■レポート■

# テレワーク時代のセキュリティ

NRIセキュアテクノロジーズ
Cyber Security Services Department セキュリティコンサルタント
**高見澤　涼**

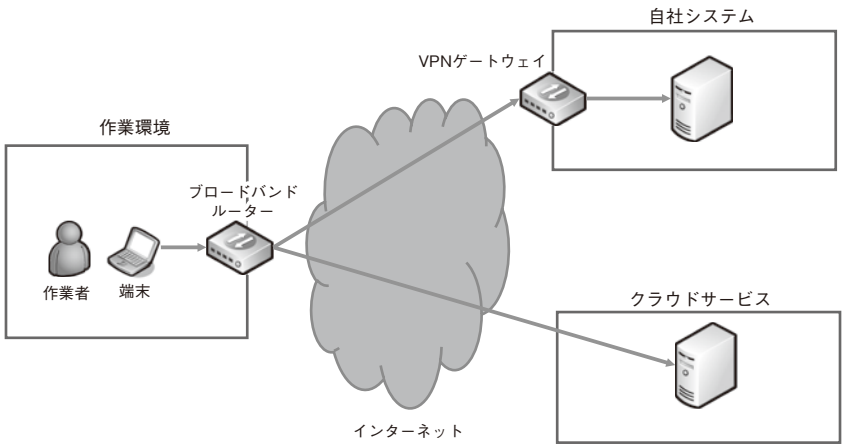
## 1．はじめに

新型コロナウイルスの感染拡大により、世界各国で不要不急の外出や人々の参集を自粛、規制する動きが広がっている。こうした動きは、企業における従業員の働き方にも影響を与えている。大きなものとしてはテレワークの利用拡大が挙げられるだろう。テレワークとはインターネット等の情報通信技術を用い、場所にとらわれずに自宅、外出先、サテライトオフィス等において業務を行う働き方である。新型コロナウイルス感染拡大以前でも、東日本大震災や、働き方改革の流れを受け、テレワークの利用は近年増加していた。総務省が毎年実施している通信利用動向調査では2012年から2018年の間で企業におけるテレワークの利用は1.6倍（11.5%から19.1%）に拡大しているとの結果が出ている（※1）。そして新型コロナウイルスがこの動きに急激な変化を加えた。緊急事態宣言が発出される前後（3月上旬と4月上旬）でテレワークの実施者率を比較したところ約2.1倍（13.2%から27.9%）増加したとの調査結果が出ている（※2）。さらに同調査において、テレワーク導入が比較的進んでいると言われる大企業においても、半数以上が未だテレワークを実施していないことも確認された。新型コロナウイルスへの対応は長期化するとの声も聞かれ、テレワークが実現できていない企業へも今後テレワークの導入が拡大していくものと思われる。

一方で、急速なテレワークの利用拡大を受

〈目　次〉

（図表１）テレワークを実現するためのIT環境




けてセキュリティに関する懸念も広がっている。有名なものでは、テレビ会議システムとして利用が急拡大したZoomにおけるセキュリティ問題が挙げられる。当該サービスでは強度の弱い暗号化アルゴリズムの利用、利用者の同意なしのFacebookへの情報送信等多数の問題が専門家により発見され、米国国防総省、NASA等多数の機関で利用禁止となった。また、トレンドマイクロ社の調査によると、３月は新型コロナウイルスに関連する不正サイトへの誘導が前月比で約3.6倍になったとのことである（※３）。今回の騒動に便乗し、不正サイトへ誘導し個人情報を搾取したり、マルウェアに感染させたりする事例も多数報告されている。

本稿では、上記を背景に、急速に利用が拡大するテレワークにおけるセキュリティ対策を整理する。整理するセキュリティ対策は複数の領域に跨るため、対策の全体像を把握しやすいよう、対策の実施対象および対象間の関係を考慮した上で説明する。また、それらセキュリティ対策は多岐にわたり、導入を進める上で様々な点に注意する必要があるため、進め方に関する注意点も短期的施策、長期的施策に分けて説明する。

## ２．テレワークにおけるセキュリティ対策

企業のIT環境は業界や規模により大きく異なり、またテレワークの実現方法も多種多様に存在するが、本稿では大抵のテレワーク環境で存在すると考えられる４つの要素（端末、作業環境、自社システム、クラウドサービス）を中心に検討を行った。テレワークでは基本的には電子情報を操作、編集するための「端末」が必要となる。そして、その端末は自宅ないし外出先を「作業環境」として作

業者が準備し、インターネットを介して、電子情報が保管されている「自社システム」か「クラウドサービス」に接続する。本章では上記要素毎にセキュリティ対策を説明する。

### （ア） 端末におけるセキュリティ

#### ① 基本的なセキュリティ対策

端末の種類としては、PC、スマートフォン、タブレット等様々な種類があり、機種やOSの種別により違いはあるもののセキュリティ対策の基本的な考え方は同じだ。まず、最初に挙げられるものはウイルス対策だ。社内ネットワークに接続して端末を利用する場合、インターネットと社内ネットワークとの境界にウイルスを検知、除去する機器を導入しているケースが多い。しかし、自宅や外出先では端末を直接インターネットに接続するため端末がウイルスに触れる可能性がより高い状態となる。そのため、テレワークにおいてはより優先度が高い対策となる。次に挙げられるのはセキュリティパッチの適用だ。端末で利用しているソフトウェアでは攻撃のきっかけとなる脆弱性が日々発見されている。攻撃者はこの脆弱性を狙い端末に対して攻撃を仕掛けてくるが、ウイルス対策と同様、インターネットからの脅威に直接さらされているテレワーク環境では、セキュリティパッチが配布されたらできる限り早急に対応することも必要である。また、テレワークでは端末を持ち歩く機会が増える。そのため、端末が紛失、盗難した際の対策も必要となる。対策の一つとして挙げられるのは保存されているデータの暗号化だ。個別データやアプリケーションの暗号化等様々な種類の暗号化があるが、ハードディスク全体を暗号化しておくことで対応が可能である。もう一つの対策としては、保存されているデータを遠隔で消去するサービス、システムを利用することも挙げられる。この対策を実施する際には、紛失、盗難時の連絡プロセスも合わせて作成し、事前に周知を徹底しておくことも重要である。

また、テレワーク環境ではシステム管理者の目が物理的に届かないところで利用されているため、上記に挙げたセキュリティ対策が適切に設定されない可能性がある。そのために、全端末の設定を遠隔で収集、操作するための仕組みも導入することが重要である。各端末の状況をクラウド上のシステムに集約し、管理者が一元的に端末の状況を確認できるソリューションも多く利用可能であり、それらを活用することも有効である。

#### ② 私用端末の対策

また、端末のセキュリティ対策においては私用端末への対策も忘れてはならない。テレワークでは、コスト削減や、社用端末の整備が間に合わない等の理由で私用端末の利用を認めるケースも多く存在する。私用端末であっても前述した基本的な対策は実施すべきであるが、さらに私用端末特有のポイントを2点ご説明する。まずは、利用できる端末を限定することである。利用端末を限定しない場合、ネットカフェや空港の共有PC等でも業

務データを利用されてしまう可能性があり、情報漏洩のリスクが高まる。そのため、私用端末の利用を開始する際には申請制とし、技術的にも許可した端末以外はアクセスできない仕組みを導入することが有用である。次のポイントは､利用できるデータの限定である。私用端末では私的なデータと業務データの境界が曖昧になり、機密情報が外部に漏洩してしまう可能性が高い。そのため、業務データは特定のアプリケーションのみでしか操作、閲覧できない、または端末にはデータが保存されない仕組みを導入することが有効である。

### （イ） 作業環境のセキュリティ

#### ① 自宅での対策

第１章でも述べたようにテレワークを行う環境としては自宅、外出先、サテライトオフィスが考えられるが、不要な外出を行わないことが求められている状況に鑑み、自宅における対策について考えてみたい｡前述の通り、テレワークには端末を接続するためのインターネット環境が必須である。通常各家庭ではインターネットと自宅ネットワークとの境界にブロードバンドルーターと呼ばれる機器を設置する。自宅内でインターネットへ接続する際はこのブロードバンドルーターに各端末を有線、または無線接続することになる。ブロードバンドルーターには、インターネットの住所録にあたるDNS（ドメインネームシステム）情報が登録されている。攻撃者がこの情報を書き換えることで、利用者は不正なWebサイトに誘導されてしまう可能性がある。この攻撃を防ぐためには２つの対策がある。１つはブロードバンドルーターのソフトウェアを常に最新の状態に保つことだ。取扱説明書等で設定を確認し、可能であれば自動更新がされるようにしておくことが重要である。もう１つはブロードバンドルーターの設定を行うための管理者ID、パスワードの変更だ。これらの情報はメーカーや機種によって初期設定が同一である場合があり、攻撃者に推測されてしまう恐れがあるため、ブロードバンドルーターの利用開始時に複雑なものに変更しておくことが有効である。

また、無線通信を利用する場合には、自宅の近隣にも電波が広がる可能性もあり、脆弱な暗号通信を利用していると通信が盗聴されてしまう可能性がある。そのため、強度の高い暗号技術であるWPA２－PSK等を利用した上で、強固なパスワードを設定することが望ましい。

#### ② 外出先での対策

今後、外出に関する自粛も緩和され自宅外での作業も広まってくることを想定し、外出先でのセキュリティ対策についても整理する。外出先での大きな脅威は悪意のあるアクセスポイントへの接続である。例えば悪意のある者がレストランの名称や駅名等その場所を想起する名称をアクセスポイントに設定することで、そのアクセスポイントを経由する通信が傍受される可能性がある。そのため、

外出先では本当にその場所で該当するアクセスポイントが提供されているかをアクセスポイント提供者に確認することが有効である。さらに当該アクセスポイントを利用してのインターネットアクセスは暗号化された通信かを確認することも重要である。

また、外出先では周囲に不特定多数の第三者がいることを意識し、覗き見防止フィルターを利用する、電話での会話では機密情報を話さない、紙の取り扱いには気を付ける等の工夫も必要である。

### （ウ） 社内システムのセキュリティ

#### ① 社内システムまでの通信に関する対策

一般的な企業では業務データを取り扱う社内システムへのアクセスは社内ネットワークに限定している場合が多い。そのため、社外から社内システムにアクセスする場合には端末と社内システムの間を暗号化した通信で結び、仮想的に社内ネットワークに接続している状況を作り出す必要がある。このための技術をVPN（バーチャルプライベートネットワーク）と呼ぶ。この技術を利用する場合には社内ネットワーク側に専用の機器を設置し、各端末と暗号化通信（VPNアクセス）を行う。この際にポイントとなるのは2点ある。

1点目はVPNアクセス時の認証である。社外から社内システムにアクセスできるということは、攻撃者も不正なアクセスを試行することができるということである。不正ログインを防ぐためには2つ以上の異なる要素を用いた認証（多要素認証）を行うことが望ましい。これは2種類のID／パスワードを使って認証することではない。それぞれに同じパスワード設定されてしまうと、十分な安全性が確保されない。そのため、ID／パスワード（知識認証）と専用のトークンから発行されるワンタイムパスワード（所有物認証）を組み合わせる等複数の要素を用いた認証を行うことが推奨される。端末に証明書をインストールすることでその端末自体が認証要素となる設定も可能であり、端末の項目でも説明したように業務で利用する端末を限定するためにもこの方式の利用は有効である。

2点目は社内ネットワーク側専用機器のVPNアクセス許容量の確認である。VPNアクセスをする際は個人にVPNアカウントを払い出し、それを用いてアクセスすることになるが、そのアカウントは専用機器の機種、またはライセンスに依ることがある。そのため、事前に利用者数と必要となるアカウント数を確認しておく必要がある。また、大人数が大容量のデータを同時に授受しようとした場合、専用機器やそこに接続されるインターネット回線がパンクしてしまう可能性がある。データ利用量を推測した上で機器の選定やインターネット回線契約を見直す必要がある。

#### ② 社内システム自体の対策

次に社内システム自体のセキュリティ対策を説明する。1点目は社内ネットワークの適

（図表２）認証要素の種類

| 種類 | 概要 | 例 |
|---|---|---|
| 知識認証 | 本人しか知らない情報を用いた認証 | ・ID／パスワード |
| 所有物認証 | 本人しか持っていない所有物を用いた認証 | ・電子証明書<br>・ワンタイムパスワードを発行するトークン |
| 生体認証 | 本人の生体情報を用いた認証 | ・指紋認証<br>・虹彩認証<br>・声紋認証 |

切な分離だ。前述の通りテレワークにおける端末の利用は社内ネットワークでの利用に比べ外部からの脅威にさらされている。また、社内ネットワーク自体も外部からのアクセスを許可しているため、攻撃者からの脅威にもさらされている。それら脅威により社内システムが侵害されてしまった場合に備えて、テレワーク業務として社外からのアクセスを許可する社内システムは、可能な限り他のシステムとネットワークを分離することが望ましい。

２点目はデータのダウンロード制限だ。これは採用しているシステムや技術に依存するところではあるが、機密度の高い情報は端末にダウンロードできない設定とすることで、情報漏洩のリスクを下げることができる。ダウンロード制限ができるかどうかは利用しているシステムに依存してしまうため、VDI（仮想デスクトップ環境）を社内ネットワークに用意し、作業者はリモートでVDIを操作するのみとし、データは一切端末には保存できないような環境を整備する等の対策を実施することも有効である。

### （エ） クラウドサービスのセキュリティ

#### ① 基本的な対策

近年クラウドサービス自体の利用は増加しているところではあるが、テレワークとクラウドサービスはとても親和性が高い。社内システムを利用する場合は前述の通り、社内システムに接続するまでの環境の整備に労力を要する。また物理的な機器の設定、管理のためには機器設置場所まで出向く必要もある。一方でクラウドサービスはインターネットでどこからでもアクセスされることを前提とし設計されており、また機器の運用管理も事業者側で実施するため、テレワークには適している。

ここでは社内システムと比較しながらクラウドサービスのセキュリティ対策を整理してみた。まず、クラウドサービスまでの通信について整理する。現在提供されているクラウドサービスでは通常暗号化通信が実装されており、利用者側で対策を講じる必要があることはほぼないと考えてよい。また、アクセス時の認証は、ID／パスワードに加えそれ以外の認証をクラウドサービス事業者側で提供し、前述の多要素認証の利用が可能となって

（図表３）テレワークにおけるセキュリティ対策

| 対象 | 分類 | 対策 |
|---|---|---|
| 端末のセキュリティ | 基本的な対策 | ウイルス対策 |
| | | セキュリティパッチ適用 |
| | | データの暗号化 |
| | | データの遠隔削除、紛失・盗難時手順の作成 |
| | | 端末状況の一元管理 |
| | 私用端末の対策 | 端末の限定 |
| | | データの限定 |
| 作業環境のセキュリティ | 自宅での対策 | ブロードバンドルーターのソフトウェア更新 |
| | | ブロードバンドルーターの管理アクセス用パスワード変更 |
| | | 無線LANにおける強固な暗号技術／パスワードの利用 |
| | 外出先での対策 | 不審なアクセスポイントの利用禁止 |
| | | 利用するアクセスポイントの暗号技術の確認 |
| | | 不特定多数がいる環境での情報漏洩の注意 |
| 社内システムのセキュリティ | 社内システムまでの通信に関する対策 | VPNの利用 |
| | | VPNアクセス許容量の確認 |
| | | VPN利用時の多要素認証の利用 |
| | 社内システム自体の対策 | 社内システムのアクセス制御 |
| | | 端末へのデータDL制限 |
| クラウドシステムのセキュリティ | 基本的な対策 | 多要素認証の利用 |
| | | アクセス制御 |
| | | 端末へのデータDL制限 |
| | サービス選定に関わる対策 | 選定基準の策定 |
| | | 推奨されるセキュリティ設定の有効化 |
| 全体に関わるセキュリティ | ログ取得 | |
| | バックアップ取得 | |

いることが多い。その認証を有効化することを忘れないでほしい。また、クラウドサービス側のネットワークは事業者側で管理するため、ネットワーク分離などの対策は利用者側での対策はないと考えてよい。データのダウンロード制御は利用するクラウドサービスに依るところが大きいため、サービス仕様や設定をよく理解し､対策を実施するべきである。その際にはできる限りダウンロード機能や各種操作権限を最小化することが望まれる。

**②　サービス選定に関わる対策**

前述の通り、クラウドサービスは利用者側での管理が少なく運用が楽である反面、事業者側で適切な管理が行われていないと、本稿冒頭での事例のように利用者側が危険にさらされてしまう。そのため、クラウドサービス事業者が十分なセキュリティ対策を実施しているか事前に確認を行うことが望ましい。第三者機関による認証を受けているか、セキュリティ対策が公開されているか、多要素認証

が利用可能か、利用されている暗号化技術は安全か等、確認項目を設定し、それに対応したサービスを選定することを推奨する。経済産業省（※4）やIPA（※5）もクラウドサービスを利用する上でのガイドラインを公開しているのでそのような資料を参照することも有用である。また、クラウドサービスでは機密情報がインターネットから誰でもアクセスできてしまうような誤設定が容易になされてしまう可能性がある。クラウドサービス利用者側でもクラウドサービス事業者が推奨するセキュリティ設定や、インターネット上の各種情報を収集した上で、適切な設定を行うことが求められる。

#### （オ） 全体に関わるセキュリティ

個別要素に関してセキュリティ対策だけでなく、複数の要素に関わる対策についても2点触れておきたい。1点目はログの取得だ。セキュリティ事故発生後の調査の意図もあるが、従業員への牽制の意味でも各種ログを取得し、それを従業員にも周知することが有効である。取得する代表的なログとしては端末における操作ログ、VPN・社内システム・クラウドサービス等の認証／操作ログが挙げられる。2点目は各種システムのバックアップである。テレワークでは通信環境の不具合や端末の故障等で操作中のデータが消失してしまう可能性がある。それらを防ぐためにも、重要な情報、システムは定期的バックアップを取得し、安全に保管しておくことを推奨する。

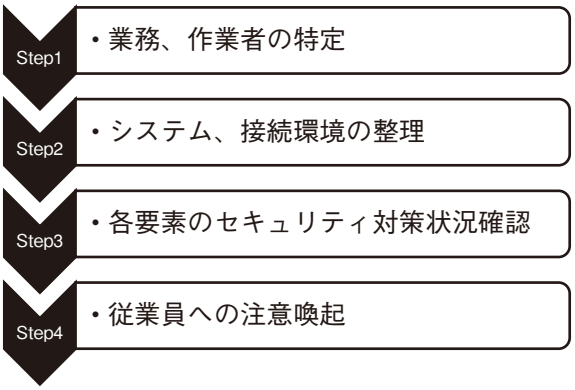
## 3．テレワークにおけるセキュリティ対策の進め方

ここまで述べたように、テレワークに関わるセキュリティ対策は複数の領域に跨り、また多くの考慮が必要となる。これまでテレワークを前提とした環境を整備していなかった場合は、適切な順序、方針で進めないと利用開始までに時間を要してしまう。本章では短期的な対策と、長期的な対策に分けて進め方を整理する。

#### （ア） 短期的対策

いち早くテレワーク業務を開始するための進め方として4つのステップで進めることを提案する。まずは、テレワークで実施したい業務とその作業者を特定する。営業担当者による顧客対応報告なのか、経理担当者による請求書処理業務なのか、優先度の高い業務を抽出する。その上で、それぞれの作業において必要なシステム、およびそれへの接続環境を明確にする。PCによる社内ファイルサーバへのアクセス、スマートフォンによるクラウドカレンダーサービスへのアクセス等、具体的に列挙してみる。そうした上で、第2章で挙げた各対策が適切に実施できているかを確認してみる。これらのステップを踏まえることで対策が必要な対象を最小限に絞り、セキュリティ対応を効率よく実施することがで

（図表４）短期的なセキュリティ対策の進め方




きる。

最後のステップとして実施すべきは従業員に対する注意喚起である。作業環境を従業員に用意してもらう必要があり、また各種対策も従業員自ら行うものがある。また、本稿冒頭でも紹介したように、社会的な不安に乗じた詐欺行為も多く観測されている。そのため、従業員が気を付けるべき事項をまとめ、テレワークを行う従業員に対して周知を実施すべきである。

### （イ） 長期的対策

テレワークを進めていく上で様々なトラブル、要望に直面するはずである。例えば、全員分のノートPCが用意できない、不具合発生時に遠隔でサポートができない等である。テレワークを前提とした業務環境でなければ、そういった問題が出てくることも不思議ではない。今回の新型コロナウイルスへの対応により、従業員側も多様な働き方を望むようになることが予想され、そのようなニーズを業務環境に反映させていくことが企業の競争力につながっていくであろう。これらの状況を踏まえると、IT環境もテレワークに適した形で構築し直すことが望ましい。本節ではそれを進める上でのポイントを４つご紹介したい。

１点目は、接続元環境の確実な確認である。社内ネットワークからのみ業務を行う場合は、大抵はその環境で利用する端末はシステム管理部門が用意したものであり、セキュリティの状況も一定水準以上あるものと考えることができる。一方、今後は様々な場所から様々な種類の端末の接続が予想される。また、私用端末の利用も進むだろう。そうなった場合に、各端末のセキュリティ状況が十分なものか担保できない。そのため、会社が用意するシステムにアクセスする場合には、都度端末のセキュリティ状況を確認する仕組みを導入することが望ましい。また、端末の状況だ

（図表５）長期的な対策を行う上での考慮点

| ポイント１ | ポイント２ | ポイント３ | ポイント４ |
| --- | --- | --- | --- |
| ・接続元環境の確認 | ・業務委託先、派遣社員のテレワーク利用 | ・従業員教育 | ・クラウドサービスへの移行 |

けではなく、その作業者が本当に作業員当人であるかの確認も必要となる。オフィスでの業務では、作業者がその場所に入館するというプロセスがあり、これにより作業者本人であることを確認することが可能だ。しかし、テレワークではシステム等を操作している作業者が本人であるかを確認するのが容易ではない。従って、第２章で説明した多要素認証を用いて、作業者本人であることを強固に確認することが必要となる。さらなる考慮が必要となる点は、多種多様なクラウドサービスへの一元的なアクセス制御である。近年、「ゼロトラスト」という概念が提唱されこのような施策の実現方法が活発に議論されており、「ゼロトラスト」環境を実現するためのソリューションも多数提案されているが、今回は紙面の関係上割愛させていただく。

２点目は、業務委託や派遣社員によるテレワークも前提とした環境構築である。多様な働き方が進む社会では、社員のみによる業務遂行も限界がある。業務委託や派遣社員等社外のリソースを活用した上での企業活動を構築していくことが求められる。ただし、あらゆる業務内容や情報への扱いを可能とするのではなく、業務の重要度や情報の機密性を考慮した上で、適切な役割分担を行うことが必要である。

３点目は、従業員への教育である。テレワークを前提とした環境を構築したとしても、作業環境の注意等従業員が担うべき対策は存在し続ける。また、周囲に上司、同僚の目がなくなるため、注意が散漫になり、また不正を起こしやすい心理状態になることも予想される。そのため、定期的にセキュリティに関する情報を発信する、eラーニングの形でセキュリティ対策を周知する等の活動を行うことを推奨する。

最後は、クラウドサービスへの移行である。クラウドサービスのセキュリティの節でも述べたが、自社でのシステム管理は機器の物理的管理が必要となり、また柔軟な機能拡張も困難である。自社管理を前提として社内システムが構築されている場合には容易な作業ではないが、利便性、コスト、セキュリティを

考慮した上で、社内システムのクラウドサービスへの移行を検討すべきである。

## 4．経営層の役割

ここまで従業員、ないしシステム管理者が考慮すべきセキュリティ対策、およびその進め方を整理してきた。最後に、経営層が実施すべきこともまとめておきたい。

テレワークを企業が推進するにあたり考慮しなければならない点はセキュリティに留まらない。まず考えられるのは人事・労務面の整備である。就業規則の改訂、業務時間の遠隔管理、人事評価制度の再検討、通信費等の自宅作業環境の費用負担等考慮する点が多い。次に、紙や押印を基本とした社内外プロセスの変更も必要である。新型コロナウイルスによる在宅勤務中でも押印のためだけに出社する例も聞かれる。また、業務面でも各従業員の成果管理がしにくくなることが考えられる。管理者としてはこれまで以上に作業や成果を明確に定義し、指示を行うことが求められてくるだろう。

上記のように、テレワークの導入には、人事、労務、経理、総務、情報システム、各事業部門等様々な部門を巻き込みながら進める必要がある。しかし、各部署の元々の存在目的と照らして、特定の部署が単体でテレワークを積極的に推進することは難しいと思われる。そのため、経営層としてはテレワーク推進の旗振りを担い、適切なリソースを配置した上で、進捗をウォッチしていくことが重要であると考えられる。

テレワークは事業継続の観点のみならず、コスト削減、有能な人材の確保、働き方改革、生産性向上等企業にとって有益な点も多く、経営層を中心に今後企業一丸となり進めていくことが求められる。

**【参考文献】**


（※1） 総務省「情報通信白書令和元年版」https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd124210.html

（※2） パーソル総合研究所「緊急事態宣言（7都府県）後のテレワークの実態について、全国2.5万人規模の調査結果を発表」https://rc.persol-group.co.jp/news/202004170001.html

（※3） トレンドマイクロ「『新型コロナウイルス（COVID－19）』便乗脅威の最新情報」https://blog.trendmicro.co.jp/archives/24414

（※4） 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版」https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

（※5） IPA「クラウドサービス安全利用のすすめ」https://www.ipa.go.jp/files/000011594.pdf