

大阪大学人間科学研究科 / 人間科学部

ネットワーク利用者ガイドライン

ネットワーク運用管理ガイドライン

目次

ネットワーク利用者ガイドライン 1

1. ネットワークを快適に利用するために 2
2. ネットワーク利用の目的 4
3. 定義 4
4. 本研究科 / 学部ネットワーク・ODIN と、学外ネットワーク 4
5. ネットワークの利用にあたって避けるべき行為 5
6. ネットワーク利用上の注意 8

ネットワーク運用管理ガイドライン 10

- 1 はじめに 11
- 2 基本事項 11
- 3 定義 11
- 4 本研究科 / 学部ネットワーク運用管理基本方針 11
- 5 情報コンテンツ 13
- 6 セキュリティインシデントが発生した場合 13
- 7 個人情報保護 13

ネットワーク利用者ガイドライン

1. ネットワークを快適に利用するために

人間科学研究科 / 人間科学部内ネットワークの快適な利用のために、利用に当たっては以下の行為を避けてください。これらの行為をした場合、警告、利用制限、利用者氏名や処分の公表などの措置をとることがあります。

①法令又は公序良俗に反する行為

(→ P. 5)

- ・ 基本的人権の侵害
- ・ 差別的表現のネットワーク上での公開
- ・ 誹謗中傷を行うこと
- ・ プライバシーの侵害
- ・ 利用資格のないコンピュータや通信機器への侵入
- ・ 知的財産権の侵害
- ・ わいせつなデータの公開
- ・ 利用権限の不正使用
- ・ ストーカ行為及び嫌がらせ行為、など。

②本学の教育・研究目的に反する行為

(→ P. 7)

- ・ 政治・宗教活動
- ・ 営利を目的とした活動
- ・ 教育・研究の目的外のデータの保持、など。

③ネットワークの円滑な利用を妨げる行為

(→ P. 7)

- ・ 通信機器の配線及び周辺機器の接続構成 の変更
- ・ ネットワークのソフトウェア構成の変更
- ・ ネットワークの正常な機能を損なうようなソフトウェアの導入や利用
- ・ 大量のファイルを一度に送受信すること、など。

また左記以外にも、次のようなことに注意してください。

- (1) 品位をもって利用する
- (2) 他人を思いやって利用する
- (3) パスワードを適正に管理する
- (4) プライバシーを守る
- (5) ネットワークのセキュリティ保持に協力する
- (6) ネチケットを守る

(→ P. 8 ～ 9)

その他、以下に示す目的や利用上の注意にしたがって、みんなが快適に利用できるネットワークの運営、維持にご協力をよろしくお願いします。



2. ネットワーク利用の目的

人間科学研究科 / 人間科学部内ネットワーク（以下「本研究科 / 学部ネットワーク」という。）は、大阪大学総合情報通信システム（ODINS: Osaka Daigaku Information Network System）の一部です。本研究科 / 学部ネットワークを利用する教職員、学生及びこれらに準ずる者（以下「利用者」という。）は、大阪大学の財産である ODINS および本研究科 / 学部ネットワークの円滑な運用の維持に協力しなければなりません。また ODINS で提供されているコンピュータネットワークおよびそれに接続されているすべてのコンピュータ・通信機器、および、それらの上で動作する通信ソフトウェアといった設備は、教育・研究を目的としています。教育研究を通じて、学術社会のみならず産業社会、市民社会、さらには地域社会に貢献できるように利用しなければなりません。

大阪大学人間科学研究科 / 人間科学部内ネットワーク利用者ガイドライン（以下「本ガイドライン」という。）は、大阪大学総合情報通信システム運用管理要項の第7に基づいて、利用者が上記の目的をよく理解し、ODINS および本研究科 / 学部ネットワークの目的を効果的に達成できるように、利用上の注意事項をまとめたものです。なお原則として本ガイドラインは、大阪大学総合情報通信システム運用管理者ガイドライン等に従うものとします。



3. 定義

ODINS とは、Osaka Daigaku Information Network System の略で、学外ネットワークと接続するため、及び部局ネットワークを構成するため設置されたすべてのコンピュータ、通信機器及びそれらの上で動作する通信ソフトウェア群によって構成されるシステムをいいます。人間科学研究科 / 人間科学部ネットワーク（以下「本研究科 / 学部ネットワーク」という。）とは、人間科学研究科 / 人間科学部（以下「本研究科 / 学部」という。）によって個別に運用管理されているネットワークをいいます。

4. 本研究科 / 学部ネットワーク・ODIN と、学外ネットワーク

本研究科 / 学部ネットワークを通じた学外との通信は、ODINS と広域通信ネットワークとの相互接続によって行われています。広域通信ネットワークは、学術目的のネットワークのみならず商用目的のネットワークなども相互に接続されており、それぞれのネットワークの規模や性能も様々です。例えば、米国の大学の Web サイト（いわゆるホームページ）を見るためには、いくつかのネットワークを経由してデータが送受信されます。学外のネットワークは ODINS および本研究科 / 学部ネットワーク内部に比べて通信容量が小さいことを覚えておいてください。すなわち同じデータ量を送受信しても、通信容量の小さいネットワークにかかる負担は、ODINS および本研究科 / 学部ネットワークにかかる負担より大きくなります。したがって、無用の大量のデータを送受信することはできるだけ避けてください。ODINS および本研究科 / 学部ネットワークを利用すると世界中にアクセスできますが、ネットワークにはそれぞれの運用規則があり、またそれを支える多くの人達がいることを忘れてはなりません。



5. ネットワークの利用にあたって避けるべき行為

ODINS および本研究科 / 学部ネットワークは、物理的にはコンピュータ同士を接続するものですが、接続されているコンピュータを利用するのは人間です。社会常識に従い、相手に対する配慮をもって利用してください。利用に当たっては、以下の行為は避けねばなりません。

法令又は公序良俗に反する行為

本学の教育・研究目的に反する行為

ODINS および本研究科 / 学部ネットワークの円滑な利用を妨げる行為

なお、ODINS および本研究科 / 学部ネットワークではその安全かつ適正な運用のために利用履歴がとられており、本項に反する行為をした場合には、警告、利用制限、所属部局への通報、利用者氏名や処分の公表などの措置をとることがあります。なお利用履歴は、運用管理及び教育上の目的を除いて、当該利用者本人の同意なしに調査しその結果を第三者に公表することはできないものとします。

5.1 法令又は公序良俗に反する行為

ODINS および本研究科 / 学部ネットワークでの行為は治外法権ではありません。日本国内においては日本国内法が適用されます。特に関連の深い法令としては、著作権法などの知的財産権諸法、いわゆる不正アクセス禁止法、刑法、民法、商法などがあります。また、外国に影響を及ぼすときは外国法の適用を受ける可能性があることにも留意せねばなりません。例えば、次のような行為をしてはなりません。また、自ら行わなくても、他人にこれを行わせた場合でも、違法とされることがあります。さらに、法令で定められていなくても、一般社会ではならない行為があります。



(1) 基本的人権の侵害

ネットワークの利用に限らず、基本的人権を尊重しなければなりません。

(2) 差別的表現のネットワーク上での公開

人種・性別・思想信条などに対する差別的な発言をネットワークで公開することは、日本国憲法の定める基本的人権尊重の精神に反することとなります。

(3) 誹謗中傷を行うこと

ネットワークの利用に限ったことではありませんが、他人を誹謗中傷することは名誉毀損で訴えられることがあります。

(4) プライバシーの侵害

ODINS および本研究科 / 学部ネットワーク利用者の個人情報尊重されますが、利用者は他人の個人情報も尊重しなければなりません。個人情報や私信などを無断で公開してはなりません。

(5) 利用資格のないコンピュータや通信機器への侵入

ネットワーク上の利用資格のないコンピュータや通信機器を使用してはなりません。ODINSおよび本研究科/学部ネットワークから他組織のネットワークへ不正に侵入した場合、大阪大学全体が外部のネットワークとの接続を切られるだけでなく、場合によっては国際問題に発展する可能性があります。また、他組織への不正な侵入を試すようなことも絶対にしてはなりません。また、侵入しなくとも、ネットワーク上を流れるデータを読み取るような盗聴行為も絶対にしてはなりません。

(6) 知的財産権の侵害

知的財産権は、人間の知的創作活動について創作者の権利に保護を与えるものです。絵画・小説・ソフトウェアなどの著作物、デザインの意匠などを尊重するよう心がけて下さい。著作物の無断複製や無断改変はしてはなりません。

例えば、本・雑誌・Webページなどに提供されている文章・図・写真・映像・音楽などを、無許可で複製あるいは改変して、自分のWebページで公開したり、ネットニュースに投稿したりしてはいけません。著作権の侵害だけでなく、会社のロゴや商品を示す商標については商法・商標法などの侵害に、芸能人の写真など肖像については肖像権の侵害になることがあります。また、大学が使用許諾契約を結んでいるソフトウェアやデータをコピーしてはなりません。

(7) わいせつなデータの公開

ODINSおよび本研究科/学部ネットワークを用いてわいせつな画像・音声などを公開してはなりません。また、それらへのリンクを提供してはなりません。

(8) 利用権限の不正使用

利用者は、有償無償を問わず、自分の利用権限(アカウント)を他人に使わせてはなりません。利用者は、パスワードを厳格に管理する責任があります。本人のログイン名で他人にコンピュータやネットワークを使用させることも、ファイル格納領域などのネットワーク資源を他人に使わせることもこれに含まれます。また、他人のログイン名でログインすること、及び、他人のログイン名を騙って、電子メール・ネットニュース・電子掲示板を使用してはなりません。

(9) ストーカー行為及び嫌がらせ行為をすること

ネットワークを通じて、相手が嫌がるような内容のメールを一方向的に送るなどの行為や大量のデータを送りつけるなどの行為はしてはなりません。



5.2 教育・研究目的に反する行為

ODINS および本研究科 / 学部ネットワークは教育・研究の円滑な遂行に資するために運用されています。教育、研究及びその支援という設置目的から逸脱する以下のような行為は、利用制限などの処分の対象になることがあります。

(1) 政治・宗教活動

ODINS および本研究科 / 学部ネットワークは大阪大学および人間科学研究科 / 人間科学部の財産ですから、特定の政治・宗教団体に利便を供するような活動に用いてはいけません。

(2) 営利を目的とした活動の禁止

広告・宣伝・販売などの営利活動のために Web ページや電子メールを用いてはなりません。

(3) 目的外のデータの保持

個人のファイル領域や Web ページ領域に、教育・研究の目的に合致しないものを置いてはなりません。

5.3 ネットワークの円滑な運用を妨げる行為

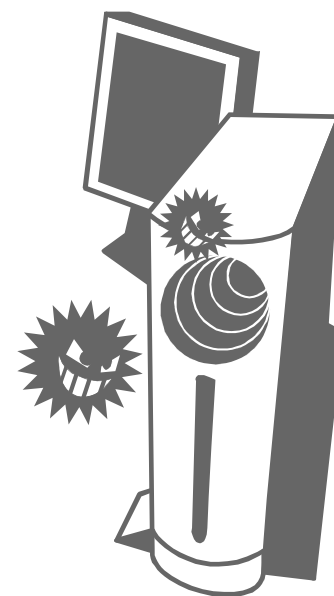
ODINS および本研究科 / 学部ネットワークの運用を妨害する行為は禁止します。物的な加害は言うまでもなく、例えば、ODINS ネットワークや本研究科 / 学部ネットワークに悪影響を与えたり、他の利用者に迷惑をかけたりするような過剰な利用は避けねばなりません。また、以下の行為は禁止されています。

(1) ODINS や本研究科 / 学部ネットワークの通信機器の配線及び周辺機器の接続構成を変更すること。また、そのようなことを試みること。

(2) ネットワークのソフトウェアの構成を変更すること。また、そのようなことを試みること。

(3) ネットワークの正常な機能を損なうようなソフトウェアを導入したり、利用したりすること。また、そのようなことを試みること。

(4) 不必要に大量のファイルを一度に送受信するなど、ネットワークの正常な機能を損なうような通信をすること。



6. ネットワーク利用上の注意

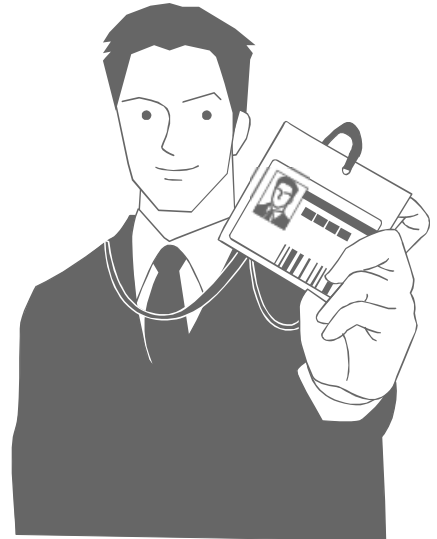
法令や公序良俗に反せず、教育・研究目的に合致した利用であっても、注意すべきことがいくつかあります。

(1) 品位をもって利用する

大阪大学の構成員としての品位を保って利用すべきことは言うまでもありません。品位に欠けるメッセージの発信は謹んで下さい。

(2) 他人を思いやって利用する

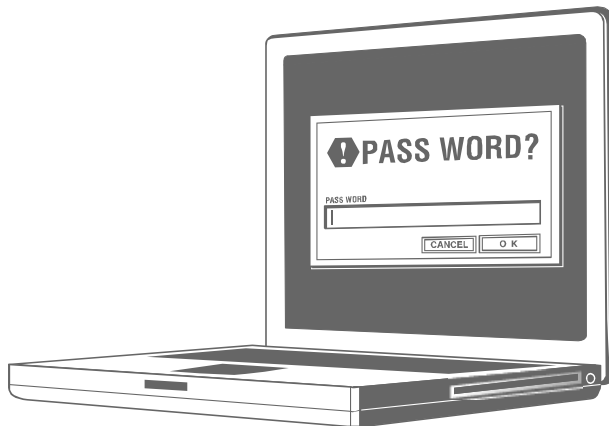
大量のデータを送受信したりすると、ODINS ネットワークや本研究科 / 学部ネットワークを利用している他の人に迷惑をかけることとなりますから、十分注意してください。メールソフトで、メールの到着状態を調べる時間間隔を極端に短くするなど、そのシステムを共有している利用者への迷惑になりますし、運用妨害になることもあります。また、サイバーメディアセンターの教育用計算機システムのように共同で利用するコンピュータ設備は、ネットサーフィンで占有したりせずに、他人に対する思いやりをもって利用してください。



(3) パスワードを適正に管理する

パスワードはあなたが正規の利用者であることを確認するために大切なものです。自分のパスワードを友人に教えたり、友人のパスワードを使ってコンピュータを用いたりしてはなりません。パスワードを教えた人、教えてもらって利用した人の双方が責任を負うこととなります。パスワードの文字列に工夫する、手帳や携帯電話などにメモしない、パスワードを定期的に変更することです。他人がパスワードを入力するとき

には、その人の手元を見ないという配慮もよく行われています。アカウントを盗用されても、直接的な経済的不利益は被らないかもしれませんが、しかし、例えば、パスワードを知られたために、自分のアカウントから他人を侮辱する内容の電子メールが発信された場合、あなたが侮辱行為者として扱われます。また、あなたのアカウントを利用して他の計算機への侵入行為が行なわれた場合（これを踏台アタックと呼びます）、アカウントを盗用された被害者が、まず最初に犯人として疑われます。



(4) プライバシーを守る

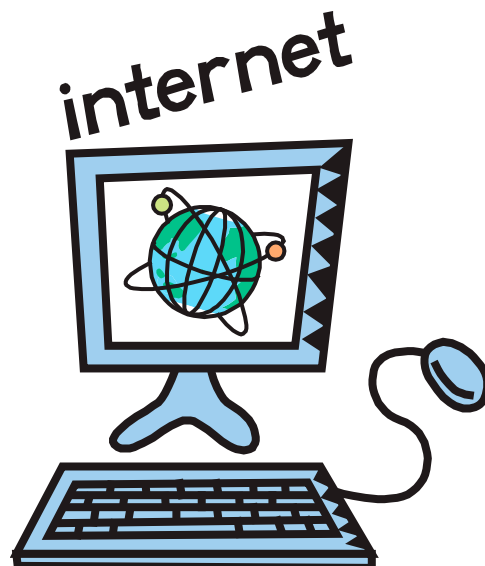
共用のサーバコンピュータに置かれたファイルには、他の利用者から読まれないようにアクセス権限を設定できることが多いので、適切に設定しましょう。誰からも読める、または誰からも書き込めるという状態は非常に危険です。また、他人のファイルが読めるようになっていたとしても、無断でその内容を見ることはやめましょう。Web ページ・ニュース・掲示板などに、個人のプライバシー情報を提供することも危険につながります。

(5) ネットワークのセキュリティ保持に協力する

上記(1)～(4)の他に、ネットワークのセキュリティを保持するために、利用者自身が注意すべきことがあります。例えば、コンピュータウィルスを持ち込まない、不審な発信元からのメールを開かない、自分の管理しているコンピュータにウィルス対策ソフト(ワクチンソフト)を導入しウィルス検知パターンを常に最新状態に保つ、本研究科/学部ネットワークやODINSの故障や異常を見つけたら、速やかにサイバーメディア室に通知する(内線 4037)、などがこれに該当します。

(6) ネチケットを守る

一般にネットワークを快適に利用する際に注意すべきことがいくつかあります。これらは、主にネットワーク・エチケット(略してネチケット)と呼ばれるものです。詳しくは、ネチケットのWebサイト(例えば、<http://www.cgh.ed.jp/netiquette/>)などを参照してください。



ネットワーク運用管理ガイドライン

1. はじめに

大阪大学人間科学研究科 / 人間科学部ネットワーク運用管理ガイドライン（以下「本ガイドライン」）は、大阪大学総合情報通信システム運用管理要項の第7に基づいて、人間科学研究科 / 人間科学部内ネットワークの適正かつ安全な運用管理に必要な事項を定めたものです。本研究科 / 学部ネットワークの円滑かつ適正な利用の促進を目的としています。共有サーバ利用者を含む、本研究科 / 学部ネットワークの運用管理に携わる者は、本ガイドラインの遵守をお願いいたします。なお本研究科 / 学部ネットワークは、大阪大学総合情報通信システム (ODINS: Osaka Daigaku Information Network System) の一部です。そのため運用・利用に際しては、原則として、大阪大学総合情報通信システム運用管理要項、大阪大学総合情報通信システム運用管理者ガイドライン等に従うものとします。

2. 基本事項

人間科学研究科 / 人間科学部ネットワークは、人間科学研究科 / 人間科学部の教職員、学生およびこれらに準ずる者の教育、研究及びその支援活動の円滑な遂行に資するために運用されなければなりません。

3. 定義

ODINS とは、Osaka Daigaku Information Network System の略で、学外ネットワークと接続するため、及び部局ネットワークを構成するため設置されたすべてのコンピュータ、通信機器及びそれらの上で動作する通信ソフトウェア群によって構成されるシステムをいいます。人間科学研究科 / 人間科学部ネットワーク（以下「本研究科 / 学部ネットワーク」という。）とは、人間科学研究科 / 人間科学部（以下「本研究科 / 学部」という。）によって個別に運用管理されているネットワークをいいます。

4. 本研究科 / 学部ネットワーク運用管理基本方針

本研究科 / 学部ネットワーク運用管理の基本方針については、次のように定めます。

4-1 一般的遵守事項

- (1) 市民社会及び大学生活において要求される倫理的及び法的な規範を遵守しなければなりません。
- (2) 知的財産権によって保護されているソフトウェアやその他著作物を、使用許諾権の範囲を超えて複製、修正または配布してはいけません。また、そのようなことを試みたり、そのような行為を行う手段を他人に提供したりしてはいけません。
- (3) 他人を誹謗中傷する内容のファイル等を送信しないでください。
- (4) 大学人としての品位を欠くような内容のファイル等を送信しないでください。

4-2 セキュリティに関する遵守事項

- (1) 他人のアカウント及びパスワードを不正に入手、所有または使用してはいけません。また、そのようなことを試みてはいけません。
- (2) 自己のアカウント及びパスワードを不正に他人に提供したり、利用させたりしてはいけません。
- (3) 運用管理に関わる正当な理由なしに、ODINS および本研究科 / 学部ネットワークに接続された機器上の情報を入手してはいけません。また、そのようなことを試みてはいけません。

4-3 通信の秘密に関する遵守事項

運用管理に関わる正当な理由なしに、通信の秘密を侵害してはいけません。

4-4 システムの適正かつ安全な運用に関する遵守事項

- (1) 本研究科 / 学部ネットワークを構成するルータ・スイッチ（ルータとは、ネットワーク上を流れるデータを他のネットワークに中継する、経路選択機能を持った機器。スイッチとは、回線やパケットの交換（スイッチング）機能を持った通信装置）などのネットワーク機器は、不正アクセスや不特定多数のコンピュータ・ユーザのネットワーク接続・通信・ネットワーク構造の変更などを未然に防ぐために、適切な設定を行ってください。運用管理に関わる正当な理由なしに、本研究科 / 学部ネットワークおよび ODINS 機器の配線及び周辺機器の接続構成を変更してはいけません。またそのようなことを試みてはいけません。
- (2) サーバを管理する者は、常にセキュリティ情報をチェックし、当該サーバのセキュリティレベルを適切な状態に維持しなければなりません。
- (3) 運用管理に関わる正当な理由なしに、本研究科 / 学部ネットワークおよび ODINS のソフトウェアの構成を変更してはいけません。また、そのようなことを試みてはいけません。
- (4) 本研究科 / 学部ネットワークおよび ODINS の正常な機能を損なうような、いかなる種類のソフトウェアも導入してはいけません。また、そのようなことを試みてはいけません。
- (5) 不必要に大量のファイルを一度に送受信するなど、本研究科 / 学部ネットワークおよび ODINS の正常な機能を損なうような通信をしてはいけません。

4-5 ログの保存

ネットワーク機器及びサーバにおいては、セキュリティインシデント（セキュリティインシデントとは、情報管理やシステム運用に関して保安上の脅威となる現象や事案のこと。ウイルス感染や不正アクセス、情報漏洩、迷惑メール送信、サービス拒否攻撃などを含む）発生時に際して、インシデントの時刻・内容等が特定できるように、各種のログ（コンピュータの利用状況やデータ通信の記録）を採取し、一定期間（約6ヶ月間）保存しておいてください。なお利用履歴は、運用管理及び教育上の目的を除いて、当該利用者本人の同意なしに調査しその結果を第三者に公表することはできないものとします。

4-6 物理的セキュリティの維持

本研究科 / 学部ネットワークにおいて上位に位置するルータ・スイッチに関しては、悪意ある者のネットワーク破壊・侵入行為を防止するために、特に設置区域の入退室管理を含めた物理的なセキュリティ対策を施すこととします。

5. 情報コンテンツ

本研究科 / 学部ネットワークを利用して学内外に発信される情報コンテンツは、社会および教育・研究に貢献するものであるようにしてください。情報コンテンツとは、Web ページや公開ファイル情報、掲示板の内容などを指します。

6. セキュリティインシデントが発生した場合

本研究科 / 学部ネットワークの適正かつ安全な運用に問題が発見された場合は、速やかにサイバーメディア室に報告するようお願いします。またセキュリティインシデントへの対処にあたっては、利用者の方々の可能な限りのご協力をお願いします。なお本研究科 / 学部ネットワーク利用者の行為に問題が認められ、当該利用者に対する何らかの措置を行う必要が生じた場合、当該利用者に対しては理由を付して通知することとします。

7. 個人情報保護

(1) 管理上知り得た利用者の個人情報、通信内容、通信先等の通信秘密を、第三者に漏らさないようにしてください。

(2) 利用履歴を調査する場合、個人情報保護の観点から次の点を遵守することとします。

システムの適正な運用維持の必要性の範囲を超えて調査を行わないこと。

当該利用者以外の個人情報を調査しないこと。

調査の結果得られた個人情報を目的以外に使用しないこと。

大阪大学人間科学研究科 / 人間科学部サイバーメディア室

2007年3月発行

印刷：株式会社ケーエスアイ

tel：06-6652-8002

fax：06-6652-8484