



2018 年度ビジネスリスクマネジメント委員会 報告書

デジタル時代のビジネスリスクマネジメント
～企業経営者が取り組むべき課題～

2019 年 8 月

公益社団法人 経済同友会

目次

はじめに	1
I. サイバーセキュリティ	
1. 企業が直面するサイバー脅威 ——IoTの進展、グローバルにサプライチェーンが展開する中で	3
2. 企業経営者はサイバーセキュリティにどうコミットしていくべきか (1) 企業経営者のマインドセットを直ちに变革すべき (2) サイバーセキュリティへのアプローチの転換を (3) 全社挙げての横断的な取り組みを	4
3. IoTに関わるサイバーセキュリティ (1) 製品サイバーセキュリティ：ライフサイクルに応じた対策を (2) 制御システムセキュリティ：可用性を重視した対策を	8
4. 社会全体としてのサイバーセキュリティへの取り組みを	10
II. IoTの進展に伴った国境を超えた個人データの移転 ——GDPRなどのグローバル・ルールへの対応	11
III. デジタル化、AI化、IoTの進展の中でのビジネスリスクマネジメント ——ITを活用した「コンプライアンス」の実現を	14
おわりに	16
2018年度ビジネスリスクマネジメント委員会 活動一覧	17
2018年度ビジネスリスクマネジメント委員会 委員名簿	18

はじめに

- ・ 経済同友会では、2017 年度、2018 年度にビジネスリスクマネジメント委員会を設置し、「法務、財務、技術等に関するビジネスリスクの調査研究と経営者のリスクマネジメント力強化」に向けて活動を行ってきた。
- ・ 2017 年度には、同委員会委員の関心が高かった①海外 M&A の失敗、②海外子会社の会計不正、③サイバー攻撃を取り上げ、専門家からのヒアリングや企業経営者の議論を通じて得られた知見をもとに、ビジネスリスクマネジメントを考える上で企業経営者が心がけるべきことについて報告書を取りまとめた。
- ・ デジタル化が急速に進展した現在、グローバルに張り巡らされたネットワークが重要なインフラとなっており、クラウドコンピューティングも普及している。また、2020 年東京オリンピック・パラリンピック開催を控える中でサイバー攻撃も懸念されることから、サイバー脅威への対応が企業経営者にとって喫緊の課題となっている。
- ・ しかし、大企業でも「経営層の理解と対策の推進」を課題として認識している企業が多く¹、また、中小企業の多くは、資金や人材不足によってサイバーセキュリティ対策が十分でない²。
- ・ そこで、2018 年度には、サイバーセキュリティを中心とした技術に関するリスクに対するマネジメントを取り上げることとした。特に、モノがインターネットでつながる IoT (Internet of Things) の急速な進展に注目して、サイバー攻撃の現状を把握するとともに、企業経営者としてどのようなリスクマネジメントに取り組むべきかという視点をもって議論した。
- ・ また、2018 年 5 月に適用が開始された GDPR (EU 一般データ保護規則) は、国境を越えた個人データ移転を規律するとともに、域外にも適用されるものであることから、特に EU 域内に拠点を有したり、EU 居住者向けにサービスを提供したりする日本企業にとっては法務面やシステム面の対応が

¹ 上場企業等を対象とした平成 28 年度内閣サイバーセキュリティセンター委託調査「平成 28 年度企業のサイバーセキュリティ対策に関する調査報告書」では、「サイバーセキュリティの取組において経営層の理解と対策の推進を課題として認識している企業は、63.2%である」と指摘している。

² 平成 29 年 6 月 30 日大阪商工会議所「中小企業におけるサイバー攻撃対策に関するアンケート調査結果」では、「『現在実施している情報セキュリティ対策で十分ではない』と回答した企業は約 7 割 (68%) となっており、その理由として「経費がかけられない」(60%)、「専門人材がないのでわからない」(48%) をあげた回答が多かった」と指摘している。

必要となることから、GDPR の概要や実践的な取り組みに関する知見も深めてきた。

- ・ さらに、昨今、検査データの改ざんや会計不正などの企業不祥事が多発している現状を真摯に受け止めるとともに、デジタル化が急速に進展する現在、コンプライアンスの実現にどのように取り組むべきか、改めて考える機会を設けた。
- ・ 本報告書は、企業経営者にサイバーセキュリティへの理解をあらためて促すため、最低限取り組むべきことを整理して、とりまとめたものである。

I. サイバーセキュリティ

1. 企業が直面するサイバー脅威

——IoTの進展、グローバルにサプライチェーンが展開する中で

- ・ デジタル化が急速に進展する現在、あらゆる情報がデータ化されている。企業では、リアルタイムでの在庫管理情報、売上や各種コスト等の財務情報、顧客情報等が IT システムによってデータ化されるとともに、インターネットを通じて、グローバルに海外子会社や委託先、取引先等と繋がっており、また、クラウドコンピューティングも普及し、今や IT システムなしの企業経営は想定することができない。
- ・ こうした中で、IT システムは、日々刻々と高度化・巧妙化するサイバー脅威に晒されており、機密情報や個人情報の漏洩やデータ改ざんのほか、システムの稼働停止による事業活動全体の停滞といった企業経営にとって極めて重大な影響を及ぼすおそれがある。その損害は、財産的なもの以上に、これまで培ってきた企業価値やブランドの毀損や、社会からの信頼失墜など、一瞬にして企業の存立に関わるほどの致命的なものとなる。一方、ほとんどのサイバー攻撃はその攻撃者を特定できず、匿名性の高い組織によるものとされ、攻撃者への賠償責任の追及は非常に困難である。
- ・ また、ここ数年、モノがインターネットで繋がる IoT が進展し、ターゲットとなる IoT 機器の増加によってサイバー攻撃の件数も急増している³。例えば、ウェブカメラが乗っ取られ、建物内部が不特定多数者に認識可能な状態になった事例が生じている。また、コネクテッドカーのハッキング、製造現場で利用される産業ロボットにネットワーク経由で侵入し不正操作がされる事例や、心臓ペースメーカー等の人命に直結する医療機器のセキュリティに脆弱性が発見された事例もある。
- ・ さらに、委託先のネットワークがサイバー攻撃を受けたり、製品に組み込むために委託先から購入した部品がマルウェアに感染していたりするなど、ビジネス全体に多大な影響を及ぼすサプライチェーンリスクも企業経営にお

³ 平成 31 年 3 月 7 日警察庁「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」では、サイバー攻撃の情勢等について、「インターネットとの接続点に設置したセンサーにおいて検知したアクセス件数は、1 日 1 IP アドレス当たり 2,752.8 件と増加傾向」にあるとされる。アクセス件数が増加している主な要因としては、探索又は攻撃の標的が IoT 機器等へ拡大し多様化が進んでいることなどが挙げられる。

ける喫緊の課題である。

- ・ われわれ企業経営者は、こうしたサイバー攻撃を企業価値や企業の存立への重大な脅威として捉え、常に対峙していく必要がある⁴。

2. 企業経営者はサイバーセキュリティにどうコミットしていくべきか

(1) 企業経営者のマインドセットを直ちに変革すべき

- | |
|--|
| <ul style="list-style-type: none">・ サイバー攻撃は、長年にわたって創造してきた企業価値やブランド、信頼を一瞬で破壊しかねない、企業の存立や持続可能性への重大な脅威である。企業経営者はこの重大な脅威に対して危機感をもつべきである。・ サイバーセキュリティは、BCP（事業継続計画）やリスクマネジメントの一環であることを超えて、将来に向けた積極的な企業の成長戦略への投資として喫緊に取り組むべきである。 |
|--|
- ・ 2018年10月の本会代表幹事ミッション（米国）では、デジタル化、特にサイバーセキュリティ分野で日本企業が立ち遅れている点を指摘する声が多く聞かれた。同報告書にも「AIの進化に伴い、サイバーセキュリティの世界も日々進化している。世界のデータ管理は大半がクラウド化しているにも関わらず、多くの日本企業は未だに自前のサーバーを所有し、独自システムでデータを管理している。汎用性の低いシステムを利用している結果、日本企業のセキュリティーシステムは3世代前のレベルに留まっており、強い危機感をもって刷新されるべき、との警告もあった。（Tanium・Orion Hindawi氏）」と記載されている⁵。
 - ・ われわれ日本の企業経営者は、こうした「多くの日本企業で導入されているシステムは、3世代遅れている」という警告を真摯に受け止め、危機感をもって、早急にデジタル化による変革やサイバーセキュリティへの投資を実践していかなければならない。
 - ・ サイバーセキュリティへの投資は、企業の利益獲得に直結するものではない。

⁴ 世界経済フォーラム（WEF）の「The Global Risks Report 2019」では、発生の可能性が高いグローバルリスクの4位に「データの不正利用または窃盗」、5位に「サイバー攻撃」が挙げられており、グローバル経営者はサイバーリスクを経営課題として捉えている。また、PwC「グローバル投資家意識調査2018」では、企業の成長に対する脅威の1位に「サイバー脅威」が挙げられている。

⁵ 2018年11月15日経済同友会「代表幹事ミッション（米国）報告書」9頁参照。

しかし、データ情報は、ヒト・モノ・カネと並ぶ重要な経営資源であり、その活用によって新たな付加価値を創造することができる。

- ・ その意味で、企業経営者は、デジタル化が指数関数的に進展する中で、サイバーセキュリティを単なるテクノロジーやコストの観点から考えるのではなく、BCP（事業継続計画）やリスクマネジメントの一環であることをも超えて、企業の存立や持続可能性を支えるための投資であると捉え、企業の成長戦略として必要な予算と人員を投入すべきである。
- ・ また、企業経営者は、「IT システムはテクノロジー特有の分野に関わる」「IT 部門に任せておけばよい」という先入観や部門任せの考えを捨て、直ちにマインドセットを変革し、リーダーシップをもってサイバーセキュリティへの投資を行うべきである。
- ・ そして、デジタル化、AI 化の急速な進展の中で、サイバーセキュリティの在り方が日々進化していくという視点を持ちながら、自社のビジネスをグローバルに展開していかなければならない。

(2) サイバーセキュリティへのアプローチの転換を

- | |
|--|
| <ul style="list-style-type: none">・ 機密性を重視した「情報セキュリティ」とともに、可用性をも重視した「サイバーセキュリティ」を意識した対策を講じるべきである。・ サイバー攻撃に対しては、100%完璧なセキュリティ対策はあり得ないことを前提として、不正侵入の早期発見と被害の最小化に向けて、直ちに復旧させるレジリエンスの考え方を採るべきである。 |
|--|
- ・ これまで、多くの企業経営者は、サイバー攻撃による機密情報や個人情報の漏洩などの機密性が損なわれることへの対策としての「情報セキュリティ」を考えてきた。
 - ・ しかし、IoT が急速に進展し、工場の操業停止や事業活動の停滞などを引き起こすサイバー攻撃が増加しつつある現状を考えれば、設備稼働の安定性を最優先とする可用性の観点からも「サイバーセキュリティ」を重視していくべきである。
 - ・ また、多くの日本企業は、常に完璧な対策を追求する傾向にある。しかし、サイバー攻撃は、日々刻々と極めて高度化・巧妙化しているため、気づかない間に対策をすり抜け、不正侵入を許してしまうという現状がある。

- ・ 企業経営者は、最新のサイバー攻撃の現状を把握するとともに、100%完璧なセキュリティ対策はあり得ないことを前提としながら、サイバー攻撃に直面した際にどのように対応していくべきかが最も重要であるというアプローチを採るとともに、サイバー攻撃の早期発見と被害の最小化のために直ちに復旧させるレジリエンスの考え方を採るべきである。

(3) 全社挙げての横断的な取り組みを

「IT システムはテクノロジー特有の分野に関わる」「IT 部門に任せておけばよい」という先入観や部門任せの考えを捨て、全社挙げての横断的な組織体制を構築すべきである。

- ・ サイバーセキュリティでは、サイバー攻撃の早期発見と被害の最小化に向けた初動対応が最も重要である。
- ・ その意味で、サイバーセキュリティには、IT システム部署だけでなく、プロダクトサービス、法務、財務、営業なども含めて全社挙げての横断的な組織体制の構築が必要である。そのためにも企業経営者が「IT システムはテクノロジー特有の分野に関わる」「IT 部門に任せておけばよい」という先入観や部門任せの考えを捨て、IT システムは企業全体のインフラそのものであること、サイバー攻撃は全社にダメージが及び、長年にわたって創造してきた企業価値や企業の存立への重大な脅威であることを企業全体で認識させるように努めるべきである。
- ・ また、組織体制の構築にあたっては、各部門や担当者の責任と権限を明確にするとともに、企業経営者が初動対応について適切かつ迅速に判断できるように直ちに必要な情報が提供されることを意識しなければならない。
- ・ 企業経営者は、こうした体制の構築とともに、全従業員のサイバー脅威に対する感度を高めていく施策を考え、必要な予算と人員の投入を検討する。その検討にあたっては、サイバーセキュリティを企業の成長戦略への投資であることを念頭に置く必要がある。
- ・ そして、2020 年東京オリンピック・パラリンピックなどの大規模なイベントを控え、取組み可能な施策は早急に講じなければならない。一方、専門人材の育成や技術的な体制構築等については、サイバーセキュリティが企業の存立や持続可能性に関わる重大な経営課題であることを念頭に置きながら

中長期的に取り組んでいくべきである。

- ・ また、構築したサイバーセキュリティ体制は適宜見直していく必要がある。

(具体的な取り組み)⁶

●早急に対応すべき施策

- ✓ セキュリティポリシーの策定、全従業員への周知徹底（経営者自身のメッセージ発信、研修）
- ✓ 自社に関連する脅威がリスクとして顕在化するシナリオの策定・評価（対応のための優先順位を付ける）
- ✓ サイバーインシデント発生時の対応態勢の整備（CSIRT：Computer Security Incident Response Team⁷）
- ✓ 適切かつ迅速な初動対応を可能とするための情報収集・報告体制の構築
- ✓ サイバー脅威に直面した事態を想定した平時における訓練、研修

●中長期的課題

・実効性のある体制構築

- ✓ 早期にサイバー攻撃を発見するためのモニタリング体制の構築（ソフトウェアによる自動検出等）
- ✓ アクセス制限など、ネットワーク接続体制の構築（インターネットに繋がる情報と遮断すべき情報を分けるなど情報のヒエラルキーを考えた上で、全体の枠組みの中で体系化する）
- ✓ セキュリティ監査の確立と実行

・人材育成など

- ✓ 企業の実情に応じたセキュリティ専門人材の育成（前提として、初等・中等教育におけるIT教育の推進）
- ✓ 上記シナリオを踏まえた人材の配置
- ✓ 全社を横断したセキュリティ統括部門の設置（プロジェクトマネジメント、テクノロジー、リスクマネジメントを融合させたチーム）

⁶ なお、経済産業省及び独立行政法人情報処理推進機構では、企業経営者を対象とした「サイバーセキュリティ経営ガイドライン Ver.2.0」を策定している（平成29年11月16日公開）。

⁷ CSIRT（Computer Security Incident Response Team）：情報システムへのサイバー攻撃に対応するための組織体制

3. IoTに関わるサイバーセキュリティ

企業経営者は、IoTの急速な進展を捉え、IoTを前提としたサイバーセキュリティを考えることが急務である。以下、ネットワークに繋がる製品に関するセキュリティと制御システムに関するセキュリティに分けて考えていく。

(1) 製品サイバーセキュリティ：ライフサイクルに応じた対策を

現在、ネットワークに繋がった膨大な数の製品を踏み台にして、サイバー脅威が拡散していく事態が生じていることから、製品開発、製造、市場運用というライフサイクルに応じた対策を講じる必要がある。

・ 製品開発・設計段階：セキュリティ・バイ・デザインの発想を

これまで製品開発や設計の段階では、製品の品質保証が重視されていたが、IoTが進展しつつある現在では、製品がネットワークに繋がる点を重視してサイバーセキュリティの機能や観点を組み込むセキュリティ・バイ・デザインの発想を採り入れるべきである。すなわち、想定されるサイバー脅威を分析した上で、製品にはどのような機能を持たせるべきか、その機能を持たせるためにはどのような設計をするべきかというアプローチを採る必要がある。このようなアプローチを採用するためにも、サイバーセキュリティに精通した人材が製品の開発・設計に関与していくべきである。

また、開発・設計段階では、多くの開発者や委託先が関わっているため、開発・設計段階の関与者に対して、サイバーセキュリティに関する継続的な教育研修が欠かせない。

・ 製造段階：サプライチェーン全体を挙げての対策を

例えば、外注先から購入した部品に脆弱性があり、それを組み込んで完成品として出荷する場合は考えられる。このようなサプライチェーンリスクについては、自社だけでなく、外注先などを含めたサプライチェーン全体で、IoTにおけるサイバーセキュリティに対する感度を高め、全体で取り組むことができる実効性がある対策を講じなければならない。

また、ネットワークへのサイバー攻撃では、最初にサプライチェーンの

脆弱な部分が狙われ、その後直ちに全体に拡散していくため、可能な限り脆弱な部分をなくすことに努めるべきである。

- ・ 市場運用段階：平時からの対応検討を

製品が市場に出荷された後に第三者から製品の脆弱性を指摘された場合に、平時からどのように対応をするべきかを考えておく必要がある。その際、特に製品製造部門や品質管理部門と連携しながら、製造や販売する製品の脆弱性に対応するためのチーム（PSIRT：Product Security Incident Response Team⁸）の構築が有効である⁹。

(2) 制御システムセキュリティ：可用性を重視した対策を

- ・ これまで、工場における製造ラインを自動運転するために必要な監視・制御システムは専用のシステムとして作られており、インターネットを通じて外部機器と繋がっていなかったため、外部からの不正侵入は少なかった。
- ・ しかし、IoT の進展によって制御システムがコネクテッドになり、外部とのデータのやり取りが急増していることから、制御システムに対するサイバー攻撃の増加が報告されている。
- ・ 特に制御システムでは可用性が重視され、システム停止の回避と安定稼働が最優先となる。
- ・ そのため、制御システムに関するサイバーセキュリティを考える上では、想定される脅威とその脅威が顕在化するシナリオとしてどのようなものが考えられるか、どの段階で検知できるかを分析することが重要である¹⁰。
- ・ その上で、早期にサイバー攻撃を検知できる体制を構築するとともに、検

⁸ PSIRT（Product Security Incident Response Team）：製造や販売する製品の脆弱性に対応するための組織体制

⁹ 自動車のハッキングへの PSIRT 対応の一例として、実装していた OTA（ソフトウェア遠隔更新機能）を開発段階から組み込んでいたため、リコールを行うことなく脆弱性の改修対応を行うとともに、事前のセキュリティ研究者との連携により、公開に合わせて改修対応（アップデートパッチ適用）を準備していたことによって適切に対処できた事例がある。

¹⁰ 2015 年 12 月、ウクライナ電力会社へのサイバー攻撃によって、住民 22 万 5,000 人に影響を及ぼす大規模停電が発生した。制御システムへの攻撃と同時にコールセンターにも攻撃を仕掛けられたとされ、コールセンターが多数の問い合わせに適切な対応をすることができなかった。

知後の対応が重要となるため、平時から訓練や研修を行い、対応能力を高めていかなければならない。

4. 社会全体としてのサイバーセキュリティへの取り組みを

- ・ サイバー攻撃は日々刻々と高度化・巧妙化しており、その対策の変化も非常に速いため、企業単独の努力だけでは十分に対応できないのが実情である。
- ・ 2020年には東京オリンピック・パラリンピック開催を控えており、わが国では大規模なサイバー攻撃が起こるのではないかという懸念もある。
- ・ そのためにも、サイバーセキュリティは、社会全体として取り組むべき問題であると捉えていくべきである。
- ・ これまで企業にとってセキュリティに関する事項は機密情報であった。しかし、サイバー攻撃が社会全体に対する脅威であり、積極的にセキュリティ対策に取り組んでいくためにも、企業同士でサイバー攻撃に関する情報共有や分析を行い、セキュリティ対応の向上に取り組んでいく ISAC¹¹のような組織を活用し、自社の対策を検討する際に他社事例を参考にしていくことが有用かつ重要である¹²。

¹¹ ISAC (Information Sharing and Analysis Center) : 同業者がサイバーセキュリティに関する情報の共有・分析、連携を行う組織であり。多くの業界で立ち上げられている。

¹² 例えば、日本の金融機関によって組織された金融 ISAC が、サイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行っている。

II. IoT の進展に伴った国境を超えた個人データの移転

——GDPR などのグローバル・ルールへの対応

- ・ モノがインターネットで繋がる IoT の進展に伴い、モノが個人情報を含むさまざまなデータを収集し、そのデータが国境を越えて移転していく時代が到来している。
- ・ この数年、世界では個人データの越境移転規制に関するルールの制定が急速に進んでおり、グローバルに展開する日本企業もその対応を迫られている現状を企業経営者は当然把握していなければならない。
- ・ 特に、2018 年 5 月に適用が開始された EU の一般データ保護規則 (GDPR) では、個人データ保護が重視され、EU 域外への個人データ移転が規制されるとともに、データポータビリティに関する権利や忘れられる権利などが保障されている。個人データ侵害が発生した場合には、認識後 72 時間以内に当局への通知が必要であり、また、GDPR 違反の場合には巨額の制裁金が課される可能性もあることから¹³、EU 域内に拠点を有する企業や EU 居住者向けにサービスを提供する企業は GDPR 違反という法務リスクに対応する必要がある。
- ・ しかし、GDPR の適用開始から 1 年経過した現在、いまだに GDPR に対応していない企業も少なくない¹⁴。未対応の企業は、グローバル化やデジタル化がますます進展する現在、早急の対応が急務である。
- ・ わが国では 2019 年 1 月に充分性の認定が得られたが、適用除外の対象は、EU 域内から日本への個人データの越境移転規制のみである。したがって、EU 域内から日本以外の国への越境移転を行う場合、例えば、EU 居住者のデータをグループ共有データベースに掲載し、世界各地のグループ企業からアクセス可能にする場合には、充分性の認定がなされた現在でも、依然として GDPR の越境移転の規律を受けることから、対応可能な体制を構築する必要がある。
- ・ なお、EU では、GDPR の他にも、「クッキー法」と言われる e プライバシ

¹³ 2000 万ユーロ以下または全世界の売上高の 4%以下のいずれか大きい金額を上限とする制裁金が課される可能性がある。

¹⁴ 2019 年 5 月 25 日付日本経済新聞によれば、日本の主要企業 100 社のうち、全体の 45%が GDPR への対応を終えていないとのことである。

一規則案の動向が注目される¹⁵。同規則は、電子通信データ全般に関する規制であり、域外適用も予定しているため、IoT を活用するビジネスをグローバルに展開する際には、多大な影響を及ぼす可能性があることに留意する必要がある。

- ・ 中国では、2017年6月にサイバーセキュリティ法が施行された。同法では、中国国内における企業に対してサイバーセキュリティ対策を求めるとともに、個人情報の取り扱いを規制する。企業のビジネス展開において、最もインパクトが大きいのは、個人情報に限られず、産業データを含む「重要データ」の国外移転規制であり¹⁶、「重要データ」の範囲などその不明確性が指摘されていることから、IoT ビジネスに関わる広範なデータローカライゼーション規制¹⁷として機能する可能性があることが懸念されている¹⁸。そのため、中国へのビジネス展開の際には十分留意しなければならない。
- ・ 2020年1月には、カリフォルニア州の消費者プライバシー法（2018年6月成立）が施行される。同法は、成立後も改正が加えられ、いまだにガイドラインの策定も完了していないため¹⁹、同州の居住者の個人情報を取得する企業は施行までの半年間のうちに対応することが急務である。
- ・ わが国の個人情報保護法は2003年に制定され（2005年全面施行）、2015年

¹⁵ 各加盟国において国内法化のステップが必要な現行のeプライバシー指令と異なり、eプライバシー規則では直接適用がされる。また、通信機能を有するあらゆるサービスが対象となり、機密保持すべき電子データとして、通信内容に加え、課金の有無にかかわらず、通信日時や通信機器の場所といったメタデータが含まれる（2017年1月に公表された規則案）。中崎尚「Q&Aで学ぶGDPRのリスクと対応策」（商事法務、2018年）264頁参照。

¹⁶ 中国サイバーセキュリティ法（ネットワーク安全法、中華人民共和国网络安全法）第37条「重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。業務の必要性により、国外に対し確かに提供する必要がある場合には、国のネットワーク安全情報化機関が国务院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。法律及び行政法規に別段の定めのある場合には、当該定めに基づいて行う。」https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf

¹⁷ 総務省平成30年版情報通信白書21頁「データローカライゼーション規制は、個人データの越境移転行為に焦点を当てる越境データ移転規制と異なり、ある国において（あるいは外国から当該国を対象に）特定の事業活動を営む場合に、当該事業活動に必要なサーバーやデータ自体の国内設置・保存を求める規制である。また、越境個人データ移転規制では原則として本人の同意があれば海外への移転が可能であるが、データローカライゼーション規制では、対象データが個人データに限られないため、本人の同意による移転は行い得ず、データの越境移転にあたっては、当該国政府の許可等が必要となることが多い。」

¹⁸ 同白書22頁参照。

¹⁹ 2019年6月現在。





改正では「個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、」同法施行後3年ごとの見直しがなされることとなっていたため²⁰、本年4月に個人情報保護委員会から「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」が公表された。

- ・ このように、個人データに関する規制については、グローバルに見ても²¹、日本政府の動きも急速に進んでいる。企業経営者も、個人データ保護法制を含むデータ法制に関する動向を絶えず注視し、対応していかなければならない。

(対応例)

- ✓ 法務部門と情報セキュリティ部門を中心とした自社グループへの影響を見極めた対応と必要な予算の確保
- ✓ 事故発生の場合には短時間に当局への通知を行う必要があることを考え、直ちに企業経営者に必要な情報提供、報告を上げることができる体制の構築
- ✓ 法務に関する体制が弱い新興国の拠点への本社スタッフ派遣、ノウハウの共有、サポート

●データ政策の国際比較

		 米国	 日本	 EU	 中国
個人情報	法律	個人情報を保護する包括的な法律なし	個人情報保護法	一般データ保護規則 (GDPR)	サイバーセキュリティ法
	域外移転	原則自由	原則として本人同意が必要		基幹情報 インフラ設備運営者 (政府機関、エネルギー、 財政、輸送等) が 保有する個人情報、 重要データは 原則域外移転禁止
産業情報	域外移転	原則自由 ※安全保障分野を除く			
	重要産業分野	クラウド使用に関する政府推奨あり	医療、金融分野にはデータ管理ルールあり	公共分野などのデータの国内管理義務あり	
データ管理/ 利用の主導者、 基本的考え		企業 データの自由な流通	米・EUと 連携したルール整備	個人 情報自己決定権	国家 データ流通の制限

出典：経済同友会「Japan 2.0 最適化社会の設計—モノからコト、そしてココロへ—」(2018年12月11日)

²⁰ 平成27年改正法附則第12条第3項

²¹ 同白書23頁「中国以外のアジア諸国では、例えばインドネシアは、個人データに対しデータローカライゼーションを規定する非常に厳しいデータ移転制限がある。」

Ⅲ. デジタル化、AI化、IoTの進展の中でのビジネスリスクマネジメント

——ITを活用した「コンプライアンス」の実現を

- ・ 昨今、わが国では、データ改ざんや不正会計等のさまざまな企業不祥事が起っており、これまでにないほど日本企業に対する信頼が大きく揺らいでいる。なぜ、このようなコンプライアンス違反が次々に起こるのか、われわれ企業経営者としても真摯に考えなければならない。
- ・ 多くの企業経営者は、コンプライアンスを重視した企業文化や風土を作り出していくための努力をしてきたし、全従業員に対して企業理念やコンプライアンスに関するメッセージを発信し続け、実践してきた。そして、今後も地道に努力していくしかないであろう。
- ・ その上で、デジタル化、AI化、さらにはIoTが急速に進展する現在、ITを活用したコンプライアンスの実現を目指すことが急務である。
- ・ 現在、企業にはあらゆるデータが存在している。例えば、会計数値、財務データだけでなく、従業員一人ひとりの出退勤時刻や時間外労働等の行動もデータ化されている。在庫管理においてもモノがインターネットに繋がるIoTの活用が増加しつつある。
- ・ このように、IT、特にAIやIoTを活用したモニタリングによって不審な行動や兆候を自動的かつ早期に発見することが可能になりつつあり、今後も技術が急速に進展していくと考えられる。
- ・ こうした最新の技術を活用したモニタリングや分析手法は、不正に対して極めて強い抑止力を有し、仮に不正が発生した場合でも、異常値の検出などを捉えることによって、早期に発見され、財産的な損害のほか、企業のブランドや信頼の低下など、被害の最小化に大きく貢献するはずである。
- ・ 一方、モニタリングが行き過ぎると、プライバシーや個人の尊厳の侵害につながる可能性もあることも認識する必要がある。最近とりまとめられた「人間中心のAI社会原則」（平成31年3月29日統合イノベーション戦略推進会議決定）²²においても、「AIの利用は、憲法及び国際的な規範の保

²² 「基本理念」として、(1) 人間の尊厳が尊重される社会、(2) 多様な背景を持つ人々が多様な幸せを追求できる社会、(3) 持続性ある社会、「人間中心のAI社会原則」として、(1) 人間中心の原則、(2) 教育・リテラシーの原則、(3) プライバシー確保の原則、(4) セキュリティ確保の原則、(5) 公正競争確保の原則、(6) 公平性、説明責任及び透明性の原則、(7) イノベーションの原則が挙げられている。

障する基本的人権を侵すものであってはならない」「AI に関わる政策決定者や経営者は、・・・(中略)・・・AI の正確な理解と、社会的に正しい利用ができる知識と倫理を持っていなければならない」と謳われている。企業経営者は技術の進展に伴って生じる倫理の問題を常に真摯に考え続け、人間中心の社会の構築につながる価値創造に挑むとともに、透明性を高めたコンプライアンス体制の構築・運用に努めていくべきである。

おわりに

- ・ サイバーセキュリティは、これからの時代においてビジネスリスクマネジメントの最重要課題の一つであり、企業の持続的な成長に向けた戦略的な投資として捉えることを強く意識すべきである。そのためにも、われわれはデジタル技術の急速な進展に対する感度を高め、日々刻々と高度化・巧妙化していくサイバー脅威について、常に危機感を持ちながら、企業経営にあたっていかなければならない。
- ・ また、リスクマネジメント全般についても、グローバル化やデジタル化の進展に伴い、リスクも高度化することから、法務、財務、技術等について常に最新の知見を得ながら、真のコンプライアンスの実現に向けて具体的に取り組むことに努めていく。
- ・ そして、われわれ企業経営者は、「企業は社会的存在である」ことを改めて認識しつつ、果敢にリスクテイクをしながら、グローバルにビジネスを展開し、社会に貢献していく所存である。

2018年度ビジネスリスクマネジメント委員会活動一覧 ※所属、役職は当時

会合	開催日	内容
第1回	2018 6/1	ミニパネルディスカッション 「外資系企業とグローバル展開する日本企業の比較」 (パネリスト) 岩本 敏男 副委員長、田中 能之 副委員長、 山崎 孝一 副委員長 (コーディネーター) 遠山 敬史 委員長
第2回	2018 8/8	前年度の総括及び今年度の委員会運営方針について ※7/3 第1回正副委員長会議開催 ※アンケート実施：サイバー攻撃の他に、海外 M&A、海外 子会社の会計不正への関心が高い結果となった（前年と同 様）。 ※10/10 2017年度ビジネスリスクマネジメント委員会報告 書公表
第3回	2018 11/21	講演：「IoT でつながる製品・設備のサイバーセキュリティ」 PwC コンサルティング合同会社 パートナー 林 和洋 氏
第4回	2019 1/25	講演： 「経営者が知っておくべき GDPR の基礎知識と運用課題」 アンダーソン・毛利・友常法律事務所 弁護士 中崎 尚 氏 講演：「NTT データグループにおける GDPR 対応について」 NTT データ 法務室長 松下 健 氏 ※1/15 第2回正副委員長会議開催
第5回	2019 3/5	講演：「サイバー攻撃の傾向とサイバーセキュリティ確保の 考え方」 警察庁 情報通信局情報技術解析課 サイバーテロ対策技術室長 野本 靖之 氏
第6回	2019 4/2	ディスカッション ① コンプライアンス、企業経営者としての原点 ② サイバーセキュリティ ※3/29 第3回正副委員長会議開催
第7回	2019 6/3	2018年度ビジネスリスクマネジメント委員会報告書案討議

2018年度 ビジネスリスクマネジメント委員会 委員名簿

2019年8月現在

委員長

遠山 敬史 (パナソニック 常務執行役員)

副委員長

岩本 敏男 (NTTデータ 相談役)

小野 傑 (西村あさひ法律事務所 代表パートナー)

木村 浩一郎 (PwCあらた有限責任監査法人 代表執行役)

幸田 博人 (イノベーション・インテリジェンス研究所 取締役社長)

田中 能之 (デュポン 取締役社長)

増田 健一 (アンダーソン・毛利・友常法律事務所 パートナー)

守本 正宏 (FRONTEO 取締役社長)

山崎 孝一 (キックマン 取締役専務執行役員)

委員

朝倉 陽保 (丸の内キャピタル 取締役社長)

浅沼 章之 (浅沼組 執行役員)

穴山 眞 (日本政策投資銀行 取締役常務執行役員)

荒川 詔四

有田 喜一郎 (群栄化学工業 取締役 社長執行役員)

池上 芳輝 (イケガミ 取締役社長)

諫山 滋 (三井化学 監査役)

石井 健太郎 (石井食品 会長)

石黒 不二代 (ネットイヤーグループ 取締役社長 CEO)

石田 茂 (電通 執行役員)

井上 哲 (フィリップ モリス ジャパン 職務執行役 副社長)

入江 仁之	(アイ&カンパニー 取締役社長)
植木 義晴	(日本航空 取締役会長)
植村 浩典	(ユー・エム・アイ 取締役社長)
大賀 昭雄	(東通産業 取締役社長)
大河原 愛子	(ジェーシー・コムサ 取締役会長)
大久保 和孝	(大久保アソシエイツ 取締役社長)
大森 美和	(バンク・オブ・アメリカ・エヌ・エイ東京支店日本における代表者 東京支店長)
岡田 和樹	(Vanguard Tokyo法律事務所 代表弁護士)
梶川 融	(太陽有限責任監査法人 代表社員 会長)
蒲野 宏之	(蒲野綜合法律事務所 代表弁護士)
上斗米 明	(パソナグループ 専務執行役員)
北地 達明	(有限責任監査法人トーマツ パートナー)
北野 泰男	(キュービーネットホールディングス 取締役社長)
木下 信行	(東京金融取引所 取締役社長)
清原 健	(清原国際法律事務所 代表弁護士)
楠原 茂	(みさき投資 取締役CFO)
窪田 政弘	(前澤化成工業 取締役社長)
栗原 美津枝	(日本政策投資銀行 常勤監査役)
桑原 茂裕	(アフラック生命保険 シニアアドバイザー)
斎藤 聖美	(ジェイ・ボンド東短証券 取締役社長)
斉藤 剛	(みさき投資 チーフ・エンゲージメント・オフィサー)
酒井 重人	(グッゲンハイム パートナーズ 取締役社長)
坂本 和彦	(Veoneer Inc. 取締役)
佐川 恵一	(リクルートホールディングス 取締役専務執行役員)
櫻井 祐記	(富国生命保険 取締役専務執行役員)
笹尾 佳子	(レオパレス21 社外取締役)

椎野孝雄 (キューブシステム 取締役 (社外))
塩見勝 (住友商事 執行役員)
正田修 (日清製粉グループ本社 名誉会長相談役)
陳野浩司 (国際金融公社 チーフ・インベストメント・オフィサー)
菅野健一 (リスクモンスター 取締役 founder)
杉野尚志 (レイヤーズ・コンサルティング 代表取締役CEO)
杉本文秀 (長島・大野・常松法律事務所 マネージング・パートナー)
関根愛子 (日本公認会計士協会 相談役)
銭高一善 (銭高組 取締役会長)
銭高久善 (銭高組 取締役社長)
高島征二 (協和エクシオ 名誉顧問)
高橋勉 (有限責任 あずさ監査法人 副理事長)
多田雅之 (アルファパーチェス 取締役社長兼CEO)
田中一行 (日立化成 取締役会長)
田中豊 (アートグリーン 取締役社長)
田沼千秋 (グリーンハウス 取締役社長)
近浪弘武 (日本コンベンションサービス 取締役社長)
津上晃寿 (キヤノントッキ 取締役会長兼CEO)
辻伸治 (SOMPOホールディングス グループCOO グループCBO 取締役 代表執行役副社長)
土屋達朗 (フジタ 取締役副社長)
富田秀夫 (リフィニティブ・ジャパン 取締役社長)
内藤隆明 (縄文アソシエイツ 取締役社長)
長嶋由紀子 (リクルートホールディングス 常勤監査役)
中原広 (信金中央金庫 専務理事)
中防保 (レイヤーズ・コンサルティング 代表取締役COO)
永山妙子 (プレリ्यूダーズ 代表取締役)

能見 公一 (ジェイ・ウィル・コーポレーション 顧問)
野田 由美子 (ヴェオリア・ジャパン 取締役社長)
野村 俊明 (安藤・間 特別顧問)
芳賀 日登美 (ストラテジック コミュニケーション R I 取締役社長)
林 明夫 (開倫塾 取締役社長)
平井 康文 (楽天 副社長執行役員)
平賀 暁 (マーシュ ブローカー ジャパン 取締役会長)
平田 正之 (D T S 取締役)
平野 圭一 (アクティヴィ 代表取締役CEO)
平野 大介 (マイスターエンジニアリング 取締役社長)
ハリー・A・ヒル (オークローンマーケティング 取締役)
廣瀬 雄二郎 (日本情報通信 取締役社長)
深堀 哲也 (レーサム 常勤監査役)
福井 英治 (オー・ジー 取締役社長)
古河 建規 (S O L I Z E 取締役会長)
堀越 健 (コマツ 執行役員CFO)
増山 美佳 (増山 & C o m p a n y 代表)
松尾 憲治 (明治安田生命保険 特別顧問)
松尾 時雄 (日本カーバイド工業 取締役社長)
松崎 正年 (コニカミノルタ 取締役会議長)
宮内 淑子 (ワイ・ネット 取締役社長)
三宅 伊智朗 (S & P グローバル・ジャパン 特別顧問)
森 正勝 (国際大学 特別顧問)
矢口 秀雄
山口 公明 (セントケア・ホールディング 取締役)
山本 達也 (エーオンジャパン 取締役社長)
横山 隆吉 (不二工機 取締役社長兼グループCEO)

横山 晴通 (不二工機 取締役専務執行役員)

渡部 一文 (アマゾンジャパン バイспレジデント)

以上101名

事務局

齋藤 弘憲 (経済同友会 執行役)

中島 美砂子 (経済同友会 政策調査部 調査役)