Independent Administrative Institution
Okinawa Institute of Science and Technology Promotion Corporation
Personal Information Protection Regulations
独立行政法人　沖縄科学技術研究基盤整備機構
個人情報保護規程

(Regulations No.001 of 2006 - April 1, 2006)
（平成１８年４月１日　平成１８年規程第００１号）
Revised (Regulations No.17 of 2010 – March 31, 2010)
改正（平成２２年３月３１日　平成２２年規程第１７号）

Contents　目次

Chapter 1. General Provisions
第１章　総則

Article 1. Purpose （目的）

The purpose of these Regulations is to set forth the handling of personal information by the Okinawa Institute of Science and Technology Promotion Corporation (hereinafter, the “Corporation”) so as to provide for the smooth and appropriate administration of the business and operations of the Corporation while protecting the rights and interests of the individual.

この規程は、独立行政法人沖縄科学技術研究基盤整備機構（以下「機構」という。）における個人情報の取扱いに関する基本的事項を定めることにより、機構の事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

Article 2. Definitions （定義）

The terms used in these Regulations shall be construed in accordance with Article 2 of the Law concerning Access to Personal Information Held by Independent Administrative Institutions (Law No. 59 of 2003; hereinafter, the “Law”).

この規程における用語の意義は、「独立行政法人等の保有する個人情報の保護に関する法律」（平成15年法律第59号。以下「法」という。）第２条の定めるところによる。

Chapter 2. Management System
第２章　管理体制

Article 3. General Manager for Personal Information Protection （個人情報総括保護管理者）

1. The Executive Director shall be the General Manager for Personal Information Protection.

   機構に、個人情報総括保護管理者（以下「総括保護管理者」という。）１名を置き、事務
   局長をもって充てる。
2. The General Manager for Personal Information Protection shall have general responsibility for the management of personal information retained by the Corporation.

   総括保護管理者は、機構における保有個人情報の管理に関する事務を総括する。

Article 4. Assistant General Manager for Personal Information Protection （個人情報副総括保護管理者）

1. The Senior Manager of the General Affairs Group of the Corporation shall be the Assistant General Manager for Personal Information Protection.

   機構に、個人情報副総括保護管理者（以下「副総括保護管理者」という。）１名を置き、総務グループ統括をもって充てる。

2. The Assistant General Manager for Personal Information Protection shall assist the General Manager for Personal Information Protection.
副総括保護管理者は、総括保護管理者を補佐する。

Article 5. Personal Information Systems Manager （個人情報システム管理者）

1. The Manager of General Affairs Section of General Affairs Group shall be the Personal Information Systems Manager.
機構に、個人情報システム管理者（以下「情報システム管理者」という。）１名を置き、総務グループ総務課長をもって充てる。
2. The Personal Information Systems Manager shall assist the General Manager for Personal Information Protection and supervise matters relating to the administration of computer systems and networks used to manage personal information.
情報システム管理者は、総括保護管理者を補佐し、保有個人情報の管理に係る電算機システム及びネットワークの運用に関する事務を統括する。

Article 6. Departmental Personal Information Protection Manager （部室個人情報保護管理者）

1. The head of each department shall be the Departmental Personal Information Protection Manager.
各部室に、部室個人情報保護管理者（以下「部室保護管理者」という。）１名を置き、
当該部室の長をもって充てる。
2. The Departmental Personal Information Protection Manager shall have general responsibility for the management of personal information retained by the department.
部室保護管理者は、当該部室における保有個人情報の管理に関する事務を統括する。

Article 7. Sectional Personal Information Protection Manager （課室個人情報保護管理者）

1. Each section shall appoint one Sectional Personal Information Protection Manager, which position shall be filled by the head of the section.
各課室等に、課室個人情報保護管理者（以下「課室保護管理者」という。）１名を置き、当該課室等の長をもって充てる。
2. The Sectional Personal Information Protection Manager shall have general responsibility for the management of personal information retained by the section.
課室保護管理者は、当該課室における保有個人情報の管理に関する事務を統括する。

Article 8. Personal Information Protection Officer （個人情報保護担当者）

1. The Sectional Personal Information Protection Manager from each section shall appoint one Personal Information Protection Officer to be the Document Management Officer as set forth in the Document Management Regulations.
   各課室等に、当該課室等の課室保護管理者が指名する個人情報保護担当者（以下「保護担当者」という。）１名を置き、文書管理規程に定める文書管理担当者をもって充てる。
2. The Personal Information Protection Officer shall assist the Sectional Personal Information Protection Manager and shall be in charge of day-to-day operations relevant to the management of the personal information retained in the section.
   保護担当者は、課室保護管理者を補佐し、各課室等における保有個人情報の管理に関する事務を担当する。

Article 9. Personal Information Protection Auditor （監査責任者）

1. The part-time auditor of the Corporation shall be appointed as the Personal Information Protection Auditor.
   機構に、個人情報保護監査責任者（以下「監査責任者」という。）を１名置くこととし、非常勤の監事をもって充てる。
2. The Personal Information Protection Auditor shall be responsible for auditing the status of management for retained personal information.
   監査責任者は、保有個人情報の管理の状況について監査する任に当たる。

Article 10. Personal InformationArticle 10. Personal Information Protection Committee （個人情報保護委員会）

1. The Corporation shall establish a Personal Information Protection Committee (hereinafter, the “Committee”) to determine important matters related to the management of retained personal information and to provide relevant communication and coordination, etc.
   機構に、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため、個人情報保護委員会（以下「委員会」という。）を設置する。
2. The Committee shall be comprised of a chairperson, vice chairperson and committee members.
   委員会は、委員長、副委員長及び委員をもって構成する。
3. The General Manager for Personal Information Protection shall serve as chairperson and shall preside over the Committee.
   委員長は、委員会を主宰し、総括保護管理者をもって充てる。
4. The Assistant General Manager for Personal Information Protection shall serve as vice chairperson and shall assist the chairperson.
   副委員長は、委員長を補佐し、副総括保護管理者をもって充てる。
5. Committee members shall comprise the Personal Information Systems Manager and other such staff members and shall be nominated by the President.

委員は、情報システム管理者並びに理事長が指名する職員をもって構成する。

6. General Affairs Section of General Affairs Group shall be responsible for the day-to-day operations of the Committee.
   委員会の事務は、総務グループ総務課が担当する。
7. In addition to the matters set forth in this article, the Committee chairperson may determine other necessary matters regarding the operation of the Committee.
   本条に定めるもののほか、委員会の運営に関し必要な事項は、委員長が定める。

Article 11. Staff Training　（職員研修）

1. The General Manager for Personal Information Protection shall provide staff members handling retained personal information adequate training in matters of retained personal information handling and increase general awareness of personal information protection.
   総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な研修を行う。
2. The General Manager for Personal Information Protection shall provide staff members involved in the management of information systems handling retained personal information with necessary training in the management, operations, and security of information systems to enable appropriate management of retained personal information.
   総括保護管理者は、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な研修を行う。

Article 12. Staff Responsibilities　（職員の責務）

Staff members shall adhere to the letter and intent of all relevant laws, ordinances and regulations, etc. and follow the instructions of the General Manager for Personal Information Protection, Assistant General Manager for Personal Information Protection, Personal Information Systems Manager, Departmental Personal Information Protection Manager, Sectional Personal Information Protection Manager, and Personal Information Protection Officer.
職員は、法の趣旨に則り、関連する法令及び例規等の定めを遵守するとともに、総括保護管理者、副総括保護管理者、情報システム管理者、部室保護管理者、課室保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

Chapter 3. Personal Information Management
第３章　保有個人情報の取扱い

Article 13. Access （アクセス制限）

1. The Sectional Personal Information Protection Manager shall restrict access to personal information to the minimum staff, as warranted by the confidentiality and nature of the retained personal information, required to achieve the purpose of use.

   課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員に限るものとする。

2. Unauthorized Staff members shall not access personal information.

   アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。

3. Staff members shall not access personal information for non-operational purposes.

   職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

Article 14. Personal Information Copying, Distribution, etc. （複製等の制限）

Staff members shall follow the instructions of Sectional Personal Information Protection Manager when handling of personal information for operational purposes in any of the following activities

職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次の各号に掲げる行為については、課室保護管理者の指示に従わなければならない。

1. Copying of personal information
   保有個人情報の複製
2. Distribution of personal information
   保有個人情報の送信
3. Distribution to outside parties or distribution of media containing personal information
   保有個人情報が記録されている媒体の外部への送付又は持出し
4. Other inappropriate management of personal information
   その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

Article 15. Error Amendment, etc. （誤りの訂正等）

Staff members, as instructed by the Sectional Personal Information Protection Manager, shall promptly correct personal information errors, etc.

職員は、保有個人情報の内容に誤り等を発見した場合には、課室保護管理者の指示に従い、訂正等を行わなければならない。

Article 16. Electronic Media, File Management （媒体の管理等）

Staff members shall store personal information media in a designated location as instructed by the Sectional Personal Information Protection Manager, and when

deemed necessary, store said media under lock and key in a fireproof safe.
職員は、課室保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。

Article 17. Electronic Media, File Destruction, etc. （廃棄等）

In the event that personal information files, media (including storage, terminals, and servers) is no longer needed, staff members, as instructed by the Sectional Personal Information Protection Manager, shall delete relevant information and/or destroy relevant media in a manner that renders it impossible to recover or decipher the retained personal information.
職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、課室保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行わなければならない。

Article 18. Personal Information Handling Records（保有個人情報の取扱状況の記録）

As warranted by the confidentiality and nature of the personal information, the Sectional Personal Information Protection Manager shall create ledgers, etc. and record the status of personal information use, storage, and handling.
課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

Article 19. Personal Information File Ledgers Management, etc. （個人情報ファイル簿の管理等）

1. The General Affairs Section of General Affairs Group shall create, store, and publish personal information file ledgers.
   個人情報ファイル簿は、総務グループ総務課が整備し、保管及び公表する。
2. The Sectional Personal Information Protection Manager shall formally request the General Affairs Section of General Affairs Group when updating the personal information file ledger and, whenever necessary, amend matters recorded to the personal information file ledger.
   課室保護管理者は、個人情報ファイル簿に記載すべき個人情報ファイルを保有したとき、又は個人情報ファイル簿に記載されている事項を訂正等する必要があるときは、個人情報ファイル簿を更新するよう総務グループ総務課に連絡しなければならない。

Chapter 4. IT Systems Security
第４章　情報システムにおける安全の確保等

Article 20. Access （アクセス制御）

1. The Sectional Personal Information Protection Manager shall take necessary measures, as warranted by the confidentiality and nature of personal information (in this article, Article 23 and Article 25 through Article 29, this shall be limited to retained personal information handled in information systems), to control access by establishing security measures (passwords, smart cards, biometrics) to verify authorization (hereinafter, “Authentication Functions”).

   課室保護管理者は、保有個人情報（以下、本条から第23条及び第25条から第29条において情報システムで取り扱うものに限る。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

2. When taking security measures described in the preceding paragraph, the Sectional Personal Information Protection Manager shall initiate any rules for the management of passwords, etc. (including regular and as-necessary reviews) and take any required security measures in order to prevent the theft of passwords, etc.

   課室保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

Article 21. Records Access （アクセス記録）

1. The Sectional Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, enact such measures as may be necessary to record access to personal information, retain access records for a predetermined period of time, and regularly audit access records.

   課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期に又は随時に分析するために必要な措置を講ずるものとする。

2. The Sectional Personal Information Protection Manager shall take any necessary measures to prevent the unauthorized modification, theft, or unauthorized destruction of access records.

   課室保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずるものとする。

Article 22. Prevention of Unauthorized External Access （外部からの不正アクセスの防止）

The Sectional Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, take such measures as

may be necessary to prevent unauthorized external access to IT systems handling personal information (e.g. firewall establishment to control access pathways).
課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずるものとする。

Article 23. Computer Virus, Unauthorized Disclosure Prevention, etc. （コンピュータウイルスによる漏えい等の防止）

The Sectional Personal Information Protection Manager shall take such measures as may be necessary to prevent the infection of IT system by computer virus, thereby preventing the unauthorized disclosure, loss, and/or damage of personal information by computer viruses.
課室保護管理者は、コンピュータウイルスによる保有個人情報の漏えい、滅失又はき損の防止のため、コンピュータウイルスの感染防止等に必要な措置を講ずるものとする。

Article 24. Encryption （暗号化）

The Sectional Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, take necessary security measures to encrypt personal information.
課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずるものとする。

Article 25. Information Verification, etc. （入力情報の照合等）

Staff members shall verify input against original copies, as warranted by the importance of retained personal information handled by information systems, in order to confirm the content of personal information before and after processing, and verify, etc. the integrity of existing personal information.
職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行うものとする。

Article 26. Personal Information Backup （バックアップ）

The Sectional Personal Information Protection Manager shall, as warranted by the importance of retained personal information, take necessary security measures to create and provide decentralized storage of personal information backups.
課室保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずるものとする。

Article 27. IT System Design Documents Management, etc. （情報システム設計書

等の管理）

The Sectional Personal Information Protection Manager shall take necessary security measures to store, copy and destroy, etc. IT system design documents, schematic diagrams, and other documentation for information systems related to personal information.

課室保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

Article 28. Personal Information Terminals （端末の限定）

The Sectional Personal Information Protection Manager shall, as warranted by the confidentiality and nature of retained personal information, take necessary security measures to restrict terminals at which retained information may be accessed.

課室保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずるものとする。

Article 29. Terminal Theft Prevention, etc. （端末の盗難防止等）

1. The Sectional Personal Information Protection Manager shall take necessary security measures to prevent the theft and/or loss of terminals.
   課室保護管理者は、端末の盗難又は紛失の防止のため、必要に応じ、端末の固定、執務室の施錠等の措置を講ずるものとする。
2. Staff members shall not remove terminals from the Corporation premises or bring in terminals from outside except when deemed necessary by the Sectional Personal Information Protection Manager.
   職員は、課室保護管理者が必要あると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

Article 30. Third Party Viewing Prevention （第三者の閲覧防止）

Staff members shall take necessary security measures to prevent the viewing of personal information by third parties when terminals are used (guidelines for logging off IT systems)

職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

Chapter 5. Server Room Security, etc.
第５章　電子計算機室等の安全管理

Article 31. Access Management （入退室の管理）

1. The Sectional Personal Information Protection Manager shall authorize persons to enter the core server room in which equipment handling personal information is located (hereinafter, the “Server Room, etc.”) and take necessary security measures confirm purpose, log room access, identity, and ensure that staff members are present when outsiders are granted access. If other media storage contains personal information, similar measures shall be taken when deemed necessary.
   課室保護管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室等（以下「電子計算機室等」という。）に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずるものとする。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずるものとする。
2. The Sectional Personal Information Protection Manager shall, when deemed necessary, simplify the management of server room access by identifying Server Room, etc. entrances and exits and restricting location signs.
   課室保護管理者は、必要があると認めるときは、電子計算機室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずるものとする。
3. The Sectional Personal Information Protection Manager may enact security measures to manage access to the Server Room, etc. and storage facilities (installing access Authentication Functions and formulating rules for the management of passwords, etc.; including regular and as-necessary reviews) and take such measures as to prevent the theft of passwords, etc.
   課室保護管理者は、電子計算機室等及び保管施設の入退室の管理について、必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

Article 32. Server Room, etc. Management　（電子計算機室等の管理）

1. The Sectional Personal Information Protection Manager shall take security measures as may be necessary to prevent unauthorized intrusions (providing locks, alarms, and monitoring equipment for the Server Room, etc.)
   課室保護管理者は、外部からの不正な侵入に備え、電子計算機室等に施錠装置、警報装置、監視設備の設置等の措置を講ずるものとする。
2. The Sectional Personal Information Protection Manager shall take preventative measures against natural disaster, etc. by providing the Server Room, etc. with anti-seismic, fireproofing, smoke proofing and waterproofing equipment, ensuring reserve power supplies for servers/other equipment and prevent damage to wiring.
   課室保護管理者は、災害等に備え、電子計算機室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等

の措置を講ずるものとする。

Chapter 6. Personal Information and Operation Outsourcing
第６章　保有個人情報の提供及び業務の委託等

Article 33. Personal Information Provisions　（保有個人情報の提供）

1. When providing personal information to outside parties other than administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, subparagraphs 3 and 4 of the Law, the Sectional Personal Information Protection Manager shall document the party receiving information by specifying the purpose of use, the legal rationale for the work in which used, the scope and content of usage records and the form of use, etc.
   課室保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わすものとする。
2. When providing personal information to outside parties other than administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, subparagraphs 3 and 4 of the Law, the Sectional Personal Information Protection Manager shall require the enactment of security measures and shall, when deemed necessary, perform on-site inspections prior to provision and periodically thereafter to confirm the status of measures, record findings and seek improvements, etc.
   課室保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講ずるものとする。
3. When providing personal information to administrative agencies and independent administrative institutions pursuant to Article 9, Paragraph 2, Subparagraph 3 of the Law, the Sectional Personal Information Protection Manager shall, when deemed necessary, take the measures as set forth in the preceding two paragraphs.

Article 34. Operations Outsourcing, etc.　（業務の委託等）

1. When outsourcing operations related to the handling of retained personal information, all necessary security measures shall be taken to avoid selection of parties lacking the capacity to appropriately manage personal information. Contracts shall contain explicit stipulations of the following matters, written

documents shall also be obtained confirming the manager, and other aspects of the management system and the matters related to inspection of personal information management at the outsourcer: 保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じなければならない。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者等の管理体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認するものとする。

(1) Obligations to protect the confidentiality of personal information
個人情報に関する秘密保持等の義務

(2) Restrictions and/or conditions on re-outsourcing
再委託の制限又は条件に関する事項

(3) Restrictions on copying, etc. of personal information
個人情報の複製等の制限に関する事項

(4) Response to unauthorized disclosure or other incident involving personal information
個人情報の漏えい等の事案の発生時における対応に関する事項

(5) Destruction of personal information and return of digital media at the conclusion of outsourcing
委託終了時における個人情報の消去及び媒体の返却に関する事項

(6) Contract cancellation procedures and other necessary measures in the event of violations
違反した場合における契約解除の措置その他必要な事項

2. When temporary staffs handle personal information, temporary staff referral contracts shall contain explicit provisions regarding the confidentiality obligations and other aspects of the handling of personal information.
保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

Chapter 7. Security Issue Responses
第７章　安全確保上の問題への対応

Article 35. Incident Reporting, Recurrence Prevention Measures, etc.　（事案の報告及び再発防止措置）

1. In the event of unauthorized disclosure or other incidents that pose security problems for personal information, staff members shall, upon learning of the incident, immediately report to the Sectional Personal Information Protection Manager and Personal Information Protection Officer responsible for the management of the personal information.
保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実

を知った職員は、速やかに当該保有個人情報を管理する課室保護管理者及び保護担当者に報告する。

2. The Sectional Personal Information Protection Manager shall take necessary measures to prevent the expansion of damage and incident recovery.
課室保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。
3. The Sectional Personal Information Protection Manager shall identify the chain-of-events leading to the incident and the extent of damage, etc. and shall report in a timely manner to the Departmental Personal Information Protection Manager, Personal Information Systems Manager, and Assistant General Manager for Personal Information Protection. However, incidents deemed particularly serious shall be immediately reported to the General Manager for Personal Information Protection.
課室保護管理者は、事案の発生した経緯、被害状況等を把握し、速やかに部室保護管理者、個人情報システム管理者及び副総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。
4. Upon receiving reports as set forth in the preceding paragraph, the Personal Information Systems Manager shall immediately report to the General Manager for Personal Information Protection and to the Departmental Personal Information Protection Manager and Sectional Personal Information Protection Manager for all other organizations relevant to the incident (excluding the organization in which the incident occurred).
前項による報告を受けた個人情報システム管理者は、速やかに総括保護管理者、その他事案に関係する組織（事案の発生した組織を除く。）の部室保護管理者及び課室保護管理者に通報する。
5. Upon receiving reports pursuant to the preceding two paragraphs, the General Manager for Personal Information Protection shall report the nature, history and damage, etc. of the incident to the President and in a timely manner as warranted by the nature of the incident.
総括保護管理者は、前ニ項に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を理事長に速やかに報告する。
6. The Sectional Personal Information Protection Manager shall analyze the factors resulting in the incident and shall take such measures to prevent further recurrence.
課室保護管理者は、事案の発生した原因を分析し、再発防止のために　必要な措置を講じなければならない。

Article 36. Public Announcement, etc.　（公表等）

The President shall, as warranted by the nature and impact, etc. of the incident,

publicly announce the facts of the incident and measures to prevent recurrence, and determine responses, etc. to persons whose information was involved in the incident.
理事長が必要があると認めるときは、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずるものとする。

Chapter 8. Inspection and Audit
第８章　点検及び監査の実施

Article 37. Inspection （点検）
The Sectional Personal Information Protection Manager shall inspect on a regular and as-necessary basis the digital recording media, processing channels and storage methods, etc. for personal information under his/her responsibility and shall report findings to the General Manager for Personal Information Protection.
課室保護管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告するものとする。

Article 38. Audit （監査）
The Personal Information Protection Auditor shall perform regular and as-necessary audits of the management of personal information and shall report findings to the General Manager for Personal Information Protection.
監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査を行い、その結果を総括保護管理者に報告する。

Article 39. Evaluation and Review （評価及び見直し）
Measures for the appropriate management of personal information shall be evaluated in response to inspection and audit findings, etc. and, when deemed necessary, shall be reviewed.
保有個人情報の適切な管理のための措置については、点検又は監査の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

Chapter 9. Miscellaneous
第９章　雑則

Article 40. Other Provisions （細則等の定め）

1. Necessary matters related to the clerical processing of and fees for requests for disclosure, requests for amendment and requests for suspension of use, etc. shall be specified separately.
   開示請求、訂正請求、利用停止請求等の事務処理及び手数料等に関し必要な事項は、別に定める。
2. In addition to these Regulations and the provisions set forth in the preceding paragraph, the Committee shall formulate necessary matters for the clerical processing of personal information.
   本規程及び前項に規定する定めのほか、個人情報保護の事務処理に必要な事項は、委員会が定めるものとする。

Supplementary Provisions (Regulations No.001 of 2006)

附　則（平成１８年規程第００１号）

These Regulations shall come into force from April 1, 2006

この規程は、平成１８年４月１日から施行する。

Supplementary Provisions (Regulations No.17 of 2010)

附　則（平成２２年規程第１７号）

These Regulations shall come into force from April 1, 2010

この規程は、平成２２年４月１日から施行する。