

総合情報環構想 2022

熊 本 大 学

令和4(2022)年3月24日

目次

1. 総合情報環境構想2022の位置付けと考え方	5
2. 総合情報環境構想2022とは	9
2.1. データ流動化の環	10
2.2. サービス最適化の環	11
2.3. リソース適正化の環	13
2.4. セキュリティ堅牢化の環	14
3. データ流動化の環	16
3.1. 大学データの網羅的な蓄積・管理	16
3.1.1. 大学データの共通化と管理	16
3.1.2. 大学活動情報の収集機構	17
3.1.3. 施設を含めた大学情報の網羅的な収集機構	18
3.1.4. IDの高度化による外部データとの連携	19
3.2. 大学データのオープン化	19
3.2.1. 貴重データのオープン化	19
3.2.2. 知のデータのオープン化	20
3.2.3. 学内オープンデータ管理機構の構築と運用	20
3.3. 大学の偏在知の集約と流通	21

4. サービス最適化の環	23
4.1. 熊本大学ポータル最適化と熊本大学アプリ	24
4.2. 教育学習支援システム群	25
4.3. 研究支援システム群	27
4.4. 運用業務支援システム群	27
4.5. 社会貢献システム群	28
5. リソース適正化の環	30
5.1. 情報ネットワーク基盤の適正化	30
5.1.1. 大学ネットワークの適正化.....	30
5.1.2. 認証基盤の適正化	32
5.2. デジタル基盤推進による業務適正化	33
5.2.1. Web 申請化、ペーパーレス化	33
5.2.2. オンライン授業、会議への対応.....	33
5.2.3. 情報連携活用.....	34
5.2.4. 業務システムのクラウド化.....	34
5.2.5. 問合せ窓口のオンライン化.....	34
5.3. ヒューマンリソースの適正化	34
5.3.1. 人材管理.....	34

5.3.2. 人材育成	35
6. セキュリティ 堅牢化の環	36
6.1. よりセキュアな認証システムの構築	36
6.1.1. 多要素認証の導入	36
6.1.2. FIDO 認証の導入	37
6.1.3. リスクベース認証の導入	37
6.1.4. 認証システムのクラウド化.....	37
6.2. 主体的監査などのセキュリティ人材育成	37
6.2.1. 本学職員による準拠性監査・技術監査の主体化	37
6.2.2. 第三者機関によるセキュリティ評価の強化	38
6.2.3. 情報部門・セキュリティ部門のスキルアップ	39
6.2.4. 有資格者設置基準の設置とシステム部門の配置	39
6.2.5. モバイルアプリによる構成員の情報セキュリティ研修の一層の強化	39
6.3. 説明可能な AI によるサイバー攻撃対策強化と SOC 体制の構築	39
6.3.1. DNS、電子メール、WAF の情報サービスの強化.....	39
6.3.2. XAI 等を利用した SOC 体制の構築.....	40
6.3.3. AI 機械学習によるログ収集と分析と可視化.....	41
6.3.4. SIEM による自動検知・報告の仕組みの構築	41

6.4. インシデント対応の強化	42
6.4.1. IT-BCP の策定.....	42
6.4.2. CSIRT 訓練の強化	42
6.5. ゼロトラスト	42
6.5.1. デジタルキャンパス化.....	42
6.5.2. ゼロトラストネットワークの導入.....	43
7. 中期目標・中期計画との関係等	44
7.1. 中期目標・中期計画との関係.....	44
7.2. 実施スケジュールに関して	44

1. 総合情報環構想 2022 の位置付けと考え方

熊本大学（以下「本学」という。）では、平成 13（2001）年度に、高度情報通信社会の急速な発展に対応して、教育研究活動、地域連携、大学運営、事務サービスの各業務において、情報技術を活用して実現に取り組むべきビジョンとして「総合情報環構想」をまとめた。また、平成 16（2004）年度の国立大学法人化に伴い中期計画がスタートし、その中で、この「総合情報環構想」に基づいた「高度情報化キャンパス」の実現に向けて様々な取り組みを行った。

具体的には、e ラーニングの導入と普及、統合認証や熊本大学ポータルに対応する種々のサービスを連携したオンラインキャンパスの構築、全学情報リテラシー教育の実現、セキュリティポリシーの制定、電子ジャーナルや各種図書サービスの充実といった電子図書館の構築、無線 LAN 基地局の増設、LAN 支線のギガビット化、全学教育用 PC 端末の充実等が実現した。

平成 21（2009）年度には第 1 期中期計画が終了し、平成 22（2010）年度から第 2 期中期計画がスタートする中で、第 2 期中期計画における総合情報環構想である「総合情報環構想 2010」の策定を行い、その実現に向けて様々な取り組みを行った。

具体的には、生涯利用可能な統合 ID である熊本大学 ID の導入と熊本大学ポータルの拡充、全学 e ポートフォリオシステムである学習成果可視化システム ASO の構築、LMS（学習管理システム；Learning Management System）の Blackboard から Moodle への移行、様々な科目のオンライン化、本学学務情報システム SOSEKI の更新、アーカイブシステム及び統合情報データベースシステムの構築、ヒューマンリソースデータベースの構築、学内無線 LAN の整備拡大、統合認証システムの認証方式の熊本大学 ID への対応、統合認証システム「学認」対応による他組織でのサービスの利用拡大、総合情報基盤センターから総合情報統括センターへの改組、公式 Web の構築、各種情報サービス・データベースのシステムレベルでの国際化対応、情報セキュリティ対策への PDCA サイクルの導入と情報セキュリティポリシーの改定整備等を実現した。

平成 27（2015）年度には第 2 期中期計画が終了し、平成 28（2016）年度から第 3 期中期計画がスタートする中で、高度情報通信社会の飛躍的な発展や総合情報環構想のうち現在までに実現した部分、新たに生じた問題等を考慮した見直しを行い、第 3 期中期計画における「高度情報化キャンパス」の進展に

資する次期総合情報環構想である「総合情報環構想2016」の策定を行い、その実現に向けて様々な取り組みを行った。

具体的には、情報サービスの環としてシラバスシステムからLMSの科目のひな形を生成するシステム、学生への周知確認システム、各種学習関連システムから収集・蓄積したデータの学習支援・IR（Institutional Research）への活用、学術リポジトリのグリーン OA（Open Access）としての拡充、様々な学生の状況に応じた使いやすい電子図書館インターフェースの整備等を行った。インフラ基盤の環としては、ネットワーク機器の導入・更新、全学無線 LAN システムの充実、全学 LDAP（Lightweight Directory Access Protocol）情報の充実及び IC カードの活用推進、仮想化及びクラウド化の推進等を行った。IR データベースの環としては、ログサーバの構築と活用、大学評価情報データベースの改修、統合情報データベースの構築、文書管理システムの構築、本学が保管する貴重資料の整備・公開等を行った。セキュリティ基盤の環としては、学内関連規程等の「政府機関等のサイバーセキュリティ対策のための統一基準群」への整合及びクラウド対応改定、全ての部局等への情報セキュリティ監査の実施、学生及び教職員に対する情報セキュリティ研修の実施、模擬サイバー攻撃による情報セキュリティインシデント対応強化訓練、IT・セキュリティ人材の育成等を行った。

20年近くに及ぶ「高度情報化キャンパス」進展への継続的な取り組みは、ここまで述べてきたように、本学内の日常的な研究活動、教育活動、業務活動の効率化、高品質化を着実に達成しつつある。加えて、これらの取り組みは、変災への対応力を高めたことも特筆すべき点である。平成28（2016）年4月の熊本地震の際は、発災後、極めて短期間にて全学的な安否確認システムが構築され、運用を開始できたことはその証左となろう。短期間の稼働を可能とした要因のひとつは、総合情報環構想に基づく着実な情報基盤の整備と継続的な運用であったことは疑う余地はない。この安否確認システムは、その後にも安否確認訓練を定期的実施するなど安定した稼働を実現しており、熊本地震の後も、平成29年7月九州北部豪雨、令和2年7月豪雨等の多くの災害に熊本は見舞われているが、その都度、効率的に安否確認情報を収集している。また、令和2（2020）年初頭より社会を一変させた新型コロナウイルス（COVID-19）の感染拡大に伴う遠隔教育等においても、総合情報環構想に基づき実施してき

た SOSEKI、LMS 等の整備・運用が、円滑な実施の一助となっている。

さて、令和 3（2021）年度現在、様々な要因により社会は大きな変革の時期を迎えている。前述のとおり、COVID-19 の感染拡大に伴い、本学においてもほぼ全科目を遠隔教育に切り替えて実施した。これは非常時対応として行ったものであったが、社会ではそれに留まらないニューノーマル（新しい生活様式）への移行が急速に進んでおり、本学においても平常時の教育改善・業務効率化等への展開、大学全体の DX（Digital Transformation）を進めていく必要がある。これには国も同様の動きを見せており、国は令和 3（2021）年 9 月に「デジタル庁」を設置し、社会全体の DX を進展させようとしている。また、平成 27（2015）年 9 月の国連サミットで採択された SDGs（持続可能な開発目標；Sustainable Development Goals）も急速な広まりを見せ、その達成に向けた貢献が社会的に強く求められており、本学においても令和 3（2021）年 8 月 25 日に熊本大学 SDGs 宣言を公表した。さらに、これらの変革によりデジタルデータで取り扱う重要な情報も増加の一途をたどっており、サイバー攻撃からデータを保護するサイバーセキュリティの重要性も、ますます大きなものとなっている。

また、国や地方公共団体等において、現在、EBPM（エビデンスに基づく政策立案；Evidence-based Policy Making）が広く進められている。大学における教育を含めた活動もその影響を受けており、合理的な根拠に基づいた、信頼性の高い計画策定と実行が必要となっている。さらに、大学構成員の多様化に伴い、画一的ではない、個々の事情に勘案し個別最適化された情報サービスの提供も肝要となってきており、これらを実現させる基盤こそが、学内に偏在、散在し、日々創出・更新される「データ」である。従来もデータ利活用基盤の構築は進めていたが、社会の急速な変容の中、大学の在り方が問われる今日において、その流れの加速と、より大規模、網羅的な構築への発展及び継続的な整備が求められている。

以上の状況を踏まえて、本学の総合情報環構想が常に時代の流れに沿った「高度情報化キャンパス」の進展に資する構想であるために、令和 2（2020）年度から令和 3（2021）年度に掛けて「総合情報環構想 2022（以下「本構想」という。）」の具現化等について検証し、令和 3（2021）年度に ICT 戦略会議において、第 4 期中期計画に資する新しい情報環構想として策定したもので

ある。

なお、本構想における「高度情報化キャンパス」とは、データ駆動型社会の進展を見据え、本学において日々実施されている研究、教育、業務等、全ての活動について、その関連のデータを、従前にはない規模にて網羅的、包括的に収集、蓄積し、それらを適切に分析することで、構成員ひとりひとりに最適化された情報サービスの提供を可能とすることに加え、データをもとにすることで、本学の有するヒト・モノ・設備等の全ての資源を機動的に最適配置し、効果的かつ効率的な活動を可能とする環境の実現を意味する。もちろん、これらのデータや情報サービスの往還がセキュアなものであることを担保する必要があることは言うまでもない。これらを本構想の目指すべき最終ゴールと設定したうえで、その具体的実現の構想を次章以降に記述するものである。

2. 総合情報環構想2022とは

本構想は、平成28（2016）年度の「総合情報環構想2016」に基づき、平成28（2016）年度から6年間の中期計画期間中に整備してきた高度情報化の成果を踏まえて、既に実現し維持と改善が必要な部分、実現していない部分、6年間で社会や本学の情勢変化等によって新たに必要になった部分及びサービスの多様化等によって必要になった部分を整理のうえ、今後の高度情報化キャンパス整備に向けて、効果的かつ効率的な実現を目指すための「構想」である。

本構想は、「1. 総合情報環構想2022の位置付けと考え方」を踏まえ、種々の施策群を「データ流動化」と「サービス最適化」、さらにそれらを円滑かつ安全に実現する「リソース適正化」と「セキュリティ堅牢化」の4つの観点に区分し、「環」という概念にてまとめている。

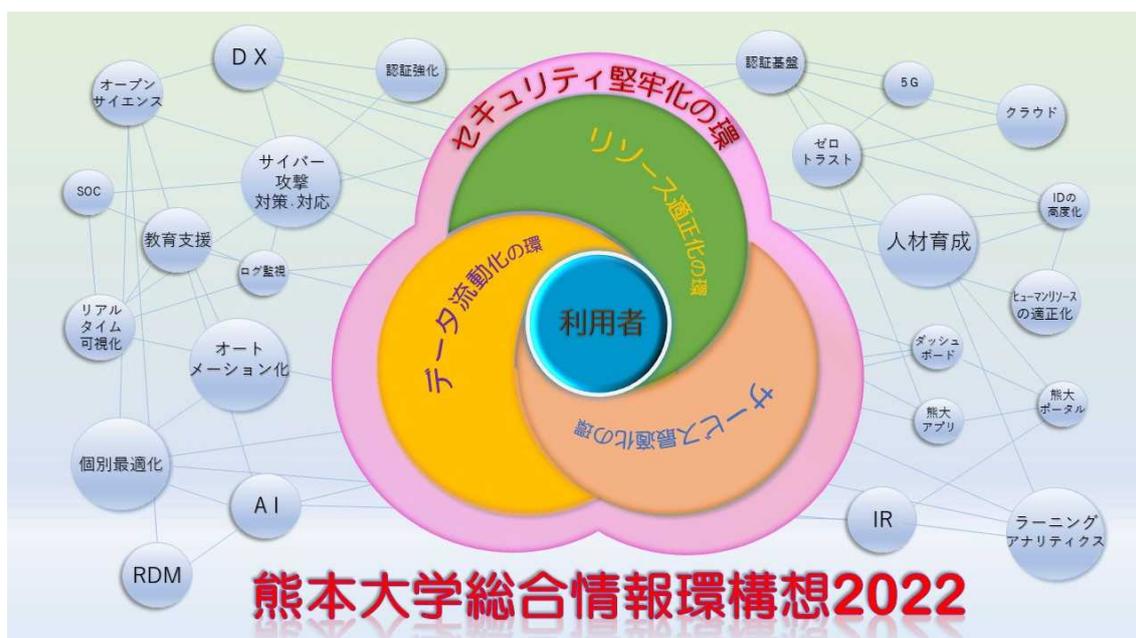


図 2-1：総合情報環構想2022の概略図

図 2-1 は、本構想の概略図である。なお、図 2-1 にあるとおり、本構想では利用者を中心に据えているが、想定される利用者と期待される効果の例は、以下のとおり考えられる。

- ・ 学生とその家族：キャンパス内外で途切れない学生生活支援、個別に最適化されたサービス・サポート
- ・ 職員とその家族：業務遂行の効率化及び効率化支援、柔軟な就労支援

- ・ 地域：課題解決へ貢献する社会連携の進展、効率的な大学リソースの運用

以下は、各「環」の概要である。

2.1. データ流動化の環

データ駆動社会の本格到来を受け、大学においても IR 等、データの入手・分析、管理とその利活用に関する意識が急速に高まっている。また 1.3 万人を超える在籍者数、18 の部局と 26 の組織から構成される本学（令和 3 (2021) 年 5 月 1 日現在）は、知識や情報の偏在化も顕著であり、効果的かつ効率的な教育、研究、業務の遂行のためには、本学の活動の「全て」を記録・蓄積・整理し、共有・流通させる仕組みが必要となる。これら大学の活動と偏在する情報を網羅的かつ緻密に、継続して記録・解析・利用できる環境の構築を目指す。

- ・ 本学に現存、あるいは将来的に生産される全ての記録データを一元管理可能な機構の実現を目指す。既にデジタル化が為されているものの管理はもちろん、紙メディアで管理されているデータ等、デジタル化されていない情報のデジタル化作業も含む。また、今後生産されるデータの仕様・書式等を統一・標準化させることで、データ管理の効率化、高精度化を図る。^{H-1-1}
- ・ 永青文庫等、本学には、人類の宝と呼ぶべき貴重データが多数存在する。これらは本学が安心、安全に管理すると同時に、人類の知の創出に資するべく、教育や研究目的にて、広く一般が利用できる体制を整える必要がある。そのため、貴重データのデジタル化を更に積極的に進め、貴重データの高精細デジタル化を図る。また、作成したデータへのアクセス方式を整備し、容易かつ安全に貴重データを利用可能な環境を整え、多様な形式の情報に対して効率的にアクセス可能な体制を整備する。^{A-3-1, A-3-2, C-1-2}
- ・ IR に加え、ユーザへの気の利いたさりげないサポート等を実現可能とする、本学の活動情報（Kumadai Act.）を大規模、網羅、高解像度、長期間に収集・蓄積可能な機構を整備する。そのために、構成員の活動情報を収集可能なゲートウェイとしての熊本大学アプリを開発・導入し、本学内での構成員の活動を見守ると同時に、活動情報、周辺情報を収集し、蓄積する。ここでは、構成員の位置情報、周囲の音等の環境情報等に加え、構成員が使用した機器やサービス等を対象とする。これらは、Kumadai Act. として、

例えば無線強度マップ、人流マップ等、総体として分析・活用されるのに加え、個人ポートフォリオとして、各構成の潜在的なニーズや特性を明らかにし、さりげないサポートを可能とする。

- 本学が管理する建屋への入館情報、PC 実習室等の利用情報、書籍、各種機器、公用車等の利用情報等、本学施設や設備に関する全ての情報も一元管理し、施設管理、機材管理の効率化と、今後の投資に対する戦略立案に資する環境を構築する。これらの情報を構成員に随時提供することで、教室、演習用 PC 等、本学資産の効率的な運用を可能とする。 E-2-1, H-1-1
- ユーザの利便性向上とデータの流動性を高めるために、本学における統合 ID である熊本大学 ID と外部の各種 ID との連動性を高めることで、学内と学外のシームレスな連携を可能とする。 H-1-1
- 研究データオープン化の潮流を受け、適切な RDM (Research Data Management) の実現を目指し、学内構成員の研究データを構成員の負担なく公開できる仕組みを構築する。さらに外部利用者等が所望の研究データについて容易にアクセス可能な検索機構を構築すると同時に、関連研究データの推薦等、本学の研究データに効果的にアクセスしてもらえるような仕組みを検討する。 A-2-1, A-2-2, A-2-3, A-3-1, D-1-3
- 各学生の受講データ等、大学が有する個人情報是一方で教育改善、業務改善、研究推進のための貴重データでもある。これら秘匿性の高いデータについても匿名化に加え、アクセス権限を明確化することにより、学内オープンデータとして共有・分析を可能とする仕組みを構築する。 B-1-1, G-1-1
- 本学内での様々な業務、教育活動を進めるにあたり、従来もいろいろな工夫が為されてきた。これら偏在している工夫やノウハウ、開発ツール等を全学で共有する仕組みを検討する。業務改善共有システムの構築に加え、共有化活動を推進するための熊大 DX 業務推進室 (熊大デジタル庁) を新設する。新設する組織は共有化推進のみならず、業務改善のための情報技術面でのサポートやツール開発支援、開発請負等も業務とする。 H-1-1

2.2. サービス最適化の環

人、システム、インフラを有機的につなげるために、安心安全な環境のもと AI などを活用しユーザ個別の最適な環境を整え、研究・教育・業務の継続的な効率化を目指す。ポータルにより個別の属性にあわせて表示を制御するなどの

効率化に加えて、利用者ニーズに基づいた探索的なアクセスや個別最適化された情報提供など、これまでにないレベルでの利用者ニーズに適応した情報利用環境を整える。研究・教育・業務において継続的に実施と改善を行う取り組みとなるよう、本学で収集されたデータをもとに、データ駆動型の実施と改善を可能とする利用環境を目指す。

- ・ 本学の多種多様なシステムから収集されたデータの分析結果をもとに、学生・教職員・その関係者が、熊本大学ポータルや熊本大学アプリなどの個別最適化された情報へアクセス可能な環境を提供する。 H-1-1, H-1-2
- ・ 動画編集システムや電子書籍システム、授業ダッシュボードなどにより学習を高度化する。 B-3-2
- ・ 本学の多種多様なシステムで収集されたデータをもとにラーニングアナリティクスや IR などを活用したキャンパスライフ（学習・教育・学生生活）を支援するシステムによりユーザの利便性を向上する。 B-1-1, H-1-1, H-1-2
- ・ 研究・教育・業務に関して分析及び可視化のために、WebAPI（Web Application Programming Interface）技術を活用しラーニングダッシュボード、経営ダッシュボード、大学ダッシュボードなどを構成する。 G-1-1
- ・ 自動化可能な評価や業務をオートメーション化するなどしてユーザの負荷を軽減し、評価やプロセスの効率化を推進する。 G-1-1, H-1-1
- ・ コミュニケーションプラットフォームなどにより、学生・教職員・その関係者が入学前から卒業・修了後までコミュニケーションや連携活動を継続的に実施できる体制を構築する。 B-1-1, H-1-1, H-1-2
- ・ 情報技術を活用した教育活動の効果向上と効率化のために、学内組織で活用される先進的な教育プラットフォームを全学及び地域社会に展開し、高度な教育活動や人材育成活動を支援する。 B-3-2, H-1-2
- ・ 教育・研究・業務など広く情報技術の活用支援を行うセンターを組織し、全学のデジタル化を推進するとともに、デジタル化により現場での問題を解決する方策を改善しながら繰り返し適用し、そのプロセスから新しいモデルやフレームワークに整理して研究成果とし、研究に止まらず研究知見を異なる現場でのサービスに展開する。 G-1-1, H-1-1
- ・ 非常時においても、遠隔授業、遠隔会議等の支援、安否確認サービス等により、教育・研究・業務を止めないサービスを展開し、支援やサービスを

高度化することで、教育・研究・業務を発展的に改善する。 H-1-1, H-1-2

2.3. リソース適正化の環

本学が保有している人と物のリソースを最大限有効活用しながら、社会情勢と限りある財源を熟考の上、ユーザビリティ向上に大きく寄与するソフトウェア展開を念頭とした以下のような基盤整備を図る。

- ・ 基幹ネットワークの高速化、冗長化、多接続に対応する整備を行い、また、トータルコストの削減と合わせて仮想ネットワーク導入の検討を行う。 H-1-1
- ・ 業務システムや認証基盤のクラウド化を推進し、ゼロトラストネットワークや BCP（事業継続計画；Business Continuity Plan）の一つである IT-BCP（情報システム運用継続計画）への対応が可能な基盤整備を行う。 H-1-1
- ・ 業務の Web 申請化やデジタル化を推進し、脱ハンコやペーパーレス化を推進する。 H-1-1
- ・ 高度化するサイバーセキュリティ攻撃に対応すべく、WAF（Web Application Firewall）、UTM（統合脅威管理；Unified Threat Management）、IPS（不正侵入防止システム；Intrusion Prevention System）、IDS（不正侵入検知システム；Intrusion Detection System）などのセキュリティ製品の有用性を検討し、現状のリスク評価に対応した多層防御体制強化を図る。 H-1-1
- ・ ユーザサービスの向上のため Shibboleth 認証による統合認証の導入を行い、さらに、サイバーセキュリティを強化すべく、防御性と利便性のバランスを考量しながら、認証要素を複数組み合わせ、認証強度を高める多要素認証や、パスワードレスで認証が行える FIDO（Fast Identify Online）認証等の導入についても検討を行う。 H-1-1
- ・ オンライン授業などで、BYOD（個人所有機器の持ち込み；Bring Your Own Device）への対応がより求められるため、安心安全安易安価の熊本大学無線 LAN の機能改善と合わせ、5G（キャリア 5G、ローカル 5G）の導入検討を行う。 H-1-2
- ・ セキュリティ対策の強化や地震等の災害時における全学的な把握のために、各施設の入退室管理等のログの一元管理を推進する。 H-1-2
- ・ ヒューマンエラー抑制のための研修体制強化に合わせ、受講状況に応じてシステムが利用できる仕組みを検討する。 H-1-2

- ・ セキュリティ（インシデントハンドリング、デジタルフォレンジクス、監査）や IT（データサイエンティストなど）の人材育成を図る。また、これに関連する特定の資格取得支援を行う。 H-1-2

2.4. セキュリティ堅牢化の環

高度化するサイバーセキュリティ攻撃に対応すべく、防御体制の強化とともに被害を最小限にするための体制も強化する。そのためには「よりセキュアな認証システムの構築」、「主体的監査等のセキュリティ人材育成」、「説明可能な AI によるサイバー攻撃対策強化と SOC（Security Operation Center）体制の構築」、「インシデント対応の強化」、及び「ゼロトラスト」の 5 項目が重要であり、以下の事項を推進する。

- ・ ユーザへの負担をかけない認証強化のため、リスクベース認証による多要素認証、FIDO 認証などの導入を検討し、また、認証システムは、オンプレミスとクラウドで二重化する。 H-1-1
- ・ 準拠性監査及び技術監査業務などを大学職員主体で行えるよう人材育成を図る。 H-1-2
- ・ 第三者機関によるセキュリティ評価を定期的に受ける。 H-1-2
- ・ サイバーセキュリティ対策のため、特徴量などの貢献度が説明可能な AI 等を利用した SOC 体制を構築する。 H-1-2
- ・ インシデント発生時の CSIRT（Computer Security Incident Response Team）での対応手順の見直しを行い、迅速かつ効率的な対応への強化を図る。 H-1-2
- ・ システムの運用者や管理者及びセキュリティ対応者のスキルアップのため、セキュリティ関連講習会参加や資格取得を推進する。 H-1-1, H-1-2
- ・ 学内におけるセキュリティに関する有資格者の設置基準を設け、システムを保有する部署への配置を推進する。 H-1-1, H-1-2
- ・ 情報セキュリティポリシー及び関連運用管理規則に基づき、全教職員、全学生に対して情報セキュリティ教育の一環として行っている情報セキュリティ研修を、モバイルアプリ上で受講できる環境を整備し、受講率向上を図る。 H-1-2
- ・ 病院以外の部局等においても、IT リスクを考慮した IT-BCP の策定を行い、CSIRT と連携して訓練を実施する。 H-1-2

- DNS (Domain Name System)、メール、WAF 等の重要情報サービスシステムに対するサイバー攻撃への対策強化策として、情報サービスシステムや情報機器において常時記録されているログの収集、分析、可視化を行い、SIEM (セキュリティ情報/イベント管理 ; Security Information and Event Management) などにより自動検知、報告の仕組みを構築する。^{H-1-1, H-1-2}
- デジタルキャンパス化に伴い、セキュリティ強化のためゼロトラストネットワークの導入を計画し、効果の見込めるシステムはゼロトラスト型セキュリティ対応を推進する。^{H-1-1, H-1-2}

※ 本章の各文末尾右肩に付されている X-X-X の番号は、関連している第 4 期中期目標・中期計画の計画番号を示している。

3. データ流動化の環

本学では以前より、学内のさまざまな活動における IT の利活用を全国に先駆けて強力で推進してきた。今や大学運営に必須のツールとなっている SOSEKI や LMS、さらに LMS を利用した eラーニングの展開等、その範囲は多岐に渡り、また、他大学等からの評価も高い。このような ICT（情報通信技術；Information and Communication Technology）利活用の結果蓄積されている各種データは、近年の大学運営における喫緊の課題である IR や EBPM、あるいは研究や教育のオープン化を強力で推進するための基盤であり、学内の全てのヒト、モノ、場所、活動情報を集約すると同時に、分析結果を学内の全てに届けることでそれらを多面的に支援する、データ往還の仕組みが重要となる。さらに、1. 3万人を超える在籍者数、18の部局と26の組織から構成される本学（令和3(2021)年5月1日現在）は、知識や情報の偏在化も顕著であり、効果的かつ効率的な教育、研究、業務の遂行のためにも、情報の記録、蓄積、整理と、それらを共有、流通させる仕組みが不可欠である。

以上を踏まえ、本「環」では、本学の活動と偏在する情報を網羅的かつ緻密に、継続して記録・解析・利用できる環境の構築について検討する。

なお、データの流動性を高めるためには、それらのデータの標準化を図ることが重要である。データの標準化に関する議論は、データのドメイン毎に盛んに為されているが、本学で収集・流動させるデータの形式についても、これら世界的な標準規格への準拠を意識することに加え、まだ確定していない分野における標準規格の制定に貢献できるように努める。

本章では以下について論じる。

- ・ 大学データの網羅的な蓄積・管理
- ・ 大学データのオープン化
- ・ 大学の偏在知の集約と流通

3.1. 大学データの網羅的な蓄積・管理

3.1.1. 大学データの共通化と管理

ICT の普及や IR に対する意識の高まりを受けて、本学でも様々な記録がデジタル化され、データとして記録できる体制が整いつつある。しかし、データの仕様や書式が部局によって異なる等、大学発の全てのデータを一元管理可能な

状況にはなっていない。これらを踏まえ、本学に現存、あるいは将来的に生産される全ての記録データを一元管理可能な機構の実現を目指す。既にデジタル化が為されているものの管理はもちろん、紙メディアで管理されているデータ等、デジタル化されていない情報のデジタル化作業も含む。また、今後生産されるデータの仕様・書式等を統一・標準化させることで、データ管理の効率化、高精度化を図る。さらに、各部局、各構成員で個別に管理されていた各種データファイル群を共通のサーバに蓄積できる体制を整える。RPA（Robotics Process Automation）は各種手続きに関する省力化が期待できるが、別の見方をすると、手続きとそれによって生産されるデータの共通化が容易に図れる仕組みとも捉えられる。これらを積極的に推進することにより、省力化というメリットを享受しつつ、大学データの共通化と一元管理を推し進めることができると考えられる。

3.1.2. 大学活動情報の収集機構

従来大学が是としていた画一的な大量消費型のサービスは既に過去のものとなりつつあり、各構成員の状況等に寄り添った個別最適化されたサービスの提供が求められつつある。このような時代背景を踏まえ、IRに加え、ユーザへの気の利いたさりげないサポート等を実現可能とする、本学の活動情報（Kumadai Act.）を大規模、網羅的、高解像度、長期間に収集・蓄積可能な機構を整備する。後述するユビキタス型の情報収集機構に加え、モバイル型の情報収集機構を開発し、導入を進める。すなわち、構成員の活動情報を収集可能なゲートウェイとしての熊本大学アプリ（仮称）を開発・導入し、学内での構成員の活動を見守ると同時に、活動情報、周辺情報を収集し、蓄積する（図3-1）。ここで収集・蓄積する情報は、構成員の位置情報、周囲の音等の環境情報等に加え、構成員が使用した機器やサービス等を対象とする。ここで集約されたデータは、Kumadai Act. データとして、例えば無線強度マップ、人流マップ等、総体として分析・活用されるのに加え、個人ポートフォリオとして、各構成の潜在的なニーズや特性を明らかにし、さりげないサポートを可能とする。

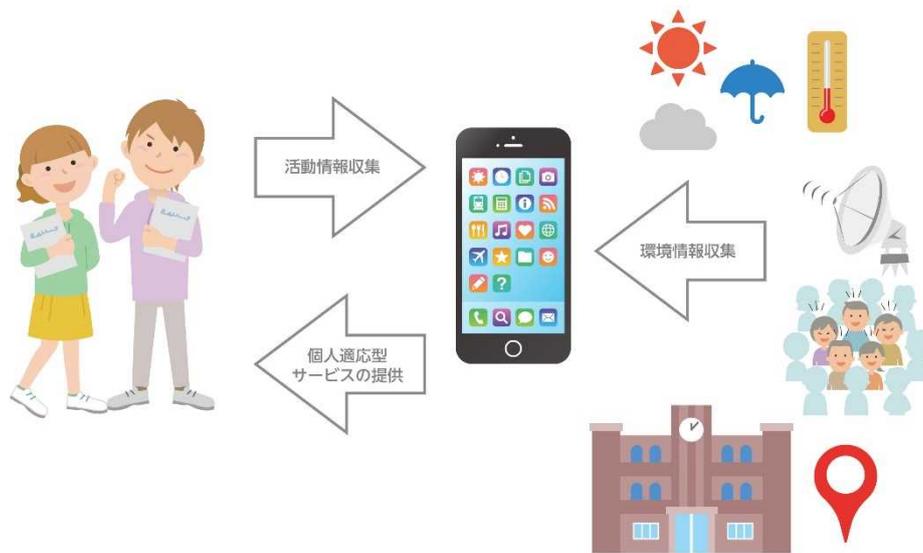


図 3-1：大学活動情報の収集

3.1.3. 施設を含めた大学情報の網羅的な収集機構

上述した各構成員の活動情報に加え、本学が管理する建屋への入館情報、PC実習室等の利用情報、書籍、エアコン等の各種機器、公用車等の利用情報等、本学施設や設備に関する情報も、本学の活動情報として有用である。また、施設・設備の効率的な運用という意味でもその重要性は高い。これらの一部は既にデータ化されているものの、個別のサーバに蓄積されおり、一元管理できているとは言い難い。さらにエアコン等、稼働データそのものが収集されていないものも数多い。このような現状を踏まえ、本学内の全ての施設・設備の情報を一元管理可能な仕組みを構築する。既に個別のサーバに蓄積されているものについては、データの一元化を図る。データ収集のできていないものについては、その設備を IoT（モノのインターネット；Internet of Things）化することで、データ収集可能な環境を整える。これらの情報を利用することで、施設管理、機材管理の効率化と、今後の投資に対する戦略立案に資することを目指す。さらに、これらの情報を構成員に随時提供することで、教室、演習用 PC 等、本学資産の効率的な運用を可能とする。そのための情報提供方式についても検討を行う（図 3-2）。



図 3-2：施設等情報の収集

3.1.4. ID の高度化による外部データとの連携

「社会の中の大学」を考慮した場合、教育、研究等の大学内での活動は、学外の活動と密接に関係しており、学内外の連動が必要となる。さらに、ID 社会において、各個人は複数の ID を管理せざるを得なくなっており、ユーザ活動における煩雑さを助長している。データの流動性・網羅性と、ユーザの利便性の両面の向上を図るべく、シングルサインオンを Shibboleth 認証に一元化することで、本学における統合 ID である熊本大学 ID と外部の各種 ID との連動性を高める環境を構築する。これにより、学内と学外の各種活動、あるいは、その結果生産された活動情報のシームレスな連携を可能とする。

3.2. 大学データのオープン化

3.2.1. 貴重データのオープン化

永青文庫等、本学には、人類の宝と呼ぶべき貴重データが多数存在する。さらに五高記念館、工学部研究資料館等の歴史的建造物、同じく工学部研究資料館に収蔵されている各種機械類の動態展示等も貴重設備、貴重データである。これらは本学が安心、安全に管理すると同時に、人類の知の創出に資するべく、教育や研究目的で広く一般人が利用できる体制を整える必要がある。既に永青文庫等はデジタル化が進んでいるが、これに倣い、各種歴史的記念物等も含めた貴重設備、貴重データのデジタル化を更に積極的に進め、貴重データの高精細デジタル化を図る。本学キャンパス内に散在する建造物のみならず、植生や地質等も貴重なデータとなる可能性を有し、それらの掘り起こしも重要な

検討事項である。さらに、作成したデータへのアクセス方式を整備し、容易かつ安全に貴重データを利用可能な環境を整え、多様な形式の情報に対して効率的にアクセス可能な体制を整備する。

3.2.2. 知のデータのオープン化

教育と研究は、大学が社会の中で担う役割の両輪であり、これらに関するデータのオープン化は、時代の要請であると同時に、知の創出に資するための極めて重要な活動である。これらを背景に、本学における「知」のデータのオープン化を進める。

全ての「知」の活動を下支えする研究データは、適切な RDM の実現を目指し、学内研究者の研究データを構成員の負担なく公開できる仕組みを構築する。さらに外部利用者等が所望の研究データについて容易にアクセス可能な検索機構を構築する。これらに加えて、外部ユーザの要望を適切に把握できるインターフェースを整備することで、要望に応じた関連研究データの推薦等、本学の研究データに効果的にアクセスしてもらえるような仕組みを検討する。ところで、研究データは、それを生み出した研究者の有する基礎・応用技術や、技術展開のショーケースである共同研究事例、さらに、地域や学協会での講演やワークショップ／セミナー活動等のアウトリーチ活動と密接な関係を有する。これらを適切に言語化し、包括的に統合することで、「知の創出」としての研究データと、「知の配信／展開／応用」としての共同研究事例やアウトリーチ活動に関する情報等をシームレスに連携した「知」のオープンデータを構築する。さらに、複数研究者の連携によって創出し得た共同研究事例等もショーケースとして公開することで、創出（研究）と配信（講演等）を一体化した本学の「知」に対する外部ユーザの活用の活性化を図る。

教育は、上述した研究活動に下支えされた、いわば「知の配信」を担うが、その教育内容のみならず、教材作成の工夫や修得度合の確認方法等、講義運営そのものの工夫にも大きな知が内在している。これらの教育データのオープン化についても検討を行う。なお、教育については、個人情報を含む秘匿性を有する部分が存在しており、それらの取り扱いについては、次節に記述する。

3.2.3. 学内オープンデータ管理機構の構築と運用

現場回帰や現場至上主義が叫ばれる中、大学は、それ自身が、特に教育にお

ける最前線の「現場」であり、それ故に、各学生の受講データ等、大学が有する個人情報、教育改善、業務改善、研究推進のための貴重データでもある。総合情報統括センターの有する情報環境の管理情報や、熊本大学病院の有する診察情報等も同じく貴重データである。これら秘匿性の高いデータについても、有効活用する仕組みの構築が、「知の創出」において極めて重要である。匿名化に加え、アクセス権限の明確化等、各種の措置を検討することで、学内オープンデータとして共有・分析を可能とする仕組みを構築する。

3.3. 大学の偏在知の集約と流通

大学業務の多忙化、煩雑化に伴って、本学内での様々な業務、教育活動を効率的に進めるために、各構成員は従来からいろいろな工夫を行ってきた。これらは、業務に関するメモであったり、ノウハウであったり、あるいは処理を円滑に進めるための自作ツール等である。これらは各構成員が独自に製作・管理している場合が多く、またその継承も困難である。特に定期的に担当部門を変更する事務部にはこの傾向が顕著である。各構成員が行った工夫や各種ツール自体が、構成員が培った貴重なデータであり、その継承を円滑に実施することで大学業務の効率化が期待できる。そこで、これら各部門に偏在している工夫やノウハウ、開発・管理ツール等を全学で共有する仕組みを検討する。業務改善共有システムの構築に加え、共有化活動を推進するための熊大 DX 業務推進室（熊大デジタル庁）を新設する（図 3-3）。新設する組織は共有化推進のみならず、業務改善のための情報技術面でのサポート、例えば、「独自開発か開発委託か」の判断等、開発方針の判断に係る支援や、ツール開発支援、開発請負等も行うことで、各構成員が専門性の高い高度な業務に専心できる環境を整える。また、共有化された工夫、ツール等を円滑に再利用可能な工夫として、高度な検索機構、ツール利用のショーケース等も整備する。



図 3-3 : 偏在知の集約と流通

4. サービス最適化の環

前構想では、熊本大学 ID を中核とし、熊本大学統合認証（シングルサインオン）によって熊本大学ポータルを中心とした利用者のニーズにあったサービス提供のさらなる推進が目指された。その結果、シラバスシステムから LMS の科目のひな形を生成するシステム及び学生への周知確認システム並びに学術リポジトリのグリーン OA としての拡充、様々な学生の状況に応じた使いやすい電子図書館インターフェースの整備、全学グループウェアシステム導入、教職員を対象とした文書管理システム等、熊本大学 ID によるサービスが拡充された。平成 28(2016)年の熊本地震では全学的な安否確認システムが構築され、その後定期的に安否確認の訓練が行われている。令和 2(2020)年の全世界的な COVID-19 の感染拡大により我々の生活が一変し、教育を止めないために遠隔教育が必要となったとき、それまで整備された SOSEKI や LMS により少ない混乱で運用された。多種多様な利害関係者がオンラインからアクセスしてサービスを利用する環境は整いつつある一方で、研究・教育・業務の効率化は進んでおらず、これまでのサービスの評価を行いつつ改善して進化する必要がある。そこで、本学で収集されたデータをもとに、データ駆動型のサービス提供と改善のサイクルを回し、これまでにないレベルでの利用者ニーズに適応した情報利用環境を目指す（図 4-1）。

以上を踏まえ、本学のサービスを最適化する環境の構築について次の項目に分けて述べる。

- ・ 熊本大学ポータルの最適化と熊本大学アプリ
- ・ 教育学習支援システム群
- ・ 研究支援システム群
- ・ 運用業務支援システム群
- ・ 社会貢献システム群

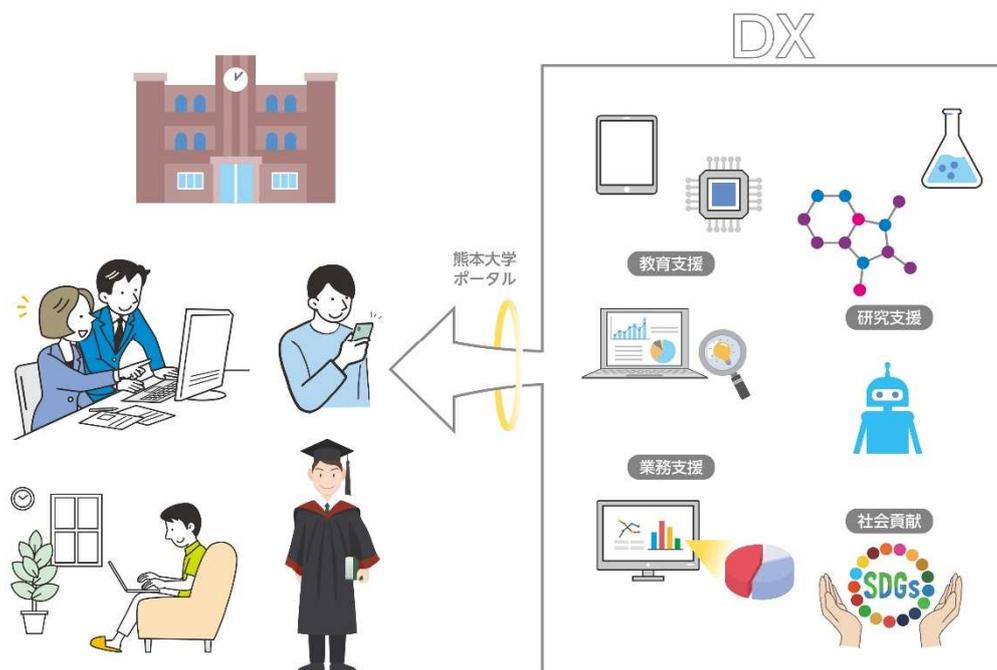


図 4-1：総合情報環境構想 2022 「サービス最適化の環」

4.1. 熊本大学ポータルの最適化と熊本大学アプリ

熊本大学ポータルはすべてのサービスの入り口であるが、リストされているサービス群の中には、毎日の頻度で利用するサービスから年に数回程度利用するサービス、あるいは数年に1回に利用するサービスなど、ユーザやユーザの属性によって使用頻度やタイミングが異なる。ここでの属性とは、所属学部学科に限らず、授業時間などの時間帯、必修の授業の違いや進級判定、卒業判定など入学してからの時期、学期始めや学期末などの時期、各種締切、専門領域、学生や教員、事務職員、技術職員などの職務・役職の違いなどを扱い、最適な提示を目指す（表 4-1）。

利用頻度	サービス
毎日	時間割 研究進捗 業務システム
年に数回	履修登録 研究費公募情報 研究業績登録 年末調整 月次業務システム

表 4-1：利用頻度とサービス

そこで、職務や役職等のユーザの属性に合わせて必要なサービスのみを表示する機能、利用頻度に合わせて優先的に表示する機能を持つ個人ポータルを構成し、以下の支援を行う。

- ・ 入学年、時間帯などの属性情報をもとにサービスを推薦する機能や時間割機能、スケジュール機能、学習進捗表示機能などを持つ個人ポータルを構成することで学習を支援する。
- ・ 公募締切や研究テーマなどの属性情報をもとに推薦する機能やスケジュール機能、研究進捗表示機能などを持つ個人ポータルを構成することで研究を支援する。
- ・ 特定の時期に利用される年末調整のサービスなど、時期などの属性情報をもとにサービスを推薦する機能、スケジュール機能などを持つ個人ポータルを構成することで業務を支援する。

さらに、熊本大学ポータルとおおよそ同等の機能を熊本大学アプリとして利用できるように提供する。熊本大学アプリはプッシュ通知機能を備えることで利用者にとって必要な情報に気付くことができ、情報へのアクセスを容易にする。

4.2. 教育学習支援システム群

- ・ Web 会議システムを利用した同期オンラインの授業が行われる中、利用者のネットワーク環境によっては Web 会議システムの通信断などにより授業の

映像や音声を聞き逃すこともあるため、Web会議システムによる映像と音声を動画編集システムにより自動的に収録し、学習者が後日いつでも授業を確認できるように支援する。

- テキストや資料などが電子書籍システムで提供されることで、学習者は学習のポイントなどを手軽に記録することができる。教授者は同期型授業を進行しながら、学習者のページの閲覧状況などが示される授業ダッシュボードを使い学習過程を把握し、学習者にあつたフィードバックや指導を行うことができる。
- 学習者の動画視聴、電子書籍の利用、LMS の利用、会議システムの利用などの記録をもとに、課題や学習の状況などを統一的に表示するラーニングダッシュボードを構成する。学習者がラーニングダッシュボードで自分の学習状況を把握し、自律して学習するスキル向上を支援する。ラーニングダッシュボードにより、学習の振り返り、課題締切の管理、学習スケジュールの管理とリマインド、学習者の履修登録から卒業や就職までをナビゲートする。ラーニングダッシュボードでは、現在の授業と過去の授業との関係を表示することで、いつでも過去授業の内容を参照することができる。また、複数の学習者の学習状況の比較や個人の学習状況の比較を可視化することにより活動の変化などを表示することで、ケアの必要な学生を予測し、学生相談室の活動を支援する。
- 学生は日に授業や事務連絡、イベント情報など多くのメールを受信したり、掲示板の通知を確認したり、通知情報にあふれている。メールダイジェストを構成し、所属情報に合わせて通知するサービスにより、通知情報に埋もれないように支援する。
- コミュニケーションプラットフォームにより、学生の入学前から卒業・修了までの学習活動や連携活動でのコミュニケーションを活性化させる。入学前には、入学の相談や入試情報などの提供、在学中は、学生生活、学習、研究、部活動、就職活動などの相談、卒業・修了後には、同窓会、後援会などの本学関係者との交流等を支援する。
- 非常時においても学習方法の変化や学習場所の変化に耐えうる学習者及び教職員の継続的な育成を行い、その時の状況に合わせて人が学習及び教育活動を継続できるシステムを提供できる組織構築を目指す。

- ・ データサイエンスの概念を理解し、ビジネスに活用できる人材を育成するために、従来の情報リテラシー科目にデータサイエンス教育を加え、新しい情報リテラシー科目を構成する。また、これまでのセキュリティ教育をより発展的に構造化し、学習者に合わせて適度なセキュリティの概念を理解できる仕組みを展開する。

4.3. 研究支援システム群

- ・ 教職員の研究業績、活動実績を自動的に収集し、業績評価に必要な項目を自動的に構成し、評価者のみが閲覧し、評価内容を速やかに登録できるシステムにより評価プロセスを効率化する。また、研究業績や研究データをもとに作成されるショーケースのサンプルからシーズ集を構成し、産業界のニーズとのマッチングを支援する。
- ・ コミュニケーションプラットフォームにより、研究室レベルから学外研究者との共同研究レベルまで、広範囲でコミュニケーションや連携活動を支援する。
- ・ 教育・研究・業務など広く情報技術の活用支援を行うセンター（以下「新センター」という。）を組織し、新センターは全学のデジタル化推進を通して、研究上、教育上、業務上の成果をデザイン研究手法により精緻化し、研究成果として発信する。

4.4. 運用業務支援システム群

- ・ 教員、職員の教育業績、研究業績、活動実績や学生の学習実績や活動実績などの指標を経営ダッシュボードで可視化する。経営ダッシュボードをもとに教職員や組織のパフォーマンスをエビデンスとして教職員の人事など経営に関わる意思決定を支援する。業績評価に必要な項目を自動的に構成し、評価者のみが閲覧し、評価内容を速やかに登録できるシステムにより評価やプロセスを効率化する。
- ・ 集められた建物情報（場所、許容人数、設備）と人の入室情報などをもとに人の流れや移動の最適化を図り、学生や教職員の移動の効率化、活動の効率化を目指す。
- ・ チャットボットなどの自動応答システムにより、学生対応窓口や学内手続きなどをナビゲートし、人による対応を削減し、自動対応を増やすことで、

- 業務支援を推進する。物品購入や旅費などの定型な手続き、教職員の業務上の定型な問い合わせなどチャットボットや RPA を利用して効率化を図る。
- ・ ネットワークを利用する必要がある授業、研究、業務など、多種多様な利用者の環境を整備するために、ネットワーク環境を測定できるシステムを整備し、利用者から利用環境のフィードバックを収集し、ネットワーク品質評価を行い、利用環境改善を推進する。
 - ・ 集められた在学生や卒業生の情報をもとに出前授業や大学案内イベント、大学訪問などでニーズのある情報を可視化した大学ダッシュボードを使い、大学のプロモーションを推進する。コミュニケーションツールを経由して大学の強みや入試情報を通知することで興味関心を引き寄せ、定型な問い合わせはチャットボットで即時対応し、複雑な問い合わせは教職員へナビゲートすることで、入学前の活動を支援する。
 - ・ 教員向けに、学習者の動画視聴、電子書籍の利用、LMS の利用、会議システムの利用などの記録及び、課題提出情報や進捗情報などを統一的に表示する先進的な教育プラットフォームを構成する。先進的な教育プラットフォームでは、教職員は単位習得状況に限らず学習者ひとりひとりが各授業回を終えたかどうかを確認でき、自分で情報を集める必要なしに学習者の状況を週単位で確認することができるため、素早く最適な学習指導が可能となる。
 - ・ 全学のデジタル化推進を通して、研究上、教育上、業務上の成果をデザイン研究手法により精緻化された研究成果は、学内での他部署や部門、専攻などのそれぞれの領域において新センターが最適化して展開することで、研究、教育、業務の効率化が推進される。
 - ・ 本学職員もデータサイエンスの概念を理解し、データ駆動型で効率よく業務を遂行できるスキルが必要となる。忙しい業務の合間に効率的にデータマネジメントやデータサイエンスの概念を学習できるよう整備する。
 - ・ BCP に沿って、非常時に業務や教育を止めないために、クラウドを利用したサービスとリモートワークシステムとを融合したシステム構築に取り組む。

4.5. 社会貢献システム群

- ・ 公開講座や科目等履修など、社会に向けて公開される科目の受講情報や受

講者情報を分析し、個別に他の科目や大学でのイベント等をリコメンデーションし、社会が必要な情報を効率よく入手できる仕組みを目指す。また、科目の受講状況をラーニングアナリティクスの知見を活用して分析し、最適な学習支援を目指すことで利用者の満足度向上を目指す。

- ・ ラーニングダッシュボードの知見を活用して、社会人学習者が学習履歴や後続授業のレコメンデーション、最適な学習方法などを利用して学び直しや継続した学習を推進する。
- ・ コミュニケーションツールを經由して大学の強みや社会にとってニーズのある研究や教育の情報を提供し、社会連携活動を支援する。
- ・ 先進的な教育プラットフォームの機能を援用して地域の人材育成に貢献する。
- ・ 全学のデジタル化推進を通して、研究上、教育上、業務上の成果をデザイン研究手法により精緻化された研究成果は、産学官に向けて発信され、新センターが様々な領域において最適化する支援を担う。
- ・ 全学情報リテラシー教育、全学データサイエンス教育、全学セキュリティ教育で利用される教材は、すべての学部生を対象としており、専門領域横断的に利用可能な教材と考えられ、個別に最適な内容を学習できるようにマイクロラーニングの形式で OER (Open Education Resource)として公開を目指す。

5. リソース適正化の環

本構想を実現するための必須条件として、インフラ基盤である「モノ」や本学構成員である教職員・学生の「ヒト」を最大限有効活用しながら、社会情勢と限りある財源を熟考の上、ユーザビリティ向上に大きく寄与するソフトウェア展開を念頭とした基盤整備を行う必要がある。また、今後 DX が進むことは必然であることから、インフラ基盤の強化・効率化だけでなくヒューマンリソースマネジメントを欠くことはできない。今後は、新しいシステムの導入だけでなく、既存システムの増強並びに既存システムの大規模更新にも重点を置く必要があり、今までと大きく異なる概念の構想が進んでいくことが想定されるため、その利便性・重要性・緊急性に十分配慮したうえで、予算の確保並びに配分を常に考慮して実施計画を立てることになる。ここでは、本構想の実現に必要なとなるリソースの適正化を念頭に記述する。



図 5-1：総合情報環境構想 2022 「リソース適正化の環」

5.1. 情報ネットワーク基盤の適正化

5.1.1. 大学ネットワークの適正化

5.1.1.1. 大学ネットワークの拡充

総合情報環境構想 2016 に基づき計画的に更新を行ってきた基幹に関わるネットワーク機器については、令和 3(2021) 年度に更新が完了することとなった

が、今後、ネットワーク機器の耐用年数とますます進むデジタル化などによる多接続化・大容量化・安定化を考慮した通信に重点を置く必要がある。また、本学の接続ノードである学術情報ネットワークについても、令和4(2022)年度から SINET6 が運用開始され、ネットワークの高速化やサービス拡充などが行われる。本学においてもその恩恵を十分に活用できるように、次期の基盤ネットワークの構成変更も含めた更新計画を策定する必要がある。さらに、拡充されてきた大学基盤ネットワークの性能を十分利用できるように支線等の部分についても点検を行う。その一環として、ネットワーク管理の負担と運用コスト軽減のために仮想ネットワークの導入を検討する。

5.1.1.2. 全学無線 LAN アクセスポイントの拡充

ハイブリッド授業が推進されると、学生が学内でオンライン授業を受講することが増加し、また教職員においてもテレワーク化が進み、学内のあらゆるところからのオンライン会議への接続が増加することが考えられる。その際、学生や教職員が、個人所有のノート PC やタブレット等のモバイル端末を学内に持ち込んで学習したり業務を行ったりする、BYOD を行う場面が今後さらに増えていくことが予想される。

そのため、現在も全学無線 LAN を構築済みであるが、私物端末の学内利用に必須のネットワーク環境として、今後はさらなる整備が必要となる。また、PC の実習を行う場合、現在は本学が配備した実習用 PC でしか実習できないが、PC 環境をネットワークに接続するだけで、端末の種類に関係なく同様の環境が得られるような仮想環境の構築を進める。ただし、これには仮想環境構築の費用だけでなく、各端末で仮想環境を利用するためのライセンス費用が発生することを考慮に入れて実現性を検討する。

5.1.1.3. 5G 導入による利用拡充

「5.1.1.2 全学無線 LAN アクセスポイントの拡充」にも記載したことが充実してくると、大学の建物内だけでなく、屋外や福利厚生施設、大学生協など、全学無線 LAN アクセスポイントの設置が困難で、全学無線 LAN に接続しにくい場所での大学ネットワークの利用も考えられる。また、災害や遠隔医療、警備、イベントなどにも対応できるように、無線 LAN の多接続化、大容量化、低遅延化、高速化が必要とされてくるため、それらに対応するために、5G（第

5世代移動通信システム)の導入が必要である。現時点では、5Gにもローカル5G、パブリック5G、プライベート5Gなど周波数帯等によるメリット・デメリットがあるため、大学でのサービスニーズに応じた周波数帯の導入を検討する必要がある。

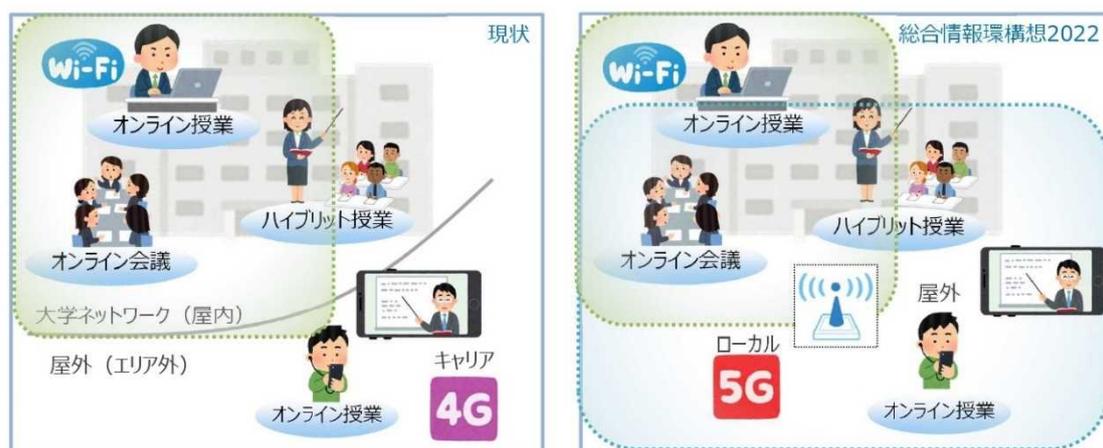


図 5-2 : 大学ネットワークの適正化

5.1.2. 認証基盤の適正化

5.1.2.1. 認証基盤の拡充

本学は、平成17(2005)年からオープンソースのシングルサインオンであるCAS (Central Authentication Service) 認証により学内の統合認証対応システムを利用しているが、今後、学修環境充実や外部コンテンツ、他機関コンテンツの利用を目的として、シングルサインオンを Shibboleth 認証に一元化する。また、登録情報の拡充を行っている学内 LDAP に搭載している情報にも効率的に連携を行い、それに合わせた運用フローも確立していく必要がある。さらに、IT-BCP の観点から 5G 回線の導入を検討の上、認証システムの冗長化、クラウド化を行い、デジタルキャンパス化を進める。これらの技術の導入が推進されれば、学外・学内の区別無く本学の情報資産へのセキュアアクセスを可能とするゼロトラストネットワークの導入を視野に入れる。

5.1.2.2. セキュリティ認証の強化

学内システムのセキュリティ認証は、一部を除いて ID とパスワードによる一要素認証に頼っているが、攻撃側におけるコンピュータの性能向上や並列処理の導入などにより危殆化している。また、ユーザがいろいろなものと同じパ

スワードを使い回すことにより、情報漏洩等によるパスワードリスト攻撃の危険性が高まることとなり、例えば公私ともに同じパスワードを利用していた場合、私的利用のパスワード漏洩により、学内のシステムへの影響を受ける可能性がある。そのため、デジタルキャンパス化推進を行ううえで、認証基盤の拡充は、より一層のセキュリティ認証強化が求められるが、安全性を重視するとユーザの利便性が損なわれてしまうため、FIDO 認証や特定の場所からのアクセス時のみ多要素認証を行うリスクベース認証の導入などの検討が必要である。顔認証や学生証・身分証明書と組み合わせた多要素認証、もしくは SMS (Short Message Service) を利用したワンタイムパスワードなどの多要素認証の実現性について調査導入を検討する。

5.1.2.3. 多層防御体制の強化

サイバーセキュリティ攻撃は近年高度化してきており、外部からの攻撃防御以外に内部ネットワークの監視強化や、BYOD 普及による私用端末などからの攻撃防御など、さまざまなパターンを想定する必要がある。そのため WAF、UTM、IPS、IDS などのセキュリティ製品の有用性や費用対効果を検討・検証し、多層防御体制の強化のために導入計画を推進する。

5.2. デジタル基盤推進による業務適正化

5.2.1. Web 申請化、ペーパーレス化

令和 3(2021)年 9 月 1 日から「デジタル庁」が発足し、デジタル政策の企画立案により、国や地方公共団体、準公共部門などの情報システムを統括・監理し、重要なシステムを整備していく方針が出されており、それに合わせ、政府推進の押印廃止、ペーパーレス化も推進されている。本学においても、それに合わせ、本学規則における押印による申請様式のうち、法律に基づき様式が定められているものや電子化することで業務が複雑・非効率となるものなどを除いた様式について、Web 申請化を実施し、ユーザの利便性を向上させる。また、この Web 申請化を踏まえ、RPA を活用した文書処理の省力化・自動化を推進する。

5.2.2. オンライン授業、会議への対応

昨今のコロナ禍を起因に、オンライン授業やオンライン会議などが普及してきており、それによる時間・移動費用などの削減や授業・会議内容の動画によ

る記録などメリットが享受できている一方、通信状態が不安定なことによるトラブル、機器の準備・後片付けが必要になる、コミュニケーションが不足する、ユーザメンテナンスの対応が必要になるなどのデメリットもあるため、場所、時間帯、接続数に影響を受けない安定した通信の確保や、オンライン環境の準備された会議室・教室の設置、ユーザメンテナンスのシングルサインオン連携、オンライン授業の専用サーバへの自動登録及び蓄積を行い、高圧縮化データによる学生の視聴ストレス低減や教育の高度化へ繋げる。また、専属ヘルプデスク設置などを進めていく必要がある。

5.2.3. 情報連携活用

デジタルキャンパスが進んだ場合、IT 機器への依存度が高くなるため、自然災害やサイバー攻撃に対応した IT-BCP の必要性が高くなる。その一環として各システムの集約された情報をもとに安否の確認、出張・研修・実習・留学・状況に応じたリアルタイムに近い状況把握を行えるようにし、また、学内においても、各施設の入退室管理等のログの一元管理により、ログを集約し分析・管理することで、リアルタイムでの状況把握のほか学内セキュリティの強化にも利用できる環境を構築する。

5.2.4. 業務システムのクラウド化

学内の業務システムのクラウド化を、長期的稼働を視野に入れ、リスク評価と IT-BCP の必要性などを考慮して優先度を決定し、上位からクラウド化を推進する。そのため、セキュリティとランニングコストを調整し、プライベートクラウド型、パブリッククラウド型、もしくは混合型の環境整備計画を検討する。

5.2.5. 問合せ窓口のオンライン化

利用者サービスの向上と、学生支援窓口で対応を行う職員の負担軽減を目的として、時間や場所を問わない対応を可能とするチャットボットを、金銭の授受や心身に関する要配慮の相談以外の窓口について導入する。

5.3. ヒューマンリソースの適正化

5.3.1. 人材管理

大学経営戦略の一環として教職員の人材の資質別の状況把握と必要な人的資

源の需要を可視化する。学内全体での長期戦略の策定を行い、その戦略に必要な人材を具現化のうえ、適材適所による業務遂行とその実績評価が行えるようにし、最終的には人材の保有スキルを最大限に活用できるような環境構築の設計を行う。

5.3.2. 人材育成

デジタル化を推進するうえでの必要条件として、情報技術の利用について学内における利用環境格差を無くし、それを利用するユーザのITリテラシーの向上を図ることが鍵となる。そのためにも、ヒューマンエラー抑制のための定期的な安全環境関係の研修実施が必須となるため、構成員全員に対して、誰でもどこでもいつでも受講可能な研修環境を整備し、受講状況の管理を行えるようにする。さらに、受講状況に応じて学内システムを利用可能とする仕組みを検討する。また、エンドユーザの基本的ITリテラシー以外に、デジタル化が進めば進むほど、IT管理側の人材の需要が伸びると予測され、システムの機能・仕組みに関する知識や、その運用により得たデータを有効活用するためのプロジェクト、マネジメント、データサイエンス、セキュリティなどのスキルを持った人材育成が必要であり、そのスキル保有のための支援と、その管理ができる体制整備を行う。

6. セキュリティ堅牢化の環

先鋭化するサイバーセキュリティ攻撃に対応すべく、防御体制を強化するとともに被害の最小限化のための体制も強化する必要がある。例えば、多様な認証情報システムに対する CF (Credential Stuffing) 攻撃、AI を悪用した高度な DDoS (分散型サービス妨害 ; Distributed Denial of Service) 攻撃、本学の教職員などに扮した電話攻撃 (ソーシャルエンジニアリング) 及びテレワークに対する攻撃などが増加しつつある。

本学では、教職員や学生全員が本学の提供する情報サービスをスムーズに利用できる環境を構築して維持して行かなければならないが、サイバーセキュリティの一層強化は本学における最重要事項の一つと言える。

サイバーセキュリティを強化するためには、図 6-1 に示すとおり「よりセキュアな認証システムの構築」、「主体的監査等のセキュリティ人材育成」、「説明可能な AI によるサイバー攻撃対策強化と SOC 体制の構築」、「インシデント対応の強化」、及び「ゼロトラスト」の5つが重要事項となる。



図 6-1 : 総合情報環構想 2022 「セキュリティ堅牢化の環」

6.1. よりセキュアな認証システムの構築

6.1.1. 多要素認証の導入

本学のネットワークと情報サービスシステムは国の重要なインフラ機関の一

部であるため、本学の情報セキュリティポリシーも常に最新版の政府統一基準群との整合を進めているが、政府機関等の対策基準策定のためのガイドライン、第6部「情報システムのセキュリティ要件」の「6.1.1 主体認証機能【基本対策事項】」において、「多要素主体認証方式」の導入が求められている。本学においても、従来のパスワード認証に、学生証・職員証 IC カード、ワンタイムパスワード生成器、利用者本人が持つ認証デバイス、指紋や静脈、顔、虹彩など本人の生体的特徴を使った認証システムの更なる導入を推進し、認証システムの強化を図る。

6.1.2. FIDO 認証の導入

本学では、多要素認証の導入時のログイン高速化のため、指紋や静脈などによる生体認証を実施直後に即ログインできるように、多要素主体認証システムとして FIDO 認証を導入することで、情報サービスシステム認証の高速化を図る。

6.1.3. リスクベース認証の導入

本学では、多要素認証の導入時のログインの簡便化のため、リスクベース認証を導入して行く必要がある。リスクベース認証は、ログイン時の動作を記録し、次回ログイン時に前回のログイン時との相違の有無を確認してから、別の認証方式を追加したり変えたりする方式を採用している。そのため、リスクベース認証は、よりセキュアな認証システムの構築に重要な要素の一つとなる。

6.1.4. 認証システムのクラウド化

本学の認証システムは二重化されているもののすべて学内にあるため、自然災害などで認証システムが停止に追い込まれる危険性がある。平成28(2016)年の熊本地震や毎年襲来する台風、線状降雨帯のような大きな自然災害がいつ発生するとも限らない。そのため学外クラウドに認証システムのクローンを設置する必要がある。IT-BCP の観点からも、学外クラウド上に本学の認証システムを設置する必要がある。

6.2. 主体的監査などのセキュリティ人材育成

6.2.1. 本学職員による準拠性監査・技術監査の主体化

本学では本学全体としての人的セキュリティや情報サービス機器のセキュリ

ティ確保のため、情報セキュリティポリシー及び関連の運用管理規則に基づき、準拠性監査と技術監査を定期的実施している。これらの監査は、内部情報等のいわゆる機微情報まで踏み込むため、大学が主体として監査業務を行うのが望ましい。準拠性監査では、外部監査人と内部監査人が組織内の各部署の教職員について人的セキュリティがどの程度確保されているかを測定する。技術監査では、指定された学内情報サービス機器に擬似攻撃を実施し、脆弱性診断などを行う。何れの場合も監査結果に基づき問題が見出された場合は、是正措置の指示等を行う。本学での準拠性監査及び技術監査については以下のような課題がある。

- ・ 内部監査人や技術監査人が常に不足している
- ・ 準拠性監査は監査前の準拠性監査人研修の受講により監査人の確保が比較的容易
- ・ 技術監査は情報安全確保支援士などの資格またはサイバーセキュリティ業務経験が必要であり、監査人の確保は容易ではない

従って準拠性監査では、人材確保は容易であり、大学が準拠性監査を主体的に実施することは可能であるが、技術監査を大学が主体的に行うのは困難である。そのため、本学では技術監査業務ができる人材を確保することが重要となっている。

6.2.2. 第三者機関によるセキュリティ評価の強化

最近組織の第三者機関によるセキュリティ評価が注目されている。その原因は、近年インターネット上の様々な通信が暗号化通信を採用するようになったからである。セキュリティ評価の一例として、セキュリティスコアカードがある。調査対象の組織の指定された IP アドレスレンジに割り当てられている情報システムや端末等の脆弱性診断を行い、その診断結果を CTI (サイバー脅威インテリジェンス ; Cyber Threat Intelligence) と照らし合わせながら最終的に点数 (スコア) を計算する仕組みである。本学もこのセキュリティ評価を導入または同等のセキュリティ評価システムを開発し、セキュリティスコアの減点された部分について分析できる人材確保が必要である。

6.2.3. 情報部門・セキュリティ部門のスキルアップ

本学のサイバーセキュリティを維持して行くために、各部署における情報部門及びサイバーセキュリティ部門のセキュリティインシデント対応に関するスキルアップが必要である。例えば、総合情報統括センターや情報企画課における教職員、特に KU-CSIRT（熊本大学サイバーセキュリティインシデントレスポンスチーム；Kumamoto University CyberSecurity Incident Response Teams）のスキルアップの底上げは当然であるが、実際のセキュリティインシデントの現場は、各部署である場合が多い。そのため、各部署では以下の資格保有者または資格保有者相当の人材育成に取り組むのが望ましい。

6.2.4. 有資格者設置基準の設置とシステム部門の配置

本学の各部署における情報部門及びサイバーセキュリティ部門のセキュリティインシデント対応担当者に有資格者設置基準の設置が必要である。例えば、総合情報統括センターや情報企画課の教職員が中心となっている KU-CSIRT と連携して、迅速かつ的確にセキュリティインシデントに対応する担当者が必要である。実際に有資格者が配置されたシステム部門を設置することで、今後の苛烈化するサイバー攻撃に迅速に対応できるようにすることが重要である。

6.2.5. モバイルアプリによる構成員の情報セキュリティ研修の一層の強化

情報セキュリティポリシー及び関連運用管理規則に基づき、全教職員、全学生に情報セキュリティ教育の一環として情報セキュリティ研修を定期的実施している。情報セキュリティ研修はオンラインで実施し、受講者は、オンラインテキストを使った学習の実施、小テスト受験、自己点検評価等を行っている。教職員の受講率は概ね良好であるが、学生の受講率向上を図るため、スマートフォンやタブレット端末で受講しやすい情報セキュリティ研修用のモバイルアプリを開発する。

6.3. 説明可能な AI によるサイバー攻撃対策強化と SOC 体制の構築

6.3.1. DNS、電子メール、WAF の情報サービスの強化

本学の DNS サービス、電子メールサービス、WAF 等のサービスは、常にサイバー攻撃に晒されている。例えば、DNS サービスの保持データを改竄する不正利用、標的型サイバー攻撃の一環としての電子メールサービスの不正利用、Wi-Fi や認証システムの認証 ID の成りすまし等の不正利用または不正利用の試

み等がある。また最近ではゼロトラストの観点から、学外と学内ネットワークの接続点に導入されるファイアウォールに加えて、WAF サービスが重要な役割を持ち始めている。これは、本学のグループウェアや LMS 等の情報サービスシステムも不正利用の対象でありサイバー攻撃の標的となるからである。すなわち WAF はサービス利用者と Web アプリケーションの間のアクセス制御を行う重要なサービスである。そのため益々重要なセキュリティサービスとなることが考えられる。従って、DNS サービス、電子メールサービスの対策強化は継続的に行い、特に WAF サービス対策の強化を図る必要がある。ただし WAF の運用管理は設定が多岐にわたって複雑になってきたため、将来の人材不足が懸念される。RPA などの AI を用いた運用管理が考えられるが、従来のブラックボックス型の AI-ML（機械学習；Machine Learning）モデルでは、アクセス制御においてアクセスをブロックするため根拠が乏しいという欠点がある。そこで、これまでの対策強化に加え以下の強化策を図る。

- ・ 最新の FW（ファイアウォール；Firewall）技術や装置の情報収集
- ・ 学外クラウドの WAF 技術やサービスの情報収集
- ・ FW/WAF 技術の共同開発や評価試験の実施
- ・ CTI と XAI（特徴量などの貢献度が説明可能な AI；eXplainable AI）を用いた WAF の導入

6.3.2. XAI 等を利用した SOC 体制の構築

最近、本学のメールサービスの認証システム、Web アプリケーションサービスの認証システムなどが CF 攻撃を受けている。また、DNS 等のインターネット基盤サービスに対する DDoS 攻撃などがある。これらのサイバー攻撃は、AI 等によって自動化され攻撃能力が向上しているため、特定の送信元 IP をブロックしてもすぐに別の送信元を用意されるなど、持続的に攻撃を続けるこれらの攻撃を防ぐのは一般的に困難である。また、DDoS 攻撃では大量の送信元 IP が得られるが、従来の説明可能ではない、所謂ブラックボックス型 AI で検出を図っても精度があまり高くない。そこで、CF や DDoS などのサイバー攻撃対策強化策として、情報サービスシステムや情報機器で常時記録されているログの分析について、XAI を用いることでサイバー攻撃の的確な検出を図る。

- ・ DNS のログ分析による本学の組織全体に対するサイバー攻撃の把握

- ・ 電子メールサービスのセキュリティの強化
- ・ WAF の強化の検討

6.3.3. AI 機械学習によるログ収集と分析と可視化

本学 DNS サービス、電子メールサービス及び WAF の各ログデータについて、XAI/ML モデルを用いて分析する。具体的には、以下の分析を行う。

- ・ 各ログ内のデータ間の因果関係を分析
 - ログ中のデータが相互にどれだけ影響を与えるかを調査する
- ・ 各ログデータを時系列データとして相関関係を分析し可視化する
 - 時系列的な変化点（アノマリ）を検出 → AI/ML モデル確定
- ・ 各ログのデータと CTI の予測モデルから規則性を検出する
 - AI/ML モデルの規則性が変化するログデータを分析 → 複数の特徴量などの貢献度が説明可能な XAI/ML モデルを確立
- ・ 確立された特徴量などの貢献度が説明可能な XAI/ML モデルに重みを付ける
 - KU-CSIRT の判断を反映させ、予測モデルの精度を向上させる

6.3.4. SIEM による自動検知・報告の仕組みの構築

本学において DNS サービス、電子メールサービス及び WAF などの各ログデータについて、常時監視を行う担当部署である SOC の設置を図る。SOC は主としてセキュリティ情報と SIEM を運用管理する。SIEM は以下の事項の総称である。

- ・ ログ管理: ログを収集し、保存管理
- ・ SIM（セキュリティ情報管理；Security Information Management）：ログデータの分析と報告及びログの長期保存
- ・ SEM（セキュリティイベント管理；Security Event Management）：リアルタイム監視、イベント相関、通知、可視化
- ・ MSS（Managed Security Service）：接続性と帯域場、モニタリング、障害復旧
- ・ SECaaS（SECurity-as-a-Service）：認証、ウイルス対策、マルウェア対策/スパイウェア、侵入検知、侵入テスト、セキュリティイベント管理

6.4. インシデント対応の強化

6.4.1. IT-BCP の策定

本学における情報セキュリティインシデント対応業務（以下「インシデント対応」という。）は、KU-CSIRT が行っている。また本学では自然災害などを想定した BCP は策定しているが、サイバー攻撃などの IT リスクを考慮した IT-BCP はまだ策定していない。すなわち重大なインシデントが発生した後の応急措置的な対応は整備されているが、その事業復旧については遅延する恐れがある。したがって IT-BCP の策定を実施する。まず、本学で IT-BCP が緊急で必要と考えられる部署から順次 IT-BCP 策定の依頼を行い、合わせて策定支援を行う。

6.4.2. CSIRT 訓練の強化

インシデント発生時に迅速かつ的確に対応するため、本学の KU-CSIRT のインシデント対応訓練を実施している。インシデント対応訓練は、万一自組織でインシデントが発生してしまったことを想定し、KU-CSIRT などの組織がインシデント対応手順に沿って、一連の対応を行うことを訓練する。しかし最近のインシデントは複雑化しており、対応訓練を強化して迅速に対応する必要がある。訓練の強化策として以下を実施する。

- ・ 状況付与型演習訓練: シナリオをもとに時系列に沿って演習を行う訓練で、従来の訓練
- ・ 教育型訓練: 従来の状況付与型演習に、場面ごとに解説を加えながら行うことで、場面ごとにおける対応の根拠の理解を促進する訓練

6.5. ゼロトラスト

6.5.1. デジタルキャンパス化

本学における DX は、デジタルキャンパス化に向けて進み始めている。COVID-19 の感染拡大の影響をきっかけとして、多くの講義がオンライン化またはオンデマンド化し、LMS の本格利用が始まった。また、教職員もテレワークで在宅勤務になり、特に大学のあらゆる会議やゼミがオンライン会議システムで行われるようになった。従来の境界型のサイバーセキュリティ対策も、テレワーク環境下ではあまり意味を持たなくなる。すなわちゼロトラストネットワークの導入が必須となる。ゼロトラストとは、情報システムに接続してくる

情報端末の点数評価を行い、その点数に応じて認証方法を変える仕組みのことである。従ってゼロトラストネットワークを導入するためには、認証の強化が必要である。

6.5.2. ゼロトラストネットワークの導入

本学にゼロトラストネットワークを導入する場合、まず認証の強化が必要である。認証システムには、XAI/ML モデルを用いて接続端末のスコアリングを実施し、接続時に通常使用している端末とは別の端末を接続した場合などに新たな別の認証を起動するようにする必要がある。

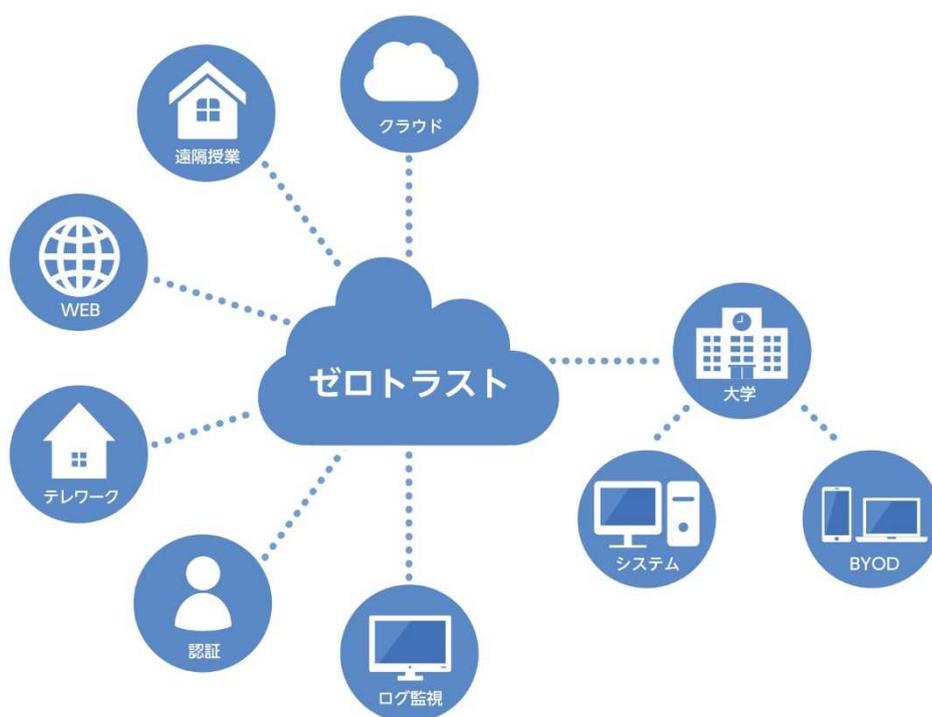


図 6-2 : ゼロトラスト

7. 中期目標・中期計画との関係等

7.1. 中期目標・中期計画との関係

本構想は、令和4（2022）年度から始まる第4期中期目標・中期計画の6年間の期間を視野に入れて作成した。例えば、第4期中期目標、中期計画における検証可能な評価指標として「学内向け申請書のWEB申請化率／90%以上」、「学生向け窓口数のオンライン化率／80%」、「業務系システムにおけるクラウド利用新規システム数／5システム以上」、「研修受講率／対象者の95%以上」、「対象施設の入退出集中管理化率／70%以上」を設定しているが、これらは本構想における「環」と以下のとおり対応している。

- ・ 学内向け申請書のWEB申請化率／90%以上
→ サービス最適化の環、リソース適正化の環
- ・ 学生向け窓口数のオンライン化率／80%
→ サービス最適化の環、リソース適正化の環
- ・ 業務系システムにおけるクラウド利用新規システム数／5システム以上
→ リソース適正化の環
- ・ 研修受講率／対象者の95%以上
→ リソース適正化の環、セキュリティ堅牢化の環
- ・ 対象施設の入退出集中管理化率／70%以上
→ データ流動化の環、リソース適正化の環

以上のとおり、本構想には第4期中期目標・中期計画の事項が含まれているが、必ずしも1対1に対応しているわけではなく、対応状況は本構想付録*のとおりである。本構想は、あくまでも本学の今後の発展を考えたときに、どのようなICT化が理想であるかを基本に考えたものであり、予算や人的裏付けを考慮せずにより幅広い事項を設定している。

中期目標・中期計画においては、その時代の趨勢や予算状況を勘案したうえで、本構想を基本的理念として具体的施策を再度検討することを前提としている。場合によっては、本構想自体も、適宜改訂し時代にあったものとする必要がある。

7.2. 実施スケジュールに関して

前項にも述べたとおり、本構想は、中期目標・中期計画そのものではなく、

その後ろ盾となる基本構想であるため、実施スケジュール等は特に意識していない。実施スケジュール等は、中期目標・中期計画に沿って、その時代の趨勢や予算状況によって適宜決定する必要がある。

* ホームページ公開版では、付録「総合情報環構想2022と第4期中期目標・中期計画との対応表」は省略している。