東京工業大学地球生命研究所

情報セキュリティ実施手順

（平成２５年７月）

目　　　　　　次

１．趣旨

東京工業大学地球生命研究所情報セキュリティ実施手順は，地球生命研究所の業務を遂行する職員および情報システムを利用する学生等が，国立大学法人東京工業大学情報セキュリティ規則（平成１７年規則第３２号）を遵守し，大学の情報資産に対するセキュリティを確保するための具体的な対策手順を定めるものである。

以下，地球生命研究所を「研究所」，研究所情報セキュリティ実施手順を「実施手順」，東京工業大学情報セキュリティ規則を「情報セキュリティ規則」という。「職員」は常勤の職員ばかりでなく非常勤職員および委託業者を含み，「学生等」は正規課程学生ばかりでなく科目等履修生や研究生など非正規課程学生も含む。また研究所の「業務」とは研究所における教育，研究，事務処理等を指す。

２．組織

研究所に関連する業務を円滑に遂行するため，情報セキュリティ規則第２１，２２，２４，２５，２６条に基づき，組織体制を以下のように定める。

情報セキュリティ統括責任者	地球生命研究所長
同 代理	研究所長が指名する副研究所長
情報セキュリティ責任者	情報セキュリティ統括責任者が指名する者及び事務部門長
情報資産管理担当者	職員
連絡担当者	情報資産管理担当者が指名する者
情報システム管理者	情報資産管理担当者が指名する者

３．遵守事項

情報コンテンツおよび情報システムを利用するにあたっては，国立大学法人東京工業大学情報倫理ポリシーおよび国立大学法人東京工業大学情報セキュリティポリシーに則り，情報倫理秩序を守り，学内外からの本学情報資産に対する侵害を阻止しなければならない。そのため，以下に掲げる事項を遵守しなければならない。

職員が遵守すべき事項

(1) 実施手順に従い，情報セキュリティの問題が生じないように業務を遂行する。

(2) 情報セキュリティ規則を遵守する。また，個人情報を取り扱う際には，

国立大学法人東京工業大学個人情報保護規程（平成１７年規程第５号）及び国立大学法人東京工業大学個人情報管理規程（平成１７年規程第６号）に従う。なお，判断がつきかねる場合には，速やかに情報資産管理担当者または情報セキュリティ統括責任者（同代理を含む。以下同様。）に相談し，指示を仰ぐ。

(3) 情報セキュリティ規則に違反する行為を発見した場合には，直ちに情報セキュリティ統括責任者および情報セキュリティ責任者に報告する。

(4) 情報セキュリティに関する事故，システム上の欠陥および誤動作を発見した場合には，情報資産管理担当者に報告し，指示を仰ぐ。情報資産管理担当者は，報告のあった事故等で重要なものについては，情報セキュリティ統括責任者および情報セキュリティ責任者に報告するとともに，情報セキュリティ統括責任者の指示の下，必要な措置を講ずる。

情報システムを利用する職員および学生等が遵守すべき事項

(1) 情報システムを利用する際には，国立大学法人東京工業大学情報倫理規則（平成１７年規則第３１号）第５条の「情報倫理とセキュリティのためのガイド」に従い，倫理的かつ防衛的に行動する。

４．情報コンテンツの管理と利用

情報セキュリティ規則第２条に定められた情報コンテンツとは，大学が管理・運用する教育，研究および事務処理に係る全ての情報（紙媒体・電磁媒体等に記録されたもの）である。そのうち，本実施手順で対象とする情報コンテンツは，以下のものとする。

(1) 研究所の業務を遂行する過程で作成または取得されたもので，法令，契約，学内諸規則等により，秘匿または保存が義務付けられているもの（国立大学法人東京工業大学文書管理規則（平成１６年規則第９９号）に定められた教員（兼任を含む）が主体となって管理する法人文書および研究所長が専決者または受任者に定められている法人文書を含む。）。

(2) 他部局等が管理する情報コンテンツの複製で，当該部局がⅡまたはⅣに分類すると定めたもの（Ⅰは非公開，Ⅲは研究所として，秘密にする必要もなければ保存する必要もないので対象外。）。

(3) その他の情報コンテンツで，情報セキュリティ統括責任者，情報セキュリティ責任者または情報資産管理担当者が重要と認めたもの。

秘匿すべき情報コンテンツの漏洩（メディアの盗難・紛失を含む。）及び保存すべき情報コンテンツの改ざん・消失（メディアの紛失，破壊等により情報

コンテンツが復元できなくなる場合を含む。）が起こらないよう，情報セキュリティ統括責任者は，情報セキュリティ責任者を通じて職員に対して日頃から本実施手順に基づき，適切な教育指導を行う。なお，業務（の一部）を外部委託する場合は，委託業者に対しても職員に準じた指導を行う。

情報コンテンツの分類

情報セキュリティ規則第４条に従い，機密性，統一性（完全性）および可用性を踏まえ，情報コンテンツをその重要性に応じ下記のⅠ～Ⅳに分類する。具体的な内容は，以下に例示する。

Ⅰ．学外および学内の他部局等に公開することのできない情報コンテンツ
（秘の情報コンテンツを含む。）
Ⅱ．学外に公開することのできない情報コンテンツ
（秘の情報コンテンツを含む。）
Ⅲ．学外に公開する情報コンテンツのうち業務上重要な情報コンテンツ
Ⅳ．上記分類Ⅰ，Ⅱ，Ⅲに掲げるもののほか業務上重要な情報コンテンツ

「業務上重要な情報コンテンツ」とは，仮にその情報コンテンツが失われ，または漏洩した場合，業務の遂行に支障を来す可能性のあるものと解釈する。分類にあたっては以下の点に注意する。

(1) 原則として，当該情報コンテンツを作成し，または取得した管理部署の情報資産管理担当者が分類を行う。複数の管理部署に所属する職員が共同で作成した情報コンテンツについては，情報セキュリティ統括責任者または情報セキュリティ責任者が指名した情報資産管理担当者が分類を行う。既存情報コンテンツの分類変更についても同様とする。
(2) 特に秘密とすべきものはⅠまたはⅡ，秘密とするには及ばないが当面公開の予定がないものはⅣ，公開するものはⅢに分類する。
(3) 分類を行う際には，破棄または分類変更までの期限を定めることができる。分類Ⅰ，Ⅱについては，必要最低限の期間のみ指定を行い，業務に支障がでない範囲で速やかに当該情報コンテンツの破棄または分類変更を行う。
(4) 他部局等が管理する情報コンテンツの複製を取得した場合には，当該部局による分類に準じた扱いを行う。ただし，消失対策は不要である。

情報コンテンツの管理および取り扱い

(1) 秘匿すべき情報コンテンツ（分類Ⅰ，Ⅱ）については，業務遂行上必

要な職員のみが閲覧できるよう，適切なアクセス制限を行う。アクセス制限の具体的な方法としては，錠を用いた物理的な制限，暗号を用いた電子的な制限などを状況に応じて使い分ける。ネットワークに接続したコンピュータに格納する場合には，不正侵入防止処置も施す。なお，正本のみでなく，すべての複製について同様の処置が必要である。

(2) 秘匿すべき情報コンテンツ（分類Ⅰ，Ⅱ）を外部に持ち出す必要がある場合（メール等の通信手段を用いる場合を含む。）には，情報資産管理担当者の許可を得る。また，情報コンテンツが漏洩しないようにするために，通信時には必ず暗号化を施し，持ち出したコピー（ディスク等の媒体に格納されたもの）に対しては物理的または電子的な漏洩防止処置を施す。この処置が困難な場合（機器の修理等に伴い持ち出す場合等）には，持ち出した情報コンテンツを読み出す可能性がある者（修理を委託した業者等）と秘密を守ることを定めた契約を結ぶ。

(3) 秘匿すべき情報コンテンツ（分類Ⅰ，Ⅱ）の複製を新たに作成する場合または複製を廃棄する場合には，情報資産管理担当者の許可を得る。廃棄を行う場合には，情報コンテンツの復元ができないようにするための処置を施す。磁気ディスク媒体の場合，OS コマンドによる通常の消去やディスクのフォーマットでは完全な消去が難しいので，専用のデータ消去ソフトを用いるか，物理的に破壊する等の処置を施す。

(4) 情報コンテンツ（分類Ⅰ-Ⅳ）を電磁的に記録して保存する場合には，バックアップ用の複製を作成し，不慮の事故による消失に備える。

(5) (1)-(4)にかかわらず，取扱いについて法令等に定めがあるもの，または契約，学内諸規則等に規定されているものについては，それに従う。

委託契約

(1) 情報コンテンツの処理・保管等を外部委託する場合は，情報セキュリティ規則第１３条に定める内容の外部委託契約を締結する。

５．情報システムの管理

盗難の防止

(1) 情報システムを盗難から守るため，機器を設置した部屋を無人とする時には施錠を行う。施錠が困難な部屋では，監視カメラを設置する等の適切な処置を施す。

不正利用の防止

(1) 正規利用者以外の者による情報システムの利用を防止するため，適切なアクセス制限を行う。アクセス制限の具体的な方法としては，物理的な入室制限，パスワード，物理トークン(IC カード，RFID 等)，生体情報等を用いたログインの制限などを状況に応じて使い分ける。

サイバー攻撃への対応

(1) OS やアプリケーションプログラムに対し，可能な限り速やかに最新のセキュリティパッチを適用する。

(2) アンチウイルスソフト，パーソナルファイアウォール，侵入検知・防止システム等のパターンファイル等を可能な限り速やかに最新のものに更新する。

停電への対応

(1) 業務上特に重要な機器については，無停電電源等を設置し，停電に対する十分な処置を施す。

委託契約

(1) 情報システムの開発・管理・保守等を外部委託する場合は，情報セキュリティ規則第１３条に定める内容の外部委託契約を締結する。

６．人的管理体制

情報セキュリティ規則および実施手順の周知

(1) 情報セキュリティ統括責任者は，情報セキュリティ責任者を通じて，情報セキュリティ規則および実施手順を守るよう，職員（情報システムの利用に関する部分については学生等を含む。）に日頃から適切な教育指導を行う。業務（の一部）を外部委託する場合は，委託業者に対しても職員に準じた指導を行う。

(2) 情報セキュリティ統括責任者は，常に実施手順を参照できるような措置を講じる。

情報セキュリティ規則の遵守状況の確認

(1) 情報セキュリティ統括責任者および情報セキュリティ責任者は，情報セキュリティ規則が遵守されているか，また，情報セキュリティに関するする問題が発生していないかを定期的に確認する。

事故・欠陥に対する報告

(1) 情報セキュリティ統括責任者は，情報セキュリティに関する事故・システム上の欠陥および誤動作の報告を受けた場合に，必要な処置を講じるよう，情報資産管理担当者に指示を行う。また，その重要性に応じて関係部署に連絡するとともに，これらの事故等を最高情報セキュリティ責任者に報告する