

## 7.2 見読性の確保について

### A. 制度上の要求事項

保存義務のある情報の見読性が確保されていること。

- 情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。
- 情報の内容を必要に応じて直ちに書面に表示できること。

(施行通知 第二 2 (3) ①)

### B. 考え方

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること。必要に応じてとは、「診療」、「患者への説明」、「監査」、「訴訟」等に際して、それぞれの目的に支障のない応答時間やスループットと、操作方法でということである。特に監査の場合においては、監査対象の情報の内容を直ちに書面に表示できることが求められている。

電子媒体に保存された情報は、そのままでは見読できず、また複数媒体に分かれて記録された情報の相互関係もそのままでは判りにくい。また、その電子媒体から情報を取り出すには何らかのアプリケーションが必要であり、表示のための編集前提となるマスタ、利用者テーブル等が別に存在したりする可能性がある。これらの見読化手段が日常的に正常に動作することが求められる。

また、必要な情報を必要なタイミングで正当な情報利用者に提供できなかつたり、記録時と異なる内容で表示されたりすることは、重大な支障となるので、それを防ぐためのシステム全般の保護対策が必要であるが、見読性の観点では、何らかのシステム障害が発生した場合においても診療に重大な支障が無い最低限の見読性を確保するための対策が必要である。

さらに、「診療」、「患者への説明」時に求められる見読性は、主治医等の医療従事者に対して保障されるべきものであり、緊急時等においても、医療従事者が診療録等を閲覧するために、必ず医療従事者以外の許可を求める必要がある等の制約はあってはならない。

### C. 最低限のガイドライン

電子媒体に保存された全ての医療情報等が、見読目的に支障のない応答時間やスループットと操作方法で見読可能であることと、システム障害においてもバックアップシステム等により診療に致命的な支障が起きない水準で見読出来ることが必要である。

#### (1) 情報の所在管理

紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。

## (2) 見読化手段の管理

電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。

## (3) 見読目的に応じた応答時間とスループット

### 1. 診療目的

- ① 外来診療部門においては、患者の前回の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。
- ② 入院診療部門においては、入院中の患者の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。

### 2. 患者への説明

- ① 患者への説明が生じた時点で速やかに検索表示もしくは書面に表示できること。なお、この場合の“速やかに”とは、数分以内である。

### 3. 監査

- ① 監査当日に指定された患者の診療録等を監査に支障のない時間内に検索表示もしくは書面に表示できること。

### 4. 訴訟等

- ① 所定の機関より指定された日までに、患者の診療録等を書面に表示できること。
- ② 保存場所が複数ある場合、各保存場所毎に見読手段を用意し、その操作方法を明示すること。

## (4) システム障害対策としての冗長性の確保

システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化や代替的な見読手段を用意すること。

## (5) システム障害対策としてのバックアップデータの保存

システムの永久的ないし長時間障害対策として、日々バックアップデータを採取すること。

## D. 推奨されるガイドライン

最低限のガイドラインに加え、障害対策として下記の対策が講じられることが望ましい。

### (1) バックアップサーバ

システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

### (2) 見読性を確保した外部保存機能

システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。

### (3) 遠隔地のデータバックアップを使用した検索機能

大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

### 7.3 保存性の確保について

#### A. 制度上の要求事項

保存義務のある情報の保存性が確保されていること。

- 法令に定める保存期間内、復元可能な状態で保存すること。

(施行通知 第二 2 (3) ③)

#### B. 考え方

保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、下記のものが考えられる。

- (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等
- (2) 不適切な保管・取扱いによる情報の滅失、破壊
- (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取り
- (4) 媒体・機器・ソフトウェアの整合性不備による復元不能

これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

#### (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等

ウイルスまたはバグ等によるソフトウェアの不適切な動作により、電子的に保存された診療録等の情報が破壊される恐れがある。このため、これらの情報にアクセスするウイルス等の不適切なソフトウェアが動作することを防止しなければならない。

また、情報を操作するソフトウェアが改ざんされていないこと、及び仕様通りに動作していることを確認しなければならない。

さらに、保存されている情報が、改ざんされていない情報であることを確認できる仕組みを設けることが望ましい。

#### (2) 不適切な保管・取扱いによる情報の滅失、破壊

電子的な情報を保存している媒体が不適切に保管されている、あるいは、情報を保存している機器が不適切な取扱いを受けているために、情報が滅失してしまうか、破壊されてしまうことがある。このようなことが起こらないように、情報が保存されている媒体及び機器の適切な保管・取扱いが行われるように、技術面及び運用面での対策を施さなければならない。また、電子的な情報を保存している媒体又は機器が置かれているサーバ室等への入室は、許可された者以外が行えないような対策を施す必要

がある。

また、万が一、紛失又は破壊が起こった場合に備えて、定期的に診療録等の情報のバックアップを作成し、そのバックアップを履歴とともに管理し、元の情報が改ざんまたは破壊された場合には、そのバックアップから診療録等の情報を復元できる仕組みを備える必要がある。この際に、バックアップから情報を復元する際の手順と、復元した情報を診療に用い、保存義務を満たす情報とする際の手順を明確にしておくことが望ましい。

### (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取り

記録媒体、記録機器の劣化による読み取り不能または不完全な読み取りにより、電子的に保存されている診療録等の情報が減失してしまうか、破壊されてしまうことがある。これを防止するために、記憶媒体や記憶機器の劣化特性を考慮して、劣化が起こる前に新たな記憶媒体や記憶機器に複写する必要がある。

### (4) 媒体・機器・ソフトウェアの整合性不備による復元不能

媒体・機器・ソフトウェアの整合性不備により、電子的に保存されている診療録等の情報が復元できなくなることがある。具体的には、システムの移行時のマスタ DB、インデックス DB の不整合、機器・媒体の互換性不備による情報復元の不完全・読み取り不能等である。このようなことが起こらないように、業務継続計画をきちんと作成する必要がある。

## C. 最低限のガイドライン

保存性を脅かす原因を除去するために真正性、見読性の最低限のガイドラインで述べた対策を施すこと及び以下に述べる対策を実施することが必要である。

### (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止

1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。

### (2) 不適切な保管・取扱いによる情報の減失、破壊の防止

1. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。
2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バック

アップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。

3. サーバの設置場所には、許可された者以外が入室できないような対策を施すこと。
4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。
5. 各保存場所における情報が破損した時に、バックアップされたデータを用いて破損前の状態に戻せること。もし、破損前と同じ状態に戻せない場合は、失われた範囲が容易にわかること。

### (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止

1. 記録媒体の劣化する以前に情報を新たな記録媒体または記録機器に複写すること。記録する媒体及び機器毎に劣化が起こらずに正常に保存が行える期間を明確にし、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体または記録機器については、そのデータを新しい記録媒体または記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。

### (4) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止

1. システムの変更に際して、以前のシステムで蓄積した情報の継続的利用を図るための対策を実施すること。システム導入時に、契約等でシステム導入業者にデータ移行に関する情報開示条件を明確にし、旧システムから新システムに移行する場合に、システム内のデータ構造が分からないことに起因するデータ移行の不能を防止すること。開示条件には倒産・解散・取扱い停止などの事態にも対応できることを含める必要がある。
2. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。
3. マスタ DB の変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。

## D. 推奨されるガイドライン

保存性を脅かす原因を除去するために、上記の最低限のガイドラインに追加して真正性、見読性の推奨されるガイドラインで述べた対策及び以下に述べる対策を実施することが必要である。

### (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止

1. 電子的に保存された診療録等の情報にアクセスするシステムでは、ウイルス対策

ソフト等を導入し、定期的にウイルスの検出を行い、ウイルスが発見された場合には直ちに駆除すること。また、ウイルス定義ファイルは常に最新の状態に保つように、端末の運用管理を徹底すること。

2. アンチウイルスゲートウェイ等を導入し、院内のシステムにウイルスが侵入することを防止すること。また、ウイルス定義ファイル更新用のサーバを導入する等の方策により、各端末に導入したウイルス対策ソフトの定義ファイル及びバージョンが、常に最新の状態に保たれるようにシステム的な対策を施すこと。

## (2) 不適切な保管・取扱いによる情報の滅失、破壊の防止

1. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。
2. サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。
3. 診療録等のデータのバックアップを定期的を取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。なお、改ざん等による情報の破壊が行われていないことが証明された場合は、元の情報が破壊された場合にその複製を診療に用い、保存義務を満たす情報として扱うこととする。

## (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止

1. 記録媒体に関しては、あるレベル以上の品質が保証された媒体に保存すること。
2. 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1もしくはRAID-5相当のディスク障害に対する対策を取ること。

## 7.4 法令で定められた記名・押印を電子署名で行うことについて

### A. 制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について改変が行われていないかどうかを確認することができるものであること。

（「電子署名及び認証業務に関する法律」 第2条1項）

### B. 考え方

平成11年4月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」においては、法令で署名または記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（平成12年法律第102号。以下「電子署名法」という。）が未整備の状態であったために対象外とされていた。しかし、平成12年5月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書等として、「民事事業者が行う書面の保存等における情報通信の技術の利用に関する法律に基づく厚生労働省令」において指定された文書等においては、Aに示した電子署名によって、記名・押印にかわり電子署名を施すことで、作成・保存が可能となった。

ただし、医療に係る文書等では一定期間、署名を信頼性を持って検証できることが必要である。電子署名は紙媒体への署名や記名・押印とことなり、Aの一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎた場合は検証ができないという特徴がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。

### C. 最低限のガイドライン

法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。

#### (1) 認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと。

1. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いな

くてもAの要件を満たすことは可能であるが、少なくとも同様の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。

2. 「電子署名に係る地方公共団体の認証業務に関する法律」(平成14年法律第153号)に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。

**(2) 電子署名を含む文書全体にタイムスタンプを付与すること。**

1. タイムスタンプは、「タイムビジネスに係る指針—ネットワークの安心な利用と電子データの 安全な長期保存のために—」(総務省、平成16年11月)等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能である事。
2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。
3. タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容に留意しながら適切に対策を講じる必要がある。

**(3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いること。**

1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。

## 8 診療録及び診療諸記録を外部に保存する際の基準

診療録等の保存場所に関する基準は、2つの場合に分けて提示されている。ひとつは電子媒体により外部保存を行う場合で、もうひとつは紙媒体のままで外部保存を行う場合である。さらに電子媒体の場合、電気通信回線を通じて外部保存を行う場合が特に規定されていることから、実際には次の3つに分けて考える必要がある。

- (1) 電子媒体による外部保存をネットワークを通じて行う場合
- (2) 電子媒体による外部保存を磁気テープ、CD-R、DVD-R等の可搬型媒体で行う場合
- (3) 紙やフィルム等の媒体で外部保存を行う場合

医療機関等であれば、電気通信回線を経由して、診療録等を外部機関に保存することが可能とされ、また、「医療情報ネットワーク基盤検討会」の最終報告でそれ以外にも外部保存に係る業務を受託可能な場合が提言されている。しかし、実際に運用する場合には安全管理に関して、技術的にも情報学的にも十分な知識を持つことが求められる。

一方、(2)可搬型媒体で外部保存を行う場合、(3)紙やフィルム等の媒体で外部保存を行う場合については、保存場所を医療機関等に限るものではなく、保存を専門に扱う業者や倉庫等においても、個人情報の保護等に十分留意して、実施することが可能である。

### 8.1 電子媒体による外部保存をネットワークを通じて行う場合

現在の技術を十分活用しかつ注意深く運用すれば、ネットワークを通じて、医療機関等の外部に保存することが可能である。診療録等の外部保存を受託する機関において、真正性を確保し、安全管理を適切に行うことにより、外部保存を委託する医療機関等の経費節減やセキュリティ上の運用が容易になる可能性がある。

電気通信回線を通じて外部保存を行う方法は、先進的で利点が多いが、セキュリティや通信技術及びその運用方法に十分な注意が必要で、情報の漏洩や医療上の問題等が発生し、社会的な不信を招いた場合は、結果的に医療の情報化を後退させ、ひいては国民の利益に反することになりかねず、慎重かつ着実に進めるべきである。

従って、電気通信回線を経由して、診療録等を電子媒体によって外部機関に保存する場合は、安全管理に関して医療機関等が主体的に責任を負い、技術的にも情報学的にも十分な知識を結集して推進して行くことが求められる。

### 8.1.1 電子保存の3基準の遵守

#### A. 制度上の要求事項

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

(外部保存改正通知 第2 1 (1))

#### B. 考え方

医療機関等の内部に電子的に保存する場合に必要な真正性、見読性、保存性を確保することで概ね対応が可能と考えられるが、これに加え、伝送時や外部保存を受託する機関における取扱いや事故発生時の対応について注意する必要がある。

真正性については、第三者が診療録等の外部保存の受託先の機関になりすまして、不正な診療録等を、外部保存の委託元の医療機関等へ転送することは、診療録等の改ざんとなる。また、電気通信回線の転送途中で診療録等が改ざんされないように注意する必要がある。

見読性については、外部機関に保存を行うことは、厳密な意味で見読性の確保を著しく難しくするよう見える。しかし見読性は本来、「診療に用いるのに支障がないこと。」と「監査等に差し支えないようにすること。」の2つの意味があり、これを両方とも満たすことが実質的な見読性の確保と考えてよい。この際、診療上緊急に必要なことが予測される診療録等の見読性の確保については、外部保存先の機関が事故や災害に陥ることを含めた十分な配慮が求められる。

診療に用いる場合、緊急に保存情報が必要になる場合を想定しておく必要がある。電気通信回線を経由して外部に保存するということは、極限すれば必ず直ちにアクセスできることを否定することになる。これは地震やテロ等を考えれば容易に想定できるであろう。

従って、万が一の場合でも診療に支障がないようにするためには、代替経路の設定による見読性を確保しておくだけでは不十分である。

継続して診療を行う場合等、直ちにアクセスすることが必要となるような診療録等を外部に保存する場合には、保存する情報の複製またはそれと実質的に同等の内容をもつ情報を、内部に備えておく必要がある。

また、保存していた情報が毀損した場合等は、保存を受託した機関は速やかに情報の復旧を図らなくてはならない。その際には、「8.1.4 責任の明確化」を参考にしつつ予め責任を明確化しておき、患者情報の確保を第一優先とし、委託機関と受託機関の間で責任の所在、金銭面でのトラブル等が生じないように配慮しておく必要もある。

診療終了後しばらくの間来院が見込まれない患者に係る診療録等、緊急に診療上の必要が生じるとまではいえない情報についても、監査等において提示を求められるケースも想定されることから、できる限りバックアップや可搬型媒体による搬送経路の確保等、ネットワーク障害や外部保存の受託先の機関の事故等による障害に対する措置を行っておくこ

とが望ましい。

保存性については診療録等を転送している途中でシステムが停止したり、障害があつて正しいデータが保存されない場合は、再度、外部保存の委託元の医療機関等からデータを転送する必要がある。その為、外部保存の委託元の医療機関等におけるデータを消去する等の場合には、外部保存の受託先の機関において、改ざんされることのないデータベースへ保存されたことを確認してから行う必要がある。

### C. 最低限のガイドライン

#### (1) 電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保

##### ① 通信の相手先が正当であることを認識するための相互認証をおこなうこと

診療録等のオンライン外部保存の受託先の機関と外部保存の委託元の医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。

##### ② 電気通信回線上で「改ざん」されていないことを保証すること

電気通信回線の転送途中で診療録等が改ざんされていないことを保証できること。なお、可逆的な情報の圧縮・回復ならびにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。

##### ③ リモートログイン制限機能を制限すること

保守目的等のどうしても必要な場合を除き、リモートログインが行なえないように適切に管理されたリモートログインのみに制限する機能を設けなければならない。

#### (2) 電気通信回線や外部保存を受託する機関の障害等による見読性の確保

##### ① 緊急に必要なことが予測される診療録等の見読性の確保

緊急に必要なことが予測される診療録等は、内部に保存するか、外部に保存しても複製または同等の内容を医療機関等の内部に保持すること。

#### (3) 電気通信回線や外部保存を受託する機関の障害等に対する保存性の確保

##### ① 外部保存を受託する機関において保存したことを確認すること

外部保存の受託先の機関におけるデータベースへの保存を確認した情報を受け取ったのち、委託元の医療機関等における処理を適切に行うこと。

##### ② データ形式及び転送プロトコルのバージョン管理と継続性の確保をおこなうこと

保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップまたは変更されることが考えられる。その場合、外部保存の受託先の機関はその区別を行い、

混同による障害を避けるとともに、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間に対応を維持しなくてはならない。

③ 電気通信回線や外部保存を受託する機関の設備の劣化対策をおこなうこと

電気通信回線や受託先の機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策をおこなうこと。

④ 情報の破壊に対する保護機能や復旧の機能を備えること

故意または過失による情報の破壊がおこらないよう、情報保護機能を備えること。また、万一破壊がおこった場合に備えて、必要に応じて回復できる機能を備えること。

#### D. 推奨されるガイドライン

(1) 電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保

① 診療録等を転送する際にメッセージ認証機能を用いること

通信時の改ざんをより確実に防止するために、一連の業務手続内容を電子的に保証、証明することが望ましい。メッセージ認証機能によりメッセージ内容が確かに本人の送ったものであること、その真正性について公証能力、証憑能力を有するものであることを保証する。

なお、メッセージ認証機能の採用に当たっては保存する情報の同一性、真正性、正当性を厳密に証明するためにハッシュ関数や電子透かし技術等を用いることが望ましい。

(2) 電気通信回線や外部保存を受託する機関の障害等による見読性の確保

① 緊急に必要なになるとまではいえない診療録等の見読性の確保

緊急に必要なになるとまではいえない情報についても、ネットワークや受託先の機関の障害等に対応できるような措置を行っておくことが望ましい。

(3) 電気通信回線や外部保存を受託する機関の障害等に対する保存性の確保

① 標準的なデータ形式及び転送プロトコルを採用すること

システムの更新等にもなう相互利用性を確保するために、データの移行が確実にできるように、標準的なデータ形式を用いることが望ましい。

② 電気通信回線や外部保存を受託する機関の設備の互換性を確保すること

回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、受託先の機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム

更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行することが望ましい。