Vol.2016-IOT-34 No.9
2016/6/25

国立51高専1法人のスケールメリットII ～情報セキュリティ監査、e-learning・標的型攻撃による情報倫理教育、ソフト・回線の共同調達～

新井 イスマイル[1,2,a)]　入江 智和[3]　千田 栄幸[4]　松野 良信[5]　池田 耕[6]　金山 典世[7]　寺元 貴幸[8]
仲野 巧[9]　野口 健太郎[6]　脇山 俊一郎[10]　加藤 靖[11,6,12]

概要：独法化以降に国立高等専門学校は 1 法人となり、51 国立高専における情報システムの企画・設計・運用に関するノウハウを共有しており、本部で企画・設計したものを調達して各高専に導入することで、運営費交付金が毎年削減される現状をしのぎながらも高度な情報システムの構築に挑んでいる。本稿では国立 51 高専 1 法人のスケールメリットの第 2 報として、(1) 情報セキュリティ監査による情報の取り扱いに関するガバナンス強化、(2) e-learning による情報倫理教育の全国展開、(3) ソフトウェアや回線の共同調達の成果について報告する。

キーワード：システムの運用、利用, システムの保守, セキュリティ/危機管理, 分散システム構築運用技術, システム評価・監査

Merits of scale of 51 national KOSENs as one institution (part II) - Cyber security audits, ethical study utilizing e-learning systems and getting targeted attack training, shared acquisition of softwares and the internet lines.

Arai Ismail[1,2,a)]　Irie Tomokazu[3]　Chida Eikoh[4]　Matsuno Yoshinobu[5]　Ikeda Koh[6]
Kanayama Noriyo[7]　Teramono Takayuki[8]　Nakano Takumi[9]　Noguchi Kentaro[6]
Wakiyama Shunichiro[10]　Kato Yasushi[11,6,12]

Abstract: Since 2004, all the national KOSENs (college of technology) are unified as one institution named National Institute of Technology. Due to the budget cut from the Ministry of Education, Culture, Sports, Science and Technology, all the national KOSENs share knowledge for planning, designing and operating information systems to cope with both cutting costs down and enhancing the quality of their information systems. Also, the headquarters plans and designs institutional information systems for all the national KOSENs. This paper reports three case studies as merits of scale for 51 national KOSENs as one institution as follows. 1) Cyber security audits for strengthening governance. 2) ethical study utilizing e-learning systems and getting targeted attack training. 3) shared acquisition of softwares and the internet lines.

Keywords: Operation and Utilization, Maintenance, Security/risk management, Distributed system implementation and operation technology, System evaluation and audit

1　明石工業高等専門学校
2　奈良先端科学技術大学院大学
3　鹿児島工業高等専門学校
4　一関工業高等専門学校
5　有明工業高等専門学校
6　国立高等専門学校機構本部
7　松江工業高等専門学校
8　津山工業高等専門学校
9　豊田工業高等専門学校
10　仙台高等専門学校

1. はじめに

独立行政法人国立高等専門学校機構法の施行に伴い、平成 16 年 4 月 1 日に全国の国立高等専門学校（以下、国立高専）が独立行政法人国立高等専門学校機構（以下、高専機構）1 法人に集約され、本部の配下で現在 51 の国立高専を運営している。高専は中学卒業後に 5 年間の一貫教育を行う高等教育機関で、一般的に 4〜5 の工学系学科を設置している。各学科の入学定員は 40 名。卒業後 2 年間さらに高等教育を享受できる専攻科の学生が数 10 名おり、さらに教職員 100 名強を合わせると 1 高専当たり 1,000 人規模となる。2 キャンパスを持つ大型高専は倍の構成員となっているため、高専機構は全体で 6 万人規模の法人となる。

高専機構全体の支出は、平成 26 年度が 812 億円 [1] となり、独法化直後である平成 16 年度の 885 億円 [2] と比べて 1 割近く減っている。国立高専の情報基盤整備は第 1 期が平成 7 年度、第 2 期が平成 13 年度、第 3 期が平成 18 年度に更新計画されており、第 1 期・第 2 期については全高専に予算措置がなされたが、第 3 期については予算不足で 6 割程度の高専しか全機器の更新ができない事態に陥った。高等教育機関として高度な教育・研究用情報システムの整備が求められる一方で、金銭コスト面での効率化が求められる。また、独法化後しばらくの間はネットワーク運用・調達が各国立高専に任されていたが、情報システム調達にあたっての仕様策定における人的コストも深刻な問題となるため、高専機構本部からトップダウンに効率よく方針を決めるよう、平成 20 年度に高専機構本部情報基盤委員会に情報基盤整備専門部会と情報セキュリティ専門部会を設置（構成員は本部の所轄教職員ならびに高専が本所属の有志数名）し、高専機構のスケールメリットを活かした効率的なネットワーク運用・調達に挑戦している。

第 1 報 [3] でも述べた通り、平成 24 年度までに下記のスケールメリットを活かした成果を得ている。

- 歴史的 PI アドレスの集約
  国立高専全体で 6B 強の歴史的 PI アドレスを保有しており、課金が開始された初年度は各校で支払ったところ年額が総額 400 万円程度となった。このアドレスの所有者を高専機構に一括集約することで IP 単価を下げて年額約 66 万円にまで削減できた。
- 機器・ソフトの一括調達
  先ほどにも述べた通り情報基盤を全ての国立高専で個別に刷新する予算はなくなったため、ファイアーウォールと認証基盤（LDAP, RADIUS）を機構本部で仕様策定し一括調達した。落札額は公表できないが当初想定していた合計費用よりも 9,000 万円削減できた。また、仕様策定を 1 部会で実施することで各高専の情報担当者の負担を軽減できた。
- ノウハウ・人材の共有
  年に 1 回、全高専の情報担当者を招集して情報担当者研修会を実施し、高専全体の情報基盤整備計画を共有したり、導入した機器やサービスの活用方法をレクチャーしている。全高専情報担当者によるメーリングリストも作成し、日々の情報共有もできるようにしており、その中で経験深い人材を発見しながら本部の部会に招いている。

表 1 情報セキュリティ監査の項目数・確認方法と指摘数

分類	項目数	確認方法			指摘数
		閲覧	ヒアリング	視察	(H27)
1	12	12	7	0	24
2	20	20	19	1	54
3	18	5	18	2	8
4	26	8	26	10	17
5	4	4	4	0	0

その後もスケールメリットを活かした取り組みを続けている。本稿ではノウハウ・人材の共有の続報としてセキュリティ監査や e-learning や標的型攻撃による情報倫理教育の詳細について報告する。また、SINET5 への移行に伴い全高専のネットワーク回線の整備を行ったことや、汎用的なソフトウェアの効率的な調達・導入を実施したためそれらについて報告する。

以降、本稿では、平成 24 年度から平成 27 年度までに得られた成果として、2 にてセキュリティ監査の実施状況、3 にて e-learning と標的型攻撃の結果、4 にてソフトウェアおよびネットワーク回線の共同調達成果について述べる。最後に、5 にて本稿をまとめる。

2. 情報セキュリティ監査

事務のガバナンス強化のために高専機構では毎年 17 高専を対象に本部の監事による監事監査および監査室による内部監査を行っている。国立高専は 51 あるため 3 年で 1 巡する。平成 24 年度からはセキュリティポリシーの運用状況を確認するために本部情報基盤整備委員会にある情報統括専門部会が情報セキュリティ監査を上記監事監査・内部監査と合同で実施している。

1 校の監事監査・内部監査・情報セキュリティ監査は 3 日間（初日午後開始・最終日午前終了のため実質 2 日間）かけて実施しており校内の対応部署がそれぞれの監査で異なるため、全教職員を対象とした監事講話を除き並行して監査を行っている。監事講話は他の高専の事例を引き合いに被監査校の特徴を解説するため、他高専との交流が少ない教職員にとっては自校の立ち位置を知る良い機会となっている。

情報セキュリティ監査のチェック項目は 5 分類あり全て

11 鶴岡工業高等専門学校
12 公益財団法人仙台応用情報学研究振興財団
a) ismail@itc.naist.jp

で 80 項目ある。以下に 5 つの分類を列挙し、各分類の項目数を**表 1** にまとめる。

(1) 組織、危機管理、自己点検及び見直し
主に組織体制や緊急時の対応方法、自己点検体制等

(2) 情報システムの利用遵守（ルール）
主に情報システムの利用方法、PC 等端末の管理方法、個人 PC 持ち込みやネットワークの利用ルール、情報漏洩対策等

(3) 利用者 ID 及びパスワードの運用管理
情報システムの ID・パスワードの運用管理、アクセス制御等

(4) 情報システムの運用管理
情報システム（サーバやスイッチ）室の入退室管理、安全・災害・バックアップ・セキュリティ対策等

(5) 情報システムの調達および外部委託
情報システム調達時のセキュリティ機能の確保等

情報セキュリティ監査員は全項目の確認事項が記載されたチェックシートに従って監査を進める。当日に全ての項目に関する資料を要求して確認する時間はないため、事前にチェックシートに記載されている確認対象の書類を要求して確認できる。事前に確認可能な項目は 15 項目ある。残りの項目については当日に資料（事前提出できないもの）の閲覧・ヒアリング（監査を行う会議室に担当者が来てくれる）・視察（現地に行く必要がある）によって確認する。内訳は表 1 の通りである。視察は最も手間と時間がかかる作業となるが、視察を要する項目数は 13 個のため監査期間内に完了可能となっている。

チェック項目に問題があると指摘事項としてカウントし、監査最終日の報告会にて指摘内容を口頭で説明する。指摘事項は速やかな改善が求められる事項となり次回の監査時に改善されていないと厳しい指導を行う予定だったが、1 巡目の際にそのような説明をしていなかったため、2 巡目が終わった際に監査報告書を被監査校に渡し、3 巡目から本格的に指摘事項の改善状況を確認することになった。なお、1 巡後には監査項目を見直すため、前回の指摘事項に全て対応したとしても次回の監査時に指摘数がゼロになるとは限らない。

分類毎の指摘数を 1 にまとめる。最も指摘数の多かった分類は 2 番目の「情報システムの利用遵守（ルール）」であった。当該分類にて指摘の多かった項目の詳細と考察を以下に列挙する。

- パソコン等の端末の外部持出ルール：パソコン等の端末，記録媒体，情報資産を外部に持ち出す場合のルールを整備し適切に運用されているか。(8 校)
  理想と現実のギャップがあるという問題もあるが、加えて高専機構のポリシー策定の実態にも要因がある。高専機構では本部にてセキュリティポリシーの雛形を作成・各高専に配布して、各高専の実情に合わせたセキュリティポリシーの策定を求めている。しかしながら、各高専に情報システムに精通した教職員が必ずしも配置されているわけではなく、また雛形に記述された内容より厳格度を落とす勇気も持てないため、結果としてほとんどの高専がほぼ雛形のまま、校内の担当委員名称のみを書き換えてセキュリティポリシーを策定している。セキュリティポリシーの雛形を配布する際に情報セキュリティ監査のチェック対象となり得ることを強くアナウンスし運用可能なポリシー策定を求めるか、柔軟性を犠牲にしてセキュリティポリシーの一元化を図る必要がある。一元化は高度な情報工学教育が実現できている高専の教育の特色を損なう可能性があるため前者の対応で済むことを願っている。
- ソフトウェアの購入手続き：高専機構「ソフトウェア管理規則」に基づき，ソフトウェアの購入手続きが適切に行われているか。(管理担当者がソフトウェア管理を適切に実施できるフローになっているか等) (8 校)
  ソフトウェア管理規則に基づくとソフトウェア購入時点でソフトウェア管理簿に登録して的確にライセンス管理する必要がある。ソフトウェアの購入を担当する部署が他の物品等を購入する部署と一緒になっており、ソフトウェアを管理する情報システム担当の部署と異なっていて、連携がうまく取れていないことが主な原因である。両部署の連携を強力にするか、ソフトウェアの購入も情報システム担当の部署に任せる等の対策が求められる。
- ソフトウェアの管理：高専機構「ソフトウェア管理規則」に基づき，ソフトウェアのオリジナルディスク，使用許諾契約書，ライセンス証明書等が適切に管理されているか。(7 校)
  教員が研究費等で購入したソフトウェアのオリジナルディスクや使用許諾書、ライセンス証明書が各教員の手元にある中、それらの所在を情報システム担当者が把握できないことが主な要因である。適切に管理できている学校は最低限、年に 1 回の上記要確認物の校内調査を実施しているため、それに倣うか、上記要確認物を 1 箇所に集めて管理することが求められる。
- パソコン等の修理手続：記録媒体を内蔵する機器（データを消去していないパソコン等）を外部の事業者に修理させる場合，情報が漏えいしない対策（修理を委託する事業者との機密保持契約等）が講じられているか。(6 校)
  情報漏洩対策の厳格化に伴い、求められる措置であるが、教職員の理解が追いついていないのが現状である。マイナンバーが記録されている PC 等の修理を受け付けない事業者が現れている [4] ことから、今後理解が進む可能性は高い。
- 記憶装置の情報消去：廃棄又はリース返却する機器内

表 2　e-learning の受講結果

年度	受講対象	受講完了	未完了校	受講完了率
26	7,084	6,811	12	96.1
27	7,112	7,030	13	98.8

部の記憶装置からすべての情報が消去され，復元が不可能な状態にされているか。(物理的もしくは磁気的破壊) (5 校)

前項目同様、教職員の理解が追いついていない。

その他に指摘数が多かった項目として、分類 (1) 組織、危機管理、自己点検及び見直しにある「見直し：委員会開催時，自己点検結果と自己点検結果に基づく改善策や情報セキュリティに関する状況の変化等をふまえ，情報システムの導入・運用，情報セキュリティ対策，ソフトウェアライセンス管理の評価を行い見直しが行われているか。また，見直しが行われた場合に，その内容が周知されているか。」が 5 校該当した。セキュリティ対策がインシデント・ドリブンになってしまっている現状が垣間見える。校外の事例を積極的に情報収集し先手を打つことが望まれる。

一方で分類 (3)〜(5) に対しては比較的指摘数が少ないことが確認できた。分類 (1), (2) はいわゆる運営側の努力が望まれる項目で、分類 (3)〜(5) は情報システム担当者の現場での努力が望まれる項目である。そういった意味では現場の担当者が情報セキュリティに対して高い意識を持って業務に携わっていると言える。

最後に監査項目が詳細でなかったため指摘に至らなかったものに個人 PC の持ち込みに対するセキュリティ対策がある。BYOD（Bring Your Own Device）については本部にてガイドラインを策定中ということもあり、今後の課題である。

3. e-learning・標的型攻撃による情報倫理教育

e-learning による情報倫理教育を平成 26 年度から開始しており、年に一度、全教職員が情報倫理教育を受ける機会を設けている。また、平成 27 年度には実際に耐性があるかを確認するために無作為に抽出した教職員に対して標的型攻撃を行った。

3.1 e-learning

情報システムは全教職員・学生が利用するものであるため、全員の情報セキュリティに対する意識を高い水準で維持することが肝要である。学生に対しては入学時や事あるごとに教員から教育しているが、教職員に対しては定期的な教育ができていなかった。とはいえ各校あるいは全高専で一斉に講習等を開催することは困難なため、e-learning を採用した。

平成 26 年度は国立情報学研究所（以下、NII）が提供す

図 1　りんりん姫（危険度チェック）

図 2　りんりん姫（ミニクイズ）

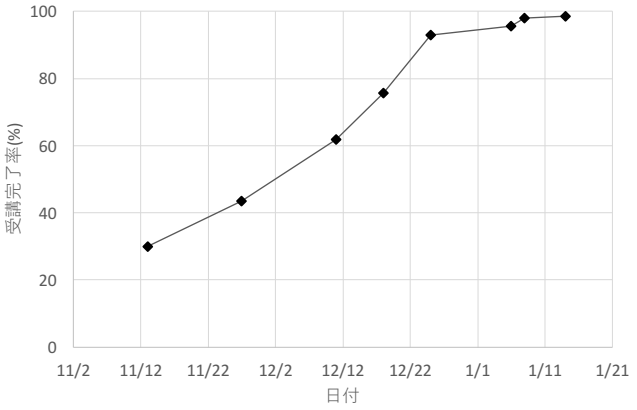


図 3　e-learning による情報倫理教育の受講完了率の推移（H27）

る「りんりん姫」*1 という moodle 上の情報倫理教育教材を利用した。りんりん姫は NII が利用促進している学認 *2（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）に対応しており、高専機構は平成 26 年度に

*1　https://security-learning.nii.ac.jp/
*2　https://www.gakunin.jp/

学認に参加しているため、コンテンツ利用にあたってユーザ登録の作業は不要であった。

りんりん姫の教材は序章から最終章まで 10 章構成となっており、各章にて 5 分〜20 分のムービーを閲覧することで学習を進める。章の最初に危険度チェック（**図 1**）があり、日常の行動のアンケート等に答えると危険がある等の注意が示され、学習前の当事者意識を高める工夫がなされている。その後、数節に渡って講義ムービーを閲覧し、章の最後のミニクイズ（**図 2**）に回答して理解度を確認する。全章受講後に 20 問（所要時間 10 分程度）の総合テストを行い、評価が 80%を超えると合格となる。全てのムービーを閲覧して総合テストが終了するまでの目安の時間は 130 分である。内容をよく理解している場合はムービーをスキップすることを許容し、総合テストに合格している状態が確認できた時点で受講完了とカウントした。

平成 27 年度は難易度を少し上げることと、高専機構で e-learning の教育・研究基盤として Blackboard[*3] を採用したことから、Blackboard 上で動作する情報倫理教育の有償コンテンツ（日本データパシフィック社「教職員のための情報倫理とセキュリティ 2015 年度版」[*4]）を導入し、前年度と同様に全教職員を対象に e-learning による情報倫理教育を実施した。学習方法はりんりん姫と大きく変わらないため詳細は省く。

e-learning の受講状況を**表 2** に示す。平成 26 年度の受講率は 96.1%となった。未受講者 273 名のうち、ある 1 つの高専が 116 名を占め、また他の 2 つの高専で 50 名ずつを占めていたため、それらの高専は校内での周知が不足していた可能性がある。平成 27 年度の受講率は最終的に 98.8%となった。平成 26 年度の実施時期が 7 月〜9 月と夏休み期間中で教員に余裕がある時期に対して、平成 27 年度は 10 月〜12 月と年末に向かう繁忙時期に実施したため、数回に渡って各校の受講状況をアナウンスしていた（**図 3**)。当初設定していた〆切の 12/25 時点で受講率は 90%に達していたものの全教職員が受講完了している高専が 5 高専しかない状況だったため、〆切を 1 ヶ月延長した結果 98.8%に達し、最も受講完了率が低い高専でも 91.0%となった。

3.2 標的型攻撃

前述の e-learning はあくまで座学であり、意識の底上げには効果があると考えられるが、体験に基づかないため、とっさに取るべき行動が取れない可能性がある。そこで、平成 27 年度に 2 度の標的型攻撃による訓練を実施した。使用したサービスはアイエックス・ナレッジ社の「メル訓クラウド」[*5] である。

1 回目は平成 27 年 12 月 22 日に高専機構の教職員から 1,080 名を無作為に抽出（1 高専あたり 20 名）して標的型攻撃メールを送信した。2 回目は平成 28 年 2 月 1 日に 1,900 名（1 高専あたり 35 名）を対象に実施した。メールの内容は**表 3**, **表 4** の通りである。1 回目の攻撃については添付の PDF を開き Web アクセスが求められるポップアップが出た後にそれを許可すると Web アクセスが発生し、そのアクセス状況で開封率が集計できる。2 回目の攻撃はメール内の URL をクリックすることで Web アクセスが発生するので、このアクセス状況で開封率が集計できる。1 回目の訓練メールは校内のメール訓練担当者（1〜2 名配置）から事前に告知して実施し、2 回目の訓練メールは事前告知なし（とはいえ、1 回目の事前告知を受けている）に実施した。1 回目と 2 回目の攻撃対象は重複しておらず 2 回目の訓練が終わるまでに 1 回目の結果は周知しなかった。

表 3 標的型攻撃メールの内容 (1 回目)

From	総務課 < 適当なユーザ ID@ランダムな英数字.jp>
件名	【周知】冬季休業日に関するお知らせ
本文	各位 今年度の冬季休業日における注意事項等を周知いたします。 詳しい内容は添付資料をご覧下さい。
添付	お知らせ.pdf

表 4 標的型攻撃メールの内容 (1 回目)

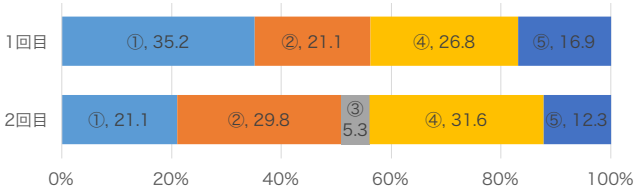
From	総務課 < 適当なユーザ ID@ランダムな英数字.jp>
件名	【重要】「標的型攻撃」最新報告
本文	各位 いつもお世話になっております。 先日「標的型攻撃」に関する報告書が発表されました。 最新レポートの URL をご案内いたしますので、ご覧下さい。 非常に見ごたえがある内容となっております。 (レポート概要) セキュリティ会社が数年に渡って追跡調査している最新情報をレポ ートしています。 レポートでは ・すでに感染しているかもしれない!?あなたの PC の見分け方 ・感染したらどうなるか ・感染を未然に防ぐためには 等をまとめています。 http://www2.....
添付	なし (URL にてサイトに誘導)

訓練結果を**表 5** に示す。全体としては 1 回目と 2 回目の開封率に差はなかった。2 回目は事前通知から間が空くことと、Web アクセスまでの手順が少ないため開封率が増加すると考えたが、平成 28 年 1 月 18 日に文部科学省から不審メールについての注意喚起が発出されており実際に公共機関を狙った不審メールが増加していた背景から差が発生しなかったと考えられる。事務職員は 1 回目よりも 2 回目

[*3] www.blackboard.com
[*4] https://www.datapacific.co.jp/u-assist/FD.html
[*5] http://www.ikic.co.jp/service/security/merukun.html

表 5 標的型攻撃メールの開封率・報告率
（上段：1 回目, 下段：2 回目）

職種	被訓練者数	開封率	全体報告率	開封者報告率
全体	1,080	15.9	19.4	82.6
	1,900	15.3	19.3	30.0
管理職等	260	15.0	16.9	89.7
	270	17.0	9.3	19.6
教員	371	16.7	12.7	56.5
	840	15.8	15.8	27.1
事務職員	287	17.8	29.6	92.2
	632	12.7	29.7	46.3
技術職員	162	12.3	20.4	125.0
	158	19.6	25.3	16.1



①：習慣で開封した
②：不審な点はないと判断して開封した
③：不審に思ったが気にせず開封した
④：不審に思ったが所属している組織（会社・団体など）に関係する内容と考え、開封した
⑤：不審に思ったが自分の業務に直接関係する内容と考え、開封した

図 4 開封者のアンケート結果

の開封率が下がっている。これは事務職員のみ大部屋に机をたくさん配置した職場環境であることから開封後に周りの職員に情報をその場で共有した可能性が高い。技術職員は事務職員ほど大部屋ではないが共同部屋を居室とすることが多いにも関わらず、開封率が上昇している。事後アンケートの中に「訓練かなと思ったので、開けてみた」、「不審に思い放置しておりました。その後、訓練だと思い開封しました。」といったものがあったり、開封者の報告率が 1 回目ではかなり高く 2 回目で極端に下がっていたりすることから、技術職員間で情報共有ができており、訓練であることが 2 回目の時点で分かっていて、興味本位で開封している可能性がある。なお、開封者のアンケートは**図 4** のような結果となった。不審に思わず開封した件数が半数となっており、訓練と分かって開封した件数が一定量ありそうとはいえ多い結果となった。今後の標的型攻撃メールに対する意識向上が課題となった。

不審なメールを受信した場合、インシデント発生時のフロー等に従うと情報セキュリティ担当者に報告することになっているため報告率を評価している。全体報告率（送信数に対する報告率）は 1 回目と 2 回目で管理職を除いて大きな差はなく、開封者の報告率は全体報告率よりも高い傾向にある。アンケートの回答を見ていると開封した理由に添えてフィルタソフトを導入する等の対策をしてほしいという意見が書かれており、組織の一員として一言告げたい意図もあるように見えた。開封者報告率が 2 回目では下がっているが、これは前段落でも述べたような文部科学省の注意喚起や不審メールの増加の背景からよくあることと捉え報告に値しないと判断したか、開封した結果を見て周囲に訓練メールであることを告げられたパターンが考えられる。本来は報告してほしい事象のためインシデント発生時のフローについて周知を図りたい。

4. ソフトウェア・回線の共同調達

以前の報告 [3] では歴史的 PI アドレスの契約集約、ファイアウォール、認証サーバの共同調達を取り上げたが、その後も共同調達可能なものは機構本部で企画・設計・調達を原則としてスケールメリットを活かしている。本稿ではソフトウェアの共同調達（主に Microsoft 製品）と SINET5 移行に合わせたネットワーク回線の整備結果について報告する。

4.1 ソフトウェアの共同調達

全校学生が共用する PC は主に自習、課題、レポート整理に用いられており、いわゆる文房具のソフトウェアとして Microsoft Office が用いられている。Microsoft には包括ライセンス [*6] が用意されており学生や非常勤講師を含む構成員の人数が 100 名以上を超える組織で契約が可能であり、ライセンス数が増えればライセンスの単価が下がるため、高専機構で契約をした方が金銭的コスト・人的コスト（人数に対するライセンスのため PC 台数の把握が不要で、機構本部職員で高専全体の管理が可能）の両面で都合が良い。平成 27 年度末現在の高専機構の Microsoft 製品の契約状況は以下の通りで、契約金額は約 8,000 万円（税込）となっている。ただし、Azure のリソース利用料はこれに含まれない。

- EES
  - 契約人数：9,795 人
    - 常勤教職員：6.329 人
    - 非常勤教員：2,441 人
    - 非常勤職員：1,025 人
  - 対象サービス
    - Office Professional Plus
      無制限に Microsoft Office がインストール可能。
    - Windows Professional Upgrade
      無制限に Microsoft Windows の任意のバージョンをアップグレード可能。アップグレードライセンスのため、インストールのライセンスは別途必要だが過去に購入したライセンスがあるので新規購入数は少ない。
    - Core CAL Suite
      個人端末で Windows Server にアクセスするためのライセンス。学生の BYOD に対応するため

[*6] https://www.microsoft.com/ja-jp/education/license/hokatsu/

図 5 SharePoint を用いた研修会 Web ページ

に本件については全学生（51,570 人）のライセンスを追加契約している。

– 特典

＊ Teacher/Student Advantage[*7]
Office 365 ProPlus が利用可能になる。クラウド・サービスに加えて個人所有の PC に 1 人 5 台まで Office 製品をインストール可能。従来は安価（1 メディア千円程度）に Windows と Office を提供するためのオプションを契約（約 1 億円）、ライセンス管理を各校からボトムアップに行っていたが、これにより金銭的コストと人的コストが削減できた。

＊ DreamSpark Standard/Premium[*8]
Standard は開発に必要となる基本的なツールを各自のアカウントでダウンロード可能になるもので、全構成員に適用できる。
Premium は各高専に 1 学科ずつ提供可能で、開発・検証目的で Windows の各バージョンやフルスペックの Visuial Studio 等もダウンロード可能になる。各高専で利用手続きしている。

- Azure[*9]
各高専でオンプレミス運用しているサーバのハードウェア保守が大変なため、IaaS（Infrastructure as a Servive）として高専機構で Azure を契約した。
- Enterprise Mobility Suite (EMS)[*10]
上記 Azure サーバのセキュリティ対策のために契約した。

Teacher/Student Advantage 特典による Office 365 は高専機構独自の工夫として、高専機構全体で 1 テナントの運用を行なっている。従来より高専機構の教職員は他高専の

*7 https://www.microsoft.com/ja-jp/education/license/advantage/office/
*8 https://www.microsoft.com/ja-jp/education/
*9 https://azure.microsoft.com/ja-jp/
*10 https://www.microsoft.com/ja-jp/server-cloud/products-Enterprise-Mobility-Suite.aspx

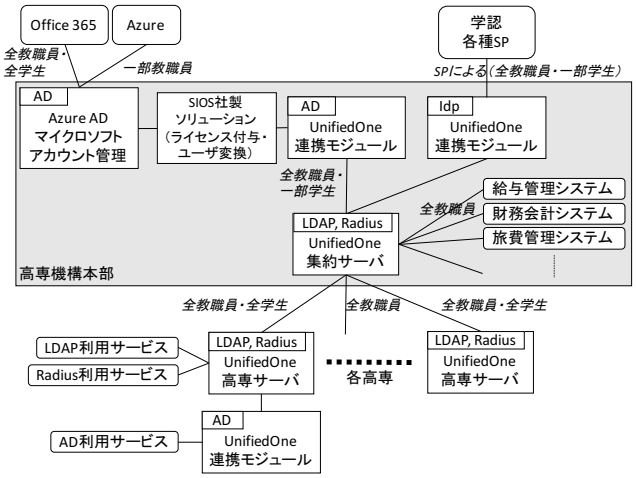


図 6 高専機構の認証サーバと各種サービスの接続

教育・研究活動の取り組みについて活発に情報交換・共同事業をしており、プロジェクト毎にサイボウズ Live[*11] や拠点校のクラウド型ファイルサーバを利用していたが、全教職員がユーザ登録されているクラウドサービスを用意することで、グループを作成するだけで良くなり、またシステムの管理・保守も一元管理できるようになった。

図 5 に平成 27 年 11 月に開催した情報担当者研修会（全高専の情報システム担当者を対象とした毎年開催される研修会）の情報共有サイトの一部を示す。SharePoint を用いて共有する Web ページを作成している。サイトの編集者をテナントのメンバーリストから選択するだけ（いちいち開催メンバーのメールアドレス等を聞く必要もない）で共同編集が可能となる。右側にあるようなドキュメント置場も作成できたり、アンケートのフォームと集計も標準の機能で実現可能である。OneDrive によるファイル共有やメールの配信先としてグループを指定することが可能で、このグループは教職員・学生が任意に作成することができる。平成 28 年 5 月現在、1,367 グループが作成されており、各高専の教職員グループに留まらず、学生の課外活動のグループや講義内の班毎のグループ等が見受けられる。ストレージの使用量も 100GB を超える高専が現れ、積極的な利用が確認された。

Azure は平成 27 年度に約 1,800 万円のプリペイド使用料を含めて実験的に契約し活用を開始した。全高専のニーズを予想することは困難だが、プリペイド契約にすると使用料のディスカウントが効くため、予想使用量よりも多めの金額を設定した。契約開始後に各高専担当者にアナウンスしたところスロースタートで利用が始まったが後半に積極的に使われだし、年度末の 3 月中旬には 200〜300 万円程度の残高（3 月中旬に管理用ポータルが切り替わり平成 27 年度末の残高が確認困難だった）となった。なお、プリペイド残高は期間短縮による払い戻しや次の契約への繰越

*11 https://cybozulive.com/

ができない。平成 28 年 4 月の消費は 160 万円となっており、このペースだと 1,920 万円に到達するため、平成 28 年度は 2,080 万円のプリペイドでスタートしている。平成 28 年 4 月の利用統計を確認したところ、月額利用料が約 10 万円と積極活用している高専は 6 校あり、いずれも従来に校内で運用していたサーバを Azure に移行することでハードウェア保守の人的コストを削減できている。全高専に利用が広まり実験用途の利用が減ってきた頃に定常的な費用を見積もることが可能となるため、運用にあたっての知見の報告はもう 1〜2 年を要する見込みである。

また、Office 365 や Azure には Microsoft アカウント（Microsoft の各種クラウドサービスを利用するための SSO アカウント）が必要である。Microsoft アカウントの管理サイト上で手動登録するか自前の Active Directory サーバと Azure AD を連携するかが選択できるが、管理コストを軽減するため後者を採用している。**図 6** に認証サーバの構成と認証ユーザの種別を示す。従来より運用している高専機構の認証サーバ（富士通製 UnifiedOne）[5] は LDAP, Radius サーバで、登録が必須となるユーザは全教職員となっており学生については任意である。ユーザ情報は全教職員を対象とする各種事務サービスに利用することとバックアップの目的を含めて高専機構本部の集約サーバに集めている。Radius は各高専の機器利用認証に用いる。導入時に AD 連携、Shibboleth Idp 連携モジュールのライセンスも含めており、各高専の需要（既に校内で AD サーバが運用されていたり、学生アカウントを Unified One に含めないポリシーの高専がある）に合わせて有効化している。Unified One の AD ユーザと Azure AD の同期は簡単であるが、Office 365 や Azure といった有償サービスのライセンス付与については自動化機能がないため、サイオステクノロジー社 [*12] 製ソリューションを追加して、Unified One の AD サーバに特定の属性の記述があるユーザに対してライセンスを自動付与するようにした。またユーザ名の作成が各高専に任されており、重複する可能性があるため、Microsoft アカウントのユーザ名には元のユーザ名の末尾に高専名を追加する等のユーザ変換機能も働いている。

4.2 ネットワーク回線の共同調達

学術情報ネットワークが SINET4 から SINET5 に移行するのに伴い、NII によるダークファイバ回線共同調達の情報がアナウンスされた。高専機構のネットワーク回線の調達は従来より各高専に任されていたが、これを機に機構本部からアナウンスをして取りまとめることを試みた。

一部先行して NII 共同調達に乗った高専は 4 高専あるが、その後、全高専周辺の回線状況を確認したところ、1Gbps のダークファイバまたは他の帯域保証回線の調達が成立しないことが判明したため、NII の 1Gbps 回線の共同調達と遜色のない性能とディスカウント額を全高専で成立させるための仕様策定・公募を行った。全高専一括調達にすると地方毎に最適な回線提供業者が異なるため、ブロック（高専を 10 エリアで区切った単位）毎の公募とした。

表 6 ネットワーク回線の共同調達結果

ブロック/例外高専	回線提供業者/調達方法
北海道	北海道総合通信
東北	東北インテリジェント通信
関東信	アルテリア・ネットワークス
北陸	アルテリア・ネットワークス
東海	TOKAI コミュニケーションズ
関西	ケイ・オプティコム
中国	エネルギア・コミュニケーションズ
四国	愛媛 CATV
九州	九州通信ネットワーク
沖縄	オキット
苫小牧、長岡、明石、奈良	NII 共同調達

全高専の調達状況を**表 6** にまとめる。基本的には最寄りの SINET DC に 1Gbps 帯域保証の回線で接続している。本調達によってこれまで 100Mbps の回線だったり、SINET に接続できないためにグローバル IP アドレスが高価でサーバが満足に設置できなかった高専のネットワーク環境が大幅に改善した。なお、平成 28 年 5 月現在で回線切替が完了した高専は 41 高専と機構本部となっており、全高専の切替が完了するのは平成 29 年 11 月の予定である。

5. おわりに

国立 51 高専 1 法人のスケールメリットを活かした情報システムの企画・設計・調達・運用状況の第 2 報として、情報セキュリティ監査、e-learning・標的型攻撃による情報倫理教育、ソフト・回線の共同調達についてまとめた。

本稿には収まらなかったが、この他にもこれまでに、管理職のリスク管理を目的として情報セキュリティトップセミナーを開催したり、実務担当者の人材育成を目的として、LDAP 講習や無線 LAN 技術講習をハンズオン込みで実施したり、セキュリティポリシーの見直しやソーシャルメディア、BYOD 等の早い時代の流れに合わせた情報システムの注意点についてまとめたガイドラインの制定等を行っているため、今後の報告事項としたい。また、平成 30 年頃に各高専の基幹スイッチやネットワーク配線の刷新や学務システムの統一等が計画されているため、限られた予算ではあるがスケールメリットを活かした高品質・低予算の情報システム整備を今後も実現したい。

謝辞 平成 28 年 5 月 27 日に国立高等専門学校機構が「IdP of the Year 2015」[*13] を受賞した。全国 51 校の国立高等専門学校と機構本部が運用する IdP、それら全体のマ

[*12] http://sios.jp/products/authentication/

[*13] https://www.gakunin.jp/jo51y8vh1-538/

ネージメントを実施し、各高専の IdP の運用管理レベルを高いレベルで保ってきたことが主な受賞理由となっている。これらは本報告の情報セキュリティ監査と前報告 [3] の認証サーバ導入の成果である。IdP 導入に際して様々なアドバイスをいただいた国立情報学研究所の皆様、導入後の多くの注文に屈せず対応いただいた富士通株式会社の担当者様、著者に挙げられなかった高専機構本部情報基盤整備委員会の教職員の皆様および日頃の情報システム運用に尽力されている各高専の教職員の皆様に感謝いたします。

参考文献

[1] 独立行政法人国立高等専門学校機構：決算報告書第 11 期事業年度，独立行政法人国立高等専門学校機構（オンライン），入手先 ⟨http://www.kosen-k.go.jp/information/kessanH26.pdf⟩ （参照 2016-5-25）.
[2] 独立行政法人国立高等専門学校機構：平成 16 年度決算報告書，独立行政法人国立高等専門学校機構（オンライン），入手先 ⟨http://www.kosen-k.go.jp/information/kessan.pdf⟩ （参照 2016-5-25）.
[3] 新井イスマイル，福嶋徹，　他：全国立高専 1 法人のスケールメリット I 歴史的 PI アドレスの集約、機器・ソフトの一括調達、ノウハウ・人材の共有，情報処理学会研究報告，Vol. 2013-IOT-23, No. 10, pp. 1–5 (2013).
[4] 富士通株式会社：富士通パーソナルコンピュータ修理規定，富士通株式会社（オンライン），入手先 ⟨https://azby.fmworld.net/support/repair/syurikitei/⟩ （参照 2016-05-27）.
[5] 富士通株式会社：国立高等専門学校機構様、全国 51 校の国立高等専門学校の認証基盤システムを統一，富士通株式会社（オンライン），入手先 ⟨http://pr.fujitsu.com/jp/news/2012/07/17.html⟩ （参照 2016-5-30）.