2020 年 4 月 14 日

テレワークを実施する際にセキュリティ上留意すべき点について

新型コロナウィルス感染症(COVID-19)対応に伴うテレワーク実施に際して、セキュリティ上留意すべき点について政府機関等、重要インフラ事業者等それぞれに向けて注意喚起を発出するとともに、国民向けにも周知しています。

新型コロナウィルス感染症(COVID-19)の影響で、テレワークの活用が急速に進んでいます。

内閣サイバーセキュリティセンター(NISC)では、政府機関等、重要インフラ事業者がテレワークを導入する際のセキュリティ上留意すべき点について注意喚起を行うとともに、国民一般向けにも注意すべき基本的なポイントの周知をしています。

テレワークの導入の必要性が高まっている中、テレワークの導入方法で迷われている方の参考となるような内容となっておりますので、周知対象の機関等や事業者のみならず、広く活用していただけるよう公開するものです。

資料１　政府機関等におけるテレワークにかかる留意事項（注意喚起）
資料２　重要インフラ事業者等におけるテレワークにかかる留意事項（注意喚起）
資料３　テレワーク実施者の方へ　～あなたのセキュリティは大丈夫ですか？～
資料４　テレワークにかかる留意事項（情報共有）
※　資料４における別紙１及び別紙２は、上記、資料１及び資料２と同一のものになります。

本件に関する連絡先
内閣サイバーセキュリティセンター
電話番号　03-5253-2111（代表）
資料１について　政府機関総合対策グループ
資料２について　重要インフラ第２グループ
資料３について　基本戦略第１グループ
資料４について　政府機関総合対策グループ及び重要インフラ第２グループ

資料１

2020 年 4 月 9 日

内閣サイバーセキュリティセンター
政府機関総合対策グループ

政府機関等におけるテレワークにかかる留意事項(注意喚起)

新型コロナウイルス感染症(COVID-19)の対応として、テレワークを採用する組織が増加しています。かかる状況を踏まえ、政府機関等がテレワークを導入する場合、セキュリティ上のリスクを把握し、適切に管理すべく注意喚起するものです。

1. 概要

2020 年 2 月 25 日、新型コロナウイルス感染症(COVID-19)の対応として、新型コロナウイルス感染症対策本部は「新型コロナウイルス感染症対策の基本方針」を発表しました。基本方針では、休暇取得の推奨や時差出勤の推進と併せて、テレワークの推進が呼びかけられており、テレワークの積極的な導入が進んでいます。政府機関等においてテレワークを導入する際には、とりわけテレワーク実施に伴うセキュリティ上のリスクを適切に把握し、管理していくことが必要です。

2. テレワーク開始に向けた事前準備

テレワークの開始にあたっては、導入目的の明確化、対象範囲の決定、導入計画の策定、職員への説明等を行い、必要に応じ、セキュリティポリシーの改訂、それに伴う各種ルールの策定、ICT 環境の確認・整備を行うことが必要です。

なお、テレワーク導入によるベネフィットとリスクのバランスについては、今回は緊急時の措置であることを考慮することも重要です。

検討においては、政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）（平成 30 年 7 月、サイバーセキュリティ戦略本部、内閣官房 内閣サイバーセキュリティセンター)[1]を確認の上、「テレワークセキュリティガイドライン 第 4 版(2018 年 4 月、総務省)[2]」において記載されていますテレワークセキュリティの保全に関して実施すべき事項も参考として活用ください。

(1) セキュリティポリシー及びルールの整備

---

[1] *サイバーセキュリティ戦略本部、内閣官房 内閣サイバーセキュリティセンター 政府機関等の情報セキュリティ対策のための統一基準群(平成 30 年度版)(平成 30 年 7 月 25 日)、https://www.nisc.go.jp/active/general/kijun30.html*

[2] *総務省「テレワークセキュリティガイドライン(2018/4/13)」、https://www.soumu.go.jp/main_content/000545372.pdf*

各機関において定めている「情報セキュリティポリシー」を踏まえ、導入しようとするテレワーク計画に照らし、PC 端末や紙情報の持ち出しルール等、テレワーク実施時のルールについて、不足分を整備します。

(2) ICT 環境の準備

テレワークにかかる ICT 環境は、「情報システム担当者のためのテレワーク導入手順書(2016 年 3 月、総務省)[3]」や、「テレワーク関連ツール一覧(2019 年 11 月、一般社団法人日本テレワーク協会)[4]」等を参考に、各機関の実態に合わせて検討します。

3. 留意事項

(1) VPN

外部からインターネットで組織と通信する際の安全策として、Virtual Private Network(VPN)を経由して、組織のネットワークに接続し、業務を実施するケースが存在します。VPN は完全ではないとの前提の下、迅速なパッチ適用を行うようにすること、加えて多要素認証の採用の検討が必要です。

(2) メール

テレワークの際に使用するメールについて、各機関が定めている「情報セキュリティポリシー」で、フリーメールや商用メールの制限がどのようになっているか、改めて確認する必要があります。また、各機関が用意した在宅勤務用のメールであっても、セキュリティ対策を一層高めるため、取り扱うデータの内容に応じて、PGP 暗号化[5]や S/MIME[6]の活用による対策が考えられます。特に PGP 暗号化は導入が容易であることから推奨します。

(3) リモートデスクトップ(RDP)

検索エンジンサービス「Shodan[7]」は、同サービスのブログ上で、Remote Desktop Protocol(RDP)をインターネット上に公開している機器が世界的に 3 月に増加している[8]としていますが、テレワーク等により増加したものと思われます。この中には、2019 年に発見された Windows の RDP サービスの深刻な脆弱性(CVE-2019-0708[通称:BlueKeep]、CVE-2019-1181/CVE-2019-1182)[通称:DejaBlue])のパッチを適用していないものもあり、留意する必要があります。各機関において、意図せず RDP ポート

---

[3] *総務省「情報システム担当者のためのテレワーク導入手順書(2016/3)」、https://www.soumu.go.jp/main_content/000668432.pdf*

[4] *日本テレワーク協会「テレワーク関連ツール一覧(2019/11/1)」、https://japan-telework.or.jp/wordpress/wp-content/uploads/2019/11/Tool-list-V4.1-20191101.pdf*

[5] *PGP(Pretty Good Privacy)は公開鍵暗号技術を利用した暗号化ソフトウェア。PGP を利用することで、メール本文やメールの添付ファイルを暗号化することができる。PGP の別実装である GnuPG(GNU Privacy Guard)は、GPG4Win(https://www.gpg4win.org/download.html)等が使用できる。*

[6] *S/MIME(Secure / Multipurpose Internet Mail Extensions)を活用することで、メール本文やメールの添付ファイルを暗号化することができる。市販のメールソフトに組み込まれていることもある。*

[7] *インターネット上の検索エンジン。Shodan を使用すると、認証が弱い機器や古いバージョンのまま運用されている機器など、セキュリティ上問題がある機器を見つけることができる。*

[8] *Shodan「Trends in Internet Exposure」、https://blog.shodan.io/trends-in-internet-exposure/*

[9]を公開している場合も考えられることから、セキュリティインシデントを防止するため、PDP ポート開放状況を確認する必要があります。

(4) 遠隔会議システム

テレワーク等で遠隔会議システムの利用が拡大しています。遠隔会議システムのうち、Zoom Video Communications 社の「Zoom」には、セキュリティ上の問題点があることを発表しました(文末「Zoom の脆弱性対策について（IPA)」参照)。

なお、「Zoom」に限らず、外部サービスである「遠隔会議システム」は外部ネットワークを使うこととなるため、潜在するリスクについて、導入前に十分調査し、各機関が許容するリスクに応じた運用方法を定めること、運用中にリスクが顕在化した際の対策をあらかじめ検討しておくことが必要です。

(5) 機密情報の保護

Twitter やインスタグラム等の SNS に投稿したテレワークの写真に、機密性の高い文書や業務情報が映り込む事例が発生しており、テレワーク実施時には特に不用意な機密情報の漏洩に留意する必要があります。また、遠隔会議を実施する際に、機密性の高い情報がカメラの背景に映り込んだり、業務情報がマイクから流れたりすることで、不用意な情報漏洩につながる蓋然性があることから、遠隔会議の実施場所や設定に配慮する必要があります。

(6) その他

① 堅牢なパスワードや多要素認証の使用
システムで用いるパスワードは他者から容易に推測されない堅牢なものとし、多要素認証が使用できる場合は活用することを検討します。

② 端末や機器のアップデート
OS やソフトウェア、アプリ、機器の脆弱性を確認したうえで、必要に応じてアップデートする等、システムの状況に応じた管理策を検討します。

③ 不審なメールへの注意
業務を装ったメールや新型コロナウイルス感染症(COVID-19)をテーマにした不審なメール等に注意し、身に覚えのないメールの添付ファイルや URL はクリックしないように組織全体に注意喚起が必要です。

④ 端末の盗難や紛失への注意
ノート PC やスマートフォン、USB メモリ等は紛失のリスクもあるため、紛失を防止するための対策に加え、暗号化の実施の検討や、個人の端末を利用する場合のセキュリティ対策を考慮します。

⑤ 無線 LAN のセキュリティ設定の確認
無線 LAN(Wi-Fi)のセキュリティ設定に留意します。

---

9 デフォルトでは、RDP は port:3389 を使用。

⑥ インシデント発生時の連絡方法の確認

テレワークによるセキュリティインシデント発生に備え、あらかじめインシデント発生時の対処方法、連絡方法を確認しておきます。

参考

- Zoom の脆弱性対策について（IPA）
  https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html
- 複数の SSL VPN 製品の脆弱性に関する注意喚起（JPCERT/CC）
  https://www.jpcert.or.jp/at/2019/at190033.html
- テレワーク実施者の方へ～あなたのセキュリティは大丈夫ですか？～(NISC)
  https://www.nisc.go.jp/security-site/telework/index.html

（参考）政府機関等の情報セキュリティ対策のための統一基準＜抜粋＞

※　次にあげる統一基準例は主なものであり、そのほかの統一基準の関連個所についても確認頂くようお願いします。

遵守事項

4.1.2　約款による外部サービスの利用

(1) 約款による外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ｱ)約款による外部サービスを利用してよい業務の範囲

(ｲ)業務に利用できる約款による外部サービス

(ｳ)利用手続及び運用手順

(b) 情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。

(2) 約款による外部サービスの利用における対策の実施

(a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

遵守事項

7.1.1　端末

(1) 端末の導入時の対策

(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

(4) 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末の導入及び利用時の対策

(a) 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末について、以下の安全管理措置に関する規定を整備すること。

(ｱ)盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置

(イ)機関等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置

(b) 情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定めること。

(c) 次の各号に掲げる責任者は、職員等が当該各号に定める端末を用いて要機密情報を取り扱う場合は、当該端末について(a)(ア)の安全管理措置を講ずること。

(ア)情報システムセキュリティ責任者　機関等が支給する端末（要管理対策区域外で使用する場合に限る）

(イ)端末管理責任者　機関等支給以外の端末

(d) 端末管理責任者は、要機密情報を取り扱う機関等支給以外の端末について、前項の規定にかかわらず(a)(ア)に定める安全管理措置のうち自ら講ずることができないもの、及び(a)(イ)に定める安全管理措置を職員等に講じさせること。

(e) 職員等は、要機密情報を取り扱う機関等支給以外の端末について、前項において(a)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び(a)(イ)に定める安全管理措置を講ずること。

遵守事項

7.3.1　通信回線

(4) リモートアクセス環境導入時の対策

(a) 情報システムセキュリティ責任者は、職員等の業務遂行を目的としたリモートアクセス環境を、機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。

遵守事項

8.1.1　情報システムの利用

(3) 情報システムの利用時の基本的対策

(a) 職員等は、業務の遂行以外の目的で情報システムを利用しないこと。

(b) 職員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機関等の情報システムを接続しないこと。

(c) 職員等は、機関等内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。

(d) 職員等は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。

(e) 職員等は、接続が許可されていない機器等を情報システムに接続しないこと。

(f) 職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

(g) 職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。

(h) 職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(ア)機関等が支給する端末（要管理対策区域外で使用する場合に限る）　機密性３情報、要保全情報又は要安定情報

(イ)機関等支給以外の端末　要保護情報

(i) 職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、定められた安全管理措置を講ずること。

(j) 職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、課室情報セキュリティ責任者の許可を得ること。

(k) 職員等は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、課室情報セキュリティ責任者の許可を得ること。

資料２

2020 年 4 月 7 日

内閣サイバーセキュリティセンター
重要インフラグループ

重要インフラ事業者等におけるテレワークにかかる留意事項(注意喚起)

新型コロナウイルス感染症(COVID-19)の対応として、テレワークを採用する組織が増加しています。かかる状況を踏まえ、重要インフラ事業者等がテレワークを導入する場合、セキュリティ上のリスクを把握し、適切に管理すべく注意喚起するものです。

1. 概要

2020 年 2 月 25 日、新型コロナウイルス感染症(COVID-19)の対応として、新型コロナウイルス感染症対策本部は「新型コロナウイルス感染症対策の基本方針」を発表しました。基本方針では、休暇取得の推奨や時差出勤の推進と併せて、テレワークの推進が呼びかけられており、テレワークの積極的な導入が進んでいます。重要インフラ分野においてテレワークを導入する際には、とりわけテレワーク実施に伴うセキュリティ上のリスクを適切に把握し、管理していくことが必要です。

2. テレワーク開始に向けた事前準備

テレワークの開始にあたっては、導入目的の明確化、対象範囲の決定、導入計画の策定、従業員説明等を行い、必要に応じ、セキュリティポリシーの改訂、それに伴う各種ルールの策定、ICT 環境の確認・整備を行うことが必要です。

なお、テレワーク導入によるベネフィットとリスクのバランスについては、今回は緊急時の措置であることを考慮することも重要です。

検討においては、「テレワークセキュリティガイドライン 第 4 版(2018 年 4 月、総務省)[1]」において、経営者、システム管理者、テレワーク勤務者それぞれの立場からテレワークセキュリティの保全に関して実施すべき事項を記載しており、自組織に相応しいセキュリティ対策の検討の際に活用できます。

(1) セキュリティポリシー及びルールの整備

自組織が定めている「情報セキュリティポリシー」を踏まえ、導入しようとするテレワーク計画に照らし、PC 端末や紙情報の持ち出しルール等、テレワーク実施時の労務管理ルールについて、不足分を整備します。

[1] *総務省「テレワークセキュリティガイドライン(2018/4/13)」、https://www.soumu.go.jp/main_content/000545372.pdf*

(2) ICT 環境の準備

テレワークにかかる ICT 環境は、「情報システム担当者のためのテレワーク導入手順書(2016 年 3 月、総務省)[2]」や、「テレワーク関連ツール一覧(2019 年 11 月、一般社団法人日本テレワーク協会)[3]」等を参考に、自組織の実態に合わせて検討します。

3. 留意事項

(1) VPN

外部からインターネットで組織と通信する際の安全策として、Virtual Private Network(VPN)を経由して、組織のネットワークに接続し、業務を実施するケースが存在します。VPN は完全ではないとの前提の下、迅速なパッチ適用を行うようにすること、加えて多要素認証の採用の検討が必要です。

(2) メール

テレワークの際に使用するメールについて、自組織が定めている「情報セキュリティポリシー」で、フリーメールや商用メールの制限がどのようになっているか、改めて確認する必要があります。また、自組織が用意した在宅勤務用のメールであっても、セキュリティ対策を一層高めるため、取り扱うデータの内容に応じて、PGP 暗号化[4]や S/MIME[5]の活用による対策が考えられます。特に PGP 暗号化は導入が容易であることから推奨します。

(3) リモートデスクトップ(RDP)

検索エンジンサービス「Shodan[6]」は、同サービスのブログ上で、Remote Desktop Protocol(RDP)をインターネット上に公開している機器が世界的に 3 月に増加している[7]としていますが、テレワーク等により増加したものと思われます。この中には、2019 年に発見された Windows の RDP サービスの深刻な脆弱性(CVE-2019-0708[通称:BlueKeep]、CVE-2019-1181/CVE-2019-1182)[通称:DejaBlue])のパッチを適用していないものもあり、留意する必要があります。組織において、意図せず RDP ポート[8]を公開している場合も考えられることから、セキュリティインシデントを防止するため、PDP ポート開放状況を確認する必要があります。

---

[2] *総務省「情報システム担当者のためのテレワーク導入手順書(2016/3)」、https://www.soumu.go.jp/main_content/000668432.pdf*

[3] *日本テレワーク協会「テレワーク関連ツール一覧(2019/11/1)」、https://japan-telework.or.jp/wordpress/wp-content/uploads/2019/11/Tool-list-V4.1-20191101.pdf*

[4] *PGP(Pretty Good Privacy)は公開鍵暗号技術を利用した暗号化ソフトウェア。PGP を利用することで、メール本文やメールの添付ファイルを暗号化することができる。PGP の別実装である GnuPG(GNU Privacy Guard)は、GPG4Win(https://www.gpg4win.org/download.html)等が使用できる。*

[5] *S/MIME(Secure / Multipurpose Internet Mail Extensions)を活用することで、メール本文やメールの添付ファイルを暗号化することができる。市販のメールソフトに組み込まれていることもある。*

[6] *インターネット上の検索エンジン。Shodan を使用すると、認証が弱い機器や古いバージョンのまま運用されている機器など、セキュリティ上問題がある機器を見つけることができる。*

[7] *Shodan「Trends in Internet Exposure」、https://blog.shodan.io/trends-in-internet-exposure/*

[8] *デフォルトでは、RDP は port:3389 を使用。*

(4) 遠隔会議システム

テレワーク等で遠隔会議システムの利用が拡大しています。遠隔会議システムのうち、Zoom Video Communications 社の「Zoom」には、セキュリティ上の問題点があることを発表しました(文末「Zoom の脆弱性対策について（IPA)」参照)。

なお、「Zoom」に限らず、外部サービスである「遠隔会議システム」は外部ネットワークを使うこととなるため、潜在するリスクについて、導入前に十分調査し、自組織が許容するリスクに応じた運用方法を定めること、運用中にリスクが顕在化した際の対策をあらかじめ検討しておくことが必要です。

(5) 機密情報の保護

Twitter やインスタグラム等の SNS に投稿したテレワークの写真に、機密性の高い文書や業務情報が映り込む事例が発生しており、テレワーク実施時には特に不用意な機密情報の漏洩に留意する必要があります。また、遠隔会議を実施する際に、機密性の高い情報がカメラの背景に映り込んだり、業務情報がマイクから流れたりすることで、不用意な情報漏洩につながる蓋然性があることから、遠隔会議の実施場所や設定に配慮する必要があります。

(6) その他

① 堅牢なパスワードや多要素認証の使用
システムで用いるパスワードは他社から容易に推測されない堅牢なものとし、多要素認証が使用できる場合は活用することを検討します。

② 端末や機器のアップデート
OS やソフトウェア、アプリ、機器の脆弱性を確認したうえで、必要に応じてアップデートする等、システムの状況に応じた管理策を検討します。

③ 不審なメールへの注意
業務を装ったメールや新型コロナウイルス感染症(COVID-19)をテーマにした不審なメール等に注意し、身に覚えのないメールの添付ファイルや URL はクリックしないように組織全体に注意喚起が必要です。

④ 端末の盗難や紛失への注意
ノート PC やスマートフォン、USB メモリ等は紛失のリスクもあるため、紛失を防止するための対策に加え、暗号化の実施の検討や、個人の端末を利用する場合のセキュリティ対策を考慮します。

⑤ 無線 LAN のセキュリティ設定の確認
無線 LAN(Wi-Fi)のセキュリティ設定に留意します。

⑥ インシデント発生時の連絡方法の確認
テレワークによるセキュリティインシデント発生に備え、あらかじめインシデント発生時の対処方法、連絡方法を確認しておく。

参考

・ Zoom の脆弱性対策について （IPA）
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

・ 複数の SSL VPN 製品の脆弱性に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2019/at190033.html

・ テレワーク実施者の方へ～あなたのセキュリティは大丈夫ですか？～(NISC)
https://www.nisc.go.jp/security-site/telework/index.html

資料３

テレワーク実施者の方へ
～あなたのセキュリティは大丈夫ですか？～

オフィスを離れ自宅や公共のスペースなど、場所や通勤等にとらわれず働くことを可能にするテレワーク。実施が増えている一方、オフィス環境と異なったり、攻撃者に狙われたりして、思わぬリスクに晒される可能性がありますので、いままで以上に各自が求められるセキュリティ対策を実践することが重要です。

テレワークを実施される方は、お使いになるシステムに求められる要件や以下の注意すべきポイントに気を付けて、仕事上の情報漏えい等や自らの端末・機器等を守る意識を高めましょう。

●　複雑なパスワードや多要素認証を使いましょう

※お使いになるシステムで用いるパスワードは複雑にし、貴重品のように管理しましょう。
※多要素認証が利用できる場合は、是非活用しましょう。USB キー等は絶対になくさないようにしましょう。

●　端末や機器を最新にアップデートしましょう

※OS やソフト、アプリ、機器をアップデートしてセキュリティの穴をふさぎましょう。セキュリティソフトも忘れずに。社内システムの場合は規程に従いましょう。
※古いルータなど、初期管理用パスワードが弱いことがあるため、しっかりしたものか確認しましょう。

●　業務を装ったりするメールや不審なメールに要注意

※攻撃者は心の隙や不安な心理をついてきます。添付ファイルは安易に開かないように注意しましょう。
※メールからのリンク先は偽サイトの可能性が。不用意にクリックしたり ID/パスワードを入力したりしないようにしましょう。

●　実は丸見え！？通信は暗号化して安心

※公共の場所での通信は、盗聴されるリスクも高まります。VPN 接続の機能などを活用して通信路を暗号化しましょう。
※メールの送受信やブラウザからの閲覧、チャットでの会話等でも、機微な情報のやり取りをしないことや、内容を暗号化するなど、盗聴のリスクを踏まえた行動をとりましょう。

●　端末の盗難、紛失に要注意

※持ち運びしやすいノート PC やスマホ、USB メモリ等は盗難、紛失のリスクも。万が一に備えてデータは暗号化しましょう。

※個人の端末を利用（BYOD）する場合は、端末内で重要なデータを扱わない残さない運用が重要。利用可否や運用ルールについて社内規程の確認を忘れずに。

●　そこは社内じゃありません

※周りは知らない人だらけ。他者からの盗み見（ショルダーハッキング）や大声での電話会議による情報漏えいに注意しましょう。

※その無線 LAN（Wi-Fi）は本当に大丈夫ですか？セキュリティ設定が甘かったり、偽の無線 LAN の可能性も。利用する際は十分注意しましょう。

●　何かあったときの連絡手順を確認

※どんなに警戒していても、いつ何が起こるかわかりません。インシデント発生時に備えて連絡方法を事前に確認しましょう。

※インシデントに気づいたら迷わず連絡。インシデント発生時の対応は速やかに。

上記のほか、総務省「テレワークセキュリティガイドライン 第４版」もご覧ください。
（URL）https://www.soumu.go.jp/main_content/000545372.pdf

また、VPN やデータの暗号化等の解説については、内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブック」にも記載がありますのでご参照ください。
（URL）https://www.nisc.go.jp/security-site/handbook/index.html

掲載：令和２年３月２７日
更新：令和２年４月３日（２・３・５番目の内容につき初期パスワードや添付ファイルへの注意喚起等を追記及び文言を修正）

掲載場所：NISC ホームページ
https://www.nisc.go.jp/security-site/telework/index.html

資料４

事　務　連　絡
令和2年4月13日

サイバーセキュリティ対策推進専任審議官等会議
構成員及びオブザーバー　各位

内閣官房内閣サイバーセキュリティセンター副センター長

テレワークにかかる留意事項（情報共有）

新型コロナウィルス感染症（COVID-19）の対応として、テレワークを採用する組織が増加していると考えられる状況を踏まえまして、内閣サイバーセキュリティセンターでは、政府機関等、重要インフラ事業者等がテレワークを導入する場合に留意すべき事項を別紙1及び別紙2のとおりまとめ、それぞれ所定の情報共有体制を通じ周知しております。

これらについては、周知対象の機関等や事業者等にとどまらず、広く活用可能と考えられる内容となっておりますので、各府省庁におかれては、所管の事業者等に対して、テレワークに関する注意喚起等を行う場合の参考にしてください。