ISIC 岩手大学 情報基盤センター報告 Σ

2018年度版（2019年３月発行）

Σ

No.4 2018

Iwate University Super Computing and Information Sciences Center

岩手大学情報基盤センター報告 Σ の由来について

学内情報ネットワークは，多くのユーザに対する情報基盤センターの高度な情報サービスの提供を可能にしている．この学内LANを支えているのが基幹部分が光ファイバからなる「IHATOVnet」（イーハトヴネット）である．

本報告の「Σ」は，現在の学内ネットワーク「IHATOVnet」の前身である「Σネットワーク」にちなんでつけられたものであり，また，一般に和を表す記号として用いられていることから，「岩手大学の全構成員が有効に利用できる統合された学内情報システム」という情報基盤センターの理想を表すものである．

目次

巻頭言

情報基盤センター長　喜多一美

情報基盤センターにおける１年間の活動をまとめた情報基盤センター報告 Σ Vol. 4(2018 年度号)をお届けします。

情報基盤センターは，本学の教育研究の基盤となる情報基盤を所掌している教育研究支援施設です。具体的な活動としては，本学のネットワークシステムの維持管理，研究用計算機サービスの提供，教育用端末や事務用管理システムの維持管理，及び各種サービスを動かすための仮想化基盤等の管理運営などを担っています。また最近では，情報セキュリティインシデントへの対応に関する業務の割合が増加しています。

大学は，教育研究を行う場であるため，重要な情報が多く存在しています。教育では，学生に関する機微情報が存在します。研究においては，先端的な研究情報が存在します。これらの情報が安全に保護され，有効に利活用されるためには，学内の情報基盤の安全性が担保されなければなりません。たとえば，学内に侵入しようとするコンピュータウイルスなどの兆候をつかみ，不正アクセスや情報流出などを未然に防ぐ必要があります。

本学では、情報セキュリティインシデント対応を担う組織として，情報基盤センターのメンバーを中核とした CSIRT（Computer Security Incident Response Team）が活動を行っています。CSIRT 活動で観察されたヒヤリハット事例などの教訓をとりまとめ，学内に周知することも大きな役割です。また，本学の情報システムはインターネットで世界とつながっていることから，地政学的な趨勢にも目を配り，今後のサイバー攻撃などの脅威動向を踏まえた方針の策定や対策の立案も求められています。このように，従来のような狭い意味での情報基盤の維持管理・運用だけではなく，地政学的な情勢をも考慮しつつ，情報セキュリティインシデントに対応する必要が生じています。

本報告が，本センターの活動をご理解いただく端緒となり，情報基盤の安全な利活用につながることを願い，結びといたします。

【特集】
情報セキュリティ・CSIRT

実施方法を変更した情報セキュリティセミナー（実施報告）

情報基盤センター　川村　暁，加治卓磨
学術研究推進部学術情報課　庭田昌紀，菊地慧子
学務部学務企画課（元・学術研究推進部学術情報課）　奥崎たまえ

1. はじめに

情報セキュリティセミナーは，原則として本学の全構成員が受講することになっている 1)。学生は，入学時・進学時に受講するスタートアップセミナーを受講し，特段の事情のある者以外の全員が受講する必要がある。また，教職員も，情報セキュリティセミナーを受講する必要がある。

受講率向上や受講者の利便性の効用等を目的とし，平成 30 年度から情報セキュリティセミナーの実施方法を改めた。利用者の受講の手間を考え，情報セキュリティ自己点検も含める形で実施することにした。

本稿では，平成 30 年度の情報セキュリティセミナーの実施状況から，セミナーの実施方法を修正した効果について論ずる。なお，本講では教職員に対する情報セキュリティセミナーの実施方法について記している。

2. 平成 30 年度の情報セキュリティセミナーの実施方法

平成 27 年度までは，本学の規則では受講は利用者の義務であると規定されていても，情報セキュリティセミナーの受講率は低かった 2)～4)。これを改善するため，平成 28 年度から受講を必須であることを改めて周知するとともに，情報セキュリティセミナーを学内各所で全 16 回開催するとともに，都合により受講できなかった者や勤務形態の都合から受講できない者の受講機会を確保するため，同セミナーを録画した VOD（Video On Demand）を視聴し e-learning 問題に合格することで受講完了できるようにした。学内各所で非常に多くの回数対面式のセミナーを開催し，また，在席で受講できる仕組みを整えても，受講率を 100%とすることはできなかった。

前年度の施策を引き継ぎ，平成 29 年度は，実施回数を削減しつつ，在席で受講できる手段を併用することにした。これは，平成 28 年度に未受講だった者への対応のために用意した VOD 視聴および e-learning 問題に合格することで受講完了とする方法を援用した[4]。すなわち，学内での対面型の情報セキュリティセミナーの実施回数を主要な数カ所だけの実施とし，それ以外は VOD 視聴し e-learning 問題に合格することで受講完了できるようにした。利用者の義務としての情報セキュリティセミナーの受講は，本学構成員に浸透しつつあったが，平成 29 年度も平成 28 年度と同様，数パーセント程度未受講な者が残る結果となった[4]。

これらを踏まえ平成 30 年度は，以下の方策で臨んだ。

(a) 情報セキュリティセミナーの受講は利用者の義務であることを改めて周知する。
(b) 受講者の利便性を考え，VOD（Video On Demand）を視聴し e-learning 問題に合格することで受講完了とする。
(c) 業務が比較的繁忙ではない夏期休暇を受講期間とし，あらかじめ受講期間および受講期日を周知する。
(d) これまで 2 月頃に別途実施していた情報セキュリティ自己点検も，情報セキュリティセミナ

ーの問題に包含する。これにより，情報セキュリティ自己点検も実施したことになる。

(e) 受講期日までに情報セキュリティセミナーが受講完了とならなかった者は，情報基盤センターシステムアカウントをロックする。

(f) アカウントがロックされた場合，後日情報基盤センターを訪れて情報セキュリティセミナーに合格することでロックを解除する。

(g) これらのことを情報基盤委員会で周知するとともに，教授会や学内の各種連絡網を通じて教職員に周知する。

次章で，平成 30 年度の情報セキュリティセミナー実施計画と受講結果を示す。

3. 平成 30 年度の情報セキュリティセミナー実施計画と受講結果

表１に，平成 30 年度情報セキュリティセミナーの実施計画を示し，表２に受講結果を示す。

前章で記したとおり，受講期間は約一ヶ月とり，適宜リマインドも行っている。受講期日が来ても受講が完了していない者には,督促の上アカウントロックを行った。しかしながら,ほぼ 100%の受講率とすることができたのは大きな成果である。

昨年度までは，情報セキュリティセミナーの実施形態が複数あったこと，職位や職種による管理が，事務処理上の負担であった。これに対し今年度は，本学の情報基盤センターシステムアカウントを利用する教職員に対し事務的には同一の処理とすることができたため，事務処理の負担が大きく軽減している。

また，(d)に記したとおり，２月頃に別途実施していた情報セキュリティ自己点検もあわせて実施した。VOD とともに合格しなければならない問題のなかに，情報セキュリティ自己点検に相当する問題も含めることで対応した。この結果，事務処理・対応が必要な２つの情報セキュリティ関連の受講管理を，１つの施策で包含できることになり，事務作業を大きく増やさない効果を生んだ。受講者にとっては，２つの別々な情報セキュリティ施策に対応せずともよいという利点がある。

表 1　平成 30 年度情報セキュリティセミナー実施計画

実施単位	実施日	内　容
事前受講者	7 月 19 日（火）～ 7 月 31 日（火）	オンラインによる学習コンテンツの視聴及び理解度テストの受験
役員，副学長，部長(聴講を希望する課長)	7 月 19 日（火）13：15～14：15	講演「RSA におけるセキュリティの考え方」
全構成員	8 月 1 日（水）～ 8 月 31 日（金）	オンラインによる学習コンテンツの視聴及び理解度テストの受験

表 2　平成 30 年度情報セキュリティセミナー受講結果

受講対象アカウント数	受講済みアカウント数	未受講アカウント数	受講免除アカウント数(※)	受講率
1016	1008	1	7	99%

※内訳　１名：休職中（10 月 1 日退職）

　　６名：産休・育休取得中

4. まとめと今後の課題

岩手大学における利用者の義務である情報セキュリティセミナーの受講のうち，教職員向けの受講方法の変更について記した。在席で受講できるようにすること，期日までに受講を完了しない場合は情報基盤センターシステムアカウントをロックすることにより，受講率をほぼ 100%とすることができた。この成果を踏まえ，次年度以降も，この方法で実施することとしたい。

今後の課題は，学生向けの情報セキュリティセミナーが入学時に実施しているスタートアップセミナー受講だけであるため，在学生向けの情報セキュリティセミナーの実施について検討することと，短期留学生などで情報資源を利用する者への情報セキュリティセミナーの実施について検討することである。

参考文献

1) 川村　暁，庭田昌紀，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，岩手大学情報基盤センター報告Σ，No.2 (2016)，pp.48-49（2016）.
2) 川村　暁，奥崎たまえ，庭田昌紀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，岩手大学情報基盤センター報告Σ，No.2 (2016)，pp.50-55（2016）.
3) 川村　暁，加治卓磨，庭田昌紀，奥崎たまえ，平成 29 年度の情報セキュリティセミナー実施状況と平成 30 年度以降の実施方法の変更，岩手大学情報基盤センター報告Σ，No.3 (2017)，pp.7-16（2017）.
4) 川村　暁，中西貴裕，奥崎たまえ，庭田昌紀岩手大学の全ての常勤教職員を対象とした情報セキュリティセミナーとその効果，学術情報処理研究，21 巻 1 号，pp. 44-54（2017）.
DOI https://doi.org/10.24669/jacn.21.1_44

実施方法を変更したソフトウェア監査の効果（実施報告）

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，菊地慧子
情報技術部情報技術室

1. ソフトウェア監査

岩手大学では，教職員等構成員（以下構成員）の使用しているソフトウェア資産の管理のため，G-License と呼ばれるシステムを利用している。教職員は，自分の管理下にある PC にインストールされているソフトウェアの使用状況（ライセンスの状況）を G-License に入力し管理する。

法人としての岩手大学は，年に一度，ソフトウェアの使用状況をとりまとめるためソフトウェア監査を行っている 1)。ソフトウェア監査は，G-License において，構成員が使用状況の報告ボタン（監査のための情報とりまとめを行うボタン）を投下することで，統計情報を得ている。ボタンを投下しないとその年度での状況が確定されない（しかし，情報は都度入力・修正できる)。

ソフトウェア監査のとりまとめには，このボタンの投下が五月雨式になされるため，事務処理に大きな手数がかかっており，問題となっていた。

本稿では，この集計作業を軽減するためにとった方法を示す。

2. ソフトウェア監査のためのボタン投下を徹底するためにとった方法

ボタンの投下は，各年度における監査の事務処理にかかる時間を考慮して，学内に周知していた。平成 29 年度までは，複数回のリマインドを要するなど，事務処理が非常に煩雑であった。

平成 30 年度からは，別稿「実施方法を変更した情報セキュリティセミナー（実施報告)」の方法と同様に，期日までに報告ボタンを投下しない場合はアカウントをロックすることとした。

(a) ソフトウェア監査および報告ボタンの投下は，利用者の義務であることを改めて周知する。
(b) 受講期日までにソフトウェア監査のための報告ボタンの投下がなされなかった場合は，情報基盤センターシステムアカウントをロックする。
(c) アカウントをロックするとともに，ソフトウェア監査を行うための状況調査を個別に実施する。
(d) これらのことを情報基盤委員会で周知するとともに，教授会や学内の各種連絡網を通じて教職員に周知する。

平成 29 年度まで複数回のリマインドを実施して集計作業に入っていたが，平成 30 年度は，期日までに報告ボタンを投下しなかった者はごく少数にとどまった。ほぼ 100%の教職員が期日までに報告ボタンを投下した。事務処理としては，報告ボタンを投下しなかった者に対応するのも若干名だけで完了することになり，仕事量が大きく削減された。

このように，報告ボタンの投下が迅速なされるようになった結果，ソフトウェア利用状況の集計にかかる日数を大きく削減できた。

3. まとめ

ソフトウェア監査のための報告ボタンが投下されない問題に対し，利用者の義務として期日を

定めて改めて周知するとともに，期日までに報告ボタンが投下されない場合は情報基盤センターシステムアカウントをロックすることとした。この結果，報告ボタンが投下されないために発生していた事務処理が大きく減り，集計作業までに必要としていた日数を大きく減少することができた。

来年度以降も，本年度と同様の方法をとることで，速やかに処理を終えることを考えている。

参考文献

1) 川村　暁，庭田昌紀，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，岩手大学情報基盤センター報告Σ，No.2 (2016)，pp.48-49（2016）.

情報セキュリティ月間（５月・11 月）の取り組み

情報基盤センター　川村　暁，中西貴裕
情報基盤センター・技術部情報技術室　栗田宏明

1. 情報セキュリティ月間

昨年度から，情報セキュリティ意識を醸成するため，５月と 11 月を情報セキュリティ月間とし，取り組みを集中して実施する期間としている。

今年度は，

- サーバ管理者向けセミナー
- PC お悩み相談会
- セキュリティ啓発ポスター，チラシの作成と学内への掲出

を実施した。

2. 情報セキュリティ月間（５月）の取り組み

５月の情報セキュリティ月間で企画した行事等を記す。

１．暗号化 USB 機器を使ってみよう！　参加２名（申し込み２名）

日時：5 月 14 日(火)～16 日(木)，20 日(月)，21 日(火)の５日間

時間：8:30～17:15　（要予約）

対象：教職員

場所：情報基盤センター　１階　事務室

備考：利用されているノート PC を持参いただくと、詳しい説明や設定ができます。

２．PC お悩み相談会　参加者２名（申し込み３名）

日時：5 月 14 日(火)～16 日(木)，20 日(月)，21 日(火)の５日間

時間：8:30～17:15　（要予約）

対象：教職員

場所：情報基盤センター　２階 教育用端末

概要：PC を安全に使うための設定の見直しや、セキュリティソフトのインストール、暗号化対応 USB 機器の利用方法等、みなさんのお悩みに情報基盤センター技術職員が答えます。

「PC を安全に使うと言われてもよく分からない…」とお嘆きの方、ぜひ、相談会に参加してみませんか？

３　ポスター等の掲示

○購買／食堂への掲示

・購買：ポスター掲示のみ依頼

・各食堂（農学部，中央，理工学部）：アクリルスタンド（A5 両面）の設置

○事務，学部掲示板など

・事務部への掲示依頼，学部掲示板への掲示依頼

3. 情報セキュリティ月間（11 月）の取り組み

11 月の情報セキュリティ月間では，５月に実施したポスターの掲示に加え，情報セキュリティセミナー，Nessus による外部公開サーバの調査もあわせて実施している。情報セキュリティセミナーについては，本報告の「実施方法を変更した教職員向け情報セキュリティセミナー（実施報告)」および「実施方法を変更したソフトウェア監査の効果（実施報告)」を参照いただきたい。

１．情報セキュリティセミナー　オンラインで実施した。同時に、ソフトウェア監査も実施している。

２．セキュリティを高めるためのＰＣお悩み相談会

参加者：申込２名　内１名キャンセル　対応延べ人数３名

日時：11 月 12 日(月) ～ 16 日(金) の 5 日間

時間：8:30 ～ 17:15　（要予約）

場所：情報基盤センター　２階 教育用端末室

対象：本学の教職員と学生

概要：PC を安全に使うための設定の見直しや、セキュリティソフトのインストール、暗号化対応 USB 機器の利用方法等、みなさんのお悩みに情報基盤センター技術職員が答えます。

３．サーバ管理者向け情報セキュリティセミナー　　参加者：7 名

日時：11 月 27 日（火）13:00～14:30

対象：サーバ管理者

場所：情報基盤センター２階　教育用端末室

概要：外部公開サーバのセキュリティ対策等について、設定方法や勘所についてお話しします。

４　ポスター等の掲示

〇購買／食堂への掲示

・購買：ポスター掲示のみ依頼

・各食堂（農学部，中央，理工学部）：アクリルスタンド（A5 両面）の設置

〇事務，学部掲示板など

・事務部への掲示依頼，学部掲示板への掲示依頼

4. まとめ

利用者の情報セキュリティ意識を涵養するため，情報セキュリティ月間を定め，種々の取り組みを行った。今年度から、情報セキュリティに関連する取り組みをまとめて実施することで、それぞれの取り組みを連携しつつ進めることができた。

開催行事・取り組みに興味や関心がある場合は，お気軽に参加いただければ幸いです。

WAF 運用から見た Web サイト攻撃の傾向

情報基盤センター
技術専門職員　田頭　徹，岩手大学 CSIRT

1. はじめに

Web サイトへの攻撃を検知・遮断する手段の 1 つとして，Web Application Firewall（以下，WAF）がある。本学では，2010 年 8 月から，一部の Web サーバの前段に WAF を配置し，セキュリティの向上を図っている。2017 年 9 月のキャンパスネットワークの更新[1)] に伴い，WAF も新しい製品へと置き換わった。本稿では，新しい WAF の運用で得られたログから，WAF 配下の Web サーバに対する攻撃の傾向を分析した結果を報告する。

2. ネットワーク構成

WAF は，クラウド型ではなく，アプライアンス型の製品を学内に設置している。図 1 に，学外ネットワークから WAF および配下の Web サーバまでのネットワーク構成を示す。

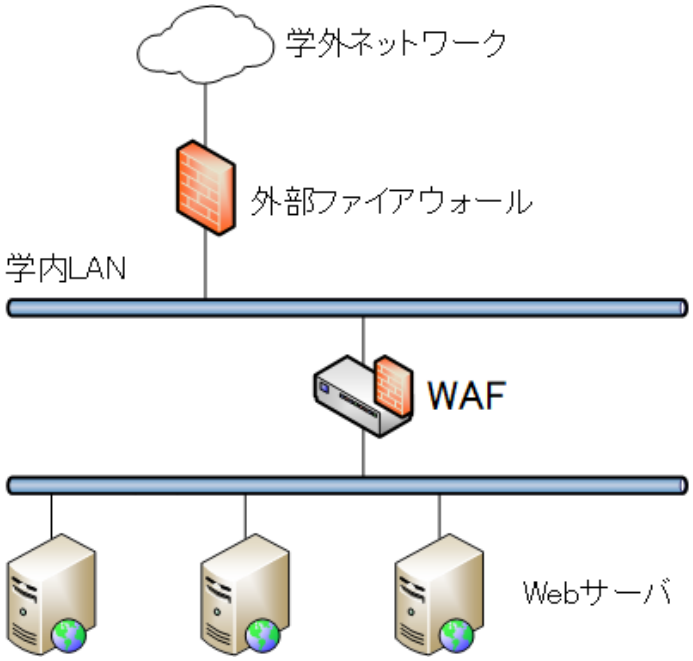


図 1　WAF とネットワーク構成

WAF は，Web サーバの前段に，リバースプロキシ構成で配置している。外部ファイアウォールとして設置している次世代ファイアウォールは，学外から見て WAF よりも前段にあり，学外からの通信において危険と判断した場合は遮断を行う構成である（但し，HTTPS など暗号化された通信については危険の有無を判断しない）。WAF は，次世代ファイアウォールを通過した通信および学内からの通信について，危険の有無を判断する。また，WAF は SSL アクセラレータも兼ねているため，クライアントと Web サーバとの通信が HTTPS であっても，攻撃を検知することができる。攻撃の検知方法は，ブラックリスト形式を採用している。

3. WAF のログ

WAF で発生したログは，WAF 本体で保持しているほか，syslog サーバへ転送している。syslog サーバへ転送されたログには，1 件の攻撃を 1 行として以下のような項目がカンマ区切りで保存されている。ログを分析するにあたり，集計や加工を行う事が容易なため，syslog サーバへ転送したログを利用した。

- リクエストの発生日時
- 接続元 IP アドレス
- 接続元ポート番号
- 接続先 IP アドレス
- 接続先ポート番号
- 攻撃の重大度
- 攻撃のタイプ
- 該当シグネチャ
- 接続元国

攻撃の重大度は，WAF において攻撃を検知するルールとともに定義されている値である。攻撃のタイプは，不適切な HTTP プロトコルや不正なメソッド，Evasion テクニック，WAF に予め定義された攻撃シグネチャによる検知の有無などであり，シグネチャによる検知の場合にはどのようなシグネチャにマッチしたかも記録される。接続元国は，リクエスト発生時点での接続元 IP アドレスを基に記録されている。

4. 攻撃の検知数と傾向

WAF 配下の Web サーバは，2018 年現在 9 台である。Web サーバの一覧を表 1 に示すが，Web サーバの具体的な IP アドレスやホスト名は伏せ，番号で記載した。

表 1　WAF 配下の Web サーバに対する攻撃検知件数と誤検知回避の設定件数

Web サーバ番号	Page View	学外からの攻撃検知件数	誤検知回避の設定件数
①	458,005	13,351	11
②	—	学内限定サイト	0
③	—	3,868	7
④	—	5,451	37
⑤	16,948	120	0
⑥	224,538	8,297	7
⑦	660,026	27,639	16
⑧	32,841	2,827	0
⑨	—	学内限定サイト	0
合計		61,553	78

表 1 に併記した Page View（PV）は，2018 年に取得した各 Web サーバのアクセス解析ツールの数値（ロボットによるアクセス件数は除外）を基にしており，業者がサーバを構築・管理して

いるサーバに関しては数値を記載していない。Web サーバの中には，1 つの IP アドレスで複数のドメインを運用（Virtual Host）しているものを含むが，IP アドレスごとの小計を記載した。

表 1 には，2018 年に各 Web サーバ（IP アドレスごと）に対して WAF が攻撃を検知した件数も記載した。また，本学内からのアクセスは，誤検知を多く含むため統計対象から除外した。一方，学外からのアクセスログには，誤検知のログも含まれているが，誤検知の多くは本学内からのアクセスで初めて発覚した事例が多く，攻撃の件数に比べて非常に少ないため，無視できる程度である。参考までに，各サーバにおいて再び誤検知しないよう設定を追加した件数も併記した。なお，検知した攻撃は遮断する設定となっているため，検知した件数と遮断した件数は等しい。

表 1 によると，Page View が多いほど，攻撃の検知数も多い傾向がある。これは，Web サイト（あるいはドメイン）が長い間利用されている事や著名であることが関係していると考えられる。

次に，攻撃の検知件数を攻撃のタイプごとに分類した結果を表 2 に示す。件数の合計が表 1 と一致しないのは，1 件の攻撃ログにおいて複数の攻撃タイプが該当したケースがあり，それぞれのタイプで 1 件としてカウントしたためである。

表 2　攻撃タイプごとに分類した攻撃の検知件数

攻撃のタイプ	件数
不適切な HTTP プロトコル	32,611
許可されていないメソッド（OPTIONS，PROPFIND，CONNECT 等）	17,641
Cross Site Scripting (XSS)	6,965
SQL Injection	6,712
推測可能なリソースへのアクセス（設定ファイルや隠しファイル等）	6,455
インジェクションの試行	2,720
Evasion の検知	1,960
非ブラウザのクライアントによる探索	1,650
コマンド実行	1,345
Denial of Service（DoS）	752
パストラバーサル	652
Server Side Code Injection	350
Session Hijacking	3
許可サイズを超過した POST	2
合計	79,818

表 2 によると，不適切な HTTP プロトコルや許可されていないメソッドに分類される攻撃が最も多い。これらは，サーバに対して特定の方法で接続を試み，その応答を確認しているものと思われる。これら 2 つは，利用している WAF のシグネチャに含まれない項目であるが，XSS や SQL Injection などはシグネチャに含まれる項目であり，どのようなシグネチャに一致したかを

見ることで，傾向を知る事ができる。ここで見られる傾向は，本学の WAF 配下にある Web サーバに対する固有の傾向の可能性があるが，他の Web サーバにおいても類似した何らかの傾向が見られると考えられる。

XSS は攻撃手法が多岐にわたるものであるが，XSS に関するシグネチャにより検知した 6,965 件のうち，5,415 件（約 78%）が eval に関するシグネチャにより検知されていた。これは，JavaScript の eval 関数の悪用を狙ったものと思われる。

SLQ Injection に関するシグネチャとしては，6,712 件のうち，5,574 件（約 83%）が SQL の like 句に関するシグネチャにより検知されていた。これは，like 句の付近で SQL Injection の脆弱性が見つかりやすい（対策漏れが起こりやすい）ことが影響していると思われる。

推測可能なリソースへのアクセスは，6,455 件のうち，/etc へのアクセスが 3,845 件，隠しファイルへのアクセス試行が 2,416 件であり，合わせて約 97%を占める。また，パストラバーサルにおいても，652 件のうち 493 件（約 76%）が /etc を狙ったものであり，攻撃者にとって価値のある情報を取得するための動作と窺える。

また，コマンド実行においては，1,345 件のうち 939 件（約 70%）が wget コマンドに関係するシグネチャにより検知されていた。これは，wget コマンドにより不審なファイルを外部サイトからダウンロードして設置する目的と推測されるが，PHP や Perl など Web システムを構成している言語から，OS のコマンドを呼び出している実装の悪用を狙ったものと思われる。

5. 攻撃の傾向から見える対策

前述の通り，Web サイトへの攻撃には傾向があり，これに応じて適切な対策が有効である事や，重点的に対策すべき点が見えてくる。例えば，XSS を狙った攻撃では，eval 関数を狙ったものが多い。eval 関数は便利なものであるが，そのリスクを把握し，極力利用しない事や影響の及ぶ範囲（スコープ）を考慮して利用する対策が求められる。また，Web システムを構成している言語から OS コマンドを呼び出す実装を避ける事も，Web 上から不正に OS コマンドを実行される事への対策となる。

アクセス試行においても，最小権限の原則を基に設定を見直し，不要な機能を有効にしないことや不要なファイルを配置したままにしない等，基本的な対策がなされているか十分に確認するべきである。また，長い間運用されているシステムや著名なサイト（ドメイン）であるほど攻撃を受ける頻度が多い傾向があるため，導入当時の古いライブラリやフレームワークの更新がなされているかも含めた点検が必要である。

6. 今後の展望

同様の機器が動作している期間中に同等の統計を継続し，年ごとの傾向を見てみると，攻撃の傾向の推移を追うことができると考えられる。また，攻撃を受けた URL を分析する事で，どのようなアプリケーションや機能が狙われているか確認することは，対策を考える上でも有用と思われる。このような分析を通じて，Web サーバのセキュリティ向上を図っていく所存である。

参考文献

1) 中西貴裕，福岡誠，金野哲士，加治卓磨，川村暁：キャンパスネットワークの更新，岩手大学情報基盤センター報告Σ，3 号（2017 年度版），pp.4-6（2017）

セキュリティ機器の運用について

情報基盤センター
大内　慎也，岩手大学 CSIRT

1.　はじめに

近年のマルウェア感染や機微情報の搾取は，スパムメールや Web アクセスが主な原因となっている。本学のユーザも「不用意にスパムメールの URL や添付ファイルを開いてしまう」「Web ブラウジング中，不正なファイルと認識せずダウンロードしてしまう」といった事がある。これらにより，マルウェア感染や機微情報が搾取される可能性があるため，CSIRT では学内のセキュリティ機器を活用して対策や対処を行っている

本稿では，セキュリティ機器の構成を紹介する。また，学内で「不正ファイル」および「不審なメール」を発見した時に，セキュリティ機器を活用した対策・対処等を記す。

2.　セキュリティ機器の構成

セキュリティ機器の構成を図 1，セキュリティ機器の概要を表 1 に示す。本学で使用しているセキュリティ機器は，「次世代 FW（ファイアウォール）」と「通信監視装置」の 2 つがある。これらは，2017 年度のネットワークシステムのリプレイスとともに導入された機器であり，それ以前には同等の監視を行う事ができなかった。 以下に，次世代 FW と通信監視装置それぞれについて説明する。

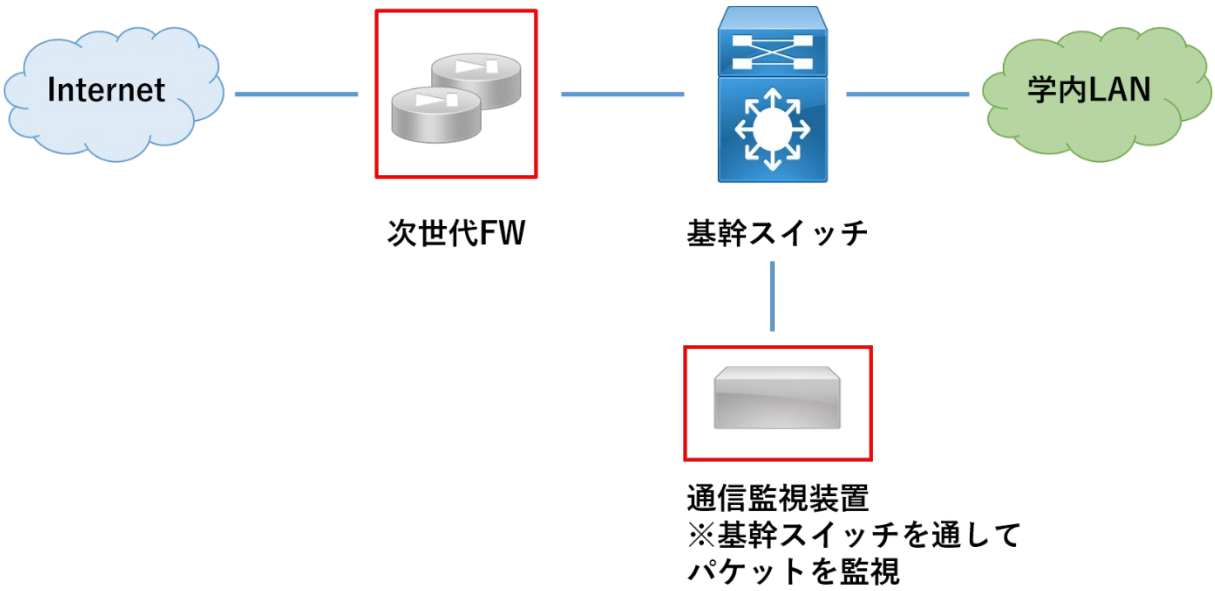


図 1 セキュリティ機器の構成

表 1 セキュリティ機器の概要

セキュリティ機器	主な機能	備考
次世代 FW	・IP アドレス・ポートの通信制御 ・不正な通信の検出・遮断 ・不正なファイルの検出・遮断 ・サンドボックス ・URL フィルタリング	・総合的なネットワークセキュリティ管理
通信監視装置	・不正な通信の検出 ・不正ファイルの検出 ・サンドボックス	・次世代 FW とは異なるサンドボックス ・補助的な役割

2.1. 次世代 FW

次世代 FW には，従来の FW の機能：「IP アドレス・ポートの通信制御」の他に，下記のような機能を持ち，学内の総合的なネットワークセキュリティ管理を実施している。

- 不正な通信の検出・遮断：
  各種 Flood 攻撃，ポートスキャンの検知，セッション数管理による防御，既知の脆弱性を利用した攻撃等を検知し，その通信を遮断・警告する機能
- 不正なファイルの検出・遮断：
  マルウェアリスクの高い不正なファイル等を検知し，その侵入を遮断する機能
- サンドボックス：
  保護された領域で不正ファイルを実行し，その挙動から不正なものか判断する機能
- URL フィルタリング：
  Web サイトアクセス時，そのサイトのカテゴリを判別し，不正なカテゴリのサイトへのアクセスを遮断する機能（※不正なカテゴリのサイトであっても，業務上必要な場合はアクセスを許可する）

2.2. 通信監視装置

通信監視装置は「不正な通信の検出」，「不正なファイルの検出」，「サンドボックス」等の検出に特化した機能を持つ。基幹スイッチを通してパケットを監視し，不正な通信・ファイルを検出する。次世代 FW と類似したセキュリティ対策機能を持つが，不正な通信やファイルを判断する基準が異なる事に加え，次世代 FW と異なるサンドボックス環境を利用している。

サンドボックスは製品によって確認できるファイル種別が限られている。本学では，次世代 FW と通信監視装置の双方のサンドボックスを併用することによって，より幅広いファイル種別への対応を実現している。そのため，通信監視装置は「次世代 FW では検出できない部分をフォローする」などの補助的な役割を持つ。

3. 不正ファイルの検出

学内から HTTP や POP などで学外サーバへアクセスした際，次世代 FW は不正と疑われるファイルを検知し，CSIRT 宛に警告メールを発する。この警告を受けて，CSIRT では以下のような調査・対処を行う。

1. 次世代 FW 内でのサンドボックスの解析結果を調査する（振る舞い，通信先など）
2. 通信監視装置でのサンドボックスの解析結果を二次調査する（振る舞い，通信先など）
3. ファイル検体のハッシュ値やファイル名から，同様のファイルが Web 上に存在しないか調査する
4. 不正なファイルと判断した場合，通信先の URL および IP アドレスを次世代 FW にて遮断し，被害の拡大を防ぐ

2018 年 4 月～2019 年 2 月の期間で，次世代 FW の警告は 71 件あり，不正な URL および IP アドレスは 50 件を遮断リストに登録した。

4. メール検体の活用

CSIRT では，ユーザから不審なメールを検体として提供するよう協力を呼び掛けている。また，自身で不正かどうか判断できないメールについても，CSIRT に提供して判断を仰ぐよう呼び掛けている。メール検体を受け取った後，以下のような調査・対処を行う。

1. メールの配送経路，URL および添付ファイルなどを確認する
   （正規のメールか，不正と疑われるメールか判断）
2. 不正なメールの場合，URL および IP アドレスを次世代 FW にて遮断する
3. 不正な URL や添付ファイルを開いてしまった連絡を受けた場合，前述の次世代 FW の警告後の処理と同様，通信監視装置と併せて調査・対処を行う

2018 年 4 月～2019 年 2 月の期間で，メール検体の提供は 272 件あり，不正な URL および IP アドレスは 206 件を遮断リストに登録した。

5. まとめ

本学で使用しているセキュリティ機器は，次世代 FW と通信監視装置の 2 つである。次世代 FW は総合的なネットワークセキュリティ管理の役割，通信監視装置は検出に特化しており補助的な役割を持つ。二つの機器を併用することによって，より幅広いセキュリティ対策を実現している。

今年度，ユーザの皆様からメール検体をご提供していただいたことにより，多数の不正な URL と IP アドレスを遮断し，マルウェア感染や機微情報の搾取等を防ぐことができました。岩手大学の情報セキュリティを維持するために，今後ともご協力をいただければ幸いです。

また，「学術サイトにアクセスできない」等，ユーザの皆様にはご不便等をお掛けすることがあります。この場合，岩手大学 CSIRT でサポート対応しておりますので，何なりとお申し付けください。どうぞよろしくお願いいたします。

参考文献

1) 中西貴裕，福岡　誠，金野哲士，加治卓磨，川村　暁：ISIC 岩手大学 情報基盤センター報告Σ 3 号（2017 年度版），pp.4-6（2017）.

【一般】

プログラミングによるビジュアル表現の愉しみ

- Processing を使った事例 その２-

人文社会科学部（芸術文化）教授　本村健太

1.　Processing によるプログラミングからの展開

アーティストやデザイナーでも比較的容易にプログラミングをすることができる言語（環境）である Processing との出会いによって，いわゆる「文系」の筆者であっても独学で何とかビジュアル表現ができるようになったことは前号の拙稿「プログラミングによるビジュアル表現の愉しみ - Processing を使った事例について - 」において明らかにした。

今回は，そのようなビジュアル表現のさらなる展開の可能性について，筆者の制作体験を通じて実現していることを紹介していきたい。表現の領域において，「ビジュアル」（本来，筆者は「ヴィジュアル」という表記を好むが）というと，「イメージ」や「画像」，あるいは「モニター」や「スクリーン」を連想させると思われるが，そこからいかに次の次元へと展開するか，その枠組みからいかに飛躍できるか，というのが筆者の大きな関心事となっている。

これから Processing を使った事例の解説を行い，その方向性での表現の可能性がいかに開かれてきているかを明らかにしたい。

2.　テキスタイルデザイン「ランダムトライアングルズ」

筆者は，視覚表現の手法について広く興味を持っており，基礎となる「ベーシックデザイン」（平面構成）の造形についても研究課題としている。ここでは，Processing を使用したプログラミングによって描き出された実践事例の一つとして，テキスタイルデザイン用の作品「ランダムトライアングルズ」シリーズを紹介する。

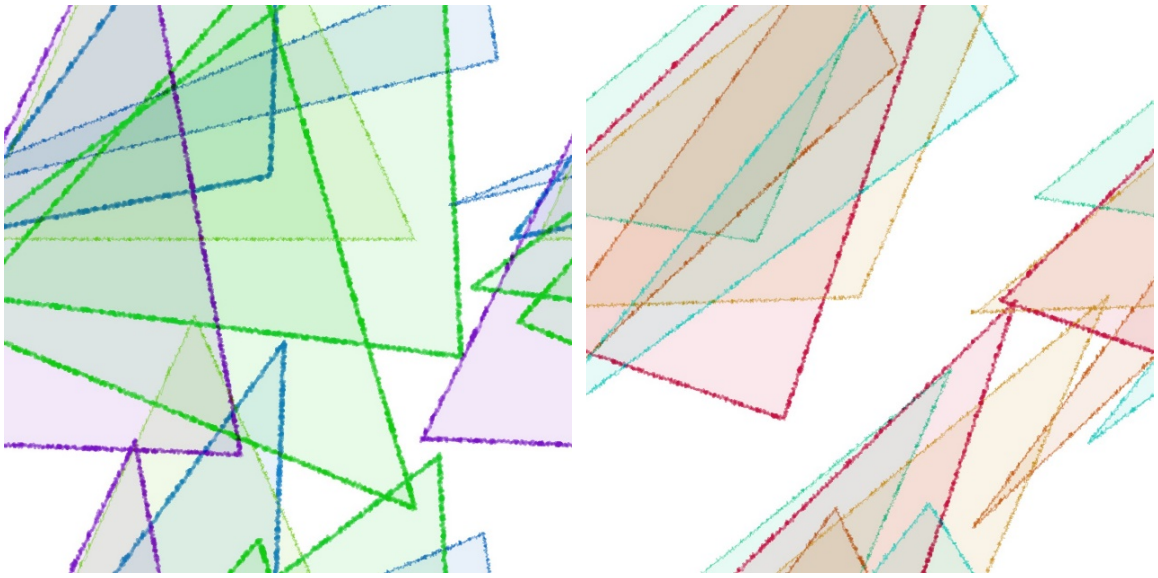


図１：テキスタイルデザイン「ランダムトライアングルズ」基本画像の例

図１は，タイル貼りされることによって上下左右が連続的な図形となるパターンデザインの

「基礎画像」の事例である。正方形（任意の長方形でもよい）の枠内に適度なランダム設定のなされた三角形が配置されているが，この枠からはみ出た部分は上下左右の反対側に描かれている。

したがって図２のように，タイル貼りされることによって平面を覆いつくすパターンとしてのテキスタイルデザインに仕上がることになる。このプログラミングの過程では，複数の三角形が多少重なり合うような設定にしたり，三角形の三辺の直線も微妙な震えを入れて面白さを試したり，また，ある程度ランダムでありながらも調和的な色合いになるように調節したりすることで独特の味わいを出すように工夫している。この作業は作者の美的感性に従うものとする。

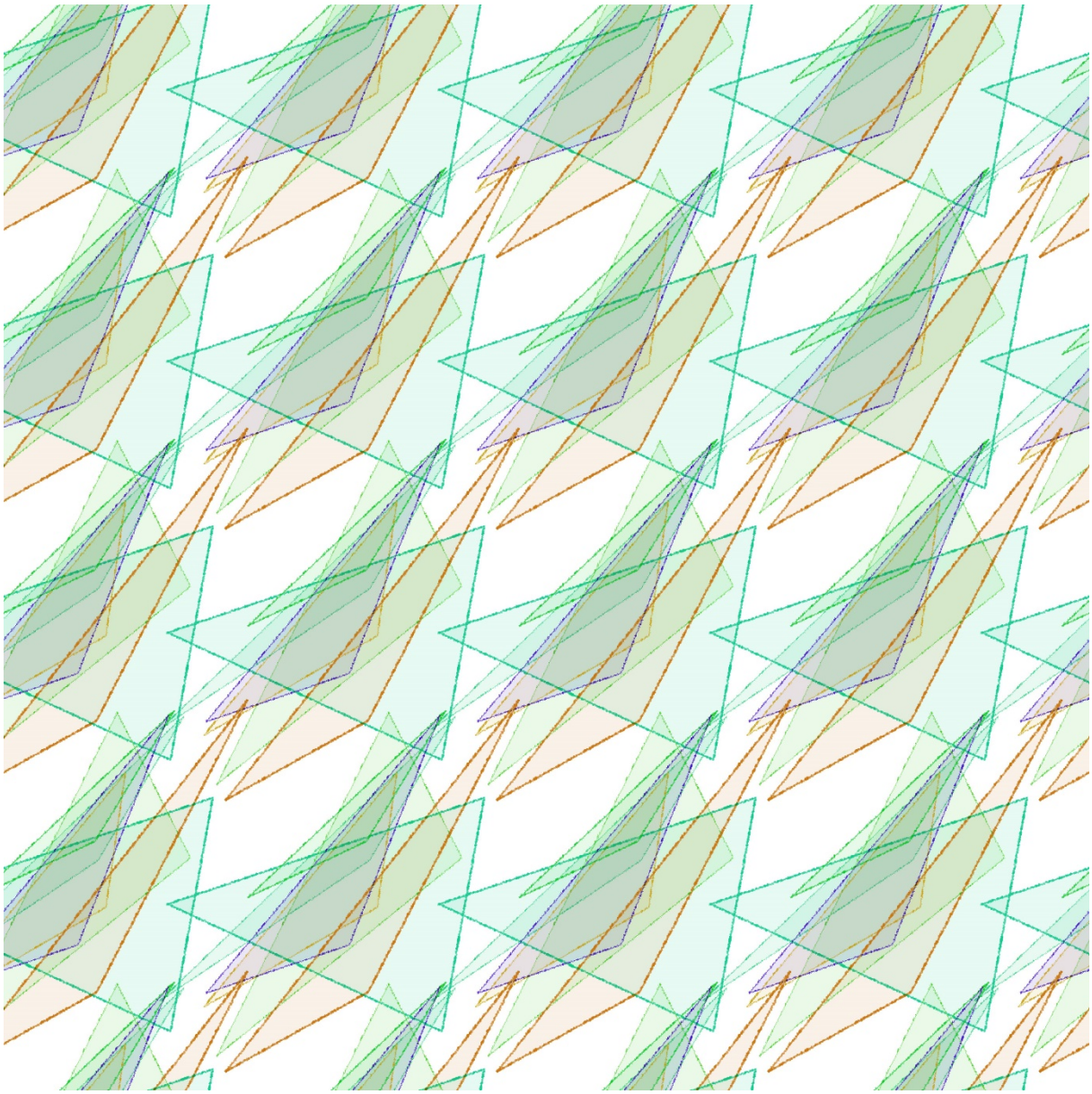


図２：テキスタイルデザイン「ランダムトライアングルズ」の一例

プログラミングによる基本画像は，１ 枚の断片としてのみ作り出される。そのサイズは任意の大きさに設定可能であり，100%のサイズでもパソコンのモニタ上で確認できる程度のものであれば，HTML で「<body background="(基本画像のファイル名).jpg"></body>」のように設定して Web ブラウザでタイル貼りの状態を容易に確認することができる。しかしながら，今回は布地にプリントされるテキスタイルデザインを目的としているため，プリントされた現物のサイズを想

定して，その倍くらいの画像サイズ（解像度：150dpi）は最低必要になる。当然，大きな絵柄のパターンを目指すのなら，基本画像も大きなサイズとなる。

図３は，このプログラミングを実行する度にランダムに描き出される基本画像を著者の好みに応じて保存するか，そのまま破棄するかの選択をした結果，残されたものの一部を使用して完成させたパターンデザインの事例である。このようにして作られるテキスタイルデザイン「ランダムトライアングルズ」は，例えば「オリジナルファブリック・マーケット」として自作の絵柄の布地を作ることのできる「HappyFabric」（https://happyfabric.me/）などの Web サイトにアップロードすることでも展開が可能となる。

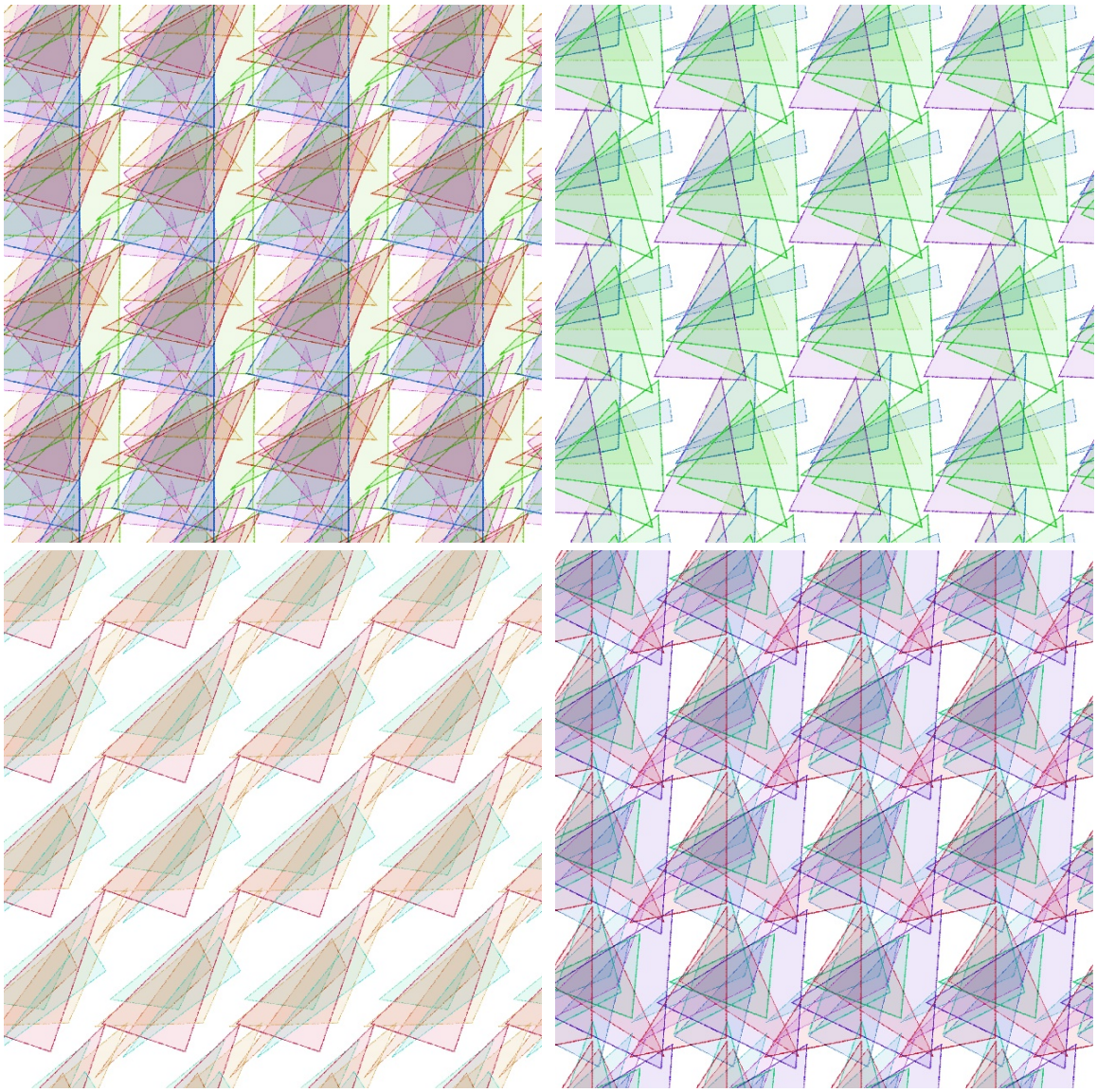


図 3：テキスタイルデザイン「ランダムトライアングルズ」シリーズの事例

実際にオリジナル布地の発注に至った経験はまだないが，すでに多少の費用をかければ難なく実現できる状態である。今回は，「ランダムトライアングルズ」，すなわち多様な三角形をモチーフとした設定でのデザイン化であったが，パターンにする工夫を少しするだけで基本的にはどんなものでも（幾何学的な形体に限らず，有機的な形状であっても）テキスタイルデザインにすることができる。もちろんそれは手描きや写真の画像処理でも可能なものであるが，わざわざプログラミングで造形することの意義は，ある程度制御は可能であるとしても，ランダム設定でその

都度新たな形体や色彩の組み合わせが提示され，作者が思いもしなかったような結果に出会うことができるということにある。また，この回数のことを考慮すれば単純な形体での作品でさえも「手描き」（この場合，PC とマウスで作画することも含む）より作業効率がよいのである。

3. 手芸「糸かけ曼荼羅」のシミュレーション

ここに紹介する手芸の「糸かけ曼荼羅」とは，ピン（釘）を板の上に円周上に立て，ある法則のもとに糸をかけていくことにより見いだされる幾何学的な模様である。写真１は，誰もが手軽に始めることができる「日本糸曼荼羅協会」による市販の制作キット（「釘打ち板」：板上にピンがすでに立ててある状態）を使って筆者が制作した結果である。まず基準となる最初のピンに糸をかけ，板の背面にマスキングテープなどで固定しておく。基本は「素数」の数だけ時計回りに飛んだピンに糸をかけ，またそこから同じ間隔で順次糸をかけていくとすべてのピンに糸がかけられ，最後は最初のピンに戻ってくることになる。（この基準のピンに最初にかけた糸と結んで固定する。）このようにして順次糸の色を変え，異なる素数の数で同じ作業を繰り返すことにより，糸かけ曼荼羅は写真１のように神秘的な美しさをたたえるものとなる。

写真１：手芸「糸かけ曼荼羅」制作キットの事例

単純な作業であるとはいえ，この作品を完成させるには数時間を要する。そこで，事前に結果の状況を確認できるように「糸かけ曼荼羅シミュレーション」をプログラミングで組んでみることにした。もちろん，筆者にも使える Processing によってである。実は Processing については iPhone や iPad でも使える無料のアプリ「Processing iCompiler」が開発されており，最初の構想からある程度かたちになっていくまでの工程ではこのアプリを多用した。また他者への提示も手軽に行うことができるという利点もある。図４および図５は，Processing アプリでのプログラミングによる途中過程のものである。ピンの数や糸の色，そして最初のピン（最上部）から何本飛んで糸をかけていくかを設定し，基準のピンに戻ってくるまでの結果が図示されている。

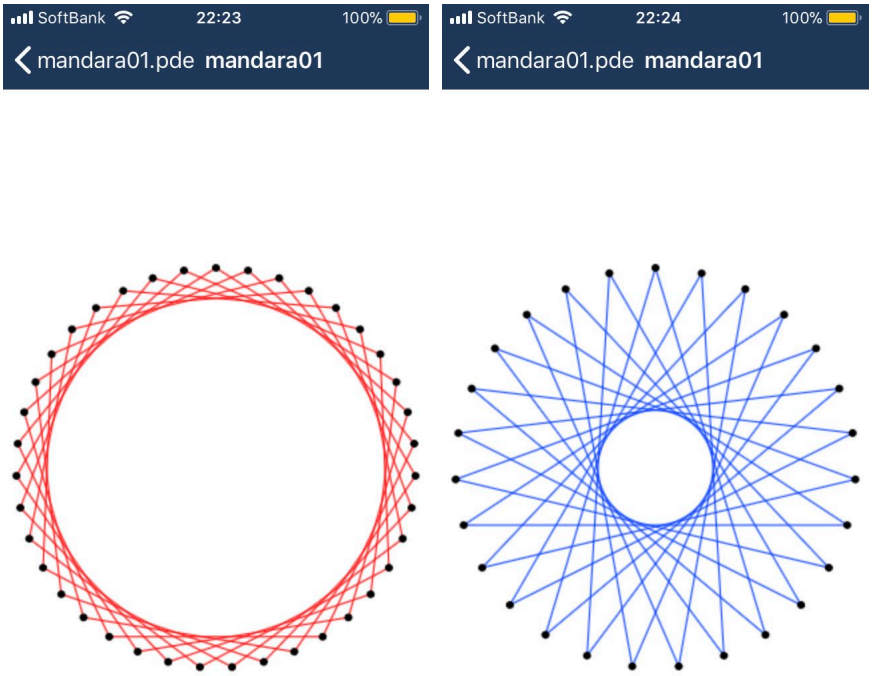


図 4：iPhone 上での「糸かけ曼荼羅シミュレーション」

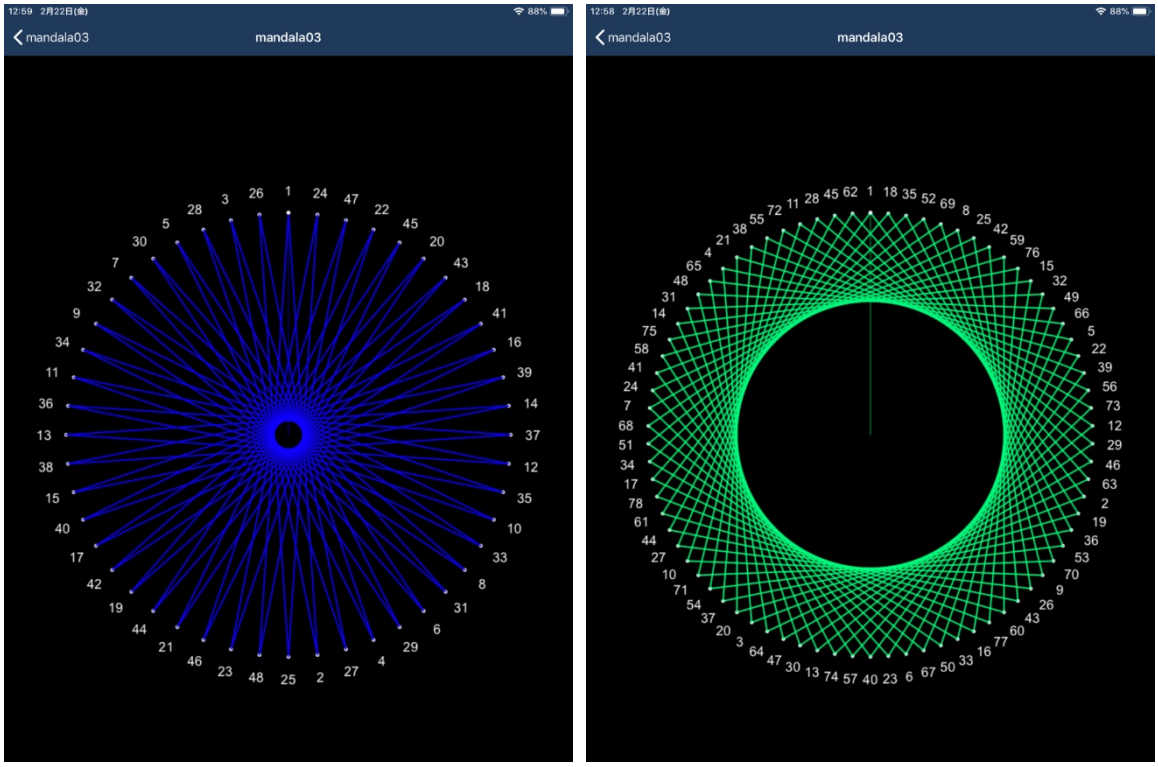


図 5：iPad 上での「糸かけ曼荼羅シミュレーション」

図 5 では，糸をかける順番をその数値で円周上に示してある。これで，一本の糸をどのような間隔で，そしてどのような順番でピンにかけていくかが把握できるようになる。糸かけ曼荼羅の作業の場面においては，この図示で十分なものといえる。プログラミング上の数値を意図したものに書き換え，その都度実行することによって必要な図が描かれるのである。

次に筆者は，複数の色の糸を異なる間隔でかけていった場合のシミュレーションを「ランダムトライアングルズ」の場合と同様に，ある程度ランダムな設定にして思いがけないものを提示する方向で別途作り上げた。これはラインアートとしての表現を目指したものであり，すでに実際の糸かけ曼荼羅を行うための前準備ではなく，ベーシック・デザインの領域で捉えることができる。図６がその一例である。ここには７本の糸がかけられている様が示されている。

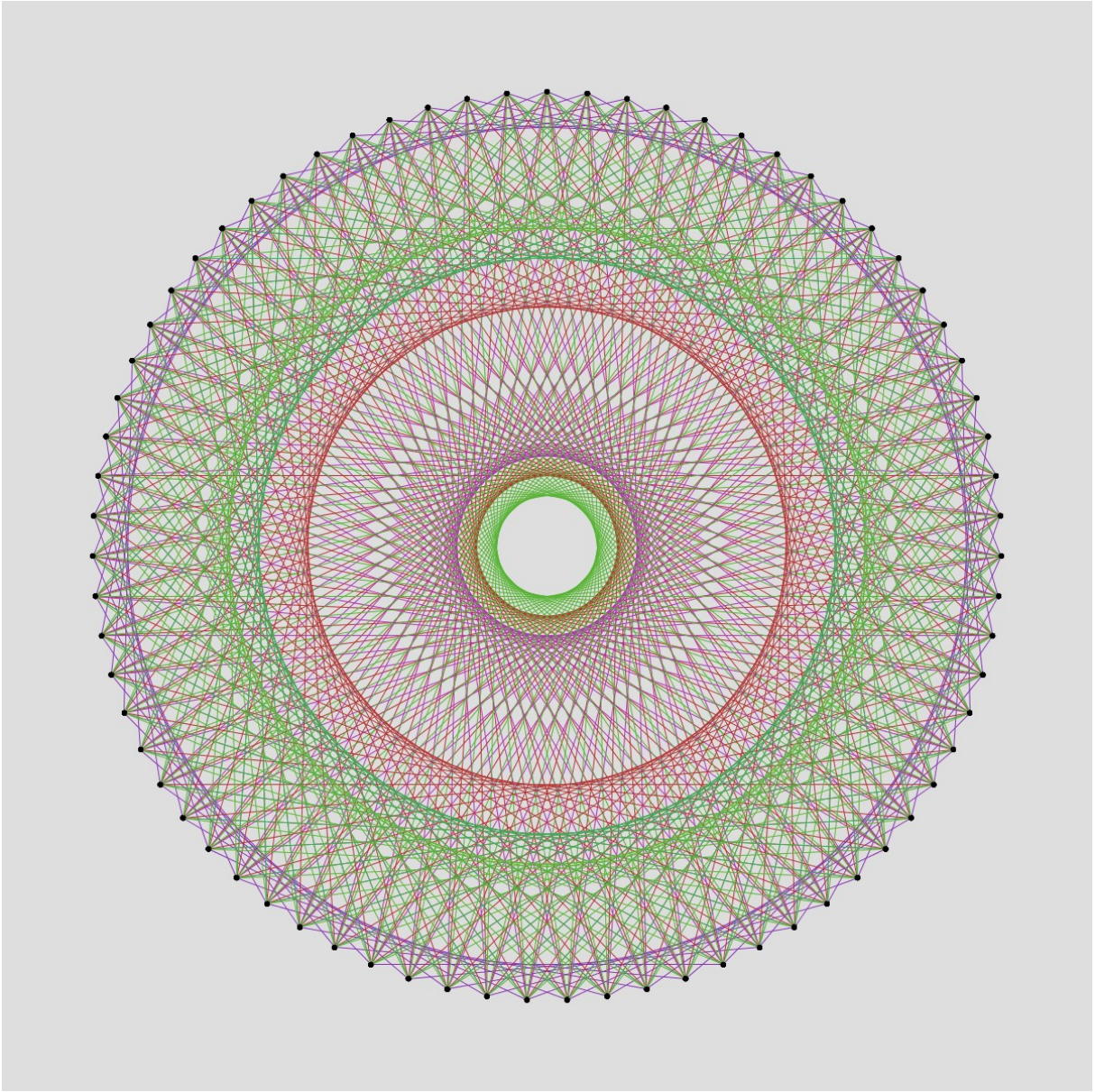


図６：ランダム設定した「糸かけ曼荼羅シミュレーション」の事例

この事例では，糸の本数（7 本）はあらかじめ指定しているが，糸の色，ピンの数，何本目のピンに順次かけていくかについてはある範囲に限定したランダム設定となっている。これはやはり，美的感性に従って設定することになる。そして，このようなプログラミングよって，実行する度に次々と，（このプログラミングでは１秒に１回）留まることなく新たな表現の可能性が示されることになる。結果として，図７のように一つのプログラミングから多様な結果が得られるようになるのである。ここでも，プログラミングが描き出すものを筆者が保存するか，しないかを判断している。（スペースキーで画像保存する設定としている。）

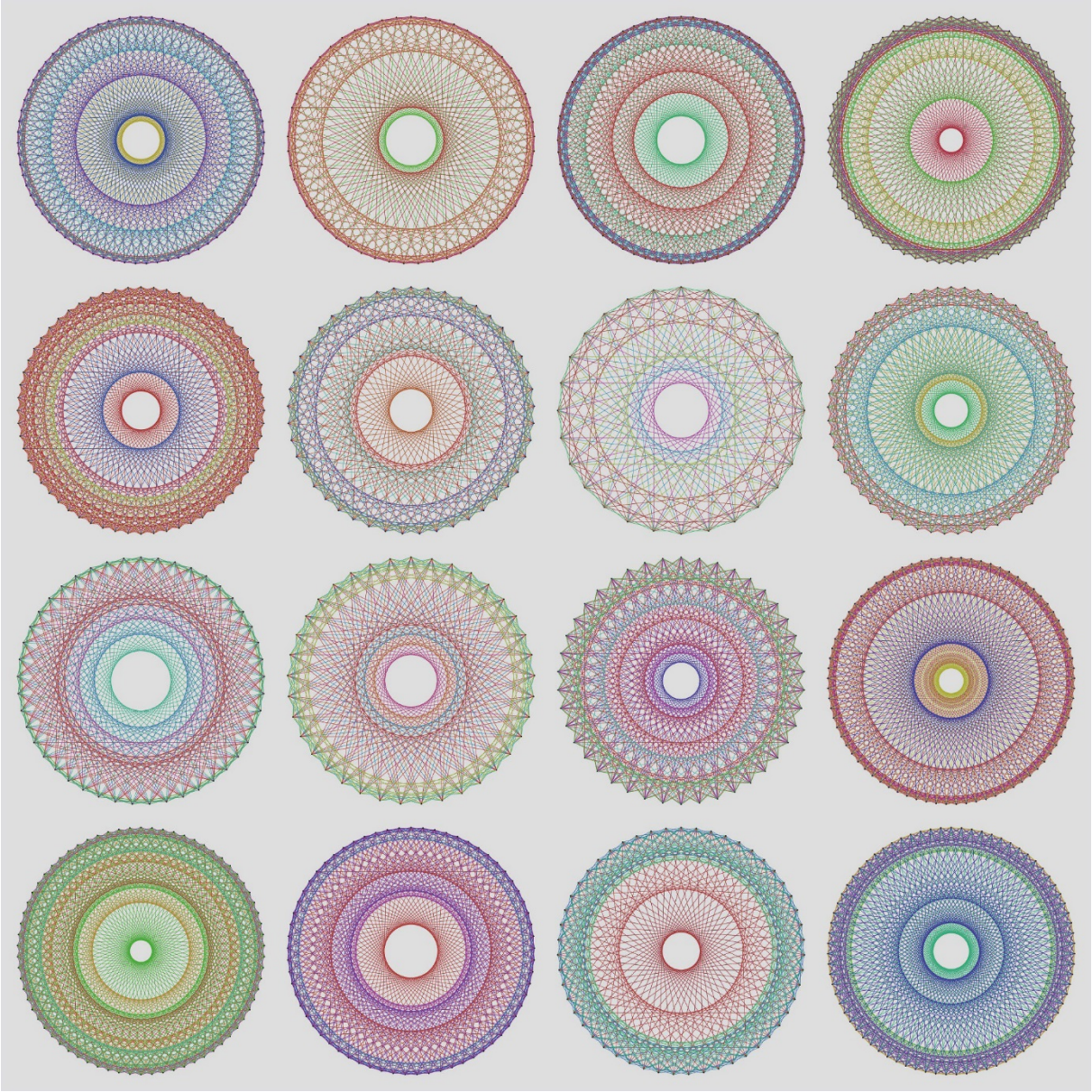


図 7：ランダム設定した「糸かけ曼荼羅シミュレーション」の多様な事例

今回は，プログラミングによるビジュアル表現に留まらず，テキスタイルデザインや手芸の糸かけ曼荼羅の事例のようにイメージ（画像）だけでなく実体のあるモノへという流れを示したかったのであるが，ここでは糸かけ曼荼羅シミュレーションの後，再びビジュアル表現の事例となってしまった。しかしながら今後は，イメージを実体化するためにレーザー加工機でアクリル板などをカットして成型する方向での展開を考えている。

【参考サイト】

・Processing 公式サイト：https://processing.org/
・オリジナルファブリック・マーケット「HappyFabric」：https://happyfabric.me/
・日本糸曼荼羅協会：https://www.itomandala.com

【活動報告】

2018 年度ネットワーク連絡会報告

情報基盤センター
川村　暁，中西貴裕

1. はじめに

2017 年度以前と同様，年度内に 2 回開催した。

2. ネットワーク連絡会 2018 Summer

富士大学で開催した。スポーツと ICT ～スポーツで地域を元気に～というテーマで開催した。

日時　平成 30 年 8 月 31 日(金) 13:30～17:20 (受付開始 13:00)

会場　富士大学 5 号館 4 階 541 講義室

テーマ　スポーツと ICT ～スポーツで地域を元気に～

主催　ネットワーク連絡会、 富士大学、 富士大学スポーツ振興アカデミー、 東北学術研究インターネットコミュニティ(TOPIC)、 TOPIC 盛岡 NOC、 岩手大学情報基盤センター

プログラム

13:00 受付開始

13:30 開会

開催校挨拶

富士大学 副学長　中村 良則 氏

13:35-13:55 講演 1　「新しいスポーツの価値を地域と共に創る」

講師

富士大学スポーツ振興アカデミー 副アカデミー長　内城 寛子 氏

13:55-14:55 講演 2　「競技スポーツにおけるデータ活用 」

講師

筑波大学体育系 准教授　河合 季信 氏

(アルベールビルオリンピック銅メダリスト:男子ショートトラック 5000m リレー)

休憩(15 分)

15:10-15:55 講演 3　「縄跳びセンシングを通した運動における多様性と美しさの発見」

講師

株式会社富士通総研 経済研究所 シニアエキスパート　内島 誠 氏

休憩(15 分)

16:10-16:55 講演 4　「ラグビーワールドカップ 2019 と釜石ラグビー ～新たな出会い、感動、絆～」

講師

釜石シーウェイブス ゼネラルマネージャー兼監督　桜庭 吉彦 氏

16:55-17:20 学内見学（富士大学スポーツセンター）

17:20 閉会

17:35 情報交換会バス出発

18:00-20:00 情報交換会

会場：マルカンビル大食堂

同時開催　TOPIC 盛岡 NOC の会 12:00-13:00 会場：富士大学 5 号館 4 階「ゼミ 12」室

参加者：４２名

3. ネットワーク連絡会 2019 Winter

岩手大学図書館で実施した。

日時　平成 31 年 2 月 15 日(金) 14:00～17:30 (受付開始 13:30)

会場　岩手大学図書館 2F 生涯学習・多目的学習室

テーマ　クラウドサービスをもう一度考える

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

プログラム

13:30 受付開始

14:00 開会

14:00-14:05 ご挨拶

14:05-14:45 講演 1　「Microsoft 365 Education が提供するクラウドサービス
～セキュリティ対策とあわせて～」

講師　日本マイクロソフト株式会社 Microsoft 365 ビジネス本部製品マーケティング部エグゼクティブプロダクトマネージャ兼文教担当部長 春日井 良隆 氏

14:45-15:25 講演 2　「クラウドストレージサービスの利便性と安全性 ～ ｂｏｘ～」

講師　伊藤忠テクノソリューションズ株式会社
情報通信事業企画室クラウドサービス営業部 覚張 正也 氏 氏

休憩(20 分)

15:45-16:25 講演 3　「企業や大学に求められる EDR の必要性と有効性について 」

講師　トレンドマイクロ株式会社ビジネスマーケティング本部エンタープライズソリューション部シニアプロダクトマーケティングマネージャー 釜池 聡太 氏

16:25-17:05 講演 4　「「インターネット上の WHOIS に関する最新動向」

講師　一般社団法人日本ネットワークインフォメーションセンター
IP 事業部課長 川端 宏生 氏，技術部課長 岡田 雅之 氏 氏

17:05-17:25 会場参加型意見交換会

岩手大学情報基盤センター 川村 暁、中西 貴裕

17:30 閉会

18:00-19:30 情報交換会

同時に開催する会合: 盛岡 NOC の会 13:00 開始

参加者：２８名

次ページから，クリッカーを用いた会場参加型意見交換会の結果を示す。なお，一部の問いで回答を集計できていない。

ネットワーク連絡会のこれから
2019 Winter Ver.

岩手大学情報基盤センター
川村 暁, 中西 貴裕

会場参加型の試み（2016から）

- ネットワーク連絡会2016 Spring
  - 会場参加型の試み
  - 参加されている方々の総体をクリアにしたい
- 盛岡NOCでの計測結果として、TOPICで集計結果を発表

今回もクリッカーを使って

- クリッカーを用いる利点
  - 会場参加型
  - 集計結果が瞬時に可視化される

クリッカーとは

学生がテレビリモコンのようなカード端末（レスポンスカード）のボタンを押すと、回答結果が集計されてリアルタイムにパソコンの画面上に表示されるというシステムです。
海外では大学における大人数の講義などにおいて一般的に活用されているようです。

クリッカー - プロジェクト4 ICT活用プロジェクト - 学生の学びを中心に据えた教職員ネットワークの構築とFDの組織化（平成21年度 文部科学省 特別教育研究）より

説明より、まず使ってみる

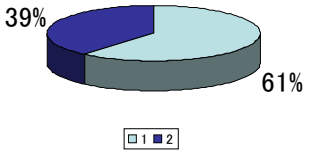
該当する番号を押してください
　次スライド

質問 クリッカーについて

1. 知っていた
2. 知らなかった

問１　クリッカーについて

1. 知っていた
2. 知らなかった



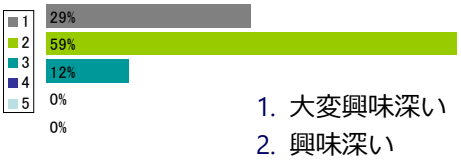
問２　年齢は？

1. １０代
2. ２０代
3. ３０代
4. ４０代
5. ５０代
6. ６０代
7. ７０代
8. ８０代
9. ９０代

本問いの回答が得られなかった

ネットワーク連絡会 6

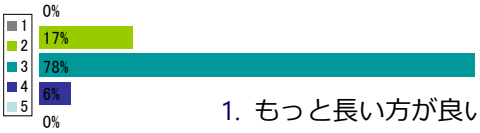
問３　今回のネットワーク連絡会は



1. 大変興味深い
2. 興味深い
3. ふつう（丁度良い）
4. 物足りない
5. 非常に物足りない

ネットワーク連絡会 7

問４　今回の講演時間は

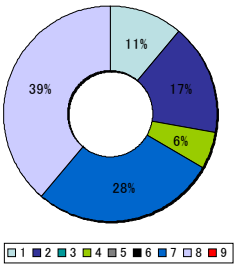


1. もっと長い方が良い
2. 多少長い方がよい
3. ちょうどよい（適切）
4. 少し短い方がよい
5. 短い方がよい

ネットワーク連絡会 8

問５
今後取り上げてほしいテーマは

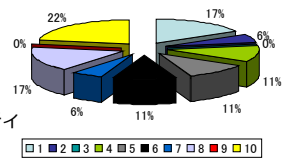
1. ネットワーク
2. セキュリティ
3. 大規模計算機
4. 大規模ストレージ
5. パソコン
6. 新しいストレージ（MRAM, SSD, etc）
7. 情報技術の活用
8. ユーザ教育
9. 情報経営



ネットワーク連絡会 9

問６　ネットワーク関連で今後とりあげてほしいことは

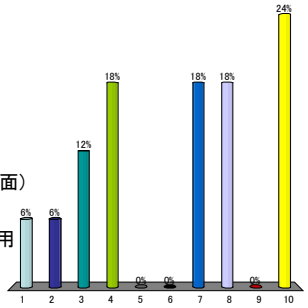
1. SDN
2. 基幹ルータ，大規模ルータ
3. 幹線系，支線系スイッチ
4. 次世代FW
5. セキュアなネットワーク
6. エンドポイントセキュリティ
7. イーサネットの最新技術
8. 無線LAN構築法
9. VPN，IPSec
10. IoT



ネットワーク連絡会 10

問７　聞いてみたい要素技術，事項は？

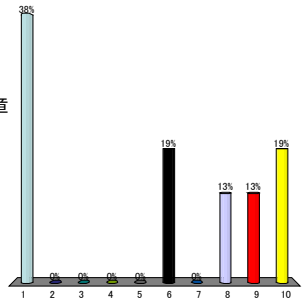
1. クラウド(電子メール等)
2. 電子証明書の活用
3. 認証(多要素認証)
4. 仮想化技術
5. 暗号技術
6. SSL，EV-SSL(技術，運用面)
7. CSIRT
8. セキュリティポリシーとその運用
9. フォレンジック
10. 学認、eduroam



ネットワーク連絡会 11

問８　今貴社・貴組織で問題になっていることは？

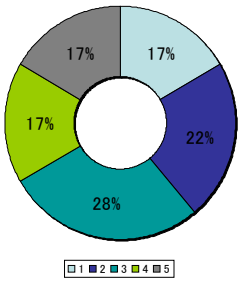
1. 技術継承
2. 日経某に弱い人がいる
3. 金曜日の17時
4. FAXで送られてくる文章
5. 一律の経費節減
6. 年齢構成の不均衡
7. 正規と非正規
8. 気合いと根性
9. 多様性と変化の仕方・させ方
10. コンプライアンス



問９，１０　BYOD

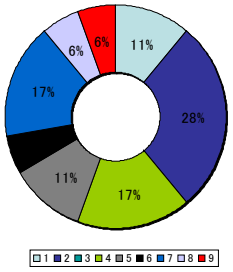
- BYOD (Bring your own device) についてお尋ねします.

問９　今後貴社・貴組織では，BYODを積極的に活用していく予定はありますか？



問１０　BYODを進める上で，障害となると考えていることは？

1. 公と私の区別はつけるのが難しい（区別が曖昧になる）
2. セキュリティリスクを取り除くのが難しい
3. 社内システムの更改が必要
4. ユーザ教育が難しい・新規施策が必要
5. OSや端末により動作に差異がある
6. 新規システム・施策を担う人材が不足している
7. 経営層の理解が不足している
8. ライセンス管理（資産管理）上の困難
9. 特になし



問１１　入門的な講演

問１１　入門的な講演を一つ程度は入れるべきですか？（新人さん等を連れてくる動機として）

1. 進めるべき（一つ程度入門的なものが必要）
2. いまのままでよい
3. 入れる必要は無い（入れることに反対）

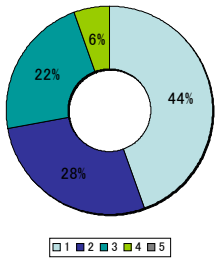
問12, 13　標的型メール

- 標的型メールについてお伺いします。

ネットワーク連絡会 18

問１２　標的型メールの被害に遭ったことはありますか？（組織）

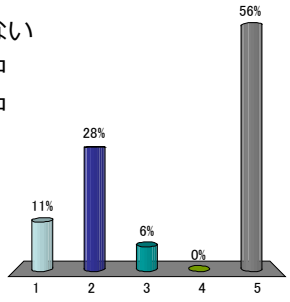
1. ない
2. ある（個人レベル）
3. ある（一部業務に支障）
4. ある（全社的に影響あり）
5. ある（全業務停止）



ネットワーク連絡会 19

問１３　標的型メール訓練を実施していますか？

1. 実施する予定はない
2. 可否を含め検討中
3. 実施に向け検討中
4. 実施する（確定）
5. 実施済み



ネットワーク連絡会 20

ありがとうございました！

- これで終わります
- 今後も、本会を皆様とともに作り上げていきたいと考えております

ネットワーク連絡会 21

平成 30 年度情報技術部活動報告

情報技術部情報技術室

1. はじめに

情報技術部は、現在情報基盤センター内に拠点を置き、主として情報基盤センターの業務を遂行している。昨年度には本学の学術系および業務系システムの更新がほぼ終了し、今年度は更新されたシステムの本学に合わせた調整などを中心に管理・運用業務を行っている。加えて、平成 28 年度に結成された CSIRT に関連する業務を遂行しているが、現在はセンター業務の中でも抜きん出て多忙化している。本稿では情報基盤センター業務の中から恒常的なシステムの管理・運用業務を除いて、主に CSIRT の業務を中心にご報告する。

2. CSIRT 業務

昨年度、システム更新に合わせて次世代ファイヤウォールを導入し、本学を出入りする怪しい通信を常時監視できる体制が整った。怪しい通信があると各システムはアラートを発する。アラートを基に発生元や原因の調査、対処等が必要となるが、アラートには誤報も多い。そこで、CSIRT のメンバにより、各システム上でアラートの中からリスク性の高いものを自動選別し、CSIRT 宛へのメールとして送信し、メンバ間での情報の共有ができるようにシステムを改良した。その成果によりアラートに対して迅速に対応できるようになった。CSIRT メンバは 2 人一組とし、週ごとの輪番体制を取り、送信されてきたアラートメールを分析し、さらにリスクの高いと疑われる場合には、発生元である現地に赴くなどして調査を行っている。アラートメールの分析・調査は、CSIRT 業務の約 80%を占めているのではないかと推測する。

2.1. CSIRT 宛メールの分析・調査

システムで発生したアラートの場合は、メールの Subject に定型文が付記されて送られてくる。定型文以外の場合は、本学構成員からの問い合わせや CSIRT からのユーザサポートに関する返信メールが多い。そこでメールの Subject をカテゴリごとに分類することによってどのような業務が多いのか解析してみた。表 1 に CSIRT 宛に送られてくるメールの Subject で分類したカテゴリを記す。このカテゴリごとに、昨年（2018 年）1 月～12 月の間に CSIRT 宛に送られてきたメールを分類し、積み上げ棒グラフにした（図 1）。

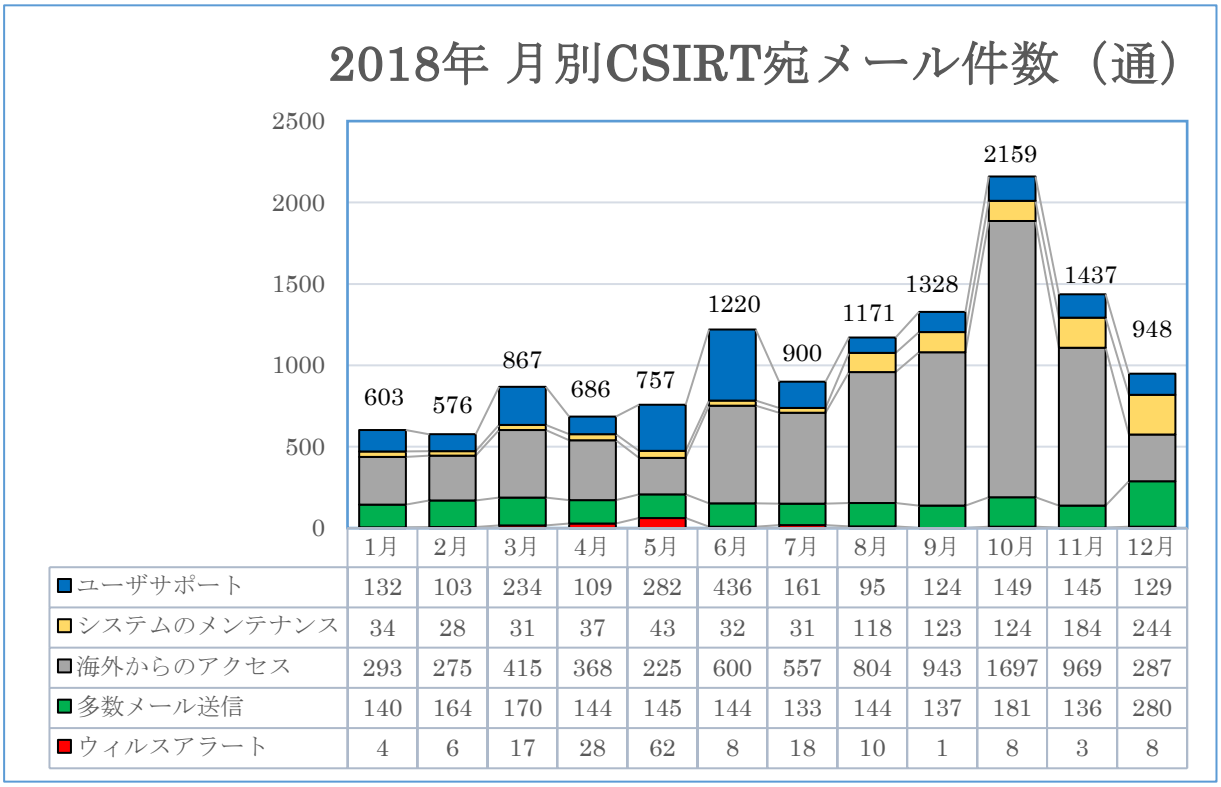
アラートごとに私的に分析した特徴を記す。

- ウィルスアラート
  5 月ごろに多く発生している。新入生や研究室に配属になった学生が、怪しいサイトに接続して発生している場合が多い。
- 多数メール送信アラート
  学会が開催される時期に会員への通知等で多く発生すると予想されたが、予想に反して年間を通して変動が少ない。

- 海外からのアクセスアラート
  意外にも海外からのアクセスアラートが大半を占め、夏休みの 8 月ごろから海外へ渡航する教職員や学生が増加していることが分かった。
- システムのメンテナンスアラート
  8 月頃からシステムアラートが増加しているが、このころからメールに飛ばす項目を増やしたことに起因している。故障が発生しているわけではない。
- ユーザサポート
  6 月にユーザサポートのメールが目立って増加している。この頃、本学において詐欺メールの訓練を行っており、そのメールの問合せが増加したことに起因している。
  今後も怪しいメールが来たら CSIRT へご一報願いたい。

表 1　CSIRT 宛メールの Subject 分類表

Subject の分類	詳細
ウィルスアラート	もしかしてウィルスをダウンロードした。 あるいはウィルスに罹っているかもしれないアラート
多数メール送信アラート	もしかしてスパムメールを大量に送信しているかもしれないアラート
海外からのアクセスアラート	もしかして海外から攻撃を受けているかもしれないアラート
システムのメンテナンスアラート	もしかしてシステムが故障しているかもしれないアラート
その他（主にユーザサポート）	本学ユーザから、詐欺メールかもしれない問合せ。セキュリティに関する問い合わせ。及びそれらに対する回答等、ユーザサポートに関するメール。



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
ユーザサポート	132	103	234	109	282	436	161	95	124	149	145	129
システムのメンテナンス	34	28	31	37	43	32	31	118	123	124	184	244
海外からのアクセス	293	275	415	368	225	600	557	804	943	1697	969	287
多数メール送信	140	164	170	144	145	144	133	144	137	181	136	280
ウィルスアラート	4	6	17	28	62	8	18	10	1	8	3	8

図 1　CSIRT 宛メールの月別推移のグラフ

2.2. IP アドレス管理システムの開発

本学のグローバル IP アドレスは情報基盤センターから各部局に割り当てている。末端の IP アドレスは各部局で管理しているが、構成員の異動等により複雑化しており詳細までは把握できていないのが現状であった。万が一情報インシデントが発生した場合、早急に当該 IP アドレスの利用者を割り出さなければならないが、現状では時間を費やしていた。末端で使用されている IP アドレスを管理することが情報基盤センターの喫緊の課題であった。そこで、本学構成員自ら Web 上で管理できるシステムを構築した。

システムは、本学の IP アドレス管理手順に従って、情報基盤センターから各部局の IP アドレス部局管理担当者に割り当てる。各部局の管理担当者は、部局内の構成員に管理者または利用者として割り当てる。末端の利用者は、自分が使用している IP アドレス毎に使用機器と使用場所、備考などのメモを付して本システムに登録する。末端の利用者が異動等により本学を離れ、本学の教職員名簿から氏名が削除された場合、上位の管理者に使用中の IP アドレスを返却できる仕組みを取っている。もちろん、本人が異動前に返却することも可能である。また、年に数回、自身が使用している IP アドレスに変更がないかチェックしていただき、適正に管理している旨を CISO に報告する機能も付加してある。

なお、IP アドレス調査システムの詳細は別稿をご覧いただきたい。

3. むすび

学術系、業務系システムの更新が終わり、システムの管理運用業務に加えて CSIRT 業務が増加傾向にある。多様化し、複雑化しつつある CSIRT 業務の中から CSIRT 宛に送られてくるメール処理に特化して業務分析した結果を報告した。年間メールの総合計数は 12,652 通あり、365 日で割ると、1 日当たり 34 通の分析・調査またはユーザサポートを熟していることが分かった。

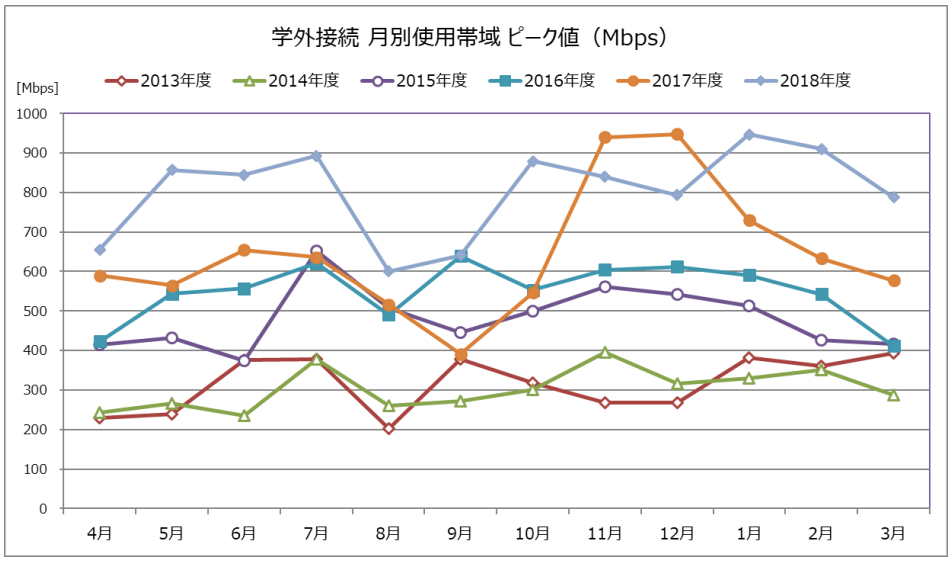
加えて、インシデントが発生した場合の対処として、末端で使用している IP アドレスの情報を管理・運用するためのシステムを開発したことも付記した。

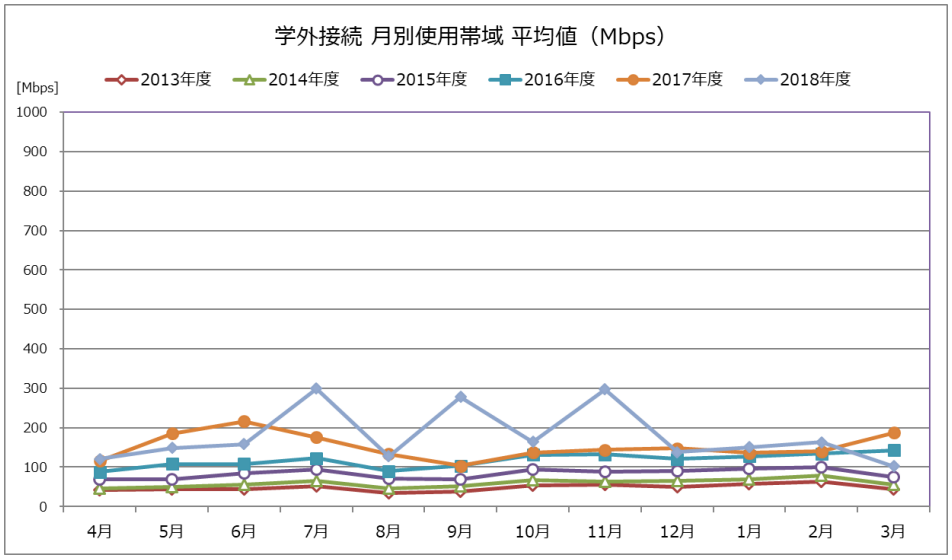
（文責：情報技術室長　栗田宏明）

【運用報告】

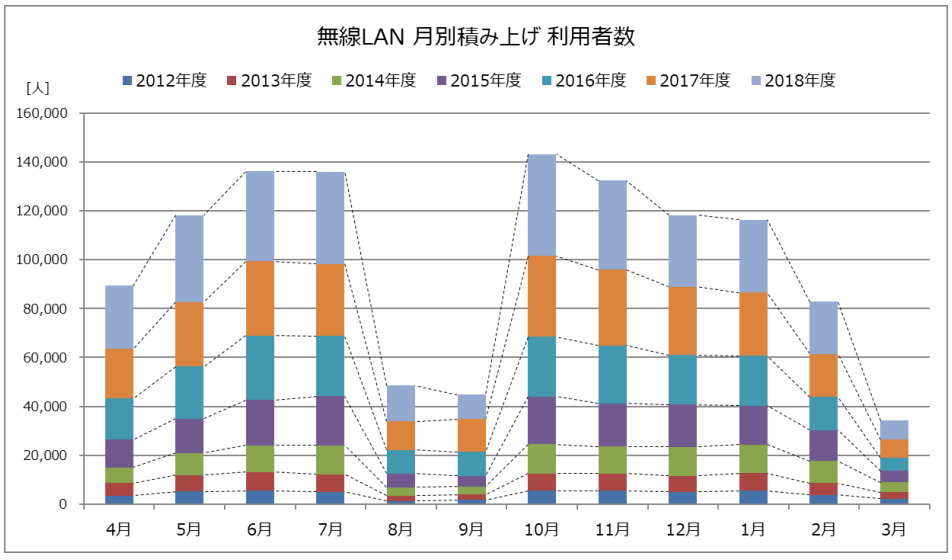
運用報告

[学外接続]

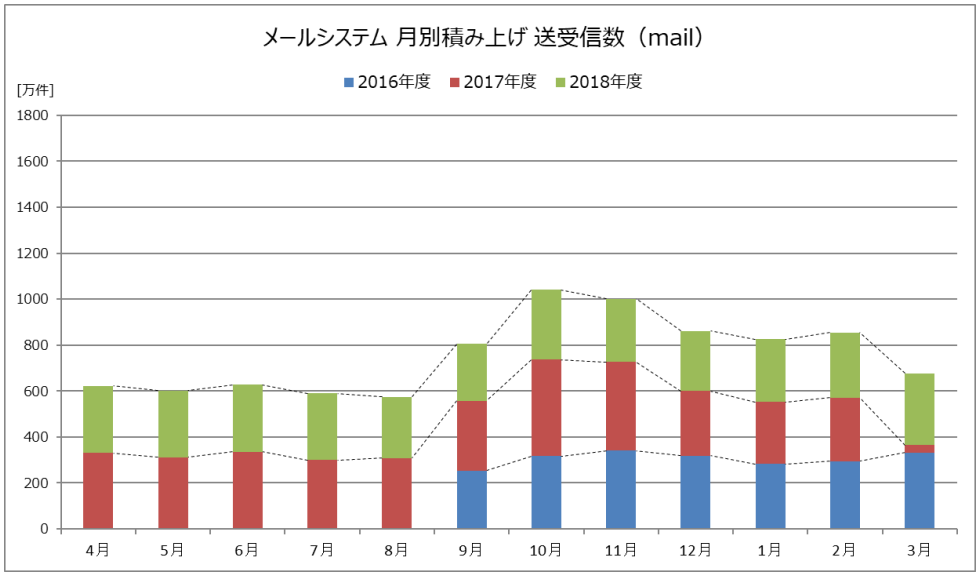


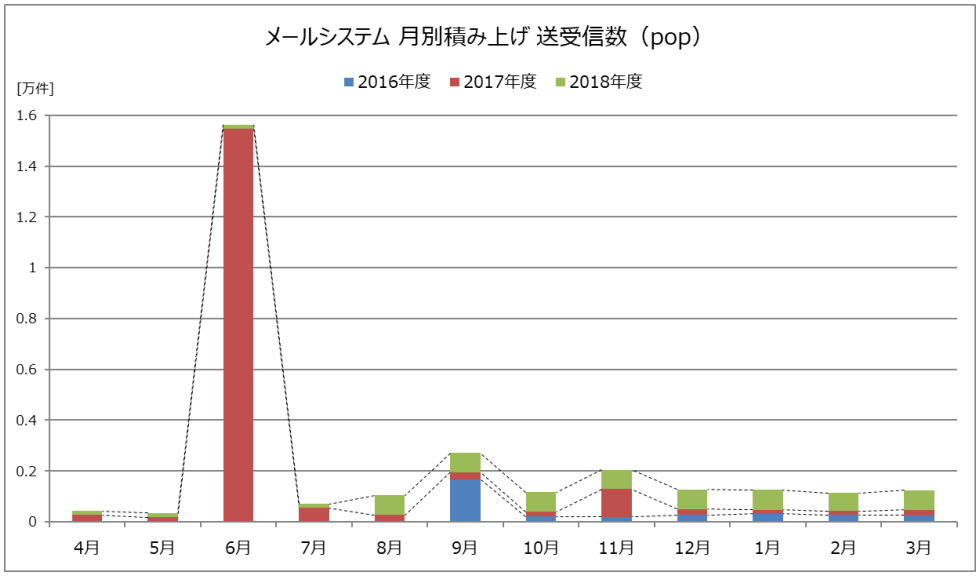


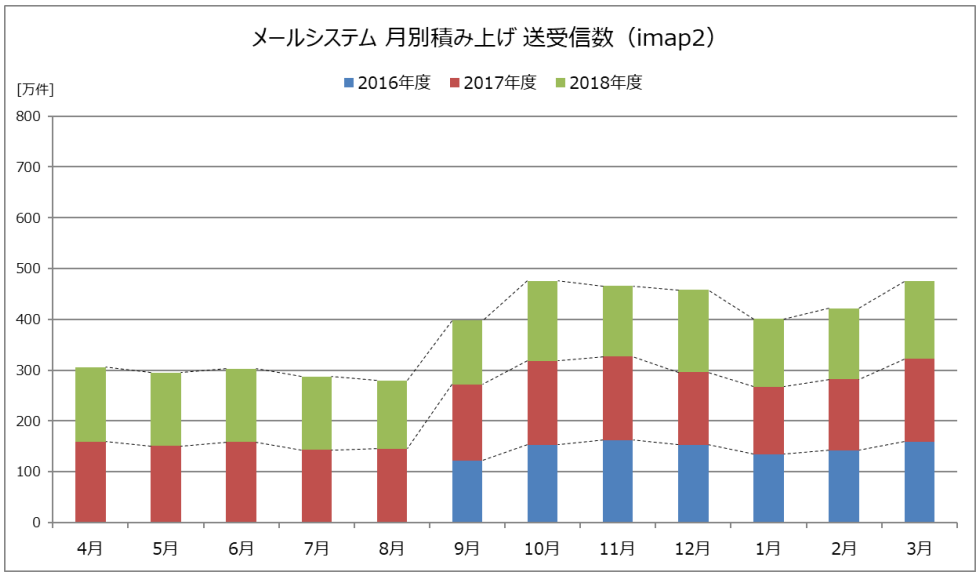
[無線 LAN]



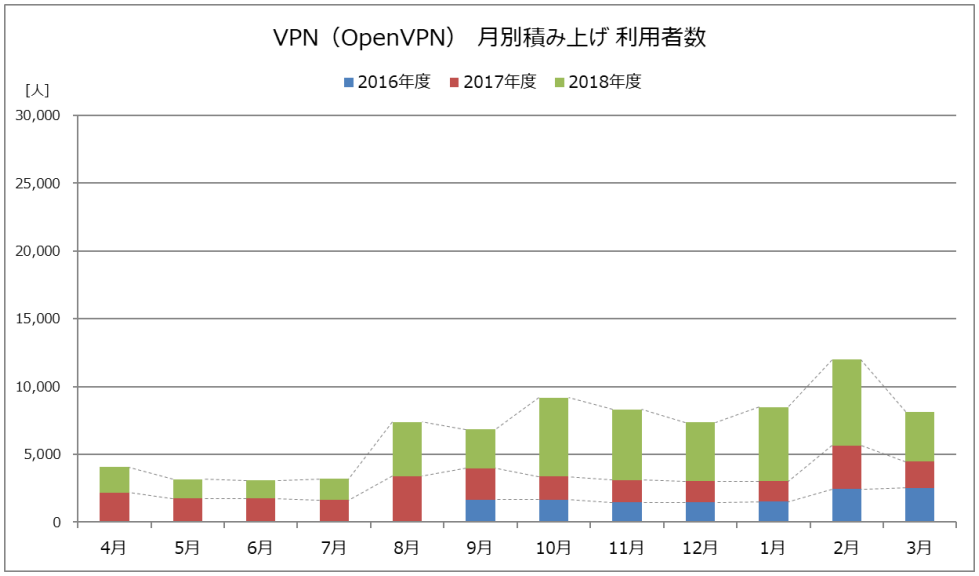
[メールシステム]（2016 年 9 月～2019 年 3 月）

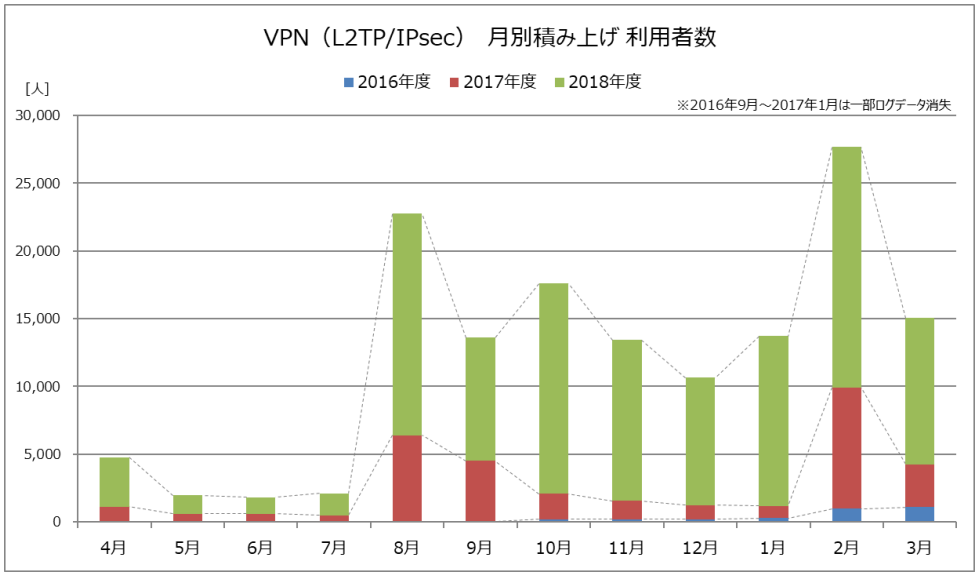


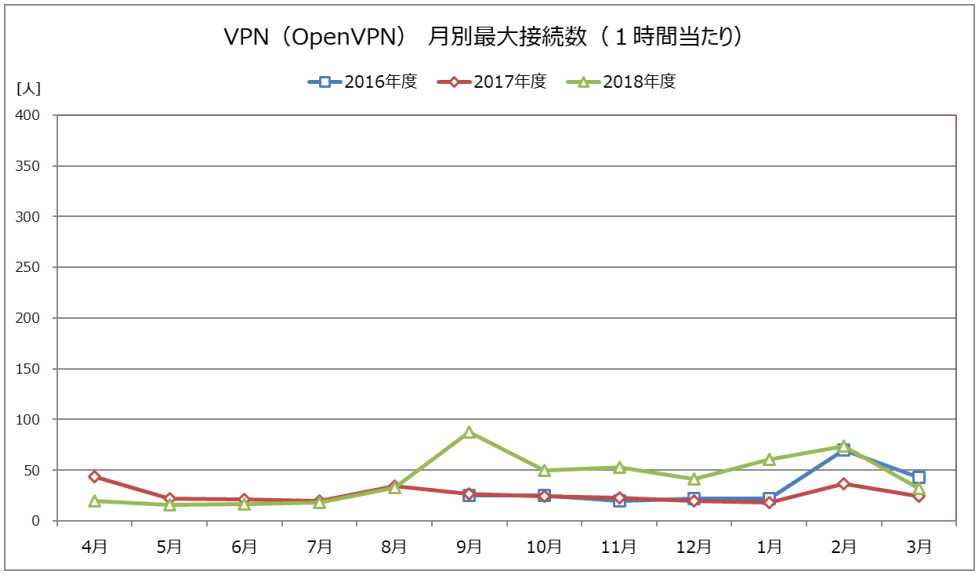


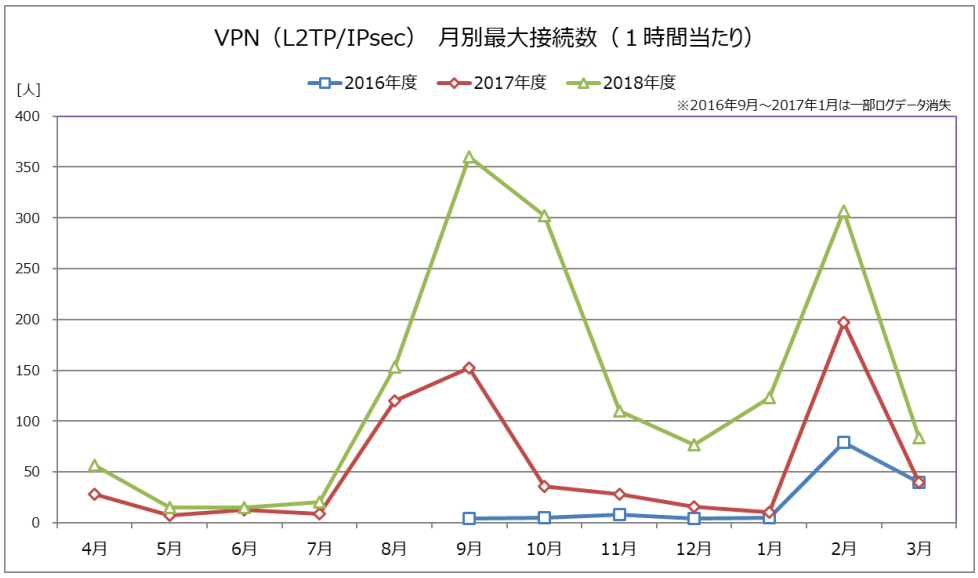


[VPN]（2016 年 9 月～2019 年 3 月）



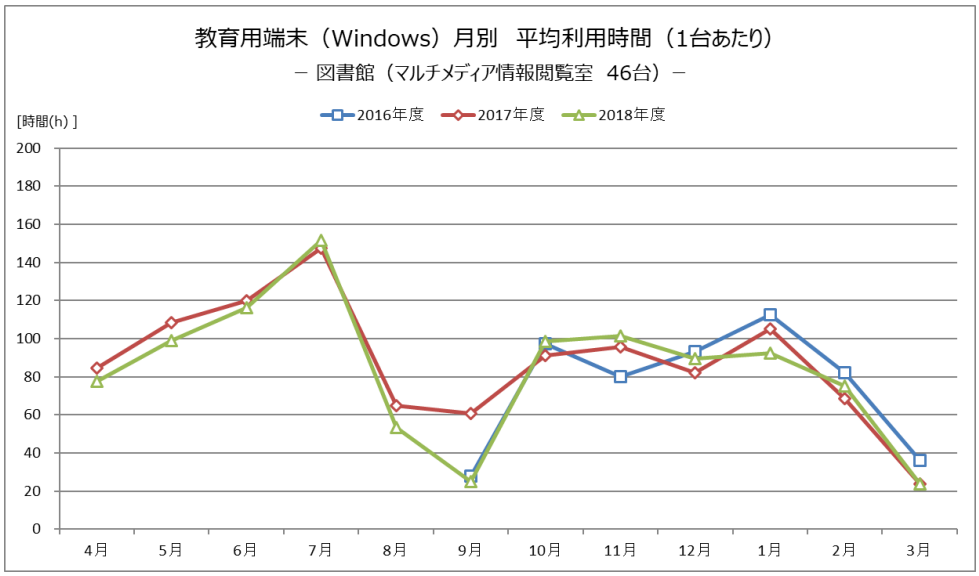


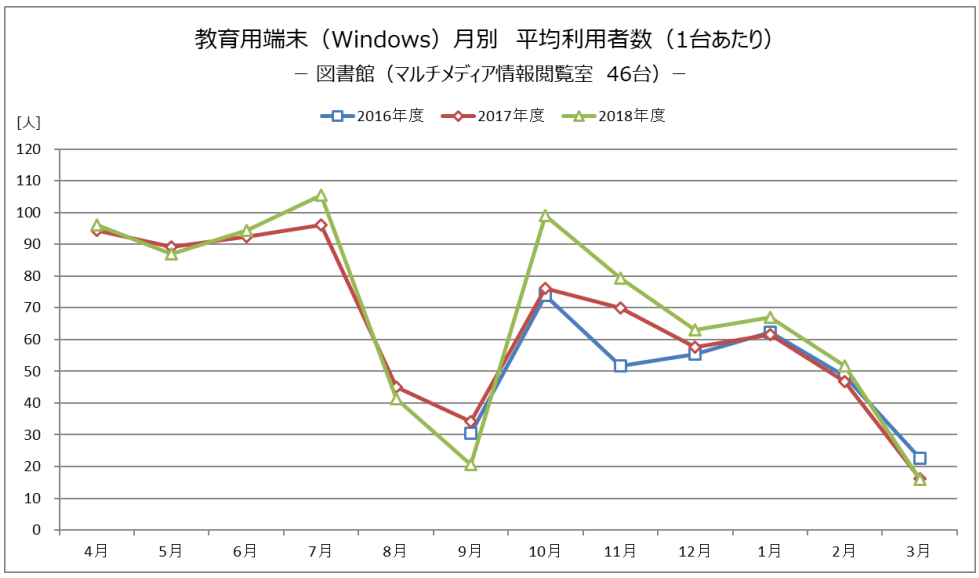




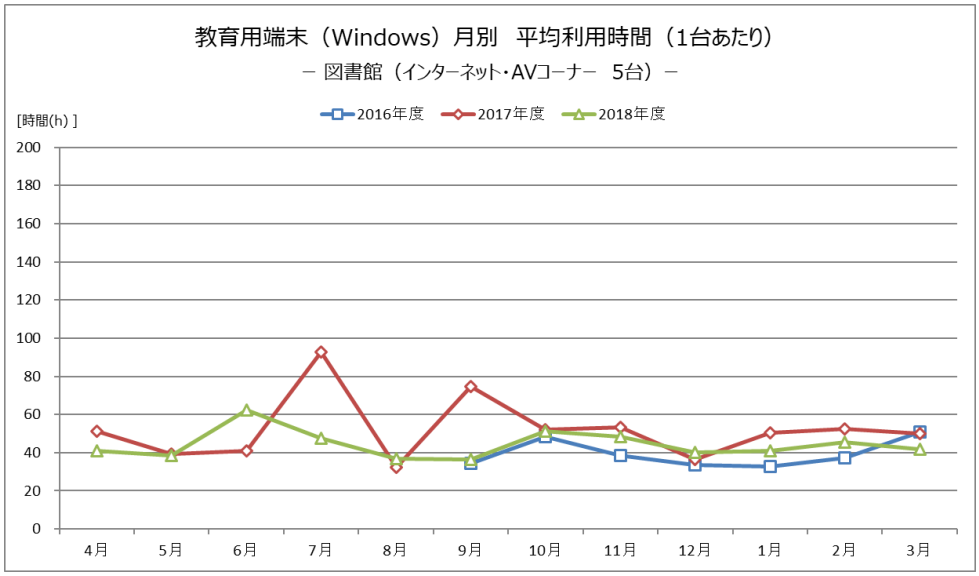
[教育用端末(Windows)]（2016 年 9 月～2019 年 3 月）

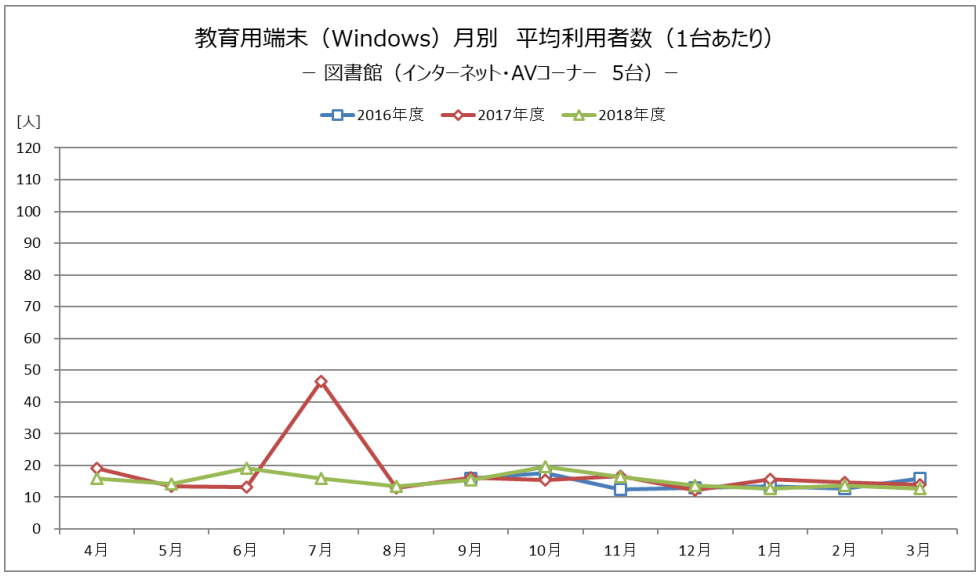
- 図書館（マルチメディア情報閲覧室）



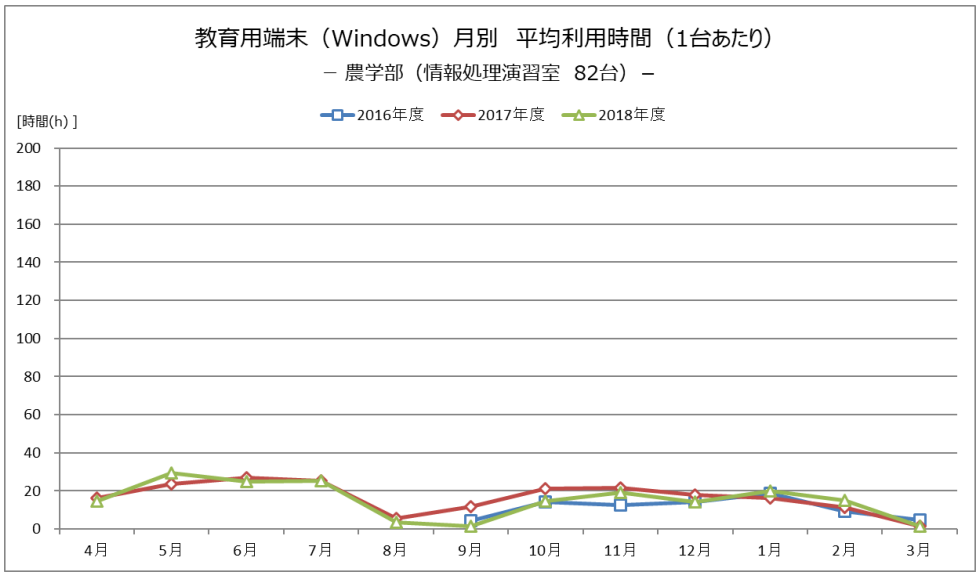


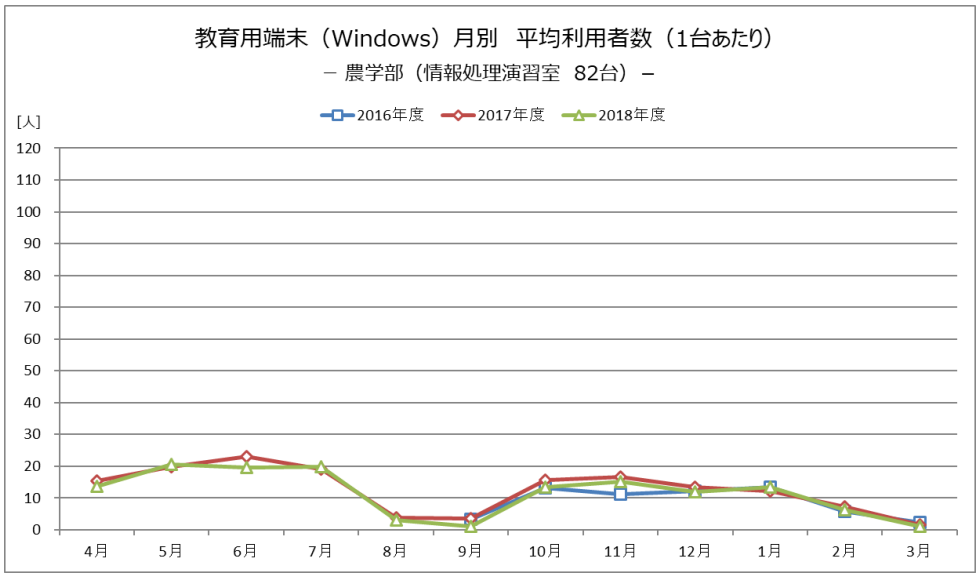
- 図書館（インターネット・AV コーナー）



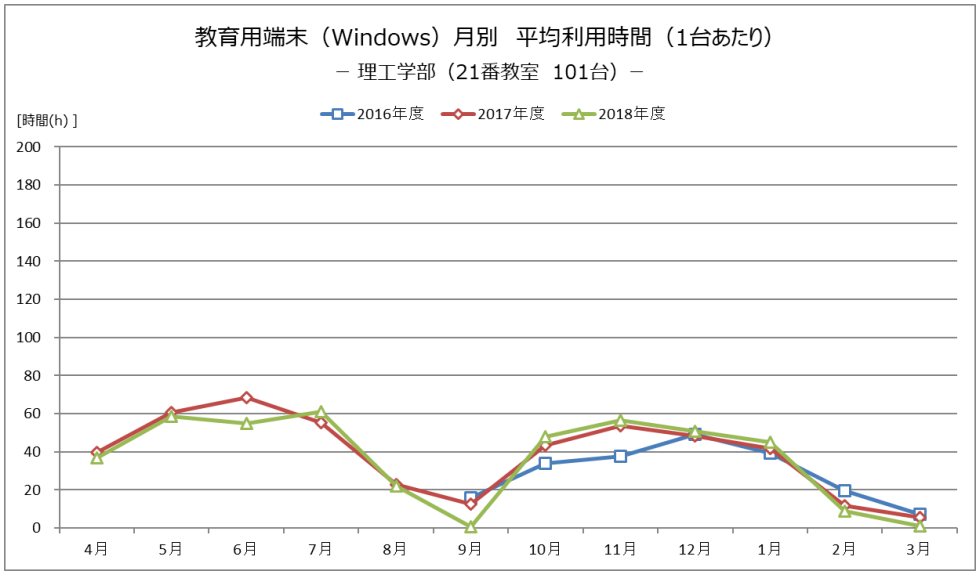


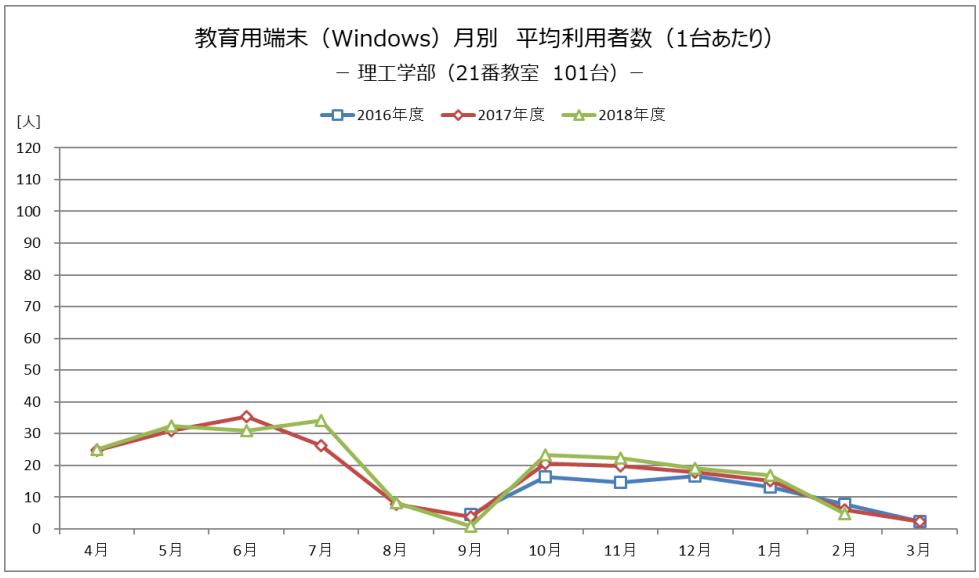
- 農学部（情報処理演習室）



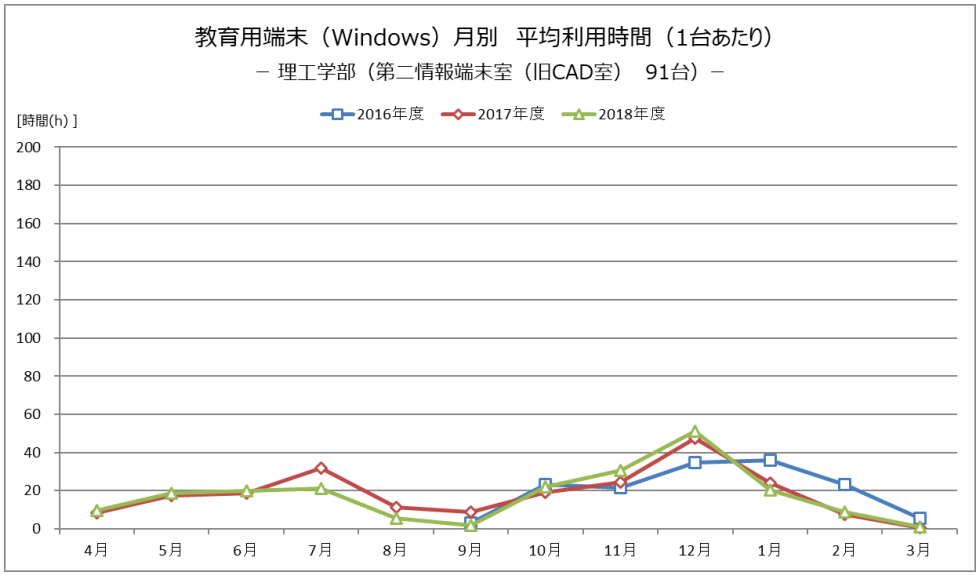

教育用端末（Windows）月別　平均利用者数（1台あたり）
－ 農学部（情報処理演習室　82台）－
2016年度
2017年度
2018年度
[人]
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

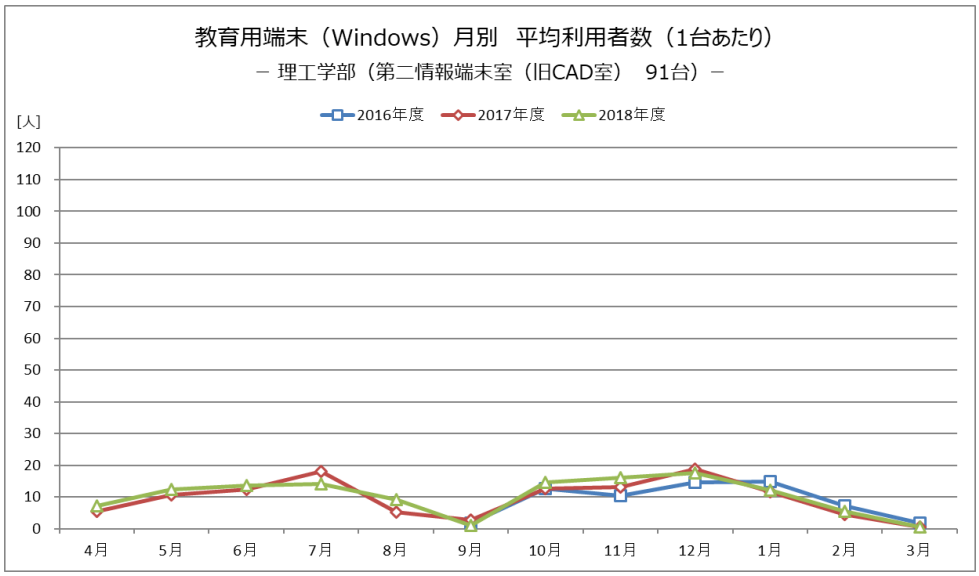
- 理工学部（21 番教室）


教育用端末（Windows）月別　平均利用時間（1台あたり）
－ 理工学部（21番教室　101台）－
2016年度
2017年度
2018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

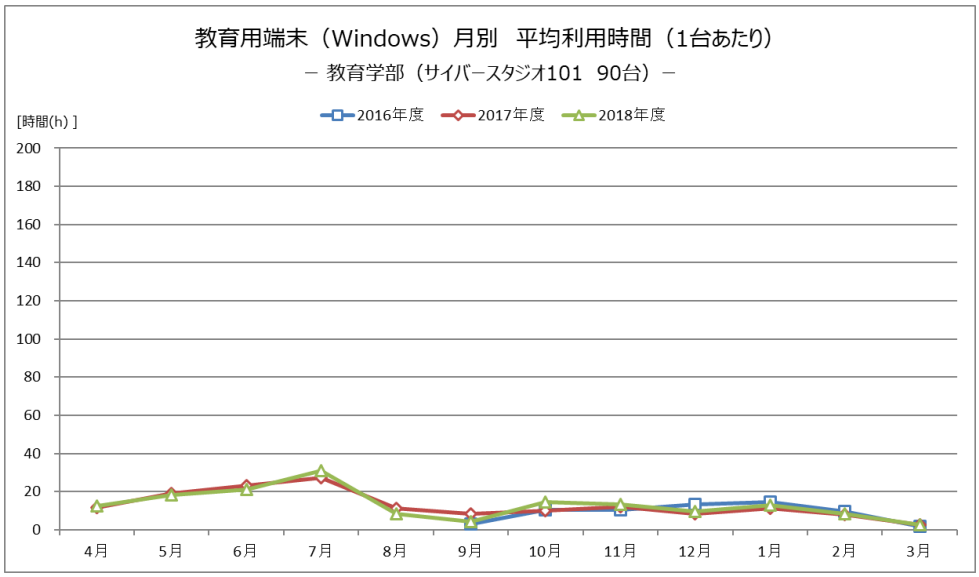

教育用端末（Windows）月別　平均利用者数（1台あたり）
－ 理工学部（21番教室　101台）－
2016年度
2017年度
2018年度
[人]
120
110
100
90
80
70
60
50
40
30
20
10
0
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月

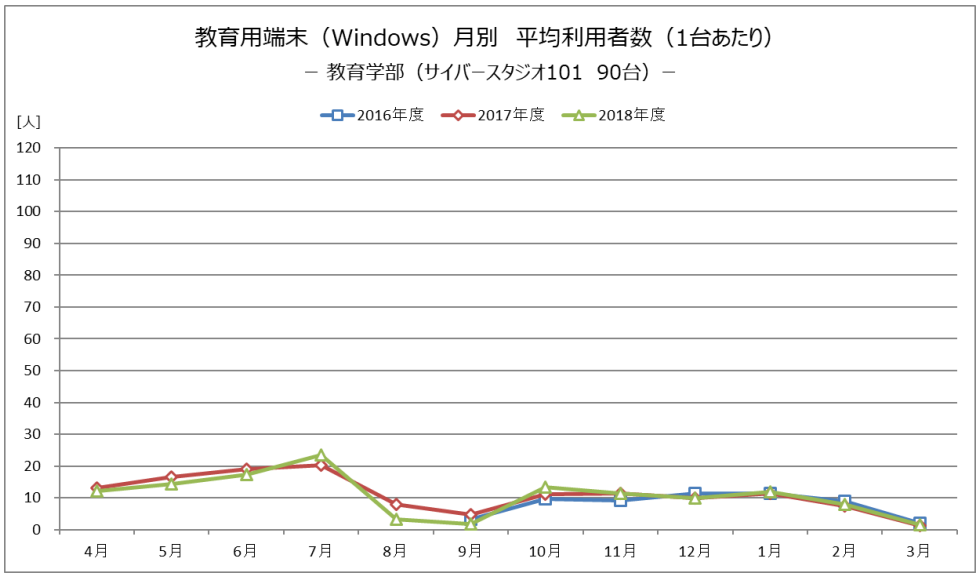
- 理工学部（第二情報端末室（旧 CAD 室））



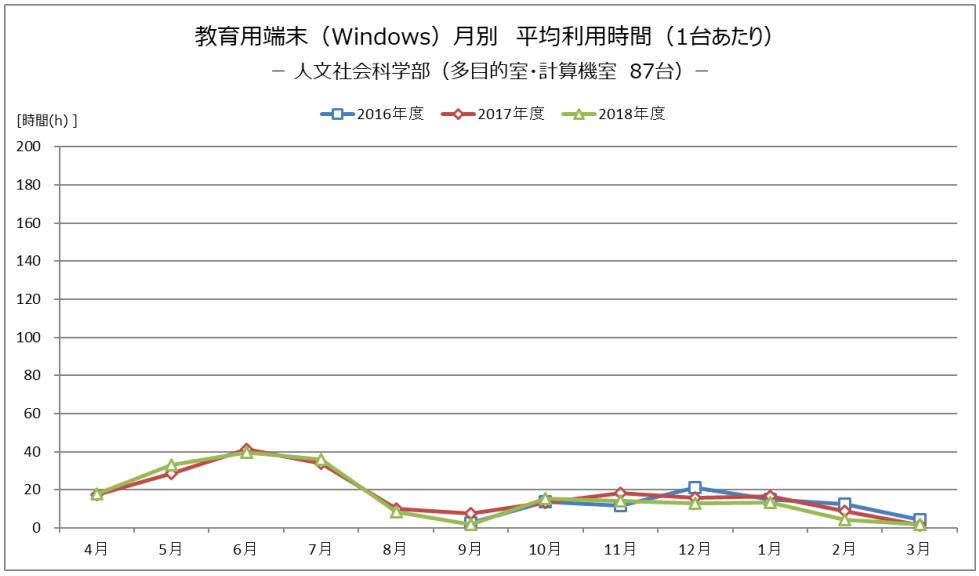


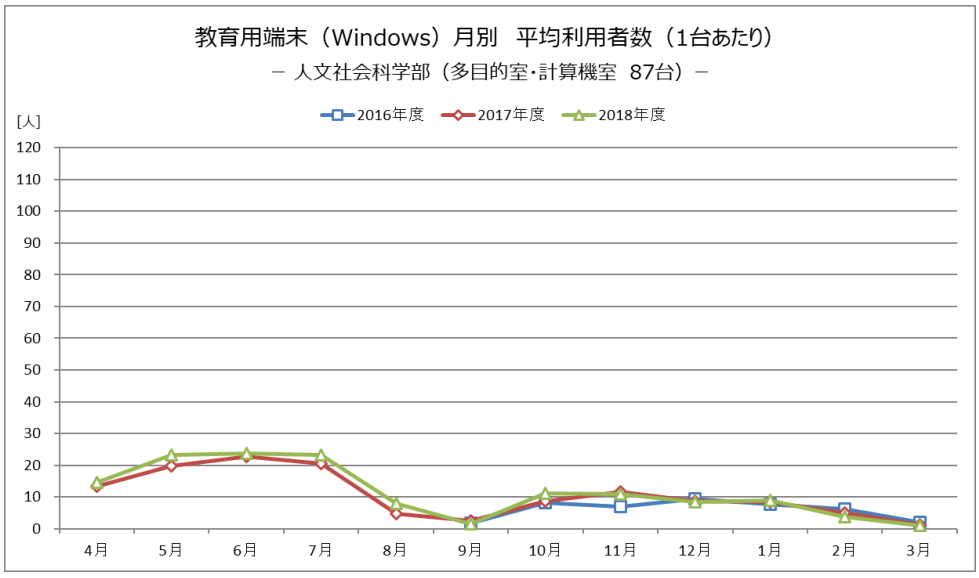
- 教育学部（サイバースタジオ 101）



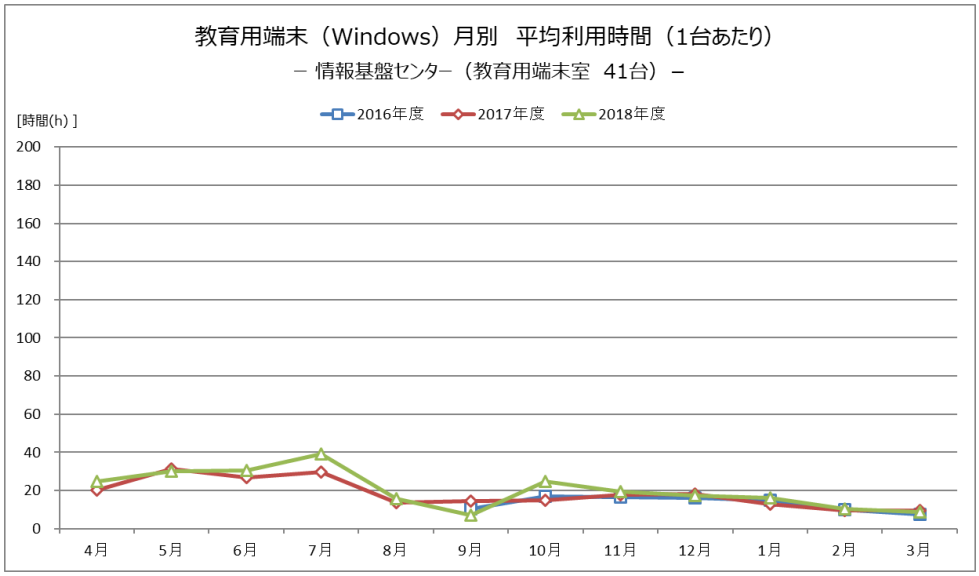


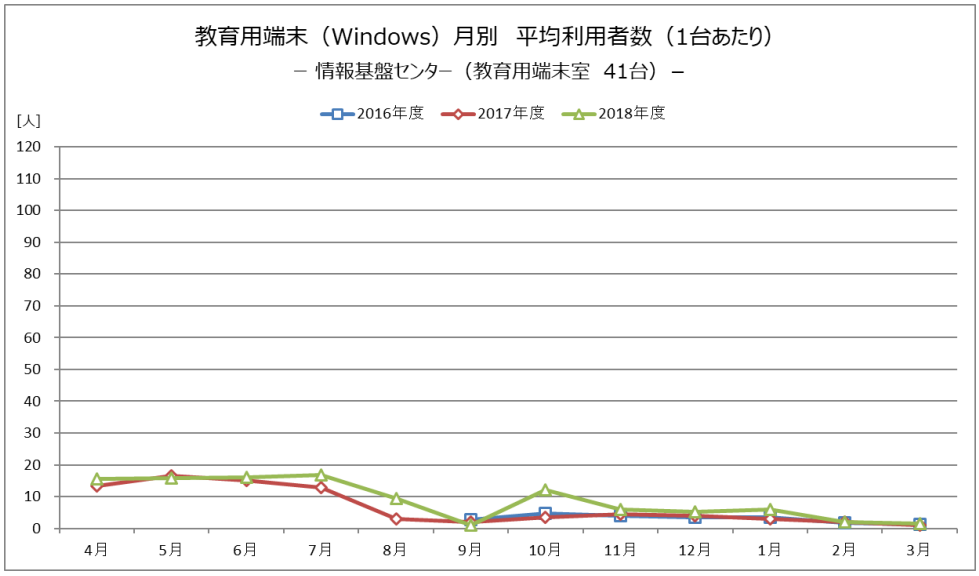
● 人文社会科学部（多目的室・計算機室）



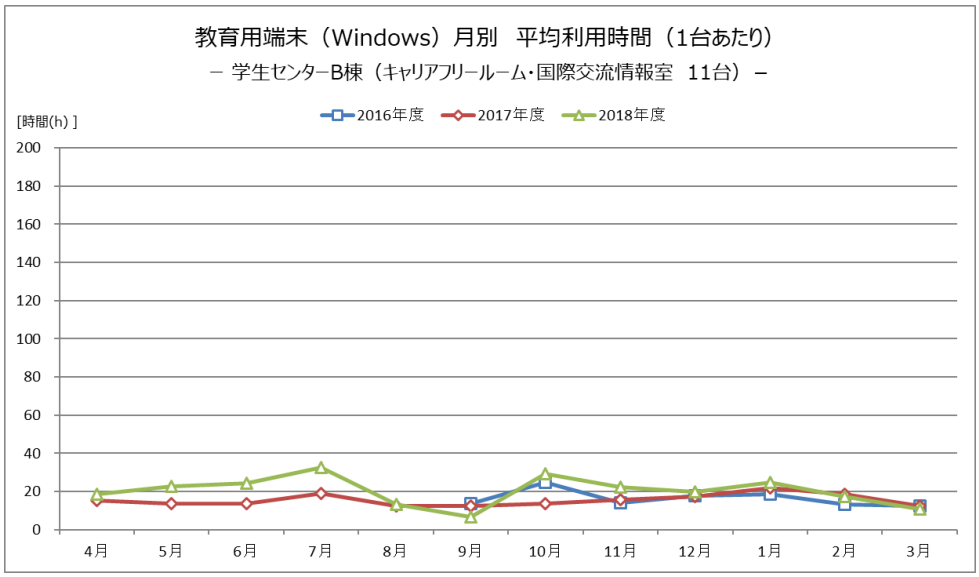


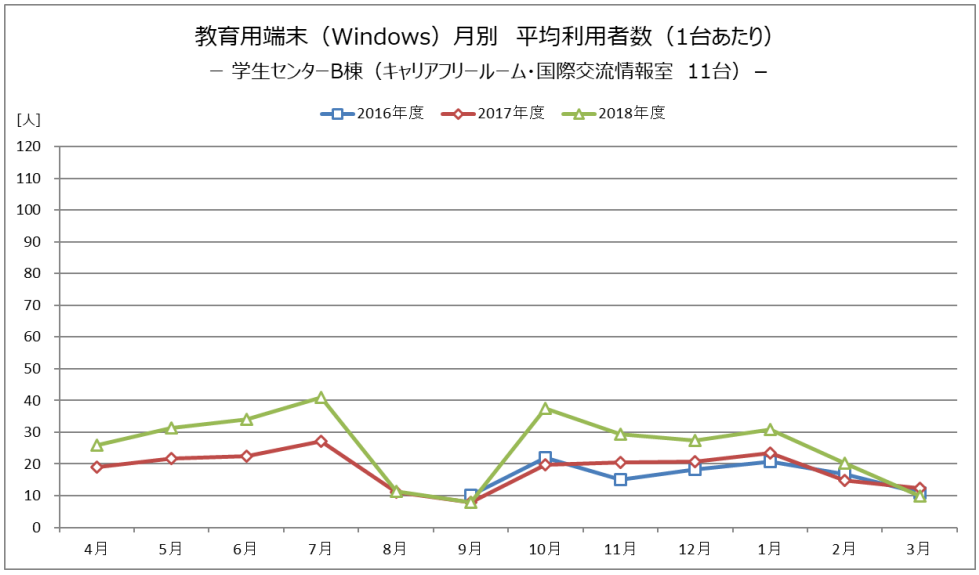
● 情報基盤センター（教育用端末室）





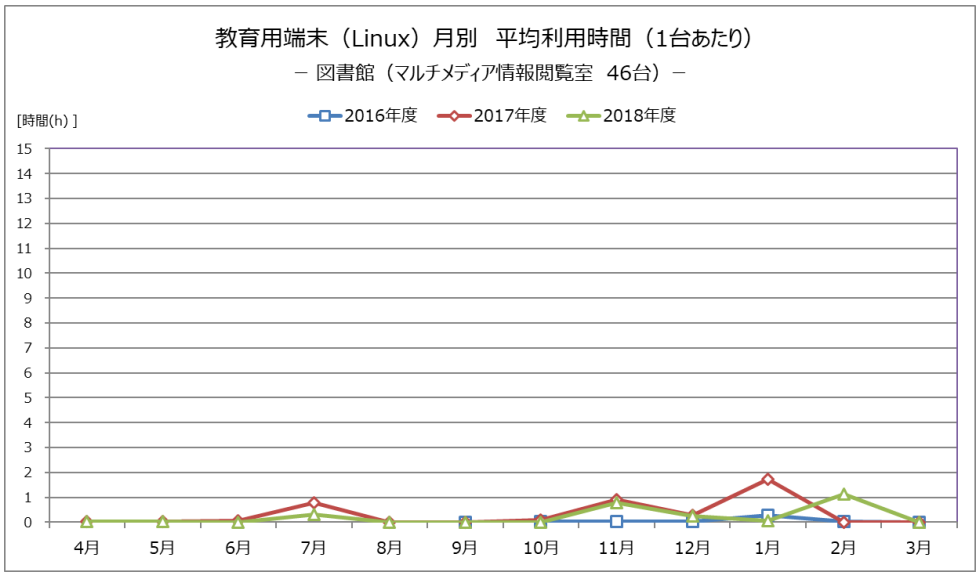
● 学生センターB 棟（キャリアフリールーム・国際交流情報室）

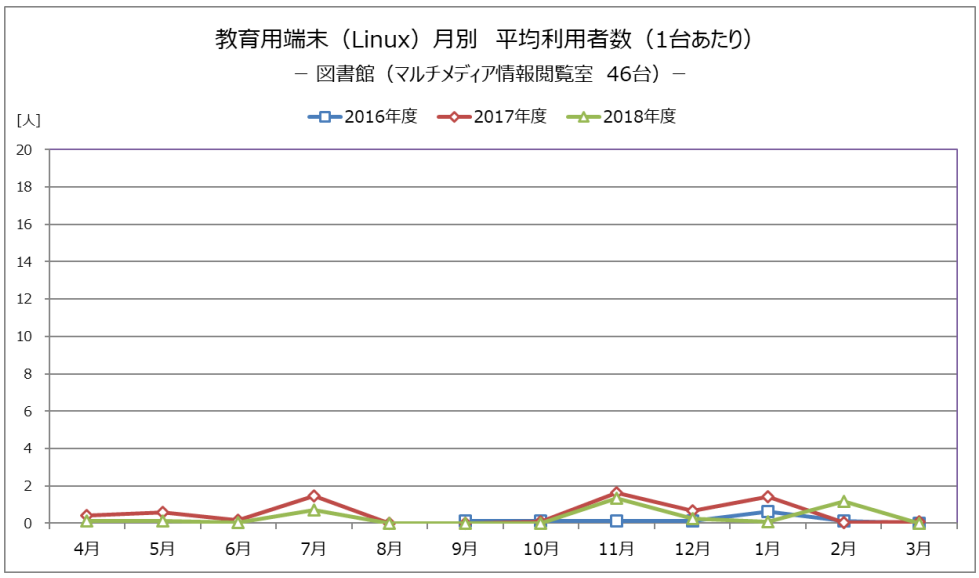




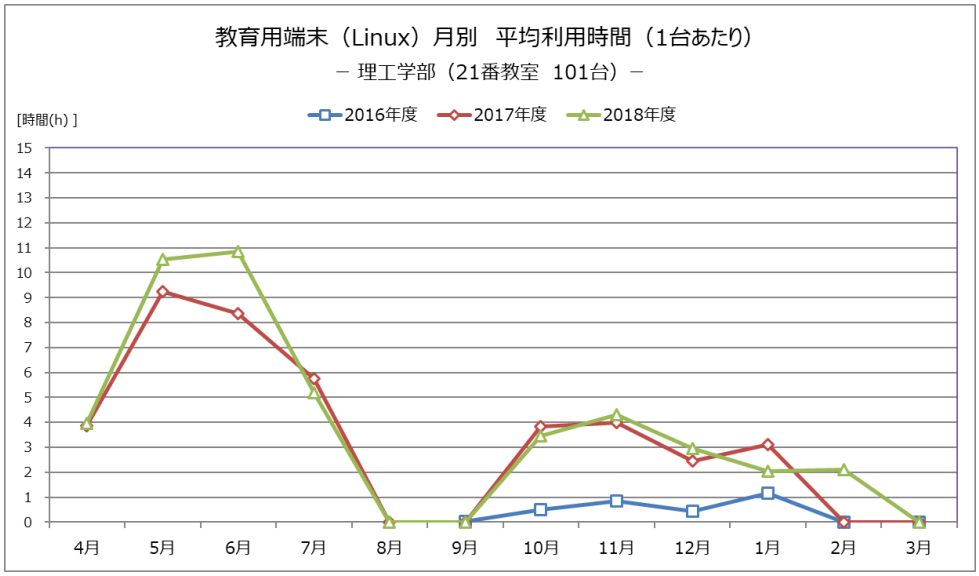
[教育用端末(Linux)]（2016 年 9 月～2019 年 3 月）

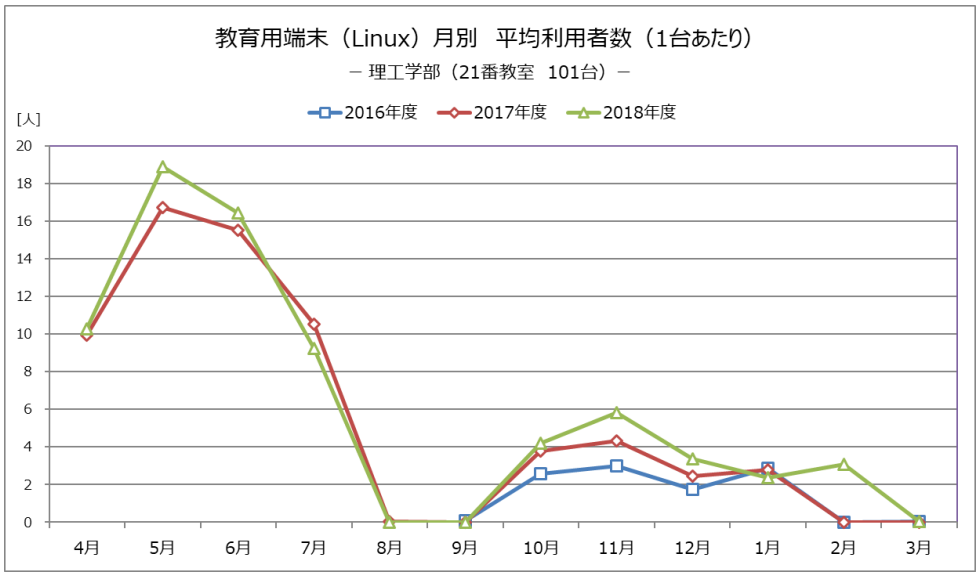
- 図書館（マルチメディア情報閲覧室）



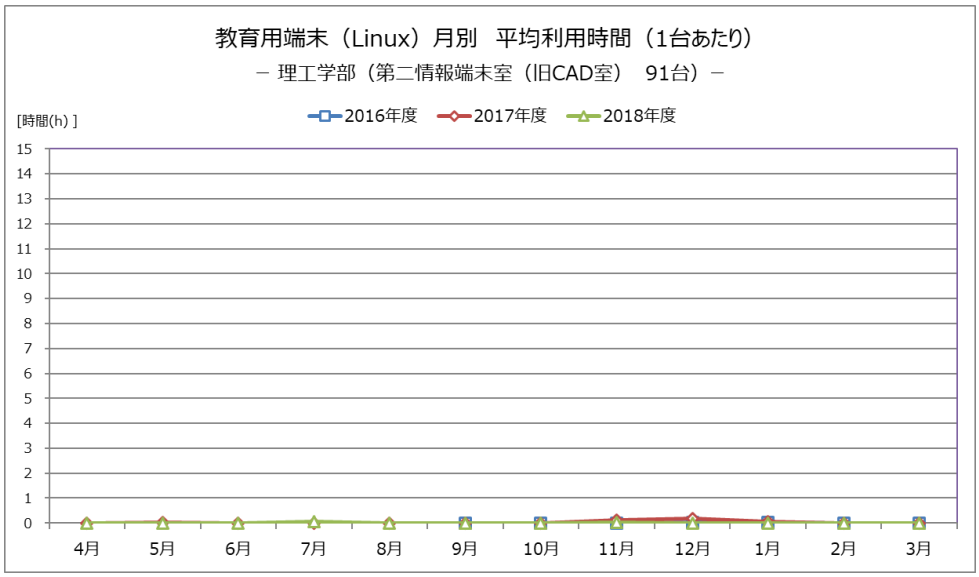


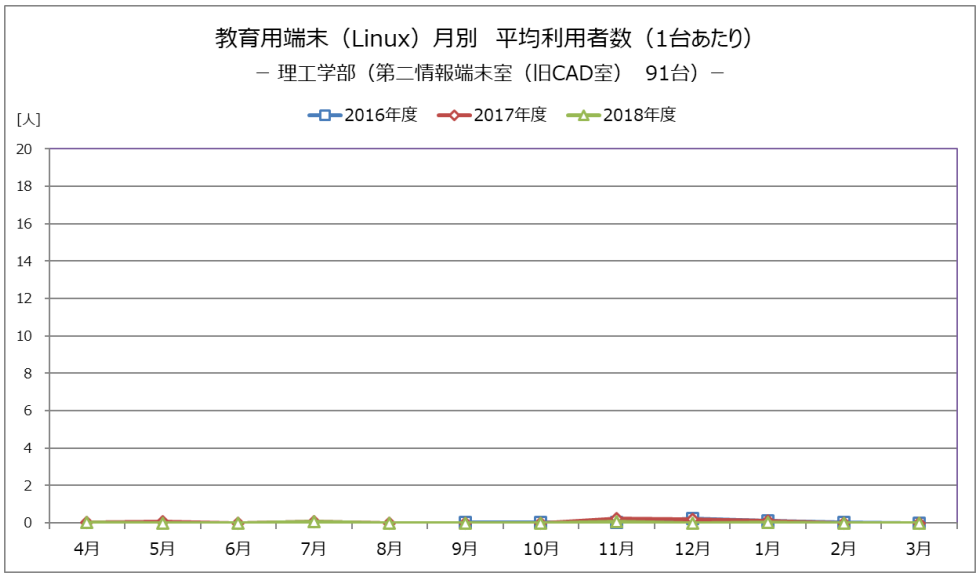
- 理工学部（21 番教室）



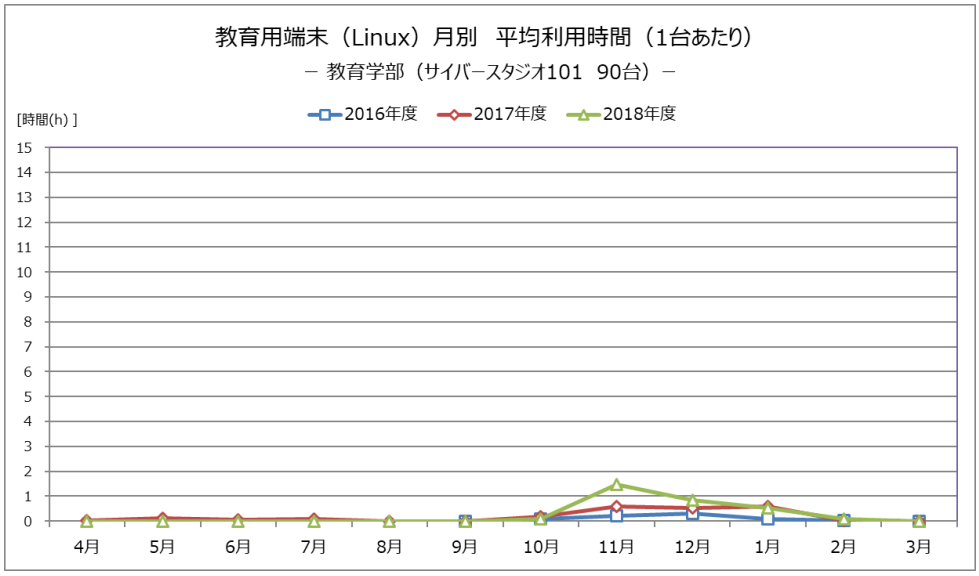


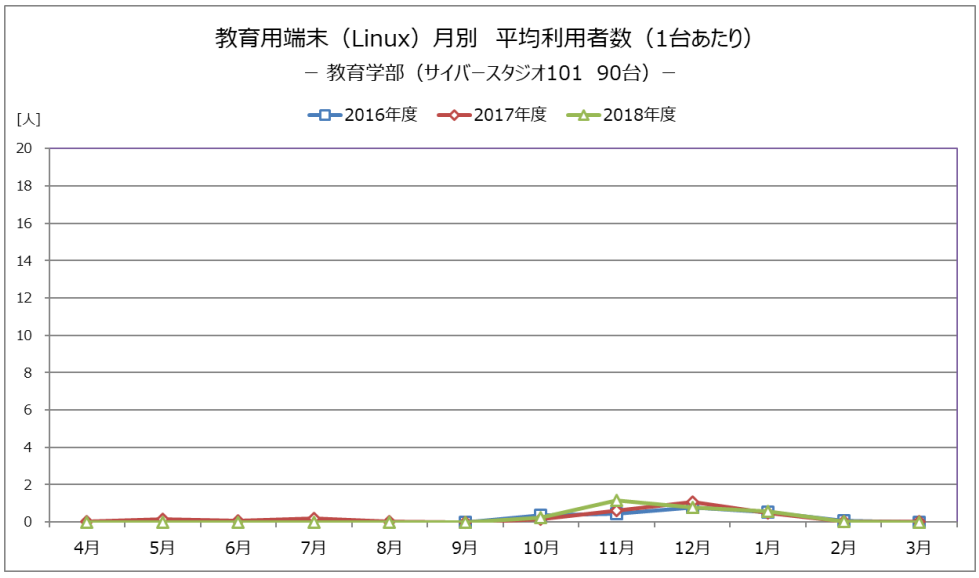
- 理工学部（第二情報端末室（旧 CAD 室））



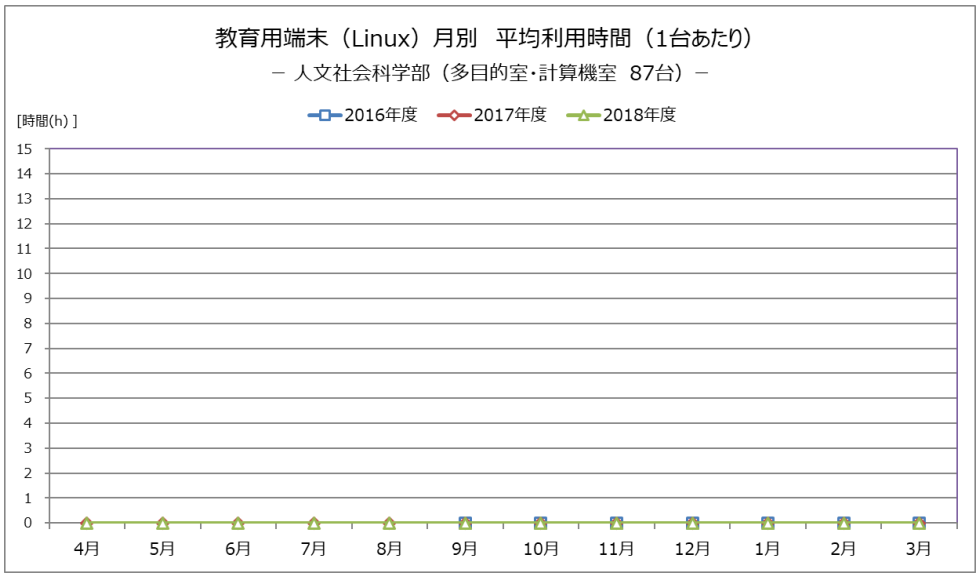


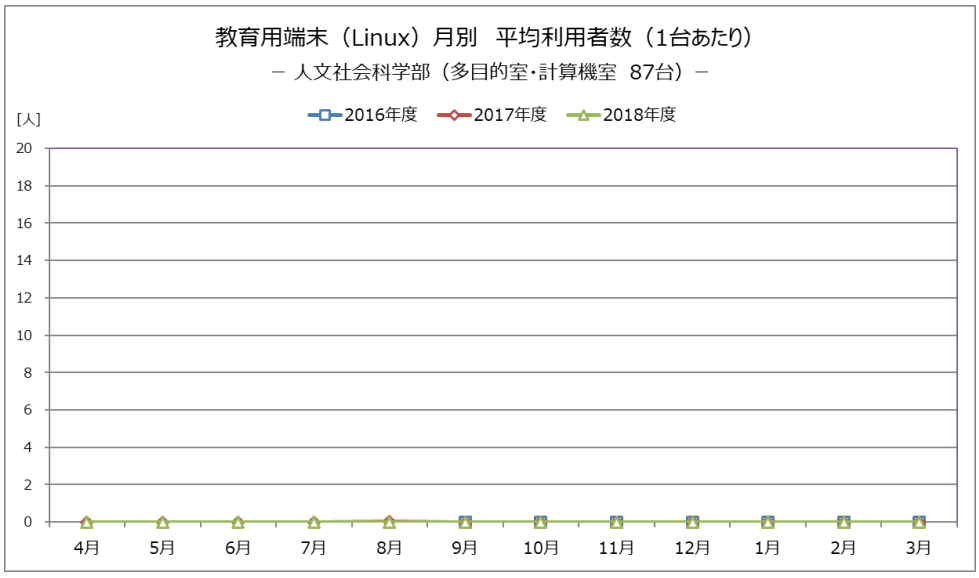
- 教育学部（サイバースタジオ 101）



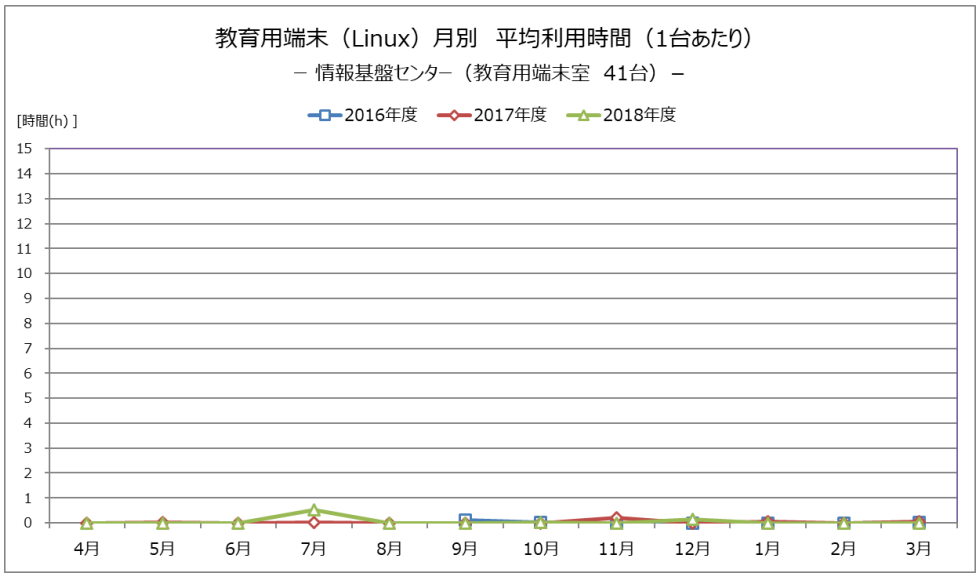


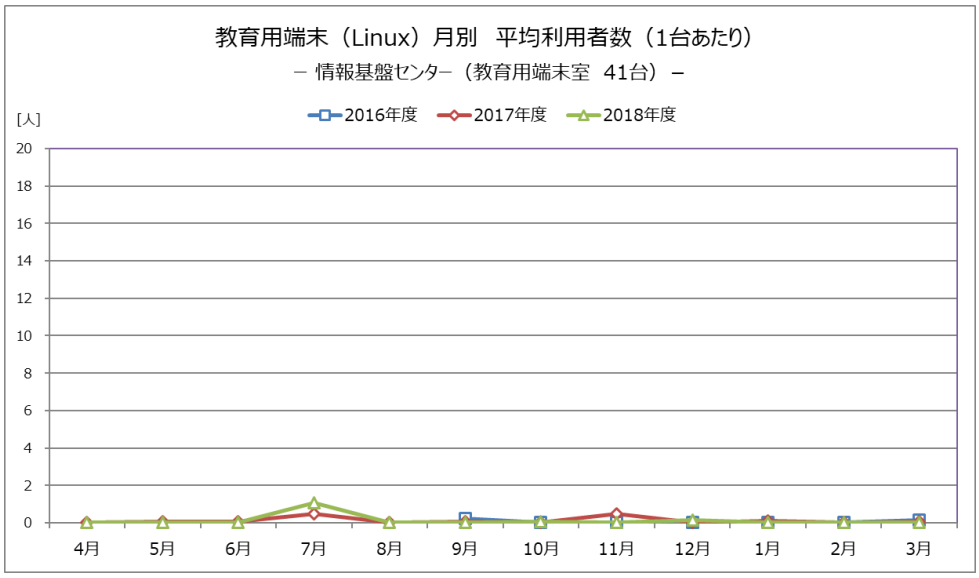
- 人文社会科学部（多目的室・計算機室）





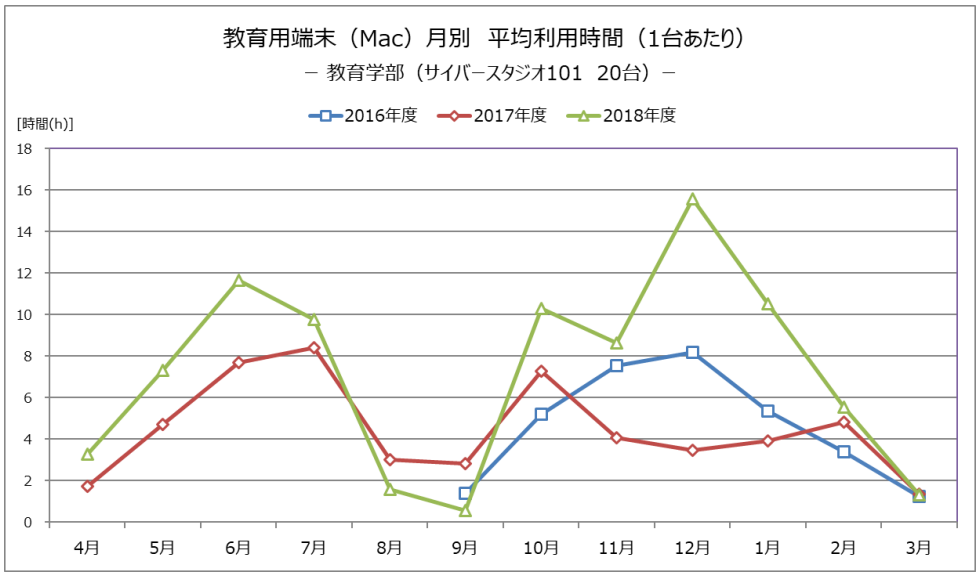
- 情報基盤センター（教育用端末室）

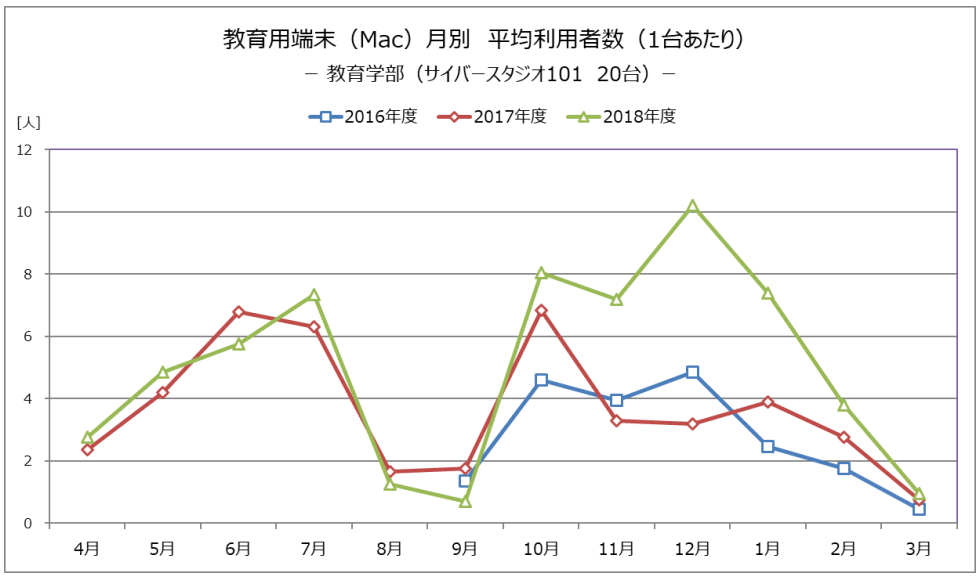




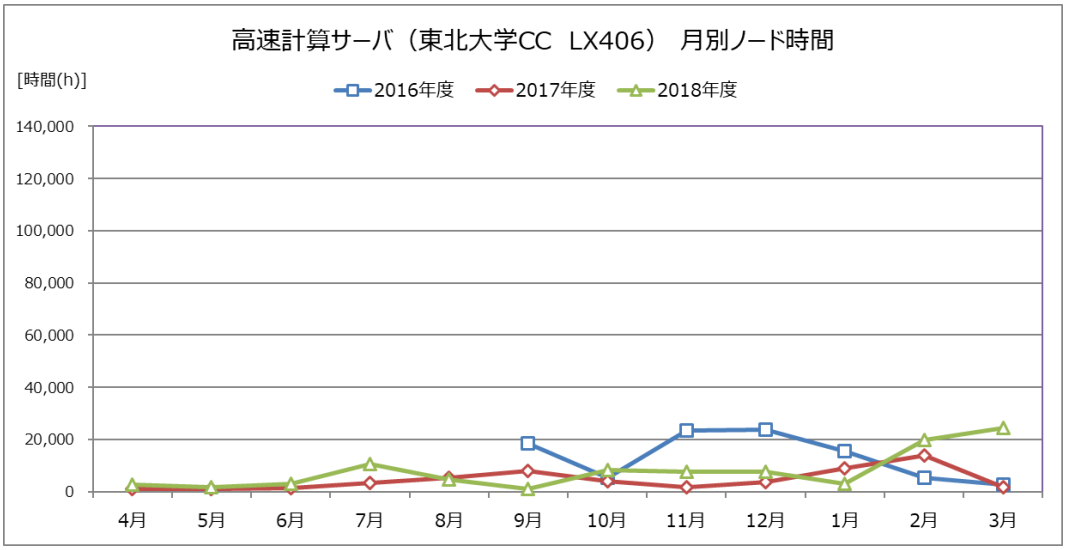
[教育用端末(Mac)]（2016 年 9 月～2019 年 3 月）

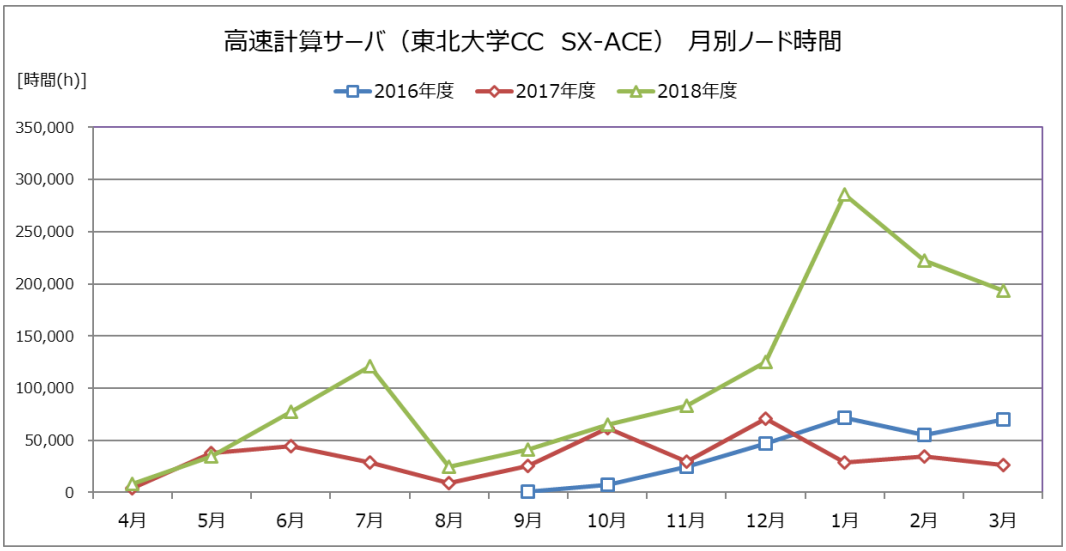
- 教育学部（サイバースタジオ 101）

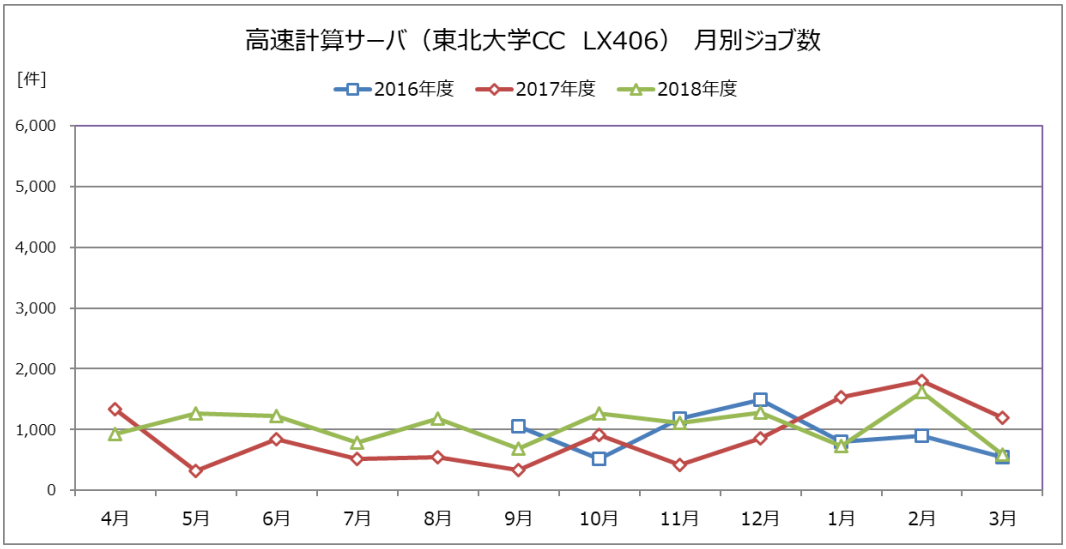


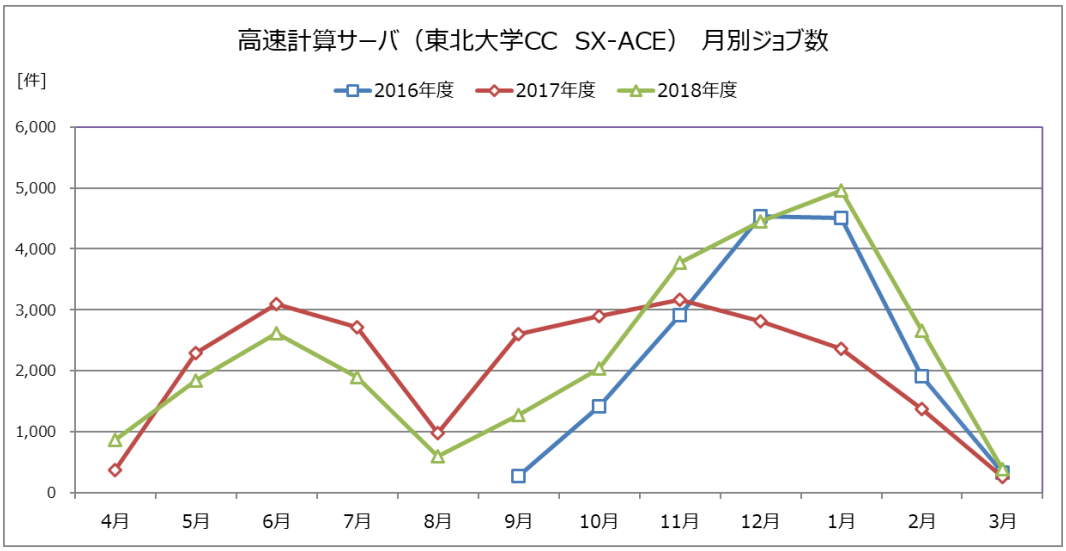


[高速計算サーバ(東北大学サイバーサイエンスセンター)]（2016 年 9 月～2019 年 3 月）









[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
2017 年度　19 件
2018 年度　15 件

[遠隔教育（収録・VOD）]

2014 年度　56 件
2015 年度　64 件
2016 年度　48 件
2017 年度　33 件
2018 年度　70 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
2017 年度　156 件
2018 年度　205 件

【利用の成果】

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

利用の成果

1. 平成 30 年度研究発表目録

1.1. 学術論文，学会発表等

- 工学研究科

  - 機械・社会環境システム工学専攻

    * 竹田裕貴，中村牧人，上野和之，丹野英幸 : 直交カットセル法を用いた大気圏再突入カプセルの連成解析，第 50 回流体力学講演会/第 36 回航空宇宙数値シミュレーション技術シンポジウム，3C05，2018 年.

    * 竹田裕貴，上野和之，石川達也，奥寺智弘，丹野英幸 : 壁面モデルを用いた直交カットセル法による大気圏再突入カプセルの空力係数予測，日本航空宇宙学会北部講演会 2019 年講演会ならびに第 20 回再使用型宇宙推進系シンポジウム，JSASS-2019-H028，2019 年.

- 総合科学研究科

  - 理工学専攻（物質化学コース）

    * 宇井幸一，○米谷直樹，村岡宏樹，鈴木映一，小川智，万代俊彦，竹口竜弥，岩野直人* (エルナー株式会社*) : γ?ブチロラクトンを主体としたアルミ電解コンデンサ用混合電解液の高温域での挙動解析，2018 年度表面技術協会・東北支部防食学会東北支部合同講演会，山形，2018 年 12 月 14 日．（○優秀発表賞を受賞）

    * Hiroki Muraoka and Satoshi Ogawa : Synthesis and ICT-Based Sensing Properties of 1,3,5-Triazine-cored Star-shaped (D-π)3-A Molecules with Various Amino-type Donor Receptors，The 15th International Symposium on Inorganic Ring Systems，PB32，Kyoto，2018.6.24-29.

    * Akihiro Okubo , Hiroki Muraoka , and Satoshi Ogawa : Synthesis and Characterization of Tetrathienylethylene Derivatives Functionalized with Aryl Groups，28th International Symposium on the Organic Chemistry of Sulfur，PA-8，Tokyo，2018.8.26-31.

    * Hiroki Muraoka and Satoshi Ogawa : Systematic Synthesis of Star-shaped D-π-A Molecules with a Different Nitrogen-containing Heteroaromatic Core and Comparative Studies of Their Optical and ICT-based Sensing Properties，28th International Symposium on the Organic Chemistry of Sulfur，OA-5，Tokyo，2018.8.26-31.

    * 岩淵直樹, 村岡宏樹, 小川智 : ピラジンをコアに有する D-π-A 分子の合成及び物性，第 29 回基礎有機化学討論会，3C02，東京，2018.9.6-8.

    * 村岡宏樹, 小川智 : アミノ基含有イオン認識部位を有する星型トリアジン誘導体の合成と蛍光センシング特性，第 35 回有機合成化学セミナー，P-52，山形，2018.9.18-20.

* 大久保晃裕，村岡宏樹，小川智：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、構造及び物性, 第 45 回有機典型元素化学討論会, O-34, 新潟, 2018.12.13-15.

* 大久保晃裕，村岡宏樹，小川智：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、構造及び物性，日本化学会第 99 春季年会，2I5-27，神戸，2019.3.16-19.

* 田口優介，村岡宏樹，小川智：アリール基で機能化した 2,4-ビス(ジメチルアミノ)-6-(3-ヒドロキシ-2-チエニル)-1,3,5-トリアジンとそのメトキシ誘導体の合成と物性，日本化学会第 99 春季年会，2I5-28，神戸，2019.3.16-19.

* 久保田頼哉，村岡宏樹，小川智：アリール基修飾型チオフェンを側鎖に有するシロール中心星型分子の合成と物性，日本化学会第 99 春季年会，2I5-31，神戸，2019.3.16-19.

* 岩淵直樹，村岡宏樹，小川智：ピラジンコアを有する直線型及び星型 D-π-A 分子の合成及び物性，日本化学会第 99 春季年会，3I5-10，神戸，2019.3.16-19.

* Hiroki Muraoka , Raiya Kubota , and Satoshi Ogawa : Synthesis and Characterization of Star-shaped Molecules with a Silole core and Aryl-functionalized Thiophene Side Chains, 平成 30 年度化学系学協会東北大会, 2P044, 秋田，2018.9.15-16.

* Hiroki Muraoka，Yusuke Taguchi，Satoshi Ogawa：
Synthesis and characterization of aryl-functionalized 2,4-bis(dimethylamino)-6-(3-hydroxy-2-thienyl)-1,3,5-triazines and their methoxy analogues，平成 30 年度化学系学協会東北大会，2P059，秋田，2018.9.15-16.

－ 理工学専攻（生命科学コース）

* 鈴木映一，戸井口侑太，八代仁：低温マトリックス中における $CF_3SO_3H-N_2$ 錯体の振動スペクトル，第 12 回分子科学討論会講演予稿集，3P017，2018 年.

－ 理工学専攻（材料科学コース）

* Songlin Xue，Daiki Kuzuhara，Naoki Aratani，Hiroko Yamada：Synthesis of a Porphyrin(2.1.2.1) Nanobelt and Its Ability To Bind Fullerene，Org. Lett. 2019, DOI: acs.orglett.9b00329.

* Songlin Xue，Daiki Kuzuhara，Naoki Aratani，Hiroko Yamada：Synthesis of Porphyrin(2.1.2.1) Nanobelts , International Conference on Porphyrins and Phthalocyanines (ICPP-10)，2018.

* Daiki Kuzuhara，Songlin Xue，Naoki Aratani，Hiroko Yamada：Constructions of Dimeric Triphyrin(2.1.1) and Porphyrin(2.1.2.1) Nanobelt , International Conference on Porphyrins and Phthalocyanines (ICPP-10)，2018.

* Hiroko Yamada , Songlin Xue , Naoki Aratani , Daiki Kuzuhara : Hexaphyrin(2.1.2.1.2.1): Substituent Effect on Synthesis, Metal Complexes, and Electronic Properties , International Conference on Porphyrins and Phthalocyanines (ICPP-10)，2018.

* 千葉裕矢, 葛原大軌, 吉本則之：分子内環化反応を用いたペンタフェン誘導体の合成，日本化学会第 99 春季年会，2019.

* 葛原大軌：環状ポルフィリン(2.1.2.1)多量体の合成，第 33 回有機合成化学若手研究者の仙台セミナー，2018.

- 理工学専攻（電気電子通信コース）

  * S. Aoyama, J. Kaiwa, P. Chantngarm, S. Tanibayashi, H. Saito, M. Hasegawa, and K. Nishidate : Oxygen reduction reaction of FeN4 center embedded in graphene and carbon nanotube: Density functional calculations, V AIP Advances 8, 115113, 9 pages (2018). (https://doi.org/10.1063/1.5053151)

  * H. Taniguchi 1, M. Matsukawa 1, K. Onodera1, K. Nishidate1 and A. Matsushita :
  Magnetic States and Bandgaps of B-Site Substituted Double-Perovskite Ba2Pr(Bi, Sb)O6, IEEE TRANSACTIONS ON MAGNETICS 55, 99, 4 pages (2018). (DOI: 10.1109/TMAG.2018.2874431)

  * 青山修也, 鹿岩潤, 長谷川正之, 西館数芽 : 燃料電池触媒の酸素還元反応におけるダイナミクスと電荷密度分布の変動, 第 7 回計算統計物理学研究会, P11, 2018 年 9 月 25 日.

  * S. Aoyama, J. Kaiwa, M. Hasegawa, and K. Nishidate : Fluctuation of charge densities during the oxygen reduction reaction process of FeN4 center embedded on the carbon system, The 5th Ito International Research Center Conference, Nov. 20, 2018.

- 理工学専攻（機械・航空宇宙コース）

  * 樺澤宏明, 高橋一至, 上野和之 : 温度不連続を許容する非平衡凝固の数値解析, 日本鉄鋼協会第 177 回春季講演大会, PS-59, 2019 年.

- 人文社会科学部

  - 人間文化課程

    * 三留颯, 白倉孝行 : 間接的互恵性の個別的評価モデルにおける最適戦略, アルテスリベラレス(岩手大学人文社会科学部紀要) 第 102 号, pp.17-24, 2018 年.

    * Nobuo Suzuki, Fumitaka Matsubara, Sumiyoshi Fujiki, Takayuki Shirakura : Phase diagram of an S = 1/2 J1-J2 anisotropic Heisenberg antiferromagnet on a triangular lattice, Journal of Modern Physics Vol.10 No.1, pp.8-19, 2019.

    * 鈴木伸夫, 松原史卓, 白倉孝行 : 二次元希釈 ANNNI モデルのドメイン相, 日本物理学会 2018 秋季大会, 京都, 2018 年 9 月 12 日.

    * 鈴木伸夫, 松原史卓, 白倉孝行 : 二次元希釈 ANNNI モデルの低温相図, 日本物理学会第 74 回年次大会, 福岡, 2019 年 3 月 17 日.

- 教育学部

  - 学校教育教員養成課程

    * Hitoaki YOSHIDA, Yoshino AKATSUKA, Takeshi MURAKAMI : Implementation of High-Performance Pseudo-Random Number Generator by Chaos Neural Networks using Fix-Point Arithmetic with Perturbation, Proceedings of Papers, NOLTA 2018, pp.46-49, 2018.

- 工学部

  - マテリアル工学科

    * 小川倫弥，葛原大軌，吉本則之：光縮環反応を用いたペリレンジイミド誘導体薄膜の作製，日本化学会第 99 春季年会，2019.

  - 機械システム工学科

    * 奥寺智弘，石川達也，竹田裕貴，上野和之：壁面モデルを適用したカットセル法による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講演会 2019 年講演会ならびに第 20 回再使用型宇宙推進系シンポジウム，JSASS-2019-H029，2019 年.

1.2. 修士論文

- 総合科学研究科

  - 理工学専攻（物質科学コース）

    * 岩淵　直樹　：ピラジン環をコアに有する直線型及び星型 D-π-A 分子の合成と物性

    * 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

  - 理工学専攻（電気電子通信コース）

    * 青山　修也　：燃料電池触媒の電子構造と酸素還元のダイナミクスに関する第一原理計算

    * 鹿岩　潤　　：フタロシアニンにおける MeN4 活性サイトの電子構造に関する第一原理計算

  - 理工学専攻（機械・航空宇宙コース）

    * 樺澤　宏明　：数値解析による温度不連続を伴う非平衡凝固数理モデルの検証

1.3. 学士論文

- 教育学部

  - 学校教育教員養成課程

    * 赤塚　淑乃　：カオス性とランダム性を有する時系列についての実験的検討

- 工学部

  - 応用化学・生命工学科

    * 虻川　大輝　：低温マトリックス赤外分光法による塩化チオニルーアミン類錯体の振動スペクトル

＊　大髙　祐珠　：亜硝酸メチルとアンモニアおよび水が形成する分子錯体の捕捉とその性質

－ **電気電子・情報システム工学科**

＊　米澤　直斗　：C60@(MeN4)x の電子状態とその原子構造

＊　三田　宙知　：C60@MeN4 の電子状態とダイナミクス

＊　小野寺　健太：C60@Ptx の電子状態

＊　村上　璃沙　：CNT@MeN4 の電子構造

＊　アシィ・アディコ：CNT@MeN4 における ORR 反応

－ **機械システム工学科**

＊　奥寺　智弘　：壁面モデルを適用したカットセル法による 30P30N まわりの圧縮性流れの数値解析

岩手大学情報基盤センター報告Σ　No.4　2018年度版
平成３１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