INTERNET SECURITY ALLIANCE

サイバーリスクハンドブック

取締役向けハンドブック　日本版

Based on the National Association of Corporate Directors
Cyber Risk Oversight Director's Handbook and
Managing Cyber Risk : A Handbook for UK Boards of Directors

経団連
Keidanren

INTERNET SECURITY ALLIANCE

prepared by

Larry Clinton

President and CEO, Internet Security Alliance

and

Josh Higgins

Director of Policy and Communications, Internet Security Alliance

サイバーリスクハンドブック

取締役向けハンドブック　日本版

サイバー攻撃は、企業や各種組織が現在直面している脅威の中で、最も急激に増大しているとともに、おそらく最も危険な脅威である。企業の取締役会は、こうした脅威への対処をますます重視するようになってきている。しかしながら、サイバー攻撃の脅威は、その性格上絶えず変化するものであるため、各社は、この問題に取締役会レベルで対処するための一貫性のある方法を模索している。こうした状況を踏まえ、インターネット・セキュリティ・アライアンス（Internet Security Alliance: ISA）と全米取締役協会（National Association of Corporate Directors: NACD）は、2014年に『企業の取締役向けサイバーリスクハンドブック（Cyber Risk Oversight Director's Handbook）』（以下、「米国版ハンドブック」という）の初版を作成した。このハンドブックが出版されるとたちまち活用され、取締役会が世界中のサイバーリスクに対処するうえで役立つことが実証された。実際に、プライスウォーターハウスクーパース（PricewaterhouseCoopers: PwC）は、同社の『グローバル情報セキュリティ調査2016（2016 Global Information Security Survey）』で、同ハンドブックの名を挙げて、次のように記した。

> 「全米取締役協会（NACD）のガイドラインでは、サイバーリスクを企業全体の視点から捉え、潜在的な法的影響を把握するよう勧告している。サイバーセキュリティリスクや準備状況について話し合い、企業全体のリスク許容度に照らしてサイバー脅威を考える必要がある」
>
> 「各企業の取締役会はこの助言に耳を傾けているようだ。本年の調査では、情報セキュリティのほとんどの面で取締役の参加率が二桁の増加を示した。参加率が増加したことで、多くのサイバーセキュリティへの取組みが向上したという声が寄せられている。サイバーセキュリティ予算会議への取締役の参加率増加とともに、セキュリティ支出が24%増加したのは偶然ではないであろう」
>
> 「主なリスクの識別、セキュリティを重視する企業文化の醸成、全体のリスクマネジメントやビジネス目標とサイバーセキュリティの連携の強化なども注目すべき成果だとする回答が寄せられている。何よりも、ビジネスの問題として、サイバーセキュリティ部門と経営陣が意見を交わせるようになったことが功を奏したのだろう」[1]

1 PricewaterhouseCoopers (PwC), *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016* (PwC, 2015), web

ISAは米国版ハンドブックの国際展開に取り組んでおり、これまで、英国、ドイツ、ラテンアメリカ版を作成してきた。その経験から、各国・地域によってコーポレートガバナンスには違いがあり、従って取締役会の役割にも差があるものの、サイバーリスク管理について取締役会が果たすべき役割の原則部分は共通性が高く、国境を越えて当てはまるということが分かってきた。

この日本版は、こうしたISAの経験に基づき、経団連とISAが協力して作成したものである。日本版の作成に当たっては、米国版ハンドブックと英国版ハンドブック『Managing Cyber Risk: A Handbook for UK Boards of Directors』を参照し、米国および英国とわが国において取締役会が果たす役割の違いに留意した。すなわち、米国や英国企業では取締役会メンバーの多くは社外取締役で、業務執行を担う経営陣を監督する役目に特化している。他方、日本企業では取締役会メンバーが同時に業務執行を担うケースも多い状況にある。したがって、本書は企業経営において業務執行をする立場および業務執行を管理監督する立場（同じ人がある部門の業務執行を担いながら全社的視点からの管理監督に携わったり、その部門に所属する関連会社を管理監督したりする場合も含む）にある取締役の方々すべてを対象読者としている。

目　　次

サイバーリスクハンドブック
取締役向けハンドブック日本版の発行に寄せて

企業経営にとってサイバーセキュリティは重要な課題である。サイバー攻撃によって企業活動が妨げられ業務が停止すること、顧客情報を含む企業活動にとっての重要情報が漏洩し顧客や市場の信頼を失うこと、等々の極めて重大な経営上のリスクが日常的に存在する。しかもこれを完全に防ぐことは不可能であると認識せざるを得ない。

また、サイバーセキュリティの課題は年々深刻化してきている。会社のサイズやブランド力に関係なくサイバー攻撃にさらされる危険性がある。取り分けIoTの時代では企業間でリアルタイムの情報連携が取られてきており、そうした連携にサイバー攻撃の介入も想定され、リスクは一企業に止まらない。

この観点で、企業経営に責任のある取締役は、経営の場において如何にサイバーリスクに対処するかを真剣に議論し、方向付けを明確にし、対応する体制の整備や予算処置を講ずる必要がある。しかし一般的に取締役はサイバーセキュリティに関して技術面、実務面で詳しく承知していることは少ないと思われる。本ハンドブックには、取締役の方々が企業経営リスクへの対処策を検討、議論する際に考慮すべき事項が整理されている。また、実際に知っておかねばならない諸事項、リスクの最小化を図るのに資することが記述されている。

本ハンドブックは、経団連会員企業の全ての取締役の方々に一読頂き、サイバーリスクをどう認識していくか、更に、どう対処していくかを考え、行動に移していって頂くようにお願いする目的で、米国の『National Association of Corporate Directors Cyber Risk Oversight Director's Handbook』およびその英国版である『Managing Cyber Risk: A Handbook for UK Boards of Directors』をベースに作成したものである。

本ハンドブックが、全ての取締役の方々にとって、サイバーリスク管理に取り組む一助となれば幸甚である。

一般社団法人日本経済団体連合会

会長　中西　宏明

はじめに

過去25年間で、企業が保有する資産の性質は大きく変化し、物理的なものからバーチャルなものへと移行してきた。フォーチュン500（Fortune 500）企業の総資産価値の90%近くは、知的財産権（IP）やその他の無形資産で構成されている[2]。情報資産の「デジタル化」の急速な拡大に伴って、企業リスクの「デジタル化」も進んでいる。それとともに、政策立案者や規制当局、株主、一般市民の間でも、企業のサイバーセキュリティリスクに対する認識がかつてないほどに高まっている。企業は、IPや経営情報の喪失、データの破壊や改変、社会的信頼の低下、重要インフラにおける障害、罰則の強化といったリスクにさらされており、こうしたリスクの一つ一つが、競争力や株価、株主価値に悪影響を及ぼす可能性があるのである。

先駆的企業は、サイバーリスクを、他の重要なリスクと同じように、リスクと報酬のトレードオフという観点で捉えている。こうした考え方は、以下の二つの理由から、サイバー領域においてはとりわけ簡単ではない。第一の理由は、サイバー脅威の複雑さの劇的な高まりである。現在、企業は従来型の手法で防御しきれない高度な攻撃に直面している。攻撃の複雑さが高まるにつれて、企業にもたされるリスクも増大する。データ漏洩によってもたらされる潜在的影響は、情報の消失・破壊の場合よりもはるかに大きい。サイバー攻撃は、組織のレピュテーションやブランドに深刻な影響を与える可能性があり、データ消失自体よりも、そのタイミングや広報といった、より間接的な要因の方が大きな影響をもたらす可能性もあるからである。サイバー攻撃の結果、企業や取締役に法的リスクが生じる可能性もある。第二の理由は、コスト削減、カスタマーサービス向上、イノベーション推進を目的とする新技術導入へのモチベーションが、かつてないほど強くなっていることである。このように様々な、時に競合する圧力が、企業のスタッフやビジネスリーダーにかかっていることから、取締役会レベルでは入念かつ包括的な監督が不可欠である。すなわち、サイバーリスクがもたらす影響を管理・軽減するためには、IT部門の枠を超えた戦略的思考が必要となる。

経団連とISAは、米国版ハンドブックに示された以下の5つの原則は日本でも当てはまると考えている。

1. 取締役は、サイバーセキュリティを、単なるITの問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要がある。
2. 取締役は、自社固有の状況と関連付けて、サイバーリスクの法的意味を理解すべきである。
3. 取締役会は、サイバーセキュリティに関する十分な専門知識を利用できるようにしておくとともに、取締役会の議題としてサイバーリスク管理を定期的に取り挙げ、十分

2 Ocean Tomo, *"Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC"* (press release), Mar.5, 2015.

な時間をかけて議論を行うべきである。
4. 取締役は、十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべきである。
5. サイバーリスクに関する取締役会における議論の内容として、回避すべきリスク、許容するリスク、保険によって軽減・移転すべきリスクの特定や、それぞれのリスクへの対処方法に関する具体的計画等を含めるべきである。

ハンドブックの記述には非上場企業に言及している部分もあるが、上記原則は、全ての取締役に当てはまる内容であり、かつ、全ての取締役にとって重要である。どんな組織にも、サイバー犯罪者等の攻撃者からの脅威に常にさらされている貴重なデータや関連資産が必ず存在する。

急速に高まりつつあるサイバーの脅威の状況

ほんの数年前まで、サイバー攻撃は、主としてハッカーやごくわずかの高度な技術を備えた者たちが行うものであった。これらの脅威は問題ではあったが、多くの企業はビジネスをする以上避けて通れないコストであると考えることができた。

しかし、現在、企業は極めて高度に洗練されたチームによる波状攻撃にさらされている。こうしたチームは、システムや個人などのターゲットを絞り込み、マルウェアを悪用して、気付かれることなく、多段階にわたる攻撃を仕掛けてくる。APT攻撃（持続的標的型攻撃）とも呼ばれるこれらの攻撃は、当初は政府機関や防衛関連企業を狙って行われた。より最近では経済全体へと広がりつつある。言い換えれば、事実上全ての組織がAPT攻撃のリスクにさらされていることを意味する。

これらの攻撃を決定付ける特徴の一つとして、ファイアウォールや侵入検知システムなど、企業の周囲に張り巡らされた防御システムを、ほぼ全てすり抜けることができるという点が挙げられる。攻撃者は、目標を達成できるまで複数の手段を検討し、あらゆる層のセキュリティの脆弱性を突いてくる。本当に高度な能力を持つ攻撃者がある企業のシステムをターゲットとすれば、ほぼ間違いなく侵入できるというのが現実である。

加えて、不満を抱いていたり研修が不十分であったりするような従業員は、企業にとっては外部からの攻撃と同じくらいか、それ以上に大きなリスクとなりうる。こうしたことから、強力で適応力が高く、外部・内部からのサイバーの脅威に対して等しく強力な防御を提供する、バランスの取れたセキュリティ対策が必要となる。低レベルの攻撃が阻止できない組織は、より高度な脅威にも対処できない[3]。

3 Verizon RISK Team, et al., *2013 Data Breach Investigations Report*, March 2013.

ネットワーク接続の拡大に伴うリスクの増大

システム同士が相互に複雑に接続するようになったため、組織が自身のネットワークのみのセキュリティを確保するだけでは、もはや十分ではない。ベンダー、サプライヤー、パートナー、顧客など、企業とネットワークを介して接続された全ての組織・事業者が、潜在的に脆弱なポイントとなる可能性がある。例えばある大手石油企業の場合、高度な能力を持つ攻撃者は、同社のネットワークには侵入できなかったが、代わりに従業員に人気の中華料理店のオンラインメニューにマルウェアを忍ばせることによって同社システムへの侵入に成功した。ひとたび同社システムに侵入した段階で、侵入者は企業内部への攻撃が可能になったのである[4]。

従来型情報システムと、防犯カメラやコピー機、ゲーム機、自動車などの非従来型システム（いわゆる、モノのインターネット（IoT））との相互接続が拡大した結果、サイバー攻撃者が侵入できる可能性があるエントリーポイントの数が急増している。したがって、企業などの組織は、より広い視野でサイバーリスクを考える必要がある。2016年には「分散型サービス拒否攻撃（DDoS攻撃）」により、Twitter、PayPal、Netflixなど、1,000社以上の企業ウェブサイトへのアクセスが著しく制限された。この攻撃は、ハッカーたちによって、家庭用デジタルビデオレコーダーやウェブカメラなど、数十万台に及ぶ機器を悪用して行われたものだ[5]。

政府機関は、主として、国の重要インフラ（電力や水道、通信・交通ネットワークなど）をサイバー攻撃から守ることに力を注いできた。こうした攻撃は技術的に可能であり、極めて重大な影響を及ぼす可能性があるが、実際に起こっているインシデントの大半は、経済的な動機によるものである[6]。サイバー攻撃者は、顧客や従業員の個人情報、財務データ、事業計画、営業秘密、知的財産権など、あらゆる種類のデータを日常的に盗み出そうとしている。また、攻撃者が、企業などのデータを暗号化し、そのデータを言わば人質にとって身代金を求める手法、いわゆる「ランサムウェア」を用いることがますます増えている。2017年5月にはWannaCryという身代金要求型マルウエアが世界的な被害を引き起こしたが、日本でも自動車工場の操業停止などの被害が起きた。WannaCryは特定企業を狙わない、いわゆる「ばら撒き型」としてメールに添付されたマルウエアを実行させたり、ワームとしてネットワークに接続しているだけで感染したりするマルウェアであったため、どの企業・個人が被害者になってもおかしくなかったものである。サイバー犯罪の被害額を推定するのは難しい。しかし、米国において年間4,000～5,000億ドル以上に達するという見積りがある一方で、損失の大部分は気付かれないままとなっている[7]。米国におけるサイバー犯罪による損失は、2013年から2015年の間に5倍になり、2019年には年間2兆ドルを超える可能性がある[8]。

4 Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines" the *New York Times,* Apr. 7, 2014
5 Samuel Burke, "Massive cyberattack turned ordinary devices into weapons" CNNMoney.com, Oct. 22, 2016
6 Verizon, *2016 Data Breach Investigations Report*, p.7.
7 Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019" *Forbes*, Jan.17, 2016
8 Ibid.

数字で見るサイバー脅威

・35%の企業が外部からのサイバー攻撃に遭っており、うち約3割で実際に被害が発生している[9]。攻撃手法として最も多く挙げられるのはシステムの脆弱性を突かれたことによる不正アクセスで、次いでID・パスワードをだまし取られたことによるなりすましも多い[10]。ランサムウェア（身代金要求型ウィルス）についても35%の組織が被害経験を持つ[11]。

・不正アクセスやウィルスに関する警察への相談は増加しており、年間12,000件を超える[12]。不正なプログラムを添付したメールを送り付ける標的型攻撃は把握されているだけでも年間6,740件と、増加傾向にある。うち90%は多数の受信者に向けて送られる「ばら撒き型」であり、広範なターゲットが狙われていると言える[13]。

・産業別にみると、製造業への攻撃が24%で最も多い。製造業で検出された攻撃の約半数は侵入のための偵察活動である。続く小売業とテクノロジー業界への攻撃は近年増加傾向にある。金融機関に対する攻撃も発生しており、短期間に集中的に行われる傾向にある[14]。

・インターネットバンキングに係る不正送金の被害額は4.6億円で、件数とともに減少傾向にあるものの、新たに仮想通貨を狙った不正送信による被害額が670億円以上と急増している[15]。

・インシデント対応組織「CSIRT」を設置している企業は、米国では56%、欧州でも33%に対し、日本では23%にとどまる[16]。米欧で設置の割合が高まるなか、日本では設置状況に大きな変化がない。

・情報セキュリティを対象に入れたリスク分析をしている企業の割合は55%に過ぎず、米国の81%、欧州の66%と比較して立ち遅れている[17]。経営陣が自社の情報セキュリティリスクや対策、投資計画を審議する会議があり、意思決定の場として機能している企業の割合も、米国の83%、欧州の72%に対して、58%にとどまる[18]。

また、中小企業の多くはこれまで、自分たちは規模が小さい会社だからサイバー攻撃のターゲットにはならないだろうと考えていたが、そうした認識は間違っている。実際、中小企業の大半が

9 独立行政法人情報処理推進機構 (IPA)「企業のCISOやCSIRTに関する実態調査 2017 –調査報告書–」[https: //www.ipa.go.jp/files/000058850.pdf]（2019年9月2日）
10 IPA、前掲。（2019年9月2日）
11 一般社団法人JPCERTコーディネーションセンター「ランサムウエアの脅威動向および被害実態調査報告書」[https: //www.jpcert.or.jp/research/Ransom–survey.pdf]（2019年9月9日）
12 警察庁「平成30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」[https: //www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf]（2019年9月9日）
13 警察庁、前掲。（2019年9月9日）
14 NTTセキュリティ株式会社「Global Threat Intelligence Report 2018」[https://www.nttsecurity.com/ja–jp/landing–pages/2018–gtir]（2019年8月28日）
15 警察庁、前掲。（2019年9月9日）
16 IPA、前掲。（2019年9月2日）
17 IPA、前掲。（2019年9月2日）
18 IPA、前掲。（2019年9月2日）
19 Patricia Harmn, “50% of small businesses have been the target of a cyber attack,” PropertyCasualty360.com, Oct. 7, 2015.

サイバー攻撃の被害を受けており、英国では被害を受けた企業の割合は75%近くに達している[19, 20]。憂慮すべきことに、米国においてサイバー攻撃を受けた小規模企業の60%が、6か月以内に倒産している[21]。さらに、小規模企業は、その企業自体が攻撃のターゲットとなるだけでなく、顧客、サプライヤー、ジョイントベンチャーといった関係を通じて、より大規模な企業への攻撃経路となってしまうことも多い。そのため、ベンダーやパートナーの管理は、他組織と相互接続されている全ての組織・事業者にとって不可欠となっている。

サイバーセキュリティの分野では、防御しなければならない企業よりも、サイバー攻撃者の方が、技術的にはるかに進んでいるというのが一般的な認識である。サイバー攻撃は、費用がほとんどかからないにもかかわらず、収益性が非常に高い。また、攻撃を仕掛けるために必要なプログラムなどのリソースやスキルは、簡単に手に入れることができる。攻撃者の技術よりもサイバーリスクに対する防御の技術が一世代遅れがちであると見ている人が多いのも、不思議ではない。また、サイバー攻撃対策に関する投資利益率（ROI）を実証することは困難であり、サイバー攻撃に対する法執行機関による対応の成功例も事実上存在しない。サイバー攻撃者のうち、起訴されたのは1%にも満たないとする推計もある[22]。

だからと言って、防御が不可能だという訳ではない。むしろ、このように防御が困難であるからこそ、取締役は、経済的に可能な限り最大限の靭性を備えた社内システムの構築に全力で取り組む必要がある。これには、高度な攻撃方法に対処できる防御・対応計画の策定も含まれる。

攻撃の理由

企業の中には、会社の規模が比較的小さいから、知名度の高いブランドではないから、クレジットカード番号や医療情報などの機密性の高い消費者データを大量には保有していないから、などという理由で、サイバー攻撃の被害を受ける可能性が低いと考えている企業もある。しかし、実際には、攻撃者は全ての産業のあらゆる規模の組織をターゲットにしており、以下のような資産を含め、価値のある可能性のあるものなら何でも探し求めている。

- 合併・買収戦略、入札等を含む事業計画
- 取引手順
- 顧客、サプライヤー、流通業者、ジョイントベンチャーパートナー等との契約書または合意書案
- 従業員のログイン認証情報
- プラントや装置の設計、建物マップ、将来計画等の施設・設備に関する情報

20 Mark Smith, "Huge rise in hack attacks as cyber-criminals target small business," *The Guardian*, Feb. 8, 2016.
21 Gary Miller, "60% of small companies that suffer a cyber attack are out of business within six months," the *Denver Post*, Oct. 24, 2016.
22 Robert M. Regoli, et al., *Exploring Criminal Justice: The Essentials* (Burlington, MA: Jones & Bartlett Learning, 2011), p.378.

・開発中の新製品やサービス等の研究・開発情報
・主要なビジネスプロセスに関する情報
・ソースコード
・従業員、顧客、契約業者、サプライヤーのリスト
・クライアント、資金提供者、受託者に関するデータ

出典：インターネット・セキュリティ・アライアンス

サイバーセキュリティと収益性のバランスの確保

企業が直面する他の重要なリスクと同様に、サイバーセキュリティだけを切り離して検討することはできない。取締役は、組織の安全保護および損失軽減と、競争環境における収益性および成長の継続的確保との間で適切なバランスを保たなければならない。

収益性を高める技術革新やビジネス手法の多くは、セキュリティを損なうこともある。例えば、モバイル技術、クラウドコンピューティング、スマートデバイスなどの技術の多くは、大幅なコスト削減やビジネス効率の向上を実現する可能性があるが、導入方法を間違うと、セキュリティ面で大きな問題が生じる可能性がある。

同様に、BYOD（個人所有機器の持ち込み）、24時間年中無休の情報アクセス、高度なビッグデータ分析の増加、長大な国際サプライチェーンの利用といったトレンドは、費用対効果が非常に高く、企業が競争力を保つうえで不可欠な要素となる場合がある。しかし、これらの手法は、組織のセキュリティを著しく損なう可能性もある。

組織が自衛する一方で、競争力を保ち、収益性を維持することは可能である。しかし、ビジネスプロセスの末端にサイバーセキュリティ対策を適用すればそれで終わりといった簡単なことではない。サイバーセキュリティは、企業の主要なシステムとプロセスに隅々まで織り込まれる必要がある。それに成功すれば、競争力を高めるうえで役立つ可能性がある。ある研究によると、以下の4つの基本的なセキュリティ管理を実施することにより、サイバー攻撃の85%は効果的に防止できることが明らかになっている。

- ユーザーによるアプリケーションのインストールの制限（「ホワイトリスト登録」）。
- オペレーティングシステム（OS）が最新アップデートで「パッチ適用済み」であることの確認。
- ソフトウェアアプリケーションの定期的なアップデートの確認。
- 管理者権限（ソフトウェアのインストールやコンピュータの構成設定の変更を行うこ

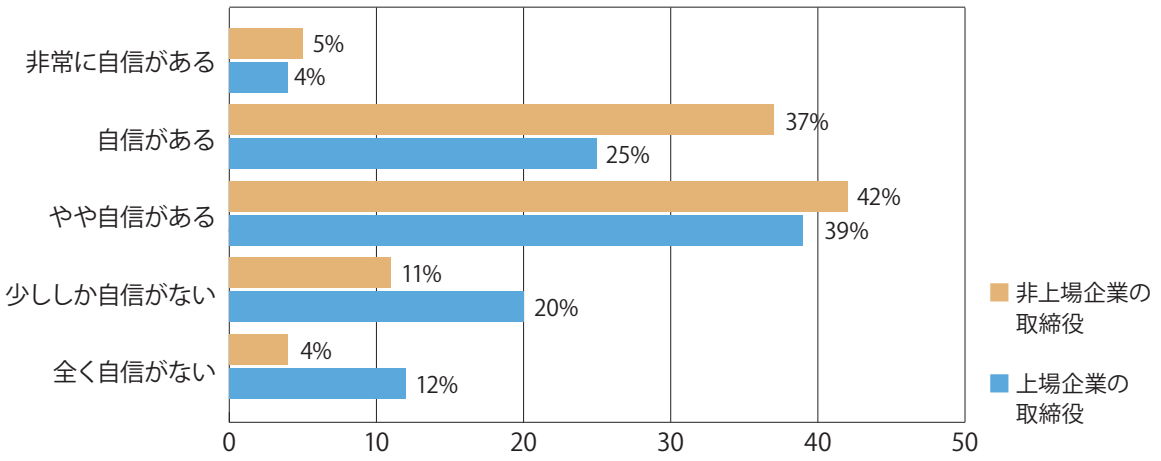
とができる権限）の制限[23]。

この研究では、上記の中核的なセキュリティ対策は、サイバー攻撃の防止に効果的なだけでなく、ビジネスの効率性を向上させるとともに、サイバー攻撃による被害を減らしたことによる経済効果を考慮に入れなくとも直接の投資利益を生み出すことが分かった[24]。

しかしながら、サイバー戦略が効果を発揮するためには、問題の発生に対応するだけのものであってはならない。優れた企業は、問題への事後対応以外にも、サイバーリスク環境に関する情報を作成したり、攻撃者が狙いそうな箇所を予測したりするなど、より積極的な、先を見越した対策を行っている。具体的には、自社のシステムやプロセスに対し厳格なテストを定期的に実施し、脆弱性を検出するといったことが行われている。

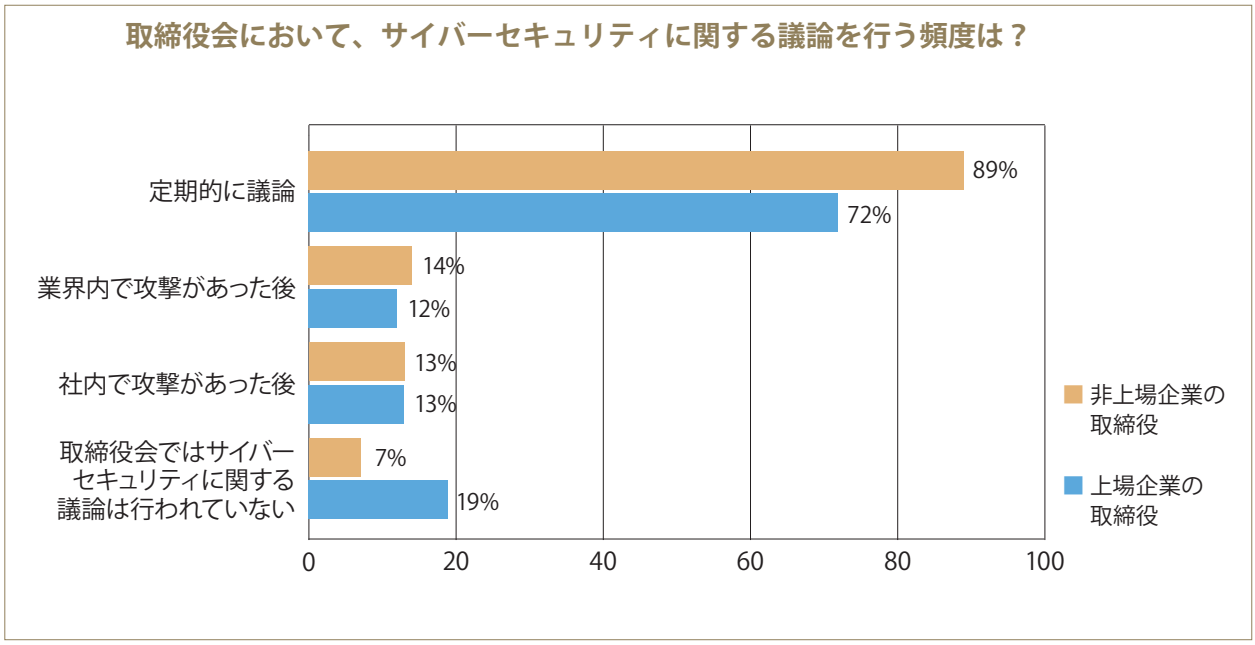
本ハンドブックで詳述する効果的なサイバーリスク監督のための5つの原則は、取締役会による議論や熟考を促すために、比較的一般化した形で提示している。当然ながら、各取締役会はこれらの推奨事項を規模、ライフサイクルステージ、戦略、事業計画、業種、事業展開地域、社風など、自社固有の特性に合わせて適応させていくことになる。

図1　サイバー攻撃に対する自社のセキュリティの確保について、どの程度自信があるか？



23 AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013. 以下も参照: Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: Internet Security Alliance, 2013).

24 AFCEA Cyber Committee, *The Economics of Cybersecurity:A Practical Framework for Cybersecurity Investment*, October, 2013.



出典：本データは米国においてNACDの2016～2017年上場・非上場企業ガバナンス調査をもとに取りまとめたものである。

取締役は、サイバーセキュリティを、単なるITの問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要がある。

企業はこれまで、情報セキュリティを、IT部門が対処すべき技術・運用上の問題として捉えてきた。このような誤解をいっそう悪化させているのは、部門ごとに分かれた企業の構造である。組織を構成する各部署や事業部門は、自部門のデータのセキュリティが自分たちの責任であることを認識しないまま放置してきた。各部門は自分たちの責任を認識せず、代わりに、IT部門だけにデータのセキュリティという重要な責任が委ねられている。しかし、大半の企業のIT部門はリソースや予算権限が限られているなかで業務を行っている。さらに、セキュリティの責任をIT部門に委ねてしまっているため、セキュリティ問題に関する重要な分析やコミュニケーションが阻害され、効果的なセキュリティ戦略の導入が妨げられている。

相互接続がますます進むエコシステムにおいては、ITが価値を創出ないし付加しているという意味で、あらゆる企業がテクノロジー企業であるといえる。企業の大半がITイノベーションに多額の投資を行うとともに、全体的なビジネス戦略や業務運営において、技術基盤がますます中心的な役割を果たすようになっている。業種や提供するサービスによっては、他企業よりさらに本質的な意味でITに依存している企業もある。サイバーリスクは、企業が自社の人的・物的資産のセキュリティや人的・物的資産が損なわれるリスクを評価するのと同じ方法で評価されるべきである。つまり、サイバーセキュリティは全社的なリスク管理に関わる問題であり、戦略的、部門横断的、経済的視点で取り組む必要がある[25]。単にIT（または技術）の問題であるだけでなく、ビジネスプロセス、人材、価値に関わる問題なのである。

サイバーリスクとビジネスエコシステム

これまでのデータ漏洩で最も注目を集めた大規模な事件の中には、従来型のハッキングとはほとんど関係がないものもある。例えば、システム侵害の代表的な原因はスピアフィッシング（特定の個人を狙った一般的な電子メール攻撃）である。また、複数の国・地域にまたがる複雑なサプライチェーンを利用する製品や生産戦略は、サイバーリスクを高める可能性がある。同様に、複雑なシステムの統合を必要とする合併・買収は、短いスケジュールで、十分なデューディリジェンスを行っていないものも多く、サイバーリスクを増大させる可能性がある。

セキュリティが確保されたシステムを構築するうえで企業が直面する他の問題として挙げられるのが、パートナー、サプライヤー、関連会社、顧客とのネットワークの接続性をどう管理するかという問題である。広く知られた重大なサイバー攻撃事件の中には、標的とされた企業のITシステムから侵入されたわけではなく、被害企業のベンダーやサプライヤーなどのいずれか1社の脆弱性

25 Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*, 2010.

に起因して被害に至ったケースもある。そうした事例は「ネットワーク接続の拡大に伴うリスクの増大」のセクション（8ページ）に示している。さらに、データを外部ネットワークやパブリッククラウドに保管している企業が増えているが、その場合、データ保管環境を自ら保有しているわけでも運用しているわけでもないため、自社のみでセキュリティを確保することは難しい。また、多くの企業が国家の重要インフラの構成要素とつながっていることから、一企業または一機関のサイバーセキュリティが、社会全体のセキュリティの問題、場合によっては国家安全保障に影響を与えるという可能性も考えられる。

以上を踏まえ、取締役は、サイバーセキュリティを自社ネットワークに関連するものとしてだけではなく、より大きなエコシステムにも関係があるものとして評価すべきである。進歩的な取締役会であれば、自社のエコシステムの中に存在する様々なレベルのリスクについて議論し、サイバーリスクに対する自社の適切な態勢や許容度を算出する場合にも、様々なレベルのリスクを考慮に入れるであろう[26]。また、取締役会は、保護の必要性が最も高い、企業が保有する重要資産や特に機密性の高いデータが何かを理解するとともに、これら価値の高い情報資産を中心に据えて組み立てられた防衛戦略を持つべきである。取締役会は、最も高い確率で起こり得る攻撃だけでなく、確率は低いものの壊滅的な影響を与える可能性がある攻撃も考慮すべきである[27]。

企業が保有する重要資産および非常に機密性の高いカテゴリーに属するデータの特定

取締役は、以下の問題について定期的に議論すべきである。

- 自社の最も重要なデータ資産は何か？
- 自社が保有する機密性の高いデータ（機密性の高い個人データなど）は何か？
- ビジネスの柱や屋台骨は何か、ビジネスに使用されているITインフラは何か？
- それらはどこにあるか？ 一つ、または、複数のシステムに置かれているか？
- データにはどのようにアクセスするのか？ アクセス権限を持っているのは誰か？
- どの程度の頻度で自社システムのデータ保護性を試す脆弱性検査を行っているか？
- ビジネスモデルやビジネス戦略にセキュリティが織り込まれているか？

取締役会レベルにおけるサイバーリスクの監督責任

サイバーリスクを監督したり、企業レベルのリスクをより広範に管理したりするために、取締役会をどう組織すべきかについては、かなり議論の余地がある。サイバーリスクは、企業全体のリスク管理の問題として対処すれば、大幅に軽減したり最小限に抑えたりすることができる。しかし、

26 NACD, et al., *Cybersecurity: Boardroom Implication* (Washington, DC: NACD, 2014)(an NACD white paper).
27 Ibid. 以下も参照: KPMG Audit Committee Institute, *Global Boardroom Insights:The Cyber Security Challenge*, Mar. 26, 2014.

従来型のリスクと同様に、サイバーリスクもまた完全に無くすことはできない。取締役会は自社を取り巻く脅威環境の性質を理解する必要がある。

以下では、米国の例を紹介する。

NACDのリスクガバナンスに関するブルーリボン委員会（NACD Blue Ribbon Commission on Risk Governance）は、リスク監督は取締役会全体としての機能であるべきと勧告した[28]。NACDの調査によると、いわゆる「ビッグピクチャー・リスク」（戦略的方向性に広範な影響を及ぼすリスクや、様々なリスク間の相互作用に関する議論など）に関しては、大半の上場企業で勧告通り取締役会全体としてリスク監督に取り組んでいることが明らかになっている。ところが、サイバーセキュリティ関連のリスク監督責任については、半数強の取締役会が、責任の大部分を監査委員会に割り当てている（図2）。しかしながら、監査委員会は、財務報告およびコンプライアンスリスクを監督する大きな責任をも同時に担っている。

どんな取締役会にもマッチする、ただ一つの手法は存在しない。サイバーリスクに関しては、全て取締役会全体レベルで議論するという選択をしている取締役会もある。また、特定のサイバーセキュリティ関連の監督責任を一つまたは複数の委員会（監査、リスク、技術などの委員会）に割り当てている取締役会もある。さらに、これらの方法を組み合わせて使用している取締役会もある。指名・ガバナンス委員会は、取組みの混乱や重複を避けるため、取締役会が選択した手法が委員会の規則の中で明確に規定されていることを確保すべきである。取締役会全体が、サイバーセキュリティに関する事項の概要について、少なくとも半年ごとに、また具体的なインシデントや状況によって必要となった場合にはその都度、報告を受けるべきである。リスク監督（とくにサイバー関連リスクの監督）の責任を負う委員会は、少なくとも四半期ごとに報告を受けるべきである。

知識共有と対話を促進するため、取締役会の中には、全取締役にサイバーリスク問題に関する委員会レベルの議論への参加を要請したり、複数の委員会に重複して席を置くクロス・メンバーシップを活用したりしている取締役会もある。例えば、あるグローバル企業の取締役会レベルの技術委員会には、プライバシーとセキュリティを顧客の観点から見ることを専門にする取締役が参加している。また、監査委員会と技術委員会の議長がそれぞれ互いの委員会の委員を兼任しており、ふたつの委員会が毎年1回共同で会合を開き、サイバーセキュリティについて「深く掘り下げる」議論等を行っている[29]。

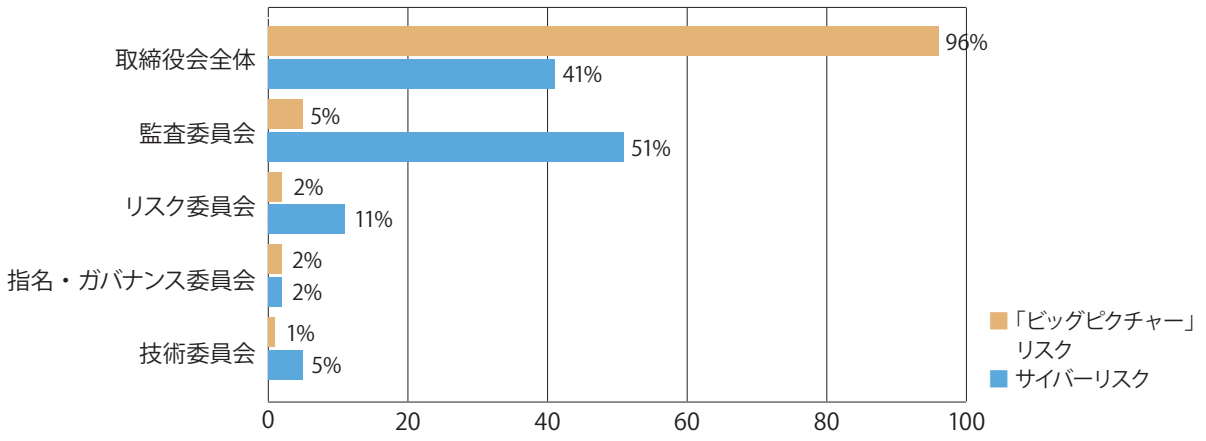
米国での上記事例のように、サイバーセキュリティを取締役会や委員会会合の議題に独立した項目として含めることは、現在では広く実践されるようになっているが、日本においても、サイバーセキュリティに関する問題は、新たな事業計画や製品提供、合併・買収、新市場への参入、新技術の導入、施設拡張やITシステムのアップグレードなどの大型資本投資等の意思決定に関係する、取

28 NACD, *Report of the Blue Ribbon Commission on Risk Governance:Balancing Risk and Reward* (Washington, DC: NACD, 2009).

29 Adapted from obyn Bew, "*Cyber–Risk Oversight: 3 Questions for Directors*," Ethical Boardroom, Spring 2015.

締役会全体での議論にも含めるべきである。

図2　**取締役会が以下のリスク監督分野に関連する職務の大部分を割り当てているのは、どのグループか?（複数選択可の回答の選択肢の一部をリストアップ）**



出典：2016～2017年NACD上場・非上場企業ガバナンス調査

取締役は、自社固有の状況と関連付けて、サイバーリスクの法的意味を理解すべきである。

開示義務、プライバシーおよびデータ保護、情報共有、インフラ保護など、サイバーセキュリティに関する法規制の状況は複雑であり、常に変化している。取締役会は、現在自社が直面する責任問題、また、場合によっては取締役個人が直面する可能性がある責任問題についても、常に留意すべきである。例えば、注目度の高いサイバー攻撃は、株主や顧客による訴訟を引き起こす可能性があるとともに、規制当局による法的措置へとつながる場合がある。訴訟においては、データ漏洩やその結果に対し、会社が十分な安全管理措置を取らず、善管注意義務を怠ったとして、原告が企業や取締役会を構成する個々の取締役を訴える可能性もある。さらに、リスクはその企業の業種や活動地域によって大幅に異なる可能性がある。加えて、訴訟となれば、その訴訟の内容や最終的な判決がどうであれ、サイバー攻撃による被害が企業のレピュテーションに与えるダメージは、深刻かつ長年に及ぶこともある。

取締役会は、（ｉ）サイバーセキュリティとサイバーリスクに関する議論の記録をいかに維持するか、（ii）その企業に適用される業界・地域・部門固有の各種法規制等にどのようにして常に通じておくか、（iii）企業の対応策を受けてさらに進化していくリスクをどう分析するか、（iv）サイバー攻撃を受けた際に何を公表するか について検討すべきである。サイバーリスクが常に重視すべき対象であるということを従業員に示すため、取締役会はサイバーセキュリティに対して積極的な姿勢で臨むべきである。そして、企業がサイバーリスク管理に適切に集中できるよう、効果的なガバナンス体制を実装する必要がある。また、取締役はサイバー攻撃対応演習に参加し、重大なインシデントが発生した場合の影響を軽減すべく会社の対応手順を学ぶとともに、取締役会が重要な決定を行う必要があるシナリオを想定して練習することが望ましい。

これを促進するために、取締役会は、ITの専門知識の収集・利用を、IT部門に依存するのではなく、取締役会レベルで行ったり、透明性を確保しながらサイバーセキュリティ対策を監督する責任を割り当てたりすることも検討すべきである。取締役会が留意すべきトピックとしては以下が挙げられる。

取締役会議事録

監督責任の割り当てにもよるが、取締役会議事録は、取締役会全体や取締役会の主要な委員会の会合の議題にサイバーセキュリティが取りあげられた際には、その旨を反映すべきである。これらの会合での議論には、特定のリスクや軽減戦略に関する最新情報のほか、企業全体のサイバーセキュリティ対策の状況や、技術と企業の戦略、ポリシー、事業活動との統合に関する報告などが取りあげられる場合がある。

コーポレートガバナンス・コードでの記述や法規制

現在、東京証券取引所のコーポレートガバナンス・コードでは『原則4-3　取締役会の役割・責務（3）』において「取締役会は、適時かつ正確な情報開示が行われるよう監督を行うとともに、内部統制やリスク管理体制を適切に整備すべきである」として、リスク管理体制の整備を取締役会の役割・責務の一つとして明記している。IT依存度の高い企業の場合、サイバーリスクの管理もその中に含まれると考えられる。

さらに、経済産業省のコーポレート・ガバナンス・システム研究会では、『グループ・ガバナンス・システムに関する実務指針』の中で、「サイバーセキュリティについては、内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れたセキュリティ対策の在り方について検討されるべきである」としている。

また、業種によっては、それぞれの業法および関連法令において、サイバー攻撃によってサービス提供に支障をきたした場合、監督官庁への報告が義務付けられている。

個人情報の保護

個人情報の保護については、2018年5月に施行されたEUの『一般データ保護規則（General Data Protection Regulation: GDPR）』がEU域内で事業を展開する企業に対して包括的な要請を行なっている。GDPRは、個人データを管理する組織と、個人データを処理する組織の両方について、様々な義務を定めている。とくに、同規則は「リスクに適切に対応する一定のレベルの安全性を確保するために、適切な技術上および組織上の措置」の実装を求めている。同規則では、また、通知義務の強化が図られており、個人データの侵害があった場合、所轄監督機関に、不当な遅滞なく（実施可能な場合は72時間以内に）届け出ることを求めている。当該通知義務に従わなかった場合、その企業に対して、同社の前会計年度の世界全体での年間売上総額の2%以下、または、1,000万ユーロ以下のいずれか高い方を上限に制裁金を科すことができる。さらに、監督機関は、幅広い調査・是正権限を有しており、GDPRによって、個人が私的な申立を行うことがかなり簡単になっている。日本でも、個人情報保護委員会が『個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理』（2019年4月）の中で、

「〇諸外国においては、多くの国で漏えい報告が義務とされている。一方、我が国では、法的な義務ではないにもかかわらず、漏えい報告について、多くの企業で適切に対応されており、これは、我が国事業者の個人情報保護に対する意識の高さとも考えられる。

〇一方、漏えい報告は法令上の義務ではないため、積極的に対応しない事業者も一部に存在している。仮に、事業者側が公表等しない場合、委員会が事案を把握できない可能性があり、適切な対応が行われない懸念がある。

〇また、事業者側から見ても、漏えい報告について、一定の軽減措置を設けることを前提に、法令上明確に位置付けた方が、企業側が報告の要否に係る判断に迷わないとも考えら

れる。

○加えて、国際的な議論の潮流の観点からしても、ICDPPCやOECDといった多国間での枠組みで、各国の漏えい報告の状況を当局間で情報共有するという方向で議論がなされている状況を考慮する必要がある」としている。

法務部門の役割

社内の法務部門やコンプライアンス部門は、社外の弁護士とともに、サイバー攻撃において重要な役割を果たす。取締役は、以下について、法務部門やコンプライアンス部門および弁護士の見解を求めるべきである。

- 法規制リスクを軽減するための枠組みの導入
- 組織のサイバーセキュリティインシデント対応計画（とくに規制当局とのやり取りや文書管理を含む）
- 将来を見通したリスク要因全般に関連する開示可能性

各種法規制等と、企業をとりまく状況は絶えず変化していることから、取締役は、法務部門やコンプライアンス部門および弁護士の見解を定期的に求めるべきである。

取締役会は、サイバーセキュリティに関する十分な専門知識を利用できるようにしておくとともに、取締役会の議題としてサイバーリスク管理を定期的に取り挙げ、十分な時間をとって議論を行うべきである。

原則1で述べたとおり、サイバーリスクは取締役会において理解し、検討されるべきである。一方で、取締役はサイバーリスクについて検討することができるほど、サイバーセキュリティの専門知識を有しているだろうか? 以下、米国の例を紹介する。

非上場企業の取締役を対象とした最近の調査では、回答者の89.1%が、取締役会においてサイバーセキュリティについて「定期的に」議論していると回答している[30]（より詳しくは、図3参照）。しかし、こうした高い活動レベルにもかかわらず、自社の取締役会がサイバーセキュリティリスクに関する「高い」レベルの知識を有していると考える取締役の割合は約14%にすぎない[31]。ある取締役は、次のように指摘している。「［サイバーセキュリティ］の管理は、いわば動く標的を追い続けるようなもの。脅威も脆弱性も日々絶えず変化しているし、サイバーリスクの管理・監督方法の基準は、まだ形成され始めたばかりだ[32]」別の取締役同士の意見交換会で、ある取締役は、次のような分かりやすいたとえを示した。「サイバーリテラシーは、ファイナンシャルリテラシーと同じように考えることができる。取締役会の全員が監査人でないとしても、誰もが財務諸表を読んでビジネスで用いられる財務用語や文脈を理解できる必要がある[33]」

サイバーセキュリティの専門知識へのアクセス向上

サイバーの脅威が増大するにつれて、取締役の担う責任（および期待）は高まっている。取締役会は、単に脅威があることを理解し、サイバーセキュリティ担当取締役または担当部門から報告を受けるだけではなく、それ以上の役割を果たすことが求められている。取締役会で行われる戦略および業績に関する議論の場合と同じように、取締役はサイバーセキュリティ担当取締役または担当部門の説明に疑問を投げかけ、建設的に異議を唱えるなど、積極的な役割を果たす必要がある。

その結果、米国においては、新たな取締役を採用して、サイバーセキュリティやITセキュリティに関する専門知識を直接取締役会に取り入れるかどうかを検討している企業もある。こうした方策は一部の企業・組織にとっては適切と考えられるが、どこにでも通用する「万能薬」は存在しない。米国の取締役と主要投資家とが行ったNACDの意見交換において、参加者らは、サイバーセキュリティ分野であれ、その他の分野であれ、個別分野に特化した、いわゆる「専門職」取締役を、全ての取締役会に加えようとする動きに対して懸念を表明した。参加者のひとりは、次のよう

30 NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p.28.
31 NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p.26.
32 NACD Audit Committee Chair and Risk Oversight Advisory Councils, *Emerging Trends in Cyber–Risk Oversight*, July 17, 2015, p.1.
33 NACD, et al., *Cybersecurity: Boardrooms Implications* (Washington, DC: NACD, 2014), p.3.

に語っている。「それはリスク回避と受けとられてしまう可能性がある。取締役会が訴えられる懸念があるから、X、Y、Zの専門家が必要だとなれば、最新の［マネジメント］スキルを一揃いそろえることになってしまう[34]」

米国だけではなく、日本においても、取締役会の空席を埋める際には、自社の戦略ニーズや状況に応じて、業界の専門知識、財務知識、グローバルな経験、その他のスキルセットなど、必要とされる資質を含め多くの要因についてバランスを取らなければならない。取締役会がサイバー分野に特化した専門知識を持つ取締役を加える選択をする以外にも、取締役会にサイバーセキュリティ問題について豊富な知識に基づく知見を導入する方法はある。以下にいくつかの戦略を挙げる。

- サイバーセキュリティ対策が目的に合致しているかどうかを検証してもらうため、独立かつ客観的な第三者である専門家に対して詳細な説明を行い、評価させる。
- JPCERT/CC、情報処理推進機構（IPA）、業界別ISAC、セプターカウンシル、日本シーサート協議会など、サイバーリスクの動向について、他社の事例から得た、業界全体を見通す知見を有する既存の独立アドバイザーを活用する。
- 関連する取締役教育プログラムに参加する（社内、社外どちらのプログラムでもよい）。
- より多様な独立取締役（必ずしもサイバーの専門家である必要はないが、サイバーおよび関連分野に関する知識を有する取締役）を取締役会に迎え入れる[35]。その際、人的な多様性（年齢、性別、民族、国籍）だけでなく、多くの取締役が持つ財務や経営の知識以外の経験（テクノロジー、ガバナンス、リスク、コンプライアンス、および倫理面など）を考慮する。

サイバーセキュリティに関する十分な専門知識へのアクセス

取締役の大半は、特定分野または専門領域の専門家でしかない。それまでに積んできた経験から特定テーマに関する専門知識を身に付けていたとしても、取締役としては、幅広い視野から企業全体のリスク管理および対応に臨むべきである。では、サイバーセキュリティに関する十分な専門知識には、どのようにしてアクセスすればよいのか。サイバーセキュリティに関する専門知識として十分なレベルとみなせるのは、どのような知識であるか。その出発点は、本ハンドブックの原則1に示した基本的理解にある。まず、取締役会は、サイバーセキュリティがITの問題ではなく、企業全体のリスク管理の問題であることを理解する必要がある。したがって、取締役会は、サイバーセキュリティをIT部門やITセキュリティ担当者に丸投げし、答えを出すよう求めることは避けなければならないのである。

34 Discussion at a joint meeting of the NACD Advisory Councils for Audit Committee Chairs and Nominating and Governance Committee Chairs, Oct. 5, 2016.
35 Andrea Bonime-Blanc, "A Strategic Cyber-Roadmap for the Board: From Sit-Back to Lean-In Governance". The Conference Board, 2016.

企業は、必ずしも、サイバーの専門家を取締役会に加える必要はない。この点については、独自の個性を有する企業それぞれが、どうすべきか意思決定するのが最善であろう。とはいえ、取締役会は、サイバーセキュリティ、ならびに、それに伴うリスク管理の問題を担当する取締役を指名すべきである。従来型リスク（地震、台風、火災など）や経済的リスク（競争、製造物責任、資産の減損など）については、インシデントの発生確率が推定できる。過去のデータからリスクの傾向や規模を把握すれば、将来の潜在的なリスクが予測可能である。また、過去の市場の変動を、そうしたリスクのもたらす影響やその軽減方法を評価するために役立てることができる。しかしながら、サイバーセキュリティについては、誰もが、いつかは必ずハッキングされると想定して対応しなければならないのである。

さらに、サイバーリスクは、いくつかの重要な点で従来型リスクとは異なっている。例えば、相互に接続され、急速に変化を続ける世界においては、企業は自らを完全に守ることができない。サイバー攻撃を仕掛けてくる敵は様々であり、国家の場合さえある。とすれば、敵は最大規模の企業さえも上回るリソースを有している可能性がある。また、サイバー犯罪者の逮捕・追跡は、従来型の犯罪者の場合と比べて実務的に一層困難であることが多い。サイバーセキュリティ対策に携わる取締役は、こうしたことを理解しておかなければならない。

セキュリティに関する専門知識へのアクセスを改善するために取締役会が検討できる方法は、いくつかある。取締役会は、複数の情報源から助言を求めることによって、抑制と均衡のシステムを構築することができる。例えば、企業は、3つの独立した情報源（必ずしも社外である必要はない）から、それぞれ報告を受ける構造を作ることが考えられる。そうした情報源として、サイバーリスク責任者の視点、サイバーリスク評価担当者の視点、業務マネージャーの視点などを含めるとよい。こうすることにより、お互いの機能や取組み方に疑問や異議を投げかけ、説明を求めることができるようになり、ひいては、サイバーリスクを様々な視点から検討することが可能になる。

取締役会のリスクレジスター[36]は、サイバー技術とサイバーリスクのセクションを明確に分けて設けるべきである。そうすれば、サイバーリスクの議論を、通常のビジネスリスク報告の一側面として定着させることができる。

取締役会でのサイバーリスク報告の強化

以下では、取締役会へのサイバーリスクに関する報告について、米国の事例を紹介する。

36 **欧州ネットワーク情報セキュリティ庁（ENISA）によると、リスクレジスターとは、リスクを把握、説明、評価するためのツールである。特定されたリスクとともに、リスクのアカウンタビリティ、対応措置（必要な場合）、レビューの日付、対応措置が完了しリスク項目をクローズした日付が記載されている。リスクレジスターは、取締役会がサイバーリスクの大きさを企業のプロファイルに照らして定量化する上で役立つ重要なツールである。企業にいくつかのリスクがあり、サイバーリスクが上位10位に含まれている場合、取締役会が費やす時間と予算を増やす必要がある。しかし、サイバーリスクがないならば、少しは気を休めることができる。リスクレジスターは、自社が影響を受ける可能性のある有害事象のポートフォリオを文書化するために使用すべきである。**

2012年の調査によると、プライバシーおよびセキュリティリスクに関して、定期的に報告を受けている取締役会の割合は40%未満である一方、そうした情報をほとんどまたは全く受け取っていない取締役会は26%であることが明らかになった[37]。それ以降、取締役会の慣行は、劇的に変化した。18ページに記したとおり、上場企業の取締役の90%近くが、自社の取締役会がサイバーセキュリティ問題に関する議論を定期的に行うとともに、経営陣の様々なメンバーから情報を受け取っていると回答している（図4）。しかし、この分野については、かなりの数の取締役が依然として改善が必要であると考えている。経営陣が取締役会に提供している情報の質について評価してほしいという質問については、サイバーセキュリティに関する情報は、最低レベルにランクされた。上場企業の取締役の4分の1近くが、経営陣が提供するサイバーセキュリティに関する情報の質について、不満または非常に不満であると回答した。受け取った情報の質について非常に満足していると回答した取締役は15%に達していない。それに比べ、財務実績については、情報の質に関する満足度が高いと評価した割合は約64%であった[38]。

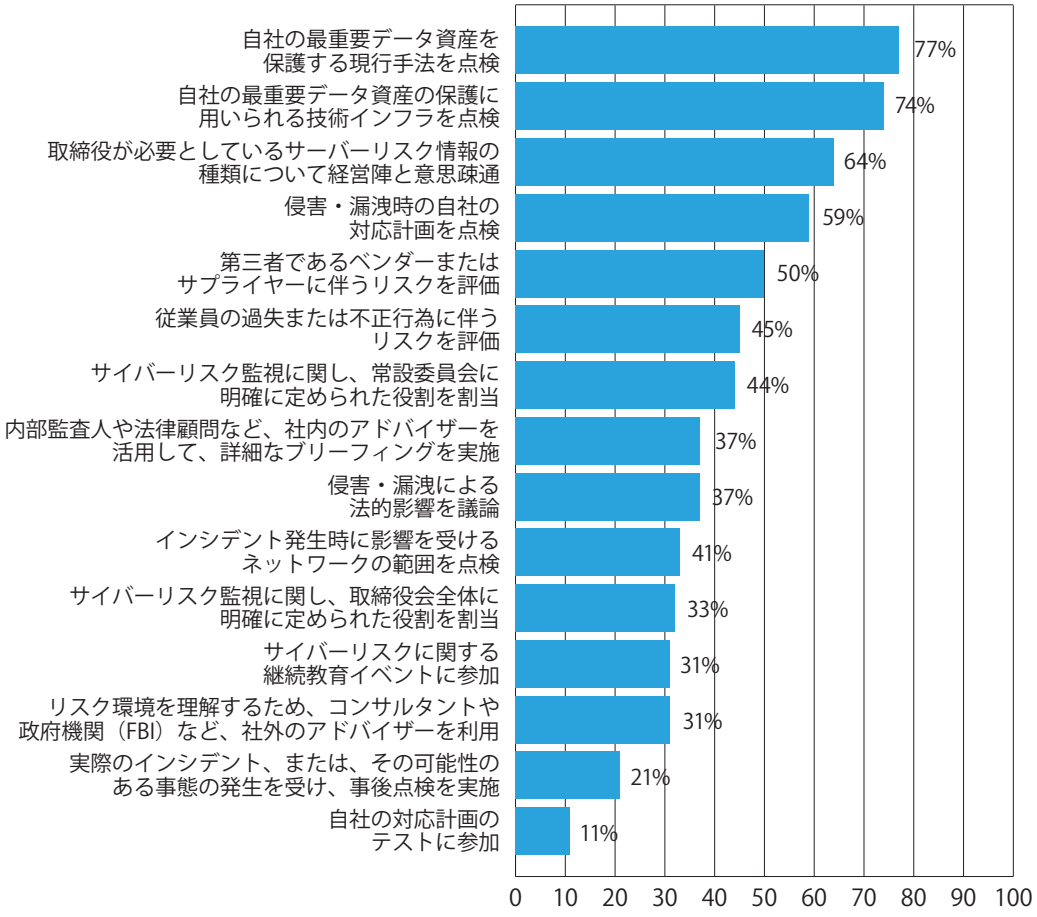
NACD調査の回答者は、経営陣からのサイバーセキュリティに関する報告が不満である要因として、以下のようないくつかの理由をあげている。

- 提供された情報を用いて実績のベンチマーク評価を行うのが難しい。社内（企業内の事業部門間の比較）、社外（同業他社との比較）の両方のベンチマーク評価が困難。
- 実績に関する透明性が不十分。
- 情報の解釈が難しい[39]。

米国においても、日本においても、サイバーセキュリティおよびサイバーリスク分析は比較的新しい分野である（財務分析よりも間違いなく成熟度が低い）ことから、報告手法が成熟するまでに時間を要すると考えられる。とはいえ、取締役会は、受け取りたいサイバーセキュリティ関連情報のフォーマット、頻度、詳細度について、希望をサイバーセキュリティ担当部門または担当取締役に明確に伝えるべきである。また、取締役会でのサイバーセキュリティ担当部門または担当取締役の報告の検討に当たっては、報告者がリスク環境の深刻さを実態よりも軽く見たいというバイアスがかかっている可能性があることに留意すべきである。ある研究によると、ITスタッフの60%は、緊急事態になるまで（つまり影響の軽減が難しくなるまで）、サイバーセキュリティのリスクを報告しないという。また、悪い結果を報告から除外しようとする傾向があることも認められた[40]。取締役会は、サイバーリスク管理および報告に関して、オープンかつ率直で、透明性の高いコミュニケーションの創出に努めるべきである。

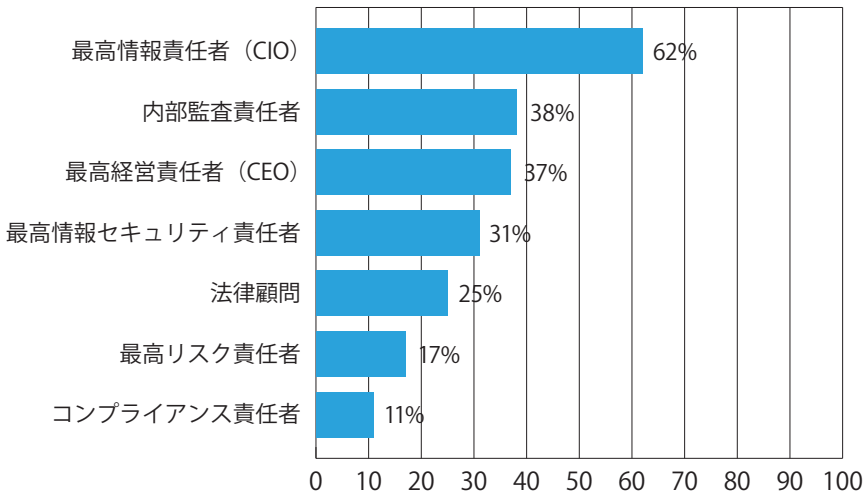
37 Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), p.7 and p.16.
38 NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p.28.
39 Ibid.
40 Sean Martin, "*Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's Serious,*" *International Business Times*, April 16, 2014.

図3 以下のサイバーリスク監督手法のうち、取締役会が過去12か月間に実施したものはどれか？



出典：2016～2017年NACD上場・非上場企業ガバナンス調査

図4 サイバーセキュリティの状況について、誰が取締役会に報告しているか？（該当するものを全て選択）



出典：2016～2017年NACD上場・非上場企業ガバナンス調査

取締役は、十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべきである。

現代において、技術は組織を一つに結びつけ統合するものである。廊下を一本挟んだ部屋にいる同僚であれ、地球の反対側にいる相手であれ、互いを結び付けてくれる。しかし、前記のとおり、多くの企業の報告体制や意思決定プロセスは過去のやり方、つまり、各部署や事業部門が比較的独立して意思決定を行っていた頃のやり方を踏襲しており、現代生活においては不可欠なデジタル上の相互依存性を十分に考慮していない。取締役は、企業全体がサイバーセキュリティに適切に取り組むよう確保すべきである。

サイバーリスク管理のための全社的手法の構築

企業は、自社独自のリスクプロファイルと脅威環境の評価から始めるべきである。企業が効果的なサイバーセキュリティの枠組みを導入するためには、自社を取り巻くリスク環境、自社独自のリスク許容範囲、潜在的なサイバーリスクを軽減するために必要なリソースの可用性を、明確に理解することが不可欠である。どこでも通用する「万能薬」は存在しない。

リスク管理の技術的管理の枠組み

2013年2月、 米国のバラク･オバマ大統領は、大統領令第13636号『重要インフラのサイバーセキュリティの向上（Improving Critical Infrastructure Cybersecurity）』に署名した。同大統領令は、 米国国立標準技術研究所（National Institute of Standards and Technology: NIST）に対し、民間部門が自主的に採用できるサイバーセキュリティのフレームワークの開発を指示したものである[41]。

2014年に公表されたNISTのサイバーセキュリティフレームワークは、サイバーリスクに対処するための政策、ビジネス、技術上の課題に整合した、一連の標準、方法論、手順、プロセスより構成される。このフレームワークは、自社内で全社的なサイバーリスク管理手法を考案する際に、企業の経営陣が使用できる共通言語を提供しようとするものである。また、サイバーセキュリティの評価を開始するに当たり、企業が次の階層のどこに位置しているかを判断するリスク管理プロセスに取り組むことを提案している。（1）部分的（2）リスク情報を活用（3）繰り返し可能（4）適応的 の4層で、後者ほど上位の階層である。

このようなレベルの管理は、全ての組織で実現するには実務的能力を上回る場合もあるだろうが、一部の要素は、米国に限らず、日本企業でも利用できると考えられる。NISTはNISTサ

41 Executive Order No. 13636–Improving Critical Infrastructure Cybersecurity, Federal Register 78, no. 33, (Feb. 19, 2013).

イバーセキュリティフレームワークのグローバル展開に積極的で、これまで日本国内でも何度か説明会を開催している。その結果、独立行政法人情報処理推進機構（IPA）が発表した『企業のCISOやCSIRTに関する実態調査2017』（2017年4月）によれば、33.4%の日本の企業が、情報セキュリティ対策を検討する際にNISTサイバーセキュリティフレームワークを参照・利用するまで認知が広まっている。他方、日本政府が制定したガイドライン類やISOシリーズの方がよく利用され、IPAの同調査によれば、最も多く参照・利用されているのが経済産業省の情報セキュリティ管理基準（56.6%）、次いで経済産業省のサイバーセキュリティ経営ガイドライン（54.8%）、さらにISO27001シリーズ（情報セキュリティマネジメントシステムに関する国際規格）（49.3%）となっている。このうち経済産業省『サイバーセキュリティ経営ガイドライン』は、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項目を提示し、付録として『サイバーセキュリティ経営チェックシート』を添付している。本ガイドラインは2015年12月に第1版が公表され、2017年11月に第2版へとバージョンアップされた。改訂のポイントとしてNISTのサイバーセキュリティフレームワークで謳われている事後対策（検知、対応、復旧）を充実させている。これはサイバー攻撃の巧妙化により、事前対策だけでは不十分になってきた情勢変化を受けたものと言える。なお、経団連は2017年12月に『Society5.0実現に向けたサイバーセキュリティの強化を求める』を発表した後、2018年3月に『経団連サイバーセキュリティ経営宣言』を公表している。

サイバーリスクのガバナンスに向けた統合的手法として求められることの例

1. サイバーリスクに関する部門横断的な当事者意識を確立する。最高情報責任者（Chief Information Officer）ではなく、最高財務責任者（Chief Financial Officer）、最高リスク責任者（Chief Risk Officer）、最高執行責任者（Chief Operating Officer）など、複数の部門に対して権限を有する経営幹部がチームを率いるべきである。
2. 組織横断的なサイバーリスク管理チームを任命する。事業部門のリーダー、法務、内部監査・コンプライアンス、財務、人事、IT、リスク管理など、一定の利害を有する関係部門の全てから代表者が参加しなければならない（下記の「鍵となる上層部の役割と責任」の抜粋を参照）。このような組織横断的な取組みを行うことの主目的は、組織内からサイバーセキュリティの弱い部分や例外を確実に無くすことである。
3. サイバーリスク管理チームは、サイバーリスクの複雑さを考慮した体系的な枠組みを用いて、将来を見越した、全社的なリスク評価を実施する必要がある。これには、法規制への準拠（コンプライアンス）を含むが、それだけに限らない。このリスク評価には、組織の脅威の現状とリスクの全体像の評価が含まれる。その後、リスク許容範囲を明確に定める。組織にとっての潜在的リスクと、そのリスクをどこまで受け入れるかの閾値を特定することは、サイバーリスクチームが、チームのミッションや目標にどの体系的な枠組みが最も適切に整合しているかを評価するうえで有益である。

4. サイバーセキュリティに関する法規制は、国・地域や業種によって大きく異なっているため、注意が必要である。原則2に記したとおり、取締役会は、自社に適用される標準や要件を確認するためのリソースを確保すべきである。サイバーセキュリティ分野における政府の関与範囲を積極的に拡大している国々もあるためである。
5. 取締役会への報告の取りまとめを行う。サイバーセキュリティ担当取締役または担当部門は、サイバーの脅威やそれに関連するリスク管理の取組みが事業に及ぼす影響を定量化する指標を追いかけ、報告することが期待される。サイバーリスク管理の有効性および自社のサイバーレジリエンシー（サイバー攻撃に対する靭性）の評価は、四半期ごとの内部監査等の実績レビューの一環として実施すべきである。こうした報告では、十分な詳細さの確保と、監査役会[42]に報告すべき戦略的に重要な点とのバランスを取るべきである。
6. 全ての部門および事業部門を対象とした、全社的なサイバーリスク管理計画および内部コミュニケーション戦略を立案・採用する。サイバーセキュリティは、その相当部分が、IT（技術）に関する要素であることは言うまでもない。しかし、法務、監査、リスク、コンプライアンスの関連部署など、関係者全てが社内計画の策定に関与するとともに、その計画に同意している必要がある。計画は定期的にテストすべきである。
7. 自社のニーズとリスク許容範囲に合致する十分なリソースを備えたサイバーリスク関連の総予算を策定・採択する。リソースに関する意思決定に当たっては、サイバーセキュリティ関連の経験を積んだ人材の深刻な不足を考慮するとともに、社内で対応できることと、第三者に外注できる、または、外注すべきことを特定すべきである。サイバーセキュリティは、IT（または技術）セキュリティの範疇に収まるものではない。そのため、サイバーセキュリティの予算を、一つの部門のみに限定してしまうべきではない。例えば、従業員のトレーニング、法規制の調査、広報、製品開発、ベンダー管理などの分野に配分することが挙げられる。また、予算を、COO、CTO、CISOなど、上層部のための人材評価や後継者育成計画に割り当てることも考えられる。後継者の準備状況を評価したり、将来これらの役職に就けるよう現在の従業員に追加のトレーニングが必要かどうか、あるいは、外部から人材を採用した方がよいかどうかを判断したりすることにより、企業のサイバー攻撃に対する準備態勢は向上する。企業は、人材評価を行うことで従業員の離職に起因する混乱を最小限に抑えることができる。

出典：インターネット・セキュリティ・アライアンス [43]

42 監査等委員会設置会社の場合は監査等委員会、指名委員会等設置会社の場合は監査委員会と読み替える。
43 Internet Security AllianceおよびAmerican National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (Washington, DC: ANSI, 2010）より作成。Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: ISA, 2013) も参照のこと。

鍵となる上層部の役割と責任

企業はそれぞれ独自の管理構造を持ち、肩書や役割、責任にも違いがある。しかし、組織横断的なサイバーリスク管理チームを設置する場合はとりわけ、経営陣の役割と責任を明確に定めておくことが有益である。以下に、役割とそれに伴う責任の例を示す。

- 最高リスク責任者（Chief Risk Officer）―サイバーリスクの検出、予防、軽減、トレーニングおよびコミュニケーション
- 最高コンプライアンス（・倫理）責任者（Chief Compliance（& Ethics） Officer）―ポリシーの策定・執行、トレーニングおよびコミュニケーション、調査
- 最高法務責任者／法律顧問（Chief Legal Officer/General Counsel）―法規制の認識、コンプライアンス、ポリシー、訴訟、調査
- 最高プライバシー責任者（Chief Privacy Officer）―プライバシー関連法・規則に関する深い知識、ポリシーの策定・執行、トレーニングおよびコミュニケーション、プライバシーに関する監査（注：代案として、この機能は、最高コンプライアンス責任者の担当に組み入れてもよい。）
- 外部弁護士（Outside Legal Counsel）―外部からの法的支援（必要な場合）、弁護士・依頼者間の秘匿特権、調査、政府・規制当局との交渉代表者

原　則　5

サイバーリスクに関する取締役会における議論の内容として、回避すべきリスク、許容するリスク、保険等によって軽減・移転すべきリスクの特定や、それぞれのリスクへの対処方法に関する具体的計画等を含めるべきである。

完全なサイバーセキュリティの確保は非現実的な目標である。通常のセキュリティと同様、サイバーセキュリティは、継続的な課題であり、終わりのあるものではない。セキュリティとコンプライアンスは同じではない。取締役会は、幅広いリスクのどの部分において、自社の経営・管理が最適化されていると考えているのかを判断する必要がある。また、他のリスク分野と同様、サイバーリスク許容度についても、自社の事業戦略や目標との整合性が保たれていなければならない。企業がサイバーリスクの分析を行う場合、全体のリスク評価を行うなかでサイバーリスクの分析を行い、サイバーリスクを他のリスクとの関連で適切に位置付けることが必要である。リスクレジスターは、そうしたプロセスに役立つ可能性がある[44]。セキュリティに関するリソース配分は、ビジネス目標とデジタルシステムに内在するリスクとのバランスを保つための機能である（「リスク許容範囲の定義」（32ページ）参照）。サイバーリスクは複数あり、それらに対処する方法も複数ある。サイバーセキュリティ担当取締役または担当部門は、取締役会に対し、リスクの現状とそれに対処するための計画について、その全体像を明確に提示する必要がある。そのため、取締役会とサイバーセキュリティ担当取締役または担当部門は、以下の問題に取り組む必要があるだろう。

- **無くなっても、あるいは、侵害を受けても構わないデータ、システム、事業活動はどれか?**

  リスク許容範囲に関する議論は、ビジネス上の実務的な留意事項として企業が受容可能なサイバーリスクのレベルを特定するうえで役立つ。これに関連して、最初の重要なステップは、基幹業務データや機密性の高いデータ（企業が保有する重要資産および非常に機密性の高いカテゴリーに属するデータの特定（15ページ）参照）と、同様に重要ではあるが必要性や機密性がそれほどは高くない、その他のデータまたはシステムを区別することである。しかし、データ漏洩はサイバーリスクを構成する唯一の要素ではない。データ漏洩に対する規制上の制裁措置など、その法的意味がデータの実際の価値を大きく上回る場合も考えられる。また、広報のまずさによるレピュテーションリスクは、侵害を受けたシステムの実際の価値よりも、むしろ外部要因の影響を受ける可能性の方が高い。

44 欧州ネットワーク情報セキュリティ庁（ENISA）によると、リスクレジスターとは、リスクを把握、説明、評価するためのツールである。特定されたリスクとともに、リスクのアカウンタビリティ、対応措置（必要な場合）、レビューの日付、対応措置が完了しリスク項目をクローズした日付が記載されている。リスクレジスターは、取締役会がサイバーリスクの大きさを企業のプロファイルに照らして定量化する上で役立つ重要なツールである。企業にいくつかのリスクがあり、サイバーリスクが上位10位に含まれている場合、取締役会が費やす時間と予算を増やす必要がある。しかし、サイバーリスクがないならば、少しは気を休めることができる。リスクレジスターは、自社が影響を受ける可能性のある有害事象のポートフォリオを文書化するために使用すべきである。

- **サイバーリスクを軽減するための投資は、基本的な防御と高度な防御とで、どのように配分すべきか?**
  より高度な脅威に対処する方法を検討する際、取締役会は、企業が保有する最重要データおよびシステムを保護するために設計された高度な防御を最も重視すべきである。大半の企業は、こうした考え方に原則として同意するものの、実際には、企業の多くが全てのデータおよび機能に対してセキュリティ対策を等しく適用している。しかしながら、受ける影響の小さいシステムやデータを高度な脅威から保護するためには、それによって保証される利益を上回る投資が必要になる可能性があることが、研究によって実証されている。これらの優先度の低い資産については、防御のコストが利益を上回る可能性があるため、より優先度の高い資産よりも許容するセキュリティリスクのレベルを上げること、あるいは、代替案として、企業はそうしたリスクの影響を保険によって移転することを検討すべきである[45]。

- **特定のサイバーリスクを軽減するうえで役立つ、利用可能なオプションはどのようなものか?**
  企業は、業界や規模に関わらず、サイバーリスクの部分的な軽減に役立つエンドツーエンドソリューションを利用することができる。そうしたソリューションには、セキュリティの枠組みやガバナンス手法の評価、従業員トレーニング、ITセキュリティ、専門家対応サービス、管理セキュリティサービスなど、一連の予防措置も含まれる。これらのツールは、財務上の損失をカバーするだけではなく、サイバー攻撃に起因して企業が被る物的損害や人身被害のリスクを軽減するうえで役立つ。また、一部のソリューションには、さらなる防御や専門知識の追加を目的とした、予防的ツール、従業員トレーニング、ITセキュリティ、専門家対応サービスの利用も含まれる。こうした付加価値サービスが含まれていることは、サイバーセキュリティをIT部門から切り離し、全社的なリスクおよび戦略に関する取締役会レベルでの議論に移すことの重要性がさらに一層高まっていることを証明している。しかし、サイバーセキュリティ担当取締役または担当部門は、目まぐるしく変化するサイバーリスクの状況を取締役会に知らせ、データの盗難、破損、破壊、さらにはセキュリティメカニズム（例：暗号化）を悪用した攻撃方法（例：ランサムウェア）など、急速に変化する技術やサイバー攻撃シナリオに迅速に対応できるよう備えておく必要がある。

- **特定のサイバーリスクのリスク移転に役立つ、利用可能なオプションはどのようなものか?**
  サイバー保険は、サイバーセキュリティ上のインシデントに関連して不測の損失が生じた場合に、それを金銭的に補償するためのものである。補償対象となるものの例として、暗号化されていないノートパソコンの紛失などによるデータの漏洩や、フィッシング詐欺、マルウェアの感染、DoS攻撃など、外部からの悪意ある攻撃などがあ

45 AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013, p.8.

る。保険会社は、引受プロセス中に、企業のサイバーセキュリティの枠組みについて、詳細なレビューを頻繁に行う。また、保険料の設定は、自社のサイバーセキュリティの長所・短所を理解するうえで役立つ強力な示唆を与えてくれる可能性がある。保険会社の多くは、テクノロジー会社、法律事務所、広報会社等と提携することによって、上記の予防措置へのアクセスも提供している。

- **サイバーセキュリティインシデントの影響は、どのように評価すればよいか?**
  関係する要素の数が非常に多いことから、インシデントの影響評価を適切に実施するのには困難が伴う。相互に接続された世界では、企業にとってのサイバーリスクは、企業が直接的かつ効果的にリスクを軽減できないところに存在する可能性がある。例えば、データ漏洩に関する広報や風評が、リスク評価プロセスを非常に複雑化してしまう場合がある。関係者（従業員、顧客、サプライヤー、投資家、報道機関、一般市民、政府機関など）は、比較的小規模な侵害と大規模かつ危険な侵害との違いが分からない、あるいは認識していない場合がある。その結果、風評被害やそれに伴う影響（メディア、投資家、その他の主要関係者の反応を含む）が、実際に起こった事象の規模や深刻度と全く釣り合わないという場合もある。取締役会は、サイバーリスク管理のための企業戦略（業務上のIT管理を含む）を策定するうえで、これらの影響について慎重に考慮すべきである。また、パートナーやベンダーとの法的取決めなど、適切なセキュリティの確保に役立つ戦略や、事象が発生した場合のレピュテーションリスクに対処するためのコミュニケーションプランを含めるという点についても、確保に努めるべきである。

リスク許容範囲の定義

リスク許容範囲とは、戦略目標を追求するなかで、企業が受け入れてもよいと考えるリスクの量を指す。したがって、それを上回った場合には、適切な措置を講じて、リスクを許容できるレベルに軽減する必要があり、リスクのレベルを定義すべきである。リスク許容範囲が適切に定義・伝達されれば、ビジネスを行い機会を捉えていくなかで、ある種の境界が定まり、行動がコントロールされるようになる。

リスク許容範囲に関する議論においては、以下の論点を取り挙げるべきである。

- 企業価値—決して受け入れられないリスクはどのようなものか？
- 戦略—どのようなリスクは受け入れる必要があるのか？
- 関係者—どのようなリスクをどの程度のレベルまで負うつもりがあるのか？
- キャパシティ—これらのリスクを管理するためにはどのようなリソースが必要か？
- 「リスク許容範囲は、企業それぞれの固有の状況および目標に基づいた判断の問題である。どこでも通用する「万能薬」は存在しない。」

出典：PwC, Board oversight of risk: Defining risk appetite in plain English (New York, NY: PwC, 2014) , p.3.

ま と め

サイバーセキュリティは、企業全体にとっての重要なリスク管理上の課題であり、ほぼすべての企業活動のあらゆるレベルに影響を及ぼす。また、脅威の複雑さと変化のスピード、財務・競争力・レピュテーションに大きな損害を与える可能性、完全な保護が目標として非現実的であるという事実など、いくつかの特徴が組み合わさり、脅威の性格は、とりわけ厄介なものとなっている。このような脅威を前にして、民間企業によるサイバーセキュリティ対策にかける費用は劇的に増加しているが[46]、それでもなお、サイバーセキュリティの経済原理は攻撃者に有利である。さらに、多くのビジネス・イノベーションに伴って脆弱性が増大するなか、リスク管理全般、とりわけサイバーセキュリティ対策は従来、大半の企業においてコストセンターであるとみなされてきた。

取締役は、自らが担っている受任者責任の観点から、また経営活動の監督という観点から、自らのサイバーセキュリティ対処能力を継続的に評価する必要がある。多くの場合、評価を通して、不足している部分と改善の余地が特定されるだろう。採用する手法は、個々の取締役会によって違いがあると考えられるが、本ハンドブックに示した各原則は、ベンチマークおよび出発点案となるであろう。取締役会は、以下のように、全社的な見地からサイバーリスクに取り組むよう努めるべきである。

- **企業にとって、また取締役会自体にも波及する可能性のある法律上の問題を理解する。**
- **十分な情報に基づいて議論ができるように、取締役は議題に十分な時間を割くとともに、専門情報を入手できるようにする。**
- **サイバーリスクの問題は、企業の全体的リスク許容度という文脈の中で議論する。**

サイバーセキュリティは、ビジネス活動のデジタル化に伴い、企業が今後長きにわたって直面していく課題である。企業が成長を指向し、ビジネスのデジタル化を進めて行くなかで、サイバーセキュリティの課題から逃れることはできない。得てして、サイバーセキュリティはビジネス活動に対するブレーキ役であるかのように受け止められるが、そうではなく、デジタル技術を活かして企業を成長させていくうえでの重要な手段と位置付けたいと思う。そのためには、杓子定規なルールや利用制約を設けるのではなく、それぞれの企業が持つ固有の文化に根ざしたバランスの良いサイバーセキュリティの取組みを実施することが必要である。大きなインシデントを起こすと、「二度と起こしてはならない」という思いが非常に大きなプレッシャーとなり、固有の企業文化に即した取組みとは比べ物にならない、がんじがらめの対策ができあがってしまう可能性すらある。であるからこそ、大きなインシデントが起きる前に、100%の防御を狙うのではなく、インシデントは必ず起こるという前提に立って、被害最小化を目的に、自社の文化を尊重し、バランス感のある、企業力を最大化するセキュリティ対策に取り組んでいく必要がある。取締役会は、そうした観点から「正しい質問」を発し、セキュリティ担当取締役や担当部門に対し、効果的なガイダンスを提供することが求められる。

46 Steve Morgan, "*Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020,*" Forbes, Mar. 9, 2016. Piers Wilson, Security market trends and predictions from the 2015 member survey, Institute of Information Security Professionals も参照。

付 属 資 料

本ハンドブックでは、実務で活用いただくためのツールを付属資料として4つ収録している。米国版ハンドブックにはより多くのツールが収録されているため、適宜ご参照いただきたい。

付属資料 A
取締役自身のセルフチェック10個の質問

取締役会の場でなくても、取締役は技術・運用だけでなく、サイバーセキュリティの様々な側面を全体的に検討したかどうか、自己評価を行うことができる。とくに、取締役会は、サイバーセキュリティをビジネスの観点から考え、戦略的なレベルで組織の準備が進められているかどうかを検討しておくべきである。取締役が自らに問いかけるべき質問としては以下が挙げられる。

1. 新たなサイバー脅威に関し、社長やCEOは、取締役間で、社内での、あるいは、外部の情報源とのオープンな情報交換を奨励しているか?
2. 自社にとって最も価値の高い情報資産は何であると考えているか? ITシステムは、これらの資産と、どのように関わり合っているのか?
3. M&A、パートナーシップ、新製品の発表など、ビジネス上の主要な意思決定において、サイバーセキュリティの側面を適時に検討しているか?
4. 自社の保有する重要資産やその他の機密性の高いデータを誰かが狙っていたと仮定して、これを撃退できるだけの十分な対策が講じられているか?これらの資産またはデータが保護されていると確信するためには、どうすればよいか?
5. サイバーセキュリティツールやトレーニングへの支出は適切に行われているか? 支出の費用対効果を正しく評価しているか? セキュリティが実際に向上しているのか、それとも、ただコンプライアンス要件を満たしているだけか?
6. 自社のサイバーセキュリティ管理は誰が行っているのか? サイバーセキュリティに関して、(i) 適切な人材が配置されているか? (ii) 報告経路、アカウンタビリティまたは責任が明確になっているか? (iii) 自社のリスクレジスターにサイバーリスクが含まれているか?[47]
7. 事象発生時において、一般市民、株主、規制当局、格付機関等とどのようにコミュニケーションするかについて検討したか? 上記のコミュニケーションの対象者別に個別の戦略を策定しているか?
8. 自社は、公共または民間セクターのエコシステム全体を対象とした、何らかのサイバーセキュリティ・情報共有機関に参加しているか? 参加すべきか?
9. 自社は、現在および将来可能性があるサイバーセキュリティ関連法規制について十分なモニタリングを行っているか?[48]
10. 自社はサイバーセキュリティインシデントをカバーする十分な保険（取締役および役員を含む）に加入しているか? カバーされているものは、具体的に何か?[49] リスク移転以外に、保険に加入するメリットはあるか?[50]

47 Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.
48 Ibid.
49 StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
50 Ibid.

付属資料 B
NISTサイバーセキュリティフレームワークと「特定・防御・検知・対応・復旧」

オバマ政権期の大統領令に基づき、米国商務省傘下の国立標準技術局（National Institute for Standards and Technology: NIST）が産業界や各種標準団体、学会などの意見を聴取して、2014年2月にNISTサイバーセキュリティフレームワークを公表した。和訳は独立行政法人情報処理推進機構（IPA）のWebサイトで入手できる。最新版は2018年2月に公表された1.1版である。

元々は重要インフラ企業向けのものとして作成されたが、重要インフラ企業以外でも有用であることが認められ、米国政府によるサイバーセキュリティ政策の中心的役割を果たし始めている。

特定、防御、検知、対応、復旧の5つのステップ（正式にはファンクションと呼んでいる）、それを細分化した23のカテゴリー、108のサブカテゴリーを規定し、何に取り組むべきかを記載している。その使い方は、記載内容の実施をすべて求めるものでなく、何をどこまで目指すかを各組織が自主的に定め、現状について評価を行い、その結果と照らして向上のアクションを採っていくという、そうした使い方を想定している。そのため、あくまでフレームワークであり、基準やガイドラインではない。

NISTのWebサイトには金融、通信、IT、石油などの企業による、業界別の応用例、利用実例が多数公表されている。NISTは本フレームワークのグローバル展開にも熱心に取り組んでおり、欧州、中国、日本などにスタッフを派遣し説明会を開催している。日本でも2014年の経団連主催の説明会以来、複数回、NIST担当官による説明会やワークショップが開催されている。

以下では、NISTサイバーセキュリティフレームワークの中で取締役が知っておくと役に立つと思われる、特定・防御・検知・対応・復旧の5つのファンクションについて説明したい。

特定（Identify）

自社のミッションや目的に照らして、何を守るべきかの優先順位を明らかにし、ガバナンスやプロセスを整備することを意味する。

防御（Protect）

技術的ソリューションの導入や運用だけでなく、入退室管理のような物理的アクセス制御、トレーニングといった人的防御の実施も含む。

検知（Detect）

異常が起こった時、適時に検知してその影響範囲を把握すること、そのために継続的にモニタリングを行なうことを意味する。

対応（Respond）

異常を分析し、影響の緩和策や拡大防止策、根絶策を、内外の関係者と連絡を取りながら進めることを意味する。

復旧（Recover）

異常によって影響を受けた資産やシステムを速やかに復旧させることを意味する。被害者やその他の利害関係者との調整も含む。

付属資料 C
「サイバーリスク・ヒートマップ」を活用したリスク管理

取締役は、経営で管理するリスクの1つとして、サイバーリスクについても理解すべきである。とくに、事業継続や事業目標達成の阻害要因となりうるサイバーリスクについては、自社が攻撃を受ける可能性（サイバー攻撃のトレンド）に注目し、また、攻撃を受けた場合のビジネスへの影響を理解しておくことが必要である。

例えば、Eコマースを行う企業にとっては、DDoS攻撃によりウェブサーバーがダウンすることは、事業目標達成に大きな影響を与えることになる。また、顧客情報の漏洩は、企業の信頼失墜・顧客離れに直結する。このようなビジネスインパクトの大きいリスクに対して、優先度を上げて対策を行うことが必要である。

一方で、サイバー攻撃が日々高度化・巧妙化するなか、100%防御することは不可能である。すなわち、100%を目指してサイバーセキュリティ対策を講じるのではなく、攻撃を受ける可能性が低く、または影響が経営に深刻な影響を与えないのであれば、「リスクを受容する」ことも経営として判断すべきである。

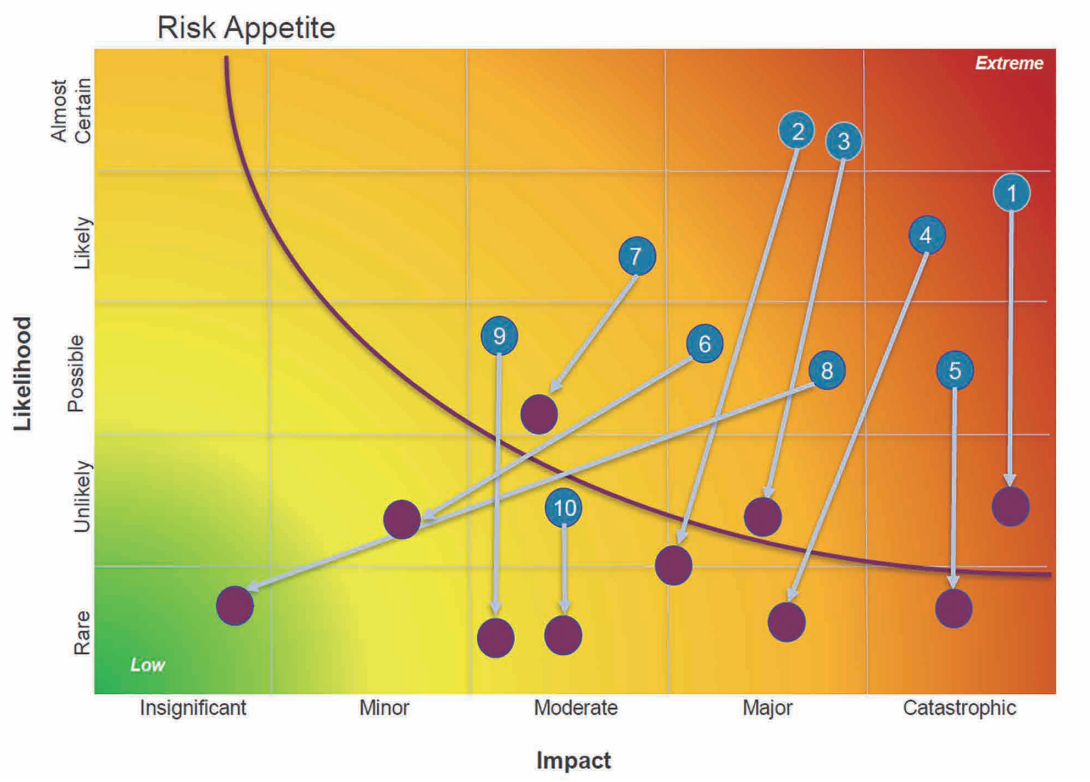
このように、優先度をつけた対策を行うためには、サイバーリスクを見える化し、全体像を把握することが重要である。このために、下記の「サイバーリスク・ヒートマップ」を用いる事が有効である。

「DDoS攻撃」「ランサムウェア」「標的型攻撃」など、サイバー攻撃による自社への影響を「発生確率」と「業務影響」の2軸で評価してプロットする。図の左下に行くほどリスクが低く、右上ほどリスクが高いことを示している。取締役会は、どこまでならリスクを受容できるかを議論し、リスク許容範囲を定める。

併せて、サイバーセキュリティ対策チームから、実施可能な対策、必要な費用、その効果の提案を受け、対策を実施した場合にどこまでリスクを低減できるかをプロットする。

ヒートマップを作成したら、リスクが高く受容できないものから優先的にリソースを配分し、セキュリティ対策チームに施策実施を指示する。

なお、ヒートマップを使う際に大切なことは、精緻さを求めすぎないことである。ヒートマップの目的は、リスクの洗い出し、その相対評価を通じた優先付け、経営方針にマッチしたリソース配分である。「発生確率」や「業務影響」の定量化に過度な正確さを求める必要はない。


Risk Appetite
Extreme
Low
Likelihood
Almost Certain
Likely
Possible
Unlikely
Rare
Insignificant
Minor
Moderate
Major
Catastrophic
Impact
1
2
3
4
5
6
7
8
9
10

付属資料 D
サイバーセキュリティに関する取締役会の姿勢・文化に関する評価

2010年、米国の『取締役会評価に関するNACDブルーリボン委員会レポート（Report of the NACD Blue Ribbon Commission on Board Evaluation）』は、取締役会の文化を「取締役会におけるコミュニケーション、相互作用、意思決定の根底を成すとともに、それらを方向づける、共有された価値。物事を実際に進めるうえでの本質」と定義した[51]。5年後、全米取締役協会（NACD）が開催した第1回グローバルサイバーサミット（Global Cyber Summit）においては、フォーチュン・グローバル500（Fortune Global 500）に関係する取締役やサイバーセキュリティの専門家が200人以上集まり、経営陣によるサイバーセキュリティへの取組みを支える、または妨げる、取締役会の文化のいくつかのあり方について議論した。参加者のひとりは、次のように語っている。

取締役会は考え方を変える必要がある。「攻撃される可能性はどの程度か」と問いかけるのではなく、むしろ「既に攻撃されている可能性が高い」と認識すべきであり、サイバーセキュリティをコストとみなすのではなく、自社の競争力を保つための投資として考えるべきであり、経営陣にサイバーの脅威の予防・防御を期待するのではなく、どの程度迅速に脅威を検知し対処できるのかを尋ねるべきなのである[52]。

取締役が、取締役の自己評価にサイバーセキュリティの要素を取り入れたいと考えた場合、出発点として、次表の質問を使用するとよい。評価は、1が最も低く、5が最も高い。

数値尺度を用いて、取締役会の文化が概ね以下の数値範囲のどこに該当するかを示す。							アクションアイテム
取締役会は、サイバーセキュリティを、主として、IT/技術の問題と考えている。	1 □	2 □	3 □	4 □	5 □	取締役会は、サイバーセキュリティを、全社的なリスク管理の問題と理解している。	
取締役会は、サイバーセキュリティの法的環境が概ね安定しており、大半の企業に同じように適用できると信じている。	1 □	2 □	3 □	4 □	5 □	取締役会は、事業計画・環境の変化に合わせて、サイバー関連の新たな法的状況に関し、定期的に法律顧問に意見を求める必要があると認識している。	
取締役会は、サイバーセキュリティに関する最新情報を、当該分野の専門家から定期的に入手する必要性を感じていない。	1 □	2 □	3 □	4 □	5 □	取締役会は、自社の新たなサイバーニーズや脅威の状況に応じて、サイバー関連の専門知識を定期的に求めている。	
取締役会は、サイバーリスク管理の具体的計画を立案する必要性を感じていない。	1 □	2 □	3 □	4 □	5 □	取締役会は、最新のデジタル技術の影響、ならびに、自社のビジネスニーズやリスクとの整合性がとれた技術管理方法を反映した、運用・管理の枠組みの立案を行っている。	
取締役会は、サイバーリスクを独自に評価し管理していない。	1 □	2 □	3 □	4 □	5 □	取締役会は、自社が抱えるサイバーリスク、許容するリスク、軽減できるリスク、移転できるリスクを事業目標に照らして分析している。	

51 *Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness* (Washington, DC: NACD, 2010), p.7.

52 引用部分は、2015年4月15～16日にワシントンDCで開催されたグローバルサイバーサミットの参加者の言葉。議論は、チャタムハウス（王立国際問題研究所）ルール（Chatham House Rule）に則って実施された。

制作・編集協力

インターネット・セキュリティ・アライアンス（Internet Security Alliance）

インターネット・セキュリティ・アライアンス（ISA）は、2000年に設立された、サイバーセキュリティに特化する国際的な業界団体です。ISA理事会は、国際企業に所属する主要なサイバーセキュリティ担当者によって構成され、実質的に経済の全部門を代表しています。ISAのミッションは、経済と先進技術や政府政策とを統合し、セキュリティが持続的に確保されたサイバーシステムを構築することです。2014年、ISAは『企業の取締役向けサイバーリスクハンドブック（Cyber Risk Oversight Director's Handbook）』初版を作成、企業の取締役会がサイバーリスク管理において果たすべき独自の役割について具体的に取り挙げました。プライスウォーターハウスクーパース（PricewaterhouseCoopers: PwC）は、同社が毎年実施している『グローバル情報セキュリティ調査（Global Information Security Survey）』において、同ハンドブックが企業取締役会に広く採用され、使用された結果、サイバーセキュリティ予算立案の改善、サイバーリスク管理の向上、サイバーセキュリティと全体的なビジネス目標との整合性の向上、利用企業におけるセキュリティ文化の創出支援が図られたと記しました。ISAについて詳しくは、www.isalliance.org をご参照ください。

一般社団法人 日本経済団体連合会

経団連は、日本の代表的な企業1,412社、製造業やサービス業等の主要な業種別全国団体109団体、地方別経済団体47団体などから構成されています（2019年4月1日現在）。その使命は、総合経済団体として、企業と企業を支える個人や地域の活力を引き出し、日本経済の自律的な発展と国民生活の向上に寄与することにあります。このために、経済界が直面する内外の広範な重要課題について、経済界の意見を取りまとめ、着実かつ迅速な実現を働きかけています。

経団連のサイバーセキュリティ委員会は、2019年に新設され、Society 5.0の前提となるサイバーセキュリティを確保するために、経営者の意識向上をはじめとした、サイバーセキュリティ強化に向けた取組みの検討を行っています。詳しくは、www.keidanren.or.jp/ をご参照ください。

日本電信電話株式会社（NTT）

NTTグループは、国内各事業会社においては移動通信、地域通信、長距離・国際通信、データ通信およびシステムインテグレーション等の事業を展開し、またグローバルにはネットワーク、サイバーセキュリティ、マネージドIT、アプリケーション、クラウド、データセンター等を、様々な業種に精通したビジネスコンサルティングサービスと組み合わせて提供し、お客さまの事業の成長と競争力の強化に貢献しています。世界のトップ5に入るICTサービスプロバイダーとして、NTTグループはGlobal Fortune 100のうちの80社以上を含む数千社のお客さま、およびパートナーと共に、お客さまの事業目標の達成や、将来に向けて持続可能な成長の実現を目指しています。詳しくは、ntt.co.jp をご参照ください。

株式会社日立製作所

日立は、OT（Operational Technology）、IT（Information Technology）およびプロダクトを組み合わせた社会イノベーション事業に注力しています。2018年度の連結売上収益は9兆4,806億円、2019年3月末時点の連結従業員数は約296,000人でした。日立は、モビリティ、ライフ、インダストリー、エネルギー、ITの5分野でLumada（ルマーダ）を活用したデジタルソリューションを提供することにより、お客さまの社会価値、環境価値、経済価値の3つの価値向上に貢献します。 詳しくは、日立のウェブサイト（http://www.hitachi.co.jp）をご覧ください。

経団連
Keidanren

INTERNET SECURITY ALLIANCE

サイバーリスクハンドブック

取締役向けハンドブック　日本版