◇◇◇◇◇◇
解　説
◇◇◇◇◇◇

九州工業大学における全学セキュア・ネットワークの導入について

中村 豊[1]
福田 豊[2]
佐藤 彰洋[3]

1　概要

九州工業大学では、2014 年 9 月に 3 キャンパス一斉にネットワーク環境を更新し、コアスイッチを 40Gbps, 戸畑および飯塚キャンパス間接続を 40Gbps とする全学セキュア・ネットワークシステムを導入した。全学セキュア・ネットワークシステムでは、大学と SINET への接続境界点に学外公開 IP へのアクセス制御を行うファイアーウォールを導入し、さらに各キャンパス毎に部局を収容可能なキャンパスファイアーウォールを導入した。また、各キャンパス内のコアスイッチは 40Gbps インタフェースを用いたバーチャルシャーシ構成による構築を行った。本報告では、これらのシステムを導入するにあたっての経緯や、事前調査、準備事項などについて述べる。また導入後 1 年 6ヶ月を経過した現状がどのようになっているのかについて述べる。

2　はじめに

九州工業大学では 2014 年 9 月に 3 キャンパス一斉にネットワーク環境を更新した。戸畑、飯塚、若松キャンパスにおけるコアスイッチは 40Gbps によるリング構成とし、40Gbps 接続によるバックボーンとした。また、戸畑、飯塚キャンパス間接続には 40Gbps 長距離伝送装置を用いて接続し、戸畑コアスイッチから飯塚コアスイッチ間において 40Gbps による接続を実現した。さらに、本学と SINET 接続の境界部分には学外公開 IP アドレスのアクセス制御を行うための境界ファイアーウォールを設置し、各キャンパスには学科・部局を収容するためのキャンパスファイアオーウォルを導入した。本報告では、これらのシステムを導入するにまでの経緯、事前調査、準備事項、利点・欠点などについて述べる。また導入後 1 年 6ヶ月を経過した現状がどのようになっているのかについて述べる。

3　システム更新のための事前準備

3.1　調達の経緯

九州工業大学では、2005 年度に戸畑キャンパスにおいてネットワーク更新がレンタル予算化され、飯塚キャンパスでは 2002 年度にネットワーク更新がレンタル予算で導入された。若松キャンパスにおいては、大学院 2 研究科のレンタル予算内にネットワーク機器が組み込まれていた。

[1]情報科学センター　准教授　yutaka-n@isc.kyutech.ac.jp
[2]情報科学センター　助教　fukuda@isc.kyutech.ac.jp
[3]情報科学センター　助教　satoh@isc.kyutech.ac.jp

表 1: 戸畑キャンパスにおける主要建物間の光ファイバー距離

コアスイッチ側	ノードスイッチ側	距離
総合教育棟サーバ室	本部事務	303.8m
	教育研究 6 号棟	285.4m
附属図書館 EPS 室	事務部サーバ室	91.6m
	教育研究 5 号棟	312.7m
	教育研究 1 号棟 (機械)	123.8m
	教育研究 1 号棟 (建設)	186.9m
総合研究 2 号棟 EPS 室	総合研究 1 号棟 (南)	107.1m
	総合研究 1 号棟 (北)	150.7m
	教育研究 8 号棟	210.1m
コラボ教育支援棟 機械室	教育研究 3 号棟	73.7m
	教育研究 4 号棟	-

このように各キャンパス毎に調達年度および調達経緯が異なるため、機器の重複や責任分界点での管理の問題など、運用上の問題点が存在した。そこで 2013 年度に全学運用組織として、情報基盤機構／情報基盤運用室が組織され、全学的なネットワーク運用組織として、整備された。

組織の整備に伴って、キャンパス毎のネットワーク予算を一本化し集約した。予算の集約化によって効率的な運用と管理体制の一元化およびセキュリティの強化を目指した。

3.2 事前調査と要求要件

実際に導入業者が決定したのは 2014 年 3 月であったが、導入のための仕様を決定する前の学内調査は 2012 年の夏頃から始めていた。以下の節では事前アンケートの内容とその結果およびキャンパス毎の事前調査および要求要件について述べる。

3.2.1 アンケート

全学セキュア・ネットワークシステム導入に際して、大学内の全ての部局に対して、ネットワークに対する要求項目に関してアンケートを実施した。主にセキュリティ強化のためのアンケートと無線 LAN AP 設置に関するアンケートであった。セキュリティ強化のアンケートでは、キャンパスファイアーウォールを設置した場合の利用の有無に関して質問した。その結果、戸畑キャンパスでは約半数の部局において、利用したいという回答が得られたため、キャンパスファイアーウォールの設置が要求項目となった。飯塚キャンパスでも同様に、ファイアーウォール装置の導入が困難な部局での要望が上がったため、キャンパスファイアーウォールの設置が要求項目となった。若松キャンパスでは既存のファイアーウォール装置として Juniper SSG シリーズが設置されていたため、これの更新のためにキャンパスファイアーウォールが必要であった。無線 LAN AP に関しては、公共性の高いエリア（具体的には講義室・会議室・実験室・リフレッシュコーナー・ロビーなど）で要望の上がった箇所に増設することを要求項目とした。

3.2.2 戸畑キャンパス

戸畑キャンパスでは、主要な建物間の接続は OM2[1] 光ファイバーであった。表 1 に戸畑キャンパス内の主要建物間の光ファイバー距離の計測結果を示す。これまでは OM2 光ファイバーであったため、

表 2: 飯塚キャンパスにおける主要学科スイッチまでの光ファイバー距離

コアスイッチ側	ノードスイッチ側	距離
情報科学センターサーバ室	事務部	123.8m
研究棟ネットワーク室	機械情報	112m
	知能情報	127.5m
	電子情報	92.0m
	情報創生	96.1m
	生命情報	124.6m

1000Base-SX での接続となっていた。将来的なトラヒックの増加や、キャンパスファイアーウォールへの収容を考慮すると、主要建物への増速は必須となるため、OM2 光ファイバーで 10Gbps 接続が可能な 10Gbase-LRM[2] インタフェースが必須の要求仕様となった。また、10Gbase-LRM では距離の制限が 220m であったため、それを超える距離となった建物（具体的には教育研究 5 号棟）には、新規にシングルモード光ファイバーを敷設し、10Gbase-LR インタフェースが要求仕様となった。教育研究 6 号棟および本部事務は既設のシングルモードファイバーを用いて、10Gbase-LR インタフェースでの接続とした。

ファイアーウォールに関しては、大学と SINET への境界部分に境界ファイアーウォールとして、学外公開 IP アドレスとして登録されている IP アドレスのみを学外からアクセス可能とする制御を行うためのファイアーウォールを導入した。これまでは Cisco Systems 社製の Catalyst3750 のパケットフィルタ機能を用いた制御であったため、UDP パケットに対してアクセス制御を行うことが困難であった。従って、境界ファイアーウォールの要求仕様として、ステートフルインスペクションが可能な事が要求要件となった。境界ファイアーウォールの導入により、学外からの UDP パケットによる攻撃（具体的には DNS, SNMP, NTP による攻撃）を防御することが可能となった。Catalyst3750 では上流側に 10Gbase-LR インタフェースを用いた接続であったため、スループットを落とすことなくファイアーウォール機能を実現するために、ファイアーウォールスループットとして 20Gbps 以上であることも必要要件となった。

戸畑キャンパス内のキャンパスファイアーウォールに関しては、2010 年度のネットワーク更新の際に工学部内の各学科において L3 ルータのアクセス制御機能を用いて学内からのパケットフィルタを実施していた。全学セキュア・ネットワークへの更新のタイミングで、工学部の部局だけではなく、本部事務および本部事務が所有していたファイアーウォール機能もキャンパスファイアーウォールへ収容変更を要求仕様とした。これらのキャンパスファイアーウォールには仮想ファイアーウォール機能を必須として 50 個まで実装できる仕様を要求要件とした。これは研究室単位での収容は困難であるが、学科ごとの収容であれば十分なライセンス数である。

3.2.3 飯塚キャンパス

飯塚キャンパスも戸畑キャンパスと同様に、情報科学センター棟、研究棟、事務棟と OM2 光ファイバーであった。このため、5 学科へのサーバ室までの 10G 化には 10Gbase-LRM インタフェースが必要要件となった。表 2 に飯塚キャンパス内のコアスイッチから主要学科スイッチまでの光ファイバー距離を示す。

飯塚キャンパス内では、キャンパス内プライベート IP アドレスの VLAN-ID が他キャンパスと衝突していたため、導入のタイミングでリナンバーが必要となった。

戸畑・飯塚間のキャンパス間接続においては、60km のダークファイバーを借料していたため、既設では 10Gbase-ZR インタフェースを用いた接続構成となっていた。全学セキュア・ネットワークシステ

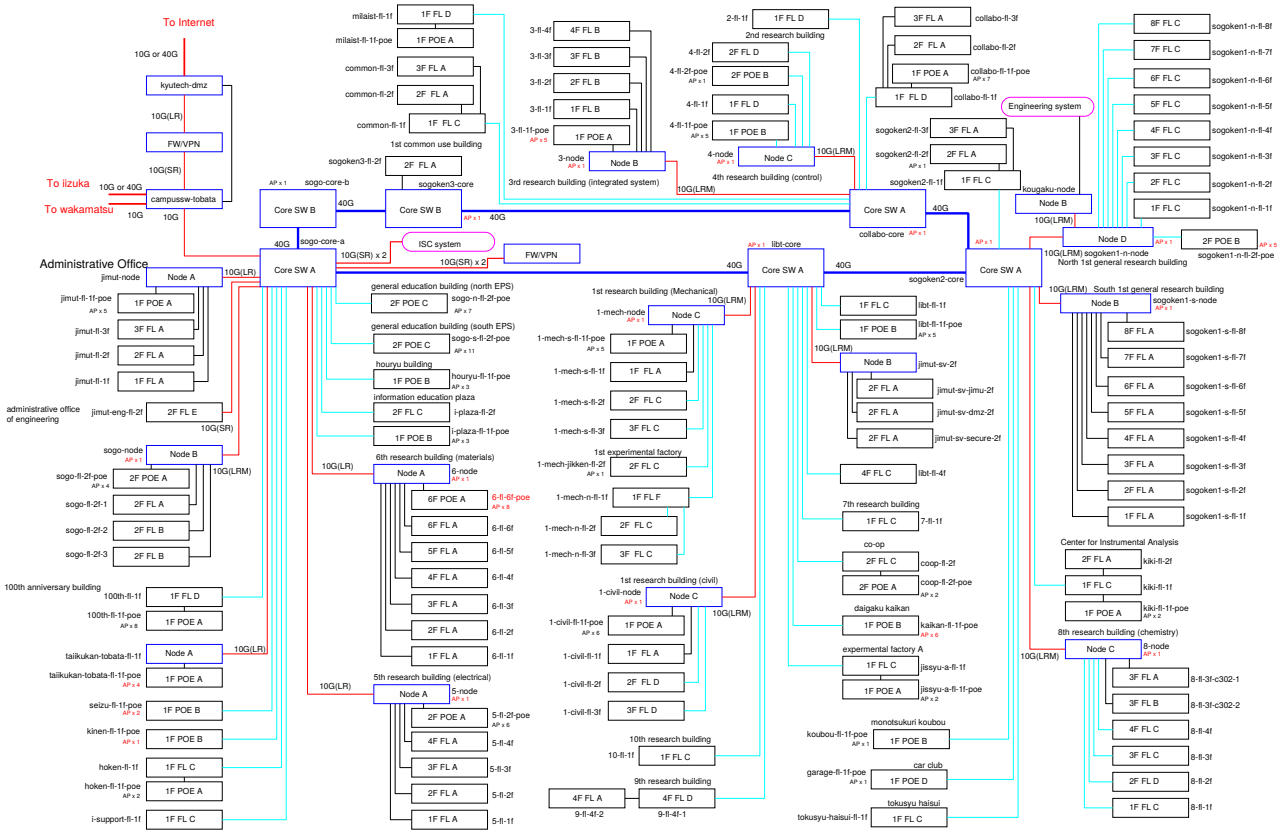

図 1: 戸畑キャンパス接続構成図

ムでは 40Gbps 化の仕様を加点項目として記述し、実際の導入となった。

飯塚キャンパス内のキャンパスファイアーウォールに関しては、5 学科がレンタル予算で学科内のネットワークを整備していたため、導入当初は 5 学科以外の部局の収容を要求要件とした。現在、電子情報工学科の学科ファイアーウォールをキャンパスファイアーウォールへ収容するための調整を行っている。

3.2.4 若松キャンパス

若松キャンパスでは、北棟、南棟の 2 つの研究棟の各フロアまで 10Gbps の接続要求が上がっており、事前に OM3 光ファイバー網の工事が実施されていた。したがって、コアスイッチ・フロアスイッチには 10Gbase-SR インタフェースを用いた接続が必要要件となった。既存のファイアーウォールおよび VPN 装置、ログ管理システムなどとの整合性を維持するため、物理的な接続構成はほとんど変更しなかった。しかし、ネットワークの全学的な運用となったため、それまで若松キャンパス内で自由に割り当てていた VLAN-ID に関しては、ほぼ全てリナンバーとなった。

若松キャンパスでは既設でファイアーウォール装置を導入し、かつ NAT 機能を提供していたため、それと同様の機能を実現できるような仕様とした。また、インシデント発生時にプライベート IP 側の調査が可能なように、Web URL フィルタ設定を導入し、syslog サーバへ転送させることとした。

戸畑キャンパスから若松キャンパスまでは既設で 10Gbase-ER インタフェースを用いた接続構成であったため、それらを踏襲するキャンパス間接続と、ファイアーウォールでの 10Gbps のスループットを要求要件とした。

全てのキャンパスにおいて、コアスイッチには将来的なサーバの仮想化や、サーバファームへのトラ

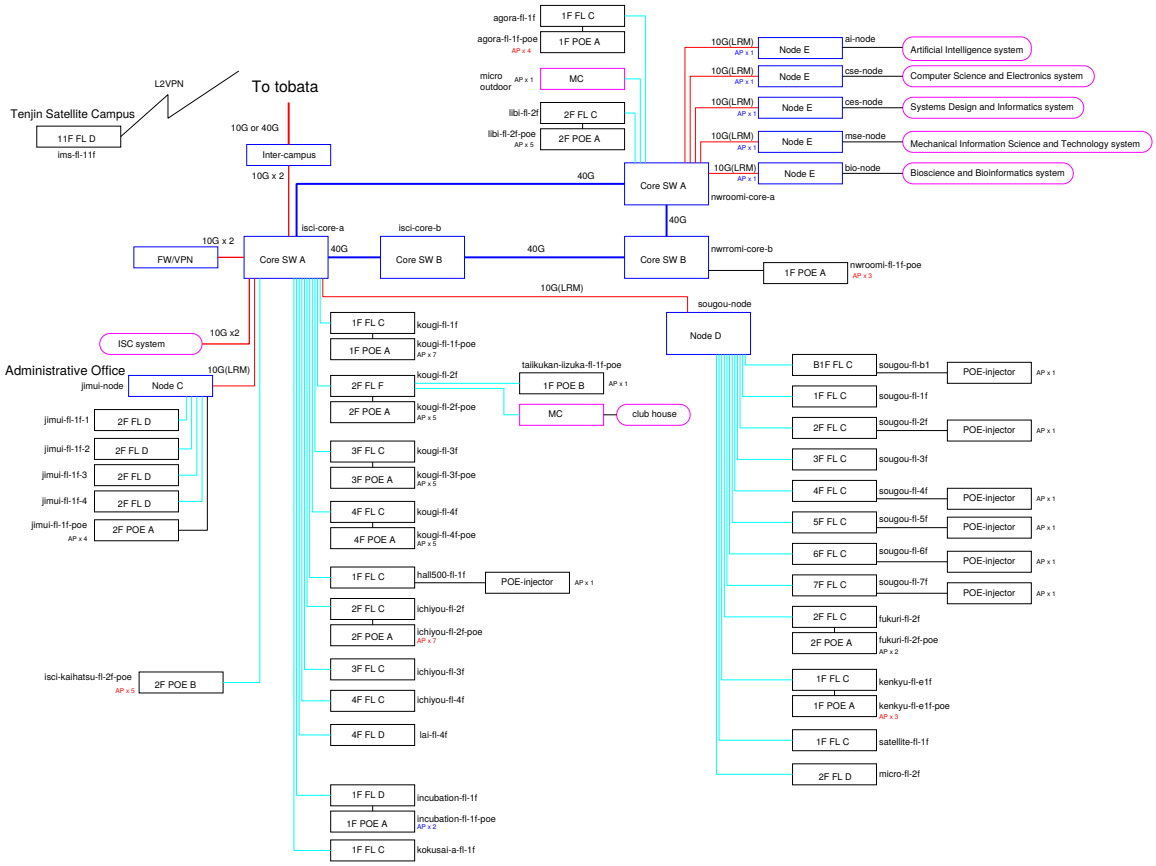

図 2: 飯塚キャンパス接続構成図

ヒック集中を考慮して、10Gbase-T インタフェースを持ったものを要求要件とした。また、管理の容易性を高めるために、コアスイッチ・ノードスイッチ・フロアスイッチに関して、同一メーカーによる同一ユーザインタフェースを提供することを必要要件とした。さらに全てのキャンパスを一括で管理するために、メーカーが提供している管理アプリケーションの提供を必要要件とした。

3.3 仕様書と接続構成

図 1 に全学セキュア・ネットワークシステム仕様書における戸畑キャンパスのネットワーク接続構成図を示す。コアスイッチは 2 種類 (Core SW A および B) で、光インタフェースを多数持つものが A、UTP インタフェースを多数持つものを B である。フロアスイッチは大きく分けて 2 種類で 24 ポート UTP を持つものがフロアスイッチ A および C、UTP ポートを 48 ポート持つものが B および D となっている。ノードスイッチは A から E までの 5 種類あり、それぞれアップリンクのインタフェース種類 (10Gbase-SR もしくは 10Gbase-LR) ダウンリンクの光インタフェース数 (0、4 もしくは 16 ポート) となっている。また、PoE スイッチは 2 種類あり、8 ポート以上無線 LAN AP を収容できるもの (PoE A および B) と、12 ポート以上収容できるもの (PoE C) となっている。

戸畑キャンパス内にはコアスイッチを 6 台設置し、それらを 40G-LR4[3] インタフェースおよび Direct Attached Cable(以下 DAC) ケーブルによるリング構成とした。リング構成のため、一部の光ファイバーが工事で切断されたとしても、迂回路が存在するため、冗長性を確保できる。また、管理を容易にするため、複数のコアスイッチを仮想化技術で 1 台のスイッチに見える事を要求仕様として設定した。ノー

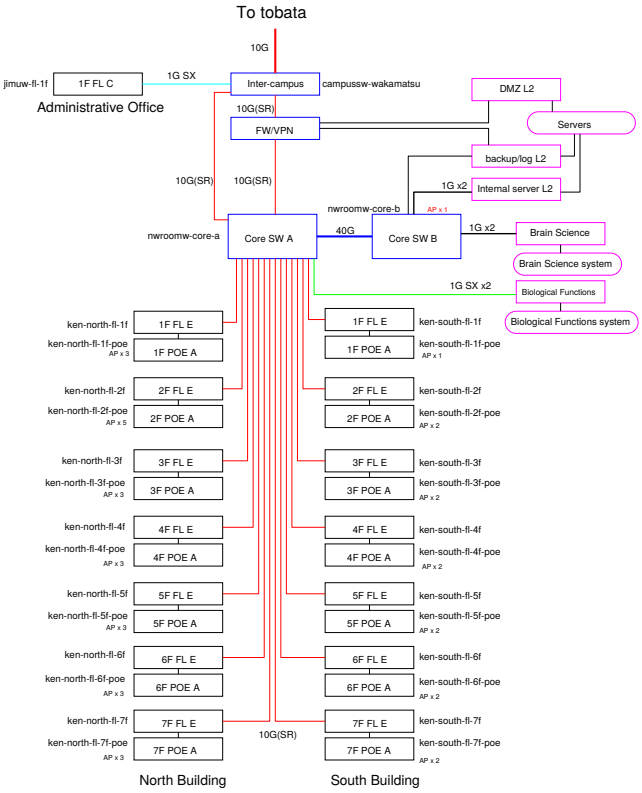

図 3: 若松キャンパス接続構成図

ドスイッチ以下はツリー構造となっている。キャンパスファイアーウォールはコアスイッチに直接収容し、L3 ルータとして運用することを前提とした。各フロアスイッチにおける必要ポート数は、全ての設置箇所の現地調査を行い、ポート数の確認を行った。

図 2 に飯塚キャンパスのネットワーク構成図を示す。飯塚キャンパスでは、コアスイッチの設置場所は情報科学センター棟サーバ室および研究棟ネットワーク室の 2 箇所で、それぞれにコアスイッチを 2 台設置する。この 4 台をリング構成として、40G-LR4 インタフェースおよび DAC ケーブルを用いて接続した。戸畑キャンパスと同様に仮想化技術を用いて、1 台のスイッチとして運用できることを要求仕様として設定した。キャンパスファイアーウォールの設置・運用に関しても戸畑キャンパスと同様である。飯塚キャンパスでは無線 LAN AP の増設要求が多かったことや、既存の無線 LAN AP が AC 電源による給電を行っていたため、PoE スイッチの設置を多数行った。

図 3 に若松キャンパスのネットワーク構成図を示す。若松キャンパスでは、以前のネットワーク構成を変更することなく装置の更新を行った。以前はファイアーウォール装置と VPN 装置を異なる装置でサービスしていたが、全学セキュア・ネットワークへの更新に伴って、ファイアーウォール・VPN を同一機種で行うこととした。また、既設の無線 LAN AP はフロアスイッチから PoE インジェクタを用いて無線サービスを提供していたが、全てのフロアに PoE スイッチを設置し、無線 LAN AP は PoE スイッチ経由での接続とした。これにより将来的に PoE 機器が増えた場合にも対応することが可能となる。

3.4 機能比較

表 3 は 2014 年 9 月時点でのメーカー毎の機能比較表である。全ての機能が提供可能なメーカーは C 社および H 社である。10Gbase-ZR(戸畑ー飯塚間接続インタフェース) 以外の機能が全て提供されている

表 3: スイッチ機能比較

スイッチ名	仕様	A 社	B 社	C 社	D 社	E 社	F 社	G 社	H 社
キャンパス間スイッチ	10Gbase-ZR	×	×	○	×	○	×	×	○
	10Gbase-ER	○	○	○	○	○	○	○	○
コアスイッチ A	10Gbase-LRM	○	×	○	○	×	○	×	○
	40Gbase-LR4	×	○	○	○	○	○	○	○
コアスイッチ B	40Gbase-LR4	×	○	○	○	○	○	○	○
	1G/10Gbase-T	×	○	○	×	×	○	○	○
フロアスイッチ PoE	12port PoE+	○	○	○	○	○	○	○	○
	24port PoE+	○	○	○	×	×	○	×	○

メーカーが F 社である。それ以外のメーカーは 10Gbase-T インタフェース、10Gbase-LRM インタフェース、40G-LR4 インタフェースでのサポートに不備があり、要求仕様を満たすことができなかった。戸畑-飯塚間接続に関して、長距離伝送装置を用いた接続を許可する事で、F 社も入札に参加することが可能となり、最終的に 3 社による入札が行われた。

3.5 スケジュール

過去のネットワーク更新では、年度末に更新作業を行ってきた。しかしながら、年度末には卒業論文・修士論文の提出・発表や、大学入試、新入生の受け入れ準備など、ネットワーク接続を維持しなければならない事が多く、ネットワークの停止を伴う更新作業はスケジュール的に困難であると予測された。そこで、全学的にネットワークを停止しても良いと思われる夏休み中、特にお盆の時期に更新作業を行うこととした。そのため調達スケジュールとしては 2014 年 9 月からのリース開始として、そこからの逆算で 2014 年 3 月に開札、2013 年 12 月に入札締め切り、2013 年 10 月に入札公告、2013 年 6 月に導入説明会となった。

4 導入

2014 年の 3 月に導入業者と導入する機器が決定し、スイッチは Juniper Network 社の EX4550, EX4200, EX3300, EX2200 が決定した。ファイアーウォール装置は Fortigate 1000C となった。また無線 LAN に関しては Aruba 社の 7200 シリーズのコントローラおよび無線 LAN AP は AP-225 が決定した。以下の節では机上設計および実際の更新について述べる。

4.1 若松キャンパス

若松キャンパスの実際の更新作業は 2014 年 7 月 19,20 日の 2 日間で行われた。基本設計は既存のまま変更しながったが、無線 LAN コントローラは、若松キャンパスには設置せず、戸畑キャンパスの無線 LAN コントローラに無線 LAN AP を収容する事とした。また、既存の IP アドレス形態は変更しながったが、VLAN ID が他キャンパスと衝突していたため、VLAN ID に関しては全学統一ルールを策定し、見直しする事となった。表 4 に VLAN ID 割り当てポリシーを示す。九州工業大学ではグローバル IP アドレスとして戸畑・若松は 150.69.0.0/16 を用いており、飯塚キャンパスは 131.206.0.0/16 を用いている。それ以外に、192.47.0.0/24〜192.47.19.0/24 の 20 個のクラス C アドレスを保有している。これら

表 4: VLAN ID 割り当てポリシー

キャンパス	ネットワーク	割当 VLAN ID
戸畑	グローバル IP	0000 から 0255
	プライベート IP	0300 から 0999
飯塚	グローバル IP	1000 から 1255
	プライベート IP	1300 から 1999
若松	グローバル IP	2000 から 2255
	プライベート IP	2300 から 2999
全学	キャンパス間のプライベート IP	4000 から 4095
	クラス C のグローバル IP	2000 から 2299
	IPv6	3000 から 3999

のグローバル IP アドレスに対する VLAN ID の割り当てと各部局で自由に割り当てたプライベート IP アドレスに関して、全学的に衝突しないようにポリシーを策定した。

4.2 戸畑・飯塚キャンパスコアスイッチ

戸畑キャンパスコアスイッチの更新は 2014 年 8 月 13,14 日の 2 日間で行われた。それに先立ち、8 月 12 日に飯塚キャンパス事務部および戸畑-飯塚間のキャンパス間接続スイッチおよび戸畑キャンパス-SINET 間の境界領域の更新が行われた。図 4 に実際に更新途中の写真を示す。

飯塚キャンパスコアスイッチの更新は 2014 年 8 月 15,16 日の 2 日間で行われた。図 5 に実際の更新途中の写真を示す。

4.3 戸畑キャンパス

戸畑キャンパスのノードスイッチ、フロアスイッチの更新は、8 月 23 日以降に更新作業を行った。戸畑キャンパスでは、これまで各学科のノードルータで行っていたパケットフィルタをキャンパスファイアーウォールへ移行する作業と、ルーティングポイントを移行する作業を同時に実施する必要があった。図 6,7 に更新前後の戸畑キャンパス内論理構成図を示す。更新前はノードルータ・コアスイッチ間では RIPv1 での経路交換を行っていたが、更新後はコアスイッチ・キャンパスファイアーウォール間を OSPF による経路交換へ変更した。ノードルータを更新するタイミングで、キャンパスファイアーウォールの仮想ルータを有効にする作業を全てのノードルータで実施した。

4.4 飯塚キャンパス

飯塚キャンパスのノードスイッチ、フロアスイッチの更新は 8 月 18 日から 22 日までの間で行われた。更新作業中に仮想ファイアーウォールへ移行したセグメントは施設課所有の電力検針、人間科学研究系およびインキュベーションセンターのセグメントであった。戸畑キャンパスと同様に既存のファイアーウォールを停止したのちに仮想ファイアーウォールを有効にすることで、ファイアーウォール機能の仮想ファイアーウォールへの集約を行った。

図 4: 戸畑キャンパスコアスイッチ

5　導入後の対応

2014 年 9 月からサービスインした全学セキュア・ネットワークシステムであるが、導入直後には複数の障害が発生した。また接続部局が増えていくことによる設定変更が頻繁に発生した。以下では導入後に起きた障害や接続部局の対応について述べる。

5.1　工学部システム対応

2015 年 3 月に工学部計算機システムのリプレースが行われた。既存環境では、工学部システム内にファイアーウォール装置を設置して、VPN 接続を行いアクセス制御を実施していたが、これらのファイアーウォール装置を戸畑キャンパス内の仮想ファイアーウォールに収容した。これまで 1Gbase-T による接続であったところを、教育研究 5 号棟ノードスイッチ、図書館コアスイッチ、総合研究 1 号棟ノードスイッチのそれぞれに、戸畑幹線ネットワーク内に接続用の 10Gbase-SX インタフェースを準備して、工学部計算機システムとの接続を行った。これにより、分散して配置されている演習用端末に対して、十分な帯域を提供することが可能となった。

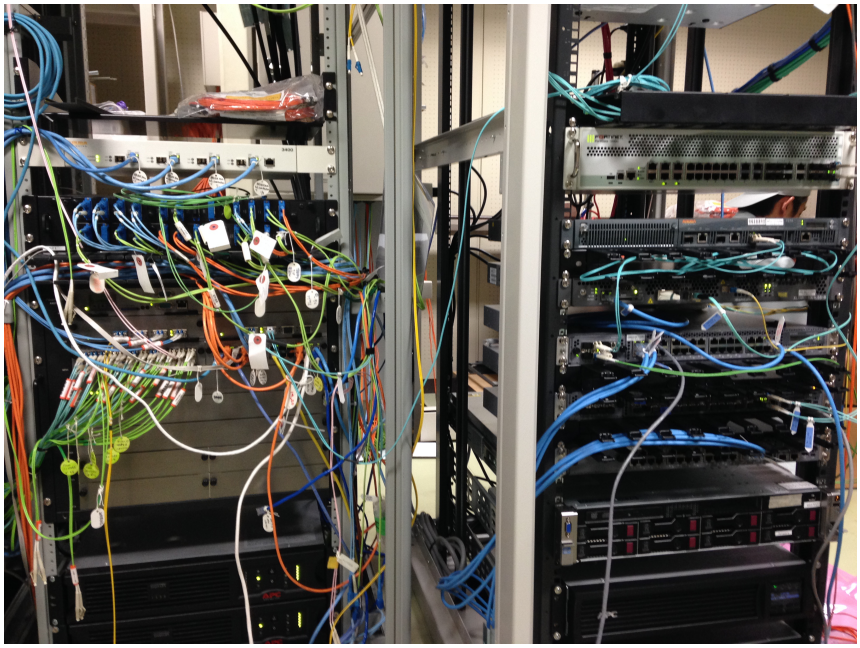

図 5: 飯塚キャンパスコアスイッチ

5.2 情報工学部電子情報工学科システム対応

2015 年 3 月に情報工学部電子情報工学科システムのリプレースが行われた。既存環境ではルーティング・ファアーウォールを学科システムで実施していたが、これらのファイアーウォール機能を飯塚キャンパス内の仮想ファイアーウォールに収容した。図 8、9 に更新前、更新後のネットワーク構成図を示す。また、部局で独自に運用していた無線 LAN システムを全学セキュア・ネットワークで調達した無線 LAN システムに基地局を追加する形で無線 LAN 環境を整備した。

5.3 情報工学部システム創成工学科対応

2016 年 3 月に情報工学部システム創成工学科システムのリプレースが行われた。既存環境では電子情報工学科と同様に学科システムでファイアーウォール・ルーティングを実施していたが、これらの機能を仮装ファイアーウォールに収容した。また、学科コアスイッチに相当する部分をシステム創成工学科に設置したノードスイッチに代替させることで、さらなるコスト削減を実現した。図 10、11 に更新前、更新後のネットワーク構成図を示す。

5.4 無線 LAN 基地局の追加設置

全学セキュア・ネットワークシステムがサービスインしたタイミングでは基地局数は戸畑キャンパス 139 台、飯塚キャンパス 77 台、屋外用 1 台、若松キャンパス 37 台の計 254 台であった [4]。それから順次基地局の整備が進められ、2016 年 2 月現在では戸畑キャンパス 153 台、飯塚キャンパス 97 台、屋外用 2 台、若松キャンパス 37 台の計 289 台まで増設されている。詳細は [5] に掲載予定である。

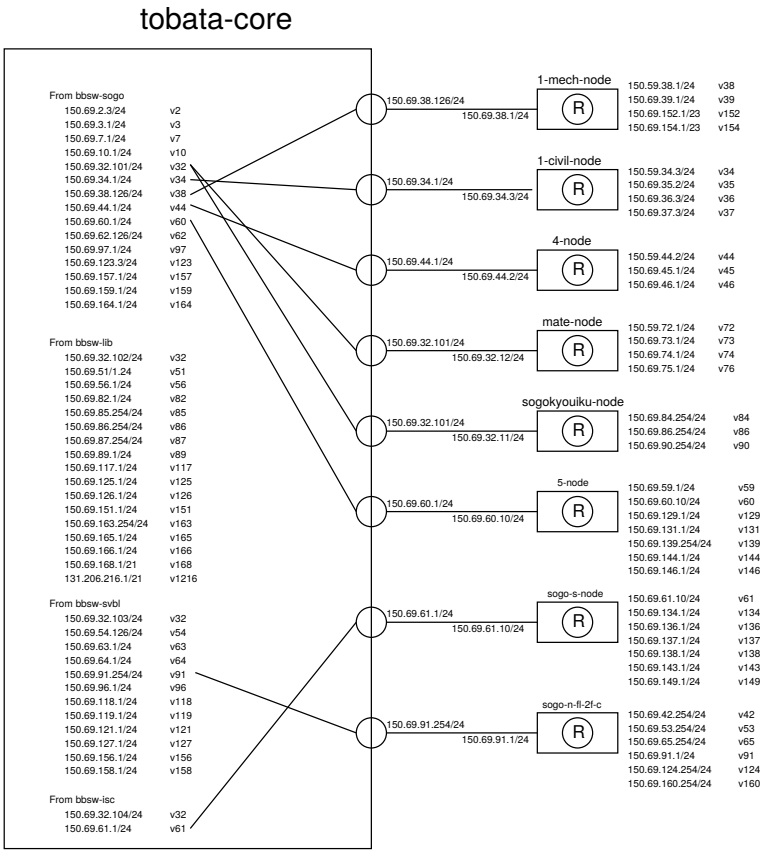

図 6: 戸畑キャンパス論理構成図 (更新前)

5.5 アンチウイルスの有効化

全学セキュア・ネットワークシステムでは、大学とインターネット接続の境界部分に境界ファイアーウォールを設置して、学外公開 IP アドレスに対してアクセス制御を実施している。境界ファイアーウォールでは、アクセス制御以外にもアンチウィルスライセンスや URL フィルタライセンス、IPS/アプリケーションコントロールライセンスが有効となっている。

本学では、2014 年 11 月 7 日から 2014 年 12 月 8 日までの間、FireEye 社 [6] による高度なセキュリティ対策機器の評価を行った。その評価期間中には学内からマルウェアのコールバックが 70 件、メールに添付されたウィルスが 540 通検出された。

これらの対策の実施が急務となったわけであるが、高度なセキュリティ機器は価格が非常に高価であるため、本学が新規に導入することは困難であった。そこで、既存の境界ファイアーウォールのアンチウィルス機能を用いた、添付メールのウィルス対策を実施することとなった。

境界ファイアーウォールにアンチウィルスポリシーを適用すると、スループットが 1.2Gbps まで低下するため、全体にポリシーを適用せずに、外部から内部に侵入してくる SMTP セッションのみに対して、アンチウィルスポリシーを適用することとした。また、いきなりすべてのメールサーバに対して適用せずに、有志の 3 サーバに対して適用しその効果を観察した。ウィルスを検知した場合は、ウィルスを除去したのちに宛先ユーザへメールを送信する設定とした。

テスト運用中の 2015 年 12 月 11 日に SMTP サーバへの大量のウィルスメールが送信されてきている事が検出された。図 12 に検出メールの例を示す。

テスト運用としては比較的安定していると評価できたので、次年度以降に全学への適用を進めていく

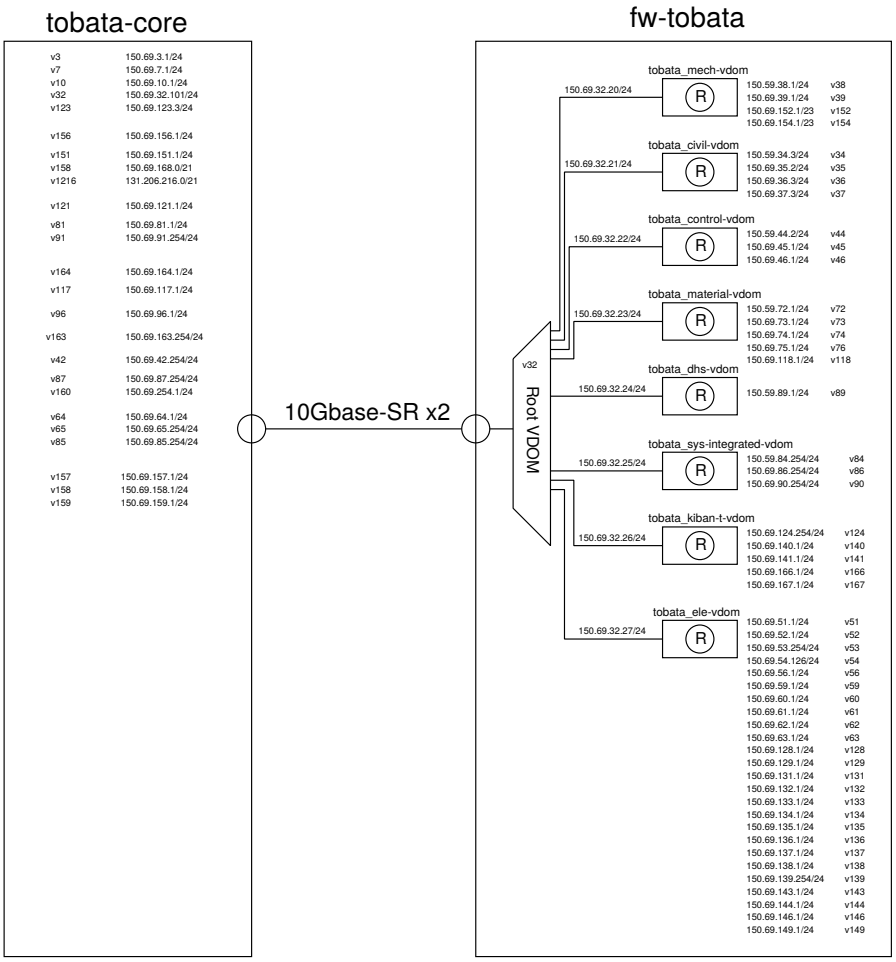

図 7: 戸畑キャンパス論理構成図 (更新後)

予定である。

6 まとめと今後の課題

更新に伴う利点として、スイッチのメーカー統一および管理権限の一体化による一元管理が可能となったこと、および、管理ツールによる全体管理が可能となった点が挙げられる。また、コアスイッチを仮想化技術により複数台を 1 台として扱うことが可能となったため、設定工数の削減が可能となった。欠点としては、コアスイッチの仮想化によるトラブルシュートの複雑さが挙げられる。コアスイッチ内でパケットロスなどの障害が発生した場合、原因を究明するための追跡が容易ではない。

今後の課題はネットワーク側の強化だけではなく、全学へ向けたサーバ構築があげられる。[6] を評価した際に、マルウェアが問い合わせを行う DNS クエリが多数検出された。これらの送信元が学内の DNS キャッシングサーバであった。これらはマルウェアが DNS 問い合わせを行う際に、端末のリゾルバを用いて、既知の DNS キャッシングサーバへ問い合わせしているものと思われる。したがって、マルウェアを調査するためには DNS キャッシングサーバの全学的な集約と A レコードの保存が必須である。今後は全学的な DNS キャッシングサーバの集約化と A レコードの保存およびそれらを解析したマルウェア検出が課題である。

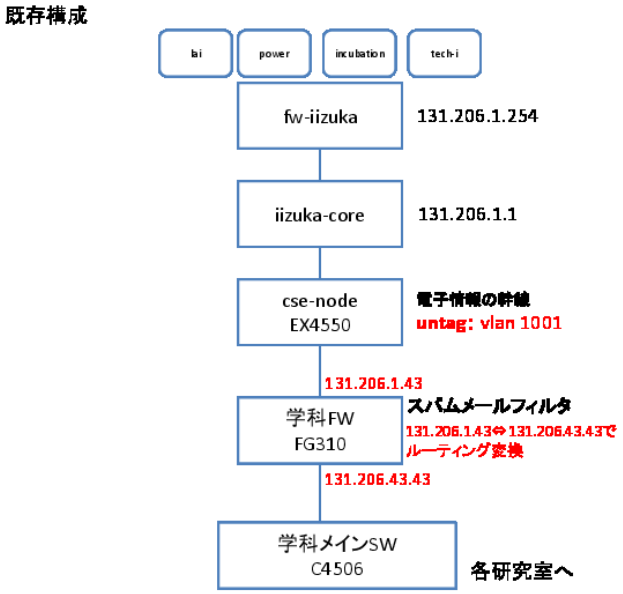

図 8: 情報工学部電子情報工学科システム更新前

参考文献

[1] 構内情報配線システム, http://home.jeita.or.jp/is/committee/tech-std/std/JIS_X_5150_kaisetsu_final.pdf

[2] IEEE P802.3aq 10GBASE-LRM Task Force, http://grouper.ieee.org/groups/802/3/aq/index.html

[3] IEEE 802.3ba Task Force, http://www.ieee802.org/3/ba/public/jul08/cole_03_0708.pdf

[4] 九州工業大学・全学セキュアネットワーク導入における無線 LAN 更新, 福田 豊, 中村 豊, 佐藤 彰洋, 研究報告インターネットと運用技術（IOT）, 2015/2

[5] 九州工業大学・全学セキュアネットワークにおける無線 LAN 利用について, 福田 豊, 中村 豊, 研究報告インターネットと運用技術（IOT）, 2016/3 (予定)

[6] FireEye. https://www.fireeye.jp/

[7] 「vvv ウイルス」の正体とは？ ランサムウェア「CrypTesla」の流入は限定的, http://blog.trendmicro.co.jp/archives/12632

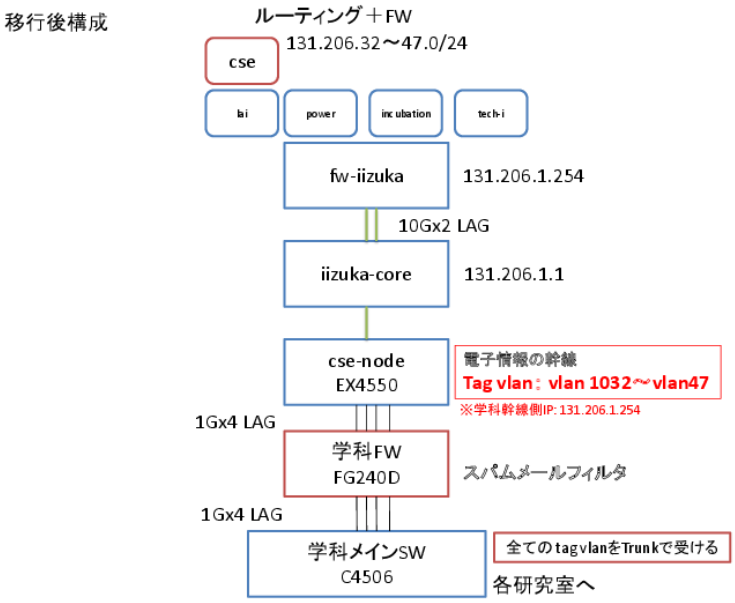

図 9: 情報工学部電子情報工学科システム更新後

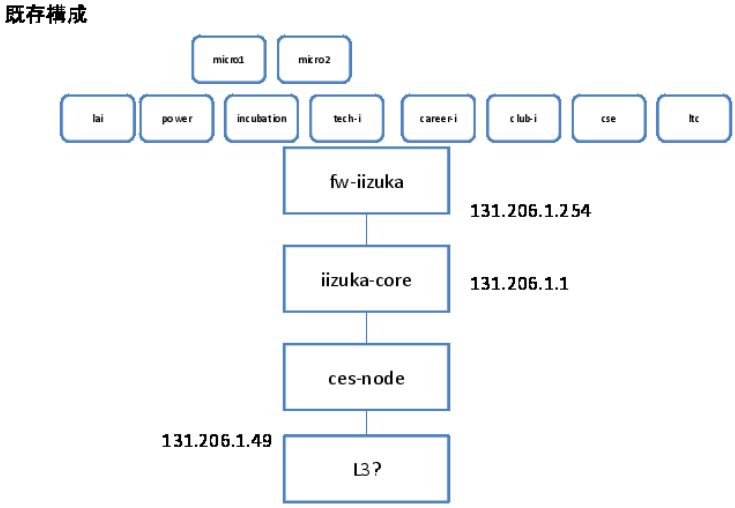

図 10: 情報工学部システム創成工学科システム更新前

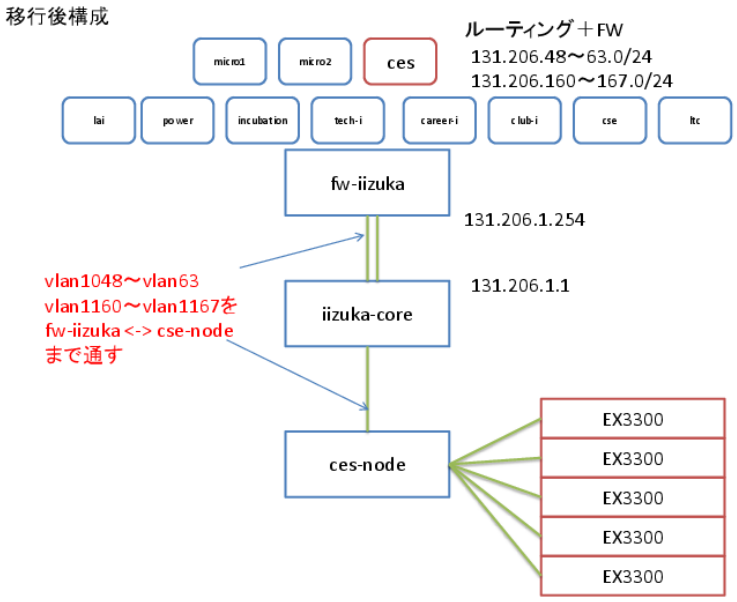

図 11: 情報工学部システム創成工学科システム更新後

Message meets Alert condition
Virus/Worm detected: JS/Nemucod.DTTU!tr Protocol: SMTP Source IP: 188.86.106.150 Destination IP: 150.69.123.7 Email Address From: SmithTabatha785@stevehaggerty.com Email Address To: jyokotak@jimu.kyutech.ac.jp http://www.fortinet.com/ve?vn=JS%2FNemucod.DTTU%21tr
date=2015-12-11 time=05:30:38 devname=fw-kyutech devid=FGT1KC3913801090 logid=0211008192 type=utm subtype=virus eventtype=infected level=warning vd="root" msg="File is infected." action=blocked service=SMTP sessionid=3116841181 srcip=188.86.106.150 dstip=150.69.123.7 srcport=52467 dstport=25 srcintf="vlan4008untrust" dstintf="vlan4008trust" proto=6 direction=outgoing filename="SCAN_invoice_09066969.zip" quarskip=File-was-not-quarantined. virus="JS/Nemucod.DTTU!tr" dtype="Virus" ref="http://www.fortinet.com/ve?vn=JS%2FNemucod.DTTU%21tr" virusid=6950299 profile="smtp-antivirus" user="" from="SmithTabatha785@stevehaggerty.com" to="jyokotak@jimu.kyutech.ac.jp" sender="SmithTabatha785@stevehaggerty.com" recipient="jyokotak@jimu.kyutech.ac.jp" analyticscksum="c82a24c41a4d06d83ea426afd4e75980079e33b3dbf2229725a3d71fe418b594" analyticssubmit=false crscore=50 crlevel=critical

Message meets Alert condition
Virus/Worm detected: JS/Nemucod.DTTU!tr Protocol: SMTP Source IP: 190.192.185.90 Destination IP: 150.69.123.7 Email Address From: StricklandHallie6860@gursimran.com Email Address To: kohgakumk@jimu.kyutech.ac.jp http://www.fortinet.com/ve?vn=JS%2FNemucod.DTTU%21tr
date=2015-12-11 time=05:28:44 devname=fw-kyutech devid=FGT1KC3913801090 logid=0211008192 type=utm subtype=virus eventtype=infected level=warning vd="root" msg="File is infected." action=blocked service=SMTP sessionid=3116660255 srcip=190.192.185.90 dstip=150.69.123.7 srcport=2417 dstport=25 srcintf="vlan4008untrust" dstintf="vlan4008trust" proto=6 direction=outgoing filename="SCAN_invoice_42326721.zip" quarskip=File-was-not-quarantined. virus="JS/Nemucod.DTTU!tr" dtype="Virus" ref="http://www.fortinet.com/ve?vn=JS%2FNemucod.DTTU%21tr" virusid=6950299 profile="smtp-antivirus" user="" from="StricklandHallie6860@gursimran.com" to="kohgakumk@jimu.kyutech.ac.jp" sender="StricklandHallie6860@gursimran.com" recipient="kohgakumk@jimu.kyutech.ac.jp" analyticscksum="ed75838efed8d5953196103cd7d65072fd491041a22ab4b83834e21a43735f4a" analyticssubmit=false crscore=50 crlevel=critical

図 12: vvv ウィルスメール検出例