○国立大学法人お茶の水女子大学情報セキュリティポリシー

（平成16年7月28日制定）

1　基本理念と方針

国立大学法人お茶の水女子大学（以下「本学」という。）は、その使命である教育と研究を達成し、社会貢献を行うために、多くの情報を資産として保有し、これを日々活用し、また、新たに生成、収集、加工及び発信している。これらの活動を支えるためには、安全で安定した情報セキュリティ基盤の確立・維持が不可欠である。

本学の各組織及び構成員は、情報資産及びその取扱いの重要性を認識し、利便性の追及だけではなく、情報セキュリティを確保する責任と義務を自覚し、情報セキュリティ関連諸法規、条約、並びに本学が定める規約等を遵守しなければならない。

上記の理念に基づき、情報セキュリティ対策のための組織と体制及び情報資産の適正な管理・運用を明確化することによって、本学の情報セキュリティ対策の統一的な基準を示し、さらには、事故時における迅速で適切な対応を図るため、国立大学法人お茶の水女子大学情報セキュリティポリシー（以下「ポリシー」という。）を定める。

ポリシーは、本学の情報資産を利用するすべての構成員に周知され、遵守されなければならない。また、ポリシーの遵守状況を定期的に点検し、改善を行うとともに、必要に応じてポリシーの見直しを行い、本学の情報セキュリティの安定した維持を目指す。

(1) 対象範囲と対象者

ポリシーの対象範囲は､以下に掲げる本学の有するすべての情報資産とする。

- 本学で扱うすべての情報（本学において作成、又は取得した文書、図画及び電磁的記録）
- ネットワーク、情報システム、これらに関連する機器及び設備（一時的に接続するものも含む）
- その他、本学が情報資産と認めるもの

また、ポリシーの対象者は、常勤、非常勤を問わず、役員、教員、職員、学生、研究生、聴講生、附属学校生徒等の大学・附属学校の全構成員（以下「全構成員」という。） 並びに本学の情報資産を使用する委託業者及び来学者等（以下「第三者」という。） とする。

(2) 用語の定義

用語の定義は、「政府機関の情報セキュリティ対策のための統一基準」、「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5月30日法律第59号） 」、及び、「ISO/IEC 27001:2005 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」にあるものと同様とする。

(3) 情報の格付けの区分及び取扱制限

本学で扱う情報資産を適正に運用するため、当該情報の重要性に応じた情報の格付けの区分及びその格付けの区分に応じた取扱制限について定める。また、本学で扱うすべての情報資産は、これらの区分及び制限に従って適正に管理する。

(4) 情報セキュリティ関連規定の体系

情報セキュリティ関連規定の体系は、情報セキュリティ対策における基本的な方針を定めた「ポリシー」、このポリシーに基づき情報セキュリティ対策の実施基準について定めた「実施規程」、及び、この実施規程を具体的な手順に展開して個別の実施事項を定めた「実施手順」から成る。全構成員は、これらの情報セキュリティ関連規定とともに、情報セキュリティ関連諸法規、条約、並びに本学が定める規約等について遵守しなければならない。

2　情報セキュリティ対策のための組織と体制

(1) 組織の構成

本学に最高情報会議を置く。最高情報会議は、全学の情報資産のセキュリティに関する総括的な意思決定と、学内及び学外に対する責任を負う。また、最高情報会議は情報資産の適正な運用に必要な措置を講ずるとともに、ポリシーを全構成員に周知し、教育を行う。また、このために必要な組織の設置を命じることができる。

(2) 役割と権限

① 情報管理総括責任者

情報管理総括責任者は、当該情報資産の管理を総括し責任を負う。緊急時にはあらゆる所管を越えて緊急措置を取る権限を持つ。

② 所管情報管理統括者

所管情報管理統括者は、当該所管における情報資産の管理を統括する。緊急時には当該所管に対して緊急措置を取る権限を持つ。

③ 所管情報管理者

当該所管において、情報資産を取り扱うすべての者は所管情報管理者であり、当該情報資産を管理する責任を負う。

3 情報セキュリティ基本対策

最高情報会議は、全構成員にポリシーの周知と教育を行う。そして、全学の情報資産を適正に管理・運用するため、また、同資産の盗難・流出・改ざん・紛失・不正行為・不正利用・破損等を阻止するため、以下の情報セキュリティ基本対策を実施する。

(1) 情報資産の取扱い

① 本学の業務等以外における取扱いの制限

本学の教育、研究及び業務（以下「本学の業務等」という。） 以外の目的で、情報又は情報資産を作成、利用、保存、移送、保護、提供及び消去してはならない。さらに、要保護情報については、本学の業務等以外の目的で、学外に持ち出し、放置、複製及び配付をしてはならない。移送する場合は、安全確保に留意して、送信又は運搬のいずれによるかを選択し所管情報管理統括者に届け出る。また、電磁的記録を提供する場合は、当該情報資産の付加情報等から不用意な情報漏えいを防止するための措置を講ずる。

② 情報の格付け区分及び取扱制限の遵守

本学の業務等を行う上で、情報又は情報資産を作成、利用、保存、移送、保護、提供及び消去する場合は、情報の格付け区分及び取扱制限を明示し、それに従って適正に管理する。また、情報資産を提供する場合は、提供先に対して当該情報資産に付された情報の格付け区分及び取扱制限に従って適正

に管理をすることを指示する。

③　廃棄時の情報の抹消

要機密情報を廃棄する場合は、すべての情報を復元が不可能な状態にしなければならない。

(2) 物理的セキュリティ

①　安全区域

要保護情報を取り扱う場合は、必要に応じて当該情報資産を他のものから隔離し、安全区域内で保管する。安全区域は、立入り及び退出を管理するための措置を講ずる。また、すべての者の安全区域への立入り及び退出を記録し、監視するための措置を講ずる。また、安全区域から情報資産の盗難、不正な持出し及び持込みを防止するための措置を講ずる。安全区域の物理的な場所は、所管情報管理者以外に公開してはならない。なお、安全区域での保管をしていない情報資産に対しても、情報の格付け区分に応じて、盗難及び学外への不正な持出しを防止するための措置を講ずる。

②　配線の防護

要保護情報を取り扱う情報システムについては、必要に応じてその電源ケーブル、通信ケーブルを含む配線を損傷及び盗聴を含む脅威から保護するための措置を講ずる。

③　冗長化

要安定情報を取り扱う情報システムについては、必要に応じてサービス提供に必要な装置を冗長構成にする。

④　情報のバックアップ

要保全情報を取り扱う情報場合は、運用状態を復元するために必要な措置を講ずる。また、当該情報をバックアップした媒体は適正に保管しなければならない。

(3) 人的セキュリティ

①　全構成員の責任及び義務の自覚

全構成員は、情報セキュリティに関して被害者にもなり得るし加害者にもなり得ることを自覚しなければならない。また、そのいずれにもならないために､全構成員の情報セキュリティ基盤維持に対する責任及び義務を自覚し、

そのための知識及び技能の習得に努めなければならない。

② 第三者による情報資源の利用及びその監督

第三者が本学の情報資産を利用する場合は、全構成員は、ポリシーの遵守義務を第三者に周知し、監督をしなければならない。外部委託の際は、受託者の技術的能力、信頼性の評価を十分に行い、必要に応じて、秘密保持に関する契約を結ぶ。

③ 異動、退職及び退学時の手続き

異動、退職及び退学等の理由により、本学における立場の変更又は本学からの離脱があった場合は、保有している情報資産のうち、本学が返却不要と定めるものを除くすべてのものについて返却を行う。所管情報管理者は、すみやかに当該主体認証情報及びその権限の見直し、削除又は停止を行う。

④ 要員の確保

情報セキュリティは常に維持する必要があるため、安定を要する情報システムを運用する場合は、必要に応じてそのための要員を確保することを原則とする。

(4) 技術的セキュリティ

① 主体認証

要保護情報を取り扱う場合は、主体認証を行う。

② アクセス制御

要保護情報を取り扱う場合は、必要に応じてアクセス制御を行う。

③ 証跡管理

要保護情報を取り扱う場合は、証跡管理のための証跡を取得し一定期間保管する。また、定期的にそれを監視・分析する。

④ 暗号化と署名の付与

要機密情報を取り扱う場合は、必要に応じて暗号化を行う。

また、真正性を要する情報を取り扱う場合は、必要に応じて署名を付与する。

⑤ 不正プログラム感染防止

全構成員は、各自の管理する電子計算機に対し、ウイルス対策ソフト等の導入により、不正プログラムの感染防止を行う。

⑥ 情報システムの保守

所管情報管理者は、当該所管の情報システムに関する不具合、脆弱性が公表された場合は迅速に対処する。

⑦　不正アクセス防止

要保護情報を取り扱う情報システムについては、必要に応じてフィルタリング、侵入監視・検知・防御等の不正アクセス対策を行う。

⑧　学外の情報セキュリティ水準低下の防止

情報管理総括責任者は、学外の情報セキュリティ水準の低下を招く行為を防止するための措置を講ずる。

(5) 違反と例外措置

①　違反措置

情報管理総括責任者は、ポリシーに対する重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、被害の拡大を防ぐとともに、違反者に情報セキュリティの維持に必要な措置を講じさせ、最高情報会議にその旨を報告する。さらに、違反が発生した当該部門の所管情報管理統括者と連携し、これらの事故等を分析し、記録を保存する。また、緊急時にはあらゆる所管を越えて緊急措置をとる権限を持つ。

②　例外措置

ポリシー遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、最高情報会議の許可を得て例外措置を取ることができる。例外措置を取った後は、速やかに最高情報会議に報告する。最高情報会議は、例外措置に係る資料を適切に管理する。

(6) 障害・事故等の対処

本学は、情報セキュリティに関する障害・事故等が発生した場合は、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備する。また、障害・事故等に係る情報については速やかに文部科学省に連絡する。さらに、障害・事故等についての報告手順を整備して全構成員に周知する。全構成員は、障害・事故等の発生を知った場合、報告手順に従い、情報管理総括責任者にその旨を報告する。さらに、情報管理総括責任者は、事故等が発生した当該部門の所管情報管理統括者と連携し、これらの事故等を分析し、記録を保存する。

4　評価と見直し

(1) ポリシー遵守状況等の点検

所管情報管理者は、情報資源の適正な管理・運用及び情報セキュリティの維持・向上に努めるため、当該所管におけるポリシーの遵守状況について定期的に点検を行う。その結果、問題がある場合は、速やかに所管情報管理統括者を経由して最高情報会議に報告し、当該事項の改善を行う。また、全構成員は、最高情報会議が定める年度計画に基づき、毎年度又は必要に応じてポリシー遵守状況の点検を行う。

(2) 監査

最高情報会議は、情報セキュリティ監査責任者を指名してポリシーの遵守状況及び情報資産が適正に管理・運用されているかについて、定期的に又は必要に応じて監査を行わせる。また、情報セキュリティ監査責任者は、監査実施計画を立案し最高情報会議に報告する。そして、監査実施計画に基づき監査を行い、その結果及び改善要望等を最高情報会議に報告等する。最高情報会議は、監査結果等を踏まえ､所管情報管理統括者に対し当該事項への対処を指示する。所管情報管理統括者は、その指示を受けて当該事項への対処を行い、その報告を最高情報会議に行う。

(3) 見直し

最高情報会議は、監査結果等を踏まえ、ポリシーの見直しを行う必要性の有無を検討し、必要があると認めた場合は見直しを行う。

附　則

このポリシーは、平成16年7月28日から施行する。

附　則

このポリシーは、平成22年3月24日から施行する。

附　則

このポリシーは、平成24年2月21日から施行する。

附　則

このポリシーは、平成24年12月12日から施行する。

附　則

このポリシーは、平成25年9月18日から施行する。