○政府機関等の情報セキュリティ対策のための統一基準（案）　新旧対照表

改定案	現行
政府機関等のサイバーセキュリティ対策のための統一基準 （令和３年度版） 令和　年　月　日 サイバーセキュリティ戦略本部	政府機関等の情報セキュリティ対策のための統一基準 （平成 30 年度版） 平成 30 年 7 月 25 日 サイバーセキュリティ戦略本部
第1部　総則 1.1　本統一基準の目的・適用範囲 (1) 本統一基準の目的 （略） 本統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策であり、政府機関等のサイバーセキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定）に基づく機関等における統一的な枠組みの中で、統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的とする。 (2)～(4)　（略） (5) 対策項目の記載事項 （略） さらに、機関等は策定した対策基準で定める対策を実施するための、実施手順を整備する必要がある。 1.2　情報の格付の区分・取扱制限 (1) 情報の格付の区分 （略）	第1部　総則 1.1　本統一基準の目的・適用範囲 (1) 本統一基準の目的 （略） 本統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策であり、政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定）に基づく機関等における統一的な枠組みの中で、統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的とする。 (2)～(4)　（略） (5) 対策項目の記載事項 （略） さらに、機関等は統一基準適用個別マニュアル群を踏まえ、実施手順を整備する必要がある。 1.2　情報の格付の区分・取扱制限 (1) 情報の格付の区分 （略）

<table>
<tr><th>改定案</th><th>現行</th></tr>
<tr><td>機密性についての格付の定義

<table><tr><td>格付の区分</td><td>分類の基準</td></tr><tr><td>機密性３情報</td><td>国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報
独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報</td></tr><tr><td>機密性２情報</td><td>（略）</td></tr><tr><td>機密性１情報</td><td>（略）</td></tr></table>
（略）

完全性についての格付の定義　（略）

可用性についての格付の定義　（略）

(2) 情報の取扱制限　（略）

1.3　用語定義
（略）

【あ】
●　（略）</td><td>機密性についての格付の定義

<table><tr><td>格付の区分</td><td>分類の基準</td></tr><tr><td>機密性３情報</td><td>国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書に相当する機密性を要する情報を含む情報
独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報</td></tr><tr><td>機密性２情報</td><td>（略）</td></tr><tr><td>機密性１情報</td><td>（略）</td></tr></table>
（略）

完全性についての格付の定義　（略）

可用性についての格付の定義　（略）

(2) 情報の取扱制限　（略）

1.3　用語定義
（略）

【あ】
●　（略）</td></tr>
</table>

改定案	現行
● （削る）	● 「委託先」とは、外部委託により機関等の情報処理業務の一部又は全部を実施する者をいう。
● 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。	● （新設）
● 「Web（ウェブ）会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像または音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。	● （新設）
【か】 ● （削る）	【か】 ● 「外部委託」とは、機関等の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。
● 「外部サービス」とは、機関等外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能を利用して機関等の情報を取り扱う場合に限る。	● （新設）
● 「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。	● （新設）

改定案	現行
● 「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して機関等に向けて独自のサービスを提供する事業者は含まれない。	● （新設）
● 「外部サービス利用者」とは、外部サービスを利用する機関等の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。	● （新設）
● （略） ● （略） ● （略） ● （略）	● （略） ● （略） ● （略） ● （略）
● 「業務委託」とは、機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、機関等の情報を取り扱う場合に限る。	● （新設）
● （略） ● （略） ● （略）	● （略） ● （略） ● （略）
● （削る）	● 「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。
【さ】 ● （略） ● （略） ● （略） ● （略） ● （略）	【さ】 ● （略） ● （略） ● （略） ● （略） ● （略）

改定案	現行
● （略）	● （略）
● 「情報セキュリティインシデント」とは、JIS Q 27000:2019 における情報セキュリティインシデントをいう。	● 「情報セキュリティインシデント」とは、JIS Q 27000:2014 における情報セキュリティインシデントをいう。
● （略）	● （略）
● （略）	● （略）
● 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。	● 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。
● （略）	● （略）
【た】	【た】
● （略）	● （略）
● （略）	● （略）
● （略）	● （略）
● （略）	● （略）
● 「テレワーク」とは、情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。	● （新設）
● （略）	● （略）

改定案	現行
【は】,【ま】　（略）	【は】,【ま】　（略）
【や】 ●　（削る）	【や】 ●　「約款による外部サービス」とは、民間事業者等の外部の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。
●　（略）	●　（略）
第2部　（略）	第2部　（略）
第3部　情報の取扱い 3.1　情報の取扱い 3.1.1　情報の取扱い 目的・趣旨　（略）	第3部　情報の取扱い 3.1　情報の取扱い 3.1.1　情報の取扱い 目的・趣旨　（略）
遵守事項 (1)～(3)　（略）	遵守事項 (1)～(3)　（略）
(4)　情報の利用・保存 (a)　（略） (b)　職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ること。 (c)　（略）	(4)　情報の利用・保存 (a)　（略） (b)　職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。 (c)　（略）

改定案	現行
(d) 職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。 (ア)～(ウ) （略） (e) （略）	(d) 職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずること。 (ア)～(ウ) （略） (e) （略）
(5)～(8) （略）	(5)～(8) （略）
3.2 （略）	3.2 （略）
第4部 外部委託 4.1 業務委託 4.1.1 業務委託 目的・趣旨 機関等外の者に、情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。 業務委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても業務委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。	第4部 外部委託 4.1 外部委託 4.1.1 外部委託 目的・趣旨 機関等外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。 外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

改定案	現行
なお、委託先で外部サービスを利用する場合は、委託先においても外部サービス特有のリスクがあることから、4.2「外部サービスの利用」で規定する内容についても委託先への要求事項に含める必要がある。 ＜業務委託の例＞ ● 情報システムの開発及び構築業務 ● アプリケーション・コンテンツの開発業務 ● 情報システムの運用業務 ● 業務運用支援業務（統計、集計、データ入力、媒体変換等） ● プロジェクト管理支援業務 ● 調査・研究業務（調査、研究、検査等） （削る） 遵守事項 (1) 業務委託に係る規定の整備 (a) 統括情報セキュリティ責任者は、業務委託に係る以下の内容を含む規定を整備すること。 (ア), (イ) （略） (2) 業務委託に係る契約 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って業務委託を実施すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 (ア)～(キ) （略） (c) , (d) （略） (3) 業務委託における対策の実施 (a)～(c) （略）	なお、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、4.1.4「クラウドサービスの利用」についても本款に加えて遵守する必要がある。 ＜外部委託の例＞ ● 情報システムの開発及び構築業務 ● アプリケーション・コンテンツの開発業務 ● 情報システムの運用業務 ● 業務運用支援業務（統計、集計、データ入力、媒体変換等） ● プロジェクト管理支援業務 ● 調査・研究業務（調査、研究、検査等） ● 情報システム、データセンター、通信回線等の賃貸借 遵守事項 (1) 外部委託に係る規定の整備 (a) 統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備すること。 (ア), (イ) （略） (2) 外部委託に係る契約 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って外部委託を実施すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 (ア)～(キ) （略） (c), (d) （略） (3) 外部委託における対策の実施 (a)～(c) （略）

改定案	現行
(4) 業務委託における情報の取扱い (a) （略） （削る）	(4) 外部委託における情報の取扱い (a) （略） 4.1.2 約款による外部サービスの利用 目的・趣旨 外部委託により業務を遂行する場合は、原則として4.1.1「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3「用語定義」において「約款による外部サービス」として定義するものを利用することも考えられる。 このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を機関等からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、4.1.1「外部委託」を適用するのではなく、本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。 遵守事項 (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。

改定案	現行
（削る）	(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。 4.1.3 ソーシャルメディアサービスによる情報発信 目的・趣旨 インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。機関等においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、民間事業者等により提供されているソーシャルメディアサービスは、.go.jp で終わるドメイン名（以下「政府ドメイン名」という。）を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、機関等のアカウントを乗っ取られた場合や、利用しているソーシャルメディアサービスが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民等に提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。 このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。 なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、4.1.2「約款による外部サービスの利用」の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、4.1.1「外部委託」及び

改定案	現行
	4.1.2「約款による外部サービスの利用」を適用するのではなく、本款に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。 遵守事項 (1) ソーシャルメディアサービスによる情報発信時の対策 (a) 統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。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)機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。 (イ)パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。 (b) 情報セキュリティ責任者は、機関等において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。 (c) 職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。
(削る)	4.1.4 クラウドサービスの利用 目的・趣旨 業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

改定案	現行
	クラウドサービスを利用する際、機関等がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、機関等による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。 遵守事項 (1) クラウドサービスの利用における対策 (a) 情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。 (b) 情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。 (c) 情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。 (d) 情報システムセキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。

改定案	現行
	(e) 情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。
4.2　外部サービスの利用 4.2.1　要機密情報を取り扱う場合 目的・趣旨 政府機関において今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。 機関等が外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。機関等が外部サービスを利用して要機密情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、機関等による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、機関等と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。 さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に早いサイクルで変化しており、利用開始時に行ったセキュリティ対策が	（新設）

改定案	現行
途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。 ＜外部サービスの例＞ ● クラウドサービス ● Ｗｅｂ会議サービス ● ＳＮＳ（ソーシャルネットワーキングサービス） ● 検索サービス、翻訳サービス、地図サービス ● ホスティングサービス ● インターネット回線接続サービス 遵守事項 (1) 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、以下を含む外部サービス（要機密情報を取り扱う場合）の利用に関する規定を整備すること。 (ア)外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 4.2 節において「外部サービス利用判断基準」という。） (イ)外部サービス提供者の選定基準 (ウ)外部サービスの利用申請の許可権限者と利用手続 (エ)外部サービス管理者の指名と外部サービスの利用状況の管理 (2) 外部サービスの選定（クラウドサービスの場合） (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、業務に特有のリスクが存在する場合には、必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めること。	

改定案	現行
(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限並びに外部サービスとの情報セキュリティに関する役割及び責任の範囲を踏まえてセキュリティ要件を定め、外部サービスを選定すること。 (3) 外部サービスの選定（クラウドサービス以外の場合） (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。 (ア)外部サービスの利用を通じて機関等が取り扱う情報の外部サービス提供者における目的外利用の禁止 (イ)外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制 (ウ)外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制 (エ)外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供 (オ)情報セキュリティインシデントへの対処方法 (カ)情報セキュリティ対策その他の契約の履行状況の確認方法 (キ)情報セキュリティ対策の履行が不十分な場合の対処方法	

改定案	現行
(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。 (d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの利用を通じて機関等が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。 (ア)情報セキュリティ監査の受入れ (イ)サービスレベルの保証 (e) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの利用を通じて機関等が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて機関等の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。 (f)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。 (g) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。 (h) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する	

改定案	現行
部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。 (i)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。 (4) 外部サービスの利用に係る調達・契約 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。 (5) 外部サービスの利用承認 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。 (b) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。 (c) 利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。	

改定案	現行
(6) 外部サービスを利用した情報システムの導入・構築時の対策 (a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。 (ア)不正なアクセスを防止するためのアクセス制御 (イ)取り扱う情報の機密性保護のための暗号化 (ウ)開発時におけるセキュリティ対策 (エ)設計・設定時の誤りの防止 (b) 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。 (7) 外部サービスを利用した情報システムの運用・保守時の対策 (a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。 (ア)外部サービス利用方針の規定 (イ)外部サービス利用に必要な教育 (ウ)取り扱う資産の管理 (エ)不正アクセスを防止するためのアクセス制御 (オ)取り扱う情報の機密性保護のための暗号化 (カ)外部サービス内の通信の制御 (キ)設計・設定時の誤りの防止 (ク)外部サービスを利用した情報システムの事業継続 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。 (c) 外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。	

改定案	現行
(8) 外部サービスを利用した情報システムの更改・廃棄時の対策 (a) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。 (ア)外部サービスの利用終了時における対策 (イ)外部サービスで取り扱った情報の廃棄 (ウ)外部サービスの利用のために作成したアカウントの廃棄 (b) 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。	
4.2.2 要機密情報を取り扱わない場合 目的・趣旨 要機密情報を取り扱わない場合であって、外部サービス提供先における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を機関等から送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、要機密情報を取り扱う場合と同等のセキュリティ対策を求めることは外部サービスの利用推進を妨げるものであるため、要機密情報を取り扱わない前提で外部サービスを利用する場合は、本款で定めた遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。 遵守事項 (1) 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、以下を含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備すること。 (ア)外部サービスを利用可能な業務の範囲 (イ)外部サービスの利用申請の許可権限者と利用手続 (ウ)外部サービス管理者の指名と外部サービスの利用状況の管理 (エ)外部サービスの利用の運用手順	（新設）

改定案	現行
(2) 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要機密情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。 (b) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。	
第5部　情報システムのライフサイクル 5.1　（略）	第5部　情報システムのライフサイクル 5.1　（略）
5.2　情報システムのライフサイクルの各段階における対策 5.2.1　情報システムの企画・要件定義 目的・趣旨 （略） また、情報システムの構築、運用・保守を業務委託する場合については、4.1「業務委託」についても併せて遵守する必要がある。	5.2　情報システムのライフサイクルの各段階における対策 5.2.1　情報システムの企画・要件定義 目的・趣旨 （略） また、情報システムの構築、運用・保守を外部委託する場合については、4.1「外部委託」についても併せて遵守する必要がある。
遵守事項 (1)　（略）	遵守事項 (1)　（略）
(2) 情報システムのセキュリティ要件の策定 (a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（外部サービスを含	(2) 情報システムのセキュリティ要件の策定 (a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービス

改定案	現行
む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。 (ア)～(ウ)　（略） (b)～(d)　（略）	を含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。 (ア)～(ウ)　（略） (b)～(d)　（略）
(3)　情報システムの構築を業務委託する場合の対策 (a)　情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。 (ア)～(ウ)　（略）	(3)　情報システムの構築を外部委託する場合の対策 (a)　情報システムセキュリティ責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。 (ア)～(ウ)　（略）
(4)　情報システムの運用・保守を業務委託する場合の対策 (a)　情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。 (b)　情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させること。	(4)　情報システムの運用・保守を外部委託する場合の対策 (a)　情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。 (b)　情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させること。
5.2.2～5.2.5　（略）	5.2.2～5.2.5　（略）
5.3　（略）	5.3　（略）
第6部　情報システムのセキュリティ要件 6.1　情報システムのセキュリティ機能 6.1.1～6.1.4　（略）	第6部　情報システムのセキュリティ要件 6.1　情報システムのセキュリティ機能 6.1.1～6.1.4　（略）

改定案	現行
6.1.5　暗号・電子署名 目的・趣旨　（略） 遵守事項 (1)　暗号化機能・電子署名機能の導入 (a), (b)　（略） (c)　情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定めること。 (2)　（略） 6.2　情報セキュリティの脅威への対策 6.2.1 , 6.2.2　（略） 6.2.3　サービス不能攻撃対策 目的・趣旨 インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、機関等の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている。	6.1.5　暗号・電子署名 目的・趣旨　（略） 遵守事項 (1)　暗号化機能・電子署名機能の導入 (a), (b)　（略） (c)　情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。 (2)　（略） 6.2　情報セキュリティの脅威への対策 6.2.1 , 6.2.2　（略） 6.2.3　サービス不能攻撃対策 目的・趣旨 インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、機関等の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

改定案	現行
遵守事項 (1)　（略）	遵守事項 (1)　（略）
6.2.4　標的型攻撃対策 目的・趣旨 （略） したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。 近年は攻撃対象の組織に対する直接的な攻撃だけでなく、委託先等の関連組織への間接的な攻撃も確認されており、より幅広い対策の検討が求められる。	6.2.4　標的型攻撃対策 目的・趣旨 （略） したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。
遵守事項 (1)　標的型攻撃対策の実施 (a)　（略） (b)　情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。	遵守事項 (1)　標的型攻撃対策の実施 (a)　（略） (b)　情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。
6.3　アプリケーション・コンテンツの作成・提供 6.3.1　アプリケーション・コンテンツの作成時の対策 目的・趣旨 （略）	6.3　アプリケーション・コンテンツの作成・提供 6.3.1　アプリケーション・コンテンツの作成時の対策 目的・趣旨 （略）

改定案	現行
また、アプリケーション・コンテンツの開発・提供を業務委託する場合については、4.1.1「業務委託」についても併せて遵守する必要がある。 遵守事項 (1)　(略) (2)　アプリケーション・コンテンツのセキュリティ要件の策定 (a)　(略) (ア)～(オ)　(略) (カ)サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。 (b)　職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項各号に掲げる内容を調達仕様に含めること。 6.3.2　アプリケーション・コンテンツ提供時の対策 目的・趣旨　(略) 遵守事項 (1)　政府ドメイン名の使用 (a)　(略) (ア), (イ)　(略) (ウ)8.1.1(9)に掲げるソーシャルメディアサービスによる情報発信を行う場合 (b)　職員等は、機関等外向けに提供するウェブサイト等の作成を業務委託する場合においては、前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。	また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1「外部委託」についても併せて遵守する必要がある。 遵守事項 (1)　(略) (2)　アプリケーション・コンテンツのセキュリティ要件の策定 (a)　(略) (ア)～(オ)　(略) (カ)サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。 (b)　職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項各号に掲げる内容を調達仕様に含めること。 6.3.2　アプリケーション・コンテンツ提供時の対策 目的・趣旨　(略) 遵守事項 (1)　政府ドメイン名の使用 (a)　(略) (ア), (イ)　(略) (ウ)4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合 (b)　職員等は、機関等外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。

改定案	現行
(2), (3)　（略）	(2), (3)　（略）
第7部　情報システムの構成要素 7.1　端末・サーバ装置等 7.1.1　端末 目的・趣旨 端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、職員等の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。端末のモバイル利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。 また、機関等の業務の遂行においては、機関等から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず機関等支給以外の端末を利用して情報処理を行う場合も考えられるが、この際、当該端末の情報セキュリティ水準が対策基準を満たさないおそれがある。このため、機関等支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で、職員等に対して機関等における厳格な管理の下で利用させることが必要である。 なお、本款の遵守事項のほか、6.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。 遵守事項 (1)～(3)　（略）	第7部　情報システムの構成要素 7.1　端末・サーバ装置等 7.1.1　端末 目的・趣旨 端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、職員等の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。端末のモバイル利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。 端末については、サーバ等の他の情報システムの構成要素と異なり、機関等の判断によっては機関等支給以外のものの利用があり得る。機関等における業務で端末を利用する以上は、機関等により支給されたものか、それ以外かにかかわらず、同等の情報セキュリティ水準が求められる。このため、本款及び8.1.1「情報システムの利用」での端末に係る規定においては、両者を対象としている箇所がある。この際、両者を区別して「機関等が支給する端末」、「機関等支給以外の端末」と表現している。単に「端末」という場合は、1.3「用語定義」において定義されているとおり機関等が支給するものを指す。 なお、本款の遵守事項のほか、6.1「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1「ソフトウェアに関する脆弱性対策」、6.2.2「不正プログラム対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。 遵守事項 (1)～(3)　（略）

改定案	現行
(4) 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）の導入及び利用時の対策	(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、職員等が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）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。	（新設）
(b) 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）について、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に関する規定を整備すること。	(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。
（削る）	(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
（削る）	(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
（削る）	(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) 統括情報セキュリティ責任者は、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機関等が支給する端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。	（新設）
(d) 情報システムセキュリティ責任者は、職員等が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）を用いて要機密情報を取り扱う場合は、当該端末について本条(b)の技術的な措置を講ずること。	(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。

改定案	現行
（削る）	(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）
（削る）	(イ)端末管理責任者　機関等支給以外の端末
（削る）	(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。
（削る）	(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。
(5) 機関等支給以外の端末の導入及び利用時の対策	（新設）
(a) 最高情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。	
(b) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続を定めること。	
(c) 統括情報セキュリティ責任者は、職員等が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について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。	
(d) 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	

改定案	現行
とを防止するための技術的な措置 (イ)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 (e) 統括情報セキュリティ責任者は、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機関等支給以外の端末を機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。 (f)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。 (g) 端末管理責任者は、職員等が機関等支給以外の端末を用いて要機密情報を取り扱う場合は、当該端末について本条(d)(ア)の安全管理措置を講ずること。 (h) 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本条(d)(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、及び本条(d)(イ)に定める安全管理措置を職員等に講じさせること。 (i)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、前項において本条(d)(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、及び本条(d)(イ)に定める安全管理措置を講ずること。 (j)職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。 (k) 職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。	

改定案	現行
7.1.2　サーバ装置 目的・趣旨 　電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に機関等が利用するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。 　（略） 遵守事項 (1)～(3)　（略） 7.1.3　（略） 7.2　（略） 7.3　通信回線 7.3.1　通信回線 目的・趣旨　（略） 遵守事項 (1)～(3)　（略）	7.1.2　サーバ装置 目的・趣旨 　電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に機関等が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。 　（略） 遵守事項 (1)～(3)　（略） 7.1.3　（略） 7.2　（略） 7.3　通信回線 7.3.1　通信回線 目的・趣旨　（略） 遵守事項 (1)～(3)　（略）

改定案	現行
（削る）	(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。
(4) （略）	(5)（略）
7.3.2 （略）	7.3.2 （略）
第8部 情報システムの利用 8.1 情報システムの利用 8.1.1 情報システムの利用 目的・趣旨 （略） なお、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）に係る規定の整備については遵守事項 7.1.1(4)、機関等支給以外の端末に係る規定の整備については遵守事項 7.1.1(5)をそれぞれ参照すること。	第8部 情報システムの利用 8.1 情報システムの利用 8.1.1 情報システムの利用 目的・趣旨 （略） なお、本款には 7.1.1「端末」と同様に、機関等が支給する端末と機関等支給以外の端末の両者を対象にしている箇所がある。また、両者を包含する場合は、「端末（支給外端末を含む）」と表現している。
遵守事項 (1) 情報システムの利用に係る規定の整備 (a) （略） （削る）	遵守事項 (1) 情報システムの利用に係る規定の整備 (a) （略） (b) 統括情報セキュリティ責任者は、職員等が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について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。

改定案	現行
（削る）	(c) 統括情報セキュリティ責任者は、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ことについての可否を判断した上で、可と判断する場合は、当該端末（支給外端末を含む）から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。
(b), (c) （略）	(d), (e) （略）
(2)～(7) （略）	(2)～(7) （略）
(8) Web 会議サービスの利用時の対策 (a) 職員等は、機関等の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。 (b) 職員等は Web 会議を主催する場合、会議に無関係の者が参加できないよう措置すること。	（新設）
(9) ソーシャルメディアサービスによる情報発信時の対策 (a) 統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。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)機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。 (イ)パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。 (b) 職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。	（新設）

改定案	現行
8.1.2　テレワーク 目的・趣旨 　働き方改革実行計画（平成 29 年 3 月 28 日　働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、職員等が業務を遂行する上で、必ずしも勤務官署に出勤する必要はなく、自宅やサテライトオフィス等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模感染症の感染予防対策として、勤務官署への出勤が抑制されるような状況下では、大半の職員等が勤務官署以外から業務を遂行できるようにテレワーク環境の整備が必要となる。 　本款では、テレワークの実施に特に必要な対策についてのみ規定しているため、本款以外に、3.1.1「情報の取扱い」、7.3.1「通信回線」及び 8.1.1「情報システムの利用」の各款、遵守事項 7.1.1(4)「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）の導入及び利用時の対策」及び遵守事項 7.1.1(5)「機関等支給以外の端末の導入及び利用時の対策」も参照すること。 遵守事項 (1)　実施規定の整備 　(a)　統括情報セキュリティ責任者は、テレワークの実施に係る規定を整備するために必要な情報セキュリティ対策の項目を定めること。なお、原則としてテレワークは機関等が支給する端末で行うよう定めること。 　(b)　テレワークに対応した情報システムの情報システムセキュリティ責任者は、前項で定められた項目を用いてテレワーク実施時の情報セキュリティ対策に係る規定を整備すること。 (2)　実施環境における対策 　(a)　情報システムセキュリティ責任者は、テレワークの実施により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	（新設）

改定案	現行
する形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対するセキュリティを確保すること。 (b) 情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行うこと。 (c) 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じること。 (d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。 (3) 実施時における対策 (a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等がチェックするべき項目を定め、職員等に当該チェックを実施させること。 (b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。 (c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。	
（削る）	8.2 機関等支給以外の端末の利用 8.2.1 機関等支給以外の端末の利用 目的・趣旨 機関等の業務の遂行においては、機関等から支給された端末を用いてこれを遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず機関等支給以外の端末を利用して情報処理を行う場合がある。この際、当該端末は機関等が支給したものではないという理由で、情報セキュリティ対策が講じられない場合、当該端末で取り扱われる情報セキュリティ水準が、対策基準を満たさないおそれがある。

改定案	現行
	このため、機関等支給以外の端末を業務において利用する可能性がある場合は、利用に当たって求められる情報セキュリティの水準が確保されるかどうかを適切に評価し、その利用の可否を判断をした上で、職員等に対して機関等における厳格な管理の下で利用させることが必要である。 なお、機関等支給以外の端末の利用に係る情報セキュリティ対策については 7.1.1「端末」及び 8.1.1「情報システムの利用」を参照のこと。 遵守事項 (1) 機関等支給以外の端末の利用可否の判断 (a) 最高情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。 (2) 機関等支給以外の端末の利用規定の整備・管理 (a) 統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続を定めること。 (3) 機関等支給以外の端末の利用時の対策 (a) 職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。 (f) 職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。