４．情報基盤システムの整備と運用

４－１　ミッションと推進体制

総合メディア基盤センターは，前身に当たる総合情報処理センターの頃より，金沢大学基幹ネットワークの管理・運用と，共同利用計算サーバ，実習室等コンピュータシステムの管理・運用，各種 IT サービスの提供を行ってきた。これら情報基盤システムの運用は，総合メディア基盤センターの重要ミッションである。

情報基盤システムの運用は平成15年度から平成18年度まで情報基盤部門で行われていた。情報基盤部門は，平成 15 年４月の改組時点で教員は車古正樹教授のみであったが，同年 10 月に井町智彦助教（当時，助手）が，平成 18 年４月に大野浩之教授が着任した。平成 18 年度まで部門長は車古教授が当たっていたが，平成 19 年４月に車古教授は副センター長としての職務に専念するため部門業務からは退き，平成 19 年度現在の部門長は大野教授である。教員以外の人員として，技術職員，技術補佐員が部門業務を担当している，平成 15 年度の時点では西川直樹技術職員（当時，技官）が情報基盤部門の業務を担当しており，平成 16 年４月に松平拓也技術職員が着任した。技術補佐員は，平成 15 年度の時点では川崎礼子，中野三智子，小松崎由香の３名であったが，小松崎技術補佐員は平成 16 年３月で退任し，平成 16 年４月より原田真由美技術補佐員が着任している。平成 19 年度より，技術職員，技術補佐員は部門所属ではなくなり，上記５名に永井克郎技術専門職員（情報部情報企画課基盤整備第二係長）を加えた６名が，情報基盤整備を含むセンター全体の業務にあたっている。

４－２　中期目標における位置づけ

本学の中期目標の中で，本ミッションに関係する事項と，目標達成のために立案したセンター中期計画を以下に示す。

Ⅰ 大学の教育研究等の質の向上に関する目標

○　学生の立場に立って，自主学習を支援する教育環境を充実・整備する。

○　策定された教育目的・目標を実現するため，学生の自主的学習を支援する制度を整備する。

○　世界へ向けて情報発信する高度の学術研究を推進し，国際的に卓越した研究志向型の総合大学を目指す。また，環日本海地域を中心としたアジア地域におけるアカデミアとしての中核的研究大学として，社会との連携・協力を促進する。

○　研究に必要な学術研究資料，設備等の共同利用，有効利用を促進する体制を整備する。

対応するセンター中期計画

・	実習設備の充実	（計画：４－１）
・	無線ＬＡＮ環境を整える	（計画：４－２）
・	学生が PC を持ち込んだ場合について，安心して利用できるネットワークシステムの提案とシステム構築支援を行う	（計画：４－３）
・	学生のネットワーク利用環境の利便性向上	（計画：４－４）
・	各種セキュリティツールの統合管理ツール等，セキュリティ管理サイクル（設計・開発・運用）の各フェーズで用いるツールを連動させ，ユーザサイトに応じた適切なセキュリティ構築や運用管理を効率的に実現する調査開発と研究を行なう	（計画：４－５）
・	ネットワークの性能測定，ネットワークの障害・輻輳検出と維持管理，負荷や障害に対応した経路選択など実際的な管理方法の確立と実用性の検討を重要な課題として調査研究を行なう	（計画：４－６）
・	新しい技術基盤を前提としたネットワークについて，その特性と活用可能性について調査研究を行う	（計画：４－７）
・	学生・教員が遭遇する情報関連問題の解決サービスを行う	（計画：４－８）
・	学術交流・国際交流	（計画：４－９）

II 業務運営の改善及び効率化に関する目標

○ 全学的な大学改革を推進するために，業務運営の改善と効率化に努める。また，金沢大学の使命達成のための教育，研究，社会貢献に関する基本戦略を定め，その実現に必要かつ最適な資源配分システムと効果的・機動的な運営体制の確立及びその運用を図る。

対応するセンター中期計画

・	関連部局と連携して大学の各種インテリジェント化，及び IT 化支援等の企画調整を行い，研究教育の効率化を図る	（計画：４－１０）
・	全学的にはセンターを中心として Web の認証方式を確立し，管理運用の効率化を図る	（計画：４－１１）

・	トラブル，迷惑行為等に対する予防，対策体制を強化し，可用性の高いネットワークを提供する	（計画：４－１２）
・	学内向け IT サービスの提供	（計画：４－１３）

III 財務内容の改善に関する目標

○ 経費節減，効率的・合理的執行を推進する。

対応するセンター中期計画

・	常に最先端技術をフォローした情報基盤（コンピュータシステム，高速ネットワークシステム）を効率よく運営するシステムの改善及び各部局の情報機器の整備統合し，効率化を図る	（計画：４－１４）
・	附属図書館情報の電子化及びオンラインジャーナルなどの支援を行うと共に，コンピュータシステムの統合を促進し効率化を図る	（計画：４－１５）

V その他業務運営に関する重要目標

○ 教育研究等の活性化を目的に結成された「北陸地区国立大学連合」を強化し発展させる。

○ 長期間にわたって施設設備の安全確保と機能保全に努め，適切な施設 マネジメントを実施する。

○ 大学情報の一括管理及び戦略的活用のため，学術情報基盤の整備を進める。

対応するセンター中期計画

・	キャンパス間ネットワークの高速化を行う	（計画：４－１６）
・	常に最先端技術を取り込んだネットワークシステム，セキュリティシステム等などを維持し，不正アクセスの防止に努める。また構成員に対して啓蒙活動を行う	（計画：４－１７）
・	spam メール対策により迷惑メールの減少を図りメールによる障害の発生を防止する	（計画：４－１８）
・	新種ウィルスの発見を高め，ウィルス感染防御を強化する	（計画：４－１９）
・	不正アクセス等に対応できるセキュリティポリシーを確立させる	（計画：４－２０）
・	不正アクセスの調査解析を行い，社会的問題の発生防止，対処の迅速化に努める	（計画：４－２１）

・	ウィルス感染防止に努める	（計画：４－２２）
・	持ち込み PC によるウィルス感染などを防御する	（計画：４－２３）

４－３　センターのシステム

センターのシステムは，大別するとコンピュータシステム，基幹ネットワークシステム，インターネットサービスシステム及び利用者情報システムの 4 種類である。

コンピュータシステムは昭和 38 年に導入されてから 4-5 年ごとにリプレースし，現在のシステムは平成 19 年 3 月に導入した。

基幹ネットワークシステムは平成元年 12 月に簡易型イーサネットを初めて構築し，以降，平成 6 年 2 月 FDDI（Fiber-Distributed Data Interface）基幹 LAN，平成 8 年 3 月 ATM（Asynchronous Transfer Mode）基幹 LAN，平成 13 年 12 月ギガビット LAN を構築した。平成 6 年 2 月 FDDI 基幹 LAN の構築時からキャンパス間のデータ系と音声系を統合し電話網の内線化を実現した。平成 8 年 3 月に ATM 基幹 LAN を設置し，また平成 13 年 12 月のギガビット LAN の構築時に研究室に情報コンセントを設置した。

インターネットサービスシステムについてはメールサービスから始まり順次サービスの充実を図っている。

利用者情報システムは，利用者 ID（IDentifier）を一括に統合管理するシステムであり，平成 19 年 3 月に導入した。このシステムにより，センターのシステム毎に利用者 ID 管理を行っていたものが一括管理することが可能となる。なお，全学の利用者情報システムについては現在調査・検討中である。

４－４　コンピュータシステム

関連する中期計画：（計画：４－１３），（計画：４－１４），（計画：４－１５）

コンピュータシステムは主として教育用システムと教育・研究用システムから構成される。既存のシステム（広報　VOL.30, No.1,2006,P21-22）は平成 19 年 3 月にリプレースされた。この時のリプレースより，新システムは総合メディア基盤センターと附属図書館のシステムが統合された形となり，経費節減の一助を担うとともに，ユーザ認証のシステムが統合されるなどの効果を得ている。リプレースにあたり最善のシステムを導入するため，総合メディア基盤センターに導入されるシステムについては，岩原前センター長を統括責任者としたシステム仕様検討組織（データ：４－１）が設置された。システム仕様検討組織は次の 6 部会であった。

・ 並列計算機導入検討部会（岩原部会長）：並列計算機及び Grid computing 等の計算サーバ導入の可否を検討。

- 実習用パソコンシステム検討部会（佐藤部会長）：実習室のパソコンシステムについて検討。
- 教育支援用パソコンシステム検討部会（鈴木部会長）：総合教育棟内の教育支援用コンピュータシステムについて検討。
- PC 必携化支援用パソコンシステム検討部会（松本部会長）：PC 必携化に伴うパソコンシステムについて検討。
- 認証システム検討部会（車古部会長）：センター利用者 ID の統合認証システムについて検討。
- サーバ等システム検討部会（井町部会長）：旧システム等で設置されていた各種サーバについて検討。

上記検討部会で検討された結果を基に前センター長を委員長とした仕様策定委員会（センターのメンバー大野，井町）で仕様が策定され，表４－１のコンピュータシステムが導入された。

表 ４－１　システムの新旧対応表

システム	旧システム	新システム	検討結果
計算サーバ フロントエンドサーバ	1 式 2 式	1 式 2 式	従来の継承
実習用パソコンシステム 第 1 実習室 第 2 実習室 第 3 実習室 第 4 自習室 自然研分室 宝町分室 鶴間町分室	 62 式 48 式 62 式 40 式 80 式 15 式 15 式	 62 式 48 式 62 式 - 100 式 30 式 20 式	平成 18 年度からの PC 必携化に伴い総合教育棟に必携 PC を使用して開講できる教室が 2 教室準備されたためセンター内実習室を 1 室減とする。 他キャンパスの PC 数は分室の要望に基づき増設する。
教育支援用コンピュータシステム	なし	オープン PC 35 式 授業支援教員用 PC　2 式	総合教育棟エントランスと情報検索室に自習用 PC の設置 画面転送やファイル配布等が可能なソフトをインストールした教員用 PC を導入する.
PC 必携化に伴うパソコンシステム	なし	20 式	貸し出しあるいは講習会などに用いる PC を導入する。
認証システム	なし	統合認証システム 1 式	センターの認証に必要な利用者 ID を一括管理できるシステムを導入する。
サーバ等システム	メ　ー　ル　，	メ　ー　ル　，	従来の機能を継承し，利用

	WEB，DNS，ファイル，プリンター，NEWS/FTP 等	WEB，DNS，ファイル，プリンター，NEWS/FTP 等	増大による処理能力の増強するサーバを導入する.

1） 研究・教育支援システム（計算サーバシステム）

計算サーバシステムは演算サーバ 1 式とフロントエンドサーバ 2 式である。演算サーバには FORTRAN，C,NASTRAN などを導入した。フロントエンドサーバは演算サーバを利用するための言語の編集や NASTRAN の入出力として使用する。計算機利用登録人数は平成 14 年度に 1,279 人であったが平成 18 年度では 546 人と減少している。リプレースにあたり大型センターへの移行を含め廃止と継続について検討した結果，既存ユーザの移行作業の労力及び大型センターへの費用負担を考慮，継続することとした。継続にあたり従来は研究利用のみであったものを，利用効率を高めるため研究利用と専門教育利用を認める事とした。利用促進のため年 1 度アプリケーション利用講習会を開催しているが，今後の課題として広報活動にも積極的に取り組む必要がある.

2） 教育支援システム

関連の中期計画：（計画：４－１），（計画：４－4）

教育環境の整備のため実習設備の充実が重要である。このため前述した検討部会で教育環境について十分検討し教育支援システムが決定された。教育支援システムは下記から構成される。

- 講義専用の教室：センター内に演習室 2 室（各 62 式）
- 講義・自習用の教室：角間キャンパス南地区 1 室（100 式），宝町キャンパス 1 室（30 式），鶴間町キャンパス 1 室（20 式）
- 自習用の部屋等：センター内に自習室 1 室（各 48 式）とラウンジ（5 式），総合教育棟に 1 室（20 式）とラウンジ（15 式）
- 貸し出し用のノートパソコン 20 式
- 教員用パソコン：総合教育棟の情報コンセントが設置された B4,C10,F10 教室で教員の画面転送やファイル配布ができるパソコン 3 式
- 教育補助としてプリンターシステムや教育専用メール/WEB サーバシステム

平成 18 年度から携帯 PC 用教室が総合教育棟に準備されセンター内の演習室の使用が減少したため，リプレース時に演習室を 3 室から 2 室にした。2 室としたのは平成 18 年度の時間割を参考に検討した結果である。

パソコンのソフトウェアの OS（Operating System）は Windows と Linux のデュアルブートであり，アプリケーションは実習担当者にアンケートを取り共通教育科目に必要なソ

フトウェアについては全て導入，部局の専門科目については無償ソフトウェアについて全て導入，有償ソフトウェアについては部局で準備したものについて導入した。

ノートパソコンを除き約350式を利用者が常に同じ環境で支障なく利用できるよう毎朝1回パソコン管理サーバからマルチキャストでパソコンに必要なシステムを再配布している。再配布することにより現在のところ多数のパソコンがあるにもかかわらず利用にあたり混乱が生じていない。

表４−２，４−３はセンター内演習室の平成１９年度の時間割である。平成19年4月から第1実習室を第1演習室に第3実習室を第2演習室と改名した。

表４－２　第１演習室　平成19年度　時間割

前期	月	火	水	木	金
1 8:45-10:15					
2 10:30-12:00				日本語Ｂ 留セ／三浦	行動科学序論２ 文／小島
3 13:00-14:30		社会調査実習 文／田邊			
4 14:45-16:15	数値解析序論 理／長山	社会調査実習 文／田邊		計算数学１ 理／岩瀬	計算機言語１・２ 理／岩崎
5 16:30-18:00	計算数理序論 理／長山	情報処理基礎 理／岩瀬		情報処理基礎 薬／清水	計算機言語１・２ 理／岩崎

後期	月	火	水	木	金
1 8:45-10:15	計算機基礎論３Ａ 理／遠藤	プログラミング序論 工／笠原			
2 10:30-12:00				日本語Ｂ 留セ／三浦	情報処理演習Ｄ 総メ／井町
3 13:00-14:30		社会調査実習 文／田邊	応用情報処理演習 工／高橋	情報処理演習Ｄ 工／今村	計算機基礎論３Ｂ 理／岩瀬
4 14:45-16:15		社会調査実習 文／田邊			
5 16:30-18:00	応用情報処理演習 工／長谷川	応用情報処理演習 工／大西	応用情報処理演習 工／高橋	計算機基礎論３Ａ 理／奥寺	

表　４－３　第２演習室　平成19年度　時間割

前期	月	火	水	木	金
1 8:45-10:15				レポート作成 留セ／岡澤	
2 10:30-12:00		情報処理Ａ 法／岡田			行動科学序論２ 文／小島
3 13:00-14:30	情報処理Ｃ 法／岡田	心理学研究法 文／小島			
4 14:45-16:15			情報機器の操作 教／三好		心理学調査実習 文／岡田
5 16:30-18:00	情報処理基礎 工／児玉	情報処理基礎 理／長尾		情報処理基礎 薬／清水	心理学調査実習 文／岡田

後期	月	火	水	木	金
1 8:45-10:15		プログラミング序論 工／笠原		レポート作成 留セ／岡澤	
2 10:30-12:00			情報処理Ｂ 法／岡田		
3 13:00-14:30	情報処理演習 留セ／太田	心理学研究法 文／小島	計算機地球学 理／遠藤	総合演習 理／早川	
4 14:45-16:15	情報処理演習Ｄ 外セ／西嶋	計算機序論１ 総メ／佐藤	計算物理学 理／出渕	コンピュータ グラフィック演習 総メ／井町	
5 16:30-18:00		計算機序論２ 総メ／佐藤	計算物理学 理／出渕		

４－５　ネットワークシステム

A）　金沢大学のネットワーク取り組み

- 昭和 52 年に全国の大学に先駆け，城内キャンパスと小立野キャンパス間の 1.5Mbps の高速専用回線費を文部省に予算要求し認められ，小立野キャンパスにメインシステムを，城内キャンパスにリモートシステムを設置した。
- 昭和 54 年に京都大学と計算機同士を専用回線で接続した。
- 平成元年に kanazawa-u.ac.jp のドメインを取得すると共に，学内予算で全学的なイーサネット LAN を構築した。同年に BITNET に加入し，平成２年に N1 ネットを用いてインターネット接続をした。
- 平成元年に KAINS（Kanazawa university Academic Integrated Network System）設立推進委員会が統合ネットワークのあり方について検討し，学長に答申した。
- 平成 4 年から SINET によるインターネットの利用が開始され，その後，補正予算により平成 5 年度光ループ LAN（FDDI），平成 7 年度スター型 LAN（ATM），平成 13 年度ギガビット LAN が構築され現在に至る。
- 平成 5 年度の補正予算により，キャンパス間の音声系とデータ系を統合し，内線化した。

B）ネットワークの改善

関連する中期計画：（計画：４－１４），（計画：４－１６），（計画：４－１７），（計画：４－１９），（計画：４－２２），（計画：４－２３）

常に最先端技術を取り込んだネットワークシステム，セキュリティシステム等などを維持・改善やそれら設備に関する関連部局の支援も重要である。

- 平成 15 年度に SINET が 1 Gbps に増強されたのに伴い，対学外ファイアウオールを専用アプライアンスに更新した。更に，平成 17 年度末に対学外ファイアウオールを１式追加導入してクラスタリング構成とし，故障時等の通信障害への対策を強化した。
- 平成 16 年度に双方向遠隔講義のネットワーク設計を支援した。双方向遠隔講義用予算によりセンター内に高性能ルータを導入し大学のメインルータとした。また，総合

教育棟及び保健学科にマルチキャスト対応のルータが導入された。

- 平成 17 年度にネットワーク管理者の説明会を２度開催し ATM ネットワークシステムの撤廃やギガビットネットワークへの切り替えを行った。
- 平成 15 年度当時，角間キャンパスと医学部キャンパス，附属学校キャンパスとの間の通信速度はそれぞれ 40Mbps，1.5Mbps であったが，角間－医学部間については平成 16 年度末に 100Mbps，平成 17 年度に 1Gbps に，角間－附属学校間については平成 17 年度末に 10Mbps, 平成 19 年度より 100Mbps に, それぞれ回線を増強した。
- 平成 15 年当時，KAINS から学外への HTTP アクセスに使用する Web Proxy サーバは，２式のアプライアンス製品と１台のワークステーションから成る構成であったが，平成 16 年度に１式のアプライアンス製品を追加し，さらに，平成 17 年度にアプライアンス製品の保守が打ち切られたため ２ 式アプライアンス製品を導入した。Web Proxy の利用増大に伴い旧２式のアプライアンス製品は故障するまで利用することにした。平成 19 年度に旧２機のアプライアンス製品を２式分の能力のある１式のアプライアンス製品に更新する予定である。

ネットワークの更新を時代に即したものとすること，可用性の高い安全・安心のネットワーク維持・管理もセンターの重要な業務である。安全・安心してネットワーク利用できるための情報の収集や，設備の改善と可用性を高めるためのネットワーク改善や監視業務にも最大限の努力をしている。

一方，研究・教育支援及び業務支援のための計画・立案支援やインターネット利用サービスの充実にも積極的に取り組んでいる。

１） ネットワークシステム構成

現在のネットワーク構成は図 4-1 に示すように一般学内ネットワーク（KAINS-G：Global network system of KAINS），学内用認証ネットワークシステム（KAINS-I ： Internal authenticated network system of KAINS），学外者用認証ネットワークシステム（KAINS-E：External authenticated network system of KAINS），電話系ネットワークシ

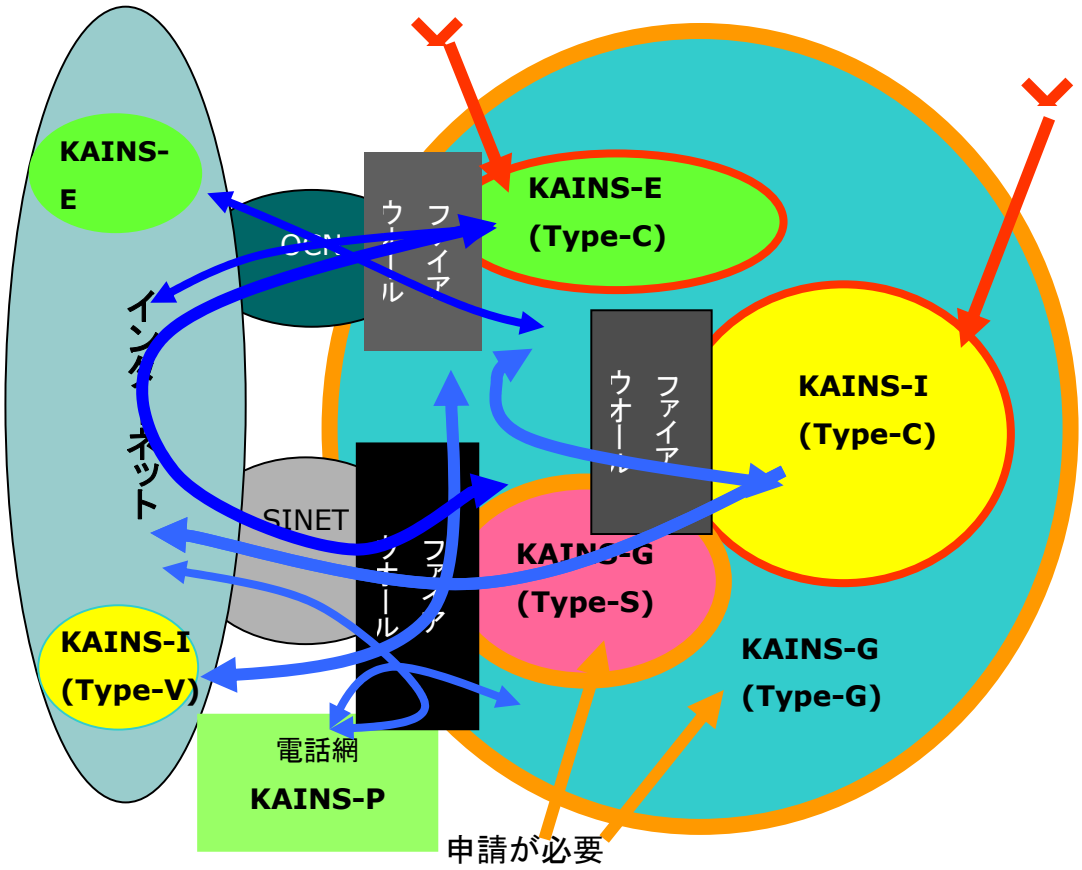

図４－１　ネットワーク概念図

ステム（KAINS-P: telePhone network system of KAINS）からなる。なお，基幹ネットワークの大部分のルータは平成 13 年度に導入したものであり，更新時期を迎えているため，平成 20 年度から 5 カ年計画で更新する案を事務局に提出した。

A）一般学内ネットワーク（KAINS-G：Global network system of KAINS）

一般学内ネットワークはグローバル IP（Internet Protocol）アドレス（133.28.xxx.xxx）が割り振られるネットワークであり，一般ネットワーク（KAINS-G(Type-G)）と Firewall DMZ（DeMilitarized Zone） 内の Secure ネットワーク（KAINS-G(Type-S)）からなる。

一般ネットワークは，平成元年にネットワークが構築されたときから存在する，グローバルネットワークアドレスを使用するネットワークである。今後の課題として，一般ネットワークはセキュリティ面で脆弱なため，接続できる情報コンセントの場所や，特定の目的

を持った情報機器のみを接続可能とする検討が必要である。

Secure ネットワークは, インターネットの利用に伴い不正アクセスが増大してきたため, 平成１2 年の早い段階でファイアウオール（外部用）を導入し，構築した。翌年の平成 13 年度にギガビット LAN の予算により，ファイアウオール（内部用）を導入し，各部局にも Secure ネットワークを構築した。

B)　学内用認証ネットワークシステム（KAINS-I：Internal authenticated network system of KAINS）

対応する中期計画：（計画：４－２），（計画：４－３），（計画：４－4），（計画：４－１７）

学内用認証ネットワークシステムはインターネット利用時にユーザ認証を必要とするネットワークであり，学内情報コンセント接続（KAINS-I(Type-C)）と学外 VPN（Virtual Private Network）接続（KAINS-I(Type-V)）からなる。

学内情報コンセント接続は, 平成 13 年度のギガビットネットワーク構築時に共有パソコンや携帯パソコン利用時に，インターネットを誰がどのようなサービスを利用したか記録収集できるファイアウオールを導入し，構築したネットワークシステムである。

このネットワークを平成１８ 年度からの PC 必携化に伴い学生が安心して利用できるネットワークシステムとネットワーク利用環境の利便性向上を目指し次のような活動をした。

- 無線 LAN 認証システム構築とレスポンス改善調査
- 内部ファイアウオールを平成 17 年度に専用アプライアンスに更新（情報教育部門の現代ＧＰの一環）。これによりバックボーンが 100Mbps から 1Gbps に高速化，教室用無線 LAN アクセスポイントを順次増設支援
- 総合教育棟の必携 PC 実習用の教室 B4,C10,F10 のネットワーク構築相談対応
- ブロードキャストストームによるネットワーク支障影響範囲の縮小のためのサブネットの再構成
- センター内実習室とラウンジに無線 LAN アクセスポイントの設置
- センター内に情報コンセントと電源を備えた自習室をオープン，自習室に Windows Vista10 式と MAC3 式を設置
- 無線 LAN 認証システムが Windows Vista 未対応でかつメーカの保守が打ち切られたため，独自で調査し対応

なお，平成 19 年から，Windows 端末の Update 情報とウィルス対策ソフトの更新情報によりインターネット接続の可否を決めるシステムを稼動する計画である。このコンセントはウィルス感染や不正利用等の発生時，ユーザ認証を行われる以前ではユーザを特定するのが困難であり，接続端末の MAC アドレス管理等の対策を検討する必要がある。

学外 VPN 接続は学外から学内とほぼ同様な利用を可能とするネットワークである。平成 15 年のサービス開始時のものはパソコンにクライアントソフトウェア（CheckPoint SecuRemote）をインストールする形態であり，利用可能な OS は Microsoft Windows 等，

特定のものに限定されていた。このため平成 18 年から Web ブラウザで利用できる VPN ゲートウェイ（f5 FirePass）を追加導入している。いずれの場合も通信は SSL により暗号化され，盗聴される危険の無い安全な通信が可能となっている。

C) 学外者用認証ネットワークシステム（KAINS-E ： External authenticated network system of KAINS）

対応する中期計画：（計画：４－９），（計画：４－１４），（計画：４－１７）

学外者用認証ネットワークシステムは，金沢大学に共同研究員として滞在する学外者や，学会・研究会で訪問した学外者が利用するネットワークである。このネットワークで利用する回線は平成 15 年からセンターが外部からのアクセステストやセキュリティチェックのため利用していた一般商用 ISP（Internet Service Provider）の OCN 回線である。平成 17 年に利用者認証スイッチ（Vernier AM6500, Vernier CS6500）とウイルススキャン機能付きセキュリティゲートウェイ（SGS5420）を導入し，VLAN（Virtual Local Area Network）を用いることで学内ネットワークを素通りさせて OCN 回線に仮想接続しているため，設備としては既存ネットワークを用いながら，参照元 IP アドレス（133.28.xxx.xxx）でアクセス制限される学内のみの情報が参照されることが無い。学外者用認証ネットワークシステムは，有線・無線のプライベート IP アドレスによる DHCP 接続環境で，アクセスポイントは学内に存在し，ユーザには通信経路上のゲートウェイを通過する際に L2TP（Layer 2 Tunneling Protocol）もしくは PPTP（Point-to-Point Tunneling Protocol）による認証を課し，通信ログをユーザ毎に取得している。

D)電話系ネットワークシステム（telePhone network system of KAINS）

電話系ネットワークシステムは，家庭や出張先から電話回線を利用して学内のネットワークに接続するネットワークである。平成 6 年にサービスを開始し現在に至っている。一般商用 ISP の発展により利用者は減少しているため廃止について検討中である。現状におけるこのネットワークのメリットは，一般商用 ISP を利用できない場所からの接続や，金沢大学の IP で契約している外部データベースの利用に使用できることである。

２）　ネットワークシステムとその管理・運用

関連する中期計画：（計画：４－１２）

ネットワークの利用が研究・教育や業務で日常的に利用されるようになった現在では，ライフラインの 1 つとして可用性の高いものでなければならない。したがって，センターでは重要ネットワークサーバの多重化やネットワーク機器の監視による障害等の早期発見に努めている。

A)ネットワーク機器・サーバの多重化

可用性を高めるために重要なネットワークサーバは多重化している。外部接続ファイアウオールのクラスタリング，学内の基幹ルータ 1 式の 2 重化，Web 参照のためのプロクシーキャッシングサーバの 5 重化，中継メールサーバ等の２－4 重化，ウイルススキャンサーバの２－4 重化がある。その他，学外との重要な接続機器で 2 重化は行っていないものについては故障時に短時間で修理できるよう，ハードウェア保守契約で対応している。2 重化については約 2 倍のコストが必要なため将来の検討課題である。また，部局等に設置してあるルータについては 1-2 式のルータを予備としてセンターに設置してある。

B)ネットワーク機器の監視

ネットワーク機器が正常に稼動しているか監視することはセンターに課せられた非常に重要な業務である。監視には機器が稼動しているか，サービスが稼動しているか，レスポンスが悪くないかなどがある。それらを下記の方法により監視を行っている。

・ ネットワーク自動監視装置（Peregrine Network　Discovery）による監視

この装置でルータ及び一段目の装置と重要ネットワークサーバ等を監視している。異常が発生した場合はメールで通知されると同時にネットワーク機器監視警告灯（業務管理室に設置）が点灯する。業務中であれば数人で監視しているため早期に対応できる。異常の場合は機器が設置されている部局の担当者と連絡をとりある程度の原因を見極め，当事者同士で復旧が困難と判断した場合は業者に連絡し対応する。

・ スクリプトを組み込んだ監視サーバによる機器及びサービス等の監視

センターが管理する大部分のサーバ等についてはサービス監視サーバ 3 式から定期的にサービスが機能しているか監視している（図 4-2)。サービスが停止している場合はメールで知らされると同時に平成 18 年度からモニターに表示（業務管理室に設置）する。業務中であれば数人で監視しているため早期に対応できる。

また，サーバのディスク容量不足で停止することのないように，サーバの空きディスク容量を定期的に監視し空き容量が 30%未満になった場合にメールで知らされる。これによりディスク容量不足によるサービス機能の停止を未然に防いでいる。

・ アプリケーションソフトによるデータ収集

利用者からレスポンスが悪いとの問い合わせがある場合，それに該当するネットワークのトラフィック容

図４－２　ネットワーク監視装置

量などのデータが重要である。このためトラッフィク容量を前述の Peregrine やアプリケーション MRTG（Multi Router Traffic Grapher）サーバで記録している。この情報によりブロードキャストストーム等が判断できる。MRTG の情報についてはセンターで日に 1 回程度監視している。また主要サーバについては，アプリケーション SmokePing を用いて ICMP（Internet Control Message Protocol）の応答時間を常時記録し，レスポンスの監視に役立てている（図 4-3）。

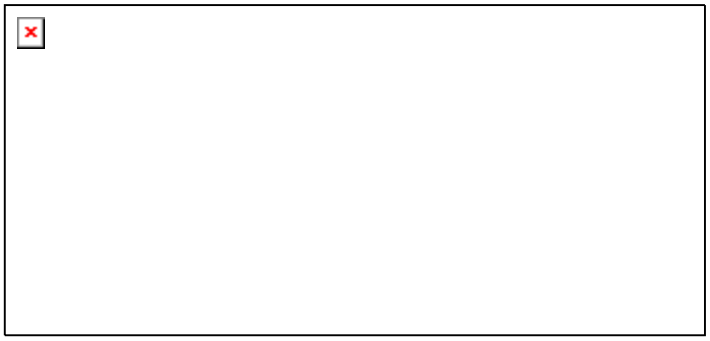

図４－３　SmokePing による ICMP 応答時間モニタの例

４－６　セキュリティ対策

関連する中期計画：（計画：４－１２），（計画：４－１７）

インターネットの利用に伴い，悪質な利用者や悪質なプログラムが増加している。トラブル，迷惑行為等に対する予防，対策体制を強化し安全・安心で可用性の高いネットワークを提供する必要がある。このためセキュリティ対策は大学において最大の重要課題である。セキュリティ対策についてはセキュリティポリシーの利用者への周知とネットワーク構成の両面から対策が必要である。

１）　セキュリティポリシー

関連する中期計画：（計画：４－２０）

当センターでは平成１２年にセンター内組織として情報セキュリティ対策専門委員会を設置した。この委員会でネットワーク利用に関する検討を行い，次の内規（データ：４－２）や，以下のガイドライン，手引き集，心得集などを作成した。

- 基幹ネットワーク管理に関するガイドライン
- ネットワーク管理者に関するガイドライン
- 外部ネットワーク管理者に関するガイドライン
- 情報コンセント管理者に関するガイドライン
- アクセス管理者に関するガイドライン
- 端末接続に関する手引き
- ネットワーク利用に関するガイドライン

・　ネットワーク利用心得

これに基づき次の業務が開始された。

A)ファイアウオールポリシーの設定業務

・学外ファイアウオールポリシー

学外からのアクセスに関しては，サーバ構築申請により許可されたサーバとする。

学内からのアクセスは特定のポート（135,137-139 など）を除き全て許可する。

ポリシーは状況に合わせ見直され現状では内部から 25（SMTP），P2P（Peer to Peer）で良く利用されるポートなどが追加される。

・認証ネットワークファイアウオールポリシー

外部からのアクセスに関しては，全て許可しない。

内部からのアクセスは http,https,smtp,pop3 など一般的に利用するポートのみ許可する。

B)稼動している端末を調査し，ネットワーク管理者に報告業務

ポートスキャンツール NMAP により年 2 回全端末の良く利用されるサービスポートを調査しネットワーク管理者に報告する。

C)サーバ構築書の審査業務

本学では，KAINS 上にサーバを構築する際には申請が必要であるが，その申請について情報セキュリティ的な問題等が無いかの審査を行っている。申請は Web 画面よりオンラインで行うことができ，審査についても Web 画面上に表示される情報を元に，使用している OS，サーバソフトウェアの種類，バージョンのチェックや，実際にサービスポートに接続しての稼動チェックなどを行っている。またユーザには年に 1 回の更新申請を義務付けているため，審査の作業は最低でも 1 年に 1 回発生する。サーバ構築申請の件数は，平成 19 年 3 月の時点で 841 件に上る。審査の作業を担当する人員は 2～3 名であり，セキュリティホール等に関する情報収集等も含めると 1 件あたりの審査には 15 分～数時間程度を要するため，申請が行われてから審査が完了するまでに数ヶ月を要する場合が多い。現在使用しているサーバ構築申請・審査システムは平成 13 年度に構築されたものであり，必ずしも現状に最適に合わない部分や作業効率の改善が見込める部分も存在するため，システムの抜本的な改善を現在検討中である。

その後，ウィルスの多発，P2Pの社会的問題化に対処するため，平成 16 年 2 月に「ネットワークセキュリティの強化に関して」を情報企画会議に提案し承認された。この規則にはネットワークの遮断措置についての諸条項が決められており，ウィルス感染や不正利用の検出時にセンターが通信の遮断を行う事について，全学的に認知された。

現在の金沢大学情報セキュリティポリシーは平成 16 年から 1 年をかけ検討・立案し，平成 17 年 4 月から施行された。金沢大学情報セキュリティポリシー（データ：４－３）は，金沢大学情報セキュリティに関する規程および情報セキュリティ方針と，遵守すべきルールを定めた対策基準（24 文書），ルールを遵守するにあたっての具体的項目をまとめた実施手順書（12 件）の，多数の文書からなる。

これらの見直し立案を，情報セキュリティ対策部会，ネットワークシステム管理部会に提示することも，センターの重要な業務である。

２）　セキュリティ対策ネットワーク構成と監視

関連する中期計画：（計画：４－２１）

不正アクセス，不正利用やウィルス感染などによりインシデントの被害者や加害者が出ないようにネットワークシステム構成を改善したり，各種ログの調査解析を行い，社会的問題の発生防止，対処の迅速化に努めることはセンターの最も重要な業務である。

A)不正利用・不正アクセスの監視

センターではファイアウオールのログを大型モニターに表示し２－3 人で監視する他，1 日 2 回程度ファイアウオールログの調査を行う。この監視や調査により端末調査依頼（データ：４－４）を月に数回ネットワーク管理者を通して利用者に通知し改善している。P2P 技術による自動ファイル共有やファイルダウンロードは禁止している。これについてもファイアウオールログの監視と侵入検知システム snort によるパケット解析により調査を行っている。この監視や調査により P2P 等と判断した場合は，当該情報機器の通信をファイアウオールで即時遮断し，「不審な通信の検出と通信遮断」（データ：４－５）としてネットワーク管理者を通して利用者に通知し，プログラムのアンインストール等の対策を依頼している。

端末調査依頼の大部分はプリンターの設定ミスや携帯パソコンの家庭環境の持ち込みによるものである。P2P 利用については留学生などに多いため，留学生に対するセキュリティ教育をどのように行うか今後の課題である。

B)ウィルス防御対策

関連する中期計画：（計画：４－１９），（計画：４－２２），（計画：４－２３）

メール系のウィルス

- 平成 13 年から学内及び学外からのメールについて，トレンドマイクロの Interscan Virus Wall を 7 式使用してウイルススキャンを行い防御していた。

・ 平成 15 年からはトレンドマイクロの Interscan Message Security Suite(IMSS)に更新し，外部用（学外→学内のメール対象）3 式と内部用（学内→学外・学内）4 式に分けて運用を行っている。検出されたウィルスメールについて，外部用では削除のみ，内部用では削除とセンターの担当者にメール通知を行っている。また，平成 15 年からウイルススキャンを通過した添付ファイル付きのメールを抽出し，調査の結果ウィルスと判断された場合は学内に注意を呼びかけている。なお，ウィルスと判断されるメールが 1 日以上続く場合は，メーカに献体し対応を要請している。

・ 平成 19 年 3 月からは学外からのメール到来経路最前段に Symantec Mail Security 8300（SMS）を導入し，2 段スキャンを行っている。後段の IMSS では一日に数件のウィルス駆除がされ，月に 2 度程一日に数十通のウィルスが駆除される。2 段スキャンは非常に効果があり 2 段化してから現在までウィルスと思われるメールが通過していない（データ：４－６）。学内の端末がウィルスに感染しウィルスを拡散させている