Innovative R&D by NTT

プライバシー情報の保護と活用を両立させる技術基盤

2014.9.4

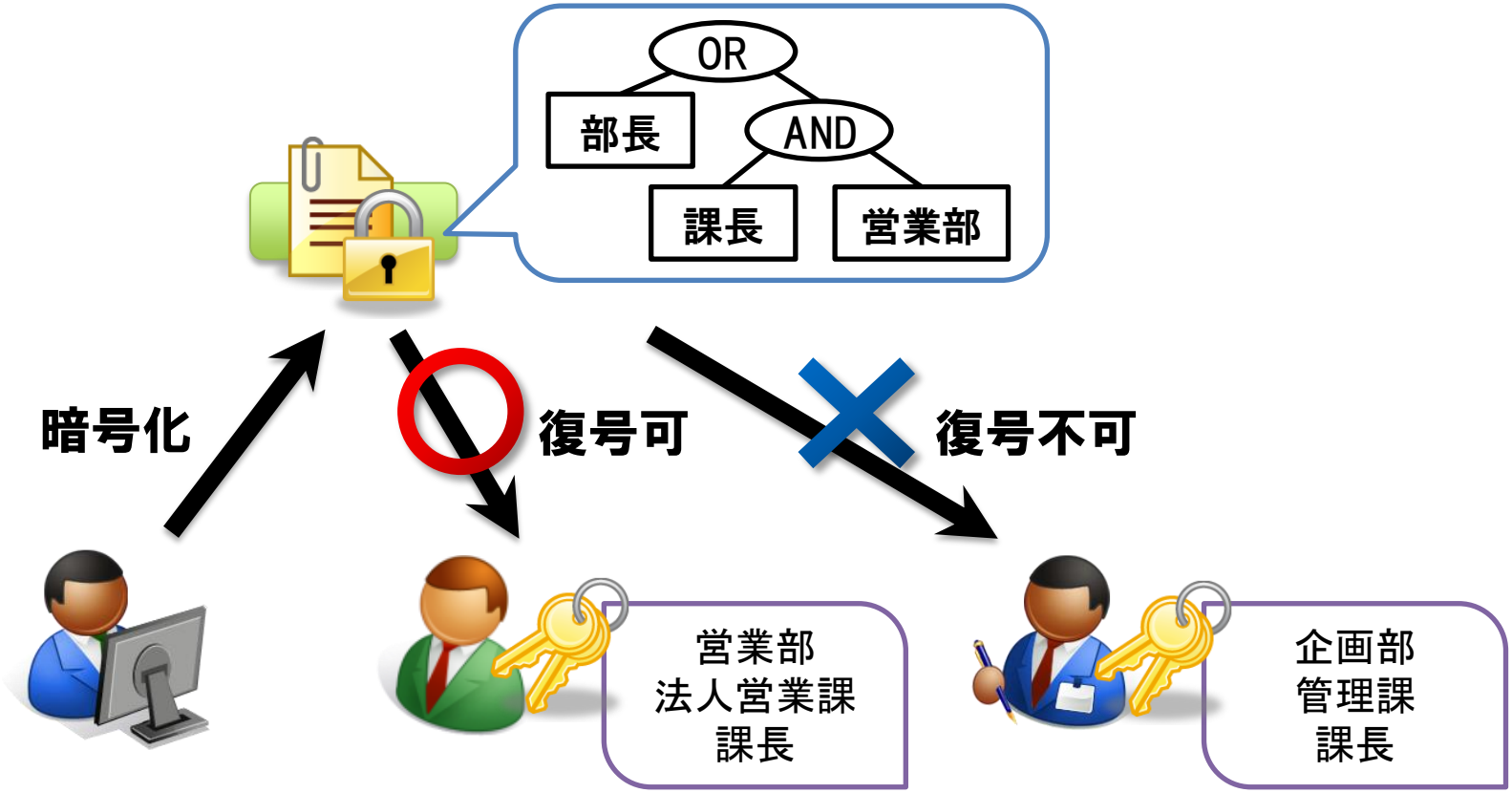
NTTセキュアプラットフォーム研究所
高橋克巳

あらまし

- プライバシー情報の保護と活用に関する暗号分野から貢献の可能性について述べる
- 暗号技術
  - もともと、暗号鍵の管理を行い情報の秘匿と開示を制御
  - 近年は、多様できめ細やかな情報の制御が可能に
- 紹介する技術
  - 時間や場所や人；条件で開示制御（インテリジェント暗号）
  - 複数人の合意で開示の制御（秘密分散）
  - 統計などの所定の計算結果を開示（秘密計算）
  - 情報を匿名化（非暗号）
- 情報の保護と活用の両立のため
  - 暗号技術をベースに人を含む系のマネジメントを融合した基盤を構築することが重要

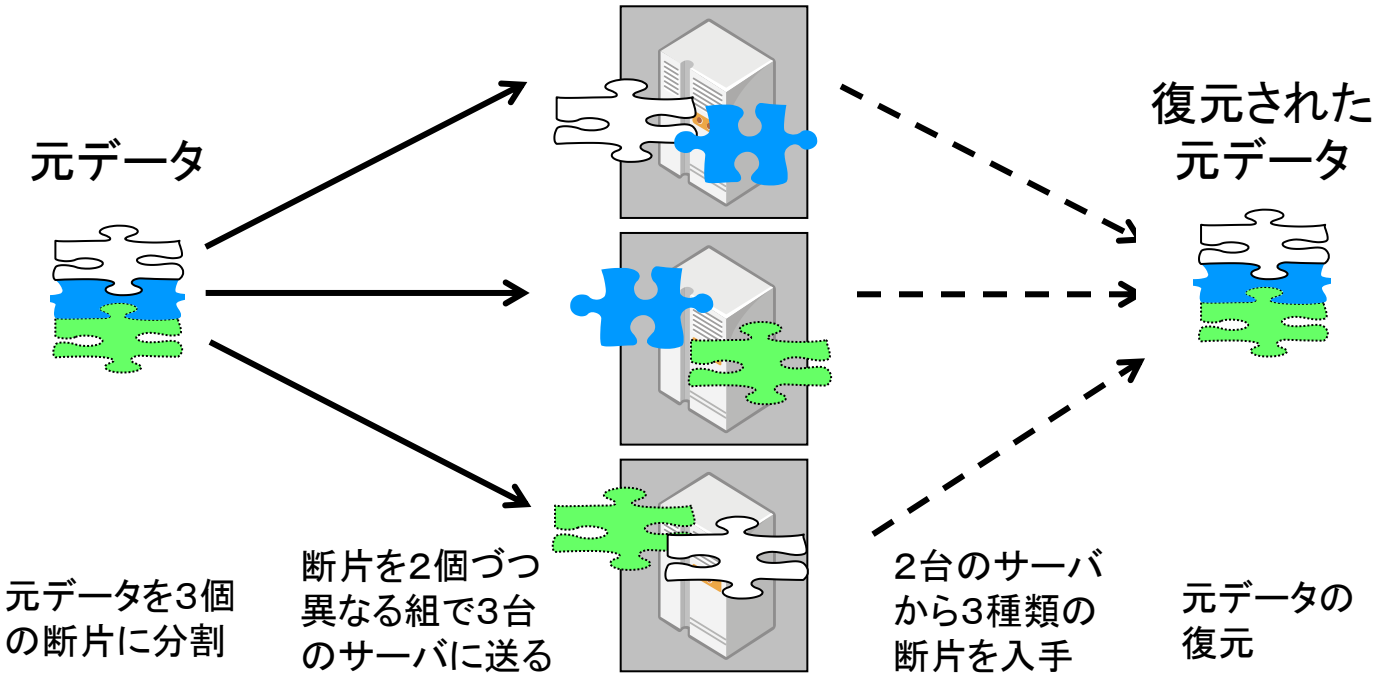
条件（時間や場所や人）で暗号の開示を制御

- インテリジェント暗号（ペアリング暗号・公開鍵系の高機能暗号）
- 図の例
  - 秘匿したいデータに条件を設定：部長または営業課長
  - 閲覧時：条件に合致した場合のみ開示される



複数人の合意で開示の制御

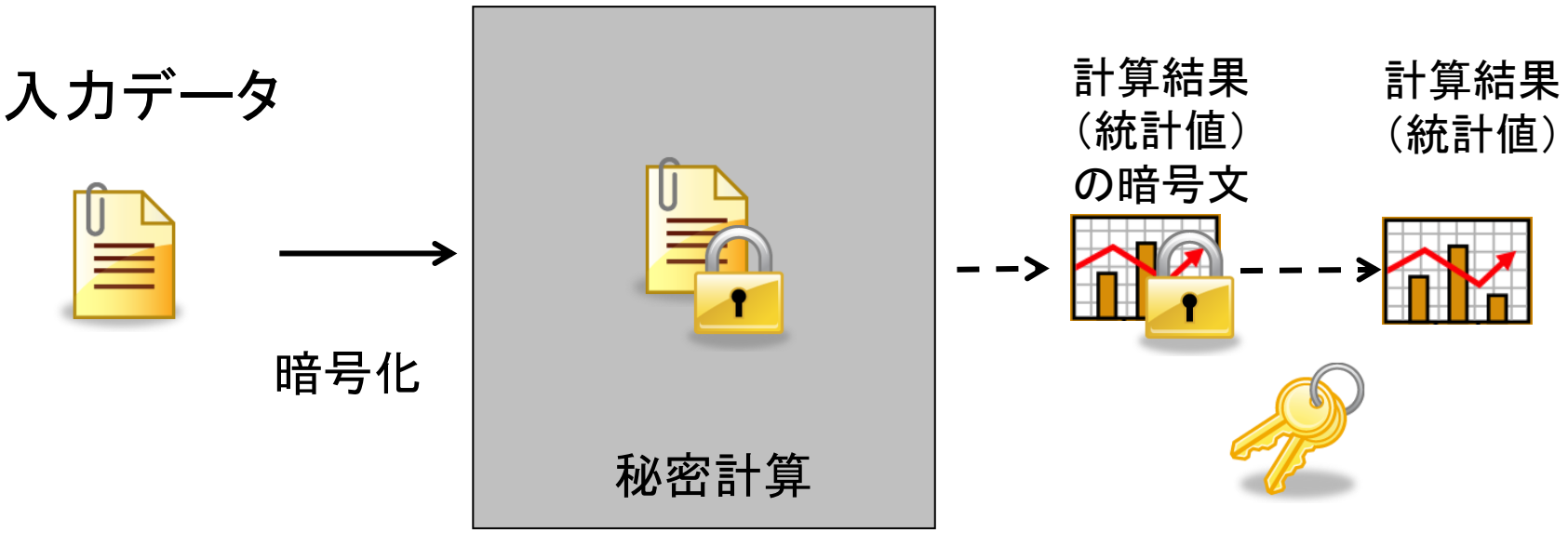
- 秘密分散
  - 図のモデル：3台に分散して2台から復元
- マルチパーティーコンピューティング
  - 管理者を分けると、複数人の合意がなければ情報開示ができない
- 1台のコンピュータからデータを盗んでも何の情報も得られない（秘匿性）
- 1台故障しても、残りのコンピュータからデータを復元できる（可用性）



3台中2台→N台中K台に拡張可能

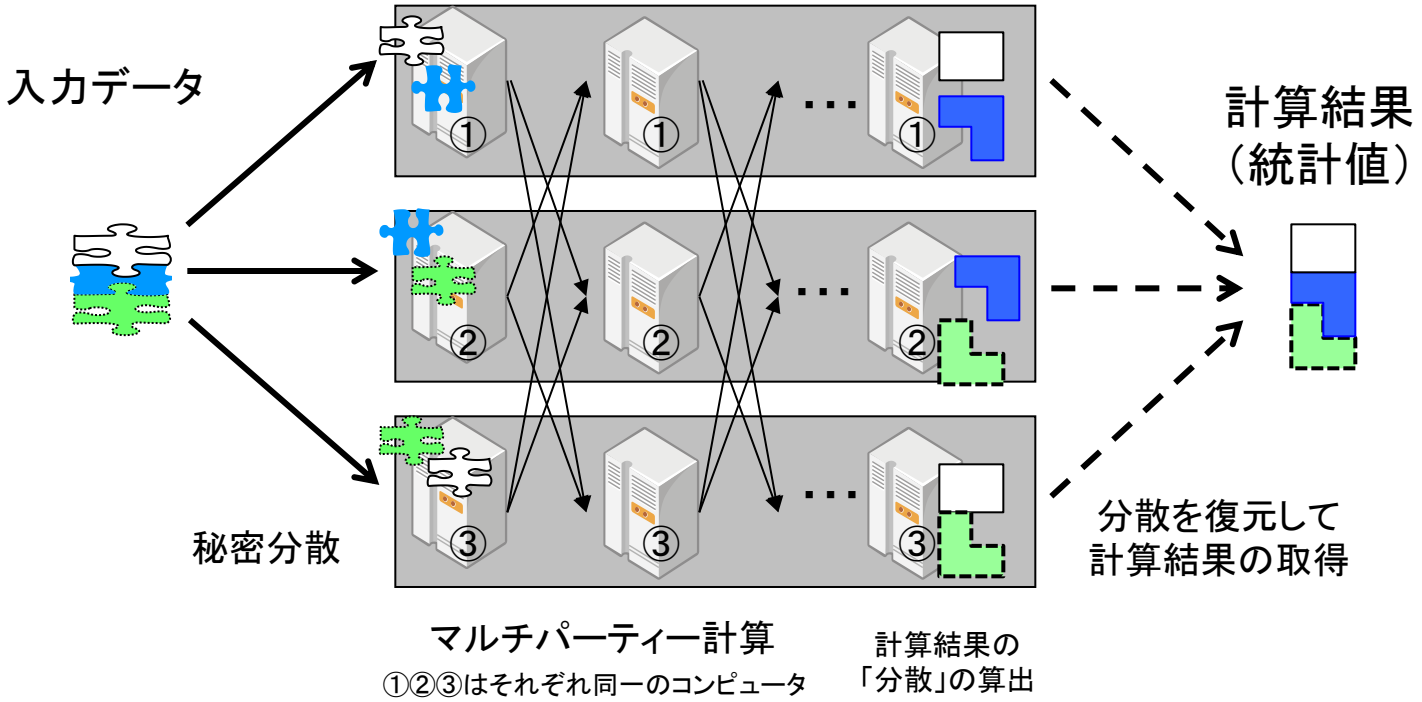
計算結果のみの開示（秘密計算）

- データを暗号化して入力
- 暗号化されたままのデータを計算
- 計算結果の暗号文が出力



計算結果のみ開示（マルチパーティー秘密計算）

- データを秘密分散して入力
- 秘密分散されたままのデータを計算
- 計算結果の秘密分散が出力



情報の個人特定性を低減（k-匿名化）

Innovative R&D by NTT

会員番号	生年月日	住 所	年 齢	購買品
1001	1979.04.01	東京都中央区A町	34	パン、ガム、新聞、…
1002	1986.12.10	神奈川県横浜市A町	26	鉛筆、弁当、漫画、…
1003	1974.10.10	東京都渋谷区B町	38	ガム、アイス、チョコ、…
1004	1991.05.05	神奈川県鎌倉市B町	22	書籍、新聞、電池、宝石、…
1005	2006.11.10	埼玉県川越市A町	6	化粧品、あめ、アイス、…
1006	1990.02.06	神奈川県厚木市C町	23	時刻表、鉄道模型、カメラ、…
1007	2003.08.15	埼玉県浦和市B町	9	ネジ、ビス、ハンマー、…
1008	2000.09.30	埼玉県大宮市C町	12	肉まん、ガム、新聞、…
1009	1983.01.01	東京都練馬区C町	30	コーラ、弁当、雑誌、…
1010	1994.07.07	埼玉県与野市D町	18	ガム、水、ドリンク剤、…

削 除　　保 護　　非保護（そのまま用いる）

会員番号	生年月日	住 所	年 齢	購買品	k-匿名性(k=3)を満たした状態
1001	1979.04.01	東京都	30代	パン、ガム、新聞、…	3
1003	1974.10.10	東京都	30代	ガム、アイス、チョコ、…	
1009	1983.01.01	東京都	30代	コーラ、弁当、雑誌、…	
1002	1986.12.10	神奈川県	20代	鉛筆、弁当、漫画、…	3
1004	1991.05.05	神奈川県	20代	書籍、新聞、電池、宝石、…	
1006	1990.02.06	神奈川県	20代	時刻表、鉄道模型、カメラ、…	
1005	2006.11.10	埼玉県	未成年	化粧品、あめ、アイス、…	4
1007	2003.08.15	埼玉県	未成年	ネジ、ビス、ハンマー、…	
1008	2000.09.30	埼玉県	未成年	肉まん、ガム、新聞、…	
1010	1994.07.07	埼玉県	未成年	ガム、水、ドリンク剤、…	

NTT

情報の個人特定性を低減（Pk-匿名化）

Innovative R&D by NTT

会員番号	生年月日	住所	年齢
1001	1979.04.01	東京都中央区A町	34
1002	1986.12.10	神奈川県横浜市A町	26
1003	1974.10.10	東京都渋谷区B町	38
1004	1991.05.05	神奈川県鎌倉市B町	22
1005	2006.11.10	埼玉県川越市A町	6
1006	1990.02.06	神奈川県厚木市C町	23
1007	2003.08.15	埼玉県さいたま市B町	9
1008	2000.09.30	埼玉県川口市C町	12
1009	1983.01.01	東京都練馬区C町	30
1010	1994.07.07	埼玉県与野市D町	18

削除　　保護（ランダム化）

会員番号	生年月日	住所	年齢
1001	1979.04.01	神奈川県厚木市C町	30
1002	1986.12.10	神奈川県横浜市A町	26
1003	1974.10.10	東京都渋谷区B町	38
1004	1991.05.05	神奈川県鎌倉市B町	24
1005	2006.11.10	埼玉県川越市A町	6
1006	1990.02.06	東京都中央区A町	23
1007	2003.08.15	埼玉県さいたま市B町	9
1008	2000.09.30	埼玉県川口市C町	12
1009	1983.01.01	東京都練馬区C町	34
1010	1994.07.07	埼玉県与野市D町	18

※後処理として、機械学習を用いて、元データに近い状態に戻す推定を行う

NTT