情報セキュリティ対策における電子情報機器の使用に対するガイドライン

［ 第5版 ］

令和 4 年 4 月 1 日改訂

（医療情報課）

Nihon University School of Medicine・Itabashi Hospital

日本大学医学部・板橋病院

Ⅰ　このガイドラインの趣旨・目的

このガイドラインは，医学部・板橋病院に勤務する教職員が，機密情報の適正かつ厳格な取扱いにあたり，パソコンやタブレット・スマートフォンなどの端末機器とその周辺機器，Ｗｅｂメールやオンラインストレージなどのインターネットサービスについて，具体的な使用ルールを定めるものである。

Ⅱ　用語の解説

1　機密情報

機密情報とは，組織にとって重大な秘密情報のことで，特定の組織を識別することができるものをいう。具体的には，研究や特許に関する情報，決裁書，契約書，人事情報（個人情報），給与情報，納入価格，システムのマスタ，パソコンの設定情報など広範囲に及んで存在し，公開することにより法人本部はもとより，医学部及び板橋病院における事業の執行や関係者に重大な影響を及ぼす情報のすべてが機密情報に該当する。

また，機密情報は，文書やデータなど有形なものだけではなく，無形なもの，つまり口頭で聞かされた機密情報も該当するため，第三者へ口外してはならない。

2　個人情報

個人情報とは，生存する個人に関する情報であって，特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができるものを含む）をいう。

個人に関する情報とは，氏名，性別，生年月日，年齢，住所，職業，続柄等の事実に関する情報に限られない。個人の身体，財産，職種，肩書，学歴・学習暦（学校の在籍記録，学籍番号，科目履修表，学業成績，人物評価など）等の属性に関する判断や評価を表すすべての情報を指し，公刊物等によって公にされている情報，映像や音声による情報（写真やビデオ等に記録したものなど）も含まれる。これら個人に関する情報が氏名等と相まって，特定の個人を識別することができることになれば，それが個人情報となる。

なお，生存しない個人に関する情報が，同時に，遺族等の生存する個人に関する情報に当たる場合は，当該生存する個人に関する情報となる。

3　要配慮個人情報

要配慮個人情報とは，人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により被害を受けた事実などによって，不当な差別や偏見その他の不利益が生じないよう，その取扱いに特に配慮を要するものとして政令で定めた個人情報をいう。

4　匿名化

匿名化とは，個人が特定できないよう，少なくとも患者ＩＤ，氏名，住所，電話番号（場合によっては生年月日も含む）をデータから削除することをいう。教育や研究などでデータの再検証が必要な場合は，患者ＩＤ，氏名，住所，電話番号などのデータを取り除き，新たに識別番号を作成し既存の患者ＩＤと置き換えるデータ加工を行い，識別番号と患者ＩＤの対応表による「連結可能匿名化」を行う。

5　暗号化

暗号化とは，第三者がディスク内のデータを閲覧してもランダムな意味を持たない文字や数値にしか見えず，内容が識別できないようにデータを変換することをいう。

6　アカウント

アカウントとは，インターネット上に展開されている多様なサービスを受ける際，サイトに入る（ログインする）ための「権利」のことをいい，個人情報を守るため，本人であることを「認証」する役割も持っている。

7　ＩＤ

ＩＤとは，「identity」のことで，個人を識別する名前と考えてよい。Google の場合は，GmailアドレスがそのままＩＤとして使用される。

III　このガイドラインの適用対象となる者

このガイドラインは，医学部・板橋病院の業務（教育・研究・診療・診療支援・事務処理など）に関わるすべての者と，医学部・板橋病院で研修や実習を受ける者，及び調査等を目的とした外部の者すべてを対象とする。よって研修生や実習生及び外来者に対しては，それらに関わる学内担当者が責任を持って，このガイドラインについて説明を行うものとする。

IV　パソコンの使用ルール

1　セキュリティレベルを設定する

医学部・板橋病院で使用するパソコン・タブレット（電子カルテ用を除く）には，使用目的や用途により，以下に示す何れかのセキュリティレベルを設定し，本体の見える場所にセキュリティシールを貼付する。セキュリティレベルが設定されていないパソコンは，医学部・板橋病院で使用することはできない。

セキュリティレベル「１」
ウイルス対策ソフトがインストールされ，ＯＳにアルファベットの大文字・小文字と数字が混在した「12文字以上」のパスワードが設定されている。

セキュリティレベル「２」
セキュリティレベル「１」に加え，BIOS（Windows）Firmware（Mac）にアルファベットの大文字・小文字と数字が混在した「12 文字以上」のパスワードが設定されている。

セキュリティレベル「３」
セキュリティレベル「１」「２」に加え,ハードディスクやSSDの全体またはデータ格納領域が「暗号化」されている。

2　セキュリティシールの取得

日本大学ソフトウェア監査における管理区域責任者から，医療情報課に取得申請を行う。なお，セキュリティレベルの判断は，パソコンの使用者が行い，実機の確認については，同監査における管理区域担当者が責任を持って実施する。

3　パスワード設定について

① パスワードは，ハードウェアやシステム毎に独立したものを使用し，少なくとも「電子カルテ用」「一般ＰＣ用」「ＮＵメール用」は，重複しないように設定する。

② パスワードは，用途により次ぎのとおり定期的にローテーションを行う。

1）電子カルテ用 ⇒ ２か月毎に変更（厚生労働省のガイドラインに準拠）

2）一般Ｐ　Ｃ　用 ⇒ ６か月毎に変更

3）ＮＵメール用 ⇒ ６か月毎に変更

医療情報課「推奨パスワード」

・数字の並びに西暦などの羅列は避ける。

・文字列に英数字の他，記号（＃・＄・％・＆・＝ など）を一つ加える。

・文字列が意味を持たない（辞書に載っていない）単なる文字の羅列にする。

※ 上記３要件を満たした安全性の高いパスワード例 「jubC#1017Fm5」「$kvCd17oV#81」

4　ウイルス感染対策

① ウイルス対策ソフトの定義ファイル更新

パソコンを使用する時は，ウイルスソフトの定義ファイルが更新されているか確認し，更新されていない場合は手動で更新を行い，常に最新の状態で使用する。

② ソフトウェアのアップデート

ＯＳやソフトウェアは，アップデートを行い，常に最新バージョンで使用する。

5　重要データのバックアップ

予期せぬ障害や操作ミスによるデータの喪失・破壊に備え，重要データは必ずバックアップを取るようにする。特に，セキュリティレベル「２」・「３」においては，パスワードの失念，ハードディスクのクラッシュ等により，データの復旧が困難となるため注意をする。

データバックアップ用として，外付けハードディスクを使用する場合は，ディスクの「暗号化」を行う。
（推奨暗号化方式：AES256）

Ⅴ　ＮＵメールの使用ルール

1　２段階認証プロセスを設定する

２段階認証プロセスは，万一，不正アクセスなどによりパスワードが盗まれた場合，アカウントの不正使用を防止するための「ログイン機能」で，セキュリティを強化することができる。

① ２段階認証プロセスの仕組み

ログイン時パスワードの入力後，セキュリティキーを求める画面が表示される。セキュリティキーは，事前に指定したスマートフォンなどに送信されるコードを入力するため，パスワードが２つになっただけでなく，コードを受信できる端末がないとログインすることができない。

② ログイン方法

ログイン時，一度２段階認証プロセスを設定したパソコンでは，通常のパスワードの入力しか求められないため，設定後のログイン方法に変更はない。

【２段階認証プロセスの設定方法】

1) Google のページにアクセスし，画面右上のユーザーアイコンから，「アカウント」をクリックする。

2) アカウント情報画面が表示されたら，ログインとセキュリティのブロックから，「Googleへのログイン」をクリックする。

3) ログインとセキュリティ画面が表示されたら，パスワードとログイン方法にある「２段階認証プロセス」が「オフ」になっていることを確認してクリックする。

4) ２段階認証プロセス画面が表示されたら，「開始」をクリックする。

5) 認証コードを取得するのに利用する携帯電話番号を入力後，コードの取得方法を選択して「次へ」をクリックする。

6) 利用できるかの確認画面が表示されたら，携帯電話に送信された「コード」を入力し，「次へ」をクリックする。

7) 入力したコードの確認が完了すると，２段階認証プロセスを有効にするかの確認画面が表示されたら，「オン」をクリックする。

8) 設定が完了したら，再度ログインを行う。通常のパスワード入力の次ぎに，２段階認証プロセス画面が表示されるので，携帯電話に送信された「コード」を入力しログインする。

2　送信取り消し機能を設定する

「送信取り消し」機能を有効にしておくと，メールを誤送信したあとでも，一定時間（最長30秒）内であれば送信を取り消すことができる。

【送信取り消し機能の設定方法】

1）受信トレイ画面の右上にある設定ボタン（歯車のアイコン）から，「設定」を選択する。

2）「全般」タブを開き，「送信取り消し機能を有効にする」にチェックを入れ，取り消せる時間を設定し，画面下部の「変更を保存」をクリックする。

3）設定有効後，メールを送信すると画面上部に「取消」が表示され，設定時間内であればクリックにより，メール送信をキャンセルすることができる。

3　添付ファイルについて

① 添付ファイルには「読み取りパスワード」を設定するWord・Excel・PowerPoint・PDF などのファイルをメールに添付して送信する場合は，個々のファイル自体に「読み取りパスワード」を設定する。

※ パスワードは，上記３「パスワード設定について」に準拠して設定する。

② パスワードの送信方法

送信先へ添付ファイルの読み取りパスワードを知らせる場合は，メールの本文とは別のメールで送信する。その際，メールの件名に，パスワードやＰＷなどの文字を表記しない。

③ 添付ファイルの格納

添付ファイルは，単一のファイルであっても「ZIP 形式フォルダ」に格納して送信する。

Ⅵ 高機能ネットサービスの活用

1　NU-Apps ドライブとは

NU-Apps ドライブは，Google が提供しているクラウドサービスで，同一のNU-Apps アカウントであれば，パソコン，タブレット，スマートフォンなど端末機器を選ばず，ファイルを管理・更新することができる。一般ユーザーは，15Ｇバイトまで無料で使用することができるが，ＮＵメールのアカウントを保有している教職員等は，無制限の容量が確保されており，NU-Apps ドライブは，学内ストレージとして認識されている。

2　NU-Apps ドライブの利用

医学部情報セキュリティ宣言により，「ＵＳＢメモリ」の使用が禁止されたため，異なる環境下のパソコンへデータを移動させる場合は，「NU-Apps ドライブ」を利用する。

① NU-Apps ドライブ基本画面の開き方

Google のページ（ＮＵメールの受信トレイなど）を開き，画面右上にあるタイル状のアイコン「Google アプリ」から，「ドライブ」をクリックする。

1) NU-Apps ドライブにファイルを格納する場合は，基本画面で「マイドライブ」を選択し，マイドライブエリアにファイルをドラック＆ドロップする。

2) NU-Apps ドライブに格納されたファイルをパソコンのローカル上で使用する場合は，当該ファイルにカーソルを置き，右クリックで表示されるメニューから「ダウンロード」を実行し，ファイルの保存先を指定する。

② 「アップロード」と「ダウンロード」

1）「アップロード」とは，Word やExcel などのファイルをGoogle ドライブへ格納することをいう。

2）「ダウンロード」とは，Google ドライブへ格納されたWord やExcel などのファイルをパソコン上で使用するために取り込むことをいう。

③ 「同期」と「共有」

1) 「同期」とは，サーバを経由して複数のデバイス間（パソコンやスマートフォンなど）で，データを常に同じ状態に保つ機能のこと。

2) 「共有」とは，サーバ上のデータを複数のユーザー同士が利用できるように設定する機能のこと。

NU-Apps ドライブ利用上の注意

・使用後は，必ずNU-Apps ドライブの「ログアウト」を行う。

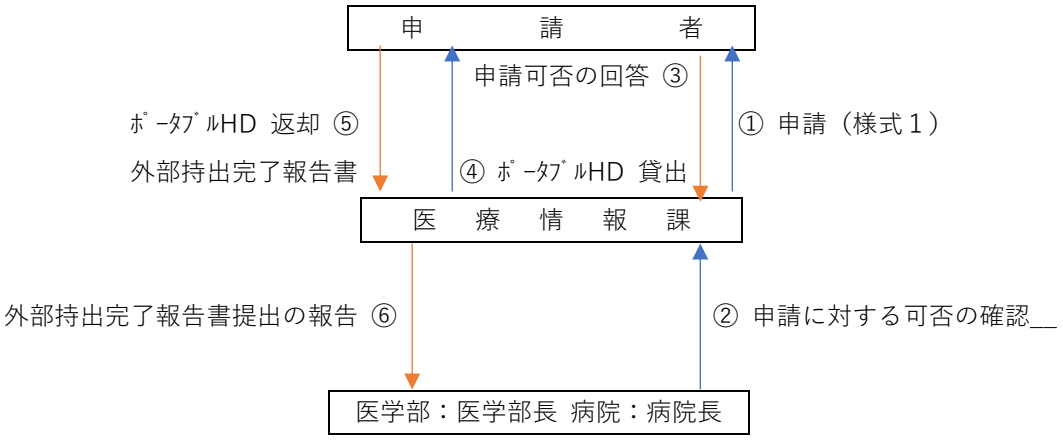
・個人で使用する場合は，ファイルを「マイドライブ」へ格納する。

・共有アイテムを使用する場合は，ファイルを共有するメンバーを十分確認する。NU-Apps ドライブ利用上の注意

Ⅶ 機密情報を学外へ持出す場合

機密情報を学外へ持出す場合は，持出す日の10 日前に，様式１「機密情報の外部持出許可申請書兼誓約書」を医療情報課へ提出し，医学部の場合は医学部長，病院の場合は病院長の許可を得て持出しが可能となる。

【機密情報の外部持出に対する運用フローチャート】



1) ① **申 請 者** 機密情報の外部持出許可申請書兼誓約書（様式１）に必要事項を記入し，医療情報課へ提出する。

2) ② **医療情報課** 申請書類（様式１）の記載内容を確認し，受け付け後，医学部は医学部長，病院は病院長に申請に対する可否の判断を求める。

3) ③ **医療情報課** 外部持出に対する可否の結果について，申請者へ回答する。

4) ④ **医療情報課** 許可が下りた場合，外部持出専用のポータブルＨＤの貸出を行う。その際，申請書類（様式１）の写しを添付する。

5) ⑤ **申 請 者** 目的の用途が完了したら，可及的速やかにポータブルＨＤ内の全データを完全に消去し，機密情報の外部持出完了書（様式１の写し）とともに医療情報課へ返却する。

6) ⑥ **医療情報課** 返却されたポータブルＨＤのデータが完全に消去されているか確認し，消去されていない場合は，申請者に注意喚起を行う。医学部は医学部長，病院は病院長へ外部持出完了報告書が提出された旨報告を行う。

以　上