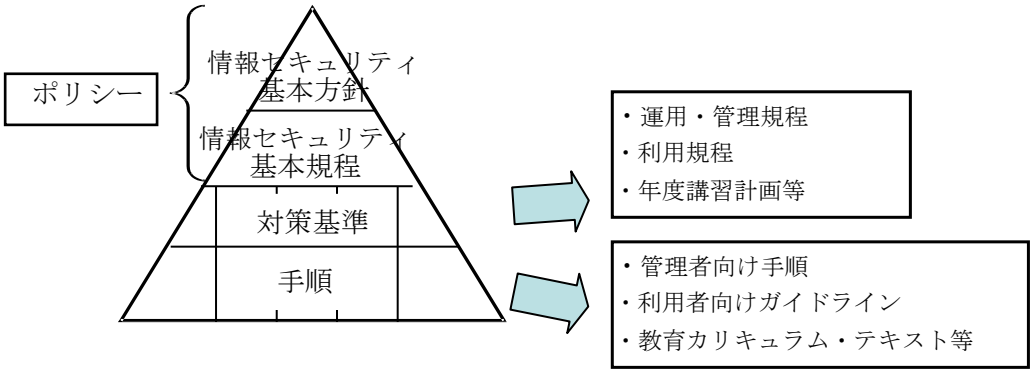
# C1001 情報セキュリティ基本規程

国立大学法人　島根大学

**はじめに**

本学情報セキュリティポリシーは，国立情報学研究所(NII)で公開されている高等教育機関における情報セキュリティポリシーのサンプル規程集を基に策定している。サンプル規程集は，政府機関統一基準を踏まえ，各機関の事情に合わせて作成する際の具体的な参考として役立つよう，大学に適した標準的かつ活用可能な情報セキュリティ規程群を策定されたものである。また，文書番号「C1000」「C1001」及び「C2101」についても，サンプル規程集を踏襲し付与した。




図．島根大学におけるポリシー・対策基準・手順の位置付け

C1001-01　（目的）

第１条　本規程は，国立大学法人島根大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め，もって本学の保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

C1001-02　（適用範囲）

第２条　本規程は，本学情報システムを運用・管理するすべての者，並びに利用者及び臨時利用者に適用する。

C1001-03　（定義）

第３条　本規程において，次の各号に掲げる用語は，それぞれ当該各号の定めるところによる。

１　情報システム

情報処理及び情報ネットワークに係わるシステムで，次のものを言い，本学情報ネットワークに接続する機器を含む。

一 本学により，所有又は管理されているもの

二 本学との契約あるいは他の協定に従って提供されるもの

２　情報

本学すべての教育・研究・診療活動を行う上で必要な情報で，次のものを含む。

一　情報システム内部に記録された情報

二　情報システム外部の機器や電磁的記録媒体等に記録された情報

三　１項一号及び二号の情報で出力された書面に記載された情報及び書面から入力された１項一号及び二号の情報

３　情報資産

　情報システム並びに情報システム内部に記録された情報，情報システム外部の機器や電磁的記録媒体等に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

４　事務情報

　事務情報とは情報のうち次のものをいう。

一　「法人文書の管理に関する規程」の対象となる法人文書

二　一号以外の法人文書で，部局長が指定した文書

５　事務情報システム

　事務情報を扱う情報システムをいう。

６　情報セキュリティポリシー（以下「ポリシー」という。）

　本学が定める「C1000 情報セキュリティ基本方針」及び「C1001 情報セキュリティ基本規程」をいう。

７　対策基準

　ポリシーに基づいて策定される規程及び，基準，計画をいう。

８　手順

　対策基準に基づいて策定される具体的な手順やマニュアル，ガイドラインを指す。

９　利用者

　教職員等及び学生等で，本学情報システムを利用する許可を受けて利用する者をいう。

１０　教職員等

　本学を設置する法人の役員及び，本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他，部局情報セキュリティ責任者が認めた者をいう。

１１　学生等

　本学通則に定める学部学生，大学院学生，研究生，研究員，研修員並びに研究者等，その他，部局情報セキュリティ責任者が認めた者をいう。

１２　臨時利用者

　教職員等及び学生等以外の者で，本学情報システムを臨時に利用する許可を受けて利用するものをいう。

１３　情報セキュリティ

　情報資産の機密性，完全性及び可用性を維持することをいう。

１４　電磁的記録

　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，コンピュータによる情報処理の用に供されるものをいう。

１５　情報セキュリティインシデント

　情報セキュリティに関し，意図的または偶発的に生じる，本学規程または法律に反する事故あるいは事件をいう。

１６　CSIRT（シーサート）

　本学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，本学に設置された体制をいう。Computer Security Incident Response Team の略。

１７　明示等

　情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には，情報ごとに格付を記載することによる明示のほか，当該情報の格付に係る認識が

共通となるその他の措置も含まれる。その他の措置の例としては，特定の情報システムに記録される情報について，その格付を情報システムの規程等に明記するとともに，当該情報システムを利用する全ての者に周知すること等が挙げられる。

C1001-04　（最高情報セキュリティ責任者）

第４条　本学情報システムの運用に責任を持つ者として，本学に最高情報セキュリティ責任者を置く。学長がこれを任命する。

２　最高情報セキュリティ責任者は，ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を行う。

３　最高情報セキュリティ責任者は，全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

４　最高情報セキュリティ責任者は，全学向け教育及び全学情報システムを担当する情報システム管理者向け教育を統括する。

５　最高情報セキュリティ責任者に事故があるときは，最高情報セキュリティ責任者があらかじめ指名する者が，その職務を代行する。

６　最高情報セキュリティ責任者は，原則として，情報セキュリティに関する専門的な知識及び経験を有した専門家を全学情報セキュリティアドバイザーとして置く。

C1001-05　（情報セキュリティ委員会）

第５条　本学の情報セキュリティ確保に関する最終決定機関として，本学に情報セキュリティ委員会を置く。

２　情報セキュリティ委員会は以下を実施する。

一　情報セキュリティ基本方針に関すること。

二　情報セキュリティマネジメントの企画及び計画に関すること。

三　情報セキュリティポリシーの策定，評価及び改訂に関すること。

四　情報セキュリティ教育の推進に関すること。

五　情報セキュリティポリシー遵守状況の把握と改善に関すること。

六　情報システムの新設・更新における情報セキュリティに係る要求仕様に関すること。

七　その他情報セキュリティ事象に関する重要事項に関すること。

C1001-06　（情報セキュリティ委員会の構成員）

第６条　情報セキュリティ委員会の構成員は，島根大学情報セキュリティ委員会規則（平成１６年島大規則第２１３号）に定めるところによる。

C1001-07　（情報セキュリティ委員会の委員長）

第７条　情報セキュリティ委員会の委員長は，最高情報セキュリティ責任者をもって充てる。

２　委員長は，会務を総理する。

C1001-08　（全学情報セキュリティ管理者）

第８条　本学に全学情報セキュリティ管理者を置く。
２　全学情報セキュリティ管理者は，最高情報セキュリティ責任者の指示により，本学情報システムの整備と運用に関し，ポリシー及びそれに基づく規程並びに手順等の実施を行う。
３　全学情報セキュリティ管理者は，情報システムの運用に携わる者及び利用者に対して，情報システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画し，ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。
４　全学情報セキュリティ管理者は，本学の情報システムのセキュリティに関する連絡と通報において本学情報システムを代表する。
５　全学情報セキュリティ管理者は，研究・学術情報機構総合情報処理センター長とする。

C1001-09　（情報セキュリティ監査責任者）
第９条　最高情報セキュリティ責任者は，情報セキュリティ監査責任者を置く。
２　情報セキュリティ監査責任者は，最高情報セキュリティ責任者の指示に基づき，監査に関する事務を統括する。

C1001-10　（部局情報セキュリティ責任者）
第１０条　各部局に部局情報セキュリティ責任者を置く。部局情報セキュリティ責任者は，国立大学法人島根大学個人情報取扱規則　第４条にて定める部局保護責任者とする。
２　部局情報セキュリティ責任者は，部局における運用方針の決定や情報システム上での各種問題に対する処置，部局におけるポリシーの順守状況の把握と周知徹底を担当する。

C1001-11　（部局情報セキュリティ管理者）
第１１条　部局に部局情報セキュリティ管理者を置く。部局情報セキュリティ管理者は，国立大学法人島根大学個人情報取扱規則　第５条にて定める保護管理者とする。
２　部局情報セキュリティ管理者は，部局情報システムの構成の決定や技術的問題に対する処置を担当する。
３　部局情報セキュリティ管理者は，情報セキュリティ管理者に対して，ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

C1001-12　（情報セキュリティ管理者）
第１２条　部局情報セキュリティ管理者は，当該部局の情報システムの管理業務において必要な単位ごとに，情報セキュリティ管理者を置く。情報セキュリティ管理者は部局情報セキュリティ管理者が推挙し部局情報セキュリティ責任者が任命する。なお，部局情報セキュリティ管理者自ら情報セキュリティ管理者を兼務することができる。
２　情報セキュリティ管理者は，部局情報セキュリティ管理者の指示により，部局の情報システムの運用の技術的実務を担当し，利用者への教育を補佐する。

C1001-13　（全学情報セキュリティアドバイザーの設置）
第１３条　最高情報セキュリティ責任者は，情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置き，CSIRT リーダー補佐とする。
２　最高情報セキュリティ責任者は，以下を例とする全学情報セキュリティアドバイザーの業務

内容を定める。
一　本学全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者への助言
二　情報セキュリティ関係規程の整備に係る助言
三　対策基本計画の策定に係る助言
四　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
五　情報システムに係る技術的事項に係る助言
六　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
七　利用者に対する日常的な相談対応
八　情報セキュリティインシデントへの対処の支援
九　前各号に掲げるもののほか，情報セキュリティ対策への助言又は支援

C1001-14　（情報セキュリティインシデントに備えた体制の整備）
第１４条　最高情報セキュリティ責任者は，CSIRT を整備し，その役割を明確化する。
２　最高情報セキュリティ責任者は，教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち，本学における情報セキュリティインシデントに対処するための責任者として CSIRT チームリーダを置く。
３　最高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。

C1001-15　（CSIRT の役割）
第１５条　最高情報セキュリティ責任者は，以下を含む CSIRT の役割を規定する。
一　報告窓口からの情報セキュリティインシデントの報告の受付
二　情報セキュリティインシデントの最高情報セキュリティ責任者等への報告
三　対外的な連絡
四　被害の拡大防止を図るための応急措置の指示又は勧告
２　最高情報セキュリティ責任者は，CSIRT の代表者（PoC（Point of Contact））を置き，CSIRT リーダー補佐とする。

C1001-16　（役割の分離）
第１６条　情報セキュリティ対策の運用において，以下の役割を同じ者が兼務しないこと。
一　承認又は許可事案の申請者とその承認又は許可を行う者（以下，本項において「承認権限者等」という。）
二　監査を受ける者とその監査を実施する者
２　前項の定めに係わらず，教職員等は，承認権限者等が有する職務上の権限等から，当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には，当該承認権限者等の上司に承認等の申請をする。この場合において，当該承認権限者等の上司の承認等を得たときは，当該承認権限者等の承認等を得ることを要しない。
３　教職員等は，前事項の場合において承認等を与えたときは，承認権限者等に係る遵守事項に準じて，措置を講ずる。

C1001-17　（情報の格付け）

第１７条　情報セキュリティ委員会は，情報システムで取り扱う情報について，電磁的記録については機密性，完全性及び可用性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

C1001-18　（情報システム運用の外部委託管理）

第１８条　最高情報セキュリティ責任者は，本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には，当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

C1001-19　（情報セキュリティ監査）

第１９条　情報セキュリティ監査責任者は，情報システムのセキュリティ対策がポリシー（情報システム運用基本方針及び本規程）に基づく手順に従って実施されていることを監査する。

C1001-20　（見直し）

第２０条　本ポリシー，対策基準及び手順を整備した者は，各規程の見直しを行う必要性の有無を適時検討し，必要があると認めた場合にはその見直しを行う。

２　本学情報システムを運用・管理する者，並びに利用者及び臨時利用者は，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う。