NATIONAL INSTITUTE FOR FUSION SCIENCE

セキュリティを考慮した核融合科学研究所キャンパス情報ネットワークの構築

Construction of the campus information network with information security measures on NIFS

山本孝志、情報ネットワークタスクグループ
核融合科学研究所　情報通信システム部
T. Yamamoto and members of information Network Task Group
The Division of Information and Communication Systems,
National Institute for Fusion Science

(Received - Aug. 29, 2018)

NIFS-MEMO-84 Oct. 05, 2018

TOKI, JAPAN

セキュリティを考慮した核融合科学研究所キャンパス情報ネットワークの構築

山本孝志、情報ネットワークタスクグループ*
核融合科学研究所 情報通信システム部

Construction of the campus information network with information security measures on NIFS

T. Yamamoto and members of Information Network Task Group
The Division of Information and Communication Systems,
National Institute for Fusion Science

Abstract

核融合科学研究所のキャンパス情報ネットワークは平成 12 年度より ATM ネットワークからギガビットネットワークへ更新された。しかし、それ以降の急速な情報化により、PC が取り扱うデータ量が増えるとともに、インターネットではセキュリティの脆弱性を利用する攻撃が頻出するようになり、キャンパス情報ネットワークにおいてもこれらに対する改善が望まれるようになった。そこで、平成 24 年度と 25 年度のキャンパス情報ネットワークの全面的な更新において、ネットワーク能力の拡大に加え、幾つかのセキュリティ対策を行った。さらに、平成 26 年度の電子メールシステムの更新時にワンタイムパスワードの導入を行った。ここでは、情報セキュリティの観点を含めつつ、キャンパス情報ネットワークの更新前後の状況と今後の展望について述べる。

The campus information network of National Institute for Fusion Science was updated from ATM network to gigabit network in FY 2000. After that, improvements in the network had been required because of the rapid computerization and infomatization; the amount of data used by PC was increased and attacks that use software vulnerabilities became prominent. A throughput of the network has been enhanced and some security measures have been introduced, on the renewal of the campus information network in FY 2012 and FY 2013. A one-time password has been applied to the mail system in FY 2014. In this document, the situation before and after updating the campus information network and future prospects are described including the viewpoint of information security.

---

* 高山有道、井上知幸、中村修、渡邊清政、中西秀哉、大砂真樹、清水一真、井上望未、大西優子、山口忠司

Key words: gigabit network, information security, one-time password, quarantine authentication system,

（2018 年 8 月 29 日）

※ 日時を明記していない記述は 2018 年 4 月 1 日時点を示す

目次

1　キャンパス情報ネットワークの概要

核融合科学研究所は恒久的なエネルギー源として期待されている核融合を研究する国内有数の機関であり、世界最先端の研究を行っている。所内には管理部、技術部、研究部に所属する職員と、総合研究大学院大学や名古屋大学などからなる学生をあわせ約 300 名が在籍し、常に国内外から多くの来訪者が訪れている。

核融合科学研究所の情報ネットワークは、データを高速で転送する装置やセキュリティを確保する装置等で構成され、世界最大級の大型ヘリカル装置(LHD)によるプラズマ実験の遂行、国内有数の能力を誇るスーパーコンピュータであるプラズマシミュレータによるシミュレーション研究の推進、国内外の大学・研究機関との共同研究や基幹業務の基盤を担っている。

研究所のネットワークは目的別に一般的な研究や事務を行うネットワークである「キャンパス情報ネットワーク（研究基盤ネットワーク、NIFS–LAN)」、LHD 実験の遂行を目的とする「LHD 実験ネットワーク（LHD–LAN)」、プラズマシミュレータによる研究の遂行を目的とする「プラズマシミュレータネットワーク（PS–LAN)」の三つのクラスタから構成される。LHD–LAN、PS–LAN は NIFS–LAN に接続されているが、それぞれの接続点には多段防御の考えからファイアウォールが設置されている。

NIFS–LAN は FDDI ネットワーク、ATM ネットワークを経て[†]、平成 12 年度よりギガビットネットワークに更新され、幹線部は 1Gbps、末端の情報コンセントは 100Mbps の帯域を約 2000 台の端末へ提供していた。その後、実験やシミュレーションで扱うデータ量が増加し、末端のパソコンも急激に高性能化され、NIFS–LAN がデータ転送のボトルネックとなる状況が見受けられた。また、国内の大学、研究機関が接続する広域ネットワーク SINET が提供する帯域も従来の 1Gbps から 10Gbps へと拡大した。さらに、長年の運用を経たためネットワーク機器の安定した保守体制をはかることが次第に困難となってきた。

情報セキュリティにおいては、事前 MAC アドレス登録による DHCP サービスの提供など先進的な取り組みを進めてきたが、固定 IP アドレスの登録の欠如やセキュリティチェックが手動であることなどが改善すべき項目であった。また、インターネットではウイルスに代表される悪意のあるプログラム（マルウェア）を配布する活動が活発化し、感染経路が従来の電子メールによるものに加え、Web サーバを経由したマルウェアも出現し、これまでのウイルス対策ソフトによるメールサーバと端末での対策だけでは十分に防ぐことが困難になってきた。電子メールそのものにおいても定常的に大量の迷惑メールが送付されるようになり、あわせてスパムの送信元になることを厳に防ぐための対策を取る必要も生じてきた。

[†] 津田健三他、「核融合科学研究所キャンパス情報ネットワーク NIFS-LAN の構築」、NIFS–MEMO–30, 2000 年 9 月

そこで、平成 24 年度と 25 年度にかけて幹線部は 10Gbps×2 と冗長性を持たせ、末端の情報コンセントへは 1Gbps を提供することを目的とした NIFS–LAN の更新を実施した。情報セキュリティ対策としては平成 25 年度にセキュリティチェックを自動化した検疫認証システムと標的型攻撃検知システムの導入を行い、平成 26 年度にワンタイムパスワードを取り入れた電子メールサービスを導入した。それぞれについて情報セキュリティ講習会などにて説明するなど周到な事前準備を行ったため、大きな混乱もなくサービスを開始することができ、当初の目的を達成することができた。

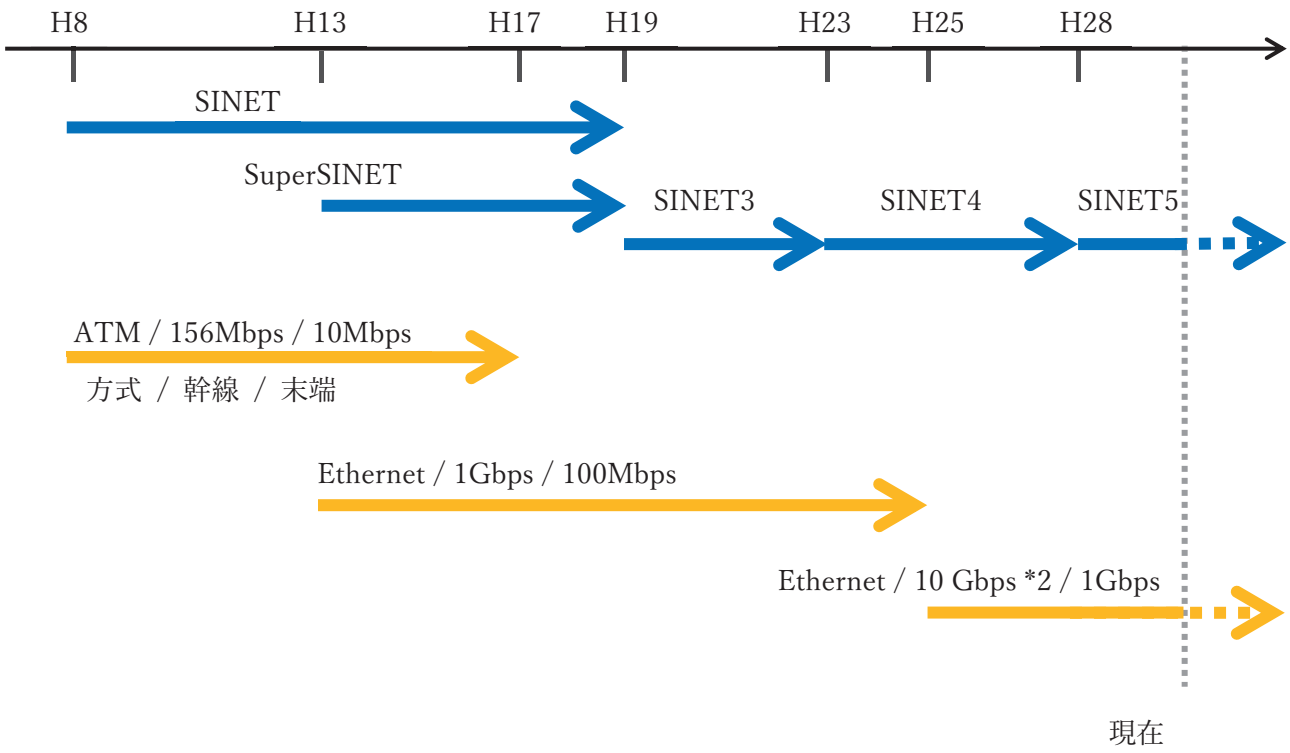


図 1. SINET と NIFS キャンパス情報ネットワークの変遷

2　キャンパス情報ネットワークのこれまで（平成 23 年度まで）

2.1　ウイルス対策ソフトとファイアウォール

核融合科学研究所が現在の土岐地区へ移転した当初は、ウイルス対策ソフトやファイアウォールが普及しておらず、研究所においても電子メール経由によるウイルス感染や外部から研究所内のサーバへの侵入などいわゆるセキュリティインシデントが度々発生していた。そこで、平成 11 年度に Windows 端末、Macintosh 端末用のウイルス対策ソフトをサイトライセンスにて一括購入を行い、所内の端末への普及に努めた。その当時はウイルス定義ファイルの更新は週一回程度だったが、当時の海外回線の帯域が細く、時間がかかったため、

所内にウイルス配布用サーバを準備した‡。

続く、平成 12 年 6 月にインターネットと NIFS–LAN との接続点にファイアウォールを設置した。導入時は、所外から所内へのアクセスについては Windows ファイル共有などセキュリティに問題がある特定のサービスのみを禁止する方式だったが、その後、一般的なファイアウォールの規則である原則禁止の方針に変更した。これにより、最低限のセキュリティ対策を実施することができた。導入当時のファイアウォールは汎用的なワークステーションに専用ソフトウェアをインストールしたものであったが、その後、性能や保守の面から専用機（アプライアンス）によるファイアウォールを導入した。運用においては大きな問題は生じなかったが、プロトコルが複雑な TV 会議システムの通過設定が一番の問題となり、機種別に開放すべきポート番号を個別に指定することにより対応を行った。

その後、このファイアウォールは保守期限を迎えたため平成 23 年度に次世代ファイアウォールを導入した。従来のファイアウォールは IP アドレスとサービスを区別するポート番号の組み合わせで通信を制御していたが、次世代ファイアウォールは制御の判断材料として通信の内容も参照するものである。同時にデータベースと比較し危険な通信を検知する機能も有する。また、一台の筐体に複数の仮想的なファイアウォールを設置することができ、管理の集中化を行うことができる。その翌年度には同一機種を購入し Active-Standby 方式で一台が故障してもサービスを継続する冗長構成を取った。

2.2　侵入検知システム

平成 12 年 6 月のファイアウォールの導入によりインシデントが発生するリスクが大幅に減少したが、ファイアウォールの機能上、設定で許可した通信は、仮にその通信内容がセキュリティの脆弱性をつく攻撃であっても通過してしまい、結果として攻撃が成功する可能性が残されていた。そこで、平成 14 年 3 月には流入する通信の振る舞いやその内容を規定のルールと比較し攻撃の可能性がある場合には警告を出す侵入検知システム（IDS）を導入した。その結果、多くの情報が得られたが、その検出内容は多岐に渡りそれが意味することを理解するには高度な技術が必要であったこと、警告は攻撃が実施されたことを通知するもので事前の警告としては利用できなかった等の理由で IDS を十分に活用することができなかった。

2.3　所外からのアクセス：VPN サービスと SSL–VPN サービス

ファイアウォールを設置したことにより、これまで制限がなかった所外から所内のサーバへのアクセスに制約がかかることになった。利用者が個人的に運用する個々のサーバについてファイアウォールで対応するのは現実的ではなく、また、セキュリティ上も問題が生じる可能性が高い。そこで、平成 14 年 8 月に専用のクライアントソフトを用いる VPN サ

‡ 山本孝志、「所内向けウイルス定義ファイルサーバの開発」、NIFS–MEMO–52、2007 年 2 月

ービスを開始した。その後、平成 18 年 8 月に所員だけではなく、LHD 共同研究者へ関連するデータへのアクセス経路を提供する役割を持つ SSL–VPN サーバへの更新を行った。SSL–VPN サービスは専用のクライアントソフトがなくても Web ブラウザを通じて安全な通信路を設定するサービスである。導入した SSL–VPN サーバは接続前にウイルス対策ソフトの有無など端末の接続前セキュリティチェック機能を有している。その際に、認証を強化するため使い捨てパスワードであるワンタイムパスワード（OTP）を導入し、これを発生するトークンを利用者へ配布した。

一方、平成 10 年 10 月より電話回線（アナログ、ISDN）経由によるリモートアクセスサービスを提供していたが、一般家庭にインターネットが普及したため、その役割りを SSL–VPN サーバが負うこととし、平成 22 年 3 月に運用を終了した。

2.4　事前 MAC アドレス登録による DHCP サービスと情報セキュリティ講習会

これらの対策後にも、まれにウイルス感染事故が発生した。特に、平成 16 年初夏に発生したウイルス感染事故において、DHCP サービスで接続していた端末の利用者が不明であることが根本的な問題として指摘された。DHCP サービスの取り止めも検討されたが、DHCP サービスはノート PC を中心に広く利用されており、固定 IP アドレスのみにした場合、1 台の端末に対し複数個の IP アドレスを割り振る必要が生じるため運用が非効率になる恐れがあった。調査の結果、DHCP サービスを提供するプログラム[§]には、指定したファイルに記載された特定の MAC アドレスのみ IP アドレスを配布する機能を有していることがわかった。そこで、利用者が Web ブラウザを用いて接続する端末の MAC アドレスと利用者情報を登録する Web システムを技術部の協力により構築し、同年 9 月より事前 MAC アドレス登録による DHCP サービスの運用を NIFS–LAN において開始した。

端末のセキュリティ状況を良好に保つために、MAC アドレス登録の条件として、登録者が該当端末のセキュリティ要件を満たしていることの確認（検疫手続き）を求めた。

1. 適切なパスワードを設定していること。
2. ウイルスに感染していないこと。
3. OS のアップデート (Windows OS については「Windows Update」、Mac OS については「ソフトウェアの更新」)が適切に行われていること。
4. ウイルス対策ソフトをインストールしていること。ウイルス定義ファイルが更新されていること。

出張などにおいて所外のネットワークに接続した後に再度 NIFS–LAN に接続する際にも上記の手順を確認することが推奨された。また、検疫手続きを安全に実施するため、他とは隔離されたネットワークを提供する検疫コーナーをシミュレーション科学研究棟事務室の一角に設置した。

---

§ ISC DHCP , https://www.isc.org/downloads/dhcp/

サービス開始時には、検疫手続きや MAC アドレスの確認方法など具体的な手順を説明する講習会を開催し、受講者を自身で端末情報を登録できる MAC アドレス登録者に認定した。インシデント動向など情報セキュリティは常に変化するため、以後、MAC アドレス講習会を毎年開催し、MAC アドレス登録者はこの受講を必須とした。

その後、MAC アドレス登録者講習会は、情報セキュリティポリシーにて要請されるセキュリティ教育の一環として行われる「情報セキュリティ講習会」に併合され、現在も年一回の開催を続けている。

2.5　所外ネットワークと無線 LAN

前項の事前 MAC アドレス登録 DHCP サービスの運用開始と前後し、より一層のセキュリティレベルを上げるために平成 16 年 8 月に来訪者用所外ネットワーク（現、ゲストネットワーク）が敷設された。これは、共同研究者など来訪者がインターネット接続に利用するネットワークであり、所内のネットワークとは分離されたネットワークである。

平成 17 年 10 月になり、NIFS–LAN の無線アクセスポイント（無線 AP）の管理体制が問題となり、運用が停止された。所外ネットワークの無線 LAN については、平成 18 年 1 月に商用プロバイダとのアクセス回線の契約が行われ、NIFS–LAN より完全に分離された。さらに、同年 9 月に新規接続時に利用者へ所外ネットワークへの接続であることを確認させる機能を有する認証サーバ[**]を導入した。これらのセキュリティ対策を施すことにより、同年 10 月より所外ネットワークの無線 AP の運用を再開した。なお、平成 18 年 1 月より所外 LAN の MAC アドレスの事前登録は不要としていた。また、これ以後、特殊な場合を除いて、NIFS–LAN の無線 AP の設置は行われていない。

2.6　電子メールサーバの集約とその運用

研究所のメールアドレスドメインである @nifs.ac.jp は計算機センターの時代からネットワーク管理組織が運用する代表メールサーバにて取り扱っていたが、それ以外にも当時は所内には複数のメールサーバが存在していた。代表メールサーバにおいても、端末に続き、ウイルス対策ソフトを導入していたが、全てのメールサーバの対策は完了していなかった。一方、情報化の進展に伴い、取り扱うメールの量が増え、特に添付ファイルによる研究、事務データのやり取りが増大し、既存のワークステーションにフリーソフトをインストールしメールサーバを構築する従来の方式は、性能的にも運用面においても能力不足となった。そこで平成 16 年 2 月にアプライアンス型メールサーバを新しい代表メールサーバとして導入し、同時にメールサーバの一元化を図った。これは、ファイアウォールと DNS の設定変更により、所内と所外をまたぐメールは全て代表メールサーバを経由させ、これにより全て

[**] Web サイトへのアクセスを行うと、初回時に限り注意を喚起するページが現れ、そのページの確認ボタンを押すことによりインターネット接続が可能となる。

のメールにおいてウイルスチェックを可能とした。

平成 18 年 10 月においては、労働管理対策の一環として、勤務時間外においては所内間のメールについては送信者に返送する方針が定まり、検討した結果、業者による新たなシステムの開発によらず既存のシステムで実装することとなった。平成 19 年 2 月より時間外配送抑制システムとして運用を開始し、3.8 節で述べる代表メールサーバの更新時まで運用を継続した。

アプライアンスサーバによる代表メールサーバは Web ブラウザでメールを送受信できるなど機能的にも満足できるものだったが、平成 19 年 12 月にハードディスク障害により運用が突然停止した。ディスク構成は RAID1（ミラーリング）＋予備構成であり 1 本のディスクが故障してもペアのディスクによる運用を継続し、同時に、自動的に予備のディスクが故障したディスクに入れ替わる構成を取っていたが、その入れ替え作業中にペアのもう一本のディスクも故障しアクセス不能となった。ディスクの復旧を試みたが障害発生より 24 時間を経過した時点でサービスの再開を優先させることとし、障害発生から 2 日後に代替機によるサービスの再開を行った。その後、幸いに元のディスクのデータを復旧させることができ、利用者のメールデータの消失は免れたが、バックアップシステムの重要性が強く認識された。その後、平成 20 年 3 月にバックアップシステムを導入し、一日一回のバックアップを取得する体制を整え、さらに、平成 21 年 1 月にアプライアンスサーバの後継機種への更新時には 2 台構成による冗長化を図り、30 分間隔で同期を取る運用を開始した。

その後、更新したアプライアンスサーバにおいて、度々、ハードディスク障害が発生した。障害の原因は RAID ボードにあり再起動で一時的に回復するが、根本的に解消するためには RAID ボードの交換とアプライアンスサーバの OS の更新が必要とされた。しかし、新しい OS ではメールのフィルタリング機能に不具合があり、前述の時間外配送抑制システムが不能になるため実施できなかった。数回に渡り不具合の修正依頼をベンダーに伝えたが、ついに改修されることなく保守期限を迎えることになった。この障害を回避するために定期的にメールサーバの再起動を実施するという想定外の運用コストが発生した。

一方、ウイルス付きメールと同様に問題視されたのは迷惑メール（スパム）である。代表メールサーバがワークステーションで構築されていた時代はフリーウェアで迷惑メール対策を試行したがはかばかしくなかった。アプライアンスサーバでも複数の迷惑メール対策機能を有したが迷惑メールと判定した場合は受け取りを拒否するものであり、誤って正規のメールが届かない可能性があるために採用を見送った。その後、平成 19 年に電子メールの送信状況を継続的に学習することにより迷惑メールの判定を行い、その確信度に応じて、流入制限を行う迷惑メール抑制専用機を導入した。これは、仮に誤判定されると配送が遅れるが消失することがない方式であり、実際、大きな問題は発生しなかった。

2.7　アクセス回線

キャンパス情報ネットワークのインターネット接続は国立情報学研究所（NII）が運営す

るSINETに接続することにより行われる。キャンパス情報ネットワークがATMネットワークにより構築されていた時代は名古屋ノードまでのアクセス回線を通信業者より購入して接続していたが、平成13年度にNIIのSuperSINETに参加した際に研究所内にSINETの接続装置（ノード装置）が設置されたため、アクセス回線に対する費用は実質的に不要となった。その後、緊急時の入館体制の確保などからNIIはSINET4より都道府県単位に新規にデータセンター（DC）を設置した。これまでノード装置が置かれていた大学・研究機関については、SINET 4終了時である平成28年3月末までDCへのアクセス回線をNIIが引き続き負担することとなった。

2.8　UPKI電子証明書発行サービス

Webサービスにおいて重要な情報を取り扱う場合は通信路が暗号化されたHTTPS通信で行う必要がある。HTTPS通信を行うためには公的認証局より発行されたSSL電子証明書を入手し、Webサーバ側にインストールする必要がある。このSSL電子証明書は通信路を暗号化する他に、接続したWebサーバが偽物ではなく本物であることを証明する機能を有する。SSL電子証明書には有効期限が設定され、期限が切れる前に再購入する必要がある。研究所では平成16年2月に導入したアプライアンス型メールサーバのWebメール機能のために導入したのが最初であり、その後、情報化の進展に伴い、研究所においても多数のSSL電子証明書が利用されるようになった。

このような状況下で、平成21年4月よりNIIは、SSL電子証明書を無償で発行する「UPKIオープンドメイン証明書自動発行検証プロジェクト」を開始した。研究所でも電子証明書の申請者が研究所に所属する者であるかどうかなどの承認手続きを確立させ、平成23年3月より参加した。その後、本サービスは平成27年1月より「UPKI電子証明書発行サービス」として事業化され、将来に渡り安定したサービスとなった。UPKI電子証明書発行サービスは有償であるが、個別にSSL電子証明書を業者より購入した場合と比較すると廉価であるため、加入を継続している。

3　キャンパス情報ネットワークの高機能化（平成24年度より）

3.1　キャンパス情報ネットワーク更新の概要

これまで2章で述べたようにキャンパス情報ネットワーク（NIFS–LAN）に対し様々な取り組みを行ってきたが、基幹となるネットワーク機器の更新は平成12年度以降より行っておらず、相対的な性能の劣化によるサービスの低下、ならびに、機器の老朽化により安定した運用が望めなくなってきた。そこで、NIFS–LANの全面更新を調整した結果、平成24年度と平成25年度において実施することになった。続く平成26年度は保守期限を迎えた電子メールシステムを更新した。

3.1.1 平成 24 年度

平成 24 年度は故障が発生した場合のキャンパス情報ネットワークへの影響の度合いを考慮し、まず基幹部のネットワーク機器の更新を優先して行った。

- 外部接続機構
- コアスイッチ
- エッジスイッチ
  - DMZ 用、管理用
- 支援統合サーバシステム
  - 仮想化サーバ、仮想化ストレージ（RAID 6)、バックアップサーバ
  - 対象サーバ：ネットワーク管理用サーバ(DNS, DHCP, ML, syslog 等)
  - サーバとストレージの接続方法：ファイバーチャネル（FC)
  - その他：UPS と連携し、停電時の自動停止、復電時の自動起動機能
- 免震ラック

3.1.2 平成 25 年度

続く、平成 25 年度はエッジスイッチの更新、ならびにセキュリティシステムの導入を行い、更新を完了させた。セキュリティについても、これまで懸念されていた検疫手続きの曖昧さと、ウイルスを含む多様化するマルウェアへの不安を各々専用システムの導入により解消した。

- コアスイッチ　10GbE ボートと光モジュールの追加
- エッジスイッチ
  - 各建物に設置
- 支援統合サーバシステムの増強
  - 仮想化サーバ 2 台追加、仮想化ストレージの HDD 追加　バックアップストレージの追加　FC スイッチ 2 台追加
  - 対象サーバ：監視サーバ、検疫認証システム、ログサーバ等
- 検疫システム
  - 検疫サーバとログサーバ
- 認証システム
- 標的型攻撃検知システム
- 免震ラックの追加
- 建物間光ファイバーの整備
- 建物内 UTP ケーブルの整備（研究 1 期棟）

3.1.3 平成 26 年度

平成 26 年度は、アプライアンスサーバでサービスを提供していた電子メールシステムの更新を行った。研究所向けにカスタマイズした電子メールサーバとワンタイムパスワード(OTP)サーバを、前年度までに導入した支援統合サーバシステムの仮想化システム上に稼

働させる方式を取った。さらに、保守期限を迎えた SSL–VPN サーバの更新を行い、新規に導入した OTP サーバを共用できるようにした。

- ワンタイムパスワード対応電子メールサーバシステム（メーリングリスト機能を含む）
  - 大容量添付ファイル送付システム
  - OTP サーバ
- SSL–VPN サーバ

3.2　情報ネットワーク設備の更新（免震ラックと通信ケーブル）

一般にネットワーク機器やサーバは 19 インチラックに収容されるが、これまで、これらを収容していたラックはシミュレーション科学研究棟が構築された当時のものであり、地震に対する備えが十分ではなかった。地震発生時にラックに搭載された機器を守ることは重要であるため免震ラックを導入した。ラック間の配線は、上部に設けたラダーを経由して行う。

今回のキャンパス情報ネットワークの更新では、コアスイッチと研究棟や実験棟などに設置したエッジスイッチ間を従来の 1Gbps から 10Gbps に増速するため、新たに建物間にシングルモードの光ファイバーを敷設した。これまで建物間接続においては、一部を除きマルチモード光ファイバーによる接続を行っていたが、既存の光ファイバーは 10GbE の規格である 10GBASE–SR に対してモード帯域幅が狭いため用いることができず、また、10GBASE–SR に対応するマルチモード光ファイバー（OM３）を敷設した場合でも最大伝送距離が 300m であり、遠方の建物については別途シングルモード光ファイバーを敷設する必要がある。シングルモード用の 10GBASE–LR 光モジュールは 10GBASE–SR 光モジュールに比べ高くなるが、光ファイバー自身のコストはシングルモードが安価であり、今後のメンテナンス性を考慮した結果、建物間接続に用いる光ファイバーはシングルモードに統一した。

エッジスイッチから各部屋の情報コンセントに提供する帯域も従来の 100Mbps から 1Gbps に増速される。研究所の多くの建物では、両者の接続にはカテゴリー5 の UTP ケーブルが配線されていた。UTP ケーブルを用いる 1000BASE–T の規格上の伝送距離はカテゴリー5e（エクステンデッド）を用いた場合が 100m と定められているが、その下位規格であるカテゴリー5 では定められていない。よって、確実に安定した帯域を利用者に提供するために、建物内 UTP ケーブルを 10GBASE–T にも対応するカテゴリー6 に更新した。平成 25 年度は研究 1 期棟を、平成 28 年度は研究 2 期棟、平成 29 年度は管理・福利棟の更新を行った。

3.3　外部接続機構とコアスイッチ

外部接続機構は SINET を結ぶアクセス回線を収容する L3 スイッチ[††]である。将来的に柔軟な接続方式を実現するために複数の 10GbE のインターフェースを持ち、ネットワーク間接続において経路を定める制御方式である BGP 対応とした。プライベートアドレスなどインターネットでは用いるべきでないアドレスをもつ通信はファイアウォールに入る前段の外部接続機構にて遮断される。

コアスイッチは NIFS–LAN の中心に位置する L3 スイッチであり、各建物に設置するエッジスイッチと接続を行う。制御部や電源などについては 2 重化しており、耐故障性を確保している。平成 24 年度はコアスイッチのみの更新であり、対向の各建物の既存のエッジスイッチの上流側が 1GbE のインターフェースであったため、コアスイッチの光モジュールも 1GbE 用の 1000BASE–SX や 1000BASE–LX を用意した。ところが、平成 12 年度に更新した旧型のスイッチとの接続が確立せず、次年度のエッジスイッチの更新まで、別途用意したメディアコンバータやスイッチを中継させることにより接続を維持した。なお、コアスイッチの更新作業に目途がついた時点で従来のコアスイッチの電源を切断したところ、その電源が故障したことからぎりぎりの更新であったといえる。

3.4　エッジスイッチ

これまでのエッジスイッチは上流 1Gbps、下流 100Mbps であったが、今回の更新で上流 10Gbps、下流 1Gbps の 10 倍の帯域に拡張した。従来のコアスイッチへの接続は 1 Gbps のリンクが 1 本あり、複数台設置する場合は 2 台まで各スイッチに 1Gbps で接続し、3 台目以降は既存のスイッチにぶら下がる形でエッジスイッチを増設した。そのため、上流とのリンクに障害が発生すると、そのリンク配下のスイッチ群は全て利用不能となった。新しいエッジスイッチでは上流のコアスイッチの接続も 10Gbps の回線を 2 本使ったマルチリンク接続を、コアスイッチのそれぞれ別のボードに接続する冗長構成を取った。また、エッジスイッチを複数台設置する箇所ではスイッチ間をまたがったマルチリンク接続を用いた。これにより片方のリンクに障害が発生しても帯域は半分になるが接続は維持される。

従来のエッジスイッチでは、利用者がネットワークケーブルを刺し間違えてループを作ることにより大量のパケットが発生し、これにより NIFS–LAN 全域に影響を及ぼすことがあった。新たに導入したエッジスイッチではループが発生した場合は一時的にそのポートを遮断し、ループが解消された後に自動復旧するループ検知機能を有する。現在でもまれにループを検出しているが、他のネットワークへの影響は見られない。

管理面においても今回導入したエッジスイッチは複数のスイッチを仮想的な単一のスイッチとみなす機能があり、予めグループ分けを行っていれば、個々のスイッチにログインしなくても、グループ全体をまとめて管理できる。特に特定の MAC アドレスがどのポートに

[††] レイヤー 3 スイッチ。ルータとも言われ、異なるネットワークを接続する機能を持つ。

接続しているかを調べるには、これまでは、該当 VLAN のエッジスイッチに個別にログインする必要があったが、今回の更新により、その手間は大幅に減った。

このエッジスイッチには、初回接続時に特定の Web ページを表示させる機能や端末が登録済みかどうか認証サーバに問い合わせる認証機能がある。3.6 節で述べる検疫認証システムを実現させるためには、この機能が必須であった。

3.5　支援統合サーバシステム

情報ネットワークは端末を集約するエッジスイッチやネットワークを管理する L3 スイッチが主体となるが、これだけでは運用することができない。それらだけでもインターネットへアクセスすることはできるが、例えば DNS サーバがなければ Web サーバに接続するには毎回 Web サーバの IP アドレスを入力する必要がある。また、DNS サーバ以外にも円滑な情報ネットワークを運用するために、電子メールやメーリングリストサーバ、IP アドレスを自動発行する DHCP サーバが必要であり、研究所では Linux などの汎用 OS 上で構築されたアプリケーションにより提供している。また、それらのサーバや各種機器にて生成されるログはログサーバにて集められる。従来のシステムではこれらのサービスを提供するためには、10 台程度の PC を運用していた。そのため、電気設備の法定点検による停電と復電作業においてはスタッフが総出で対応に追われ、また、予期せぬ停電時では個別に設置した UPS の残量を超えると電源断による強制停止の恐れがあった。

平成 15 年頃より、このような分散したサーバを統合する方法として、大型のシャーシに多数のカード型の PC を挿入するブレードサーバと、一つの物理的な端末を論理的に複数台の端末として扱う仮想サーバ技術が広まった。特に後者はハードウェア性能の飛躍的な向上により複数台の論理的な仮想サーバがサーバとして求められる十分な能力を提供できるようになり、物理的なリソースがあればごく短時間で仮想サーバの追加が行えるようになった。

そこで、研究所においても今回の NIFS–LAN の更新において、支援サーバ群を仮想化サーバ上に構築することとした。平成 24 年度は、仮想化サーバ 2 台、仮想化ストレージ 1 台を導入し、DNS や DHCP などの主要な支援サーバを仮想サーバへ移行した。仮想化サーバと仮想化ストレージ間はファイバーチャンネルで接続し、ディスク構成は RAID6 の冗長構成とした。さらに、バックアップサーバを用意し、定期的に仮想サーバのバックアップを取ることにした。同時に、UPS と連携する仕組みを導入し、停電時の自動停止、復電時の自動起動機能を導入した。

平成 25 年度は、3.6 節で述べる検疫認証システムを仮想サーバ上に導入するために、仮想化サーバ 2 台の追加と既存の仮想化ストレージのハードディスクドライブの追加を行った。これにより、いずれかの仮想化サーバに障害が発生した場合も、サービスを提供する仮想サーバを健全な仮想化サーバに移動させることによりサービスの継続が可能となった。また、仮想化サーバと仮想化ストレージとの間にはファイバーチャネルスイッチを導入し

両者の接続においても冗長構成を確保した。

その後、平成 26 年 3 月に 2 台目の仮想化ストレージの導入、バックアップサーバのストレージの増強、バックアップソフトウェアの導入を行い、平成 27 年 3 月には、電子メールシステムを仮想サーバ上に導入するために 2 台目の仮想化ストレージのハードディスクドライブの追加を行った。平成 29 年度では平成 24 年度に導入した仮想化ストレージが保守期限切れとなったため、これを更新した。

3.6 検疫認証システムとゲストネットワーク

検疫認証システムは前述の事前 MAC アドレス登録システムが発展したもので、検疫サーバにアクセスした際にダウンロードされるプログラムがその端末のセキュリティチェック[‡‡]を行い、問題がなければ自動的に検疫有効期間を延長するものである。これにより、確実に検疫が行われ、また、利用者は NIFS–LAN ならばどこでも検疫を受けられるようになった。この検疫認証システムは平成 26 年 9 月より運用を開始し、従来の検疫コーナーは検疫認証システムの運用開始後の同年 12 月に廃止した。

これまで来訪者向けゲストネットワークは会議室など限られた箇所でのみ接続できたが、動的 VLAN を導入したため、NIFS–LAN の全ての情報コンセントから利用できるようになった。研究者が情報コンセントに独自のハブを接続し複数台の端末を接続していても、端末毎にゲストネットワークと NIFS–LAN への接続の選択が可能である。

なお、運用開始後にいくつか改善点が見つかったため平成 28 年 3 月に改修を行った。主な改修点は登録された端末に対する MAC アドレス登録者の変更機能の追加、検疫期間内で検疫に失敗した場合でも検疫期限内ならば NIFS–LAN の接続を維持すること、ゲストネットワークからの登録と検疫の有効化などである。

3.7 標的型攻撃検知システム

近年のマルウェアの自己改変の速度にウイルス対策ソフトの定義ファイルの更新が追いつかず、結果として侵入の余地が拡大している。これらに対抗するために、機器内にサンドボックスと言われる仮想サーバ環境を持ち実際に流入してきた疑わしいプログラムを実行させることにより、マルウェアを検知する標的型攻撃検知システムが登場した。研究所でも 2.2 節で述べたように侵入検知システムを導入していた時期があったが誤検知が多く有効活用ができていなかった。一方、標的型攻撃検知システムは実際にプログラムを実行することにより判定するため、精度が高い。導入前に試験運用を行うなど、その機能を確かめ、平成 25 年度の更新時に導入を行った。現在も運用を行っており、やや過検知の傾向があるが、非常に良好な検知結果を得ている。

---

‡‡ サポート期限内の OS であること、OS のアップデートが適切に行われていること、ウイルス対策ソフトを有し、ウイルス定義ファイルが更新されていること。

その具体例として、平成 27 年 7 月に発生した事例がある。これは、所員が業務に関連するサイト（サイト A）をアクセスした際に標的型攻撃検知システムが警報を出したもので、担当者により、該当端末に対する所定のセキュリティチェックを行い、問題がないことを確認した。その数日後、文部科学省より、サイト A にセキュリティ上の問題が発覚しアクセスログを調査したところ、研究所の端末よりアクセスがあったが問題ないかとの照会があった。これに対し、すでに事象を把握しており、該当端末の健全性を確認したという明確な回答を速やかに行うことができた。

3.8　OTP 認証によるメールサービス

所員のアカウントを悪用され代表メールサーバがスパムメールの発信源となった過去の経緯から、パスワード漏えいによるスパムの発信源にならない対策を考慮した結果、平成 26 年度に更新時期を迎えていたメールシステムに SSL–VPN と同様の OTP を導入することとなった。メールサービスは SSL–VPN と比べ、対象者も利用頻度も多くなるため、OTP の導入に対し慎重な意見も出されたが、受注ベンダーのカスタマイズによりこれを実現することができた。SSL–VPN では小型のキーホルダー型トークンを使っていたが、常に携帯する必要があるため、名刺サイズの薄いカード型 OTP カードに切り替え、所内向け説明会を開催した後に、平成 27 年 10 月に運用を開始した。OTP 認証は Web メールにて行い、通常のパスワードの認証が成功した後に OTP カードに示される数字を入れる方式である。OTP 認証が完了すると、その端末からメールサービスが利用可能になる。メールクライアントソフトウェアで POP や IMAP によりアクセスする場合も一度は Web ブラウザ経由で OTP 認証を行う必要がある。この OTP 認証によるメールサービスは他には見られない研究所独自のサービスであったと思われる。

3.9　ファイアウォール

平成 29 年 10 月には、業務と関係のない Web サイトへのアクセスを制限する URL フィルタリングの運用を開始した。これは、所内のネットワークよりインターネットへアクセスする Web サイトを次世代ファイアウォールが有する機能で「オークション」、「ギャンブル」、「教育機関」、「ニュース」、「マルウェアサイト」など約 60 のカテゴリーに分類し、それぞれのカテゴリー別にアクセスの制御を行うものである。法律やモラルに強く反すると判断されるカテゴリーやセキュリティ的に問題があるカテゴリーについては、警告の画面を表示させ接続を遮断する。モラルに抵触する可能性があると判断されるカテゴリーについては注意喚起の画面を表示させる。これら以外については、通常のアクセスとする。この様なポリシーに基づいた URL フィルタリングを実施することにより、Web 閲覧中に悪意のある広告などからセキュリティ的に問題があるサイトへ自動転送されても、その閲覧を阻止することが可能となった。

3.10 アクセス回線

2.7 節で述べたように SINET へのアクセス回線は SINET 5 の運用開始時の平成 28 年 4 月より研究所にて用意する必要があった。そのため、平成 28 年度において愛知 DC と 10GbE で接続するアクセス回線を 2 年間の契約期間で調達した。全国各地に配備された SINET5 の DC は互いにメッシュ状に接続されるなど、SINET そのもののネットワークの信頼性は極めて高く設計されている。しかし、研究所から SINET を見た場合、アクセス回線が単一の障害箇所となる可能性がある。そこで、近隣の商用プロバイダの協力を得て、岐阜情報スーパーハイウェイの回線を利用し 100Mbps+のバックアップ回線を敷設した。バックアップ回線の経路制御は BGP により行い（マルチホーム接続)、商用プロバイダのネットワークを経由して岐阜 DC に接続している。平成 28 年 8 月に愛知 DC 向けのアクセス回線の終端装置に障害が発生したが、障害の間もインターネット接続はバックアップ回線経由で継続することができた。

その後、平成 30 年度から SINET 5 の運用終了予定の平成 33 年度末までの契約期間とする新規のアクセス回線の契約を平成 29 年度に行った。通常のインターネット接続用として 10GbE を 2 回線、L2/L3VPN[§§]接続用として同じく 10GbE を 2 回線用意した。インターネット接続用回線は岐阜 DC と商用プロバイダとの間で BGP によるマルチホーム接続を行い、SINET に障害が発生した場合は商用プロバイダ経由でインターネットに接続するよう設定した。現存の岐阜情報スーパーハイウェイ回線経由のバックアップも引き続き有効としている。もう一方の L2/L3VPN 接続用回線は岐阜 DC に対し直接 LAG 接続を行っている。この回線は、総研大関連の L2VPN と SNET[***]の L2/L3VPN が利用している。

3.11 情報セキュリティ講習会

情報セキュリティ講習会は平成 26 年度より所員を初めネットワークを利用する関係者全員が受講対象となった。近年の講演では外部講師による情報セキュリティの動向全般と、所内講師による所内の情報セキュリティ対策の変更点等が説明されている。全員が受講するため、同一内容の講習会を毎年複数回開催している。いずれも参加できない場合は、講習内容を撮影したビデオを閲覧することにより受講に代えている。平成 28 年度から講習会終了時に理解度チェックを行っている。

4 今後の課題

今後の課題として、情報セキュリティ緊急対応チームの確立と無線 LAN の展開などがあげ

---

§§ SINET が提供する広域 VPN 回線。閉域性を確保したセキュアな通信環境が得られる。

*** 編集 SNET タスク、「平成 17 年度 SNET（スーパーSINET 利用共同研究用ネットワーク）利用成果報告」、NIFS–MEMO–51、2006 年 11 月

られる。

4.1　情報セキュリティ緊急対応チームの確立

情報セキュリティ緊急対応チーム（Computer Security Incident Response Team、CSIRT）は、ウイルス感染などセキュリティインシデントが発生した際に被害を最小限にするために活動する情報セキュリティポリシーに明記された組織である。CSIRT が取り扱う活動には関係部署との連絡、被害状況の把握、インシデント発生の理由解明、事後対策が含まれる。2018 年 3 月に自然科学研究機構 CSIRT の設立と同時に核融合科学研究所 CISRT（NIFS–CSIRT)が設立されたが、具体的な対応方法が明文化されていない部分があるなど、情報セキュリティポリシーと共に整備する必要がある。技術的な面では、マルウェアの解析を含むフォレンジック調査を行う技能の取得が必要である。

4.2　無線 LAN の展開

2.5 節で述べたようにセキュリティを重視した結果、研究所内において無線 LAN はゲストネットワークのみ利用可能である。一方、無線 LAN の規格は順次改訂され、安全に接続するための技術は順次進歩している。また、接続が無線 LAN のみである端末も普及しており、研究活動において無線 LAN が必要とされるシーンも増えている。予算面や管理運用面などから早急な設置は行えないが、NIFS–LAN においても段階的に無線 LAN のアクセスポイントの設置を検討すべき段階にあると思われる。

4.3　その他

その他の課題として、保守期限を迎えるネットワーク機器の円滑な更新や業務運用の効率化が挙げられる。種々のクラウドサービスがすでに広く提供されており、必要に応じてこれらを活用することが考えられる。一方、大学共同利用機関法人として他機関との共同活動を念頭に置けば、技術的な裏付けなしに情報ネットワークを運用することは得策ではなく、先進的な技術を学ぶ機会の増加も課題としてあげられる。

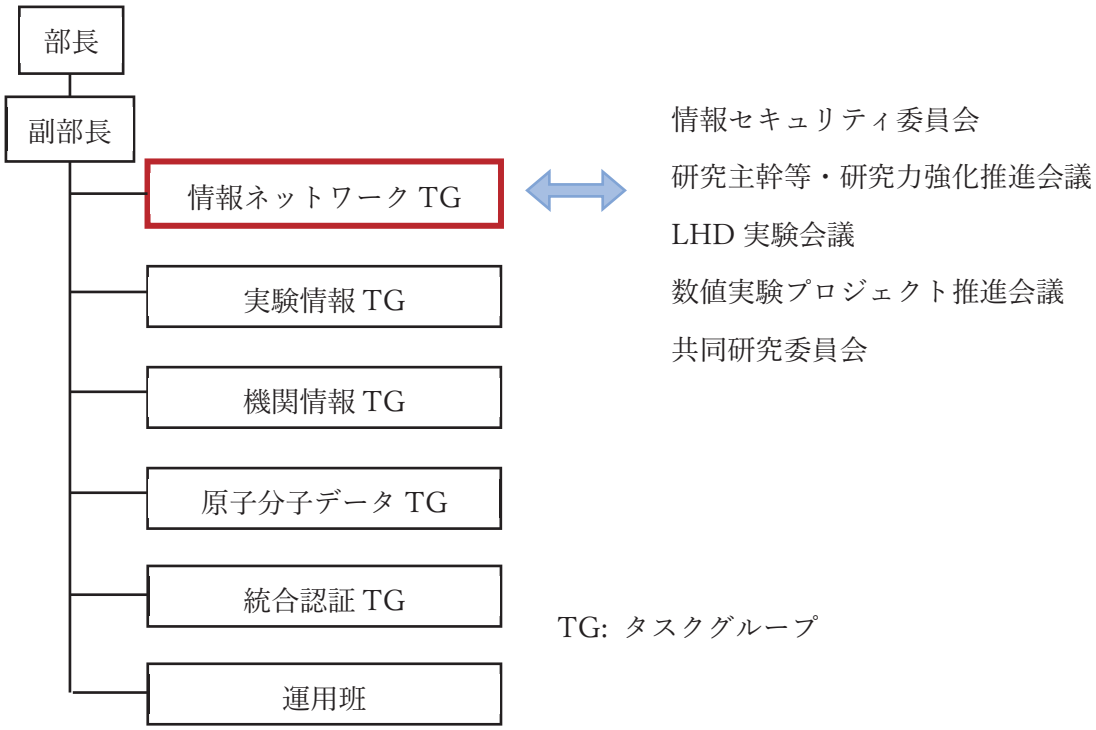
5　謝辞

着任時の計算機センターから現在の情報通信システム部情報ネットワークタスクグループに至るメンバーを初めとする所員の皆様の協力がなければ、このような強固なキャンパス情報ネットワークを作り上げることは不可能でした。深く感謝いたします。

（付録）

1　キャンパス情報ネットワークの運用組織

核融合科学研究所設立当初は計算機センターが NIFS–LAN、LHD–LAN 運用グループが LHD–LAN、理論・シミュレーション研究センターが PS–LAN の運用を担っていたが、組織の改編などを得て平成 25 年度に発足した情報通信システム部情報ネットワークタスクグループが一括して研究所のネットワーク全体の運用を担うこととなった（付表 1 、付図 1 ）。現在（平成 30 年 4 月）の情報ネットワークタスクグループは、研究部 4 名、技術部 3 名、管理部 1 名、非常勤職員 3 名（兼任を含む）の 11 名からなる。



付図 1. 情報通信システム部組織図

付表１．核融合研情報ネットワーク運用組織の沿革

平成元年４月	「核融合科学研究所」発足（名古屋市）
	大型ヘリカル装置建設（岐阜県土岐市に建設）推進母体として新たな大学共同利用機関となる
	• 計算機センター設立　大型汎用計算機と情報ネットワークを管理
９年７月	現在の土岐地区へ移転
同年９月	LHD 実験 LAN 運用グループ発足
同年 10 月	LHD 完成
10 年３月	LHD ファーストプラズマ
16 年４月	大学共同利用機関法人「自然科学研究機構」設立
	• 計算機センターが計算機・情報ネットワークセンターに改組
17 年 12 月	大型汎用計算機が LHD 数値解析システムに改称
19 年４月	シミュレーション科学研究部設置
	• 計算機・情報ネットワークセンターがシミュレーション科学研究部ネットワーク作業班と計算機作業班に改組
22 年４月	研究組織を改編統合、ヘリカル研究部設置
	• ネットワーク作業班がネットワーク管理運用室に改組、 LHD 実験 LAN 運用グループと統合
23 年４月	LHD 数値解析システムが LHD 数値解析サーバに改称
25 年４月	情報通信システム部設置
	• ネットワーク管理運用室が情報通信システム部情報ネットワークタスクグループに改組

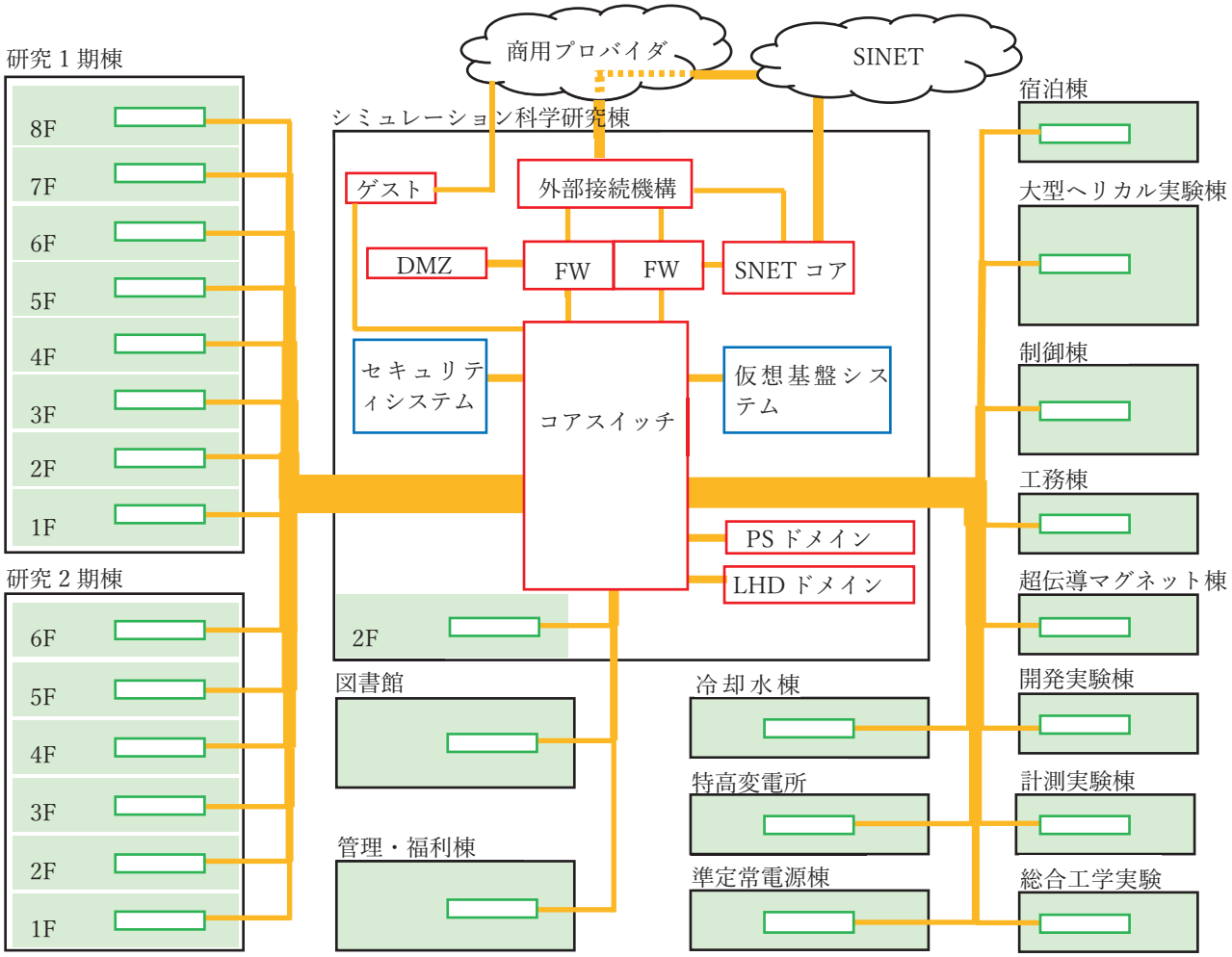
2　キャンパス情報ネットワーク導入作業とその接続構成図

平成 11 年度より平成 28 年度におけるキャンパス情報ネットワークの導入作業一覧を付表 2 に、現時点のキャンパス情報ネットワークの接続概要図を付図 2 に示す。

付表 2. キャンパス情報ネットワーク導入作業一覧

平成 11 年 6 月	サイトライセンスによるウイルス対策ソフトの導入
平成 12 年度	ギガビットネットワークの導入 • GPS 信号に基づく時刻配信サーバ（NTP サーバ）の導入
平成 12 年 6 月	ファイアウォールの導入
平成 13 年 10 月	ファイアウォールの運用ポリシーの変更
平成 14 年 3 月	侵入検知システム（IDS システム）の導入
平成 14 年 8 月	VPN サービスの導入
平成 16 年 2 月	アプライアンス型メールサーバの導入
平成 18 年 1 月	所外ネットワーク（現ゲストネットワーク）が商用プロバイダ経由となる
平成 18 年 8 月	SSL–VPN サーバの運用開始 • ワンタイムパスワード（OTP）の導入
平成 19 年 3 月	迷惑メール抑制システムの導入
平成 21 年 1 月	冗長構成を取ったアプライアンス型メールサーバの更新
平成 23 年 3 月	UPKI 電子証明書発行サービスへの参加
平成 23 年 12 月	次世代ファイアウォールの導入 SSL–VPN サーバの更新
平成 24 年 3 月	次世代ファイアウォールの冗長化
平成 24 年度	キャンパス情報ネットワーク（コアスイッチ）の更新 • 既存のエッジスイッチと 1GbE で接続
平成 25 年度	キャンパス情報ネットワーク（エッジスイッチ・セキュリティシステム）の更新 • エッジスイッチを更新し、10GbE x 2 で接続 • 検疫認証システムの導入 • 標的型検知システムの導入
平成 26 年度	メールシステムの更新 • メーリングリストサーバの統合 • 大容量添付ファイルの対応 • OTP 認証への対応
平成 26 年 4 月	サポート切れ OS に対する対応（マイクロソフト社 Windows XP）

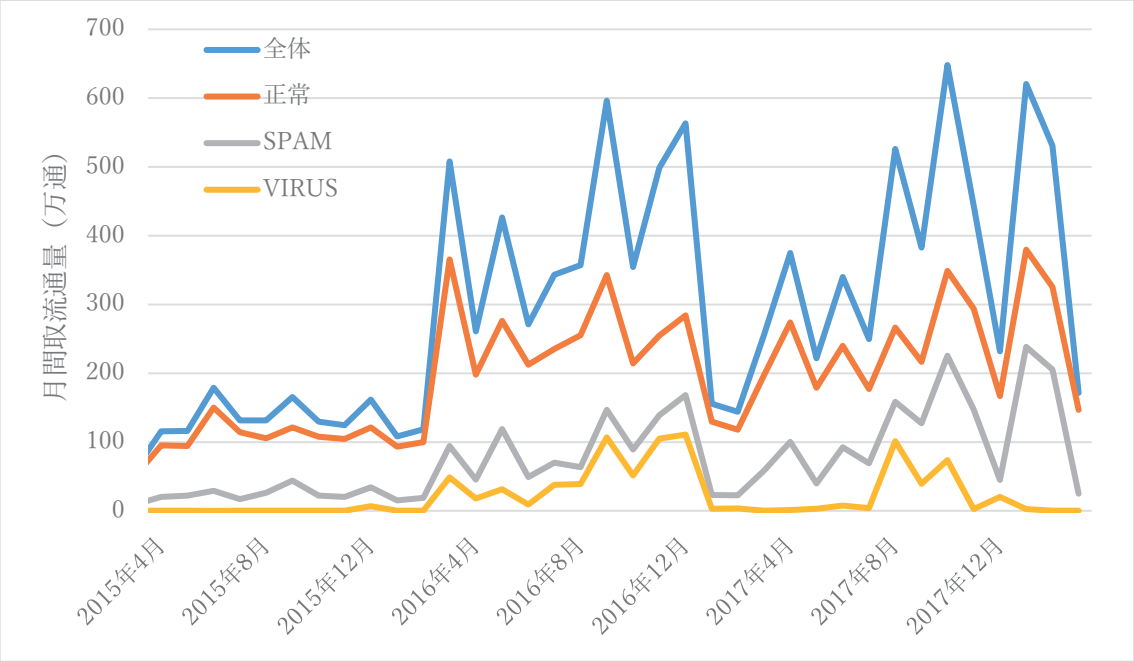
平成 26 年 9 月	検疫認証システムの運用開始
平成 27 年 8 月	ゲストネットワーク商用プロバイダの変更
平成 27 年 10 月	BGP バックアップ回線の導入
平成 27 年 10 月	SSL–VPN サーバの更新
平成 27 年 10 月	OTP を用いたメールシステムの運用開始
平成 28 年 3 月	検疫認証システムの改修
平成 28 年 4 月	SINET5 アクセス回線の導入
平成 29 年 10 月	URL フィルタリングの運用開始
平成 30 年 4 月	SINET5 アクセス回線の更新



付図 2．キャンパス情報ネットワーク接続概要図

3　代表メールサーバが取扱うメール流通量とスパムフィルターについて

代表メールサーバによるメールの月間流通量を付図 3 に示す。代表メールサーバは受信したメールを正常、SPAM（迷惑メール）、VIRUS（ウイルス付きメール）に判別し対応した処理を行う。2016 年 3 月から飛躍的に取扱量が増加しているが、これは SPAM の増加が一因にあることがグラフの形状より暗示される。全期間について、正常、SPAM、VIRUS 間の相関を求めた（付表 3）。正常と SPAM の相関係数が 0.89 であり、高い正の相関がある。正常なメールの流量は SPAM の流量とは無関係であることが想定されるが、SPAM の判別が不完全な場合、一部の SPAM を正常なメールと誤認する可能性があり、その結果として、両者に高い相関が出現したことが推測される。すなわち、現時点での代表メールサーバのスパムフィルターには改善の余地があることを示唆していると解釈できる。



付図3.　代表メールサーバの月間取扱い数。代表メールサーバでは受信したメールを正常、SPAM、VIRUS に区別する。

付表 3. メールの種別における相関行列

	正常	SPAM	VIRUS
正常	1.00	0.89	0.57
SPAM	0.89	1.00	0.57
VIRUS	0.57	0.57	1.00

4　他機関との交流

近年のセキュリティの攻撃は、これまでのハッカーの自己顕示欲から組織的な営利目的、テロ破壊活動等に目的が変わっており、より巧妙な手段を用いて行われるようになっている。これらに対応するには、高度な技術的手法の理解のほか、攻撃の意図の背景を含む適切な情報を先行して入手し、また、想定される被害を最小限にするためにも、関連する機関の担当者レベルからの交流が必要である。

4.1　共同利用機関におけるセキュリティワークショップ

まず、関連機関との連携として、「共同利用機関におけるセキュリティワークショップ（SWS)」があげられる。これは、普段、情報交換の機会が少ない大学共同利用機関特有の問題点について各機関の担当者が直接集い情報セキュリティ対策を中心に情報を交換し、ひいては、大学共同利用機関全体のセキュリティレベルの底上げをはかることを目的としている。平成 11 年に高エネルギー研究機構と国立天文台の呼びかけから始まり、核融合研は第 3 回から参加した。SWS は当初年二回の開催だったが、4 年目から年一回の開催となり、現在に至る。現在の主な参加機関は核融合研の他、高エネルギー研究機構、国立天文台、総研大葉山、岡崎三機関、理化学研、阪大レーザー研、阪大核物理研、高輝度光科学研究センターなどであり、最近では極地研、日文研、国立情報学研究所と JPCERT/CC が加わるなど国内の有力な研究機関のセキュリティ担当者が集っている。研究所は第 4 回（平成 12 年）と第 14 回（平成 22 年）においてホストとなった。SWS は各機関の情報セキュリティ担当者や情報ネットワーク担当者が直接顔をあわせ信頼関係の構築を行うことができ、各機関の個別の問題に対する有益な助言や、最新のセキュリティ状況の確認などを行うことができる貴重な機会である。複数の機関のセキュリティ対策を知ることにより、研究所の欠けている部分や弱い部分が具体的に知ることができ非常に有益である。実際に SWS に参加して得られた情報を元にウイルス対策ソフトウェアのサイトライセンス、アプライアンス型メールサーバ、次世代ファイアウォール、標的型攻撃検知システム等の導入の切っ掛けとなった。

4.2　岐阜市近郊ネットワーク懇談会

平成 13 年度に研究所が SuperSINET に参加した結果、所内に SINET への接続装置（ノード装置）が設置された。その後継である SINET3（平成 19 年度運用開始）において核融合研は、他の大学・研究機関を SINET へ接続する機能を有する岐阜県唯一の SINET ノード校となった。あわせて、研究所は岐阜県が運営する岐阜情報スーパーハイウェイを利用していたため、複数の機関が研究所を両者の接続地点として利用した。そのうち、一部の機関は研究所が設置したスイッチを利用して接続した（岐阜薬科大学、岐阜県研究機関、岐阜大学)。平成 23 年度に運用が開始された SINET4 では都道府県単位にデータセンター（DC）

が設置され、平成 28 年 4 月の SINET5 の運用開始とともに核融合研はノード校の役目を終え、それまで研究所を経由して SINET に接続していた各機関は DC 経由の接続に変更した。これらの経緯より平成 13 年より岐阜大学が主催する「岐阜市近郊ネットワーク懇談会」に参加するなどの情報交換を行っている。主な参加機関は、岐阜大、岐阜県総合企画部、情報科学芸術大学院大学、岐阜高専等の約 16 校であり、現在もおよそ年一回の懇談会が開催され、各機関の状況など情報交換を行っている。平成 27 年に設置した BGP バックアップ回線は、この懇談会において得た情報から設置したものである。

4.3 JPCERT コーディネーションセンター

JPCERT コーディネーションセンター（JPCERT/CC）とはセキュリティインシデントに対応する国内の代表的な組織である。付録 4.1 節の SWS において JPCERT/CC の参加者より、国民の社会活動に大きな影響を与える重要インフラ等の組織に対して情報セキュリティに関する脅威情報やそれらの分析・対策情報を中心とする早期警戒情報を提供する活動について紹介があった。研究所内の関係部署と検討した結果、この活動への参加を申し込むこととなり、JPCERT/CC のヒアリングを受け、参加が認めらた。これにより新たな質の高いセキュリティ情報を入手できるようになり、また、JPCERT/CC が緊急と認めた場合、担当者に直接連絡が来る体制を整えることができた。