2-5 情報・ネットワーク

1. ネットワーク

1-1 特高第一変電設備・CVCF電源更新への対応

特高第一変電設備およびCVCF電源更新に伴う停電にあたり、対外ネットワーク接続（SINET5）および平日業務を継続するために必要な電源系統の整備とネットワーク接続系統の切り替えを実施した。

1-2 情報・ネットワークシステムの老朽化対策

ネットワークシステムの老朽化対策のため、情報計算機室3台、中央管理棟2台、研究交流施設6台、正門守衛所1台、ユーティリティ管理棟1台のネットワークスイッチを更新した。ライセンス期間終了に伴いメールセキュリティゲートウェイの更新を行った。新機種ではアンチウイルス・アンチスパム機能に加え、メールコンテンツフィルタに対応した機器に更新した。

1-3 実験計測データ解析用計算機基盤のネットワーク構築

ビームライン実験計測システムから創出される大容量の実験データをSPring-8サイト内で解析を行うための解析用計算機基盤の整備に伴い、セキュアな広帯域ネットワークを構築した。今後、サイト外からの利用のためのVPNシステムの導入を計画している。

1-4 その他情報セキュリティに関する対応

近年の情報セキュリティリスクへの対応として、メールフィルタリングシステムの更新を行った。加えて、SPring-8の情報基盤である認証システムの老朽化対策を行い、高度なセキュリティ維持のための対応を行った。

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年を経過した機器について老朽代替を実施した。

対外中立用ストレージは、SPring-8 OA-LANと外部インターネットの間にセキュリティ確保のために設けられたネットワーク中立ゾーンに接続する、外部公開サーバ群が共用するデータストレージである。主に外部公開サーバの、仮想化されたイメージファイルや、各サーバ上のコンテンツデータを保存している。

今回の更新に当たっては構成を見直し、従来のストレージにおける複雑な構成を単純化し、また用途に対して必要十分な性能を確保した上で、導入コスト・ランニングコストを大幅に低減させた。従来のストレージでは保存するデータの用途に応じ、本体内蔵の高回転SASディスク12基、同増設用の外付けFCディスク7基、コンテンツデータ用の外付け大容量SATAディスク14基を使い分けていた。一方、今回の更新では、高信頼性が保証されるようになった大容量ディスク12基に統一した上で、容量は約1.5倍を確保した。また仮想計算機イメージファイルなどの高速アクセスに対しては、キャッシュメモリ容量と10 Gbit/sのネットワーク帯域で対応している。

2-2 実験データ配送サービスの運用開始

2012年より導入した実験データリポジトリ用グラスターファイルシステム用のストレージは、2015年度以降実験データ配送サービス用のストレージとしても活用してきた。本ストレージについて使用機材の老朽化により2015年からストレージキャッシュ、RAIDコントローラーに障害が見られるようになり、補修部品の入手も困難となった。

更新に当たっては必要十分な性能を精査し、IOやストレージコントローラーの点数が多いInfiniBand方式の分散ストレージから、対外中立用ストレージ同様の大容量キャッシュメモリを持つNASストレージに変更した。またストレージで用いるNAS OSや、高速なRAID方式（ストライピングと冗長パリティ二重化）についても、対外中立用ストレージと合わせ、管理の容易化を図っている。

2-3 入館管理システムの老朽化対策

入館管理システムの建屋外カードリーダーにおいて2016年9月の大雨時に、防滴ボックスの漏水が原因とみられる機器の一時的な異常が発生した。屋外カードリーダーを総点検したところ、屋外防滴ボックスの前面扉パッキン、並びにアクリル窓のシーリングが劣化しており、庇等がない設置場所においては防滴ボックス内に少量の湿潤が存在する事が確認できた。

そこで入館管理システムの長期安定的な運用を継続するため、共用施設46か所、理研独自建屋10か所のカードリーダー防滴ボックスについて、扉パッキンの交換とアクリル窓シーリングの打ち直しを実施した（図1）。

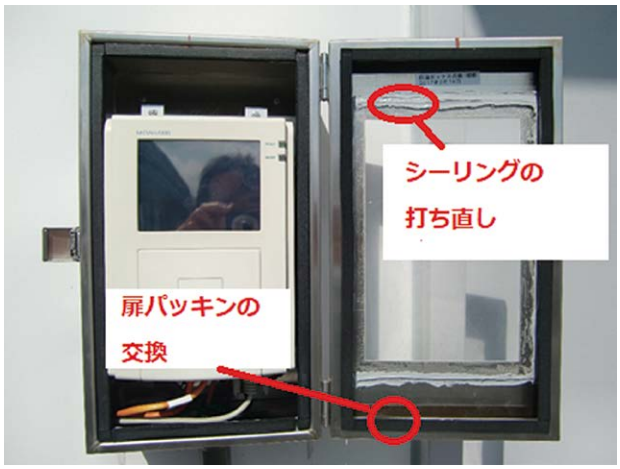

図1　入館管理システムカードリーダー防滴ボックスの補修状況

2-4　フィッシングメール、標的型攻撃メール増加への対応

2016年度も継続してフィッシングメールや標的型攻撃メールが増加した状態が継続した。特に、不正メール大量送信のブラックリストに載っていない計算機を乗っ取って、成りすましのメールを送り付ける手法が主流となっている。この場合、メールセキュリティアプライアンス装置をすり抜けて、各メールユーザーの受信フォルダに通常着信してしまうので、サイトへのフィッシングメール着信が判明次第ただちに注意喚起を行うことが重要になった。

そこで2015年度に引き続き、入り口対策として職員に対しての注意喚起、情報提供の呼びかけと情報提供窓口の周知を随時実施した。

制御・情報部門
松下　智裕