ISIC 岩手大学 情報基盤センター報告 Σ

2016年度版(2017年3月発行)

Σ

No.2 2016

Iwate University Super Computing and Information Sciences Center

目次

巻頭言

情報基盤センター長
喜多一美

岩手大学情報基盤センターΣは，情報基盤センターの活動や報告をまとめたものです。この度、平成 28 年度の活動報告がまとまりましたので、年報としてお届けします。

昨年度，情報基盤センターとなってから初の活動報告を作成することができました。昨今の情勢をふまえ，情報基盤センターでも情報セキュリティに関する取り組みを強化したことをお伝えしました。平成 28 年度も，岩手大学の情報基盤を堅守するため，情報セキュリティに関する取り組みをはじめとする様々な活動・事業を行っております。

平成 28 年度は，教育研究用コンピュータシステムが更新されました。これは，各学部などにある教育用端末室や，情報基盤センターの基幹システム（サーバ，ストレージ），および，高速計算機が該当します。今回の入れ替えでは，教育用端末室の改善と高速計算機の調達方法の見直しを図りました。

教育用端末室では，端末イメージの管理をよりきめ細やかに実施できるよう，ネットブート方式を取り入れました。また，端末の起動時間を短縮するため，補助記憶装置をハードディスクドライブ（hard disk drive, HDD）ではなくソリッドステートドライブ（solid state drive, SSD）にしました。この結果，利用者が電源投入からログインして利用出来るようになるまでの時間が概ね２分以内となり，旧システムより大幅に短縮しています。また，教育用端末室は計算機を使った講義で利用されるため，講義支援システムを導入しました。

高速計算機は，本システムからは，自前での調達をやめ．外部の計算機資源を機関（岩手大学）として利用する方式に改めました。これは，自前での調達は諸事情から厳しい状況になったことを踏まえたものです。外部の計算機資源としては，本学の利用形態と利用者サポート，契約面などを含めて総合的に検討した結果，東北大学サイバーサイエンスセンター大規模科学計算システムを機関利用することになりました。この計算機システムは，ベクトル型のスーパーコンピュータ SX-ACE とスカラー型の並列コンピュータ LX 406Re-2 からなります。本学はこれまでは１系統（並列コンピュータ）だけだったものが，２系統の処理様式の異なるスーパーコンピュータを利用できるようになりました。

昨今重要性を増しつつある情報セキュリティについては様々な取り組みを行いました。一番大きな内容は、本学における情報関連規則等を大幅に見直した点です。今までの規則は平成 20 年頃に制定されたものであり、現状に対応し切れていませんでした。特に、情報セキュリティに関しては、インシデントが発生した際に迅速に対応できるような体系に変更しました。その他にも、分かり易いハンドブックの作成、全構成員のセキュリティ意識を涵養するためセキュリティセミナーの大幅な拡充等が挙げられます。また，サーバそのものや標的型攻撃メール等への対策等も行っています。標的型攻撃メール等に関する情報発信は，ウェブページおよびメールマガジン「オンラインシグマ」で行っています。

情報セキュリティは最も脆弱な部分が”蟻の一穴”となることから，今後も，情報セキュリティ確

保に対する皆様方のご理解とご協力を賜れば幸いです。

情報基盤センターは，本学の情報基盤を支え，これからの時代の変化もふまえつつ，岩手大学と地域に貢献していきたいと考えております。

【特集1】
教育研究用新コンピュータシステム

平成 28 年 9 月に稼働した情報基盤センター
教育研究用新コンピュータシステムについて

情報基盤センター
川村　暁，中西貴裕
技術専門職員
加治卓磨，金野哲士，福岡　誠
システム創成工学科　知能・メディア情報コース（仕様策定委員会委員長）
安倍　正人

1. はじめに

岩手大学では，概ね５年周期で教育研究用コンピュータシステムの更新を行っている。平成 23 年 9 月に導入された旧システムを入れ替えた新システム（以降，新システム）は，入れ替えから既に七ヶ月ほど経過している。

本システムは，教育用端末室・研究用計算基盤（ソフトウェアも含む）・電子メールシステムとこれらを支える仮想化基盤・認証系・ファイルサーバおよびネットワーク機器で構成されており，大学の諸活動の基盤となる重要なシステムである。

本稿では新システムについて，どのような点を重視して更新したのか，その結果，更新前のシステムと比較して機能強化された点を，利用者の目線に立って記す。

なお，新システムの変更点については，岩手大学情報基盤センターウェブページに掲出済みなので参照いただきたい。

情報基盤センター教育研究用システム更新に伴う変更点（学内限定）
https://isic.iwate-u.ac.jp/usersguide/update2016.html

2. 新システムで目指したこと

教育研究用コンピュータシステムの更新では，旧システムでユーザからの改善要求の多かった点を満たすと共に，今後長期間（最低でも５年間）にわたって本学の教育研究の基盤となることを意識して仕様を策定し，システムを更新した。なお，機種とシステムを最新版にした以外の変更がなく，利用方法にも大きな変更を加えなかったプリンタについては，本稿では言及しない。

2.1. 教育用端末：起動時間の大幅な短縮を目指して

教育用端末では，旧システムで問題となっていた起動時間の短縮（旧システムではユーザがログインしてから利用可能になるまで数分ほど時間がかかっていた）や，セキュリティ更新の頻度が増加したこと等へ対応するためのメンテナンス性の向上，講義支援システムの導入による講義支援機能の充実，プリンタシステムのセキュリティを意識した設計への転換を図った。

教育用端末のスペックは以下の通りである。

【Windows/Linux】

ＯＳ　Windows 8.1 Pro 64bit / CentOS Linux 7.2
ＣＰＵ　Intel Core i5 4590 (4Core 3.3GHz)
メモリ　8GB
ストレージ　ソリッドステートドライブ（SSD）　128GB

オプティカルドライブ　　スーパーマルチドライブ　DVD-R DL(最大 8 倍速)
グラフィックス　Intel(R) HD Graphics 4600 1GB
ＵＳＢポート　　USB2.0×4 （フロント×2、リア×2)、USB3.0 x2（リア×2）
ディスプレイ　　19 インチスクエア（人文社会科学部，学生センター）
21.5 インチワイド（その他）

【Mac】

ＯＳ　　Mac OS X 10.11（El Capitan）
ＣＰＵ　Intel Core i5 (4Core 3.2GHz)
メモリ　8GB
ストレージ　　ハードディスクドライブ（HDD）　1TB
グラフィックス　AMD Radeon R9 M380 2GB
ＵＳＢポート　　USB3.0×4
ディスプレイ　　27 インチワイド

■教育用端末にインストールされているソフトウェアのうち，共通のもの.

専門教育等で利用するソフトウェアは，学部（設置場所）により異なるため，記載していない。

【Windows/Linux】

Microsoft Office Professional Plus 2016
Microsoft Visual Studio Professional 2015

【Mac】

Microsoft Office for Mac 2016
Shade3D Standard Ver.16
Adobe Creative Cloud
ESET NOD32 Antivirus 4

教育用端末の設置箇所と台数を図 1 に示す。旧システムから若干の台数の変動があるが，大きな変更はなされていない。

教育用端末の起動時間を短縮するために，起動時に時間を要している要因について検討した。ユーザが教育用端末の電源を入れてから利用できるまでの処理を大まかに示す。

電源オン　→　BIOS　→　OS のブート処理　→　ログオン処理

最も時間を要しているのは,教育用端末に内蔵された HDD から OS を立ち上げる処理である。旧システムではこの部分に 2 分弱程度かかっていると推察された。ここを短縮すれば起動時間を大きく減ずることができるが，HDD を利用している場合，HDD のデータ転送速度の制約から劇的に縮減することは難しい。そこで新システムにおいては，HDD と比較して読み書き速度が高速な SSD を採用した。SSD は半導体記憶素子を用いた補助記憶装置であり，機械的な動作を伴う HDD よりデータの読み込みが非常に高速である。特にランダムアクセス性能に優れるため，OS の起動時のような，不連続なデータの読み込みが連続して発生する場面で特に効果を発揮する。

次に，ユーザがログイン操作を行った後，パソコンが利用可能になるまでの待ち時間の短縮について考えた。ユーザのログイン処理では，ユーザの認証と OS の設定が成された後，ユーザホーム等がマウントされる。ユーザホーム等は，ユーザ毎に割り当てられたディスクスペースであ

る。情報基盤センターに設置されたファイルサーバの当該の領域が割り当てられ，ネットワーク経由でマウントされる。このログイン後の処理にかかる時間を軽減すべく，ファイルサーバの構成を強化した。このほか，ログオン後に実行される処理・スクリプトについて，処理形態を含めた見直し・改善を行っている。

最後に，メンテナンス性と起動時間を増加させない端末イメージの管理方式として，ネットブート方式を採用した。端末は，一度読み込んだ内容を SSD にキャッシュすることで，２回目以降の起動時間が早くなる構成にした。様々な工夫により，端末の起動時間は，電源投入から２分以内とすることが出来た。実際には，１分強で起動しているようである（起動時のネットワークやサーバの負荷状況によっても変動がある）。

教育用端末

教育用端末室の紹介

現在、学内に設置されているパソコンは以下の通りです。
各端末室でパソコンを利用するには、情報基盤センターからメールアドレスの発行を受ける必要があります。

また、利用する方の所属によって、利用可能な場所と端末の種類に一部制限がありますので注意して下さい。基本的に情報基盤センター・図書館・学生センターと、各自の所属学部設置の端末室が利用可能となっています。

ただし、講義やイベント、メンテナンス等で利用できない日時があります。詳しくは、各部屋の掲示等で確認して下さい。

建屋	Windows	Mac	利用可能者所属	利用可能時間帯（平日）
情報基盤センター棟 2階 教育用端末室	41台	0台	全学構成員	8:30-17:15
図書館 2階 マルチメディア情報閲覧室	46台	0台		9:00-21:00 10:00-18:00（土・日）
学生センター B棟 1階 キャリア支援室	5台	0台		8:30-20:00
学生センター B棟 1階 国際課談話室	6台	0台	留学生優先	8:30-17:15
人文社会科学部 6号館 1階 計算機室	42台	0台	人文社会科学部	8:00-20:00
人文社会科学部 6号館 1階 多目的視聴覚室	45台	0台		講義時のみ
教育学部 総合教育研究棟（教育系） 1階 サイバースタジオ101	90台	20台	全学構成員	8:30-19:30
理工学部 1号館 2階 21番教室	101台	0台	理工学部	8:00-21:00
理工学部 共通講義棟 3階 ＣＡＤ室	91台	0台		
農学部 北講義棟 2階 情報処理演習室	82台	0台	農学部	8:30-20:00

※ 図書館の利用可能時間帯は、時期によって変更されます。詳しくは、図書館のホームページで確認して下さい。
※ 各学部の端末室の利用スケジュールはこちらで確認して下さい。
※ **端末室は全て飲食禁止です。**

図１　教育用端末の設置箇所と台数

教育用端末（情報基盤センターウェブページ）から転載。なお，学生センターA 棟３階の端末は，情報基盤センターが運用している端末ではないため掲載していない。学生センターA 棟３階の端末については教育推進機構に問い合わせいただきたい。

また，端末イメージの更新を従来のシステムよりも時間をかけずに行えるため，臨時の設定等が必要な講義にも対応しやすくなっている。

2.2.　教育用端末：講義支援システムの導入

各学部および情報基盤センターの教育用端末室には，講義支援システム（eWatcher）を導入した。これは，講師機で学生機を制御することで，コンピュータ教室での講義をサポートするシス

テムである。実態は，講師機が制御側，学生機が被制御側になるよう，ソフトウェアで制御するものである。

講義支援システムの機能を列挙する。

- 講師機本体に接続されているワンタッチキーボードから利用できる機能
  - 学生機の一斉電源オン/オフ
  - 講師用画面の学生機への転送（講師の画面を学生に見せる）
  - 学生機の画面を講師機で受信（学生の画面を見る）
  - 学生機のキーボード/マウスのロック（使用不可にする）
  - 学生機の Internet Explorer の禁止/許可
  - 学生機の画面のブラックアウト（黒画面にする）
- 講義支援システム（eWatcher）画面のメニューツールから利用できる機能
  - 学生機への URL 転送（ブラウザの強制起動）
  - 学生機のリモート操作
  - 出席確認
  - アンケート
  - ファイル配布/レポート回収　など

講義支援システムは様々な機能を持っているので，教育用端末室を利用する多くの講義で利用しやすいように講習会を実施した。また，教育用端末の利用方法などは，情報基盤センターウェブページに掲載している。講義支援システムについては，新システム導入時に実施した講習会の VOD (Video On Demand) と資料を記載している。新システムの講習会の詳細については，本報告の「新システム利用者講習会報告」を参照して欲しい。

岩手大学情報基盤センター　利用案内　教育用端末室（岩手大学内公開）
https://isic.iwate-u.ac.jp/usersguide/pcroom/
岩手大学情報基盤センター　利用案内　講義支援システム（岩手大学内公開）
https://isic.iwate-u.ac.jp/usersguide/pcroom/use.html#ewatcher
岩手大学情報基盤センター　ストリーミングビデオ
9.16　講義支援システム eWatcher 講習会（教職員限定，岩手大学内公開）
https://isic.iwate-u.ac.jp/media/

2.3. ユーザホームの修正—セキュリティ強化のために—

各ユーザの情報を格納するファイルサーバについては，ユーザの情報格納の方法に一部変更を加えた。一般のユーザホームから，ウェブページ公開用のウェブホームを分離し，それぞれ最適なファイルアクセス権を設定した。教育用端末には，ユーザホームとウェブホーム等をマウントしている。

これは，情報基礎などの教育利用においてウェブページの作成と公開を行う事が多いが，ウェブページ用のファイルを通常のファイル（文章や表計算など）と同じ領域に格納するのはセキュリティ的な懸念があったためである。外部公開を前提としたファイルのアクセス権は緩く設定しなければならないが，個々人のファイルのアクセス権は厳しく設定する必要がある。これまでは，各ユーザが公開用のファイルのアクセス権を変更する等で対応してきたが，これをより安全なものに置き換えた。

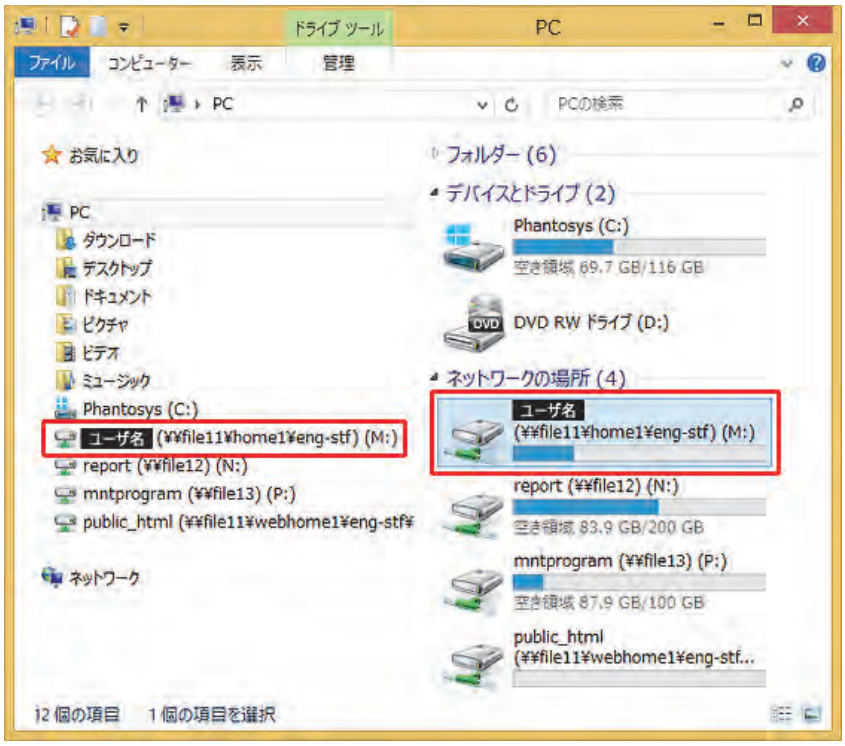


図 2　教育用端末でのユーザ領域のマウント状況（情報基盤センターウェブページから転載）

詳しくは，情報基盤センターウェブページを参照して欲しい。

岩手大学情報基盤センター　利用案内　教育用端末　データ保存（岩手大学内公開）

https://isic.iwate-u.ac.jp/usersguide/pcroom/use.html#backup

2.4.　研究用計算基盤：高速計算機の調達方法の見直し

情報基盤センターの前身は，工学部電子計算機室である。この来歴が示すように，旧システムまでは主に研究に用いられる高速計算機を導入していた。

新システムでは，以下の理由から高速計算機を本学で調達せず，外部の計算機資源を定額で賃借する方式に切り替えた。

- **性能面の制約**　計算機そのものの性能向上が著しいため，５年という長期間にわたって演算処理性能の高い高速計算機の導入が難しいこと。十分な性能を望むと，費用的な制約から現実的ではない。さらに，計算機にも処理様式に基づく種類がある（得手不得手が異なる：適応分野が異なる）が，複数種類を設置することは不可能であったこと。
- **利用・活用支援の制約**　情報基盤センターの人的リソースの面から，高速計算機利用についての十分なサポートが難しいこと。高速計算機は導入すれば誰でも使えるというわけではなく，運用上のサポートが必須となる。本センターの規模では，特にユーザが作成したプログラムの最適化支援などが出来ないため，ユーザの先進的な利用が進みにくい状況にあった。
- **環境への配慮**　高速計算機は電力消費が著しい。さらに安定して稼働させるためには，高速計算機からの廃熱を十分に処理できる空調が必要となる。光熱費の削減，ひいては環境へ配慮するためには，最も大きなエネルギー消費源かつ発熱源である高速計算機への対策が不可欠であったこと。

新システムでは，全国共同利用施設である東北大学サイバーサイエンスセンターの大規模科学

計算システム（ベクトル計算機 NEC 製 SX-ACE と並列（スカラー）計算機 NEC 製 LX 406Re-2）を，岩手大学という組織が定額で利用することにした。また，東北大学サイバーサイエンスセンターで実施しているプログラムコードの最適化などの支援も受けられるようになった。このプログラム作成に関わる支援は，本センターが独自で高速計算機を運用していたときには提供していないサービスである。利用方法および東北大学サイバーサイエンスセンター大規模科学計算システムの詳細については，ウェブページを参照して欲しい。

東北大学サイバーサイエンスセンター大規模科学計算システム（学内公開）
https://isic.iwate-u.ac.jp/usersguide/server/tohoku.html
東北大学サイバーサイエンスセンター大規模科学計算システム
http://www.ss.cc.tohoku.ac.jp/

研究用ソフトウェアの中には，ライセンスの制約から，外部の計算機資源で動かすのに適さないものがいくつかあった。詳細は，2.6 教育研究用ソフトウェア利用環境の提供　を参照いただきたい。

2.5. 教育研究用ソフトウェア：MATLAB の全学包括ライセンスの導入

理工系の教育において，数値計算に関連するソフトウェアは非常に良く用いられる。ここで，各分野において必要な計算にも対応しており，かつ，広範な分野に利用されているものとして，MathWorks 社の MATLAB が有名である。

本学では，特に利用の多い理工学部（改組前は工学部）の教育用端末室に限定して MATLAB を導入してきた。しかしながら，学内の研究教育環境を充実し，教職員及び学生の利便性を向上するため，全学を包括するライセンス体系である Total Academic Headcount (TAH) ライセンスを導入した。これにより、岩手大学の全教職員が大学として選択した 50 の MATLAB 製品を利用できる。たとえば研究室で，研究用のパソコンに MATLAB をインストールして利用することが可能であるので，教育研究に活用していただきたい。

利用方法の詳細や，利用できる MATLAB 製品については，ウェブページを参照して欲しい。

岩手大学情報基盤センター　利用案内　ソフトウェア（岩手大学内公開）
https://isic.iwate-u.ac.jp/usersguide/soft/matlab.html

なお，本学の構成員で無くなった場合（退職した，転出した，卒業・修了した等），本学の TAH ライセンス下で利用していた MATLAB は継続利用出来ない。また，不正利用を防止するため，ライセンスキーは周期的に更新する必要がある。継続して利用される場合は，MATLAB のライセンスキーの更新作業が必要になるので，ご理解とご協力を賜りたい。

なお, 本節の内容は,「岩手大学全構成員が個人の PC でも MATLAB を利用できる MATLAB TAH ライセンス」に詳述している。

2.6. 教育研究用ソフトウェア利用環境の提供：Mathematica，SAS

教育研究で利用されるソフトウェアのうち，Mathematica と SAS については，ライセンスの関係で，東北大学の大型計算機基盤にインストールすることが出来ない。このため，本センターの有する仮想化基盤に，これらのソフトウェアを動作させるためのサーバを用意している。

詳細については，以下の URL を参照いただきたい。

利用案内　教育・計算サーバ（学内限定公開）
https://isic.iwate-u.ac.jp/usersguide/server/

これら以外のソフトウェアで，ライセンスの関係から東北大の計算基盤で利用できないもののうち，パソコンなどにインストールして利用できるものがある。これらについては，2.8 節を参照して欲しい。

利用案内　ソフトウェア（学内限定公開）

https://isic.iwate-u.ac.jp/usersguide/soft/

2.7. 学外接続（VPN）: 広範な端末からの接続が可能に

大学の外のネットワークから，学内に接続し，学内限定のサービスやシステムを利用しなければならないことがある。このような場合，仮想的な通信路を構築する技術である VPN (Virtual Private Network) を用いることになる。

旧システムでは，SSL-VPN（Secure Sockets Layer Virtual Private Network の略語）を用いていた。SSL-VPN は，ウェブブラウザで専用のウェブページにアクセスして SSL-VPN を利用する。ブラウザさえあれば利用できるので利用の難易度は低いが，反面，利用できるブラウザと OS が限定されること，進化の早いフマートフォンやタブレットへの対応が難しいこと，本学の SSL-VPN では Java applet を用いていたため Java の脆弱性とサポート状況に影響を受けるという弱点があった。特に，普及著しいスマートフォン対応の制約を解消する必要があった。また，セキュリティ意識の高まりと共にセキュアなアクセスの需要が増加しているため，同時利用数の増加に対応する必要もあった。

新システムでは前システムで不足していた点を補うため，L2TP および OpenVPN を提供することにした。それぞれがサポートする OS を示す。このように，様々な OS で利用可能になっている。なお，L2TP は OS 提供の機能を利用するものであるが，OpenVPN は専用のソフトウェアを利用する。

L2TP	Apple Mac OS X（情報基盤センターでは 10.11 で動作確認）
	Apple iOS（iPhone / iPad）
	Google Android
OpenVPN	Microsoft Windows （Vista / 7 / 8.1 / 10）
	Apple Mac OS X （10.9 / 10.10 / 10.11）
	Apple iOS（iPhone / iPad），Google Android
	Linux（準備中）

詳しい使い方，設定方法については，情報基盤センターウェブページを参照いただきたい。

岩手大学情報基盤センター　利用案内　ネットワーク

https://isic.iwate-u.ac.jp/usersguide/network/vpn/

なお，学外からの接続においては，通信キャリア（回線および機器）によって利用できない（接続の不都合がある等）場合がある。通信キャリアや機器の制約は，機器やソフトウェアが要因である場合はユーザがどうこうできるものではないため，出張前などに，事前準備（テスト）をしていただきたいと考えている。よく寄せられる質問などは，ヘルプに掲載している。特に，特殊な場合の対応法（特定のキャリアで発生する現象 : VPN 接続に成功したが学内サイトを閲覧できない。）も掲載しているので，参考にしていただきたい。

岩手大学情報基盤センター　利用案内　ネットワーク　ヘルプ

https://isic.iwate-u.ac.jp/usersguide/network/vpn/win.html#help

2.8. そのほか

情報基盤センターのシステムは，本学の教育研究の基盤となるシステムである。よって，できるだけサービス提供が途切れないような構成にした。主要かつ枢要な機器などは冗長化し無停電電源装置を配置すること，メンテナンス性とセキュリティに配慮すること，費用対効果を含めて検討すること，などである。

電子メールシステムについては，特集２の「岩手大学の電子メールの概要　電子メールが届くまで」も参照していただきたい。本学の電子メールと関連する事項について簡単に記述している。電子メールシステムについては，旧システムの構成を踏襲した構成としつつ，各種設定を迷惑メールや標的型攻撃等を考慮した構成としている。

また，教育研究で利用されるいくつかのソフトウェアのうち，東北大学サイバーサイエンスセンター大規模科学計算システムで利用できないものでありかつ新システムの仮想化基盤で運用するのにふさわしくないものについては，当該ソフトウェアを研究室のパソコンなどに導入して利用することが可能である。但し利用には，利用申請などが必要となるので，詳細は情報基盤センターまでお尋ねいただきたい。

利用案内　ソフトウェア（学内限定公開）
https://isic.iwate-u.ac.jp/usersguide/soft/

3. まとめ

平成 28 年 9 月に稼働した新システムについて概説した。新システムは旧システムと比較して，多くの点で改善を図った。

新システムにより，本学の教育研究活動に貢献できれば幸いである。

また，５年度後の更新に向けて，新システムの課題点や改善点などを探りつつ，安定的な運用を心がけていきたい。

参考文献

1)　利用案内：教育用端末の紹介，岩手大学情報基盤センター（オンライン），入手先〈https://isic.iwate-u.ac.jp/usersguide/pcroom/produce.html〉（参照 2017-03-10）.

岩手大学全構成員が個人の PC でも MATLAB を利用できる MATLAB TAH ライセンス

情報基盤センター
中西貴裕

1. MATLAB と TAH ライセンス

MATLAB は信号処理，通信システム設計や制御系設計等の工業分野から，金融工学を含む最適化計算を行う数理科学分野にまで活用できるソフトウェアで，世界で広く使用されている。これまでも情報基盤センター教育研究用コンピュータシステムで，MATLAB のライセンス契約を行っていたが，大規模に使用できたのは MATLAB 本体と Simulink と呼ばれるモデリング，シミュレーション用ソフトウェアのみで，数多くある Toolbox と呼ばれる有用な拡張パッケージが使用できなかった。

2016 年 9 月から稼働した，新たな教育研究用コンピュータシステムでは，MATLAB TAH ライセンス契約により，事前に選択した 50 の Toolbox 等 MATLAB 製品（前述の MATLAB 本体や Simulink を含む）を本学の構成員であれば，個人で所有している PC 等にも導入し使用できることとなった。

本稿では，本学の MATLAB TAH ライセンス契約の内容とその利用方法について紹介する。

2. 本学の MATLAB TAH ライセンス契約

2.1. 選択された 50 製品

本学の MATLAB TAH ライセンス契約では，表 1 に示す 50 製品が選択されており，このライセンス契約の期間は 2016 年 9 月 1 日～2021 年 8 月 31 日の 5 年間となっている。それぞれの製品の概要については以下で紹介しているが，多岐にわたる分野の Toolbox があり，一通り目を通すだけでも胸が躍る。

岩手大学 MATLAB TAH ライセンス製品紹介（PDF ファイル）
https://isic.iwate-u.ac.jp/usersguide/data/soft/matlab_tah.pdf

2.2. 3 種類のライセンス形態

MATLAB TAH ライセンスには，以下に挙げる 3 種類のライセンス形態がある。Concurrent ライセンスは，学部や学科等の端末室での利用を目的としたライセンス形態であり，利用の際には情報基盤センターにご相談いただくこととなっている。教職員は Designated Computer（Campus）ライセンス，学生は Standalone Named User（Student）ライセンスで利用することとなる。

- Concurrent
  - 学部学科等の端末室で利用
  - 情報基盤センターのライセンスサーバを参照（学外での利用不可）
- Designated Computer（Campus）
  - 教員個人 PC や研究室の PC で利用
  - 教職員がライセンス処理しライセンスは PC に紐づけられる
- Standalone Named User（Student）
  - 学生個人 PC，大学から貸与され学生自身が管理している PC で利用
  - ユーザがライセンス処理し PC のユーザごとにライセンスが紐づけられる

表 1 岩手大学 MATLAB TAH ライセンス契約で選択した 50 製品

1	MATLAB	26	Communications System Toolbox
2	Simulink	27	MATLAB Compiler
3	Bioinformatics Toolbox	28	MATLAB Compiler SDK
4	Control System Toolbox	29	Neural Network Toolbox
5	Curve Fitting Toolbox	30	Global Optimization Toolbox
6	Data Acquisition Toolbox	31	System Identification Toolbox
7	DSP System Toolbox	32	Computer Vision System Toolbox
8	Image Processing Toolbox	33	Image Acquisition Toolbox
9	Instrument Control Toolbox	34	Robust Control Toolbox
10	Optimization Toolbox	35	Simulink Design Optimization
11	Parallel Computing Toolbox	36	Aerospace Toolbox
12	Signal Processing Toolbox	37	Aerospace Blockset
13	Simscape Multibody	38	Spreadsheet Link EX
14	Simscape	39	Mapping Toolbox
15	Simulink Control Design	40	Partial Differential Equation Toolbox
16	Stateflow	41	Simulink Real-Time
17	Statistics and Machine Learning Toolbox	42	Database Toolbox
18	Symbolic Math Toolbox	43	RF Toolbox
19	Simulink Coder	44	Fuzzy Logic Toolbox
20	MATLAB Coder	45	Simulink Desktop Real-Time
21	Embedded Coder	46	Model Predictive Control Toolbox
22	Simulink 3D Animation	47	Robotics System Toolbox
23	Fixed-Point Designer	48	SimRF
24	Simscape Power Systems	49	Phased Array System Toolbox
25	Wavelet Toolbox	50	Simscape Electronics

2.3. MATLAB TAH ライセンスの利用方法

MATLAB TAH ライセンス利用の大まかな手順を以下に示す。

1. アクティベーションキーの入手（学生，教職員で異なる）
2. Mathworks アカウントの作成とライセンスの関連付け
   ライセンス関連付けの際アクティベーションキーが必要
3. インストールファイルのダウンロード
4. PC へのインストール
   学生用 Student ライセンスの場合はインストール時にアクティベーションキーによるアクティベーションが必要
5. ユーザごとのアクティベーション
   学生用 Student ライセンスは PC のユーザごとにアクティベーションを行う必要がある
   教職員用 Campus ライセンスの場合この手順は不要

具体的な手順については，情報基盤センターWeb ページの利用案内 https://isic.iwate-u.ac.jp/usersguide/soft/matlab.html（学内限定）をご参照いただきたい。

2.4. MATLAB TAH ライセンス利用における注意事項（ライセンスの更新）

本学 TAH ライセンスでは，運用上，毎年 4 月に，ライセンス更新のためのアクティベーションが必要となっており，このアクティベーションを行わないと，4 月末にライセンスが期限切れとなり，MATLAB が使用できなくなる。ライセンス更新のためのアクティベーションについても，前述の利用案内ページにて手順等を公開している。

3. 講習会の実施とその資料

MATLAB TAH ライセンスやMATLABの基本的な使用方法に関する以下の講習会を実施した。

2016 年 8 月 8 日　MATLAB TAH ライセンス利用講習会

2016 年 9 月 14 日　MATLAB 講習会 教職員向け

2016 年 9 月 14 日　MATLAB 講習会 初心者向け

これらの講習会の資料と収録したビデオは情報基盤センターWeb ページ https://isic.iwate-u.ac.jp/media/（学内限定）で公開している。

4. おわりに

本稿では，情報基盤センター教育研究用コンピュータシステムとして，今年度新たに導入した MATLAB TAH ライセンスの概要と，その中で選択している MATLAB 50 製品について説明し，また，MATLAB TAH ライセンスの利用方法や使用するための学習資料・講習会について紹介した。

この MATLAB TAH ライセンスの導入が，本学の教育・研究の発展につながることを期待している。

東北大学サイバーサイエンスセンター
大規模科学計算システムの機関利用

情報基盤センター
中西貴裕，川村　暁

1. はじめに

本学では，1966 年に富士通信機（現富士通）FACOM-231 が導入されて以来，日立製作所 HITAC, SGI Origin, SGI Altix, SGI UV と機種を変えながらも，約 50 年間，独自の科学技術計算環境を維持してきた。この頃からすでに，東北大学をはじめ 7 つの旧帝国大学や国立情報学研究所では，全国共同利用施設として大型計算機センターが運営されていたが，本学のネットワーク学外接続通信帯域が不十分だったこともあり，プログラムのコンパイル・実行・結果確認等の操作やデータ等の送受信がスムーズに行えないなど，良いとは言いがたい利用環境だったため，全学的にこれらを利用する形態ではなく，先生方ユーザ個人としての利用にとどまっていた。

2012 年に本学の学外接続の通信帯域が 1Gbps となり，また，東北大学サイバーサイエンスセンターから，機関利用として，大規模科学計算システム使用に係る負担金等について本学にとって条件のよいものとしていただけたこともあり，2016 年 9 月の教育研究用コンピュータシステムの更新の際，本学独自の科学技術計算環境を持たず，全面的に東北大学サイバーサイエンスセンター大規模科学計算システム（以下，東北大学科学計算システム）を利用することとなった。

本稿では，この科学技術計算環境の変更について報告する。

2. 東北大学科学計算システムで利用可能な計算機資源

東北大学科学計算システムの機関利用により，本学の構成員であれば，個人や研究室での費用負担なく，表 1 に示す計算機資源が利用できる。本学で所有していた高速計算サーバ（共有分散メモリ型スカラ計算機）の性能が，全体で 1.28TFLOPS，640GB メモリ，ディスク容量（Work 領域）10TB だったことを考えると，利用できる計算機資源が大幅に増加していることがわかる。

表 1 東北大学科学計算システムで利用可能な計算機資源

ベクトル計算機 SX-ACE
● ノード数 2560 ● 1 ノードあたりマルチコアベクトルプロセッサ(4core) 276GFLOPS，64GB メモリ ● システム全体で 707TFLOPS，164TB メモリ
クラスタ型スカラ計算機 LX 406Re-2
● ノード数 68 ● 1 ノードあたり Intel Xeon E5-2695v2 2.4GHz(12core/socket)×2（合計 24core） 128GB メモリ ● システム全体で 31.33 TFLOPS，8.5TB メモリ
ディスク利用
● 1 人 1TB まで（申請により制限の解除も可能，ベクトル・スカラ両計算機で共通）
アプリケーション
● 非経験的分子軌道計算プログラム Gaussian09 Gaussian09 実行ノードは頻繁に使用される一時ディスク領域を SSD で構成

3. 東北大学科学計算システムの利用について

3.1. 利用申請等手続き

東北大学科学計算システムの利用には申請が必要となっている。申請等，東北大学サイバーサイエンスセンターとの手続きは，利用上の相談を除き，岩手大学情報基盤センター経由で行う。利用申請書（図 1)，利用変更届，利用取り消し届等，手続きに必要なものは以下の情報提供ページに記入例などと共に用意されているので，こちらを利用されたい。

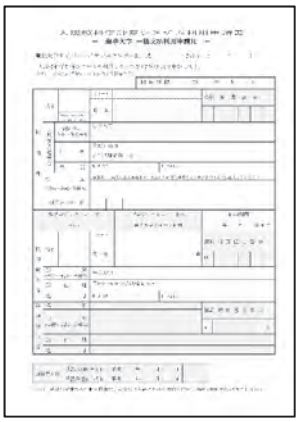


図 1 利用申請書

東北大学大規模科学計算システム利用に関する情報提供ページ
https://isic.iwate-u.ac.jp/usersguide/server/tohoku.html（学内限定）

利用申請が東北大学で受理されたると（申請日を除き 3,4 日後，外国人の方はさらに 3,4 日後になることがある)，東北大学から申請したユーザに承認書が郵送される。この承認書には利用パスワードや利用者番号等が重要な情報が記載されているので，紛失等しないよう必ず保管しておいていただきたい。

東北大学科学計算システムへのログインやプログラムの実行方法など，基本的な利用方法についても，前述の情報提供ページに利用者講習会の動画等と共に用意されている。

3.2. 利用相談

プログラムの最適化や利用上の不具合などの相談については，東北大学サイバーサイエンスセンターで利用相談窓口をご用意いただいている（連絡先は上述の情報提供ページ参照)。東北大学科学計算システムのベクトル計算機 SX-ACE は，これまでの本学高速計算サーバとアーキテクチャが異なり，その性能を十分に発揮するプログラムの作成には若干の工夫が必要となるため，このように相談窓口として手厚い人員をご用意いただけていることは大変心強い。

3.3. 成果報告

本学で運用していた高速計算サーバでも同様だったが，大きな規模のシステムを整備・維持・し拡充を進めていくためには，そのシステムがどれほど役に立っているか，その成果を示すアピールしていく必要がある。東北大学サイバーサイエンスセンターでも，大規模科学計算システムを利用して得られた研究成果の提出が求められている。本学のユーザについては，岩手大学情報基盤センターにて取りまとめることとなっており，ご協力いただきたい。

また，大規模科学計算システムを利用して得られた研究成果を論文等で発表する際にも，東北大学サイバーサイエンスセンターを利用した旨，明記していただきたい。この際の例を以下に示す。

「本研究の実験結果の一部は、東北大学サイバーサイエンスセンター大規模科学計算システムを利用して得られた。」

Part of the experimental results in this research were obtained using supercomputing resources at Cyberscience Center, Tohoku University.

4. 科学技術計算ソフトウェア

本学で運用していた高速計算サーバ等では，東北大学科学計算システムで利用できるソフトウェアとして挙げた Gaussian09 の他にも，ANSYS や Pointwise など様々な科学技術計算ソフトウェアを提供していた。これらのうち，高度な並列計算で利用される ANSYS Research CFD とその並列計算ライセンス ANSYS CDF HPC については，本学で契約したものを東北大学科学計算システムで利用できるようにしていただいている。

他の, 高度な並列計算で使用されないものについては, 基本的にはライセンス契約のみを行い，各研究室等の計算機にインストールして利用していただくこととした。ただし，東北大学科学計算システムで利用できる ANSYS Research CDF については，GUI による事前・事後の処理が必要なため，岩手大学内で利用できるライセンスも用意している。

研究室等の計算機にインストールする際に必要となるインストールメディア（DVD 等）は，情報基盤センターにて貸し出すこととしており，使用の際に必要となる，ライセンスサーバ等の情報も，この際伝えることとしている。

なお，岩手大学内で利用できるソフトウェアについては，研究室でこれら科学技術計算ソフトウェアを使用するための計算機を用意するのが難しい場合や，本格的に使用する前に，試験的に使用される場合などのため，本学教育研究用仮想化基盤上にアプリケーションサーバ(appli.cc.iwate-u.ac.jp)を構築し，ここでも利用できるようになっている。アプリケーションサーバの OS は Linux で，ユーザ登録の申請等は特に必要なく，学内からは SSH でリモートログインできる。

2916 年 9 月より稼働している教育研究用コンピュータシステムでは, 科学技術計算ソフトウェアとして, 本学全構成員が私物の PC 等にもインストールして MATLAB を使用できる, MATLAB TAH ライセンスも新たに加わっているが，これについては，本報告内別稿にて紹介する。

現在の教育研究用コンピュータシステムとして利用できる科学技術計算ソフトウェアをその利用形態ごとにまとめたものを表 2 に示す。

表 2 科学技術計算ソフトウェアの配置

東北大学科学計算システムで利用できるもの
● ANSYS Research CFD（5task, 16 並列） ● ANSYS CFD HPC（16 並列，上記とあわせ最大 32 並列）
東北大学科学計算システムで利用できるもの
● ANSYS Research CFD（5task, 16 並列） ● ANSYS CFD HPC（16 並列，上記とあわせ最大 32 並列）
研究室等の計算機にインストールして利用できるもの（アプリケーションサーバでも利用可）
● ANSYS Research CFD（5task, 16 並列） ● ANSYS Academic Teaching Mechanical and CFD（5task1 式） ● Pointwise（2 式） ● FieldView（8 並列 1 式） ● Gaussview（Windows 版サイトライセンス） ● Mathematica（ネットワークライセンス 10）
情報基盤センターサーバ（sas.cc.iwate-u.ac.jp）でのみ利用できるもの
● SAS（同時利用数無制限）

5. 利用講習会等

東北大学科学計算システム利用に先立ち，以下の講習会等を実施した。

2016 年 7 月 1 日　東北大学サイバーサイエンスセンター大規模科学計算システム利用講習会
2016 年 8 月 31 日　情報基盤センター新システム講習会 第 4 部「科学技術計算」

また，東北大学サイバーサイエンスセンターで実施された以下の講習会も，東北大学と岩手大学をテレビ会議システムで結び，岩手大学で受講できる形態で実施していただいた。

2016 年 9 月 26 日　UNIX 入門
2016 年 9 月 27 日　大規模科学計算システムの利用法
2016 年 9 月 28 日　OpenMP プログラミング入門
2016 年 9 月 29 日　MPI プログラミング入門
2016 年 9 月 30 日　SX-ACE における高速化技法の基礎
後半はハンズオンのため東北大学のみで受講可

東北大学では同様の講習会を毎年春と秋に実施されており，来年度以降も同様に，岩手大学から受講させていただけることとなっている。

6. 利用状況

東北大学科学計算システムの利用状況については本報告内の運用報告「東北大学サイバーサイエンスセンター大規模科学計算システム」を参照されたい。正式利用開始から 7 カ月が経過しているが，登録ユーザ数，利用ノード時間，実行ジョブ数など増加しており，順調に利用が進んでいることがわかる。

7. おわりに

本稿では，新たに機関利用させていただくこととなった，東北大学大規模科学計算システムの概要および利用方法とそれに伴う本学科学技術計算ソフトウェア利用方法，利用促進のための講習会と現在の利用状況について述べた。

最後に，この機関利用は，東北大学サイバーサイエンスセンターの皆さまはじめ，本学の多くの方々のご協力により実現できたことであると感謝しております。今後も，ユーザの皆さまとともに，研究のためのより良い計算機環境を実現していきたいと思います。

【特集2】
電子メール

岩手大学の電子メールの概要

電子メールが届くまで

情報基盤センター
川村暁，中西貴裕
技術専門職員　加治卓磨

1. はじめに

岩手大学情報基盤センターは，岩手大学内の情報基盤の整備，運営，維持管理を担っている。ネットワーク上で用いられるサービスである電子メールについても，平成 9 年導入の教育研究用コンピュータシステムから全構成員へのアカウント発行を開始し，システム・仕組み等の数度かの更新を経て現在に至る。

電子メールが一般的に利用されるようになるに従い，電子メールの黎明期にはなかった問題が顕在化している。大量に届く迷惑メールや，攻撃を指向した電子メール（標的型メール）は，電子メールの利便性を損なうだけではなく，利用者または組織へ被害が及ぶ可能性もあるため，対策することが求められている。

このような状況を受け，現在運用している電子メールシステムは，多段防御の考え方で構成されている。本稿では，平成 28 年 9 月に導入された新システムの電子メールシステム部分の概要を示す。ここでは，ネットワークで用いられるレイヤを踏まえた（沿った）記述にはせずに，利用者にメールが届く経路で何が行われているのか？に着目して記した。このため，ネットワーク的な厳密性・狭義の電子メールシステムからは距離がある記述となっている。

なお，情報セキュリティ上の観点から，利用している製品名や詳細な情報については伏せて記している箇所があることを了承頂きたい。

2. 電子メールシステムの概要

図 1 に，岩手大学情報基盤センターで運営している電子メールシステムの概要を示す。図左側インターネット(A)から，図右側，メールサーバ(E)の経路で処理されている。前述の通りネットワークのレイヤに基づく考え方では厳密性に欠けるが，利用者にメールが届く経路で何が行われているのか？に着目して記したためである。ご了承頂きたい。

図 1　岩手大学の電子メールシステムの概念図

(D)のウイルス対策ソフトウェアは，論理的にはサーバとして振る舞うため記載している。

図１は，インターネット側から本学に設置された電子メールサーバまで，どのようにメールが届いているのかを示している。ユーザが学内からメールを利用する場合は，(E)の電子メールサーバにアクセスすることになる。ただし，ユーザが外部向けに電子メールを送信する場合は，(E)の電子メールサーバにメールを送り，(E)→(D)→(C)→(B)→(A)となることに注意してほしい。

図中，(A)から(E)について，順に記す。

(A) インターネット

本学では，国立情報学研究所（NII）が構築，運営している学術情報ネットワーク [1]（SINET: Science Information NETwork．現在は SINET5）に接続している。

(B) ファイアウォール

岩手大学へ接続してくる全ての通信について，本学のキャンパスネットワーク運営ポリシー・利用目的と，セキュリティ上の制約を踏まえた上で接続の可否を決定する装置である。

自由度・利便性とセキュリティは相反する部分があるため，ファイアウォール設定は，利用者の利用ニーズとセキュリティ的な制約条件に基づき，暫時ファイアウォールの設定を改定しながら運営している。

電子メールについて記すと，ポート番号及び IP アドレスで制御がなされている。

(C) 迷惑メール対策（除去）機器

迷惑メールや攻撃メールなどを判別し，隔離する機能を持った機器 [3]である。隔離されたメールは，然るべき手順を踏むことで復帰させることが出来る。

(D) 電子メールサーバ上のウイルス対策ソフトウェア [4]

電子メールは，電子メールサーバ上に構築されたウイルス対策ソフトウェアで処理される。ウイルス対策ソフトウェアで危険なメールだと判別された場合，攻撃を意図した添付ファイルを除去する，件名にフラグを付けるなどの処理 [4]がなされた後，電子メールサーバに送られる。

なお，情報基盤センターが教職員対象で学内に配布しているウイルス対策ソフトおよび教育用端末室に導入されているソフトウェアとは別のソフトウェアになっている。

(E) 電子メールサーバ

電子メールサーバは，電子メールの送受信を処理する。電子メールサーバに一般的に施される不正なメールやセキュリティ面を踏まえた設定を施している。また，送受信する電子メールは，(D)に示したウイルス対策ソフトウェアでウイルスチェックを行っている [4]。

3. システムとしての電子メールのセキュリティ対策

第２章で触れたとおり，各機器において電子メールのセキュリティを高める工夫を施している，この考え方は多層防御的な考え方となっている。

インターネットから入ってきたところと，実際にメールを配信するときと，多段階で防御を行う構成になっている。このうち，電子メールサーバよりもインターネット側に位置する迷惑メール対策機器については，参考文献 3)を参照して欲しい。本機器は迷惑メールを除去する為に設置しているので，これが機能停止となると迷惑メールの除去に関して問題が生じる。機器の故障に対応するため，機器を冗長化するなどの対策を行っている。

電子メールサーバに導入されているウイルス対策ソフトウェア [4]は，前述の通り，情報基盤センターが教職員対象で学内に配布しているウイルス対策ソフトおよび教育用端末室に導入されて

いるソフトウェアとは別のソフトウェアとしている。これは，全てを同一のもので統一した場合，たまたま当該のソフトウェアだけが脅威を検知できないため筒抜けになる，という事態を軽減するためである。異なるソフトウェアがあれば，それぞれの対応動作が異なることを期待できるため，総合的なセキュリティレベルが向上する，と考えたためである。

4. まとめ

岩手大学情報基盤センターで運用している電子メールシステムについて，セキュリティ面から整理した。様々な制約を踏まえつつ，多段防御を構成するようなメールシステムになっていることを示した。

このような構成にしていても迷惑メールや攻撃を指向した電子メールは日々届いているので，十分に注意しつつ利用してほしい。また，電子メールをふくめ，セキュリティ的に相談したいことなどがある場合は，岩手大学 CSIRT (Computer Security Incident Response Team)[2]までご連絡いただきたい。なお，このメールアドレスは受付専用となっていることを申し添える。

CSIRT（Computer Security Incident Response Team）
ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください
e-mail: csirt@iwate-u.ac.jp
Tel: 019-621-6096 内線（6096）

技術的な相談は，これまで通り，情報基盤センターまでご相談いただきたい。

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp

参考文献

1) 学術情報ネットワーク SINET（オンライン），入手先（https://www.sinet.ad.jp/）（参照 2017-02-10）.
2) 岩手大学 CSIRT：岩手大学情報基盤センターお問い合わせ（オンライン），〈https://isic.iwate-u.ac.jp/center/inquily.html〉（参照 2017-03-10）.
3) 迷惑メール対策機器：岩手大学情報基盤センター（オンライン），〈https://isic.iwate-u.ac.jp/usersguide/security/antispam.html〉（参照 2017-03-10）.
4) ウイルス付きメール対策機器：岩手大学情報基盤センター（オンライン），〈https://isic.iwate-u.ac.jp/usersguide/security/kaspersky.html〉（参照 2017-03-10）.

電子メールの利用について

教職員と学生の場合

人文社会科学部
後藤尚人

1. はじめに

岩手大学の教職員は岩手大学ドメインの電子メール（～@iwate-u.ac.jp：以後「大学メール」と表記）をよく使っているが、学生はあまり使っていない。教職員にとって大学メールは業務上必要なツールであるものの、学生には、業務という概念はなく、使われている電子メールは、プライベートなコミュニケーション・ツールとしての携帯メール（スマホを含む）になる。もっとも、LINE などの普及に伴い、携帯メールも使われる頻度は下がっていると思われる。

教職員は仕事の道具として大学メールを使い、学生はプライベートで携帯メールや LINE を使う。おおむねこれが現状認識だとして、「大学メールの利用」という観点から、どのような問題が生じているのか、また、現状を改善する方策は可能なのかについて、考えをまとめてみる。

2. 教職員のメール利用：公私混同

教職員は大学メールを使う頻度が高く、利用促進的には問題がない。とはいえ、利用頻度が高いがゆえに、フィッシングメール等に引っかかってしまう確率も相対的に高くなる。メール利用時におけるセキュリティについては、情報基盤センターが出している『情報セキュリティハンドブック 電子メール編』（2016）等を参照していただくとして、ここでは大学メールの利用目的について言及しておきたい。

上述のように、教職員は大学メールを業務遂行のための道具として使うことになっている。ところが、業務にとどまらず、《私用》での利用がないわけでもなさそうで、各自が何のために大学メールを使うのか、再認識する必要がある。ウイルス感染やフィッシングメール等に引っかかった原因が《私用》メールだったとして問題化すると、メディアの格好の餌食になるだけでなく、各方面に多大な迷惑をかけることになってしまう。

ただし、公用と私用との区別は明確でもなく、そこにはグレーゾーンが含まれている。たとえば教員が書籍をアマゾンで購入するとして、受注確認メールのアドレスを大学メールに設定している場合、その書籍が教育研究目的に合致するのか否かで評価は分かれそうであるが、購入する書名だけでそれを判断するのは難しい。後藤が担当している人文社会科学部国際文化課程の文化システムコース（旧カリ）では、「アイドル文化における自意識消費」や「アニメにおける銭湯という表象」という卒論も出てくるため、指導教員がアイドル本やアニメ（に関する文献）を購入したとしても、教育研究目的に合致している。また、教員の個人研究費は削減され続けており、公費で賄えない分は私費で購入するしかないため、公費購入ならば公用で、私費購入ならば私用と区別することも有用とは言えない。

公費購入で教育研究目的以外の物品は購入しないとしても、私費で教育研究目的のものを買うこともあるし、アマゾンや楽天などの通販ショップでのやり取りに大学メールを使っている場合、あるときは公用であって、あるときは私用という場合も考えられる。とすれば、通販ショップで

のやり取りに大学メールを使っていたとしても、そのことだけで白黒つけるのは難しい。

このように、教職員が私用で大学メールを使っているかどうかは、外形的には判別しにくいため、最終的には利用者本人のモラルの問題になる。教職員自身が、私用で使っていると思っているなら、そうした通販サイトの連絡には、大学メールではなく、他のプロバイダ等のメールを使うべきであろう。

3. 学生のメール利用：使わない

学生は入学年度に「情報基礎」を受講することもあり、初年度は大学メールもそれなりにチェックしているものの、仲間同士の LINE や SNS でのやり取りが増えるにつれて、大学メールは忘れさられてしまう。学務関連の連絡事項や授業でのレポート提出等も「アイアシスタント」でできるため、学生が大学メールを使う機会もあまりない。

ほとんど私用でしかメールを出したことがない学生が、教員宛に携帯から送ってくるメールは、往々にして、メールの件名（subject）がなく、差出人名は（おまじないのような）ID なので誰のことか分からず、宛先もなく、本文はコンテクストのない単語の羅列で、差出人にしかわからない内容になっていたりする。

携帯メールだと自身を名乗らなくても相手の携帯のアドレス帳に自身のアドレスが登録されていれば送信者自身の名前が相手の携帯端末に自動的に表示されるため、学生は教員宛に送るメールも同様に教員のパソコンに送信者の名前が表示されると勘違いしているのか、さすがにそれはないとしても、日頃の習慣で、つい自身を名乗らずにメールを送信してしまうのかもしれない。

上述の文化システムコースでは、コース担当教員とコースの所属学生全員を登録したメーリングリスト（ML）を作り、学生のアドレスは大学メールに加えて、本人の希望により携帯等のアドレスも加えていた。その ML を利用するに際しては、携帯等のアドレスを変更した場合には速やかに届け出ることや、ML に送信する場合は、件名を明記し、メール本文に送信者が誰なのかが分かるように書くことなどを注意したこともあり、送信者が誰なのかが分からないメールはほとんどなかったが、宛先不明でエラーとなるアドレスがよく出てきた。学生は機種変更に伴ってキャリアを換えたり、人間関係をリセットしたいときなどに自身のアドレスを変更し、友人等にはその旨を連絡しても、ＭＬ管理者への連絡はなおざりにしてしまう。

文化システムコースの ML では、学生の携帯等のアドレスにメールが届かなくなっても、学生の大学メールのアドレスも登録していたので、学生は自身の大学メールで連絡事項等を確実に受け取ることができたにも関わらず、ひとたび大学メールを使わなくなると、大学メールにアクセスしなくなるため、情報がコース専攻生全員には行き渡らなくなってしまう。

大学メールの転送サービス（情報基盤センター）に関しても例外ではなく、大学メールを自身の携帯へ転送するように設定した後、携帯メールのアドレスを変更しても大学メールの転送設定のことは忘れてしまい、そのままにしておく学生がいる。自身に届かないメールについては、宛先不明の迷子メールになっていても、それを知る術はないため、いつまでも放置され続けてしまう。

そのような状況になると、教員側から学生に直接メールで連絡することができなくなる。学生の大学メールのアドレスに急を要する連絡事項のメールを送っても、大学メールをチェックする習慣が消えてしまった学生がそのメールを見ることはない。締切に遅れたレポートを学生が大学

メールに添付して送ってくることがあり、その学生なら教員側からのメールをチェックするだろうと思っても、学生が大学メールを使うのは添付ファイルを送信する場合だけで、一度メールを送信してしまえば、その後は大学メールをチェックすることはなく、連絡は途絶えてしまう。

このように学生が大学メールを使わなくなってしまうと、教員側から学生への連絡手段が制限されてしまう。卒論指導も終盤に入った 11 月に、学生がゼミに出てこなくなったため、メールで連絡をとろうとしたら、大学メールは音信不通で、学生の携帯への電話は「現在使われておりません…」となり、さらに家族もいる自宅の固定電話も「現在使われておりません…」となって、母親の携帯電話にメッセージを入れても当該学生からは反応がなく、父親の携帯電話を通じてようやく卒論指導に関する連絡が取れたということがあった。こうした事態は、学生が大学メールをチェックする習慣さえあれば、回避できたはずである。

4. 学生に大学メールを使わせる方策：授業関連で使う

学生がプライベートで LINE 等を使うのは当然で、そこに大学メールが入り込む余地はないし、大学メールを使う必然性もない。けれども、学生が社会に出た後、企業や事業所で使うメールは大学メールと同じように、パソコン（やスマホの Web メールなど）でやり取りすることになると思われるため、大学メールを使いこなせるに越したことはない。

とはいえ、学生に大学メールを使えと言っても、必要がないものは使われない。ならば、学生が大学メールを使わなければならない環境を作ればいいはずである。

たとえば、授業にかかわる教員と学生のやり取りは全て大学メールで行うという方針を徹底する、としてはどうだろうか。

授業を欠席する場合は、授業開始時間前までに大学メールで欠席する理由を明記して連絡すれば無断欠席扱いにはしないとか、アイアシスタントで提出するレポートも、締切を過ぎた場合には、大学メールに添付されたものであれば（減点はするものの）受け付けるとか、学生が教員に授業関連の連絡をする場合に、メールならば大学メールのみ受け付けるようにすれば、必然的に大学メールの使用頻度は上がると思われる。また、学科やコース等で個別に ML を立ち上げる場合にも、登録アドレスは大学メールに限り、携帯アドレス等は受け付けないようにするのも効果的だと思われる。

教員と学生間の連絡は基本的には公務であるため、メールを利用する場合は、必ず大学メールを使うというのは理にかなっている。かといって、大学メール以外はいっさい禁止ということでもなく、公務ではないと判断した場合や授業に直接関わらないような場合で LINE の方が便利であれば、LINE を使ってもいいし、その時どきで臨機応変に対応すればいい。

5. メールやネットでの表現：文書作成の作法

この原稿を見れば分かるように、日本語の文章表現には句読点の打ち方や段落のわけ方等の決まりがある。たとえば段落冒頭は一文字字下げし、段落は一つのまとまった内容を単位とするなどは学校で習うはずである。けれども、ネット環境に慣れ親しみ、あまり新聞や本を読まないと思われる学生のレポートは、字下げはなされず、段落ごとに空行が入っていることが多い。もっともこの現象は学生にのみ見られるものでもなく、後藤が編集者となった文献において、ある大学教員の原稿が、ブログ調で書かれ、字下げはなく、段落というまとまりもなく、文章が自由な改行によって《詩的》に表現されていて驚いたことがある。お願いしていた原稿はエッセーでは

なく論文だったため、他の原稿と揃えるため、こちらで文章をまとめて段落を作り、論文調に整える作業が必要となった。

メールやブログでの書き方に字下げや段落のまとまりを要求しても、そうした作法はもともと文字数や枚数に制限あり、むやみに空行を作ることが許されなかった時代のもので、そもそも枚数という概念がないネット時代においては説得力を持たないのかもしれない。字下げをしないで段落の切れ目に空行を入れる手法は、HTML 文書においては行頭の（半角）スペースが認識されず、行頭は常に詰まって字下げができないことから、改行後の段落を見やすくするためになされた工夫であったが、改行ごとに空行があれば、改行した次の行を目立たせるという字下げ本来の趣旨にも沿うため、この手法にも一理あると思われる。

しかしながら、メールの書き方に見られるように、句点を打つようなところで適当に改行したり、読みやすくするために適度に空行を入れるという書き方に慣れてしまうと、いつの間にかそれがあたり前になり、ゼミでの資料も同様の作法で作成されてしまう。内容さえよければ、文書作成の作法はどうでもいいという判断をしている教員も多いとはいえ、アカデミックな文書作成の作法はまだ生きていることを確認する必要はある。

言葉は時代と共に変化してゆくものだとすれば、表記法も、いずれはネットでの作法が主流になり、字下げなどは古くさい風習になってしまうかもしれない。けれども、現時点では新聞や研究書などの出版界ではネット流の作法が主流にはなっていないのだから、大学においてはきちんとした文書作成の作法を守るように指導してゆきたい。

標的型攻撃メール訓練の実施報告

情報基盤センター
川村　暁

1. 標的型攻撃メール訓練

電子メールは，業務に欠くことの出来ない基本的なツールの一つである。普及して利用されていることから，電子メールを攻撃の一手段として，悪意のある者に悪用される場合がある。このようなメールにより，情報流出などへ至った事例がたびたび報道されている。特に，攻撃対象とする組織に最適化した文面の攻撃用のメールを送付する，標的型攻撃メールも散見される。

このような状況を受け，組織における外部からの攻撃への耐力を高めるため，標的型攻撃メール訓練が実施されつつある。岩手大学においても，この種の攻撃に対する本学の現状を測り今後の対策に生かすことと，および，このような攻撃があり得ることを広く周知することを目的として，全教職員を対象とした標的型攻撃メール訓練を実施した。

本稿の記載は，諸般の事情によりごく簡単なものとなっていることをご了承いただきたい。

2. 標的型攻撃メール訓練の実施方法

この訓練の実施では，以下の段階を踏んで実施した。

１．情報基盤センター内から全学的な委員会等に提案して実施することを決定する
２．全教職員に本訓練の事前通知を行う
３．訓練メールを全教職員宛で送付する。文面は２種類用意し，ランダムに送付した
４．結果の集計と評価を行う

訓練メールは２種類用意しそのどちらかを，一人一通受け取っている。

なお，本訓練の評価結果については，2017 年度の情報セキュリティセミナーなどを通じて全構成員に周知する計画としている。

3. 標的型攻撃メール訓練の結果

全体的な傾向として，セミナーを未受講だった方の訓練メールを開封した率（開封率）が高い傾向が見られた。また，事務・技術職員よりも教員の開封率が高めになった。

訓練メールは２種類用意しランダムに送付したが，文面により開封率に大きな差が出た。非常に巧妙な標的型攻撃メールの対応が非常に難しいことはよく知られている [1)~3)]が，本訓練でも同様の傾向が見られた。

4. 来年度以降の訓練の実施について

本訓練は，本学の標的型攻撃メールに対する耐力を高めることと，現状を把握することを目的として実施した。避難訓練などと同様に，各構成員の対応力を醸成するためには，定期的な訓練の実施が必要であろうと考えている。

最後に，本訓練の実施にご協力いただきました岩手大学の教職員の皆様方，および，実務を担った情報基盤センタースタッフに感謝いたします。

参考文献

1) 標的型攻撃は“防げない”：日経 ITPro（オンライン）
〈http://itpro.nikkeibp.co.jp/article/Watcher/20140411/550093/〉（参照 2017-03-24）.
2) 標的型攻撃、脅威の手口：日経 ITPro（オンライン）
〈http://itpro.nikkeibp.co.jp/article/COLUMN/20140317/544182/〉（参照 2017-03-24）.
3) 標的型攻撃への対策：総務省 国民のための情報セキュリティサイト（オンライン）
〈http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/07.html〉（参照 2017-03-24）.

【一般】

学内カンパニー「iFive」の活動

スマートフォン向けアイアシスタント補助アプリ「がんちゃんねる」の開発

工学研究科電気電子・情報システム工学専攻
村上雅俊

1. 学内カンパニーとは

岩手大学が行っている事業に，「ものづくりエンジニアリングファクトリー」があります[1)]。その中の活動の一つとして学内カンパニー活動があります[2)]。学内カンパニーとは，学生たちが模擬的な企業活動を学内で行うことを通して実践力と社会性を学ぶことを目的とした活動で，社会に貢献できる学生を送り出すことを目指しています。

2. 学内カンパニーiFive

iFive は IT 系の学内カンパニーです。企業理念は「IT で岩手大学を盛り上げる」です。そのため，岩手大学が所有している有益な情報のスピードと質を向上させることを目的に現在活動しています。

3. iFive の沿革

iFive の活動は 2016 年から始まり，今年で 2 年目になります。実践的にソフトウェアを開発したい，またエンジニアとしての能力を付けたいとの思いで，初めは情報システム工学科の学生が 1 人で iFive を発足しました。次第に人数を増やし，現在は 9 人で活動しています。

4. iFive の活動

有益な情報として我々が最初に着目したのが，アイアシスタントです[3)]。アイアシスタントとは，シラバスや授業記録に加え，個人向けの情報，科目ごとの電子掲示板や課題・レポート，ドリルにアンケートなど，受講期間を通じて，教員と学生が双方向的に活用できる多彩な機能を備えた学習支援システムです。

アイアシスタントに掲載される個人向けの情報として，奨学金や授業料など重要な情報が含まれます。そのため，アイアシスタントに掲載されている情報は岩手大学が学生に提供している有益な情報と言えます。

しかし，アイアシスタントは PC 向けのソフトウェアであることと，新着情報が大量にあることから，必要な情報が見つけにくいことが問題でした。

この問題点を解決するために，iFive ではスマートフォン向けのアプリの開発に取り組みました。アプリ名は「がんちゃんねる」です（図１）。「がんちゃんねる」は，アイアシスタントに掲載されている新着情報をスマートフォンで見られます。そのため，場所を選ばず，迅速に情報を得ることができます。さらに検索機能があるため，自分が欲しい情報だけを素早く得ることができます。

図１は，左から「がんちゃんねる」のログイン画面，記事一覧，記事詳細の画面です。アプリを起動すると最初にログイン画面が表示されます。学籍番号とパスワードを入力し，ログイン認証が成功すると，記事一覧が表示されます。ここで上下にスライドするとスクロールして記事を探

すことができます。ルーペのアイコンをタップし，文字を入力すると，その文字を含む記事がハイライトされます。記事のタイトルをタップすると，記事詳細が表示されます。

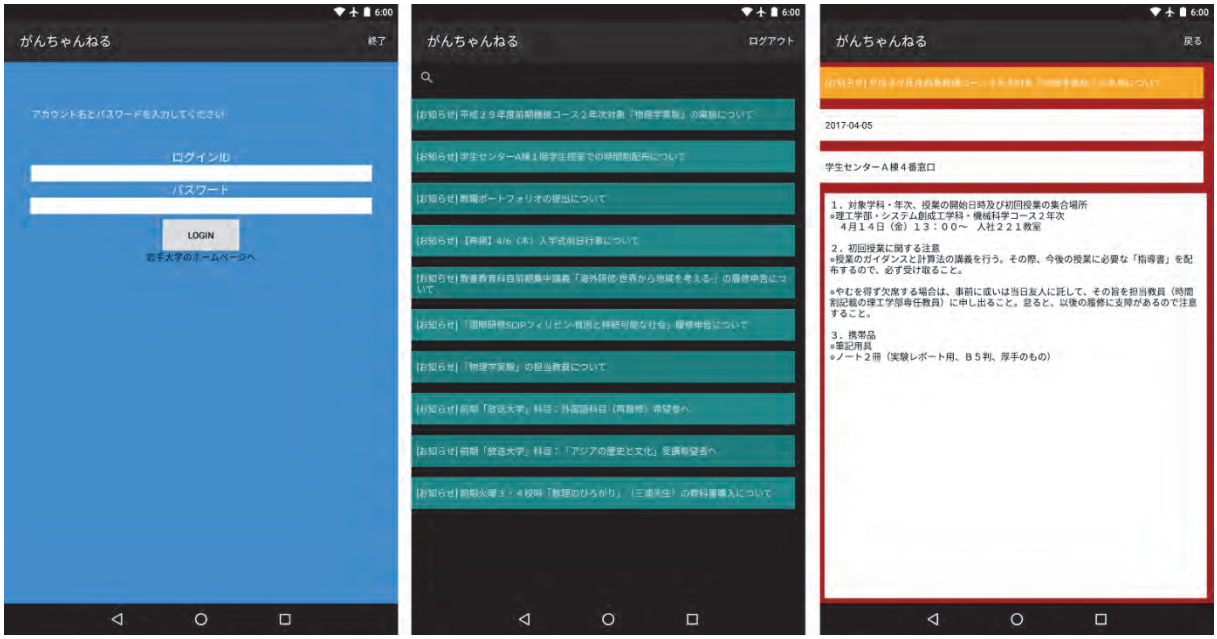


図 1:「がんちゃんねる」のスクリーンショット

5. 今後の課題

Android 版の「がんちゃんねる」はリリースできる段階まで開発が進んでいます。そのため，「がんちゃんねる」をリリースし，アイアシスタントを使用している方々の手にがんちゃんねるが届くようにすることが課題です。配信方法としては，Google Play を予定しています。また，iOS 版の「がんちゃんねる」も，現在，開発を進めています。

なお，リリースに向けては，「がんちゃんねる」の著作権に関することや，アプリ名の商標に関することも解決しなければなりません。カンパニーとして活動するには，使い勝手の良いアプリを作ることだけではなく，その周辺に存在する様々な案件についても対応しなければならず，勉強中です。

6. 今後の展望

「がんちゃんねる」は現段階ではアイアシスタントの情報のみ取得できますが，他の情報も得られるように拡張していきたいと考えています。具体的にはサークルや大学生協，近隣地域などの情報です。また，「がんちゃんねる」とは違う岩手大学を盛り上げるアプリを考察中です。さらに iFive は，技術の勉強会を開催し，技術交流の場も提供したいと考えています。それにより，各々がエンジニアとして高い技術力を付け，エンジニア同士のつながりが増えることを期待しています。

参考文献

1) 岩手大学理工学部附属ものづくりエンジニアリングファクトリー（オンライン）〈http://www.ef.iwate-u.ac.jp/〉（参照 2017-03-07）.
2) 岩手大学ものづくりエンジニアリングファクトリー：学内カンパニー（オンライン）

〈https://iwate-u-gakunai-company.jimdo.com/〉（参照 2017-03-07）.
3)　岩手大学教育推進機構：アイアシスタント（オンライン）
〈http://uec.iwate-u.ac.jp/ia/ia/top.html〉（参照 2017-03-07）.

【活動報告】

平成 28 年度ネットワーク連絡会活動報告

情報基盤センター
川村　暁，中西貴裕

1. はじめに

本年度は，例年通り年２回の開催とした。また，岩手大学で開催した回においては，昨年に引き続き，クリッカーを用いた会場参加型のアンケートも実施した。

2. ネットワーク連絡会 2016 Summer

日　時：平成 28 年 9 月 9 日(金) 13:30～17:00 (受付開始 13:00)
会　場：岩手医科大学創立 60 周年記念館 9 階　第一講義室
テーマ：医療の現場における情報の取扱いと実践
主　催：ネットワーク連絡会、TOPIC 盛岡 NOC、岩手医科大学、岩手大学情報基盤センター、
　　東北学術研究インターネットコミュニティ(TOPIC)
同時に開催した会合：TOPIC 盛岡 NOC の会　13:00-13:30
ネットワーク連絡会 2016 Summer プログラム

13:00 受付開始
13:30 開会挨拶
13:35-14:20 講演 1
「これからの病院情報システムを支える人材育成の重要性　～医療情報技師のご紹介～」
講師　大阪大学大学院医学系研究科医学専攻 情報統合医学講座 医療情報学
　　准教授 三原 直樹 氏
14:20-15:00 講演 2
「大学病院におけるビックデータ分析とその活用方法について」
講師　岩手医科大学総合情報センター事務室長 齋藤 匡俊 氏
休憩(30 分)
15:30-16:10 講演 3
「被災地支援における TV 会議システムの効果的運用の検討 」（仮）
講師　岩手医科大学総合情報センター事務室 横田 暁史 氏
16:10-16:55 講演 4
「遠隔診療での診察録画情報について」（仮）
講師　岩手医科大学皮膚科学講座研究員 小野寺 好広 氏
17:00 閉会

17:30 情報交換会　岩手医科大学「木の花会館１階」
参加者：４２名（情報交換会参加者２６名）

3. ネットワーク連絡会 2017 Winter

ネットワーク連絡会 2017 Winter は，講師による講演を３つと，クリッカーを用いた会場参加

型の意見交換会を行い，集約した参加者のいまの考えを今後の活動に活かすことを考えた。

3.1. ネットワーク連絡会 2017 Winter

日　時：平成 29 年 1 月 23 日(月) 13:30～17:00 (受付開始 13:00)

会　場：岩手大学図書館 2F 生涯学習・多目的学習室

テーマ：教育・地域での ICT 活用

主　催：ネットワーク連絡会、TOPIC 盛岡 NOC、岩手大学情報基盤センター、
東北学術研究インターネットコミュニティ(予定)

同時に開催する会合：TOPIC 盛岡 NOC の会 13:00-13:30

ネットワーク連絡会 2017 Winter プログラム

13:00 受付開始

13:30 開会挨拶

13:35-14:35 講演 1

「ICT を活用した理科教育」

講師　岩手大学 教育学部 教授 名越 利幸 氏,
岩手大学 教育学研究科教職実践専攻（教職大学院） 黒坂 優 氏

休憩(20 分)

14:55-15:40 講演 2

「岩手県統合型 GIS「いわてデジタルマップ」の概要について」

講師　岩手県 政策地域部 情報政策課 木村 幸地 氏

休憩(15 分)

15:55-16:40 講演 3

「組織での情報セキュリティ対策について」

講師　東日本電信電話株式会社 青山 優子 氏

16:40-17:00

会場参加型クリッカーを用いた意見交換会

岩手大学 情報基盤センター 川村 暁、中西 貴裕

17:00 閉会

17:30-19:00 情報交換会　岩手大学生協 理工学部食堂 2F 「ラボ」

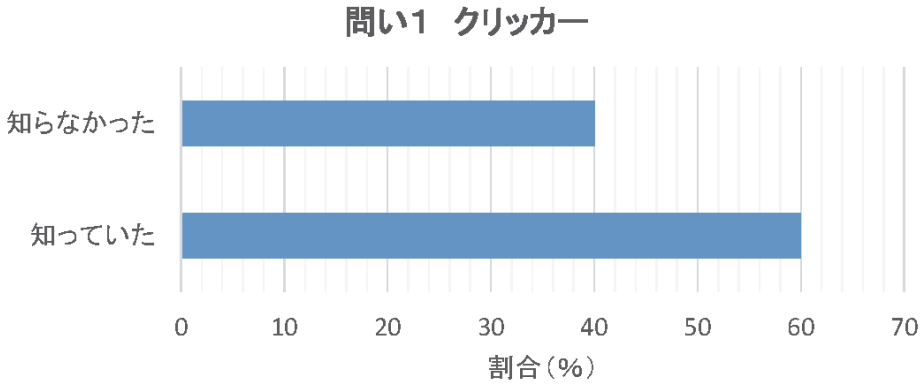
参加者：３０名（情報交換会参加者１９名）

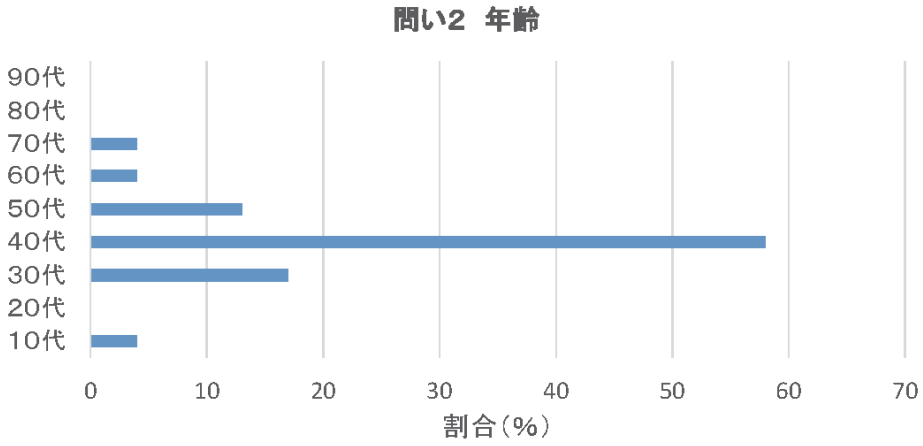
3.2. クリッカー

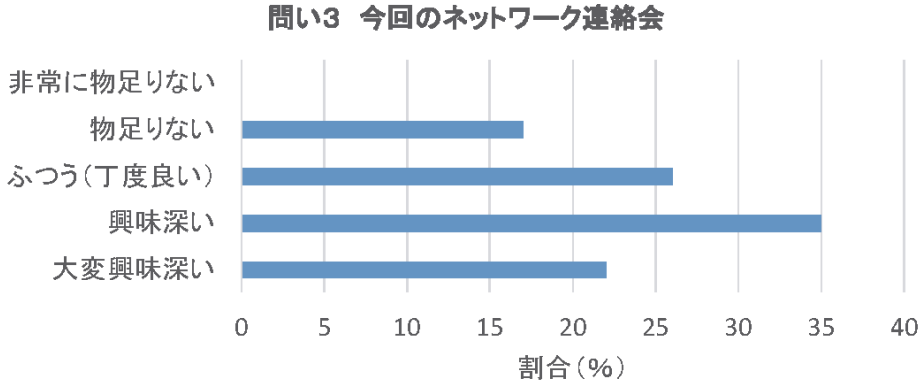
ネットワーク連絡会 2016 Winter では，会場参加型の試みとして，クリッカーを用いた意見交換会を行っている。会場の参加者にクリッカーと呼ばれる小型端末を配布し，質問に対する答え（レスポンス）を返してもらうことにより，参加者の総体を測ることができる。

ネットワーク連絡会 2017 Winter においても，クリッカーを用いた意見交換会を実施した。図１から図４にその結果を示す。

なおクリッカーは，岩手大学学務部が保有するものを用いた。







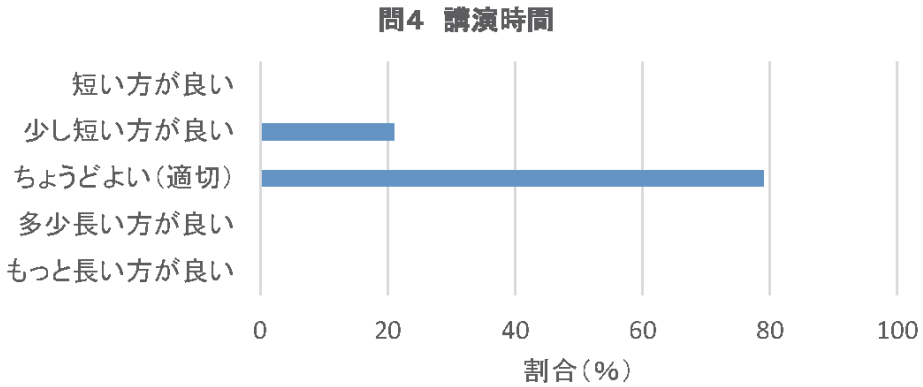
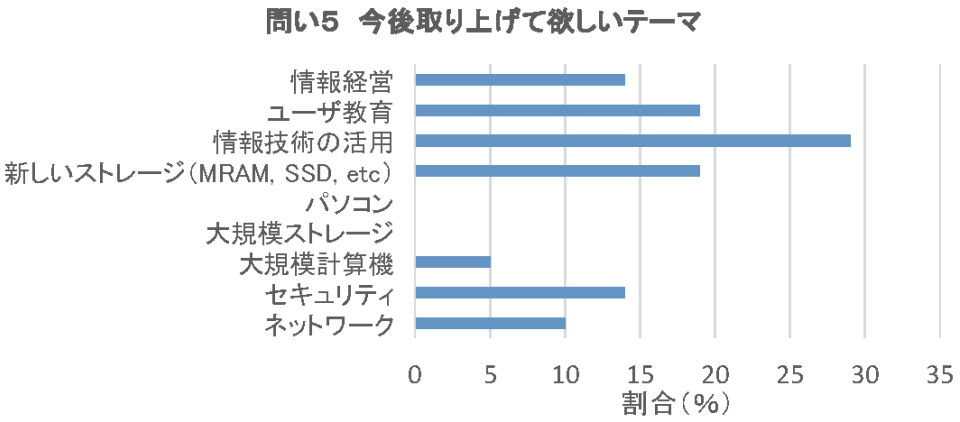
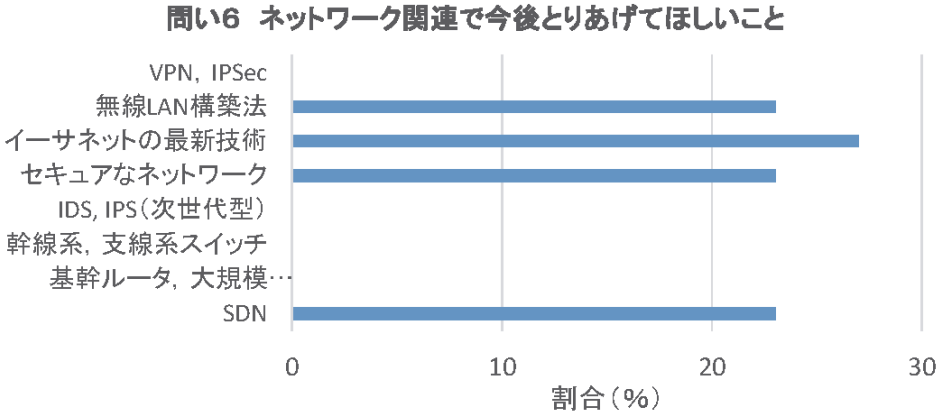
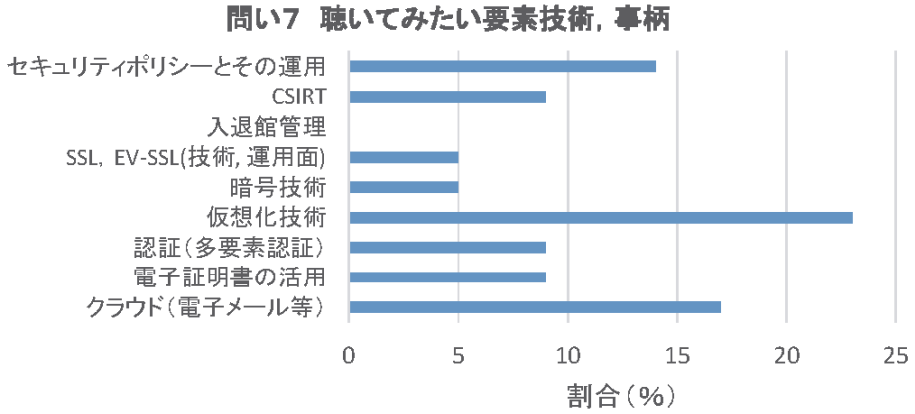


図 1　ネットワーク連絡会 2017 Winter クリッカーによるアンケート結果 (1)







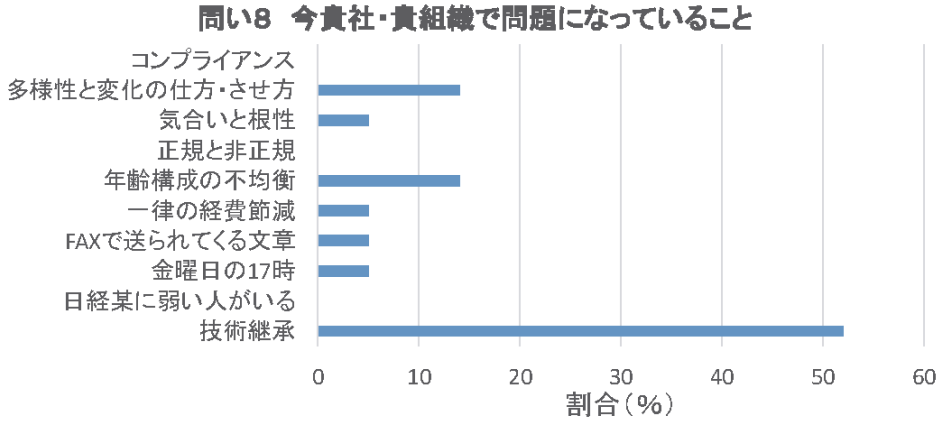
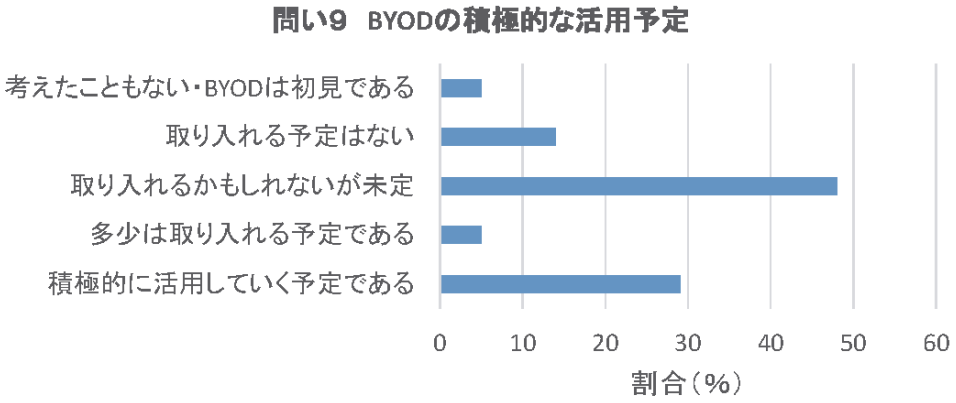
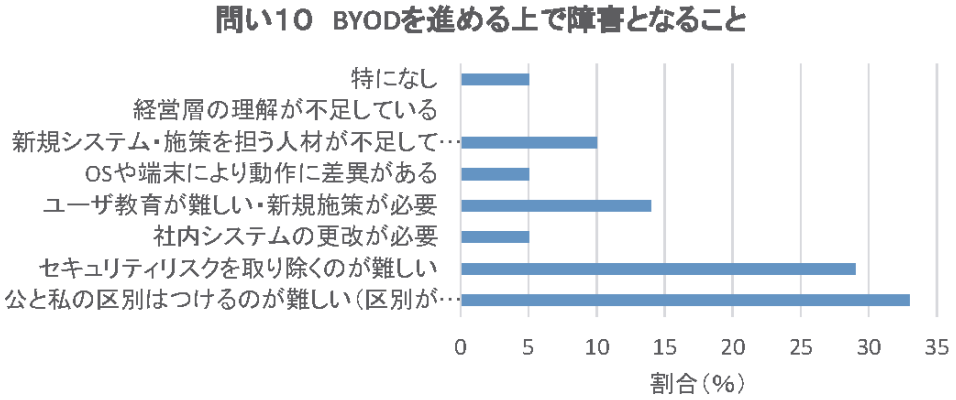
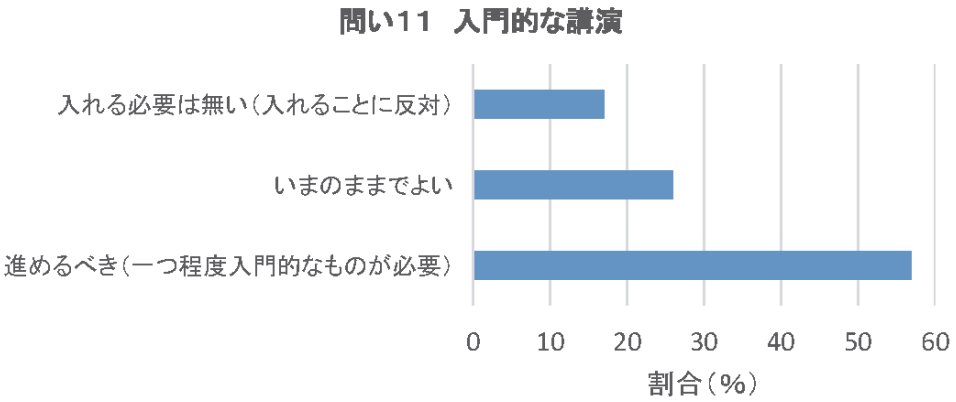


図 2　ネットワーク連絡会 2017 Winter クリッカーによるアンケート結果 (2)







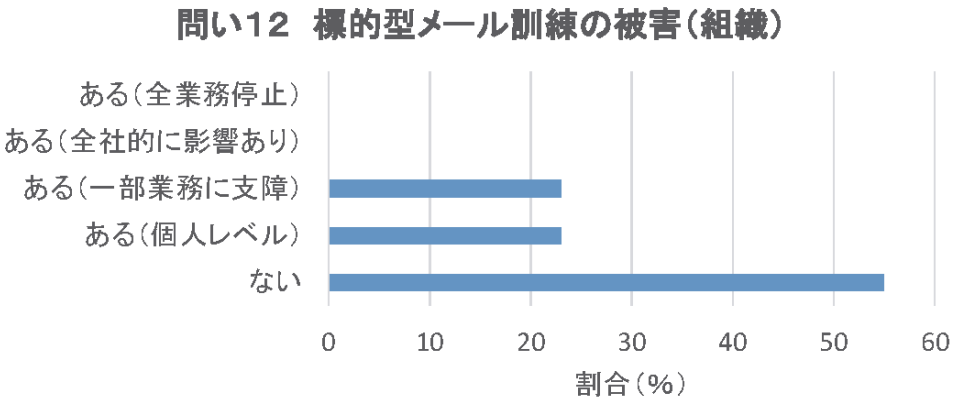


図 3　ネットワーク連絡会 2017 Winter クリッカーによるアンケート結果 (3)

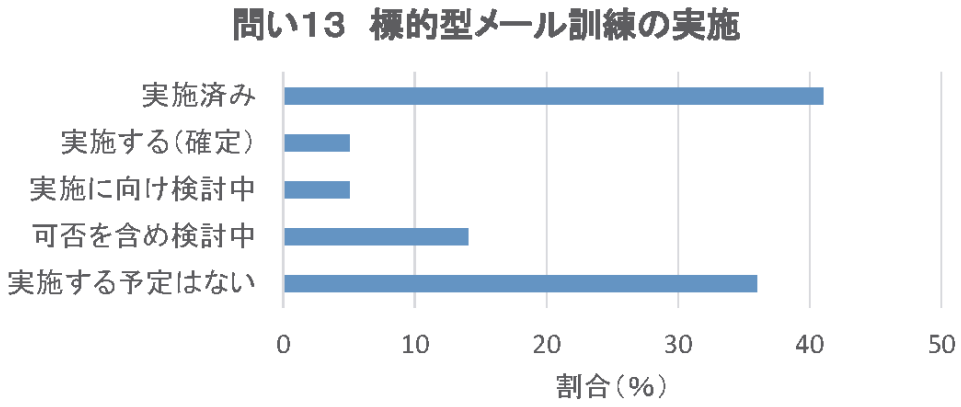


図 4　ネットワーク連絡会 2017 Winter クリッカーによるアンケート結果 (4)

この結果は，匿名で集計されるクリッカーの特性もあり，当会への参加者の総体をよく表していると考えられる。意見交換で示された興味関心・講演内容への要請に基づき，次回以降のネットワーク連絡会を運営していければと考えている。

4.　ネットワーク連絡会総会報告

ネットワーク連絡会 2017 Winter では総会も実施し，「ネットワーク連絡会会則」および「ネットワーク連絡会における個人情報の取り扱いについて」の改正が発議され，賛成多数で承認された。改正は，岩手大学総合情報処理センターから岩手大学情報基盤センターへの組織の変更を反映させたものである。

表 1　ネットワーク連絡会会則の改正部分

改正後	改正前
(省略) 第七条　連絡会に、会長一名、副会長二名を置く。 2　会長は、岩手大学情報基盤センター長をもって充てる。 3　副会長のうち、一名は岩手大学情報基盤センター専任教員をもって充て、もう一名は会員の互選により選出する。 (省略) 第八条　連絡会の事務を処理するため事務局を置く。 2　事務局は、岩手大学情報基盤センター内に置く。 (省略)	(省略) 第七条　連絡会に、会長一名、副会長二名を置く。 2　会長は、岩手大学総合情報処理センター長をもって充てる。 3　副会長のうち、一名は岩手大学総合情報処理センター専任教員をもって充て、もう一名は会員の互選により選出する。 (省略) 第八条　連絡会の事務を処理するため事務局を置く。 2　事務局は、岩手大学総合情報処理センター内に置く。 (省略)

5.　今後の展望

ネットワークとその周辺に関する講演を聴き，またネットワークを通じた交流の場としてのネットワーク連絡会は大きな意味があると思われる。今後も，岩手におけるネットワーク関連コミュニティの中核的な活動の場として，ネットワーク連絡会を発展させていくように努めて行きたい。

クリッカーを快くお貸しいただいた岩手大学学務部に感謝いたします。

情報技術部の業務内容について

情報基盤センター　技術室長
栗田宏明
技術専門職員
金野哲士，田頭　徹，鈴木健之，福岡　誠，加治卓磨

1. はじめに

小職を含む情報基盤センターの技術職員 10 名は，本籍は本学の技術部にあるが，情報基盤センターの業務を兼務しており，大半は兼務先である情報基盤センターに関連する業務を遂行している。情報基盤センターの業務は，情報ネットワークと情報セキュリティを基盤とした“①情報基盤に関連した業務“と，研究・教育用に利用されている“②学術系システムに関連した業務“，および本学事務職員が使用している“③業務系システムに関連した業務“の３つに分類される。それらの業務の中から，システムの管理・運用業務のように恒常的な業務を除いて，本年度行った大きな３つの業務，１．業務分析，２．CSIRT の結成，３．学術系システムの更新業務についてご報告する。

2. 業務分析について

本学の運営交付金の削減等により技術部を取り巻く情勢はますます厳しくなって行くと予想される。そのことから技術部の将来構想について大学全体として検討することとなった。検討のための一つの参考資料として，情報技術部の業務の現状がどのようになっているのか業務の洗い出しと分析を行った。

2.1. 各業務内容の収集と集計および分析方法について

始めに，情報技術部ではどのような業務を遂行していて，どのくらいの労力を要しているのか業務量の算出には“プロジェクト見積”等で用いられている“工数”と同様の方法で集計することとした。構成員一人一人から自身の業務内容を箇条書きに出してもらい，個々の作業ごとに 1 回にかかる時間を分単位で精査する。さらに年間を通してその業務が何回あるかを出し，時間と回数を掛け算すると，1 つの業務に対して年間に必要な業務遂行時間が算出される。それを構成員全員分で合計する。

次に，その合計時間を本学の就業規則で決められている 1 日の就業時間 7 時間 45 分（465 分）で割り算すると，業務遂行に必要な日数が算出される。

続いて，年間の就業日数を 240 日として，前述の業務遂行に要する日数を割り算すると，年間の業務遂行に必要な人数が算出される。なお，分母を 240 日とした根拠は，2016 年 1 月から 12 月までの就業日数が約 240 日であったからである。

2.2. 集計時の配慮等について

個人個人の業務内容と，それに係る時間を回収する際には特に匿名性に気を遣った。同じ業務であっても，A さんは数時間でこなせるものが，B さんは数日かかってしまう場合もある。これは，各人の得手不得手や専門分野が異なることも原因となっている。専門分野が異なるため，同一の問題（タスク）の処理時間は自ずと差が出る。このように，ある問題（タスク）に対する処理

能力および専門分野には個人差があることから，構成員間での相互評価としてしまうと正確な工数が出せない。このため，個人から出された業務は同じ内容の業務ごとに束ね，全体としての集計表にまとめた。その集計表を構成員に回覧し，最終確認および加筆修正したものが表１である。

2.3. 集計結果

集計結果を表１に示す。各種システムの管理・運用のような恒常的な業務に加えて，主に業務系システムに関連した開発業務も遂行している。開発業務は，毎年同じ規模の案件があるとは限らないこと，年間を通して開発時期が違うことなどから恒常的な業務とは切り離して集計した。

表１　情報技術部の年間業務遂行に必要な人数

（１）恒常的な業務		
年間就業時間	1,446,950 分	
年間就業日数	3,112 日	1 日の就業時間を 7 時間 45 分（465 分）として計算
年間就業人数	13.0 人	1 年の就業日数を 240 日として計算

（２）開発業務		
年間就業時間	505,200 分	
年間就業日数	1,086 日	1 日の就業時間を 7 時間 45 分（465 分）として計算
年間就業人数	4.5 人	1 年の就業日数を 240 日として計算

情報技術部構成員は現在 10 名である。表１より，恒常的な業務と開発業務を合わせると，年間一人当たり約 1。8 人分の業務を遂行していることが分かった。

2.4. 業務分析における課題

表１には，システムの障害対応やインシデント発生等による突発的な緊急対応の業務が含まれていない。災いは必ずやってくるが，その時期や規模は予想がつかない。万が一緊急事態が発生した際には昼夜を問わず迅速な対応を要する。

次章では，CSIRT を結成したことについて述べるが，このように情報基盤センター以外の意図しないところから業務が舞い込んでくる場合がある。このような案件によって従来の業務内容を根本的に見直さなければならないことも発生する。

3. CSIRT の結成について

昨今，国立大学法人等において，情報セキュリティインシデントが急増していることから，情報セキュリティ対策を強化すると同時に，万が一インシデントが発生した場合にその原因解析や影響範囲の調査を行う CSIRT（Computer Security Incident Response Team）を結成するよう文科省より指示があった。それに対応して，情報基盤センター教員と情報技術部の一部で構成した CSIRT を結成し活動を開始した。CSIRT 活動には情報セキュリティと本学のシステムに関する高度な技術や知識を必要とし，加えて緊急対応を要することも予想されることから即戦力となる精鋭 5 名の技術職員を選出した。2 章の業務分析で述べたとおり，現状の業務を遂行するためにこれ以上人員を割くわけにはいかないので，CSIRT の 5 人は消防団のように普段は恒常業務を遂行し，緊急事態が発生した場合には CSIRT 活動を優先するよう重責を担っている。実際に，アカウント窃取の疑い事例が発生した場合や，外部からの攻撃とおぼしき迷惑メールが急増した場合などでは，他の業務より優先して問題解決にあたるなどの対応を，事象の発生の都度行ってい。平成２９年１月までの約半年間に行った業務遂行に要した時間と延べ人数を表２に示す。

表２　CSIRT の業務遂行に要した時間と延べ人数（平成 29 年 1 月まで）

	遂行時間（時間）	遂行延べ人数（人）
不信メール等対応	9.6	37
PC 挙動不審等対応	23.3	11
不信パケット等調査	139.0	6
広報	200.5	124
調査	21,416.0	50
業務遂行合計	21,788.3	228

表２において，**「不信メール等対応」**は，偽装あるいは標的型と思われるメールを受信した旨等の通報に対応した業務を含み，最近になって通報回数が急増している。**「PC 挙動不審対応」**には，ブラウザで不要な広告や偽の警告が表示される等の対応業務も含まれている。**「広報」**は，本学構成員に対する注意喚起等のほかに，構成員全員に対してセキュリティセミナーの実施や，セキュリティ教育用 VOD の収録と配信業務なども含まれる。周囲から“**「調査」**は業務なのか？”と問われることが多いが，我々を襲ってくる脅威の進化は秒進分歩であり，常に新しい情報を調査・習得するとともに，構成員への周知と対策を講じなければならない。敵を知らなければ防御はできない。ゆえに**「調査」**は最も重要な業務であり，CSIRT 業務のなかで大半を占めている。

4. 学術系システムの総入れ替え

約 5 年周期で行われている学術系システムの更新が今年度あった。メールサーバなど基幹システムと，各学部や図書館に設置されている実習用端末約 550 台の総入れ替えをした。作業は，授業が行われていない　お盆の前後 2～3 週間の間に行なわなければならず，大変な難業であった。作業期間が短かったにもかかわらずケガもなく安全に予定通り導入できた。

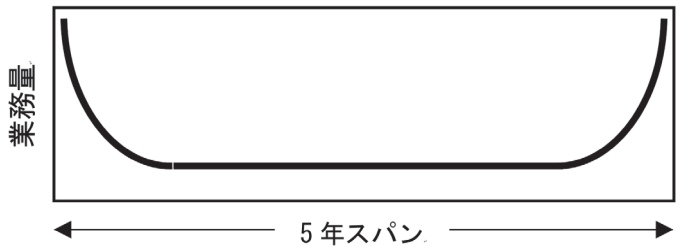


図１　システム更新に伴う業務量の変化の推定

更新に係る業務量を定量的に表すことは難しい。しかし，これまでに実施しているシステムの更新作業から，以下の傾向があるように思われる。システムの更新直後には，入れ替え作業と共に本学に合わせた調整作業が大半を占め，しばらく時間がたつと恒常的な管理・運用業務に落ち着く。時間が経過して約 5 年後の次期更新時期が近づくにつれ，現行システムの故障対応業務や次期更新に向けた準備作業などにより業務量が増えるものと想像される。

更新に伴う業務量の変化のイメージを図１に示した。

5. むすび

数多い情報基盤センター業務の中から，管理・運用業務など恒常的な業務を除き，今年度だけに特化した 3 つの業務についてご報告した。

新システム利用者講習会報告

情報基盤センター
川村　暁，中西貴裕

1. はじめに

平成 28 年度 9 月に稼働した新システムの利用者講習会について報告する。これまでと比較して，講義支援システムについての講習会と，大型計算機の設置元である東北大学サイバーサイエンスセンターが実施している講習会が増加している。

2. 開催した講習会

開催した講習会を示す。なお，東北大学サイバーサイエンスセンター大規模科学計算システムに関する講習会は 2.2 節を参照いただきたい。

2.1. 教育用端末，MATLAB 等

何れも，新システムへの切り替え前後の 2016 年夏期に実施している。

8 月 8 日　MATLAB TAH ライセンス利用講習会
8 月 31 日　情報基盤センター新システム講習会
　第 1 部「システム概要」～第 2 部「ネットワーク・サーバ」　約 40 分
　第 3 部「教育利用　教育用端末、教育用サーバ」　約 30 分
　第 4 部「科学技術計算」　約 30 分
9 月 14 日　MATLAB 講習会
　教職員向け約 90 分　　初心者向け（ハンズオンデータあり）　約 60 分

講義支援システム講習会は，各学部で開催した（教職員限定）。

9 月 15 日　10:30-11:30　教育学部　総合教育研究棟(教育系) 1 階 CS101 室
　14:30-15:30　人文社会科学部　6 号館 1 階 多目的視聴覚室
9 月 16 日　10:30-11:30　理工学部　1 号館 2 階 21 番教室
　14:30-15:30　農学部　北講義棟 2 階 情報処理演習室

2.2. 東北大学サイバーサイエンスセンター大規模科学計算システム

東北大学サイバーサイエンスセンター大規模科学計算システムの講習会は，本学で実施したもののほかに，東北大学サイバーサイエンスセンターで実施している各種講習会を，テレビ会議システムを用いて岩手大学で受講したものも含む。

何れも，東北大学サイバーサイエンスセンター大規模科学計算システムへの切り替え前後の 2016 年夏期に実施している。

7 月 1 日　東北大学サイバーサイエンスセンター大規模科学計算システム利用講習会
8 月 31 日　情報基盤センター新システム講習会 第 4 部「科学技術計算」

以下の講習会は，東北大学サイバーサイエンスセンターで実施された講習会を，東北大学と岩手大学をテレビ会議システムで結び，岩手大学で受講して実施した。

9 月 26 日　UNIX 入門

9 月 27 日　大規模科学計算システムの利用法

9 月 28 日　OpenMP プログラミング入門

9 月 29 日　MPI プログラミング入門

9 月 30 日　SX-ACE における高速化技法の基礎　後半はハンズオンのため東北大で受講可能

2.3. 講習会の VOD（Video On Demand）による公開

講習会に参加できなかった場合に，後から確認できるようにするため，講習会を撮影して VOD で公開している。

ストリーミングビデオ（岩手大学情報基盤センター．学内限定公開）

https://isic.iwate-u.ac.jp/media/

3. まとめ

システム入れ替えに伴い開催した講習会について報告した。新規部分について，講習会の開催を増やした。

今後も，利用する方にわかりやすく情報を発信し，システムを活用していただけるよう努力したい。

平成 27 年度および平成 28 年度の情報セキュリティに関する取り組み

情報基盤センター
川村　暁

1. はじめに

岩手大学情報基盤センター・岩手大学 CSIRT（Computer Security Incident Response Team）では，本学の情報セキュリティレベルを向上させるべく，様々な取り組みを行っている。本稿では，平成 27 年度および平成 28 年度に実施した事項についてまとめた。なお，日々行っている事項（システムの維持管理，利用者に対するセキュリティ・技術的な対応．電話，メール，情報セキュリティに関する調査研究・技術習得および研修参加等）は除いたうえで記している。

2. 情報セキュリティに関する取り組み

2.1. 平成２７年度

情報セキュリティに関する取り組みが増えつつあること，社会的な要請などをふまえ，CSIRT（Computer Security Incident Response Team）立ち上げの準備を行っている。

継続　全教職員の教育系アカウント（メールアドレス等）のパスワードの再設定。

継続　ソフトウェア監査。

改善　新採用教職員研修：前期，後期に１回実施を毎月実施へ改善（７月から毎月開催に拡充)。

改善　スタートアップセミナー：新入生・転入生に対するシステム・セキュリティ講習（４月)。
全新入生（学部，大学院)・転入生対象．セミナーの実施，セキュリティパンフレットの作成と配布。

改善　利用者（一般向け）情報セキュリティセミナー（３回開催)：年１回開催を年３回開催へ充実。

改善　オンラインシグマによる情報発信：情報発信の強化．特に情報セキュリティ等について。

改善　ウイルスメールに対する防御方法の調査及び周知：注意喚起　ファイルの拡張子の表示　等。

改善　情報基盤センター報告 Σ を復刊（３月)：情報セキュリティに関する啓蒙記事などを複数掲載。

新規　情報の保護に関する暗号化機能搭載 USB 機器の調査及び普及啓蒙活動など。

新規　弘前大学との，情報システムに関する相互監査の実施（対象：情報基盤センターのシステム)。

新規　学外公開サーバ等管理者への管理状況調査。IP アドレス，OS，稼働しているもの等。

新規　CSIRT 立ち上げ準備：属人的な活動ではなく，組織として対応できるような体制の準備。

2.2. 平成２８年度

年度当初に CSIRT を立ち上げ，活動を開始している。人員については，情報基盤センターの所属の専任教員および技術職員・技術専門職員・事務職員で構成している。専従しているわけではないこと，情報セキュリティ対策の関連業務が漸増しつつある中で，どのようにして「増加していくタスク」に対応していくかが大きな課題である。

継続　ソフトウェア監査。

改善　新採用教職員研修（毎月２回程度開催)。

新規　CSIRT 立ち上げ（4 月 1 日）と活動開始：インシデント等への準備と対応を属人ではなく組織で行う。

改善　スタートアップセミナー：新入生・転入生に対するシステム・セキュリティ講習（4 月）。未受講者に対するフォローアップの実施と受講管理。

改善　オンラインシグマによる情報発信：脅威状況に応じた臨時号，セキュリティポータルとの連携等。

改善　ウイルスメールに対する防御方法の調査及び周知：注意喚起　標的型攻撃等の警報の発令など情報提供の強化。

改善　情報の保護に関する暗号化機能搭載 USB 機器の調査及び普及啓蒙活動：セミナーと連動しつつ学内への浸透を図る。

改善　サポートされない OS・ソフトウェアの利用停止：対象 OS・ソフトウェアの周知を実施。

新規　情報セキュリティハンドブックの編纂：全教職員対象。A5 冊子とし配布済み。

基本編（19 頁），電子メール編（38 頁）：本学の規則等を踏まえ，ユーザに遵守頂きたい事項を記載した。

英語縮約版（A4 で 8 頁）：基本編と電子メール編を包含したものとした。母語が日本語ではない方向けに，利便性などを考えて編纂した。

新規　サーバ管理者向け情報セキュリティセミナー：サーバ管理における注意点，セキュリティの動向等について，外部講師による講演を実施した。

新規　経営層向け情報セキュリティセミナー：情報セキュリティ経営や，セキュリティの動向等について，外部講師による講演を実施した。

大幅に改善　利用者（一般向け）情報セキュリティセミナー（14 回開催）。学内（上田キャンパス）だけではなく，教育学部附属学校園，御明神牧場（農学部附属寒冷フィールドサイエンス教育研究センター），釜石サテライト（岩手大学三陸復興・地域創生推進機構）でも実施。

新規　情報セキュリティセミナー未受講者のフォローアップ：未受講者用 e-learning コンテンツの作成と受講管理等。情報基盤センターに設置した Moodle で実現した。

新規　外部公開サーバに対する脆弱性調査：脆弱性スキャナ Nessus を利用．対象サーバ数：150 程度。サーバ管理者に対する調査結果のフィードバックを含めて実施している。

新規　全教職員に対する標的型攻撃メール訓練の実施：2 月後半に実施した。結果は来年度に実施する情報セキュリティセミナーで周知する計画である。

改善・新規　ウイルス対策ソフトを，全学を包括するセキュリティソフトへ更新。

新規部分　全構成員（学生も利用可能なもの）への更新（新規部分の一部は平成 29 年度 5 月頃に提供開始予定）。スマートフォン・タブレットにも対応する。

新規　全教職員に対する IP アドレス利用状況調査の実施。

新規　情報セキュリティ図上演習の実施：インシデント対応について。今後の対応における知見を得た。

継続　弘前大学との，情報システムに関する相互監査の実施（対象：情報基盤センターのシステム）。

継続　情報基盤センター報告Σの発行(本書)：セキュリティに関する啓蒙記事も掲載されている。

新規　岩手大学教養教育基礎ゼミナール『学びのはじめ』（教育推進機構）に記事を寄稿。

「4　スマートフォン、ソーシャルメディアと上手につきあうために」（川村）

3. まとめ

本学の情報セキュリティレベル向上のために平成 27 年度および平成 28 年度に実施した，岩手大学情報基盤センター・岩手大学 CSIRT の取り組みについて記した。年度毎の推移を見ると，平成 28 年度に新規に実施されたものや，これまでの実施方法に改善を加えたものが多くある。また，内部的な要因ではなく外部的な要請などをふまえたものもある。

今後も，本学の情報セキュリティレベルの向上に寄与していけるよう，着実な活動を行っていきたい。

岩手大学の情報関連規則の見直し

簡素化し誰でも理解しやすい規則にするために

情報基盤センター
川村　暁
学術研究推進部学術情報課
庭田昌紀

1. はじめに

岩手大学の情報関連の規則は，国立情報学研究所で作成しているサンプル規定集 [1]や，文部科学省の示す方向性等を踏まえて制定された。制定後は新規事項へ対応するため，規則の条文や文言の改廃や，必要に応じた追加等を行ってきた。このため，全体像がぼやけてしまい，構成員へ周知を図るのが難しい状態にあった。情報セキュリティの観点からも，規則を守ることが目的化するのではなく，規則を守ることで情報セキュリティレベルが向上することが望ましい。これを達成するためには，読んで理解することができ，わかりやすい規則体系となっている必要がある。

全学の計算機上で取り扱う情報について示唆を与える立場にある情報基盤センターでは，情報セキュリティを強化する必要性の高まりと文科省からの要請を鑑みて，情報関連規則の整理統合を図った。本稿では，どのような方向性で整理統合を行ったかを示す。

2. 規則改正のポイント：誰でも読んで理解できるように

平成 29 年 3 月末まで有効だった規則は，文部科学省や国立情報学研究所が策定したサンプル規定集を，本学向けに手直ししたものが母体になっていた（次頁図１）。一度作成されたものに，新規の事案（例：特定個人情報の保護）が出現するたびに，改訂を繰り返したものになっている。このため，たとえていえば，増改築を繰り返した温泉旅館のような状況にあった。規定に出てくる文言についても，繰り返された改定の影響で不明瞭になっている箇所も散見された。規定の親子関係についても，据わりが悪いものがあった。

そこで，規則全体を俯瞰した上で，整理統合し，見通しが良いものする作業を行った。この作業により，規則の分量も削減することが出来た．次頁図２に，規則の全体像を示す。

3. 全構成員への周知：わかりやすいハンドブックの作成

規定を遵守してもらうためには，全構成員へ浸透を図る必要がある。このため，わかりやすいハンドブックを順次作成することにした。手始めに，教育研究活動で利用頻度が高いであろうパソコンと電子化された情報（例：文書ファイル，表計算ファイルなど）の取り扱い方法と，重要なコミュニケーションツールである電子メールについて取り上げた。それぞれ，情報セキュリティハンドブック基本編，同電子メール編として発行し，全学に配布済みである。また，母語が日本語ではない方向けに，基本編と電子メール編の英語縮約版を作成し，学内に周知している。

来年度以降は，改定された規定の全体像等について，階層別（サーバ管理者向け，一般ユーザ向け，経営層向け等）のハンドブックを作成し，周知を図る予定である。

ポリシー	実施要項	手順･ガイドライン等
国立大学法人岩手大学情報セキュリティ基本方針 国立大学法人岩手大学情報システム運用基本規則	岩手大学情報システム運用･管理要項	情報システムにおける情報セキュリティ実施手順 例外措置実施手順
	岩手大学情報システムリスク管理要項	情報システム運用リスク評価手順
	岩手大学情報システム非常時行動計画に関する要項	インシデント対応手順
	岩手大学情報格付け要項	情報格付け取扱手順 岩手大学における情報の取り扱いについて
	岩手大学情報システム利用要項	PC 利用ガイドライン 電子メール利用ガイドライン ウェブ利用ガイドライン ウェブ公開ガイドライン 利用者パスワードガイドライン パスワード付与または暗号化による情報セキュリティ対策手順 岩手大学ソーシャルメディア利用ガイドライン （付属資料：ソーシャルメディアのトラブル事例）
	岩手大学情報セキュリティ講習実施要項	
	岩手大学情報セキュリティ監査要項	
	国立大学法人岩手大学情報セキュリティインシデント緊急対応チーム設置要項	

図 1　改正前の規則の全体像

ポリシー	実施要項	手順・ガイドライン等
国立大学法人岩手大学情報システム運用基本方針 国立大学法人岩手大学情報システム運用基本規則	岩手大学情報システム運用・管理要項	情報システムにおける情報セキュリティ対策手順 例外措置実施手順
	岩手大学情報ネットワーク運用管理要項	IP アドレス管理手順 情報システム運用リスク評価手順
	岩手大学情報システム非常時行動計画に関する要項	インシデント対応手順
	岩手大学情報格付け要項	情報格付け取扱手順 岩手大学における情報の取り扱いについて
	岩手大学情報システム利用要項	岩手大学情報システム利用ガイドライン
	岩手大学情報セキュリティ講習実施要項	
	岩手大学情報セキュリティ監査要項	
	国立大学法人岩手大学情報セキュリティインシデント緊急対応チーム設置要項	

図 2　改正された規則の全体像

4. まとめ

岩手大学の情報関連規則の見直しについて記した。見直しによって，規則全体を整理統合できた。また，整理統合したことによって規則全体の見通しが良くなった。

今後は，改定された規則を学内に周知することと，わかりやすく記述したハンドブックを作成することが課題である。これにより，本学の情報セキュリティレベルの底上げを図りたい。

情報セキュリティセミナー

実施形態の変更と未受講者のフォローアップ

情報基盤センター
川村　暁
学術研究推進部学術情報課
奥崎たまえ，庭田昌紀

1. はじめに

組織の全構成員に対する情報セキュリティ意識の涵養は大きな課題となりつつある。ダムが蟻の一穴から決壊しかねないように，組織体においても，最も弱いところからセキュリティに関する事案が生起することが考えられる。

本学では一般のユーザ，すなわち全教職員に対して，情報セキュリティセミナーを毎年開催している。一昨年度までは年１回，昨年は年３回開催した。しかしながら，セミナー受講の対象者とセミナー参加者数には大きな隔たりがあること，即ち，参加割合が低いことが問題であった。

この問題を解決するため，情報セキュリティセミナーの開催回数を大幅に増やすこと・対象者別の開催とすること・未受講者に対するフォローアップ用コンテンツを提供することの三段構えの対応とした。

2. これまでの情報セキュリティセミナーの実施状況（平成 24 年度以降）

平成 24 年度から平成 27 年度までの，情報セキュリティセミナーの参加状況等を示す。

2.1. 平成 24 年度 情報セキュリティセミナー（年１回実施）

開催日時：12 月 5 日（水）13:15～14:30

講演内容：サイバー犯罪の現状、著作権法の改正、ファイル共有ソフトの危険性、無線 LAN のセキュリティについて

参加人数：23 名

参加率　：3.0%

2.2. 平成 25 年度 情報セキュリティセミナー（年１回実施）

開催日時：12 月 4 日（水）13:30～14:40

講演内容：ソフトウエアライセンスの管理、著作権法の改正、ファイル共有ソフト等の著作権問題について

参加人数：22 名

参加率　：2.8%

2.3. 平成 26 年度 情報セキュリティセミナー（年１回実施）

開催日時：12 月 24 日（水）13:30～14:30

講演内容：パスワード漏えいによる不正アクセスを受けた事例の紹介、パスワード漏えいの主な例とその対策方法について

参加人数：25 名

参加率　：3.2%

2.4. 平成 27 年度 情報セキュリティセミナー（年 3 回実施）

昨年度（平成 27 年度）は，セミナー実施回数を 3 回とした。

2.4.1. 第 1 回

開催日時：11 月 10 日（火）13:10～14:30

講演内容：パスワードの安全な運用方法とフィッシング対策について、情報漏えいを未然に防ぐ情報の取扱いルールについて

参加人数：26 名

参加率　：3.5%

2.4.2. 第 2 回

開催日時：平成 27 年 12 月 16 日（水）16:30～18:00

講演内容：パスワードの安全な運用方法とフィッシング対策について、情報漏えいを未然に防ぐ情報の取扱いルールについて

参加人数：17 名

参加率　：2.3%

2.4.3. 第 3 回

開催日時：平成 28 年 3 月 30 日（水）13:30～15:00

講演内容：パスワードの安全な運用方法とフィッシング対策について、情報漏えいを未然に防ぐ情報の取扱いルールについて

参加人数：16 名

参加率　：2.2%

2.4.4. 平成 27 年度の参加者総計と考察

第 1 回から第 3 回の参加者の総計は，２６名＋１７名＋１６名＝５９名（7.9%）となった。開催回数を増加した効果は認められるが，対象が全教職員であることを考えると決して高い数値とはいえない。開催曜日と時間帯について検討する必要もありそうである。

本学は，盛岡市上田キャンパス以外に，教育学部附属学校園（幼稚園・小学校・中学校は盛岡市加賀野，特別支援学校は盛岡市東安庭）や，岩手大学農学部附属寒冷フィールドサイエンス教育研究センター（滝沢農場は滝沢市，御明神牧場は雫石町），岩手大学三陸復興・地域創生推進機構釜石サテライト（釜石市），および，県南地域（北上市の金型技術開発センター等）などの遠隔地にも拠点を有している。それぞれの施設には教員，職員（事務職員および技術職員）が常駐しているため，これらの拠点に属している者が盛岡市上田にあるキャンパスに出向いてセミナーに参加することは現実的ではない。実際に，これら遠隔地拠点からの参加者はほぼゼロであった。

3. 平成 28 年度の情報セキュリティセミナー

3.1. 参加率の向上を目指した改善

平成 28 年度は，平成 27 年度までのセミナーの抱える問題点を解消することを目標とした。このため，セミナー開催回数を大幅に増やすこと，遠隔地拠点でもセミナーを開催することを考えた。また，教職員は大きく教員と事務・技術職員に分けてセミナーを実施した。教員対象のセミナーは教員が参加しやすいよう，教授会の前に 30 分程度のセミナーとした。教授会前のため長い時間のセミナーは設定し難かったためである。事務・技術職員向けのセミナーについては，1 時

間前後のセミナーとした（実施場所などによる変動はある）。

今年度のセミナーでは，情報セキュリティの基礎を成す事項であるパソコンなど情報機器の取り扱いルールや電子化された情報そのものの取り扱い（パソコンで取り扱う情報とほぼ同義），および，電子メールについてとりあげた。表１に，セミナー実施計画を示す。なお，この表に記載の無い拠点（岩手県沿岸部のエクステンションセンター，岩手県南部にあるものづくり等の連携拠点）については，原則として，セミナーのいずれかに参加するか，または，後述する未受講者のフォローアップを行うこととした。

表１　平成 28 年度情報セキュリティセミナー実施計画

<table>
<tr><th>実施(所属)区分</th><th>主な対象者</th><th>実施(予定)日時
日付は平成28年度</th><th>実施内容, 時間など</th><th>備考</th></tr>
<tr><td>人文社会科学部</td><td>人文社会科学部所属の教員</td><td>1月17日(火)15:00～</td><td rowspan="4">･基本編のみ(15分程度)
※ 電子メール編は平成29年度上半期に実施</td><td rowspan="4">･学部事務/附属校園事務受講可
･各機構･センターの教員は，所属する学部教授会セミナーで受講(必須)</td></tr>
<tr><td>教育学部</td><td>教育学部所属の教員</td><td>11月15日(火)14:55～</td></tr>
<tr><td>理工学部</td><td>理工学部所属の教員</td><td>1月31日(火)15:10～</td></tr>
<tr><td>農学部</td><td>農学部所属の教員</td><td>10月18日(火)15:10～</td></tr>
<tr><td>附属幼稚園</td><td>教育学部附属幼稚園所属の教諭</td><td>11月14日(月)15:00～</td><td rowspan="4">･基本編(15～20分)
･電子メール編(15～20分)
※ 計40分程度</td><td rowspan="4">附属学校園所属の事務職員は，附属学校園で開催されたセミナーを受講している場合がある.</td></tr>
<tr><td>附属小学校</td><td>教育学部付属小学校所属の教諭</td><td>1月16日(月)13:30～</td></tr>
<tr><td>附属中学校</td><td>教育学部附属中学校所属の教諭</td><td>12月15日(木)16:00 ～</td></tr>
<tr><td>附属特別支援学校</td><td>教育学部附属特別支援学校所属の教諭</td><td>1月12日(木)10:30～</td></tr>
<tr><td rowspan="4">事務／技術職員
※特任教員受講可</td><td rowspan="4">事務職員，技術職員
(12/14　金型技術研究センター所属の職員)</td><td>11月15日(火)11:00～</td><td rowspan="4">･基本編(20～30分)
･電子メール編(20～30分)
※ 計60分程度</td><td rowspan="3">いずれかの1回に参加</td></tr>
<tr><td>11月16日(水)13:30～</td></tr>
<tr><td>11月18日(金)13:30～</td></tr>
<tr><td>12月1日(木)11:00～</td><td>オンライン(フォローアップ)を受講</td></tr>
<tr><td>附属農場等*</td><td>滝沢農場，御明神牧場所属の職員</td><td>12月14日(水)16:00～</td><td colspan="2">御明神牧場にて実施</td></tr>
<tr><td>宮古エクステンションセンター**</td><td rowspan="3">各エクステンションセンター所属の職員</td><td></td><td colspan="2">本学でセミナーを受講</td></tr>
<tr><td>久慈エクステンションセンター**</td><td></td><td colspan="2">釜石サテライトにて受講</td></tr>
<tr><td>大船渡エクステンションセンター**</td><td></td><td colspan="2">別途受講方法連絡(オンライン受講など)</td></tr>
<tr><td>釜石サテライト**</td><td>釜石サテライト所属教員，職員</td><td>12月16日(金)11:00～</td><td>･基本編(20～30分)
･電子メール編(20～30分)
※ 計60分程度</td><td>釜石サテライト所属の教職員は，基本編＋電子メール編を受講とした.</td></tr>
<tr><td>金型技術研究センター***</td><td></td><td></td><td colspan="2">12/1(木) 実施のセミナーを受講</td></tr>
<tr><td>オンライン
(フォローアップ用. 動画と問題)</td><td>(セミナー未受講者，および，
オンライン受講が標準の方)</td><td>2月13日(月)
～3月17日(金)</td><td>動画(基本編，電子メール編)
およびフォローアップ問題</td><td>未受講者および遠隔地拠点でセミナーに参加できなかった者</td></tr>
</table>

* 岩手大学農学部附属寒冷フィールドサイエンス教育研究センター　** 岩手大学三陸復興･地域創生推進機構　*** 理工学部附属金型技術研究センター

3.2.　情報セキュリティハンドブックに基づくセミナーの実施

セミナーの内容は，本学の諸規則・規定を簡便に記載した情報セキュリティハンドブック基本編および同電子メール編を用いて行った。このハンドブックに準拠することで，本学の諸規則・規定に準拠出来るものとなっている。内容もできるだけわかりやすくなるように，図表を多数取り入れ，サイズも常備しやすい A5 版とした。

セミナーでは，参加者は本ハンドブックを参照しつつ，情報基盤センターの講師による解説を聞く形式とした。

セキュリティハンドブックについては，本センター報告の別記事を参照頂きたい。

3.3.　未参加者へのフォローアップ

何らかの理由でセミナーを受講できなかった方に対しては，セミナーを撮影した動画を VOD (Video On Demand)としたものおよびフォローアップ問題の受講で代替できるようにした。これらのコンテンツは，ネットワーク経由で受講できる（ただし，学内限定公開としている）。

フォローアップ問題は，合格率を 80%以上に設定した。それぞれの問題は，セキュリティハンドブックや VOD を参照すれば回答が得られるようにした。

これにより，スケジュールの都合で受講できなかった方などを含め，全教職員を対象とした実施体制を整えることが出来た。

表 2　平成 28 年度情報セキュリティセミナー実施結果

(a) 教員向けセミナー

	学部	受講対象者数	セミナー受講者数		計	受講率	
			教授会前	職員向け等		教授会前	総受講率
教員	人文社会科学部	76	52	1	53	68.4%	69.7%
	教育学部	87	74	1	75	85.1%	86.2%
	理工学部	140	108	0	108	77.1%	77.1%
	農学部	112	43	2	45	38.4%	40.2%
	特任教員	75	0	22	22	29.3%	29.3%
合計		490	277	26	303	56.5%	61.8%

備考1　教授会前セミナーの受講率と，教授会前セミナーおよび職員向けセミナー受講者を足したもの（総受講率）を示した.
備考2　特任教員は，職員向けセミナーを受講することとしたため，教授会前のセミナーの受講は 0 となっている．勤務日などの関係を勘案して案を定めた.

(b) 事務系および技術系職員向けセミナー

	部局等	受講対象者数	セミナー受講者数						計	受講率	備考
			上田キャンパス				御明神牧場	釜石サテライト			
			第１回 (11/15)	第２回 (11/16)	第３回 (11/18)	補講 (12/1)	(12/14)	(12/16)			
事務系職員	総務部	46	6	12	18	3	0	0	39	84.8%	
	財務部	41	17	12	12	0	0	0	41	100.0%	
	学務部	69	20	24	20	1	0	0	65	94.2%	
	学術研究推進部	55	12	18	20	3	0	0	53	96.4%	
	地域連携推進部	18	1	7	5	1	0	3	17	94.4%	
	人文社会科学部	9	4	0	0	0	0	0	4	44.4%	
	教育学部	29	5	6	4	0	0	0	15	51.7%	
	理工学部	37	5	11	10	1	0	0	27	73.0%	
	農学部	50	4	10	22	1	0	0	37	74.0%	
	計	354	74	100	111	10	0	3	298	84.2%	
技術系職員	理工学系技術部	44	18	14	8	3	0	0	43	97.7%	
	農学系技術部	27	13	0	4	0	9	0	26	96.3%	
	情報系技術部	10	4	1	5	0	0	0	10	100.0%	
	計	81	35	15	17	3	9	0	79	97.5%	
その他*		98**	15	9	18	15	0	1	58	59.2%†	**教員，研究員**等含む
合計		533†	124	124	146	28	9	4	435	81.6%†	

*　研究推進機構，RI総合実験センター，三陸復興・地域創生推進機構，COC推進室等.
** 職員向けセミナーだが，勤務日などの関係から特任教員は，教授会前に実施される教員向けセミナーではなく職員向けセミナーを受講する場合があるため．職員にこれら教員を含んだ数である.
† 前項**の理由から，受講総数（分母）に若干誤差を含む．このため，パーセントは参考値として記した，

(c) 附属学校園向けセミナー

		教諭など			備考　受講した事務職員			総割合
		対象者数	受講者数	受講割合	対象者数	受講者数	受講割合	
教諭など	附属幼稚園	9	9	100. 0%	2	2	100. 0%	100. 0%
	附属小学校	33	32	97. 0%	5	4	80. 0%	94. 7%
	附属中学校	22	11	50. 0%	0	0	0. 0%	50. 0%
	特別支援学校	34	28	82. 4%	6	4	66. 7%	80. 0%
合計		98	80	81. 6%	13	10	76. 9%	81. 1%

表 3　平成 28 年度情報セキュリティセミナー受講率

	受講対象者数	受講者数	受講率
全構成員（教職員）	1033	786	76.1%

表 4　平成 28 年度情報セキュリティセミナーフォローアップ集計結果

なお，受講対象者（職種など）により受講範囲が異なる。このため，定められた範囲のフォローアップを修了した数を，フォローアップ受講者（完了した者）に記している。

	フォローアップ対象者数	フォローアップ受講者（完了した方）	受講率（完了した方）
教員＋特任教員	168	119	70.8%
職員	58	35	60.3%
計	226	154	68.1%

表 5　平成 28 年度情報セキュリティセミナーのフォローアップを含んだ受講率

受講者数は，セミナーを受講した方＋フォローアップを完了した方の合計。

	受講対象者数	受講者数	受講率
全構成員（教職員）	1033	940	91.0%

3.4. 情報セキュリティセミナーの実施結果と考察

表 2 に，セミナーの参加状況を示す。なお，数値に若干（数名程度）の不整合がある。これは，受講範囲が職位・職種・勤務地の関係で複雑であったため重複して計上している方が若干名おられること（複数回受講した方も含む），および，受講範囲が不足していた方がおられたため，その方はセミナーを受講していてもフォローアップの対象に含まれたためである。

表 2(a)から，各学部教授会前に実施したセミナーは，学部によって参加率に差がみられた。このばらつきは，参加者の多い学会や行事などがあった可能性が示唆される。よって来年度以降は，ほかの行事などとの日程を勘案した上でセミナーの日程を設定する必要があると考えている。

表 2(b)に示した事務・技術職員は，事務連絡網を使って参加を促したこともあり，セミナーの参加率は非常に高くなっている。また，遠隔地拠点に常駐している方（たとえば，牧場では動物を飼育しているため，技術職員他が常駐している）をカバーするため，遠隔地（滝沢市や雫石町にある農場・牧場）でもセミナーを開催した効果であろう。

表 2(c)は，教育学部附属学校園のセミナー参加率である。学校園では，校務の中で児童生徒の個人情報を取り扱うことが多いと考えられるため，それぞれの学校園毎にセミナーを実施した。出張してセミナーを実施したこともあり，セミナー参加率を高くすることが出来ている。

本年度の全教職員に対するセミナー受講率は，76.1%となった（表 3）。この数値は，本学の一般向けの情報セキュリティセミナー史上最高の数値となった。実施側の負担も大きく増加しているが，それに見合うだけの成果が得られたのではないかと考えている。

セミナー受講率は 76.1%となり，非常に高い数値ではあるが，2 割以上の方は情報セキュリティセミナーが未受講の状態であった。このため，情報セキュリティセミナーを VOD (Video On Demand) としたものおよび学習用 e-learning コンテンツを用意した。フォローアップ学習用のコンテンツは，情報基盤センターで構築した Moodle 上に，基本編用 17 問，電子メール編用 15 問の理解度を測る問題を設置した。全構成員に配布済みの情報セキュリティハンドブック基本編

および電子メール編を参照しつつ VOD を視聴した上で，理解度を測る問題で正当率が 80%以上で合格とした。

平成 28 年度岩手大学情報セキュリティセミナー　情報基盤センター（学内限定）
https://isic.iwate-u.ac.jp/security/index.html
岩手大学情報基盤センター学習サイト（学内限定）
https://study.cc.iwate-u.ac.jp/

表 4 に，セミナー未受講者のフォローアップの結果を示す。何らかの理由で受講できなかった方に対し，繰り返し受講を促すなどした結果，情報セキュリティセミナー未受講者のうち 7 割程の方はフォローアップを完了している。

表 5 は，平成 28 年度の情報セキュリティセミナー受講者数＋フォローアップ完了者数の合計である。全構成員に対して 91.0%という特筆すべき受講率とすることができた。これは，大学という組織は職種や職能が大きく異なる集団である上，本学はいくつかの拠点がある事を考えると，複数段の方策をとったことが奏功したと推察している。

4. まとめ

全教職員対象の情報セキュリティセミナーについて，昨年度までの低い参加率を改善するための取り組みとその結果について考察した。多数の方々は盛岡市上田の大学キャンパス内で勤務しているが，岩手県内に多数ある拠点にも勤務者がいること，職種も教員と事務・技術職員があることから，実施回数・実施形態に大きな修正を加えた。セミナーの実施回数の大幅な増加や，出張してのセミナー実施，教員については参加し易いであろう教授会前にセミナーを設定することにより，参加率を大きく向上することが出来た。

また，セミナーを受講できなかった方へのフォローアップとして，オンラインでセミナーの動画を視聴し，問題を解く教育用コンテンツを用意した。こちらの受講率は，68.1%（平成 28 年度末現在）である。

これらの施策の結果，情報セキュリティセミナー受講者とおフォローアップを完了した方をあわせた総受講率は 91.0%という高率とすることができた。

来年度以降は，平成 29 年 4 月に改正された，情報セキュリティに関する諸規定・規則の周知や，刻々と変化しているセキュリティ動向を踏まえたセミナーを実施し，本学の情報セキュリティレベルの向上を図っていきたいと考えている。

情報セキュリティハンドブック

基本編・電子メール編，英語縮約版の編纂
－情報セキュリティの啓蒙活動の一環として－

情報基盤センター
川村　暁，中西貴裕
学術情報課情報企画グループ
庭田昌紀

1. はじめに

大学の各部門の権限や活動，構成員の従うべき事項などは，規則・規定など一連の文章によって定められている。構成員はこれらに準拠することになっている。ここで，情報セキュリティ関連の規則・規定を俯瞰すると，法律的な文書であること，情報分野に関する専門的な用語・言い回しが頻出すること等から，全構成員に理解を求めるのが難しい状態にあった。

情報セキュリティの取り組みにおいても，最低限の基準を示す規則・規定を遵守してもらうことが必要である。即ち，大学全体のセキュリティレベルの向上のためには，全教職員に対して，規則・規定を周知し，遵守できる方策を考える必要があった。さらに，社会的な要請などから，組織体の情報セキュリティレベルの向上が非常に強く求められ，要求される状況にある。情報セキュリティに関する事案を生じた場合の各種報道の様子を想起頂きたい。

これらを踏まえ情報基盤センターでは取り纏め役の川村が中心となり，岩手大学の情報セキュリティレベルを引き上げる施策の一環として，情報セキュリティハンドブックを編纂した。本稿では，セキュリティハンドブックの大凡の内容と位置づけについて記す。

2. 情報セキュリティハンドブックを編纂した意図と位置づけ

組織の情報セキュリティを高めるためには，組織全体を俯瞰し，もっとも脆弱な部分の底上げを図る必要がある。これは，組織全体のレベルは，もっとも脆弱な部分のレベルで規定されるためである。

それでは，大学全体のセキュリティレベルを高めるにはどうすれば良いかと考えたとき，全構成員に対して，最低限守るべきこと・知っておく必要があることについて，わかりやすく周知することが必要になる。

はじめにで記したとおり，大学の各部門の権限や活動，構成員の従うべき事項などは，規則・規定など一連の文書によって定められているため，これを遵守することが求められている。しかしながら，規定・規則は，法律的な文書である。また，情報セキュリティ関連の規則・規定は，情報分野に関する専門的な用語・言い回しも頻出するうえ，その時々の必要に応じて改廃を繰り返したものとなっている。さらに，情報セキュリティの強化という観点から，全構成員に周知する必要性にも迫られている。

これら全ての相反しかねない項目に対応するため，全構成員が理解しやすく，最低限遵守していただきたい事項をわかりやすく提示できるような情報セキュリティハンドブックを３編，編纂した。３編それぞれについて，次節以降で触れる。

- 情報セキュリティハンドブック　基本編　2016 年度版　A5 版
- 情報セキュリティハンドブック　電子メール編　2016 年度版　A5 版
- Computer and Information Security Handbook 2016
  1st Edition [Academicians and Staff Members] 2016
  --- Basics and Email (English Abridgement Version) ---　A4 版

3. 情報セキュリティハンドブック　基本編

情報セキュリティハンドブック基本編は，電子化された情報，すなわち，パソコン上で取り扱う情報の取り扱いと注意点，情報を取り扱っているパソコンの取り扱いと注意点について記している。

情報の取り扱いは，岩手大学の規則・規定（例：文書取り扱い規則，情報格付け手順）が最も基本的なものとなる。この部分は，総務広報課の取り扱う部分となる。情報基盤センターは，学内の情報基盤を担う部署であるので，利用者サイドと最も関連がある，パソコン上で取り扱う情報の周辺について検討した。これらをわかりやすく記したのが，情報セキュリティハンドブック基本編である。情報の取り扱いについては，規則を遵守するための最低限を見定め，“機密性”だけに絞った形で記述している。

4. 情報セキュリティハンドブック　電子メール編

個人情報等を含んだファイルを，電子メールでやり取りする場面は多くある。個人情報は当然保護される必要はあるが，実際の業務においてどのような点に留意すれば良いのかが，一般の利用者にはわかりにくい（判断しがたい）状態にあった。このため電子メール編では，実際に電子メールを運用する際に，どのような点に注意すれば良いのか？について記述した。

本ハンドブックでは，電子メールの利用方法だけではなく，電子メールを取り扱うパソコンについての注意点や，個人情報を含むファイルをどのように取り扱うとよいかを記している。電子メールで問題となる，迷惑メールや攻撃を指向したメールについても取り上げた。特に，電子メールソフト毎のお薦めの設定を掲載している。たとえば，本学では規定・規則で禁止されている HTML 形式でのメールの送信を標準としないためにはどうすればよいか？など，具体的な事柄を記している。現在利用している電子メールソフトの設定を確認する際に，活用いただきたい。

5. Computer and Information Security Handbook (English Abridgement Version)

Computer and Information Security Handbook は，母語が日本語ではない教員・研究員の方々向けに，情報セキュリティハンドブック 基本編 および情報セキュリティハンドブック 電子メール編 の内容を網羅した英語縮約版となっている。全構成員を包含する対策を考えた際に，日本語版の情報セキュリティハンドブックでは十分に手当てできない部分となるため，本ハンドブックを編纂することにした。

英語版は規則・規定は日本語版が正式であること，本手引きはあくまで利用者の利便性のため，という立ち位置で作成している。これは，情報基盤センターが各種規定の英語訳版を作成することはふさわしくないが，現実には母語が日本語ではない方々が多数所属していることを踏まえたものである。即ち，全構成員に情報セキュリティ関連規則・規定を周知するためには，日本語版では対応できない方々へのケアが必要であろうとの判断に基づいている。

このハンドブックは製本はせず，情報基盤センターセキュリティポータル上に電子的に公開している（PDF 版を掲出した）。

6. 情報セキュリティハンドブックの頒布，周知方法

ハンドブックを作成することが目的ではなく，全教職員に情報関連の規則・規定を周知し，ひいては情報セキュリティレベルを向上させることが目的である。目的を満たすためには，全構成員にどのようにして頒布するかおよび周知するかが問題となる。

情報基盤センターでは，情報セキュリティレベルを向上させるための取り組みとして，情報セキュリティセミナーを開催している。これまでは年１回（平成 27 年度は３回）の開催であったものを，今年度は全教職員を網羅することを考えて，セミナー実施回数を 14 回と大幅に増加している。セミナー実施に併せてハンドブックを頒布することにした。また，セミナーそのものも原則として全教職員は参加しなければならないものとした。セミナー自体もハンドブックの内容に沿って実施し，内容の浸透を図っている。

なお，これら３つのハンドブックは，情報基盤センターセキュリティポータル（岩手大学内）において公開している。

岩手大学情報基盤センターセキュリティポータル　（学内限定公開）
https://isic.iwate-u.ac.jp/security/index.html

情報セキュリティハンドブック［教職員用］　（学内限定公開）
https://isic.iwate-u.ac.jp/security/rule/handbook.html

情報セキュリティハンドブック 基本編　（学内限定公開）
https://isic.iwate-u.ac.jp/security/rule/pdf/security_handbook_2016.pdf

情報セキュリティハンドブック 電子メール編　（学内限定公開）
https://isic.iwate-u.ac.jp/security/rule/pdf/security_handbook_mail_2016.pdf

Computer and Information Security Handbook –Basics and e-mail
(English Abridgement Version)　（学内限定公開）
https://isic.iwate-u.ac.jp/security/rule/pdf/security_handbook_eng_2016.pdf

7. まとめ

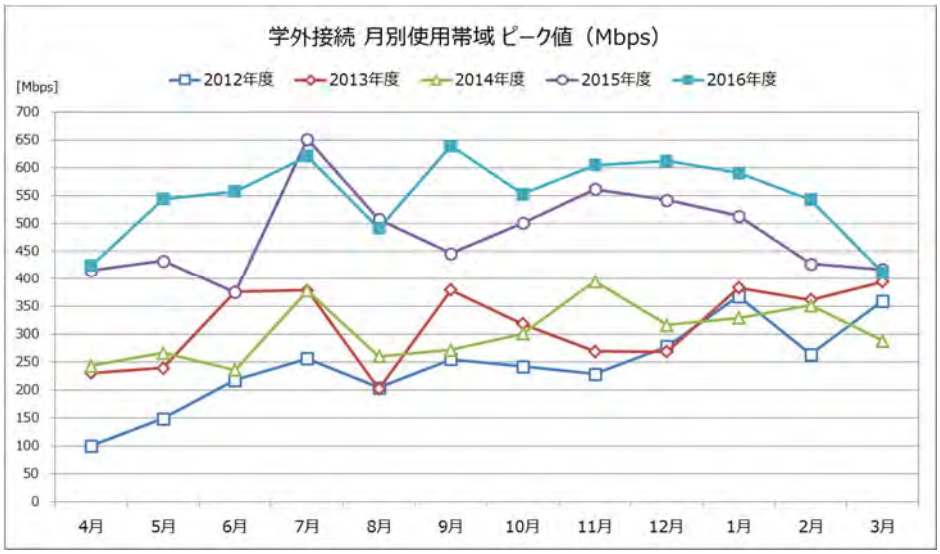
情報セキュリティハンドブックの編纂と，頒布・周知方法について記した。本学の全教職員に浸透させることを最優先とし，内容を出来るだけ簡素にしたこと，本ハンドブックに準拠すれば本学の規定を満足することが出来ること，頒布・周知方法を工夫したことを述べた。情報の取り扱いについては，機密性だけに絞った記述とした。これにより記述が簡素化され，かつ，励行するのも難しくない記載とすることが出来た。

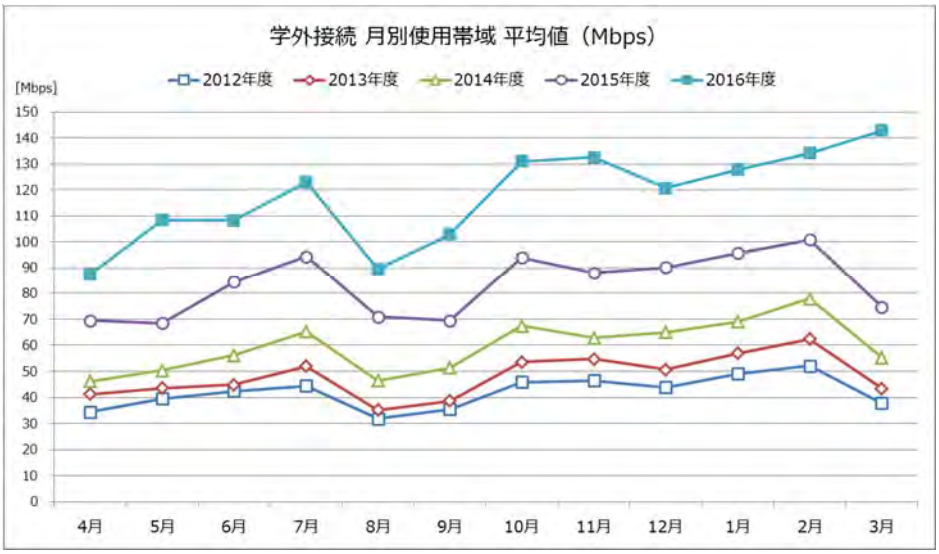
本ハンドブックにより，全教職員の情報セキュリティに関する意識が涵養され，ひいては本学の情報セキュリティの水準が向上することを願っている。

【運用報告】

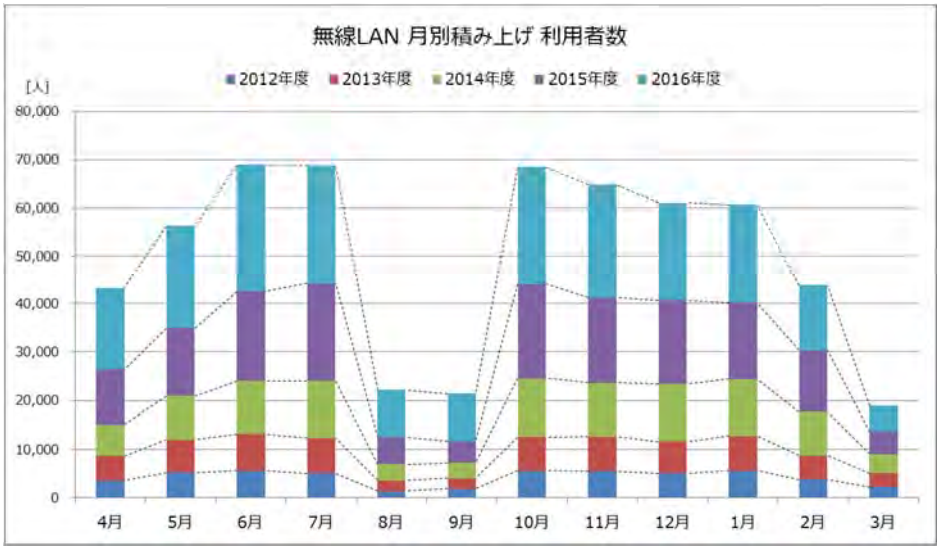
運用報告

[学外接続]

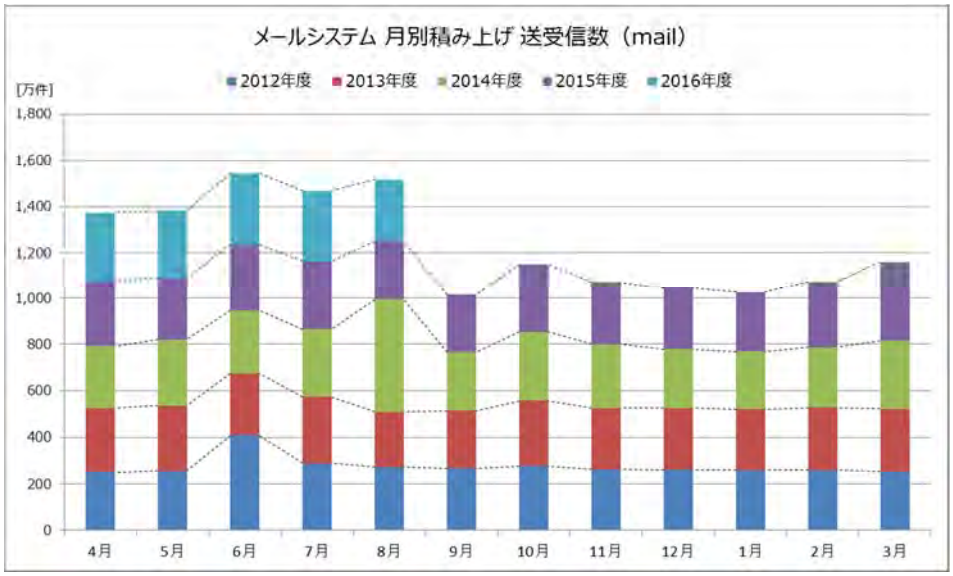


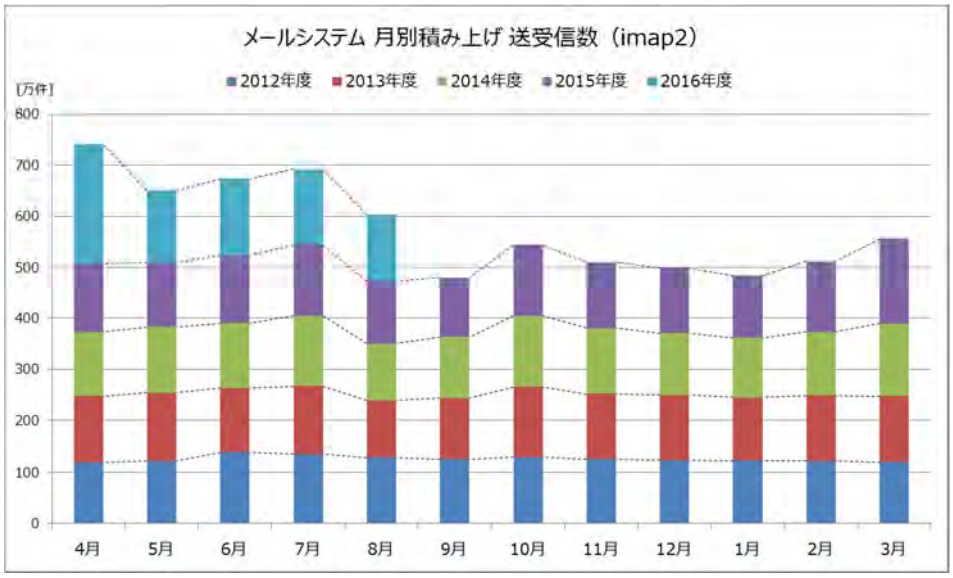


[無線 LAN]

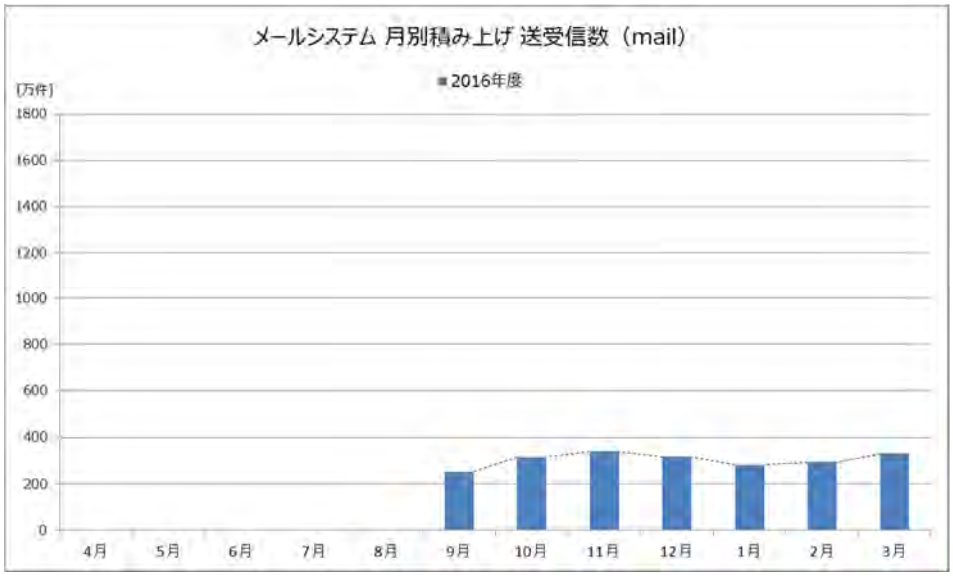


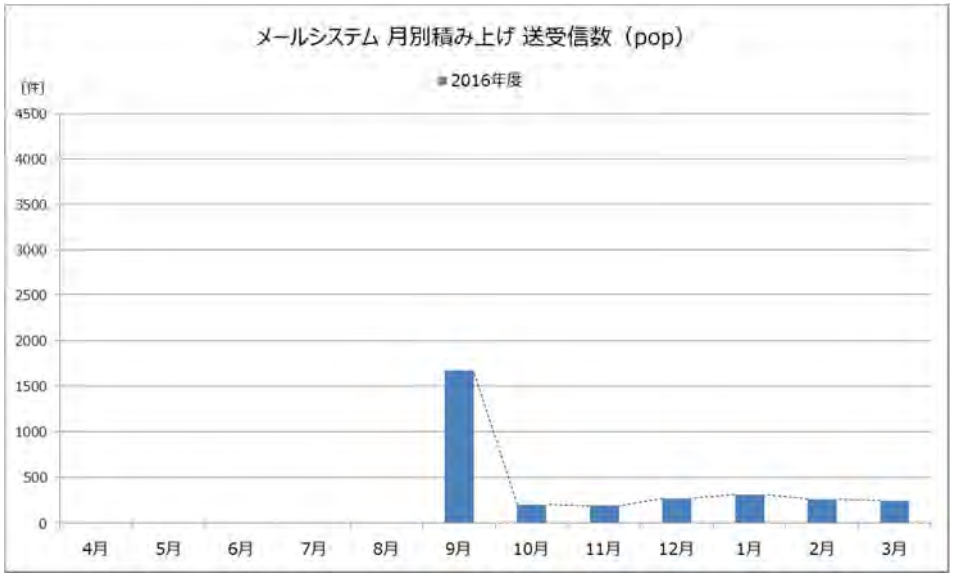
[旧・メールシステム]（2012 年 4 月～2016 年 8 月）

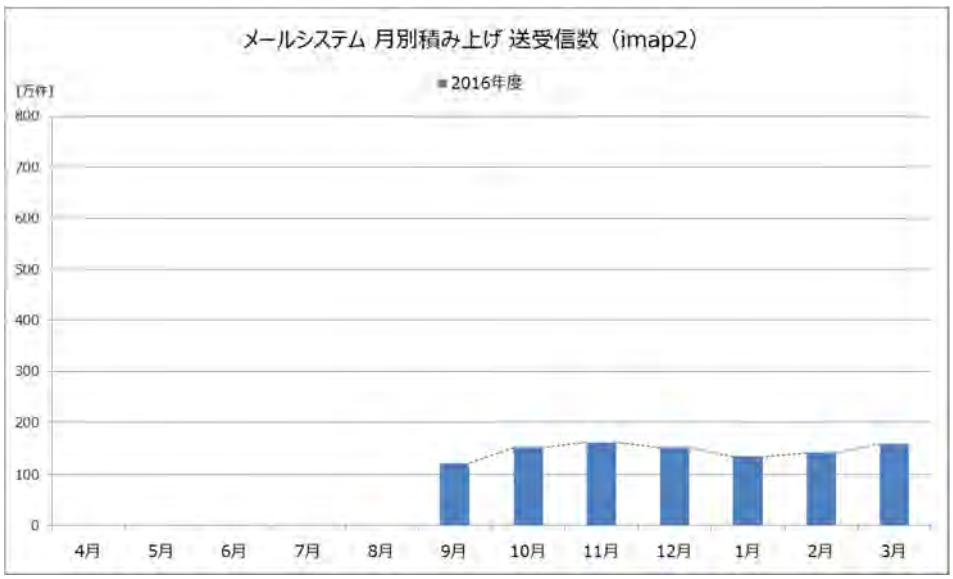




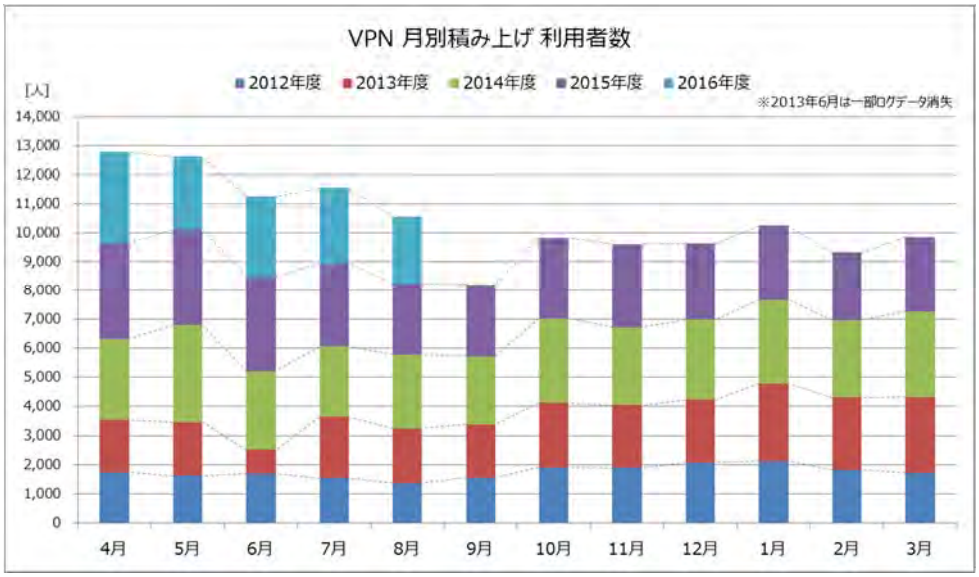
[新・メールシステム]（2016 年 9 月～2017 年 3 月）

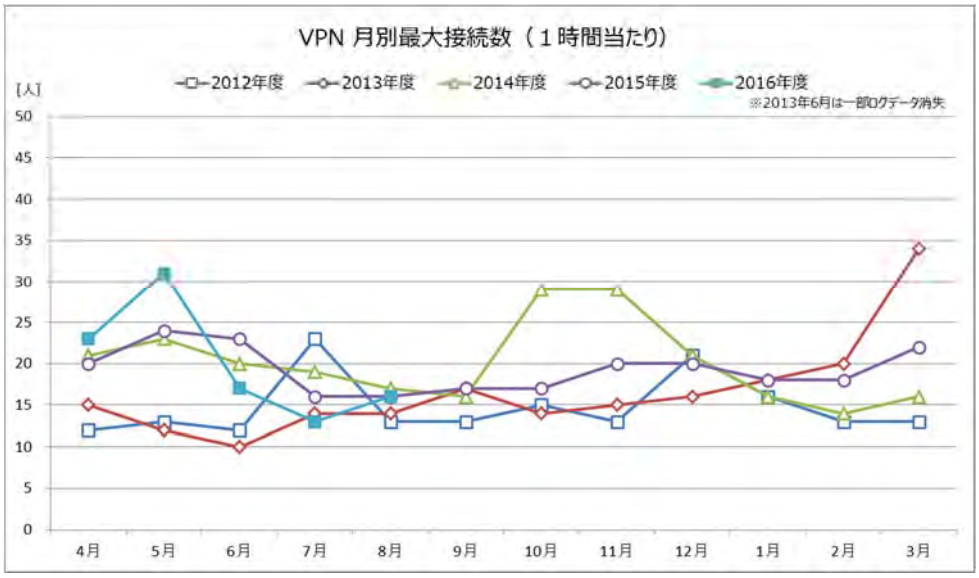




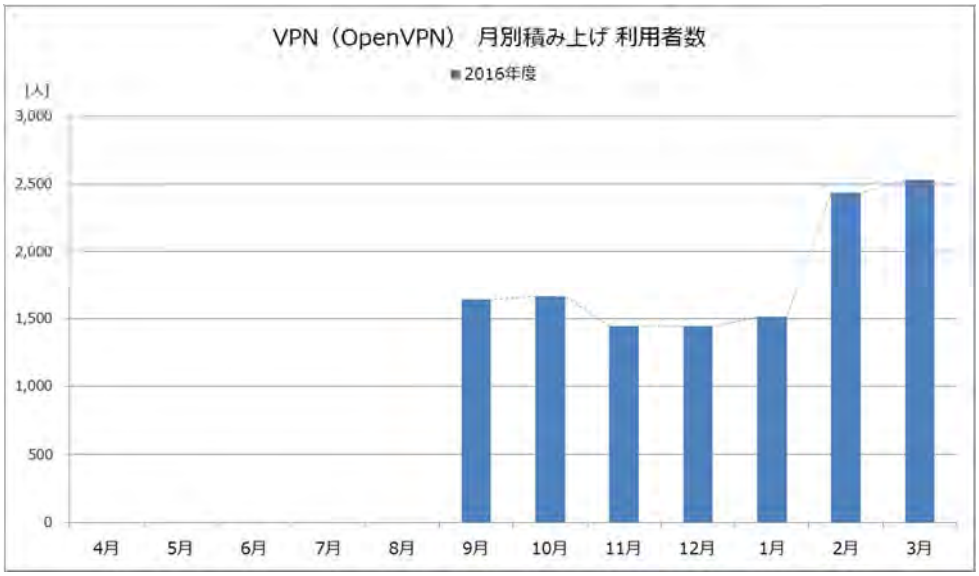


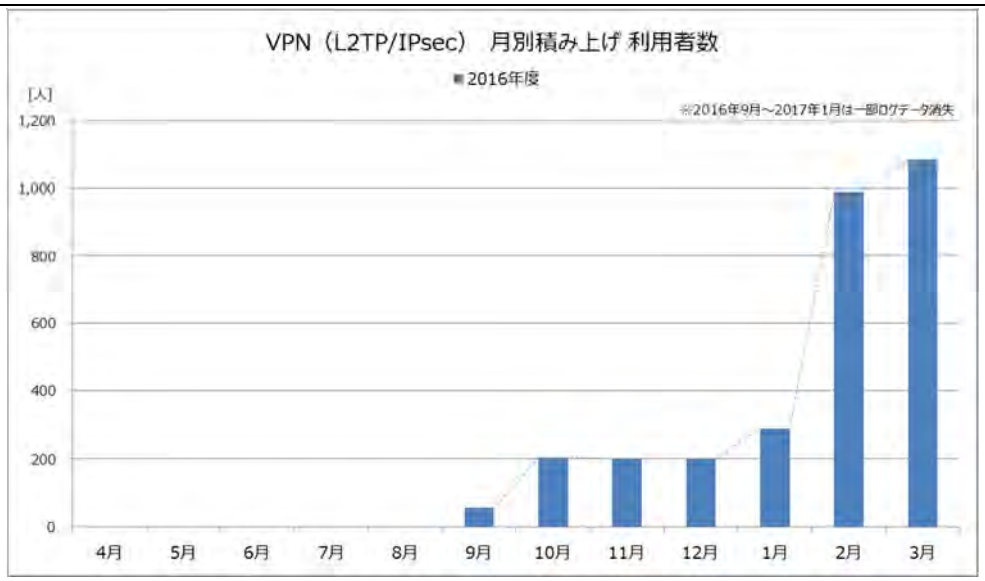
[旧・VPN]（2012 年 4 月～2016 年 8 月）

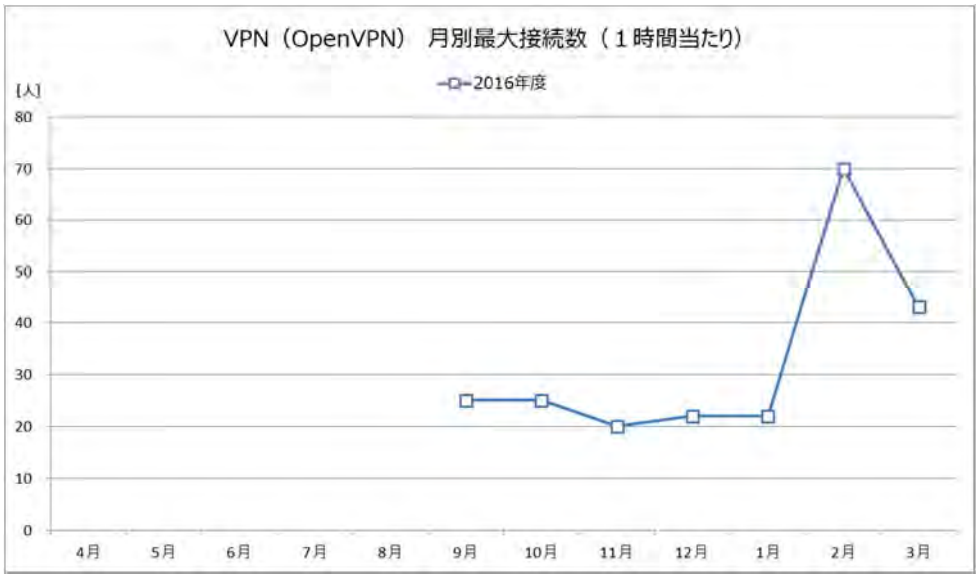


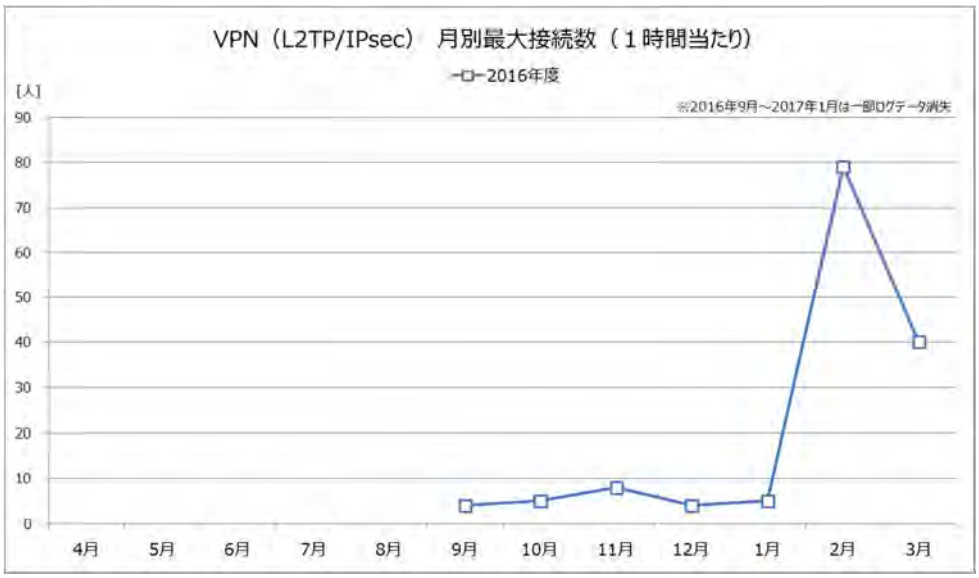


[新・VPN]（2016 年 9 月～2017 年 3 月）



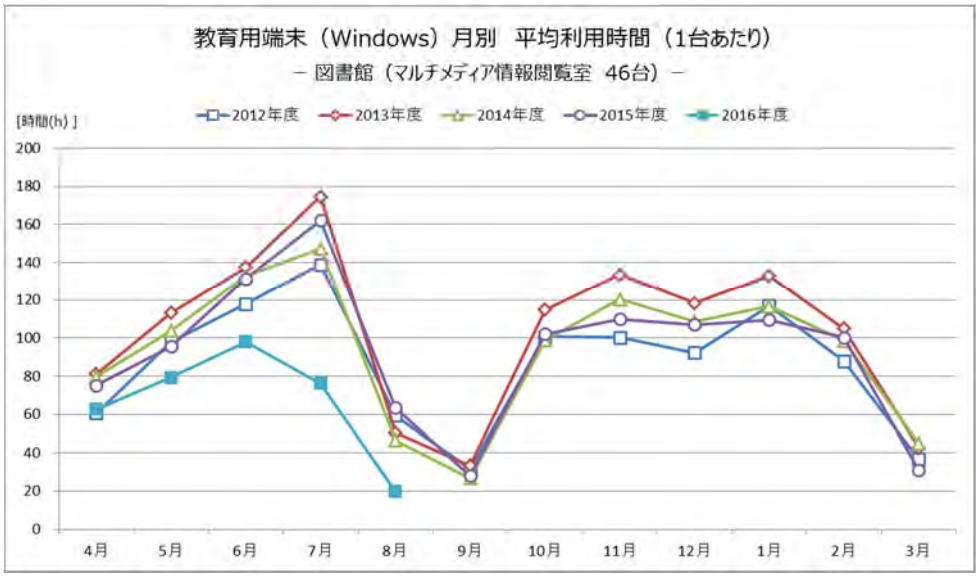

VPN（L2TP/IPsec） 月別積み上げ 利用者数
■2016年度
[人]
※2016年9月～2017年1月は一部ログデータ消失
1,200
1,000
800
600
400
200
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

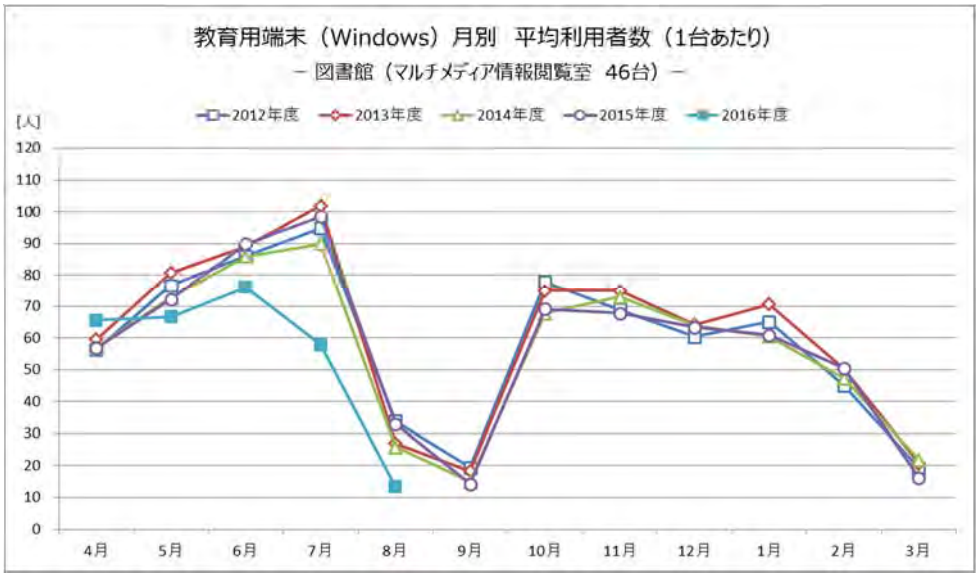

VPN（OpenVPN） 月別最大接続数（１時間当たり）
2016年度
[人]
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月


VPN（L2TP/IPsec） 月別最大接続数（１時間当たり）
2016年度
[人]
※2016年9月～2017年1月は一部ログデータ消失
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

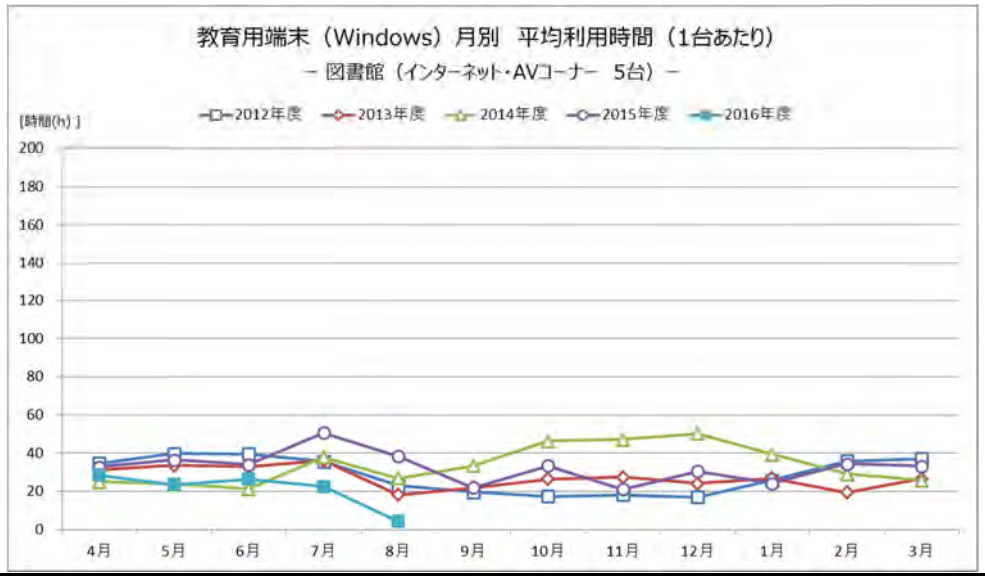
[旧・教育用端末(Windows)]（2012 年 4 月～2016 年 8 月）

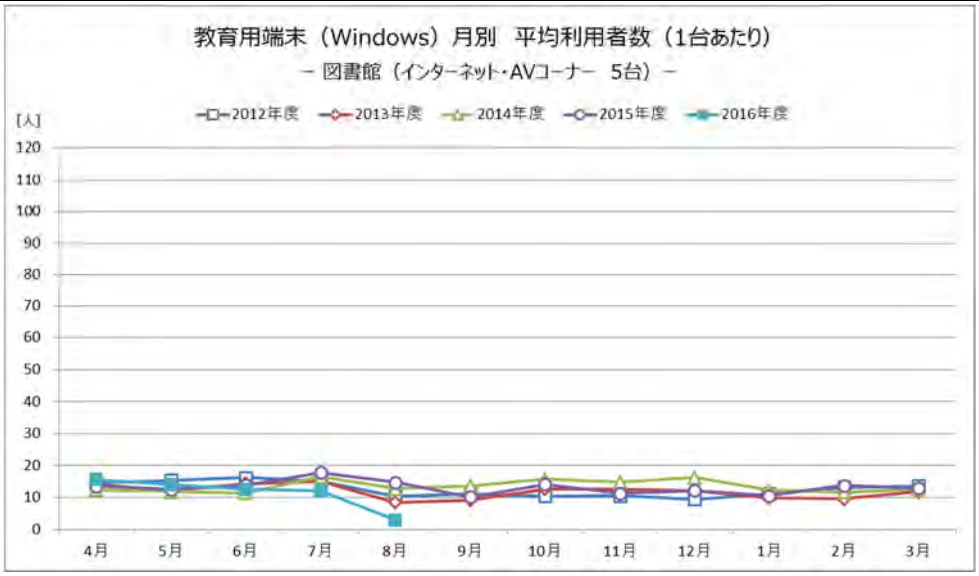
- 図書館（マルチメディア情報閲覧室）



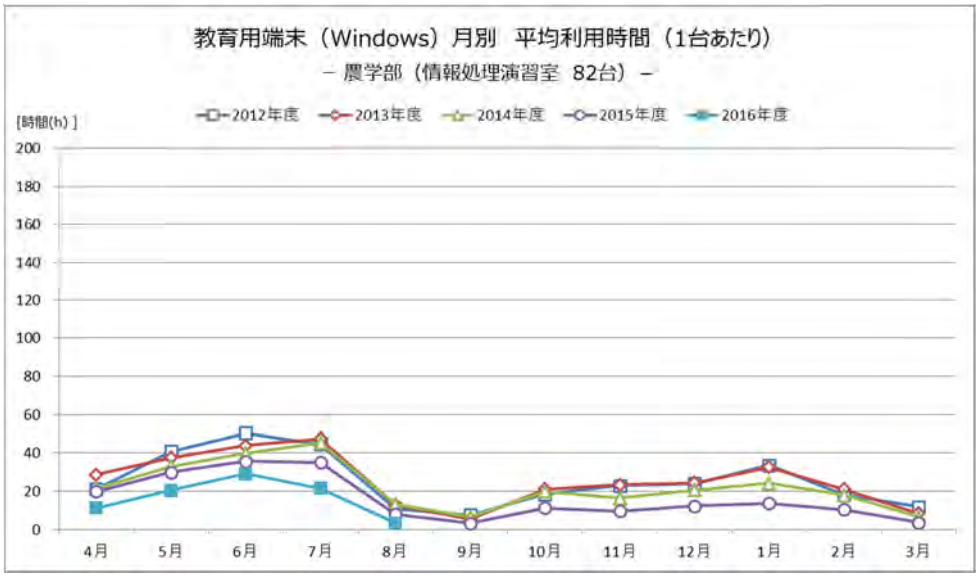


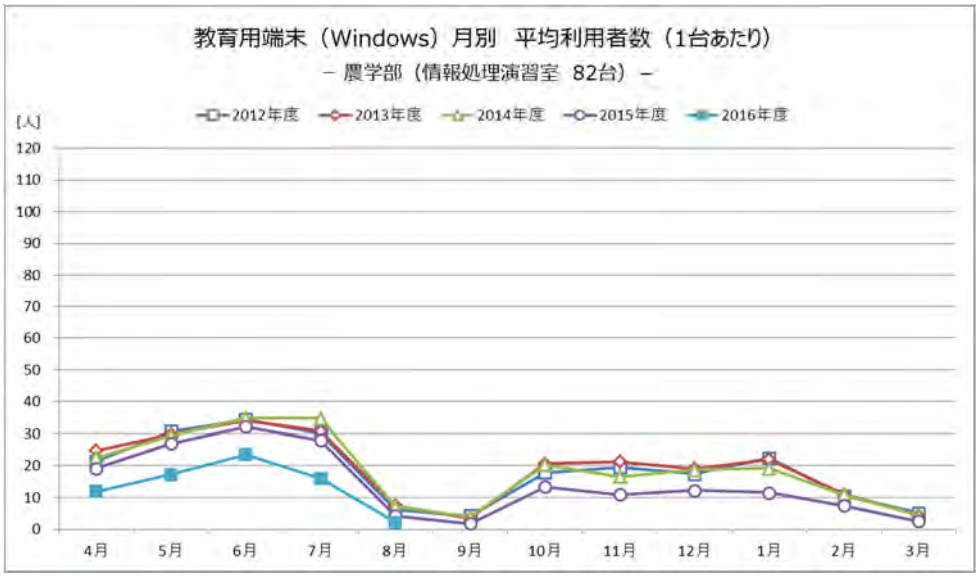
- 図書館（インターネット・AV コーナー）



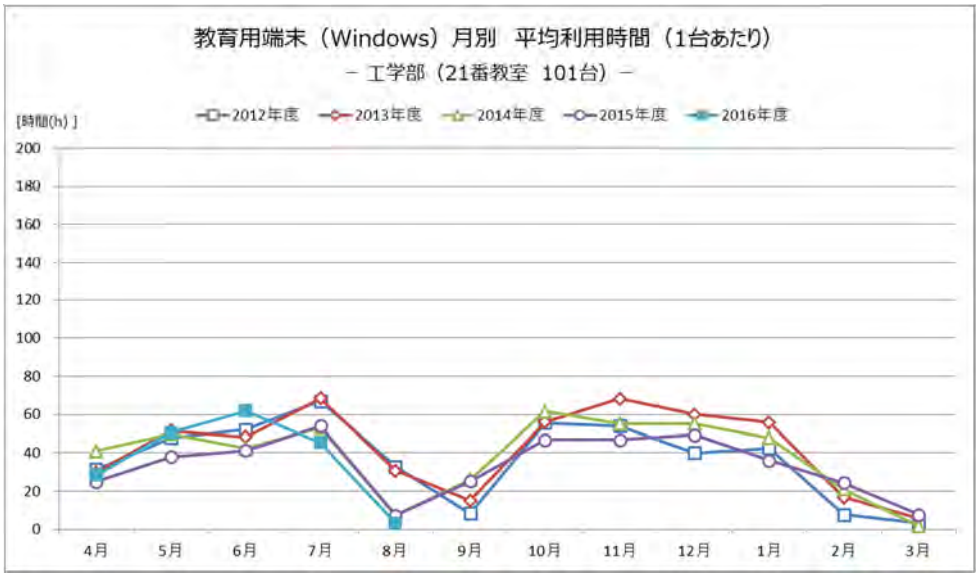

教育用端末（Windows）月別　平均利用者数（1台あたり）
－ 図書館（インターネット・AVコーナー　5台）－
[人]
2012年度
2013年度
2014年度
2015年度
2016年度
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

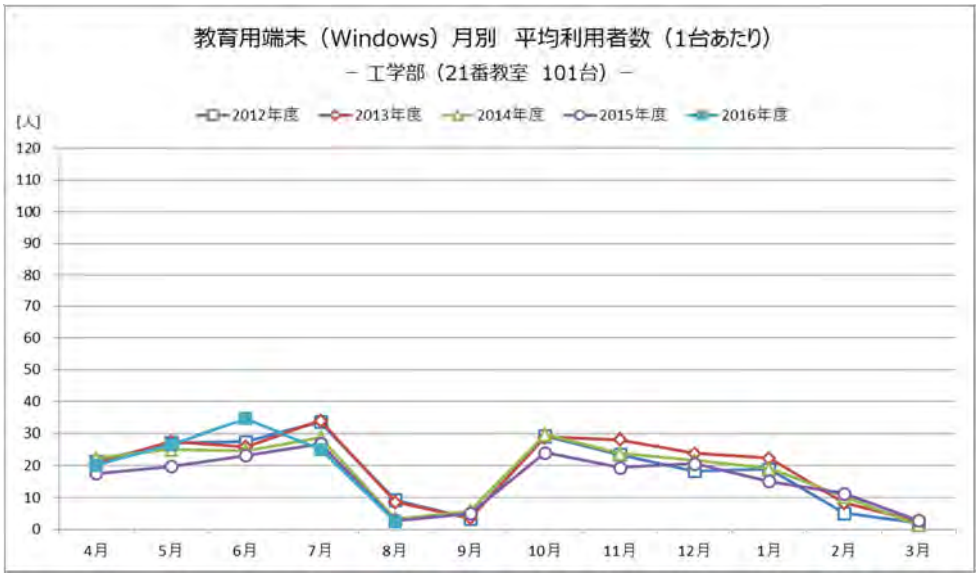
- 農学部（情報処理演習室）


教育用端末（Windows）月別　平均利用時間（1台あたり）
－ 農学部（情報処理演習室　82台）－
[時間(h)]
2012年度
2013年度
2014年度
2015年度
2016年度
200
180
160
140
120
100
80
60
40
20
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

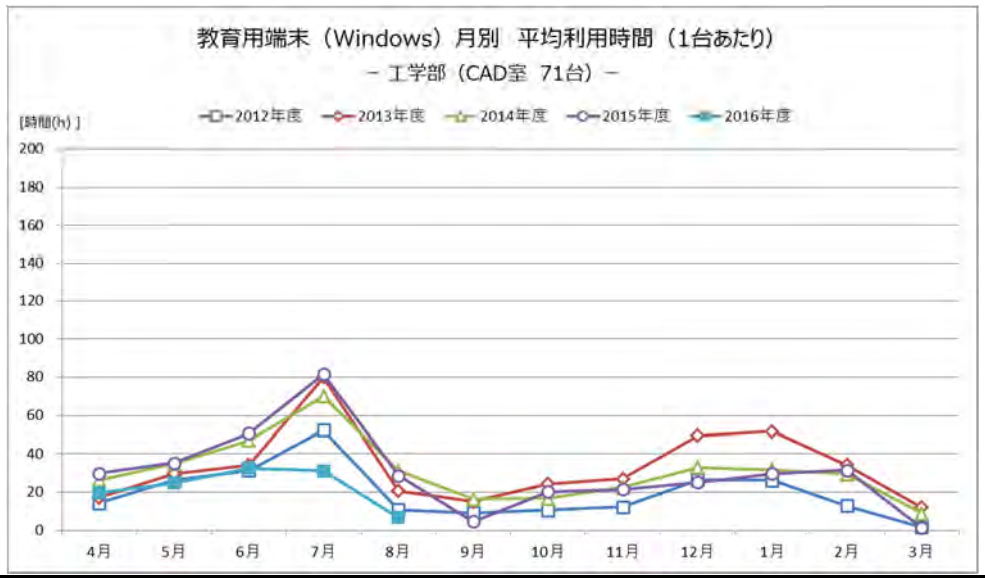

教育用端末（Windows）月別　平均利用者数（1台あたり）
－ 農学部（情報処理演習室　82台）－
[人]
2012年度
2013年度
2014年度
2015年度
2016年度
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

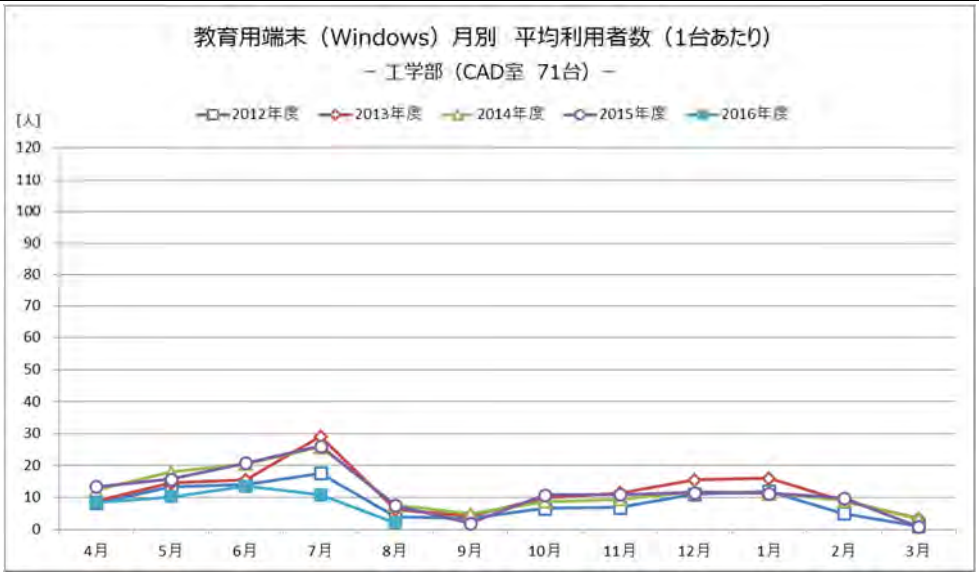
- 工学部（21 番教室）



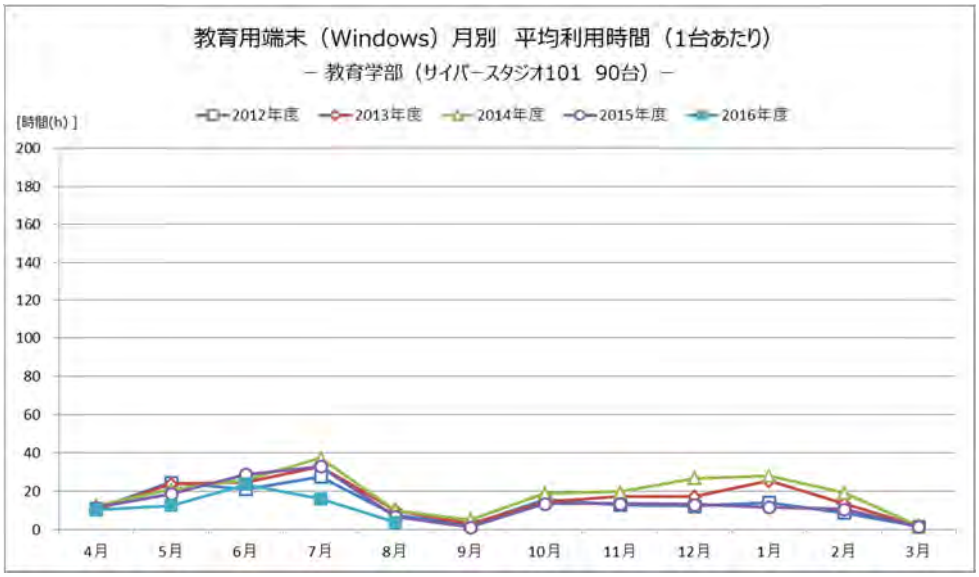


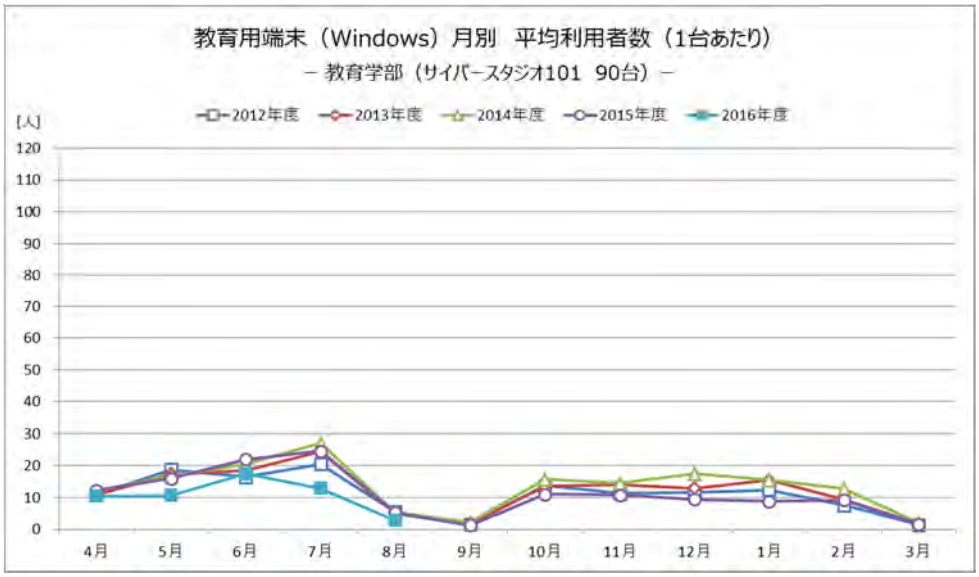
- 工学部（CAD 室）



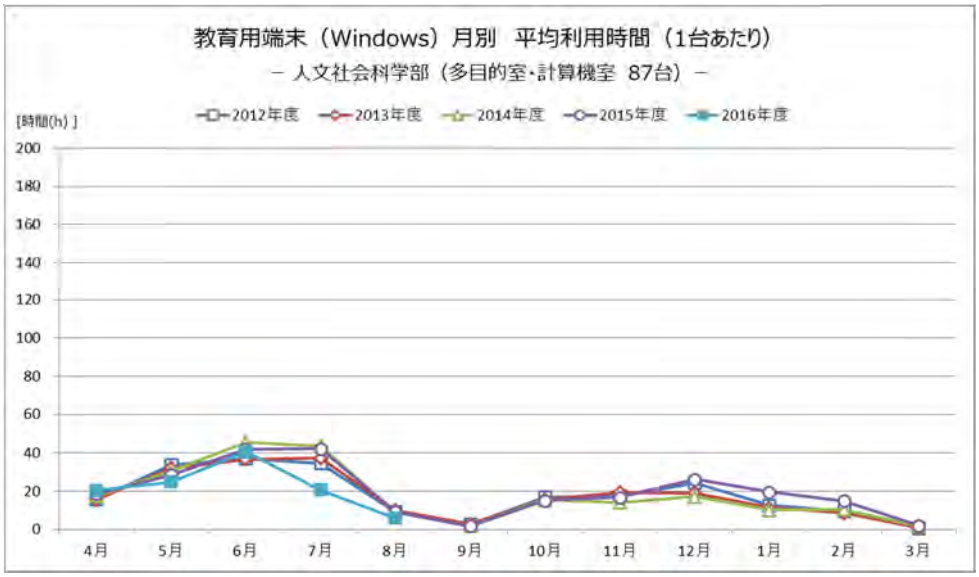


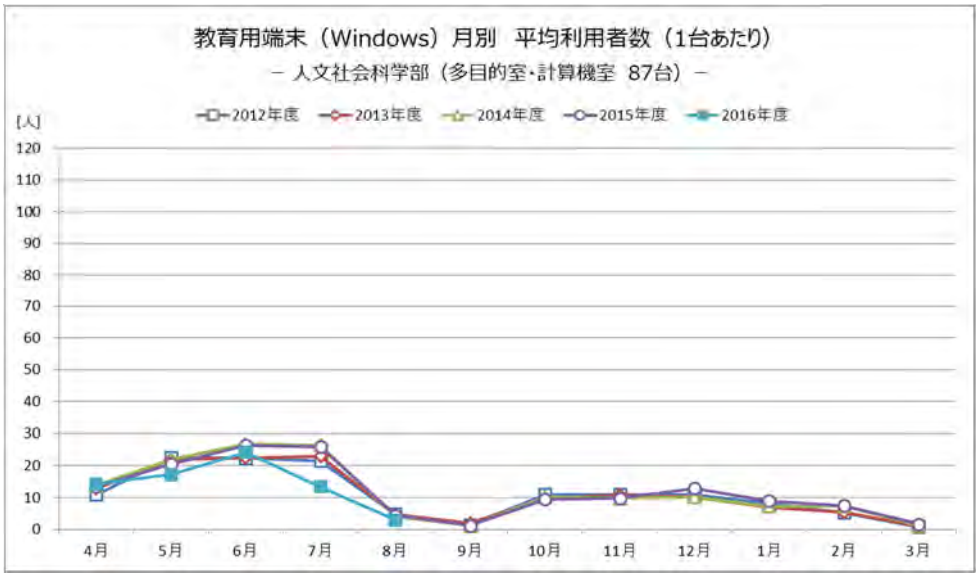
- 教育学部（サイバースタジオ 101）



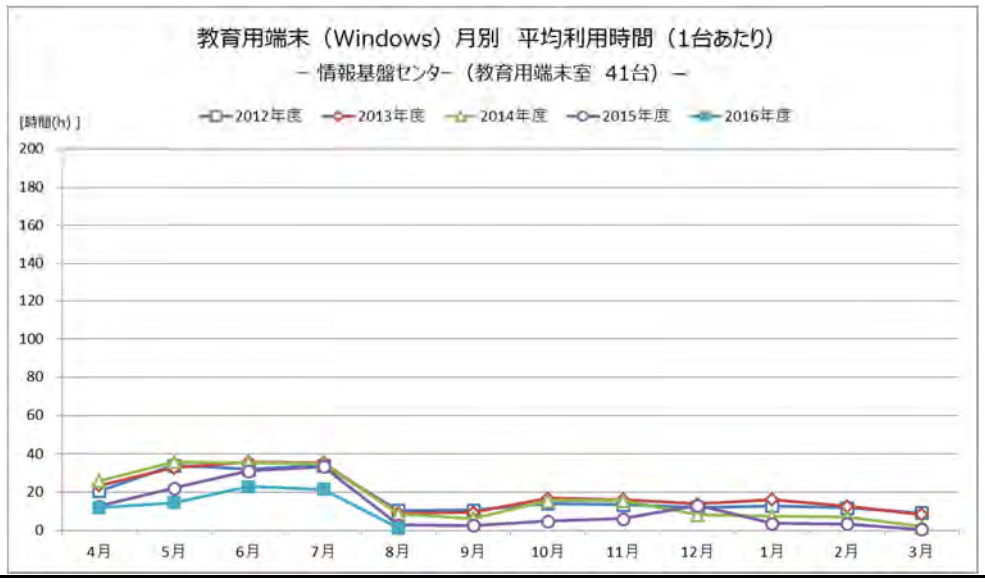


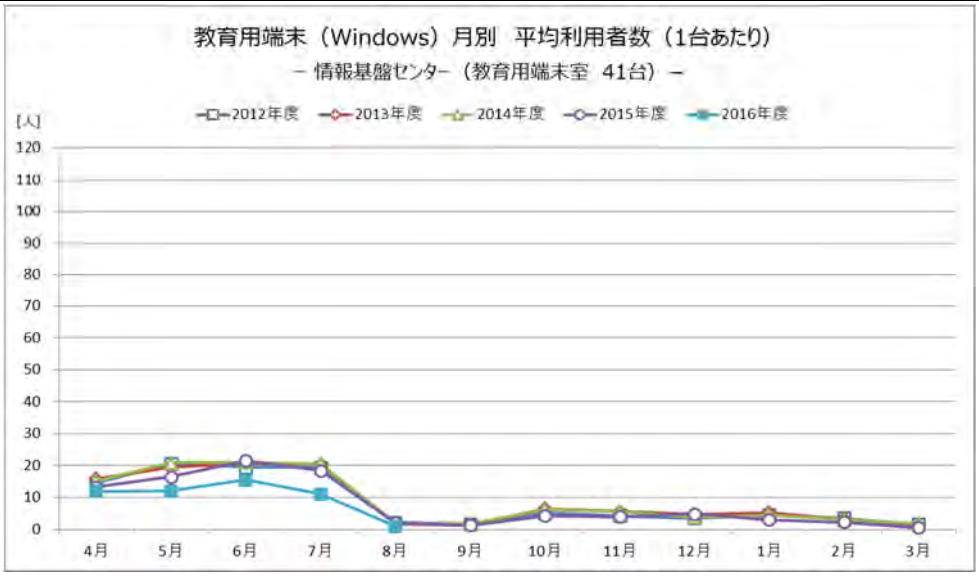
- 人文社会科学部（多目的室・計算機室）



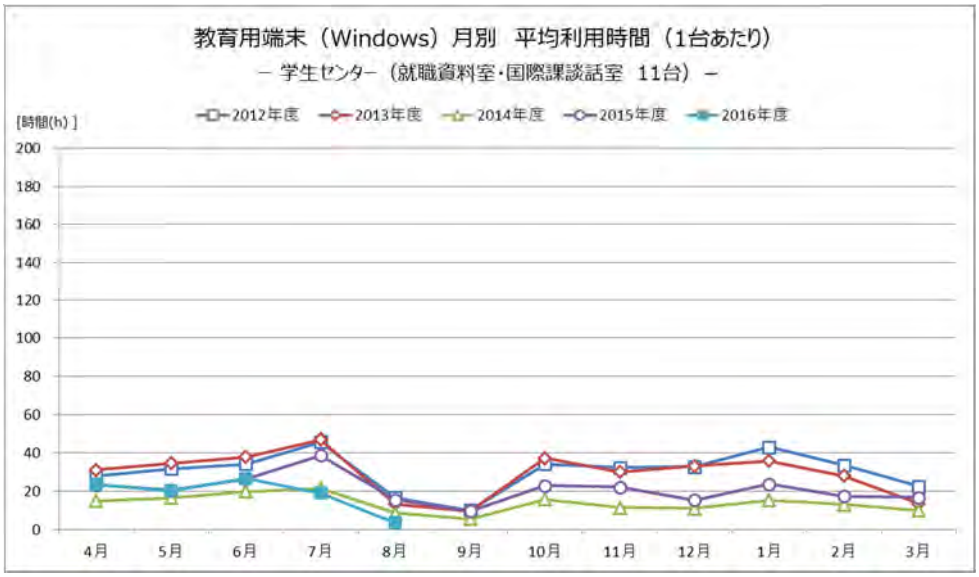


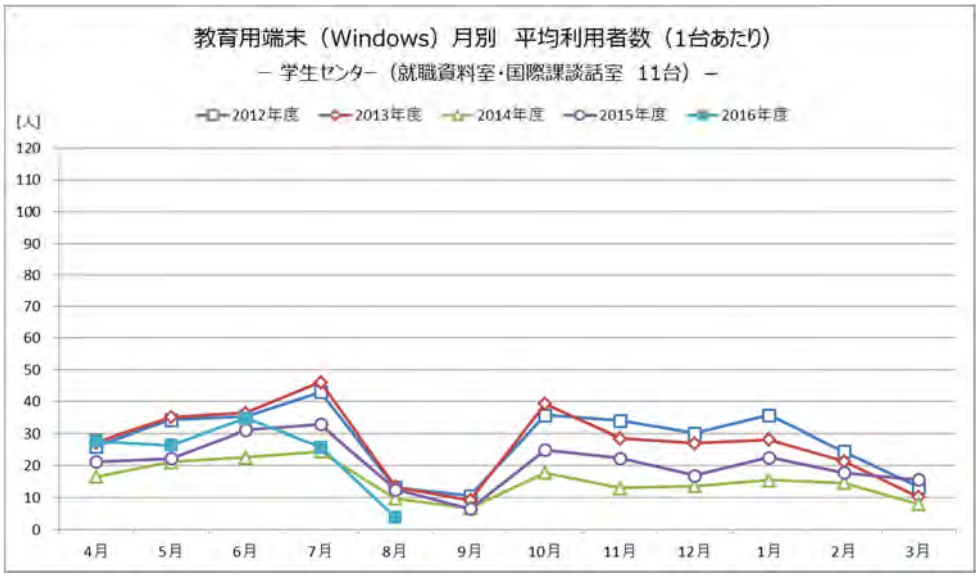
- 情報基盤センター（教育用端末室）





- 学生センター（就職資料室・国際課談話室）

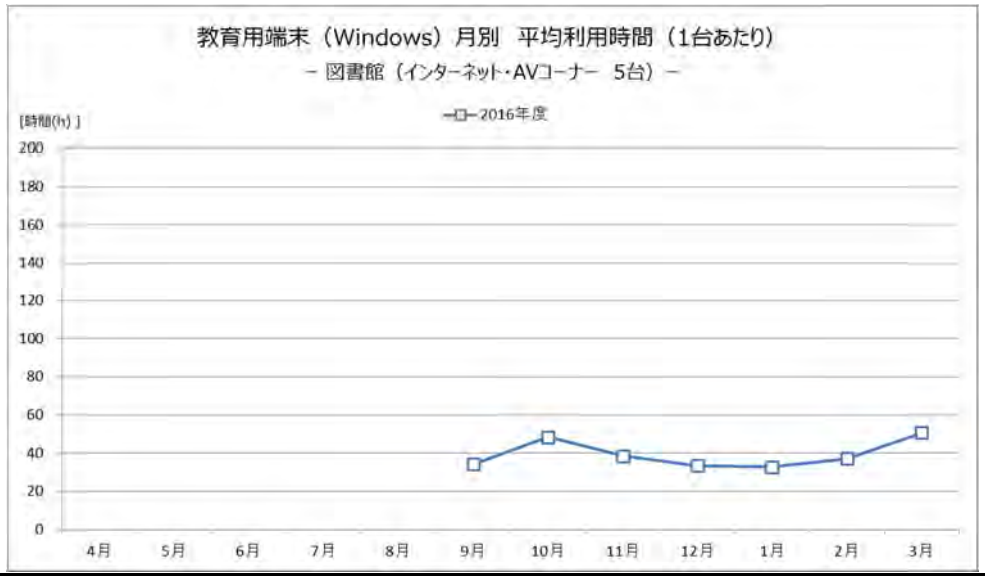




[新・教育用端末(Windows)]（2016 年 9 月～2017 年 3 月）

- 図書館（マルチメディア情報閲覧室）

- 図書館（インターネット・AV コーナー）




教育用端末（Windows）月別　平均利用者数（1台あたり）
－図書館（インターネット・AVコーナー　5台）－
2016年度
[人]
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

- 農学部（情報処理演習室）

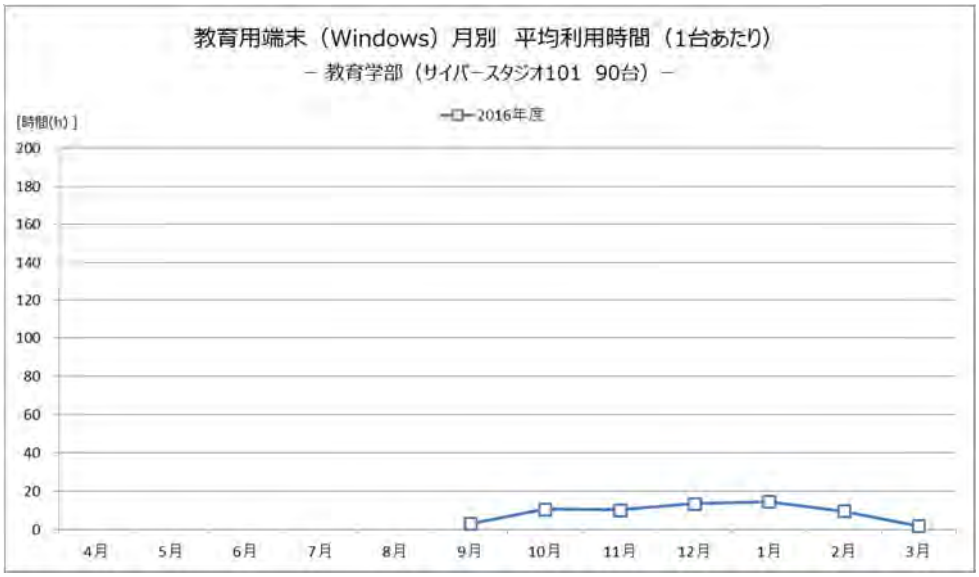

教育用端末（Windows）月別　平均利用時間（1台あたり）
－農学部（情報処理演習室　82台）－
2016年度
[時間(h)]
200
180
160
140
120
100
80
60
40
20
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月


教育用端末（Windows）月別　平均利用者数（1台あたり）
－農学部（情報処理演習室　82台）－
2016年度
[人]
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

- 理工学部（21 番教室）

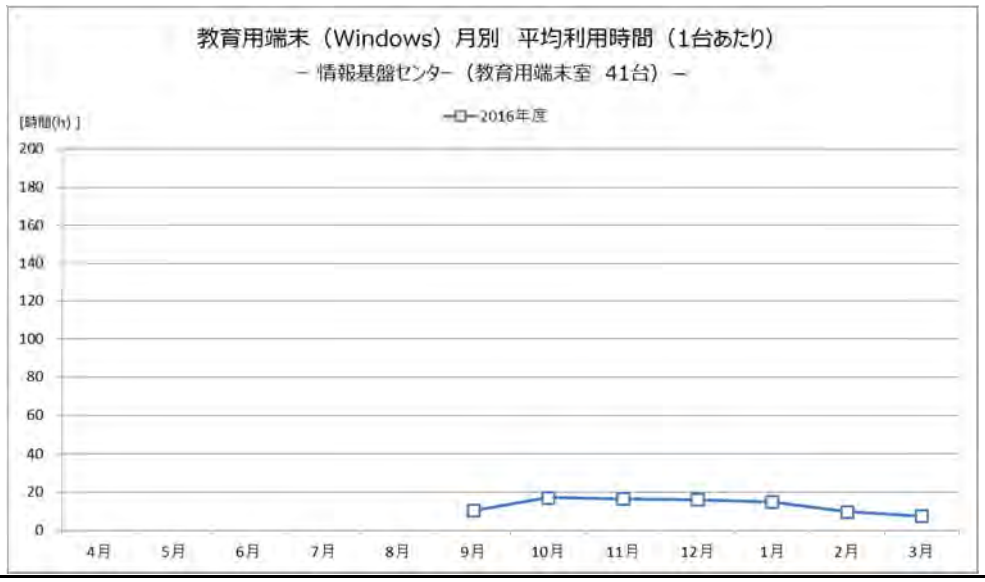
- 理工学部（CAD 室）

- 教育学部（サイバースタジオ 101）



- 人文社会科学部（多目的室・計算機室）

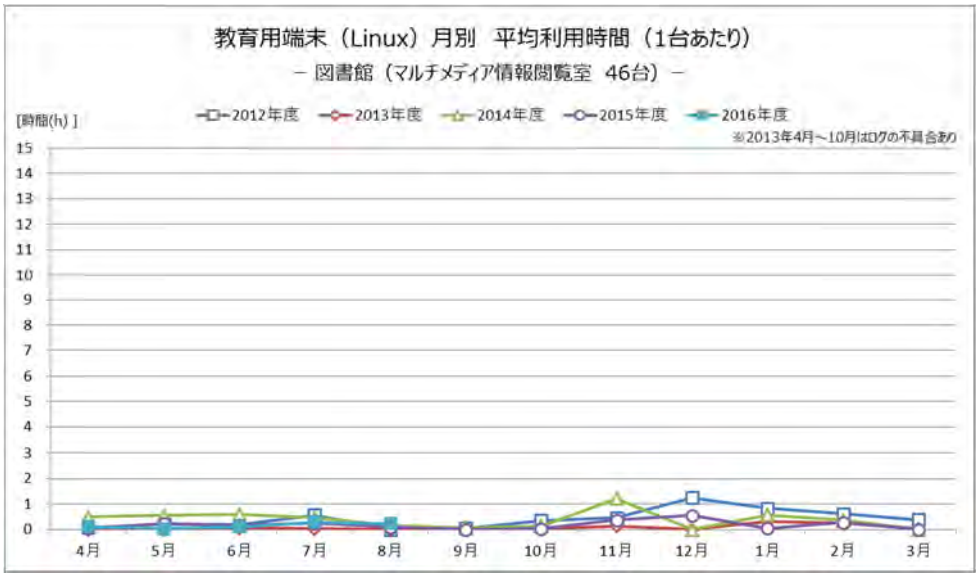
- 情報基盤センター（教育用端末室）

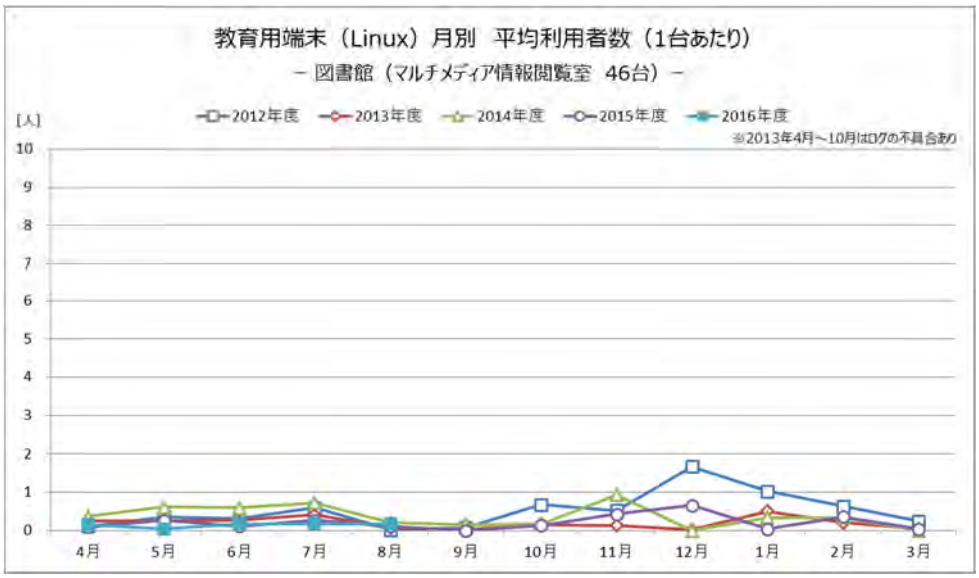


- 学生センターB棟（キャリアフリールーム・国際交流情報室・グローバルビレッジ）

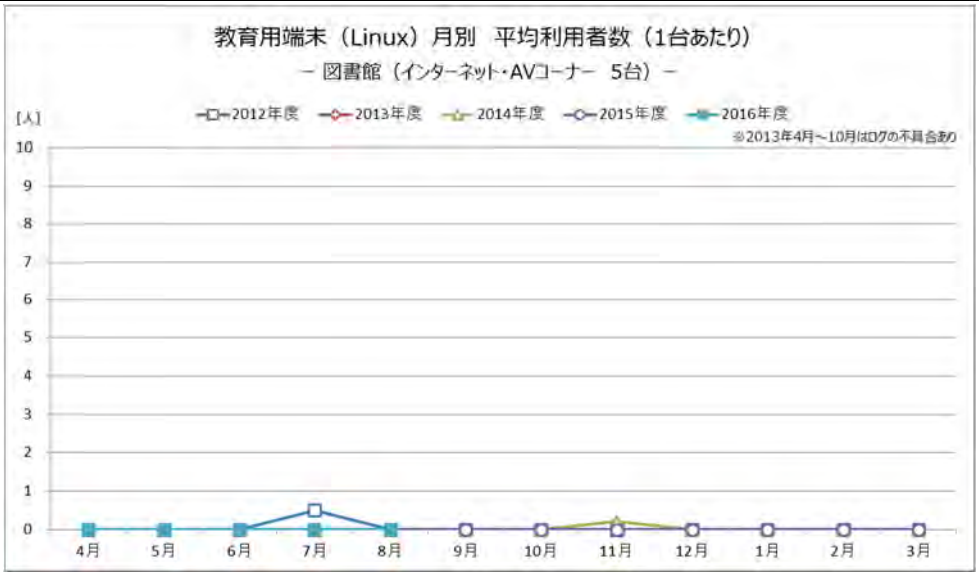
[旧・教育用端末(Linux)]（2012 年 4 月～2016 年 8 月）

- 図書館（マルチメディア情報閲覧室）

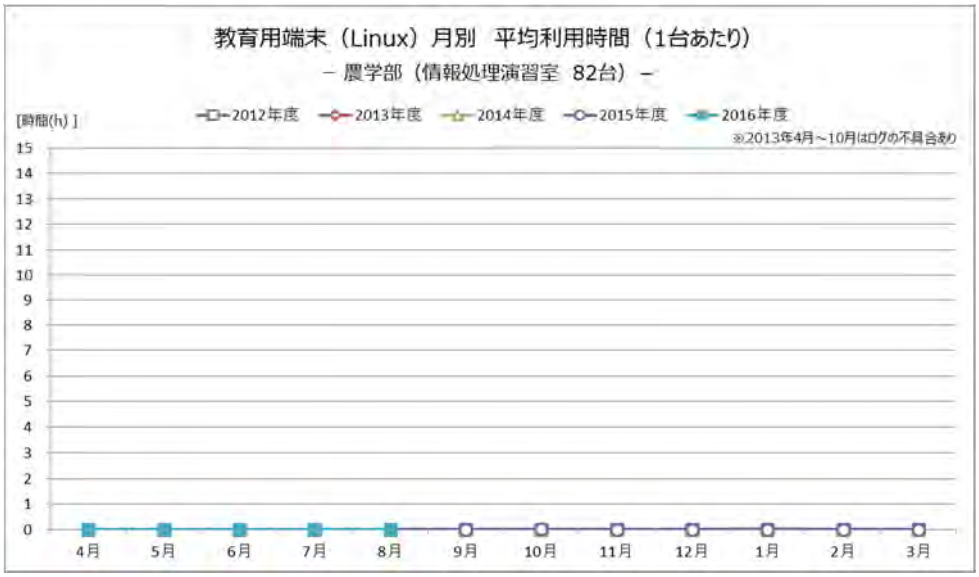




- 図書館（インターネット・AV コーナー）

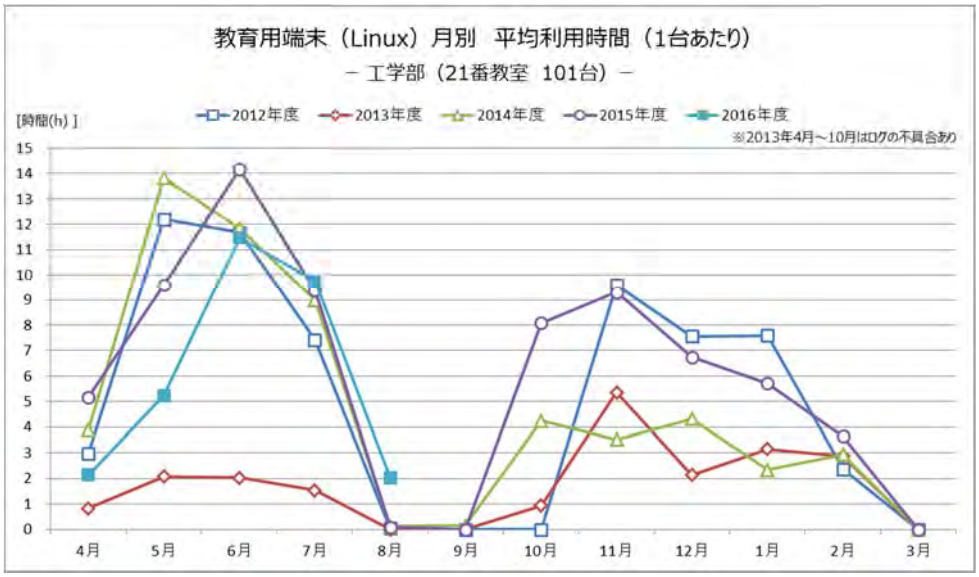

教育用端末（Linux）月別　平均利用者数（1台あたり）
－ 図書館（インターネット・AVコーナー　5台）－
[人]
2012年度
2013年度
2014年度
2015年度
2016年度
※2013年4月～10月はログの不具合あり
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

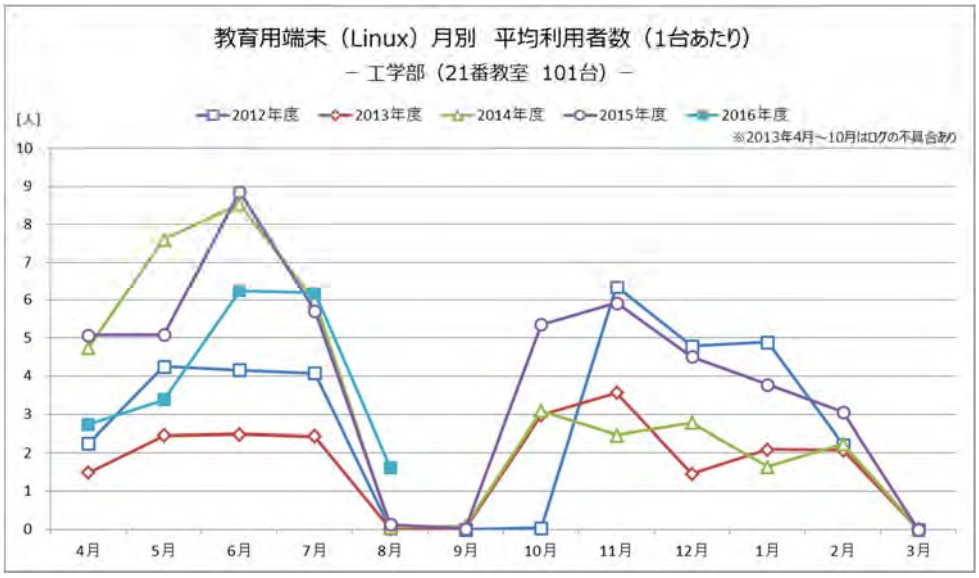
- 農学部（情報処理演習室）


教育用端末（Linux）月別　平均利用時間（1台あたり）
－ 農学部（情報処理演習室　82台）－
[時間(h)]
2012年度
2013年度
2014年度
2015年度
2016年度
※2013年4月～10月はログの不具合あり
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

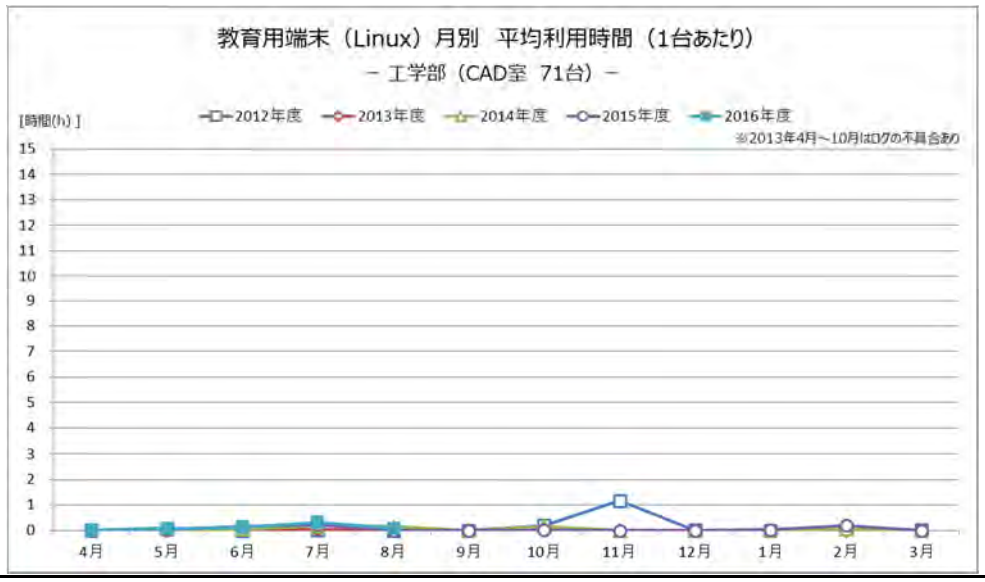

教育用端末（Linux）月別　平均利用者数（1台あたり）
－ 農学部（情報処理演習室　82台）－
[人]
2012年度
2013年度
2014年度
2015年度
2016年度
※2013年4月～10月はログの不具合あり
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

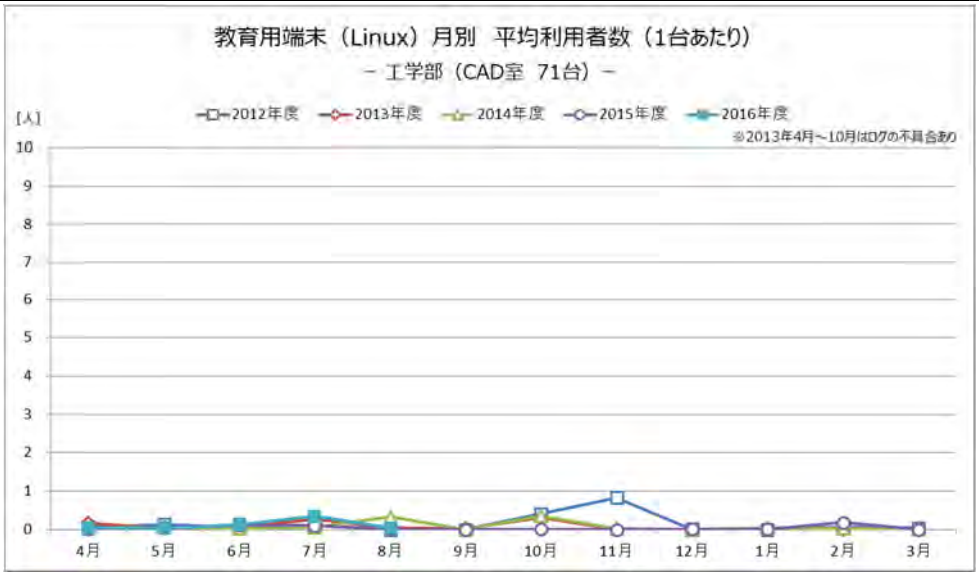
- 工学部（21 番教室）



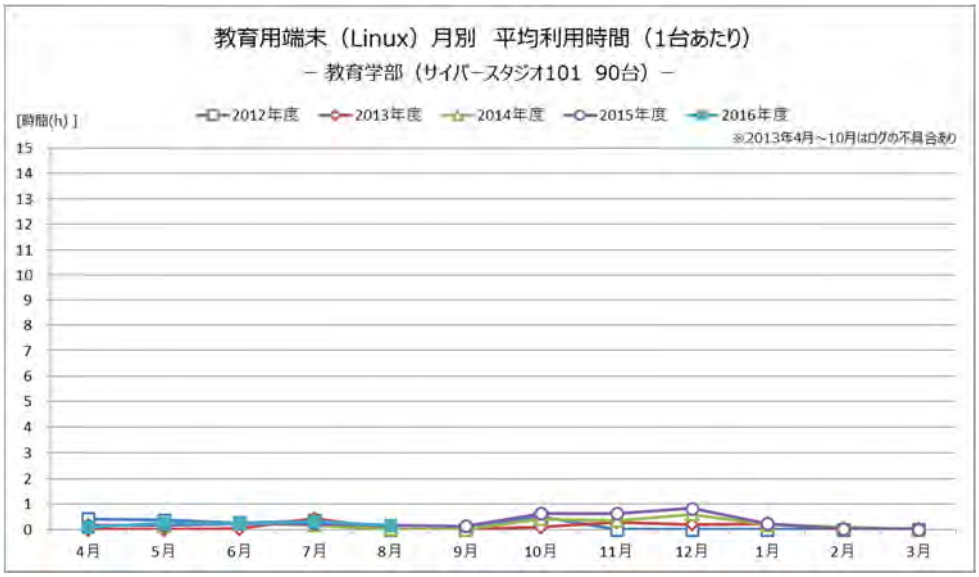


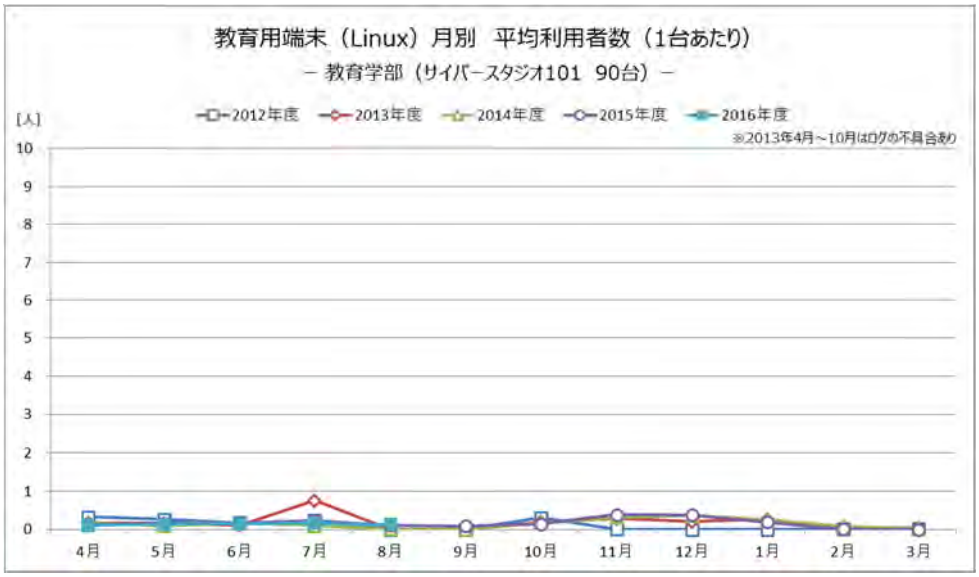
- 工学部（CAD 室）



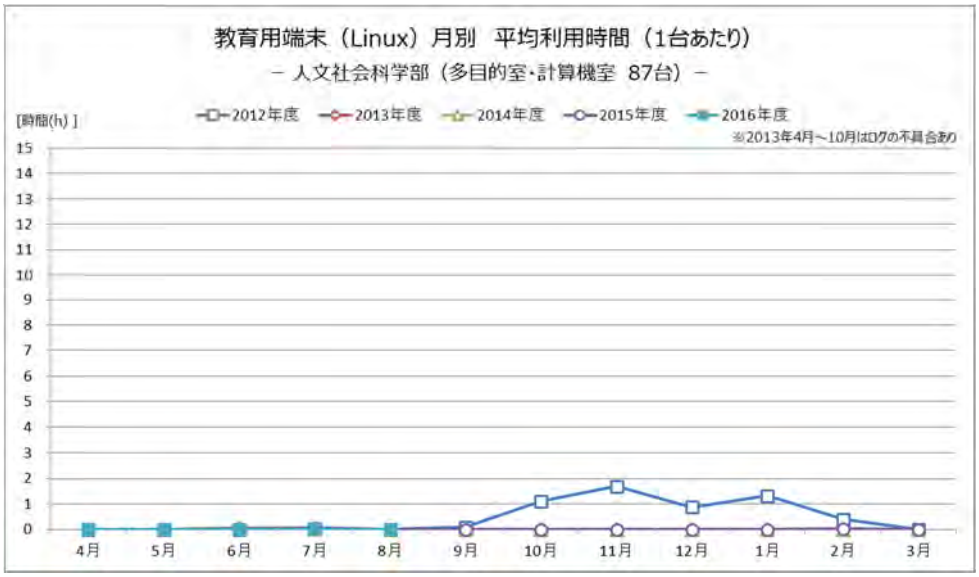


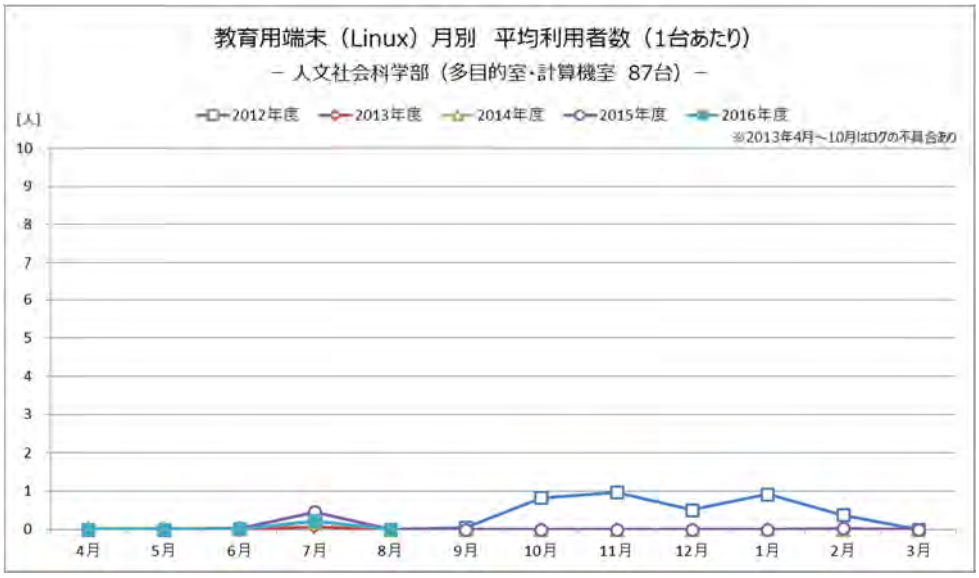
- 教育学部（サイバースタジオ 101）



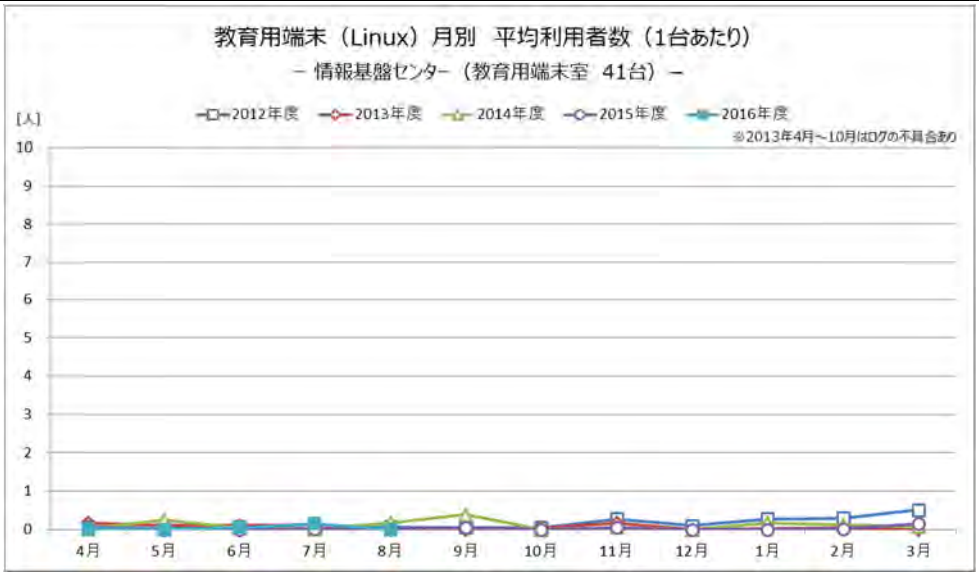


- 人文社会科学部（多目的室・計算機室）

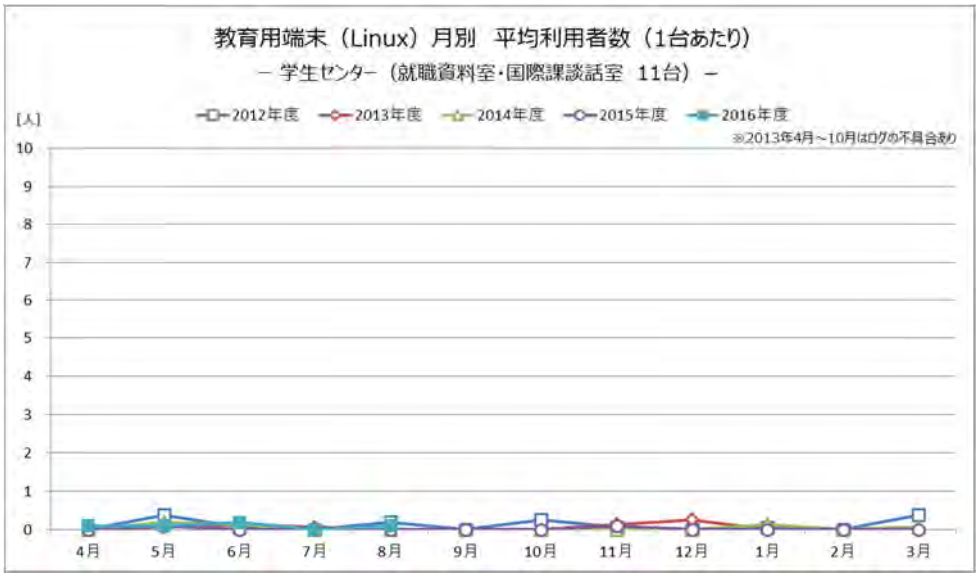




- 情報基盤センター（教育用端末室）

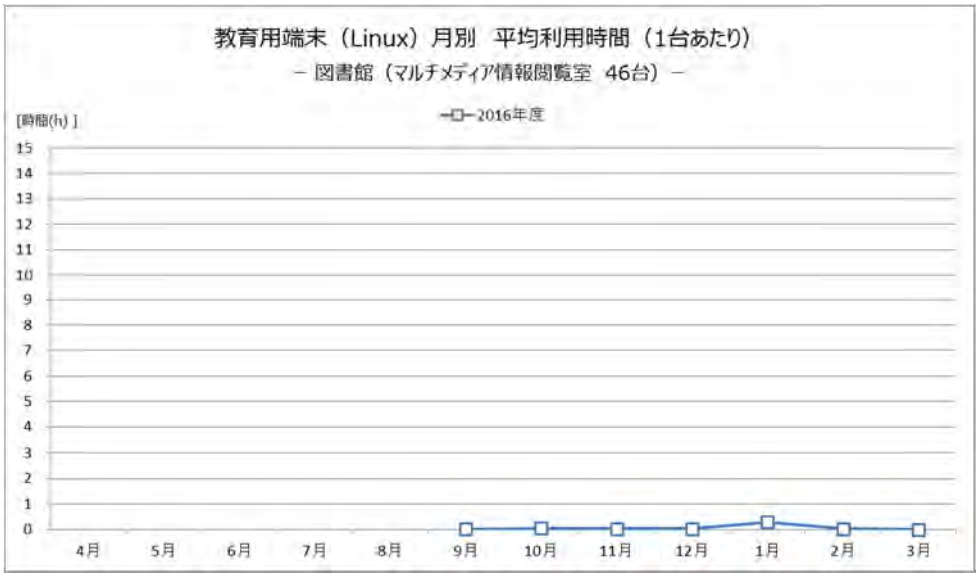


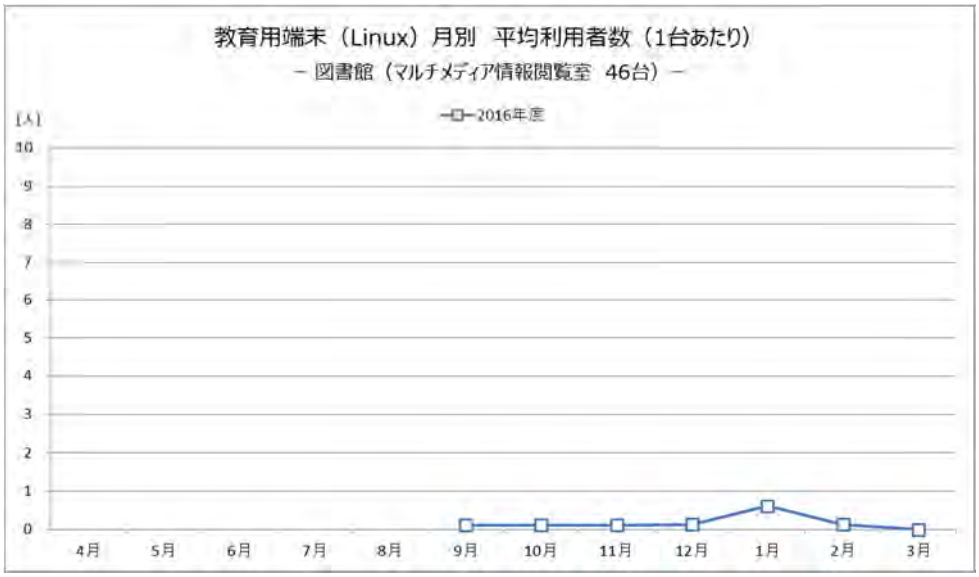
- 学生センター（就職資料室・国際課談話室）



[新・教育用端末(Linux)]（2016 年 9 月～2017 年 3 月）

- 図書館（マルチメディア情報閲覧室）

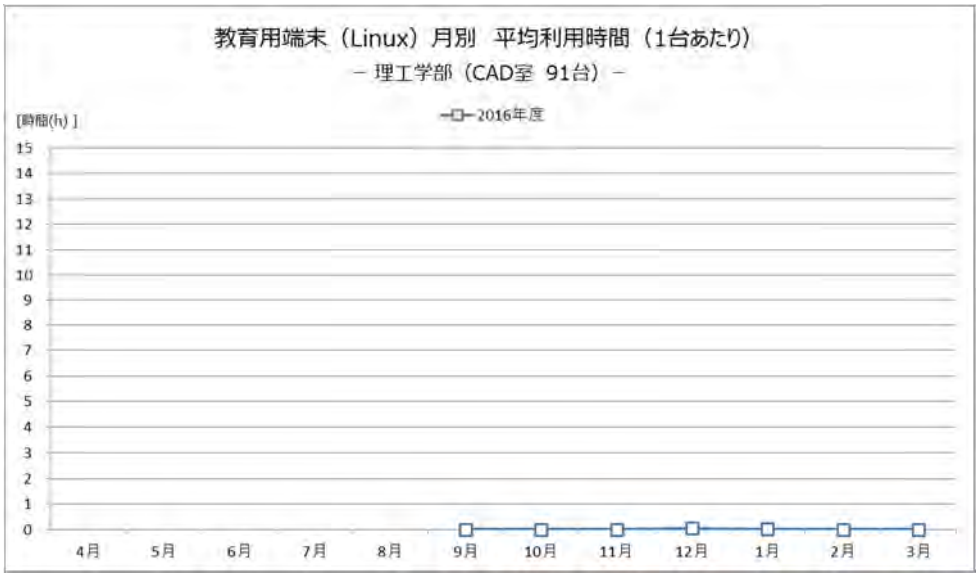


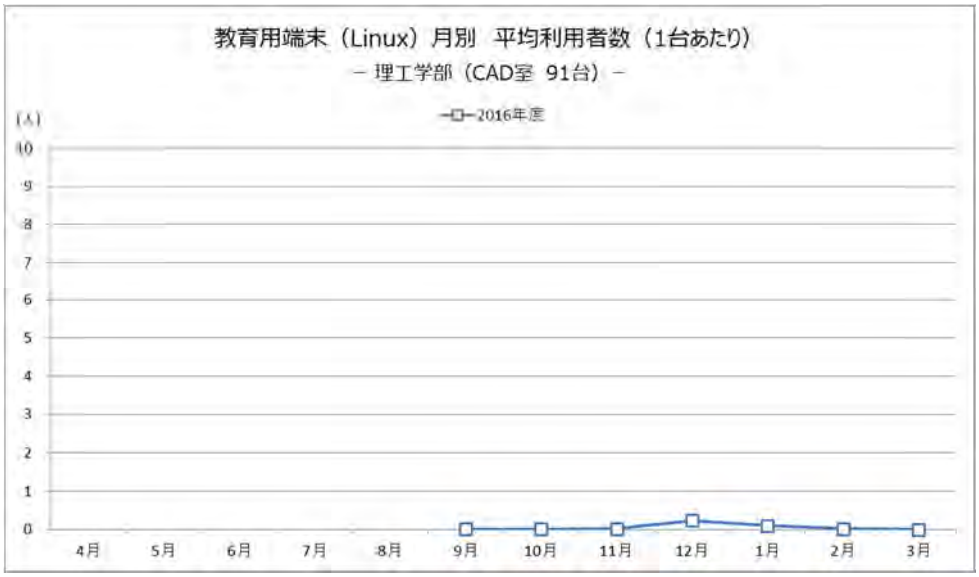


- 理工学部（21 番教室）

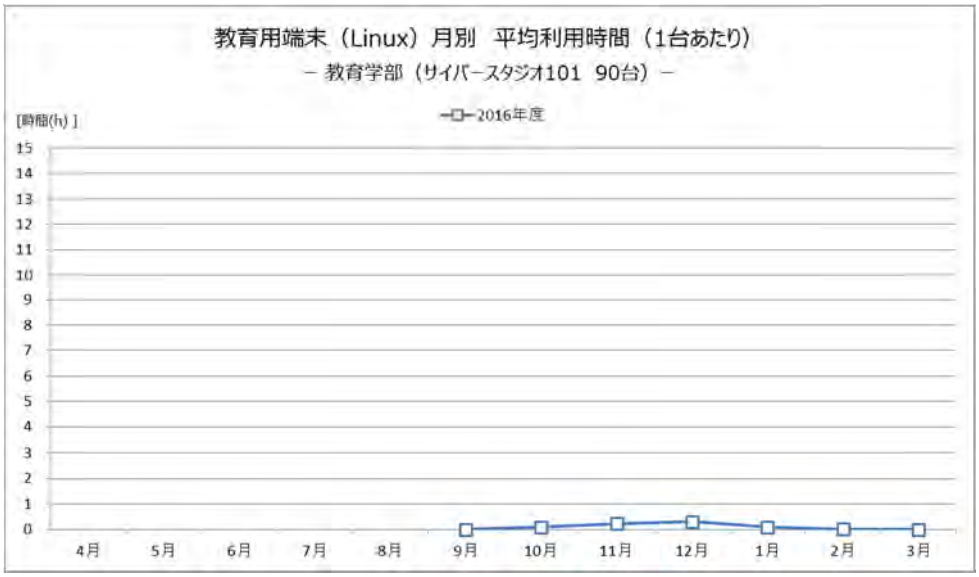

教育用端末（Linux）月別　平均利用者数（1台あたり）
－ 理工学部（21番教室　101台）－
2016年度
[人]
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

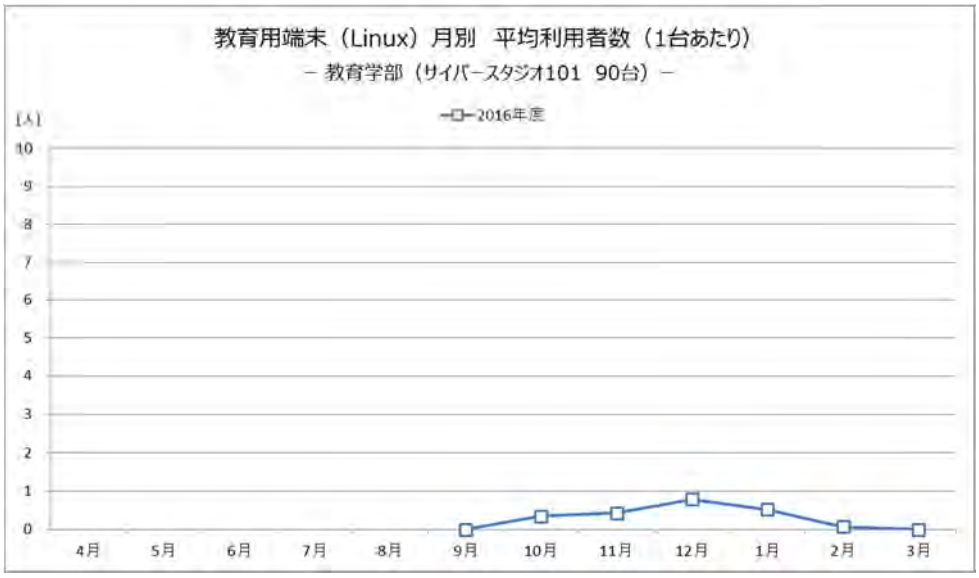
- 理工学部（CAD 室）


教育用端末（Linux）月別　平均利用時間（1台あたり）
－ 理工学部（CAD室　91台）－
2016年度
[時間(h)]
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

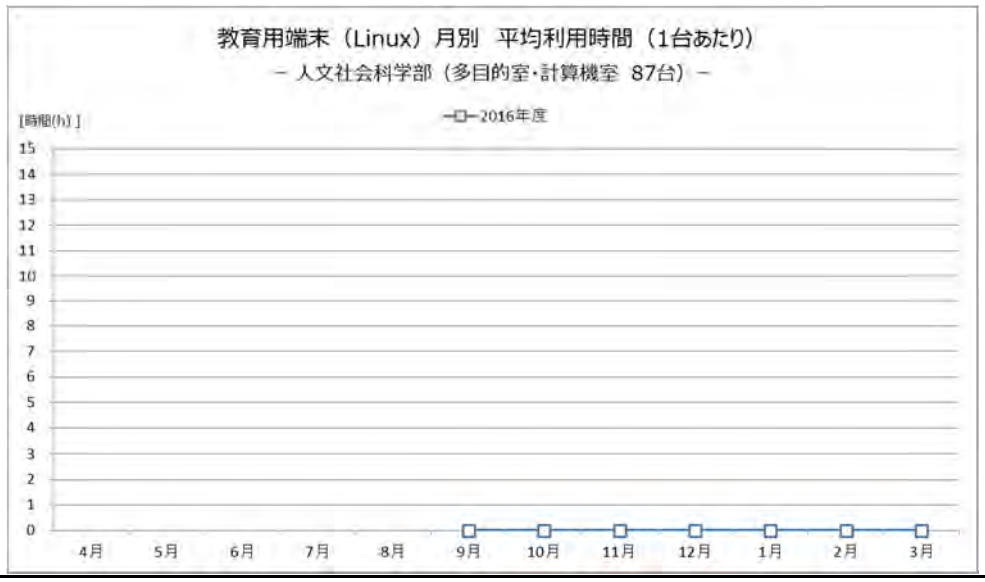

教育用端末（Linux）月別　平均利用者数（1台あたり）
－ 理工学部（CAD室　91台）－
2016年度
[人]
10
9
8
7
6
5
4
3
2
1
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

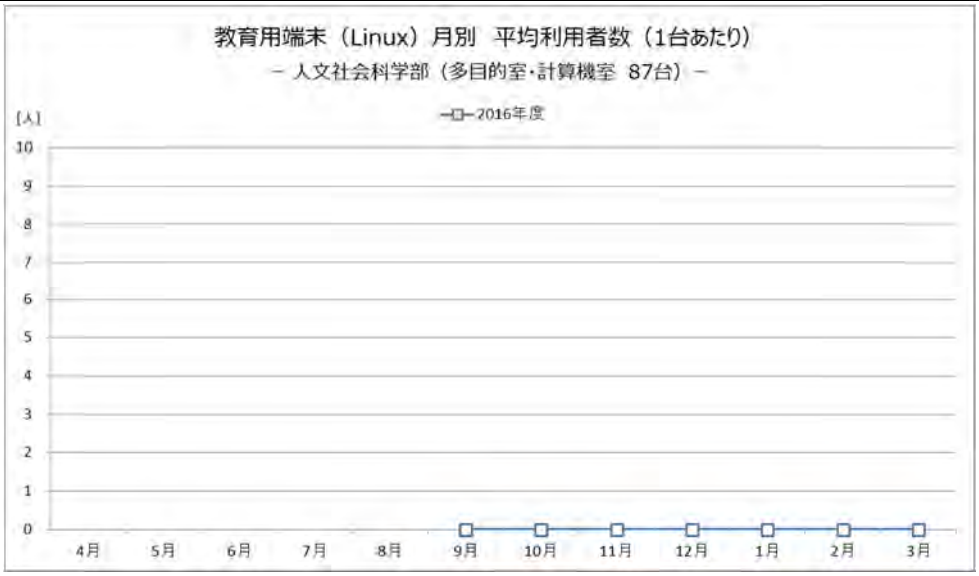
- 教育学部（サイバースタジオ 101）



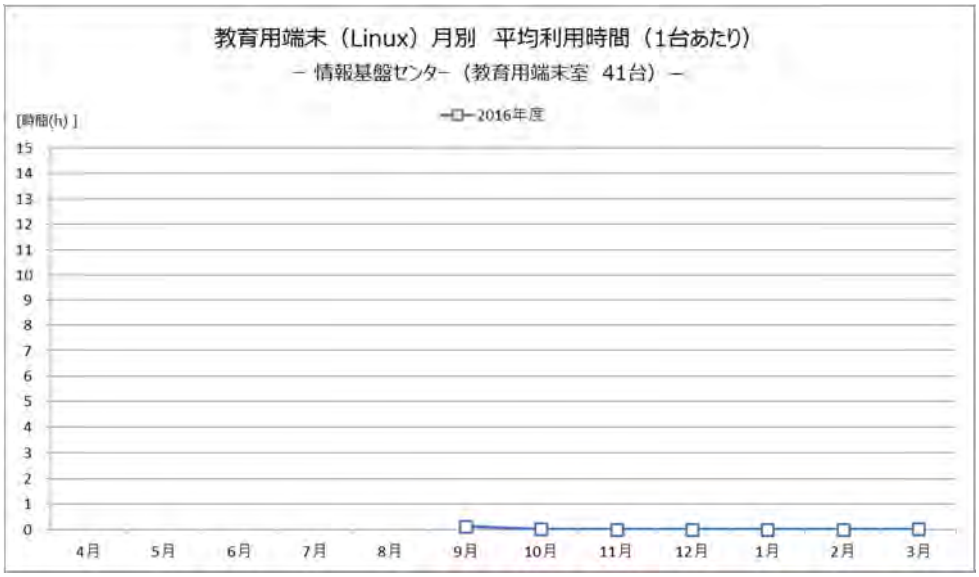


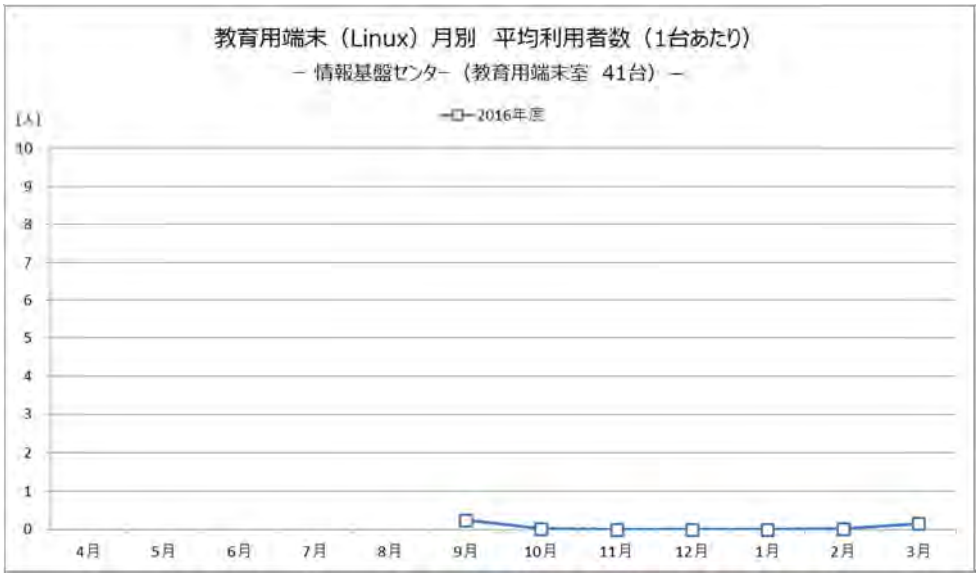
- 人文社会科学部（多目的室・計算機室）





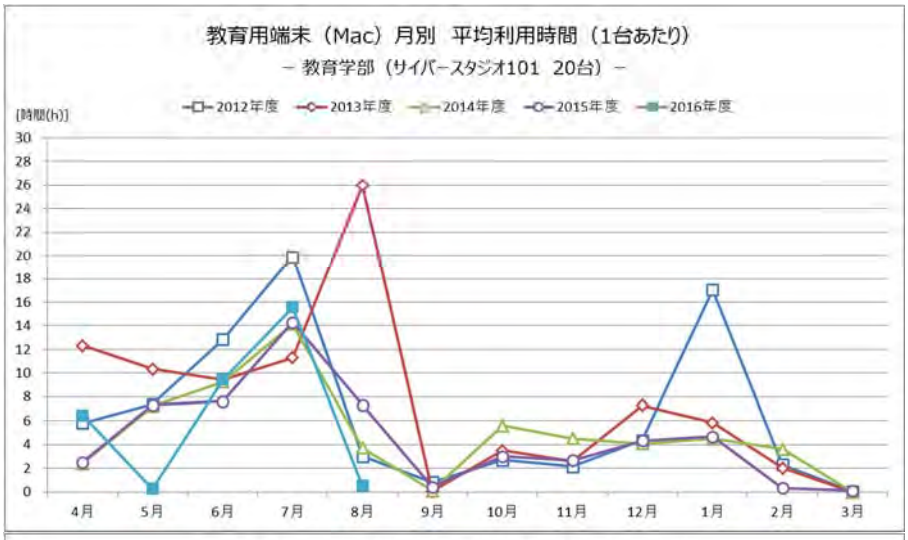
- 情報基盤センター（教育用端末室）

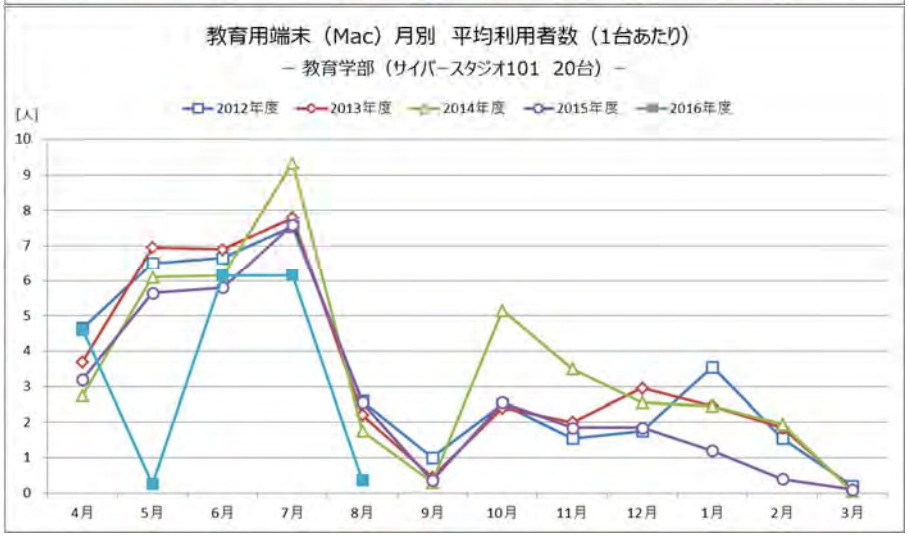




[旧・教育用端末(Mac)]（2012 年 4 月～2016 年 8 月）

- 教育学部（サイバースタジオ 101）

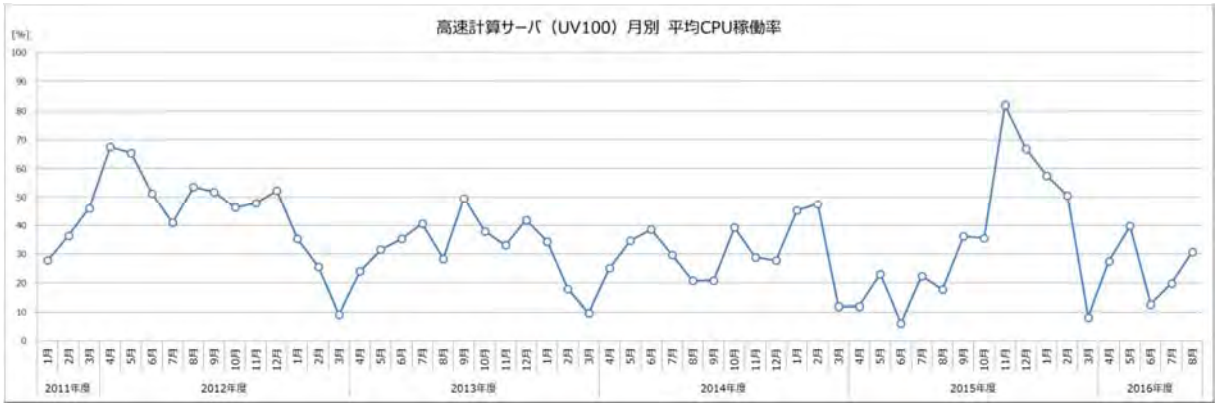




[新・教育用端末(Mac)]（2016 年 9 月～2017 年 3 月）

- 教育学部（サイバースタジオ 101）

[旧・高速計算サーバ(SGI-UV100)]（2012 年 4 月～2016 年 8 月）



[新・高速計算サーバ(東北大学サイバーサイエンスセンター)]（2016 年 9 月～2017 年 3 月）

[ネットワーク障害対応]

2014 年度　15 件
2015 年度　16 件
2016 年度　11 件

[遠隔教育（収録・VOD）]

2014 年度　56 件
2015 年度　64 件
2016 年度　48 件

[ユーザサポート対応]

2014 年度　114 件
2015 年度　125 件
2016 年度　190 件

[CSIRT 対応]

2016 年度

問い合わせへの対応	81 件
講習会の開催	16 件
印刷物の発行・配布	4 件
VOD 配信	3 件
臨時等の情報発信	26 件
学習用コンテンツ作成	2 件
調査等	25 件

【利用の成果】

高速計算サーバ（UV100）利用の成果

1. 平成 28 年度研究発表目録

1.1. 学術論文，学会発表等

- 大学院工学研究科
  - 応用化学・生命工学専攻
    - Hiroki Muraoka, Takumi Obara, and Satoshi Ogawa：“Systematic synthesis, comparative studies of the optical properties, and the ICT-based sensor properties of a series of 2,4,6-tri(5-aryl-2-thienyl)pyrimidines with the D-?-A system”, Tetrahedron Lett. 2016, 57, 3011.
    - Yuta Toiguchi, Hitoshi Yashiro, Eiichi Suzuki, “Matrix-isolation infrared spectra of fluorinated sulfonic acids”, 平成 28 年度化学系学協会東北大会講演要旨集, 1P032, (2016).
    - 平 丁徳，八代 仁，鈴木 映一：低温マトリックス法と量子化学計算による亜硝酸メチル,チオ亜硝酸メチル―三フッ化ホウ素錯体の構造と性質, 第 10 回分子科学討論会講演予稿集, 3P107, (2016).
    - 池田咲季，八代仁，鈴木映一：“ナフタレン誘導体/β-シクロデキストリン包接錯体結晶の発光に及ぼす第三成分の影響，第 10 回分子科学討論会講演予稿集，3P050，（2016）.
    - Eiichi Suzuki, Gaku Taguchi, Yuta Toiguchi, Hitoshi Yashiro, “Thionyl chloride-methanol complex: a quantum chemical and matrix-isolation study”, 日本化学会第 97 春季年会講演要旨集, 1PA-010, (2017).
  - フロンティア材料機能工学専攻
    - Seiji Uryu : “Numerical study on collective excitations in graphene”, Physical Review B 94 (2016) 155451.
- 教育学部
  - 技術教育科
    - Hitoaki Yoshida, Takeshi Murakami, Taiki Inao, and Satoshi Kawamura : “Origin of Randomness on Chaos Neural Network”, Trends in Applied Knowledge-Based Systems and Data Science, Vol.9799, (2016) pp.587-598.
    - Hitoaki Yoshida, Mitsuaki SASAKI and Takeshi Murakami : “Implementation of Chaos Neural Network which Generates Multi-Subseries with Different Periods”, Proceedings of The 34th JSTE Tohoku Section Conference, (2016) pp.57-58.

* Hitoaki Yoshida, Mitsuaki SASAKI, Takeshi Murakami and Satoshi KAWAMURA : “Study on Properties of Periodic Chaos and Controlling Method of Islands in Chaos Neural Network Outputs”, Proceedings of The 34th JSTE Tohoku Section Conference, (2016) pp.59-60.

- 情報基盤センター

* Satoshi KAWAMURA and Hitoaki YOSHIDA : “KANSEI (Emotional) Information Classifications of Music Scores Using Self Organizing Map”, Trends in Applied Knowledge-Based Systems and Data Science, Vol.9799, (2016) pp.574-586.

* Satoshi KAWAMURA, Masato Saito, and Hitoaki YOSHIDA : “FPGA Implementation of Neuron Model Using Piecewise Nonlinear Function on Double-Precision Floating-Point Format”, Trends in Applied Knowledge-Based Systems and Data Science, Vol.9799, (2016) pp.620-629.

1.2. 修士論文

- 大学院工学研究科

– 応用化学・生命工学専攻

* 小原　巧弥　：含窒素複素芳香環をコアユニットに用いた星型オリゴチオフェン誘導体の合成および物性

* カン　ジャスミン：ヘテロールをコアユニットとする縮環型オリゴチオフェン誘導体の合成と物性
* 小向　和希　：屈曲した分子構造を持つπ共役拡張型ドナー分子群の合成と有機半導体への応用

* 佐々木ひかる：金属イオン認識部位を導入した星型 1,3,5-トリアジン誘導体の合成と蛍光センシング特性

* 池田　咲季　：シクロデキストリン－有機芳香族分子包接結晶の発光特性と構造

* 平　　丁徳　：シクロデキストリン誘導体に包接された有機分子の励起三重項ダイナミックス

– フロンティア材料機能工学専攻

* 佐藤　宏樹　：リチウムイオン二次電池における室温イオン液体／天然黒鉛電極界面での電気学的挙動の解明

1.3. 学士論文

- **工学部**
  - **応用化学・生命工学科**
    - ＊ 大久保　晃裕：アリール基で機能化したテトラチエニルエチレン誘導体の合成と物性
    - ＊ 金澤　　桃　：シクロデキストリンに包接されたナフタレン誘導体の光化学反応
    - ＊ 津田　悠介　：シクロデキストリンに包接された芳香族分子の長寿命励起三重項減衰過程
    - ＊ 田口　　学　：低温マトリックス赤外分光法による塩化チオニルとアルコールの相互作用に関する研究
- **教育学部**
  - **技術教育科**
    - ＊ 下野　翔吾　：一般的なカオスから抽出した乱数の性質

東北大学サイバーサイエンスセンター大規模科学計算システム

利用の成果

1. 平成 28 年度研究発表目録

1.1. 学術論文，学会発表等

- 大学院工学研究科

  - 応用化学・生命工学専攻

    * Yuta Toiguchi, Hitoshi Yashiro, Eiichi Suzuki, “Matrix-isolation infrared spectra of fluorinated sulfonic acids”，平成 28 年度化学系学協会東北大会講演要旨集, 1P032, (2016).

    * 平 丁徳，八代 仁，鈴木 映一：低温マトリックス法と量子化学計算による亜硝酸メチル,チオ亜硝酸メチル―三フッ化ホウ素錯体の構造と性質, 第 10 回分子科学討論会講演予稿集, 3P107, (2016).

    * Eiichi Suzuki, Gaku Taguchi, Yuta Toiguchi, Hitoshi Yashiro, “Thionyl chloride-methanol complex: a quantum chemical and matrix-isolation study”, 日本化学会第 97 春季年会講演要旨集, 1PA-010, (2017).

  - 機械システム工学専攻

    * 中村牧人，上野和之，竹田裕貴（岩手大）：直交カットセル法を用いた圧縮性流れ解析，第 30 回数値流体力学シンポジウム，(2016).

    * 竹田裕貴，上野和之（岩手大）：直交カットセル法による柱状物体まわりの圧縮性流れの数値解析，日本航空宇宙学会北部支部創立 30 周年記念 2017 年講演会ならびに第 18 回再使用型宇宙推進系シンポジウム，(2017).

    * 上野和之，竹田裕貴，落合里実，中村牧人（岩手大），丹野英幸（JAXA）：カプセル形状模型の空力不安定性数値解析, 日本航空宇宙学会北部支部創立 30 周年記念 2017 年講演会ならびに第 18 回再使用型宇宙推進系シンポジウム，(2017).

  - 社会環境工学専攻

    * 千田昌磨，大内皓平，千葉陽子，高橋明彦，岩崎正二，大西弘志：小型 FWD 試験機を用いた道路橋床板の合理的点検法構築に関する一検討，第 24 回鋼構造年次論文報告集 (2016).

    * 千田昌磨，大内皓平，千葉陽子，高橋明彦，岩崎正二，大西弘志：衝撃振動試験による RC 床板の健全度評価手法の可能性に関する研究，第 9 回床板シンポジウム (2016).

1.2. 修士論文

- **大学院工学研究科**

  - **応用化学・生命工学専攻**

    * 小原　巧弥　：含窒素複素芳香環をコアユニットに用いた星型オリゴチオフェン誘導体の合成および物性

    * カン　ジャスミン：ヘテロールをコアユニットとする縮環型オリゴチオフェン誘導体の合成と物性

    * 小向　和希　：屈曲した分子構造を持つ π 共役拡張型ドナー分子群の合成と有機半導体への応用

    * 佐々木ひかる：金属イオン認識部位を導入した星型 1,3,5-トリアジン誘導体の合成と蛍光センシング特性

  - **機械システム工学専攻**

    * 落合　里実　：飛行物体と非圧縮性三次元流れの数値解析

    * 竹田　裕貴　：直交カットセル法による物体まわりの非粘性圧縮流れの数値解析

  - **社会環境工学専攻**

    * 葛西　智文　：構造系改良のための既設小規模鋼橋の温度変化による実挙動

    * 千田　昌磨　：小型 FWD 試験機を用いた道路橋床板の合理的点検法に関する研究

1.3. 学士論文

- **工学部**

  - **応用化学・生命工学科**

    * 大久保　晃裕：アリール基で機能化したテトラチエニルエチレン誘導体の合成と物性

【規定，規則（付録資料）】

本章では，岩手大学の情報システムおよび情報セキュリティに関わる規則，規定についての参考資料として，「改正前の規則，規定の構成」と，「改正後の規則の構成」，および，情報セキュリティハンドブック各種（基本編，電子メール編，英語縮約版）を掲載します．

正式な規則，規定は，岩手大学内公開のウェブサーバで公開されています．

＜規則，規定の掲載場所：岩手大学内で公開＞

- ✓ 岩手大学 情報基盤センター内 利用案内
  関連規則へのリンク等が掲載されている
  https://isic.iwate-u.ac.jp/usersguide/
- ✓ 岩手大学 情報基盤センター内 セキュリティポータル
  ページ中程に，セキュリティ関連規則・ガイドラインが掲載されている
  https://isic.iwate-u.ac.jp/security/
- ✓ 岩手大学教職員ポータル
  規則・指針・制度を参照して下さい
  https://www.adm.iwate-u.ac.jp/

改正前の情報システム，情報セキュリティ関係の規則，規定（岩手大学）

ポリシー	実施要項	手順･ガイドライン等
国立大学法人岩手大学情報セキュリティ基本方針 国立大学法人岩手大学情報システム運用基本規則	岩手大学情報システム運用･管理要項	情報システムにおける情報セキュリティ実施手順 例外措置実施手順
	岩手大学情報システムリスク管理要項	情報システム運用リスク評価手順
	岩手大学情報システム非常時行動計画に関する要項	インシデント対応手順
	岩手大学情報格付け要項	情報格付け取扱手順 岩手大学における情報の取り扱いについて
	岩手大学情報システム利用要項	PC 利用ガイドライン 電子メール利用ガイドライン ウェブ利用ガイドライン ウェブ公開ガイドライン 利用者パスワードガイドライン パスワード付与または暗号化による情報セキュリティ対策手順 岩手大学ソーシャルメディア利用ガイドライン （付属資料：ソーシャルメディアのトラブル事例）
	岩手大学情報セキュリティ講習実施要項	
	岩手大学情報セキュリティ監査要項	
	国立大学法人岩手大学情報セキュリティインシデント緊急対応チーム設置要項	

図１　改正前の規則，規定の全体像

ポリシー	実施要項	手順・ガイドライン等
国立大学法人岩手大学情報システム運用基本方針 国立大学法人岩手大学情報システム運用基本規則	岩手大学情報システム運用・管理要項	情報システムにおける情報セキュリティ対策手順 例外措置実施手順
	岩手大学情報ネットワーク運用管理要項	IP アドレス管理手順 情報システム運用リスク評価手順
	岩手大学情報システム非常時行動計画に関する要項	インシデント対応手順
	岩手大学情報格付け要項	情報格付け取扱手順 岩手大学における情報の取り扱いについて
	岩手大学情報システム利用要項	岩手大学情報システム利用ガイドライン
	岩手大学情報セキュリティ講習実施要項	
	岩手大学情報セキュリティ監査要項	
	国立大学法人岩手大学情報セキュリティインシデント緊急対応チーム設置要項	

図２　改正された規則，規定の全体像

岩手大学情報基盤センター

情報セキュリティハンドブック

基本編

第一版［教職員編］2016年編纂

― パソコンに保存された情報を守り，情報流出の加害者にならないために ―

目　次

Iwate University Super Computing and Information Sciences Center

情報セキュリティハンドブック 基本編 編纂にあたって

CISO 兼 情報基盤センター長　喜多一美

ここ数年，情報セキュリティの脆弱性を狙った事案（インシデント）が頻発しております。我々大学もインシデントと無縁では無く、情報セキュリティ強化の取り組みに対する社会の要請は強さを増しています。本学においても、より一層の情報セキュリティレベルの向上を図るため、全構成員に対しての情報セキュリティ教育を強化することになりました。

本ハンドブックは、本学の各種規則や要項等を踏まえ、電子化された情報をどのように取り扱うべきかに重点をおいて編集しました。特に今回は、情報保護に関するルールの概略と電子化情報を保護するための方法について、なるべく分かりやすく記載したつもりです。

本ハンドブックに記載されていることは、構成員によって守って頂く最低限の内容であり、本ハンドブックの活用により皆さんのセキュリティレベルが向上し、結果として本学全体のセキュリティレベルも向上することを期待します。

情報セキュリティに関する連絡・相談先
なにかあったら 岩手大学CSIRT（情報基盤センター内）へ！

ウイルスに感染してしまった？怪しいメールに引っかかってしまった？など，日々パソコンを使っている中で不安に思うこともあるでしょう．

情報セキュリティに関する相談は，岩手大学CSIRTへ！

情報セキュリティ上の重大な事態に至らないためにも，焦らずかつ躊躇せずにご相談下さい．

攻撃者の攻撃から岩手大学を守るためにも，皆様のご協力が必要です．

CSIRT（Computer Security Incident Response Team）
ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください
e-mail: csirt@iwate-u.ac.jp

技術的な相談は，情報基盤センターへ

ネットワークがつながらない，新規に情報システムを導入したいなど，情報システムに関する一般的な（技術的な）相談は，情報基盤センターまでお願いいたします．

教育研究系システム担当または業務系システム担当が，皆様の問題解決に努めます．

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp

第１章
岩手大学の情報保護に関するルール（概略）

個人情報を含むパソコン上のファイルを取り扱う場合にどのように取り扱えば良いか？を考える上で，本学の規則・ルールは重要な情報を示してくれます．規則・ルールは，関連する諸機関等が示しているひな形を，本学に適応する形で制定されたものと考えられるためです．

本章では，本学の規則・ルールを俯瞰し，電子化された情報の取り扱いに関連する部分の解説をします．（より詳細な情報が必要な場合は，ガルーンなどで公開されている規則・ルールなどを直接参照ください）

本手引きでは，本学の規則・ルールを守ることと，特に社会からの強い要請がある個人情報を含む電子ファイルの取り扱いについて解説します．本章の内容は，その基礎となります．

備　考

情報の管理規則の詳細については，大枠は諸規則（総務部総務広報課）などで定められています．規則等はガルーンを参照ください．

情報基盤センターは，個人情報等を含む情報のうちパソコンで取り扱うもの（データ，電子メール等）について検討しています．

電子化された情報の取り扱いHOW TO

パスワード付与または暗号化の対象とされる情報

(1) 入試問題等
- 入試問題（学部，大学院）
- 試験の答案（電子化している場合）

(2) 個人情報の含まれるファイル

個人情報および機微な個人情報を含むファイル

【例】
- 学生の推薦状
- 教員任用に関わる教員調書
- 学生の個人調書・ポートフォリオ　学生相談　学生の名簿（氏名入りの場合）
- 成績（氏名入りの場合）
- 研究室の連絡簿
- 高校訪問に用いるデータ（OBOGデータなど）
- アンケート調査票や結果（個人名等が含まれる場合）

方法（対策）

(1) パソコン

誰でも保存された情報にアクセスできる状態を防止するため，すべてのパソコンにおいて，以下を義務化する．

パスワードロック（ログインパスワードの付与．暗号化ではない）

自動ログインの禁止

(2) 電子データを第三者に渡すとき

USBフラッシュメモリ・USB HDDの場合

→　**ファイルの暗号化 または 暗号化対応のUSB機器**とすること

メールで送付する場合

→　**ファイルの暗号化**

(3) メールをアーカイブするとき　（メールソフトでパソコンに保存する場合等）

パソコンがパスワードロックされ自動ログインが禁止されており，かつ，不特定多数がアクセスできない状態にすること．

備　考

ここで示した取り扱いHOW TOに準拠していただくことにより，岩手大学における文書取り扱いに関する規定等を満たすことができます．

規定等の記載を纏めた概念図を次ページに示します．

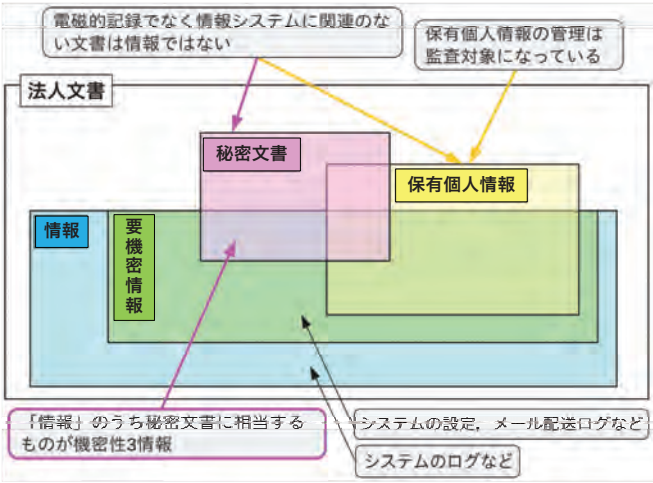


図　岩手大学の各種規定等で定められている文書取り扱いのまとめ(概念図).

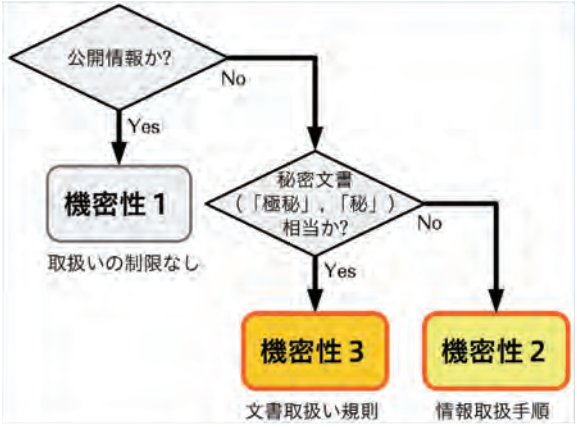


図　岩手大学の各種規定等で定められている文書格付け手順(概念図).

第２章
電子化された情報を保護するための方法

パソコンのセキュリティレベルを維持するために

基礎編
- 日々のパソコンの管理について
- パソコンの自動ログインの禁止（パスワード入力を必須に）
- パスワードの付け方，管理の仕方
- サポートの切れたOS・ソフトウェアの利用禁止

運用編
- オフィスソフトの暗号化機能の利用方法
- 暗号化対応USB機器の利用方法

基礎編
日々のパソコンの管理について

研究・教育・業務で使うパソコンを安全にお使い頂くため，日頃から励行して頂きたい事柄を示します.
- **OS，ソフトウェアは最新の状態を保つ**
- **セキュリティアップデートは欠かさずに実行する**
- **ウイルス対策ソフトウェアを導入し，最新の状態を保つ**
  情報基盤センターでは，岩手大学の教職員が業務に使用するPCを対象としてウィルス対策ソフトウェアを配布しています（学内限定）
  https://isic.iwate-u.ac.jp/usersguide/security/antivirus.html
- **定期的に［業務に使うパソコンやUSBフラッシュメモリ等の完全スキャン］を実施する**
- **不特定多数の者がアクセス出来る状態にしない**
  自動ログインの禁止など，適切な対応をお願いいたします
- **パスワードは適切なものを設定し，適切に運用する**
  パスワードポリシーを満たすパスワードを設定してください
- **サポートの切れたOS・ソフトウェアは利用しない**
  セキュリティ面から，サポート切れのものを使い続けるのは危険です
  特殊なソフトウェアの場合等で特別な事由がある場合は，情報基盤センターまでご相談ください
- **気になる事柄がある場合は，迷わずに相談を！**

CSIRT（Computer Security Incident Response Team）
ウイルス感染や情報漏洩といった情報セキュリティ侵害するトラブルは下記までご報告ください
e-mail: csirt@iwate-u.ac.jp

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp
技術的な問い合わせはこちらまで

■ パソコンの設定についての情報源（情報基盤センター）■

岩手大学情報基盤センターセキュリティポータルからたどれます！
https://isic.iwate-u.ac.jp/security/

他にも情報を掲載しています．皆様のセキュリティ対策にご活用ください.
- 利用禁止となっている主要OS・ソフトウェア一覧（2016年度版）
  https://isic.iwate-u.ac.jp/security/safeguard/ban/
- パソコンの自動ログイン解除方法（パスワード認証の有効化）
  https://isic.iwate-u.ac.jp/security/safeguard/logon/
- セキュリティ対策
  https://isic.iwate-u.ac.jp/usersguide/security/
- ウイルス対策ソフトウェア
  https://isic.iwate-u.ac.jp/usersguide/security/antivirus.html
- ソフトウェアのアップデート方法
  https://isic.iwate-u.ac.jp/usersguide/security/swupdate.html

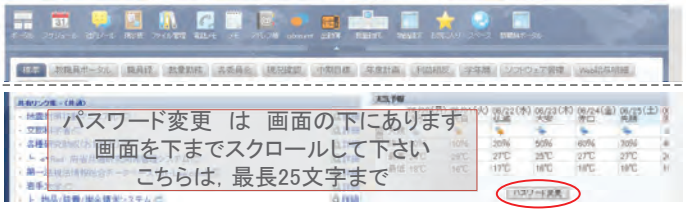
パスワードの種類とルール

■　岩手大学では，２種類のアカウントがある　■
- **事務系（職員番号）と対応するパスワード**
- **教育系（メール等）と対応するパスワード**

それぞれのパスワードは，別のものを設定してください（同じにしない）.

■　パスワードは，以下のルールに則って！　■
- **パスワードの長さ：８文字以上（推奨１５文字以上）**
- **英字，数字，記号の３種類を必ず含む**こと．英文字は大文字小文字があると尚良い　→　英字のみ，数字のみ，記号のみのパスワードは設定しない
- 禁止：ユーザ名，スペースはパスワードに含めない
- 禁止：他のサービスと同じパスワードは使わない（SNS，通販サイトなど）

事務系（職員番号）のパスワード変更：ガルーンから



https://iwjmcg.adm.iwate-u.ac.jp/

教育系（メール等）のパスワード変更：情報基盤センターHPから

https://isic.iwate-u.ac.jp/index.html

サポートが切れたOS・ソフトウェアの利用の禁止

岩手大学の情報セキュリティレベルの向上のため，個々人・組織で利用しているパソコン・サーバ上で稼働しているOSと利用しているソフトウェアについて，サポートが切れたものは利用を自粛してください．

一般ユーザ　クライアントOS

- 利用禁止
  - Microsoft Windows XP 以前
  - Mac OS X 10.6 以前
- 来年度中に利用禁止
  - Microsoft Windows Vista （サポート期限：2017年4月11日）
  - Mac OS X 10.7 および 10.8
  - Mac OS X Server は元となった Mac OS X に準じた扱いとします

サーバOS（Windows Server）

- 利用禁止：Microsoft Windows 2000 Server，Windows Server 2003/R2
- 以下は、NAS などで利用されている可能性があるので注意してください
  - 利用禁止：Microsoft Windows Home Server，Windows Home Server 2011
  - 2016年度中に利用禁止：Microsoft Windows Storage Server 2003/R2
    （サポート期限：2016年10月9日）

Microsoft Office（Windows）

- 利用禁止
  - Microsoft Office 2003 以前
- 2017年度中に利用禁止
  - Microsoft Office 2007 （サポート期限：2017年10月10日）

Microsoft Office（Mac）

- 利用禁止
  - Microsoft Office 2008 for Mac 以前のバージョン
- 2017年度中に利用禁止
  - Microsoft Office for Mac 2011 （サポート期限：2017年10月10日）

一太郎（個人版の場合、法人版とは異なる）

- 利用禁止
  - 一太郎 2013 以前のバージョン
- 2016年度中に利用禁止
  - 一太郎 2014 （サポート期限：2017年2月7日）

Adobe Acrobat（Reader を含む）

- 利用禁止
  - Acrobat X 以前のものすべて（Reader も含む）
  - ※ MS Windows Vista 対応の，サポートされているAcrobat 製品は存在しません．
- 2017年度中に利用禁止
  - Acrobat XI （Reader も含む，サポート期限：2017年10月15日）

ウェブブラウザ，Java および Flash Player

- 原則として，開発元から提供されている最新版を利用する
  （原則）利用禁止：提供元での最新版ではないもの（古いバージョン）

※ ただしJava については，システムに組み込まれている場合や，特定のシステムでバージョンが規定されている場合はアップデートする事が出来ません．この場合，最新版ではないソフトウェアはセキュリティ上の脅威になるので，管理には注意を払うこと．

※ 利用するシステムの制約のため古いブラウザが必要な場合は，複数のブラウザをインストールして利用するなどして，セキュリティ確保に努めてください．

Microsoft SQL Server

- 利用禁止：Microsoft SQL Server 2005 以前

※ 製品に組み込まれている場合があるのでご注意下さい．

※ Microsoft SQL Server 2007のサポート期限は2017年4月11日です．

Exchange Server（Microsoft）

- 運用停止：Microsoft Exchange Server 2003 以前

サーバOS（Linux, BSD等）

- 利用禁止（原則）
  サポートライフサイクル等アップデートの提供が終了したもの
  （除く：自前でパッチをあてるなど適切な管理がなされているもの）

※ 自前でパッチを当てて運用している場合以外で，distributionの標準的なアップデート方法を用いている場合は，当該distributionのサポート終了日以降はネットワークには接続しないこと．

※ 運営しているサービスのリプレース時期の関係などで，若干の期間について稼働しなければならない場合は，稼働の方法・ネットワークへの接続形態などを含めた技術的な検討（fire wall設定の見直し等）が必要になるため情報基盤センターに相談すること．

■ 情報源 ■

利用禁止となっている主要OS・ソフトウェア一覧（2016年度版）
（岩手大学情報基盤センター セキュリティポータル内）
https://isic.iwate-u.ac.jp/security/safeguard/ban/

平成28年度第一回情報化推進委員会資料
「サポートが切れたOS・ソフトウェアの利用の禁止について」（PDFファイル）
https://isic.iwate-u.ac.jp/security/safeguard/ban/bp20160601.pdf

[参考1] 総務省 国民のための情報セキュリティサイト「サポート期間が終了するソフトウェアに注意」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/11.html
[参考2] Microsoft公式 「マイクロソフト サポート ライフサイクル」
https://support.microsoft.com/ja-jp/gp/lifeselect/
[参考3] JPCERTコーディネーションセンター「Mac OS X のセキュリティアップデートの提供期間に注意」
https://www.jpcert.or.jp/tips/2012/wr122901.html/
[参考4] 情報処理推進機構（IPA）「Windows Server 2003 のサポート終了に伴う注意喚起」
https://www.ipa.go.jp/security/announce/win2003_eos.html
[参考5] ジャストシステム公式 「サポート製品一覧 - 統合製品」
http://support.justsystems.com/jp/list/?pjflg=0&spflg=1

OS,ソフトウェアのサポート状況の確認方法

情報基盤センターでは，一次情報に基づいて，OS，ソフトウェアについてのサポート状況の情報提供を行っています．

情報提供・発信　［情報基盤センター］セキュリティポータル　オンラインシグマ

一次情報はOS,ソフトウェアの製造元（開発元）のホームページなども参照してください．

一般ユーザ，サーバ管理者

使っているパソコン・サーバ等の，OSおよびソフトウェア

サポートされている → 問題なし

サポート期限が切れている学内での利用が推奨されないバージョン → 原則，利用禁止

利用し続けなければならない理由がある場合
→　情報基盤センターに届け出る

ネットワークから切り離して運用（スタンドアロンなど*）
更新計画，運用方針をセットで考える

＊　スタンドアロン運用の場合でも，USBメモリでデータを受け渡す場合は，USBへのデータコピー時と，当該機器で処理後のデータを受け入れる際の，ウィルスチェックを行って下さい．セキュリティ確保への自覚りをお願いいたします．

利用を停止できない場合の例

- 特殊なソフトウェアであり，更新できない　（例：計測機器など）
- 特定ハードウェアの制御のため，OSやソフトウェアを変更することが出来ない
- システム更新計画中であり，次期システム稼働までは現行システムを使わざるを得ない
- ソフトウェア部品などを更新するとシステム全体が動かなくなる

例外的な運用を必要とする場合

- スタンドアロン運用（≒ネットワークから切り離しての運用）が可能な場合以外は，セキュリティを高めつつシステムを運用するための方策を，情報基盤センターと協議する．
- 更新計画または終了計画も同時に示してほしい．
  更新計画の例　来年度予算で更新を計画している　等．
  終了計画の例
  ○○事業で利用しているので，○○事業終了と共にシステムも廃止する．
  現在利用中のユーザがいるが，××年度で利用者が０となる．××年度で廃止する．

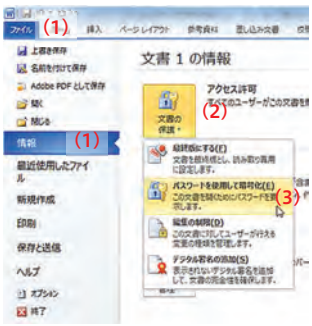
※ サポートが切れているOSやソフトウェアは，セキュリティ上の重大なリスクとなります．皆様のご理解とご協力のほど，よろしくお願いいたします．

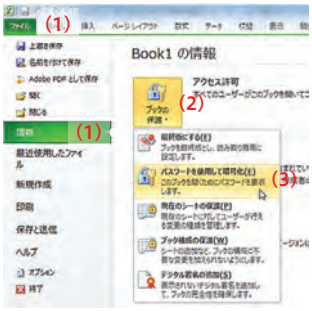
運用編　パスワード付与によるファイルの暗号化

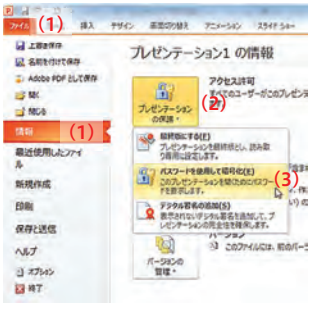
ファイルの暗号化方法 Microsoft Office（Windows版）

Microsoft Office 2007以降では標準機能で暗号化に対応しています．
(1) アプリケーション内の「ファイル」タブから「情報」をクリックする．
(2) それぞれ以下を選択．
　Word：文章の保護
　Excel：ブックの保護
　PowerPoint：プレゼンテーションの保護
(3) メニューから、パスワードを使用して暗号化(E)を選択する．パスワードを入力して暗号化を施す．

※ 画面は Office 2010のものです．
　バージョンにより画面イメージに差異があります．







ファイルの暗号化方法 Microsoft Office（Mac OS X版）

基本的な操作はWindows版のOfficeと同様ですが，Office 2008 for MacではPowerPointにパスワード機能が搭載されていません．

また Office 2011 for Mac では，パスワードの文字数が15字までに制限されています．Windows側で16字以上のパスワードを登録した場合Mac側で開く事ができません．

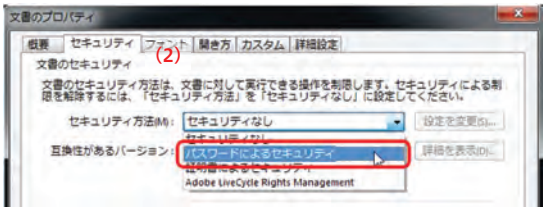
WindowsとMacでファイルのやり取りをする場合は，パスワードを15文字以内にするか，Office 2016 for Mac の利用を推奨します．

まとめ　できるだけ Office 2016 for Mac（以降）を利用すると問題になりにくい．
　　Office 2011 for Macはパスワードの長さ制限がある（15文字まで）。

ファイルの暗号化方法
PDF : Adobe Acrobat (Windows版)

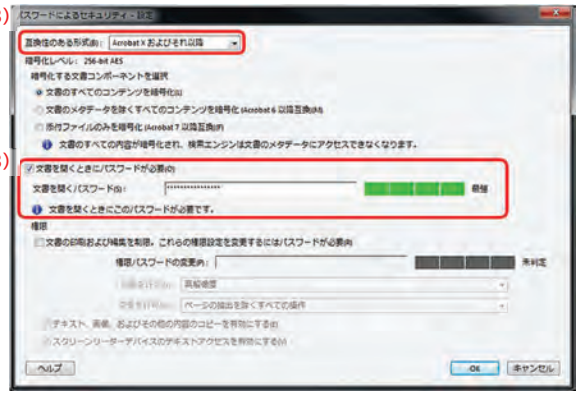
※ Adobe Acrobat Readerでは暗号化できません.
※ Adobe AcrobatのPDF出力機能では暗号化できません.

Adobe Acrobatではファイルのプロパティを以下の手順で変更すると暗号化できます.
(1) ファイルを開き「ファイル」メニューの「プロパティ」をクリックします.
(2) 「セキュリティ」タブの「セキュリティ方法」を「パスワードによるセキュリティ」にします.



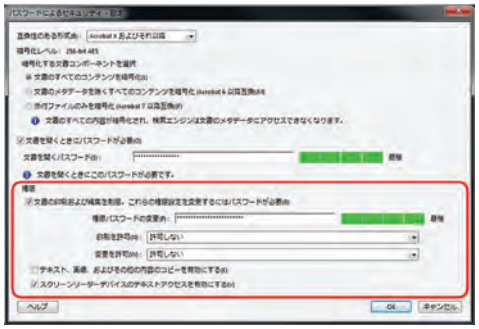
(3) 新しいウィンドウが表示されるので，「互換性のある形式」を「Acrobat 7.0およびそれ以降」とします．また，「文書を開くときにパスワードが必要」にチェックを入れパスワードを入力し「OK」ボタンをクリックします.
※ 「Acrobat Xおよびそれ以降」を推奨します.
(4) プロパティ変更後はファイルを保存してください．次回からファイルを開くとパスワード入力を求められるようになります.

(3)



補 足

「文書の印刷および編集を制限」にチェックを入れると，印刷や編集を無効にすることができます.
※ PDF文書を開く操作を制限するためのパスワードとは別のものにしてください.



ファイルの暗号化方法
PDF : プレビュー.app (Mac OS X版)

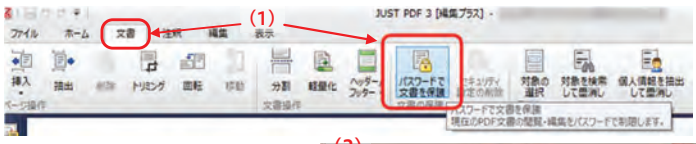
Mac OS X (macOS) では，OS標準のプレビュー.app でPDFファイルを暗号化することが出来ます.

(1) 暗号化したいPDFファイルを開き「ファイル」メニューの「PDFとして書き出す...」をクリックします.
(2) ダイアログが表示されるので「詳細を表示」をクリックします.
(3) 「暗号化」にチェックを入れパスワードを入力したのち「保存」ボタンをクリックします.

次回からファイルを開くとパスワード入力を求められるようになります.

ファイルの暗号化方法
PDF : JUST PDF 編集 (Windows版)

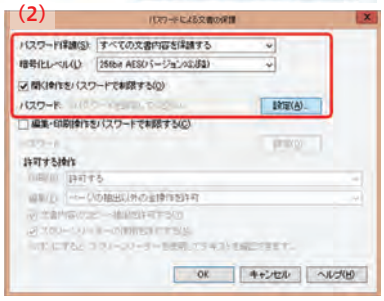
※ Just PDF 3 [編集プラス] を使用した設定方法です．バージョンによって操作が異なる場合があります.
Just PDFでも以下の手順で暗号化できますが，設定後はファイルを保存する必要があります.



(1) ファイルを開き「文書」タブの「パスワードで文書を保護」をクリック.
(2) 新しいウィンドウが表示される.
「パスワード保護」
→「すべての文書内 容を保護する」
「暗号化レベル」
→「128bit AES(バージョン7以降)」
※ 推奨は「256bit AES(バージョンX以降)」
「開く操作をパスワードで制限する」にチェックを入れ，「設定」をクリック.
(3) パスワード設定用のウィンドウが表示される.
パスワードを入力し「OK」をクリック.

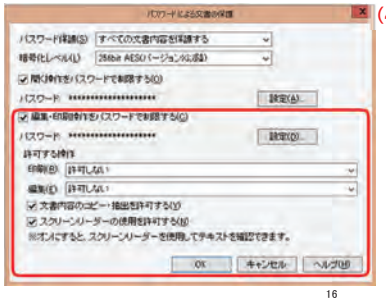
パスワード登録後はファイルを保存してください．次回からファイルを開くとパスワード入力を求められるようになります.

(2)



(3)

(4)



補 足

(4)「編集・印刷操作をパスワードで制限する」にチェックを入れると，編集や印刷を無効にすることができます.

※ PDF文書を開く操作を制限するためのパスワードとは別のものにしてください.

暗号化対応USB機器について（利用のススメ）

USBで接続しただけでは情報が見えない.
パスワードを入力して初めて，暗号化された情報にアクセス出来る.
パスワードが間違っているとアクセス出来ない.

■ 暗号化対応USBフラッシュメモリ，暗号化対応USB HDD ■

- 情報は自動的に暗号化されます.
- 内容を見るためには，パスワードが必要です.
- パスワードを知らない者は，暗号化された情報を見ることが出来ません.

- **当該USB機器を紛失した場合でも，情報が暗号化されていれば，暗号を解除するパスワードを知らない者は情報を見ることが出来ない**
- 情報が保護される ≒ 我が身を守ることに繋がります.
  （不正アクセス行為の禁止等に関する法律の要件を満たしうる）

※ パスワードを忘れた場合・機器が故障した場合，情報を取り出せなくなります．情報のバックアップを必ずとるようにしてください.
※ バックアップメディアは，施錠された引き出しの中等で保管して下さい.

■　暗号化対応USB機器を使う際の注意　■

- 使用しているPCで問題なく利用できるか確認してから利用しましょう．
  とくに，WindowsとMacでデータのやりとりをする際は，どちらにも対応しているか，予めテストしてから利用しましょう．
- パスワードを忘れると内容を閲覧出来なくなります．パスワードの管理には十分注意しましょう．
- 個人情報を含む情報を持ち出す際，暗号化して保護されていることは大変重要です．自らを守るだけではなく，本学も守ることに繋がります．
- バックアップは忘れずに．電子機器はいつか壊れます．
  定期的なバックアップの習慣を！
  ※ 施錠される引き出し中など，バックアップメディアの管理にも注意してください．

■　補足　■

いくつかの暗号化対応のUSB機器については，情報基盤センターで試用のため貸し出すことが可能です．利用している機器との相性（OSやチップセット，ドライバとの相性により利用できない場合があります）を確認してから購入する際の参考として下さい．昨年度発行した，情報基盤センター報告Σでも，暗号化対応USB機器について掲載しています．

暗号化対応のUSB機器は，岩手大学生協ほかで購入することができます．

［参考］

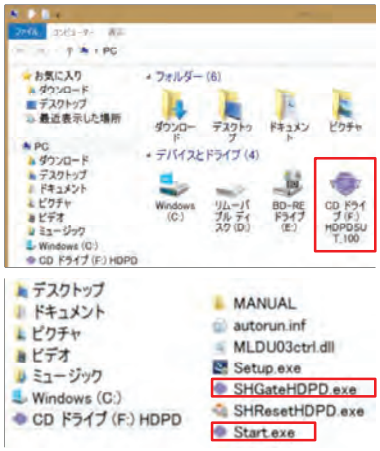
USB記憶媒体の暗号化について（情報基盤センターセキュリティポータル内）
https://isic.iwate-u.ac.jp/security/safeguard/usb/
情報基盤センター報告Σ　1号(平成24～27年度) 2016年3月発行
https://isic.iwate-u.ac.jp/center/issue.html

IODATA HDPD-SUT-1.0K

暗号化対応USB機器の一例としてとりあげました．
次ページに図を示します（Windows）．

ハードウェア暗号化+パスワードロック対応の，耐衝撃ポータブルハードディスクです．

- 対応OS：　Windows または Mac (Windows Server等含む)
  対応OSはメーカーサイトを参照下さい．
- 分類：　ハードウェア暗号化（AES 256bit）
- 認証：　パスワード．管理ソフトのインストールは不要．
- Interface : USB 3.0／2.0（MicroBコネクター）．USBから給電
- 初期状態：NTFSでフォーマット（Macで利用する際はフォーマットする必要あり）
- 特徴：　購入時はWindowsで使用できるように設定されています．
  また，ディスクのファイルシステムをexFAT形式で初期化すると，
  WindowsとMac間でデータ共有も可能です（両方で利用できる）．
- 補足：　Macでディスクファイルシステムを初期化する場合は付属のマニュアルを参照．



注意　画面はWindows 8.1のものです．

図　接続後の様子．
認証前は仮想CDドライブが認識される（上）．
CDドライブには，認証用アプリケーションが格納されている（下）．

図　初期設定画面．
初回利用時には，認証用のパスワードを設定する．パスワードを忘れるとアクセス出来なくなるので注意してほしい．

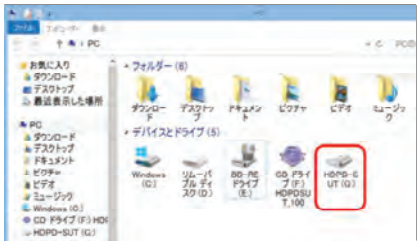


図　認証の様子．
仮想CD内のStart.exeを起動すると，パスワード入力を求められる（左上）．
認証に成功した様子（左下）．
認証に成功すると，暗号化されたハードディスク領域がOSに認識される（右）．

＜参考＞ OSの設定をセキュリティ・プライバシーの面から見直す

一般的なPCに搭載されているOSの標準設定は，ユーザの使いやすさを優先した設定になっています．OSの設定を見直すことにより，より安全な状態で利用することが可能になります．

セキュリティと利便性はトレードオフの関係にありますので，メリットとデメリットをご理解の上，ご利用下さい．

※　PC一般の利用と同様に，設定の適用は利用者ご自身の責任で実施して下さい．

■ 情報源（情報基盤センター内）■

- 岩手大学情報基盤センター セキュリティポータル内
  https://isic.iwate-u.ac.jp/security/
- ファイル拡張子の表示方法　　※ ウイルス対策の面からも推奨します．
  https://isic.iwate-u.ac.jp/security/safeguard/file_ext.html
- セキュリティとプライバシー設定（Windows 10対象）
  便利な機能を実現するためには，源となる情報を（Microsoft等）事業者にネットワークで送信しています．
  本センターでは，Windows 10について，望ましい設定例を調査し，セキュリティポータルに掲載しています．
  https://isic.iwate-u.ac.jp/security/safeguard/setup/win10.html

■ 外部リンク（リンクは手引き作成時に確認しています）■

- Windows 10のプライバシー設定をひもとく（リンク先：ITPro）
  http://www.atmarkit.co.jp/ait/articles/1509/10/news040.html
- Windows 8におけるGPSセンサーと動作の確認（リンク先：ASCII.jp）
  http://ascii.jp/elem/000/000/865/865751/
- 内蔵カメラの無効化　～不用意な撮影を防ぐために～
  意図しないときにカメラが動作する事を防ぐため，カメラを無効化してしまうという方法もあります．利用状況を踏まえた上で検討して下さい．
  設定方法はPC毎に異なります．
  参考１（Let's Note）　http://faq.askpc.panasonic.co.jp/faq/docs/003978
  参考２（Levono）　https://support.lenovo.com/jp/ja/documents/ht074191
- ブラウザのセキュリティ設定　（リンク先：トレンドマイクロ）
  ブラウザのセキュリティ設定についての概説です．
  http://www.is702.jp/column/1138/
- [Mozilla Firefox] プライバシーとセキュリティの設定　（リンク先：Mozilla）
  https://support.mozilla.org/ja/products/firefox/privacy-and-security
- Windows 8.1ミニTips 64　（リンク先：マイナビニュース）
  Internet ExplorerのInPrivateブラウズとホームページ設定を活用する
  ブラウザの設定をセキュアにする方法の一例となります．
  セキュアな設定にすると不便になる面もあるため，セキュリティと利便性のバランスの判断は，利用する方にゆだねられています．
  http://news.mynavi.jp/column/win81tips/064/

付　録
情報セキュリティ関連の規則へのリンク集

- 岩手大学 情報基盤センター内 利用案内
  関連規則へのリンク等が掲載されている
  https://isic.iwate-u.ac.jp/usersguide/
- 岩手大学 情報基盤センター内 セキュリティポータル
  ページ中程に，セキュリティ関連規則・ガイドラインが掲載されている
  https://isic.iwate-u.ac.jp/security/
- 岩手大学教職員ポータル
  規則・指針・制度を参照して下さい
  https://www.adm.iwate-u.ac.jp/

セキュリティ事案はCSIRTへ連絡！

CSIRT（Computer Security Incident Response Team）

ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください

e-mail: csirt@iwate-u.ac.jp

TEL: 019-621-6096 （情報基盤センター）

セキュリティ的に気になることがあった場合には，躊躇せずご連絡下さい．早期対応が大学のセキュリティを守ります！
早期対応には，皆様の”気づき”が重要です．

技術的な問い合わせは情報基盤センターへ

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp

情報セキュリティハンドブック 基本編
第一版［教職員編］ 2016年編纂
－ パソコンに保存された情報を守り，情報流出の加害者にならないために －
平成28年10月発行

発 行 者 岩手大学情報基盤センター
Iwate University Super Computing and Information Sciences Center
連 絡 先 (020-8550) 岩手県盛岡市上田3丁目18－8 岩手大学情報基盤センター
印 刷 杜陵高速印刷株式会社

岩手大学情報基盤センター

情報セキュリティハンドブック
電子メール編

第一版［教職員編］ 2016年度

― 電子メールを安心・安全に使うために知っておきたいこと ―

目 次

Iwate University Super Computing and Information Sciences Center

情報セキュリティハンドブック 電子メール編 編纂にあたって

CISO 兼 情報基盤センター長　喜多一美

現在、私達の生活や仕事にとって、電子メールは必要不可欠なコミュニケーションツールになっています。電子メールの送付元は玉石混合の状態にあり、生活や仕事にとって重要なメールもあれば、商品のコマーシャルのようなスパムメールもあります。ここで、我々が注意しなければならないメールは、私達あるいは社会への攻撃を指向した標的型メールです。最近の標的型メールは非常に巧妙になり、情報基盤センターで用意した対策機器・システムを巧みに掻い潜り利用者に届きます。標的型メールの罠にかかると、知らない間に自分のパソコンが外部攻撃の踏み台になっていたり、個人情報や機密情報が抜き取られたりします。場合によってはランサムウェアによってパソコンが人質となって身代金を要求されたりします。

本ハンドブックは、電子メールを安全に利用するための手引きです。本ハンドブックに記載されていることは、構成員によって守って頂く最低限の内容であり、本ハンドブックの活用により皆さんのセキュリティレベルが向上することを期待します。

情報セキュリティに関する連絡・相談先
なにかあったら 岩手大学CSIRT（情報基盤センター内）へ！

ウイルスに感染してしまった？怪しいメールに引っかかってしまった？など，日々パソコンを使っている中で不安に思うこともあるでしょう．

情報セキュリティに関する相談は，岩手大学CSIRTへ！

情報セキュリティ上の重大な事態に至らないためにも，焦らずかつ躊躇せずにご相談下さい．

攻撃者の攻撃から岩手大学を守るためにも，皆様のご協力が必要です．

CSIRT（Computer Security Incident Response Team）
ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください
e-mail: csirt@iwate-u.ac.jp

技術的な相談は，情報基盤センターへ

ネットワークがつながらない，新規に情報システムを導入したいなど，情報システムに関する一般的な（技術的な）相談は，情報基盤センターまでお願いいたします．

教育研究系システム担当または業務系システム担当が，皆様の問題解決に努めます．

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp

第1章
電子メールを安全に，安心して利用するために

電子メールは，コミュニケーションツールとして日常的に利用されています．電子メールの利用では，仕事と関係の無いメール（SPAMメール等）も問題ですが，攻撃目的のメールも多数送られてきています．

危険な電子メールの被害に遭わないため，はじめに，電子メールと攻撃の状況について記します．これを踏まえて，どのように電子メールを利用すべきか？を示します．

- 電子メール受信時の注意
- 悪意のあるメールの見分け方・対応の仕方
- 標的型攻撃について（盗聴，対応，情報源）
- 情報基盤センターからの悪意のあるメール等に関する情報提供

電子メール受信時の注意

－ウイルスや情報の盗難に警戒を！－

電子メールからウイルスに感染させるのは古典的方法ですが，効果があるからこそ今も多く用いられています．ばらまき型や標的型攻撃でも，未発見の脆弱性を突くように細工された添付ファイルを用いるなどして悪用されます．

愉快犯的なものだけではなく，金銭目的や情報そのものに価値を見いだす集団が，業として攻撃をしているとの観測もあります．我々の保有する個人情報や研究に関する情報も，ある種の集団からは欲しい情報と見なされている可能性は否定できません．

情報セキュリティにおいて，皆様の情報資産および安全を守り，ひいては本学の安全を守るためにも，皆様のご理解・ご協力をお願いいたします．

■ 基本的な対策 ■　全員が必ず守るべき項目です．

OS，ソフトウェアは，サポート期限内のものを使うことと，セキュリティアップデートを行って最新の状態を保って下さい．

ウイルス対策ソフトウェアを必ず導入し，セキュリティアップデートを行って最新の状態を保って下さい．

もしも侵入されてしまった場合やメール誤送信時の被害を軽減するために，機微な個人情報はパスワード付与により暗号化して送付することを心がけましょう．

1．OS，ソフトウェアは定期的にアップデートし最新の状態を保つ　→ 基本編 を参照
2．アンチウイルスソフトを導入し，最新の状態を保つ
3．電子メールソフトの設定を見直す　→ 第２章
4．機微な個人情報を取り扱う場合は，送付するファイルをパスワード付与により暗号化する　→ 第３章
5．疑問がある場合は即CSIRTに相談！

104

■ 電子メール受信時の基本的な対応 ■　必ず守って下さい

インターネットが実社会と同じく玉石混淆であるのと同様に，電子メールも（割合に差異はあれど）玉石混淆な状態にあります．
我々が問題とするのは諺でいえば "石" に対応する部分で，特に，悪意を持つ者やそれに利用されてしまっている者・物*となります．

＊サーバやPC等の管理状態が悪く悪意のある者に踏み台（隠れ蓑）に利用されてしまった場合等を想定．

このような状態ですから，我々に届く**電子メールは，［玉も石も混淆］**しています．

いろいろなものが届く電子メールを安全に取り扱うための原則を示します．

1．覚えの無いメールや怪しいメールは破棄する／閲覧しない
　　判断に迷った場合：送信者情報・ヘッダ情報を確認！
2．電子メールに対応したアンチウィルスソフトを導入する
3．添付ファイルを開く際は十分注意する
　　判断に迷った場合：送信者情報・ヘッダ情報を確認！
4．電子メールソフトは，HTMLメールを表示しない設定にする
5．リンクをクリックする際は，最低限リンク先を確認する
6．疑問がある場合は即CSIRTに相談！

■ ＜参考＞なぜ基本的な対応が必要なのか？ ■

1.は，利用者を誘導して攻撃を仕掛けようとする場合や，OS等のセキュリティホール（脆弱性）等を突くメールを防ぐための対策となります．
2.は，電子メール受信時に，アンチウイルスソフトで検疫し，既知の脅威を取り除きます．セキュリティ的な防御を固める対策となります．
3.は，攻撃を指向した添付ファイルから身を守るための対策です．攻撃者は利用者の誤認を誘うこと等により，ウイルス攻撃をしかけようとします．
4.は，HTMLメール特有の攻撃への対策です．HTMLメールでの文章の修飾機能の悪用およびHTML処理の脆弱性を狙った攻撃への対応となります．
5.は，リンク先の詐称や利用者の誤謬を誘うことを狙った攻撃を防ぐ対策です．
6.は，悪意のある攻撃者の攻撃は防ぎ得ない（例：内部情報を収集した上で，当該の者が開かざるを得ない攻撃メールを送ってくる）ので，おかしいな？と思った場合は，些細なことでもCSIRTに相談して下さい．
皆様方**の気づき・心がけが，本学を脅威から守ります！**

＜参考＞
悪意のあるメールの見分け方と対応方法

■ 危険な（怪しい）メールを受け取ったら... ■

知らない相手からのメールの場合は，以下を確認して下さい．

- 宛先（別名だけではなくメールアドレスを確認）
  　他人になりすましたメールが届くこともあります*
- 文面が不審ではないか？メールの内容は適当か？
- 日本語がおかしくないか？
  　特に母語が日本語以外の方は注意が必要！
  　母語に翻訳して正しくとも，日本語では不適の場合があるので十分注意して下さい．

知り合いからのメールであっても，なりすまし等の可能性があるため注意が必要です．
大学名を騙って，ID＋パスワードを窃取しようとするメール等がたびたび確認されています．
　対処：大学ウェブページなどほかの情報源で情報の裏付けをとる！

また，世間を騒がせている標的型の攻撃≒業務に関係あるメールに見せかけたメール（標的型攻撃）により被害に遭った大学もあります．
　例：省庁からのメールに偽装したもの
　　事務部や業者からのメールに偽装したもの 等 が確認されています．

＊メールの仕組み上，なりすましが可能です．ただし，ヘッダまで観察すれば見破ることは可能です．

■ 危険な（怪しい）メールを受け取ったら... ■

- 危険な（怪しい）メールには対応しない
  　返信すると，貴方のメールアドレス等の情報が相手に筒抜けになってしまいます．
- 添付ファイルを実行しない・開かない（閲覧しない）・保存しない
  　実行するとウイルスに感染する可能性があります．
- メールのURLをクリックしない
  　攻撃用のサイトに誘導され，情報窃取の被害に遭う可能性があります．
  　未知の脆弱性を悪用したサイトの場合，ウェブページを閲覧しただけでウイルス感染する場合があります．

■　お気づきの点があれば，即CSIRTへ連絡！　■

添付ファイルを開いてしまった，情報を入力してしまった等の場合，即CSIRTへ連絡下さい．
皆様の気づきが，本学のセキュリティレベルの維持のために最も重要です．

CSIRT（Computer Security Incident Response Team）
ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください
e-mail：csirt@iwate-u.ac.jp

■ 危険な（怪しい）メールの例... ■

下のいずれかに該当する場合，悪意のあるメールの可能性を疑って下さい．
判断に迷った場合は，CSIRTまでご相談下さい．

- "お金を振り込みます" メール
- "寄付してほしい" メール
- "添付ファイルを読め" と要求するメール
- "IDとパスワードを入力" させようとするメール
  　銀行，郵便局，宅配業者，通販事業者を騙る場合が多い
  　本学で提供しているサービス（Active! mail）を騙り，ID+パスワード情報を摂取しようとする攻撃も散見されます
- "個人情報を入力" させようとするメール
- "差出人名・題名・本文などが無記入" のメール
- "差出人に心当たりのない，添付ファイル付き" メール
- "送付先間違いを装った" メール
- "債権回収の最後通告" メール　等々　　*** これらは一例です ***

■ 標的型攻撃に注意！ ■

特定の組織・個人を狙って行われる攻撃が「標的型攻撃」です．電子メールでも行われることから，どなたでも標的となる可能性があります．
標的型攻撃では，ターゲットとする組織・職務内容などを踏まえた内容のメールが送付されます．この場合当該メールは職務上「開かざるを得ない」ものとなります．
本学においても，本学が提供しているActive! mailと本学名を騙った（偽装した）メールが送付された事例等が観測されています．
恐ろしいことに，周到に仕組まれた標的型攻撃のメールは判別は殆ど不可能との指摘もあります（各セキュリティベンダ等）．
繰り返しとなりますが，電子メールに関連して疑問に思われること・お気づきの点がございましたら，即CSIRTまでご連絡下さい．
重大な事態に発展することを防ぐには，皆様の気づきと刻をおかずのご相談にかかっています．

■ 情報源 ■

- よくある相談と回答(FAQ)：メール関係（IPA 情報処理推進機構）
  　https://www.ipa.go.jp/security/anshin/faq/faq-mail.html
- 標的型サイバー攻撃対策 (IPA. 情報処理推進機構)
  　https://www.ipa.go.jp/security/ta/
- 迷惑メールに関する情報提供とご相談　(財団法人 日本データ通信協会　迷惑メール相談センター)
  　http://www.dekyo.or.jp/soudan/ihan/
- 迷惑メールに関する情報提供 (財団法人 日本産業協会　電子商取引モニタリングセンター)
  　http://www.nissankyo.or.jp/e-commerce/
- NISCサイバーセキュリティ意識啓発動画ポータル (内閣サイバーセキュリティセンター)
  　https://www.youtube.com/user/NISCchannel
- 岩手大学　情報基盤センター　https://isic.iwate-u.ac.jp/
- 同　情報セキュリティポータル　https://isic.iwate-u.ac.jp/security/

情報基盤センターからの
悪意のあるメール等に関する情報提供

■ 敵を知ることの必要性 ■

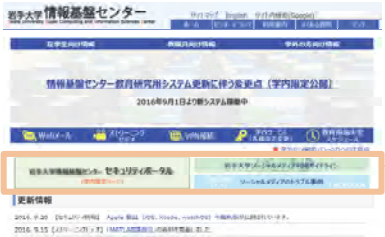
電子メールを用いた攻撃は日々，手を変え品を変えて行われています．攻撃は，直接的なウイルスだけではなく，特定の標的に対して効果を発揮するよう細工のされたものなど様々です．
電子メールを利用する際には，迷惑メール等の流行をいち早く察知し，危ういものには近づかない態度が肝要です．

■ 情報基盤センターの情報提供 ■

現在，どのような"攻撃"が行われているのか，どのような悪意のあるメールが流行っているのか，など，現在の状況を知る手がかりの一つとして，情報基盤センターでは，以下の方法で学内に向けて情報発信を行っています．

- オンラインシグマを通じた情報提供
- 情報基盤センターウェブページを通じた情報提供
  　情報基盤センタートップページ および 情報セキュリティポータル

本センターの情報も参照しつつ，安全に電子メールを利用して頂ければと考えております．



情報基盤センター
https://isic.iwate-u.ac.jp/

セキュリティ設定などを纏めたページ，セキュリティポータルへのリンクなどがあります

中略

重要なお知らせを掲載します．セキュリティ的に注意を要する事項なども掲載します．

セキュリティアップデートなどの情報を掲載しています．

岩手大学情報基盤センター　セキュリティポータル
https://isic.iwate-u.ac.jp/security/

← 脆弱性情報等を掲載しています

← 行って頂きたいセキュリティ設定（推奨の設定）が掲載してあります
（情報化推進委員会を経て掲載しているものも多くあります）

← 岩手大学のセキュリティ関連規則・ガイドラインを掲載しています

← 情報基盤センターが実施したセキュリティ関連の講習会の動画や資料を掲載しています

← セキュリティ的な緊急時の連絡先を記載しています
緊急時はCSIRTまで連絡を！

第２章
電子メールソフトウェアのお薦め設定

メール受信について

お薦め設定１　テキスト形式でメールを表示
２　自動で画像などを表示しない
３　送信者情報を表示する
４　自動で添付ファイルを開かない

メール作成・送信について

必須の設定　　テキスト形式でメールを作成
（HTML形式でのメール送信は規則で禁止されています）

もう一工夫 ～送信する情報を守る～

1　宛先をよく確認する　　（メールアドレス）
2　送付する情報を暗号化する（パスワード保護）
3　送付する内容に気をつける（情報の重要度）
業務に関連する情報や，機微な個人情報を含む場合は特に注意してください．

Thunderbird 45.1.1 編 (Windows, Mac)

受信メールの表示形式

Mac版は，メニューの「オプション」が「設定」となる以外は同等です．

HTMLメールを受信すると，標準設定ではHTML形式で表示されます．ただし，外部コンテンツの場合，標準でブロックされます（表示されない）．
この状態のままでは，悪意のあるHTMLメールによる攻撃等に対し無防備なため，HTML形式のメールを受信した際にもテキスト形式で表示するよう，設定を変更してください．

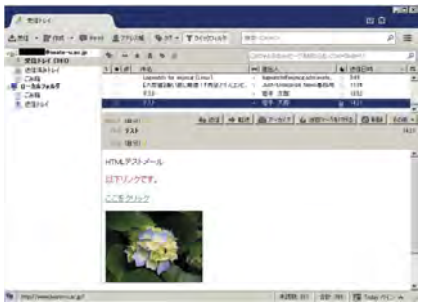


図　HTMLメール受信時の様子．標準設定ではHTML表示されます．
（この例では，画像も表示されています）

[テキスト形式で表示するための設定の変更]
メニューボタン→「表示」→「メッセージの表示形式」→「プレーンテキスト」を選択してください．

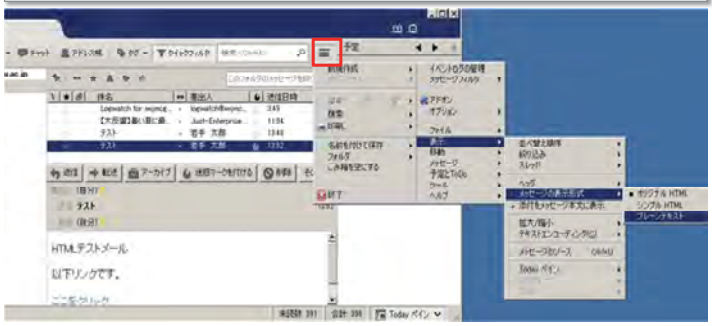


図　HTMLメールの表示形式の設定方法．
メニューボタン→「表示」→「メッセージの表示形式」→「プレーンテキスト」を選択．

添付ファイルの表示

画像が添付されたファイルの場合，自動的に画像が表示されます．
添付ファイル（画像、テキスト）をプレビューしない設定を行ってください．
メニューボタン→「表示」→「添付をメッセージ本文に表示」のチェックをはずす

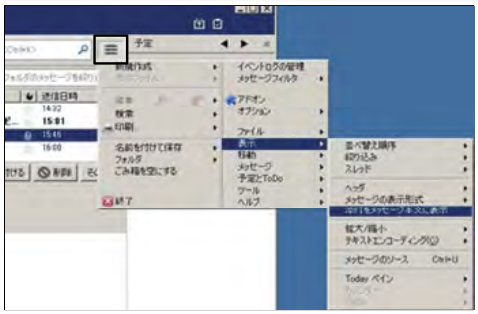


図　添付ファイルのプレビュー機能も無効化．
添付ファイルを本文に表示のチェックを外す．

差出人情報の表示

Mac版は，メニューの「オプション」が「設定」となります（読み替え）．

迷惑メール・攻撃メールを見分けるためには，メールの差出人情報をよく確かめる必要があります．
メールアドレスが表示されない場合は，差出人の隣の領域（例では 岩手太郎）にマウスカーソルを合わせることで表示されます（マウスオンでメールアドレス表示）．
ヘッダにメールアドレスを常に表示させるため，設定を変更してください．
(1) メニューボタン→「オプション」→「オプション」
(2) 「表示」→「詳細」タブ→「アドレス帳に…表示しない」のチェックをはずして，「OK」

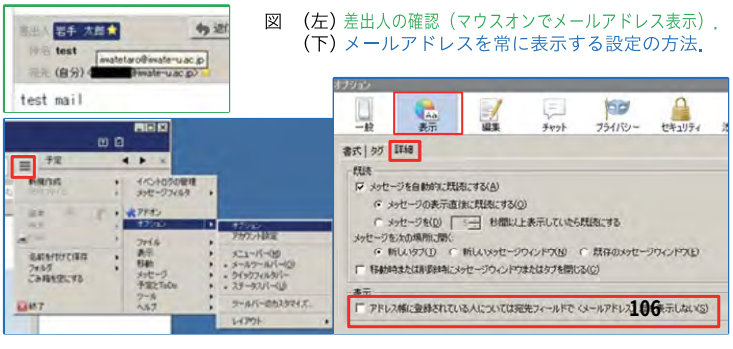
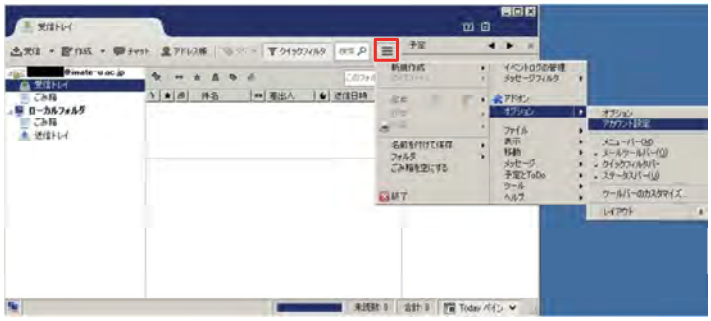


図　(左) 差出人の確認（マウスオンでメールアドレス表示）．
(下) メールアドレスを常に表示する設定の方法．

メール作成の標準設定

Mac版は，メニューの「オプション」が「設定」となります（読み替え）．

標準はHTML形式です．
メール作成時の標準形式をHTML形式ではなくテキスト形式とするため，以下の設定を行ってください．
(1) メニューボタン→「オプション」→「アカウント設定」を選択
(2)「編集とアドレス入力」→「HTML形式でメッセージを編集する」のチェックをはずし，「OK」ボタンを押す



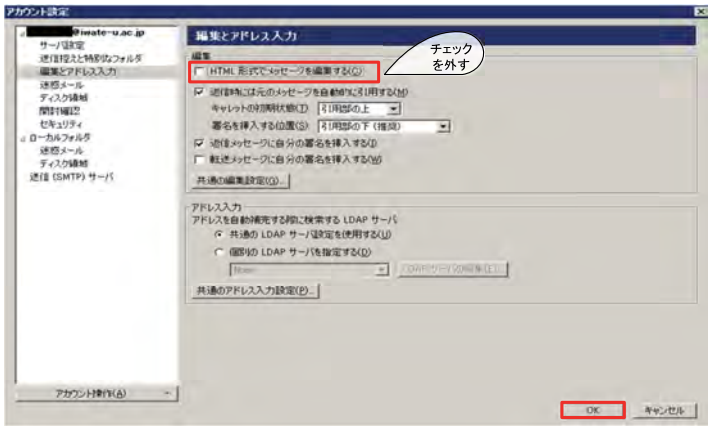
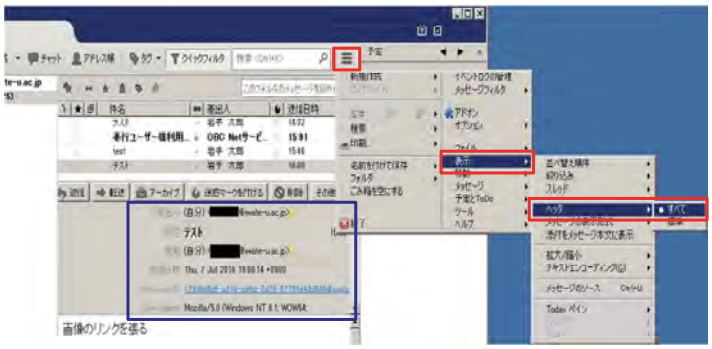


図　メール作成形式をテキスト形式にする方法．

メールヘッダの確認方法

怪しいメールだな，という時には，メールヘッダを確認してください．
Thunderbirdでメールヘッダ全体を表示するには，メールの一覧で該当のメールが選択された状態で，メニュー ボタン→「表示」→「ヘッダ」→「すべて」を選択してください．下図上：詳細なヘッダを表示，下図下：標準状態 となっています．



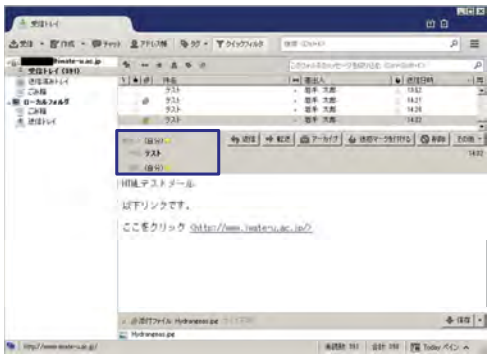


図　メールヘッダの詳細表示．
詳細な表示（上）では，メールヘッダ情報が詳細に表示されている．
標準状態（下）では，最小限の情報が表示されている．

Outlook 2016 編（Windows）

受信メールの表示形式

HTMLメールを受信すると，標準設定ではHTML形式で表示されます．ただし，外部コンテンツの場合，標準でブロックされます（表示されない）．
この状態のままでは，悪意のあるHTMLメールによる攻撃等に対し無防備なため，HTML形式のメールを受信した際にもテキスト形式で表示するよう，設定を変更してください．

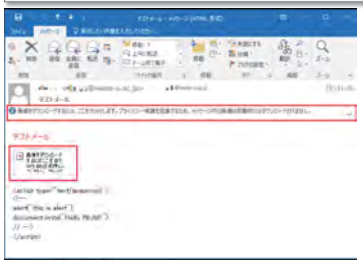


図　HTMLメール受信時の様子．標準設定ではHTML表示されます．
（この例では，画像は表示されていません）

［テキスト形式で表示するための設定の変更］
「ファイル」タブをクリックし，「オプション」をクリックします．Outlookのオプションが表示されたら，「セキュリティセンター」を選択し，「セキュリティセンターの設定」をクリックします．
「セキュリティセンター」が表示されたら，「電子メールのセキュリティ」をクリックし，「テキスト形式で表示」欄の以下の項目にチェックを入れます．

- すべての標準メールをテキスト形式で表示する
- すべてのデジタル署名されたメールをテキスト形式で表示する

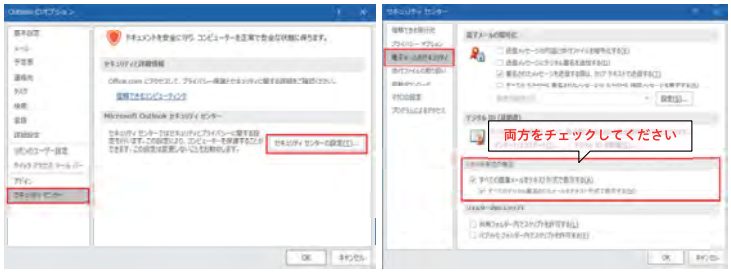


図　受信したHTMLメールのテキスト表示への変更方法．
Outlookのオプションからセキュリティセンターの設定を選択し（左），セキュリティセンター（右）で設定する．

添付ファイルの表示

メール全体のプレビュー部分において，添付ファイルは自動でプレビューされません．添付ファイルを右クリックして「プレビュー」をクリックするとプレビュー表示されます．プレビューする場合は，注意して行ってください．
なお，プレビュー機能を完全に無効化するには，複数箇所の設定が必要です．詳細は情報基盤センターのセキュリティポータルを参照してください．

差出人情報の表示

迷惑メール・攻撃メールを見分けるためには，メールの差出人情報をよく確かめる必要があります．
Outlookは，メールの一覧（プレビューのオン／オフいずれの場合も）において，デフォルトで差出人名のみを表示し，メールアドレスは表示しません．メールを選択して表示した際（プレビューウィンドウも含む）は，デフォルトで差出人名とメールアドレスの両方を表示します（標準設定）．

メールヘッダの確認方法

怪しいメールだな，という時には，メールヘッダを確認してください．．
Outlookでメールヘッダ全体を表示するには，メールの一覧から該当のメールをダブルクリック等で個別ウィンドウを表示し，「ファイル」→「プロパティ」を選択します．プロパティの「インターネットヘッダー」の欄でメールヘッダ全体を確認できます．

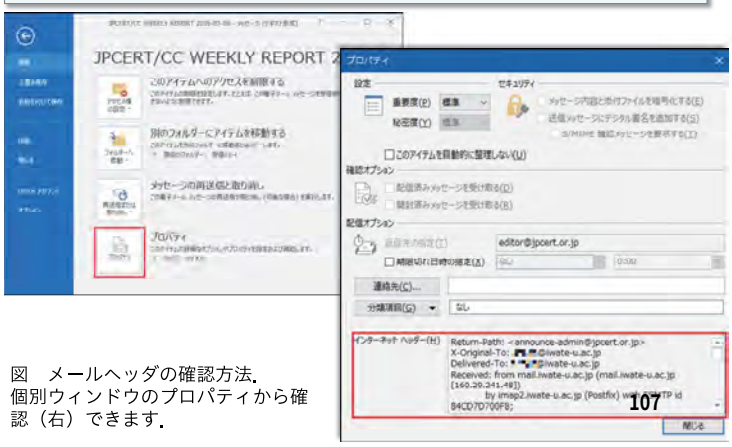


図　メールヘッダの確認方法．
個別ウィンドウのプロパティから確認（右）できます．

メール作成の標準設定

メール作成の標準設定はHTML形式です．フォントサイズや文字色などの装飾アイコンがアクティブな状態です．メール作成ウィンドウのタイトルバーに「メッセージ（HTML形式）」と表示されています．

図　作成されるメールの形式の確認方法．タイトル部分に注目．

メール作成時の標準形式をHTML形式ではなくテキスト形式とするため，以下の設定を行ってください．
(1) Outlookの「ファイル」をクリックし，「オプション」を選択します．
(2) 「メール」をクリックする．
(3) 「メッセージの作成」の項にある「次の形式でメッセージを作成する」のプルダウンをクリックし，「テキスト形式」選択し「OK」．

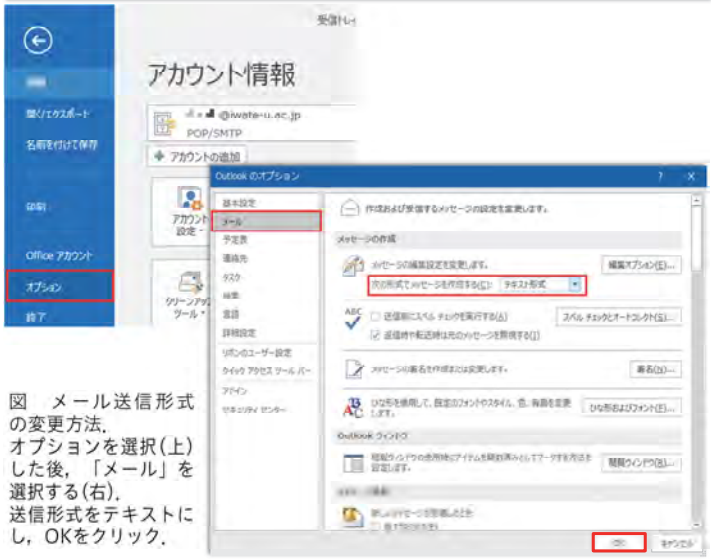


図　メール送信形式の変更方法．
オプションを選択(上)した後，「メール」を選択する(右)．
送信形式をテキストにし，OKをクリック．

Windows Live Mail 2012 編 (Windows)

Windows Live Mail 2012は，Windows Essentials 2012に含まれる「メール」であり，Windows 8.1以降でストアからダウンロード可能なアプリの「メール」とは異なります．

受信メールの表示形式

Windows Essentials 2012 のサポートは2017年1月10日に終了します．他のソフトへの乗り換えを推奨します！

受信メールの表示形式の標準設定はHTML形式です．リンク部分にオンマウスすると、下部のステータスバーにURLが表示されます．オンマウスによる外部リンクの先読みやポップアップはされません．
この状態のままでは，悪意のあるHTMLメールによる攻撃等に対し無防備なため，HTML形式のメールを受信した際にもテキスト形式で表示するよう，設定を変更してください．

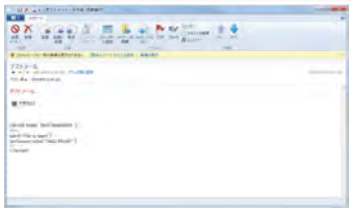


図　HTMLメール受信時の様子．標準設定ではHTML表示されます．
（この例では，画像は表示されていません）

[テキスト形式で表示するための設定の変更]
左上の▼マークをクリックし，「オプション」→「メール」を選択します．メールのオプション設定が表示されたら，「読み取り」タブを選択します．
ここで，「メッセージはすべてテキスト形式で読み取る」をチェックします．

注 意
この設定でHTMLメールを受信すると，メール本文はテキストのみになり，HTMLファイルが添付された状態になります．メール本文の文字列にハイパーリンクが設定されていた場合リンク部分は本文に表示されません（添付になったHTMLファイルを開いて確認するしかありません）．

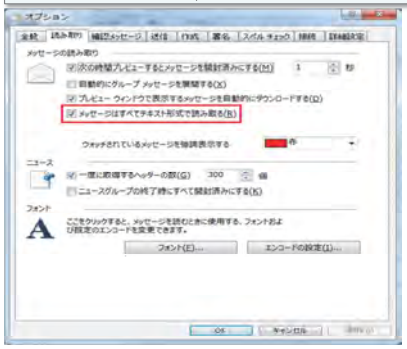


図　受信したHTMLメールのテキスト表示への変更方法．
左上の▼マークをクリックし，「オプション」→「メール」を選択．メッセージをテキスト形式で読み取るにチェック．

添付ファイルの表示

デフォルトでメールのプレビューが有効であり，メール一覧からSubject/Fromを選択すると，プレビューウィンドウに本文を表示します．また，添付ファイルに画像がある場合は，画像も本文と一緒に表示します（デフォルトでは、左側がフォルダツリー，中央がSubject/From，右側がプレビュー部分）．
プレビューを無効にするには，上部にある「表示」タブから「プレビューウィンドウ」の▼を選択し，「オフ」を選択します．ただしこの設定ではメールの一覧が表示される状態となり，一覧からメールをダブルクリックで選択してメールを表示して下さい（操作感が大きく変わります．ご注意下さい）．

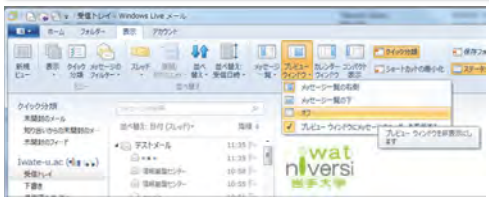


図　プレビュー機能の無効化．オフを選択して下さい．

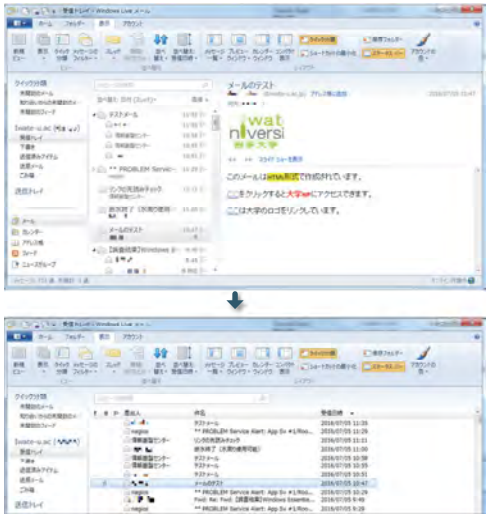


図　プレビュー機能のオン／オフでの画面イメージの差．
上：オン（プレビュー有効）
下：オフ（プレビュー無効）

差出人情報の表示

迷惑メール・攻撃メールを見分けるためには，メールの差出人情報をよく確かめる必要があります．
Live Mailでは，メールの一覧（プレビューのオン／オフいずれの場合でも）において，デフォルトで差出人名のみを表示し，メールアドレスは表示しません．メールを選択して表示した際（プレビューウィンドウも含む）は，デフォルトで差出人名とメールアドレスの両方を表示します．

メールヘッダの確認方法

怪しいメールだな，という時には，メールヘッダを確認してください．．
Live Mailでメールヘッダ全体を表示するには，メールの一覧から該当のメールを右クリックし「プロパティ」を選択します．プロパティの「詳細」タブをクリックすると、メールヘッダ全体を確認できます．

図　メールヘッダの確認方法．
メールのプロパティの詳細で表示できる．

メール作成の標準設定

メール作成時のデフォルトの形式（テキスト or HTML）を設定可能です．
(1) 左上の▼マークをクリックし，「オプション」→「メール」を選択
(2) メールのオプション設定が表示されるので，「送信」タブを選択
(3) 以下二つの設定を行う．
「受信したメッセージと同じ形式で返信する」のチェックを外す
「メール送信の形式」で「テキスト形式」を選択する
「受信したメッセージと同じ形式で返信する」にチェックが入っている場合，「メール送信の形式」で「テキスト形式」が選択されていても，HTML形式のメールに対する返信は強制的にHTML形式となるため，注意が必要です．

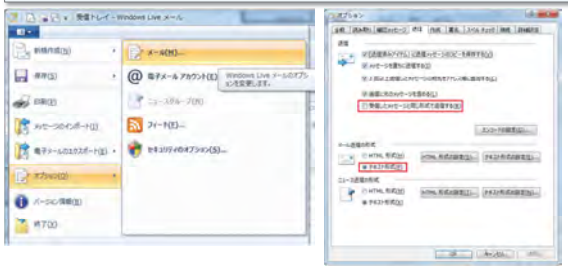


図　メール作成時のデフォルト形式の指定．

Shuriken 2016 編（Windows）

受信メールの表示形式

HTMLメールを受信すると，標準設定ではHTMLパートが表示されます．ただし，迷惑メールフォルダに分類されているメールはテキスト部分が表示されます．

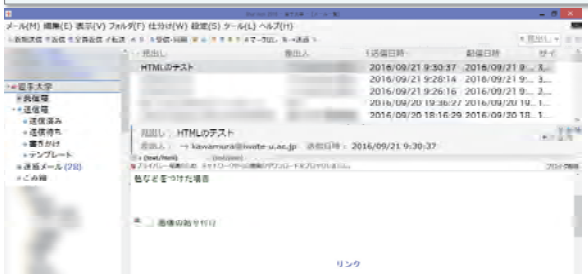


図　HTMLメール受信時の様子．標準設定ではHTML表示されます．
（標準設定では，添付ファイルでも画像等は表示されません）

［テキスト形式で表示するための設定の変更］

メニューから，「設定」→「共通の設定」を選択します．次に，「表示・動作」→「アイコン表示にするファイル種類」を「テキスト・HTMLメール以外」に設定します．これで受信されるすべてのメールはテキスト表示が標準になります．

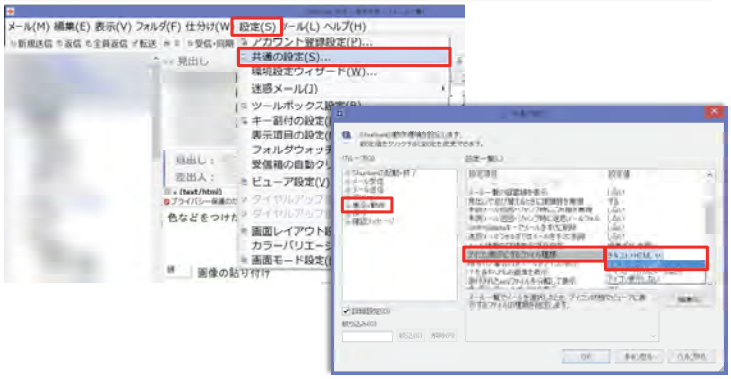


図　HTMLメールのテキスト表示への変更方法．
表示されたプルダウンメニューでテキスト以外を選択すると，受信時の標準動作がテキスト表示となる．

添付ファイルの表示

画像が添付されたファイルの場合，自動的に画像が表示されません．
Shurikenでは添付ファイルは一般的に，下図右のように”どのように処理するか”を明示する必要があります．添付ファイルを開く・閲覧する場合は，メールの素性に十分注意して開いて下さい（ウイルス・攻撃への警戒を！）．

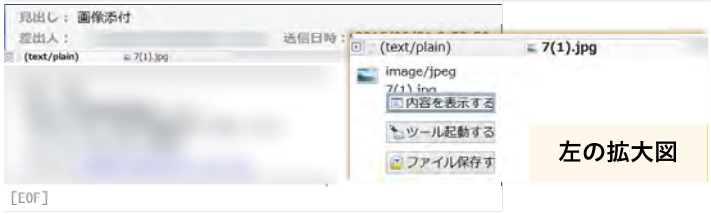


図　アイコン表示される添付ファイルと処理の選択画面．
アイコン（この場合は画像）をクリックすると，右の画面が表示される．ユーザが明示的に処理内容を選択する必要がある（自動的には開かれない・処理されない）．

差出人情報の表示

迷惑メール・攻撃メールを見分けるためには，メールの差出人情報をよく確かめる必要があります．
差出人のメールアドレスを表示するには，宛先をクリックして下さい．
詳細なヘッダ情報を表示するには，見出しをクリックして下さい．

図　宛先をクリックしてアドレス情報を確認した結果．
迷惑メールでの表示例．全要素が異なり怪しい．

図　見出しの表示例．ヘッダの詳細な情報が表示される．

メール作成の標準設定

メール作成の標準設定はテキスト形式です．
メールの形式をHTMLメールにした場合，テキスト形式には戻せません．
必要が無い場合は，標準のテキスト形式のままでメールを作成することを強く推奨します．

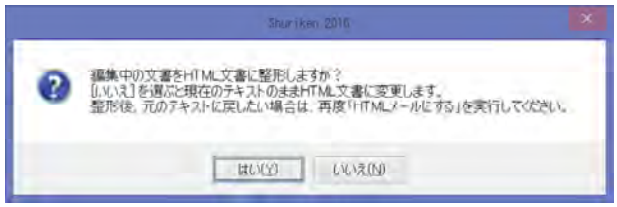


図　メール作成画面でHTMLメールとする場合の動作．HTML形式とする場合，警告（中）が表示される．「はい」を選択するとHTML形式に切り替わる（下）．

Mac mail 9.3 編（Mac）

受信メールの表示形式

受信メールの表示形式の標準設定はHTML形式です．リンク部分にオンマウスすると，URLがツールチップで表示されます．リンク先もプレビュー表示されますし，画像も表示されます．
テキスト表示にする設定は，このメールソフトには存在しません．このため，少しでもセキュアにするために，以下の設定を行ってください．

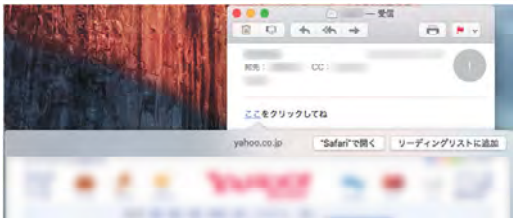


図　HTMLメール受信時の様子．HTML形式で表示されます．また，リンク先もリンク右隣の矢印をクリックするとプレビュー表示されます（Webアクセス）．

［少しでも危険性を減らすための変更］

画像をブロックするか否かの設定は，［メール］⇒［環境設定．．．］をクリックして環境設定ダイアログを表示します．そして［表示］をクリックし「メッセージ内のリモートコンテンツを読み込む」のチェックを外します．

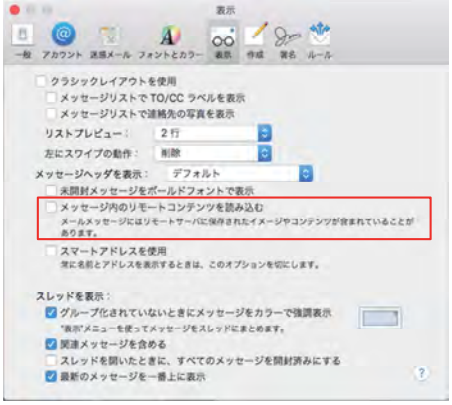


図　画像などを読み込まないように設定．
「メッセージ内のリモートコンテンツを読み込む」のチェックを外す．

添付ファイルの表示

Mac mailは，デフォルトでメールのプレビューが有効です．メール一覧からSubject/Fromを選択すると，プレビュー部分に本文を表示します．また，メール全体のプレビュー部分において添付ファイルはアイコンとして表示されますが，画像は自動でプレビューされます．
画像プレビューは無効化できませんでした．

差出人情報の表示

迷惑メール・攻撃メールを見分けるためには，メールの差出人情報をよく確かめる必要があります．
Mac mailでは，メールの一覧において，差出人名が有る場合は表示し，無い場合はメールアドレスを表示します．メールを選択してプレビュー表示した際は，標準設定では差出人名とメールアドレスの両方を表示します．

メールヘッダの確認方法

怪しいメールだな，という時には，メールヘッダを確認してください．．
メールヘッダ全体を表示するには，［表示］→［メッセージ］→［すべてのヘッダ］を選択します．

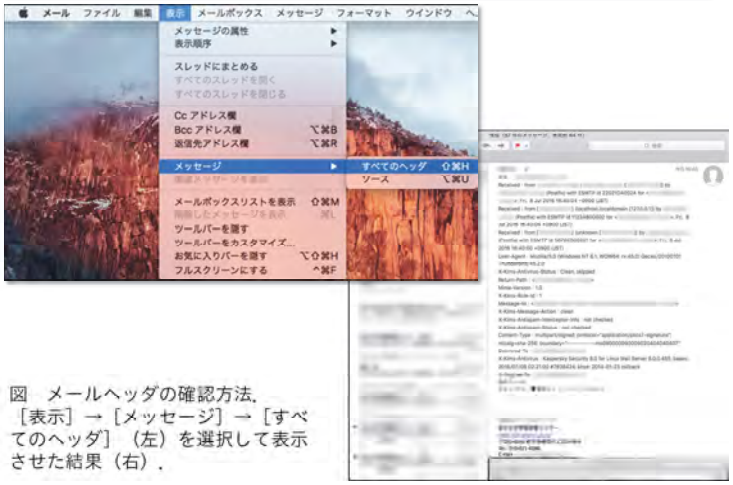


図　メールヘッダの確認方法．
［表示］→［メッセージ］→［すべてのヘッダ］（左）を選択して表示させた結果（右）．

メール作成の標準設定

Mac mailは，メール作成の標準設定はHTML形式です．
しかし，加飾しなければTEXT形式で送信されます（Content-Type：text/plainを確認）．
→　フォントサイズや文字色などの装飾アイコン の機能を使わない

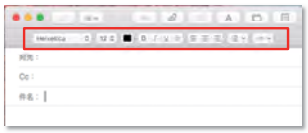


図　メール作成画面．
加飾アイコン は触らない！
（加飾しなければテキスト形式になる）．

テキスト形式を標準に

標準設定をテキスト形式にするには，環境設定から行います．
(1)［メール］→［環境設定．．．］をクリックして環境設定ダイアログを表示
(2)［作成］をクリックし「メッセージのフォーマット」を「標準テキスト」に設定

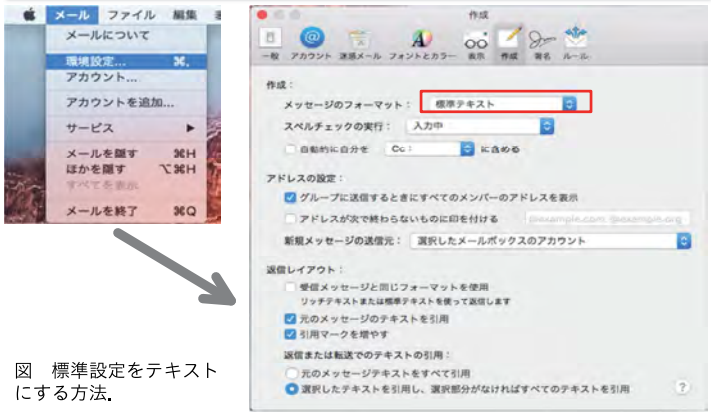
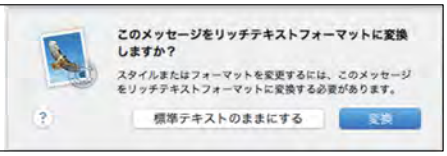


図　標準設定をテキストにする方法．

※　注意　※
テキストの設定でメール作成時に加飾を行うと，右図のメッセージが表示されます．



（参考）Active! Mail 編（ウェブメール）

メール受信についての設定

＜PC版・スマートフォン版＞
受信メールの表示形式の標準設定は テキスト形式 となっています．
- リンク（aタグ）がある場合は，リンクURLが本文にテキストで表示されます．
- imgタグによる画像も表示されません
- HTML形式の場合、ツールバー部分にメールをHTML表示するボタンが表示されます（ボタンを押すことで表示を切り替える）

テキスト表示の場合，リンク部分にオンマウスすると，ブラウザのステータスバーにURLが表示されます（ブラウザの機能）．オンマウスによる外部リンクの先読みやポップアップはされません．

図　HTMLメール受信時の様子．標準でテキスト形式で表示されます．
赤枠は，HTML表示に切り替えるボタンです．

メール作成の標準設定

＜PC版・スマートフォン版＞
送信メール作成時の標準形式 テキスト形式 となっています．
HTML形式でメールを作成する機能を有しますが，本学の場合はセキュリティに配慮し，無効としています．

＜モバイル版＞
メール作成の標準設定は，テキスト形式です．

Active! mail利用時の注意

Active! mail（ウェブメール）は，出先から利用する場合が多いと思われます．通常使っている環境（メールソフト）と異なるためか，受信された迷惑メールに対して，普段とは違った対応をしてしまう事例も散見されます．
Active! mail（ウェブメール）を使う場合は，気持ちに余裕を持ち，迷惑メールの文言に惑わされないこと，**おかしいな？という場合にはCSIRTに即連絡！**を，お願い致します．

CSIRT（Computer Security Incident Response Team）
ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください
e-mail: csirt@iwate-u.ac.jp

メールソフト別リンク先URLの確認方法

リンク先URL確認の必要性

HTMLの<A>タグでは，リンク先と別名を指定できます．このため，攻撃を指向したメールでは，一見した限りでは正当なリンク先と見せかけて利用者を攻撃用サイトに誘導する手法が頻用されます．
リンク先をクリックする前に，リンク先URLの確認は必須です．

リンク先URLの確認方法

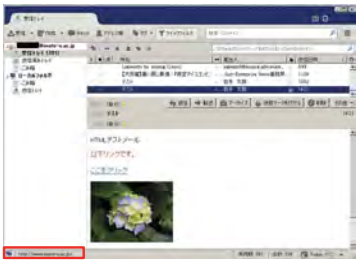


図　Thunderbird．
リンク先にマウスを乗せると，画面左下にリンク先URLが表示される．

図　Outlook．
リンク先にマウスを乗せると，ツールチップ内にリンク先のURLが表示される．

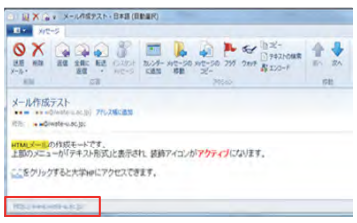


図　Windows Live Mail．
リンク先にマウスを乗せると，画面下段ステータスバーにリンク先URLが表示される．

図　Shuriken．
HTMLメールをHTMLで表示している場合に，リンク先にマウスを乗せると，画面下段ステータスバーにリンク先URLが表示される．

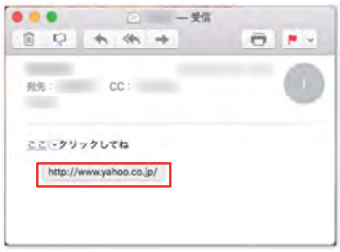


図　MacMail.
リンク部分にオンマウスすると，URLがツールチップで表示される．

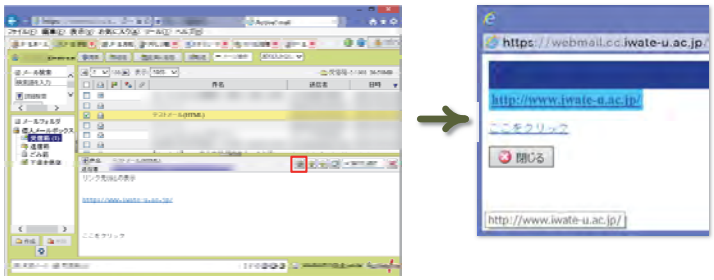


図　Active! Mail（Internet Explorer 11）.
標準はテキスト形式で表示されている．HTML表示にするアイコンをクリックすると，HTML表示画面が現れる（右）．
リンク先URLは，IE 11の場合は，リンク部分にオンマウスすると，URLがツールチップで表示される．

＜参考＞　Firefoxで常時リンク先URLを表示するアドオン

Firefoxでは，Webコンテンツのリンク先をツールチップで表示するアドオンがあります．リンク先URLを確認する際に，マウスのそばにリンク先URLが表示されるので非常に便利です．また，フォントサイズ・折り返しなども設定できます．

- 入手：[Firefox] ツール→アドオンから，URL tooltipを検索しインストールする
- 設定：[Firefox] ツール→アドオンから，URL tooltipの設定をクリック

注意　このアドオンは商用製品ではないため，利用する際は，サポートなどがないことを踏まえた上でご利用下さい（フリーウェア，オープンソース共通の考え方です）．

図　URL Tooltipの導入方法（Firefox Add-on）.
アドオンから，URL Tooltipを検索し，インストールする．Firefoxの再起動後有効になる（初回のみ必要）．

第３章
添付ファイルの取り扱い
―情報流出を防ぐ―

暗号化機能の紹介

Microsoft Officeや，PDFファイルでの，パスワード付与による暗号化について紹介します．

機微な情報を電子メールで送付する場合は，送出する情報をパスワード付与して暗号化することにより，流出のリスクを軽減することが出来ます．

データを持ち出す場合も，パスワードで内部データが暗号化されるUSB機器を利用することで，当該機器紛失時のダメージを軽減できます（技術的手段を用いないとデータを取り出せないため）．

備　考

情報の管理規則の詳細については，大枠は諸規則（総務広報課）などで定められています．規則等はガルーンを参照ください．

情報基盤センターは，個人情報等を含む情報のうちパソコンで取り扱うもの（データ，電子メール等）について検討しています．

取り上げるソフト
Microsoft Office 2013（Windows, Mac）
Adobe Acrobat（Windows）
JustSystems JustPDF 3（Windows）
Pdf.（Mac）

Microsoft Office

Microsoft Officeでは，アプリケーションの機能により，ファイル単位で暗号化できます．
ただしバージョンによっては，暗号化に対応していなかったり，下位バージョンではファイルを開く事ができない場合があります．また，パスワードを忘れてしまうとファイルを開くことが出来なくなりますので注意してください．

Windows版：Office 2007以降を推奨
2003以前は，暗号強度が弱いため非推奨です．
また，ソフトウェア自体のサポート期間に注意して下さい．
サポート終了日　Office 2003：2014年4月9日　Office 2007：2017年10月10日

Mac版　：Microsoft Office 2016 for Macを推奨
2016 for Mac以前の版は暗号化機能が不十分（または機能が一部非搭載）です．
また，サポート期限（Office 2011 for Mac：2017年10月10日）に注意して下さい．

Word 2010, 2013（Windows）

設定手順　「ファイル」タブ(A)→「情報」(B)→「文書の保護」(C)
→「パスワードを使用して暗号化」(D)

パスワードを入力(E)した後保存して下さい．暗号化されたファイルは，次に開く際にはパスワード入力が求められます．

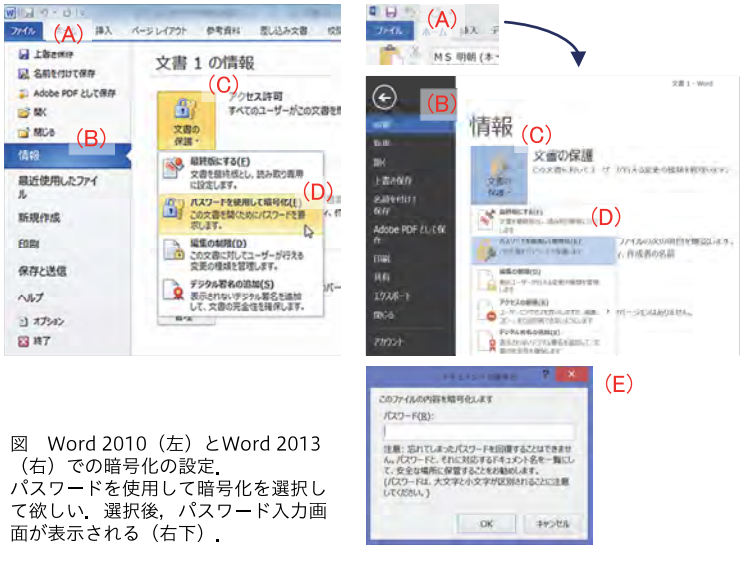


図　Word 2010（左）とWord 2013（右）での暗号化の設定.
パスワードを使用して暗号化を選択して欲しい．選択後，パスワード入力画面が表示される（右下）．

Excel 2010, 2013（Windows）

設定手順　「ファイル」タブ(A)→「情報」(B)→「ブックの保護」(C)
→「パスワードを使用して暗号化」(D)

パスワードを入力した後保存して下さい．暗号化されたファイルは，次に開く際にはパスワード入力が求められます．

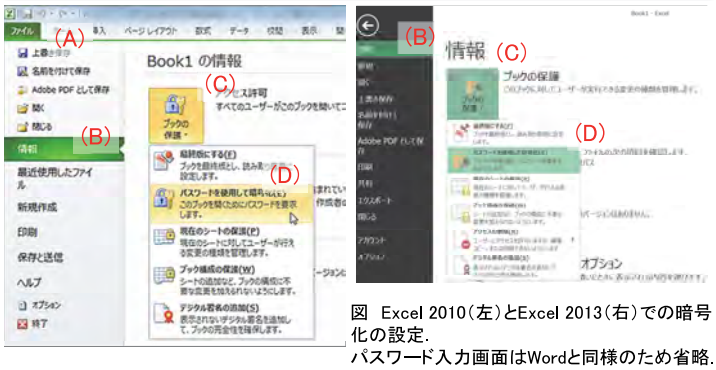


図　Excel 2010（左）とExcel 2013（右）での暗号化の設定.
パスワード入力画面はWordと同様のため省略.

PowerPoint 2010, 2013（Windows）

設定手順　「ファイル」タブ(A)→「情報」(B)→「プレゼンテーションの保護」(C)
→「パスワードを使用して暗号化」(D)

パスワードを入力した後保存して下さい．暗号化されたファイルは，次に開く際にはパスワード入力が求められます．

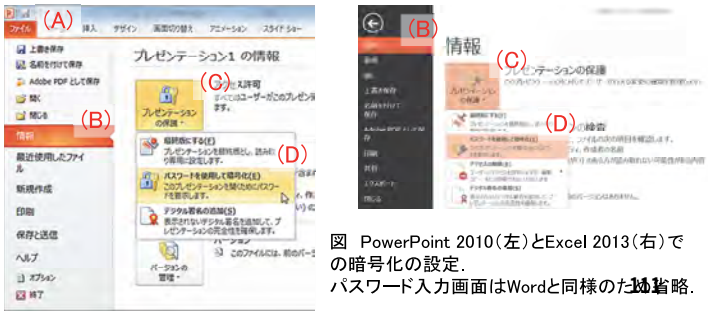


図　PowerPoint 2010（左）とExcel 2013（右）での暗号化の設定.
パスワード入力画面はWordと同様のため省略.

■ Mac版Officeでの注意 ■

Mac版のOfficeも，基本的な操作はWindows版のOfficeと同様です．ただし，Mac版Officeですべてのファイル形式（Word, Excel, PowerPoint）に対応しているのはOffice 2016 for Mac以降となります．

- Office 2008 for Mac：PowerPointにパスワード機能が非搭載
- Office 2011 for Mac ：パスワードの文字数が15字までに制限されている
  → Windows側で16字以上のパスワードを登録した場合，Mac側で開く事ができない

このため，WindowsとMacでファイルのやり取りをする場合，パスワードを15文字以内にするか，Office 2016 for Mac の利用を推奨します． また，パスワードを忘れてしまうとファイルを開くことが出来なくなりますので注意してください．

Mac版　：Microsoft Office 2016 for Macを推奨

Word 2016 (Mac)

Excel 2016 (Mac)，PowerPoint 2016 (Mac) でも，ほぼ同等の操作でパスワード付与が行えます．

方法A　アプリケーション内の“校閲”タブ (A1) →「情報」 (A2) →「文章の保護」 (A3)
方法B　メニューバー「ツール」(B1) →「文書の保護」(B2)

表示されたパスワードによる保護（3）で，パスワードを入力した後保存して下さい．**確認のため，パスワードは再入力が求められます．**

暗号化されたファイルは，次に開く際にはパワード入力が求められます．パスワードは忘れないようにして下さい．

(3)

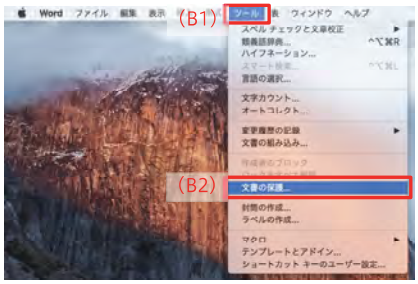


図　Word 2016 (mac)の画面.
画面上　校閲　→文書の保護.
画面左　ツール→文書の保護.
画面右　パスワードによる保護の画面.
パスワードは再入力を求められます．

＜参考＞ ZIPによる暗号化

■ ZIP等圧縮ファイルを利用する場合の注意点 ■

実験データなどを送るために，ZIPなどの圧縮ファイルを利用する機会も多いと思われます．アーカイバを利用する場合の注意点を記します．

1. 相手の環境を考える

圧縮ファイルに用いられる形式は多数存在します．このため，相手のパソコン・OSで扱うことが出来るか確認してから使ってください．未対応の形式の場合，相手のパソコンで開くことが出来ない場合があります．

2. 同一の形式でも支障が出る場合がある

OSが異なる場合，ファイルシステムの文字コードが異なるため，圧縮ファイル中のファイル名やフォルダ名が文字化けする・余分なファイルが格納されてしまう場合があります．

特に，MacとWindowsで圧縮ファイルをやり取りする場合，Macで圧縮したものをWindows側で開こうとすると文字化けや余分なファイルが格納されていて不都合が発生することが知られています．

3. 圧縮ファイルへのパスワード付与も検討する

格納した情報が重要なもの・保護すべきもの（例：個人情報等）の場合は，圧縮ファイルにパスワードを付与してください．

■ ファイル圧縮で利用するソフトウェアについて ■

OS標準のファイル圧縮機能（アーカイバ）では，パスワード付与・異OS間でのファイルのやりとりに十分対応しているとはいえません．そこで，WindowsおよびMacで利用できるアーカイバをいくつか紹介します．

詳しくは，パスワード付き暗号化によるファイル保護（情報基盤センターセキュリティポータル内）をご覧下さい．

https://isic.iwate-u.ac.jp/security/safeguard/file/encrypt.html

1. Windows

Windows準拠のアーカイバではパスワード認証による暗号化機能が実装されていません．そのため， Explzh（無料．ただし業務利用は有料），7-Zip（無料），WinRAR（有料） などのアーカイバを別途インストールする必要があります．

また，Macでもファイルを圧縮・解凍する場合は，ファイル名の文字化けが発生するため，Microsoft Office や PDF を利用した方が安全です．

2. Mac

OS標準のコマンドでパスワード付与に対応しています．手順などは，パスワード付き暗号化によるファイル保護（情報基盤センターセキュリティポータル内）をご覧下さい．

※ Windowsで解凍すると文字コードが異なるためファイル名の文字化けが発生します．

Windwosでもファイル名を正常に表示させたい場合は，ZIPANG（無料）やMacWinZipper（有料）などのアーカイバを別途インストールする必要があります．

PDF：暗号化設定

PDFファイルの暗号化は，暗号化に対応しているソフトウェアで行います．

- Windows：Adobe Acrobat，JustSystem Just PDF　※ Acrobat Readerでは暗号化出来ません ※
- Mac　　：プレビュー機能（PDF）

パスワード付与により暗号化されたファイルは，パスワードが適合しないと内容を閲覧出来ません．このため，パスワードの取り扱いに注意して下さい．

Adobe Acrobat

画面などはWindows版のものです．

Adobe Acrobatで，暗号化したいPDFファイルを開きます．次に，ファイルのプロパティを変更します．

1．「ファイル」メニューの「プロパティ」をクリックする．
2．「セキュリティ」タブの「セキュリティ方法」を
　　「パスワードによるセキュリティ」に設定する．
3．「互換性のある形式」を「Acrobat 7.0およびそれ以降」にする．
　　※　暗号強度から，「Acrobat Xおよびそれ以降」を推奨．
　「文書を開くときにパスワードが必要」にチェックを入れ．パスワードを入力し「OK」ボタンをクリックする．
4．プロパティ変更後はファイルを保存してください．暗号化されたPDFが保存されます．
　次回から当該のファイルを開くとパスワード入力を求められます．

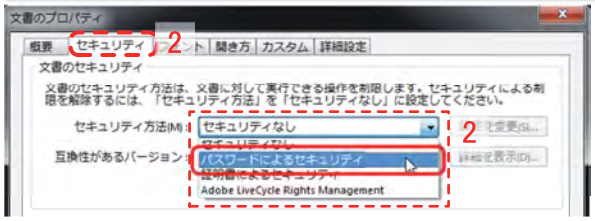
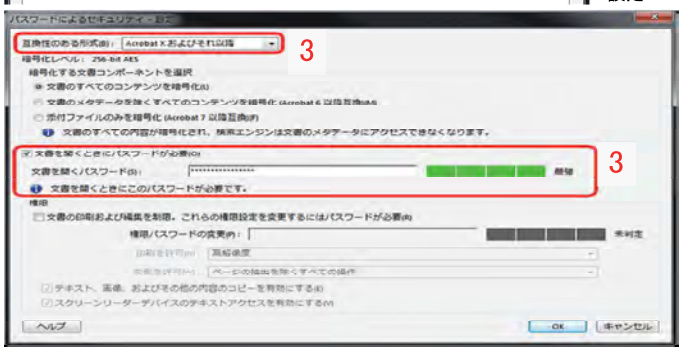


図　Adobe Acrobatでの，PDFの暗号化設定.



JustSystems Just PDF (Windows)

※Just PDF 3 [編集プラス] を使用した設定方法です．バージョンによって操作が異なる場合があります．

Just PDFでも以下の手順で暗号化できます．暗号化の設定後はファイルを保存してください．

1．ファイルを開き「文書」タブの「パスワードで文書を保護」をクリックする．
2．「パスワード保護」を「すべての文書内容を保護する」にする．
　「暗号化レベル」は「128bit AES(バージョン7以降)」に設定．
　　※ 暗号強度から「256bit AES(バージョンX以降)」を推奨．
　続けて「開く操作をパスワードで制限する」にチェックを入れ「設定」ボタンをクリックする．
3．パスワード設定用のウィンドウが表示されるので，パスワードを入力し「OK」ボタンをクリックする．

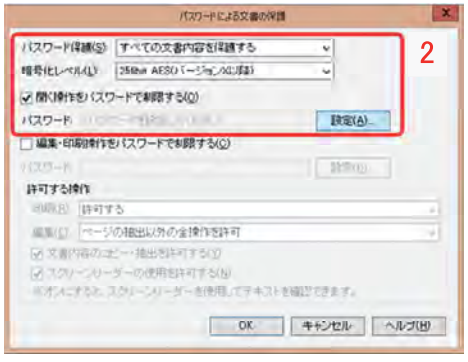


図　JustSystems Just PDF [編集] での，PDFの暗号化設定.

プレビュー機能（PDF）（Mac）

Mac OS Xでは，OS標準の プレビュー機能(PDF) で，PDFファイルを暗号化することが出来ます．予めOfficeのPDF出力機能などにより，PDFファイルを作成してください．

1．PDFファイルを開き「ファイル」メニューの「PDFとして書き出す...」をクリックします．
2．ダイアログが表示されるので「詳細を表示」をクリックします．
3．「暗号化」にチェックを入れパスワードを入力したのち「保存」ボタンをクリックします．
4．次回からファイルを開くとパスワード入力を求められるようになります．

図　Mac OS X標準のプレビューアを用いた暗号化方法．

＜参考＞ PDF：高度な設定

PDFファイルの暗号化では，閲覧者に対して，印刷や編集（コピーアンドペーストなど）について，制限を加えることが出来ます．
閲覧は許可するが印刷は許さないなど，資料の内容に応じた制限とすることが出来ます．

Adobe Acrobat

「文書の印刷および編集を制限」(A)にチェックを入れると，印刷や編集を無効にすることができます．ここで，PDF文書を開く操作を制限するためのパスワードとは別のものにして下さい．

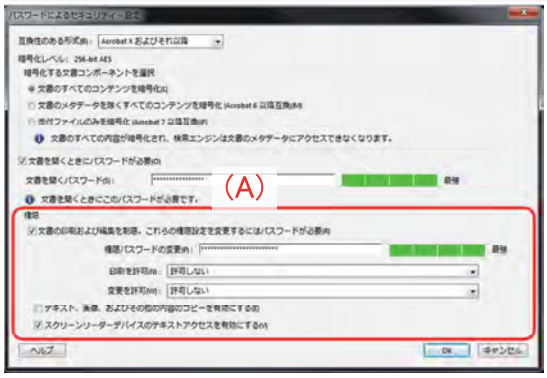


図 Adobe Acrobatでの，権限の設定方法．

JustSystems Just PDF

「編集・印刷操作をパスワードで制限する」(B)にチェックを入れると，編集や印刷を無効にすることができます．
PDF文書を開く操作を制限するためのパスワードとは別のものを設定して下さい．

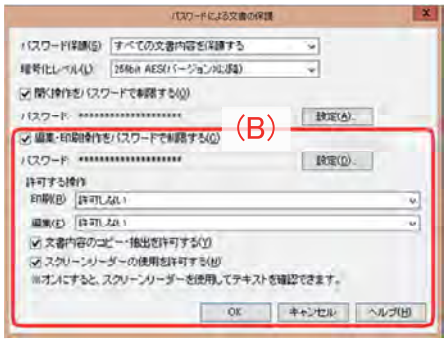


図　Just PDFでの，権限の設定方法．
編集・印刷動作をパスワードで制限するにチェックを入れる．

付　録
情報セキュリティ関連の規則へのリンク集

- 岩手大学 情報基盤センター内 利用案内
  関連規則へのリンク等が掲載されている
  https://isic.iwate-u.ac.jp/usersguide/
- 岩手大学 情報基盤センター内 セキュリティポータル
  ページ中程に，セキュリティ関連規則・ガイドラインが掲載されている
  https://isic.iwate-u.ac.jp/security/
- 岩手大学教職員ポータル
  規則・指針・制度を参照して下さい
  https://www.adm.iwate-u.ac.jp/

セキュリティ事案はCSIRTへ連絡！

CSIRT（Computer Security Incident Response Team）

ウイルス感染 や 情報漏洩 といった
情報セキュリティに関するトラブルは下記までご報告ください

e-mail: csirt@iwate-u.ac.jp

TEL: 019-621-6096 （情報基盤センター）

セキュリティ的に気になることがあった場合には，躊躇せず
ご連絡下さい．早期対応が大学のセキュリティを守ります！
早期対応には，皆様の”気づき”が重要です．

技術的な問い合わせは情報基盤センターへ

岩手大学情報基盤センター
〒020-8550 岩手県盛岡市上田3-18-8
TEL: 019-621-6096
FAX: 019-621-6097
e-mail: isic@iwate-u.ac.jp

情報セキュリティハンドブック　電子メール
第一版［教職員編］ 2016年度
― 電子メールを安心・安全に使うために知っておきたいこと．フィッシング被害にあわないために ―
（平成28年11月発行）

発 行 者　岩手大学情報基盤センター
Iwate University Super Computing and Information Sciences Center
連 絡 先　(020-8550) 岩手県盛岡市上田3丁目18－8　岩手大学情報基盤センター
印　　刷　杜陵高速印刷株式会社

Computer and Information Security Handbook 2016
1st Edition [Academicians and Staff Members] 2016
--- Basics and Email (English Abridgement Version) ---

Note: The Japanese version of this document is the original. This English translation is provided for the user's convenience.

Security Portal, Iwate University Super-Computing and Information Sciences Center
(In Japanese) https://isic.iwate-u.ac.jp/security/

Contents

Information security consultations to Iwate University CSIRT!

Take advantage of the Iwate University Computer Security Incident Response Team (CSIRT) information security consultation service!

Even though we use PCs every day, sometimes things happen that can cause us to feel uneasy.

Do you suspect that your device may have been infected with a virus?

Have you taken unwise actions regarding a suspicious email?

The Iwate University CSIRT is here to help! Do not let a minor worry grow into a serious information security problem. We promise to handle all inquiries with patience and understanding, so please do not hesitate to consult us. Everyone's cooperation is required to protect Iwate University from "Hacker Attacks".

e-mail: csirt@iwate-u.ac.jp Tel: 019-621-6096

Technical consultations should be addressed to Iwate University Super-Computing and Information Sciences Center (ISIC)

Is your computer connected a network?

If not, please consult ISIC regarding general PC-related problems.

e-mail: isic@iwate-u.ac.jp Tel: 019-621-6096

Part 1: Basics

Chapter 1: Iwate University information protection rules (outline)

Iwate University defines the rules and regulations for personal information handling. While, generally speaking, the General Affairs Public Relations Section ("総務広報課": Soumu Kouhou Ka) is responsible for document handling procedures, ISIC provides specific guidance related to digitized information document handling. By following this guideline, you can ensure you are in compliance with Iwate University rules, while simultaneously satisfying your social responsibilities regarding personal information protection.

Remarks

The Japanese edition of the Iwate University rules is the original.

English translations (including this handbook) are provided for the user's convenience.

The HOW TO of digitized information handling

Information to be safeguarded by password protection and/or encryption

(1) Entrance Examination Problems
- Issues related to entrance examinations (departments and graduate school)
- Examination answers (when computerized)

(2) Files containing personal information

EXAMPLE
- Student letters of recommendation
- Student personal records
- Documents with student full names, including:
  - ✓ Examination results
  - ✓ Laboratory communications
  - ✓ Graduate lists
- Questionnaire investigations that include personal information

Methods (measures)

Take the following measures to prevent unauthorized members of the general public from accessing information.

Mandatory

(1) PC
- Use password locks (restrict access by using a strong login password).
- Never use automatic login functions

(2) When you deliver electronic data to a third party
- USB flash memory or USB hard disk drives (HDD)
  - ① Encrypt the target files.
  - ② Use encryption-supporting USB devices

(3) When sending files by email
- Encrypt the target file. (Take particular care when transferring the password.)

(4) Email archive (When saving emails to your PC)
- Ensure your PC is protected with a password lock. (Disable any automatic login features.)

By following these measures, you can satisfy the rules of Iwate University.

A flowchart showing the established rules is provided below. (The "情報格付け手順", information rating procedure is based on Iwate University) rules. The chart explains information handling procedures based on how the information is rated (The "情報取り扱い手順", information handling procedure).

Terminology explanatory notes

Confidential level 1: Unrestricted Information

Confidential level 2: Classified Information (National security information, restricted data)

Confidential level 3: Restricted Information

Note: The Japanese version is the original. The English translation is provided for the user's convenience.

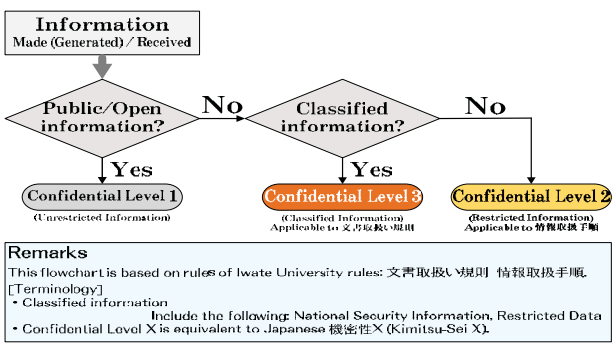


Fig. 1: Information rating procedure flowchart.

Chapter 2: Methods for protecting digitized information

To maintain your PC at a high security level

Basics (computer maintenance)

(1) Keep your operating system and all software up to date

(2) Have a (single) active antivirus product running and keep it updated
- ISIC distributes antivirus software for Iwate University members (University-limited) https://isic.iwate-u.ac.jp/usersguide/security/antivirus.html

(3) Run complete scans at regular intervals: PCs, USB devices (such as flash memory and HDDs)

(4) Ensure that no unauthorized persons can access your PC and/or data
- Use of automatic login functions is prohibited. (Ensure that a login password must be entered for each access.)

(5) Set a strong login password for all accounts
- Ensure that each password satisfies our password policy

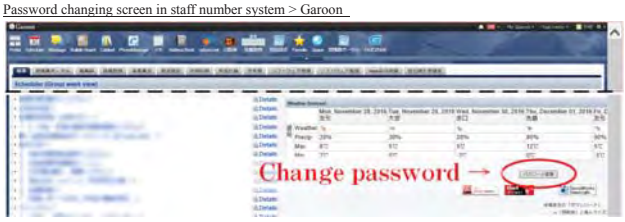
(6) Do not use an OS or software product that is no longer supported by the manufacturer.

Iwate University information system- Two kinds of ID and passwords-

Password

When creating a password, the following guidelines should be used.
- Use a minimum of eight characters (ideally 15 characters or more. Max: 25 characters).
- Do not use a dictionary word, a name, two short words joined together, or a sequences of numbers.
- Use a mixture of upper and lowercase letters.
- Include numbers and special characters.
- Do not use the same password more than once.

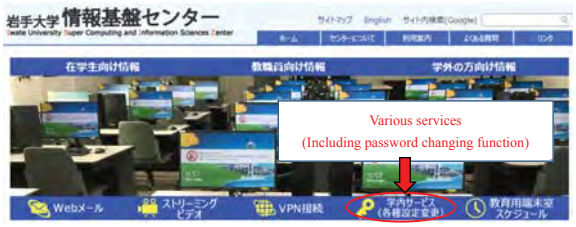
Password changing screen in staff number system > Garoon



https://iwjmcg.adm.iwate-u.ac.jp/

Fig. 2: Garoon password change screen.

Password changing screen in education computing system > ISIC Home Page



https://isic.iwate-u.ac.jp/index.html

Fig. 3: Garoon password change screen.

OS and Software Support Deadlines

Never use an OS or software product that is no longer supported by the manufacturer.

It is very dangerous to use an OS or software product that is past its end of life (EOL), because manufacturer support ends and updates are no longer provided.

[EOL information links]

Adobe products and Enterprise Technical Support periods covered under the new Lifecycle Policy [Adobe]
https://www.adobe.com/support/products/enterprise/eol/eol_matrix.html

Microsoft Lifecycle Policy and Lifecycle Search [Microsoft]
Lifecycle Policy: https://support.microsoft.com/en-us/lifecycle/
Lifecycle Search: https://support.microsoft.com/en-us/lifecycle/search

When will Microsoft terminate support for your version of Windows or Office? [ZDNET]
http://www.zdnet.com/article/when-will-microsoft-pull-the-plug-on-your-version-of-windows-or-office/

Application (Information protection)

Encrypt important information, including personal information and "Confidential Level 2" and "Confidential Level 3" data. See also Fig. 1.

Preferred information protection methods

- ✧ File Encryption (use software-supported encryption functions)
- ✧ Encryption-supported USB devices

[File encryption]

When you encrypt a file, we recommend the use of software-supported encryption functions.

[Word, Excel, PowerPoint]

Windows Microsoft Office 2007 or later
Macintosh Microsoft Office 2011 or later
As Office for Mac 2011 does not provide a full encryption function, we strongly recommend the use of Office for Mac 2016.

[PDF]
Windows, Mac Adobe Acrobat
Acrobat Standard Before X (10): End of Support
XI (11): End of core support on 2017/10/15
Mac
Preview.app OS standard application

Reference materials

Refer to Microsoft web page(s).
Search words:
Password protect documents, workbooks, and presentations
Add or remove protection for your document, workbook, or presentation

Securing PDFs with passwords [Adobe]
https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html

[Encryption-supporting USB devices]

Information recorded on encryption-supporting USB devices cannot be read if a proper password is not supplied.

However, you should always pay attention to the following:

(1) The password is the key to safety.
(2) Always test it before use.
- In most cases, USB devices work without problems.
- Check the USB chipset compatibility.

(3) Backup data to prevent loss.
- Regular backups really help in the case of hardware problems.
  - ✓ Backups are basic countermeasures. When a virus *, ** infection is found and the file system cannot be restored to the original state, the only safe solution is to restore the system to the uninfected state by using a backup.

* Files that were infected with a virus. In the case of an unknown malware threat, the security software may not remove the infection.
** Ransomware: This is a form of malware that encrypts files, and then requires ransom money to be paid in exchange for the decryption key.

Example of how to use a USB encryption device (External link)

Three ways to keep sensitive files encrypted on a flash drive or external hard drive
http://www.pcworld.com/article/2980184/storage/3-ways-to-keep-sensitive-files-encrypted-on-a-flash-drive-or-external-hard-drive.html *NOTICE: The URL does not start a new line*

Part 2: Email

Chapter 1: Ensure that you use email safely and securely

Many viruses, worms, and other malware, are designed to spread themselves throughout the Internet via email, which makes email a security hazard. Accordingly, we want you to be particularly careful about certain types of emails.

You can be attacked at any time!
Use caution every day!
Consult CSIRT if you have any suspicions!

Install antivirus software, and keep it running and up-to-date
In the case of HTML mail, use particular caution
Numerous attacks take advantage of HTML format emails
Do not open attachments from unknown senders
Do not click password reset links
Always verify the information contained within
Never give out your password in response to an email request
When sending an email, you must pay particular attention to the destination and content.

- ✧ Is the address correct?
- ✧ Is the information protected appropriately (e.g., encrypted)?
- ✧ Have you taken precautions against data leaks?

See also (Source of information, External link)

Kaspersky http://me.kaspersky.com/en/images/KESB_Whitepaper_KSN_ENG_final.pdf

Chapter 2: Recommended email software settings

The normal settings for most email programs are designed for user convenience. However, settings that are convenient for users are also convenient for attackers. (They make attacks much easier). This is also true for viruses and targeted attacks.

Accordingly, ISIC recommends the following settings to enhance security:

(1) Sending email in HTML format is prohibited.
- Iwate University rules prohibit sending emails created in HTML format.
- Use plain text format whenever you send an email.

(2) If the email program does automatically recognize an attached file, do not run it.
- DISABLE (turn off) the following features in your email program:
  - A) Automatically display images
  - B) Automatically display, open, or execute attached files

(3) Set the email program to display any received HTML mail in text format.

- View all email messages in plain text format.

(4) Check each website or URL/link for safety: Is the link suspicious, illegal, or a potential pathway for attacks?
- CHECK Use a confirmation method to verify the "true link destination."
- CHECK Use a confirmation method to verify the email header

Email program setup example (External Link)

NIST SP 800-45 Version 2, Guidelines on Electronic Mail Security [NIST]
http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

When you search following words by search engine, reference materials (documents, web sites) are found.
"email client" security guidelines *NOTICE: Do not remove the double quotations*

Chapter 3: Handling file attachments to prevent data leaks

(The information handling refers to Chapter 1.)

Information handling rules are set forth in Iwate University.

In particular, measures such as encryption are necessary whenever sending files that include (sensitive) personal information and Confidential Level 2/3 information (see, Fig. 1) via email.

One effective method for increasing security against data leaks when sending encrypted files is to send file decryption passwords by a separate (following) email.

Separate
Email containing the encrypted file
including Confidential Level 2 or Confidential Level 3 information.
Email containing the decryption password.

Appendix: Collection of links related to Iwate University information security rules.
NOTICE! The Japanese version is the original.
These are only available within the Iwate University campus network.

Editor's postscript

Satoshi Kawamura, Associate professor, Iwate University Super-Computing and Information Sciences Center (ISIC)

This guide was created by ISIC in order to raise the information security level of Iwate University. Ass. Prof. Kawamura, who played a key role in the creation of Japanese edition, also assisted in producing the English translation. It is provided for the convenience of persons whose mother language is not Japanese (such as foreign researchers and foreign students).

The Japanese edition of the handbook and rules are the official versions. This English version is an abridged translation. However, if you follow of the guidelines contained in this handbook, you will be in compliance with Iwate University rules.

ISIC anticipates that the information security level of Iwate University will be enhanced by this guide.

岩手大学情報基盤センター報告Σ　No.2　2016年度版
平成２９年３月発行

発 行 者　岩手大学情報基盤センター
Iwate University Super Computing and Information Sciences Center
連 絡 先　(020-8550) 岩手県盛岡市上田3丁目１８－８　岩手大学情報基盤センター