令和 7 年度 TC 論文

教育研究機関における情報基盤整備と運用の実践的視点

東京科学大学

TC カレッジ　情報系 TC コース

桑名亮一

目次

第 1 章 緒論

1.1. 国立大学法人等の職員としての教育研究支援の実績

著者は、大学共同利用機関法人 高エネルギー加速器研究機構(以下、KEK)に特別技術専門職として 2009 年に着任した。先端加速器推進部に所属し、国際会議、国際連携スクール等の各種の支援、また KEK の web サイトのリニューアル等の業務を支援していた。その後、2012 年には情報セキュリティ業務を専任として担うこととなった。さらに 2020 年には国立情報学研究所(以下、NII)に特任技術専門職として着任し、大学間連携に基づく情報セキュリティ体制の基盤構築（以下、NII-SOCS）の業務支援を行った。

2021 年に東京工業大学へ着任し、オープンファシリティセンターの技術職員として、情報セキュリティに関する業務、データエンジニアリング等を主軸とした DX に関する業務を行っている。2024 年 10 月に東京工業大学は東京医科歯科大学と統合し東京科学大学となった。これを要因とし、すずかけ台キャンパスの教育研究業務の情報支援も新たに開始している。ここでは、多様な教育研究活動を抱える組織において、セグメント毎に独立した運用や、その担当者の技術的な知識の不均一から発生している等の課題を改めて認識した。

これらの業務を行う上で、関係者との目的と優先順位の合意や、そのための文書化、その後の目標まで到達するために必要なプロセスの明確化などが有用であり、これらの取り組みが組織全体の信頼性や継続性にいかなる価値をもたらすのかを実践的視点から明確化する。

1.2. 「TC カレッジ」の情報系コースとめざすべき TC 像について

国立大学法人等における学術情報基盤の整備等に対する支援等を行う技術職員は、実際の技術操作や学生に扱わせる機器を管理する教育支援系、研究者が使う高度な機器や新しいデバイス等の導入・維持・運営を行う研究支援系、大学内の情報関係の基盤設備を継続的に運営保守する施設管理系など様々ではあるものの、いずれも専門の技術を用いて利用効率や運営コストを下げつつ高品質な情報基盤を提供することが目的となっていると考えている。

TC カレッジにおける情報系コースは、国立大学法人における情報基盤の専門技術職員を体系的に育成するための高度教育プログラムと認識している。大学のネットワーク、サーバ、情報システム、情報セキュリティ、DX 推進などの実務を支える技術者に対し、基礎から応用、そして研究支援企画力まで段階的に能力を向上することを目的とされていたと考える。カリキュラムは初級・中級・上級に分かれ、IT 基礎、ネットワーク運用、情報セキュリティ、業務効率化、DX プロジェクト実践などを講義・演習・実務参加を通じて学ぶ。さらに実務成果を論文としてまとめ審査を受けることで、研究者と対等に議論し組織の情報基盤を牽引できる「テクニカルコンダクター（TC)」として認定されると考えている。このことから、目指されるべき情報系の職員としては、単なる運用担当ではなく、大学の研究・教育活動を技術で牽引することと考えられる。

1.3. 申請の経緯

大学の情報基盤は年々複雑化し、ネットワーク高度化、情報セキュリティ強化、クラウド活用、DX 推進など、多岐にわたる領域が高度な専門知識を前提とするようになってきた。情報に関係した支援を行う技術職員の多くは、日常の運用業務の中で個別の問題解決を積み重ねてきているが、筆者は前々職からの経験により、俯瞰的な視点で設計思想やアーキテクチャを理解し研究者と対等に議論する必要性が技術職員には必要であり、今後の社会においてはこのような技術者が必要になることを強く感じている。

特に、海外の大学や研究機関における情報系技術職の在り方を知ることができる環境にいた中で、日本との構造的な違いを痛感することが多かった。特に欧州では、ネットワークエンジニアやセキュリティエンジニアは“高度専門職”として位置づけられ、明確な職務範囲と裁量が付与され、専門性そのものが評価の中心となっているように感じている。設計権限や技術選定、セキュリティ判断の責任を担い、研究活動と並ぶ大学基盤の中核として専門性を発揮しているように見えていた。一方、日本では技術者が「よろず屋」として雑務に追われることも多く、専門性を長期的に蓄積するキャリア構造が十分に整っていないように思えることもある。この構造的な違いを理解したことで、筆者自身も海外の専門職に近い形で「技術を軸としたキャリア」を築き、知識の深さで組織に貢献できる存在になりたいと考えに至っている。

TC カレッジは、まさにこのギャップを埋め、技術職員が専門職として成長する

ために設計された教育体系を持っていると感じた。体系的なカリキュラム、講義や演習、技術論文の作成、他大学の技術者との議論など、専門性を深める機会が豊富に用意されており、自分の経験を確かな知識として再構築できると強く感じた。こうした理由から、海外の技術者と並ぶことができるような高い専門性を持った技術職員として大学の情報基盤を支えたいという思いから、今回申請した。

1.4. 本論文の構成

本論文は、情報系コースが目指す TC 像に則った教育研究支援、およびそれらに関連する業務の事例で構成している。

第 1 章 緒論

国立大学法人等の 3 つの組織で行った業務の概要を示し、TC カレッジの情報系コースとめざすべき TC 像や申請の経緯、また本論文の構成について触れる。

第 2 章 東京工業大学以前の情報セキュリティ業務

東京科学大学以前に所属していた組織での情報セキュリティに関する様々な業務の紹介、また組織体制などにも触れながら、全体を振り返る。

第 3 章 東京工業大学での情報セキュリティ業務

東京工業大学で行った情報セキュリティ業務について説明する。

第 4 章 東京工業大学 業務改革推進室での業務

東京工業大学で行った DX 業務について説明する。

第 4 章 東京科学大学のすずかけ台キャンパスでの業務

東京科学大学すずかけ台キャンパスで試用的に開始している教育研究支援業務について説明する。

第 5 章 総括

すべての業務を総括し、情報系の技術職員についての考察を述べ、今後の展望についても述べる。

第 2 章 東京工業大学以前の情報セキュリティ業務

KEK に特別技術専門職として 2009 年に着任した。先端加速器推進部に所属し、国際会議、国際連携スクール等の各種の支援、また KEK の web サイトのリニューアル等の業務を支援していた。2012 年には情報セキュリティ業務を専任として担うこととなった。長期間専任 1 名の状態であったため、組織が関わる情報セキュリティの多くに携わる機会をいただいた。2020 年には NII に特任技術専門職として着任し、大学間連携に基づく情報セキュリティ体制の基盤構築（以下、NII-SOCS）の支援を行った。本章ではこの KEK と NII の業務について記載する。

2.1. KEK での情報セキュリティ業務

KEK の先端加速器推進部の業務において、USB の自動実行/再生を悪用した Conficker や AdobePDF などに寄生する Gumblar などを国際会議、国際連携スクールで発見し報告する、KEK の web サイトのリニューアル作業の相談を行うなどの縁があり、2012 年 2 月に高度情報利用推進室へ着任し、同時に KEK CSIRT の専任、および HEPnet-J のセキュリティ担当者を兼ねることとなった。在籍当時の KEK CSIRT には筆者の他数名が兼務で所属しており、インシデントの対応は筆者が原則対応することとし、種類や規模に応じて他の兼務者が参画するかどうかが高度情報利用推進室長でもある統括情報セキュリティ責任者により判断された。専任であったことから KEK で内外の様々なセキュリティインシデント対応や脆弱性への対応などへ携わる機会を得た。

ここでは、KEK の情報基盤を支えるネットワークである KEK セキュアネットワーク、情報セキュリティ体制を紹介し、公開されているインシデント事案への対応や脆弱性対応など情報セキュリティ業務について携わったものから一部を紹介する。

2.1.1. KEK のセキュアネットワーク

所属していた当時の KEK のネットワーク(図 1)について説明する。KEK つくばキャンパスのネットワークはセキュアネットワークと命名され、セグメントは大きく 3 つに分類できる。

1. DMZ

   外部からの通信を受け付けることが可能なネットワークセグメントとして用意されている。ネットワーク用語として一般的に用いられる DeMilitarized Zone（非武装地帯）と同じである。

2. 機構内 LAN

   この機構内 LAN は、組織ごとに定められた 20 以上のネットワーク等により構成され、計算科学センターが統括管理されている。一般的な教職員は、有線と無線どちらの機器でもネットワーク接続のためには申請システムで承認を得た上で機構内 LAN へ接続することが可能となり、これにより利用者の特定が可能となっている。なお、インターネットや DMZ からの機構内 LAN を宛先とした通信はできない。

3. EX クラスタ

   EX クラスタはインターネットと完全に同じ外部のネットワークとして設置されている。共同利用者等の短期外来者が一時的に利用するなど目的で設置されており、eduroam やゲストネットもここに設置されている。これらも利用者の特定が可能となっている。

これらのネットワークは、web 上で 2003 年 6 月には運用されていることが確認できる[1]。また、Firewall(以下、FW)は、1998 年から運用を開始しており、情報セキュリティ対策を早期から実施していたことが推測できる。また、加速器など大型実験装置のための制御ネットワーク等は機構内 LAN 配下に構築しており、万が一インシデントが発生した場合には、構内 LAN との通信遮断を物理的に行い隔離された制御ネットワークで運用可能としている。

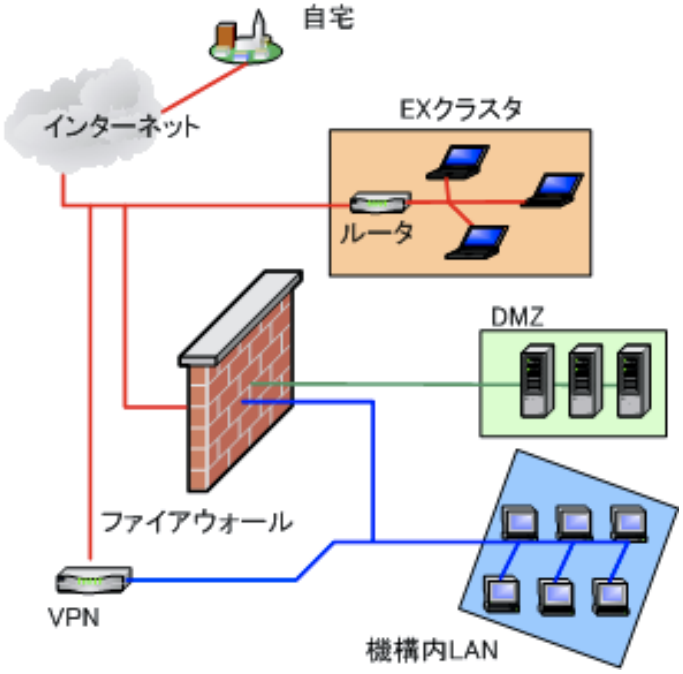


図 1. KEK のネットワーク

2.1.2. KEK の情報セキュリティ関連規定と管理体制

KEK における情報セキュリティおよびガバナンスを適切に維持するための組織体制と規則体系について記載する。KEK の情報セキュリティ関連規則と管理体制については、KEK から公開されている情報セキュリティ 11 の対策から、その概要を確認することが可能である[2]。

2.1.3. 情報セキュリティの関連規定

KEK の組織体制や規則体系については、1990 年代から存在していたが、2005 年の「政府機関の情報セキュリティ対策のための統一基準(以下、統一基準)」を基に再構成された。KEK CSRT は、2003 年から JPCERT/CC から立ち上げのための指導を受けながら検討され 2007 年に設立された。

KEK 全体に共通する基本的な規定から、各種の実施手順に至る階層構造(図 2)が採用されており、KEK の他の規則群との整合を持った運用がなされている。統一基準が改正されるたびに、もしくはなにかしら運用に問題が発生した場合に適宜見直しも実施されており、監査や自己点検も筆者の着任以前から実施されており、また十分に機能している。

特筆すべき点として、統一基準との大きな違いとして、KEK の体制では、各組織

の情報技術に精通している教職員を情報セキュリティマネージャとして組み込んでおり、この情報セキュリティマネージャが集まり専門的な技術の検討や各組織での課題を共有するなどの議論を行う情報セキュリティ管理部会も設置されている。また、例外措置申請など規則を遵守する仕組みも必要に応じて整備し動作している。

図 2. KEK の情報セキュリティ規則等について(情報セキュリティ 11 の対策より)

2.1.4. 情報セキュリティの管理体制

KEK では、経営層による情報セキュリティ委員会の方針決定と監督機能を基盤に KEK CSIRT を含む情報セキュリティ管理部会による支援、情報セキュリティを実施する各部門や教職員が相互に連携する構造(図 3)を構築している。これにより、意思決定の透明性や責任の所在を明確化し、各組織でばらつきが発生するようなリスク管理なども KEK 全体として一貫性を担保することとしている。

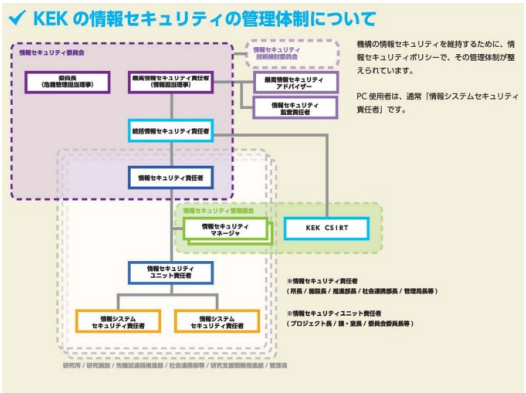


図 3. KEK の情報セキュリティ管理体制 (情報セキュリティ 11 の対策より)

2.1.5. 緊急時対応手順の策定

KEK CSIRT の着任後の最初の業務は緊急対応手順の策定となった。過去のセキュリティインシデント事案の報告書や情報セキュリティ管理部会の議事録などを参考に緊急対応手順の案を作成した。案は、KEK CSIRT は再発防止の技術的な責任を負うなどの過去の知見を組み込んだ原案まで 2 か月程度の時間を要した。その後、情報セキュリティ管理部会を得て情報セキュリティ委員会での承認まで着手から 8 か月ほどの時間を必要とした。2013 年には、KEK の全構成員に広く周知するために、A4 のリーフレット(図 4)を作成しこの手順の説明会を各部局に対して複数回実施した。

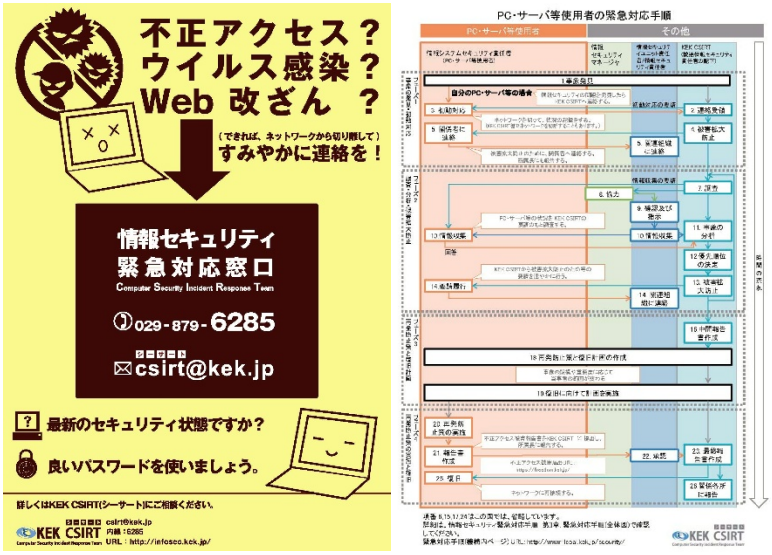
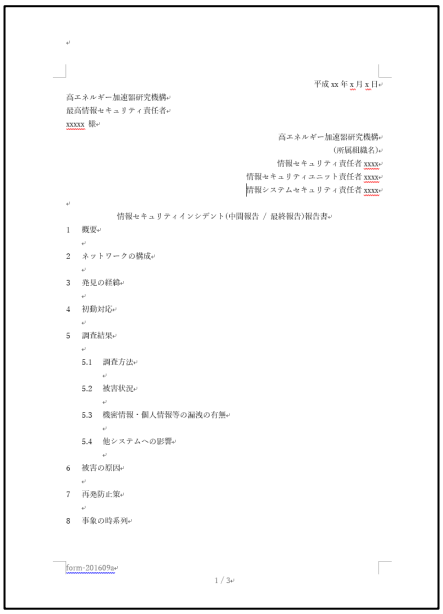


図 4. KEK 緊急対応手順 リーフレット

リーフレットの効果としては、情報セキュリティに関する相談は実際にこれを見て連絡をされた相談者が多かった。また情報セキュリティ運用の補助ツールとして、インシデントの対応時には、このリーフレットを用い対象者への詳細な説明を行うなど、十分な活用ができたと考えている。

補足として、上記のリーフレット内に記載している事象への対応自体の報告書となる「15.中間報告書」については、当初 CSIRT が作成していたが、スパイウェ

ア等への対応の急増や最終的には被害には至っていない事案が多くなった 2014 年に機器管理者が作成することとなった。そのため、緊急対応手順を改定し、また利用者が迷わないよう報告書を記載できるよう、ひな形(図 5)を準備した。全部で 3 ページあり、2 ページ目以降には記載方法を用意した。



平成 xx 年 x 月 x 日

高エネルギー加速器研究機構
最高情報セキュリティ責任者
xxxxx 様

高エネルギー加速器研究機構
(所属組織名)
情報セキュリティ責任者 xxxx
情報セキュリティユニット責任者 xxxx
情報システムセキュリティ責任者 xxxx

情報セキュリティインシデント(中間報告 / 最終報告)報告書

1 概要
2 ネットワークの構成
3 発見の経緯
4 初動対応
5 調査結果
5.1 調査方法
5.2 被害状況
5.3 機密情報・個人情報等の漏洩の有無
5.4 他システムへの影響
6 被害の原因
7 再発防止策
8 事象の時系列

form-201609

1 / 3

図 5.情報セキュリティインシデント報告書 ひな形

このひな形の作成以降は影響範囲が大きい事案などは機器管理者が用意する報告書とは別に、KEK CSIRT から別途に詳細な技術内容を記した調査報告書を作成する場合もあった。

緊急対応手順は、プロセスの詳細を記載することやプロセスの回数を増やすなどの細かい改定を必要としたものの、筆者自身が KEK CSIRT として行ったインシデント対応は例外なくこの手順の中で収まったことは、この緊急対応手順の基となった過去のインシデント対応が非常に的確であったことを示している。また、KEK CSIRT が再発防止の技術的な責任を持ち続けたことなどを要因として、実際に同様の被害が再発することも在籍中には発生しなかった。

2.1.6. スーパーコンピュータのセキュリティインシデント事案対応事例

2013 年 11 月 1 日、KEK スーパーコンピュータシステムにおいて、利用者のパスワードを用いた本人以外の何者かによる、なりすましとみられる不正アクセスが発見された。これを受けて同日システムの運用を停止し、被害状況の調査を開始した KEK CSIRT と外部情報セキュリティ専門チームによる独立した調査により、不正アクセスおよびシステムの健全性に対して、以下の結論を得た。

- スーパーコンピュータシステムの 3 つのフロントエンドサーバ及び、一つの管理用サーバに対して、10 月 21 日に利用者本人以外の第三者による、盗まれたパスワードが悪用されたとみられる不正なログインが 3 名のアカウントを用いて行われた。
- 不正なログイン上では、管理者権限奪取を試みたが失敗した。
- 不正ログインされたサーバにおいて、システムの改竄や削除等システムの健全性を疑わせる事実はない。
- 計算サーバ本体への被害は確認されていない。
- ユーザデータ領域について利用者全員に対して調査を行った。全アカウントについて確認が完了し、いずれも改竄やデータ削除などの被害は認められていない。
- システム周辺の機器についても被害は認められていない。

以上により、スーパーコンピュータシステム自体には、フロントエンドサーバを含め健全性を疑わせる事実はなく、改ざんやデータ削除などの被害も認められなかった。

この調査の結果から、再発防止策として、公開鍵認証とパスワード認証を併用する方法によりログイン認証を強化、利用者に対する情報セキュリティ教育の徹底、ログ監視の強化等を実施した上で、2013 年 12 月 10 日に運用が再開された。運用再開後も、システム上での不審な行動の監視等、情報セキュリティ強化策が適宜行われた。

本攻撃と類似した攻撃が 2014 年初頭にも確認され、2014 年 2 月には最高情報セキュリティ責任者により、緊急対応の依頼が外部からログイン可能な DMZ の各システムの管理者に対しても OS のアップデートの実施要請が行われ、すべての機器の更新がなされた。

また、いくつかのシステム上に秘密鍵を設置しないよう、秘密鍵の探索を定期的に実施し、発見した場合は公開鍵認証のファイル削除を実施するようになった。その他、

利用者に対して秘密鍵とパスワードの管理に関して厳重に取り扱うことや鍵ペアを作成する場合にはパスフレーズを設定するなども強く推奨している。

この攻撃キャンペーンは拡大を続け、国内の数か所のシステムで同様の事案が発生し、その後も大学・研究機関での不正アクセスが各所から報告された。スーパーコンピュータシステムの情報セキュリティに関する組織間の連携が不可欠な状況であった。相互の状況を理解し今後の連携を目指すため、KEK を含む国内のスーパーコンピュータシステムを運用する 8 拠点の運用担当者が集まり、セキュリティ連携研究会が 2014 年 3 月に開催され、連携を強化するための活動が継続されている。この枠組みに対しては、調査の途中で入手できた攻撃者が利用する各種バイナリファイルの可読部分を出力する string コマンドで文字列を取り出し、そこから特徴的な文字列を選び、被害を検出する手法を共有した。これにより、本攻撃キャンペーンの検知を可能とし、多少なりとも被害を減らすことの一助になったのではないかと考えている。

この事案を重大と考えていただいた日本シーサート協議会では、SSH サーバセキュリティ設定検討 WG を立ち上げていただき、SSH サーバセキュリティ設定ガイド[3]を発行するまでの協力を得ることとなった。

2.1.7. 脆弱性の対応事例 ShellShock の事案対応事例

2014 年 9 月に発見された Unix 系システムで多く使用されている GNU bash の脆弱性については、ShellShock と命名され、「インターネット史上最も危険な脆弱性のひとつ」として評価された。本項ではこの対応について説明する。

2.1.7.1. 脆弱性の概要

Bash は「関数を環境変数としてエクスポートできる」機能があり、()の関数定義を読み込んだ後、本来は無視すべき文字列まで実行してしまう欠陥に脆弱性番号である CVE-2014-6271 が割り当てられた。具体的には、HTTP,DHCP,SSH など非常に多岐にわたる環境変数に変換される入力経路から、OS 上で任意のコマンドが発行可能となる。

```
() { :; }; <任意のコマンド>
```

この攻撃の例でまず確認されたものは、HTTP でのアクセスの際に用いる Web ブラウザの情報である User-Agent を改変したものであった。web ページに設置するお問合せフォームなど、この頃は CGI で作成することが主流であり、それらを設置すると攻撃を受ける。

認証不要で任意のコマンドが実行されること、bash が使われる場所が悪用されることなどから大きな問題となり、2025 年現在もまだ攻撃が観測されている。

2.1.7.2. 対応

対応期間が極めて短期間であったため、事象を時系列に沿って整理し記載する。

9 月 24 日(水)

深夜に CVE-2014-6271 の情報を Twitter(現 X)の情報収集の中で確認した。手元にあったサーバでコマンドを発行してみたものの自身が施したセキュリティ対策により、コマンドは実行による攻撃は成功できなかった。

9 月 25 日(木)

出勤後、すぐに検証用サーバで確認し、一般的なセキュリティ対策を行ったサーバで攻撃が成功できることを確認した。また、この時点ですでに攻撃者による実害がない探索行動が開始されていることも CSIRT に情報展開を行った。非常に重大な脆弱性と判断され緊急で CSIRT の打ち合わせを行った。この時点では日本語の情報は少なく、JPCERT/CC、もしくは IPA 等の情報も公開されていなかった。信頼できる情報元から本情報が公開されたら DMZ 機器管理者への周知を行うこととした。また実通信の解析情報や web の情報から探索行動を行ったと思われる IP アドレスに対しては、通信を遮断することとも決定した。この打ち合わせの後、本件に関連した脆弱性として、CVE-2014-7169 が追加された。

午後には、ShellShock に関する脆弱性情報が JPCERT/CC より公開され[5]、公開内容を確認整理の上、響確認および適切な対応が行うよう DMZ 機器管理者に周知した。

夕方に再度、CSIRT で打ち合わせを行い、KEK の FW で web に利用されるポートを遮断することを最高情報セキュリティ責任者へ進言することが合意された。ポートを遮断とは、インターネット上から KEK の web ページが全て開かなくなることを意味する。この遮断を実行するかを判断できる内容もこのうち合わせで整理し提案内容を合意した。また、ポートの遮断解除の申請を受けつけるための案内文から、遮断までのプロセスの検討を行い、関係者が滞りなく実施するために必要なものが準備できるよう合意を行った。しかしながら、最高情報セキュリティ責任者と連絡が取れなかったため翌日に持ち越しとなった。

用意した申請は、webopen 申請と名付けた。OS の基本情報や安全性検証のためのコマンドの発行結果などを記載して、その返答をメールで送付する仕組みとした。この安全性検証のコマンドは、Shellshock BASH Vulnerability Tester をもとに作成した。提案では、申請を受け付け問題がないと判断できれば、遮断を速やかに解除することとし、この流れは規則との整合性を維持するために例外措置の一部であることの再確認も行った。

なお、例外措置の議論は、情報セキュリティ管理部会で行うことが定められている。そのため、統括情報セキュリティ責任者の責任において仮承認とし、ポートの解放は一時的なもので本審査は別途行うこととした。本審査は、緊急の情報セキュ

リティ管理部会を 9 月 30 日(火)に実施することとなった。

9 月 26 日(金)

最高情報セキュリティ責任者と協議し、FW の遮断する方針で進めることとなった。FW の遮断を解除するためには脆弱性の解消を必要とすることとした。遮断について DMZ 機器管理者にメールで周知を行った。この後の午前 11 時頃に後続の CVE 番号のパッチが Redhat 系で追加されたことを幸いにも確認できた。

DMZ 機器管理者のメーリングリストでは、機器管理者同士の活発な情報交換がなされている。webopen 申請の案内の以前に DMZ 機器管理者のコミュニティの中で脆弱性の深刻さの理解を深めていただき、機器管理者自身から遮断もやむを得ない状況であると遮断に対して強い反発はでなかった。

午前中の申請の受付開始から、多数の申請が提出され KEK の組織を支えるような基盤となるシステムや外部との連携などに利用される機器など影響度の高いと認識していたシステム群は、概ね遮断前に仮承認の段階に至ることとなった。

午後の後半には FW の遮断を実施した。この遮断を実施した 2 時間後には、サーバを自由に操作可能にする webshell を仕込むコマンドが観測された。なお、以前から行っている FW の監視で DMZ から不審な outbound 通信がないことも確認できていたことから、紙一重で被害を未然に防ぐ対応となった。

9 月 30 日(火)

Mac OS X のパッチが公開される。この時点で脆弱性番号に追加された脆弱性も増え、CVE は 6 つになっていた。

緊急の情報セキュリティ管理部会も開催され、全 DMZ の機器を対象とした詳細な安全確認を行うため、webopen 申請を Safecheck 申請と改めることとなった。web ページを用意し、6 つの CVE に対応する安全性検証コマンドなど詳細な情報も追加し、確認に漏れがないようにした。申請がなかったホストは 11 月初旬に通信遮断を行い、再度 DMZ 機器とする場合には一からの手続きを必要とすることとなった。

11 月 6 日(火)

Safecheck 申請から以下の分類となった。

- 安全性確認の申請処理完了ホスト数 368
- 廃止申請ホスト数 30
- 例外措置申請提出ホスト数　5
- 廃止予定ホスト数　5
- 未完了ホスト数　3

例外措置申請は、管理部会で審査された。例外措置の多くのホストはアプライアンスであり、製造元から修正パッチがまだ提供されていないものであった。11 月 5 日正午の時点で安全性確認が行われなかった「廃止予定ホスト」と「未完了ホスト」の 8 台は、11 月 6 日に予定通りに MAC アドレスを停止し、これを持って対応を完了とした。

2.1.8. 平時の業務

KEK CSIRT の専任として、平時の業務も多くある。情報セキュリティの対策を行う上で、情報収集を行い早期の認知を行うことは脆弱性による被害等の有無の大きな分かれ道となる。そのため情報セキュリティに関わる情報収集業務が必要となってくる。また、外部組織との連携も可能な限り参加し、異なる視点や専門性を得ながら認知の偏りを補正することも行った。

その他、情報セキュリティの相談対応、情報セキュリティ管理部会の幹事、情報セキュリティ監査、情報セキュリティ自己点検、DMZ が設置されているセグメントの管理者の他に、KEK の新任職員研究会や、総研大の新入生ガイダンスなどでの話者なども務めた。

2.1.8.1. 情報セキュリティに関する情報収集

情報セキュリティにおける攻撃の検知や対応の前提として、「その攻撃を知っているか」が対応の品質を決定する重要な要因となる。ここで記載する情報収集は情報セキュリティ対策の起点となる。

情報収集は、日本のみならずアメリカや EU の情報セキュリティ関連の web サイトや海外を含めた研究所や大学、先端的な体制を有する民間の組織や高度な情報セキュリティを有するベンダーなど多種多様な情報源からとしている。この情報収集の業務には 2014 年頃から自動化にも取り組んだ。自動化には、CUI ベースでは Linux 上でシェルスクリプト用い様々な自動化を元々行っていたこと、また GUI ベースの自動化も 2000 年代から web 制作の中でいくつかを利用していたことから、それらの延長での実装となった。GUI については、Python, Windows PowerAutomate もしくは、AI の活用など様々な自動化ツールが現在普及しているが、2013 年当時はこの手のソフトはまだ多くなく Sikulix、Selenium, その後には UiPath なども利用した。

2.1.8.1.1. ハニーポットの運用

着任後のインシデント対応では攻撃者に対する理解不足を強く痛感することがあった。フィッシング攻撃のマルウェアの実行後や脆弱性を悪用し管理権限奪取後な

ど、攻撃者が侵入後にどのようなことを行うのかの知見を補うために、マルウェアを実機に感染させ観察する環境を独自回線上に用意(図 6)し独自の情報収集を行った。特に APT グループに関連するマルウェアは、時間の許す限り分析を行った。

マルウェアのバイナリの解析には主に X-Ways Forensics や IDA Pro を利用した。実際に攻撃者が入ってくることは稀であったが、それでも攻撃者の実際の行動を観察した内容はインターネット上で知ることができない挙動であり、得られた知見は非常に大きかった。攻撃者が利用した IP アドレスやドメインなどの IoC（Indicator of Compromise：侵害の痕跡）は後ろに記載する通信遮断にも適用していた。

図 6.解析環境に用いた実機(2019 年 SWS 発表スライドより)

2.1.8.1.2. 外部組織との連携

KEK は外部組織との連携も古く、1999 年から行われている SWS(共同利用機関におけるセキュリティワークショップ)がまず挙げられる。これは、全国の共同利用機関、および国立大学附置研究所など共同利用者を抱える研究機関として共通の課題を議論する、また最新の技術について意見交換、担当者間での交流を目的に開催されている。1999 年から 2001 年までは年 2 回の実施であったが、その後は年 1 回の各持ち回りで開催され、各機関の取り組み状況の紹介や対応の報告などのサイトレポート、先端のネットワークおよびセキュリティ技術の紹介などのテクニカルレポート、そして共通の課題などが活発に行われている。

また、KEK の CSIRT は、2004 年頃に 1 年ほどの時間をかけ JPCERT/CC の指導を受けながらの立ち上げが検討された。この時点以前から、JPCERT/CC や

IPA との連携も始まっている。また、CSIRT の枠組みでもある日本 CSIRT 協議会には、民間の参加もまだ少ない 2012 年 5 月に加盟し、その後、いくつかの国立大学法人等の CSIRT の加盟推薦も行った。

さらには、つくば市には多種多様な国立研究開発法人や大学などもあることから、つくば近隣の大学研究組織を対象と情報交換会を立ち上げるなども行った。その他にも、アジア 3 国の高エネルギー物理学研究機関のセキュリティの情報交換会をはじめ大きな枠組みから小さい枠組みまで様々な外部組織と緊密な連携を行えた。

このような枠組みでは相互の理解や信頼を深め、よりよい情報セキュリティを共通の目標としていた。このような枠組みに身を置けたことによる恩恵は非常に大きく、単独では解決できないような課題をいくつか解決できたとも考えている。

2.1.8.2. 組織内の相談受付

KEK CSIRT に着任時から最後まで、相談受付を行っていた。相談は、電話とメールで受け付けていた。当時の KEK では、機内 PHS が運用されており、それを個人用と CSIRT 用の 2 台を常に所持し相談対応を実施していた。相談内容は、パソコンの基本的な設定からインシデントに繋がるものまで多岐にわたる。件数は月による変動は大きいものの、平均をとると月 6 件程度の対応をおこなった。

また、対面相談では、相談内容と合わせ、望ましくないプログラムやマルウェアの感染兆候の有無などを PC の健全性の確認を行い、また相談者自身で確認する方法なども提供し、構成員全体の情報セキュリティ対策の底上げを着実に行った。

2.1.8.3. 情報セキュリティの啓発活動

被害を予防する措置として、情報収集で得られた知見は組織の全構成員の意識向上のために隔月開催した情報セキュリティ講習会等や情報セキュリティに関する相談対応やドキュメント作成などでも活かされた。また、脆弱性情報のうち被害に繋がる可能性があると判断したものは DMZ の機器管理者などに対して注意喚起なども行った。

2.1.8.4. 予防措置としての通信遮断

情報収集から得られた攻撃者が利用したいわゆる IoC である IP アドレスやドメインについては、2016 年 3 月から予防的にいくつかの条件を設けて FW で遮断するようにした。2018 年頃には JPCERT/CC や IPA サイバーレスキュー隊など外部から連絡が来る前に事象を認識することを可能となり、連絡があった IoC のほぼ全ては、連絡が来る前に通信遮断等の対応を実施済みとなっていた。

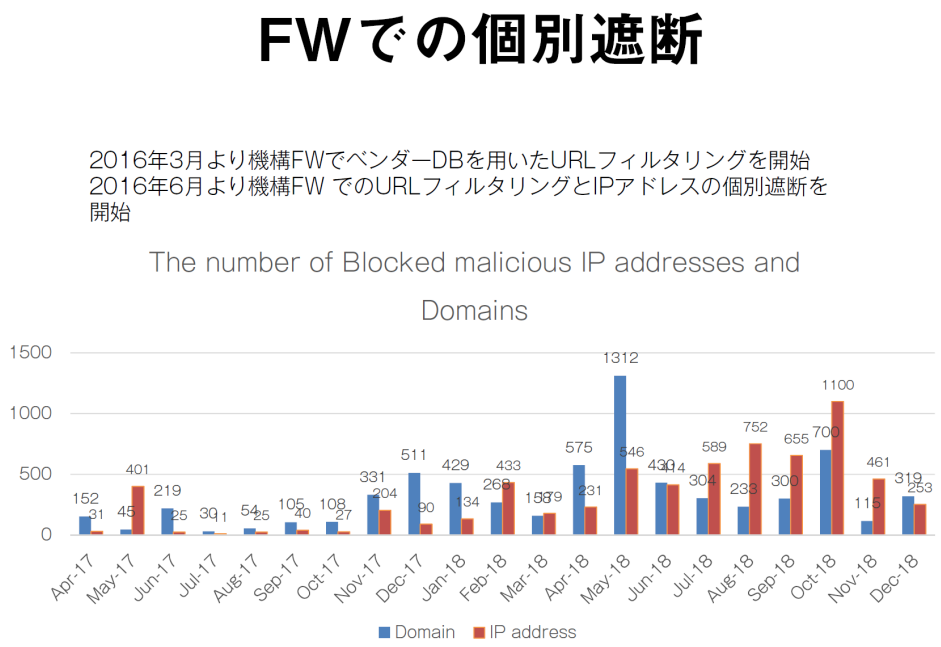


図 7. FW での個別遮断統計(2016 年)

この遮断については、情報収集と同様に自動化を進め、2019 年頃には遮断可否判断の流れ中の大半を自動的に処理(図 8)するようにした。

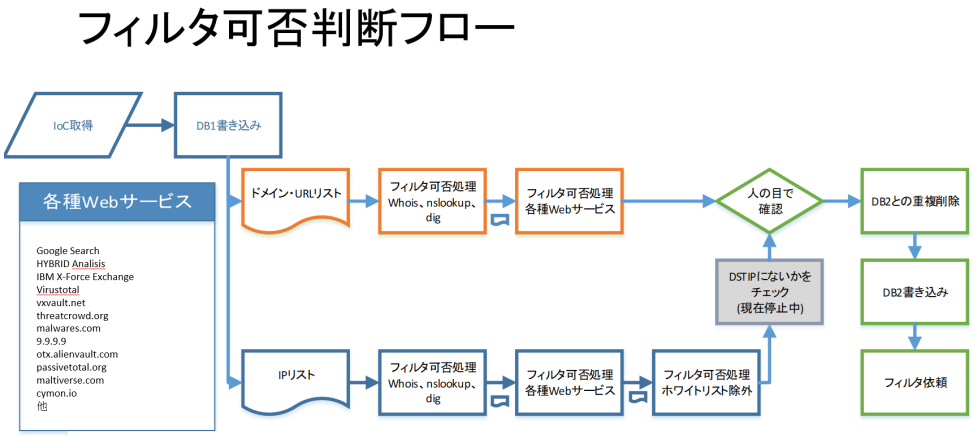


図 8. 遮断実行までの判断フロー (2019 年 SWS 発表スライドより)

2.1.9. KEK CSIRT の行動規範の策定と遵守

2016 年頃から情報セキュリティに求められることが多くなり、今までセキュリティに携わったことがなかった職員なども携わるようになった。

そのため、行動規範のようなものがあったほうがよいとの統括情報セキュリティ責任者の意向があり、NTT-CERT の協力も得て行動規範を作成した。筆者が出した案は CSIRT で合意され、この 7 つを規範とした。

KEK CSIRT は、行動規範を常に念頭に置き、業務を遂行したいと考えています。

1. 事実を見極める。
2. チーム力を最大限に発揮する。
3. コミュニケーションに心を砕く。
4. 冷静に対応する。
5. 慎重かつ大胆に行動する。
6. 品質の向上に努める。
7. ポジティブに行動する。

KEK CSIRT で行った技術的な機能の担当は、筆者の後任のさらに後任となっている。2023 年にその後任者の居室にお伺いした際に、上の行動規範が額装されて壁に飾られているのを見て、このような指針は後に残りやすいものであることを再認識した。

2.1.10.KEK の情報セキュリティを振り返り

2012 年の当時の国立大学法人としては、先進的な取り組みが多くみられた。要因として、1988 年の KEK の前身である高エネルギー物理学研究所の事案の影響があったのではないかと考えている。

KEK の情報セキュリティ対応の歴史は古く、記事として確認できるものでは、毎日新聞社の記事「西独から集団“ハッカー”」で昭和 62 年 2 月 3 日がある。また、我が国でハッカーに関する事件が報じられたもっとも古いものと記載されている[5]。

この事案以降から情報セキュリティへの取り組みは現在まで続いていると考えられる。筆者の着任時には、この昭和 62 年の事案に携わられた方々の一部もまだ在籍しており、着任した 2012 年にはすでに多くの知見を伴った体制があった。また前述のネットワークの分離、ログの集中管理、監視、また検知の仕組みも計算科学センターが主体的となり段階的に導入され、技術的にも十分に機能していた。

学術機関である KEK の性質上、「研究の自由」や「オープン性」を重視する文化は、情報セキュリティに対する意識がまだ醸成されていないこの時点で情報セキュリティ文化の形成の障壁となったと考えられえる。その中で情報セキュリティ規則を形式的ではなく実践的に機能することを可能とする体制が整えられていたことは、当時を振り返る今でも偉業がなされていたと感じている。

2.1.11.組織体制の振り返り

情報セキュリティの対応では、正解が存在せず、情報をとりまく環境にあわせ制度の変更も多い。そしてインシデントが発生するとその説明責任は非常に重い。情報セキュリティの組織体制については、世界を見ても非常に多種多様な問題が上がっている。KEK のセキュリティ体制は、このような問題に対応可能な他に見ない新しい組織モデルとなりえるものではないかと考えている。

本業務の経験を通じて特に特筆すべきこととして、情報セキュリティの被害発生

は個人の問題や責任追及の対象ではなく、組織の体制が現実の情報セキュリティ体制に適合していない課題であり、大きな被害の再発防止策には必ず組織の改善が含まれた点である。その改善のために、結果の成否より、「どのような条件があり、どのような判断を行うか」という判断プロセス自体の合理性と妥当性が重視された。この構造は正解が事前に存在しない領域において非常に有効なものと考えている。また、最高情報セキュリティ責任者の役割においても、判断プロセスの透明性を担保し説明責任の役割を一元的に担うことが重要とされたが、これにより現場の恣意的な判断や政治的な判断から解放されたとも認識している。

一方で、この組織体制を支えるためには、判断を行うための再発防止の比較案等の条件整理などのレポーティングが多く、また自身の対応を常に問い直す必要もあり一定の負荷が伴ったとも認識している。緊急対応手順の報告書作成者の変更などから、この組織体制の人的コストが高かったことがわかる。

このような組織体制は、「判断がどのように生まれ、どのように自組織を修正するか」の透明性を維持しながら合理的な判断を継続的に行える組織であり、失敗したとしても組織の改善が行われる。不確実性が高い、正解が存在しない、環境変化が激しい、説明責任が重い等の領域においては、このような組織体制の有効性は極めて高い。さらに組織文化よりも組織設計への依存度が高くなる。これは、先端的でありながら実践的な組織体制の一つの形でもあると考える。

2.1.12.まとめ

KEK を離れた現在でも、2023 年に KEK で開催された情報セキュリティセミナー[6]に講演者として呼んでいただくことや、2024 年に開催されたつくば近隣の大学研究組織を対象と情報交換会にオブザーバ参加させていただくなど、今も関係性は続く。

2.2. NII-SOCS の支援業務

NII では、大学間連携に基づいてサイバーセキュリティ人材を養成すると同時に、攻撃検知・防御能力の研究成果を適宜適用することで、国立大学法人等におけるサイバーセキュリティ基盤の質の向上を図ると共に、サイバーセキュリティ研究の推進環境と、全ての学術研究分野に対する安心・安全な教育研究環境を提供するための研究開発等が進められている。

サイバーセキュリティ基本法の改正等を背景に、国立大学法人等は自主的なサイバーセキュリティ体制の強化に一層取り組むことが求められている。そうした自主的な取り組みを促進するため、NII-SOCS を実施し、大学間が連携（Collaboration）するための環境整備及び参加機関が学内のサイバーセキュリティ体制を確立するための支援事業が、平成 29 年度から情報セキュリティ運用連携サービス（NII Security Operation Collaboration Services: NII-SOCS）として行われている[7]。

本事業は SOC(Security Operation Center)のサービスではなく、また、セキュリティベンダー等が提供する SOC サービスを代替するものでもない。NII-SOCS においては検知システム等を用いて警報分析及び各機関への通知を行われるが、全ての攻撃等を対象とするものではなく、参加機関が主体となって警報分析を行い対応することが原則となっている。

日々高度化するサイバー攻撃に関する情報や大学等学術機関のセキュリティ対策に関する情報共有・発信を行うことを目的として、2020 年に特任技術専門職として学術基盤推進部 学術基盤課 NII-SOCS チームに着任した。

2.2.1. NII-SOCS における観測データの流れについて

SINET 上に流れる通信を基に NII-SOCS が行う業務の主な流れとしては、以下のとおりである。

1. センサー群・観測システム群からの警報や通信のセッション情報の取得と集約

   SINET 上に配置した 3 種類の検知システムからの警報情報、および通信のセッション情報を取得し、専用の機器群で集約する。

2. 解析・可視化・蓄積

   集約された情報は、リアルタイムもしくは巡回観測方式で解析と可視化がされる。

3. 警報通知とポータルサイトを通じた情報共有

   前項で被害が疑わしい警報情報やセッション情報があった場合には、各参加機関の NII-SOCS 担当者に対してメールで通知を行う。なお、メールにはポータルサイトの情報を記載し、実際の情報を取得するためには、ポータルサイトを閲覧する必要がある。

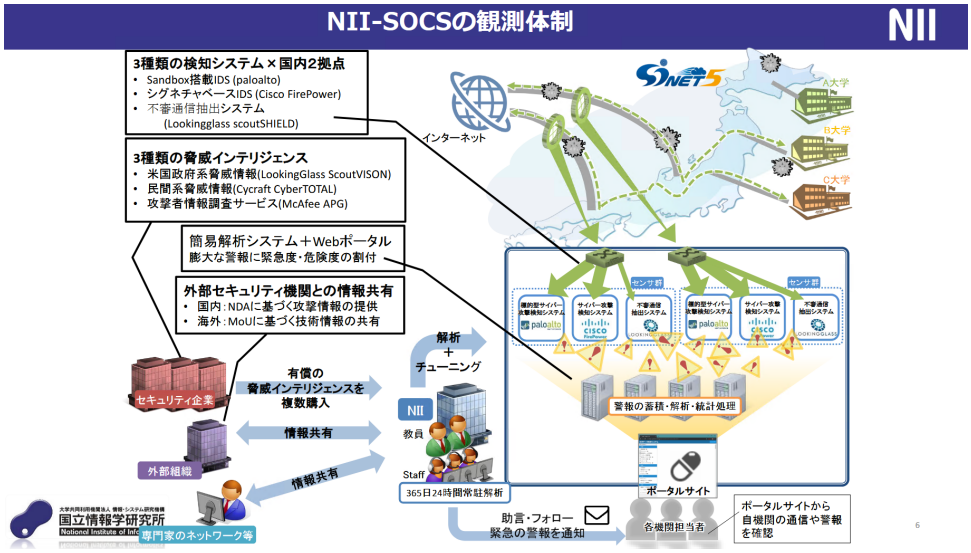


図 9.NII-SOCS の観測体制[8]

その後、各参加機関の担当者が通知を確認することにより、各機関の判断で対応されることとなる。この NII-SOCS の中で行った業務については、記載できないものも多いが、可能な範囲で以下に記載する。

2.2.2. 日々の担当業務

NII-SOCS で導入されている脅威インテリジェンスや OSINT (Open Source Intelligence)に基づく情報収集確認が多くの時間を要した業務となった。これらは、NII-SOCS のセキュリティ体制を底上げする上で重要な役割を担っている。ここでは日々の業務を記載する。

2.2.3. 脅威情報の収集と解析

脅威インテリジェンス機能と web 上の公開情報である OSINT は、発生している攻撃キャンペーンや脆弱性、攻撃者の新手法などをいち早く認識し、解析のプロセスに組み込むことにより、3 種類の検知システムでは検知できない攻撃を検知することが可能である。攻撃に利用された IP アドレスなどを照合する確認作業は、検知システムで可視化されなかった攻撃を早期に発見し、攻撃者の潜伏期間の長期化や被害拡大を防ぐことに繋がる。また、他組織の類似の攻撃情報により、参加機関に攻撃が到達する前段階で通知することも可能とし、インシデント発生数を低減させる。機械的な監視では捉えきれない外部の文脈に基づいた異常を発見できる点は前職の知見が大いに生かされ、またここでも能力のさらなる向上につながる知見を得ることができた。

なお、実施した内容はシステムに多少の差異があるもの KEK で実施した脅威情報の収集とログ分析をシステムが変わっているため新規で作成しなおし発展を含める形で自動化を行った。NII-SOCS の業務の内容から web 上から収集した情報は IP アドレスのみであったが、毎日、悪性の IP アドレスを 40 万件程度取得した。このうち 7 万 IP 程は過去 1 週間で悪性が確認できない新規のものであり、これらを検索対象として被害が疑わしいものの発見に寄与した。

2.2.4. 事例紹介の作成

NII-SOCS では、各参加機関の NII-SOCS 担当者からの応答に対して、月次でまとめ、可能な限り参加機関に情報提供している。着任している期間はこの対応を行った。

2.2.5. Web-API の提供

各参加機関の NII-SOCS 担当者はポータルサイトにログインして情報を取得している。これに対して、各参加機関からは自動化を視野にいれた Web-API の提供の声がいくつかでていた。新機能実装自体は着任前に完成されていたものの、具体的な使用方法例はまだなく、各参加機関は利用可能な状態に至っていなかった。

そのため、この Web-API の機能を提供できるよう、説明資料や実行例などを用意し、希望があった参加機関にはオンラインで説明も行った。

2.2.6. 研修用コンテンツの作成

各参加機関の NII-SOCS 担当者は本サービスの多くの利用はポータルサイトからとなる。ポータルサイト上で提供される情報は専門性が高いため、2019 年からはその説明会を対面で実施された。新型コロナウイルスの流行した時期でもあったため、オンライン化が要望され、2020 年に研修用の動画コンテンツを作成し、サービスポータルに掲載した。操作説明が主の研修はこの動画で対応されている。

2.2.7. その他の支援

NII-SOCS の業務ではないが、過去に繋がりがあった大学の情報セキュリティ担当者から不審な通信を外部組織から受け取ったときにどのように対応することが望ましいかとの相談を受けた。フロー図(図 10)と説明文書を用意し、対応方法について説明を行う機会などもこの在籍期間中にいただいた。

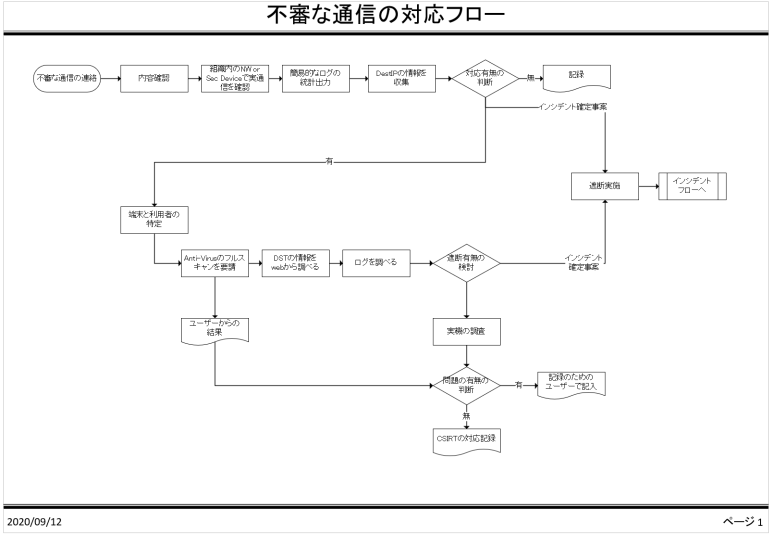


図 10.不審な通信の対応フロー

2.2.8. まとめ

NII-SOCS の単一機関にとどまらず、複数の大学・研究機関が連携し、攻撃検知や防御能力を共有・強化するという設計は、学術ネットワークの性質上、極めて意義が深いと考えている。

NII-SOCS では、通信内容そのものにアクセスすることなく、ヘッダーから得られる送信元 IP、宛先 IP、プロトコルなどの接続の記録から、異常通信や攻撃の兆候を検知するという軽量かつプライバシーに配慮した監視・分析手法を行っており責任分界点が明瞭なアプローチだと感じている。

また、ヘッダーのみの分析の限界があることを改めて認識できた。たとえば暗号化された通信の中身や、巧妙な攻撃手法、あるいは正規通信に見せかけた攻撃などは、ヘッダーレベル分析だけでは判断が非常に難しい。そのため、これを補うために参加機関側の情報として何を提供すればより大学全体が安全になるかなど、防御手段を検討する必要性があることも認識できた。

ここでは結果として短い期間となってしまったものの、次の東京工業大学、また他機関の将来のセキュリティ体制に還元することで、学術ネットワーク全体に貢献できる大きな可能性を頂けた。

第 3 章 東京工業大学での情報セキュリティ業務

3.1. オープンファシリティセンターの情報基盤支援部門について

東京工業大学のオープンファシリティセンターの情報基盤支援部門は，学内の各種情報サービスの提供を行うため，各種システムの開発や運用管理，利用者サポートが行っている。学術情報国際センターの教員及び研究推進部情報基盤課のスタッフと協力して各種システムについてのサービス提供を行っており，今後も学内ニーズの変化に応じて細やかな技術サポートを継続的に行っていくことで，より使いやすい学内情報サービス環境の実現を目指している。

主な学内システムは以下の通り。ソフトウェア包括契約サービス

- 東工大キャンパス共通認証・認可システム
- キャンパスネットワークサービス及びサーバ代行サービス
- キャンパス無線 LAN
- 教育用計算機システム

3.2. 東京工業大学での情報セキュリティ業務

東京工業大学では、オープンファシリティセンターに所属し情報基盤課に派遣されることにより、東工大 CERT の一員として情報セキュリティ対策の支援を行うこととなった。ここでの業務の多くはインターネット上の脅威情報と FW のログを照らし合わせることにより、検知できなかった被害の有無を調査するが主な業務となった。

3.2.1. 公開情報を元にした調査と対応

インターネット上で公開された脅威情報等を基にした調査を実施している。この調査の件数は毎月 40 件から 80 件程度の幅となっている。この他にも外部組織からの情報受領を起因とする調査などもあり、マルウェア感染に関連した学内端末から学外へ行う通信を主に分析する。

これらの調査は、KEK や NII で行ったプロセスと同様である。それらで実装していた自動処理は計算リソース不足により実現できていない。また、自動処理を手動で実施するためにこの調査件数が限界となっている。

計算リソース不足の認識がありつつ実装は試している。しかし、メモリ不足によるスワップ発生を起因とし、同一 OS 上の日常使いの Windows 上で行う他の業務で使用するアプリケーションは応答なしになる、Windows 自体がブルースクリーンになるなど、通常の業務に大きく支障がでるため使用を断念している。扱う IP アドレスやドメインのリストがメモリ上の負担となりやすく、NII で行った自動化と同等のものを使うだけで 30GB 程度のメモリを確保する必要があることが認識できた。
この手動による調査でもある程度の成果は得られており、以下のような対応に発展させている。

- 通信の遮断
- 誤検知と判断した通信は、ベンダーへ連絡しカテゴリの変更申請
- 他組織の被害が確実なものとして確認できた場合には、連絡対応(月 1 件から 3 件)

3.2.2. その他セキュリティ製品等の調査、および PoC

東工大 CERT が扱っているログ分析基盤を高度化するために、現在導入しているログ分析基盤の他に様々な製品の調査を行い、プロトタイプの使用について結果をまとめるなども行った。また、情報セキュリティに関するインテリジェンス製品なども同様に PoC を実施し、選択肢を提示するなどを行う。

PoC（Proof of Concept）は概念実証を意味する。この PoC を行うことにより、無駄な投資を防ぐ、カタログスペックだけではわからない現場のプロセスとの親和性が確認できるなどの効果が得られ、本格導入するかどうかの判断に寄与できる。

3.2.3. まとめ

東工大 CERT の情報基盤課で行った業務では、前職の経験が十分に機能しない場面が多々あった。特に情報セキュリティは関連技術が急速に進化し、専門知識は毎年のように大きく変化している。情報セキュリティに関わる人たちの全員のバランスは非常に難しいと感じた。この差については様々な要因が考えられるが、現在も明確な解決策が見つかっていない状態となっている。東工大 CERT の業務と並行して業務改革推進室の支援も行うこととなり、業務の割合は次第に業務改革推進室の支援へとシフトしていくこととなった。

第 4 章 東京工業大学での業務改革推進室での支援業務

東京工業大学 業務改革推進室の支援業務は、東工大 CERT の業務と並行し、東京工業大学の DX の一部とされたマスターデータ WG へ 2021 年 10 月から参画することとなった。業務の割合は次第にマスターデータが大きくなり、2022 年 11 月からは業務改革推進室へ派遣され、マスターデータと文書決裁システムの運用等に業務の主軸を移すこととなる。

4.1. マスターデータ

東京工業大学では、業務を遂行するための様々なシステムが学務部、総務部、財務部等の各部署により管理運用されている。それぞれのシステムで個別にデータを作成更新がなされているため、所属する教職員や学生の情報も表記ゆれ等の問題が発生している状況である。それを解消するために 2021 年度からマスターデータに関するマスターデータ WG が業務改革推進室の下に設置され、これに 2021 年 10 月から参加した。

4.1.1. マスターデータについて

マスターデータの歴史は古くさかのぼれば、1960 年台から始まったメインフレームと呼ばれる大型汎用機では顧客名や住所など比較的変更が少ないデータをマスターファイルと呼び扱われていた[10]。

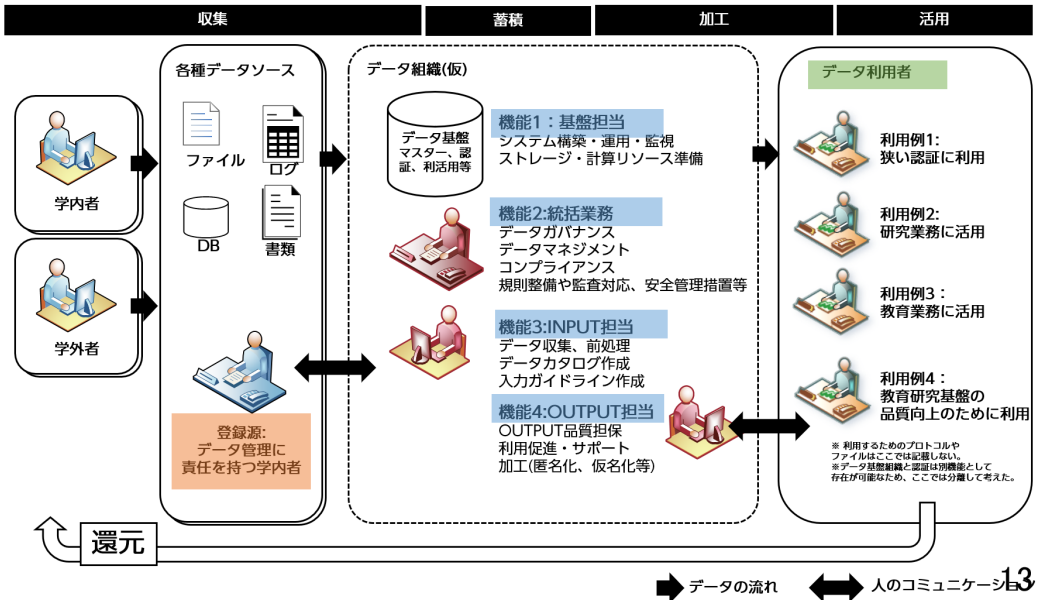
1990 年代にはいると、企業では、販売・製造・会計・人事等の複数の業務システムを統合するための ERP (Enterprise Resource Planning) システムが普及し始め、業務共通のデータを資産としてとらえ、顧客マスターや取引マスターなど一元管理を行われたものの、個別システムによるマスター化までで組織横断的なガバナンスに至る事例はわずかであった[11]。

2000 年代にはいると、データウェアハウス (DWH) や EAI (Enterprise Application Integration) など、システム間の連携やデータ統合の仕組みが進化し、マスターデータを複数部門で同期・共有し、データに対して整合性や監査などの必要性、つまりマスターデータの信頼性が重要視されるようになった。また、この時期に、「データ品質」や「データガバナンス」などデータに関するキーワードが急速に増加し、

技術だけではなく、組織やプロセス視点などを含めたマスターデータマネジメント（MDM:Master Data Management）も普及していった。
2000 年代後半には、マスターデータを企業資産と捉えて、単一に信頼できるレコードの意味を持つゴールデンレコードを目指す動きが活発になった。
近年では、ビッグデータやクラウド、AI やリアルタイム分析などの新技術や新モデルとマスターデータ管理の融合するフェーズに入っており、マスターデータ管理とデータガバナンスは単なる制度や運用から、戦略的データ資産化やデータ価値創出などの一因として扱われるようになっている[12]。

4.1.2. マスターデータ WG の運用組織の提案について

マスターデータ WG への参画の中では、政府の DX や個人情報保護、オープンデータの動向、全国の大学等と NII が連携して構築する学術認証フェデレーション「学認（GakuNin)」の次世代認証基盤の最新情報、他組織の最新事例などの情報を展開するとともに、マスターデータの意識差異がマスターデータ WG 内でも多くあったため、用語の定義をまず作成し提案した。
その中で、マスターデータ管理と本格的な利活用を実施する場合には、以下の機能が必要であると考えて情報を展開した。



この組織では、マスターデータを組織的に運用するための機能として以下 4 つの機能を用意した。

- データ基盤機能

- 統括業務機能
- INPUT 機能
- OUTPUT 機能

提案を行った 2022 年の段階で、一般的にマスターデータの導入は、1 年目から定量効果が出始め、3 年で十分に投資回収可能なモデルと呼ばれるようになっており、実際の事例も多々存在している[13]。

また、上記の図を作成の後に、実際の担当者が考えるべきとしたが以下の 1 から 8 までの手順で設計と構築を今度進めることも提案した。

1. 現状分析

   現在各部局に点在するデータを取りまとめが数年前に実施されていた。その後更新が行われていないため、再度の分析を実施し、業務プロセス、データ品質、運用体制などを再確認する。

2. 背景と目的と対象範囲の再定義

   本マスターデータの背景、目的、対象範囲、そして既存の課題を再度定義し、利点などを明確化する。また、費用対効果も試算する。

3. 要件定義

   マスターデータとして管理すべき情報の項目、データの粒度、識別子、更新責任、整合性などの原則を定義する。

4. データモデル設計

   エンティティ、属性、リレーション、コード体系などを確認し、本学共通のデータ構造を確立する。また、正規化、階層化、命名規則などの指針となるドキュメントの整備も行う。

5. データ移行計画

   プロトタイプの作成、およびそれを用いた既存システムからマスターデータが格納される基盤へデータ移行するための方針、移行方法、データクレンジング手順を決定し、品質チェック方法なども検討する。また、ここで利用者へのデータ提供や他システムへの連携設計も行う。

6. マスターデータ基盤構築

   プロトタイプで得られた知見を基にし、DB 構成、インターフェース、権限管理、バッチ処理設計など技術的な詳細をまとめ、構築する。

7. データガバナンス体制の構築と整備

   継続的にデータの品質が維持できるよう、データ管理責任者、更新承認フロー、メンテナンスルールなど運用ルールを設計する。

8. 運用設計

   日常の運用手順、定期的な品質監視などを定義し、どの程度の時間が必要かも検証する。またどの程度の段階でスケールアップが必要かなども設計する。

上記以外に関係者、特にデータ入力を担当する職員へのデータスチュワードの教育や研修体制、利用者サポート、データ品質の検証評価、そして今後広がるデータの利活用に向けた拡張計画なども必要であることも記載したものを提供した。

4.1.3. まとめ

本プロジェクトは、提案まで行えたものの大学統合により人的資源の懸念から凍結となった。この中では DMBOK 等様々なデータを扱う業務、データエンジニアやデータサイエンティストに関わる知識を学びなおすことができ、また情報セキュリティやそれ以前で得られた組織運営の知見が設計の段階だけでも多く応用できたことや EU 圏で行われているデータマネジメントとの差異の認識を改めてできたことなど多くの発見を得らえた。なお、東京科学大学としてより発展させた形の検討が 2025 年現在進められている。

4.2. 文書決裁システムの運用支援

東京工業大学 業務改革推進室では、事務局などが組織的に行う業務に関する申請の電子化を DX(Digital Transformation)の一環としている。この電子申請を迅速に実現するために、T2APPs(Tokyo Tech Application & Approval system）と名付けた文書決裁システムを 2021 年 4 月から本格的に運用開始した。

前項のマスターデータ WG のとりまとめを行っている業務改革推進室への技術支援を 2022 年 11 月から本格的に実施することとなった。

4.2.1. T2APPs の概要

T2APPs の利用者は構想段階から東京工業大学の全構成員としており、これを利用するためには東京工業大学の認証基盤である東工大ポータルの SAML 認証によるシングルサインオンを必要とすること、また申請以外の様々な業務に対応できる汎用性を持つことなどが要件とされた。この要件から基盤となるシステムは、住友電工情報システム株式会社 楽々WorkflowII とされた。システムは大きく二つに分けられ、学生や教職員から申請を受け付ける本番環境と業務担当部署が利用し本番環境前のテスト構築や動作確認などを実施する開発環境を用意されていた。

T2APPs の本番環境には、東工大ポータル、および学生の情報を管理する学務部から、ユーザーID や氏名、所属情報など、合計 258 項目の様々な情報の提供を日々受けている。そこからユーザー情報、組織情報、ユーザー情報と組織情報の紐づけを行うためのグループ情報等を再成形し T2APPs に取り込むことにより、日々更新される教職員や学生をはじめとした東京工業大学の全構成員の最新情報を自動的に反映していた。

開発環境では、実際の人員配置に似せたデモアカウントを用意しており、T2APPs で申請文書管理の利用を希望した業務担当部署に所属する職員に対してのみ提供している。これにより業務担当部署に所属する職員自身で申請文書管理を開発することを可能としている。また、製造元が提供している e ラーニングがあることから、開発環境にはその受講を可能とする環境も併せて用意している。

T2APPs では、ユーザーの権限を大きく以下の 3 つに分類している。

- 申請を行うグループ
- 申請文書管理を行うグループ
- T2APPs 管理グループ

申請を行うグループには、東京工業大学の全構成員が入り、さらにこの中の大きな区分として教職員と学生がある。これにより、各業務担当部署は、申請者を学生、教職員、またはその両方を申請者として設定することが可能となっている。

申請文書管理を行うグループは、主に事務職員が入っており組織図と同一の配置構造を持たせている。また、申請文書管理の管理権限も組織図に記載されている業務担当部署に対して原則与えられ、ユーザーには与えていない。属性情報の一つである組織図上の所属情報に権限が振られるため、人事異動などのユーザーの変更に影響されない。そのため、ユーザーは当該部署から別の部署に異動すると文書管理は行えなくなり、また別の部署から当該部署へ異動すると文書管理が行えることとなる。最後の T2APPs 管理グループは業務改革推進室のユーザーを手動で設定している。

4.2.2. サーバの引継ぎとシステム改善

筆者は、この文書決裁システムの運用への業務支援を 2022 年 11 月から行うこととなり、支援の当初は申請文書管理の実装支援を行いながら、楽々WorkflowII のマニュアルの確認や現状の構成確認などを行っていた。サーバの運用については 2023 年 4 月から本格的に引継ぎ T2APPs の基盤全体の運用管理を行った。

4.2.2.1. 引継ぎの後に実施したサーバ運用の改善について

サーバの運用を 2023 年 4 月から引継ぎ、運用と様々な改善を行っている。本製品は、製造元によりインストールが実施され、そのまま使用されていた。

引継ぎ直後に実施したのは、バックアップから復元が可能かどうかの確認し、問題が発生した場合にいつでも別のサーバ上で復元できる手順を確立した。また、引継ぎ当時はサーバ上のパフォーマンスを起因とするトラブルが発生していた。問題が発生した後に応急処置的な対応になることを防ぐため、本番環境と開発環

境の複数台存在するサーバを集中監視するためオープンソースの統合監視ソフトウェアである Zabbix を導入し毎朝 1 回目視で確認するようにした。アラートを設定することも可能であるが、毎日の変化に少しでも気が付けるよう目視での確認を継続している。その他、IP アドレスやユーザーの権限などによるアクセス制限を行うなども実施した。

2023 年 5 月からは、毎月第 3 木曜日の夜に月例メンテナンスを行うようにした。この月例メンテナンスにより、OS/ミドルウェア/楽々WorkflowII 等のアップデートを行い、可能な限り最新の状態を保つこととした。また、製造元の情報を毎日確認し、改善につながるような内容があれば業務改革推進室内にその情報を展開し次回の月例メンテナンスに変更を加えるものを準備するようにした。マシンスペックを起因とするような問題が発生するたびに設定変更を加えていくことで、2023 年 8 月頃から問題は発生していない。

4.2.2.2. ログ分析システムの導入

申請文書管理を行う業務担当部署からは、申請者から受けた問い合わせや、申請の承認経路の途中で問題が発生した等の様々な問い合わせが業務改革推進室に日々よせられる。これらの問題の切り分けを行うために、ログ分析システムである Splunk を 2023 年 6 月に導入した。楽々WorkflowII の基本機能からもログの閲覧は可能であるが、問題の発生区分ごとにファイルが作成され、さらに日毎に分離されるテキストファイルにログが保存される仕組みである。そのためログを閲覧するには、複数のテキストファイルを確認することとなるが、業務担当部署も申請者からの伝聞からの問題発見も多く、伝言になった曖昧な情報から問題の切り分けを迅速に実施することは困難だった。ログ分析システムを導入してからは、曖昧な情報からでもその症状を確認することができるようになり、また同じ時間帯に発生した事象を確認することが容易になったため、問題の原因を見つけることができるようになった。

4.2.2.3. デザインの変更

引継ぎ当時は、製造元のロゴなどが表示されている状態であった。T2APPs のロゴを作成し、デザインの変更を 2023 年 8 月に実施した。デザインの変更により申請者の混乱が生じる懸念があったが、そのような声は業務改革推進室には届かなかった。

図. 引継ぎ当時の画面イメージ

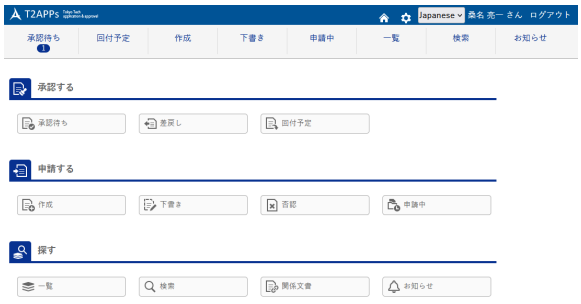


図. デザイン変更を行った画面イメージ

ロゴについては、東京工業大学のシンボルマークである燕を主題とし、2 匹の燕で、Application や Approval の頭文字を表現するようなデザインが採用された。作成については、手書きで書いた 2 匹の燕のシルエットを Adobe Illustrator でパスを取った。配色については、東京工業大学ビジュアルアイデンティティマニュアルに記載されているロイヤルブルーを使用することとした。

図. 作成した T2APPs のロゴ

4.2.2.4. メニュー等の整理

申請文書管理の実装支援では申請者となって申請を進めるテストを行っている。その際に申請を行うグループに表示しないことが望ましい機能がいくつかあることに気が付き問題提起を業務改革推進室に行った。その結果、T2APPs の 3 種類のユーザー権限で表示される各種メニューについて、それぞれの権限でどの機能が必要かどうかを再検討し、2023 年 8 月に整理を実施した。また、本番環境と開発環境で表示するメニューも異なっていたため整合性を取るため同様の表示にした。申請文書管理を行うグループには、今後必要とされる機能も考えられたが、この時点で利用がないものは無効に設定した。また、開発環境のデモアカウントについても不要なものが多く登録されていたため、不要なものを削除するなども合わせて実施した。

4.2.2.5. ライセンスの増強

開発環境には、専用のライセンスを使用しており、同時アクセスは 5 アカウントまでとなっていた。6 アカウント目からは、ログインしようとすると上限に達したとの表示がされる。この上限に達した数の計測を行い、2023 年 8 月には 1247 回上限に達していることが確認された(図 4)。この情報をもとにライセンスの調達を行い、11 月に増強することにより同時アクセス数の上限が撤廃された。なお、ログの出力設定を 7 月に変更したことにより計測が可能になったため、それ以前に上限に達していた数は不明である。

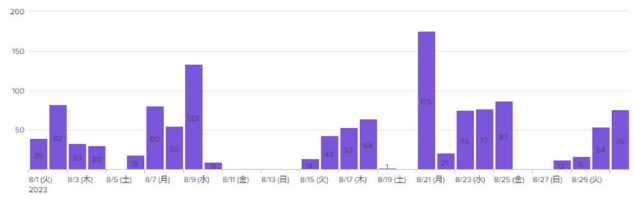


図. 2023 年 8 月に発生した同時アクセスの上限のエラー状況

4.2.2.6. 法人番号検索の再構築

いくつかの申請文書では他組織の名称や住所を入れたいとの要望がテスト段階からあり、国税庁が法人番号公表サイトで提供する法人番号情報をもとに POPUP で呼び出すよう楽々WorkflowII の機能により実現している。しかし、この法人番号の情報は 2020 年 3 月に構築した当時のままだった。業務担当部署から 2024 年度は最新の情報を利用したい要望があったことから、2024 年 1 月に新たに法人番号検索の実装を行った。

この実装では、既存の法人番号検索から変更点が大きく 2 点あった。1 点目は法人番号公表サイトにあるリソース定義書に準拠した内容に変更したこと、2 点目はこの法人番号の情報が自動的に更新される仕組みを作成したことである。自動的に更新される仕組みは、Microsoft Power Automate を用い web から最新情報を週 1 回ダウンロードし、WSL 2 からデータベースに接続しデータの更新を行うようにした。

なお、法人番号公表サイトの情報に準拠したことにより、呼び出し方法が以前と異なることから、既存のものとは別に version 2 として新規に作成した。そのため、現在は 2 つの法人番号検索が存在する状況になっている。

4.2.2.7. 楽々WorkflowII の各種パラメータ変更

本番環境と開発環境の設定が異なる部分が引継ぎ時点では多くみられた。本番環境と開発環境の整合性を保つよう修正を行っている。整合性を保つことにより、問題の発生を防ぎ、メンテナンス性が向上し、バージョンアップの実施の煩雑さを軽減している。楽々WorkflowII のコンフィグの修正については、diff コマンドで本番環境と開発環境の比較を行い、差が発生している箇所について製造元のマニュアルを確認してから修正する。その際に行数を合わせるなども実施した。

4.2.2.8. その他

当初から申請文書管理実装支援を行った。また、月例報告などを残すことを提案し2023 年 11 月から作成するなども行っており、関係する委員会で報告されるようになってきている。
その他、楽々WorkflowII を専門に扱った開発を行っている委託業者 2 社との関係の構築や、情報セキュリティの問題が発生した場合に備え、セキュリティベンダーとの関係構築を行うなど、有事の際には迅速に対応できるよう運用体制の強化も行った。

4.2.3. 申請文書管理の実装手法について

事務局が実施する業務には申請から開始するものが多く存在する。申請文書管理の T2APPs への実装については業務担当部署と共同で実施している。その大きな流れについて述べる。

4.2.3.1. プロジェクトの開始

申請業務の担当部署が T2APPs の利用希望を業務改革推進室に連絡することにより T2APPs の本番環境への実装の第一歩となる。実装を希望する内容が T2APPs で提供している内容に沿っているかどうか等の意見交換を実施した後にキックオフミーティングを必ず実施した。

キックオフミーティングではメンバーの顔合わせと共にプロジェクトの意義や目的の明確化がなされる。これを実施することにより参加メンバーの役割も明確化され、今後発生するタスクの重複や抜けを防ぐ等に影響していると考える。

また、ミーティングの後には T2APPs の開発環境へのログイン権限等を設定し、業務担当部署に提供している。開発環境上で e ラーニングの受講やテスト的な構築を実施されることにより、申請文書管理の技術的な実装や管理などの理解を進めていただく。なお、場合によっては T2APPs の実装のイメージをしやすくするために、現状の Excel や Word ファイルの申請様式をもとに業務改革推進室により開発環境上で仮のものとして実装することもあった。

4.2.3.2. 現状分析と要件定義

申請文書管理に関する業務を対象に現状分析を実施する。BPM（Business Process Management）を基礎として、業務担当部署の業務手順だけではなく、申請者の申請手順と業務担当部署の範囲外になりやすい申請者自身の目的と前後の手順なども確認し、またそれに関わる直接的な利害関係者と間接的な利害関係者も確認していく。これに合わせて申請にある情報から誰がどのような情報を追加し利用しているか、それらをまとめる報告書や提出先があるか等の把握も実施する。また、必要に応じて業務の根拠となる関連規則や法律等の確認も実施する。これら業務の深堀により業務担当部署で再認識が行われ、これ以降の流れで抜けの発生が軽減されると考えている。

現状分析した結果を用い、再度その全体の流れを確認する会を実施する。申請業務全体を俯瞰することにより、現状の問題点を言語化できるようになり、新しい解決方法などが浮かぶことも多い。ここで出た意見をもとに要件を定義していく。申請者、業務担当部署、および関係者の導線を再設計する。再設計では、現状の問題点を解決のために、現状とは大きく異なる導線になることもある。特に異なる関係者による重複した確認などは省略される場合が多い。

また、本番稼働までの現実的なスケジュールもここで再度確認され、それに向かい、各種関係者に必要な情報提供の開始も始まる。

4.2.3.3. 申請文書管理の設計と実装

現状分析と要件定義で決定した内容に従い開発環境上で実装を進めていく。前項までに申請で取得する情報などが確定しているが、システムに実装する場合には細かい情報が抜けている場合も多い。例として住所の情報取得が必要な場合、郵便番号の取得が必要かどうか、住所を分割する必要があるかなどである。そのため、業務担当部署における情報の再利用性なども検討にいれ、設計の再確認を詳細に行いながら実装していく。実装では、申請者の申請画面、業務担当部署の管理画面、申請が進むことにより発生するメールの文面などを、日々発生する業務で実際に使っている場面を想像しながら検討を行う。また、英訳も必要に応じて実施している。

4.2.3.4. 本番準備

旧手続きからの移行方法や業務担当部署による申請管理文書を利用した日々発生する業務の詳細な再確認が確認され、現状分析と要件定義で出た問題点が解決できているかなどを含めたテストを実施する。合わせて申請者向けのマニュアル作成やホームページ修正など本番稼働に向けた準備を行う。

4.2.3.5. 本番稼働

楽々WorkflowII の基本機能には、申請文書管理のインポートエクスポートや申請を受け付けなくするメンテナンスモードなどが存在している。これらの機能を用いて開発環境で作成した申請文書管理を本番環境へメンテナンスモードで移植する。本番環境へ移植後、権限が意図した通りに設定されているか、開発環境と比較しながら確認していく。

確認が完了したらメンテナンスモードを解除し、必要に応じて関係者に案内を実施していく。

4.2.3.6. プロジェクトの振り返り

この申請文書管理の本番環境までを振り返りを本番稼働した数か月後に実施する。ここでは申請文書管理の実装により達成できたことや効果、成果などの文書化を行い、プロジェクトの反省点や実装後確認された課題なども共有し、さらなる改善に向けた方針を確認している。振り返りを実施してどの実装でも確認された成果については、以下の通りである。

- Excel や Word ファイルに申請者自身で記載することで発生していた表記ゆれが減った。
- 学生からの申請の場合には、指導教員の承認得てから業務担当部署に届くものもある。このような承認経路の場合でも業務担当部署による把握が可能となり支援しやすくなった。
- 申請の集計などが簡単に実施することができるようになり、繁忙期の負荷が減った。

4.2.4. 文書化技術

この業務においては、文書化の技術が多く必要となった。主に必要となった文書化の手法については、特定のプロセスを適切に進める文書化手順とほぼ同等であり、情報処理推進機構(IPA)の組込みソフトウェア向け開発プロセスガイドやプロジェクトマネジメントの標準と言われる PMBOK® ガイドなどでその技法は十分に学ぶことができる。

この文書化技術と文書の運用を行っている中で、いくつかの条件が満たされない場合に例外が多く発生し、期待する結果が得られない場面に遭遇した。みなさまの何かの助けになるかもしれないと考え箇条書きで記載する。

文書化の段階のアンチパターン

- プロセスが明確化されない。
- 責任と作業の境界が不明瞭。
- 期待するアウトプットが明確でない。
- プロセス単体を完了するために必要なものが何かが認識されていない。
- プロセスを実際に確認していない。
- 見えない関係者が存在する。
- 詳細を記載しすぎる。

運用の段階のアンチパターン

- ツールとして利用していない
- 例外が常に発生する可能性を考慮しない。
- 文書を読まない。内容を把握している人がいない。
- 現実の内容が変わっても文書は放置。

また、間近の問題解決のために関係者への思いが至ってない場面にもいくつか出会っている。このような場合には、倫理観を確認する作業が必要となり以下の点を確認した記録もあったため合わせて記載する。

- これは誰かが不当な扱いを受けないか
- ヒアリングの内容は事実と異なっていないか、前後に情報が隠れていないか
- 規則等基本的な倫理に反していないか
- 弱い立場などを不当に利用していないか
- この実装は、後で思い出して誇れるものか

このような話題を振る場合には、軽率に扱うとすべてが覆るリスクになることも併せて説明しているつもりであるが、同時に正しく伝えることが難しい話であるとも感じている。

4.2.5. DX として

様々な背景から様々な場所で DX（digital transformation）が進んでいる。しかし、業務の電子化が進んではいるものの、そこから先の Transformation に到達できない事例も多い。本章の文書決裁システムも同様の状態であることを認識している。本来の DX は単なるシステム化に留まらず、データとシステム、プロセス、AI 等を統合し、組織を継続的に最適化する機能が必要と考えている。

まず一般的に DX に至るためには以下の 3 つのステップが必要と考えられている。

1. デジタイゼーション

   アナログ情報をデジタル化する

2. デジタライゼーション

   業務プロセスをデジタル化する。（効率化、コスト削減なども含む）

3. DX

   データ、AI、自動化を活用し、プロセスや組織、ビジネスモデルを再構築する。

これらを実現するための技術領域は広く、データ統合基盤、データマネジメント、継続的な分析とシミュレーション、組織の縦割りを超えたプロセスの自動化、クラウド、AI の組み込み、そして情報セキュリティを組み込んだ設計などが必要となる。

データ統合基盤、データマネジメントにマスターデータは含まれ、データを信用できる状態にする。データが信用できない場合は、コストが高くなり運用が続けられないなどのリスクも含まれるようになる。

継続的な分析とシミュレーションでは、BI やダッシュボードが必須とし、重要業績評価指標（Key Performance Indicator）の一元管理などを行い、人が分析レポートを作る必要がなく、情報を必要とする教職員自身で理解を深める体制を構築する。またそれを支えるために、分析や評価、未来予測の自動処理や精度の品質保持のために劣化の自動検知が必要となる。

組織の縦割りを超えたプロセスの自動化では、与えられた権限の範囲でシステムを接続し情報連携を可能とし、組織内の各部署が効率よく業務を行えるようにする。これにより、部署が別部署の依頼で情報を渡す場合の感情的な問題を排除できると考えている。

クラウド、AI の組み込みについては DX の本質ではないと考えている。クラウドの強みとしては、最新の状態がいつでも利用できる拡張性や災害対策の面では大きな恩恵を受けると考えている。一方で緊急時の利用費用の難しさやデータ管理、インターネット依存、カスタマイズ性や他クラウドへの移行の難しさなどのデメリットもある。ＡＩについてはプロセスに適切に組み込むことにより自然と業務の品質が向上する。

セキュリティを組み込んだ設計については、必要となる領域は広く説明は難しい。基本的な要素としては DX を支えるシステム群は、アカウントベースの認証と権限は信頼の最小化が必要となりやすい。そして異常検知と変化検知を継続的に実施し異変を察知する仕組みが必要となる。

結論としては、ＤＸはデータを軸として、業務、組織、技術を継続的に最適化するための仕組みを構築ものと考えている。また、継続的に実施することからサイクルが必須となる。これらを実装するための最初の一歩はプロセスの可視化と考えている。

本業務については、2024 年 3 月に開催された第 24 回令和 5 年度 高エネルギー加速器研究機構技術職員シンポジウムなどで情報共有したものを再編している。

4.2.6. まとめ

2024 年 10 月に東京工業大学は、東京医科歯科大学と統合し、東京科学大学となり、T2APPs については廃止とされた。製品名である楽々Workflow II を全面に出し新たな方法で運用することなり、本業務については終了となった。

東京工業大学では T2APPs を DX の一環としていたが、実施している申請文書管理は東京工業大学全体を見ると多くはない。同様の申請文書管理が東京科学大学でさらに拡充されることにより、業務担当部署と業務担当部署が連携した部署横断型の申請を提供することが可能となることを期待する。またシステムにデータが蓄積され正しく活用されることにより業務の改革がより一層進み、その結果が全構成員に還元されることを期待する。

第 5 章　東京科学大学すずかけ台キャンパスの情報基盤支援

東東京科学大学の情報に関する支援体制は情報基盤センターが行っている。大岡山キャンパスには旧学術国際情報センターが湯島キャンパスには旧統合情報機構がある。すずかけ台には対面の相談人員は配置しておらず、旧学術国際情報センターの頃から配置の要望があった。統合したことを機にすずかけ台キャンパスの情報に関する研究教育業務の支援を情報基盤センター長の下で 2025 年 7 月から試験的に実施することとなった。

事前にサービスの提供内容について、全学の標準的な手順から逸脱することを防ぐことを目的に支援の内容や対象者の定義を行い、その範疇を原則とした。また、対応の事前準備として、東京科学大学で導入されている Slack を用いた各サービスのチャンネルを洗い出し、その質問と対応に目を通した。これは現在も継続して観察している。

5.1. 日常の研究業務支援

東京科学大学では全学のコミュニケーションツールとして Slack を利用している。ここでは学内外の各サービスのヘルプ用のチャンネルも用意されているが数は 200 に近い状態である。そのため、小規模では発生しないような問題、例えば情報量の増大によるチャンネル乱立やスレッド追従が困難となる、決定事項の再利用性が困難になるなどの課題が顕在化していると考えている。大岡山キャンパスでも目的の情報にたどり着けない、探しても見つからないなどの声をよく聞く。

すずかけ台キャンパスでは、数名配置の部署も多く部署ごとの IT リテラシーの差も表層に表れやすい。そのような部署に対しては、本サービス説明時に現状のＤＸに関連する課題が共有いただけたりするため、Slack の場合では目的のヘルプチャンネルや探し方などのノウハウを提供したりすることもある。Slack のＤＭで個別の相談があった場合には、東京科学大学のワークスペースを確認し、情報があればそれを提供する。ない場合には一般的な説明を作成し返答し、関連する窓口が明確であればその情報を提供している。

5.2. ネットワーク・情報セキュリティ支援業務

すずかけ台キャンパスは、昭和 50 年に長津田キャンパスとして開設されている。そのためネットワークの整備状況についても他のキャンパス同様に歴史は長い。現在では、ケーブル敷設やネットワーク設計を行った担当者は世代交代している部署も多く、引継ぎが不十分なままの運用が継続されている事例もある。長年の経緯から不透明化しているネットワーク環境を可視化できるようにし、ネットワーク基盤の信頼性と保守性を回復することを目的とした支援を行っている。

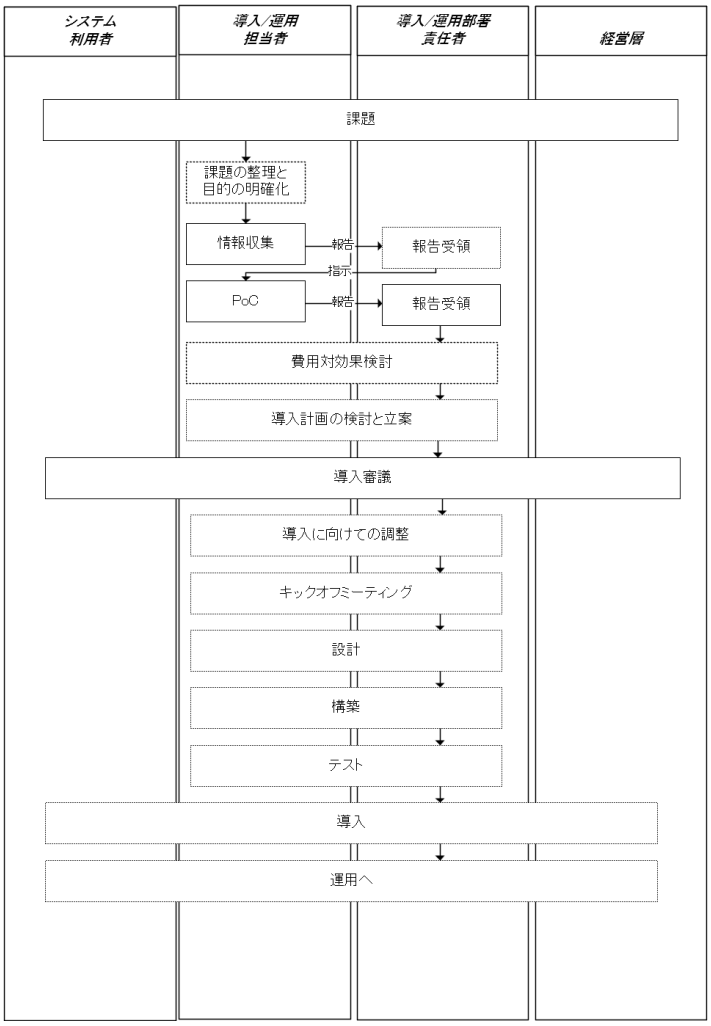
現在まで対応を行った、もしくは現在進行中の事案としては、以下のようなものがある。

- 有線ネットワークが断線状態にあった部署におけるネットワークの回復支援
- ネットワーク配線の見直し支援
- 東京科学大学の学外から自組織がどのように見えているかの調査と改善点の提示

5.3. 導入支援業務

東京工業大学でシステムを導入する場合、多くの場合は各部署が個別に進めていた。東京科学大学の理工学系でもそれは継続している。そのため、品質が部署ごとにばらつく、似たようなシステムが導入されている等の問題が多く発生している。

そのため、情報に関するシステムの導入支援を行っている。相談件数はまだ少ないが、主に現状を把握するためのヒアリングから開始する。また、筆者が過去に行った調達をまとめたものを用意し、現在のプロセスに応じて、そこから部分的に提示するなどを行っている。



5.4. まとめ

この対応の報告に関連した情報基盤センター長を含めた打ち合わせを隔週で実施することとした。2 回行ったら 1 回報告することとなる。優先度判断を間違えない、現場判断の偏りを減らすなどを目的としてできるだけ細かい報告を行うこととした。

現段階ではまだ試用期間であるものの、本サービスの需要は高いと考えている。支援のフローやエスカレーション基準、対応記録のルールなどの整備もこれからでありできる限り早期に実現したいと考えている。

第 6 章　総括

6.1. まとめ.

前々職の KEK では、KEK CSIRT を中心に情報セキュリティに関する支援全般を担い、特に研究者のインシデント対応を早期に完了させ研究業務に早く戻ってもらうことを第一優先としつつも可能な限り安全な環境を維持することに努めた。さらに、NII-SOCS では先端的な技術を用いた分析業務に携わり、参加機関の情報セキュリティ担当者への支援を行った。東京工業大学では、情報セキュリティに携わりながら、DX の実装業務を行った。
情報系の技術職員としては、ネットワークやセキュリティ機器や新しいデバイス等の導入・維持・運営を行う研究支援系と大学内の情報関係の基盤設備を継続的に運営保守する施設管理系の要素が複合的に必要であることがわかる。また、利用者の対応では、実際の技術操作方法などを提供する必要があり、これは教育支援系の知見も必要となることが多い。携わった業務を統括的に見ると、情報系の技術職員としては、以下のように問題が起きない、もしくは問題が発生しても早期にもとに戻すようにすることが主軸となっていると考えている。

- 障害が発生しないようにする。/障害が発生しても早期に復旧させる。
- 攻撃を未然に防ぐ。/攻撃で被害を受けても早期に検知して復旧させる。

もちろん影響がでないようにバックアップを行う、同じ問題は再発させないなども含む。安全性、安定性、継続性を重視し、日々必要な様々な基盤を確実に動かすことに高い優先度が設定されている。

情報系の技術職員として業務に携わると組織内の様々な立場の関係者と多く接する。業務を行う上で、良い情報だけでなく悪い情報を認識した上で関係者との目的と優先順位の合意や、そのための文書化、その後の目標到達に必要なプロセスの明確化を行う必要が多い。関係者の中には便利さや業務の効率性に高い優先度を設定している場合も多い。目的、優先度の違い、時間の範囲などが業務の特性上大きく異なることも認識している。それぞれ異なる重要な役割を担っていることから、このような差異は自然に発生するものとも考えている。これらの差異は、丁寧な議論を行うことができれば関係者がそれぞれ補い合う強力なパートナーとして発展しチームとして最大限のパフォーマンスを発揮させることができ、また大きな結果に繋がることを前々職の KEK で多く体験させていただけた。

現在は技術が急速に進化しており、専門知識は毎年大きな変更を余儀なくされており、また複雑化もしている。専門の技術者でもついていくことが非常に難しいと感じている。専門でない関係者の中では、知識を積み重ねていないことを背景として、技術者以上に説明を受けても理解しきれないことが多くなっていることを感じている。

東京科学大学に統合された現在では、これらの知見を活かし、すずかけ台を中心に情報系の技術支援全般のサービスを開始している。急速に利用が促進されたDX 等の利用方法などを丁寧な説明とメリットデメリットの提示をわかりやすく説明することを心掛けながら、全体の情報技術の底上げにつなげたい。また、相談件数の桁が変わる手前で常にサービス自体の見直しを行い、安定したサービスを常に提供できるように努めていきたい。

6.2. 今後の展望.

情報系の技術は過去数十年進化が止まることがなく、今後もさらに加速度的に進化していくことが予想されている。特に生成 AI は、情報セキュリティにおいては運用の自動化や脅威分析に至る広域に影響をすでに与えている。データエンジニアリングの領域においても、データ品質管理、再現性、メタデータ管理などが技術的な課題だけでは解決しない、組織の合意形成の対象となり組織を表すシステムとしての性格を強めており、情報技術の進化は、どの領域においても複雑化している。

こうした日々変化する膨大な情報を前にしても安易な解釈や過剰な単純化をするのではなく、何が事実か、何が推論か、何がわからないのか。を丁寧に読み解く必要がある。間違った情報は組織にとってリスクになる場合もある。情報を見ただけでは、事実と解釈の境界は一見では間違うことも多いことから、慎重に見極める必要があり、正しく見極めた上での決定は揺らぐことは少なく継続性も高い。

組織において情報利用を推進していくためには、理論を現実的な実践にするための懸け橋として技術職員が不可欠と考えている。また、様々な情報を基にした決定がマネジメント層によりなされ、様々な関係者が信頼しあい支えあいながら進めていくことを望んでいる。その中で技術職員として、関係者が理解しやすい形で技術的な情報を伝えながら、場合によっては反発や失敗リスクを理解したうえで提案をし続け、技術的な課題の責任を負い、相手から嫌われる可能性を承知し

つつ必要な忠告を行うことが必要であると考えている。そのよりどころとしたいのは「事実を見極める力」と「人を尊重する誠実さ」であり、これらを丁寧に説明しつつ関係者で落としどころを模索することがよりよい結果へ繋がるものと考えている。

今日の情報系における知見は、多くの関係者の献身と協働の積み重ねによって成り立っている。私たちはそれに報いるためにも、より良い情報基盤の運用と価値創出の循環を築き上げていく必要がある。ここに示した内容がその端緒として寄与することを期待したい。

研究業績および研究支援業績

共著論文 ※旧姓：馬場

[1] 粗い分割のキャンパスネットワークにおける IP アドレス棚卸作業
鈴木 聡, 村上 直, 湯浅 富久子, 金子 敏明, 馬場 亮一, 中村 貞次, 橋本 清治, 西口 三夫
研究報告インターネットと運用技術（IOT）

[2] 2018-IOT-40 EPJ Web of Conferences
Long-term experiences in keeping balance between safety and usability in research activities in KEK 2018
https://www.epj-conferences.org/articles/epjconf/abs/2019/19/epjconf_chep2018_08001/epjconf_chep2018_08001.html

[3] HEPiX Fall 2017 Workshop
Current Status and Future Directions of KEK Computer Security
https://indico.cern.ch/event/637013/contributions/2739326/

総説・テクニカルレポート、関連する発表

[1] 第 20 回 共同利用機関におけるセキュリティワークショップ
セキュリティに関する情報収集方法と自動処理等について
2016 年 8 月 22 日開催

[2] 第 21 回 共同利用機関におけるセキュリティワークショップ
KEK tec report
2018 年 1 月 25 日開催

[3] 日本シーサート協議会 SSH サーバセキュリティ設定ガイド V1.0
茂岩祐樹 DeNA CERT 株式会社ディー・エヌ・エー, 寺田真敏 HIRT 株式会社日立製作所, 徳田敏文 IBM-CSIRT 日本アイ・ビー・エム株式会社, 戸田洋三 JPCERT/CC 一般社団法人 JPCERT コーディネーションセンター, 中野渡敬教 Fuji Xerox-CERT 富士ゼロックス株式会社, 中村暢宏 YIRD ヤフー株式会社, 馬場亮一 KEK CSIRT 高エネルギー加速器研究機構, 平岡洋介 JSOC 株式会社ラック, 宮本久仁男 NTTDATA-CERT 株式会社 NTT データ, 宮本靖 Met-CIRT メットライフ生命保険株式会社, ラウリ コルツパルン CDI-CIRT 株式会社サイバーディフェンス研究所
https://www.nca.gr.jp/activity/sshconfig-wg.html

[4] 国立情報学研究所 NII-SOCS
警報検索システム Web-API 利用ガイド v1

[5] NII-SOCS 研修
https://meatwiki.nii.ac.jp/confluence/x/XiFsB
(NII-SOCS 参加機関担当者のみ閲覧可能)

[6] 情報セキュリティ緊急対応手順説明会
https://www2.kek.jp/proffice/archives/confdb/detail.php=CID=LECT31.html

その他、セキュリティ講習会、新任職員研修会、KEK 新入生ガイダンス等多数。

参考資料

[1] KEK Computing Newsletter 2003 年 6 月 20 日 発行（No. 181）
https://ccwww.kek.jp/kekccnl/CN_NEWS/NEWS_n181.html

[2] 情報セキュリティ 11 の対策
https://www2.kek.jp/uskek/pdf/11measures20170316J-pict.pdf

[3] SSH サーバセキュリティ設定検討 WG
http://nca.gr.jp/activity/sshconfig-wg.html

[4] Activity Report 2013 Computing Research Center
https://www2.kek.jp/arl/about/crc/

[5] 高度情報化とセキュリティ
https://www.jstage.jst.go.jp/article/johokanri/31/7/31_7_627/_pdf/-char/ja

[6] 情報セキュリティセミナー
https://www.kek.jp/ja/research/conference/20231016

[7]大学間連携に基づく情報セキュリティ体制の基盤構築（NII-SOCS: NII Security Operation Collaboration Services）
https://www.nii.ac.jp/service/nii-socs/

[8] 大学間連携に基づく情報セキュリティ体制の基盤構築(NII-SOCS)について
https://www.nii.ac.jp/openforum/upload/2-setsumeikai20210119_nii-socs.pdf

[9] 東工大 CERT が考える、コラボレーションとセキュリティの最適解
https://ascii.jp/elem/000/004/055/4055915/

[10] A Brief History of Master Data
https://www.dataversity.net/articles/a-brief-history-of-master-data/

[11] Evolving from Data Management to Master Data Management
https://support.sas.com/resources/papers/proceedings12/125-2012.pdf

[12] The Evolution and Future of Master Data Management (MDM)
https://profisee.com/blog/evolution-future-master-data-management/

[13] The Business Case for Modern Master Data Management Using the Forrester Consulting ROI Calculator
https://www.reltio.com/resources/blog/forrester-total-economic-impact-tei-roi-calculator/

謝辞

TC 論文主査の友石 正彦教授（東京科学大学 情報基盤センター長 / 副理事（情報基盤担当））、ご多用の中、副査をご快諾いただきました松浦 知史教授（東京科学大学 情報基盤センター / 教授／副センター長）、鈴木聡 准教授（高エネルギー加速器研究機構 計算科学センター）には、本論文執筆にあたりご指導ご鞭撻を賜り、篤く御礼申し上げます。

清水良幸部門長(東京科学大学 リサーチインフラ マネジメント機構 情報基盤支援部門)には、TC カレッジ情報系初級コースから大変お世話になりました。深く感謝申し上げます。

TC カレッジ 情報系 TC コース担当の河本直哉課長(山口大学 総合技術部 情報技術課)には、大変お世話になりました。深く感謝申し上げます。

本支援業務の遂行にあたり、高エネルギー加速器研究機構 計算科学センターをはじめとした皆様、国立情報学研究所 NII-SOCS の関係者皆様、東京科学大学の皆様より多大なるご支援と有益なご助言を賜りました。ここに記して深く感謝申し上げます。

特に高エネルギー加速器研究機構では、様々な方々と多くの時間を共に過ごさせていただけました。その日々の中で業務の知識や経験だけでなく、互いに誠実に向き合い困難の中でも前を向くこと、心のこもった言葉や行動を積みかさねていくこと、そして目的や目標に真摯に向き合うこと、周囲への想像力を欠かさないこと、静かな覚悟と誠実さの積み重ねで得ることができるもの等、あげれば限がないようなものが、数百年と続けるアカデミックに本当に必要なことだと皆様の背中から学ばせていただきました。豊かで美しい生きざまに触れられたことに深く感謝し、その教えや姿勢をこれからの自分の道の中で大切にしていきたいと思います。

良いことも悪いこともご一緒した皆さまのおかげで、私は成長し、支えられ、今の私があります。ご協力いただきました皆さまに心から感謝の意を表します。