日本金融監査協会ウェビナー

AML/CFT対策におけるAI活用と管理

2021.12.23 | SAS Institute Japan株式会社

ソリューション統括本部
Fraud & Security Intelligenceソリューショングループ
シニアマネージャー 内山 剛

本資料について

- 本資料は講演者の個人的な見解を示したものであり、SAS Institute Japan 及び SAS Institute Inc. の公式な見解を示したものではありません。
- 本資料に記載された内容について、正確性及び網羅性が保証されるものではありません。
- 本資料に記載された見解は作成時点のものであり、今後変更される場合があります。
- 本資料の無断転記・転載はご遠慮ください。

「The Power to Know®（知る力）」を全てのお客さまに

SAS Instituteのご紹介

幅広いアナリティクス・ソリューションと豊富な業種別知識により、高い顧客満足度を維持しお客さまの確信を生み出し続けています。

- アナリティクス ソフトウェア・サービスのリーディング・カンパニー
- 世界の銀行トップ100行のうち99行がSASを活用
- 2020年は約30億ドルの収益を上げ、45年連続で黒字を達成
- 日本では幅広い業種で1,500 社 2,300 サイトの導入実績
- 売上の26%以上を研究開発に投資
  →大手ソフトウェア企業平均の2倍以上を継続投資

SAS Institute Inc.

設立	：1976年
所在地	：米国ノースカロライナ州キャリー
代表者	：Dr. James Goodnight（CEO,設立者）
所在国	：世界59ヶ国
従業員数	：全世界で12,000人以上

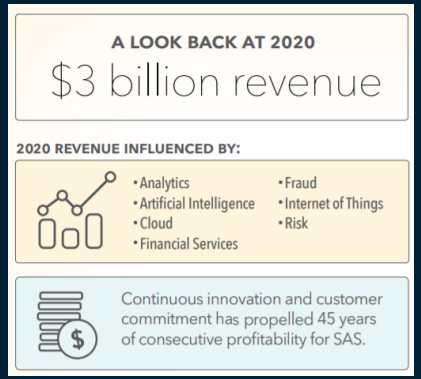
SAS Institute Japan 株式会社

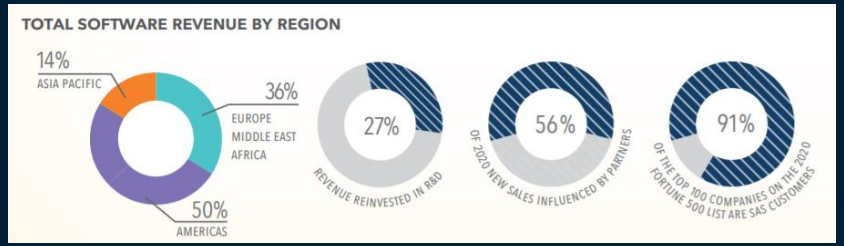
設立	：1985年
所在地	：東京・大阪
代表取締役社長	：マイケル・キング

アナリティクスのリーディング・カンパニー

SASのデータと実績

SAS Institute データ





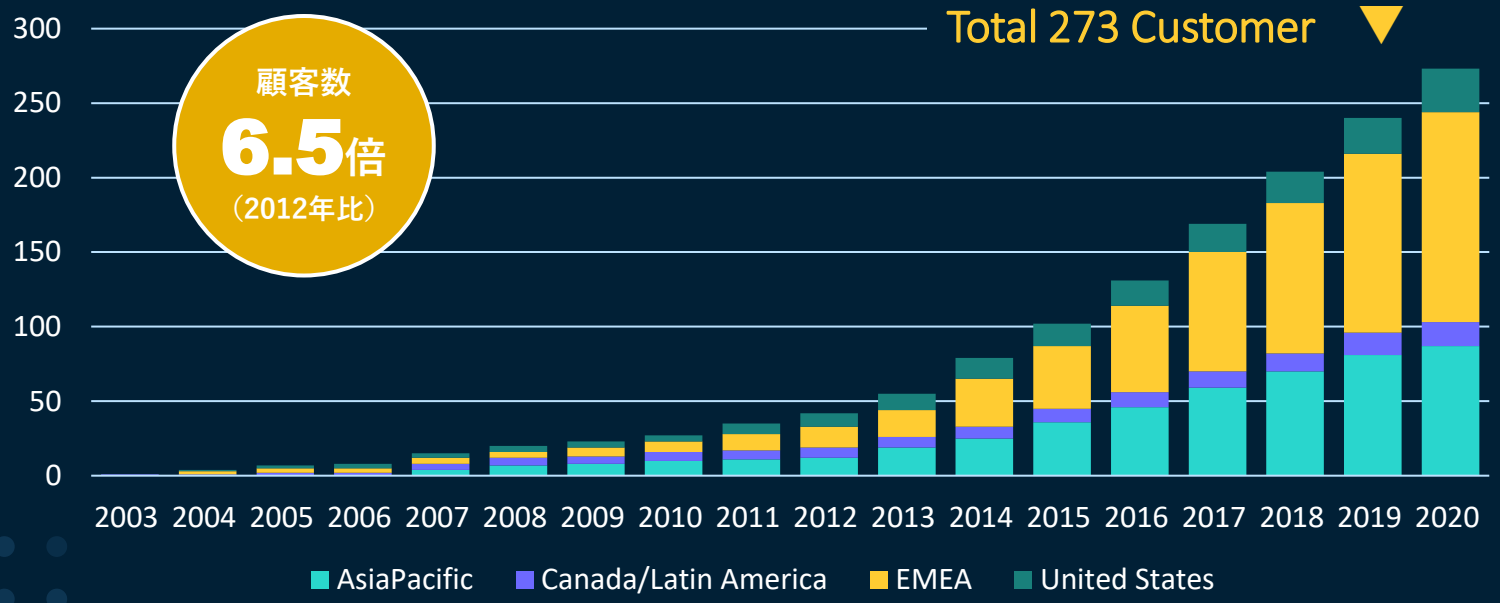
SAS Institute Japanの導入実績

製造	コニカミノルタジャパン株式会社、株式会社ブリヂストン、三菱重工航空エンジン、TOYO TIRE 株式会社、株式会社村田製作、住友ゴム株式会社、日本製紙株式会社、日本たばこ産業株式会社、キリンビール株式会社、等
金融サービス	みずほ銀行、三菱UFJ銀行、三井住友銀行、りそな銀行、横浜銀行、福岡銀行、四国銀行、JCB、クレディセゾン、イオンクレジットサービス、かんぽ生命保険、東京海上日動火災、等
医薬	アステラス製薬、EAファーマ、イーピーエス、エイツーヘルスケア、小野薬品、興和、サノフィー、塩野義製薬、第一三共、大正製薬、武田薬品工業、中外製薬、日本医療データセンター、ノバルティス、ファイザー、藤本製薬、等
教育・官公庁・医療	東京大学、京都大学、一橋大学、慶応義塾大学、中央大学、同志社大学、福岡大学、総務省統計局、統計数理研究所、日本貿易振興機構、国立循環器病研究センター、国立がん研究センター、国立健康・栄養研究所、等
通信・インフラ	NTTドコモ、KDDI、NTTコムウェア、東京電力、等
流通・運輸	イオン、ニッセン、ディノス、 日本航空、全日空、ソラシドエア、 等

AML/CFT領域での実績

SAS Compliance Solution の導入実績

SAS Compliance Solution は、2003年のリリース以後、継続的に顧客を増やし続けています。2012年のリスク・ベース・アプローチのコンセプトが明確化された、改定FATF勧告以後、特に多くのお客様にご採用頂いております。



本日の結論

“管理なくしてAIなし”

今日お話すること

1. AML/CFTにおけるAI活用事例

2. AI活用検討のポイントとモデル管理の重要性

AML/CFTにおいて次に求められるテクノロジー

Next Generation AML

現在のAML

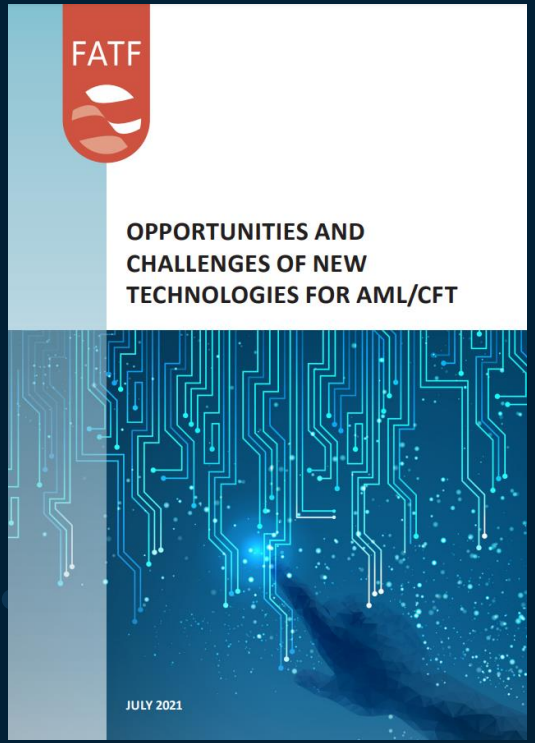
次世代AML

Rules ルールロジック	Analytics データ分析	Robotics ロボティックス	Semantic Analysis 意味解析	Artificial Intelligence 人口知能
Heuristic rules	Anomaly / outlier detection	Robotic Process Automation	Unstructured data analysis	Machine Learning
Tuning/ thresholds	Network analysis	Alert & Case triage	Linguistic analysis	Smart process automation
Sanctions & PEP Screening	Data exploration & visualization	Process orchestration	Automated reporting	Automated decision making

Source: “Innovations in AML and KYC platforms“, Celent, 2018
https://www.celent.com/ja/insights/629012081

AML/CFTにおいて次に求められるテクノロジー

FATF Paper



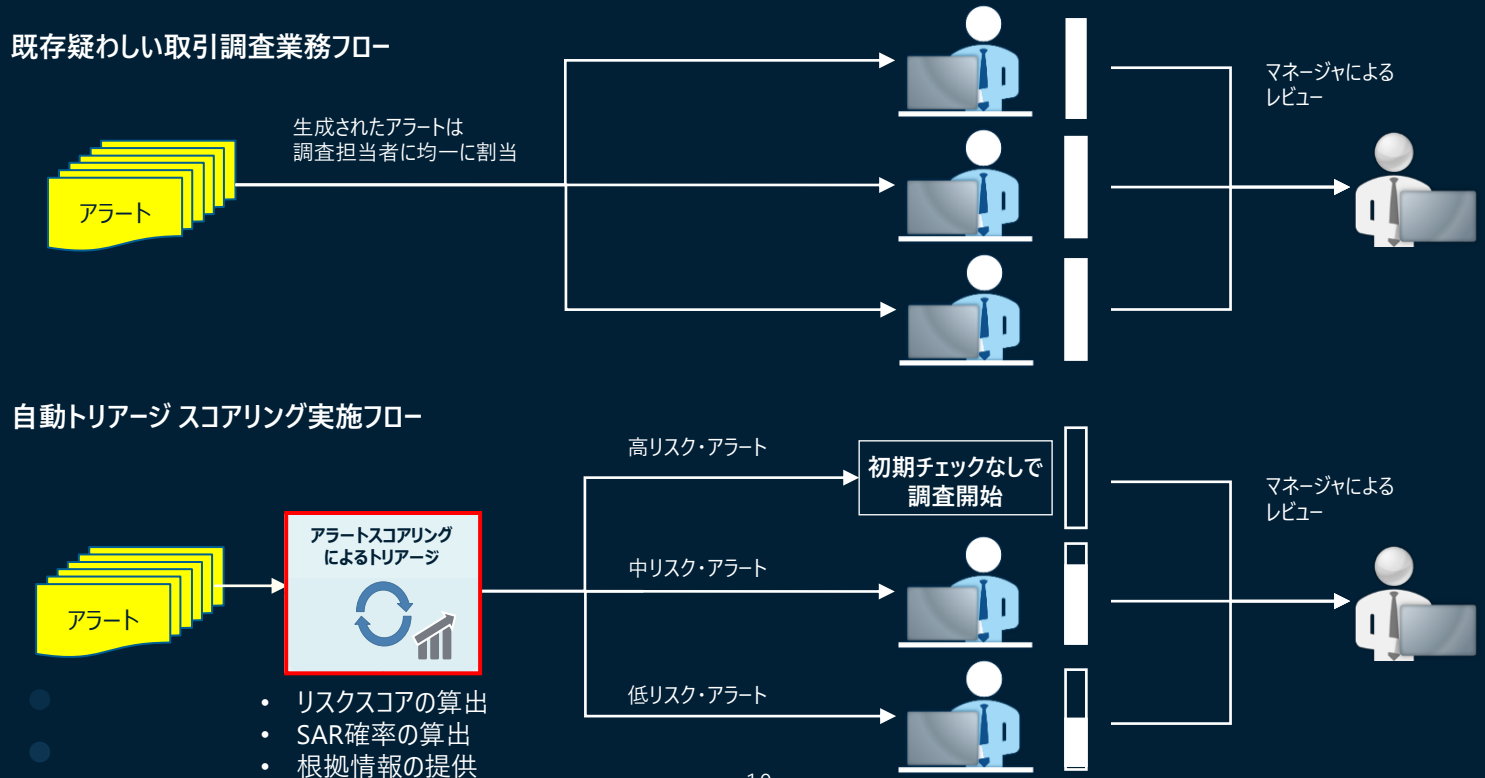
Opportunities and Challenges of New Technologies for AML/CFT, July 2021

- Artificial Intelligence(AI)
- Natural Language Processing and soft computing techniques
- Distributed Ledger Technology
- Digital Solution for Customer Due Diligence
- Application Programing Interfaces(API)

Opportunities and Challenges of New Technologies for AML/CFT
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-for-aml-cft.html

AML/CFTにおけるAI活用事例①

アラート・トリアージによる業務効率化



AML/CFTにおけるAI活用事例①

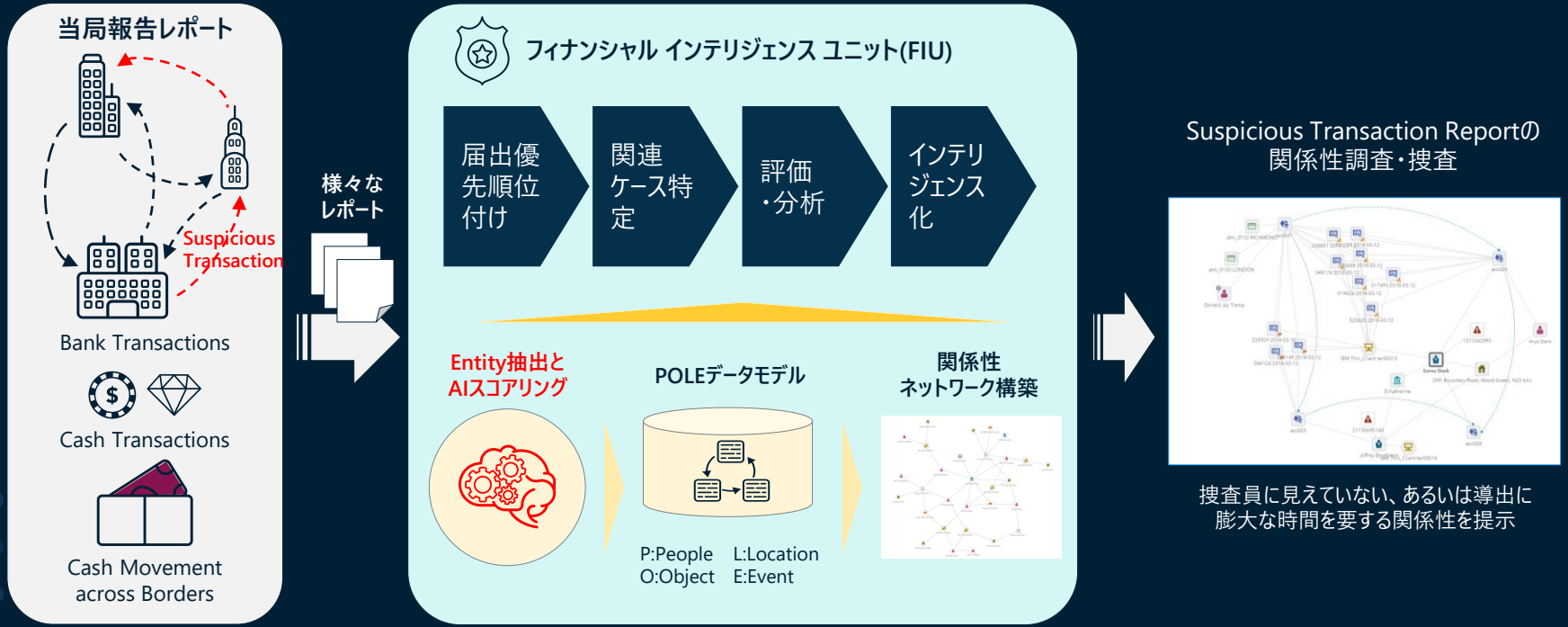
アラート・トリアージによる業務効率化

届出要否判定の根拠情報の提供イメージ

アラートID	信頼度（リスク度）	AIが高リスクと考える理由	AIが低リスクと考える理由
100012	99.81%	・過去届出履歴のある相手先への送金 ・現金出金の頻度の急激な増加 ・端数なし数字の振込が急激に増加	(なし)
100134	96.45%	・過去届出履歴あり ・捜査関係事項の照会履歴あり ・多頻度の現金出金あり	(なし)
…	…	…	…
…	…	…	…
101564	1.96%	・現金出金の頻度増加	・業種がオフィスビル賃貸であるため賃貸借契約に基づく入出金の可能性あり
100032	0.02%	(なし)	・長期の高額総資産顧客（30年以上） ・ギャンブル・証券取引などで多数の振替が発生した可能性あり

AML/CFTにおけるAI活用事例②

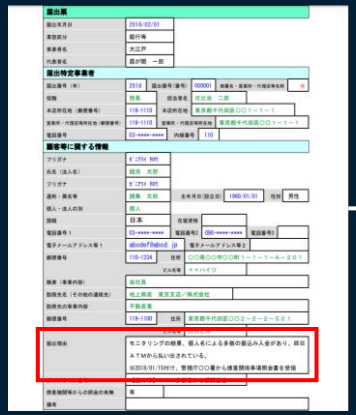
FIUにおけるSuspicious Transaction Reportの分析



AML/CFTにおけるAI活用事例②

FIUにおけるSuspicious Transaction Reportの分析

Source Documents
（国内疑わしい取引報告の届け出理由にあたる情報）



Document Store

Data Cleansing /Words Decomposition

Context Extraction

コンテキストの抽出
- c1: Used Car･Import Export
- c2: PEPs
- c3: Trading Goods
- c4: immigrants

Predictive Model/ Scoring

Words	Freq	parts of speech
Iran	1	Noun
Exports	1	Verb
Approve	1	Verb
used car	2	･･･
Jewelry	1	Noun
InportExport	1	Noun

Investigation Priority
High

Low

AI活用を目指した取り組みの落とし穴

POC“祭り“の後に見えてきたこと

- 解釈・説明できない機械学習モデル
  - Black-Box / White-Box
- 業務活用に至らない機械学習モデル
  - 業務フロー / データとスコアリングのサイクル
- 保守・運用の議論のない取り組み
  - モデルの陳腐化、塩漬け
  - 都度開発、デグレできない

今日お話すること

1. AML/CFTにおけるAI活用事例

2. AI活用検討のポイントとモデル管理の重要性

機械学習モデルを活用したシステムを構成する要素

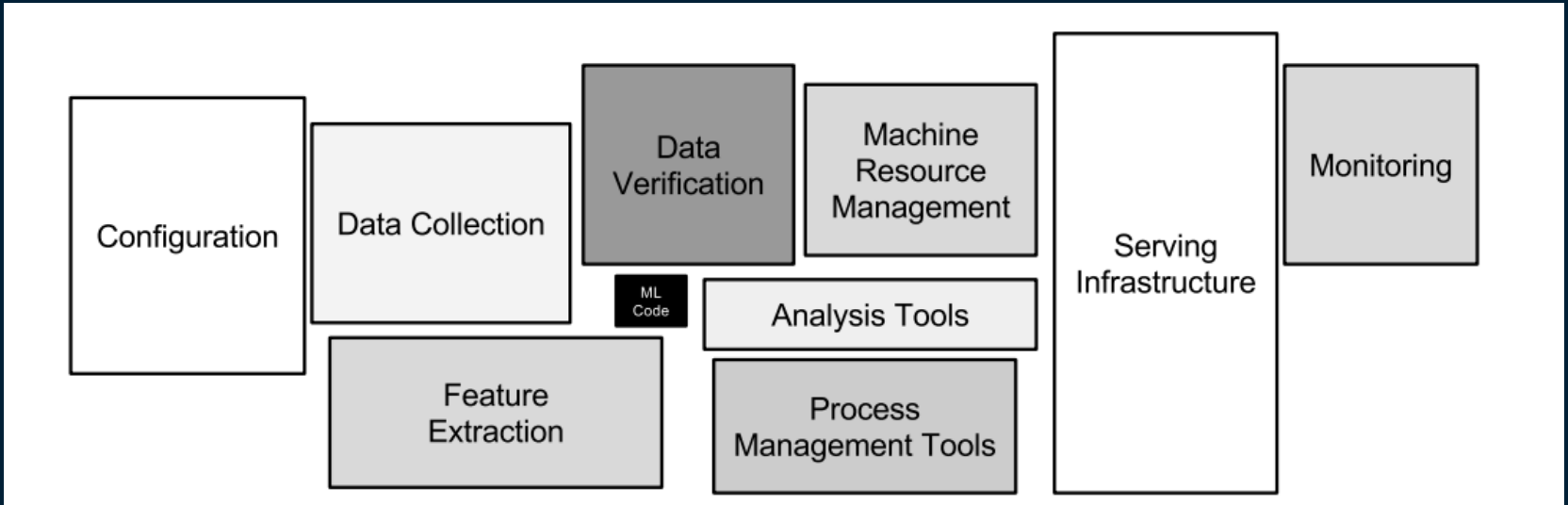


Figure 1: Only a small fraction of real-world ML systems is composed of the ML code, as shown by the small black box in the middle. The required surrounding infrastructure is vast and complex.
引用：『Hidden Technical Debt in Machine Learning Systems』
https://proceedings.neurips.cc/paper/2015/file/86df7dcfd896fcaf2674f757a2463eba-Paper.pdf

機械学習モデルの解釈性・説明性についてのニーズの高まり

ＡＩネットワーク社会推進会議 AI利活用ガイドライン

ＡＩ利活用ガイドライン “AI利活用原則” 抜粋

⑨透明性の原則	AIサービスプロバイダー及びビジネス利用者は、AIシステム又はAIサービスの入出力の検証可能性及び判断結果の説明可能性に留意する。
⑩アカウンタビリティの原則	AIサービスプロバイダ及びビジネス利用者は、消費者的利用者及び間接利用者を含むステークホルダーに対しアカウンタビリティを果たすよう努める。

ＡＩ利活用ガイドライン ～ＡＩ利活用のためのプラクティカルリファレンス～ ＡＩネットワーク社会推進会議
https://www.soumu.go.jp/main_content/000637097.pdf

機械学習モデルの解釈性・説明性についてのニーズの高まり

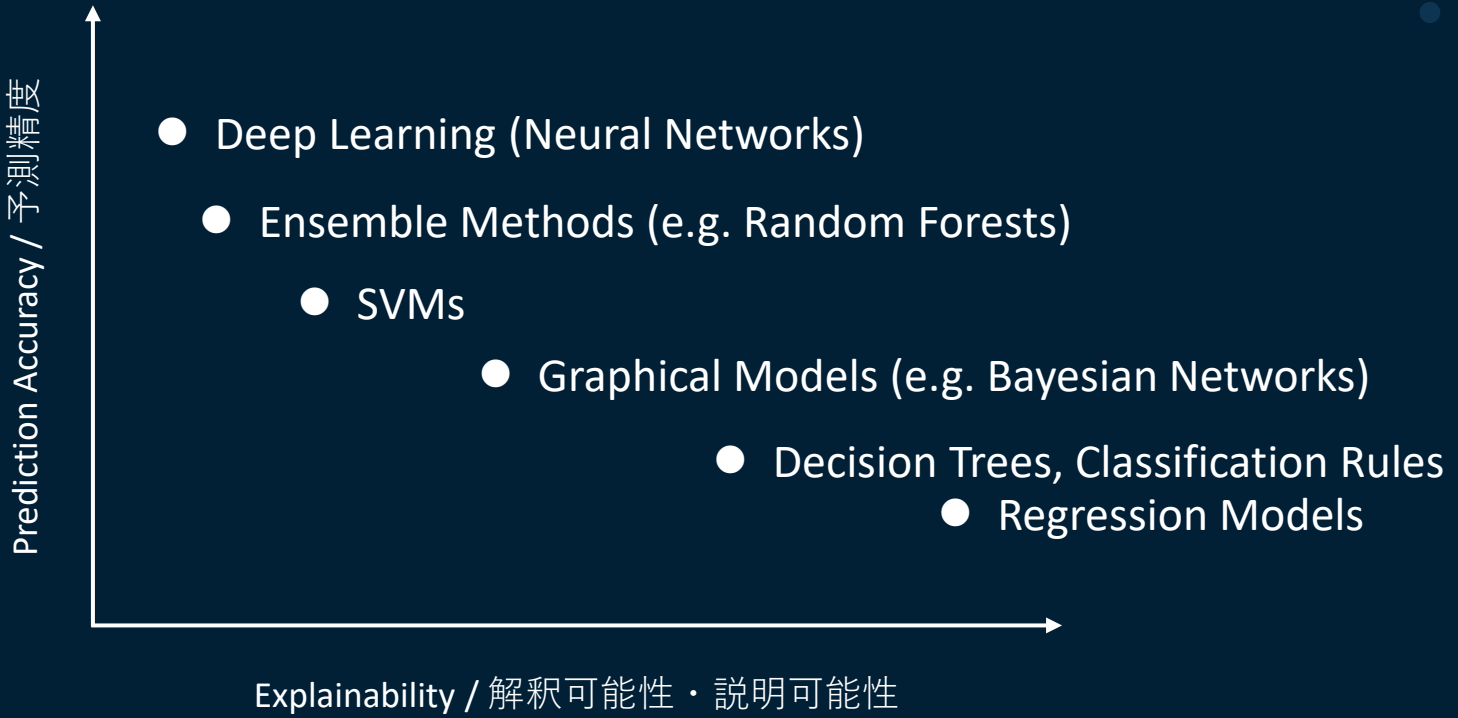
2015年以降、AIの解釈可能性に関する記事・論文が急激に増加

FIGURE 6. Surveyed articles by year (2004–2018)

引用：『Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)』
https://ieeexplore.ieee.org/document/8466590

機械学習モデルの精度と解釈性・説明性

”一般的には”トレードオフの関係にある

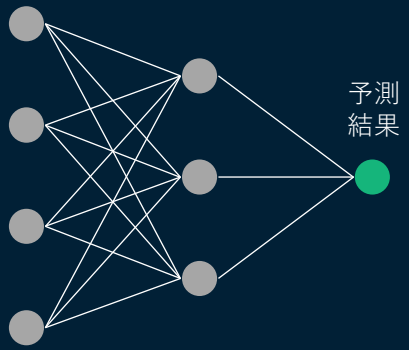


機械学習モデルの精度と解釈性・説明性

“Explainable AI“とは
複雑なモデルに対してExplanation Modelモデルを作って解釈する技術

複雑なモデル

- Deep Learning (Neural Networks)
- Ensemble Methods (e.g. Random Forests)

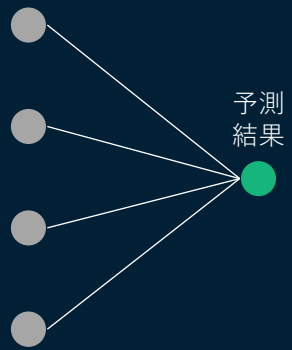


モデルが複雑であり、解釈が困難
Black-Box

Explanation Modelで
局所的に近似する

複雑なモデル

- Regression Models / 線形モデル



人間が理解できるシンプルなモデル
White-Box

機械学習モデルの精度と解釈性・説明性

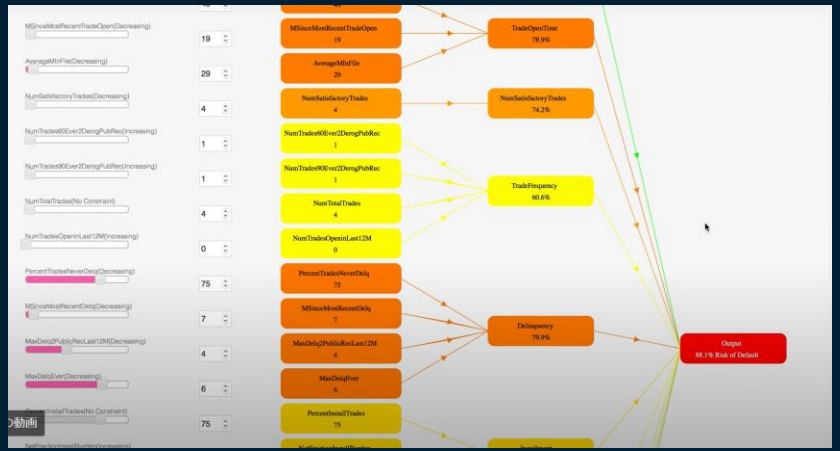
精度の高いモデル＝Blackboxではない

FICO xAIコンペにおけるデューク大学チームの例：

- ✓ 2018年米国、FICO主催のxAIの機械学習コンペ。
- ✓ テーマは、提供データモデルに対して精度が高く複雑なBlack-Boxモデルを構築し、その上でそのモデルがどのように機能しているのかを解釈・説明するというもの。
- ✓ このコンペは、暗黙的に複雑でBlack-Boxなモデルの方が精度が高いという前提に立っていた。

- ✓ 様々な企業・大学・研究機関が参加。その中でデューク大学チームは1週間ほどの基礎分析を経て、Black-Boxモデルを利用しなくても精度の高いモデルが構築できることを発見。その後、Black-Boxモデルと同等精度の完全に説明可能なWhite-Boxモデルとモデルのメカニズムを説明する動的ダッシュボードを作って提出。
- ✓ 結果、コンペのルールに反するため評価対象から外れる。

デューク大学チームが作成したダッシュボード



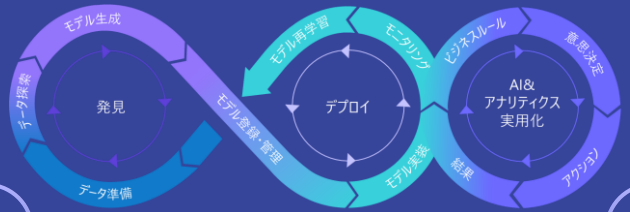
https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/6
http://dukedatasciencefico.cs.duke.edu/
https://www.fico.com/en/newsroom/fico-announces-winners-inaugural-xml-challenge

機械学習モデルを実装したシステム構築に求められること

“ModelOps” = モデル管理（保守・運用）の実現

ModelOps

「Model Operationalization（モデルの運用化）」
を実現するためのフレームワーク



DataOps

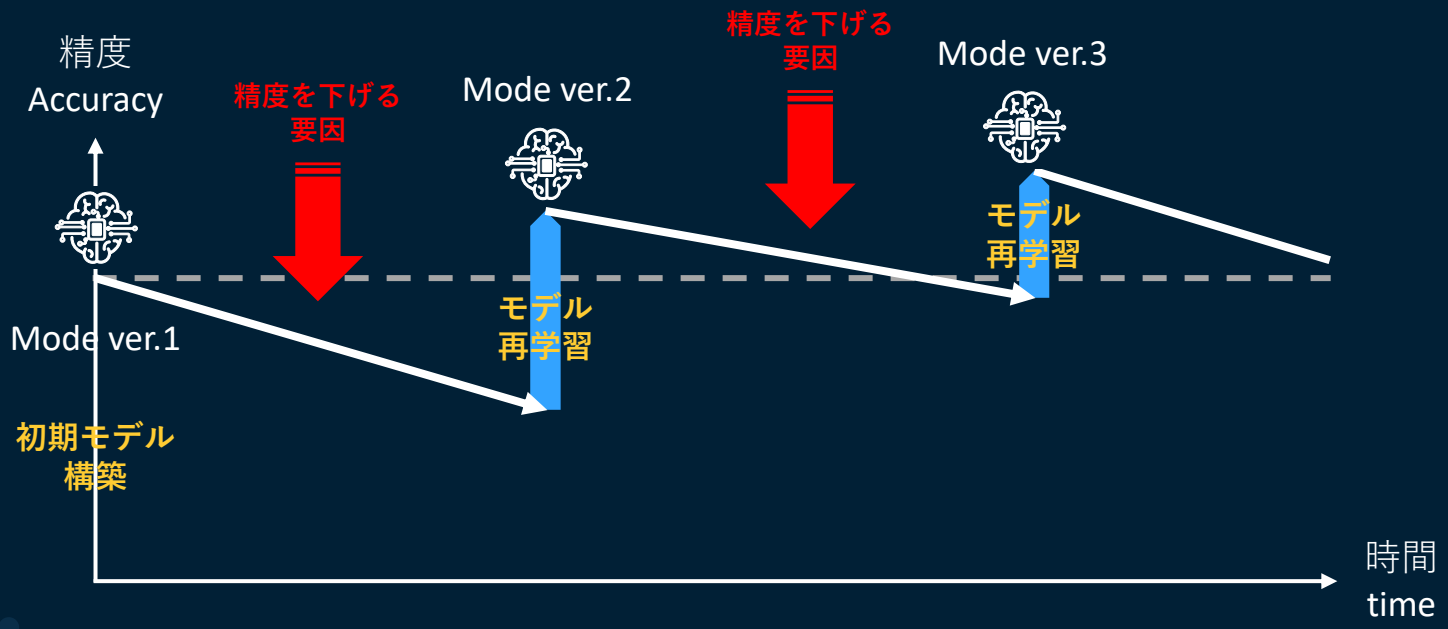
データ提供部門と利用部門間で
ツールやプロセスのプロトコルを
整理しデータ活用の強化を目指す
フレームワーク

DevOps

システムの開発と運用の効率を高
め迅速なビジネス価値を創出する
ことを目指すフレームワーク

なぜモデルの管理が必要か

モデルは時間とともに陳腐化、定期的な再学習が必要



モデル精度を下げる要因とは

Model Driftの発生

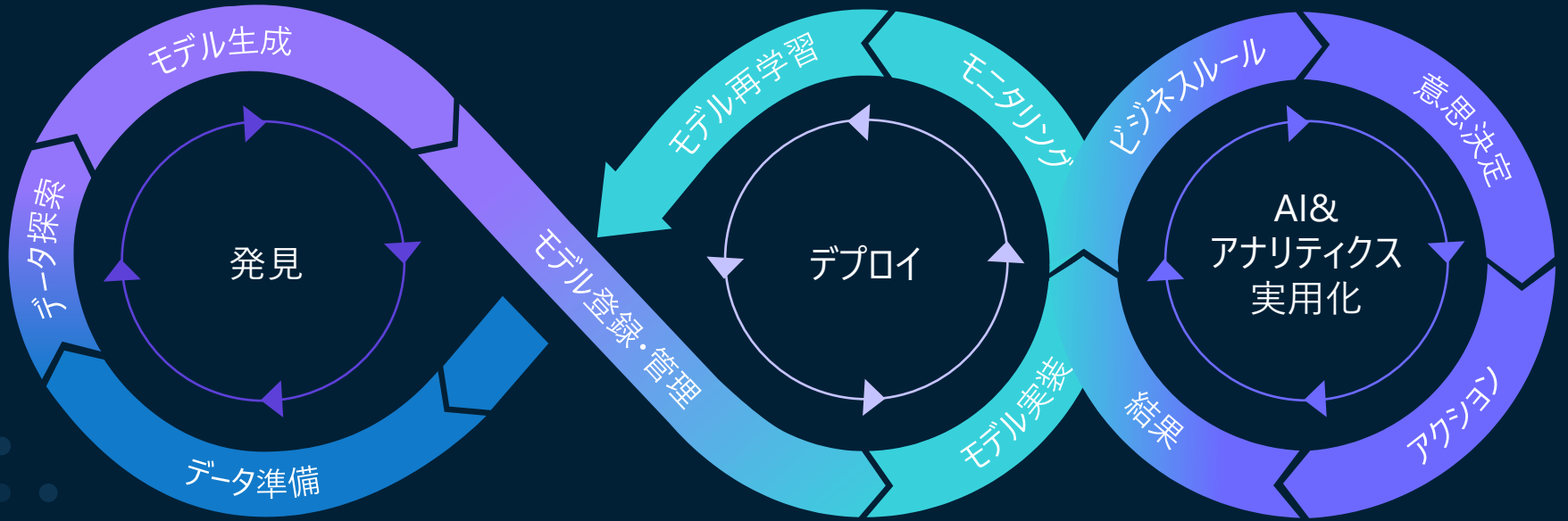
Model Drift	説明	ドリフトの例
概念ドリフト (Concept Drift)	**時間とともに目的変数の統計的属性が変化することで予測しようとする本当の概念も変化するパターン。**	✓マネーロンダリング・不正の手口が変化する ✓COVID-19による手口の変化
データドリフト (Data Drift)	**時間とともにモデルに投入する説明変数自体の統計的特性に変化が生じるパターン。**	✓新商品投入による売り上げの変化 ✓COVID-19による顧客行動の変化
上流データの変化 (Upstream data changes)	**時間とともにシステムの上流でデータ定義自体に変更が加えられる、入力のやり方に変更があるようなパターン。**	**✓数値の定義が変更される** **✓カテゴリデータのカテゴリが一つ増える** **✓入力が行われなくなって欠損になる**

→すべてのドリフト要因を網羅的に検知することは現実的ではない。モデル精度をしっかりモニタリング・管理するのが得策

継続的なモデル管理

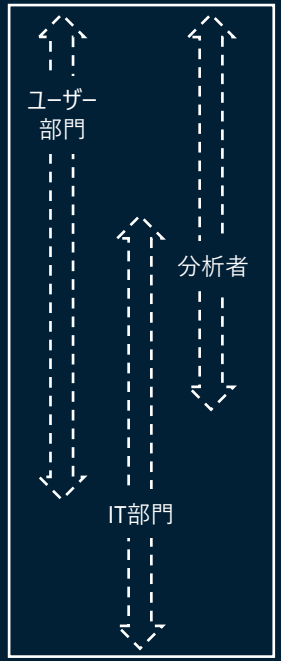
ModelOps ~アナリティクス・ライフサイクル

AI/Analyticsモデルのライフサイクル。ライフサイクルは、分析者・部門によってのみ実行されるのはなく、分析者・IT部門・ビジネスユーザー部門間での役割分担によって実現する。



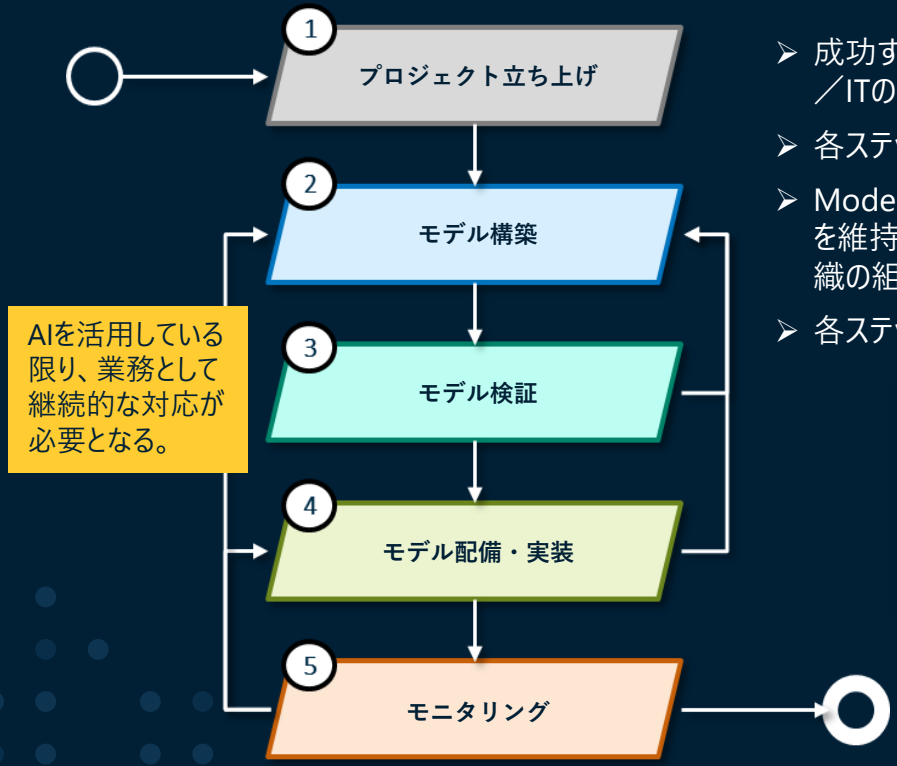
モデル管理の要点

プロセス整備が必要な観点

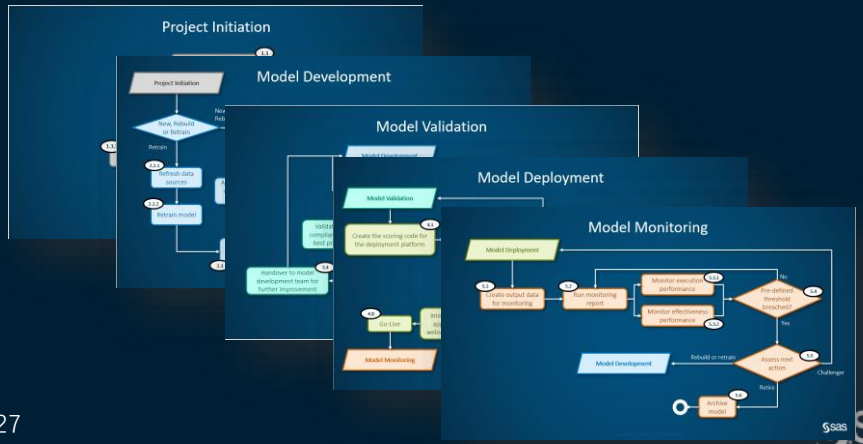
プロセス整備の観点	概要	現状はどうなっているか？	役割分担は？
モデルのデプロイ	構築・更新した機械学習モデルを本番環境上でシステムから呼び出せるようにするための一連のプロセス。	• 更新したモデルの実装にどれくらいの時間を有するか？	
モデルのモニタリング	**モデルのパフォーマンスの変化・低下を検知できるようにモデルの"継続的な"監視を行うプロセス。**	• モデル精度監視が出来ているか？ • 定期的な精度評価が可能なプロセス・仕組があるか？	
モデル管理	**モデルを管理、保存。モデルを再現可能とする仕組み及びプロセス。**	• 過去モデルの再現が可能か？1年前のモデルにデグレードできるか？	
モデルガバナンス	**ログデータの取得、モデルの解釈性・説明性についてのチェックを行うプロセス。**	• モデル運用上のログは取れているか？ • 構築モデルの解釈・説明についてドキュメント化されているか？	

AIプロジェクト立ち上げ

プロジェクト初期からModelOpsを考慮した検討が必要



- 成功するAI活用プロジェクトではプロジェクト初期からビジネスユーザ／分析者／ITの連携が必須
- 各ステップでの3者の役割を定義し、対応プロセスの定義が必要
- ModelOpsは、1回のプロジェクトではなく、AIを活用する限り、継続的に体制を維持し業務として対応することが必須。ModelOpsを考慮した全社的な組織の組織の見直しも検討が必要
- 各ステップ毎の業務フローを設計（弊社サンプル）



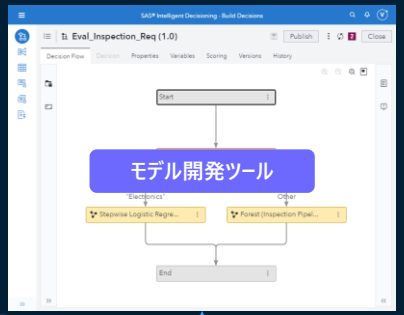
AIプロジェクト立ち上げ

ModelOpsの実行に必要なシステム・ツールの検討

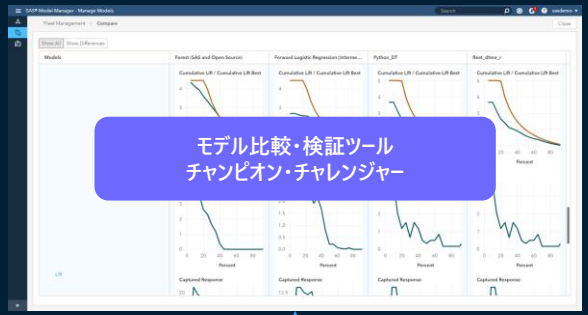
- ModelOps全体で様々なツール・技術が利用可能
- 業務プロセス設計と同時にシステムプロセスの設計も必須

プロジェクト立ち上げ

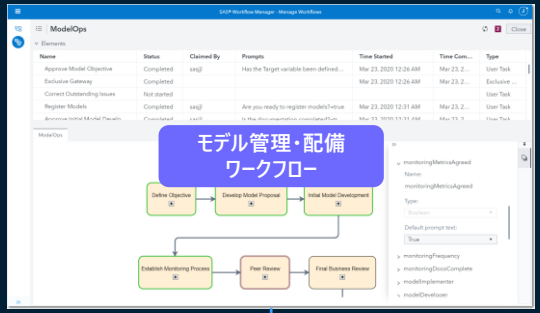
モデル構築



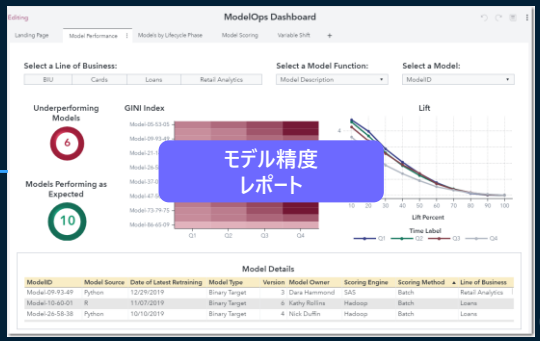
モデル検証



モデル配備・実装



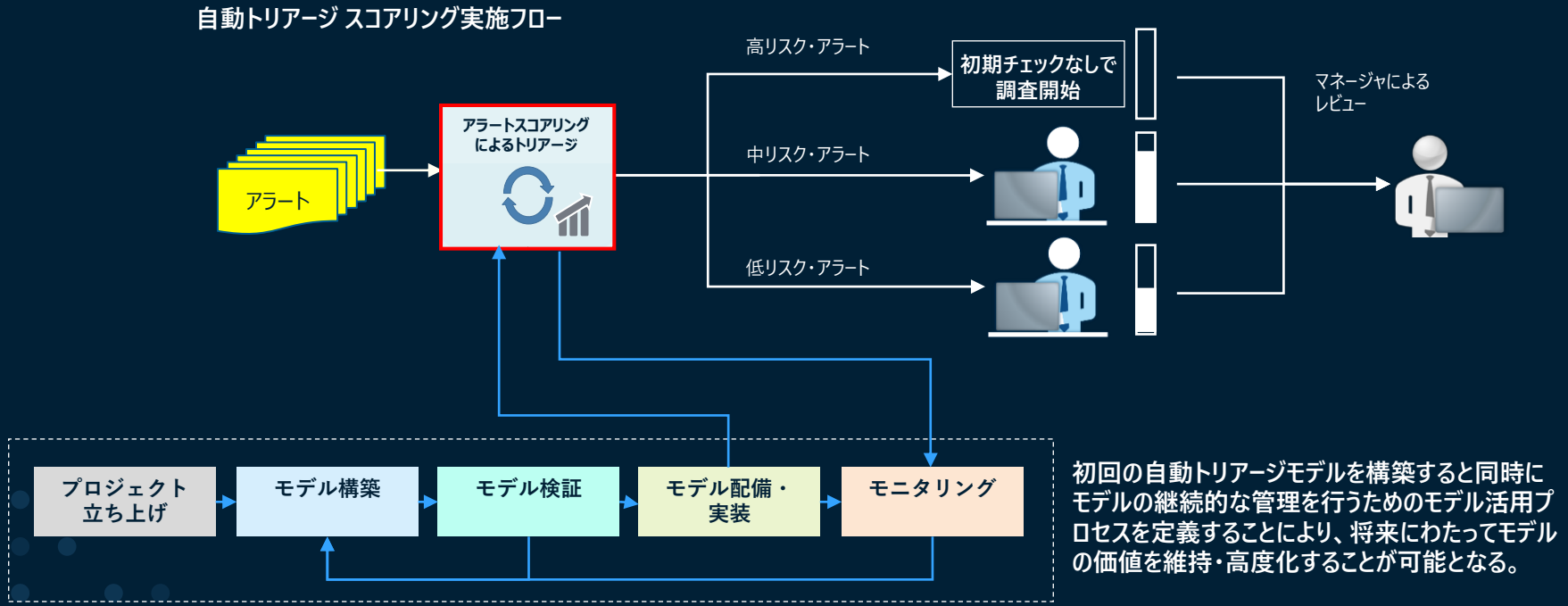
モニタリング



単一ツールでカバーすることが最も効率的ではあるが、既存の分析者が利用している分析ツール、IT部門が利用しているコード管理ツール等を含めた検討が必要

AI活用におけるModelOpsの実現

アラート・トリアージによる業務効率化



初回の自動トリアージモデルを構築すると同時にモデルの継続的な管理を行うためのモデル活用プロセスを定義することにより、将来にわたってモデルの価値を維持・高度化することが可能となる。

本日の結論

“管理なくしてAIなし”

SAS リンク集

- SASの銀行向けソリューション
  - https://www.sas.com/ja_jp/industry/banking.html
- 銀行向けリスク管理ソリューション～ガバナンスとコンプライアンス～
  - https://www.sas.com/ja_jp/solutions/risk-management.html#ガバナンスとコンプライアンス
- デモリクエスト
  - https://www.sas.com/ja_jp/software/how-to-buy/request-price-quote.html
- 本講演についてのお問い合わせ
  - JPNSASInfo@sas.com

sas.com

金融犯罪の不正取引検知へのAI活用

株式会社ラック
金融犯罪対策センター
センター長 小森 美武

LAC
株式会社ラック

Agenda

1. 金融犯罪対策センター（FC3）紹介
2. AIが対象とする金融犯罪と犯罪手口
3. AIによる金融犯罪の不正取引検知
4. 今後の展望
5. まとめ

1. 金融犯罪対策センター

FC3：Financial Clime Control Center

LAC
ともに、イキル

株式会社ラック

- 1986年に受託システムインテグレータとして創業
- 1995年からサイバーセキュリティ事業を開始
- 事業内容
  - セキュリティソリューションサービス（売上比率43%）
  - システムインテグレーションサービス（売上比率57%）
- 事業所：東京、名古屋、福岡、シンガポール
- 代表者：代表取締役社長　西本逸郎
- 売上高：436億円（グループ連結、2021年3月期）
- 従業員数：2,265名（グループ連結、2021年4月1日現在）
- 上場：東京証券取引所(ジャスダック市場)、証券コード：3857

JSOC JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

LAC Security Academy

Agile Development Center

金融犯罪対策センター
FC3 : Financial Crime Control Center

Profile

【略歴】2020年 MUFG → LAC へ

【現職】LAC 金融犯罪対策センター長

【銀行職歴】

①サイバー犯罪・金融犯罪対策
（当局対応・米銀との情報連携窓口）

②リスク管理・調査・英国ロンドン等

【公職】日本サイバー犯罪対策センター
幹事（2018～2020年）

【サイバー犯罪対策】

インターネットバンキング不正送金対策

サイバー犯罪対策体制の高度化
被害手口分析・プロファイリング
各種対策の立案・検討

【金融犯罪対策】

ATM不正取引対策
決済連携セキュリティ

【アプリのレビュー】

口座開設・諸届・Mable・コインの
本人認証セキュリティ

金融犯罪対策センター

FC3: Financial Crime Control Center

「金融犯罪対策の駆け込み寺」
として金融サービスの提供者を支援

金融犯罪の抑止に向けた、防御・検知・対策をサポート
安心・安全な金融サービス環境の実現に貢献

私たちは、
金融犯罪被害をゼロにしたい！

ラックのサイバー
セキュリティ技術

巧妙化が進む
犯罪手口への
最適な対策を提供

金融機関
の実務知見

金融犯罪対策センター 活動内容

金融犯罪セキュリティ対策ご支援

- デジタル金融サービスを、顧客保護の観点で分析・評価。リスクを指摘＆対策をアドバイス
- 不正防止に有効な「認証高度化」や「ソリューション設計方法」の提示（下記①～③）
  - ① フィッシング・なりすまし防止
  - ② ユーザ認証の高度化（多要素認証の導入など）
  - ③ リスク分析・不正検知のためのソリューションの設計に関わる支援（AI不正取引検知など）

金融犯罪対策の最先端ソリューションの研究開発

- **AI(機械学習や深層学習)を活用した最先端の「不正取引検知」手法の研究開発**
  →インターネットバンキング・ATM取引・クレジットカード等への活用を想定

金融業界・大学・サイバー犯罪対策組織との連携

- 日本サイバー犯罪対策センター（JC3）…最新の犯罪手口・対策の共有。警察庁とも間接連携
- 大学研究室… AIの最先端知見の共有・産業転用で連携
- 経営層向け講演会…講演会（金融ISAC、フィッシング対策協議会、JC3等)、金融機関の役員勉強会

2. AIが対象とする金融犯罪と犯罪手口

金融犯罪と特殊詐欺

- 金融犯罪は、「特殊詐欺」や「サイバー犯罪」など手口によって分類される
- 今回のAI活用の検証では「特殊詐欺」と呼ばれる手口に着目

特殊詐欺とは

高齢者等を様々な手段で信用させ、銀行振込やキャッシュカード詐取等の方法により、最終的に現金をだまし取る犯罪

特殊詐欺の分類

オレオレ詐欺	金融商品詐欺
預貯金詐欺	キャッシュカード詐欺盗
架空料金請求詐欺	交際あっせん詐欺
還付金詐欺	ギャンブル詐欺
融資保証金詐欺	その他の特殊詐欺

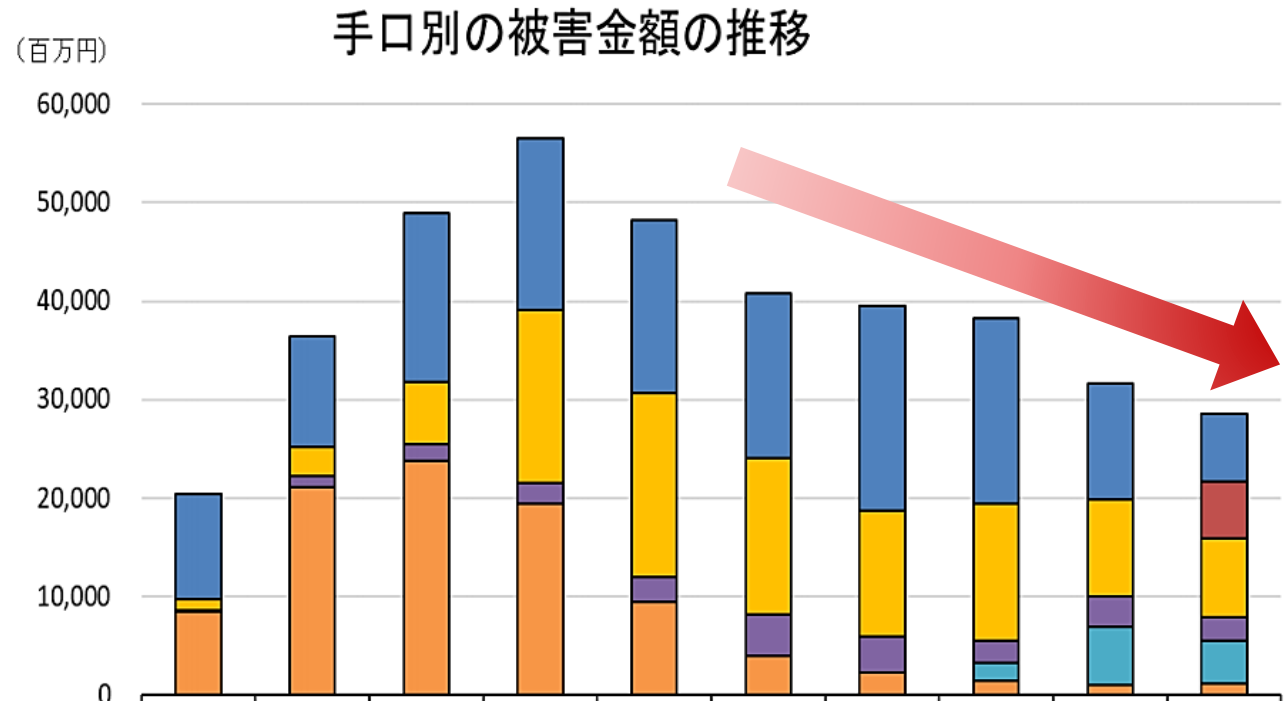
令和2年における
年間の特殊詐欺被害額

285.2億円

警察庁公表

警察庁・SOS47 特殊詐欺対策ページより引用
https://www.npa.go.jp/publications/statistics/sousa/sagi.html

特殊詐欺の被害



	H23	H24	H25	H26	H27	H28	H29	H30	R1	R2
合計	20,404	36,436	48,949	56,551	48,198	40,766	39,475	38,287	31,583	28,523
オレオレ詐欺	10,705	11,200	17,133	17,490	17,509	16,715	20,794	18,891	11,765	6,792
預貯金詐欺										5,819
架空料金請求詐欺	1,038	3,010	6,339	17,581	18,753	15,826	12,766	13,840	9,859	7,976
還付金詐欺	254	1,128	1,688	1,992	2,546	4,260	3,585	2,251	3,010	2,492
キャッシュカード詐欺盗								1,892	5,909	4,264
上記以外	8,407	21,098	23,790	19,487	9,390	3,965	2,329	1,413	1,040	1,181

警察等の対策によって
オレオレ詐欺が急減

犯罪者の収入源が縮小

新たな手口にシフト

預貯金詐欺
還付金詐欺
キャッシュカード詐欺盗

ATMの不正出金について

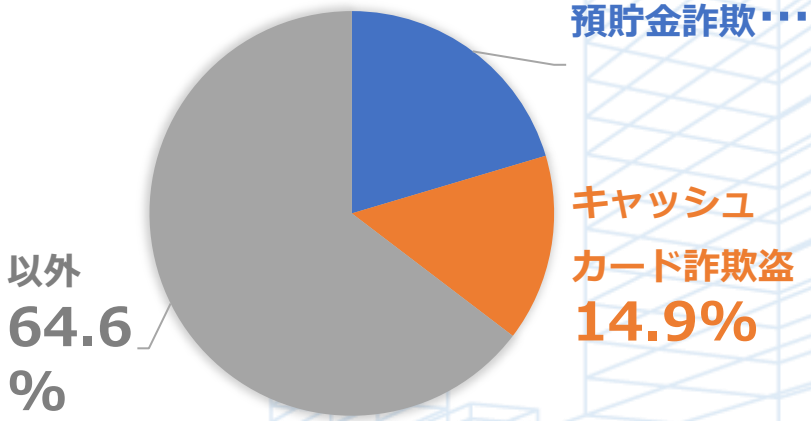
最近では高齢者からキャッシュカードを騙し取ったり、盗み取ったりしてATMで不正出金を行う「預貯金詐欺」、「キャッシュカード詐欺盗」の手口が増加、特殊詐欺被害全体の1／3を占める。

犯行の手口

高齢者宅を訪問し
カード・暗証番号を詐取・窃取

犯罪者がATMで
不正出金

特殊詐欺被害額の内訳（令和2年）



預貯金詐欺	親族、警察官、銀行協会職員等を装い、あなたの口座が犯罪に利用されており、キャッシュカードの交換手続きが必要であるなどの名目で、キャッシュカード、クレジットカード、預貯金通帳等をだまし取る（脅し取る）ものをいう。
キャッシュカード詐欺盗	警察官や銀行協会、大手百貨店等の職員を装って被害者に電話をかけ、「キャッシュカードが不正に利用されている」等の名目により、キャッシュカード等を準備させた上で、隙を見るなどし、キャッシュカード等を窃取するものをいう。

ラックは三菱UFJ銀行と協働で
ATM不正出金において
AIを利用した不正取引検知の
概念実証実験（PoC）を実施

MUFG
三菱UFJ銀行

LAC

PoCの結果
AI不正取引検知モデルによる
不正取引の検知率

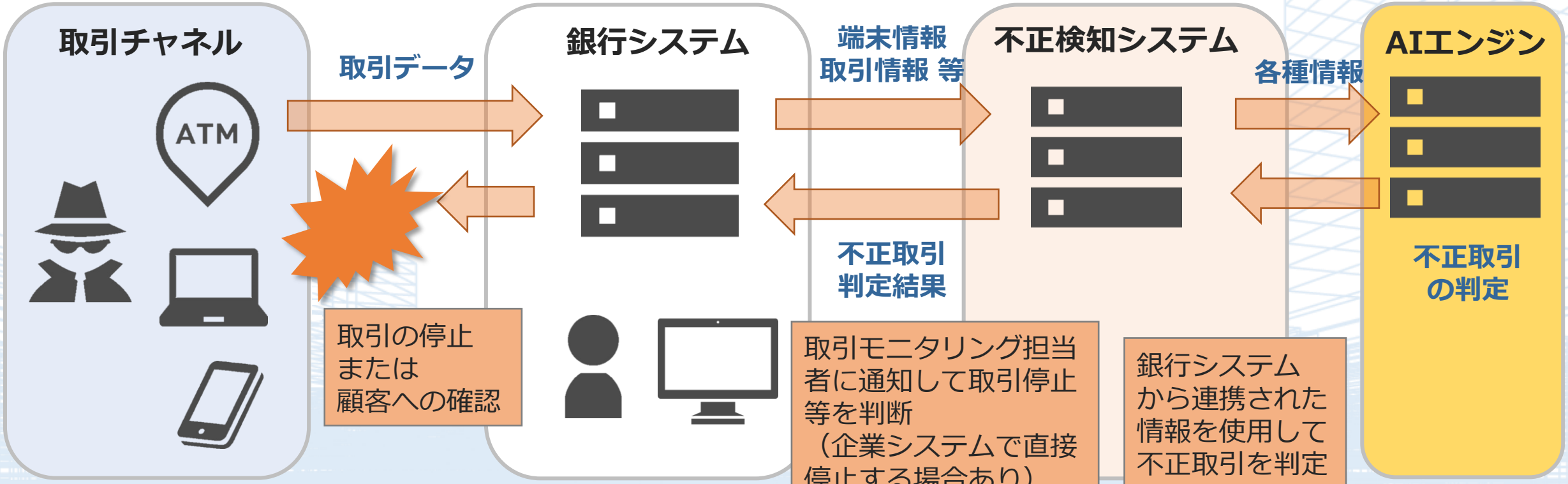
94%

※不正利用された取引のうち、AIが検知した取引件数の割合（24時間365日の時間帯でのの検証結果）

3．AIによる金融犯罪の不正取引検知

AI不正取引検知システムの概略

- ATMやインターネットなどを使用する取引で、犯罪者による不正利用の可能性が高い取引を検知し、取引の停止等を行う仕組み
- 銀行システムに不正検知システム＆AIエンジンを接続し、取引情報を元にAIが判定した「不正取引か否か」の結果を連携する



不正検知システムに求められる要件

リアルタイム性

- 不正取引を早期に検知し、取引停止・取引確認等の対策を可能とすること（特に資金の移動を伴う取引）

高い判定精度

- 高い「検知率」 ＝ できるだけ多くの不正取引を検知する
  ⇒ **安全性の向上**
- 低い「誤検知率」 ＝ 顧客の正常な取引を誤って不正と判定する件数を減らす
  ⇒ **顧客に迷惑を掛けない・利便性を低下させない**

高い説明性

- 不正取引と判定した理由の説明を容易にできるようにすること

不正検知エンジンの比較（ルールベース vs AI）

ルールベース
複数のデータ項目の値を組み合わせたルールを作成し、ルールにヒットする取引を不正と判定する

AI(機械学習)
過去のデータを学習してモデルを構築し、AIモデルが不正を判定する

項目	ルールベース	AI（機械学習）
リアルタイム性	対応可能	対応可能
判定精度	不正取引の検知率を上げると、顧客の正しい取引を誤って検知する誤検知率も増加	**誤検知率を上げずに不正取引の検知率を上げることが可能**
説明性	ルールの内容が明確であり、判定理由の説明が可能	判定理由の説明は難しい
コスト	定期的なルールの見直しが必要（運用コスト発生）	定期的なモデルのチューニングが必要（運用コスト発生）

ラックの不正検知AIの特徴

ラックの**不正検知AIは金融犯罪対策に特化**しており、
一般的なAIエンジンと比較して以下の特徴・強みを持つ。

①金融犯罪対策のノウハウ・知見

- 金融犯罪対策センター（FC3）が持つ金融犯罪対策に対する深い知見により、
  AIの「特徴量エンジニアリング」（犯罪パターンの設定）が可能

②ラック独自のAI先端技術

- 「超不均衡データ」(不正：真正取引＝1：数万～数十万)へのアプローチが可能
- **日本初の「超不均衡データへのアプローチ」の産業転用を実現**

AI不正取引検知 概念実証実験（PoC）概要

目的・概要

- 目的　：ATM不正利用における不正検知精度の検証
- データ：ATM取引データ
  データは事前に正常な取引（正例）と不正な取引（負例）の2つで
  ラベリングされており、正例と負例の二値分類の問題となる。

金融犯罪の不正検知における難題は非常に比率が偏ったデータ(超不均衡データ)

分析環境と体制

- 環境　：AWS上に分析環境を構築（各種セキュリティ対策実施済）
- 体制　：全員がデータ分析／AIの専門家
  （日本ディープラーニング協会のE資格所有者）

PoC実施にあたっての課題と解決策

① 「超不均衡データ」に対するアプローチ

② 「特徴量エンジニアリング」（犯罪パターンの設定）

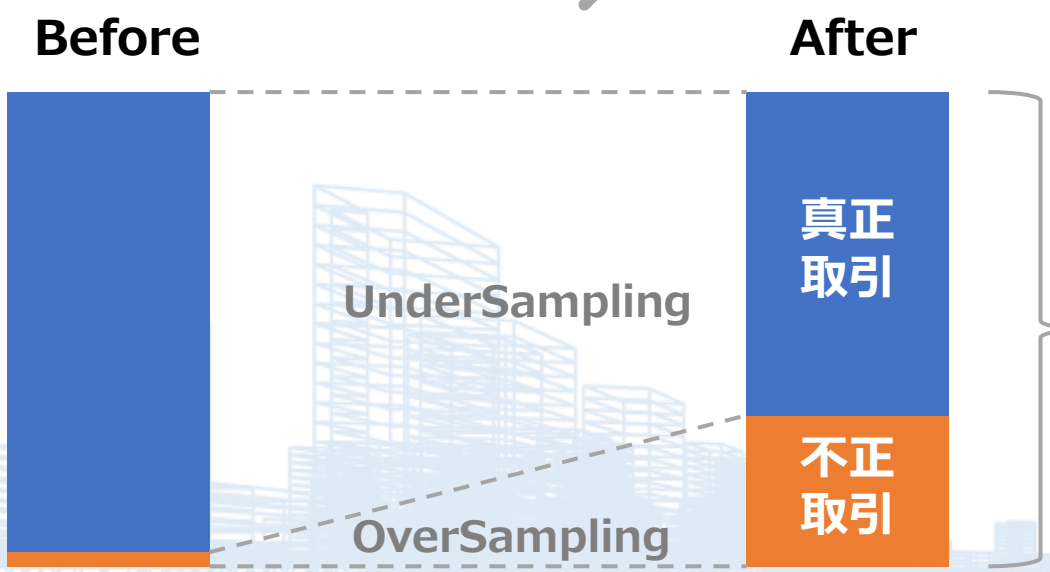
PoC実施にあたっての課題と解決策

①「不均衡データ」に対するアプローチ（データ量の調整）

- PoCデータは、不正取引が真正取引に比べて極端に少ない不均衡データ
- このため、一般的な不均衡データに対するアプローチとして、
  学習用データの比率調整を実施＝**日本初の産業転用を実現**

真正取引データを間引く(UnderSampling)

不正取引データをカサ増し(OverSampling)

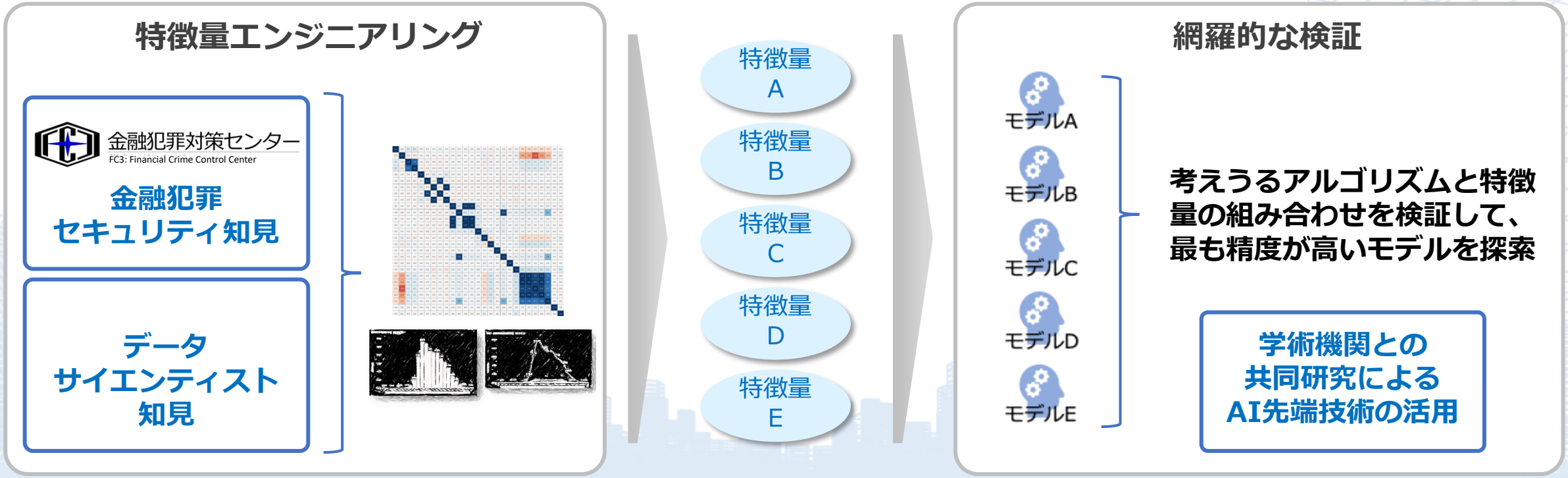


ポイント
データ特徴量が最も引き出せるようにすること

PoC実施にあたっての課題と解決策

② 「特徴量エンジニアリング」（犯罪パターンの設定）

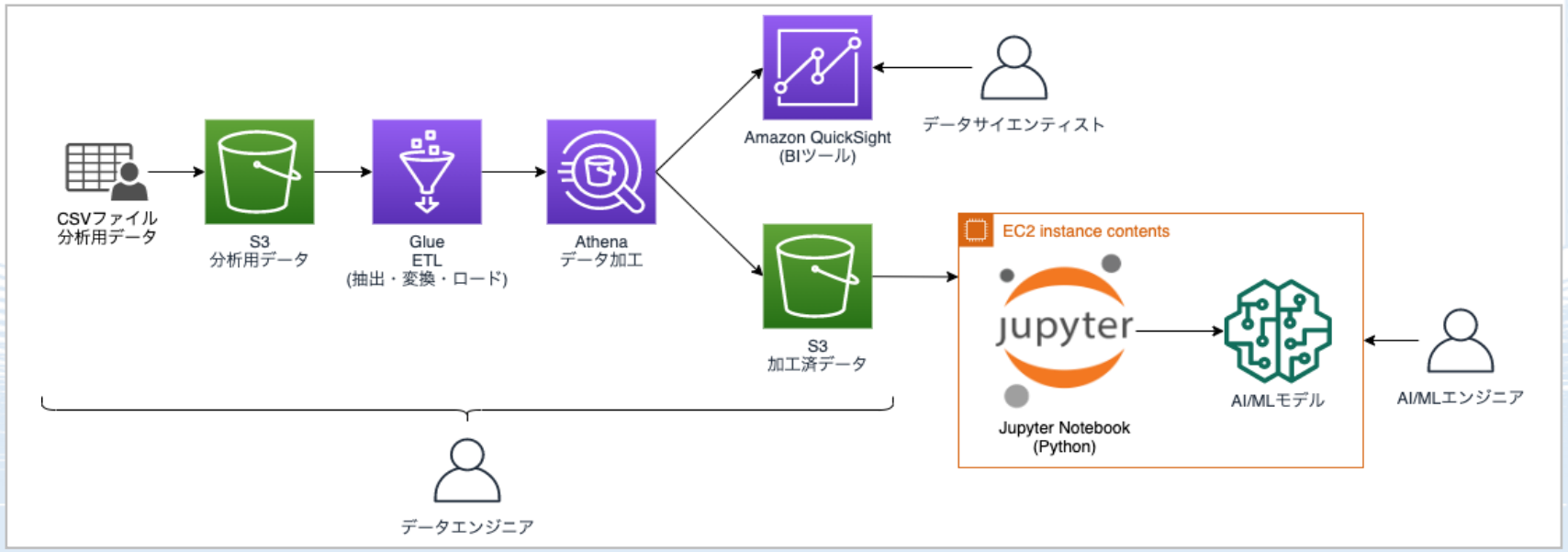
- 金融犯罪対策センターが保有している金融犯罪対策のノウハウ・知見とデータサイエンティストの知見を融合し、AIモデルの「特徴量エンジニアリング」に反映
- 学術機関との共同研究によるAI先端技術を活用し、アルゴリズムと特徴量の組み合わせによるモデルの探索を網羅的に実施



検証の進め方

- 検証は、データの加工・観察／理解からスタートし、特徴量エンジニアリング、分析を経て不正検知モデルを作成
- また、モデルの評価・改良を繰り返すことで検知精度の向上を図った
- 各工程において専門家を配置、品質の高い検証を進めた

データ加工 → データ観察 データ理解 → 特徴量 エンジニア リング → 分析方針 検討 → 不正検知 モデル作成 → 評価モデル 改良



データ加工におけるデータエンジニアの役割

データ加工 → データ観察 データ理解 → 特徴量 エンジニア リング → 分析方針 検討 → 不正検知 モデル作成 → 評価 モデル改良

データエンジニア

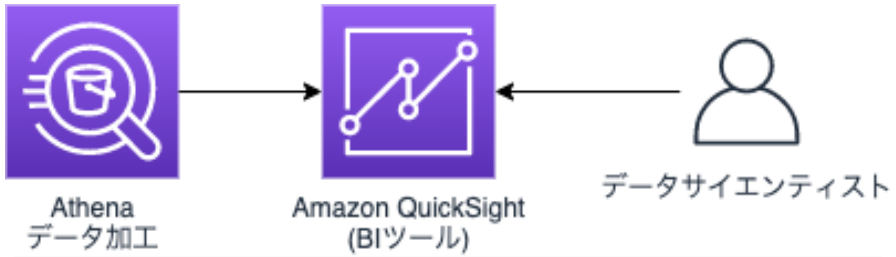
PoCデータをAWSデータ加工・分析サービスのGlue/Athenaを使って、生データを分析に必要なデータを加工

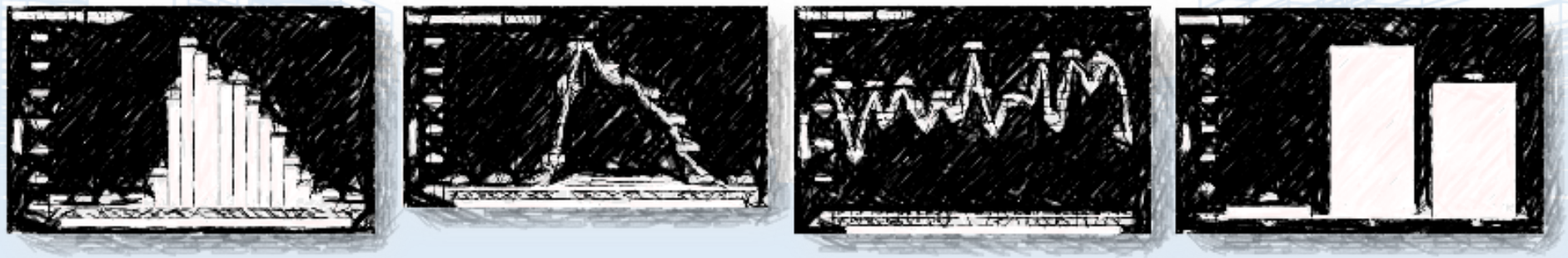
データ観察・理解におけるデータサイエンティストの役割

データ加工 → **データ観察 データ理解** → 特徴量 エンジニア リング → 分析方針 検討 → 不正検知 モデル作成 → 評価 モデル改良

データサイエンティスト

AWSのBIツールであるQuickSightを使って、
様々な切り口でデータを可視化して、不正データの特徴を見つける



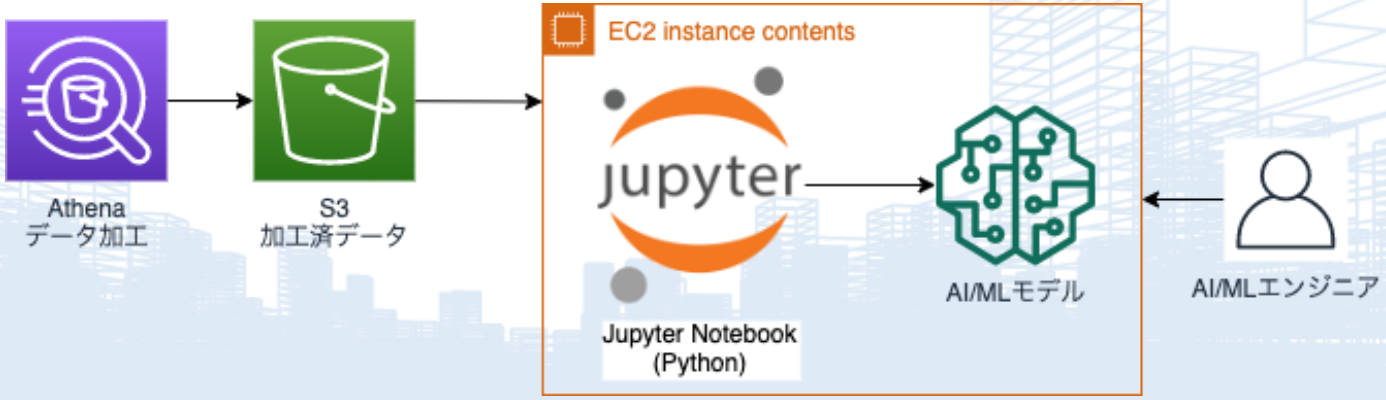


不正検知モデル作成におけるAI／MLエンジニアの役割

データ加工 → データ観察 データ理解 → 特徴量 エンジニア リング → 分析方針 検討 → 不正検知 モデル作成 → 評価 モデル改良

AI／MLエンジニア
Jupyter Notebook上でPythonを使ってデータ特徴量と各種AI/ML(機械学習)手法を組み合わせてAIモデルを評価

- 不均衡データの比率調整(Undersampling,Oversampling,SMOTEなど)
- ラックの金融犯罪に対する知見に基づき、不正取引の特徴量エンジニアリング
- 様々なAI分析手法を網羅的に試行し、検知率がもっとも高くなる特徴量とAI分析手法を検証



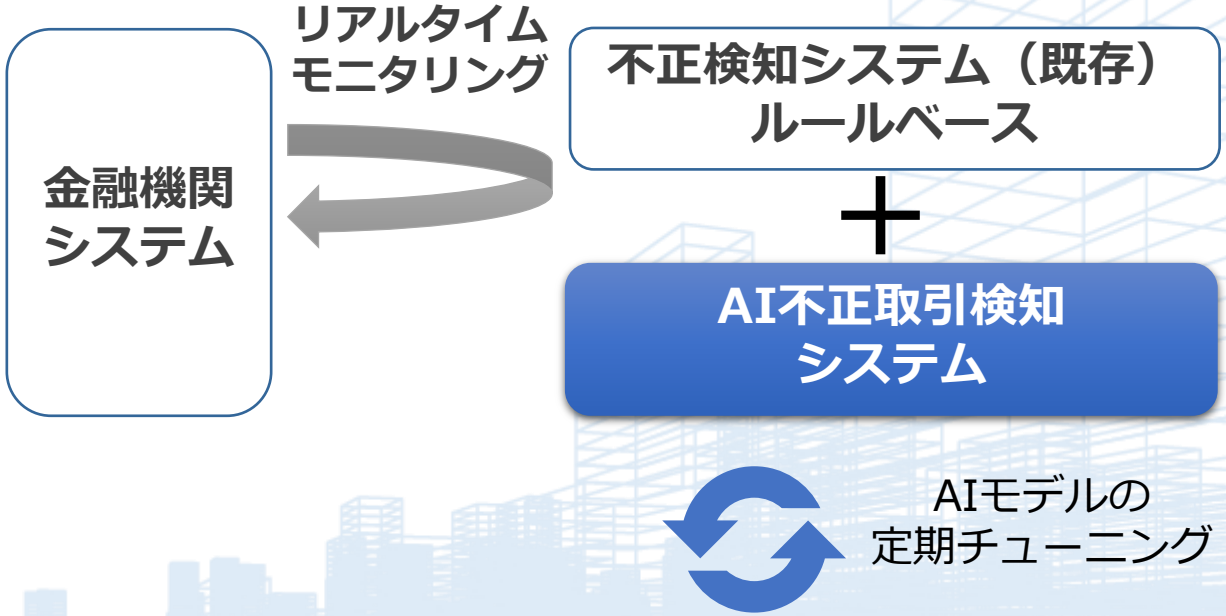
4. 今後の展開

今後の展開

- 今回のPoCでは「ATM不正出金」を対象としたが、「還付金詐欺」や「インターネットバンキング不正送金」など他の手口への応用も可能
- ラックは今後、AIモデルを「AI不正取引検知システム」として実用化を目指す

AI不正取引検知システム（単独で金融機関システムと接続）

AI不正取引検知システム（既存の不正検知システムと並存）



5. まとめ

まとめ

- ラックは、今回のAI不正取引検知のPoCで、金融機関の実用に耐える基準を満たしてATM不正利用の不正検知率94%を達成することができました。

- 今後は、インターネットバンキング不正利用の分野においても研究を進め、金融機関向け「AI不正取引検知システム」を実用化することで、特殊詐欺やサイバー犯罪など金融犯罪被害の抑止に貢献することを目指してまいります。

金融犯罪対策センター

金融犯罪対策センター

FC3: Financial Crime Control Center

私たちは、金融犯罪被害をゼロにしたい ――――
金融犯罪対策センターは、その強い思いから生まれました。

対策にお悩みの金融事業者様にとっての “駆け込み寺” に

金融サービスを利用する**「顧客保護」**の視点に立ち、金融機関や決済サービスを提供する事業者様に対して、なりすましによる不正取引などの金融犯罪に対抗するためのコンサルテーションや対策ソリューション（認証プロセスの高度化、不正取引リスクの分析・検知など）を提供して参ります。

最先端の対策ソリューションの研究・開発

サイバー犯罪の技術は日々進歩しており、次々と新しい犯行手口を編み出して、お客様資産の窃取を狙っています。これに対抗するため、主にAI技術（機械学習・深層学習）を中心として、**先端技術を活用した対策ソリューション**の研究・開発に取り組んでいます。

金融犯罪被害の抑止に貢献すべく情報発信も実施

金融犯罪対策センターの目指す究極のゴールは **“日本のサイバー金融犯罪被害をゼロにする”** ことです。日本サイバー犯罪対策センター（JC3）や学術機関など外部組織との連携や、様々な情報発信や啓発活動を通じて、このゴールに向かって取り組んで参ります。

主な提供サービスと概要

コンサルティングサービス	金融サービスや決済サービスにおいて、以下のような観点のリスク評価や改善のためのアドバイスを行います。 ✓ サイバー犯罪対策のセキュリティ評価 ✓ アカウント開設・ユーザ登録プロセスにおけるセキュリティ ✓ 顧客がサービスを利用する際の認証プロセス ✓ キャッシュレス決済など社外サービスとの連携リスク ✓ 不正取引に対する分析・検知・対応の仕組み ✓ 定期コンサルティングサービス
対策ソリューションの設計・導入支援	被害の発生を未然に防ぐためのソリューション提供や、導入に際しての技術的なサポートを提供します。 ✓ 金融犯罪対策におけるAI不正取引検知ソリューション ✓ フィッシングサイトや偽アプリへの対策 ✓ なりすましを防ぐための高度な認証ソリューション ✓ 不正な取引を検知・防止するソリューション
アドバイザリーサービス	経営層やサービス所管部門の責任者を対象としたプライベートセミナーを開催します。

ご清聴ありがとうございました

私たちは、
金融犯罪被害をゼロにしたい！

金融犯罪対策センター
FC3: Financial Crime Control Center

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。