

教職員グループウェアと全学メールのG Suite移行について

総合生存学館情報セキュリティ幹事趙亮

2018年10月16日(2019年5月22日、公開のため微修正)

本学は、いままで学内運用だった教職員グループウェアと全学メール(KUMail)をGoogle Suite for Education(以下G Suite)に移行しようとしている([1, 2])。グループウェアの移行は12月頃、メールの移行は、11月から来年の8月までの予定とされている(図1)。

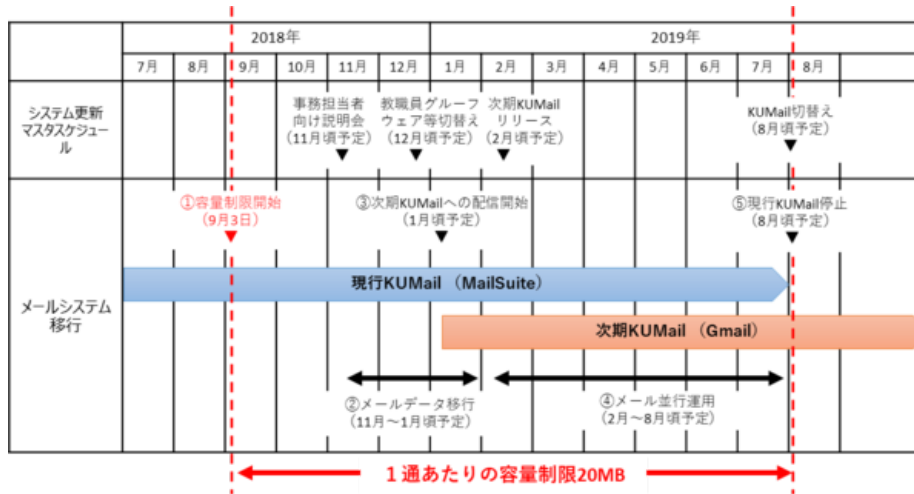


図1 グループウェアとメールシステムの移行スケジュール(出所:[3])

この移行は、情報セキュリティ基本モデルの大転換であり、本学や教職員に大きな影響を与える極めて重大な案件と考える。それに関わらず、学内の検討は不十分のように思われる。実際、この移行は、「京都大学クラウドサービス利用ガイド第2版」(2018年4月)p6に掲載される勧告(下記)と逆行する。

“「とても重要なサービス」はオンプレミス^{*1}での提供を継続する方が得策であろう”

情報セキュリティでは、利便性と安全性のトレードオフを考えるリスク管理が必要と言われる。そのため、重要なサービス、例えばKUINSのネットワークインフラは、対象を複数のレベルに分け、それぞれに見合う体制で管理するのが基本である^{*2}。今回の移行は、利便性もリスクも低い学内運用のレベルから利便性もリスクも高い外国の一営利企業の運用に切り替えることであり、KUINS IIIをやめて情報機器をすべてKUINS IIに晒すことに匹敵する大転換とぼくは考える。

重要情報が載らない前提での経営的判断だそうだが、本学の死活に関わるほど重要なインフラに投資しなくてはならない。グループウェアに上がっている情報で重要でないもの(公開されてもよいもの)はどれくらいあるか。自分のメールが重要でない(公開されてもよい)と思う教職員は何人いるか。諺「ただより高いもの

^{*1} オンプレミスとは、自社運用(型)とも訳され、情報システムのハードウェアを使用者(通常は企業)が自社保有物件やデータセンター等の設備内に設置・導入し、それらのリソースを主体的に管理する運用形態をいう(<https://ja.wikipedia.org/wiki/オンプレミス>より引用)。Google Suite for Educationのようなパブリッククラウドサービスと逆の運用形態である。

^{*2} 本学の情報ネットワークは、KUINS IIとKUINS IIIに分けられており、異なる体制で管理されている([4])。KUINS IIIは、直接外部からアクセスできないプライベートネットワークになっており、KUINS IIに比べ、利便性がそよくないが、その代わりに、外部からの直接攻撃を心配する必要がなく、管理にそれほど神経を使わなくても大きな問題になる可能性が低い。KUINS IIとIII、この2レベルの構成が本学情報ネットワークインフラの基本モデルであり、そのおかげで、KUINS IIIにつながっている情報機器の管理体制は(KUINS IIの機器より)甘くなっているが、大きな案件があまりなく、利用者も管理者も満足している。もしKUINS IIIをやめてすべての情報機器をKUINS IIに晒すと、とんでもないことになってしまうのであろう。

はない (there is no such thing than a free lunch)」があるように、安くて便利なサービスを手に入れることには、その代わりに我々が失いかねないものの対価を評価せねばならない。この文書は、すでに盛んに宣伝されてきた移行のメリットを省略し、あまり周知されていないリスクを自分なりに分析してみる。専門家でもないので不十分あるいは間違いもあるかもしれないが、本学情報セキュリティの向上を願って皆さん議論の材料となれば幸いである。

懸念1 本学のデータが本学の手の届かないところに行ってしまうこと。

グループウェアと全学メールに重要情報がないという前提は現実でない。いままで公開されては困るような情報がたくさん載ってきたが、インフラとして学内に閉じているから漏洩等のリスクが低い。そうして慣れてきた教職員に対して今後重要でない (公開されてもよい) 情報だけ載せて送るようにしろと言っても達成できるとは思えない。まず重要かどうかの判断は、普通の人では判断できないことが多い。一見重要でなさそうな情報でも、一定の条件 (例えば量) が揃えば重要な情報になり得る^{*3}仮に本当に重要でない情報のみ載ることができても、重要な情報はどうやって送るか？

ここで大事なのは、Google が信用できる会社かどうかではなく、我々は自分の手で自分たちのデータをコントロールできなくなることである。デジタルのデータだから、複製されても、どう利用 (悪用、流出) されても我々では分からないのである。研究の新しいアイデアをメールで意見交換することもあるだろう。移行したら、流出されて他人のノーベル賞に繋がることだってありえる。しかも、我々ではわかりやしない。

懸念2 新たなリスクに晒される。

よくある誤解は、メールはハガキみたいなものだから移行してもリスクが変わらない。確かに (暗号化されていない) メールはハガキみたいなものである。しかし、ハガキでも、学内便のハガキと、アメリカに行って返ってくるハガキと、漏洩リスクの違いが明らかであろう。教職員の間には送られるメールは、いままでは学内便であったが、移行したらアメリカや知らないところにある Google のサーバに行って返ってくることになる。

もうひとつよくある誤解は、あの Google だから情報セキュリティ万全であろう。確かに Google は、おそらくほかの IT 会社より高い技術力を持っているだろう。しかしよく考えて下さい。それだから危ない事情がある。Google を狙っているのは、世界最強レベルのハッカー (クラッカー) はもちろん、犯罪組織やテロリスト、政府機関などもある。Yahoo! や Facebook でも、クラッキングされて数千万や1億人以上の情報漏洩を許した。Google も、約半年前に約 50 万人の情報漏洩事件を起こした。プログラムのバグによるだそうだが、報道されるまで半年も隠したという不誠実な対応が世間から批判を浴びている ([5])。本学のデータは、学内運用ならそこまで狙われることもないが、Google に渡すと、攻撃される可能性が確実に増えるのだが、安全になるとまったく言い切れない。しかも本学はそれを把握できないし、調べることもできない。

懸念3 過剰にデータが収集される。

安くて便利なサービスを提供する代わりに Google が得ようしているものを見極め、提供してよいものか、よいなら損害の起きる確率及び損害額など、移行の前に検討せねばならない。懸念1で示した本学のデータのほか、さらに我々が収集されてもよいと同意せねばならない^{*4}情報のリストを示す (参考資料 [8] より引用)。

表 1: Google に収集されてもいいと同意せねばならない情報 ([8])

	情報	収集方法	メール機能との関係
1	氏名、メールアドレス、パスワード	大学提供	必要

^{*3} いわゆるビッグデータ分析。いうまでもないが、Google 等の IT 巨大企業は、営利企業である以上、ビッグデータを集め自社の利益を上げる宿命である。それに乗ることは、は対等な Win-Win 関係ではない。

^{*4} 4-8 に関しては、Google の使用条件では「収集することがある」となっている。

2	予備のメールアドレス, 電話番号, 住所	大学提供	提供すべきでない
3	電話番号, 写真, その他の情報	利用者提供	必要ないが, 利用者選択可
4	端末情報*5	Google 次第	必要ない
5	ログ情報*6	Google 次第	必要ないが, 提供してもよい
6	位置情報*7	Google 次第	必要ない
7	固有のアプリケーション番号*8	Google 次第	必要ない
8	ブラウザまたは端末に関する情報*9	Google 収集	必要ない

表 1 から分るように, 全学メールの機能に必要な情報がたくさん入っている。とりわけ, 電話番号 (2, 3, 4) や住所 (2), 位置情報 (6) 等の収集は, メール機能にして過剰 (いままでの KUMail では使用されていない) で, ユーザトラッキングに役立つ情報こそ Google が入手しようとしているもの *10 であることを示す。

Google に渡った情報がどのように使われるかは, Google 次第である。本学には信用する以外選択肢ない。Google が信用できるとしても, Google の数百のパートナー社も同様に信用していいか (Facebook とケンブリッジ・アナリティカの事件が記憶に新しい)。そもそも Google がいつまで信用していいか, だれも分からない。利用をやめようと思っても渡した (収集された) データの回収は我々にはできない。

懸念 4 法的問題

Google のサービスを利用するためには, Google のポリシーや規約に同意せねばならない。本学の教職員が位置情報等 (表 1 参照) を Google に提供する義務はないと思われるので, サービス導入に当たり, Google の利用規約 [7] 2.4 節で示すように, 各教職員にリスクの説明と同意確認が必要であろう。

また, メール扱いについて, 教職員が海外の A 国で全学メールを利用したとしよう。A 国は, 自国内にある Google のサーバーを利用したため Google に対してメールの開示を強制できるか, Google の資料を読む限りでは分からなくて, 法律専門家による説明がほしい。ほかに法的問題がないかも検討してもらいたい。

懸念 5 可用性の懸念

本学の教職員が中国に行かれることが相当あると思われるが, 中国では Google のサービスが利用できない。従って移行後の全学メール等が使えない (現在学内運用の KUMail は使える)。おまけに VPN もブロックされているのでやるようがない。ほかに Google のサービスが使えない国・地域もあるかもしれないし, 今後アメリカの世界戦略によって増えるかもしれない。

結論とアクション

重要な情報インフラは, 予算と人員を割当て自前で運用しなければならない ([6, 10]) と言っておきながら本学が逆のことをしようとしている。Google に限らず, 外のクラウドに移行することは, リスクが大変高く, 万が一情報漏洩が起きた場合の損失額を考えると, いま投資するほうが安く済む。Google サービスへの移行を中止し学内運用で賄うよう, 再考を切に願っている。

参考文献

- [1] 情報環境機構広報誌「info! 第 13 号」, <http://www.iimc.kyoto-u.ac.jp/whatsnew/information/info13.pdf>, 2018 年 9 月 1 日アクセス。

*10 ITmedia News, Google, 「位置情報オフにしてもユーザーを追跡」報道後、サポートページをひっそり更新, <http://www.itmedia.co.jp/news/articles/1808/17/news062.html>, 2018 年 9 月 3 日アクセス。

- [2] 次期教職員グループウェア・教職員用メール (KUMail) についてのお知らせ ,http://www.iimc.kyoto-u.ac.jp/ja/services/portal/member/ku_internal/newgw.html, 2018 年 9 月 1 日アクセス .
- [3] 教職員用メール (KUMail) の移行について ,http://www.iimc.kyoto-u.ac.jp/ja/services/portal/member/ku_internal/newkumail.html, 2018 年 9 月 1 日アクセス .
- [4] 京都大学学術情報ネットワークシステム (KUINS), http://www.iimc.kyoto-u.ac.jp/ja/services/kuins/kuins_system.html, 2018 年 9 月 1 日アクセス .
- [5] 津山恵子, 個人情報流出隠蔽のグーグルや Facebook が陥る大企業病。自ら明らかにしない体質 ,<https://www.businessinsider.jp/post-177122>, 2018 年 10 月 16 日アクセス .
- [6] 京都大学クラウドサービス利用ガイド第 2 版 ,http://www.iimc.kyoto-u.ac.jp/services/ismo/ku_internal/cloud_service_guide_20180401.pdf, 2018 年 9 月 1 日アクセス .
- [7] G Suite for Education (オンライン) 契約 ,https://gsuite.google.com/intl/ja/terms/education_terms.html, 2018 年 9 月 1 日アクセス .
- [8] G Suite for Education のプライバシーに関するお知らせ ,https://gsuite.google.com/terms/education_privacy.html, 2018 年 9 月 1 日アクセス .
- [9] G Suite for Education のコアサービスと追加サービス ,https://support.google.com/a/answer/6356441?hl=ja&ref_topic=6047382, 2018 年 9 月 1 日アクセス .
- [10] ITmedia News, 研究データを 10 年守れ! 京都大学が導入した長期保存システムはオンプレとクラウドの“ハイブリッド” が実現の鍵に ,<http://www.itmedia.co.jp/news/articles/1805/21/news063.html>, 2018 年 9 月 3 日アクセス .