

第4節

コロナ禍におけるデジタル活用で浮上した課題

コロナ禍において社会全体で急速なデジタル化が進められていたが、それに伴い、デジタル社会を実現するためには、様々な側面において課題があることが顕在化した。これらの課題は従来からあったものが多いが、コロナ禍において、社会全体がデジタル活用を行ったことにより、より問題が顕在化した、又は、深刻化したものである。

総務省が実施した調査^{*1}においても、デジタル化が進まない理由としては、「情報セキュリティ」、「リテラシー」、「利活用が不十分」、「通信インフラが不十分」及び「端末が十分に行き渡っていない」といった点が挙げられている。

これらの課題を解決しなければ、コロナ禍で経験したデジタル化に対して否定的な意見を持つ人が増え、デジタル化が定着しないおそれがあるため、これらの課題解決は益々重要となっている。

1 セキュリティリスクへの対応

新型コロナウイルス感染症の流行により、急速かつ強制的に社会全体のデジタル化が進展し、テレワークやオンライン授業など、従来利活用が十分に進んでいなかった分野でもデジタル化が進んでいる。それに伴い、デジタルに慣れていない利用者が増えるとともに、インターネットに接続される機器・アプリケーションなどが増え、システム構成や利用形態が多様化している。また、標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況が発生している。このような変化に伴い、セキュリティリスクに対応することが益々重要となっている。

1 セキュリティ被害

ア 情報セキュリティ10大脅威

情報処理推進機構（IPA）が毎年公表している情報セキュリティ10大脅威^{*2}においては、組織に対する脅威として、1位が「ランサムウェアによる被害」、2位に「標的型攻撃による機密情報の窃取」が挙げられているが、3位に「テレワーク等のニューノーマルな働き方を狙った攻撃」が新しくランクインした。

また、個人に対する脅威についても、コロナ禍では、デジタル手段による支払いやオンラインショッピングの利用が増える中、1位が「スマホ決済の不正利用」、2位が「フィッシングによる個人情報等の詐取」となっている（図表2-4-1-1）。

*1 総務省（2021）「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

*2 <https://www.ipa.go.jp/security/vuln/10threats2021.html>

図表 2-4-1-1 情報セキュリティ10大脅威 2021 (IPA)

順位	個人	昨年 順位
1位	スマホ決済の不正利用	1位
2位	フィッシングによる個人情報等の詐取	2位
3位	ネット上の誹謗・中傷・デマ	7位
4位	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位
5位	クレジットカード情報の不正利用	3位
6位	インターネットバンキングの不正利用	4位
7位	インターネット上のサービスからの個人情報の窃取	10位
8位	偽警告によるインターネット詐欺	9位
9位	不正アプリによるスマートフォン利用者への被害	6位
10位	インターネット上のサービスへの不正ログイン	8位

NEW：初めてランクインした脅威

順位	組織	昨年 順位
1位	ランサムウェアによる被害	5位
2位	標的型攻撃による機密情報の窃取	1位
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ビジネスメール詐欺による金銭被害	3位
6位	内部不正による情報漏えい	2位
7位	予期せぬIT基盤の障害に伴う業務停止	6位
8位	インターネット上のサービスへの不正ログイン	16位
9位	不注意による情報漏えい等の被害	7位
10位	脆弱性対策情報の公開に伴う悪用増加	14位

(出典) IPA (2021)「情報セキュリティ10大脅威 2021」を基に総務省が作成

イ テレワークにおけるセキュリティ被害事例

テレワークは、一部の従業員が利用するものから、Web会議を含め、一般的な業務・勤務形態となることから、セキュリティ被害が増大している。例えば、テレワークでは、オフィス以外から企業のシステムに接続するため、VPN機器を活用することが多いが、そのVPN機器の脆弱性を利用した不正アクセスなどが発生している（図表 2-4-1-2）。セキュリティ被害が生じた場合、会社の機密情報・顧客の個人情報等が流出する可能性もあり、また、会社自体の信用が低下する可能性がある。このように、テレワークでセキュリティ被害が生じた場合、影響は大きくなる可能性がある。

図表 2-4-1-2 テレワークにおけるセキュリティ被害事例

被害機関	内容
日新製糖株式会社	VPN機器の脆弱性をつかれ、社外からのリモートアクセスを管理するシステムに対しての不正アクセスがあり、リモートアクセスのログ情報が流出した。同社では、これに伴いVPN機器の使用を停止した。2020年12月1日公表。
三菱重工業株式会社	社員が在宅勤務時に社内ネットワークを経由せず、社外のSNSに接続したところウイルスに感染した。社員が感染したパソコンを社内ネットワークに接続したことで、社内へ感染が拡大した。その後サーバーに対して外部からの不正アクセスを受けた。2020年8月7日発表。
株式会社ディーカレット	金融系企業。社員のアクセス時ログ情報が不正アクセスを受けて盗まれた。顧客の個人情報や暗号資産の流出はないと説明。2020年12月1日発表。
札幌大学	VPNの脆弱性をつかれ、事務職員のテレワーク用のシステムがサイバー攻撃を受けた。事務職員9名分のIDが漏えいした。パスワードの機密情報の漏えいはなかったと発表。2020年12月4日第2報を公表。
米フォーティネット社製VPN装置を使用していた機関	VPN装置の欠陥が悪用され、国内の企業や行政機関がサイバー攻撃を受けていた。ID、パスワードの認証情報が被害にあった。例示されているのは、警察庁、日本政府観光局、リクルート、札幌大学。(2020年12月1日付、中日新聞記事による)

(出典) 総務省 (2021)「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

ウ オンライン教育におけるセキュリティ被害事例

オンライン教育においても、ランサムウェア攻撃により10万人以上の生徒がオンライン授業を受けられなくなる、ビデオ会議アプリの脆弱性を利用した攻撃により新学期ガイダンス中に不適切な映像等が共有される、教師による個人情報の誤った共有といったセキュリティ事案が発生している（図表 2-4-1-3）。

テレワークの拡大により利用が激増したWeb会議システム「Zoom」は、学校の遠隔授業向けに無料でサービスを提供し、多くの学校がサービスを利用していたが、セキュリティ上の懸念から、各組織でZoomの使用を制限する措置を実施した^{*3}。

*3 NHK ニュース (2020.04.05)「利用者2億人「Zoom」がセキュリティーに問題と発表」(<https://www3.nhk.or.jp/news/html/20200405/k10012369171000.html>)
CNN (2020.04.05)「米NY市、学校に「ズーム」の使用中止を指示 安全性に懸念」(<https://www.cnn.co.jp/tech/35151881.html>)

オンライン教育を受けるのは学生であり、また、学生の数が多いこともあり、オンライン教育におけるセキュリティ被害が生じた場合、影響が大きくなる可能性がある。

図表 2-4-1-3 オンライン教育におけるセキュリティ被害事例

被害機関	内容
米国メリーランド州ボルチモア郡の公立学校	2020年11月28日に米国のメリーランド州ボルチモア郡の公立学校がランサムウェア攻撃を受けた。これによって、11万5千人の自宅学習中の学生が突然遠隔授業を受けられなくなった。
国立大学法人香川大学	2020年4月17日の経済学部の新学期ガイダンスをZoomで行った。途中、Zoombombingの被害を受けた。開始10分ほどで、共有機能を使い、性的な映像や外国語の文字が画面に表示された。
公立大学法人公立諏訪東京理科大学	遠隔授業実施の際、教員（専任）が担当科目の履修学生（41名）に対し、学生1名の個人情報に係る情報（学籍番号等のプライバシーに関する基本情報）を3分間程度画面に共有した。41名の学生に対して学校から個人情報に関する不正利用がないよう依頼を行った。

（出典）総務省（2021）「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

2 セキュリティ対策の重要性

このようなセキュリティ被害を防ぐためには、常に最新のセキュリティアップデートを適用する、パスワードとして第三者に推測されにくい複雑なものを設定するなどの基本的なセキュリティ対策が重要である。ただ、テレワークやオンライン教育の場合、身近に相談できる人がいないため、より手厚い支援が必要となる。

総務省としても、テレワークセキュリティに関して、専門相談窓口を開設するとともに、テレワークセキュリティガイドラインを策定している^{*4}。また、新型コロナウイルスの影響により、これまで未導入だった中小企業等においても、テレワークの導入が広がる中、テレワークセキュリティガイドラインを補うものとして、中小企業等においても実現可能性が高く優先的に実施すべきセキュリティ対策を示したチェックリストを新たに策定している^{*5}。

2 リテラシー向上の必要性

デジタルによる効用を最大限活用するとともに、セキュリティなどのデジタル化の負の課題を解決するためには、デジタルの利用側のリテラシーの向上は重要である。

デジタル社会に向けて、スマートフォン・タブレットといった端末だけではなく、ウェブ会議など様々な目的で利用できるアプリケーションが登場している。このように多様化するICTツールについて、それぞれ使い方が異なり、また、必要なセキュリティ対策等が異なる。全てのツールについて利用者側で習熟することは難しく、デジタルの提供側が必要なセキュリティ対策を行う、UI/UXを改善するといった取組も重要ではあるが、それだけではなく、利用者側においても、基本的な操作方法を習熟することは重要である。

また、先述したZoomに関しては、システムの改善がなされ、パスワード設定や、待機室というホストからの承認を得ることで初めてミーティングに参加できる機能や、途中からは会議に参加できない仕組みであるミーティングロックが導入されている。他にも画面共有機能を主催者のみに設定できる機能や、スクリーンショットに機密データが表示されないようスナップショットをばかす機能が追加されている。このように日々革新される機能を有効に活用するためのリテラシーも求められている。

セキュリティに関しても、適切なパスワード設定をする、アプリケーションを定期的にアップ

*4 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/#guide

*5 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/#checklist

デートするといった基本的な対策で解決できる点も多く、そのようなリテラシーも身につける必要がある（図表2-4-2-1）。

図表2-4-2-1 セキュリティ対策のためのアプリケーションの最新化



（出典）総務省（2020）「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料」

新型コロナウイルス感染症に関しては、インターネット上で様々な情報が氾濫したが、その中には多くの偽情報も含まれ、SNSの普及を背景とした世界的なインフォデミックの危険性が指摘された（詳しくは第2章補論を参照）。膨大な情報の中から受け取った情報の真偽を見極める姿勢が個々人に求められており、情報リテラシーの向上も重要となっている。

これらのリテラシーは、デジタル化が急速に進展したために新たに必要となるリテラシーである。リテラシーが十分でないことが原因で、デジタル化によるメリットが享受できず、取り残されてしまうことがないように、必要な支援を実施することが重要である。

そのため、総務省では、民間企業や地方公共団体などと連携し、デジタル活用に不安のある高齢者等の解消に向けて、オンラインによる行政手続きやサービスの利用方法等に対する助言・相談等を実施する事業（デジタル活用支援推進事業）などの取組を行っている。

3 デジタルデータの取扱い

1 パーソナルデータの取扱い

デジタル社会では、日常生活における様々なデータを収集し、活用することになる。データを最大限活用することがデジタル社会の効用を最大限発揮することとなるが、そのデータには、健康情報などのパーソナルデータが含まれることとなる。今回のコロナ禍では、世界的な健康に対する脅威への対応として、世界各国でスマートフォンを活用した市民の行動履歴や接触者履歴等のデータの収集と分析が行われ、さらなる感染拡大防止のための予防や注意喚起を行うことを可能とした。一方で、こうした公衆衛生の観点からのユーザの位置情報や行動履歴の取得に関する議論においては、パーソナルデータ利用における公共の福祉とプライバシー等の個人の人権との間のバランスの問題が浮き彫りとなった（図表2-4-3-1）。

図表 2-4-3-1 各国における接触確認アプリの比較（2020年）

大 ↑ プライバシー 影響度 ↓ 小	国	導入時期（DL数）	接触把握方法 （位置情報利用／Bluetooth利用）	電話番号等の個人情報取得	陽性者データ管理 （中央サーバー型／個別端末分散型）
	中国	2月（不明）	自己申告（位置情報、決済情報等は当局が把握可能）	電話番号等を予めプラットフォームのアプリ導入の際に取得	中央サーバー型
	インド	4月11日（9000万以上：人口比7%）	位置情報＋Bluetooth	位置情報・電話番号取得（氏名、年齢、性別、職業、渡航歴、喫煙歴も取得）	中央サーバー型
	イスラエル	3月22日（150万以上：人口比17%）	位置情報（Bluetooth併用型の開発を進める）	位置情報	分散型
	オーストラリア	4月26日（500万以上：人口比20%）	Bluetooth	電話番号取得（氏名、郵便番号、年代も取得）	中央サーバー型
	シンガポール	3月20日（140万以上：人口比25%）	Bluetooth	電話番号取得	中央サーバー型
	英国、フランス	5月中	Bluetooth	なし	中央サーバー型を検討中
	ドイツ、スイス、エストニア等	5月中	Bluetooth	なし	分散型を検討中 （Google・AppleのAPI活用）

（出典）新型コロナウイルス感染症対策チーム事務局（2020）「接触確認アプリの導入に係る各国の動向等について」

このうち個人が所在する場所を示す位置情報は、場合によっては個人の趣味嗜好、さらには思想信条まで推測することを可能とするものであり、また、当該情報を一定期間継続して取得することで、個人の行動状況を把握することも可能となる。特にGPS測位に関する位置情報は、携帯電話基地局を利用した位置情報よりもより詳細な所在地を示すものであることから、その取得によりさらに容易で詳細な把握が可能となる。

これらのデータを活用することは、コロナ禍のような緊急時だけでなく、平常時においても生活の利便性は大きく向上する一方、プライバシーや個人情報保護とのバランスを考える必要があり、今後も多くの議論がなされていく必要があるであろう。

2 政府によるデータ収集とオープンデータの活用

我が国においては、新型コロナウイルス感染症拡大防止の取組に関し、政府や地方公共団体は、民間企業の協力を仰ぎながら、統計データを活用した地域での人流把握等を実施してきている。この取組を契機として、平常時においてもデータを活用した政策判断が推進されることが期待できる一方で、政府が民間企業にデータ提供を要請する際のルールや条件を明確化することや、データの活用に当たっては、データ連携ができるよう標準化を進めることなどが重要である。

また、オープンデータをめぐっては国や地方公共団体が公表している情報が機械判読しにくい又はデータの形式が揃っていないといった課題がかねてより指摘されている。分野横断的に活用可能な共通の仕様を設定し、機械判読性の高いデータ形式での公開を徹底していく必要があるだろう。

4 通信インフラの増強

デジタル社会は、デジタルデータの流通量が増大するが、それを支える通信インフラの増強も重要である。NTTコミュニケーションズによると、1回目の緊急事態宣言期間中である2020年5月中旬の日中の通信量は、同年2月24日週との比較で最大約6割増加した^{*6}。在宅勤務や休校措置の拡大で、遠隔会議や動画視聴の機会が増えたことが、通信量急増の原因と考えられ、同年4月から遠隔授業が本格的に開始されることで、通信量のさらなる増加が想定された。

総務省は、2020年4月3日に学生等の学習に係る通信環境の確保に課する要請を電気通信事業

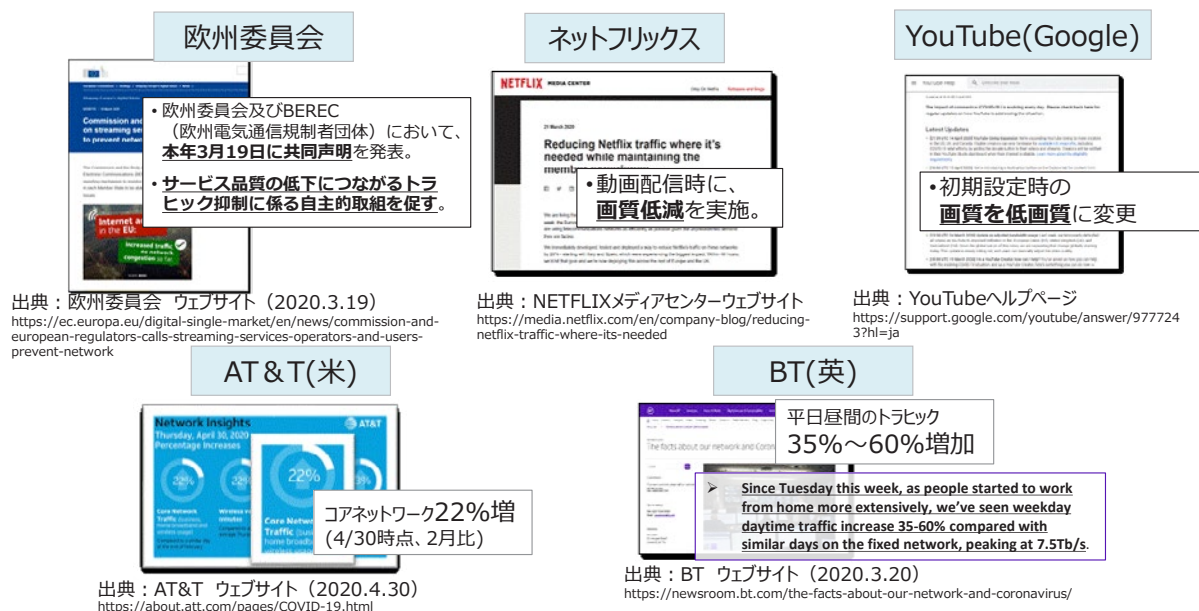
^{*6} NTTコミュニケーションズ「インターネットトラフィック（通信量）推移データ」(<https://www.ntt.com/about-us/covid-19/traffic.html>)

者関連4団体に対して行った^{*7}。学生等の自宅等の通信環境によっては携帯電話の通信容量制限等により学習を行うことが困難となる場合も想定されることから、通信容量制限等について柔軟な措置を講じること等について要請したものである。

1回目の緊急事態宣言の解除以降、特に平日昼間の通信量は目に見えて減少しており、技術的に深刻な問題までには達しなかった。総務省報告書^{*8}によると、新型コロナウイルス感染症の拡大に伴う在宅時間が増加する「巣ごもり」現象が生じる中、インターネットトラフィックは年間で約6割増と急増したが^{*9}、ピーク時間帯のトラフィックに十分耐えられるよう設計してあること、東京2020オリンピック・パラリンピックに向けて十分に設備投資を行っていたことから、インターネットサービス品質は維持された。

海外においても、インターネットトラフィックは急増しているが、欧州委員会及び欧州電気通信規制者団体（BEREC）がコンテンツ事業者にトラフィック抑制に係る自主的な取組を促すことで、ネットワーク障害等の影響を回避した^{*10}（図表2-4-4-1）。

図表2-4-4-1 海外における新型コロナウイルス感染症拡大によるインターネットトラフィックへの影響



（出典）総務省（2020）「インターネットトラフィック研究会 第1回会合（総務省提出資料）」

今後、デジタル社会に向けて、テレワークやオンライン教育等が普及し、映像伝送など大容量通信の増加が予想される。また、ゲーム、オンラインライブ、OSのソフトウェア配信やアップデート等のイベントが原因で一時的にトラフィックが増加することも多い。快適なデジタル社会のためには、単にインターネットに繋がるだけではなく、通信速度の低下や遅延が生じないよう、インターネット品質も重要である。

そのため、今後は、デジタル社会におけるインターネットトラフィック増加に耐えうるような更なるインフラ増強、インターネットトラフィックへの負荷軽減策などの取組がより一層重要である。

^{*7} 総務省（2020）「新型コロナウイルス感染症の影響拡大に伴う学生等の学習に係る通信環境の確保に関する要請」（https://www.soumu.go.jp/menu_news/s-news/01kiban03_02000630.html）

^{*8} 総務省（2021）「インターネットトラフィック研究会報告書」（https://www.soumu.go.jp/main_content/000752366.pdf）

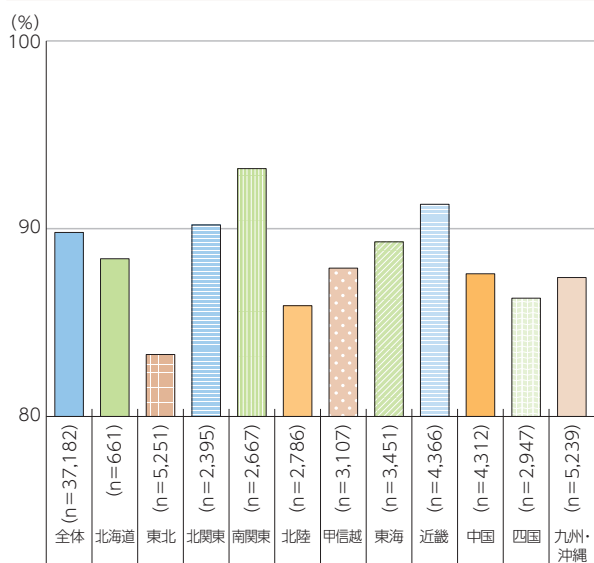
^{*9} 総務省「インターネットにおけるトラフィックの集計・試算」によると、2020年5月集計では、前年同月比57.4%増となった。

^{*10} 具体的には、Netflixは30日間にわたりヨーロッパ域内の配信ビットレートを削減させた。YouTubeは動画再生品質の初期設定値を一時的に低減させていた。

5 地理的条件等による格差の是正やアクセシビリティの確保

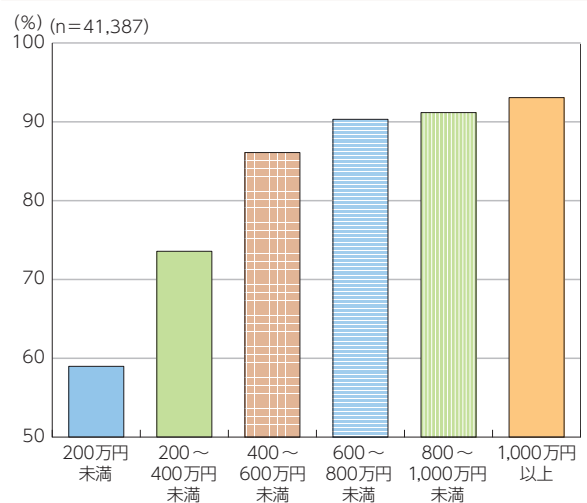
新型コロナウイルス感染症の感染拡大は、我が国でも特定の地域に限定した事象ではなく、全国規模で現在も続く事象である。感染拡大防止の観点から外出抑制などが行われる中、消費行動や企業活動においてデジタル活用が進んだことは先に述べた。しかし、実際の活用状況をみると、地域や年収等による差が見受けられる。例えば、インターネット利用率について、地域や世帯年収によって異なる（図表2-4-5-1、図表2-4-5-2）。

図表2-4-5-1 インターネット利用率（2020年、地域別）



（出典）総務省「通信利用動向調査」

図表2-4-5-2 インターネット利用率（2020年、世帯年収別）



（出典）総務省「通信利用動向調査」

その理由として、住民や企業の経営者・従業員の意識の違いも考えられるが、デジタル活用の前提となる情報通信インフラの整備状況が地域で異なること、経済的状況によりデジタル活用に必要な端末の保有状況が異なること等がこのような格差が生じる要因の一つになっていることも考えられる。

今後、コロナ禍のような非常時だけでなく、平常時においても、全ての人がデジタルによる恩恵を享受できるようにするには、5Gや光ファイバといった情報通信インフラの整備を全国で進めること等を通じて、地理的条件等による格差を是正することが重要である。

また、デジタルサービスの利用時における操作性の難しさや手続きの煩雑さをデジタル化の障壁として挙げる意見もある。先に述べたユーザ側のリテラシー向上も重要であるが、サービス提供者側がUI/UXに配慮し、ユーザにとって使い勝手の良いサービスを提供することを通じて、年齢、障害や言語等の違いを踏まえつつも、ICT機器やサービスに誰もがアクセスできるようアクセシビリティを確保することは重要な課題である。

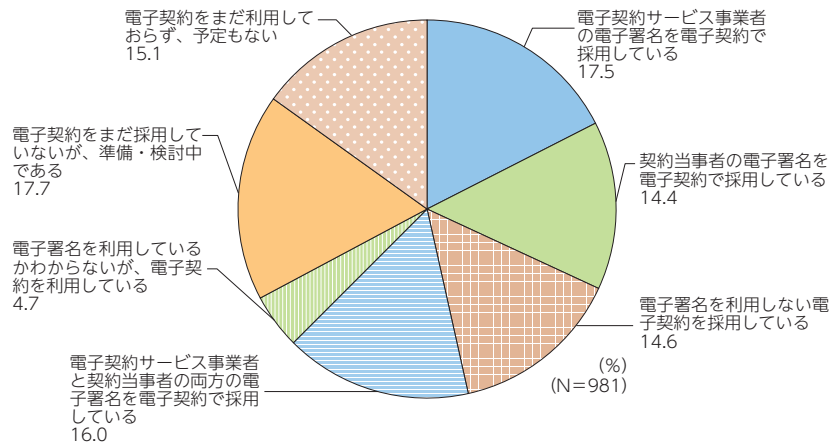
6 デジタル化を前提とした業務・慣習の見直し

緊急事態宣言下で導入が進んだテレワークであるが、その導入に関する我が国特有の課題、特に官公庁のテレワークが進まない要因の一つとして指摘されているのが、押印や書面を前提とした手続きの存在である。民間企業でも書面での契約書類の作成や押印行為のために出社せざるを得ず

レワークができない事象が発生している^{*11}。

これに対し、電子契約の利用を開始する企業が出てきている。一般財団法人日本情報経済社会推進協会（JIPDEC）と株式会社アイ・ティ・アールが共同で実施した「企業IT利活用動向調査2021」^{*12}によると、電子契約の利用企業は、前回調査時（2020年7月）の41.5%から67.2%に拡大し、今後の予定を含めると、8割強が電子契約を利用する見込みとなっている（図表2-4-6-1）。

図表2-4-6-1 電子契約の利用状況（2021年1月）



（出典）JIPDEC/ITR（2021）「企業IT利活用動向調査2021」

新型コロナウイルス感染症の影響が長期化する中、感染拡大の予防を図りつつも、社会経済活動を維持していくためには、デジタル化を前提とした新しい業務やサービス提供の在り方の確立が求められており、これまでの慣習を見直し早急に新しい生活様式に移行していく必要がある。

*11 日本経済新聞（2020.04.02）「ハンコ押すため出社…契約書類、在宅勤務の壁」（<https://r.nikkei.com/article/DGXMZO57566900S0A400C2EE8000?s=4>）

*12 <https://www.jipdec.or.jp/topics/news/20210318.html>