BNCTプロジェクトにおける医療情報セキュアデータベースの構築

Secure database for medical information in the BNCT project

岡山大学　自然科学研究科　野上 保之　横平 徳美　山内 利宏　福島 信行　日下 卓也
岡山大学　中性子医療研究センター　市川 康明
岡山大学　医歯（薬）学総合研究科　冨田 秀太
岡山大学　情報統括センター　河野 圭太

BNCTプロジェクト

ホウ素中性子捕捉療法（BNCT）

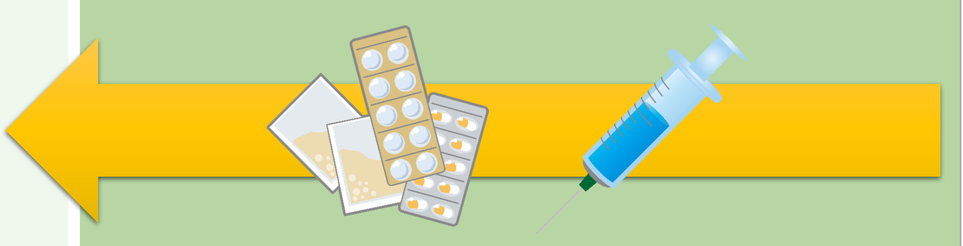
岡山大学医学部が研究を進める
次世代のがん治療法

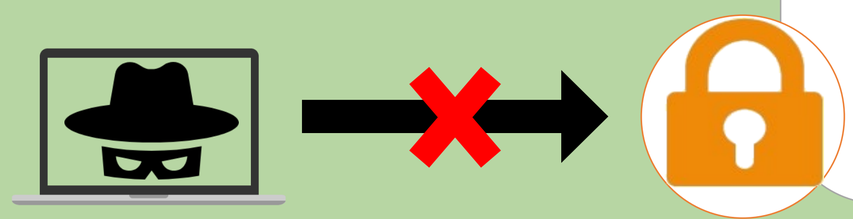
ホウ素原子を
がん細胞に導入
→ 中性子線を照射
→ がん細胞内部で
核分裂を起こす
→ がん細胞が破壊する

正常細胞への影響が少ない

医療 × ICT

- 医療情報のビッグデータ活用
- 医療データ保護のための暗号技術





医療データ

個人情報　カルテ

CT画像　ゲノム情報

セキュアデータベースのサーバ・クライアントモデル

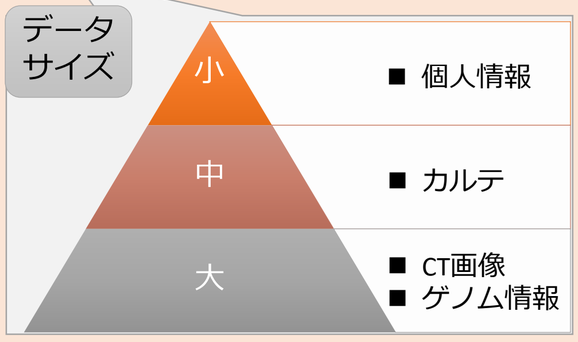
クライアント

インターフェース

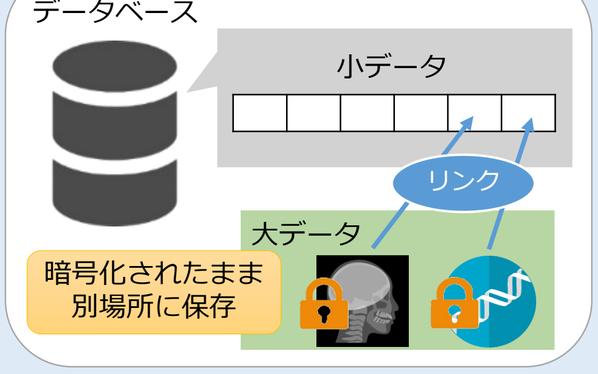
	ブラウザ	ネイティブアプリ
汎用性	◎	△
処理速度	○	◎
プログラミング言語	JavaScript WebAssembly	C / C++ / C# Java

医療データの暗号化 & 復号　＋　ユーザ認証 (e.g. PPV)

データサイズ



サーバ

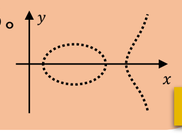


医療データを分散して
データベースサーバに保存
→ データ消失リスク減

暗号技術

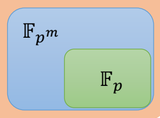
楕円曲線暗号（ECC）

楕円曲線上の離散対数問題（ECDLP）を利用した暗号。短いビット長で高強度の暗号化が行える。



CVMA

循環ベクトル乗算アルゴリズム（CVMA）による離散対数問題（DLP）を利用する。



AES

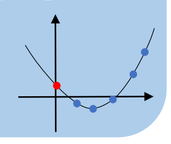
現在最も広く利用されている共通鍵暗号アルゴリズム。高速な暗号化が行える。

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

分散技術

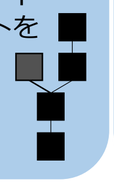
(k,n)しきい値秘密分散法

秘密情報を n 個に分割する。そのうち k 個を使用すると、秘密情報を復元できる。



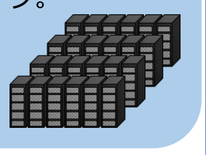
ブロックチェーン

分散型台帳技術。
順序つけられたレコード（ブロック）のリストを保存している。



Hadoop

大規模データの分散処理を支えるソフトウェアフレームワーク。



小データの暗号化

複数のデータをまとめて暗号化が行える
岡大発 **ECC & CVMA** を使用

岡大発 ECC

- 拡大体を用いて、任意のビット長のデータで高ビット強度のECCを実現できる
- 高速に暗号化を行う
- サイドチャンネル攻撃の耐性が高い

岡大発 CVMA

- 拡大体上での高速な乗算アルゴリズム
- 世界最高速のアルゴリズムを提案

ECC 暗号化手順

1. データを楕円曲線上の有理点に変換する
2. 秘密鍵を用いてスカラー倍算を行う
3. 算出された新しい有理点を暗号化されたデータとして保存する

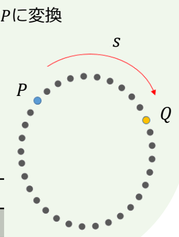
ID	名前	性別	年齢	病状
1	田中太郎	男	50	風邪

曲線上の有理点Pに変換

暗号化 $Q = sP$

データに戻す

ID	名前	性別	年齢	病状
?	?	?	?	?



大データの暗号化

高速に暗号化が行える 岡大発 **AES** を使用

岡大発 AES

- 最小ハードウェア実装が可能
- 逐次拡大と正規基底を用いることで効率的な演算を実現

AES 暗号化手順

1. ヘッダ情報（暗号化方式など）を作成する
2. ファイルをバイナリ形式で読み込み拡大体上の要素に変換し、行列へ保存する
3. 暗号化処理を行う
4. ヘッダを結合してバイナリ形式で書き出す

様々なファイル容量・形式