要因やサプライチェーンに関連する要因についても考慮する。**

【出典】経済産業省「システム管理基準」（2023年4月26日）
https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kanri-2023.pdf

２．テーマ選定理由③

（3）「サイバーセキュリティ経営ガイドライン Ver 3.0」

・経営者が認識すべき３原則（その2）
サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、**サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要**

・サイバーセキュリティ経営の重要10項目
指示９：**ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策**

【出典】経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 3.0」（2023年3月24日公表）（pp.12-13、pp.29-30）
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

２．テーマ選定理由④

（4）当研究会の取り組み

- サイバーセキュリティがIT部門のみの問題として扱われがちである一方で、地政学リスクはIT部門の問題ではないと捉えている方が多いのではないかと思われる。
- 当研究プロジェクトでは、地政学リスクが情報システムのBCPに与える影響について検討した結果を報告する。

3．地政学リスクとは

①特定地域における紛争、武力行使、政情不安又は大規模災害等により、企業の事業活動におけるサプライチェーンや市場に影響が生じるようなリスク

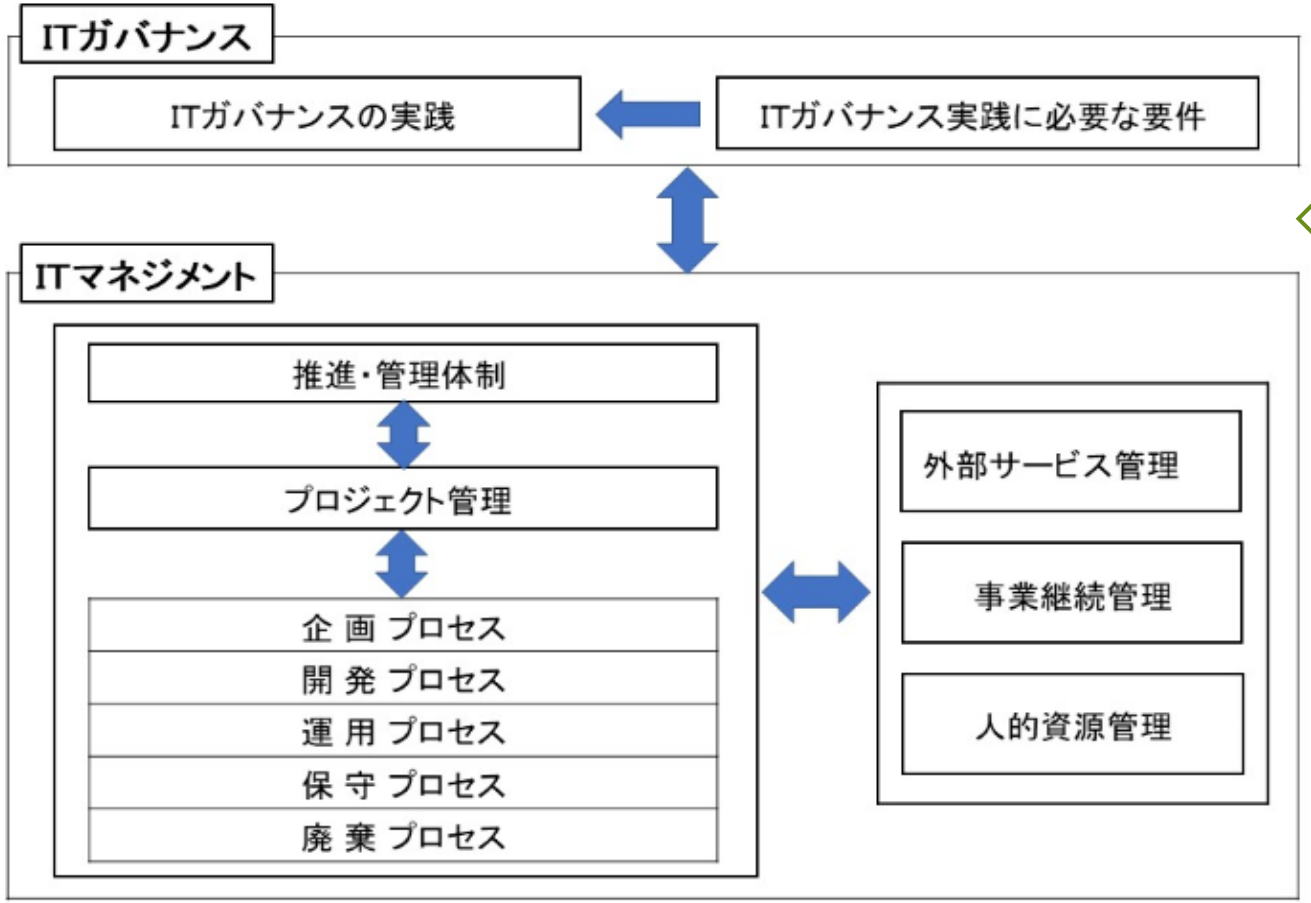
（発表者注）「地政学的リスク」と表記される場合も多い。
【出典】前出「サイバーセキュリティ経営ガイドライン Ver 3.0」脚注3（p.4）

②地政学とは、地球社会を閉じた政治システムと考え、そこで生じる諸問題を、国境や資源、ヒトやモノの流れ、領土やアイデンティティなどに焦点を当てて、様々なスケールで考察すること。

【出典】「現代地政学事典」（現代地政学事典編集委員会/人文地理学会編、丸善出版、2020年1月発行）p. i 刊行にあたって

４．ITガバナンスとITマネジメント①

（1）ITガバナンスとITマネジメントの関係



ITガバナンスにおける取締役会等の活動は、ステークホルダーへの対応及びITマネジメントとそのプロセスに対する評価、指示、モニタから構成される。（p.9）
（図はp.4より転載）

【出典】４．ITガバナンスとITマネジメント①～②
前出：経済産業省「システム管理基準」（2023年4月26日）

４．ITガバナンスとITマネジメント②

（2）地政学リスクに起因するリスク事象への対応

✓ITガバナンスにおけるリスクの評価と対応

・組織体の目的及びIT戦略の目標を達成するために、達成に及ぼす影響についてリスクを評価し、ITシステムの利活用に関する事業継続の方針を策定する。

・地政学リスクの影響は、組織体の事業目的、事業分野における特性、組織体の業種・業態特性、ITシステムの利活用の特性などにより大きく異なる。

✓事業継続に関わるITマネジメント

・上記方針に基づいて、情報システムの業務継続を実現するために、情報システムの業務継続計画を策定し、訓練、検証、報告及び改善を行う。

５．企業の取組状況①

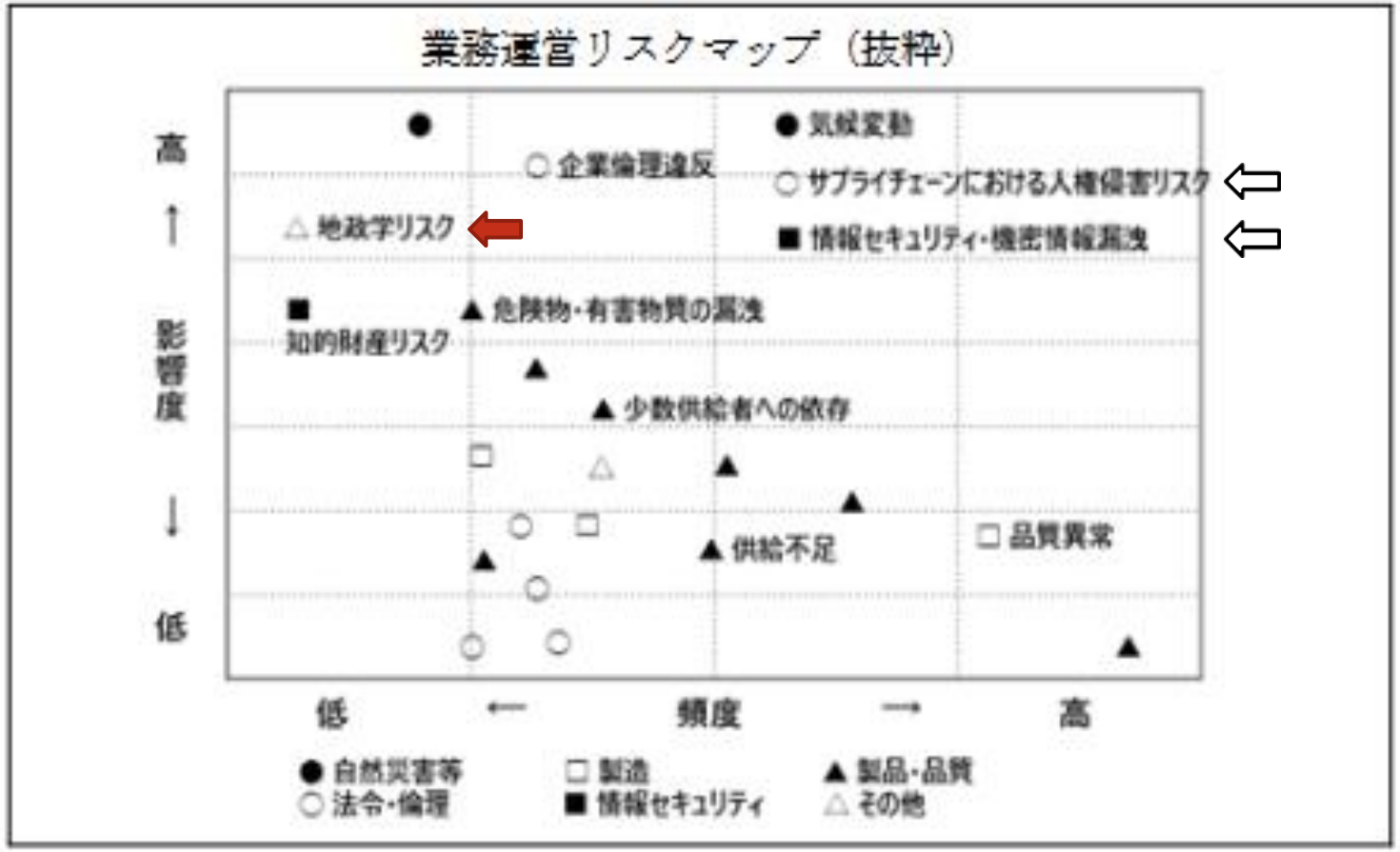
【出典】５．企業の取組状況①～③
金融庁「記述情報の開示の好事例集 2022」（2023年1月31日公表）
https://www.fsa.go.jp/news/r4/singi/20230131/01.pdf

（1）投資家・アナリストが期待する主な開示のポイント
：人的資本、多様性 等（p.58）

・グローバル展開をする企業は、サステナビリティ情報の開示において、例えば、人権に関する地政学リスク等、ロケーションについて着目することも有用

5．企業の取組状況②

（2）帝人株式会社有価証券報告書（2022年3月期）の開示例（p.124）



５．企業の取組状況③

（3）オムロン株式会社有価証券報告書（2022年3月期）の開示例（p.129）
地政学リスク［主な取組み］

- 主要国の関税引上げや安全保障貿易管理に基づく輸出規制、新興技術等に対する取引制限等の政策に対する分析と評価
- 取引形態やサプライチェーンの見直し
- 製品を複数拠点で並行して生産する体制の構築

6．地政学リスクの特性①

（1）発生要因別分類

	発生要因	地域的特性	主な影響	他のリスクカテゴリーとの関連
①	テロ、クーデター、戦争・紛争等	特定の国・地域において発生	サプライチェーン	–
②	経済安全保障上の各種規制	特定の国・地域が対象		–
③	政治的・軍事的目的あるいは活動資金獲得目的によるサイバー攻撃	特定の国・地域・団体等からの攻撃		サイバーセキュリティリスク
④	人権侵害	特定の国・地域において発生		人権リスク

６．地政学リスクの特性②

（2）リスクアセスメント、優先順位付けにおける特性

・リスクの高い国・地域は、一定の時間軸の中ではある程度特定されるが、予見は困難。（前頁①と④）

・特定の製品・サービスが影響を受ける。（前頁②）

・他のリスクカテゴリーと一緒に検討。（前頁③と④）

⇒発生可能性・影響度を考慮し、自社に適合したリスクシナリオを作成（原因事象型アプローチ）し、リスクアセスメントを行い、優先順位付けも含め、既存の結果事象型BCPの見直しを行う。

7．サプライチェーンの強靭化

■ 企業はサプライチェーン全体の強靭化に向けた取組みを加速すべき

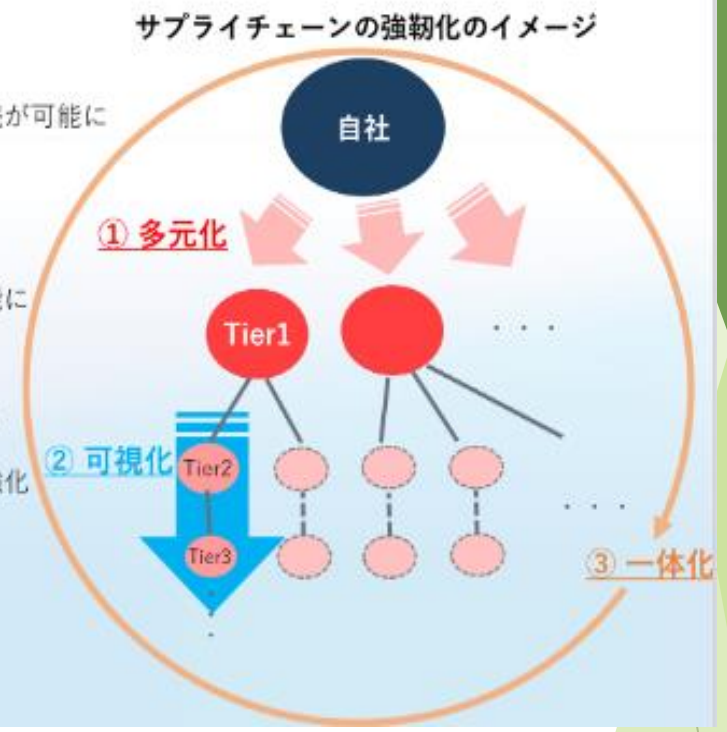
✓ ①多元化、②可視化、③一体化の３つの取組みによってサプライチェーンの強靭化を推進

政府は**強靭化に向けた税制措置**等により支援

① 多元化
あるサプライチェーンが
機能不全になっても事業継続が可能に

② 可視化
何をどこに供給すべきか、
在庫をいかに確保すべきか、
非常時にも迅速に判断が可能に

③ 一体化
サプライチェーン全体を貫く
ＢＣＰの策定等により
事業活動のレジリエンスを強化



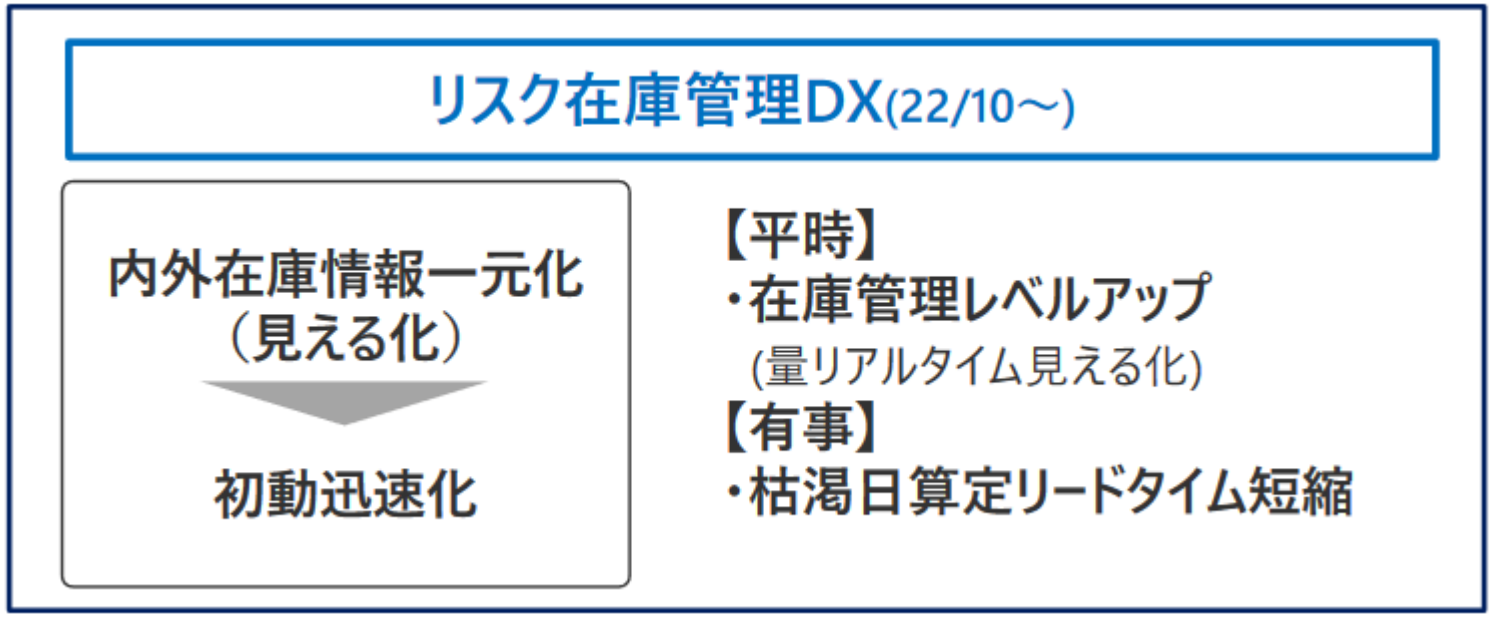
【出典】一般社団法人日本経済団体連合会「非常事態に対してレジリエントな経済社会の構築に向けて － 新型コロナウイルス感染症の経験を踏まえて －」（2021年2月16日公表）
https://www.keidanren.or.jp/policy/2021/016.html

8．サプライチェーンの多元化

	2022年5月			対前年同月比		
（%）	全体	大企業	中小企業	全体	大企業	中小企業
調達先・仕入先の分散	38.1	33.6	39.4	3.0	2.1	3.2
生産・物流拠点の分散	19.5	22.1	18.7	-1.0	-1.2	-1.0
代替生産先・仕入先・業務委託先・販売場所の確保	19.0	17.5	19.4	-0.2	0.7	-0.5

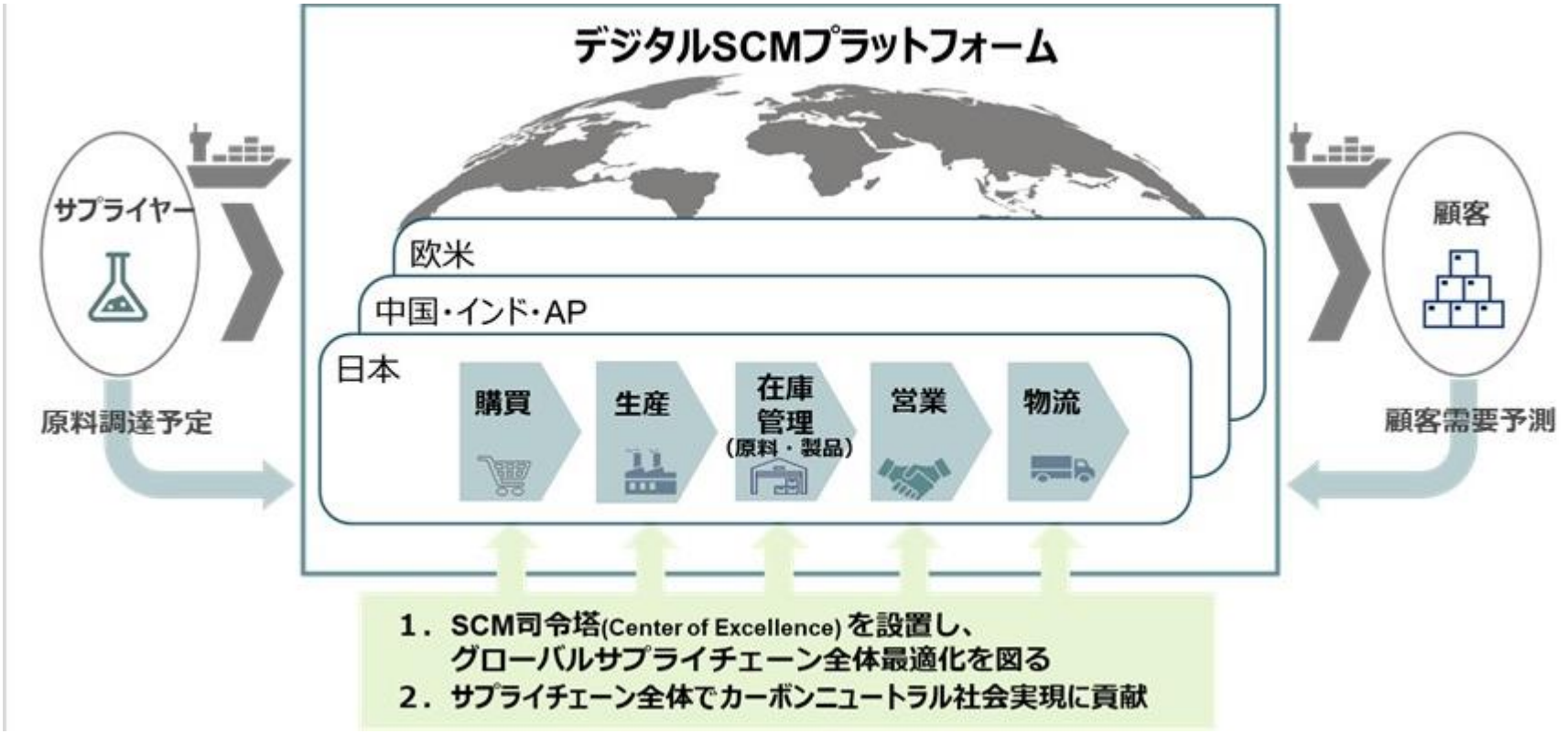
【出典】帝国データバンク「事業継続計画（BCP）に対する企業の意識調査（2022年）」（2022年6月14日）
事業中断リスクに備えた実施・検討内容（複数回答：母数は、事業継続計画(BCP)を「策定している」「現在、策定中」「策定を検討している」のいずれかを選択した企業5,800社）
https://www.tdb.co.jp/report/watching/press/pdf/p220606.pdf

９．サプライチェーンの可視化の例①



【出典】株式会社デンソー「半導体戦略説明会」資料（2022年6月1日）p.4
https://www.denso.com/jp/ja/-/media/global/about-us/investors/business-briefing/20220601_semicon_material_jp.pdf

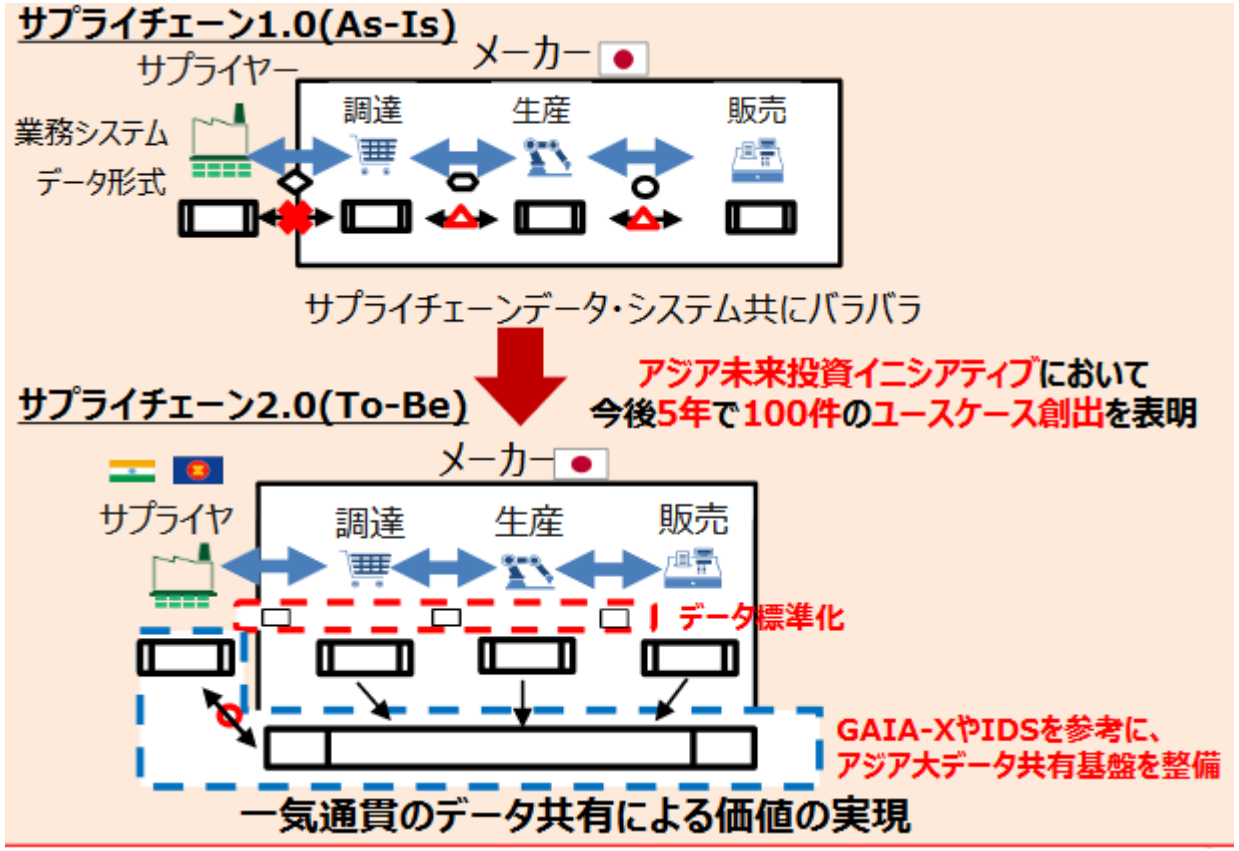
９．サプライチェーンの可視化の例②



【出典】ＤＩＣ株式会社プレスリリース（2023年4月24日）：グローバル全体最適のための「デジタルSCMプラットフォーム」を構築 －先進のデジタル技術を活用した持続可能で強靭なサプライチェーンを実現－
https://www.dic-global.com/ja/news/2023/ir/20230419171310.html

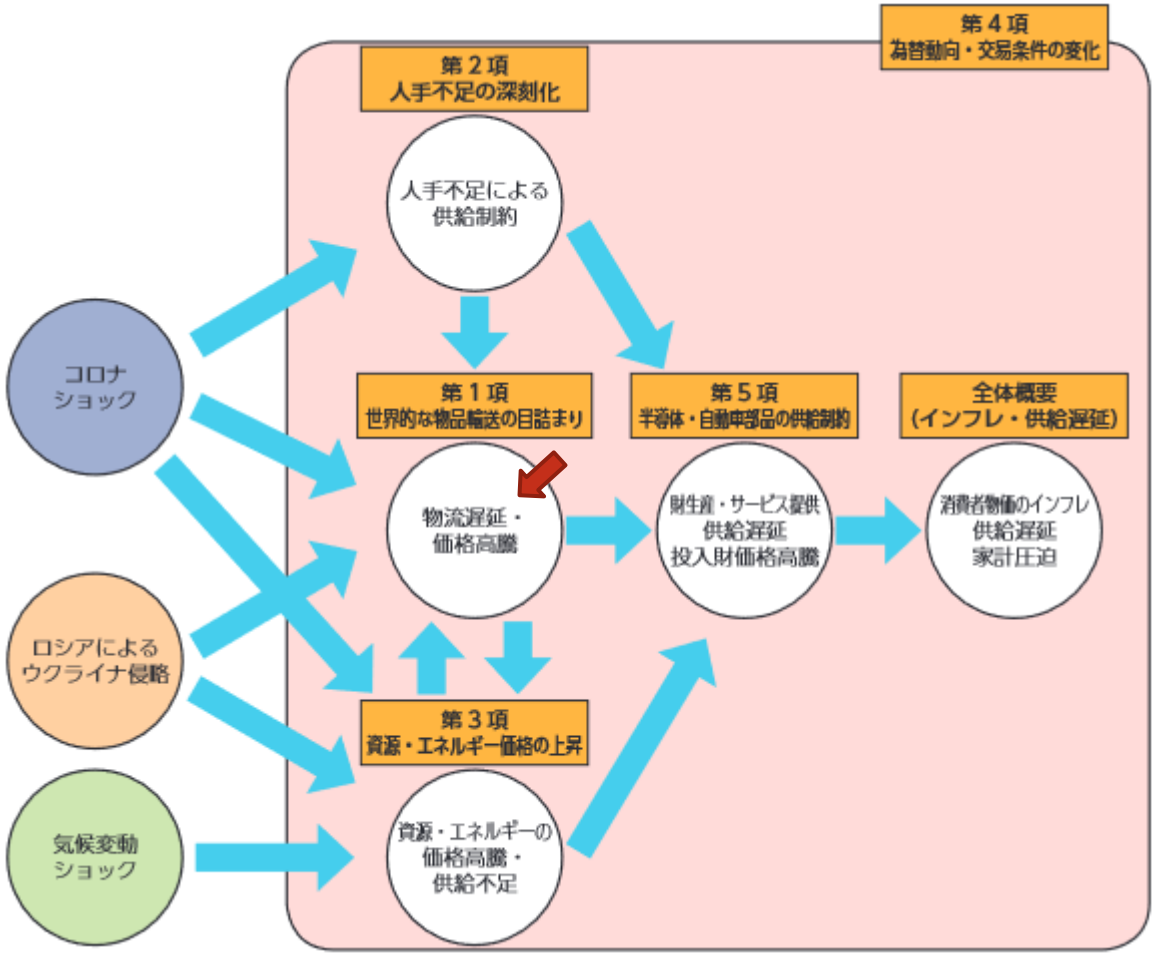
9．サプライチェーンの可視化の例③

・データ連携によるアジアのサプライチェーンのアップグレードの検討事例



【出典】経済産業省「産業構造審議会経済産業政策新機軸部会（第3回）」（2022年2月4日）事務局説明資料4（p.33）
https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/pdf/003_04_00.pdf

10. SCMを下支えする物流の強靭化①

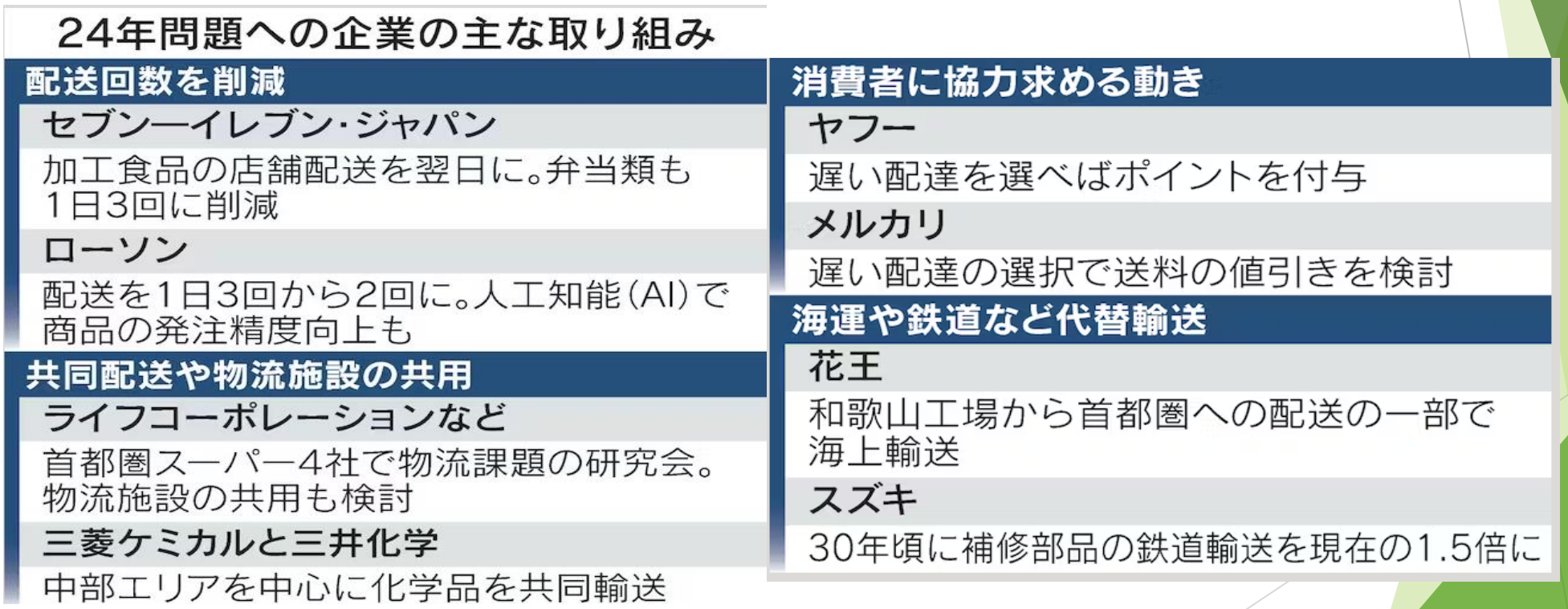


【出典】「通商白書2022」第Ⅰ部_第1章_第2節 世界的な供給制約の高まり
第I-1-2-1図 サプライチェーンにおける供給制約の関係図

10. SCMを下支えする物流の強靭化②

（1）物流「2024年問題」

・24年4月からトラック運転手に時間外労働の上限規制が適用され、輸送能力の縮小は避けられない。



24年問題への企業の主な取り組み

配送回数を削減

セブン―イレブン・ジャパン

加工食品の店舗配送を翌日に。弁当類も1日3回に削減

ローソン

配送を1日3回から2回に。人工知能（AI）で商品の発注精度向上も

共同配送や物流施設の共用

ライフコーポレーションなど

首都圏スーパー4社で物流課題の研究会。物流施設の共用も検討

三菱ケミカルと三井化学

中部エリアを中心に化学品を共同輸送

消費者に協力求める動き

ヤフー

遅い配達を選べばポイントを付与

メルカリ

遅い配達の選択で送料の値引きを検討

海運や鉄道など代替輸送

花王

和歌山工場から首都圏への配送の一部で海上輸送

スズキ

30年頃に補修部品の鉄道輸送を現在の1.5倍に

【出典】2023年6月6日（火）日本経済新聞朝刊（3）面

11. ソフトウェアサプライチェーン①

（1）ソフトウェアサプライチェーンに対する脅威の増大

・ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、クラウドやオンプレミスなどのソフトウェアに対するセキュリティ脅威が近年増大。2021年12月に発見され、世界的に大きな影響を及ぼしたApache Log4jは、脆弱性情報が公開された直後からさまざまなマルウェアや国家支援型サイバー攻撃グループによって悪用されていることが報告されている。

【出典】経済産業省「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」第9回（2023年2月28日）資料3「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/009_03_00.pdf

11. ソフトウェアサプライチェーン②

(2) ソフトウェアの適切な管理について

- ソフトウェアに対するセキュリティを強化し、企業の信頼・安全につなげていくためには、ソフトウェアを適切に管理していくことが重要。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- SBOMとは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのことで、世界的に導入企業が増加している。

【出典】前出：第9回「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」資料3

11. ソフトウェアサプライチェーン③

(3) SBOM導入の主なメリット

- 脆弱性管理のメリット：脆弱性残留リスクの低減、脆弱性対応期間の低減、脆弱性管理にかかるコストの低減
- ライセンス管理のメリット：ライセンス違反リスクの低減、ライセンス管理にかかるコストの低減
- 開発生産性向上のメリット：開発遅延の防止、開発にかかるコストの低減

【出典】前出：第9回「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」資料3、
同参考資料「SBOM（Software Bill of Materials）の導入に関する手引（案）」（2023年度、意見公募手続予定）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/009_s01_00.pdf

12. 経済安全保障推進法関連①

(1) サプライチェーン強靭化取組に関する進捗について

- 2022年12月、11物質※を特定重要物質に指定。
- 民間事業者等が作成する供給確保計画の認定要件（供給安定性）として、「事業継続性確保のため、事業継続計画が策定されていること。」も挙げられている。

※抗菌性物質製剤、肥料、永久磁石、工作機械・産業用ロボット、航空機の部品、半導体、蓄電池、クラウドプログラム、天然ガス、重要鉱物及び船舶の部品

【出典】
内閣官房「経済安全保障法制に関する有識者会議」第6回（2023年4月5日）資料5「サプライチェーンの強靭化に向けた取組について」
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai6/siryou5.pdf
内閣府「安定供給確保を図るための取組方針」及び認定供給確保計画の概要
https://www.cao.go.jp/keizai_anzen_hosho/sc_houshin.html

12. 経済安全保障推進法関連②

(2) サプライチェーン強靭化に向けたリスク点検

- 物資所管各省において、特定重要物資を中心にサプライチェーンリスクの点検・評価を行い、対応策を検討。点検結果については、①各省庁におけるリスク対応への取組の強化に加えて、②省庁間で連携すべき課題の把握と省庁横断的な政策の立案･遂行につなげる。
- サプライチェーンリスクの点検・評価を踏まえ、我が国にとって重要な物資のサプライチェーン強靭化に必要な更なる措置を検討し、経済安全保障推進法の着実な実施と不断の見直し、更なる取組の強化を図る。

【出典】前出：第6回「経済安全保障法制に関する有識者会議」資料5

12. 経済安全保障推進法関連③

(3) セキュリティ・クリアランス（SC）制度検討状況

- 高市早苗経済安全保障相が6月6日の記者会見で、セキュリティー・クリアランス制度の導入に向けた中間論点整理を公表した。2014年に施行した特定秘密保護法に基づく「適性評価」を民間企業などに広げた「産業版」と位置づける。
- 主要7カ国（G7）で同制度がないのは日本だけだ。政府は財界や法律の専門家でつくる有識者会議の議論をもとに、24年中の法整備を視野に入れる。

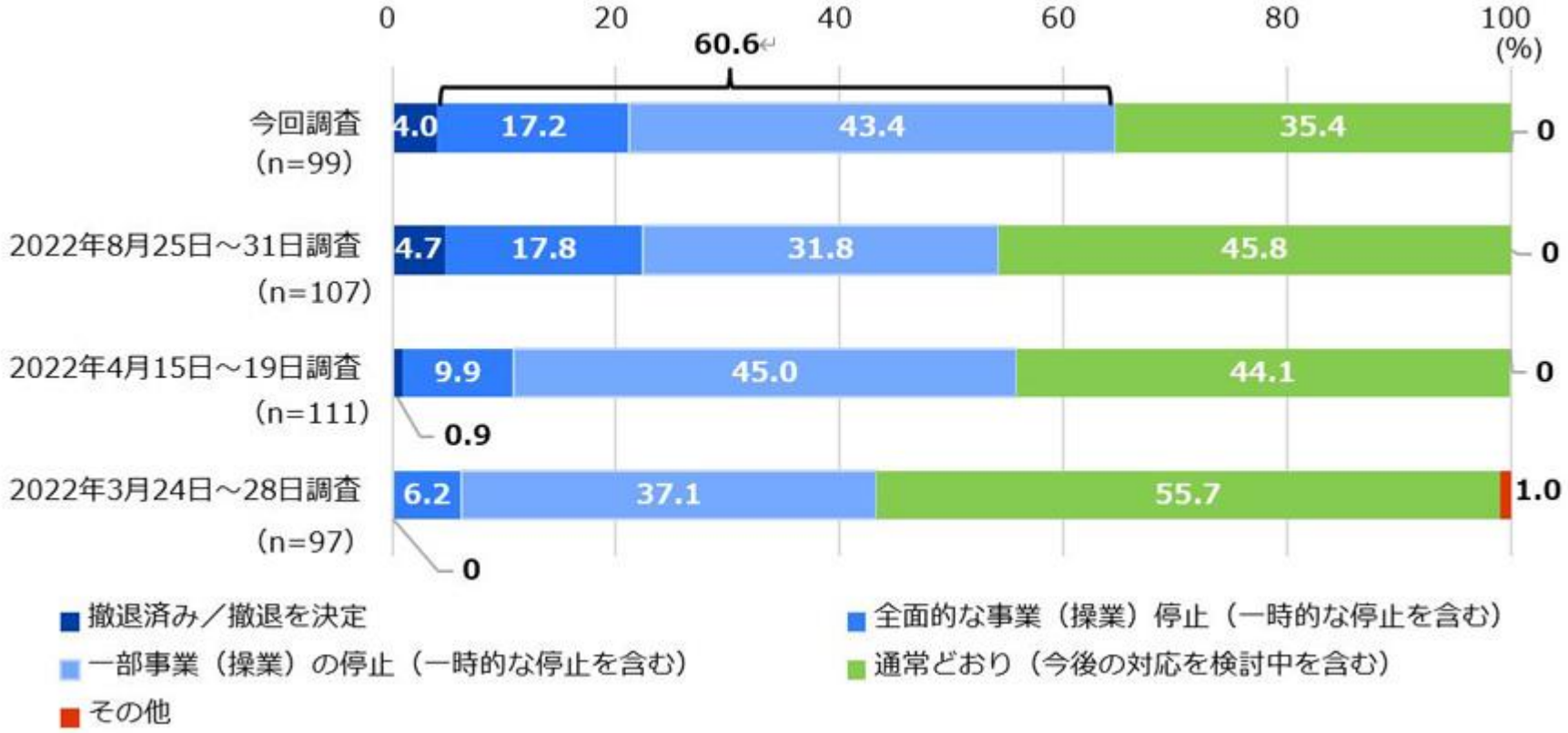
【出典】2023年6月7日（水）日本経済新聞朝刊1,3,4面「機密情報取り扱いに資格 来年にも立法　経済安保の体制整備」
経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」（2023年6月6日）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html

13. 撤退計画の立案について①

　紛争等が生じる可能性がある場合には、事前に撤退計画を検討しておくことが大切である。そうしておくことで、人権への負の影響の特定・評価や、その緩和策の検討を行うことができ、撤退をするとしても、ステークホルダーへの負の影響を可能な限り緩和した責任ある形で撤退することが可能になる。緩和策としては、例えば、従業員と安全上の懸念について対話を行いその結果を踏まえて対応策を講じること、危機が続く間は従業員が継続して収入を得られるようにすることなどが考えられる。

【出典】経済産業省「責任あるサプライチェーン等における人権尊重のためのガイドライン」（2022年9月13日公表）
4.2.2 紛争等の影響を受ける地域からの「責任ある撤退」（pp.24-25）
https://www.meti.go.jp/press/2022/09/20220913003/20220913003-a.pdf

【参考】ロシア事業の現状（JETRO調査）



【出典】独立行政法人日本貿易振興機構（ジェトロ）「ロシア・ウクライナ情勢下におけるロシア進出日系企業アンケート調査結果（2023年1月）―侵攻から1年、厳しさ増す日系企業を取り巻く情勢―」（2023年2月22日公表）
https://www.jetro.go.jp/news/releases/2023/979249b4def8a139.html

13. 撤退計画の立案について②

（1） IT部門における撤退計画の立案について

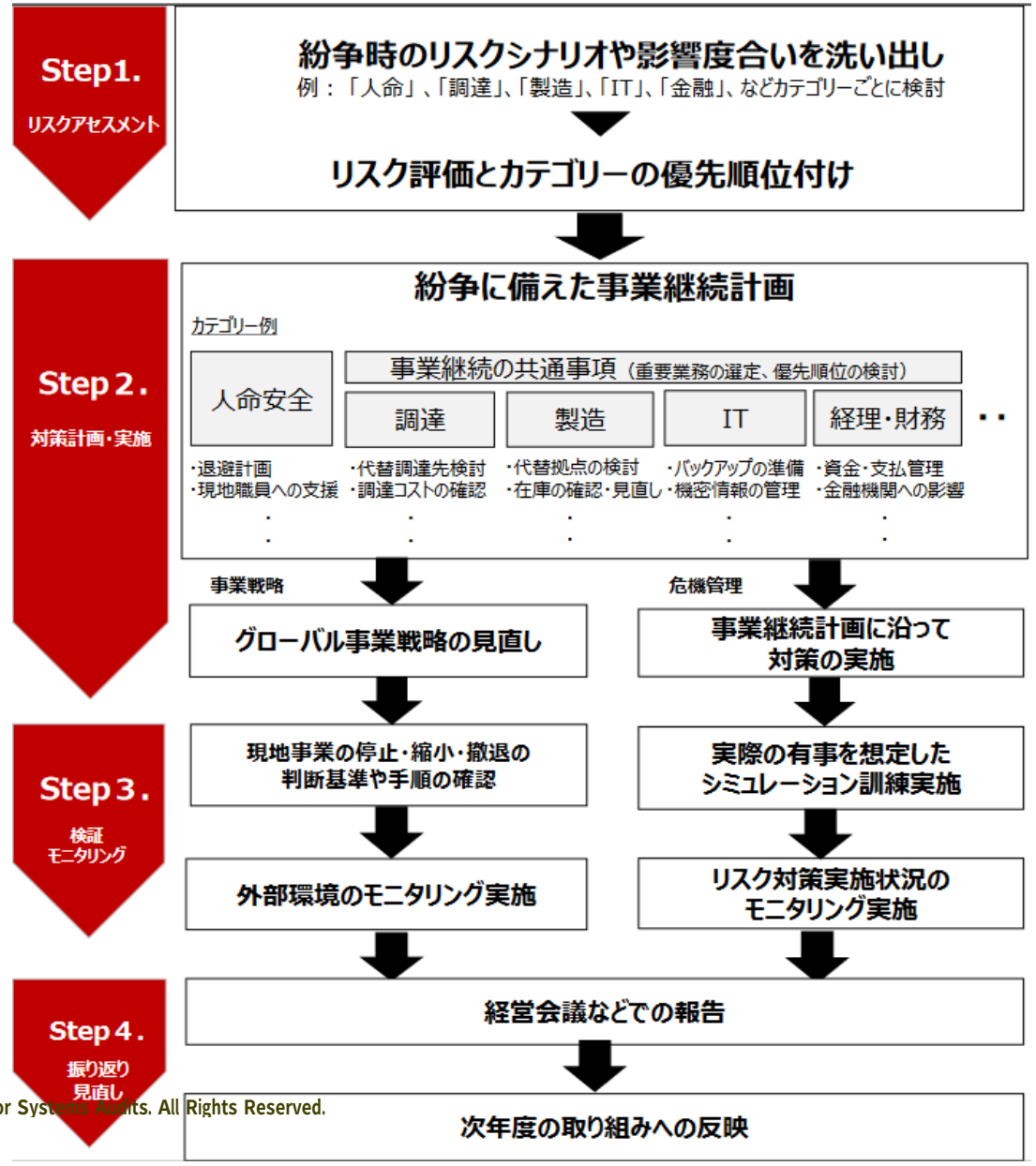
・事前準備：重要なデータの暗号化、バックアップ

・紛争等発生時の対応：重要なデータの移送、廃棄、ハードウェア・ソフトウェアの処分

・人員の安全確保・避難計画は、全社的計画に包含

（注）撤退以外に、事業縮小や停止も検討される。

14. リスクアセスメント～対策の一例



【出典】損保ジャパンRMレポートIssue233（2022.10.28発行）「地政学リスクと企業における紛争危機への備え～台湾危機に関する情勢分析や今後の備え～」（p.8 図1 対策イメージ図）
https://image.sompo-rc.co.jp/reports/r233.pdf

15. 最後に

・地政学リスクも包含したＢＣＰを組織のビジネスプロセス、ガバナンスに組み込み、IT部門も含め、全社的対応として取り組んでいくことにより、機動的・柔軟で継続的な改善を図っていくことが必要。