レポート

モバイル世界における電子バンキング、電子決済、Eコマース

フィンテック関連法

2018年1月／2月 ■ 第21巻 ■ 1号

サイバーセキュリティ：あらゆる取締役会に求められる知識と行動

Paul Gupta、Ariana Y. Goodell共著

Paul Guptaは、Reed Smith LLPのデータセキュリティ・知的財産訴訟グループのパートナーで、サイバーセキュリティ、特許訴訟、商標・著作権紛争の専門家です。Ariana Goodellは、Reed Smithの知的財産・テクノロジー・データグループのアソシエートで、サイバーセキュリティ、データプライバシー、情報ガバナンス関連を専門としています。
www. reedsmith.com

サイバー攻撃がますます増え、その被害が大きくなるにつれ、企業の取締役会がこれらの攻撃に対して防止策と軽減策を優先してきていないという認識が高まりつつあります。

大規模なデータ流出が初めて報告された2005年以来、企業の業務、収益、株価そして社会的信用に対するサイバー攻撃からの危険は急激に拡大しています。2015年までに検知されたセキュリティ侵害インシデントは5000万件を超えました。より最近の例では、2017年5月のWannaCryランサムウェア攻撃は、北朝鮮の国家支援があるとされるハッカーの仕業と考えられ[1]、世界各地で企業活動に大混乱を引き起こしました。最初の伝染からわずか2日間でWannaCryランサムウェアは150か国で20万人以上のユーザーに被害をもたらしました。[2]

この攻撃だけで収益損失は40億ドルに上り[3]、このうち10億ドル分はシステムダウンによる長期の業務中断があった最初の4日間に発生したと見られています。[4] マルウェア攻撃による被害は向こう数年間で劇的に増加するとサイバーセキュリティ専門家は予想しています。

一方で、取締役会への調査では、取締役はサイバー攻撃の現状とリスクを認識しているという結果が出ています。しかしその反面、同じ調査では、サイバーセキュリティ問題に対して取締役会が割り当てるリソースは比較的ささやかなものだという結果です。

今号で取り上げる内容：

THOMSON REUTERS

42023363

さらには、当社の実体験では、あまりに多くの企業がサイバー攻撃に対して準備不足で、企業トップレベルのリーダーシップがサイバー攻撃の防止・軽減への取り組みを加速すべきだと思われます。

サイバー攻撃に対する企業取締役会の対策の必要性は、一般メディアでも取り上げられることが増えてきました。例えば、ウォールストリートジャーナルは、2018年1月10日付の記事で、「先ごろエキファックスで起こったデータ不正流出を受け、企業取締役会はサイバーセキュリティリスクに関する見識拡大に動いている」と報じています。[5] 同記事では、サイバー犯罪者が企業の社会的信用を失墜させ、損害賠償と訴訟費用で数千万ドルもの損害を出しているなかで、取締役会のなかにはサイバーセキュリティに関する監督を強化し、取締役会メンバーにどう責任を割り振りするかを検討しているところも出てきています。さらにこの記事では、自分が取締役を務める企業はサイバー攻撃に対して適切な対策を取っていないと危惧する取締役が多数いるにも関わらず、情報技術リスク・戦略を専任とする取締役や委員会を持っているところは少数だとも報じています。

同記事は、取締役会の人事と機能を改善することで、サイバーレジリエンスを向上させる方法を取り上げています。取締役会に欠員が生じて新メンバーを探す場合、サイバーセキュリティの脆弱性と軽減策のベストプラクティスに関する実務知識を持つ人物の選任を優先事項とすべきです。また取締役会は、技術要員に頼るのでなく、サイバー攻撃に対処するプラン開発とモニタリングに対して主張を強めるべきです。取締役会には一般的に最高財務責任者（CFO）や他の財務部門役員の尽力をまとめる能力のあるメンバーがいるのと同様に、最高情報責任者（CIO）や最高情報セキュリティ責任者（CSIO）の尽力をまとめることができるメンバーも置くべきです。そして、財務上の概念や専門用語に詳しい取締役会メンバーがいるのと同じく、取締役会はサイバー問題に対する知識があり、コンピューター用語に詳しいメンバーを少なくとも数名置くべきです。この記事の説明にもある通り、サイバー問題は法的な意味合いを帯びてきている点を指摘すべきでしょう。したがって、サイバーセキュリティとそれに関連する法律問題両方の経験があるメンバーが最低でも1名いればとりわけ有用となります。

I. 取締役会がリーダーシップを発揮すべき6つの分野

取締役会がサイバー関連でリーダーシップを発揮すべき分野は少なくとも6つあります：

フィンテック関連法レポート
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

年間購読料・年6号発行・1020ドル

a. 第1分野 セキュリティをチーム活動にする

適切な指導とモニタリングによって、あらゆるレベルの社員がサイバーセキュリティに貢献することができます。しかし、効果的なレスポンスを確保するためには、データセキュリティに対する社員の取り組みには念入りな調整が必要です。調整がないと、サイバーセキュリティ侵害が起こる確率が高まり、侵害の検知と対応の実施が遅れる結果となる場合があります。データセキュリティに関する取り組みで調整が重要なのは、データ流出によって被害を受けた人には通常迅速に対応と通知を行うよう、法律、規制、そして契約面での要件によって義務付けられているためです。2018年5月に施行されたEU一般データ保護規則（GDPR）は、データ流失があった場合、72時間以内に通知する義務を課しています。

取締役会は、上級管理職の賛同を得て、部門を越えたチームを構築すべきです。セキュリティチームは、最低でも最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、物理的セキュリティ部門長、人事部門長、そして法務顧問のスタッフを含め、様々なステークホルダーにより構成されるべきです。チームの役割を細かく定義し、取締役はマネージャーに対し明確なコミュニケーションラインの設立を指示し、社員教育を通じて認識を高め、上層部への報告に関する適切な手順を確立すべきです。

b. 第2分野 社員のITアクセスモニタリング

企業の最高機密や個人情報（PII）に社員がアクセス可能であることは日常的であり、そのため内部犯行による漏洩リスクの最小化を図る安全措置を講じるべきです。取締役会は、離職するとわかっている社員に対して会社財産とネットワークへのアクセスを適時に停止するプロセスを実行すべきです。これに加えて、取締役会は、頻繁な検査によってIT部門社員の不正を未然に防止し、「危険ゾーン」にいる社員を監視すべきです。危険ゾーンの社員とは、PIIに常時アクセスすることができる社員を指します。最後に、取締役会は社員の職務変更に応じてアクセスのレベルを審査するプロセスを実施すべきです。

c. 第3分野 データマッピングとデータ保持に関する強力なプランを開発

企業がデータ資産とネットワークを保護できるようになるためには、その前にそのデータがどこで格納されていて、誰がアクセスできるかを理解する必要があります。サーバーセキュリティ侵害が起こった場合、侵害を受けたデータとその格納デバイスを隔離することは通常インシデントレスポンスの最初のアクションアイテムです。

したがって、取締役会はデータマッピング、データ保持、廃棄を監視すべきです。これは米証券取引委員会（SEC）が注視する分野です。SECは、2015年のサイバーセキュリティ検査イニシアチブで、サイバーセキュリティ関連問題で登録企業を検査するプロセスのなかで、SECのコンプライアンス検査局（OCIE）は「エンタープライズデータ損失防止と…データマッピング関連情報に対する企業方針ならびに手順を、とりわけ情報の所有権と企業がどのように個人情報を記録または事実確認するかに重点を置いて検査する。」としています。[6]

報告されたサイバーセキュリティ侵害は、企業には業務上必要でなく、また法的に保持する理由のない電子保存情報（ESI）に関わる場合が何度も起きています。取締役会は、有効期限を過ぎた情報資産は負債に変わる点に注目する必要があります。したがって、企業の正確なデータマップを作成することは不可欠です。

不要となったESIが特定できるよう、企業はデータマッピング演習とデータ保持演習の両方を行うべきです。保持する必要がなくなった情報を特定することで、企業はサイバーセキュリティ侵害での不要なESIの漏洩による損失リスクを効果的に軽減することが可能となります。

d. 第4分野 見落としている点は何か考える

取締役会は、サイバーセキュリティ対策に影響を及ぼす可能性のあるすべての問題を包括的に検討するよう管理職に指示すべきです。サイバーセキュリティ対策に何百万ドルも投じ、高度なハッキング防止プログラムを配備している企業であっても、物理的セキュリティへの注意を怠ってハッカーに隙をつかれる場合があります。外部ベンダーによって巨額損失が引き起こされる場合もあります。外部ベンダーのサイバーセキュリティは企業のサイバーセキュリティと同じくらい重要です。取締役会は、企業が外部ベンダーとの契約を見直し、ベンダーのネットワークアクセス監査を行っていることを確認すべきです。

e. 第5分野 IT事業継続計画を維持

先ごろ起こったWannaCryマルウェア攻撃によって、サイバーインシデントが企業の基幹業務に多大な混乱を巻き起こすことがはっきりしました。例えば、英国の国民保険サービスは、「WannaCry」攻撃で身代金を払わなければ重要ファイルを削除すると脅されたため、数千件に上る手術や診療予約のキャンセルを余儀なくされました。[7] したがって、取締役会メンバーは、業務停止期間を最小限にとどめるための防衛戦略の骨組みとなる効果的な事業継続計画を企業が準備していることを確認すべきです。加えて、取締役メンバーは、社内外リソースを有効活用してサイバーセキュリティ対策を評価する定期検査を行うよう管理職に指示すべきです。

f. 第6分野 まず訴訟に備える

重大なデータ不正流出の被害者は、しばしば集団訴訟という形で、さかんに訴訟を起こしています。データ流出の後には、原状回復の取り組みのなかで、敵対者が企業取締役や企業の過失を証明するのに使う可能性のある機密情報が生じます。

しかし、他の証拠上の秘匿特権、とりわけ弁護士依頼人間秘匿特権と職務活動の成果の法理を適用することで、そのような情報は保護される場合があります。小売業者とクレジットカード発行者を巻き込んだ最近の例[8]では、弁護人がデータ流出後に行われた復旧のための調査作業を保護することができました。小売業者は、自社店舗でのクレジットおよびデビットカード決済を狙ったサイバー攻撃に遭った後、クレジットカード会社を訴えました。小売業者の法務顧問はサイバーセキュリティ調査会社を雇い、データ漏洩のフォレンジック調査を実施しました。クレジットカード会社が調査に関連する記録を法務顧問に請求した際、調査会社の雇用は小売業者に対する法的アドバイス支援が目的であったとの理由で、裁判所はその証拠開示請求をおおむね退けました。

インシデントレスポンス（IR）チーム内での束縛のない自由なコミュニケーションの流れを確保するため、取締役会はIR作業のあらゆる段階で弁護士が関与することを確実にすべきです。これには防止策（例えば、サイバーセキュリティ方針の開発と社内監査）やサイバーセキュリティ侵害に対応する復旧の取り組みが含まれます。IRチームは外部サイバーセキュリティ専門家も雇用すべきです。[9]

加えて、IRチームはメタデータと「証拠保全」情報の保存には留意し、訴訟ホールドを保持すべきです。

II. 規制と訴訟の背景

米連邦・州政府機関は、データ漏洩があった企業に対し、規制適用措置を取ることが増えています。さらには、サイバーセキュリティとプライバシーの侵害に関連する派生訴訟が数多く起こっています。サイバーセキュリティに関して取締役会レベルで適切なビジネス判断を行っていたと裁判所が判断したため、多数の訴えが却下となりました。規制執行と派生訴訟の増加にともない、取締役会として企業のサイバーセキュリティプランに関与することは重要です。

a. SECによる規制適用

SECはサイバー犯罪を米国市場に対する「最大の脅威」と考えています。[10] 新しくSEC委員長に就任したジェイ・クレイトン氏は、米上院議会での指名承認公聴会で、上場企業はサイバーセキュリティに関する情報開示が十分でないと思うと述べました。[11] さらには、クレイトン氏はとりわけサイバーセキュリティ経験のあるメンバーが1名でも取締役会にいるかを開示することを企業に義務付ける法案に賛成であるとし、サイバー問題に対して取締役会がどのように取り組んでいるかを投資家は知るべきだと考えていると付け加えました。[12]

> *「私の意見は、サイバーセキュリティの分野において… サイバーセキュリティ問題を把握している取締役会レベルでの十分な監視が行われているかという面で、十分な開示があるとは考えていないというものです。企業がサイバー問題に関心を払ってきたか、取締役会に専門知識を持つ人物がいるか、投資家は知っておくべきだと私は考えます。それは企業が知っておくべきだという意見に賛同します。大企業を運営するうえで重要な部分であり、大企業ならば誰もがサイバー攻撃のリスクがあります。」*[13]

SECは最近、サイバーセキュリティリスクとデータ流出に関する情報開示をめぐって上場企業を訴える可能性があると示唆しています。これには取締役に対する規制適用も含まれます。

SECはすでに、複数の登録投資顧問会社に対し、サイバーセキュリティの不備があったとして、制裁措置を取っています。例えば、2015年には大手投資会社のR.T.ジョーンズが、ハッキングに遭った際に、義務付けられたサイバーセキュリティに関する方針と手続きを事前に構築することを怠ったとしてSECより措置を受けました。このデータ漏洩によって、同社顧客を含む約10万人分の個人情報が流出しました。[14] ジョーンズ社は、不正行為を肯定も否定もすることなく、規制標準手順（Regulation S-P）のルール30(a)に今後は違反または違反を招く行為をしないことに同意し、SECとの和解に至りました。同社はまた譴責を受け、制裁金7万5000ドルを課されました。[15]

サイバーインシデントの発生は株価を大きく変動させる可能性があるため、規制当局と原告の法務顧問双方がサイバーセキュリティ侵害または脆弱性の非開示とIRプランの実施不備の両方を訴訟の原因とする可能性が高まることを前提に取締役会メンバーは考えるべきです。適切なプラン開発にあたって、取締役会メンバーは、規制当局からの規制適用というリスクの高まりを考慮すべきです。

b. 他の連邦・州当局による規制適用の動き

米財務省を含む他の連邦機関とニューヨーク州各機関もまた、サイバーセキュリティに取締役会を関与させる規制の施行を目指しています。

規制案制定事前通告（ANPR）で、米財務省は、取締役会レベルでの承認と「サイバーセキュリティに関わる専門知識」を含めたサイバーセキュリティガバナンスの改善を米大手銀行に対し義務付けるという基準についてパブリックコメントを受け付けました。[16] コメント受付期間は2017年1月17日に終了し、銀行管理当局はANPRで収集した情報に基づいてより詳細な規制案を作成し、後日公開して一般の意見を求める予定です。新規制案は現時点ではまだ発表されていません。

ニューヨーク州金融サービス局は、既存の連邦・州規則を超える要件を持つ、これまでにない厳しい基準のサイバーセキュリティ規則を施行しました。これらの要件には、14の事項に重点を置いた包括的なサイバーセキュリティ方針と上席執行役員による書面での認可を義務づけることが含まれます。[17] ニューヨーク当局がこの規則を施行したことで、サイバーセキュリティに関して範囲を拡大する方向で公共政策が動きつつあることが明らかになりました。他の州も近い将来、同様の規則を施行すると思われます。[18]

c. 訴訟

データ漏洩に関しては、信託者の義務違反や証券詐欺などで企業取締役や役員を提訴する多数の株主代表訴訟が起きています。[19] 通常、訴えの多くは似通った事実の流れに沿っており、顧客の個人・金融情報を守る内部管理の整備を怠ったり、企業がデータ漏洩を投資家から秘匿する原因となった、または秘匿を許すことになったという理由で、企業はその受託者の義務に違反したというものです。米商工会議所の報告書によれば、Edelson PCとLieff Cabraser Heimann & Bernstein LLCを含む弁護士事務所4社は、進化を続ける法的環境を巧みに利用しようと、取締役会を相手取ったプライバシーとサイバーセキュリティ関連訴訟の大部分を率いています。[20]

多くの訴訟で、訴えられた企業がサイバーセキュリティに関して適切なビジネス判断を行っていたと認められたため、原告は注意義務要件を満たしていなかったとして訴えは却下されています。これらのビジネス判断には、データ流出前にセキュリティ対策を導入していたこと、データ流失後に変更を行ったこと、企業のデータセキュリティ対策に関する報告書を経営陣から取締役会の審査委員会と企業責任委員会に提出したことなどが含まれます。

III. サイバー問題に関連した取締役会の課題の現時点での分析

過去3年間にわたり、情報システムコントロール協会（ISACA）、コーン・フェリー、スペンサースチュアート、世界経済フォーラムなどの組織は、サイバーセキュリティにおける取締役会の役割に強い関心を示してきました。以下の報告書では、現時点で取締役会はどれほどサイバーセキュリティに対して馴染みがあるか、そして企業リーダーとしてのその役割は何かを分析します。

a. 2014年ISACAによる報告書

2014年にISACAと内部監査協会（IIA）調査研究財団は次の報告書を発表しました：*「サイバーセキュリティ：取締役会が聞くべき質問とは何か」* 本報告書のきっかけとなったのは、内部監査協会エグゼクティブセンターによる「2014年監査の現状を測る」調査で、取締役会メンバーの65%がサイバーセキュリティを高リスクと認識している反面、サイバーセキュリティ対策に積極的に関与していると答えたのはわずか14%だったことです。[21] 本報告書では、取締役会メンバーがサイバー攻撃の可能性を認識し、適切に防御するための方法は何かに重点を置いています。

同報告書によれば、取締役会はセキュリティガバナンス管理と企業のインシデントレスポンスプロトコルを熟知しているべきです。[22] 取締役会はまた、企業のセキュリティフレームワーク（HIPAA法、PCI-DSSなど）とサイバーセキュリティに対し内外部に常時存在する脅威を認識することが必要です。[23] 潜在的なサイバーセキュリティ脅威には以下が含まれます：社員が私的デバイスを職場に持ち込むことやスマートデバイスを持ち込むこと（いわゆるBYOD）、災害復旧と事業継続、定期的なアクセス見直し、ログ検査。[24]

クラウドコンピューティングと外部アウトソーシングもまた取締役会が認識すべきリスクです。クラウドコンピューティングは、企業が日常的に使うインターネットソリューションを含みます。これらはsalesforce.comやbox.net、またはMicrosoft 365かもしれません。[25] クラウドコンピューティングの代わりに、企業は給与計算、買掛金、売掛金など主要業務プロセスを外部アウトソーシングする場合もあります。外部サービスについては管理が欠如しているため、企業にとって重大なサイバーセキュリティリスクとなる可能性があります。[26]

ISACA報告書ではまた3つの防衛コンセプトを紹介しています。このコンセプトは取締役会と企業がサイバー攻撃の可能性に対し防御する助けとなります[27] この3つの防衛線に対しては2者が責任を負います。すなわち上級管理職と取締役会です。上級管理職は第1の防衛線に立っています。彼らにはサイバーセキュリティ方針・基準を実施し、ネットワークとインフラを日常的にモニタリングする責任があります。[28] CISOが第2の防衛線です。CISOは、財務管理、セキュリティ、リスクマネジメント、品質管理、検査、そして企業のコンプライアンスを統括する責任を負います。CISOは、IT業務で適切なモニタリング、レポーティング、トラッキングが行われていることを確認する義務があります。[29] 最後に、上級管理職と取締役会は第3の防衛線に立っています。両者は第1・第2防衛線が適切に機能するよう内部監査を実施する責任があります。[30] 上級管理職と取締役会が共同で内部監査を実施することが重要です。[31]

b. 2015年コーン・ケリーによる報告書

サイバー攻撃の増加を受け、コーン・ケリーは、*「デジタル時代をナビゲートする：取締役と役員のためのサイバーセキュリティ決定版ガイド」*という取締役会がサイバーセキュリティ対策を講じる際に有用な報告書を発表しました。[32] サイバーセキュリティ対策は取締役の新しい役割ですが、取締役会メンバーが従来担当してきた専門分野とは関連がないため、多くの取締役は準備不足であると感じています。したがって、サイバー攻撃の脅威とセキュリティについては、取締役会メンバー全員が互いに同じ考えであるよう企業は確認することが重要です。[33] いったんサイバー攻撃が重大リスクであると認識されれば、他のリスクに対するのと同じ実行力とプロセスを持って対処し、主要かつ総合指標と共に常に取締役の目に入る場所にとどめるべきです。[34] 取締役会の最も重要な役割は、的確な質問をすることです。これにはビジネスで培った知恵と昔ながらの常識が必要であるかもしれませんが、必ずしもサイバーセキュリティの専門知識は必要ではありません。[35] 的確な質問をすることで、企業上部からの整合性が得られ、また企業がサイバーセキュリティに関して確実にしっかりと取り組む助けとなります。[36]

取締役会会議で的確な質問をする以外に、取締役会がサイバーセキュリティの第1防衛線に立つための具体的な方法が3つあります。まず、取締役会の新メンバーを指名する際には、サイバーセキュリティに関する知識を持つ候補者を対象とすべきです。[37]

次に、上級管理職がサイバー攻撃に対し強固な防止・検知・対応策を作成し実施する際には、取締役会が関与すべきです。[38] 最後に、取締役会は経営幹部と常時コミュニケーションをとり、指標を使ってサイバーセキュリティのモニタリングにあたるべきです。[39]

c. 2016年スペンサースチュアートによる報告書

2016年にスペンサースチュアートは初の*2016年版グローバル取締役会調査を実施しました。*この総合調査では、企業にとってリスクとは何か、そして取締役会の長所と弱点は何かと考えるかと取締役会メンバーに聞き取りを行いました。取締役会メンバーは、サイバー攻撃増加を受けて、より戦略的でダイナミックかつ応答性が高い役割を果たそうとしています。[40] これらの攻撃は、企業に経済的損失と社会的信用の失墜をもたらす可能性がありますが、リスク監視の範囲を拡大することになります。[41] スペンサースチュアートによる主な調査結果には、サイバー攻撃に対する取締役会の認識と準備の度合い、取締役会にとって最も関連性の高い政治問題、そして戦略目標達成において取締役会が直面する課題が含まれます。

グローバルで取締役会が最大の懸念を表すのは、規制・社会的信用のリスクに対してであり、次にサイバーセキュリティです。これは取締役会がアクティビストやサプライチェーンリスクに対して抱く懸念と比較した結果です。[42] サイバー攻撃に対して企業が抱く懸念レベルと実行している対策の準備度レベルを1～5の5段階で示すといくつかという質問に対し、企業からの回答は平均では自社のサイバーセキュリティに対するリスクと準備度レベルは3.2というものでした。[43] つまり、平均すると企業はサイバー攻撃を中程度から重大な脅威と考えているということです。同様に、平均では、企業は中程度から重大なレベルでサイバー攻撃に対する準備があります。[44] さらには、平均的な取締役会はサイバーセキュリティに関する取締役会プロセスを3.0と評価しています。[45] これは取締役会がサイバー攻撃に関する取締役会プロセスは標準だと考えているということを意味します。

取締役会メンバーは、サイバーセキュリティは自社にとって最も関連性の高い3つの政治問題のひとつだと示唆しています。39%の取締役会メンバーがサイバーセキュリティは関連性の高い政治問題だと考えています。[46] これは、経済（65%）、規制環境（59%）に続く3番目に高い結果です。[47] 興味深いことに、取締役会のわずか9%がサイバーセキュリティは企業の戦略目標を達成するうえでの課題だと見ています。[48] これは優秀な人材の確保・維持と比較した結果ですが、41%の取締役は、人材は難問だと考えています。[49]

d. 2017年版全米取締役協会（NACD）のサイバーリスク監視に関するハンドブック

取締役会がサイバーセキュリティ監視における自らの役割拡大に関心を寄せていることを受けて、全米取締役協会（NACD）は、役員と取締役向けにサイバーセキュリティリスク管理に関するガイダンスを含むハンドブックを新たに出版しました。[50] NACDは、サイバーリスク監視強化にあたってすべての企業取締役会が考慮すべきと考える5項目のアクションアイテムを特定しました。そのアクションアイテムには以下が含まれます。

1. サイバーセキュリティはITに限った問題ではなく、企業全体のリスク管理問題として理解し、アプローチする。
2. それぞれの企業の独自状況に関連するサイバーリスクの法的な意味合いを理解する。
3. サイバーセキュリティ専門知識に対する適切なアクセスを確保し、サイバーリスク管理に関する議論は定期的に適切な時間を割り振って取締役会の議題で取り上げる。
4. 経営陣は、十分な人員と予算を割り当て、企業全体としてのサイバーリスク管理の枠組みを構築するという期待を確定する。

5. サイバーリスクに関する取締役会経営陣の議論には、どのリスクを回避し、受け入れ、軽減し、または保険を通じて譲渡すべきかに加え、各アプローチに関連する具体的なプランを認識することを含めるべき。[51]

e. 2017年世界経済フォーラムによる報告書

企業がビジネスのニーズを満たすためにテクノロジーとインターネットを使うなかで、世界経済フォーラムはビジネスリーダーがそのようなテクノロジーの固有リスクを確実に認識するよう尽力してきました。[52] 世界経済フォーラムはサイバーセキュリティには2つの主要アイデアがあると考えています。まず、サイバー攻撃に対する回復力を確保するにはリーダーシップが不可欠な役割を果たすというアイデアです。次に、より効果的なサイバー戦略を構築し総合戦略プランに組み込むためには、企業リーダーにはサイバーセキュリティのみにとどまらない心構えが求められるということです。[53] *「サイバーレジリエンス強化のための取締役会向け原則とツール」*と題した報告書で、世界経済フォーラムは取締役会に対しサイバーセキュリティでの課題に効果的に対処し、サイバーレジリエンスを導入するための10原則を提示します。

第1原則は、サイバーレジリエンスに対して責任を負うことです。取締役会は、サイバーリスク監視・レジリエンスに対する最終責任を負うべきです。取締役会は、既存の委員会に監視委員会を権限委譲する、あるいは新しい委員会を設立して権限委譲することも可能です。[54]

第2原則は、サイバーセキュリティでの指揮権を握ることです。取締役会に新メンバーが加わったら、サイバーレジリエンストレーニングを受け、脅威と傾向に関して継続的に最新情報を受けるべきです。取締役会メンバーはまた、独立した専門家に依頼してアドバイスと援助を受けるべきです。[55]

第3原則は、経験豊富な成果責任（アカウンタビリティー）責任者を任命することです。この責任者は、サイバーレジリエンスに関する企業の能力、管理、実施状況について、取締役会に報告を行う責任があります。[56]

第4原則は、サイバーレジリエンスを企業の戦略プランに統合することです。これには、予算とリソース配分でサイバーレジリエンスを統合することが含まれます。[57]

第5原則は、企業のリスク選好度・容認度を評価し、認識することです。リスク選好度に企業の戦略プラン、規制要件、該当する業界基準との整合性が持たせることは重要です。[58]

第6原則は、リスク・脅威・イベントを評価し報告する責任を経営陣に対し負わせることです。これは、取締役会議では毎回議題とすべきです。[59]

第7原則は、アカウンタビリティー責任者がサイバーレジリエンスプランの作成・実施・テスト・継続的モニタリングを行う際に、経営陣はきちんとサポートすることです。これらの事項はすべて定期的に取締役会に報告されるべきです。[60]

第8原則は、企業のステークホルダーとの間にコミュニティを作ることです。組織としてのサイバーレジリエンスを確保するためには、経営陣がステークホルダーと適切に協力することが重要です。[61]

第9原則は、第三者による審査を毎年実施することです。[62]

最後に、第10原則は、サイバーレジリエンスの効果を確実にするため、取締役会のサイバーレジリエンス履行状況を評価することです。[63]

IV. サイバーセキュリティに関する取締役会の準備度チェックリスト

一般的に、取締役会はサイバーセキュリティを取り上げることには乗り気ではありません。しかし、サイバー攻撃が重大なリスクとなった現在、このトピックに慣れ親しむことは不可欠です。次が、サイバー世界で積極的に取り組み、安全を確保するために、取締役会が取るべき行動のチェックリストです。

1. 取締役会とスタッフ全員が確実に知識を持つ

- 会社にはセキュリティ面でのリーダーはいますか？
- 取締役会に少なくとも1名はサイバーセキュリティの専門知識を持つメンバーがいますか？

2. 既存のリソースと潜在的リソースを理解する

- IT予算はいくらですか？
- IT管理チームはどのような構成ですか？
- 当社にとってプライバシー委員会を設立することのメリットは何ですか？

3. リスクを評価する

- 会社が顧客やサプライヤーなどから収集するデータには何がありますか？
- 会社のITインフラはどのようなものですか？
- 会社ではIT業務をアウトソースしていますか？そうであれば、外部企業・人はどのようにその情報を扱っていますか？
- 業界でのIT基準・規則はどのようなものですか？
- 社内外で当社が収集する情報に対するリスクとは何ですか？
- 収集する情報の安全性を確保するために埋めることが必要な情報収集での「抜け穴」は何ですか？
- 継続的なリスク評価を実行する

4. 新しい方針を実施する

- 方針と手順を作成し、実施します
- 防止プランを作成し、実施します
  - 会社が収集する情報をどうやってサイバー攻撃から守りますか？
  - 現在すでに実施済み、またはこれから実施予定の具体的な戦略と手順には何がありますか？
- インシデントレスポンスプランを作成し、実施します
  - サイバー攻撃にどう対処しますか？
  - 現在すでに実施済み、またはこれから実施予定の具体的な戦略と手順には何がありますか？

5. 保険適用範囲を検証し、サイバー攻撃関連の賠償責任に保険をかける

- データ流出によるプライバシー侵害には保険が適用されますか？
- サイバーセキュリティリスクには保険が適用されますか？
- 以下が含まれる「利益（事業中断）保険」をかけるようにしてください。
  - システム障害

- サイバー恐喝
- 電子資産の復旧
- 構外利益保険

文末脚注:

[1] Ellen Nakashima、「米国家安全保障局はWannaCryのコンピューターワームに北朝鮮の関与があると判断」Washington Post（1970年）、http://wapo.st/2s2G1Gg?tid=ss tw-bottom& utm term;=.50891976d 352（最終検索日2017年8月11日）

[2]「ランサムウェアによるサイバー攻撃が拡大中 - 欧州刑事警察機構」BBC News（2017年）、http://www.bbc.com/news/technology-39913630（最終検索日2017年8月11日）。Jonathan Berr、「WannaCryランサムウェア攻撃による損失は40億ドルに達する可能性」CBS News（2017年）、http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/（最終検索日2017年8月11日）。

[4]「2017年のランサムウェアによる被害は50億ドル、2015年の3億5000万ドルから急増」Cybersecurity Ventures（2017年）、http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/（最終検索日2017年8月11日）

[5]Joann S. Lublin & AnnaMaria Andriotis、「ハッキング防止に取締役会が役割を拡大」The Wall Street Journal（2018年）、https://www.wsj.com/articles/boards-seek-bigger-role-in-thwartin g-hackers-1515596400（最終検索日2018年1月17日）

[6]コンプライアンス検査室（OCIE）、OCIEの2015年サイバーセキュリティ検査イニシアチブ2015年9月15日発行第4巻8号、ウェブサイトはこちら:https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

[7]Alex et al.、「なぜWannaCryマルウェアは英国民保険サービスに大混乱を引き起こしたのか」NBCNews.com（2017年）、http://www.nbcnews.com/news/world/why-wannacry-malware-ca used-chaos-national-health-service-u-k-n760126（最終検索日2017年8月16日）

[8]Genesco, Inc.対Visa U.S.A., Inc.事件302F.R.D. 168（M.D. Tenn. 2014年）

[9]Reed Smithは、データ損失インシデントの際の通知戦略を企業が明確化する助けとなる、そのタイプでは初めてのツールを開発しました。詳しい情報はこちら:www.BreachRespondeRS.com

[10]Carmen Germaine、「SECはサイバーセキュリティへの関心を規制適用に向ける意向」LAW 360（2017年7月17日午後4時18分）、https://www.law360.com/articles/937197/sec-poised-to-turn-cybersecurity-focus-into-enforcement

[11]「クレイトンSEC委員長はサイバーセキュリティ開示改善を支持」トムソン・ロイター税務・会計部門（2017年）、https://tax.thomsonreuters.com/media-resources/news-media-resources/checkpoint-news/daily-newsstand/clayton-backs-improvements-to-cybersecurity-disclosures/（最終検索日2017年8月11日）

[12]同上

[13]「SEC委員長指名のジェイ・クレイトンは前職ゴールド・マンサックス弁護士としての仕事を弁明」2017年3月23日 C-SPAN.org, https://www.c-span.org/video/?425840-1%2Fsec-nominee-jay-clayton-defends-prior-work-lawyer-goldman-sachs& start;=7116 （最終検索日2017年11月28日）

[14]SECは投資会社をサイバー攻撃前に適切なサイバーセキュリティ方針と手順の導入を怠ったとして起訴」SEC（2017年7月2日、3日午後4時18分）、https://www.sec.gov/news/pressrelease/2015-202.html

[15]同上

[16]Alejandro H. Cruz, Craig A. Newman & Michael F. Buchanan、取締役会でのサイバー:リスクと監視のバランスが必要」PATTERSON BELKNAP（2017年7月18日午後4時28分）、https://www.pbwt.com/privacy-and-data-security/data-security-law-blog-2/cyber-board-room-balancing-ris k-oversight/

[17]同上

[18]Michael Krimminger & Cleary Gottlieb Steen、「金融機関に対するニューヨーク当局によるサイバーセキュリティ規則が適用開始」HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION（2017年7月26日午後2時58分）、https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institution s-enter-into-effect/

[19]例としてPalkon対Holmes事件を参照。2014 WL 5341880（D.N.J. 2014年）

[20]賠償責任のエンジニアリング：「原告弁護士団がデータプライバシー・セキュリティ訴訟の拡大へ働きかけ」米商工会議所法改革機関 http://www.instituteforlegalreform.com/research/engineered-liability-the-plantiffs-bars-campaign-to-expand-data-prviacy-and-security-litigation（最終検索日2017年11月21日）

[21]内部監査協会（IIA）調査研究財団6、サイバーセキュリティ：取締役会が聞くべき質問とは何か（2014年）

[22]同上、14ページ

[23]同上

[24]同上

[25]同上、9ページ

[26]同上

[27]同上

[28]同上、16ページ

[29]同上

[30]同上

[31]同上

[32]コーン・フェリー、「デジタル時代をナビゲートする：取締役と役員のためのサイバーセキュリティ決定版ガイド」（2015年）

[33]同上、2ページ

[34]同上

[35]同上、3ページ

[36]同上、2ページ

[37]同上、5ページ

[38]同上

[39]同上

[40]スペンサースチュアート、「2016年版グローバル取締役会調査2」（2016年）

[41]同上

[42]同上、18ページ

[43]同上

[44]同上

[45]同上、21ページ

[46]同上、16～17ページ

[47]同上

[48]同上、19～20ページ

[49]同上

[50]「2017年版NACDによるサイバーリスク監視に関する取締役向けハンドブック」全米取締役協会（NACD）（2017年）、https://www.nacdonline.org/Store/ProductDetail .cfm ?ItemNumber= 10687（最終検索日2017年11月21日）

[51]同上。

[52]世界経済フォーラムによる報告書3、「サイバーレジリエンス強化のための取締役会向け原則とツール」（2017年）

[53]同上、4ページ

[54]同上、8ページ

[55]同上

[56]同上

[57]同上

[58]同上

[59]同上

[60]同上

[61]同上

[62]同上

[63]同上