情報処理学会論文誌 Vol.63 No.3 879–894 (Mar. 2022)

事業継続性に配慮した認証基盤システムの構築と運用

土屋 雅稔[1,a)] 中村 純哉[1,b)]

受付日 2021年6月1日, 採録日 2021年12月3日

概要：大学を含む公的機関にとって，各種の異常事態に対する事業継続性の確保は，重要な課題の 1 つである．本論文では，2 つの観点から認証基盤システムの事業継続性について検討する．第 1 に，大規模災害に対する事業継続性について検討する．大規模災害に対する事業継続性を確保するには，情報システムを安全な遠隔地に設置するだけでなく，異常時の挙動について十分に検証する必要がある．本論文では，認証基盤システムを遠隔地に設置する場合の設計上の留意点と，平常時の停電を利用して異常時の挙動を定期的に検証する運用経験について述べる．第 2 は，感染症によるロックダウンに対する事業継続性である．キャンパスがロックダウンされた場合，従来は対面形式で行われていた各種手続きをオンライン化する必要がある．しかし，安全な認証という前提を保ちつつ，各種手続きをオンライン化することは，決して容易なことではない．本論文では，複数の多要素認証手段を組み合わせることにより，できるだけ安全に各種手続きをオンライン化する方法と，COVID-19 パンデミックにおける対処経験について述べる．

キーワード：事業継続，認証基盤，多要素認証，COVID-19 パンデミック

Construction and Operation of Authentication Infrastructure System to Ensure Business Continuity

Masatoshi Tsuchiya[1,a)] Junya Nakamura[1,b)]

Received: June 1, 2021, Accepted: December 3, 2021

Abstract: This paper examines the business continuity of an authentication infrastructure system from two perspectives. The first perspective is the business continuity against large-scale disasters. In order to ensure business continuity against a large-scale disaster, it is necessary not only to place the information system in a safe remote location, but also to verify its behavior in case of abnormalities thoroughly. This paper describes the design considerations for an authentication infrastructure system in a remote location and explains our operational experience to verify its behavior. The second perspective is the business continuity against lock-downs caused by infectious diseases. This paper describes our online procedures, which combine multiple multi-factor authentication methods, and explains our experience in dealing with the COVID-19 pandemic.

Keywords: BCP, authentication infrastructure, multi-factor authentication, COVID-19 pandemic

1. はじめに

近年，組織内で各種業務に関わる情報システムは増加する一方である．それらの情報システムが個別にユーザ情報を保存し，個別にユーザ認証を行うことは，情報システムのセキュリティを維持する観点からも，ユーザの利便性の観点からも好ましくない．そのため，情報システムのユーザ情報を統合し，ユーザ認証を連携してシングルサインオン（Single Sign On; SSO）を実現する**認証基盤システム**が必要とされている [1], [2], [3].

認証基盤システムの設計に対する要件として，本論文では，以下の 3 点について考える．第 1 の要件は，事業継続性の確保である．大学を含む公的機関にとって，大規模災害や感染症などの各種の異常事態に対する事業継続性の確保は，重要な課題の 1 つである [4], [5], [6]．豊橋技術科学大学（以下，本学）は，東南海地震発生時には震度 6 強

[1] 豊橋技術科学大学情報メディア基盤センター
Information and Media Center, Toyohashi University of Technology, Toyohashi, Aichi 441–8580, Japan
[a)] tsuchiya@imc.tut.ac.jp
[b)] junya@imc.tut.ac.jp

が想定されている地域に立地しており[*1]，地震を主要なリスク要因とする事業継続計画（Business Continuous Plan; BCP）は重要な課題として認識されている．認証基盤システムは，各種の情報システムの基盤として動作するシステムであるから，事業継続性についても慎重な配慮が必要である．第2の要件は，安全な認証方式の提供である．認証基盤システムの導入によりSSOが実現されている組織では，アカウントが窃取された場合の影響はきわめて大きい．従来のユーザ名・パスワードに基づく認証は，アカウントの窃取に対する耐性が十分ではないため，多要素認証を導入することが一般的である [7], [8]．第3の要件は，パスワード初期化（復旧）などの各種手続きのオンライン化である．本学は，留学生が全学生の13.7%を占めるほか，ダブルディグリープログラムによって海外提携校に長期滞在する学生も多い．2013年にはマレーシアに教育拠点を設置している[*2]．それにともない，海外拠点や提携校で活動している利用者に対して，各種手続きをオンラインで提供する必要がある．

大規模災害においては，建築物の損壊や停電，ネットワーク回線の物理的な途絶などの各種の障害の発生があり得るから，キャンパス内に設置された情報システムの稼働を維持することはきわめて困難である．そのため，遠隔地のデータセンタ（DC）に情報システムを設置し，稼働を維持するという設計方針が広く採用されている [9], [10], [11]．この設計方針を採用する場合，2種類の障害についての十分な検討が必要である．第1は，遠隔地DCと大学キャンパスを接続するネットワーク回線のトラブルなどが原因となって，大学キャンパスの人員や設備は健全であるにもかかわらず，遠隔地DCのシステムが利用できない場合である．第2は，大規模災害の発生などが原因となって，大学キャンパスの人員や設備が利用できなくなった場合の挙動である．しかも，この2種類の障害に対する対策は，相反する関係にある．前者の障害に対応するには，一部の業務システムを大学キャンパス側に残し，障害時にも業務を継続できるよう設計する必要がある．つまり，平常時には，遠隔地DCのシステムは，大学キャンパスのシステムと連携して動作しなければならない．しかし，後者の障害が発生したときには，遠隔地DCのシステムは，大学キャンパスのシステムに依存することなく動作しなければならない．よって，これらの対策を両立するためには，なんらかのシステム切替が避けられない．

障害発生を検知し，システム切替を行う設計は一般的ではあるが，頑健なシステム切替を実現することは非常に困難である．頑健性を高めるには，平常時から計画的かつ人為的に障害を発生させることにより，事前の設計どおりにシステムが自動的に縮退することを確認する手法が有効である [12]．ただし，この手法は，十分な人員と予算を必要とする手法であり，人員と予算に厳しい制約が課せられている状況で，広範に実施することは難しい．そのため，本論文では，本学キャンパスの受電設備の法定点検にともなう年1回の停電を計画的な障害と見なして，自動切替の頑健性を改善する運用経験について述べる．

近年の認証基盤システムでは，アカウントの窃取に対して十分な耐性を持つ認証方式を提供するため，多要素認証を導入することが一般的である [7], [8]．しかし，安全な認証という前提を保ちつつ，アカウント情報の交付やパスワード初期化（復旧）などの各種手続きをオンライン化することは，決して容易なことではない．たとえば，アカウント情報の交付後に多要素認証用のデバイスを登録する必要があるが，登録時にはそのデバイスを多要素認証で利用できないため，認証強度も低下する．逆に，パスワードの忘失によってパスワードの初期化が必要となる場合には，多要素認証用のデバイスは利用できても，パスワードが利用できないため，やはり認証強度が低下する．本論文では，郵送が可能なマトリクスコードとTOTPトークンを組み合わせることによって，多要素認証による安全性を維持しつつ，かつ，各種手続きをオンライン化する実施例を示す．加えて，COVID-19パンデミックによるキャンパスのロックダウン状況において事業を継続するために，各種手続きのオンライン化が有効だったことを示す．

本論文の構成は，以下のとおりである．最初に，2章と3章では，遠隔地に情報システムを配置し，認証基盤システムの各種手続きをオンライン化する場合の設計上の留意点について述べる．2章では，2014年から2019年まで運用した第1世代システムについて，3章では，2019年から運用している第2世代システムについて述べる．次に，4章では，各システムの運用経験と，COVID-19パンデミックに対する対応について述べる．最後に，5章で結論を述べる．

2. 第1世代システムの構成と問題点

この章では，非常時に必要となるシステムを遠隔地に設置するという方針により設計した第1世代システムの構成と問題点について述べる．第1世代システムは，2014年3月に稼働を開始し，2019年秋に稼働を終了した．

2.1 基幹通信システムの選定

先に述べたとおり，本システムの設計にあたっては，本学キャンパスの設備が大規模災害により利用できない非常時において必要となるシステムを，遠隔地DCに設置するという方針をとる．この節では，非常時に必要なシステムの範囲について検討する．

筆者らは，地震などの大規模災害発生時において何をお

[*1] 南海トラフ巨大地震対策検討ワーキンググループの報告 http://www.bousai.go.jp/jishin/nankai/nankaitrough_info.html による．
[*2] https://ignite.tut.ac.jp/cie/penang/

いても維持しなければならないシステムは，大学と構成員の通信手段であると考える．その理由は，災害発生時に必要となる各種の作業（たとえば，安否確認など）はすべて，通信手段の確保が必要だからである．現代では，そのような通信手段としてメールとウェブを想定することが一般的である．本学では，すべての構成員（教職員および学生）に対してメールが利用できるアカウントを発行し，メールを各自の携帯電話に転送するように指導している．各種通知（たとえば，休講通知など）はすべてメールによって行われているため，多くの学生は転送設定していることが期待される．

以上より，第 1 世代システムでは，非常時に稼働を継続する通信用システムとして，メールシステムと大学公式ウェブサーバを想定する．さらに，これらの通信用システムが動作するには，大学ドメインの権威 DNS サーバおよびメールシステムのユーザ認証基盤としての LDAP サーバが不可欠である．以後，これらのシステムをまとめて，**基幹通信システム**と呼ぶ．

2.2 遠隔地 DC の選定

基幹通信システムを配置する遠隔地 DC の設置場所の選定条件として，本学キャンパスと同時に被災する可能性が低く，かつ，ネットワーク回線が確実に確保できること，という 2 点を考慮する．以下では，その検討過程について述べる．

筆者らは，ネットワーク回線が確実に確保できるという条件を満たす DC として，学術情報ネットワーク SINET4 のコアノードが収容されている DC を候補として検討した．SINET4 のコアノードは，他のコアノードと 2 系統以上の回線により接続されており，回線冗長が確保されている（**図 1**）．コアノードは，札幌，仙台，東京，金沢，名古屋，大阪，広島，博多と全国に 8 ノード存在し，本学キャンパスのネットワークは名古屋 DC に接続されている．8 ノードのうち，大阪 DC および名古屋 DC は，東南海地震によって本学キャンパスと同時に被災する可能性があること，東京 DC はラックの借用費用が高価であること，金沢 DC は回線が比較的細いことから，それぞれ除外する．

残るコアノードはいずれもかなりの遠隔地にあるため，本学キャンパスの最寄り空港からの直行便が存在し，アクセスが比較的容易と考えられた札幌 DC と博多 DC を候補として検討する．NII の協力を得て，両 DC と名古屋 DC のレイテンシを測定したところ，札幌 DC のレイテンシは 24 msec，博多 DC のレイテンシは 17 msec であり，博多 DC のレイテンシがわずかに小さかった．以上の検討から，博多 DC を，基幹通信システムを収容する遠隔地 DC として選定する．

なお，遠隔地 DC は，DC 内に設置された機器に障害などが発生した場合に対応要員が駆けつけるまでに時間を要するという欠点がある．そのため，キャンパス内または近接地に DC を確保するという方法が有効な場合もある [4], [5]．しかし，本学が主要なリスク要因として想定している東南海地震の想定被害地域はきわめて広範囲であるため，そのような方法は非現実的である．

2.3 ネットワーク設計

遠隔地 DC と本学キャンパスのネットワーク設計にあたっては，2 つの条件を考慮する．第 1 に，本学キャンパスが災害などで停電した場合であっても，インターネットから遠隔地 DC に対する通信が維持される必要がある．第 2 に，本学キャンパスで業務が行われている平常時においては，本学キャンパスから遠隔地 DC に対して，インターネットを経由することなく，低レイテンシかつセキュアな接続が利用できる必要がある．

第 1 世代システムのネットワーク構成の概要を**図 2** に示す．第 1 の条件を満たすため，本学キャンパスと遠隔地 DC に，それぞれルータを設置する．そのうえで，豊橋ルータは，大学全体のネットワーク（133.15.0.0/16）に対する経路を広告し，博多ルータは，基幹通信システムの

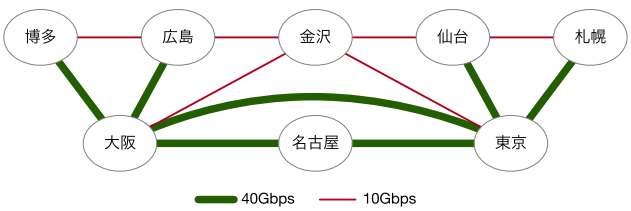


図 1 SINET4 コアノードのネットワークトポロジ
Fig. 1 Network topology among SINET4 core nodes.

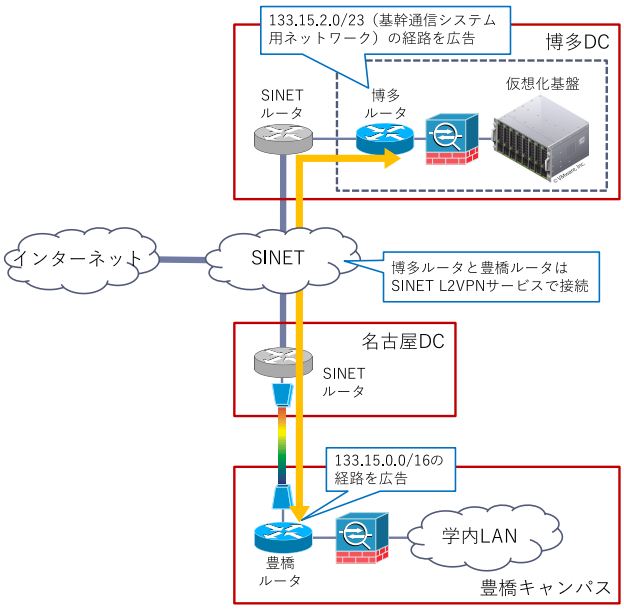


図 2 ネットワーク構成（第 1 世代）
Fig. 2 Network structure of the first generation system.

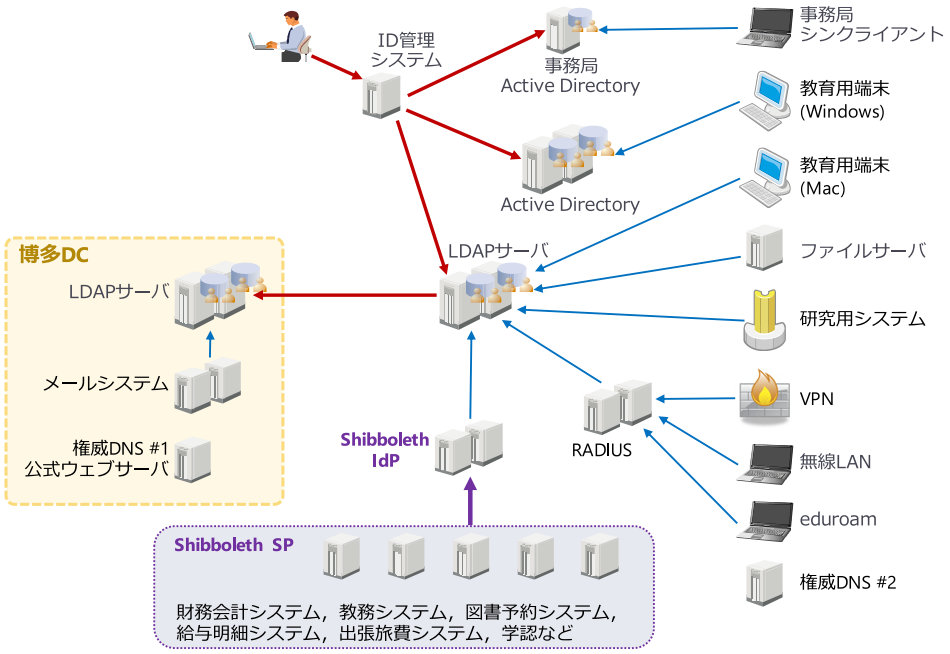


図 3 システム構成（第 1 世代）
Fig. 3 Structure of the first generation system.

ネットワーク（133.15.2.0/23）に対する経路を広告する[*3]．インターネット上の接続元から見ると，博多ルータが広告している経路がより限定的であるから，インターネット上の接続元から基幹通信システムに接続する場合には，本学キャンパスを経由することなく接続できる．したがって，本学キャンパスが大規模災害などにより停電している場合であっても，特別な切替を必要とすることなく，基幹通信システムに対する接続は維持される．第 2 の条件を満たすため，本学キャンパスと博多ルータ間には，SINET の L2VPN サービスを利用した静的な経路を設定する．これにより，本学キャンパスから基幹通信システムに対する通信は，SINET に閉じた経路を利用することができ，ほぼ学内ネットワークに準じたセキュリティを確保できる．

2.4 システム設計

これまで述べた方針に基づいて設計した第 1 世代システムの構成を図 3 に示す．以下では，第 1 世代システムの設計に関する考慮点について述べる．

遠隔地 DC は，障害発生時に対応要員が駆けつけるまでに時間を要するという欠点がある．そのため，遠隔地 DC には仮想化基盤を設置し，基幹通信システムを構成するすべてのサーバは，仮想化基盤上の仮想マシンとする．仮想化基盤の物理ノードに障害が発生した場合でも，別の物理ノードにフェイルオーバすることにより，対応時間を確保することができる．ただし，この方針では，仮想マシンが物理ノードをフェイルオーバする際の短時間のシステム停止が避けられない．基幹通信システムのうち，権威 DNS サーバと大学公式ウェブサーバについては，短時間のシステム停止は許容可能[*4]であるから，単一の仮想マシンとして構成する．それ以外のメールシステムおよび LDAP サーバについては，active-active または active-standby の冗長構成を採用し，システム停止を回避する．

認証基盤システムを構成するサブシステムのうち，基幹通信システムに含まれないサブシステムは，本学キャンパス側に設置する．第 1 に，本学キャンパスと遠隔地 DC とのネットワーク接続が故障した場合にも本学の業務を継続するためには，ユーザ管理システムと Shibboleth Identity Provider（以下，IdP）は本学キャンパスにも設置されている必要がある．第 2 に，災害発生などの非常時に新規ユーザの追加が必要となるような状況は考えにくい．そのため，ユーザ管理を行う ID 管理システム，ID 管理システムによってユーザ情報が登録されるプライマリ LDAP サーバは，本学キャンパス側に設置する．遠隔地 DC に設置する LDAP サーバは，本学キャンパスから情報が同期（sync replicate）されるセカンダリサーバとする．

なお，第 1 世代システムでは，パブリッククラウドではなく，遠隔地 DC に仮想化基盤を設置する方針を採用する．この方針の理由は 2 つある．第 1 に，基幹通信システムにメールシステムが含まれており，性能要件の保証が必要である．第 1 世代システムのメールシステムの性能要件を，

[*3] 正確には，各ルータが接続する SINET ルータが経路を広告し，SINET ルータと博多・豊橋ルータ間はスタティックルーティングでパケットが転送される．

[*4] 権威 DNS サーバについては，本学キャンパスの権威 DNS サーバおよび SINET の分散セカンダリ DNS サービスで冗長化している．

表 1 に示す．この性能要件は，第 1 世代システム以前のシステム [13] の動作記録に基づいて求めた要件であり，本学程度の規模の利用者が十分な使用感を維持するために重要な指標である．この性能要件からさらに，ストレージの性能要件が求められる．しかし，第 1 世代システムの設計時には，ストレージの性能要件が保証された IaaS は，価格その他の要因により現実的ではなかった．第 2 に，第 1 世代システムの設計時には，メールシステム（特に教職員が利用するメールシステム）を SaaS として外部委託することについてのコンセンサスが十分に確立されていなかった [14]．

2.5 多要素認証の導入

第 1 世代システムの設計時においてすでに，パスワード漏洩やフィッシングによるアカウント乗っ取り事例が報告されており，多要素認証の必要性が指摘されていた [1], [2], [3], [8]．そのため，第 1 世代システムでは，接触式 IC カードに格納された個人証明書による多要素認証を導入する [15]．ただし，接触式 IC カードの調達コストとの兼ね合いから，研究費管理や物品発注などの限定された重要システムと，重要システムを利用する教職員のみを対象とし，それ以外の構成員（学生を含む）については対象外とする．そのため，履修登録システム[*5]などの重要な個人情報を扱うシステムについては，学外ネットワークからのアクセスを制限する．

2.6 問題点

第 1 世代システムでは，基幹通信システムを必要最小限度として設計したため，利用者視点からは分かり難い制限が 2 点発生した．第 1 に，本学キャンパスの停電時には IdP が利用できない．そのため，利用者は，学術認証フェデレーション[*6]を通じて連携している電子ジャーナルを閲覧できない．第 2 に，本学キャンパスの停電時には RADIUS サーバが利用できない．そのため，eduroam[*7]に参加している他機関に利用者が滞在している場合であっても，当該機関の無線 LAN を利用できない．どちらの制限も，利用者から見える電子ジャーナルや無線 LAN は動作しているにもかかわらず，利用者から見えないシステムが停止しているために使えないという制限であり，利用者視点からは非常に分かり難い．

表 1 第 1 世代メールシステムの性能要件（抜粋）
Table 1 Performance requirements of the first generation mail service.

SMTP サーバ	同時接続数	260 セッション以上
	スループット	26 通/秒以上
IMAP サーバ	同時接続数	4,000 セッション以上
POP3 サーバ	アクセス数	15 回/秒以上
ウェブメール	同時接続数	200 クライアント以上

[*5] 本学の履修登録システムでは，教員は指導学生の成績を，学生は自分の成績を確認することができる．
[*6] https://www.gakunin.jp/
[*7] https://www.eduroam.jp/

3. 第 2 世代システムの構成

第 2 世代システムは，第 1 世代システムを引き継いで 2019 年秋から運用を開始した．

3.1 基幹通信システムの選定

第 2 世代システムの設計時点では，メールシステムを外部委託する事例が十分に蓄積されており [7], [16]，予算など各種の制約からも，メールシステムをパブリッククラウドの SaaS に移転することは既定事項だった．この節では，この制約条件に基づき，第 2 世代システムの基幹通信システムの選定について述べる．

パブリッククラウドのメールシステムを利用する場合，そのユーザ認証方式としては，利用組織（大学）の IdP を用いる方式と，サービスプロバイダの IdP を用いる方式の 2 通りが考えられる [3], [7]．第 2 世代システムでは，2 つの理由から，利用組織の IdP を用いる方式を採用する．第 1 の理由は，本学キャンパスのネットワーク接続の状況である．図 4 に示すとおり，本学キャンパスと遠隔地 DC に関係するネットワーク障害は，頻度は決して大きくはないが，無視はできない頻度で発生している．そのため，ネットワークが停止している状況でも，本学キャンパス内の業務システムを利用した業務を継続できるように設計する必要がある．それには，少なくともセカンダリとして動作する IdP を学内ネットワークに配置する必要があるが，サービスプロバイダの IdP と組合せて，そのような配置を実現することは困難である．

第 2 の理由は，多要素認証の拡張（3.4 節）にあたって，段階的に進める必要があるという点である．第 2 世代システムの運用期間中には，メールシステムだけでなく，各種業務システムのパブリッククラウドへの移転は不可避である．そのため，多要素認証の対象者を拡大し，学内外を問わず，システムを安全に利用できる認証基盤が必要であ

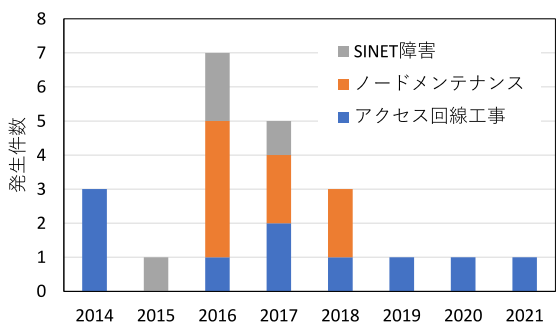


図 4 ネットワーク障害の発生状況
Fig. 4 Statistics of network incidents.

る．しかし，多要素認証を導入すると，利用者の負担感は基本的に大きくなる．**図 5** に示すとおり，本学の認証基盤は多数の業務システムから参照されているため，認証方法の変更は業務に大きな影響を生じる．そのため，学内ネットワークから接続した場合は多要素認証を強制せず，学外ネットワークから接続した場合は多要素認証を強制する，というような段階的な導入が必要である．ただし，先行事例 [2] とは異なり，SP ごとに管理者側で制御する方式とする．サービスプロバイダの IdP では，このような柔軟な設定には対応が困難である．

第 1 世代システムの問題点（2.6 節）および上記の分析から，第 2 世代システムの基幹通信システムとして，大学公式ウェブサーバ，メールシステム，IdP，RADIUS サーバ，LDAP サーバおよび権威 DNS サーバを選定する．**表 2** に，第 1 世代システムと第 2 世代システムの基幹通信システムの変化を示す．

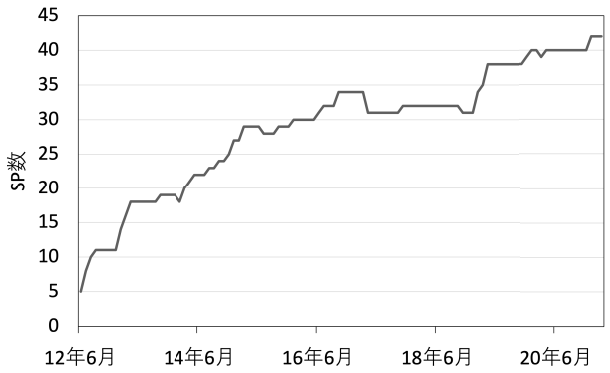


図 5 学内フェデレーションに参加している Service Provider（SP）
Fig. 5 Number of SPs in our local federation.

3.2 システム設計

これまで述べた方針に基づいて設計した第 2 世代システムの構成を**図 6** に示す．以下では，第 2 世代システムの設計に関する考慮点について述べる．

第 2 世代システムでは，基幹通信システムを収容するためにパブリッククラウドの IaaS を採用する．2.4 節で述べたとおり，第 1 世代システムでは，メールシステムに関する性能要件を保証するために，遠隔地 DC に設置した仮想化基盤上に基幹通信システムを収容していた．それに対し，第 2 世代システムでは，メールシステムが SaaS に移転するため，メールシステムに関する性能要件を考慮する必要がなくなり，より安価なパブリッククラウドの IaaS を利用できる．ライセンス契約および予算的な理由から，基幹通信システムを収容するパブリッククラウドとして Microsoft Azure を選択する．東南海地震によって本学キャンパスと同時に被災する可能性がある大阪リージョンを除外すると，Microsoft Azure 東京リージョンが，基幹通信システムの収容先として適切である．また，メールシステムとし

表 2 基幹通信システムの比較
Table 2 Comparison of core services of the first and second generation systems.

	第 1 世代システム	第 2 世代システム
公式ウェブサーバ	○	○
メールシステム	○	（SaaS に移転）
LDAP サーバ	○	○
権威 DNS サーバ	○	○
IdP		○
RADIUS サーバ		○

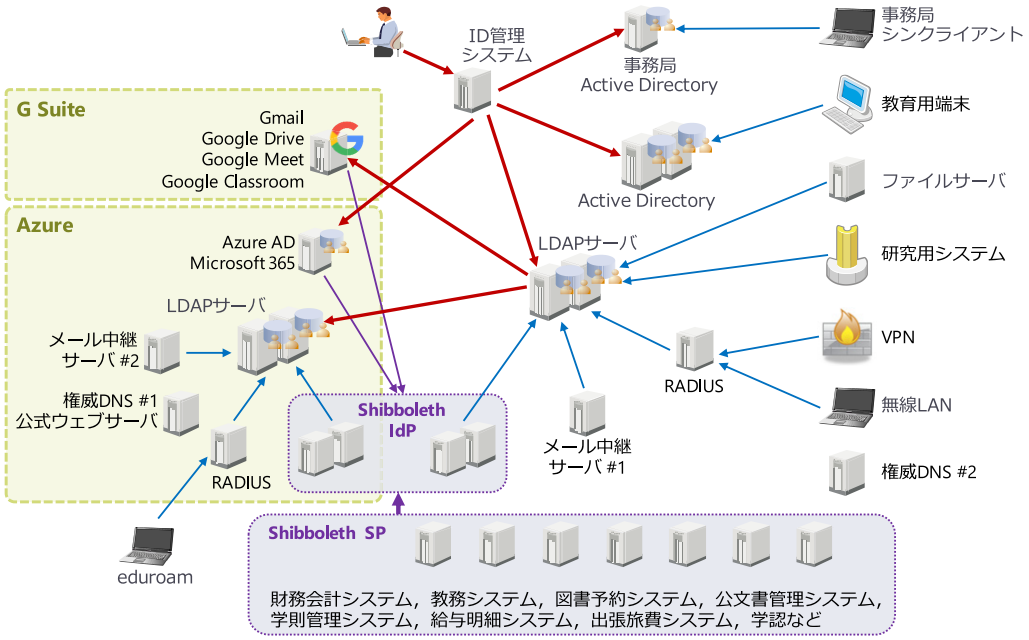


図 6 システム構成（第 2 世代）
Fig. 6 Structure of the second generation system.

ては，利用者が個人的にも利用している事例が多く[*8]，操作方法に習熟していると期待される Gmail を選択する．

本学キャンパスと SINET のネットワーク接続が停止している場合にも，学内ネットワークに接続している利用者は学内システムに基づく業務を継続できること，また逆に，学外ネットワークに接続している利用者は学外システム（メールシステムを含む）に基づく業務を継続できることが必要である．この要件を満たすため，権威 DNS サーバと IdP を学内・学外の 2 カ所に設置し，接続元ネットワークに基づいて負荷分散するよう設定する．具体的には，学内ネットワークから IdP の IP アドレスの問合せがあった場合には学内 IdP の IP アドレスを回答し，学外ネットワークから問合せがあった場合には学外 IdP の IP アドレスを回答する[*9]．学内 IdP と学外 IdP でセッション情報の共有は行っていないので，接続元ネットワークが変わったときには再ログインが必要になる．しかし，接続元ネットワークが頻繁に変わる（つまり，学内外を頻繁に移動する）ような状況は珍しいと考えられるので，セッション情報を共有するためにシステムが複雑化するデメリットを避けることを優先する．

ユーザ管理システムの配置およびサービスの冗長構成については，第 1 世代システム（2.4 節）と同様の方針をとる．

3.3 ネットワーク設計

図 7 に，第 2 世代システムのネットワーク構成を示す．第 1 世代システムと同様，第 2 世代システムでも，本学キャンパスと Microsoft Azure それぞれに設置された LDAP サーバ間で，ユーザ情報の同期が発生する．これらの情報を安全に送受信するため，SINET クラウド接続サービスで本学キャンパスと Microsoft Azure の仮想ネットワークを接続する．SINET クラウド接続サービスは，SINET の L2VPN 機能によって様々なクラウドサービスに対するセキュアなネットワーク回線を提供するサービスである．SINET とクラウドサービスの接続方式はサービスごとに異なり，Microsoft Azure では Azure ExpressRoute[*10] を利用する．第 2 世代システムでは，必要となる通信帯域・転送量ともに少ないことから，通信帯域 50 Mbps の従量制プランを選択する．

大学業務において，メールは重要なコミュニケーション手段である．3.2 節で述べたとおり，第 2 世代システムのメールシステムとして Gmail を採用すると，たとえ学内に閉じたメールであっても，その利用のためにはインターネット接続が必須である．第 1 世代システムでは，インターネット回線が SINET しかなかったことから，ネットワーク障害時（図 4）には，しばしばメールシステムが利用できなくなった．この問題を解決するため，第 2 世代システムでは別途フレッツ光回線を用意する．メインの SINET 回線に障害が発生した際には，自動でフレッツ光回線にルーティングが切り替わるように，豊橋ルータで制御する．これにより，インターネット接続の冗長性を確保する．

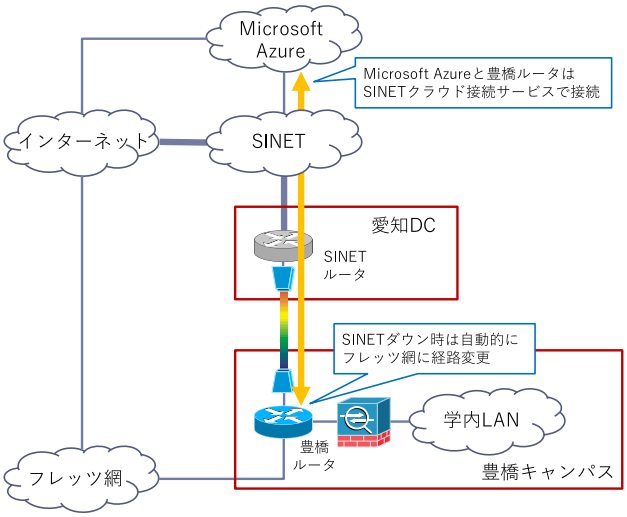


図 7 ネットワーク構成（第 2 世代）
Fig. 7 Network structure of the second generation system.

3.4 多要素認証の拡張

第 2 世代システムの認証方法の設計にあたっては，2 つの要件がある．第 1 は，多要素認証の対象範囲の拡大である．第 1 世代システムの多要素認証では，接触式 IC カードの調達コストとの兼ね合いから，教職員のみを対象とし，それ以外の構成員は対象外としていた．しかし，アカウント乗っ取り事例の多発により，対象システムおよび対象アカウントを大幅に拡大する必要がある．第 2 は，本学キャンパスに物理的に来訪できない利用者に対するアカウント管理手続きの提供である．1 章で述べたとおり，国際交流の活発化にともなって，海外拠点や提携校で活動している利用者に対して，アカウント情報の交付やパスワード初期化（復旧）などの各種手続きをオンラインで提供する必要がある．この節では，上記の 2 つの要件を満たす認証方法の設計について述べる．

3.4.1 所持要素の選択

多要素認証とは，認証の 3 要素（知識要素・所持要素・生体要素）のうち，どれか 2 つ以上の要素を確認する認証方式である．大学情報システムにおいては，運用コストの観点から，知識要素と所持要素を組み合わせることが一般的である．所持要素としては，IC カードに格納された個人証明書，TOTP トークン，またはマトリクスコードなどが

[*8] 第 1 世代システムのメールシステムでも，学外プロバイダへのメール転送を許可していた．その転送先を調査したところ，Gmail の利用者が圧倒的に多数だった．
[*9] したがって，学内ネットワークに接続している端末であっても，学外のパブリック DNS キャッシュサーバを参照している場合は，学外 IdP を利用することになる．
[*10] https://azure.microsoft.com/en-us/services/expressroute/

一般的である．ただし，所持要素の性質により，達成される認証強度が大きく異なる点に注意が必要である．この項では，第2世代システムにおける所持要素の選択理由について述べる．

ICカードに格納された個人証明書の複製耐性は，非常に高い．また，PINによって保護されているため，紛失に対しても耐性がある．そのため，ICカードを所持している人間は，正当な利用者であると強く推認できる．しかし，ウェブブラウザとICカードが認証のために通信するには，ICカードリーダの設定が必要であり，利用者サポートコストが非常に高い．また，ICカード媒体が，かなり高価である．

TOTPトークンの複製耐性は比較的高く，正当な利用者が意図しない複製は困難である[*11]．紛失に対する耐性は，TOTPトークンの保護機能に依存する．たとえば，TOTP生成時に指紋認証やPINを要求するTOTPトークンであれば，紛失に対しても耐性がある．したがって，所持している人間は，正当な利用者または正当な利用者が意図した第3者であると推認できる．利用者が所有する情報機器にインストールするタイプのソフトウェアトークンは，Google Authenticatorなど無償の実装が公開されており，安価に利用できる．ただし，TOTPトークンを安全に登録する方法について，慎重な検討が必要である．

なんらかの紙媒体に印刷されたマトリクスコードは，正当な利用者が意図した複製は容易であるばかりか，正当な利用者が意図しない複製（盗撮など）の危険性もあり，複製耐性は非常に低い．また，紛失に対する耐性も，まったくない．したがって，所持している人間が，正当な利用者であることの証明としての強度が限定的であるだけでなく，マトリクスコードを厳重に保管するよう利用者を教育しなければならない．ただし，容易に郵送が可能であるという利点はある．

以上の分析から，第2世代システムにおける多要素認証の対象アカウントの拡大に対応するには，日常的に利用する所持要素としてはソフトウェアTOTPトークン（以後，単にTOTPトークンと表記した場合は，ソフトウェアTOTPトークンを指す）が現実的な選択肢である．ただし，TOTPトークンの登録を含む各種手続きをオンラインで安全に実施するために，マトリクスコードを併用する．

3.4.2 各種手続きの設計

第1世代システムでは，パスワード初期化（復旧）やアカウント情報の交付については，大学窓口にて身分証を提示して職員に直接依頼する方式を想定しており，手続きのために大学キャンパスを訪問できるという強い前提を置いていた．第2世代システムでは，国際交流の活発化に対応するため，パスワード初期化やアカウント情報の交付などの各種手続きをオンラインで提供する方法を検討する．

[*11] 正当な利用者が意図して複製することは，TOTPトークンのコピー機能などを用いれば可能である．

（0）利用者は，初期化用メールアドレスを事前に登録する．登録用ウェブサイトは，TOTPトークンによる多要素認証を要する．
（1）利用者は，パスワード初期化を依頼するウェブサイト（認証を要しない）で，ユーザ名を入力する．
（2）システムから初期化用メールアドレスに，臨時パスワードを送付する．
（3）ユーザ名・臨時パスワード・マトリクスコードを使って認証できるウェブサイトで，新しいパスワードを設定する．
（4）システムから初期化用メールアドレスに，パスワードが初期化されたことを通知する．

図 8 パスワード初期化（復旧）手順
Fig. 8 Password recovery procedure.

最初に，パスワード初期化（復旧）手順を，**図 8** に示す．パスワードを初期化するときは，他の手続きとは異なり，記憶要素を利用することができないため，一時的に認証強度が低下することが多い．図8の手順は，記憶要素の代わりに事前に登録した初期化用メールアドレスを利用することによって，できるだけ認証強度を維持することを意図している．図8の手順に対する攻撃としては，初期化用メールアドレスの登録を上書きする，または，初期化用メールアドレス宛のメールを窃取する，という2通りの方法が考えられる．前者については，初期化用メールアドレスの登録時に多要素認証を要求することによって対策とする．後者については，本論文のシステムで可能な対策は多くない．ただし，利用者には，不審なパスワード初期化通知メールが届くため，少なくとも攻撃を検知する機会があるはずである．

次に，アカウント情報の交付手順について検討する．第2世代システムにおけるアカウント情報の交付とは，TOTPトークンをオンラインで登録するために必要な3つの認証要素（ユーザ名，パスワードおよびマトリクスコード）を交付することを指す．大学窓口でアカウント情報を交付する場合には，3つの認証要素を直接に書面で交付することができる．しかし，オンラインでアカウント情報を交付する場合は，管理者が初期化したパスワードを第3者に知られないように利用者に通知することが困難である．先に述べたとおり，第2世代システムでは，初期化用メールアドレスが登録されている利用者は，ユーザ名とマトリクスコードを用いて，自身でパスワードを初期化できる．したがって，管理者から利用者に対してユーザ名とマトリクスコードを交付した上で，管理者から利用者に対してパスワードを通知する代わりに，利用者から管理者に対して初期化用メールアドレスを通知することにより，アカウント情報の交付が完了したと見なすことができる．

大学キャンパスを物理的に訪問できない少人数の利用者

表 3 各種処理に必要な認証要素（+ は当該要素が必要であることを示す）
Table 3 Authentication devices required for each procedure.

	ユーザ名	パスワード（知識要素）	TOTP トークン（所持要素）	マトリクスコード（所持要素）	初期化用メールアドレス（所持要素）
TOTP トークン登録	+	+		+	
初期化用メールアドレス登録	+	+	+		
パスワード初期化（復旧）	+			+	+
Gmail, Classroom（学外ネットワークから接続）	+	+	+		
Gmail, Classroom（学内ネットワークから接続）	+	+			

（1）大学窓口から対象者に，マトリクスコードを郵送．
（2）対象者から大学窓口に，初期化用メールアドレスとして登録を希望するメールアドレスからメールする．
（3）大学窓口から手順（2）のメールアドレス宛に，テレビ会議の URL を通知．
（4）テレビ会議で，パスポートの提示をもって本人確認とする．本人確認後，大学窓口から対象者に，口頭でユーザ名を通知．
（5）本人確認後，大学窓口は，手順（2）のメールアドレスを初期化用メールアドレスとして設定．
（6）図 8 の手順により，対象者がパスワードを初期化する．

図 9 オンラインアカウント情報交付手順（案）
Fig. 9 Proposed procedure of on-line account activation.

に対するアカウント情報の交付手順案を，**図 9** に示す[*12]．アカウント情報の交付にあたっては，本人確認が必須である．国内の利用者に対しては，本人限定受取郵便を利用することが可能[*13]だが，国外の利用者に対しては，そのような配送方法の指定が利用できないため，なんらかの本人確認を手順に組み込む必要がある．図 9 の手順では，パスポートをテレビ会議で提示することによって，一応の本人確認と見なしている．しかし，テレビ会議では，簡易な偽造パスポートでも識別することは困難であるから，他の手段による本人確認と組み合わせる必要がある．図 9 の手順では，マトリクスコードは郵送，初期化用メールアドレスはメール，ユーザ名はテレビ会議というように，パスワード初期化に必要な 3 つの認証要素が，すべて異なる通信経路で送られている．そのため，攻撃者が，すべての認証要素を窃取することはかなり困難であると考えられる．ただし，テレビ会議の URL がメールにより通知されているため，URL が攻撃者に漏洩する可能性は否定できない．したがって，テレビ会議の実施時には不審な第 3 者が参加していないことを確認する必要がある．

表 3 に，各種手続きに必要な認証要素を示す．第 2 世代システムでは，ユーザ認証に関わる情報の修正手続きとして，TOTP トークンの登録，初期化用メールアドレスの登録，パスワード初期化の 3 つを想定している．これらの手続きはいずれも，多要素認証が必要となるように設計されている．3.4.1 項で述べたとおり，マトリクスコードは複製および紛失に対する耐性が低いため，日常的に利用することは困難な所持要素であるが，郵送が容易であるという利点がある．そのため，第 2 世代システムでは，ユーザ認証に関わる情報の修正手続きにのみマトリクスコードを利用し，日常的には TOTP トークンを利用するというように使い分けることによって，多要素認証と各種手続きのオンライン化を両立する．

[*12] 図 9 の手順案は，パスワード初期化手順（図 8）とは異なり，COVID-19 パンデミック時にはいまだ実施されておらず，検討段階だった．そのため，ここでは「手順」ではなく「手順案」としている．
[*13] 行政手続におけるオンラインによる本人確認の手法に関するガイドライン，https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf による．

4. 運用状況

4.1 本学キャンパス停電時の挙動

本学キャンパスは，受電設備の法定点検にともなって，毎年 1 回全面的に停電する．この停電によって，本学キャンパスが被災した状況をシミュレーションすることができる．

基幹通信システムにおいて，停電が契機となって発覚した障害件数の変化を**図 10** に示す．第 1 世代システムおよび第 2 世代システムの稼働直後（2014 年および 2019 年）は，構築時の設定ミスに起因する障害が発生している．上述のとおり，基幹通信システムは，本学キャンパスで動作しているシステムから独立して動作するように設計されているが，実際に構築してみると様々な設定ミスによって障害が発生している．このような障害は，人間がシステム設計・構築している以上は避けられない障害であって，計画的に障害を減らす対策が重要である．

4.2 ネットワーク障害時の回線切替

第 2 世代システムで導入したフレッツ光回線（3.3 節）の稼働状況は，以下のとおりである．災害によるネットワーク障害は発生していないものの，SINET ノードのメンテナンスやアクセス回線の工事によって，2019 年 6 月から 2021 年 5 月までに 6 回，SINET 回線からフレッツ光回線に切り替わった．ほとんどの場合で，設計どおりに回線切替が自動的に行われたが，ルータの OS アップグレードにともなう仕様変更によって回線復旧に失敗した事例もあった．4.1 節で述べたとおり，異常時の挙動を平常時に検証することが重要と考えられる．

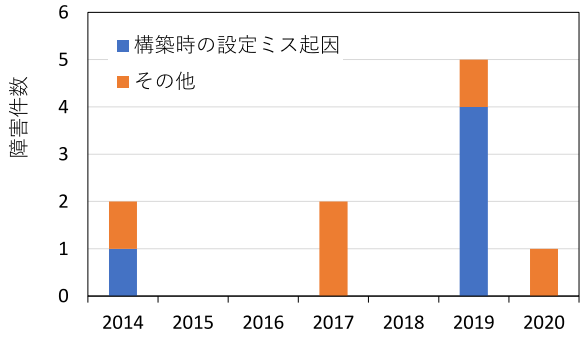


図 10 停電時に発生した障害件数

Fig. 10 Statistics of troubles occuring when electric power of our campus is out.

表 4 第 2 世代システムへの移行スケジュール

Table 4 Transition schedule from the first generation system to the second generation system.

2019 年 9 月	基本部分が稼働
10 月	全構成員の Google アカウントを作成
11 月	メールシステム移転開始
12 月	メールシステム移転完了
2020 年 3 月	パスワード初期化（復旧）サービス稼働
	遠隔地 DC を廃止
4 月	マトリクスコード送付

4.3 メールシステム移転にともなう TOTP トークン登録状況

第 1 世代システムから第 2 世代システムへの移行は，2019 年秋から 2020 年春にかけて段階的に実施した．**表 4** に，移行スケジュールの概要を示す．この節では，第 1 世代システムから第 2 世代システムへのメールシステムの移転状況について述べる．

第 2 世代システムでは，2019 年 11 月から 12 月にかけて，メールシステムを Gmail に移転した．筆者らは，2007 年から全学構成員を対象とするメールシステムを運用している [13]．過去のシステム更新（2010 年および 2013 年）では，SMTP や IMAP などの各種サーバのホスト名およびユーザ認証情報を維持したため，利用者側の設定変更は発生しなかった．しかし今回は，オンプレミスなメールシステムから Gmail への移転であり，利用者側の設定変更が避けられない．そのため，筆者ら（管理者）は，移転開始前に IMAP 経由ですべてのメールをコピーしたうえで，移転期間中は新旧両方のシステムにメールが配送されるように設定した．このように準備しておくことにより，利用者は，移転期間中であればいつでも，各自の都合の良い時期に，旧システムの利用を中止して，新システムの利用を開始できた．**図 11** に，メールシステム移転についての問合せ件数の推移を示す．移転期間中の問合せ件数の合計は 79 件であり，利用者の協力により，比較的順調に移転が行われたと思われる．

第 2 世代システムでは，多要素認証の対象を拡大するため，学外から Gmail を利用する場合，TOTP トークンを用いた多要素認証を必須とするように設定（表 3）した．2019 年 9 月から 2021 年 3 月までの TOTP トークンの登録件数を**図 12** に，登録率を**図 13** に，それぞれ示す．図 12 より，TOTP トークン登録の 1 回目のピークが，メールシステム移転時（2019 年 11〜12 月）に発生していることが分かる．メールシステムの移転完了までに TOTP トークンを登録した利用者の割合は，30%（868 人）であり，かなり小さい．この理由は，2 つ考えられる．第 1 に，学内から Gmail を利用する場合には，従来と同様に，ユーザ名・パスワード認証のみで利用できるように設定（表 3）しているため，学外からメールを参照しない利用者（メールを転送している利用者を含む）は，TOTP トークンの登録を

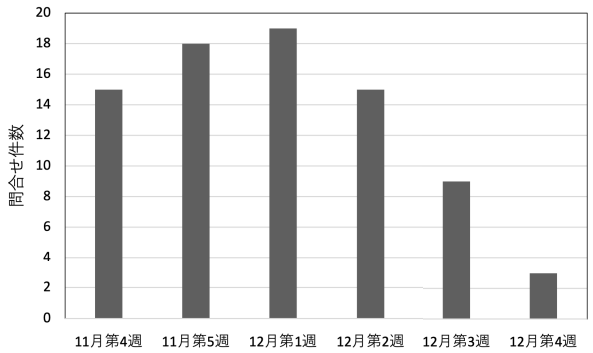


図 11 メールシステム移転問合せ件数

Fig. 11 Statistics of transition support of mail system.

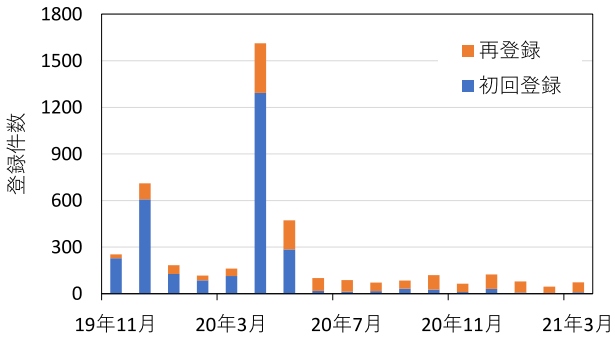


図 12 TOTP トークンの登録件数

Fig. 12 Statistics of registration of TOTP tokens.

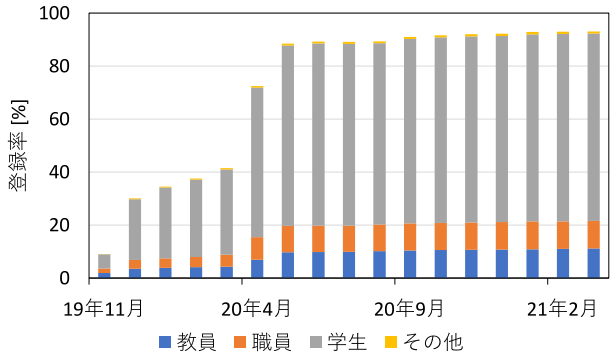


図 13 TOTP トークンの登録率（登録を完了している利用者の割合）

Fig. 13 Ratio of users using TOTP tokens.

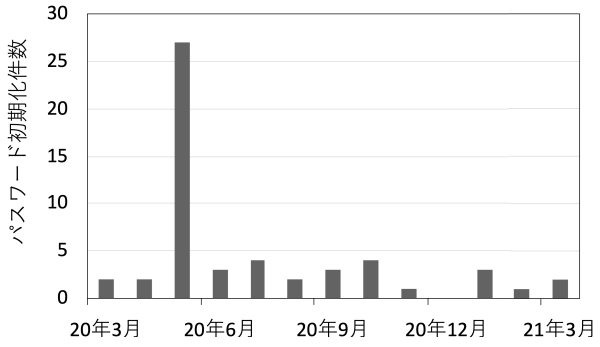


図 14 パスワード初期化（復旧）頻度
Fig. 14 Statistics of password recovery.

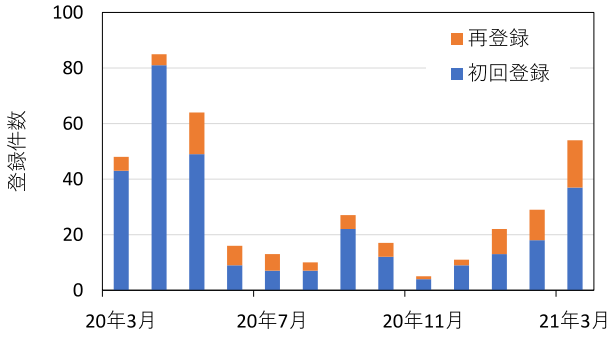


図 15 初期化用メールアドレスの登録件数
Fig. 15 Statistics of registration of e-mail addresses for password recovery.

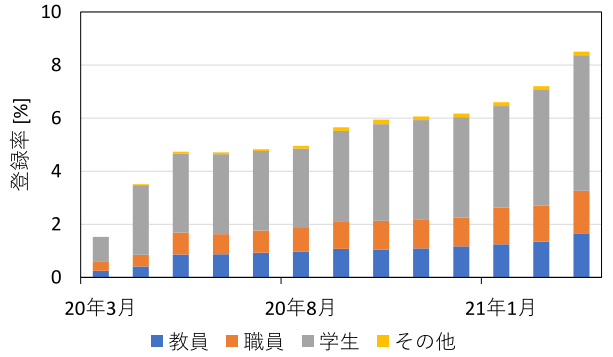


図 16 初期化用メールアドレスの登録率（登録を完了している利用者の割合）
Fig. 16 Ratio of users registering e-mail addresses for password recovery.

要しないからである．第 2 に，Thunderbird や Outlook などのメーラを使っている利用者の多くが，アプリケーション専用パスワード[*14]に基づいて認証する方式を選択したからである．また，図 13 より，TOTP トークンの登録時期について，利用者の種別による違いは見られない．

予算上の制約により，第 2 世代システムでは，利用者個人が所有する情報機器（主としてスマートフォン）に TOTP トークンをインストールする方式を選択している．そのため，利用者がスマートフォンを機種変更した際に適切に TOTP トークンの情報を移行しないと，TOTP トークンの再登録が発生する．図 12 より，TOTP トークン登録の 2 回目のピーク以後の期間（2020 年 6 月～2021 年 3 月）に，TOTP トークンの再登録が 680 件（平均 68 件/月）発生していることが分かる．よって，ソフトウェア TOTP トークンを採用した場合には，定常的に TOTP トークンの再登録が発生するため，再登録に対応できるように設計する必要がある．

4.4 パスワード初期化（復旧）の利用状況

メールシステムの移転完了後の 2020 年 3 月に，パスワード初期化（復旧）システムを稼働した．この節では，パスワード初期化の利用状況について述べる．

図 14 に，パスワード初期化の頻度を示す．2020 年 3 月から 2021 年 3 月までに行われたパスワード初期化は 54 件（平均 4.2 件/月）であり，1.9%の利用者がパスワード初期化を行っている．講義が開始した 2020 年 5 月のピークを除外しても 27 件（平均 2.2 件/月）であり，定常的にパスワード初期化が必要とされていることが分かる．記録が不完全であるため定量的な比較は困難だが，窓口で直接にパスワード初期化が依頼されていた回数と定性的に一致している．

図 15 に初期化用メールアドレスの登録件数，**図 16** に初期化用メールアドレスの登録率を示す．図 8 に示すとおり，パスワード初期化が実施されたことは初期化用メールアドレス宛に通知されるため，アカウントの安全を保つために初期化用メールアドレスの登録は重要である．しかし，2021 年 3 月時点で初期化用メールアドレスの登録率は 8.5%（240 人）に留まっており，改善を要する．2021 年度の新入生向けオリエンテーションにおいて，初期化用メールアドレスを登録するよう案内したところ，2021 年 5 月時点の登録率は 23%（657 人）に改善した．今後，在学生向けの案内を強化する予定である．

4.5 COVID-19 パンデミックに対する対応

COVID-19 パンデミックにともなって，本学では，2020 年 4 月に，2020 年度講義の開講延期および遠隔講義化，キャンパスへの立ち入り制限（ロックダウン）が決定された．この節では，COVID-19 パンデミックに対する対応状況，特にロックダウン状況における TOTP トークンの登録手順について述べる．

筆者らは，最初に遠隔講義の実施プラットフォーム（Learning Management Service; LMS）について検討し，Google Classroom[*15]（以下，Classroom と呼ぶ）を選定した．選定理由は，以下の 3 点である．第 1 に，Classroom は，Google 社によるテレビ会議システムやクラウドストレージサービスと結合されており，遠隔講義を実施するため

[*14] https://support.google.com/accounts/answer/6010255
[*15] https://classroom.google.com/

に必要な機能がひととおり揃っている．第2に，Classroomは，Google社のSaaS基盤上で動作しているため，負荷耐性が高いことが期待される．COVID-19パンデミックにともなう遠隔講義化は，従前の部分的な遠隔講義の実施とは異なり，実験などの例外的な科目を除くほとんど全科目を対象としており，負荷耐性はきわめて重要である．第3に，2019年10月に全構成員を対象としてGoogleアカウントを作成（表4）していたため，新たなシステム構築はほとんど必要ではなく，G Suiteの設定変更によってClassroomの利用を開始できる[*16]．Classroomの難点としては，本学教員はほとんど誰も使ったことがない新しいシステムであり，遠隔講義の準備と同時にClassroomの利用方法に習熟しなければならないという点がある．そのため，以前からLMSとしてMoodle[*17]を利用している教員に限って，Moodleの利用継続を認めることにした．

次に，TOTPトークンの登録方法について検討した．第2世代システムでは，学外からClassroomを利用する場合，TOTPトークンを用いた多要素認証を要求するよう設計している（表3）．図13より，2020年3月時点のTOTPトークン登録率は41%（1,172人）であるから，新入生だけでなく在学生についても，キャンパスがロックダウンされた状況でTOTPトークンを登録する方法が必要である．一時的に多要素認証を要求しないよう設定変更する案も検討したが，改めて認証強度を強化するときにTOTPトークンが未登録である利用者に対する対応が困難になることが予想されるため，多要素認証を要求する方針は維持する．本学キャンパスに来訪できない少人数の学生に対するアカウント情報の交付手順案（図9）は，テレビ会議を個別に実施する手順を含んでおり，多人数の学生を対象とする手順としては現実的ではない．この問題を解決するため，本人確認を簡略化した手順（**図17**）を設計した．図17の手順では，学生証のスキャン画像を添付したメールによって送信者の本人確認を行っている．したがって，図17の手順は，学生証を窃取または拾得した第3者がアカウントを乗っ取ることができる脆弱性があるが，パンデミック対応の限定された期間においては，許容し得るリスクであると考える．

2020年4月から，TOTPトークンの登録手順（図17）を，メールと郵送によって学生に周知した．図12より，TOTPトークン登録の2回目のピークが，ロックダウン状況に対応するために発生していることが分かる．TOTPトークンの登録率（図13）は，2020年3月時点の41%（1,172人）から，2020年5月時点では88%（2,577人）に達している．このように迅速にTOTPトークン登録を行えたことから，図17の手順は，おおむね現実的かつ効果的であったと考えられる．

*16 現実には，設定変更の影響の検討を含む膨大な業務が生じる．
*17 https://moodle.org/

（1）（新入生の場合）大学窓口から学生に，ユーザ名・パスワードをレターパックプラスで送付する．
（2）大学窓口から学生に，マトリクスコードを郵送する．
（3）学生は，ユーザ名・パスワード認証を試みる．
（4）失敗した場合は，パスワードの初期化（復旧）が必要なので，学生証のスキャン画像を添付したメールを大学窓口に送信．
（5）大学は，当該メールのメールアドレスを初期化用メールアドレスとして登録．
（6）学生は，図8の手順により，パスワードを初期化する．
（7）学生は，ユーザ名・パスワード・マトリクスコードを用いて，TOTPトークンを登録．

図17 COVID-19パンデミック時の学生向けTOTPトークン登録手順

Fig. 17 Emergency registration procedure of TOTP tokens for students on COVID-19 pandemic.

5. 結論

本論文では，大規模災害に対する事業継続性と，各種手続きのオンライン化に配慮した認証基盤システムの構築と運用について述べた．大規模災害に対する対策としては，基幹通信システムを学外DCに設置する方針を採用し，設計にあたって考慮すべき点と，キャンパスの停電を利用して計画的に品質を高める運用経験について述べた．また，TOTPトークンとマトリクスコードを組み合わせた各種手続きのオンライン化が，感染症によるロックダウン状況下における事業継続のために有効だったことを示した．

第2世代システムは2025年までの運用を予定しているため，筆者らは第3世代システムの設計を開始している．第2世代システムの問題点として，システムの複雑化によって設定ミスなどの各種トラブルが増加した点がある．これは，予算的な制約により本学キャンパスとSINETの接続回線の冗長化が困難だったため，Shibboleth IdPを本学キャンパスとMicrosoft Azureの2カ所に設置したことが主な原因である．その対策として，SINET6の導入に合わせて，岡崎（愛知）DCと浜松（静岡）DCの2カ所に接続先を冗長化することを検討している．この冗長化が実現されれば，2カ所にShibboleth IdPを設置する必要性が減少し，システムを簡素化できると考えられる．また，第2世代システムにおいて多要素認証の利用範囲を大幅に拡大したため，多くの利用者は，TOTPトークンの利用に習熟したと考えられる．したがって，第3世代システムでは，本学特有の設定をできるだけ縮小し，IDaaSの利用を検討する．

謝辞 豊橋技術科学大学情報メディア基盤センター技術スタッフの皆様による，本論文のシステムの構築および運用に対する大きな貢献に深く感謝します．

参考文献

[1] 松平拓也, 笠原禎也, 高田良宏, 東 昭孝, 二木 恵, 藤田翔也：金沢大学における統合認証基盤の現状と課題，大学 ICT 推進協議会 2013 年度年次大会論文集 (2013)（オンライン），入手先 ⟨https://axies.jp/_files/report/publications/papers/papers2013/axies_w3e-4.pdf⟩.

[2] 河野圭太，稗田 隆，中村素典：Shibboleth と OpenAM の連携による認証レベルを制御可能なシングルサインオン基盤の構築，学術情報処理研究，Vol.21, No.1, pp.71–81（オンライン），DOI: 10.24669/jacn.21.1_71 (2017).

[3] 浜元信州, 井田寿朗, 齋藤貴英, 小田切貴志, 綿貫明広, 横山重俊：複数クラウドを利用した 2 段階認証対応全学認証基盤の構築と運用，学術情報処理研究，Vol.24, No.1, pp.94–103（オンライン），DOI: 10.24669/jacn.24.1_94 (2020).

[4] 野口 宏, 大瀧保広, 鎌田 賢：BCP としての学内データセンターの設置とその活用方針, 学術情報処理研究, Vol.18, No.1, pp.24–32（オンライン）, DOI: 10.24669/jacn.18.1_24 (2014).

[5] 沖野浩二，金森浩治，黒田 卓：富山大学における BCP の検討，学術情報処理研究，Vol.17, No.1, pp.17–24（オンライン），DOI: 10.24669/jacn.17.1_17 (2013).

[6] 松浦健二，上田哲史，佐野雅彦，関 陽介，松村 健，八木香奈枝：徳島大学における情報システム BCP および非常時のワイヤレスアクセスラインの整備，学術情報処理研究，Vol.18, No.1, pp.99–107（オンライン），DOI: 10.24669/jacn.18.1_99 (2014).

[7] 野口 宏，大瀧保広，高橋幸雄，鎌田 賢：Office365 と Shibboleth の多要素認証対応 SSO 環境の構築，学術情報処理研究，Vol.20, No.1, pp.82–89（オンライン），DOI: 10.24669/jacn.20.1_82 (2016).

[8] 永井靖浩，古村隆明，針木 剛，西垣昌代：IC カードと電子証明書について 7 年間運用の考察と将来の選択肢，大学 ICT 推進協議会 2016 年度年次大会論文集 (2016)（オンライン），入手先 ⟨https://axies.jp/_files/report/publications/papers/papers2016/WD11.pdf⟩.

[9] 河原達也, 森 信介, 赤坂浩一：新しい汎用コンピュータシステムの概要, 京都大学学術情報メディアセンター全国共同利用版 [広報], Vol.12, No.1, pp.2–6 (2013)（オンライン），入手先 ⟨https://www.media.kyoto-u.ac.jp/accms_web/wp-content/uploads/2016/07/2013-1.pdf⟩.

[10] 秋山剛志：基幹サービスのデータセンターでの運用について, 大学 ICT 推進協議会 2011 年度年次大会論文集, pp.311–316 (2011)（オンライン），入手先 ⟨https://axies.jp/_files/report/publications/papers/papers2011/2011_D11-3.pdf⟩.

[11] 井上春樹，長谷川孝博，八巻直一，水野信也，峰野博史，松尾廣伸，山崎國弘，北川誠人，吉田仙良，岡田良介，堀 格人，秋元 勝，坂田智之，永田正樹，萩野勝哉，関睦実，岩本祥吾，川畠正也，塩崎雅基：進化するクラウド情報基盤，静岡学術出版 (2011).

[12] Chang, M.A., Tschaen, B., Benson, T. and Vanbever, L.: Chaos Monkey: Increasing SDN Reliability through Systematic Network Destruction, *Proc. 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM '15*, pp.371–372 (online), DOI: 10.1145/2785956.2790038 (2015).

[13] 土屋雅稔：認証基盤と連携したメールホスティング環境の構築，学術情報処理研究，No.13, pp.5–16（オンライン），DOI: 10.24669/jacn.13.1_5 (2009).

[14] 上田 浩，古村隆明，石井良和，外村孝一郎，植木徹：Office365 への移行と認証連携事例の評価，大学 ICT 推進協議会 2013 年度年次大会論文集 (2013)（オンライン），入手先 ⟨https://axies.jp/_files/report/publications/papers/papers2013/axies_w3e-6.pdf⟩.

[15] 土屋雅稔，中村純哉：豊橋技術科学大学における身分証の IC カード化，情報処理学会研究報告，Vol.2015-IOT-29, No.29, pp.1–6 (2015)（オンライン），入手先 ⟨http://id.nii.ac.jp/1001/00141881/⟩.

[16] 小野 悟，黒木謙信，谷 重喜：プラクティス連携による学内統合認証基盤の構築，学術情報処理研究，Vol.17, No.1, pp.25–32（オンライン）, DOI: 10.24669/jacn.17.1_25 (2013).

付 録

A.1 ソフトウェア構成

表 A·1 に，第 1 世代システム（2 章）および第 2 世代システム（3 章）の構成ソフトウェアの詳細を示す．入札の競争性を確保するため，筆者らは，機能要件と性能要件を仕様として指定し，構成ソフトウェアを仕様として明記することはできるだけ避けている．実際に，第 2 世代システムの調達にあたっては，複数社からの提案を受け付け，それぞれの構成ソフトウェアは大きく異なっていた．

A.2 第 2 世代システムの画面例

ここでは，第 2 世代システムの認証画面や登録画面の例を示す．はじめに，パスワード認証の画面を，**図 A·1** に示す．多要素認証を要求する操作では，パスワード認証を実施した後，**図 A·2** (a) に示す画面で認証方式を選択する．この画面において「ワンタイムパスワードアプリを使ってログイン」を選ぶと，図 A·2 (b) の画面で TOTP トークンの入力を要求される．

初期化用メールアドレスの登録では，多要素認証の後，**図 A·3** の画面が表示され，登録を希望するメールアドレスを入力する．

パスワード初期化の画面遷移を，**図 A·4** に示す．まず，パスワードが分からない利用者は，パスワード認証画面で，パスワードの初期化を選ぶ（図 A·4 (a)）．その後，利用者は自分のユーザ名を入力し（図 A·4 (b)），マトリクスコードのレスポンスを入力する（図 A·4 (c)）．マトリクスコード認証に成功すると，臨時パスワードが初期化用メールアドレスに送付される（図 A·4 (d), (e)）．利用者は通知メールに記載された臨時パスワードを入力し（図 A·4 (f)），新しいパスワードを入力する（図 A·4 (g)）．これでパスワード初期化は完了し，パスワードが初期化されたことが初期化用メールアドレスに通知される（図 A·4 (h)）．

TOTP トークン登録の画面遷移を，**図 A·5** に示す．利用者は，パスワード認証（図 A·1）およびマトリクスコード認証（図 A·4 (c)）によって，本人確認を行うと，図 A·5 (a) の画面が表示される．ここで表示された QR コードを，ソフトウェア TOTP トークンでスキャンすることにより，TOTP トークンが登録できる．登録完了後，TOTP トークンに表示される TOTP を入力することで，正しく TOTP トークンが登録できたことを確認する．確認が終了する

表 A·1 システム構成
Table A·1 System structure.

	調達方法	第 1 世代システム	第 2 世代システム
ID 管理システム	入札	EXGEN LDAP Manager 6 (single instance)	EXGEN LDAP Manager 6.9 (single instance)
LDAP サーバ		OpenLDAP 2.4.23 (active-active)	OpenLDAP 2.4.46 (active-active)
Shibboleth IdP		Shibboleth IdP 2 (active-active)	WisePoint Shibboleth 8 (active-active)
RADIUS		FreeRadius 2.1.12 (active-active)	FreeRadius 3.0.13 (active-active)
メールシステム		Postfix 2.6.6 + Dovecot 2.0.9 (active-active)	Gmail
権威 DNS	内製	ISC BIND 9.8.4 (active-active)	ISC BIND 9.11.5 (active-active)
公式ウェブサーバ		Apache 2.2.22 (single instance)	Apache 2.4.38 (single instance)
メール中継サーバ		—	Postfix 3.4.14 (active-active)

図 A·1 パスワード認証画面
Fig. A·1 Password authentication screen.

(a) 認証方式の選認
(a) Selection of authentication method

(b) TOTP 認証
(b) TOTP authentication.

図 A·2 多要素認証画面
Fig. A·2 Multi-factor authentication screen.

図 A·3 初期化用メールアドレス登録画面
Fig. A·3 Recovery address registration screen.

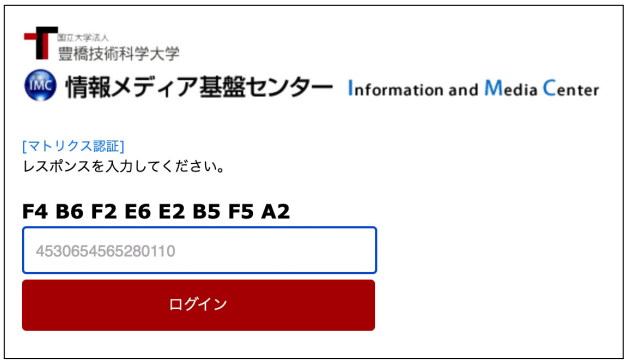
と，TOTP トークンの登録を通知するメールが，初期化用メールアドレスに送信される（図 A·5 (b)）．

(a) パスワード初期化の選択

(a) Selection of password recovery

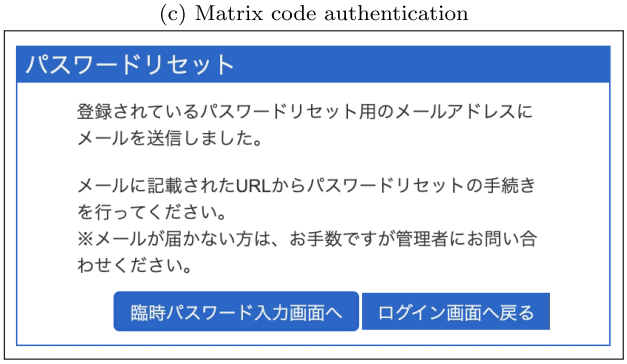
(b) ユーザ名の入力

(b) Input of username



(c) マトリクスコード認証

(c) Matrix code authentication

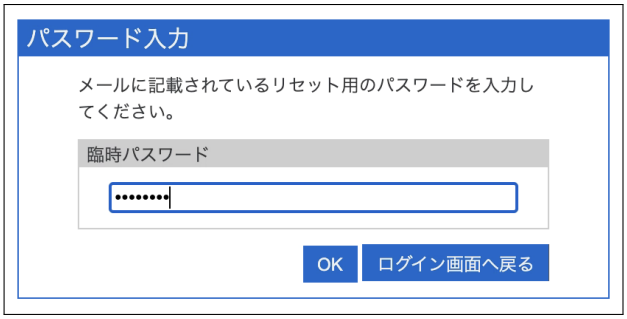


(d) 臨時パスワードのメール送付

(d) Delivery of temporary password.

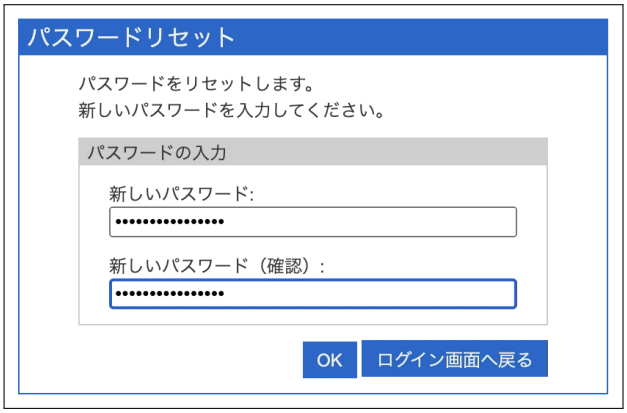
(e) 臨時パスワードの通知メール

(e) Notificatiion of temporary password.



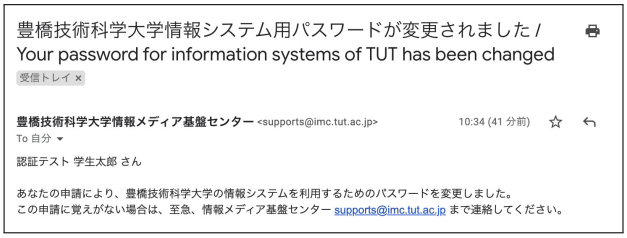
(f) 臨時パスワードの入力

(f) Input of temporary password.



(g) 新しいパスワードの入力

(g) Input of new passowrd.



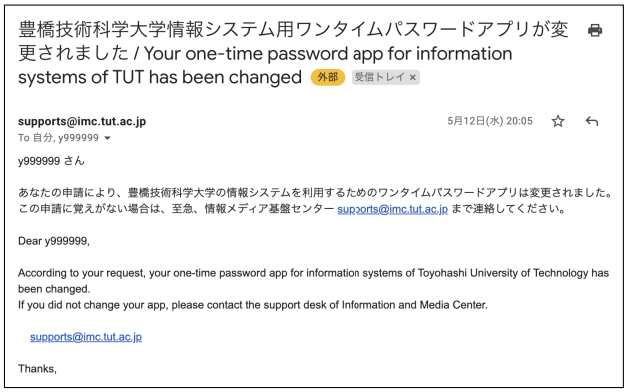
(h) パスワード初期化の通知メール

(h) Notification of password recovery.

図 A·4 パスワード初期化画面

Fig. A·4 Password recovery screen.

(a) TOTP トークンの登録
(a) Registration of TOTP token.



(b) TOTP トークン登録の通知メール
(b) Notification of TOTP token registration.

図 A·5 TOTP トークン登録画面
Fig. A·5 TOTP token registration screen.

土屋 雅稔 （正会員）

1998 年京都大学工学部卒業．2004 年同大学大学院情報学研究科博士課程単位認定退学．同年豊橋技術科学大学情報処理センター助手．2007 年同大学情報メディア基盤センター助教．2014 年同大学情報メディア基盤センター准教授．自然言語処理に関する研究に従事．博士（情報学）．言語処理学会，人工知能学会各会員．

中村 純哉 （正会員）

2006 年豊橋技術科学大学工学部知識情報工学課程卒業．2008 年同大学大学院工学研究科知識情報工学専攻修了．2014 年大阪大学大学院情報科学研究科コンピュータサイエンス専攻博士後期課程修了．同年豊橋技術科学大学情報メディア基盤センター特任助教．2017 年同大学助教．2021 年同大学准教授．分散アルゴリズム，分散システム，情報システムの研究に従事．博士（情報科学）．電子情報通信学会，IEEE，IEEE Computer Society 各会員．