外部データセンターを利用した 新潟大学無線LANシステムの構築

青山茂義[1,a)]　宮北和之[1]　三河賢治[1]

概要：新潟大学では，2019 年 3 月に無線 LAN システムを含む，全学のネットワークシステム更新を行った．更新時の重要な課題の一つは，情報基盤センターの障害や被災時などにも，学内の他部署のネットワークを継続利用可能にすることであり，無線 LAN の基幹システムに対しても，外部データセンター利用による BCP （Business Continuity Planning）対策を行った．また，もう一つの重要な課題は，速やかなセキュリティインシデントレスポンスをいかに実現するかであった．これは，有線 LAN のセキュリティシステム（人的セキュリティ体制含）と統合することにより実現した．また，スマートフォン端末を始めとするネットワーク端末普及による利用者増や授業アンケート等での多人数利用を想定して，同時利用者数 5,000 人まで対応可能な無線 LAN システムを構築した．本論文では，大学のように，多くのユーザの同時利用が想定される環境においてデータセンターを利用した無線 LAN システムに関する考察と報告を行う．

キーワード：無線 LAN，BCP，ネットワークセキュリティ

Development of Niigata University Wireless Network System using External Data Center

Shigeyoshi Aoyama[1,a)]　Kazuyuki Miyakita[1]　Kenji Mikawa[1]

Abstract: In Niigata University, the campus network system including the wireless network system was replaced in March 2019. An important subject in the replacement is construction of nonstop-network even for a system failure or a disaster of main server rooms in the campus. For the base part of wireless network system, we perform the BCP measure using the data center. Another important subject is keeping the quick security incident response. We actualize the quick security incident response by way of the integration of the security system with the wired network system. In order to deal with the increasing network users mainly because of the smartphone, we develop the wireless network system for 5,000 users in simultaneous utilization. In this paper, we discuss the wireless network system of Niigata University using a data center.

Keywords: Wireless Netowork, BCP, Network Security

1. はじめに

近年の東日本大震災（2011 年），熊本地震（2016 年），北海道胆振東部地震（2018 年）など，大規模地震災害に伴い，企業や大学における BCP 対策や DR（Disaster Recovery）に対する意識が高まっている [1], [2]．情報システムの BCP 対策としては，クラウドや外部データセンター利用を行う組織が増加している．しかしながら，データを組織外へ置くことによる情報セキュリティリスクの増大や，組織外のサーバ室にある情報機器等への速やかな障害対応やセキュリティレスポンスに必要な体制構築などの新たな問題が発生する．そのため，旧来の自組織内のサーバ室の運用から，組織外のクラウドやデータセンターを利用しながら，セキュアで安定した情報システムの構築・運用をしなければいけないというパラダイムシフトが起きている．

[1] 新潟大学　情報基盤センター
Center for Academic Information Service, Niigata University
[a)] aoyama@cais.niigata-u.ac.jp

新潟大学では，中越大震災や東日本大震災を受けて，建物の耐震補強や学内の重要施設へ自家発電設備を設置するなど，被災対策を行っている．主サーバ室に対しても，無停電化（商用電源停止後 72 時間継続運転可能）やラックの耐震固定を行っている．そのため，外部へのネットワーク接続が確保されていれば，北海道胆振東部地震（2018 年）のようなブラックアウト（商用電源停止）がおきた場合でも，スマートフォン等からインターネット経由でメールやウェブ等のネットワークサービスは継続利用可能である．

しかしながら，火災や中越大震災の長岡高専で起きたような大規模建物損壊への対応まではできておらず，万が一発生した場合には長期間のネットワークサービス停止が発生する．全国的には，大学内にデータセンター棟などを設置する動きはあるが，建物自身の耐震を考慮した新棟やコンテナ棟を一から作る必要があったり [1]，火災対策としてサーバ室への不燃ガス投入システム等の維持管理費など，予算面から民間のデータセンター相当の災害対策を施した施設を構築することは難しい．強固な災害対策を施した比較的高価なデータセンターのラックを一台借用しても月額 20 万円程度 [2] である事を考えると，大学内での予算確保も容易である．クラウド利用も考えられるが，自組織管理外機器を利用することに伴う情報セキュリティリスクやクラウド事業者倒産時のデータ保全など別な問題点もある．そこで，本学では，現実的な方法として，重要な情報基盤を SINET ノードへの接続性がよいデータセンター上に持っていくこととした．

無線 LAN は，学生やゲスト等のセキュリティレベルの低い持ち込み端末が接続される場合が多い．そのため，セキュリティインシデントの発生率が一般的に高く，速やかなセキュリティレスポンスも要求される．円滑な CSIRT（Computer Security Incident Response Team）の活動を実現するためには，セキュリティ監視，ネットワーク遮断，ネットワーク認証やホスト管理などを組み合わせた情報システムを構築する必要があり，各大学で工夫が行われている [3], [4], [5], [6], [7], [8], [9], [10], [11]．また，人的な CSIRT 体制構築とインシデントレスポンスの手順等の整備も重要である [12], [13]．管理・運用コストを考えると，これら（技術面，人員面）の手順等は有線 LAN と無線 LAN が統合されていることが望ましい．新潟大学では，2019 年 3 月のネットワーク更新に合わせて，有線 LAN のウェブユーザ認証と無線 LAN のウェブユーザ認証のインシデントレスポンス上の運用統合を行った．

無線 LAN の管理システムに対しても，BCP 対策，及び，コスト削減の観点から，クラウドシステムの利用が進んでいる．しかしながら，2.3 節で後述するように，無線 LAN 端末に対する速やかなセキュリティインシデントレスポンスのために必要な自組織内のセキュリティシステムとの連携が困難であったり，ある程度のスケールメリット持つ大規模無線 LAN システムの場合は，クラウド利用の方が必ずしもコストが低いとも言えない．

そこで，本学では，セキュリティインシデントレスポンスを考慮した無線 LAN システムをデータセンターを中心にして構築することにした．本論文の第 2 章では，新潟大学無線 LAN システムの概略の説明を行い，速やかなセキュリティインシデントレスポンスや無線 LAN システムに関して行った BCP 対策等に対する考察，及び，設計についての報告を行う．

2. 新潟大学情報基盤センター無線 LAN システム

2.1 情報基盤センター無線 LAN システムの概要

本節では，以降の理解を深めるために，図 1 を用いて，新潟大学情報基盤センター無線 LAN システムの概略を説明する．無線 LAN 管理コントローラ，認証スイッチ，認証サーバ，セキュリティシステム，ネットワークサービス系サーバ（DNS, DHCP, シスログ，ネットワーク管理，ネットワーク監視）などの無線 LAN 運用に必要な基幹システムは全てデータセンターに設置されている．そのため，データセンターが被災して運用継続できない場合を除いて，無線 LAN の基幹システムは継続運用可能である．また，障害対策のために，無線 LAN 管理コントローラについては，冗長化されている．

DR を考慮して，データセンターのフルバックアップはシステム更新時にとり，新潟大学内，及び，データセンター内に保管している．また，運用途中のメンテナンスや設定変更が発生した場合には，その差分についてバックアップを取って保管している．日々の差分が発生するものについては，新潟大学内に夜間バックアップを取っている．尚，夜間バックアップの対象は，無線 LAN 管理コントローラ，認証サーバ，ネットワークサービス系サーバ（DNS, DHCP, シスログ，ネットワーク機器管理，ネットワーク登録情報管理，ネットワーク監視）である．また，データセンター上の一部の機器（認証サーバ, DHCP サーバ, シスログサーバ, ネットワーク登録情報管理サーバ）は，冗長化や二重化のため，情報基盤センターにも設置されているので，それらについては，データセンター側に夜間バックアップを取っている．

キャンパス内には，合計 323 台（導入時）の無線 LAN アクセスポイント（無線 AP）が設置されている．新潟大学では，教室，ロビー，会議室などの公共性の高い所に情報基盤センターがまとめて設置しているが，研究室等は受益者負担で増設するので今後は合計台数が増加していく．無線 LAN 管理コントローラと無線 AP の間は，L3 トンネンリング技術により，学内 LAN 上に無線 LAN 用仮想ネットワークが構築されている．無線 LAN 用仮想ネットワーク内では，表 1 にある 8 つの VLAN と認証前 VLAN が流

れている．各無線 AP では，マルチ SSID が運用されており，その無線 AP に必要な VLAN が割り当てらている．

近年は，従来のようにネットワークのスイッチ上に直接 VLAN 設定を行わずに，多くのメーカでは，IPSec 等の L3 トンネリング技術を用いた無線 LAN システム構築が可能である．L3 トンネリング方式を用いるメリットは，拡張性と冗長性にある．学内には，情報基盤センター以外の部署の管理する L3 スイッチ配下のネットワークが複数あるが，そこに無線 AP を増設する場合，無線 LAN 用の VLAN を設定してもらう必要がある．しかしながら，VLAN 設定を行うことのできるスキルの技術者がいないことが多く，管理部署での VLAN 設定作業が難しい場合が多い．また，本学では，認証前後で VLAN を切り替えるダイナミック VLAN を採用しているが，多くの部署のスイッチではダイナミック VLAN 方式に対応していないので，そのような部署では本無線 LAN システムへの無線 AP の増設がそもそもできない．

また，L3 での接続性が確保されていれば，その冗長性をそのまま利用できるので，スパニングツリー（STP）の設計や設定の必要がない．実際，本学の場合でいうと，無線 AP からデータセンターまでの冗長性を考えると主な通信経路となり得る最低 8 台のネットワークスイッチの VLAN と STP の設計を考慮する必要がある．しかしながら，L3 トンネリングの場合は，無線 LAN 管理コントローラと無線 AP への IP アドレスの割り当てのみで終わるので，設計や運用コストの大幅削減となる．

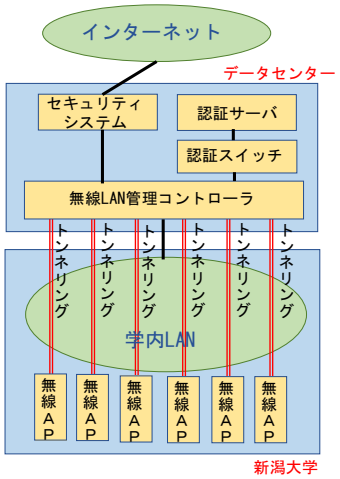

図 1　無線 LAN システムの概略図

新潟大学情報基盤センター無線 LAN システムでは，用途により SSID 毎に VLAN が割り当てられている．表 1 の一般ユーザ 1 から一般ユーザ 5 は，教職員・学生等の一般ユーザが用いるウェブユーザ認証タイプの無線 LAN である．これらは，同一 SSID 名が用いられているため，一般ユーザにとっては基本的な違いはない．負荷分散のため，この 5 つの VLAN の中から 1 つを各建物にランダムに割り当てている（1 台の認証スイッチや同一の建物に利用者が集中する場合は，運用状況を見て，建物単位ではなく無線 AP 単位で再割り当てを行う予定である）．

5 つ VLAN を用意しているのは，認証スイッチ 1 台あたりの最大同時接続認証数が 1,024（カタログ値）であるので，最大同時接続可能な認証ユーザ数 5,000 を実現するための技術的理由による．最大同時接続可能な認証ユーザ数として，更新前の 2,000 から 5,000 に増やしたのは，以下の理由である．更新前の無線 LAN システムは，主に学生のメールやウェブ閲覧等の散発的利用を想定しており，大きな会議でのサーバ上の資料の同時閲覧や大人数での授業での同時利用をあまり想定していなかった．今回のネットワーク更新に伴い，大人数が同時利用できる無線 LAN 環境構築へのユーザからの希望も多数でており，これらの同時利用を想定して，更新前の二倍程度以上の最大同時接続認証が可能な無線 LAN システムを導入することにした．

尚，現在，実際に設定されている同時利用可能なグローバル IP アドレス数は，4,064 である．今後も無線 LAN アクセスポイントを順次増設していくので，これまで利用していなかったユーザの利用が増えていく．そのため，今後の必要に応じて, 5,000 までは対応可能なシステム構成とした．

表 1　無線 LAN ネットワーク用の VLAN と認証方式

VLAN	認証タイプ	認証方式
一般ユーザ用 1	ユーザ	PSK
一般ユーザ用 2	ユーザ	PSK
一般ユーザ用 3	ユーザ	PSK
一般ユーザ用 4	ユーザ	PSK
一般ユーザ用 5	ユーザ	PSK
ゲスト用	ユーザ	CaptivePortal
eduroam 用	端末	EAP-PEAP
将来移行用	端末	EAP-PEAP

ゲスト用 VLAN は，宿舎などに滞在しているゲスト用であり，ウェブユーザ認証タイプの無線 LAN である．ゲストは新潟大学の教職員ではない想定なので，新潟大学の外側（ファイヤーウォールの外）のネットワークに接続されている．eduroam 用 VLAN は，国際無線 LAN ローミング基盤 eduroam[14] 用の VLAN である．これにより，他大学等からの来学者が自組織で発行されている eduroam アカウントで本学の無線 AP に接続できる．こちらも，学外ネットワークとして，取り扱われる．

将来移行用 VLAN は，クライアント認証方式（EAP-PEAP）の無線 LAN である．ウェブユーザ認証方式は，既存の他の情報システムのアカウントで認証できるため，新しくアカウント発行業務が発生しないので運用コストが低い．しかしながら，ウェブユーザ認証方式は，セキュリティ面では，盗聴される可能性が高いなどクライアント認証方式に劣る．また，端末の OS やブラウザのバージョンアップに伴うセキュリティ強化があった場合，認証画面のリダイレクト方式に不具合が出る可能性も大きく，将来に

わたって安定運用できる保証もない．そのため，今回の無線 LAN システム更新のタイミングで，技術的にはクライアント認証方式も運用可能な状態（SSID をステルスモードとしてユーザには通知していない）で全学展開した．

現在，学内の利用可能なグローバル IP アドレスが不足しているので，部局等からの IP アドレス回収を行い，運用上の問題点など慎重に検討（登録作業者の確保等）の上，数年後を目処にクライアント認証タイプへ順次移行する計画である．eduroam では，クライアント側の証明書を使わずに汎用性も高い EAP-PEAP 方式とクライアント証明書を使ってセキュリティ強度が高いとされる EAP-TLS 方式のどちらも利用可能である．本学の eduroam のアカウント発行の運用は汎用性をとって，EAP-PEAP 方式を採用している．将来移行用 VLAN ではどちらの方式も利用可能な形で導入しているが，今後，運用コストやセキュリティ面からどちらの方式を採用するかについては，今後の検討課題とする．

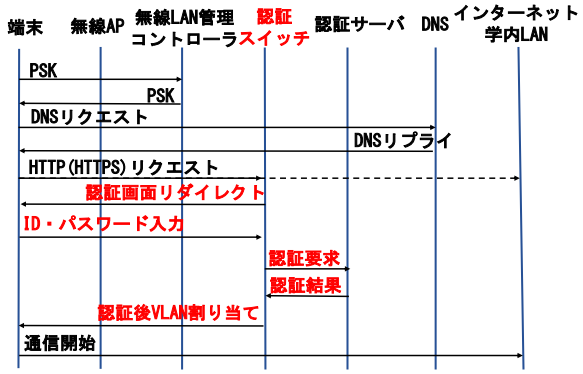

図 2　一般ユーザ用 VLAN の認証フロー

ここで，一般ユーザ用の無線 LAN システム（表 1 の一般ユーザ用 1~5）の認証フローを図 2 を用いて説明する．ユーザは，通常の PSK 方式の暗号キー認証を行う．その後，ウェブ閲覧を行うと，認証スイッチが通信摂取し認証画面のリダイレクトを行う．端末がウェブのユーザ認証画面を表示後，ユーザは ID とパスワードを入力し，ウェブのユーザ認証を行う．認証サーバにより認証が許可されたら，認証スイッチはその SSID に対応した VLAN 割り当てを行い，通信が可能となる．尚，IP アドレス等は，認証サーバ上の DHCP サーバから割り当てられる．図 2 の赤字が認証スイッチのユーザ認証時の VLAN 割り当て機能を使っている部分である．

2.2　無線 LAN のセキュリティインシデントレスポンスに対する考察

2000 年代後半から，スマートフォンが急激に普及し，ほとんど全ての学生や教職員がネットワーク端末を所持して通学する時代になった．Wi-Fi の自動接続設定にしている場合も多く，過去に無線 LAN に接続したスマートフォン等は，ユーザの接続意思に関わらず無線 AP の電波圏に入ると自動接続してしまい IP アドレスを消費する．大学では，数千～数万の大規模ユーザがいるので，ネットワークを実際には利用していないユーザの IP アドレスを全てグローバル IP アドレスとして運用するのは難しい．

グローバル IP アドレス節約ため，大学を含む多くの組織の無線 LAN システムでは，NAT 等の IP アドレス変換を採用し，プライベート IP アドレスをグローバル IP アドレスに変換している場合が多い．しかしながら，NAT の外側にあるセキュリティ機器からのインシデント発生通知や外部のセキュリティ組織等からの通報は，発生時間や IP アドレスを基本に行われる．そのため，ユーザや端末の特定は，各種ログ（アドレス変換時のポート番号，認証ログや DHCP ログ等）を付き合わせる必要あり，煩雑で時間がかかる．受け取った情報だけでは特定が困難な場合には，更に，通報者への付加情報等の問い合わせ時間などもかかる．また，大量の NAT ログ等を長期間残す必要があり，コストもかかる．それらを回避するための最もシンプルで確実な方法は，一つのグローバル IP アドレスに一人のユーザ（一台の端末）が対応していればよい．

本学では，円滑なセキュリティレスポンスのため，プライベート IP アドレスを用いずに，グローバル IP アドレスを 1,000 割り当てていたが，IP アドレス不足により接続できない不具合が 2011 年頃から発生した [15]．本学では，2 万人近いネットワークユーザがおり，そのほとんどがスマートフォン等を携帯していると予想されるので，無線 AP が全学展開されてくると，数千程度のグローバル IP アドレスを割り当てたとしても，不足が起きることは簡単に予想できる．

これを解消するため，2012 年から，無線 LAN 管理コントローラと認証スイッチのダイナミック VLAN 機能を連動させた無線 LAN システムを構築した [15]．基本的なアイデアは，認証スイッチのダイナミック VLAN 機能を用いて，ウェブユーザ認証前はインターネット等への通信が出来ないプライベート IP アドレス（VLAN）を割り当て，認証後はグローバル IP アドレスを割り当てる所にある．これにより，インシデントを発生させたグローバル IP アドレスと発生日時がわかれば，認証データベースから即座にユーザ特定が可能になった．このダイナミック VLAN 導入により，大学にスマートフォンを持ってきただけであり，学内ネットワーク利用意思のないユーザのスマートフォン等は，グローバル IP アドレスを消費しなくなった．実際のピーク利用時などのグローバル IP アドレスの削減率は 80~90% 程度という大きな削減効果があり [15]，数千個のグローバル IP アドレスを無線 LAN 用 DHCP に割り当てれば足りると予想できる．

本学で，今回の更新でのクライアント認証方式を見送った理由を将来移行用 VLAN の認証フロー（図 3）を用いて

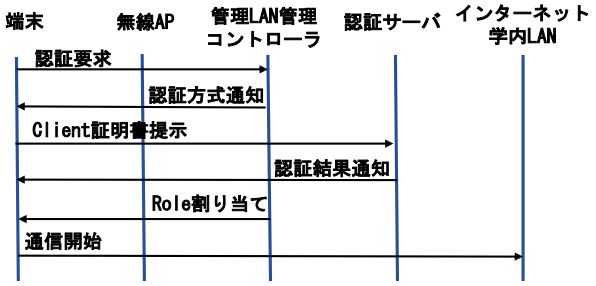

図 3 将来移行用 VLAN の認証フロー

簡単に説明する．認証要求後は，認証方式通知，Client 証明書提示，認証結果通知，Role 割り当て，通信開始と一連の動作が円滑に進んで行く．図 2 のような認証スイッチによるダイナミック VLAN の手順がないので，ユーザの意思表示によるプライベート IP アドレスからグローバル IP アドレスに切り替えることができない．クライアント認証の際に，ダイナミック VLAN を用いることは可能であるが，基本的に初回接続時の認証のみ（例：eduroam）であるので，ウェブユーザ認証のようなグローバル IP アドレスの節約効果は期待できない．

そのため，プライベート IP アドレス利用の場合は前述のようにセキュリティレスポンス時間の遅延が発生し，グローバル IP アドレスの利用の場合はグローバル IP アドレスの枯渇問題がある．クライアント認証方式は，ウェブユーザ認証より，一般的にセキュリティ強度が高いが，無線 LAN に割り当て可能な IP アドレスが十分でなく，試験用に図 3 の認証方式の無線 LAN の導入だけを行った．将来拡張用ネットワークを，実運用に乗せるための試みは，本論文の対象外とするが，クライアント認証と本論文のウェブユーザ認証との併用での導入開始を検討している．

2.3 新潟大学の CSIRT 体制の概略と無線 LAN システムへの対応

前節で説明した一つのグローバル IP アドレスを一人のユーザ（一台の端末）に割り当てることは，外部 SOC を利用した 365 日 24 時間のセキュリティインシデントの即時対応体制を構築する上で重要になる．大学の教職員だけで，365 日 24 時間体制を構築するのは現実的ではないので，基本的には外部の情報セキュリティ会社等を利用することになる．前述の NAT を利用した場合の各種ログを付き合わせてユーザを特定する方法は，単純に手間がかかるだけではなく，情報セキュリティ会社の標準的な業務支援の提供プログラムにはないために，そもそも契約を締結できない可能性が高い．また，契約可能な場合であっても，本学で行っている認証データベース上で，IP アドレスからユーザを瞬時に検索してアカウント停止等するだけというようなシンプルな方式と比較すると，費用が何倍にも膨らむことが簡単に予想できる．セキュリティ支援契約の費用は，一般的にかなりの高額（年間数百万円～数千万円）であるので，インシデント対応のための作業工数を減らすことは費用面でのインパクトが大きい．

無線 LAN を含む今回のネットワーク更新に伴い，セキュリティ機器やネットワーク機器の構成等が大幅に変わったので，これまで行っていた情報セキュリティ会社との業務契約の内容を見直して再契約する必要があった．特に，今回の更新では外部データセンターに主要機器を設置したが，新潟大学の外部にある機器は既存契約の対象外であった．そのため，既存の問題点を洗い出しつつ外部データセンターを含む CSIRT 体制の再構築を行った．既存の体制についても，これまでに発表や報告を行っていないが，他の組織でも参考になる部分があると思われるので，無線 LAN に関係する部分を中心に新潟大学の CSIRT 体制を説明する．

新潟大学では，中央（本部）CSIRT と部局 CSIRT の二段構成の中央集約・分散ハイブリッド型 CSIRT を採用している．中央 CSIRT は，情報基盤センターと情報系事務組織を母体として，新大 CSIRT と呼ばれている．また，各部局には部局 CSIRT が設置されており，セキュリティインシデント発生時は，中央 CSIRT のセキュリティレスポンス業務を支援し，常時は部局のセキュリティ管理を行う．また，365 日 24 時間体制のセキュリティ監視とネットワーク遮断を行うために，外部 SOC と監視契約を結んでいる．更に，情報セキュリティ会社（以降 CSIRT 業務支援会社）と CSIRT 業務の支援契約（セキュリティインシデント対応・分析，講習会講師，セキュリティ対策改善提案等）も結んでいる．

重大なセキュリティインシデント発生時は，初動対応として，ファイヤーウォールにて学外ネットワークとの遮断を行うが，誤報や誤遮断防止等のため，原則的に外部 SOC ではなく CSIRT 業務支援会社か新大 CSIRT が行い，深夜・休日等で外部 SOC から本学や CSIRT 業務支援会社への連絡（電話と E メール）がつかない場合は外部 SOC のセキュリティ技術者が即時遮断を行う．外部 SOC からの通報後は，即座にインシデント対応開始となるが，実際の遮断までは，30 分程度であり，その間に対応者の確保，セキュリティインシデント内容の確認，本学のインシデント対応手順や類似の過去事例の確認等を行って，その後のユーザ対応等へと進んで行く．

無線 LAN システムもこの即時対応開始のセキュリティレスポンス体制に組み込むことが理想的であるが，本学の IDS やファイヤーウォールとの連携が必須である．また，外部 SOC が対応出来る機器は，基本的にはメーカや機種が限定されている．無線 LAN 管理システムの BCP 対策として，クラウド上の無線 LAN 管理サービス利用が考え

られるが，これらの IDS やファイヤーウォールとの連携が難しく，通常の監視契約や業務支援契約の対象外ともなってしまう．そこで，本学ではデータセンター上にセキュリティシステムも含める形で，無線 LAN 管理システムを構築することにした．

更新前のインシデントレスポンス体制では，CSIRT 業務支援会社から派遣された常駐のセキュリティ技術者が先行インシデントの対応中の場合などには，即時対応をとれない可能性があり，その点が大きな問題点であった．そこで常駐者方式はやめて，CSIRT 業務支援会社内に複数のセキュリティ技術者からなる常時対応体制を構築していただき，遮断等の一次対応は原則的にリモート作業とした．複数名の体制となったことで初動対応の確実性があがった一方で，常駐者方式ではないので，費用削減効果もあり半額程度に収まった．デメリットとしては，実機調査等の二次対応のためには，外部 SOC の連絡から 90 分から 120 分程度（新潟大学への駆けつけ時間）かかるので，大学内に常駐者を置くよりも時間がかかることである．しかしながら，インシデントを発生させたユーザや部局 CSIRT が実際に対応できるのはそれよりも遅い場合が多いので，大きな問題にはならないと判断した．

2.4 無線 LAN システムへの BCP 対策のスタンス

本論文では，学術情報ネットワーク（SINET）の新潟ノードが災害時にも利用可能，又は，早期復旧するという前提で BCP 対策を考える．SINET のノードは民間データセンター内にあり，大地震などの被災時でもネットワークが停止しないか早期復旧が期待できる．無線 LAN システムの BCP 対策としては，無線 LAN システムの基幹部分（無線 LAN 管理コントローラ，認証システム，DNS, DHCP 等）を考え，被災した部局等のネットワーク機器や電源復旧した時点から利用可能なシステム想定とする．

本学の主サーバ室は，自家発電装置により，無停電源化されている．商用電源からの電源供給が停止した場合，瞬時に切り替わるので，サーバやネットワーク機器のシャットダウンは発生しない．発電用燃料は，通常稼働時から見積もって 72 時間の連続運転可能な量を常時備蓄している．また，医歯学系キャンパスにも，無停電化されたサーバ室（データセンターに直接接続されているサーバ室含）がある．そのため，北海道胆振東部地震発生後の商用電源供給停止によるブッラクアウトが起きた場合にも，SINET 新潟ノードとサーバ室間のネットワーク接続が確保されていれば，最低数日間程度は，スマートフォンなどの 4G/LTE 回線経由やインターネット経由でサーバ室内のメールサーバのメール閲覧などが可能である．ただし，サーバ室の耐震設計や火災対策は，大学内の他の建物と同様であるので，大地震や火災などに対する被災対策にはなっていない．新規に大学内にデータセンター相当の施設を設置する可能性もあるかとは思うが，BCP 的に重要な機器を絞ってから民間データセンターのスペースを借用した方が通常は安価である．そこで，今後は，メールサーバなどの BCP 上の重要情報基盤も，同一データセンターへの移動を検討していくことになっている．尚，ネットワーク基盤の DR に関しては，後述のように，文理系キャンパスとデータセンターに，ネットワーク復旧に必要な全てのバックアップをとっている（1 日 1 回更新）．

2.5 バックボーンネットワーク

有線 LAN 全体については，本論文の対象外であるが，無線 LAN のバックボーンネットワークは有線 LAN であり，有線 LAN の BCP 対策や障害対策が無線 LAN の BCP 対策や障害対策に直結する．そのため，無線 LAN の BCP 対策や障害対策に関係する部分を中心に本節ではバックボーンネットワークの説明を行う．図 4 は，無線 AP と無線 LAN 運用システム間のバックボーンネットワークの概略図である．本学では，6 台のコアスイッチ，11 台のエリアスイッチで，L3 の基幹ネットワークシステムを構成している．本学では，学部や大学院等の大規模組織毎に L3 スイッチを基本的に 1 台配置し，その L3 スイッチ配下のネットワークをエリアと呼んでいる．L3 スイッチ毎にエリア内のルーティングや VLAN 等の管理を自律して行うので，他の L3 スイッチへの接続断が発生した場合でも，学部等のエリア内でのネットワーク通信が可能である．拠点スイッチ 4 台もエリアスイッチとして機能しており，部局別調達のエリアもあるので，合計 17 エリアとなっている．各エリアには，本学では認証フロアスイッチと呼んでいる L2 スイッチ 10~20 台程度が 10Gbps（一部 1Gbps）で高速接続されている．無線 AP は，この認証フロアスイッチに UTP ケーブル（1000BASE-T, PoE 利用）により直結されている．尚，認証フロアスイッチは，有線接続の MAC アドレス認証とウェブユーザ認証に用いているが，無線 LAN システムのウェブユーザ認証には用いておらず，データセンターの認証スイッチ 5 台が無線 LAN システムの認証を集約して行っている．

無線 AP から認証フロアスイッチ，認証フロアスイッチからエリアスイッチには一本のケーブルで接続されていて冗長構成ではないので，これらのスイッチや無線 AP の故障時には，該当する無線 AP のサービスは停止してしまう．しかしながら，同一部局内の他の無線 AP 設置場所や情報基盤センターや図書館などへの比較的小さな移動で無線 LAN の利用可能なので，費用対効果から冗長構成にしてはいない．また，原則 24 時間以内復旧（平日営業時間の 2 時間以内での現場復旧対応開始）のサポート契約を結んでおり，実運用としても同日復旧可能なので，平常時にはあまり大きな影響は出ない．しかしながら，被災時等にエリアスイッチや認証フロアスイッチへの電源供給が停止

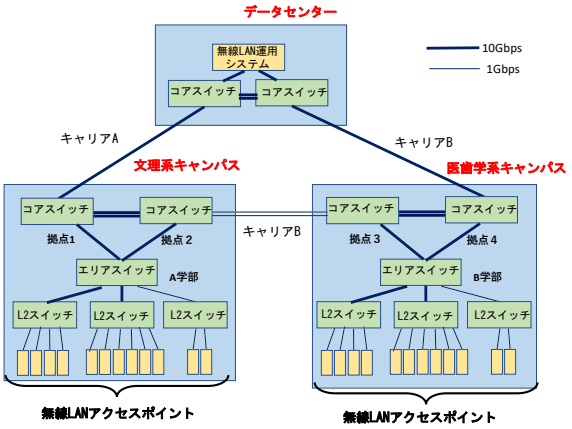

図 4　無線 LAN アクセスポイントと無線 LAN 運用システム間のバックボーンネットワークの概略図

した場合には，無線 AP への電源供給（PoE）も停止するので利用できない．費用面から全ての無線 AP の無停電化は難しいと思われるが，商用電源停止の場合でも利用可能なように一部の無線 AP の無停電化は今後の課題とする．

全学のエリアスイッチは拠点にあるコアスイッチにつながっているので，拠点コアスイッチの障害はキャンパス全体や全学（DNS 等のサーバの配置場所による）に影響する可能性がある．そこで，同一キャンパス内の 2 拠点（文理系は図 4 の拠点 1 と 2, 医歯学系は拠点 3 と 4）に対する冗長接続を行っている．同一キャンパス内のコアスイッチ 2 台は仮想化スイッチ技術（遠隔 L3 スタッキング）により，1 台として動作している．そのため，ルーティングによる冗長構成ではなく，物理的に離れた 2 台のスイッチへのリンクアグリケーションによる冗長構成である．

コアスイッチ 6 台は，物理的なリング接続になっている．データセンターの 2 台も 1 台の仮想スイッチとして運用しており，論理的な 3 台の L3 スイッチによるトライアングル構成である．そのため，例えば，文理系キャンパスの拠点 1 の被災・障害・メンテナンス時でも，物理的な拠点 2→ 拠点 3→ 拠点 4→DC 経由で，無線 LAN 運用システムへのアクセスが可能である．また，同センターから上位の SINET 経由でインターネットアクセスも可能である．

データ内に設置されているネットワーク機器 (SINET 接続用ルータ，ファイヤーウォール，学内接続用ルータ，無線 LAN 管理コントローラ，SINET 接続用光ケーブル，光終端装置等）は，全て冗長化されている．そのため，データセンター内のハードウェア一台の故障やケーブル一本の断線時などでもネットワークの継続運用可能である．尚，ネットワーク運用に必要なサーバ類 (DNS，DHCP，認証，ログ，バックアップ等）の方は．学内サーバ室との冗長構成としている．

データセンターへの機器設置前には，移動後の構成に準じて，拠点 1 においてデータセンターコアスイッチ等を仮設置し，実環境で試験運用を行なった．データセンターへの移設後にネットワーク遅延など発生していないか ping や学外の通信速度測定サイトなども用いて通信試験を行なったが，実運用に影響すると思われるような顕著な遅延は発生していはなかった．それらは，本論文の対象外であるので，詳細報告は行わない．しかしながら，無線 LAN の実運用に用いるサーバがキャンパス内に置いてあるのとデータセンター内に置いてあるので，どの程度の遅延等発生するのかは興味がある問題であり，無線 LAN 運用システムをデータセンター内に設置してよいかどうかの判断にも影響するので，その一例として，ftp の計測結果を表 2 と表 3 で示す．

表 2 と表 3 では，1MB の 5 万ファイルを送付（put）した場合と取得（get）した場合の所要時間の測定結果である．送信元や送信先に記載されている DC コアは，データセンター内へ移設前，又は移設済のコアスイッチに直接接続されているサーバの意味（図 5 ）である．また，拠点 1 コアは，拠点 1 のコアスイッチに接続されているサーバである．既に，どちらも実環境で運用開始しているコアスイッチであるので，他の通信の影響を少なくするため，測定は深夜時間帯（get は 1 時 30 分，put は 2 時）に測定を行なった．また，移設作業は，2019 年 2 月 17 日の日中に行なった．利用した機器は，FTP サーバ（3CDaemon）側と FTP クライアント（Windows Server 2016 standard 標準搭載）側のいずれも HP DL380 Gen10 （Xeon Gold 6134 3.2GHz, 64GB Memory, 10Gb SFP+）である．これらをデータセンターコアスイッチと拠点 1 コアスイッチに 10Gb SFP+モジュールを用いて光ケーブルで直接接続した．また，データセンターコアスイッチと拠点 1 コアスイッチ間も光ケーブルで直接接続 (SFP+) した．測定条件の大きな違いは，図 5 のようにコアスイッチ間の接続が同室内（移設前）であるか 10km 程度の商用キャリアの 10Gbps 専用線（移設後）が使われているかどうかだけである．

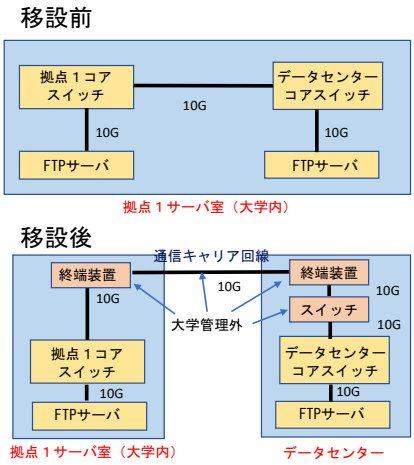

図 5 ftp 実験の構成概略

get コマンドの場合は，3 日間の平均で移設前 7 分 41 秒，移設後 10 分 1 秒であり，約 30%の遅延が発生した．また，put コマンドの場合は，3 日間の平均で移設前 3 分 26 秒，移設後 8 分 24 秒であり，約 145%の遅延が発生した．これらは，新潟大学以外の複数台のネットワーク機器が間に挟まったことによる遅延と思われるが，新潟大学以外の設備であり詳細確認ができない点，移設終了しており再試験が行えない点，1 ファイル辺り 0.01 秒程度で送受信しており実運用に影響しない点から，それ以上の通信試験等は行わないことにした．また，実運用としても，導入後約 9 か月が経過しているが，データセンター移行に起因する遅延や障害も発生していなく，大学キャンパス内の他のサーバ室でシステム運用しているのと大差はない．

表 2 大量ファイル（1MB5 万ファイル）のコピー（get）

送信元	送信先	測定日時 月/日/時刻	時間 分:秒
拠点 1 コア	DC コア（移設前）	2/15/1:30	7:06
拠点 1 コア	DC コア（移設前）	2/16/1:30	7:39
拠点 1 コア	DC コア（移設前）	2/17/1:30	8:17
拠点 1 コア	DC コア（移設後）	2/18/1:30	10:12
拠点 1 コア	DC コア（移設後）	2/19/1:30	9:42
拠点 1 コア	DC コア（移設後）	2/20/1:30	10:09

表 3 大量ファイル（1MB5 万ファイル）のコピー（put）

送信元	送信先	測定日時 月/日/時刻	時間 分:秒
DC コア（移設前）	拠点 1 コア	2/15/2:00	4:00
DC コア（移設前）	拠点 1 コア	2/16/2:00	3:07
DC コア（移設前）	拠点 1 コア	2/17/2:00	3:13
DC コア（移設後）	拠点 1 コア	2/18/2:00	8:55
DC コア（移設後）	拠点 1 コア	2/19/2:00	7:17
DC コア（移設後）	拠点 1 コア	2/20/2:00	8:59

3. 終わりに

本論文では，2019 年 3 月に新潟大学で行ったネットワーク更新に伴って行った新潟大学情報基盤センター無線 LAN システムに対する BCP 対策と DR に関する考察・報告を行った．データセンター利用による運用変更を実現しながら，セキュリティレスポンス時間の短縮可能なシステムを構築した．この時間短縮は，データセンター上に有線用のセキュリティシステムとダイナミック VLAN 利用可能なシステム構築により実現した．導入後，約 9 か月が経過しているが，データセンター移行に起因する遅延や障害も発生しておらず，学内サーバ室での運用と大差ない運用ができている．

参考文献

[1] 野口宏, 大瀧保広, 鎌田賢, BCP としての学内データセンターの設置とその活用方針, 学術情報処理研究, No.18, pp.24-32 (2014).
[2] 沖野浩二, 金森浩治, 黒田卓, 富山大学における BCP の検討, 学術情報処理研究,No.17,pp.17-24 (2013).
[3] 田島浩一, 西村浩二, 近堂徹, 岸場清悟, 相原玲二, ホスト登録を用いたネットワーク認証システムの実装と評価の実装と評価, 学術情報処理研究, No.11, pp.42-49 (2007).
[4] 浜元信州, 青山茂義, 三河賢治, 全学ネットワークアクセス認証システムの導入, インターネットと運用技術シンポジウム 2009, IPSJ Symp. Series Vol. 2009, No.15, pp.1-8 (2009).
[5] 浜元信州, 五十嵐瑛介, 青山茂義, 三河賢治, ホスト登録システムを利用したネットワークアクセス認証システムの運用, 情報処理学会研究報告, Vol.2010-IOT-9 , No.4, pp.1-6 (2010).
[6] 清水さや子, 横田賢史, 吉田次郎, 萩原知明, 鈴木 直樹, 戸田勝善, キャンパスネットワーク運用評価と MAC-IP 監視管理システムの構築, 学術情報処理研究, No.18, pp.53-60 (2014).
[7] 浜元信州, 井田寿郎, 齋藤貴英, 酒井秀晃, 小田切貴志, 横山重俊, 動的 VLAN を利用した全学認証ネットワークの構築, 学術情報処理研究, No.20, pp.65-74 (2016).
[8] 宮北和之, 山本一幸, 青山茂義, 三河賢治, ネットワークアクセス認証連動型 IP 管理データベースの運用と機能拡張について, 情報処理学会研究報告, Vol.2016-IOT-33, No.2, pp.1-6 (2016).
[9] 近堂徹, 田島浩一, 吉田朋彦, 岸場清悟, 岩田則和, 西村浩二, 相原玲二, アクセス制限機能を提供するキャンパスネットワークの実装と評価, 学術情報処理研究, No.21, pp.36-43 (2017).
[10] 鈴木聡, 村上直, 湯浅富久子, 金子敏明, 馬場亮一, 中村貞次, 橋本清治, 西口三夫, 荒い分割のキャンパスネットワークにおける IP アドレス棚卸作業, 情報処理学会研究報告, VOL.2018-IOT-40, No.11, pp.1-5 (2018).
[11] 青山茂義, 山本一幸, 宮北和之, 三河賢治, ホスト登録システムへの非利用 IP アドレスの特定機能実装と IP 棚卸し, 学術情報処理研究, No.22, pp.23-30 (2018).
[12] 青山茂義, 三河賢治, 大学 CSIRT 体制に対する考察と新潟大学への適用 I, 大学 ICT 推進協議会年次大会論文集, vol.2018, pp.1-2(2018).
[13] 中西 貴裕, 福岡 誠, 金野 哲士, 田頭 徹, 鈴木 健之, 田口 慎, 大内 慎也, 木村 優太, 加治 卓磨, 川村 暁, 岩手大学における持続可能な情報セキュリティインシデント対応体制の構築, 学術情報処理研究, No.22, pp.44-53 (2018).
[14] 国立情報学研究所, euroam JP の概要, https://www.eduroam.jp/about/ (2019 年 5 月 23 日 最終確認).
[15] 山本一幸, 青山茂義, 三河賢治, 動的 VLAN を利用した新潟大学無線 LAN システムの設計と運用, 学術情報処理研究, No.18, pp.43-52 (2014).