プライバシー保護データマイニングシンポジウム
フィンテックにおけるイノベーション創出を目指して
（2018年10月31日（水））

金融分野におけるセキュリティ：高機能暗号や機械学習*

日本銀行金融研究所
情報技術研究センター
宇根正志

＊本講演の内容は、発表者個人に属し、日本銀行の公式見解を示すものではありません。

日本銀行金融研究所情報技術研究センター（CITECS）

- 金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポート（2005年4月設立）。
  - 主な役割は、①国際標準化の推進、②金融業界内の情報共有体制の整備、③新しい情報セキュリティ技術の研究開発。

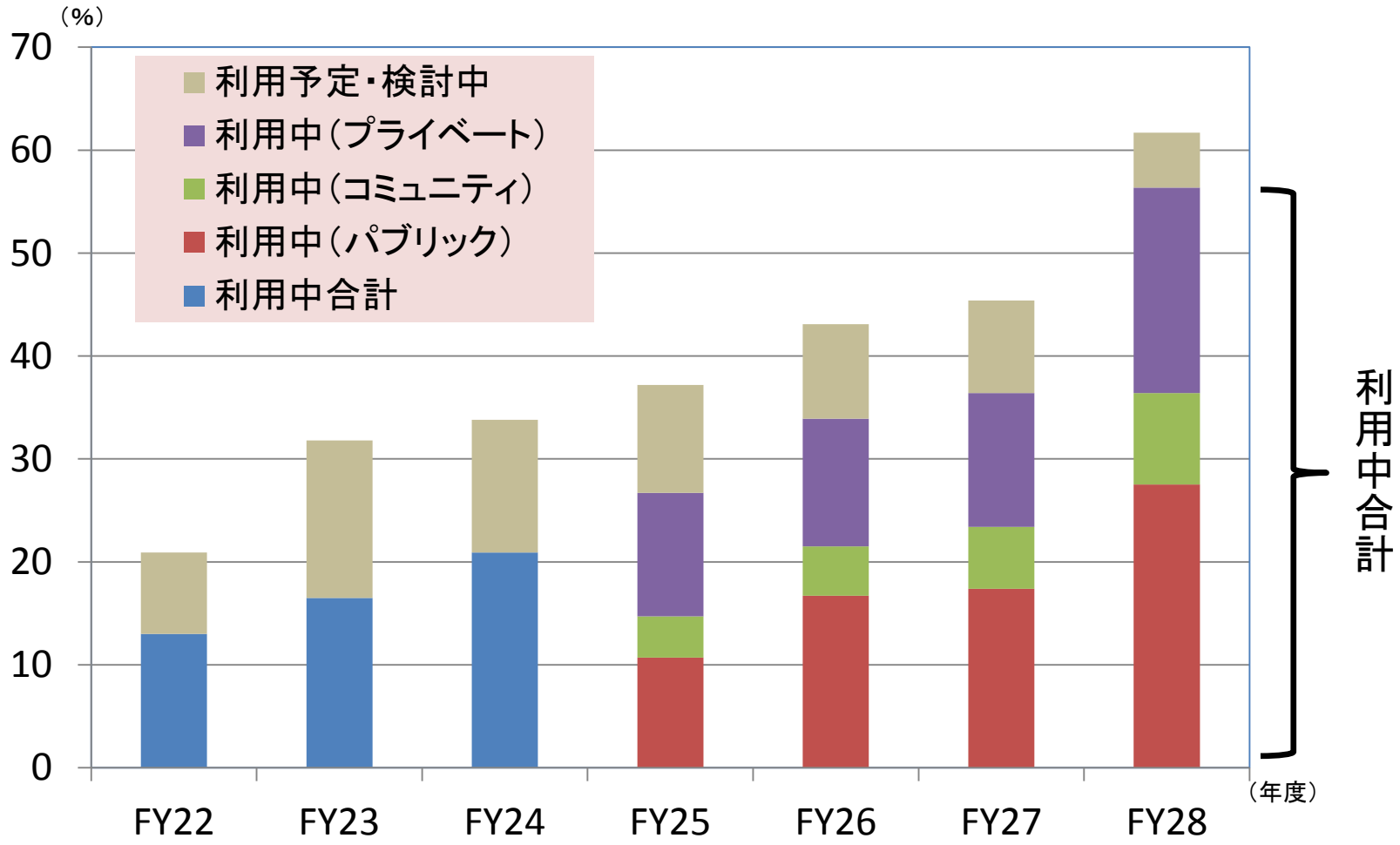
- 最近の主な研究テーマ
  - 量子コンピュータの影響と暗号移行のあり方
  - 金融機関のオープンAPI
  - **機械学習システム**
  - 電子マネー・暗号通貨
  - 金融分野におけるIoT
  - **高機能暗号の活用**
  - ・・・

第19回情報セキュリティ・シンポジウム
（2018年3月1日）

出典：日本銀行金融研究所、「金研ニュースレター」、2018年3月。（写真：野瀬勝一氏）

クラウド活用の広がり

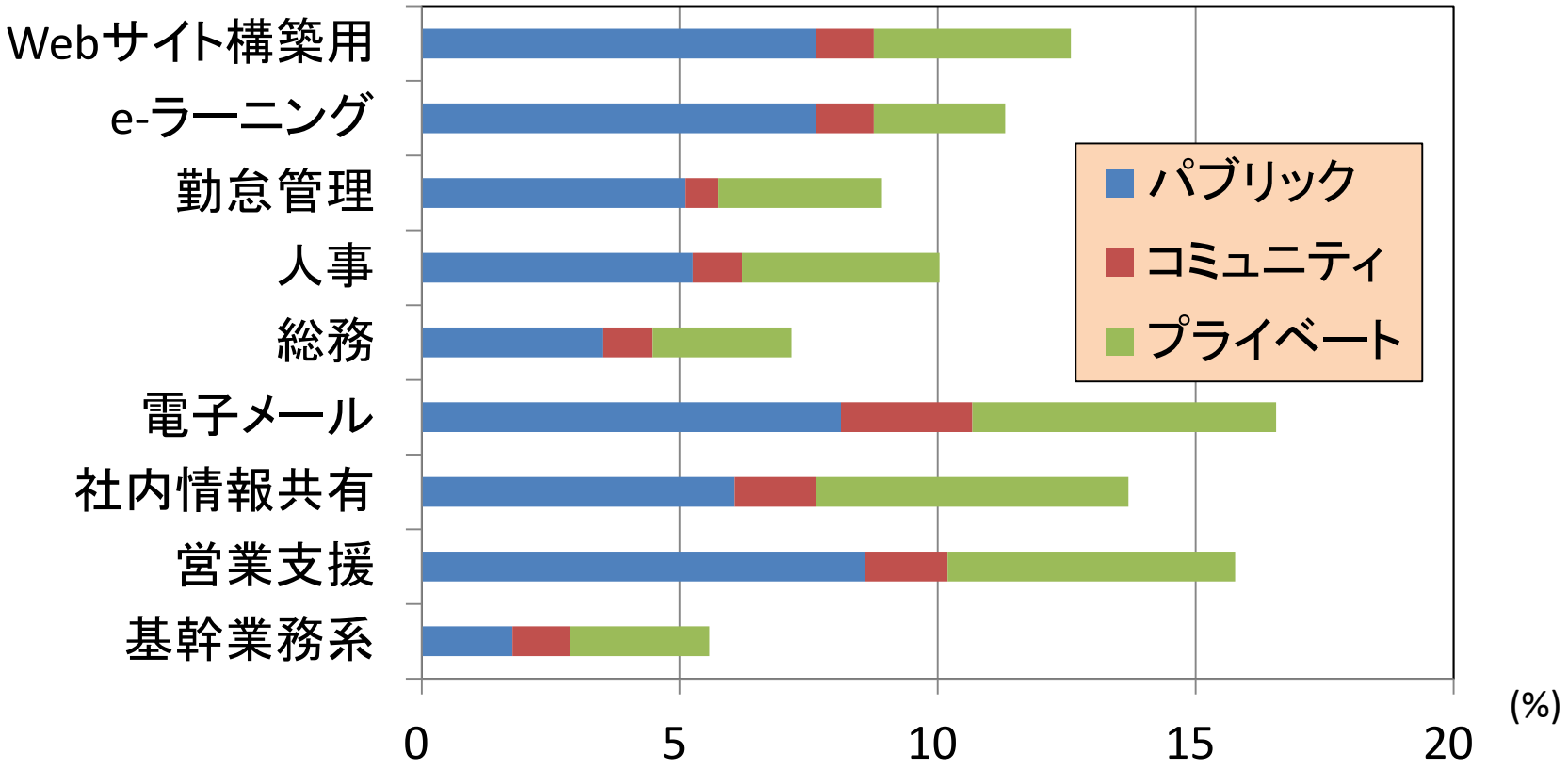
・クラウドを活用する金融機関の割合は増加傾向。



（出典）金融情報システムセンター、『金融機関におけるFinTechに関する有識者検討会報告書』、2017年6月.

クラウド活用の用途

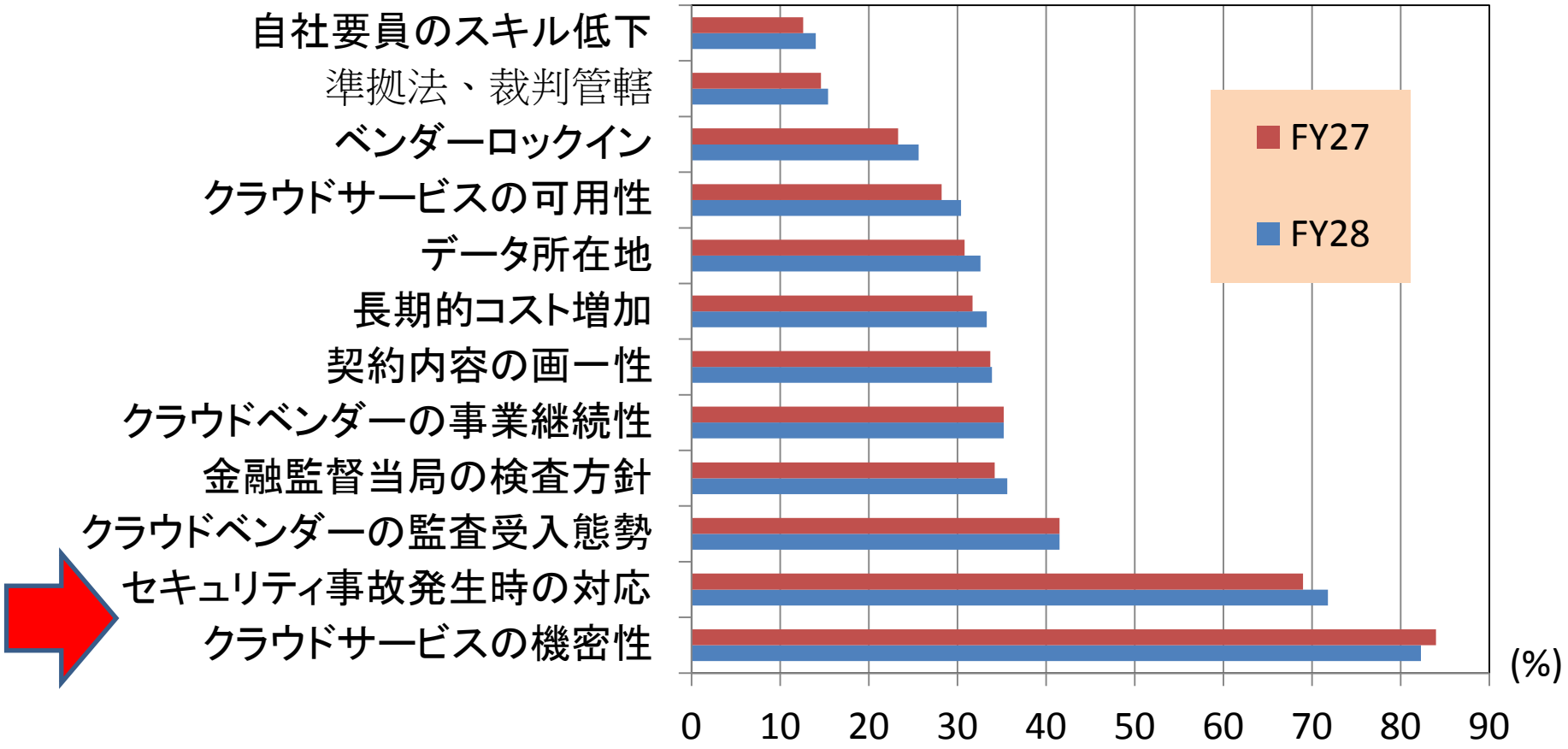
- 各業務に「クラウドを活用している」と回答した先の割合（H28年度）



出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表5-3、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞

クラウドサービス利用に対する懸念・不安

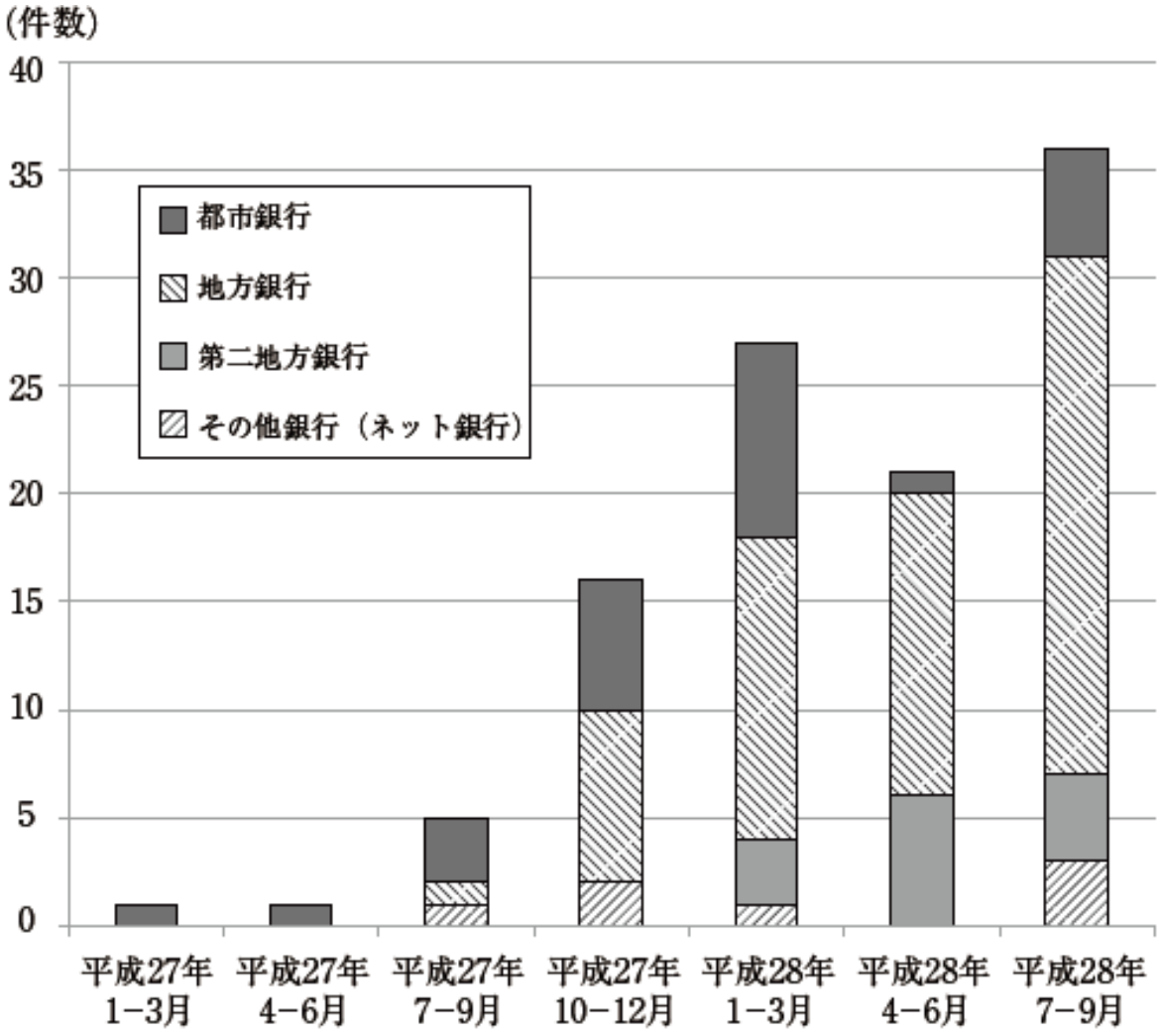
- 「クラウドサービスの機密性」や「セキュリティ事故発生時の対応」等を懸念。



出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表5-4、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞

FinTechにかかる取組み

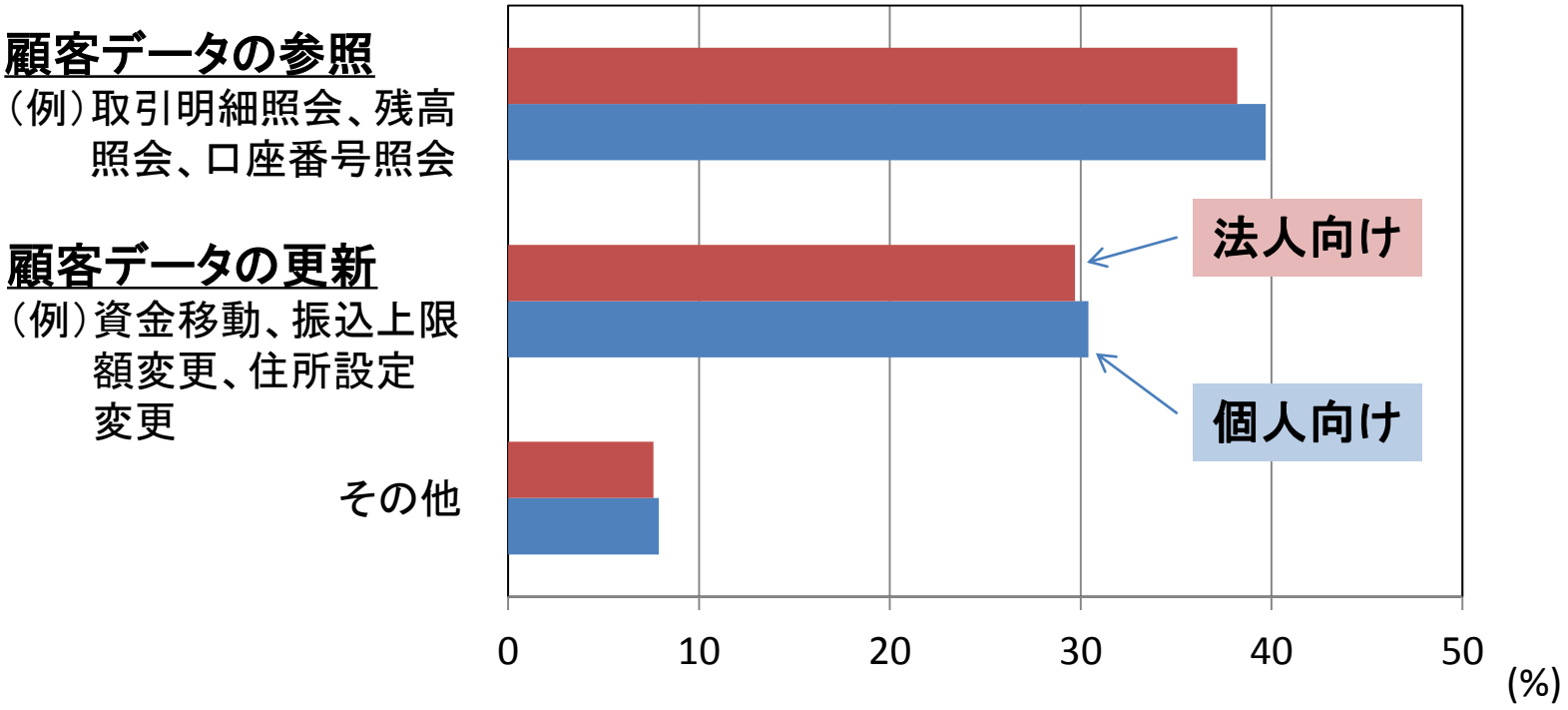
- 国内金融機関のFinTechに関連するプレスリリース件数（※）



（出典）金融情報システムセンター、『金融機関におけるFinTechに関する有識者検討会報告書』、2017年6月.

オープンAPIの取組み

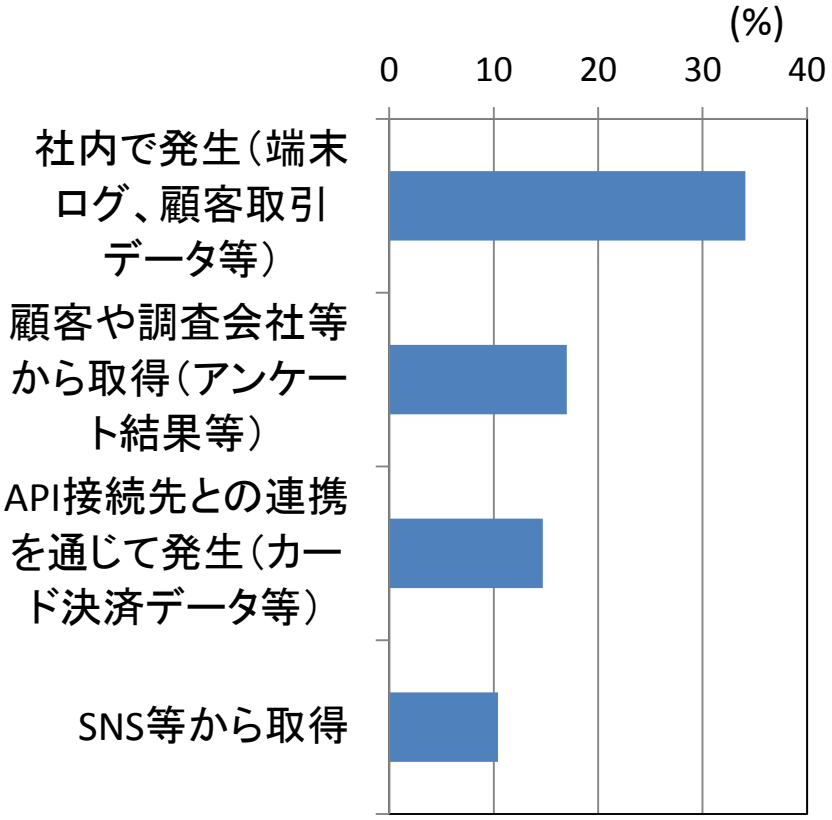
- 個人向け、および、法人向けのオープンAPIに関して、「既に取り組んでいる」「導入準備」または「検討中」と回答した先の割合（H28年度）

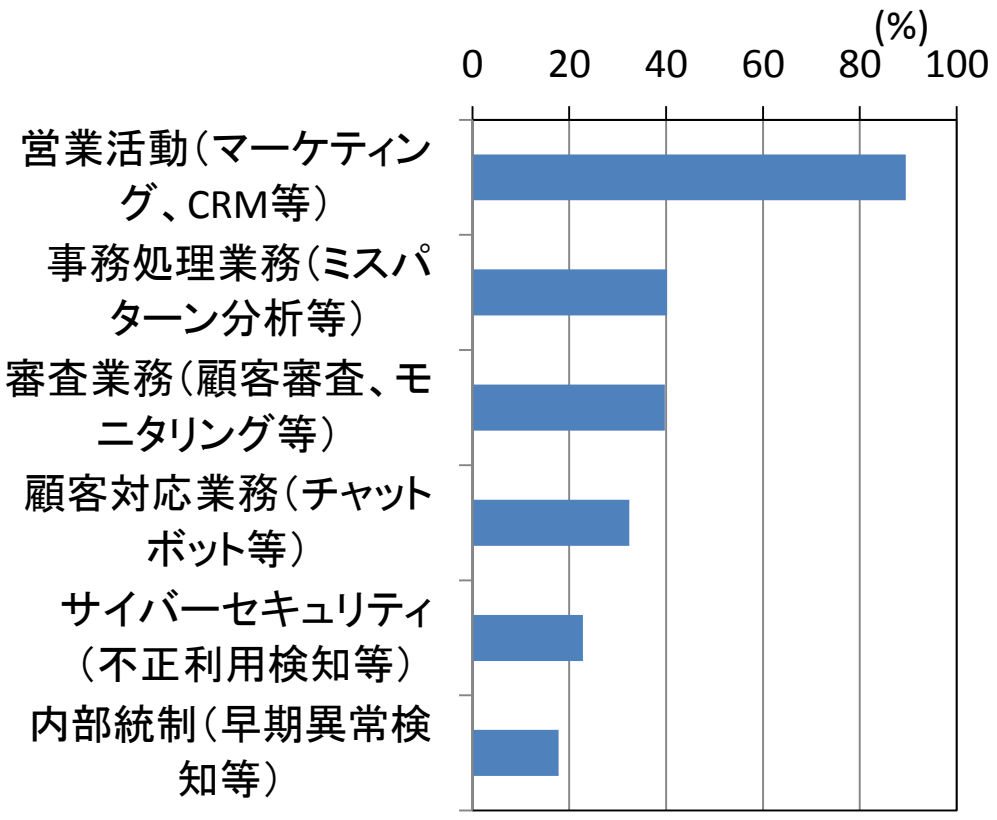


出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表1-5, 1-6、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞

ビッグデータの活用

【**データ種別**ごとの金融機関の割合】【**目的**ごとの金融機関の割合】



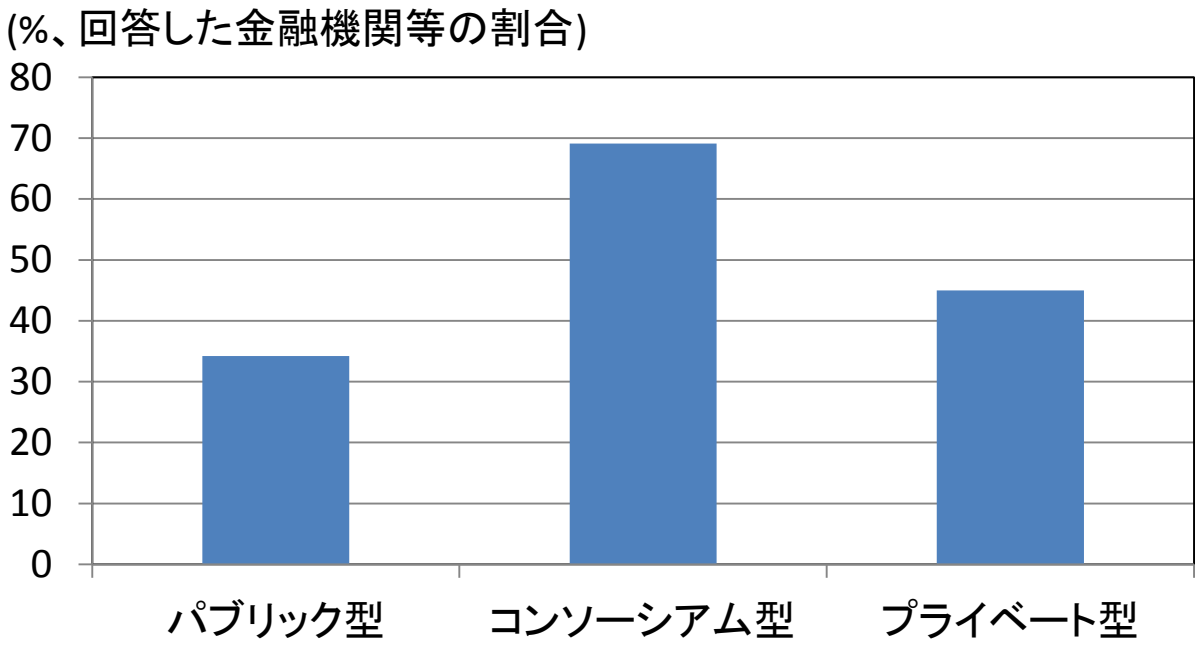


出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表1-3, 1-4、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞
備考：「ビッグデータ」は、「社内外の大量の業務データのうち、社内外で取得されていたが、自機関ではこれまで活用できていなかったデータ」と定義。

ブロックチェーンや分散台帳

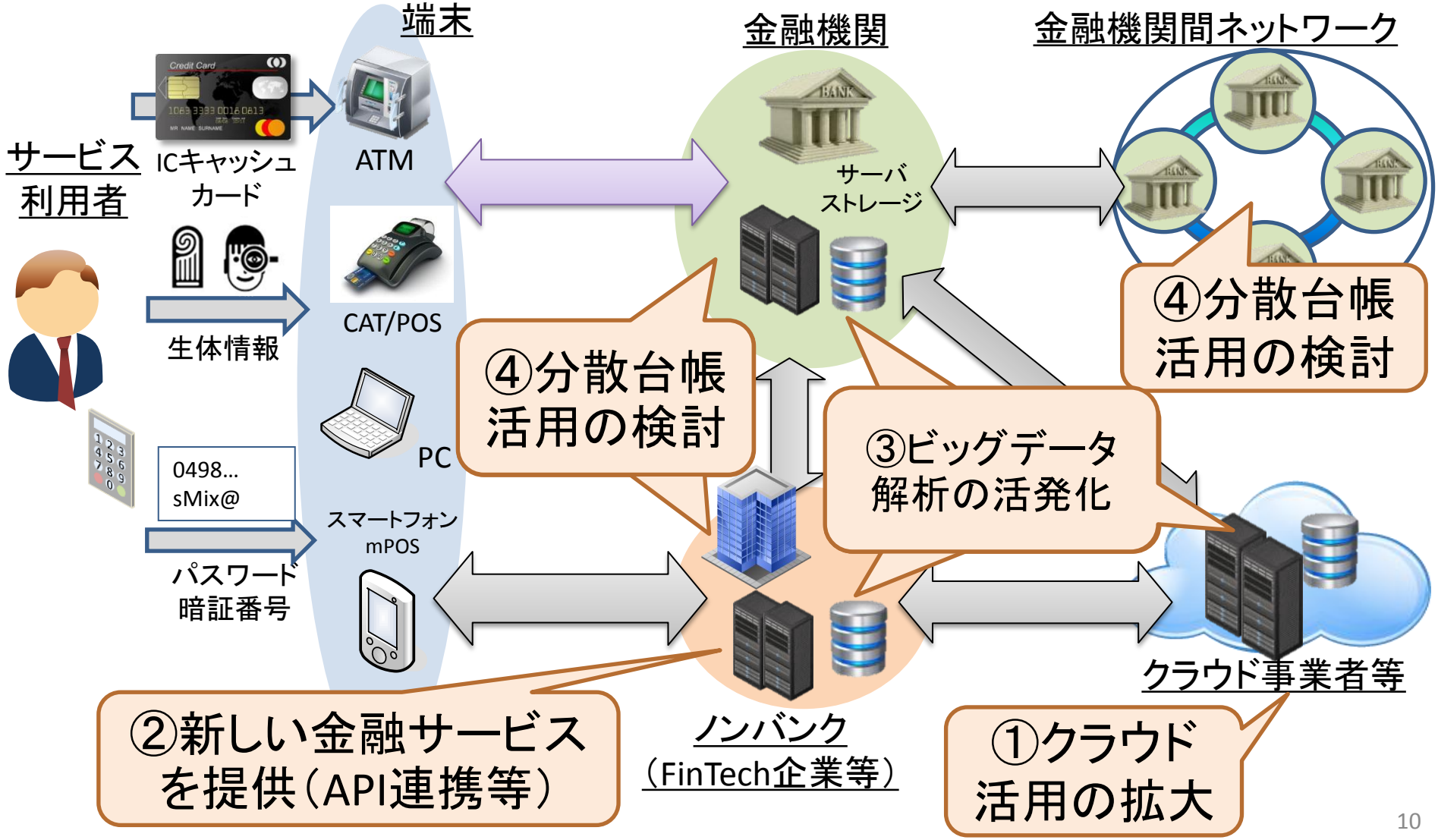
- 「すでに取り組んでいる」「準備段階」あるいは「検討中」と回答した金融機関との割合は、全体で25.9%（28年度、FISC調査）。

【ブロックチェーンまたは分散台帳のタイプ別の取組み状況】



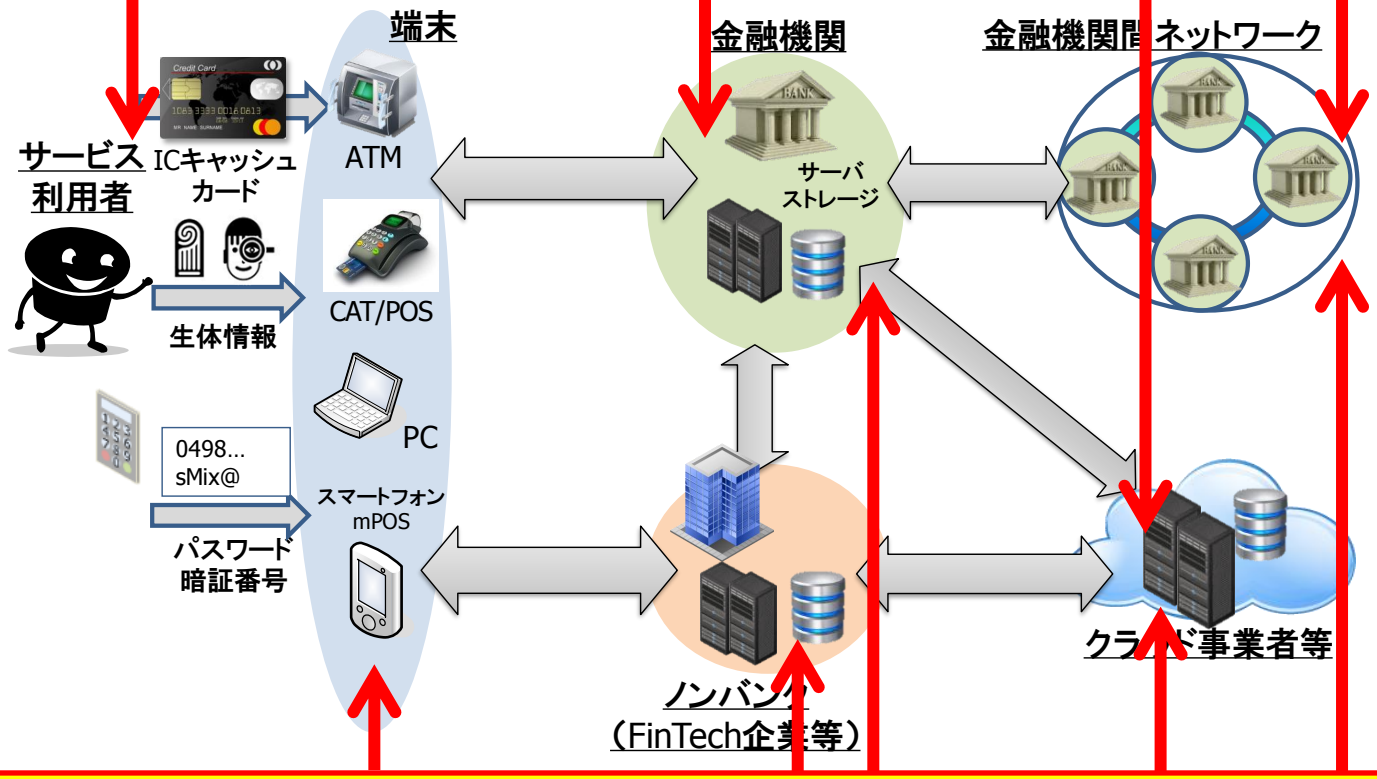
出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表1-8、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞

さまざまな企業・組織間のサービス・業務・データの連携が広がっている



セキュリティと利便性をどう両立させるか

データの漏洩・改変リスクの高まりとガバナンス
（さまざまな企業等がデータを取り扱うようになる）



（セキュリティ対策実施時における）利便性の低下
（暗号化・復号処理、鍵管理等の負担が増加する可能性）

高機能暗号のメリット

■ 基本的な暗号機能に加えて、高度な機能を実現する暗号技術

- □ データを「暗号化したまま」一定の処理を実行可能
  - ✓ データを暗号化したまま統計解析等の演算処理を実行できる（準同型暗号）
  - ✓ データを暗号化したままキーワード検索を実行できる（検索可能暗号）
- □ データの共有を「効率良く」実行可能
  - ✓ 暗号化したデータの復号権限を利用者の属性に応じて制御できる（属性ベース暗号）

高機能暗号をうまく活用できないだろうか？

情報技術研究センターにおける研究活動

■ 高機能暗号の金融分野への応用にかかる研究

【CSEC研究会のホームページの一部】

【 CSEC優秀研究賞 】

定期開催のCSEC研究発表会においてCSECに申込のあった発表を対象とし、高い完成度を持つ優れた論文だけではなく、今後の発展が有望視されるような、もしくは新たな分野を切り開くような萌芽的な研究発表も含めて表彰します。表彰数は、原則として各定期研究会における発表数の 10% 程度とします。本表彰の選考は、CSEC運営委員会による推薦と、推薦対象に対する運営委員等による評点平均に基づき、選考委員会（CSEC幹事団および推薦論文担当）により実施します。同委員会の委員長であるCSEC研究会主査により表彰されます。

【 平成29年度/2017年度 】

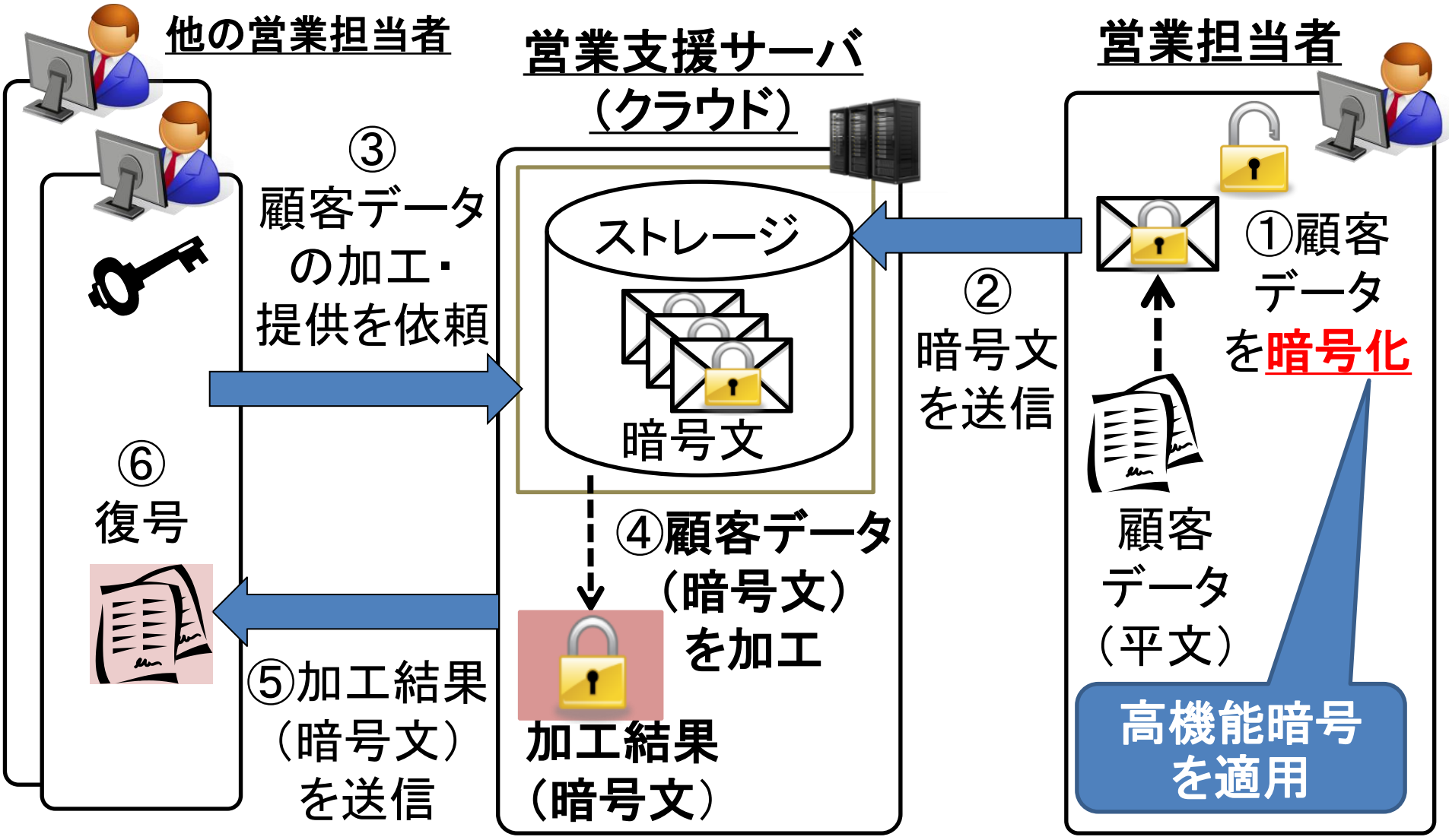
- 第78回 CSEC研究発表会
  - 高機能暗号の金融分野での応用に関する考察: 清藤武暢(日本銀行金融研究所)　青野良範(情報通信研究機構 サイバーセキュリティ研究所)　四方順司(横浜国立大学大学院環境情報研究院)
  - サイト関連情報に基づいたWebサイト脅威度推定機能の提案: 藤井翔太(株式会社日立製作所)　鬼頭哲郎(株式会社日立製作所)　重本倫宏(株式会社日立製作所)　藤井康広(株式会社日立製作所)

出典：http://www.iwsec.org/csec/csec_award.html#CSECAward

■ 情報セキュリティ・シンポジウム（2017.3.9）

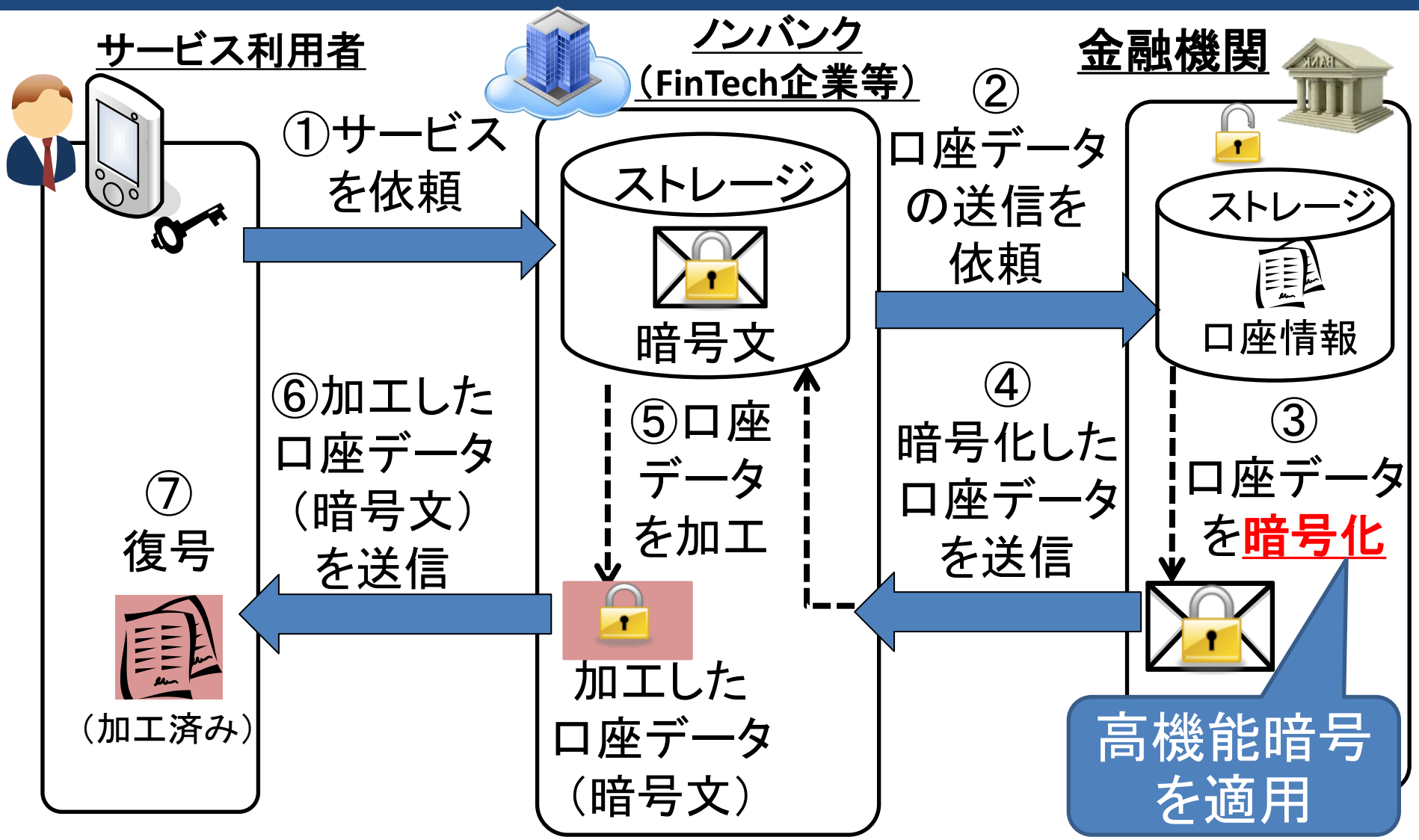
- テーマ：**新たな金融サービスを支える高機能暗号：セキュリティと利便性の両立に向けて**

営業支援サービスでの活用（イメージ）



出典：清藤・青野・四方、「公開鍵暗号型の高機能暗号を巡る研究動向」IMES Discussion Paper No.2017-J-8、日本銀行金融研究所、2017年

口座情報サービスでの活用（イメージ）



出典：清藤・青野・四方、「公開鍵暗号型の高機能暗号を巡る研究動向」IMES Discussion Paper No.2017-J-8、日本銀行金融研究所、2017年

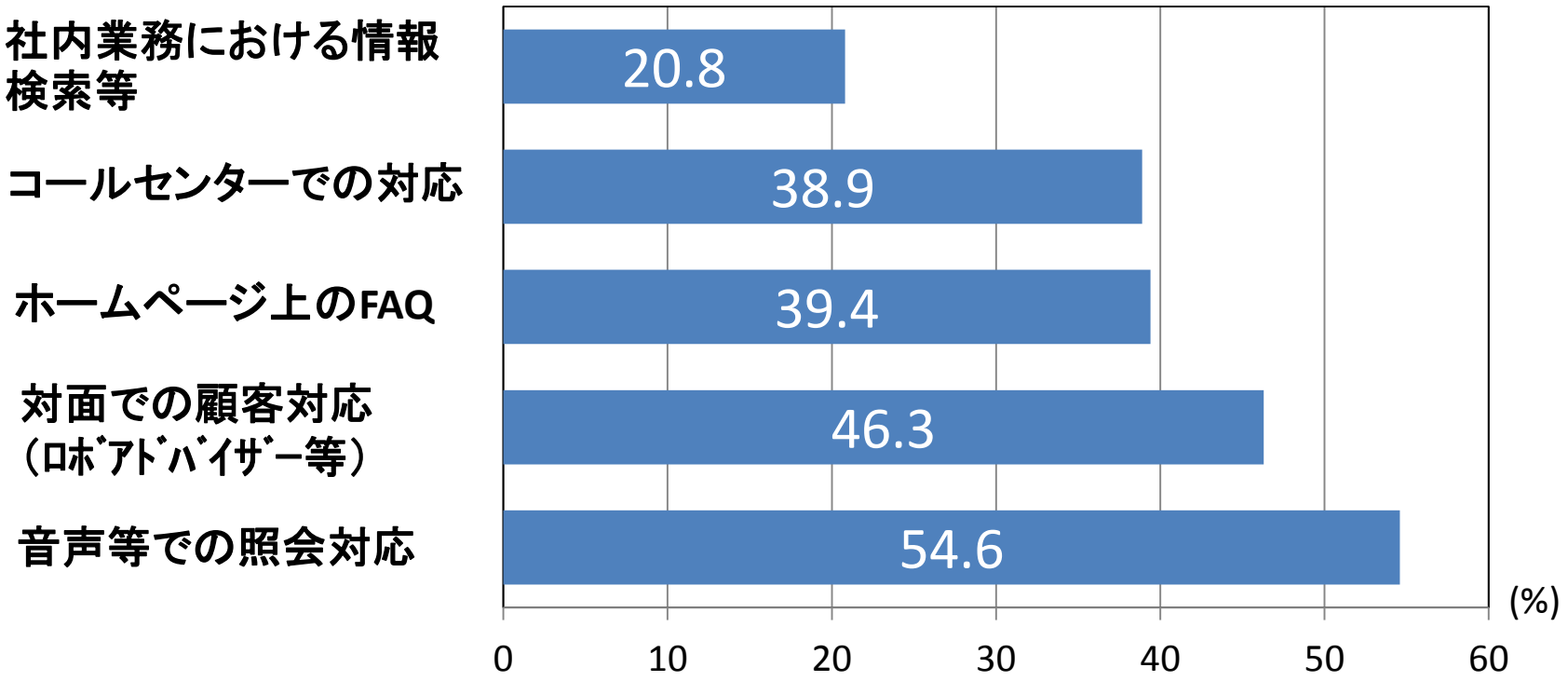
高機能暗号にかかる課題

- 営業支援サービスや口座情報サービスのモデルにおける評価
  - セキュリティ
    - ✓処理対象のデータの機密性が向上。
  - 利便性
    - ✓従来の暗号を利用する場合よりも、鍵管理のコストが低減するものの、暗号処理コストは増加する傾向。
- 課題
  - メリット・デメリットの明確化
  - 高機能暗号の活用事例の蓄積と理解・研究の促進
  - セキュリティ等にかかる客観評価や標準化

金融機関によるAIの活用の目的

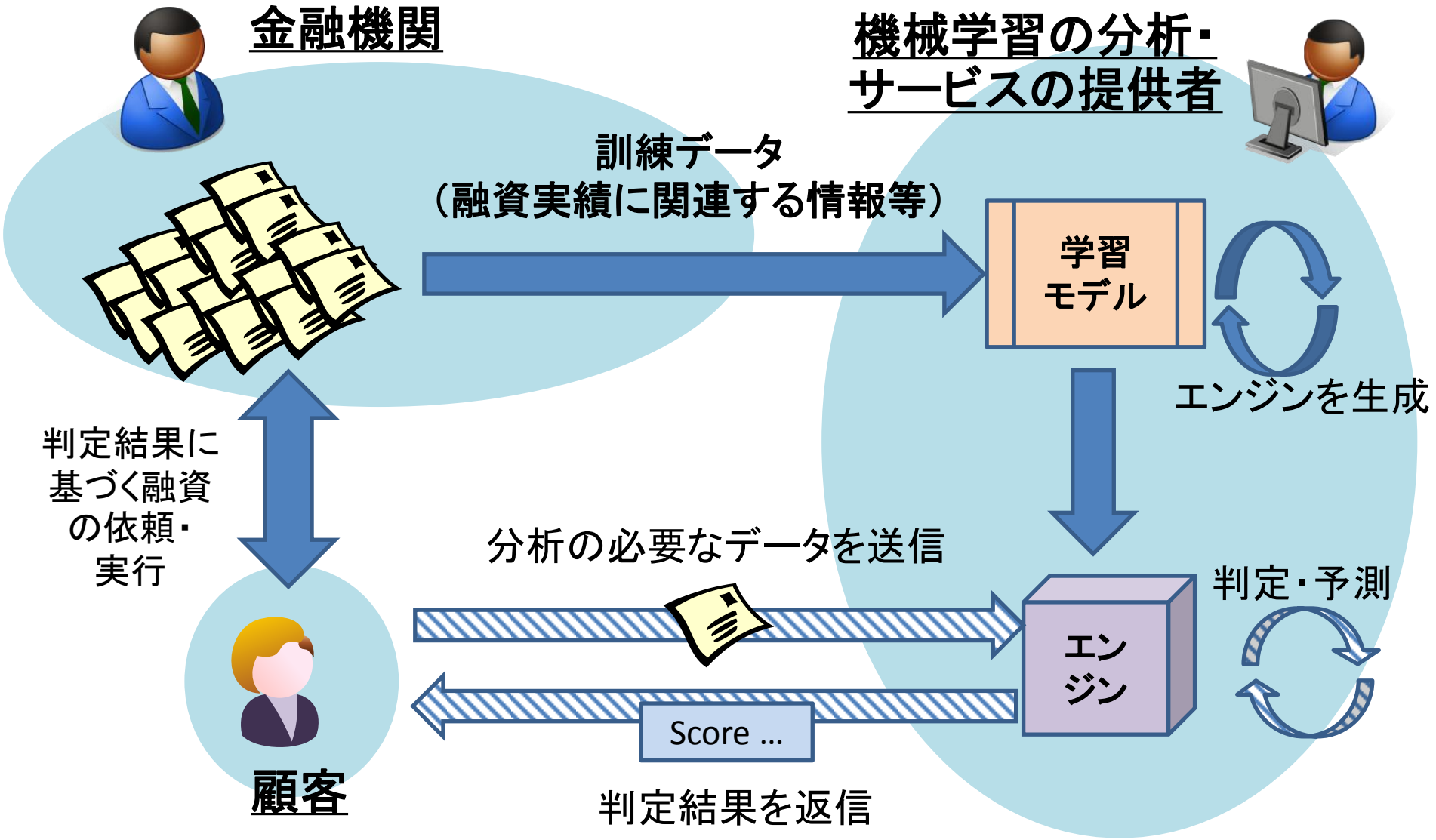
- AIを「導入中」「準備段階」または「検討中」と回答した金融機関等の割合は、36.8%（28年度、FISC調査）。

【各活用目的における金融機関等の割合】

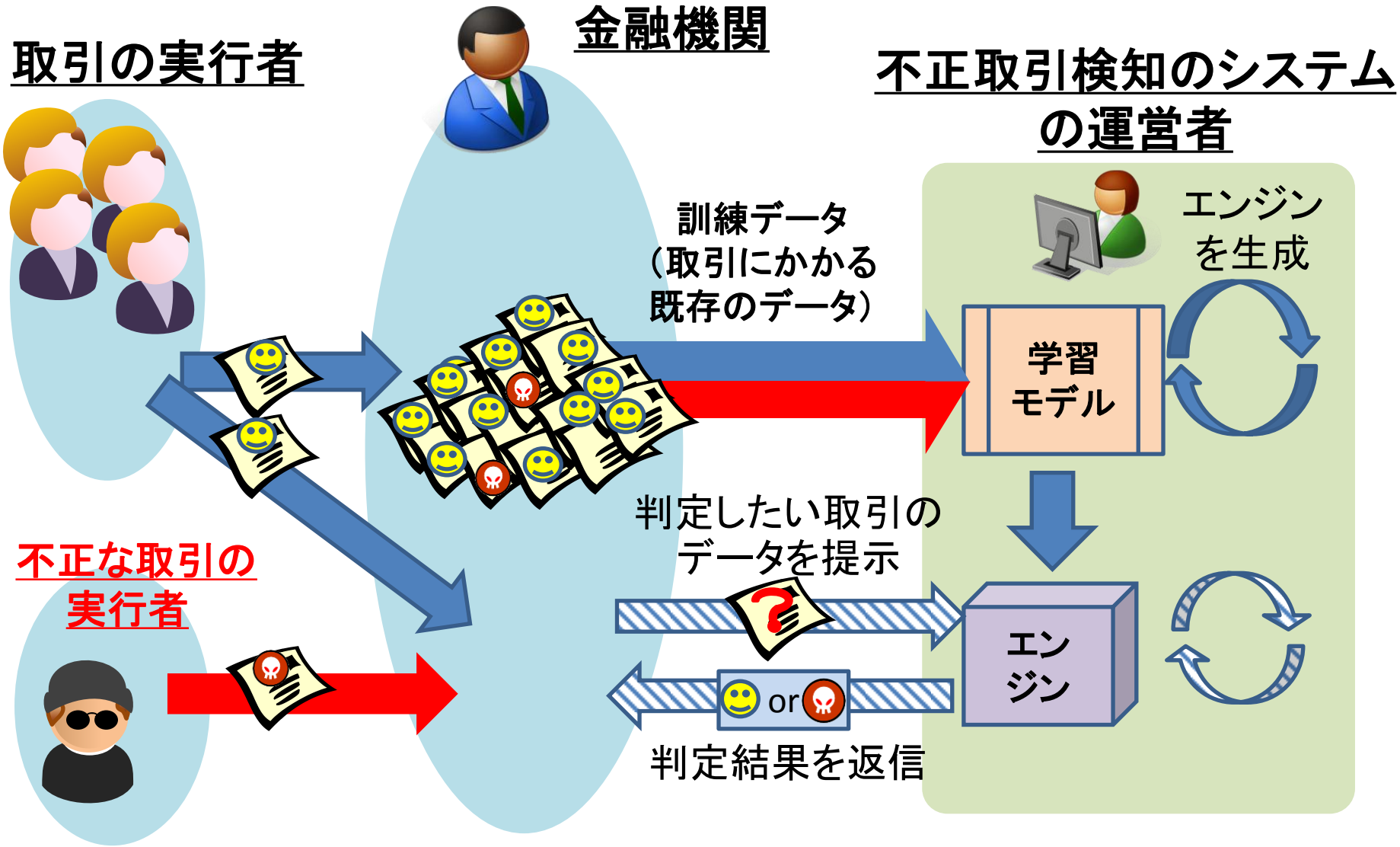


出典：金融情報システムセンター「平成29年度金融機関アンケート調査結果」（平成29年10月）
＜図表1-2、調査対象期間：平成28年4月～平成29年3月、有効回答機関数：676＞

資金貸出・融資分析のモデル



不正な取引の検知のモデル



情報技術研究センターにおける研究活動

■ **機械学習システムの脆弱性や対策にかかる研究動向をサーベイ(宇根・井上ペーパー)**

- **CSS 2018 (2018.10.22～25)において発表。**

【CSS2018プログラムの一部】

2B1: 敵対的学習 (座長: 高橋　健志)

2B1-1: 機械学習システムの脆弱性と対応策にかかる研究動向について

宇根 正志(日本銀行)

○ 井上 紫織(日本銀行)

2B1-2: 画像分類深層学習器に対する Model Extraction 攻撃の検証

○ 岡田 莉奈(NTTセキュアプラットフォーム研究所)

長谷川 聡(NTTセキュアプラットフォーム研究所)

2B1-3: 深層学習における高い非認識性を持つ電子透かしの疎構造に対する埋め込み

◎ 南波 涼太(筑波大学大学院)

佐久間 淳(筑波大学大学院、理化学研究所 革新知能統合研究センター、JST CREST)

2B1-4: 実世界でも攻撃可能なAudio Adversarial Example

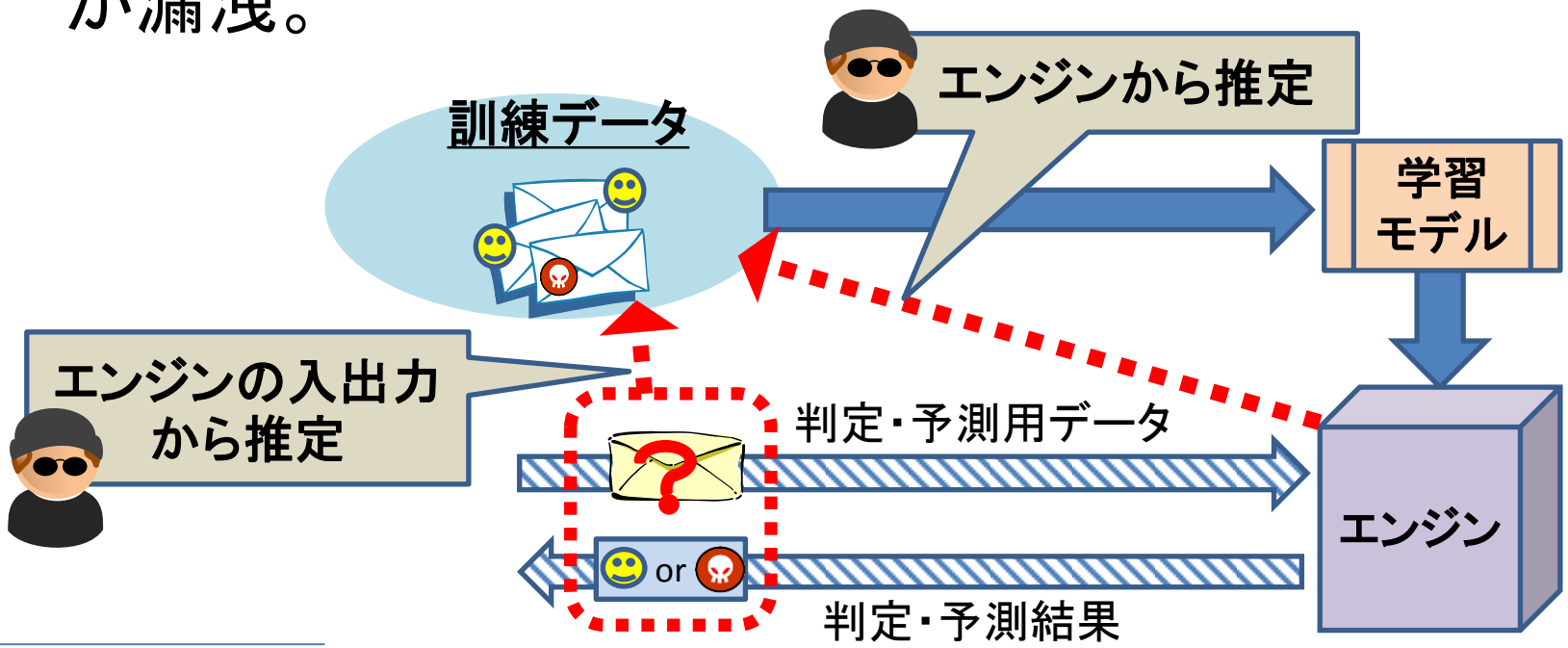
◎ 矢倉 大夢(筑波大学 / 理化学研究所 革新知能統合研究センター)

佐久間 淳(筑波大学 / 理化学研究所 革新知能統合研究センター / JST CREST)

出典:　https://www.iwsec.org/css/2018/program.html#i2B1

訓練データにかかる情報の漏えい

- エンジンやその入出力から、訓練データにかかる情報が漏洩。



（参考文献）

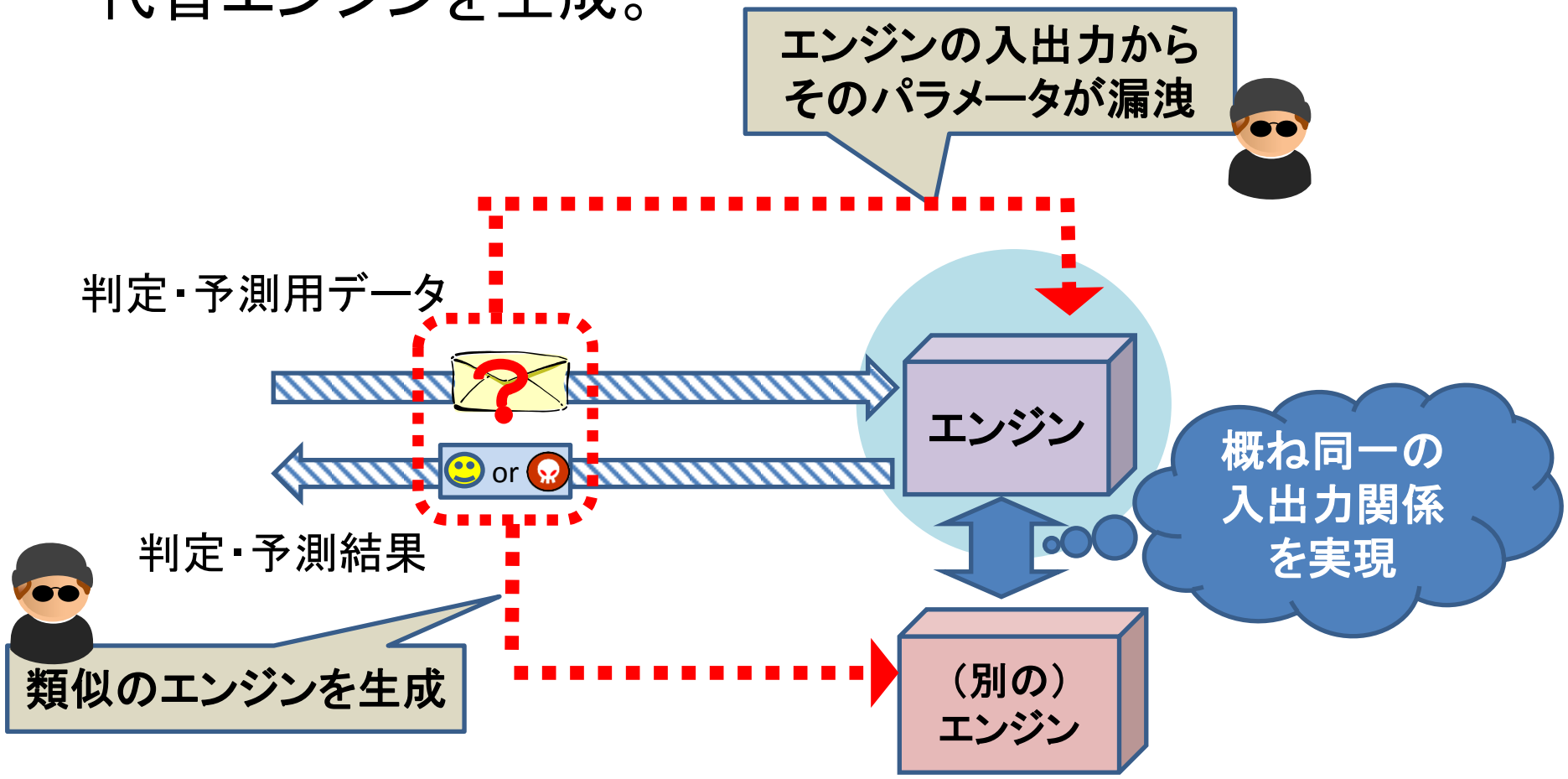
・Shokri, Reza, Marco Stronati, Congzheng Song, and Vitaly Shmatikov, “Membership Inference Attacks Against Machine Learning Models,” Proceedings of the 2017 IEEE Symposium on Security and Privacy, IEEE, 2017, pp.3-18.

・Ateniese, Giuseppe, Giovanni Felici, Luigi V. Mancini, Angelo Spognardi, Autonio Villani, and Domenico Vitali, “Hacking Smart Machines with Smarter Ones: How to Extract Meaningful Data from Machine Learning Classifiers,” arXiv: 1306.4447v1, 2013.

・Fredrikson, Matt, Somesh Jha, and Thomas Ristenpart, “Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communication Security, ACM, 2015, pp.1322-1333.

エンジンにかかる情報の漏えい

- エンジンの入出力等から、そのパラメータが漏洩。
  代替エンジンを生成。

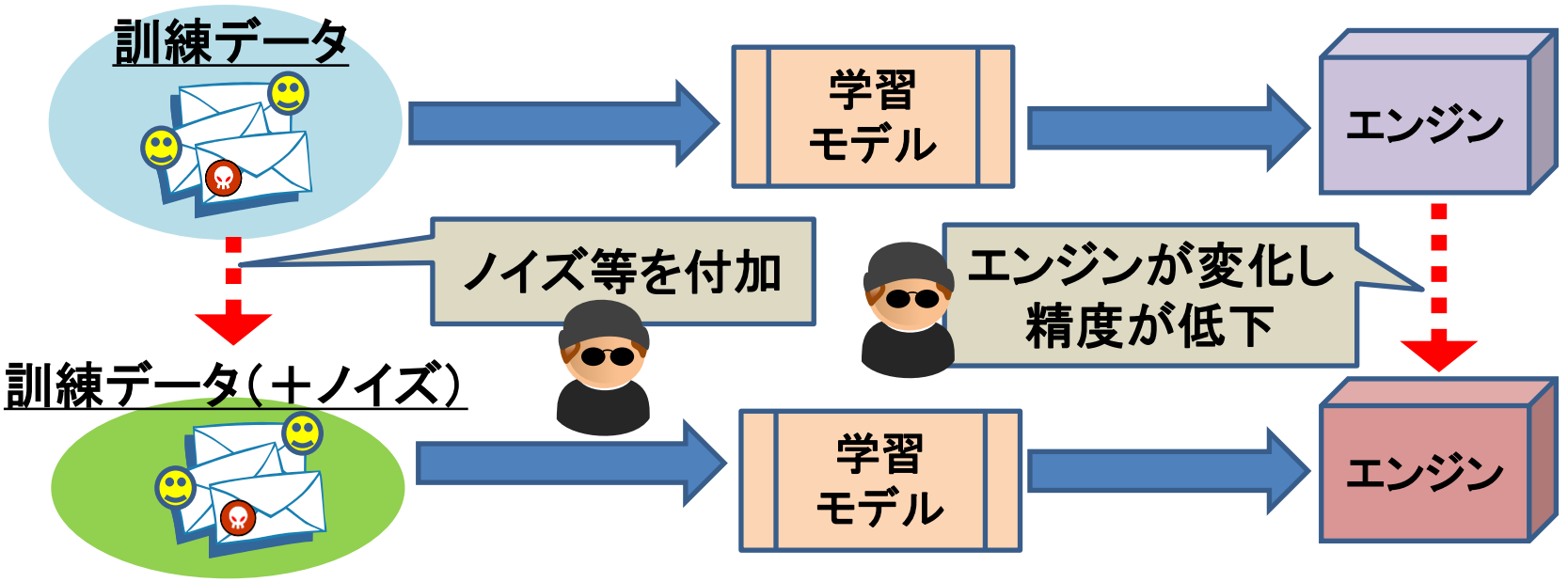


（参考文献）

Tramèr, Florian, Fan Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart, “Stealing Machine Learning Models via Prediction APIs,” Proceedings of the 25th USENIX Security Symposium, USENIX, 2016, pp.601-618.

訓練データの変化によるエンジンの精度低下

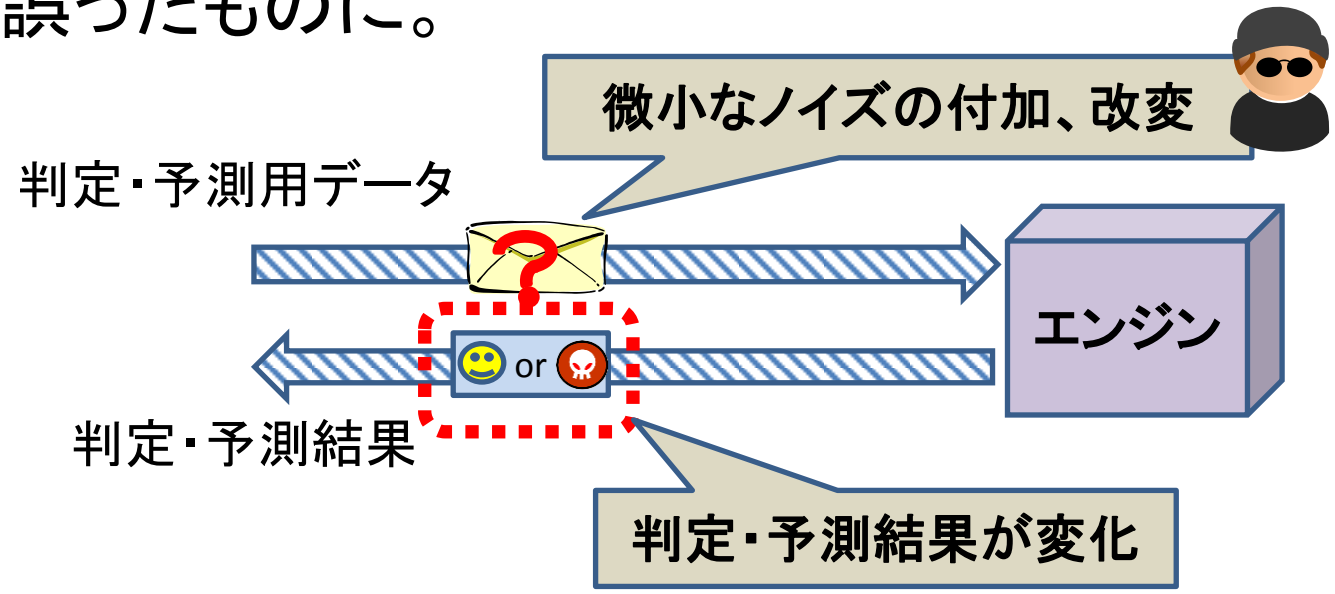
- 訓練データの微小なノイズや改変により、エンジンが変化して精度が低下。



（参考文献）
・Biggio, Battista, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrndić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli, “Evasion Attacks Against Machine Learning at Test Time,” Machine Learning and Knowledge Discovery in Databases, LNCS 8190, Springer, 2013, pp.387-402.
・Kloft, Marius, and Pavel Laskov, “Online Anomaly Detection under Adversarial Impact,” Proceedings of the 13th International Conference on Artificial Intelligence and Statistics (AISTATS), 2010, pp.405-412.
・Mei, Shike, and Xiaojin Zhu, “Using Machine Teaching to Identify Optimal Training-Set Attacks on Machine Learners,” Proceedings of the 29th AAAI Conference on Artificial Intelligence, Association for the Advancement of Artificial Intelligence (AAAI), 2015, pp.2871-2877.

入力データの変化による誤った判定・予測

- エンジンへの入力データのノイズや改変により、判定・予測が誤ったものに。



（参考文献）
・Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus, “Intriguing Properties of Neural Networks,” Proceedings of 2014 International Conference on Learning Representation, Computational and Biological Learning Society, 2014.
・Papernot, Nicolas, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami, “Practical Black-Box Attacks against Machine Learning,” Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, ACM, 2017, pp.509-519.
・Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy, “Explaining and Harnessing Adversarial Examples,” Proceedings of 2015 International Conference on Learning Representation, 2015.
・Carlini, Nicholas, and David Wagner, “Towards Evaluating the Robustness of Neural Networks,” Proceedings of 2017 IEEE Symposium on Security and Privacy, IEEE, 2017, pp.39-57.

対策の方針

- エンジンや訓練データにかかる情報の盗取への対策
  - 確信度が攻撃に用いられる場合、確信度を出力しないエンジンを利用、また、詳細な確信度が漏洩しないように運用。
  - 訓練や判定・予測を「暗号化したデータ」に対して実行。
    - 高機能暗号や秘密分散技術を活用。
- 訓練データや入力データの操作による攻撃の対策

✓学習モデル等の入力時に不正なデータを検知・排除。

・不正なデータを判定するニューラルネットワーク

・主成分分析、分布の差異の統計的分析

✓不正なデータによる影響を軽減・解消。

・データの正規化（ドロップアウト、平均値フィルター等）

各対策にかかる手法の厳密な評価は今後の課題。

（参考文献）
Carlini, Nicholas, and David Wagner, “Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods,” *Proceedings of the 10th ACM Workshop on Security and Artificial Intelligence (AISec)*, ACM, 2017, pp.3-14.

まとめと今後の課題

- 金融機関が、クラウド事業者、FinTech企業等とデータを連携してサービスや業務を行うケースが増えてきている。
  - セキュリティと利便性を両立させる方法として、高機能暗号が有力な候補の1つ。
- AIや機械学習の活用に向けた動きが活発化。
  - 機械学習システムのセキュリティについても、今後の研究動向を注視していくことが必要。
  - 金融分野向けの機械学習システムに、既知の脆弱性や攻撃・対策がどう影響するかが注目される。
- ユーザーと技術者・研究者が連携して適切な活用方法を検討していくことが有用。