２６．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通信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所内 LAN システムが導入された。NIH-NET は、所員の e-mail の利用・Web サイト閲覧・研究用 Web 基盤の提供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「感染研公式 Web サイト」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、公式 Web サイトはページ更新・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 日の「政府機関の情報セキュリティのための統一基準」の決定に伴い、研究情報セキュリティ規範は平成 18 年度に「セキュリティ対策実施手順」に改定・平成 18 年 10 月より運用開始することで、統一基準への準拠を行った。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 間の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。「国立感染症研究所情報セキュリティポリシー」は、平成 28 年度から「厚生労働省セキュリティポリシー」に統合され、またこの時同時に「セキュリティ対策実施手順」に対して政府統一基準に準拠するいくつかの改訂を行った。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を機に、厚生労働省管轄の各機関に情報セキュリティ体制の更なる整備と強化が求められた。感染研は、対応策として同年末にインシデント対策組織である CSIRT

（Computer Security Incidence Response Team）を設立し、情報運営委員会がその実質的な主体となって活動を開始した。また、平成 30 年度より、標的型メール攻撃への対応として新たにメール検知・エンドポイント検知・クライアント管理の3つの追加セキュリティ対策システムの運用を開始した。

Ⅱ.体制

国立感染症研究所の情報システムは、研究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、研究情報セキュリティ委員会を親委員会として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、LAN への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

   ネットワーク障害の発生時に、発生警告の受け取り、障害箇所と原因の調査、障害対応のエスカレーション、保守業者への連絡、修理の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、古いコンテンツにある情報の国民への提供に対応していたが、令和 2 年 2 月の侵入事案を受けて、これを停止した。

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 14 のシステムがある）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。また、端末に対してセキュリティツールの配布を行うとともに、通常インターネット接続業務に利用される端末については、クライアント管理ツールとエンドポイントマルウェア起動検知ツールのインストールを行い、それぞれサーバ連携を行うことで、要保護情報の取り扱いを事務局・当該部局の委員の双方が管理できる体制を作っている。これらの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

令和元年度に行った、通常業務以外の活動は以下のとおりであった。

（1）かねてより運用していた継続者向け e-learning システ

ムは、基盤となるシステムが古く、アップデートの限界を迎えていた。そのため、新たに近年大学等で e-learning 用のサービスとして台頭してきた Moodle を導入して、その上に情報セキュリティ講習教材を作り、継続者向けの情報セキュリティ講習とした。

(2)戸山庁舎 RI 区域の一部を一般実験区域に変更する工事に伴い、新たに実験施設用回線を敷設した。

(3)神奈川県における HDD 廃棄に伴う業者の不適切な扱いによる情報流出事案を受け、機器廃棄を取り扱う総務部に対して情報セキュリティ体制監査を実施し、記憶媒体の廃棄手続きの際の情報セキュリティ強化ならびに、調達時の情報セキュリティ実施手順の順守について指導を行った。

(4)標的型メール攻撃訓練を実施した。

Ⅴ. 令和元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. 19/07/12 **図書館から発生した大量通信に関して**

19:30 頃より 30 分程度、B1 図書館のどこかに対してゲノムセンターのサーバから大量通信が行われた 1GB 近い通信量が発生していたため、図書館システムが停止した。

2. 20/02/28 **www0 から掲示板サイトへの不正な投稿**

旧公式 Web サイトに 15 年以上前から残されていたファイル共有ツールの脆弱性を利用して、このサーバに不正に侵入したうえ某掲示板サイトへの書き込みが行われた。発覚は3月4日であるが、ログを調査して 2 月 28 日より準備作業が行われていたことがわかった。現在、この影響で旧サイトの公開停止と、全 CGI プログラムの運用停止が継続中である。

3. 19/03/02 **www.niid.go.jp への DRDoS 攻撃**

17 時 35 分に発生した DRDoS 攻撃によって、公式サイトのクラウド基盤が公式サイトに向かう全通信を遮断した。21 時 7 分復旧。

4. 20/05/02 **サーバスイッチ・外部向けネットワーク機器群への UPS 故障**

同日午前5:00に、戸山庁舎管理棟 2F サーバ区画・スイッチラックに置かれ、スイッチおよびファイアウォールに電源を供給している UPS が機器障害のため停止した。このため、NIH-NET 全域ですべての通信が途絶した。9:55にバックアップの UPS に電源系統を交換することで復旧。理由は、UPS の経年劣化とみられるが、次期システムではよりモニタリングしやすい機器を調達することが求められる。