国立研究開発法人物質・材料研究機構
情報セキュリティ規程

令和７年３月１８日
２０２５規程第６９号

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（法第２５条により内閣に設置される組織をいう。以下同じ。）が策定した「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群」に基づき、国立研究開発法人物質・材料研究機構（以下「機構」という。）における情報セキュリティの確保に関する基本的な事項を定めることにより、機構全体のサイバーセキュリティ対策を含む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。

（適用対象）

第２条　この規程を実施するために必要な事項は、別に定める対策基準等の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　この規程の適用対象とする者は、機構の役員、国立研究開発法人物質・材料研究機構定年制職員就業規則（平成１８年３月３１日　１８規程第４６号）、国立研究開発法人物質・材料研究機構キャリア形成職員就業規則（平成２０年３月３１日　２０規程第１６号）及び国立研究開発法人物質・材料研究機構任期制職員就業規則(平成１８年３月２８日　１８規程第４７号)の適用を受ける者、国立研究開発法人物質・材料研究機構客員研究者等取扱規程（平成１８年４月１９日　１８規程第３３号）の適用を受ける者並びに派遣職員、その他機構の指揮命令に服している就労者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。

３　この規程の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）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。）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。

４　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情報セキュリティ に係る要求があり、理事長がこれを認めたときは、この規程によらず、当該要求に基づき情報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）「文書」とは、職員等が職務上作成し又は取得した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。）をいう。

（２）「各部門等」とは、国立研究開発法人物質・材料研究機構組織規程（令和５年２月２８日　２０２３規程第７号。以下「組織規程」という。）第３

条に定める機構の組織をいう。
（３）「情報資産」とは、、前条第３項に規定された情報をいう。
（４）「情報セキュリティ」とは、情報資産が備えるべき次に掲げる性質を健全に保つことをいう。
イ　機密性　情報資産にアクセスすることが認可された者だけがアクセスできることをいう。
ロ　完全性　情報資産の正確さ及び完全さが保護されていることをいう。
ハ　可用性　許可された職員等が、必要な時に情報資産にアクセスすることを保証されていることをいう。
（５）「脅威」とは、自然災害、機器障害、意図的な不正行為等、損失を発生させる直接の要因をいう。
（６）「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、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。
（７）「統一基準」とは、法第１３条に基づきサイバーセキュリティ戦略本部が定める政府機関等の情報セキュリティ対策のための統一基準をいう。
（８）「区域」とは、執務室、サーバー室等の情報資産を取り扱う区画された室等をいう。
（９）「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であり、国立研究開発法人物質・材料研究機構情報セキュリティ対策基準（令和７年３月１８日２０２５情報基盤達第１号）をいう。

第２章　情報セキュリティ対策のための基本方針

（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・体制を構築する。

（最高情報責任者）
第５条　機構に情報セキュリティに関する全業務を統括する最高情報責任者を置く。
２　最高情報責任者は、理事長をもって充てる。
３　最高情報責任者は、機構横断的に対応を必要とする事項への対策を講ずる。

（最高情報セキュリティ責任者）
第６条　機構に、最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）を置く。
２　ＣＩＳＯは、この規程に定める機構の情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。
３　ＣＩＳＯは、別に定める対策基準に定められた自らの担務を、対策基準に定める責任者に担わせることができる。
４　ＣＩＳＯは、情報基盤統括部門担当理事をもって充てる。

（最高情報セキュリティ副責任者）
第７条　ＣＩＳＯは、ＣＩＳＯを助けて機構における情報セキュリティに関する事務を整理し、ＣＩＳＯの命を受けて機構の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副責任者（以下「副ＣＩＳＯ」という。）を必要に応じて置くことができる。

（情報セキュリティ委員会）
第８条　ＣＩＳＯは、別に定める対策基準等の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し、委員長及び委員を置く。

（情報セキュリティ監査責任者）
第９条　ＣＩＳＯは、その指示に基づき実施す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１人を置く。
２　情報セキュリティ監査責任者は、ＣＩＳＯが指名する者をもって充てる。

（統括情報セキュリティ責任者・情報セキュリティ責任者）
第１０条　ＣＩＳＯは、各部門等に、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置く。
２　情報セキュリティ責任者は、各部門等の長をもって充てる。
３　ＣＩＳＯは、第１項の情報セキュリティ責任者のうち、情報セキュリティ責任者を統括し、ＣＩＳＯ及び副ＣＩＳＯを補佐する者として、統括情報セキュリティ責任者１人を選任する。

（区域情報セキュリティ責任者）
第１１条　情報セキュリティ責任者は、要管理対策区域ごとに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１人を置く。

（情報セキュリティ管理者）
第１２条　情報セキュリティ責任者は、各部門等の情報セキュリティ責任者を補佐するため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、国立研究開発法人物質・材料研究機構定年制職員給与規程（平成１３年４月２日　１３規程第９号）別表第４又は別表第６の各区分に該当する定年制職員若しくは当該区分に相当する任期制職員若しくは無期労働契約転換職員であって、各組織に属する職員の服務一般を管理監督する者又は情報セキュリティ責任者が指名した者とし、情報セキュリティ責任者の命を受け、組織規程第３条第２項に定めた組織及び第４条から第１８条までに定めた組織の情報セキュリティ（情報システムセキュリティを除く。）に関する業務を総括整理する。
３　情報セキュリティ管理者は、その担当する範囲を指定し、複数名置くことができる。

（情報システムセキュリティ責任者）
第１３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事務の責任者として、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こと。

（最高情報セキュリティアドバイザー）
第１４条　機構に、最高情報セキュリティアドバイザー（以下、「ＣＩＳＯ補佐官」という。）を置く。
２　ＣＩＳＯ補佐官は、ＣＩＳＯの指名する者又はＣＩＳＯが委嘱する外部有識者をもって充てる。
３　ＣＩＳＯ補佐官は、その担当する範囲を指定し、複数名置くことができる。
４　ＣＩＳＯ補佐官を外部有識者に委嘱する場合、手当及び旅費を支給することができる。手当は、国立研究開発法人物質・材料研究機構アドバイザー等の取扱

いについて（平成１８年４月１９日　１８達第１６号）第６条第２号を、旅費は、第７条を準用する。

（兼務を禁止する役割等）

第１５条　職員等は、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ないこととする。

（１）この規程の規定による承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う許可権限者

（２）この規程の規定による監査を受ける者とその監査を実施する者

２　職員等は、承認等を申請する場合において、自らが許可権限者であるときその他許可権限者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、当該許可権限者の上司又は適切な者に承認等を申請し、承認等を得ることとする。

（資産管理）

第１６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１７条　機構は、機構の目的等を踏まえ、第２３条に定める自己点検の結果、第２４条に定める情報セキュリティ監査の結果、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、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じるものとする。

（情報セキュリティ文書）

第１８条　機構は、自組織の特性を踏まえ、この規定に基づき、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となる対策基準を定めなければならない。

２　対策基準は、統一基準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。

（対策推進計画）

第１９条　ＣＩＳＯは、第１７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。）を定めなければならない。

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しなければならない。

（例外措置）

第２０条　機構は、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について、別に定めるものとする。

（教育）

第２１条　機構は、職員等が自覚をもって対策基準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うものとする。

（情報セキュリティインシデントへの対応）
第２２条　ＣＩＳＯは、情報セキュリティインシデントに対処するため、適切な体制としてＣＳＩＲＴ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　ＣＩＳＯは、職員等のうちから ＣＳＩＲＴに属する職員等として専門的な知識又は適性を有すると認められる者を選任する。そのうち、機構における情報セキュリティインシデントに対処するための責任者として ＣＳＩＲＴ責任者を置く。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員等を定める。
３　情報セキュリティインシデントの可能性を認知した者は、対策基準において定める報告窓口に報告しなければならない。
４　ＣＳＩＲＴ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、必要な措置を講じなければならない。

（自己点検）
第２３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２４条　機構は、対策基準がこの規程及び統一基準に準拠し、かつ実際の運用が対策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うものとする。

（対策の見直し）
第２５条　機構は、第１７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１７条の評価結果を踏まえ、対策基準の評価及び見直しを行うものとする。
３　ＣＩＳＯは、情報セキュリティ対策の運用、第２３条に定める自己点検、前条に定める情報セキュリティ監査、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２６条　機構は、機構で取り扱う情報に、機密性、完全性及び可用性の観点に区別して、別に定める分類に基づく格付を付さなければならない。
２　機構は、機構と機構外の組織等間での情報の提供、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しなければならない。

（情報の取扱制限）
第２７条　機構は、情報の格付に応じた取扱制限を定めなければならない。
２　職員等は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。
３　職員等は、機構と機構外の組織等間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。
４　前各項の取扱制限及び措置については、別に定める。

（情報のライフサイクル管理）

第２８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とされる取扱いが損なわれることがないように、必要な措置を定め、実施するものとする。
２　前項の取扱いについては、別に定める。

（情報を取り扱う区域）
第２９条　機構は、機構が管理する又は機構外の組織等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（以下「要管理対策区域」という。）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。
２　要管理対策区域の設定及び当該区域における対策基準については、別に定める。

（外部委託）
第３０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　情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託を実施する際に対策基準に規定されている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、仕様内容にも含めなければならない。
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３１条　機構は、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３２条　機構は、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、非常時における情報セキュリティ対策についても、勘案するものとする。
２　機構は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認するものとする。

（暗号・電子署名）
第３３条　機構は、自組織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、実施させるものとする。

（情報システムの利用）
第３４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職員等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。

（雑則）

第３５条　この規程に定めるもののほか、情報システム及び情報システム上で扱う情報の取扱いについて必要な事項は、理事長が別に定める。

附　則

１．この規程は、令和７年４月１日から施行する。

２．国立研究開発法人物質・材料研究機構情報セキュリティポリシー（平成２４年６月５日）は、廃止する。

３．国立研究開発法人物質・材料研究機構情報セキュリティ規程（平成２４年６月５日　２４規程第３４号）は、廃止する。