■ 関連規則･情報

(1) 情報セキュリティポリシーと情報スタンダード
http://www.cc.mie-u.ac.jp/cc/policy/
三重大学情報セキュリティポリシー
教育研究情報セキュリティスタンダード
事務情報セキュリティスタンダード
附属病院情報セキュリティスタンダード

(2) その他、全学規則類
http://www.mie-u.ac.jp/gakunai/kisoku/index.htm
三重大学個人情報保護規程
三重大学法人文書管理規程
三重大学事務用電子計算機業務処理要項
三重大学大学院医学系研究科･医学部情報ネットワーク利用要領
三重大学医学部附属病院情報ネットワーク利用要領
三重大学医学部附属病院総合医療情報システム運用管理規程
三重大学医学部附属病院診療記録等の電子保存システムに関する運用管理規程

■ Related regulations and information

(1) Information Security Policy and Information Standards
http://www.cc.mie-u.ac.jp/cc/policy/
Mie University Information Security Policy
Education and Research Information Security Standards
Information Security Policy for Offices
University Hospital Information Security Standards

(2) University-wide Regulations and Other Information
http://www.mie-u.ac.jp/gakunai/kisoku/index.htm
Mie University Personal Information Protection Regulations
Mie University Corporate Documentation Management Regulations
Summary of Mie University Business Computer Work Processes
Mie University Graduate School of Medicine/Faculty of Medicine Procedures for Use of the Information Network
Mie University Hospital Procedures for Use of the Information Network
Mie University Hospital Integrated Medical Information System Operation Management Regulations
Mie University Hospital Operation Management Regulations on the Electronic Storage System for Medical Records, etc

■ 相关规则・信息

(1) 信息安全方针与信息标准
http://www.cc.mie-u.ac.jp/cc/policy/
三重大学信息安全方针
教育研究信息安全标准
事务信息安全标准
附属医院信息安全标准

(2) 其它、全校规则类
http://www.mie-u.ac.jp/gakunai/kisoku/index.htm
三重大学个人信息保护章程
三重大学法人文件管理章程
三重大学事务用电子计算机业务处理要点
三重大学大学院医学系研究科・医学部信息网络利用要领
三重大学医学部附属医院信息网络利用要领
三重大学医学部附属医院综合医疗信息系统运行管理章程
关于三重大学医学部附属医院诊疗记录等电子保存系统的运行管理章程

キャンパスネットワーク利用ガイドライン
2018年6月発行
発行者：三重大学総合情報処理センター　http://www.cc.mie-u.ac.jp

本書に関するお問い合わせは、
TEL：059-231-9772
MAIL：support@cc.mie-u.ac.jp
までお願いいたします。

MIE UNIVERSITY
三重大学総合情報処理センター
Center for Information Technologies and Networks

三重大学キャンパスネットワークを利用するすべての皆様へ
For everyone using the campus network at Mie University
致使用三重大学校园网的全体人员

キャンパスネットワーク利用ガイドライン

Campus Network Guidelines

校园网使用指南

MIE UNIVERSITY
三重大学総合情報処理センター
Center for Information Technologies and Networks

本ガイドラインは、学内におけるコンピュータやキャンパスネットワークおよびキャンパスネットワーク経由でのインターネット※の利用について、特に注意が必要とされる内容を抜粋したものです。教職員、学生はもちろんのこと、キャンパスネットワークを利用する全関係者が対象となります。以下の点に注意を払い、利用者として自覚と責任を持って行動してください。これらに違反した場合、注意や処罰の対象となります。また、学外活動や私生活においても、本学の学生や教職員として良識と節度ある行動をお願いします。

※以後、「学内におけるコンピュータやキャンパスネットワークおよびキャンパスネットワーク経由でのインターネット」は、「キャンパスネットワーク」と記述します。

1. 規則を守りましょう

キャンパスネットワークの利用については、「三重大学情報セキュリティポリシー」と「教育研究情報セキュリティスタンダード」（セキュリティスタンダードは、教育研究、事務、附属病院の3部構成です）等の規則を遵守する必要があります。三重大学総合情報処理センターホームページで公開していますので、各自確認してください。

「三重大学情報セキュリティポリシー」http://www.cc.mie-u.ac.jp/cc/policy/

2. 教育・研究・事務業務目的に限定

キャンパスネットワークは、教育・研究・事務業務に関する目的に限定されています。この目的に沿わない不適切な行為、違法行為、倫理に反する行為を禁じます。

3. 違法コピーの禁止・違法コンテンツのダウンロード禁止

音楽、映像、本、ソフトウェアなどの著作物を、違法にコピーして配布したり、ライセンス規約を守らずに利用してはいけません。また、違法に配信されている音楽・映像コンテンツを、それと知りながらダウンロードすることは違法であり、刑事罰の対象となる場合があります。

4. ファイル共有ソフトの利用禁止

キャンパスネットワークにおいて、P2P型のファイル共有ソフト（Winny、Share、Cabos等）の利用は禁止されています。これらソフトウェアでは、違法なソフトウェア配布やウィルス混入ソフトウェアの配布が横行しています。また、これらソフトウェアでは、データをダウンロードしたパソコンが自動的にそのデータの発信者になるため、大きな罪に問われる可能性があり、特に注意が必要です。本学では、違法行為や不適切な利用の可能性がある通信を監視しており、疑わしい場合は通信を遮断して実機調査することがあります。

5. ソフトウェアライセンスの適正管理

利用規約に定められた台数を超えてソフトウェアをインストールすることはライセンス違反となります。利用規約をよく読み、遵守してください。また研究室・講座等ではソフトウェアの台帳管理をすることが義務付けられています。

6. 大量ダウンロードの禁止

学内から「自由に」使って良いように見えるサービスでも、本学とサービス提供元との間で利用条件が定められているのが普通です。例えば、多くの電子ジャーナルや商用データベースでは、ダウンロードツール等を利用して一度に大量のコンテンツをダウンロードすることは禁じられています。

7. ID・パスワードの管理

全ての利用者には、自分が保持するID・パスワード、情報機器、ソフトウェア等を安全に管理する義務があります。パスワードを推測するなどして、他人のIDを盗用することは犯罪となります。また、自分のID・パスワードを他人に貸与することは決してしないでください。

パスワードには、アルファベット大文字、小文字、数字、記号などを組み合わせた意味のない文字列を利用し、最大文字数内でできるだけ長めにするようにしてください。また、インターネット上の異なる複数のシステムで同一のパスワードを使用することは大変危険ですので、異なるパスワードを付与するようにしてください。パスワードは記憶するのが望ましいですが、それができない場合は、パスワード管理ソフトの利用なども良いでしょう。

8. ソフトウェアを最新の状態に

OS（Windows、MacOSX等）やアプリケーションは常に最新版にアップデートしてください。特に、ブラウザ（Internet Explorer、Firefox、Chrome、Safari等）、Flash Player、Adobe Readerなどのインターネットアクセスでよく用いられるソフトウェア類は確実にアップデートしてください。自動更新が可能なソフトウェアも増えていますが、その機能を有効にした上で、適切に自動更新が機能しているかどうか、時折確認しましょう。

9. ウィルス対策の徹底

キャンパスネットワークに接続される全てのコンピュータには、ウィルス対策ソフトをインストールする必要があります。また、定期的にコンピュータ内の全ファイルにウィルスチェックを行ってください。ネットワークのほか、USBメモリなどの物理メディアによる情報の受け渡しも重大なウィルス感染経路です。

なお、ウィルス感染が疑われる際は、速やかに端末をネットワークから切断し、総合情報処理センターにご連絡ください。（電話 059-231-9772 / メール support@cc.mie-u.ac.jp）

10. インターネットからダウンロードしたソフトウェアに注意

有償無償含め数多くのソフトウェアがインターネット上で配布されています。こうした配布物の中には、偽物ソフトウェアや本来のソフトウェアと抱き合わせる形で不要なソフトウェアを混入したもの、ウィルス等が混入されているものまであります。信頼のおけないサイトからのダウンロードは避け、正規の配布元から取得してください。また、インストール時に抱き合わせソフトウェアが一緒にインストールされてしまわないか、十分に確認をしてください。

11. フィッシング詐欺に注意

フィッシングと呼ばれる騙し討ち型の詐欺行為が急増しています。多くの場合、「有効期限切れパスワードの変更のお願い」等を装ったメールによって本物そっくりの偽サイトに誘導し、ID・パスワードを奪取するものです。近年では文面も巧妙に偽装されているため、詐欺と気づけない場合があります。パスワードに関係するような重大な内容については、メールが本物かどうか一旦踏み留まって確認してください。また、「ウィルスが検出されました」、「パソコンの機能が低下しています」などの偽表示による詐欺も多く発生しています。警告を無視することはよくありませんが、偽の警告もあり得るということにも留意してください。

12. 情報漏洩に注意

ノートパソコン、外付けハードディスク、USBメモリなど、重要な情報が入った情報機器の紛失や盗難に注意してください。盗難による被害は学内でも数多く発生しています。また、重要情報については、USBメモリなどでの運搬や、学外への持ち出しが禁じられている場合があります。インターネット経由でのクラウドサービス上へのデータ保管なども「学外への持ち出し」となります。また、最近ではクラウドサービスと連携したソフトウェアの利用によって意図せず情報漏洩する場合がありますのでご注意ください。

13. Windows 7の接続禁止（2020年1月14日以降）

キャンパスネットワークではセキュリティ更新のできない機器の接続は禁止となっています。2020年1月14日以降、Windows 7のセキュリティ更新が終了するため、キャンパスネットワークへの接続は違反行為となります。同様に、Office 2010の使用も禁止されますので、どちらも後継製品への切り替えをしてください。

These guidelines summarize things to be aware of when using campus computers, the campus network and the Internet via the campus network*. These guidelines are for everyone using the campus network, including faculty and students. Please notice the following points and behave appropriately as a user of the campus network. Violations of these guidelines may be subject to warnings or disciplinary actions.

* "Campus computers, the campus network and the Internet via the campus network" is described as the "campus network" in this document.

1. Observe the regulations

To use the campus network, you must follow the "Mie University Information Security Policy" (in Japanese) and the "Information Security Standards for Education and Research" (in Japanese) (the security standards consist of three parts – education and research, office work, and the university hospital). These regulations are available on the Mie University Center for Information Technologies and Networks website.

The Mie University Information Security Policy (in Japanese): http://www.cc.mie-u.ac.jp/cc/policy/

2. Limited usage for education, research and office works

The campus network is provided for educational, research and office purposes only. Do not use it for improper, illegal or immoral purposes.

3. Illegal copying and downloading of illegal content are prohibited

Do not unlawfully copy or distribute music, videos, books, software or other copyrighted works in breach of license agreements. Furthermore, knowingly downloading audio-visual content distributed unlawfully is an offence and may be subject to criminal punishment.

4. Use of file-sharing software are prohibited

Do not use P2P file-sharing software (Winny, Share, Cabos, etc) on the campus network. Such software is often used to distribute unlawful software and viruses. Also, when you download data with such software, your computer automatically shares the data, which could lead to serious offenses. The university monitors potentially illegal or improper communications and may block access to the network or investigate your PC in the case of suspicious circumstances.

5. Appropriate management of software licenses

Installing software on more PCs than allowed by the user agreement is a license violation. Please read and follow by user agreements. Furthermore, you must keep a ledger of software used in laboratories and seminars, etc.

6. Large-volume downloads are prohibited

Though, the service may seem to be free on campus, there are usually conditions of use established between the university and the service provider. For example, using programs to download a large volume of content at once is prohibited by many electronic journals and business.

7. Management of IDs and passwords

All users must look after their IDs, passwords, IT devices, and software, etc. Access to the ID of other users by guessing their passwords or other means is a crime. Also, never give your ID or password to another person.

Please use a meaningless character string combining with uppercase and lowercase letters, numbers, and symbols for your password. Also try to make the password as long as possible within the character limit. We recommend using a different password for each system. Please memorize the passwords. If this is not possible, you may use password management software etc.

8. Use the newest version of software

Please update the OS (Windows, Mac OS X, etc) and applications to the newest version. In particular, please make sure to update software used to access the Internet, such as the Internet browser (Internet Explorer, Firefox, Chrome, Safari, etc), Flash Player, and Adobe Reader. Many software can be updated automatically. Please enable the update function and periodically check whether it is updated correctly.

9. Install anti-virus software

You have to install anti-virus software on all computers connected to the campus network. Please also periodically run a virus check on all files on the computer. Viruses can also be transmitted by physical media such as USB sticks, in addition to over the network.

When your computer may be infected with a virus, disconnect it from the network immediately and contact Center for Information Technologies and Networks.

(Tel: 059-231-9772 / E-mail: support@cc.mie-u.ac.jp)

10. Be careful of software downloaded from the Internet

A huge quantity of paid and free software is distributed on the Internet. Such products may be imitations or contain unnecessary software packaged with the main program or viruses. Please acquire software from a legitimate distributor and do not download from unreliable sites. Also, please carefully check whether any packaged software will be installed with the main program during installation.

11. Phishing

Scam operations called "phishing" are increasing. In many cases, the user is directed to a perfect imitation of a legitimate site by a mail requesting to input ID and password, after which the operator of fake site has control of the user's ID and password. Recently, such mails have become sophisticated, making them difficult to detect. When you get a mail relating to passwords or other important details, please take a moment to consider whether it is genuine or not. Also, scams using false pop-up dialogues such as "A virus has been detected" or "Your PC is running slowly" are common. Although it is inadvisable to ignore warnings, please bear in mind that such warnings may be fake.

12. Leakage of information

Please guard against loss or theft of information devices such as PCs, external hard drives or USB sticks which contain important information. Theft occurs frequently on the campus. Also it may be prohibited to ship USB sticks etc. containing important information or take them off campus. Storing data on online cloud services is also considered to be "taking data off campus." In addition, it is reported recently that information was unintentionally leaked through the use of software linked with cloud services.

13. Connection of Windows 7 is prohibited (from January 14, 2020)

It is prohibited to connect devices that cannot receive security updates to the campus network. Security updates for Windows 7 is ending from January 14, 2020, after which the connection of devices running Windows Vista to the campus network will be prohibited. Similarly, the use of Office 2010 will be prohibited. Please switch to a successor product.

本指南是关于利用校内电脑，校园网以及经由校园网的互联网※时需要特别注意的内容摘录。适用对象除了教职员工和学生之外，还包括所有使用校园网的相关人员。校园网的使用者必须熟知以下各条规范，自觉地担负起使用者的责任。违背本指南的行为，将会受到警告或处罚。另外在校外活动以及私生活方面，也请本校学生和教职员工保持应有的良识和品行。

※以下将“校内电脑，校园网以及经由校园网的互联网”表述为“校园网”。

1. 遵守规则

使用校园网时，必须遵守“三重大学信息安全方针”与“教育研究信息安全标准”（安全标准包括教育研究部门，事务部门和附属医院3个部分）等的规则。这些规则已在三重大学综合信息处理中心网站上公布，请各位校园网利用者在充分理解本指南的基础上加以确认。

“三重大学信息安全方针”http://www.cc.mie-u.ac.jp/cc/policy/

2. 用途限制

校园网仅限用于教育，研究，事务业务。禁止与这些用途不相符的不恰当行为，违法行为，违反伦理的行为。

3. 禁止违法复制，禁止违法内容的下载

不得违法复制或传播音乐，影像，书籍，软件等具有版权的作品。此类作品利用时必须遵守用户许可协议。对于违法传播的音乐，影像内容，在知情的情况下进行下载也属于违法行为，可能会受到刑事处罚。

4. 禁止使用文件共享软件

禁止在校园网内使用P2P型文件共享软件（Winny， Share， Cabos等）。这些软件经常被用于违法软件的传播以及病毒的传播。而且这些软件会使得下载数据的电脑自动成为这些数据发送者，从而涉及到重大犯罪，请特别加以注意。本校对于违法行为及疑似不正当利用的通信进行监视，发现可疑情况时将会将通信切断，并对使用电脑进行调查。

5. 软件用户许可协议的管理

超过利用规则所规定的电脑数量安装软件是违反用户许可协议的行为。请仔细阅读利用规则并予以遵守。研究室，讲座等有义务对软件安装实施登记管理。

6. 禁止大量下载

学校内看上去可以“自由”利用的服务，其实本校与服务提供商之间通常也有利用条件的协定。例如，许多电子杂志及商业数据库禁止利用下载工具等一次性下载大量内容。

7. ID · 密码的管理

所有使用者都有安全管理自己的ID · 密码，信息装置，软件等的义务。猜测他人密码，盗用他人ID等是犯罪行为。绝对不要将自己的ID · 密码借给别人使用。

密码应由大写字母，小写字母，数字，符号等无意义的字符串组成，并在最大字符数内尽量使用较长的密码。另外在互联网上数个不同系统中使用相同密码会非常危险，请设置不同的密码。密码最好用记忆记住，如果记不住也可以使用密码管理软件等方法。

8. 保持软件的最新状态

OS（Windows、Mac OS X等）及应用软件须及时升级为最新版本。特别是浏览器（Internet Explorer，Firefox，Chrome，Safari等），Flash Player，Adobe Reader等互联网访问经常使用的软件类更须及时升级。尽管具有自动更新功能的软件正在增多，校园网利用者也须在启动这些自动更新功能的基础上，时常检查这些自动更新功能是否有效。

9. 彻底实施病毒防范措施

所有接入校园网的电脑都必须安装杀毒软件。必须定期对电脑内的所有文件进行病毒检查。必须清楚地认识到，除了网络之外，USB储存器等物理媒介的信息传递也是病毒感染的重要途径。

另外，如果怀疑电脑已经被病毒感染，则须立即切断电脑与网络的连接，

并与综合信息处理中心联系（联系电话：059-231-9772 / 邮箱： support@cc.mie-u.ac.jp）。

10. 警惕从互联网下载的软件

互联网上传播着许多免费或收费的软件。在这些软件中混入了假冒软件以及与原来软件捆绑在一起的不需要软件，甚至还有含病毒等的软件。应避免从不可靠的网站下载，请从正规的传播渠道获取。另外在安装时，请充分确认有没有一起安装了捆绑软件。

11. 警惕网络钓鱼欺诈

被称作网络钓鱼的欺骗、欺诈行为正在急剧增加。大多数情况是通过伪装成“过期密码更改的请求”等邮件，诱骗访问与官方网站完全一样的假冒网站，然后骗取ID和密码。近年来措词也被伪装得十分巧妙，有时会很难识破是欺诈。对于与密码相关的重大内容，请首先仔细确认邮件是不是欺骗邮件。此外还经常发生“检测出了病毒”、“电脑的性能正在降低”等虚假消息的欺诈。无视警告虽然不好，但也必须注意可能会是虚假警告。

12. 防止信息泄漏

警惕笔记本电脑、外接硬盘、USB储存器等含有重要信息的信息装置的遗失或被盗。校内曾多次发生过被盗事件。不要使用USB储存器等来传递重要信息。禁止将存有重要信息的USB储存器等带出学校。使用互联网云服务上的数据保管等也属于“带出学校”。最近还发生了因使用云服务相关软件而在无意之间泄漏了信息的事件，务必引以为戒。

13. 禁止Windows 7上网（2020年1月14日以后）

校园网禁止无法进行安全更新的装置上网。自2020年1月14日起，Windows 7因安全更新支持结束，上校园网将成为违规行为。同样使用Office 2010也被禁止，请将两者都改换成后续产品。