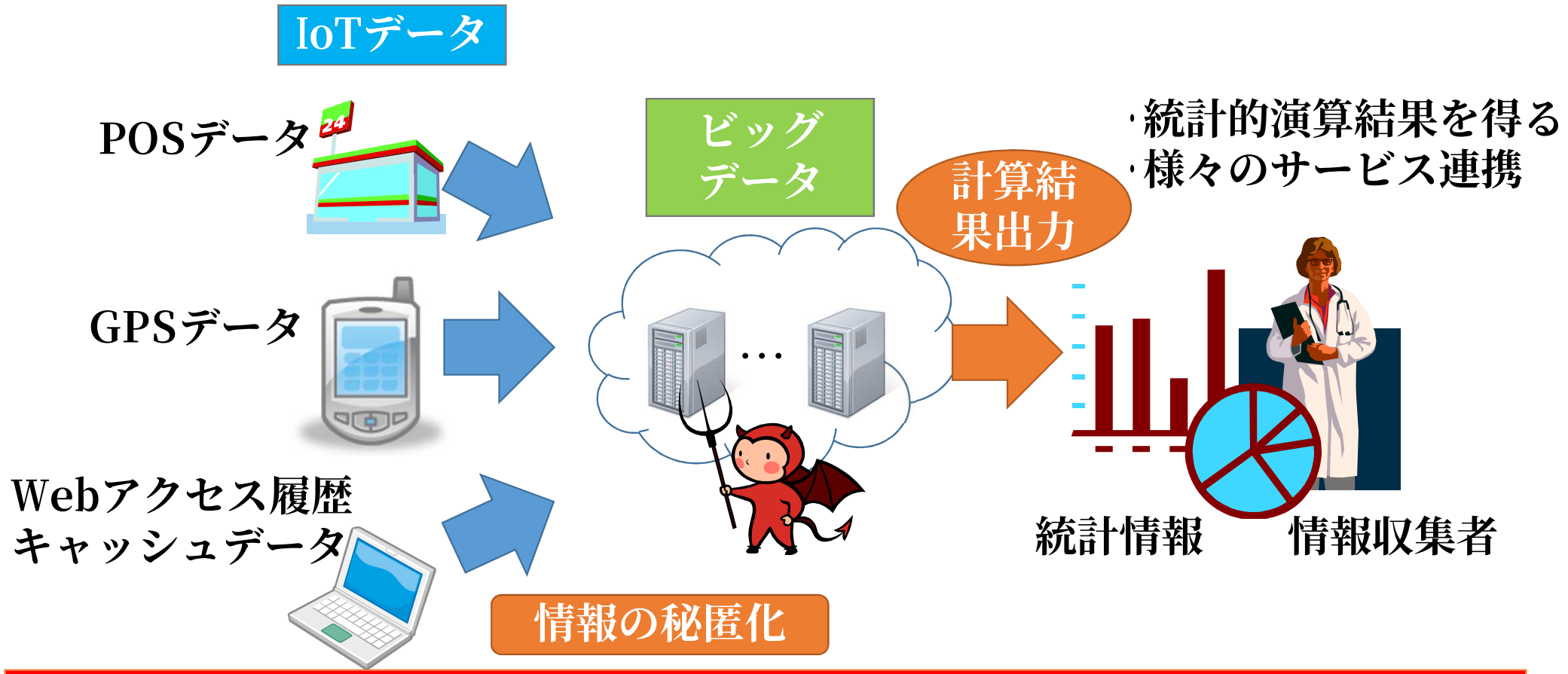
超スマート社会を支える セキュリティープラットフォームの構築

東京理科大学　工学部電気工学科
教授　岩村 恵市

2018年11月13日

今回の技術（特許）の背景



秘密情報を含むビッグデータの有効活用とプライバシー保護の両立

本技術によって実現されること

（１） 計算能力の低いIoTデバイスにも実装可能で、秘匿計算に対応できる秘匿データ生成技術

（２）IoTデバイスから受信したデータ（相手認証含む）を検証するデータ認証技術

（３） 受信した秘匿データをそのまま使って、種々の秘匿計算を行える秘匿計算技術

（４） 受信した秘匿データを復元せずに必要なデータを検索できる秘匿検索技術

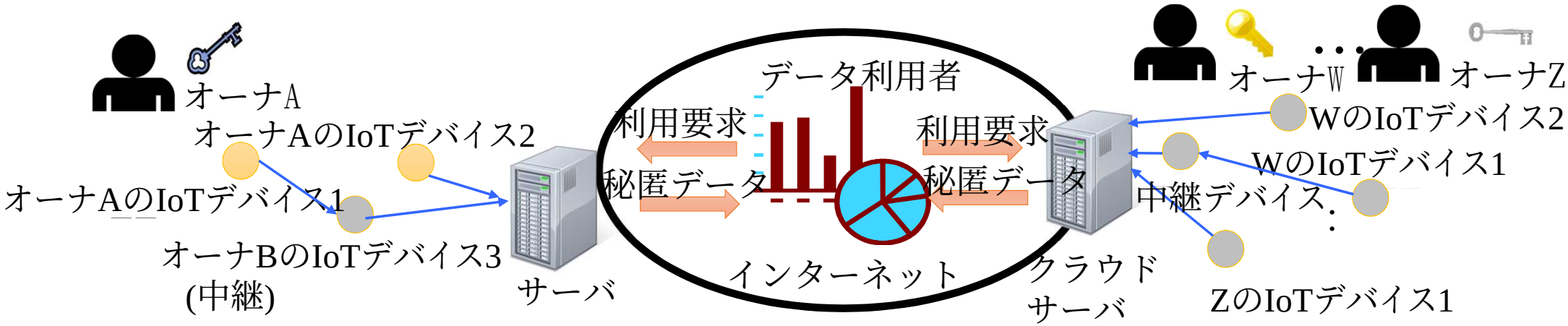
（５） 秘匿計算した結果の正当性を検証できる秘匿計算検証技術

（６） 秘密情報のオーナがその復元や秘匿計算などの利活用を制御できる秘密分散技術

（７） 実数計算にも適用できる秘匿計算技術

（８） 保存された秘匿データを効率的に更新する秘匿データ長期保存技術

今回の特許の概念図



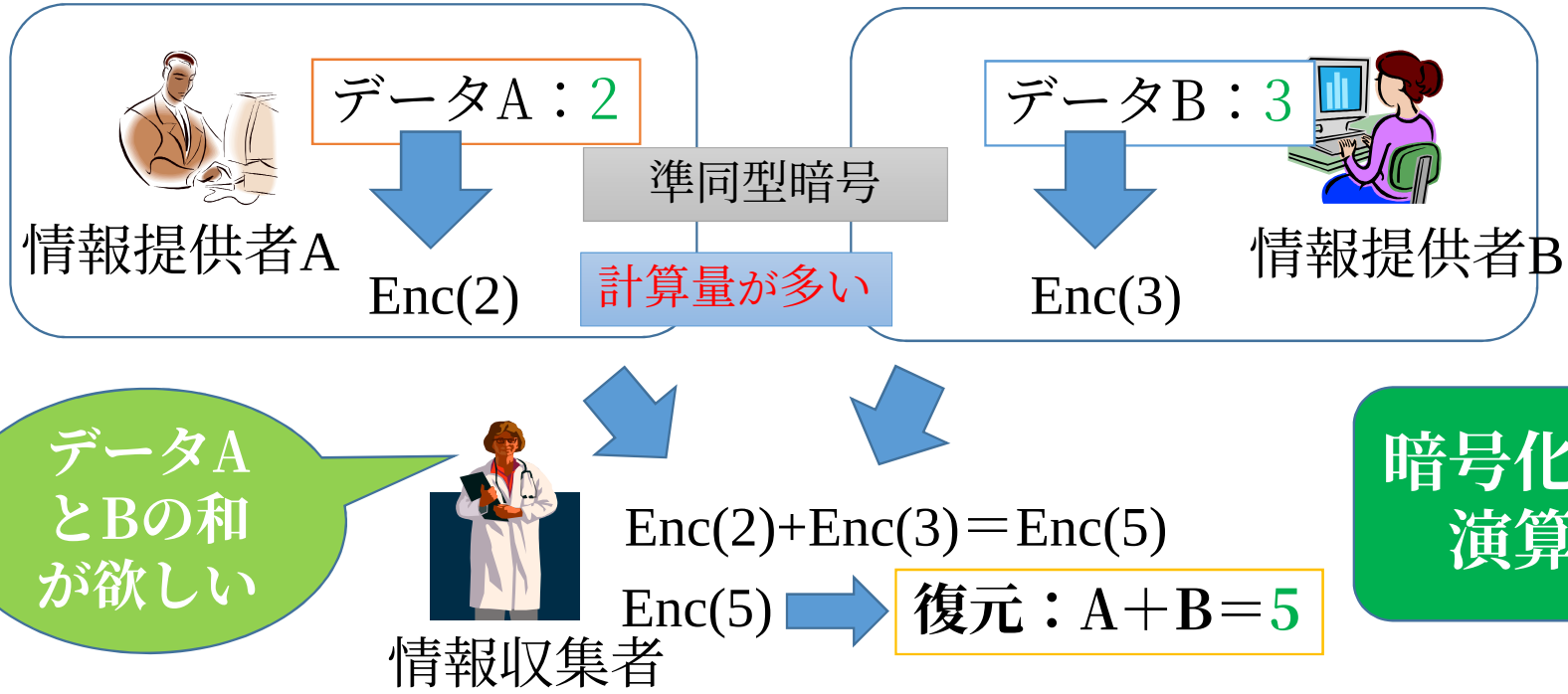
応用例 1

- IoT機器からの測定データを秘匿送受信＋復元せずに秘匿計算
- ユーザにクラウドを提供し、個別情報は秘匿したまま秘匿計算
- 自らの情報を秘匿したまま、連携して他企業を含むデータの利活用
- データは全て秘匿保存し、復元することなくデータ検索

秘匿計算：入力を秘匿しながら計算する技術

データを保護しながら演算する技術として準同型暗号がある

準同型暗号は一般的に計算量が多いことが知られている



岩村研の技術：秘密分散法による軽量安全な情報秘匿と秘匿計算

準同型暗号による秘匿計算例(従来)

- 加算（a+bを計算する場合）
  - a,bを暗号化⇒c1=g^a、c2=g^bを計算　（離散対数問題）
  - a+bの暗号文を計算⇒c1・c2=g^{a+b}

- 乗算（a･bを計算する場合）
  - a,bを暗号化⇒c1=a^e、c2=b^eを計算
  - a･bの暗号文を計算⇒c1･c2=$(a･b)^e$

ポイント１：べき乗剰余演算は計算量が多く、一般に安全性確保のため
gやeは2048ビット以上の大きな値
ポイント２：加算と乗算を同時に実現する準同型暗号は非常に複雑
※秘密分散の1万倍程度の処理時間

秘密分散法とは？

n個のサーバからk個(n≦k)を選択し分散情報を集めて元の秘密情報を復元

S1

秘密情報

n個のサーバに分散

W11

分散情報1

W12

分散情報2

W1n

分散情報n

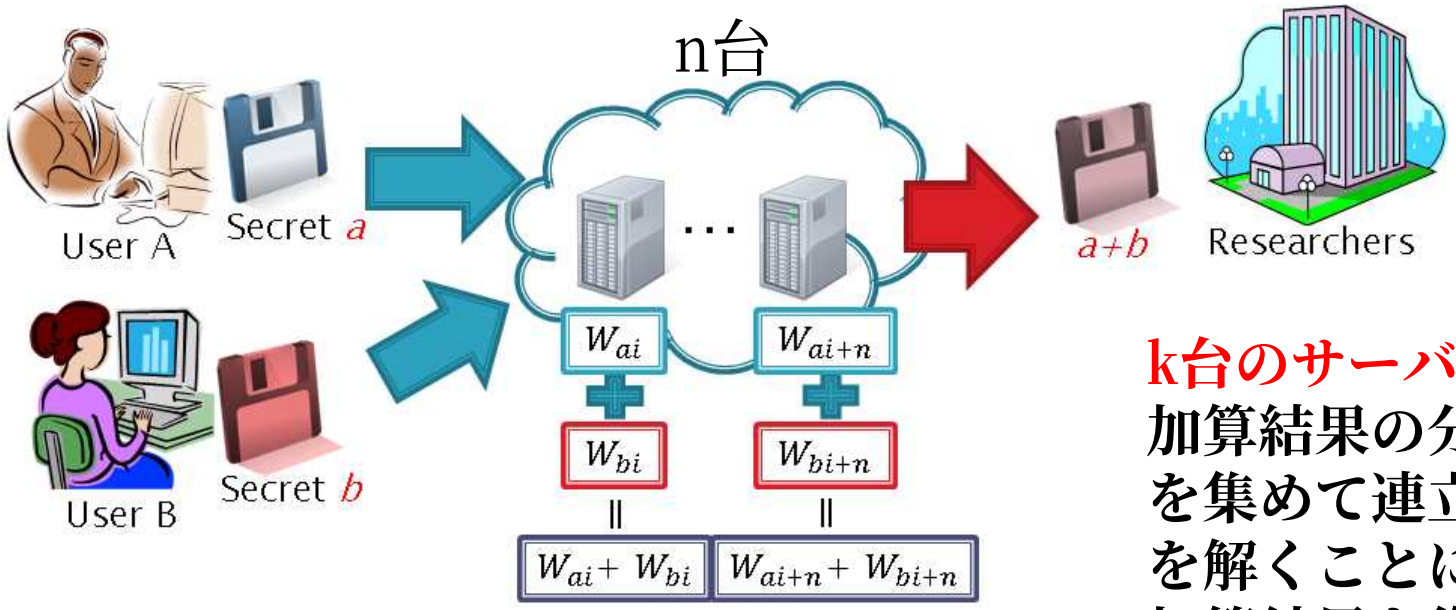
S1

利点

1.k個未満の分散情報からは一切の情報を得ることができない(情報漏洩耐性)
2.n-k個以下の分散情報は予備とできる(欠損耐性)
3.軽量な秘匿演算が可能

秘匿計算（加算）

- 秘匿加算：各分散情報を足し合わせるだけ。



k台のサーバから
加算結果の分散情報
を集めて連立方程式
を解くことにより、
加算結果を復元可能

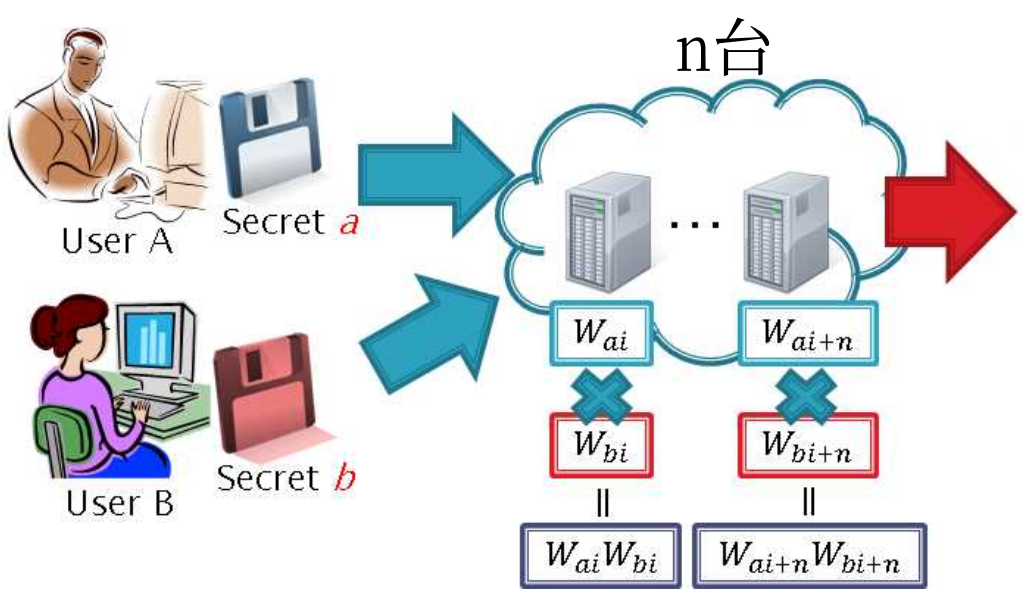
$$W_{a1} = a + a_1 x_1 + a_2 x_1^2 + \cdots + a_{k-1} x_1^{k-1}$$

$$W_{b1} = b + b_1 x_1 + b_2 x_1^2 + \cdots + b_{k-1} x_1^{k-1}$$

$$W_{a1}+W_{b1} = (a+b)+(a_1+b_1)x_1+(a_2+b_2)x_1^2+\cdots+(a_{k-1}+b_{k-1})x_1^{k-1}$$

秘匿計算 (乗算)

- **秘匿乗算：各分散情報を掛け合わせるだけ。**



乗算結果は2k-1個の
分散情報を集めて
連立方程式を解く
ことにより復元可能
⇒kのほぼ倍の2k-1台
以上のサーバ(プレイヤ)
が必要

$$w_{a1} = a + a_1 x_1 + a_2 {x_1}^2 + \cdots + a_{k-1} {x_1}^{k-1}$$

$$w_{b1} = b + b_1 x_1 + b_2 {x_1}^2 + \cdots + b_{k-1} {x_1}^{k-1}$$

$$w_{a1} w_{b1} = ab + (a_1 b + a_2 a) x_1 + (a_2 b + a b_2 + a_1 b_1) {x_1}^2 + \cdots + a_{k-1} b_{k-1} x_1^{2k-2}$$

今回の技術（特許）のポイント

- **暗号技術と秘密分散技術を組合せて下記技術を実現**

（１） 計算能力の低いIoTデバイスにも実装可能な秘匿データ生成
⇒暗号技術（乱数による秘匿）

（２） IoTデバイスからのデータ認証技術
⇒暗号技術を応用した認証（復元値または乱数の一致）

（３） 受信秘匿データをそのまま使っての秘匿計算技術
⇒暗号化データを使った秘匿計算

（４）受信した秘匿データを復元しないデータの秘匿検索技術
⇒秘匿計算を用いた秘匿検索

（５） 秘匿計算結果の秘匿計算検証技術
⇒演算結果に含まれる乱数の演算結果で検証

（６）秘密情報のオーナがその利活用を制御できる
⇒暗号と組合せているので鍵による制御が可能

今後の展開

- **暗号技術と秘密分散技術を組合せて下記技術も実現可能**

（７） 実数計算にも適用できる秘匿計算技術
（８） 保存された秘匿データを効率的に更新する秘匿データ長期保存技術

応用例２

・ニューラルネットへの秘匿計算の適用
・暗号技術の危殆化に対応

実用化への課題と企業への期待

- 高度なプログラミングスキル
  - 理論的には世界最速を実現可能
- アプリケーションに応じた最適化
  - 鍵生成・管理に関する方法等
  - 具体的なパラメータに応じた最適化
  - アプロケーションに応じた新たな手法の研究

本技術に関する知的財産権

(1)発明の名称 ：生成装置、復元装置、送信装置、受信装置、生成プログラム、
復元プログラム、送信プログラム、及び受信プログラム

出願番号 ：特願2018-175393

出願人 ：学校法人東京理科大学

発明者 ：岩村惠市

(2)発明の名称 ：分散装置、秘匿演算装置、検証復元装置、分散システム、
秘匿演算検証復元システム、及びプログラム

出願番号 ：特願2018-185931

出願人 ：学校法人東京理科大学

発明者 ：岩村惠市

お問い合わせ先

東京理科大学
研究戦略・産学連携センター
担当ＵＲＡ：辻本

ＴＥＬ　０３－５２２８－７４４０
ＦＡＸ　０３－５２２８－７４４１
E-mail　ｕｒａ@ａｄｍｉｎ.ｔｕｓ.ａｃ.ｊｐ