D3251 情報機器取扱ガイドライン

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  A3201 | 新規作成（PC取扱手順） | 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  A3201 | 「PC取扱ガイドライン」として、書式や表現を見直し | 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  A3201 | 「情報機器ガイドライン」として、対象をPCに限定しないように記述を見直し | 長谷川明生（中京大学） |
| 2015年10月9日  C3251 | 情報機器の利用実態に合わなくなった箇所の修正 | 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 |
| 2017年10月17日  C3251 | 用語をC2103（情報格付け基準）で用いているものに統一 | 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 |
| 2019年12月27日  D3251 | 全面的に見直しして改定 | 長谷川明生（中京大学） |
| 2021年10月16日  D3251 | 在宅勤務向けに追記 | 長谷川明生（中京大学） |

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：D2201（情報システム利用規程）で指定した情報機器の利用手順に関して述べている。ここでいう情報機器とは、利用者が相対して操作する端末等を想定している。学内ネットワークに接続して利用するBYOD機器を含む。

1. 一般利用者向け利用手順

解説：ここでいう一般利用者とは、情報機器を学内ネットワークに接続して利用する者のことである。大学が利用に供している端末を使う利用者も含む。

1.1 利用者は本学のネットワーク機器や端末等の設備を損傷する可能性のある行為および電源等の本学資源の無断使用をしてはならない。

解説：主として大学内の共用スペースに設置する共同利用端末に関して、端末設備を物理的に破損する行為等を禁止する。これら端末を損傷する行為に対する対策は、規定等による対策の他に、管理者による適切な監視体制の整備等も重要である。  
学内には利用者による電源の利用が許可された場所がある。それ以外の場所では無断で電源を使用すべきではない。学外での電源の利用について、許可されていない場所での管理者に無断での機器の充電等は盗電として犯罪になることがある。

1.2 利用者は以下に掲げる行為をはじめとする、他の利用者の利用を妨げる行為をしてはならない。

(a) 共用端末の占有行為。端末をロックして長時間離席する行為も含む。  
ただし、講義等で特に許可された場合を除く。

(b) プリンタ出力の放置、プリンタの紙詰まりや紙切れ、トナー切れを放置する行為。

解説：ここに掲げられている事項の他に、ディスク記憶領域や、計算能力、メモリ等の占有行為の禁止が必要になる場合があるかもしれない。しかし、これらの計算機資源の占有が危惧される場合には、クォータ等、システム側で対応を考えた方がよい。  
また、ライセンス上、同時起動数が制限されているようなアプリケーションを導入している場合は、同様の規定が必要であろう。  
さらに、前項と同様、管理者による監視体制の整備や、プリンタのトラブル等に迅速に対応できる体制作りも重要である。

1.3 利用者は以下に掲げる行為をはじめとするネットワーク帯域を占有する行為をしてはならない。

(a) 教育研究上必然性のないストリーミングサービス等の利用によりネットワーク帯域を占有すること

(b) 大きなデータのやり取り

(c) 高い頻度で問い合わせパケット等を送出するアプリケーションの使用

解説：基本的には、1.2項の規定に含まれるとも考えられるが、場合によっては、広範囲に影響が及ぶため独立した項目としている。「大きなデータ」等の具体値をネットワーク性能等に応じて示す方がよい。オンライン講義等ではネットワーク利用帯域が少なくなるように工夫すること。

1.4 利用者は、情報格付け規定において規定されている要保護情報や、その他重要なデータの取り扱いに関して以下の各号を遵守しなければならない。

(a) 要保護情報を情報機器内部、あるいは外部記憶メディアに保管する場合は、暗号化するものとし、その暗号化鍵を適切に管理すること。  
ただし、暗号化以外に十分な保護対策が採られていると管理者が認める場合はこの限りでない。

(b) 要保護情報を電子メール等を用いて送信する場合は暗号化するものとし、その暗号化鍵は別途安全な手段を用いて送信すること。

(c) 在宅勤務のために備品となる情報機器、あるいは要保護情報を保管した情報機器を持ち出す必要がある場合には、事前に○○に届け出でなければならない。また、持ち出し利用にあたっては要保護情報が流出しないように最善の注意をはらうものとする。

解説：個人情報等、重要な情報の保管、送信時の暗号化の必要性について述べている。(a)の但し書きは、バックアップ用メディア等で、暗号化すると著しく利便性が損なわれるような場合に、メディアを厳重に管理することで暗号化に代えられるとしたもの。

1.5 利用者は、USBメモリ、各種メモリカード等の外部記憶メディアを利用する場合には、以下の各号を遵守しなければならない。

(a) ファイルを保存した外部記憶メディアを放置しないこと。

(b) 放置してある、または出所が定かでない外部記憶メディアを端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、管理者に届け出ること。

(c) 使用済みの外部記憶メディアを譲渡、または廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。ボリューム（外部記憶メディアにおけるデータの格納場所）を暗号化し、暗号化キーを破棄することでも可とする。

解説：外部記憶メディアの内容を自動実行する設定にしている場合には、メディアを挿入するだけでソフトウェアが実行され、悪意のあるソフトウェアがインストールされる可能性に留意すること。  
メディアを廃棄、譲渡する場合は、OS上でファイルを消去しただけでは、記録情報が復元される可能性に注意すること[[1]](#footnote-1)。なお、データ破壊に関しては、「要保護情報等の重要な情報」を記録した外部記憶メディアに対象を限定するという考え方もある。

1.6 利用者は、演習室等、共用スペースに設置してあるPC端末を利用する場合は、設置者の指示に従って利用すること。

1.7 利用者は、以下に掲げる各事項を発見したときは、すみやかに管理者に連絡をするとともに、「インシデント対応手順」に従って行動すること。

(a) 共用端末のOSやアプリケーション、あるいは、大学内に設置されているホストコンピュータやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合。

(b) 大学内の情報機器上で、著作権を侵害しているおそれのあるコンテンツや、機密情報、個人情報等にアクセス可能となっていることを発見した場合。

(c) 大学外のサービス上で、大学の機密情報や、構成員の個人情報等が公開されている、または、大学が権利を有するコンテンツが無断で使用されていることを発見した場合。

(d) 要保護情報流出を発見した場合

解説：ネットワークやPC端末の管理業務をしていない一般利用者であっても本項目に掲げるような脆弱性等を発見した場合に報告させることで、構成員のセキュリティや知的財産に関する意識を向上させるとともに、管理業務の効率化をはかることができる。もちろん、管理側では、これら報告に対処する体制作りが必要である。

1.8 利用者は、大学外のネットワークから大学内の情報システム（不特定多数に公開されているもの（Webサービスなど）を除く）にアクセスする場合は以下の各号を遵守しなければならない。

(a) アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意を払うこと。万一、認証情報が漏洩した場合、またはその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。

(b) 信頼性が保障できない端末（ネットカフェの端末等）からの、本学のサービスのうち認証を要求するものへのアクセスは禁止する。

解説：本項は、利用者が、大学内のPC端末やゲートウェイサーバ等にリモートアクセス可能な場合に必要な規定である。リモートアクセスのための認証情報が漏洩した場合には、深刻な被害をもたらす可能性が高いことを利用者が十分に理解していることが大切である。

2. 特権利用者向け利用手順

解説：特権利用者は、PC端末を管理する権限を持つ特権利用者（Windows®であればAdministrator、UNIX®であればrootに代表される管理者アカウントの利用者）を指している。具体的には、演習室や図書館等に設置されているPC端末を管理するセンター職員や、個人でPC端末を管理する教員や事務職員、研究室に導入されているPC端末を管理する大学院生等が含まれる。学生等の私物PCを学内ネットワークに接続することを許可している場合は、その私物PCの所有者も含まれる。

2.1 特権利用者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、以下に掲げる規定を遵守しなければならない。

(a) 利用しているOS、アプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。

(b) ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

解説：主として利用されるOS、アプリケーションに関しては、具体的なチェック方法、修正方法を示しておくことが望ましい。  
また、ウイルス対策ソフトウェアをサイトライセンスにより導入している場合、学内からのみデータベースの更新が可能な場合がある。この場合、休暇中等に自宅で感染してしまう可能性があるので注意が必要。場合によっては検疫ネットワークの導入等も検討する。

2.2 特権利用者は、自らが管理する端末に、アプリケーションをインストールし、利用する際には、以下に掲げる規定を遵守しなければならない。ただし、研究・教育目的およびそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合にはこの限りでない。

(a) ネットワーク帯域を極度に圧迫するアプリケーションをインストール、利用してはならない。

(b) 自端末宛以外のパケットを傍受するアプリケーション（パケットスニファ）をインストール、利用してはならない。

(c) P2Pファイル交換ソフトウェアをインストール、利用してはならない。

(d) その他、情報システム利用規程、その他の本学ネットワークの利用に係わる規定等に反するネットワークアプリケーションをインストール、利用してはならない。

解説：主にネットワークに関連するアプリケーションのインストールについて規定している。(a)ではネットワーク資源の浪費、(b)では通信の秘密、(c)では著作権侵害等に関して問題が生じそうなアプリケーションを原則禁止している。大学の実態に応じて、これらの問題に関する教育を十分に行った上で、届出制等の形で利用を認めることも考えられる。  
なお、情報システム利用規程の関連規定についても参照のこと。

2.3.特権利用者は、自らが管理する端末に関して、以下の各規定を遵守すること。

(a) 利用者が当該端末を認証なしで利用できるようにしてはならない。  
端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。  
アカウントの発行状況や利用状況（利用者識別の設定できないシステムにあっては、利用状況が把握できるもの）について部局責任者に定期的に報告すること。

(b) ネットワークを経由して、不特定多数の第三者が端末にアクセスできないようにすること。

(c) 当該端末にアカウントを有さない者に端末を使用させないこと。  
ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。

(d) サーバの管理端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとること。共用端末にあっては、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。

(e) 移動可能な端末においては、短時間であっても端末を放置しないこと。  
保管時は施錠可能な場所に保管すること。

(f) 端末が管理権限をもたない者によって、DVD、USBメモリやネットワーク等を用いて起動されないように設定すること。

解説：端末にDVDやUSBメモリ等の外部記憶メディアを接続し、その外部記憶メディアから起動したり、ネットワーク上の他の機器に接続させて起動したりして、当該端末の認証機能を回避して起動することにより、サーバや当該端末の内蔵記憶ディスクにアクセスすることができる場合がある。それらへのアクセスを防ぐため、特権利用者が意図したメディア以外から起動できないようにする必要がある。そのために、BIOSで当該メディア以外から起動できないように設定した上で、BOISパスワードを設定したり、UEFIで当該メディア以外から起動できないように設定する等の対策をすること。

(g) 端末を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要保護情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

解説：PC端末への許可されていない者のアクセスや端末機器自体の盗難等を防止するための規定である。(f)は、管理者権限を有さない利用者が管理者権限を得る危険性を排除するためである。(g)は、1.5項(c)と同様に、PC端末から重要情報や認証情報が漏洩する危険性を排除するためである。リースおよびレンタルの機器に関してはデータの完全削除をソフトウェア的に実施すること。なお、データ破壊に関しては、「要保護情報等の重要な情報」を記録した端末に対象を限定するという考え方もある。

2.4 特権利用者は、自らが管理する情報機器に関して、利用者が大学外のネットワークから当該端末にアクセスできるようにする場合は、以下の各規定を遵守すること。

(a) アクセスに使用するポート番号、VPNソフトウェア名等をセンターに届け出ること。

(b) 通信内容は全て暗号化されるようにすること。

(c) パスワードのみ（ワンタイムパスワードを除く）による認証方式は原則として避けること。

(d) 特権アカウント（rootなど）によるリモートアクセスは原則として行えないように設定すること。

(e) 大学が提供するネットワーク以外（電話回線など）の方法でアクセスできるようにしてはならない。教育・研究目的等で、特に必要な場合には、センターの許可を得ること。

解説：1.8項の規定に加えて、特権利用者が、VPNサーバソフトウェア等をインストール、運用する場合の注意点を述べている。  
(c)は、通信が暗号化されていても、認証パスワードが脆弱であれば不正侵入を許してしまう可能性を考慮したもの。

2.5 特権利用者は、自らが管理する情報機器を対象として実施される情報セキュリティ監査に対して、必要な協力を行うこと。

1. メモリカードの廃棄・譲渡時における内部のデータ消去に関するユーザ向けガイドラインhttp://home.jeita.or.jp/page\_file/20120906151218\_mfFqh0cvox.pdf [↑](#footnote-ref-1)