医療情報・個人情報を取り扱う上でのガイドライン

社会医療法人・慶明グループ施設共通のガイドラインとする

令和3年12月版

(株)ケイメイ　開発室

Ⅰ．目的

本ガイドラインは、パソコン・タブレット端末・スマートフォンの利用ルールの設定，職員のセキュリティ意識向上の為、行動基準を設定することによりウイルス感染や情報の紛失・盗難などを未然に防ぎ、個人情報の漏洩・流出事故の防止や業務システムの安定運用が行える事を目的とする。

Ⅱ．ガイドラインの適用構成

1．　施設内での下記機器の利用に関する事

施設内で利用する全てのパソコン・タブレット端末・スマートフォンに関する取り扱いルール

2．　下記機器の施設外持ち出し、持ち込みに関する事

施設内で利用している全てのパソコン・タブレット端末・スマートフォンに関する社外持ち出しに関する取り扱いルール及び外部から持ち込む機器の取り扱いに関するルール

3．　施設外からの施設内ネットワークへの接続に関する事

外部からの施設内ネットワークへ接続する場合のルール

4．　ネットワーク機器の持ち込み

ネットワーク機器を持ち込み、施設内ネットワークに接続する場合のルール

5．　その他

5-1）IT機器※1を持参して移動中の注意事項

5-2）IT機器廃棄時の注意事項

5-3）テレワーク※2に関する注意事項

5-4）職員へのセキュリティ意識に関する事

1．　施設内機器の利用について

① 施設内設置のパソコン・タブレット端末・スマートフォンのローカルログインパスワード及びネットワークログインパスワードを必ず設定する。

a）推測されやすいパスワードは設定しない。

b）パスワードは定期的（６月と１２月の年２回）に変更することを推奨する。

c）業務上共有の必要があるパスワードに限り、所属長もしくはその担当者と情報を共有する。

d）パスワードをメモし、机上やディスプレイに貼付しない。

② インターネット接続に関して

a） 業務上必要とするサイト以外への接続を禁ずる

b） セキュリティ更新が最新でないパソコンもしくはセキュリティソフトウェアがインストールされていないパソコンからのインターネット閲覧を禁ずる

c） 推奨ブラウザ※3としてグーグルクロームの利用をお願いする

※業務上、インターネットエクスプローラーなど接続できない場合は、セキュリティ対策が施されている環境下での接続を許可する

d） 電子カルテなどの業務用パソコンは基本ソフトのアップデートを止めているため、マイクロソフトエッジ、インターネットエクスプローラーを最新状態に保つことができません。インターネットの閲覧は控え、どうしても必要な場合は、グーグルクロームを利用するようお願いします。

③ メールの送受信に関して

a） 身に覚えのない送信者からのメール及び添付ファイル及び本文中のURL※4を開かない事

b） 機密情報・個人情報を送信する際は、添付ファイルにパスワード保護して上で送信する事

※添付ファイルとパスワードは同一メールにしない事

c） 業務メールアカウントをセキュリティ対策の施されていないスマートフォンやタブレット端末に設定しない事

d） yahoo、hotmail他、慶明グループドメイン※5以外を業務用メールアカウントとして利用しない事

④ アプリケーション※6のインストール及び利用に関して

a） 業務に関係ないアプリケーションのインストールを禁ずる

b） アンインストールしてもクラウド※7上にアカウントが残るアプリケーションに関しては、利用するアカウントとパスワードに既存利用のアカウントや共通のパスワードを使用しない事

⑤ 機密情報・個人情報の保存・印刷・破棄に関して

a） 業務上個人情報をシステムとは別アプリケーション（エクセル・PDFなど）にエクスポート※8保存

する際は暗号化する事

b） 機密情報・個人情報を印刷する際は、垂れ流しにしない事。出力本人が印刷デバイスに到着してから印刷開始するようにパスワード保護する事

c） 機密情報・個人情報が印刷された紙媒体を破棄する場合は必ずシュレッダーにかける事

d） 機密情報（アカウント・パスワード）をセキュリティ対策されていないスマートフォン・タブレット端末に保存しない事。また一般ベンダーのクラウドサービスへの保存も禁ずる
※一般ベンダー（amazon,icloud.yahoo,google，dropbox他）

⑥ パソコンへの外部機器接続に関して

a） 下記条件において外部接続機器（USBメモリ、外付けハードディスク）の接続を禁ずる
・セキュリティ対策されていないパソコンに接続される可能性がある外部接続機器
・施設パソコン以外のパソコンに接続される可能性がある外部接続機器
・定期的にデバイス内ファイルのセキュリティスキャンを実施していない外部接続機器

b）外部接続機器の利用基準
・パスワードロックの機能が施されている外部接続機器
・定期的にセキュリティスキャンが実行される外部接続機器
・上記を満たしていても機密情報は紛失を考慮して保存対象から除外する事が望ましいものとする

２．　施設内外への機器の持ち込み・持ち出しに関して

①施設間の移動に関して

a）　施設間で貸し借り、使い回しなどパソコン・タブレット端末・スマートフォンを移動する際には施設固有の情報を消去する事

b）　保護していたローカルログインパスワードの使い回しをしない事

c）　ブラウザ上のキャッシュはクリアする事

d）　メールアカウントを消去する事

e）　移動先で必要としないアプリケーションは削除する事

②個人所有の機器に関して

a）原則個人所有のパソコン・タブレット・スマートフォンの施設内ネットワークへの接続を禁ずる

b）業務上必要な場合は、所属長の判断の上、利用する事

c）個人所有のパソコン・タブレット・スマートフォンへの業務ファイル保存を禁じる。

③委託業者・外部業者の機器・作業に関して

a）原則外部業者のパソコン・タブレット・スマートフォンの施設内ネットワークへの接続を禁ずる

b）外部業者にパソコン機器などのメンテナンスを実施してもらう場合、パスワードが漏洩しないようにする事

c）外部業者からデータを受け取る際は、極力メールの添付を利用する事

d）外部業者へデータを渡す場合、必ず所属長の確認を得る事。

e）データは暗号化した状態で渡し、パスワードはメールで送ること

※暗号化したデータとパスワードを同包しない事

３．　施設外からの施設内ネットワークへの接続に関して

① 下記の場合を除き、原則施設内ネットワークへの外部接続を禁ずる

a）接続する機器に十分なセキュリティ対策がされており、テレワークの場合は所属長の許可が得られた技法で接続される場合。

外部業者からの接続の場合、システムエンジニアに相談の上、安全が確認されてから許可を出すこと。

４．　ネットワーク機器の持ち込みに関して

① 下記の場合を除き、原則持ち込みネットワーク機器の施設内ネットワークの接続を禁ずる

a）施設内業務用ネットワークから物理的に切り離されたネットワーク環境がある場合、そのネットワークへの接続を許可する

b）業務上必要な場合は、所属長の許可を得た上で行う事

※対象となる機器は有線ハブ、無線ルーター、無線アクセスポイント

５．　その他

①移動中の注意事項

a） 盗難や置き忘れに十分注意する。

b） 原則、重要・機密データは持ち歩かない

c） 重要データを持ち歩く必要が生じた場合は必ず暗号化する事。

②廃棄時の注意事項

a） 紙媒体はシュレッダーで裁断する。

b） 情報（データ）が格納されているパソコンや電子媒体を廃棄する場合、情報（データ）の消去や媒体自体の破壊等を行い廃棄する。

c） クラスドサービスの退会などの場合は、使用していたログインアカウントとパスワードを再利用しないようにする事

③テレワークに関する注意事項

a） 利用するパソコンは十分なセキュリティ対策がされている事を確認した上で所属長の許可を得たパソコンである事

b） ネットワーク接続する為の手法は、必ず所属長（システムエンジニア）の指示・判断を得、個人

で不用意にフリーソフトなどで対応しない事

c） 接続が許可された個人パソコンを利用する場合、接続先の資源をダウンロードしない事

④職員へのセキュリティ意識に関する事

a）インターネットは便利な反面、情報の流出、流出による個人・企業への精神的・金銭的被害に繋がる事を十分考慮した上での利用を行う事

b）情報の流出またはその可能性に気づいた場合は、必ず所属長に相談する事

※情報流出を起こした機器、時間、閲覧していたサイトはUTM※9に全て記録されています

c）職場のネット環境・機器を私的に利用しない事

※個人機器の接続ログもルーター上に記録されています

参考文献

厚生労働省「医療情報システムの安全管理に関するガイドライン（第 5 版）」

https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf

経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン（第 2 版）」

https://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン（第 1 版）」

https://www.soumu.go.jp/main_content/000567229.pdf

総務省「テレワークセキュリティガイドライン（第5版）」
https://www.soumu.go.jp/main_content/000752925.pdf

本文中で使用されている専門用語について

※1　IT機器

主にパソコン・タブレット端末・スマートフォンの事を指しますが、情報を保存できるハードディスク、USBメモリなどの記憶媒体やパスワードが記憶されているモバイルルーターなどのネットワーク機器も含まれます。

※2　テレワーク

職場以外の場所からパソコン・タブレット端末・スマートフォンなどを利用して職場内のネットワークに接続し、職場内資源（共有ファイルなど）にアクセスしたり、リモートコントロールされる職場パソコン上の業務アプリケーションを起動して作業をおこなう事などです。

※3　ブラウザ

インターネットを閲覧するためのソフトウェアです。代表的な物として、グーグルクローム、マイクロソフトエッジ、インターネットエクスプローラー、サファリなどがあります。

ウィルスの入り口にもなるとも言われる、これらのソフトウェアはパソコンの基本ソフトのアップデートにより最新状態を維持する事が重要となります。

グーグルクロームは、設定によりソフトウェア起動時に最新版に更新する事が可能です。

古いブラウザを使用してインターネットを閲覧すると、ウィルス侵入の危険性が高まりますので使用を控えてください。

※4　URL

インターネットサイトのアドレス（場所）の事です。メールの本文などに貼り付ける事によってメール受信者を目的とするインターネットサイトに誘導する事も可能です。

http://　や　https://　で始まる記述が主なURLとなります。後者は暗号化通信ですが、前者は暗号化されない通信をおこなうため、盗聴の危険性が高まります。暗号化されていないサイトでの個人情報入力や取引は避けて下さい。

※5　ドメイン

インターネット上に存在するコンピューターやネットワークを識別するための名前の事です。慶明グループのドメインは下記になります。

（keimei.or.jp）（keiimei-group.co.jp）（keimeisw.or.jp）（eyetop.co.jp）（wawu2.jp）（miyazaki-green.co.jp）

上記は、企業のインターネット上の場所（住所）となり、その場所を運営する企業の信頼度がドメインを選択する際、重要となります。

（yahoo.co.jp）（amazon.co.jp）などは、企業に所属する人も含め全ての人に提供されるドメインです。無料のドメインもあり数多くのユーザーが利用するドメインとなります。反面サイバー攻撃を受ける頻度が高いドメインでもあります。

※6　アプリケーション

パソコン・タブレット端末・スマートフォン上で動作するソフトウェアの事です。

※7　クラウド（サービス）

インターネット上の記憶媒体（場所）の事です。

作業場所をインターネット上に置くことで、情報を失う危険性と作業するパソコンなどがインターネット環境さえあれば利用できるという特徴で、急速に利用が普及しました。

クラウドサービスを利用するという事は、便利な反面、重要な情報が全てインターネット上にあるという事とメンテナンスが他人まかせになるため、漏洩の危険性と向き合うことにもなります。

※8　エクスポート

情報を書き出す（保存）するという事です。ワードやエクセルなどのドキュメントを保存するのとは違い特定のデータを選択して書き出す手法です。電子カルテや財務システムを含め多くの業務用ソフトウェアに付いている機能でもあります。また書き出したデータは、互換性を重視するためにCSVと言われるファイルで保存される事が一般的で、CSVファイルはメモ長などで簡単に開く事が出来ます。メールに添付したり、他記憶媒体に保存する際は、必ずパスワード保護するようにしてください。

※9　UTM

インターネットの出入り口に設置し、外部からの不正攻撃をブロックするための機器です。

設置状況につきましては、別紙をご参照ください。