3-5 情報・ネットワーク

1．ネットワークシステムの維持管理および高度化

1-1　制御系ネットワーク更新

SPring-8の制御系ネットワークシステムは、ノード数1000を越える巨大なネットワークシステムであり、高い性能と安定性を実現するために様々な改善を行っている。2008年度から実施している、XFEL制御系および安全管理システムの統合を目指したネットワーク設備の更新作業として、IPアドレス体系の見直しによる論理構成の変更を行った。併せて制御系ネットワークシステムのセキュリティ向上のために、制御系境界ファイアウォールの更新を行った。

IPアドレス体系の見直しに際して、XFEL制御系、安全管理システムだけでなく、将来予想される施設監視システムの統合管理を考慮し、これら全てのネットワークで情報の集中と共有が容易に実現できるように設計した。同時に、近年、SPring-8制御系で利用が急増しているネットワーク接続型の組み込み機器などで、特定のネットワークトラフィックに対してブロードキャストパケットに起因する脆弱性が指摘されている。ネットワークセグメントを最適化し、ファイアウォール構成を変更することで、不要なブロードキャストパケットの低減を図った。

制御系ファイアウォールは、放射線発生装置であるSPring-8が安定に運用を継続するためのセキュリティ維持装置であり、制御システムへの厳重なアスセス管理を行っている。このファイアウォール機器が単一障害点にならない様に冗長化の構築を行った。また、三脚ファイアウォール構成からデュアルファイアウォール構成にすることで、制御系ネットワークの独立性を高め、XFELとSPring-8の独立運用と統合運用の両立を目指した。

SPring-8の放射線入退管理システムの更新に伴い、安全管理システム用ネットワーク（入退管理システム用ネットワークと放射線モニタ用ネットワーク）を制御系ネットワークに統合した。この際、旧来から運用して老朽化したCisco Catalystスイッチを制御系ネットワークで統合管理しているHP ProCurveスイッチに更新した。これにより、ネットワーク監視システムProCurve Manager Plusによる統合管理が可能となり運用の効率性と安定性が向上した。今後、安全管理システム用ネットワークの機能毎にネットワークセグメントの見直しと更新を行い、更なる運用の効率化を進める予定である。

1-2　全系ネットワークの高度化

SPring-8のネットワークシステムは、上述の制御系ネットワークの他に、利用実験のためのBL-USER-LAN、施設運営のためのOA系ネットワークなどがあり、これらも最重要な基幹システムとして運用している。そのため、近年特に問題となっているネットワーク上の脅威へ対応するためには、セキュリティの強化が特に重要となる。2009年度は、トンネリングソフトウェアやP2Pソフトウェアのトラフィック判別機能を備えたファイアウォール機器の導入を行い、高度なネットワークセキュリティ環境の維持を目指した。導入にあたって、2011年度に予定している高速対外接続ネットワーク（SINET4）への切り替えやXFEL解析LANの導入を考慮し、トータルスループット4 Gbps以上で充分なポート密度を有する機器を選定した。

近年のネットワーク機器の高性能化／高機能化を受けて、ネットワーク機器の老朽化対策と併せて機器の統合／集約が効率的に実施可能となってきた。2009年度は、中央管理棟のネットワーク機器の更新を行い、安定性／可用性を維持・向上させた上で、機器の台数を約半数まで減らすことができた。現在、サイト内のネットワーク機器の台数は400台を超えた。XFELの建設とともにまだ増えつつあるため、ネットワーク構成の簡素化と機器の台数の削減を進めて行く予定である。

ネットワークシステムの安定運用に際して必要となるネットワーク監視系の強化を行った。全系で400台にもおよぶ複雑且つ巨大なネットワークシステムを構成する機器類の死活管理やトラフィックの可視化を行い、運用の効率化を実現している。この監視系の導入によって、障害発生時の検出／通知および障害箇所の分析を自動化し、障害復旧時間を劇的に短縮できるようになった。

1-3　無線LANアクセス環境の更新

SPring-8の共同実験利用者や所内スタッフ向けの無線LANアクセス環境の更新を行い、安定性と可用性の向上を図った。従来導入していた独立動作型のアクセスポイントから集中管理型のシステムに変更することで、運用管理の効率化を実現した。2009年度末の時点で、約220台のアクセスポイントが運用中であり、SPring-8サイト内の主要な建家をカバーしている。現在のところ、一部のOSや無線LANドライバの利用環境において動作の不安定性が報告されているが、メーカーと協力して更なる安定性向上を図っている。

2. 情報システム

2-1 電子メールサーバーの更新

現在利用している電子メールのサーバー機器が2010年中にリース期限となることを機に、新しいメールサーバーの整備を進めた。新しいメールシステムにおいては、運用の安定性をより高めるため機器の耐障害性を上げ、機器障害発生時のダウンタイムやデータ消失のリスクを最小限にすることを第一に設計した。そこで、無停止型サーバーと、高速大容量の冗長RAIDストレージシステムを採用した。

また、ハードウエアの性能向上を活用して、新たなメールサービスとして、IMAPサービスを追加できるようにした。IMAPサービスでは、メールをサーバー上に残し、未読既読の管理や下書きの保存、共有を一元的に行える。また、IMAP4対応のメールクライアントソフトウエアや、Webブラウザを使用してメールを読み書きできる。サーバーに接続できれば、どのPCからでも自分のメールを管理することが可能となる。

このIMAPをサービスするために、サーバー計算機は、CPUのマルチコア化（8コア、従来1コア×2）と、大容量ストレージ（冗長分を除いた実容量2 TB）が必要であり、ストラタス 4410システムを採用した。IMAPを含むメールシステムソフトウエアは従来のメール専用アプライアンスと同等の管理機能を持つ、Sendmail MailCENTER＋Transware Active!Mail とした。現在、2010年度前半のサーバー入れ替えへ向けて、インストール・調整中である。

2-2 統合認証システムの構築

前年度の入館管理システムの更新により、SPring-8 スタッフ、利用者のID管理システムも入館管理システムに変更された。そこで入館管理システムのIDデータベースをもとに、情報システム関連のアカウント管理一元化を目指して、統合認証システムの構築を始めた。

これは、メールサーバーで使用するユーザー名・パスワードの管理を始め、スタッフ専用ページへのログイン用アカウントを共通化するものである。本システムには標準的なLDAP（Lightweight Directory Access Protocol）を採用することにした。LDAPの複数のオープンソースプロダクトを、新電子メールシステムのテストベンチ上でテストした結果、安定性とデータのメンテナンス性に優れたCentOS Directory Serverを採用した。

統合認証システムは2009年中に一部の職員向けページの認証用に運用を開始した。引き続きメールサーバーに適応するためのブラッシュアップや、可用性向上のためのハードウエア整備を継続して行っている。

2-3 対外接続のセキュリティ向上

外部インターネット（学術情報ネットワークSINET経由で接続）と、所内ネットワークの間に、外部公開用サーバーのための「ネットワーク中立ゾーン（DMZ）」を設けた。このDMZは、外部からの不正アクセスが所内に到達できないようにするためのものであり、いわゆるサイバー攻撃から所内ネットワークを保護するためのものである。DMZ自体は外部ネットワークに晒された状態になることから、Webデータの改ざんなどを防止するWAF（Web Application Firewall）や、所内用と分離運用が可能な専用仮想サーバー、ストレージの導入整備を継続して行っている。

2-4 事務系業務用サーバー計算機の仮想化統合

従来事務系のサーバーは、ハードウエアがそれぞれ独立していて冗長性がなく、障害発生時には業務が停止していた。そこで、事務系各部署などで個別に管理されていた6台のサーバー計算機（データベース、アプリケーション、ファイルサーバー用）を、仮想OSを実行する2台のサーバー計算機（冗長構成）と外部ストレージ、バックアップ装置に統合し、入室管理された情報計算機室の施錠ラックに集約することで解決した。

制御・情報部門
田中　良太郎