宮崎大学新キャンパス情報システムの構築

Construction of New Campus System at University of Miyazaki

青木　謙二,　園田　誠,　黒木　亘,　川畑　圭一郎

Kenji AOKI, Makoto SONODA, Wataru KUROGI and Keiichirou KAWABATA

宮崎大学

University of Miyazaki

宮崎大学では，本学における教育・研究・業務の基盤として運用しているキャンパス情報システムの更新を行い，2019 年 4 月から新システムの運用を開始した．新キャンパス情報システムは，情報基盤システム，教育研究業務支援システム，情報ネットワークシステムから構成される．今回のシステム更新では特にクラウドサービスの利用および情報セキュリティ対策の強化を重視してシステムを構成した．本論文では，新システムを構築するにあたって旧システムとの違いや情報セキュリティ対策の強化のために導入したシステムについて報告する．

キーワード：情報システム，セキュリティ，ネットワーク，サーバ

University of Miyazaki has updated its campus information system, which is used as an infrastructure for education, research, and works at the university, and started operating the new system in April 2019. The new campus information system consists of an information infrastructure system, an education, research and work support system, and an information network system. In this system update, the system configuration was made with particular emphasis on using cloud services and strengthening information security. In this paper, we report the differences between the new system and the old system, and the systems introduced for information security measures.

Keywords: Information system, security, network, server

1. はじめに

宮崎大学では大学を取り巻く社会環境の変化や ICT 技術の進歩に対応した教育・研究・業務を支える ICT 基盤を構築するために, 4 年ごとにキャンパス情報システムの更新を行ってきた. 現在の大学を取り巻く環境に目をやると，ICT 技術の発展と普及が進み，インターネットの利用が非常に身近で便利になった一方，ネット利用犯罪や標的型サイバー攻撃など ICT 技術を利用した脅威もまた身近になってきている．特に，特定の組織を狙った標的型サイバー攻撃が急増しており, 今後もますます増加することが予想され, これまでの対策では防ぐことができない状況になりつつある. 多くの個人情報や研究情報を保有する大学は恰好のターゲットである．また，これらの攻撃によって情報が漏えいした場合に組織に向けられる社会の目は厳しく, このような事態が生じた場合は，大学としての信用を失ってしまう．この

情報基盤センター
〒889-2192　宮崎市学園木花台西 1-1
Information Technology Center
〒889-2192 1-1, Gakuenkibanadai-nishi, Miyazaki, JAPAN
E-mail：aoki@cc.miyazaki-u.ac.jp

ような状況のなか，重要な情報を守るために，また，大学が世間からの信頼を失わないためにも，万全な情報セキュリティ対策が必要である．そこで，2019 年度のキャンパス情報システムの更新に当たっては，セキュアなシステムを構築することを最も重要な目的として，システム更新を行った．本論文では，新システムを構築するにあたって旧システムの課題や新システムの構成，情報セキュリティ対策について報告する．

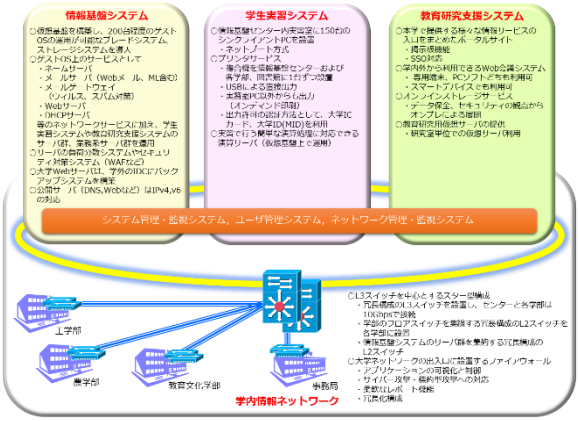


図 1　旧システム概要

2.　旧システム

2.1.　満足度調査

旧システムのシステム構成を図 1 に示す．旧システムの構成は情報基盤システム，学生演習システム，教育研究支援システム，情報ネットワークシステムからなる．また，各システムのログを収集し管理・監視するシステムがすべてのシステム横断的に存在する．

新キャンパス情報システムの仕様策定にあたっては，利用者に旧システムの満足度についてアンケート調査を行い，結果を参考にした．アンケートは，教職員および学生を対象とし，有線・無線ネットワーク，メール，プリンタ，仮想サーバ，ホスティングサービス，オンラインストレージ，ウイルス対策ソフトについて利用状況と満足度をたずねた．教職員 270 名，学生 148 名より回答を得た．満足度調査の結果を図 2 に示す．満足度調査では，回答選択肢を「満足」，「普通」，「不満」とした．図 2 の結果より，すべての調査項目に対して満足と普通を合わせると 8 割以上を占めており，全体的に満足度は高いことがわかった．ただし，無線ネットワークについては，満足 23%，普通 57%，不満 20%となり，他のサービスと比較し，満足度が低く不満度が高い結果となった．このことについて，無線ネットワークの速度・同時接続性などの性能についてたずねたところ，満足 19%，普通 57%，不満 25%であるあった．この結果と自由記述の回答から，同時接続性の問題が無線ネットワーク対する満足度を下げていると考えられた．また，オンラインストレージの保存容量が不足していることがうかがえた．

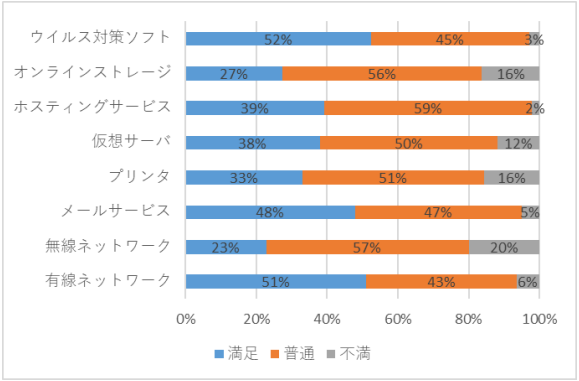


図 2　旧システムの満足度調査

2.2.　課題と検討

新システムを考える上では，満足度調査のアンケート結果および以下のような状況や課題を考慮し構成を検討した．

学生演習システムにおいては、実習用 PC とプリンタが課題となっていた。本学では，平成 22 年度より学生の PC 必携化を行っており，授業等は学生個人の PC を使って行うことが多くなっていたが，実習用 PC が残っており，利用率が低く，廃止することを検討した．また，プリンタは，情報基盤センターと図書館，各学部に 1 台ずつ設置していたが利用率が低く，廃止すること検討した．しかし，必要性を主張する教員が一定数いたため数量を減らして存続

することとした.

情報基盤システムでは, メールシステムについて検討した. 旧システムではオンプレミスで運用しており, サーバライセンスのコストやスパムやウイルス対策のコストなど管理コストがかかっていた. このため, SaaS のクラウドサービスを利用することを検討した. 教職員については, 学外へ情報を置くことに抵抗があったためオンプレミスでの運用とし, 学生については機密情報を扱うことがほとんどないこと, また, アンケート調査で反対意見がなかったことから, クラウドサービスを利用することとした.

旧システム全体に対して, セキュリティの強化は喫緊の課題であった. セキュリティでは, ネットワークでのセキュリティとエンドポイントでのセキュリティを考える必要があるが, ネットワークでは, これまでシグネチャ型のファイアウォールのみであったため, 未知のマルウェアに対応することができなかった. そこでサンドボックス型のファイアウォールの導入と Web サーバへ host 型の WAF（Web Application Firewall）を導入することを検討した. エンドポイントでのセキュリティ対策は, これまでもウイルス対策ソフトを大学で包括的に契約し, 教職員, 学生へ配布, インストールさせていたが, これだけでは対応できない高度なサイバー攻撃に対応するため, EDR（Endpoint Detection & Response）の導入を検討した.

旧システム外の業務システムについても検討した. 学内には Oracle データベースを使用したシステムがいくつか存在していたが, 各システムで Oracle データベースを調達し, それぞれサーバを立てており, 導入コスト, 保守コストが全学的に高額になっていた. そこで, 統一した Oracle データベースサーバを構築し, これを各システムから使用することを検討した.

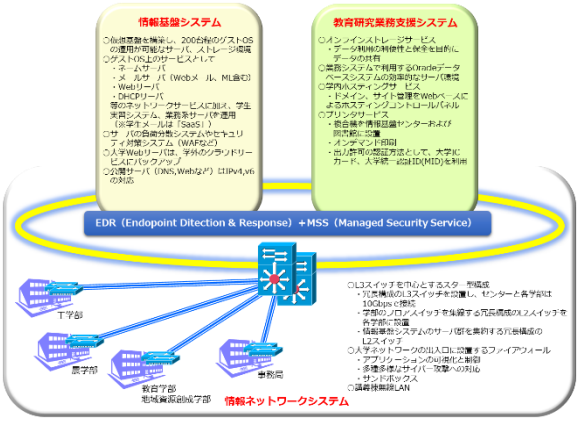


図 3　新システム概要

3. 新システムの構築

3.1. システム構成

以上の満足度調査および検討事項を踏まえ構築した新システムの構成を図 3 に示す. 新キャンパス情報システムは, 情報基盤システム, 教育研究業務支援システム, 情報ネットワークシステムで構成される. 情報基盤システムは主に仮想サーバ基盤, 教育研究業務支援システムは Oracle サーバ, 情報ネットワークシステムはネットワークスイッチが含まれる. また, これらのセキュリティを確保するために EDR および MSS（Managed Security Service）を導入した.

新システムの仕様策定にあたっては, クラウドサービスの利用およびセキュリティの強化を柱とし機器の性能機能および構成を検討した. また, 費用の削減と予算の確保を目的に, これまで 4 年間のリース期間を 5 年間に延ばした. これにより, 全体で使用できる予算がこれまでより多く確保することができた. また, 次回の更新では, 現在は調達が異なる事務情報システムおよび清武キャンパス（医学部キャンパス）情報システムについても統一して調達するために, リース期間が合うように期間を変更した.

調達に係る日程は以下のとおりである.

- 2018 年 2 月　情報システムに関する利用者アンケート

- 2018 年 3 月　資料提供招請
- 2018 年 4 月　仕様策定委委員会設置
- 2018 年 6 月　仕様書案策定
- 2018 年 8 月　仕様書策定
- 2018 年 10 月 開札
- 2019 年 4 月　本稼働開始

また，これとは別に追加調達として 2019 年度に多要素認証システム，サーバメモリの増強およびストレージ容量の増強を行った．

3.2. 情報ネットワークシステム

情報ネットワークシステムの構成を図 4 に示す．情報ネットワークシステムの基本的な構成は旧システムと同様であり，L3 スイッチを中心とするスター型構成である．図 4 の赤字で示した外部接続 FW（Fire Wall），コアスイッチ（L3 スイッチ），学部集線スイッチ（L2 スイッチ），講義棟無線 AP（Access Point），サーバエリア FW，サーバエリア集線スイッチ，事務エリア FW が新システムにおいて更新された機器である．黒字で示したものは既存の機器であり，既存機器と更新機器との不整合が起こらないように機器構成を考慮した．

外部接続 FW，コアスイッチ，学部集線スイッチ，サーバエリア FW，サーバエリア集線スイッチはそれぞれ 2 台で冗長構成になっている．また，本学は医学部がある清武キャンパスと外部接続回線を冗長化しており，一方のキャンパスの外部接続回線が途絶した場合に，もう一方のキャンパスの外部接続回線に迂回して接続する構成としているが，システム更新においてもこの構成を継続した．

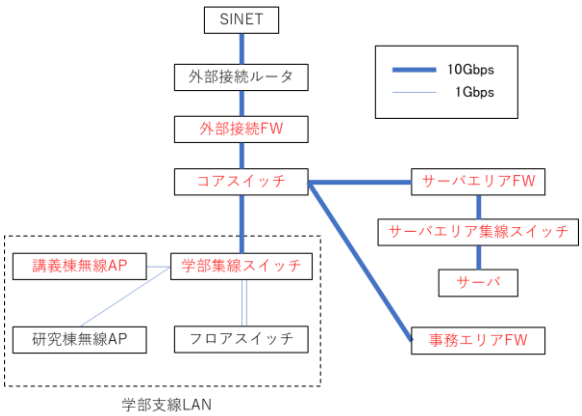


図 4　ネットワーク構成

幹線およびサーバエリアは 10Gbps 接続，支線は 1Gbps 接続である．スイッチ類は旧システムでは Cisco 社製であったが，新システムでは ALAXALA 社製を採用した．また，講義棟無線 AP は Cisco 社製から Aruba 社製に変更した．これにより，価格を抑えることができた．旧システムと比較し，機能や設定の違いはあるものの性能的には向上した．外部接続 FW のセキュリティ機能としては，アプリケーション制御，アンチスパム，アンチウイルス，IPS を持つが，特に旧システムでは備えていなかったサンドボックス機能を備えている．これにより，シグネチャ型の FW では防ぐことのできなかったマルウェアを防ぐことができる．

3.3. 情報基盤システム

サーバシステムは，200 台程度の仮想サーバをゲスト OS で運用できるものとした．表 1 に旧システムと新システムのサーバ基盤構成を比較した．旧システムでは省スペース，省電力，高性能を目指しブレードサーバを導入したが，現在では 1 台でより高性能かつ安価なサーバが登場していることからラックマウント型の IA サーバを導入した．また，サーバ台数も 16 台（ブレード）から 5 台に削減することができた．

データストレージは，年々仮想サーバの数やユーザのデータ保存容量が増えていることから一人当たりの保存容量を増やす必要があり，全体容量を 80TB から 120TB に増やした．

表 1　新旧サーバ構成

	旧	新
仮想サーバ基盤	VMware vSphere 5.5 ブレードサーバ 16ブレード	VMware vSphere 6.5 ラックマウントサーバ 5台＋3台（Oracle用）
ストレージ	80TB	120TB
WAF	ハード	ソフト
遠隔バックアップ	IDC にハウジング	クラウドサービス

Web サーバには WAF を導入した. 旧システムではアプライアンス型の WAF を導入していたが，新システムではソフトウェアによる host 型の WAF をそれぞれの Web サーバに導入した. データのバックアップは，旧システムではデータセンタにストレージをホスティングしてバックアップを取っていたが, 新システムではクラウドサービスのストレージを使用してバックアップを取る仕組みとした.

教職員用メールについては旧システムと同様にオンプレミスでサーバを構築し, メールソフトとしてクオリティア社の DEEP Mail を採用した．スパムメール対策には，ファイア・アイ社の FireEye ETP を用いた．これはクラウドサービスでスパムメールを検証し，検知，排除するシステムである．また, 外部接続 FW によってもスパムメール対策を行った. メールの保存容量は 50GB と大幅に増やし，一般的なフリーメールの保存容量に比べ遜色のないようにした．学生用メールは，オンプレミスでの運用をやめ, クラウドサービスであるマイクロソフト社の Office365 のメール機能のみを使用することとした. スパムメール対策およびウイルス対策は Office365 が提供するものを使用している．メールの保存容量は 50GB である.

3.4. 教育研究業務支援システム

オンラインストレージは North Grid 社の Proself をオンプレミスで構築した．ただし，情報漏えい防止のためにアクセスは学内限定とし，教職員および学生全員に提供した. 利用者個々の保存容量は 5GB から 50GB へ増量した.

実習用 PC は廃止したが，図書館に共用 PC が 20 台程度設置してあり，これを管理運用するためにネットブートシステムであるソフトオンネット社の Z!BootOS を継続して導入した.

プリントサービスは, プリンタを 5 台から 2 台に削減し，京セラ社の ECOSYS P8060cdn を導入した．旧システムでは，利用率が低く，また複合機としての利用が少なかったため, 台数を削減し, 複合機から印刷単機能のプリンタに変更した. また，旧システムではドライバを利用者に提供し, 利用者が PC にインストールしてソフトウェアから直接プリントジョブを投入する方式であったが, 新システムでは印刷したいファイルを Web でアップロードする方式に変更した.

Oracle データベース専用のサーバ群を 3 台の IA サーバで構築した. Oracle データベースを仮想サーバ基盤で使用する場合, 全ての物理サーバ台数分のライセンスが必要となるため，一般の仮想サーバ基盤とは分離して Oracle データベースを使用するサーバのみを集約した. これによりライセンス料を節約することができた.

3.5. 情報セキュリティ対策

情報セキュリティ対策としてこれまで同様に ESET 社のウイルス対策ソフト Endpoint Antivirus Ver.6 を Windows，Mac，Linux へ提供できるようにした．これは，教職員および学生の個人所有の端末にも使用できる．また，ウイルス対策ソフトでは対応できない攻撃に対応するために EDR を導入した．認証においては, パスワード流失などによるリスト攻撃の被害が後を絶たず, パスワードのみの一要素認証ではもはや安全でないことが言われている. そこで, 多要素による認証を実現するための多要素認証システムを導入した．EDR と多要素認証を全学的に導入した事例はまだ少ない.

3.5.1. EDR

近年, シグネチャ型のウイルス対策ソフトでは猛威を振るうランサムウェアやマルウェアに対応できなくなっていることから，EDR が注目されている．EDR とは，Endpoint Detection & Response のことである．これま

で PC やサーバなどのエンドポイントを保護する有効な方法はウイルス対策ソフトを導入することであったが，サイバー攻撃の脅威がますます高度なものになり，シグネチャ型のウイルス対策ソフトではこれらを検知，阻止することができなくなってきている．これに対して，EDR は，エンドポイントを包括的に監視し，悪意のある異常な挙動を検出することができる．また，エンドポイントの活動を継続的に監視および分析することにより，攻撃活動の内容と範囲を特定し，フォレンジック調査に活用することができる．

アメリカ国立標準技術研究所（NIST）のサイバーセキュリティフレームワークや経済産業省のサイバーセキュリティ経営ガイドラインでは，防御（Protect）だけでなく，侵入を検知（Detect）し，対応（Respond）し，速やかに復旧（Recover）させることの重要性が指摘されている．また，内閣サイバーセキュリティセンター（NISC）の「政府機関等の対策基準策定のためのガイドライン(平成 30 年度版)」でも未知の不正プログラムの検知およびその実行の防止の機能を有するソフトウェア，つまり EDR の導入と活用を示している．

EDR として，サイバーリーズン社の Cybereason EDR を導入した．これは Windows, Mac, Linux の OS に対応している．Cybereason EDR は，エンドポイントの膨大なログデータを，AI を活用して解析することで，サイバー攻撃の兆候をリアルタイムに検知し，防御することができる．また，監視サービスとして MMS（Managed Security Service）を提供する．

EDR は PC またはサーバの管理者が自らインストールしてもう必要がある．本学の方針として，機密性 3 の情報を扱う教職員 の PC へのインストールを義務化し，情報基盤センターの Web ページからダウンロードしてインストールすることとした．ただし，総ライセンス数が限られるため PC は原則一人 1 台とした．また，サーバはすべてインストールすることとした．また，事務職員が使用する PC へはすべてインストールした．図 5 に EDR の構成の概要を示した．PC やサーバにインストールされた EDR は各機器の状態を監視しており，その状況をクラウド上にある管理サーバへ送信する．学内の管理者は管理サーバへアクセスすることにより学内の端末の状況を確認することができる．また，監視サービス（MSS）も利用しており，MSS は管理サーバを監視し，異常を検知した場合は分析者が確認をしたうえで即座に管理者に通知する．また，1 か月に一回月次レポートの提出と説明が行われる．

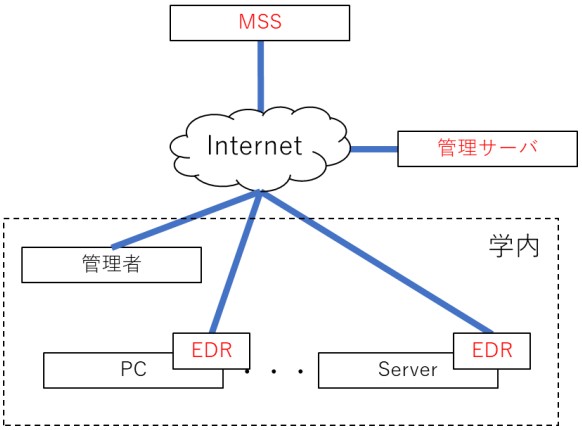


図 5　EDR 構成

本システムでは，EDR を 2,000 ライセンス契約しており，そのうち 1,200 ライセンス程度が使用されている．全学的には推計で 3000 台程度 PC やサーバがあることから，約半数程度で利用されている．

3.5.2. 多要素認証

多要素認証（MFA）には，ウォッチガード社の AuthPoint を導入した．MFA を導入することにより，パスワードの紛失や盗難に起因するネットワークの遮断や情報漏えいのリスクを削減することができる．また，本システムはクラウドサービスであるため，容易なセットアップと運用管理を行うことができる．また，今回導入した製品は，ネットワーク，VPN，およびクラウドアプリケーションへのアクセスを一

つのインターフェースで認証することができる特徴を持っている. 利用者の身元を証明する認証要素としてプッシュメッセージ，QR コード，ワンタイムパスワード（OTP）が使用可能である. システムとアプリケーションへのアクセスを許可する際には, モバイルデバイス固有情報が許可された利用者のスマートフォンと一致する必要があり, 攻撃者がシステムに侵入するために, 利用者のデバイスをクローン化してもデバイス固有情報が異なるため, 認証はブロックされる仕組みとなっている.

利用者は自分のスマートフォンを使用して認証を受けることができる. 利用者は，専用のアプリを利用者個人のスマートフォンにインストールし, このアプリを使用してスマートフォンを認証用デバイスとして登録する. 認証の際には, プッシュベースの認証やスマートフォンのカメラによるオフラインでの QR コード認証などが可能である. 本学ではプッシュベースの認証を採用した.

本システムでは, 学外から学内のネットワークに接続するための SSL-VPN 接続において認証時に多要素認証を実施することとし, システムを構築した．図 6 に MFA の構成の概要を示す. ユーザが学内サービスを利用する際に, まず SSL-VPN サーバへアクセスし, 大学統一 ID で認証する．この認証に通ると MAF により, 当該ユーザのスマートフォンアプリへプッシュ通知が届き, 確認ボタンを押すことにより

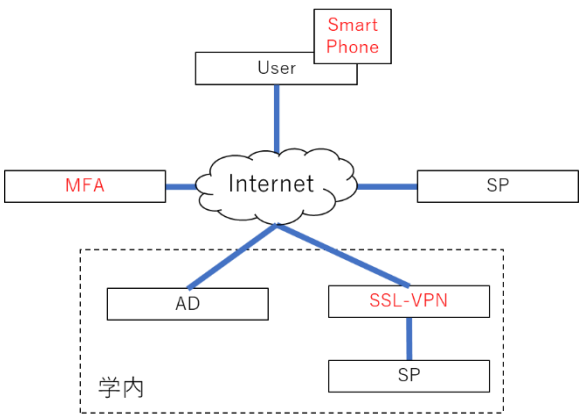


図 6　MFA 構成

認証にパスし，VPN 接続され学内のサービスを利用できるようになる．MFA と学内の AD サーバは定期的に同期を行い，MFA は最新のユーザ情報を保持している.

現在は SSL-VPN の認証にのみ使用しているが, 将来的には本学がオンプレミスおよびクラウドサービスで提供するすべてのサービスについて本多要素認証により認証を行う予定である．SaaS のクラウドサービスでは多要素認証を提供しているものもあるが, サービスごとに異なる認証では利用者も管理者にも負担がかかるため, 様々なサービスに対応できる本多要素認証システムは利便性が高い.

4.　運用状況

本システムは，2019 年 4 月より本運用を行っており, 基本的にはトラブルなく稼働している．ただし，いつくかの問題があり改善を図る必要がある.

教職員用のメールシステムについてはスパム判定が強力すぎ, メールが届かない場合が旧システムに比べ多い. いくつかのブラックリストを参照しているため, 何らかの原因で送信元のサーバが一つでもブラックリストに掲載されると即座にスパム判定され遮断される. 回復には送信元の問題が解決し, ブラックリストからの削除が行われない限り届かないため, 回復に非常に時間がかかる．また，学生用メールシステムでは, クラウドサービスの障害によりメール配送が遅延することが起こった. クラウドサービスであるため, 本学からは手の打ちようがない. 詳細な状況を把握することができないため, 利用者の問い合せにも回答することができない.

プリンタシステムでは動作が不安定なことがある．PDF ファイルをプリンタサーバへアップロードした際にファイルが破損し, 正常に印刷できないことがあり, 不明な文書が数十枚も印刷されたことがあった.

遠隔バックアップでは, 性能が十分でなく一

日に 40TB 程度しかバックアップでず, 初期バックアップに非常に長い時間を要した．また, リストアについても自由に行えない問題もある. これまでのストレージのホスティングによるバックアップに比べると自由度が制限され非常に不便である.

Oracle データベース用のサーバ群のストレージやメモリの性能が想定していたよりも不足しており, 十分でなかったため追加調達で補強した.

満足度調査で不満の多かった無線ネットワークは, 授業での一斉使用においても問題は報告されておらず, 改善が図られたものと考えられる.

5. おわりに

本論文では，宮崎大学が 2019 年 4 月より運用を開始している新キャンパス情報システムの構成について報告した. 本システムは，情報基盤システム，教育研究業務支援システム，情報ネットワークシステムから構成され, 特にクラウドサービスの利用および情報セキュリティ対策の強化を重視して構成されたシステムとなった. 来年度は本システムの満足度について利用者にアンケート調査を行い, システムの評価を行っていく予定である.

参考文献

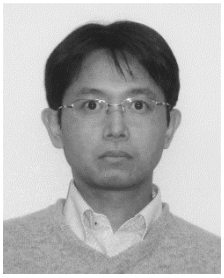
(1) 林 治尚，島 信幸, 井内 善臣，畑 豊，太田 勲 : 兵庫県立大学の情報新システム（第 III 期）の設計と構築, 大学情報システム環境研究，Vol.18，pp.51-62，(2015).

(2) 青木　謙二，園田　誠，黒木　亘 : 大規模災害に備えたキャンパス情報ネットワークの構築, 大学情報システム環境研究, Vol.18, pp.43-50，(2015).

(3) 内閣サイバーセキュリティセンター，政府機関等の対策基準策定のためのガイドライン（平成 30 年度版），https://www.nisc.go.jp/active/general/pdf/guide30.pdf，(2018)

(4) Anton Chuvakin, Named: Endpoint Threat Detection & Response, Gartner Blog Network, https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/, (2013)

著者略歴



青木　謙二　2002 年　鹿児島大・工学部・教務職員, 2003 年　鹿児島大・学術情報基盤センター・助手, 2007 年 同・助教, 2009 年 宮崎大・情報戦略室・講師, 2010 年　同大・情報基盤センター・准教授, 専門は情報科学, システム開発, 博士（工学）.

園田　誠　1993 年 宮崎大学・情報処理センター・技術職員，2003 年 同大・総合情報処理センター・技術職員，2007 年 同大・情報支援センター・技術職員，2010 年 同大・情報基盤センター・技術専門職員.

黒木　亘　2006 年 宮崎大学・情報広報係・事務職員, 2008 年 同大・総合情報処理センター・事務職員，2008 年 同大・情報支援センター・事務職員，2013 年 同大・情報基盤センター・技術職，2017 年　同大・情報基盤センター・技術専門職員.

川畑　圭一郎　2013 年 宮崎大学・情報基盤センター・技術職員.

(2020年2月21日原稿受付)
(2020年4月24日採録決定)