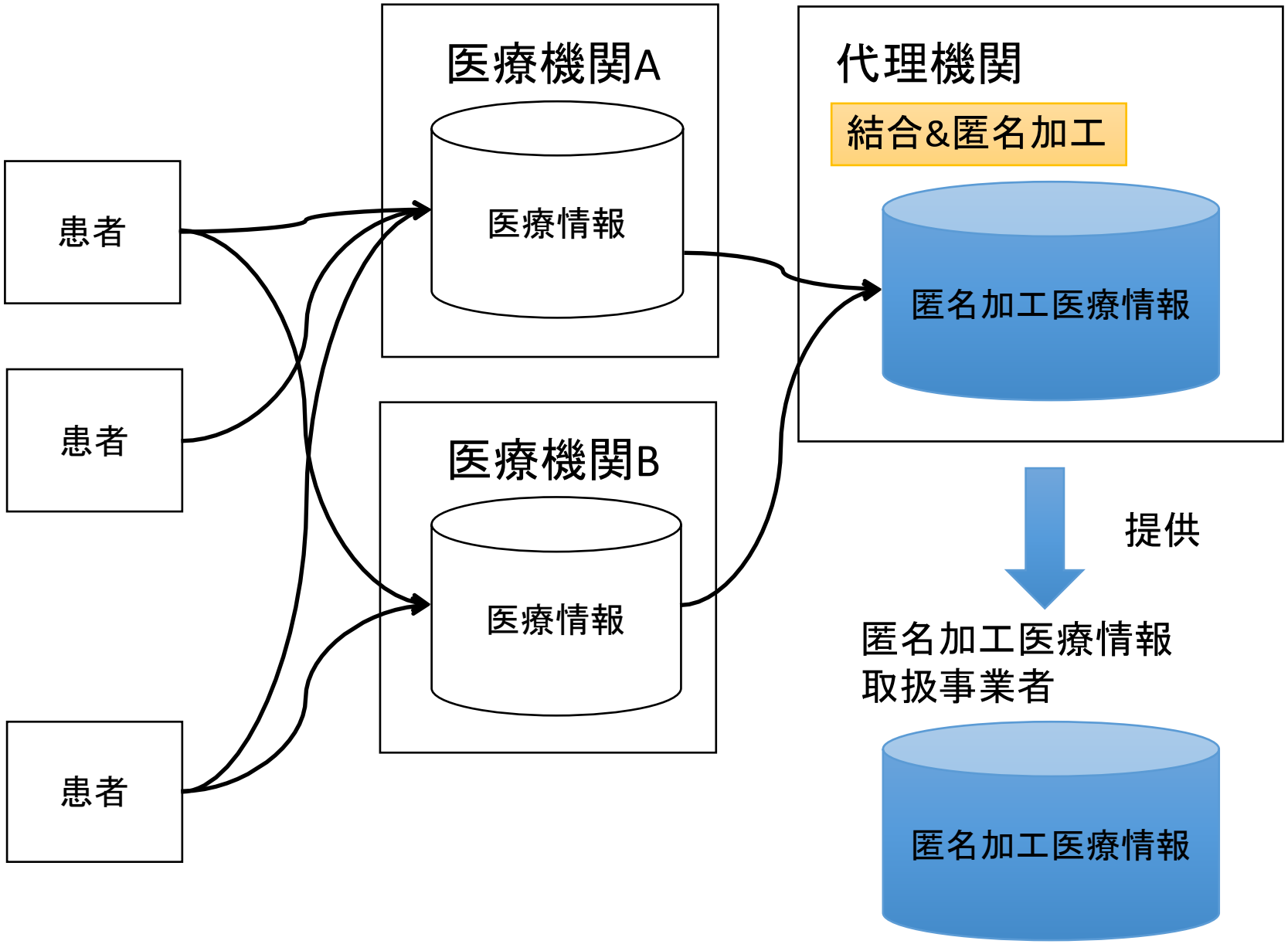
データ結合と秘密計算

筑波大学/ JST CREST/ 理研AIP
佐久間　淳

次世代医療基盤法が想定する匿名加工医療情報情報の流通



匿名加工医療情報は本人への連絡ができない

氏名	性別	年齢	処方コード
小野小町	F	36	xxxx
紫式部	F	47	yyyy
織田信長	M	23	zzzz

代理機関
匿名加工医療情報

性別	年齢	処方コード	症例
F	36	xxxx	A
F	47	yyyy	B
M	23	zzzz	C

氏名	性別	年齢	症例
小野小町	F	36	A
紫式部	F	47	B
織田信長	M	23	C

連絡できない・してはならない

取扱事業者

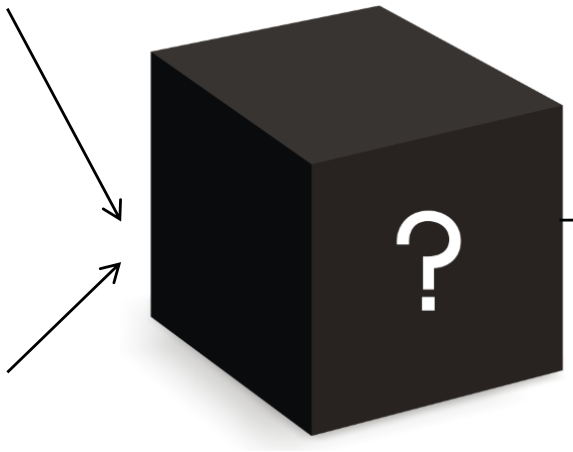
性別	年齢	処方コード	症例
F	36	xxxx	A
F	47	yyyy	B
M	23	zzzz	C

副作用の疑い？

秘密計算

ID/属性	属性3	属性4
紫式部		
小野妹子		
楠木正成		
明智光秀		

ID/属性	属性1	属性2
紫式部		
小野妹子		
足利尊氏		
明智光秀		



データ解析
結果

- 計算の過程において，結果を除くいかなる情報も漏れない
- 様々な実現法があるが，ここでは暗号を利用した方法を

暗号化したままデータ解析
準同型暗号

秘密の数字: m_1=250万
m_1の暗号文: c_1=Enc (m_1)

秘密の数字: m_2=40万
m_2の暗号文: c=Enc (m_1)

秘密の数字: m_3=330万
m_3の暗号文: c_3=Enc (m_3)

暗号化のため内容は
解析者にわからない

解析者

c_1, c_2, c_3

$c=c_1 \times c_2 \times c_3$

暗号化したまま
データ解析を実行

実際には…

$c=c_1 \times c_2 \times c_3$
$=Enc(m_1) \times Enc(m_2) \times Enc(m_3)$
$=Enc(m_1+m_2+m_3)$
$=Enc(250万+40万+330万)$
$=Enc(620万)$

準同型暗号

収入の総和が
(暗号化したまま)
計算できている

臨床情報と遺伝情報を交えた遺伝子検査

検査希望者

家族歴

問診
身体検査
血液検査
尿検査
生理検査
X線検査
MRI/MRA

遺伝因子の解析

SNPs解析

臨床検査によるリスク予測

	相対危険度
喫煙	1.5
肥満	1.7
高血圧	2.3
脂質異常症	2.1
糖尿病	2.5
慢性腎臓病	1.4

病院

総合評価によるリスク予測

	予測確率(%)
心筋梗塞	10
脳梗塞	5
脳出血	3

個人にとって最適な
疾患予防法の実践
・食事療法・禁煙
・高血圧・糖尿病・脂質異常症
などの治療

遺伝因子によるリスク予測

	遺伝子型	相対危険度
SNP 1	*TT*	1.3
SNP 2	*CG*	1.2
SNP 3	*AT*	0.8
SNP 4	*GG*	1.4
SNP 5	*CC*	0.7
SNP 6	*GT*	1.2
SNP 7	*TT*	1.4
SNP 8	*GG*	1.3
SNP 9	*CG*	0.9
・・・		
・・・		
SNP 100	*CT*	1.2

遺伝子
検査機関