研究ノート

わが国の電気事業者における サイバーセキュリティガバナンス強化の検討

A Study on Enhancing Cybersecurity Governance of Japanese Electric Utilities

キーワード：サイバーセキュリティ，ガバナンス，取締役会，CISO

外　﨑　静　香

社会全体でデジタル化が進むにつれて，サイバー攻撃が増加している。これまでは個人や政府機関，一般企業への攻撃が多かったが，最近では重要インフラ（通信，交通，電力，ガス，水道等）への攻撃が世界中で増加している。殊に電力のような公益事業は，経済社会活動や市民生活，更には国家運営にまで影響を及ぼす惧れがあることから，サイバー攻撃の恰好の的になり得る。このような攻撃に備えるためにも，電気事業者には，有事を未然に防止し，かつ，有事の際に迅速・適切に対応できる「守りのガバナンス」の構築が必要である。そこで本稿では，わが国の電気事業者のセキュリティガバナンスの一検討材料として，海外のセキュリティ対策に関する実態を整理した。その結果，海外では経営層がセキュリティ対策に関与する仕組をとる企業が多く，セキュリティ関連の専門性を有する人材（CISO等）の取締役への登用によるガバナンス強化を重要視していることを示した。

1. はじめに

近年，デジタル技術を活用して，既存事業の効率化や新たな価値の創出を目指すデジタルトランスフォーメーション（DX）が様々な業界で進展しており，電気事業者についても同様の変化が見られる。電気事業者は，生活に欠かせないインフラ産業として，保有する設備の保守管理や電力の安定供給，顧客管理や顧客サービスの向上のために，これらのデジタル技術を活用して効率的な事業運営に努めている。ところが，事業のデジタル化に伴い，社内のネットワークに部外者が侵入する機会が増加している。さらに最近，海外では，社内ネットワークだけに留まらず，そこを経由して電力用の制御システムにまで侵入し，そのシステムを操作して，物理的な被害を与える事例も発生するようになった。これらのサイバー攻撃に対し，企業独自の対策や，サイバーセキュリティサービス企業による対策ソフトウェアの開発等が日々行われている。このように，DXの推進に伴い，サイバーセキュリティの問題は避けて通ることができないため，技術面での対策が各所で行われ始めた。

一方で，セキュリティに関する上記のような対策を社内でどのように進めるかは，企業によって異なる。わが国では，情報通信業や金融業におけるセキュリティ対策は比較的進んでいるものの，セキュリティ関連の問題発生率が最も高い生活インフラサービス（水道・ガス・電力）におけるセキュリティ対策は，全業種の平均以下と評価さ

れている[1]。対策が進まない一因として，取締役会メンバーにおけるリスクの認識や関与度の低さを指摘する声もある[2]。取締役会は，「会社の業務執行の意思決定機関」および「取締役の職務執行の監督機関」としての役割があるが，会社の方針としてセキュリティに関する業務を執行するか否かを最終的に決めるのは，前者としての役割である[3]。つまり，必要とされるセキュリティ関連の課題やその対応策について，担当部門から説明・提案を行ったとしても，取締役会でそれを執行する決定が出なければ対応することができないため，取締役会メンバーのセキュリティリスク認識が重要となる。

また，取締役会で対応策の議論が行われたとしても，サイバー攻撃は日時を問わず行われているため，事象の発生から対応策の検討，その執行の決定までが迅速でなければならない。突発的な問題を可能な限り早く解消するためには，問題の発生からすぐに対策を考えることのできる瞬発力と，対策を会社の方針として承認する意思決定力，対応のために人を動かすことのできる機動力が必要である。

昨今のデジタル化の進度に鑑みると，サイバーセキュリティに関連するリスクから企業を守って事業を継続させるためには，セキュリティへの対応が必須となる。特に電気事業については，通常の事業運営に加え，2021年に開催が予定されている東京オリンピック・パラリンピック（以下，「東京五輪」という）に向けても，セキュリティ対応が求められるようになっている。そこで本稿では，すでにサイバー攻撃を受けた経験のある海外の企業に着目し，そのガバナンス面でのセキュリティ対応の実態を明らかにすることで，わが国の電気事業者のサイバーセキュリティにおける，「守りのガバナンス」を構築するための一助とする。

以下，第2章では，攻撃が集中するイベントであるオリンピック・パラリンピックに関連して実際に発生したサイバー攻撃の事例や，2021年に開催予定である東京五輪に向けたセキュリティ対策について整理する。さらに，社会インフラに対する攻撃傾向について述べることで，セキュリティガバナンスの重要性を示す。第3章は，海外でのセキュリティ対策のための取組に関し，企業におけるガバナンスの実態や課題について明らかにしたうえで，電気事業者がセキュリティ対策のためにとったガバナンス体制の事例を紹介する。第4章では，わが国のセキュリティガバナンスの現状と政策の動きについて整理する。そして第5章では，本稿全体を振り返り，わが国の電気事業者等の重要インフラがセキュリティ対策に取り組む際に必要なガバナンス体制についての一考を提示する。

2. 世界におけるサイバー攻撃の動向

これまでのサイバー攻撃には，インターネットに接続されている社内パソコンを経由して社内ネットワークに不正に侵入するという手口が多かった。しかし，2020年初頭に世界的流行となった新型コロナウイルスの感染予防対策として在宅勤務を導入する企業が急増したことにより，従業員の自宅ネットワークセキュリティの脆弱性や，メールを利用した攻撃が世界中で増加している[4]。

そこで，運営にもステークホルダーにも影響力の大きいイベントであるオリンピック・パラリンピックを例に，過去のサイバー攻撃や，わが国での対策を紹介したうえで，現在増加している，社会インフラに対する新たな攻撃の傾向を紹介する。

---

[1] トレンドマイクロ（2019）22頁，27-28頁。
[2] 同上30頁。
[3] 取締役会以外を意思決定機関とするガバナンス体制もあるが，本稿では，取締役会を意思決定機関としている場合について議論する。
[4] VMWCR (2020), pp.7-8. 英国・米国・シンガポール・イタリアで実施された調査によれば，新型コロナウイルス発生以降，91%の企業が，在宅勤務によるサイバー攻撃の増加を実感している。

2.1 オリンピック・パラリンピックのサイバーセキュリティ

2.1.1 サイバー攻撃の歴史

過去10年間で行われたオリンピック・パラリンピックでは，表1のとおり，様々なサイバー攻撃を受けている。直近では，2018年に開催された平昌オリンピックの開会式でのトラブルが記憶に新しい。競技自体に大きな影響を及ぼす攻撃はなかったものの，開会式の直前にオリンピック組織委員会のインターネット環境に障害が発生し，インターネットテレビやWi-Fiが繋がらなくなるという問題や，大会公式ウェブサイトのシステム障害によってチケット印刷が妨害されるという問題が生じた。この原因は，Olympic Destroyerというコンピューターウイルスによるものと特定され，2020年10月20日には，その攻撃を行った犯人がロシア連邦軍参謀本部情報総局（GRU：Glavnoe Razvedyvatel'noe Upravlenie）であったことが発表された[5]。その他の大会の開催国でも，平昌大会と同様に，大会前の準備段階から大会当日までの長期間にかけて，世界中から数多のサイバー攻撃を受けている。

オリンピック・パラリンピックは世界規模の巨大イベントであるため，攻撃を与える側にとっては，多くの注目を浴びるだけでなく，チケットやグッズの購入，宿泊施設の予約等，大会に関連して提供される個人情報を窃取し，その情報自体の売買，あるいはクレジットカード情報の不正利用によって経済的利益を得ることもできる[6]。ゆえに，大会と関連のある団体・企業等は，世界中からの攻撃を集中的に受けることが予想されるため，それに対応できる体制の構築が必須である。

2.1.2 わが国での取組

わが国では，来る2021年に開催予定である東京五輪でのサイバーセキュリティ対策が，目下の大きな課題となっている。実際に，GRUが東京五輪

表 1　過去のオリンピックにおけるサイバー攻撃

開催年	開催地	攻撃件数	攻撃の件数・詳細
2018年	平昌（韓国）	6億550万件（準備期間から大会期間にかけて）	● 大会公式ウェブサイトのシステム障害 ● プレス用のネットワーク遮断 ● 会場内のネットワーク遮断 ● フィッシングメール
2016年	リオデジャネイロ（ブラジル）	5億件	● ネットワーク遮断 ● 大会公式ウェブサイトへの攻撃 ● 組織委員会の情報窃取 ● 大会関連サイトを利用したフィッシング詐欺 ● 大会関連組織（政府，警察，銀行等）への攻撃による，個人情報の窃取
2014年	ソチ（ロシア）	1万4千件超	● 競技場スクリーンの改竄 ● 大会データの窃取
2012年	【デジタル化※開始】ロンドン（英国）	2億5千万件	● 大会の工事事業者への攻撃による工事の遅延 ● 電力供給システムへの攻撃 ● 通信妨害 ● 大会公式ウェブサイトへの攻撃 ● チケット販売を悪用した攻撃 ● フィッシングメール ● 不正アクセス
2010年	バンクーバー（カナダ）	不明	● フィッシングメール

※ここでいう「デジタル化」とは，チケットのオンライン販売や競技のインターネット配信，会場のネットワーク整備，オリンピック専用モバイルサービス等を指す。

[5] GOV.UK (2020)およびDOJ (2020). なお，米国司法省は2020年10月15日に，2015年から2019年にかけて，ロシアの国益のために様々な国の政府・企業・イベント等を狙ったサイバー攻撃に関与したとして，GRUのメンバー6人を起訴した。

[6] NISC（2019）11頁。

の妨害を狙った攻撃を仕掛けていたということが2020年10月19日に発表され[7]，サイバー攻撃の脅威が身近に差し迫っていることが広く知られるようになった。

東京五輪の開催にあたり，わが国では既に，内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）[8]内の組織である東京2020グループが中心となって，「リスクマネジメントの促進」および「対処態勢の整備」への取組を推進している[9]。この取組の対象者は，大会の運営に大きな影響を及ぼし得るサービス事業者とされており，電力の安定供給の確保も重要課題の一つであるため，電気事業者も対象に含まれている。さらに，日本シーサート協議会（NCA：Nippon Computer Security Incident Response Team Association）[10]は，従来から会員間で開催していたサイバーセキュリティ演習に加えて，東京五輪でサイバー攻撃を受けた場合に備えた演習を2019年11月に行った。その翌月には，電力ISAC（JE-ISAC：Japan Electricity Information Sharing and Analysis Center）[11]が，大会期間中に電力設備がサイバー攻撃を受けたことを想定した演習を行っている。また，経済産業省では，「電力サイバーセキュリティ対策会議」を2020年2月に開催した。同会議では，電力会社11社[12]の社長で構成する「電力サイバーセキュリティ対策委員会」の設置が決定され，大会期間中の電力の安定供給確保のために，サイバー攻撃に備えることになった。このように，東京五輪が成功するよう，電気事業者も精力的にサイバーセキュリティ対策を行っている。しかしながら，関係する組織間での横断的な連携が取られている一方で，有事対応の際の旗振り役となる社内の意思決定機関の設定については各社に対応が任されているため，問題発生後に素早く方針を決定・実行できる意思決定機関の組成が必要である。

2.2 社会インフラに対する最近の攻撃傾向

これまで，電気事業をはじめとする社会インフラのサイバーセキュリティ対策は，企業内における情報系技術（IT：Information Technology）のネットワークがメインであり，エアギャップ[13]で外部ネットワークと隔離されている制御系技術（OT：Operational Technology）のネットワークはセキュリティ対策が不要とされていた。しかし，昨今のDXによって，ITとOTのネットワークが統合されるようになり，OTも外部ネットワークに繋がるようになったため，セキュリティ対策が必要となった。最近では，サイバー攻撃の対象がITからOTに変化しており，世界におけるOT関連の攻撃数は2018年以降2000%以上増加し，今後も増加し続けることが予測されている[14]。

電気事業者について言えば，OTはシステムの要であり，監視制御システム（SCADA：Supervisory Control And Data Acquisition）[15]や産業用制御システム（ICS：Industrial Control System）[16]が運用されることで電力設備が動いている。つまり，ICSやSCADAの停止は電力供給に直結するため，供給

---

[7] GOV.UK (2020).

[8] ITの急速な発展と普及に伴うサイバーセキュリティの確保を目的とした「サイバーセキュリティ基本法」が2014年に成立したことに基づき，2015年に内閣官房に設立された。

[9] NISC (2020) 。

[10] NCAは，CSIRT同士が連携してセキュリティリスクに対応することを目的として，2007年に設立された。会員数は2020年1月現在400社超であり，電力会社からは東京電力ホールディングス（東京電力HD），中部電力，北海道電力が参加している。詳細はウェブサイト（https://www.nca.gr.jp）を参照のこと。

[11] 電気の安定供給に貢献するために，電気事業者間でサイバーセキュリティに関する脅威情報等を共有・分析し，適切・迅速に対応することを目的として，2017年3月に設立された組織である。会員は，電気事業者やその関係機関に加え，サイバーセキュリティについて技術・知識を有する法人で構成されている。会員間だけでなく，海外のインフラ事業者や海外のISAC（欧州はEE-ISAC，米国はE-ISAC）とも連携し，セキュリティ関連の情報共有を行っている。

[12] 北海道電力，東北電力，東京電力HD，中部電力，北陸電力，関西電力，中国電力，四国電力，九州電力，沖縄電力，電源開発。

[13] 内部ネットワークのセキュリティの安全を高めるために，インターネット等の外部ネットワークと接続する機器から物理的に隔離すること。

[14] IBM（2020）6-7頁。

[15] SCADAとは，異なる地点に置かれたセンサーからデータを収集し，そのデータをICSに送信するシステムである。電力業界においては，送電線や変電所等を流れる電力量・経路を監視し，変電所の機器を制御する役割を担う。

[16] ICSとは，SCADAを含む，物理的な産業プロセスの管理・制御をする技術やシステムのことで，電力業界では，発電や送電，検針の処理に利用されている。

の停止によって，企業の経済活動に大きな影響が及ぶだけでなく，一般の人々の生活に支障を来し，生命にも影響が及ぶ惧れがある。特に，電力業界をはじめとする重要インフラに対する攻撃では，国家自体に影響を及ぼすための「兵器」としてマルウェアが使われる傾向にあり[17]，その際に利用されるマルウェアが，電力用の制御システムに特化した「Industroyer[18]」である。同マルウェアが社内ネットワークに侵入することで，SCADAの監視する制御装置に直接働きかけることが可能となり，物理的な被害を生じさせる。

さらに，米国の電気事業者を対象にしたサイバー攻撃について，攻撃者や攻撃の目的を分析したレポートによると，これまでの攻撃者には個人ハッカーやハクティビスト[19]，競合他社が多く，金銭や顧客データの窃取，事業運営の妨害といった目的で攻撃を行うことが多かったが，近年では，組織犯罪グループや国家組織，内部・外部関係者といった攻撃者が，これまでの目的に加え，重要インフラの破壊や人命・安全への脅威等の目的でサイバー攻撃を仕掛けるようになっている[20]。

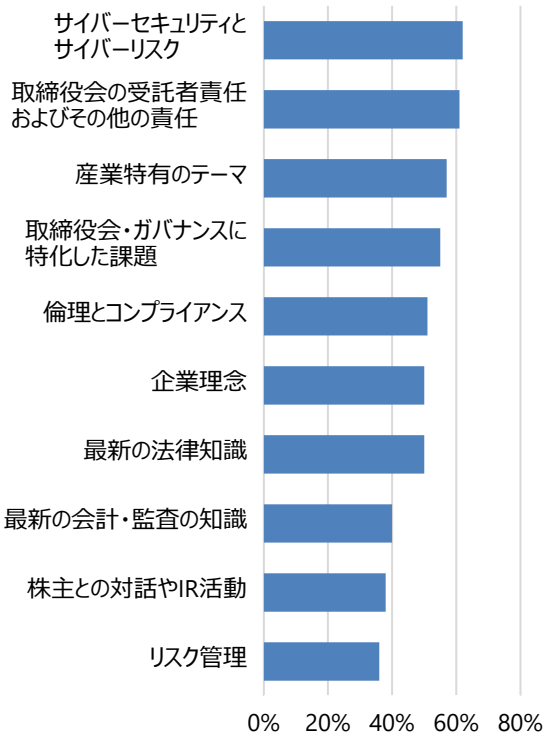
このように，社会インフラに対するネットワークを通じた攻撃が日々巧妙になっていることから，攻撃を防ぐための予防的対策や，攻撃を受けた際の対応の検討・意思決定を迅速に行うことのできる組織体制を整えておくことが重要である。

3. 海外のサイバーセキュリティ対策の組織体制

次に，国外企業がセキュリティリスクに対応するためにガバナンス上で行った取組について，その実態を明らかにした。

3.1 取締役会における議論の実態

企業によっては，取締役会で建設的な議論を行うために，就任前や就任後，必要に応じて取締役に対して研修を行い，必要な知識を習得する機会を設けている。図1は，様々な国の取締役が実際に受けている研修で，テーマとして取り入れられている項目とその割合を示している。僅差ではあるが，「サイバーセキュリティとサイバーリスク」が最も多く，取締役が学ぶべき重要なテーマであることが確認できる。つまり，取締役にはサイバーセキュリティ関連の知識の向上が求められており，セキュリティの議論に対応できることが期待されている。また，米国企業の取締役を対象とした，「取締役は何にもっと時間を費やすべきか？」という質問への回答では，12項目の選択肢のうち，サイバーセキュリティ等を含む「IT関連リスク」が2番目に多く挙がっており，取締役自身も，取締役会におけるセキュリティリスク対応の重要性



出典：Deloitte & SOCIETY (2019) をもとに当所にて作成

図 1　取締役の研修事項

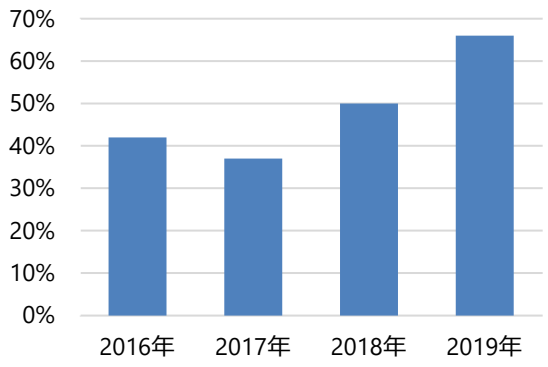
[17] Ponemon & Siemens (2019), p. 13.
[18] Crashoverride とも呼ばれる。本稿 3.3.1 で紹介するウクライナのサイバー攻撃に使用されている。
[19] 「ハッキング」と「アクティビスト」を組み合わせた造語。政治的・社会的な主張をするために過激なサイバー活動を行うハッカーを指す。有名なハクティビスト集団として「Anonymous」があり，何かしらの目標を持ったうえで政府機関や多国籍企業等のウェブサイト等に DDoS 攻撃を仕掛け，運営側に障害を生じさせるといった活動をしている。
[20] Deloitte（2019）3 頁。

を感じている[21]。取締役のセキュリティ対応の重要性に関しては，世界経済フォーラム（WEF）[22]でも言及しており，電気事業者の取締役に対し，サイバーセキュリティへの率先した取組を呼びかけている。その理由として，セキュリティリスク対策という新たな文化を社内に浸透させ，それに対応するための変化を社内にもたらすことは，取締役にしかできないという点を挙げている[23]。

以上から，取締役会ではサイバーセキュリティの議論が必要とされており，取締役はその重要性についても認識していることが分かる。

このような中，建設的な議論に向けた取組として取締役会でサイバーセキュリティに関する情報の説明を徹底した企業では，取締役が自社のセキュリティ対応について自信を示すようになっている。

図2は，米国内企業の取締役を対象にした，「自社はサイバーセキュリティについて適切な対策がなされていると思うか？」という質問に対し，「自信がある/とても自信がある」と回答した割合の2016年以降の推移を表したものである。図中で



出典：NACD (各年) をもとに当所にて作成

図 2　自社のサイバーセキュリティ対応への取締役の自信度の推移

は2017年以降に自信度が高まっており，その理由について，世界中の取締役を会員に持つ全米取締役協会（NACD：National Association of Corporate Directors）[24]は，取締役に対する説明の徹底のために，報告手法や透明性の強化を行ったことが一因であると見ている[25]。取締役に対するこのような取組の一つとして，CISO（Chief Information Security Officer）の活用が挙げられる。

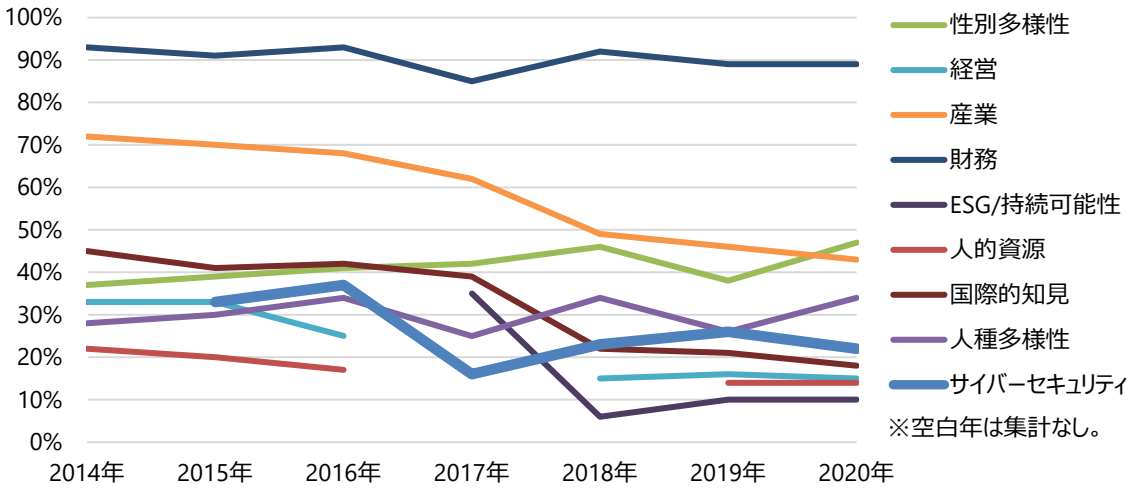
3.2 取締役会におけるCISOの重要性

米国では，情報システムのセキュリティに責任を負う，CISOやCIO（Chief Information Officer），CSO（Chief Security Officer）といった役職（以下，「CISO等」という）がある。これらはわが国ではあまり聞き慣れない役職であるが，既にわが国でも広く知られているCEO（Chief Executive Officer）やCOO（Chief Operating Officer），CFO（Chief Financial Officer）のように，CxOと表記される役職の一つとして，米国企業の中で重要視されている。これまでの取締役会では，サイバーセキュリティ関連の議論を行わなければならない取締役が問題点についてしっかり理解できているのかが懸念されていた。しかし今では，CISO等を採用している企業の多くで，取締役会でのセキュリティ関連の報告や説明をCISO等に任せており[26]，これによって，取締役会でのセキュリティ関連の議論が深まっていると考えられている。

図3は，2014年から2020年にかけて，世界中の取締役を対象に，取締役に求められる専門性について調査した結果の推移である。回答として選択できる項目は各年で少しずつ異なり，時代を反映して新たに設けられたものもある[27]。全ての期間において，経営の要である「財務」に関する知識が

---

[21] PwC (2015) 11 頁。
[22] WEF は，官民間の連携を通じて世界情勢の改善に取り組むべく，1971 年に設立された国際的な非営利財団である。同組織は，世界中のビジネス界・政界・学界から構成されており，毎年，世界や地域，産業毎の課題を設定し，戦略を検討している。
[23] WEF (2020), p. 7.
[24] 1977 年に設立され，現在は 2 万 1,000 人超の会員を持つ。同組織では，取締役のパフォーマンスを向上させるために，取締役に対する教育を行っている。
[25] NACD (2020), p. 19.
[26] Fortinet (2019), p. 6 によると，2019 年 1 月から 2 月にかけて行った調査では，CEO または取締役会に CISO 等が直接報告している企業が 63%あり，多くの企業でセキュリティ関連の報告を CISO 等が行っていることを示している。
[27] 図に表示していないが，ほかにも「IT 戦略」や「法律」という項目がある。「IT 戦略」は「サイバーセキュリティ」とほぼ同様の動きであり，「法律」は 20%前後を横ばいに推移している。



出典：PwC (各年) をもとに当所にて作成

図 3　取締役に求める専門性の推移

求められるのは勿論のこと，ここ数年で注目されるようになった「性別多様性」や「人種多様性」への知識が求められる傾向にある。2015年以降は，これまで取締役にとって不可欠であると思われていた「経営」の知識よりも，「サイバーセキュリティ」に関する知識の方が，取締役に求められる専門性として高い割合を示している。また，世界中の企業のCEO 1,300名に対して行った調査によれば，59%のCEOが，企業における最も重要な役職として，サイバーセキュリティの専門家を挙げている[28]。このことから，これからの取締役会メンバーには，経営の知識以上に，セキュリティ関連の知識を有する人物も求められることが分かる。

そこで，今後どのようにして取締役会にCISO等を取り込むかが課題となる。先述のとおり，CISO等の役割はサイバーセキュリティの対応であるため，セキュリティに関する技術的な専門性を有することは当然であるが，取締役会メンバーとする場合，上記専門性に加えて，それを企業の中で運用するスキルやリーダーシップも持ち合わせている者を探さなければならない。

3.3 ガバナンスの再構築による対応事例

ここでは，国外の電気事業者がセキュリティ対策を強化するために行ったガバナンスの再構築について，3件の事例を紹介する。

3.3.1 DTEK

2015年から2017年にかけて，ウクライナ国内の複数の電気事業者がサイバー攻撃を受けた。攻撃の手口として，電力会社に対し関係者を装ったフィッシングメールを送る，あるいは，不正に入手した資格情報を利用することで，社内ネットワークに侵入し，制御システムを操作して停電を発生させたとみられる[29]。ほかにも，原子力発電所の放射線モニタリングシステムに攻撃が仕掛けられ，発電所自体のシステムに実害は生じなかったものの，モニタリングシステムが機能しなくなり，現場が混乱するという事象が発生した[30]。

これらの攻撃に関する詳細な情報や，それによるガバナンスの見直しについては，いずれの電気事業者からも公表されていないが，2017年に攻撃を受けたウクライナ最大手の総合エネルギー事業者DTEKでは，その翌年からデジタル関連の取組を促進している。例えば，2019年にはDX部門長を経営層に取り込むとともに，サイバーセキュリ

[28] KPMG（2018）。
[29] CISA (2018).
[30] Reuters (2017).

ティを含むデジタル化関連の複数のプロジェクトを開始した[31]。

この事件を皮切りに，インフラへの攻撃手段の一つになるとして，サイバー攻撃に対する関心が世界中で高まり，電力会社はサイバーセキュリティ対策に注意を払うようになったとみられている。

3.3.2 CMS Energy

CMS Energyは，1886年に米国ミシガン州に設立されたエネルギー会社であり，電力・ガスの小売事業を行うConsumers Energyと，独立発電事業を行うCMS Enterprisesを子会社に持つ。

同社では，以前はサイバーセキュリティに特化した取締役を置いていなかった。しかし，スマートグリッドの普及によるセキュリティ脅威の増加や，トルコ人を装った中国人組織による社内サーバーへの膨大な量の攻撃が検出されたことで，サイバーセキュリティへの懸念が増大した[32]。そこで同社では，取締役会でセキュリティ関連のリスクを説明することができる人物を求めるようになった。その結果，セキュリティの専門家として様々な産業でセキュリティについて指揮した経験を有するMyrna Soto氏を，2015年から取締役として起用することにした。

一方で，同社取締役となったSoto氏によれば，取締役会にサイバーセキュリティに強い人物がいるからとはいえ，社内のセキュリティ関連のリスク対応を一手に引き受けるのではなく，その専門性を活かして，専門外である他の取締役が議論を進めていけるように先導することが必要であると述べている[33]。

3.3.3 Enel Group

イタリアの多国籍エネルギー企業であるEnelは，サイバーセキュリティ対策として，2016年にサイバーセキュリティ部門を設立している。設立の目的として，対応の速さが必要な事象が生じた際に，合理的かつ柔軟な意思決定ができるようにすることを挙げている[34]。また，2018年には，セキュリティ戦略の提案や承認を行い，その進捗を監督するために，Cyber Security Risk Committeeを設け，取締役であるCEOが議長を務めた。

ところが，2020年6月7日にマルウェア（ランサムウェア）SNAKE（別名EKANS）の攻撃を受けた[35]。同社の報告によると，当該攻撃で社内ネットワークに影響が及び，顧客対応のためのITサービスの質が一時的に低下したものの，発電所の運転には影響がなく，重大な問題は生じなかった[36]。

4. わが国のサイバーセキュリティ対策の動向

以上のように，海外ではセキュリティリスクへの対応として，CISO等の経営層への取込や，ガバナンスの再構築を行っていることが明らかとなった。そこで以下では，わが国のセキュリティ対応の現状と政策の動向を示す。

4.1 取締役会での議論とガバナンスの実態

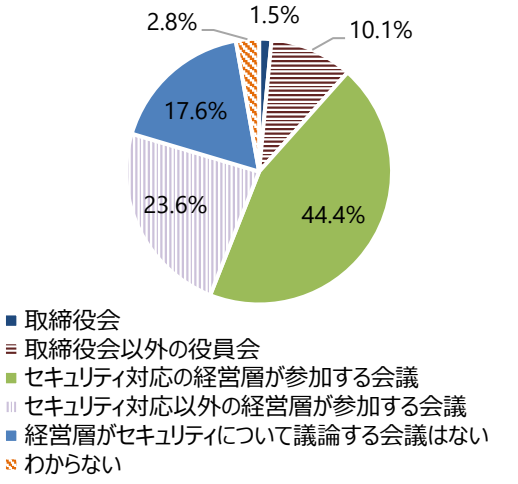
CISO等を任命している日本国内企業を対象とした調査によると，サイバーセキュリティに関する議論を行う会議体は図4のとおりである。セキュリティ関連の議論が行われるのは，「セキュリティ対応の経営層が参加する会議」が最も多く，次いで，「セキュリティ対応以外の経営層が参加

[31] DTEK (2019).
[32] CTN (2013).
[33] Forbes (2019).
[34] Enel (2017), p. 145.
[35] わが国でも翌6月8日に，自動車メーカーである本田技研工業が，同マルウェアの攻撃を受けている。この攻撃により，メールや内部のサーバーへの接続に障害が発生し，日本だけでなく海外の事業にも影響が及び，国内外の工場で生産・出荷が停止するといった被害が生じた。当該攻撃に関する詳細は不明だが，NYTimes (2020) によれば，マルウェアは社内ネットワークを通じて侵入しており，しかも，マルウェア自体を同社用に作成して標的を絞っていたと見られることから，同社のデータや個人情報の窃取を目的とするのではなく，工場等の制御系システムを狙った攻撃であったと推測されている。また，本件について，Forbes (2020) では，新型コロナウイルスの世界的流行の影響で在宅勤務になったことに起因する可能性も示唆している。
[36] Enel (2020), p. 27.

する会議」が多いことから，経営層が参加する会議でのセキュリティの議論が過半数を占めている。一方で，「取締役会」が最も少ないことや，「経営層がセキュリティについて議論する会議はない」が17.6%であることから，経営層全体での議論の機会が少ないことが分かる。そこで次に，わが国の企業による，ガバナンス上でのサイバーセキュリティ対応について見る。

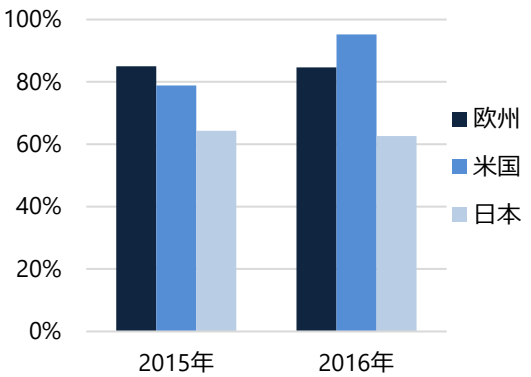
わが国では，情報システムや情報セキュリティに関する責任者は，IT部門の部長が担うことが多く，CISO等のような，企業全体の情報セキュリティ対策を統括する役職を設けている企業は，欧米と比較すると少ない（図5）。2015年から2016年の日米欧のCISO設置率推移を見ても，米国は約17%増加しており，CISOの拡充が更に強まっているのに対し，わが国では大きな変化が見られない。また，図6は，経営層がCISOに就任している割合について，日米に加え，英国，シンガポール，豪州の比較を表したものである。海外ではその割合が高いが，わが国は海外のおよそ半数であり，経営層のセキュリティ対策への関与が低い。

国内企業のCISOに対して，現在社内で重視されている自身の役割を調査した結果を示したのが図7である。これによれば，CISOが社内で実際に担っている役割は，「経営層との橋渡し」が一番多く，次に僅差で「セキュリティ対策の推進」が挙がった。「経営層との橋渡し」とは，リスクの洗い出しだけでなく，経営層に対し，問題が生じた際



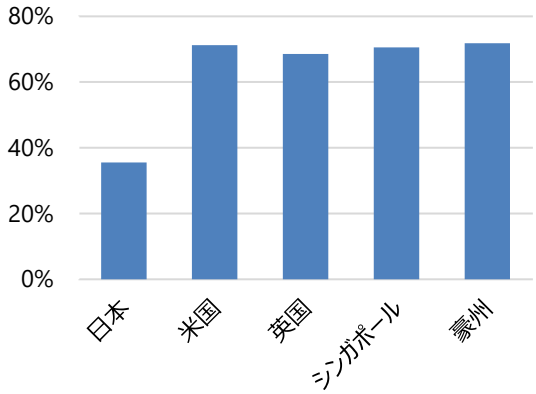
出典：IPA (2020) をもとに当所にて作成

図 4　サイバーセキュリティが議論される会議体



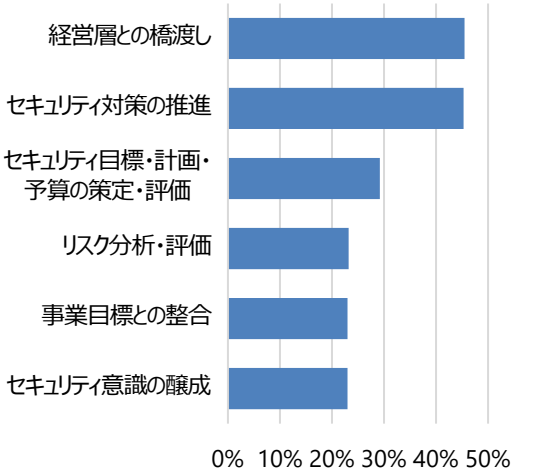
出典：IPA (2017) をもとに当所にて作成

図 5　日米欧におけるCISOの設置状況の推移



出典：NRI (2018) をもとに当所にて作成

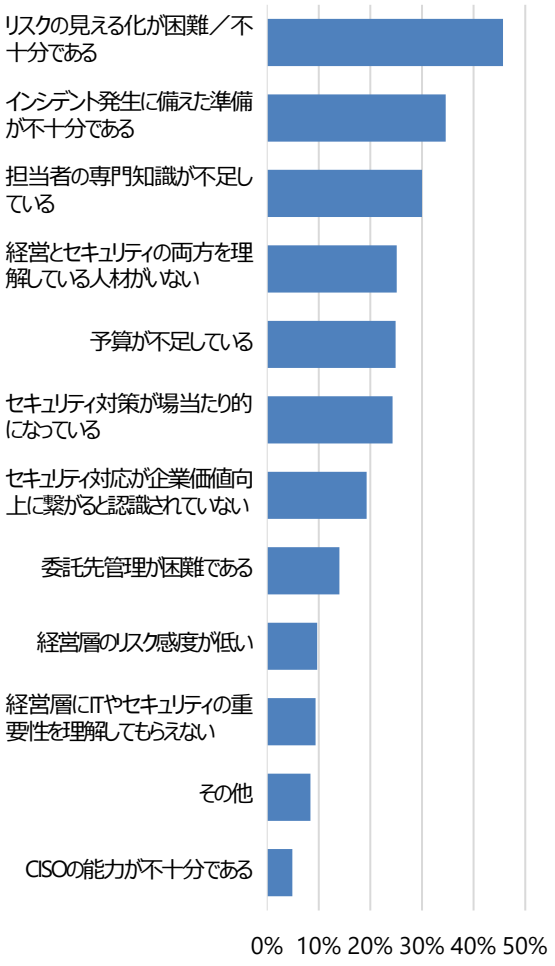
図 6　経営層に就任しているCISOの割合



出典：IPA (2020) をもとに当所にて作成

図 7　重視されているCISOの役割（上位5位）

の状況説明からその対応策の提示等，専門的な知識に基づく説明を行ったうえで，その提示した対応を実行するか否かの意思決定を諮るまでを指す。これに対し，CISO等を任命する国内企業がセキュリティについて認識している課題は，図8のとおりである。CISOを採用していることもあって，経営層におけるリスク感度やセキュリティの重要性の理解度の低さに関する課題は少なかったが，「担当者の専門知識が不足している」や「経営とセキュリティの両方を理解している人材がいない」といった課題が3位と4位に挙がっており，CISOを採用していてもなお，セキュリティに関する知識やそれを経営に活かすことが課題となっていることが分かる。



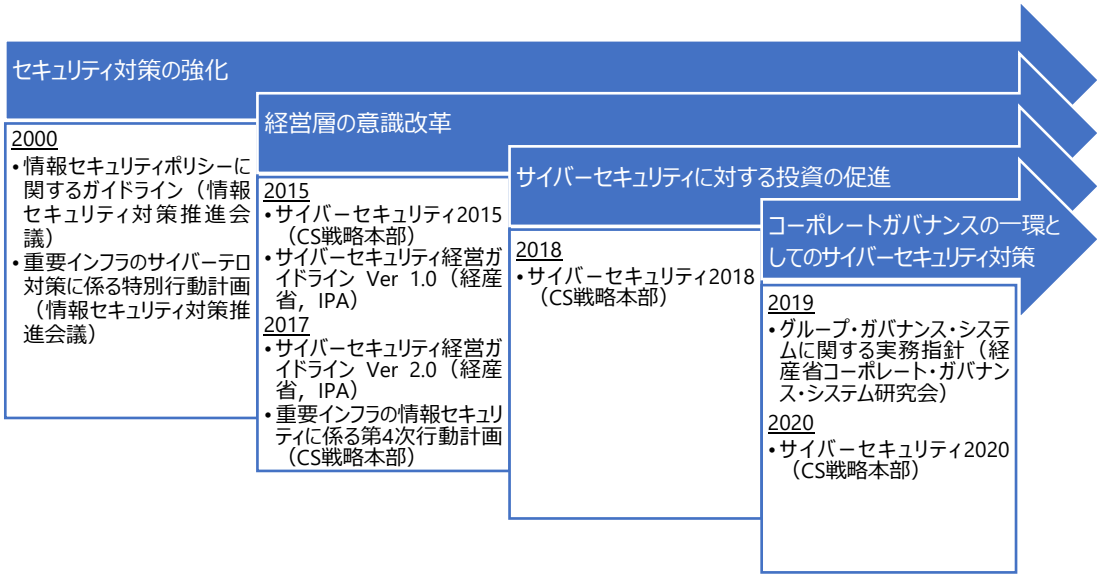
出典：IPA (2020) をもとに当所にて作成

図 8　サイバーセキュリティに関する課題認識

4.2 対策に向けた動き

企業のサイバーセキュリティ対策を促進するための政府の動きを表したのが，図9である。わが国の政府は，セキュリティ対策を強化させるために内閣官房情報セキュリティ対策推進室を2000年に設置して以降，様々な取組を進めてきた。

国による具体的な施策は，内閣のサイバーセキュリティ戦略本部（以下，「CS戦略本部」という）が2015年に策定した年次計画「サイバーセキュリ



出典：NISC各資料をもとに当所にて作成

図 9　企業のサイバーセキュリティ対策促進に向けた政府の取組の動き

ティ2015[37]」に始まる。同計画には，経営層がサイバーリスクを経営上の最重要課題として認識し，セキュリティ対策に積極的に関与することを促進するための取組として，「経営層の意識改革」が盛り込まれた。上記取組の推進のために，経済産業省と独立行政法人 情報処理推進機構（IPA：Information-technology Promotion Agency）[38]が共同で，経営層が認識すべき事項をまとめた指針である「サイバーセキュリティ経営ガイドラインVer 1.0」を策定した。改訂版のVer 2.0では，セキュリティ対策を，コストではなく投資であると位置付け[39]，経営者のより一層のセキュリティ意識向上を促している。また，電力を含む重要インフラを対象にした「重要インフラの情報セキュリティ対策に係る第4次行動計画[40]」もSC戦略本部で策定されており，セキュリティへの認識を高めるよう，経営層の在り方について具体的に示している。

2018年には，既出の「経営層の意識改革」に加え，更なる取組として，「サイバーセキュリティに対する投資の推進」がサイバーセキュリティ2018[41]に盛り込まれた。同取組は，市場で評価されるようなセキュリティ対策を，経営層が継続的に講じることを目的とする。具体的には，セキュリティへの自社の対応状況についての情報発信・開示や，セキュリティ対策製品の導入，セキュリティ保険の活用が，セキュリティに対する投資の取組例として示されている。

最近では，新しい取組として，「コーポレートガバナンスの一環としてのサイバーセキュリティ対策」が策定された。これは，サイバーセキュリティ2019[42]の計画に基づいて経済産業省のコーポレート・ガバナンス・システム研究会が策定した，「グループ・ガバナンス・システムに関する実務指針[43]」で示されており，自社内だけに留まらず，関連する企業全てのセキュリティ対策に取締役が取り組むよう求めている。同指針を踏まえてこの新しい取組を後押しすることが，サイバーセキュリティ2020[44]で決定されている。

以上のような政府を中心とした動きのほかにも，非営利団体 JCERTコーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）[45]やIPAが，国内のセキュリティ対策の向上を目的とした取組を行っており，両者が連携して，脅威となる最新のセキュリティ情報についての注意喚起，ソフトウェアの脆弱性やその対策情報を提供している。特に電力等の重要インフラについては，優先的に情報を提供する旨が「情報セキュリティ早期警戒パートナーシップガイドライン[46]」にて定められている。

上記のとおり，現在わが国の電力業界では，セキュリティ対策を推進するために，政府が中心となって，電力業界全体での取組を推進するための施策を提示している。しかしながら，経営層の対応の必要性や具体的な取組についての方策が示されるようになったのは，ここ数年である。ゆえに，近い将来，経営者には，セキュリティ対策の重要性やデジタル化の必要性の理解，対策への率先的な取組が当然に求められるようになると考えられる。

5. おわりに

電気事業のデジタル化が進んでいる今，サイバー攻撃等のサイバーセキュリティリスクが高まっており，有事の際に迅速に対応できる体制を整

[37] NISC（2015）。セキュリティ戦略の年次計画として毎年発表されている。
[38] 2004年に，経済産業省所管の政策実施機関として，情報セキュリティの強化や，IT 人材の育成のための活動を行うために設立された。
[39] 経産省（2017）1頁。
[40] 第4次行動計画（2017）。2000年に策定された「重要インフラのサイバーテロ対策に係る特別行動計画」に始まる。
[41] NISC（2018）。
[42] NISC（2019）。
[43] 経産省（2019）。「サイバーセキュリティ2019」で，コーポレート・ガバナンスの一環としてセキュリティ対策を位置付けたことを受けて策定された。
[44] NISC（2020）。
[45] 1996年に，コンピュータ緊急対応センター（JCERT）として，サイバー関連情報の海外との連携や，国内でのセキュリティ上の問題の情報発信をするために設立された。
[46] IPA ほか（2019）。

えておく必要がある。そこで本稿では，わが国の電気事業のセキュリティリスクに対する「守りのガバナンス」の構築について検討すべく，海外の取組や対応事例に関する実態を整理した。

その結果，海外ではセキュリティ対策について，取締役会でもその重要性を認識しており，取締役会の議論の充実のためにCISOを活用するだけでなく，経営層にCISOを取り込むことでガバナンスの強化を図っていることが明らかとなった。

一方でわが国では，取締役会におけるセキュリティ対策への取組についての必要性は理解されているが，海外に比べてCISO等の役職自体の普及が進んでおらず，取締役会でのセキュリティ関連の議論の実施についても改善が必要な状況にある。そのような状況に対し，セキュリティ対策への取組を進めるべく，政府を中心とした様々な施策が進められている。最近では，政府が中心となって経営層の認識を高める施策が設けられたことから，今後は，経営層のセキュリティ対策に関する積極的な取組や議論の充実化が期待される。加えて，2021年には東京五輪の開催が予定されていることから，電気事業者におけるセキュリティ対策については，より強固な取組が必要となるであろう。

電気事業者をはじめとする重要インフラには，サイバー攻撃等の問題発生時に，その原因を理解し，より良い解決策を議論したうえで，それを実行する，という一連の行動が迅速にできるガバナンス体制の整備が必要である。そこで，とるべき体制として，本稿で言及した「CISO等の経営層への取込」がその一案として考えられる。

ただし，その有用性の検証は行われていないため，その体制が実際に機能するのか，そして，有効に機能させるためにはどのようにすべきかといった実効性評価については，今後の研究課題としたい。

【参考文献】

※ウェブサイトの最終閲覧は全て2020年11月5日。

CISA (2018) : Cybersecurity and Infrastructure Security Agency, *Cyber-Attack Against Ukrainian Critical Infrastructure*, IR-ALERT-H-16-056-01, Aug. 23, 2018, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

Convene (2017)：Azeus Convene, *Combating Cybersecurity Risks in the Boardroom*, 2017, https://www.azeusconvene.com/wp-content/uploads/white-papers/CCRB-whitepaper_Bv01.pdf

CTN (2013)：CIO Talk Network, Cyber Warfare: *A New Enemy for Utilities*, 2013, https://www.ciotalknetwork.com/cyber-warfare-a-new-enemy-for-utilities/

Deloitte（2019）: Deloitte「電力業界のサイバーリスク経営　サプライチェーンと制御システムに対する脅威の高まり」（2019）＜https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/energy-resources/er/jp-er-managing-cyber-risk-2.pdf＞

Deloitte & SOCIETY (2019)：Deloitte and SOCIETY for Corporate Governance, *Board Practices Report,* 2019

DOJ (2020)：U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, Oct. 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

DTEK (2019)：DTEK, *DTEK to Invest UAH 350 Million in the Digital Transformation of Its Business in 2019*, Apr. 16, 2019, https://dtek.com/en/media-center/press/dtek-to-invest-uah-350-million-in-the-digital-transformation-of-its-business-in-2019/

Enel (2017)：Enel, *Sustainability Report 2016,* Apr. 2017, https://www.enel.com/content/dam/enel-com/documenti/investitori/sostenibilita/2016/sustainability-report_2016.pdf

Enel (2020)：Enel, *HALF-YEAR FINANCIAL REPORT*, Jun. 30, 2020, https://www.enel.com/content/dam/enel-com/documenti/investitori/informazioni-finanziarie/2020/interim/en/half-year-financial-report_30june2020.pdf

EY (2020)：EY「EY グローバル情報セキュリティサーベイ 2020」（2020 年 5 月 1 日）

Forbes (2019)：Forbes, *Corporate Boards Are Snatching Up Cybersecurity Talents*, Aug. 30, 2019, https://www.forbes.com/sites/chenxiwang/2019/08/30/corporate-boards-are-snatching-up-cybersecurity-talents/#76c51514479f

Forbes (2020)：Forbes, *Honda Hacked: Japanese Car Giant Confirms Cyber Attack On Global Operations*, Jun. 10, 2020, https://www.forbes.com/sites/daveywinder/2020/06/10/honda-hacked-japanese-car-giant-confirms-cyber-attack-on-global-operations-snake-ransomware/#2d12f4ee53ad

Fortinet (2019)：Fortinet, *The CISO and Cybersecurity: A Report on Current Priorities and Challenges*, Apr. 26, 2019, https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-ciso-and-cybersecurity.pdf

Gov.UK (2020)：GOV.UK, Press release, *UK exposes series of Russian cyber attacks against Olympic and Paralympic Games*, Oct. 19, 2020, https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

IBM (2020) : IBM Security「IBM X-Force 脅威インテリジェンス・インデックス 2020」（2020 年 2 月）

IPA（2017）: IPA「企業の CISO や CSIRT に関する実態調査 2017」（2017 年 4 月 13 日）

IPA (2020)：IPA「企業の CISO 等やセキュリティ対策推進者に関する実態調査」（2020 年 3 月 25 日）

IPA ほか (2019) : 情報処理推進機構ほか「情報セキュリティ早期警戒パートナーシップガイドライン」（2019 年 5 月）

KPMG (2018)：KPMG, *P&U CEOs are confident growth is on the horizon*, Nov. 14, 2018, https://home.kpmg/za/en/home/insights/2018/09/2018-kpmg-ceo-outlook-power-and-utilities.html

NACD (各年)：National Association of Corporate Directors, Public Company Governance Survey, 2017-2020.

NISC (2015) : サイバーセキュリティ戦略本部「サイバーセキュリティ 2015」（2015 年 9 月 25 日）＜https://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf＞

NISC (2018) : サイバーセキュリティ戦略本部「サイバーセキュリティ 2018」（2018 年 7 月 25 日）＜https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf＞

NISC (2019) : サイバーセキュリティ戦略本部「サイバーセキュリティ 2019」（2019 年 5 月 23 日）＜https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf＞

NISC（2020）: 内閣サイバーセキュリティセンター 東京 2020 グループ「東京 2020 大会に向けた取組の実施状況について」(2020 年 10 月 26 日) ＜https://www.nisc.go.jp/conference/cs/ciip/dai23/pdf/23shiryou05.pdf＞

NRI (2018) : NRI SECURE「NRI Secure Insight 2018 企業における情報セキュリティ実態調査」＜https://www.secure-sketch.com/hubfs/e-book/NRISecure_Insight2018_Report.pdf＞

NRI (2019) : NRI SECURE「NRI Secure Insight 2019 企業における情報セキュリティ実態調査」＜https://www.secure-sketch.com/hubfs/e-book/NRISecure_Insight2019_Report.pdf＞

NYTimes (2020) : The New York Times, Honda Hackers May Have Used Tools Favored by Countries, Jun. 12, 2020, https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html

Ponemon & Siemens : Ponemon Institute and Siemens, *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?*, Oct. 4, 2019, https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1599074232/siemens-cybersecurity.pdf

PwC (2015) ; PwC「取締役会では何が問題にされているのか」（2015 年 2 月）＜https://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/what-matters-in-the-boardroom1502.pdf＞

PwC (各年) : PwC, *Annual Corporate Directors Survey*, 2014-2020.

Reuters (2017)：Reuters, *Cyber attacks affect some radiation checks at Ukraine's Chernobyl site,* Jun. 28, 2017, https://www.reuters.com/article/us-cyber-attack-ukraine-chernobyl-idUSKBN19I2CI

Utility Dive (2020)：Utility Dive, *Enel ransomware attack highlights the value of a top-down security culture*, Jul. 8, 2020, https://www.utilitydive.com/news/enel-ransomware-attack-highlights-the-value-of-a-top-down-security-culture/581179/

WEF (2020) : World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers*, Jun. 2020

経産省 (2017) : 経産省・IPA「サイバーセキュリティ経営ガイドライン Ver 2.0」（2017 年 11 月 16 日）＜https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf＞

経産省 (2019) : 経産省「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」（2019 年 6 月 28 日）＜https://www.meti.go.jp/press/2019/06/20190628003/20190628003_01.pdf＞

第 4 次行動計画(2017) : サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2020 年 1 月 30 日改定）＜https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf＞

トレンドマイクロ（2019）: トレンドマイクロ「法人組織におけるセキュリティ実態調査　2019 年版」（2019 年 10 月 15 日）。

トーマツ（2017）: 監査法人トーマツ「取締役会の機能向上等に関するコーポレートガバナンス実態調査報告書」（2017 年 3 月）＜https://www.meti.go.jp/meti_lib/report/H28FY/000429.pdf＞

外﨑 静香（とのさき しずか）
電力中央研究所　社会経済研究所