C2201 情報システム利用規程

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A2201 | 新規作成（利用規程） | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A2201 | 「情報システム利用規程」として構成等を修正 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2011年3月31日  A2201 | 対象範囲を明確化し、取扱制限事項を追加・変更するとともに条文構成を整理 | 長谷川明生（中京大学） |
| 2013年7月5日  B2201 | 高等教育機関における情報システム利用の実態に合わせた修正 | 長谷川明生（中京大学） |
| 2015年10月9日  C2201 | 文書番号の変更のみ | － |
| 2016年2月5日  C2201 | C2601及びC2603の両規程の新規策定に伴い、整合をとるために全体的な調整を実施 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：この文書は、大学の情報システムのための利用規程の雛形として使われることを想定している。大学の情報システム利用規程の策定では、規程の改変の機会を少なくするように、規程には具体的な記述を記載せず、具体的項目を内規や手順に記載することが一般的である。この雛形の利用に当たっては、この点にも留意してほしい。また、この文書では、情報機器の利用、ウェブブラウザ利用や電子メールの利用および一般利用者向けのウェブ公開基準については、ガイドラインとして作成し強制力を持たせないこととしている。ガイドラインではなく、違反した場合にペナルティを課す手順や内規とする場合には、対応するガイドラインの修正だけでなく対応する条項（C2201-13、C2201-14およびC2201-15）の修正が必要である。  
Ａ大学では、ネットワーク接続の際にも認証が行われるので、利用者全員がアカウント（全学アカウントと呼ぶ）を持つことを想定した規程となっている。学会開催時等の訪問者のネットワーク利用についても臨時の全学アカウント発行が必要とされる。Ａ大学では、このアカウントは管理運営部局（情報メディアセンター）が全学アカウントとして交付している（詳細は第五条を参照）。Ａ大学とアカウント管理体制が異なる場合には、Ａ大学との差異に配慮した利用規程としなければならない。この規程は、PC等の端末やネットワークを利用する際に利用者が守らなければならない一般規定であって、事務情報システムおよび教務・事務用アプリケーションの利用にあたっては、それぞれの利用規程や手順書に従う必要がある。（ただし、手順書部分の改訂は未着手である。）  
現在のひな形の規程は部局や研究室等でシステムを構築、または、ASP、PaaSやクラウド等のアウトソースを考慮していないが、電子メールのアウトソースやクラウドの利用が大学でも進行しており、実際の規程制定では、それらも考慮する必要がある。考慮事項として、アカウント管理の規程との整合性、電子メール等の情報の保全や業者との紛争処理が国内法で対応できるかといったことがあげられる。  
なお、情報システム利用規程の定めに反した行為があった場合に、それに対する懲戒として、学生・職員の所属によるもの（学部長による停学処分など）と情報メディアセンターによるもの（一定期間の利用禁止処分など）の2種類がありうる。前者は、懲戒規程などによって所属部局で対応すべきものであるが、所属によって懲戒の内容に差異が生じないようにするため、あるいは違反行為の認定に専門知識が必要とされる場合に、情報メディアセンターの助言を得ることが望ましい。後者の懲戒について、学生に対する利用制限によって、情報処理演習システムを利用する科目の履修や教務システムを用いる手続きに支障が生じて結果として留年など過度の不利益を招かないよう、教学との関係に対する配慮が必要である。

C2201-01　（目的）

第一条　この規程は、A大学（以下「本学」という。）における情報システムの利用に関する事項を定め、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

解説：この項目では、上記のように、システムやネットワークの利用目的を明示し、規程制定の理由を示す。

C2201-02　（定義）

第二条　この規程において、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。

一　運用基本方針　本学が定める「C1000 情報システム運用基本方針」をいう。

二　運用基本規程　本学が定める「C1001 大学情報システム運用基本規程」をいう。

三　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。

四　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者をいう。

五　利用者等　利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。

六　全学アカウント A大学全学認証基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

七　その他の用語の定義は、運用基本方針及び運用基本規程で定めるところによる。

解説：上記のように、本規程内で引用される手順書等への参照や用語を明確にしておく。

C2201-03　（適用範囲）

第三条　この規程は本学構成員および別途定める手続きにより許可を受けて本学情報システムを利用する者に適用する。

解説：規程の制限が及ぶ範囲を明確にする。研究および教育用に利用する私物の扱いにも留意して規程を整備する必要がある。また、格付けされた情報を格納した情報機器やクラウドストレージも情報システムの対象とし規程の対象とする。  
BYOD機器、パブリッククラウドの個人での利用やASP等の利用についても規程外にならないように制定する必要がある。A大学では、部局や研究室で独自に構築するシステムに適用する規程は部局が準備することになっている。なお、「C3501 各種マニュアル類」は各大学にて策定することを想定した文書であって本サンプル規程集の策定対象外である。研究用の情報システムであっても、成績処理や事務会計処理に使用している場合には事務情報システムとみなされることに注意。本学の公開情報をWeb等により閲覧する行為は本利用規程の範囲外である。

C2201-04　（遵守事項）

第四条　利用者等は、この規程及び本学情報システムの利用に関する手順及び本学個人情報保護規程を遵守しなければならない。

解説：利用に際して、利用手順書や他の規程との関連を記述する。

C2201-05　（全学アカウントの申請）

第五条　本学情報システムを利用する者は、C2603 全学認証基盤アカウント利用規程およびその関連手順に従い、全学アカウントの交付を受けなければならない。

２　来訪者に本学情報システムを臨時的利用させることを目的として全学アカウントの交付を受ける場合、申請者は来訪者に本規程を遵守させなければならない。同目的による全学アカウントの利用が不要になった場合、申請者は速やかに全学実施責任者に届け出なければならない．

解説：Ａ大学では、アカウントの管理方法についての規程は以下のようになる。Ａ大学では、IDとパスワードによる全学統一認証方式を採用し、ネットワークを含めて、全学統一認証に対応した情報システムの利用にあたって全学アカウントを用いている。これは政府機関統一基準の「知識による主体認証情報」に相当する。全学統一認証に対応しないシステムの管理責任者は、それぞれにアカウントの発行のルールを定めて、すべての利用について状況を把握しておかなければならない。研究室のWebやWikiの供用アカウントの管理については、研究教育活動に支障のでないような配慮が必要であろう。  
全学アカウントは、全学実施責任者（管理運営部局のセンター長が相当、「C1001情報システム運用基本規程」のC1001-08（第八条）の解説を参照のこと）から交付を受けなければならない。Ａ大学では、利用の申請と承認は全学情報システム運用委員会が処理をするが、利用承認とアカウント指定を行うのは全学実施責任者なので、申請宛先も全学実施責任者となっている。ただし、実際の処理については、職員と学生についてはほとんど無条件に全学アカウントを発行し、それ以外の者の申請に当たっては関係部局長（来学中に利用する訪問者などの臨時利用者を受け入れた部局の長など）の認印を要件とするなどの申請処理手順を定めておいて、実質的な判断を不要とするものとする。学会等での来訪者のネットワーク利用についても考慮が必要である．  
なお、ネットワークの接続と利用にあたってアカウントが必要な認証ネットワークの場合は、このまま適用可能であるが、ネットワーク接続にオンラインでの認証が不要の場合はアカウント条項にかわる利用開始手順を記述しておく。学外からのインターネットを介しての利用に関しては、大学の実情に合わせて適宜変更する必要がある。  
また、盗聴によるアカウント情報漏洩防止注意するとともにeduroam等の利用を妨げないような規程を考えなければならない。暗号化されたWeb メールサービスを提供することにより、学外からのメールソフトによる電子メールサーバへの直接アクセスを禁止している大学もある。アカウントにはSSHのパスフレーズやワンタイムパスワードのアルゴリズムも含まれる。また、クラウドサービスやアウトソースした場合のアカウント管理についても考慮する必要がある。

C2201-06　（IDとパスワードによる認証の場合）

第六条　利用者等は、全学アカウントの利用に際して次の各号に掲げる事項を遵守しなければならない。

一　利用者等は、全学アカウントを利用して、学外から本学情報システムにアクセスする場合には、定められた手順に従ってアクセスしなければならない。

二　自分の全学アカウントを他者に使用させ、または主体認証情報を他者に開示してはならない。

三　他者の主体認証情報を聞き出し、又は使用してはならない。

四　主体認証情報（パスワード）は、C3255利用者パスワードガイドラインに従って適切に管理しなければならない。

五　利用者は、全学アカウントによる認証接続中の利用者端末において、他の者が無断で画面を閲覧・操作することができないように配慮しなければならない。

六　学外の不特定多数の人が操作（利用）可能な端末を用いて全学アカウントによる認証接続を行ってはならない。

七　全学アカウントを他の者に使用され、またはその危険が発生した際には、直ちに本基盤の運用責任者に届け出なければならない。

八　姓名の変更等識別コードの変更が必要になった際は、遅滞なく本基盤の運用責任者に届け出なければならない。

九　本基盤の利用者の資格を喪失した際又は利用する必要がなくなった際は、別途定める様式により、本基盤の運用責任者に全学アカウント廃止を届け出なければならない。ただし、個別の届出が必要ないと、あらかじめ本基盤の運用責任者が定めている場合は、この限りでない。

十　識別コードもしくは主体認証情報を失念した場合は、別途定める様式により、本基盤の運用責任者に識別コード再交付の申請を行うこととする。

C2201-06-2 （ICカードを用いた認証の場合）

第六条の２　IC カードの交付を受けた利用者は、IC カードの管理について次の各号を遵守しなければならない。

一　IC カードを本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。

二　IC カードを他の者に付与又は貸与したり、他の者のIC カードを使用したりしてはならない。

三　IC カードを紛失しないように管理しなければならない。紛失した際には、直ちにIC カードを発行責任組織にその旨を報告しなければならない。

四　IC カードを利用する必要がなくなった際、又は利用資格がなくなった際には、遅滞なくこれを発行責任組織が定める手続きによりに返納しなければならない。

五　IC カードに記載された券面及び格納された電子証明書の内容が変更される場合には、遅滞なく発行責任組織にその旨を報告しなければならない。

六　運用責任者がICカードに格納した電子証明書を、運用責任者の許可なく削除してはならない。

七　IC カード使用時に利用するPIN は、利用者パスワードガイドラインに準じて適切に管理しなければならない。

２　IC カードについて前項第三号の報告を受けた発行責任組織の長は、直ちに本基盤の運用責任者に報告しなければならない。

解説：上記の規程例は、ICカード等の「所有による主体認証」を利用する場合に、上記規程を置き換えるものである。利用承認の規程も、「パスワードの交付」から「ICカードの貸与」等に変更する必要がある。

C2201-07　（情報機器の利用）

第七条　利用者等は、様々な情報の作成、利用、保存等のための情報機器の利用にあたっては以下の各号に従わなければならない。

一　利用者等は、本学情報ネットワークに新規かつ固定的に情報機器を接続しようとする場合は、事前に接続を行おうとする部局の部局総括責任者に接続の許可を得なければならない。（ただし、情報コンセントや無線LANからあらかじめ指定された方法により本学情報システムに接続する場合はこの限りではない。）

二　利用者等は、一項により許可を受けた情報機器の利用を取りやめる場合には部局総括責任者に届け出なければならない。

三　情報機器において、認証システムおよびログ機能を動作させることが定められている場合には、それらの機能を設定し、動作させなければならない。不正ソフトウェア対策機能が導入されている機器にあっては、その機能が最新の状態でシステムを保護するように努めなければならない。

四　情報機器は既知の脆弱性の影響を被ることのないよう可能な限り最新の状態を保たなければならない。

五　利用者等は、情報漏えいを発生させないように対策し、情報漏えいの防止に努めなければならない。

六　利用者等は、情報機器の紛失および盗難を発生させないように注意しなければならない。

七　情報機器の紛失および盗難が発生した場合は、すみやかに部局技術担当者に届け出なければならない。

八　別途定める「C3251 情報機器取扱ガイドライン」に従い、これらの情報機器の適切な保護に注意しなければならない。

解説：本条で扱う情報機器とは、「C2501 事務情報セキュリティ対策基準」1.3の情報システムに関する定義を満たした上で、大学の備品か利用者の私物かによらず、本学の情報資産を扱うものをいう。スマートフォンやPDAおよびPC機能を持ちネットワークに接続可能な装置等を含む。情報機器の学外利用に際しては、盗難や紛失の他に覗き見等による情報漏えいに注意しなければならない。このような機器の利用について、情報漏えいとともに不正アクセスソフトウェア対策の観点からも考慮しなければならない。

C2201-08　（利用者等による情報セキュリティ対策教育の受講義務）

第八条　利用者等は、毎年度１回は、年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。

２　教職員等は、着任時、異動時に新しい職場等で、本学情報システムの利用に関する教育の受講方法について部局総括責任者に確認しなければならない。

３　教職員等は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、部局総括責任者を通じて、全学実施責任者に報告しなければならない。

（４　利用者等は、情報セキュリティ対策の訓練に参加しなければならない。）

解説：情報セキュリティ教育の受講義務について、規程として明文化した条項である。オンライン教育や講義等を通じて年１回は、すべての利用者がセキュリティ教育を受講することが必要である。情報セキュリティ訓練規程および手順が定められている場合には、訓練参加義務を規定化する。

C2201-09　（情報の取り扱い）

第九条　利用者等は、格付けされた情報について、情報格付け取扱手順（C3103）に従い、文書に明示された方法にしたがって取り扱わなければならない。

解説：C1001-19にしたがってC2103およびC3103が策定され、教職員等はB2103およびC3103に従って文書の格付けし、格付け文書の取り扱いを文書に明示しなければならない。利用者はC3103にあるように文書に明示された方法に従って文書を取り扱う。

本規程の対象としているシステムや機器では、格付けになじまないという考え方もあるが、情報格付け基準で対象外システムを明記しておいて、格付けは包括的に実施するという考え方もあるので、この条項を置いた。なおA大学では学生に情報の格付け権限はない。

C2201-10 （制限事項）

第十条　利用者等が本学情報システムについて以下の各号に定める行為を行おうとする場合には本学実施責任者の許可を受けなければならない。

一　ファイルの自動公衆送信機能を持ったP2Pソフトウェアを教育・研究目的で利用する行為

二　教育・研究目的で不正ソフトウェア類似のコードやセキュリティホール実証コードを作成、所持、使用および配布する行為

三　ネットワーク上の通信を監視する行為

四　本学情報機器の利用情報を取得する行為及び本学情報システムのセキュリティ上の脆弱性を検知する行為

五　本学情報システムの機能を著しく変える可能性のあるシステムの変更

解説：Ａ大学では、構成員による知的財産権侵害と意図せぬ情報漏洩やファイルの流出を防ぐためにファイルの自動公衆送信機能を持ったP2P ソフトウェアの利用を研究教育目的にのみ許可制としている。ここで自動公衆送信とは著作権法での用語であり、自動公衆送信機能を持ったP2P ソフトウェアとは、ファイルを自動的にダウンロードし、またダウンロードしたファイルやファイルの断片を自動的に不特定多数に再送信するような機能を持ったP2Pソフトウェアのことをいう。マルウェア研究に関しても同様の扱いとしている。

C2201-11　（禁止事項）

第十一条　利用者等は、本学情報システムについて、次の各号に定める行為を行ってはならない。

一　当該情報システム及び情報について定められた目的以外の利用

二　指定以外の方法での学外からの全学アカウントを用いての本学情報システムへのアクセス

三　あらかじめ指定されたシステム以外の本学情報システムを本学外の者に利用させる行為

四　守秘義務に違反する行為

五　差別、名誉毀損、侮辱、ハラスメントにあたる行為

六　個人情報やプライバシーを侵害する行為

七　前条に該当しない不正ソフトウェアの作成、所持および配布行為

八　著作権等の財産権を侵害する行為

九　通信の秘密を侵害する行為

十　営業ないし商業を目的とした本学情報システムの利用

解説：本サンプル規程集の「C1001 情報システム運用基本規程」第三条十号「教職員等」の解説にあるように、大学の活動との関連で同窓会、生協、TLO、インキュベーションセンター、地域交流センター、財団などが利用することは想定される。ただし、その利用の目的を大学の教育・研究活動および運営を支援する業務に限定して、営利業務のネットワークを別に用意するとしている大学の例があり、A大学もそのような運用をしている。二項については手順書等で明示。  
ただし、大学施設内の組織や関連事業の営利業務に利用できることを利用規程の定めあるいは全学総括責任者の判断によって認めるような方針もありえる。

十一　過度な負荷等により本学の円滑な情報システムの運用を妨げる行為

十二　不正アクセス禁止法に反する行為、またはこれに類する行為

十三　その他法令に基づく処罰の対象となる行為

十四　上記の行為を助長する行為

解説：利用に際しての禁止条項および制限事項を上記で条文化している。

C2201-12　（違反行為への対処）

第十二条　利用者等の行為が前条に掲げる事項に違反すると被疑される行為と認められたときは、部局総括責任者は速やかに調査を行い、事実を確認するものとする。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。

２　部局総括責任者は、上記の措置を講じたときは、遅滞無く全学総括責任者にその旨を報告しなければならない。

３　調査によって違反行為が判明したときは、部局総括責任者は全学総括責任者を通じて次の各号に掲げる措置を講ずること依頼することができる。

一　当該行為者に対する当該行為の中止命令

二　管理運営部局に対する当該行為に係る情報発信の遮断命令

三　管理運営部局に対する当該行為者のアカウント停止、または削除命令

四　本学懲罰委員会への報告

五　本学学則および就業規則に定める処罰

六　その他法令に基づく措置

解説：前条の禁止規定に明白に違反した場合の対処、処罰について上記のように明示する。一般に、部局総括責任者が処罰可能なのは管轄部局のみで、他学部や管理運営部局に対しては、全学責任者を通じて処罰を依頼するのが自然であろう。

解説：以下（第十三条～十四条）の条文は、利用者が守るべき手順書を示している。

C2201-13　（電子メールの利用）

第十三条　利用者等は、電子メールの利用にあたっては、別途定める「C3252 電子メール利用ガイドライン」に従い、規則の遵守のみならずマナーにも配慮しなければならない。

C2201-14　（ウェブの利用および公開）

第一四条　利用者等は、ウェブの利用およびウェブによる情報公開に際し、以下の各号に従わなければならない。

一　利用者等は、ウェブブラウザを利用したウェブサイトの閲覧、情報の送信、ファイルのダウンロード等を行う際には、「C3253 ウェブブラウザ利用ガイドライン」に従わなければならない。

二　利用者等は、部局情報システム運営委員会に許可を得て、「C3254 情報発信ガイドライン」に従いウェブページを作成し、公開することができる。

三　利用者等は、ウェブサーバを運用し情報を学外へ公開する場合は、事前に部局情報システム運営委員会に申請し、許可を得なければならない。また、ウェブサーバを公開する利用者は、運用期間中、ウェブサーバの脆弱性対策や情報の改ざんに関する点検を定期的に行わなければならない。

四　ウェブページやウェブサーバ運用に関して、規程やガイドラインに違反する行為が認められた場合には、全学実施責任者は公開の許可の取り消しやウェブコンテンツの削除を行うことができる。

C2201-15　（学外からの本学情報システムの利用）

第十五条 利用者等は、学外からの本学情報システムへのアクセスにおいて、以下の各号にしたがわなければならない。

一　利用者等は、学外から全学アカウントを使って本学情報システムへアクセスするには事前に全学実施責任者の許可を得たうえで、指定された方法で利用しなければならない。

二 利用者等は、アクセスに用いる情報システムを許可された者以外に利用させてはならない。

三　利用者等は、全学実施責任者の許可なく、これらの情報システムに要保護情報を複製保持してはならない。

解説：学外へ持ち出した情報機器や、学生、教職員等の自宅PC等、学外の情報システムからの本学ネットワークへの接続や学内システムの利用にあたっては、全学実施責任者の事前許可が必要である。学外との接続方法についてはVPN等情報センターが指定するのが一般的である。  
eduroam等の制約にならないように条文に工夫が必要である。ログおよびアンチウイルス機能に関しては実情に合わせて条文を変更することも可能であるが、証跡管理の点からは好ましくない。ネットカフェ等、情報セキュリティ対策が不十分な情報システムやネットワークからの学内情報システムの利用は情報漏えいのリスクが大きく推奨できない。C2201-07に集約することが可能と思われる。

C2201-16　（安全管理義務）

第十六条　利用者等は、自己の管理する情報機器について、本学情報ネットワークとの接続状況に関わらず、安全性を維持する一次的な担当者となることに留意し、次の各号にしたがって利用しなければならない。

一　ソフトウェアの状態および不正ソフトウェア対策機能を最新に保つこと。

二　不正ソフトウェア対策機能により不正プログラムとして検知されるファイル等を開かないこと。

三　不正ソフトウェア対策機能の自動検査機能を有効にしなければならない。

四　不正ソフトウェア対策機能により定期的にすべての電子ファイルに対して、不正プログラムが存在しないこと確認すること。

五　外部からデータやソフトウェアを情報機器に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正ソフトウェアが存在しないことを確認すること。

六　常に最新のセキュリティ情報に注意し、不正ソフトウェア感染の予防に努めること。

C2201-17 (インシデント対応)

第十七条　利用者等は、本学情報システムの利用に際して、インシデントを発見したときは、「C3102 インシデント対応手順」に従って行動しなければならない。