

大阪大学におけるネットワーク環境の構築とその運用

原口 直大, 南 吉英

大阪大学 情報推進部 情報基盤課

haraguchi-n@office.osaka-u.ac.jp

minami-yo@office.osaka-u.ac.jp

概要：大阪大学総合情報通信システム (Osaka Daigaku Information Network System: ODINS) は、大阪大学におけるキャンパスネットワークであり、学内の教育研究活動を支える ICT 基盤である。本稿では、現在の ODINS の概要を説明し、特に今年度導入したシステムに着目してその特徴を述べる。さらに、ODINS が抱える問題として、利用者数の増加や提供サービスの拡大に伴う運用管理の複雑化を挙げ、現在取り組んでいる解決策を紹介すると共に、今後の展望について議論する。

1 はじめに

大阪大学総合情報通信システム (Osaka Daigaku Information Network System: ODINS) は、大阪大学のキャンパスネットワークであり、平成 25 年 5 月現在で教職員 9742 人、学生 25547 人を抱える大学の教育研究活動を支えている [1]。ODINS ではネットワークインフラとしての環境整備だけではなく、ネットワークを安全に保つためのセキュリティ強化装置の運用や、大阪大学のサーバ管理者等を対象に、情報処理技術向上を目的とした講習会の開催も行っている。本稿では、ODINS の構築経緯について説明し、特に今年度導入したシステムに着目してその特徴を述べる。さらに、ODINS が抱える問題として、利用者数の増加や提供サービスの拡大に伴う運用管理の複雑化を挙げ、現在取り組んでいる解決策を紹介すると共に、今後の展望について議論する。

2 ODINS に関する概要および構成

2.1 ODINS の沿革

1994 年に吹田および豊中の両キャンパス間を接続し、キャンパス間的高速通信を目的とした、第 1 期 ODINS の運用を開始した [2]。ODINS の沿革の概要を、表 1 に示す。

第 1 期 ODINS では、Asynchronous Transfer Mode (ATM) を導入することにより高速通信を可能とし、情報伝播の円滑化による業務の効率化を図った。1996 年度に運用を開始した第 2 期 ODINS では、インターネットの普及によるネットワーク利用の需要の増加に伴い、ネットワーク接続範囲の拡大、帯域の増強、ネットワークスイッチの増設といった、ネットワークの増強を行った。1999 年に運用を開始した第 3 期 ODINS

表 1: ODINS の沿革

| 日付 | 内容 |
|-----------------------|------------------|
| 1994 年 (平成 4 年) 3 月 | 第 1 期 ODINS 運用開始 |
| 1996 年 (平成 8 年) 8 月 | 第 2 期 ODINS 運用開始 |
| 1999 年 (平成 11 年) 3 月 | 第 3 期 ODINS 運用開始 |
| 2001 年 (平成 13 年) 11 月 | 第 4 期 ODINS 運用開始 |
| 2007 年 (平成 19 年) 10 月 | 大阪外国語大学 統合 |
| 2008 年 (平成 20 年) 4 月 | 第 5 期 ODINS 運用開始 |
| 2013 年 (平成 25 年) 4 月 | 第 6 期 ODINS 運用開始 |

では、キャンパスネットワーク整備が安定したこと、利用者から講義や講演会におけるマルチメディア化の要望が高くなった事を受け、ATM を利用したマルチメディア講義システムを導入した。マルチメディア講義システムは、単に開講される講義を遠隔地へリアルタイム配信するだけではなく、要求に応じて録画済み講義の再生やインターネットを経由した配信を行えるシステムであった。

2001 年に運用を開始した第 4 期 ODINS では、計算機の高速度化や高速通信に対するさらなる需要に対応するため、ネットワーク全体を、ギガビットイーサネットを用いて刷新した。また、本学に対する不正アクセスを始めとしたサイバー攻撃に対応するため、セキュリティ強化装置の導入を行った。

2008 年に運用を開始した第 5 期 ODINS では、第 4 期 ODINS の運用において課題となったネットワークスイッチの故障率増大や、ネットワークループや構成変更の煩雑さに対応するため、Open Shortest Path First (OSPF) 機能や、ネットワークループ防止機能を持つ機器を導入した。また、この頃に増加が問題となっていた迷惑メールへの対策として、Mail Transfer Agent (MTA) 型のアンチスパムアプライアンスを導入し、対策を希望する部局への適用を行った。加えて、無線 LAN に対する需要を受け、本学構成員を対

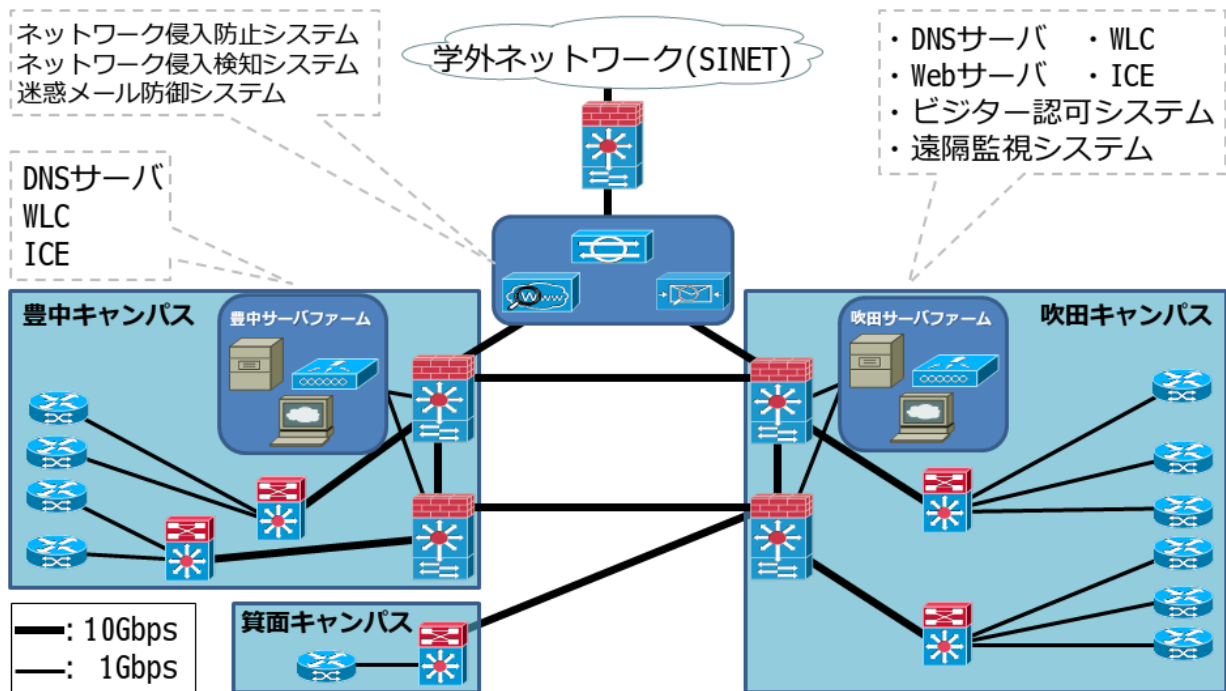


図 1: 大阪大学におけるネットワーク構成

象に、全学的にキャンパス無線 LAN システム環境の整備を行った。学外の訪問者に対しては、キャンパス無線 LAN システムの一時利用をするためのアカウント発行システムである、ビジター認可システムを構築した。

2013 年より運用を開始した第 6 期 ODINS では、キャンパス無線 LAN システムの提供範囲の拡大を行った。また、不正侵入防止システムの導入や、アンチスパムアプライアンスをキャンパス全体に適用するために、MTA 型から透過型に変更し、セキュリティの強化を行っている。

2.2 ネットワーク構成および提供サービス

現在の ODINS の主なネットワーク構成を、図 1 に示す。本学では、ネットワーク規模の大きな吹田キャンパスと豊中キャンパスに、基幹となるコアスイッチを 2 台ずつ設置し、冗長化構成を取っている。

表 2 に、ODINS が過去に提供していた、および現在提供している第 5 期 ODINS までのサービスとその提供時期を示す。

第 1 期 ODINS では、メールサーバや DNS サーバといった現在のネットワークの基盤となるサーバ群を、ネットワークサーバシステムとして導入した。また、データベース検索や文献検索、文書処理などの広範なサービスをどこからでも利用可能とする共通ユーティリティサービスを展開している。加えて、ATM を利用したネットワークの整備により、図書館文献情報や教

育用システム、スーパーコンピュータを遠隔で利用可能となった。第 3 期 ODINS で整備したマルチメディア講義システムについては、ATM を利用することが前提であったこと、また、より安価で操作性の高い製品が市場に提供され始めたことに伴い、2001 年にサービス提供を終了した。

第 4 期 ODINS では、ギガビットイーサネットを利用したネットワークの整備、ネットワークセキュリティ監査装置やメール監査装置、VLAN 管理用装置といったセキュリティ強化装置、不正アクセス防止装置など、現在も継続運用しているサービスの前身として整備を行った。この整備によって、本学が抱えていたセキュリティに関する問題や高速通信に対する要望は改善された。

加えて、第 4 期 ODINS 運用中である 2005 年度より、大阪大学のサーバ管理者等を対象に、情報処理技術向上を目的とした講習会の開催も行っている。開催した講習会として、Linux や Windows サーバ管理者を対象にしたセキュアなサーバ構築に関するものや、本学構成員を対象にしたコンピュータやネットワーク利用におけるセキュリティに関するものが挙げられる。今年度についても、本学のセキュリティ性向上の為、Linux サーバに関するセキュリティ講習会の開催を予定している。

第 5 期 ODINS では、拡大するネットワークの運用および管理に多大な労力を有することから、ODINS 管轄の装置の監視を行うネットワーク管理システムの導入を行った。ネットワークの監視が行えるようになっ

表 2: ODINS が提供するサービス

| サービス名 | 開始時期 | 更新時期 | 終了年 |
|-----------------------|-------------|----------------|--------|
| ATM を利用したネットワーク | 第 1 期 ODINS | 第 2 期 ODINS | 2001 年 |
| ネットワークサーバシステム | 第 1 期 ODINS | 随時 | - |
| 共通ユーティリティサービス | 第 1 期 ODINS | - | - |
| マルチメディア講義システム | 第 3 期 ODINS | - | 2001 年 |
| 不正アクセス防止装置 | 第 4 期 ODINS | 第 5, 6 期 ODINS | - |
| ギガビットイーサネットを用いたネットワーク | 第 4 期 ODINS | 第 5 期 ODINS | - |
| セキュリティ強化装置 | 第 4 期 ODINS | 第 5, 6 期 ODINS | - |
| 講習会の開催 | 第 4 期 ODINS | 随時 | - |
| ネットワーク管理システム | 第 5 期 ODINS | - | - |
| キャンパス無線 LAN システム | 第 5 期 ODINS | 第 6 期 ODINS | - |
| ビジター認可システム | 第 5 期 ODINS | - | - |

たことから、ネットワーク障害に対して迅速に対処することが可能となり、ネットワーク障害の影響を抑える事を可能とした。

3 第 6 期 ODINS 整備の概要と問題点

本節では、第 6 期 ODINS 整備によって導入されたサービスについて説明し、運用面において発生している問題点とその解決策について議論する。

3.1 第 6 期 ODINS について

第 6 期 ODINS で導入したサービスについて、表 3 に示す。

表 3: 第 6 期 ODINS で導入したサービス

| サービス名 | 備考 |
|------------------|-----------------|
| キャンパス無線 LAN システム | 第 5 期 ODINS の拡張 |
| ネットワーク侵入防止システム | 第 5 期 ODINS の拡張 |
| ネットワーク侵入検知システム | 第 5 期 ODINS の拡張 |
| 迷惑メール防御システム | 透過型へ変更 |
| ネットワークサーバシステム | 随時更新 |

第 6 期 ODINS では、第 5 期 ODINS の整備によって安定化したネットワーク運用を前提とし、新たなサービスの提供を中心として整備を行った。また、運用負担の軽減のためのシステム導入を行った。不正侵入防止システムの導入や不正侵入検知システムの性能強化を行い、セキュリティ性能が向上した。以下では、現在問題となっているキャンパス無線 LAN システム利用者増加に伴う業務負担、および透過型アンチスパム

アプライアンスの導入と問題点について、それぞれ 3.2 項、3.3 項で述べる。

3.2 キャンパス無線 LAN システム利用者増加に伴う業務負担

ODINS では、大学構成員および来訪者のネットワークアクセス環境の向上を目的とし、第 5 期および第 6 期 ODINS の整備によって、キャンパス無線 LAN システムを導入した。平成 25 年 10 月現在、424 台のキャンパス無線 LAN システムのアクセスポイントが設置されている。提供範囲拡大に伴い、利用者数が増加している。キャンパス無線 LAN システムのアクセスポイント数および利用者数の推移について、表 4 に示す。

表 4: キャンパス無線 LAN システムのアクセスポイント数と利用者数の推移

| 年度 | アクセスポイント数 | 年間利用者数 | |
|------|-----------|---------------|--------|
| | | IEEE802.1x 認証 | Web 認証 |
| 2008 | 28 | 1 | 1 |
| 2009 | 100 | 1 | 565 |
| 2010 | 128 | 9643 | 1682 |
| 2011 | 195 | 16931 | 3378 |
| 2012 | 292 | 18963 | 6105 |
| 2013 | 424 | 8153 2 | 7473 3 |

表 4 に示した年間利用者数は、一日あたりの利用者数を年間毎に合計し、IEEE802.1x 認証と Web 認証別に示したものである。1 については、ログを統計解析に用いる予定ではなかった事、サーバ更新に伴いデータが誤って削除されてしまった事に伴い欠損している。2 については、2013 年 4 月 1 日から 9 月 30 日までの集計となっている。3 に関しては、2013 年 4 月 1 日から 6 月 30 日までのログが削除されていた

事に伴い、7月1日から9月30日までの集計となっている。

表4の通り、キャンパス無線LANシステムのアksesポイント数と利用者数は増加傾向にあることがわかる。

提供範囲拡大および利用者数増加に伴い、キャンパス無線LANシステムへの接続方法、アksesポイント設置場所、電波の安定性や接続に伴い発生したエラーなどに関する問い合わせが増加しており、運用における大きな負担となっている。操作方法やアksesポイント設置場所に関する情報は、説明会やWebページを通じて利用者へ提供している。接続に伴い発生したエラーに関する問い合わせは多岐にわたり、ODINS運用担当が事前に把握していない問題も多い。下記に実際に起こった問題の例を示す。

- Web認証を用いた接続に関する問題
- DHCPによってIPアドレスが適切に割り振られない問題
- 使用するSSIDの間違いといった、使用手続きの問題
- DNSサーバのIPアドレスの設定に関する問題

特に多く寄せられた問い合わせとして、Web認証を用いた接続に関する問題が挙げられる。通常、Webブラウザを用いて80番ポートへのHTTP通信を行った際に、自動的に認証ページへリダイレクトされるが、特定のセキュリティソフトが、HTTP通信のリダイレクトを許可していない事があり、正常に認証ページが表示されないことがある。このような挙動はODINSのシステムではなく、利用者のパソコンのOSや導入されているソフトウェアが原因となって発生するため、原因の特定と解決が困難である。本件に関しては、Web認証を用いたキャンパス無線LANシステムの利用マニュアルに特定のセキュリティソフトの設定によりHTTP通信のリダイレクトを許可していない事がある旨を明記し、利用者に対して一時的にセキュリティソフトの機能を切るか、HTTP通信のリダイレクトの許可設定を行うことを周知している。

また、今まで接続出来ていたのに急に接続出来ないという問い合わせに対して、利用者のパソコンの状況を確認した所、キャンパス無線LANシステムから割り振られるIPアドレスが、予期しているものと異なっていることが分かった。確実な理由の特定には至っていないが、利用者がキャンパス無線LANシステムを利用した環境の電波状況や、ODINSが整備していない無線LANアksesポイントから発せられる電波などの干渉により引き起こされたものと考え、継続調査

を行っている。この問題については、利用者が一度IPアドレスを解放し再接続を行う事で解消している。

使用手続きに関する問題は、スマートフォンなど、キャンパス無線LANシステム利用マニュアルに記載していない端末やOSに対して適宜対応を行い、マニュアルを作成し配布を行った。キャンパス無線LANシステムでは、DNSサーバのIPアドレスを含め、自動設定での利用を指示している。しかしながら、利用者側でDNSサーバのIPアドレス設定などを行っていた場合、DHCPによってIPアドレスが適切に割り振られない問題が発生している。この場合も、キャンパス無線LANシステムの利用マニュアルを案内すると共に、DNSサーバのIPアドレス設定を、自動設定となるよう促している。

キャンパス無線LANシステムに関する他の課題として、来年度に本学構成員となる方を対象とした、利用方法の周知が挙げられる。利用者からの問い合わせを総合すると、キャンパス無線LANシステムの存在は認知しているが、利用方法が不明であったり、ODINSの存在やキャンパス無線LANシステム利用マニュアルの配布先を知らないといった問題が浮き彫りとなった。そのため、今後はODINSに関するサービスの周知方法やキャンパス無線LANシステム利用マニュアルの配布方法について検討を行う必要がある。

3.3 透過型アンチスパムアプライアンスの導入と問題点

第5期ODINSでは、MTA型のアンチスパムアプライアンスを対外ネットワークとの接続点に設置し、迷惑メール対策を行っていた。しかしながら、MTA型のアンチスパムアプライアンスを利用するために、導入する部局のネットワークに応じた、DNSの設定を行っていた。また、本学ではグレイリスト方式と呼ばれる迷惑メール判定方法を用いていた為、メール配送に遅延が発生していた。加えて、正常なメールについても迷惑メールとして削除される可能性があったことから、ホワイトリスト登録作業が発生し、大きな業務負担となっていた。

これらの問題を解決するために、第6期ODINSでは、透過型アンチスパムアプライアンスを導入した。透過型の導入に伴い、MTA型で問題となっていたDNSの設定作業に関する負担が解消された。また、迷惑メールと判定されたメールをアプライアンスサーバで破棄するのではなく、特定のヘッダを付与した上で利用者へ配送する設定に変更した。その結果、メールが利用者へ即時配送され、利用者自身でメール振り分けを行う事が可能となった事から、ホワイトリスト登録

による迷惑メール誤判定防止の作業が無くなり、運用の負担が解消された。

しかしながら、迷惑メールについても全て利用者が受信してしまうことから、メールボックスを圧迫する問題が発生した。この問題を解決するため、特に構成員が多い部局を対象に、明らかに迷惑メールであると判定されたメールを、アンチスパムアプライアンスにより削除する運用の検証を行った。3ヶ月間検証を行った結果、正常なメールが迷惑メールとして削除された可能性があるメールに関する問い合わせは1件であり、その内容は、問い合わせ者の誤解であった事が判明した。また、本検証を行うための設定作業は軽微であることから、全学的にも導入可能な運用であると考えられる。したがって、今後、この運用を全学的に適用するためのルール策定などを行う予定である。

4 その他の課題と今後の展望

ODINS が抱えるその他の課題として、以下の点が挙げられる。

- 本学の新棟建設で新たに整備されるネットワーク機器の増加
- 上記に伴う保守費の増加
- 保守業務負担の軽減を目的とした、キャンパス無線 LAN システムのアウトソーシング化
- 本学で利用を禁止しているアプリケーションの制御
- 本学構成員が所有するスマートフォンや PC など、大学所有ではない機器に対するセキュリティ管理

これらの課題については継続して検討を行い、平成28年度に導入を予定している第7期 ODINS の整備によって、その解決を図りたい。

5 おわりに

本稿では、ODINS の沿革と、現行システムについて説明し、現在抱えている多数の課題とその解決策について議論した。システム改修を重ねる毎に問題は徐々に解決しているが、利便性の向上とサービス提供範囲拡大、および利用者のネットワークに対する要求品質の高度化に伴い、業務負担の問題が多く発生しており、これは今後も拡大することが懸念される。また、ネットワークサービスの高度化や個人所有の端末のネットワーク接続増加などに伴い、セキュリティ対策もさら

なる強化が必要である。また、利用者に対してより利便性の高いサービスを提供するためには、手厚いサポート体制が不可欠である。そのため、運用体制の見直しや、ネットワーク整備のための費用負担のあり方の検討などを行う必要がある。また、現行システムの維持だけでなく、時代に即した新しいサービスを提供し、学内の教育研究活動を支える ICT 基盤として、ODINS を発展させてきたい。

謝辞

ODINS について、長年に渡り構築に携わっていた情報推進部情報基盤課の中島重雄課長補佐、木越信一郎専門職員には、多くのご助言を頂きました。また、論文執筆にあたってサイバーメディアセンター 松岡茂登教授、長谷川剛准教授のご指導を賜り、論文の完成に至りました。この場を借りて、感謝の意を表します。

参考文献

- [1] 大阪大学プロフィール, <http://www.osaka-u.ac.jp/ja/guide/about/profile>, pp.20-24, 2013
- [2] 大阪大学総合情報通信システム ODINS, <http://www.odins.osaka-u.ac.jp/about/about.html>, 2013