資料２

NISC National center of Incident readiness and Strategy for Cybersecurity

コーポレートガバナンスにおける サイバーセキュリティの取扱いについて

令和4年6月

内閣官房 内閣サイバーセキュリティセンター
基本戦略第1グループ

近年のリスク・サイバー攻撃の動向

＜環境変化に伴うリスクの動向＞

- グローバルサプライチェーンを経由する製品・サービスの拡大・浸透（オープンAPI、OSSの普及）
- クラウドサービスの利用拡大
- デジタル化により攻撃の誘引性増
- デジタルサービス間連携が隙に
- 技術の悪用（AI技術の活用等）
- デジタル参画増によるリテラシー差異、人材不足・偏在が隙に

＜国際情勢に伴うリスクの動向＞

- 国家の関与が疑われる攻撃
- サプライチェーンの過程で不正機能等が埋め込まれるリスク（サプライチェーン・リスク）の顕在化
- サイバー空間に関する基本的価値観の相違の顕在化（国家によるデータ収集・管理・統制の動きも）

＜近年の攻撃傾向＞

- サイバー攻撃の組織化・洗練化・増大
- サプライチェーンの弱点を悪用した大規模攻撃
- ランサムウェアの広がり　FY20下期21件 → FY21下期85件（二重脅迫の傾向）
- VPNやクラウドサービスの脆弱性悪用
- 匿名性化技術による追跡の回避
- 重要インフラ・サービスへの攻撃（経済社会への影響増）
- 国民情報や知的財産の窃取
- 民主プロセスへの干渉（虚偽情報拡散・世論誘導）

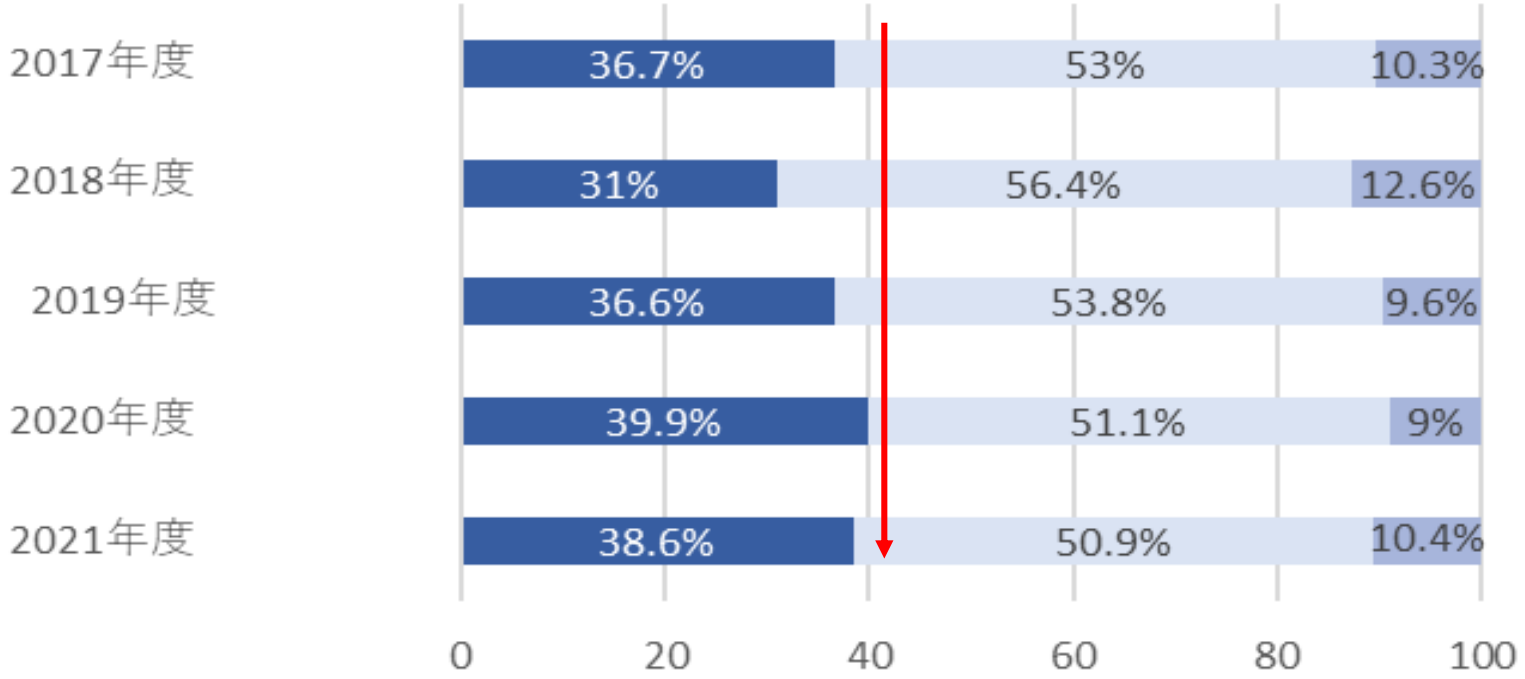
[出典]「サイバーセキュリティ戦略」（2021年9月閣議決定）「３．サイバー空間を取りまく課題認識」より作成

サイバー攻撃の量的な増加、対象の変容・拡大、手法の複雑化・巧妙化、目的の多様化

経営層の関与①

■ ここ数年、セキュリティへの経営層の関与度合いは大きく進展していない。

■日本企業におけるセキュリティへの経営層の関与度合い



■経営層は、セキュリティリスクを経営課題のひとつと認識しており、セキュリティリスクや重大なセキュリティ対策については、経営会議等で審議・決定される

■経営層は、セキュリティリスクや重大なセキュリティ対策の重要性を認識しているが、取組みは主にIT部門などに任せ経営会議で議論されない

■経営層は、セキュリティリスクおよび対策について重要性を認識しておらず、ほとんど会話することがない

［出典］ （一社）日本情報システムユーザー協会 各年度の「企業IT動向調査報告書」よりNISC作成

（参考）米国の動向

米国ではサイバーセキュリティについて、経営層であるCEOが取締役会に報告する割合が56%との報告がある。

※ “NACD Public Company Governance Survey 2019-20”（2019.12）

経営層の関与②

- セキュリティ対策実施のきっかけはインシデント事例に基づくケースが多く、米国と比較して、経営層のトップダウン指示に基づくケースは低い。
- 自社のセキュリティに対する課題認識について、「経営層・役員」と「部長」の間で差異がみられる。

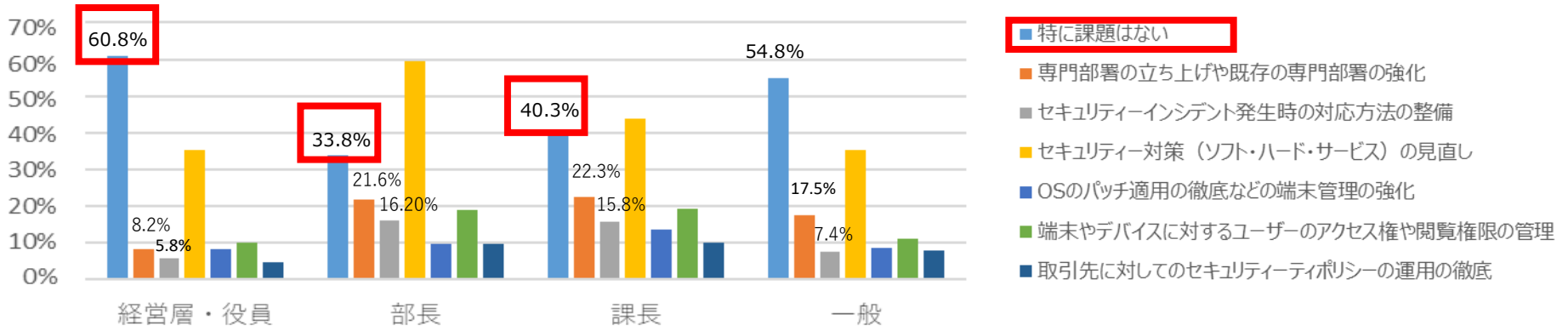
■直近1年に実施したセキュリティ対策の実施のきっかけや理由

	日本	米国
1位	27.6% 他社でのセキュリティインシデント事例	54.8% 経営層のトップダウン指示
2位	25.6% 自社でのセキュリティインシデント事例	25.0% 他社でのセキュリティインシデント事例
3位	21.6% 経営層のトップダウン指示	24.5% 株主や取引先からの要請

※ 左記以外の選択肢：
・監督省庁からのセキュリティ対策強化の要請（自治体からの要請を含む）
・関連法規の改定（具体的な要請内容を記載）
・持株会社や親会社からの要請
・競合他社の実施状況との比較
・外部監査・第三者評価の結果
・内部監査・内部有識者からの指摘
・COVID-19に伴うテレワーク対応
・東京2020大会（オリンピック・パラリンピック）に伴う対応
・DX化推進に伴う対応
・その他（具体的に記載）
・わからない

[出典] NRIセキュアテクノロジーズ㈱「NRI Secure Insight 2021」（2022年2月）

■自社におけるセキュリティインシデントに対する課題（役職別）

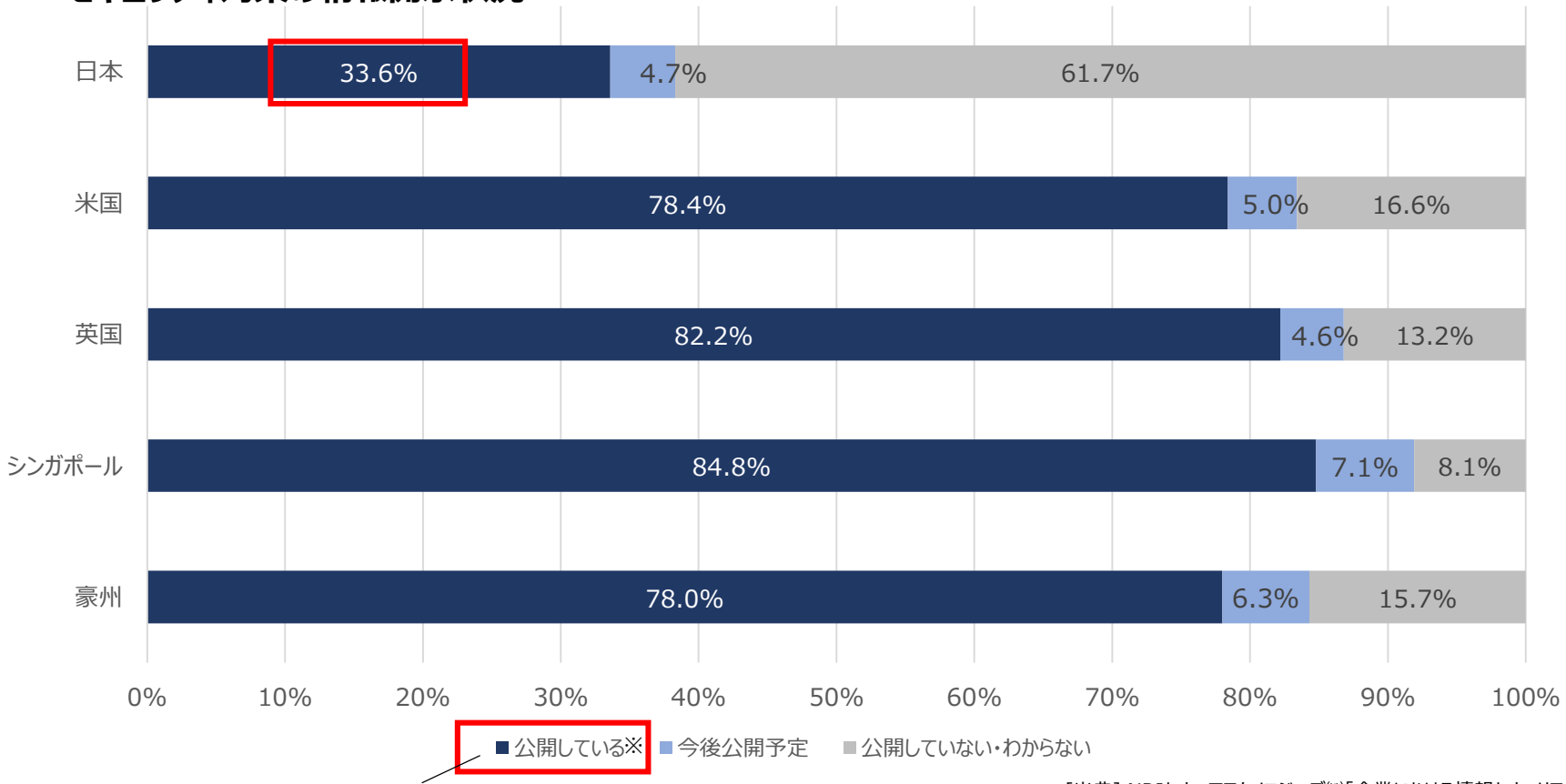


[出典] NTTビジネスソリューションズ(株)「サプライチェーン攻撃に関する市場調査レポート」（2022年5月）よりNISC作成

セキュリティ対策の情報開示

■ 2018年時点の国際比較では、セキュリティ対策の情報開示は他国と比べて進んでいないとされている。

■セキュリティ対策の情報開示状況



※「企業のWebサイトの情報セキュリティに特化したページ（情報セキュリティ報告書等）で公開している」
「企業のWebサイトの情報セキュリティ以外のページ（CSR、年次報告書等）で公開している」
「業界団体やISAC等のコミュニティ内で公開・共有している」
「講演会やセミナー等で公開している」

[出典] NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査2018」(2018年7月)

※ なお、2019年から2021年の間で、有価証券報告書にリスク事項として「セキュリティ」を記述している企業は58%から81%に上昇している。
[出典] (一社)IT団体連盟「サイバーインデックス企業調査2021」（2021年11月）

セキュリティに関する専門性の情報開示

■ 専門性に関する開示の中で、サイバーセキュリティについて取り扱われる事例は僅少。

■日本企業におけるスキル・マトリックスへの記述状況

- 2021年6月、コーポレートガバナンス・コードにおいて、「各取締役の知識・経験・能力等を一覧化したいわゆるスキル・マトリックスをはじめ、経営環境や事業特性等に応じた適切な形で取締役の有するスキル等の組み合わせを取締役の選任に関する方針・手続と併せて開示すべきである」とされた。
- 2021年6月時点で株式時価総額トップ100企業のうち、スキル・マトリックスを開示している企業は50社。
- 上記50社のうち、「セキュリティ」に関する項目を設けていた企業は6%（3社）。

［出典］コーン・フェリー・ジャパン「スキル・マトリックスの開示状況」（2021年6月） よりNISC確認

■米国経営層において強化する必要がある専門知識の領域

[出典] “NACD Public Company Governance Survey 2016-17”(2016.11)

※**NACD** (National Association of Corporate Directors：全米取締役協会)

（参考）機関投資家ヒアリング調査

■ 機関投資家からも、具体的な開示項目に関する言及はないが、体制やリスク等に関するわかりやすい開示が求められている。

機関投資家による投資先企業のサイバーセキュリティ対策状況の確認について

- ✓ セキュリティ体制は機能していることが重要。現場と経営陣が円滑につながっているかを確認したい。
- ✓ 扱う情報が多い業種・業態のリスクは高いと考える。データの流出が企業の存続に関わるようなケースでは詳細に確認する。
- ✓ 開示情報のエビデンスは重視していない。エビデンスがあってもリスクはゼロにならない。プライバシーマークやISO認証などは若干の安心材料だが、体制や想定リスクに関する質問に対し、クリアな情報が提示されることが重要。
- ✓ 事故発生の可能性はゼロにならないので、リカバリーの体制が取られているのかを含めた開示を期待。
- ✓ サイバーセキュリティの世界は、人権デューデリジェンスに近い捕捉の難しさがあると感じている。PDCAを通じたレベルアップを前提に、基準や取組事項をまとめた行動計画を普及させるべきではないか。

今後参考となりそうなポイント（機関投資家等によるDXやリスク管理等に関する評価方法について）

- ✓ 「気候関連財務情報開示タスクフォース（TCFD）」が「ガバナンス」、「戦略」、「リスク管理」、「指標と目標」の４つの柱に関して開示のプロトタイプを示している。投資家はこうした動きになじみはじめており、他のリスクに関しても開示のプロトタイプとして、わかりやすい開示を求める動きが出てくる可能性がある。
- ✓ 法律で開示が求められている情報の内容は各社とも似通っており、あまり読むことはない。自社にとって致命的なリスクをメリハリをもって示すことが重要。

[出典] 経済産業省 産業サイバーセキュリティ研究会 第8回ワーキンググループ2（経営・人材・国際）資料（2022年3月）

サイバーリスクの経営へのインパクト

■ サイバーリスクの経営へのインパクトには様々なものが存在する一方で、このようなリスクは経営層・投資家双方で認識されづらい状況。

初動対応時のコスト

- 事故原因・影響範囲調査
- 復旧・再発防止
- 弁護士等費用

※ ランサムウェアの場合、約80億円の身代金が要求されたケース等も報道されている[1]

事業への影響

- 生産・営業停止
  → 売上へのインパクト（×日数）
- ブランドイメージの毀損、株価下落
  ※ 民間調査では約8割の企業[2]
- 取引先からの信用下落

事後対応にかかるコスト

- 損害賠償
- 情報漏洩に対する罰則

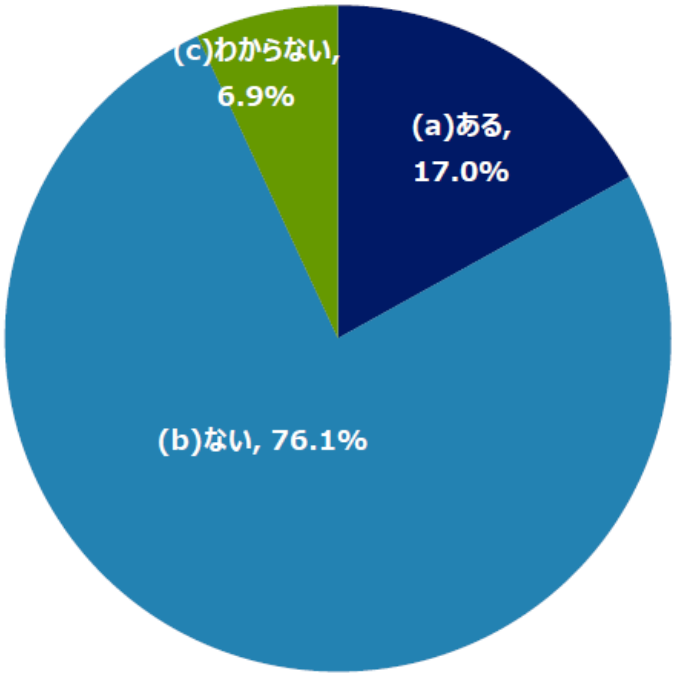
[1] “REvil gang asks for $70 million to decrypt systems locked in Kaseya attack” (2021年7月4日)
https://www.bleepingcomputer.com/news/security/revil-ransomware-asks-70-million-to-decrypt-all-kaseya-attack-victims/
[2] (株)サイバーセキュリティクラウド プレスリリース（2022年2月） https://www.cscloud.co.jp/news/press/202202174115/
[全体項目] JNSA「インシデント損害額調査レポート2021」（2021年8月）等よりNISC作成

取引先企業におけるサプライチェーン・リスク

■ 取引先企業がサイバー攻撃の被害を受け、自社に影響を及ぼす事案も一般的になりつつある。

取引先等を経由したサイバー攻撃被害の経験

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



(N=1876)

[出典] 経済産業省 産業サイバーセキュリティ研究会 第8回ワーキンググループ2（経営・人材・国際）資料（2022年3月）

サイバーリスクハンドブック：取締役向けハンドブック

■ 2019年10月にNACD（全米取締役協会）・ISA（米国インターネット・セキュリティ・アライアンス）による「Cyber Risk Oversight Director's Handbook」（米国版ハンドブック）を参考に、すべての取締役に当てはまる原則を整理。

サイバーセキュリティ経営ガイドラインの改訂

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。（2017年ver2.0）
- 近年のサイバーセキュリティ経営を取り巻く情勢の変化等を踏まえ、2022年度中に改訂を実施予定。

1．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

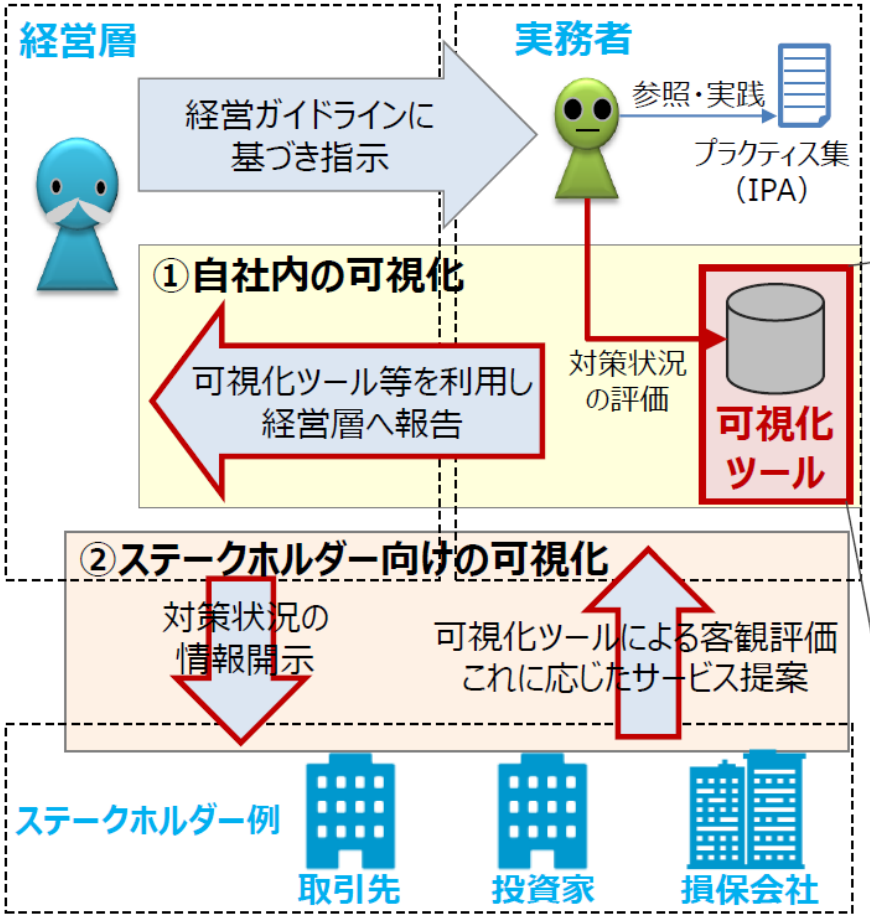
2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

[出典] 経済産業省 産業サイバーセキュリティ研究会 第7回ワーキンググループ2（経営・人材・国際）資料（2021年2月）

サイバーセキュリティ経営可視化ツールWeb版

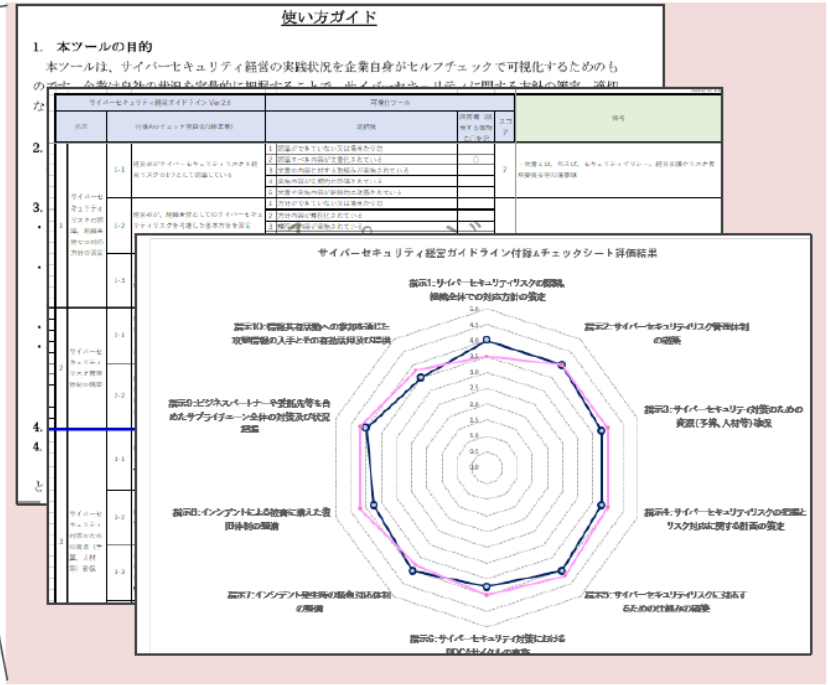
■ 「経営ガイドライン」に基づく指示への対策状況に関し、経営層による自社リスクの可視化や把握、ステークホルダー（取引先、投資家等）とのコミュニケーションに活用できる評価ツール。（2021年8月Web版公開）



特徴

- 39個の質問に回答⇒実践状況をレーダーチャート表示
- 過去の診断結果とも比較（経年変化）可能※
- 各業種の平均値とも比較可能※
- 「サイバーセキュリティ経営ガイドラインVer.2.0実践のためのプラクティス集」の実践事例も表示可能※

（※β版からの改良点）



https://www.ipa.go.jp/security/economics/checktool/index.html

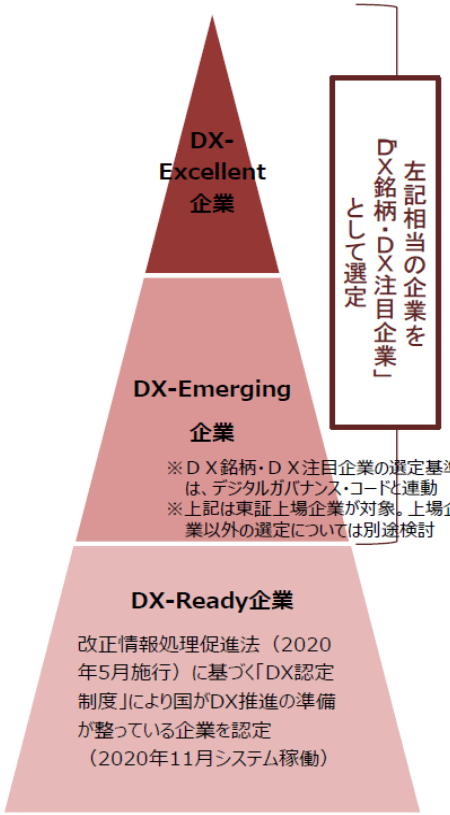
[出典] 経済産業省 産業サイバーセキュリティ研究会 第8回ワーキンググループ2（経営・人材・国際）資料（2022年3月）

デジタルガバナンス・コード等に基づくインセンティブ

- DXを進める企業におけるステークホルダーとの対話の在り方を示す「デジタルガバナンス・コード」について、「経営者がサイバーセキュリティリスクを経営リスクの1つとして認識」することをはじめ、望ましい方向性に係る取組例等を明記。
- DX投資促進税制の要件の1つとなっている「DX認定制度」の認定基準や、「DX銘柄・DX注目企業」の選定時の評価基準として活用。（インセンティブ）

DX経営の推進

◆DX企業の体系



左記相当の企業を「DX銘柄・DX注目企業」として選定

※ＤＸ銘柄・ＤＸ注目企業の選定基準は、デジタルガバナンス・コードと連動
※上記は東証上場企業が対象。上場企業以外の選定については別途検討

※「DX認定」は、「DX投資促進税制」の要件の一つとなっている。

評価基準

◆デジタルガバナンス・コード(2020年11月策定)
経営者が企業価値向上に向け実践すべき事項
1．経営ビジョン・ビジネスモデル
2．戦略
3．成果と重要な成果指標
4．ガバナンスシステム（セキュリティ）

望ましい方向性に係る取組例より：
○経営者がサイバーセキュリティリスクを経営リスクの1つとして認識し、CISO 等の責任者を任命するなど管理体制を構築するとともに、サイバーセキュリティ対策のためのリソース（予算、人材）を確保。
○情報処理安全確保支援士（登録セキスペ）の取得を会社として奨励。
○サイバーセキュリティを経営リスクの一つと捉え、その取組を前提としたリスクの性質・度合いに応じて、サイバーセキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等への記載を通じて、開示を行っている。

認定基準：
○戦略の実施の前提となるサイバーセキュリティ対策を推進していること。
※サイバーセキュリティ経営ガイドライン等に基づき対策を行い、セキュリティ監査（内部監査を含む）を行っていることの説明文書等が提出されることをもって確認する。
※中小企業においては、SECURITY ACTION制度に基づき自己宣言(二つ星)を行っていることを確認する方法でも可とする。

サイバーセキュリティ経営の推進

1st Step サイバーセキュリティ経営の明確化
➢「サイバーセキュリティ経営ガイドライン」(2017年10月Ver2.0)の普及・定着【累計10万DL】

2nd Step サイバーセキュリティ経営の定着
➢「プラクティス集」(2020年6月第2版)「体制構築・人材確保の手引き」(2021年4月第1.1版)の整備により、サイバーセキュリティ経営を現場レベルで推進

3rd Step セキュリティの高い企業であることの可視化
➢「可視化ツール」の普及によるサイバーセキュリティ経営の可視化の推進

活用推奨

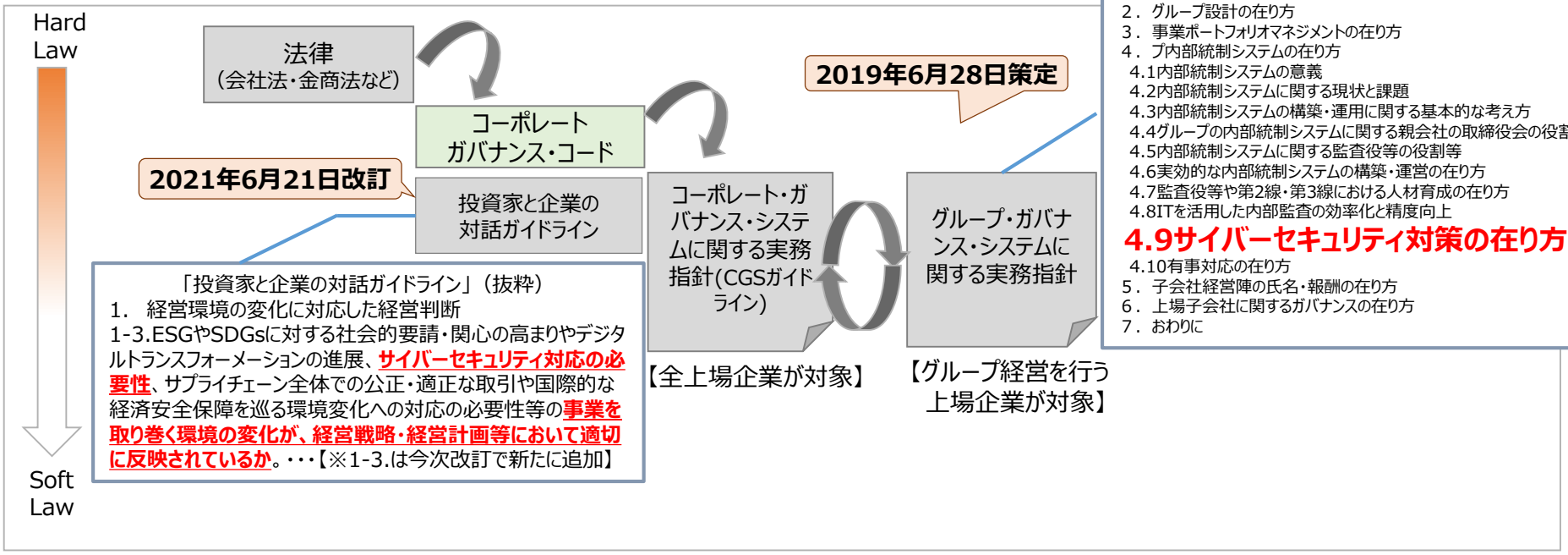
活用推奨

◆Web版「可視化ツール」※
※経営ガイドライン実践状況の可視化ツールV1.0
→①経営層による自社リスクの可視化/把握
②ステークホルダー（取引先、投資家、損保会社）とのコミュニケーションに活用

[出典] 経済産業省 産業サイバーセキュリティ研究会 第8回ワーキンググループ2（経営・人材・国際）資料（2022年3月）

コーポレートガバナンス・コードに係る位置づけ

■ 2021年6月に改訂された、「スチュワードシップ・コード」及び「コーポレートガバナンス・コード」の附属文書である「投資家と企業の対話ガイドライン」（2021年6月改訂）において、新たに、サイバーセキュリティ対策の必要性等を含む事業環境変化の経営戦略・経営計画等への反映について明記された。



（参考）重要インフラ行動計画に基づくコミットメント強化

■ 重要インフラ事業者に関しては、近日改定予定の「重要インフラのサイバーセキュリティに係る行動計画」において、取締役の責任等に関する整理の記載とともに、「障害対応体制の強化に資する組織統治の在り方について規定化をする」こととした。今後、「安全基準等策定指針」に反映を行い、取組推進を図る。

「重要インフラのサイバーセキュリティに係る行動計画(案)」【2022年1月パブリックコメント版より抜粋】

IV. 1.1 組織統治の一部としての障害対応体制

（略）重要インフラ事業者等においては、組織の各階層において適切な責任と権限を明確にし、組織一丸となって重要インフラ防護を行う必要があるが、経営層のコミットメントによる組織運営上のリスクのひとつとして、重要インフラ防護の観点を含める必要がある。

内閣官房は、本行動計画において、障害対応体制の強化に資する組織統治の在り方について、安全基準等策定指針において、規定化をする。

重要インフラ事業者等は、本行動計画及び策定された安全基準等策定指針を踏まえ、自組織の障害対応体制の改善に努めるものとする。

(1) 組織統治に必要な観点

組織統治の一部として障害対応体制を強化するためには、「サイバーセキュリティ関係法令Q&AハンドブックVer1.0(令和2年3月2日 内閣官房内閣サイバーセキュリティセンター)」における４つの観点が必要となる。

① 内部統制システムとサイバーセキュリティとの関係

組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。経営層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。

具体的にいかなる体制を構築すべきかは、一義的に定まるものではなく、各組織が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各組織において決定されるべきである。また、組織の意思決定機関は、サイバーセキュリティ体制の細目までを決める必要はなく、その基本方針を決定することでもよい。

② サイバーセキュリティと取締役等の責任

組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

個人情報の漏えい等によって第三者が損害を被ったような場合、経営層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

③ サイバーセキュリティ体制の適切性を担保するための監査等（略）

④ サイバーセキュリティと情報開示

サイバーセキュリティに関する組織の情報を開示することは、組織の社会への説明責任を果たすとともに、組織運営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。また、自組織のサイバーセキュリティ対策の強化もつながることも期待できる。

そこで、組織としては、既存の開示制度を積極的に活用して、サイバーセキュリティに関する取組を開示することが望ましい。

サイバーセキュリティに係る情報開示の考え方整理

■ サイバーセキュリティに関する法令の論点解説等を示したハンドブックにおいて、サイバーセキュリティに関する情報開示の考え方を示している。

「サイバーセキュリティ関係法令Q＆Aハンドブック」【抜粋】

Q6 サイバーセキュリティと情報開示

（２）事業報告

会社法第435条第2項に基づき、株式会社は事業報告を作成することが義務付けられている。株式会社は、内部統制システムに関する決定又は決議をしたときは、その決定又は決議の内容の概要及び当該システムの運用状況の概要を事業報告に記載しなければならないところ（会社法施行規則第118条第2号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる（サイバーセキュリティと内部統制システムとの関係についてはQ3を参照されたい。）。

（３）有価証券報告書

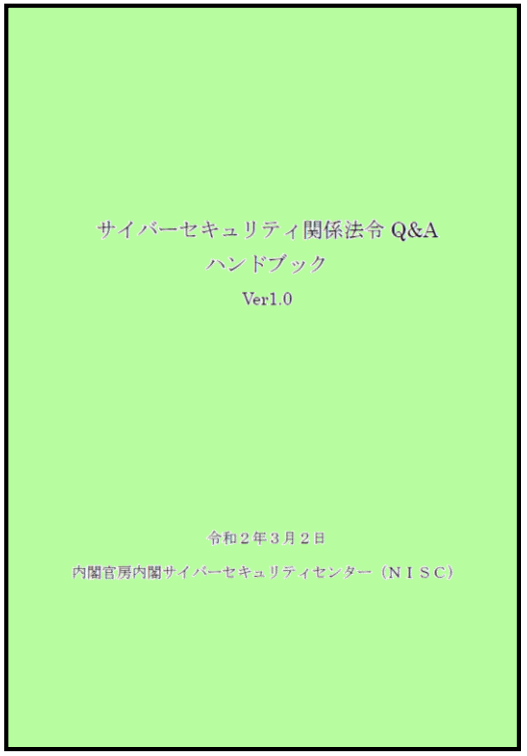
金融商品取引法第24条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項等について、内閣総理大臣に提出することが義務づけられている。その他事業の内容に関する重要な事項の中には、事業等のリスクが含まれるところ（企業内容等の開示に関する内閣府令第15条第1項第1号に定める第3号様式）、サイバーセキュリティに関するリスクをこの事業等のリスクとして開示することが考えられる。

（４）コーポレート・ガバナンスに関する報告書

証券取引所による開示制度の一環として、コーポレート・ガバナンスに関する報告書が挙げられる。有価証券上場規程（東京証券取引所）第204条第12項第１号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する基本的な考え方などを記載したコーポレート・ガバナンスに関する報告書を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている。コーポレート・ガバナンスに関する報告書では、内部統制システムに関する基本的な考え方及びその整備状況を記載することとされているところ（有価証券上場規程施行規則第211条第4項第5号）、サイバーセキュリティに関する事項をこの内部統制システムの一部として開示することが考えられる。

（５）適時開示

有価証券上場規程第402条等に基づき、上場会社は、剰余金の配当、株式移転、合併の決定を行った場合や災害に起因する損害又は業務遂行の過程で生じた損害が発生した場合等においては、直ちにその内容を開示することとされている。サイバー攻撃に起因して損害が発生する場合には、この災害に起因する損害又は業務遂行の過程で生じた損害として損害・損失の内容や今後の見通しを開示することが考えられる。



［出典］NISC「サイバーセキュリティ関係法令Q＆Aハンドブック」(2020年3月)

サイバーセキュリティ対策情報開示の手引きの策定

■ 民間企業のサイバーセキュリティ対策の情報開示の促進のため、民間企業にとって参考となり得る情報開示の事例等をまとめた手引きを策定し、2019年6月に公表。

背景

- ✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要。**

目的

- ✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進。
- ✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**を**事例集として**示す。

活用主体

- ✓ **サイバーセキュリティ対策の情報開示**に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

- ✓ **開示書類**を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

本編　サイバーセキュリティ対策情報開示の手引き

1．本手引きの趣旨・目的【内容】
- ✓ サイバーセキュリティリスクの増大と対策の必要性
- ✓ サイバーセキュリティ対策の情報開示の意義
- ✓ 本手引きの目的、想定参照主体、及び内容・構成等

2．情報開示の手段【内容】
- ✓ 代表的な開示書類の紹介

3．企業における情報開示の在り方【内容】
- ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策
- ✓ 開示にあたってのポイントと記載例

4．今後の方向性について【内容】
- ✓ 手引きの改定の在り方等の今後の方向性

参考資料①　関連施策等の紹介

【内容】
- ✓ 本手引きに関連した様々な施策やガイドライン等について紹介

参考資料②　開示書類の事例集

【内容】
- ✓ サイバーセキュリティ対策の情報開示にかかる実際の開示書類の例について紹介

企業の開示姿勢等に関する分析・格付け

- 日経500社を対象に、総合的に企業のサイバーセキュリティへの取組及び開示姿勢に関する分析を実施。
- また、特に優良であり模範となる企業に星を付与する「格付け」を実施。（2021年度は42社に星を付与）

調査手法

- 調査対象：日経500種平均構成銘柄を構成する500社
- 調査期間：2021年7月～9月上旬
- 総合得点：以下の２項目の合算
- 調査内容：

公開情報	有価証券報告書、コーポレートガバナンス報告書、統合報告書、企業ウェブサイトの記載内容、およびイベント講演、ISMS認証、Pマーク、技術資格取得者数等を調査。	 有価証券報告書等
アンケート	公開されていないサイバーセキュリティーの取組を確認するため企業へアンケート調査を実施。IPAサイバーセキュリティ可視化ツールを参考に独自の設問を作成。	 アンケート調査（全18問）

［出典］（一社）日本IT団体連盟　「サイバーインデックス企業調査2021」（2021年11月）

（参考）米国証券取引委員会（SEC） 開示ルールの変更

- 3/9に米国証券取引委員会（SEC）が「サイバーセキュリティのリスク管理、戦略、ガバナンス、インシデントの開示に関する規則」の改定を提案。
- 重大なセキュリティインシデント判断後の4営業日以内の情報開示、取締役会メンバーのサイバーセキュリティ専門知識保有状況の開示等を要求する変更が行われている。

改訂事項の一覧

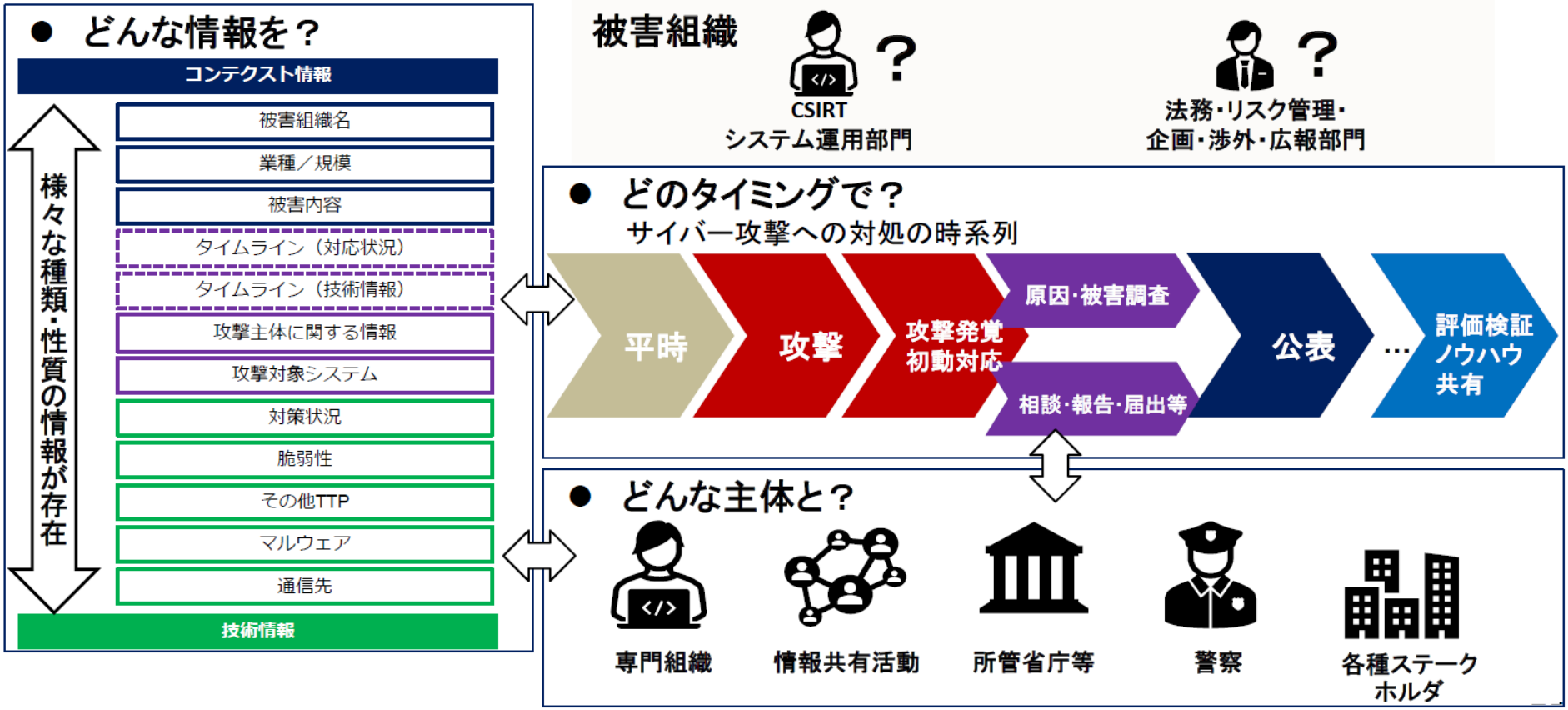
項番	改訂内容
1	登録者が**重大なサイバーセキュリティインシデントを受けたと判断した後、4営業日以内にサイバーセキュリティインシデントに関する情報を開示**するよう要求。
2	以前に開示したサイバーセキュリティインシデントに関する最新情報を提供するよう登録者に要求する。また、これまで未開示だった個別の重要でないサイバーセキュリティインシデントが全体として重要になった場合、経営陣にわかる範囲で、これらのフォームを必要な開示に修正することを提案。
3	以下開示を要求。 ➢ サイバーセキュリティリスクを特定および管理するための登録者のポリシーと手順（ある場合） ➢ サイバーセキュリティリスクに関する取締役会の監督の役割を含む、登録者のサイバーセキュリティガバナンス ➢ サイバーセキュリティ関連のリスクを評価および管理し、関連するポリシー、手順、および戦略を実装する際の管理者の役割と関連する専門知識
4	登録者の**取締役会のメンバーがサイバーセキュリティの専門知識を持っているかどうかについての開示を要求。**
5	米国外の企業（「FPI」）にサイバーセキュリティの開示を提供するよう要求。提出する年次報告書は、自国内の開示内容と一致させることを要求。
6	レポートトピックとして「サイバーセキュリティインシデント」を追加。
7	開示内容はインラインXBRL形式で提供することを要求。

［出典］ 米SEC “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure” (2022.5)を基にNISC作成

（参考）サイバー攻撃被害に係る情報の共有・公表ガイダンス

総務省、経済産業省、警察庁、NISC

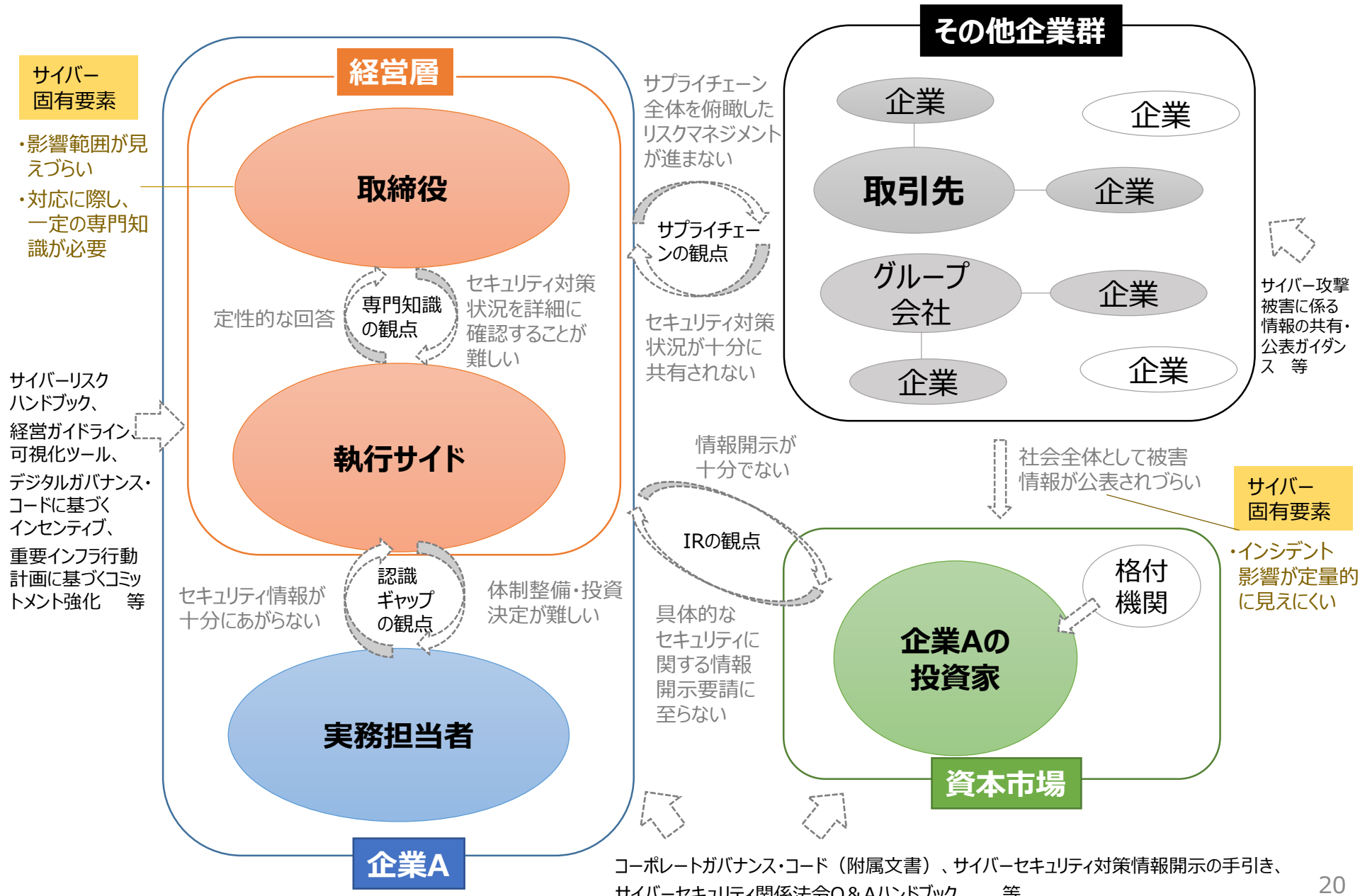
■ サイバー攻撃被害に関する円滑かつ効果的な情報共有を促進するため、攻撃被害を受けた組織の立場にも配慮しつつ、攻撃被害に係る情報を取り扱う際の実務上の参考となるガイダンスを年内に策定予定。



［出典］ 総務省、経済産業省、警察庁、NISC「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 の開催について」(2022年4月)

経営層とステークホルダーに起こり得る課題（概念図）

議論用



コーポレートガバナンス・コード（附属文書）、サイバーセキュリティ対策情報開示の手引き、
サイバーセキュリティ関係法令Q＆Aハンドブック　　等

本日ご議論いただきたいこと

① 経営層、投資家等において、コーポレートガバナンスの一環として、サイバーセキュリティに係るリスクがどのように認識されているか？

② 企業が取組を進める上で、サイバーセキュリティに係る固有性を含め、どのような課題があるか？どのような政策的な対応、又はその強化が考えられるか？