４． 導入するICT機器・ソフトウェアのセキュリティ上の課題と対策について

ここでは、ICT 製品・ソフトウェアを導入する際にセキュリティ上検討すべき事項や、課題と対策について紹介します。

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成16年12月24日医政発第1224001号・薬食発第1224002号・老発第1224002号厚生労働省医政局長・医薬食品局長・老健局長通知）（以下、「個人情報ガイドライン」という。）に示されているとおり、介護サービス事業所は多数の利用者やその家族について他人が容易には知り得ないような個人情報を詳細に知りうる立場にあり、個人情報の適切な取扱いが求められています。ICT 製品・ソフトウェアを導入すると、その情報システムには個人情報が一元的に集約されることになるため、その取り扱う個人データの漏えい、滅失又はき損した場合には、利用者やその家族、従業員に被る権利利益の損害への影響は、ICT製品・ソフトウェアを導入前と比べてより大きくなると考えられます。したがって、安全管理のための組織的、人的、物理的、及び技術的安全管理措置を一層強化することが求められることになります。

個人情報ガイドラインでは、以下の表のように安全管理措置の事項が挙げられています。ここでは、特に情報システムの導入と関連する事項を抽出し記載します。

図表 １９　個人情報ガイドラインにおける安全管理措置の事項（一部抜粋）

安全管理措置として考えられる事項	記載内容
個人情報保護に関する規程の整備・公表	・個人データを取り扱う情報システムの安全管理措置に関する規程等についても整備を行う。
物理的安全管理措置	・入退館（室）管理の実施 ・盗難等に対する予防対策の実施 － 操作ログ等のモニタリングの実施 － 記録媒体の持込み、持出しの禁止 ・機器、装置等の固定など物理的な保護 ・個人データを取り扱う端末に付与する機能を限定
技術的安全管理措置	・個人データに対するアクセス管理（ID／パスワード等による認証、権限管理） ・個人データに対するアクセス記録の保存 ・不正が疑われる異常な記録の存否の定期的な確認 ・個人データに対するファイアウォールの設置 ・外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認 ・ソフトウェアに関する脆弱性対策（セキュリティパッチの適用、システム固有の脆弱性の発見及びその修正等）
個人データの保存	・個人データを長期に渡って保存する場合には、保存媒体の劣化防

安全管理措置として考えられる事項	記載内容
	止等個人データが消失しないよう適切に保存する。 ・個人データの保存にあたっては、照会などに対応する場合等、迅速に対応できるよう、インデックスの整備など検索可能な状態で保存しておく。
不要となった個人データの廃棄、消去	・不要となった個人データの情報機器を廃棄する場合には、記憶装置内の個人データを復元不可能な状態に消去して廃棄する。 ・個人データの廃棄の際の取扱いについて、委託契約においても明確に定めておく必要がある。

技術的安全管理措置としてより具体的な対応内容については、医療機関等において医療情報システムの導入する際のガイドラインとして「医療情報システムの安全管理に関するガイドライン」（平成 17 年 3 月 31 日医政発第 0331009 号·薬食発第 0331020 号·保発第 0331005 号）（以下、「医療情報ガイドライン」という。）に記載があります。この医療情報ガイドラインの「6 章 情報システムの基本的な安全管理」に記載されている項目から、ICT 製品・ソフトウェアの機能と関連する項目でかつ最低限遵守が求められる項目を抽出し、この項目に対して今回の実証事業で利用した６社のソフトウェアの対応状況をヒアリングしています。

図表 ２０　医療ガイドラインの安全管理項目のうち実証事業で使用した６社の対応状況

	A 社	B 社	C 社	D 社	E 社	F 社
対応している	25	17	14	22	14	17
一部対応している	0	5	2	1	6	3
対応していない、もしくは対象外	3	6	12	5	8	8

この結果から、医療情報ガイドラインとして最低限遵守が求められる項目について全てに対応している製品はないことがわかります。導入する ICT 製品・ソフトウェアの機能をよく理解し、セキュリティ対策としてどのようなリスクが存在するのか、予め委託先とよく協議をしておくことが重要となります。

医療情報ガイドラインの安全管理措置の項目のうち、物理的安全対策と技術的安全対策の内容を例に具体的な対応状況について解説します。

＜物理的安全対策と技術的安全対策の対応について＞

１．物理的安全対策について

医療情報ガイドラインでは物理的安全対策として、個人情報が保存されている機器の設置場所や記録媒体の保存場所の施錠管理、個人情報が存在する PC 等の重要な機器への盗難防止用チェーンの設置、窃視防止の対策などを求めています。これらは導入する ICT 製品・ソフトウェアの機能によってすべて実現される内容ではなく、介護サービス事業所に設置する機器の運用ルールに関連するものです。したがって、ICT 製品・ソフトウェアを提供するベンダーに任せるのではなく、新たに機器を設置する際には提供するベンダーと相談をして、介護サービス事業所としてどのように対応するか検討することになります。

２．技術的安全対策について

技術的安全対策では、物理的安全対策と同様に介護サービス事業所の運用ルールで対策を検討する事項もありますが、導入する ICT 製品・ソフトウェアの機能によって実現される内容もあります。例えば、システムへの認証です。ガイドラインでは、情報システムへのアクセスにおける利用者の識別と認証を求めています。これは運用ルールでは実現することは難しく、今回の実証で利用した ICT 製品・ソフトウェアでは、すべての製品で ID とパスワードによる認証により対応をしています。さらに、医療情報ガイドラインでは、パスワードを利用する場合には、パスワードの暗号化や定期的な変更や、英数字記号を含めた８文字以上の文字列の使用を求めています。今回の実証で利用した ICT 製品・ソフトウェアでは、いくつかの製品では定期的な変更が求められないもの、英数字記号を含めた８文字以上の文字列が条件となっていないものがありました。このような場合には、介護サービス事業所の運用ルールを定めて対応を検討することになります。また、アクセスの記録（アクセスログ）では、今回の実証で利用した製品のうち対応をしているものがほとんどですが、一部に利用者の特定など具体的な操作内容までのアクセスを記録していないものがありました。したがって、導入する ICT 製品・ソフトウェアの機能仕様について、事前にベンダーと確認して個人情報ガイドラインや医療情報システムガイドラインへの対応状況や対応していない場合の運用ルール等による対応策について検討しておくことが重要となります。

介護サービス事業所は、個人情報ガイドラインや医療情報システムガイドラインで求められているセキュリティ対策を十分に理解した上で、事業規模や現在の個人情報の取扱い方も踏まえて、個人データの種類に応じて適切な管理方法を検討し安全対策を講ずる必要があります。導入するソフトウェアや委託先に任せるだけでは個人情報ガイドラインや医療情報ガイドラインには適合できないということを踏まえ、事業者自らの運用管理規程の見直し、導入する ICT 製品・ソフトウェアの機能の整理、システム管理委託先の業者との委託契約内容の精査を行い、できる限り安全対策が講ぜられるよう検討する必要があります。

ICT 製品・ソフトウェアを導入する際にセキュリティの安全対策を検討する内容として、

- 組織規程や運用管理規程、入退室管理、機器や装置等の保護等、介護サービス事業所として対応を検討すべきもの
- 導入する ICT 製品・ソフトウェアの機能により対応可能なもの
- ICT 製品・ソフトウェアの機能では対応できない事項については運用において代替が可能なもの
- 委託先の監督、契約内容において対応を検討すべきもの

に大きく分けられます。医療ガイドラインの情報システムの基本的な安全管理のうち、最低限遵守をすべき項目について抜粋し、上記の検討の範囲を参考資料に記載しています。具体的な対応項目について検討をする際の参考としてください。