25. 研究情報運営委員会

（情報基盤　研究情報ネットワーク（NIH-NET）の運営状況）

研究情報運営委員長　椎野　禎一郎

概　要

Ⅰ.沿革

国立感染症研究所では、平成 5 年度より所内の研究者向け情報ネットワーク回線の試験運用を開始し、翌平成 6 年度より研究情報ネットワーク（NIH-NET）整備事業として本格的な情報ネットワークが導入された。NIH-NET は、所員の e-mail の利用・Web サイト閲覧・公式 Web サイトの開設などの所員のインターネット利用基盤であると共に、各部が科研費・事業費等で構築・運用している個別情報システムにネットワーク環境とインターネット接続サービスを提供することで、事業費・研究費の効率化に寄与している。平成 10 年には感染研の各庁舎を結ぶテレビ会議システムに回線を提供、平成 23 年には電話回線の IP 化に参画し、庁舎間回線の情報・音声網共通化を行った。平成 24 年度より、政府の情報システム最適化計画に従い、公式 Web サーバと感染症情報センター（現感染症疫学センター）の情報システムが統合され、新たに「所外向け Web サーバ」として NIH-NET から独立し、その運用のために新たにホームページ管理運営委員会が設置された。同時に、所外向け Web サーバはページ更新・管理を一元的に行う Web アプリケーション（CMS）を商用 IaaS 環境で運用する、いわゆるシステムのクラウド化を実現した。このシステムは、平成 27 年 4 月からシステム構成をほぼ同一にしたままで「政府共通プラットフォーム」上に移行され、サーバ能力が増強された。一方、NIH-NET は、平成 24 年度のシステム更新時に仮想サーバシステムを本格導入するとともに回線系にネットワークパーティション機能を持つネットワークスイッチを導入し、他の情報システムも同一インフラ内で構築可能な共通基盤回線としての性格を持たせることで一層の低コスト化・高性能化・省電力化を実現した。平成 28 年度のシステム更新では、このコンセプトをさらに推し進め、主要なサーバをすべて仮想マシンとして運用する構成とした。また、研究環境における情報量の増大に対応するため、ネットワーク末端まで 1Gbps で通信できる環境と、3 拠点および SINET 間の通信帯域の増強を行った。

情報ネットワークに付随する情報セキュリティリスクの増大に対応するため、NIH-NET では平成 13 年度に「研究情報セキュリティ規範」を整備した。平成 17 年 12 月 13 日に、政府の情報セキュリティ政策会議において、「政府機関の情報セキュリティのための統一基準」が決定され、NIH-NET では平成 18 年度にこの統一基準に適応した「セキュリティ対策実施手順」を平成 18 年 10 月より運用開始をした。これらの文書には、情報セキュリティ監査と情報セキュリティ教育の実施が義務づけられており、両者とも平成 15 年度から実施されている。平成 19 年より NIH-NET を含めた所内の情報システムのセキュリティに総合的に対応するため、研究情報委員会を情報セキュリティ委員会に組織再編した。平成 23 年 4 月には、情報セキュリティ委員会の策定した「国立感染症研究所情報セキュリティポリシー」が施行された。これに従って、NESID−NIH-NET 間情報共有の際の情報セキュリティ実施手順および所外向け Web サーバ情報セキュリティ実施手順が、それぞれ平成 24 年 10 月と平成 25 年 3 月に定められた。平成 27 年度 6 月に発覚した日本年金機構における情報漏えい事案は、厚生労働省管轄の各機関に標的型メール攻撃等のインシデント発生時の即応能力を求める体制整備をせまった。研究情報運営委員会は、本省サイバーセキュリティ担当参事官室に相談するとともに、インシデント対策組織である CSIRT（Computer Security Incidence Response Team）の設立を所に促し、同年度末にこれが発足した。平成 28 年度には、

サイバーセキュリティ担当参事官室による情報セキュリティ監査による指摘を受け、この実施手順に最新の厚生労働省セキュリティポリシーで追加されているいくつかの項目を追加する改訂を行った。

Ⅱ.体制

国立感染症研究所の情報システムは、情報セキュリティ委員会の管理下にある。NIH-NET の効率的な運用のために、情報セキュリティ委員会のもとに各部署の正職員からそれぞれ選出された運営委員からなる研究情報運営委員会（以下「運営委員会」）が置かれている。運営委員会は、登録ユーザ・機器の管理とトラブル支援を行い、通常のネットワーク運用業務は数名の研究職員と期間業務職員からなる運営委員会事務局によって行われる。情報セキュリティ上のインシデンスが発生した際には、CSIRT 事務局が CSIRT 対応要員（ほぼ運営委員と同一）と共にその収拾にあたる。このほかに、障害対応・情報セキュリティ監視（SOC 機能）・運営技術支援のため、ネットワーク管理業者と契約を結んでいる。

Ⅲ. 業務内容

現在、NIH-NET では以下の業務が行われている。

1. ユーザ・機器の登録
   各委員からの申請にしたがい、各種登録作業を処理している。
2. 障害の一次対応と業者への指示
   ネットワークの障害発生時に、障害箇所と原因の調査、保守業者との交渉、修理に際する指示等を行っている。
3. 旧公式 Web サーバのコンテンツの維持
   平成 23 年度まで運用されていた公式 Web サーバを維持することで、古いコンテンツが失われないようにしている。
4. 電子メールサービス
   @nih.go.jp 及び@niid.go.jp のドメイン名で電子メール（Web メールによる外部からの利用も含む）が使えるよう整備している
5. 研究者への Web 環境の提供
   研究に関わる情報収集に欠かせない外部研究機関等の Web サービスへの接続環境を提供している
6. 所員への情報支援
   所内 Web サーバを用いて、設定情報、セキュリティ情報、利用案内等を行っている
7. 個別情報システムのための基盤整備
   各研究部等の情報発信に利用される個別情報システム（現在公式には 13 システムある）への回線とインターネットでの名前解決環境の提供を行っている。また、nih.go.jp および niid.go.jp ドメインを管理することで、これらの個別システムに FQDN を提供している。
8. 情報セキュリティ対策
   技術的セキュリティ対策を担う firewall やプロキシサーバに、政府機関等から得た不正アクセス情報を適用している。情報セキュリティ対策の妥当性は、毎年第三四半期に行われるセキュリティ監査で検証され、ここで明らかにされた指摘に対して、設定見直し、機器選定、ポリシーの見直し等の対策を行っている。
9. 講習会の実施
   運用的セキュリティ対策として、新規登録者向け講習会と e-learning による継続者講習会を実施している。新規ユーザへの講習会は、対策実施手順の示す通り2ヶ月に一度2時間の講義が行われている。また、既存ユーザの再教育を e-learning によって行っている。

Ⅳ. 今年度の活動内容

平成 28 年度に行った、通常業務以外の活動は以下のとおりであった。

（1）NIH-NET ネットワーク・サーバ・運用体制の各システムの更新工事の仕様策定・入札/業者決定・更新作業を行った

（2）追加セキュリティ対策として、クライアント管理ツールとエンドポイント対策ツールの統括サーバの設営を行った

（3）標的型メール攻撃訓練を実施した

（4）厚生労働省の情報セキュリティ監査の報告を受け、最新の情報セキュリティ統一基準に合わせた体制への変更作業を行った

Ｖ．平成 28 年度中の主なシステム障害とセキュリティインシデンスは以下の通りである。

1．16/08/22　**村山庁舎 6 号棟 1 階の床上浸水**

台風９号による浸水被害

６号棟 1 階機器室のスイッチ電源ケーブル等が水没

2．16/08/31　**DDBJ からの返事が来ない**

外部メールセキュリティサービスによるスパムチェックの基準が厳しくなったため。後日、修正された

3．17/01/19　**栄養研 LAN から外部への不審な大量通信の試み**

栄養研クライアントへの Trojan.zbot (zeus)の注入

2017/1/15 午前 11:15 ごろ起動（侵入経路・時間は不明）

1/19 午前中に除去

3．17/03/15　**SINET 回線用ルータの不全による通信の遅延**

WindowsUpdate の通信量増大にともなう回線容量の飽和→なんらかの原因で SINET と接続しているルータの設定が half-duplex に変更→大幅な遅延の発生

WindowsUpdate への方策を色々取ったが、4 月の更新（Windows 10 Creators Update）も非常に大きいためこのあと通信遅延が長期にわたり問題となった