3-5 情報・ネットワーク

1. ネットワーク

1-1 SPring-8対外接続ネットワーク回線の切り替え

2016年3月末に対外接続ネットワーク回線のSINET4からSINET5への移行により、回線接続インターフェースが毎秒1ギガビットから毎秒10ギガビットに広帯域化された。広帯域化への対応と老朽化対策のため、対外接続ファイアウォールを更新した。更新にあわせて対外公開サーバ用ネットワークまで毎秒10ギガビット接続に対応した。今後の実験データ転送サーバのアップグレードにより、広帯域伝送に対応する予定である。さらに、更新後のファイアウォールは侵入防御機能に対応し、公開サーバへのサイバー攻撃に対するセキュリティ向上が見込まれる。

1-2 ネットワークシステムの老朽化対策

2009年度から着手した、ネットワーク物理配線の老朽化・陳腐化対策を進めた。2015年度は、放射光普及棟の情報コンセント配線の改修、及び蓄積リングDゾーンの幹線用光ファイバーの整備を実施した。放射光普及棟は15カ所29口の情報コンセント配線を改修し、1ギガビットイーサネット（1000BASE-T）に対応した。蓄積リングDゾーンは最も初期に建設された建屋であることに加え、光ファイバー利用用途の増加により、光ファイバー芯数が不足していた。光ファイバーの新規使用要求に対応するため、Aゾーンネットワーク基幹部からDゾーンノードラック間に幹線用としてシングルモードファイバーを増設した。

1-3 無線LANシステムの老朽化対策

無線LANシステムを構成する基地局のうち、共用施設15台、専用施設13台を更新した。2012年度より着手した無線LANインフラ部の更新が完了し、現在はコントローラー2台、基地局328台の構成で運用している。また、実験ユーザー・ゲスト向け無線ネットワークのインターネット出口ファイアウォールを更新し、通信帯域が毎秒100メガビットから毎秒1ギガビットに向上した。

2004年から運用開始し、ハードウェアの老朽化とソフトウェアサポートが終了していた実験ユーザー・ゲスト向け認証システムを更新した。新認証システムは、仮想化基盤上に構築することにより可用性が向上し、長期間サポートされるオペレーティングシステムを採用したことにより2020年まで運用継続可能となる見込みである。

1-4 ネットワーク監視システムの更新

2009年度に導入したネットワーク監視システムのメーカーサポートが2015年に終了したため、新たにネットワーク監視システムを構築した。新システムではオープンソースのZabbixをベースとし、各ネットワーク機器メーカー別のテンプレートを開発することで、ネットワーク機器本体の疎通・死活監視だけでなく、冷却ファン・電源モジュールの故障や温度センサー等の異常検知に対応した。

2. 情報システム

2-1 老朽化した情報基盤の更新

情報基盤システム用ハードウェアについて、老朽対策として運用開始後6～8年を経過したサーバについて老朽代替を実施した。所内情報仮想サーバは、SPring-8 OA-LANに接続する各部署の業務用サーバ計算機（インターネット非公開）を仮想化統合したものである。これらは情報計算機室の限られたラックスペースと電力容量を有効に利用するため、ブレード型計算機を使用している。初期に導入したブレード型計算機は、ブレードを挿入する筐体のファームウェアサポートが終了し、新型のブレード型計算機と混在運用ができなくなっている。

今回の更新に当たり、ブレード型計算機は1台当たり8 core、16 GBメモリから、16 core、128 GBメモリの新機種で置き換え、台数を4台と半減させた。これにより維持コスト、特にLinux OSの年間ライセンス費用の削減に貢献している。

2-2 実験データ配送サービスの運用開始

2014年度にシステム開発を行った実験データ配送サービスについて、実運用のための設定、調整を実施し、9月1日付で本運用を開始した。事前調整として高可用運用のための仮想サーバ計算機の調整、ユーザー認証のための調整、死活監視系のインストールと調整などを実施した。また利用規約の制定と掲載、ユーザー向けサイトへのリンクの準備と、それらに伴うシステムトップページの修正を行った。

正式運用開始後、2016年3月末まで336件のデータアップロード・ダウンロード利用があった。

2-3　フィッシングメール、標的型攻撃メール増加への対応

近年のフィッシングメールや標的型攻撃メールの増加によって、SPring-8内においても、不審メールの着信に関する相談が増えている。

そこでネットワーク上のセキュリティアプライアンスを高性能化する対策とともに、入口対策として職員に対しての注意喚起、情報提供先窓口の明確化と情報提供の呼びかけ、不審メールについての情報提供が有った場合の追跡方法について体系化して実施した。

不正なURLのメールがネットワーク上のフィルタをすり抜けて着信し、そのURLがアクセス可能であった場合は、Webアクセスのログから所内からのクリックが無いか、有った場合はアクセスした端末を特定した上でウイルス検査を実施している。

制御・情報部門
松下　智裕