○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（一部に改め文を含む）

以下の新旧対照表に掲げるもののほか、政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）（平成 28 年８月 31 日サイバーセキュリティ戦略本部）中「府省庁」を「機関等」に、「行政事務従事者」を「職員等」に、「府省庁対策基準」を「対策基準」に、「行政事務」を「業務」に改める。

改定案	現行
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　年　月　日 サイバーセキュリティ戦略本部	政府機関の情報セキュリティ対策のための統一基準 （平成 28 年度版） 平成 28 年８月 31 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 情報セキュリティの基本は、機関等で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、それぞれの機関等が自らの責任において情報セキュリティ対策を講じていくことが原則である。 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。	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 情報セキュリティの基本は、府省庁で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、それぞれの府省庁が自らの責任において情報セキュリティ対策を講じていくことが原則である。しかし、府省庁共通の IT 環境の利用、府省庁間の情報流通の現状を踏まえると、政府機関全体の統一的な枠組みを構築し、それぞれの府省庁の情報セキュリティ水準の斉一的な引上げを図ることが必要である。 本統一基準は、「政府機関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）に基づく政府機関における統一的な枠組みの中で、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

(2) 本統一基準の適用対象 (a) 本統一基準において適用対象とする者は、全ての職員等とする。 (b) 本統一基準において適用対象とする情報は、以下の情報とする。 (ア)職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。） (イ)～(ウ)　（略） (c) 本統一基準において適用対象とする情報システムは、本統一基準の適用対象となる情報を取り扱う全ての情報システムとする。	(2) 本統一基準の適用範囲 (a) 本統一基準において適用範囲とする者は、全ての職員等とする。 (b) 本統一基準において適用範囲とする情報は、以下の情報とする。 (ア)行政事務従事者が職務上使用することを目的として府省庁が調達し、又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。） (イ)～(ウ)　（略） (c) 本統一基準において適用範囲とする情報システムは、本統一基準の適用範囲となる情報を取り扱う全ての情報システムとする。
(3), (4)　（略）	(3), (4)　（略）
(5) 対策項目の記載事項 本統一基準では、機関等が行うべき対策について、目的別に部、節及び款の３階層にて対策項目を分類し、各款に対して目的及び趣旨並びに遵守事項を示している。 内閣官房内閣サイバーセキュリティセンターが別途策定する政府機関等の対策基準策定のためのガイドラインには、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）が例示されるとともに、対策基準の策定及び実施に際しての考え方等が解説されている。基本対策事項は遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要がある。 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。	(5) 対策項目の記載事項 本統一基準では、府省庁が行うべき対策について、目的別に部、節及び項の３階層にて対策項目を分類し、各項に対して目的、趣旨及び遵守事項を示している。遵守事項は、府省庁対策基準において必ず実施すべき対策事項である。府省庁は、内閣官房内閣サイバーセキュリティセンターが別途整備する府省庁対策基準策定のためのガイドライン及び政府機関統一基準適用個別マニュアル群において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、府省庁対策基準を策定する必要がある。 （新設）
1.2　情報の格付の区分・取扱制限 (1) 情報の格付の区分 （略）	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>なお、機関等において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本統一基準の遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。また、他機関等へ情報を提供する場合は、自組織の対策基準における格付区分と本統一基準における格付区分の対応について、適切に伝達する必要がある。</td><td>府省庁において格付の定義を変更又は追加する場合には、それぞれの府省庁の対策基準における格付区分と遵守事項との関係が本統一基準での関係と同等以上となるように準拠しなければならない。また、他府省庁へ情報を提供する場合は、自身の格付区分と本統一基準における格付区分の対応について、適切に伝達する必要がある。</td></tr>
<tr><td>機密性についての格付の定義

<table>
<tr><th>格付の区分</th><th>分類の基準</th></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>国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人</td></tr>
</table></td><td>機密性についての格付の定義

<table>
<tr><th>格付の区分</th><th>分類の基準</th></tr>
<tr><td>機密性３情報</td><td>行政事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
（新設）</td></tr>
<tr><td>機密性２情報</td><td>行政事務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報

（新設）</td></tr>
</table></td></tr>
</table>

改定案		現行	
	（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の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		（新設）
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の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	機密性１情報	情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 （新設） （新設）
（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）		（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）	

【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。 ● 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。 ● 「機関等内通信回線」とは、一つの機関等が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該機関等の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。機関等内通信回線には、専用線やVPN等物理的な回線を機関等が管理していないものも含まれる。 ● （略） ● 「基盤となる情報システム」とは、他の機関等と共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。 ● （略） ● 「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。 ● （略） ● （略） 【さ】 ● （略） ● 「CYMAT（サイマット）」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動	【か】 ● 「外部委託」とは、府省庁の情報処理業務の一部又は全部について、契約をもって府省庁外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。 ● 「府省庁外通信回線」とは、通信回線のうち、府省庁内通信回線以外のものをいう。 ● 「府省庁内通信回線」とは、一つの府省庁が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該府省庁の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。府省庁内通信回線には、専用線やVPN等物理的な回線を府省庁が管理していないものも含まれる。 ● （略） ● 「基盤となる情報システム」とは、他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。 ● （略） ● 「府省庁」とは、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成11年法律第89号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和23年法律第120号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。「府省庁」と表記する場合は、単一の機関を指す。 ● （略） ● （略） 【さ】 ● （略） ● 「CYMAT（サイマット）」とは、サイバー攻撃等により政府機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して

改定案	現行
的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。	機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。
● （略）	● （略）
● （略）	● （略）
● 「情報」とは、「1.1(2) 本統一基準の適用対象」の(b)に定めるものをいう。	● 「情報」とは、「1.1(2) 本統一基準の適用範囲」の(b)に定めるものをいう。
● （略）	● （略）
● （略）	● （略）
● （略）	● （略）
● 「情報セキュリティ対策推進体制」とは、機関等の情報セキュリティ対策の推進に係る事務を遂行するため、当該機関等に設置された体制をいう。	● （新設）
● （略）	● （略）
● 「職員等」とは、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の管理対象である情報及び情報システムを取り扱う者をいう。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。	● 「行政事務従事者」とは、府省庁において行政事務に従事している国家公務員その他の府省庁の指揮命令に服している者であって、府省庁の管理対象である情報及び情報システムを取り扱う者をいう。行政事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。
【た】	【た】
● 「対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。	● 「府省庁対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
● 「端末」とは、情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機関等が調達又は開発するもの以外を指す「機関等支給以外の端	● 「端末」とは、情報システムの構成要素である機器のうち、行政事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、府省庁が調達又は開発するものをいう。端末には、モバイル端末も含まれる。

改定案	現行
末」がある。また、機関等が調達又は開発した端末と機関等支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。 ● （略） ● （略） ● 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。 【は】，【ま】（略） 【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。 ● 「要管理対策区域」とは、機関等の管理下にある区域（機関等が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。 第2部　情報セキュリティ対策の基本的枠組み 2.1　導入・計画 2.1.1　組織・体制の整備 目的・趣旨 （略）	● （略） ● （略） ● 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。 【は】，【ま】（略） 【や】 ● 「約款による外部サービス」とは、民間事業者等の府省庁外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。 ● 「要管理対策区域」とは、府省庁が管理する庁舎等（外部の組織から借用している施設等を含む。）府省庁の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。 第2部　情報セキュリティ対策の基本的枠組み 2.1　導入・計画 2.1.1　組織・体制の整備 目的・趣旨 （略）

改定案	現行
なお、最高情報セキュリティ責任者は、統一基準に定められた自らの担務を、最高情報セキュリティ副責任者その他の統一基準に定める責任者に担わせることができる。	なお、最高情報セキュリティ責任者は、統一基準に定められた自らの担務を、統一基準に定める責任者等に担わせることができる。
遵守事項 (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置 (a) （略） (b) 機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置くこと。	遵守事項 (1) 最高情報セキュリティ責任者の設置 (a) （略） (b) （新設）
(2) 情報セキュリティ委員会の設置 (a) 最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。	(2) 情報セキュリティ委員会の設置 (a) 最高情報セキュリティ責任者は、府省庁対策基準等の審議を行う機能を持つ組織として、府省庁の情報セキュリティを推進する部局及びその他行政事務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。
(3) （略）	(3) （略）
(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置 (a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する者として、統括情報セキュリティ責任者１人を選任すること。 (b)～(d) （略）	(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置 (a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者を補佐する者として、統括情報セキュリティ責任者１人を選任すること。 (b)～(d) （略）

(5)　(略)	(5)　(略)
(6)　情報セキュリティ対策推進体制の整備 (a)　最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制を整備し、その役割を規定すること。 (b)　最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。	(新設)
(7)　情報セキュリティインシデントに備えた体制の整備 (a)　(略) (b)　最高情報セキュリティ責任者は、職員等のうちから CSIRT に属する職員等として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、機関等における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めること。 (c)　(略) (d)　最高情報セキュリティ責任者は、CYMAT に属する職員を指名すること。(国の行政機関に限る。)	(6)　情報セキュリティインシデントに備えた体制の整備 (a)　(略) (b)　最高情報セキュリティ責任者は、行政事務従事者のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。 (c)　(略) (d)　最高情報セキュリティ責任者は、CYMAT に属する職員を指名すること。
(8)　兼務を禁止する役割 (a)　(略) (ア)承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う者（以下本条において「承認権限者等」という。） (イ)（略） (b)　(略)	(7)　兼務を禁止する役割 (a)　(略) (ア)承認又は許可（以下本項において「承認等」という。）の申請者と当該承認等を行う者（以下本項において「承認権限者等」という。） (イ)（略） (b)　(略)
2.1.2　対策基準・対策推進計画の策定 目的・趣旨	2.1.2　府省庁対策基準・対策推進計画の策定 目的・趣旨

改定案	現行
機関等の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、機関等として遵守すべき対策の基準を、情報セキュリティに係るリスク評価の結果等を踏まえた上で定めるとともに、計画的に対策を実施することが重要である。	府省庁の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、府省庁として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。
遵守事項 (1) 対策基準の策定 (a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠した対策基準を定めること。また、対策基準は、機関等の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。	遵守事項 (1) 府省庁対策基準の策定 (a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠した府省庁対策基準を定めること。
(2) （略）	(2) （略）
2.2 運用 2.2.1 情報セキュリティ関係規程の運用 目的・趣旨 （略）	2.2 運用 2.2.1 情報セキュリティ関係規程の運用 目的・趣旨 （略）
遵守事項 (1) 情報セキュリティ対策の運用 (a), (b) （略） (c) 情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行すること。 (d) 情報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、職員等から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告すること。 (e) 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告すること。	遵守事項 (1) 情報セキュリティ対策に関する実施手順の整備・運用 (a), (b) （略） （新設） (c) 情報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、行政事務従事者より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告すること。 （新設）

(2) （略）	(2) （略）
2.2.2 例外措置 目的・趣旨 （略）	2.2.2 例外措置 目的・趣旨 （略）
遵守事項 (1) 例外措置手続の整備 (a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下本款において「許可権限者」という。）及び審査手続を定めること。 (b) （略）	遵守事項 (1) 例外措置手続の整備 (a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び、審査手続を定めること。 (b) （略）
(2) （略）	(2) （略）
2.2.3 教育 目的・趣旨 （略） また、機関等における近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。	2.2.3 教育 目的・趣旨 （略） また、政府機関等における近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。
遵守事項 (1) 教育体制の整備・教育実施計画の策定 (a) （略） (b) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すこと。	遵守事項 (1) 教育体制等の整備 (a) （略） （新設）
(2) 教育の実施 (a) 課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を適切に受講させるこ	(2) 教育の実施 (a) 課室情報セキュリティ責任者は、行政事務従事者に対して、情報セキュリティ関係規定に係る教育を適切に受講させること。

改定案	現行
と。 (b) （略） (c) 課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及び CSIRT に属する職員等に教育を適切に受講させること。また、国の行政機関における課室情報セキュリティ責任者は、CYMAT に属する職員にも教育を適切に受講させること。 (d) 課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告すること。 (e) 統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。	(b) （略） (c) 課室情報セキュリティ責任者は、CYMAT 及び CSIRT に属する職員に教育を適切に受講させること。 （新設） (d) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。
2.2.4　情報セキュリティインシデントへの対処 目的・趣旨　（略）	2.2.4　情報セキュリティインシデントへの対処 目的・趣旨　（略）
遵守事項 (1)　（略）	遵守事項 (1)　（略）
(2) 情報セキュリティインシデントへの対処 (a)～(f)　（略） (g) 国の行政機関における CSIRT は、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。また、独立行政法人及び指定法人における CSIRT は、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関における CSIRT は、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。 (h) CSIRT は、認知した情報セキュリティインシデントがサイバー攻撃	(2) 情報セキュリティインシデントへの対処 (a)～(f)　（略） (g) CSIRT は、府省庁の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。 また、認知した情報セキュリティインシデントがサイバー攻撃又はそ

改定案	現行
又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。 (i) 国の行政機関における CSIRT は、認知した情報セキュリティインシデント又は独立行政法人及び指定法人から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「大規模サイバー攻撃事態等への初動対処について（平成 22 年3月 19 日内閣危機管理監決裁)」に基づく報告連絡を行うこと。 (j)～(m) （略）	のおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。 さらに、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態においては、「大規模サイバー攻撃事態等への初動対処について（平成 22 年3月 19 日内閣危機管理監決裁)」に基づく報告連絡も行うこと。 (h)～(k) （略）
(3) （略）	(3) （略）
2.3 点検 2.3.1 情報セキュリティ対策の自己点検 目的・趣旨 （略）	2.3 点検 2.3.1 情報セキュリティ対策の自己点検 目的・趣旨 （略）
遵守事項 (1) 自己点検計画の策定・手順の準備 (a) （略） (b) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等ごとの自己点検票及び自己点検の実施手順を整備すること。 (c) 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。	遵守事項 (1) 自己点検計画の策定・手順の準備 (a) （略） (b) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。 （新設）
(2) （略） (3) 自己点検結果の評価・改善 (a) 情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己	(2) （略） (3) 自己点検結果の評価・改善 (a) 統括情報セキュリティ責任者及び情報セキュリティ責任者は、行政事務従事者による自己点検結果を分析し、評価すること。

改定案	現行
点検結果を分析、評価すること。また、評価結果を統括情報セキュリティ責任者に報告すること。 (b) 統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を最高情報セキュリティ責任者に報告すること。 (c)（略）	統括情報セキュリティ責任者は評価結果を最高情報セキュリティ責任者に報告すること。 (b)（略）
2.3.2　情報セキュリティ監査 目的・趣旨　（略）	2.3.2　情報セキュリティ監査 目的・趣旨　（略）
遵守事項 (1) 監査実施計画の策定 (a)　（略） (b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定めること。	遵守事項 (1) 監査実施計画の策定 (a)　（略） (b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の指示を、最高情報セキュリティ責任者から受けた場合には、追加の監査実施計画を定めること。
(2) 監査の実施 (a)　（略） (ア)～(イ)　（略） (ウ)被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること	(2) 監査の実施 (a)　（略） (ア)～(イ)　（略） (ウ)自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること
(3) 監査結果に応じた対処 (a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示すること。 (b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者から	(3) 監査結果に応じた対処 (a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を情報セキュリティ責任者に指示すること。 （新設）

改定案	現行
の改善の指示のうち、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。 (c) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。	(b) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。
2.4　見直し 2.4.1　情報セキュリティ対策の見直し 目的・趣旨 （略） また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策基準及び対策推進計画に反映することも重要である。	2.4　見直し 2.4.1　情報セキュリティ対策の見直し 目的・趣旨 （略） また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策推進計画に反映することも重要である。
遵守事項　（略）	遵守事項（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 業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下本款において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての職員等が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、職員等は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。	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 行政事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての行政事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、行政事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

改定案	現行
なお、国の行政機関における秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本統一基準の規定に基づき、適切に情報が取り扱われるよう留意すること。また、独立行政法人及び指定法人における機密性３情報の管理に関しては、本統一基準の規定に基づき対策を講ずること。	なお、秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本統一基準の規定に基づき、適切に情報が取り扱われるよう留意すること。
遵守事項 (1)～(2) （略）	遵守事項 (1)～(2) （略）
(3) 情報の格付及び取扱制限の決定・明示等 (a), (b) （略） (c) 職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと。	(3) 情報の格付及び取扱制限の決定・明示等 (a), (b) （略） (c) 行政事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下この項において「決定者等」という。）に確認し、その結果に基づき見直すこと。
(4) 情報の利用・保存 (a)～(c) （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) 機器等に保存する場合は、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に接続しない端末、サーバ装置等の機器等を使用すること。 (イ) 当該情報に対し、暗号化による保護を行うこと。 (ウ) 当該情報を保存した機器等について、盗難及び不正な持ち出し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。	(4) 情報の利用・保存 (a)～(c) （略） (d) 行政事務従事者は、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。

改定案	現行
(e) （略）	(e) （略）
(5) 情報の提供・公表	(5) 情報の提供・公表
(a)～(b) （略）	(a)～(b) （略）
(c) 独立行政法人及び指定法人における職員等は、機密性３情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	（新設）
(d) （略）	(c) （略）
(6) 情報の運搬・送信	(6) 情報の運搬・送信
(a) 職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。	(a) 行政事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他府省庁の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。
(b) 職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。	(b) 行政事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。
(7) （略）	(7) （略）

(8) 情報のバックアップ (a), (b) （略） (c) 職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。 3.2　情報を取り扱う区域の管理 3.2.1　情報を取り扱う区域の管理 目的・趣旨　（略） 遵守事項 (1)　（略） (2) 区域ごとの対策の決定 (a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。 (b)　（略） (3)　（略） 第4部　外部委託 4.1　外部委託 4.1.1　外部委託 目的・趣旨 （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。 （削る）	(8) 情報のバックアップ (a), (b) （略） (c) 行政事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。 3.2　情報を取り扱う区域の管理 3.2.1　情報を取り扱う区域の管理 目的・趣旨　（略） 遵守事項 (1)　（略） (2) 区域ごとの対策の決定 (a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。 (b)　（略） (3)　（略） 第4部　外部委託 4.1　外部委託 4.1.1　外部委託 目的・趣旨 （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 項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。 また、民間事業者が不特定多数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 節において「約款による外部サービス」として定義するものを利用し、行政事務を遂行する場合も外部委託の一つ

改定案	現行
＜外部委託の例＞　（略） 遵守事項 (1) 外部委託に係る規定の整備 (a) （略） (ア)委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本款において「委託判断基準」という。） (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) （略） (ア)～(イ) （略） (ウ)委託事業の実施に当たり、委託先企業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)～(キ) （略） (c) （略） (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、委託先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、上記(b)(c)の措置の実施を委託先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、仕様内容に含めること。また、委託判断基準及び委託先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。	の形態であるが、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、その際は本項に代えて 4.1.2 項「約款による外部サービスの利用」を適用すること。 ＜外部委託の例＞　（略） 遵守事項 (1) 外部委託に係る規定の整備 (a) （略） (ア)委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準 (イ)（略） (2) 外部委託に係る契約 （新設） (a) （略） (ア)～(イ) （略） (ウ)委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 (エ)～(キ) （略） (b)（略） (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、委託先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、上記(a)(b)の措置の実施を委託先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府省庁に提供し、府省庁の承認を受けるよう、仕様内容に含めること。

(3), (4) （略）	(3), (4) （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。	4.1.2　約款による外部サービスの利用 目的・趣旨 外部委託により行政事務を遂行する場合は、原則として 4.1.1 項「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 節において「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、種々の情報を政府機関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、本項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　（略）	遵守事項　（略）
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	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。政府機関においても、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、政府機関のアカウントを乗っ取ら

改定案	現行
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。 （略） 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　（略） 4.1.4　クラウドサービスの利用 目的・趣旨 （略） 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。	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。 （略） 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 項の規定と同様に、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、本項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　（略） 4.1.4　クラウドサービスの利用 目的・趣旨 （略） クラウドサービスを利用する際、政府機関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、政府機関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。

改定案	現行
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)～(e) （略）	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、政府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)～(e) （略）
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）	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）
遵守事項 (1) 実施体制の確保 (a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めること。 (b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機関等が定める運用管理規程等に応じた体制の確保を、最高情報セキュリティ責任者に求めること。 (c) 最高情報セキュリティ責任者は、前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。	遵守事項 (1) 実施体制の確保 (a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。 (b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する府省庁が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。 （新設）

(2) 情報システムのセキュリティ要件の策定 (a) (略) (ア) (略) (イ)情報システム運用時の監視等の運用管理機能要件(監視するデータが暗号化されている場合は、必要に応じて復号すること) (ウ) (略) (b) (略) (削る) (c), (d) (略)	(2) 情報システムのセキュリティ要件の策定 (a) (略) (ア) (略) (イ)情報システム運用時の監視等の運用管理機能要件 (ウ) (略) (b) (略) (c) 情報システムセキュリティ責任者は、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。 (d), (e) (略)
(3) (略)	(3) (略)
(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) (略) (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。	(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) (略) (新設)
5.2.2 情報システムの調達・構築 目的・趣旨 (略)	5.2.2 情報システムの調達・構築 目的・趣旨 (略)
遵守事項 (1) (略)	遵守事項 (1) (略)
(2) (略)	(2) (略)
(3) 納品検査時の対策	(3) 納品検査時の対策

改定案	現行
(a) （略）	(a) （略）
(b) 情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。	（新設）
5.2.3～5.2.5 （略）	5.2.3～5.2.5 （略）
5.3 情報システムの運用継続計画	5.3 情報システムの運用継続計画
5.3.1 情報システムの運用継続計画の整備・整合的運用の確保	5.3.1 情報システムの運用継続計画の整備・整合的運用の確保
目的・趣旨	目的・趣旨
業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、国の行政機関においては、府省業務継続計画と情報システム運用継続計画を策定し運用している。独立行政法人及び指定法人においても、業務の特性に応じて、中期目標による指示等により、法人の業務継続計画と情報システムの運用継続計画を策定し運用している。	業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、府省庁において業務継続計画を策定し運用している。
非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。	一方、非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。
なお、こうした業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。	なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。
遵守事項	遵守事項
(1) 情報システムの運用継続計画の整備・整合的運用の確保	(1) 情報システムの運用継続計画の整備・整合的運用の確保
(a) 統括情報セキュリティ責任者は、機関等において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は、非常時における情報セキュリティに係る対策事項を検討すること。	(a) 統括情報セキュリティ責任者は、府省庁において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。
(b) （略）	(b) （略）

改定案	現行
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　主体認証機能 目的・趣旨 （略） また、機関等の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。 遵守事項 (1) 主体認証機能の導入 (a) （略） (b) 情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。 (c) （略） (2) （略） 6.1.2～6.1.5　（略） 6.2　情報セキュリティの脅威への対策 6.2.1　ソフトウェアに関する脆弱性対策 目的・趣旨 機関等の情報システムに対する脅威としては、第三者が情報システムに侵入し機関等の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、国民向けに提供するサービスが第三者に侵入され、個人情報等の重要な情	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　主体認証機能 目的・趣旨 （略） また、政府機関の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。 遵守事項 (1) 主体認証機能の導入 (a) （略） （新設） (b) （略） (2) （略） 6.1.2～6.1.5　（略） 6.2　情報セキュリティの脅威への対策 6.2.1　ソフトウェアに関する脆弱性対策 目的・趣旨 政府機関の情報システムに対する脅威としては、第三者が情報システムに侵入し政府の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、

改定案	現行
報の漏えい等が発生した場合、国民生活に多大な影響を及ぼすとともに機関等に対する社会的な信用が失われる。 （略） なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。 遵守事項 (1) ソフトウェアに関する脆弱性対策の実施 (a) （略） (b) 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施すること。 (c) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。 (d) 情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。 （削る） 6.2.2 （略）	国民向けに提供するサービスが第三者に侵入され、個人情報等の重要な情報の漏えい等が発生した場合、政府に対する社会的な信用が失われる。 （略） なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2 項「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。 遵守事項 (1) ソフトウェアに関する脆弱性対策の実施 (a) （略） (b) 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。 （新設） (c) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。 (d) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。 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。 遵守事項 (1)　サービス不能攻撃対策の実施 　(a)　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。 　(b), (c)　（略） 6.2.4　（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） 　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）	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、政府機関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。 遵守事項 (1)　サービス不能攻撃対策の実施 　(a)　情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この項において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。 　(b), (c)　（略） 6.2.4　（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） 　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 項「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）

改定案	現行
(ア), (イ)　(略) (ウ)実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと。 (エ)電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。 (オ), (カ)　(略) (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。	(ア), (イ)　(略) (ウ)実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。 (エ)電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。 (オ), (カ)　(略) (b) 行政事務従事者は、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 機関等では、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を用意し、国民等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の機関等のものであると確認できることが重要である。また、機関等になりすましたウェブサイトを放置しておくと、機関等の信用を損なうだけでなく、国民等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。	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 府省庁では、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を用意し、国民等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の府省庁のものであると確認できることが重要である。また、政府機関になりすましたウェブサイトを放置しておくと、政府機関の信用を損なうだけでなく、国民等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。
遵守事項 (1) 政府ドメイン名の使用 (a) 情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。ただし、次に掲げる場合を除く。	遵守事項 (1) 政府ドメイン名の使用 (a) 情報システムセキュリティ責任者は、府省庁外向けに提供するウェブサイト等が実際の府省庁提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用するよう仕様に含めること。ただし、4.1.3 項に掲げる場合を除く。

改定案	現行
(ア)指定法人が政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。 (イ)独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用する場合。この場合において、当該法人は、あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断すること。 (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。	(b) 行政事務従事者は、府省庁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、前号と同様、政府ドメイン名を使用するよう調達仕様に含めること。
(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。 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	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、行政事務従事者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。モバイル端末の利用に当たっては、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。 （新設）

改定案	現行
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) 端末の導入時の対策 (a) （略） （削る） (b) （略） (2), (3) （略） (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。	なお、本項の遵守事項のほか、6.1節「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項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、7.3.2項「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) 端末の導入時の対策 (a) （略） (b) 情報システムセキュリティ責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。 (c) （略） (2), (3) （略） （新設）

改定案	現行
(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。	
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	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。仮に政府機関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

改定案	現行
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。 　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」、6.2.3「サービス不能攻撃対策」、7.3.2「IPv6 通信回線」において定める遵守事項のうちサーバ装置に係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本款での共通的な対策に加え、それぞれ 7.2「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。 遵守事項　（略） 7.1.3　複合機・特定用途機器 目的・趣旨 （略） 　また、機関等においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の目的を達成するために必要な機能を有した特定用途機器が利用されている。さらに、特定用途機器の中には、インターネットに接続されるいわゆる IoT 機器があるが、近年 IoT 機器の脆弱性をついた攻撃が数多く発生しており、IoT 機器が踏み台となって他の情報システムへの攻撃に利用されるなど、社会的問題となってきている。このため、これらの機器に対する情報セキュリティ対策が必要となる。	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。 　なお、本項の遵守事項のほか、6.1 節「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 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、6.2.3 項「サービス不能攻撃対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本項での共通的な対策に加え、それぞれ 7.2 節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。 遵守事項　（略） 7.1.3　複合機・特定用途機器 目的・趣旨 （略） 　また、府省庁においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

改定案	現行
したがって、複合機やIoT機器を含む特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして適切に対策を講ずることが重要である。	したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。
遵守事項 (1)　(略)	遵守事項 (1)　(略)
(2) IoT機器を含む特定用途機器 (a)　(略)	(2) 特定用途機器 (a)　(略)
7.2　電子メール・ウェブ等 7.2.1　電子メール 目的・趣旨 (略) なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。	7.2　電子メール・ウェブ等 7.2.1　電子メール 目的・趣旨 (略) なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。
遵守事項 (1) 電子メールの導入時の対策 (a)～(c)　(略) (d) 情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。	遵守事項 (1) 電子メールの導入時の対策 (a)～(c)　(略) (新設)
7.2.2　ウェブ 目的・趣旨 (略) なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。	7.2.2　ウェブ 目的・趣旨 (略) なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項 (1) ウェブサーバの導入・運用時の対策 (a) （略） (ア)～(エ) （略） (オ)インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。 (b) （略） (2) （略） 7.2.3 ドメインネームシステム（DNS） 目的・趣旨 （略） なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。 遵守事項 （略） 7.2.4 データベース 目的・趣旨 本款における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。 （略） 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・暗号・電子署名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	遵守事項 (1) ウェブサーバの導入・運用時の対策 (a) （略） (ア)～(エ) （略） (オ)サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。 (b) （略） (2) （略） 7.2.3 ドメインネームシステム（DNS） 目的・趣旨 （略） なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。 遵守事項 （略） 7.2.4 データベース 目的・趣旨 本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。 （略） なお、本項の遵守事項のほか、6.1 節「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・暗号・電子署名等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「IPv6 通信回線」におい

改定案	現行
事項のうち、データベース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　（略） 7.3　通信回線 7.3.1　通信回線 目的・趣旨　（略） 遵守事項 (1) 通信回線の導入時の対策 (a)～(c) （略） (d) 情報システムセキュリティ責任者は、職員等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。機関等内通信回線へ機関等支給以外の端末を接続する際も同様とする。 (e)～(k) （略） (2)～(5) （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）	て定める遵守事項のうち、データベース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　（略） 7.3　通信回線 7.3.1　通信回線 目的・趣旨　（略） 遵守事項 (1) 通信回線の導入時の対策 (a)～(c) （略） (d) 情報システムセキュリティ責任者は、行政事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。 (e)～(k) （略） (2)～(5) （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）

改定案	現行
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	遵守事項
(1) 情報システムの利用に係る規定の整備	(1) 情報システムの利用に係る規定の整備
(a) （略）	(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。	(b) 統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した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安全管理措置に関する規定及び許可手続を定めること。
(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。	（新設）
(d) 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。当該手順には、以下の事項を含めること。	(c) 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。
(ア) 職員等は、国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体を使用すること。	
(イ) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措	（新設）

改定案	現行
置を講ずること。 (e) 統括情報セキュリティ責任者は、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際の許可手続を定めること。	
(2) （略）	(2) （略）
(3) 情報システムの利用時の基本的対策 (a)～(f) （略） (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。	(3) 情報システムの利用時の基本的対策 (a)～(f) （略） (g) 行政事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。 (h) 行政事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、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の許可を得ること。 （新設） （新設） （新設）
(4) 電子メール・ウェブの利用時の対策 (a) （略）	(4) 電子メール・ウェブの利用時の対策 (a) （略）

改定案	現行
(b) 職員等は、機関等外の者と電子メールにより情報を送受信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、次に掲げる場合は除く。 (ア)指定法人が、政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。 (イ)独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用すると判断する場合。 (ウ)電子メールを受信する機関等外の者が、職員等から送信された電子メールであることを認知できる場合（政府ドメイン名又は前二号に基づき取得したドメイン名が使用できない場合に限る。）。	(b) 行政事務従事者は、府省庁外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合は除く。
(c)～(f) （略）	(c)～(f) （略）
(5), (6) （略）	(5), (6) （略）
(7) 不正プログラム感染防止 (a) （略） (b) 職員等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断するなど、必要な措置を講ずること。	(7) 不正プログラム感染防止 (a) （略） (b) 行政事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。
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	8.2 府省庁支給以外の端末の利用 8.2.1 府省庁支給以外の端末の利用 目的・趣旨 行政事務の遂行においては、府省庁から支給された端末を用いて行政事務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

改定案	現行
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。 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。	府省庁支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は府省庁が支給したものではないという理由で、行政事務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、府省庁対策基準を満たさないおそれがある。 したがって、そのような可能性がある場合は、府省庁支給以外の端末を行政事務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、府省庁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。 また、府省庁支給以外の端末であっても、府省庁から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1 項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、行政事務従事者に安全管理措置を講じさせる必要がある。
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。	遵守事項 （新設）
(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。 （削る）	(1) 府省庁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、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。 (b) 統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

改定案	現行
（削る）	(c) 情報セキュリティ責任者は、府省庁支給以外の端末による行政事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を定めること。
（削る）	(d) 前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。
(3) 機関等支給以外の端末の利用時の対策	(2) 府省庁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。	(a) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項 8.2.1(1)(c)で定める責任者の許可を得ること。
（削る）	(b) 行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。
（削る）	(c) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。
(b) 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。	(d) 行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。