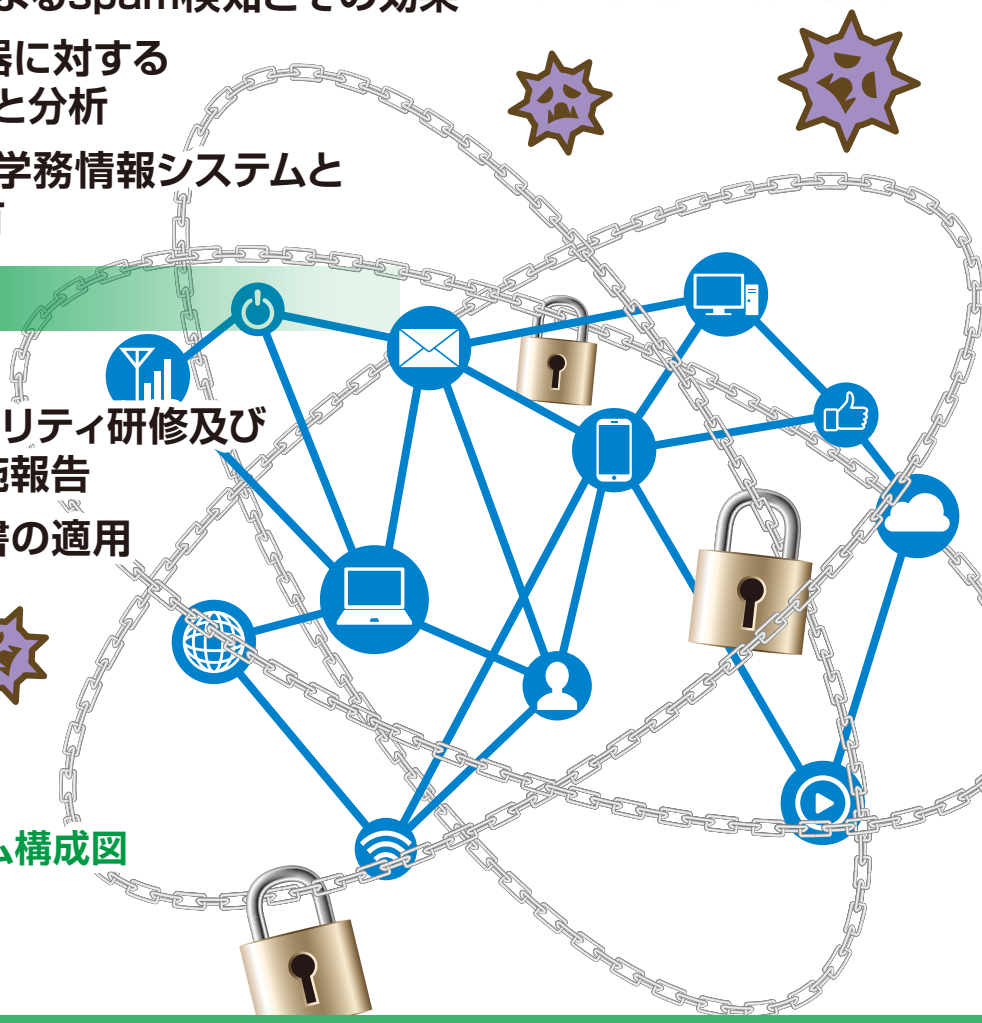
Journal of IPCs vol.39

https://www.cc.oita-u.ac.jp/journal/vol.39.pdf



OITA UNIVERSITY

大分大学学術情報拠点（情報基盤センター・医学情報センター）

〒870-1192　大分市大字旦野原700番地　情報基盤センター　https://www.cc.oita-u.ac.jp/

〒870-5593　由布市挾間町医大ケ丘1-1　医学情報センター　http://www.med.oita-u.ac.jp/mic/

発行　2019年3月　情報基盤専門委員会広報部会

情報系センターの役割の変遷

学術情報拠点副拠点長　吉田和幸

学術情報拠点情報基盤センターの沿革の Web ページをみると、「計算機センター」から「情報処理センター」、「総合情報処理センター」となり、大学統合時に「医学情報センター」と統合し、その後、図書館と統合して現在に至っている。当初の「計算機センター」の役割は、九大大型計算機センターの計算サービスの受付窓口とともに独自の計算サービスの提供であった。200MByte のディスクと 192kword(=384kByte)の主記憶という、現在から見るとスマホよりずっと小さな計算機であったが、研究データの処理等に活用された。

1990 年の情報処理センター設置に合わせて、学内 LAN、情報処理教育用 PC が導入された。ただし、計算サービスは、センターの提供するサービスのうち大きな部分を占めていた。学内 LAN に接続するサーバの処理能力等を考慮し、当時のダウンサイジングの流れにより、メールサーバ等を学内に複数設置して、協調して運用していた。対外接続は、インターネットとしてまだ SINET はなく、JAIN(Japan Academic Inter-University Network), KARRN （Kyushu Area Regional Research Network)などに加入して、インターネットに接続していた。計算サーバである汎用機同士を接続する N1 ネットワークにも参加した。

2002 年の総合情報処理センター設置によるシステム更新では、「情報処理教育用 PC」から「教育用 PC」となり、同時に LMS(Learning Management System) (当初 WebCT、その後 WebClass, 現在は Moodle)が導入された。このシステム更新とほぼ同時期に、ファイアウォールという位置づけで、本格的なインターネットルータが導入され、情報セキュリティ管理も行うようになった。大分県が運用する豊の国ハイパーネットにもこの時期に参加し、県内の大学研究機関との相互交流や、県内の高校との高大連携の推進に利用されている。

一方、1995 年に大分医科大学医学情報センターは、当初からインターネット等の ICT 環境を学内にサービスする組織として設置された。インターネットには KARRN（その後、SINET）といった学術系インターネットのみならず、商用インターネットにも接続し、冗長構成をとっていた。

大学統合、その後、学術情報拠点の設置を経て、現在に至っている。現在、センターがかかわっている課題として、まず、サイバーセキュリティがあげられる。ファイアウォール等の機器の導入、運用による不正侵入の検知、遮断に加えて、CSIRT(Computer Security Incident Response Team)などの体制整備などである。ICT 環境整備に関しては、サーバのクラウド化（特にパブリッククラウド利用の可否）、BYOD(Bring Your Own Device)としてどの程度、持ち込み端末を許可、推進するかなどの課題がある。現在、更新作業中の教育情報システムが、運用を開始したら、4 年後の次のシステム更新に向けて、調査等が始まる。

日頃のシステム運用や、今回のシステム更新にあたってご不便をおかけすることへの利用者各位のご協力に感謝いたします。

新教育情報システムについて

学術情報拠点　副拠点長　吉田和幸

現在、情報基盤センター・医学情報センターが教育用 PC として運用しているシステムは、導入後 4 年ほど経過しており、OS の陳腐化など更新の時期を迎えていた。そのため、学術情報拠点（情報基盤センター・医学情報センター）では、2019 年 3 月に教育情報システムを更新する。本稿では、新教育情報システムのうち、教育用 PC について述べる。

教育用 PC では、マルウェアの侵入を防ぎ、正常な動作環境を維持するシステムを導入している。現システムでは、両キャンパスで異なる方式の動作環境維持システムを導入している。旦野原キャンパスでは、ネットブート方式のシステムであり、電源投入のたびにブートサーバから OS をダウンロードする。一方、挾間キャンパスでは、PC のブート時に、変更があったところを検出して、削除するシステムを導入している。ネットブート方式は、高速なネットワークを必要とするが、Windows Update など、更新が必要な場合は、ブートサーバ中の OS イメージを更新すればいい。一方、ブート時に検査する方式の場合には、Windows Update のときは、すべての PC でブート時の検査を停止して Windows Update を行う必要があった。今回の更新では、運用の手間が少ないネットブート方式に統一した。高速なネットワークを必要とするネットブート方式のために旦野原キャンパスでは、学内 LAN の構成を多少見直した。LAN の構成変更が難しい挾間キャンパスでは、ブートサーバと PC との間に中継サーバ（リンクサーバ）を置いて、ブート時間の短縮を図っている。

教育情報システム（教育用 PC）の構成図を図 1，2 に示す。図に明示していないが、プリンタの配置は、従来通りである。変更点は、次の通りである。

1．情報基盤センター第 2 実習室の PC の配列を見直して 2 台減らし、図書館に配置する PC を 2 台増やした。
2．情報基盤センター第 3 実習室をセンター1 階に移動させる。

今後、システム更新に際して、ご不便をおかけすると思いますが、ご理解とご協力をお願いいたします。

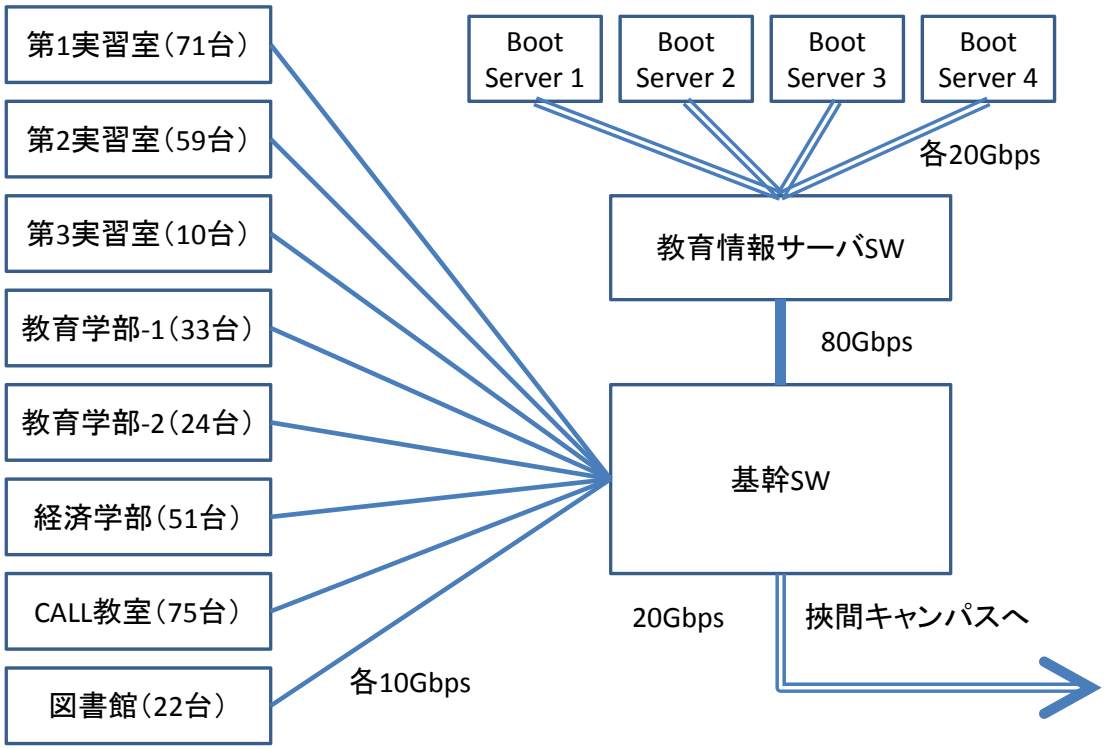


図1．教育情報システム構成図（旦野原キャンパス）

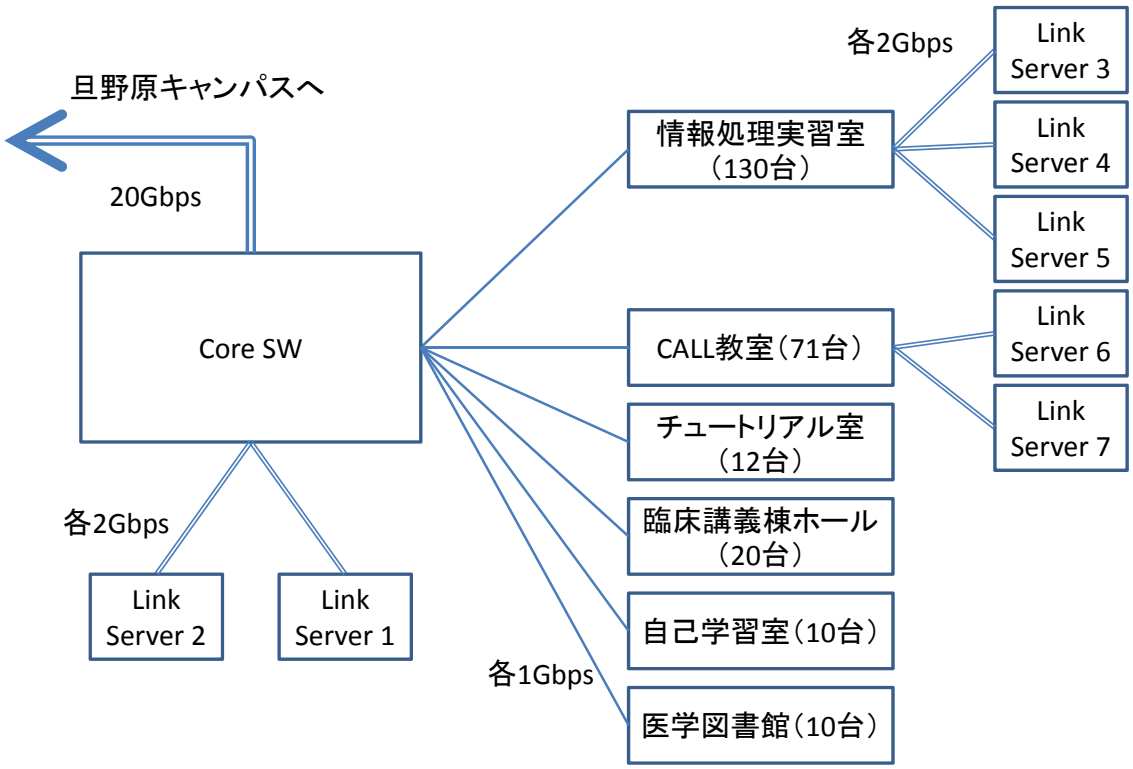


図2．教育情報システム構成図（挟間キャンパス）

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.5
2018/6/28

送信元メールアドレス検査による spam 検知とその効果

吉田和幸[†1]，池部実[†2]，吉崎弘一[†1]

概要：インターネットの普及に伴い，電子メールは通信手段の基盤となっている．一方，電子メールは不正侵入のきっかけとなりやすいため，spam 対策は不可欠である．従来から用いられてきた spam 対策は，送信メールサーバの FQDN が，メールサーバらしいか，利用者端末らしいかを判断する S25R，一時エラー後のメールサーバの動作を確認するグレイリスティング，spam を送信したメールサーバの一覧表（ブラックリスト）など，メールサーバを検査するものが多かった．しかしながら，ID/パスワードの流出により，プロバイダのメールサーバ等の正規のサーバから送られる spam も増えてきている．そのため，2017 年 5 月より送信元メールアドレスの検査を強化した．本稿では，spam 検出方法とその運用結果について述べる．

キーワード：メール，spam，spam 対策

Anti-spam measures by sender mail address check and its effect

KAZUYUKI YOSHIDA[†1]　MINORU IKEBE[†2]
KOICHI YOSHIZAKI[†1]

Abstract: With the spread of the Internet, e-mail is the basis of communication means. Meanwhile, countermeasures against spam are indispensable because e-mail tends to trigger illegal invasions. Spam countermeasures conventionally used check sender MTAs, such as S25R for judging whether the FQDN of the sender MTA is like a mail server or user terminal, gray listing for checking the operation of the sender MTA after a temporary error, or sender MTA is on blacklist. However, due to the leakage of ID / password, spam sent from an authorized server such as a provider's MTA is increasing. Therefore, from May 2017 the inspection of the sender's mail address was strengthened. In this paper, we describe spam detection method by checking sender mail address and its operation result.

Keywords: e-mail, spam, anti-spam measures

1. はじめに

インターネットの普及に伴い，電子メールは通信手段の基盤となっている．一方，電子メールは不正侵入のきっかけとなりやすいため，spam 対策は不可欠である．従来から用いられてきた spam 対策は，送信メールサーバの FQDN が，メールサーバらしいか，利用者端末らしいかを判断する S25R, 一時エラー後のメールサーバの動作を確認するグレイリスティング, spam を送信したメールサーバの一覧表（ブラックリスト）など，メールサーバを検査するものが多かった．しかしながら，ID/パスワードの流出により，プロバイダのメールサーバ等の正規のサーバから送られる spam も増えてきている．大分大学情報基盤センターが運用するメールサーバでの，2016 年，2017 年の spam 検知数の推移を図 1，図 2 に示す．2016 年 9 月以降正常と判定されたメール(ham)の数が増減を繰り返すようになったため，2017 年 5 月より送信元メールアドレスの検査を強化した．

本稿では，2 章で，従来行ってきた spam 検知手法について述べる．3 章では，送信元メールアドレスによる検知法について述べ，4 章でメールログから集計した検知数により，効果について示す．5 章では，まとめと今後の課題について述べる．

2. メールシステムの構成と従来実施してきた spam 対策

2.1 メールシステムの構成

大分大学のメールシステムは，インターネットからメールを受信して spam 対策を行う MTA(mail transfer agent, サーバ名 ajimu)とそれを通過したメールを受け取って受信者のメールボックスに配送する MDA(mail delivery agent)からなる[1]．ajimu での spam 対策の構成を図 3 に示す．図 3 では，各対策で spam と判定された場合には左に，ham（通常メール）と判定された場合には下に進む．

2.2 従来から実施してきた spam 対策

(1) throttling

throttling とは「spam 発信 MTA は timeout が短い」,「spam 発信 MTA は SMTP(Simple Mail Transfer Protocol)の確認応答手順を無視してメールを送る」との仮説に基づき，コネクション確立後の応答をわざと遅延させ，送信 MTA がこちらの応答を待たずにメールを送信してきた場合，spam と判断して受信を拒否する対策手法である[2]．throttling は遅延時間のみをパラメータとして設定する．

†1 大分大学学術情報拠点情報基盤センター
Information Technology Center, Oita University
†2 大分大学理工学部共創理工学科知能情報システムコース
Computer Science and Intelligent Systems, Oita University

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.5
2018/6/28

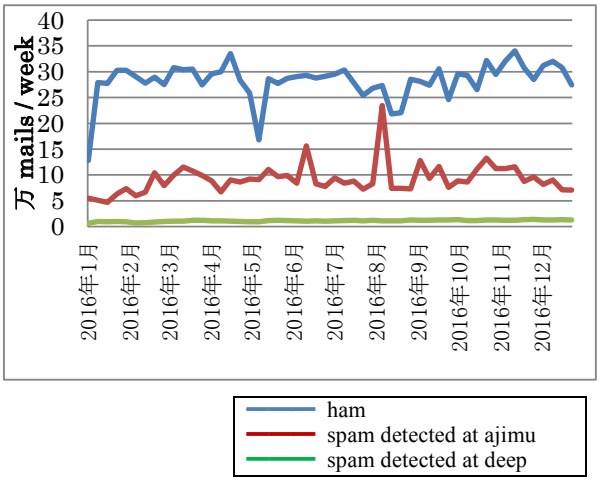


図 1　2016 年のメール受信数の内訳

Figure 1　Number of e-mails on 2016.

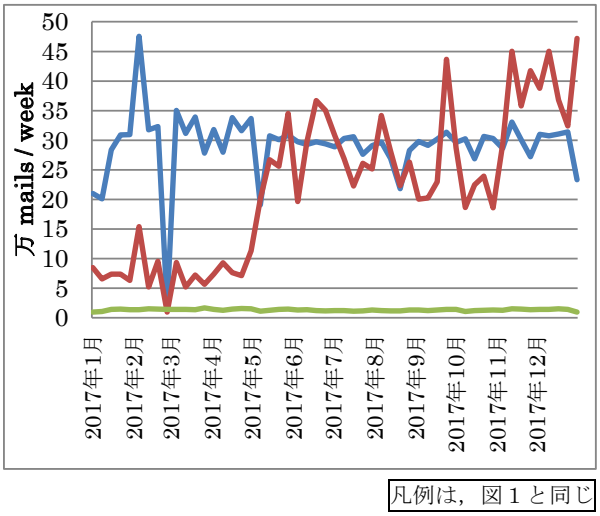


図 2　2017 年のメール受信数の内訳

Figure 2　Number of e-mails on 2017

(2)　送信元／宛先の検査

送信元メールアドレス，宛先メールアドレスの検査についてはドメイン部，ローカル部に分けて行う．

ドメイン部：(ア) . TLD(Top Level Domain)が，local または localdomain は，エラーとする．(イ)　DNS に登録がなければ一時エラーとする．(ウ)　A レコードが 127.0.0.1 と登録されていれば，エラーとする．(エ) 学外から来たメールの送信元アドレスのドメイン部が oita-u.ac.jp のときエラーとする．

ローカル部：(ア) ドメイン部が oita-u.ac.jp のときに，ldap にアカウントの有無を問い合わせる．アカウントが存在しなければエラーとする[3].

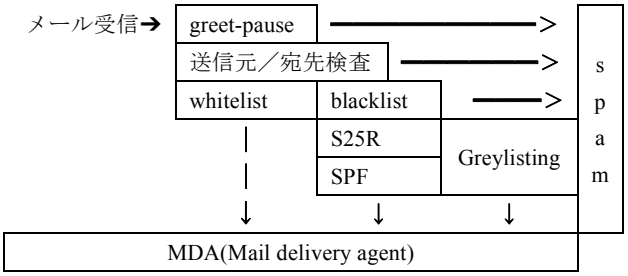


図 3．メールサーバでの spam 対策の構成

Figure 3. Antispam measures on MTA(ajimu)

(3)　whitelist

whitelist は，信頼できる MTA の IP アドレスを記述したリストである．通常 MTA からのメールであっても，spam 対策において spam と誤検知するケースが存在する．そのため，whitelist に spam 対策で誤検知されるが，信頼できる MTA の IP アドレスをリストすることで, 誤検知される通常メールを受信できる．大分大学においては，dnswl.org[4]および独自に作成した whitelist を使用している．whitelist に記載された MTA から送信されるメールは spam 対策を省くことで，通常メールを遅延なく受信できる．

(4)　blacklist

blacklist は, spam 送信 MTA の IP アドレスを登録したリストである．メールの送信者と受信者の間に TCP コネクションが確立した時に，blacklist に掲載されている IP アドレスからのアクセスを拒否する対策である．blacklist として Sorbs.net[5]や Spamhaus Project[6]を用いている．

(5)　S25R

S25R は接続してきた MTA の FQDN を S25R のルールと照合し，エンドユーザコンピュータであるかどうかを推定する．エンドユーザコンピュータの多くは FQDN を設定していない．あるいは，エンドユーザコンピュータに対して FQDN を設定していても，IP アドレスの下位 16 ビットなど多くの数字を含むことが多い．図 4 に S25R で検知可能な FQDN の例を示す．S25R では，エンドユーザコンピュータからの spam をほとんど検出できる．しかし，通常の MTA の中には，S25R の規則に該当する FQDN を設定していることがある．そのため，このような MTA からの通常メールをエンドユーザコンピュータからの spam と誤検知する可能性がある．そのため，S25R で spam とされた場合は, すぐに spam とするのではなく greylisting により再度検査を行う．

ml-192-168-0-1.exampl.jp
adsl-192-168-0-1.example.com
1.0.168.192.example.net

図 4. S25R で検知可能な FQDN の例

Figure 4. Example FQDNs detected by S25R

(6) **SPF**

SPF(Sender Policy Framework)[7]は SMTP によるメールの送受信において，送信者の正当性を検証し送信者のドメインの偽称を防ぐ送信ドメイン認証方式である．SPF はメール受信時に，メールが送信者であるメールアドレス（エンベロープ送信者）のドメインから送信されたものかどうかを検証することで，メール送信者の正当性を確認する．送信側はあらかじめ自ドメインの権威 DNS サーバに，自ドメインでメール送信を許可する MTA を特定する SPF レコードを登録する．同時にその他の MTA からメールの送信があった場合の判定を SPF レコードの末尾に「記号(+, -, ~)all」の形式で記述する．「+」は当該ドメインの送信 MTA として認証(pass)，「-」は拒否(fail)，「~」は当該ドメインの送信 MTA ではないが，通常 MTA の可能性があることを示す(softfail)．SPF レコードの記述例を図 4 に示す．例えば，図 4 の example.jp の SPF レコードの場合，192.0.2.0/24 のネットワークから送信されたメールは，自ドメインからのメールであるため認証成功とし，それ以外のネットワークからのメールは認証拒否とする．

example.jp. IN TXT “v=spf1 +ip4:192.0.2.0/24 –all”
example.com. IN TXT “v=spf1 +ip4:192.0.2.0/24 +all”
example.info. IN TXT “v=spf1 +ip4:192.0.2.0/24 ~all”

図 5　SPF レコードの記述例

Figure 5. Example of SPF record

(7) **Greylisting**

greylisting[8]は tempfailing 手法のひとつで，「spam 発信 MTA は再送をしない」との仮説に基づいた対策手法である．一時エラーにより受信を拒否し，一定時間経過後に再送されたメールのみを受信する．再送した MTA は一定期間 greylisting の autowhitelist に登録される．autowhitelist に登録されていれば再送要求はせず，すぐにメールを受信する．ただし，短時間で再送された場合には，再度一時エラーで応答する．多くの spam 発信 MTA は配送効率を重視しているため，仮説通りに動作し，spam 排除の効果が高い．しかし，MTA に再送を要求するため配送遅延が大きくなりやすく，1 時間以上の遅延が発生する場合も多い．そのため，我々は，S25R, SPF で spam 判定されたメールのみ greylisting で検査する．

3. 送信元メールアドレスの検査

3.1 エンベロープ From とヘッダ From

送信元メールアドレスが現れるエンベロープ From, ヘッダ From の 2 か所について検査を行う．エンベロープ From は，メールを送る smtp プロトコル[9]の中で現れるものである．2 章(2)で行っている検査は，このエンベロープ From について検査をしている．smtp プロトコルの例を図 6 に示す．一方，ヘッダ From は，メールの中の From:ヘッダ[10]

送信元 MTA		宛先 MTA
	←	220
EHLO mail.example.jp	→	
	←	250
MAIL FROM:<foo@example.jp>	→	
	←	250
RCPT TO:<baa@example.com>	→	
	←	250
DATA	→	
	←	345
（メールデータの送信）	→	
.	→	
	←	250

図 6 smtp プロトコルの概要

Figure 6. Outline of smtp

に現れるメールアドレスである．通常，これら 2 つの送信元メールアドレスは同じものであるが，メーリングリスト等で，エンベロープ From は書き換えられることがある．

3.2 ドメイン名ブラックリスト／ホワイトリスト

独自のドメイン名ブラックリスト／ホワイトリストを作成するとともに，Spamhaus Project[6]のドメイン名ブラックリストを参照する．ホワイトリストには，属性型 JP ドメインをはじめ，受信するメール数が多いドメインを列挙している．ブラックリストには，筆者に届いた spam の送信元アドレスから再度送られてきそうなドメインを列挙している．ブラックリストの一部を図 7 に示す．たとえば，jp.com は，apple.co.jp.com, netflix.co.jp.com というドメイン名の送信元アドレスとし使われたことがある．

jp.com
ssl.com
service.com

図 7. 独自ドメイン名ブラックリスト(部分)

Figure 7. Example of domain blacklist

3.3 メールアドレスブラックリスト

筆者に届いた spam のうち，ドメイン名ブラックリストに登録できないものは，メールアドレスそのものをブラックリストに列挙する．メールアドレスブラックリストの一部を図 8 に示す．

3.4 表示名の検査

メールの From ヘッダの形式を図 9 に示す．From ヘッダは，＜と＞で囲まれたメールアドレスとその前に書かれる表示名からなる．Amazon からのメールでは，表示名に Amazon.co.jp と書かれている．それをまねて，表示名に Amazon.co.jp と書かれた spam も多数ある．そのため表示名がこのようになっていて，メールアドレスのドメイン部が

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.5
2018/6/28

*amazon.co.jp，あるいは，*amazon.com でないものは，spam とする．現在，このような検査を netflix についても行っている．

3.5 適用順

ドメイン名の検査は，ホワイトリスト，ブラックリスト，spamhaus の dbl の順であり，MTA の IP アドレスの検査より優先する．Id，パスワードの流出等により，プロバイダのメールサーバから spam が送られる可能性があるからである．通常のメールも同じブラックリストに載せたメールアドレスを使っている可能性があるため，IP アドレスホワイトリストに載っていない MTA から来たメールのみにメールアドレスブラックリストを適用する．表示名の検査は，ヘッダ From のみで，独立しているので，最初に行っている．

jp@icloud.com
noreply@icloud.com
noreply2@icloud.com
noreply3@icloud.com
noreply4@icloud.com
appleid@id.apple.com
appleid@appleid.apple.com
support@appleid.apple.com
info@mail.rakuten-card.co.jp
support@mail.rakuten-card.co.jp
webshop_noreply@emagazine.rakuten.co.jp
partner@shop.rakuten.co.jp
order@rakuten.co.jp

図 8.　メールアドレスブラックリスト（部分）
Figure 8. Example of mail address blacklist

From: 表示名 <メールアドレス>

図 9. From ヘッダの形式
Figure 9. Format of From header

4. 運用結果

2017 年 12 月 31 日から 2018 年 5 月 26 日までの 5 か月 (21 週間）メール数の集計結果を表 1 に，Greylisting の詳細を表 2 に示す．表 1，2 で，「Accept」は，再送により受信したメール数，「Autowhite」は，greylisting の autowhite list に載っているため，一時エラーなしで受信したメール数，「1st」は，最初に一時エラーとしたメール数，「2nd or more」は，短期間で再送されたため一時エラーとした回数である．greylisting により受信したメール数は，「Accept」＋「Autowhite」であり，検知した spam 数(greylist deny)は，

Spam 数　＝　「1st」－「accept」

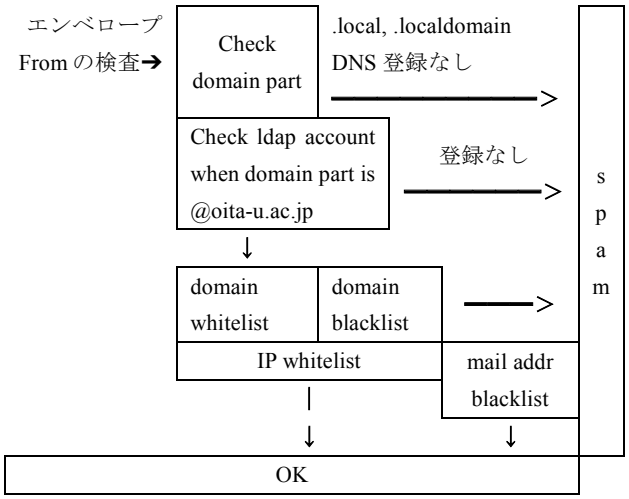


図 10. エンベロープ From の検査
Figure 10. Check for envelope From

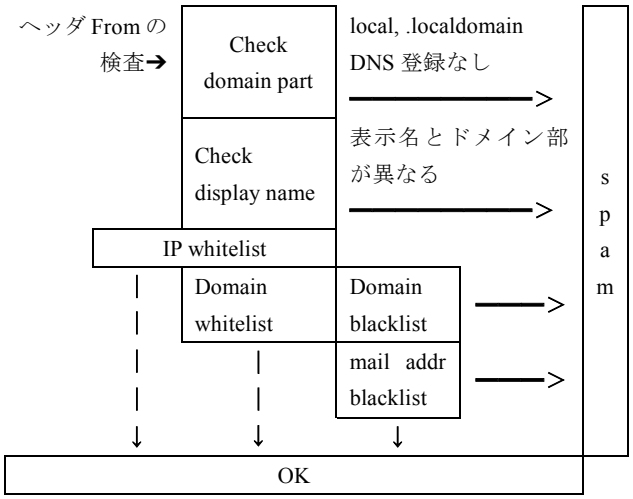


図 11　ヘッダ From の検査
Figure 11. Check for Header From

である．Ham（通常メール）および Greylist 関連の集計はメール数である．しかし，Greylist 以外の spam 数は，受信拒否の回数である．同じメールが何回も再送されている可能性もあり，多めに現れている．Ham(通常メール)数が，753 万通に対して，spam 数が，1320 万通と 2 倍近く多いのは，このためである．Firewall で Malware が検知された場合，当該 smtp コネクションはリセットされる．そのログには IP アドレスが表示されないため，Malware 欄の IPv4,IPv6 の内訳は不明である．

表 1 から，Ham(通常メール)753 万通のうち，受信時に再送遅延を強いているのは，「Greylist-accept」の 13 万 8 千通であり，受け取ったメールの 2%ほどである．

表 1 の spam 1320 万通のうち，envelope From での検知数は 1018 万通で 77%であり，Header From での検知数は 88

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.5
2018/6/28

表 1　受信したメール数の内訳
Table 1 Breakdown list of received mails

種別	内訳	IPv4	IPv6	合計
ham	Whitelist	6,174,805	12,857	6,187,662
	SPF	278,458	0	278,458
	Greylist Accept	136,505	1,875	138,380
	Greylist Autowhite	925,671	4,481	930,152
	Subtotal	7,515,439	19,213	7,534,652
Spam	Greet-pause	7,331	63	7,394
	Envelope From	9,994,512	190,802	10,185,314
	Envelope To	1,499,262	6	1,499,268
	User unknown	254,788	0	254,788
	Header From	880,135	8,179	888,314
	Greylist deny	342,424	54	342,478
	Blacklist	15,536	41	15,577
	Malware	-	-	2,973
	Subtotal	13,003,988	199,145	13,206,106
Total		20,519,427	218,358	20,740,758

表 2. Greylisting 関連の詳細
Table 2. Detail of mail counts Greylisting

	IPv4	IPv6	total
accept	136,505	1,875	138,380
autowhite	925,671	4,481	930,152
1st	478,929	1,929	480,858
2nd or more	2,104,963	228	2,105,191

表 3. エンベロープ From での検知の詳細
Table 3. Detail of number of mails detected at Envelope From

	IPv4	IPv6	Total
DNS に登録なし	313,064	6,121	319,185
local / localdomain	33,388	428	33,816
学外から oita-u.ac.jp	139,416	0	139,416
Mail addr blacklist	905,804	105,539	1,011,343
Domain blacklist	367,499	18,192	385,691
Spamhaus dbl	8,229,232	60,519	8,289,751
その他	6,109	3	6,112
Total	9,994,512	190,802	10,185,314

万通であり 7%である．

表 3. にエンベロープ From での検知の詳細を，表 4 にヘッダ From での検知の詳細を示す．表 3，4 とも，spamhaus dbl の検知が，80%ほどを占めている．Spamhaus dbl で検知されるメールを送ってきた MTA は，5 か月間で，14966 であった．その MTA のドメイン名について第 2 レベルまでについての集計の一部を表 5 に示す．属性型 jp ドメイン名を持った MTA も 174 位，400 位，545 位，878 位，2472 位に現れている．

5 か月間で検知したメールアドレスは，108 種で，約 102

表 4. ヘッダ From での検知の詳細
Table 4. Detail of number of mails detected at Header From

	IPv4	IPv6	Total
DNS に登録なし	93,292	414	93,706
local / localdomain	2,890	0	2,890
Mail addr blacklist	13,920	2,571	16,491
Domain blacklist	12,972	509	13,481
Spamhaus dbl	733,372	80	733,452
@がない	22,668	4,605	27,273
表示名	1,014	0	1,014
その他	7	0	7
Total	880,135	8,179	888,314

表 5. Spamhaus dbl で検知されたメールの送信元 MTA のドメイン名（部分）
Table 5. Sender MTAs detected by spamhaus dbl (part)

順位	検知数	ドメイン名（第 2 レベルまで）
1	1971558	lstn.net
2	886538	co.in
3	589367	sendinmail.net
4	504962	omicspublishinggroup.com
5	167494	websoftmedia.online
6	156061	ijoear.online
7	147954	24x7mailers.com
8	146499	fifa14.top
9	136599	amazonaws.com
10	131028	ijoer.online
54	25284	myvps.jp
67	17949	outlook.com
174	4211	ac.jp
204	3130	google.com
400	581	ne.jp
545	286	or.jp
878	88	ad.jp
2472	15	co.jp

万回検知した．表 6.に mail address blacklist で検知したメールアドレスの一部を示す．Mail address blacklist には，250 のメールアドレスを登録している．spam の送信元メールアドレスは，一過性のものもあり，その送信元メールアドレスから大量の spam を数時間送り続け，その後，その送信元メールアドレスからは，まったくメールが来なくなることもある．大量に検知される spam の送信元メールアドレスは，通常メールとしても使われるメールアドレスの場合と，そうでない場合がある．メールアドレスで遮断したことを察知したためか，大量のメールを同じ送信元メール

表 6. Mail address blacklist の検知数(部分)
Table 6. Number of spams by mail address blacklist(part)

順位	検知数	送信元メールアドレス
1	210234	noreply@email.apple.com
2	157512	info@mail.rakuten-card.co.jp
3	129684	order@rakuten.co.jp
4	74696	<do_not_reply@jp.oakley.com>
5	39112	<shipment-tracking@amazon.co.jp>
6	34165	myinfo@rakuten.co.jp
7	29603	<point@shop.rakuten.co.jp>
8	28660	<info@lows-jp.com>
9	28648	<info@mailthx.com>
10	28223	<info@thing-jp.com>
11	25015	<info@youtube-info.jp>
12	20575	<store-news@amazon.co.jp>
13	18618	<e-issues@shop.rakuten.co.jp>
14	18384	<yahoo@google-index.jp>
15	15919	<partne@uniqlo.com>
16	12896	<shipment_tracking@amazon.co.jp>
17	11964	support@mail.rakuten-card.co.jp
18	10314	<do_not_reply@line.me>
19	10112	<info@uk-mailer.com>
20	10006	<mail@googlehappy.net>

アドレスで送ると spam 判定されやすくなるためか，spam 送信者が送信元メールアドレスを微妙に変更することもある（表 6．5 位と 16 位など）．

5. おわりに

送信元メールアドレスそのものや，そのドメイン部を検査することによって spam 検知することの効果について大分大のメールサーバのログに基づいて報告した．ドメインブラックリスト，メールアドレスブラックリストへの登録は，手作業であり，登録するかどうかは筆者の経験によるところが大きい．登録基準を明らかにしていくことが今後の課題である．

謝辞 日頃，メールシステムの運用に．ご協力いただいています安徳先生をはじめとする医学情報センターの方々，情報基盤センターのスタッフの方々に感謝いたします．

参考文献

[1] 松井，金高，加来，池部，吉田. “milter の組み合わせによる低配送遅延を目指した spam 対策メールサーバの設計と導入の効果について”，情報処理学会論文誌, Vol.55, No.12, 2014, pp.2498-2510.
[2] 吉田. “Throttling による spam メール抑制の効果について”，情報処理学会研究報告，2005, Vol.2005-DSM-37, pp.69-74.
[3] 松竹，吉田. “メールの安定運用のためのメールゲートウェイにおけるサーバ連携について”，情報処理学会研究報告，2011, Vol.2011-IOT-14, No.9, pp.1-6.
[4] “DNSWL.ORG“. https://www.dnswl.org/, (参照 2018-05-23).
[5] “SORBS.NET”. http://www.sorbs.net, (参照 2018-05-23).
[6] “The Spamhaus Project”. https://www.spamhaus.org/, (参照 2018-05-23).
[7] Schlitt, W. “Sender Policy Framework(SPF) for Authorizing Use of Domains in E-Mail“. RFC4408, 2006.
[8] “Greylisting.org – a great weapon against spammer”. http://www.greylisting.org/, (参照 2018-05-23).
[9] J. Klensin. “Simple Mail Transfer Protocol”, RFC5321, 2008.
[10] B. Leiba. “Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields”, RFC6854, 2013

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.8
2018/6/29

ハニーポットを用いたIoT機器に対するパスワードリスト攻撃の収集と分析

清松天樹[†1]　池部実[†2]　吉田和幸[†3]

概要：Miraiをはじめとした IoT 機器を狙ったマルウェアが次々と出現している．このようなマルウェアは IoT 機器の管理の不十分さ，IoT 機器の脆弱性を狙っており，感染した IoT 機器は踏み台となるため IoT 機器のシステム管理者にとって大きな脅威となっている．我々は，学内 LAN に設置したハニーポットを用いて Telnet サーバ(TCP/23, TCP/2323)へのコネクション接続状況を調査している．これまでの Telnet サービス向けハニーポットでは TCP コネクションを確立した後，接続を切断していた．本研究では Telnet サービスのエミュレートプログラムを開発し，ログイン ID とパスワード収集機能を実装した．Mirai はソースコードが github で公開され，利用しているパスワードリストは既知である．本論文では約 3 か月間収集したパスワードリストや攻撃の送信元とその分析結果について述べる．今回観測したログイン ID とパスワードの組み合わせは 522 種類，観測したパスワードリストは 965 種類であった．最も多く使用されたパスワードリストは Mirai の持つパスワードリストをすべて含み，さらに Mirai の保持していないログイン ID とパスワードの組が存在していた．

キーワード：IoT 機器，Telnet，ハニーポット，パスワードリスト攻撃

Collection and analysis for password list attacks to the IoT devices using honeypot system

TENKI KIYOMATSU[†1]　MINORU IKEBE[†2]
KAZUYUKI YOSHIDA[†3]

Abstract: Malware aiming at IoT devices including Mirai has been appearing one after another. Such malware aims at insufficient management of IoT devices and vulnerability of IoT devices, and infected IoT devices becomes a stepping stone, which is a big threat to system administrator of IoT devices. We are collect the connection status of the Telnet server (TCP / 23, TCP / 2323) using the honeypot built on the campus LAN.The honeypot for the Telnet service has disconnected after establishing a TCP connection. we develop an emulation program for Telnet service and implement function login ID and password. Mirai is published with source code in github, and the password list which Mirai uses is known.
In this paper, we describe the password lists and attacks collected for about 3 months, and their analysis.The number of combinations of login IDs and passwords was 522, and the number of password lists appeared most was 965.password lists included all Mirai's password lists, and there were also several pairs of login IDs and passwords that Mirai did not use.

Keywords: IoT devices, Telnet, honeypot, password list attacks

1. はじめに

IoT(Internet of Things，モノのインターネット)を活用することで業務の効率化や快適な生活を実現できるとして注目されている．IoT 機器とは，自動車や家電をはじめとしてインターネットに接続する様々な機器を意味する．例えば，ネットワークカメラは，高所や水辺など人間が現地で常時観測が困難な場所に設置し，遠隔から映像を確認することで観測場所の状況を把握する．IoT 機器に搭載されている計算資源は端末コスト削減のため，通信の暗号化・復号処理に割り当てる CPU リソースの余力がないことがある．このような IoT 機器を管理者が遠隔から管理するために IoT 機器では通信の暗号化・復号の必要のない Telnet サービスが動作していることがある．Telnet サービスでは ID とパスワードを用いてログインすることで遠隔操作が可能となる．しかし，IoT 機器のパスワードが初期設定のままの場合や，初期設定からパスワードを変更できない場合がある．パスワードが初期設定のままでは攻撃者に容易に侵入されてしまう．

2016 年 10 月に警察庁の発表したインターネット観測結果等(平成 28 年 9 月期)によると，Mirai マルウェアに感染した IoT 機器を発信元とした Telnet サービスを標的とした通信が増加していた[1]．2016 年 9 月 20 日にはジャーナリストであるブライアン・クレブスのウェブサイトへの攻撃や，インターネット関連企業である OVH に対しての大規模な攻撃に Mirai が利用されたと報告されている[2]．この Mirai は Telnet サービスに対してログインを試行する．Mirai はログインに成功すると IoT 機器を遠隔操作し，マルウェ

†1 大分大学院工学研究科工学専攻
Graduate School of Engineering, Oita University
†2 大分大学理工学部共創理工学科知能情報システムコース
Faculty of Science and Technology, Oita University
†3 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.8
2018/6/29

アをダウンロードさせられる．マルウェアに感染した IoT 機器はボットとして動作し，感染拡大のための Telnet サービス探索活動や先に示したような攻撃の踏み台として利用される．また，Mirai には Telnet サービスを探索する中で，TCP/23 番ポートと TCP/2323 番ポートを 9 対 1 の割合で接続する特徴がある[2]．Mirai は 2016 年 10 月 1 日に，国外の Web サイトでソースコードが公開された．その後，Mirai をベースとしてプログラムを書き換えたと考えられる Mirai ボットの亜種の活動も確認されている[3]．

我々は，これまで学内ネットワーク上にハニーポットを設置し，不正通信の動向や攻撃手法を調査してきた．これまで Web アプリケーションの脆弱性を狙った攻撃を調査するために TCP/80 番ポート, TCP/8080 番ポート宛の HTTP リクエストの収集・分析[4]や，IoT 機器の Telnet サービスへの通信状況調査のために TCP/23，TCP/2323 番ポート宛の通信を観測してきた[5]．本研究では，IoT 機器に対する攻撃の詳細な手法を観測するために，低対話型ハニーポット Honeyd[6]に，Telnet サービスのログイン機能をエミュレートするプログラムを実装した．エミュレートプログラムでは，試行されたログイン ID とパスワードを収集する機能を実装した．今回は，IoT 機器の Telnet サービスを狙った攻撃のうち，マルウェアが次の感染先を探索する際の活動についての状況を把握することを目的として，開発したエミュレートプログラムを組み込んだハニーポットを稼働させ，約 3 ヶ月分の観測結果をもとにデータを分析した結果を報告する．

本論文の構成を以下に示す．第 2 章では本研究で用いた低対話型ハニーポットである Honeyd の特徴について述べ，第 3 章では Telnet サービスに対するパスワードリスト攻撃の観測方法を述べる．第 4 章にて観測データをもとに分析した結果と考察について述べる．最後に 5 章で本研究のまとめと今後の課題について述べる．

2. Honeyd

本研究では低対話型ハニーポットである Honeyd を用いた. Honeyd は 1 台の物理マシンで複数の仮想ホストをエミュレートでき，各仮想ホストでは特定 OS が稼働しているように見せかけられるオープンソースソフトウェアである．

ハニーポットには高対話型と低対話型の 2 種類がある．高対話型ハニーポットは，脆弱性を含む実際の OS やアプリケーションプログラムを用いるため，攻撃者の侵入後の詳細な挙動を観察できるが，攻撃者に攻撃の踏み台とされる可能性があるため慎重な運用が必要である．一方，低対話型ハニーポットは実際の OS やアプリケーションプログラムの機能の一部をエミュレートし攻撃を観察する．攻撃者を観測できるのは機能をエミュレートした範囲に制限される．そのため，実際に攻撃者に侵入され踏み台とされることはなく安全な運用が可能である．しかし，エミュレートした機能の範囲でしか情報を取得できないため，高対話型と比較して得られる情報は限定的である．

Honeyd は低対話型ハニーポットであるため, マルウェアに感染せず危険性が低く高対話型ハニーポットに比べて，安全に運用できる．また，Honeyd は 1 台の物理ホストで複数のホストをエミュレートする機能をもつため，本研究のようにログインおよびパスワード試行を複数の IP アドレスで観測することに適している．

本研究では Telnet サービスのログイン部分をエミュレートするプログラムを実装し，Honeyd に組み込んだ．telnet による TCP/23，TCP/2323 番ポート宛の通信に対してログイン ID とパスワードの入力を促し，Telnet サービスが動作しているように見せかけ，攻撃者のログイン ID とパスワードの入力パターンを観測した．

3. パスワードリスト攻撃の観測方法

3.1 従来の Honeyd サーバの Telnet サービスに対する攻撃の観測方法

先行研究[5]におけるハニーポットで Telnet サービスへの通信状況の観測方法および, Honeyd サーバの設置環境を図 1 に示す．学内ネットワークからサブネット長 24 のサブネットをハニーポット用として割り当て, Honeyd を当該サブネットに設置している. Honeyd でエミュレートしている IP アドレスは， 254 個のうち 251 個である．

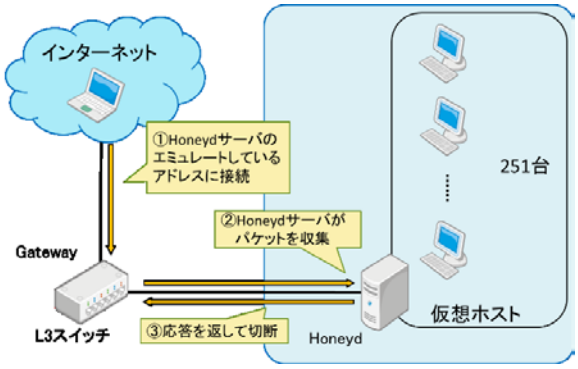


図 1　Honeyd サーバの設置環境

Honeyd サーバがエミュレートしている 251 個の IP アドレスの Telnet サービスに対する通信の観測方法を以下に示す．エミュレートした Telnet サービスは，TCP/23 番ポートおよび TCP/2323 番ポートで接続を待ち受けている．

1. Telnet サービスに対して TCP コネクションの確立要求(TCP SYN)を受信
2. 送信元に対して TCP SYN/ACK を応答し，相手からの TCP ACK を待機
3. 送信元からの TCP ACK を受信し，TCP スリーウェイハンドシェイクが成功し，Telnet サービスへの接続を確立
4. Telnet サービスへの接続直後に Honeyd 側から接続を切断

上記に示した観測方法の中で，以下の 6 項目をアクセスログとして記録した．また実際のアクセスログを図 2 に示す．送信元 OS 判別に p0f[7]を用いている．ただし，p0f では IP パケットから OS を判別できない場合もあるため，アクセスログには送信元 OS の記述がない場合もある．

- 受信時刻(JST)
- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号
- 送信元 OS

```
Fri Jun  1 16:06:16 JST 2018 From 219.218.19.249 35072 To 133.37.17.240 23 OS:"Linux 2.6 .1-7"
Fri Jun  1 16:06:17 JST 2018 From 209.97.142.159 37926 To 133.37.17.193 23 OS:"Linux 2.2 20-25"
Fri Jun  1 16:06:17 JST 2018 From 5.250.81.10 58828 To 133.37.17.202 23 OS:""
```

図 2 Honeyd で記録したアクセスログ

図 3 に Honeyd サーバにてエミュレートしている IP アドレス A に対して検証用クライアントから telnet で接続を試みたときの結果を示している．TCP コネクションの確立後，すぐに切断される．

#	コマンドおよび結果
1	$ telnet A
2	Trying A ...
3	Connected to A.
4	Escape character is '^]'.
5	Connection closed by foreign host.

図 3　Honeyd サーバへのログイン試行(1)

従来の Honeyd サーバにて収集したアクセスログにおいてアクセス数や送信元 OS に着目し分析した．分析結果 Telnet サービスへの攻撃が増加していること，判別できた送信元 OS において Linux の比率が高かったことを確認した[6].

3.2 新しい Honeyd サーバの観測方法

そして，本研究では従来収集していたアクセスログに加えて Telnet サーバのログイン機能をエミュレートさせる機能を追加し，送信者が試行したログイン ID とパスワードを収集した．送信者が試行したログイン ID とパスワードの組を既知のパスワードリストと比較し，送信元の特性を調査する．

従来の Honeyd サーバに加えて，Telnet サービスのログイン機能をエミュレートするプログラムを実装した Honeyd サーバ 2(以下，Honeyd サーバ 2)を新たに同じサブネットに設置した．Honeyd サーバ 2 の設置環境を図 4 に示す．従来，ハニーポット用サブネットで使用していた IP アドレス 251 個のうち 10 個を Honeyd サーバ 2 でエミュレートする IP アドレスとして割り当てた．

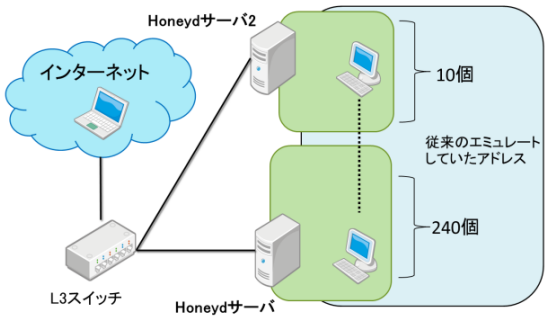


図 4　Honeyd サーバ 2 の設置環境

Honeyd サーバ 2 でエミュレートしている 10 個の IP アドレスに対する Telnet サービスへのアクセスの流れを以下に示す．Honeyd2 でエミュレートした Telnet サービスは，従来と同様に TCP/23 番ポートおよび TCP/2323 番ポートで接続を待ち受けている．下記に示した観測方法の中で，受信時刻，送信元 IP アドレス，試行したログイン ID とパスワードをログとして保存する．

1. Telnet サービスに対して TCP コネクションの確立要求(TCP SYN)を受信
2. 送信元に対して TCP SYN/ACK を応答し，相手からの TCP ACK を待機
3. 送信元からの TCP ACK を受信し，TCP スリーウェイハンドシェイクが成功し，Telnet サービスへの接続を確立
4. 従来の Honeyd サーバと同様のアクセスログを記録
5. 送信元に Telnet サービスへの ID の入力を促す
6. ID が入力されると，パスワードの入力を促す
7. パスワードが入力されると，認証失敗と応答
8. 再度，ID とパスワードの入力を促す．
9. ID とパスワードの試行を 3 回繰り返すと，通信切断

図 5 は Honeyd サーバ 2 にてエミュレートしている IP アドレス B に対して検証用クライアントから telnet で接続を試みたときの結果を示している．Honeyd2 サーバでは TCP コネクションの確立後ログイン ID の入力を待つ(図 5:7 行目)．ここではログイン ID として test として入力した．その後 Honeyd2 サーバはパスワードの入力を待つ(図 5:8 行目)．パスワードはエコーバックされないため表示されていないが test と入力している．パスワードの入力を受けた Honeyd サーバ 2 はログインを拒否し，新しい ID とパスワードの入力を受け付ける．これを後 2 回繰り返して，ログ

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.8
2018/6/29

イン ID とパスワードの取得し，コネクションを切断した．

#	コマンドおよび結果
1	$ telnet B
2	Trying B ...
3	Connected to B.
4	Escape character is '^]'.
5	Red Hat Enverprise Linux Server release 5.4 (Tikanga)
6	Kernel 2.6.18-164.el5 on an x86_64
7	Username: test
8	Password:
9	% Access denied
10	
11	Username: test1
12	Password:
13	% Access denied
14	
15	Username: test2
16	Password:
17	% Access denied
18	Connection closed by foreign host.

図 5　Honeyd サーバ 2 へログイン試行(2)

4. 観測データの解析結果と考察

3.2 説で示した収集方法により集めたアクセスログ，およびパスワードログのうち，2018 年 2 月 22 日から 2018 年 6 月 1 日までの 99 日分のデータを分析した．データ分析に用いた期間中において，TCP/23 番ポートおよび TCP/2323 番ポート宛のコネクション確立数は 1,151,553 件，Telnet サービスに対するログイン試行回数は 326,594 件，Telnet サービスに対するログインを試行した送信元 IP アドレス数は 5,094 であった．

4.1 ログイン試行回数分析

1 日あたりの TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクション確立数を示したグラフを図 6 に示す．図 6 のグラフより TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクションの確立数は 2018 年 5 月 9 日をピークとして約 9 万件があり，その他の日は平均 1 万件程度であった．

1 日あたりのログイン試行回数を図 7 に示す．図 6 に示したように TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクション確立数は常時 1 万件程度にも関わらず，2018 年 3 月 26 日を境にログイン試行の回数が急激に減少した．この現象は利用している IP アドレスがハニーポットとばれてしまったことなど理由はいくつか考えられるが現在のところこの症状の原因は判明していない．

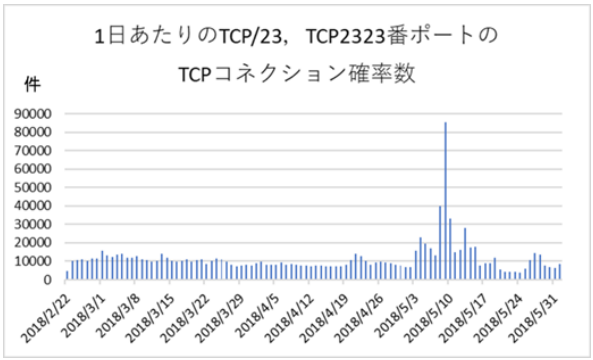


図 6　1 日あたりの TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクションの確立数

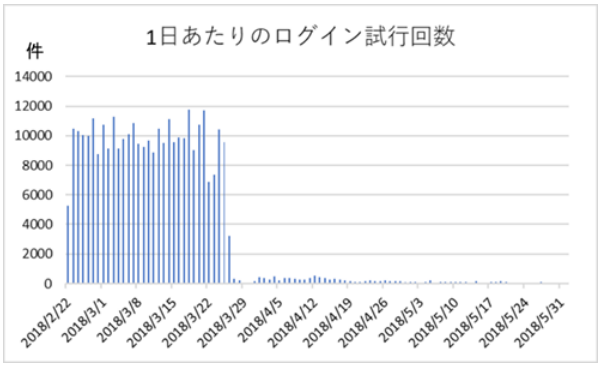


図 6　1 日あたりの Telnet サービスへのログイン試行回数

4.2 試行されたログイン ID とパスワードの分析

調査期間中に試行されたログイン ID とパスワードを送信元 IP アドレスごとに集計した．送信元 IP アドレスごとにログイン ID とパスワードの組を集計した結果から重複を排除した結果をパスワードリストと呼ぶ．集計結果よりパスワードリストは 965 種類であった．965 種類のパスワードリストのうち，上位 5 個のパスワードリストを使用した送信元 IP アドレス数を表 1 に示す．また 1 つの送信元 IP アドレスでのみ使用されたパスワードリストを 827 個存在した．Telnet サービスにログインを試行した送信元 IP アドレス数は 5,094 であるため，表 1 よりパスワードリスト A が 58.9%を占めていた．

一番多く観測したパスワードリスト A を表 2 に示す．表 2 中のログイン ID とパスワードのうち，Mirai で使用されるログイン ID とパスワードを網掛けして表している．

表 1　同一パスワードリストを用いた送信元数

パスワードリスト	送信元 IP アドレス数
A	3001
B	522
C	49
D	45
E	22

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.8
2018/6/29

表 2 から今回多く観測されたパスワードリスト A は Mirai の持つパスワードリストをすべて含み，さらに Mirai の保持していないログイン ID とパスワードの組が存在していたことから Mirai の保持するパスワードリストを拡張した亜種が活発に活動していると推測される．

表 3 にログイン試行に用いられたログイン ID とパスワードの組のうち，上位 10 件を示す．最も多かったログイン ID とパスワードの組は文字化けしていたため 16 進数で表示している．表 3 から文字化けしていた最多の組以外はパスワードリスト A に含まれていた．多く試行されたパスワードは 1234 と数字が並んでいた．表 3 中の 2 番目と 6 番目の組はワイヤレスルータのデフォルトパスワード，4 番目の組は防犯カメラのデフォルトのパスワードであった．このように攻撃者側は製品のデフォルトのパスワードや，安易なパスワードを狙っていた．

表 3　試行回数上位の ID とパスワードの組

	試行回数	ID	パスワード
1	7549	(0x0603)	(0x0E09)
2	7121	root	aquario
3	7116	admin	1234
4	3608	root	xc3511
5	3597	admin	123456
6	3591	root	5up
7	3586	root	GM8182
8	3585	root	juantech
9	3584	support	support
10	3582	root	123123

5. まとめと今後の課題

5.1 まとめ

本研究では Honeyd を用いて，Telnet サービスのログイン機能をエミュレートし，Telnet サービスへのログイン試行に用いられるログイン ID とパスワードの組を 99 日分取得し分析した．その結果 2018 年 3 月 26 日以降にログイン試行数が急激に減少したこと，また Mirai の持つパスワードリストを拡張したパスワードリストを用いるマルウェアが活発に活動していること，安易なパスワードや製品のデフォルトのパスワードが狙われやすいことを確認した．

5.2 今後の課題

●ログイン試行の減少の原因の調査

2018 年 3 月 26 日以降，TCP/23 および TCP/2323 宛の TCP コネクション数は変化していないにも関わらず，Telnet サービスへのログイン試行が急激に減少していた．現時点でこの原因は特定できていない．しかし，IoT 機器への攻撃を調査するためには，ログイン試行される必要がある．Honeyd サーバ 2 宛のパケットを解析し，ログイン試行が減少している原因を調査する．

●ログイン試行した送信元からの他ポートに対する攻撃の調査

本研究ではハニーポットで取得したログイン ID とパスワードの組について分析した．この他にもハニーポットにて TCP/23，TCP/2323 以外のポートに対するアクセスや，送信元 OS や送信元ポート番号などを収集している．これらの情報と Telnet サービスへログイン試行した IP アドレスの情報を組み合わせて分析することにより，IoT 機器を狙ったマルウェアによる，Telnet サービス以外の攻撃についても調査することができると考えている．

●IoT 機器を狙ったより詳細な攻撃の把握

今回は IoT 機器の Telnet サービスを狙った攻撃のうち，マルウェアが次の感染先を探索する際の活動についての状況把握を目的として調査した．今後はマルウェアからのログイン試行に対して，ログインを成功させる機能を追加し，ログイン成功後のマルウェアの挙動についても観測することを検討している．

参考文献

[1] 警察庁, “インターネット観測結果等(平成 28 年 9 月期)”, https://www.npa.go.jp/cyberpolice/important/2016/19361.html (参照 2018-5-30)
[2] IT メディア編集部, “ITmedia IoT マルウェア「Mira」とは何か”, http://techfactory.itmedia.co.jp/tf/articles/1704/13/news010.html (参照 2018-5-30)
[3] “ITmedia NEWS IoT マルウェア「Mirai」の亜種が急拡大、日本でも感染か？”, http://www.itmedia.co.jp/news/articles/1711/28/news061.html (参照 2018-05-30).
[4] 池部実, 宮崎桐果, 吉田和幸, “ハニーポットによる大分大学におけるダークネット宛通信の分析”, 情報処理学会研究報告インターネットと運用技術研究会(IOT), Vol.2015-IOT-29, pp.1-8, 2018 年 1 月
[5] 上妻麻美, 橋本涼, 池部実, 吉田和幸, “ハニーポットを用いた TCP/23 番ポートへの通信の解析”, 第 69 回電気・情報関係学会九州支部連合大会, p.272, 2016 年 9 月
[6] “Honeyd”. http://www.Honeyd.org/ (参照 2018-5-30)
[7] “p0f”. http://lcamtuf.coredump.cx/p0f3/ (参照 2018-6-4)

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2018-IOT-42 No.8
2018/6/29

表２　パスワードリスト A

ログイン ID	パスワード	ログイン ID	パスワード	ログイン ID	パスワード
666666	666666	guest	guest	root	ikwb
888888	888888	mother	fucker	root	ivdev
Admin	5up	root	0	root	juantech
Administrator	admin	root	1001chin	root	jvbzd
admin	1111	root	1111	root	klv123
admin	1111111	root	123123	root	klv1234
admin	1234	root	1234	root	oelinux123
admin	12345	root	12345	root	oelinux1234
admin	123456	root	123456	root	pass
admin	1234567890	root	1234567890	root	password
admin	1988	root	1234qwer	root	qazxsw
admin	54321	root	54321	root	realtek
admin	7ujMko0admin	root	5up	root	root
admin	Win1doW$	root	666666	root	system
admin	admin	root	7ujMko0admin	root	ttnet
admin	admin1234	root	7ujMko0vizxv	root	user
admin	cat1029	root	888888	root	vizxv
admin	ipcam_rt5350	root	GM8182	root	xc3511
admin	meinsm	root	Win1doW$	root	xmhdipc
admin	pass	root	Zte521	root	zlxx.
admin	password	root	admin	root	zsun1188
admin	smcadmin	root	alpine	service	service
admin	vertex25ektks123	root	anko	supervisor	supervisor
admin	zhongxing	root	aquario	supervisor	zyad1234
admin1	password	root	default	support	support
administrator	1234	root	dreambox	tech	tech
default	antslq	root	founder88	ubnt	ubnt
guest	12345	root	hi3518	user	user
guest	friend	root	hunt5759		

出典：大学 ICT 推進協議会 2018 年次大会 [MB2-6]

OneRoster 規格に基づいた 学務情報システムと学習支援システムの情報共有

吉崎 弘一, 中島 順美, 吉田 和幸

大分大学 情報基盤センター

kyoshi@oita-u.ac.jp

Information Sharing between Student Information System and Learning Management System Based on OneRoster Standard

Koichi Yoshizaki, Junmi Nakashima, Kazuyuki Yoshida

Information Technology Center, Oita University

概要

高等教育機関で広く導入されている学務情報システムと学習支援システムは、一般に独立したシステムであり、両システム間で開講科目や履修者の情報を自動的に共有するには、何らかの手法を導入する必要がある。本研究では、学務情報システムが管理する情報を、他システムと共有するための国際標準規格である OneRoster に基づいた REST API を用いることで、システム間の効率的な学務情報の共有を実現した。また、API サーバに簡易なデータ加工機能を実装することで、システム間の柔軟な学務情報の活用を実現した。

1 はじめに

日本国内の高等教育機関では、機関内で開講する科目や履修者情報を管理する学務情報システム（SIS: Student Information System）と、教材提示や課題提出などの学習活動を支援する学習支援システム（LMS: Learning Management System）が、共に導入されていることが多い。SIS が管理する開講科目や履修者等の学務情報は、当該科目で LMS を利用する際にも一般に必要となる。学務情報を両システム間で自動的に共有するには、機関独自の手法に基づきシステムをカスタマイズすることでも実現可能だが、カスタマイズ費用を低減させ、メンテナンス性を向上させるには、広く普及した標準規格に基づいた手法で情報共有をすることが望ましい。 本研究では、この学務情報のシステム間共有に、近年、米国の初等・中等教育でしばしば使われる国際標準規格である OneRoster [1]を用いた。

2 OneRoster 規格とは

2.1 概要

OneRoster 規格は、標準化団体の IMS Global が策定し、主に学務情報システム（SIS）が管理する情報を、学習支援システム（LMS）等の他システムで利用するための国際標準規格である[1]。同規格は IMS Global が策定した Learning Information Services（LIS）規格[2]を参考に、主に初等・中等教育での利用を想定して取り扱う情報を簡略化している。

LIS 規格と OneRoster 規格では、取り扱う情報そのものに加え、情報の提供方法も異なる。LIS 規格では、SOAP/http と LDAP に対応しているのに対し、より最近に策定された OneRoster では、REST API 及び CSV ファイル（バルク または デルタ）に対応しており、特に指定した情報のみ利用できる REST API と、差分データを取り扱うデルタ形式の CSV ファイルでは、効率的な情報共有が可能である。なお、SIS/LMS の OneRoster 対応状況としては、日本国内でも広く利用されている Moodle[3]では、本稿執筆時点で公的なサポートはしておらず、Canvas[4]等のいくつかの LMS でのみ OneRoster 規格に対応しているのが現状である[5]。

2.2 OneRoster v1.1 で共有する学務情報

本研究では、2018 年 9 月現在の最新バージョンである OneRoster v1.1 を用いた。同バージョンの OneRoster は、下記 3 種に分類した情報の共有を可能にする（提供が任意の情報も含む）が、本研究では、Class Roster に属する情報を利用した。

Class Roster: 科目や授業の情報、クラスを担当する教員、履修学生など

Resources: 科目や授業で使用する教科書や教材など

Gradebook Results: 課題のタイトルや締切り、評価結果など

なお、OneRoster 規格は初等・中等教育での利用を想定して策定されたが、次章で述べる本学での SIS-LMS 間の情報連携では、問題なく利用することができた。また、米国での利用を想定した値の設定、例えば SCED (School Codes for the Exchange of Data)の値を設定する項目は必須ではないため、今回はそれらの項目に値を設定せずに用いた。

3 システム間の学務情報の共有

3.1 システム構成

現在、大分大学では SIS として CampusSquare（新日鉄住金ソリューションズ株式会社）[6]、LMS として Moodle[3][7], LePo[8], ALC NetAcademy（株式会社アルク）[9]の 3 種を運用している。汎用的な学習に用いることができる LMS として、学内で広く利用している Moodle と、情報基盤センターで開発し、限られた科目のみを利用対象とする LePo[5]がある。また、英語学習専用 LMS として NetAcademy を運用している。Moodle と LePo は共にオープンソースソフトウェアとしてソースコードが公開されており、情報共有のためのシステムカスタマイズが行いやすいため、本研究ではこれら 2 種の LMS と SIS の情報共有についてのみ言及する。

3.2 2018 年度前期までの SIS-Moodle の取り組み

2017 年度前期から 2018 年度前期までは、SIS と LMS 間の学務情報の自動共有として、LMS は Moodle のみを対象としてきた（図 1）。この共有では、本学独自の記述形式の CSV ファイルを用いて、日次処理で Moodle に学務情報を反映する。この SIS-Moodle 間で共有する情報を表 1 に示す。これらの情報を用いることで、Moodle に対して 1) SIS に登録した全ての授業に対応したコースの作成・更新、2)SIS に登録した担当教員・履修者情報に対応したコースメンバーの登録・更新、の 2 つの自動処理を、開講期間中は毎日 1 回行っている。CSV ファイルに一度掲載された科目や担当教員/履修者が、後日の CSV ファイルから削除された場合は、当該コースや担当教員/履修者は、Moodle 上で非表示となる。

なお、本学では、LMS 利用時の教員の負担を減らすため、原則として SIS に登録した全授業を対象として Moodle にコースを自動作成しており、2017 年度は開講授業総数の約 2 割で、Moodle を何らかの活動で利用した。この学務情報の SIS-Moodle 間の自動共有に加え、表 2 のシステムカスタマイズ/運用を Moodle に対して行うことで、柔軟な LMS 運用を可能にしている。

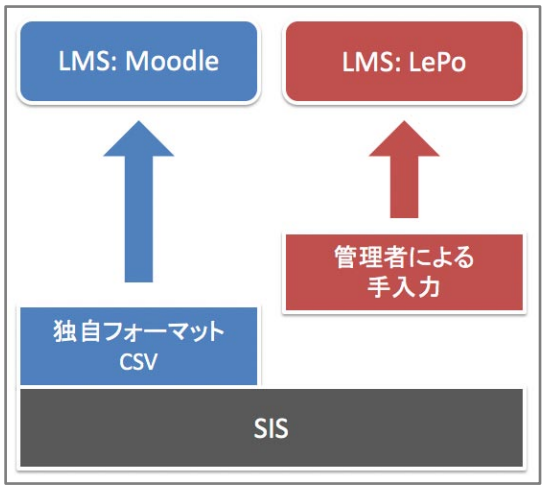


図 1　2018 年度前期までの学務情報の共有

表 1 SIS-Moodle 間で共有する情報

種別	共有する情報
ユーザ情報	氏名，ユーザ ID，メールアドレス
科目情報	開講年度，科目コード，科目区分（前期/後期など），開講科目名，時間割コード, 曜日コード, 時限，担当教員ユーザ ID, 開講所属コード，開講所属名
履修情報	履修年度，科目コード，時間割コード，履修学生ユーザ ID

表 2 学務情報連携に関する主な LMS カスタマイズ

項番	カスタマイズ内容
1.	**SIS に非登録の授業等の LMS コース登録** SIS 連携コースと管理者が LMS 上で作成したコースを区別して登録・運用
2.	**SIS に登録済み授業の LMS コース非表示** SIS 連携で非表示になったコースと管理者が LMS 上で非表示にしたコースの区別
3.	**SIS に非登録の教員・学生の LMS 登録** SIS 連携で登録した各コースの教員 / 学生と LMS 上で登録したそれの区別

3.3　2018 年度後期以降の SIS-LePo の取り組み

前述の本学における 2018 年度前期までの取り組みでは、以下の 2 つの問題点があった。

独自フォーマット CSV の利用: 本学独自の CSV 形式で情報共有をしているため、SIS/LMS のシステム更新や他システムで学務情報が必要となる度に、本学独自のカスタマイズが発生

連携情報に合致しない LMS 利用: SIS/LMS 間で学務情報を連携する際には、連携する LMS ごとに表 2 で述べたカスタマイズが発生

この 2 つの問題点を解消するため、OneRoster 規格に基づいた以下の情報共有を、2018 年度後期から試験的に実施する。なお、この取り組みでは、学務情報システム CampusSquare と学習支援システム LePo を用い、同学務情報システムと Moodle の情報共有は、3.2 節で述べた手法から 2018 年度中の変更は予定していない（図 2）。

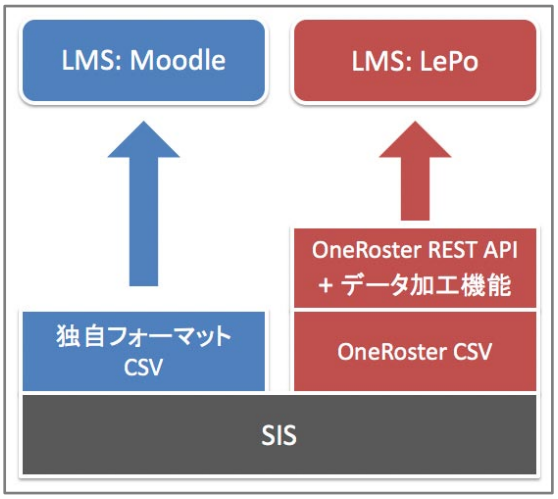


図 2　2018 年度後期以降の学務情報の共有計画

OneRoster 規格に基づいた CSV ファイルの提供

本学で運用する SIS（CampusSquare）のシステム更新に併せて、従来の独自形式の CSV ファイルに加え、OneRoster 規格に基づいた CSV ファイルも、2018 年 9 月より提供を開始した。両形式の CSV ファイルは、SIS から指定したサーバに対して毎日 1 回提供する。OneRoster 規格に基づく CSV ファイルでは、OneRoster v1.1 の必須項目は全て記述する一方、記述する科目の情報は当該年度のみを対象とし、それらの情報を OneRoster のバルク形式の CSV ファイルで提供した。この CSV ファイルの記述内容は表 1 と同等の情報を含み、このことはこれまで SIS-Moodle 間で行ってきた連携処理も、今後、OneRoster 規格の CSV ファイルに移行可能であることを意味する。

OneRoster 規格に基づいた REST API の提供

CSV ファイルの状態では、SIS が直接提供する学務情報を教育機関内で広く活用することが難しい。このため、OneRoster 規格に基づいた CSV ファイルを読み込み、同規格の REST API 仕様に基づき学務情報を JSON データとして提供する API サーバを開発した。この API サーバは、現在、OneRoster 規格で記述可能な全ての情報には対応していないが、3.2 節で Moodle に対して述べたコースとコースメンバーに対する日次処理を実行するのに必要な情報には対応している。

データ加工をした OneRoster REST API の提供

SIS が直接提供する学務データには合致しないコースやコースメンバーでの LMS 利用も想定される場合、学務データを利用する各々のシステムで、表 2 で示したようなカスタマイズを行うのは、作業の重複になり非効率である。このため本研究では、表 2 で示した 1. 及び 2. に対応する LMS 上のコース利用に変更がある場合は、OneRoster REST API サーバの設定ファイルに変更事項を記載することで、その事項を反映した JSON ファイルを応答する簡易的なデータ加工機能を実装した。これにより対象とする学期で、OneRoster REST API が提供するコース情報に完全に同期した状態で、LePo のコース運用を可能にした。

LePo での OneRoster REST API の活用

学習支援システム LePo では、前述の簡易なデータ加工機能を含む OneRoster REST API を利用することで、これまで Moodle に対して実現してきた、SIS に登録された授業及びその担当教員・履修学生を、LMS 上のコース及びコースメンバーに反映することを可能にした。現状では、SIS が提供する OneRoster CSV ファイルは日次で更新しているため、LePo から OneRoster REST API へのアクセスも日次処理として行った。

4 まとめ

本研究では、これまで本学独自の手法でのみ学務情報の連携をしてきた SIS-LMS に対して、国際標準規格である OneRoster v1.1 を用いた連携手法も試験的に導入した。提案した手法では、SIS が直接提供する OneRoster 規格に基づく CSV ファイルのデータを変換し、同規格に基づく REST API として学務情報を提供する API サーバを構築するこ

とで、情報の効率的な活用を可能にした。また、API サーバに簡易なデータ加工機能を実装したことで、学務情報の柔軟な活用も可能である。なお、本研究では、IMS Global が提供する OneRoster の仕様情報に基づき、OneRoster 規格に基づくバルク形式の CSV ファイル及び REST API を構築したが、これらの取り組みに対して、IMS Global から OneRoster 規格の仕様を満たしたことを、認証されたわけではない。

今後の課題としては、現在、OneRoster 規格に従った CSV ファイルを REST API に変換する以外には、簡易なデータ加工機能のみ実装している OneRoster REST API サーバの機能を改善し、学務情報を必要とする学内の各種 Web アプリケーションやネイティブアプリケーションに、安全で効率的に、かつ柔軟に情報を提供する API サーバとして機能改善をすることが挙げられる。

謝辞

Moodle の運用では日頃よりご協力頂いております、安徳恭彰先生をはじめとする医学情報センターのスタッフの方々、及び情報基盤センターのスタッフの方々に感謝いたします。

参考文献

[1] “OneRoster and Learning Information Services”, https://www.imsglobal.org/activity/onerosterlis
[2] “IMS Learning Information Services Overview”, https://www.imsglobal.org/ims-learning-information-services-overview
[3] “Moodle”, https://moodle.org/
[4] “Canvas by Instructure”, https://www.canvaslms.com/
[5] “OneRoster Certified Products”, https://www.imsglobal.org/ cc/statuschart/oneroster
[6] “CAMPUSSQUARE”, https://www.nssol.nssmc.com/solution/popup/campussquare/
[7] 吉崎弘一, “学習支援システムの更新について”, 大分大学情報基盤センター広報誌, vol.37, pp.8-9
[8] “LePo”, https://lepo.info
[9] “ALC NetAcademy NEXT”, https://www.alc-education.co.jp/nanext/

Web メールの国別認証制限

情報セキュリティ強化の一環として、本学で運用する Web メール（DEEPMail）には国別認証制限を導入しています。特に日本国外から Web メールを利用する予定のある学生・教職員は、下記事項を踏まえて国別認証制限の設定をご確認ください。

【国別認証制限とは？】

国別認証制限とは、予め許可した国のネットワークからのみ、Web メールの利用を許可する機能です。これにより、許可していない国からの不正なメール利用を未然に防いでいます。同機能では Web メールシステムへのログインに加え、外部メーラーからの Web メール利用（SMTP-AUTH / POP3 / IMAP4）も対象になります。初期設定では許可国として「日本」のみ許可しており、**許可国を追加するには未許可国への渡航前に、既に許可している国のネットワークから Web メールシステムにログインし、許可対象国を追加しておく必要があります**（下図）。

認証許可対象国の追加・解除操作：「オプション」＞「個人環境の設定」＞「国別認証制限」から設定

【国別認証制限の注意点】

この国別認証制限に関して、以下の点にご注意ください。

- 情報セキュリティの確保のため、**帰国後不要になった許可対象国については、速やかに登録を解除**してください。解除は登録と同じ画面から行うことができます。
- **航空機内の無線 LAN サービスや一部の SIM カードでは、滞在している国と国別認証制限の判定に用いる IP アドレスの示す国が異なることがあります**のでご注意下さい。
- 現在、Web メールにワンタイムパスワードを用いた二段階認証を導入することを検討しています。この二段階認証の導入後は、国別認証制限の設定を変更する可能性があります。設定を変更する際は、情報基盤センターWeb ページ等で予め周知いたします。

e-learningによる情報セキュリティ研修及び標的型メール攻撃訓練の実施報告

学術情報課　隅田 寿夫

１．初めに

大分大学では情報セキュリティ対策基本計画で定めた３か年計画に基づく取り組みとして、教職員を対象とした e-learning による情報セキュリティ研修及び標的型メール攻撃訓練を毎年度実施している。

実施３年目となる平成30年度の実施状況について報告を行う。

２．e-learningによる情報セキュリティ研修について

１）　利用教材について

情報基盤センターが提供している日本データパシフィック株式会社作成の「INFOSS 情報倫理」（速習版）を利用している。

本教材は毎年度、内容の見直しが行われており、本年度は2018年度版を利用した。

２）　実施方法について

情報基盤センターが運用する学習支援システムである Moodle を利用した e-learning 形式により実施した。

各教職員が大学で発行した個人アカウントで Moodle にログインし、教材による学習と 20 問からなる修了テストを受験することを研修完了の要件とした。

３）　研修対象者について

大分大学が発行した個人メールアカウントを持つ全教職員を対象とした。

４）　まとめ

平成30年度の研修受講率は全体で約94%であった。昨年、一昨年と比較して受講率は増加しており、教職員の情報セキュリティに対する意識が向上していることが伺える結果となった。

受講率を上げるための方策として、受講期間の延長、各部局長宛ての未受講者リストの送付及び未受講者本人に対するメールでの直接の受講依頼を行なった。

本研修は研修対象者が全員受講することを目標に来年度以降も継続して実施する予定である。

来年度に向け、さらに受講率を向上させるための取り組みとして未受講者に対する何らかのシステム利用制限や、より簡便に研修を受講できる工夫が必要と考えている。

また、英語版教材の提供を含めた新規教材の導入等の検討を行う予定である。

２．標的型メール攻撃訓練について

１）　実施方法について

民間業者が提供している標的型メール訓練支援サービスを利用し実施した。

対象となるメールアカウント宛てにＵＲＬ方式のフィッシングメールを模した訓練メールを送信し、メール本文中のＵＲＬをクリックした場合は別画面に誘導し、誘導先の画面で注意喚起を行った。

２）対象とした訓練メールの送付先について

大分大学が発行したすべての個人・組織メールアカウント宛てに送付した。

３）訓練メールの内容について

実際に不審メールとして注意喚起が行われているソフトウェアライセンスの不正利用の疑いに対する警告を装い、本文中のＵＲＬリンクをクリックするように促すフィッシングメールを模した内容とした。

なお、使用する企業名称等は実在する名称の一部分を変更し、架空の名称を用いた。

４）まとめ

訓練メール本文のＵＲＬリンクをクリックしたユーザの割合は全体の約 9.5%であった。

メールの内容が異なるため、単純な比較はできないが前年度に比べて、クリックしたユーザの割合は減少しており、これまでの訓練の成果が伺われる結果であった。

次年度以降も継続して訓練の実施を予定しており、他機関等の実施例も参考として、実施方法の改善を行う予定である。

Web サーバへのサーバ証明書の適用

Web サーバにサーバ証明書を適切に用いることで、Web ブラウザと Web サーバ間の安全な情報送信を可能にし、Web ページの信頼性も向上させることができます。最近では Chrome ブラウザで証明書を用いない http://から始まる URL の Web ページにアクセスすると、「保護されない通信」という警告が表示されます（図 1）。**oita-u.ac.jp ドメインで運用する Web サーバには、情報基盤センター / 医学情報センターに申請することでサーバ証明書を無償取得できます**ので、Web サーバ管理者の方は積極的にご活用下さい。

図 1 Chrome ブラウザ（v72）で http://から始まる URL の Web ページを表示した際の警告

【本学のドメインで運用する Web サーバで無償利用可能なサーバ証明書】

本学の教職員から情報基盤センターに申請することで、oita-u.ac.jp ドメインで利用可能なサーバ証明書を、国立情報学研究所が運用するサービスから無償取得できます。**このサーバ証明書は実在証明型（OV：Organization Validation）であり、その Web サーバの管理組織が日本国内に実在する大分大学、及び本学の特定部署であることを証明**します（図 2）。

図 2 情報基盤センターで利用する実在証明型サーバ証明書

なお、Internet Security Research Group が運用する Let's Encrypt サービス等からもサーバ証明書を無償取得できますが、これらの多くはドメイン認証型（DV: Domain Validation）証明書であり、管理組織は証明しません。このため、**本学ドメインで運用する Web サーバでは、原則として、より高い信頼性がある上記の実在証明型サーバ証明書を申請の上、ご利用下さい**。

【サーバ証明書の申請方法】

前述の実在証明型サーバ証明書の申請方法は、Web サーバの種類に応じて以下の 2 種があります。なお、どちらの申請方法でも、サーバ証明書の有効期限は発行日から 25 ヶ月後になります。

1. **情報基盤センター / 医学情報センターが提供する Web ホスティングサービスで運用する Web サーバ**

   本学に在籍する常勤の教職員から情報基盤センター/医学情報センター宛てに、以下の情報と共にメールで申請して下さい。下記 2.の場合とは異なり、ご連絡の際に TSV ファイルを提出する必要はありません。

   - 管理者氏名
   - 管理者所属
   - 管理者メールアドレス
   - 証明書を使用する部局等の名前(英語表記)
   - 証明書をインストールする Web サーバの FQDN

2. **上記以外の Web サーバ**

   以下の Web ページをご確認の上、サーバ証明書の発行申請をしてください。なお、**申請には当該 Web サーバでの操作を伴う TSV ファイルの作成が必要**です。Web サーバの管理を外部企業に委託し、TSV ファイルの生成を同企業に依頼できる場合であっても、情報基盤センターへの証明書発行申請は、本学に在籍する常勤の教職員から行ってください。

電子証明書申請ページ	https://www.cc.oita-u.ac.jp/app/page-1002/page-1034/

委員会名簿(2018.4.1 現在)

学術情報拠点

役職名等	氏名	任期
拠点長	古城 和敬	2017. 10. 1～2019. 3. 31
副拠点長（情報基盤センター担当）	吉田 和幸	2018. 4. 1～2020. 3. 31
副拠点長（医学情報センター担当）	安徳 恭彰	2018. 4. 1～2020. 3. 31

学術情報拠点運営会議

役職名等	氏名	任期
拠点長	古城 和敬	2017. 10. 1～2019. 3. 31
副拠点長（医学図書館担当）	岸田 哲子	2018. 4. 1～2020. 3. 31
副拠点長（情報基盤センター担当）	吉田 和幸	2018. 4. 1～2020. 3. 31
副拠点長（医学情報センター担当）	安徳 恭彰	2018. 4. 1～2020. 3. 31
学術情報室長	中島 誠	2017. 11. 16～2019. 11. 15
情報基盤室長	真鍋 正規	2017. 11. 16～2019. 11. 15
専任教員	吉崎 弘一	2015. 4. 1～
教育学部　准教授	衛藤 裕司	2018. 4. 1～2020. 3. 31
経済学部　講師	越智 学	2017. 4. 1～2019. 3. 31
理工学部　教授	工藤 孝人	2017. 4. 1～2019. 3. 31
医学部　教授	石崎 敏理	2018. 4. 1～2020. 3. 31
福祉健康科学部　教授	大杉 至	2018. 4. 1～2020. 3. 31
研究・社会連携部長	堀池 幸浩	2018. 4. 1～

情報基盤専門委員会

役職名等	氏名	任期
拠点長	古城 和敬	2017.10. 1～2019. 3.31
副拠点長（情報基盤センター担当）	吉田 和幸	2018. 4. 1～2020. 3.31
副拠点長（医学情報センター担当）	安徳 恭彰	2018. 4. 1～2020. 3.31
情報基盤室長	真鍋 正規	2017.11.16～2019.11.15
専任教員	吉崎 弘一	2015. 4. 1～
協力教員（情報基盤担当）	池内 秀隆	2017.11.16～2019.11.15
教育学部　教授	市原 靖士	2018. 4. 1～2020. 3.31
経済学部　教授	豊島 慎一郎	2018. 4. 1～2020. 3.31
理工学部　教授	園井 千音	2017. 4. 1～2019. 3.31
福祉健康科学部　助教	川上 健二	2018. 4. 1～2020. 3.31
医療情報部長	下村 剛	2018. 4. 1～
医学部医学科　教授	谷川 雅人	2018. 4. 1～2020. 3.31
医学部看護学科　教授	井上 亮	2018. 4. 1～2020. 3.31
学術情報課長	黒栁 裕子	2017. 4. 1～

情報基盤室

役職名等	氏名	任期
情報基盤室長 協力教員（情報基盤担当）	真鍋 正規	2017.11.16～2019.11.15
専任教員（情報基盤担当）	吉田 和幸	2018. 4. 1～2020. 3.31
協力教員（情報基盤担当）	市原 靖士	2017.11.16～2019.11.15
協力教員（情報基盤担当）	池内 秀隆	2017.11.16～2019.11.15

情報基盤専門委員会　広報部会

役職名等	氏名	任期
副拠点長（情報基盤センター担当）	吉田 和幸	2017. 1. 1～2018.12.31
副拠点長（医学情報センター担当）	安徳 恭彰	2017. 4. 1～2018.12.31
学術情報拠点　准教授	吉崎 弘一	2017. 1. 1～2018.12.31
教育学部　教授	甘利 弘樹	2017. 1. 1～2018.12.31
経済学部　准教授	柴田 茂紀	2017. 1. 1～2018.12.31
理工学部　教授	園井 千音	2017. 1. 1～2018.12.31
福祉健康科学部	栄留 里美	2017. 4. 1～2019. 3.31
医学部　准教授	下田 恵	2017. 1. 1～2018.12.31
情報基盤センター技術職員	矢田 哲二	2017. 1. 1～2018.12.31

委員会／会議(2017 年 4 月～2018 年 3 月)

2017 年

4 月	21 日	大学 ICT 推進協議会理事会（TV 会議）
5 月	18 日	大学 ICT 推進協議会 2017 年度通常総会
	30 日	文部科学省関係機関最高情報セキュリティ責任者会議
6 月	23 日	第 14 回国立大学法人情報系センター協議会総会〔徳島大学〕
	24 日	IOT 研究会（通算 38 回）〔徳島大学〕
7 月	11 日	第 1 回学術情報拠点運営会議
9 月	1～2 日	2017 年度 IS 研九州ブロック研究会
	15 日	大学 ICT 推進協議会理事会（TV 会議）
	22 日	第 2 回学術情報拠点運営会議
	25 日	第 12 回国立大学法人情報系センター研究集会〔岡山大学〕
	26 日	第 21 回学術情報処理研究集会〔岡山大学〕
10 月	30 日	第 3 回学術情報拠点運営会議
12 月	6 日	第 4 回学術情報拠点運営会議
	7･8 日	第 10 回インターネットと運用技術シンポジウム〔熊本市国際交流会館〕
	13～15 日	大学 ICT 推進協議会 2017 年度年次大会〔広島国際会議場〕
	20 日	第 47 回九州大学情報基盤研究開発センター全国共同利用運営委員会

2018 年

1 月	26 日	第 5 回学術情報拠点運営会議
2 月	16 日	第 6 回学術情報拠点運営会議（メール会議）
	28 日	Ja Sakai/AXIES/IMS 合同カンファレンス 2018〔名古屋大学〕
3 月	5～6 日	第 26 回国公立大学情報システム研究会総会
	9 日	第 7 回学術情報拠点運営会議（メール会議）
	22 日	大学 ICT 推進協議会理事会（TV 会議）
	23 日	第 8 回学術情報拠点運営会議

2017 年度業務記録（情報基盤センター業務）

業務日誌

2017 年 4 月～2018 年 3 月

[4 月] 新入生利用者 ID・利用ガイド配布
前期ゲスト ID 発行
学内進学者のメール転送受付
大学ホスティングサービスを学内サーバからさくらインターネットへ移行完了
Windows Vista 利用者に注意喚起

[5 月] 昨年度退職者、卒業生 ID 停止
基盤情報システム入替にともない、メールサーバを新規サーバに移行
SymantecEndpointProtection バージョンアップ(12.1 RU6 MP7)

[6 月] 昨年度退職者、卒業生 ID 削除
教育情報システム Windows サーバのセキュリティアップデート実施

[7 月] 大学無線 LAN システム FEREC ファームウェア更新

[9 月] 技術職員研修

[10 月] 後期ゲスト ID 発行
Symantec Endpoint Protection バージョンアップ(14 RU1 MP2)
学習支援システム WebClass 運用終了
前期離籍学生 ID 停止
文部科学省主催平成 29 年度情報セキュリティ技術向上研修（技術職員 1 名参加）
情報基盤専門委員会広報部会

[11 月] 前期離籍学生 ID 削除
学外からの SSH アクセスに関する注意喚起

[1 月] 平成 30 年度情報基盤センター実習室予約受付
Moodle STACK プラグイン導入

[2 月] 広報発行
VPN サービスの運用開始
定年退職予定者へ退職後の利用者 ID 利用についてを通知
サーバルームガスエアコン入替

[3 月] 大学無線アクセスポイント一部入替
新入生向け利用ガイド作成
INFOSS 情報倫理 2018 年度版 Moodle で研修開始
漏洩が疑われる利用者 ID に関する注意喚起

各種申請書受付件数

（件数）

（1）「プリンタ利用申請書」（様式第 1 号）	104
（2）「固定 IP アドレス申請書」（様式第 2 号）	268
（3）「実習室利用申請」※Web フォーム	62
（4）「Moodle コース作成申請」※Web フォーム	34
（5）「ワクチンソフト利用申請」※Web フォーム	176
（6）「ホスティングサービス利用申請書」（様式第 3 号）	11
（7）「ファイアウォール開放設定申請書」（様式第 4 号）	35
（8）「サブドメイン名申請書」（様式第 5 号）	4
（9）「サブネットワーク申請書」（様式第 6 号）	0
（10）「無線 LAN アクセスポイント設置申請書」（様式第 7 号）	41
（11）「一時インストール申請書」（様式第 8 号）	5
（12）「メーリングリスト申請書」（様式第 9 号）	31
（13）「進学生メール転送申請」※Web フォーム	41
（14）「利用者 ID の利用停止申請」※Web フォーム	38
（15）「電子証明書の発行申請」※メール	5

平成29年度業務記録（医学情報センター業務）	
4月	医学科・看護学科・大学院生・研修医オリエンテーション実施
	情報基盤システム更新(看護学科棟ＮＷ更新作業)
	第1回看護学科 自己・標本学習室検討会
5月	PC・USBデータの取り扱いに関する講習会(看護学科)
	臨大プロジェクターシステムサポート作業(図書館)
6月	自己学習室ネットワーク環境変更
	国立大学法人情報系センター協議会
	情報基盤システム更新(校舎講義棟実習棟ＮＷ更新作業)
	自己学習室・標本学習室使用方法評価会議看護学科講習会
	平成29年度国立大学法人情報系センター協議会総会
7月	管理棟ネットワーク環境変更
	情報処理実習室緊急メンテナンス
8月	基盤情報システム学生端末セキュリティメンテナンス作業(267台)
	情報基盤システム更新
	・図書館・卒後・臨床講義棟・福利施設・福利厚生棟ＮＷ更新作業
	・基礎臨床研究棟4Ｆ～8Ｆ・院生研究棟5Ｆ～8Ｆ ＮＷ更新作業
9月	情報基盤システム更新(基礎臨床研究棟1Ｆ～3Ｆ・動物ＲＩ棟・および院生研究棟１Ｆ ＮＷ更新作業)
	学生PCメンテナンス
	病院情報管理システムネットワークスイッチ仕様策定委員会
	平成29年度CBT試験打ち合わせ
	第12回国立大学法人情報系センター研究集会
	第21回学術情報処理研究集会
	IS研九州ブロック会議
10月	**編入生オリエンテーション実施**
	自己学習室・標本学習室使用方法評価会議看護学科講習会
	CBT試験環境構築（集中動作テスト）
	第2回看護学科 自己・標本学習室検討会
11月	
12月	情報基盤システム更新(付属病院施設NW更新)
1月	CBT試験環境構築2回（体験テスト、本試験）
	看護学科講習会(PCとUSBメモリーの利用方法講習会(2年生)
	第3回看護学科 自己・標本学習室検討会
2月	CBT試験**対応**(追試験)
3月	**附**属病院施設無線AP取替(49台)

◆病院再整備関係

＊病棟全体病院再整備LAN構築支援

挾間キャンパス（医学情報センター）の業務報告

■各種申請情報

1. 固定 IP アドレス申請・端末申請件数

件

PC 等	858
プリンタ	47
サーバ	3
テレビ会議	1
その他	15

2. その他申請 件

ワクチンソフト利用申請	875
ホスティングサービス利用申請	6
ファイアウォール開放設定申請	7
サブドメイン名申請	6
無線 LAN アクセスポイント設置申請 ※受け付けていません	なし
メーリングリスト申請	7
利用者 ID 利用停止申請	75
電子証明書発行申請	0
利用者 ID 発行申請・ユーザ登録件数	504
ワンデイアカウント申請	88

■学生端末

1. プリンタ利用状況 ページ

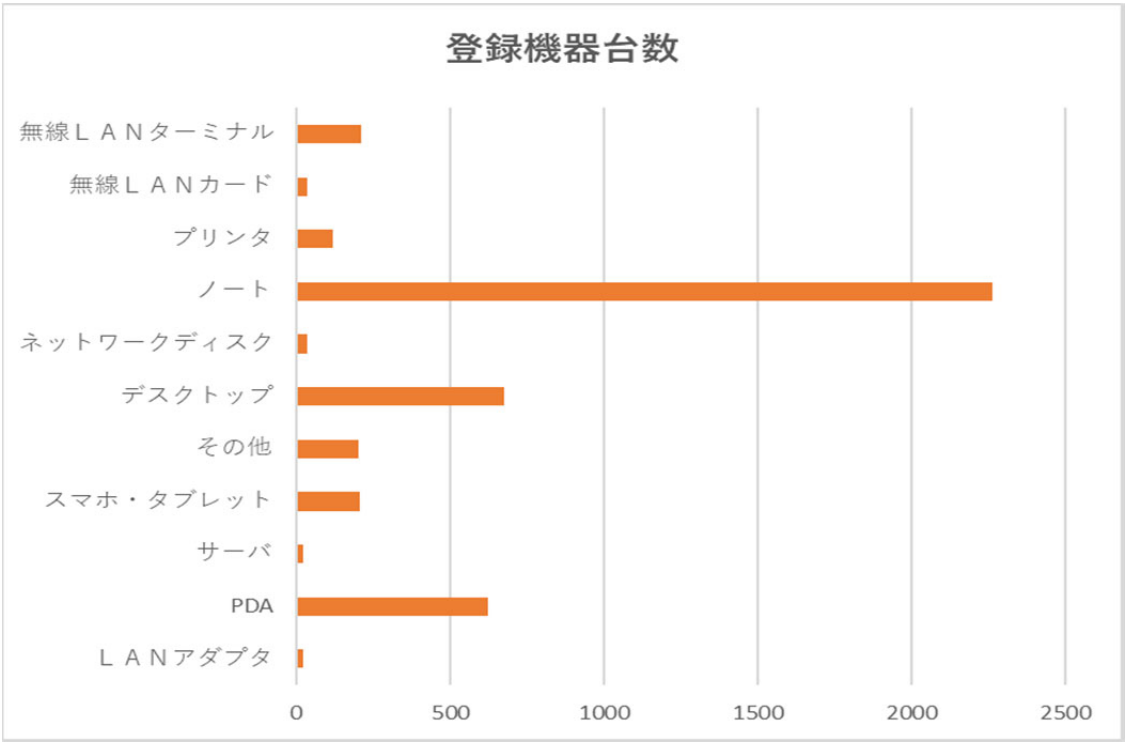
カラー・ページ数	117,011
モノクロ・ページ数	1,414,459
総ページ数	1,531,470
両面ページ数	1,019,942
片面ページ数	511,528

2. 端末平均利用時間 2.9 時間
貸出ノートパソコン 4.3 時間

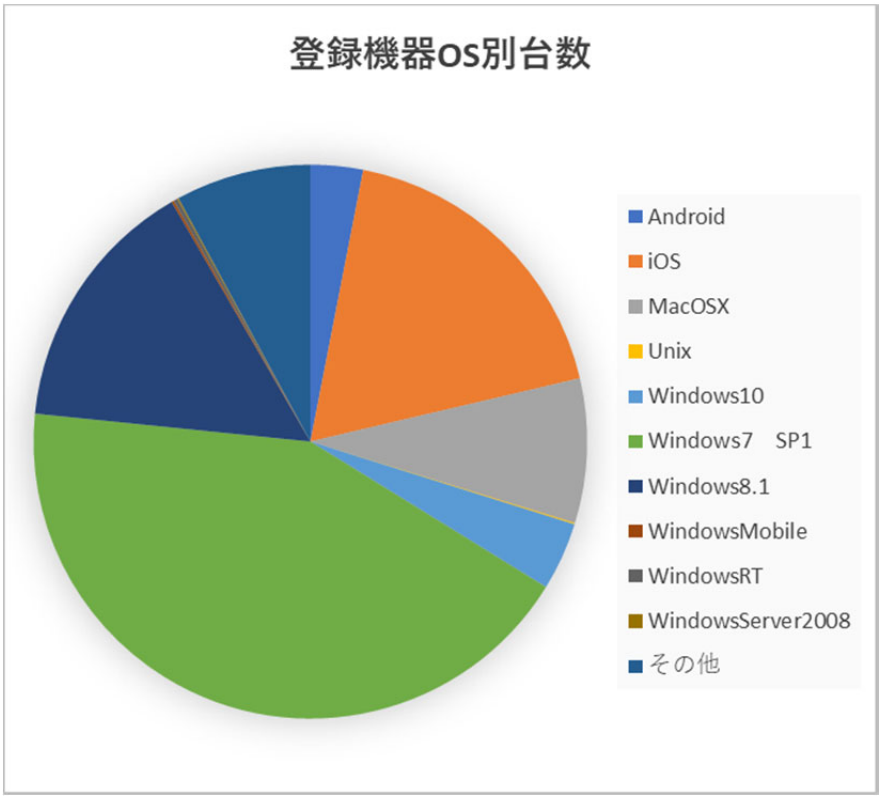
■挟間登録機器情報

機器名	台数
ＬＡＮアダプタ	24
PDA	621
サーバ	21
スマホ・タブレット	208
その他	201
デスクトップ	674
ネットワークディスク	36
ノート	2,263
プリンタ	118
無線ＬＡＮカード	36
無線ＬＡＮターミナル	209
合計	4,411

※無線 LAN ターミナルは、当センターが管理している機器です。



OS	台数
Android	116
iOS	691
MacOSX	319
Unix	3
Windows10	150
Windows7　SP1	1,620
Windows8.1	569
WindowsMobile	5
WindowsRT	9
WindowsServer2008	3
その他	299



基盤情報システムネットワーク更新（～2017.12.19）

今回基盤情報システム更新時期を迎えて、ネットワークセキュリティと研究施設の無線強化の為、大規模な更新を行いました。

■概要

従来の単一プライベートネットワーク構成では、接続台数の増加に応じプリンタ検索などのブロードキャストパケットがキャンパス全範囲に及びネットワークの帯域占有率が増加し、他の通信に影響を及ぼしていました。このため、小範囲の複数プライベートネットワーク構成に変更し、ブロードキャストパケットの到達範囲を絞って帯域を確保することにより、通信状況を改善しました。

挟間キャンパス学内 LAN は、内部をプライベートネットワークに区切り学外からの不正アクセス防止を行なっています。機器学内 LAN 接続に接続される機器は、MAC 認証（機器申請）および Web 認証（利用者 ID 申請）を経ることでインターネット利用が可能となります。

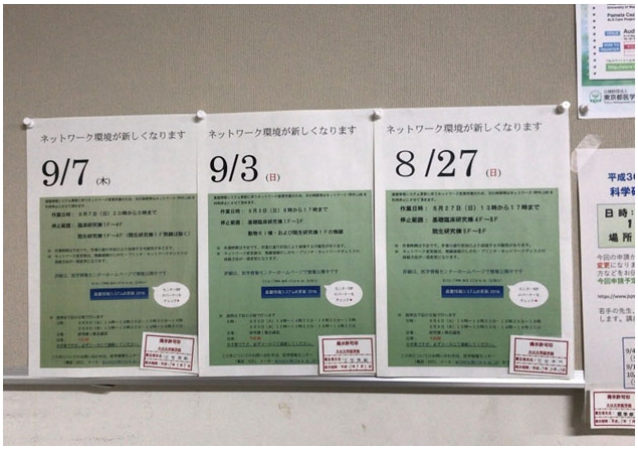
機器申請と ID 申請は、学内で従事するとみなされた職員のみになります。

■機器更新にかかる変更項目

1. 無線ＡＰ ・・・120 台から 152 台に増設
   - ・新規追加施設：東院会館，外国人宿舎
   - ・電波の弱い箇所には，小型 AP を設置
   - ・SSID を変更
   - ・VLAN が変わった場合のローミング機能を停止
2. ネットワーク認証・・・ほぼ現状通り、LDAP での認証後 16 時間使用継続可能
   認証画面を HTTPs に変更し、暗号化を行う
3. プロキシ・・・手動設定から自動取得に変更
4. ネットワーク体系・・・単一プライベートアドレスから小範囲の複数プライベートアドレスへ
   - ・プリンタ等の固定アドレス機器の設定変更が必要
5. 固定アドレス機器(647 台)
   - ・対象機器：プリンタ・NWHDD・サーバなど
   - ・変更内容：変更前)固定 IP アドレス手動設定→変更後)DHCP サーバから自動取得
6. 認証方式
   - ・MAC 認証（機器登録）と Web 認証（利用者登録）の併用
   - ・認証ロジック（別紙）

■変更内容の通知

- ・機器責任者(使用者)・所属に変更情報をメールにて連絡（計 3 回）
- ・NW 更新の説明会
  切替 9 カ所各 4 回程度説明会を開催
- ・ポスターの掲示(棟ごとの掲示板と各医局事務所の掲示版)



■VLAN 構成について

更新前 VLAN　41 個

更新後 VLAN　126 個（新規 85 個　継続　19 個　廃止　22 個）

■作業履歴

1. スケジュール

日　程	作　業	停止するサービス	停止時間と回数
2017 年 2 月 21 日～23 日	挟間の無線ＡＰの入替	通信	数分間の停止が 1 回
4 月 23 日	LAN 切替（看護学科棟・課外活動施設）	ネットワーク全般	8:30 - 10:30
6 月 15 日	LAN 切替（スキルスラボ・情報棟）	ネットワーク全般	7:00 - 13:00
6 月 25 日	LAN 切替（校舎講義棟）	ネットワーク全般	8:00 - 14:30
7 月 20 日	LAN 切替（管理棟）	ネットワーク全般	20:00 - 7:00
8 月 20 日	LAN 切替（図書館・卒後臨床研修センター棟・医療情報棟・福利施設・臨床講義棟・福利厚生棟）	ネットワーク全般	13:00 - 17:00
8 月 27 日	LAN 切替（基礎臨床研究棟 4 階・5 階・6 階・7 階・8 階）	ネットワーク全般	8:00 - 17:00
9 月 3 日	LAN 切替（基礎臨床研究棟 1 階・2 階・3 階））	ネットワーク全般	8:00 - 14:00
9 月 7 日	LAN 切替（院生研究棟・臨床研究棟 1 階・2 階・3 階・4 階）	ネットワーク全般	20:00 - 24:00
12 月 19 日	LAN 切替（付属病院施設）	ネットワーク全般	19:00 - 21:40

2. センター準備作業

・キャンパス全域無線 AP 入替前の周知

・認証除外機器の把握と整備

・NW 更新説明会の周知と開催準備(1 エリアに対して 1 か月前から作業

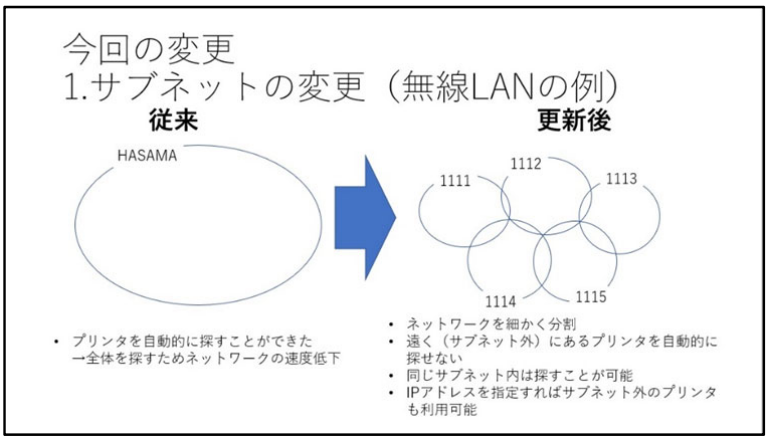
・事前の IP アドレス変更の説明の周知

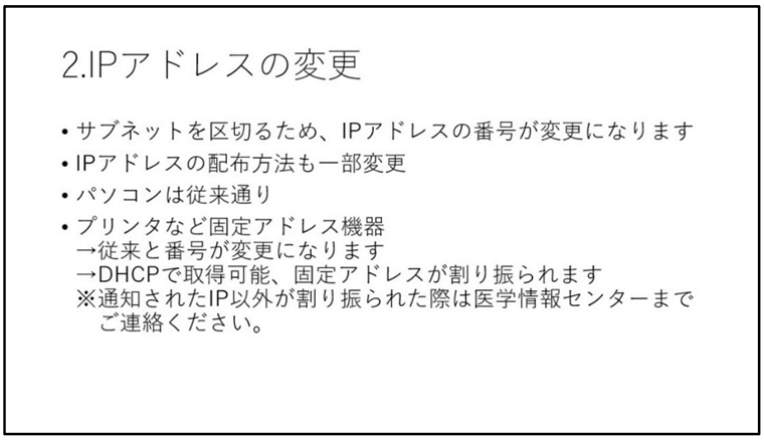
・機器登録情報の更新

3. 更新後

・無線システム NWHDD やプリンタなど認証除外機器への接続方法のご案内

■説明会時の説明資料





Moodle の利用促進に向けて

医学情報センターでは, Moodle の利用を促進するため, 2 つのことを行いました。

1．超簡易版マニュアルの作成とホームページ上への掲載

基本的な操作の流れについて記載したマニュアルを作成し,医学情報センターのホームページに掲載しました。

■内容

・Moodle のログイン

・参加コースの確認

・コース編集(教員/学生　追加)

・ファイルの追加

■掲載先の URL

http://www.med.oita-u.ac.jp/mic/moodle/how_to_moodle.pdf

2．Moodle 講習会

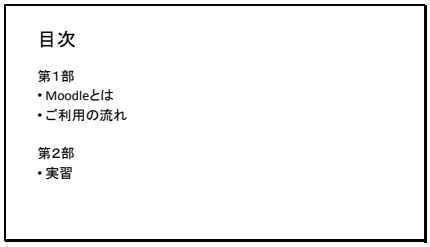
センターで運営中の学習支援用サイトを利用中の講座を対象に,Moodle の利用の仕方について知ってもらうための講習会を開催しました。当日は,前半に基本的な操作の流れを説明,後半に実際の操作を体験していただきました。

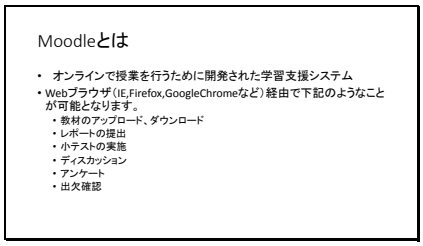
■内容

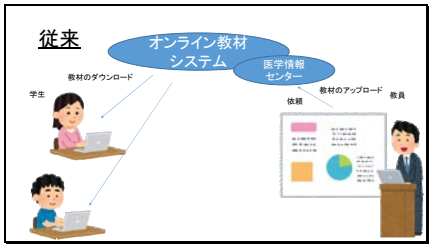
第 1 部　Moodle とは

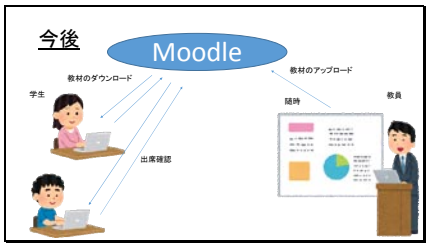
第 2 部　実際の Moodle 操作

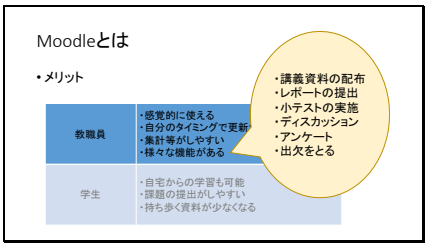
■説明資料

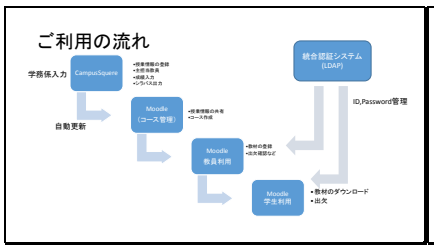


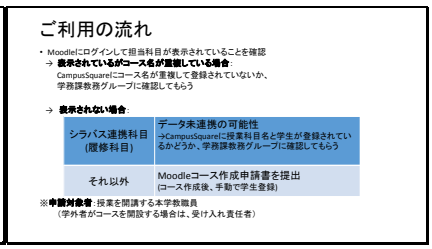








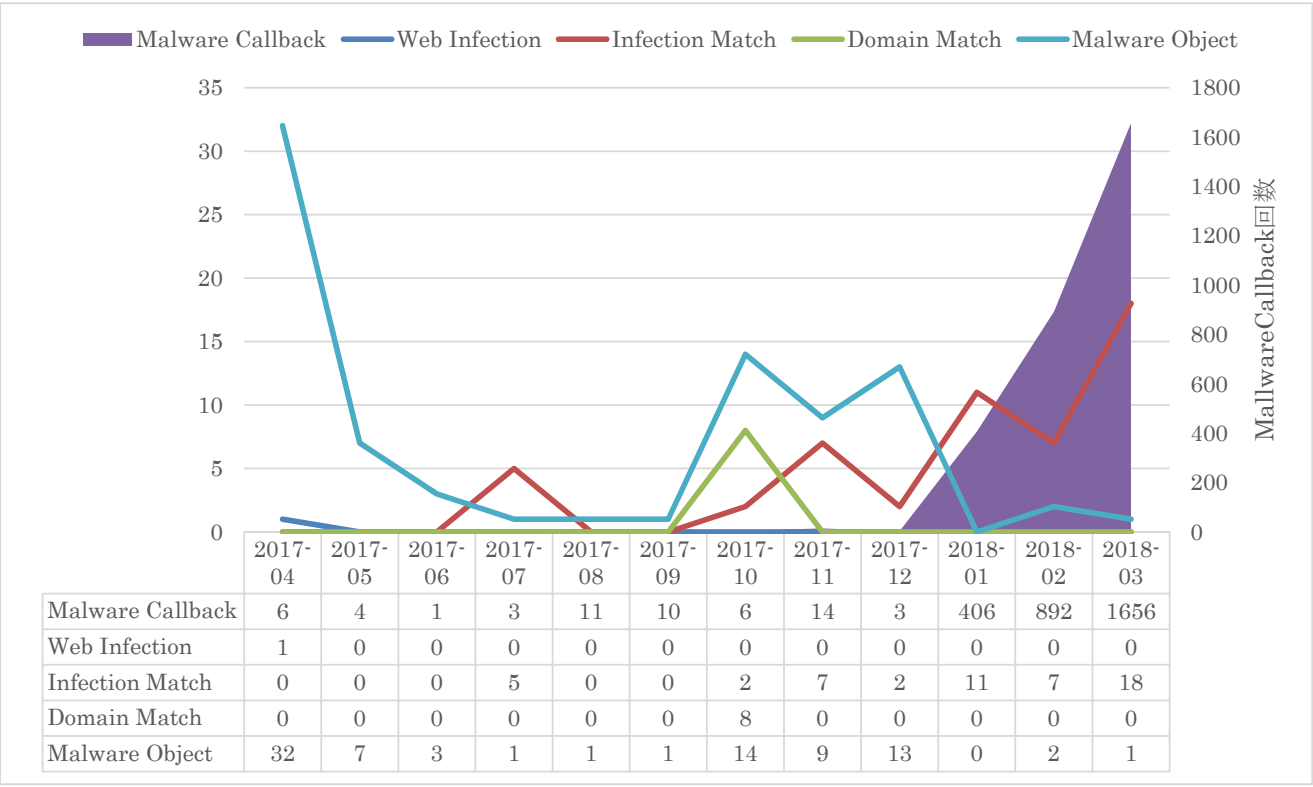




システム利用統計

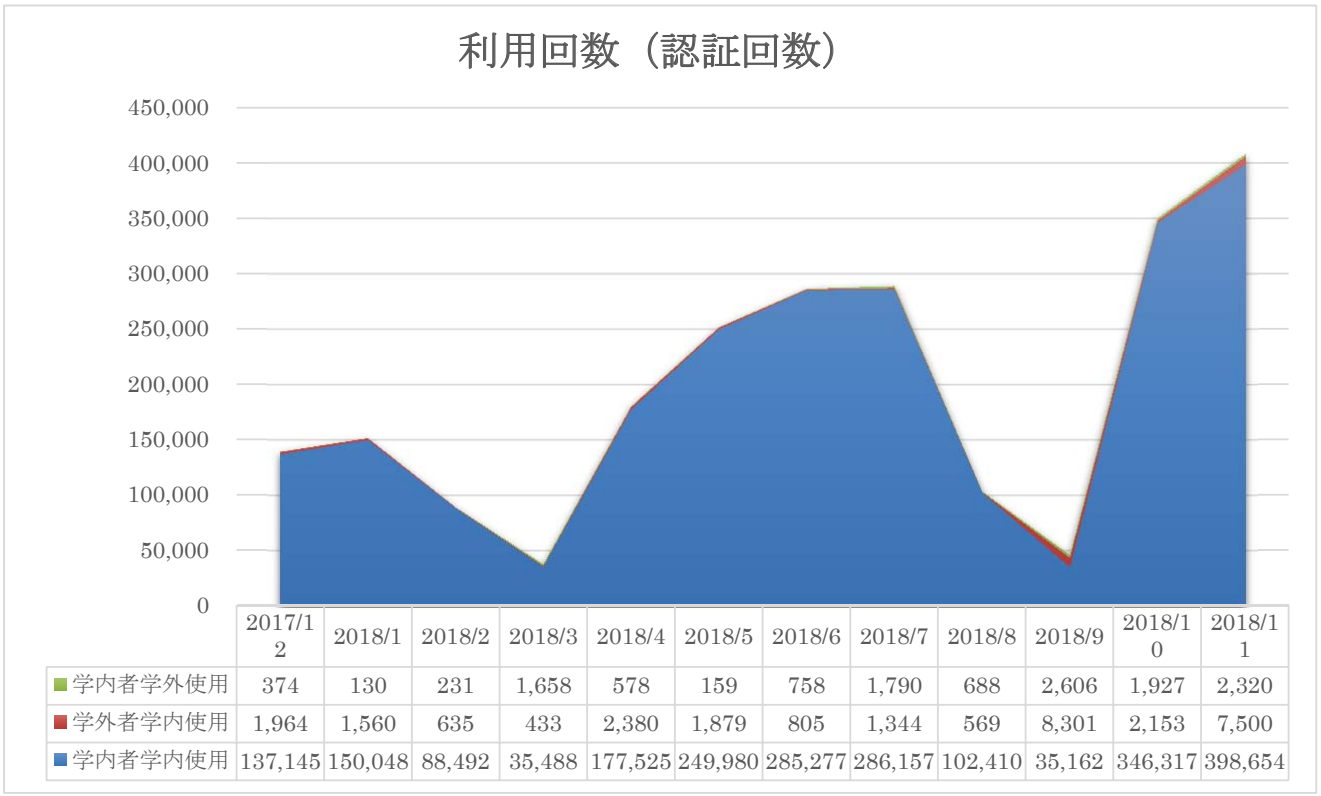
DEEPMail 送受信数（2017/4/1～2018/3/31）

サンドボックス検知状況（2017/4/1～2018/3/31）

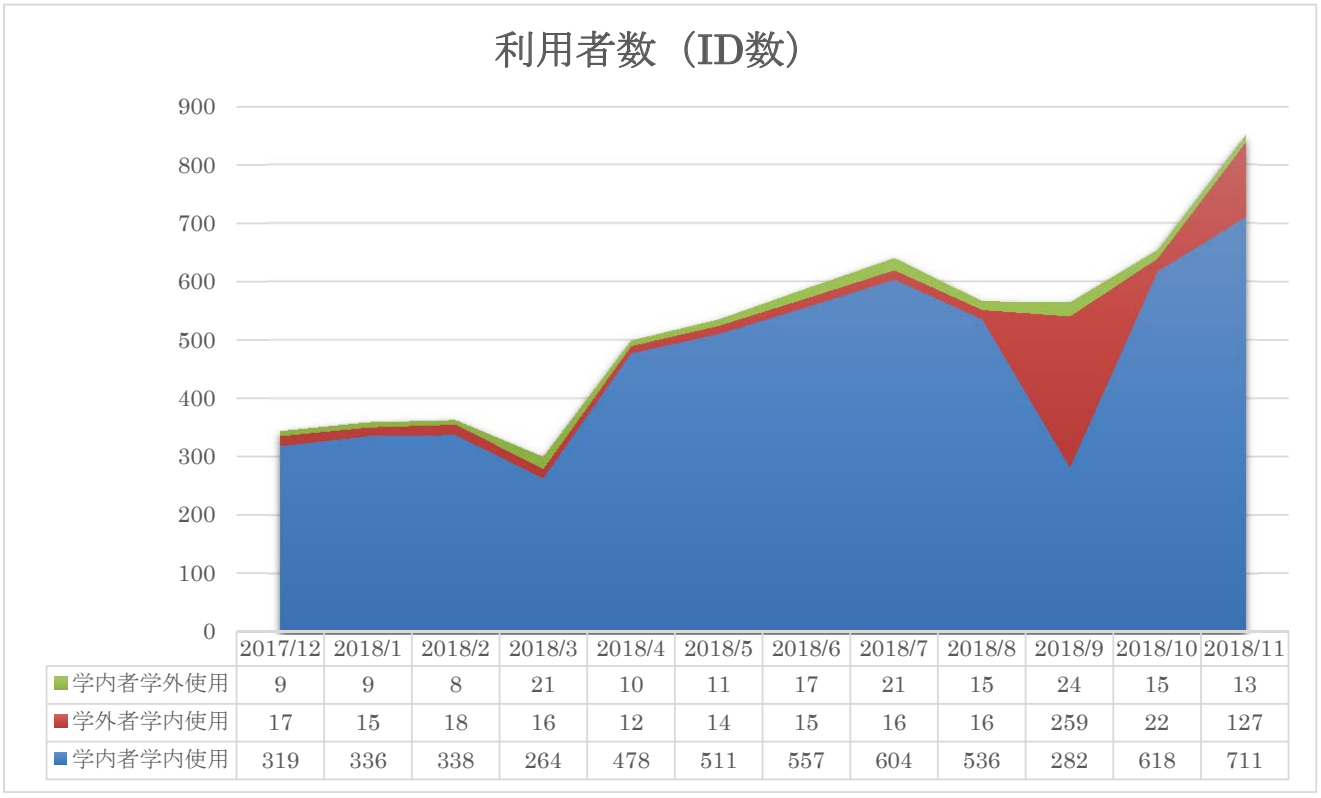


	2017-04	2017-05	2017-06	2017-07	2017-08	2017-09	2017-10	2017-11	2017-12	2018-01	2018-02	2018-03
Malware Callback	6	4	1	3	11	10	6	14	3	406	892	1656
Web Infection	1	0	0	0	0	0	0	0	0	0	0	0
Infection Match	0	0	0	5	0	0	2	7	2	11	7	18
Domain Match	0	0	0	0	0	0	8	0	0	0	0	0
Malware Object	32	7	3	1	1	1	14	9	13	0	2	1

eduroam 利用状況(2017/12～2018/11)

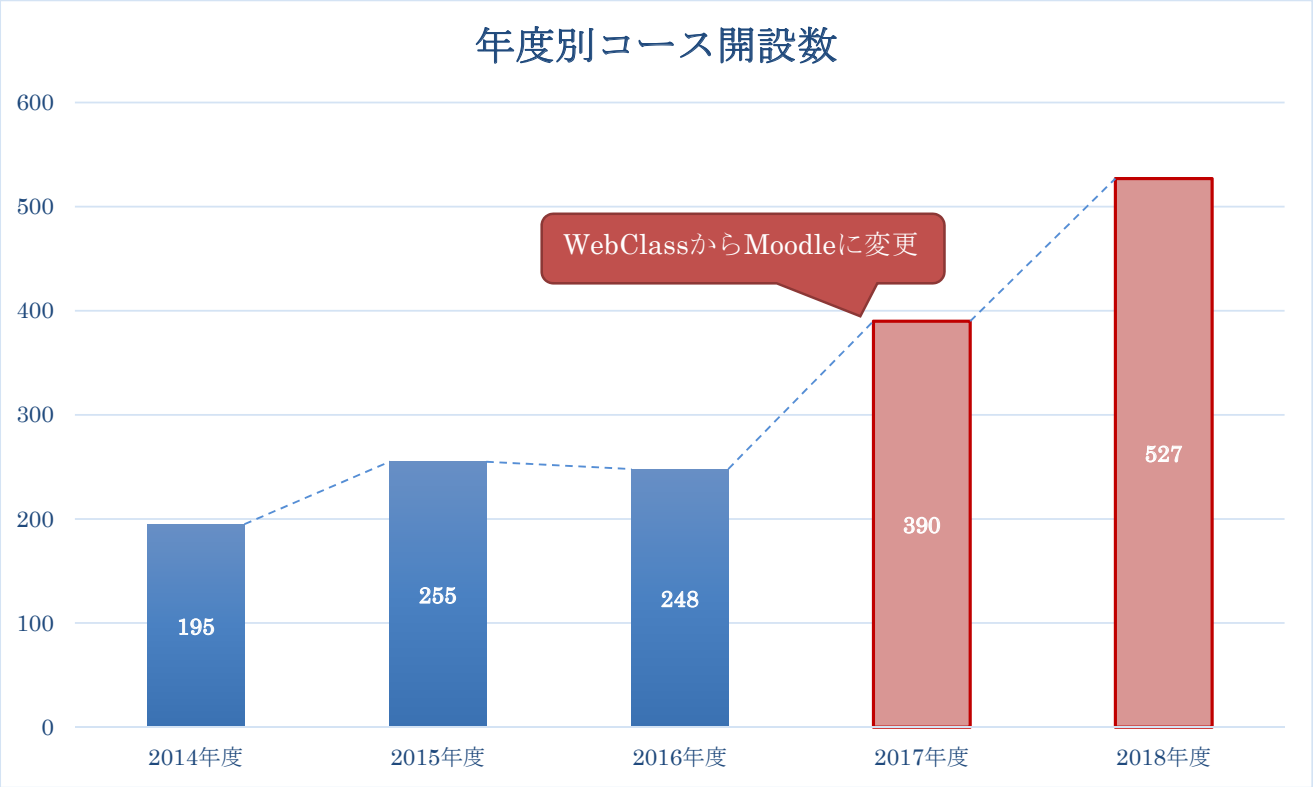


	2017/12	2018/1	2018/2	2018/3	2018/4	2018/5	2018/6	2018/7	2018/8	2018/9	2018/10	2018/11
学内者学外使用	374	130	231	1,658	578	159	758	1,790	688	2,606	1,927	2,320
学外者学内使用	1,964	1,560	635	433	2,380	1,879	805	1,344	569	8,301	2,153	7,500
学内者学内使用	137,145	150,048	88,492	35,488	177,525	249,980	285,277	286,157	102,410	35,162	346,317	398,654



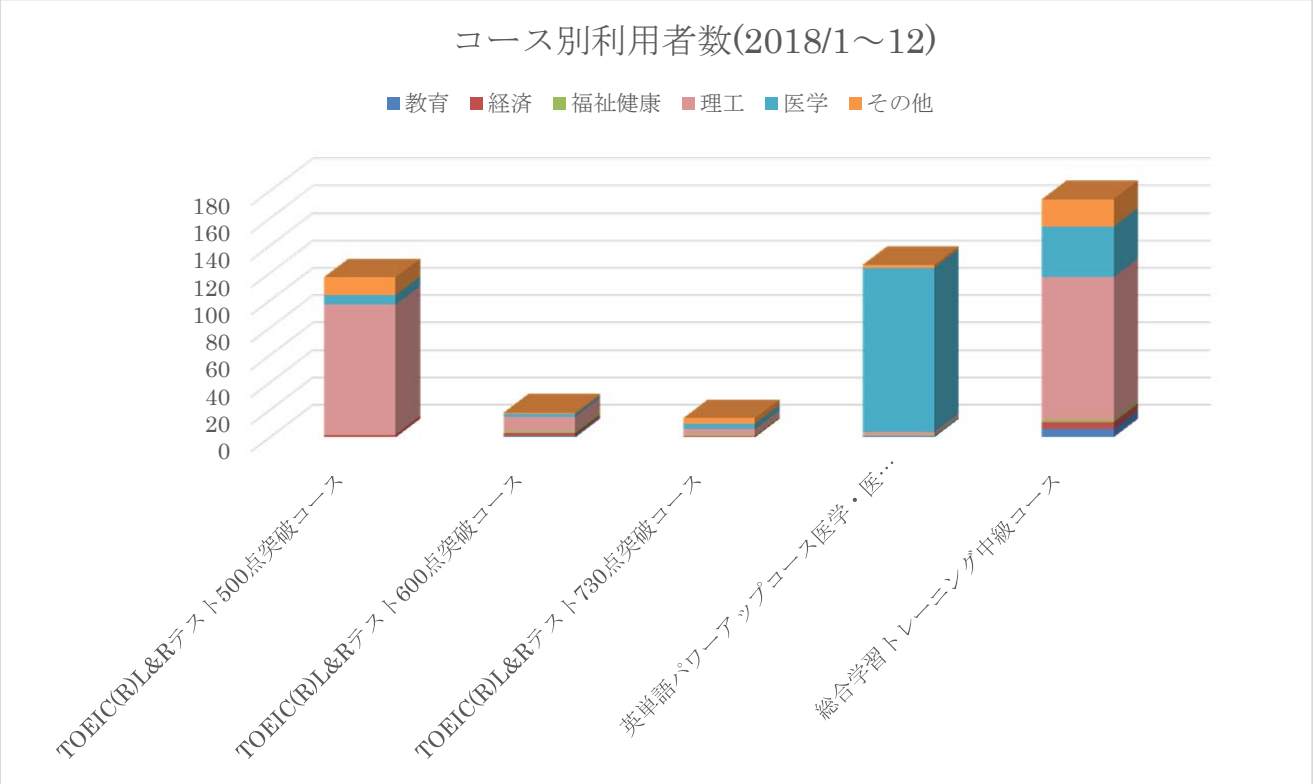
	2017/12	2018/1	2018/2	2018/3	2018/4	2018/5	2018/6	2018/7	2018/8	2018/9	2018/10	2018/11
学内者学外使用	9	9	8	21	10	11	17	21	15	24	15	13
学外者学内使用	17	15	18	16	12	14	15	16	16	259	22	127
学内者学内使用	319	336	338	264	478	511	557	604	536	282	618	711

学習支援システム利用状況（WebClass, Moodle）

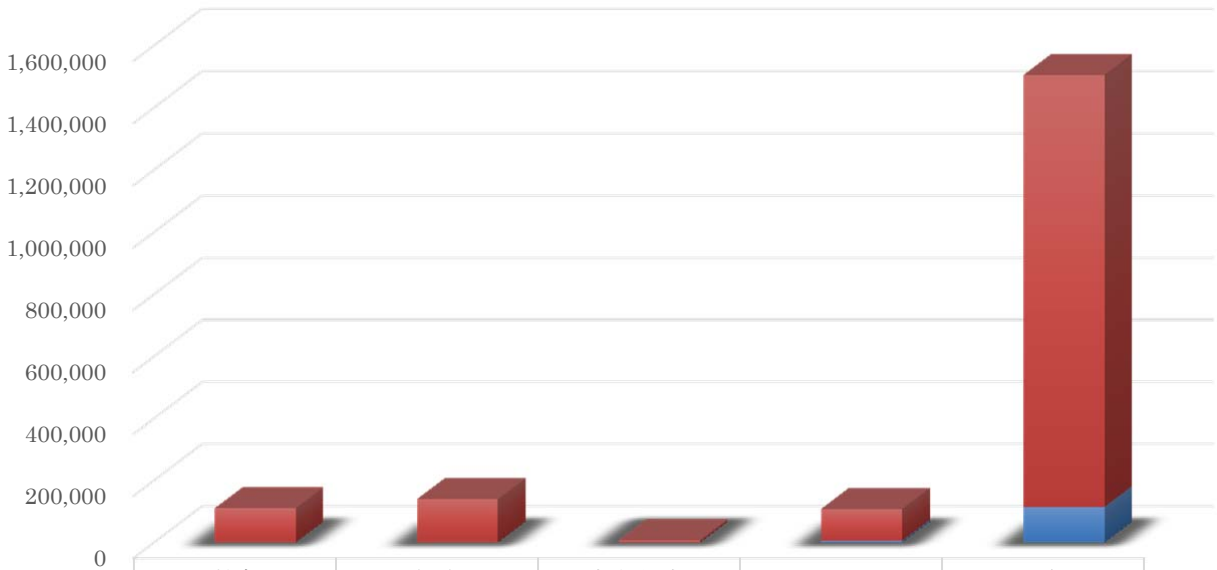


※教材が３個以上登録されているコースの数

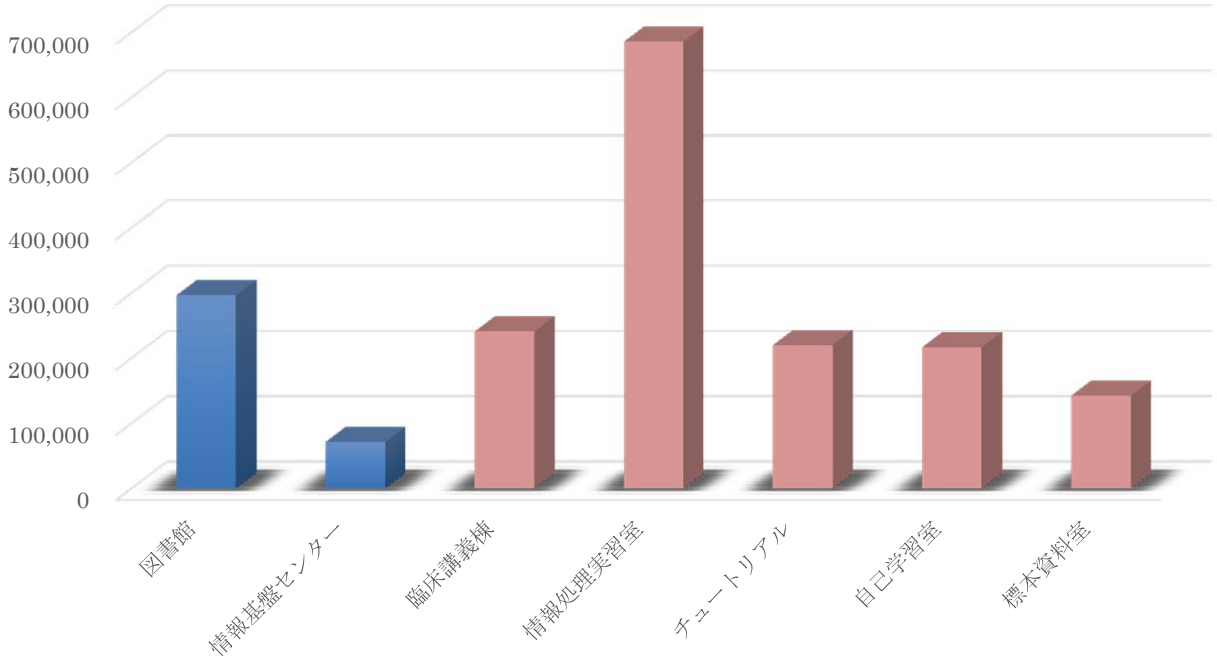
ALC NetAcademy 利用状況



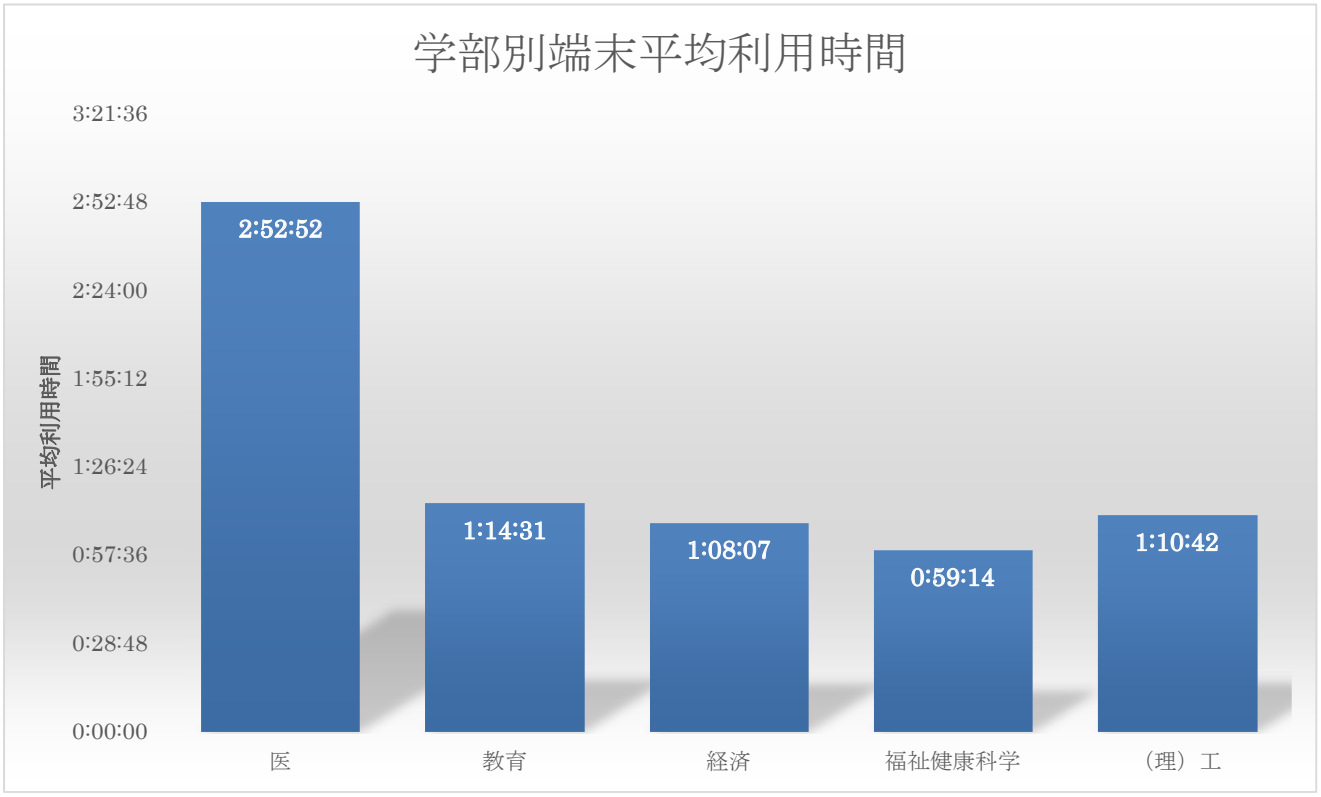
プリンタ利用状況



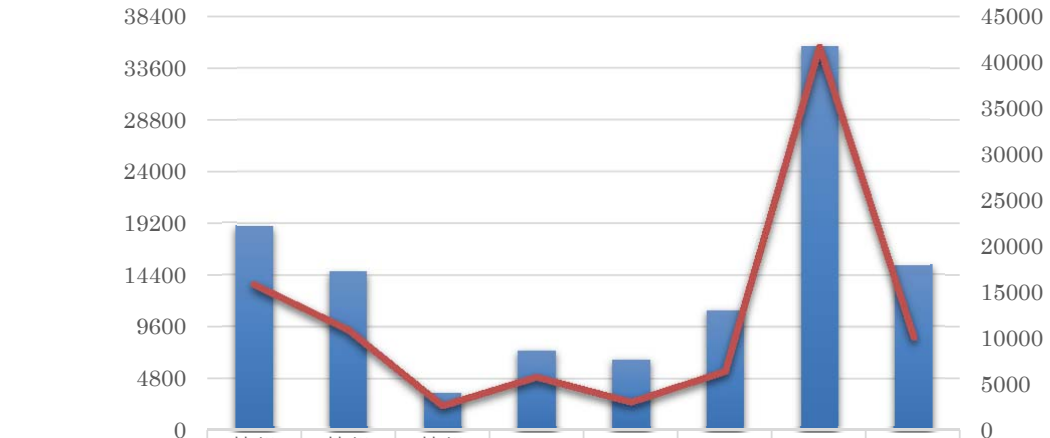
	教育	経済	福祉健康	理工	医学
白黒	109,766	139,354	7,867	102,701	1,389,814
カラー	745	391	0	5,806	114,795



教育情報システム端末利用状況（2017/4/1～2018/3/31）

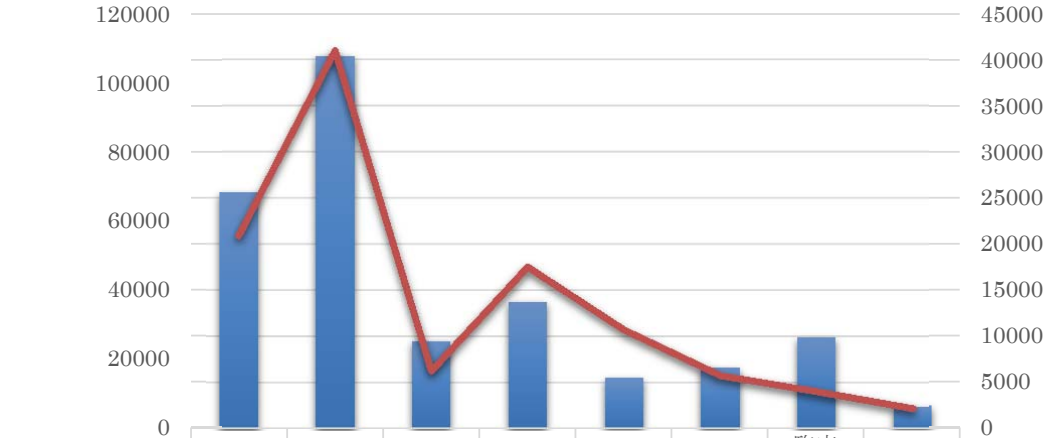


旦野原キャンパス実習室別端末利用状況



	情報基盤センター第1実習室	情報基盤センター第2実習室	情報基盤センター第3実習室	経済学部実習室	教育学部システムD	教育学部システムE	図書館	CALL教室
利用時間[h]	18967	14803	3542	7478	6635	11198	35627	15332
ログオン回数	15896	10988	2730	5847	3131	6479	41704	10131

挾間キャンパス教室別学生端末利用状況



	自己学習室	情報処理実習室	チュートリアル教室	臨床講義棟ホール	標本資料室	医学図書館	臨床講義棟ホール貸出PC	標本資料室貸出PC
利用時間累計	68327.9	107828	25389.2	36762.2	14743.8	17800.6	26392.7	6282.9
ログオン回数	20931	40992	6279	17533	10727	5778	4041	2201

基盤情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/4/25	2017/7/28	トラブル	旦野原	サーバ	メールが見れない、Proself が開かない	2017/4/25　サーバー再起動にて回復 当該サーバは、故障発生後に NetApp に移行が完了しているため、様子見としたい。
2017/4/26	2017/4/26	トラブル	挾間	ﾈｯﾄﾜｰｸ	OpMager から無線 AP の死活監視エラー （別作業中に NTT が発見）	アライドスイッチの Off/On で回復 NTT 保守範囲外 NTT 要因対象外
2017/4/30	2017/9/13	トラブル	旦野原	サーバ	ajimu1 からのアラートが発生しており、コンソールにて操作不可（大分電子　佐藤申告）	2017/4/30　サーバー再起動にて回復 7/14　バックアップに起因している可能性があるため、バックアップ方式をサーバ毎に見直し実装する。 9 月第 3 週より新しいバックアップ方法で実施。
2017/5/10	2017/5/11	トラブル	旦野原	ﾈｯﾄﾜｰｸ	ノードスイッチ2、教育情報用スイッチ7、教育情報用スイッチ8ダウン（システムアラート）	12 分後に自然復旧 5/11 教育科学福祉部の電気室内の電源不具合の解消の作業があったため、一時停電となったことが判明。
2017/5/11	2017/5/11	トラブル	旦野原	サーバ	サービス停止の警報メール発報	ns2 の DNS サービス再起動により正常化 ns2 の IPv6 の GW 追加 不足していた CPU、メモリリソースを後日（5/14）に増設対応
2017/5/15	2017/5/17	トラブル	旦野原	サーバ	ファイルサーバ B のディスク (box3-6)LED が、黄色点灯	HDD 交換対応 5/15　HP に交換対応依頼 5/17　交換
2017/5/18	2017/5/18	トラブル	共通	サーバ	DEEPMail に Web 以外からのログインができなくなっている	正規データの再アップデート対応で回復 ・ベンダーにてアップデートサイトのデータを正しいものに修正 ・大分電子にて手動アップデート作業
2017/5/21	2017/7/12	トラブル	共通	サーバ	旦野原キャンパスの計画停電に伴い、電源切替（商用→電源車）時と切替後の正常な給電状況の確認を行ったが、その数分後に全てのサーバ機器がダウンとなった。	手動による UPS 出力再開 ・個別の手動起動 6/22　ログ解析の結果 UPS の故障等異常は確認されなかった。操作ミスの可能性も考えられるが、機器不良等の可能性も考慮しパーツの交換ができないか交渉中。7/12　初期不良の可能性のため NMC を交換
2017/5/21	2017/5/25	トラブル	挾間	サーバ	挾間キャンパスの計画停電に伴い、電源切替（商用→発電機）に時間がかかり（15 分程）、既設 UPS に接続されていたファイルサーバ C、OCT 用 FW がダウンとなった。	5/21 仮想サーバ（5 台）の手動起動 ※自動起動設定 ファイルサーバ C と OCT-FW を既設 UPS 収容から新 UPS へ収容を変更。 OCT-FW の停電による警告アラームも再起動を実施し、解消。
2017/5/27	2017/10/4	トラブル	共通	サーバ	監視システム上で yufu がダウンしたままなのを確認（大分電子　佐藤申告）	5/27　yufu の再起動にて回復 7/12 本来であれば Alaxala に飛ぶべきパケットが違うとこに飛んでいた。設定等に誤りもなく原因も不明であり様子見とする。（吉田先生了承済み）
2017/6/15	2017/6/30	トラブル	共通	サーバ	印刷物に 404 Not Found というエラーが表示される	IE のみ事象が発生することが確認できている。 印刷については、しばらく IE 以外のブラウザを利用するか、セキュリティ更新プログラムをアンインストールして利用することで回避できる。 6/20　学内での問合せが多いことから、回避方法がないか再度メーカーサポートへ調査依頼実施。 6/30　修正版の Windows Update が提供されたことにより解消

基盤情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/6/21	2017/11/29	トラブル	挾間	サーバ	Web サーバのカウンタが動かない	6/22 5:10 サーバ再起動し復旧 通信部分での異常であったため、様子見としたい。次回の PC一斉起動時に再現するか確認することとする。 8/9 再度事象発生 8/29 再度事象発生 10/25 www、www3 サーバの VLAN を NetApp に追加 事象が再発しないか当面監視する。
2017/8/7	2018/1/31	トラブル	旦野原	サーバ	ZION に登録されたデータが編集できない	1/31 更新作業を実施し登録者の閲覧編集が可能になった 他ユーザのスケジュールを登録する際に、公開区分が「予定あり」「非公開」「所属グループ」の場合、登録者の閲覧・編集が不可能になってしまう不具合。 メーカーにてバージョンアップ手順書を作成中 竹内さんと適用日程について調整
2017/8/28	2017/8/28	トラブル	挾間	ﾈｯﾄﾜｰｸ	フロア SW（fs-46）16 番ポートがダウンし、配下の NW が接続できなくなった。	16 番ポートに接続しているケーブルを 24 番ポートに差し替え復旧。 機器の交換は見送り。代替器は準備済み。
2017/9/21	2017/10/19	トラブル	旦野原	ﾈｯﾄﾜｰｸ	SINETへ接続している対外接続スイッチ(AX3830)の 1 番ポートの SFP ＋故障	9/21 19:35 吉田先生が SPF+ を抜き差しし、動き出した。 SPF+ の代替え物品が到着次第、取替実施する。 10/19 交換 基盤システム保守対象外（別契約保守）
2017/9/25	2017/12/25	トラブル	共通	サーバ	DEEPmail の受信 box に受信できない	From ヘッダにおいて文字コードが UTF-32 のメールを受信後、新着メールが保存される new ディレクトリから受信トレイ (inbox) へ移動する際に当該ヘッダ情報の解析処理 (parsing) に失敗し本事象が発生 当該メール (UTF-32 の From ヘッダのメール) に対してデコード処理中に停止する問題を改修したモジュールを作成し適用する。 現在、改修作業を終了し検証中。近日中にリリース予定。 12/25 リリース完了。
2017/10/15	2017/10/15	トラブル	挾間	ﾈｯﾄﾜｰｸ	停電作業後、復電時に PoE スイッチ PoE-163、PoE-164 との通信断	最終版 config を設定し直し復旧 PoE スイッチの設定変更後、config のセーブを行っていなかったため、設定が戻ってしまったことにより通信ができなくなった。
2017/10/15	2017/10/18	トラブル	挾間	ﾈｯﾄﾜｰｸ	FXC-06 の監視ができない	再起動し復旧 スイッチは正常に稼働していたためそのまま運用し、監視の復旧方法を検討していたが、再起動するしかなかったため再起動を実施。
2017/10/16	2017/10/16	トラブル	挾間	ﾈｯﾄﾜｰｸ	AP011、AP013 配下での通信不可	最終版 config を設定し直し復旧 PoE スイッチの設定変更後、config のセーブを行っていなかったため、設定が戻ってしまったことにより通信ができなくなった。全スイッチ最新版の config がセーブされているかチェックを実施。

基盤情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/10/25		トラブル	挟間	ﾈｯﾄﾜｰｸ	フロア SW 24 番ポートの通信不可 校舎講義棟 2F	再起動し復旧 通信は復旧したが、ランプ表示と通信速度が一致していない。メーカーよりリンクランプ不具合の可能性もあると回答あり。12/5（火）12 時～機器交換予定。 機器交換後もスイッチのランプ表示に変化が見られないため、通信速度に異常はないものと判断。 春の Windows アップデート迄保留する。 ノード SW ～ fs078 間にて 100M 通信である事を確認。4/12 切分けし、LAN コネクタ接続不良のため、コネクタ取替えにて 1G の正常通信へ復旧。
2017/11/25	2017/11/27	トラブル	挟間	ﾈｯﾄﾜｰｸ	学生福利フロアスイッチの通信断	ブレーカーを ON にし復旧 学生福利で多量の電気機器が使用されたと想定される。今後フロアスイッチの電源系統を分けるかは大学で検討する。
2017/12/15	2017/12/15	トラブル	挟間	ﾈｯﾄﾜｰｸ	プリンターが誤った IP アドレスを取得する	設定変更前のデータに戻し復旧 12/19 の病院 VLAN 設定に向けて、事前に LDAP 設定変更作業を行ったが、内容に誤りがあった。
2017/12/23	2018/1/30	トラブル	共通	サーバ	sepp サーバ通信不可	再起動後復旧 ログイン画面より進まず、Windows がフリーズしたためと考えられる。sepp クライアントソフトのインストール及び、それまで未適用だった windows アップデートを適用してから不具合が散見されるため、ひとまず最新の windows アップデートを適用し様子見とする。 1/10 ｗｉｎｄｏｗｓアップデート適用
2018/1/13	2018/1/24	トラブル	共通	サーバ	SFP スイッチの信号受信レベル低下 （Proactive Care Incident Report によるアラート通知）	3PAR/FC-SW の SFP を交換 （FC-SW のＳＦＰ不良） 12/18 に 3par の 3-2-4 番ポート (FC ポート) の信号受信レベルが低い事象が発生していた。他のポートより低い値のため 1/24 に機器交換を実施。
2018/1/21	2018/1/30	トラブル	共通	サーバ	ring.ix の httpd がダウン	httpd のプロセスを一旦完全に終了させた後に再起動 大学でバージョンアップ作業を実施。 今後作業を実施する際は再起動の実施とＮＴＴへの情報共有を頂きたい。
2018/1/24	2018/1/26	トラブル	共通	サーバ	スナップショットが取れない	証明書の再作成を行い復旧。 証明書の期限が 1 年後 (2019/1/25) に切れるので更新処理をルーティン化、できれば自動化するか、期限を延ばせるかを調査中。 FireEye の証明書更新は最長に変更。
2018/1/15	2018/1/16	トラブル	挟間	ﾈｯﾄﾜｰｸ	外国人宿舎にて無線接続ができない	Proxy サーバにて、VLAN1201 へのアクセス許可リストの追加 病院棟ネットワーク切替の際に、外国人宿舎 VLAN1201へのプロキシアクセス許可がなかった。
2018/1/6	2018/1/9	トラブル	挟間	ﾈｯﾄﾜｰｸ	AX-08 および配下の機器との通信不可 （通信不可のアラート発生）	1/6 23 時過ぎ 仮設電源にて電源復旧 1/7 1:30 正常電源に復旧 1/9 OpManager 上で故障回復報告が遅れたスイッチ（fs-077）についてもノードスイッチと併せログに問題無い事を安徳先生に報告。

基盤情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2018/1/26	2018/1/29	トラブル	挾間	ﾈｯﾄﾜｰｸ	ネットワーク障害　プロキシ負荷	FW の DoS プロテクション　tcp_port_scan 閾値を 100/ 秒から 1,000 に変更した ロードバランサのパーシステンス設定（セッションを維持する仕組み）が 10 時間となっており、偏ったアクセスのバランスを取り直すため一時的に止めた。 ⇒ 1/26FW の閾値設定変更 ⇒ 1/29 ロードバランサの設定を元に戻す
2018/2/25	2018/3/15	トラブル	共通	サーバ	esxi-05 及び esxi-05 上で動作中だった shibboleth2,smgr などのサーバがダウン	省電力モードをＯＦＦに設定（esxi-01 ～ 08） VMware 社、HP 社にログを送り解析中 HP 社から省電力モードＯＮの場合、省電力に入った場合、仮想サーバがダウンする事象が発生するとの報告あり　3/15 完了
2018/3/5	2018/3/5	トラブル	挾間	ﾈｯﾄﾜｰｸ	東院会館 ｆｓ 111 ダウン	大学側でブレーカーを戻し回復 前日の落雷による影響と思われる
2018/3/14	2018/3/14	トラブル	挾間	ﾈｯﾄﾜｰｸ	学外から　http://printkanri01.med.oita-u.ac.jp:9191/user　へアクセス出来ない	対処なし 安徳先生にて対応
2018/3/16		トラブル	共通	サーバ	NTP3 サーバの SSH ダウン （アラート発生）	再起動し回復 NTP 機能は動作していたが、サーバにログインできなくなっていた。再起動で回復したがログも出力されておらず様子見としたい。
2018/3/21	2018/3/22	トラブル	共通	サーバ	ファイルサーバＢダウン	ストレージバックプレーン 1 基盤交換
2018/3/23	2018/3/23	トラブル	共通	サーバ	医学部のホームページが学外から閲覧できない	大学様にて対応実施 大学様にて設定変更した事が原因と思われる 再起動の際に過去の設定が反映された。

教育情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/4/3	2017/4/3	Q/A	共通	サーバ	教育情報システムで導入した NewTech サーバで、ファームが提供されたが、大分大学で適用する必要があるか。	大学様で導入した機器とは別の種類の機器用のファームのため、適用の必要はない。
2017/4/5	2017/8/3	トラブル	挾間	PC	オリエンテーションや一斉授業等で IE やアプリケーションが重くなったり、ハングアップする PC が多い。	PC 側のログを確認したところ、IE や explorer、Office で AppHang XProcB1 や AppHang Transient といったエラーが出力されている。これらのエラーを解決する方法としては、下記のような対応が考えられる（いずれもマスタ PC で修正後配信が必要）。 ・regsvr32 jscript.dll の実行 ・IE の設定で GPU レンダリング設定をソフトウェアレンダリングに変更 ・不要なアドオンの停止 ・レジストリ HungAppTimeout（ハングアップ判断時間）の延長（表示のみ） デスクトップ PC に上記設定を組み込んだマスタを作成済 (5/17)。 8/3 に自己学習室にて一斉起動による状況確認を実施。特に問題なし。
2017/4/13	2017/4/14	トラブル	旦野原	netboot	今朝から、図書館と第 3 実習室 (Wingnet なし分) の PC が起動しなくなった。	サーバのディスク容量不足のため Wingnet なし分のマスタイメージが正常に作成されなかったため。Wingnet なし分のマスタイメージを ccboot2 へ移動させ、ccboot1 のディスク容量の空きを 48GB から 129GB まで拡張し、正常動作を確認。 翌日 office が起動できなかった件は、office の修復を実行し、正常動作を確認。
2017/4/26	2017/9/19	要望	挾間	PC	ユーザ辞書の登録を行ってほしい。	ユーザ辞書の登録は、すでに登録している人の情報を削除してしまうため、まとめて実施しない方がよいと思われる。 ユーザ辞書が利用できない件については、昨年実施した imjp10 フォルダの作成が必要と思われるため、PC 側にフォルダ作成バッチを組み込むかファイルサーバ側でフォルダを作成するしかない。 デスクトップ PC、ノートブック PC それぞれのマスタにバッチファイルを組み込み済み (5/17、6/19)。
2017/5/8	2017/5/8	トラブル	旦野原	プリント管理	旦野原実習室から印刷ができない。	プリント管理サーバが認証に使用している samba サーバのディスクが容量不足となっていたため、実習室からのプリンタ割り当てができにくくなっていたため。4 月までは、最大 1 ヶ月分のログを 20GB 上限で 5 個分ローテーションして保存するように設定していたが、4/23 頃から急激にログが増え始め、5/7 の夕方頃にディスク容量が足りなくなったと考えられる。古いログを削除して正常動作を確認。Samba のログレベルを落とし、ローテート上限は 5G に変更。
2017/5/15	日程調整中	要望	挾間	PC	シマンテックの最新版を教室の PC にインストールして欲しい。	No.612、614 の対応時に合わせてマスタ PC へインストールを実施済み。
2017/5/19	2017/6/11	トラブル	旦野原	PC	4 月にサーバのディスク容量不足でエラーとなっていた旦野原の wingnet なしのマスタ PC で、office 関連の Windowsupdate 適用時にエラーとなる。	色々と対応方法を実施したが、改善されなかったため office を再インストールして正常に Windowsupdate できるようになった。
2017/5/23	2017/6/2	トラブル	挾間	PC	図書館のノートブックが、STOP: c000021a {Fatal System Error} と表示され起動されない。	PC のディスク及びメインボードを交換後、配信作業を実施、確認済み。

教育情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/5/29	2017/5/30	トラブル	旦野原	PC	CALL 教室の PC でヘッドセットを交換しても録音した音声にノイズが入る。	PC 側の不具合と思われるため、PC のメインボードも交換して正常動作を確認。 予備のヘッドセットが残り 4 台となっている。
2017/5/30	2017/6/12	要望	図書館	サーバ	図書館の Opac サーバの証明書を更新して欲しい。	6/12 に証明書を更新し、正常に表示されることを確認。
2017/6/5	2017/6/11	要望	旦野原	サーバ	6/11 の旦野原キャンパスの教室閉鎖時に合わせて、ネットブートサーバとプリント管理関係のサーバの WindowsUpdate を行ってほしい。	6/11 に各サーバへ WindowsUpdate を実施。
2017/6/7	2017/6/11	要望	共通	サーバ	SPSS のバージョンアップを行ってほしい。	SPSS のライセンス管理サーバへ Ver24 を利用できるようにライセンスを登録。
2017/5/8	2017/6/29	トラブル	挾間	印刷管理	メールプリントの機能を利用して印刷ができない。 「キャンセルされたプリントジョブ」というメールが届く。	PaperCut のシステムに登録されているユーザにメールアドレスが含まれていないため。原因について調査中。 システム移行時に既存を含め、ユーザにメール属性が付加されない形となっていたため。 6/29 にメール属性の付加を実施。
2017/6/28	2017/10/25	トラブル	挾間	PC	情報処理実習室で瞬快のイメージ配信中に 30 台以上の PC への配信がエラーとなった。	再配信実施時にはエラーとならなかったため、一時的にネットワーク側で何か問題が発生したのではないかと思われる。その後再発しないため様子見。
2017/7/3	2017/7/4	トラブル	旦野原	PC	第 1 実習室の PC2 台 (cc10027,cc10058) の電源が入らない。 （症状） ・電源スイッチを押すと、入って切れてを繰り返すもしくは、入ってすぐ切れたままとなる ・正常なPCの電源コードを接続しなおしても同じ ・一晩放電させてみたが症状は変わらず	ハード交換を実施。
2017/7/10	2017/7/17	Q/A	挾間	PC	学生用パソコンのトップページにお知らせを表示したい。	PC のスタートアップに ie のショートカット置くことにより対応する。
2017/7/20	2017/7/25	Q/A	挾間	瞬快	瞬快サーバ上の不要イメージ削除方法について教えて欲しい。	ProjectWeb に登録している「瞬快サーバシステムリカバリリソース (ディスクイメージ) の管理方法 .xlsx」を元に説明を実施。
2017/7/21	2017/7/21	Q/A	旦野原	PC	実習室ごとに異なるアプリ一覧の表示制御を変更したい。どこで処理をしているか教えて欲しい。	スタートアップにあるバッチファイルにて制御している。
2017/7/25	2017/8/23	Q/A	旦野原	PC	(1) 図書館のプリンタで印刷をかけたが何も印刷されなかった (7/20) (2) 文字化けしたデータが大量に印刷された (7/23) こちらで再度確認したところ、一般ユーザでプリンタの手動登録が可能だった。そこで ・実習室 PC で一般ユーザがプリンタを手動で追加できなくすることは可能か。 ・手動で追加したプリンタに印刷した場合、PaperCut のジョブログには記録されないと思うが、今回、(2) のケースでは itcpr の出力が PaperCut のジョブログに記録され、「キャンセル済」となった。これは，どういったケースが考えられるか。7/23 に itcpr の出力端末で操作していないことは確認済み。	手動追加の禁止手順は、プリンタ側の IP フィルタの設定を行い、プリントサーバ以外からはジョブを受け付けない設定を行うことで可能と考えられる。 ただ、IP アドレスでのフィルタとなるため、指定した IP からは、一切のアクセスが出来なくなる。プリンタの Web 画面等を開く可能性のある IP は、許可 IP に入れておく必要がある。ただ、この手順の場合、プリンタの追加は可能であるが、追加したプリンタからは印刷できない。 2 点目の手動でのジョブのキャンセル手順は、リリースステーションを利用しない場合では、以下 2 点が考えられる。 (1) ユーザ Web 画面の「保留中のジョブをリリース」からキャンセル可能 ※ こちらは、設定で無効に出来るが、現在の設定がどちらか、確認が必要 (2) クライアントのスプーラーから手動で削除 クライアントからの印刷をネットワークからローカルへ変更したため、一旦終了とする。

教育情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/8/3	2017/8/18	トラブル	挟間	PC	自己学習室　SJK-044 WindowsUpdate 実行時に再起動途中で停止する。No.605 の現象がこの 2 ヵ月の間に 3 度発生（実質 5 回中 3 回） 情報処理実習室 SJI-080 画面が表示しない。ディスプレイは他の PC を接続すると表示するので、本体側のビデオカードの問題と思われる。	いずれもメインボード交換を実施。 8/18 に瞬快サーバへ MAC アドレスを追加して正常動作を確認。 SJI-088、SJI-116 についてもマザーボードの変更を実施し、8/23 に瞬快サーバへの登録を実施済み。
2017/8/18	2017/8/24	Q/A	共通	サーバ	Esx24 （ccboot1 が載っているサーバ）で、デバイスエラーが出ている。CSS ランプも点灯している。	ハード的なエラーは検知されなかったため（誤検知の可能性あり）、エラーを解除できるか確認中。ディスクの障害であったため、予防交換を実施(8/24)。エラーメール送信ができなかった件も SMTP サーバの設定を行い正常動作を確認。
2017/8/24	2017/9/21	Q/A	旦野原	ブートサーバ	CCBoot1 サーバのイメージを利用して起動する PC のログイン画面の表示が他のサーバと比較して 1 分程度遅い。	シマンテックのネットワーク脅威防止等のサービスを停止後、DHCP サービスの再起動を実施したところ、他のサーバとほとんど同じ時間で起動するようになった。
2017/9/7	2017/9/20	トラブル	挟間	プリント管理	PaperCut に、特定の ID でログインできない。	LDAP に Felica カード登録が設定されていなかったため。Waku については、Felica カードの登録ができない状況になっていたため、プログラム修正後、カードを登録し、ログインできることを確認済み。
2017/9/7	2017/10/2	要望	挟間	瞬快	瞬快 WindowsUpdate 連携の実行結果のメール送信先を変更したい。	手順を連絡済み。スケジュールごとに設定する必要がある。 島岡先生個人のメールアドレスから micenter へ変更済み。
2017/9/14	2018/4/5	Q/A	挟間	ハブケーブル	標本室の貸出用ノートブックに対して瞬快の配信処理を実施したところ、マルチキャスト配信が他の教室に比べて 6 割程度のスピードしか出ない。図書館の貸出用ノードブックを接続するハブにて、7 ポートに接続している PC の配信処理に時間がかかる。ポートを変えると処理が通常通りとなる。	標本室のハブ経由の場合のみ遅いため、ハブもしくはケーブルの問題と思われる。調査中。標本室については、ケーブルを交換することにより、通常の速度と同程度となった。追加の図書館分については、ハブの交換を含め対応を検討中。 ケーブル交換については、3/23 に実施済み。 学生ホールのケーブルも同様の状況となっているため、確認、交換して欲しい。(3/30) 4/5 に学生ホール対応済み。
2017/9/26	2017/10/26	トラブル	挟間	リリースステーション	情報処理実習室後方リリース PC の画面がブラックアウトしており、電源は落ちていませんでしたが操作が出来なかった。 強制終了後、添付ファイルの通りドライブのスキャンおよび修復中 (C)**%…となり、その後正常に稼働した。	特に問題は発生していないようであるが、Windows Update のタイミングで発生している可能性があるため、念のため全台フェリカドライバのアップデートを適用。
2017/9/26	2017/10/18	トラブル	挟間	プリンタ	1 部の PDF ファイルの印刷が、ゼロックスプリンタのみ正常に出力されない。OKI プリンタでは出力される。	8 月の Windowsupdate 以降ゼロックスのプリンタで発生している既障害と思われる。最終的な修正は、Windowsupdate による修正を待つしかないがそれまでは、下記の方法で回避して欲しいとのこと。 ・プリンタを右クリックして印刷設定を開く。 ・詳細設定タブの用紙 / 出力の「アプリケーションズーム」をクリックし、「する」になっていることを確認し、倍率を 99 もしくは 101 に変更する。 ・[OK] で保存していく。 上記設定では、改善されなかったため、プリンタの原稿サイズの設定を現在の B5 から A4 に変更することにより、正常動作を確認。 今後印刷時に用紙サイズのエラーが発生した場合は、プリンタ側でプリント中止ボタンを押下する必要がある。

教育情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/10/18	2017/10/19	トラブル	挾間	PC	情報処理実習室の PC3 台が正常に起動しない。 SJI-010,018 モニターに画像が移らない (ほかのモニターに接続しても同様) 。 SJI-046　電源ユニットの不具合 (電源が入らない) 。	SJI-010 と 018 はメインボード交換を実施。SJI-046 は電源ユニットの交換を実施。SJI-010 と 018 は、10/19 に瞬快サーバ、DHCP サーバへ交換後の MAC アドレスを登録済み。
2017/10/20	2017/10/26	トラブル	共通	印刷管理	旦野原のゲストユーザは、半期に一度新規に追加、削除作業を実施しているが、FelicaID は、以前のものを再利用している。10 月以降ゲストユーザから印刷できなくなっているが、PaperCut 側でユーザの削除処理を停止した影響があるか。	現在、前期に FelicaID を利用していたユーザが削除されていないため、同じ ID を 2 人のユーザが使用するように設定されていると考えられる。このような場合、プリント管理サーバ側でエラーとなり、新規登録されたユーザが印刷できなくなっていると思われる。 次回 (10/26)、SCSK 様が大学へ訪問した際にユーザの削除処理を実施する。また、今後は、年 2 回の自動削除処理の実行も検討したい。 ID の重複していた不要なユーザを削除し、正常動作を確認。 年 2 回の作業は、SCSK 様からリモートにて手動で実施する。
2017/10/24	2017/10/24	トラブル	旦野原	プリンタ	図書館に設置しているゼロックスプリンタの 1 台が、最近毎日のように紙詰まりが発生するので、一度見て欲しい。	トレイの給紙ローラ部の劣化のため。給紙ローラを交換。
2017/10/25	2017/10/26	トラブル	旦野原	PC	第 2 実習室の教卓の PC のディスプレイの設定が、これまで「複製」だったものが「拡張」に変わってしまった。	プロジェクタを利用する PC にて、vDisk イメージを割り当て、マルチディスプレイの設定を行うことにより復旧。 原因については、PC とプロジェクタの間に入っている EDID 保持器もしくはプロジェクタに問題が発生し、イメージに保持されているディスプレイと異なるディスプレイを接続した状態となり、表示モードが拡張に変更となったと考えられる。
2017/10/25	2017/11/14	要望	挾間	サーバ	医学部 PC 教室用の瞬快サーバの残りディスク容量が、30GB 程度まで減少しているため、容量の拡張を行いたい。	サーバのディスク容量を 300GB から 350GB に拡張する作業を実施した。
2017/11/22	2017/11/24	トラブル	挾間	プリンタ	医学情報センターから自己学習室の OKI 複合機の web 画面にアクセスする事が出来ない。	プリンタに設定しているゲートウェイアドレスに誤りがあったため。アドレスを修正いただき正常動作を確認。今年の夏ごろにボードを交換した際にアドレスを間違って登録したと思われる。
2017/11/24	2017/11/24	Q/A	旦野原	PC	ネットブートシステムの VHD ファイルの容量拡張を行いたい。	容量拡張手順について、パナソニックより連絡済み。サーバの残容量も少なくなってきているため、拡張を実施したいが、不要ファイルを削除してある程度空きが増えたため、春休みまで様子を見て判断する。
2017/12/11	2017/12/13	Q/A	旦野原	印刷管理	旦野原の学生が，実習室から印刷をかけたものをリリースステーションで印刷をしようとしたところ，「キューへ追加中」のままとなり，印刷されなかった。 (1) spool01/itcpr に出していたので，(2) printkanri01/itcpr に出し直してもらったところ，正常に印刷された。 状況を見ていたが，(2) の印刷時にも，(1) のジョブは「キューへ追加中」と表示されたままだった。 その後，いくつか確認をしてみたところ， ・(1) に関してプリンタにはエラーも印刷ジョブのログもなかった ・(1) に関してポイントは引かれていなかった，また，PaperCut の管理画面で確認したところジョブとしてもログがなかった この症状は，1 回だけで，その後，事務室で印刷をテストしてみたが，再現しなかった。原因はなにが考えられるか。	PaperCut・プリンタ側にログが残されていないことから、原因の追究が、現状は難しい。 現象が多発するようであれば、サーバの監視と、ネットワークアナライズを実施する。 本現象が多発していないようであれば、一度、様子見としたい。 本現象が初めてで、今のところ再発もしていないため、再発時に連絡。

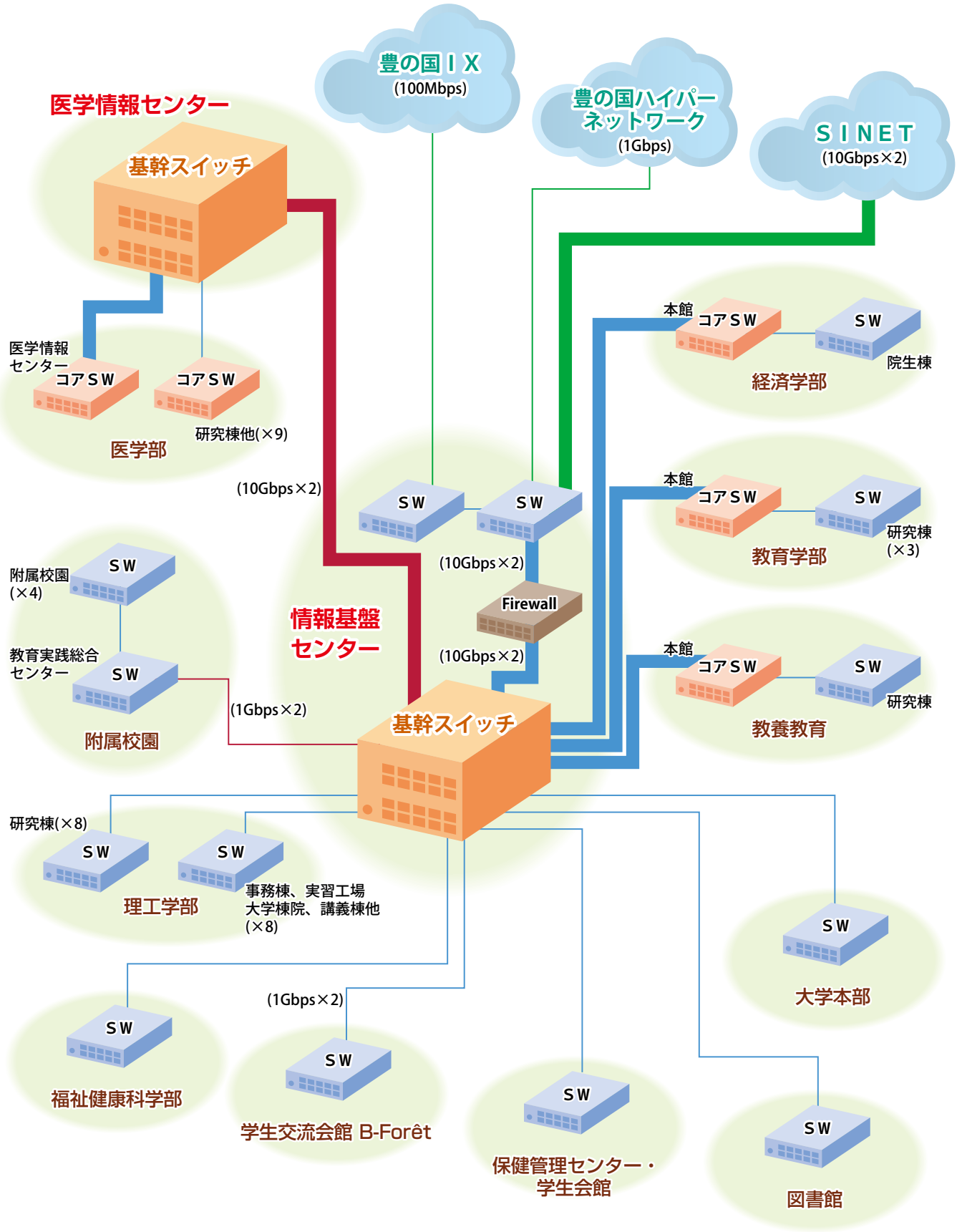
教育情報システムトラブル対応表

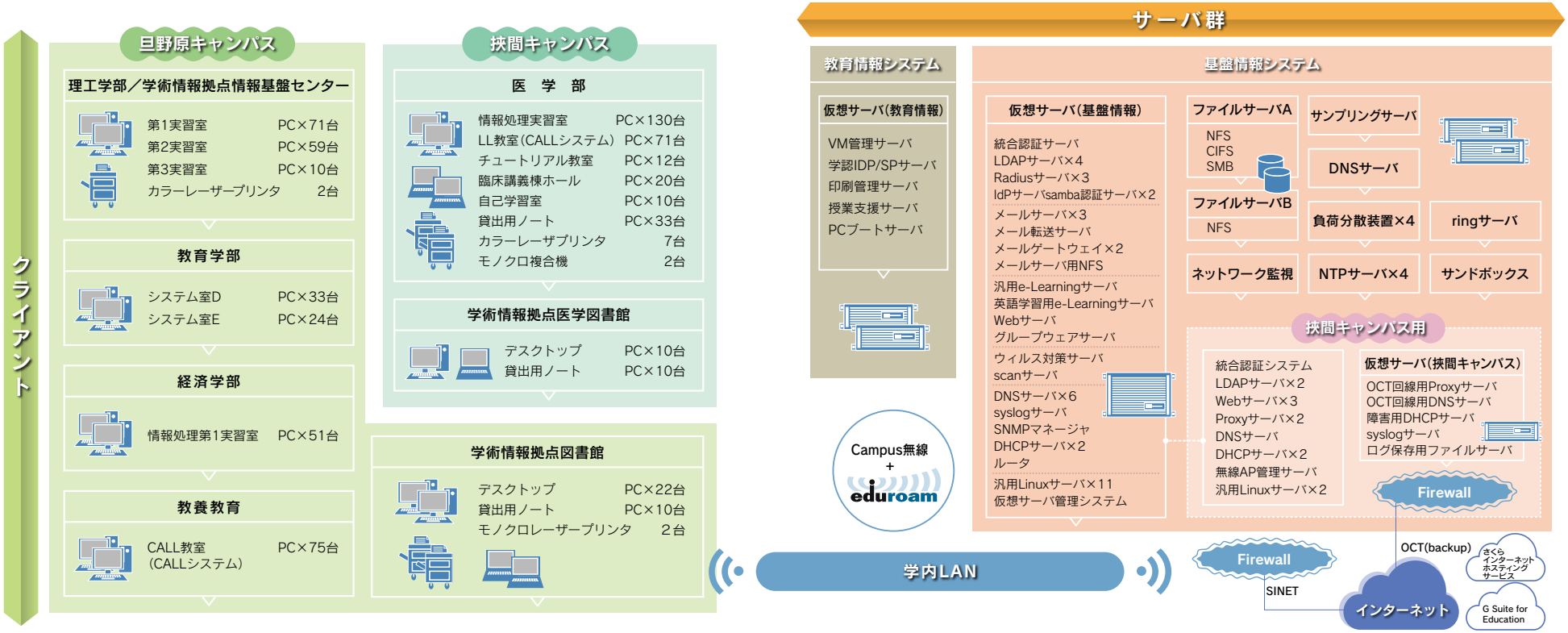
発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2017/12/18	2018/1/5	トラブル	挾間	PC	挾間情報処理実習室 PC の SJI-019,103,118 が2ヶ月以上連続して Windowsupdate に失敗している。	電源関係のハードの問題。電源ユニット交換により正常動作を確認。
2017/12/18	2017/12/18	Q/A	挾間	PC	貸出用 PC でログイン情報を取得したいが方法はあるか。	ログイン情報について、aaa サーバで取得しているものが見やすいため、確認方法を連絡。
2018/1/5	2018/1/15	トラブル	挾間	PC	医学部標本室の PC が 1 台 BOOT Failure - Press any key to continue と表示され起動しない。	ハードディスクの問題であった。ディスク交換後、瞬快でイメージ配信を実施して正常動作を確認。
2018/1/11	2018/3/27	トラブル	旦野原	PC	以下の障害が発生した。 ・WINGNET なしイメージの PC が数台起動しない ・WINGNET ありイメージの PC の Office 起動時に，ライセンス確認の画面が表示される	原因は、どちらも boot1 サーバの C ドライブの容量不足。運用に不要と思われるファイルの移動を行い、仮復旧（イメージ使用中のため）。 ・WINGNET なしについては boot1 以外のサーバを使用するようにメニューを変更。後日、boot1サーバにイメージを同期させメニューを戻して完了。 ・WINGNET ありについては昨日のイメージにロールバックし翌日、正常に更新されることを確認して完了。 翌日 WINGNET なしのイメージが boot1 サーバに正常にコピーされない状態は解消されなかった。クライアント台数が比較的少ないため、当面イメージは 3 台のサーバで運用し、春休みに調査を実施する。 3/12 にサーバのディスク容量を 200GB 増加した。 3/27 に boot1 サーバへコピー処理を実施し、問題なくコピーされることが確認できた。ディスクの断片化が進んでいたため（通常 1 週間に 1 度自動で実施）、手動で実施後、2%程度まで減少したことを確認。
2018/1/15	2018/6/11	トラブル	共通	サーバ	CPU 脆弱性対応について	年初より報道されている「CPU の脆弱性」対応について ・今回の脆弱性は、悪意あるプログラムが攻撃対象のサーバ上で実行された場合に、従来保護されていたメモリに格納されているデータが参照可能となるものです。 ・データの改ざんの可能性はありません。攻撃者が外部ネットワーク（インターネット等）からリモートアクセスをするだけではメモリデータを参照する事はできません とのことから、Netboot やプリント管理サーバのセキュリティパッチ適用については、再起動を伴うため、春休みの対応としたい。 3/12 までに Windows サーバのシマンテックを最新とし、3/12 にプリント管理関連とネットブート関連のサーバのセキュリティパッチの適用を実施した。 リモートデスクトップでサーバに接続できなくなるセキュリティパッチが提供されたため、6/10 に Netboot とプリント管理サーバについては、再度最新のセキュリティパッチの適用作業を実施した。
2018/1/16	2018/1/19	トラブル	挾間	サーバ	瞬快サーバでイメージ配信処理時に KMS 認証エラーとなる。	瞬快サーバでウィルス対策ソフトが起動しない状態となっており、FW の設定が有効となって瞬快サーバと通信ができなかったため。設定時は Windows の FW は無効で、ウィルス対策側を有効としていたため、ウィルス対策ソフトの最新のバージョンをインストールすることにより、ウィルス対策ソフトが正常に起動され初期セットアップ時と同様の設定に戻した。

教育情報システムトラブル対応表

発生日	完了日	区分	キャンパス	システム区分	トラブル／質問	対応／回答
2018/1/19	確認中	トラブル	旦野原	PC	CALL 教室の音声不具合が再発し、9 台のヘッドセットを交換した。	残りのヘッドセットが少なくなってきているため、予備を追加できるか検討する。その後 13 個交換して残りが 5 個となった。 3 月中に 8 個追加、以降も必要であれば追加する。 5 月中に追加予定。→ 7 月中に変更。
2018/1/25	2018/2/7	トラブル	挾間	PC	図書館の学生用ノートブックで、ログオン後何も表示されない現象が発生した。	瞬快のイメージを再配信することにより正常動作を確認。 再発したため、ディスク交換後再配信して正常動作を確認。
2018/1/26	2018/1/29	Q/A	挾間	PC	学生用 PC で 16 時間ログインし続けているとシャットダウンされるようになっていると思うが、時間を短くすることは可能か。また、シャットダウンする前にメッセージを表示することは可能か。	起動時のバッチファイルに組み込んでいるため､設定変更は可能である｡また現在はシャットダウンする15分前からメッセージが表示されている。
2018/1/29	2018/1/31	トラブル	旦野原	PC	旦野原の学生用 PC で、「問題が発生したため，PC を再起動する必要があります。」といったようなメッセージが表示され再起動を繰り返すことがある。	イメージを再作成することにより、正常動作を確認。
2018/2/7	2018/2/20	保守	共通	UPS	UPS 定期保守作業 (バッテリ交換) の実施。	事務局 1 台、センター 8 台の UPS のバッテリ交換を実施。
2018/2/19	2018/4/2	トラブル	旦野原	PC	実習室 PC にインストールしていただいた AutoCAD のライセンスが切れ，再インストールが必要となった。プロファイルの操作が必要と思われる。 ・psetup で 1 回起動させてイメージを作成しないと，毎回起動時にインストールと環境設定が走る ・psetup で起動させた後に作成したイメージだと，他のユーザで書き込みができない ・設定情報の保存先を確認したが，数か所あり，訂正箇所を特定できない 当初インストールした際の設定情報を至急お知らせいただいたい。	インストール後のレジストリ情報をエクスポートして、その情報を修正 してログインスクリプトへ書き込む必要があるため、次回訪問時に対応予定。 4/2 にプロファイルの対応を実施。手順について大学様に説明。
2018/3/9	2018/3/12	トラブル	旦野原	PC	第 1 実習室 PC(cc10066) が起動しなくなった。電源を入れると，電源の On/Off が繰り返される。	該当 PC のメインボードを交換して正常動作を確認。
2018/3/19	2018/3/23	トラブル	旦野原	PC	一部 PC(Wingnet なし PC) が再起動を繰り返す。手動でイメージを作成するとその日は正常に動作するが、翌日また同様の現象となる。	Wingnet なし PC のマスタ機の起動が Windows のマークの画面で停止しており、そのため夜間のタスクが失敗して正常でない状態のイメージが作成されていたことが原因と思われる。マスタ機の PC を手動で電源を落とし、手動で起動させたところ正常に起動することを確認。翌日から正常動作を確認。今後また発生するようであれば、夜間の自動更新タスクの見直しを実施。
2018/3/20	2018/3/29	Q/A	挾間	印刷管理	卒業生の印刷ポイントを集計する方法を教えて欲しい。	全てのユーザで残ポイントを含むレポートを出力 (CSV) し、必要ユーザのフィルタは EXCEL 上で実施する方法となる。
2018/3/26	2018/4/4	要望	共通	印刷管理	新入生の印刷ポイントの登録用データは 4/3 中に提供予定なので、登録をお願いしたい。	4/4 に旦野原キャンパスにて登録予定なので、それまでに登録する印刷ポイントを教えて欲しい。 旦野原：5000、挾間：250 で新入生のポイントの登録を実施。なお、ユーザの削除については、ライセンスが超過しているため 4 月中に実施予定 (5/1 完了)。

キャンパスネットワークシステム構成図




クライアント
旦野原キャンパス
理工学部／学術情報拠点情報基盤センター
第1実習室 PC×71台
第2実習室 PC×59台
第3実習室 PC×10台
カラーレーザープリンタ 2台
教育学部
システム室D PC×33台
システム室E PC×24台
経済学部
情報処理第1実習室 PC×51台
教養教育
CALL教室（CALLシステム） PC×75台
挟間キャンパス
医　学　部
情報処理実習室 PC×130台
LL教室（CALLシステム） PC×71台
チュートリアル教室 PC×12台
臨床講義棟ホール PC×20台
自己学習室 PC×10台
貸出用ノート PC×33台
カラーレーザプリンタ 7台
モノクロ複合機 2台
学術情報拠点医学図書館
デスクトップ PC×10台
貸出用ノート PC×10台
学術情報拠点図書館
デスクトップ PC×22台
貸出用ノート PC×10台
モノクロレーザープリンタ 2台
サーバ群
教育情報システム
仮想サーバ（教育情報）
VM管理サーバ
学認IDP/SPサーバ
印刷管理サーバ
授業支援サーバ
PCブートサーバ
基盤情報システム
仮想サーバ（基盤情報）
統合認証サーバ
LDAPサーバ×4
Radiusサーバ×3
IdPサーバsamba認証サーバ×2
メールサーバ×3
メール転送サーバ
メールゲートウェイ×2
メールサーバ用NFS
汎用e-Learningサーバ
英語学習用e-Learningサーバ
Webサーバ
グループウェアサーバ
ウィルス対策サーバ
scanサーバ
DNSサーバ×6
syslogサーバ
SNMPマネージャ
DHCPサーバ×2
ルータ
汎用Linuxサーバ×11
仮想サーバ管理システム
ファイルサーバA
NFS
CIFS
SMB
ファイルサーバB
NFS
ネットワーク監視
サンプリングサーバ
DNSサーバ
負荷分散装置×4
NTPサーバ×4
ringサーバ
サンドボックス
挟間キャンパス用
統合認証システム
LDAPサーバ×2
Webサーバ×3
Proxyサーバ×2
DNSサーバ
DHCPサーバ×2
無線AP管理サーバ
汎用Linuxサーバ×2
仮想サーバ（挟間キャンパス）
OCT回線用Proxyサーバ
OCT回線用DNSサーバ
障害用DHCPサーバ
syslogサーバ
ログ保存用ファイルサーバ
Firewall
Campus無線
+
eduroam
学内LAN
Firewall
SINET
OCT(backup)
さくらインターネットホスティングサービス
インターネット
G Suite for Education

大分大学学術情報拠点（情報基盤センター）

利用ガイド（2017 年度）

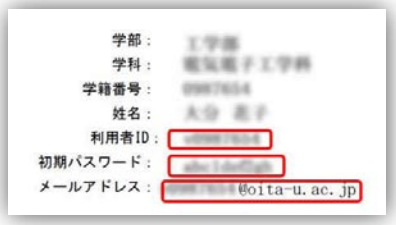
http://www.cc.oita-u.ac.jp/

窓口：情報基盤センター1 階　事務室（平日 9:00～17:00）
電話：内線 7985（外線 097-554-7985）
Mail：center@oita-u.ac.jp
Web：http://www.cc.oita-u.ac.jp/（お問い合わせフォーム）

■1. 利用者ＩＤカードについて

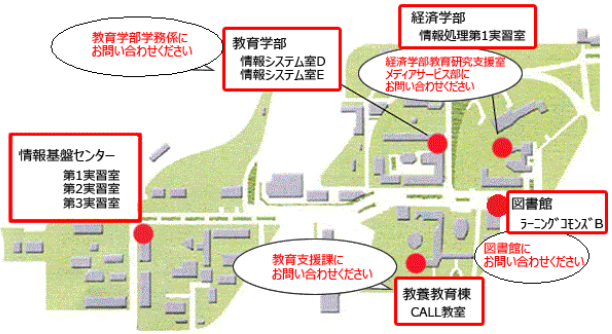
センターから、**利用者ID**と**初期パスワード**を印刷した名刺大の**利用者IDカード**が提供されます。皆さんの所属の学部･学科で配布を受けてください。

初回利用時には、必ず初期パスワードの変更が必要です。実習室、研究室のパソコン等で変更を行えます。



■2. 利用者ＩＤとパスワードで利用可能なシステム

2-1. 情報教育システム



【1】実習室パソコン

実習室のPCを起動すると、下図の画面が表示されます。利用者IDカードに記載されている、利用者IDと初期パスワードを入力してください。画面に従い、入力条件に注意し、パスワード変更を行ってください。

【2】プリンタ（オンデマンドプリンタ）

プリンタは、図書館（2台）、情報基盤センター1F 印刷室（1台）に設置しています。実習室または図書館のパソコンから、どちらのプリンタにも印刷をすることができます。

以下の方法で印刷できます。

■印刷方法

（1）プリンタは図書館（libpr）または情報基盤センター（itcpr）のどちらかを選択します。必要なポイントは同じです。図書館のプリンタはモノクロ A4 サイズのみとなっています。

（2）プリンタが設置されている場所に行き、プリンタ操作端末にログインします。次の3つの方法のいずれかでログインします。

（方法1）学生証を磁気カードリーダに通す。

（方法2）登録済み Felica カードを IC カードリーダにかざす。

（方法3）利用者IDと**変更した**パスワードを手入力する。

（3）ログインすると保留中のジョブ･リストが表示されます。印刷したいドキュメント名を選んで、印刷してください。

（4）ドキュメントが印刷され、印刷ポイントが減算されます。

注1）印刷ジョブは24時間放置していると自動的に削除されます。

注2）何らかの原因で印刷できなかった場合は、**すぐに図書館カウンターまたは情報基盤センター事務室までご連絡ください！放置していると、障害が解消された後に出力されてしまう場合があります！**

注3）用紙トレイを開けたり電源を触ったりしないでください！エラーメールが送信されます。

注4）印刷には印刷ポイントが必要です。詳しくは情報基盤センターHPをご覧下さい。
http://www.cc.oita-u.ac.jp/modules/inpico/index.php?content_id=3

2-2. 電子メール（DEEPMail）

【1】電子メールアドレスについて

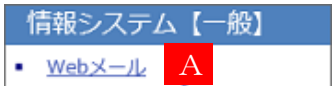
あなたの利用者ID@oita-u.ac.jp

【2】DEEPMail とは

DEEPMail は、全学での推奨メールサービスです。ブラウザ（閲覧ソフト）から利用できる電子メールソフトです。どのパソコンやモバイル端末からでも DEEPMail の機能を利用できます。

【3】DEEPMail の利用方法

ブラウザを起動し、情報基盤センターHP の「WEB メール」をクリックします。



利用者IDと**変更した**パスワードを入力し、ログインしてください。

注1）サーバでのメールの保管期間は400日間となっています。保管用のフォルダを作成し、受信トレイからメールを移動すれば、在学期間中はサーバにメールを保存しておくことができます。

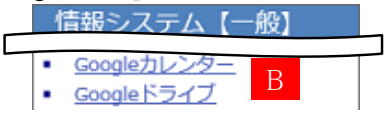
注2）携帯電話への着信通知設定をしておくと便利です。

注3）添付ファイルは、マナーとして5MB 以内にしましょう。5MB を超えるファイルは、DEEPMail オプションの「Web ファイル機能」を利用しましょう。

2-3. カレンダー/ドライブ（G Suite）

【1】カレンダー/ドライブの利用方法

ブラウザを起動し、情報基盤センターHPの「Google カレンダー」/「Google ドライブ」をクリックします。



利用者IDと**変更した**パスワードを入力し、ログインしてください。

注1）カレンダーの詳細は以下をご覧下さい。
http://www.cc.oita-u.ac.jp/modules/pico/index.php?content_id=146

注2）ドライブの詳細は以下をご覧下さい。
http://www.cc.oita-u.ac.jp/modules/pico/index.php?content_id=150

2-4. 学習支援システム

【1】Moodle（授業補助教材）の利用方法

ブラウザを起動し、情報基盤センターHPの「Moodle」をクリックします。

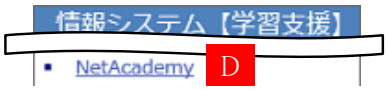
利用者IDと**変更した**パスワードを入力し、ログインしてください。

＜コンテンツについて＞

コンテンツとして、「INFOSS 情報倫理」および授業で利用するものがあります。「INFOSS 情報倫理」は、大分大学に所属する人は誰でも利用できます。早い機会に学修して、情報セキュリティの基礎を身につけておきましょう。授業で利用するコンテンツに関しては、授業担当の教師より指示があります。

【2】NetAcademy（英語教材）の利用方法

ブラウザを起動し、情報基盤センターHPの「NetAcademy」をクリックします。



利用者IDと**変更した**パスワードを入力し、ログインしてください。

＜コンテンツについて＞

コンテンツとして、「総合英語トレーニング中級コース」、「TOEIC L&R テスト 500・600・730 点突破コース」、「英単語パワーアップコース医学・医療編」の3コースがあります。本教材を利用して、TOEIC 等、英語の検定試験にチャレンジしてください。なお、英語の講義で、本システムを利用することがあります。その際は、教師の指示に従ってください。

2-5. 無線LAN

【1】無線LANのアクセスポイントと設定値について

ESSID	暗号化	事前共有キー
2010OITA1 2010OITA2 2010OITA3 2010OITA4 2010OITA5	WPA2/AES	OITAUNIVERSITY1592 （半角大文字です！）
eduroam	WPA2/AES	-

※設定方法は各パソコン等の無線 LAN の説明書をご覧下さい。

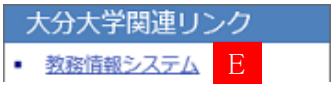
自分のパソコンを大学で使用する場合は、無線LANで接続できます。本学の「キャンパスネットワークシステム」では上記のESSID のアクセスポイントが設置されています。これらのアクセスポイントは学内各所に設定されていますので上記の設定値を参照して利用してください。利用の都度、認証サーバにより利用者IDと**変更した**パスワードで認証を行います。

注1） 利用するパソコンはワクチンソフトが必須となっています。
注2） モバイルルータ、テザリングなどは、アクセスポイントとの干渉を防ぐため、サービスの停止または電源を切るなどしてください。
注3） eduroam は事前共有キーの入力は不要です。利用者IDと変更したパスワードを入力して接続します。

2-6. 教務情報システム（CampusSquare）

【1】教務情報システム（CampusSquare）の利用方法

ブラウザを起動し、情報基盤センターHPの「教務情報システム」をクリックします。



利用者IDと**変更した**パスワードを入力し、ログインしてください。
注1） 履修登録や成績照会などのシステムです。
注2） システムに関するお問い合わせは、教育支援課へ。

■3. システム利用上の注意

3-1 情報教育システム室（実習室）の利用について

（1） 教育・研究目的以外の使用はできません。
（2） 授業時間中は受講者以外の立入は禁止です。
（3） 埃などから機器を守るため、窓は常に閉めておくようにしてください。
（4） 飲食は指定された場所でお願いします。
（5） 自習利用時間中であっても、携帯電話による通話はしないでください。
（6） パソコン等使用機器に異常があった場合は、事務室まで速やかに連絡してください。（事務室 554-7985）
（7） パソコン等へのソフト組み込みや許可されていない機器の接続は禁止です。また、各自のドキュメントフォルダ以外には、ファイルを作成しないでください。

3-2 電子メールの利用について

（1） 自分のメールアドレス（利用者 ID）を他人に使用させてはいけません。
（2） 不審な添付メールは開かないようにしてください。
（3） 大容量のファイルをメールに添付しないでください。（5MB 以内。ただし携帯電話へ送信する場合は、1MB 以内。）
（4） 不要メールは削除、必要なメールはファイルに保存するなどして既読メール、送信済メールは随時サーバから削除するようにしてください。

3-3 インターネットの利用について

（1） 出所が定かでない外部記憶メディアをパソコンに挿入しアクセスすることは、ウィルスに感染している場合もあり大変危険です。中身を確認する前にウィルスチェックを行うようにしてください。
（2） インターネットは匿名ではありません。自分の行動に責任をもって利用するよう心がけてください。

3-4 パスワードの管理について

（1） センター発行のパスワードは、銀行の暗証番号と同じように大切なものです。定期的に変更して、管理には十分注意してください。
（2） 万が一、パスワードを忘れたら、学生証持参のうえ、本人が情報基盤センター事務室までお越しください。

■4. 情報基盤センターホームページ

http://www.cc.oita-u.ac.jp/

全ての情報は情報基盤センターホームページにて、詳細を公開しています。実習室のPCにログイン後表示される「お知らせ」・「FAQ」も随時更新していますので、確認しましょう！（一部、学内制限となっています。ご注意ください。）

挾間キャンパス（医学情報センター）の利用案内

■サービスの提供

全職員・学生向け

情報基盤システム(1 つのアカウントで複数の情報システムを利用可能
ウィルスソフト(symantec endpoint)
メールシステム(deepmail)
e-Learning システム(Moodle・Alc Netacademy)
学内インターネットサービス(有線と無線システム)
時刻サーバー（NTP サーバー）
廃棄パソコンのハードディスククラッシャー提供
学内周知文書システム
google カレンダー
ファイルサーバー
ウィルス感染などの相談受付とサポート
FW ポート開放申請受付
メーリングリスト申請受付
TV 会議システムサポート
web にて各種申請の受付（ID・端末）

職員向け

SPSS(職員のみ提供)
BUNGO⇔学内 LAN 間ファイル転送システム

学生向け

教育情報システム(学生端末とプリンターシステム

(1)	情報処理実習室	１３０台
(2)	ＬＬ教室	７１台(内１台は教員機)
(3)	チュートリアル教室	１２台
(4)	臨床講義棟ホール	２０台
(5)	自己学習室	１０台
(6)	医学図書館	１０台
(7)	医学情報センター	１台

ノートパソコン貸出システム(学生対象)

(1)	医学部	１６台
(2)	医学図書館	１０台
(3)	看護学科	１６台
(4)	医学情報センター	１台

学生端末にインストールされているソフトウェア

(1) ＯＳ ： Microsoft Windows 10

(2) マイクロソフト Word, Excel, Powerpoint

(3) SPSS Statistics Base 同時アクセス７０）

(4) シマンテックエンドポイント

(5) フリーソフト: Java, Acrobat reader, Flash Player, IrfanView

カラーレーザプリンタ

(1) 情報処理実習室	２台
(2) ＬＬ教室	２台
(3) チュートリアル教室	１台
(4) 臨床講義棟ホール	１台
(5) 自己学習室	１台

モノクロ複合機

(1) 情報処理実習室	１台
(2) 自己学習室	１台

CBT 試験サポート
LL 教室コールシステム技術提供

ホームページ
ホスティングサービス
ドメインサービス
HP サーバーの提供