セキュリティ規程

平成15年10月　1日 規程第15－47号
改正:平成16年　3月29日 規程第16－27号
改正:平成16年　6月29日 規程第16－39号
改正:平成16年11月　1日 規程第16－55号
改正:平成17年　5月12日 規程第17－46号
改正:平成17年　7月19日 規程第17－69号
改正:平成17年　9月30日 規程第17－105号
改正:平成18年　4月25日 規程第18－28号
改正:平成19年　4月　4日 規程第19－13号
改正:平成19年　8月　8日 規程第19－62号
改正:平成20年　3月25日 規程第20―25号
改正:平成21年10月20日 規程第21－43号
改正:平成22年4月14日 規程第22－32号
改正:平成23年11月30日 規程第23－53号
改正:平成25年3月28日 規程第25－19号
改正:平成26年3月27日 規程第26－16号

目次

第 1 章　総則

（目的）

第 1 条　この規程は、国立研究開発法人宇宙航空研究開発機構(以下「機構」という。)の管理する区域における秩序の維持、適正かつ円滑な業務の遂行の確保、ロケット、人工衛星、航空機、施設設備その他の重要な資産及び重要な情報の防護を行うため、必要な基本的事項を定め、もって機構のセキュリティの確保を図ることを目的とする。

（適用範囲等）

第2条　機構のセキュリティ確保に関する事項ついては、別に定めるところによるほか、この規程の定めるところによる。

2　機構が、受託業務を実施する場合において、委託者から委託契約に基づいてセキュリティに係る要求があり、理事長がこれを認めたときは、本規程によらず、当該要求に基づきセキュリティ管理を行うものとする。

（定義）

第3条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（1）「職員」とは、就業規則(規程第 15―23 号)及び就業特則(規程第 15―24 号)の適用を受ける者をいう。

（2）「文書等」とは、機構の役員又は職員（以下、「役職員」という。）が職務上作成し、又は取得した文書、書面及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式でつくられた記録をいう。以下同じ。）をいう。

（3）「情報」とは、役職員が職務上作成し、又は取得した文字や数字などの記号やシンボルの媒体によって伝達され、ある物事に関する知識や意味内容をあらわすもので、文書等に化体されたものをいう。

（4）「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

（5）「保有個人情報」とは、機構の役職員が職務上作成し、又は取得した個人情報であって、機構の役職員が組織的に利用するものとして、機構が保有しているものをいう。ただし、文書管理規程（規程第１５－２１号）第 3 条第 1 項 2 号に定める機構の法人文書に記録されているものに限る。

（6）「本人」とは、個人情報によって識別される特定の個人をいう。

（7）「情報システム」とは、ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成されたものであってその組み合わせにより、情報の記録、処理、通信等の業務処理を行うものをいう。

（8）「各部門・部等」とは、組織規程（規程第 15-3 号）第 5 条から第 10 条に定める機構の部門、部等の組織をいう。

（9）「各部署」とは情報システムの管理、運用責任を行う単位として、本項 12 号で定める最高セキュリティ責任者等が別に定める機構の組織をいう。

（10）「セキュリティ事案」とは、セキュリティの対象として第5条に定める情報、情報システム、資産、業務及び管理区域に対して、機構のセキュリティに脅威を与える事態の発生、又はそのおそれをいう。

（11）「セキュリティ事故」とは、セキュリティ事案のうち、本規程及びその他関連する諸規定に抵触する役職員の行為による、機構のセキュリティに脅威を与える事態の発生又はそのおそれをいう。

（12）「最高セキュリティ責任者等」とは、第6条の2で定める最高セキュリティ責任者及び第7条で定めるセキュリティ統括をいう。

（基本原則）

第4条　役職員は、一致協力して、セキュリティの確保に努めるものとする。

2　セキュリティに関する業務は、必要とされる水準について、総合的、体系的かつ継続的に確保することを基本とする。

3　セキュリティに関する業務は、現場の状況と事実に即して、迅速かつ的確に対応することを基本とする。

4　セキュリティに係る重大な侵害又は損傷があるときは、機構の資源及び関係機関の協力を結集して可能なかぎり速やかに解決するよう努めるものとする。

（リスク評価）

第４条の２　機構は、第5条で定めたセキュリティの対象に対し、脅威を明らかにし、それぞれの重要性、利用環境等を考慮したリスク評価を行った上で、必要となるセキュリティ対策を講じるものとする。

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を見直さなければならない。

（PDCAサイクルによる継続的改善）

第４条の３　機構は、セキュリティ対策の実施状況及び効果並びにその結果としてのセキュリティの状態及び社会情勢を踏まえ、セキュリティ対策を継続的に改善しなければならない。

２　第6条で定めるセキュリティ委員会は、機構のセキュリティの管理状況を確認し、必要に応じて継続的な改善のための措置を講じなければならない。

（セキュリティの対象）

第5条　機構は、次の各号に掲げるもののうち、機密性、完全性又は可用性を確保すべき重要なものを、意図的な不正行為その他の脅威から防護し、セキュリティを確保することによって、円滑な業務の遂行を図る。

（1）情報（第3条第1項第4号に定める個人情報を含む。）

（2）情報システム

（3）有形資産（ロケット、人工衛星、航空機及びこれらに必要な施設設備並びにこれらを構成する機器、材料等）

（4）業務（ロケットの打上げ、人工衛星の追跡管制、航空機の運用等）

（5）エリア（前各号を保管又は取り扱う、機構の管理・占有する土地及び建物）

2　前項各号によりセキュリティの対象となるものの、定義、区分及び管理方法は、第3章以下に定めるところによる。

第2章　実施体制

第1節　統括組織

（セキュリティ委員会）

第6条　機構のセキュリティに関する基本方針、計画等の重要事項及び基準等の共通事項の調査審議等を行うため、セキュリティ委員会(以下「委員会」という。)を置く。

2　委員会の任務は次の号に掲げる事項とする

⑴セキュリティに関する基本方針、基準等の策定
⑵セキュリティに関する計画等の承認。
⑶セキュリティに関する全社的な事項の調整。
⑷セキュリティに関するマネージメントレビューの実施
⑸セキュリティ教育及び訓練の実施状況及び結果に関すること
⑹セキュリティ監査の結果に関すること
⑺個人情報の点検の結果に関すること
⑻その他セキュリティに関する重要事項及び共通事項の調査審議
3 委員会は副理事長、理事、及び執行役をもって構成する。
4 委員長は、副理事長とし、委員会を代表し、会務を統括する。
5 委員長代理は、最高セキュリティ責任者とし、委員長が不在又は委員長に事故があるときは、その職務を代理する。
6 委員会が必要と認める場合には、第 3 項に定める役職員のほか委員長が指名する役職員又は外部の有識者を会議の構成員に加えることができる。
7 委員会が特に必要と認める場合には、外部の機関に専門的事項等の調査検討を委託できる。
8 委員会には、専門事項について調整するための部会を置くことができる。
9 委員会の審議結果は委員長が決定し、特に重要な事項について理事長に報告するものとする。
10 委員会の運営に関する事務は、セキュリティ・情報化推進部が行う。
11 その他委員会の運営に必要な事項は、セキュリティ・情報化推進部長が別に定めるところによる。

（最高セキュリティ責任者）
第６条の２　機構のセキュリティに関する全業務を統括し、全社横断的に対応を必要とする事項への対策を講ずるため、最高セキュリティ責任者を置く。
２　最高セキュリティ責任者は、セキュリティ・情報化推進部担当理事をもってあてる。
３　最高セキュリティ責任者が不在又は最高セキュリティ責任者に事故があるときは、セキュリティ統括がこれにあたる。
４　最高セキュリティ責任者は、特に重要な事項について、前条に定める委員会に附議する。

（セキュリティ監査責任者）
第６条の３　機構に、セキュリティ監査責任者を置く。
２　セキュリティ監査責任者は、評価・監査室担当理事をもってあてる。
３　セキュリティ監査責任者は、機構全体のセキュリティ監査に関する業務を統括する。

（セキュリティ監査実施者）
第６条の４　評価・監査室に、セキュリティ監査実施者を置く。
２　セキュリティ監査実施者は、セキュリティ監査責任者の命を受け、機構全体のセキュリティ監査に関する業務を実施する。

（最高セキュリティアドバイザー）
第６条５　機構に、最高セキュリティアドバイザーを置く。
２　最高セキュリティアドバイザーは、最高セキュリティ責任者が指名する者をもってあてる。

（セキュリティ統括）
第7条　機構に、セキュリティ統括を置く。
2　セキュリティ統括は、情報化統括をもってあてる。
3　セキュリティ統括は、最高セキュリティ責任者を補佐し、その命を受け、機構全体のセキュリティに関する業務を総括整理する。

（セキュリティ統括補佐）
第8条　機構に、セキュリティ統括補佐を置く。
2　セキュリティ統括補佐は、セキュリティ・情報化推進部長をもってあてる。
3　セキュリティ統括補佐は、最高セキュリティ責任者等の命を受け、機構のセキュリティに関する業務を総括整理する。

（情報システムセキュリティ統括）
第9条　削除

（情報システムセキュリティ統括代理）
第10条　削除

（情報システムセキュリティ統括補佐）
第11条　削除

第2節　管理組織
（セキュリティ統括管理責任者）
第12条　各部門・部等にセキュリティ統括管理責任者を置く。
2　セキュリティ統括管理責任者は、各部門・部等の長をもってあてる。
3　セキュリティ統括管理責任者は、所属する各部門・部等におけるセキュリティに関する業務を統括する。

（セキュリティ統括管理責任者補佐）
第13条　各部門・部等のセキュリティ統括管理責任者の下にセキュリティ統括管理責任者補佐を置く。
2　セキュリティ統括管理責任者補佐は、セキュリティ統括管理責任者が指名し、セキュリティ統括管理責任者の命を受け、部門・部等のセキュリティに関する業務を総括整理する。
3　セキュリティ統括管理責任者補佐は、その担当する範囲を指定し、複数置くことができる。

（セキュリティ担当者）
第14条　前条に定めるセキュリティ統括管理責任者補佐の下に、セキュリティ担当者を置く。
2　セキュリティ担当者は、その担当する範囲を指定し、セキュリティ統括管理責任者補佐が指名する者をもってあてる。
3　セキュリティ担当者は、指定された範囲におけるセキュリティに関する事務を行う。

（エリア管理責任者）
第15条　次表に掲げる事業所等に、エリア管理責任者を置き、事業所の長等をあてる。

事業所等	エリア管理責任者（事業所の長等）
本社、調布航空宇宙センター及び飛行場分室	航空技術部門長
筑波宇宙センター	筑波宇宙センター所長代理

相模原キャンパス	宇宙科学研究所長
東京事務所	総務部長

2　エリア管理責任者は、管轄する区域におけるエリアセキュリティに関する業務を統括する。
3　エリア管理責任者は、代理順位を明らかにした代理者を 2 名以上置くものとする。
4　エリア管理責任者は、第 1 種及び第 2 種管理区域におけるセキュリティを確保するために、それぞれを担当するエリア管理実施責任者を置くことができる。
5　各部門・部等のセキュリティ統括管理責任者は、エリア管理責任者の置かれる事業所等におけるエリアのセキュリティ管理に関する業務について、エリア管理責任者の指示に従うものとする。

（情報システム部署責任者）
第16条　削除

（情報システム部署管理者）
第17条　削除

（情報システム責任者）
第18条　各部門・部等のセキュリティ統括管理責任者又はセキュリティ統括管理責任者の命を受け事務の委任を受けたセキュリティ統括管理責任者補佐（以下、「セキュリティ統括管理責任者等」という。）の下に、各部署で管理、運用する情報システム毎に情報システム責任者を置く。
2　情報システム責任者は、セキュリティ統括管理責任者等の命を受け、当該情報システムセキュリティに関する業務を統括する。

（情報システム管理者）
第19条　各部署の情報システム責任者の下に情報システム管理者を置くことができる。
2　情報システム管理者は、情報システム責任者の命を受け、情報システムセキュリティに関する業務を総括整理する。

（管理体制の変更）
第20条　各部門・部等のセキュリティ統括管理責任者は、セキュリティ統括管理責任者補佐、セキュリティ担当者、情報システム責任者、及び情報システム管理者を変更したときは、最高セキュリティ責任者等に、速やかに報告しなければならない。

第3章　情報のセキュリティ
第 1 節　情報セキュリティ通則
（情報取扱の定義）
第21条　本章において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。
（1）「閲覧」とは、情報の内容を調べ、読むことをいう（情報システムを利用して電磁的記録の内容を調べ、読むことを含む。）。
（2）「複製」とは、手書き、複写機等の機器又は情報システムを利用して、情報の複製物を作成することをいう。
（3）「持出し」とは、情報を、通常の保管場所の外に移動させ、持ち出した者の管理の下に置くことをいう。
（4）「貸出し」とは、情報を機構内外の関係者に預け、一定の期間、相手方の管理の下に置くことをいう。
（5）「提供」とは、情報を伝達又は引き渡し、その廃棄を含め相手方の管理の下に置くことをいう。
（6）「廃棄」とは、情報を物理的（電磁的記録の場合は、電磁的）に抹消することをいう。
（7）「移管」とは、保有する情報の原本の管理を、他のセキュリティ統括管理責任者の管理下に移すことを

いう。

（情報管理の一般原則）

第22条　機構が保有する情報であって、特にそのセキュリティを確保すべきものは、重要度及びリスク評価に基づき、第24条から第26条に定める情報のカテゴリに区分して管理を行う。

2　情報の区分指定は、各部門・部等のセキュリティ統括管理責任者等（ただし、AA 情報の管理について、セキュリティ統括管理責任者から事務の委任を受けられるセキュリティ統括管理責任者補佐は、決裁規程第 2 条に定める部長等以上に限る。）が行うものとする。区分指定は、情報の性質に応じ過不足ない適切な区分に指定しなければならない。

3　各部門・部等のセキュリティ統括管理責任者等は、第24条に定める AA 情報及び第25条に定める A 情報（以下「要保護情報」という。）については、指定した情報を登録するための登録台帳と、情報の閲覧、複製、持出し、貸出し、提供、廃棄の管理に関する事実を記録するため管理台帳を作成する。

4　指定された情報を、閲覧、複製、持出し、貸出し、提供、廃棄又は移管する場合は、本章の定めるところにより、原則としてセキュリティ統括管理責任者等の許可のもと実施し、記録を残さなければならない。

5　法律、政令、条例(以下「法令等」という。)に基づき、国等が秘密情報等を閲覧、持出し、複写等(以下「閲覧等」という。)を実施する場合においては、本規程の定めによらず、当該法令等で定めるところによる。ただし、この場合であっても、国等に対し、当該情報がセキュリティ確保を要する情報であることを伝え、適切な管理を依頼し、提供した事実の記録を残さなければならない。

（役職員の心得）

第23条　役職員は、機構が保有する情報には、国の安全及び利益の確保並びに国際間の取り決めに基づき、厳重に管理することが求められる重要な情報が含まれていることを十分に認識しなければならない。

2　役職員は、情報を適正に管理することは、機構の重要な使命であることを認識し、不注意、ずさんな管理等により情報を漏えいすることのないように十分に注意しなければならない。

3　役職員は、情報の漏えい等のリスクを低減すべく、セキュリティの対象となる情報の取得・保有を最小限に止めなければならない。

（AA 情報）

第24条　特に限られた機構内外の関係者のみ知りうる状態を確保する必要がある情報のうち、漏えい、破壊、改ざん、滅失又は毀損等により、国の安全若しくは利益に著しく損害を与えるおそれがあるもの又は機構の事業の遂行を著しく困難にするおそれがあるものであって、以下の各号のいずれかに該当するものを「AA情報」とする。

（1）国際約束に基づいて輸入された技術及び機器に関する情報のうち、その内容を特定の関係者以外の者に漏洩することを防止する必要のある情報

（2）国家安全保障上の観点から厳重な取扱いを行う必要のある情報として政府が要請等を行ったもの、又は政府の要請等に基づき機構自らが指定した情報

（3）外国為替令(昭和 55 年政令第 260 号。以下「外国為替令」という。)別表第 4 項に掲げるロケット等に係る技術であって、機構のロケットが所定の機能、性能を有するために不可欠な構成機器、システムの製造に関する情報

（4）漏えい、破壊、改ざん、滅失又は毀損等により、重大な支障を生ずるおそれがあり、対策を講じなければロケット、人工衛星、宇宙ステーションの開発、打上げ、運用等を実施又は継続できない情報

（5）前各号に類する情報であって、セキュリティ統括管理責任者の指定する情報

（A 情報）

第25条　機構内外の関係者のみ知りうる状態を確保する必要がある情報のうち、漏えい、破壊、改ざん、滅失又は毀損等により、機構の事業の円滑な遂行、機構の財産上の利益及び契約当事者としての地位、協力協定、協同研究等の相手方の利益、個人の人権及びプライバシー等の機構及び関係者の正当な地位及び利益を侵害するおそれがあるものであって、以下の各号のいずれかに該当するものを「A 情報」とする。

（1）外国為替令別表に掲げる技術であって、構成機器、システムの製造に関する情報

（2）契約相手方、共同研究相手方から入手した情報であって、関係者以外の者への開示を制限するなど特別な取扱いが必要な情報

（3）機構の技術、人事、経理、契約等に関する情報であって、漏えい等により機構の業務及び利益を著しく侵害するおそれのある情報

（4）前各号に類する情報で、漏洩により業務遂行に支障を生ずるおそれがあり、対策を講じなければ機構の行う事業の円滑な遂行が困難となる情報

2　第3条第1項第5号で定める保有個人情報のうち、以下の各号のいずれかに該当するものを「A 個人情報」という。

（1）役職員及び機構の業務に関係する個人に関する情報のうち、住所、自宅電話番号、生年月日その他の非公知であって本人及び特定の関係者を除いては、通常知り得ない私生活上の情報、及び人事関係、給与・諸手当等に関する情報

（2）機構外の個人からの問い合わせ、記名式アンケート、及び苦情・意見等への対応記録（但し、氏名・連絡先のみの場合は除く。）

（3）独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号。以下、本章において「個人情報保護法」という）第2条に規定される個人情報ファイルであって本人の数が1，000名を超えるもの。

（B 情報）

第26条　要保護情報に相当する情報ではないものの、機構の円滑な業務遂行のため、開示等の取扱いに一定の留意や手続きを要する情報で、セキュリティ統括管理責任者の指定した情報を「B 情報」とする。

2　第3条第1項第5号で定める保有個人情報のうち、本章第5節に定めるところにより、「B 情報」として管理すべきものであって、以下の各号のいずれかに該当するものを「B 個人情報」とする。

（1）所属、役職、職員番号、勤怠管理等の機構内で使用する役職員の個人の情報、及び内線電話番号表、座席表、委員会等の名簿、来訪者記録等専ら機構内又は部門・部等で横断的・共通的に使用する情報（A 個人情報に該当するものを除く。）

（2）非常時の連絡の用に供する緊急連絡網及び業務上の関係者の連絡の用に供する電話番号表（以下「緊急連絡網等」という。ただし、A 個人情報に該当するものを除く。）

（3）連絡先として会社、所属部部署・担当、氏名等の名刺情報、及びこれらをまとめたもの（A 個人情報に該当するものを除く。）

（各部門・部等の実施計画）

第27条　各部門・部等のセキュリティ統括管理責任者は、セキュリティの対象となる情報の管理に関し、情報の区分のためのガイドライン、リスク評価の方法、情報セキュリティ PDCA サイクル活動の計画を含む、各部門・部等の管理のための実施計画を定めるものとする。

第 2 節　AA 情報の取扱

（AA 情報の登録及び抹消）

第28条　セキュリティ統括管理責任者等が AA 情報を区分指定するにあたっては、AA 情報として取り扱う期

間及び当該情報にアクセスできる関係者を定め、登録台帳に登録しなければならない。
2　AA 情報は、取得時又は作成開始時に、前項の登録を行うものとし、記載する文書等が作成中であっても、完成後と同等の管理を行わなければならない。
3　AA 情報として指定する範囲は、原則として当該情報が含まれる最小限の部分としなければならない。
4　AA 情報にアクセスできる関係者の指定は、必要最小限の個人の単位で行うものとし、部・課等の組織の単位で行ってはならない。
5　AA 情報の指定・登録時に定めた期間が経過したとき、又は期間の途中であってもAA 情報として取り扱う必要がなくなったとき、若しくは当該情報が不要となり廃棄しようとするときは、区分指定を解除し、登録を抹消しなければならない。取扱期間が満了した情報は、指定が解除されたものとみなす。

（AA 情報の表示）
第29条　AA 情報を記載する文書には、識別のため全てのページに区分表示を行い、また抜き取り防止のために必要なページの表示等を行わなければならない。電磁的記録媒体に記録されている情報（以下、「電子情報」という。）についても同等の措置をとるものとする。

（AA 情報の保管）
第30条　AA 情報は、第1種管理区域内の書庫等に施錠して保管しなければならない。電子情報として保管する場合は、ネットワークに接続されてない第1種管理区域内に設置された情報システムに保管しなければならない。

（AA 情報の閲覧）
第31条　AA 情報の閲覧は、あらかじめ指定された関係者のみが閲覧することができる。
2　あらかじめ指定された関係者が閲覧するときは、事前に書面による申請を行い、セキュリティ統括管理責任者等の許可を得て、第1種管理区域内で行わなければならない。電子情報の場合も、ネットワークに接続されていない第1種管理区域内に設置された情報システムで行わなければならない。
3　前項の閲覧の事実は、管理台帳に記録しなければならない。

（AA 情報の複製）
第32条　AA 情報は、業務上特に必要がある場合を除き、複製してはならない。
2　複製するときは、あらかじめ指定された機構内の関係者が、事前に書面による申請を行い、セキュリティ統括管理責任者等の許可を得て、第1種管理区域内で行わなければならない。電子情報の場合も、ネットワークに接続されていない第1種管理区域内に設置された情報システムで行わなければならない。
3　前項の複製の事実は、管理台帳に記録するとともに、複製された情報について登録台帳に登録しなければならない。

（AA 情報の持出し）
第33条　AA 情報の原本は、第37条に定める移管の場合を除き、保管場所から持ち出してはならない。業務上特に必要がある場合は、あらかじめ指定された機構内の関係者に限り、複製して持ち出すことができる。
2　持出しを行うときは、あらかじめ指定された機構内の関係者が、事前に書面による申請を行い、セキュリティ統括管理責任者等の許可を得なければならない。
3　前項の許可を得て、AA 情報を持ち出す場合は、カバン等に保管の上、関係者自ら携行するものとする。電子情報を記録媒体に記録して持ち出す場合も同様とする。なお、持出しにあたって、複製物を作成する場合（電子情報の複製を含む）は、第32条の複製の手続きによるものとする。
4　前項の規定により作成した複製物は、必要が無くなったときは、直ちに廃棄しなければならない。

5　前三項の持出しの事実（複製物の作成及び廃棄を含む）は、管理台帳に記録しなければならない。

（AA 情報の貸出し）

第34条　AA 情報の原本は、保管場所から貸し出してはならない。業務上特に必要がある場合は、あらかじめ指定された関係者に対してのみ、複製により貸し出すことができる。

2　貸出しを行うときは、あらかじめ指定された関係者が、事前に書面による申請を行い、セキュリティ統括管理責任者等の許可を得なければならない。許可に当たっては、あらかじめ返却期限を定めなければならない。

3　前項の許可を得て、AA 情報を貸し出す場合には、第33条第3項及び同 4 項を準用する。

4　前二項の貸出しの事実及び当該情報の返却の事実（複製物の作成及び廃棄を含む）は、管理台帳に記録しなければならない。

（AA 情報の提供）

第35条　AA 情報の原本は、提供してはならない。業務上特に必要がある場合は、あらかじめ指定された関係者に対してのみ、複製物を提供することができる。

2　前項にかかわらず、緊急を要し、業務の円滑かつ適切な遂行に著しい支障を及ぼすとセキュリティ統括管理責任者が認めた場合は、臨時の措置として、情報システムを利用して暗号化された複製情報を、第 2 種管理区域に持ち出し、適切なセキュリティ対策を施した情報システムを使用して電子メールその他の電子的伝送手段で提供することができる。

3　提供を行うときは、あらかじめ指定された関係者が、事前に書面による申請を行い、セキュリティ統括管理責任者等の許可を得なければならない。

4　前項の許可を得て、AA 情報を提供する場合は、第33条第 3 項を準用する。

5　前三項の提供の事実は、提供元の管理台帳に記録しなければならない。

6　提供を受けた部門・部等のセキュリティ統括管理責任者等は、第28条の登録の手続きにより、当該情報を登録台帳に登録し、AA 情報として必要な管理を行わなければならない。

（貸出し又は提供の条件）

第36条　AA 情報を、機構外の関係者に貸出し又は提供するときは、セキュリティ統括管理責任者等は、関係者が所属する企業等の法人に、保管及び取扱場所、受領した情報の管理体制に関し、本規程と同等の内規をもって管理することを確約させなければならない。

（AA 情報の移管）

第37条　AA 情報を、他のセキュリティ統括管理責任者の管理へ移管する場合、移管先を記録した上で、移管元の登録台帳から抹消するものとする。

2　移管に当たって保管場所から持ち出すときは、第33条第3項の方法による。

3　移管を受けた他のセキュリティ統括管理責任者等は、第28条の登録の手続きにより、当該情報を登録台帳に登録し、AA 情報として必要な管理を行わなければならない。

（AA 情報の廃棄）

第38条　AA 情報を記録した文書等を廃棄するときは、関係者自ら、焼却し、又は、シュレッダー、メディアクラッシャー等を利用し物理的に裁断又は破砕し、電子情報は、消去ツール等によって復元不可能な状態にしなければならない。

（関係者以外への開示）

第39条　あらかじめ指定された関係者以外の者が、AA 情報の閲覧又は貸出しもしくは提供を受ける必要が

あるときは、当該情報を管理するセキュリティ統括管理責任者等に対して、事前に書面による申請を行い、許可を受けなければならない。

2　前項の申請を受けたセキュリティ統括管理責任者等は、申請の目的、理由、必要性等を厳格に審査し許可を与えるものとする。なお、許可にあたっては、アクセスさせる情報の範囲を最小限にするほか、当該情報が、セキュリティの確保が必要な情報であること及びセキュリティ確保のために本規程と同等の措置をとらなければならないことを明示し、条件としなければならない。

3　前項の許可を受けて AA 情報を閲覧させるときは、第31条の定めるところによるほか、関係者の立会いのもと行わなければならない。

4　第 2 項の許可を受け、AA 情報を貸出し又は提供するときは、第34条又は第35条の定めるところによるほか、貸出し又は提供先で、本規程と同等の管理をさせなければならない。

第 3 節　A 情報

（A 情報の登録及び抹消）

第40条　セキュリティ統括管理責任者等が A 情報を区分指定するにあたっては、A 情報として取り扱う期間及び当該情報にアクセスできる関係者の範囲を定め、登録台帳に登録しなければならない。

2　A 情報の指定は、原則として当該情報が含まれる範囲に限定しなければならない。但し、文書、文書ファイル、電子情報のフォルダ単位で指定することを妨げない。

3　A 情報にアクセスできる関係者の指定は、部・課等の組織の単位で行うことができる。

4　A 情報の登録を抹消する場合は、第28条第5項を準用する。

（指定前の A 情報の取扱い）

第41条　指定を受ける前であっても、A 情報に該当しうる情報を取り扱う場合には、鍵のかかる書庫、引き出し等への保管、情報の暗号化等の適切な処置を講じ、セキュリティの確保に努めなければならない。

（A 情報の表示）

第42条　A 情報を記載する文書等には、識別のための区分表示を行わなければならない。電子情報についても同等の措置をとるものとする。

（A 情報の保管）

第43条　A 情報は、第2種管理区域内の書庫等に施錠して保管しなければならない。電子情報として保管する場合は、第2種管理区域内に設置され、アクセス制御された情報システムに保管しなければならない。

（A 情報の閲覧）

第44条　A 情報は、あらかじめ指定された関係者のみが閲覧することができる。

2　A情報を閲覧するときは、第2種管理区域内で行わなければならない。電子情報の場合も、第2種管理区域内のアクセス制御された情報システムで行わなければならない。

（A 情報の複製）

第45条　A 情報は、業務上必要がある場合を除き、複製してはならない。

2　複製するときは、あらかじめ指定された機構内の関係者が、セキュリティ統括管理責任者等の許可を得て、第2種管理区域内で行わなければならない。電子情報の場合は、第2種管理区域内の情報システムで行わなければならない。

3　前項の複製の事実は、管理台帳に記録するとともに、複製された情報について登録台帳に登録しなけれ

ばならない。

（A 情報の持出し）

第46条　A 情報は、業務上必要がある場合に限り、あらかじめ指定された機構内の関係者のみが持ち出すことができる。

2　持出しを行うときは、あらかじめ指定された機構内の関係者が、セキュリティ統括管理責任者等の許可を得なければならない。

3　前項の許可を得て、A 情報を持ち出す場合は、カバン等に保管の上、関係者自ら携行するものとする。電子情報を記録媒体に記録して持出す場合も同様とする。なお、持出しにあたって、複製物を作成する場合（電子情報の複製を含む）は、一時利用のものを除き、第45条の複製の手続きによるものとする。

4　前項の規定により作成した複製物は、必要が無くなったときは直ちに廃棄しなければならない。

5　前三項の持出しの事実（複製物の作成及び廃棄を含む）は、管理台帳に記録しなければならない。

（A 情報の貸出し）

第47条　A 情報は、業務上必要がある場合に限り、あらかじめ指定された関係者に対してのみ、貸し出すことができる。

2　貸出しを行うときは、あらかじめ指定された関係者が、セキュリティ統括管理責任者等の許可を得なければならない。許可に当たっては、あらかじめ返却期限を定めなければならない。

3　前項の許可を得て、A 情報を貸し出す場合には、第46条第3項及び同 4 項を準用する。

4　前二項の持ち出しの事実及び当該情報の返却の事実（複製物の作成及び廃棄を含む）は、管理台帳に記録しなければならない。

（A 情報の提供）

第48条　A 情報の原本は、提供してはならない。業務上必要がある場合は、あらかじめ指定された関係者に対してのみ、複製物を提供することができる。

2　提供を行うときは、あらかじめ指定された関係者が、セキュリティ統括管理責任者等の許可を得なければならない。

3　前項の許可を得て、A 情報を提供する場合は、相手方への手渡しによる他以下の各号の方法によることができる。なお、提供にあたって、複製物を作成する場合は、一時利用のものを除き、第45条の複製の手続きによるものとする。

（1）配達の履歴等が確認できる郵便等による手段。

（2）ファクシミリ、電子メールその他の電子的伝送手段。この場合、提供先の電話番号、メールアドレス等を十分に確認するとともに、ファクシミリよる場合には提供直前に受信者に連絡のうえ、提供直後にその受信を確認し、また電子メールによる場合には当該情報を暗号化して送付するものとする。

4　前三項の提供の事実は、送付元の管理台帳に記録しなければならない。

5　提供を受けた部門・部等のセキュリティ統括管理責任者等は、第40条の登録の手続きにより、当該情報を登録台帳に登録し、A 情報として管理しなければならない。

（貸出し又は提供の条件）

第49条　A 情報を、機構外の関係者に貸出し又は提供するときは、セキュリティ統括管理責任者等は、関係者が所属する企業等の法人に、保管及び取扱場所、受領した情報の管理体制に関し、本規程と同等の管理をすることを確約させなければならない。

（A 情報の移管）

第50条　A情報を、他のセキュリティ統括管理責任者の管理へ移管する場合、移管先を記録した上で、移管

元の登録台帳から抹消するものとする。

2　移管に当たって保管場所から持ち出すときは、第46条第3項の方法による。

3　移管を受けた部門・部等のセキュリティ統括管理責任者等は、第40条の登録の手続きにより、当該情報を登録台帳に登録し、A 情報として必要な管理を行わなければならない。

（A 情報の廃棄）

第51条　A 情報を廃棄するときは、原則として、関係者自ら、焼却し、又は、シュレッダー、メディアクラッシャー等を利用し物理的に裁断又は破砕し、電子情報は、消去ツール等によって復元不可能な状態にすること。

2　A 情報が含まれる資料等の廃棄を外部に委託する場合は、機構内で梱包した状態のまま溶解処理を行わせる等セキュリティ確保に必要な措置を講じなければならない。

（関係者以外への開示）

第52条　あらかじめ指定された関係者以外の者が、A 情報の閲覧又は貸出しもしくは提供を受ける必要があるときは、当該情報を管理するセキュリティ統括管理責任者等に対して、事前に書面による申請を行い、許可を受けなければならない。

2　前項の申請を受けたセキュリティ統括管理責任者等は、申請の目的、理由、必要性等を審査し許可を与えるものとする。なお、許可にあたっては、アクセスさせる情報の範囲を最小限にするほか、当該情報が、セキュリティの確保が必要な情報であること及びセキュリティ確保のために本規程と同等の措置をとらなければならないことを明示し、条件としなければならない。

3　前項の許可を受けて、A 情報を閲覧、貸出し又は提供するときは、本節各条の定めるところによる。

4　以下の者からの請求による場合は、申請の目的、理由、必要性等を口頭で確認の上、第 1 項の書面による事前の申請については、省略することができる。なお、管理台帳への記録は省略することはできない。

（1）関係者に指定されていない役職員

（2）法令等により守秘義務を負う公務員等

（3）機構の取引基本契約書・標準契約書等で守秘義務を負い、且つ機構の情報の取扱に関し、機構のセキュリティと同等の管理を行う義務を負っている契約の相手方

第４節　Ｂ情報

（Ｂ情報の指定）

第53条　Ｂ 情報の指定は、原則として当該情報が含まれる範囲に限定しなければならない。ただし、文書、文書ファイル、電子情報のフォルダ単位で指定することを妨げない。

２　Ｂ情報にアクセスできる者の範囲を、指定した機構内外の関係者に限定することができる。

３　Ｂ 情報にアクセスできる関係者の指定方法については、第27条に基づき各部門・部等のセキュリティ統括管理責任者の制定する管理のための実施計画に定める。

（指定前のＢ情報の取扱い）

第54条　指定を受ける前であっても、Ｂ 情報に該当しうる情報を取り扱う場合は、書庫等への保管など適切な処置を講じ、セキュリティの確保に努めるものとする。

（Ｂ情報の表示）

第55条　Ｂ 情報を記載する文書には、原則として識別のための区分表示を行わなければならない。電子情報についても同様とする。

（Ｂ情報の保管）

第56条　Ｂ 情報は、第2種管理区域内の書庫等に保管しなければならない。電子情報として保管する場合は、第2種管理区域内に設置された情報システムに保管しなければならない。

（Ｂ情報の閲覧）

第57条　Ｂ情報は、役職員及び機構外の関係者のみが閲覧することができる。

（Ｂ情報の複製）

第58条　Ｂ情報は、役職員及び機構外の関係者のみが、業務上必要な範囲で複製することができる。

（Ｂ情報の持出し）

第59条　Ｂ情報は、役職員のみが、業務上必要な範囲で持ち出すことができる。

２　Ｂ情報を持ち出す場合は、紛失・盗難等に留意する。

（Ｂ情報の貸出し）

第60条　Ｂ情報は、業務上必要な範囲で役職員及び機構外の関係者に、貸し出すことができる。

２　前項の貸出しの事実は、貸出し先が機構外の関係者である場合には、その記録を残さなければならない。

（Ｂ情報の提供）

第61条　Ｂ情報は、業務上必要な範囲で役職員及び機構外の関係者に、提供することができる。

２　前項の提供の事実は、提供先が機構外の関係者である場合には、その記録を残さなければならない。

（貸出し又は提供の条件）

第62条　Ｂ情報を、機構外の関係者に貸出し又は提供するときは、セキュリティ統括管理責任者等は、関係者が所属する企業等の法人に、当該関係者以外に開示しないことを確約させなければならない。

（Ｂ情報の廃棄）

第63条　Ｂ情報を廃棄するときは、第51条（Ａ情報の廃棄）の規定を準用する。

（関係者以外への開示）

第64条　役職員及びあらかじめ指定された関係者以外の者が、B 情報の閲覧又は貸出しもしくは提供を受ける必要があるときは、当該情報を管理するセキュリティ統括管理責任者等に対して、事前に書面による申請を行い、許可を受けなければならない。

2　前項の申請を受けたセキュリティ統括管理責任者等は、申請の目的、理由、必要性等を審査し許可を与えるものとする。なお、許可にあたっては、アクセスさせる情報の範囲を最小限にするほか、当該情報が、セキュリティの確保が必要な情報であること及びセキュリティ確保のために本規程と同等の措置をとらなければならないことを明示し、条件としなければならない。

3　前項の許可を受けて、B 情報を閲覧、貸出し又は提供するときは、本節各条の定めるところによる。

4　以下の者からの請求による場合は、申請の目的、理由、必要性等を口頭で確認の上、第１項の書面による事前の申請については、省略することができる。なお、記録は省略することはできない。

（1）関係者に指定されていない役職員（第53条第2項により B 情報へのアクセスを関係者限定とした場合）

（2）法令等により守秘義務を負う公務員等

（3）機構の取引基本契約書・標準契約書等で守秘義務を負い、且つ機構の情報の取扱に関し、機構のセキュリティと同等の管理を行う義務を負っている契約の相手方

第5節　個人情報

第1款　個人情報通則

（取扱いの総則）

第65条　役職員は、個人情報保護法の趣旨に則り、関連する法令及び規程等の定め並びにセキュリティ統括管理責任者の指示に従い、保有個人情報を取り扱わなければならない。

2　役職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

（不正な利用及び取得等の禁止）

第66条　役職員は、以下をしてはならない。

（1）その業務に関して知り得た個人情報の内容をみだりに他人に知らせること。

（2）その業務に関して知り得た個人情報の内容を不当な目的に利用すること。

（3）偽りその他不正の手段により個人情報を取得すること。

（利用目的の明示）

第67条　役職員は、本人から直接書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）に記録された当該本人の個人情報を取得するときは、次に掲げる場合を除き、あらかじめ、本人に対し、その利用目的その他必要な事項を明示しなければならない。

（1）人の生命、身体又は財産の保護のために緊急に必要があるとき。

（2）利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき。

（3）利用目的を本人に明示することにより、機構、国の機関、独立行政法人等又は地方公共団体が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき。

（4）取得の状況からみて利用目的が明らかであると認められるとき。

2　前項に定める利用目的の明示方法については、取得の態様により、以下に掲げる方法によらなければならない。

（1）役職員が本人から直接、書面等の提出を受け取得するとき。
イ. 申請書等の様式、もしくは記入要領・案内等を記載した書面に記載。
ロ. 窓口における掲示。ただし、申請書等を受け付ける窓口を設置する場合に限る。
ハ. 口頭による説明。ただし、上記イ及びロによることができない場合に限る。
（2）郵送等の方法により提出を受け取得するときは、提出される申請書等の様式、もしくは記入要領・案内等を記載した書面に記載。
（3）オンライン申請システム等、電磁的方法により提出を受け取得するときは、入力画面もしくは記入要領・案内等を記載した書面。

（利用の制限及び正確性の確保）
第68条　役職員は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を閲覧、複製、持出し、貸出し、提供及び廃棄（以下、本節において「利用」という。）してはならない。
2　役職員は、利用目的の達成に必要な範囲内で、保有個人情報が過去又は現在の事実と合致するよう努めなければならない。
3　役職員は、保有個人情報の内容に誤り等を発見した場合には、セキュリティ統括管理責任者の指示に従い、訂正等を行う。
4　役職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。

第2款　個人情報の管理
（A 個人情報の管理）
第69条　A 個人情報の管理については、本章第3節の A 情報の管理についての規定を準用する。
2　A 個人情報の利用は、あらかじめ指定された関係者のみが、利用目的の範囲内で、本章第3節各条に定める手続きにより、行うことができる。
3　前項の規定にかかわらず、セキュリティ統括管理責任者等が、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を利用することができる。ただし、保有個人情報を利用目的以外の目的のために利用することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。
（1）本人の同意があるとき、又は本人に提供するとき。
（2）法令の定める業務の遂行に必要な限度で保有個人情報を機構内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。
（3）行政機関（行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号。以下「行政機関個人情報保護法」という。）第二条第一項に規定する行政機関をいう。以下同じ。）、他の独立行政法人等又は地方公共団体に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。
（4）前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。
4　前項の規定は、保有個人情報の利用又は提供を制限する他の規程類及び法令の規定の適用を妨げるものではない。
5　セキュリティ統括管理責任者等は、第2項及び第3項3号又は4号の規定に基づき、保有個人情報を機構外の者に貸出し又は提供するときは、貸出し又は提供を受ける者に対し、当該個人情報について、その利用の目的若しくは方法の制限その他必要な制限を付し、又はその漏えいの防止その他の個人情報の適切な管理のために必要な措置を講ずることを求めるものとする。

（A 個人情報に該当する緊急連絡網等の取り扱いの例外）

第70条　A 個人情報に該当する非常時の連絡の用に供する緊急連絡網及び業務上関係者間の連絡の用に供する電話帳等（以下「緊急連絡網等」という）については、第44条（閲覧）、第45条（複製）及び第46条（持出し）を適用しない。

2　緊急連絡網等を、機構の管理区域外で閲覧するときは、覗き見に注意し、関係者以外に閲覧させてはならない。

3　緊急連絡網等を、その利用者を関係者と指定し配布するときは、配布したものを複製として登録台帳に登録することを省略することができる。複写の禁止や、一連の通し番号等を表示する等の方法により関係者以外に渡らないよう注意しなければならない。

4　配布された緊急連絡網等を、関係者が機構の管理区域外へ持ち出す場合は、セキュリティ統括管理者等の許可及び管理台帳への登録を省略することができる。持出しに当たっては、関係者自身が携行し、盗難、紛失に注意しなければならない。

（B 個人情報の管理）

第71条　B 個人情報の管理については、本章第4節の B 情報の管理についての規定を準用する。

2　B 個人情報の利用は、利用目的の範囲内で、あらかじめ指定された関係者のみが、本章第4節各条に定める手続きにより、行うことができる。

3　B 個人情報の管理に関し、第69条（A 個人情報の管理）第3項から第5項を準用する。

（個人情報の開示等の手続き）

第72条　保有個人情報の開示等及び所管官庁への報告等に関する事項は、「個人情報の開示等に関する規程（規程第 17－8 号）」の定めるところによる。

第4章　情報システムのセキュリティ

第 1 節　情報システムのセキュリティ管理

（情報システムのセキュリティ対策）

第73条　情報システムのセキュリティについて、情報システムの利便性を確保しつつ、情報システムに格納される第 3 章に定める情報の重要度、情報システムが利用される第 6 章に定める業務の重要度及びリスク評価に応じ、以下の物理的及び技術的対策により確保するものとする。

（1）物理的対策　　パソコン等情報システムの盗難・紛失対策、サーバ室等への入退出管理等

（2）技術的対策　　パスワード等によるアクセス制御、アクセス・ログの取得、コンピュータ・ウイルス対策、サービス不能攻撃対策等

2　前項の各対策の基準は、最高セキュリティ責任者等が別に定めるところによる。

（情報システムの整備及び運用状況等の把握）

第74条　セキュリティ統括管理責任者は、定期的に、情報システムの整備及び運用状況をとりまとめ、最高セキュリティ責任者等に報告するものとする。

（情報システムセキュリティ確保のための措置）

第75条　各部門・部等のセキュリティ統括管理責任者は、情報システムセキュリティ確保のために特に必要と認められる場合は、情報システムの使用制限、運用停止その他の必要な措置を行うことができる。

2　各部門・部等のセキュリティ統括管理責任者は、前項の措置について、最高セキュリティ責任者等に報告するものとする。

3　前項の報告を受け、最高セキュリティ責任者等は、各情報システムに対して必要な措置を講ずるものとする。

第 2 節　情報システムの利用

(情報システムを利用する者の義務)

第76条　役職員は、不正アクセス行為の禁止等に関する法律(平成 11 年 8 月 13 日法律第 128 号)その他の法令及びこの規程その他の機構の規則を遵守しなければならない。

2　役職員は、業務の遂行を目的として、情報システムを利用しなければならない。

3　役職員は、パスワードの適正な管理等情報システムセキュリティ対策を適正に行わなければならない。

4　役職員は、情報システムを利用する場合に於いて、ネットワーク接続、無線 LAN の利用、PC 等の持ち込み・持ち出しをする場合、セキュリティ統括管理責任者が別途定める所定の手続きにより、許可を得なければならない。

5　役職員は、情報システムを整備・運用する場合に於いて、ネットワーク接続、経路変更、無線 LAN ルータの設置、情報システムの移動・持ち込み・持ち出し及び重要なシステムの設定変更等をする場合、セキュリティ統括管理責任者が別途定める所定の手続きにより、許可を得なければならない。

6　役職員が情報システムを利用するにあたって必要なセキュリティ上の基準については、最高セキュリティ責任者等が別に定めるところによる。

(禁止行為)

第77条　役職員は、情報システムの整備、運用及び利用において次の各号に掲げる行為をしてはならない。

(1)不正アクセス行為の禁止等に関する法律(平成 11 年 8 月 13 日法律第 128 号)に規定する不正アクセス行為及びその他の不法行為をすること。

(2)セキュリティを確保する上で支障を及ぼす情報システム構成の変更、業務上不適切なソフトウエアの使用、不適切なパスワードの設定、正常な情報システムの稼働を妨げる行為等により、情報システムセキュリティを損なうこと。

(3)情報システムを用いて、業務上知り得た秘密及び個人情報を他に知らせること。

(4)情報システムを用いて、機構の信用を傷つけ、その利益を害し又は職員全体の不名誉となる行為をすること。

(5)不適切なサイトへのアクセスなど公序良俗に反する行為をすること。

(6)情報システムを株式売買、通信販売等の私的な目的に使用すること。

(7)業務遂行を目的として、役職員の私有の情報システム、及び、公共の場に設置され不特定多数の者に利用されるパソコン等最高セキュリティ責任者等が別に定める情報システム(以下、「業務外情報システム」という。)を使用してはならない。また、職務上知ることのできた情報(公知の情報を除く)を業務外情報システムに搭載してはならない。なお、本号にいう「情報システム」とは、第3条第 1 項第7号にかかわらず、パソコン、サーバ及びワークステーション並びにUSB メモリその他の外部記憶装置をいう。

2　情報システムの整備及び運用にあたる職員は、前項各号に該当する行為の他、個人情報をみだりに閲覧し、又はその業務に関して知り得た個人情報を他人に知らせ若しくは不当な目的に使用してはならない。

(禁止行為の調査)

第78条　情報システムの整備及び運用にあたる職員は、適宜に情報システムを点検し、職員が前条に定める禁止行為を行った疑いがあるときは、最高セキュリティ責任者等に報告するものとする。最高セキュリティ責任者等は、当該報告に基づき、当該職員の所属する部門・部等のセキュリティ統括管理責任者等への通知を行うものとする。

2　セキュリティ統括管理責任者等は、職員が前条に定める禁止行為を行った疑いがあるときは、実状調査を行うものとする。
3　前項の実状調査の結果、職員が前条に定める禁止行為を行ったと認める相当の理由があるときは、当該職員はセキュリティ統括管理責任者等が行う事情聴取に応じなければならない。

第5章　資産のセキュリティ

第1節　資産セキュリティ通則

（資産セキュリティの一般原則）

第79条　機構が保有する有形資産のうち、特にセキュリティを確保すべきものは、重要度リスク評価に基づき、第80条第1項各号に定めるセキュリティ資産のカテゴリに区分して管理を行う。
2　セキュリティ資産の各カテゴリーへの指定は、各部門・部等のセキュリティ統括管理責任者等（ただし、AA 資産の管理について、セキュリティ統括管理責任者から事務の委任を受けられるセキュリティ統括管理責任者補佐は、決裁規程第 2 条に定める部長等以上に限る。）が行ない、指定したセキュリティ資産は、カテゴリ毎に必要な管理を行わなければならない。
3　セキュリティ資産の管理は、本章の規定によるほか、資産管理に関する諸規則の定めるところにより管理を行う。

（有形資産の区分）

第80条　機構が保有する有形資産のうち、セキュリティを確保すべき有形資産を、重要度及びリスク評価に基づき、次の各号のとおり区分して管理を行う。

（1）AA 資産

関係する役職員及び機構外関係者のうち業務上特に必要性が認められ、指定を受けた者に限りアクセスすることができる有形資産で、

イ．「AA 情報」に区分される技術が内包されている物品
ロ．国際約束に基づいて輸入された機器等の物品で、厳重な管理を要する物品
ハ．滅失若しくは破損により、機構のミッション達成に致命的な影響が生じるか又は社会的信用が著しく傷付けられるおそれのある物品

（2）A 資産

役職員及び機構外関係者のうち業務上必要性が認められ、指定を受けた者に限りアクセスすることができる有形資産で、

イ．「A 情報」に区分される技術が内包されている物品
ロ．国際約束に基づいて輸入された機器等の物品で、一定の管理を要する物品
ハ．滅失若しくは破損により、機構のミッション達成に大きな影響が生じるか又は機構の社会的信用が傷つけられるおそれがある物品

第2節　AA 資産

（AA 資産の登録）

第81条　AA 資産に指定されたセキュリティ資産は、アクセスできる関係者の範囲を定め、登録台帳に登録しなければならない。AA 情報が含まれる物品については、当該 AA 情報にアクセスできる関係者の範囲と同一でなければならない。
2　AA 資産の指定は、指定する範囲を明確にし、できる限り最小限の範囲としなければならない。
3　各部門・部等のセキュリティ統括管理責任者等は、AA 資産の登録台帳を整備し、また、年に 1 回管理状況の内部監査を実施しなければならない。ただし、資産取扱要領に基づく資産の棚卸しで代用することができる。

（AA 資産の保管・使用場所）

第82条　AA 資産に指定されたセキュリティ資産は、第1種管理区域に保管しなければならない。容易に持ち運べるものは、第1種管理区域内の鍵つきの容器に保管しなければならない。

2　AA 資産は、原則として第1種管理区域内で使用しなければならない。

3　AA 資産を、機構外の関係者に使用させる場合も、前二項に準じた措置をとらなければならない。

4　指定前であっても、AA 資産に該当しうる資産の取り扱いは、第1項及び第 2 項に準じた措置をとり、セキュリティの確保に努めなければならない。

（AA 資産の持出し・輸送）

第83条　業務の必要から、やむを得ず AA 資産を第 1 種管理区域外に持ち出し、業務に供する場合は、警備員の立哨等、防護のために必要な措置をとらなければならない。AA情報の含まれる物品については、当該 AA 情報を外部から知られないための措置を講じなければならない。

2　持ち出しの際に、AA 資産の輸送を委託する場合は、AA 資産を容器等に収容し、施錠又は封印し、予め緊急時の連絡体制を整備した上で、原則として関係者が同行しなければならない。

（AA 資産の廃棄）

第84条　AA 資産を廃棄する場合は、機密性の高い物品については、そこに含まれる機微な情報が漏洩しないよう必要な措置を関係者自身が講じたうえで、廃棄しなければならない。

第3節　A 資産

（A 資産の登録）

第85条　A 資産に指定されたセキュリティ資産は、アクセスできる関係者の範囲を定めて、指定しなければならない。A情報が含まれる物品については、当該 A 情報にアクセスできる関係者の範囲と同一でなければならない。

（A 資産の保管・使用場所）

第86条　A 資産に指定されたセキュリティ資産は、第2種管理区域に保管しなければならない。容易に持ち運べるものは、第2種管理区域内の鍵つきの容器に保管しなければならない。

2　A 資産は、原則として第2種管理区域内で使用しなければならない。

3　A 資産を、貸付又は機構外の関係者に使用させる場合も、前二項に準じた措置をとらなければならない。

4　指定前であっても、A 資産に該当しうる資産の取り扱いは、第1項及び 2 項に準じた措置をとり、セキュリティの確保に努めなければならない。

（A 資産の持出し・輸送）

第87条　業務の必要から、やむを得ず A 資産を第2種管理区域外に持ち出し、業務に供する場合は、防護のために必要な措置をとらなければならない。A情報が含まれる物品については、当該A情報を外部から知られないための措置を講じなければならない。

2　持ち出しの際に、A 資産の輸送を委託する場合は、A 資産を容器等に収容し、施錠又は封印しなければならない。

（A 資産の廃棄）

第88条　A 資産を廃棄する場合は、第84条の規定を準用する。

第6章　業務のセキュリティ

（セキュリティ確保を要する業務）

第89条　機構の行う業務のうち、特にセキュリティを確保すべきものは、各部門・部等のセキュリティ統括管理責任者等が、重要度及びリスク評価に基づき、下記のカテゴリに区分し、区分に応じた管理区域内でこれを実施するものとする。

（1）AA 業務

ロケット打上げ業務、人工衛星の追跡管制業務、航空機の運用業務、ロケット・人工衛星・航空機の開発にかかる試験業務のうち、妨害等により機構のミッション達成に致命的な影響を与える恐れがあるものを AA 業務とし、第 1 種管理区域内で実施されなければならない。

（2）A 業務

AA 以外の業務のうち、A 情報以上の情報を取り扱う業務や、妨害等により機構のミッション達成に影響を与えるおそれがあるものを A 業務とし、第 2 種管理区域で実施されなければならない。

（管理区域外での業務）

第90条　業務上の必要により、前条に定めるセキュリティの確保を要する業務を、指定された管理区域外で実施するときは、可能な限り区分に応じた管理区域相当のセキュリティ確保のために必要な措置を講じなければならない。

第7章　エリアのセキュリティ

第 1 節　エリアセキュリティ通則

（管理区域の区分と指定）

第91条　機構の管理・占有する社屋及び敷地（これらの付属施設・設備を含む。以下「社屋等」という。）のうち、セキュリティを確保すべき区域（以下、「管理区域」という。）を、次の各号のとおり区分する。

（1）第 1 種管理区域

特に厳重な管理を要する区域で、関係する役職員及び機構外関係者のうち業務上特に必要性が認められ、各部門・部等のセキュリティ統括管理責任者等又はエリア管理責任者の置かれる事業所等のエリア管理責任者（以下、「エリア管理責任者等」という。）の許可を受けた者以外の者の出入りを禁止する区画。

（2）第 2 種管理区域

厳重な管理を要する区域で、関係する役職員及び機構外関係者のうち業務上必要性が認められ、エリア管理責任者等の許可を受けた者以外の者の出入りを禁止する区画。

（3）第 3 種管理区域

役職員及び受付で入域許可証を交付された者以外の者の出入りを禁止する区画。

2　情報、情報システム、有形資産及び業務のセキュリティは、前項で定めた管理区域に次表のとおり区分することにより確保する。

管理区域	分野	対象
第1種管理区域	情報	AA 情報の保管・使用
	情報システム	AA 情報に区分される情報を搭載した情報システムの保管・使用
	資産	AA 資産の保管・使用
	業務	AA 業務の実施
第2種管理区域	情報	A 情報の保管・使用、及び B 情報の保管
	情報システム	A 情報を搭載した情報システムの保管・使用、及び B 情報を搭載した情報システムの保管
	資産	A 資産の保管・使用
	業務	A 業務の実施

3　第 1 項の管理区域の指定は、エリア管理責任者等が行うものとする。設定は、原則として、第3種管理区

域を外縁とし、それぞれの直近下位のセキュリティレベルの管理区域に囲まれるように設定しなければならない。

（エリア管理責任者等の任務）

第92条　エリア管理責任者等は、管理区域の区分に応じ、本章の各節の定めるところにより、防護壁、監視装置等の整備、鍵、ID カード等の施錠管理、警備員による監視、入域管理等必要な措置を講ずるものとする。

2　エリア管理責任者等は、管理区域におけるセキュリティの確保のために必要があると認められる場合には、立ち入りの禁止その他必要な措置又は指示を行う。

3　エリア管理責任者等は、許可なく管理区域へ立ち入る等（セキュリティ確保のための設備・機器等の損壊行為を含む。）管理区域内のセキュリティに脅威を与えるおそれのある行為をさせてはならない。

4　エリア管理責任者等は、前項の行為が発生したときは、すみやかに、当該行為をしている者の退去命令若しくは中止命令又は当該行為の用に供した物の撤去命令等必要な措置を講ずるものとする。

5　エリア管理責任者等は、自己の所掌する管理区域における、管理区域の指定、防護の方法及び入域管理の方法その他のエリア管理に必要な事項を、実施要領等で定めるものとする。

（役職員等の義務）

第93条　役職員等は、第3種管理区域以上の管理区域に入場するときは、常に身分証及び入域許可証を携行しなければならない。エリア管理責任者等に求められたときは、提示しなければならない。

2　役職員等は、開錠して入域する者の後に続いて認証を受けずに入域し、或いは、他人の身分証又は入域許可証等を使用し入域してはならない。また、他人名義で入域許可を求め、或いは、鍵を借り受けてはならない。

（緊急時の入域）

第94条　エリア管理責任者等は、緊急の事態が発生したときには、消防車輌、救急車輌、警察車輌、電気・ガス事業用応急作業車輌その他法令上特別の権限を有する車輌及び者を、入域者身分証又は入域許可証を不所持のまま、管理区域に入れることができる。この場合、エリア管理責任者等は、原則として、所定の入域者身分証所持者による立会いを行わせるものとする。

（施設公開）

第95条　一般公開のイベントを含め施設の公開は、原則として第 1～第 3 種管理区域に該当しない社屋等（以下、「一般管理区域」という。）又は第3種管理区域で実施しなければならない。

2　例外的に第2種管理区域を公開するときは、エリア管理責任者等の許可のもと、情報漏えいの防止、資産の破壊防止及び業務妨害の防止に必要な措置を講じた上で、職員の立会いの下に行うことができる。

3　施設の一般公開を行うときは、エリア管理責任者等は予め防護計画を作成し、一般公開対応者及び関係するエリア管理実施責任者に周知しなければならない。また、見学者に対して、案内図、立て札、ロープなどで、公開範囲を明示しなければならない。

4　広報目的及び機構の活動への理解促進を目的として、以下に定める要件を満たした場合は、限定的に第 1 種管理区域に、関係者以外の者を業務目的以外で立ち入らせることができる。

（1）当該立ち入りが、国民への情報提供・広報活動、又は機構の活動への理解促進のうち、特に有益と認められるものであること。

（2）当該区域に格納されているセキュリティの対象が、AA 情報又は AA 資産のうち機密性の極めて高い資産である場合には、情報の盗取、漏えい等が起きないための必要な措置を講じ、完全性・可用性の極めて高い資産である場合には、盗取、破壊等の防止のために必要な措置を講じていること。

（3）エリア管理責任者等が別途定める手順に従って、その事前の入域許可を得ていること。

第 2 節　第 1 種管理区域

（第 1 種管理区域の防護）

第96条　第 1 種管理区域は、原則として第 2 種管理区域の内側に設定し、堅固な囲障を周囲に設置し、常時施錠された状態としなければならない。窓等の開口部がある場合には、容易に侵入されないよう強化しなければならない。

2　第 1 種管理区域には、内部に保管する情報、資産等のセキュリティ事案への対処のため、監視カメラ等の記録装置を設置しなければならない。

3　第 1 種管理区域内に、第91条第 2 項表に掲げるセキュリティの対象が複数格納されるときは、書庫・保管庫等を分けて収納し、アクセス制御を徹底しなければならない。

（第 1 種管理区域への入域）

第97条　エリア管理責任者等は、第 1 種管理区域で保管又は実施される第91条第 2 項表に掲げるセキュリティの対象に関係する者をあらかじめ関係者として指定しなければならない。

2　第 1 種管理区域には、原則としてあらかじめ指定された関係者のみが、当該区域で行われる業務を目的として入域することができる。

3　第 1 種管理区域においては、入域及び退場の都度、入退場の記録を残さなければならない。入域及び退場の管理は、原則として電子認証システムによるものとする。

4　第1種管理区域に入域する場合には、エリア管理責任者等が許可をした場合を除き、撮影機能付きの機器を持ち込んではならない。

5　エリア管理責任者等は、当該区域で行われる業務を目的として、関係者以外の者から第 1 種管理区域への入域許可を求められたときは、作業の目的及び内容、入域の範囲及び態様、必要性並びに妥当性等を審査して、入域を許可することができる。

（第 1 種管理区域の防護の例外）

第98条　AA 資産に区分される屋外に設置された空中線（アンテナ）等の大型構造物について、前条第 1 項の防護に必要な措置を取ることが困難又は妥当でないとエリア管理責任者等が認めるときは、周囲の第 2 種管理区域の防護のために必要な措置を強化することで、第 1 種管理区域として指定することができる。

第 3 節　第 2 種管理区域

（第 2 種管理区域の防護）

第99条　第2種管理区域は、原則として第3種管理区域の内側に設定し、強固な囲障を周囲に設置し、常時施錠された状態としなければならない。窓等の開口部がある場合には、容易に侵入されないよう強化しなければならない。

（第2種管理区域への入域）

第100条　エリア管理責任者等は、第2種管理区域で行われる業務に関係する役職員及び機構外関係者をあらかじめ関係者として指定しなければならない。

2　第2種管理区域には、原則としてあらかじめ指定された関係者及びエリア管理責任者等の許可を受けた者のみが、当該区域で行われる業務を目的として入域することができる。

3　第2種管理区域においては、入域の管理は、原則として電子認証システムによるものとする。

4　第2種管理区域で撮影をする場合は、エリア管理責任者等の許可を得なければならない。

5　エリア管理責任者等は、当該区域で行われる業務を目的として、関係者以外の者から第2種管理区域への入域許可を求められたときは、入域の目的、必要性及び妥当性等を審査して、入域を許可することがで

きる。

第 4 節　第 3 種管理区域

（第 3 種管理区域の防護）

第101条　第 3 種管理区域は、フェンス等の囲障を設置することで、一般管理区域又は機構の管理地外との境界を識別し、無用の者が立ち入れない状態としなければならない。

2　第 3 種管理区域は、原則として、外部からの侵入を検知する装置を備え、監視カメラにより常時監視を行わなければならない。

3　エリア管理責任者等は、侵入者を検知できるよう 24 時間警備を実施し、連絡体制を整備しなければならない。

4　前二項の警備により、侵入を検知したときは、エリア管理責任者等は、直ちに現状の確認を行い、侵入者を識別した場合は、予め定められた連絡網に従い、必要な通報をおこなわなければならない。

（第 3 種管理区域の入域）

第102条　第3種管理区域には、原則として役職員及びエリア管理責任者等の許可を受けた者のみが入域することができる。

2　エリア管理責任者等は、役職員以外の者から、第 3 種管理区域への入域許可を求められたときは、入域の目的を確認して、入域を許可することができる。

（第 3 種管理区域の防護の例外）

第103条　第 3 種管理区域を設定しようとする敷地の土地の形状などの物理的制約や、法令や賃貸借契約等の制約などにより、第 3 種管理区域として備えるべき防護の要件を充たすことが困難なときは、可能な範囲で防護のための措置を講じるとともに、当該区域内の内側にある第 2 種以上の管理区域の防護方法を強化しなければならない。

2　前項の制約により、侵入検知装置や監視カメラの画像の常時監視又は侵入検知時の緊急対応等の警備が困難な場合には、発報や画像を一定期間記録することでこれに代えることができる。

第8章　セキュリティ教育

（セキュリティ教育及び訓練）

第104条　最高セキュリティ責任者等は、定期及び臨時に、役職員に対しセキュリティ管理に係る教育及び訓練を行うものとする。

2　最高セキュリティ責任者等は、毎年度、役職員に対するセキュリティ教育訓練計画を策定し、これに基づき実施するものとする。

3　役職員は、前項の計画に基づくセキュリティ教育及び訓練を受けなければならない。

4　最高セキュリティ責任者等は、セキュリティ教育及び訓練の実施状況及び結果について、第 6 条に定める委員会に報告しなければならない。

第9章　セキュリティ監査

（セキュリティ監査）

第105条　セキュリティ監査責任者は、定期又は臨時にセキュリティ管理に係る監査を行うものとする。

2　セキュリティ監査責任者は、毎年度、セキュリティ監査計画を策定し、これにもとづき実施するものとする。

3　役職員は、監査に協力しなければならない。

（個人情報の点検）

第106条　セキュリティ統括管理責任者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、毎年度、個人情報保護点検計画を策定し、点検を行い、必要があると認めるときは、その結果を最高セキュリティ責任者等に報告しなければならない。

（監査結果の報告等）

第107条　セキュリティ監査責任者は、セキュリティ監査の結果について、第 6 条に定める委員会に報告しなければならない。

2　最高セキュリティ責任者等は、個人情報の点検の結果について、第 6 条に定める委員会に報告しなければならない。

3　最高セキュリティ責任者等は、セキュリティ監査及び個人情報の点検の結果を踏まえ、必要に応じ、セキュリティを確保するための措置を講ずるものとする。

第10章　契約上の措置

（契約における措置）

第108条　機構が契約を締結する場合は、当該契約者（下請け契約者を含む。以下同じ。）に対し、この規程及びセキュリティに関する機構の規則等に規定するセキュリティ確保のための以下に掲げる事項の遵守を契約上の義務とさせるとともに、遵守義務に違反した場合の規定を契約に明記しなければならない。

（1）機構のA情報以上の情報を使用させる場合は、守秘義務を負わせ、情報の複写、第三者への開示・提供等に機構の許可を要し、その保管に留意させる等、セキュリティに関する機構の諸規定と同等の措置をとらせること。

（2）機構のB情報以上の情報を使用させる場合は、情報の複写、第三者への開示・提供等に機構の許可を要し、その保管に留意させること。

（3）前二号の情報を取り扱う情報システムに関し、ウイルス対策、ファイル交換ソフトの利用禁止等、機構の情報システムセキュリティと同等の水準の対策をとらせること。B情報以上の情報を内包する資産についても同等の措置をとらせること。

（4）契約上の義務の履行のため、機構の管理区域内に入域させる場合は、事前に許可を求め、エリア管理責任者等の機構の指示に従わせること。

2　機構が、就業規則及び就業特則の適用がない個人と委嘱その他の契約を締結するときは、前項の規定を準用する。

3　機構が、大学生、大学院生、研修生等を受け入れるときは、第1項の規定を準用するとともに、必要に応じて、有形資産、情報及び情報システムへのアクセス制限、セキュリティに関する教育その他必要な措置を講ずるものとする。

（個人情報を取り扱う業務の委託）

第109条　前条に加え、機構の保有個人情報を取り扱う業務（当該業務において、新たに機構の名義をもって個人情報を取得させる場合を含む。以下同じ。）を、委託するときは、個人情報の適切な管理を行う能力がある者に行わせなければならない。

2　前項の委託を行わせるときは、前条第1項各号に定める事項に加え、契約書に以下に掲げる事項を明記するとともに、委託先における責任者等の管理体制、個人情報の管理の状況についての検査に関する事項等必要な事項について書面で確認しなければならない。

（1）個人情報に関する秘密保持等の義務

（2）再委託の制限又は条件に関する事項

（3）個人情報の複製の制限に関する事項

（4）個人情報の漏洩等の事案発生時の対応に関する事項

（5）委託終了時における個人情報の消去及び媒体の返却に関する事項
（6）違反した場合における契約解除、損害賠償等その他必要な事項
3　機構の保有個人情報を取り扱う業務を、派遣労働者に行わせるときは、労働者派遣契約書に秘密保持義務等個人情報の取り扱いに関する事項を明記しなければならない。

第11章　セキュリティ事案等への対応
（セキュリティ事案等への対応）
第110条　各部門・部等のセキュリティ統括管理責任者は、セキュリティ事案が発生した場合に備え、あらかじめ緊急処理体制を確立しておくものとする。
2　セキュリティ事案に該当すると思われる事象を発見した役職員は、速やかに、適切な応急処置をとるとともに、第一報として、各部門・部等のセキュリティ統括管理責任者へ報告する。
3　前項の第一報を受けた各部門・部等のセキュリティ統括管理責任者は、必要に応じ速やかに緊急処理体制を発動する等の適切な処置を講ずるものとする。また、明らかにセキュリティ事案に該当しないと判断できる場合を除き、最高セキュリティ責任者等に報告し、必要な指示を受けるものとする。
4　セキュリティ事案の発生した各部門・部等のセキュリティ統括管理責任者は、事案の事実関係の調査及び原因究明を行い、再発防止策を講じるとともに、それらの内容を整理のうえ、最終報告として最高セキュリティ責任者等に報告するものとする。
5　報告を受けた最高セキュリティ責任者等は、必要に応じて、類似事案の発生防止のため、各部門・部等のセキュリティ統括管理責任者に調査を命じ、必要な措置をとるよう指示する。また、特に重大なセキュリティ事案については、副理事長及び理事長に報告するものとする。

（個人情報の漏えいを含む場合の措置）
第111条　各部門・部等のセキュリティ統括管理責任者は、個人情報の漏えいに関するセキュリティ事案の場合には、事案の内容、影響等に応じて、事実関係の公表、当該事案に係る本人への対応等の措置を講ずるものとする。
2　理事長は、個人情報の漏えいに関する重大な事案の報告を受けた場合、その実情調査及び原因究明を行い、再発防止のために必要な措置を講ずるとともに再発防止策の公表を行う。

（懲戒等）
第112条　第3条第1項第11号のセキュリティ事故については、その違反の程度に応じ、就業規則又は就業特則に基づく懲戒等の措置を行うものとする。
2　最高セキュリティ責任者等は、セキュリティ事案の報告を受け、当該事案がセキュリティ事故に該当すると認めるときは、前項の措置を行うため人事部長に報告するものとする。

第12章　雑則
（事務の委任）
第113条　最高セキュリティ責任者等及びセキュリティ統括管理責任者は、必要な事項を指示して、この規程に定める事務を委任することができる。

（特例措置）
第114条　最高セキュリティ責任者等は、機構のセキュリティ確保のために特に必要と認められる場合は、セキュリティの対象へのアクセス制限その他必要な措置を行うことができる。
2　セキュリティ統括管理責任者は、緊急にセキュリティの対象へのアクセスの必要が生じ、本規程に定める手続きを経ていては、業務の円滑かつ適切な遂行に著しい支障を及ぼすと認めるときは、セキュリティ確保に支障を及ぼさない範囲で自らの判断で、臨時の措置として、本規程の定めるところによらず、関係者

以外の者にアクセスを許すことができる。
3　前二項の措置を取った場合は、事後に台帳への記録等、必要な手続きを行わなければならない。

（監査時等のアクセス）
第115条　最高セキュリティ責任者等及びその委任を受けたもの、又はセキュリティ監査責任者が、第105条に定めるセキュリティ監査、第78条に定める禁止行為の調査、第110条に定めるセキュリティ事案等の対応及び前条第 1 項の措置を目的として、第5条で定めるセキュリティの対象となる情報、情報システム、有形資産及び業務にアクセスし、各管理区域に立ち入る場合は、各部門・部等のセキュリティ統括管理責任者又はエリア管理責任者等の許可を得ることを要しない。但し、その場合においても、情報、有形資産及び業務について、機密性を有する内容に触れないことを条件とする。

（その他）
第116条　本規程の実施にあたり必要な事項は、第6条に定める委員会での調整を経て、セキュリティ・情報化推進部長が別に定めるところによる。

附　則
この規程は、平成15年10月1日から施行する。

附　則（平成16年3月29日　規程第16-27号）
この規程は、平成16年4月1日から施行する。

附　則（平成 16 年 6 月 29 日　規程第 16-39 号）
この規程は、平成16年7月1日から施行する。

附　則（平成 16 年 11 月1日　規程第 16-55 号）
この規程は、平成16年11月1日から施行する。

附　則（平成 17 年 5 月 12 日　規程第 17-46 号）
この規程は、平成17年5月12日から施行し、平成17年5月1日から適用する。

附　則（平成17年7月19日　規程第17-69号）
この規程は、平成17年7月19日から施行し、平成17年7月1日から適用する。

附　則（平成17年9月30日　規程第17-105号）
この規程は、平成17年10月1日から施行する。

附　則（平成18年4月25日　規程第18-28号）
この規程は、平成18年5月1日から施行する。

附　則（平成19年4月4日　規程第19-13号）
この規程は、平成19年4月4日から施行し、平成19年4月1日から適用する。

附　則（平成19年8月8日　規程第19-62号）

この規程は、平成19年8月8日から施行し、平成19年8月1日から適用する。

附　則（平成20年3月25日　規程第20-25号）

この規程は、平成20年4月1日から施行する。

附　則（平成21年10月20日　規程第21-43号）

この規程は、平成21年11月2日から施行する。

附　則　（平成22年4月14日　規程第22－32号）

この規程は、平成22年4月14日から施行する。

附　則　（平成２３年１１月３０日　規程第２３－５３号）

１．この規程は、平成２４年４月１日から施行する。本規程の施行に際して、本規程以外の規程、理事長決定、本部長決定、通達及び部長決定のうち「情報セキュリティ規程」又は「情報システムセキュリティ規程」とあるのは「セキュリティ規程」と、「情報セキュリティ管理責任者」並びに有形資産又は業務のセキュリティに関して「各本部・部等の長」とあるのは「セキュリティ統括管理責任者」と、「秘情報」「部外開示制限情報」「社外開示制限情報」とあるのは、それぞれ「AA 情報」「A 情報」「B 情報」と読替えるものとする。また、機構内の文書の区分表示で「秘情報」「部外開示制限情報」「社外開示制限情報」と表示されているものは、それぞれ「AA 情報」「A 情報」「B 情報」と表示を読替えるものとする。

２．「情報セキュリティ規程（規程第１５－４８号）」、「情報システムセキュリティ規程（規程第１５－４９号）」及び「特殊輸入機器管理規程（規程第１５－５２号）」は、廃止する。

３．本規程の施行に伴い、制文規程（規程第１５－１号）第3条から第7条までに定める他の規程、理事長決定、本部長決定、通達及び部長決定のうち、規程の名称、責任者の名称及び情報区分の名称のみを変更する必要があるものについては、本規程により改正するものとする。

４．過去に文書管理規程（規程第１５－２１号）の規定により、「取扱指定文書」に指定されたものについては、本規程第 26 条第 1 項の規定に基づき、各本部・部等のセキュリティ統括管理責任者が「B 情報」として指定したものとみなす。

附　則　（平成25年3月28日　規程第25－19号）

この規程は、平成25年4月1日から施行する。

附　則　（平成26年3月27日　規程第26－16号）

この規程は、平成26年4月1日から施行する。