資料 1-2

政府機関の情報セキュリティ対策のための統一規範（案）

平成 23 年 4 月 21 日
平成 24 年　月　日改定
情報セキュリティ政策会議決定

第一章　目的及び対象

（目的）

第一条　本規範は、政府機関の情報セキュリティを確保するため、政府機関のとるべき対策の統一的な枠組みを定め、各政府機関が自らの責任において対策を図るための措置を講ずることにより、もって政府機関全体の情報セキュリティ対策の強化・拡充を図ることを目的とする。

（対象）

第二条　本規範の対象となる政府機関は、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若しくはこれらに置かれる機関（以下「府省庁」という。）とする。

2　本規範の対象となる情報は、情報処理及び通信に係るシステム（以下「情報システム」という。）内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報とする。

3　本規範の対象となる者は、政府職員（府省庁において行政事務に従事している国家公務員をいう。）及びそれぞれの府省庁の指揮命令に服している者のうち、それぞれの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（以下「行政事務従事者」という。）とする。

4　本規範の対象となる情報の格付の区分は、機密性、完全性、可用性について、別表に掲げるものとする。

第二章　政府機関の情報セキュリティ対策のための基本指針

（リスク評価）

第三条　各府省庁は、別に定める政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針（以下「運用指針」という。）に基づき、当該府省庁の保有する情報及び利用する情報システム並びに当該情報及び情報システムに係る脅威を明らかにし、情報及び情報システムごとにその重要性、利用環境等を考慮したリスクの評価（以下「リスク評価」という。）を行った上で、必要となる情報セキュリティ対策の水準を決定しなければならない。

２　評価を行ったリスクに変化が生じた場合は、前項のリスク評価及び対策の水準を見直さなければならない。

（省庁情報セキュリティ文書）

第四条　各府省庁は、当該府省庁の特性を踏まえつつ、本規範に準拠して府省庁における情報セキュリティ対策の基本的な方針（以下「省庁基本方針」という。）及び情報セキュリティ対策基準（以下「省庁対策基準」という。）を定めなければならない。省庁基本方針及び省庁対策基準（以下「省庁基準」という。）の呼称は各府省庁で独自に定めることができる。

２　省庁基本方針は、本規範と同等以上の情報セキュリティの管理が可能となるように定めなければならない。

３　省庁対策基準は、別に定める政府機関の情報セキュリティ対策のための統一管理基準（以下「統一管理基準」という。）及び政府機関の情報セキュリティ対策のための統一技術基準（以下「統一技術基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。

４　各府省庁は、前条に規定したリスク評価の結果を踏まえ、省庁基本方針及び省庁対策基準の評価及び見直しを行わなければならない。

第三章　政府機関の情報セキュリティ対策のための基本対策

（管理体制）

第五条　各府省庁は、情報セキュリティ対策を実施するための組織・体制を整備しなければならない。

２　各府省庁は、最高情報セキュリティ責任者を１人置かなければならない。

３　最高情報セキュリティ責任者は、省庁基準の策定等を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置かなければならない。

４　最高情報セキュリティ責任者は、本規範にて規定した当該府省庁における情報セキュリティ対策に関する事務を統括し、当該府省庁の行政事務従事者に対して、別表に掲げる情報セキュリティ対策を講じさせなければならない。

5　最高情報セキュリティ責任者は、前項に係る措置について、統一管理基準に定める責任者及び管理者に分掌させることができる。

（例外措置）

第六条　各府省庁は、省庁基準に定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を省庁基準の中で定めなければならない。

（教育）

第七条　各府省庁は、行政事務従事者に対し、自らが自覚をもって省庁基準に定めた情報セキュリティ対策を実施するために、情報セキュリティに関する教育を行わなくてはならない。

（障害・事故等への対応）

第八条　各府省庁は、情報セキュリティに関する障害・事故等（以下「障害・事故等」という。）の発生又はそのおそれがある場合に備えた必要な措置を講じなければならない。

2　障害・事故等の発生を知った者は、省庁基準に定める責任者に報告を行わなければならない。

3　省庁基準に定める責任者は、障害・事故等の発生の報告を受け又は自ら知ったときは、必要な措置を講じなければならない。

（自己点検）

第九条　各府省庁は、情報セキュリティ対策の自己点検を行わなければならない。

（監査）

第十条　各府省庁は、省庁基準が統一規範に準拠し、かつ実際の運用が省庁基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。

（情報セキュリティ報告書）

第十一条　各府省庁は、自己点検及び監査の結果を反映した情報セキュリティ報告書を毎年度作成し、公表しなければならない。報告書の構成、細目は別に定める。

2　各府省庁は、作成した情報セキュリティ報告書に基づいて省庁基準を見直し、必要な措置を講じなければならない。

（外部委託）

第十二条　各府省庁は、情報処理に係る業務を外部委託する際には、必要な措置を定め、実施しなければならない。

（業務継続計画及び情報システム運用継続計画）

第十三条　各府省庁は、業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性確保のための検討を行わなければならない。

2　各府省庁は、業務継続計画及び情報システム運用継続計画を整備する場合には、当該業務継続計画及び情報システム運用継続計画と関係があると認めた情報システムについて、業務継続計画及び情報システム運用継続計画との整合性を考慮し、必要な措置を講じなければならない。

（情報の格付）

第十四条　各府省庁は、取り扱う情報に、機密性、完全性、可用性の観点から格付を付さねばならない。

2　各府省庁は、府省庁間での情報の移送、提供に際しては、第二条第四項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。

（情報の取扱制限）

第十五条　各府省庁は、情報の格付に応じた取扱制限の種類を定めなければならない。

2　各府省庁は、取り扱う情報に、前項で定めた取扱制限を付さねばならない。

3　各府省庁は、府省庁間での情報の移送、提供に際しては、情報の取扱制限を明示等しなければならない。

（情報のライフサイクル管理）

第十六条　各府省庁は、情報の作成、入手、利用、保存、移送、提供及び消去の各段階で、情報の格付の区分及び取扱制限の種類に応じて必要とされる取扱いが損なわれることがないように、別表に基づき、必要な措置を定め、実施しなければならない。

（情報システムの利用管理）

第十七条　各府省庁は、情報システムの利用者及びその利用範囲を定め、その適切な確認を行うために、必要な措置を定め、実施しなければならない。

（情報取扱区域）

第十八条　各府省庁は、府省庁の内外において情報を取り扱う区域を「情報取扱区域」とし、区分を定めるとともに、求める対策及び利用の制限を整備しなければならない。

（情報システムのライフサイクル管理）

第十九条　各府省庁は、所管する情報システムの計画、構築・運用、移行・廃棄及び見直しの各段階において情報セキュリティを確保するための措置を定め、実施しなければならない。

（情報システムに係る文書及び台帳整備）

第二十条　各府省庁は、所管する情報システムに係る文書及び台帳を整備しなければならない。

（機器等の購入及びソフトウェア開発・運用・保守）

第二十一条　各府省庁は、機器等の購入及びソフトウェア開発・運用・保守について、必要な措置を定め、実施しなければならない。

（暗号・電子署名）

第二十二条　各府省庁は、府省庁における暗号及び電子署名の利用について、必要な措置を定め、実施しなければならない。

（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）

第二十三条　各府省庁は、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ついて、必要な措置を定め、実施しなければならない。

（統一管理基準及び統一技術基準への委任）

第二十四条　本規範に特別の規定があるものを除くほか、本規範の実施のための手続その他その執行について必要な細則は、統一管理基準及び統一技術基準で定める。

附則

第一条　内閣官房情報セキュリティセンターは、統一規範に基づいた府省庁の情報セキュリティ対策について必要な範囲で検査し、評価する。

2　内閣官房情報セキュリティセンターは、毎年度前項の評価を取りまとめて情報セキュリティ政策会議に報告し、その概要を公表するものとする。

第二条　情報セキュリティ政策会議は、統一規範決定後一年後を目途として、新たな脅威の発生や府省庁における運用の結果を踏まえて検討し、その結果に基づいて必要な措置を講ずる。

第三条　政府機関の情報セキュリティ対策の強化に関する基本方針（平成 17 年9月 15 日情報セキュリティ政策会議決定）は廃止する。

別表（第二条第四項関係）

機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

格付の区分	分類の基準
完全性２情報	行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

別表　（第五条第四項及び第十六条関係）

〔行政事務従事者の遵守事項〕

（情報の作成と入手及び利用時の対策）

一　情報の作成や変更時等に格付及び取扱制限を決定及び明示等するとともに、明示された格付及び取扱制限に従って情報を取り扱うこと。

（情報の保存時の対策）

二　要機密情報を保存する際は、読取制限の属性を付与したり、アクセスが限定された共有フォルダに保存する等の適切なアクセス制御を行うこと。また、要保全情報を保存する際は、上書き禁止の属性を付与する等の適切なアクセス制御を行うこと。

三　要機密情報を含む電磁的記録媒体、書類又は重要な設計書については、施錠ができる書庫・保管庫に保存する等の適切な保存を行うこと。

（情報の送信又は運搬時の対策）

四　要機密情報を電磁的記録媒体に保存する際並びに情報を送信又は運搬する際には、必要に応じて、パスワードによる保護又は情報の暗号化を実施すること。

五　要保全情報を電磁的記録媒体に保存する際並びに情報を送信又は運搬する際には、必要に応じて、電子署名を付与すること。

（情報のバックアップ）

六　業務に係る情報の滅失等が、業務の遂行に影響を与える可能性が高いと判断される場合、適切な頻度でバックアップ又は複写を取得すること。

（情報の保存期間の対策）

七　業務に係る情報は、定められた保存期間に従って保存し、保存期間の延長が不要な際には速やかに消去すること。

（情報の提供時の対策）

八　要機密情報を自府省庁の要管理対策区域外に送信又は運搬あるいは提供する場合は、手順に従い、第五条第五項に規定した責任者に許可又は届出を行うこと。

九　電磁的記録を公表又は提供する場合は、ファイルのプロパティ等に含まれる作成者名、組織名、作成履歴等、公表に不要な付加情報を削除する等、不用意な情報漏えいを防止するための措置を講じること。

十　自府省庁の行政事務従事者以外の者に情報を提供する場合は、格付及び取扱制限の意

味も含めて伝達すること。

（情報の消去時の対策）

十一　電磁的記録媒体や書面を廃棄する場合は、全ての情報を抹消すること。

（府省庁支給以外の情報システムによる情報処理又は要管理対策区域外での情報処理の対策）

十二　要管理対策区域外に情報システムを持ち出して情報処理を行う時は、情報の格付に従い、第五条第五項に規定した責任者に許可又は届出を行うこと。

十三　府省庁支給以外の情報システムにより情報処理を実施する時は、情報の格付に従い、第五条第五項に規定した責任者に許可又は届出を行うこと。

（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）

十四　国民等、自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規定に従うこと。

十五　国民等、自府省庁外の者に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、「.go.jp」で終わるドメイン名を使用すること。

（不正プログラム感染及び拡大の防止）

十六　不正プログラムの感染防止のため以下の行為を行わないこと。

・安全性が確実ではないファイルをダウンロードする。
・安全性が確実ではないファイルを移送、提供等する。
・安全性が確実ではないファイルを開き、あるいは実行する。

十七　不正プログラムに感染した恐れがある場合には、当該電子計算機の通信回線への接続を速やかに切断し、第五条第五項に規定した責任者等に連絡し、その指示に従うこと。

（識別コード又は主体認証情報等の管理）

十八　主体認証情報（パスワード等）の管理に当たって、「他者に知られない」「他者に教えない」「忘れない」「容易に推測可能なものを用いない」「定期的に更新する」ことを徹底すること。

十九　主体認証情報格納装置（IC カード等）の管理に当たって、「他者に貸与しない」「紛失しない」こと。

二十　識別コード（ユーザ ID 等）が不要になった場合又は主体認証情報が他者に使用された（又は使用される危険性が生じた）場合には、直ちに第五条第五項に規定した管理者に届け出ること。

（身分証明書の明示）

二十一　要管理対策区域内において、身分証明書を他の行政事務従事者が常時視認できるようにすること。

（端末の利用時の対策）

二十二　モバイル端末を利用する際、第五条第五項に規定した責任者の承認を得るとともに、要機密情報は必要最低限のものだけを自府省庁の要管理対策区域外に持ち出すよう心がけ、必要に応じて暗号化する等、適切に利用すること。

二十三　端末を業務目的のみで使用し、端末において利用可能と定められたソフトウェアのみを利用すること。

（通信回線の利用時の対策）

二十四　許可されていない電子計算機及び通信回線装置を通信回線に接続せず、許可された通信回線のみを利用すること。

（電子メールの利用時の対策）

二十五　業務情報を含む電子メールを送受信する場合には、第五条第五項に規定した責任者が指定（自府省庁によって運営又は外部委託されているものをいう。）した電子メールサービスを利用すること。また、受信メールはテキストで表示すること。

（ウェブの利用時の対策）

二十六　ウェブブラウザのセキュリティ設定を適切に行うこと。（あらかじめ第五条第五項に規定した管理者が設定している場合には、それに従って適切に使用すること。）

二十七　ウェブサイトに要機密情報を入力して送信する場合は、次の事項を確認すること。

(a)送信内容が暗号化されていること。（ウェブブラウザの鍵アイコン表示等による確認）

(b)送信先が想定している組織のウェブサイト（サイト証明書等による確認）

（兼務の禁止）

二十八　情報セキュリティについての責任者（又はその上司）の立場にあって、情報セキュリティに関する申請を自らが行う場合には、自分以外の適切な承認権限者に申請すること。

（情報セキュリティ対策の教育）

二十九　情報セキュリティ対策についての教育を、年に一度は受講すること。また、異動で新しい職場等に着任した場合は、その事実が発生した日から三か月以内に、異動先の

課室情報セキュリティ責任者に教育の受講方法を確認すること。（新たに第五条第五項に規定した責任者又は管理者となった場合は、それぞれの職務に応じた情報セキュリティ対策についての教育も含む。）

（障害・事故等の対処）

三十　障害等の発生を確認した場合、第五条第五項に規定した責任者に連絡するとともに対処手順等に従いその対処に努めること。

（外部委託時の対策）

三十一　委託先に業務に係る情報を提供する場合は、必要最小限とし、外部委託終了時には委託先に不要な情報を返却、廃棄又は抹消をさせること。