国立研究開発法人　理化学研究所

情報セキュリティ対策基準

第 4.1 版　　2023 年 5 月

情報セキュリティ委員会

目次

第１章　目的 1
第２章　定義 1
第３章　情報の格付けと取扱制限 2
３．１．　情報の範囲 2
３．２．　情報の目的外での利用の禁止 2
３．３．　情報の格付けと取扱制限の付与 2
第４章　管理区域の指定 4
４．１．　管理区域クラスの指定及び対策 4
４．２．　管理区域における対策の実施 4
第５章　情報の取扱い 4
５．１．　格付けと取扱制限の明示 4
５．２．　格付けと取扱制限の再付与 5
５．３．　格付けと取扱制限の変更 5
５．４．　情報の取扱い 5
５．５．　情報の保管 5
５．６．　情報の提供、又は公表 5
５．７．　管理区域外での利用等 5
５．８．　情報の消去 5
５．９．　情報のバックアップ 5
第６章　情報セキュリティ対策 6
６．１．　情報セキュリティ対策の運用 6
６．２．　例外措置 6
６．３．　情報セキュリティインシデントへの対応 6
第７章　情報セキュリティ教育 6
７．１．　教育体制の整備 6
７．２．　教育の実施 7
第８章　自己点検 7
８．１．　自己点検計画の策定及び実施 7
８．２．　自己点検の実施 7
８．３．　自己点検への対応 7
第９章　情報セキュリティ監査 7
９.１．　監査実施計画 7
９．２．　監査の実施 8
９．３．　監査結果への対応 8
第１０章　業務委託 8
１０．１．　業務委託 8
１０．２．　外部サービスの利用 9

１０．３．　クラウドサービス利用における対策 9
第１１章　情報システムのライフサイクル 9
１１．１．　情報システム台帳の整備 9
１１．２．　情報システムライフサイクルにおける対策の整備 10
１１．３．　情報システムの調達及び構築 10
１１．４．　情報システムの運用 10
１１．５．　情報システムの更改・廃棄 10
１１．６．　情報セキュリティ対策の見直し 10
１１．７．　情報システムの運用継続計画 10
第１２章　情報システムのセキュリティ要件 11
１２．１．　主体認証機能 11
１２．２．　情報セキュリティの脅威への対策 11
１２．３．　暗号・電子署名利用時の対策 11
第１３章　情報システムの構成要素 11
１３．１．　端末・サーバ装置等 11
１３．２．　電子メール・ウェブ等 12
１３．３．　通信回線 12
第１４章　情報システムの利用 12
１４．１．　情報システムの利用に係る手順 12
１４．２．　情報システム利用の基本事項 12
１４．３．　IP アドレス・ドメイン名の例外割り当てについて 13
１４．４．　電磁的記録媒体の利用 13
１４．５．　所外情報システムの利用手続き 13
１４．６．　ソーシャルメディアサービスによる情報発信 14
１４．７．　テレワーク 14

改訂履歴

日付	版	改訂内容
2019/4/1	1.0	初版
2020/3/26	2.0	第３章　情報の格付けと取扱制限　機密性の格付け、 第9章 情報セキュリティ監査　監査結果への対応など
2021/4/1	3.0	第4章 管理区域における「区域情報セキュリティ責任者」を追記 第１０章 約款による外部サービス、ソーシャルメディアサービス、 クラウドサービスの利用手続きについて明記 第１２章 認証データ管理を追記 など
2022/4/1	4.0	令和3年度版政府統一基準への対応 第1章 情報の格付けと取扱制限 第12章 情報システムのセキュリティ要件 第13章 情報システムの構成要素 を変更 １４．７ テレワークを追加
2023/5/19	4.1	令和4年9月29日規程第535号 「情報化/デジタル統括責任者及び情報化/デジタル統合戦略会議設置規程」改正のため

第１章　目的

国立研究開発法人理化学研究所（以下「研究所」という。）は、研究所おける情報セキュリティ対策を実施するために、「政府機関の情報セキュリティ対策のための統一規範平成 28 年 8 月 31 日サイバーセキュリティ戦略本部決定)」に基づき、研究所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た「情報セキュリティ対策規程」を平成 30 年 10 月 1 日に施行した。

この情報セキュリティ対策基準は、「情報セキュリティ対策規程」を実施するために必要な事項及び手続きについて「政府機関の情報セキュリティ対策のための統一基準（平成 30 年 7 月 25 日施行)」を元に、情報セキュリティ委員会（以下「委員会」という。）により定められ、「政府機関等のサイバーキュリティ対策のための統一基準（令和３年度版）（令和 3 年 7 月 7 日施行)」に沿って改定されたものである。

第２章　定義

この対策基準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)　「部門」とは、別に定める情報セキュリティ対策に係る管理の組織単位をいう。

(2)　「部署」とは、情報セキュリティ対策に係り、部門が定める管理組織の最小単位をいう。

(3)　「役職員」とは、役員及び職員（研究所との間で雇用契約を締結し研究所の業務に従事する者）をいう。

(4)　「外部人材」とは、役職員以外の者をいう。

(5)　「利用者」とは、次号で定める情報、第 10 号で定める情報システム及び第 13 号で定める研究所ネットワークを利用する役職員及び外部人材をいう。

(6)　「情報」とは、研究所の業務において作成し、収集し又は取得した情報をいう。

(7)　「情報サービス」とは、情報の加工、蓄積、授受等を行い、利用者に提供することをいう。

(8)　「情報システム」とは、情報サービスの提供を行うシステム、ハードウェア及びソフトウェアで、研究所の業務に供するものをいう。

(9)　「所外情報システム」とは、研究所の資産でない PC、サーバ、スマートフォン、タブレット端末、USB メモリ等の情報システムをいう。

(10)　「ネットワーク」とは、複数のシステムを接続し、協調動作させるための配線、ルータ及びスイッチ等のハードウェア並びにアドレス、プロトコル及びプログラム等のソフトウェアをいう。

(11)　「研究所ネットワーク」とは、研究所が情報システムを接続し、制御し、及び運用する業務に供するネットワークをいう。

(12)　「情報セキュリティ」とは、情報、情報システム及び研究所ネットワーク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（アクセスを許可された者だけがこれにアクセスできる状態が確保されていることをいう。）

　ロ）　完全性（情報及びその処理方法の正確さ並びに完全さが確保されていることをいう。）

　ハ）　可用性（必要時に中断することなくアクセスできる状態が確保されていることをいう。）

(13)　「情報セキュリティインシデント」とは、情報の流失、漏えい、改ざん、破壊、障害等により情報、情報システム及び研究所ネットワークの情報セキュリティが損なわれることをいう。

(14) 「外部サービス」とは、所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、当該機能において研究所の情報が取り扱われる場合に限る。

(15) 「業務委託」とは、研究所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、全て含むものとする。ただし、当該業務において研究所の情報を取り扱わせる場合に限る。

第３章　情報の格付けと取扱制限

３．１．　情報の範囲

本対策基準における「情報」の範囲は、情報のうち国立研究開発法人理化学研究所文書管理規程（平成 15 年規程第 29 号）（以下「文書管理規程」という。）第 2 条第 1 項で定義される「法人文書」に相当するものとする。ただし、同規程第 3 条で対象外とする、研究データ、実験ノート等も含むものとする。

３．２．　情報の目的外での利用の禁止

全ての利用者（以下特に主語の記載がない場合は「全ての利用者」とする。）は、自らが担当している業務の遂行のために必要な範囲に限って、情報を作成、入手、利用、保存、提供、運搬、送信、消去、複写、加工等（以下「利用等」という。）すること。

３．３．　情報の格付けと取扱制限の付与

情報の利用等に際しては、当該情報の機密性、完全性及び可用性についてそれぞれ格付けと取扱制限を定め、情報セキュリティ責任者の許可を受け、付すこと。

イ）機密性（アクセスを許可された者だけがこれにアクセスできる状態が確保されていること）

	格付け区分（政府統一基準）	格付け区分(理研)	情報の分類基準
要機密情報	機密性 3 情報	極秘情報	研究所で取り扱う情報のうち、３．１で定めた情報の範囲において、文書管理規程 第 26 条に規定する秘密文書区分「極秘」としての取扱いを要する情報
		秘情報	研究所で取り扱う情報のうち、３．１で定めた情報の範囲において、文書管理規程 第 26 条に規定する秘密文書区分「秘」としての取扱いを要する情報
	機密性 2 情報	部署内	独法等情報公開法第 5 条の不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、機密性３情報以外の情報のうち、直ちに一般に公表することを前提としていない部署内で知ることができる情報
		所内	独法等情報公開法第 5 条の不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、機密性３情報以外の情報のうち、直ちに一般に公表することを前提としていない研究所内で知ることができる情報

機密性 1 情報	公表予定なし	独法等情報公開法第 5 条の不開示情報に該当すると判断される蓋然性の高い情報を含まない情報のうち、公表予定のない情報。
	公開	公開予定の情報または公開済みの情報

（例）機密性についての取扱制限

取扱制限の種類	指定方法
再配付について	再配付禁止、再配付要許可
保存場所について	指定箇所限り、管理区域限り、所内限り
開示について	非開示、制限無し
取扱者の制限について	○○限り、○○委員限り、指定者限り、要 NDA
取扱場所の制限について	所内限り、部内限り、○○室内限り
期限の設定について	○月○日まで○○禁止、○○の期間内は○○禁止
複合条件について	取扱制限が多岐に渡る場合、当該情報に対し別に情報の格付けと取扱制限を定め指定すること
その他	特に厳重な取扱いが必要な情報については、必要に応じて記載すること

ロ）完全性（情報及びその処理方法の正確さ並びに完全さが確保されていること）

格付けの区分	分類の基準
要完全性情報	研究所で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、研究所の業務の遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
無指定	要完全性情報以外の情報（書面を除く。）

（例）完全性についての取扱制限

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後、復元不可能な方法により消去

ハ）可用性（必要時に中断することなくアクセスできる状態が確保されていること）

格付けの区分	分類の基準
要可用性情報	研究所で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、研究所の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
無指定	要可用性情報以外の情報（書面を除く。）

（例）可用性についての取扱制限

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
バックアップについて	バックアップ要、バックアップ不要

保存場所について	○○において保存

第４章　管理区域の指定

４．１．　管理区域クラスの指定及び対策

部門情報セキュリティ責任者及び区域情報セキュリティ責任者は、所管区域に対し、当該区域の安全性を確保し、当該区域で取り扱う情報や情報システム等のセキュリティを確保するため、必要とする管理区域クラスの指定や管理区域にアクセスできない者（以下「部外者」という。）の定義、及び対策を定めること。

イ）　管理区域クラスの指定及び対策（例）

クラス	説明	例	対策
クラス３	当該情報システム及び関連する機器の管理者、保守作業者等以外の立ち入りを制限する、厳重な対策を実施する必要がある区域。	要機密情報を取り扱う情報システムが設置されるサーバ室、セキュリティ機器・コアスイッチ・WANルータ等の重要なネットワーク機器が設置されるサーバ室。	IDカード、生体認証、施錠等により、許可された者のみ立ち入れるよう処置する。ネットワークラック等についても同様。
クラス２	研究所の職員及び関係者以外の立ち入りを制限する等、情報セキュリティを確保するための対策を実施する必要がある区域。	執務室、金庫、鍵付きロッカー等、要機密情報を取り扱い、保管等する可能性のある施設。	扉等により、部外者の容易な立ち入りを制限する。また、職員等の不在時は施錠を行う。
クラス１	クラス２，３以外の要管理対策区域。(建物内など部外者の立ち入りを制限する区域)	建物内のロビー、応接室、打合せ室等、職員及び許可を受けた部外者が立ち入ることのできる区域。	建物入口でのカード認証等により、部外者の立ち入りを制限する。
クラス０	所定の手続きを済ませた部外者が容易に立ち入ることのできる区域。	研究所構内、ホール、食堂等、守衛所で所定の手続きにより部外者が立ち入ることのできる区域。	守衛所で所定の手続きを済ませた者のみ入構させる。

４．２．　管理区域における対策の実施

イ）区域情報セキュリティ責任者は、管理区域のクラス指定、及び必要とする対策を利用者に周知し、実施させるとともに監督すること。

ロ）区域情報セキュリティ責任者は、管理区域における情報システムの災害対策について定め、実施すること。

ハ）全ての利用者は管理区域における対策を遵守すること。

第５章　情報の取扱い

５．１．　格付けと取扱制限の明示

取扱制限が付される情報に、当該情報の参照者が認識できる方法を用いて格付と取扱制限を明示すること。

５．２．　格付けと取扱制限の再付与

既に格付けと取扱制限が付された情報を利用等（特に加工）する場合、当該情報に格付けと取扱制限を付した当該部署の情報セキュリティ責任者の許可を受け、当該情報の機密性、完全性、可用性を踏まえて適切な格付けと取扱制限を定めること。

５．３．　格付けと取扱制限の変更

情報の格付けと取扱制限を変更する場合、当該情報に格付けと取扱制限を付した当該部署の情報セキュリティ責任者の許可を得ること。

５．４．　情報の取扱い

情報に付された取扱制限に応じて、当該情報を取り扱うこと。

５．５．　情報の保管

イ）情報の取扱制限に基づき適切なアクセス権限を付し、当該情報を保管すること。

ロ）情報の取扱制限に基づきバックアップ、冗長化、及び保存場所の耐震対策等の要件を定め必要な措置を講じること。

ハ）情報の取扱制限に基づき情報が処理される情報システムを管理区域に設置すること。

５．６．　情報の提供、又は公表

イ）取扱制限に基づいて、情報を提供、又は公表すること。

ロ）提供先においても当該情報の取扱制限を遵守させ、監督すること。

ハ）当該情報のプロパティ、校正履歴等は公表や提供に際して不要な付帯情報を、情報の取扱制限に基づき削除すること。

５．７．　管理区域外での利用等

モバイル端末や電磁的記録媒体等による情報の持ち出し、及び電子メールやファイル転送等により管理区域外で情報を扱う場合、特に情報セキュリティ責任者の許可を受け、情報の取扱制限に基づき暗号化及びパスワードロック等の情報セキュリティ対策を講じること。

５．８．　情報の消去

イ）管理区域内外で使用される情報について、その使用が終了した場合、情報の取扱制限に基づき速やかに消去すること。

ロ）要機密情報の記録された電磁的記録媒体を廃棄する場合、当該電磁的記録媒体内の全ての情報について、復元を困難にするための措置を講じること。

５．９．　情報のバックアップ

イ）情報の取扱制限に基づき情報をバックアップすること。

ロ）前項により作成したバックアップについて、取扱制限に基づき保存場所、保存方法、保存期間等

を定め管理すること。

ハ）保存期間を過ぎたバックアップについては、復元を困難にするための措置を講じ、消去、又は廃棄すること。

第６章　情報セキュリティ対策

６．１．　情報セキュリティ対策の運用

イ）統括情報セキュリティ担当部署は、研究所における情報セキュリティ対策に係る事務を統括する。

ロ）情報セキュリティ責任者は、利用者から情報セキュリティ対策基準、実施手順に係る課題、及び問題点の報告を受けた場合、統括情報セキュリティ担当部署に報告すること。

ハ）統括情報セキュリティ担当部署は、前項で受けた報告を評価し、対応の必要がある場合、最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）に報告し、必要に応じて情報セキュリティ委員会に諮ること。

ニ）CISO は、必要に応じて統括情報セキュリティ担当部署に対応を指示すること。

６．２．　例外措置

イ）情報セキュリティ対策規程、この対策基準、及び情報セキュリティ対策推進計画等の運用において、研究所の業務に不都合をきたす場合、統括情報セキュリティ担当部署に相談し、必要に応じて例外措置を申請することができる。CISO は、例外措置の申請の可否を判断する者及び審査手続きを定める。

ロ）統括情報セキュリティ担当部署は、例外措置の適用記録を整備し、例外措置の申請者に対して定期的に状況の報告を求める。

６．３．　情報セキュリティインシデントへの対応

イ）情報セキュリティインシデントを発見、又は発生の報を受けた場合、別に定める手順により通報し、初期対応にあたること。

ロ）情報セキュリティインシデント対策チーム（Computer Security Incident Response Team。以下「CSIRT」という。）は、情報セキュリティインシデントの発生の報を受けた場合、別に定める手順により連絡先に通報し、情報セキュリティインシデント対応作業にあたること。

ハ）CISO は、統括情報セキュリティ担当部署に、情報セキュリティインシデントの再発防止策の検討と実施を指示すること。

ニ）統括情報セキュリティ担当部署は、情報セキュリティインシデントの発生状況、対応策、再発防止策等についてとりまとめ、研究所内に周知すること。

第７章　情報セキュリティ教育

７．１．　教育体制の整備

イ）統括情報セキュリティ担当部署は、情報セキュリティに係る教育（以下「情報セキュリティ教育」という。）について教育実施計画を策定し、実施体制を整備すること。

ロ）統括情報セキュリティ担当部署は、情報セキュリティに係る状況を鑑み、適宜教育実施計画を見直すこと。

７．２．　教育の実施

イ）全ての利用者は、情報システムや研究所ネットワークを実際に利用することとなった場合、速やかに情報セキュリティ教育を受けなければならない。教育を受けていない状態が続く場合には、CISO は、部門情報セキュリティ責任者等に対して改善を求めるほか、当該利用者及び部署の研究所ネットワークや情報サービスの利用停止を含め必要な措置を講ずるものとする。

ロ）CISO は、CSIRT に属する職員に CSIRT 要員育成に必要な教育を受けさせること。

ハ）統括情報セキュリティ担当部署は、情報セキュリティ教育の実施状況を CISO に報告すること。

第８章　自己点検

８．１．　自己点検計画の策定及び実施

イ）統括情報セキュリティ担当部署は、対策推進計画に基づき、必要に応じて情報セキュリティ対策の実施状況に係る自己点検（以下「自己点検」という。）計画を策定し、実施すること。

ロ）統括情報セキュリティ担当部署は、情報セキュリティに係る状況を鑑み、自己点検計画を見直すこと。

８．２．　自己点検の実施

イ）統括情報セキュリティ担当部署は、研究所の部門、及び部署に対し自己点検計画に基づき、自己点検の実施を指示すること。

ロ）統括情報セキュリティ担当部署より自己点検の指示を受けた場合、速やかに実施し回答すること。

８．３．　自己点検への対応

イ）統括情報セキュリティ担当部署は、自己点検の回答をとりまとめ、分析及び評価すること。

ロ）統括情報セキュリティ担当部署は、自己点検の評価において重大な問題点が発見された場合、速やかに部門情報セキュリティ責任者、又は情報セキュリティ責任者に改善を指示するとともに CISO に報告すること。

ハ）統括情報セキュリティ担当部署は、自己点検の分析、及び評価結果を CISO に報告すること。

ニ）CISO は、自己点検結果を評価し、問題点が発見された場合、統括情報セキュリティ担当部署、及び部門情報セキュリティ責任者に改善を指示すること。

ホ）統括情報セキュリティ担当部署、及び部門情報セキュリティ責任者は、CISO より受けた改善指示の対応状況について適宜 CISO に報告すること。

ヘ）CISO は、自己点検の評価結果を鑑み対策推進計画を見直すこと。

第９章　情報セキュリティ監査

９．１．　監査実施計画

情報セキュリティ監査責任者は、情報セキュリティに係る状況、及び対策推進計画に基づき監査実施計画を定めること。

９．２．　監査の実施

イ）情報セキュリティ監査責任者は、監査実施計画に基づき研究所の情報セキュリティ対策に係る監査を実施し、CISO に報告すること。

ロ）情報セキュリティ監査責任者は、監査を実施するために情報セキュリティ監査班を設置することができる。

９．３．　監査結果への対応

イ）CISO は、監査の結果、改善が必要な事項が発見された場合、対策推進計画の見直しを行うとともに、必要に応じて統括情報セキュリティ担当部署、及び部門情報セキュリティ責任者に対し改善を指示すること。

ロ）統括情報セキュリティ担当部署、及び部門情報セキュリティ責任者は、指示を受けた事項について改善計画を策定、措置し、CISO に報告すること。

第１０章 業務委託

１０．１．業務委託

イ）統括情報セキュリティ担当部署は、情報システムの構築、運用、保守等又はアプリケーションソフトウェア等の開発、保守等を業務委託する際の情報セキュリティ対策における要件を、必要に応じて検討し、手順を整備すること。

ロ）情報、及び情報システムに係る業務の一部、又は全部を業務委託する場合、情報セキュリティ責任者の許可を受け、前項の手順に従い情報セキュリティ対策の要件を定め仕様書に記載すること。

ハ）委託業務において、委託先に対し情報セキュリティ対策要件の遵守を求め、また履行状況を確認すること。

ニ）委託業務において、要機密情報を扱わせる場合、情報セキュリティ責任者の許可を得、情報の取扱制限を遵守するとともに、必要とされる手続及び情報セキュリティ対策を委託先に講じさせること。

ホ）委託業務において、情報セキュリティインシデントが発生した場合を想定し、必要に応じて業務委託先との連絡体制、及び対応について定めること。

ヘ）委託業務において、委託先が他の委託先に再委託する場合、再委託先にも委託先と同等の情報セキュリティ対策の要件を定め、遵守させ、履行状況を確認すること。

ト）委託業務の終了に伴い、委託先において取扱われた研究所の情報を返却又は抹消させ、これを確認すること。ただし別の定めがある場合を除く。

チ）委託業務において情報セキュリティインシデントの発見又は報告を受けた場合、第６章３「情報セキュリティインシデントへの対応」に従うこと。

１０．２．外部サービスの利用

イ）統括情報セキュリティ担当部署は、外部サービスの利用に関する規定（外部サービス利用判断基準及び外部サービス提供行者の選定基準、利用手続、利用状況の管理）を整備すること。

ロ）情報セキュリティ責任者は、利用する外部サービス契約毎に管理者を定め、監督させること。

ハ）情報セキュリティ責任者は、要機密情報を取り扱う場合、取り扱う情報の格付け及び取扱制限、情報セキュリティに関する役割及び責任の範囲を踏まえ、外部サービスの利用を検討し、統括情報セキュリティ担当部署に相談した上で、イ）の規定に従って外部サービスを選定し、情報セキュリティ対策を適切に講じること。

ニ）情報セキュリティ責任者は、 外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様及び契約に含めること。

ホ）情報セキュリティ責任者は、要機密情報を取り扱わない場合であっても、サービスの提供条件等から利用に当たってのリスクが許容できることを確認した上で外部サービスを選定し、情報セキュリティ対策を適切に講じること。

ヘ）情報セキュリティ責任者は、別に定める手続きにより利用内容や点検事項を確認し、外部サービスの利用について、利用者に許可を与える前に統括情報セキュリティ担当部署に相談し、利用者に許可を与えた後には統括情報セキュリティ担当部署に利用登録をすること。

１０．３．クラウドサービス利用における対策

イ）統括情報セキュリティ担当部署は、クラウドサービス（事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの）を用いて研究所の情報を扱う際の要件及び情報セキュリティ対策に係る手順を必要に応じて定めること。

ロ）情報セキュリティ責任者は、所管部署おいて利用されるクラウドサービス毎に管理者を定め、監督させること。

ハ）情報セキュリティ責任者は、研究所の情報をクラウドサービスにおいて扱う必要がある場合、別に定める手続きにより利用内容や点検事項を確認し、クラウドサービスの利用について、利用者に許可を与える前に統括情報セキュリティ担当部署に相談し、利用者に許可を与えた後には統括情報セキュリティ担当部署に利用登録をすること。

ニ）クラウドサービスを用いて研究所の情報を利用する場合、イ）に定める手順及び当該情報の取扱制限を遵守すること。

第１１章 情報システムのライフサイクル

１１．１．情報システム台帳の整備

イ）統括情報セキュリティ担当部署は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について情報システム台帳を登録、運用するための手順を整備すること。

ロ）情報システム管理者は、情報システム台帳を、前項の手順に応じて利用または修正し、整備すること。
ハ）情報システム管理者は、情報サービスを運用する情報システムを更改等する際には、情報システム台帳に必要事項を記載すること。
ニ）情報セキュリティ責任者は、情報システム台帳を管理し所管する情報システムの運用状況を監督すること。
ホ）統括情報セキュリティ担当部署は、情報システム台帳の共有を求めることができる。

１１．２．情報システムライフサイクルにおける対策の整備

情報化/デジタル統括責任者（Chief Information Digital Officer。以下「CIDO」という。）、及びCISOは、調達、構築及び運用に係る情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制を整備すること。

１１．３．情報システムの調達及び構築

イ）統括情報セキュリティ担当部署は、必要に応じて研究所における情報システムの調達、及び構築に係る手順を定め、機器等の選定基準を整備すること。
ロ）情報セキュリティ責任者及び情報システム管理者は、情報システムを調達及び構築する際に、前項の手順を遵守すること。

１１．４．情報システムの運用

イ）情報システム管理者は、情報システムの情報セキュリティ機能を維持し、適切に運用しなければならない。
ロ）情報システム管理者は、所管する情報システムのログ等、運用に係る作業記録を保管し管理すること。
ハ）情報システム管理者は、CSIRTの求めにより当該情報システムの設定情報、ログ、運用に係る作業記録を開示すること。

１１．５．情報システムの更改・廃棄

イ）情報システム管理者は、情報システムの更改を行う場合、当該情報システムが扱う情報の格付けと取扱制限に基づき、必要な情報セキュリティ対策を講じること。
ロ）情報システム管理者は、情報システムの廃棄に伴い、当該情報システムが扱う情報の格付けと取扱制限に基づき、不要な情報を抹消し確認すること。

１１．６．情報セキュリティ対策の見直し

情報システム管理者は、情報セキュリティに関する状況、運用及び監視等により得られた知見等に基づき、所管する情報システムにおける情報セキュリティ対策を常時点検し、見直すこと。

１１．７．情報システムの運用継続計画

イ）統括情報セキュリティ担当部署、部門情報セキュリティ責任者、及び情報セキュリティ責任者は、研究所において非常時優先業務を支える情報システムの運用継続性について検討し、必要がある場合、対策を講じること。
ロ）統括情報セキュリティ担当部署、部門情報セキュリティ責任者、及び情報セキュリティ責任者は、前項に定める非常時における優先業務を支える主要な情報システムについて情報セキュリティに係る対策事項の定期的な訓練及び点検を実施すること。

第１２章 情報システムのセキュリティ要件

１２．１．主体認証機能

イ）情報又は情報システムへアクセス可能な利用者を特定するために、主体認証機能を導入すること。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講じること。
ロ）主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するため不正ログインを検知または防止するための措置を講ずること。
ハ）識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。
ニ）統括情報セキュリティ担当部署は、研究所の役職員及び研究所と一定の関わりのある者が、研究所の提供する情報サービスを利用する場合において用いる、本人であることを確認（以下、「認証」という）する情報・人的管理に関する基盤サービスにおける認証データの管理・運用の方針を定め、研究所が提供する情報サービスに係る情報システムの管理者に示さなければならない。

１２．２．情報セキュリティの脅威への対策

イ）統括情報セキュリティ担当部署は、ソフトウェアに関する脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策を講じるための手順を整備すること。
ロ）不正プログラム対策の講じられていない情報システムにおいて、研究所の情報を取扱い、又は研究所のネットワークに接続してはならない。
ハ）情報システムが不正プログラムに感染した可能性を認識した場合、速やかに当該情報システムをネットワークから切り離す等の処置を講じた上で、６．３「情報セキュリティインシデントへの対応」に従うこと。

１２．３．暗号・電子署名利用時の対策

イ）統括情報セキュリティ担当部署は、要機密情報、要完全情報を扱う際に必要となる、暗号化、及び暗号鍵管理の手順を定めること。
ロ）情報を暗号化する、又は情報に電子署名を付与する場合、必要に応じて前項の手順に従うこと。
ハ）暗号化された情報の復号、又は電子署名の付与に用いる暗号鍵について、必要に応じてイ）の暗号鍵管理手順に従うこと。

第１３章 情報システムの構成要素

１３．１．端末・サーバ装置等

イ）要保護情報を取り扱う端末及びサーバについては、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等に対する物理的脅威への対策や不正プログラム感染等に対する脆弱性対策等を講じること。
ロ）複合機及び特定用途機器(IoT 機器)については、購入時のセキュリティ要件を明確にするとともに、適切な設定や利用終了後のデータ削除といった情報セキュリティ対策を講じること。

１３．２．電子メール・ウェブ等

電子メール、ウェブ、ドメインネームシステム(DNS)、データベースを使いデータの送受信を行う場合、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他や、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為への対策を講じること。

１３．３．通信回線

研究所の当該サーバ装置や端末に接続する通信回線及び通信回線装置を導入・運用する際は、通信回線の運用主体又は物理的な回線の種類によって異なる情報セキュリティリスクに考慮し、導入・運用すること。

第１４章 情報システムの利用

１４．１．情報システムの利用に係る手順

イ）統括情報セキュリティ担当部署は、情報システムの利用に係る情報セキュリティ要件を、必要に応じて検討し手順を整備すること。
ロ）利用者は、情報セキュリティ対策規程、情報セキュリティ対策基準群、及び前項で定める手順を遵守し、情報システムを利用すること。

１４．２．情報システム利用の基本事項

イ）研究所が認める業務以外の目的で情報システムを利用してはならない。
ロ）所外情報システムを研究所の業務で利用する場合、及び所外情報システムで研究所の情報を扱う場合は、情報セキュリティ責任者の許可を得なければならない。
ハ）所外情報システムを、管理区域に持ち込み、研究所のネットワークに接続する場合は、情報セキュリティ責任者の許可を得なければならない。
ニ）情報セキュリティ責任者の許可を受けていない通信回線に情報システムを接続してはならない。
ホ）研究所が利用を禁止するソフトウェアを情報システム及び業務で利用する所外情報システム上で使用してはならない。研究所の業務において使用する必要のある場合、統括情報セキュリティ担当部署の許可を得ること。
ヘ）情報セキュリティ責任者の許可無く、情報システム、及び電磁的記録媒体を管理区域から持ち出してはならない。
ト）ソフトウェア、ハードウェア、及びその他のライセンスを遵守しなければならない。
チ）ソフトウェアその他の著作物の著作権を侵害してはならない。
リ）情報システムのターミナル操作ロック等、第三者による不正操作や情報の窃取を防止しなけれ

ばならない。

ヌ）要機密情報が記録される情報システムを使用する場合、情報の格付けと取扱制限に基づき情報の暗号化、パスワードロック、及び情報システムのロック等の情報セキュリティ対策を講じること。

ル）要機密情報が記録された情報システム及び電磁的記録媒体を管理区域外に持ち出す場合、前項の情報セキュリティ対策の他、情報セキュリティ責任者が定める情報セキュリティ要件を遵守すること。

ヲ）情報セキュリティ責任者は、所管する要機密情報の管理区域外への持ち出し、利用に伴う情報セキュリティ対策の要件を定め利用者に周知し、講じさせること。

１４．３．IP アドレス・ドメイン名の例外割り当てについて

イ）研究所の IP アドレス（134.160.0.0/16）に研究所のドメイン名（riken.jp/riken.go.jp）以外のドメインを付与する場合、６．２「例外措置」の手続きに従うこと。

ロ）研究所のドメイン名（riken.jp/riken.go.jp）に研究所の IP アドレス以外を付与する場合、６．２「例外措置」の手続きに従うこと。

ハ）イ）及びロ）の場合であっても、情報セキュリティ対策規程、及びこの対策基準を遵守すること。

１４．４．電磁的記録媒体の利用

要機密情報を USB メモリ、SD カード、外付け HDD 等の電磁的記録媒体において扱う場合、以下の事項を遵守すること。

- コンピュータウイルス対策ソフトウェア等を用いて電磁的記録媒体の安全性を確認すること。
- 情報の暗号化及びパスワードロック等の対策を講じること。
- 用途完了後は復元を困難にする手続きにより速やかに情報を削除すること。

１４．５．所外情報システムの利用手続き

イ）情報セキュリティ責任者は、部署の利用者が所外情報システムを研究所の業務に用いる場合、及び所外情報システムを用いて研究所の情報を扱う場合、別に定める申請書の記載内容を確認した上で、許可を与え、統括情報セキュリティ担当部署に登録すること。

ロ）利用者は、上記の所外情報システム利用に当たって、原則として、所外情報システムに研究所の要機密情報を保存してはならない。また、申請書に記載の内容を遵守すること。

ハ）情報セキュリティ責任者は、所外情報システムの利用において、許可期間、使用状況等を確認し、不適切な利用が認められた場合、当該利用者に改善を勧告、指示等すること。研究所は、これらの状況を確認するため、当該所外情報システムの検査を行う場合がある。

ニ）前項の勧告、指示等を受けた者は、速やかに改善すること。改善されない場合、研究所は、当該所外情報システムを隔離する場合がある。また不適切なアプリケーションの消去を指示することがある。

１４．６．ソーシャルメディアサービスによる情報発信

イ）CISO は、ソーシャルメディアサービスを用いて研究所の情報を発信する際の要件及び情報セキュリティ対策に係る手順を必要に応じて定めること。

ロ）情報セキュリティ責任者は、研究所の情報をソーシャルメディアサービスにおいて発信する必要がある場合、利用されるソーシャルメディアサービス毎に管理者を定め、監督させること。

ハ）情報セキュリティ責任者は、別に定める手続きにより利用内容や点検事項を確認し、ソーシャルメディアサービスの利用について、利用者に許可を与える前に統括情報セキュリティ担当部署に相談し、利用者に許可を与えた後には統括情報セキュリティ担当部署に利用登録をすること。

ニ）ソーシャルメディアサービスを用いて研究所の情報を発信する必要がある場合、イ）に定める手順、及び当該情報の取扱制限を遵守すること。

ホ）要完全性情報の提供にソーシャルメディアサービスを用いる場合、研究所ウェブサイトにおいても当該情報をあわせて提供すること。

１４．７．テレワーク

イ）統括情報セキュリティ担当部署は、テレワーク実施時の情報セキュリティ対策に係る規定及びテレワーク実施時の対策等に関する手順を整備すること。なお、原則としてテレワークは研究所が支給する端末で行う。ただし、私物など所外の端末を利用してテレワークを実施する場合も、上記の手順に従うこと。

ロ）情報セキュリティ責任者は、職員等が定められた手順に従い、テレワークの実施について必要となる通信環境や端末の利用時に情報セキュリティが確保されるような措置を講じること。

ハ）情報セキュリティ責任者は、テレワーク実施時の対策等に関する手順に従い、テレワーク実施前及び実施後に職員等が情報セキュリティ対策に必要な項目をチェックさせること。職員等は、定められた手順に従い、自宅等の認められた場所でのみテレワークを実施すること。

以上