Vol.2019-IOT-47 No.2
Vol.2019-SPT-35 No.2
2019/9/19

兵庫県立大学の情報新システム（第IV期）におけるネットワークの再設計と構築

林 治尚[1,a)]　新居 学[1,2]　島 信幸[1]

概要：県内に多数のキャンパスを有する兵庫県立大学では，教育・研究のインフラとして全学統一的に導入している各種情報システムのリプレイスを行い，2019 年春から新システム（第 IV 期）の運用を開始した．これに併せ，キャンパス毎に FW やセキュリティ機器等を配置する従来のネットワーク形状から，データセンターに設置し集中管理する形へと再設計した．本稿では，この新システムでのネットワークの再設計と構築などに関して報告する．

Network redesign and construction for New Information Systems (phase IV) in University of Hyogo.

Abstract: University of Hyogo has a large number of campuses in Hyogo prefecture. We planned to replace some information systems (such as network system and information processing education system) as the infrastructure of academic and research activities for our University. These operations (IVth period systems) have been started in March 2019. At this replace, we reconstructed the network system which arranged FW and security devices at every campus to concentrate these types of equipment at the datacenter. In this paper, we report our design, construction, and system migration of new systems.

1. はじめに

2004 年 4 月に兵庫県立大学は，当時の神戸商科大学，姫路工業大学，県立看護大学の県立 3 大学を母体として，大学本部などを新たに設け発足した．県内に分散する拠点を，教育・研究・大学運営のインフラとしてネットワークシステムで結び，その上に情報処理教育システムや学生情報システムなど，各種の大学情報システムを全学統一的に導入し，運用を行っている．

教育・研究用のシステムのみならず，職員用の事務システムなど大学運営用も含めて，リース期間の異なる多数の情報関連システムを導入しているが，主要システムは大別して，開学からの第 I 期システム（2004 年春運用開始），第 II 期システム（2009 年春運用開始），第 III 期システム（2014 年春運用開始）と続き，2019 年春に新システムへの移行期を迎えた．

本稿では，第 IV 期となる新システムについて，ネットワークの再設計や構築，移行作業などに関して報告する．

2. 情報関連システムの改編

2.1 兵庫県立大学の概要

本学は，8 学部 14 研究科の総合大学であり，教職員と学生などを合わせると 7500 人程度である（2019 年 4 月現在）．拠点としては，旧大学の拠点などに加えて，新設や移転もあり，現在では県内に 15 箇所以上を有する．

- 神戸商科（“学園都市”，神戸市西区）
- 姫路工学（“書写”，姫路市書写）
- 播磨理学（“光都”，赤穂郡上郡町）
- 姫路環境人間（“新在家”，姫路市新在家）
- 明石看護（“明石”，明石市北王子町）
- 神戸情報科学（“ポートアイランド”，神戸市中央区）
- 淡路緑景観（“淡路”，淡路市）
- 豊岡ジオ・コウノトリ（“豊岡”，豊岡市）
- 神戸防災（“HAT 神戸”，神戸市中央区）

の 9 キャンパスを中心に，政策科学研究所（神戸市西区），

[1] 兵庫県立大学学術総合情報センター
Library and Information Center, University of Hyogo, 2167 Shosha, Himeji, Hyogo 671-2280, Japan
[2] 兵庫県立大学工学研究科
[a)] hayashi@laic.u-hyogo.ac.jp

Vol.2019-IOT-47 No.2
Vol.2019-SPT-35 No.2
2019/9/19

図 1 兵庫県立大学 拠点図（2019 年 4 月現在）

高度産業科学技術研究所（赤穂郡上郡町），自然・環境科学研究所（三田市・淡路市・豊岡市・佐用町・丹波市），地域ケア開発研究所（明石市）の附属研究所などから構成される (図 1)．この他さらに附属高等学校・附属中学校（赤穂郡上郡町），産学連携・研究推進機構（姫路市）などの関連組織もある．

各拠点の規模は様々であるが，キャンパス別の学生数としては，総学生数に対しおおよそ，神戸商科 C と姫路工学 C でそれぞれ 30%ずつを，播磨理学 C と姫路環境人間 C でそれぞれ 15%ずつを占めている．

2.2 情報関連システムの状況

このように県内に広く点在しているため，拠点間の通信基盤をどう確保するかが開学にあたり課題となった．これには，兵庫県が県域の基幹的な情報基盤として 2002 年から運用を開始した “兵庫情報ハイウェイ”（以下，HJHW）[1], [2] の民間開放系を用いることで対処している．

本学の “ネットワークシステム” は，L2/L3 スイッチとファイアウォール（FW）やセキュリティ機器などで構成される．その上に，目的やセキュリティポリシー別に多くの VLAN を設定して，全学統合認証を中心とした，各種サーバとクライアント PC などの情報機器とその利用環境統合システムである “情報処理教育システム”，学務・教務システムである “学生情報システム”，各拠点での授業・講演を双方向配信するための “遠隔授業システム” など，教育・研究のインフラとなる各種システム [3], [4], [5], [6] と，さらに “財務会計”，“旅費”，“人事給与” などの業務サーバを中心とし，グループウェアや IT 資産管理を含む，主に職員用の “事務系情報基盤システム”[7] などを全学統一的に導入し，大学として運用している (表 1)．

3. 新ネットワークの設計と構築

2004 年の開学以来，これらの主要システムはリース契約で，基本的に 5 年単位で更新しており，今回，第 IV 期となる新システムを 2019 年春に導入することとなった．

3.1 リプレイス方針

2017 年春，学術総合情報センター運営委員会にて全学ワーキンググループを組織し，ここで “情報処理教育システム” と “ネットワークシステム”のリプレイス方針を検討し，県への予算要求と仕様策定を行った．

新システムでは，従来通りの各種サービスを維持しつつ，学内で希望の多い各種サービスの拡充と利用環境の向上をまずは目指した．サーバ仮想化による集約，IC カード学生証によるオンデマンドプリント，学生の利便性向上のための全学無線 LAN システムの設置，拠点間回線の増強，サンドボックスによるセキュリティ強化など，いくつかの新項目について予算の増額要求を行った．このうち，無線 LAN とサンドボックスについては緊急性などを鑑みて別枠として認められたものの，他は認められず，リプレイス予算としてはほぼ前回通りとなった．

しかしながら前回と比べ，特に各種ライセンス費用などが大幅に値上がりしたため，第 IV 期システムとしては，基本的構成などは第 III 期までと同様とするが，各拠点での利用状況などを含めて再度検討した．またこれまでと同様に “費用と手間のかからない” システムを目指し，ユーザに対しては，出来る限り移行を意識させることないように，リプレイスを行うこととした．

予算確保，仕様検討・策定などの作業を経て，2018 年初夏に一般競争入札を行った．情報処理教育システムは富士通 (株)，ネットワークシステムは NTT 西日本 (株) が落札し，同年秋から構築・導入，2019 年 3 月 1 日に新システムの稼働を開始した．

3.2 ネットワーク設計

本学のネットワークは，拠点間および SINET との出入口への経路などの通信基盤として，HJHW を利用している．ここに本学側で用意した情報処理教育システム用，学生情報システム用，図書システム用，遠隔授業システム用，事務システム用など，利用目的別・セキュリティポリシー別の VLAN を各拠点出入口のスイッチにて束ね，HJHW を通して拠点間を結ぶ構成としている．但し，HJHW の民間開放系では利用可能帯域が無制限ではないため，例えば本学としてデータセンター（DC）を設置し，ファイルサーバなどを含む全サーバをそこに集約する，という設計はこれまで見送ってきた．全学統合認証を用いて，各種サービスも基本的には全学から利用できる形としているものの，

表 1　主な情報関連システム（第 I 期～第 IV 期）の契約業者

システム名	第 I 期	第 II 期	第 III 期	第 IV 期
ネットワークシステム	NTT 西日本 (株)	NTT 西日本 (株)	NTT 西日本 (株)	NTT 西日本 (株)
情報処理教育システム	富士通 (株)	富士通 (株)	富士通 (株)	富士通 (株)
学生情報システム	東芝 (株)	NTT 西日本 (株)	NTT 西日本 (株)	（入札公示中）
遠隔授業システム	富士通 (株)	NTT 西日本 (株)	(株) 教映社	（更改予定）
図書システム	(株) リコー	(株) リコー	(株) リコー	（更改予定）
事務系システム	（県有システムを利用）	（県有システムを利用）	NTT 西日本 (株) 他	NTT 西日本 (株) 他

（リース開始年月の違いやリース延長などもあるため，それぞれ多少のずれがある）

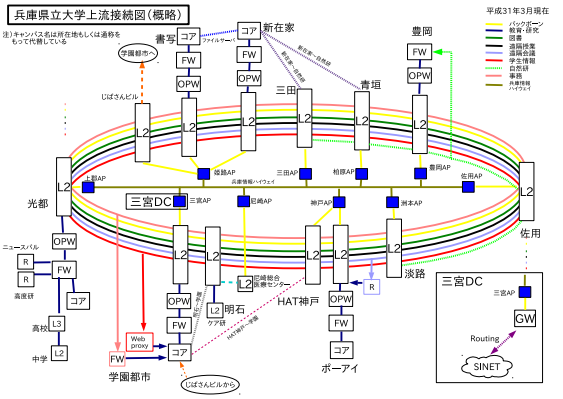

図 2　兵庫県立大学ネットワーク接続概念図（2019 年 3 月まで）

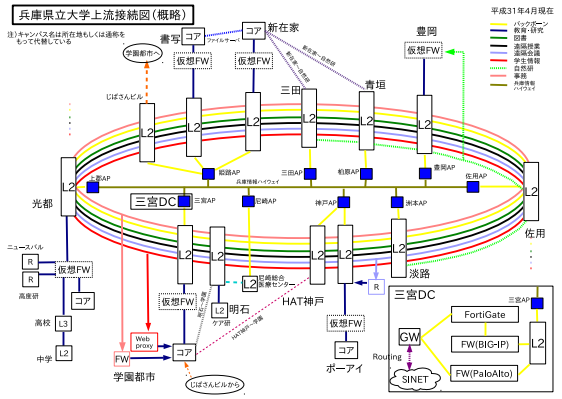

図 3　兵庫県立大学ネットワーク接続概念図（2019 年 4 月時点）

各キャンパスでの利用ポリシーの細かな差異があったり，拠点別での障害などができる限り相互に影響を及ぼさないようにするため，それぞれのキャンパスに FW や UTM などのセキュリティ機器も配置したある種の “半独立型” となっていた．

今回のリプレイスでは，各拠点内は従来通り，L3 のキャンパスコアスイッチなどを中心とし，タグ VLAN 対応の L2 スイッチを用いて，必要とする場所に必要となる VLAN を用意できる形とした．その一方，各拠点分の FW とセキュリティ機器を一ヶ所に集約する方針とした．

HJHW は県内に閉じたループ構造となっているため，本学では，SINET のノードと最寄りの HJHW のアクセスポイント（以下 AP）を繋ぎ，インターネットとの接続点としている．繋ぎ先の AP は，ノードの統廃合などにより随時変更してきた．今回のリプレイス前までには，ノードと AP 間の DC に，大学全体としての GW 用スイッチを設置していた (図 2)．

今回，今後の拠点間回線の増強を視野に入れ，機器費用面や特に管理運用面なども考慮し，DC への全学サーバ群の統合への第一歩として，各拠点に設置していた FW とセキュリティ機器をそれぞれ統合し，DC に設置することとした．

3.3　機器の選定

これまで導入していた FW とセキュリティ機器は，拠点の規模や方向性などにより，Fotinet 社の UTM アプライアンス FortiGate であったり，McAfee 社の Firewall Enterprise （旧 Sidewinder）などを設置していた拠点もあったが，基本的には，FW 機（UNIX マシンで iptables ベースでの制御）と，セキュリティ機器として，検疫用の TREND-MICRO 社 InterScan Web Security/ Messaging Security と，NetAgent 社の特定通信型 FW である OnePointWall を設置していた．

これら従来型の FW とセキュリティ機器では，昨今の攻撃の高度化・巧妙化への細かな対応が困難であり，加えて後継機の販売終了などもあって，特に機器管理面でも考慮し，今回，次世代型 FW などを導入し DC に集約配置することとした．

そこで学内外との通信を 2 つに大別して機器を検討した．従来の FW に相当し，基本的に学内から学外へのアクセスを中心にコントロールするための “アウトバウンド”FW となる機器と，そして対外 Web やメール，DNS など基本的に学外からアクセスされる各種サービスをコントロールするための “インバウンド”FW となる機器を，それぞれ導入することとした．

前者には，パロアルトネットワークス社の次世代型 FW（NGF）である PaloAlto を選択した [8]．PA-5220 を 1 台，DC に設置し，仮想ファイアウォールインスタンス（VSYS）で，それぞれのキャンパス分の FW を構築することとした．

後者には，大学としての学外への各種サービスを，様々な脅威から防御するために，F5 ネットワークス社のアプリケーションデリバリコントローラ（ADC）である BIG-IP を

選択した [9]．i4600 を 1 台，DC に設置した．DoS/DDoS 攻撃から防御するファイアウォールである BIG-IP AFM（Advanced Firewall Manager）と，トラフィックを管理する BIG-IP LTM（Local Traffic Manager）により，必要となる各種サービスを管理・防御する．

ネットワーク機器のリプレイス対象は，これら FW とセキュリティ機器のみならず，各拠点のコアとなる L3 スイッチ，エッジやフロア用の L2 スイッチなども含まれている．全学で L3 を計 7 台，L2 を計 105 台導入し，各拠点と DC 含む基幹部分に設置した．

図 3 は，新ネットワークでの拠点接続概念図である．

3.4 先行導入システム類

一方，今回のリプレイスで予算要求した中で，セキュリティ強化のためのサンドボックスと，学生の利便性向上のための無線 LAN システムに関しては，緊急性などを考慮して別枠で予算が認められ，リプレイスに先行して設置・導入した．

セキュリティ強化のためのサンドボックスシステムには，Fortinet 社の FortSandbox を中心とし，各拠点のメールサーバの前段に FortiMail を配置して検疫を強化した [10]．2018 年春から稼動を開始した．

無線 LAN システムは学生の利便性向上を目的とするもので，講義室を中心に，図書館や食堂などで利用できるように設計した．Cisco 社の製品を中心として，学生の居る 9 キャンパスに，計 316 台の Cisco Aironet 2800 シリーズの AP を設置した．無線 LAN コントローラー Cisco 5520 Wireless Controller を全学で 2 台，FW として PaloAlto PA-820，認証用にエイチ・シーネットワーク (株) の Account@Adapter [11] を導入し，eduroam で利用できるようにした．AP 用として PoE が必要となるため，“ネットワークシステム”でリプレイス対象となる L2 スイッチの一部について，この無線 LAN システムの中で PoE L2 スイッチとして先行導入した．こちらは 2018 年初秋より稼動を開始した．

また，この無線 LAN システムに含まれる，DNS フィルタリングサービスである Cisco Umbrella [12] は，無線 LAN のユーザのみならず，学内の一般ユーザ（クライアント利用者）にも適用し活用することとした．

4. 新ネットワークへの移行とトラブル

今回はネットワーク構成を大きく変更することから，移行に時間がかかることが想定されたので，可能なところから順次，設定・導入を行うこととした．

4.1 移行方針

ネットワークの継続的な安定稼働を主眼とし，ユーザに移行をあまり意識させないためにも，大きく 2 段階に分けて移行を行うことにした．まず第一段階として，拠点内の L3，L2 スイッチの入れ換えを行い，さらに従来の拠点設置の FW を，DC 設置の NGF である PaloAlto に移行し，これまで通りに利用できることを確認する．次に，この状況でネットワークが安定稼働していることを確認した後，第二段階として，ADC である BIG-IP 側に，Web サーバ系や先行導入した FortiMail を含むメールサーバ系など，各種サービスを順次移行することとした．図 4 は，各拠点での物理構成の変更概念図である．

4.2 移行でのトラブル

各拠点の FW は，大学統合当初は統一的なルールで運用していたが，キャンパスの事情などの理由により，本学のセキュリティポリシー範疇内でそれぞれ追加・変更してきた．さらに，例えばその当時のシステムに必要な設定が，互換性のために残したままになっているケースが多数あるなど，まずはこれらの認識と整理が大変な作業となった．その上で今回，従来型の FW での iptables の設定を，PaloAlto の設定に置き換えたが，ルールの思わぬ抜け落ちが発生した．そのため，入れ替えての稼働直後に，通信ができないケースが稀にではあるがいくつか見つかり，都度対処を行った．

またこれらのトラブル以外にも，移行に関して以下に示すような事案が生じた．

4.2.1 移行作業とスケジューリング

このネットワークシステムは，本学の情報関連システムのみならず，教育・研究・大学運営のインフラであるため，運用し続けながら，新システムに問題なく移行しなくてはならない．本学は拠点が県内に広く点在しているため，拠点での設置や立ち会い確認などの実作業に，人員の配置と移動も含めた日程調整が必要となる．その上，機器の導入・構築・テストといったシステム側の都合だけでなく，大学の部局別・拠点別に様々異なる学務予定などを第一に優先せねばならない．機器の入れ換えが中心だったこれまで数度のリプレイスの際にも，このスケジューリングに苦心したが，今回はネットワーク構成を大きく変更したため，さらに困難を極めた．

4.2.2 スイッチでのフラッピング

FW を入れ換えた後，一見問題なく通信出来ているのに，突然繋がらなくなるなど不安定になるケースが散発した．症状の発生自体が稀のため，原因がすぐにはつかめなかった．FW のルール設定を再確認したり，念の為，経路上にあるスイッチやケーブルも交換してみたが，症状は収束しなかった．そこでネットワーク構成を再度確認して，いくつかの可能性から，推定した上でのテストを繰り返し，原因を特定した．

従来のネットワーク構造での VLAN(図 5) では問題は生

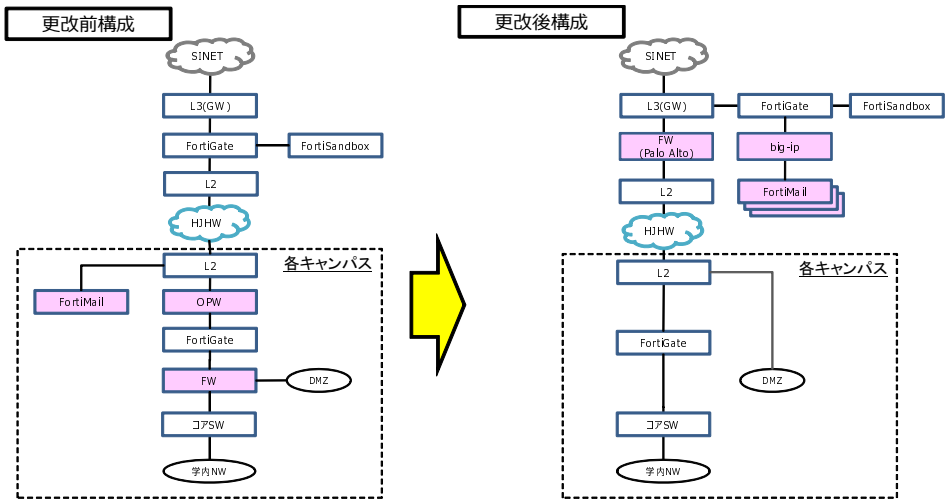

図 4　拠点ネットワークの物理構成変更 概念図

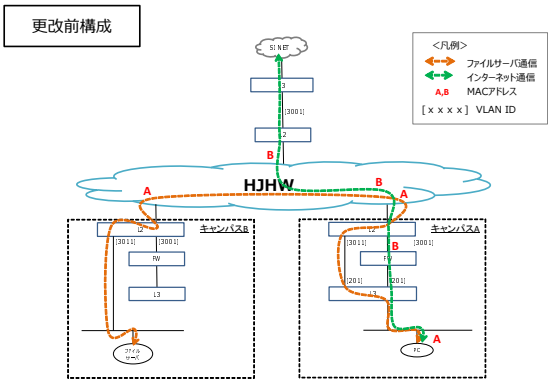

図 5　更新前構成 概念図

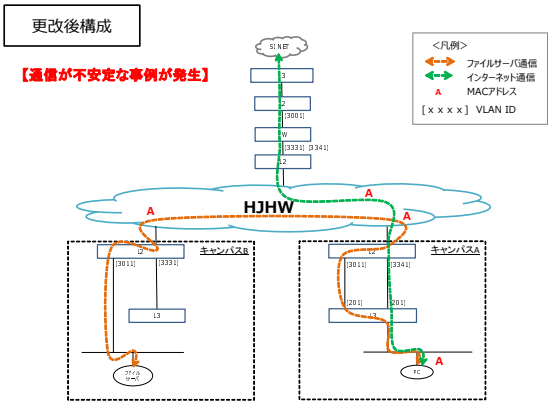

図 6　更新後構成 概念図

じなかったのだが，FW の入れ換え後，このままの VLAN 構成では，HJHW の一つのブリッジドメインに，複数の VLAN から同じ MAC アドレスが流れてしまうことが判った (図 6)．これによって，スイッチでフラッピングが発生するために，通信が不安定となっていたと判明した．

これは上流側（HJHW の CISCO ASR）の設定による，いわゆる Q-in-Q トンネルでの制約であり，MAC アドレスベースの VLAN では，ブリッジドメインを分ける設計でない限り，このような症状が発生してしまう．そこで本

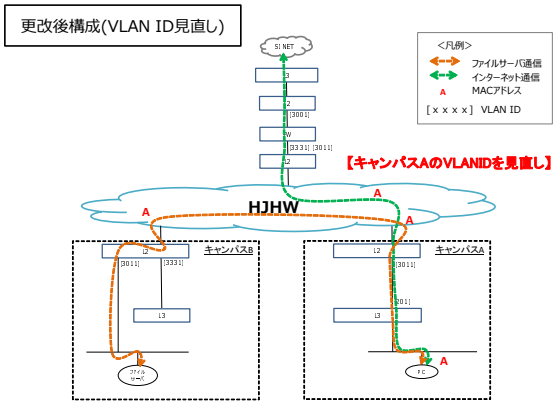

図 7　更新後構成（VLAN 見直し後） 概念図

学側でネットワーク構造と VLAN 設計自体を見直して，このような箇所を洗い出し，症状が発生しないように改善した (図 7)．

4.2.3　複数のアプライアンスの組み合わせ

先行して導入した FortiSandbox/FortiMail に，今回，PaloAlto と BIG-IP を導入したが，こういった異なるセキュリティ系アプライアンスを複数導入したことで，どの機器が，いつ，どうして通信を止めているのかなどが，直観的にも判りにくくなってしまった．例えば，機器設定内のとあるオプションを選択することで，実際にどういう設定がされてどこまでどう影響が出るのかなどの詳細や，またそれぞれ設定した “ルールセット” がどういった時に適用されるのかなどの詳しい説明を，メーカーに問い合わせても製品の性格上はっきりと開示されることが少ないため，実際にテスト系を作って tcpdump などで流れるパケットを確認するなど，影響を調査しながら試行錯誤しつつ設定を検討した．

5. おわりに

第 IV 期目となるリプレイスに伴うネットワーク構成の再設計について報告した．

本学の情報インフラの基盤として，これまで同様の利用を基本的に可能としつつ，FW とセキュリティ機器を DC に集約するネットワーク構成に改編した．また同時にリプレイスを行った “情報処理教育システム”も大きな問題なく移行を完了した．ユーザ側での大きな設定変更などはなく，機器入れ換えなどでの利用停止はあったものの，日々の利用面でユーザにあまり意識させることなく移行することができた．

BIG-IP 側に各種サーバを移設する作業については，メールや DNS などは完了したものの，学内にある各種対外公開用 Web サーバなどについては，これから順次の作業となっている．また現時点では，導入した新たなセキュリティ機器の機能をまだまだ十二分には活用できておらず，これからの最適化や微調整が今後必要である．

さらに，本学として長年の課題事項であった拠点間回線の強化が，近々に実現する可能性が高くなってきている．その際には今回導入した各種機器などの再設定だけでなく，拠点間（もしくは拠点–DC 間）を直接接続するなどさらに大きく変更せねばならず，ネットワーク構成自体を根本からまた再設計する必要が生じることになるだろう．

参考文献

[1] URL http://web.pref.hyogo.jp/pa11/pa11_000000121.html
[2] 津川誠司: “兵庫県における情報通信基盤の運用と課題”, 情報処理学会研究報告, 2009-IOT-7, **10**, pp. 1 – 6 (2009)
[3] 林 治尚, 高橋 豊, 馬越健次, 鈴木 胖: “大学統合に伴う学内ネットワークの再構築と遠隔授業システムの運用”, 情報処理学会研究報告, 2006-DSM-41, pp. 79 – 84 (2006)
[4] 村上登志男，林 治尚: “複数拠点を結ぶ学校組織内ネットワーク運用事例”, 情報処理学会研究報告, 2007-DSM-46, pp. 37 – 42 (2007) 2007(72), 37 – 42
[5] 林 治尚, 馬越健次, 鈴木 胖, 太田 勲: “兵庫県立大学における情報新システムの構築と移行”, 情報処理学会研究報告, 2010-IOT-10, **3**, pp. 1 – 6 (2010)
[6] 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, **18**, pp. 51 – 62 (2015)
[7] 林 治尚, 畑 豊, 太田 勲: “兵庫県立大学における大学法人化に係る情報関連システムの改編”, 情報処理学会研究報告, 2013-IOT-23, **9**, pp. 1 – 5 (2013)
[8] URL https://www.paloaltonetworks.jp/products/secure-the-network/next-generation-firewall
[9] URL https://www.f5.com/ja_jp/products/big-ip-services
[10] URL https://www.fortinet.com/jp
[11] URL https://www.hcnet.co.jp/products/security/radius/accountadapter.html
[12] URL https://www.cisco.com/c/m/ja_jp/umbrella/index.html