MICT 利用上の留意事項

目次

１）MICT のセキュリティ対策

利用機器（パソコン、タブレット、スマホ）とパスワードについて

・施設の管理者は、「MICT」を利用するスタッフと利用機器について把握し、台帳に記載して、適正に利用されているか確認をしてください。
・OS、ブラウザは、最新のものにして、ウイルス対策ソフトを導入してください。ファイル交換ソフトはインストールしないでください。
・「在宅版カルテ・情報ストックシステム（Man・Go!）」、「在宅連絡帳（MCS）」のパスワードは、保存しないでください。パスワードは、2 か月に一度程度、変更してください。
・機器を起動する際のパスワード（画面ロック）は、8 文字以上の英数字混じりのものに設定してください。
・機器を他者（自分の家族も含む）に渡す（機種変更する、譲渡する、リースを終えて返却するなど)場合には、必ず、内容を徹底的に消去し、他者が利用、機器内に残っているデータが閲覧できないようにしてください。

利用機器の紛失・盗難の際の対応

・直ちに、他の機器を使い、「在宅版カルテ・情報ストックシステム（Man・Go!）」、「在宅連絡帳（MCS）」にアクセスし、自分のパスワードを変更してください。
・直ちに、MICT 事務局に、詳しい状況を電話やメールで通知してください。
必要により、MICT 事務局から運営会社に連絡し、その利用者の利用を一時停止してもらいます。
・事業所管理端末の場合、直ちに、機器の携帯電話会社に連絡し、可能なら、機器のリモートロックなどの処置をしてもらってください。

他の連携方法との使い分けや併用

MICT は連携手段の一つであり、万能ではありません。必ず、状況に応じて、他の連携方法との使い分けや併用をしてください。
・急ぐ場合は、電話で連絡をする。

・規則上、文書が必要な場合は、紙の文書を作成する。
・デリケートな内容の場合は、対面で情報交換を行う。

「MICT」で利用するスマホ・タブレットのセキュリティ対策盗難・紛失対策

・「在宅版カルテ・情報ストックシステム（Man・Go!）」、「在宅連絡帳（MCS）」のパスワードは保存しない。
・パスワードで、画面をロックする。（８桁以上の英数字&記号の組み合わせで）
Android と iPhone での設定の方法は、以下を参照してください。
被害に遭う前に！スマホユーザーが今すべきセキュリティ対策 2.2 画面をロックする
https://japan.norton.com/android-security-2-3070
・携帯電話会社のリモートロックやデータの強制消去サービスを利用する。

ウイルス感染対策

・OS やアプリは常に最新の状態にアップデートする。
・不要なアプリはインストールしない。
・アプリは信頼できる場所（メーカーやキャリアが用意する正規のアプリケーション・ストア） からインストールする。
・Android 端末の設定画面で「提供元不明のアプリ」という項目のチェックを外しておく。
・Android 端末では、アプリをインストールする際にアクセス許可を確認する。
・不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止する。
・メールの添付ファイル、URL リンクを不用意に開かない。
・ウイルス対策ソフトや不要な通信を遮断するファイヤーウォールソフト等などのセキュリティソフトを導入する。
・携帯電話会社のセキュリティ対策サービスを利用する。

情報漏洩対策

・安全な回線（携帯電話の回線や施設内の無線 LAN）を使う。街中などの無線 LAN スポット（Wi-Fi 環境）は利用しない。
・許可されたスタッフ以外とは、機器の共有をしない（自分の家族にも使わせない）。
・無線 LAN を利用する場合、親機やサービスの設定として、SSID をステルス設定（自分の存在を知らせるためのビーコン信号を停止させ、見えなくなる設定。機器の使用説明書を参照）にする。
・万が一、個人情報の漏洩またはそのおそれが生じたことにより法律上の賠償責任を負担するための各種費用を保証する保険（個人情報漏えい保険、医療機関用団体サイバー保険等）に加入することを推奨する。

２）MICT 台帳の内容

各施設又は組織において、MICT の利用に関して、下記の内容の台帳を作成し、管理する。

１）MICT の管理責任者

２）MICT の施設管理者として、MICT に登録した者（実際に、スタッフの登録・削除・変更などの作業を行う者）

３）MICT の管理権限を付与した者（複数可）

４）MICT 利用者のリスト

・氏名・所属・職種
・MICT の ID（登録メールアドレス）
・利用開始日
・利用端末（複数の場合全て）
　種類（PC、タブレット、スマホ）・機種の名称
　利用端末の利用場所　施設内・施設外（具体的に）
　利用するネットワークの種類（施設内有線 LAN･施設内無線 LAN･キャリア）公衆無線 LAN は不可
　端末起動時パスワードの設定の有無
　コンピュータウイルス対策ソフトの導入の有無
　業務に使用しないアプリケーションや機能について
　削除又は停止、あるいは、業務に対して影響がないことを確認したか
・MICT 運用ポリシーを読んだか
・MICT 講習会の受講・講習ビデオの視聴の有無
・スタッフ誓約書の取得年月日
・利用システム区分（在宅版カルテ・情報ストックシステム（Man・Go!）・在宅連絡帳（MCS））

３） 参考資料

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
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf
（**P64-67**）

6.9 情報及び情報機器の持ち出しについて

6.9　情報及び情報機器の持ち出しについて

B．考え方

昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。

一方で、在宅医療、訪問診療等の増加、モバイル端末の発展により医療情報を持ち出すニーズや機会が増加していることも事実である。

情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末や CD-R、USB メモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。

まず重要なことは、「6.2　医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」の「6.2.2　取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3　リスク分析」を実施することである。

その上で、医療機関等において把握されている情報若しくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報若しくは情報機器に対して対策を立てなくてはならない。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。

一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取扱いについての把握や規制は難しくなるが、情報の取扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報若しくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報若しくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。

ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

従って、情報若しくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。

ノートパソコンや、タブレット、スマートフォン等を用いて情報システムにログインする場合においても、2 要素認証を用いることが望ましい。利用者の識別・認証に係る説明や留意点については、「6.5 技術的安全対策」の記載を参照されたい。

スマートフォンを利用する際の安全対策については、「スマートフォン・クラウドセキュ リティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～」（総務省；平成 24 年 6 月）が参考になる。

また、以降のガイドラインと内容は重複するが、タブレット PC 及びスマートフォンを用いる場合の守るべき事項をまとめると以下のようになる。

- 機器自体の管理を、運用管理規程を定めて実施すること。盗難・紛失を早期に発見することはもちろんのこと、不要なアプリの存在や、パスワードの設定が適切であること等を定期的に確認しなければならない。
- 端末自体の起動パスワード等の設定は必須であり、パスワードを用いる場合、パスワードは容易に推定されることがないものとし、かつ定期的な変更を行わなければならない。
- 端末内に患者等の情報が保存されている場合、あるいはアクセス先に存在する患者等の情報を表示や編集できる場合は、その機能を持つアプリ自体にもパスワードを設定し、端末内に情報が存在する場合は暗号化しなければならない。
- 業務に用いる機能に影響を与えないために、必要最小限のアプリ以外はインストールしないこと。OS のメモリ管理機能で、メモリを隔離して他のアプリの影響を受けないアプリが構築可能な場合は、確実にメモリ隔離ができることを確認することが必要である。
- ネットワークは 6.11 章の基準を満たしたもの以外は利用しないこと。特に公衆無線 LAN はリスクが大きいため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、6.11 章の基準に則った利用を認める。また、自動的に公衆無線 LAN に接続してしまう端末も存在するので、業務アプリ起動時に VPN 接続を確立しない場合は、公衆無線 LAN への自動接続機能を切る必要がある。
- 個人の所有する、あるいは個人の管理下にある端末の業務利用（以下「BYOD」（Bring Your Own Device）という。）は原則として行うべきではない。上記の要件を実現するためには端末の OS の設定を変更する必要があるが、この機能は管理者に限定されなければならない。管理者以外による設定の変更を技術的あるいは運用管理上、禁止できない限り、BYOD は行えない。
- 覗き見防止対策の実施が望ましい。

C. 最低限のガイドライン

1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
3. 情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。
6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。

8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。
9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
10. 個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。

D. 推奨されるガイドライン

1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。

2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。
3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。
   - BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。
   - 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。