Appendix 2

アカウントにはご注意を

Google アカウントに限らず，いろいろなサービスの登録情報の流出が問題となっている．流出してからではなく，普段から個人でできるリスク対策を講じておこう．

1 情報流出の危険性を考えて利用する

アカウント乗っ取りやアカウント流出など，インターネットにかかわる被害が多くなっている．インターネットを利用したサービスを利用していると自分にはかかわりがないと思っていてもかかわってくることもある．

最近多いのがアカウント認証の連携機能だ．Google や Facebook，Twitter のアカウントを使って別のサイトのサービスが利用できるというもの．利点としては，それぞれのサービスで新たにユーザー名やパスワード，他の個人情報を登録する必要がなくなる．

しかし，**“連携する”**ということは，連携先のサービスで情報が流出するなどの事態が起これば，連携元の登録情報も流出してしまう可能性があるということも意味する．よって，連携サービスは，便利である一方でリスクもあることを考えて利用しよう．

2 安全策は 2 段階認証

今は，サービス提供側から情報が流出した場合には，利用者側がどんなに気をつけていてもどうすることもできない．だからと言って，利用者側が何の対策（**リスクマネジメント**）も立てていなければ，サービス側の情報流出のたびに自分の情報が漏れていないか，やきもきしなければならず，万が一，プライバシーにかかわる情報が漏れてしまったら，本人だけの問題では済まなくなってしまう危険性もある．

通常はアカウントとパスワードだけでサービスにログインすることができる．しかし，これではサービス側からアカウントとパスワードの情報が流出してしまえば，誰でもそのアカウントでログインできてしまう．そのために Google や Microsoft などの主要なサービスは，**「2 段階認証」**を行うことを推奨している．

2 段階認証とは，アカウントとパスワード以外に自分の携帯電話の電話番号を登録し，認証時に**「確認コード」**が自動的に携帯メールに送信され，その**「確認コード」**を入力しないとログインできないという仕組みである．これにより，アカウントとパスワードが漏れてしまったとしても，ログインの度に携帯メールに送られてくる**「確認コード」**までは知ることはできないので，他人が自分になりすましてログインすることを防ぐことができるのである．

また，Yahoo！JAPAN のサービスは，不正ログインがあった場合には，**「アラート」**が指定メールアドレスに届くように設定することができる．

「2 段階認証」や**「不正ログイン時のアラート」**など，利用者側でも一定の防御策を講じておくことはリスクマネジメントの観点からも有効な手段だ．

3 Google の 2 段階認証

Google の 2 段階認証は次のステップで行う．

① **パスワードを入力する：**Google にログインするごとに通常通りパスワードを入力する．

② **確認コードを入力する：**登録した携帯電話でテキスト，音声通話，モバイルアプリを介して受け取ったコードの入力を求められるので 6 ～ 8 ケタのコードを入力する．

これだけだと**「使いたいときにすぐに使えない」**と思われてしまうかもしれないが，その回避策（簡易的方法）も準備されている．特徴としては次のようなものである．

- 2 段階認証では，ログイン時に使う PC ごと，スマートフォン・タブレット端末ごとに確認コードの入力が必要になる．
- ただし，特定の PC からのアクセスであればコードの入力を省略するように設定できる．一度この設定を行えば，その PC からのログインであれば通常通りパスワードの入力のみでログインできる．
- 別の PC から Google アカウントにログインすると確認コード入力画面になる．指定した携帯電話に Google から自動的にメールが届き，そこに書かれたコードを入力するとログインできる．あるいは，後に紹介する確認コードアプリで生成されたコードを入力する．認証後は，Google のアプリが通常通りに使えるようになる．

4 2 段階認証を設定する

2 段階認証の設定方法

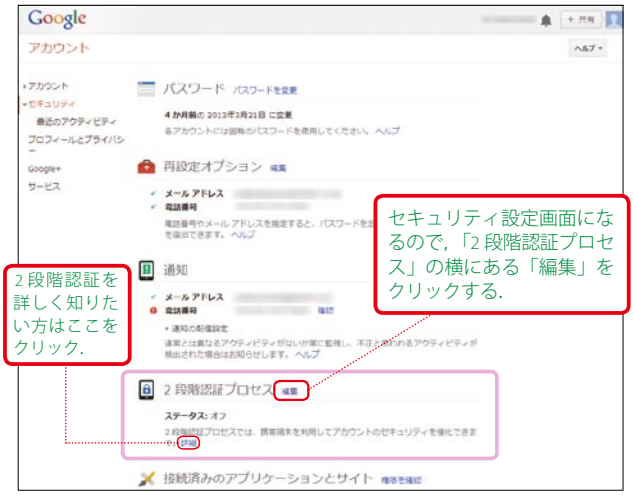
①Google のトップページにアクセスし，右上の**「自分のアカウント名が書かれている部分」**をクリックし，あらわれたメニューから**「アカウント」**をクリックする（❶）．

❶

②アカウント設定画面になるので，左のメニューから**「セキュリティ」**をクリックする（❷）．

❷

③セキュリティ設定画面になるので，**「2 段階認証プロセス」**の文字の横にある**「編集」**をクリックする（❸）．ここで説明文にある**「詳細」**をクリックする Google の 2 段階認証の紹介ページが開かれる．詳しく知りたい方は読んでみるとよいだろう．



❸

④**「2 段階認証プロセス」**の入口ページとなるので，右にある**「設定を開始」**をクリックする（❹）．①で**「使ってみる」**をクリックした場合もこのサイトとなる．

❹

⑤ログイン画面となるので，「パスワード」を入力してログインする（❺）

❺

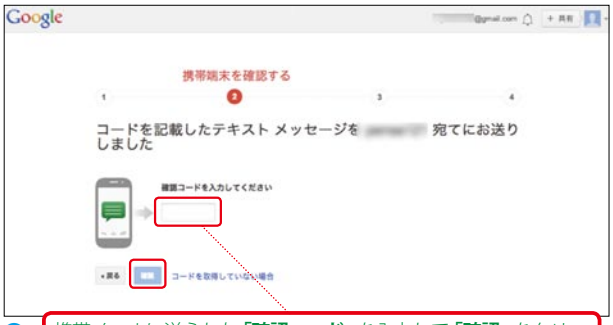
⑥2 段階認証に使いたい携帯端末の情報を登録する画面となる（❻）．**第 1 ステップ**として，**登録したい携帯電話のメールアドレスの@マーク前の情報を入力**し，携帯キャリアを選択する．

「コードの受け取り方」は音声通話でも構わないが，通常は**「テキストメッセージ（SMS）」**を選択する．

下部にある**「コードを送信」**をクリックする．

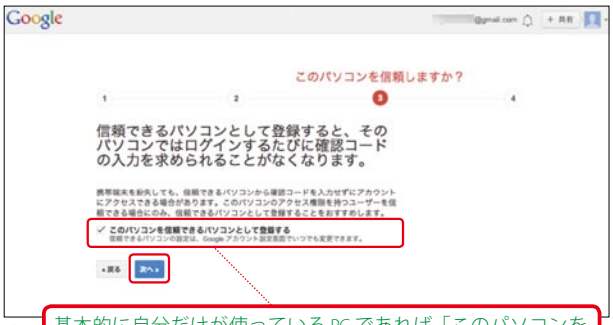
❻

⑦ **第 2 ステップ：**⑦で登録した携帯メールに**「確認コード」**が送られるので，その**「確認コード」**を空欄に入力し，**「確認」**をクリックする（❼）．
　コードが正しければ，次のステップに移る．



❼ 携帯メールに送られた**「確認コード」**を入力して**「確認」**をクリックする．

⑧ **第 3 ステップ：**現在設定を行っている PC が「信頼できるかどうかを登録する．基本的に自分だけが使っている PC であれば**「このパソコンを信頼できるパソコンとして登録する」**にチェックを入れ**「次へ」**をクリックする（❽）．
　信頼できるパソコンを登録することで，その PC からログインする限りは，2 段階認証は適用されず，通常通り使うことができる．

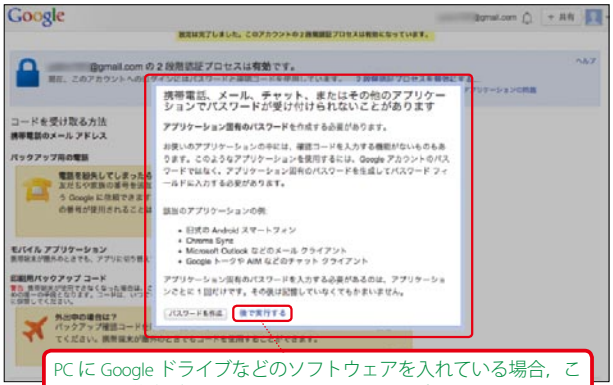


❽ 基本的に自分だけが使っている PC であれば「このパソコンを信頼できるパソコンとして登録する」にチェックを入れ「次へ」をクリックする．

⑨ **第 4 ステップ：**最終確認段階となる．ここで**「確認」**をクリックすれば **2 段階認証が有効**となる（❾）．

❾ **「確認」**をクリックすると 2 段階認証が有効になる．

⑩「確認」後，❿のような**警告**がでることがある．2 段階認証を設定することによって，PC やスマホなどで使っていた Google アカウントを利用するアプリケーション（Google ドライブなど）で **2 段階認証に対応していないアプリケーションはそのままでは利用できなくなる．**
　これらは後で設定できるので，ここでは**「後で実行する」**をクリックする．

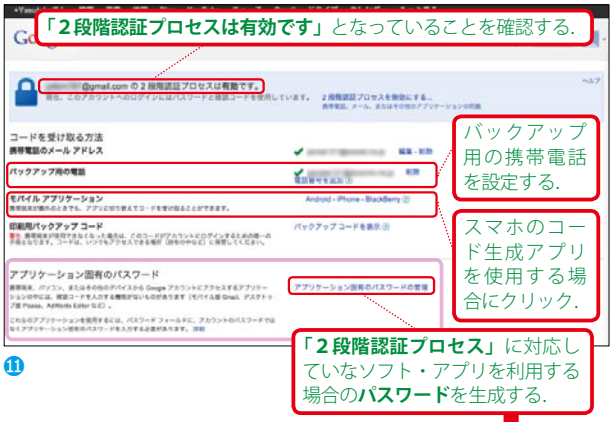


❿ PC に Google ドライブなどのソフトウェアを入れている場合，このような**警告**が出る．ソフトウェアごとにパスワードを作成し認証させる必要がある．ここでは**「後で実行する」**をクリック．

⑪「**2 段階認証プロセスは有効です**」となっていることを確認する（⑪）．これで 2 段階認証の設定は完了である．

ここで登録した PC 以外（スマホ・タブレットも含む）から Google にログインしようとすると，携帯メールに届いた「確認コード」を入力しない限り，Google にログインすることはできなくなる．

また，このままだと **Google アカウントを利用するアプリケーションで，2 段階認証に対応していないものは起動できなくなる**ため，それらの設定も各々コードを使って行う必要がある．



⑪

2 段階認証に対応していないアプリケーションのパスワード作成

2 段階認証を設定すると「2 段階認証に対応していないアプリケーション」は起動できなくなる．例えば Google ドライブやカレンダー，WindowsMail や Apple Mail などのメールソフトで Gmail を受診するように設定していると Gmail の認証で引っかかってしまう．

そこで，それらのアプリケーションを起動させるために，アプリケーションごとにパスワードを作成し，起動を許可していく作業が必要となる．

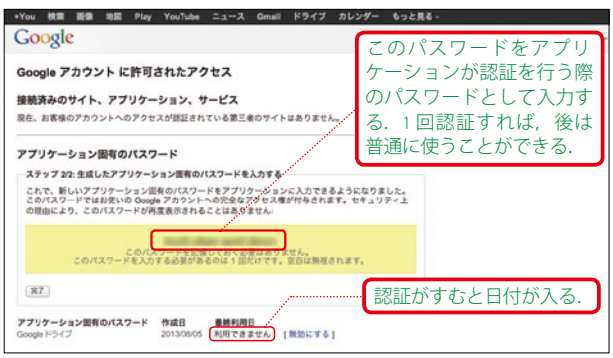
① ⑪の画面で下のほうにある「**アプリケーション固有のパスワードの管理**」をクリックする．

② パスワード作成画面になるので，下にある「**どのアプリケーション用のパスワードかわかるような名前を入力してください．**」と書かれてある下の欄に，アプリケーション名を入れて「**パスワードを生成**」をクリックする．これは便宜的なものなので，どのアプリケーションを登録したのか，後でわかるような名称であれば構わない（⑫）．

③ パスワードが生成される（⑬）．このパスワードをそれぞれのアプリケーションの認証の際に今までのパスワードの代わりに入力する．この作業はアプリケーションごとに 1 回だけ行えばよく，その後は普通に使うことができる．

少し面倒だが，アプリケーションごとにこの作業を行う必要がある．iOS や Android アプリも同様に行う．

⑫



⑬

バックアップ用携帯電話

2段階認証では，携帯電話をもっていないときや，紛失してしまった場合に登録したPC以外からGoogle関連にアクセスすることはできなくなってしまう．そのような場合に備えて，バックアップ用の電話を登録しておくことをオススメする．

①⓫の画面で中程にある**「バックアップ用の電話」**の下にある**「電話番号を追加」**をクリックする．

②バックアップ用の電話番号を入力する画面となるので，電話番号を入力する（⓮）．携帯電話を2台持っている人も少ないだろうから，ここでは入力する電話は固定電話や職場の電話番号になることが多いだろう．その場合には，**「コードを受け取る方法」**として**「音声通話」**を選択する．**「保存」**をクリックすれば終了である．

⓮ バックアップ用の電話番号を入力する．

③**「アカウント」**設定の**「セキュリティ」**の**「通知」**設定を見ると，**「バックアップ用の電話」**が設定されている（⓯）．

⓯ **「バックアップ用の電話」**に新しい電話番号が登録される．

2段階認証は一見すると面倒と思われてしまうかもしれない．しかし，自分自身は気をつけていても**“アカウントの乗っ取り”**による不正ログインをいつされるかわからない．特に医療者は，メール（Gmail）だけでなく，カレンダー（スケジュール）やメモ，Googleドライブに保存されたファイルなど重要な情報を扱っていることがあるので**“できうる限りのリスク対策”**はしておこう．

5 確認コードを生成してくれるアプリ

ここまでの設定でGoogleの2段階認証の設定は完了している．そのままPCやモバイル端末を使用すればよいが，PCならまだしも，モバイル端末でアプリを起動し，ログインし，再度メールを開いて，**「確認コード」**をコピーして，確認コードを入力して，ログインが完了，という作業は少し面倒である．

そのため，スマートフォン・タブレット用には**「確認コード生成専用アプリ」**がある．このアプリを使えば，Googleアカウント IDと紐づけられた**確認コードが自動的に生成**され，そのコードをコピーしてからログインすればよい．アプリの確認コードはデフォルトでは時間で切り替わるようになっているので，時間内にコードを入力するよう注意したい．

Google 認証システム（Android 版）

Android 端末では，Google 確認コード生成アプリとして**「Google 認証システム」**を使う（⑯）．Google Play で検索して，ダウンロードしよう．

⑯ Android 端末では，Google 確認コード生成アプリとして**「Google 認証システム」**を使う．Google Play からダウンロードしよう．

Google Authenticator（iOS 版）

iOS（iPhone/iPad）版の Google 認証システムは**「Google Authenticator」**という名称のアプリである（⑰）．App Store で検索して，ダウンロードしよう．

⑰ iOS（iPhone/iPad）版の Google 認証システムは**「Google Authenticator」**というアプリである．App Store からダウンロードしよう．

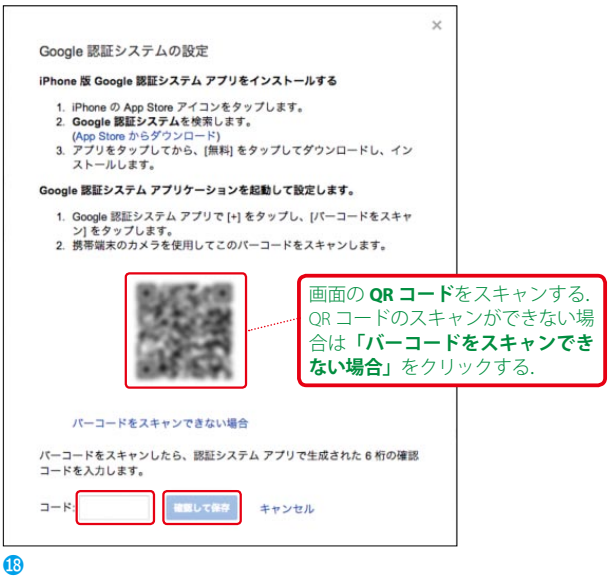
これらのアプリは，**「確認コード」**を生成してくれるアプリで，Android や iPhone で Google アカウントを利用するアプリを使用する際に必要となる．このアプリで生成された「確認コード」は，2 段階認証の登録をしていない PC からログインする際の**「確認コード」**としても使うことができる．

Google Authenticator（iOS 版）の使い方

ここでは iPhone を使った例を紹介する．

① iPhone で**「Google Authenticator」**を起動する前に，PC で⑪の**「モバイルアプリケーションの設定」**から**「iPhene」**をクリックする．

② **「Google 認証システムの設定」**画面が開き，画面に **QR コード**が表示される（⑱）．



⑱

③ここで**「Google Authenticator」**（⑲）を起動する．「ようこそ」という画面になるので，右上のメニュー，またはメッセージの下の**「+」**をタップする（⑳）．

④**「トークンを追加」**という画面になるので，**「アカウント」**と**「キー」**を入力するが，ここで，**「アカウント」**には**「Gmail アドレス」**を，**「キー」**には先程②で表示された**「QR コード」**を読み込み，キーを読み取り入力する（㉑）．

これを QR コードのスキャンができない場合は②で**「バーコードをスキャンできない場合」**をクリックしてあらわれるコードを入力する．

入力したら**「完了」**をタップする．

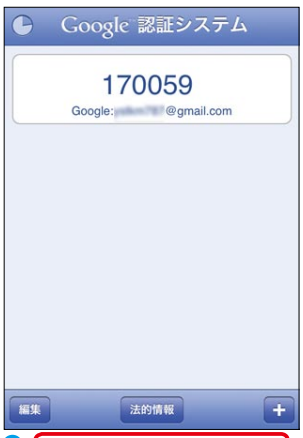
⑤これで**「Google Authenticator」**が Google と関連付けられ，使用することができるようになる（㉒）．**「Google Authenticator」**を使えば，携帯でメールが読めない環境でも**「Google Authenticator」**で生成されたコードを使って，Google にログインすることが可能である．

この作業で，Google アカウントと iPhone の「Authenticator」を関連付け，Google にログインするたびに Google が確認コードを生成する作業を iPhone の「Authenticator」がかわりに行ってくれるようになる．

⑲「Google Authenticator」を起動する．

⑳「+」ボタンをタップする．

㉑「アカウント」には「Gmail アドレス」を，「キー」には先程②で表示された「QR コード」を読み込み入力する．



㉒これで「Authenticator」が Google と関連付けられ，使用できるようになる．

6 Facebook・Twitterはなるべく連携サービスを利用しない

最近多いのが，Facebook アカウントの連携だ．Facebook は，基本的には実際の個人情報を入力する．さらに，出身高校や大学などの付帯情報を多く含む．Facebook の個人ページを開けば，右の広告欄に大学求人情報などが出される．それは，入力した情報から関連する情報サービスが連携されているためだ．

そのため，他サービスとの連携サービスを使うことは，Facebook の情報がそのまま他のサービスに受け継がれることになる．

Facebook と連携ができるサービスを使うときは，その連携先サービスが Facebook と連携する必要があるのかを十分に見極めるべきだろう．そうでなければ，面倒でもサービスごとの登録が望ましい．

7 インターネットは公開が基本

Google サービスは，公開が基本だ．その最たるサービスが Google ＋だが，Google ドライブや Google カレンダー，本書では紹介しなかった Google グループも基本は“公開”が原則となっている．

そもそもインターネットの原則は，公開することが基本だからだ．インターネットが今のように発展したのは，情報公開の歴史といってもよい．これまで閉鎖空間でしか知り得なかった情報を手軽に，いつでもどこでも手に入れることができるようなった．医療に関する情報は，患者や市民，どんな立場の人でも入手可能になった．これを原則**“公開しない（非公開）”**にすることは，インターネットの基本原則からは外れてしまう．

医療者は，機密情報をグループでやりとりしながら研究を進めることが多い．そのため，共有サービス，特に本書で紹介した Google サービスを利用し，グループ間で情報を共有する際は**“共有設定”**に特に気をつけたい．本書では随所でこのことについて触れているが，共有設定時には，現在の共有設定の状態はどのようになっているか，プレテストするなどしてから本導入することをオススメする．

（2013 年 8 月 10 日）