経営層向けセミナー　経営者のためのサイバーセキュリティ戦略

～リスクを軽減し、サプライチェーンを守る

経営課題としてのサイバーセキュリティと法律実務

2024年3月14日

森・濱田松本法律事務所 カウンセル弁護士

慶應義塾大学大学院 政策・メディア研究科 特任准教授（非常勤）

蔦　大輔

セキュリティインシデントがもたらす経済的損失

調査・分析実施主体	対象期間	経済的損失の概要	損失額
トレンドマイクロ （サイバー攻撃による法人組織の被害状況調査：2023年11月）	2021年～2023年	過去3年間でのサイバー攻撃の被害を経験した法人組織の平均の累計被害額	**1億2,528万円** ランサムウェア被害を経験した組織は**1億7,689万円**
警察庁 （令和４年におけるサイバー空間をめぐる脅威の情勢等について：2023年3月16日）	2022年	ランサムウェア被害に関連して要した調査・復旧費用の総額	24％が100万円未満 16％が100万円～500万円未満 14％が500万円～1000万円未満 **33％が1000万円～5000万円未満** 13％が5000万円以上
日本ネットワークセキュリティ協会(JNSA) （調査研究部会インシデント被害調査WGによる「サイバー攻撃被害組織アンケート調査（速報版）」：2023年10月）	2017年1月～2022年6月	ランサムウェア感染組織、Emotet感染組織、ウェブサイトからの情報漏えい組織の被害金額の平均	ランサムウェア：**2,386万円** Emotet：**1,030万円** Webからの漏えい ・クレカ番号含む：**3,843万円** ・個人情報のみ：**2,955万円**

サイバーセキュリティに関する様々なリスク

1. 情報セキュリティリスク

- 企業が保有する機密情報や個人情報が漏えい等するおそれ

2. システムリスク・事業継続リスク

- 利用しているシステムが停止し、業務に影響を及ぼすおそれ

3. サプライチェーンリスク

- 製品製造の過程で悪意ある機能が組み込まれるおそれ
- 製品、情報などの一連の商流の中で、脆弱な組織が狙われるおそれ

4. リーガルリスク

- 情報漏えいや業務停止等により、規制当局による法執行や、関係者に対する賠償問題となるおそれ

5. レピュテーションリスク

- インシデントの発生が明るみに出ることで企業のレピュテーションに影響を及ぼし、株価や取引関係に影響を及ぼすおそれ

サイバーセキュリティに関係する主な法令の大まかな分類

基本法・理念法	サイバーセキュリティ基本法、情報処理促進法、デジタル社会形成基本法　など
体制整備・経営	会社法、金融商品取引法、各業法　など
情報管理	個人情報保護法、マイナンバー法、不正競争防止法、知的財産法、各業法など
労務管理	労働契約法、労働基準法、労働安全衛生法　など
サプライチェーン	独占禁止法、下請法、経済安全保障推進法　など
通信	電気通信事業法、電子署名法、NICT法　など
通商・経済安全保障	外為法、経済安全保障推進法　など
インフラ防護	各業法、経済安全保障推進法　など ※「重要インフラ」と「基幹インフラ」
製品安全	製造物責任法、電気通信事業法、電気事業法、道路運送車両法、航空法、薬機法など
刑事法	刑法、不正アクセス禁止法、不正競争防止法、刑事訴訟法 など

近年の主なサイバーセキュリティ関連法制度等（欧米）

	欧州	米国
インフラ防護等	**NIS2指令** 2024年10月までに国内法化予定	**重要インフラインシデント報告法（CIRCIA）** 2024年3月までに規則案公表、そこから18ヶ月以内に最終規則を公布
製品セキュリティ（IoT製品等）	**サイバーレジリエンス法案** 2023年11月に欧州理事会と欧州議会が政治的に合意	**USサイバートラストマーク** 2024年開始予定
情報開示		**SEC新開示ルール**

会社法とサイバーセキュリティ

会社法とサイバーセキュリティの関係性
➡ **内部統制システム構築義務**としてのセキュリティリスク管理体制

- **内部統制システムとは**

  会社が営む事業の規模、特性等に応じたリスク管理体制。ここにいう「リスク」の一つとしてサイバーセキュリティに関することも含まれ得る

- **内部統制システムに関する義務**
  - 大会社等の取締役（会）に内部統制システム構築に関する事項の決定義務（会社法348条3項4号など）
  - それ以外の会社の取締役も、内部統制システムを構築しない場合に、会社に対する善管注意義務・忠実義務違反とされる可能性

内部統制システム構築義務と役員の責任

■ 取締役会等でどこまで決定する必要があるか

- 目標の設定、目標達成のために必要な内部組織及びその権限、内部組織間の連絡方法、是正すべき事実が生じた場合の是正方法等に関する**重要事項（要綱・大綱等）を決定**することで足りる
- 具体的な内部統制の体制の在り方は、各会社が営む**事業の規模や特性等に応じて、その必要性、効果、実施コスト等を勘案**して各会社にて決定

■ 役員の責任

- 内部統制システムの不備によりセキュリティ事故が発生し、会社に損害が発生した場合、役員が会社に対する損害賠償責任を負う可能性
  ① 会社に対する責任（会社法423条）
  ② 第三者に対する責任（会社法429条）
- 義務違反の有無は、いわゆる経営判断原則の枠組みによる

義務の水準等について

- 義務水準は事業内容や規模等を踏まえた実務慣行によって定まるため、**同規模、同業他社等で採用されている体制との比較**の観点が重要

- 義務水準の検討に当たっては、実務上のガイドライン等が充実し、サイバーセキュリティ確保の重要性が高まっていることも要考慮。**以前問題ないとされたものが数年後も同様に評価されるとは限らない。**構築後も継続的にモニタリングし、適時アップデートを

- 過去に同様の原因によるセキュリティインシデントがあった等、インシデントを予見すべき特別な事情があるならば、その事情を踏まえた対応を行うべき（**再発防止策の適切な実施**など）

内部統制システムに関する裁判例

■ セキュリティインシデントと内部統制システム

◆広島高判令和元年10月18日LEX/DB25564819

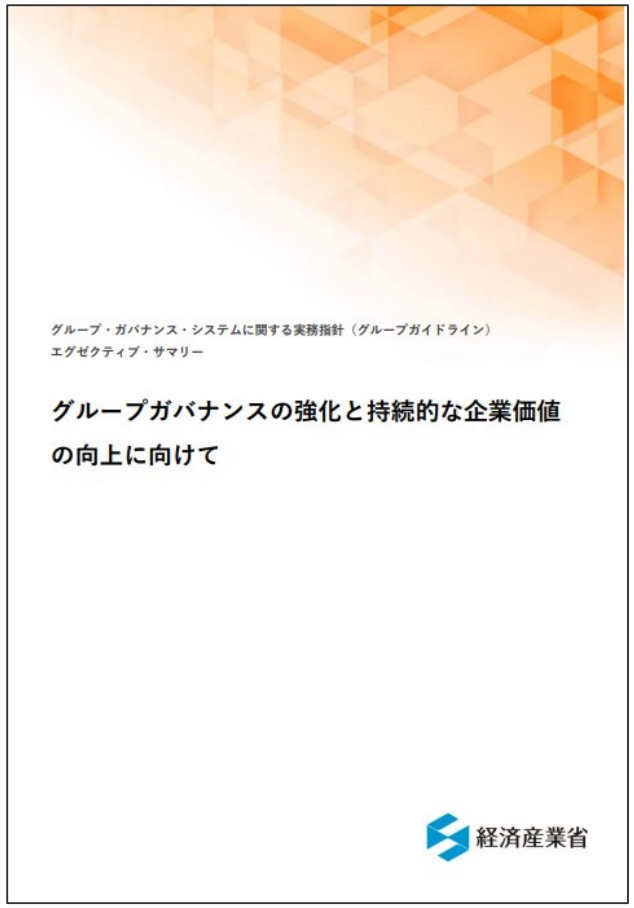
「…グループにおいては、**事業会社経営管理規程等の各種規程が整備され、それらに基づき、人事や事業計画への関与、グループ全体のリスク評価と検討、各種報告の聴取等を通じた一定の経営管理をし、法令遵守を期していたものであるから、企業集団としての内部統制システムがひととおり構築され、その運用がなされていた**といえる。そして、会社法は内部統制システムの在り方に関して一義的な内容を定めているものではなく、あるべき内部統制の水準は実務慣行により定まると解され、その具体的内容については当該会社ないし企業グループの事業内容や規模、経営状態等を踏まえつつ取締役がその裁量に基づいて判断すべきものと解される」

＜参考＞グループガイドライン

■ グループ・ガバナンス・システムに関する実務指針

- ✓ 経済産業省が2019年に策定
- ✓ **サイバーセキュリティは、内部統制システム上の重要なリスク項目**である
- ✓ 具体的検討にあたっては**サイバーセキュリティ経営ガイドラインを適宜参照**すべき

- ➢ ベストプラクティス等をまとめたものであり、記載された取組みが必須というわけではない
- ➢ しかし、**サイバーセキュリティに関する内部統制システム構築義務として求められる水準を検討するにあたっては、一定の影響を及ぼす**と考えられる



＜参考＞サイバーセキュリティ経営ガイドライン

- 経済産業省とIPAが策定（2023年3月にver3.0公開）
- サイバーセキュリティ経営の重要10項目（経営者が指示すべき項目）
- 2023年10月に、IPAが実践のためのプラクティス集を公開（ver3.0対応）

指示１	サイバーセキュリティ**リスクの認識、組織全体での対応方針**の策定
指示２	サイバーセキュリティ**リスク管理体制**の構築
指示３	サイバーセキュリティ対策のための**資源（予算、人材等）確保**
指示４	サイバーセキュリティ**リスクの把握とリスク対応に関する計画**の策定
指示５	サイバーセキュリティ**リスクに効果的に対応するための仕組み**の構築
指示６	**PDCAサイクル**によるサイバーセキュリティ**対策の組織的改善**
指示７	インシデント発生時の**緊急対応体制**の整備
指示８	インシデントによる被害に備えた**事業継続・復旧体制**の整備
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
指示10	**サイバーセキュリティに関する情報の収集、共有及び開示の促進**

＜参考＞重要インフラのサイバーセキュリティに係る行動計画

■ 任務保証を踏まえた重要インフラサービスの安全かつ持続的な提供
■ 官民一体で重要インフラのサイバーセキュリティ確保に向けた取組を推進

- サイバー攻撃や自然災害等に起因するサービス障害等をリスクと捉え、許容範囲内に抑制
- 組織全体での対応を促進。経営の重要事項としてサイバーセキュリティを位置づけ、経営層のサービス障害等に対する責任を明記
- 経済安全保障推進法の基幹インフラ防護とは別の制度

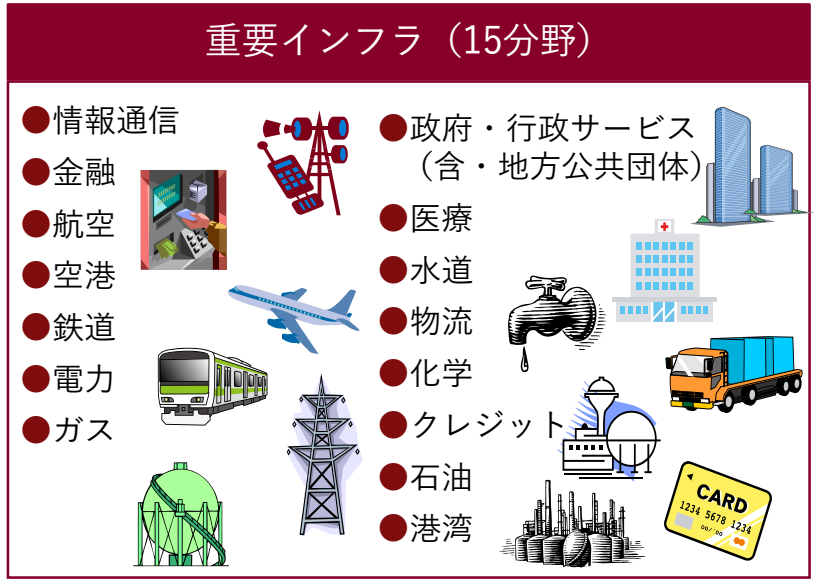
– サイバーセキュリティ戦略本部が15の重要インフラ分野を指定

※ 2024年3月8日に「港湾」を追加

– 分野に属する事業を行っている者すべてが重要インフラ事業者として行動計画の対象となるわけではない

– 「主たる」「主要な」「小規模なものを除く」といった限定あり

※ 詳細は行動計画別紙1「対象となる重要インフラ事業者等と重要システム例」を参照



金融商品取引法とサイバーセキュリティ

金融商品取引法とサイバーセキュリティの関係性
➡ サステナビリティ情報開示・内部統制報告・適時開示　など

- **有価証券報告書におけるサステナビリティ情報の開示**
  - サステナビリティ情報には、サイバーセキュリティ、データセキュリティに関する事項が含まれうる
- **内部統制報告制度の改訂**
  - ITへの対応として、サイバーリスクの高まりを踏まえセキュリティ確保が重要である旨の記述が追加
- **適時開示（証券取引所規則）**
  - 現状は基本的にバスケット条項（投資判断への著しい影響）のみ
  - 米国SECにおける新たなルール策定（2023年7月）の影響

金商法等に基づくサイバーセキュリティ関連の主な開示

平時	・セキュリティ対策 ・リスク管理体制 ・ガバナンス等 の公表・開示	● **金融商品取引法** ① 有価証券報告書等における**サステナビリティ開示** ※「サステナビリティ情報」には、サイバーセキュリティやデータセキュリティ等が含まれうる ② 内部統制報告制度（J-SOX法）改訂： サイバーリスクが強調
有事	セキュリティインシデントに関連する 公表・開示	● **金融商品取引法・有価証券上場規程** ・臨時報告書（金融商品取引法）、 ・適時開示（有価証券上場規程） ① 災害（重要な災害） ※「災害」には人災も含む ② バスケット条項 ※上場会社の運営、業務若しくは財産又は当該上場株券等に関する重要な事実であって投資者の投資判断に著しい影響を及ぼすもの（有価証券上場規程）

有価証券報告書におけるサステナビリティ情報開示

■ サステナビリティ情報とは

- 企業の中長期的な持続可能性に関するもの。
- 具体的には、環境、社会、従業員、人権の尊重、腐敗防止、贈収賄防止、ガバナンス、**サイバーセキュリティ、データセキュリティ**に関する事項が含まれうる（金融庁「記述情報の開示に関する原則（別添）－サステナビリティ情報の開示について－」

■ サステナビリティ情報の開示

- 「ガバナンス」「リスク管理」「戦略」「指標・目標」の4つに沿って記載。
- ガバナンスとリスク管理は全ての企業で開示が必要、戦略と指標・目標については、一部を除き各企業が重要性を判断して開示
- **具体的にどのようなテーマを選定して記述するかは、法令による限定はなく、**ガバナンスとリスク管理を通じて、自社の業態や経営環境、企業価値への影響等を踏まえ、サステナビリティ情報の重要性を判断。よって、**サイバーセキュリティに関する開示は、法令上必須とされているわけではない（重要と判断すれば記述が必要）。**

＜参考＞サステナビリティ情報開示の具体例（抽象化）

■ ガバナンス

CEOを委員長とする情報セキュリティ委員会において、サイバーセキュリティに関するリスクの状況と評価、リスク低減計画の進捗を定期的に報告・協議し、対策を講じており、特に重要なリスクを取締役会に報告しています。…

■ リスク管理

情報セキュリティ管理責任者のもと、重大インシデントを集約し取締役会に報告しております。また、内部規程やこれに基づく内部監査や第三者評価を実施するとともに、業界団体との意見交換・連携を行っています。…

■ 戦略

ISMSの国際規格やNISTのサイバーセキュリティフレームワークに沿って、サイバーセキュリティリスクに対応するための体制を構築しています…

サイバー攻撃に対する予防や攻撃を受けた場合の対応、復旧および再発防止を重要なテーマとして選定し、これらに対応して以下の施策を実施しています。

（1）サイバー攻撃の予防…

（2）…

■ 指標

定期的に演習を実施しており、●年●月期は●件の演習を実施しました。…過去5年間における重大なセキュリティインシデントの発生件数は●件でした。…

米国証券取引委員会：セキュリティ関連の開示ルール

■ 米国証券取引委員会（SEC）による開示ルールの採択

SECは、2023年7月26日付で、上場登録会社に対し、主に以下の2つを義務付ける規則を採択

（1）サイバーセキュリティ体制に関する定期開示（年次）

✓ サイバーセキュリティに関するリスク管理、戦略、ガバナンスの開示

（2）重大なサイバーセキュリティインシデントの臨時開示

✓ サイバーセキュリティインシデントが重大であると**判断してから４営業日以内**に提出

✓ インシデント発見から不当な遅延なく重大性を判断

■ 制度の観点からの日本への影響

日本においても同種の制度導入に向けての議論の可能性

＜参考＞大手議決権行使助言会社の最新の方針

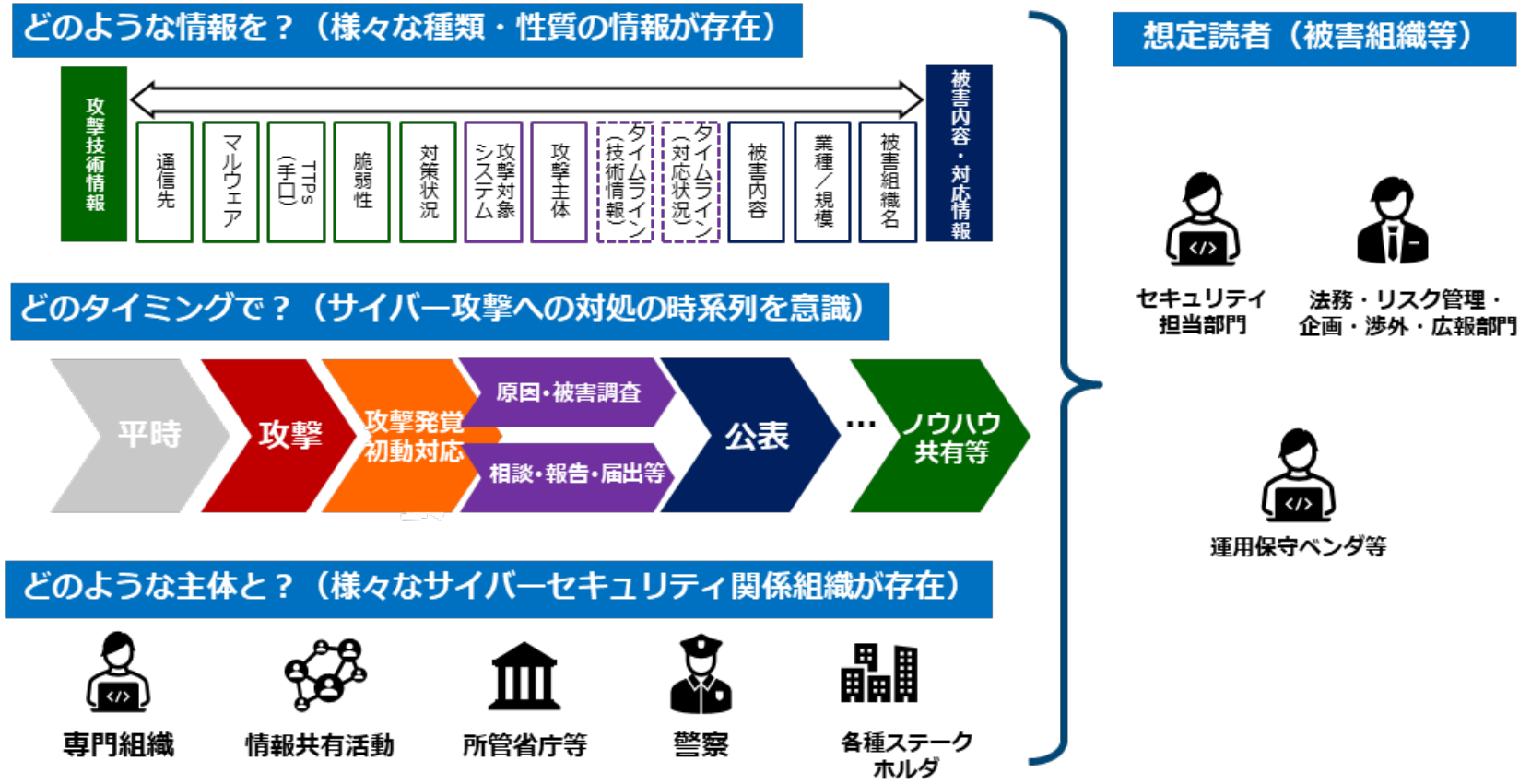
■ グラスルイス（Glass Lewis）の日本市場向けの助言方針（2024 Benchmark Policy Guidelines）にサイバーリスクが追加

◆ サイバーリスクの監督（サマリ）

サイバーリスクの監督についての考え方に関する**新たな論点を追加**した。サイバー関連の潜在的な不利益を考慮すると、**サイバーリスクは全ての企業にとって重大な懸念事項である**と考える。 したがって、企業はこれらのリスクを可能な限り検証し、軽減することが重要であると考える。このような観点から、**全ての企業に対して、サイバーセキュリティに関わる事項を監督する取締役会の役割について、明確な開示を行うことを推奨**する。さらに、急速に変化を続けるこの重要な課題につい て、企業が取締役に対して、どのように熟知させているかを開示することは、企業がこの問題につい て真剣に取り組んでいるということを株主が理解する一助になると考える。**原則として、サイバー関連の問題における企業の監督や開示に基づいた助言判断は行わない。ただし、サイバー攻撃によって株主に重大な損害が生じた場合、この点に関する企業の情報開示を精査し、その開示内容や監督が不十分であると考えられる場合には、しかるべき取締役に対して反対助言を行う場合がある。**

サイバー攻撃被害に係る情報の共有・公表ガイダンス

- サイバーセキュリティ協議会内の検討会（事務局：警察庁、総務省、経済産業省、NISC、JPCERT/CC）における検討を経て2023年3月に策定



https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_gaiyou.pdf

ご清聴ありがとうございました

Lawyer profile

蔦　大輔

Daisuke　Tsuta

カウンセル

東京弁護士会所属

TEL: 03-6266-8769

daisuke.tsuta@mhm-global.com

主要な取扱分野

サイバーセキュリティ、個人情報保護、IT・ICT

- サイバー攻撃の予防、攻撃を受けた後の対応に関する助言、サポート、従業員による内部不正対応
- 個人情報保護・データ利活用、インターネットサービスに関するサポート
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」、「サイバーセキュリティ関係法令Q&Aハンドブック」の策定に関与

著作・論文

- 「クロスセクター・サイバーセキュリティ法」（商事法務NBLで連載中、2023年）
- 『類型別　不正・不祥事への初動対応』（中央経済社、2023年、共著）
- 『情報刑法Ⅰ　サイバーセキュリティ関連犯罪』（弘文堂、2022年、共著）
- 『60分でわかる！改正個人情報保護法超入門』（技術評論社、2022年、共著）
- 『事例に学ぶサイバーセキュリティ 多様化する脅威と法務対応』（経団連出版、2020年、共著）

その他、著書・論文・講演多数

オンライン名刺

経歴

京都大学法学部卒業、神戸大学法科大学院修了

財務省近畿財務局、総務省行政管理局、内閣官房内閣サイバーセキュリティセンター(NISC)にて任期付公務員として執務（2014年～2020年）

主な活動

2016年 情報ネットワーク法学会理事（～2020年）

2021年 総務省 IPネットワーク設備委員会 事故報告・検証制度等タスクフォース　構成員

2022年 筑波大学大学院 人文社会ビジネス科学学術院 ビジネス科学研究群 非常勤講師

2022年 サイバーセキュリティ協議会 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 委員

2022年 警察庁 サイバー被害の潜在化防止に向けた検討会 委員

2023年 慶應義塾大学大学院政策・メディア研究科 特任准教授

2023年 日本弁護士連合会 弁護士業務における情報セキュリティに関するワーキンググループ 委員

2023年 経済産業省 サイバー攻撃による被害に関する情報共有の促進に向けた検討会 委員

2023年 サイバーセキュリティ法制学会理事

2023年 警察庁 キャッシュレス社会の安全・安心の確保に関する検討会 委員

2024年 総務省サイバーセキュリティタスクフォース ICTサイバーセキュリティ政策分科会 構成員

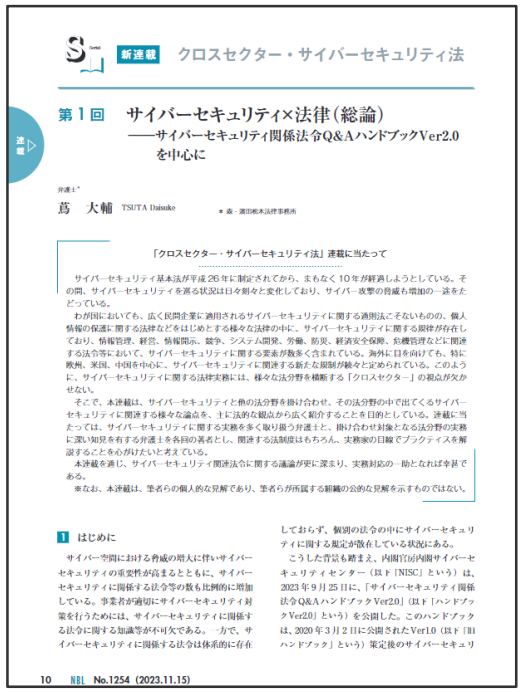
受賞歴等

The Legal 500 Asia Pacific 2024のTMT部門においてNext Generation Partnersに選出

【PR】連載「クロスセクター・サイバーセキュリティ法」

■ NBL（商事法務）において2023年11月から連載中

- ✓ サイバーセキュリティと特定のテーマを掛け合わせた実務上の論稿
- ✓ 掛け合わせ対象となる各分野を主に取り扱う弁護士の共著
- ✓ 雑誌連載は全10回を予定（2024年3月14日現在第4回まで）



新連載 クロスセクター・サイバーセキュリティ法

第1回 サイバーセキュリティ×法律（総論）
——サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0を中心に

弁護士
葛 大輔 TSUTA Daisuke
＊森・濱田松本法律事務所

「クロスセクター・サイバーセキュリティ法」連載に当たって

サイバーセキュリティ基本法が平成26年に制定されてから、まもなく10年が経過しようとしている。その間、サイバーセキュリティを巡る状況は日々刻々と変化しており、サイバー攻撃の脅威も増加の一途をたどっている。

わが国においても、広く民間企業に適用されるサイバーセキュリティに関する通則法こそないものの、個人情報の保護に関する法律などをはじめとする様々な法律の中に、サイバーセキュリティに関する規律が存在しており、情報管理、経営、情報開示、競争、システム開発、労働、防災、経済安全保障、危機管理などに関連する法令等において、サイバーセキュリティに関する要素が数多く含まれている。海外に目を向けても、特に欧州、米国、中国を中心に、サイバーセキュリティに関連する新たな規制が続々と定められている。このように、サイバーセキュリティに関する法律実務には、様々な法分野を横断する「クロスセクター」の視点が欠かせない。

そこで、本連載は、サイバーセキュリティと他の法分野を掛け合わせ、その法分野の中で出てくるサイバーセキュリティに関連する様々な論点を、主に法的な観点から広く紹介することを目的としている。連載に当たっては、サイバーセキュリティに関する実務を多く取り扱う弁護士と、掛け合わせ対象となる法分野の実務に深い知見を有する弁護士を各回の著者とし、関連する法制度はもちろん、実務家の目線でブックティスを解説することを心がけたいと考えている。

本連載を通じ、サイバーセキュリティ関連法令に関する議論が更に深まり、実務対応の一助となれば幸甚である。

※なお、本連載は、筆者らの個人的な見解であり、筆者らが所属する組織の公的な見解を示すものではない。

1 はじめに

サイバー空間における脅威の増大に伴いサイバーセキュリティの重要性が高まるとともに、サイバーセキュリティに関係する法令等の数も比例的に増加している。事業者が適切にサイバーセキュリティ対策を行うためには、サイバーセキュリティに関係する法令に関する知識等が不可欠である。一方で、サイバーセキュリティに関係する法令は体系的に存在しておらず、個別の法令の中にサイバーセキュリティに関する規定が散在している状況にある。

こうした背景も踏まえ、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という）は、2023年9月25日に、「サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0」（以下「ハンドブック Ver2.0」という）を公開した。このハンドブックは、2020年3月2日に公開されたVer1.0（以下「旧ハンドブック」という）策定後のサイバーセキュリ

10 NBL No.1254（2023.11.15）

回	サイバーセキュリティ×[テーマ（予定）]
1	法律（総論）
2	個人情報保護法（個人データ漏えい等対応）
3	**会社法（内部統制システム構築義務）**
4	**ディスクロージャー（金商法に基づく開示等）**
5	**経済安全保障（インフラ防護、セキュリティ・クリアランス）**
6	競争法（サプライチェーンリスク対策など）
7	システム開発（システムの脆弱性と法的責任など）
8	労働法（セキュリティと労務管理）
9	危機管理（有事対応）
10	防災（BCPなど）