情報セキュリティ規程

平成15年10月1日　規程第15-48号
改正:平成16年3月29日　規程第16-28号
改正:平成 16 年 6 月 29 日　規程第 16-40 号
改正:平成 17 年 5 月 12 日　規程第 17-47 号
改正:平成 17 年 9 月 30 日　規程第 17-106 号
改定:平成 20 年 3 月 25 日　規程第 20-23 号
改正:平成 22 年 4 月 14 日　規程第 22－33 号

第1章　総則

（目的）

第1条　この規程は、セキュリティ規程（規程第15-47号）第24条の規定に基づき、盗取、漏えい、改ざん、破壊、消去、焼失その他の脅威から、独立行政法人宇宙航空研究開発機構(以下「機構」という。)の重要な情報を防護するとともに、その機密性、完全性及び可用性を確保すること(以下「情報セキュリティ」という。)について、基本的な事項を定めることを目的とする。

（定義）

第2条　この規定において、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) 「情報」とは、文書、図面及び電磁的記録をいう。

(3) 「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。

(4) 「閲覧」とは、関係する役員及び職員（以下「役職員」という。）または機構外の関係者に対し、第13条に定める閲覧場所で情報を開示することをいう。

(5) 「複製」とは、役職員が手書き、複写機等の機器または情報システムの利用により、情報の副本を作成することをいう。当該副本は、以下「複製情報」という。

(6) 「持出し」とは、役職員が情報を第12条に定める保管場所の外に移動させ、当人の管理の下に置くことをいう。

(7) 「貸出し」とは、役職員が指定した期日までの間に限り、機構内外の者に情報を預け、相手方の管理の下に置くことをいう。

(8) 「送付」とは、機構内外の者に情報を渡し、廃棄を含め相手方の管理の下に置くことをいう。

(9) 「各本部・部等」とは、セキュリティ規程（規程第 15―47）第 2 条第 4 号に定める機構の本部・部等の組織をいう。

第2章　情報の区分

（情報の区分）

第3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する。

(1) 極秘情報
　秘密の保全が最高度に必要であってその漏洩が国の安全又は利益に著しく損害を与えるおそれがあるもの

(2) 秘情報
　秘密の保全が必要であってその漏洩が国の安全若しくは利益に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

(3) 部外開示制限情報
　開示することにより、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、共同研究契約等の相手方の利益、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り、機構内外の関係者以外に開示が制限されているもの

(4) 社外開示制限情報

開示することにより、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、共同研究契約等の相手方の利益、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り、役職員及び機構外の関係者以外に開示が制限されているもの

第3章　管理区域

（管理区域の区分）

第4条　機構の社屋及び敷地(これらの附属施設・設備を含む。以下「社屋等」という。)のセキュリティの確保を効果的かつ効率的に実施するため、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、セキュリティ規程(規程第15―47号)第11条に規定するエリア管理責任者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、セキュリティ規程(規程第15―47号)第11条に規定するエリア管理責任者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。

第4章　情報セキュリティの管理体制

（情報セキュリティ統括）

第5条　機構に情報セキュリティ統括を置く。

2　情報セキュリティ統括は、セキュリティ担当理事をもってあてる。

3　情報セキュリティ統括は、情報セキュリティに関する業務を統括する。

（情報セキュリティ管理責任者）

第6条　各本部・部等に情報セキュリティ管理責任者を置く。

2　情報セキュリティ管理責任者は、各本部・部等の長をもってあてる。

3　情報セキュリティ管理責任者は、所属する各本部・部等の保有する情報のセキュリティに関する業務を統括する。

（情報セキュリティ管理責任者補佐）

第7条　各本部・部等の情報セキュリティ管理責任者の下に情報セキュリティ管理責任者補佐を置く。

2　情報セキュリティ管理責任者補佐は、情報セキュリティ管理責任者が指名し、情報セキュリティ管理責任者の命を受け、所属する各本部・部等の保有する情報のセキュリティに関する業務を総括整理する。

（情報セキュリティ担当者）

第8条　文書管理規程(規程第15―21号)第4条に定める担当課等に情報セキュリティ担当者を置く。

2　情報セキュリティ担当者は、文書管理規程第7条に定める文書管理担当者の他、必要に応じ情報セキュリティ管理責任者が指名する者をもってあてる。

3　情報セキュリティ担当者は、担当課等における情報セキュリティに関する事務を行う。

第5章　秘密情報等の管理

（秘密情報等の管理並びに指定及び解除）

第9条　極秘情報、秘情報、部外開示制限情報及び社外開示制限情報(以下「秘密情報等」という。)の管理並びに指定及び解除は、次の各号に定めるところにより行う。

(1) 極秘情報は、情報セキュリティ統括がその管理にあたるものとし、取扱い期間及び情報にアクセスできる者を定めて指定及び解除する。
(2) 秘情報は、情報セキュリティ管理責任者又は情報セキュリティ管理責任者の命を受け事務の委任を受けた情報セキュリティ管理責任者補佐のうち決裁規程別表第1に定める部長等にあたる者がその管理にあたるものとし、取扱い期間及び情報にアクセスできる者を定めて指定及び解除する。
(3) 部外開示制限情報は、情報セキュリティ管理責任者又は情報セキュリティ管理責任者の命を受け事務の委任を受けた情報セキュリティ管理責任者補佐(以下「情報セキュリティ管理責任者等」という。)がその管理にあたるものとし、取扱い期間及び情報にアクセスできる組織又は者を定めて指定及び解除する。
(4) 社外開示制限情報は、情報セキュリティ管理責任者等がその管理並びに指定及び解除を行う。
2 取扱い期間が満了した秘密情報等は、取扱い期間が延長された場合を除き、指定が解除されたものとみなす。

(秘密情報等の識別表示)
第10条 極秘情報は、「極秘」と表示するなどの方法により識別しなければならない。
2 秘情報は、「秘」と表示するなどの方法により識別しなければならない。
3 部外開示制限情報は、「部外開示制限」と表示するなどの方法により識別しなければならない。
4 社外開示制限情報は、「社外開示制限」と表示するか又は情報セキュリティ管理責任者等が別に定める方法により識別しなければならない。

(台帳類の整備)
第11条 情報セキュリティ統括は、極秘情報のセキュリティ管理を行うため、登録台帳及び管理台帳を作成するものとする。
2 情報セキュリティ管理責任者等は、秘情報及び部外開示制限情報のセキュリティ管理を行うため、登録台帳及び管理台帳を作成するものとする。

(秘密情報等の保管)
第12条 極秘情報は、第1種管理区域に設置した鍵のかかる書庫等に保管するものとする。
2 秘情報は、第1種管理区域に保管するものとする。
3 部外開示制限情報は、第2種管理区域に設置した鍵のかかる書庫等に保管するものとする。
4 社外開示制限情報は、第2種管理区域に保管するものとする。

(秘密情報等の閲覧)
第13条 極秘情報の閲覧は、情報セキュリティ統括の許可を得て、第1種管理区域で行うものとする。
2 秘情報の閲覧は、情報セキュリティ管理責任者等の許可を得て、第1種管理区域で行うものとする。
3 部外開示制限情報及び社外開示制限情報の閲覧は、第2種管理区域で行うものとする。

(秘密情報等の複製)
第14条 役職員は、業務上特に必要があり、情報セキュリティ統括を経て理事長の承認を得た場合を除き極秘情報を複製してはならない。
2 役職員は、業務上特に必要があり、情報セキュリティ管理責任者等の承認を得た場合を除き、秘情報または部外開示制限情報を複製してはならない。
3 役職員は、社外開示制限情報を、業務に必要な場合に限り、最小限の範囲において、複製することができる。
4 秘密情報等を複製した場合、複製情報は原本と同様に取り扱うものとする。

(管理区域外への持ち出し)
第15条 役職員は、業務上特に必要があり、情報セキュリティ統括を経て理事長の承認を得た場合を除き第1種管理区域外に極秘情報を持ち出してはならない。
2 役職員は、業務上特に必要があり、情報セキュリティ管理責任者等の承認を得た場合を除き、第1種管理区域外に秘情報の持出しをしてはならない。
3 役職員は、業務上特に必要があり、情報セキュリティ管理責任者等の承認を得た場合を除き、第2種管理

区域外に部外開示制限情報の持出しをしてはならない。
4 役職員は、秘密情報等の持出しをするときは、常に携行しなければならない。また、情報システムを利用して秘密情報等の持出しをする場合には、第 19 条第 3 項に基づき取り扱われる情報システムを使用する。

（廃棄）
第16条 秘密情報等を廃棄するときは、焼却、細断、消去等の方法により、復元できないように確実に行わなければならない。

（貸出し）
第17条 役職員は、業務上特に必要があり、情報セキュリティ統括を経て理事長の承認を得た場合を除き、機構内外の者に極秘情報の貸出をしてはならない。
2 役職員は、業務上特に必要があり、情報セキュリティ管理責任者等の承認を得た場合を除き、機構内外の者に秘情報、部外開示制限情報及び社外開示制限情報の貸出しをしてはならない。ただし、社外開示制限情報の役職員への貸出しは、この限りでない。
3 前項の規定により貸出しを行った場合には、指定された期日までに返却させなければならない。

（送付）
第18条 極秘情報は、送付してはならない。
2 役職員は、業務上特に必要があり、情報セキュリティ管理責任者等の承認を得た場合を除き、秘情報、部外開示制限情報及び社外開示制限情報を機構内外の者に送付してはならない。ただし、社外開示制限の役職員への送付は、この限りでない。

（秘情報の持出し、貸出しまたは送付の条件及び方法）
第 18 条の 2 秘情報を第 9 条第 1 項第 2 号により指定を受けた機構外の者に貸出しまたは送付するときは、情報セキュリティ管理責任者等は、当該者が所属する法人等に、以下の事項を確約させなければならない。
(1) 第 4 条第 1 号に定める管理区域に相当する区域を備え、当該者以外のアクセスを規制すること
(2) 第 5 条または第 6 条に相当する取扱責任者を定めること
(3) その他本規程に定める必要な措置を定めた社内規則を備え、当該社内規則に従って情報を取り扱うこと。
2 秘情報の原本及び情報システムの利用による複製情報は、持出し、貸出しまたは送付してはならない。
3 秘情報を貸出しまたは送付する場合の方法は、情報セキュリティ管理責任者等の責任の下、手渡しによる接受のみとする。
4 前2項に関わらず、緊急を要しかつ業務の円滑かつ適切な遂行に著しい支障を及ぼすと情報セキュリティ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、または第 19 条に基づき取り扱われる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貸出しまたは送付することができる。

（部外開示制限情報の貸出しまたは送付の条件及び方法）
第 18 条の 3 部外開示制限情報を第 9 条第 1 項第 3 号により指定を受けた機構外の者に貸出しまたは送付するとき時は、当該者以外に開示しないことを所属する法人等に確約させなければならない。
2 部外開示制限情報の原本を持出し、貸出しまたは送付してはならない。
3 部外開示制限情報を貸出しまたは送付する場合の方法は、以下の各号のいずれかによる。
(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、送付先の電話番号、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送付直前に受信者に連絡のうえ、送付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。

（情報システムにおける取扱い）
第 19 条 極秘情報及び秘情報を搭載する情報システムは、第 1 種管理区域内に設置するとともに、第 1 種管理区域外に接続するネットワークに記録及び格納してはならない。ただし、第 18 条の 2 第 4 項に規定する

場合はこの限りでない。
2 秘情報の記録、処理、通信等の業務処理を行う情報システムには、役職員を認証するシステムを導入する等十分なセキュリティ対策を講ずるものとする。
3 前 2 項に定めるもののほか、秘密情報等を搭載する情報システムの取扱いについては、情報システムセキュリティ規程(規程第 15―49 号)にて定める。

(教育及び訓練)
第20条 情報セキュリティ統括は、毎年度、役職員に対する情報セキュリティ教育訓練計画を策定し、各本部・部等の協力を得て実施するものとする。
2 役職員は、前項の計画に基づく情報のセキュリティ教育及び訓練を受けなければならない。

(監査)
第21条 情報セキュリティ統括は、毎年度、情報セキュリティ監査計画を策定し、実施するものとする。
2 役職員は、前項の監査に協力しなければならない。
3 情報セキュリティ統括は、第1項の監査の結果を踏まえ、必要に応じ、情報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。

(契約等における措置)
第22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義務を遵守すること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。
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、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義務を遵守することを契約上の義務とするとともに、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。
3 機構が、大学生、大学院生、研修生等を受け入れるときは、前項の規定を準用するとともに、必要に応じて、情報へのアクセス制限、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。

第23条 (削除)

第24条 (削除)

(情報セキュリティ確保のための措置)
第25条 情報セキュリティ統括は、情報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、秘密情報等へのアクセスの制限その他必要な措置を行うことができる。

第6章 役職員の心得等

(役職員の心得)
第26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洩することのないよう十分に注意しなければならない。

(指定前の情報の取扱い)
第 27 条 役職員は、秘密情報等の区分の指定を受ける前であっても、機構の重要な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、情報セキュリティの確保に努めるものとする。ただし、極秘情報及び秘情報の情報については、情報の作成開始時に第 9 条第1項第1号及び第 2 号の定めに準じた措置を実施しなければならない。

第28条 (削除)

第7章　雑則

（事務の委任）

第29条　情報セキュリティ統括、情報セキュリティ管理責任者及び情報セキュリティ管理責任者補佐は、理事長の承認を得て、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30条　情報セキュリティ管理責任者は、緊急に秘情報及び部外開示制限情報を使用する必要が生じ、この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、臨時の措置として、指定された者以外に情報を閲覧、アクセスさせるなどの特例措置を講ずることができる。

（受託業務のセキュリティに係る要求の優先）

第31条　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、当該要求に基づきセキュリティ管理を行うものとする。

（法令等の優先）

第32条　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、この場合においても、閲覧等を行う国等に対して、当該情報は秘密情報等である旨を連絡するとともに、可能な範囲で関係者以外に漏らさないこと、鍵のかかる書庫に保管すること等情報セキュリティ確保に必要な措置を要請するものとする。

第33条　（削除）

（細則）

第34条　この規程を実施するために必要な事項は、各本部・部等の長が通達等により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　16―28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　第16－40号）

この規程は、平成16年7月1日から施行する。

附　則（平成 17年5月12日　第17－47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9月30日　第17－106号）

この規程は、平成17年10月1日から施行する。

附則（平成20年3月25日　規程第20－23号）

1　この規程は、平成20年4月1日より施行する。

2　本規程第3条(3)に定める情報区分の定義の変更にともない、制文規程第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、同様の変更を要するものについては、本規程により改正するものとする。

附則　（平成22年4月14日　規程第22－32号）

1 この規程は、平成22年4月14日から施行する。

２ 特殊技術資料取扱規程（平成15年10月1日　規程第15－50号）及び特殊コンピュータ・プログラム取扱規程（平成15年10月1日　規程第15－51号）は、廃止する。