コンピュータネットワークシステム KAINS（第４期）の構築

仮屋一昭* ，永吉弘己*

Construction of the Computer Network System － KAINS

Kazuaki KARIYA and Hiromi NAGAYOSHI

当センターでは，研究業務と事務処理のための情報インフラであるコンピュータネットワークシステムKAINS(Kagoshima prefectural institute of industrial technology's Advanced Information Network System)を運用しているが，平成18年２月に第４期となるKAINSシステムを新たに構築し運用を開始した。

基幹ネットワークは，Windows Server 2003をファイルサーバに，Linux(RedHat)をインターネット関連サーバに設置して，伝送速度１Gbpsのファーストイーサネットを介して，クライアントパソコンを接続した。また，ネットワークセキュリティの問題に対応するために，アプライアンス型専用ツールを導入し，ファイアウォール，コンテンツフィルタリング，アンチウィルス，アンチスパム，不正接続防止・監視等の対策を行った。

Keyword :コンピュータネットワーク，LAN，情報セキュリティ，コンテンツフィルタリング，不正接続防止

１． 緒 言

平成12年に「IT基本法」が制定されて６年が経過した。この間に，高度情報通信ネットワーク社会の形成を目指して，インフラの整備が予想を上回る早さで進展し，現状では，世界で最も低廉かつ高速なブロードバンド環境が実現している。このようにして，インターネットは，生活の一部となり様々な利益を得ることができるようになった。一方では，セキュリティに関する問題も多く見受けられるようになった。総務省の平成17年情報通信白書によると，パソコンからのインターネット利用者のうち，平成16年にセキュリティに関する被害を受けた人は86.5%となっている。被害内容は，「迷惑メールの受信」が72.4%と最も多く，次いで「ウイルスの発見」(43.1%)，「ウイルス感染」(20.3%)となっている。

当センターにおいても，平成18年２月に情報セキュリティの確保を重要ポイントとしたコンピュータネットワークシステム第４期KAINSを構築した。本報告では，KAINS構築の基本的な考え方，ネットワークの構成，機能及び運用状況についてセキュリティ対策を中心に述べる。

２． KAINS構築の経緯

当センターでは，昭和62年の開所と同時に，図１に示すスーパミニコン(VAX)とパソコン端末により，DECnetプロトコルによる所内LANを構築した[1)]。その後，ネットワーク化，ダウンサイジングといったキーワードが流行した平成４年に，TCP/IPとIPXのマルチプロトコルによる図２に示すパソコンLAN(第１期KAINS)[2)]を構築した。第１期KAINSではインターネット（平成３年７月JUNETに参加）に接続し，すでに電子メールとネットニュースの利用を行っていた。その後のWWWの登場とWindowsへの移行により平成９年12月にTCP/IPプロトコルによるコンピュータネットワークシステム第２期KAINS[3)]を構築した。第２期KAINSは，当センターの研究業務と事務処理のための重要な情報インフラとなり，構築に当たっては，職員の要望と技術動向の調査を行い，システムの基本設計を行った。平成13年12月に図３に示すWindows2000Serverを基幹ファイルサーバとし，Windows2000Professionalをクライアントパソコンとした第３期KAINSを構築した。第３期KAINS構築時はCPUクロックアップが顕著に行われ，パソコン購入から数ヶ月も経過しない間に劇的に改善されたCPUを搭載したパソコンが登場した。現在では，CPUのクロックは３GHzを超えたあたりから限界に近づきつつあるようで，１チップ上に複数個の

図１ 昭和62年 VAX

*電子部

図２　平成４年　第１期KAINS

図３　平成13年　第３期KAINS

CPUを搭載したCPUが開発されるようになっている。このような中で，平成18年２月に図４に示す第４期KAINSの構築を行った。

３．KAINS構築の基本的な考え方

第４期KAINSを構築するに当たり，第３期までのKAINSの基本的な考え方に加え,次の事項を基本的な考え方とした。第３期までの基本ネットワーク構築方針を（１）から（６）に示す。

（１）通信プロトコルにTCP/IPを使用する。

（２）ファーストイーサネットスイッチを設置し，高速ネットワークを実現する。

（３）ネームサーバやメールサーバ，ニュースサーバ，WWWサーバ及びファイアウォールについては，機能性と信頼性の面からUNIXマシンとする。

（４）イントラネット関連のサーバは，WindowsNTマシンとし，クライアントからはネットワークドライブとして共有することから，信頼性を重視し，クラスタリングを行う。

図４　平成18年　第４期KAINS

（５）クライアントパソコンは，高速性もさることながらセキュリティと安定性が重要であることからWindowsNTマシンとする。

（６）ファイアウォールを設置し，セキュリティ対策を考慮したネットワークとする。

以上の基本方針のなかでオペレーティングシステム(OS)等は最新のヴァージョンを用いることにし，上記に下記（７）・（８）の項目を加えて第４期KAINS構築の基本的な考え方とした。

（７）ネットワークセキュリティの確保

従来からファイアウォールを設置し，セキュリティ対策を行ってきたところであるが，近年では，外部からの侵入やウィルス対策のみではなくスパムメール対策やコンテンツフィルタリングを行う必要が出てきた。また，データ流出の対策等を行う必要もある。このため，アプライアンス型の専用ツールを導入し，ファイアウォール，コンテンツフィルタリング，アンチウィルス，アンチスパム，不正接続防止・監視を行う。

（８）ファイルサーバの信頼性向上と共用ディスクの増加

最近の文書は，写真や図解を多用する傾向にあり，１文書のファイルサイズが飛躍的に増大している。このため，共用ディスクの増加とサーバの信頼性向上のためにFTサーバ(Fault Tolerant Server)を導入する。

４．KAINSの構成

図５にKAINSの構成図を，表１にサーバ類の仕様を示す。

４．１ ネットワークシステムの構成

イーサネットスイッチとサーバおよびクライアントパソ

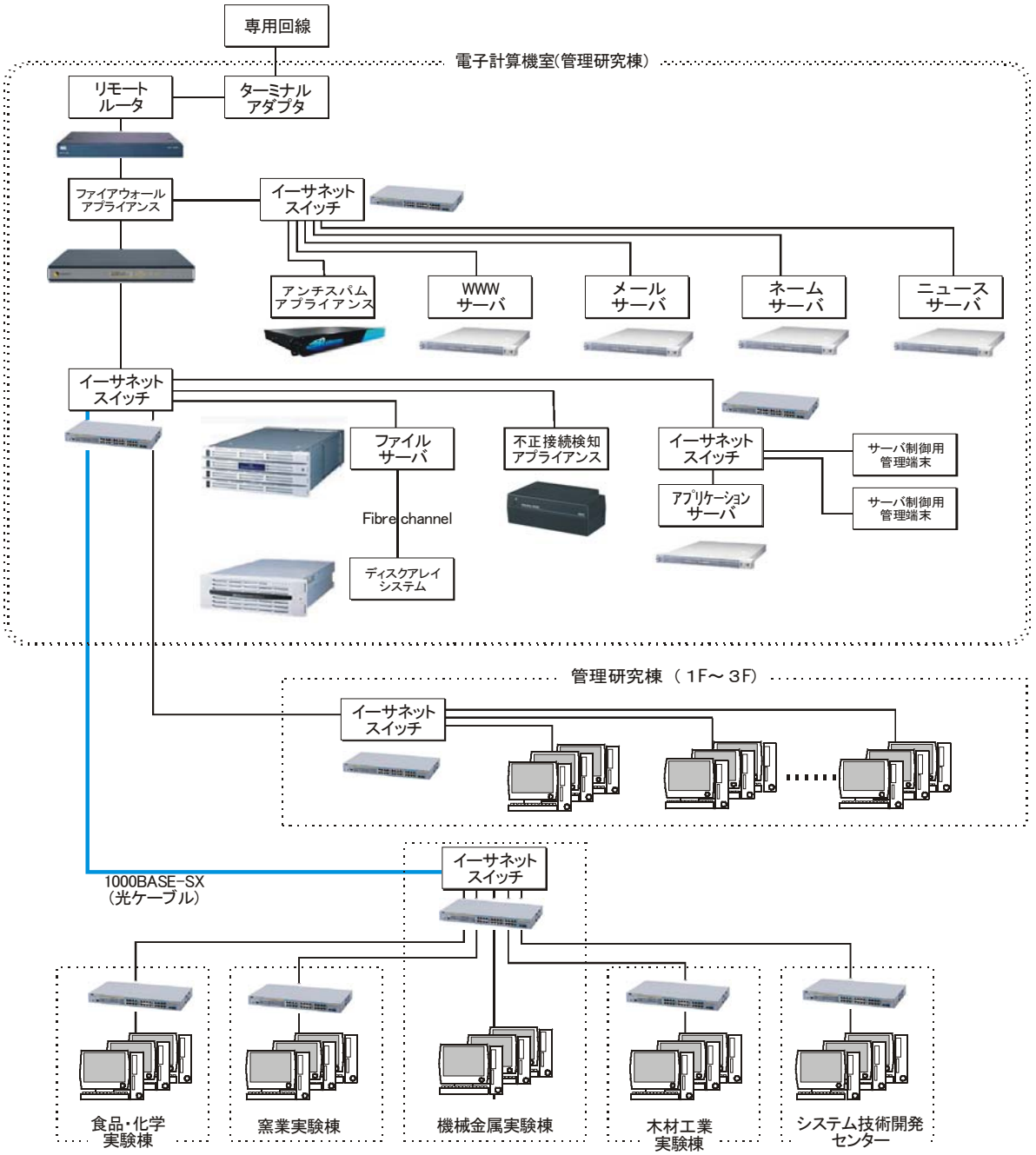

図５　第４期KAINSの構成図

表１　サーバ類の主な仕様

サーバ等		ファイルサーバ	アプリケーションサーバ	WWWサーバ メールサーバ ネームサーバ ニュースサーバ	クライアントパソコン
モデル		Express5800/320Lc-R	Express5800/110Rg-1	Express5800/110Rg-1	FLORA 330W(DG6)
CPU		Intel Xeon™プロセッサ	Intel Pentium4プロセッサ	Intel Pentium4プロセッサ	Intel Celeron D プロセッサ330
	クロック周波数	2.80GHz	3.20 GHz	3.20 GHz	2.66GHz
	二次キャッシュ	512KB	1MB	1MB	256KB
メモリ		1GB (DDR200)	1GB (ECC付きDDR2-533)	1GB (ECC付きDDR2-533)	512MB (PC2700)
内蔵HDD		160GB*2(RAID1)	160GB*2(RAID1)	160GB*2(RAID1)	40GB
インストールOS		Windows Server 2003	Windows Server 2003	RedHat Enterprise Linux	Microsoft Windows XP Professional(SP2)
備考		CPU・メモリ等は，二重化を行っているため、実際の搭載数(容量)の2倍。			

コン間は，1000Base-TXで接続した。また，管理研究棟と実験棟の接続には，距離の制約から1000Base-SXによる光ケーブルを使用した。５棟ある実験棟の中央部に位置する機械金属実験棟に光対応のイーサネットスイッチを設置し，ここから他の４実験棟へは，1000Base-TXで接続した。KAINSに接続しているコンピュータ類は，クライアントパソコンの他，研究報告サービス（メビウス）やCADシステム等が接続されている。これらのシステムは，100Base-TXで従来から接続されているため，イーサネットスイッチは100Baseと互換性を保ち，従来からあるシステムが支障なく運用できるようなネットワークにした。

外部との接続は，専用回線を介してインターネットに接続している。現在の通信速度は1.5Mbpsである。

外部ネットワークと内部ネットワーク間にファイアウォールアプライアンスを設置して，外部からの不正アクセスを不可能にした。

４．２ コンピュータシステムの構成

内部ネットワークは，Windows Server 2003をファイルサーバとして設置し，WindowsXPを搭載した53台のクライアントパソコンを設置した。

ファイルサーバは，文書や研究データの蓄積を行うために利用されるサーバであり，KAINSシステムの基幹をなすサーバである。このため，システムの信頼性を確保する必要から，CPU,メモリ，ハードディスク，PCIスロットなどのサーバが持つ主要なハードウェア・コンポーネントを二重化し，ハードウェアの一系統に障害が発生した場合にもシステムの連続稼働を実現することが可能な，フォールト・トレイラントサーバを用いた。CPUやメモリ，LAN,ハードディスクなどの主要なハードウェアを機能ごとにモジュール化し，万が一障害が発生した場合でも障害発生部分のモジュールを瞬時に切り離して処理を継続することが可能である。また，システムを停止することなく障害部分の交換が可能である。

記憶装置は，データの信頼性と，高速なアクセスを確保するために,Fibre Channelディスクアレイ装置を用いた。Fibre Channelとは，コンピュータと周辺機器を結ぶためのデータ転送方式の一つで，主に，高い性能が必要なサーバで，コンピュータ本体と外部記憶装置を接続するのに利用されている。機器の接続には同軸ケーブルか光ファイバーを用い,機器間の最大距離は光ファイバーの場合で10km,同軸ケーブルの場合で30mである。当センターでは，光ファイバーを用いてディスクアレイ装置と接続しており，高速データ転送が可能である。ディスクアレイ装置の実効記憶容量は1300GByteである。記憶装置の増大に伴って，バックアップ装置の容量が問題になった。従来からのテープ媒体を用いたバックアップ装置で，広く普及しているDDS(Digital Data Storage)やDLT(Digital Linear Tape)の規格では，DDSが最大で圧縮機能を用いて40Gbyte程度で，DLTでは70GByte程度であり十分なバックアップの容量を得ることができない。最近ではLTO(Linear Tape-Open)と呼ばれる規格が用いられ最大1.6TByteのバックアップ容量のものが見受けられるが，ディスクアレイ装置全体を一挙にバックアップを行うには，バックアップに要する時間が長すぎる欠点がある。このため，ファイルサーバにおいては，テープデバイスによるバックアップは行わず，データバックアップ用にディスアレイ装置（NAS，最大記憶容量1.6TByte）を別途用意して，バックアップを行うことにした。バックアップ作業は，なるべくデータアクセスのない時間帯に行うこのが望ましく，深夜12時からバックアップ作業を行うスケジュールにおいても，基幹業務開始前には終了できるようになった。

その他，アプリケーションサーバを設置し，ウィルス対策，不正接続防止・監視を行っている。

DMZ(DeMilitarized Zone)には，WWWサーバ，メールサーバ,ネームサーバ,ニュースサーバを物理的に４台設置し，また，スパムメール対策用アプライアンスを設置した。

５． システム環境の設定

システム環境については，基本的に第３期KAINSを踏襲しているため，基本理念は同一であるが，概要を示す。

５．１ ユーザとグループの設定

ユーザ名は，第３期KAINSで使用していたユーザ名をそのまま使用した。様々なアプリケーションとの互換性を考慮して８文字以内としている。ドメイン名はkains2006とし，グループ名には９つの職制上の部名を使用し，各ユーザごとに所属部に登録した。

５．２ フォルダ等の設定

ディスクアレイ装置は，所内の各ユーザが共通にアクセスし共有できるドライブ，グループ単位で共有できるドライブ及び各ユーザ単位でアクセスできるドライブの３つに分割した。第３期KAINSで使用していたファイルをそれぞれのフォルダにコピーした。

６． インターネットとイントラネット環境

ドメインネームサービスやメール，ネットニュース及び外部への情報発信用のWWW等の各サービスは，DMZ上の各サーバで行うようにした。ネームサーバはbind，メールサーバはpostfixとcourier imap/pop，ニュースサーバはinn，WWWサーバはApacheを使用した。また，サーバサイドスクリプト言語PHPにより行事予定や施設予約などの各機能を実現している。所内データベースは，Microsoft Accessを使用し，企業情報等の管理を行っている。データベースに

アクセスするために，VBScriptによるスクリプトを開発し入出力支援を行っている。

７．セキュリティ対策

第３期KAINSにおいても次のようなセキュリティ対策を行っていた。

（１）インターネットに接続するルータにパケットフィルタリングを設定し，不要なパケットが通過しないようにした。

（２）ファイアウォールにはFireWall-１を設置し，インターネット経由から内部ネットワークへのアクセスを不可能にした。

（３）内部ネットワークから外部へのWWWなどのアクセスは，squidによるプロキシサーバを経由して行うようにした。

（４）バリアセグメント上の各サーバとファイアウォールはrexecやrcpなどのリモートコマンドの記述を削除し，これらのサービスを使用できないようにした。

（５）この他，コンテンツフィルタリング，アンチスパム対策等も行ってきた。

これらのセキュリティ対策は，基本的にネットワーク管理者の定期的なメンテナンスが重要で，最近ではネットワーク管理全体の中でセキュリティ対策に費やす時間が占めるようになってきていた。近年では，セキュリティ対策をメインにしたアプライアンス型の専用ツールが多く販売されるようになり，これらの多くの機種ではメンテナンスの自動化や遠隔管理が行われるようになっている。このため，本システムでは，アプライアンス型の専用ツールを導入しネットワーク管理の軽減化を図った。

７．１　ファイアウォール，コンテンツフィルタリング，アンチウィルス対策

ファイアウォールは，シマンテック社製　Symantec Gateway Security 5400 Series(以後SGS)を導入した。SGSは，ファイアウォール，VPN，アンチウイルス，コンテンツフィルタリング，侵入防止等のセキュリティ機能を統合し，ハードウェアとソフトウェアが一体で提供されるアプライアンス製品である。またSGSは，プロキシ型ファイアウォールのため，HTTP，FTP，SMTP，POP3 などのアプリケーションのレベルで，攻撃や不適切な構文，異常キャラクタ，不正なコマンドなどの不審な部分が含まれていないかどうかなど，通信の内容をチェックできる構造となっている。

７．２　アンチスパム対策

メールは情報交換や事務連絡等のための主要なツールになっているが,無差別に送られてくる宣伝・勧誘メール(以後スパムメール）などでコミュニケーションツールとしての利便性が失われつつある。このため，送られてくるメールをフィルタリングしてスパムメールを隔離または削除する必要がある。このような機能を有するフリーのソフトウェアも多く存在するすが，本システムではBarracuda Networks 社製のBarracuda Spam Firewallを導入した。

７．３　不正接続防止・監視対策

インターネットからの侵入，ウィルス感染対策については，前述の対策を行っているが，ネットワーク内部からの侵入やウィルス感染については，脆弱さが残っていた。ネットワークへの接続を許可されていないパソコン（持ち込みパソコンなど）は，ウイルス感染の原因や，Winny（P2Pファイル交換ソフト）による個人情報の流出などの危険性を秘めているため，無許可パソコンを検知し，不正なアクセスを防止することで内部からのセキュリティを確保する必要があった。本システムでは，日本電気社製のInterSec/NQ30aを導入して，不正接続の監視と接続未許可パソコンの不正接続を防止している。

８．　運用状況

８．１　SGSの運用状況

セキュリティ対策ツールの中でSGSの機能であるファイアウォール,アンチウイルス,コンテンツフィルタリング,侵入防止等については，旧KAINSでも，それぞれ個別のツールを用いて対策を行っていた。このため，KAINSユーザからは，従来のシステムと同様の感覚で操作できている。コンテンツフィルタリングは，WEBサイトを約30種類のカテゴリに分類し，WEBサイトへのアクセスを禁止したいカテゴリを登録する仕様なっている。当センターでは，社会的に影響のある８カテゴリを登録している。さらに，各カテゴリは，得点による制限を加えることができる。禁止登録されたカテゴリでも利用したいサイトが含まれる場合があり，得点による制限で微調整を行っている。

８．２　Barracudaの運用状況

Barracudaによるスパムメール対策では，表２のような結果になっている。Barracudaが稼働し始めてから平成18年７月までの受信メール集計である。総受信件数197,670件の内，無条件に許可となっている件数が51,475件26％であり，全体の３/４は，スパムメールとなっている。

表２　受信メールの集計

拒否	132,879
拒否:ウィルス	87
隔離	4,994
許可:タグ付	8,235
許可	51,475
総受信件数	197,670

図６は，平成18年７月１日から７月25日までの日ごとの集計を表したグラフである。縦軸がメールの件数である。棒グラフの最上位の灰色領域が許可されたメールで他の領域はスパムメールである。この集計からもメールの３/４程度は,本来の情報伝達とは何ら関係のないメールである。最近のスパムメールは，巧妙化し本来のメールか判断ができないものも見受けられる。スパムメールのフィルタリング精度を上げることが今後の課題である。

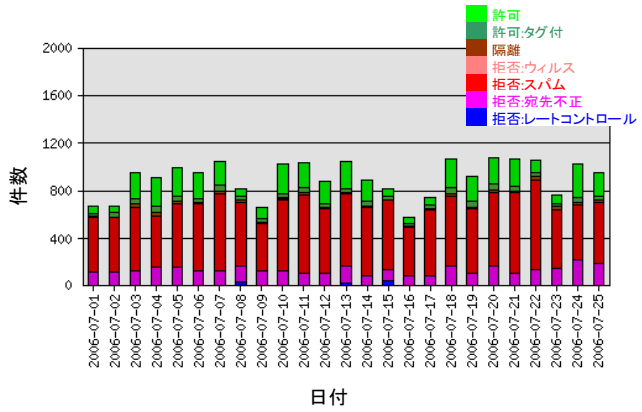

図６　受信メールの日ごとの集計

８．３　不正接続防止・監視ツールの運用状況

各職員が使用するクライアントパソコンについては，不正接続防止・監視サーバにIPアドレス，MACアドレスやその他必要項目を登録しているが，今回更新したクライアントパソコン以外にも多くのパソコンや計測機器が存在している。このため，KAINSに接続を希望するパソコンや計測機器等をあらかじめ示された様式に従ってネットワーク管理者に通知してもらい，許可されたパソコン等のみを監視サーバに登録した。登録されていないパソコン等はKAINSに参加できず，また，ネットワークに接続されたプリンタ等も利用できない。第３期KAINSの時期に，パソコン等の機器が増加し，IPアドレスの設定ミス等でアドレスの衝突が起き,ネットワークに障害が発生することが希にあった。このため，利用頻度の低いパソコンや計測機器等の接続はDHCP接続を行っているが，DHCP接続されたパソコンの管理が困難になっていた。本ツールによる不正接続防止は，KAINSに参加しているパソコンを確実に管理できるようになった。

９．結　　言

KAINS構築の基本的な考え方に沿って，ネットワークセキュリティを確保した第４期KAINSを構築できた。従来からのユーザマンインターフェースをそのまま踏襲し，ネットワーク基幹部分において，最新技術を導入できた。

運用開始から約６ヶ月経過した。現在では運用開始時にあった設定等の不備によるネットワーク障害等も発生せず，安定したネットワーク環境となっている。

今回は，セキュリティ対策にアプライアンス型専用ツールを３種類導入した。基本的にこれらのツールは，メンテナンスフリーを唱っており，どの機種もブラックボックス化されている。何も問題が発生していない場合や，通常の設定変更等では，快適な管理が行えるが，問題が発生した場合に内部仕様等がわからず，苦慮した場合があった。

コンテンツフィルタリングであるが，英語圏で構築された基本データベースを用いている。このとき，日本国内では全く問題にならないキーワードが，データベースに登録されている場合があるので注意を要する。ホームページ作成において，外国人が閲覧するためのホームページでなくても，ネットワーク上で活用されているセキュリティデータベースは，国外で構築された可能性が高いことを考慮する必要がある。

参 考 文 献

1)永吉ら：鹿児島県工業技術センター研究報告,**2**,121-124(1988)

2)永吉ら：鹿児島県工業技術センター研究報告,**6**,57- 62(1992)

3)永吉弘己：鹿児島県工業技術センター研究報告,**11**,35-40(1997)