「組織暗号」紹介
IoTシステムへの応用を目指して

2016年8月26日

才所　敏明
toshiaki.saisho@advanced-it.co.jp
(株)IT企画

本日の話題

（１）自己紹介＆(株)IT企画活動紹介

（２）中央大学研究開発機構・辻井Gの活動紹介

（３）NICT委託研究成果「組織暗号」解説

（４）NICT委託研究活動「組織暗号の実証実験」紹介

（５）IoT関連活動への期待

（６）IoT関連活動状況紹介

（1）自己紹介＆(株)IT企画活動紹介

自己紹介

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門

＊本社情報システム部門に所属 、東芝Gの技術部門・研究部門の
研究開発活動環境の整備・高度化を推進

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門

＊東芝のセキュリティ技術センター発足と同時にセンター長就任
＊その後、東芝Gのセキュリティ技術開発・事業支援活動を推進

2007年10月～　(株)IT企画を設立

＊情報技術および情報セキュリティ技術分野の研究開発や
その応用事業に対するプロフェッショナルサービスを開始
＊法政大学、日本大学で情報セキュリティに関する講義担当

2013年5月～　中央大学研究開発機構

＊国立研究開発法人情報通信研究機構（NICT）より委託の
「組織間機密通信のための公開鍵システムの研究開発」PJへ
研究員として参加

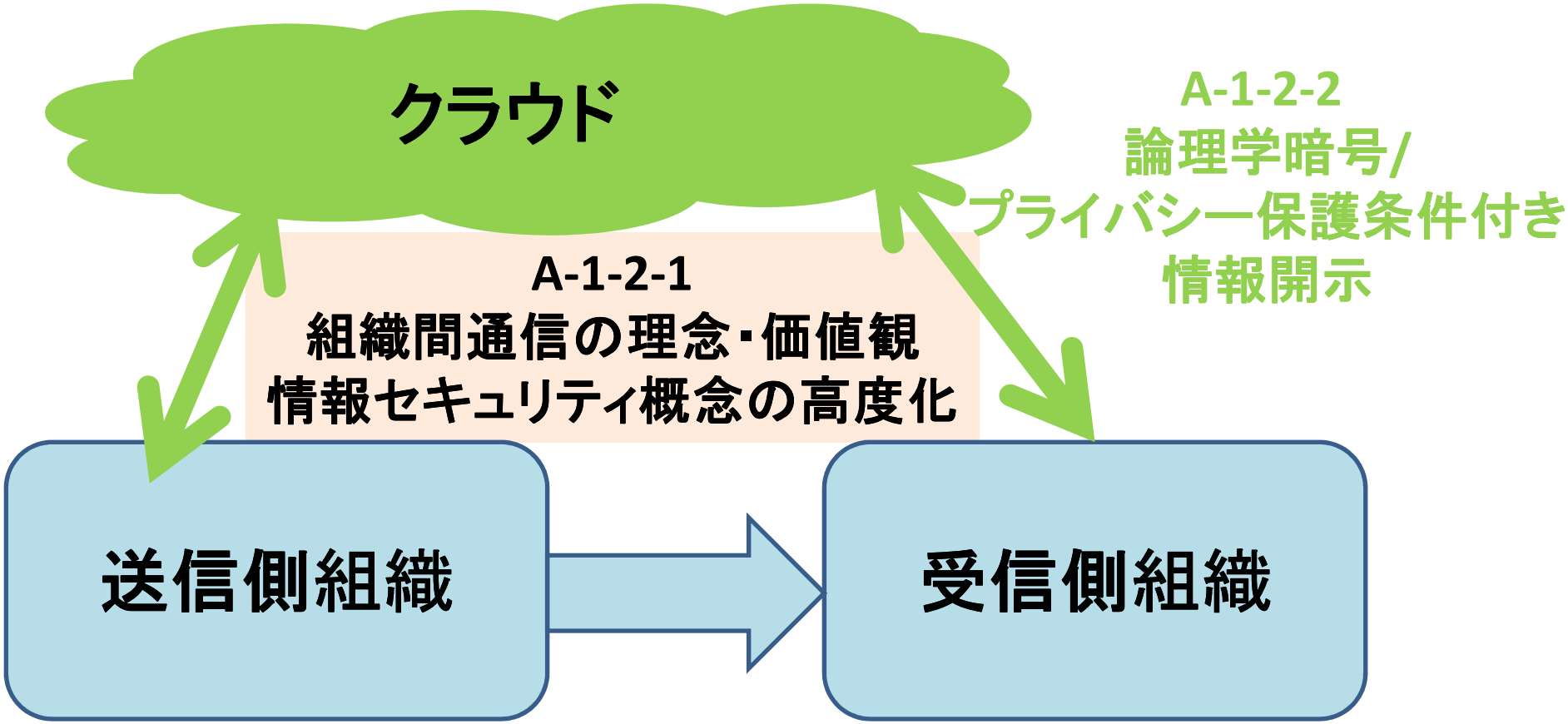
(株)IT企画活動紹介

- 大学向け教育活動
  - 法政大学・日本大学の講師
  - 九州大学、慶応大学での講義・講演
- 大学・研究機関向け研究活動
  - 中央大学研究開発機構
- 企業向け研究開発・事業企画支援活動
  - 大分・福岡等の企業の顧問
  - 技術・製品・システム・人材保有企業のコンサル
  - 技術調査・動向把握および対応戦略立案支援
    - モバイル決済、仮想通貨、ブロックチェーン、バイオメトリクス、FIDO、TEE、TrustZone、サイバー攻撃対策、IoT

（２）中央大学研究開発機構
辻井Gの活動紹介
（NICT委託研究内容のみ）

組織間機密通信のための公開鍵システムの研究開発

クラウド環境に於ける機密情報・パーソナルデータの保護と利用の両立に向けて



A-1-1 多変数公開鍵暗号方式/楕円ElGamal・Cramer-Shoup暗号方式

研究開発成果概要図

（３）NICT委託研究成果
「組織暗号」解説

組織間の通信（組織通信）

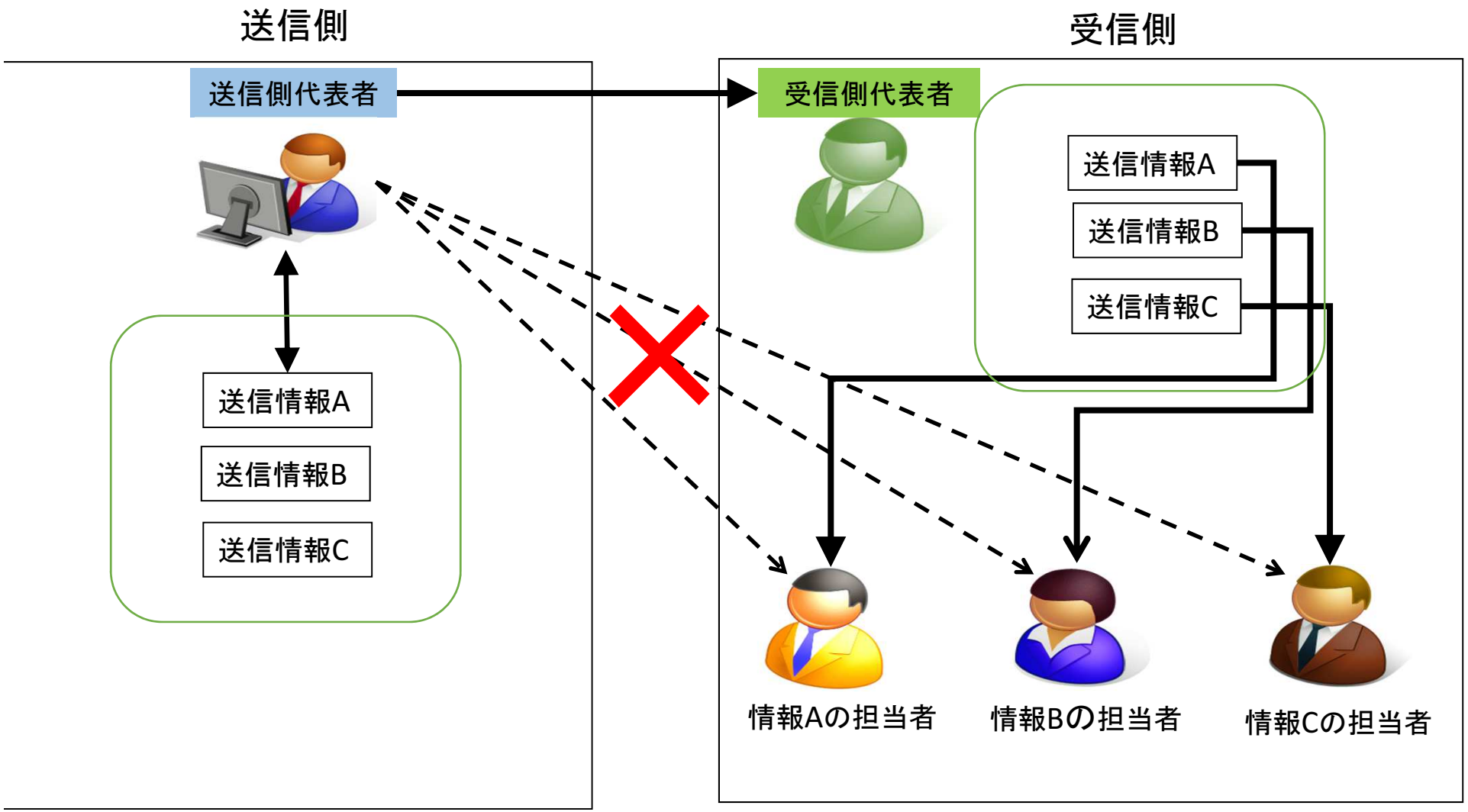
（1）自治体間の個人情報に関する通信の急増

社会保障・税番号（マイナンバー）の配布開始、
社会保障分野，税分野，災害対策分野において、
マイナンバーの利用が順次開始される予定。
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。

（2）医療・介護機関間の医療情報に関する通信の急増

医療・介護の総合的なサービス体制においては、
患者・利用者の視点に立ってサービスが提供され、
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・利用者の医療情報の相互利用が促進される。

組織通信の特徴　－　転送の発生



組織通信のための暗号：組織暗号

機密情報保護のための暗号技術

送信者は受信者を特定し、

その受信者のみが復号できるよう暗号化を実施

従来の暗号技術（個人通信向け暗号技術）の課題

受信者が復号する必要が無く、

その暗号化情報を他の利用者に安全に送信する場合でも、

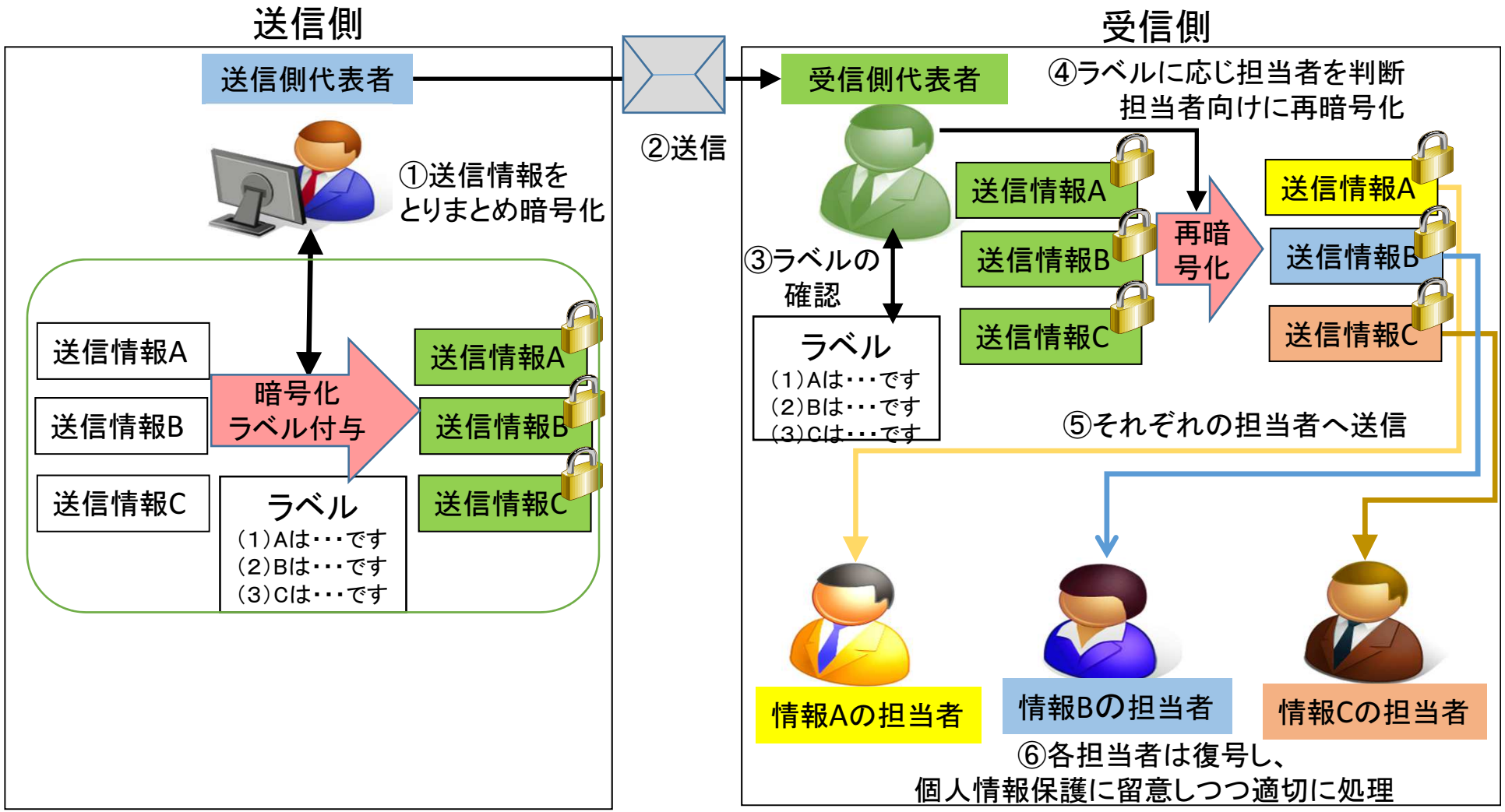
受信者は、必ず一旦復号し、

あらためて利用者向けに暗号化を行う必要がある

従来の暗号技術は、転送の多い組織通信には不向き！

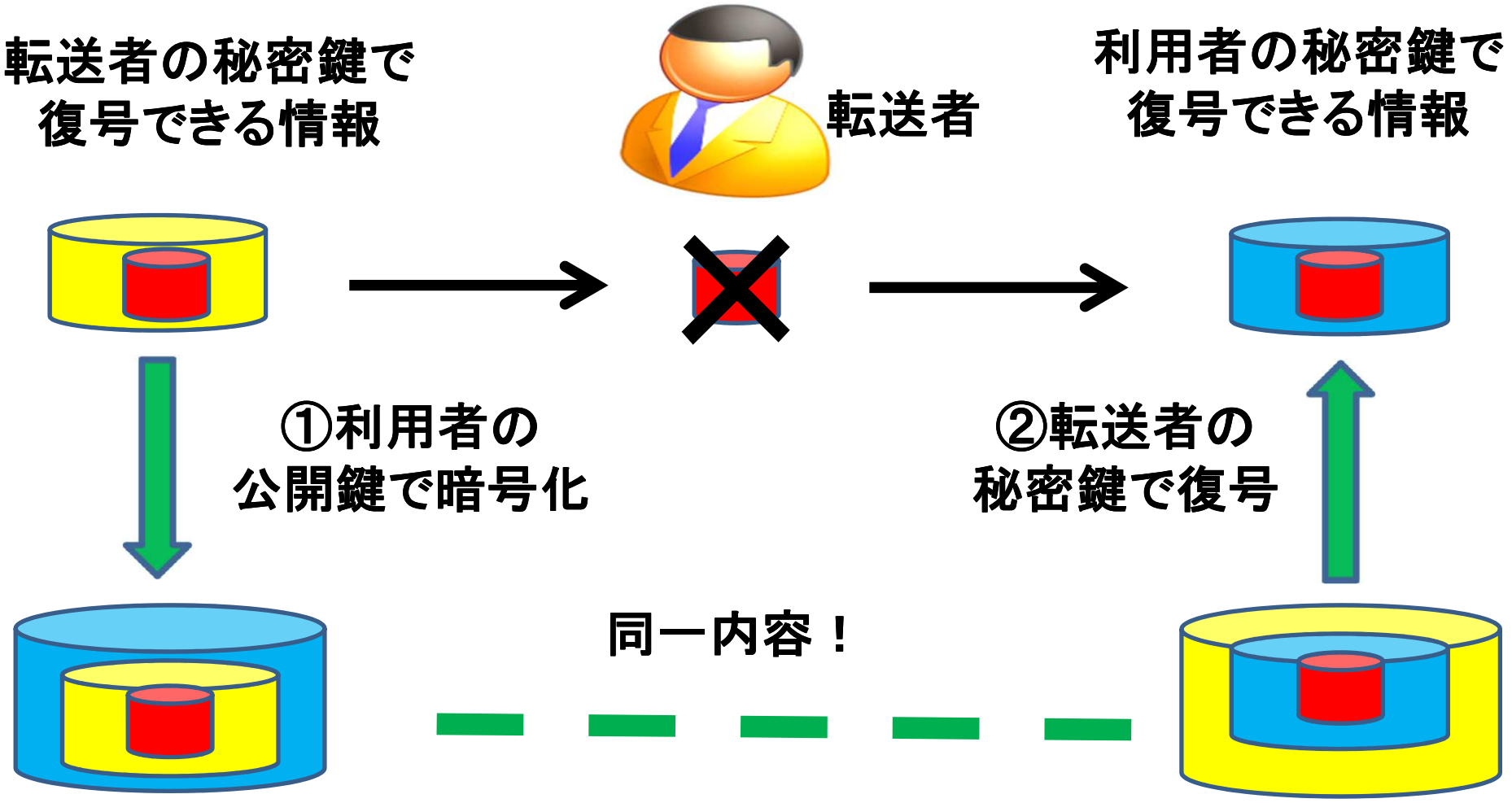
➔ 安全な転送が可能な暗号が　組織暗号！

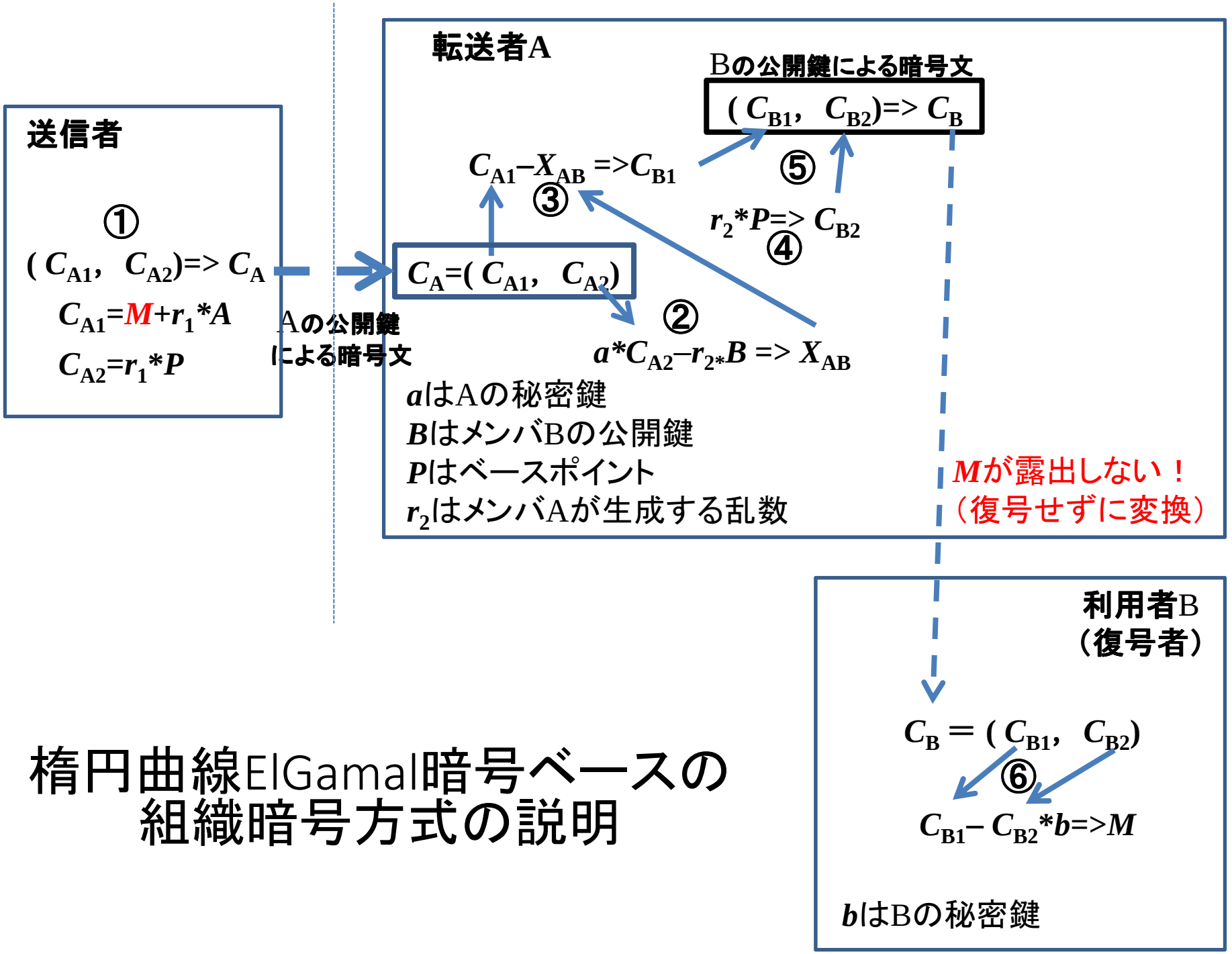
安全な転送を可能とする組織暗号



組織暗号は、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」の成果

組織暗号では、なぜ安全に転送が可能なのか？





楕円曲線ElGamal暗号ベースの組織暗号方式の説明

（４）NICT委託研究活動
「組織暗号の実証実験」紹介

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）

組織暗号実証実験式次第（2015年6月5日）

司会　　才所敏明　中央大学　研究開発機構　専任研究員

14:45～　　挨拶

吉高昌広　　兵庫県　企画県民部　情報企画課長
辻井重男　　中央大学　研究開発機構　機構教授

14:55～　　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

15:35～　　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　事務局長
中央大学　研究開発機構　客員研究員

15:50～　　組織暗号　－兵庫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

16:05～　　組織暗号　－実験システム動作説明－

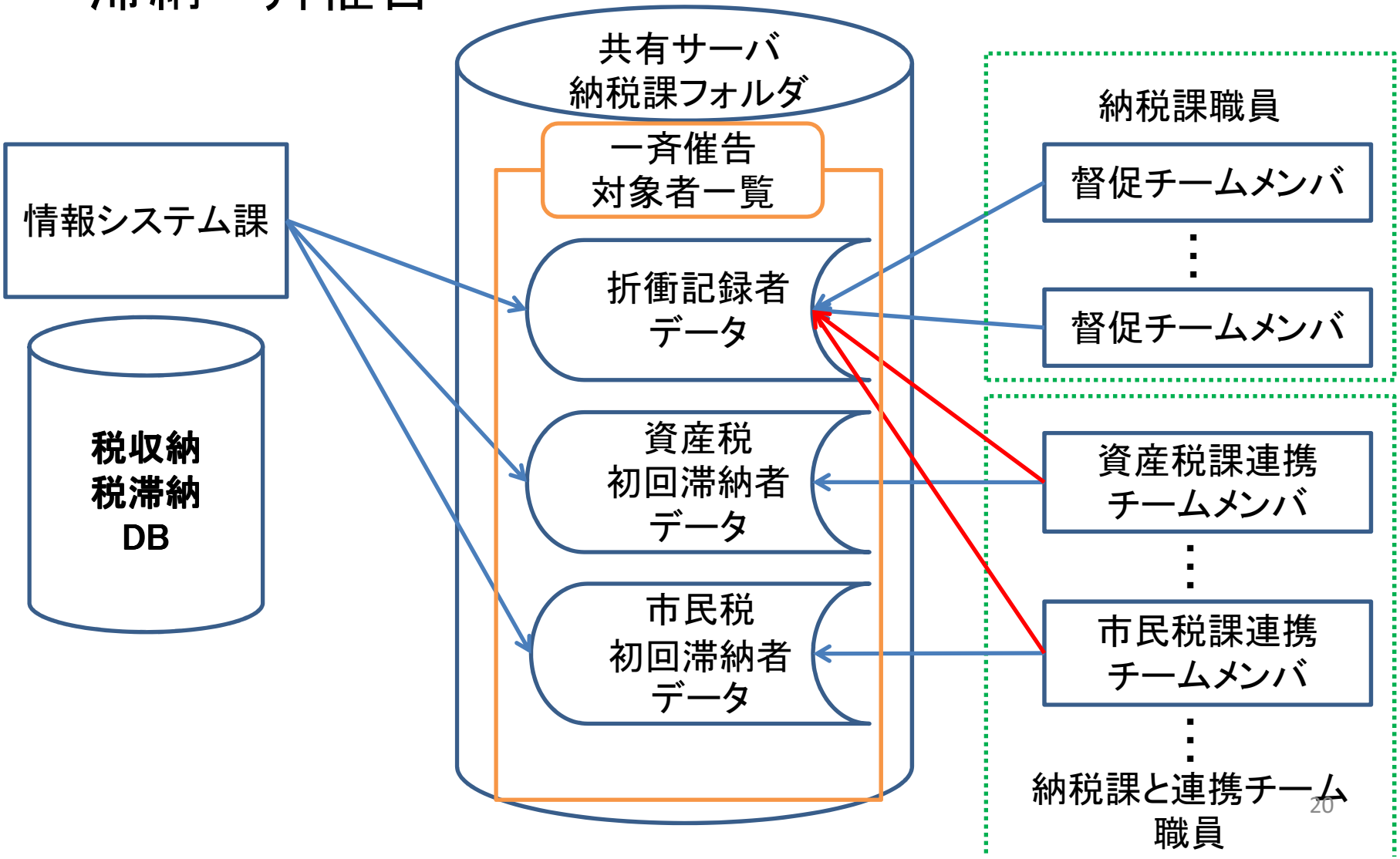
庄司陽彦　　YDKコミュニケーションズ
中央大学　研究開発機構　客員研究員

16:25～　　質疑応答

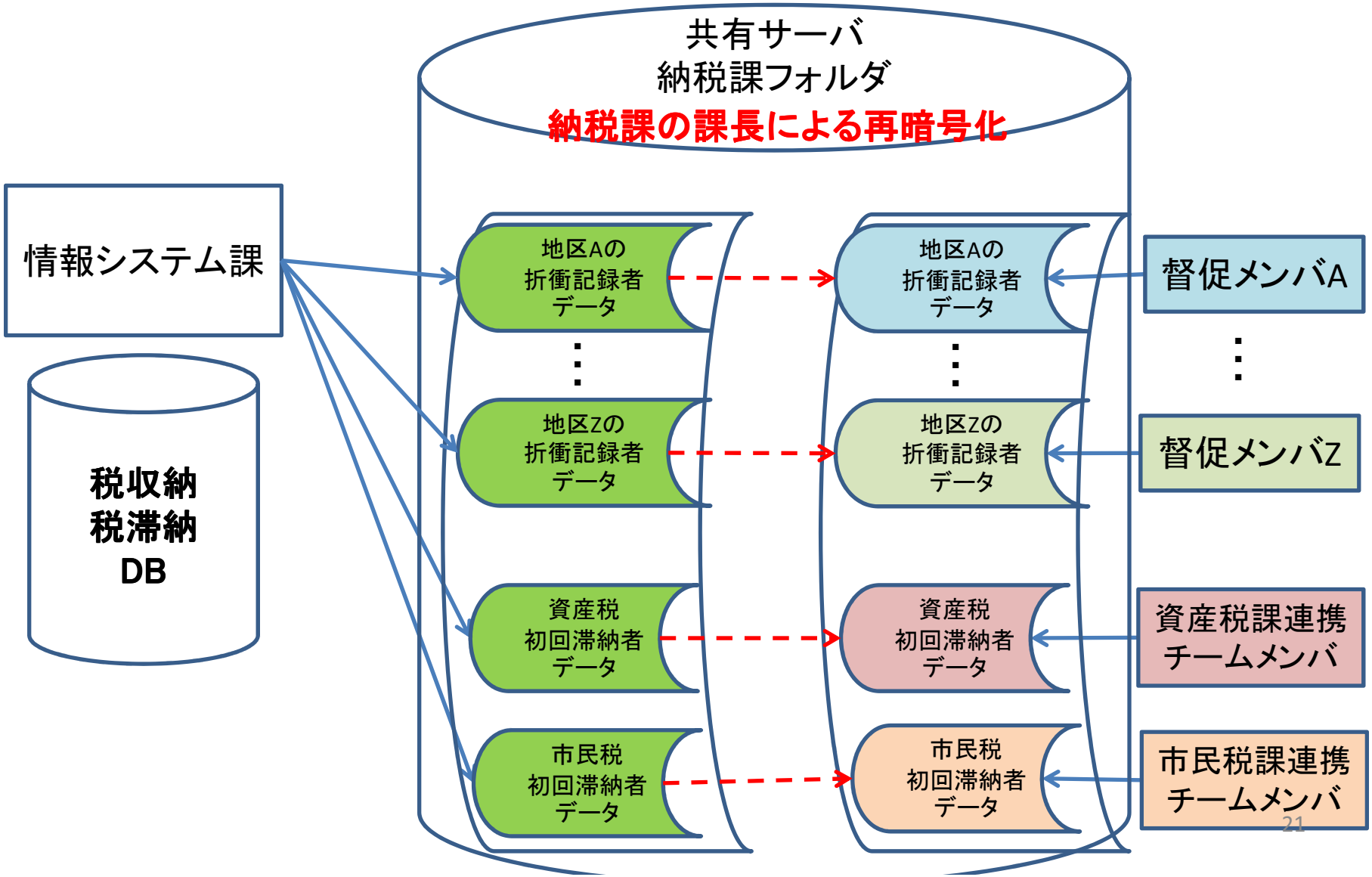
（　16:45　終了予定　）

組織暗号適用可能業務例
（兵庫県・西宮市）

滞納一斉催告

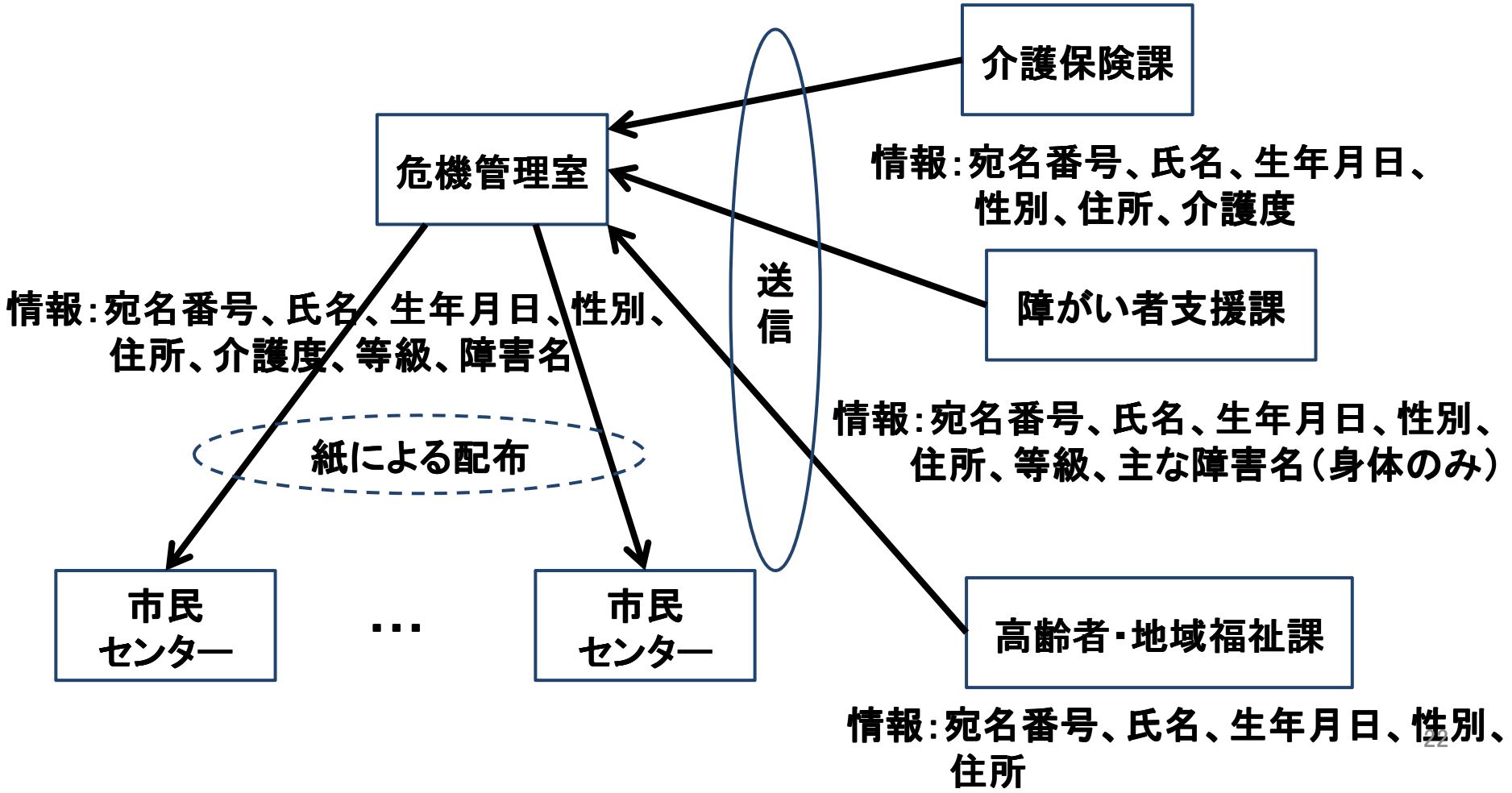


滞納一斉催告のデータの安全な引渡し案

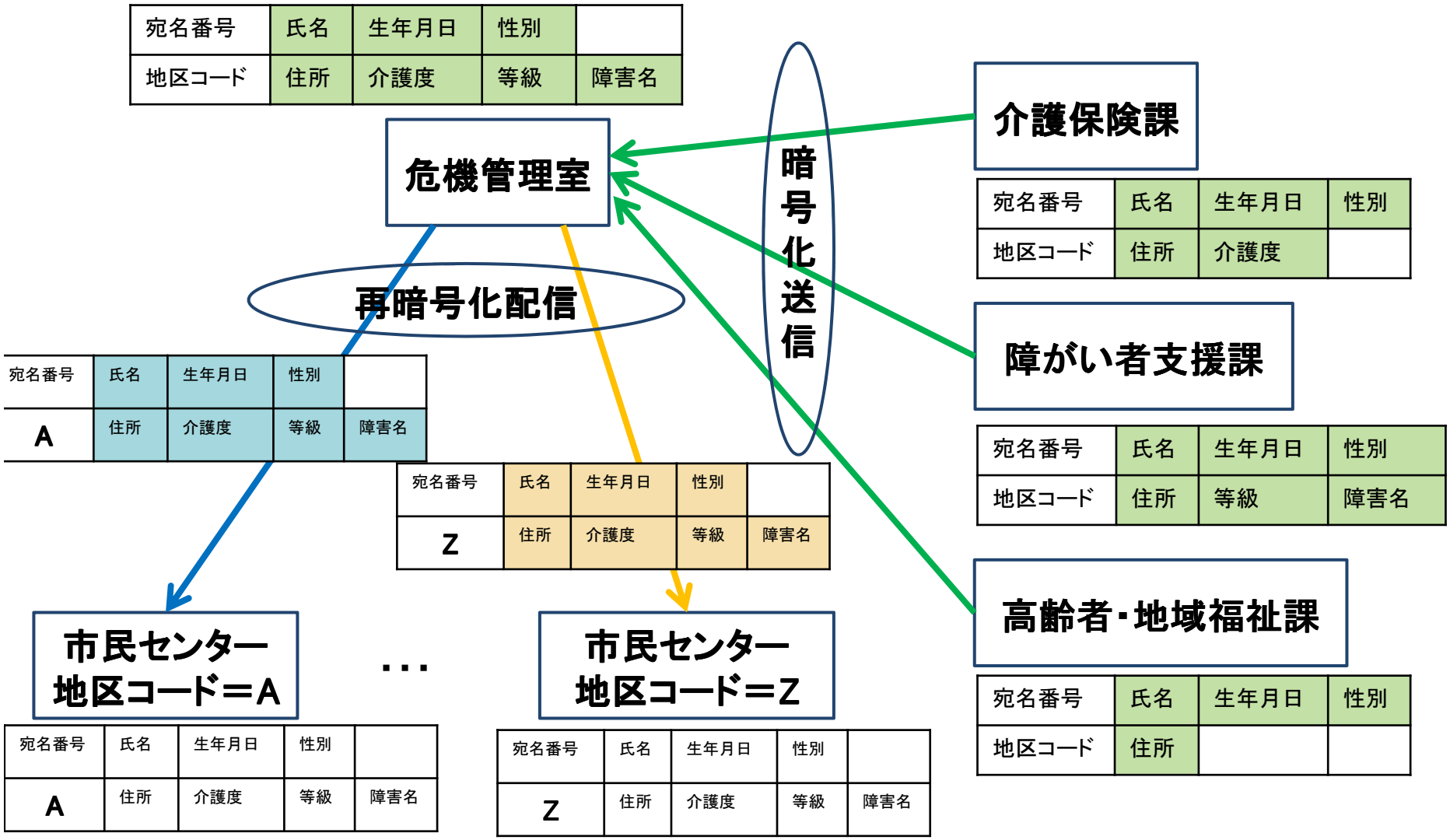


組織暗号適用可能業務例
（兵庫県・加古川市）

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



兵庫県での実証実験の模様

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－

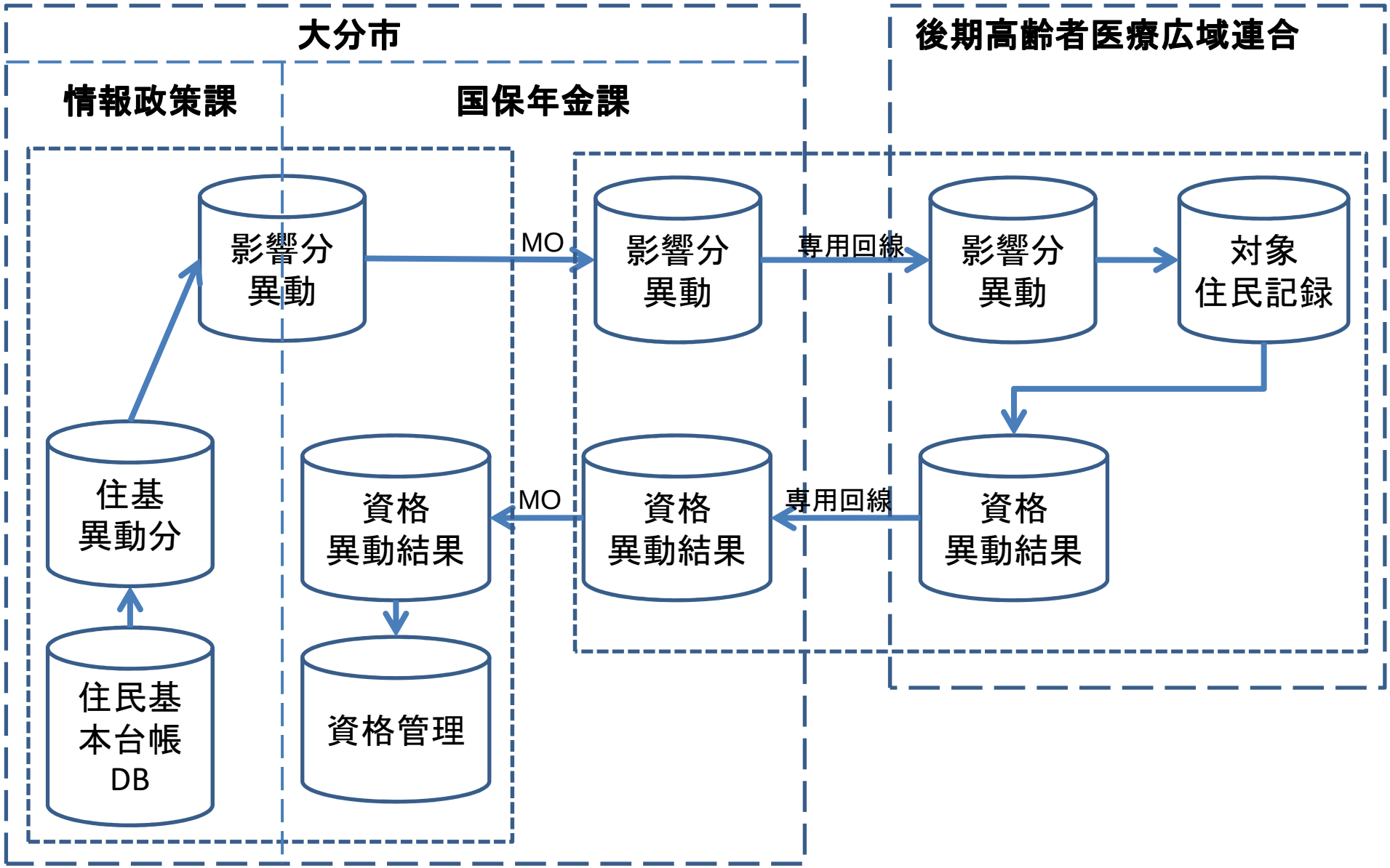
庄司陽彦　　YDKコミュニケーションズ

11:45～　質疑応答

（　12:00　終了　）

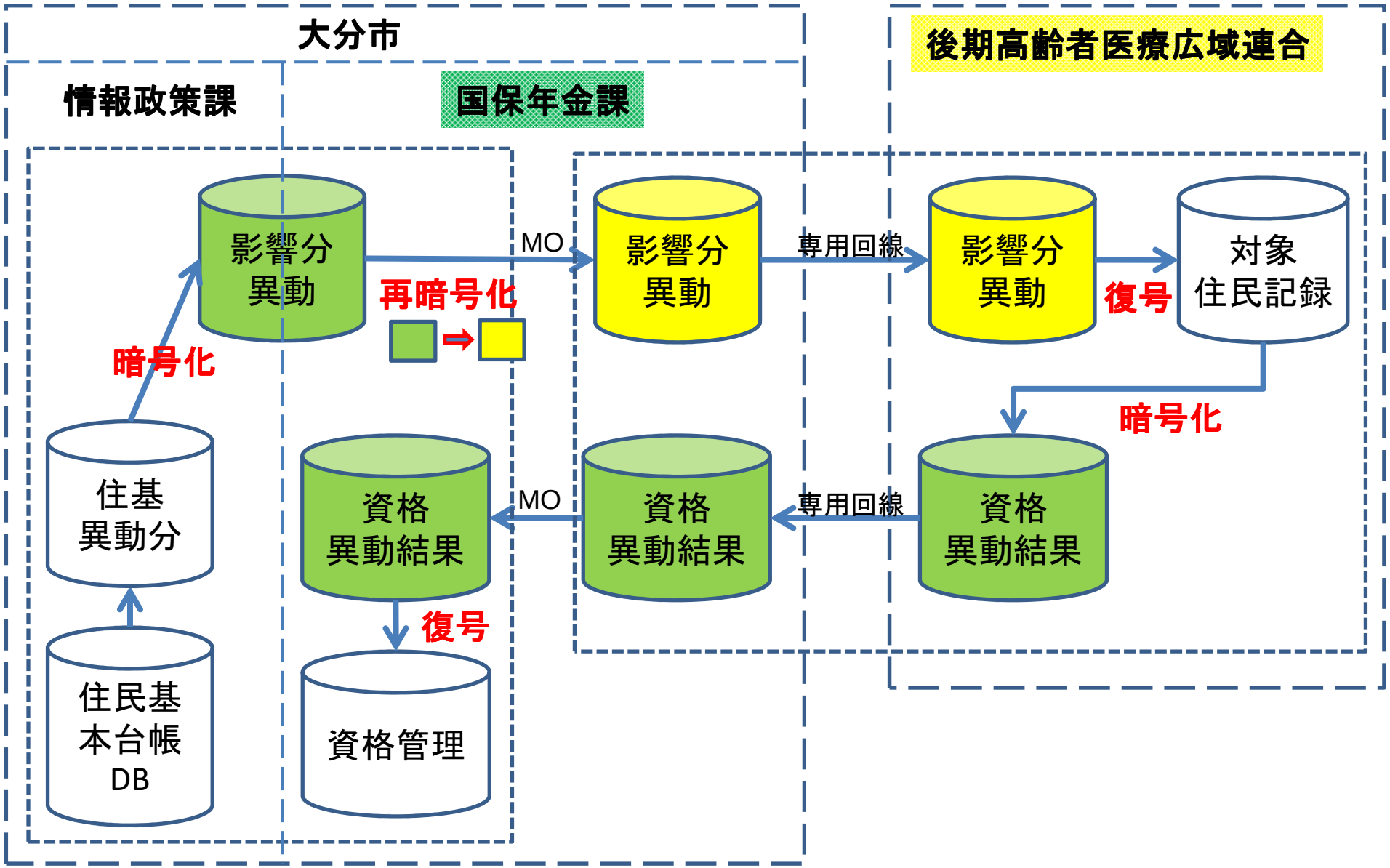
大分市役所

後期高齢者医療資格付与



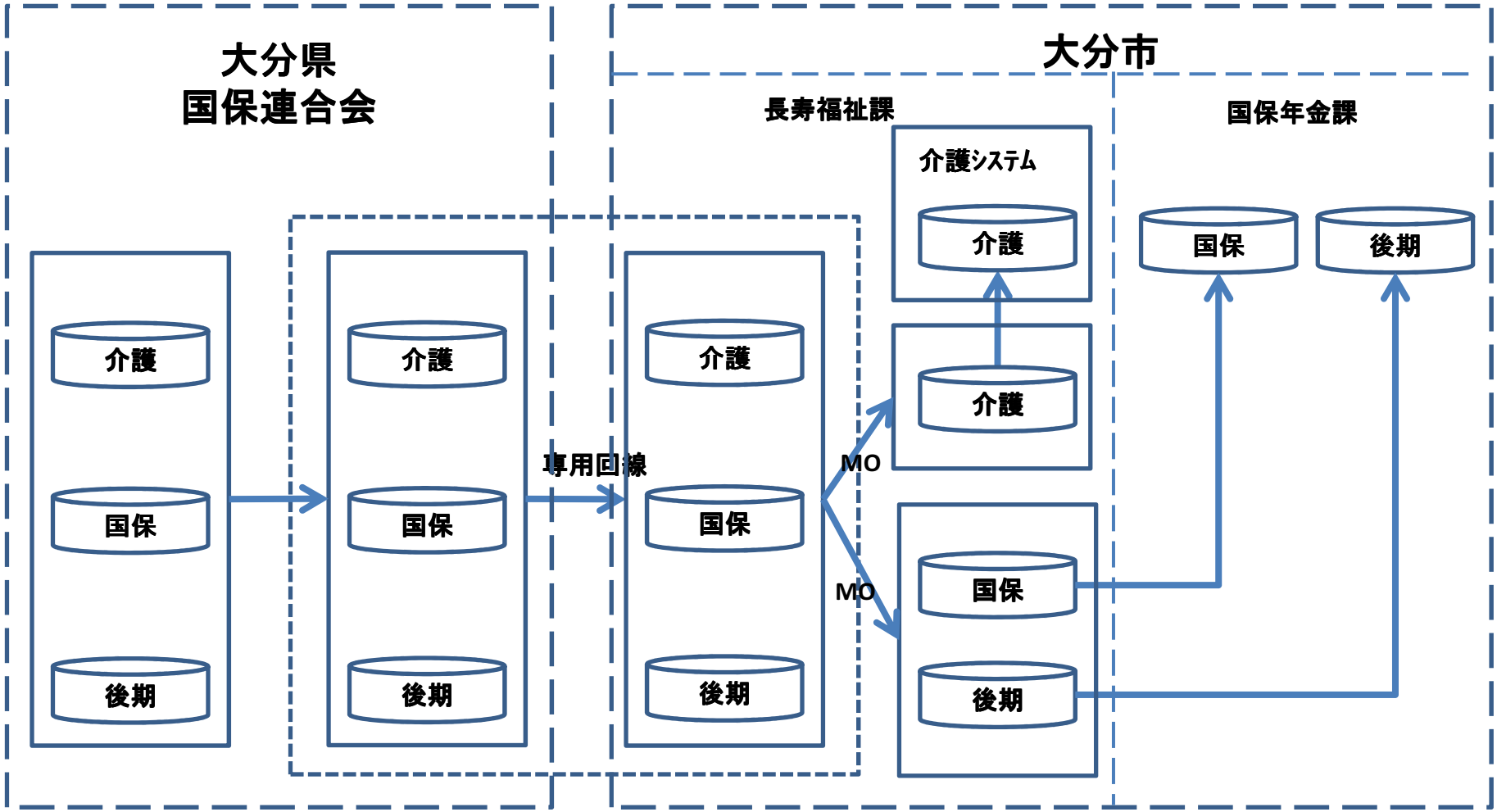
大分市役所

組織暗号適用方式例



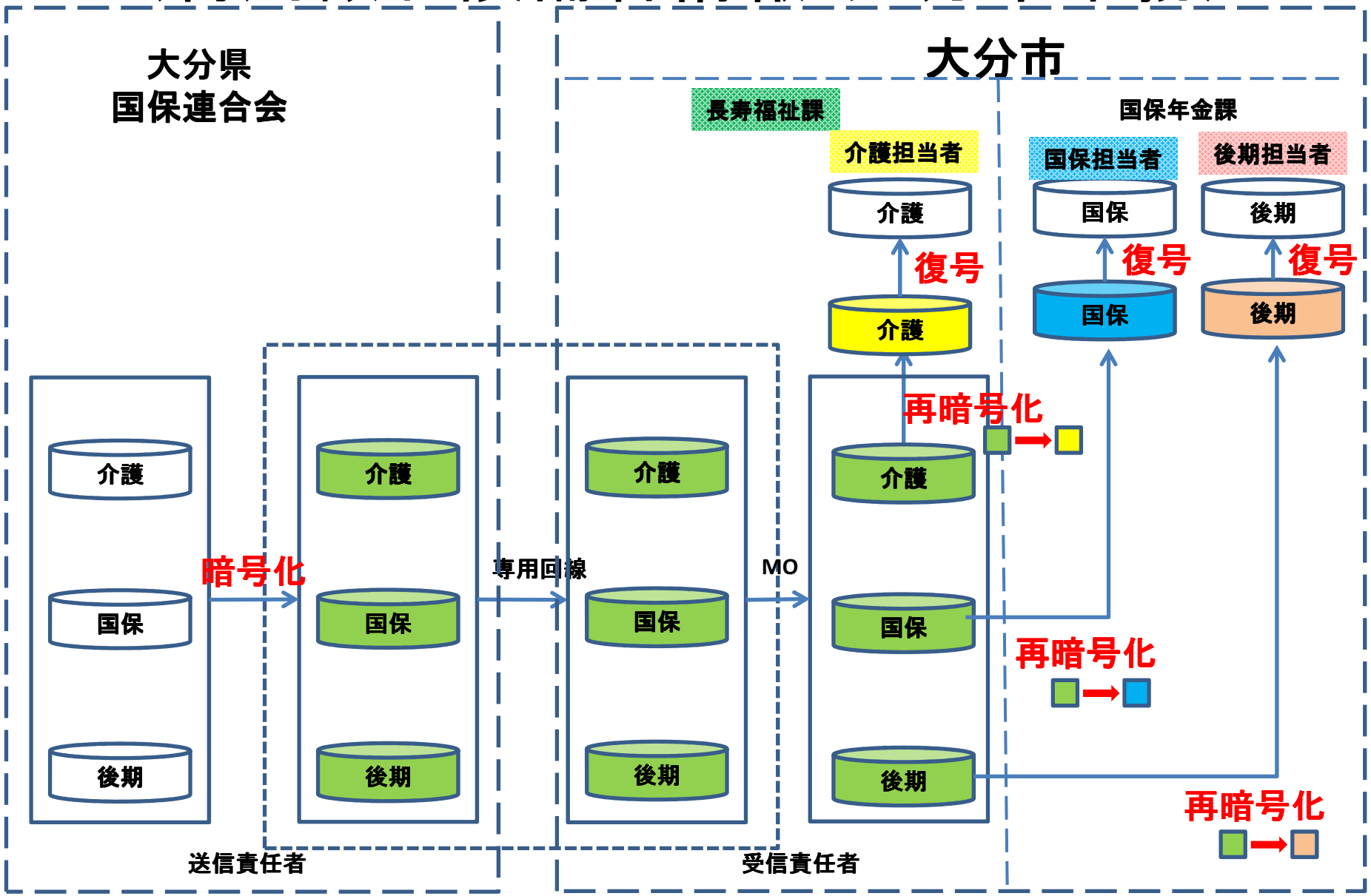
大分市役所

公的年金からの特別徴収
（特別徴収候補者情報・大分市業務）



大分市役所

公的年金からの特別徴収
（特別徴収候補者情報・大分市業務）



大分県での実証実験の模様

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

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（2015年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

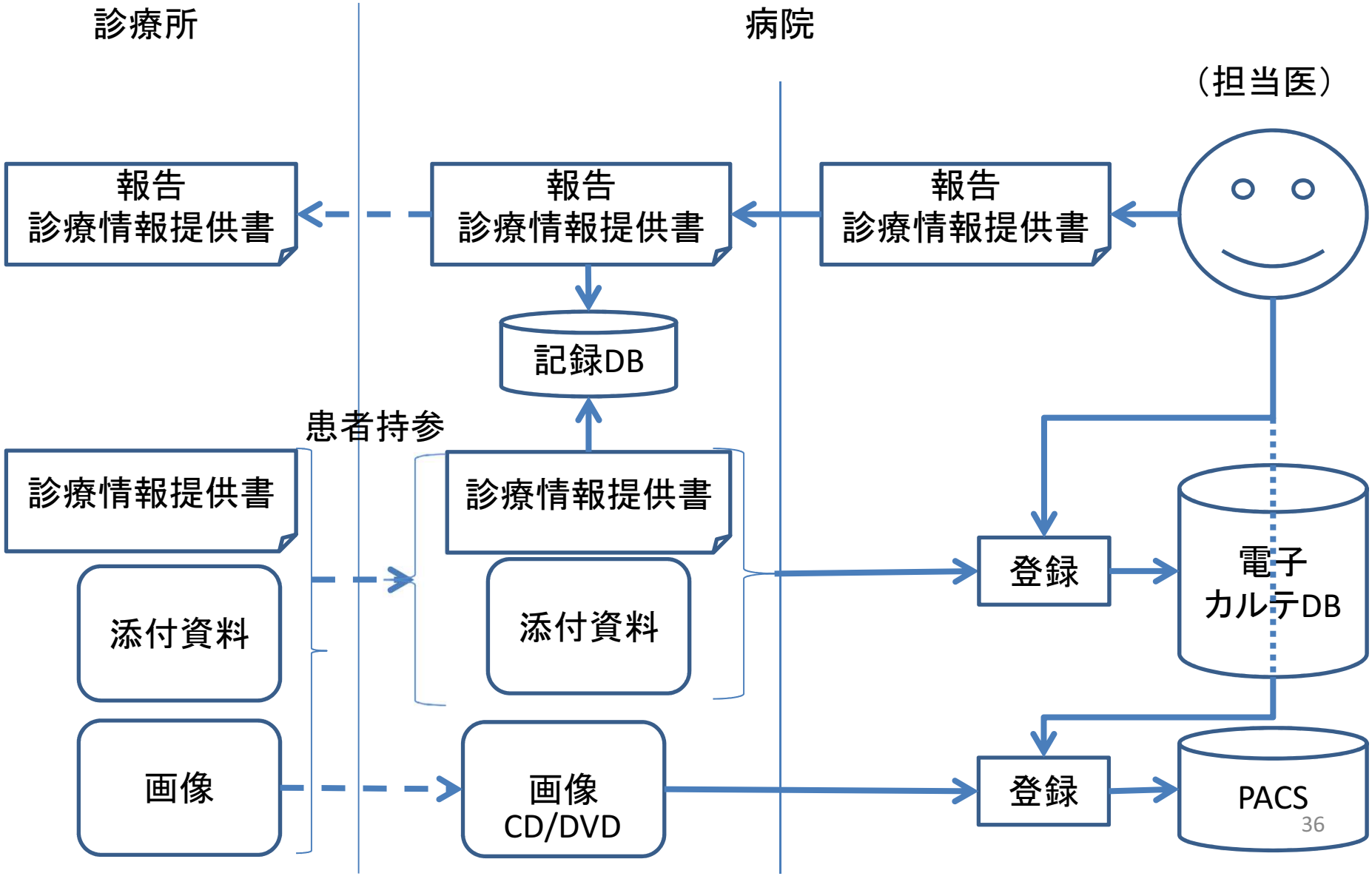
②医療情報送受・共有業務への適用例

③実験システムによるデモ

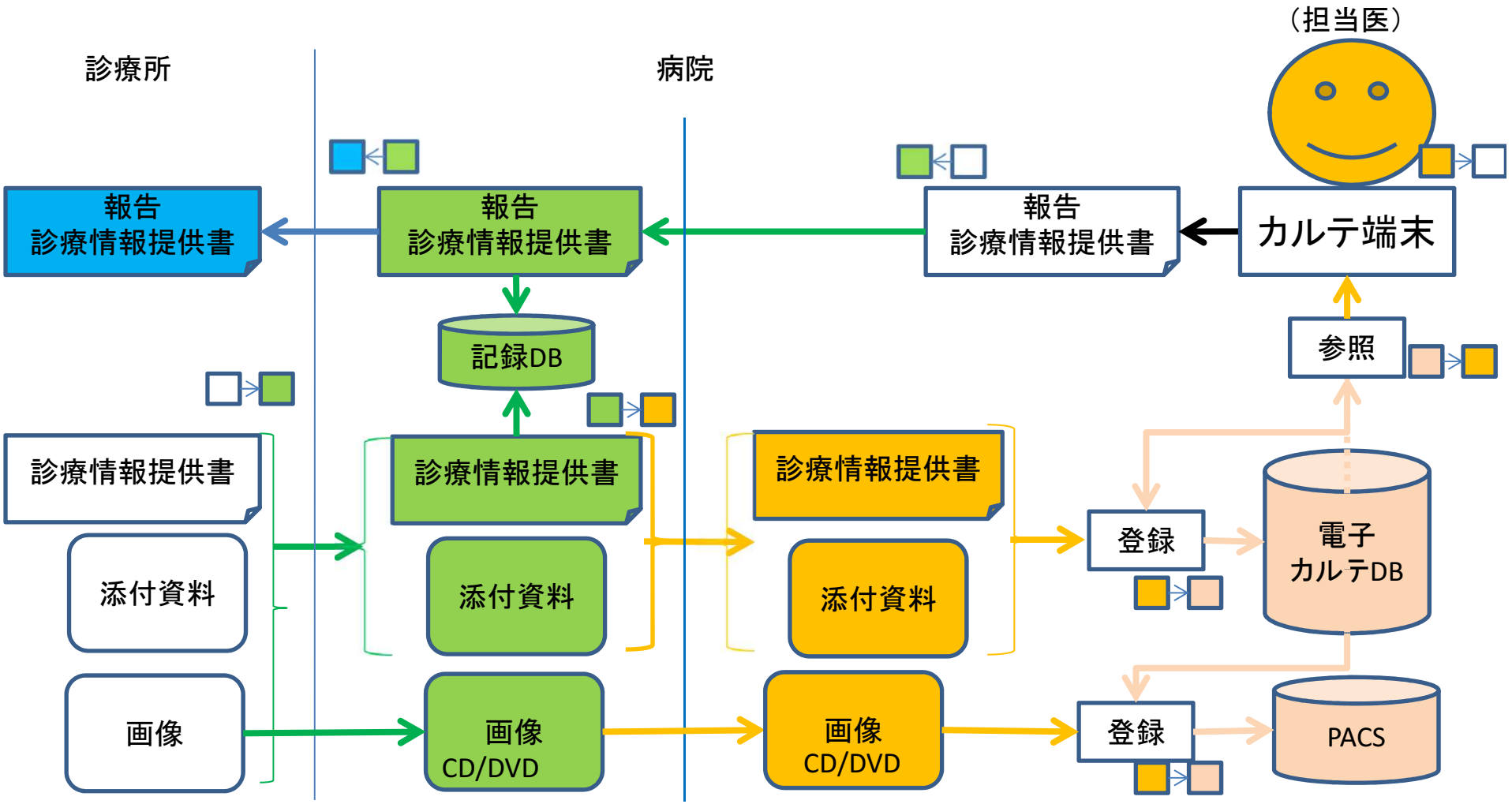
才所敏明

16:55～　質疑応答

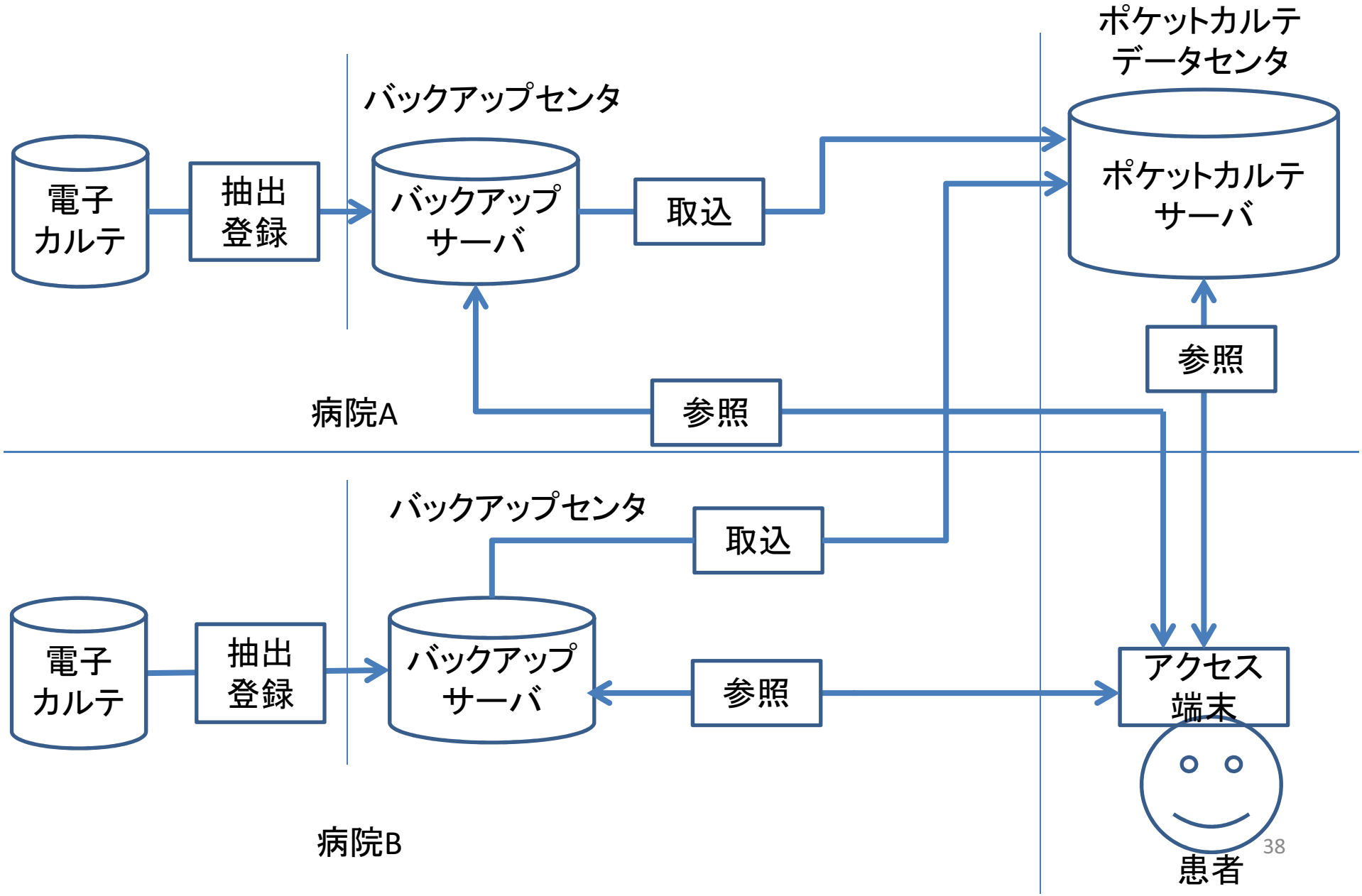
（1）紹介状（診療情報提供書）



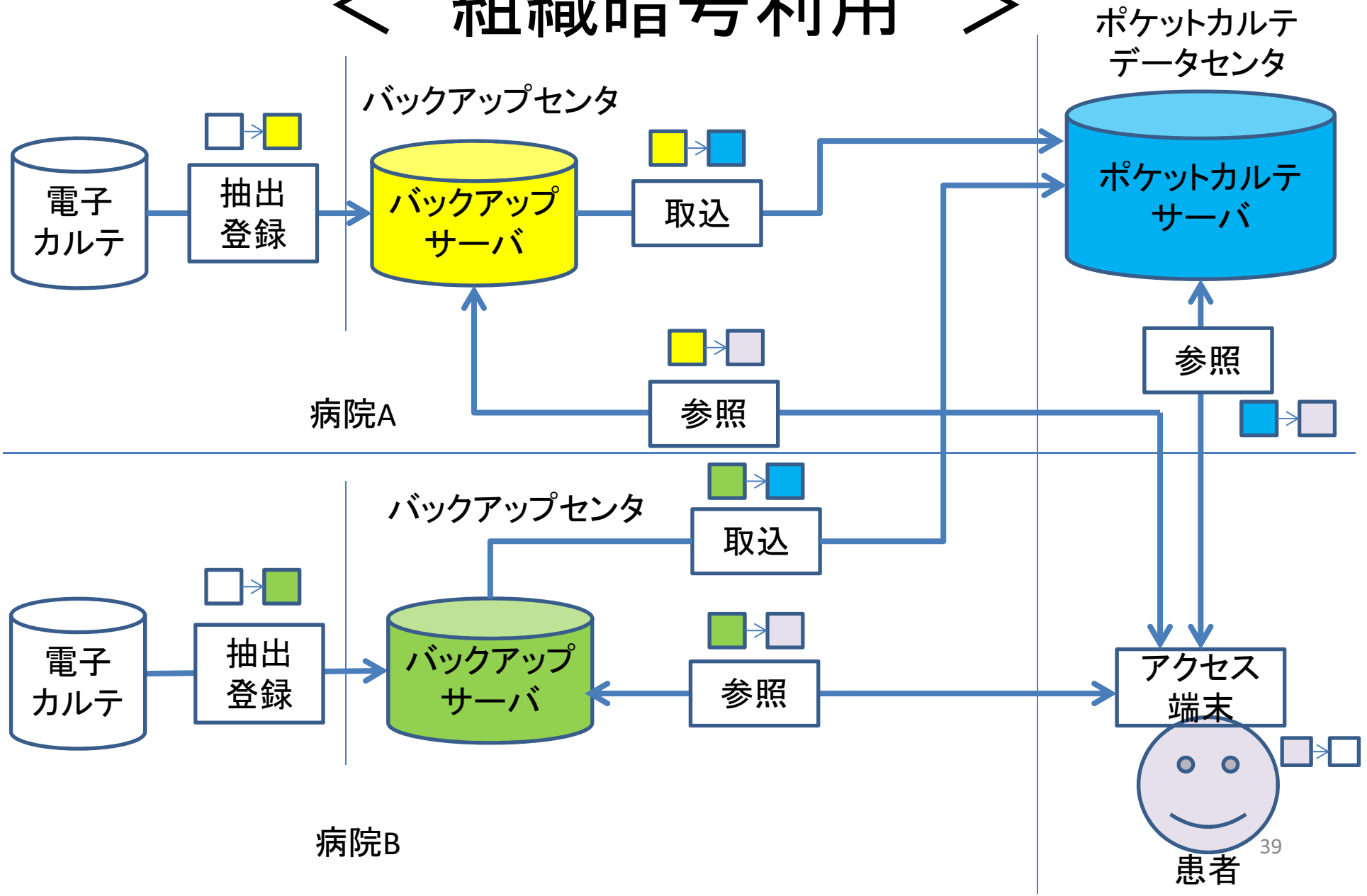
紹介状（診療情報提供書）
＜組織暗号利用＞



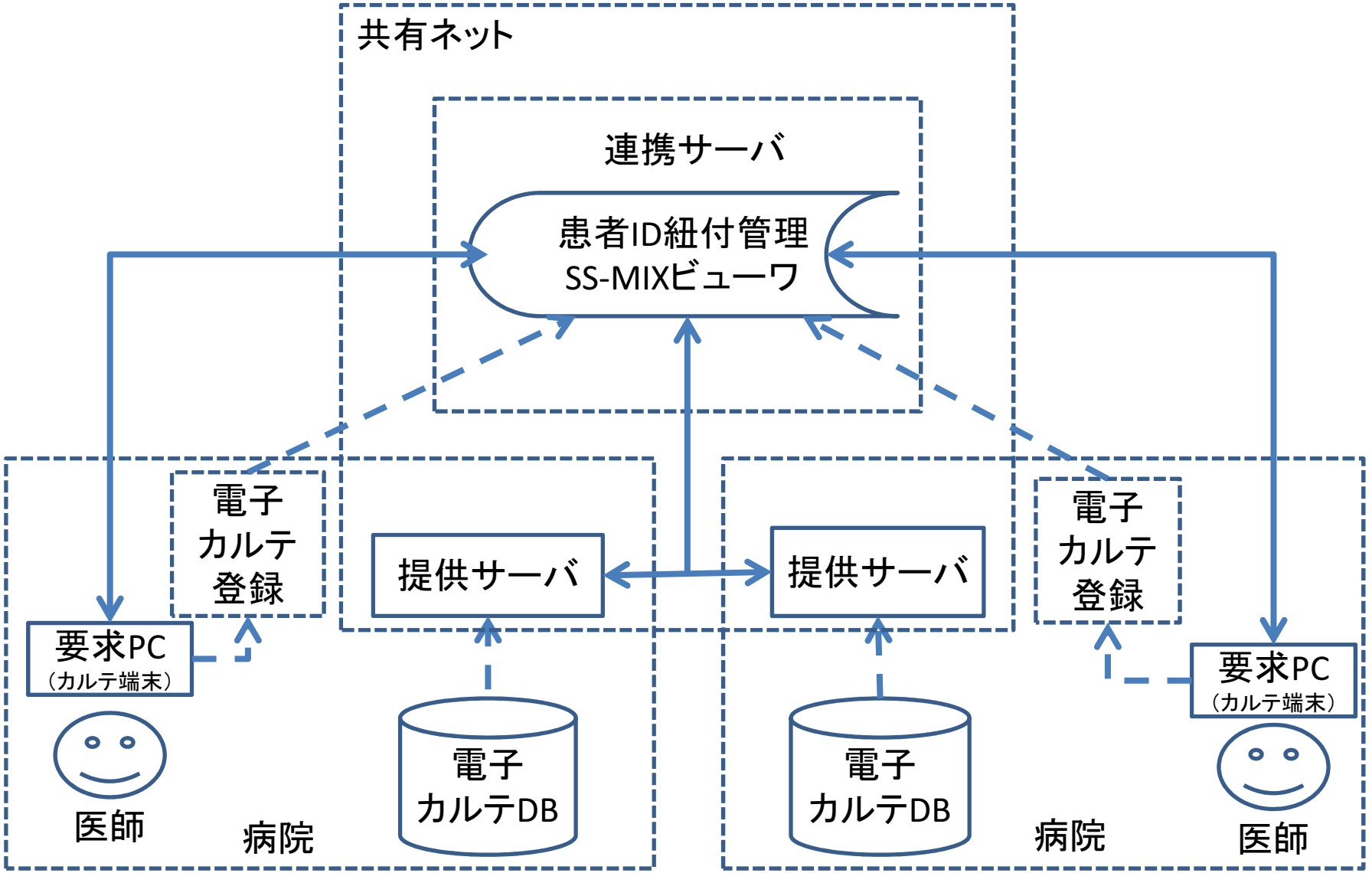
（2）ポケットカルテ


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　＞

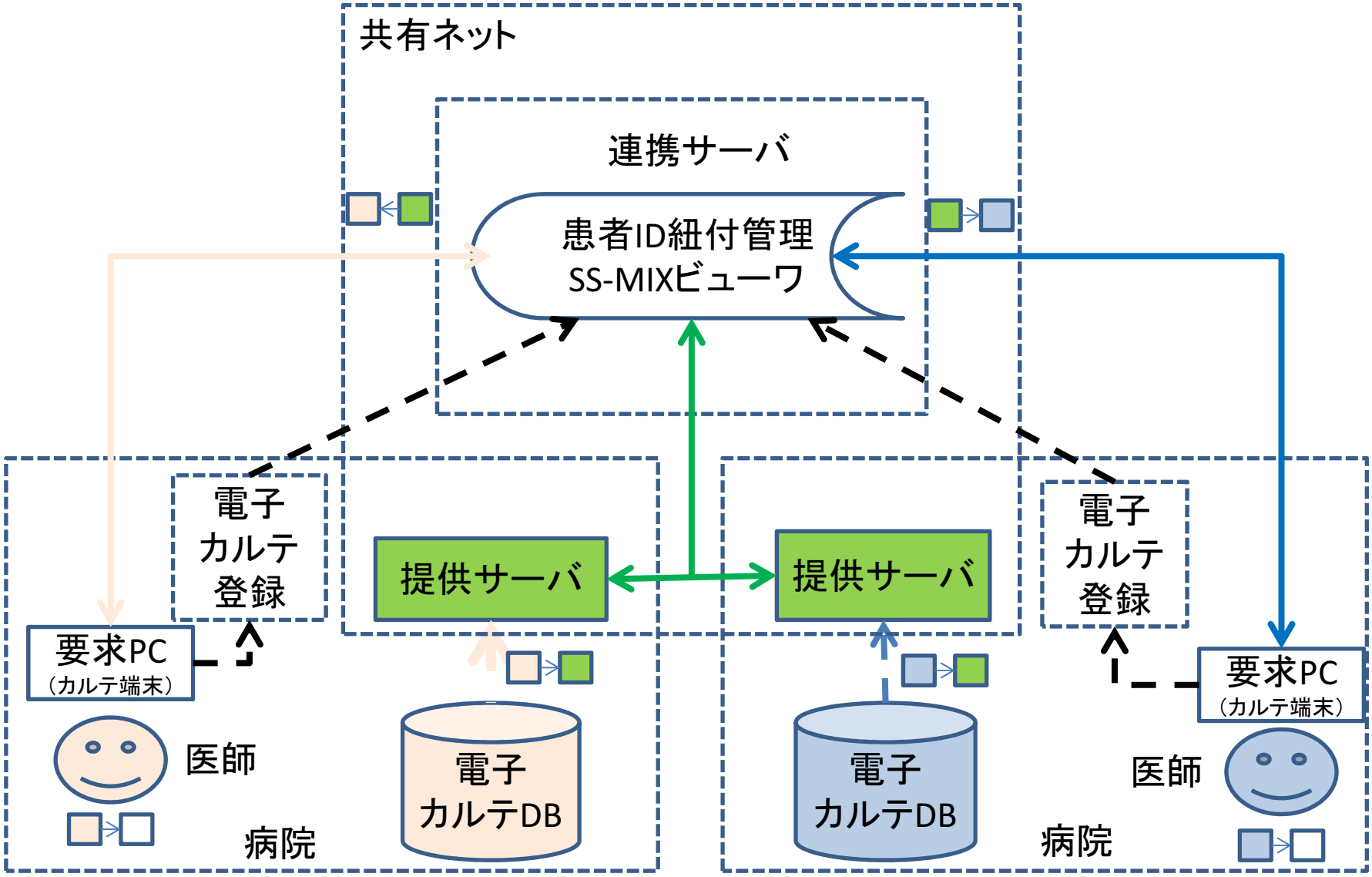


（3）電子カルテの共有



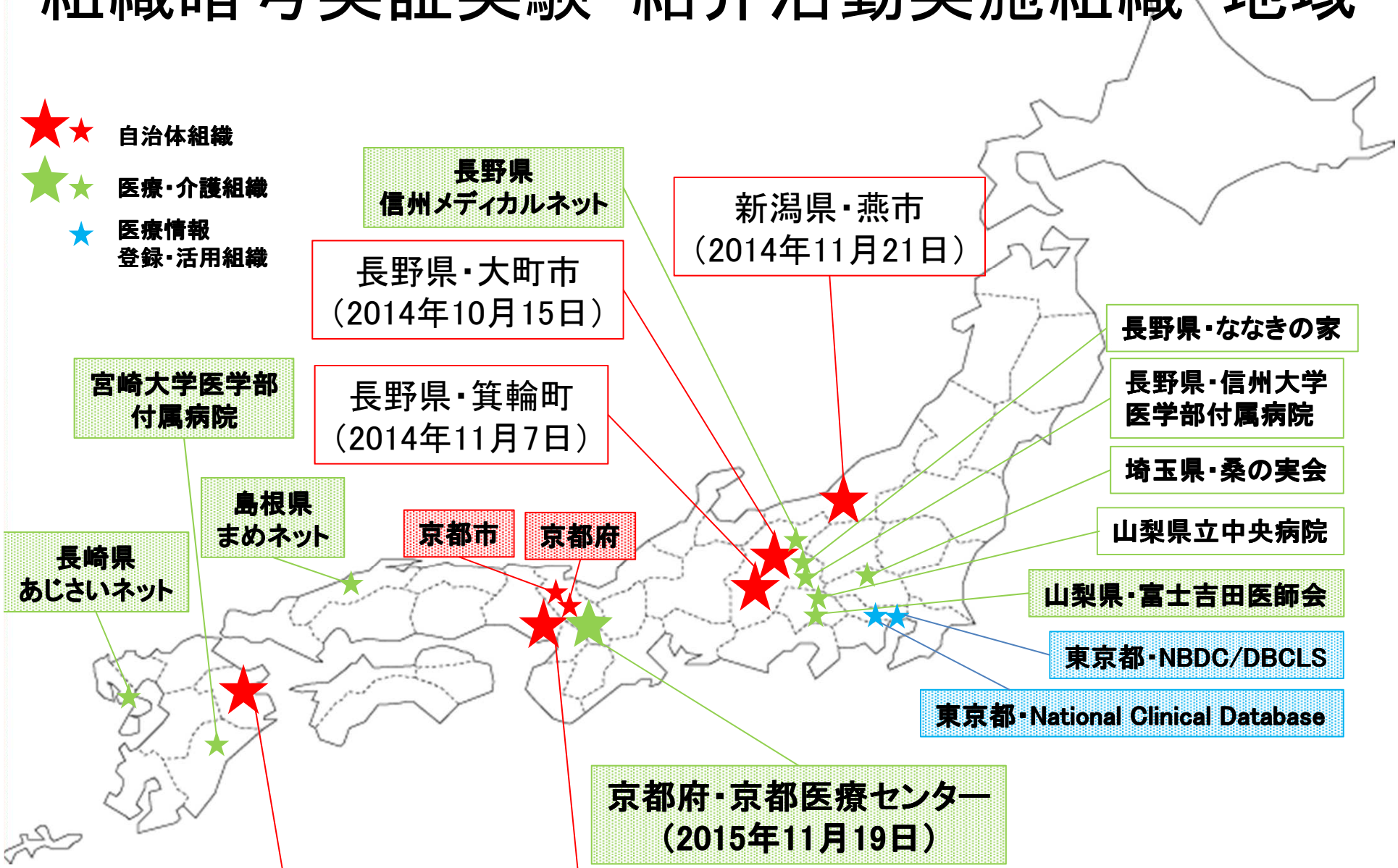
アクセス制御（患者が閲覧できる病院を指定）

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）

組織暗号実証実験・紹介活動実施組織・地域



組織暗号の社会実装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

（５）IoT関連活動への期待

情報セキュリティの専門家集団

（１）暗号・認証要素技術（中央大学研究開発機構）

軽量暗号、軽量認証技術

暗号化状態処理技術

高速秘密分散処理技術

（２）システムセキュリティ技術

システムセキュリティ分析・基本設計技術

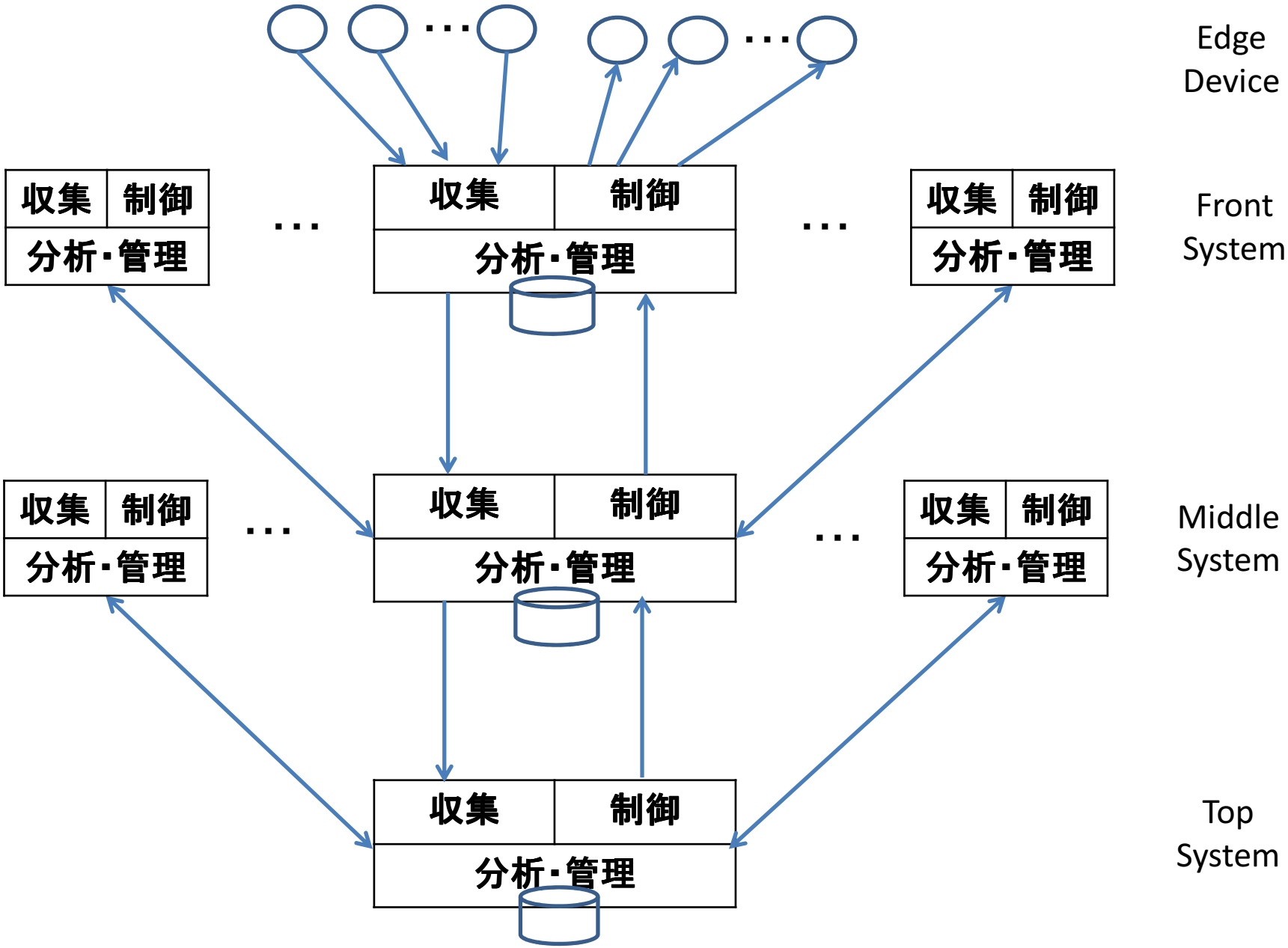
暗号・認証要素技術の応用技術

（３）セキュアシステム実装技術

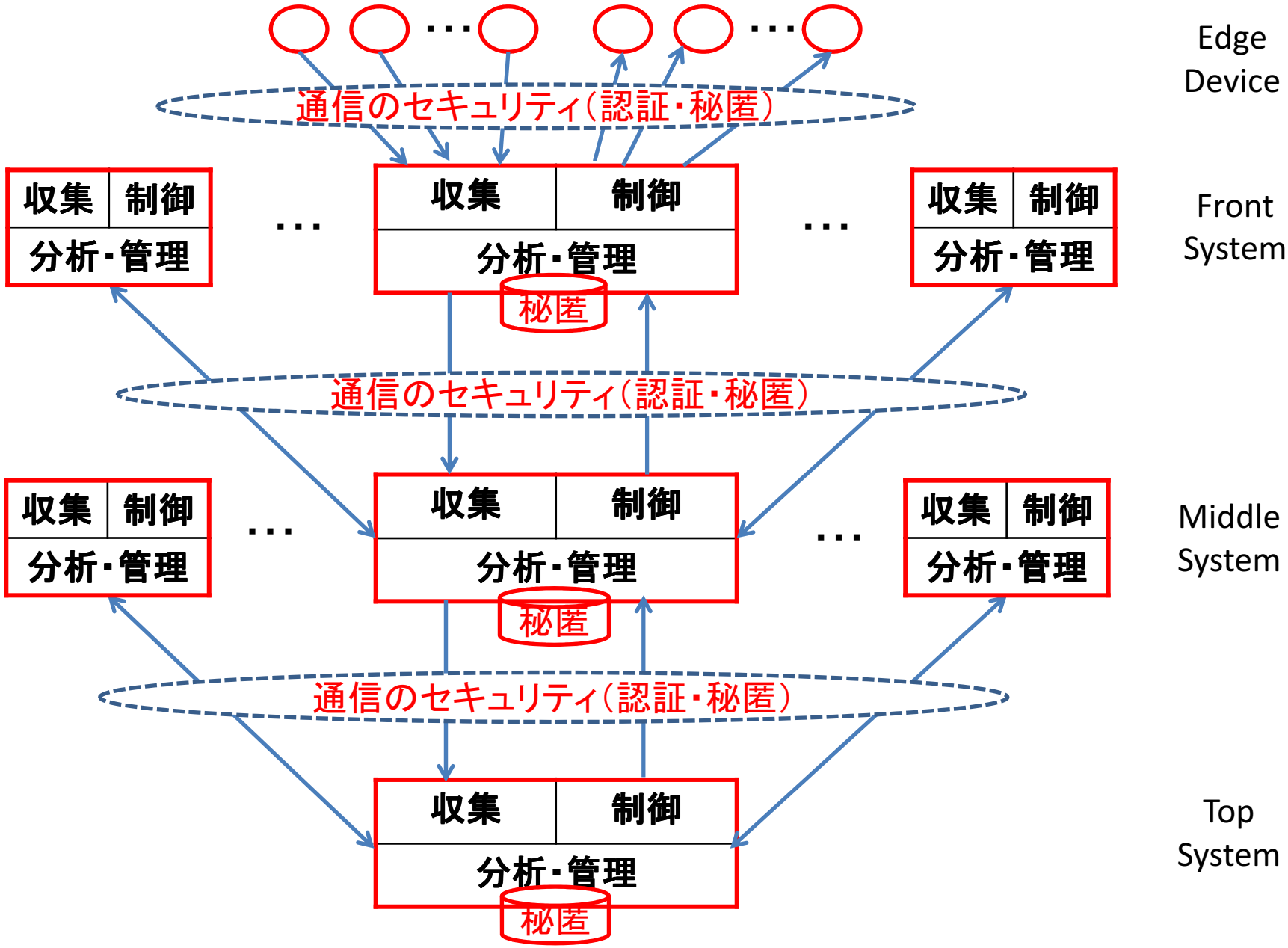
（４）公的資金対応PJ企画・提案技術

（６）IoT関連活動状況紹介

IoTネットワークアーキテクチャ

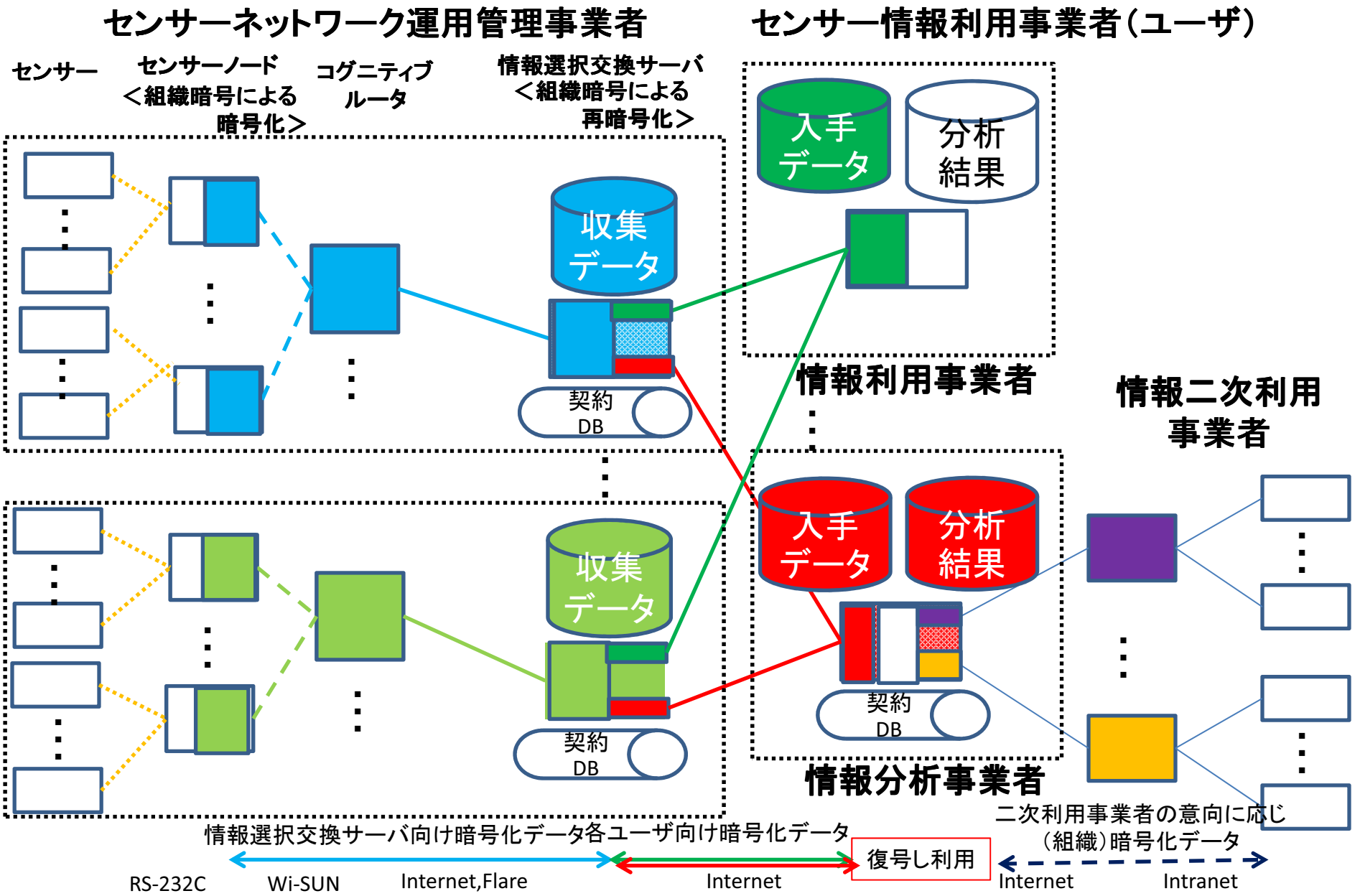


IoTネットワークにおけるセキュリティ

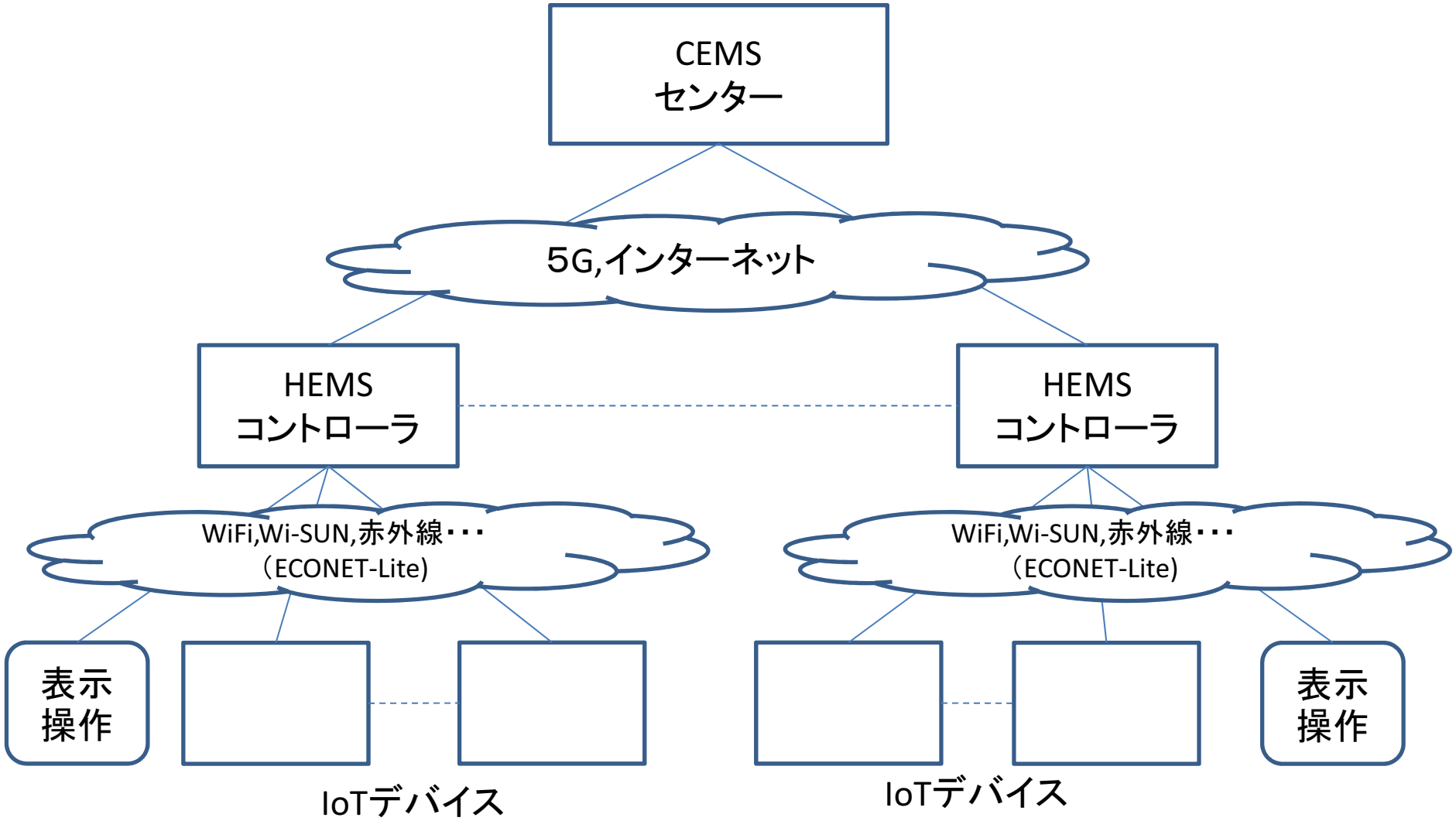


IoTマルチテナントセキュアネットワーク

中央大学研究開発機構　才所敏明（2016.05.06 版）

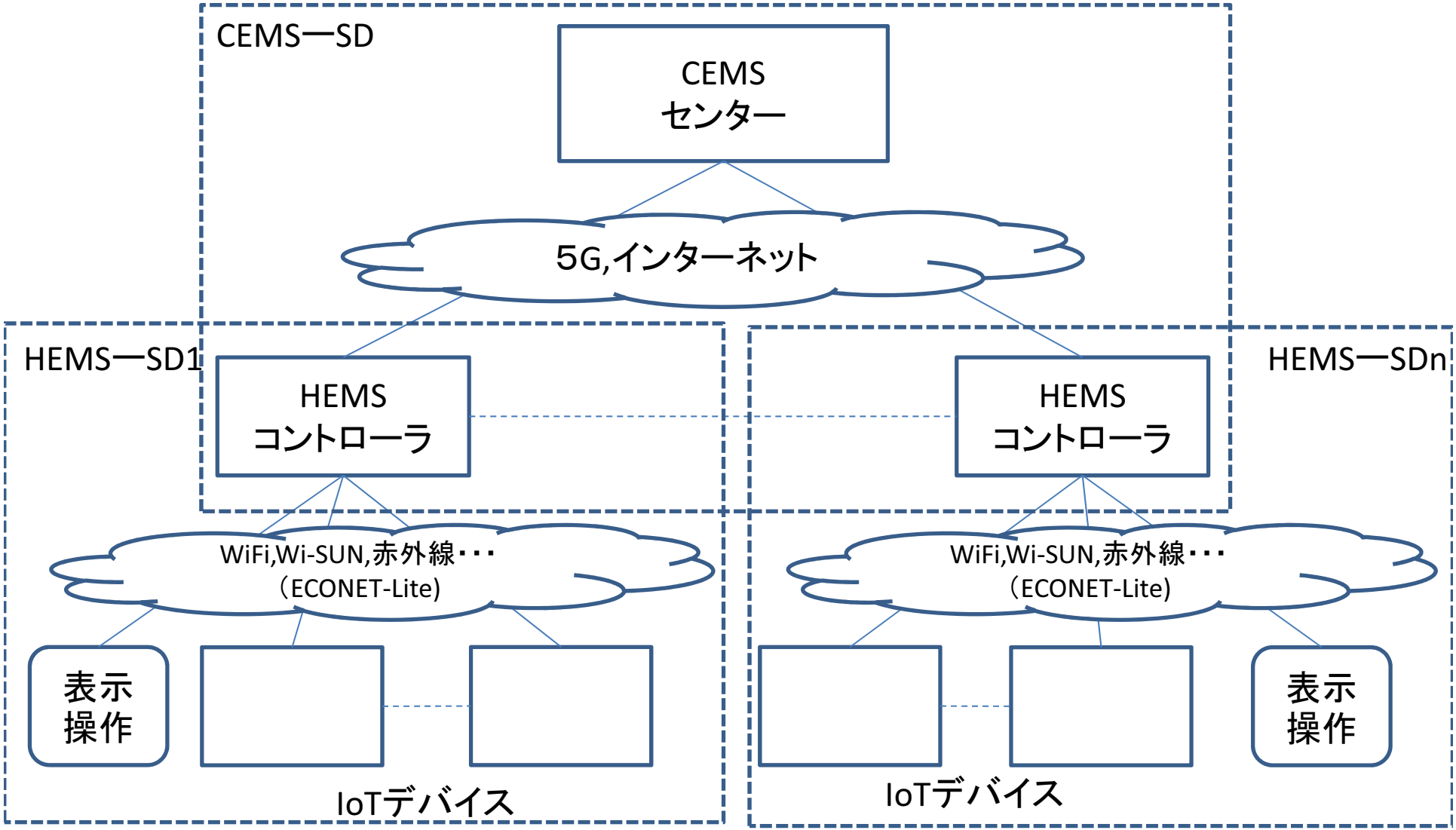


CEMS-HEMSアーキテクチャ



CEMS-HEMSアーキテクチャ

セキュアドメイン（SD）の連鎖による全体として安心安全なIoTネットワークの実現



終