情報セキュリティ規程

平成２８年１１月９日　規程第２８－７３号
改正：平成　３１年3月２５日　規程第３１－１８号
改正：令和４年3月３１日　規程令和第４－２３号

（目的及び適用範囲）

第１条　本規程は、サイバーセキュリティ基本法（平成２６年法律第１０４号）第１３条に基づきサイバーセキュリティ戦略本部が定めた「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）に基づき、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。）の情報、情報システム及び有形資産の情報セキュリティを確保するために必要な基本的事項を定める。

２　外部の機関から情報セキュリティ確保に関して本規程とは異なる要請があり理事長がこれを認めたときは本規程によらないことができる。

（定義）

第２条　本規程中の用語の定義は次の各号に定めるところによるほか、統一基準の最新版に定めるところによる。

（１）「部門・部等」とは、組織規程（規程第１５－３号）第５条から第１０条の規定により機構に置かれる組織をいう。ただし、同規程第７条第２項の規定により機構に置かれる組織を除く。

（２）「ＣＳＩＲＴ」とは、発生した情報セキュリティインシデントに対処するため機構に設置される体制をいう（Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍの略）。

（３）「情報」とは、以下のすべてをいう。

（ア）役職員が業務上使用することを目的として機構が調達し、又は開発した情報処理若しくは通信の用途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）その他の情報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。）であって、役職員が業務上取り扱う情報

（ウ）（ア）及び（イ）のほか、機構が調達し、又は開発した情報システムの設計又は運用管理に関する情報

（エ）（ア）から（ウ）までのほか、役職員が業務上取り扱う情報であって、文書又は有形資産に化体された情報

（４）「情報セキュリティ」とは、情報の機密性、完全性、可用性を維持することをいう。

（５）「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象（本規程又は情報セキュリティ関係規程への違反若しくは不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象をいう。）、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

（６）「情報セキュリティ対策」とは、第１６条により定められた対策基準及び対策推進計画に基づく実施事項をいう。

（７）「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機構が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

（８）「有形資産」とは、以下に定めるものその他の有体物（情報を内包するものに限る。）のうち、情報システムに区分されないものであって、機構が調達又は開発するもの（管理を外部委託しているものを含む。）及び機構内で管理しているものをいう。

（ア）ロケット

（イ）人工衛星

（ウ）（ア）及び（イ）に必要な設備
（エ）（ア）から（ウ）までを構成する機器及び材料
（９）「内包」とは、一体不可分な状態（分離することにより性質又は価値を損なう場合を含む。）で組み込まれていることをいい、形状又は配合として組み込まれていることを含む。
（１０）「業務委託」とは、機構の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、すべて含むものとする。ただし、当該業務において機構の情報を取り扱わせる場合に限る。
（１１）「外部サービス」とは、機構外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において機構の情報が取り扱われる場合に限る。

（最高情報セキュリティ責任者）
第３条　機構に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責任者を置く。
２　最高情報セキュリティ責任者は、セキュリティ・情報化推進担当理事をもってあてる。
３　最高情報セキュリティ責任者は、情報セキュリティに係る重要事項につき理事会議に報告する。

（最高情報セキュリティ副責任者）
第３条の２　機構に、最高情報セキュリティ責任者を補佐し、最高情報セキュリティ責任者の命を受けて機構の情報セキュリティに関する事務を総括整理する最高情報セキュリティ副責任者を置く。
２　最高情報セキュリティ副責任者は、セキュリティ・情報化推進担当理事補佐をもってあてる。

（情報セキュリティ委員会）
第４条　機構に情報セキュリティ委員会を置く。
２　情報セキュリティ委員会は、機構の情報セキュリティに係る対策基準、対策推進計画のほか、情報セキュリティに関し必要な事項について審議する。
３　情報セキュリティ委員会の構成については最高情報セキュリティ責任者が定める。

（情報セキュリティ監査責任者）
第５条　機構に、情報セキュリティ対策の実施状況に係る監査に関する事務を統括する者として情報セキュリティ監査責任者を置く。
２　情報セキュリティ監査責任者は、評価・監査部長をもってあてる。

（情報セキュリティ責任者）
第６条　部門・部等に、各部門・部等の情報セキュリティ対策に関する事務を統括する情報セキュリティ責任者を置く。
２　情報セキュリティ責任者は部門・部等の長をもってあてる。

（情報セキュリティ責任者補佐）
第７条　情報セキュリティ責任者の下に情報セキュリティ責任者補佐を置く。
２　情報セキュリティ責任者補佐は、情報セキュリティ責任者が指名し、その命を受け、各部門・部等のセキュリティに関する業務を整理する。

（統括情報セキュリティ責任者）
第８条　機構に、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ため、統括情報セキュリティ責任者を置く。
２　統括情報セキュリティ責任者はセキュリティ・情報化推進部長をもってあてる。

（区域情報セキュリティ責任者）
第９条　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の区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者を置く。
２　区域情報セキュリティ責任者は社屋等管理規程実施要領（総務部長通達第１５－８号）第１４条に基づき置かれた社屋等管理実施責任者をもってあてる。ただし、社屋等管理実施責任者が置かれていない場合は、社屋等管理責任者をもってあてる。

（情報セキュリティ管理者）
第１０条　情報セキュリティ責任者の下に、部署ごとに情報セキュリティ対策に関する事務を管理する情報セキュリティ管理者を置く。
２　情報セキュリティ管理者は、情報セキュリティ責任者の直近下位の組織の長又は情報セキュリティ責任者が指名する者をもってあてる。

（ＩＴマネージャ）
第１１条　情報セキュリティ責任者は、それぞれの部門・部等にＩＴマネージャを置くことができる。
２　ＩＴマネージャは、情報セキュリティ責任者が、その担当する範囲を指定して指名する者をもってあてる。
３　ＩＴマネージャは、指定された範囲における情報セキュリティに関する事務を行う。
４　ＩＴマネージャは、複数置くことができる。

（情報システムセキュリティ責任者）
第１２条　情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する業務の責任者として情報システムセキュリティ責任者を当該情報システムの企画に着手するまでに選任する。

（最高情報セキュリティアドバイザー）
第１３条　機構に情報セキュリティに関して専門的な知識及び経験に基づき最高情報セキュリティ責任者に対して助言等を行う最高情報セキュリティアドバイザーを置く。
２　最高情報セキュリティアドバイザーは最高情報セキュリティ責任者が指名又は委嘱する者をもってあてる。

（ＣＳＩＲＴ）
第１４条　機構に、発生した情報セキュリティインシデントに対処するためＣＳＩＲＴを設置する。
２　最高情報セキュリティ責任者は、役職員のうち専門的な知識又は適性を有すると認められる者をＣＳＩＲＴメンバーとして選任する。
３　最高情報セキュリティ責任者は、ＣＳＩＲＴメンバーのうち、機構における情報セキュリティインシデントに対応するための責任者としてＣＳＩＲＴ長を置くとともに、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う者を定める。

（兼務の禁止）
第１５条　役職員は、情報セキュリティ対策の運用において、以下の役割を兼務してはならない。
（ア）承認又は許可（以下「承認等」という。）が必要とされている場合に、当該承認等を求める申請者と当該承認等を行う者（以下「承認権限者等」という。）
（イ）監査を受ける者とその監査を実施する者
２　役職員は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が

承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得なければならない。

（対策基準及び対策推進計画の策定）

第１６条　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、情報セキュリティ対策を総合的に推進するための対策推進計画を定める。

２　対策推進計画には、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全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含める。

（１）情報セキュリティに関する教育

（２）情報セキュリティ対策の自己点検

（３）情報セキュリティ監査

（４）情報システムに関する技術的な対策を推進するための取組み

（５）前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組み

３　セキュリティ・情報化推進部長は、情報セキュリティ委員会における審議を経るとともに最高情報セキュリティ責任者の承認を得て、統一基準に準拠し、かつ機構の業務、取り扱う情報、保有する情報システム及び有形資産に関するリスク評価の結果を踏まえた対策基準をセキュリティ・情報化推進部長通達として制定する。

４　前項の対策基準には次の各号に定める事項を含める。

（１）情報、情報システム及び有形資産の格付基準

（２）業務委託により役職員以外の者に機構関連業務を行わせる場合の対策

（３）外部サービスの利用に関する対策

（４）雇用の開始、終了及び人事異動時等に関する情報セキュリティ対策

（情報セキュリティ対策に関する実施手順の整備）

第１７条　統括情報セキュリティ責任者は、本規程又は本規程に基づき定める対策基準により実施手順を整備すべき者が別に定められている場合を除き、機構における情報セキュリティ対策に関する実施手順を整備し、実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告する。

（課題等の報告義務）

第１８条　情報セキュリティ責任者又は情報セキュリティ管理者は、役職員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しなければならない。

２　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しなければならない。

（違反に係る報告義務）

第１９条　役職員は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ責任者にその旨を報告しなければならない。

２　情報セキュリティ責任者は、前項の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任者を通じて、最高情報セキュリティ責任者に報告しなければならない。

（例外措置手続き）

第２０条　最高情報セキュリティ責任者は、定められた対策の内容と異なる代替の方法を採用すること又は定められた対策を実施しないこと（以下「例外措置」という。）の適用の申請を審査する者（以下

「許可権限者」という。）及び審査手続きを別途定める。
2　統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求める。
3　役職員は、業務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ることを条件として、代替の方法を採用し又は規定されている方法を実施しないことができる。
4　許可権限者は、例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者に報告する。
5　統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告する。

（セキュリティ教育）
第２１条　統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。
2　情報セキュリティ管理者は、前項に定める教育実施計画に基づき、役職員に対して、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。
3　役職員は、第１項に定める教育実施計画に従って、適切な時期に教育を受講しなければならない。
4　情報セキュリティ管理者は、ＣＳＩＲＴメンバーに教育を適切に受講させる。
5　情報セキュリティ管理者は、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へ報告する。
6　統括情報セキュリティ責任者は、教育の実施状況を分析及び評価し、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係る教育の実施状況について報告する。
7　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、役職員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さなければならない。

（情報セキュリティインシデントに備えた事前準備）
第２２条　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む機構関係者への報告手順を整備し、報告が必要な具体例を含め、役職員に周知する。
2　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の機構外との情報共有を含む対処手順を整備する。
3　統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、機構業務の実施のため特に重要と認めた情報システム及び有形資産について、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。
4　統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、機構業務の実施のため特に重要と認めた情報システム及び有形資産について、その訓練の内容及び体制を整備する。
5　統括情報セキュリティ責任者は、情報セキュリティインシデントについて機構外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機構外の者に明示する。
6　統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認する。

（情報セキュリティインシデントへの対処）
第２３条　役職員は、情報セキュリティインシデントの可能性を認知した場合には、機構の報告窓口に報告し、指示に従わなければならない。
2　ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。
3　ＣＳＩＲＴ長は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責

任者に速やかに報告する。
４　ＣＳＩＲＴは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行う。
５　情報システムセキュリティ責任者は、所管する情報システムにつ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、定められた対処手順又はＣＳＩＲＴの指示若しくは勧告に従って、適切に対処する。
６　ＣＳＩＲＴは、機構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、機構を所管する国の行政機関に連絡する。
７　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。
８　ＣＳＩＲＴは、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて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に対して、対処全般に関する指示、勧告又は助言を行う。
９　ＣＳＩＲＴは、ＣＳＩＲＴ以外の者が行った情報セキュリティインシデントに関する対処の内容を聴取するとともに、ＣＳＩＲＴが自ら行った対処内容と合わせてこれを記録する。
１０　ＣＳＩＲＴは、情報セキュリティインシデントに関して、機構を所管する国の行政機関の方針に基づき、機構を所管する国の行政機関を含む関係機関と情報共有を行う。

（情報セキュリティインシデントの再発防止・教訓の共有）
第２４条　情報セキュリティ責任者は、ＣＳＩＲＴから応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告する。
２　最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示する。
３　ＣＳＩＲＴ長は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者、その他必要な者に共有する。

（情報セキュリティ対策の自己点検）
第２５条　統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定する。
２　情報セキュリティ責任者は、役職員ごとの自己点検票及び自己点検の実施手順を整備し、年度自己点検計画に基づき役職員に自己点検の実施を指示する。
３　役職員は、前項の指示に基づき自己点検を行わなければならない。
４　情報セキュリティ責任者は、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等の観点から自己点検結果を分析及び評価し、評価結果を統括情報セキュリティ責任者に報告する。
５　統括情報セキュリティ責任者は、前項の自己点検結果を踏まえ、機構に共通の課題の有無を確認する等の観点から自己点検結果を分析及び評価し、評価結果を最高情報セキュリティ責任者に報告する。
６　最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、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改善を指示し、改善結果の報告を受ける。
７　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、役職員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さなければならない。

（監査）
第２６条　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を策定する。
２　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と判断した場合には、追加の監査実施計画を定める。
３　情報セキュリティ監査責任者は、次の各号に定める事項を含む監査を実施する。
（１）機構の対策基準に統一基準を満たすための適切な事項が定められていること
（２）実施手順が機構の対策基準に準拠していること
（３）被監査部署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
４　情報セキュリティ監査責任者は、監査結果を監査報告書として最高情報セキュリティ責任者に報告する。
５　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。
６　統括情報セキュリティ責任者は、前項の指示のうち、機構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。
７　情報セキュリティ責任者は、本条第５項の指示のうち、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。

（対策基準、対策推進計画等の見直し）
第２７条　最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策基準について必要な見直し及び対策推進計画についての定期的な見直しを行う。
２　統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告する。

第２８条　削除

（管理区域の設定）
第２９条　総務部長は、本規程及び本規程に基づき定める対策基準を参照したうえで、管理区域等のセキュリティ対策について必要な事項を定める。

附　則
１．この規程は平成２８年１１月９日から施行し、平成２８年１１月１日から適用する。
２．セキュリティ規程（規程第１５―４７号）については廃止する。
３．前項にかかわらず、セキュリティ規程第２１条から第６４条、第６９条、第７０条から第７１条、第７３条から第７８条及び第１０８条については、本規程第１６条第３項に定める対策基準が制定されるまでの間、なお効力を有するものとする。
４．本附則第２項にかかわらず、セキュリティ規程第１５条、第９１条から１０３条までについては、平成２９年１月３１日までの間、なお効力を有するものとする。
５．本規程の施行に伴い、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、部門長決定、通達及び部長決定のうちその規定において「セキュリティ規程」とあるものを「情報セキュリティ規程」とのみに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。また、「セキュリティ規程」とあるものを「総務部長が定めるところ」とのみ変更する必要があるものについても、同様とする。
６．本規程の施行に伴い、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、部門長決定、通達及び部長決定のうちその規定において「セキュリティ規程」とあるものが、本附則第４項に定める「セキュリティ規程」の各条項に該当する場合、本附則第４項でさだめられた期間、「セキュリティ規程」がなお効力を有するものとする。

附　則（平成３１年３月２５日　規程第３１－１８号）
この規程は、平成３１年４月１日から施行する。

附　則（令和４年３月３１日　規程令和第４－２３号）
この規程は、令和４年４月１日から施行する。