

クラウドサービス導入とメールアカウント一括管理システムの構築

中川 卓也* 大向 雅人** 福田 豊*

Introduction of Cloud Service and a Mail-Account-lumping-Management System

Takuya NAKAGAWA, Masato OHMUKAI, Yutaka FUKUDA.

ABSTRACT

Since the Internet has been spread widely nowadays, it is inconvenient that e-mails cannot be checked from the outside. We report in this article that the introduction of cloud service and a mail-account-lumping –management system highly saved labor to maintain the system. Using cloud service enabled us to eliminate the mail server. The mail-account-management system realized the one time registration of the users for several servers. As a result, administrator’s burden was reduced substantially.

KEY WORDS: cloud service, Google Apps, introduction of a lumping-management system.

1. はじめに

明石高専のネットワークは事務用 LAN と研究用 LAN の 2 系統が敷かれている。事務用 LAN とは教職員の事務作業を行うためのネットワークで、教務や学生指導関係等の機密データを取り扱うため、学生や校外の者がアクセスできないネットワークとなっている。一方、研究用 LAN とは学生や教職員の学習・教育・研究活動等において校内外を問わず自由にアクセスすることができるネットワークとなっている。研究用 LAN の利用は主に学生であり、約 1000 人が利用している。また、現在のネットワークは VLAN (Virtual LAN : 単一のネットワークを複数に分割する技術) を導入しているため、これら 2 系統の LAN は論理的に分かれており、相互通信ができない構成となっている。

ネットワーク全体の維持管理においては、人員の都合により極力メンテナンスが不要かつセキュアであることが求められている¹⁾。事務用 LAN では教職員のアカウント管理やメールサービス等に加え、論理的に他

と独立しているネットワーク状態 (学生や校外者等がアクセスできない状態) の維持管理を行なっている。その一方で、研究用 LAN では利用者のアカウント管理やメールサービス・ファイルサーバの提供 (主に学生向け)、及び情報センター演習室における端末機器の管理 (OS やインストールソフトのライセンス管理等も含む) を行っており、より少ない人数で管理できれば都合が良い。

そのような状況下においてサーバ群を自前で構築し管理運営を行った場合、サーバ群の管理やメンテナンス等の保守も行わなければならない。そのため、管理者には専門知識と高度なスキルが要求され、少人数で管理を行うにはかなりの負担となる。それに加えて、学内にメールサーバを構築しているため、メールチェックを行うには学内研究用 LAN に接続された PC からメールチェックを行う必要があった。つまり、明石高専のユーザが学外からメール送受信できなかった。インターネットが普及してきた近年において、学内からしかメールチェックができないのは大きなデメリットである。そこで、研究用 LAN のサーバ群の一部に

*技術教育支援センター、**電気情報工学科

関してはリース契約を行い、基本的なメンテナンス等もリース契約に加えるなど、管理者にかかる負担の軽減を行った。さらに、近年注目されている Web メールサービスが含まれるクラウドサービスを導入することにより、メールサーバを廃止して管理サーバ台数を最小限にすることができた。その結果、管理者のさらなる負担軽減となっただけでなく、最終的にはコスト削減をも行うことができた。本論文において、導入したクラウドサービスとその効果について詳述する。

2. クラウドサービス導入前の認証システム

クラウドサービス導入前（以下、旧研究用 LAN と呼ぶ）の認証システムのイメージを図 1 に示す。図 1 より、旧研究用 LAN を最初に利用するためには、下記の手順を踏む。

- ①旧研究用 LAN 管理者がユーザ情報管理ソフト（以下、LDAP Account Manager と呼ぶ）に利用者情報の登録（ID やパスワード等）を行う
- ②LDAP Account Manager に登録された利用者情報が LDAP サーバに登録される
- ③LDAP サーバに登録されている利用者情報を Message Transfer Agent（以下、MTA と呼ぶ。通常はメールサーバと呼ばれる）が参照してメールの送受信を行う
- ④利用者は学内研究用 LAN 及びメールサーバが利用可能となる

上記、手順①～④を行うと、利用者は学内に設置された PC から認証を行うことができるようになり、ID とパスワードを入力すると LAN を自由に利用（以下、ユーザ認証と呼ぶ）することができる。

旧研究用 LAN においては、演習室等端末を利用する機会が多く、管理が行き届かない端末が接続されるため、プロキシサーバを介して自由にユーザ認証を行う構成であった。しかし、MTA が学内にあり、新着メールを確認するためには必ず学内 PC から確認しなければならないと、明石高専のユーザが学外からメール送受信できないといった問題点が残った。

3. 検討事案

1 章でも述べたように、明石高専においては少人数体制で管理・運営を行っているため、管理者にかかる負担を軽減する必要があることは最優先事項である。それに加えて、ネットワークの利便性が向上している近年において、学外から研究用 LAN のメールが確認できるようにすることが必要になってきた。この 2 点を念頭におき新しいネットワーク構築の検討を行った。

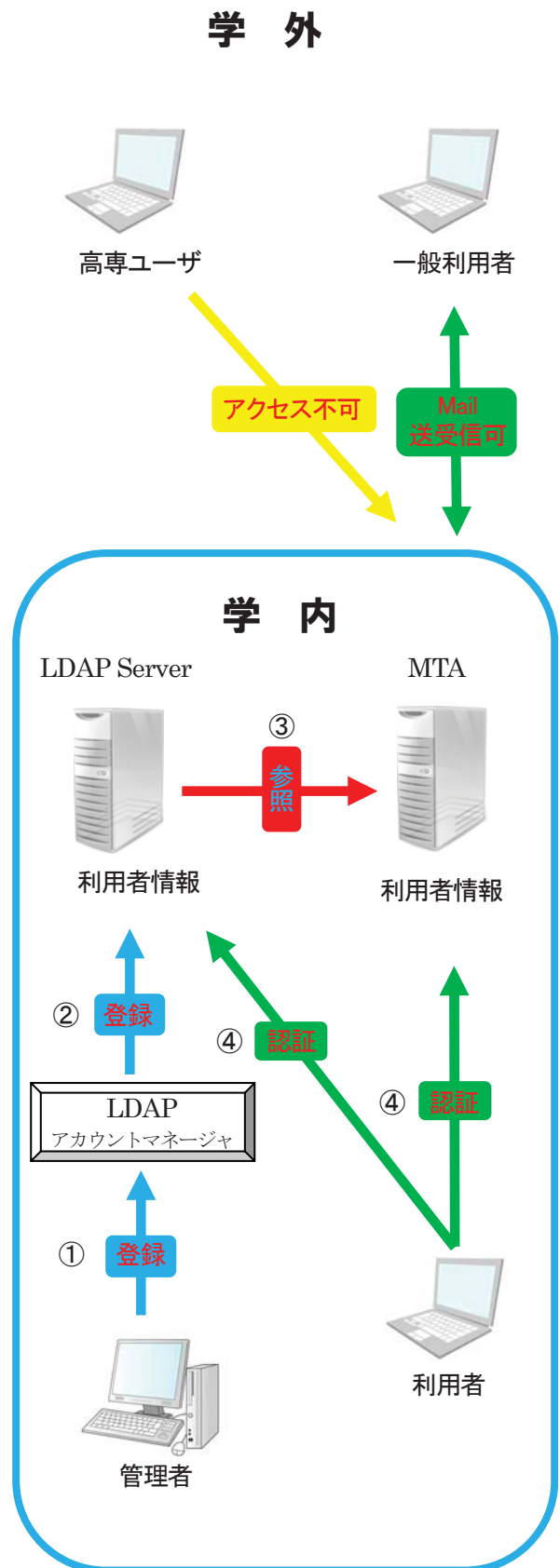


図 1 旧研究用 LAN サーバの認証システムイメージ

3・1 メールサーバをDMZ領域におく

DMZ (demilitarized zone: 非武装地帯) 領域とは、組織の内部ネットワークと危険の多い外部ネットワーク (一般的にインターネットと呼ばれる) との間に設置されている隔離されたネットワーク領域のことをいう。DMZ 領域の特徴は、内部ネットワークと外部ネットワークから DMZ 領域に接続することを許容しながらも、DMZ 領域からは外部ネットワークだけに接続を許容している点にある。つまり、DMZ 領域内からは内部ネットワークに接続することができない。言い換えると、何者かが DMZ 領域に侵入したとしても、内部ネットワークを保護しながら外部ネットワークに対してサービスの提供を可能にする。すなわち、DMZ 領域は侵入者にとって袋小路として機能することになる。DMZ 領域にメールサーバを置いたときのイメージを図 2 に示す。

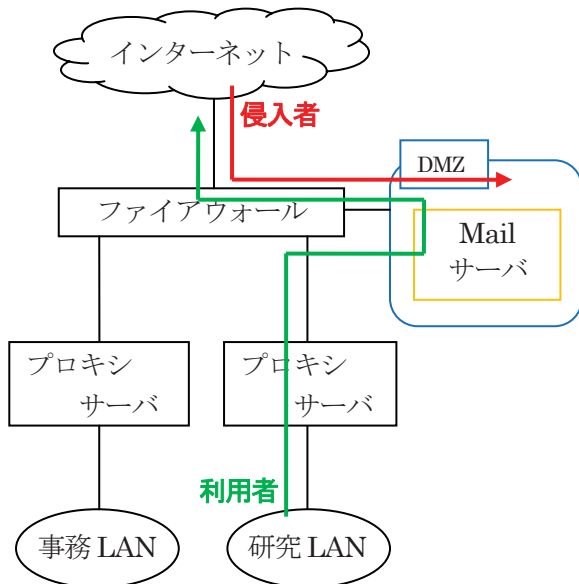


図 2 DMZ 領域にメールサーバを置いたときのイメージ図

この DMZ 領域にメールサーバを置くことで、学内からはもちろん、学外からのメールチェックも可能となる。この場合、DMZ ホスティング機能を利用して外部からのアクセスに対して、メールサーバのセキュリティを確保している。セキュリティを確保しているとはいえ、完全に被害をなくすことができることを保証するものではなく、被害を最小限に止めるための機能であるため、どうしても外部からの攻撃にさらされるリスクは完全に除去できない。また、学内にメールサーバを設置するため、管理者の負担等は今までと変わら

ないままになってしまう。

3・2 Active Mail (Web メール) の導入

研究用 LAN において Active Mail 導入の検討をおこなった。まず、Active Mail 導入のメリットを示す。

- Active Mail は Web メールであるため、インターネットができる環境であれば学内、学外を問わずメールが確認できること

次に、Active Mail 導入のデメリットを示す。

- Active Mail のライセンスを購入する必要があること
- Active Mail を導入するためには、専用のサーバを用意する必要があること
- Active Mail は利用ユーザ数によって価格 (ライセンス維持費) が変わるため、利用者約 1000 人分のライセンス維持費が発生し、かなり高額になってしまうこと
- Active Mail はブラウザ (特にインターネットエクスプローラ) がバージョンアップすると、表示がおかしくなるという問題が生じることがあった。なので、ブラウザの修正パッチが配布されるまでの期間、表示がおかしいまま使うか、古いバージョンのブラウザを使わなければならない状況を強いられること

また、DMZ の場合と同様、サーバを学内に設置するため、管理者の負担等は今までと変わらないままになってしまう。

3・3 Google Apps (クラウドサービス) の導入

Google Apps (クラウドサービス) とは Google 社が提供しているオンラインアプリケーションサービスで、Gmail (Web メール) やカレンダー、ドキュメント (Web ドライブ) 等のクラウドサービスの総称である。そのため、インターネットができる環境であれば学内・学外を問わずサーバへのアクセスが可能となる。また、運用サーバは Google が管理・運営を行うため、本校の管理者が管理する必要がなくなる。さらに、学内の管理サーバが不要となるため、コスト削減にもつながるといったメリットがある。

ただし、何か問題が生じた場合には“アメリカ合衆国カリフォルニア州の法律が適用²⁾”されるので、日本にとって重要な情報を他国法律下の元におくことに不安が残る。こういった不安は、企業の重要な情報や国家機密相当の情報にかかわらない限り“そのような可能性がある”ことを把握していれば良いと思われる。また、メールというシステム自体が、なりすまし (発信者の身元を偽ること) やウイルスの感染原因になるなどセキュリティ面での脆弱性を

併せ持つため、それほど重要視するものではないと考えられる。

3・4 検討事案のまとめ

上記の検討案を考慮した結果、人的な体制や対費用的効果を考えると、Google Apps (クラウドサービス) の導入が最も使用に耐え、効果的であるという結論に至り、導入を行うこととなった。

4. クラウドサービス導入後の認証システム

クラウドサービス導入後 (以下、新研究用 LAN と呼ぶ) は Web 認証システムを導入した。Web 認証システムとは校内ネットワークを利用するためのユーザ認証システムである。また、メールシステムは Google Apps の導入を行った。Google Apps を導入するにあたり、ユーザ管理ソフト (以下、Unicorn ID Manager と呼ぶ) の導入と Google Apps を導入するための支援設定 (メールアカウントを *****@s.akashi.ac.jp とする設定等) のシステム構築を行った。

4・1 新研究用 LAN を利用するために

新研究 LAN のサーバシステムのイメージを図4に示す。図4より、新研究用 LAN を最初に利用するためには、下記の手順を踏む。

- ①管理者が Unicorn ID Manager に利用者情報 (ID やパスワード等) の登録を行う
- ②Unicorn ID Manager に登録された利用者情報が LDAP サーバと Google Apps に登録される。利用者は新研究用 LAN 及び Google Apps が利用可能となる
- ③学内に設置された PC から Web 認証を行うことができるようになる。利用者は ID とパスワードを入力すると新研究用 LAN、及び Google Apps を利用することができる
- ④学外からも Google Apps を利用することができる
上記、手順①～④を行うと、Web 認証が行えるようになり、学外からもメールチェックができるようになる。

4・2 Unicorn ID Manager について

Unicorn ID Manager とは、複数のシステムで管理していた利用者情報等をブラウザ上で一括集中管理するためのソフトである。つまり、管理者はブラウザ上から利用者情報を一括して登録・変更・削除することができるようになり、シンプルな管理・運用を行うことが可能となった。そのため、Unicorn ID Manager を導入したことにより、利用者情報に関する管理業務の効率化を図ることができるようになった。

4・3 Google Apps 導入の利点

Google Apps はクラウドサービスであるため、利用者は学内・学外を問わずメールが利用できるようになり、利便性の向上が図られた。それに加えて、学内にサーバを必要としないため、運用サーバを削減することができた。その結果、管理者の運用負担を軽減するだけでなく、サーバ導入に伴うコストの削減につながった。

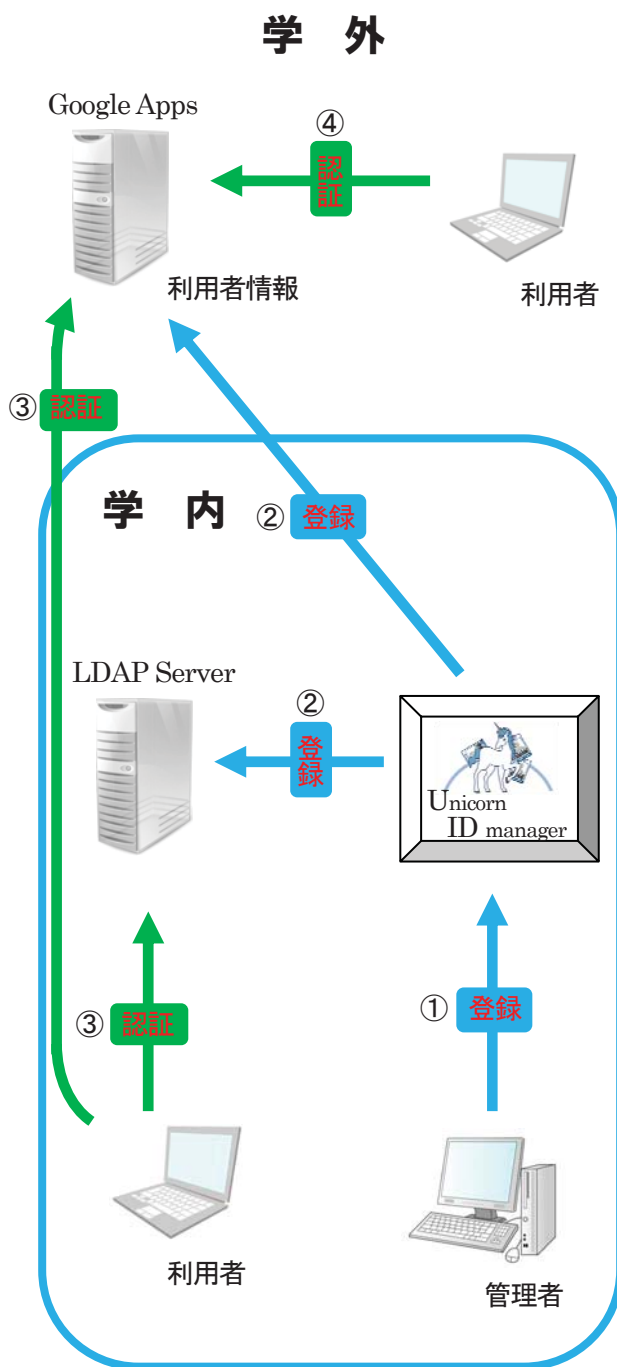


図4 新研究用 LAN サーバ認証システムのイメージ

新研究用 LAN の認証システムでは Google Apps を導入したことにより、個々の利用者が学内アカウントの Web 認証と Google Apps (Gmail アカウント) のパスワード変更が同時にできるようになりセキュリティ面の向上につながった。ただし、Web 認証と Google Apps (Gmail アカウント) のパスワードを同時変更が可能なのは学内から変更した時に限定される。

5. クラウド導入による付加サービスの提供

Google Apps を導入するにあたり、明石高専においては、在校生だけでなく卒業生に対してもサービスの提供を行っている。サービスを提供するにあたり、在校生のメールアドレスを*****@s.akashi.ac.jp、卒業生のメールアドレスを*****@ob.akashi.ac.jp としている。明石高専を卒業後にアドレス変更や廃止する事のないメールアドレス（以下、生涯メールシステムと呼ぶ）を提供することによって、同窓会やクラブ OB 会等の連絡ができるというだけでなく、卒業生同志のつながりに結びつく等、卒業後における人と人とのつながりの活性化に結びつくと考えられ、十分な価値があると考えられる。

また、先にも述べたように、Google Apps はクラウドサービスで、導入時には利用者一人につき 5GB までのファイルを Web ドライブに保管できるサービスを提供していた（2014 年 10 月以降は容量が無制限と変更されている）。しかし、Web ドライブを利用するにあたり、不正利用するといった問題を想定しておく必要がある。不正利用とは、音楽ファイルや画像ファイルといった著作権問題を含んだファイル等を無断で保管するといった場合が想定される。仮に、在学生がそのような行為を行った場合、サービスの一時停止といったペナルティを課すなど直接指導を行うことができるが、卒業生の場合はそういったことができない。そのため、卒業生に対しては Web ドライブの利用ができないよう機能制限を行って対応している。

6. Google Apps 利用率

2015 年 5 月 15 日における Google Apps (クラウドサービス) 全体の利用者割合に関するグラフを図 6 に示す。図 6 より、全体としては 85% が Google Apps を利用している。

次に、学年別の Google Apps 利用者割合を図 7 に示す。本科 1~3 年生と専攻科 1・2 年生は入学時より Google Apps の利用者である。また、授業における利用頻度（連絡や課題等の提出等での利用）が高いということもあり、利用率は高くなっている。

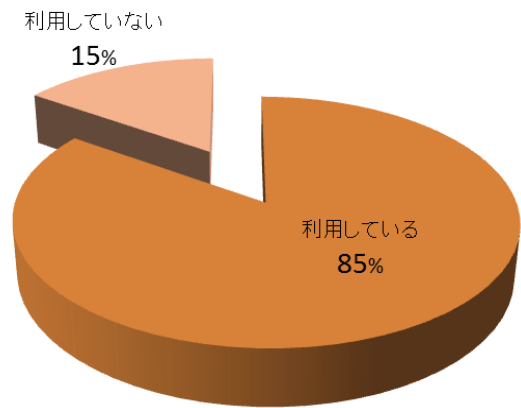


図 6 全体の利用者割合

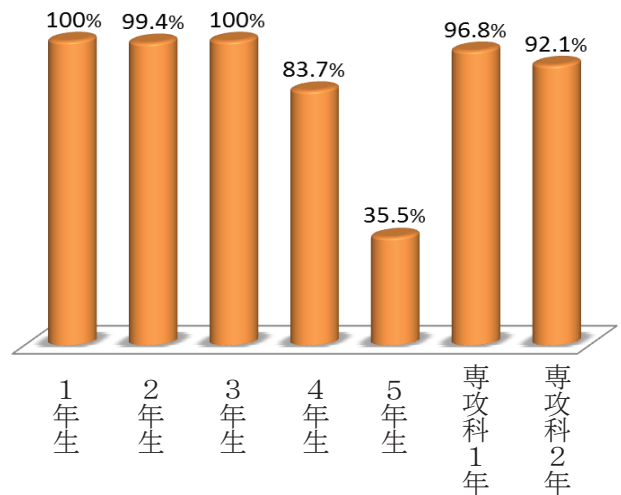


図 7 学年別 Google Apps 利用者割合

図 7 より、本科 2 年生と専攻科 1・2 年生の利用率が若干低くなっている。これは、本科 2 年生には転科生がおり、新年度の授業ではまだ利用していないこと。また、専攻科 1・2 年生には休学している学生がおり、利用していないことが原因となっている。

また、本科 4・5 年生の利用者割合が少ないことがわかる。これは、本科 4・5 年生は旧研究用 LAN のメールシステムから新研究用 LAN の Google Apps ヘシステム移行した過渡期であることが原因であると考えられる。なぜなら、旧研究用 LAN のメールシステムは学外からメール確認できなかったため、Google Apps 導入する以前から個人的にフリーメール (Gmail や Yahoo mail 等) を取得・利用している学生が多かった。そのため、Google Apps 導入後も授業における利用頻

度が少なく、Google Apps を利用するメリットがあまりなかったため、Google Apps ではなく以前に取得したフリーメールを使っている学生が多いためだと思われる。

以上より、過渡期の利用者がいることを踏まえると、利用率はかなり高く、導入したメリットは大きいといえる。

7. まとめ

これまでのことをまとめると、Google Apps (クラウドサービス) を導入したことにより、

- Web メールが利用できるようになり、インターネットができる環境であれば学内・学外を問わず新着メールの確認ができるため、利便性が向上した
- Web ドライブの利用サービスが提供されており、利用者の利便性が向上した
- 運用サーバを削減することができ、サーバの導入費用や運用・保守費を削減する等、コスト削減につながった
- 利用者は、学内の Web 認証 (学内アカウント) のパスワード、及び、メールアカウント (Gmail アカウント) のパスワードが同時に変更できるようになり、セキュリティ面の向上につながった
- 在校生に対しては*****@s.akashi.ac.jp を、卒業生に対しては*****@ob.akashi.ac.jp のアカウントサービスの提供を行っている
- 卒業生に対し『生涯メールシステム』を提供することによって、卒業後の人と人とのつながりに結びつき、今後の明石高専の活性化につながると考えられる
- Web ドライブの利用については、不正利用防止の

観点から在校生のみ利用可とし、卒業生に対しては機能制限を行っている。

・過渡期の利用者も含めて利用者割合は 85% と高く、Google Apps を導入したメリットは大きいということがいえる。

次に、Unicorn ID manager を導入したことにより、
・管理者は、利用者の一括登録・変更・削除ができるようになり、運用負担を大幅に軽減できた

ということがいえる。

今後の課題としては、

・2015 年 4 月に Google Apps の認証に関する API において仕様変更が行われたため、Unicorn ID Manager 及び Google Apps 連携ツールの修正を余儀なく行った。そのため、プログラム修正を行うにあたり、メンテナンス費用が発生した。今後において、そのような事例が起こる可能性があること

・Google Apps のサービス提供がいつまで続くのか?

・Google Apps のサービス提供が終了した際、現システムからの移行にともなって混乱が生じる
という問題点が考えられるが、技術革新の目覚ましい昨今において、今以上により良いサービスが提供されていることが考えられる。

参考文献

- 1) 新井イスマイル, 福嶋 徹, 井谷武史, 中川卓也, 福田 豊, 佐村敏治, 渡部守義, 堤 保雄: “汎用端末での利用者認証を可能としたセキュアな教育支援用ネットワークの構築”, 論文集「高専教育」, 第 37 号, pp. 489-494 (2014).
- 2) <https://www.google.com/intl/ja/policies/terms/> 抜粋