ISSN 1343−9928

大学情報システム環境研究

2023年9月 VOL. 26

国公立大学情報システム研究会

目　　次

巻頭言

With コロナ及び After コロナの時代に大学を変革する DX の実現に向けて
To realize a real digital transformation in high education in an era of coexistence with COVID-19 and in post COVID-19 environment

会長　徐　浩源（Haoyuan XU）
横浜国立大学　学長特任補佐

文部科学省高等教育局は、令和 5 年 4 月末の事務連絡で、新型コロナウイルス感染症が 5 類感染症に移行する基本的な感染対策の考え方を通知しました。これまで 3 年余りにわたり、学生の学修機会の確保と感染対策の両立を図るためのさまざまな工夫を講じてきましたが、With コロナ・After コロナでは、日常における基本的な感染対策を行いながらも、大学などにおいては、教育研究活動の継続を前提とした上で、学生の学修機会の確保、学修者本位の教育活動を実施することが重要とされます。

さて、これまで構築してきた大学の情報インフラ環境は、新型コロナ蔓延していた時期に思う通り設計した IT サービスや設備の機能を利用者側、つまり学び側の学生や教える側の教員、研究を推進する研究者にはその価値を充分に提供することができませんでした。このような世界規模の出来事によって、多くの大学は、バーチャルキャンパス、スマートユニバーシティ、デジタルキャンパス、デジタルユニバーシティの構想などを打ち出し、ポストコロナを見据えた、新たな大学の DX「Digital Transformation」改革構想やプランを検討及び披露しました。デジタル技術の活用による大学の教育と研究活動、各種業務の運営に変革をもたらそうとしています。いわゆる、デジタルを活用した大学・高等教育の高度化を実現しようという動きが始まっています。

コロナは、この世界を一変させました。With コロナ・After コロナの時代には、大学教育のデジタライゼーションが欠かせないと、文科省が 2023 年度の「大学教育のデジタライゼーション・イニシアティブ推進委託事業」の公募が発表しました。Society5.0 に求められる新たな価値を創造できる人材育成に向けてデジタル技術で大学教育の価値を最大限に高め、学習者セントリックの学びを創造することに目指しているためだと思います。

また、大学が取り組む DX は、クラウドコンピューティングやデータセンター技術の進歩により、これまでの単なる情報のデジタル化とは異なり、バーチャルと現実との融合などを考える必要があり、真のＤＸの本質を求め試行錯誤で掘り下げることにチャレンジしなければなりません。IS 研の論文誌は、まさにこれらの課題解決に向けてさまざまな取り組みや試みを議論や発表の場となっています。ぜひ、IS 研会員の皆様が本論文誌というプラットフォームで日本の大学の DX の実現に向けて活躍することを期待しています。

xR 技術を活用した教育 DX システムの実証評価

Experimental evaluation of an educational DX system using xR technology.

東 昭孝, 西山 宣昭, 堀井 祐介，小林 恵美子
Akitaka HIGASHI, Nobuaki NISHIYAMA, Yusuke HORII and Emiko KOBAYASHI

金沢大学
Kanazawa University

金沢大学学術メディア創成センターは，2021 年度から全学 DX を推進する組織として，次世代の教育システムを目指し，メタバースの利用や，リアルタイム VFX システムを用いたスタジオでの撮影等，教育を中心とした DX 活動に取り組んでいる．特に DX 活動の中心となる教育 DX システムとして，VR や MR の総称である xR を大学の全構成員が利用できる xR キャンパスシステムの整備を進めている．現在システムは整備中であるが，一部の講義で VR ヘッドセットを利用して，システムに組み込み予定の DX 教材を開発して講義で利用した．本稿では，金沢大学における教育 DX システムの構築状況，講義で実証した評価について報告する．
キーワード：DX，VR，xR，教材作成

The Emerging Media Initiative at Kanazawa University has been working on DX activities to promote higher education since 2021. With the aim of creating a next-generation education system, we have particularly committed ourselves to making original contents with a real time VFX system in studios for metaverse. Setting an educational DX system in the center of the DX activities, we are currently developing the xR Campus System for the use of all members of the university. Although we are in the process of completing the system, we have developed and implemented some of the DX educational contents with a use of VR headsets for a few lectures in real classes. This paper reports on the present status of the educational DX system at Kanazawa University and the evaluation of the system and contents which have been used in the real classes.
Keywords：DX，VR，xR, Creation of teaching materials

1. はじめに

金沢大学学術メディア創成センターは，2021 年度に全学の DX 計画を戦略的に統括・推進するコア組織として改組により体制強化され，教育を中心とした DX 活動を推進している．特にメタバース内で講義を行えるように DX を推進している．メタバース内で効果的な講義を行うために，3D データを活用した DX 教材を作成して，システムを利用して講義で利用できるように取り組んでいる．DX を推進するためには，システムの整備が必要であり，作成した DX 教材を利用するために，ソフトウェア開発の専門知識がある職員を雇用し，システムの開発と整備を進めている．VR（仮想

*金沢大学学術メディア創成センター
〒920-1192　石川県金沢市角間町
Information Media Center, Kanazawa University
〒920-1192 Kakuma-machi, Kanazawa
E-mail: higashi@staff.kanazawa-u.ac.jp

現実)・AR（拡張現実)，VR と AR を包括する MR（混合現実）を含んだ拡張現実の総称である xR を対象として，様々なデバイスで利用可能なシステムとして整備している．代表的なシステムとして，作成した DX 教材を通常のブラウザで閲覧・操作を行い，専門的な知識が無くとも DX 教材を利用可能なシステムや，VR・MR ヘッドセット，スマートフォンでメタバースとして，講義で自由に利用できるシステムの構築を進めている．他にもリアルタイム VFX システムを活用した撮影が可能な講義にも利用可能なスタジオを整備した．このスタジオでは，作成した DX 教材を利用した撮影も可能である．システム開発では主に Unity と呼ばれるエンジンを利用しており，主にゲーム開発を中心として利用されているものであるが，近年はゲーム産業以外でも活用されている．教職員の大学の研究・業務，学生の就職活動や就職後の業務等，将来役立つ技術と判断し，この技術の支援活動も行っている．また Unity を通じてプログラミング教育の講義や，スタジオのリアルタイム VFX システムを利用した講義も行っている．今回，VR ヘッドセットで重点科目の一つで専用の DX 教材を開発し，講義を行った．本稿では，これらの DX 活動のシステムの構築状況，DX 教材を利用した講義で実証した評価について報告する．

2. 教育 DX システム整備

2.1 概要

作成した DX 教材を講義で利用するためには，3D データを表現可能なシステムが必要不可欠である．そのための取り組みとして，様々な DX システムの整備を進めている．現在，整備を進めているシステムを紹介する．概要として，図 1 に DX 取り組み全体図を示す．

2.2 DX 教材データベースシステム

xR キャンパスシステム（図 1 ②-2）では，VR ヘッドセットを利用するサービスを提供予定だが，整備まで時間がかかることや，VR ヘッドセット等，デバイスの準備をするのが大変であり，すぐに DX 教材を活用するのは難しい．それを補うため，ブラウザで 3D データの閲覧・操作を行い，講義に利用可能な DX 教材データベースシステム（図 1 ②-1）を構築中である．クラウドサービスにも可能なシステムは提供されているが，特定の利用者にアクセス制御することが難しいことや，閲覧記録を取れない等の理由により，独自システムで構築している．DX 教材を登録後，学習管理システム等のリンクから閲覧用の URL に誘導することで，通常講義で容易に利用することが可能になる．対応データは，3D データの obj 形式・fbx 形式，360 度静止画・動画，Unity のアセット教材（WebGL 形式）等の様々な形式が利用可能である．講義の利用を考慮して講義関係者のみ閲覧可能なアクセス制御を可能にし，アクセスログの提供を行い，講義に耐えられるシステムとしている．認証は金沢大学統合認証システムを利用し，全学 ID である金沢大学 ID による認証で，シングル・サイン・オンにより，金沢大学の全構成員がシームレスに利用可能である．認証なしの閲覧設定も可能で，学外者にも利用可能である．

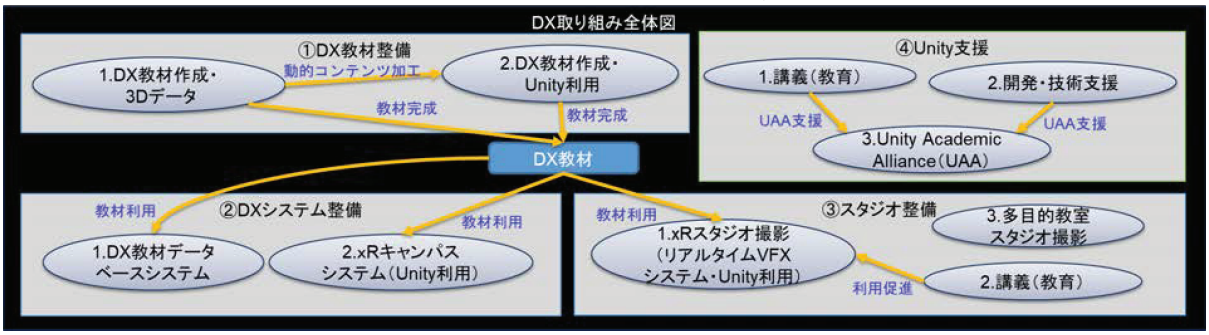


図 1 DX 取り組み全体図

2.3　xR キャンパスシステム

xR キャンパスシステム（図 1 ②-2）は，メタバース内で，アバターとして自分の分身が参加可能なシステムである．同様のサービスは存在しているが，独自で作成した 3D データを組み合わせて任意の表現が可能な DX 教材を利用できるサービスがない．また同時に同じ空間に参加できる人数制限があり講義の履修者全員の参加が難しいこと等の理由により，高い教育効果が見込める講義を行うことは難しいと判断した．そのため，独自でシステムを開発して整備を進めている．作成した DX 教材を利用した講義や，避難訓練等の各種イベント，相談室のような機能の実装を進めている（図 2）．講義を中心に考えており，VR ヘッドセット，パソコン，スマートフォンで利用可能とし，全講義情報と担当教員，履修者情報を反映して，全学 ID である金沢大学 ID で認証することで，全構成員が全講義ですぐに利用できるように整備を進めている．

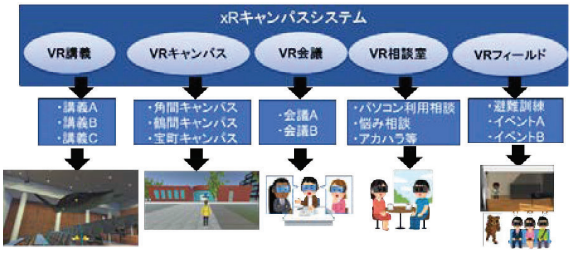


図 2 xR キャンパスシステム概要図

3.　DX 教材

3.1　教育 DX と狙い

教育で DX を活用するためには，まずは従来と比較して理解度が深まる教育効果を見込めるデジタル教材の作成（図 1 ①-1）が必要不可欠と考えた．従来の Zoom や Webex 等のオンライン配信による講義の課題として「講義に集中しにくい」「人との交流が少ない」「授業への意欲が低下すること」「課題が多いこと」等が挙げられることが多い[1]．この課題の解決策として，リアルタイムに臨場感がある空間で 3D データを利用した教材を講義や撮影で利用することで高い教育効果が見込めるのではないかと判断し，DX 教材の作成を開始した．

3.2　DX 教材作成と作成方法

DX 教材は，用途に合わせて様々な作成方法を用いている．Maya や Blender 等の 3D モデリングソフトで最初から 3D データを作成する方法，3D スキャナーの利用，フォトグラメトリと呼ばれる 2 次元の写真データから 3D データを作成する方法，3D データそのものではないが，360 度カメラを利用した 360 度静止画や 360 度動画を利用して教材を作成する方法で教材を作成している．それぞれの DX 教材の作成方法の比較を表 1 に示す．評価の◎○△×は，◎が最も高評価で×が最も低評価である．費用は一番安価な手法が◎，習熟時間は，経験が少なくても利用できる手法が◎，作成時間は，一番早く完成する手法が◎，後加工は，それぞれの手法で作成した後に，3D モデリングソフト等で，見た目の修正，データ量の削減，穴埋め処理等の手間が一番かからない手法が◎として評価したものである．

表 1 DX 教材作成方法の比較表

手法	費用	習熟時間	作成時間	完成度	後加工
3Dモデリング	◎	×	×	◎	◎
3Dスキャナー	×	○	○	○	△
フォトグラメトリ	△	△	△	○	△
360度静止画・動画	△	◎	◎	○	○

しかしながら，3D データを作成して閲覧・操作するだけでは，従来の教材と比較して教育効果が高まるとは言えない．そのため作成した 3D データの教材を Unity にインポートして，プログラムを利用（図 1 ①-2）し，3D データの一部を動かすことや，説明音声の再生，効果音や視覚的な表現を行い，説明テロップ等を表示することで，教育効果が高まる DX 教材として利用できるように取り組んでいる．

3.3　教材利用

作成した DX 教材は，後述する xR スタジオや xR キャンパスシステム，DX 教材データベースシステム等の様々な用途で無駄なく効率的に利用可能である．簡易 3D モデリングツールの Unity の ProBuilder を利用して 3D キャ

ンパスデータも作成を進めているが，クラウドサービスでメタバースを体験可能な Cluster[2]や VRChat[3]のサービスにもデータをアップロードし，世界中の誰でも金沢大学のキャンパスを体験できるように整備を進めている．この 3D のキャンパスデータの教材は，xR キャンパスシステムでも利用を予定している．360 度静止画・動画の教材は，通常は立ち入りが難しい場所の紹介や，遠隔地にある文化遺産等の説明で活用可能である．

3.4　体験型講義向け DX 教材作成

実際の講義利用のため，体験型の講義として，臨場感を重視して，VR ヘッドセットの Meta Quest 2[4]を対象に Unity を利用して DX 教材を作成した．自身がアバターとなり操作し，2 パターンの学習モードから選択して臨場感のある体験ができる．一つめのモードは，相手のアバターと対人距離を「密接距離」「個体距離」「社会距離」「公衆距離」をゲーム感覚で体験可能なパーソナルスペース教材である．自身のアバターと歩き回るアバターとの距離や対人距離を表示して体験可能である．もう一つのモードは，図 3 の通り，国籍と性別の違いで「対人距離の文化的違い」を体験する教材である．3 個の国籍と性別の違いで 6 種類の会話の距離を体験できる教材である．この二つのモードで体験可能な教材は，Meta Quest 2 のコントローラーを用いて操作するが，実際に歩いて利用することも可能である．

図 3 対人距離体験 VR プログラム

4.　スタジオ整備

4.1　xR スタジオ

2022 年 4 月に，本センターにあったパソコン実習が可能な演習室を廃止して xR スタジオとして整備した（図 1 ③-1）．このスタジオでは，グリーンバックのカーテン・カーペットを整備してクロマキーが利用可能である．またリアルタイム VFX システムである Vizrt[5]システムを導入した．このシステムは，大手の放送局や e-スポーツの撮影等でも利用されており，撮影中にリアルタイムに 3D グラフィックスを DX 教材・背景・テロップ等と合成し，その場での視聴や Zoom や Webex 等を利用したオンライン配信が可能なシステムである．録画してオンデマンドでの利用が可能で，視聴・オンライン配信・録画と 3 つを同時に行うことも可能である．カメラの映像と Vizrt，Unity，Unreal Engine 上で動作している DX 教材も撮影で利用することが可能で，ライブスイッチャーでリアルタイムに合成（図 4）し，配信することができる．

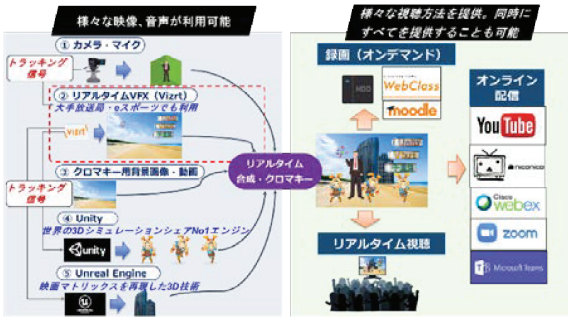


図 4　xR スタジオ概要図

xR スタジオの撮影スペースの横には，高性能なパソコンや 3D スキャナー，モーションキャプチャ等の各種機器を整備して，撮影した動画の編集や，DX 教材の作成支援，教育支援の場所としても活用できる施設となっている．xR スタジオからの配信は講義（図 1 ③-2）やイベントのみではなく，学会や研究集会等でも利用している．また遠隔でも，モーションセンサーでアバターとなり，利用できるように整備を進めている．

4.2　多目的教室スタジオ

アクティブラーニングの講義等で利用され

ている多目的教室にも，通常講義も兼用しながら，必要に応じてグリーンバックのカーテン・カーペットを準備してクロマキーによる撮影が可能なスタジオを整備した（図 1 ③-3）．幅が広いグリーンバックを整備したことで，走り回るような運動系の撮影や，多人数が同時に参加するグループワークの撮影が効果的に撮影可能である．必要な機材を搬入することで，xR スタジオと同様の撮影も可能である．

5. Unity 支援

5.1 Unity Academic Alliance

システム開発の中心として利用している Unity は前述したとおりゲーム産業以外でも，自動車産業・建設産業・不動産産業等，民間企業でも様々な用途で利用されている．将来的にも役立つ技術であり，3D データの扱い方も学習できること，比較的習得しやすい C#言語を利用しているためプログラミング学習に適していること，市場が急速に拡大しているメタバースとの親和性も良い等の理由により，教育支援を開始した．その一環として，2021 年 10 月に Unity Academic Alliance[6]（以下，UAA とする.）の契約を締結して支援を行っている（図 1 ④-3）．これは Unity の指導者を教育するための支援や，学生に対して教育支援が可能な取り組みである．Unity 認定試験受験料の無償化，ライセンスベース製品の割引き等の特典を受けることが可能である．

5.2 Unity 開発支援

Unity を利用した講義や研究，Unity 開発に興味のある学生・教職員が増えてきている．これらの人達のために Unity の開発支援を行っている（図 1 ④-2）．まだ少数だが DX システム開発の経験を活かして，Unity の利用方法・開発手法・プログラミング方法等の支援の取り組みも行っている．

5.3 Unity 講義

UAA の教育支援の取り組みやデータサイエンス教育の一つとして，2022 年 10 月（第 3 クォーター）から，Unity を利用した講義（図 1 ④-1）を違う内容の科目として年間 3 科目開講した．それぞれ全 8 回で，プログラミングから始まり，Unity の開発方法を学びながら，実践的な演習形式でサンプルゲームを開発する．将来を見越して Unity 開発が可能な人材の育成を進めている．

6. DX 教材の評価

6.1 講義利用

金沢大学で開講されている重点科目の一つである「異文化間コミュニケーション」[7]では，文化背景の異なる人々と効果的，かつ，適切にコミュニケーションを行うために必要な基礎的能力の構成要素について学習している．この講義は最大 52 人の学生が履修可能で，複数の教員が担当となり，全 8 回の同じ内容で 1 学期あたり 4～8 科目，1 年で 24 科目程の講義が行われている．重点科目ということもあり，毎回高倍率の抽選が行われている人気講義である．全 8 回のうち，国籍や性別の違いによる，対人距離の感じ方を学ぶ回がある．従来は学生同士が実際にお互いに距離を確認して，国籍や性別による対人距離を学んでいる．コロナ禍ということもあり，近距離で体験することを避けるために，この体験を DX 教材として提供することになった．今回は，この対人距離を学ぶ回を対象に 3 科目の講義で利用した．今回は 50 人程の学生が歩けるスペースの教室の準備は難しいため，椅子に座って教材を利用した．

6.2 講義支援

3.4 節で開発した DX 教材を約 60 台の VR ヘッドセットにインストールして準備した．講義日の前日に 400m 離れた教室に搬送し，バッテリーの充電を実施した．講義中は,5 人程の職員が VR ヘッドセットの配布，説明等の支援を実施した．VR ヘッドセットは，外から映像が確認できないため，代わりに装着して，映像を確認しないと何の問題が発生しているのかも不明であり，講義を円滑に進めるためには，複数人の支援は必須だったと言える．

6.3　アンケート結果

DX 教材体験後，今後の VR 教育の方向性を探ること，講義で DX 教材を VR で利用した際の有用性，メリット，デメリットを調査するため，講義中に LMS で記名式の授業アンケートを実施した．設問は 8 項目で 127 人の回答があった．回答について考察する．

設問 1 今まで VR ヘッドセットを使ったことがありますか？

回答は図 5 の通りである．大多数の学生が今回の講義で初めて VR ヘッドセットを利用したとの回答であった．そのため，操作方法がわからない学生が多かったが，すぐに慣れて問題なく操作できている学生が多かった．これは事前の説明資料の配布と教員が電源の入れ方からすべて詳細に説明したことによるものが大きい．

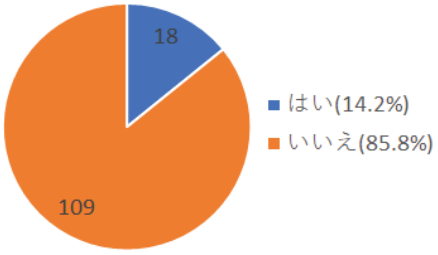


図 5 設問 1 回答

設問 2 この VR 教材によって対人距離の文化・性別による違いを体験できましたか？

回答は図 6 の通りである．肯定的な回答が 93.7%を占めており，講義の目的通り違いを体験できたと言える．VR で臨場感のある体験で違いを感じられたのではと考えられる．

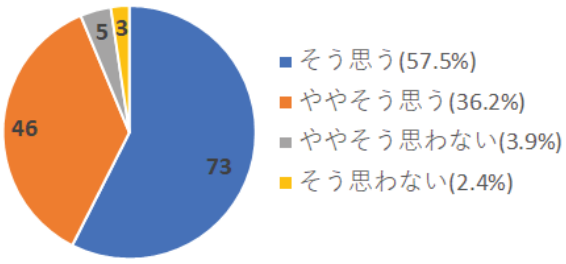


図 6 設問 2 回答

設問 3 この VR 教材によって対人距離の文化・性別による違いを理解できましたか？

回答は図 7 の通りである．こちらも肯定的な回答が 93.7%を占めており，理解が深まる教材を作成した言える．教材実行中も対人距離の説明等を確認可能であり，その機能の補助もあり，理解度が深まったと考えられる．

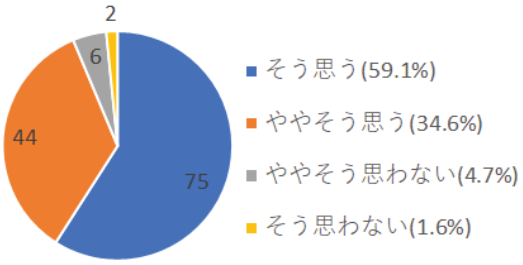


図 7 設問 3 回答

設問 4 この VR 教材の使い勝手や操作性は満足できるものでしたか？

回答は図 8 の通りである．操作性に満足している回答が 83.4%を占めており，操作性も概ね問題ないと思われるが，通常の VR ヘッドセットの操作とは違う点もあり，改善の余地はあると考える．今後，より講義がスムーズに進行できるように改良していく必要性を感じた．

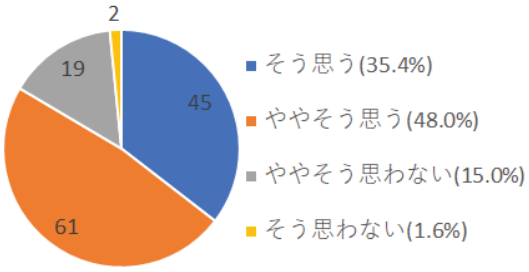


図 8 設問 4 回答

設問 5 通常の対面またはオンデマンド教材での教員からの説明・講義に加えて VR 教材を使用することで，学習が効果的に行えると思いますか？

回答は図 9 の通りである．肯定的な意見が 88.2%を占めており，VR の教材を併用することは効果的な学習と感じた学生が多くいることがわかる．臨場感のある体験によることが大きいと考えられる．

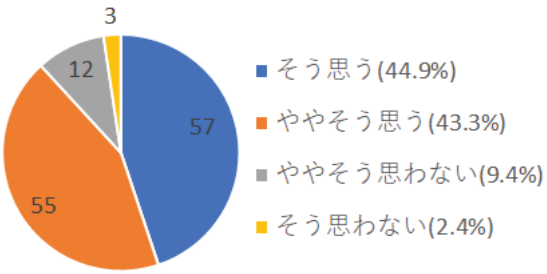


図 9 設問 5 回答

設問 6 ゲームをよくする方だと思いますか？

回答は図 10 の通りである．ゲームに慣れている学生は，VR ヘッドセットの操作もスムーズに行えると判断して実施した設問だが，現在の学生は全員がすぐに操作に慣れて操作しており，相関関係はなかったと言える．

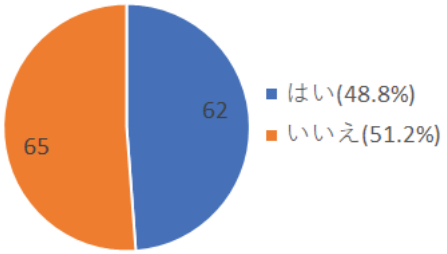


図 10 設問 6 回答

設問 7 この VR 教材は総合的に有意義なものでしたか？

回答は図 11 の通りである．総合的に満足した学生が 92.9%を占めており，VR ヘッドセットで利用する DX 教材は高い教育的効果が見込めると言える．

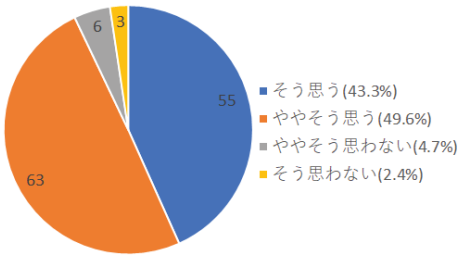


図 11 設問 7 回答

設問 8 本 VR 教材について，どうぞ率直なご意見をお聞かせ下さい．

この設問は自由記述である．いくつかの回答について報告する．否定的な意見として，酔って気持ち悪くなった・アプリの起動方法がわかりにくかった・操作がわかりにくい部分があった・実際に歩いて体験したかった・眼鏡を付けていると使いにくかった・機器が重かった・曇って見えにくかった等の意見があった．眼鏡では使いにくい，機器に関わる問題はすぐの解決は難しいが，教材やシステムを改良することで改善できる意見もあり，今後の参考にしたい．肯定的な意見としては，楽しめた・刺激的だった等の意見があった．ゲーム感覚で楽しむことができるため，通常の講義よりも楽しく刺激的に学習できたのではないかと思われる．

6.4 課題

アンケート結果から，概ね高評価と言える結果であったが，多くの課題も浮き彫りになった．大きな課題は以下の通りである．

- 1 科目あたり 50 人中 3 人程は途中で気持ち悪くなる VR 酔いが認められ，講義に参加できなかった学生がいた
- 教員は学生がどの画面を表示しているか，正常に操作できているかが不明であった
- VR ヘッドセットを初めて利用する学生が多く，DX 教材のアプリケーションを起動するまでに時間がかかった
- 何台かはコントローラーが効かない，電源が入らない等が発生し，体験ができなかった学生がいた
- 従来は 20 分程で完了する体験だったが，45 分ほどの時間が取られ，他の学習にかけられる時間が少なくなった
- 60 台の VR ヘッドセットの搬送と充電は大変だった
- 50 人程の学生に教員 1 人で対応は難しい

今後，これらの課題について，どのように解決していくか検討していく必要がある．一例として VR ヘッドセット以外のスマートフォン等で利用可能にする，教員が学生の画面を確認する手段の提供等が考えられる．

6.5 評価

アンケート結果から DX 教材を VR として利用した講義は，高い評価を得たと言える．今回の DX 教材は対面講義での利用のため， 3.1 節に挙げた課題とは直接的な比較はできないが，この DX 教材をオンラインで利用したと仮定した場合，全員が関心を持って講義に取り組んでいたことから「講義に集中しにくい」「授業への意欲が低下すること」の 2 個について改善したと言える．ただし，通常講義と比較すると様々な課題があり，通常利用は，時期尚早と感じた．今回で得た経験をもとに改善を進め，DX 教材として意味のある役に立つ教材を作成していく必要性を強く感じた．

7. まとめ

本稿では，本学の DX 活動の様々な取り組みを紹介した．DX 教材は，作成から xR スタジオ撮影・xR キャンパスシステム等のシステム利用・MR ヘッドセットでの利用と一連の流れで様々な用途で利用可能である．課題として，本学の DX 活動では 3D データの扱い，システム整備，Unity で DX 教材作成等，専門性の高いスキルが必須であり，人材の確保や高いスキルを身に着けることが重要である．

今回 DX 教材を VR ヘッドセットで 50 人程の講義で実践利用して評価・考察した．支援が行き届く 50 人程の中規模の体験型の講義形態で臨場感のある教材が適していたこともあるが，学生から高い評価を得たことから，DX 教材の有用性を確認できた．今後，様々な形態の講義とそれに合う DX 教材を作成し，実施効果を検証していく必要性を強く感じた．様々な課題も浮き彫りとなり，課題を解決しながら高い教育的効果がある教材作成，システム整備が必要である．今後もメタバース，xR を中心とした取り組みをもとに，スピード感をもって DX を展開し，様々な取り組みの実施し，新しい形の教育を推進していく．

参考文献

(1) 岡田 佳子, 学生からみたオンライン授業のメリットとデメリット ーオンライン環境下のアクティブラーニングに焦点を当ててー, 長崎大学 教育開発推進機構紀要, 11, pp.25-41, 2021 年 3 月
(2) Cluster, https://cluster.mu/ (2023 年 3 月 2 日参照)
(3) VRChat, https://hello.vrchat.com/ (2023 年 3 月 2 日 参照)
(4) Meta Quest 2, https://www.meta.com/jp/(2023 年 3 月 2 日 参照)
(5) Vizrt, https://www.vizrt.com/ (2023 年 3 月 2 日 参照)
(6) Unity Academic Alliance, https://unity.com/ja/products/unity-academic-alliance (2023 年 3 月 2 日 参照)
(7) 異文化間コミュニケーションシラバス, https://eduweb.sta.kanazawa-u.ac.jp//portal/Public/Syllabus/SyllabusSearchStart.aspx?lct_year=2022&fac_cd=-&lct_no=74C00a.413&je_cd=1(2023 年 3 月 2 日 参照)

著者略歴

東　昭孝
平成 29 年金沢大学大学院自然科学研究科電子情報科学専攻修了．博士（工学）．平成 6 年ソフトウェア開発会社に入社．平成 19 年 8 月より金沢大学にて学内ポータルのシステム構築・運用を担当，現在は令和 3 年 4 月に金沢大学学術メディア創成センター助教として従事．

西山　宣昭
昭和 60 年九州大学大学院修士課程農学研究科農芸化学専攻修了．工学博士，現在，金沢大学学術メディア創成センター教授．生物物理・化学物理・ソフトマターの物理，科学教育の研究に従事．

堀井　祐介
平成 10 年大阪大学大学院言語文化研究科言語文化学修了．博士（言語文化学）．現在，金沢大学数理・データサイエンス・AI 教育センター教授，専門分野は，大学評価，学習支援，デンマーク語，北欧神話，ポータルシステムの研究に従事．大学教育学会，日本高等教育学会，日本比較教育学会，高等教育質保証学会会員．

小林　恵美子
平成 9 年 University of Oklahoma コミュニケーション学研究科博士課程修了．Ph.D.（Communication）．現在，金沢大学国際基幹教育院教授，専門分野は，ジェンダーと逸脱行動の文化比較，合理的意思決定モデル，日米比較，コントロール理論，ホフステッドの文化次元，犯罪理論の異文化適応性，異文化間コミュニケーションの研究に従事．American Society of Criminology，International Association for Cross-Cultural Psychology，日本教育社会学会会員．

組織内端末の Web アクセスの規則性に着目したプロキシログ中の異常検知

Anomaly detection of proxy log focused on website access pattern of organization device

名倉 悠 *，青木 茂樹 *,†，宮本 貴朗 *,†
Yu NAGURA*, Shigeki AOKI*,†, and Takao MIYAMOTO*,†

大阪府立大学 *　　大阪公立大学 †
Osaka Prefecture University　Osaka Metropolitan University

近年，不正侵入して組織内の機密情報を窃取する攻撃が増加している．このような攻撃は未然に防ぐことが難しいため，侵入後の迅速な検知が求められている．攻撃の早期発見には情報システム内に蓄積されたログを解析し，各端末の普段とは異なる挙動を検出する必要がある．本稿では，組織内で使用される端末の通信は，使用するユーザごとに固有の規則性が現れると仮定し，確率モデルによりユーザの通信パターンを学習して異常を検知する手法を提案する．実験では，大阪府立大学の職員用端末のログと，公開データセットを用いて有効性を確認した．また，不特定多数が使用する端末のログを用いた場合や従来手法を用いた場合との比較評価を行った．

キーワード: ログ解析，侵入検知，確率モデル

Recently, cyber attacks that compromise devices, and steal confidential information are increasing. Since it is difficult to prevent intrusion of them, rapid detection of the infected devices is needed. In order to detect the devices early, we need to find unusual behaviors of each device. In this paper, we assume that communication patterns of devices used within organization are unique to each user, and propose a method for anomaly detection using probability model learned the communication pattern of the device. In order to confirm the effectiveness of our method, we conducted experiments using proxy log of devices used by staffs of Osaka Prefecture University.

KeyWords: Log analysis, Intrusion detection, Probability model

1　はじめに

近年，端末に不正侵入し，機密情報を窃取する攻撃の増加が社会問題となっており，情報システムを健全に運用するために，対策が急務となっている．従来では，ネットワークの境界に Firewall を設置することや，シグネチャ型侵入検知システムを適用することにより，不審な通信を遮断して組織内ネットワークへの侵入を未然に防ぐなどの対策が行われてきた．しかし現在では，標的型攻撃 [1] のように攻撃の複雑化，巧妙化が進んでおり，侵入前に検知する従来の手法だけでは十分な対策が行えず，情報漏洩のリスクが効果的に解消されない問題がある．このため，侵入された後に端末の挙動を解析し，迅速に異常を検知するシステムの開発が求められている．

標的型攻撃等の検知のため，教師あり学習手法を用いた手法が多く提案されている．しかし，情報システムに対する攻撃の検知においては，攻撃の種類が膨大であることや，亜種攻撃など未知の攻撃の発生頻度が高いために，十分な教師付きデータを収集することが難しい．そこで，今日では教師付きデータを必要としない教師なし学習を用いた研究が盛んに行われている．このような教師なし学習による異常検知手法の例として，文献 [2] が挙げられる．この手法では，Proxy ログの各行をクラスタリングして，得られたクラスタ番号を端末ごとに並べた系列を作成し，系列中のクラスタ間遷移の出現頻度を用いて異常を検知している．し

*大学院人間社会システム科学研究科
Graduate School of Humanities and Sustainable System Sciences
†情報基盤センター
〒 599–8531 大阪府堺市中区学園町 1–1
Center for Information Initiative
1–1, Gakuen-Cho, Naka-ku, Sakai, Osaka, 599–8531, Japan.

かし，異常ログが長期間連続した場合などに正しく異常として検知することが難しいという課題がある．

一方文献 [3] では, 情報端末の位置情報などから抽出した，ユーザの普段の行動パターンを表すシンボルの系列を学習することで高精度に異常を検知する手法を提案している．

本稿では，組織内で使用される利用者が固定された端末の通信は，使用するユーザごとに固有の規則性が現れると仮定し，Proxy ログから抽出したユーザ固有の通信パターンを学習した確率モデルを用いて，異常を検知する手法を提案する．実験では，大阪府立大学の職員用端末の Web アクセス履歴と，公開データセットを用い，本手法の有効性を確認した．また，不特定多数が使用する端末を用いた場合や従来手法 [2] との比較評価を行った．

2　関連研究

本研究に関連する研究として，Proxy ログの各行に付与したシンボルの遷移確率を基に異常を検知する文献 [2] と，シンボルの遷移単体ではなく，遷移を基にして得られる規則性を学習して異常を検知する手法を紹介している文献 [4]，無線 LAN 利用ログから抽出した端末の利用状況の時系列パターンを基に異常検知する手法 [3]，Proxy ログの各行に付与したシンボルの時系列パターンを基に異常検知する手法 [5] について述べる．また，URL の文字列を利用した異常検知の研究として，文献 [6, 7] について述べる．

文献 [2] の手法では，まず Proxy ログの各行から URL の全長や受信データサイズなどの 67 次元の特徴量を抽出し，クラスタリングする．その後 Proxy ログを端末ごとに分類し，各ログに付与したクラスタ番号を時系列順に並べてクラスタシーケンスを作成する．クラスタシーケンス中のクラスタ間遷移を bi-gram で抽出し，各遷移の発生確率を求める．全ての遷移について発生確率を求めた後，各ログについて，前後 5 行の間に存在する遷移の確率を用いてスコアリングする．そして，算出したスコアが閾値より小さい場合に異常なログとして検出する．この手法では，スコアリングの際にシーケンス中の 11 行のログのみに注目していることから，異常ログが長期間連続する部分でスコアが大きくなり，異常を正しく異常として検知することが難しい場合がある．

一方，文献 [4] では，シンボルの系列を用いた異常検知手法について取り上げており，様々な異常検知手法をその性質や特徴ごとに分類したうえで幅広く紹介している．紹介されている異常検知手法の 1 つに，シンボル間の遷移にマルコフ性を仮定し，遷移を学習した後に新たなシンボル系列の生起確率を求めて異常検知する手法がある．文献 [3] では，無線 LAN 利用ログから端末の位置情報や送受信パケット数を抽出し，これらの特徴量の時系列変化をユーザの普段の行動パターンとして確率モデルで学習して行動認証を行っている．端末が普段の行動には見られない不審な移動をしていた場合，その一連の行動の生起確率が小さくなる．そこで生起確率が閾値より小さい場合に異常として識別する．このように行動パターンを学習して異常検知を行うことで，高精度な検知を可能にしている．また文献 [5] では，Proxy ログの各行から特徴量を抽出してクラスタリングした後，クラスタシーケンスを作成し，ユーザの通信パターンを学習する手法を提案している．検出対象のクラスタシーケンスが，学習した確率モデルから生成される確率を求め，閾値より小さい場合に異常として検知している．しかしこの手法では，長いセッションが多いことや，要素数が少ないクラスタが多数存在する影響で，シーケンス長が極端に長い正常シーケンスが存在する場合などに誤検知が多く発生することが課題として挙げられている．

URL から抽出した文字列を用いて異常検知を行っている研究について述べる．文献 [6] では，URL や HTML タグから特徴量を抽出し，CBA アルゴリズムを用いて不審な URL を検出する手法を提案している．この研究では，URL から抽出する特徴量として，“;” や “_” をはじめとした記号や特定の単語が現れる回数を利用している．また文献 [7] では，HTTP リクエストのパラメータから特徴量を抽出し，各パラメータの文字列を，アルファベットや数字などの属性ごとに新たに定義したクラスに変換する．変換したクラス列を学習し，解析対象のデータから新たに作成したクラス列との類似度を用いて異常検知を行う手法を提案している．以上の文献 [6, 7] では，異常検知において URL の文字列をそのまま扱うのではなく，加工して様々な情報を抽出している．近年では一般的にセキュリティ意識が高まっており，HTTP 通信暗号化を施した通信が用いられている．そのため Proxy ログに記録される Web アクセス履歴では URL のパス以下のパラメータが容易に取得できないことが多くなっている．本手法ではこのような事態を想定し，URL のドメイン部分から多くの情報を抽出できるよう，文献 [6, 7] を特徴量選定の参考としている．

表 1: 特徴量の一覧

特徴量	次元
受信データサイズ	1
ドメインの長さ	1
ドメインに含まれる数字の数	1
ドメインに含まれる大文字の数	1
ドメインに含まれる単語の数	1
リクエスト URL 内の IP アドレスの有無	2

3　提案手法

提案手法は大きく分けて，特徴抽出，クラスタシーケンス作成，確率モデル作成，異常検知の 4 ステップで構成されている．以下，それぞれのステップについて詳しく述べる．

3.1　特徴抽出

本手法では，ユーザが行った各通信の特徴が Proxy ログの各行のパラメータに現れると考え，文献 [2, 6, 7] を参考に，Proxy ログから SSL 通信の場合でも安定して抽出できると考えられる，表 1 に示す 6 種類，7 次元の特徴量を抽出する．まず，受信データサイズ，ドメインの文字列の全長，ドメインに含まれる数字の数，ドメインに含まれる大文字の数，“.” (ドット) で区切ったドメインに含まれる単語の数を特徴量として抽出する．これらは各特徴量の尺度を合わせるために平均 0，標準偏差 1 となるように標準化する．次に，リクエスト URL の文字列中に，IP アドレスが直接書きこまれている部分が存在するかを調べる．一般に，正常なサイトの URL 中に IP アドレスが含まれることは稀であり，URL 中に IP アドレスが含まれることの異常検知に対する重要度は高いと考えられるため，存在する場合に $(1, 0)$，存在しない場合に $(0, 1)$ となるように 2 次元のベクトルで表す．こちらも他の 5 次元の特徴量と同様に標準化する．本手法で使用するログと抽出する特徴量，抽出方法の具体的な例を図 1 に示す．図 1 の例では，受信データサイズはログに記述された通り 1508 Byte である．また，ドメインに関しては，リクエスト URL 中の “www.ABCD.1234.com” の部分に着目する．この場合，ドメインの全長が 17，数字の数が 4，大文字の数が 4 である．単語の数はドメインの文字列をドット記号で区切ってカウントし 4 となる．リクエスト URL 内の IP アドレスの有無については，先述したように URL 部分に着目して調べる．この例では IP アドレスの文字列が存在しないため，特徴ベクトルは $(0, 1)$ となる．

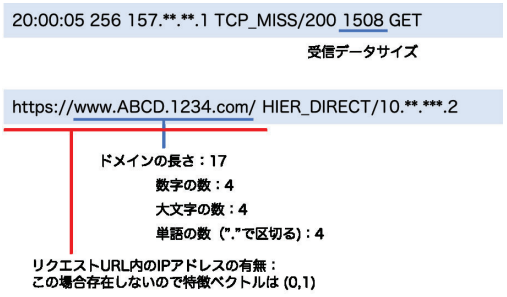


図 1: ログと特徴量抽出の例

3.2　クラスタシーケンス作成

前節で作成した特徴ベクトルを混合ガウスモデル (Gaussian Mixture Model, GMM) によりクラスタリングする．GMM とは，複数のガウス分布を重ね合わせ，データ点がそれぞれの分布に所属する確率を求め，最も所属確率が高い分布をそのデータ点が所属するクラスタとして決定する手法である．クラスタリング後，各クラスタにつけたラベルを用いて，ログの各行にラベル付けを行う．

一般的に，ある個人が業務等において組織内の端末を用いてアクセスする Web ページの閲覧パターンには，それぞれ固有の特徴が表れると考えられる．特に，ポータルサイトからメール，各種業務に用いるシステムやページへのアクセス等，各場面での短期的な遷移はある程度習慣化されており，そのユーザの特徴が顕著に表れると考えられる．そこで，個人の各業務で行われる短期的な通信パターンを正しく学習できるように，時間情報を基に Proxy ログを分割し，複数行のログの組からなるセッションを定義する．セッションに含まれる各ログに与えられたクラスタのラベルの系列をクラスタシーケンスとする．クラスタシーケンスの作成の例を図 2 に示す．まず，Proxy ログを，送信元 IP に注目して端末ごとに分類する．次に，端末ごとにセッション単位に分割する．セッション単位への分割には各ログのタイムスタンプに注目する．あるログから次のログまでのタイムスタンプの間隔が 15 秒以内の場合は同じセッションとして扱い，15 秒を越える場合にはそこで分割し，別のセッションとして扱う．セッションに分割した後，クラスタリング時に付与されたクラスタのラベルの系列を，時系列順を維持したまま抽出し，クラスタシーケンスとする．

3.3　確率モデル作成

前節で作成した端末ごとのクラスタシーケンスの集合を用いて，単純マルコフ連鎖の確率モデル

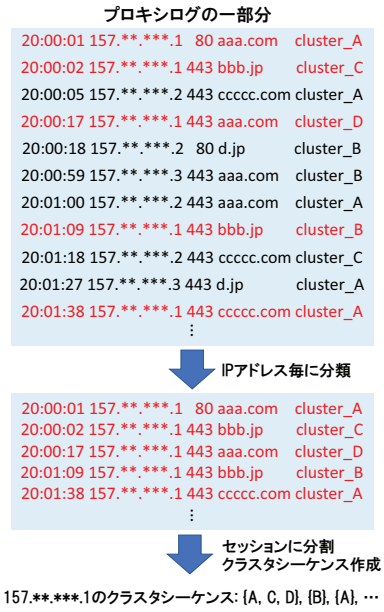


図 2: クラスタシーケンス作成の例

を作成する．

まず，シーケンス中に現れるあるクラスタから次のクラスタへと遷移する確率を求める．遷移の確率は式 (1) で表される．

$$P_i = P(X_{i+1}|X_i) \tag{1}$$

ここで，X_i，X_{i+1} はそれぞれシーケンス中の i，i+1 番目のクラスタのラベルを表す．求める遷移確率 P_i は条件付き確率であり，シーケンス中の i 番目のクラスタのラベルからの遷移のうち，i+1 番目のクラスタのラベルへと遷移するものの割合として求める．端末ごとに作成したシーケンス中に存在する全てのクラスタ間遷移について遷移確率を求め，それらを成分とした状態遷移行列を作成し，異常検知に用いる確率モデルとする．ここで，マルコフ連鎖では各シーケンスの先頭状態が決定される確率を初期分布として定義する必要がある．しかし本手法では，シーケンスの生起確率を用いて異常検知を行うことから，初期状態は固定しなければならず，任意の値で決定することができない．そこで，先頭記号 (“[BOS]”) を設置し，全てのシーケンスは必ず先頭記号から始まることとし，各シーケンスの最初のクラスタのラベルは先頭記号からの遷移確率で決定する．

3.4　異常検知

前節で作成した確率モデルを用いて異常を検知する．学習に用いたものとは別の期間の Proxy ログに対して，3.2 節と同様の手法によりクラスタシーケンスを作成する．ここで作成したクラスタシーケンスが，学習済みの確率モデルから生成される確率を求め，尤度とする．マルコフ連鎖において各状態は独立であるため，シーケンスの生起確率はシーケンス中の全遷移の確率の積で求められる．また，尤度について，小数点以下の比較を平易にするために対数尤度を用いて求め，シーケンスの長さによる不均衡を解消するためにシーケンス長で正規化を行う．求める尤度 D を式 (2) に示す．

$$D = \frac{1}{T}\log_{10}\prod_{i=1}^{T-1} P_i \tag{2}$$

ここで，P_i は前節で述べた i 番目のクラスタのラベルから i+1 番目のクラスタのラベルに遷移する確率を表している．T はクラスタシーケンスの全長であり，長さ T のクラスタでは，$T-1$ 回の遷移が行われている．ここで，例えば普段訪れるページとは全く類似しないページに訪れた場合など，検出対象のクラスタシーケンスに現れる遷移の中には，学習した確率モデルに存在しない遷移が含まれている場合がある．遷移確率が 0 の場合正しく尤度を求められないため，遷移確率に十分小さい値を与える．式 (2) で算出する対数尤度 D は，シーケンス中に出現頻度が低い遷移が多く含まれているほど値が小さくなる．したがって，普段の通信パターンに類似した正常なシーケンスでは尤度が大きくなり，そうでない場合は尤度が小さくなる．算出した尤度が閾値より大きい場合，そのシーケンスおよびセッションは正常とし，閾値以下の場合，異常であると判断する．

4　実験と考察

4.1　実験条件

本手法の有効性を確認するために実験を行った．実験では，大阪府立大学（以下，本学とする）の Proxy サーバに記録された職員用端末 10 台の Web アクセス履歴に，MWS2018 の BOS データセット [8] から抽出した異常ログを挿入したデータと，同様にチェコ工科大学 (CTU) が公開している CTU データセット [9] から抽出した異常ログを挿入したデータを使用した．実験に使用するデータセットの詳細については次節で述べる．

また，本手法で用いる GMM クラスタリングでは，クラスタリングを行う前にあらかじめクラスタ数を決定する必要がある．本手法では，ベイズ情報

量基準 (Bayesian Information Criterion, BIC) を用いて最適なクラスタ数を推定して決定している．BIC とは，統計モデルの有効性を評価するための指標の 1 つであり，この値が小さいほど有効性が高いモデルとなる．実験では，クラスタ数を 1 から十分大きな値まで 1 ずつ増加させながらクラスタリングを行い，BIC を用いて分類結果を評価し，BIC の値が最小となる時のクラスタ数を異常検知で用いるクラスタ数としている．さらに本手法では，外れ値による極端な影響を抑えるため，クラスタの要素数が 50 以下のクラスタを全てまとめ，新たな 1 つのクラスタとした．実験結果の評価には，ROC (Receiver Operating Characteristic) 曲線を描いたときの，AUC (Area Under the Curve) 値を用いた．

4.2　実験データ

実験に用いるデータについて述べる．本学職員用端末のログには正常／異常のラベル付けはされていないが，実験に用いるログの期間には異常を報告されていないことから，本実験では全て正常として扱った．公開データセットについては，各データに含まれる異常ログを抽出し，実験データに挿入後も異常ログとして扱う．また，異常ログの挿入について，BOS データセットの場合は C2 (Command and Control) サーバと通信しているログを，CTU データセットの場合はボット通信を行っているログを抽出し，職員用端末の Web アクセス履歴の任意の部分に，その部分の時刻に変換して時系列順を維持したまま挿入した．

その後，本学職員用端末が不審な通信を行っていることを疑似的に再現するため，挿入するログの送信元 IP アドレスを挿入先の端末と同じ IP アドレスに変換した．どちらのデータを使った実験においても，正常ログのみが含まれる本学職員用端末の Web アクセス履歴を用いて学習し，当該端末の別期間の Web アクセス履歴に異常ログを挿入したデータを用いて評価した．

4.2.1　実験データ 1 (BOS 混合データ)

MWS2018 データセットのうちの 1 つである BOS データセット [8] は，標的型攻撃のマルウェアをローカルネットワークに接続された端末に感染させ，感染後の挙動を記録したデータセットである．BOS データセットは，端末と C2 サーバとの通信状況によって，進行度 1 から進行度 8 までの段階が定義されている．マルウェアを実行したが C2 サーバとの通信が発生しなかった場合に進行度 1，2，マルウェアの実行後 C2 サーバとの通信が発生したが，成立しなかった場合に進行度 3，4，5，マルウェアの実行後，C2 サーバとの通信が発生し，かつ成立していた場合に進行度 6，7，8 と定義され，期間ごとにデータが分類されている．なお，提供されているデータは pcap 形式であるため，あらかじめ pcap 形式のデータを Proxy ログの形式に変換した．

表 2: BOS 混合データの内訳

データ	日付	正常	異常
学習データ			
本学職員用端末 Web アクセス履歴	2019/9/29 から 7 日間	端末ごとに異なる	0
テストデータ			
本学職員用端末 Web アクセス履歴	端末ごとに異なる	22476	0
BOS データセット	2018/1/23, 26	0	1617

表 3: CTU 混合データの内訳

データ	日付	正常	異常
学習データ			
本学職員用端末 Web アクセス履歴	2019/9/29 から 7 日間	端末ごとに異なる	0
テストデータ			
本学職員用端末 Web アクセス履歴	端末ごとに異なる	26840	0
CTU データセット	2013/8/20	0	1501

実験では，学習用データには本学職員用端末の Web アクセス履歴中の 2019 年 9 月 29 日から 7 日間分のログを抽出して使用した．ここで，組織内端末の通信パターンは曜日ごとに特徴が現れると考え 7 日間とした．なお，一度でも端末が通信を行った日のみを 7 日間分使用している．そのため，ログが一行も存在しない日については日数にカウントしていない．これにより，起算してから 7 日目のログの日付や，抽出するログの行数は端末ごとに異なっている．テストデータには，本学職員用端末の，9 月 29 日から 8 日目以降の Web アクセス履歴に，BOS データセットの進行度 8 のデータ (2017 年 12 月 23 日，26 日) から C2 サーバと通信が行われている異常ログを抽出し，挿入した 24093 行のログを使用する．テストデータについてはどの端末を用いた実験においても同じ行数としている．以下，本学職員用端末のデータと BOS データセットとの混合データセットを BOS 混合データとする．表 2 に内訳を示す．

表 4: 実験結果

端末	学習データ数	AUC (BOS)	AUC (CTU)
端末 A	77324 行	0.99	0.92
端末 B	79443 行	0.99	0.95
端末 C	70096 行	0.83	0.86
端末 D	81650 行	0.86	0.98
端末 E	32346 行	0.98	0.97
端末 F	35187 行	0.99	0.93
端末 G	71545 行	0.98	0.95
端末 H	51914 行	0.92	0.96
端末 I	36146 行	0.96	0.96
端末 J	69730 行	0.98	0.95

4.2.2　実験データ 2 (CTU 混合データ)

CTU データセット [9] はチェコ工科大学 (Czech Technical University in Prague, CTU), Stratosphere Research Laboratory の Stratosphere IPS Team が研究用に収集，作成したデータセットである．マルウェアによる通信をキャプチャしたトラフィックデータや IoT 端末のトラフィックデータなど多数の研究用データセットが公開されている．本実験ではその中でもマルウェアによるボットネットトラフィックをキャプチャし，端末の挙動を観測したラベル付きデータを使用した．

学習用データには BOS 混合データと同様に本学職員用端末の 2019 年 9 月 29 日から 7 日間のログを使用した．テストデータには起算から 8 日目以降の本学職員用端末の Web アクセス履歴に，CTU データセット中の MALWARE CAPTURES に収録されている 2013 年 8 月 20 日のデータ (CTU-Malware-Capture-Botnet-4/2013-08-20_capture-win2.weblogng.labeled から取得) からボット通信を行っているログを一部抽出し，挿入した 28341 行のログを使用する．こちらのデータもどの端末を用いた実験においても同じ行数としている．以下，本学職員用端末のデータと CTU データセットとの混合データセットを CTU 混合データとする．表 3 に内訳を示す．

4.3　実験結果

実験に使用した 10 台の本学職員用端末を順に端末 A〜端末 J とする．表 4 に端末ごとに使用した学習データのログの行数と，BOS 混合データでの AUC 値，CTU 混合データでの AUC 値を示す．また，BOS 混合データを用いた実験結果の ROC 曲線を図 3 に，CTU 混合データを用いた実験結果の ROC 曲線を図 4 に示す．BOS 混合データを用いた結果の AUC 値は 0.83〜0.99，CTU 混合データを用いた結果の AUC 値は 0.86〜0.98 となった．実

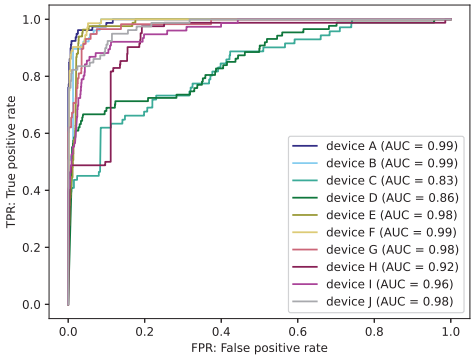


図 3: BOS 混合データの ROC 曲線

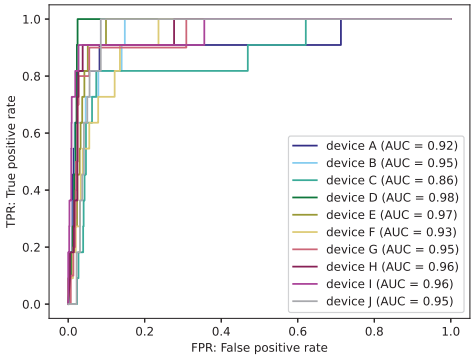


図 4: CTU 混合データの ROC 曲線

験結果の大半がどちらのデータを用いた場合でも AUC 値 0.95 以上を記録し，本手法の有効性を確認できた．端末ごとに普段の通信パターンを学習したことにより，学習データに用いたログの行数によらず，全体を通して高い検知精度となったと考えられる．しかしながら，中には精度が低い端末や BOS 混合データセットと CTU 混合データセットとの間で AUC 値に大きな差がある端末が存在している．次節で，それぞれのケースについて考察する．

4.4　誤検知，検知漏れにおける考察

全てのデータにおいて誤検知が発生する原因として，正常ログの中には要素が少ないクラスタに分類されるログも存在することが挙げられる．例えば普段訪れないページにアクセスすると，出現頻度が小さいクラスタ間遷移が発生し，結果として尤度が小さくなることがある．これにより，正常なシーケンスでも誤って異常であると識別される場合がある．学習時には存在しない遷移がテストデータ中に現れるケースもいくつか存在しており，この場合遷移確率に小さい値が与えられるため，尤度がかなり小さくなり正常なシーケンスが異常であると識別されやすい傾向があった．本実験では，このような誤検知を抑えるよう外れ値を

考慮して極端に要素数が少ないクラスタをまとめて 1 つのクラスタとして扱う処理を行ったが，この処理の最適化が必要であると考えられる．

両データセットの実験結果ともに検知精度が低くなっている例について述べる．端末 C の結果は，AUC 値が BOS 混合データで 0.83，CTU 混合データで 0.86 となり，どちらも本実験で使用した 10 台の中で最も検知精度が低い．これは，多数の正常ログで構成されたシーケンス長が大きいシーケンスの中に，数行の異常ログが含まれていた場合に，正しく異常シーケンスとして識別できないことが大きな原因であったと考えられる．また，異常ログの一部が，正常データのクラスタに割り当てられたために，尤度が大きく算出され，誤って正常としている場合があり，こちらも検知精度が低くなった原因となっている．

続いて端末 A や，端末 D，端末 F に見られるような，BOS 混合データと CTU 混合データとで AUC 値に差があり，一方の精度が低くなっている例の原因について考察する．本実験では，公開データセットから抽出した異常ログを本学職員用端末の Web アクセス履歴に挿入する際，それぞれ任意の行に挿入している．また，同じ職員用端末のデータを用いた場合でも，BOS 混合データを挿入する場合と CTU 混合データを挿入する場合とで挿入する箇所も異常ログの行数も異なっている．したがって，セッション中の異常ログの数や，セッション中の正常ログと異常ログの比率，セッションの長さなどがデータセットにより異なる．そのため，BOS 混合データと CTU 混合データとで AUC 値の傾向が異なる結果になったと考えられる．また検知精度の低さについては，こちらも端末 C の場合と同様の理由による検知漏れが発生している傾向が見られた．

以上で述べた検知漏れの大きな原因となった，セッションが長く正常ログの割合が大きいセッションについては，実環境においても，通常の Web ページの閲覧中に C2 サーバとのビーコン通信が発生した場合などに発生しうると考えられるため，対策の検討が必要であると考えられる．

4.5 比較実験 1：不特定多数が利用する端末を用いた実験

4.5.1 比較実験条件 1

組織における業務用に用いられる端末ではなく，不特定多数のユーザがそれぞれの目的のために用いる端末の Web アクセス履歴を用いて実験を行った．不特定多数のユーザが使用する例として，本学の共有スペースに設置されている学生用の端末を用いた．これらは利用可能な時間であれば学生が任意の時間に任意の端末を利用できる．実験ではこれら学生用端末 3 台の Web アクセス履歴を使用した．実験データについては，4.2 節で述べた実験条件と同様に作成した．各端末の 7 日間の Web アクセス履歴を学習データとし，8 日目以降の Web アクセス履歴に BOS，CTU データセットから抽出した異常ログを挿入したものをテストデータとした．なお，テストデータのログの行数は 4.2 節で述べた実験データと同じ 24903 行，28341 行で揃えた．

表 5: 学生端末の実験結果

端末	AUC (BOS)	AUC (CTU)
端末 X	0.59	0.78
端末 Y	0.87	0.95
端末 Z	0.81	0.80

4.5.2 比較実験結果，考察 1

実験に使用した 3 台の端末をそれぞれ端末 X，端末 Y，端末 Z とする．表 5 に実験結果を示す．表のとおり，AUC 値にはかなりばらつきがあることが分かる．端末 Y の AUC 値は職員用端末を用いた場合と大差ない結果となっているが，端末 X，端末 Z の AUC 値は職員用端末と比較して低い結果となっている．4.3 節で示した実験結果と比較して，Web アクセス履歴の性質によって，実験結果が大きく変わることが分かった．

検知精度が低くなる原因については，概ね 4.4 節で述べた例と同じ傾向があると考えられる．学生用の端末は，学生が任意のタイミング，任意の期間，任意の目的で用いるため，訪れる Web ページの性質や滞在時間も多岐にわたる．このため，出現頻度が小さいクラスタ遷移や，学習データに存在しないクラスタ遷移が多く発生し，正常セッションであるにも関わらず異常であると識別される例が顕著に現れた．そのため，全体的に検知精度が低くなっていると考えられる．このように，不特定多数が利用する端末が行う通信には規則性が表れづらいため，上手く学習できない．本手法は，組織内の職員の端末のような，通信がある程度固定化，習慣化されている端末に対して特に有効であると考えられる．

表 6: 従来手法 [2] の検証に用いた特徴量の一覧

特徴量	次元
受信データサイズ	1
URL の全長	1
URL のパスの長さ	1
URL のクエリの長さ	1
URL でクエリされた値の数	1
リクエスト URL 内の IP アドレスの有無	2
リクエストファイルの有無	2
宛先 IP アドレスの 2 進数表記	32

表 7: 従来手法 [2] を用いた場合の実験結果

端末	AUC (BOS)	AUC (CTU)
端末 A	0.18	0.75
端末 B	0.22	0.77
端末 C	0.08	0.71
端末 D	0.51	0.92
端末 E	0.13	0.36
端末 F	0.04	0.76
端末 G	0.20	0.77
端末 H	0.28	0.76
端末 I	0.09	0.60
端末 J	0.29	0.85

4.6　比較実験 2：従来手法 [2] との比較

4.6.1　比較実験条件 2

従来手法との比較を行うため，文献 [2] で用いられている手法を用いて実験を行った．使用する実験データ，クラスタ数については 4.1 節，4.2 節で述べた条件と全て同一とした．ただし，従来手法では学習データとテストデータを分割していないため，この実験ではデータを連結して使用している．表 6 に今回の比較実験で抽出した特徴量を示す．ここで，従来手法で抽出されているが，今回の実験で用いるデータでは抽出が不可能な特徴は省略している．また，URL のパス以下の情報については，HTTPS 通信などでログに記録されていない場合，値が 0 となるよう加工した．宛先 IP アドレスの 2 進数表記については，宛先 IP アドレスを 2 進数に変換し，それぞれの桁を 1 次元，計 32 次元の特徴ベクトルとして扱っている．これらの特徴量は抽出後全て平均 0，標準偏差 1 となるように標準化した．尤度の算出方法については，従来手法と同じ条件でスコアリングを行った．

4.6.2　比較実験結果，考察 2

表 7 に端末 A〜端末 J それぞれの実験結果を示す．従来手法を用いた場合の AUC 値は，BOS 混合データでは 0.04〜0.51，CTU 混合データでは 0.36〜0.92 となり，こちらも全体的に提案手法より検知精度が低い結果となった．特に，BOS 混合データでは検知精度が大幅に低下しており，異常データをほとんど検知できていない結果となった．従来手法ではセッションを定義せず，bi-gram を用いて遷移を抽出しスコアリングを行っているため，提案手法よりも検知精度が低くなったと考えられる．

検知漏れが多く発生した原因について順に考察する．まず，従来手法においても遷移確率の導出時，スコアリング時に条件付き確率を使用している．ここで，異常ログはそれぞれ同じクラスタに属していることが多く，異常ログから異常ログへの遷移が起こった場合，同じクラスタから同じクラスタへの遷移が多く起こることとなる．これらにより，たとえ全体のログの行数に対する異常ログの割合が小さい場合でも，異常ログから異常ログへの遷移確率が，いくつかの正常ログから正常ログへの遷移確率よりも大きく算出されることがある．そして，同じクラスタに分類されている異常ログが長く連続している期間があった場合に，多くの異常ログを正しく異常であると識別できない問題が発生していた．スコアリングは注目したログの前後 5 行のログを用いて行っているが，注目した異常ログの前後 5 行のログの中に，正常ログから異常ログへの遷移，もしくは異常ログから正常ログへの遷移が存在していた場合は正しく識別できることが多かった．これは，正常ログから異常ログへの遷移や異常ログから正常ログへの遷移の出現確率が低いためである．しかし，注目した異常ログの前後 5 行のログ全てが同じクラスタに属している異常ログであった場合，尤度が高くなり，正しく異常であると識別できなかった．BOS 混合データには数百行の異常ログが連続，もしくは密集している時間帯が存在しており，この問題が顕著に表れ，検知精度が著しく低下したと考えられる．提案手法の場合では，この時間帯の正常，異常を含めた数百行のログが少数のセッションにまとまっているため，検出精度に与える影響が軽微であったと考えられる．今回の従来手法との比較実験では抽出した特徴量が若干異なっていることや，異常検知をログ単位で行う等の相違点がいくつかあるため，提案手法との単純な比較はできないが，セッションに区切る考えを導入し，ユーザの通信パターンに着目した確率モデルを用いることで，提案手法は従来手法よりも高精度に異常

検知できることを確認した．

4.7　考察

これまで 4 節全体で述べた実験結果から，提案手法では組織内の利用者が固定された端末が行う普段の通信の規則性を正しく学習し，普段見られない通信が発生した場合に異常として検知できることを確認し，また，提案手法が従来手法と比べて優れた検知精度であることを確認した．今後の検知精度向上の課題として，正常ログが多く含まれるシーケンス中に少数の異常ログが含まれている場合に正しく検知するための対策が挙げられる．そのための例として，遷移確率が単純な条件付き確率だけではない他の確率モデルを用いた場合の有効性の検証などが挙げられる．

5　おわりに

本稿では，情報システムに蓄積されたログの解析により，通常の通信パターンとマルウェア感染時の通信パターンの違いに着目し，ユーザの通常の通信パターンを表す確率モデルを作成し，検知対象のクラスタシーケンスの生起確率を用いて異常を検知する手法を提案した．実験では 10 台の本学の職員用端末の Web アクセス履歴と 2 種類の公開データセットを用いて本手法の有効性を確認し，さらに本学の学生用の端末を用いて学習を行った場合と，bi-gram を利用した従来手法を用いた場合で比較評価を行った．今後の課題としては，誤検知を削減するために有効な対策の検討が必要であり，例えば本実験で用いていない他の確率モデルを用いた場合の有効性の検証などが挙げられる．

参考文献

[1] 総務省：標的型攻撃への対策，国民のための情報セキュリティサイト（オンライン），入手先 <https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/07.html>（参照 2021-2-19)

[2] 石井 将大，猪俣 漸，京山 剛大，ほか：プロキシログのクラスタ間遷移に着目した異常検知手法の評価，暗号と情報セキュリティシンポジウム 2018 講演論文集，4B2-5 (2018)

[3] 八切 有市，青木 茂樹，宮本 貴朗：ユーザの行動パターンに注目した無線 LAN 利用における認証，情報処理学会研究報告，Vol.2019-IOT-44 No.2 (2019)

[4] Varun Chandola, Arindam Banerjee, and Vipin Kumar：Anomaly detection for discrete sequences:A survey, IEEE, Vol. 24, No. 5, pp. 823-839 (2012)

[5] 名倉 悠，青木 茂樹，宮本 貴朗：プロキシログから抽出した通信パターンによる異常検知，暗号と情報セキュリティシンポジウム 2022 講演論文集，2B4-2 (2022)

[6] Sandra Kumi, ChaeHo Lim, and Sang-Gon Lee : Malicious URL Detection Based on Associative Classification, Entropy 2021, Vol.23(2), pp.182-194（オンライン）, 入手先 <https://doi.org/10.3390/e23020182 >(2021)

[7] 鐘本 楊 : Web アプリケーションに対するサイバー攻撃の効率的な検知，京都大学学術情報リポジトリ KURENAI,（オンライン）入手先 <https://doi.org/10.14989/doctor.k22573 > (2020)

[8] 高田 雄太, 寺田 真敏, 松木 隆宏, ほか:マルウェア対策のための研究用データセット〜MWS Datasets 2018〜，情報処理学会研究報告，Vol. 2018-CSEC-82，No. 38，pp. 1-8 (2018)

[9] Stratosphere : Stratosphere Laboratory Datasets,（オンライン），入手先 <https://www.stratosphereips.org/datasets-overview> (参照 2021-10-19)

著者略歴

名倉 悠　2021 年 大阪府立大学現代システム科学域知識情報システム学類卒業．2023 年 同大大学院人間社会システム科学研究科博士前期課程修了．現在，BIPROGY 株式会社．在学中，情報セキュリティに関する研究に従事．

青木 茂樹　1998 年 大阪府立大学総合科学部卒業．2004 年 同大大学院工学研究科博士後期課程修了．同年，熊本電波工業高等専門学校電子制御工学科助手．2006 年 大阪府立大学総合教育研究機構講師，学術情報センター兼務．現在，大阪公立大学大学院情報学研究科准教授，情報セキュリティセンター，情報基盤センター兼務．専門は情報セキュリティ，情報システム工学，パターン認識．博士（工学）．

宮本 貴朗　1987 年 大阪府立大学大学院総合科学研究科修士課程修了．1988 年 同大大学院工学研究科博士後期課程退学．同年 同大計算センター助手．現在，大阪公立大学大学院情報学研究科教授，情報学研究科長，情報セキュリティセンター長，情報基盤センター副センター長．専門は情報セキュリティ，情報システム工学．博士（工学）．

標的型サイバー攻撃検知技術によるセキュリティ懸念の調査と対応事例

Report on Security Concerns Surveys and Effective Use Cases with Malicious Intrusion Process Scan

伊藤智博*
Tomohiro Ito

山形大学*
Yamagata University*

暗号化通信が当たり前になり，通信内容を検査して，ウィルススキャンをすることが困難である．標的型サイバー攻撃検知技術によって，IP アドレス毎の危険度やヘッダーなどの情報が時系列で可視化され，脅威の特定が容易になった．その対応事例として，不正な実行プログラムのダウンロードやサーバへの侵入，外国への SSL-VPN を調査した．本論文では，標的型サイバー攻撃検知技術によって、情報セキュリティ懸念を迅速に調査できる可能性について述べる．
キーワード：標的型サイバー攻撃検知，不正アプリ検知，　TLS 通信検査，NDR
Encrypted communication has become commonplace, and it is no longer possible to examine the contents of communication and scan for viruses. The risk level and headers information of each IP addresses would be visualized in time series by malicious intrusion process scan technology, and making risk identification easier. We reported the surveys of the malicious program downloads, the intrusion for server and the SSL-VPN connection to foreign countries as the effective use cases. The malicious intrusion process scan technology can quickly survey the information security concerns.
Keywords: Malicious Intrusion Process Scan, Malicious Program, TLS Traffic Inspection, Network Detection and Response

1. はじめに

大学では学生などの持ち込み端末が多くなっている [1-5]．宮崎大学では 2010 年から段階的に持込端末を導入している [1]．2016 年の大学 ICT 推進協議会 （AXIES） ICT 利活用調査部会の報告によると全学的に導入している大学が 32% であった [2]．

*大学院理工学研究科
(兼任)情報ネットワークセンター
〒992-8510 山形県米沢市城南4-3-16
Graduate School of Science and Engineering
〒992-8510 4-3-16, Johnan, Yonezawa-shi, Yamagata, JAPAN
E-mail：tomohiro@yz.yamagata-u.ac.jp

エンドポイントプロテクション(EPP)の導入は，持込端末のマルウェアの駆除が可能である．しかし，AV-TEST の Security レポートによると，2018 年のウィルスとマルウェアの生成件数は，1.375 億件であり，1 日当たりに 38 万件の新種が出現した [6]．事実上，パターンマッチングによる EPP では、マルウェアからの脅威を防げないであろう．

端末内でソフトウェアの不審な動作を検知する EDR は，端末内のプログラムの挙動やアクセス先のログを収集し，ログを解析することで，ランサムウェアやマルウェアを検知する．宮崎大学では，職員向けに EDR を導入した [7]．しかし，本学では，予算やプライバシー保護の観点から，持込端末に EDR を導入することは難しい．

表 1 に示すように，大学における主なセキュリ

ティ懸念は，3 つに分類される．1 つ目は，大学のサーバからの外部への不正な通信であり，大学のサーバに侵入し，改ざんや不正なプログラムを動作させ，大学のサーバから外部に不正な通信を試みるものである（表 1 の 1）．2 つ目は，情報漏洩などのりクスの高い通信であり，利用者端末に不正なプロラムをインストールし，情報窃取脅威に発展するものである(表 1 の 2)．3 つ目は，違法性の高い通信であり，著作権侵害コンテンツのダウンロードやソフトウェアの契約に違反した輸出などに発展する場合である（表 1 の 3）．

大学における主な情報セキュリティ懸念は，機械的に検知できる場合とできない場合がある．表 1 の 1 と 2 は，通信先の IP アドレスやシグネチャーをデータベース化した統合脅威管理(UTM)装置によって，機械的に検知・遮断が可能である [13]．表 1 の 3 は，UTM のアプリケーションフィルター機能により，違法性の高い通信に使われるプログラムを機械的に検知できる．しかし，プログラムの利用による違法性を機械的に検知することは不可能に等しい．

暗号化通信(HTTPS 通信)は，電子証明書によって，サイトに信頼性や安全性を担保できる．2019 年ごろから，無料の電子証明書が提供されるようになった．多くのサイトが常時暗号化通信（常時 SSL 化）に対応した．2020 年には，フィッシングサイトも常時 SSL 化された．言い換えれば，SSL 化されたサイトが安全である証明がなくなった．

暗号化通信は，まったく情報が読み取れない訳ではない．Server Name Indication（SNI）要素や TLS1.2 のサーバ証明書の情報は，読み取れる．SNI では，端末から閲覧したいホスト名をサーバに知らせるために，TLS の暗号通信を要求する Client Hello メッセージ内に閲覧ホスト名を SNI 要素として平文で送信する [14]．TLS1.2 では，サーバ証明書の情報がサーバから端末に Server Hello として平文で送信される．近年では，利用者のプライバシー保護や通信先の秘密を守るために，サーバ証明書や SNI 要素を暗号化した TLS1.3 や ESNI が標準化された [15),16]．

通信パケットを監視し，通信の振る舞いから標的型サイバー攻撃を検知する技術が登場する．実行ファイルを一旦保護された空間で動作させ，その動作挙動から脅威を検知するサンドボックス型とネットワークの通信挙動から脅威を検知する NDR(Network Detection and Response)型の 2 つである．

表 1　大学における主な情報セキュリティ懸念

番号	分類	主な原因や内容	機械的検知
1	大学のサーバから外部への不正な通信	(原因)サーバ内のプログラムの脆弱性 [8)] (原因)サーバの利用者アカウントの搾取や乗っ取り [8)] (内容)サーバに侵入し、改ざんや不正なプログラムによる外部へのメール送信やポートスキャンを実施 [8)]	IP アドレスや URL データベースから検知可能
2	情報窃取脅威の可能性の高い通信	(原因)学内端末がマルウェアやバックドアに感染 [9)] (原因)フィッシングメールなどを使って，不正なアプリをインストール [9)] (内容)ダークネットなどの不正な通信先への通信 [10)] (内容)サイバー空間における様々な経路を介した情報窃取等の国外等への技術流出	非暗号通信やメールは，UTM のアンチウィルス機能で検知可能．IP データベースによる検知可能.
3	違法性の高い通信	(原因)利用者の知識不足や標的型攻撃 [11)] (内容)著作権侵害コンテンツのダウンロードやアップロード (内容)ソフトウェアの使用許諾や米国再輸出規制などに違反したプログラムなどの輸出 (内容)安全保障輸出管理上の機微な情報がサイバー空間を介して流出 [11,12)]	UTM のアプリケーションフィルター機能で実行プログラムを検知可能(P2P など)

NDR 型の商品化について，著者が調査したところ, 2017 年時点で，PFU 社の iNetSec MP や Trend Micro 社の Deep Discovery Inspector が販売されていた．その後，Vectra AI 社の Vectra Platform, DARKTRACE 社の Darktrace Cyber AI Platform，Fortinet 社の FortiAI が商品化されている．本学では，競争入札の結果，PFU 社の iNetSec MP 2040F を 2018 年に導入した．iNetSec MP 2040F には、PFU 独自の標的型サイバー攻撃検知技術が搭載されている [17]．

NDR 装置は，スイッチからのミラーパケットを全て読み取り，通信の整合性や通信先，コンテンツの種類，HTTP のレスポンスヘッダーや TLS 通信のメッセージを高速に抽出する [18]．その抽出情報から，通信先へのアクセスの頻度，実行ファイルのダウンロード割り出し，危険サーバを時系列に可視化，相関解析を行う [19-21]．危険サーバへのアクセス頻度や周期性を元に，端末の評価値（危険度）を割り出している [19]．危険サーバを分類する機能 [22]や電子証明書の検査技術 [23]の機能を有している．

本学では，NII SOCS，サービス監視，利用者からの情報セキュリティ上の通報への対応として，ファイアウォールのログを分析し，利用者への通知とその対処を依頼している．しかし，常時 SSL 化による暗号化通信や研究室での無線 LAN ルータ利用が多くなるにしたがって，セッション単位の記録であるファイアウォールのログでは，利用者端末の特定が困難であった．そこで，セッションのヘッダーやレスポンスボディを分析できる NDR 装置を使用して，情報セキュリティ上の通報の調査を迅速にできると考えた．

本論文では，標的型サイバー攻撃検知装置の導入によって，セキュリティ懸念の調査とその対応への有効性について報告する．

2. 標的型サイバー攻撃検知装置の設置

2.1　キャンパスネットの構成

図 1 に示すように，キャンパスネットワークは，SINET6 の山形 DC と 4 つのキャンパスを 10Gbps の主回線で接続している．それぞれのキャンパスには，1Gbps のバックアップ回線を接続している．主回線は，SINET6 の仮想大学 LAN サービスや L2VPN を利用して，キャンパス間の接続をタグ VLAN によって多重化した．

ネットワークの冗長化は，IP ルーティング技術を使用した．小白川，飯田，米沢キャンパスには，ボーダールータを設置した．バックボーンネットワークは，ボーダールータから主回線とバックアップ回線に接続した．2 つの回線の冗長化制御には，OSPF と iBGP を使用した．

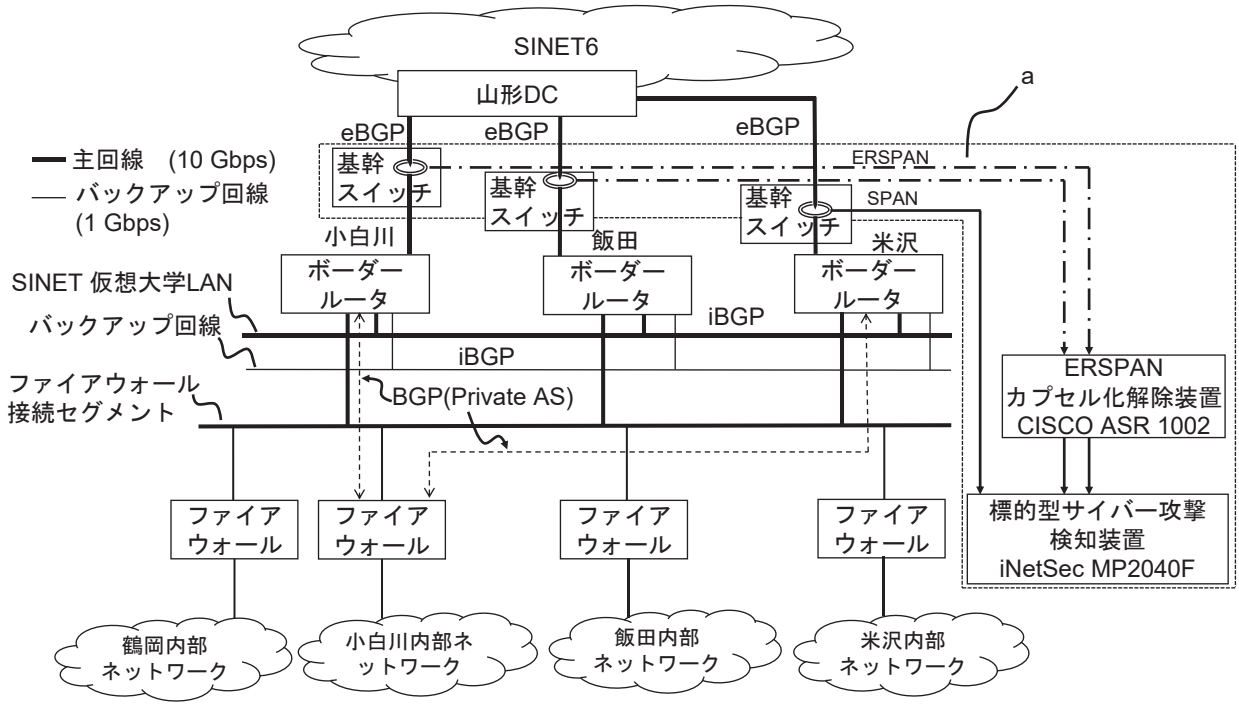


図 1　キャンパスネットワークの論理構成と標的型サイバー攻撃検知装置の導入部分(a)

インターネットへの接続は，主回線の障害時に，バックボーンネットワーク経由して，他のキャンパスからインターネットに接続している．ファイアウォールは，複数のボーダールータとプライベート AS による BGP 経路制御によって，冗長化した．ファイアウォール接続セグメントは，SINET6 の仮想大学 LAN を使用して，主回線に構築した．

山形 DC と本学に分散配置された 3 台のボーダールータのインターネット接続通信をポートミラーリングすることで，全学のインターネット通信パケットを 1 台の NDR 装置に送信した．

2.2 機器の構成と運用方針

NDR 装置を導入するにあたり，主に使用した機器を表 2 に示す．

表 2 NDR 装置の導入に必要な機器

名称	型番
NDR 装置	PFU iNetSec MP 2040F
基幹スイッチ	CISCO Catalyst 6807XL
カプセル化解除装置	CISCO ASR 1002
ファイアウォール	CISCO ASA 5555-X with FirePOWER Service

運用方針として，本学の公式な DNS キャッシュサーバや SPAM 検知装置をホワイトリストに登録した．EPP や UTM の定義ファイルのダウンロードサイトもホワイトリストに登録した．無料で提供されるドメインバリデーション電子証明書(無料 DV 電子証明書)を発行する認証局の CA 証明書は，フィッシングサイトに利用される可能性があるため，ホワイトリストに登録しなかった．

2.3 ポートミラーリングの設計

図 1 の a は，NDR 装置の導入に伴い追加した部分である．NDR 装置は，本学で，最も通信量の多い米沢キャンパスに設置した．米沢キャンパスのインターネットの通信をポートミラーリング(Switching Port Analyzer, SPAN)によって，NDR 装置に送信した．小白川または飯田キャンパスのインターネットの通信は，基幹スイッチのカプセル化リモート SPAN(ERSPAN)機能によって，米沢キャンパスに設置された ERSPAN カプセル化解除装置に送信した．カプセル化解除装置は，GRE カプセル化および ERSPAN のヘッダー情報を削除し，通信パケットを NDR 装置に送信する．

2.4 評価方法

調査期間は，2021 年 9 月から 2022 年 6 月の 10 か月間とした．調査エリアは，全学とした．NII SOCS，サービス監視，利用者からの情報セキュリティ上の通報を受けた端末について，初動対応と通報内容以外のリスク調査を実施した．

初動対応は，ファイアウォールのログから通信の有無を確認した．通信が有の場合，NDR 装置を用いて，通報日時における通報内容の通信セッションの検知の可能性や実行ファイルの有無を調査した．利用者に，事実関係の調査依頼と対処方法を伝えた．調査時間は，通報確認から利用者の調査完了の報告までの平均時間とした．

通報内容以外のリスク調査とは，NDR 装置を用いて，該当端末に通報内容以外の情報セキュリティ懸念を確認し，二次的な情報セキュリティ上の懸念を未然に防ぐことを目的としている．通報内容以外のリスクの調査の調査期間は，通報日時から 1 カ月前とした．通報内容以外のリスクは，NDR 装置のタイムライン通信表示機能を用いて，検知した危険サーバへの通信の中から通報内容以外の情報セキュリティ懸念を調査した．通報内容以外のリスクが検知された場合，それ以前の日時以外に，同様または他の通報内容以外のリスクを調査した．また，同じ危険サーバへの通信の周期性も確認した．

3 結果

3.1 情報セキュリティ通報とその検知結果

表 3 に，情報セキュリティ上の通報内容，NDR 装置の検知数および通報以外のリスクの検知のまとめを示す．

表 3　情報セキュリティ上の通報内容，NDR 装置での検知数および通報内容以外のリスク

番号	通報元	通報内容	通報数	検知数	調査時間※	通報内容以外のリスク概要
1	NII SOCS	フィッシング詐欺サイトアクセス	16	0	ー (120 分)	なし
2	NII SOCS	Log4j の脆弱性利用	3	0	ー (60 分)	外国の情報セキュリティ上懸念の残る SSL-VPN 通信（調査時間 90 分）
3	NII SOCS	不正アプリダウンロード	5	1	20 分 (120 分)	なし
4	サービス監視	通信機器異常	1	1	10 分	なし
5	利用者	不正アプリダウンロード	1	1	30 分	なし

※調査時間は，通報確認から利用者の調査完了までの時間である．() 内の時間は、NDR の効果を得られなった場合の調査時間である．

表 3 の 1,2 に示すように，フィッシング詐欺サイトアクセス，Log4j の脆弱性の通報は，検知件数が 0 件であった．また，フィッシング詐欺サイトへのアクセスと同時に不正アプリをダウンロードした場合は表 3 の 3 に分類した．NDR 装置は，人為的に発生するウェブアクセスのような周期性のない通信を検知できなかった．表 3 の 2 の Log4j の脆弱性利用では、通報 3 件に対して 1 件の通報内容以外のリスクが発見された．通報内容以外のリスクは，外国の情報セキュリティ上懸念の残る SSL-VPN 通信であった．

表 3 の 3 に示すように，NII SOCS から通報のあった不正アプリダウンロードの疑いに関しては，通報 5 件に対して 1 件は検知できた．表 3 の 4,5 のように，本学のサービス監視や利用者の情報セキュリティ上の通報を発見したケースでは，その原因となる通信を精査する過程で，NDR 装置が効果を発揮した．

3.1.1 不正アプリダウンロードの調査と対応

表 3 の 5 に該当する不正アプリダウンロードは，利用者から「メールに添付されている Excel ファイルを開いて，マクロを有効化した」との通報から，調査が開始された．NDR 装置のタイムラインには，「活動 : 実行ファイルのダウンロード」と検出され，危険度は高であった．図 2 の a に示すように，通信概要のアクセス先には，HTTP アクセスの URL で，ファイル名は記述されていなかった．関連ファイルは，dll の拡張子のファイル名であり，実行ファイルであった(図 2 の b).

図 2　DLL ファイルのダウンロードの確認画面

レスポンスヘッダーからは，実行ファイルをダウンロードした事実が確認できた．レスポンスヘッダーによると Content-Type は「application/x-msdownload」，Content-Disposition は「attachment; filename="xxx.dll"」と表示されていた．レスポンスボディには，0x4D5A と表示され，実行プログラムを示唆していた．

ファイアウォールのログには，HTTP アクセスの URL が記録されていた．本学のファ

イアウォールでは、レスポンスヘッダー情報を記録できないので，実行可能なファイルをダウンロードした形跡は残らない．

利用者には，DLL ファイルのダウンロードが確認された事実を伝え，マルウェアやコンピュータウィルスの感染の可能性が高いのでウィルススキャンを依頼した．調査時間は 30 分であった．

表 3 の 3 に該当する不正アプリのダウンロードは，NII SOCS からの通報により，調査を開始した．主にフィッシングによって，不正なアプリをインストールさせようする行為であった．5 件中 1 件の検知で，NDR 装置の効果は限定的であった．検出できた 1 件は，android アプリの apk ファイルダウンロードであった．NDR 装置の検知したアクセス先は，http://から始まり，apk ファイル名で終わる URL であった．User Agent には，「Mozilla/5.0 (Linux; Android 10; xxx-xxx) AppleWebKit (以降，省略)」と表示されており，端末の OS や型式を確認できた．

学内 LAN に接続されているデバイスの MAC アドレスから，無線 LAN ルータであった．設置責任者に，端末のメーカー名，ＯＳ，型式や不正アプリのファイルダウンロードの疑いがあるので，調査を依頼した．5 分後に無線 LAN ルータの設置責任者から回答があり，「利用者が誤ってスマートフォンに届いた SMS の URL をタップした．アプリがダウンロードされ，怪しいと思ったので，インストールはしていない」との回答であった．

NDR 装置は，調査時間を 1 時間以上短縮できた．NDR で検知できた際の調査時間は 20 分で，検知できない際は 120 分であった．

3.1.2　通信機器の障害の調査と対応

表 3 の 4 に該当する通信機器の障害は，サーバセグメントの 1 台のサーバのウェブ機能停止の障害検知から調査が開始された．教育実習用サーバラックに導入されている透過型ファイアウォール(Fortigate 200D)が機能停止し，実習用サーバラックへの通信が全て停止するという大規模な障害であった．

NDR 装置で，サーバセグメントの IP アドレスを対象に危険度を調査した．100 台中 1 台の IP アドレスの危険度が「中」と表示されていた（図 3 の a）．該当 IP アドレスは，ウェブ機能が停止したサーバの IP アドレスとは異なった．タイムラインを調査すると，ウェブ機能が停止する 2 時間前に，「リスク : 怪しいファイルを操作することによってダウンロードされた不審なファイルを検出した」と通信の種類に表示されていた(図 3 の b)．リスクの概要には，アクセス先の URL に拡張子 exe の実行ファイルが含まれていた．レスポンスヘッダーには，Content-Type が「application/x-msdos-program」と表示されていた．レスポンスボディには，0x4D5A と表示され，実行ファイルのダウンロードが確認された．

図 3　危険度「中」を示したサーバのタイムライン

情報セキュリティ上の重大な懸念が予想され，緊急対応を行った．すぐに，CSIRT の責任者に報告した．利用者への業務の影響を最小にするために，代替サーバを準備しながら，該当サーバの影響範囲の把握を急いだ．3 時間後に，該当サーバをネットワークから切り離した．その 1 時間後には，代替サーバへの切り替え作業が完了した．

調査開始から実行ファイルのダウンロードの確認までの調査時間は 10 分であった．機能停止したサーバに着目して，調査をしていたら，外部からの侵入を発見できなかった可能もある．NDR 装置は，サーバの不正な実行プログラムのダウンロードを検知でき，感染

拡大を未然に防ぐ効果がある．

3.1.3　電子証明書の検査技術による情報セキュリティ上懸念の残る通信調査

表 3 の 2 に該当する Log4j の脆弱性利用の通信は，NII SOCS から学外への LDAP ポートや本学ウェブサーバへの攻撃の通信についての調査依頼があった．NDR 装置では，389 や 636 ポートへの通信は，確認できなかった．ファイアウォールのログから，通報 3 件に対して 1 件が，外国の IP アドレスの 389 ポートへの通信であった．該当端末の利用者に確認したところ，利用者がアプリを操作する過程で発生する正常な通信であった．調査時間は 60 分であった．

該当端末の通報内容以外のリスク調査で，NDR 装置の検知情報には，図 4 の a に示すように，危険度が「重大」と表示された．学外の IP アドレスへの暗号化通信のアクセスが確認され，「活動:C&C 通信」が検知された(図 4 の b)．NDR 装置のタイムラインをさかのぼると，同様の通信は 1 カ月に 20 回程度あり，周期性が確認された．さらにタイムラインをさかのぼると，同様の通信は長期的に繰り返されていた．

図　4　通報内容以外のリスク調査におけるタイムライン

図 5 の a に示すように，攻撃に利用した疑いのある SSL/TLS サーバ証明書や CA 証明書による検知であった．図 5 の b に示すように，アクセス先は，https://から始まり，ホスト名には IP アドレスが記される URL であった．図 5 の c に示すように，電子証明書の Subject Common Name(SCN)には，”vpn”の文字列が含まれ，外国の情報セキュリティ上懸念の残る通信相手のドメインであった．この段階で，二次的な情報セキュリティ懸念が疑われた．

図　5　電子証明書の検査技術によって検知された通信先の情報

通信プロトコルは，正規の手順であった．それゆえに，不正なアプリがインストールされた可能性は低かった．該当端末がポートスキャンするような通信は，NDR 装置のタイムラインやファイアウォールのログからも確認されなかった．この時点で，二次的な情報セキュリティ上の懸念の可能性は低いと判断した．調査に費やした時間は 90 分であった．後日 CSIRT による調査で，当該研究室の通常活動の一環であることが確認できた．

NDR 装置が検知できた理由は，周期的な暗号化通信であったからだと推察している．本学の公式なウェブサーバは学外に設置され，無料 DV 電子証明書を使っている．しかしながら，NDR 装置によって，このサーバへの暗号化通信を不正な通信として検知した例は極めて少なかった．それゆえに，無料 DV 電子証明書の発行機関を信頼しない運用ポリシーによる検知というよりは，周期性によって検知された可能性が高いと考えられる．

3.1.4　NII SOCS の通報を検知不能な通信や NDR 装置でのみ検知可能な通信

表 3 の 1 のフィッシング詐欺サイトへのアクセスが検知できなかった点について考察する．ファイアウォールのログから，フィッシング詐欺サイトへのアクセスは HTML のウェブページへのアクセスであった．NDR 装置の危険度は，主に「中」や「高」であった．NDR 装置は，実行ファイルのダウンロードを不正な通信のフェーズの 1 つして検知するように設計されている [19]．しかし，HTML ベースのウェブページへのアクセスでは、実行プログラムではないため，不正な通信のフェーズとして検知されないと推察した．

表 3 の 4 は，NDR 装置でのみ検知できた通信であった．ファイアウォールのログからは，1 カ月ほど前から侵入を試みた通信があった．NDR 装置は，実行プログラムをダウンロードした段階で，不審な通信として検知した．その他にも，HTTPS の通信において URL が IP アドレスのみの通信があり，通信の危険度は「高」であった．この通信は，同一端末の他の通信から，正常なアプリの C&C 通信であった．検知例が少ないので決定できないが，IP アドレスのみが記録された HTTPS 通信は TLS1.3 の不審な挙動の通信を検知したのであろう．

3.2　電子証明書検知のための改善点

無料 DV 電子証明書の認証局の R3(Let's Encrypt)やメーカー独自認証局から発行された電子証明書が，ソフトウェアの自動アップデートに使われていた．定期的にアップデートプログラムが実行され，周期性が高いため，不正な通信として検知された．IP アドレス当たりのタイムラインの件数は，10 万件以上であった．NDR 装置のデータベースの使用率が 70%以上になり，処理能力が低下した．

R3 の認証局は，フィッシングサイトの電子証明書の発行に使われることが多い．R3 の認証局を NDR 装置のホワイトリストに登録すれば，フィッシングサイトへの不正な通信を検知できなくなる．そこで，表 4 に示すように，アップデートサイトの SCN をホワイトリストに登録した．

表 4 ホワイトリストに登録した SCN

SCN	認証局
*.ubuntu.com	R3
*.gnome.org	R3
*.zabbix.com	R3
ftp.jaist.ac.jp	R3
*.redhat.com	Red Hat Entitlement Operations Authority
*.fortinet.com	Support

4　結論

標的型サイバー攻撃検知技術は，情報セキュリティ上の事実関係を迅速に調査できる．本学のファイアウォールのログに記録されないレスポンスヘッダーの情報から，利用者端末の機種や実行プログラムのダウンロードを調査できる．暗号化通信であっても，電子証明書の情報から，情報セキュリティ上懸念の残る通信相手を調査できる．

謝辞

論文の執筆にあたり，ご助言・ご指導をいただきました本学米沢キャンパス長を始め執行部の皆様に感謝申し上げます．日頃から，本学のセキュリティ確保やログの解析に従事していただいている情報系センターのスタッフの皆様に感謝申し上げます．

参考文献

(1) 青木謙三，園田誠，黒木亘，川畑圭一郎，廿日出勇：”宮崎大学におけるパソコン必携化の取り組み”，”情報処理学会研究報告, Vol. 2015-IOT31”, pp.1-5 (2015)

(2) 和田智仁：” 大学における必携デバイスに関する一考察　– タブレット必携化の取組を踏まえて—”, ”学術情報処理研究，No. 24”, pp. 28–35 (2020)

(3) 大学 ICT 推進協議会 (AXIES) ICT 利活用調査部会：”2016 年度　BYOD を活用した教育改善に関する調査研究　結果報告書”, ”2016 年度 BYOD を活用した教育改善に関する調査研究結果報告書” https://axies.jp/report/ict_survey/2016survey/ (2022 年 6 月 10 日参照)

(4) 櫻田武嗣,三島和宏,萩原洋一,澤隆彦：”端末の無い PC 教室の実現 – BYOD 化のための仮想端末教室の設計と実現–”, “コンピュータ＆エデュケーション, Vol.42“ , pp.12-18　(2017)

(5) 根本 貴弘, 三島 和宏, 青山茂義：”青山茂義:コロナ禍を含む約 5 年間の仮想端末室の利用状況の報告と考察”, ”学術情報処理研究, No. 25”, pp. 29–38 (2020)

(6) AV-test:　“SECURITY REPORT 2018/19”　https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf　(2022 年 6 月 19 日参照)

(7) 青木 謙二, 園田 誠, 黒木 亘, 川畑 圭一郎: ”宮崎大学新キャンパス情報システムの構築”, ”大学情報システム環境研究, Vol. 23”, pp. 3-10 (2020)

(8) NISC： 政府機関等のサイバーセキュリティ対策のための統一基準 https://www.nisc.go.jp/policy/group/general/kijun.html (2022 年 9 月 29 日参照)

(9) 油谷曉：” 大学という組織のセキュリティ事情”, ”情報の科学と技術 Vol. 70”, pp.249-254 (2020)

(10) 笠間 貴弘, 井上 大介：”大規模ダークネット観測と能動的スキャンによるマルウェア感染 IoT 機器の分類”, ”情報処理学会論文誌 Vol. 58”, pp.1388-1398(2017)

(11) 橋本靖明：”サイバー・セキュリテイの現状と日本の対応”, ”国際安全保障 Vol.41”. pp.27-43 (2013)

(12) 文部科学省： 大学の国際化と危機管理について ～安全保障貿易管理に関する観点から～ https://www.mext.go.jp/content/20210304-mxt_gakkikan-000013198_11.pdf (2022 年 9 月 29 日参照)

(13) 鈴木 彦文, 永井 一弥, 浅川 圭史, 今井 美香, 不破 泰：”信州大学認証ネットワーク「セキュアネット 2010」における認証スイッチの拡張と整備”, "学術情報処理研究 Vol. 14", pp.21-30(2010)

(14) D. Eastlake 3rd： ”Transport Layer Security (TLS) Extensions: Extension Definitions”, RFC 6066, (2011).

(15) E. Rescorla: ”The Transport Layer Security (TLS) Protocol Version 1.3”, RFC 8446, (2018).

(16) C. Huitema: ”Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”, RFC 8744, (2020).

(17) PFU：”サイバー攻撃検知・SOC 運用効率化 iNetSec MP 2040”, https://www.pfu.ricoh.com/inetsec/products/mp/　(2022 年 6 月 20 日参照)

(18) 羽藤 逸文,山下 康一,小出　和弘: “情報処理装置，方法およびプログラム”, JP Patent No. 5917678.

(19) 小出 和弘, 道根 慶治: : ”不正活動判定方法および不正活動判定用プログラム，並びに，情報処理装置，活動判定方法および活動判定用プログラム”, JP Patent No. 6097849.

(20) 寺田 成吾, 道根 慶治,小林 峻：”情報処理装置，通信検査方法及びプログラム”, JP Patent No. 7045949.

(21) 小林　峻,小出　和弘,寺田　成吾：”情報処理装置，方法およびプログラム”, JP Patent No. 5925287.

(22) 寺田 成吾,道根 慶治：”情報処理装置，不正活動分類方法および不正活動分類用プログラム”, JP Patent No. 6869100.

(23) 小林 峻,寺田 成吾：”情報処理装置，方法およびプログラム”, JP Patent No. 6084278

著者略歴

伊藤智博　1998 年山形大学工学部物質工学科卒業，2003 年同大大学院理工学研究科博士後期課程修了，同年 4 月同大学情報処理センター助手，2007 年同大学学術情報基盤センター助教，2009 年 10 月同大大学院理工学研究科助教（同大工学部学術情報基盤センター兼務），2010 年 8 月から国立情報学研究所　学術認証フェデレーシ

ョンタスクフォースの委員を兼任，2013 年 4 月同大大学院理工学研究科准教授，2013 年から国立情報学研究所 学術認証運営委員会作業部会の委員を兼任，2015 年から山形県警 サイバー犯罪等テクニカルアドバイザー を兼任， 博士（工学）

北陸ブロック　活動報告

福井大学総合情報基盤センター

技術職員　吉川雄也

03/09/2023　1

金沢大学 学術メディア創成センター

- 金沢大学 学術メディア創成センター（2021/4～）
  - 前身
    - 理学部計算機室（1963～）
    - 金沢大学情報処理センター（1971～）
    - 金沢大学総合情報処理センター（1990～）
    - 総合メディア基盤センター（2003～）
  - 全学のDX計画を戦略的に統括・推進するコア組織
    - 全学DX推進を支える最先端の情報システムの設計・開発
    - 次世代デジタルコンテンツやシステム開発技術にたけた人材をコンテンツデザイナー（CD）として新たに採用
    - xR(VR・AR・MR)等のDX技術を駆使した教材の開発
    - スタジオでの動画コンテンツの撮影・編集
    - 作成したDXコンテンツを自在に利活用するためのシステム開発

    etc
  - 前身の役割も引き続き担当

2

教育DXの活動の目的

■ 次世代の教育システムを目指して、 xR技術の教育での活用に着手

●DX教材（VRコンテンツ、MRコンテンツ）の開発

●DX教材の配信・視聴システムの開発

●xRスタジオの整備

3

総合情報基盤システム

2022/3/1から運用中

■ 仮想化
- ➢ サーバ：　仮想プラットフォーム
  - VMware + OracleVM による IaaS
  - RedHat, Ubuntu, MS Windows Server, etc
  - ユーザのwebサーバ等は、学外SaaSへ移行
- ➢ 演習室：　ネットワークブート
  - CPU、メモリは本体のものを使用
  - 演習室1室
- ➢ 共用PC：　シンクライアント（画面転送型）
- ➢ メール：　学生Gmail、教職員オンプレ

■ バックアップ
- ➢ 外部データセンター

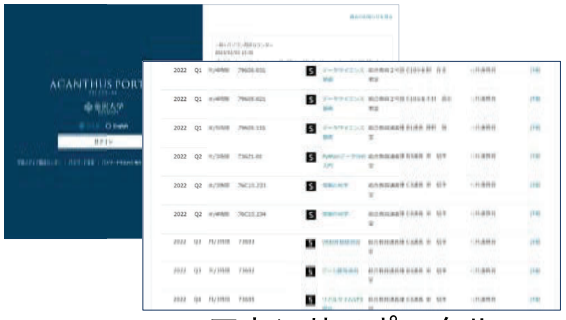
4

オンライン対応

- 講義、会議のリモート化
  - 必携PC、LMS活用
  - WebEx
  - Zoom
  - Microsoft Teams

5

全学ポータルシステム・LMS



アカンサスポータル

WebClass（全学向けLMS）

Moodle（留学生向けLMS）

6

事務システム

- 事務用パソコン
  - シンクライアント
- メールサービス
  - Office365利用
  - 標的型攻撃メール疑似体験の実施
- 研修
  - 情報セキュリティ研修

今年度に更新予定

7

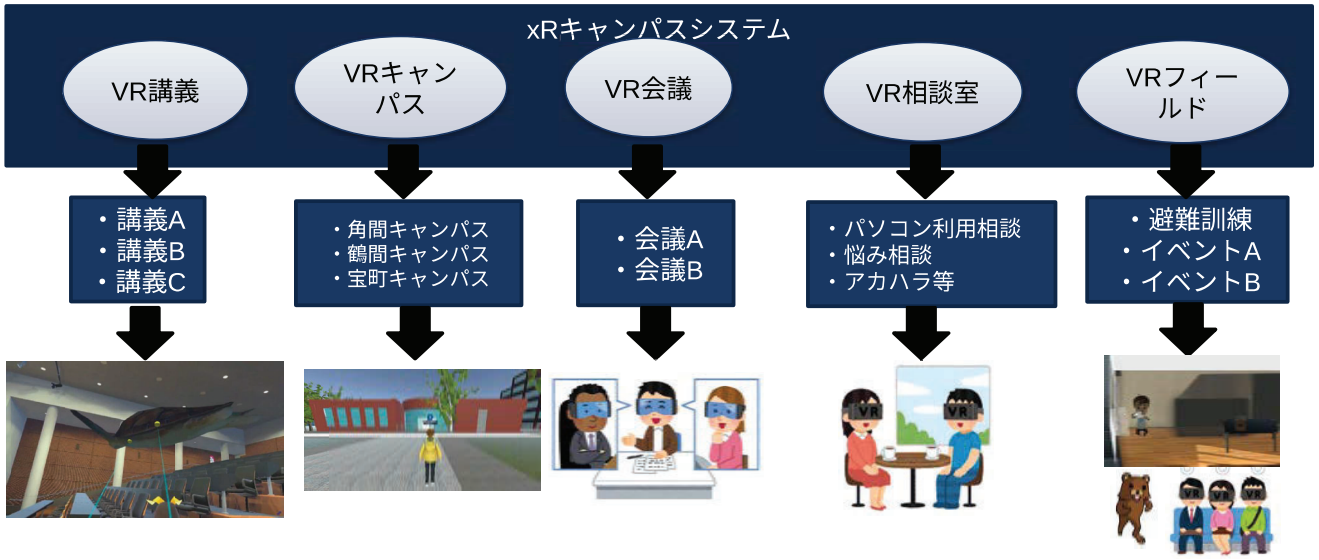
DXシステム整備

- DX教材データベースシステム
  - ・ブラウザでDX教材を利用
- xRキャンパスシステム
  - ・VRヘッドセット、スマートフォン、Windows、macOS等でDX教材を利用

8

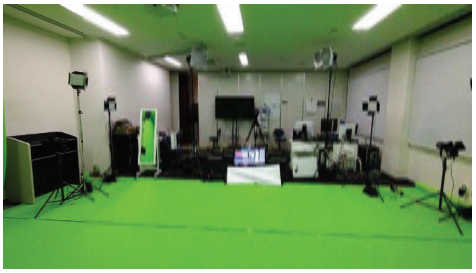
xRキャンパスシステム整備

- VRヘッドセット、スマートフォン、パソコン等で利用。MRとの連動も予定
- 全講義で利用、全構成員が利用可能なように開発中



xRスタジオ整備

- グリーンバックによるクロマキー対応
- 撮影領域の横で、撮影した動画等の教材作成
- リアルタイムVFXシステム導入
  - Vizrt（大手放送局でも利用）を導入
  - Unity、Unreal Engine等と連携したxRスタジオ整備

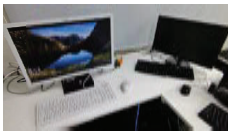


Vizrtワークステーション

Vizrt（Viz Airtist）操作用卓
Vizシナリオ操作用パソコン

PTZカメラ

プレゼン資料投影用パソコン
映像スイッチャー
音声スイッチャー
撮影確認用モニタ
PTZカメラコントロールユニット



ネット配信用パソコン
Unity・Unreal Engine映像出力用パソコン

組織概要

情報環境・DX統括本部（昨年度改組）

- 遠隔教育研究イノベーションセンター(遠隔教育Uから)

教員：3+1(兼務)、技術職員：3

- **情報社会基盤研究センター** RCACI : Research Center for Advanced Computing Infrastructure

教員：5+1(兼務)、技術職員：14

- 情報環境システムの整備・運営
- 教育研究活動のサポート
  - 高速ネットワーク
  - 大容量ファイルサーバ
  - 大型並列計算機群
  - プライベートクラウドシステム
  - ユーザ端末
  - 各種ソフトウェア
- ユーザ計算環境の構築
  - JAISTコンテナレポジトリ

http://www.jaist.ac.jp/iscenter

2

11

更新システム

【情報環境システム】

I. 常用ワークステーションシステム
  1. 携帯型ワークステーションシステム　Surface Pro → Surface Pro 8

II. 高速大容量ファイルサーバシステム
  1. プライベートクラウド用ファイルサーバシステム　NetApp SolidFire H-610S-4 --> Fujitsu ETERNUS HX6100
  2. 事務職員用ファイルサーバシステム　NetApp FAS2650 --> Fujitsu DS224C
  3. オンラインストレージシステム　Nextcloud --> Box

III. 高速キャンパスネットワークシステム
  1. ボーダルータシステム　Juniper MX204 --> MX304; Cisco ASR1002 -- > NSC540
  2. ファイアウォールシステム　Palo Alto Networks PA-5220 --> PA-3430
  3. コアルータ装置　Cisco Nexus 7710 --> Arista 7280CR3
  4. 高度無線LAN管理システム　Cisco 5520 --> 9800-40

IV.セントラルサービスシステム
  1. 資産管理システム　ConviBASE --> ConviBASE

V. 図書館情報システム
  1. 図書館情報システム　iLiswave-J V3 --> iLiswave-J V3

VI. その他周辺機器類
  1. 大型プリンタ　Canon ImagePROGRAF TX-3000 --> TX-3100

※ 学務システムは別調達

6

12

今年度導入の概要

情報環境システム(ハード)調達

オンラインストレージ：Nextcloud→Box (学内→学外)

円安による価格上昇

納入時期の問題

システムによっては、ほぼ同性能機種にリプレース

→ リース期間の検討：４年→５年

ソフトウェア調達

予算削減効果あるが、予算策定上は不安要素

円安等によるライセンス費用の上昇 → 購入内容の検討も必要

Adobe包括契約廃止の効果

今年度は研究室などに意向調査の上で必要数を購入

大学支出：約1300万円→400万円

13

SC22概要

開催期間：2022/11/13-18

開催地：米国テキサス州ダラス

Kay Bailey Huchison コンベンションセンター

※SC18と同じ

実施形態：Exhibitionは対面のみ

３年ぶりの現地参加

特徴：

例年よりも2割程度、参加者減

日本関連機関では、不参加ブース若干あり

14

JAISTブース

備考：

円安影響などで旅費増加のため参加者２名（本郷＋学生）
ブース設置を業者に依頼せずに対応
来年度も引き続き参加予定

15

(主に)今年度の取り組み

- 情報セキュリティ研修
  - 外部講師を招いて教職員対象の研修
  - 学生・教職員対象の演習型オンライン研修
- 情報コンセントのVLAN変更の自動化
  - vlan変更受付のインターフェースから事務方が入力
- uid発行申請のオンライン化
- Google Workspace の二段階認証の必須化
- 脆弱性診断

ネットワーク更新に向けて

- ネットワーク経路の整理・変更
- FWの不要なルールを削除
- スイッチのポートアサインの見直し
- 幹線分配スイッチの削減
- 電源(分電盤やブレーカ)管理方法の検討
- 物理接続情報の管理(光ケーブル)

03/09/2023　17

システム更新に向けて

- 署名方法およびその検証方法の見直し
- 演習室とセンター間を 10Gbps に
  - ネットワークブート用のサーバ
- 仮想基盤のストレージ増強

03/09/2023　18

今後の課題

- ネットワーク・システム更新に向けて
  - 運用が始まると変えられないことを今のうちに
  - 何年間も既存踏襲されてきたものを変えるチャンス

- 限られた人員で業務をまわす
  - 「もっと頑張る」より”仕組み”をつくる

東北・関東ブロック報告

山形大学 情報ネットワークセンター
田島 靖久

IS研 東北・関東ブロック会議

- 参加機関
  - 一橋大学
    - 学内無線LAN(1284Wireless)整備とその後の対応について
  - 横浜国立大学
    - 横浜国立大学のIT環境の動向
  - 山形大学
    - 2022年度活動報告

一橋大学

- 学生・教職員用学内無線LAN
  - 2021.8より運用開始
    - ARUBA, AP+LCX
  - Trouble shootings
    - LCX 不具合 （ケーブル障害、ローミング問題）
    - Web会議利用によるショートパケット増加が原因のシステム負荷増加
      - キャンパスを越えてコントローラの負荷分散
    - ランダムMAC address問題、自動接続問題
      - マニュアル整備による設定の徹底
      - 低レート通信(2.4GHz)カット
    - 稼働状況の可視化対応計画
  - 無線LANのニーズがコロナ禍で大きく変化

横浜国立大学

- 2024.3 教育研究支援システム更新
  - PC教室・図書館設置のPCの廃止
    - 2023.4よりPC学生必携化実施
  - 認証サービス以外のサービスをクラウド化
  - 2024.9 教育研究用ネットワーク更新
    - 高速化(GbE)
    - 全教室無線LAN整備
- 事務DX推進 (2022.5～)
  - TF（電子決済・学務系業務改善・情報伝達…）
- 情報セキュリティ
  - 教材作成・ISMS対応

山形大学

- SINET6移行
  - 全キャンパスDC 10G接続 + 仮想大学VLAN
    - 鶴岡 1G→10G
  - BGPによるDC接続回線のキャンパスを越えた冗長化
    - バックアップ回線（フレッツ網）
- ネットワーク機器更新1年延期
  - 半導体不足による調達期間問題
- 「情報処理」講義外注（3年ごと3回目）
  - コロナ禍で対面講義からオンデマンド講義に移行
- 学生証問題
  - 生協が組合員証をアプリに移行(2023.01)

東海地区における活動について

戸田 智基
名古屋大学 情報基盤センター

2023年3月10日

第45回東海地区国公立大学情報システム研究会

- **日時**
  - 2023年2月15日(水) 14:00～16:50 オンライン開催
- **テーマ**
  - **教育DXの取り組みとLearning Analytics**
- **参加者所属機関**
  - 名古屋大学
  - 岐阜大学
  - 三重大学
  - 愛知教育大学
  - 愛知県立大学
  - 富士通Japan株式会社
  - 九州大学（招待講演）
  - 株式会社セールスフォース・ジャパン（招待講演）

プログラム

- **近況報告**
  - 名古屋大学，岐阜大学，三重大学，愛知教育大学，愛知県立大学
- **招待講演①**
  - 講演者：島田 敬士（九州大学）
  - 講演題目：九州大学における教育DXの取り組み
    ～クラウド基盤導入，支援体制構築，データ駆動型教育の実践～
- **招待講演②**
  - 講演者：藤田 友吾，黒沢 潤（セールスフォース・ジャパン）
  - 講演題目：Tableauを活用した大学のアナリティクス事例や
    教育データの利活用のご紹介
- **情報交換**
  - 名古屋大学，岐阜大学，三重大学，愛知教育大学，愛知県立大学

招待講演①：九州大学 教育DXについて

教育の情報化に向けた三本柱

- **環境：クラウド型教育学習支援システム**
  - 新規サービスの立ち上げ
  - 適応的なサーバのスケールアップ／ダウン
- **支援：supportQ（サポQ）**
  - 学習支援窓口のワンストップ化
  - チャットボットによる自動応答
- **分析：ラーニングアナリティクス**
  - データに基づく学習・教育の分析評価
  - 研究と運用の両輪を推進

招待講演②：Tableauについて

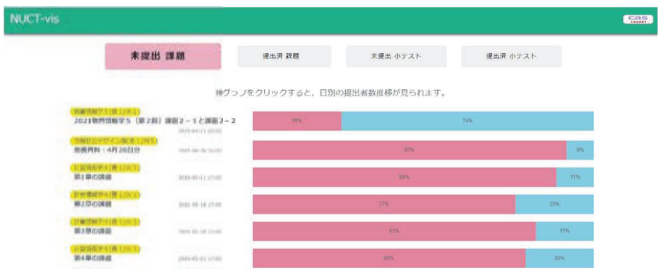
人がデータを見て理解できるようになることを支援

- **データ可視化ツール**
  - データベースに接続して所望のデータを可視化
- **様々な機能を実現**
  - **Tableau Prep Builder**：データ準備をシンプルに
  - **Tableau Desktop**：ビジュアル分析により深い洞察を提供
  - **Tableau Prep Conductor**：データ準備を自動化
  - **Tableau Catalog**：データカタログでデータの透明性を確保
  - **Tableau Server/Cloud**：情報共有して洞察を広く活用
  - などなど

情報交換：名古屋大学における事例紹介

LMSの利便士改善ツールの開発

- **NUTT（Nagoya University Time Table）**
  - LMS講義サイトへのアクセス性の向上
  - **機能①**：講義サイトを学期ごとに時間割表の形式で表示
  - **機能②**：講義ごとのメモの提供
- **NUCT-vis**
  - 未提出課題の一覧を表示
  - **機能①**：課題・小テストを提出状況ごとに一覧表示
  - **機能②**：受講生全体の提出割合の表示



近畿ブロック活動報告

2023.03.10
大阪公立大学 情報基盤センター
宮本 貴朗

国公立大学情報システム研究会総会

活動報告

大阪公立大学
Osaka Metropolitan University

- 近畿ブロック会議
  - 2023.02.20（月）14:00～17:30
  - ハイブリッド開催

  - 参加大学
    - 大阪教育大学
    - 大阪公立大学
    - 兵庫県立大学
    - 京都教育大学

  - 情報提供
    - 富士通社内IT部門DXの取り組みとServiceNowの展開について
    - 大学におけるセキュリティ強化について

本年度の主なトピックス

大阪公立大学 Osaka Metropolitan University

- システム整備・更新
  - 大阪教育大学
    - SINET接続およびキャンパス間接続のトポロジ変更と増速
    - 付属学校へのシステム導入（GIGAスクール対応）
  - 大阪公立大学
    - 大学統合（大阪府立大，大阪市立大）によるシステム導入
    - BYOD（PC必携化）への対応
  - 兵庫県立大学
    - 事務系システム・業務系サーバの更新
    - クラウドサービス（Gmail, Google Workspace）の併用開始
  - 京都教育大学
    - 9月にシステム更新（更新時期を冬から夏へ）
    - Webメールの二要素認証，文字化けなどの不具合対応

大阪教育大学

大阪公立大学 Osaka Metropolitan University

- 学外ネットワークの増速とキャンパス間接続形態の変更
  - SINETの増速 10Gbps
  - 池田，天王寺，平野キャンパスをSINET直結に
- 附属学校へのシステム導入
  - GIGAスクール対応のため，無線LANを増強
  - 生徒用端末の導入，校務システムの導入
- 天王寺キャンパス合築棟ネットワーク機器調達
  - マルチギガ対応スイッチ，WiFi6の導入
- その他
  - 新入生のBYOD対応
    - 利用可能サービス，大学メール(大教Googleアカウント)，統合認証システム，大教Microsoft365アカウント，大学WiFiに接続　など

大阪公立大学

大阪公立大学 Osaka Metropolitan University

- 2022.04.01に大学統合
  - キャンパスネットワークの構築
    - キャンパス間ネットワーク，キャンパスネットワーク，無線LAN，…
  - 情報基盤システム
    - IDの一元化，認証基盤の構築，クラウド連携，メール，SSO，ポータル，Web，オンラインストレージ，…
  - 人事給与システム，教務学生システムの新規開発
  - 財務会計システムの一元化
  - 電子決済システムの導入
  - 教育支援系システム
    - 情報教育システム，LMS，ポートフォリオシステム，出席管理システム，…
  - ソフトウェアライセンス
  - PC必携化，無線APの増設
  - 図書館システム（2023.04稼働予定）の開発

  - 今回未着手なのは情報教育システム， CALLのみ
  - 2025年，森之宮キャンパス開設
    - スマートシティのデータセンター設置

兵庫県立大学

大阪公立大学 Osaka Metropolitan University

- Sandboxのリプレイス
- 事務系システムのリプレイス
  - 財務会計，人事給与，旅費精算
  - 事務用業務端末，プリンタ，ファイルサーバ，ネットワーク
  - 学生情報システム
    - コロナ禍で学生の利用が増加
- 学生サービス
  - 学生メールのGmail化，Google Classroom の（補完的）導入
  - Webメール，学生情報システム，OPACなどの二要素認証の導入
- 情報セキュリティ
  - 標的型攻撃メール訓練の実施

京都教育大学

大阪公立大学 Osaka Metropolitan University

- システムリプレイス
  - 9月にシステムを更新
    - 従来は冬の更新だったが，今回から夏の更新に変更
  - 主な問題点
    - Webメールの文字化け
    - Webメール二要素認証の制限
    - VLANの不具合
      - スイッチのVLAN数制限
- 情報セキュリティ
  - セキュリティ監査の実施
    - 大阪教育大学の協力を得て，外部からの監査
  - 標的型攻撃メール訓練の実施
    - 学生がひっかかるケースが増加
  - セキュリティ講習

2022年度
九州ブロック活動報告

宮崎大学 情報基盤センター
2023年3月10日
IS研総会

2022年度 九州ブロック活動報告

- 2022年9月2日(金)10:00～17:00（ Zoom）
- 現状報告
  - 九州大学　情報基盤研究開発センター
    - Microsoft 365 Exchange Onlineの基本認証廃止、全学VPNサービスの導入について 等
  - 九州工業大学　情報基盤センター
    - 情報統括本部への改組、学内情報システム（ 全学統合ID 、M365、教研システム、ネットワーク）の状況等
  - 佐賀大学　総合情報基盤センター
    - 組織体制変更（DX推進室設置他）、電子決済システム（グループウェア）導入、RPA 他、学内情報基盤運用状況 等
  - 長崎大学　ICT 基盤センター
    - 新情報基盤システム稼働開始、教職員電子メール移行＋多要素認証実践、対面授業状況、情報セキュリティ活動等
  - 熊本大学　総合情報統括センター
    - ネットワーク増設、DX Plus対応、出席管理システム構築、 SPARC採択、 新型コロナ対応（ PC・ルーター貸与、講義形態） 等
  - 大分大学　情報基盤センター/医学情報センター
    - SINET6 対応状況、基盤情報・教育情報システム状況 等
  - 宮崎大学　情報基盤センター
    - 屋外無線LAN 他ネットワーク環境整備、多要素認証、特権管理、情報セキュリティ対策の自己点検 等
  - 鹿児島大学　情報基盤統括センター
    - 情報基盤統括センターへの改組、新キャンパス情報ネットワーク運用開始、新電子計算機システム運用開始 等
  - 鹿屋体育大学　スポーツ情報センター
    - 学内情報システムの稼働状況、 新型コロナ禍での学生のPC・iPad 利活用傾向、 新情報基盤システム検討 等
- 情報交換
  - 大学DXに関する討議　現在地と将来に向けたアプローチ
  - 2023年度の開催日時　2023年9月1日(金)　宮崎にて開催予定

情報セキュリティ対策自己診断システムの構築

宮崎大学 情報基盤センター

2023年3月10日

IS研総会

情報セキュリティ監査

- 情報セキュリティに関する規程等の整備
- 平成24年度から実地による情報セキュリティ監査
- クライアント端末（PC）
  - 情報システム管理者規程に定める情報セキュリティ対策が実施されているか？
  - 情報基盤センター職員が書面（事前調査票）及び実地で監査
  - 実地監査では，事前調査票の記載事項に間違いがないかを数台を抽出して確認
  - 問題がある場合は，実地監査中に指導・改善
  - 実地監査中に改善ができない場合は，後日，再監査を行い確認
  - それでも改善することができない場合には，改善勧告
  - 改善勧告を受けた管理者は，セキュリティ対策を実施後，改善報告書を提出
- 利点
  - 監査時に管理者に対して直接，情報セキュリティの教育が可能
- 欠点
  - 実地監査を受けるのは4年に一回
  - 事前調査票を記入する際にPCのどこの何を確認すればよいかわからない管理者が多い
  - 事前調査票の内容が不正確（実機の状態と乖離）
  - 全数を詳細に監査することは不可能

情報セキュリティ対策自己点検

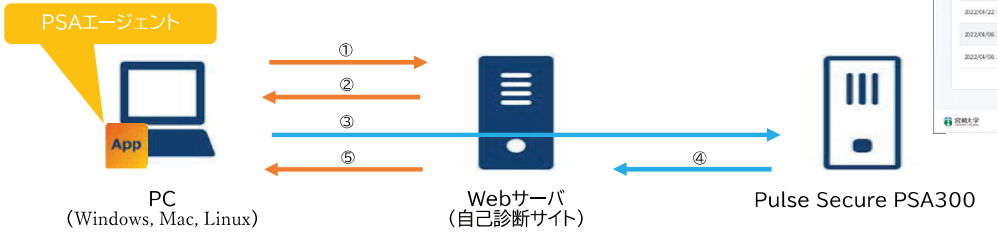
- 情報セキュリティ対策の状態を自ら確認する「自己点検」を推進
- 課題
  - 個々の管理者（個人のPCについては利用者）が確認することが困難
  - どれだけの管理者が自己点検を行っているか把握することが不可能

- 「自己診断システム」を構築
  - 「検疫システム」や「IT資産管理ツール」のような、接続の制限やPCの制御，常時監視を行うものではない
    - 抵抗感を軽減
    - 費用を抑える
    - マルチOS（Windows, Mac, Linux）対応

自己診断システム

- 目的
  - 実地監査の負担軽減（自己点検）
  - 実施状況の把握（オンライン）
  - PC管理者の負担軽減・確実な実施（自動診断）

- システム



自己診断システム

- 診断項目

診断項目	基準
OSのバージョン	エディション，バージョン
OSアップデート日	＜90日
ファイアウォール動作	有無
ウイルス対策ソフト動作	有無
ウイルス対策ソフト定義ファイル更新日	＜5日
ウイルス対策ソフトスキャン実施日	＜5日
EDR動作（機密性3情報保有PCのみ）	有無
ログインパスワードの設定（自己申告）	英数記号を含む8文字以上
スクリーンロック設定	有無
HDD暗号化（持ち出しPCのみ）	有無

自己診断システム

- 診断方法
  - 自動診断
  - 自己申告

自動診断

自己申告

実施方法

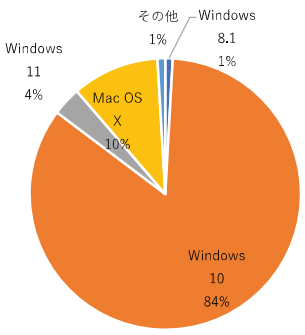
- 情報セキュリティ対策講習（eラーニング）と併せて実施
  - 説明文に自己診断を実施することを記載
  - 問題に自己診断を実施したか設問
- 期間：2022年4月１2日～2020年7月10日（3か月間）
- 対象者：本学の教職員および学生を含む全構成員
- 対象PC：本学のネットワークに接続するPC

  - 情報セキュリティ対策講習は義務化しているが，自己診断システムを使った自己点検については義務化していない．

実施結果

- 実施者：1,263名（学生785名，教職員478名）
  - 本学構成員（約7,600名）の16%程度

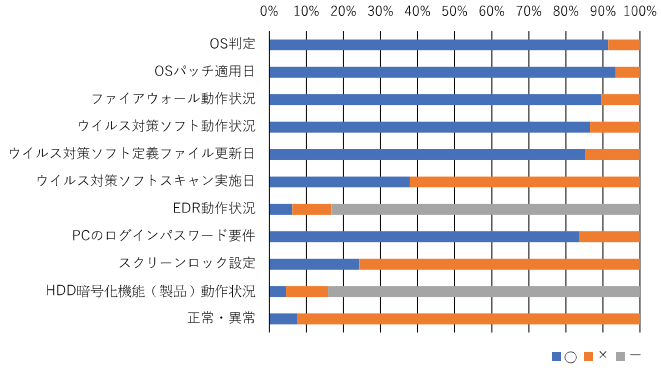
- 実施PC：1,397台
  - 自動診断：1,181台
  - 自己申告：216台



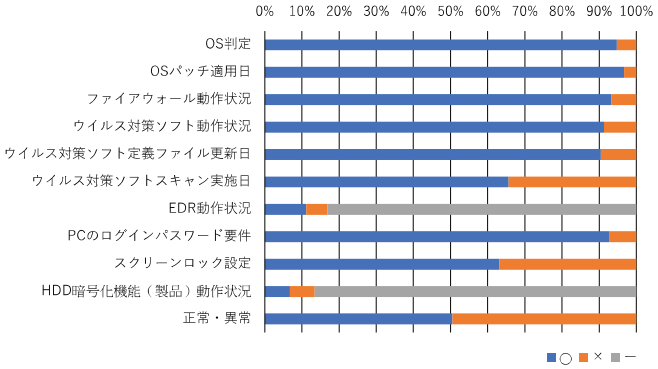
診断OSの割合

実施結果

- 診断結果の比較
  - 改善のきっかけになっている



初回診断結果



最終回診断結果

まとめ

- オンライン自己診断システムの構築
- 自己診断の実施
- 結果（対策状況）の把握

- 課題
  - 実施率の向上
  - 継続的な実施
  - システムの改修
  - 結果の全学へのフィードバック

事 務 局 だ よ り

2022 年度 IS 研活動報告

１．総会（ハイブリット開催）　会場：富士通株式会社　本社事務所　24 階　大会議室

日　　時： 2023 年 3 月 10 日（金）　14:00～17:15

参加実績（順不同）

お茶の水女子大学	大分大学	大阪教育大学	大阪公立大学	大阪府立大学 大学院
金沢大学	北見工業大学	岐阜大学	順天堂大学	長崎大学
名古屋大学	一橋大学	兵庫県立大学	福井大学	北陸先端科学技術大学院大学
宮崎大学	室蘭工業大学	山形大学	横浜国立大学	

【プログラム】

開会挨拶

会長　横浜国立大学　　徐　浩源

論文発表(1)
「xR 技術を活用した教育 DX システムの実証評価」

金沢大学　　東　昭孝

北陸ブロックからの事例発表
「IS 研北陸ブロック活動報告」

福井大学　吉川 雄也

東北・関東ブロックからの事例発表
「東北・関東ブロック報告」

山形大学　田島　靖久

論文発表(2)
「組織内端末の Web アクセスの規則性に着目したプロキシログ中の異常検知」

大阪府立大学大学院　名倉　悠

東海ブロックからの事例発表
「東海地区における活動について」

名古屋大学　戸田　智

近畿ブロックからの事例発表
「近畿ブロック活動報告」

大阪公立大学　宮本　貴朗

論文発表(3)
「標的型サイバー攻撃検知技術によるセキュリティ懸念の調査と対応事例」

山形大学　伊藤　智博

九州ブロックからの事例発表
「情報セキュリティ対策自己診断システムの構築」

宮崎大学　青木　謙二

閉会挨拶

議長　大阪公立大学　宮本　貴朗

2. 各ブロック活動

北海道ブロック活動(2023 年 2 月 2 日 / Teams によるオンライン会議)
「北海道地区大学情報システム研究会」を開催

参加者所属機関(敬称略・順不同)

・北見工業大学　(1 名)　・室蘭工業大学　(4 名)
・小樽商科大学　(4 名)　・旭川医科大学　(2 名)　・
・公立千歳科学技術大学　(1 名)※中座

・富士通 Japan 株式会社(北海道支社、教育ソリューションビジネス推進部)

テーマ:大学ＤＸ

1. 世話人挨拶
北見工業大学　情報処理センター長　升井　洋志様

2. ご講演
国立大学法人北海道国立大学機構　小樽商科大学　グローカル戦略推進センター教学 IR 室　准教授　　西出　崇様より
『IR のための情報基盤とその活用-小樽商科大学の事例を中心に-』についてご講演

講演概要：
- IR は組織内の状況や課題を把握し、その情報を活用し意思決定や企画立案のツール
- 大学がおかれている厳しい環境、説明責任の必要性などを理由に IR が注目されている
- 部局横断的かつ専門的に分析をし、活用することが組織内外から求められている
- 私学での志願者確保など、IR の目的や位置付けは大学により様々
- 定常的なデータのモニタリングや課題志向の調査と分析、データマネジメントを実施
- ツールや基盤、データの管理方法は組織によって様々
- データを自動的に抽出・加工、定期的なレポート出力
- オープンソース製品を中心に構成（仮想マシン上にサーバを構築）
- 日常業務の基盤は RStudio Server を活用
- IR は分析結果が、改善や意思決定に直結するわけではなく、統計分析の素養がない人にも解り易く示し、コミュニケーションや意思決定を促進することが重要
- 現状は可視化に留まる、課題や問題意識がなければ分析が成立しない

ご講演への質疑応答内容
1) 貴学では基盤をオープンソース系で構築され、アップデートが大変だと思うが、どのように対応されているか？
- 特にアンケート基盤 respon は月 2 回程度アップデートがあり、スクリプトを記述して対応している。
本来は IR 基盤として情報センターと連携して管理すべきと考えている。

3. 富士通 Japan からの情報提供
富士通株式会社　Japan リージョン　ビジネスマネジメント本部　戦略企画室　シニアエバンジェリスト　西本 伸一氏より
『データドリブン時代におけるテクノロジーの社会実装について』を情報提供

4. 意見交換会　各大学様からの大学の DX に対する取組みや検討状況などの紹介

1) 北見工業大学
- 3 大学法人統合　国立大学機構として 2022 年 4 月よりスタート
- データ統合は、今年度から検討予定
- 3 大学全体の課題と個々の課題。課題が二重化している
- 数理・データサイエンス・AI 教育特定分野校となっている。
- コンソーシアムにて他大学への啓蒙など教研を担う役割を考えている

2) 小樽商科大学
- センターのスタッフ体制：計 4 名
- 2022 年度 3 大システムを更新
  - キャンパス NW システム　　認証不具合あり旧 SSL-VPN を継続利用中
  - 仮想デスクトップシステム　　学外利用に課題
  - メールシステム　　Microsoft 側障害が多い、メール障害のため通知不可
- SINET6 に更新
- 商用データセンター北見 L2VPN 利用

3) 室蘭工業大学
- SINET6 への更新（100Gbps）昨年 5 月、室蘭データセンター開設
- 全学情報基盤システム 2023 年 9 月稼働予定
キャンパス情報ネットワークと情報基盤教育システムを一本化
- 遠隔授業対応（BYOD の活用、対面、遠隔授業への対応）
- 1 年生向けヘルプデスク開設
- プライベートクラウドを使った授業の実施
- ガルーンへグループウェアを更新（現在 FIT&GAP 検証中）
- ISMS BCMS 昨年 9 月琉球大学との相互監査
- サーベイランス審査　3 月予定
- 技術補佐員の雇用開始。学生アルバイト採用
- Wi-fi 認証 eduroam 一元化
- 有線 LAN 教員セグメント分離化を検討
- 電子メールを活用する外部のサービスを導入

5. 事務局からの連絡事項、閉会

東北・関東ブロック活動報告

２０２３年２月３日（金）　オンライン開催（Ｔｅａｍｓ）

参加者所属機関(敬称略・順不同)

山形大学	情報ネットワークセンター
横浜国立大学	国際戦略推進機構
一橋大学	情報基盤センター
富士通 Japan 株式会社	東京エリア本部東京第二統括ビジネス部、東日本エリア本部山形支社、東日本エリア本部福島支社、東エリア本部神奈川支社、東日本エリア本部エリアビジネス推進統括部

主要プログラム

（1）開会挨拶	東北・関東ブロック世話人 山形大学　情報ネットワークセンター　田島 靖久
（2）進行につきまして	事務局連絡事項
（3）報告・発表	（発表順）
① 一橋大学	発表者：一橋大学　情報基盤センター　中田 亮太郎 「学内無線(1284Wireless)整備とその後の対応について」 -2022 年度の主な取り組み・学内無線 LAN - 1284Wireless(概要、NW 構成等)・トラブル対応(原因と対応)・今後の対応について(稼働状況の見える化の検討)
② 横浜国立大学	発表者：横浜国立大学　国際戦略推進機構　徐 浩源 「横浜国立大学の IT 環境の動向」 -教育研究システムの更新(BYOD の徹底 他)・事務 DX の推進(検討会議のすすめ方、スケジュール、検討状況)・情報セキュリティの推進(セキュリティ教材のビデオ教育への切り替え、ITSC の情報セキュリティマネジメント)について
③ 山形大学	発表者：山形大学　情報ネットワークセンター　田島 靖久 「2022 年度活動報告」 －SINET6 移行(2022.04～)・Network 更新延期決定・情報処理講義更新・改組(2022.10～学術基盤機構設置)・Security 事案・学生証のこれから
（4）富士通からのご紹介	発表者：富士通 Japan 株式会社　東日本エリア本部　エリアビジネス推進統括部　寺下 一欣 「データ利活用・DX を推進するこれからの大学ソリューション」 -AI(ChatGPT)・大学向けソリューション・富士通の大学ビジョン・大学変革とデータ活用・IDYX(現 Fujitsu CaaS Data e-TRUST)
（5）閉会挨拶	東北・関東ブロック世話人 山形大学　情報ネットワークセンター　田島 靖久

北陸ブロック活動(2023 年 2 月 20 日（月）15:00-17:30 オンライン開催)

参加者所属機関(敬称略・順不同)

・金沢大学	(学術メディア創成センター)
・北陸先端科学技術大学院大学	(情報社会基盤研究センター)
・福井大学	(総合情報基盤センター)
・富士通 Japan 株式会社	(北陸支社第二ビジネス部)

主要プログラム

１．　世話人挨拶　　:福井大学　吉川 雄也

２．　会員報告・ディスカッション　　:会員代表者より、組織概要、システムの導入・稼働状況や課題等について発表し、意見交換を行った。

・金沢大学
学術メディア創成センター概要、教育 DX の活動（xR キャンパスシステム）を中心に総合情報基盤システム（2022/3/1 稼働）や事務システム（2023 年度更新）に関する情報を共有。

・北陸先端科学技術大学院大学
昨年、DX 推進に向けて改組、統括本部配下に設けられた 2 センター概要や 2022 年度調達の情報環境システムに関する情報を共有。
3 年ぶりの現地開催となった SC22 概況、JAIST ブースに関する情報も共有。

・福井大学
総合情報基盤センター概要、2022 年度の主な取り組み、全学ネットワーク更新やセンターシステム更新に関する情報を共有。

なお、本日の概要は、3 月 10 日開催の IS 研総会にて北陸ブロックの事例報告とする。

３．　事務局連絡　　:

・3 月 2 日（木）15:00～16:00　2022 年度第二回 世話人会について
・3 月 10 日（金）14:00～17:30　第 31 回 国公立大学情報システム研究会総会について
北陸ブロックからの事例報告（活動報告内容・発表者）の検討

以上

東海ブロック活動報告

2023 年 2 月 15 日(水) 14:00～16:50　オンライン会議/テーマ： Learning Analytics

参加者所属機関(敬称略・順不同)

名古屋大学	戸田、出口、後藤
岐阜大学	村上、長谷川
三重大学	田ノ上
愛知教育大学	福井
愛知県立大学	落合
九州大学	島田
富士通 Japan 株式会社	東海支社 第一ビジネス部、パートナー・プロモーション戦略統括部 プロモーション推進部
株式会社セールスフォース・ジャパン	Tableau 事業統括　公共広域営業本部　藤田、 ソリューション・エンジニアリング本部　黒沢

主要プログラム

(1)開会挨拶	東海ブロック世話人 名古屋大学　戸田	
(2)近況報告	(発表順)	
① 名古屋大学	東海国立大学機構として、岐阜大学と情報基盤の足並みをそろえている。 23 年度から機構 LMS へ統一展開するため、現在準備を進めている。	
② 岐阜大学	名古屋大学と同様機構 LMS への統一を進めている。また、来年度、全学システムの切り替えがあるため、 新システムの稼働を急務として進めている。	
③ 三重大学	5 年に 1 度の全学システムのリプレイスのタイミングであり、稼働に向けて準備を進めている。	
④ 愛知教育大学	24 年 3 月稼働に向けて次期システムの仕様書案の説明会を先日開催。各社の意見を集め仕様書を定めていく。 円安・物価高の影響で現行のシステムを移管するのすら予算的に厳しい状況	
⑤ 愛知県立大	愛知県立大学の文系学生を対象にしたシステム公開の準備を進めている。 愛知教育大学同様に、円安・物価高の影響から、予算的に厳しい状況	
(3)基調講演	「九州大学における教育 DX の取り組み ～クラウド基盤導入、支援体制構築、データ駆動型教育の実践～」	国立大学法人 九州大学　大学院システム情報科学研究院 教授　島田
(4)講演	「Tableau を活用した大学のアナリティクス事例や 教育データの利活用のご紹介」	株式会社セールスフォース・ジャパン　Tableau 事業統括 公共広域営業本部　藤田 ソリューション・エンジニアリング本部 黒沢
(5)情報交換	【話題提供】名古屋大学における学生利便性向上を目指した LMS 連携システムの開発	名古屋大学　戸田
(6)閉会挨拶	東海ブロック世話人 名古屋大学　戸田	

近畿ブロック活動報告

2022 年 2 月 21 日(月) 現地（梅田ダイビル）対面及びオンラインミーティング（Zoom)によるハイブリッド開催

参加者所属機関(敬称略・順不同)

大阪教育大学	情報処理センター
京都教育大学	情報処理センター
大阪公立大学	情報基盤センター
兵庫県立大学	学術総合情報センター
富士通株式会社	デジタルシステムプラットフォーム本部　クラウドサービス統括部 グローバルソリューションビジネスグループ　インフラ＆ソリューションセールス本部
富士通 Japan 株式会社	大阪第二統括ビジネス部第三ビジネス部、京都支社

主要プログラム

(1)開会挨拶		近畿ブロック世話人 大阪公立大学　宮本 貴朗先生
(2)講演		富士通株式会社　デジタルシステムプラットフォーム本部　クラウドサービス統括部　高橋　勉 「富士通社内 IT 部門 DX の取り組みと ServiceNow の展開について」
(3)トピックス報告		
①	大阪教育大学	学外ネットワークの増速とキャンパス間接続携帯の変更、附属学校へのシステム導入（GIGA スクール対応)、令和 3 年度補正予算の対応、天王寺キャンパス合築棟ネットワーク機器調達に向けた準備（予算)、新入生への BYOD 整備に向けた対応
②	大阪公立大学	「大学統合その後の対応について」キャンパスネットワークの構築、情報基盤の構築、人事給与・教務システムの新規開発、財務会計システムの一元化、電子決済システムの導入、教育支援システムの構築、PC 必携課・無線 AP の増設対応（1500 台)、2025 年森ノ宮キャンパス開設に向けた対応
③	兵庫県立大学	兵庫県立大学の説明、2022 年からの話（全学セキュリティ・事務システム)、1 年間で対応してきたこと（学生の Gmail 化、GoogleClasroom サービス活用の検討、学外からのアクセス用ポータルの構築、標的型攻撃メール訓練 MudFix の導入、情報教育システムリプレイス向けての仕様書策定)
④	京都教育大学	システム更新（9 月の更新/更新への問題点：Web メールの文字化け、Web メール二要素認証の制限、VLAN の不具合)、新型コロナウイルス関連（原則対面授業を実施、CO2 濃度の測定、Google workspace for Education の有償プランの見直し)、情報セキュリティ（セキュリティ監査、標準型攻撃メール訓練、セキュリティ講習)、PC 必携化への PC 購入推奨（必携化はまだ)
(4)情報提供		富士通株式会社　グローバルソリューションビジネスグループ　インフラ＆ソリューションセールス本部 入澤　晃二　「大学様におけるセキュリティ強化について」
(5)閉会挨拶		近畿ブロック世話人 大阪公立大学 宮本　貴朗先生

2022 年度　九州ブロック活動報告(2022 年 9 月 2 日,Zoom)

参加者所属機関(敬称略・順不同)
・宮崎大学　　(情報基盤センター)
・九州大学　　(情報基盤研究開発センター)
・九州工業大学　　(情報基盤センター)
・佐賀大学　　(総合情報基盤センター)
・長崎大学　　(ICT 基盤センター)
・熊本大学　　(総合情報統括センター)
・大分大学　　(情報基盤センター・医学情報センター)
・鹿児島大学　　(情報基盤統括センター)
・鹿屋体育大学　　(スポーツ情報センター)

・富士通株式会社　　(福岡支社 第二ビジネス部、宮崎支社、エリアビジネス推進統括部 ＤＸＢＣ部)

主要プログラム
① 開会ご挨拶　　宮崎大学
② 各大学様　現状ご報告/発表（現況報告・システム運用課題や研究概要等）

・九州大学　　Microsoft 365 Exchange Online の基本認証廃止、全学 VPN サービスの導入について等
・九州工業大学　　情報統括本部への改組、学内情報システム（全学統合 ID、M365、教研システム、ネットワーク）の状況等
・佐賀大学　　組織体制変更（DX 推進室設置他）、電子決済システム（グループウェア）導入、RPA 他、学内情報基盤運用状況等
・長崎大学　　新情報基盤システム稼働開始、教職員電子メール移行＋多要素認証実践、対面授業状況、情報セキュリティ活動等
・熊本大学　　ネットワーク増設、DX-Plus 対応、出席管理システム構築、SPARC 採択、新型コロナ対応（PC・ルーター貸与、講義形態）等
・大分大学　　SINET6 対応状況、基盤情報・教育情報システム状況等
・宮崎大学　　屋外無線 LAN 他ネットワーク環境整備、多要素認証、特権管理、情報セキュリティ対策の自己点検等
・鹿児島大学　　情報基盤統括センターへの改組、新キャンパス情報ネットワーク運用開始、新電子計算機システム運用開始等
・鹿屋体育大学　　学内情報システムの稼働状況、新型コロナ禍での学生の PC・iPad 利活用傾向、新情報基盤システム検討等

③ 情報提供・情報交換会
・大学 DX に関する討議
現在地と将来に向けたアプローチ
・IS 研ご紹介
活動内容、他
・2023 年度の開催日時について
2023 年 9 月 1 日（金）／宮崎にて開催予定

以　上

『総会開催』及び『論文募集』について

IS 研では，各地域ブロックでの研究活動の他に，これら活動内容についての情報交換や会員相互の啓発と親睦を図る為に，年 1 回の総会を開催しております．

本総会では，日頃の研究成果の講演発表や大学における情報システムの利活用に関する諸問題についての討議を行うなど，会員にとって大変有意義なものであると考えております．

一方，大学における情報システム環境を科学的な見地から研究し，学問としての社会的な評価を確立すべく，上記地域ブロック活動や総会で発表された論文を論文誌として発行することも本研究会の大事な事業の一つであります．

つきましては，2023 年度の総会と論文募集について下記の通りご案内させていただきます．会員の皆様におかれましては奮ってご投稿賜りますようお願い申し上げます．

今年度は,大学における情報システムの利活用全般， 特にシステム導入事例等,会員の共通の利益に資する内容で募集いたします．

情報センター部門以外の方も投稿できますので，ぜひご投稿をお願いいたします．

尚，ご投稿論文の論文誌掲載につきましては，事前に地域ブロック活動又は総会で発表することを前提としておりますので，これらのスケジュールを念頭において執筆いただきますようお願い申し上げます．

記

1．総会日時　：2024 年 3 月上旬（午後）
2．場所　　：オンラインまたはハイブリッドで開催

3．講演／論文テーマ　：以下のような情報システムの利活用に関し,特にシステム導入事例等,会員の共通の便益に資する内容で募集

1)　情報システムの導入・構築，管理・運営に関する内容
2)　情報システムの利活用に関する内容（活用事例等）
3)　情報システムに携わる人材の育成や利用者の教育に関する内容
4)　情報システムを管理運営する組織や人材，利用規定やポリシーなどに関する内容
5)　情報システムの評価や将来計画に関する内容
6)　その他，大学の情報システムに関する内容で，会員間で情報共有すると有益なもの

4．論文応募要領　：10 月ご案内予定
募集案内に添付された申込書にて事務局宛ご応募願います．

5．執筆要領　：『大学情報システム環境研究』執筆要領 ご参照．

6．論文誌発行スケジュール（予定）

1)　論文募集 ・・・・・・・・・・・・・・・・・ 2023 年 10 月
2)　論文(発表･論文誌投稿)応募締切・・・・・ 2024 年 1 月 31 日
3)　論文及び発表原稿締切 ・・・・・・・・・ 2024 年 2 月 23 日
4)　査読・修正期間 ・・・・・・・・・・・・・・・・ 3 月～6 月
5)　論文誌発行 ・・・・・・・・・・・・・・・・・・ 7 月

7．その他　：
本研究会の論文誌は国立国会図書館および科学技術振興機構(JST)に寄贈され，記載論文は両機関のデータベースに収録，公知の技術情報となります．JST 収録については，論文抄録(要約)の原文無料記載を許諾しており，また，論文および発表予稿は論文誌掲載後，本研究会ホームページ上で公開される予定になっています．予めご承知おき願います．

以 上

論文誌「大学情報システム環境研究」について

編 集 委 員 会 規 則

1．国公立大学情報システム研究会（以後，IS 研という）は，論文誌「大学情報システム環境研究」を円滑に発行するための論文誌編集委員会（以後，委員会という）を置く．

2．委員会は，IS 研によって発行する論文誌に投稿された論文，報告，解説等について一定の査　読者を決定すると共に，それらに対する査読者の所見にしたがって論文誌掲載の可否を審議決定する．
   1)　委員会は，IS 研総会までに投稿された論文等で，掲載して価値のあるものについては，その年度内に発行する論文誌に掲載できるよう努めなければならない．
   2)　委員会は，その他論文誌発行に関する必要事項を審議決定することができる．

3．委員会は，会長，各地域ブロックの世話人と事務局員で構成する．

4．委員会に委員長を置く．
   1)　委員長は委員の互選によって決定する．
   2)　委員長の任期は1年とし，再任を妨げない．
   3)　委員長は委員会を招集し，その議長となる．

5．各年度の第1回委員会は，IS 研総会の前に開催されなければならない．
   第2回以降の委員会は，電子メールによる持ち回り会議に換えることができる．

6．委員会は，必要に応じて委員以外の者の意見を聴取することができる．

以　上

発 行 要 領

1．論文誌の発行は，年1巻を原則とする．

2．原稿の受付は，年度始めから総会開催の1ヵ月前迄を原則とする．

3．投稿の受付は，教育・研究機関，または賛助会員に限定するものとする．

4．投稿する原稿は，IS 研総会または地域ブロック研究会において発表しなければならない．
   投稿された原稿は，論文または解説，報告，その他（総説・展望・技術紹介 etc.）として取り扱うものとする．

5．投稿された原稿の査読は，論文誌編集委員会で行うことを原則とする．ただし，原稿の専門分野によっては，委員以外の者に依頼することができる．

6．投稿する原稿の執筆要領については，別途定める．

7．論文誌の印刷および配布については，IS 研事務局に一任する．

以　上

査 読 要 領

1．「論文」の査読について

1）査読者は以下の項目を調査し，論文として適当であるか否かを査読し，加筆・修正した査読用原稿とともに，２週間以内に編集委員長に報告するものとする．

2）査読者は２名以上とする．

3）調査項目
(1) オリジナルな研究の報告であるか　・・・　「原著論文」として評価する．
(2) 初めての試み・実験の結果報告等　・・・　「実践論文」として評価する．
(3) 文章表現などに不適切な表現がないか．
(4) 追試し，再現性をテスト出来るだけの情報（引用文献リストなど）が記載されているか．
(5) 出来るだけ簡潔・明瞭に書いてあるか．

2．「解説」「報告」「その他（総説・展望・技術紹介 etc.）」の査読について

1）査読者は以下の項目を調査し，解説，報告，その他（総説・展望・技術紹介 etc.）として適当であるか否かを査読し，加筆・修正した査読用原稿とともに，２週間以内に編集委員長に報告するものとする．

2）査読者は１名以上とする．

3）調査項目
(1) 広範囲の人々の関心を引き起こしそうな話題，考え方，アイデア，実験結果等を含む解説，報告，その他（総説・展望・技術紹介 etc.）であるか．
(2) 文章表現などに不適切な表現がないか．
(3) 読者を納得させることが出来るだけの情報（引用文献リストなど）が記載されているか．
(4) 出来るだけ簡潔・明瞭に書いてあるか．

3．IS 研における著作権の帰属について

1）著作権は基本的に著者に帰属するものとする．

2）IS 研総会運営，IS 研論文誌発行に必要な範囲で執筆者に利用許諾を受ける形式とする．

以　上

論文誌「大学情報システム環境研究」執筆要領

Guideline to Prepare the Paper for “Academic Information Processing Environment Research"

○山　太郎*，△川　花子†

Taro MARUYAMA* and Hanako SANKAKUGAWA†

□□大学*　　富士通株式会社†

□□ University*　　FUJITSU LIMITED†

論文誌「大学情報システム環境研究」掲載論文に関して,日本語タイトル,英文タイトル,日本語執筆者名,英文執筆者名,日本語所属,英文所属,電子メールアドレス,日本語アブストラクト,日本語キーワード,英文アブストラクト,英文キーワード,本文の形式,フォントの種類,大きさ,図・表に関する指示,参考文献の書き方,著者略歴,写真の位置,印刷時の体裁を定める.執筆者はできるだけここの指定に従うことを期待されている.

キーワード：大学情報システム環境研究，執筆要領，印刷見本

The author can find the details about how to prepare a camera-ready paper for “Academic Information Processing Environment Research" from the view point of position, font, and size of title, author name(s), affiliation, abstract, keywords, figure, table, references, and so on in Japanese and English respectively. The author is strongly expected to follow the guideline to prepare a camera-ready paper for “Academic Information Processing Environment Research".

Keywords：Guideline for “Academic Information Processing Environment Research”, camera-ready paper

*情報基盤センター

〒000-0001 □□県□□市□□1-1-1

Information Technology Center

〒000-0001 1-1-1, □□, □□-shi, □□, JAPAN

E-mail：○○@□□.ac.jp

†大学ビジネス推進部

〒105-7123 東京都港区東新橋 1-5-2

Higher Education Business Promotion Dept.

〒105-7123 1-5-2, higashi-shinbashi, Minato-ku Tokyo, JAPAN

E-mail：△△@jp.fujitsu.com

1. はじめに

論文誌「大学情報システム環境研究」は国公立大学情報システム研究会(IS 研究会）が年 1 回発行する論文集である．大学における情報システムの管理・運営や利活用などに関する内容を報告することで会員相互の情報共有を円滑に行うことを目的としている．またこのような日頃の活動に関する報告がなかなか権威ある学術論文誌に論文として採録されにくい現状を踏まえ，業績として認められるように,学会と同レベルの査読を行っている．本誌に投稿するには，事前に各地区ブロックの研究会で発表するか，年に 1 回の総会で発表することが要請されている．改めて関係者の貢献を歓迎したい．ここではこの論文誌に

論文，報告などを投稿する際にまもるべきスタイルについて解説する．

2. 基本方針

- 記述言語は日本語または英語とすること．
- 最終原稿は PDF ファイルとすること．その際，フォントを埋め込んであることが望ましい．
- 原稿は A4 ポートレイト(縦長，詳細は後述）とし，特に枚数に制限を設けないが，通常の学会論文誌に準じて 8 ページ程度が望ましい．記述が冗長にならないように十分に注意すること．
- 論文については原著論文，実践論文の 2 種類があり，特に「オリジナルな研究，世界で初めての実験・試行の結果について述べたもの」は原著論文とし，先進的な試みについて述べたもの等は実践論文として取り扱う．
- 論文(原著，実践）の他に，解説，報告，その他(総説・展望，技術紹介など）という分類を設ける．
- 分類については，著者が申告するものとするが，論文誌編集委員会において分類の変更が必要と判断した場合には著者の了解のもとに分類の変更を行う．
- 編集委員会において，発表内容にコメントがついた場合は修正を求める．その際の締切は原則として修正依頼の連絡後二週間以内とする．ただし最終原稿の締切については，状況に応じて論文誌編集委員会が指定するものとする．
- 原則として論文は 2 名以上の査読委員が，その他の原稿は 1 名以上の査読委員が査読を行う．査読委員は論文誌編集委員会が推薦して，事務局から査読を依頼する．

3. 原稿の内容と体裁

3.1 印刷時の体裁

1. 原稿は A4 ポートレイト(縦長）とする．
2. 上余白は 20㎜，下余白は 15㎜ 程度とする．
3. 左余白，右余白は，25㎜ 程度，段落の間は 10㎜ 程度とする．
4. 本文は読みやすい文字間隔・行間隔をとること．
5. 本文のフォントは後述するように 10.5 ポイントとするが，10.5 ポイントが難しい場合は 11 ポイントでも良い．
6. 1 ページは 41 行×20 字× 2 段組とする．

3.2 見出しなど

表題から電子メールアドレスまでの記載順位は以下の順とし，これらについては一段組で中央揃えとする．文字フォントも下記に指定されたもの，またはそれにできるだけ近いものを採用すること．

1. 日本語タイトル
   ゴシック体，14 ポイントとし，太字で強調すること．
2. 英文タイトル
   Century，14 ポイントとする．
3. 日本語執筆者名
   明朝体，12 ポイントとし，次のような点に注意すること．
   - 名字と名前の間は全角のスペース 1 個を挿入する．
   - 複数の執筆者がいる場合には，名前はカンマで区切ること．
   - 所属毎に，マークで識別して，所属部局，住所，電子メールアドレス等の補足情報は脚注に記述する．ここでの脚注マークには数字以外のマーク(*、†、‡、等）を使用すること．
     なお，電子メールアドレスの記載は任意である．
4. 英文執筆者名

Century, 12 ポイントとし，次のような点に注意すること．

- 名前と名字の間は半角のスペース 1 個を挿入し，名字は全て大文字で記載する．
- 執筆者が 2 名の場合は and でつなぐ．著者が 3 名以上の場合には，最後の人はカンマと and でつなぐ．
- 所属毎に，日本語名と同じマークで相互の関係を明示し，日本語の補足情報と同様に英文の補足情報を脚注に日本語の情報に続けて記述する．

5. 日本語所属
   明朝体，10.5 ポイントとする．組織の代表名のみ記述する．
6. 英文所属
   Century, 10.5 ポイントとする．組織の代表名のみ記述する．

3.3 アブストラクトとキーワード

第 3.2 節で示した項目に続けて，アブストラクトとキーワードを次の要領で記述する．これらは左詰め,両端揃えで,一段組とする．

1. 日本語アブストラクト
   明朝体，10.5 ポイントとする．見出し（概要，アブストラクトなどという言葉）をつけずに本文のみを記載し，出来れば行間を少し詰め，本文との区別を分かりやすくすること．また 1 行の幅を本文の行幅よりも少し短くし，区別がつくようにしても良い．
2. 日本語キーワード
   明朝体，10.5 ポイントとする．例は本稿を参考にされたい．
3. 英文アブストラクト
   Century, 10.5 ポイントとする．日本語アブストラクトと同様の配慮を行う．例は本稿を参考にされたい．
4. 英文キーワード
   Century, 10.5 ポイントとする．例は本稿を参考にされたい．

3.4 本文

本文は二段組とし，著作の種別によらず，同一の形式とする．本文は明朝体，10.5 ポイントとする．次のような点に注意すること．

1. 英語の略語には括弧書きで(フルスペル)をそえること．
2. 句読点は“,”と“.”(カンマとピリオド)とし，“、” と“。”ではないので注意されたい．
3. 項番の付与方法は次の例に従うこと．見出しはゴシックとすること．
   1. セクション
   1.1 サブセクション
   また，「1. セクション」のようなセクションの見出しは本文よりやや大きめの 13 ポイントとする．また「2.1 サブセクション」のようなサブセクションの見出しは本文とセクションの見出しの中間の大きさの 12 ポイントとする．
4. 図・表については次の通りとする．
   - 原則として本文中に取り込むこと．
   - 段組の制約を受けないが，二段にまたがる場合には上か下にまとめること．
   - 図には図の下に，表には表の上に名称を記載するものとし，名称の表現については次の通りとする．
     図・表種別，図・表番号，スペース 1 個，図・表の名称
     ＜例＞
     図 1　システム構成図
5. 参考文献は文末(著者略歴の前）に「参考文献」という見出し(ゴシック左詰め）に続けて，両括弧付の通し番号，著者名，論文タイトル，書名または論文誌名，巻号，ページ数，発行年という順番で記載し，参考文献は引用場所

[1),2)] というように記載することとする. URL による引用は，時間の経過につれて実体を参照できなくなる可能性があるので，できるだけ避けて欲しいが，やむを得ない場合には例のように記述する [3)]．参考文献は引用順に記載すること.

6. 著者略歴は参考文献の後に「著者略歴」という見出し(ゴシック左詰め) に続けて，著者の写真(第一著者のみ，白黒が望ましい，40㎜×30㎜)，名前(ゴシック)，略歴(全員) を写真の右側から書き始め，二段組で記載する. 略歴は，原則的に改行なしで一人分を 10 行程度以内にまとめる.

謝辞

本研究の実施に際しては〇×大学の□△教授に有益なご指導を頂きました．ここに記して感謝の意を表します.

参考文献

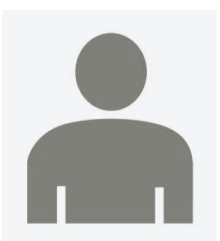
(1) 〇山太郎，△川花子，□谷吉男 : “大学情報システム環境研究 Vol18”，pp. 13 - 18(xxxx)

(2) 国公立大学情報システム研究会 http://www.is-ken.gr.jp/

(xxxx 年 x 月 x 日　原稿受付)

(xxxx 年 x 月 x 日　採録決定)

著者略歴



〇山太郎 xxxx 年情報環境大学卒業，xxxx 年同大学院〇〇研究科博士後期課程修了，同年 4 月同大学〇〇学部助手，xxxx 年同大学情報処理教育センター准教授，xxxx 年同大学教授，xxxx 年 4 月から xxxx 年 4 月まで情報基盤センター長，工学博士.

△川 花子 xxxx 年 3 月□□大学卒，同年 4 月富士通株式会社入社，SE 部門に配属，以来関東地区の大学研究所関係のシステム構築・運用支援・PKG 開発などに従事，xxxx 年 4 月から現職.

国公立大学情報システム研究会
会　　則

第１条　（名称）

本研究会は，「国公立大学情報システム研究会」（略称 IS 研）と称する．
（以下，本会と称す）

第２条　（目的）

本会は，大学における情報・通信処理の基盤となる情報システムの構成・構築法，運用管理等に関連する事項，情報・通信処理機能および情報サービスについて科学的な見地から研究し，学問としての社会的な評価を確立する事を目指すとともに会員相互の啓発と親睦を図ることを目的とする．

第３条　（事業）

本会は，第２条に定める目的を達成するため次の事業を行う．
１．情報システム及び情報サービス機能に関する開発・研究活動,および大学における情報システムの利活用に関する調査・研究活動．
２．会員相互の情報交換，研究発表会の開催及び論文誌「大学情報システム環境研究」の発行．
３．今後の情報産業の発展に資する事業．
４．その他，本会の目的を達成するために必要な事業．

第４条　（会員）

本会は，次の各号に掲げる会員をもって組織する．
１．正会員　　本会の目的に賛同して入会を希望する，情報システムの構築・運用に携わる大学の機関及び大学等の教職員．
２．賛助会員　本会の目的に賛同し，事業を賛助する団体．
会員の入退会については，世話人会の判断において許可する．

第５条　（世話人）

本会の活動を円滑に推進するため，地域毎に世話人をおく．
１．世話人は，地域ブロック内の正会員による互選によって決定する．
２．任期は2年とし，再任は妨げない．
３．任期内において世話人に異動ある場合は，その任期は前任者の残任期間とする．

第６条　（地域ブロック活動）

本会は地理的に近接した正会員によって構成する，地域ブロックを単位とし，日常の研究活動を行う．
地域ブロックは，北海道，東北・関東，東海，北陸，近畿，中国・四国，九州の 7 地域とする．

第7条　（世話人会）

本会には世話人会をおき，地域ブロック活動に基づく全体的な活動を円滑に推進するために必要な事項を審議決定する．世話人会は，会長，各地域ブロックの世話人並びに賛助会員で構成し，議長が招集する．

１．議長の互選．
２．地域ブロックの追加・変更に関する事項．
３．総会の企画と推進．
４．その他，全国に共通した，会の運営・会務の執行に関する事項．

第8条　（会長）

本会に，会長をおく．

１．会長は，世話人会の推薦をもって充てる．
２．任期は2年とし，再任は妨げない．

第9条　（総会）

総会は，本会の活動方針等，本会の活動に必要な事項を審議決定する．

１．総会は，世話人会の招集によって年1回開催する．
２．次の事項は総会に提出して，その承認を受けなければならない．
　(1) 会則の改訂
　(2) その他，世話人会において必要と認めた事項

第10条　（事務局）

本会の事務は，事務局において処理し，会務全般の事務を取り扱う．

１．本会の事務局は会員の所属する機関におく．
２．各地域内に地域ブロック事務局をおき，ブロック活動に関する事項を取り扱う．

第11条　（会計）

１．本会の経費は次の各号により支弁する．
　(1) 賛助会員からの賛助金
　(2) その他の収入
２．本会の会計年度は，毎年4月1日に始まり，翌年3月31日に終わる．

第12条　（その他）

本会の活動にあたっては，その詳細につき別に定めるものとし，必要に応じて会員相互の負担により実施する．

附則

この会則は，平成5年3月24日から施行する．

附則

この会則は，平成9年3月31日から施行する．

附則

この会則は，平成13年12月6日から施行する．

附則

この会則は，平成14年12月4日から施行する．

附則

この会則は，平成16年12月2日から施行する．

第7条 （地域ブロック活動）

本会は地理的に近接した正会員によって構成する，地域ブロックを単位とし，日常の研究活動を行う．

地域ブロックは，北海道，東北・関東，東海，北陸，近畿，中国・四国，九州の 7 地域とする．

附則

この会則は，平成24年4月1日から施行する．

第1条 （名称）

「国公立大学センター情報システム研究会」を「国公立大学情報システム研究会」に変更．

第2条 （目的）

大学センターを大学に変更．

第3条 （事業）

１項．情報システム及び情報サービス機能に関する開発・研究活動,および大学における情報システムの利活用に関する調査・研究活動．に変更．

附則

この会則は，平成26年3月7日から施行する．

第8条 （世話人会）

本会には世話人会をおき，地域ブロック活動に基づく全体的な活動を円滑に推進するために必要な事項を審議決定する．世話人会は，会長，各地域ブロックの世話人並びに賛助会員で構成し，議長が招集する．

１．議長の互選．

２．地域ブロックの追加・変更に関する事項．

３．総会の企画と推進．

４．その他，全国に共通した，会の運営・会務の執行に関する事項．

附則

この会則は，平成26年3月7日から施行する．

第9条 （会長）

本会に，会長をおく．

１．会長は，世話人会の推薦をもって充てる．

２．任期は2年とし，再任は妨げない．

附則

この会則は，平成21年12月3日から施行する．

（世話人の宿泊費、旅費、等）

世話人が IS 研の運営上必要に応じて行う世話人会，編集委員会，総会，等の活動にて発生する諸経費（交通費，宿泊費，等）については，世話人の所属する各機関の規定上の取扱いを十分確認の上，特に問題なき場合に限り，IS 研賛助会員企業による負担が可能とする．但し，負担できるのは，各世話人から事務局へ予めの要請があった場合によるものとする．

附則

この会則は，平成21年12月3日から施行する．

（総会，地域ブロック活動における懇親会費用について）

総会，及び各地域ブロック活動における懇親会（交流会等）の費用は，基本的に会費制，または，総会，当該ブロック活動の参加費用から充てるものとする．但し，IS 研賛助会員企業からも可能な範囲で補填する場合もあり得るものとする．

附則

この会則は，令和3年4月1日から施行する．

第５条（論文誌代金）を削除

正会員は,本会より配布される論文誌代金として年額 5,000 円を納入するものとする．ただし，本会の収入規模上，消費税納入を免除されている間は，消費税を請求・徴収しないものとする．

第１２条　（会計）

(1) 論文誌代金を削除

１．本会の経費は次の各号により支弁する．

(1) 論文誌代金

(2) 賛助会員からの賛助金

(3) その他の収入

２．本会の会計年度は，毎年４月１日に始まり，翌年３月３１日に終わる．

以　上

編集後記/Editor's Note

国公立大学情報システム研究会（IS 研）の論文誌「大学情報システム環境研究」第 26 号をお届けします。本号には 3 編の論文と 5 編の地域ブロックの活動報告を掲載しています。論文は，xR 技術の教育への応用に関する報告が 1 編，セキュリティ強化に関する報告が 2 編という内訳になっています。また，地域ブロックの報告には，情報基盤整備，DX 推進，新型コロナ対応，セキュリティ強化などに関する各大学の活動が報告されており，興味深い内容となっています。

2023 年 5 月 8 日に新型コロナウイルス感染症は 5 類感染症に移行しました。このことに象徴されるように，コロナ禍以前の生活が徐々に戻ってきています。当会の総会も 2020 年から 2022 年までの 3 年間はオンライン開催でしたが，2023 年 3 月 10 日の「第 31 回国公立大学情報システム研究会総会」は，対面とオンラインのハイブリッドで開催されました。運営の難しさがありましたが，参加しやすく有意義な総会でした。

この 3 年間，大学の情報部門は新型コロナ対応に追われ大変でしたが，オンライン授業や遠隔会議の普及，LMS の拡充，業務の電子化がこれまでにない速度で進みました。これからは，新型コロナ対応で導入したシステムの最適化，DX 推進，AI の活用，セキュリティ強化が各大学で進められていくと思われます。アフターコロナの時代に，これらに関する研究成果が多数発表されることを期待しています。

引き続き，本学会への投稿や参加のご協力をお願いいたします。

発行にあたりご協力頂きました皆様，特にご寄稿頂いた方々，査読・校正等に御尽力いただきました編集委員や査読委員の方々，ならびに研究会事務局の皆様に深く御礼申し上げます。

編集委員長
宮崎大学　廿日出 勇

会 員 所 属 機 関 一 覧

（順不同）

機　関　名		所　在　地	電話番号
帯広畜産大学	情報処理センター	〒080-8555　帯広市稲田町西2線11番地	0155-49-5701
釧路公立大学	事務局総務課総務担当	〒085-8585　釧路市芦野4-1-1	0154-37-3211
北見工業大学	情報処理センター	〒090-8507　北海道北見市公園町165番地	0157-26-9587
室蘭工業大学	情報教育センター	〒050-8585　室蘭市水元町27-1	0143-46-5900
山形大学	情報ネットワークセンター	〒990-8560　山形市小白川町1-4-12	023-628-4209
会津大学	情報センター	〒965-8580　会津若松市一箕町鶴賀上居合90	0242-37-2524
お茶の水女子大学	情報基盤センター	〒112-8610　文京区大塚2-1-1	03-5978-5885
一橋大学	情報基盤センター	〒186-8601　国立市中2-1	042-580-8440
横浜国立大学	国際戦略推進機構	〒240-8501　横浜市保土ヶ谷区常盤台79-1	045-339-4392
金沢大学	総合メディア基盤センター	〒920-1192　金沢市角間町	076-234-6911
北陸先端科学技術大学院大学	情報社会基盤研究センター	〒923-1292　能美市旭台1-1	0761-51-1300
福井大学	総合情報基盤センター	〒910-8507　福井市文京3-9-1	0776-27-8074
名古屋大学	情報基盤センター	〒464-8601　名古屋市千種区不老町	052-789-4346
愛知教育大学	ICT教育基盤センター	〒448-8542　刈谷市井ケ谷町広沢1	0566-26-2199
愛知県立大学	学術情報部図書情報課	〒480-1198　長久手市茨ケ廻間1522-3	0561-64-1111
岐阜大学	情報連携統括本部	〒501-1193　岐阜市柳戸1-1	058-293-2040
三重大学	総合情報処理センター	〒514-8507　津市栗真町屋町1577	059-231-9725
大阪教育大学	情報基盤センター	〒582-8582　柏原市旭ケ丘4-698-1	072-978-3824
大阪公立大学	情報基盤センター	〒599-8531　大阪府堺市中区学園町1-1	072-254-9154
兵庫県立大学	姫路工学キャンパス学術情報課	〒671-2280　姫路市書写2167	079-267-6906
島根大学	学術情報機構　総合情報処理センター	〒690-8504　松江市西川津町1060	0852-32-6091
徳島大学	情報センター	〒770-8506　徳島市南常三島町2-1	088-656-7555
香川大学	総合情報センター	〒760-8523　高松市幸町2－1	087-832-1292
九州大学	情報基盤研究開発センター	〒819-0395　福岡市西区元岡744	092-802-2613
九州工業大学	情報基盤センター	〒820-8502　飯塚市川津680-4	0948-29-7555
長崎大学	ICT基盤センター	〒852-8521　長崎市文教町1-14	095-819-2222
熊本大学	半導体・デジタル研究教育機構附属情報統括センター	〒860-8555　熊本市中央区黒髪2-39-1	096-342-2111
大分大学	学術情報拠点情報基盤センター	〒870-1192　大分市旦野原700	097-554-7985
宮崎大学	情報基盤センター	〒889-2192　宮崎市学園木花台西1-1	0985-58-7816
鹿児島大学	学術情報基盤センター	〒890-0065　鹿児島市郡元1-21-35	099-285-7474
鹿屋体育大学	スポーツ情報センター	〒891-2393　鹿屋市白水町1	0994-46-4917

※ 機関名は，「＊＊大学法人」を省略しております．(2023年9月時点)

※ 住所、電話番号に修正、変更等ございましたら事務局(fj-isken-bureau@dl.jp.fujitsu.com)までご連絡ください．

国公立大学情報システム研究会　事務局

〒105-7123 東京都港区東新橋１－５－２
（汐留シティセンター）

E-mail ： fj-isken-bureau@dl.jp.fujitsu.com
URL　　： https://csis.ufinity.jp/isken/