セキュリティ・トランスペアレンシー・コンソーシアム

活動成果

経営層への提言

可視化データによるサイバーセキュリティ透明化と ガバナンス強化

2026 年 3 月 24 日

セキュリティ・トランスペアレンシー・コンソーシアム

目次

1　はじめに

サイバーセキュリティにおいて経営者に求められることは、ガバナンス、リスク管理、コンプライアンスの 3 要素、いわゆる GRC に集約されます。組織内外のサイバーセキュリティのリスクや法令遵守状況を正しく把握することで、適切なサイバーセキュリティの経営判断を実施し、事業遂行者によるセキュリティの正しい実行を管理することで企業ガバナンスを実現し、法令に基づいて組織内外のステークホルダーに正確に報告することが必要です。

しかし、サイバーセキュリティは経営者からは目に見えない点が多く、組織のサイバーセキュリティの状況を正確に把握することは容易ではありません。そこで、経営者にとって必要な情報を可視化することについて、セキュリティ・トランスペアレンシー・コンソーシアムで検討しました。 本提言書では、各種法令・ガイドラインが可視化について言及していることを紹介し、可視化が不完全で発生した事例、それらを解決する可視化データ、可視化データがあるとどう解決するのか、について提言します。

2　サイバーセキュリティ経営に対する「可視化」への要求

ここ数年で、我が国のコーポレート・ガバナンスにおけるサイバーセキュリティ対策への経営者の関与の重要性が高まってきました。企業の目的にサイバーセキュリティの活動が則していることを、経営者が管理する必要があります。その要因として、2017 年に経済産業省が発行した「サイバーセキュリティ経営ガイドライン Ver.2.0」（後に Ver.3.0 に改版）で「経営者が認識すべき 3 原則」と「サイバーセキュリティ経営の重要 10 項目」が提示されたことが挙げられます。同書の中では、経営者がサイバーセキュリティ対策のためにリーダーシップを発揮することが求められています。さらにサイバーセキュリティ対策のため、経営者の「役割」と「対応事項（努力義務）」が明確化されたことが重要です。 一方、海外ではサイバーセキュリティ被害や情報漏えいなどが発生した場合に、法律や規則で罰金や罰則が科せられるとともに、政府機関、規制当局、株主等へ被害に至った経緯に関する迅速な報告が義務付けられています。定められた期間内に報告できない場合、更なる罰則が科せられます。 日本ではサイバーセキュリティ対策の比重が高まってきた状況ですが、海外では規則化され、コーポレート・ガバナンスの中にサイバーセキュリティ対策を組み込まないと企業として生き残れない状況となっています。経営者には「役割」以外に「責任」が定められ、「対応事項（努力義務）」に代わり「規則（厳守）」が課せられました。本章の各節で、海外（米国、EU）の指令・規則・規制、および日本のガイドラインと法制度を解説します。

2.1　アメリカでの法規制やルール策定の状況

- 重要インフラに係るサイバーインシデント報告法

米国の重要インフラに係るサイバーインシデント報告法（CIRCIA ：Cyber Incident Reporting for Critical Infrastructure Act）は、16 分野の重要インフラ事業者においてサイバーインシデント発生時に早急かつ的確な対応を行うことで重要インフラの安全性を高めるものです。最終規則は 2025 年 10 月までに発表予定であり、2026 年に施行を予定しています。 本法律は、報告の期限、被害対象のシステム／

サービス、対応措置などを含む詳細な情報を提供することを義務付けています。これらの報告義務を果たさない場合、情報開示請求や民事執行手続きなどの罰則が科せられます。 報告を早急かつ的確に行うため、企業内のエスカレーションルートの整備や報告内容の随時収集をする必要があります。この法律に対しても経営層主導で対策し、報告内容の整理と発行までの承認等のシステムを確立すべきと言えます。

- 米国証券取引所のサイバーセキュリティ開示最終規則

米国のサイバーセキュリティ開示に関する最終規則（Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure）は、法律ではなく米国の証券取引委員会（Securities and Exchange Commission、以下 SEC）が定めた上場企業向けサイバーセキュリティ関連（リスク管理、戦略、ガバナンス、インシデント等）の開示規則です。 目的は 2 点あり、「上場企業のサイバーセキュリティリスク管理の透明性を高め、投資家がより正確な情報に基づいて投資判断を行えるようにする」および「市場全体の信頼性を向上させ、サイバーインシデントによる市場の混乱を最小限に抑える」となります。 上場企業はサイバーインシデントを発見した場合、そのインシデントが重要であると企業が判断してから 4 日以内に Form 8-K と呼ばれる臨時報告書にて報告することが義務付けられています。また、臨時報告書以外に Form 10-K と呼ばれる年次報告書にて、サイバーセキュリティの脅威によるリスクの取締役会による監視について記述することが義務付けられています。臨時報告書、年次報告書ともに一般公開されますので、企業のサイバーセキュリティリスク管理の取り組みが周知され、株主は株売買の参考にし、企業の株価上下動の要因になります。 この規則も経営層主導で対策し、報告を行うためのシステムを確立すべきと言えるでしょう。

2.2　EU での法規制やルール策定の状況

- NIS2 指令

EU の NIS2 指令（Network and Information Systems Directive Rev.2）は、日本語名で「改正ネットワークおよび情報セキュリティ指令」といい、サイバーセキュリティリスク管理の強化を目的としています[1]。 NIS2 指令は、サプライチェーンセキュリティの強化、有事の対応準備、プロセス整備が求められ、経営陣はサイバーセキュリティリスク管理策の承認・実施監督・違反責任を負います。違反時には罰金が科せられます。またサイバーインシデント発生時には報告の必要があります。一次報告が 24 時間以内、二次報告が 72 時間以内、最終報告が 1 か月以内となります。 なお「指令」とは、EU による法体系の一種で、指令に基づき各国が国内法として制定することで法律としての効力を持ちます。

[1] https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/nis2.html

- サイバー・レジリエンス法

EU のサイバー・レジリエンス法（CRA：Cyber Resilience Act）は、デジタル製品の安全性を高め、サイバー攻撃から消費者や企業を保護することを目的としています[2]。 対象となるデジタル製品はインターネットに接続可能なハードウェア、ソフトウェアであり、非常に多くの製品が対象となります。 同法は、企業に対し、製品のライフサイクル全般（開発段階～出荷前～出荷後サポート）にわたったセキュリティ対策を組み込むことを義務付けています。またサイバーインシデントが発生した場合、迅速な対応と報告（24 時間以内）を行うことを求めています。さらにサイバーインシデント発生時の原因究明・対応の効率化のため、SBOM（Software Bill of Materials）の作成を義務付けています。 この法律に対し、経営層のリーダーシップによる全社一体となった対応（ライフサイクルのフェーズごとに担当部署・担当者が異なるため）が必要と言えます。

- GDPR

EU の GDPR（General Data Protection Regulation）は、日本語名を一般データ保護規則と言い、2018 年 5 月から施行されました[3]。日本の個人情報保護法のように個人情報の保護を目的としていますが、企業に対し個人情報やプライバシーの厳格な管理を課している点、個人の権利が強化されている点、および高額な制裁金が科されている点が日本の個人情報保護法よりも厳しいと言えます。 GDPR では、「個人情報を使用する際、対象者への自由意思による、明確で分かりやすい同意が必要」、「個人情報の漏えい時には 72 時間以内の報告」、「データ保護責任者（(DPO：Data Protection Officer）の任命が必須」の 3 点が義務付けられており、これらに違反した場合、制裁金につながります。 違反事例として、企業が敷地内に設置した防犯カメラが公共スペースを部分的に映してしまっていたことが地域住民の監視と認識されました。そして監視していることを十分に明示していなかったとして制裁金が科されました。この事例から GDPR の厳格さがうかがえます。 この規則も経営層主導で対策し、企業内での明確なルールの策定と報告体制・報告システムを構築することが必要と言えます。 なお、EU では「規則」は法体系の一種で「指令」よりも強力になります。EU で共通の法律となります。

[2] https://www.jetro.go.jp/biznews/2024/12/aa7bc2b5b206dc9d.html

[3] https://moltsinc.co.jp/media/knowledge/9791/

2.3　日本でのガイドランや法律の制定

- 経営層に言及している代表的なサイバーセキュリティガイドライン

経営層に言及している代表的なサイバーセキュリティガイドライン 日本国内には経営が関係するセキュリティガイドラインが複数存在しています。特に、代表的なものとして 3 点を挙げることができます。

- サイバーセキュリティ経営ガイドライン Ver3.0[4]
  2023 年 10 月　経済産業省刊
- 金融分野におけるサイバーセキュリティに関するガイドライン[5]
  2024 年 10 月　金融庁刊
- 医療情報システムの安全管理に関するガイドライン第 6.0 版[6]
  2023 年 5 月　厚生労働省刊

サイバーセキュリティ経営ガイドライン Ver.3.0 では、「経営者がリーダーシップを発揮すること」「サプライチェーンの末端まで管理の目を行き届かせること」「関係者との密なコミュニケーション」が重要とした上で、組織全体の枠組み、リスクの把握と継続的管理、リソースの確保、情報収集などを経営者主導で実施することが求められています。 金融分野におけるサイバーセキュリティに関するガイドラインでは、サイバーセキュリティ基本法で金融業は重要インフラ事業者として指定されていることから「その責務として、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めること」が重要であると記載されています。さらに「サイバーインシデントによる業務の中断等は、経営責任が問われかねない問題である」とした上で「経営陣の主体的な関与が求められる」としています。 医療情報システムの安全管理に関するガイドライン 第 6.0 版では、同書が 4 分冊から成り「概説編（Overview）」「経営管理編（Governance）」「企画管理編（Management）」「システム運用編（Control）」があります。「経営管理編（Governance）」の冒頭では、経営者は法令を遵守すること、職員や関係事業者に法令を遵守させることとあり、その上で経営者の責任を詳細に記載しています。

- 能動的サイバー防御

能動的サイバー防御（Active Cyber Defense）は、国家安全保障戦略の一環でサイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、検討されてきました。[7]内容として以下の 4 点が盛り込まれています。

---

[4] https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
[5] https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf
[6] https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
[7] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

① 官民連携の強化
② 通信情報の利用
③ 攻撃者のサーバ等への侵入・無害化
④ NISC の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置

そして、2025 年 5 月に上記 4 点が反映された「サイバー対処能力強化法」及び「整備法」が公布されました。①②がサイバー対処能力強化法に反映され、③④は整備法に反映されています。

能動的サイバー防御の仕組みは、①で官民連携による情報共有、②で外部からのサイバー攻撃の検知、④で設置された組織が無害化実施の実行判断、③で外部からのサイバー攻撃を警察／自衛隊が無害化（テイクダウン）することになります。

ここで①の官民連携による情報共有では、情報提供元となる重要インフラ事業者は、情報提供以前に、自社の IT 機器の脆弱性対応を強化し、官に対し IT 機器登録制度で条件を満たす IT 機器を届け出ることになります。また届け出た IT 機器にインシデントが発生した場合、早急に報告することが義務付けられています。更にインシデント報告を怠ったたり、報告に不備があった場合、罰金が科せられます。

サイバー対処能力強化法および整備法において、重要インフラ事業者の経営層は、自社のリスクガバナンスを強化し、サイバーリスクを経営リスクとして認識する必要があります。①の官民連携の強化よる情報共有は、国家安全保障戦略に企業が組み込まれることを意味するので、然るべき責任が発生することになるからです。

また、重要インフラ事業者でなくても、重要インフラ事業者と取引のある企業においては官民連携のスキームに巻き込まれる可能性があります。同企業の経営層は、契約や情報提供に関する規程の整備とシステムの構築が必要となるでしょう。

3　経営に影響を与えたセキュリティ問題

近年のサイバーインシデント、法令違反および事故に伴うセキュリティに関連した事件は年々数が増加し、規模も増大しています。影響は企業の一部門にとどまらず、経営全体に大きな影響を与え、経営層の責任が問われています。経営者の責任は、経済産業省の「サイバーセキュリティ経営ガイドライン」、TrendMicro 社の「経営層・セキュリティ責任者・インシデントレスポンス担当 3 者の立場で考えるセキュリティインシデント」等で指摘されており、

表 3-1 のように分類できます。

表 3-1　経営者の責任

経営層の責任の種類	説明
ガバナンス上の経営責任[8]	サイバーリスクを事業リスクとして軽視、または適切に管理していなかった。
法的・規制対応責任	法令、規則、業界規制などルールの不遵守。義務づけられた事故報告を怠った。
説明責任・信頼責任[9]	顧客・株主・取引先に対して、被害の内容や対応策を迅速かつ正確に説明できない。
予見・予防責任	想定したリスクを軽視し予防策を講じなかった。適切なリソースを割かなかった。 サプライチェーンや委託先のセキュリティリスクを見過ごした。
対応・監督責任	インシデント発生後の初動対応が遅れた。 経営層がリーダーシップを発揮せず、組織が混乱した。
倫理的責任[10]	顧客や社会から預かった情報資産を守る「社会的使命」を果たさなかった。

近年発生した経営者に影響が大きい、または、世間を騒がせたセキュリティ事故は、個人情報保護違反、暗号資産流出、Log4J2 の影響、ランサムウェア攻撃などを挙げることができます。それぞれの、経営者の責任は**表 3-2** に示すように、法整備が進んでいる個人情報保護の違反や、顧客の資産を預かる暗号資産流出で責任範囲が広く、自社事業への影響が大きいランサムウェア攻撃が続いています。Log4J2 は比較的経営者の責任範囲は狭いですが、多くの企業に影響が出た事例です。

[8] https://www.soumu.go.jp/main_content/000528735.pdf

[9] https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[10] https://www.ipa.go.jp/security/economics/csm-practice.html

表 3-2　事例ごとの経営層の責任

経営層の責任の種類	個人情報保護違反	暗号資産流出	Log4J2 影響	ランサムウェア攻撃
ガバナンス上の経営責任	○	○	○	○
法的・規制対応責任	○	○		○
説明責任・信頼責任	○	○	○	○
予見・予防責任	○	○		○
対応・監督責任	○	○	○	○
倫理的責任	○	○		○

また、NIST サイバーセキュリティフレームワーク 2.0（以下、NIST CSF 2.0）で事件の発生した要因と被害拡大の要因を当てはめると、同フレームワークの 6 つの機能のうち「識別」と「対応」の不備が大きな割合を占めています。つまり、識別の失敗と対応の失敗が致命的で被害拡大を招いています。

3.1　個人情報の保護違反による制裁金

EU の GDPR の違反は、多くの制裁金を科せられます。制裁金には、サイバーセキュリティ管理の不備（個人情報の漏えい等）での制裁金、報告の遅延および正確さを欠くことによる制裁金の加算があります。また個人情報の対象者の同意を分かり易く得るという点に違反した場合でも制裁金が科されます。一方で正確で迅速な報告を行った場合、制裁金が軽減された事例があります。

制裁金には、軽度の違反と重度の違反の 2 種類があり、重度の違反では 2,000 万ユーロまたは当該企業の全世界年間売上高の 4%のいずれか大きい方が科されます。実際の制裁例として、某企業が 2021 年に 7 億 4600 万ユーロ（1,000 億円超）の制裁金を科されました[11]。

この制裁金が発生した原因は、個人情報と管理体制の把握の失敗による管理体制の不備の放置、セキュリティの実施状況の把握の失敗による必要な保全措置の欠如が大きいです。これらを可視化するデータがあれば経営層がすぐに気が付いて、違反を回避できたかもしれません。また、セキュリティ実施状況の把握が遅れた場合、報告期限である 72 時間以内を守れず、制裁金が増えることがあり得ます。報告書をまとめるためのデータがそろっていないと、時間内の報告することが困難です。

3.2　暗号資産流出による巨額賠償金と事業継続不可

暗号資産が流出した事例では、企業の従業員や委託先の従業員が踏み台となり、アカウントを乗っ取られたケースが目立ちました。企業のガバナンスが従業員およびサプライチェーンの従業員に浸透していないことが直接の原因であり、企業のサイバーセキュリティ上の管理責任が果たされていなかったことが真の原因となります。

[11] https://privtech.co.jp/blog/law/gdpr-ico.html

本事例の多くで金融庁から業務改善命令を受けています。これは同時に当該企業が社会的信用を失うことになります。また全顧客の全資産を賠償することで企業として経営が傾き、さらに事業の継続が不可能になるなどの被害が出ています[12]。

この被害が発生した原因は、組織全体のリスク管理の失敗と重大な脆弱性への対応の欠如です。マルウェアが管理者の端末に感染しただけで顧客の資産にアクセスできるのはセキュリティ状況を把握していなかったから放置されていたと考えられます。事業のリスクやセキュリティ状況のデータを経営層が十分に把握していなかったことが原因です。また、攻撃された端末の所有者が業務委託先の担当者であったことも注目しなければなりません。サプライチェーン管理の不備が重大な事故につながった事例です。サプライチェーンの状況を経営者が十分に把握していませんでした。さらに、監督官庁への被害報告が稚拙だとも言われています。報告に必要なデータがすぐに集まらず整理するのに時間がかかった可能性が高いです。これが、重大な業務改善命令を発令されたことに繋がります。

3.3　重大な脆弱性 Log4J2 による世界規模の混乱

2021 年 12 月、Java ベースのログ出力ライブラリ「Apache Log4j」の 2.x 系バージョンで確認された深刻な脆弱性を修正したバージョンが公開されました。

その後も修正が不完全であったことなどを理由に 2 件の脆弱性が修正されました。広く利用されているライブラリであるため、影響を受ける対象（サービス、製品）が多く存在するとみられ、攻撃が容易であることから世界的な問題とされました。実際、影響を受けているサービスや製品を多くの企業が公表しています[13]。

また Microsoft 社は、中国、イラン、北朝鮮、トルコの国家支援を受けているとみられるグループ、アクセスブローカーとして追跡している複数のグループによる悪用を確認したと報告しています。

この事例で混乱が発生した原因は、情報資産がリストアップされていなかったこと、Log4J2 の脆弱性の影響評価に時間がかかったことです。多くの企業で経営層が資産や事業のリスク、セキュリティ状況を可視化するデータをまとめておらず、世界中の多くの企業が対応に追われたことが問題になりました。また、ソフトウェアメーカーとしては Log4J2 の含有の有無と、その影響についての説明責任を求められました。提供する製品や仕様している機器の状況を素早く説明でいるだけのデータがそろっていれば、混乱は発生しなかったでしょう。

3.4　ランサムウェア攻撃がもたらす被害

ランサムウェアは身代金要求型のサイバー攻撃です。PC やサーバ内のデータを暗号化し、使えなくして、復号して元に戻す代償として金銭（身代金：Ransom）を要求します。最近では二重・三重の脅迫が主流となっています。身代金を払わなければデータを公開すると脅したり、顧客や取引先にランサムウェアを仕掛けると脅したりされています。

ランサムウェアの事例では、情報資産、ソフトウェア資産に不正アクセスされるという企業の情報システムの脆弱性と復旧の備えが問題になります。また、ランサムウェア攻撃はサプライチェーンに対して

---

[12] https://piyolog.hatenadiary.jp/entry/20180920/1537414861

[13] https://piyolog.hatenadiary.jp/entry/2021/12/13/045541

踏み台攻撃を仕掛けている事例も多くあります[14]。ランサムウェアは企業にとって「止まる」「失う」「責められる」の三重苦をもたらします。

ランサムウェアの弊害は多岐にわたり、以下が挙げられます。

- 業務停止（サービス提供停止、生産ライン停止、物流の混乱）
- 金銭的損失（身代金、復旧費用、売上減少）
- 情報漏えいリスク
- 法的・規制上の影響（監督官庁への報告義務が発生）
- 企業のブランド・信頼の失墜（セキュリティが甘い企業と認識される）
- 経営層の責任追及
- 長期的影響

このセキュリティ事故が発生し、影響が拡大した原因は、暗号化された対象データの把握に時間がかかったことと、保護するべきデータ資産に適切なセキュリティ措置が施されていないことに気が付かなかったことが大きいです。経営者が事業や資産のリスクのデータを集めて把握して、適切なセキュリティが実施されていることを示すデータをもっていなかったことが原因です。さらに、委託先などサプライチェーンのセキュリティ管理の不透明さから侵入されています。ランサムウェアの侵入口は、委託事業者のセキュリティ管理を、経営者が把握してなかったことが原因です。また、影響が特定できずに顧客やデータオーナーへの説明に多大な時間を要したことも、事故対応の拙さを指摘されています。ランサムウェア攻撃を受けた企業は事故の説明責任を果たすことが重要です。説明はデータに基づいて実施する必要がありますが、そのデータがなかったので、説明が不完全で時間がかかった要因でした。

4　経営者をサポートする「可視化データ」

企業の規模およびサプライチェーンの規模が大きくなるほど全体の把握が困難になります。経営者が的確な判断をするには、データに基づくこと、データがコーポレート・ガバナンスと紐づいていること、データが使いやすく見やすい形になっていることが重要です。

NIST サイバーセキュリティフレームワーク 2.0 版の 6 つの機能のうち、特に「識別」と「対応」において、経営者がリーダーシップを発揮することで、状況把握、適切な意思決定、および適切かつ迅速な報告を行うことができます。これがセキュリティに対する経営責任を果たすことにつながります。

当コンソーシアムが 2024 年に公開した知見集「セキュリティ透明性確保に向けた可視化データ活用～脆弱性管理編～」では、可視化データを**図 4-1** とし、脆弱性管理における例として、ソフトウェア構成情報（SBOM を含む）及びネットワーク構成情報及びソースコード及びバイナリコード及び開発文書などが構成情報に該当し、外部アクセス可否情報及びシステム設定情報などが状態情報、脆弱性情報などがリスク情報に該当することを示しました。

[14] https://piyolog.hatenadiary.jp/entry/2024/08/19/074417

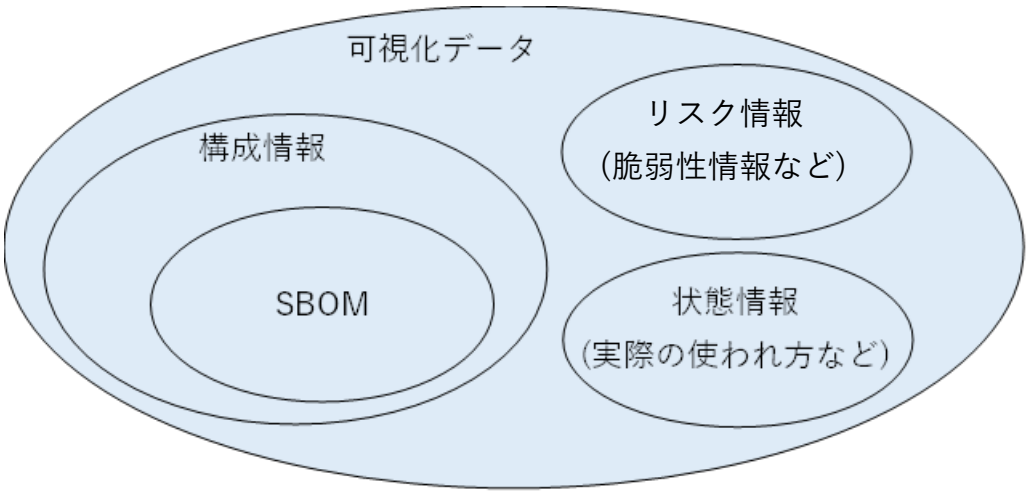

図 4-1　可視化データの分類

当コンソーシアムは経営者の管理責任と説明責任をサポートする可視化データとして、インシデント事例に対応する可視化データを検討し、**図 4-2** のように事業情報、サプライチェーン情報、説明責任情報を加えた拡張を実施しました。事業情報には、財務情報などが該当し、サプライチェーン情報は委託先情報、説明責任情報は外部への公開に関する情報に該当します。更に**図 4-2** に示すように、①資産や事業リスク、②セキュリティ状況、③サプライチェーン、④説明責任の 4 種類にまとめることができます。①資産や事業リスクは事業情報や構成情報に相当します。これは何を守るべきかを可視化するためのデータです。②セキュリティ情報は、リスク情報と状態情報に対応します。これは、どのように守っているかを可視化するためのデータです。③サプライチェーンは、サプライチェーンを把握するための可視化データとなります。これは、昨今のセキュリティインシデントはサプライチェーンが関連することが多く、サプライチェーンを把握するために可視化データが必要になります。④説明責任は、外部への説明のための可視化データとなります。これは、経営者の真価が問われるのは、インシデントが発生したときの外部への説明です。外部への説明に利用可能な情報を可視化データとして準備しておくことが求められているためです。これらから経営層を取り巻く状況を加味して整理したのが**図 4-3** となります。

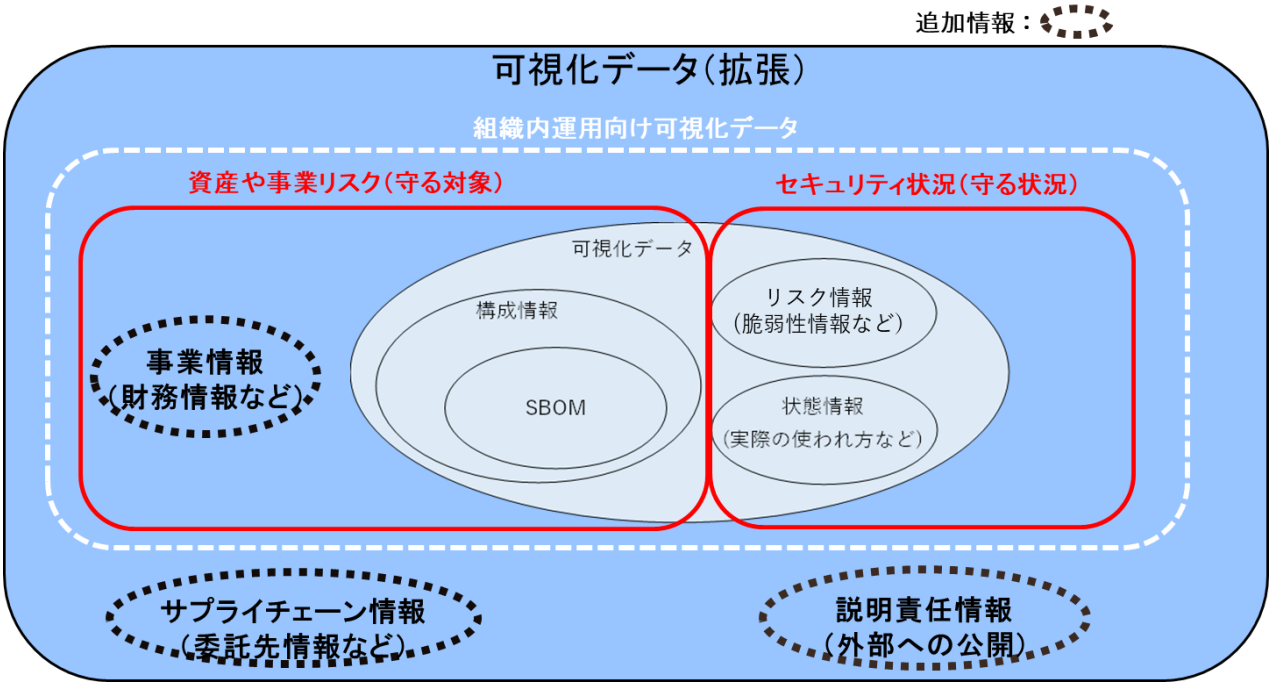

図 4-2　経営層向けに拡張した可視化データ

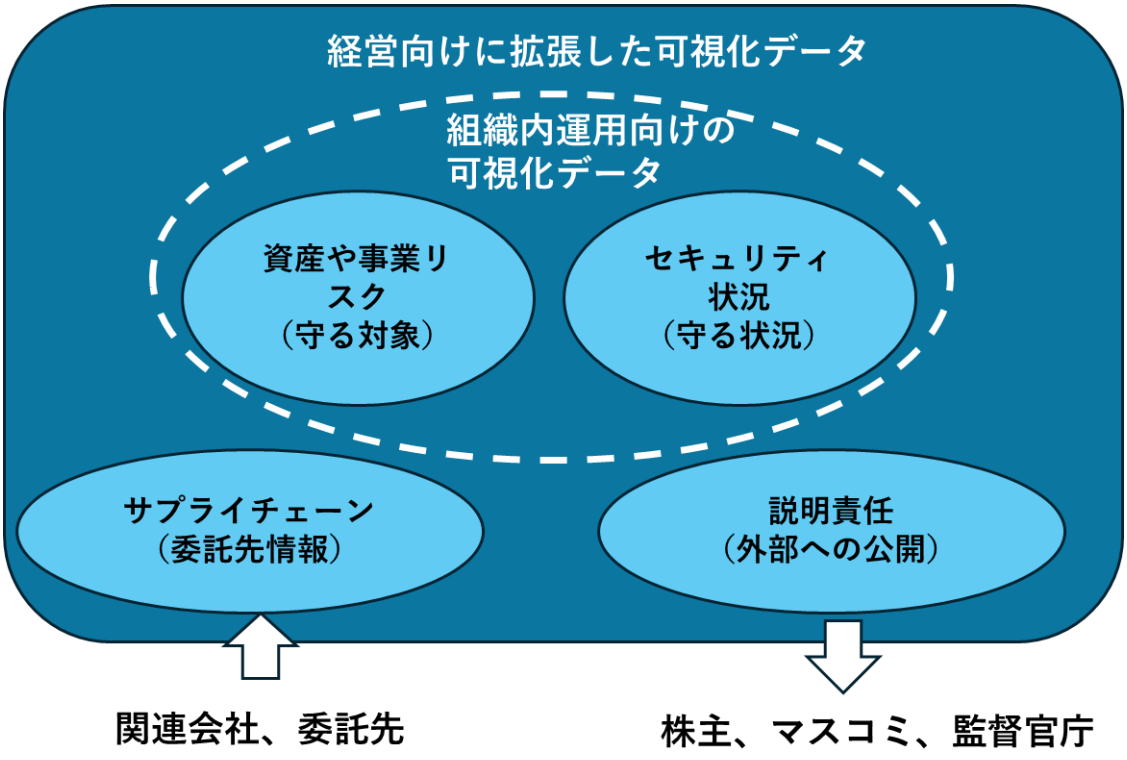

図 4-3　経営層向けに拡張した可視化データの分類

経営者の責任とこれらの可視化データの対応関係は**表 4-1** の通りです。経営層の多くの責任が 4 つの可視化データで対応できることが分かります。

表 4-1　経営者の責任と可視化データ

経営層の責任の種類	資産や事業リスク	セキュリティ状況	サプライチェーン	説明責任
ガバナンス上の経営責任[15]	○	○	○	
法的・規制対応責任	○	○	○	○
説明責任・信頼責任[16]	○	○	○	○
予見・予防責任	○	○	○	
対応・監督責任	○	○		○
倫理的責任[17]				○

- 資産や事業のリスクを可視化

企業の情報資産、従業員と関係者の個人情報、外部から収集した個人情報および預かり資産の状況を正確に把握することが第一歩です。また、どのようなソフトウェアを利用しているかを可視化するには SBOM が有効です。ソフトウェアは守るべき資産を保管、活用するための重要なシステムを把握することに役立ちます。

次にこれらの情報が「誰に」「どこから」「どうやって」「どういう被害に合うか」という事業リスクアセスメント（リスクの洗い出し、危険度の評価、リスクの対策を確立）を行います。一般的にビジネスインパクト分析の手法を用いて、経営者が把握すべき影響を分析します。　資産とリスクアセスメント結果を経営者が把握できるように可視化する必要があります。

可視化データの例は次の通りです。

事業資産一覧
財務諸表関連データ
個人情報管理台帳
ビジネスインパクト分析結果
SBOM

- セキュリティ状況を可視化

企業の情報システム、モノおよびヒトの脆弱性を診断します。組織のどこに影響が発生する可能性があるかを把握します。情報システムについては SBOM で可視化した情報に基づいて、セキュリティ情報を

[15] https://www.soumu.go.jp/main_content/000528735.pdf

[16] https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[17] https://www.ipa.go.jp/security/economics/csm-practice.html

可視化します。モノおよびヒトについては SBOM とは別の手段で可視化データ化します。

これらの可視化データと前項で洗い出した資産とリスクアセスメント結果の可視化を組み合わせて、定期的にリスクを監視することでリスク管理のサイクルを回すことができ、状況を把握できます。

可視化データの例は次の通りです。

脆弱性分析結果
サイバーリスクアセスメント結果
セキュリティアセスメント結果
インシデントレポート

- サプライチェーンの可視化

サプライヤー、サービス提供事業者、協力会社等のサプライチェーンがサイバーインシデントの起因になるケースがあります。最近はサービスプロバイダーのシステムを利用したり、業務を委託したりするケースが多くなっています。自組織ではないので経営者からは見えにくくなっています。

サプライチェーンとの契約内容により、定期的に実施する内容、従業員のトレーニング状況などセキュリティ管理体制と実績を可視化し、経営層にて把握できることが必要です。

可視化データの例は次の通りです。

企業セキュリティ評価・監査結果
契約書のセキュリティ条項
定期的なレポート
連絡体制

- 説明責任に必要な情報を可視化

セキュリティの不備や事故が発生した場合に、監督官庁などに迅速に報告するための組織体制とシステムを確立し、情報を可視化して経営層にて把握できるようにします。なお、可視化が法令に対応した形で表示されると、報告を行う際、使い勝手がよくなります。

可視化データの例は次の通りです。インシデント報告書は国家サイバー統括室が「サイバー攻撃による被害発生時のインシデント報告様式の統一について」[18]において統一資料を策定しています。

SEC Form 10-K、Form 8-K、有価証券報告書
被害と影響の情報
インシデント報告書
記者会見資料

[18] https://www.nisc.go.jp/policy/group/cyber/yoshikiichigenka.html

5 「可視化データ」が活用される世界

可視化データを定義して収集することで、0 章でしめした過去のセキュリティ事故の被害の発生を低減、または、被害の拡大を抑制することが可能になります。サマリを**表 5-1** に示します。具体的な効果は以降の節で説明します。

表 5-1 可視化データの効果

可視化データ	個人情報保護違反	暗号資産流出	Log4J2 影響	ランサムウェア攻撃
資産や事業のリスク	個人情報を管理体制の把握	組織全体のリスク管理	リストアップの効率化	暗号化された資産の把握
セキュリティ状況	保全措置の把握	脆弱性への対応	脆弱性検討の効率化	適切な対策がされているかの確認
サプライチェーン		業務委託先の管理状況		侵入経路の抑制
説明責任に必要な情報	規制当局の報告内容	監督官庁への正確な報告	顧客への情報提供	データオーナーへの説明

5.1 個人情報保護違反の防止と規制当局への連絡が迅速化

GDPR 違反は個人情報収集の告知の不備と、管理のずさんさが原因になっています。可視化データ「資産や事業リスク」を用いて、個人情報に関連する法令を正確に把握し、企業の法令対応状況を可視化し、個人情報の収集に関する法令への対応を確実にすることで、違反を回避することができます。そして、可視化データ「セキュリティ状況」を把握して常に監視することで、セキュアに管理していることを証明することが可能になります。

しかし、セキュリティでは個人情報を保有する以上、リスクをすべて回避することは不可能です。万が一の場合には、規制当局への迅速な対応が要求されます。可視化データ「説明責任に必要な情報」を迅速に対応することで、制裁金が大幅に減額された例も存在します。

5.2 暗号資産流出を抑制して事後対応も改善

暗号資産流出の対策は、何といってもセキュリティ被害を出さないことですが、ここでも可視化データで改善できます。まずは、顧客資産を預かっているという重大リスクを可視化データ「資産や事業のリスク」で明確にし、セキュリティ規則が自社従業員およびサプライチェーン従業員まで浸透しているかを可視化データ「セキュリティ状況」「サプライチェーン」で把握することで、暗号資産を流出させない対策（踏み台攻撃に安易に引っかからない、トランザクションデータが改ざんされない）ことに繋がります。

万が一暗号資産が流出した場合、監督官庁や金融庁に状況と可視化データ「説明責任に必要な情報」を用いて迅速に報告できます。特に、金融機関などの重要インフラ事業者は、情報や資産の流出の被害が自社だけでなく、顧客にまで影響します。迅速に説明責任を果たすことで、顧客がその影響をハンドリングでき、顧客の被害の最小化につながります。

5.3　重大な脆弱性への効果的な対応

Log4J2 のような部品としてのソフトウェアの脆弱性に対しても、可視化データで改善が可能です。可視化データ「資産や事業のリスク」の一要素であるビジネスインパクト分析結果を用いて、優先的に検査するべき対象のシステムを特定することから始めることで、事業上のリスクが高いシステムから対応することが可能になります。

可視化データ「資産や事業のリスク」の一要素である SBOM により情報資産、ソフトウェア資産を可視化することで、問題が発生したソフトウェア部品を使用しているかどうかの確認が行えます。現場の負荷が軽減されて迅速に対応することが可能になります。そして、そのソフトウェアの影響を評価するために可視化データ「セキュリティ状況」の脆弱性分析結果を用いることで、対応の優先度を掌握することができます。これは一般にトリアージと呼ばれ、対策の時期を決定することができます。

そして、メーカやサービスプロバイダーは顧客に対して説明しなければなりません。可視化データ「説明責任に必要な情報」を利用して、正確な情報を迅速に報告することで信頼の維持および向上に結び付けることができます。

5.4　ランサムウェア攻撃による事業停止の回避と適切なインシデント対応

ランサムウェアの対策は、ランサムウェアによる攻撃を受けないことですが、ここでも可視化データで改善できます。可視化データ「資産や事業のリスク」によって、企業とって暗号化されると致命傷になる資産の管理状況を可視化データ化し、経営者が把握することが必要です。また、ランサムウェア攻撃が可視化データ「サプライチェーン」でサプライチェーンが踏み台にされていることをしっかりと把握し、対策を指示することも必要です。経営者が認識することで、セキュリティ措置の実施を現場任せにすることがなくなります。万が一、ランサムウェアの被害に合った場合でも経営層は適切な指示が出せ、情報資産の復旧のための準備も指示することができます。そして、可視化データ「セキュリティ状況」を利用することで、保全対策がしっかりされているかを把握することで、リスクに応じた防御態勢がなされていることを検証し、セキュリティガバナンスを実現することができます。

最後に、ランサムウェア攻撃は情報漏えいに直結しています。可視化データ「説明責任に必要な情報」を用いて、データオーナーに正確かつ迅速に状況を通知することが可能になります。漏えいした情報によっては、迅速に対応すれば実害が発生しないケースもあります。

6　おわりに

経営層はデータに基づくサイバーセキュリティマネジメントが強く求められつつあり、本書では可視化データを定義することの重要性とその必要性について述べてきました。可視化データを把握して、セキュリティ関連の情報の透明性を高めることで、データに基づいたサイバーセキュリティの判断と適切

な指示や報告が可能なることを示しました。
　経営層に求められる可視化データの特定、収集、分析、活用ができる体制を整備することが必要です。そこで、下記にように提言します。

(a) 必要な可視化データの特定
それぞれの組織のガバナンスを達成するめに、4 分類の可視化データにおいて、個々の企業で必要な具体的な可視化データを特定することを検討してください。
(b) 可視化データの収集機能の整備
可視化データを収集する組織的なプロセスや自動化システムの導入を検討してください。SBOM の収集、脆弱性分析、セキュリティアセスメント、インシデントレポートの提出などを定常化してもらうようにしてください。
(c) 可視化データの分析
収集した可視化データを経営層が分析できるようにしてください。例えば、ダッシュボード上で可視化データを網羅的に表示して、状況の変化や不測の事態を観測できるようにして、説明責任を果たせるようにしてください。
(d) 可視化データの活用
データドリブン型の経営を実践する上でも、可視化データにもとづいてサイバーセキュリティに関する経営判断をおこなえるようにしてください

　今後、本コンソーシアムでは、具体的な可視化データの定義について検討していきます。本書に賛同し、ともに活動して頂ける皆さまをお待ちしております。以下のウェブサイト、もしくは連絡先までお気軽にお問合せください。

- セキュリティ・トランスペアレンシー・コンソーシアム オフィシャルウェブサイト
  https://www.st-consortium.org/
- セキュリティ・トランスペアレンシー・コンソーシアム事務局
  stc-info@st-consortium.org

2026 年 2 月 1 日における本コンソーシアムの参加事業者は以下のとおりです。

- アズビル株式会社
- 一般社団法人沖縄オープンラボラトリ
- ＮＲＩセキュアテクノロジーズ株式会社
- ＮＴＴ株式会社
- 株式会社アシュアード
- 株式会社ＮＴＣ
- 株式会社ＮＴＴデータグループ
- 株式会社ＦＦＲＩセキュリティ
- 株式会社ジークス

- 株式会社ＰＥＧＡＳＵＳ　ＨＯＬＤＩＮＧＳ
- 株式会社ラック
- Ｃｏｖａｌｅｎｔ株式会社
- サイバートラスト株式会社
- シスコシステムズ合同会社
- 東京エレクトロン株式会社
- ＴＩＳ株式会社
- 日本電気株式会社
- 株式会社日立製作所

用語集

用語	定義
経営者	ソフトウェアサプライチェーンを構成する事業者や、ソフトウェ アサプライチェーンを通じて提供される製品・システム・サービ スを利用する事業者の経営層
SBOM	ソフトウェアの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インベントリー(一覧表) のこと。コンポーネントやその依存関係をすべて表現している場合もある。OSS だけではなくプロプライエタリソフトウェアに活用することもでき、広く一般に公開するほか関係者だけに提示するという使用方法も存在する。
可視化データ	サプライチェーンにおいて事業者間で授受される製品・システム・サービス等などにおけるソフトウェアやハードウェアについての「構成」や「状態」、「リスク」を表現する情報のこと。 SBOM は製品などのソフトウェアについての「構成」を表現した情報であり、可視化データに含まれる。
サプライチェーン（Supply Chain）	製品とサービスの調達から始まり、ライフサイクル全体に及ぶ、組織の複数の階層間でのリソースとプロセスのリンクされたセット [ISO 28001:2007, NIST SP 800-53 Rev.5]
脆弱性（Vulnerability）	一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2014]
Form 8-K	アメリカの証券取引委員会（SEC）に登録している上場企業が提出する臨時報告書。日本で言う「適時開示情報」や「決算短信」に近く、四半期報告書／年次報告書（Form 10-Q／Form 10-K）の間に発生した重要な重大事象を迅速に投資家に知らせる目的で用いられる。 https://en.wikipedia.org/wiki/Form_8-K
Form 10-K	アメリカの証券取引委員会（SEC）に登録している上場企業が提出する年次報告書で、1 年間の財務情報や経営状態を網羅的に開示する公的文書。米国版有価証券報告書に該当する。 https://en.wikipedia.org/wiki/Form_10-K