セキュリティ基盤技術の研究開発

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
盛合　志帆

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

「サイバーセキュリティ戦略」における暗号技術

平成27年9月4日
閣議決定

- サイバーセキュリティのコア技術の保持
  - 日々高度化・巧妙化するサイバー攻撃等を予測して対応していくためには、攻撃や防御のための技術の原理、システム等の仕組みなどを自ら考え開発するために必要なコア技術の保持が必要
- 暗号研究
  - 新たな産業創出の種
  - 安全保障の観点等から国として維持することが不可欠
  - 公的研究機関や大学等の適切な研究機関において推進

NICT第4期中長期計画 (2016-2020) における目標

【中長期計画】1-4. サイバーセキュリティ分野　(3) 暗号技術

機能性暗号技術

IoTの展開に伴って生じる新たな社会ニーズに対応するため、新しい機能を備えた機能性暗号や軽量暗号・認証技術の研究開発に取り組む

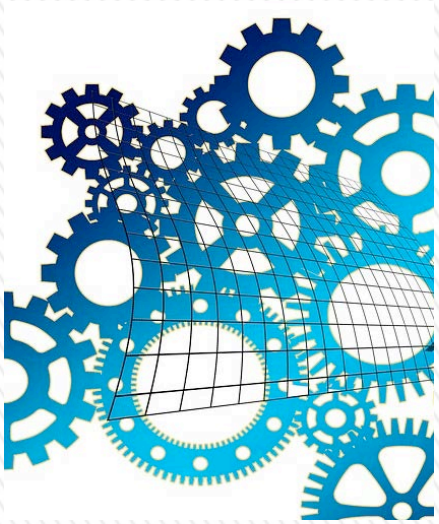
暗号技術の安全性評価

暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化に貢献するとともに、安心・安全なICTシステムの維持・構築に貢献

プライバシー保護技術

パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発を行い、適切なプライバシー対策を技術面から支援

- 暗号技術の安全性評価における日本随一の研究拠点
  - ✓ 中立公平で信頼性の高い安全性評価情報の継続的発信
- セキュリティ＆プライバシー保護技術の研究連携拠点に
  - ✓ S&Pの新たな研究開発テーマでの国内外研究連携拠点を目指す
- 社会で活用される研究開発成果の創出と社会展開
  - ✓ パーソナルデータ利活用や改正個人情報保護法施行に資する技術開発



機能性暗号技術

機能性暗号技術

IoTの展開に伴って生じる新たなニーズに応える機能を備えた暗号。”高機能”だけじゃない。

IoT環境における制約・要件

- 小型化，省電力化
- 早いレスポンス
- 制限された計算能力/メモリ量
- 安全なストレージ

新たな社会ニーズ

- データ保護と利活用との両立
- 長期利用を見越した安全な鍵管理
- 匿名性と不正者検出との両立
- 安全なデータ検索

これらの社会ニーズを解決する機能性暗号技術の創出を目指す

検索可能暗号　グループ署名

軽量暗号/認証　プロキシ暗号　秘匿計算　IDベース暗号

準同型暗号　群構造維持暗号/署名

路車間通信でプライバシー保護を実現する軽量グループ署名

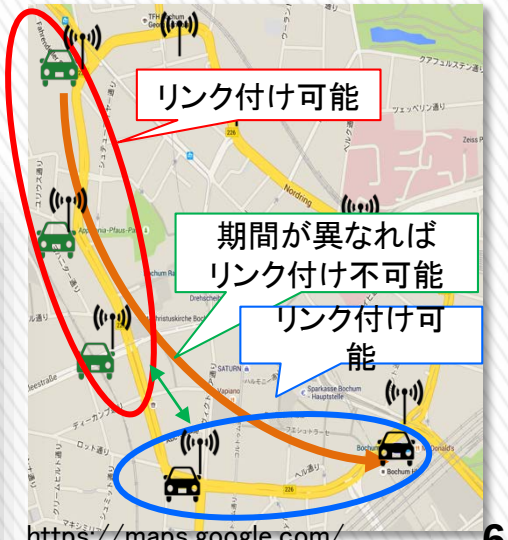
» 車が路側機に位置情報等を送る際に、正当なメッセージであることを示すために署名をつける（IEEE 1609.2等）

→ 情報を送り続けることで、通勤経路などの**プライバシー漏洩の懸念**あり

» 同じ車でも異なる期間に作成された署名がリンク不可能となる**期間に依存した匿名性**をもつ軽量グループ署名を実現

» 廃車や署名鍵漏洩に対応した**鍵失効機能**

» IoTデバイス上で**現実的な署名生成効率**（数百msec）



https://maps.google.com/

Emura, Hayashi, Ishida, “Group Signatures with Time-bound Keys Revisited: A New Model and an Efficient Construction”, appeared in ASIACCS 2017, ACM

暗号化したまま演算ができる

準同型暗号の演算制御

江村, 林, 國廣, 佐久間
「まぜるな危険 準同型暗号」
CSS2016最優秀論文賞受賞

軽量暗号ガイドラインの作成

» IoT時代に軽量暗号の利用促進をはかるため、軽量暗号を選択・利用する際の技術的判断に資するための**軽量暗号ガイドライン**を作成

» 日本語・英語版, CRYPTRECサイトより公開予定

目次

家電, スマートテレビ, 物流管理, 農業, 医療, 産業用システム, 自動車 …

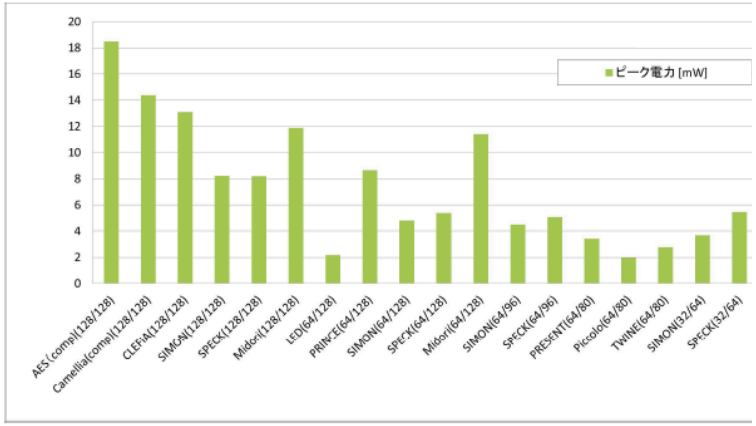


図 3.20　Enc,Serial 実装のピーク電流

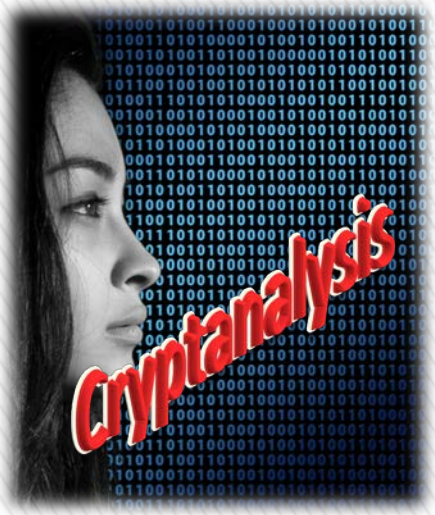
技術分野	ハッシュ関数
名称	Keccak
設計者	Guido Bertoni(STMicroelectronics)、Joan Daemen(STMicroelectronics Peeters(NXP Semiconductors)、Gilles Van Assche(STMicroelectronics
発表年 (発表学会等)	2008 (NIST SHA-3 Competition)
仕様参照先	http://keccak.noekeon.org/
特徴	Keccak はスポンジ構造から成り、内部パラメータにより様々なバリエ を構成できる。置換関数は 7 種類が定義されており、それぞれ Keccak 25、50、100、200、400、800、1600) と表される。ここでは、軽量暗号の Keccak-f[100]、Keccak-f[200]、Keccak-f[400] を利用した方式について掲
安全性解析状況	SHA-3 として標準化された方式に関する解析論文が多数存在するが、現 命的な脆弱性は報告されていない。
標準化状況	Keccak-f[1600] を利用した方式は SHA-3(FIPS 202) に採用されている。
利用実績等	SHA-3 としては多くのアプリケーションで導入されつつある。 http://csrc.nist.gov/groups/STM/cavp/documents/sha3/sha3val.html http://www.3gpp.org/DynaReport/35-series.htm
オープンソース情報	http://keccak.noekeon.org/files.html https://github.com/gvanas/KeccakCodePackage

Keccak-f[b]	n	r	r'
Keccak-f[100]	80	20	20
Keccak-f[200]	64	72	72
Keccak-f[400]	128	144	144

*n:出力長、r:入力ブロック長、r':出力ブロック長

ハードウェア実装 [4](130nm process)

	Area [GE]	Latency [clk]	Throughput [kbps]
Keccak-f[100]	1250	800	2.5
Keccak-f[200]	2520	900	8.00
Keccak-f[400]	5090	1000	14.40



暗号技術の安全性評価

暗号技術の安全性評価

プライバシ保護機能の実現や
ポスト量子コンピューティング
時代に向けて

現在利用されている暗号技術

- 電子政府推奨暗号
- 国際標準暗号
- その他デファクト暗号

RSA, ECC, AES, SHA*, …

安全性評価

安心・安全なICTシステムの維持・構築に貢献

今後の利用が想定される暗号技術

- ペアリング暗号
- 準同型暗号
- 格子暗号
- 多変数多項式公開鍵暗号

安全性評価

新たな暗号技術の信頼性向上・普及・標準化に貢献

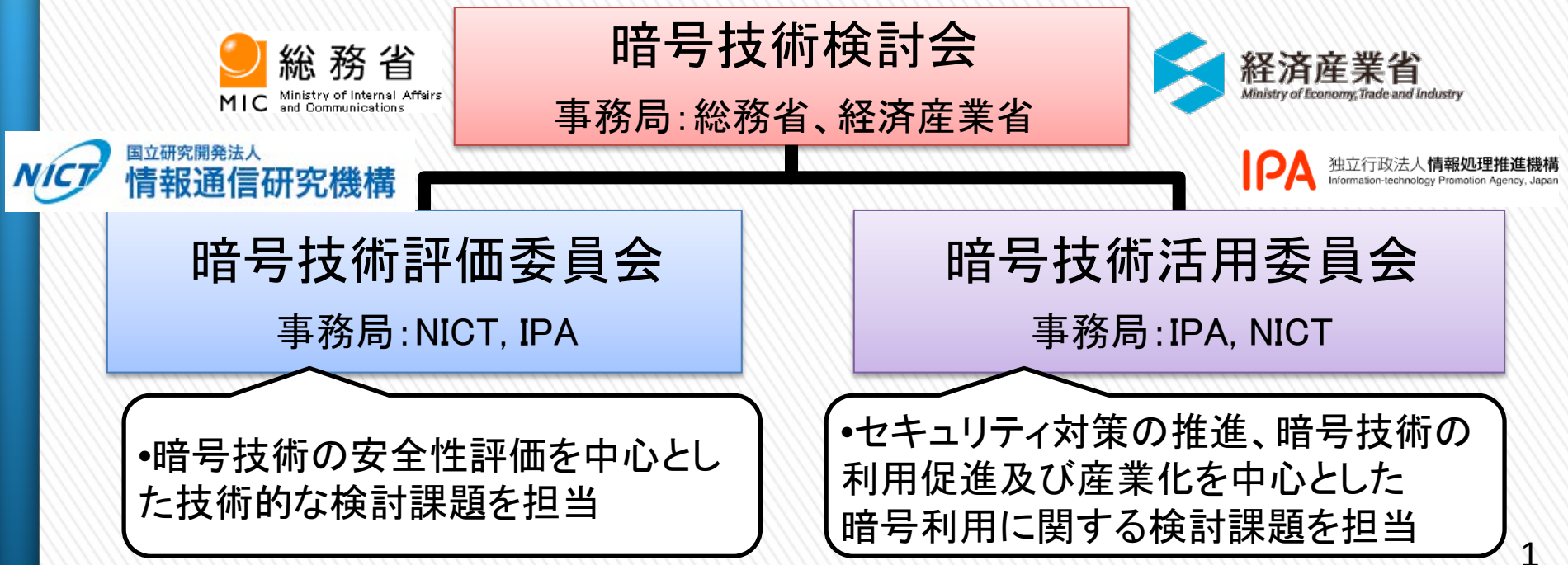
安全性を評価する技術及び理論

数体篩法、関数体篩法、格子理論、代数方程式理論（グレブナー基底）など

CRYPTREC

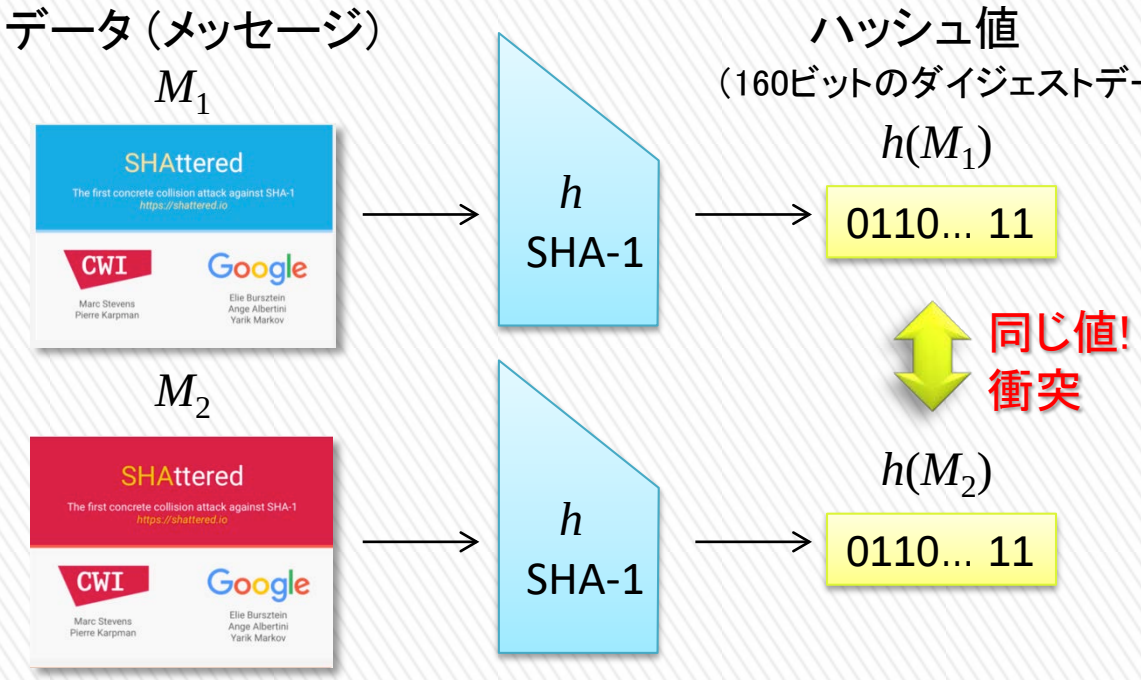
- Cryptography Research and Evaluation Committees

  目的：電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討することを通じてセキュアなIT社会の実現を目指す。



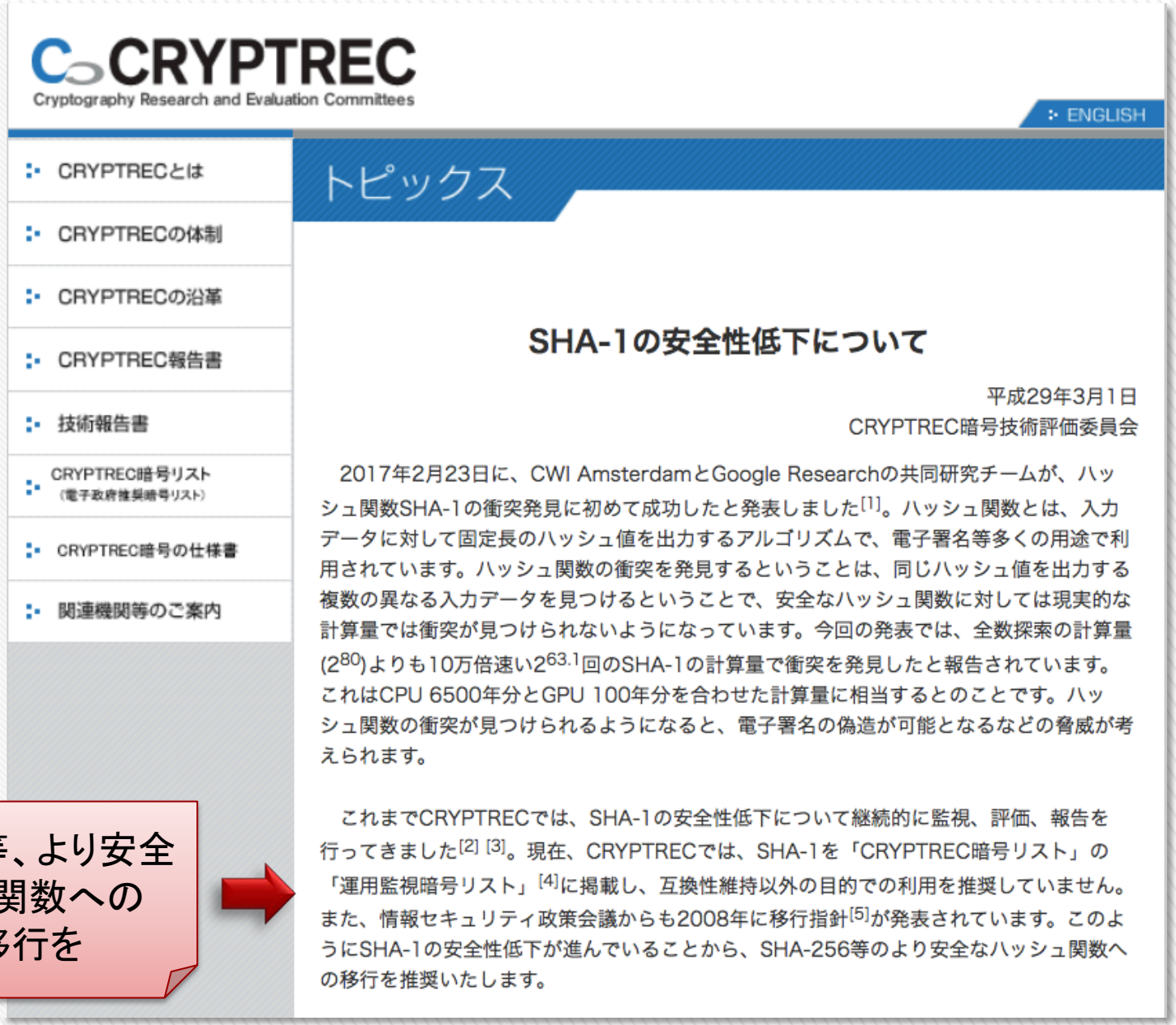
SHA-1の安全性低下

» 2月23日に CWIとGoogle Researchの共同研究チームが，ハッシュ関数SHA−1の衝突発見に初めて成功したと発表⇒電子署名等の偽造が可能に



衝突を見つけるのに
$2^{63.1}$回のSHA−1計算量
= CPU 6500年分と
GPU 100年分を
合わせた計算量

CRYPTRECからの速報



CRYPTREC
Cryptography Research and Evaluation Committees

ENGLISH

- CRYPTRECとは
- CRYPTRECの体制
- CRYPTRECの沿革
- CRYPTREC報告書
- 技術報告書
- CRYPTREC暗号リスト（電子政府推奨暗号リスト）
- CRYPTREC暗号の仕様書
- 関連機関等のご案内

トピックス

SHA-1の安全性低下について

平成29年3月1日
CRYPTREC暗号技術評価委員会

2017年2月23日に、CWI AmsterdamとGoogle Researchの共同研究チームが、ハッシュ関数SHA-1の衝突発見に初めて成功したと発表しました[1]。ハッシュ関数とは、入力データに対して固定長のハッシュ値を出力するアルゴリズムで、電子署名等多くの用途で利用されています。ハッシュ関数の衝突を発見するということは、同じハッシュ値を出力する複数の異なる入力データを見つけるということで、安全なハッシュ関数に対しては現実的な計算量では衝突が見つけられないようになっています。今回の発表では、全数探索の計算量(2^{80})よりも10万倍速い$2^{63.1}$回のSHA-1の計算量で衝突を発見したと報告されています。これはCPU 6500年分とGPU 100年分を合わせた計算量に相当するとのことです。ハッシュ関数の衝突が見つけられるようになると、電子署名の偽造が可能となるなどの脅威が考えられます。

これまでCRYPTRECでは、SHA-1の安全性低下について継続的に監視、評価、報告を行ってきました[2] [3]。現在、CRYPTRECでは、SHA-1を「CRYPTREC暗号リスト」の「運用監視暗号リスト」[4]に掲載し、互換性維持以外の目的での利用を推奨していません。また、情報セキュリティ政策会議からも2008年に移行指針[5]が発表されています。このようにSHA-1の安全性低下が進んでいることから、SHA-256等のより安全なハッシュ関数への移行を推奨いたします。

SHA-256等、より安全なハッシュ関数への速やかな移行を

ポスト量子コンピューティング時代に向けた動き

- NIST, ISO/IEC等で耐量子計算機暗号（PQC, Post-Quantum Cryptography) への移行・標準化プロセスが開始
  - “RSA-2048を解読する量子コンピュータが2030年までに出現”
- NISTによる標準化スケジュール

Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*
2 years later	Draft Standards ready

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

- 耐量子計算機暗号の安全性評価が急務

格子暗号の安全性評価

» TU Darmstadt Lattice Challenge

http://www.latticechallenge.org/

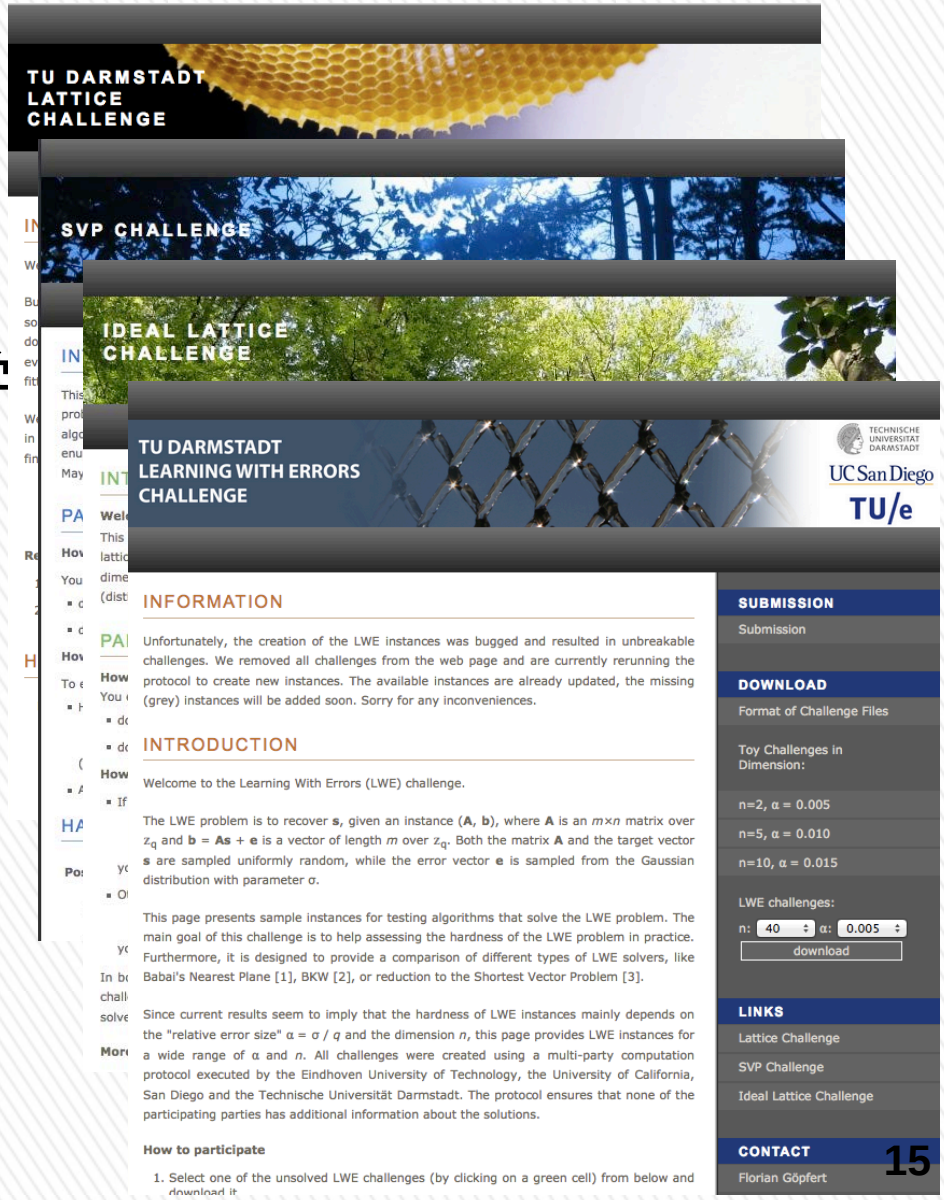
> 独ダルムシュタット工科大学が2008年より主催しているさまざまな格子問題のコンテスト

+ Lattice Challenge

+ SVP Challenge

+ Ideal Lattice Challenge

New + LWE Challenge



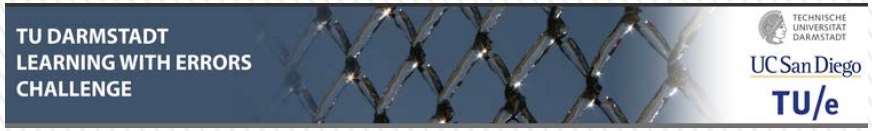
格子暗号の安全性評価: 世界記録の更新

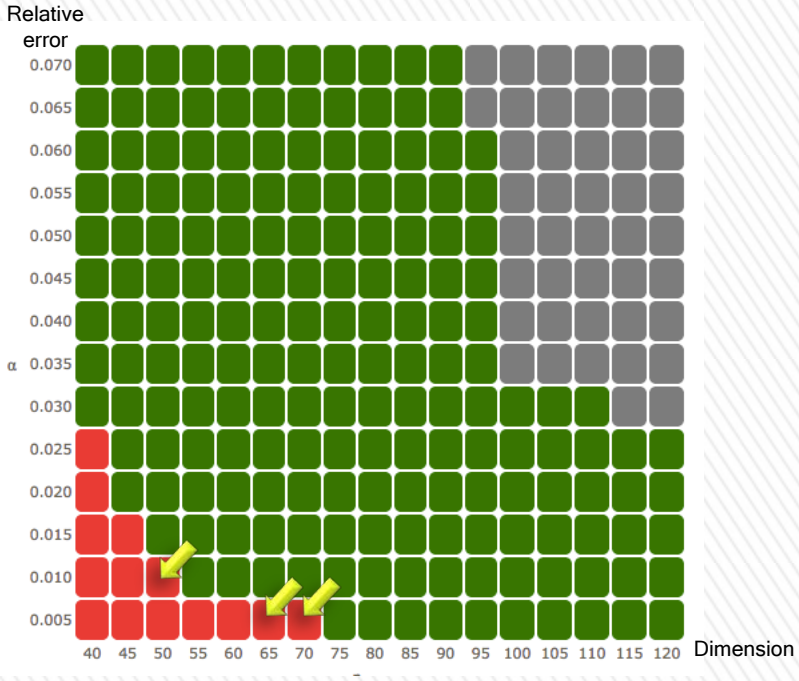
HALL OF FAME

Position	Dimension	Euclidean norm	Contestant	Submission
1	825	117.64	Yoshinori Aono Phong Nguyen	Details
2	800	103.95	Yoshinori Aono Phong Nguyen	Details
3	775	100.14	Yuanmi Chen Phong Nguyen	Details
4	750	87.76	Yuanmi Chen Phong Nguyen	Details
5	725	80.65	Yuanmi Chen Phong Nguyen	Details

APPROX-SVP HALL OF FAME

Position	Dimension	Index	Seed	Euclidean norm	Contestant	Solution
1	652	653	0	626850	Yuntao Wang; Yoshinori Aono; Takuya Hayashi; Jintai Ding; Tsuyoshi Takagi	vec
2	652	653	0	626936	Yuntao Wang; Yoshinori Aono; Takuya Hayashi; Tsuyoshi Takagi	vec
3	652	653	0	661210	Jean-Christophe Deneuville	vec
4	652	653	0	661349	Yuntao Wang, Yoshinori Aono, Takuya Hayashi, Tsuyoshi Takagi	vec
5	600	601	0	542883	Jean-Christophe Deneuville	vec





NICTメンバを含むチームが出した世界記録 (2017.3.5 現在)

プライバシー保護技術

データ統合利活用：新たな成長戦略の鍵

このセンサーデータは信頼できるのか？

データ漏洩対策は大丈夫？

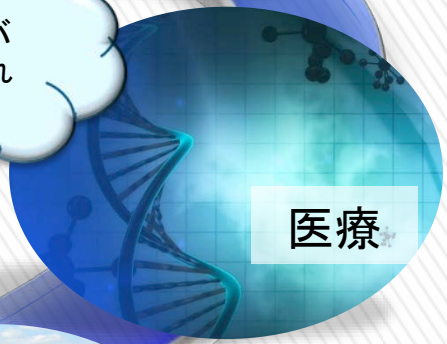
移動履歴

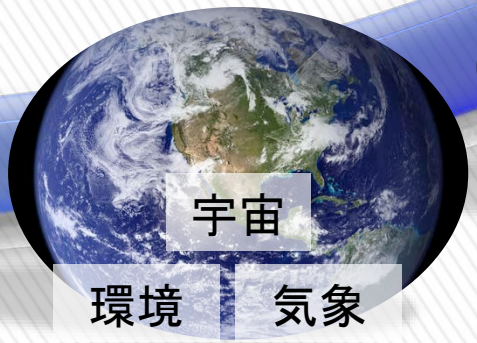
購買履歴

興味・関心

検索キーワード

私のプライバシーは守られている？





セキュリティ・プライバシー対策: データビリティの必須要件

Datability is all about the ability to use large volumes of data **sustainably** and **responsibly**.

[CeBIt 2014, held in Hannover, Germany]

データビリティとは、大規模なデータを持続可能かつ責任ある形で活用する能力のことです。

［CeBIt 2014（ドイツ、ハノーバー）にて提唱］

【sustainable】

- **継続的な対応を可能にするリソース整備**
- **データ・マネジメント＆ガバナンスの確立**
- **セキュリティ対策**

【responsible】

- **社会問題／環境問題の解決（スマートシティ、ヘルスケア、エネルギー活用、経済活動等）**
- **プライバシー／個人情報の問題**

情報通信審議会　情報通信技術分科会　技術戦略委員会（第13回）
資料13-6「データビリティサイエンス」（大阪大学 理事・副学長 八木教授）より

データ統合利活用における プライバシー/個人情報保護

パーソナルデータ利活用には
プライバシー保護が不可欠
cf. 改正個人情報保護法
全面施行（2017.5）

AI 技術による
分析・解析

新たな知見・イノベーション
多様な経済分野でのビジネス創出

改正個人情報保護法のポイント

（一部）

①個人情報の定義の明確化
個人識別符号の概念

【個人情報】

生存する個人に関する情報であって、

1) 氏名、生年月日、住所等により特定の個人を識別することができるもの（他の情報と容易に照合でき、それにより特定の個人を識別することができるものを含む）

例：データベース化されていない書面・写真・音声等に記録されているもの

2) **個人識別符号**（①又は②）が含まれるもの

① 特定の個人の身体の一部の特徴を電子計算機のために変換した符号

例：顔認識データ、認証用指紋データ等

② 対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

例：旅券番号、免許証番号等

②匿名加工情報の新設

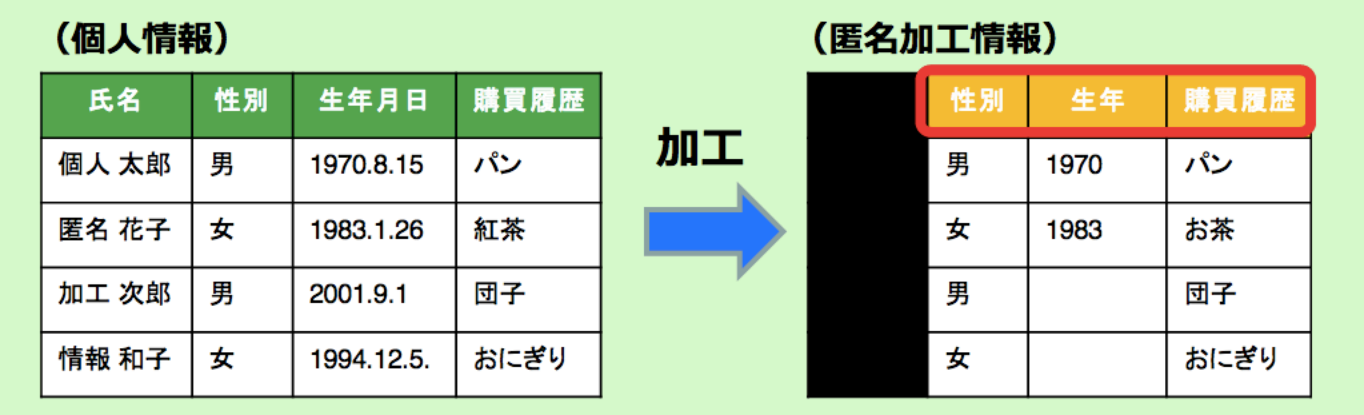
【第三者への提供】分野横断利活用のポイント

- 本人の同意を取れば提供可能
- 委託、事業承継、共同利用に伴って提供する場合には、「第三者」に提供するものとはされない
- **「匿名加工情報」**に加工すれば、本人の同意をとらなくても自由に利活用可能
  → 新事業や新サービスの創出、国民生活の利便性の向上を期待

匿名加工情報

» 個人の特定性を低減したデータ
  > 「個人情報を加工して、通常人の判断をもって、個人を特定することができず、かつ、加工する前の個人情報へと戻すことができない状態にした情報」

» 加工方法
  > 特定の個人を識別する項目の削除や、情報を”丸める”など
  > 「匿名加工情報作成マニュアル」(経済産業省, 2016.8)
  > 「匿名加工情報「パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」」(個人情報保護委員会, 2017.2)



「匿名加工情報制度について」(個人情報保護委員会事務局 参事官 小川久仁子) 資料より

匿名加工情報:
社会実装に向けた研究開発課題

» 匿名加工技術の評価技術　有用性指標と安全性指標
  > いかに再識別のリスクを低減し、データの有用性を保ったまま加工するか
  > NICTでも第4期中長期計画にて取り組み

» PWS CUP　匿名加工・再識別コンテスト
  > 2015年から情報処理学会 コンピュータセキュリティシンポジウムにて開催
  > PWS組織委員会委員長：菊池浩明(明治大)
  > 後援：個人情報保護委員会
  > PWS CUP 2016
    + 匿名加工部門：顧客情報データと購買履歴データを有用性を残して安全に匿名加工する
    + 再識別部門：元の顧客データをヒントにして、匿名加工された購買履歴から顧客を識別する

http://www.iwsec.org/pws/2016/pwscup.html

データ統合利活用における データセキュリティ

暗号・認証技術により
データ機密性・データ信頼性を
確保することで
分野横断でのデータ利活用を促進

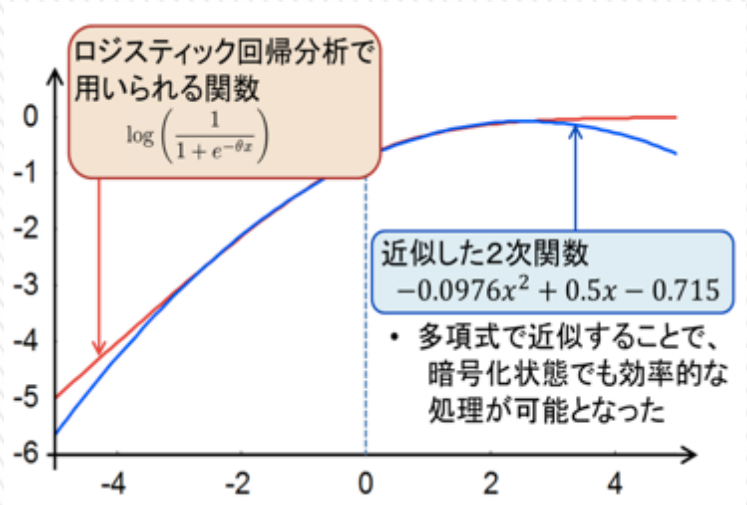
AI 技術による
分析・解析

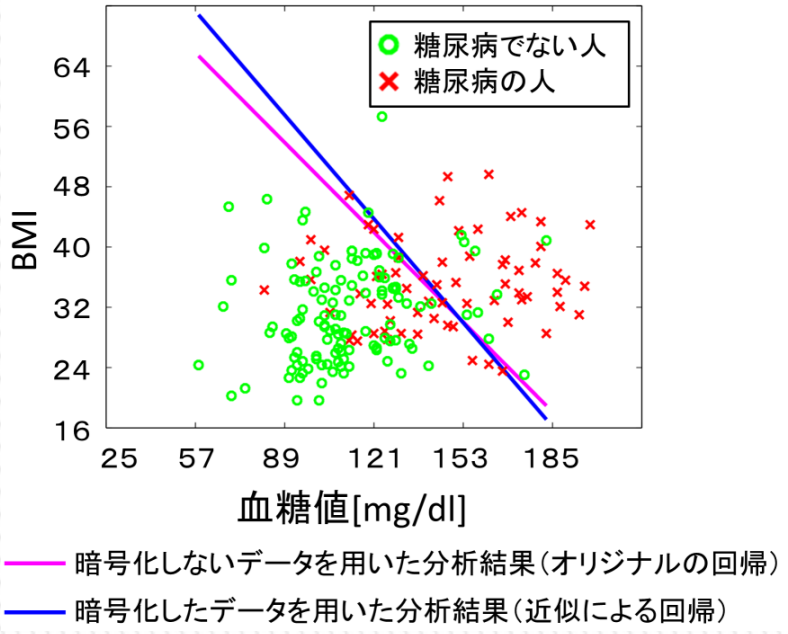
暗号化したまま
分析・解析!?

新たな知見・イノベーション
多様な経済分野でのビジネス創出

暗号化したままビッグデータ分類

- ビッグデータ解析で多用されているロジスティック回帰分析をデータを暗号化したまま計算可能に
- 暗号化された1億件のデータを30分以内で複数グループに分類できることをシミュレーションで確認
  - NICTプレスリリース「**暗号化したままデータを分類できるビッグデータ向け解析技術を開発**」(2016.1.14)



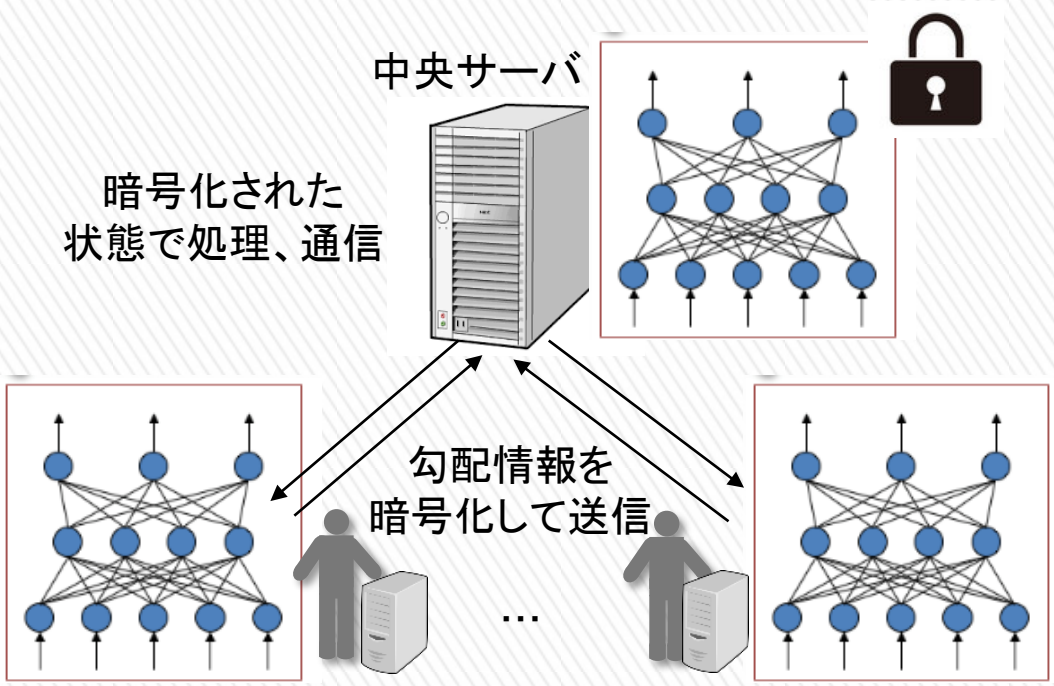


暗号化したまま深層学習*

* 深層学習(deep learning)
多層構造のニューラルネットワークを用いた機械学習

» 多数の参加者が持つデータセットを互いに秘匿したまま深層学習を行うプライバシー保護深層学習システムを提案

下記の機械学習用データベースで性能確認
- MNIST(手書き数字認識)
- SVHN (Googleストリートビュー写真から連続した数字を認識)
- Speechデータセット



N人の参加者と中央サーバ1台による深層学習
(分散協調学習)

「イノベーション創発に資する人工知能基盤技術の創出と統合化」
研究総括: 栄藤 稔(NTTドコモ), 文科省 AIPプロジェクトの一環として運営

JST CREST「人工知能」採択課題

» 「複数組織データ利活用を促進するプライバシー保護データマイニング」

> 研究代表者:盛合 志帆(NICT). 神戸大 小澤誠一, (株)エルテスと連携

課題

複数の異なる業種・組織が有する実社会の
膨大なデータを統合して利活用する際、
プライバシー保護・データ機密性の確保が課題

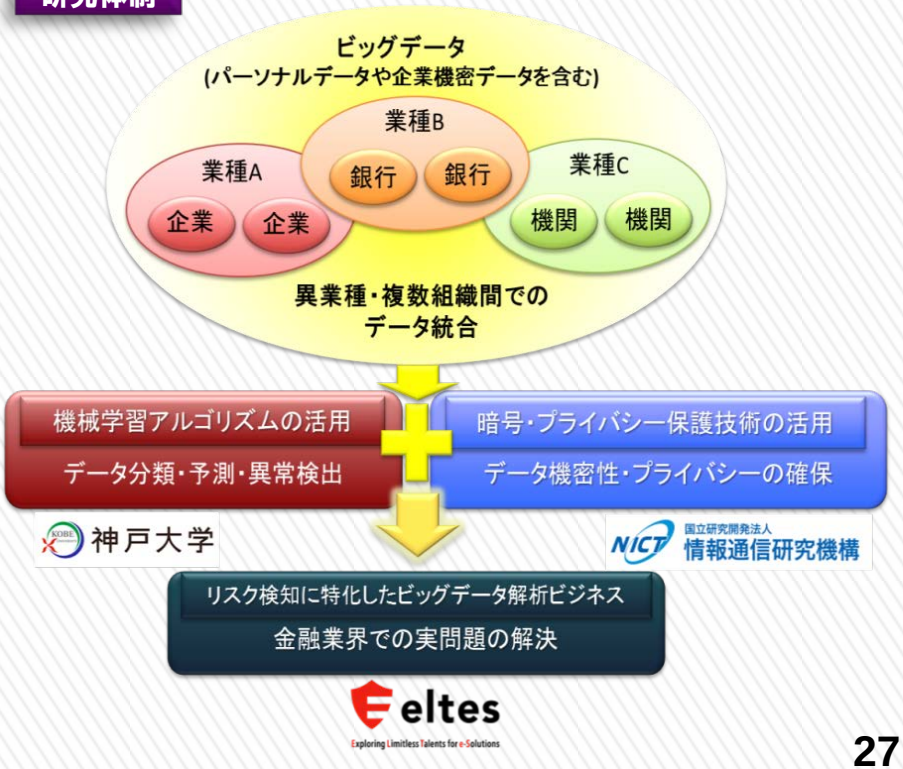
研究課題

暗号技術や人工知能技術を活用し、
プライバシーを保護した状態で
高速にデータ分析や異常検知を行う技術を
研究開発

解決する社会問題

金融分野における社会問題の解決に活用.
金融機関以外がもつデータを利活用した
①インターネットバンキング不正送金の検知
②個人向け融資における 適正利率の導出
⇒ フィンテックにおけるイノベーション創出をめざす.

研究体制



まとめ

» NICT第4期中長期計画（サイバーセキュリティ分野）で推進中のセキュリティ基盤技術の研究開発の紹介
  > IoTの展開に伴って生じる新たな社会ニーズに対応するための機能を備えた機能性暗号技術
  > 新たな暗号技術の普及・標準化および、安心・安全なICTシステムの維持・構築に貢献するための暗号技術の安全性評価
  > パーソナルデータの利活用に貢献するためのプライバシー保護技術