○独立行政法人国際協力機構サイバーセキュリティ対策に関する規程

(平成29年4月3日規程(情)第14号)

改正 平成29年11月24日規程(情)第32号　令和元年7月12日規程(情)第4号
令和2年1月31日規程(情)第3号　令和2年3月31日規程(総)第7号
令和3年4月1日規程(総)第11号　令和4年3月31日規程(情)第2号
令和5年3月31日規程(情)第6号　令和6年3月13日規程(情)第7号

目次

第1章　目的及び適用対象

(目的)

第1条　この規程は、サイバーセキュリティ基本法(平成26年法律第104号。以下「法」という。)第26条第1項第2号に基づきサイバーセキュリティ戦略本部が作成する国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティ対策の基準である「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群」(令和5年7月4日決定。)に含まれる「政府機関等のサイバーセキュリティ対策のための統一規範」(以下「統一規範」という。)及び「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。)に準拠し、独立行政法人国際協力機構(以下「機構」という。)がとるべきサイバーセキュリティ対策を含む情報セキュリティの目的及び対象範囲等の基本的な考え方を定めることを目的とする。

(定義)

第2条　この規程における用語の定義は、別に定めるもののほか、次のとおりとする。

⑴　「対策基準」とは、機構における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準を指し、細則として定めるもの。

⑵　「機構情報セキュリティポリシー」(以下「機構ポリシー」という。)とは、この規程及び対策基準をいう。

⑶　「運用規程」とは、対策基準に定められた対策内容を個別の情報システムや業務において運用するため、あらかじめ定める必要のある具体的な規定及び基準を指し、準内部規程として定めるもの。

⑷　「実施手順」とは、対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順及び手続を指し、準内部規程として定めるもの。

⑸　「情報セキュリティ関係規程」とは、機構ポリシー、運用規程及び実施手順を総称したものをいう。

⑹　「情報セキュリティ対策推進体制」とは、機構の情報セキュリティ対策の推進に係る業務を遂行するため、機構に設置された体制をいう。

⑺　「情報システム」とは、ハードウェア及びソフトウェアからな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う。

⑻　「外部電磁的記録媒体」とは、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であって、情報システムによる情報処理の用に供されるものに係る記録媒体の内、USB メモリ、外付けハードディスクドライブ、DVD-R 等の可搬媒体をいう。

⑼　「業務継続計画」とは、機構において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。

(適用対象)

第３条　この規程の適用対象とする者は、次に掲げる者とする。

⑴　機構の役職員、非常勤勤務者及び名称の如何を問わず機構の指揮命令を受けて業務に従事する者並びに派遣労働者等であって、次項に規定する情報を取り扱う者（以下「役職員等」という。）。

⑵　前号に掲げる者以外で、機構と契約上の守秘義務を負い、かつ、次項に規定する情報を取り扱う者(以下「情報取扱事務従事者」という。)。

2　この規程の適用対象とする情報は、役職員等及び情報取扱事務従事者が職務上取り扱う情報であって、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情報システムに入力された書面に記載された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。

第２章　情報セキュリティ対策のための基本指針

(管理体制)

第４条　機構は、情報セキュリティ対策を実施するための組織・体制を整備するものとする。

2　機構は、最高情報セキュリティ責任者を１人置き、情報システム部（情報セキュリティ及び個人情報保護）担当理事をもって充てる。

3　最高情報セキュリティ責任者は、機構ポリシー及び機構の保有個人情報等の管理に係る審議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する。

4　最高情報セキュリティ責任者は、機構の情報セキュリティ対策の業務を統括するとともに、その責任を負う。

5　最高情報セキュリティ責任者は、第４項に定める所管事項を対策基準に定める責任者等に担わせることができる。

6　最高情報セキュリティ責任者は、自らを助けて機構における情報セキュリティ対策の業務を整理し、機構の情報セキュリティ業務を統括する最高情報セキュリティ副責任者１人を必要に応じ任命するものとする。

(資産管理)

第5条　機構は、機構の資産の状況を把握するため、所管する情報システムに係る文書及び台帳を整備するものとする。

（リスク評価と対策）

第6条　機構は、組織の目的等を踏まえ、第12条に定める自己点検及び第13条に定める情報セキュリティ監査の結果並びに法に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講ずるものとする。

（機構ポリシー）

第7条　機構は、機構ポリシーを統一規範及び統一基準に準拠し、これ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るものとする。

2　機構は、機構ポリシーを定める際に外務省より外務省ポリシーを参考とするよう求められた場合、外務省ポリシーを参考とし、必要に応じて、機構ポリシーに反映させるものとする。

（対策推進計画）

第8条　最高情報セキュリティ責任者は、第6条の評価の結果を踏まえた情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。

2　機構は、対策推進計画に基づき情報セキュリティ対策を実施するものとする。

（例外措置）

第9条　機構は、機構ポリシー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定める。

（教育）

第10条　機構は、役職員等及び情報取扱事務従事者が自覚をもって機構ポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行い、又は行わせるものとする。

（情報セキュリティインシデントへの対応）

第11条　機構は、情報セキュリティインシデント（JIS Q 27000：2019における情報セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施するものとする。

2　情報セキュリティインシデント及びその可能性を認知した者は、機構ポリシーに定める報告窓口に報告するものとする。

3　機構ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け、又は認知したときは、必要な措置を講じるものとする。

（自己点検）

第12条　機構は、情報セキュリティ対策の自己点検を行うものとする。

（情報セキュリティ監査）

第13条　機構は、機構ポリシーが統一規範及び統一基準に準拠し、かつ、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を確認するため、情報セキュリティ監査を行うものとする。

（対策の見直し）

第14条　機構は、第6条の評価に変化が生じた場合には、情報セキュリティ対策を見直すものとする。

2　機構は、第6条の評価の結果を踏まえ、機構ポリシーの評価及び見直しを行うものとする。

3　最高情報セキュリティ責任者は、情報セキュリティ対策の運用、自己点検、情報セキュリティ監査及び法に基づきサイバーセキュリティ戦略本部が実施する監査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、対策推進計画の見直しを行うものとする。

第3章　情報セキュリティ対策のための基本対策

（情報の格付）

第15条　機構は、取り扱う情報に、機密性、完全性及び可用性の観点に基づき区別し、分類した格付を付するものとする。

2　機構は、国の行政機関、独立行政法人及び法第13条に定義する指定法人（以下「他の機関等」と総称する。）への情報の提供、運搬及び送信に際しては、前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するものとする。

（情報の取扱制限）

第16条　機構は、情報の格付に応じた取扱制限を定めるものとする。

2　機構は、取り扱う情報に、前項で定めたその取扱制限を付するものとする。

3　機構は、他の機関等への情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等するものとする。

（情報のライフサイクル管理）

第17条　機構は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要な取扱いがなされるように、必要な措置を定め、実施するものとする。

（情報を取り扱う区域）

第18条　機構は、機構の事業所又は機構外の組織から借用している施設等、機構の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施するものとする。

（外部委託）

第19条　機構は、機構の情報を取り扱わせる業務を委託する場合には、必要な措置を定め、実施するものとする。

2　機構は、業務委託を実施する際に要機密情報を取り扱わせる場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様にも含めるものとする。

3　機構は、クラウドサービスを利用する場合には、情報セキュリティを確保するための措置を定め、実施するものとする。
4　機構は、機器等の調達に当たり、機器等の開発等で不正な変更が加えられない管理がなされている等のサプライチェーン・リスクへの適切な対処を含む選定基準を定めるものとする。

(情報システムのライフサイクル全般にわたる情報セキュリティの確保)

第20条　機構は、所管する情報システムの企画、調達・構築、運用・保守、更改・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、実施するものとする。

(情報システムの運用継続計画)

第21条　機構は、所管する情報システムに係る運用継続のための計画を整備する際には、業務継続計画及び機構ポリシーとの整合性を確保し、整備及び運用するものとする

(情報システムの利用)

第22条　機構は、情報システムの利用に際して、情報セキュリティを確保するために役職員等及び情報取扱事務従事者が行わなければならない必要な措置を定め、実施させるものとする。

(対策基準への委任)

第23条　本規程に定めるもののほか、本規程の実施のために必要な事項は、対策基準で定める。

附　則

この規程は、平成29年4月3日から施行し、平成29年4月1から適用する。

附　則(平成29年11月24日規程(情)第32号)

この規程は、平成29年11月24日から施行する。

附　則(令和元年7月12日規程(情)第4号)

この規程は、令和元年7月12日から施行する。

附　則(令和2年1月31日規程(情)第3号)

この規程は、令和2年1月31日から施行する。

附　則(令和2年3月31日規程(総)第7号)

この規程は、令和2年4月1日から施行する。

附　則(令和3年4月1日規程(総)第11号)

この規程は、令和3年4月1日から施行する。

附　則(令和4年3月31日規程(情)第2号)

この規程は、令和4年4月1日から施行する。

附　則(令和5年3月31日規程(情)第6号)

この規程は、令和5年4月1日から施行する。

附　則(令和6年3月13日規程(情)第7号)

この細則は、令和6年4月1日から施行する。