共通事項

統一基準

第３部 情報についての対策

3.1.1 情報の格付け

(1) 情報の格付け

3.1.1 (1) (a)	基本	情報セキュリティ委員会は、行政事務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備すること。

3.2.1 情報の作成と入手

(1) 業務以外の情報の作成又は入手の禁止

3.2.1 (1) (a)	基本	行政事務従事者は、行政事務の遂行以外の目的で、情報を作成し、又は入手しないこと。

(2) 情報の作成又は入手時における格付けの決定と取扱制限の検討

3.2.1 (2) (a)	基本	行政事務従事者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。
3.2.1 (2) (b)	基本	行政事務従事者は、府省庁外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

(3) 格付けと取扱制限の明示等

3.2.1 (3) (a)	基本	行政事務従事者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示等し、必要に応じて取扱制限についても明示等すること。

(4) 格付けと取扱制限の継承

3.2.1 (4) (a)	基本	行政事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

(5) 格付けと取扱制限の変更

3.2.1 (5) (a)	基本	行政事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。
3.2.1 (5) (b)	基本	行政事務従事者は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

3.2.2 情報の利用

(1) 業務以外の利用の禁止

3.2.2 (1) (a)	基本	行政事務従事者は、行政事務の遂行以外の目的で、情報を利用しないこと。

(2) 格付け及び取扱制限に従った情報の取扱い

3.2.2 (2) (a)	基本	行政事務従事者は、利用する情報に明示等された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。

(3) 要保護情報の取扱い

3.2.2 (3) (a)	基本	行政事務従事者は、行政事務の遂行以外の目的で、要保護情報を府省庁外に持ち出さないこと。
3.2.2 (3) (b)	基本	行政事務従事者は、要保護情報を放置しないこと。

3.2.2（3） (c)	基本	行政事務従事者は、機密性３情報を必要以上に複製しないこと。
3.2.2（3） (d)	基本	行政事務従事者は、要機密情報を必要以上に配付しないこと。
3.2.2（3） (e)	強化	行政事務従事者は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる必要性があると思料される場合には、格付けの変更に必要な処理を行うこと。
3.2.2（3） (f)	強化	行政事務従事者は、書面に印刷された機密性３情報には、一連番号を付し、その所在を明らかにしておくこと。

3.2.3 情報の保存

(1) 格付けに応じた情報の保存

3.2.3（1） (a)	基本	行政事務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。
3.2.3（1） (b)	基本	行政事務従事者は、情報の格付けに応じて、情報が保存された電磁的記録媒体を適切に管理すること。
3.2.3（1） (c)	基本	行政事務従事者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面のうち要機密情報を記載した書面、又は重要な設計書を適切に管理すること。
3.2.3（1） (d)	基本	行政事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
3.2.3（1） (e)	基本	行政事務従事者は、要保全情報を電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。
3.2.3（1） (f)	基本	行政事務従事者は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。
3.2.3（1） (g)	基本	行政事務従事者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。

(2) 情報の保存期間

3.2.3（2） (a)	基本	行政事務従事者は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

3.2.4 情報の移送

(1) 情報の移送に関する許可及び届出

3.2.4（1） (a)	基本	行政事務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する場合には、課室情報セキュリティ責任者の許可を得ること。
3.2.4（1） (b)	基本	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報を記載した書面を移送する場合には、課室情報セキュリティ責任者に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

(2) 情報の送信と運搬の選択

3.2.4（2） (a)	基本	行政事務従事者は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

(3) 移送手段の決定

3.2.4（3） (a)	基本	行政事務従事者は、要保護情報又は重要な設計書を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、課室情報セキュリティ責任者に届け出ること。ただし、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報を記載した書面の移送であり、課室情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

（4）書面に記載された情報の保護対策

3.2.4（4） (a)	基本	行政事務従事者は、要機密情報を記載した書面又は重要な設計書を運搬する場合には、情報の格付けなどに応じて、安全確保のための適切な措置を講ずること。

（5）電磁的記録の保護対策

3.2.4（5） (a)	基本	行政事務従事者は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。
3.2.4（5） (b)	基本	行政事務従事者は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
3.2.4（5） (c)	基本	行政事務従事者は、要保全情報である電磁的記録を移送する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。
3.2.4（5） (d)	基本	行政事務従事者は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めたときは、情報のバックアップを取得すること。
3.2.4（5） (e)	基本	行政事務従事者は、要安定情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。
3.2.4（5） (f)	強化	行政事務従事者は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること。

3.2.5 情報の提供

（1）情報の公表

3.2.5（1） (a)	基本	行政事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付けされるものであることを確認すること。
3.2.5（1） (b)	基本	行政事務従事者は、電磁的記録を公表する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。

（2）他者への情報の提供

3.2.5（2） (a)	基本	行政事務従事者は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を府省庁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。
3.2.5（2） (b)	基本	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報を記載した書面を府省庁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に届け出ること。ただし、課室情報セキュリティ責任者が届出を要しないと定めた提供については、この限りでない。
3.2.5（2） (c)	基本	行政事務従事者は、要保護情報又は重要な設計書を府省庁外の者に提供する場合には、提供先において、当該情報に付された情報の格付けに応じて適切に取り扱われるための措置を講ずること。
3.2.5（2） (d)	基本	行政事務従事者は、電磁的記録を提供する場合には、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。

3.2.6 情報の消去

（2）書面の廃棄方法

3.2.6（2） (a)	基本	行政事務従事者は、要機密情報を記載した書面を廃棄する場合には、復元が困難な状態にすること。

第４部　情報セキュリティ要件の明確化に基づく対策

4.3.1 情報システムのセキュリティ要件

(1) 情報システム計画・設計

4.3.1（1）（a）	基本	情報システムセキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ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。
4.3.1（1）（b）	基本	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を決定すること。
4.3.1（1）（c）	基本	情報システムセキュリティ責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。
4.3.1（1）（d）	基本	情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、情報システムを更改し、又は開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。
4.3.1（1）（e）	基本	情報システムセキュリティ責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。
4.3.1（1）（f）	強化	情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、その中から当該セキュリティ機能に関してITセキュリティ評価及び認証制度に基づく認証を取得している製品を情報システムの構成要素として選択すること。

(2) 情報システムの構築・運用・監視

4.3.1（2）（a）	基本	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、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。

(3) 情報システムの移行・廃棄

4.3.1（3）（a）	基本	情報システムセキュリティ責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。

(4) 情報システムの見直し

4.3.1（4）（a）	基本	情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

(5)　情報システムの台帳整備

4.3.1（5）（a）	基本	情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を統括情報セキュリティ責任者に報告すること。
4.3.1（5）（b）	基本	統括情報セキュリティ責任者は、すべての情報システムに対して、当該情報システムで取り扱う情報及び当該情報の格付けを含む事項を記載した台帳を整備すること。

第５部　情報システムの構成要素についての対策

5.1.1 電子計算機及び通信回線装置を設置する安全区域

(1) 立入り及び退出の管理

5.1.1（1）（a）	基本	情報システムセキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずること。

5.1.1（1） (b)	基本	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情報システムについては、安全区域を物理的に隔離し、立入り及び退出を管理するための措置を講ずること。
5.1.1（1） (c)	強化	情報システムセキュリティ責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。
5.1.1（1） (d)	強化	情報システムセキュリティ責任者は、安全区域から退出する者の主体認証を行うための措置を講ずること。
5.1.1（1） (e)	強化	情報システムセキュリティ責任者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。
5.1.1（1） (f)	強化	情報システムセキュリティ責任者は、安全区域へ継続的に立ち入る者を承認する手続を整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載するための文書を整備すること。
5.1.1（1） (g)	強化	情報システムセキュリティ責任者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。
5.1.1（1） (h)	強化	情報システムセキュリティ責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。

（2）訪問者及び受渡業者の管理

5.1.1（2） (a)	強化	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。
5.1.1（2） (b)	強化	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。
5.1.1（2） (c)	強化	情報システムセキュリティ責任者は、安全区域への訪問者がある場合には、訪問相手の行政事務従事者が訪問者の安全区域への立入りについて審査するための手続を整備すること。
5.1.1（2） (d)	強化	情報システムセキュリティ責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。
5.1.1（2） (e)	強化	情報システムセキュリティ責任者は、安全区域内において訪問相手の行政事務従事者が訪問者に付き添うための措置を講ずること。
5.1.1（2） (f)	強化	情報システムセキュリティ責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。
5.1.1（2） (g)	強化	情報システムセキュリティ責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。（ア）安全区域外で受渡しを行うこと。（イ）業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、記録媒体に触れることができない場所に限定し、行政事務従事者が立ち会うこと。

（3）電子計算機及び通信回線装置のセキュリティ確保

5.1.1（3） (b)	強化	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情報システムについては、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。

（4）安全区域内のセキュリティ管理

5.1.1（4） (a)	基本	行政事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。
5.1.1（4） (e)	強化	情報システムセキュリティ責任者は、安全区域内での作業を監視するための措置を講ずること。

（5）災害及び障害への対策

5.1.1（5） (b)	強化	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については、安全区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

5.2.1 電子計算機共通対策

(1) 電子計算機の設置時

5.2.1 (1) (a)	基本	情報システムセキュリティ責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。
5.2.1 (1) (c)	基本	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電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。
5.2.1 (1) (d)	基本	情報システムセキュリティ責任者は、電子計算機について、情報セキュリティについての機能の必要性の有無を検討すること。
5.2.1 (1) (e)	基本	情報システムセキュリティ責任者は、情報セキュリティについての機能の必要性があると認めた電子計算機について、当該機能を設けること。
5.2.1 (1) (h)	基本	情報システムセキュリティ責任者は、電子計算機関連文書を整備すること。
5.2.1 (1) (j)	強化	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については、サービス提供に必要な電子計算機を冗長構成にすること。

(2) 電子計算機の運用時

5.2.1 (2) (a)	基本	情報システムセキュリティ管理者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。
5.2.1 (2) (b)	基本	情報システムセキュリティ責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。
5.2.1 (2) (d)	基本	情報システムセキュリティ責任者は、電子計算機を管理する行政事務従事者及び利用者を変更した場合には、当該変更の内容を、電子計算機を管理する行政事務従事者及び利用者を特定するための文書へ反映すること。また、当該変更の記録を保存すること。
5.2.1 (2) (g)	基本	情報システムセキュリティ責任者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

第６部　個別事項についての対策

6.1.1 機器等の購入

(1)　情報セキュリティ確保のための府省庁内共通の仕組みの整備（6.1.1）

6.1.1 (1) (a)	基本	統括情報セキュリティ責任者は、機器等の選定基準を整備すること。
6.1.1 (1) (b)	基本	統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

(2)　機器等の購入の実施における手続

6.1.1 (2) (a)	基本	情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。
6.1.1 (2) (b)	基本	情報システムセキュリティ責任者は、機器等の納入時において、納入された機器等が選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加えること。
6.1.1 (2) (c)	基本	情報システムセキュリティ責任者は、機器等の納入後の情報セキュリティ対策に関する保守・点検等の必要性の有無を検討し、必要と認めた場合には、実施条件を明確にし、それらの実施者である機器等の購入先又は他の事業者との間で、その内容に関する契約を取り交わすこと。
6.1.1 (2) (d)	基本	情報システムセキュリティ責任者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行うときは、これについて、ITセキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。

6.1.2 外部委託

(1) 情報セキュリティ確保のための府省庁内共通の仕組みの整備（6.1.2）

6.1.2（1） (a)	基本	統括情報セキュリティ責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。
6.1.2（1） (b)	基本	統括情報セキュリティ責任者は、委託先の選定手続及び選定基準を整備すること。
6.1.2（1） (c)	強化	統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

(2) 委託先に実施させる情報セキュリティ対策の明確化

6.1.2（2） (a)	基本	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、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を明確にし、委託先候補に事前に周知すること。
6.1.2（2） (b)	基本	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、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法を整備し、委託先候補に事前に周知すること。
6.1.2（2） (c)	基本	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、委託先における情報セキュリティ対策の履行状況を確認するための方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を整備し、委託先候補に事前に周知すること。

(3) 委託先の選定

6.1.2（3） (a)	基本	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、選定手続及び選定基準に基づき、委託先を選定すること。
6.1.2（3） (b)	強化	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、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法に従って、委託先の候補者の情報セキュリティ水準を確認し、委託先の選定における評価の一要素として利用すること。

(4) 外部委託に係る契約

6.1.2（4） (a)	基本	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、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を当該契約に含めること。（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
6.1.2（4） (b)	基本	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、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めること。（ア）当該委託業務に携わる者の特定（イ）遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容
6.1.2（4） (c)	基本	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、外部委託契約の継続に関しては、選定手続及び選定基準に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。
6.1.2（4） (d)	基本	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、委託先の提供するサービス（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定手続及び選定基準に基づき、その是非を審査すること。

(5) 外部委託の実施における手続

6.1.2（5） (b)	基本	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、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、定められた対処方法に従い、委託先に必要な措置を講じさせること。
6.1.2（5） (c)	基本	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、定められた方法に従い、委託先における情報セキュリティ対策の履行状況を確認すること。

（6） 外部委託終了時の手続

6.1.2（6）（a）	基本	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、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。

6.1.3 ソフトウェア開発

（1）ソフトウェア開発体制の確立時

6.1.3（1）（a）	基本	情報システムセキュリティ責任者は、ソフトウェア開発について、セキュリティにかかわる対策事項（本項（2）から（5）の遵守事項）を満たすことが可能な開発体制の確保を、情報システムを統括する責任者に求めること。
6.1.3（1）（b）	基本	情報システムセキュリティ責任者は、ソフトウェア開発を外部委託する場合には、委託先が実施すべき対策事項（本項（2）から（5）の遵守事項）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

（2）ソフトウェア開発の開始時

6.1.3（2）（a）	基本	情報システムセキュリティ責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。
6.1.3（2）（b）	基本	情報システムセキュリティ責任者は、ソフトウェアの開発及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。

（3）ソフトウェアの設計時

6.1.3（3）（c）	基本	情報システムセキュリティ責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。
6.1.3（3）（e）	基本	情報システムセキュリティ責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書のST評価・ST確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

（4）ソフトウェアの作成時

6.1.3（4）（c）	強化	情報システムセキュリティ責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

（5）ソフトウェアの試験時

6.1.3（5）（b）	基本	情報システムセキュリティ責任者は、情報セキュリティの観点から実施した試験の実施記録を保存すること。

6.2.1 府省庁外での情報処理の制限

（1） 安全管理措置についての規定の整備（6.2.1）

6.2.1（1）（a）	基本	統括情報セキュリティ責任者は、要保護情報について府省庁外での情報処理を行う場合の安全管理措置についての規定を整備すること。
6.2.1（1）（b）	基本	統括情報セキュリティ責任者は、要保護情報を取り扱う情報システムを府省庁外に持ち出す場合の安全管理措置についての規定を整備すること。

（2）許可及び届出の取得及び管理（6.2.1）

6.2.1（2） (a)	基本	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁外で情報処理を行う場合には、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。
6.2.1（2） (b)	基本	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外で情報処理を行う場合には、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に届け出ること。
6.2.1（2） (c)	基本	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は、府省庁外での要保護情報の情報処理に係る記録を取得すること。
6.2.1（2） (d)	基本	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は、機密性３情報、完全性２情報又は可用性２情報について府省庁外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。
6.2.1（2） (e)	基本	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は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。
6.2.1（2） (f)	基本	行政事務従事者は、要保護情報について府省庁外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。
6.2.1（2） (g)	基本	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁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。
6.2.1（2） (h)	基本	行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを府省庁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に届け出ること。
6.2.1（2） (i)	基本	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は、要保護情報を取り扱う情報システムの府省庁外への持出しに係る記録を取得すること。
6.2.1（2） (j)	基本	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は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。
6.2.1（2） (k)	基本	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は、機密性２情報であって完全性１情報かつ可用性１情報である情報を取り扱う情報システムを府省庁外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。
6.2.1（2） (l)	基本	行政事務従事者は、要保護情報を取り扱う情報システムを府省庁外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持出しにとどめること。

（3）安全管理措置の遵守（6.2.1）

6.2.1（3） (a)	基本	行政事務従事者は、要保護情報について府省庁外での情報処理について定められた安全管理措置を講ずること。
6.2.1（3） (b)	基本	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。
6.2.1（3） (d)	基本	行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報を取り扱う情報システムを府省庁外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

6.2.2 府省庁支給以外の情報システムによる情報処理の制限

（1） 安全管理措置についての規定の整備（6.2.2）

6.2.2（1） (a) 基本 統括情報セキュリティ責任者は、要保護情報について府省庁支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

（2）許可及び届出の取得及び管理（6.2.2）

6.2.2（2） (a) 基本 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、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。

6.2.2（2） (b) 基本 行政事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムにより情報処理を行う必要がある場合には、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に届け出ること。

6.2.2（2） (c) 基本 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は、府省庁支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。

6.2.2（2） (d) 基本 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は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

6.2.2（2） (e) 基本 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は、機密性２情報であって完全性１情報かつ可用性１情報である情報について府省庁支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

（3）安全管理措置の遵守（6.2.2）

6.2.2（3） (a) 基本 行政事務従事者は、要保護情報について府省庁支給以外の情報システムによる情報処理を行う場合には、当該情報システムについて定められた安全管理措置を講ずること。

6.2.2（3） (b) 基本 行政事務従事者は、機密性３情報、完全性２情報又は可用性２情報について府省庁支給以外の情報システムによる情報処理を終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

6.3.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止

（1） 措置についての規定の整備

6.3.1（1） (a) 基本 統括情報セキュリティ責任者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。

（2） 措置の遵守

6.3.1（2） (a) 基本 行政事務従事者は、府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずること。

S1の公開Webサーバの導入

統一基準

第４部 情報セキュリティ要件の明確化に基づく対策

4.1.1主体認証機能

(1) 主体認証機能の導入

4.1.1（1） (a)	基本	情報システムセキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。
4.1.1（1） (b)	基本	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。
4.1.1（1） (d)	基本	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。（ア）利用者が定期的に変更しているか否かを確認する機能（イ）利用者が定期的に変更しなければ、情報システムの利用を継続させない機能
4.1.1（1） (e)	基本	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。
4.1.1（1） (g)	基本	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項が適用可能かどうかを検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。（ア）正当な主体以外の主体認証を受諾しないこと。（誤認の防止）（イ）正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）（ウ）正当な主体が容易に他者に主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）（エ）主体認証情報が容易に複製できないこと。（複製の防止）（オ）情報システムセキュリティ管理者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）（カ）必要時に中断することなく主体認証が可能であること。（可用性の確保）（キ）新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）（ク）主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）
4.1.1（1） (m)	強化	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。
4.1.1（1） (n)	強化	情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を設けること。

4.1.2 アクセス制御機能

(1) アクセス制御機能の導入

4.1.2（1） (a)	基本	情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。
4.1.2（1） (b)	基本	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。

4.1.2（1） (c)	強化	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。
4.1.2（1） (d)	強化	情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。

4.1.3 権限管理機能

（1）権限管理機能の導入

4.1.3（1） (a)	基本	情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。
4.1.3（1） (b)	基本	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。
4.1.3（1） (c)	強化	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。
4.1.3（1） (d)	強化	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、主体認証情報の再発行を自動で行う機能を設けること。

4.1.4 証跡管理機能

（1）証跡管理機能の導入

4.1.4（1） (a)	基本	情報システムセキュリティ責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。
4.1.4（1） (c)	基本	情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。
4.1.4（1） (d)	基本	情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。
4.1.4（1） (f)	強化	情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。

4.1.5保証のための機能

（1）保証のための機能の導入

4.1.5（1） (a)	基本	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情報システムについて、保証のための対策を行う必要性の有無を検討すること。
4.1.5（1） (b)	基本	情報システムセキュリティ責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。

4.1.6 暗号と電子署名（鍵管理を含む）

（1） 暗号化機能及び電子署名の付与に係る方式の整備

4.1.6（1） (a)	基本	統括情報セキュリティ責任者は、府省庁において使用する暗号化及び電子署名の付与について、そのアルゴリズム及び実装方式を定めること。
4.1.6（1） (b)	基本	統括情報セキュリティ責任者は、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。なお、複数のアルゴリズムが選択可能な場合には、少なくとも一つを電子政府推奨暗号リストの中から選択すること。

4.1.6（1） (c)	基本	統括情報セキュリティ責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等（以下「鍵の管理手順等」という。）を定めること。
4.1.6（1） (d)	基本	統括情報セキュリティ責任者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存方法及び保存場所（以下「鍵の保存方法等」という。）を定めること。

（2）暗号化機能及び電子署名の付与機能の導入

4.1.6（2） (a)	基本	情報システムセキュリティ責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。
4.1.6（2） (b)	基本	情報システムセキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。
4.1.6（2） (c)	基本	情報システムセキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。
4.1.6（2） (d)	基本	情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。
4.1.6（2） (e)	強化	情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。

第５部　情報システムの構成要素についての対策

5.2.3 サーバ装置

（1）サーバ装置の設置時

5.2.3（1） (a)	基本	情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化すること。
5.2.3（1） (b)	基本	情報システムセキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。
5.2.3（1） (c)	基本	情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。

5.3.1 通信回線を介して提供するアプリケーション共通対策

（1）アプリケーションの導入時

5.3.1（1） (a)	基本	情報システムセキュリティ責任者は、通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備すること。

5.3.3 ウェブ

（1）ウェブの導入時

5.3.3（1） (e)	強化	情報システムセキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。

5.4.1 通信回線共通対策

（1）通信回線の構築時

5.4.1（1） (i)	基本	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

S1の公開Webサーバの運用

統一基準

第４部　情報セキュリティ要件の明確化に基づく対策

4.1.1主体認証機能

（2） 識別コードの管理

4.1.1（2）（b）	基本	行政事務従事者は、自己に付与された識別コードを他者に付与及び貸与しないこと。
4.1.1（2）（c）	基本	行政事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。
4.1.1（2）（d）	基本	行政事務従事者は、行政事務のために識別コードを利用する必要がなくなった場合は、その旨を情報システムセキュリティ管理者に届け出ること。ただし、個別の届出が必要ないと、情報システムセキュリティ責任者が定めている場合は、この限りでない。
4.1.1（2）（e）	強化	行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

4.1.3 権限管理機能

（2）識別コードと主体認証情報の付与管理

4.1.3（2）（a）	基本	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。
4.1.3（2）（b）	基本	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を明確にすること。（ア）主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続（イ）主体認証情報の初期配布方法及び変更管理手続（ウ）アクセス制御情報の設定方法及び変更管理手続
4.1.3（2）（c）	基本	情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。
4.1.3（2）（d）	基本	権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。
4.1.3（2）（e）	基本	権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。
4.1.3（2）（f）	基本	権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（発行、更新及び変更を含む。以下この項において同じ。）すること。
4.1.3（2）（g）	基本	権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。
4.1.3（2）（h）	基本	権限管理を行う者は、行政事務従事者が情報システムを利用する必要がなくなった場合には、当該行政事務従事者に交付した主体認証情報格納装置を返還させること。
4.1.3（2）（i）	基本	権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。
4.1.3（2）（j）	強化	権限管理を行う者は、単一の情報システムにおいては、１人の行政事務従事者に対して単一の識別コードのみを付与すること。
4.1.3（2）（k）	強化	権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、情報セキュリティ責任者からの事前の承認を得ること。

4.1.3（2） (1) 強化 権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。

（3） 識別コードと主体認証情報における代替手段等の適用

4.1.3（3） (a) 基本 情報システムセキュリティ管理者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった行政事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。

4.1.4 証跡管理機能

（2） 証跡の取得と保存

4.1.4（2） (a) 基本 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ責任者が情報システムに設けた機能を利用して、証跡を記録すること。

4.1.4（2） (b) 基本 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

4.1.4（2） (c) 基本 情報システムセキュリティ管理者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対応すること。

（3）取得した証跡の点検、分析及び報告

4.1.4（3） (a) 強化 情報セキュリティ責任者又は情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ統括情報セキュリティ責任者若しくは情報セキュリティ責任者に報告すること。

（4）証跡管理に関する利用者への周知

4.1.4（4） (a) 基本 情報セキュリティ責任者又は情報システムセキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムセキュリティ管理者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

4.2.1 セキュリティホール対策

（2）情報システムの運用時（4.2.1）

4.2.1（2） (a) 基本 情報システムセキュリティ責任者は、電子計算機及び通信回線装置の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した文書を更新すること。

4.2.1（2） (b) 基本 情報システムセキュリティ管理者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。

4.2.2 不正プログラム対策

（2）情報システムの運用時（4.2.2）

4.2.2（2） (h) 基本 情報セキュリティ責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。

4.2.3 サービス不能攻撃対策

（2）情報システムの運用時（4.2.3）

4.2.3（2） (a) 強化 情報システムセキュリティ管理者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

4.2.4 踏み台対策

（2）情報システムの運用時（4.2.4）

4.2.4（2） (a)	強化	情報システムセキュリティ管理者は、定められた監視方法に従って情報システムを監視し、その記録を保存すること。

第５部 情報システムの構成要素についての対策

5.2.3 サーバ装置

（2）サーバ装置の運用時

5.2.3（2） (c)	基本	情報システムセキュリティ管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。
5.2.3（2） (d)	基本	情報システムセキュリティ責任者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。
5.2.3（2） (e)	基本	情報システムセキュリティ管理者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。
5.2.3（2） (g)	強化	情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。

5.3.1 通信回線を介して提供するアプリケーション共通対策

（2）アプリケーションの運用時

5.3.1（2） (a)	基本	情報システムセキュリティ管理者は、サービスのセキュリティ維持に関する規定に基づいて、日常的及び定期的に運用管理を実施すること。

5.3.3 ウェブ

（2）ウェブの運用時

5.3.3（2） (a)	基本	行政事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

S1の公開Webサーバの廃棄

統一基準

第３部　情報についての対策

3.2.6 情報の消去

（1）電磁的記録の消去方法

3.2.6（1）（b）	基本	行政事務従事者は、電磁的記録媒体を他の者へ提供する場合には、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。
3.2.6（1）（c）	強化	行政事務従事者は、電磁的記録媒体について、設置環境等から必要があると認められる場合は、当該電磁的記録媒体の要機密情報を抹消すること。