別紙２

【ＭＣＳのセキュリティ対策】

１　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

(1) 施設の管理者は、ＭＣＳ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すること。
(2) 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すること。ファイル交換ソフトはインストールしない。
(3) 機器を長時間操作しない場合、クリアスクリーン等の対策を実施すること。(他人がのぞき見したり、操作できたりできる状態のまま放置しない)
(4) ＭＣＳ（メディカルケアステーション）のパスワードは、保存しない。
(5) 機器にＰＩＮ・パターン・パスワード等によるデバイスロックの設定をすること。
(6) 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ＭＣＳを利用したり、機器内に残っているデータが閲覧できないようにしたりすること。

２　利用機器の紛失・盗難の際の対応

(1) 直ちに、他の機器を使い、メディカルケアステーションにアクセスし、自分のパスワードを変更すること。
(2) 直ちに、市に、詳しい状況を電話やメールで通知すること。必要により、市から運営会社であるエンブレース株式会社に連絡し、そのＭＣＳユーザーの利用を一時停止する。
(3) 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うこと。

３　ＭＣＳで利用するスマホ・タブレットのセキュリティ対策

(1) 盗難・紛失対策
①機器の保管場所に鍵をかけるなどし、利用していないときに不特定個人が利用できるようにしない。
②パスワードで､画面をロックする設定の方法は､以下を参照すること｡(Android､iPhone)
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
③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。
(2) ウイルス感染対策
①ＯＳやアプリは常に最新の状態にアップデートする。
②不要なアプリはインストールしない。
③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 端末では、不明なアプリのインストールを許可しない)
④Android 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。
⑤ＭＣＳの偽サイトやＭＣＳを偽るメール等に注意し、メールの添付ファイル、ＵＲＬリンクを不用意に開かない。
⑥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。
(3) 情報漏洩対策
①無線ＬＡＮ（Ｗｉ－Ｆｉ）に接続して利用する場合、ＷＰＡ２－ＡＥＳ、ＷＰＡ２－ＴＫＩＰ等通信が暗号化されているものから接続し、暗号化されていない・管理者が

正体不明等の信頼できない無線ＬＡＮには接続しない。
②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)。

４　ＭＣＳ管理台帳の内容

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

(1) ＭＣＳの管理責任者
(2) ＭＣＳ管理者権限を付与した者（複数可）
(3) ＭＣＳユーザー情報
①氏名・所属・職種
②ＭＣＳのＩＤ（登録メールアドレス）
③利用開始日
④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・施設内無線・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
⑤ＭＣＳ運用ポリシーを読んだか
⑥講習会の受講・講習ビデオの視聴の有無
⑦スタッフ誓約書の取得年月日
(4) 施設の利用規程