「ポピーねっとやまがた」 運用ポリシー
別冊

目次

１．ＩＴ機器の安全対策

ポピーねっとやまがたのみならず、施設のあらゆる医療情報システムは、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版を考慮して、安全管理の対策を適切に講じる必要がありますが、ここでは、やまがたポピーねっとに関連する対策についてその主なポイントを記述します。

１－１．ＩＤ・パスワードの管理

ポピーねっとやまがたは、個人ごとに設定及び管理されたポピーねっとやまがたの ID 及びパスワードによって利用することができます。ID 及びパスワードの管理を以下の通り徹底しておこないます。

（１） パスワードはメモを残したりせず、人目にふれないように細心の注意を払ってユーザー個人が管理し共有しない。
（２） 一つの ID を複数人で共有しない。
（３） パスワードは、英数混合８ケタ以上とし、定期的（最長で２か月に１回）に必ず変更する。
（４） 利用が終わったら必ずログアウトする。
（５） パソコンの場合、離席時にも必ずログアウトする。
（６） スマホやタブレット、パソコンなど、利用するすべての端末にはロックをかける。

１－２．IT 機器のセキュリティ対策

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版の「6.9 情報及び情報機器の持ち出しについて」の「Ｂ.考え方」では、ノートパソコンやＵＳＢメモリーのみならず、「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」についても、「C. 最低限のガイドライン」として、「 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。」、「6. 情報機器に対して起動パスワードを設定すること。設定にあ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。」を勧めています。

ポピーねっとやまがたを在宅などモバイルの環境で利用する場合も、上記ポイントに留意しながら、スマートフォン、タブレットなどのモバイル端末についても次頁表のような運用を徹底してください。

また、BYOD（ユーザー個人所有の端末の業務使用）を許可するかどうかは事業所ごと情報管理者の判断となり許可を必要としますが、BYOD であるかどうかに関わらず、紛失などの情報漏えいリスク等を考えて同様の運用をしてください。

セキュリティ推奨項目	説明
ナンバーロック	スマートフォン、タブレットなどに他者がログインできないよう、数字列などによるパスワード認証（8文字以上）を設定し、定期的に変更する。
情報機器と情報の取り扱い	持ち出した情報を、定められている以外のアプリケーションがインストールされた情報機器で取り扱わないこと。 また、持ち出した情報機器には、定められている以外のアプリケーションをインストールしないこと。いずれのケースも、例えばファイル交換ソフト（Winny 等）等をインストールしないこと。
ウィルス対策ソフトのインストール	スマートフォンやタブレットに適切なウィルス対策ソフトをインストールしておく。
リモートワイプサービスの利用	スマートフォン、タブレットなどの端末内に残るデータをリモート環境からアクセスし、削除することができるサービス。万一の際に指示することで削除可能となる。
緊急回線停止サービスの利用	万一の際に、スマートフォンやタブレットの回線を遮断することで他者による不正なアクセスを防ぐ。
端末管理・利用者管理（MDM）サービスの利用	利用者側の管理者が一括して、各スタッフの利用状況や各端末の状態を確認、強制設定、ロックできる。
ブラウザ設定（ID等情報の都度入力）	IDやパスワードを記憶する設定にしない。
MCSの操作（コピー等の制限）	定められた手順を守り、情報のダウンロードや、コピー、画面ショットの取得などを行わない。

また、事業所内に設置されたサーバー、パソコン、ノートパソコンなどをスタッフが施設外に持ち出すことを禁止、または持ち出す場合は管理者の承認を事前に得るなどの運用を決めておく必要があります。

そのためには「情報および情報機器を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的、期間を別途定める書式でシステム管理者に届出て、承認を得ること。」「システム管理者は情報が格納された可搬媒体および情報機器の所在について台帳に記録すること。そして、その内容を定期的にチェックし、所在情報を把握すること。」（厚生労働省の「医療情報システムの安全管理に関するガイドライン」より抜粋）といった内容を設けることが考えられます。

１－３．個人情報漏えいの現状について

・ＩＴ機器の紛失・盗難等の実態について

以下は、IT 機器の紛失・盗難等の実態調査結果です。この調査結果では、電子メールや FAX での誤送信の割合がとても高くなっていますので、それらを利用する場合の注意を喚起する必要があります。また、やまがたポピーねっとを利用する端末の紛失・盗難時の情報漏えいのリスク を回避するためにも「**１－１．ＩＤ・パスワードの管理**」や、「**１－２．IT 機器のセキュリティ対策**」の徹底が重要になります。

紛失・盗難、誤送信の年間発生確率

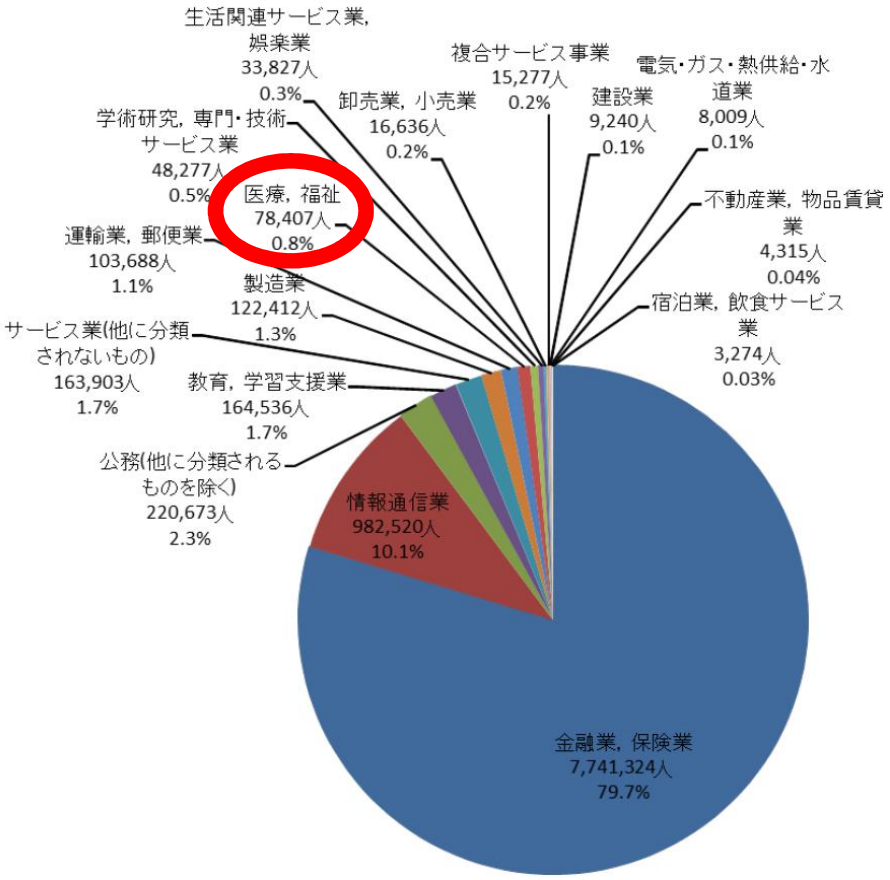
調査対象	2010年	2009年
携帯電話	6．4%	6．6%
パソコン	3．7%	3．1%
USBメモリ	4．7%	4．1%
電子メール（誤送信）	40．3%	17．1%
FAX（誤送信）	39．0%	12．1%

出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「情報セキュリティインシデントに関する調査報告書～発生確率編～」

・業種別での個人情報漏えいの人数

以下は、業種別での個人情報漏えいの人数です。「医療・福祉」関連の個人情報漏えい比率は 0.8%です。漏えいしている事実に目を向けて、個人情報管理の運用を日々徹底していく必要があります。

業種別比率（人数）

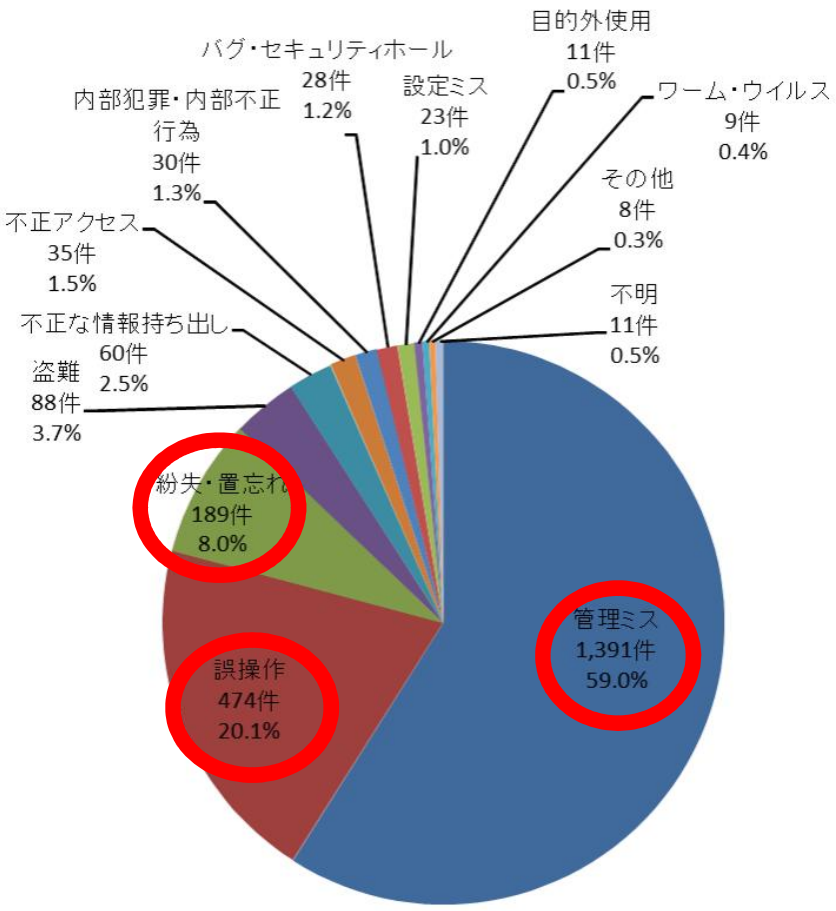


出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「2012 年　情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

・個人情報漏えい件数の原因比率

以下は、個人情報漏えい件数の原因比率です。「管理ミス」、「誤操作」、「紛失・置き忘れ」で約 90%を占め、また「管理ミス」の約半分は、信用金庫や信用組合、地方銀行での紛失や誤廃棄であったとのことです。それに対して、バグ・セキュリティホールは、1.2%であり、情報漏えいのほとんどがヒューマンエラー等人的な原因です。ですので、システム提供事業者によるさらなるセキュリティ向上と合わせて、現場での教育等による個人情報管理の運用を日々徹底していく必要があります。

漏えい原因比率（件数）



出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「2012 年　情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

２．スタッフ誓約書と教育

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版の「6.6 人的安全対策」の「(1) 従業者に対する人的安全管理措置」の「C.最低限のガイドライン」にて、「医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。」として、「1．法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。」また、「2．定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。」さらに、「３．従業者の退職後の個人情報保護規程を定めること。」としています。

２－１．スタッフ誓約書

ポピーねっとやまがたを利用するかどうかにかかわらず、上記ガイドラインに基づいた安全管理のためにも事業所内スタッフとの契約は重要です。スタッフ誓約書の記載内容のポイントは以下の通りです。

（１）スタッフは、就業規則やマニュアルなどの諸規定を遵守し、患者等の個人情報のみならず、事業所内で知り得た業務に関連する一切の情報をも許可なく漏えいしてはならない、とします。
（２）退職後も漏えいしない、とします。
（３）ＩＴ機器についての取扱い、返却時の注意点などを記載します。
（４）事業所が定めた利用目的外での使用を禁止します。
（５）患者その他の第三者のプライバシーその他の権利を侵害するような行為を一切しない。

スタッフ誓約書のひな型を用意しましたので、必要に応じ修正して作成し、最適なもので誓約をとるようにしてください。

２－２．スタッフ教育

事業所ごとに作成したポピーねっとやまがた MCS 運用ポリシーを徹底するために、事業所の責任者によって、事業所内のグループ管理者およびユーザーに対して、定期的に教育を行います。また、やまがたポピーねっとの位置づけをユーザー全員で共通認識したうえで、取り扱っている個人情報等の重要性を日々認識し、情報の取扱いに注意していきましょう。

また、パスワードの管理や離席時のログアウトなど、基本的なことも日々心がけていくことが大切であることを共有しましょう。

３．ポピーねっとやまがた運用ポリシーの作成と運用のポイント

ポピーねっとやまがた運用ポリシーは、以下のポイントを踏まえて、施設ごとに最適な運用管理ができるように作成し、作成したポピーねっとやまがた運用ポリシーに基づいて、全ユーザーで運用を徹底するように心がけてください。

３－１．情報漏えい発生時の対応について

情報漏えい発生時の対応方法や体制を整え、周知しておくことはとても重要です。情報漏えいによる直接的・間接的被害を最小限に抑えるためにも、また再発防止のためにも適正な措置を行うことができるよう対応方法を準備しておきましょう。情報漏えいのタイプは、パソコンやモバイル端末、帳票などの紛失・盗難、メールやＦＡＸなどの誤送信、内部犯行、システムへの不正アクセスなどさまざまです。また、関係のない人に患者の情報をうっかり口頭で漏らしてしまうことも情報漏えいの一つといえます。

情報漏えいに関する兆候や具体的な事実を確認した場合は、責任者に速やかに報告することを徹底し、情報漏えい対応のための体制づくりを行い必要な方策を講じてください。適切な対応についての判断を行うためにも５Ｗ１Ｈ（いつ、どこで、だれが、何を、なぜ、どうしたのか）の観点で、漏えいした情報の量（件数）と内容、どのような形で保存されていた情報か（暗号化、認証パスワード保護など）などの事実を調査し整理してください。漏えいした情報に個人情報が含まれている場合は、個人情報保護法に準拠した対応が必要となります。

詳しくは、ＩＰＡ（独立行政法人　情報処理推進機構　セキュリティセンター）が発行している「情報漏えい発生時の対応ポイント集」などを参考に準備しておくことをお勧めします。

３－２．端末紛失時の対応について

端末を盗難などにより紛失した場合も、責任者に速やかに報告するとともに、パスワードを変更することをお勧めします。また、株式会社日本エンブレース　メディカルケアステーション　サポートデスクに連絡をとり、該当するポピーねっとやまがたユーザーＩＤの一時停止をすることもお勧めします。