国立研究開発法人産業技術総合研究所情報セキュリティ規程

制定　平成28年７月15日　28規程第52号
（17規程第75号の全部改正）
最終改正　平成29年６月22日　29規程第13号　一部改正

目次

第１章　総則

第１節　目的・適用範囲

（目的）

第１条　この規程は、国立研究開発法人産業技術総合研究所（以下「研究所」という。）が取り扱う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に必要な事項を定めることにより、継続的かつ効率的に業務を遂行することを図り、もって研究所の社会的信頼を確保することを目的とする。

（定義）

第２条　この規程において、次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。

一　情報　第３条第２項各号に定めるものをいう。

二　情報システム　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、研究所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。

三　外部委託　研究所の情報処理業務の一部又は全部について、契約をもって研究所外の者に実施させることをいい、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。

四　情報セキュリティ　情報及び情報システムが備えるべき性質を健全に保つことをいう。

五　職員等　職員及び契約職員をいう。

六　役職員等　役員及び職員等をいう。

七　外部人材　外部人材受入事前登録要領（23要領第45号）第２条第１号に規定する者をいう。

八　利用者　役職員等及び外部人材をいう。

九　記録媒体　情報が記録され、又は記載される有体物をいい、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）及び、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（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）をいう。

十　外部電磁的記録媒体　電磁的記録媒体のうちUSBメモリ、外付けハードディスクドライブ、DVD-R等をいう。

十一　機密性　情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。

十二　完全性　情報が破壊、改ざん又は消去されていない特性をいう。

十三　可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。

十四　通信回線　複数の情報システム又は機器等（研究所が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、研究所の情報システムにおいて利用される通信回線を総称したものをいう。ただし、研究所が直接管理していないものを含み、その種類（有線又は無線、物理回線又は仮想回線等）は問わないものとする。

十五　通信回線装置　通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置（ハブ、スイッチ、ルータ、ファイアウォール等を含む。）をいう。

十六　サーバ装置　情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、研究所が調達又は開発するものをいう。

十七　端末　システムの構成要素である機器のうち、利用者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボード、マウス等の周辺機器を含む。）をいい、特に断りがない限り、研究所が調達又は開発するもの（モバイル端末を含む。）をいう。

十八　特定用途機器　テレビ会議システム、IP電話システム、ネットワークカメラシステム

等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

十九　機器等　情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

二十　部門等　国立研究開発法人産業技術総合研究所組織規程（26規程第72号。以下「組織規程」という。）第６条第３項各号に規定する研究推進組織、同条第４項に規定する研究推進組織、第13条第２号に規定する監査室及び同条第３号に規定する評価部、組織規則（26規則第６号）第３条に規定するオープンイノベーションラボラトリ及び連携研究ラボ並びに組織規程第３章第２節に規定する本部組織、同規程第３章第３節に規定する事業組織及び同章第４節に規定する特別の組織に組織規則の定めるところにより置かれる部、室（部の下に置かれる室を除く。）、センター、スクール及びユニットをいう。

二十一　ネットワーク　複数の機器等を接続して情報を伝送し、協調動作させるための配線、ルータ、スイッチ等のハードウェア、及びアドレス、プロトコル、プログラム等のソフトウェアをいう。

二十二　研究所ネットワーク　研究所内に設置されたネットワーク及びそこから論理的に延長されたネットワーク並びに研究所の業務に供するため研究所外に設置されたネットワークであって、次に掲げるものをいう。

イ　AISTネットワーク　情報基盤部が研究所の基幹業務及び研究業務に供するために構成及び管理するネットワーク並びに部門等が構成及び管理し、当該ネットワークにのみ接続するプライベートネットワーク

ロ　個別管理ネットワーク　部門等又は外部機関が独自に構成及び管理するネットワークであって、次に掲げるネットワーク

（１）　完全閉鎖ネットワーク　部門等又は外部機関が独自に構成及び管理するネットワークであって、他のネットワークに接続しない完全に閉じたネットワーク

（２）　外部接続ネットワーク　部門等が業務を目的として構成及び管理するネットワークであって、AISTネットワークと直接接続せずにインターネットと接続するネットワーク

（３）　非AISTネットワーク　外部機関の機関が構成及び管理するネットワークであって、AISTネットワークと直接接続せずにインターネットと接続するネットワーク

二十三　情報サービス　情報に対して検索、編集、伝送等の処理を行うことをいう。

二十四　外部接続機器　外部接続ネットワークに接続されている情報システム及び情報サービス等のうち、研究所の業務のために運用し、インターネットからアクセスできるものをいう。

二十五　情報セキュリティ関係規程　この規程、要領、実施手順等をいう。

二十六　情報セキュリティ事象　情報セキュリティ関係規程を含む情報セキュリティ方針への違反若しくは管理策の不具合の可能性、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する事象をいう。

二十七　情報セキュリティインシデント　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。

二十八　来訪者　役職員等及び外部人材以外の者であって、会議、講演会等で研究所に来所する者をいう。

二十九　実施手順　この規程及びこの規程に基づく要領（以下「要領」という。）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をいう。

三十　基盤となる情報システム　他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

三十一　秘密文書　国立研究開発法人産業技術総合研究所文書管理・決裁規程（16規程第44号）第２条第３号に規定されている文書をいう。

（適用範囲）

第３条　この規程は、利用者に適用する。

２　この規程は、次の各号のいずれかに該当する情報に適用する。

一　利用者が業務上使用することを目的として研究所が調達し、又は開発した情報システム若しく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。）

二　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、利用者が業務上取り扱う情報

三　前二号以外の情報であって、研究所が調達し、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

３　この規程は、前項各号に規定する情報を取り扱う全ての情報システムに適用する。

（法令等の遵守）

第４条　利用者は、情報及び情報システムの取扱いに関し、情報セキュリティ関係規程のほか関係法令を遵守しなければならない。

第２節　情報の格付の区分

（情報の格付の区分）

第５条　情報は、機密性、完全性及び可用性の３つの観点を区別し、格付けをする。

２　機密性の格付の区分は、次の表の左欄に掲げるとおりとし、その分類の基準は、当該格付の区分ごとにそれぞれ同表の右欄に掲げるとおりとする。

格付の区分	分類の基準
機密性３情報	研究所で取り扱う情報のうち、秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	研究所で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「情報公開法」という。）第５条各号における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
機密性１情報	情報公開法第５条各号における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

３　完全性の格付の区分は、次の表の左欄に掲げるとおりとし、その分類の基準は、当該格付の区分ごとにそれぞれ同表の右欄に掲げるとおりとする。

格付の区分	分類の基準
完全性２情報	研究所で取り扱う情報（書面情報を除く。）のうち、その改ざん、誤謬又は破損により、外部機関及び個人の権利が侵害され又は研究所の運営に影響（軽微なものを除く。）を及ぼすおそれのある情報
完全性１情報	完全性２情報以外の情報（書面情報を除く。）

４　可用性の格付の区分は、次の表の左欄に掲げるとおりとし、その分類の基準は、当該格付の区分ごとにそれぞれ同表の右欄に掲げるとおりとする。

格付の区分	分類の基準
可用性２情報	研究所で取り扱う情報（書面情報を除く。）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、外部機関及び個人の権利が侵害され又は研究所の安定的な運営に影響（軽微なものを除く。）を及ぼすおそれのある情報
可用性１情報	可用性２情報以外の情報（書面情報を除く。）

５　前三項の場合において、一の情報に複数の格付に該当する情報が混在している場合には、その情報は、当該格付中の最上位の格付により取り扱うものとする。

第２章　情報セキュリティ対策の基本的枠組み

第１節　組織・体制

（最高情報セキュリティ責任者）

第６条　研究所に、最高情報セキュリティ責任者（以下「CISO」という。）を置き、理事長が役員のうちから指名する。

２　CISOは、研究所の情報セキュリティに関する業務を統括する。

３　CISOは、その権限に属する業務の一部を次条の最高情報セキュリティ責任者補佐、第９条第１項の情報セキュリティ監査責任者、第11条第１項の統括情報セキュリティ責任者、第16条第１項のネットワーク管理責任者等に、委任することができる。

（最高情報セキュリティ責任者補佐）

第７条　研究所に、１人又は２人以上の最高情報セキュリティ責任者補佐（以下「CISO補佐」という。）を置くことができる。

２　CISO補佐は、CISOが役職員等のうちから指名する。

３　CISO補佐は、CISOを補佐する。

（情報セキュリティ委員会）

第８条　研究所に、情報セキュリティ委員会（以下「委員会」という。）を置く。

２　委員会は、情報セキュリティに関する必要な事項を審議する。

３　委員会の組織及び運営に関して必要な事項は、要領で定める。

（情報セキュリティ監査責任者）

第９条　研究所に、情報セキュリティ監査責任者を置き、役職員等のうちからCISOが指名する。

２　情報セキュリティ監査責任者は、CISOの指示に基づき実施する監査に関する業務を統括する。

（事業所長等）

第10条　所長又は事業所長（以下「事業所長等」という。）は、その置かれる事業所等(組織規程第５条第３項に規定する事業所等をいう。以下同じ。)における情報セキュリティ責任者の情報セキュリティ対策を監督する。

（統括情報セキュリティ責任者）

第11条　研究所に、統括情報セキュリティ責任者を置き、CISOが役職員等のうちから指名する。

２　統括情報セキュリティ責任者は、事業所長等及び情報セキュリティ責任者を統括する。

３　統括情報セキュリティ責任者は、AISTネットワークに接続されている全ての機器等の管理を監督する。

（情報セキュリティ責任者）

第12条　部門等に、情報セキュリティ責任者を置き、部門等の長をもって充てる。

２　情報セキュリティ責任者は、その所属する部門等における情報セキュリティ対策に関する業務を統括し、並びに情報及び情報システムの管理を監督する。

３　部門等に所属しない利用者の情報セキュリティ責任者は、別表の左欄に掲げる利用者の所属の区分に応じ、それぞれ同表の右欄に定めるとおりとする。

４　第16条第１項のネットワーク管理責任者は、情報セキュリティ責任者とみなす。ただし、その管理する外部接続ネットワークの性質に照らし、特別な事情がある場合は、この限りでない。

（情報システムセキュリティ責任者）

第13条　部門等が所管する情報システム（外部接続ネットワーク及び外部接続機器を除く。）ごとに、情報システムセキュリティ責任者を置き、情報セキュリティ責任者が当該部門等に所属する役職員等のうちから指名する。ただし、研究所共通の情報システム（AISTネットワークを含む。）の情報システムセキュリティ責任者は、情報基盤部長をもって充てる。

２　情報セキュリティ責任者は、部門等で新たに情報システムを調達し、又は開発する場合には、当該情報システムの企画に着手するまでに、第１項に規定する指名を行わなければならない。

３　情報セキュリティ責任者は、情報システムセキュリティ責任者を指名したとき又は変更したときは、統括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。

４　情報システムセキュリティ責任者は、当該部門等が管理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を管理する。

５　第17条第１項の外部接続機器管理者は、情報システムセキュリティ責任者とみなす。ただし、その管理する外部接続機器の性質に照らし、特別の事情がある場合は、この限りではない。

（システム担当者）

第14条　部門等に、１人又は２人以上のシステム担当者を置き、当該部門等の職員等のうちから情報セキュリティ責任者が指名する。ただし、情報セキュリティ責任者が特別な事情があると認める場合は、この限りでない。

２　情報セキュリティ責任者は、２人以上のシステム担当者を指名したときは、当該システム担当者のうちから主システム担当者を指名するものとする。

３　情報セキュリティ責任者は、システム担当者又は主システム担当者を指名したとき又は変更したときは、統括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。

４　システム担当者は、当該部門等の情報セキュリティ責任者を補佐し、情報セキュリティ対策を実施する。

（区域情報セキュリティ責任者）

第15条　区域（情報セキュリティ責任者が部門等における施設及び環境に係る情報セキュリティ対策を行う単位ごとに定める区域をいう。以下同じ。）に、区域情報セキュリティ責任者を置き、当該区域を管理する情報セキュリティ責任者が当該情報セキュリティ責任者の部門等に所属する役職員等のうちから指名する。

２　情報セキュリティ責任者は、区域情報セキュリティ責任者を指名したとき又は変更したときは、統括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。

３　区域情報セキュリティ責任者は、その置かれる区域における情報セキュリティ対策の業務を統括する。

（ネットワーク管理責任者）

第16条　外部接続ネットワークごとに、ネットワーク管理責任者を置き、職員等のうちからCISOが指名する。

２　ネットワーク管理責任者は、外部接続ネットワークに対する情報セキュリティ対策に関する業務を統括する。

３　ネットワーク管理責任者は、その担当する外部接続ネットワークに接続されている全ての外部接続機器の管理を監督する。

４　ネットワーク管理責任者は、担当する外部接続ネットワークに接続されている全ての外部接続機器の管理状況を統括情報セキュリティ責任者に定期的に報告しなければならない。

（外部接続機器管理者）

第17条　外部接続機器ごとに、外部接続機器管理者を置き、当該外部接続機器を接続する外部接続ネットワークのネットワーク管理責任者が、情報セキュリティに関する知識を十分に有する者のうちから、指名する。

２　外部接続機器管理者は、ネットワーク管理責任者の指示を受け、その担当する外部接続機器に対する情報セキュリティ対策に関する業務を管理する。

３　外部接続機器管理者は、外部接続機器の管理状況をその接続する外部接続ネットワークを担当するネットワーク管理責任者に定期的に報告しなければならない。

（最高情報セキュリティアドバイザー）

第18条　研究所に、必要に応じ、最高情報セキュリティアドバイザーを置くことができる。

２　最高情報セキュリティアドバイザーは、情報セキュリティに関する専門的な知識及び経験

を有する役職員等又は研究所以外の者から、CISOが指名又は委嘱する。

３　最高情報セキュリティアドバイザーは、CISOに対し研究所の情報セキュリティに関する専門的な助言を行う。

（CSIRT）

第19条　研究所に、研究所において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に設置される体制（以下「CSIRT」という。）を置く。

２　CSIRTにCSIRT責任者を置き、統括情報セキュリティ責任者をもって充てる。３　CISOは、CSIRTを整備し、その役割を明確化する。

４　CSIRTの組織及び運営に関して必要な事項は、要領で定める。５　CISOは、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

（情報セキュリティ対策本部）

第20条　CISOは、重大な情報セキュリティインシデントに対処するため、情報セキュリティ対策本部（以下「対策本部」という。）を組織することができる。

２　対策本部は、CISOの命を受けて、研究所ネットワークのセキュリティ確保のために、必要な措置を講じ、又はCSIRTその他の組織に対して必要な措置を指示することができる。

３　対策本部の組織及び運営に関して必要な事項は、要領で定める。

（兼務の禁止）

第21条　役職員等は、情報セキュリティ対策の運用において、次の各号に掲げる役割を兼務してはならない。

一　情報セキュリティ関係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者（以下、本条において「承認権限者等」という。）

二　情報セキュリティ関係規程の規定により監査を受ける者とその監査を実施する者

２　利用者は、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対し承認等を申請し、承認等を得るものとする。

（外部人材及び来訪者）

第22条　情報セキュリティ責任者は、外部人材又は来訪者に情報又は情報システムを利用させる場合には、必要に応じ誓約書を提出させ、情報セキュリティの確保のために必要な措置を講じなければならない。

２　情報セキュリティ責任者は、外部人材又は来訪者に前項の規定により誓約書を提出させる場合には、次の各号に掲げる事項を明示させなければならない。

一　情報セキュリティに関係する規程の遵守に関すること。

二　秘密保持の義務に関すること。

三　情報システムの取扱いに関すること。

四　契約に違反した場合の措置に関すること。

五　その他CISOが特に必要と認める事項

３　役職員等は、外部人材又は来訪者を受け入れて、情報及び情報システムを利用させる場合

には、受け入れた外部人材又は来訪者に対して、情報セキュリティ関係規程を遵守するよう指導及び監督しなければならない。

第２節　対策推進計画の策定

（対策推進計画の策定）

第23条　CISOは、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計画（以下「対策推進計画」という。）を定めるものとする。

２　対策推進計画には、研究所の業務、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次の各号に掲げる取組の方針、重点及びその実施時期を含めなければならない。

一　情報セキュリティに関する教育

二　情報セキュリティ対策の自己点検

三　情報セキュリティ監査

四　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

五　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

第３節　情報セキュリティ関係規程の運用

（情報セキュリティ対策に関する実施手順の整備・運用）

第24条　統括情報セキュリティ責任者は、研究所全体に係わる情報セキュリティ対策に関する実施手順を情報セキュリティ実施ガイドとして整備（要領で整備すべき者を別に定める場合を除く。）し、実施手順に関する業務を統括し、整備状況についてCISO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、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の実施手順を整備しなければならない。

３　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関係規程に係る課題及び問題点の報告を受けた場合には、統括情報セキュリティ責任者に報告するものとする。

（違反への対処）

第25条　利用者は、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には、直ちにその所属する部門等の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又は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、直ちに当該重大な違反の事実があった事業所等の事業所長等に報告しなければならない。

３　前項の報告を受けた事業所長等は、直ちに統括情報セキュリティ責任者を通じて、CISOに報告しなければならない。

４　職員等は、故意若しくは重大な過失によりこの規程に違反した場合又は重大な情報セキュリティの侵害を行った場合には、国立研究開発法人産業技術総合研究所職員就業規則（17規程第２号）、国立研究開発法人産業技術総合研究所任期付職員就業規則（17規程第３号）又は国立研究開発法人産業技術総合研究所契約職員就業規則（17規程第４号）の定めるところにより処分されることがある。

５　外部人材は、故意若しくは重大な過失によりこの規程に違反した場合、重大な情報セキュ

リティの侵害を行った場合又はこの規程に基づく役職員等の指示に従わなかった場合には、その受入制度による契約等を解除されることがある。

（例外措置）

第26条　情報セキュリティ責任者は、この規程の適用を受けることが研究所の業務の適正な遂行を著しく妨げると認める場合等は、統括情報セキュリティ責任者にこの規程に規定された情報セキュリティ対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないこと（以下「例外措置」という。）の承認を得なければならない。

２　CISOは、例外措置の審査手続を別に定める。

３　情報セキュリティ責任者は、例外措置の適用を受けようとする場合には、前項の審査手続（以下「審査手続」という。）に従い、例外措置の適用の申請をしなければならない。やむを得ない理由により事前に申請ができない場合には、例外措置の実施後速やかに申請し、承認を得なければならない。

４　統括情報セキュリティ責任者は、例外措置の決定を行う場合には、審査手続に従って審査し、承認の可否を決定するとともに、例外措置の適用審査記録の台帳を作成し、当該例外措置の適用の対象、代替の方法等を記録しなければならない。

第３章　教育

（教育体制等の整備）

第27条　統括情報セキュリティ責任者は、情報セキュリティ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しなければならない。

（教育の実施）

第28条　統括情報セキュリティ責任者は、利用者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実施しなければならない。

２　利用者は、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。

３　情報セキュリティ責任者は、その置かれる部門等に所属する職員等及び外部人材に研修の有用性を周知し、積極的な受講を促すとともに、研修に参加しやすい職場環境の整備に努めるものとする。

４　統括情報セキュリティ責任者は、CSIRTに属する職員等に教育を適切に受講させなければならない。

５　統括情報セキュリティ責任者は、CISOに情報セキュリティに関する教育の実施状況について報告しなければならない。

第４章　情報セキュリティインシデントへの対処

（情報セキュリティインシデントに備えた事前準備）

第29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研究所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、役職員等に周知しなければならない。

２　統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の研究所と外部機関との情報共有を含む対処手順を整備するものとする。

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、業務遂行のため

に特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備しなければならない。

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、業務遂行のために特に重要と認めた情報システムについて、その訓練の内容及び体制を整備しなければならない。

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研究所以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研究所外の者に明示するものとする。

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ものとする。

（情報セキュリティインシデントの認知時における報告・対処）

第30条　利用者は、情報セキュリティインシデントの可能性を認知した場合には、直ちにその所属する部門等の情報セキュリティ責任者に報告し、その指示に従わなければならない。

2　情報セキュリティ責任者は、前項の規定により報告を受けた場合には、速やかに必要な指示を行うとともに、当該情報セキュリティインシデントに関係する事業所等の事業所長等に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、CSIRTその他関係者にその旨を報告しなければならない。

3　ネットワーク管理責任者は、外部接続ネットワーク上の情報セキュリティインシデントを認知した場合には、外部接続機器管理者に適切な指示を行うとともに、CSIRTに報告しなければならない。

4　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ものとする。

5　CSIRT責任者は、情報セキュリティインシデントであると評価した場合には、当該情報セキュリティインシデントについてCISOに速やかに報告しなければならない。

6　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情報セキュリティインシデントからの復旧に係る指示又は勧告を行なうものとする。

7　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、研究所で定める対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処しなければならない。

8　情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等を定めている場合には、当該運用管理規程等に従い、適切に対処するものとする。

9　情報セキュリティ責任者は、利用者から報告のあった情報セキュリティインシデント及び対処内容を体系的に記録し、必要に応じこれを活用できるよう適正に保存しなければならない。

（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31条　情報セキュリティ責任者は、前条第６項の規定によりCSIRTから応急措置の実施又は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CISOに報告しなければならない。

２　CISO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ものとする。

３　CSIRT責任者は、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等に共有するものとする。

第５章　点検

第１節　情報セキュリティ対策の自己点検

（自己点検）

第32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自己点検計画を策定するものとする。

２　統括情報セキュリティ責任者は、利用者ごとの自己点検票及び自己点検の実施手順を整備するものとする。

３　情報セキュリティ責任者は、自己点検計画に基づき、利用者に自己点検の実施を指示しなければならない。

４　利用者は、情報セキュリティ責任者からの前項の指示に基づき、第２項の自己点検票及び自己点検の手順を用いて自己点検を実施しなければならない。

（自己点検結果の評価・改善）

第33条　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は、利用者による自己点検結果を分析し、評価するものとする。

２　統括情報セキュリティ責任者は、前項の規定による評価の結果をCISOに報告しなければならない。

３　CISO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ものとする。

４　利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行なわなければならない。

第２節　情報セキュリティ監査

（情報セキュリティ監査）

第34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定めなければならない。

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の指示をCISOから受けた場合には、追加の監査実施計画を定めなければならない。

３　情報セキュリティ監査責任者は、監査実施計画に基づき、監査を実施する際に、次の各号

に掲げる事項について必要に応じ確認しなければならない。

一　情報セキュリティ関係規程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。

二　実施手順が情報セキュリティに関する規程類に準拠していること。

三　自己点検の適正性の確認を行うなどにより、被監査部門等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、監査を行う場合には、被監査部門等から独立した情報セキュリティ監査を実施する役職員等に対して監査の実施を依頼するものとする。

5　前項の監査を実施する者は、監査を行ったときは、遅滞なく監査した内容に基づき監査調書を作成し、定められた期間保存するものとする。

6　情報セキュリティ監査責任者は、前項の監査調書に基づき監査報告書（以下「監査報告書」という。）を作成し、監査実施計画が定める期限までに、CISO及び委員会に報告しなければならない。

7　情報セキュリティ監査責任者は、必要に応じ、研究所以外の者に監査の一部を請け負わせることができる。

（監査結果に応じた対処）

第35条　CISO及び委員会は、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情報セキュリティ責任者及び情報システムセキュリティ責任者に指示するものとする。

2　CISO及び委員会は、監査報告書の内容を踏まえ、監査を受けた部門等以外の部門等においても同種の課題及び問題点がある可能性が高く、かつ、緊急に同種の課題及び問題点があることを確認する必要があると認める場合には、他の情報セキュリティ責任者及び情報システムセキュリティ責任者に対しても、同種の課題及び問題点の有無を確認するよう指示するものとする。

3　情報セキュリティ責任者及び情報システムセキュリティ責任者は、監査報告書等に基づいてCISO又は委員会から改善を指示されたことについて、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CISO又は委員会に報告しなければならない。

第６章　見直し

（情報セキュリティ関係規程の見直し）

第36条　CISO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、委員会の審議を経て、この規程及び要領について必要な見直しを行うものとする。また、統括情報セキュリティ責任者は、実施ガイドについて必要な見直しを行い、定期的に見直し状況についてCISOに報告するものとする。

（対策推進計画の見直し）

第37条　CISOは、情報セキュリティ対策の運用及び自己点検・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、委員会の審議を経て、対策推進計画について定期的な見直しを行うものとする。

第７章　雑則

（情報セキュリティ関係規程の周知）

第38条　CISOは、利用者に情報セキュリティ関係規程を周知徹底させるため、情報セキュリティ関係規程に関連する全ての文書を適切な手段によって掲示するものとし、情報セキュリティ関係規程及びこれらに関連する全ての文書に変更が発生した場合には、遅滞なく周知するものとする。

（委任）

第39条　この規程に定めるもののほか、研究所が情報セキュリティの確保に関し必要な事項は、要領で定める。

附　則（28規程第52号・全部改正）

（施行期日）

第１条　この規程は、平成28年７月15日から施行する。

（経過措置）

第２条　この規程の施行前に改正前の国立研究開発法人産業技術総合研究所情報セキュリティ規程の規定により行われた申請、承認、許可その他の行為は、この規程の施行後は、この規程の相当規定に基づいて行われた申請、承認、許可その他の行為とみなす。

附　則（29規程第13号・一部改正）

この規程は、平成29年７月１日から施行する。

別表（第12条第３項関係）

利用者の所属	情報セキュリティ責任者
組織規程第６条第１項各号に規定する研究推進組織に所属する利用者	領域長又は総合センター長
組織規程第13条に規定する本部組織（第２号及び第３号を除く。）に所属する利用者	組織規程第13条に規定する本部組織（第２号及び第３号を除く。）の長
組織規程第21条第１項に規定する事業組織に所属する利用者	所長又は事業所長
組織規程第22条第１項に規定する特別の組織に所属する利用者	ＴＩＡ推進センター長
前欄までに掲げる利用者以外の利用者	所長又は事業所長