2020 年 6 月 11 日

テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について

内閣サイバーセキュリティセンターは、新しい生活様式の実践のために、テレワーク等への継続的な取組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、重要インフラ所管省庁それぞれに向けて注意喚起等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、テレワークや遠隔会議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では、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公表を行いました。

これまで積極的なテレワークや遠隔会議システムの活用等に取り組まれてきていると思われますが、緊急事態措置が終了した後においても新しい生活様式の実践に向けて、こうした取組を継続的に行っていくため、情報セキュリティ上留意すべき点について、政府機関等、重要インフラ所管省庁それぞれに向けて注意喚起、事務連絡を発出するとともに、国民向けにも周知しています。

様々な分野で、テレワーク等の取組が定着していく中、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内容となっておりますので、これらについて公開することにしました。なお国民向けについては Facebook 公式アカウント及び LINE 公式アカウントにて参考となる情報※を公開しております。

資料１ テレワーク等への継続的な取組に際しての留意事項（注意喚起）

資料２ テレワーク等への継続的な取組に際しての留意事項

※「セキュリティの在り方もこの機会に組織として考えよう」（2020 年 5 月 21 日）

https://www.facebook.com/nisc.jp/

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１グループ

資料１

2020 年 6 月 11 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

テレワーク等への継続的な取組に際しての留意事項(注意喚起)

新型コロナウイルス感染症(COVID-19)の対応として、政府機関等においてもこれまで積極的なテレワークや遠隔会議システムの活用等に取り組まれたものと思われますが、緊急事態措置が終了した後においてもこうした取組を継続的に行っていくために、情報セキュリティの観点から留意すべき点についてお知らせいたします。

なお、企業向けとして特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）より「緊急事態宣言解除後のセキュリティ・チェックリスト」も公表されていますので、参考としてお知らせいたします。

https://www.jnsa.org/telework_support/telework_security/index.html

１．情報セキュリティリスクの再評価

今般のテレワークにおいて進められた業務のうち、情報セキュリティ対策に不安が生じたものや当初テレワークの計画を想定していた時からテレワークの利用状況に変更があったもの（取扱業務量の増加、利用者の増加、利用対象者の制限範囲拡大、対象業務の制限範囲拡大、機能追加等）については、改めてリスク評価を行うことが重要です。リスクが高いと判断された場合には、テレワークの対象業務の見直しや必要に応じた追加的な対策（技術的な措置の付加、実施条件の付加等）の検討を行い、改めてテレワークの可否に係る考え方を整理した上で、テレワークで行える業務の計画作りに反映していくことが有効であると考えられます。

２．各機関における情報セキュリティ関連規程の確認と必要に応じた改定

今般の経験に照らして、各機関で定められた情報セキュリティ関連規程の実効性を確認することが重要です。例えば、リスク評価を踏まえて追加的な対策を決定した際には情報セキュリティ関連規程に追記することが重要です。また、この間一時的・緊急的な対応を図るために例外措置を採用したケースなどにおいて、改めてその措置の有効性が確認できる場合には、必要なセキュリティ措置を伴った上で、例外措置ではなく普段の運用の一形態として位置づけることも有効であると考えられます。

３．利用端末・関連機器等の確認

（１）支給端末の利用について

機関からの支給端末の利用に関し、組織外への持ち出しに係る管理等が円滑かつ適切に進められていたかについて確認することが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認することも重要です。必要に応じて手続きや対策の見直しを行ったり、支給台数が業務量に十分に対応していない場合などには可能な導入手当てや対策の検討を行ったりすることが有効であると考えられます。

（２）支給外端末の利用について

支給外端末の利用に関し、利用状況（情報の格付けや取扱制限、対象業務、接続する機関等内通信回線、情報システム等）や必要に応じた例外措置等の手続きの実施について確認することが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認することも重要です。必要に応じて手続きや対策の見直しを行ったり、支給外端末に代わるような支給端末の導入の検討を行ったりすることも有効であると考えられます。

なお、要機密情報を取り扱った場合、必要がなくなる都度当該情報を消去し、支給外端末の利用終了後速やかに抹消するなど、情報漏えい対策を行うことが重要です。

（３）インターネット回線や公衆通信回線等の機関等外通信回線の利用について

テレワークの実施においては、インターネット回線や公衆通信回線等の機関等外通信回線から機関等内通信回線及び当該機関等内通信回線へ接続されている情報システムへ接続されることから、機関等内通信回線及び当該機関等内通信回線へ接続されている情報システムの情報セキュリティを確保するための措置を講ずることが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けていないか等について確認することも重要です。必要に応じて手続きや対策の見直しを行うことが有効であると考えられます。

４．遠隔会議システムの利用状況の確認

これまでに内閣サイバーセキュリティセンターより遠隔会議システムについての注意喚起を発出いたしました（令和２年４月３日付、４月９日付（部分））。

遠隔会議システムについては、省庁内で統一的に導入しているシステム以外に、部局単位で導入しているシステムもあるため、省庁内の導入・運用状況を把握することが重要です。この他、外部委託先や外部の組織・個人との打ち合わせや会議において、外部委託先や外部の組織・個人が提供する遠隔会議システムを利用する場合が考えられるため、省庁内の利用状況を把握することが重要です。

これまでの遠隔会議システムに関する省庁内の導入・運用状況及び外部委託先や外部の組織・個人が提供する遠隔会議システムの利用状況について確認し、どのような情報の取り扱いまで利用可能とするかを含め必要なセキュリティ対応が実施されているか

について確認することが重要です。安全性を確保しつつ、有効活用を行うために、必要な情報セキュリティ関連規定が整備されることが求められます。

５．情報セキュリティ対策推進体制の関与

上記の取組においては、各機関における情報セキュリティ対策推進体制が積極的に関わり、情報セキュリティ関連規程との整合性や技術的な側面について、確認することが求められます。

（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６月 10 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

テレワーク等への継続的な取組に際しての留意事項

新型コロナウイルス感染症(COVID-19)の対応として、重要インフラ事業者等においてもこれまで積極的なテレワークや遠隔会議システムの活用等に取り組まれたものと思われます。
４月７日付けで、テレワークにかかる留意事項を重要インフラ事業者等宛に注意喚起しましたが、緊急事態措置が終了した後においてもこうした取組を継続的に行っていくために、情報セキュリティの観点から留意すべき点についてお知らせいたします。

１．情報セキュリティリスクの再評価

今般のテレワークにおいて進められた業務のうち、情報セキュリティ対策に不安が生じたものや当初テレワークの計画を想定していた時からテレワークの利用状況に変更があったもの（取扱業務量の増加、利用者の増加、利用対象者の制限範囲拡大、対象業務の制限範囲拡大、機能追加等）については、改めてリスク評価を行うことが重要です。リスクが高いと判断された場合には、テレワークの対象業務の見直しや追加的な対策の検討を行い、今後の業務遂行において手続き、規程等に反映していくことが必要です。

２．組織におけるポリシーの確認と必要に応じた改定

今般の経験に照らして、各組織で定められたポリシーの実効性を確認することが重要です。例えば、リスク評価を踏まえて追加的な対策を決定した際にはポリシーに追記することが重要です。また、この間一時的・緊急的な対応を図るために例外措置を採用したケース等において、改めてその措置の有効性が確認できる場合には、必要なセキュリティ措置を伴った上で、例外措置ではなく普段の運用の一形態として位置づけることが必要です。

３．利用端末・関連機器等の確認

（１）支給端末の利用について

組織からの支給端末の利用に関し、組織外への持ち出しに係る管理等が円滑かつ適切に進められていたかについて確認することが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認することも重要です。適宜、手続きや対策の見直しを行うことや、支給台数が業務量に十分に対応していない場合等には、支給端末の追加導入の検討を行うことが必要です。

（２）支給外端末の利用について

支給外端末の利用に関し、利用状況（情報の格付けや取扱制限、対象業務、接続する組織内通信回線、情報システム等）や必要に応じた例外措置等の手続きの実施について確認することが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認することも重要です。適宜手続きや対策の見直しを行うことや、支給外端末に代わるような支給端末の導入の検討を行うことが必要です。

なお、要機密情報を取り扱った場合、必要がなくなる都度当該情報を消去し、支給外端末の利用終了後速やかに抹消する等、情報漏えい対策を行うことが重要です。

（３）インターネット回線や公衆通信回線等の組織外通信回線の利用について

テレワークの実施においては、インターネット回線や公衆通信回線等の組織外通信回線から組織内通信回線及び当該組織内通信回線へ接続されている情報システムへ接続されることから、組織内通信回線及び当該組織内通信回線へ接続されている情報システムの情報セキュリティを確保するための措置を講ずることが重要です。また、関連する OS やソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認し、適宜手続きや対策の見直しを行うことが必要です。

４．遠隔会議システムの利用状況の確認

テレワークの実施にともない遠隔会議システムの利用が拡大しています。外部サービスである「遠隔会議システム」については、外部ネットワークを使うこととなるため、組織での導入・運用状況及び外部委託先や外部の組織・個人が提供する遠隔会議システムの利用状況について確認し、必要なセキュリティ対応が実施されているかについて確認することが重要です。また、遠隔会議システムにおいて、どのような情報の取り扱いまで利用可能とするかを含め、安全性を確保しつつ、有効活用を行うために、必要なポリシーを整備することが重要です。

５．情報セキュリティ対策推進部署の関与

上記の取組においては、組織における情報セキュリティ対策を推進する役割を担う部署が積極的に関わり、情報セキュリティ関連規程との整合性や技術的な側面について、確認することが重要です。

なお、昨日発行の NISC 重要インフラニュースレター(2020 年 6 月 9 日発行 第 263 号)にも掲載（1.(2)緊急事態宣言解除後のセキュリティ・チェックリスト(JNSA)(05/20)）していますが、企業向けとして特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）より「緊急事態宣言解除後のセキュリティ・チェックリスト」も公表されていますので、参考としてお知らせいたします。

https://www.jnsa.org/telework_support/telework_security/index.html