

# プライバシーマネジメントの 確立のために②

## 個人情報保護法と情報システムの安全管理

医療情報システムの安全管理に関する  
ガイドライン(案)による

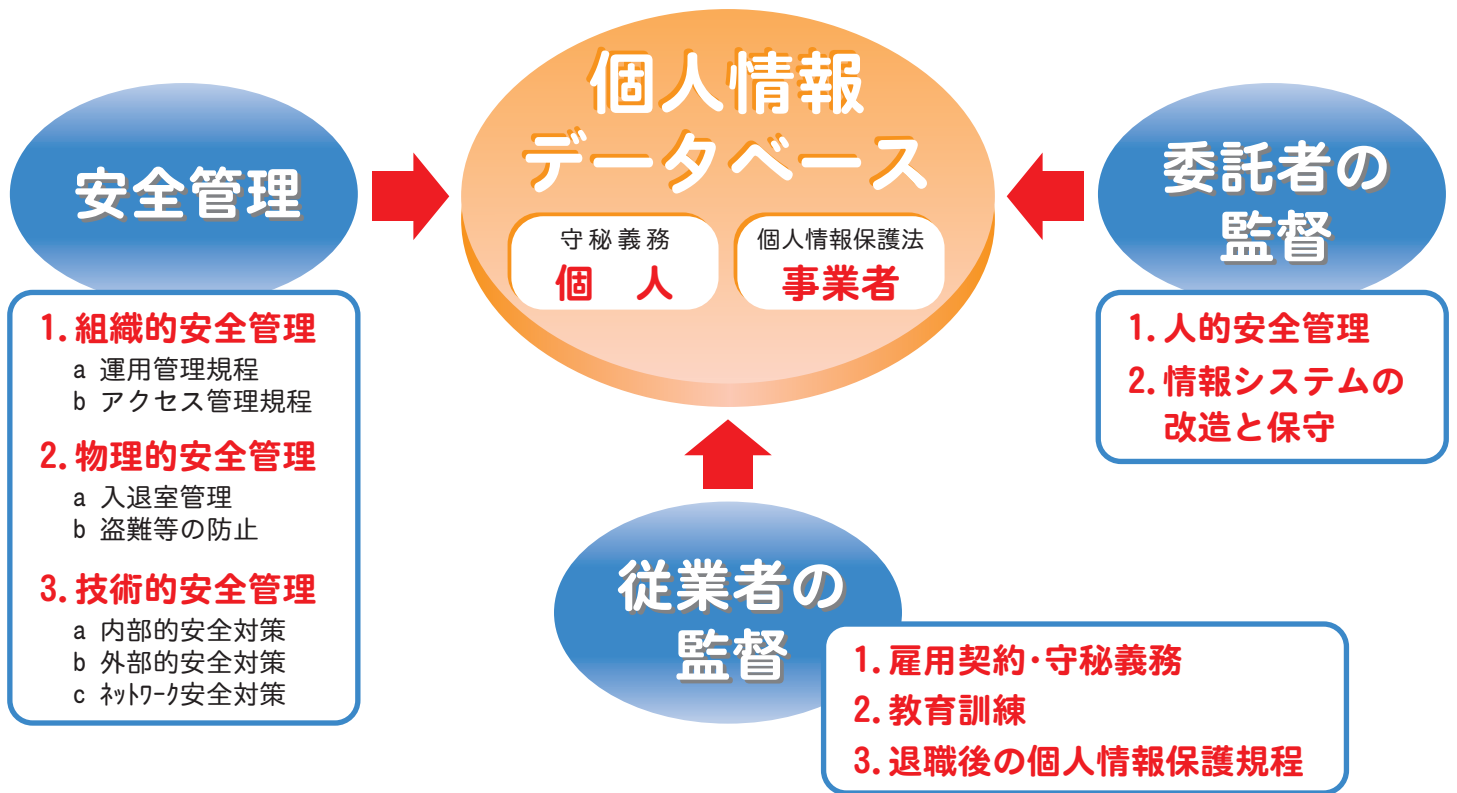
# 目 次

【規程】

・ 情報システムの基本的安全管理□	□P-1	
・ 安全保存□	□P-1	
・ 作成責任の所在の明確化□	□P-2	
・ 運用管理について□	□P-2	— 1章
・ 組織的安全管理対策(体制、運用管理規程)□	□P-3	— 2章
・ 物理的安全対策□	□P-3	— 3章
・ 技術的安全対策①～③□	□P-4～5	— 4章
・ 安全保存(真正性の確保について)□	□P-5	— //
・ 安全保存(見読性の確保について)□	□P-6	— //
・ 安全保存(保存性の確保について)□	□P-6	— //
・ 人的安全対策□	□P-7	— 5章
・ 委託先安全対策□	□P-7	— 6章
・ 情報システムの改造と保守□	□P-8	— //
・ 情報の破棄□	□P-8	— 7章

# 情報システムの基本的安全管理

※情報システムの安全管理の方針の制定と公表  
(安全管理が十分であることの説明責任)



注)当ガイドラインは医療関係者向けに作成されていますが、より高度のセキュリティを構築する為に医療関係者を介護事業者に読み替えて作成してあります。

## 安全保存

電子保存の3基準【通知第2.1.(1)】



保存義務のある情報の真正性が確保されていること。

- 故意または過失による虚偽入力、書換え、消去及び混同を防止すること。
- 作成の責任の所在を明確にすること。

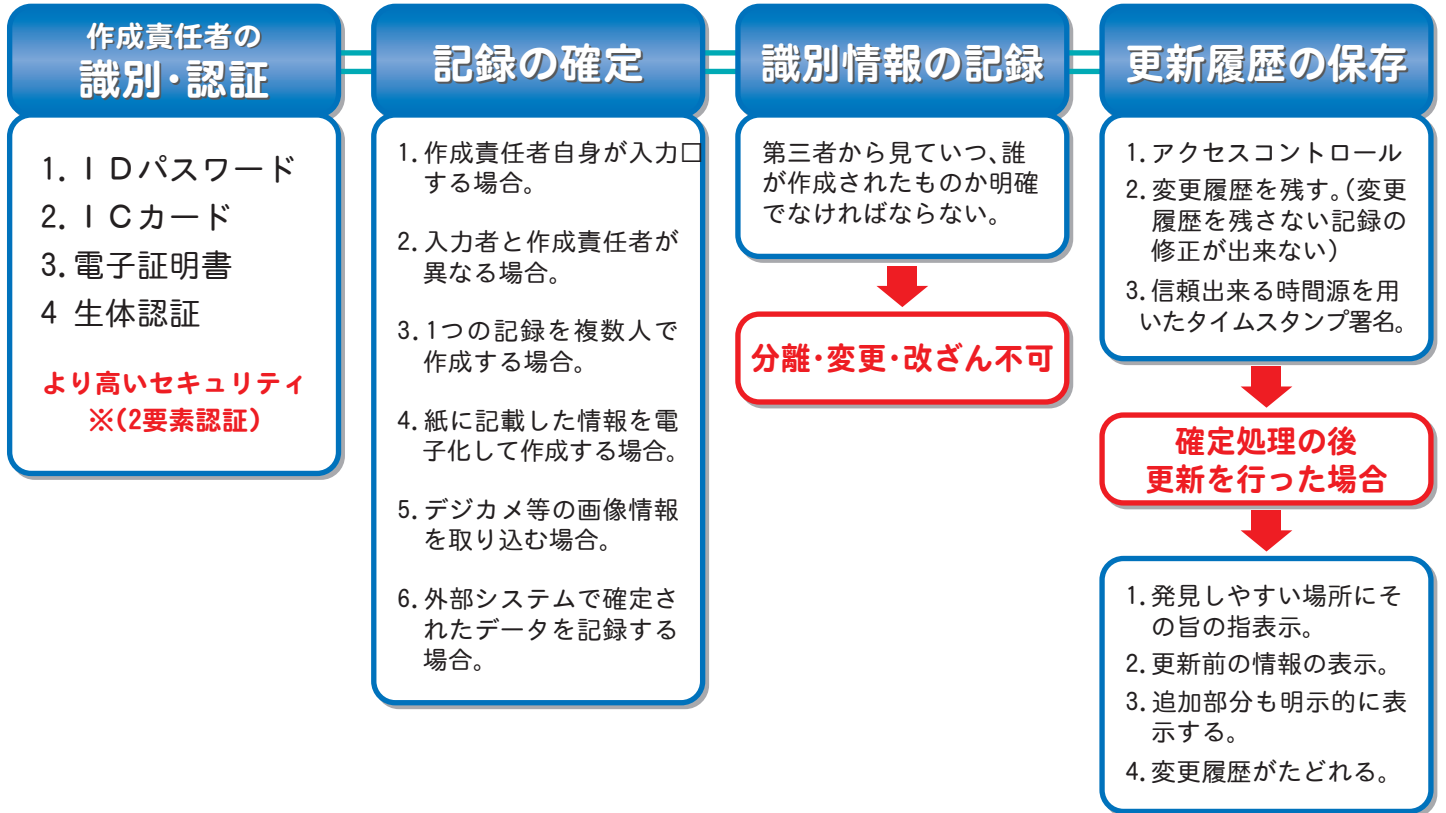
保存義務のある情報の見読性が確保されていること。

- 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。

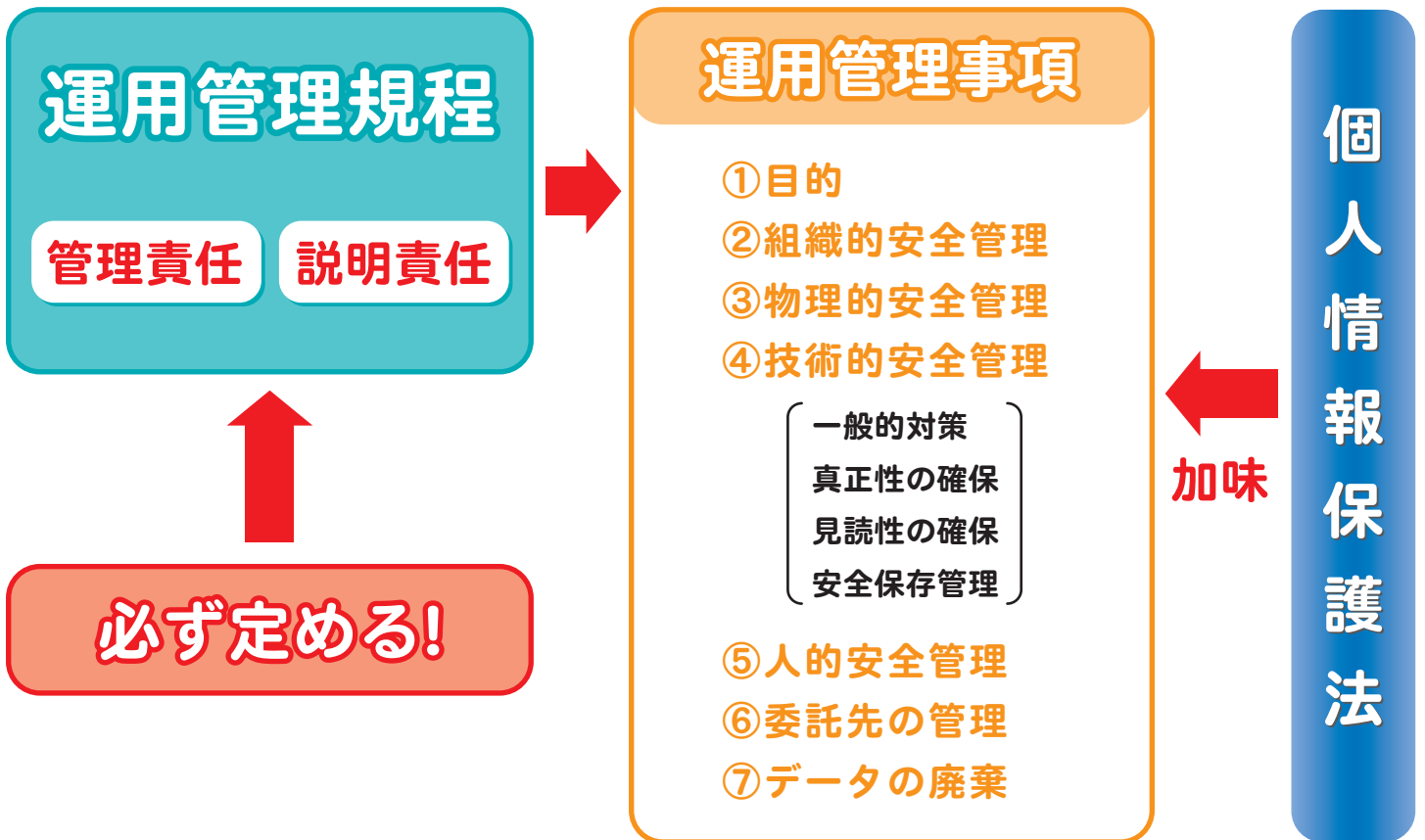
保存義務のある情報の保存性が確保されていること。

- 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。

# 作成責任の所在の明確化



## 1章 運用管理について



## 2章 組織的安全管理対策（体制、運用管理規程）

### 考え方

安全管理について、①従業者の責任と権限を明確に定め、②安全管理に関する規程や手順書を整備運用し、③その実施状況を確認しなければならない。

- (1)安全管理対策を講じるための組織体制の整備
- (2)安全管理対策を定める規程等の整備と規程等に従った運用
- (3)介護情報取り扱い台帳の整備
- (4)介護情報の安全管理対策の評価、見直し及び改善
- (5)事故又は違反への対処

※運用管理規程には必ず以下の項目を含めること。

- ・ 理念
- ・ 利用者等への説明と同意を得る方法
- ・ 事業所内の体制、外部保存に関わる院外の人および施設
- ・ 監査
- ・ 契約書・マニュアル等の文書の管理
- ・ 苦情の受け付け窓口
- ・ 機器を用いる場合は機器の管理

### ガイドライン

1. 情報システム運用責任者の設置及び担当者(システム管理者を含む)の限定を行うこと。
2. 個人情報参照可能な場所においては、来訪者の記録・識別、入退を制限するなどの入退管理を定めること。
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取り扱いを委託する場合、委託契約において安全管理に関する条項を定めること。
5. 運用管理規程等において下記の内容を定めること。
  - (a)個人情報の記録媒体の管理(保管・授受等)の方法について定めた規程
  - (b)リスクに対する予防、発生時の対応の方法。

## 3章 物理的安全対策

### 考え方

物理的安全対策とは、情報システムにおいて個人情報が格納される、コンピュータ、情報媒体等を物理的な方法によって保護することである。

- (1)入退館(室)の管理
- (2)盗難、窃視等の防止
- (3)機器・装置・情報媒体等の物理的な保護

### ガイドライン

1. 個人情報が保管されている機器の設置場所および記録媒体の保存場所には施錠すること。
2. 個人情報の物理的保存を行っている区画への入退管理を実施すること。
  - ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。
  - ・ 入退者の記録を定期的にチェックし、妥当性を確認すること。
3. 個人情報が存在するPCなど重要な機器に盗難防止用チェーンを設置すること。
4. 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

## 4章 技術的安全対策①

### 考え方

- (1)職員への識別および認証□
- (2)アクセス権限の管理
- (3)アクセスの記録□
- (4)不正ソフトウェア対策

### ガイドライン

1. ID、パスワード等により、介護記録データへのアクセスにおける識別と認証を行うこと。
2. 動作確認等で個人データを使用するときは、漏洩等に十分留意すること。
3. 介護施設内の介護従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。
4. アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと。
5. ウィルスなどの不正なソフトウェアの混入を防ぐ適切な措置をとること。

## 4章 技術的安全対策②

### (1)利用者の識別および認証

#### 認証方法

1. ID、パスワード
2. ICカード
3. 電子証明書
4. 生体認証

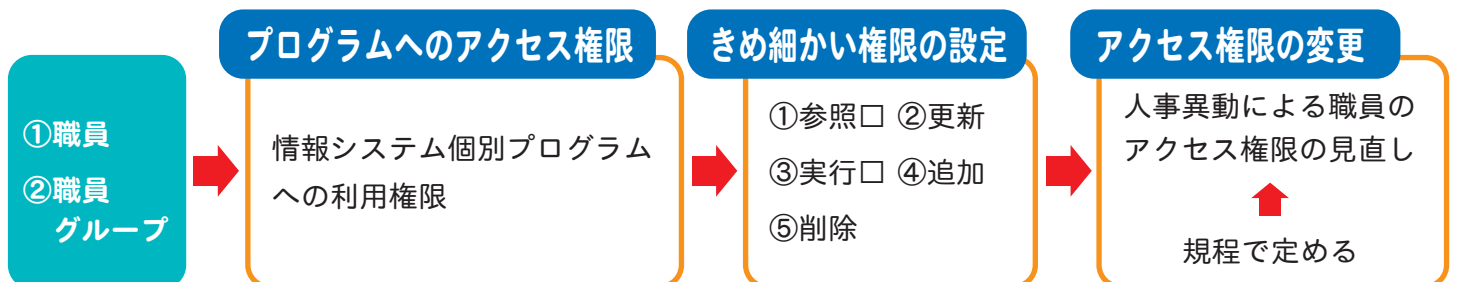
#### リスク

1. ID/パスワードが書かれた紙が貼ってある。
2. パスワードが設定されていない。
3. 容易にパスワードが推測できる。
4. パスワードを定期的に変更しない。
5. ICカード、USBキーを他人に貸与、無断借用で利用者が特定出来ない。
6. 退職した職員のIDが有効になったままである。
7. コンピュータウィルスによりID、パスワードが盗まれる。
8. 代行作業者にパスワードを教えている。
9. 端末から離席した時に他人に使用される。

#### 対策

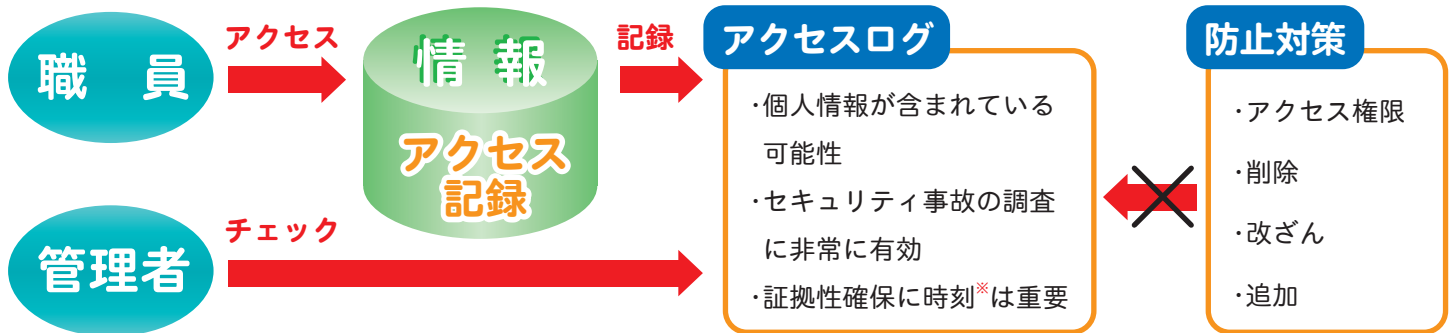
1. 2要素認証
2. スクリーンロック
3. ID、パスワードが本人以外に利用されない対策
4. 緊急時の代替アクセスルールの確立

### (2)アクセス権限の管理



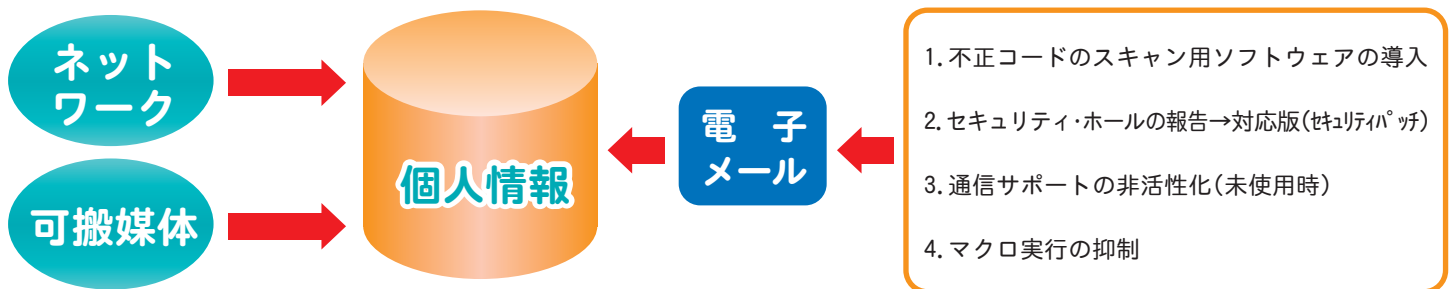
## 4章 技術的安全対策③

### (3) アクセスの記録(アクセスログ)

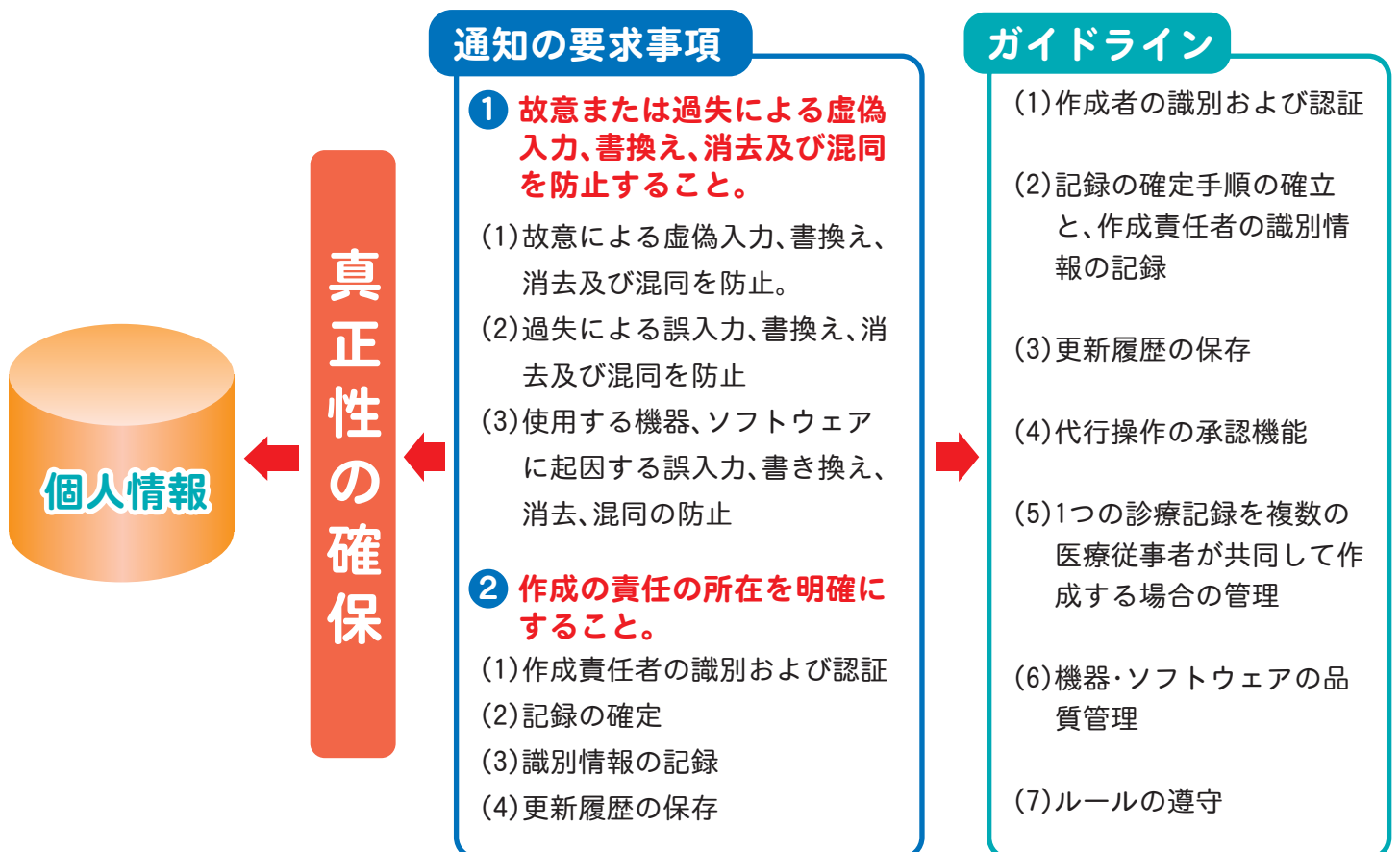


※時刻は組織内全てのシステムで同期をとる。

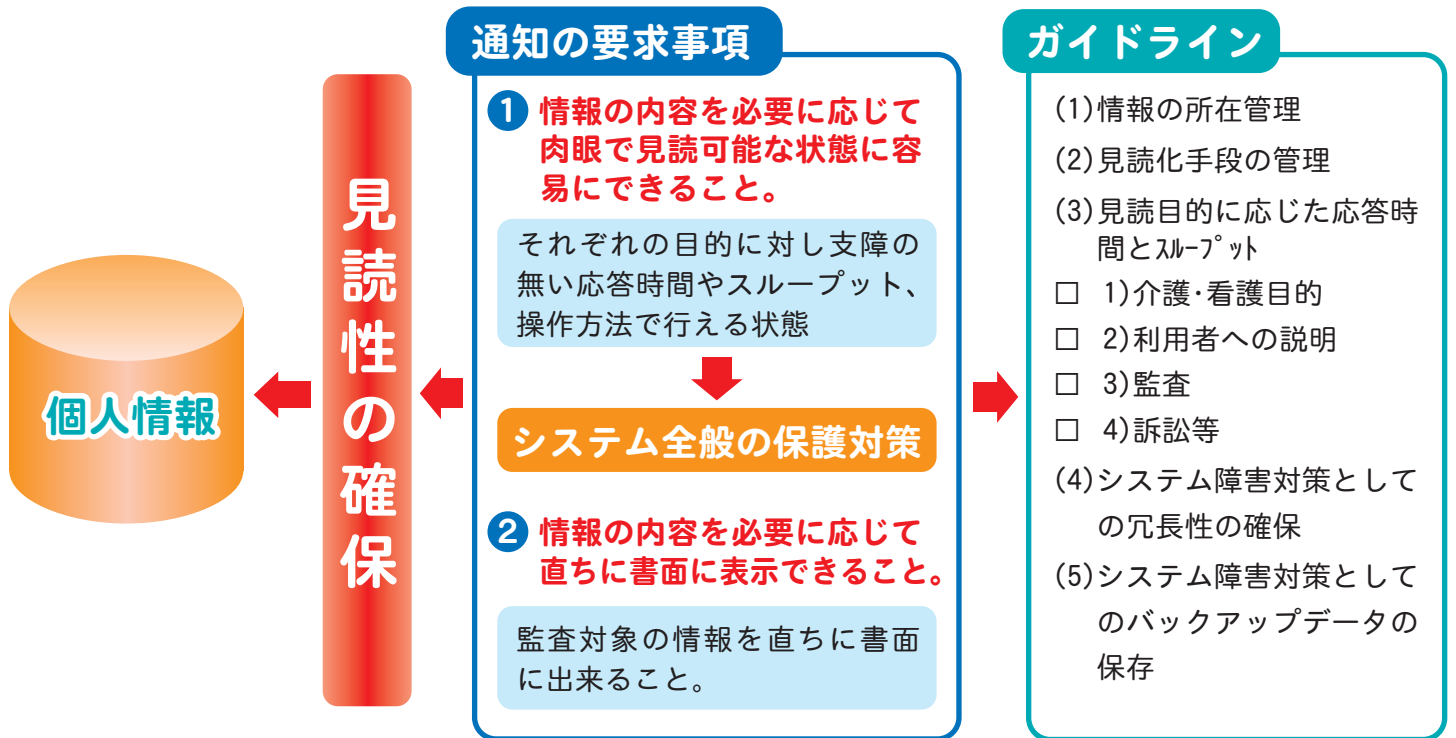
### (4) 不正ソフトウェア対策



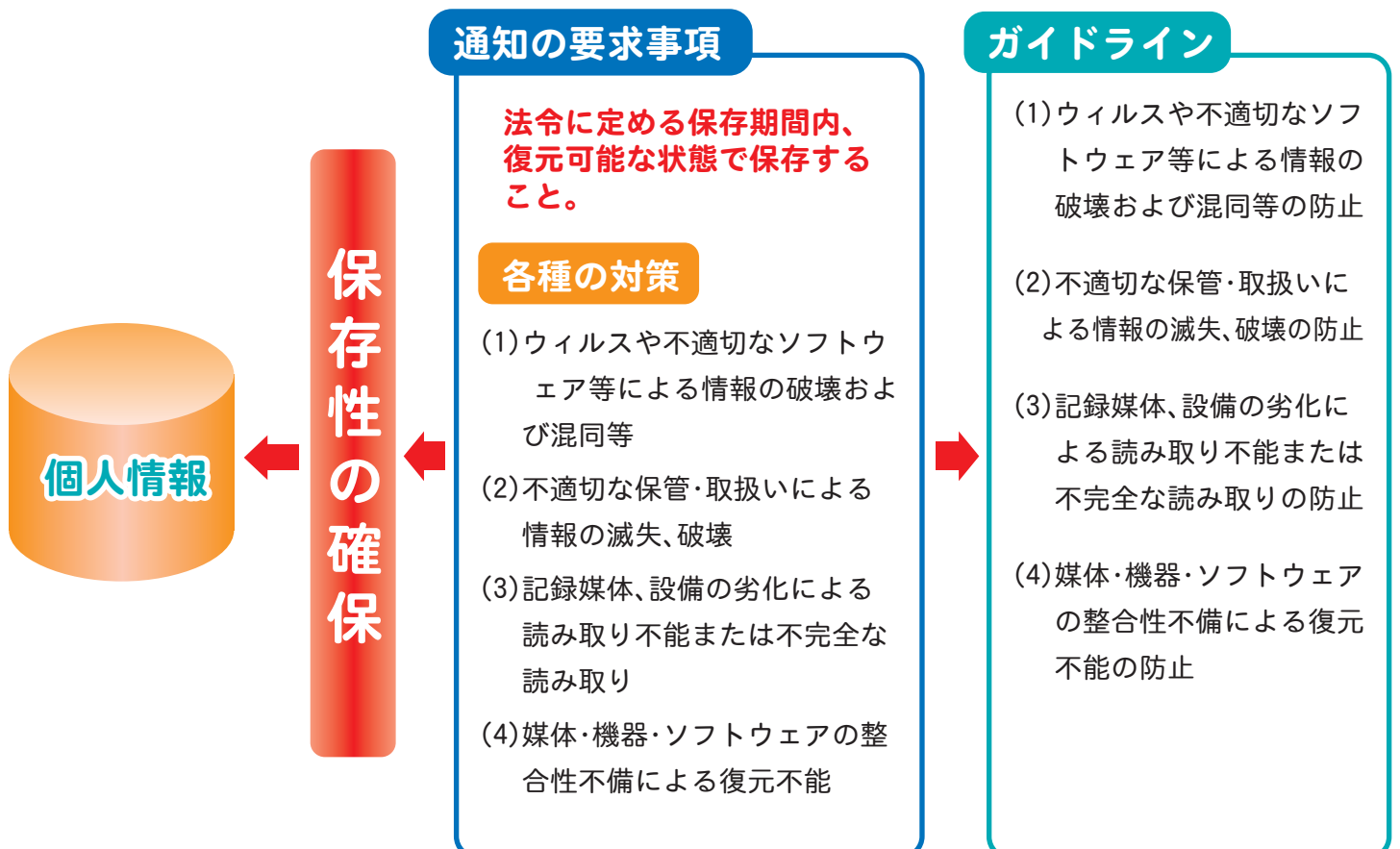
## 4章 安全保存 (真正性の確保について)



## 4章 安全保存（見読性の確保について）



## 4章 安全保存（保存性の確保について）



## 5 章 人的安全対策

### 考え方

- (a) 介護業務で介護情報を取り扱い、法令上の守秘義務のある者
- (b) 職員、その事務委託者など介護するための業務に携わり、雇用契約の元に個人情報を取り扱い、守秘義務を負う者
- (c) システムの保守業者など雇用契約を結ばずに個人情報を維持するための業務に携わる者
- (d) 利用者、訪問客など、個人情報にアクセスする権限を有しない第三者
- (e) 個人情報の外部保存の委託においてデータ管理業務に携わる者

### 従業者に対する人的安全管理措置



### ガイドライン

1. 介護従事者以外の事務職員の採用にあたっては、雇用及び契約時に守秘・非開示契約を締結することなどにより安全管理を行うこと。
2. 定期的に従事者に対し教育訓練を行うこと。
3. 従事者の退職後の個人情報保護規程を定めること。

## 6 章 委託先安全対策

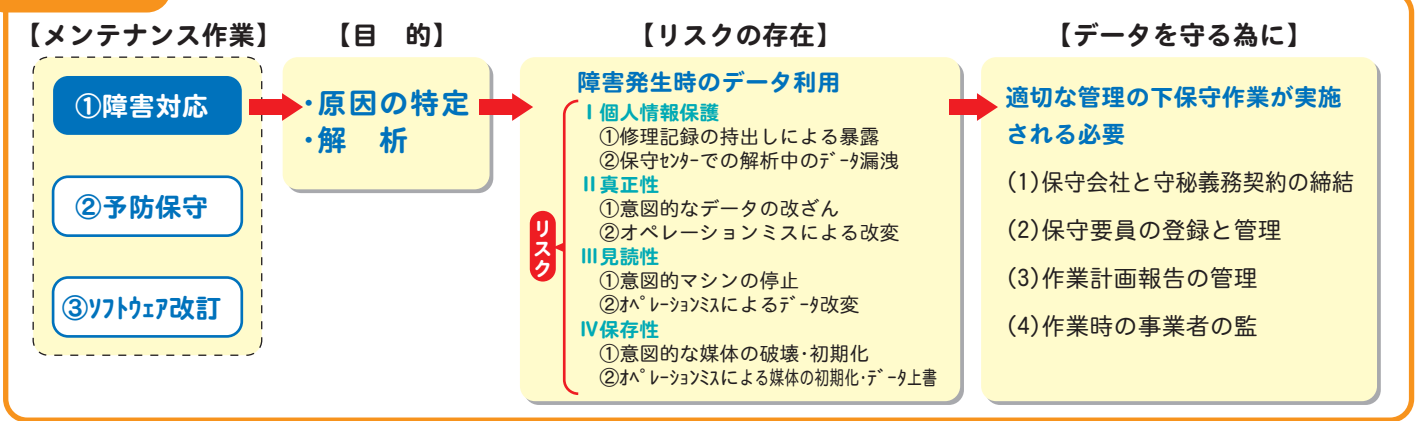
### 事務取扱委託業者の監督及び守秘義務契約

### ガイドライン

1. プログラムの異常等で、保存データを救済する必要があるときなどやむをえない事情で事務、運用等で、**外部受託業者**を採用する場合は、施設内における適切な個人情報保護が行われるように、以下のような措置を行うこと。
  - (1) 包括的な委託先の罰則を定めた就業規則等で裏づけられた**守秘契約**を締結すること。
  - (2) 保守作業など電子保存システムに直接アクセスする作業の際には、**作業者・作業内容・作業結果**の確認を行うこと。
  - (3) 清掃など、直接電子保存システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
  - (4) 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は**委託先と同等の個人情報保護に関する対策**および**契約**がなされていることを条件とすること。
2. プログラムの異常等で、保存データを救済する必要があるときなど、やむをえない事情で**外部の保守要員**が個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた**守秘契約**等の秘密保持の対策を行うこと。

# 6章 情報システムの改造と保守

## 考え方



## ガイドライン

- (1) 守秘義務** …… 1. 保守会社と個人情報保護に関する契約を締結しこれを遵守させること。  
2. 保守会社の取扱い者との守秘義務契約を確認する。  
3. 動作確認で個人データを使用するときは、明確な守秘義務の設定と、終了後の確実なデータの消去を求めること。
- (2) 保守要員の登録と管理** 1. サーバーに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、作業記録を残すこと。  
2. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。  
3. 保守要員の離職や担当変更等に対して保守用アカウントを削除できるよう、報告を義務付けまた、アカウント管理体制を整えておくこと。
- (3) 作業計画報告の管理** メンテナンスの際、日単位に作業申請の事前提出、終了時業報告書の提出を求めること。事業者側の責任者が逐次承認すること。
- (4) 作業時の監督** …… 保守会社の個人情報の組織外持ち出しに対し、置き忘れ等に対し取り扱いの運用管理規程を定めさせること。事業所側
- (5) 組織外持ち出し** …… 責任者が逐次承認すること。
- (6) リモートメンテ** …… リモート保守によるシステムの改造や保守が行われる場合、必ずメッセージログを採取し、事業所側責任者が確認すること。
- (7) 再委託** …… 再委託が行われる場合は再委託先にも保守会社と同等の義務を課すこと。

# 7章 情報の破棄

## 考え方

介護に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報がお互いに関連して存在する場合は一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もある。実際の廃棄に備えて、事前に廃棄プログラムなどの手順を明確化したものを作成しておくべきである。

## ガイドライン

- 1. 情報種別ごとに廃棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業員の特定、具体的な破棄の方法を含めること。
- 2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。
- 3. 破棄を外部事業者へ委託した場合は、「事務取扱委託事業者の監督及び守秘義務契約」に準じ、さらに委託者が確実に情報の破棄が行われたことを確認する事。
- 4. 運用管理規程において下記の内容を定めること。