第4節 5G時代のサイバーセキュリティ

1 深刻化・複雑化を増すサイバーセキュリティ

これまで述べてきたように、5GやAI、IoTといった先端技術の活用が社会により一層普及し、データの活用がさらに盛んになることで、経済・社会のデジタル化が一層進展し、我々の生活はより便利で豊かなものとなる。一方で、デジタル化の進展により、サイバーセキュリティに関するリスクへの対応の重要性が高まっている。2018年に閣議決定されたサイバーセキュリティ戦略[*1]においても、サイバー空間と実空間の一体化が進展する中では、サイバー攻撃により深刻な影響が生じる可能性が指数関数的に拡大することについて述べられている。我々が真にデジタル化による恩恵を受けるためには、先端技術やデータの活用を進めるとともに、サイバーセキュリティに関する取組についても着実に進めることが重要である。

1 最近のセキュリティ事案

近年では国内外の様々なサイバー攻撃が報道等で話題となっているが、年々その手口も多様化してきており、サービスやサーバの停止、情報漏洩など大きな被害を発生させることも珍しくなくなってきている（図表3-4-1-1）。国内においてもセキュリティに関する事例として、次のようなものが話題となった。

図表3-4-1-1 昨今のサイバー攻撃の事例

国内事例	
2015年6月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年11月	東京オリンピック・パラリンピック競技大会組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年6月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年5月	国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）
2018年1月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
2020年	三菱電機、NECやNTTコミュニケーションズにおいて防衛関連情報を含む情報が外部へ流出した可能性が判明（不正アクセス）

海外事例	
2015年4月	フランスのテレビネットワーク TV5 Monde がサイバー攻撃を受け、放送が一時中断（標的型攻撃）
2015年6月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年5月	世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年9月	エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）

（出典）総務省

＊1 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf

ア　スマホ決済の不正利用に係る事案

2019年10月の消費税増税に伴う経済対策として、キャッシュレス決済での支払について還元が受けられる制度が始まったこともあり、2019年にはキャッシュレス決済の利用が拡大した。その中でもスマートフォンを利用した決済は、その手軽さや企業による大規模なキャンペーンが実施されたことから利用が拡大したが、それに伴ってセキュリティ事案も発生した。

独立行政法人情報処理推進機構（IPA）がとりまとめた「情報セキュリティ10大脅威　2020」[*2]においても、個人向け脅威の第1位に「スマホ決済の不正利用」が挙げられている（図表3-4-1-2）。

図表3-4-1-2　情報セキュリティ10大脅威　2020「個人」及び「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい（規則は遵守）
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

（出典）IPA（2020）「情報セキュリティ10大脅威　2020」を基に作成

例えば、コンビニエンスストア「セブンイレブン」を運営するセブン＆アイ・ホールディングス傘下のセブン・ペイは、2019年7月1日にバーコード決済サービス「7pay（セブンペイ）」のサービスを開始した。しかしながら、報道発表[*3]によれば、「身に覚えがない取引があった」旨のユーザからの報告がサービス開始の翌日から相次ぎ、同月4日には新規会員登録を停止することとなった。当該サービスはモニタリング体制の強化等の対策を実施したものの、同年8月には、サービス再開に向けた抜本的な対策のためには相当な時間を要するとして、同年9月のサービス廃止を発表した。

これは、攻撃者がどこかで不正に入手したIDやパスワードを利用したリスト型攻撃により引き起こされたもので、セブン＆アイ・ホールディングスは、二要素認証の導入といった、攻撃への安全対策が不十分だったこと等を理由として挙げている。

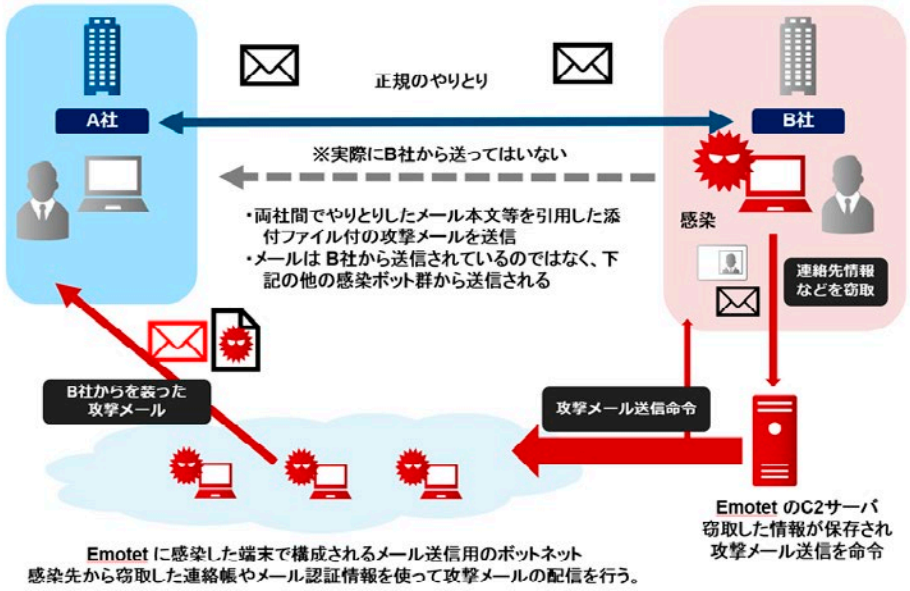
イ　マルウェア「Emotet」による被害の増加

また、一般社団法人JPCERTコーディネーションセンターによれば、2019年に入り、日本国内においてマルウェア「Emotet」に係る報告が増加してきているという[*4]（図表3-4-1-3）。

マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードを指すが、このマルウェアの特徴は、攻撃の対象となる者が実際に送信したメールなどを引用することにより、通常の業務でのメールを装った形で攻撃メールを送るという点である。

＊2　https://www.ipa.go.jp/files/000080871.pdf
＊3　セブン&アイ・ホールディングス（2019）「「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について」（https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf）
＊4　一般社団法人 JPCERT コーディネーションセンター（2019）「マルウエア Emotet の感染に関する注意喚起」（https://www.jpcert.or.jp/at/2019/at190044.html）

図表 3-4-1-3　Emotet感染拡大の流れ



（出典）一般社団法人JPCERTコーディネーションセンター（2019）「JPCERT/CC インシデント報告対応レポート2019年10月1日 ～ 2019年12月31日」*5

IPAによれば、当該攻撃メールにはファイルが添付されており、そのファイルを開くことによりマルウェアに感染するが、最近ではファイルをダウンロードするためのURLをメール本文に記載し、ダウンロード及び実行させるという手口も報告されているとのことである*6。IPAが公表している「情報セキュリティ10大脅威　2020」によれば、公益財団法人東京都保健医療公社や首都大学東京において感染が確認されており、2020年1月には、新型コロナウイルスに便乗した内容でメールが送信されているという。

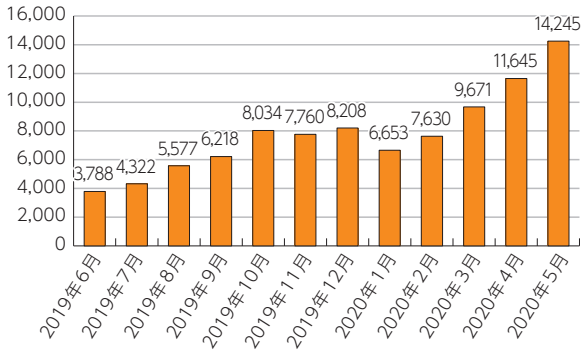
実際に送信されたメールの文面を利用し、過去にやりとりした相手からのメールであると攻撃対象者に信用させようとする点や、被害に遭ったユーザのメールをもとにして攻撃メールを作成する点など、攻撃手法がこれまでの標的型メールよりも巧妙になってきている。

＊5　https://www.jpcert.or.jp/pr/2020/IR_Report20200121.pdf
＊6　独立行政法人情報処理推進機構（IPA）（2019）「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」（https://www.ipa.go.jp/security/announce/20191202.html）

ウ　巧妙化するフィッシング詐欺

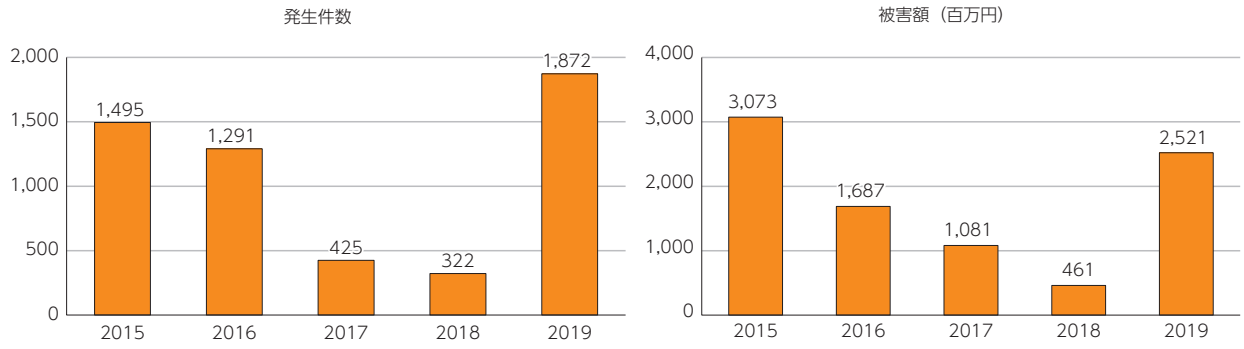
さらに、フィッシングによる個人情報の詐取も2019年に増加しており、上記で紹介した10大脅威の個人向け脅威の第2位として挙げられている。フィッシング対策協議会が2020年6月に公表した報告[*7]によると、フィッシングの報告件数は2020年1月から5月までにかけて急増しており、2020年5月には14,245件に達している（図表3-4-1-4）。また、警察庁のとりまとめ[*8]によれば、2019年9月からインターネットバンキングに係る不正送金事犯による被害が急増しているとのことであり、被害の多くは、SMS（ショートメッセージサービス）や電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられるとしている。2019年の発生件数は1,872件、被害額は約25億2,100万円と、発生件数は過去最高であった2014年に次ぐ件数となり、被害額も前年と比べて大幅に増加している（図表3-4-1-5）。

図表3-4-1-4　フィッシング報告件数



（出典）フィッシング対策協議会（2020）「2020/05 フィッシング報告状況」を基に作成

図表3-4-1-5　インターネットバンキングに係る不正送金事犯の発生件数及び被害額の推移



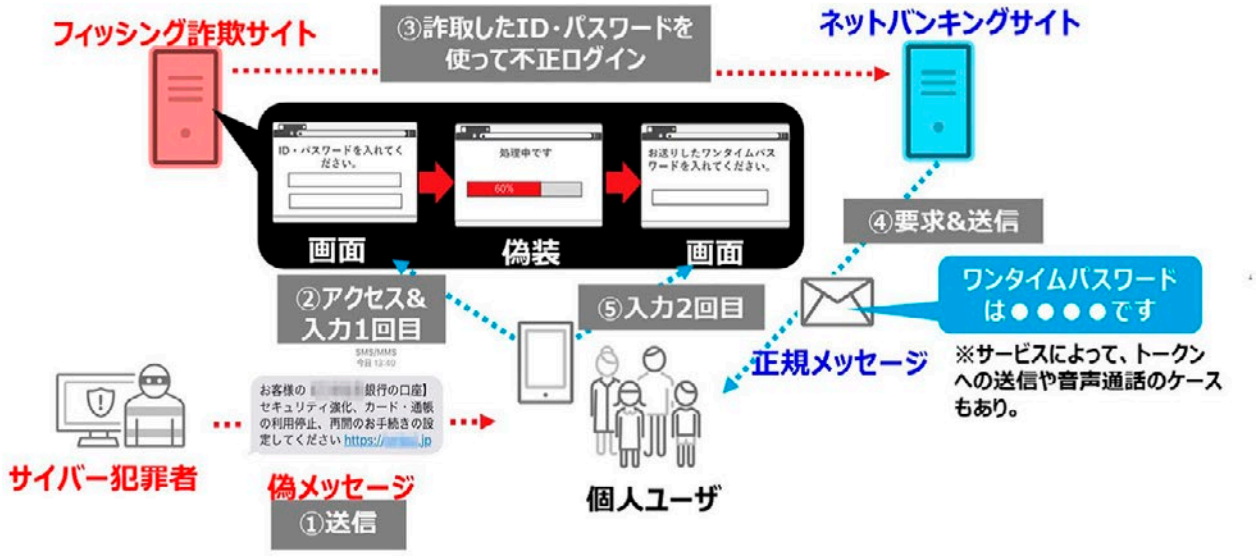
（出典）警察庁（2020）「令和元年におけるサイバー空間をめぐる脅威の情勢等について」を基に作成

トレンドマイクロからもフィッシングについての注意喚起がなされているが、同社によると、近年の傾向として、我が国のccTLD（country code Top Level Domain）である「.jp」を使用するものが増加しているほか、携帯電話事業者や宅配業者、金融機関を装ってSMSを利用し、ユーザの情報を詐取しようとする事案（スミッシング）が増加しているとのことである[*9]。特に、スミッシングについては、攻撃者が送信元を偽装して国際SMSを送信した場合、本来の送信元からのSMSと同一のスレッドで表示されるため、あたかも正規のメッセージであるかのように表示されてしまうといい、こういった巧妙な手口も被害の拡大の要因の一つであると考えられる[*10]。

＊7　フィッシング対策協議会（2020）「2020/05 フィッシング報告状況」（https://www.antiphishing.jp/report/monthly/202005.html）
＊8　警察庁（2020）「令和元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/R01_cyber_jousei.pdf）
＊9　トレンドマイクロ（2019）「国内ネットバンキングの二要素認証を狙うフィッシングが激化」（https://blog.trendmicro.co.jp/archives/22696）
＊10　トレンドマイクロ（2019）「法人システムを狙う脅迫と盗用　2019年上半期セキュリティラウンドアップ」（https://resources.trendmicro.com/jp-docdownload-form-m144-web-2019-1h-security-round-up.html）

さらに、国内の金融機関などがセキュリティ対策として提供している、ワンタイムパスワードや、乱数表といった認証情報を詐取する手口も確認されており、このような二要素認証の突破を狙うフィッシング詐欺は金銭被害に直結する脅威であると警告している（図表3-4-1-6）。

図表3-4-1-6　フィッシング詐欺によるワンタイムパスワード突破の概要



（出典）トレンドマイクロ（2020）「2019年年間セキュリティラウンドアップ」*11

2　セキュリティ事案による影響

ア　経済的な影響

先に述べたように、社会全体のICT化が進展するにつれて、これらサイバーセキュリティに関する事案はサイバー空間にとどまらず、我々の生活にも直接影響を与えるようになってきている。

例えば、令和元年版情報通信白書でも、様々な主体によりサイバーセキュリティに関する問題が引き起こす経済的損失が算出されているが、全世界で6,000億ドルから多いもので22兆5,000ドル、日本国内でも1社当たり数億円の損失が生じるものと算出されている（図表3-4-1-7）。

図表3-4-1-7　サイバーセキュリティに関する問題が引き起こす経済的損失

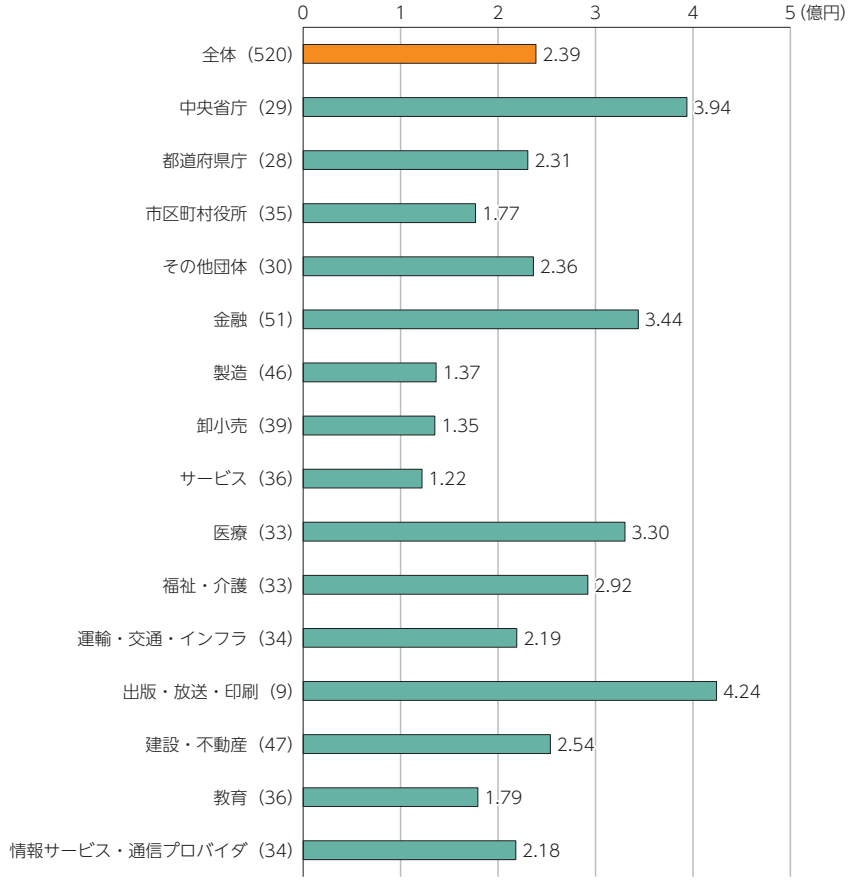
調査・分析の実施主体	対象の地理的範囲	対象年	経済的損失の概要	損失額
CSIS、McAfee	全世界	2017年	サイバー犯罪により生じるコスト	6,080億ドル
RAND Corporation	全世界	2017年	サイバーセキュリティインシデントにより生じるコスト	【直接】2,750億ドル ～6兆6,000億ドル 【直接＋波及】7,990億ドル ～22兆5,000億ドル
Cybersecurity Ventures	全世界	2021年【予測】	サイバー犯罪による損害額	6兆ドル
Microsoft、Frost & Sullivan	アジア太平洋	2017年	サイバーセキュリティインシデントによる損害額	1兆7,450億ドル
Accenture	日・米・加・英・独・仏・伊・西・豪・シンガポール・ブラジル	2018年	サイバー犯罪により生じる1社当たり平均コスト	1,300万ドル
	日本	2018年	サイバー犯罪により生じる1社当たり平均コスト	1,357万ドル
JNSA	日本	2018年	個人情報漏えいにより生じる1件当たり平均損害賠償額	6億3,767万円
トレンドマイクロ	日本	2017年	セキュリティインシデントにより生じる1組織当たり平均年間被害額	2億1,153万円

（出典）総務省（2019）「令和元年版情報通信白書」

＊11　https://resources.trendmicro.com/jp-docdownload-form-m197-web-2019-annualsecurityreport.html

また、トレンドマイクロが2019年に民間企業、官公庁及び自治体を対象に実施した調査[*12]においても、調査対象となった組織全体での年間平均被害総額は約2.4億円となり、4年連続で2億円を超えている（図表3-4-1-8）。

図表3-4-1-8　セキュリティインシデントによる年間平均被害総額



※（）内の数字はサンプルサイズ

（出典）トレンドマイクロ（2019）「法人組織におけるセキュリティ実態調査2019年版」を基に作成

ここ最近においても、例えば、先に挙げたセブンペイに係る事案に関して、セブン・アンド・アイ・ホールディングスの発表[*13]によると、2019年7月31日現在で、808人に合計約3,900万円の被害が生じたことが明らかになっている。

イ　生活への影響

サイバー攻撃による現実世界への影響は経済的な損失にとどまらない。例えば、2019年8月23日にはAmazonが提供しているアマゾン・ウェブ・サービス（AWS）が、空調設備の停止により大規模な障害を起こしたが、報道によると、その影響で決済サービスやオンラインショッピング、オンラインゲームやSNSなど、AWSを利用している幅広いサービスが停止することとなった。また、行政分野においても、2019年12月に発生した自治体向けのクラウドサービスの障害[*14]は、長期間にわたって数多くの自治体の運営に影響を及ぼした。これらの事案はサイバー攻撃により発生したものではないものの、サイバー攻撃がサイバー空間だけでなく我々のリアルな生活の様々な場面で影響を与えうることを再認識させるものであった。

＊12　トレンドマイクロ（2019）「法人組織におけるセキュリティ実態調査2019年版」（https://resources.trendmicro.com/jp-docdownload-form-m164-web-sor2019.html）
＊13　https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf
＊14　日本電子計算（2019）「自治体専用IaaSシステム「Jip-Base」の障害について」（https://www.jip.co.jp/news/20191205/）

2 5G時代に高まるサイバーセキュリティのリスク

総務省が2019年8月に公表した、「IoT・5Gセキュリティ総合対策」[*15]においては、5Gのサービス開始に伴う複数の新たなリスクが指摘されている。当該対策においては、ネットワーク機能の仮想化・ソフトウェアやモバイルエッジコンピューティングといった、5Gのネットワークの特徴を踏まえたセキュリティ確保の在り方について検討を行う必要があるとしているほか、従来に比べて産業用途でのIoT機器の設置・運用が増加していくことや、従来インターネットから隔離された形で運用されていた産業機器やインフラなどがインターネットに接続される可能性が高くなることを踏まえたセキュリティ対策が今後より一層重要になるといった指摘がなされている。

特に、5Gの普及に伴って予想されるIoTの普及は、今後、サイバー攻撃のリスクを一層高めることにつながるだろう。既に平成30年版情報通信白書で取り上げたとおり、IoTはその特長から、多くのセキュリティ上の課題が指摘されているところである（図表3-4-2-1）。

図表3-4-2-1　IoTの特徴とセキュリティ上の課題

性質	セキュリティ上の課題
脅威の影響範囲が大きい	HEMSやコネクテッドカー等のIoT機器はインターネット等のネットワークに接続していることから、ひとたび攻撃を受けると、ネットワークを介して関連する IoT システム・IoT サービス全体へその影響が波及する可能性が高く、IoT機器が急増していることによりその影響範囲はさらに拡大してきている。
脅威の影響度合いが大きい	自動車分野、医療分野等において、IoT機器の制御（アクチュエーション）にまで攻撃の影響が及んだ場合、生命が危険にさらされる場面さえも想定される。さらに、IoT機器やシステムには重要な情報（例えば個人の生活データ、工場のデバイスから得た生産情報等）が保存されている場合もあり、こうしたデータの漏えいも想定される。
IoT機器のライフサイクルが長い	自動車の平均使用年数は12～13年程度と言われていたり、工場の制御機器等の物理的安定使用期間は10年～20年程度のものが多く存在するなど、IoT機器として想定されるモノには10年以上の長期にわたって使用されるものも多く、構築・接続時に適用したセキュリティ対策が時間の経過とともに危殆化することによって、セキュリティ対策が不十分になった機器がネットワークに接続されつづけることが想定される。
IoT機器に対する監視が行き届きにくい	IoT機器の多くは、パソコンやスマートフォン等のような画面がないことなどから、人目による監視が行き届きにくいことが想定される。こうした場合、利用者にはIoT機器に問題が発生していることがわかりづらく、管理されていないモノが勝手にネットワークにつながり、マルウェアに感染することなども想定される。
IoT機器側とネットワーク側の環境や特性の相互理解が不十分	IoT機器側とネットワーク側それぞれが有する業態の環境や特性が、相互間で十分に理解されておらず、IoT 機器がネットワークに接続することによって、所要の安全や性能を満たすことができなくなる可能性がある。特に、接続するネットワーク環境は、IoT機器側のセキュリティ要件を変化させる可能性があることに注意をすべきである。
IoT機器の機能・性能が限られている	センサー等のリソースが限られたIoT機器では、暗号等のセキュリティ対策を適用できない場合がある。
開発者が想定していなかった接続が行われる可能性がある	IoTではあらゆるものが通信機能を持ち、これまで外部につながっていなかったモノがネットワークに接続され、IoT機器メーカやシステム、サービスの開発者が当初想定していなかった影響が発生する可能性がある。

（出典）総務省（2018）「平成30年版情報通信白書」

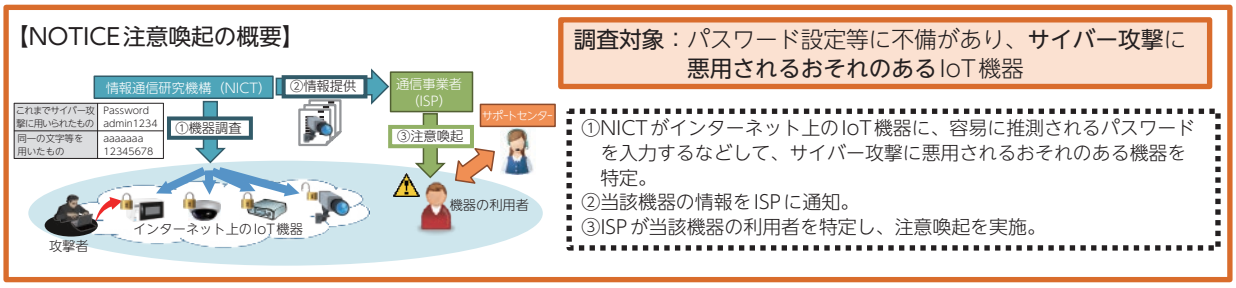
2020年1月に総務省が公表した「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]」[*16]においても、IoT機器のセキュリティ対策の拡充の必要性が説かれている。また、前述のIPAがとりまとめた「情報セキュリティ10大脅威　2020」においては組織に係る脅威の第9位として「IoT機器の不正利用」が挙げられている。当該項目においてIPAは、製造者がリスク検討を不十分なまま製品を開発してしまう可能性を指摘しており、その脆弱性が悪用されることにより、攻撃の踏み台とされたり、機能を不正利用されたりするなどして時に甚大な被害を発生させると述べている。また、利用者側におけるIoT機器を利用しているという意識の欠如やそれらの機器がインターネットにつながっていることについての意識の薄さも被害の拡大につながるとしている。

このようにIoT機器に係るリスクが高まる中、総務省及び情報通信研究機構（NICT）はIoT機器のセキュリティを確保するための取組である「NOTICE」を2019年2月から実施しており、インターネット・サービス・プロバイダと連携の上で、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行っている（図表3-4-2-2）。2020年5月に公表された本取組の2019年度の実施状況に係る報道発表[*17]によると、調査対象となった約1.1億のIPアドレスのうち、ID及びパスワードが入力可能であったものが約10万件、そのうちID及びパスワードによりログインできたものは延べ2,249件であったとしている。また、当該取組に加え、

＊15 https://www.soumu.go.jp/main_content/000641510.pdf
＊16 https://www.soumu.go.jp/main_content/000666176.pdf
＊17 総務省、国立研究開発法人情報通信研究機構、一般社団法人ICT－ISAC（2020）「脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況（2019年度）」（https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00067.html）

NICTはマルウェアに感染しているIoT機器を特定し、インターネットプロバイダから利用者へ注意喚起する取組についても2019年6月から実施しているところであり、マルウェアに感染しているとしてインターネットプロバイダに対する通知の対象となったものは1日当たり多い日では598件にのぼったとのことである。

図表3-4-2-2　NOTICEによる注意喚起の概要



（出典）総務省

先に述べたとおり、5Gの商用化開始に伴い、IoT機器の普及がこれまで以上に進むことが予想されるが、それらの機器のリスクは見落とされがちである。そのため、上記のような取組による注意喚起を通じて、IoT機器の利用に当たってのセキュリティリスクに関する利用者の意識を醸成していくことがこれまで以上に重要となってくるだろう。

3　サイバーセキュリティに係る国際連携

1　国際的なイベントの開催とサイバーセキュリティ

ア　オリンピック・パラリンピックの開催に伴い高まるリスク

さらに、2021年に開催が予定されている東京2020大会の開催もこのようなリスクを高める契機となりうる。

内閣サイバーセキュリティセンター（NISC）のとりまとめた「サイバーセキュリティ2019」[*18]によると、オリンピック・パラリンピックなどの国際的なイベントの開催時は、サイバー攻撃の脅威が広がると指摘している。同書では、過去のオリンピック・パラリンピックにおいて確認されたサイバー攻撃の例を紹介している（図表3-4-3-1）。これによると、2012年ロンドン大会、2016年リオ大会及び2018年平昌大会においてサイバー攻撃が確認されているとしており、2016年リオ大会においてはWebの改ざん、2018年平昌大会では開会式においてサービスが利用不可になるなどの被害が発生したとのことである。

図表3-4-3-1　過去の大会におけるサイバー攻撃

大会	確認された状況
2012年ロンドン大会	・大会公式サイトに対して約2億件の悪意ある接続要求 ・開会式直前にオリンピックスタジアムへの電源系への攻撃情報を入手し、必要な対処を実施 等
2016年リオ大会	・大会公式サイトに対する執ようなサイバー攻撃 ・大会関係組織の一部のWebの改ざん 等
2018年平昌大会	・大会準備期間に約6億件、大会期間中に約550万件のサイバー攻撃 ・開会式においてサイバー攻撃に起因して一部のサービスが利用不可等の報道あり

（出典）内閣サイバーセキュリティセンター（2019）「サイバーセキュリティ2019」を基に作成

また、2019年に開催されたラグビーワールドカップについてもサイバー攻撃の標的となったことが明らかになっている。報道[*19]によると、ラグビーワールドカップの開催期間中に、組織委員会に対し、大量のデータを送信してサービスの提供を不可にする、DDoS攻撃が行われたほか、職員らに対して、パスワードなどを詐取することを目的として、フィッシングメールが送りつけられたという。

先に述べたサイバーセキュリティ2019によると、このような国際的なイベントは、最高度の注目を集めること、

＊18　https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf
＊19　日本放送協会（2019.11.23）「ラグビーW杯組織委にサイバー攻撃」（https://www.nhk.or.jp/politics/articles/lastweek/26369.html）

また、国籍を超えた多数の利用者が関わることで、誤解や思い込みなど正常な判断ができなくなった状態による誤作動等を引き起こし得るような人間の脆弱性が高まることから、政治的及び精神的目的の攻撃のターゲットとなりやすいとのことであり、このことを踏まえれば、東京2020大会についてもサイバー攻撃の対象となることが想定されるだろう。

イ　開催に当たり必要となるサイバーセキュリティ対策

このような懸念も踏まえ、総務省は2020年1月に「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]」を公表した。

当該提言においては、先に述べたIoT機器のセキュリティ対策の必要性について述べられているほか、社会全体としてサイバーセキュリティ対応力を強化する必要性があることが挙げられている。その対応策として、現在、総務省が実施している、国の機関、独立行政法人、指定法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習（CYDER）に関して、地方公共団体の受講促進の取組を進めることが提言されている。

また、同提言においては、情報共有体制の強化についても触れられている。NISCは、サイバーセキュリティに係る脅威・インシデント情報を収集するとともに、これらの情報について大会組織委員会を始めとした関係機関等に提供し、事態に対処するための、「サイバーセキュリティ対処調整センター」を設置しているところであるが、さらに、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的とする、ISACを通じた事業者間連携が必要であるとしている。例えば、ICT分野全般については、2016年3月に「ICT-ISAC」として一般社団法人化されたが、他分野においても更なる情報共有機能の強化が期待されるところである。

さらに、大会期間中に訪日外国人の利用が見込まれる公衆無線LANの安全対策の必要性も述べられている。同提言では、提供サービスに係る公衆無線LANのセキュリティ対策の状況等についての提供者から利用者への適切な周知や、利用者の適切な判断を可能とするための、リテラシー強化のための取組が必要であるとされている。

そして、サイバーセキュリティ対策や事故報告の法令への位置づけや、分野ごとの所管省庁や業界団体によるガイドライン及び基準の策定といった取組についての周知等や、各地方公共団体における情報セキュリティ対策及び緊急時連絡体制の確保等の徹底といった、制度的な枠組みの改善が必要だとしている。

2　サイバーセキュリティの確保に向けた各国間での連携

さらに、国際的なデータ流通が活発となっている現代においては、海外からの脅威も深刻なものとなっている。例えば、2018年12月には、米国及び英国は、中国を拠点とするAPT10と呼ばれるサイバー攻撃グループに対する非難を表明し、日本の外務省及びNISCも同様の声明を発表している。また、2020年1月には三菱電機がサイバー攻撃を受け、個人情報や機密情報などが流出したことが公表されたが、報道によると、この攻撃も海外を拠点とするサイバー攻撃集団によるものとされている。さらに、同月にはNECが同社の防衛事業部門で使用している社内サーバの一部が第三者による不正アクセスを受けたことを公表したが、これについても海外の組織的な攻撃によるものであると報道されている。

このような海外からのサイバー攻撃の深刻化が懸念される状況においては、海外の関係機関との連携を通じた情報交換・共有等がサイバーセキュリティの確保において重要となってきている。そのため、政府を中心として海外の関連機関との協力の強化が図られている。

例えば、各国政府との協力関係の強化に関しては、首脳・閣僚のハイレベル協議や国際会議への参加、法執行機関間の連携強化により、サイバー空間における法の支配の推進、自由、公正かつ安全なサイバー空間の堅持に日本政府として積極的に寄与しているところである。また、二国間協議を通じた我が国のサイバーセキュリティ関係施策や考え方等の積極的な発信や連携の具体化等についても推進しているところであり、特に、ASEAN各国との間では、NISC及び関係省庁が連携して、人材育成への協力や、「日・ASEAN情報セキュリティ政策会議」等の定期的な開催を通じた情報交換等を実施するなどしている。

さらに、脅威情報を共有するための組織であるISACを核とした国際的な連携も進められている。例えば、前述のICT-ISACは、国際連携ワークショップの開催などを通じて、米国のICT分野のISACとの連携を進めるための取組に着手しているところであるが、今後、より効率的な情報共有が行われていくことが期待される。

4 新たなセキュリティリスク

1 サプライチェーンリスクへの懸念

これらに加えて、近年では、新たなセキュリティリスクとして、サプライチェーンリスクへの懸念も出てきている。

令和元年版情報通信白書でも述べたとおり、現在ではグローバルバリューチェーンと呼ばれる世界規模での分業体制が多くの分野で見られる。この分業体制により、様々な製品が安く生産できるというメリットがあるが、一方で、様々な地域の多くの企業が生産等に関与することから、新たなリスクの要因ともなり得る。先述したIPAの情報セキュリティ10大脅威でも、企業向けの脅威の第4位としてこうした「サプライチェーンの弱点を悪用した攻撃の高まり」が挙げられている。

2019年に策定された、「IoT・5Gセキュリティ総合対策」においても、このようなリスクの例として、ICTの製品やサービスを製造・流通する過程における不正なプログラムやファームウェアの組み込み、改ざんなどを挙げているほか、委託等の契約関係がある関係者のうち、サイバーセキュリティ対策が不十分な者が踏み台とされうることについても言及している。

2 海外における新たなリスクへの対応

こうした背景もあり、米国においては、安全保障上の懸念などから、政府機関や米国企業による中国企業からの調達の禁止等の取組がなされている（図表3-4-4-1）[*20]。例えば、2019年には、2019年度国防権限法に基づき、安全保障上の容認できないリスクの懸念から、米国政府機関による中国企業5社が製造する通信機器やビデオ監視装置の調達を禁止する措置が発効となった。また、米国の連邦政府通信委員会（FCC）は、安全保障上の懸念を理由として、連邦政府から補助金を受領する米国の通信会社に対し、中国企業2社からの製品の調達を禁止することを決定し、2020年に実施される見込みとなっている。

図表3-4-4-1　米国における中国企業規制の動き

年月日		出来事
2018年	8月13日	2019年度国防権限法（National Defense Authorization Act）が成立し、政府機関による、ファーウェイ、ZTE、ハイクビジョンなど5社からの製品調達を禁止する規定が追加（1年後に発効）。
2019年	5月15日	商務省が米国製品等のファーウェイ本社と関連企業68社への輸出規制を公表。 大統領が安全保障等に対するリスク等をもたらす取引を禁止する権限を商務長官に委任する大統領令に署名（商務長官は150日以内に詳細な規則を公表）。
	5月20日	米国製品等のファーウェイへの輸出規制のうち、一部取引を90日間猶予（8月19日まで）。
	5月23日	大統領が何らかの形でファーウェイを通商協議の取引材料に含む可能性があると発言。
	6月29日	米中首脳会談後、大統領が米国製品等のファーウェイへの輸出を認める方針を表明。
	8月13日	2019年度国防権限法に基づき、政府機関によるファーウェイ等からの製品調達禁止措置発効。
	8月19日	米国製品等の輸出規制について、ファーウェイの関連企業46社をエンティティー・リストに追加。一部取引の猶予期間を90日間延長（11月18日まで）。
	10月28日	連邦通信委員会が、補助金を受領する国内の通信会社に対しファーウェイとZTEの製品を使わないよう求める採決を、11月19日に実施する旨を公表。
	11月18日	米国製品等のファーウェイへの輸出規制について、一部取引の猶予期間をさらに90日間延長（20年2月16日まで）。
	11月20日	商務省が、ファーウェイへの輸出許可を申請した企業に対して審査結果の伝達を開始した旨を発表。
	11月22日	連邦通信委員会が、補助金を受領する国内の通信会社に対しファーウェイとZTEの製品を使わないよう求めることを正式決定。
	11月26日	商務省が、ファーウェイやZTE等を念頭に、「外国の敵対勢力」が手掛けた通信機器が米通信網や安全保障に危険を及ぼすと判断すれば、商務長官が取引をやめるよう米企業に求める規制案を公表（意見公募を踏まえて施行される見込み）。
2020年	2月13日	米国製品等のファーウェイへの輸出規制について、一部取引の猶予期間をさらに45日間延長（20年4月1日まで）。

（出典）内閣府（2020）「世界経済の潮流　2019年　II」を基に作成

＊20 内閣府（2020）「世界経済の潮流　2019年　II」https://www5.cao.go.jp/j-j/sekai_chouryuu/sa19-02/index-pdf.html

中国企業のネットワーク構築への参入を制限する対応はオーストラリアにおいてもとられている[*21]一方で、ドイツの通信事業者は中国企業を5G通信網構築の事業者として選定する[*22]など、各国によって対応が分かれている。

3 日本における対応

このサプライチェーンリスクについては、既に日本国内で顕在化しつつあるといえる。先に述べた三菱電機への攻撃は、報道によると、海外にある同社の関係会社から国内の拠点に広がったとのことであり、NECへの攻撃についても、地方の子会社のパソコンが狙われたとの報道がなされている。これらの攻撃は、社内でもサイバーセキュリティに関する対策が不十分な地方や海外の拠点を狙っており、サプライチェーンリスクを狙った攻撃の一種ととらえることができるだろう。

こうしたサプライチェーンリスクに対応するため、2018年に開催されたサイバーセキュリティ対策推進会議及び各府省情報化統括責任者連絡会議の合同会議において、情報システム・機器・役務等の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減するための新たな取組として、調達に係る審査の段階で必要な情報を入手し、評価することが申し合わされた[*23]。

また、第5世代移動通信システム（5G）の導入のための特定基地局の開設計画の認定の条件としてサプライチェーンリスクを含むサイバーセキュリティ対策を講じることを定めているほか、ローカル5Gにおいては免許時に同様の条件を付すこととしている。さらに、2020年5月には特定高度情報技術活用システムの開発供給及び導入の促進に関する法律が成立し、事業者が課税の特例の適用を受けるに当たって、サイバーセキュリティの確保等が求められることとなった。

今後、こうした取組に加え、IoT・5Gセキュリティ総合対策でも述べられているように、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程においてハードウェア脆弱性が存在する可能性を踏まえた対策が必要であると言える。例えば、同対策で挙げられているような、ビッグデータやAIを活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発やその活用が有用であると考えられる。

また、攻撃者がサプライチェーンの中の事業者のうち、サイバーセキュリティに関する対策が進んでいない者を狙って攻撃を行うということに鑑みれば、地方の情報通信サービス・ネットワークも含めたセキュリティ対策を一層向上していくことも求められるだろう。

5 企業による対策の現状

このようにセキュリティに係るリスクが増大する中、企業はどのように対応しているのだろうか。

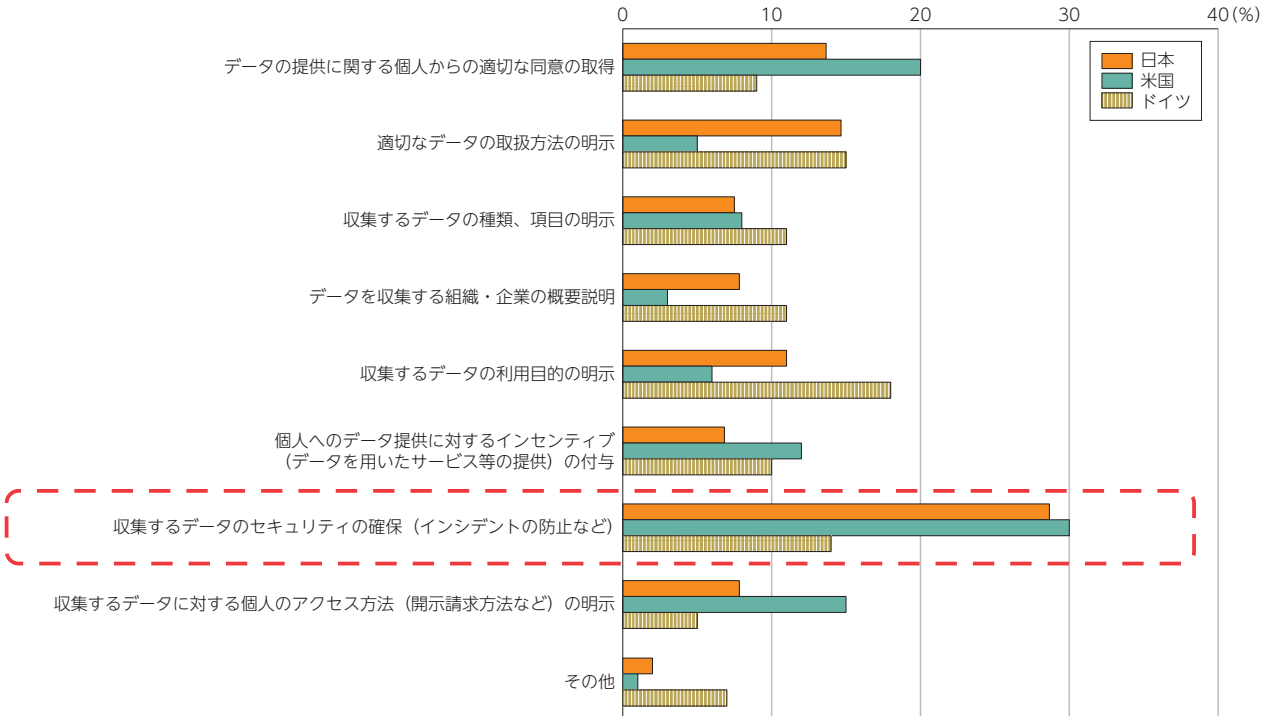
1 セキュリティ対策についての認識

我が国の企業はサイバーセキュリティに対する比較的高い危機意識を有している。FireEyeが2019年に実施した8か国（日本、米国、カナダ、フランス、ドイツ、英国、中国及び韓国）のサイバーセキュリティ担当の役員を対象にしたアンケート調査[*24]によると、2020年におけるサイバーセキュリティに関するリスクについて、日本では72%の回答者が悪くなると回答しており、これは全体の平均（56%）と比べると高く、米国（74%）に次ぐ割合となっている。

また、パーソナルデータに関するアンケートの結果からも、企業はセキュリティ対策を重要と認識していることがうかがえる。例えば、パーソナルデータの収集に当たって最も重視する点を尋ねた質問では、日本企業の3割近くが「収集するデータのセキュリティの確保」を最も重視する点として挙げており、選択肢の中で最も多くなっている（図表3-4-5-1）。

＊21 JETRO（2020）「中国企業による対内投資認可は減少、背景に両国政府の規制強化の動き」（https://www.jetro.go.jp/biz/areareports/2020/10344b67c618682d.html）
＊22 JETRO（2020）「スケジュール通りに進むかドイツ5G導入」（https://www.jetro.go.jp/biz/areareports/2020/e3161550d29d8d4e.html）
＊23 内閣サイバーセキュリティセンター（2018）「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（https://www.nisc.go.jp/active/general/pdf/chotatsu_moshiawase.pdf）
＊24 FireEye（2019）“FireEye Cyber Trendscape Report”（https://www.fireeye.com/offers/rpt-cyber-trendscape.html）

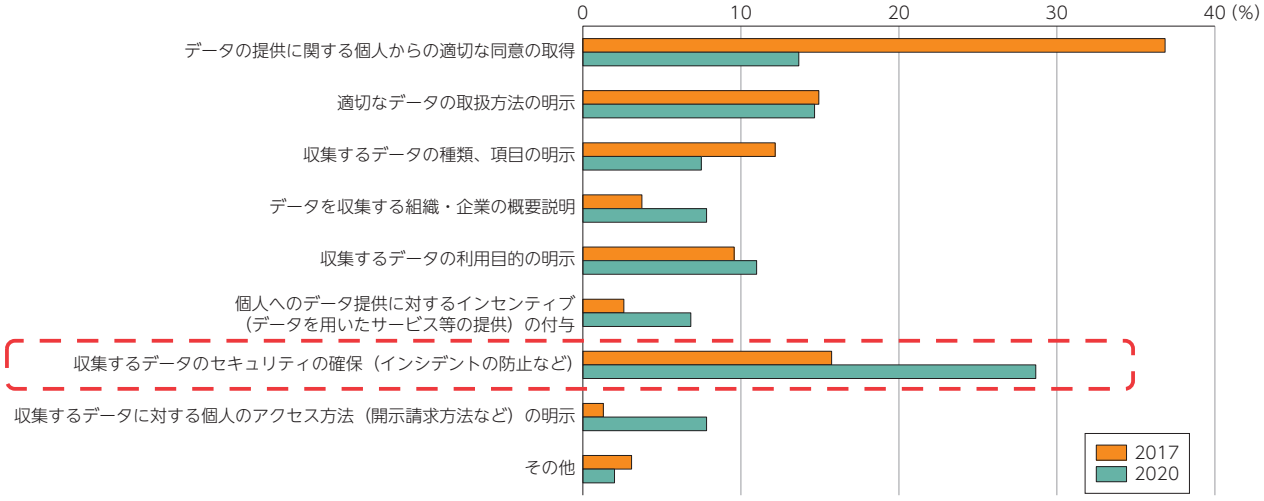
図表3-4-5-1　企業がパーソナルデータの収集に当たって最も重視する点



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

また、2017年の調査と比較すると、セキュリティの確保について最も重視すると回答する割合が大幅に増加している。これらの設問はパーソナルデータの収集に当たって留意している点であるものの、各企業におけるセキュリティに対する関心が高まっていると言えよう（図表3-4-5-2）。

図表3-4-5-2　日本企業がパーソナルデータの収集に当たって最も重視する点



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

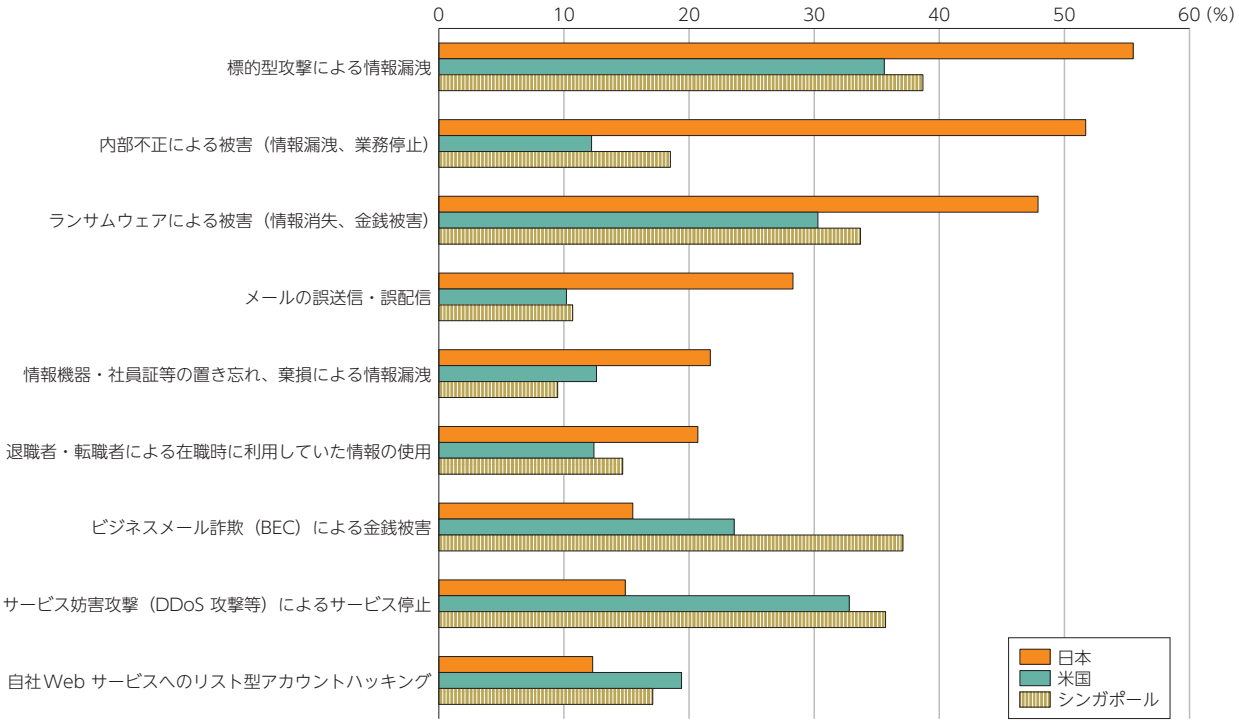
一方で、各企業はどのような脅威を想定しているのだろうか。

NRIセキュアテクノロジーズが2018年から2019年までにかけて日本、米国、シンガポールの企業を対象に実施したアンケート*25において、自社で最も脅威となる事象についての質問を行っている。各国とも「標的型攻撃による情報漏洩」や「ランサムウェアによる被害」を挙げている企業が多くなっている（図表3-4-5-3）。しかし、米国及びシンガポールの回答者が「サービス妨害攻撃（DDoS攻撃等）によるサービス停止」や「ビジネスメール詐欺（BEC）による金銭被害」を懸念しているのに対し、日本企業は「内部不正による被害」や「メールの誤送信・誤配信」等の社内からの脅威を上位に挙げるなど、社外からの攻撃に対する懸念が海外に比べるとやや弱く

＊25 NRI セキュアテクノロジーズ（2019）「NRI Secure Insight 2019」（https://www.nri-secure.co.jp/report/2019/insight2019）

なっていることがうかがえる。

図表 3-4-5-3　自社で最も脅威となる事象（最大３つ選択）



（出典）NRI セキュアテクノロジーズ（2019）「NRI Secure Insight 2019」を基に作成

2　セキュリティ対策の現状

それではこのような意識のもと、我が国の企業はどのような取組を進めているのだろうか。

トレンドマイクロは、セキュリティ対策の各項目の実施状況について、各項目の満点を100%とした場合の達成度を「セキュリティ対策包括度」として評価している（図表3-4-5-4）。この評価によると、各企業においては、「クライアント端末上で行っているOSの脆弱性対策」や「クライアント用アプリケーションの脆弱性対策」、「メールのセキュリティ対策」、「ネットワークを守るためのセキュリティ対策」、「社内ネットワークにおける不審な通信や挙動の監視」、そして「サイバー攻撃や情報漏えいに関する注意喚起」といった対策が進んでいることが分かる。また、同社は、分析において、このスコアが高い法人の特徴として、技術的対策では「ネットワークを守るためのセキュリティ対策」、「社内ネットワークにおける不審な通信や挙動の監視」といったネットワークセキュリティで点数が高く出ており、組織的対策では「サイバー攻撃や情報漏えいに関する従業員教育」、「サイバー攻撃や情報漏えいに関する注意喚起」といったサイバー攻撃や情報漏えいに対するセキュリティ意識に関して点数が高く出ている傾向が見られるとしている。

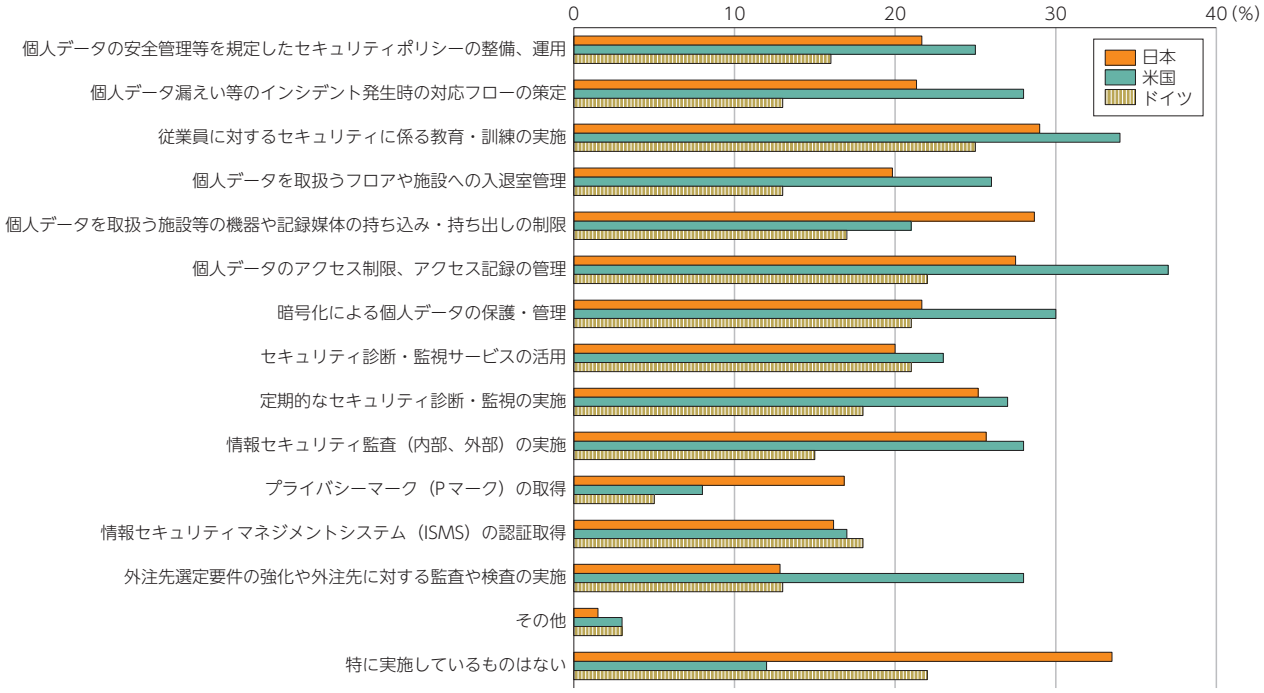
図表 3-4-5-4　セキュリティ対策の実施状況

セキュリティ対策		セキュリティ対策包括度
技術的対策	クライアント端末に対して行っているセキュリティ対策	53.7
	クライアント端末上で行っているOS の脆弱性対策	73.0
	クライアント端末上で行っているクライアント用アプリケーションの脆弱性対策	70.3
	組織内サーバに対して行っているセキュリティ対策	40.8
	組織内サーバで行っているOSの脆弱性対策	68.4
	組織内向け業務アプリケーション、システムの脆弱性対策	66.7
	公開サーバに対して行っているセキュリティ対策	40.2
	公開サーバで行っているOSの脆弱性対策	68.8
	公開サーバ上で行っているWebアプリケーションの脆弱性対策	68.2
	公開サーバ上で行っているサーバ用ソフトウェアの脆弱性対策	66.5
	サーバに対する不正な改変への対策	68.5
	メールのセキュリティ対策	71.1
	社内での実行ファイル（プログラムファイル）の取り扱い	58.0
	ネットワークを守るためのセキュリティ対策	71.8
	社内ネットワークにおける不審な通信や挙動の監視	70.3
	社内にある重要な情報の保護	63.4
組織的対策	重要なITシステム、ネットワーク、サービス構成の文書化	47.8
	個人情報や機密情報などの情報資産の重要度の分類、棚卸	52.0
	セキュリティポリシーの整備	50.6
	セキュリティ・情報管理の監査	60.8
	セキュリティインシデント発生時の対応プロセス	65.4
	セキュリティインシデント発生時の対応人員、組織	59.2
	セキュリティ関連情報の収集	64.9
	従業員によるインターネットやサービスの利用に関するガイドライン	61.2
	サイバー攻撃や情報漏えいに関する従業員教育	68.5
	サイバー攻撃や情報漏えいに関する注意喚起	72.4

（出典）トレンドマイクロ（2019）「法人組織におけるセキュリティ実態調査2019年版」を基に作成

また、本章で紹介してきた日本、米国及びドイツの３か国の企業の従業員向けのアンケートにおいても、パーソナルデータを安全に管理・保護するためのセキュリティの取組として重要と考えているものを尋ねたところ、どの国においても、「従業員に対するセキュリティに係る教育・訓練の実施」、「個人データのアクセス制限、アクセス記録の管理」が上位３位に入る結果となった（図表 3-4-5-5）。そのほか、日本では「個人データを取扱う施設等の機器や記録媒体の持ち込み・持ち出しの制限」が上位に入っている。一方で、米国では、「暗号化による個人データの保護・管理」といった、データが流出した時に備えた対策も３割の企業によって導入されているほか、「外注先選定要件の強化や外注先に対する監査や検査の実施」といった、サプライチェーンリスク対策にもつながるものを重視している。

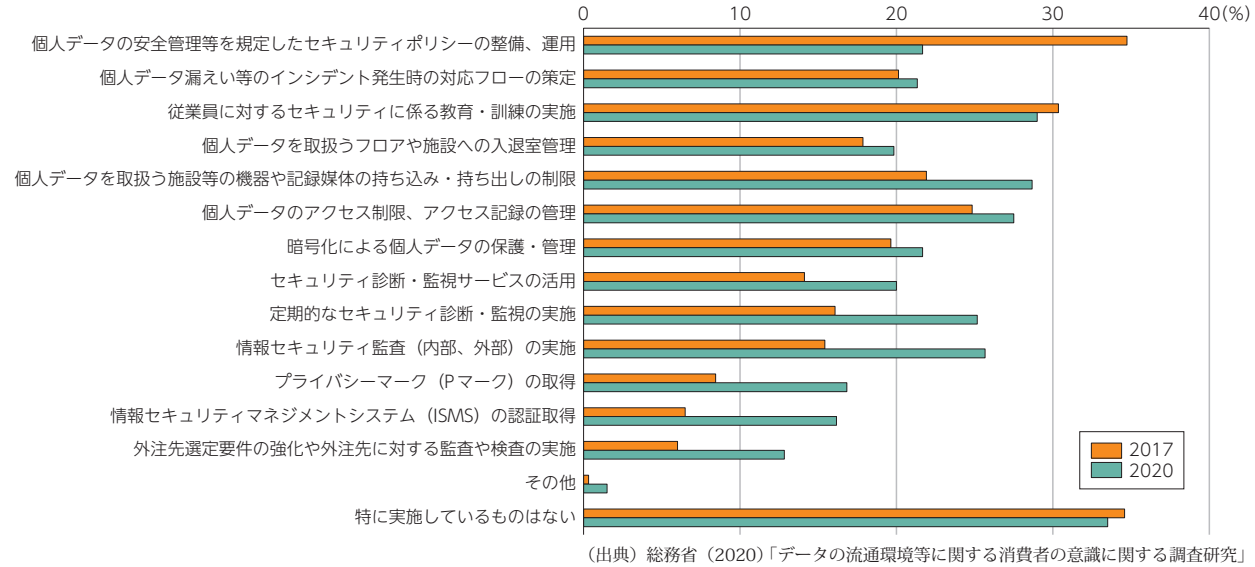
図表 3-4-5-5　企業がパーソナルデータを安全に管理・保護するセキュリティの取組として重要と考えるもの（複数選択）



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

また、日本企業の回答に焦点を当てて３年前の調査との比較を行うと、近年では、セキュリティポリシーの整備、運用などを以前ほど重視しない傾向にある一方で、セキュリティ診断・監視や、情報セキュリティ監査、PマークやISMSといった認証の取得などがパーソナルデータを安全に管理・保護するセキュリティの取組として近年重視されているといえる（図表3-4-5-6）。

図表 3-4-5-6　日本企業がパーソナルデータを安全に管理・保護するセキュリティの取組として重要と考えるもの（複数選択）



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

3　セキュリティ対策の課題

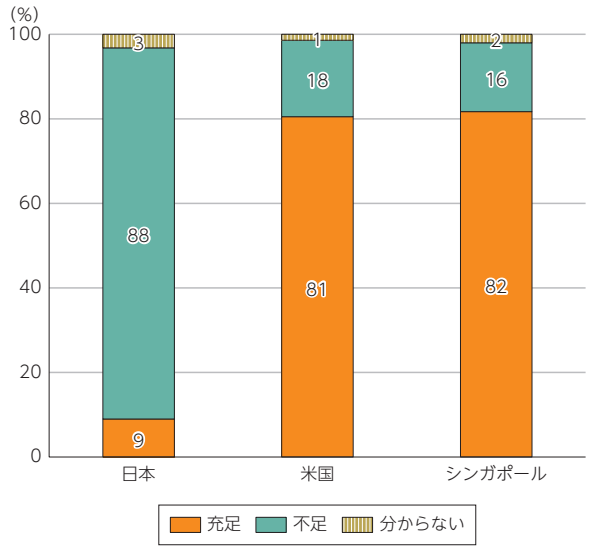
このように各企業において対策が実施されているところであるが、一方で対策に当たっての課題も表出している。

前述したFireEyeの調査によるとサイバーセキュリティと業務運営のバランスについて、対象８か国全体では約６割の回答者が難しい又はとても難しいと回答しているのに対し、我が国では７割以上の回答者が難しい又はとて

も難しいと回答しており、我が国のサイバーセキュリティ担当役員が他国に比べてサイバーセキュリティの対応に苦慮していることがうかがえる。

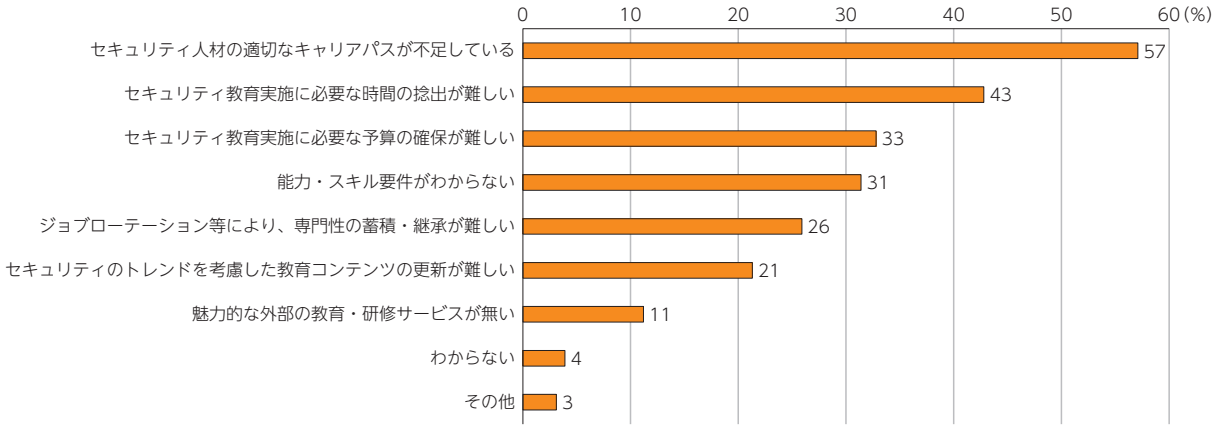
また、NRIセキュアテクノロジーズのアンケートでのセキュリティ対策に従事する人材の充足状況に関する質問においては、米国及びシンガポールの８割以上の企業が充足していると回答したのに対し、約９割の日本企業はこれらの人材が不足していると回答している（図表3-4-5-7）。この人材不足の理由を日本企業に尋ねると、大半の企業がセキュリティ人材の適切なキャリアパスの不足や、セキュリティ教育実施に必要な時間の捻出の困難さを挙げている（図表3-4-5-8）。

図表3-4-5-7　セキュリティ対策に従事する人材の充足状況



（出典）NRIセキュアテクノロジーズ（2019）「NRI Secure Insight 2019」を基に作成

図表3-4-5-8　日本企業におけるセキュリティ人材の育成・教育における課題



（出典）NRIセキュアテクノロジーズ（2019）「NRI Secure Insight 2019」を基に作成

6　さらなるセキュリティ対策の必要性

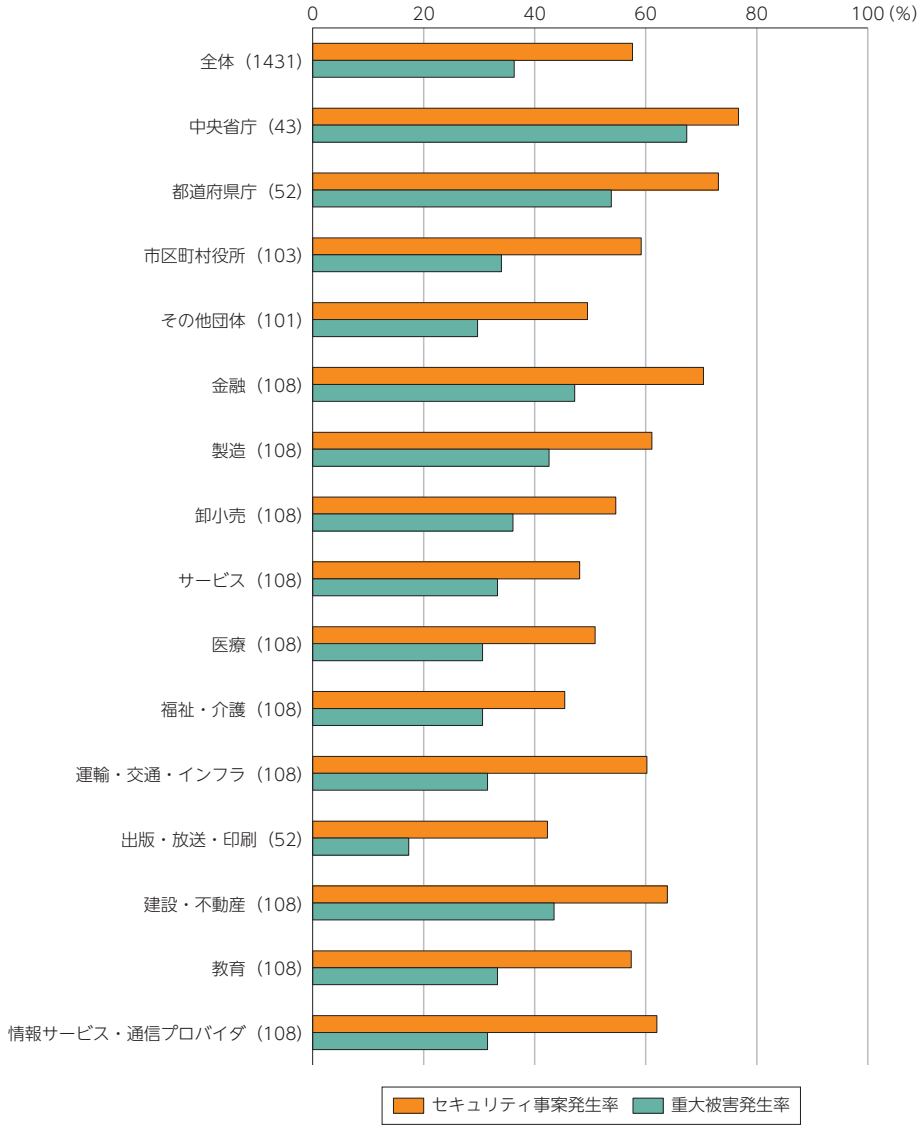
1　サイバーセキュリティに係るリスクの高まり

これらの結果からは、我が国の企業はセキュリティ対策の必要性を認識して対策を進めていることが分かるが、人材不足など、対応に苦慮しているようである。特に、この人材不足については、令和元年版情報通信白書を始め、これまでの白書でも取り上げているところであり、サイバーセキュリティ対策における日本企業の長期的な課題となっているが、その充足に当たっての課題に着目すると、キャリアパスの不足やセキュリティ教育の実施に必要な時間や費用の問題など、企業内におけるセキュリティ対策の優先度に起因するものと思われるものが散見される。

しかしながら、日本企業も海外の企業と同様、サイバーセキュリティのリスクにさらされていることに留意すべきである。トレンドマイクロの調査によると、調査対象となった組織の57.6%が2018年4月から2019年3月までの間に何らかのセキュリティ事案を経験し、36.3%が個人情報の漏えいをはじめとする重大な被害を受けていることが明らかになっている（図表3-4-6-1）。幅広い業種の法人や組織においてセキュリティ事案やそれによる重大被害が発生していることが見て取れるが、同社は、セキュリティ事案の発生率が全体平均を下回る業種におい

ても、可能性としてセキュリティインシデントに気づける十分な体制が整備されておらず、すでに侵害されているリスクもあるのではないかと推察しており、実際はこれ以上のセキュリティ事案が発生していることを示唆している。

図表 3-4-6-1　セキュリティ事案及び重大被害の発生率



※（）内の数字はサンプルサイズ

（出典）トレンドマイクロ（2019）「法人組織におけるセキュリティ実態調査2019年版」を基に作成

このように現在既に多くの企業等がサイバーセキュリティ上のリスクにさらされているが、前述したようにデータの活用の拡大や5Gの利用拡大に伴うIoTの普及、そしてオリンピック・パラリンピックの開催などにより、サイバーセキュリティのリスクは高まりつつあり、企業がサイバー攻撃の標的となる事案もこれまでよりも一層増加すると考えられる。このような攻撃から組織を守るためにも、これまでよりも一層の対策を進めていくことが必要だろう。

2　消費者の安心感の醸成

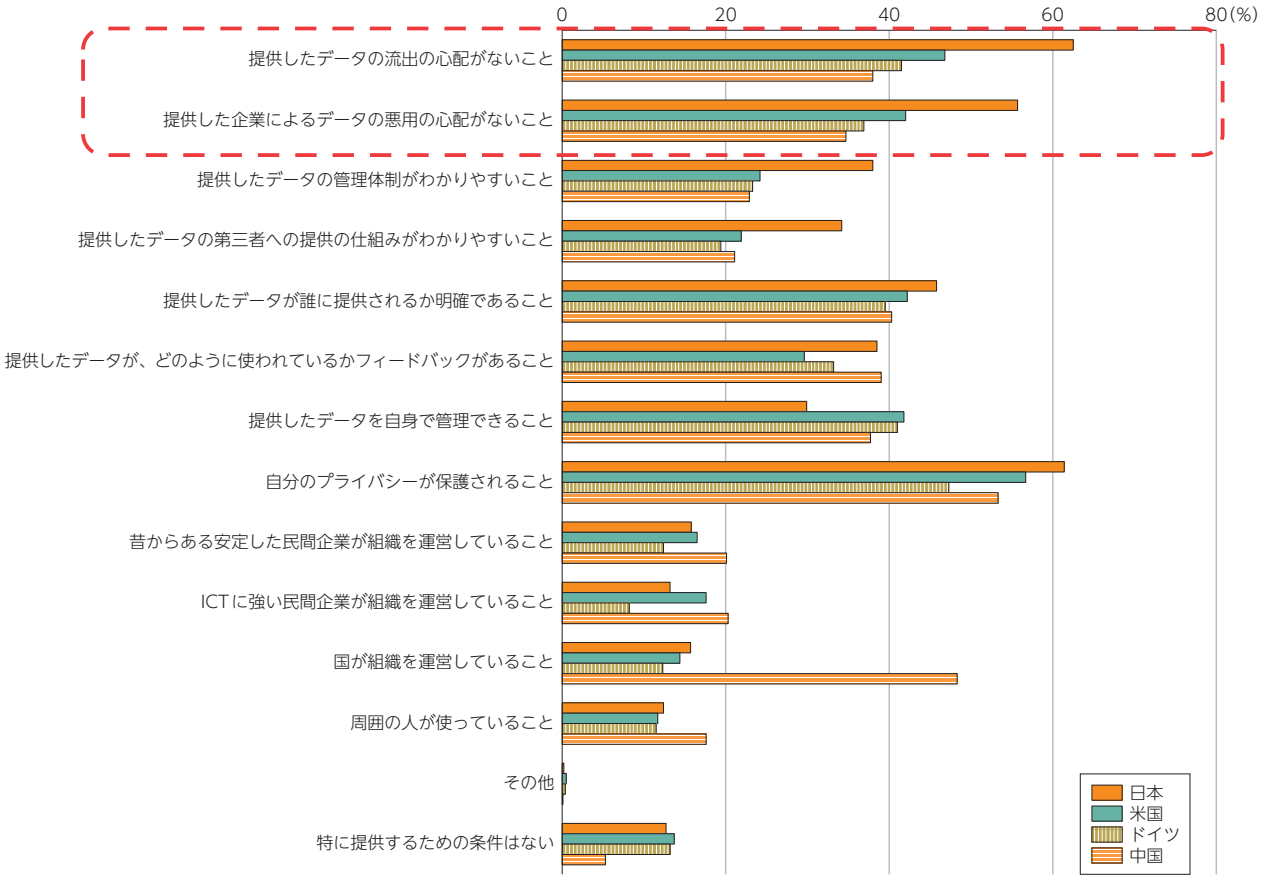
さらに、このリスクの高まりに加えて、消費者がセキュリティの確保に対して高い関心を有していることにも留意する必要がある。

これまで本章で言及してきたとおり、我が国の消費者は米国、ドイツ及び中国の消費者に比べて、パーソナル

データの提供に当たり安心や安全性を重視する傾向にある。

例えば、パーソナルデータの提供を求められた場合に提供してもよいと思う条件を聞いた設問に対しては、日本の回答者のうち６割を超える者が「提供したデータの流出の心配がないこと」を挙げており、他国と比較して15ポイント以上大きくなっている（図表3-4-6-2）。また、「提供した企業によるデータの悪用の心配がないこと」についても６割弱と、我が国の消費者が他国の消費者よりもデータの悪用についても心配していることが分かる。

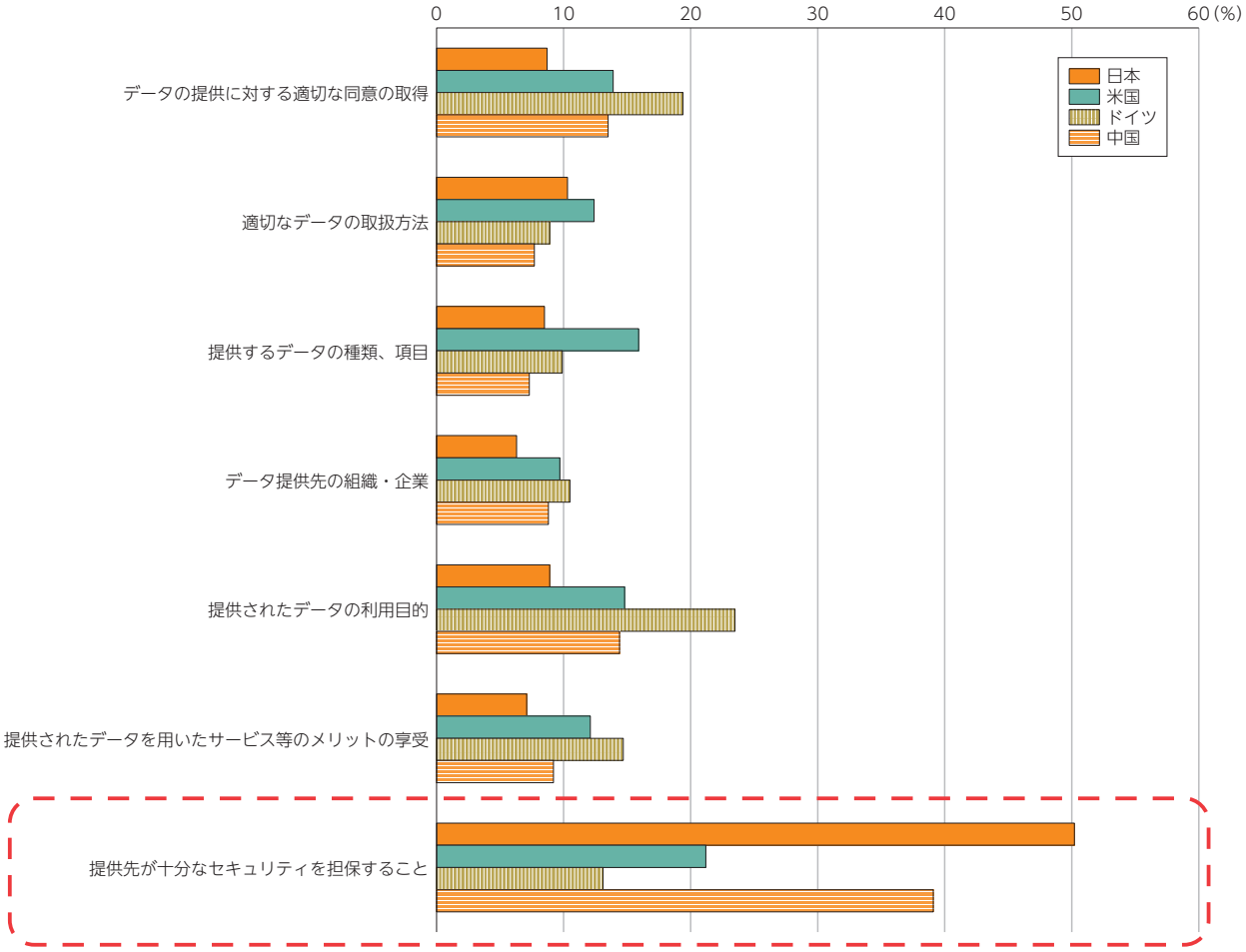
図表3-4-6-2　消費者がパーソナルデータの提供を求められた場合に提供してもよいと思う条件（複数選択）



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

また、自身のパーソナルデータを提供する際に最も重視する事項について尋ねた設問においても、「提供先が十分なセキュリティを担保すること」を選択した消費者は半数にものぼり、他国の消費者に比べた、我が国の消費者のセキュリティへの関心がうかがえる結果となっている（図表3-4-6-3）。

図表 3-4-6-3　消費者がパーソナルデータを提供する際に最も重視する事項



（出典）総務省（2020）「データの流通環境等に関する消費者の意識に関する調査研究」

本章での分析により、データの活用が企業経営に様々なプラスの効果をもたらすことが明らかになったが、セキュリティ対策の不備は、これからの企業経営に必要となるパーソナルデータの円滑な取得を難しくしかねない。消費者が安心してデータを企業に預けられるためのセキュリティ対策は必須であり、ひとたびセキュリティ事故が発生した際の損失は財政的影響のみならず、企業の信用失墜にもつながる。5G時代のデータ活用を進めるためには、これまでにも増したセキュリティ対策が不可欠であると言えるだろう。

コラム COLUMN 4 活用が進むブロックチェーン技術*1

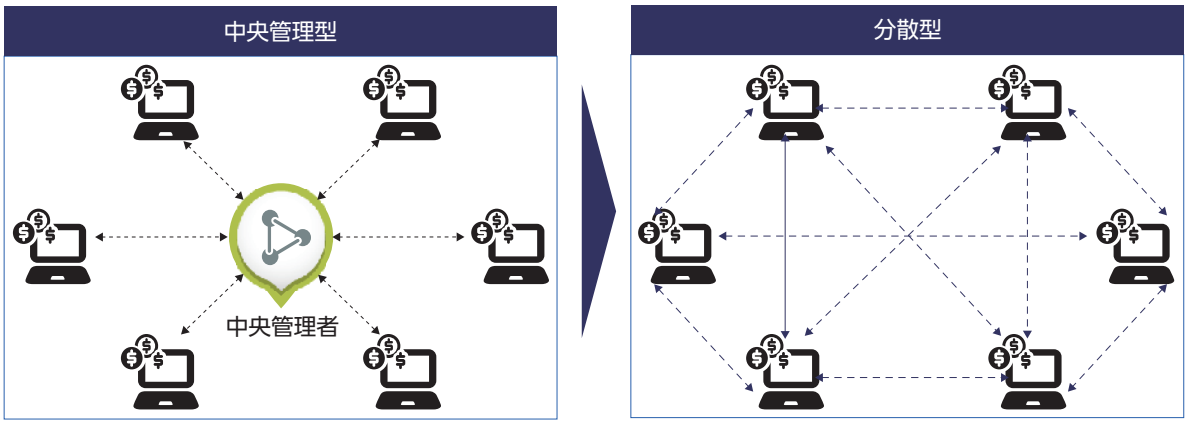
1 ブロックチェーン技術の概要

(1) ブロックチェーン技術の特徴

近年、従来型の中央管理型のデータベースに変わる技術として、ブロックチェーン技術に注目が集まっており、様々な分野での活用が期待されている。

平成30年版情報通信白書でも述べたとおり、ブロックチェーン技術とは、情報通信ネットワーク上にある端末同士を直接接続して、暗号技術を用いて取引記録を分散的に処理・記録するデータベースの一種であり、「ビットコイン」等の暗号資産に用いられている基盤技術である。(図表 1)

図表1　管理手法のイメージ



(出典) 総務省 (2020)「ブロックチェーン技術の活用状況の現状に関する調査研究」

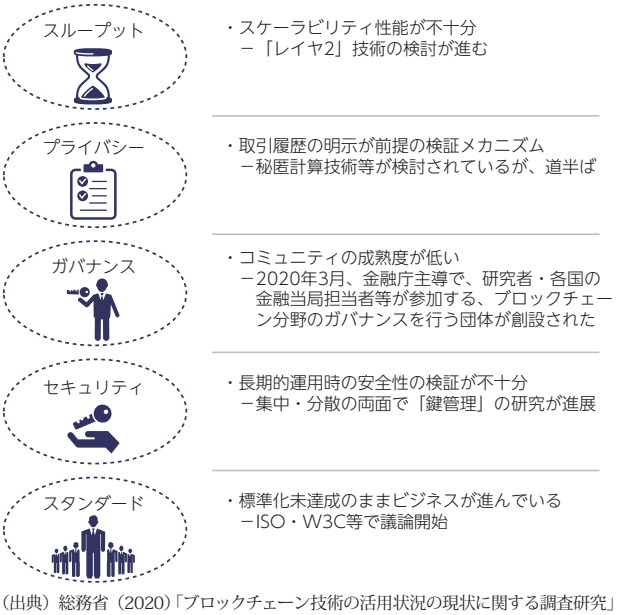
このブロックチェーンを活用したデータベースは、従来型のデータベースに比べ、三つの点で優れていると言われている。①分散管理・処理を行うことでネットワークの一部に不具合が生じてもシステムを維持することができる可用性、②取引データが連鎖して保存されているため過去の記録と整合的な改ざんはほぼ不可能であり、また、データの改ざんをリアルタイムで監視可能である完全性、③従来のデータベースでは取引において必要であった仲介役が不要になることによる取引の低コスト化である。

(2) 現状における技術的な課題と利用領域の拡大

このような特長を持つブロックチェーンであるが、一方で、いくつかの課題も指摘されている (図表2)。これらの課題に対しては対応が進められているところであり、例えばスケーラビリティ性能については、ブロックチェーン自体の処理性能の向上や、ブロックチェーン外部のシステムとの連携により解決するといった方策が検討されているところである。

このような課題がある一方で、様々な事業者によりブロックチェーン技術を利用するためのサービスがBlockchain as a service (BaaS) として提供されるなど、ブロックチェーン技術が幅広い領域で利用されるようになった。これらのサービスを利用することで、比較的簡易にブロックチェーン技術を活用したアプリを構築することが可能となり、ブロックチェーンの活用領域の拡大に寄与している。

図表2　現状の課題



(出典) 総務省 (2020)「ブロックチェーン技術の活用状況の現状に関する調査研究」

*1　本コラムは、総務省 (2020)「ブロックチェーン技術の活用状況の現状に関する調査研究」を基に執筆した。

2　各分野における活用状況

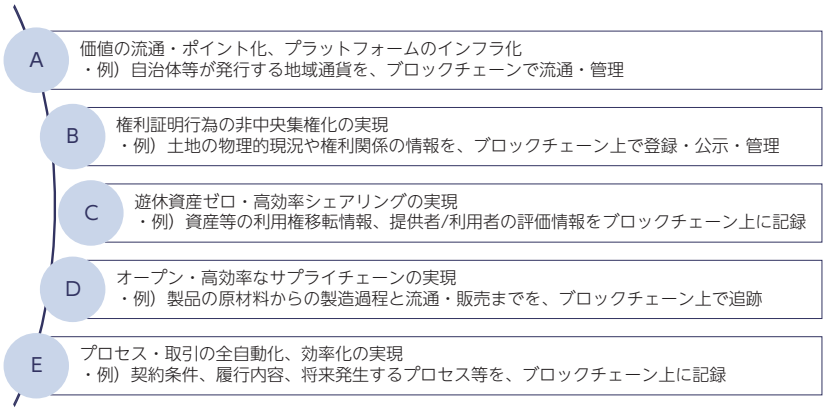
(1) 金融分野以外における活用事例

ア　活用が期待される事例の類型

当初は暗号資産に代表されるように、金融分野での活用が先行していたブロックチェーン技術であるが、近年ではその他の分野においても活用に向けた検討が進められている。

それらの分野におけるブロックチェーン技術の活用場面として５つが主に考えられる*2（図表３）が、本稿においてはそれらの主なユースケースについて紹介を行う。

図表３　ブロックチェーン技術による社会変革の可能性



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

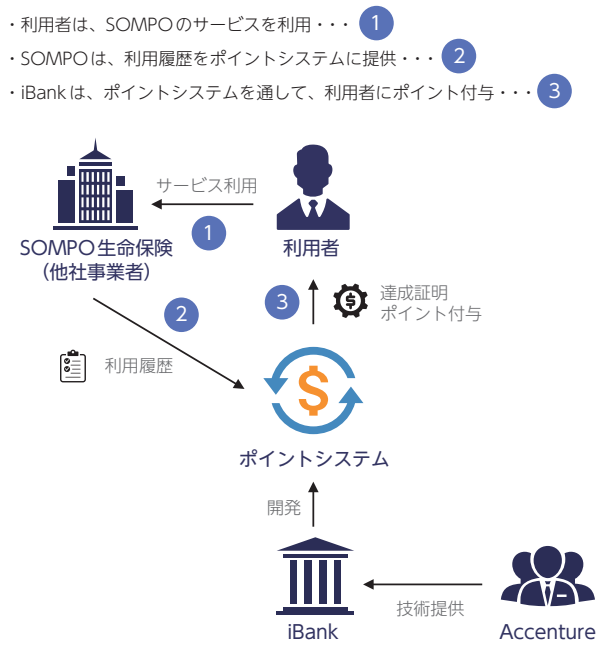
（ア）価値の流通・ポイント化、プラットフォームのインフラ化（iBank）

銀行代理業等を営むiBankは、2020年３月に、SOMPOひまわり生命保険と共同で、先着3,000ユーザに対しブロックチェーンを活用したポイントサービスの企画を実施することを表明した。

このサービスにおいては、キャンペーン達成の判定からポイント付与まで、スマートコントラクトで自動化するとしている。

ブロックチェーン技術を活用することにより、例えば、子どもがお年玉として獲得したポイントでの用途を限定するなど、ポイントの取得形態等に応じた、個別の情報を付与することができる。また、ポイント管理システムをオープン化することにより、様々なポイントサービス、利用メニューを簡易に拡充することが可能になっている。

図表４　iBankによるサービスのイメージ



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

（イ）権利証明行為の非中央集権化の実現（ソニー・ミュージックエンタテインメント）

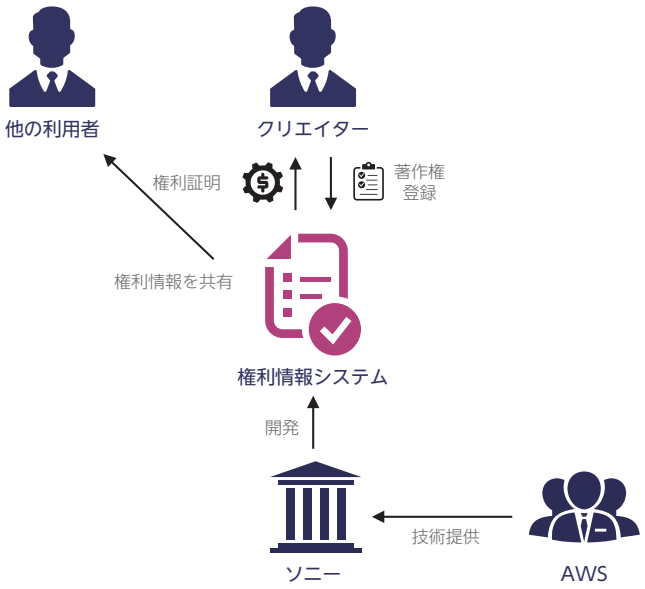
ソニー・ミュージックエンタテインメントは、ブロックチェーンを用いて、音楽著作権の登録管理を簡易化し、クリエイターが権利情報処理に係る作業の効率を高めることを目的として、2019年に本取組の構想を発表し、Amazonやレコード会社等とも連携して運用に向けた実証実験に取り組んでいる。

＊2　経済産業省（2016）「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書概要資料」（https://www.meti.go.jp/main/infographic/pdf/block_c.pdf）

ブロックチェーン技術の活用により、従来、書面でのやり取り等も多く、創作活動を行うクリエイターが権利処理を行う負担が大きかったものが、著作権情報処理システムを介した簡易な情報の管理が可能になるとしている。

さらに、権利処理の体制を、ブロックチェーンを用いてステークホルダー全体で共有することで、中央主権的な仕組を防ぐことが可能となり、音楽業界に存在していたステークホルダー間での複雑な権利関係から解放された、関係各所に配慮した取引が可能となる。

図表5　ソニー・ミュージックエンタテインメントによるサービスのイメージ



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

（ウ）遊休資産ゼロ・高効率シェアリングの実現（LIFULL）

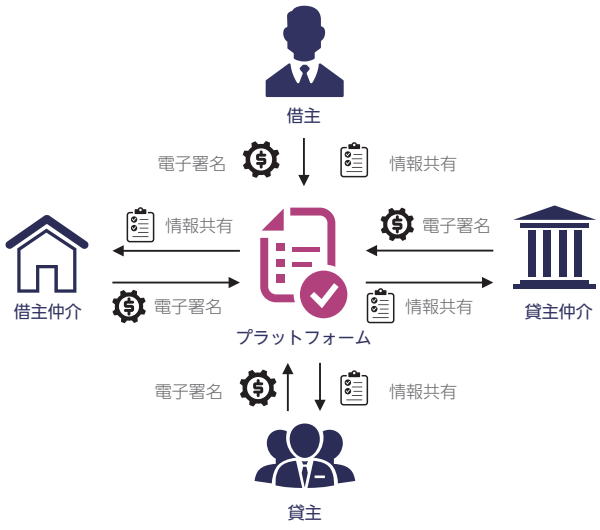
不動産サービス事業を運営するLIFULLは2019年11月から、ブロックチェーンを用いた不動産情報の安全・効率的な管理、そして不動産賃貸契約を簡易に完結可能な仕組みの構築を目指し、実証実験を開始している。

従来、データベース内の契約情報は意図的にねつ造が可能であり、電子署名による本人認証も、コストや認証機関の不正についての懸念があったが、ブロックチェーン技術の活用により、安全な契約情報の管理が可能となった。

また、不動産賃貸契約についても、従来借主の審査・契約手続・引渡しに時間を要していたものが、スマートコントラクトにより、安全・効率的に契約を締結することが可能になったという。

図表6　LIFULLによるサービスのイメージ

・借主・貸主はプラットフォームを通して、安全・効率的に情報を共有する
・賃貸借契約書を電子化することで、従来の事務手続等が不要になる
・プロセスの処理状況を可視化し、事務コスト・処理時間を短縮出来る



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

（エ）オープン・高効率なサプライチェーンの実現（カレンシーポート）

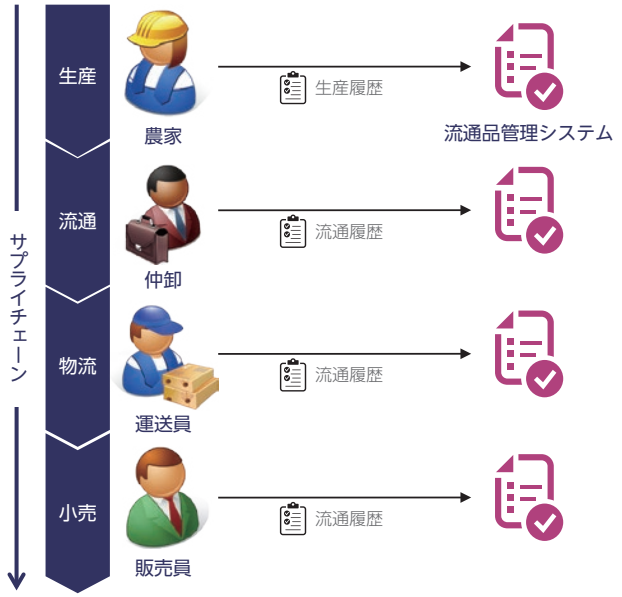
ブロックチェーン技術を活用したサービスを提供するカレンシーポートは、ベジテック、三菱総合研究所と共同して、事業者が生産・流通履歴等の情報を入力・管理する、食品トレーサビリティプラットフォームを開発し、2019年1月から2月にかけて実証実験を実施した。

このプラットフォームの活用により、ブロックチェーンを介して流通品の生産履歴等を管理することが可能となり、従来よりも事故品の特定や回収、そして流通品の情報管理が容易になるとしている。

また、本サービスによって、ブロックチェーンを介して、サプライチェーンに関わる事業者毎にシステム構築を行うことなく、情報を共有可能となることから、複数のサプライチェーンを従来よりも簡易に管理することが可能である。

図表7　カレンシーポートによるサービスのイメージ

・ブロックチェーンにより、安全・効率的に流通品の情報を管理出来る
・事故品が発生した場合、特定・回収することが容易



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

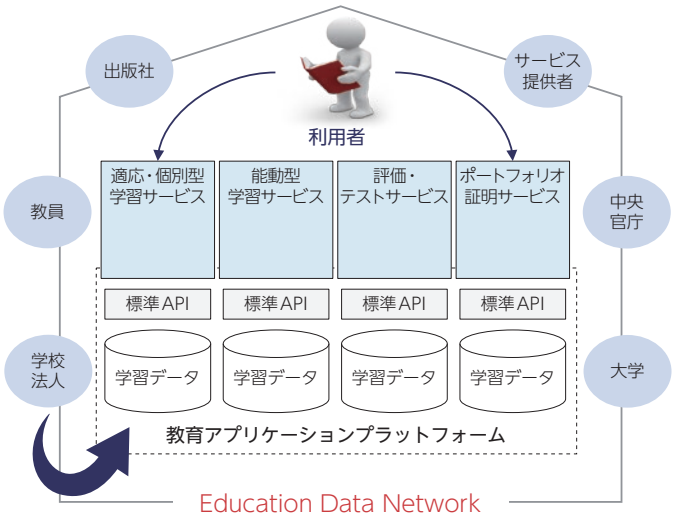
（オ）プロセス・取引の全自動化、効率化の実現（ソニー・グローバル・エデュケーション）

ソニー・グローバル・エデュケーションは、2016年、ブロックチェーンによる学習到達・活動記録のオープン化技術を開発し、ブロックチェーンを用いて、生徒の学習履歴の管理を効率化し、生徒の学習の効率化、正確な学習履歴の評価を可能とするサービスを富士通等に提供している。

このサービスを活用することで、初等教育のみならず、リカレント教育等、個人が学んだ学習データを蓄積・活用することが可能となるほか、学習データを基に、学習者向けに教育コンテンツのリコメンドや、転職マッチングサービス等を提供が可能となる。また、学習データのポータビリティが確保され、ブロックチェーンを通して、個人の学習データを、事業者やサービスを問わずに利用出来る環境の構築ができる。

図表8　ソニー・グローバル・エデュケーションによるサービスのイメージ

・ソニーグローバルエデュケーションは、ブロックチェーン技術を基に、学習者のデータ管理を行うネットワーク「Education Data Network」を提供
－学習者がプラットフォーム上のサービスを利用することで、データが蓄積する
－外部事業者は、それらのデータを活用し、自社のサービスを高度化可能



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

イ　日本通運における活用事例

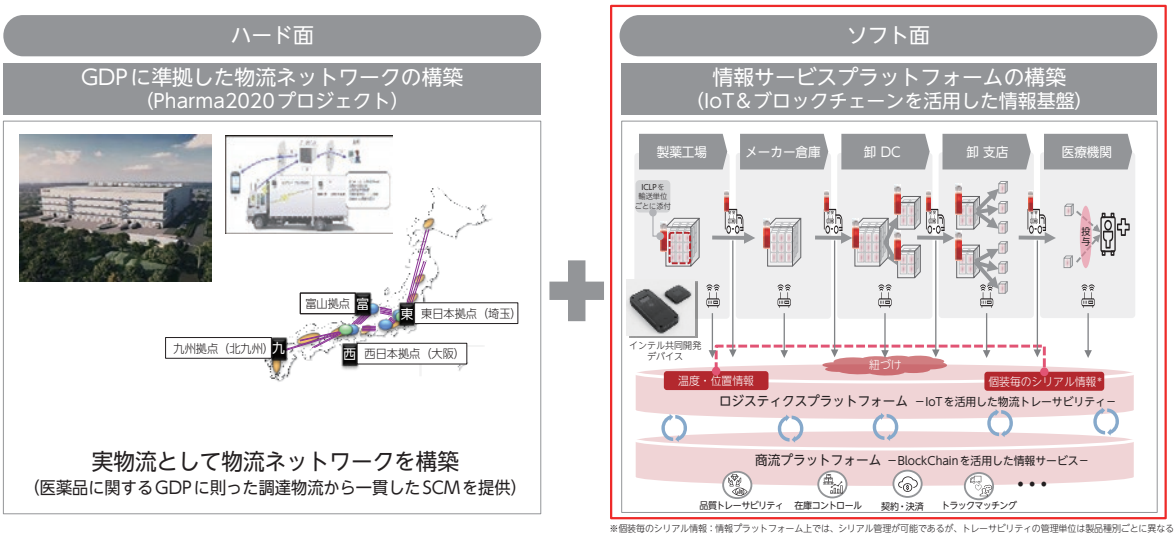
様々な分野において活用が進むブロックチェーン技術であるが、日本通運においては医薬品の物流に生かす取組が進められている。

医薬品の流通においては、流通過程における医薬品の品質保証の基準であるGDP（Good Distribution

Practice）が定められており、温度管理をはじめとする完全性*3の保持や偽造薬の流通の防止が求められている。この基準への準拠のためには、ハード面のほか、運用手順やトレーサビリティといったソフト面も求められるが、同社ではこれを実現するためのソフト面の取組の一環として、ブロックチェーン技術を活用している。本取組を通じて様々な業界の関係者を巻き込んだ商流サービスプラットフォーム構築することにより、同社は流通上のコスト負担の肥大化という業界の課題を解決し、産業基盤の強化に貢献することを目指している。

図表9　日本通運の取組の概要

ハード面として倉庫、車両を中心とした物流ネットワークの構築を確実に進めつつ、GDPの実現に向けオープンに活用できるIoTプラットフォームとBlockchainを活用した商流サービスプラットフォーム構築を目指す。



（出典）日本通運

同社によれば、ブロックチェーン技術の採用を決めた背景として、情報の公開性を保ちつつ、多くのステークホルダーにリアルタイムで情報共有を行うことができることがあるとのことである。同社はこの技術の活用により、品質トレーサビリティや、在庫のコントロール、契約・決済の簡素化やトラック業者・物流拠点の稼働の最適化を実現することを期待している。現在、温度情報や位置情報の継続的な記録等を検証する技術検証を終え、医薬品業界の物流構造を模した条件下での業務検証を実施しているとのことである。

（2）金融分野における活用状況

ア　Libraの発行を巡る動き

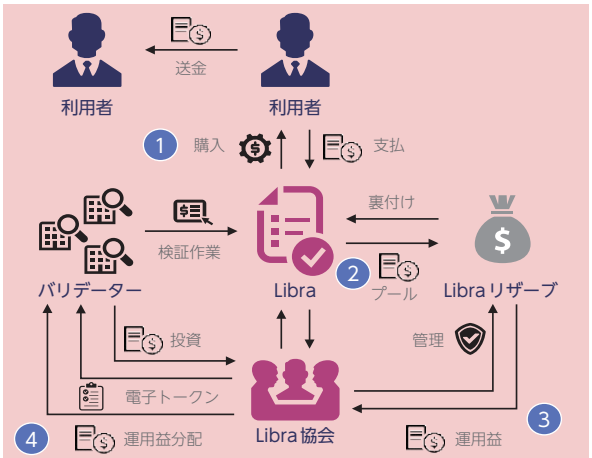
かつては暗号資産の中核技術として金融分野で用いられていたブロックチェーン技術であるが、それ以外の場面における活用も模索されだしている。その中の動きとして注目すべきものはFacebookが開発を主導するデジタル通貨「Libra（リブラ）」の発行に向けた動きだろう。

Libraは2019年に構想が発表され、現在、非営利団体「リブラ協会」が構想策定・実証を進めているデジタル通貨である。

当初、このデジタル通貨が他の暗号資産と異なる特長として提唱していた点としては、主要法定通貨のバスケットに連動させ、価値を安定させるという点が挙げられる。現在の多くの暗号資産は、取引量が少ないことや、値動きに上限が無いこと、規制の影響を受けやすいこと等から、価格の変動が激しく専ら投機手段として用いられており、価格の安定性が求められる用途での活用は困難な状況である。一方、このデジタル

図表10　Libraのサービスのイメージ

・利用者は、料金を支払い、Libra購入・・・ 1
・Libraは利用者からの資金を法定通貨でリザーブとして保存・・・ 2
・リザーブの一部は利回りの低い国債などに投資・・・ 3
・Libra協会はバリデーターに資金運用益を一定割合で分配・・・ 4



（出典）総務省（2020）「ブロックチェーン技術の活用状況の現状に関する調査研究」

＊3　医薬品が製造販売承認に基づき製造され、市場出荷された状態を維持し、品質の劣化、改ざん、破壊されないこと。

通貨は、発行額と同額のドル、円といった法定通貨を保全することで、価格の安定性が高い仮想通貨（ステーブルコイン）を構築することを目指していた。

そのため、この通貨の普及により、従来の銀行送金等より低い手数料で、短期間で国際送金が可能になることが期待されていた。

イ　規制当局等の反応

しかし、この動きに対して通貨当局等から懸念を示す発表が相次いでいる。例えば、米国連邦議会は個人のプライバシーや国家安全保障への懸念から開発の一時停止を要請しているほか、規制当局からもマネーロンダリング等、犯罪へ用いられることへの懸念の声が上げられている。

このような懸念の声もあり、構想が発表された2019年6月時点では、28事業者のリブラ協会への参加が予定されていたものの、7事業者が脱退を表明し、2019年10月のリブラ協会創設時の参加事業者は21事業者であった。また2020年4月には、法定通貨へのバスケットを断念し、単一の法定通貨に裏付けられた複数種類のステーブルコインを発行する可能性を表明した。

一方で、このような動向も受けた形で、各国の中央銀行もデジタル通貨の発行に向けた技術検証等に取り組んでいる。例えば中国人民銀行は2019年10月に世界で最初にデジタル通貨を発行するとの見通しを表明したほか、欧州中央銀行や日本銀行などは2020年1月に中央銀行によるデジタル通貨の発行を視野に入れた新しい組織を設立すると表明したところである。

暗号資産の中核技術として注目が集まったブロックチェーン技術であるが、ここ最近では様々な分野での活用が検討されだしている。また、金融分野においても暗号資産という枠を超え、我々の生活に身近な通貨のあり方も変えようとしている。今後、この技術の活用が生活の隅々まで進むにつれ、我々の生活は大きく変わっていくだろう。

コラム COLUMN 5

O2OからOMOへ*1

1 O2O・OMOとは何か

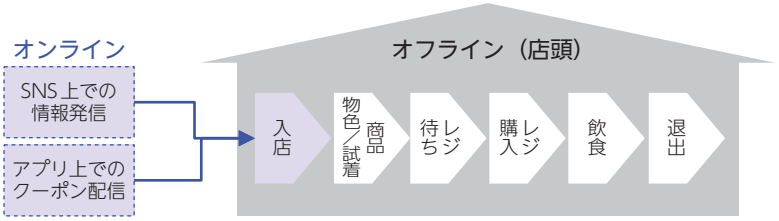
インターネットの普及とともに、これまで実店舗でのみ事業を展開していた事業者によって、SNSによる情報発信やアプリでのクーポンの配信など、オンライン上で活動することで実店舗へと顧客を誘導する取組が活発に行われるようになっている。このようにオンライン上での情報発信活動を積極的に行い、商品の購買やサービスの利用増等につなげる取組はO2O（Online to Offline）と呼ばれる。

さらに近年OMO（Online Merges Offline）という業態にも注目が集まっている。これは、消費者がオフライン（実店舗）上に居つつもオンライン（インターネット）上のサービスを利用できることで、従来オフライン上で体験できなかった新たなサービスが体験できるものであり、オフラインとオンラインの境目がなくなった状態を指すものとされる。

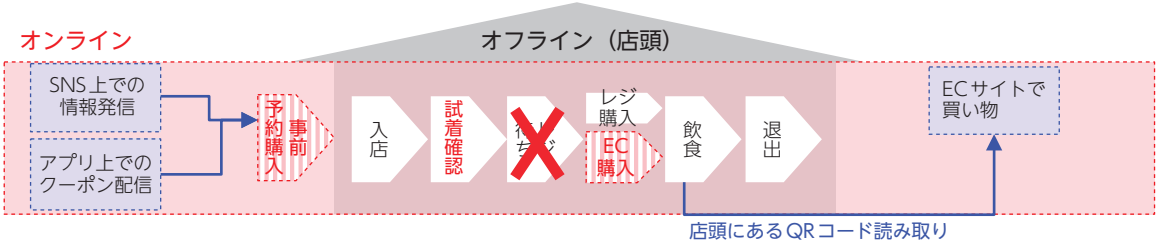
インターネットの普及と、さらにIoTの進展により、オフラインとオンラインが高度に融合されたSociety 5.0の社会においては、今後こうしたOMOの事業者は増えていくと予想される。本稿では先行事例として、我が国及び海外の小売事業者のOMOの取組の特長を、消費者及び小売事業者のメリットとともに紹介したい。

図表1　O2O及びOMOのイメージ

O2Oのイメージ（基本的にはオンライン→オフラインによるマーケティング施策）



OMOのイメージ（O2Oに加え、オフライン→オンライン、さらにオフライン上でのオンラインによる取組もある）



（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

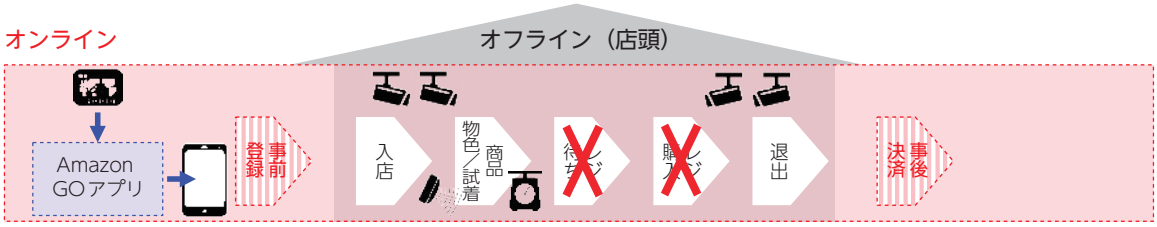
2 特徴的な取組事例

（1）アマゾン（米国）

アマゾンは、米国内において2018年1月より、レジのない実店舗「Amazon Go」をオープンしている。顧客は事前にクレジットカード情報を登録した専用アプリに表示したQRコードを入場ゲートにかざして入店し、欲しい商品を手に取ったままゲートから退店すると、アカウント情報と商品情報が紐づき後払いとして請求される（図表 2）。店内に配置された多数のカメラや商品棚に設置された重量センサーや音声マイクを組み合わせて、店内の顧客の商品をピックアップする動きを捕捉し、買い物している商品を認識することにより、このようなタッチ＆ゴー型の店舗を可能にしている。米国内では、その店舗網を2020年3月現在で26店舗に拡大しつつある。

*1　本コラムは、総務省（2020）「O2O及びOMOの現状に関する調査研究」を基に執筆した。

図表２　Amazon Goのサービス概要



✓事前に専用アプリをスマートフォンにインストールし、クレジットカード情報を紐づけ

✓入店後、店内に無数に配置されたカメラや商品棚に設置された重量センサーやマイクにより、店内の顧客の商品をピックアップする動きを捕捉することで、購入商品情報を記憶

✓退出後、購入商品情報と顧客情報を紐づけ、アプリ登録されたクレジットカードより自動的に引き落とされる

（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

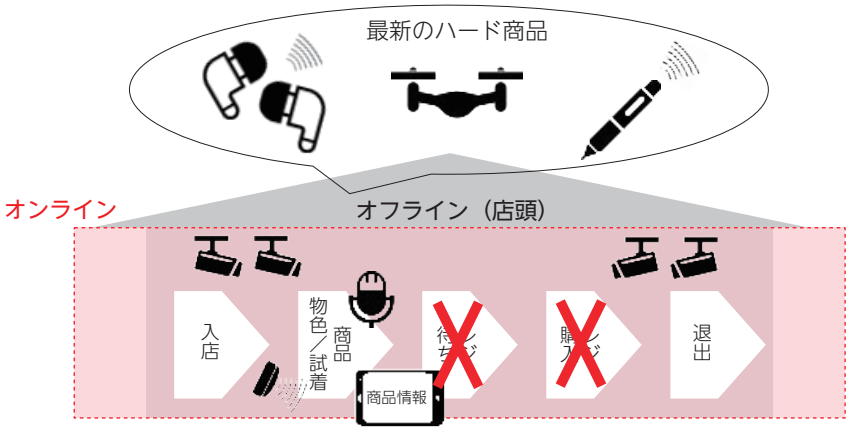
顧客にとっては、レジ決済が不要であることから、レジに並ぶ、現金やクレジットカードなどの支払い金額を準備するといった動作がいらないというメリットがあり、アプリを入り口のゲートにかざし、商品を手に取ってそのまま退出するだけで支払いが完了してしまうという、新たな買い物体験をすることができる。一方、事業者にとっては、これまでオンラインだけでしか捕捉することができなかった会員の購買活動をオフラインでも捕捉することが可能となり、実店舗の改良や新たな実店舗の開発が可能となる。また、「Amazon Go」で活用する技術をパッケージングしたJust for Walkと呼ばれるソリューションの提供を開始すると公表するなど、新たなビジネスに繋がる可能性もある。

(2) b8ta（米国）

2015年に米国で創業した同社は、Retail as a Service（RaaS）の概念を提唱する。スタートアップ企業が中心に製造するスマートホームデバイス、IoT製品、ドローン等、先進的なハード商品を店頭に展示するが、あくまでも消費者に対して商品と触れ合う体験を提供することに特化し、販売は一切しない「売らない」事業スタイルを取る。2020年1月現在、世界の25店舗において1,000以上のブランドが出店し、消費者と商品の関わり（エンゲージメント）は5,000万以上に上っており、今後は日本国内でも2020年夏を目標に2店舗の出店が予定されている[*2]。

同社の扱う商品は、例えば骨伝導型イヤホン、自撮り撮影用ドローン、アプリ連携したボールペン等、消費者がこれまでに体験したことがなく使用に当たって説明を要するものが多い。そのため、同社では商品ごとにタブレットを設置し、消費者はタブレットを用いて使い方の説明や利用事例等のコンテンツを閲覧する。この際、商品の製造主はタブレットの利用状況や店内のカメラやセンサーから来店者の情報を収集し、自社のマーケティングに活用することができるようになっている（図表 3）。

図表３　b8taのサービス概要



✓他小売店舗で見られない最新のハード商品を手に取ることが可能

✓店内はほぼ店員がおらず、設置されるタブレットで商品情報を閲覧する

✓店内のカメラやセンサー等で来店者の情報を収集

（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

消費者にとっては、他の小売事業者では取り扱っていないような、先進的な商品にいち早く触れることができる

＊2　三菱地所（2020）「新しい形の小売形態を展開する「b8ta Japan」社に出資　東京・有楽町に日本国内初出店が決定」（https://www.mec.co.jp/j/news/archives/mec200130_b8ta.pdf）

一方、商品を製造しているスタートアップ企業にとっても、これまで店頭で取り扱われなかった商品に対する消費者の反応について情報を収集できるというメリットがある。また、b8ta社は、展示品の販売をしない一方で、消費者情報を収集・提供するために展示スペースを貸し出すことで、スタートアップ企業から収益を得ている。さらに、先進的なハード商品に対する消費者の反応データを属性別に収集し分析することにより、反応の良い商品の傾向や、そういった商品を開発できるスタートアップ企業の傾向をつかみ、連携するスタートアップ企業や取り扱う商品について、消費者の支持を集めそうなものを抽出することができる可能性がある。

(3) パルコ（日本）

ア　取組の概要

日本国内においてもOMOに取組む事業者が増えてきている。

全国で商業施設を運営するパルコでは、2010年頃より、顧客との関係構築・維持のためにSNSや外部アプリ等を活用したO2O施策に積極的に取り組んできた。2012年頃からは、オフライン上での消費者行動を十分に理解した上で、顧客の求める機能を有するオンラインサービスを設計することを目指し、経営課題としてテクノロジー活用を前提とした消費者とのコミュニケーション方法の検討に着手した。その後、2014年秋には消費者一人ひとりに最適なサービスやコンテンツを最適なタイミングで配信する仕組みを構築した独自アプリ「POCKET PARCO」を公開している。

このアプリの導入によって、従来のクレジット機能付きハウスカードによる顧客の購買履歴に加え、顧客の来店のきっかけ（来店前行動）、来店中行動、来店後行動までを定量的に捉えることができるようになった（図表 4）。さらに、今後は、本アプリを活用して来店可能性の比較的高いと見込まれるアプリユーザーに対して、個人の特徴を踏まえた最適なマーケティングを実施することを目指している。

図表 4　POCKET PARCOの機能概要

機能名	概要	情報収集可能な消費者行動
CLIP	アプリ内のショップブログ記事を閲覧する際、お気に入りの記事を登録するとポイントが付与される。	【来店前】 来店きっかけとなった可能性のある情報が把握できる。
CHECK IN	来店時にアプリを操作することで、チェックインと見なされポイントが付与される。	【来店中】 来店したタイミング（時間、店舗）が把握できる。
WALKING	スマートフォンの歩数計測機能とアプリをユーザーが連携許可することで、来店中の一定歩数分ポイントが付与される。	【来店中】 来店中の消費者行動（一定歩数）が把握できる。
CONVERSION	アプリへ事前に登録したクレジットカードで買い物をすることで、ポイントが付与される。	【来店中】 来店中の消費者行動（購入）が把握できる。
STAR RATING	来店後の顧客に対して、プッシュ通知にてアンケート評価（5段階）を依頼され、回答することでポイントが付与される。	【来店後】 来店後の消費者意識（来店した店舗への評価）が把握できる。

（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

さらに2016年以降は、AR、VR、MRなどの仮想現実技術やIoT等のテクノロジーが従来に比べ比較的安価に活用可能となったことから、実店舗上での消費者行動に関連するデータ収集を進めている。その一環として、顧客の買い物に係る行動の情報が一つのプラットフォーム上で管理できる仕組みである「PARCO as a Service」の実現に向け、建替え工事を経て2019年11月にグランドオープンした旗艦店の渋谷PARCOの5階に、「PARCO CUBE」と呼ばれるOMO施策を取り入れたスペースを導入し、11ショップが出店している。各ショップの売場面積は従来の約半分であるため、店頭の商品在庫は絞っているが、各ショップのEC在庫データがパルコのECサイト「PARCO ONLINE STORE」と連動しているため、PARCO CUBEの各ショップや共用部に設置されているデジタルサイネージで、店頭在庫のない商品を閲覧することが可能となっている。来店した顧客は、サイネージ画面に表示されるQRコードを自身のスマートフォンで読み取ることで画面に表示された商品の情報をスマートフォンに転送でき、その後「PARCO ONLINE STORE」で決済し購入することができる。またPARCO CUBEの一部ショップでは、姿見のようなフォルムで、撮影した映像が数秒遅れで表示され背面の試着姿を確認できる「CUBE MIRROR」を導入している。加えて同フロアの吹抜け空間や外通路では、AR技術を活用した空間演出サービスも提供しており、顧客はこれらをスマートフォンで体験することができる。

本施策により、消費者にとっては、パルコに来店することでしか購入・体験できない商品・コンテンツを楽しむことができるほか、店頭レジで購入する際にも、「POCKET PARCO」や電子レシート等のテクノロジー活用により簡便化等が期待できる。さらに、同社は今後、顧客が自身の嗜好に合った魅力的な商品の紹介を受けることができるようにすることも想定している。

一方、事業者側にとっても、消費者とのタッチポイントを来店中だけでなく、来店前、来店後にも持つことができるため、消費者に関する定量的情報をより多く収集でき、従来、従業員の属人的なノウハウとなっていた消費者行動について、細かな分析が可能になる。

イ　OMO施策を進める上での課題意識や今後の見通しについて

OMO施策を進めるに当たり同社は、個人情報保護に配慮をしながらオフライン上での消費者行動を十分に理解した上で、顧客の求めているような機能を有するオンラインサービスを設計することが重要と考えている。そのほか、顧客の行動理解を進めるため、購入情報の収集だけではなく、来店前・来店中・来店後といったあらゆる時間軸上で顧客とのタッチポイントを作ることも重視している。

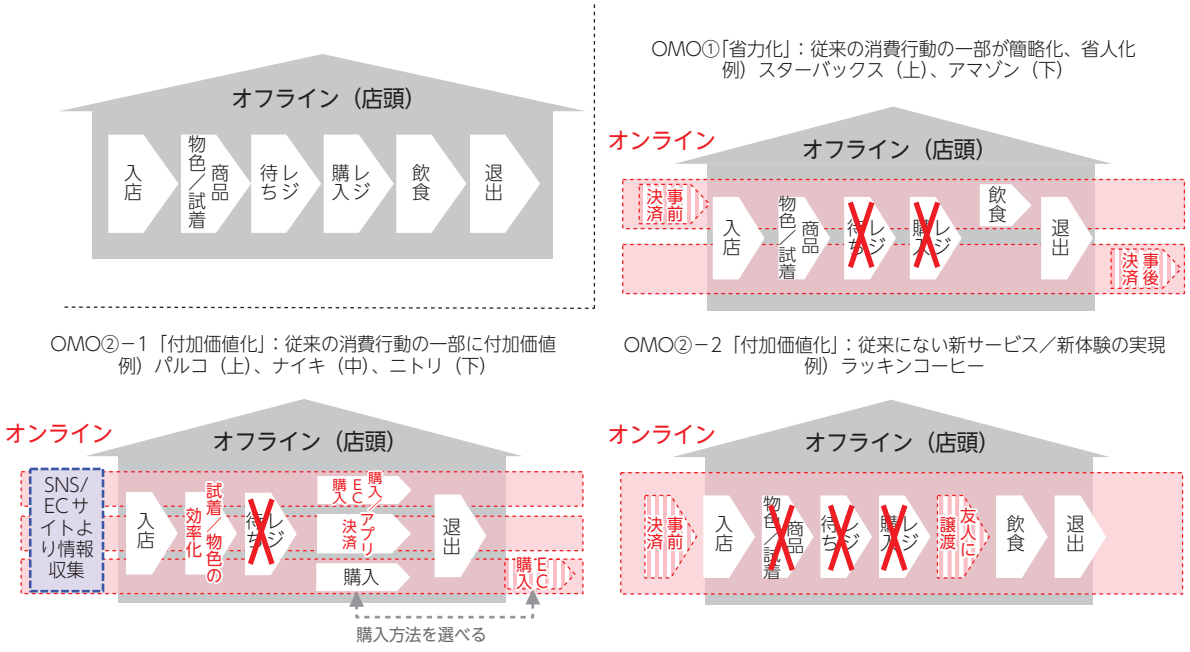
同社は、ECサイトで手に入る商品はECサイト上でも購入可能であることから、商品購入の価値提供だけであれば消費者の店舗への来店機会が減少していくのではないかとの考えを有している。そのため、パルコのような実店舗を有する小売事業者は、単なる商品購入のスペースとなるのではなく、「宝探しのように見るだけでわくわくする」ような、リアルかつ唯一無二の体験ができる店舗設計を行うべきだと考えているという。一方で、テクノロジー（オンライン）の活用に関連するノウハウは、他社から見て模倣しやすいものであり、そればかりに注視してはならないとしている。小売業界における唯一無二の存在を目指すためには、リアル店舗（オフライン）のコンセプトや空間設計、そして接客における工夫が重要であり、リアル店舗構築に向けたツールとしてテクノロジーの活用を進めたいとしている。

3　OMOは小売業にどのような変化をもたらすか

上記事例からOMOが小売業にもたらす変化をまとめると、消費行動、決済、タッチポイントの増加、の3点が挙げられる。

まず、OMOの進展による消費行動の変化については、図表 5の3パターンでの変化が考えられる。一つは省力化であり、従来の消費行動の一部が簡略化又は省人化される。もう一つは付加価値化であり、従来の消費行動の一部に付加価値が加わるというものである。また、この付加価値化には、従来にない新サービスや新体験を実現するという形のものも考えられる。

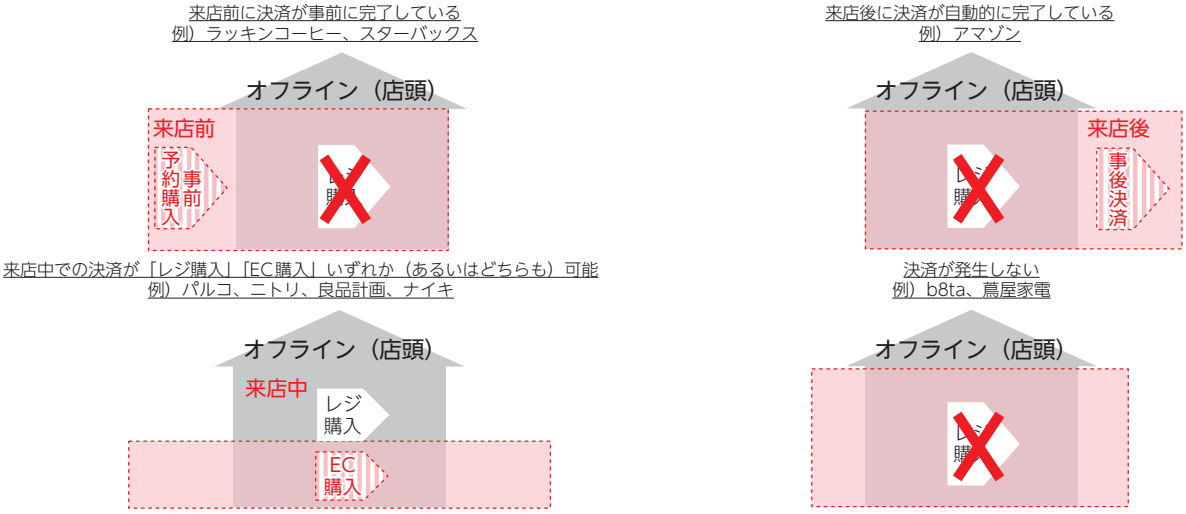
図表5　OMOによる消費行動の変化



（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

次に、決済の変化については、O2O施策では店頭への集客・誘致を進め、来店中のレジ決済による売上げの向上を目指していたのに対し、OMO施策では、スマートフォンアプリ上での決済など、来店中に限らず、来店前から来店後までのより広いタイミングにおける決済を可能とする。これにより、消費者は省力化等の付加価値を有する新しい買い物を体験することができる（図表 6）。

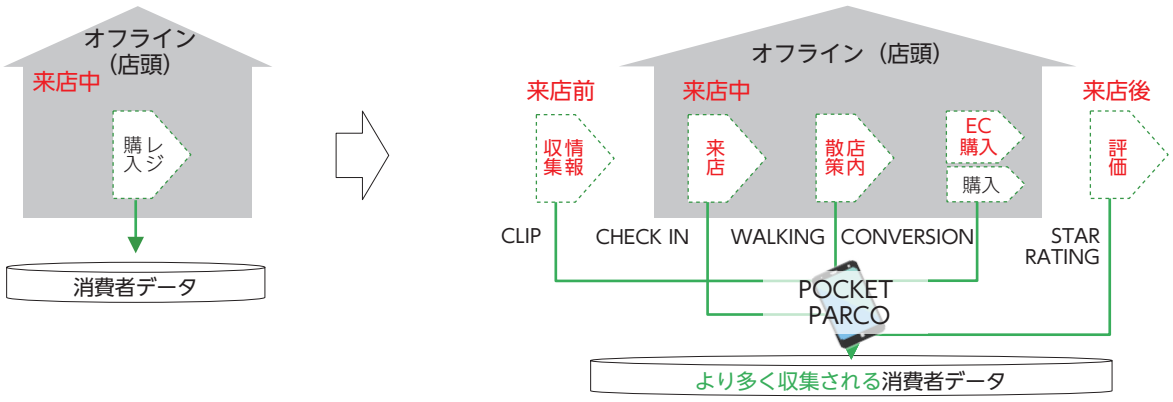
図表6　OMOによる決済の変化



（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

さらに、事業者側にとっても、OMO施策を打つことで従来よりも消費者とのタッチポイントを増やすことができ、消費者行動に紐づくデータをより多く収集することができる。前述のパルコにおけるアプリを活用した事例のように、収集した消費者データにより、事業者は消費者行動をさらに深く理解することができ、よりよいサービス提供につながると期待される（図表 7）。

図表7　OMOによる消費者とのタッチポイントの増加（パルコの例）



タッチポイント増加により、収集できる消費者データの量が増加

（出典）総務省（2020）「O2O及びOMOの現状に関する調査研究」

このようなOMO施策をより推進させるために、今後小売事業者は、収集した消費者データの活用による、店頭での消費者の体験の向上を目指すことが求められることが考えられる。また、このような消費者のデータ利活用に向けた理解度促進を進めるためにも、パーソナルデータ保護に関する企業努力は重要である。さらに、決済手段が店頭のレジ上だけでなく、事前決済、事後決済、あるいはEC上での決済等、従来型の店舗よりも多岐にわたることから、今までの店舗における売上高ベースのKPI[*3]だけでなく、OMO施策の効果を適切に測ることができるようなKPIへの見直し等、ICT活用の推進に向けた企業基盤の整備も必要であろう。

＊3　重要業績評価指標（Key Performance Indicatorの略）