自治体・医療機関における組織暗号の実証実験

2016年1月21日

中央大学研究開発機構

才所敏明　近藤健　庄司陽彦
五太子政史　辻井重男

本発表は、国立研究開発法人情報通信研究機構（NICT）からの委託研究「組織間機密通信のための公開鍵システムの研究開発」の元に実施した、再暗号化機能を実現する楕円エルガマル暗号ベースの組織暗号の活用可能性の調査・検討を目指した3年間の活動内容・成果の報告です。

発表内容

（１）組織通信と組織暗号

（２）自治体業務における組織暗号の活用可能性

（３）医療・介護業務における組織暗号の活用可能性

（４）今後の課題

（1）

組織通信と組織暗号

組織暗号とは

（1）個人情報等の機密情報の組織間の配信に適した暗号方式

従来の暗号方式は、個人間通信向けの暗号方式

組織暗号は、組織間通信向けの新たな暗号方式

（2）受信側組織で機密情報の転送者・利用者を指定可能な暗号方式

従来の暗号方式は、送信側主導の暗号方式（送信者が利用者を特定）

組織暗号は、受信側主導の暗号方式

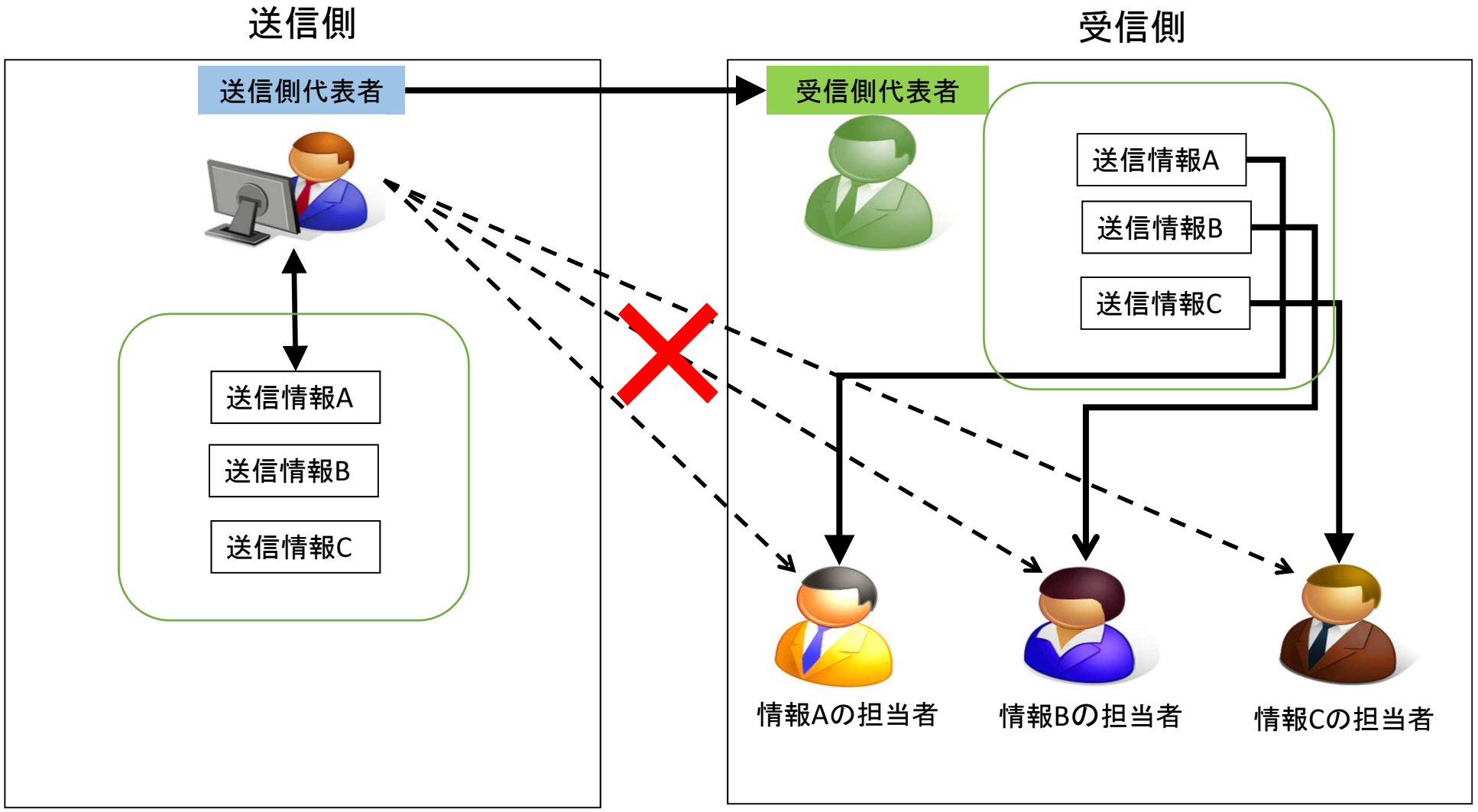
（3）暗号化情報の復号鍵の安全な変更が可能な暗号方式

従来の暗号方式では、一旦復号する（平文に戻す）必要がある

組織暗号では、復号することなく、復号鍵の変更（再暗号化）が可能

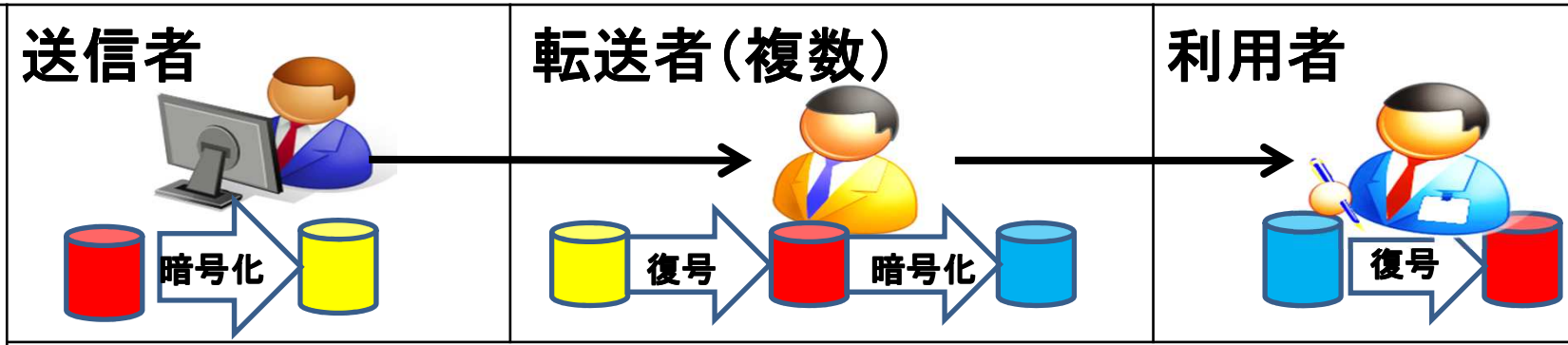
組織暗号は、個人情報の相互利用が増加する
行政・医療分野での活用が期待される暗号方式

組織間通信


送信側
受信側
送信側代表者
受信側代表者
送信情報A
送信情報B
送信情報C
送信情報A
送信情報B
送信情報C
情報Aの担当者
情報Bの担当者
情報Cの担当者

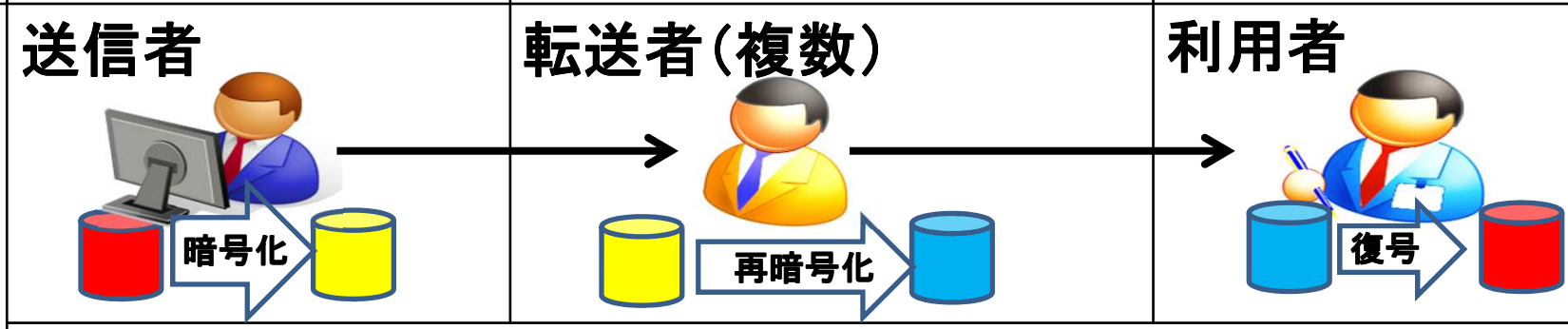
組織暗号の安全性

従来の暗号方式



転送者は機密情報を、**一旦復号する（平文に戻す）必要**が有り、
転送者の数に応じ、情報漏えいのリスクが増大

組織暗号方式

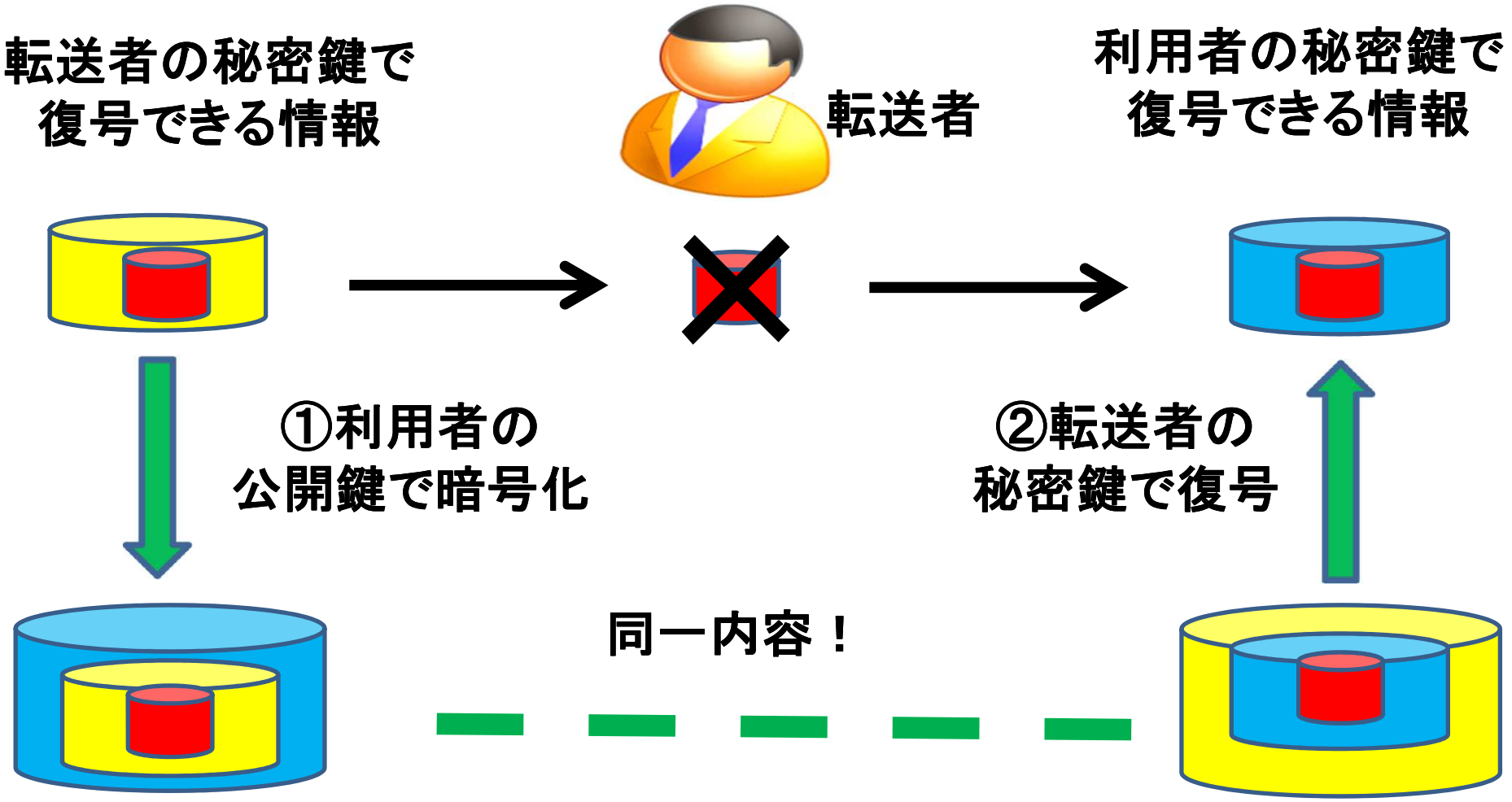


転送者は機密情報を、復号する（平文に戻す）ことなく転送でき、
転送プロセスでの情報漏えいのリスクを軽減可能

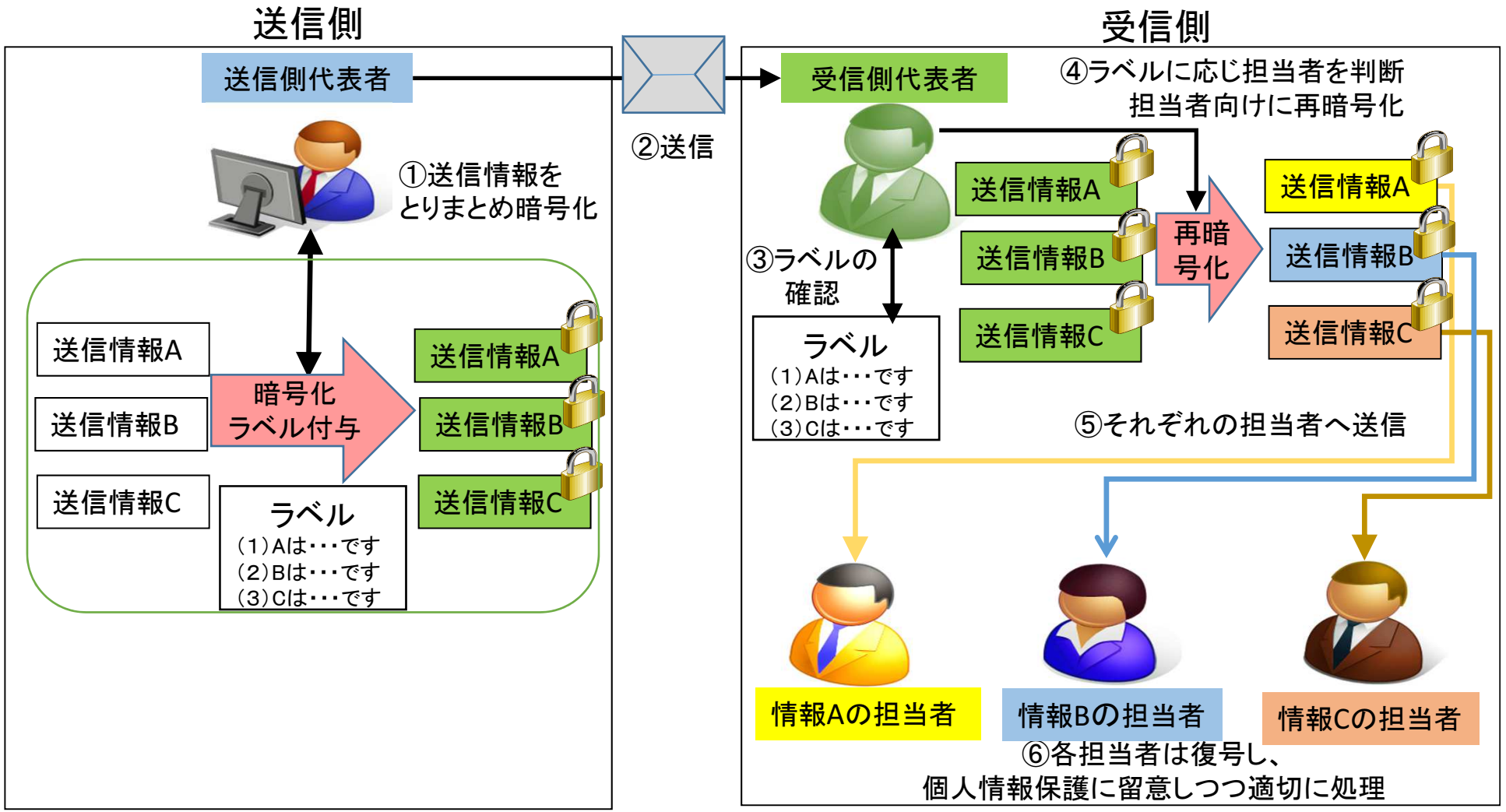

は、平文の機密情報


は、暗号化された機密情報

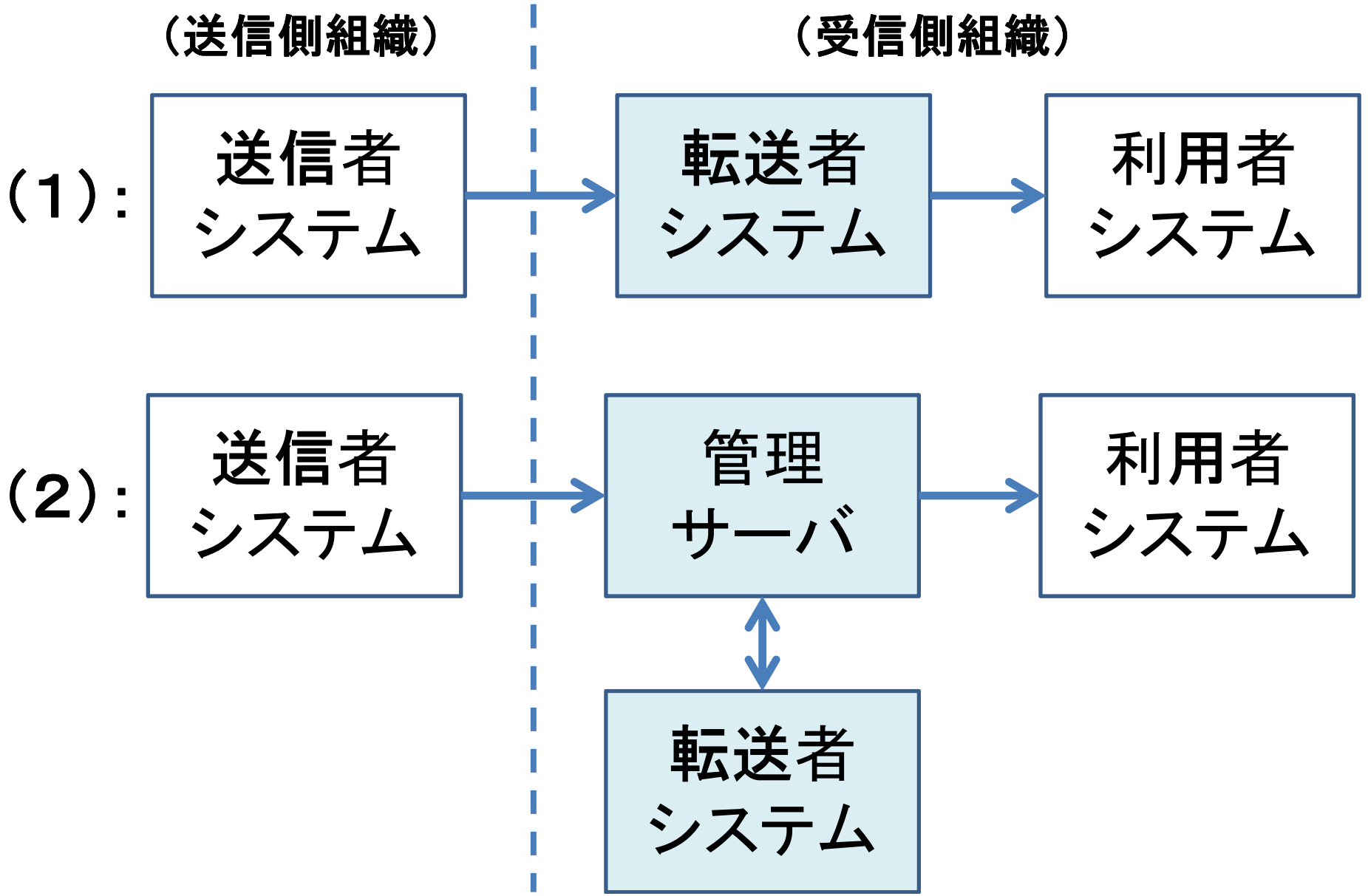
組織暗号では、なぜ安全に転送が可能なのか？



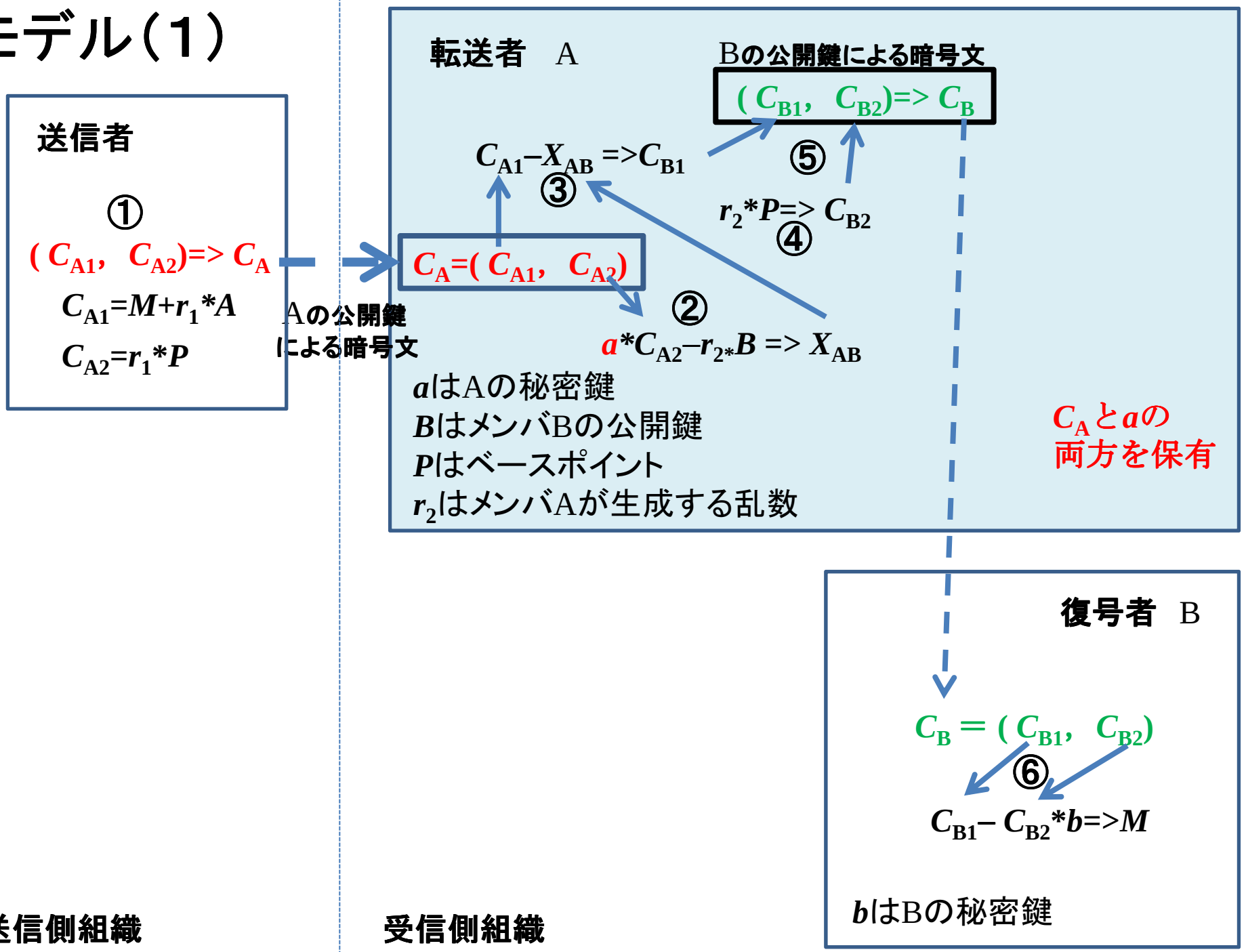
組織間通信と組織暗号


送信側
送信側代表者
①送信情報を
とりまとめ暗号化
送信情報A
送信情報B
送信情報C
暗号化
ラベル付与
送信情報A
送信情報B
送信情報C
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
②送信
受信側
受信側代表者
④ラベルに応じ担当者を判断
担当者向けに再暗号化
③ラベルの
確認
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
送信情報A
送信情報B
送信情報C
再暗
号化
送信情報A
送信情報B
送信情報C
⑤それぞれの担当者へ送信
情報Aの担当者
情報Bの担当者
情報Cの担当者
⑥各担当者は復号し、
個人情報保護に留意しつつ適切に処理

組織暗号応用組織間機密情報配信モデル



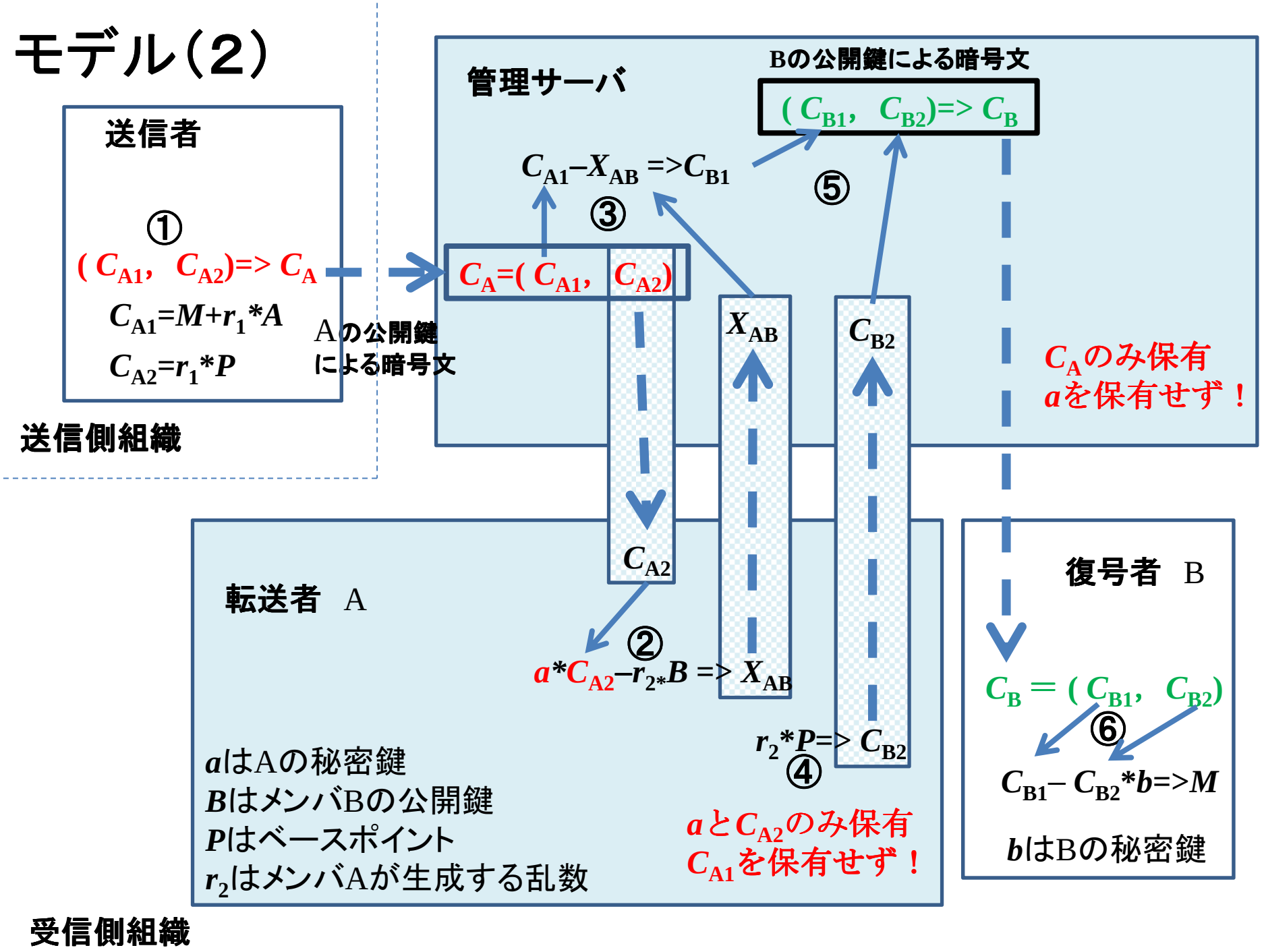
モデル(1)



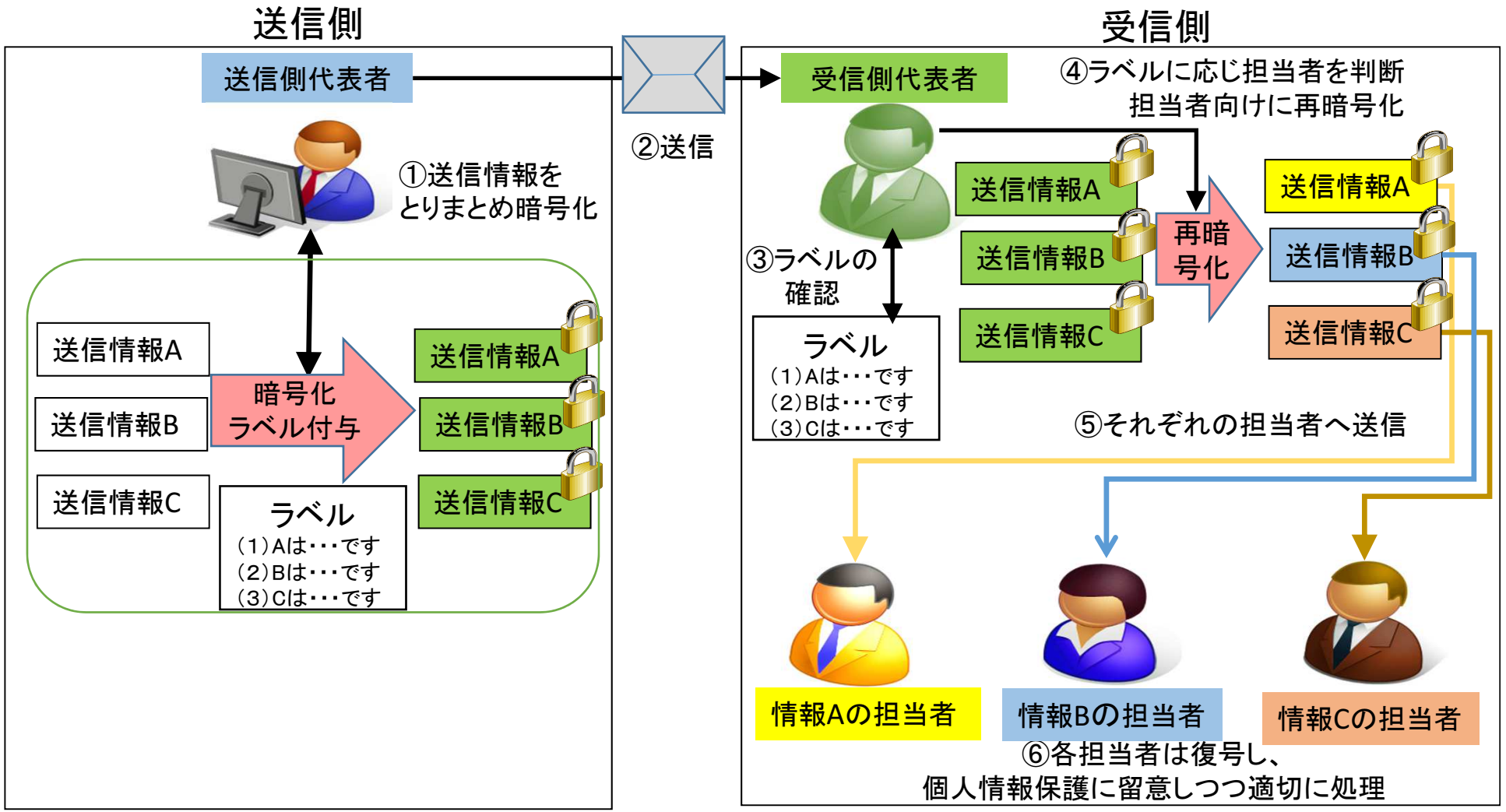
送信側組織

受信側組織

モデル（2）


送信者
①
$(C_{A1}, C_{A2}) \Rightarrow C_A$
$C_{A1}=M+r_1*A$
$C_{A2}=r_1*P$
Aの公開鍵による暗号文
送信側組織
管理サーバ
Bの公開鍵による暗号文
$(C_{B1}, C_{B2}) \Rightarrow C_B$
$C_{A1}-X_{AB} \Rightarrow C_{B1}$
③
⑤
$C_A=(C_{A1}, C_{A2})$
X_{AB}
C_{B2}
C_Aのみ保有
aを保有せず！
C_{A2}
転送者 A
②
$a*C_{A2}-r_{2*}B \Rightarrow X_{AB}$
$r_2*P \Rightarrow C_{B2}$
④
aとAの秘密鍵
BはメンバBの公開鍵
Pはベースポイント
r_2はメンバAが生成する乱数
aとC_{A2}のみ保有
C_{A1}を保有せず！
受信側組織
復号者 B
$C_B=(C_{B1}, C_{B2})$
⑥
$C_{B1}-C_{B2}*b \Rightarrow M$
bはBの秘密鍵

組織間通信と組織暗号


送信側
送信側代表者
①送信情報を
とりまとめ暗号化
送信情報A
送信情報B
送信情報C
暗号化
ラベル付与
送信情報A
送信情報B
送信情報C
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
②送信
受信側
受信側代表者
④ラベルに応じ担当者を判断
担当者向けに再暗号化
③ラベルの
確認
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
送信情報A
送信情報B
送信情報C
再暗
号化
送信情報A
送信情報B
送信情報C
⑤それぞれの担当者へ送信
情報Aの担当者
情報Bの担当者
情報Cの担当者
⑥各担当者は復号し、
個人情報保護に留意しつつ適切に処理

（2）

自治体業務における
組織暗号の活用可能性

自治体業務と組織暗号

2013年の番号関連四法の成立により
社会保障・税番号（マイナンバー）導入が決定
（2016年より，社会保障分野，税分野，災害対策分野へ）

行政機関や地方自治体などが保有する個人情報の
相互利用が促進されることになる

組織暗号は、
個人情報の保護に留意しつつ利活用が求められる
自治体業務の中で、幅広く活用いただけることを期待

自治体向け組織暗号紹介活動

- **実証実験実施自治体**
  - 長野県・大町市（2014年10月15日）
  - 長野県・箕輪町（2014年11月7日）
  - 新潟県・燕市（2014年11月21日）
  - 兵庫県（兵庫県、西宮市、加古川市）（2015年6月5日）
  - 大分県（大分県、大分市、中津市）（2015年9月3日）
- **組織暗号紹介と意見交換のための訪問自治体**
  - 京都府・京都市（2015年9月15日）

大分県での実証実験式次第

組織暗号実証実験式次第（2015年9月3日）

司会　　才所敏明　中央大学　研究開発機構　専任研究員

10:00～　挨拶

大場善次郎　ハイパーネットワーク社会研究所　理事長・所長

辻井重男　　中央大学　研究開発機構　機構教授

10:10～　講演「情報通信・セキュリティ概念の高度化とその具体的方策」

辻井重男

10:50～　組織暗号　－自治体での活用可能な業務例－

近藤健　　NPO法人中央コリドー情報通信研究所　理事

11:05～　組織暗号　－大分県内自治体想定業務への適用案
および操作実験の構成・内容紹介－

才所敏明

11:25～　組織暗号　－実験システム動作説明－

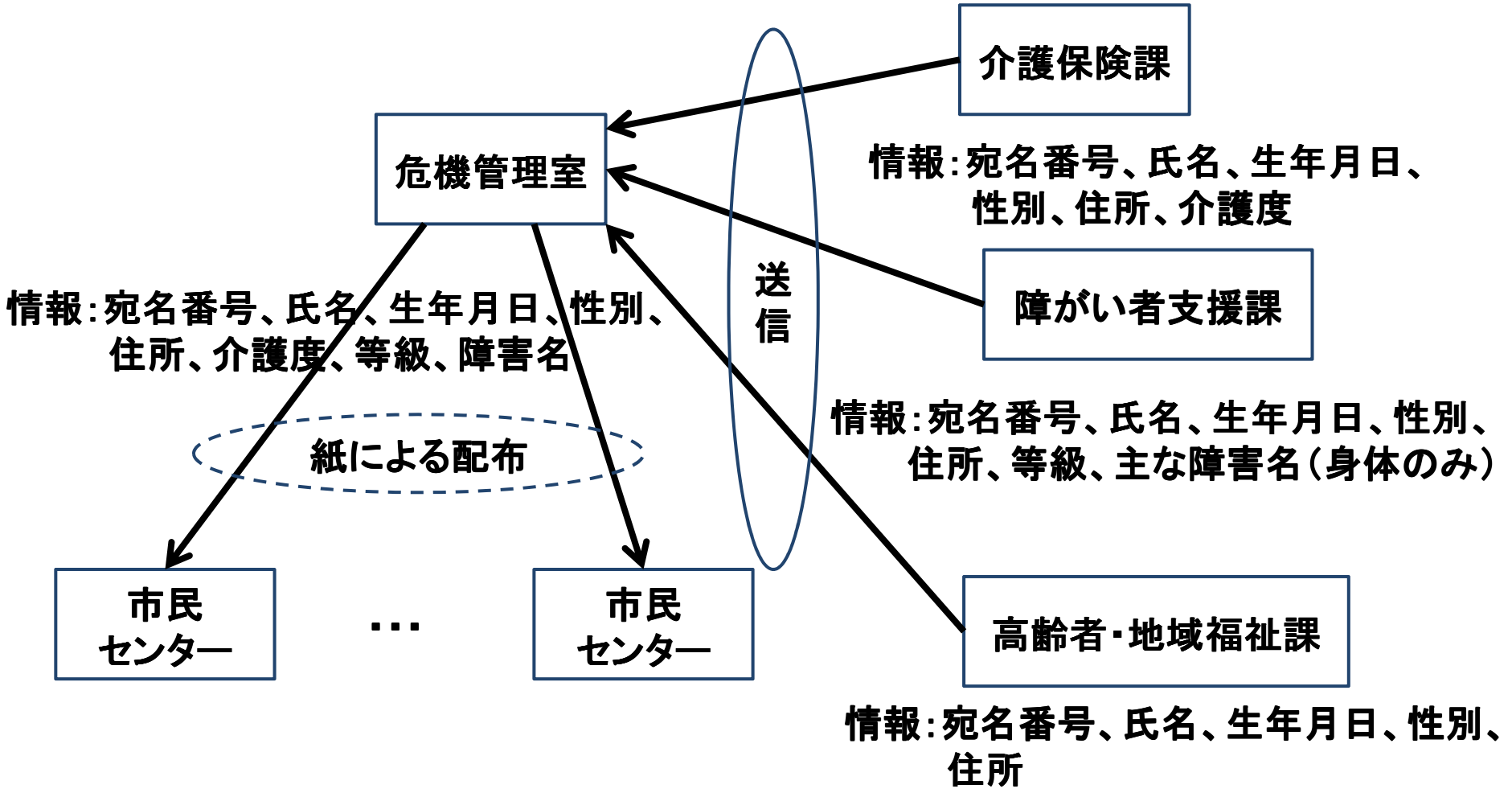
庄司陽彦　　YDKコミュニケーションズ

11:45～　質疑応答

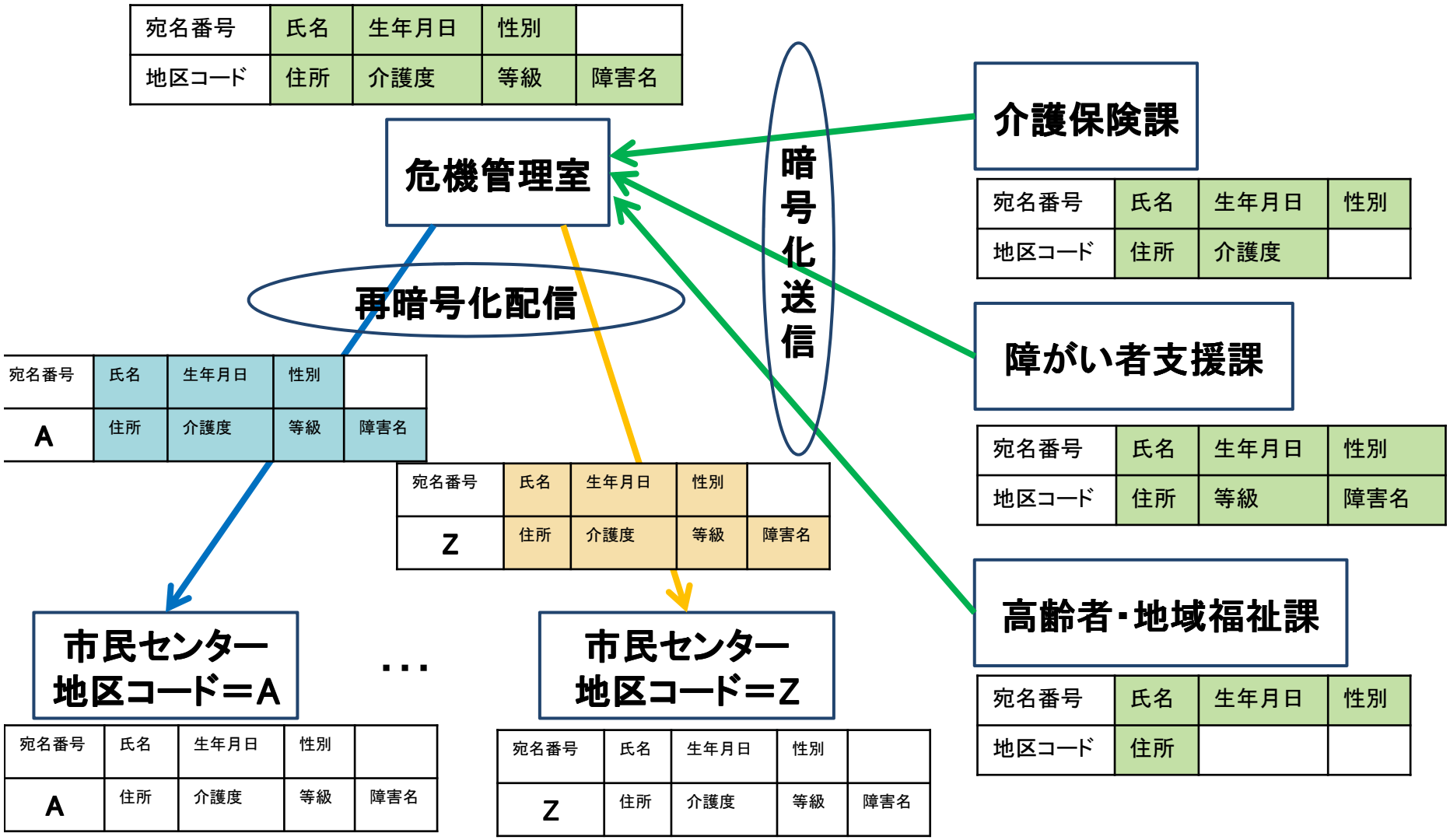
（　12:00　終了　）

組織暗号適用可能業務例
（兵庫県・加古川市）

避難行動要支援者情報配布業務



避難行動要支援者情報の安全な送信と市民センターへの安全な配信



大分県での実証実験の模様

実証実験参加者

- 参加人数　各回40名～50名程度

- 参加組織

  自治体、外郭団体

  一般民間企業

  システム開発ベンダ、コンサル企業

  大学・研究開発機関

  報道機関

大分合同新聞2015年9月4日朝刊5頁

ネット上のやりとり 情報漏えい防げ

組織暗号実証実験

自治体や企業関係者らが出席

自治体や企業など団体間でのネット上のやりとりで、情報漏えいの危険性が低いとされる「組織暗号」の実証実験が3日、大分市のホルトホール大分であった。自治体や企業の関係者ら約40人が出席した。

マイナンバー制度の開始を控え、個人情報の保護の重要性が一層増していることから、ハイパーネットワーク社会研究所（大分市）と中央大学研究開発機構（東京都）が主催した。

組織暗号では外部から受信した情報を解読しないまま再暗号化して担当者に送ることができる。解読後の情報に触れる人を担当者に限定できるため団体内での情報漏えい防止に優れているとされる。

実験は県内の市が県国保連合会から年金データの提供を受けるという想定で実施。立ち会った県情報政策課の担当者は「思ったよりも簡単な操作で扱えた。暗号化されていない情報に触れる人が少ないほど漏えいの危険性が狭まる」と話した。

大分放送：9月3日イブニングニュースにて放映

＜　実証実験からの知見　＞
自治体側の反応・感想要約

（1）組織暗号の再暗号化（復号せず鍵の付替え）機能への驚き
（2）日々取り扱っている個人情報の重要性の再認識
（3）実際に使用する場合のサポートへの期待
　　モジュールの商品化、市販パッケージへの組込み、SI支援
（4）個人情報の安全な取扱いには、
　　配信プロセスの安全性だけでは不十分
（5）情報技術への不安、不信　　情報漏えい事件の報道など
（6）従来の紙ベースから情報技術利用への変化の責任の重さ
（7）先進的技術の独自採用は困難

（３）

医療･介護業務における組織暗号の活用可能性

医療・介護業務と組織暗号

2014年の医療介護総合確保推進法の成立により，
医療・介護サービスの提供体制の改革が決定
（地域包括ケア体制の整備へ）

医療・介護サービスに関わる様々の専門組織や
専門家の間での患者・利用者の個人情報の相互利用が
促進されることになる

組織暗号は、
個人情報の保護に留意しつつ利活用が求められる
医療・介護業務の中で、幅広く活用いただけることを期待

医療機関向け組織暗号紹介活動

- 組織暗号紹介と意見交換のための訪問医療機関
  長野県・信州メディカルネット（2015年7月15日）
  島根県・まめネット
  （しまね医療情報ネットワーク）（2015年7月23日）
  京都府・京都医療センター
  （2015年8月6日、20日、9月14日）
  山梨県・富士吉田医師会（2015年8月21日）
  長崎県・あじさいネット
  （長崎地域医療連携ネットワーク）（2015年9月25日）
- 実証実験実施医療機関
  京都府・京都医療センター（11月19日）

京都医療センターでの実証実験式次第

組織暗号実証実験式次第（2015年11月19日）

司会　才所敏明　中央大学研究開発機構　専任研究員

15:45～　開会および配布資料確認

15:50～　挨拶

北岡有喜　独立行政法人国立病院機構 京都医療センター　医療情報部長

辻井重男　中央大学研究開発機構　機構教授

16:00～　講演「組織間通信における情報漏洩と組織暗号の実用化」

辻井重男

16:35～　紹介「組織暗号」

①特徴機能

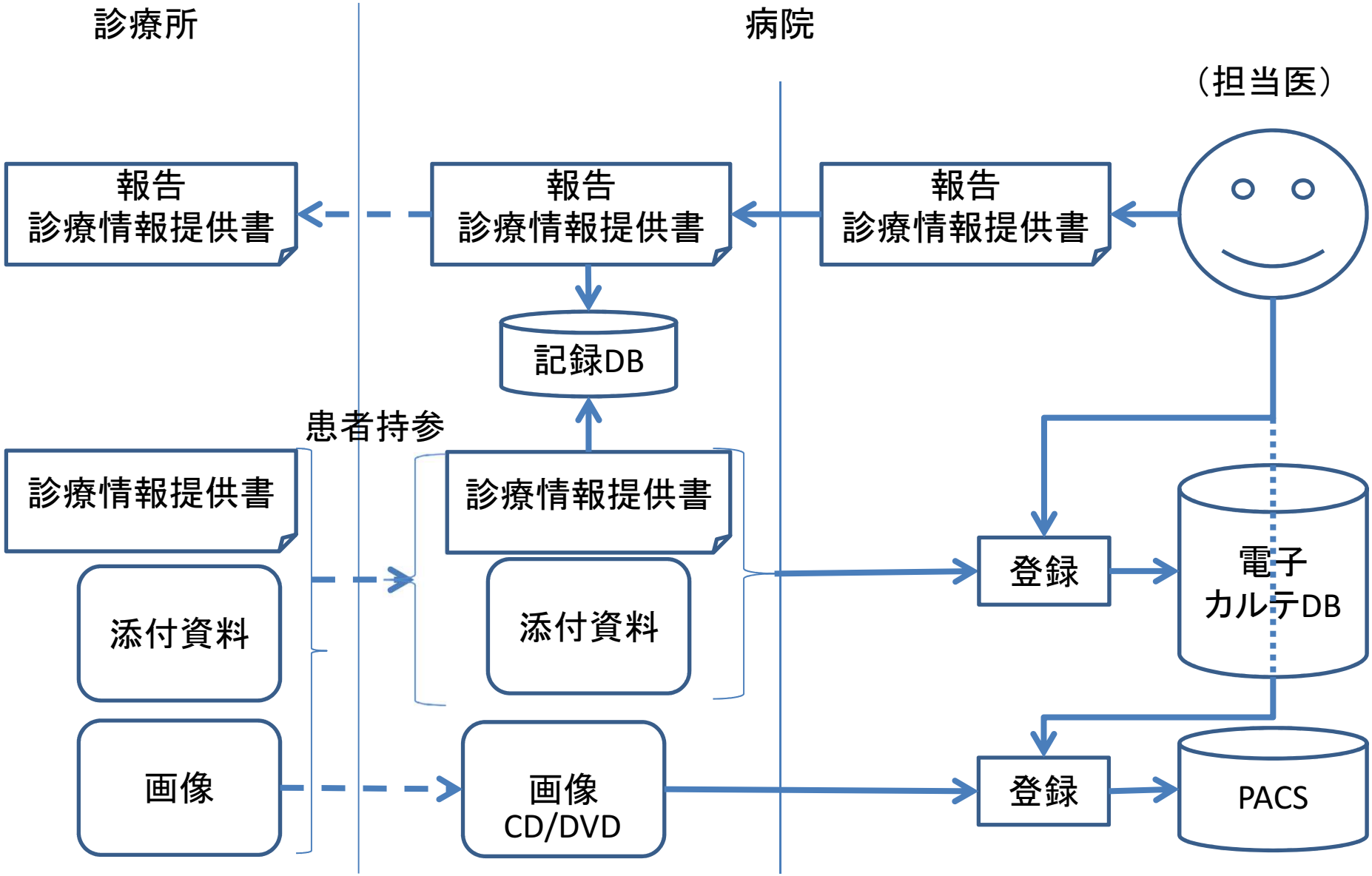
②医療情報送受・共有業務への適用例

③実験システムによるデモ

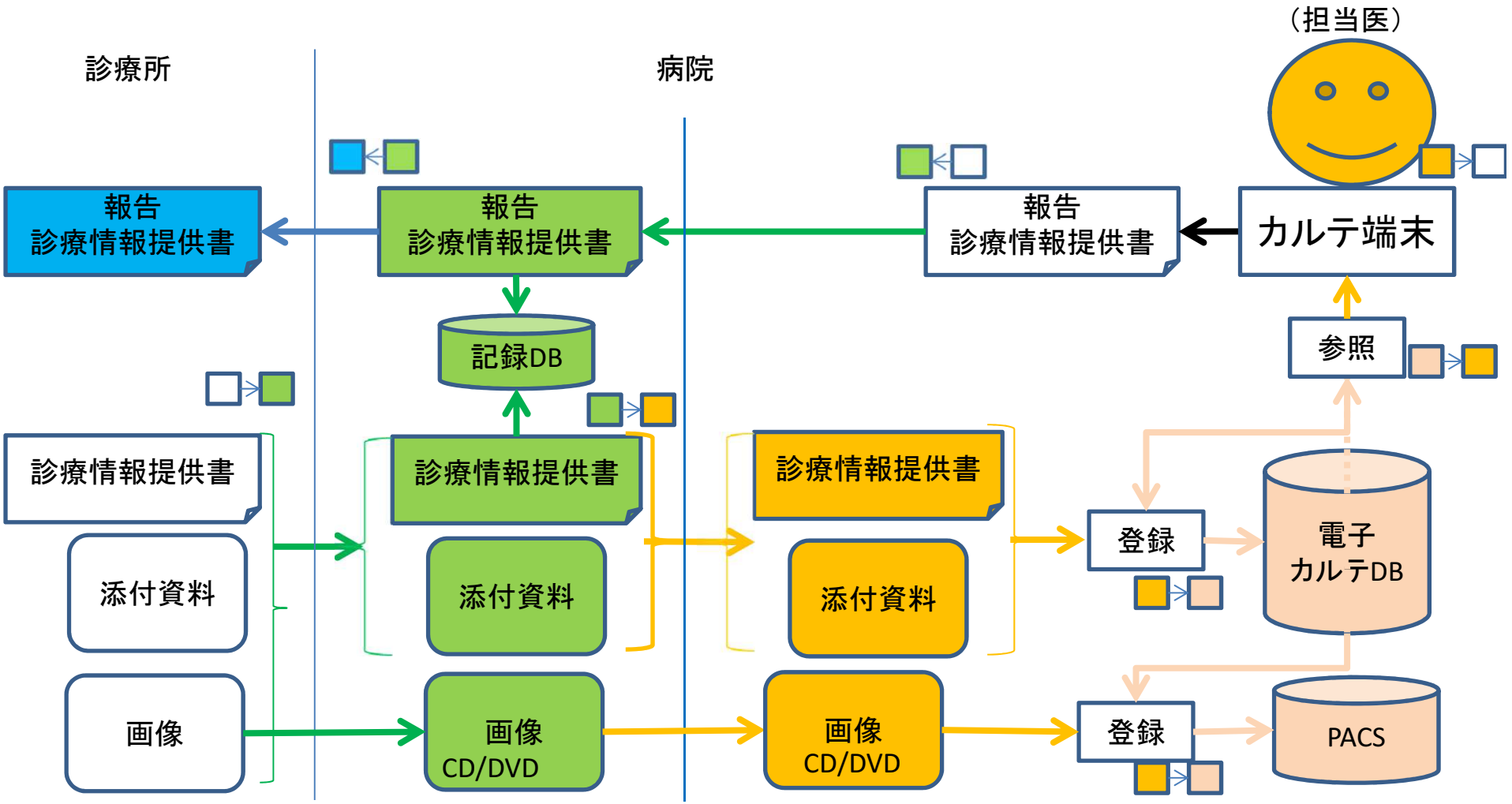
才所敏明

16:55～　質疑応答

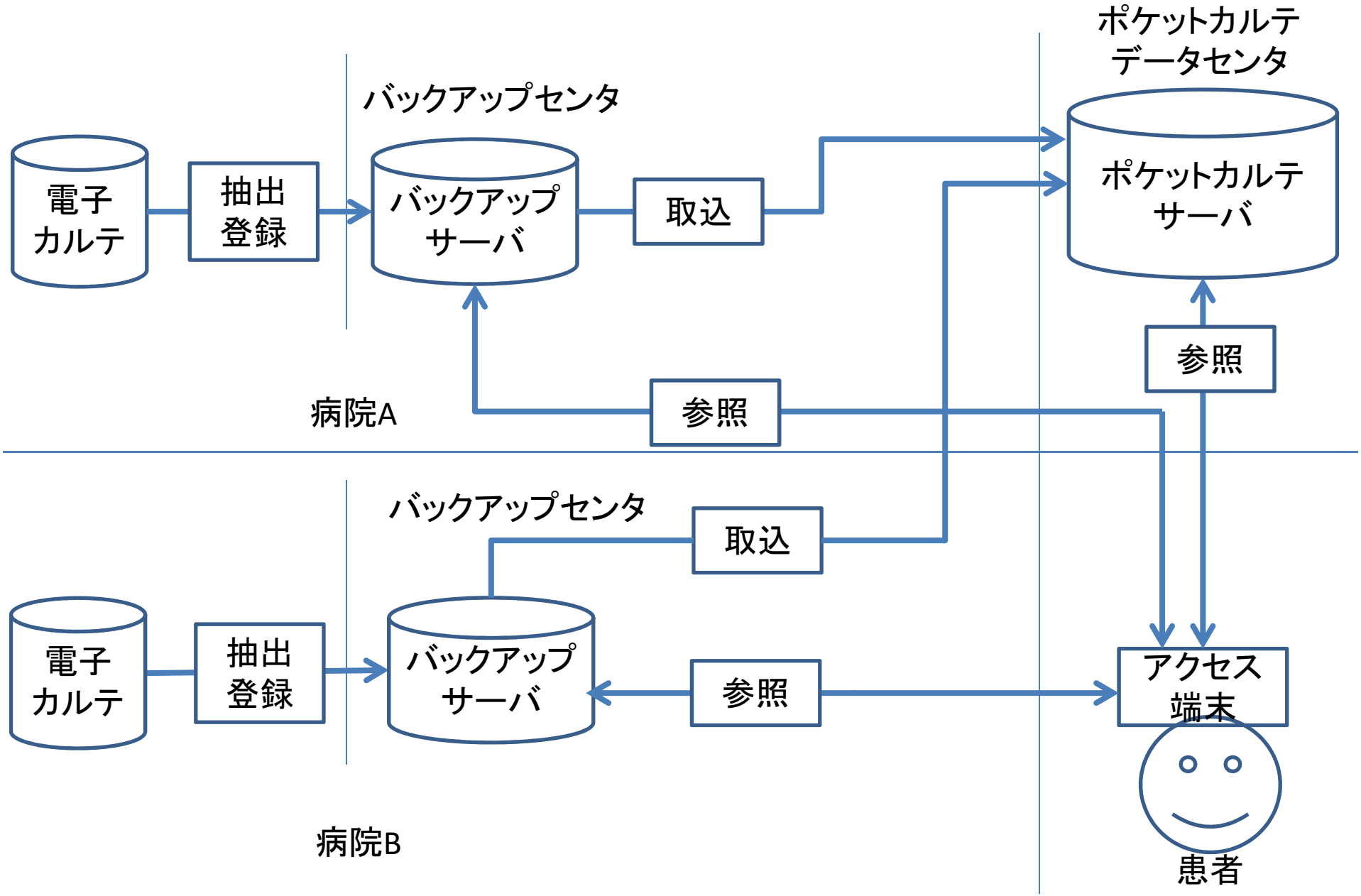
（1）紹介状（診療情報提供書）



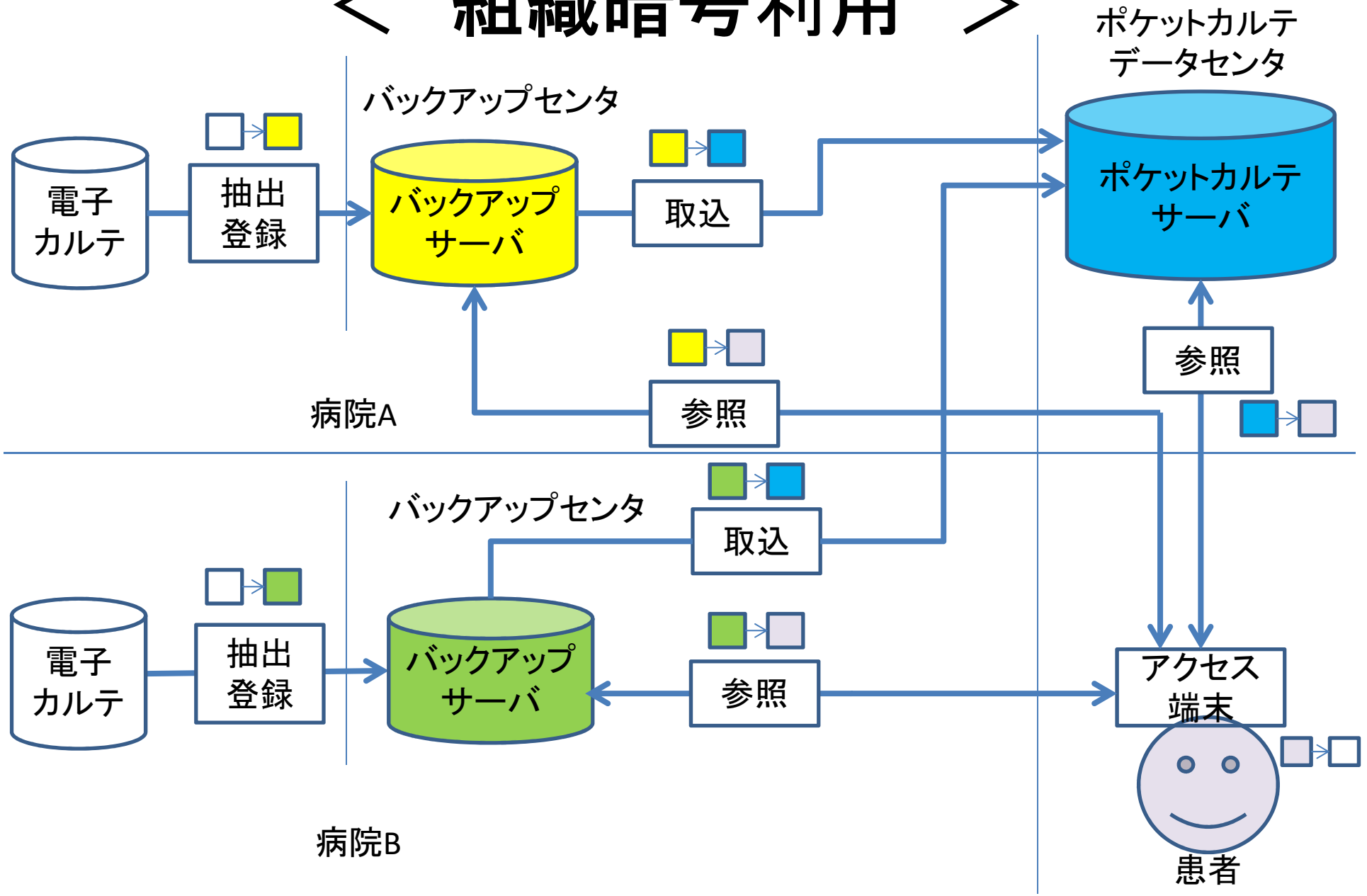
紹介状（診療情報提供書）
＜組織暗号利用＞



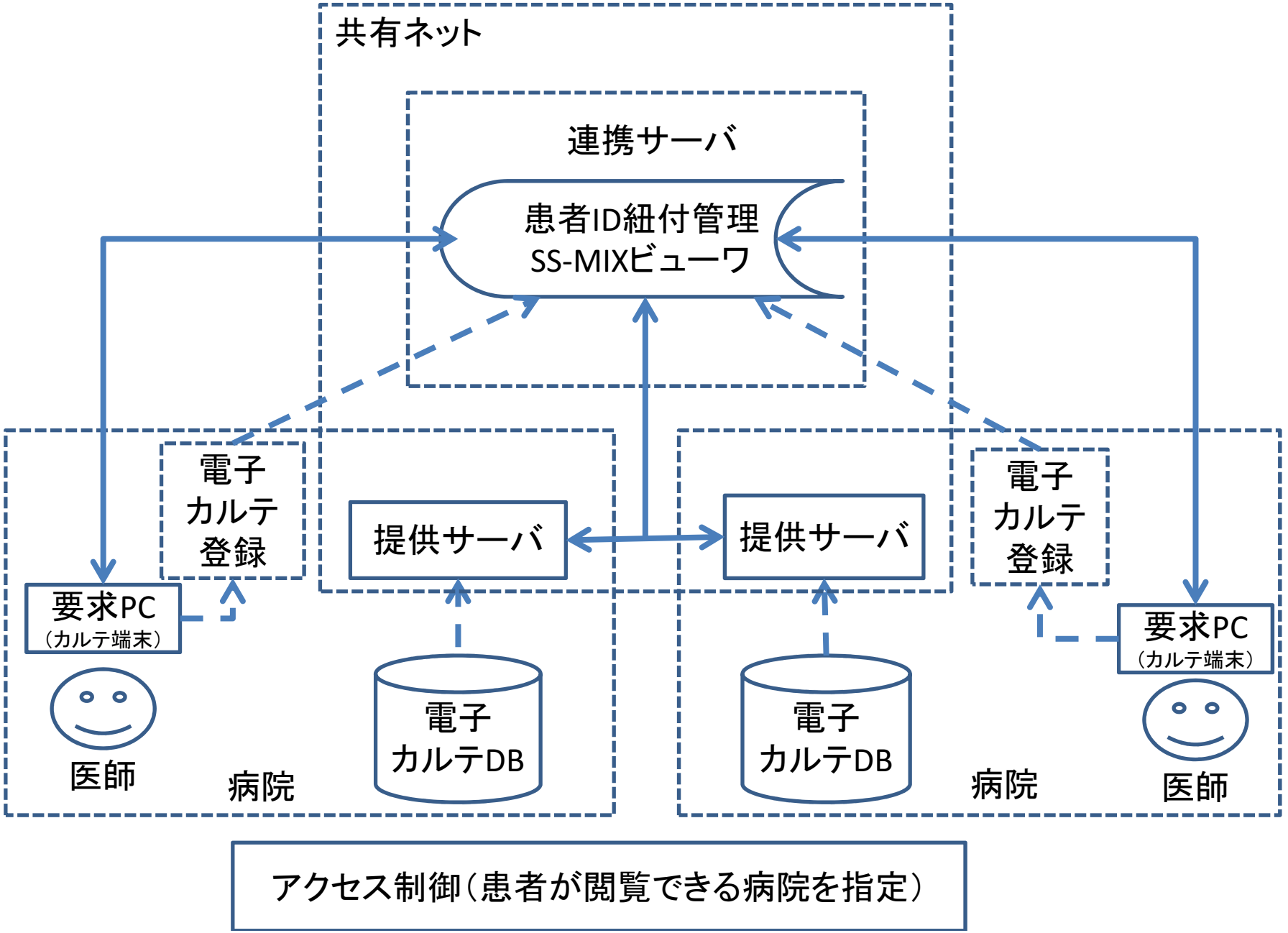
（2）ポケットカルテ


ポケットカルテ
データセンタ
バックアップセンタ
電子
カルテ
抽出
登録
バックアップ
サーバ
取込
ポケットカルテ
サーバ
参照
病院A
参照
バックアップセンタ
取込
電子
カルテ
抽出
登録
バックアップ
サーバ
参照
アクセス
端末
病院B
患者

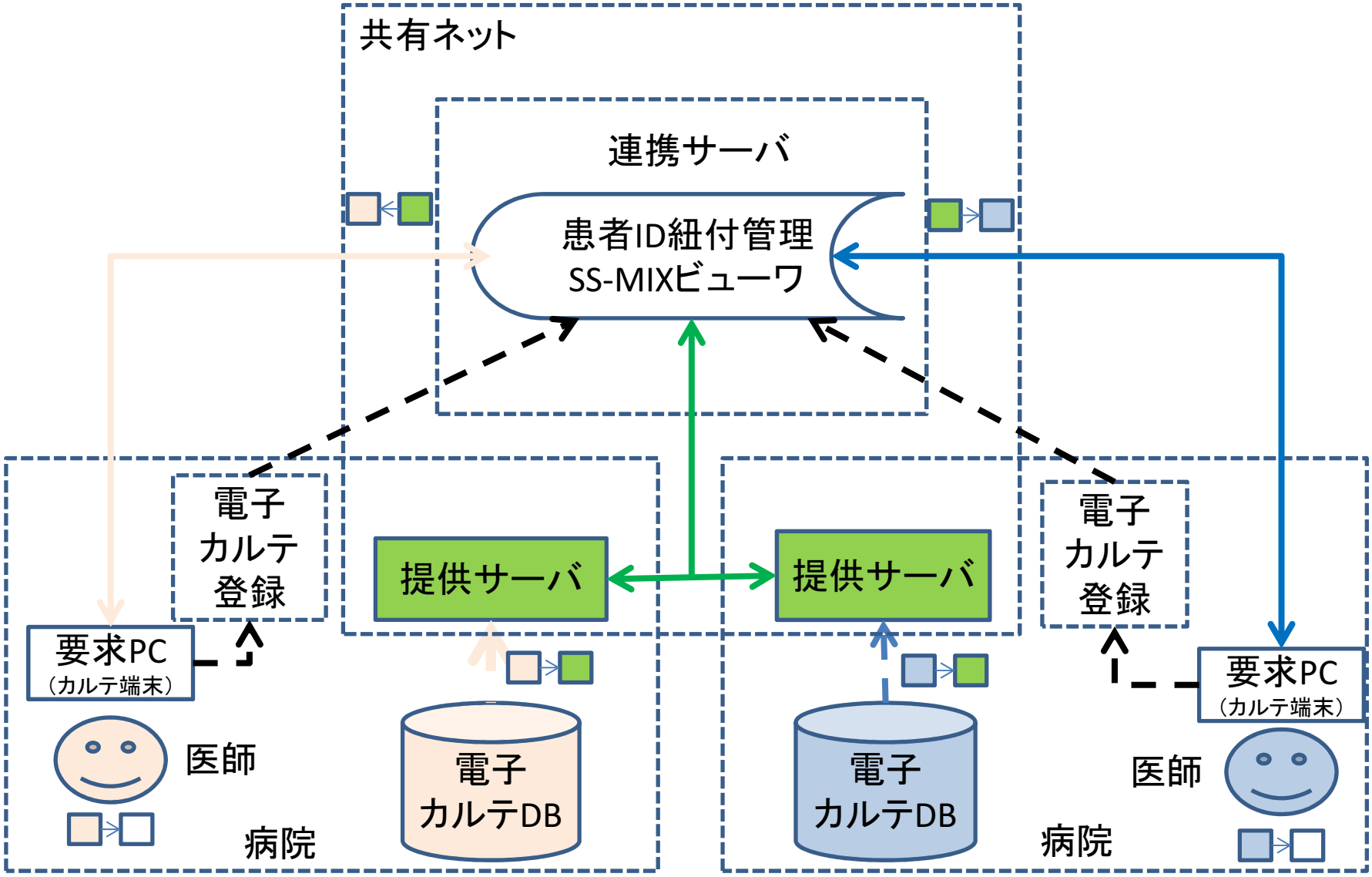
ポケットカルテ
＜　組織暗号利用　＞



（3）電子カルテの共有


共有ネット
連携サーバ
患者ID紐付管理
SS-MIXビューワ
電子
カルテ
登録
提供サーバ
提供サーバ
電子
カルテ
登録
要求PC
（カルテ端末）
電子
カルテDB
電子
カルテDB
要求PC
（カルテ端末）
医師
病院
病院
医師
アクセス制御（患者が閲覧できる病院を指定）

電子カルテの安全な共有



アクセス制御（患者が閲覧できる病院を指定）

紹介活動・実証実験での意見

（1）紙データの紹介状では、地域連携室の一般事務員が見ることになるが、見て欲しくない情報であり、こういうものがあってしかるべき。

（2）検査センターと医療機関、病院と調剤薬局の組織間通信に活用できそう。 特に、病院から調剤薬局へ送る処方箋については、組織暗号の利用により、厚生労働省が認可しかねている電子処方箋の実現、技術革新の可能性があるのでは。

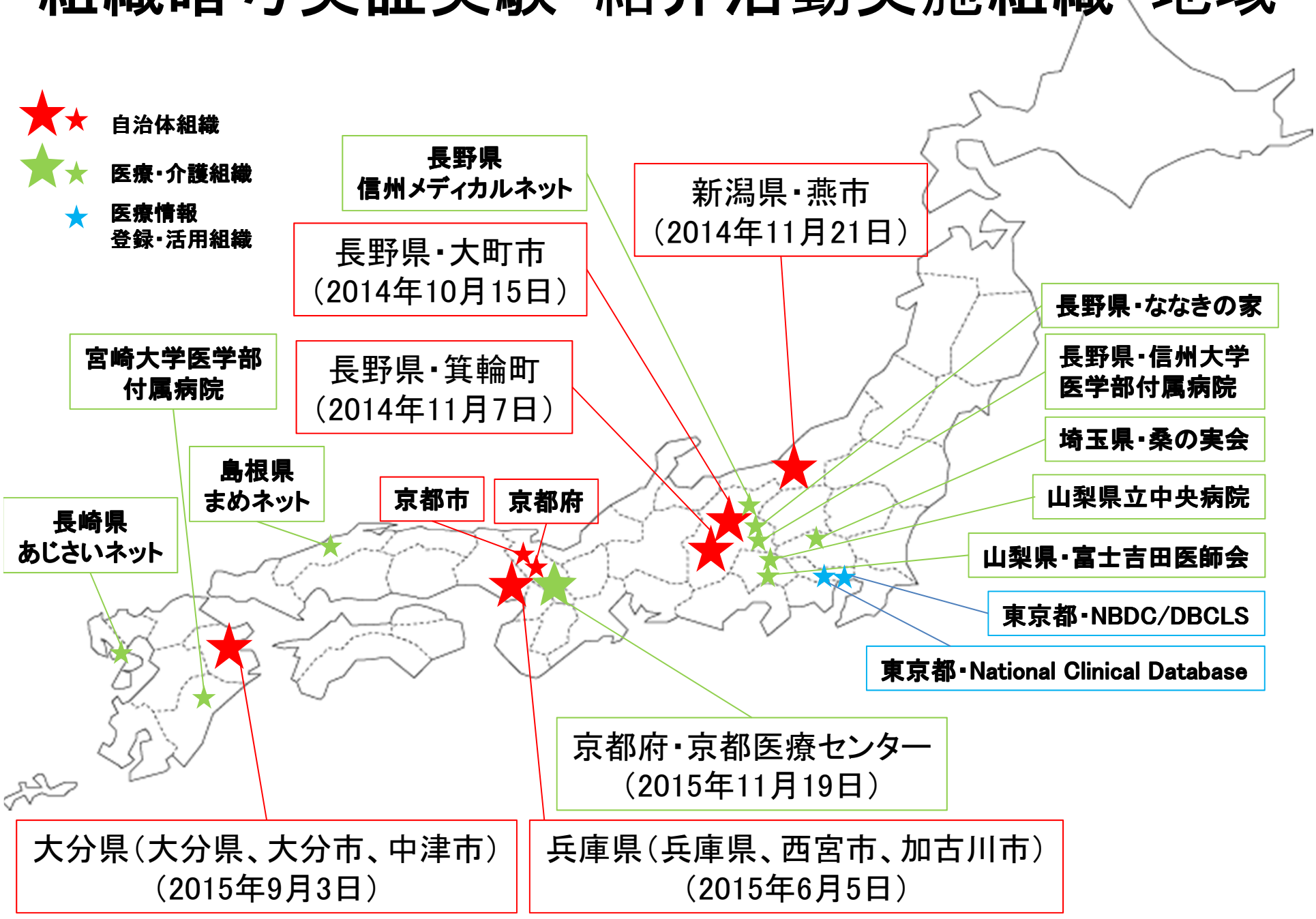
（3）院内・共有ネットワーク内では情報共有が最優先。暗号化は、緊急時の情報共有の妨げになるのでは？情報セキュリティは、院内システム・共有ネットワークを閉域網とすることにより維持している。

（4）院内システム・共有ネットワークは、法令や監督官庁のガイドラインに準じて構築・運用している。（監督官庁のガイドライン、法令で明確な指針が出ていないデータの暗号化については・・・）

（４）

今後の課題

組織暗号実証実験・紹介活動実施組織・地域



組織暗号の実用化に向けた主要課題と克服策

①組織暗号応用システムの導入・実装支援環境の整備

②自治体業務や医療・介護業務での
組織暗号利用に対する関係省庁のご理解・ご支援

③分野ごとの個人情報・医療情報を取り扱う業務を支える
安心安全情報処理基盤の開発

➔利用組織、ベンダ、研究開発部隊を含めた、
実業務での組織暗号実証PJの推進

➔先進的技術の現場の課題への適用方式および
暗号化状態処理・秘密分散状態処理の研究開発PJの推進

謝辞

本研究は，国立研究開発法人情報通信研究機構（NICT）における高度通信・放送研究開発委託研究課題「組織間機密通信のための公開鍵システムの研究開発―クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて―」の下に行ったものである．関係各位に感謝する．

終