

秘密分散バックアップした医療データの 部分復元システムとその安全性評価

2017/2/8

1195064 田中麻実

工学専攻科 基盤工学専攻

情報システム工学コース

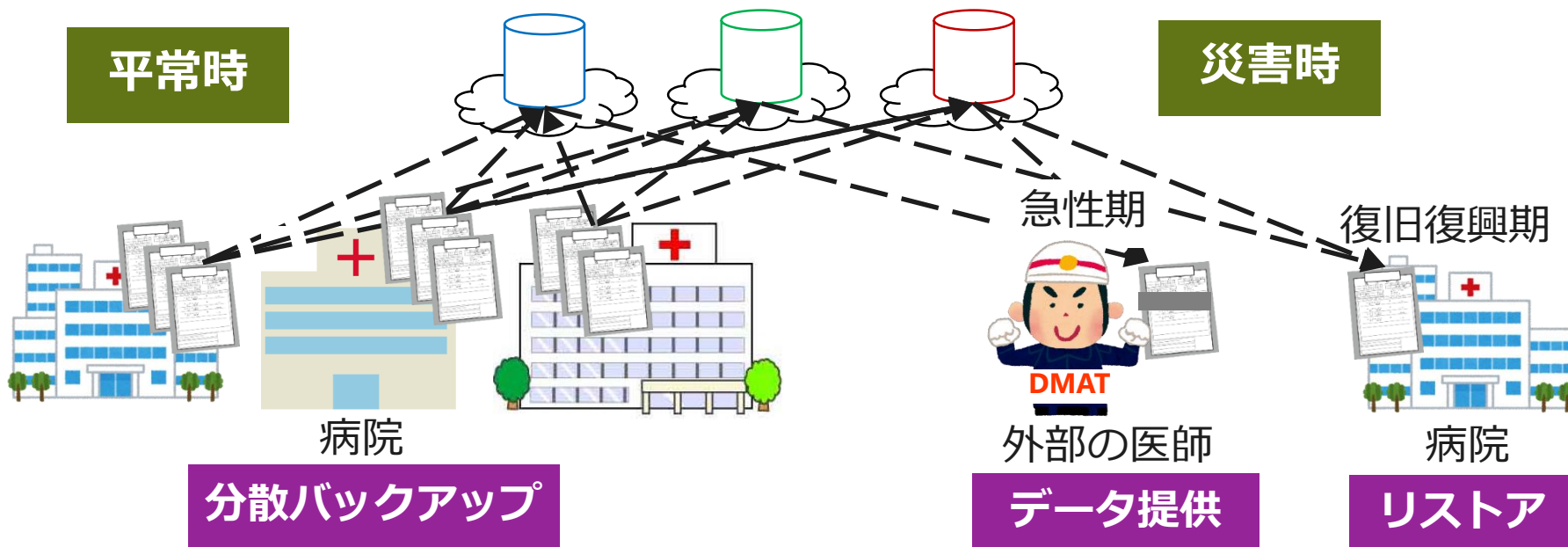
ネットワーク信号処理研究室

背景

- ・ 広域災害によって電子カルテなどの医療データが流出
被災地での医療行為に支障



- ・ 医療データを遠隔地に分散バックアップ
 - 秘密分散法を用いる研究
- ・ 被災地での医療行為にバックアップした医療データ活用



医療データを被災地で活用するための要件³

- 医療データは個人情報
 - 提供する情報の制限
 - 医療データ閲覧者の制限
 - 閲覧可能環境の制限
- 災害時医療データを読むシステムが被災しバックアップデータが読めない可能性
 - データの閲覧に特別な機材を必要としない



- 被災地での医療行為に必要な情報のみを提供
不必要な情報の提供を制限

秘密分散バックアップした医療データを
部分復元可能な秘密分散システム

医療データの分散バックアップ

- 医療データは個人情報
病院外に保存するときはデータの秘匿化が必要¹
- バックアップデータの冗長化
➡ 秘匿化と冗長化の両立
- 秘密分散法
 - 分散情報(シェア)は個人情報ではないという見解
(経済産業省)
 - 医療データの分散バックアップに
秘密分散法を用いた研究²

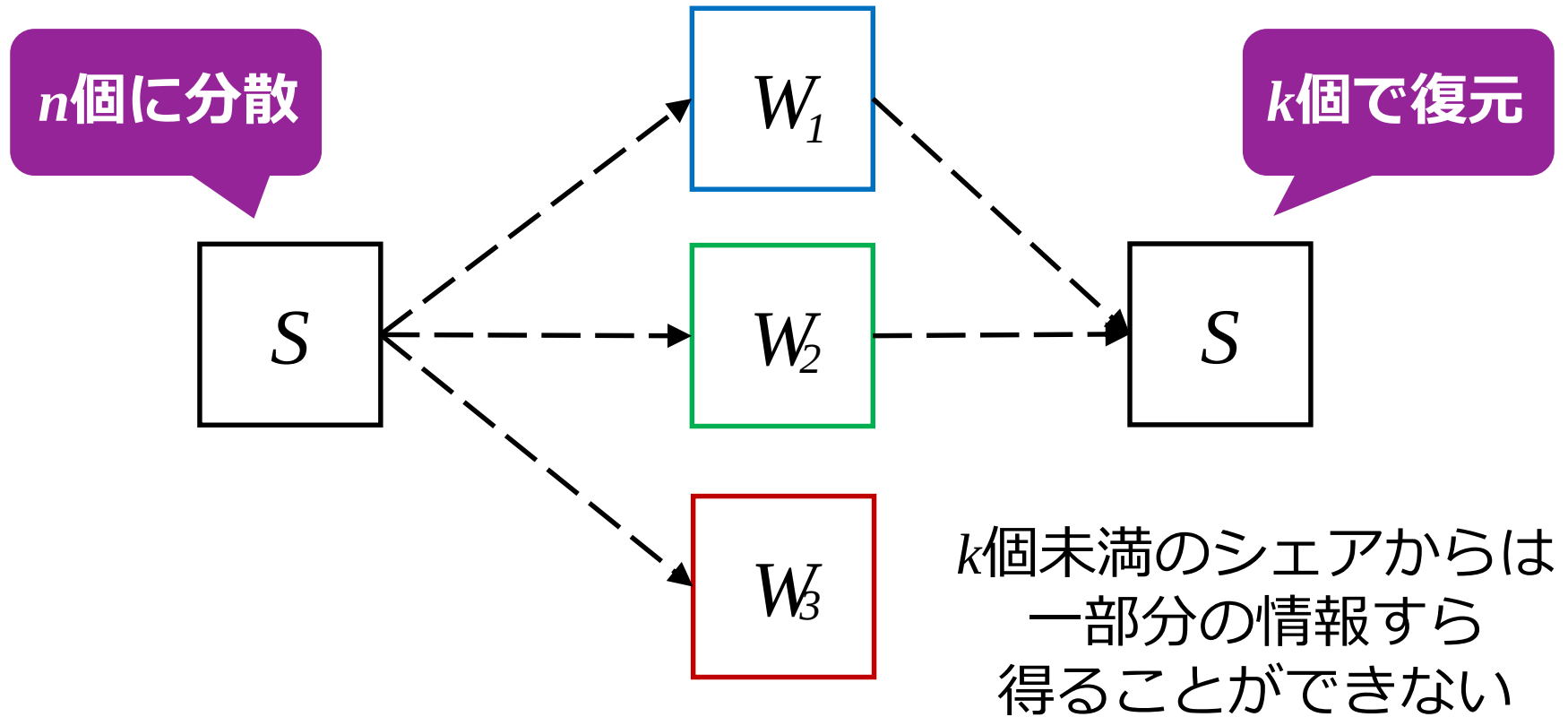
医療データの分散バックアップに秘密分散法を用いる

¹医療情報システムの安全管理に関するガイドライン第4.3版H28.3厚生労働省

²医療サービスの継続性を担保する電子カルテ秘密分散バックアップ技術の研究開発
(愛媛大学, 大阪大学, 京都大学, 兵庫医師大学, 福井大学)

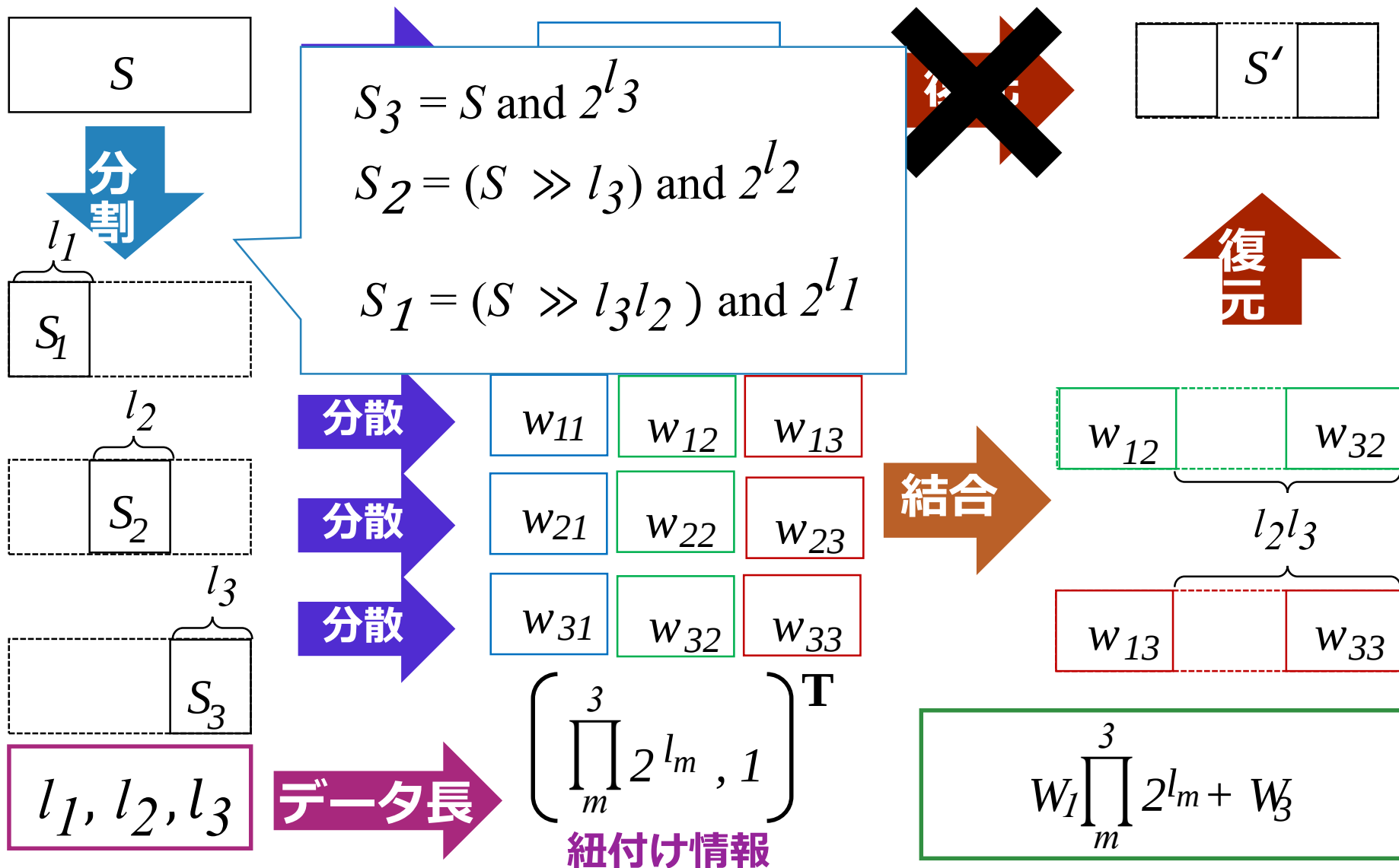
(k,n) しきい値秘密分散法

- データの秘匿化・冗長化が可能



部分復元アルゴリズム

- 秘密分散法は部分的に復元できない



部分復元アルゴリズムの評価

- 紐付け情報を用いて復元できる情報を制限
 1. 提供する情報の制限
 2. 医療データ閲覧者の制限
 3. 閲覧可能環境の制限
 4. データの閲覧に特別な機材を必要としない

- 紐付け情報
 - データ形式が既知である場合作成可能
 - 医療データのデータ形式は既知
- シェア
 - ネットワーク上に存在

不正復元の可能性

紐付け情報の作成とシェアの入手を制限

紐付け情報の作成とシェアの入手を制限

部分復元制御データにより**不正復元を防止**

紐付け情報

シェアを入手する権限
復元スクリプト など



復元PC

シェアストレージ群

シェアを結合
してから配付

結合済シェア

- 紐付け情報で結合済シェア操作不可
- シェアの入手に制御データ必要

➡ **紐付け情報の作成とシェアの入手を制限**

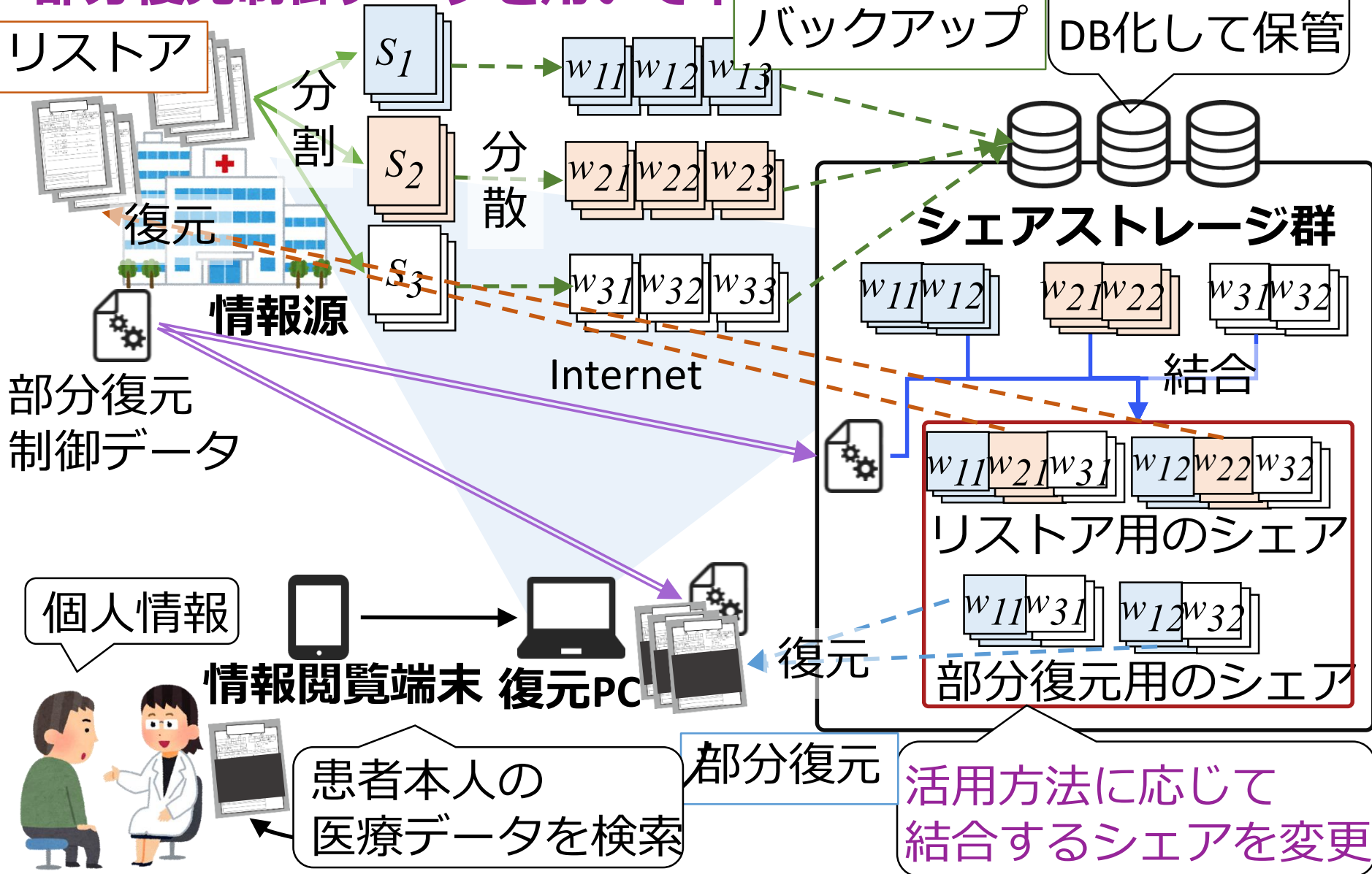
部分復元可能な秘密分散システム

部分復元制御データを用いて不

秘密分散
バックアップ

シェアを
DB化して保管

リストア



部分復元
制御データ

Internet

シェアストレージ群

結合

リストア用のシェア

部分復元用のシェア

個人情報

情報閲覧端末 復元PC

復元

部分復元

患者本人の
医療データを検索

活用方法に応じて
結合するシェアを変更

部分復元可能な秘密分散システムの評価

10

部分復元制御データにより不正復元を防止

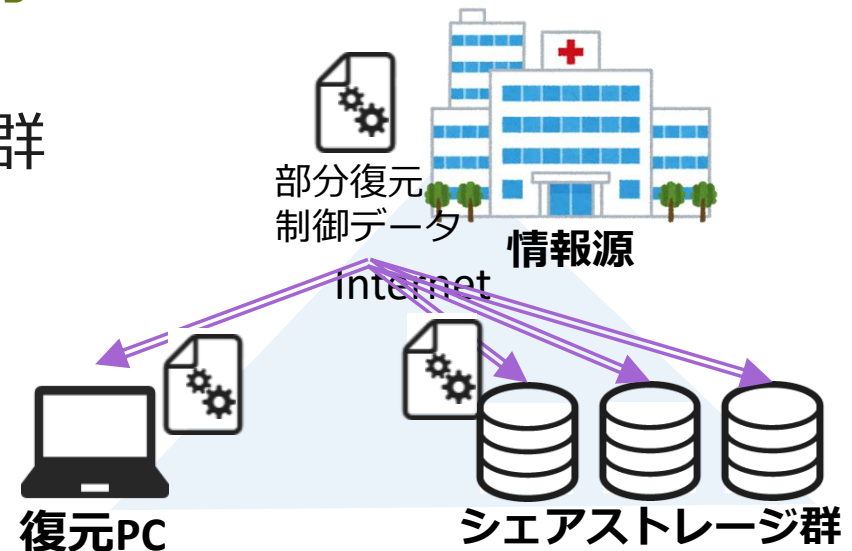
復元PC・情報閲覧端末により復元する環境・閲覧者を制限

1. 提供する情報の制限
2. 医療データ閲覧者の制限
3. 閲覧可能環境の制限
4. データの閲覧に特別な機材を必要としない

・部分復元制御データの不正入手

- 部分復元制御データの配付
- 復元PC・シェアストレージ群

➡ 部分復元制御データの不正入手を防ぐ要件



部分復元制御データの不正入手を防ぐ要件¹¹

- 部分復元制御データの不正入手が発生する条件

- 配付相手が不当
- 盗聴・盗難対策なし
- 誰でも端末を操作可能

部分復元制御データの不正入手が発生しない条件

盗聴・盗難対策		有	無
端末・操作者	侵入検知		
正当	無		
	有		
不当	有		
	無		

- 部分復元制御データの不正入手を防ぐ要件

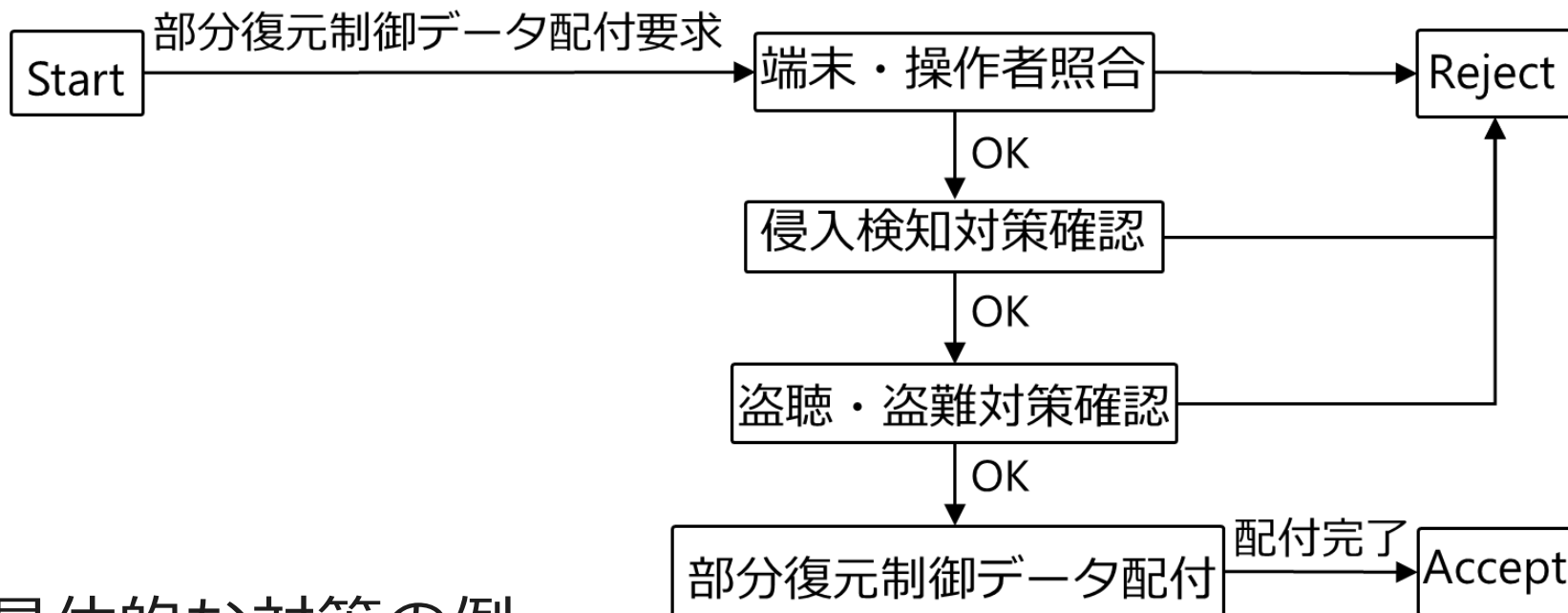
(「端末」⇔「登録端末」)∧

(「端末操作者」⇔「登録端末」)∧

「侵入検知」∧「盗聴盗難対策」⇒「事前情報配付」

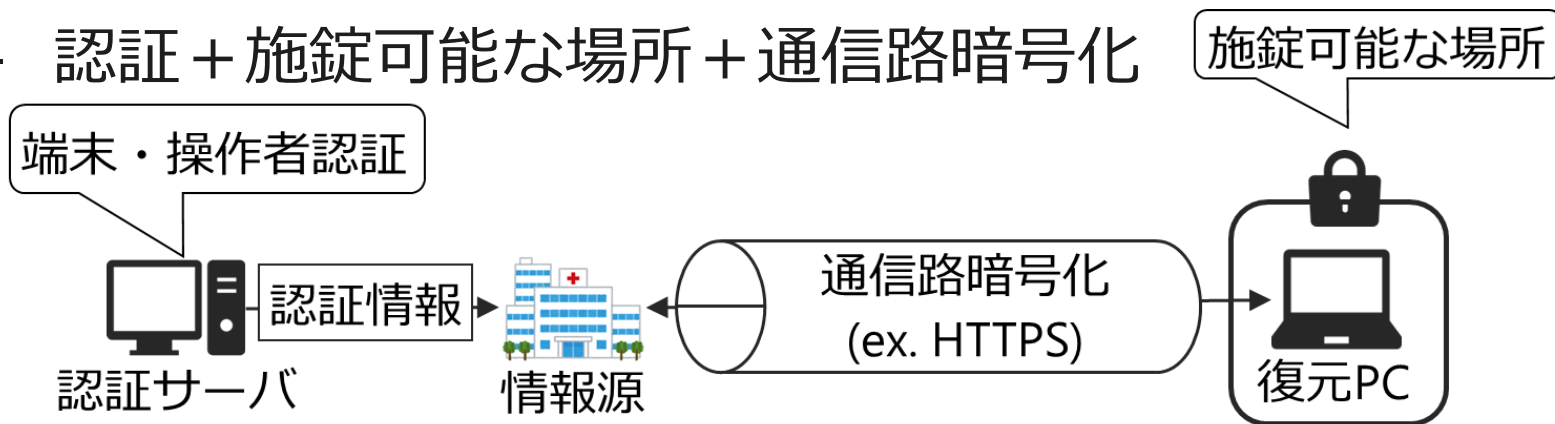
不正入手を防ぐ要件を満たす対策

• 要件を満たす状態遷移



• 具体的な対策の例

- 認証 + 施錠可能な場所 + 通信路暗号化



まとめ

- バックアップした医療データを被災地での医療行為に活用
- 医療データを活用する際の要件
 1. 提供する情報の制限
 2. 医療データ閲覧者の制限
 3. 閲覧可能環境の制限
 4. データの閲覧に特別な機材を必要としない
- 部分復元可能な秘密分散システム
 - 部分復元制御データを用いて情報と不正復元防止
 - システムでの不正復元を防ぐ要件
- 今後の課題
 - ビューワースの設計