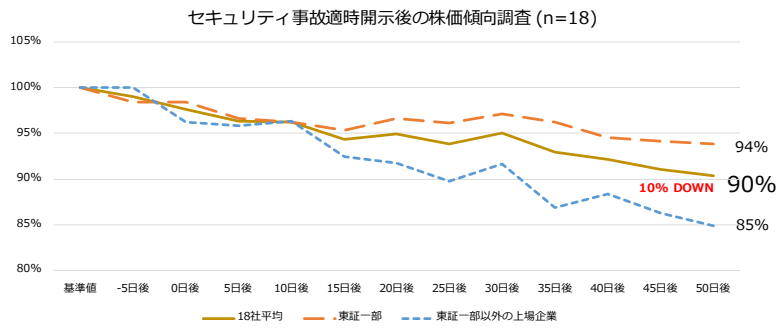
2018 年 9 月

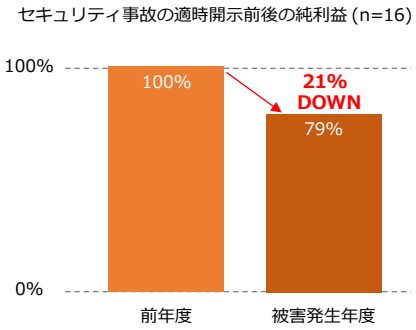
取締役会で議論するためのサイバーリスクの数値化モデル
～サイバーリスクの金額換算に関する調査～

【要旨】

- サイバー犯罪が世界経済に与える損失額は、2014 年には約 47 兆円であったが、2017 年には 3 割増の約 63 兆円（GDP の 0.8%に相当）までに増加したとされる [1]。日本においても、サイバー犯罪によって年間 1 兆円前後の経済損失が発生していると考えられる。

- 日本国内で情報流出等の適時開示を行った企業を JCIC が調査したところ、株価が平均 10%下落し、純利益が平均 21%減少していることが分かった。また、数百億円もの直接的被害を受けた企業、経営者が報酬を返上した企業も存在する。公表されたセキュリティ事故は氷山の一角であり、全ての企業がリスクに晒されている。もはや、サイバーセキュリティは IT 部門だけの問題ではなく、企業経営の持続的成長を揺るがす経営リスクである。





- 経営リスクに対する監督機能である取締役会において、日本企業は海外企業に比べサイバーリスクを議論し、対策を検討できていない現状がある。改正会社法によって強化された取締役会の責務とサイバーリスクの高まりという 2 つの側面から、日本企業もコーポレートガバナンスの一環でサイバーリスクを議論すべき段階にある。

- また、政府も取締役会でのサイバーリスクの議論を推進する必要がある。デジタル化とサイバーセキュリティは、2020 年に名目 GDP600 兆円経済の実現を目指す日本の成長戦略に欠かすことのできない課題であるという認識のもと、日本政府は企業の取締役や経営者に対するサイバーリスクの啓発を促進すべきである。

【取締役会でサイバーリスクを議論するために求められること】

1. コーポレートガバナンス・コードへのサイバーリスク記載

上場企業のコーポレートガバナンス報告書にサイバーリスクに関する考え方や整備状況を記載するよう促進する必要がある。その際には、金融庁、経済産業省、日本取引所グループ等が協力することが必須である。

2. サイバーリスクの数値化モデル

取締役や経営者等が事業リスクを共通で理解できる「サイバーリスクの数値化モデル」を標準化し、経営視点でサイバーリスクを把握できるようにする必要がある。「数値化モデル」については、このレポートで例示した。

3. 取締役、監査役、投資家、経営者等への啓発

マネージメント層やステークホルダー等が正しくサイバーリスクを理解するために、取締役関連団体や経済団体等を通じて各種セミナーや広報活動、トレーニングプログラムにより啓発する必要がある。

[1] CSIS and McAfee「Economic Impact of Cybercrime 2018」https://www.csis.org/analysis/economic-impact-cybercrime

1. 経営リスクとしてのサイバーリスク

企業内でサイバーセキュリティを議論する場合、新たな脆弱性が発見された、新たな攻撃手法が増加している等の技術的な観点での議論に終始しがちである。しかし、企業経営者の立場からすると、技術動向は重要であるが、自社の経営にどの程度の金銭的影響が発生し、経営責任はどの程度発生する可能性があるのかということに関心があるはずだ。経営の観点からサイバーリスクを議論するためには、経営者の共通言語である財務諸表を用いてリスクの金額換算を行い、IT に詳しくなくともリスクを把握できるようにする必要がある。

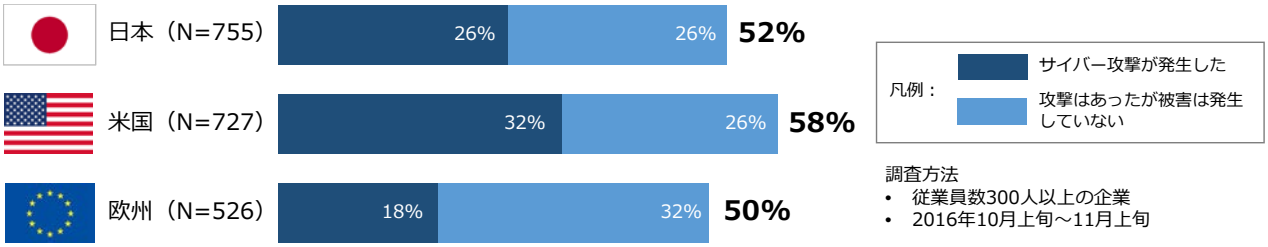
図表 1 は、近年サイバー攻撃によって発生したセキュリティ事故の例である。1 回のサイバー攻撃によって大規模な金銭的損害が発生し、経営者責任が問われているケースが世界で発生していることがわかる。

図表 1　金銭的被害が発生したセキュリティ事故の例（公開情報をもとに JCIC 作成）

#	公表時期（昇順）	国・地域	組織名	金銭影響	インシデント種別	説明
1	2013/12/15	米国	小売り	**70億円**	不正アクセス	顧客のクレジットカード情報がPOS 端末から流出し、同年4半期の利益は前年比46%も落ち込んだ。その後、CEOとCIOが辞任。
2	2014/7/9	日本	教育	**260億円**	内部犯行	約3504万件の情報漏えいが発生し、情報セキュリティ対策費260億円を特別損失として計上。純利益は前年同期比82.2%減。
3	2015/6/1	日本	公共機関	**10億円**	マルウェア感染	標的型攻撃によって職員のパソコンが感染し、約125万件の個人情報の漏えいが発生。
4	2016/2/4	バングラデシュ	銀行	**1080億円**	マルウェア感染	サイバー攻撃により銀行端末から海外の外貨準備金口座に対し、不正送金が発生。
5	2017/6/28	米国	製薬	**360億円**	ランサムウェア	ランサムウェアに感染し、のコンピューターネットワークが侵害された。
6	2017/8/16	デンマーク	運輸	**330億円**	ランサムウェア	ランサムウェアによって同社の4カ国の拠点が被害にあい、数週間にわたり輸送の遅延などの混乱。
7	2017/12/10	米国	運輸	**440億円**	ランサムウェア	「NotPetya」と呼ばれるランサムウェアに感染し、運送システムに大規模な影響が発生した。
8	2017/12/20	日本	航空	**3.8億円**	ビジネスメール詐欺	取引先を装ったメールで旅客機のリース料等の振込先を変更するよう依頼され、偽の銀行口座に約3億8000万円を振り込んだ。
9	2018/1/26	日本	仮想通貨取引所	**580億円**	不正アクセス	サイバー攻撃により仮想通貨NEMが流出。その後、ネット証券会社が36億円で同社を子会社化。
10	2018/4/24	米国	ネット事業	**38億円**	不正アクセス	数億件もの情報流出を2年間公表せず、投資家に不利益を与えたとして38億円の制裁金をSECへ支払うよう要請。
11	2018/4/25	米国	信用調査	**260億円**	不正アクセス	サイバー攻撃によって1.4億人分の情報が流出。同社のCEO、CIO、CSOは辞職した。
12	2018/5/16	日本	ゲーム	**34億円**	不正アクセス	VPNアクセス経由の不正アクセスを受けて、13タイトルのオンラインゲームが停止。代表取締役社長が1年間無報酬になると発表。

公表されているセキュリティ事故は氷山の一角であり、全ての企業がリスクに晒されていると言える。独立行政法人情報処理推進機構（IPA）が行った調査によると、日本だけではなく、米国や欧州でも 5 割以上の企業が過去 1 年間にサイバー攻撃が発生していたと答えている（図表 2）。

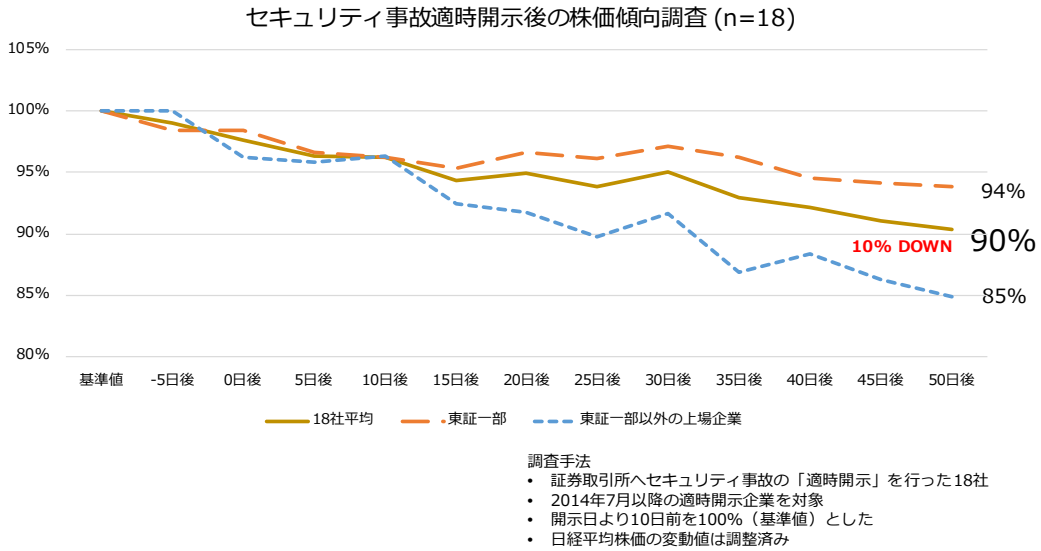
図表 2　前年度にサイバー攻撃が発生した企業（IPA 調査 [2]をもとに JCIC 作成）



[2] https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

セキュリティ事故等の適時開示を行った日本の 18 社の株価傾向を JCIC が調査したところ、適時開示後 50 日後には株価が平均 10%減少していることが分かった（図表 3）。東証一部以外の企業（東証二部、ジャスダック、マザーズ、札証）の平均下落率は 15%であることから、セキュリティ事故は中小企業への株価影響が大きいと言える。中小企業のビジネスが特定事業に依存しており、その事業へのサイバー攻撃による影響は大企業に比べて大きいことが理由であると考えられる。

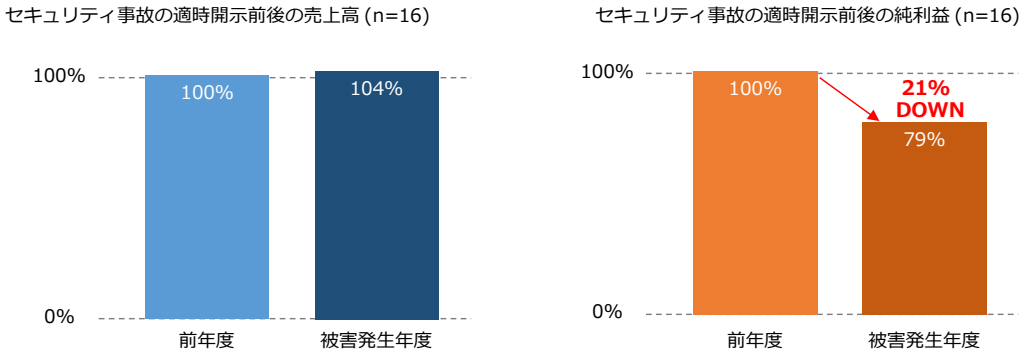
図表 3　セキュリティ事故の適時開示後の株価影響（証券取引所の株価データをもとに JCIC 作成）



調査手法
- 証券取引所へセキュリティ事故の「適時開示」を行った18社
- 2014年7月以降の適時開示企業を対象
- 開示日より10日前を100%（基準値）とした
- 日経平均株価の変動値は調整済み

更に、セキュリティ事故等の適時開示を行った日本の 16 社の売上高と純利益を調査したところ、売上高は平均 4%上昇したが、純利益は平均 21%減少していることがわかった（図表 4）。純利益が大幅に減少した理由は、事故対応調査や再発防止のための特別損失が発生したことが主な理由である。

図表 4　セキュリティ事故の適時開示後の売上と純利益の傾向（企業業績データをもとに JCIC 作成）



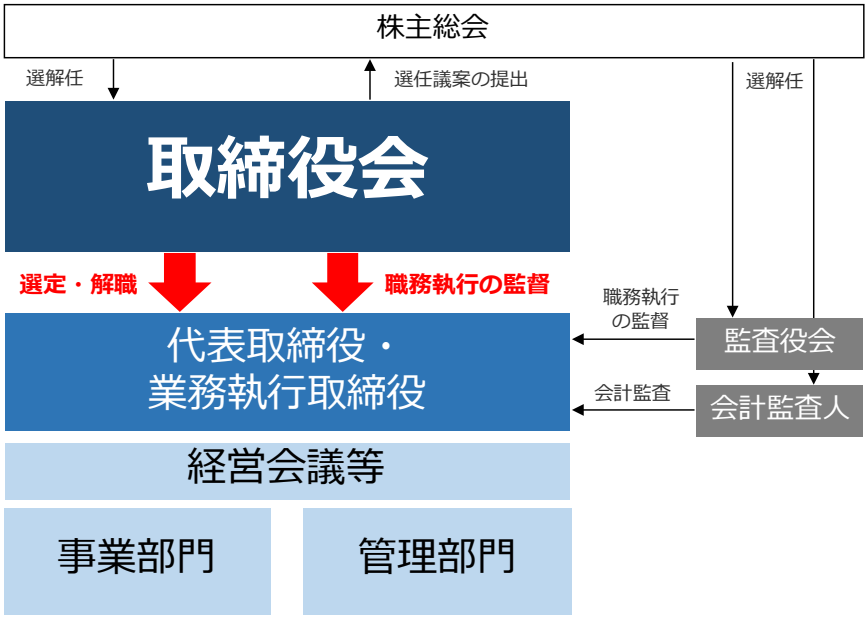
調査手法
- 証券取引所へセキュリティ事故の「適時開示」を行った16社
- 2014年7月以降の適時開示企業を対象
- 上場直後で過去決算データのない企業（2社）は調査の対象外とした
- 被害前年度の売上高と純利益を100%とした

このように、サイバー攻撃により、企業の株価が低下し、純利益も減少する傾向にある。その結果として、経営者の責任が問われるようになり、報酬を返上したり、辞任したりするケースも発生している。これらのことから、サイバーセキュリティを IT 部門だけに任せるのではなく、経営リスクとして経営者自らが積極的に取り組む必要がある。

2. 取締役会でサイバーリスクを議論していない日本企業の現状

2015 年 5 月、日本においてコーポレートガバナンス（企業統治）の強化等を目的とした改正会社法が施行した。この改正により、経営リスクに対する取締役会の監督機能が強化された（図表 5）。取締役会は原則として毎月開催し、議事録を作成することが求められ、個々の取締役の経歴、報酬の妥当性、役員数の妥当性、経営リスクの管理、さらには次世代の役員候補が育成されているか等についても議論されることになった。また、この取締役会が適切に運営されているかを評価する「取締役会の実効性評価サービス」を行う監査法人やコンサルティング会社も登場している。

図表 5 改正会社法によって強化された取締役会の責務

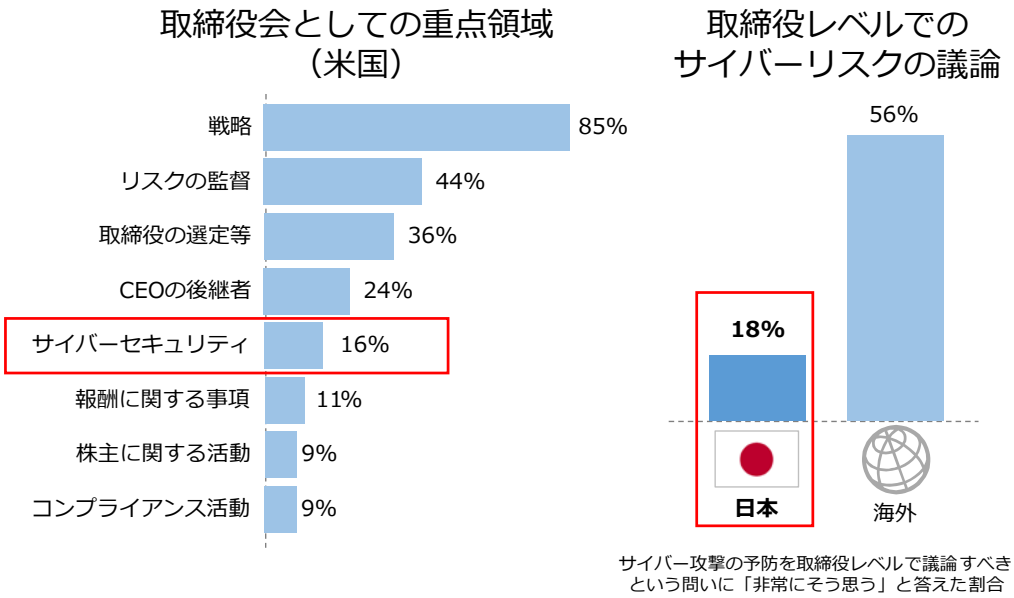


前述の通り、サイバーリスクにより企業価値が一瞬にして減少するため、経営リスク管理の一環でサイバーリスクを取締役会で議論する企業が海外では多い。米国では、16%の回答者がサイバーセキュリティは取締役会での重点領域であると答えており、報酬や株主、コンプライアンス活動に関する議論の割合よりも多い（図表 6）[3]。また、サイバー攻撃の予防を取締役レベルで議論すべきであるかという問いに対し「非常にそう思う」と答えた割合は海外では 56%に対して、日本企業では 18%のみであった[4]。日本の上場企業では、取締役会の責務が強化されつつある段階ではあるが、サイバーリスクには国境がなく、日本企業も置かれているリスク環境は海外企業と同じであるため、日本企業もコーポレートガバナンスの一環でサイバーリスクを議論すべき段階にある。

[3] Deloitte Touche Tohmatsu「Board Practices Report 2014」

[4] KPMG Japan「サイバーセキュリティサーベイ 2013」、「サイバーセキュリティサーベイ 2016」より筆者作成

図表 6　取締役レベルでのサイバーリスクの議論に関する考え方



また、米国では、取締役に対する啓発活動が盛んに行われている。NPO 法人の全米取締役協会（National Association of Corporate Directors。17,000 人以上の取締役が参加する団体）では、2017 年 1 月に取締役が認識しておくべき事項をまとめた「サイバーリスクハンドブック」を発行した（参考資料を参照）。このサイバーリスクハンドブックでは、サイバーセキュリティに関して取締役が実施すべき 5 つの原則の他、取締役会での質問リスト、企業買収時の相手先リスク評価（サイバーデューデリジェンス）についても触れられており、非常に充実した内容である。また、全米取締役協会では、取締役向けに 16 時間のオンライントレーニングコースも用意している。トレーニングを受講した取締役には証明書が発行され、同組織のウェブサイトに取締役の名前が公開されるため、トレーニング受講の動機づけになっていると考えられる [5]。

[5] https://www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=53791

更に、先行事例として取締役会の諮問委員会として「サイバーセキュリティ委員会」を設置する動きもある。General Motors 社は、2017 年 12 月、取締役会の中に「Cybersecurity Committee（サイバーセキュリティ委員会）」を発足し、取締役 3 名を任命した（図表 7）。取締役会の「監査委員会」、「報酬委員会」、「リスク委員会」等とサイバーセキュリティを同レベルで取り扱っていることから、同社のサイバーセキュリティに対する積極的な姿勢がわかる [6]。

図表 7　General Motors 社の取締役会諮問委員会

GENERAL MOTORS COMPANY

Board Committee Membership

Director	Audit	Cybersecurity	Executive Compensation	Finance	Governance and Corporate Responsibility	Risk	Executive
Mary T. Barra							Chair
Linda R. Gooden	●	Chair				●	●
Joseph Jimenez			●		●		
Jane L. Mendillo	●			●			
Michael G. Mullen	●	●				Chair	●
James J. Mulva			●	Chair		●	●
Patricia F. Russo			●	●	Chair		●
Thomas M. Schoewe	Chair	●		●		●	●
Theodore M. Solso (1)							●
Carol M. Stephenson			Chair		●		●

(1) Independent Lead Director

株主や投資家もサイバーセキュリティに関心を示している。最新の調査によると、およそ 2/3 の投資家はサイバーセキュリティの投資拡大を最優先事項にすべきと考えているのに対して、CEO の回答は半数以下に留まる（図表 8）[7]。サイバー攻撃の被害によって企業価値が低下する事例が増えているため、投資した金額は最低でも回収したいと考える投資家がサイバーセキュリティ投資を優先すべきと考えるのは当然のことと言える。このような状況の中、英国の The Investment Association（英国投資家協会）は、2018 年 5 月にサイバーセキュリティに投資することを経営層に求める報告書を発行した [8]。また、The Investment Association は、この取り組みを支援するために、企業、規制当局、公的機関と協力して Cyber Security Committee を設立している。

図表 8　サイバーセキュリティに関する投資拡大を最優先事項と考えている割合　（製品やサービス以外）

[6] https://www.gm.com/investors/corporate-governance.html

[7] PwC「CEO 意識調査／投資家意識調査 2018」 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/investor-survey.html

[8] https://www.theinvestmentassociation.org/media-centre/press-releases/2018/ia-helps-asset-managers-tackle-cyber-security-threats.html

3. 取締役会でサイバーリスクを議論するために求められること

日本企業の取締役会でサイバーリスクが議論できていない主な原因は 3 つある（図表 9）。「ガバナンス視点での規制やガイドラインが存在しないこと」、「取締役が共通で理解できる指標が存在しないこと」、そして「取締役、監査役、投資家、経営者等に対する認知や啓発が足りていないこと」である。それぞれの課題について、解決策を以下に考察する。

1 つ目の「ガバナンス視点での規制やガイドラインが存在しないこと」については、日本取引所グループが金融庁の協力のもとに公表している「コーポレートガバナンス・コード」にサイバーリスク事項を記載することが有効と考えられる。しかし、このコーポレートガバナンス・コードは、2018 年 6 月に改訂されたばかりであり、サイバーリスクの追加には時間を要すると考えられる。そこで、経済産業省が公表している「コーポレート・ガバナンス・システムに関する実務指針（CGS ガイドライン）」にサイバーリスクの項目を追加することを優先させるべきである。また、経済産業省と独立行政法人情報処理推進機構（IPA）が策定している「サイバーセキュリティ経営ガイドライン」に、取締役会で経営者がサイバーリスク状況を報告することについて明記すべきである。同ガイドライン ver2.0 では、サイバーセキュリティリスク管理体制構築の一例として「取締役、監査役はサイバーセキュリティリスク管理体制が構築、運用されているかを監査する」と記載されているのみであるが、具体的に取締役会の議題として挙げるべきと明記する必要がある。

2 つ目の「取締役が共通で理解できる指標が存在しないこと」については、サイバーリスクを金額換算し、IT に詳しくなくともリスクを把握できるようにする必要がある。取締役はビジネスやガバナンスのプロフェッショナルであるが、IT やサイバーセキュリティの専門知識を身に着ける必要は必ずしもない。後述するサイバーリスクを金額換算した「サイバーリスク指標モデル」を普及させ、IT に詳しくない取締役や役員でも経営の観点からリスクを把握できるようにする必要がある。

そして 3 つ目の「認知や啓発」については、CISO（最高情報セキュリティ責任者）やサイバーセキュリティ技術者に対する啓発やトレーニングは国内でも充実してきたが、ビジネスやガバナンスのプロフェッショナルに対する啓発は不十分である。そこで、取締役関連団体や経済団体に対する啓発活動を行い、これらの組織を通じた各種セミナーや広報活動等を促進する必要がある。また、全米取締役協会や英国投資家協会の動向を参考に、サイバーリスクを理解するためのトレーニングプログラムを普及させる必要がある。これらのトレーニング開発にあたっては、プログラムの品質低下や陳腐化を防ぐために、トレーニングプログラムや講師に対する認証制度も検討する必要がある。

図表 9 取締役等に対する意識向上施策

想定される原因	解決策
① ガバナンス視点での規制やガイドラインが存在しない	**コーポレートガバナンス・コード、CGS ガイドライン、サイバーセキュリティ経営ガイドライン**等へのサイバーリスク事項の追加。そのために、金融庁、経済産業省、日本取引所グループ等が横断的に協力することが求められる。
② 共通理解できる指標が存在しない	**「サイバーリスク指標モデル**（後述）**」**を普及させ、IT が専門でなくとも、サイバーリスクを把握できるようにする。
③ 取締役等に対する認知や啓発が足りていない	**取締役関連団体や経済団体への啓発、各種セミナーや広報活動等の促進、役員向けのトレーニング開発。**

4. サイバーリスクを金額換算した「サイバーリスク指標モデル」

サイバーリスクは歴史上新しい分野であり、災害や自動車事故等に比べて過去データが少ない。近年、海外ではサイバーリスクの数値化の研究に取り組んでいるが、データ収集や複雑な計算処理に社内リソースを要するため、必ずしも日本企業に適しているとは言えない（参考資料を参照）。そこで、最大損害額（PML、Probable Maximum Loss）やベンチマーク値を用いることが、日本企業の経営層がサイバーリスクを理解することに有効であると考えられる。図表 10、11 は、JCIC が作成した「サイバーリスク指標モデル」の例である。このモデルをもとに各企業でリスク値を算出し、取締役会への報告等で活用することが可能である。

図表 10 サイバーリスク指標モデル（**年商 1000 億円企業**における社内報告資料の例）【潜在損失額】

		想定損失額の目安	算出根拠
直接被害	①個人情報漏えいによる金銭被害	▲80億円	JNSA一人当たり損害賠償額より算出 （基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価×顧客数≒80億円）
	②ビジネス停止による機会損失	5営業日あたり ▲20億円	社内ヒアリングより算出 （1日あたりの生産量×商品単価≒2億円） （1日あたりのECサイト売上≒2億円）
	③法令違反による制裁金	▲40億円	EUデータ保護指令（GDPR）の制裁金 （全世界の売上高の4%≒40億円）
	④事故対応費用	▲0.6億円	過去事例や業者ヒアリングにより算出 （調査費用、データ復旧費用、応急処置費用等）
間接被害	⑤純利益への影響	▲10.5億円	JCIC調査実績より算出 （前期純利益50億円×21%≒10.5億円）
	⑥時価総額への影響	▲300億円	JCIC調査実績より算出 （時価総額3000億円×10%≒300億円）

【解説】

① セキュリティ事故によって個人情報が漏えいした場合の想定損害額。日本ネットワークセキュリティー協会（JNSA）が公開している JO モデル [9]を用いた損害賠償額算定式より算出。詳細は JNSA の「想定損害賠償額の解説 [10]」を参照。

② サイバー攻撃に起因して社内システムや EC サイトの停止によって、業務が停止し、本来得られるはずだった売上機会の損失額。社内の関係部署へヒアリングを行い算出。2017 年のランサムウェアによる被害事例から、事業中断期間は 5 営業日とした。なお、簡易的に算出する場合は、「年間売上額÷365 日×事業中断期間（5 日間）」によって算出することも可能。

③ 海外に事業展開を行っている企業の場合、現地の法規制に違反したことにより、制裁金や罰金を課せられる場合がある。2018 年 5 月に施行された「EU の一般データ保護規則（GDPR）」によって、違反した企業は高額の制裁金（前年度の全世界年間総売上額の 4%、または 2,000 万ユーロのいずれか高い方の金額が上限）が課せられる。

④ サイバー攻撃を受けたかどうかや攻撃を受けた場合の影響範囲や原因を調査するための費用（フォレンジック費用）、データの復旧費用、応急処置や再発防止のためのセキュリティ強化費用。日本の過去の事例から、事故対応費用は数百万円～数千万円が一般的であるが、各企業でセキュリティ業者等にヒアリングを行い算出することが望ましい。

[9] JNSA Damage Operation Model for Individual Information Leak

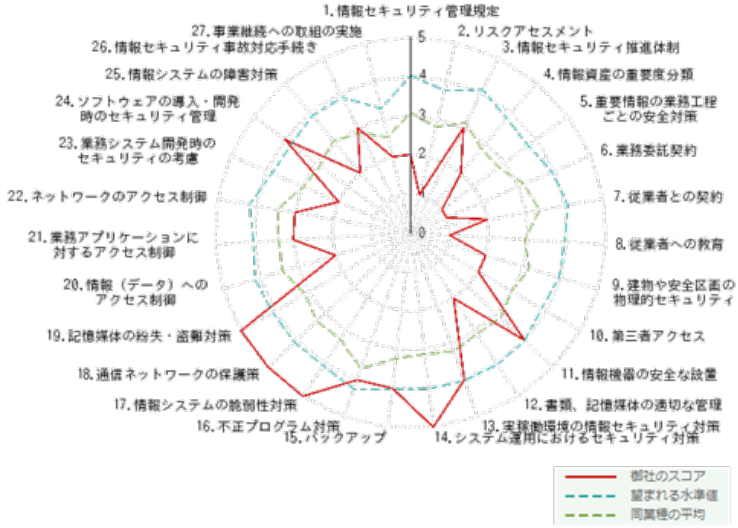
[10] http://www.jnsa.org/result/incident/data/2016incident_survey_attachment_ver1.0.pdf

⑤　特別損失等による純利益減少額。JCIC の調査実績より算出。18 社を調査した結果、セキュリティ事故発生前年度に比べ、21%の純利益減が発生（図表 2 参照）。

⑥　株価下落による時価総額減少額。JCIC の調査実績より算出。16 社を調査した結果、セキュリティ事故の適時開示 50 日後に株価が 10%減少（図表 3 参照）。

図表 11　サイバーリスク指標モデル（**年商 1000 億円企業**における社内報告資料の例）
【ベンチマークとセキュリティ投資額】

⑦ベンチマーク結果	偏差値 42.7	同業種の水準値に比べ低水準であり、大規模な損害が発生する可能性が高い。
⑧業界水準を満たすためのセキュリティ投資額	5年累計 13億円	偏差値50以上を確保するために必要な投資額 初期： 3億円（設備、導入、コンサルティング費用） 年間： 2億円（人件費、監視保守費用）



当社のスコア	76/135点 （偏差値 42.7）
同業種に望まれる水準値	107/135点
同業種の平均	84/135点

独立行政法人情報処理推進機構（IPA）
情報セキュリティ対策ベンチマークにて作成

※IPAのベンチマークツールは簡易的なものである。自社のセキュリティ対策状況の詳細を把握する場合、各種フレームワークや成熟度モデルを用いる必要がある。

【解説】

⑦　自社のセキュリティ対策状況と他社の対策状況を比較した結果。情報処理推進機構（IPA）の情報セキュリティ対策ベンチマーク[11]を用いて算出。

⑧　セキュリティレベル向上のために必要な 5 年間の累計投資額。セキュリティ業者等にヒアリングを行い算出。

なお、上記のモデルは企業規模や業種に関わらず、共通で利用できるように簡略化したモデルである。より詳細なリスク評価については、保険会社やコンサルティング会社等が提供している。

[11] https://www.ipa.go.jp/security/benchmark/index.html

取締役会での議論を一過性のものにすべきではない。自社のサイバーセキュリティの取り組みの進捗状況を KPI（Key Performance Indicator）として定め、四半期に一度程度の頻度で取締役会に報告し、議論すべきである（図表 12）。この KPI に加え、サイバー空間で起きている攻撃の傾向、他社の取り組み、関連する法規制の動向も取締役にとって有益である。

図表 12　経営陣への定期報告例 [12]

2018年度　セキュリティ投資額	計画	実績	昨年比
	¥200 M	¥195 M	18% ↑

施策導入状況

セキュリティ施策		KPI	実績
リスク管理体制	サイバーセキュリティ関連人員の増員	CSIRT 7名→10名	社員 +1名
			外注 +2名
		運用要員 3名→5名	外注 +2名
サプライチェーン	系列企業・ビジネスパートナーの対策実施状況確認	+5社（68%→82%）	4社へ実施（76%）
業界内情報共有	情報提供の仕組み構築	完了	完了
	情報取得の仕組み構築	完了	遅延 19年度 3月予定

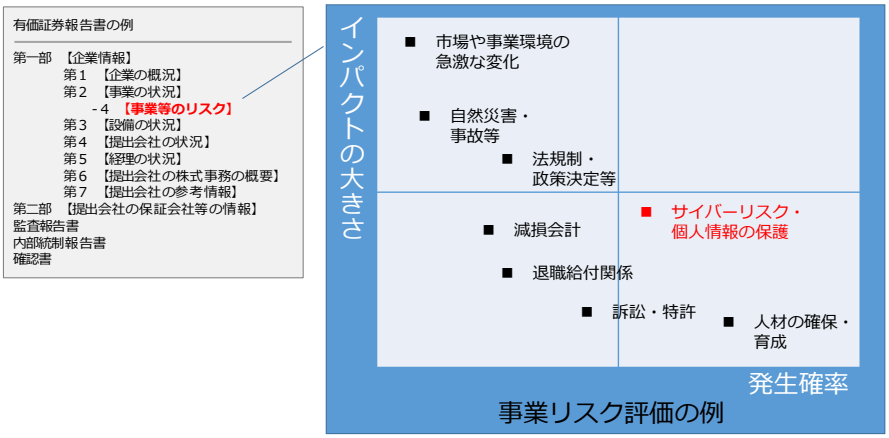
運用状況

管理項目			実績	昨年比
セキュリティ事故	発生件数		124件	-5%
	想定損失		¥20 M	-6%
	復旧費用		¥1 M	+5%
リスク特定	リスク分析対象システム		231	+1%
	指摘事項数	High	53	+2%
		Medium	230	-3%
		Low	78	-4%
	対応進捗率		43%	+6%pt
教育	セキュリティ教育対象者		1,936名	+1%
	セキュリティ研修実施回数		36回	±0%
	研修受講率		85%	+2%

5.　サイバーセキュリティへの取り組みがもたらす経済効果

取締役会でサイバーリスクに関する議論が進むと、取締役や経営者はサイバーリスクを自分事として捉えるようになる。そして、自社の経営リスク全般においてサイバーリスクの位置づけが合意され、どの程度対策にリソースを費やすべきかという意思決定が行われるようになる。図表 13 は、有価証券報告書に記載されている「事業等のリスク」について、発生確率とインパクトの大きさを自社内で整理した例である。リスク環境は日々変動するため、この事業リスク評価は毎年実施する必要がある。

図表 13　事業リスク評価の例

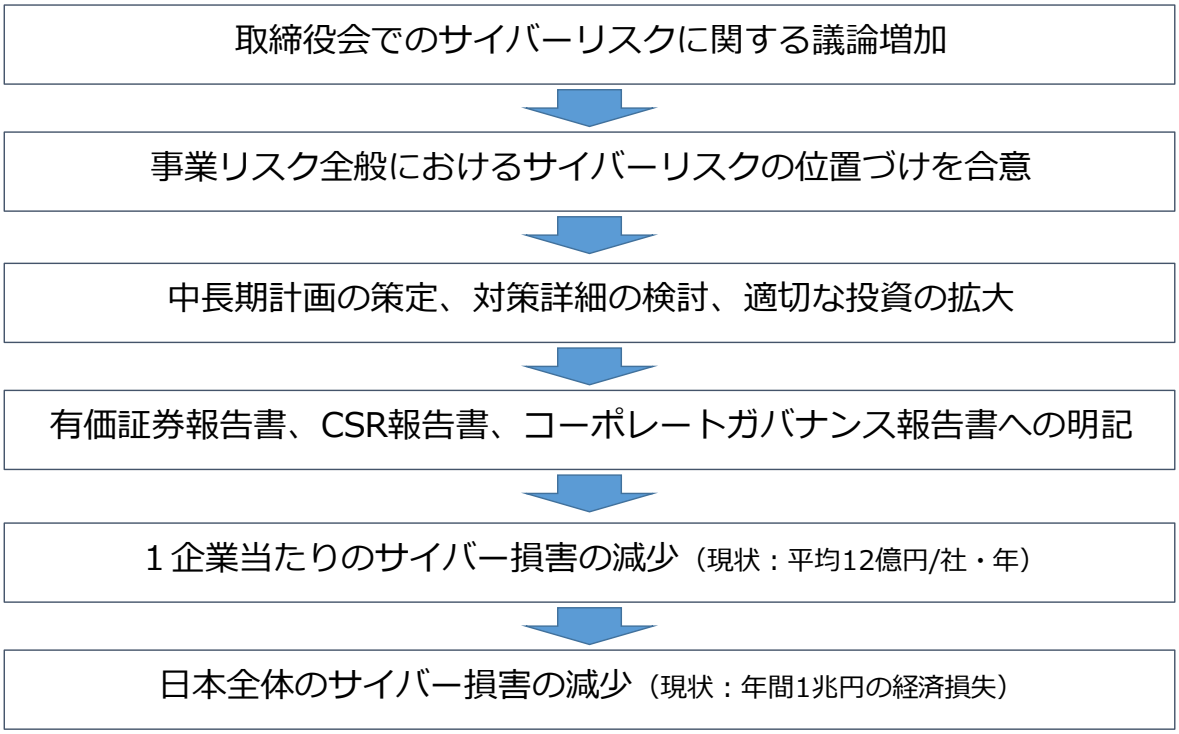


[12] https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/strengthening-digital-society-against-cyber-shocks.pdf

事業リスク評価の中でのサイバーリスクの位置づけが合意された後、セキュリティ対策の中長期計画を策定し、自社にとって適切な投資が行われる。また、企業の各種公開資料（有価証券報告書、CSR 報告書、コーポレートガバナンス報告書）にサイバーリスクへの取り組み状況が記載され、投資家に対して情報開示が行われる。企業にとっては、適切なセキュリティ対策を実施することで、攻撃を受けた後の経営インパクトを最小化することが期待できる[13]と同時に、新規事業やイノベーション等の攻めに転じることができる。

また、国レベルでも大きな経済効果が期待できる。インターネットがもたらす世界の経済効果は GDP の 3～6%程度[14]である一方、世界のサイバー犯罪による損失額は 2017 年に約 63 兆円（GDP の 0.8%）に達したとされる。日本でもサイバーセキュリティ対策が進むことにより、国内のサイバー損害（年間約 1 兆円の経済損失）を減少させることができると同時に、安心安全なデジタル社会の実現により日本の成長を推し進めることができる（図表 14）。

図表 14　サイバーセキュリティに取り組むメリット



[13] Accenture「Cost Cyber Crime Study」によると、1 社あたり平均 12 億円/年の被害が発生。https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

[14] https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

参考資料　海外のサイバーリスク数値化に関する研究例

タイトル	組織名	発表時期	概要
A Framework for Quantitative Assessment[15]	IMF（国際通貨基金）	2018 年 6 月	バリューアットリスク（VaR、最大損失額）によるサイバーリスクの定量的分析を実施。50 か国の最新の被害事例を分析に用いた。この分析によると、1 年間の金融機関のサイバー被害は 11 兆円に上る。これは、世界の 8000 社の金融機関の総純利益（120 兆円）の 9%に相当する。なお、1 企業当たりの平均損失額は 70 億円、中央値は 5 億円であった。
THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE[16]	Ponemon, Centrify	2017 年 5 月	セキュリティ事故が発生した世界 113 社の株価を調査。113 社の株価は平均 5%下落した。セキュリティを強化している企業は平均 7 日で株価が回復したが、セキュリティが手薄な企業は、株価の回復に平均 90 日かかっている。
The Cyber-Value Connection[17]	CGI IT UK	2017 年 4 月	セキュリティ事故発生後の株価を調査。インシデント後、恒久的に株価が 1.5%低下した。また、極端なケースでは株価が 15%減少し、時価総額が 140 億円減少した企業もあった。
A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact[18]	University of Maryland	2015 年 7 月	Cyber Disruption Index（CDI、サイバー破壊指数）という計算手法によりサイバー攻撃の影響を分析。攻撃タイプを 5 つに分類し（SNS ハイジャック／公開サービス停止／内部システム破壊／データ破壊／機器への攻撃）、3 つの次元（範囲／規模／期間）に沿ってサイバー攻撃の影響を測定する。

[15] http://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

[16] https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf

[17] https://www.cgi-group.co.uk/sites/default/files/files_uk/pdf/cybervalueconnection_full_report_final_lr.pdf

[18] http://www.cissm.umd.edu/sites/default/files/CategorizingDisruptiveCyberActivity%20-%20080615.pdf

参考資料　全米取締役協会「サイバーリスクハンドブック」の記載内容 [19]

背景・考え方：
①サイバー攻撃の脅威の潜伏と拡大、②つながりの拡大に伴うリスクの増加、③収益性とサイバーセキュリティ対策のバランス
原則 1：全社リスクの一環としてのサイバーセキュリティリスク認識
原則 2：サイバーセキュリティリスクの法的側面の理解
原則 3：サイバーセキュリティ専門知識の適切な習得
原則 4：サイバーセキュリティ管理フレームワークの整備
原則 5：サイバーセキュリティ対策について具体的な議論を実施
付録 A：経営者に対する取締役会での質問リスト
付録 B：企業買収時におけるサイバーセキュリティの考慮事項
付録 C：サイバーリテラシーを評価するための質問事項
付録 D：サイバーセキュリティの企業文化の評価
付録 E：役員レベルのサイバーセキュリティ評価指標
付録 F：サイバーリスクダッシュボードの例
付録 G：米国国土安全保障省のサイバーセキュリティ情報
付録 H：米国連邦政府のサイバーセキュリティ情報
付録 I：CISO（最高情報セキュリティ責任者）との信頼構築方法

参考文献

- ATKearney,「Cybersecurity in ASEAN」(2018), http://www.southeast-asia.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/cybersecurity-in-asean-an-urgent-call-to-action
- CSIS and McAfee,「Economic Impact of Cybercrime」(2018), https://www.csis.org/analysis/economic-impact-cybercrime
- Marsh & McLennan Companies,「MMC CYBER HANDBOOK」(2018), https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf
- PwC,「CEO Survey and Global Investor Survey」(2018), https://www.pwc.com/jp/ja/knowledge/thoughtleadership/investor-survey.html
- The Investment Association and KPMG,「Building Cyber Resilience in Asset Management Report」(2018), https://www.theinvestmentassociation.org/media-centre/press-releases/2018/ia-helps-asset-managers-tackle-cyber-security-threats.html
- Accenture,「Cost Cyber Crime Study」(2017), https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017
- Emanuel Kopp ; Lincoln Kaffenberger ; Christopher Wilson,「Cyber Risk, Market Failures, and Financial Stability」(2017), https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
- KPMG,「Cybersecurity Survey」(2017), https://home.kpmg.com/jp/ja/home/insights/2017/06/cyber-security-survey-2017.html
- National Association of Corporate Directors,「NACD Director's Handbook on Cyber-Risk Oversight」(2017), https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf
- Ponemon Institute and IBM,「Cost of Data Breach Study」(2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN
- Hubbard Decision Research,「How to Measure Anything in Cybersecurity Risk」(2016),

[19] https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf

[本調査に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com

主任研究員　平山敏弘　hirayama@j-cic.com