証券業界におけるAML/CFT水準の向上
および 共通化・高度化に関するホワイトペーパー

2019.10.1

証券コンソーシアム KYC共通化ワーキンググループ

（空白のページ）

[略称一覧]

本書では以下の略称を用いている。

略称	正式名称
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism ; マネー・ローンダリング及びテロ資金供与対策
BPO	Business Process Outsourcing ; ビジネスプロセスアウトソーシング
CDD	Customer Due Diligence ; 顧客管理
CSA	Control Self Assessment ; 統制自己評価
DNFBPs	Designated Non-Financial Businesses and Professions ; 指定非金融事業者および職業専門家
EDD	Enhanced Due Diligence ; 厳格な顧客管理
FATF	Financial Action Task Force ; 金融活動作業部会
FSRBs	FATF-Style Regional Bodies ; FATF型地域体
JAFIC	Japan Financial Intelligence Center ; 警察庁刑事局組織犯罪対策部組織犯罪対策企画課犯罪収益移転防止対策室
KYC	Know Your Customer ; 顧客確認
ML/FT	Money Laundering and Financing of Terrorism ; マネー・ローンダリング及びテロ資金供与
NRA	National Risk Assessment ; 犯罪収益移転危険度調査書
PEPs	Politically Exposed Persons ; 政府等において重要な地位を占める者
RBA	Risk Based Approach : リスクベース・アプローチ
RPA	Robotic Process Automation ; ロボティック・プロセス・オートメーション
SDD	Simplified Due Diligence ; 簡素な顧客管理
WG	Working Group ; ワーキンググループ
外為法	外国為替及び外国貿易法（財務省　2017年10月1日施行）
金融庁ガイドライン	マネー・ローンダリング及びテロ資金供与対策に関するガイドライン （金融庁　2018年2月公表、2019年4月改正）
反社	反社会的勢力
犯収法	犯罪による収益の移転防止に関する法律（警察庁　2019年4月1日施行）
マネロン	マネー・ローンダリング

[用語の定義]

本書における各用語の定義は以下の通り。

用語	定義
CDD	リスク低減措置のうち、特に個々の顧客に着目し、自らが特定・評価したリスクを前提として、個々の顧客の情報や当該顧客が行う取引の内容等を調査し、調査の結果をリスク評価の結果と照らして、講ずべき低減措置を判断・実施する一連の流れ
CDD情報	口座開設手続きで確認が必要となる情報（「取引時確認」に必要な情報を除く）を指す。具体的には下記のとおり ・外国PEPs該否 [犯収法] ・共通報告基準（Common Reporting Standard / CRS）における申告に関する情報（国籍、居住国、納税者番号等）[実特法] ・内部者該否情報（上場会社等との関係、当該会社証券コードと内部者区分、インサイダー情報）[金商法] ・適合性原則に関する確認項目 [金商法]
CSA	業務の管理者と従業員が、組織のリスクマネジメントとコントロールプロセスの妥当性を評価するための手法
eKYC	H30.11.30に改正された犯収法施行規則で、新たに追加された本人特定事項の確認方法（規則6条1項1号ホ～ト）の通称
FATF勧告	FATFが策定したマネロン・テロ資金対策の国際基準
On-boarding	顧客との取引開始・口座開設に伴う一連の手続き
On-going	取引中に伴う一連の手続き
イエロー・ブラックリスト	各企業が、自社で管理をしている自社業務に悪影響を与える可能性のある個人・組織をまとめたリスト
疑わしい取引	犯収法第8条で規定される、ある取引における財産が犯罪による収益である等の疑いがある場合に、特定事業者が速やかに行政庁に届け出ることを求めている取引
オンライントレードシステム	有価証券などの金融商品をインターネットを通じて売買するために金融機関が顧客に提供するシステム
顧客リスク格付	当該顧客に該当する商品・サービス、取引形態、国・地域、属性等のリスク要素ごとに一定の評点を付すなどしたものから格付けすること
閾値/敷居値	境界となる値。その値を境に、上下で意味や条件、判定などが異なるような値のこと。 本文中では”閾値”を使用するが、金融庁ガイドラインの引用部分については原文のまま”敷居値”を使用する
実質的支配者	法人の事業活動に支配的な影響力を有すると認められる個人のこと
取引モニタリング	マネロン・テロ資金供与リスクがあると想定される取引の検知と、それに基づく特定の顧客や取引の排除を通じてリスクを低減させる手続き
取引時確認	金融機関等が、顧客との間で犯収法令7条等にある取引を行う際に必要な確認 [犯収法4条1項]。 具体的には、「本人特定事項、取引を行う目的、職業」を確認すること
ピアプロファイル（データ）	一般的な取引の態様との比較（また使用する取引データ）
非居住者	国内に住所、または、現在まで引き続き1年以上居所を有さない個人（法人については、本店または主たる事務所の所在地により内国法人または外国法人の判定が行われる）

用語	定義
ヒストリカル プロファイル（データ）	当該顧客の過去の取引との比較（また使用する取引データ）
フィルタリング	制裁対象者等の一定のリストと証券会社自身の顧客情報を照合することにより、顧客の属性に起因するマネロン・テロ資金供与リスクを低減させる手続き
本人特定事項	「取引時確認」で確認が必要な事項 [犯収法4条1項]。 具体的には、顧客の「氏名、居住及び生年月日」を指す
本人確認書類	犯収法規則7条で規定される本人特定事項を確認するための書類。 具体的には、マイナンバーカード（表面）、運転免許証、運転経歴証明書、パスポート、住民票、健康保険証などが該当する
本人確認記録	金融機関等が「取引時確認」を行った際に、作成が義務付けられている記録[犯収法6条1項]。 「本人特定事項、確認した本人確認書類の名称・発行者・記号番号・確認日、取引を行う目的・職業、外国PEPs該否」 等を記載
マイナンバー 確認書類	個人番号（マイナンバー）を確認できる以下の何れかの書類 [所得税法]。 マイナンバーカード（裏面）、通知カード、マイナンバー記載付き住民票（もしくは記載事項証明書）
リスクウェイト	顧客リスク格付けを行う際に、それぞれのリスク要素の掛け目となる係数
リスクの特定	自らが提供している商品・サービスや、提供形態、取引に係る国・地域、顧客の属性等のリスクを包括的かつ具体的に検証し、直面するマネロン・テロ資金供与リスクを特定すること
リスクの評価	特定されたマネロン・テロ資金供与リスクの自らへの影響度等を評価すること
リスクの低減	自らが直面するマネロン・テロ資金供与リスクを低減させること
リスクベース・ アプローチ	自らが直面しているリスクを適時・適切に特定・評価し、リスクに見合った低減措置を講ずること
ローリング・レビュー	定期的な顧客情報の確認・更新

目次

1

はじめに

1.1. KYC共通化WGの取組み

KYC共通化WGは、複数の証券会社ならびに証券業界に関係するテクノロジー企業で構成され、証券会社とその利用者、および規制当局の各ステークホルダーがメリットを享受できる業界横断的な金融インフラの構築をめざして2018年8月に発足した。証券会社各社の事務手続き負担の削減と、各社を利用する顧客の利便性向上を目的として、証券業界共通となるサービスの実現にむけた活動をおこなった。

WG発足当初は、口座開設手続きにおけるKYC業務の一元化と証券会社間でのKYC結果情報の共有をスコープとして、事業化を前提とした議論を実施した。しかし、On-boardingに絞っての事業化では、利用する各社の十分なコストメリットが見いだせないとの結論に至った。こうした中、FATFの第4次対日相互審査のオンサイト審査を2019年秋に控え、業界を取り巻く環境として、金融機関等は本邦当局によりAML/CFTでの実効的なリスクベース・アプローチを強く求められる状況にある。そしてこの要求水準は、国際社会におけるテロの脅威等の高まりに伴って、今後も高まることが予想されている。こうした動向を背景に、2019年4月からは検討のスコープを広げることとし、On-boarding/On-goingを区別せず、AML/CFT態勢の高度化を実現する業界共通的なサービスの立ち上げを目指して活動を継続してきた。そして今般、活動の一つの成果として、次節に示す目的でホワイトペーパーを発行することとなった。なお、WGのこれまでの活動やホワイトペーパー以外の成果の詳細は、本書Appendixにまとめている。

1.2. 本書の目的と位置づけ

本書の目的は、証券業界全体のAML/CFT水準の向上につなげるため、証券各社がAML/CFTに関して共通認識を持って関連業務をおこなえるようにすることである。そのため本書では、WGのこれまでの活動も踏まえて、証券業界に求められている事項、ならびに水準向上のための構想を整理しており、以下について取り纏めている。

1) FATFや本邦当局が金融機関等に求めるAML/CFT水準に対し、証券業界としての一つの共通的な考え方（具体的な対応例）と、これを満たすためのシステム要件（３、４章）
2) AML/CFT態勢高度化の一つの方策として、システム共同化や顧客に関するデータの集約・分析・活用をおこなう場合の論点整理と解決策の検討結果（５章）

想定する対象読者は、証券会社における全てのAML業務関係者であるが、３章以降は特にコンプライアンスやシステムの担当者が関係する内容である。

本書は、WGのプロジェクトマネージャー企業の一つである日本電気株式会社が取りまとめを担当し、WGリーダー・サブリーダー企業および各幹事企業が協力して執筆を行ったものである。ただし、本書で述べられた意見や解釈は執筆者個人に属するものであって、筆者らが所属する企業の公式見解を示すものではない。

2

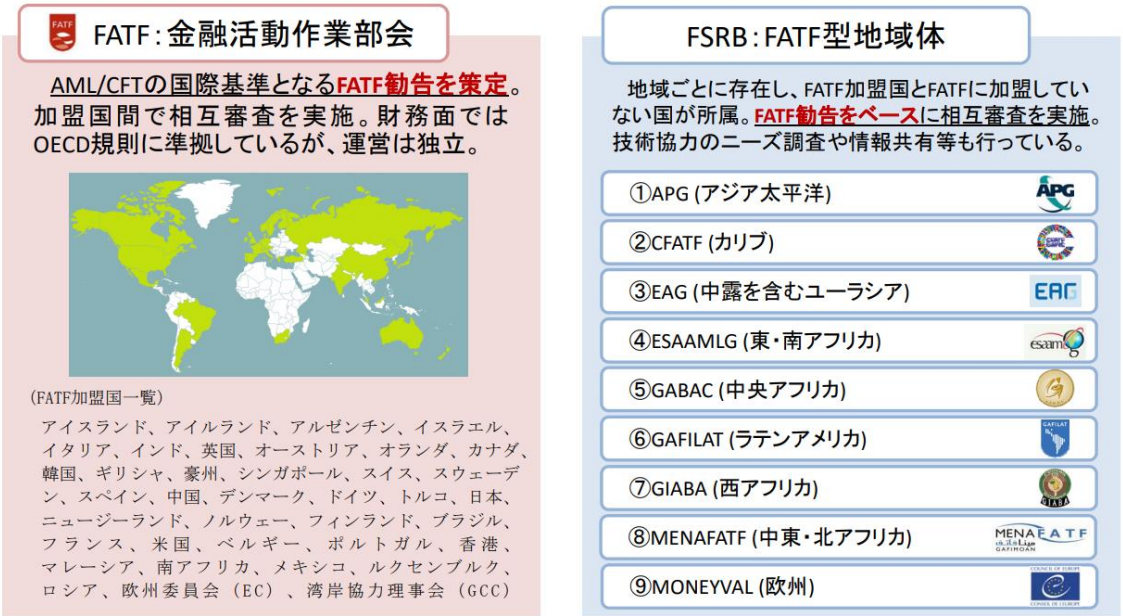
AML/CFTに関する規制動向と証券業界の取組み

2.1. AML/CFTに関する規制動向

FATFは、日本を含む加盟各国や地域、機関に対し、AML/CFTの国際基準となる「FATF勧告」の遵守を求めており、その遵守状況について、加盟国間で相互に審査を実施している（図2-1）。2008年に実施された第3次対日相互審査では、日本に対し、49項目中、重要勧告である顧客管理措置（CDD）やテロ資金供与の犯罪化を含む25項目で要改善（不備10項目、一部履行15項目）という、先進国G8の中でも低い評価が下されている[1]。日本は、フォローアップ対象国となった後もFATFから名指しで不備への迅速な対処を促されたため、指摘項目に対応する改正犯罪収益移転防止法や改正テロ資金提供処罰法の施行等をおこなうことで態勢整備を進めていった。こうした経緯の後、第4次対日相互審査が2019年に行われており、金融機関等へのインタビュー実施を含むオンサイト審査が2019年秋に実施される予定である。

図2-1：FATFの活動[2]

- マネロン・テロ資金対策の国際基準（FATF勧告）を策定し、その履行状況について相互審査を行う多国間の枠組み。（1989年設立）
- G7を含む36カ国・地域と2地域機関がFATFに加盟しており、その他9つのFATF型地域体を加えると、FATF勧告は、世界190以上の国・地域に適用。



[1] 警察庁による第3次相互審査のまとめ（P.5, 6, 7）より抜粋
<https://www.npa.go.jp/sosikihanzai/jafic/kondankai/shiryo01.pdf>（最終閲覧日：2019.9.30）

[2] 財務省国際局による関税・外国為替等審議会 外国為替等分科会 配布資料（P.1）より抜粋
<https://www.mof.go.jp/about_mof/councils/customs_foreign_exchange/sub-foreign_exchange/proceedings/material/gai20190614/05.pdf>（最終閲覧日：2019.9.30）

今回の第4次相互審査では、第3次相互審査基準のテクニカルコンプライアンス・アセスメント（技術的な適合性評価）に加えて、新たな基準としてエフェクティブネス（有効性評価）が追加されており、これら2つの観点から審査が行われる。

テクニカルコンプライアンス・アセスメントは、国の関連する法的・制度的枠組みと、管理当局の権限と手続きの制定を評価するもので、40項目の勧告（Recommendation；R）に対し、それぞれC（Compliant）、LC（Largely compliant）、PC（Partially compliant）、NC（Non-compliant）の4つの評価基準で評価される。

一方、新たな基準であるエフェクティブネスは、テクニカルコンプライアンス・アセスメントと異なり、FATF勧告の実施を評価し、定義された結果の達成度を確認するものである。最上位の目標、3つの中間的な効果、11の直接的な効果（Immediate Outcome（以下、「IO」という））により構成され（図2-2）、HE（High level of effectiveness）、SE（Substantial level of effectiveness）、ME（Moderate level of effectiveness）、LE（Low level of effectiveness）の4つの評価基準で評価される。

図2-2：エフェクティブネスの構成[3]

最上位の目標（high-level objective）：金融システム及び経済全般が資金洗浄、テロ資金供与及び拡散金融の脅威から保護され、金融部門の完全性が強化され、安心と安全に貢献すること。	
中間的な効果（intermediate Outcomes）	**直接的な効果（Immediate Outcomes）**
政策、調整及び協力が資金洗浄及びテロ資金供与のリスクを軽減している。	①資金洗浄及びテロ資金供与のリスクが理解され、適切な場合には、資金洗浄、テロ資金供与及び拡散金融との闘いに向けて行動が国内的に調整されている。
	②国際協力が情報、金融機密情報及び証拠を適切に提供するものとなり、犯罪者とその資産に対する行動を促進している。
犯罪収益及びテロを支援する資金が金融その他の部門に入り込むのが防止されており、また、当該部門によって探知され、報告されている。	③金融機関やDNFBPsがAML/CFTの義務についてそのリスクに応じて履行するよう、監督者が適切に監督し、モニターし、規制している。
	④金融機関やDNFBPsがAML/CFTの予防措置についてそのリスクに応じて的確に講じており、疑わしい取引を報告している。
	⑤法人その他の法的取極めが資金洗浄やテロ資金供与に濫用されないようになっており、その実質的受益者に関する情報が権限ある当局に障害なく利用可能となっている。
資金洗浄の脅威が探知され取り除かれており、犯罪者は制裁を受け不法収益が没収されている（deprived）。テロ資金供与の脅威が探知され取り除かれており、テロリストは資源を取り上げられ、テロ資金供与した者は制裁を受け、テロ行為の防止に寄与している。	⑥金融機密情報その他すべての関連情報が資金洗浄やテロ資金供与の犯罪捜査に権限ある当局によって適切に利用されている。
	⑦資金洗浄犯罪及び行為が捜査され、行為者が訴追され、効果的で比例的で抑止的な制裁を受けている。
	⑧犯罪収益及び手段（instrumentalities）が没収されている。
	⑨テロ資金供与犯罪及び行為が捜査され、テロ資金供与を行った者が訴追され、効果的で比例的で抑止的な制裁を受けている。
	⑩テロリスト、テロ組織及びテロ資金提供者が資金を調達し、移動させ、使用することが防止されていて、NPO部門の濫用がなされていない。
	⑪大量破壊兵器の拡散に関与する個人・団体が、関連する国連安保理決議に従って、資金を調達し、移動させ、使用することが防止されている。

[3] 警察庁平成25年懇談会第1回配布資料（P.25）より抜粋
<https://www.npa.go.jp/sosikihanzai/jafic/kondankai/shiryoh2501.pdf>（最終閲覧日：2019.9.30）

11のIOのうち4つ目のIO4では、金融機関やDNFBPsによるリスクに応じた十分な対応の実現度を評価する。IO4における主要課題の具体的な内容は以下の通り[4]。

1. 金融機関・DNFBPsは自己のML/CFのリスクおよびML/FTの義務をどの程度理解しているか。
2. 金融機関・DNFBPsは自己のリスクに見合ったリスク軽減措置をどの程度十分に適用しているか。
3. 金融機関・DNFBPsは顧客管理措置および記録保持措置（実質的支配者情報や継続的モニタリングを含む）をどの程度十分に適用しているか。
4. 金融機関・DNFBPsは、以下の強化された措置または特別の措置をどの程度十分に適用しているか。
   （a）PEPs
   （b）コルレス先銀行
   （c）新しいテクノロジー
   （d）電信送金規則
   （e）テロ資金供与関係の対象者への金融制裁
   （f）FATFが特定した高リスク国
5. 金融機関・DNFBPsは、犯罪収益と疑われるものやテロ支援を疑われる資金について、報告義務をどの程度果たしているか。内報を防ぐ現実的な方策は何か。
6. 金融機関・DNFBPsは、AML/CFTに関する義務を履行するため内部管理および手続きを（金融グループレベルも含め）どの程度きちんと適用しているか。

第4次相互審査のエフェクティブネスの国別評価結果は、2019年7月時点で図2-3の通りであり、金融機関が遵守すべきIO4に関連する項目では、いずれの国もほぼ、MEもしくはLEと低い評価となっている。

[4] 白井真人・芳賀恒人・渡邉雅之（2018）『マネー・ローンダリング反社会的勢力対策ガイドブック』第一法規.（P.43）より抜粋

図2-3：エフェクティブネスの国別評価結果[5]

Jurisdiction	Report Date	Assessment body/bodies	IO1	IO2	IO3	IO4	IO5	IO6	IO7	IO8	IO9	IO10	IO11
Albania	Dec/18	MONEYVAL	ME	ME	ME	SE	ME	SE	ME	ME	LE	ME	LE
Andorra	Sep/17	MONEYVAL	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME
Antigua & Barbuda	Jul/18	CFATF	ME	ME	LE	ME	ME	ME	LE	ME	ME	LE	LE
Armenia	Jan/16	MONEYVAL	ME	SE	ME	SE	SE	ME	LE	LE	SE	SE	SE
Australia	Apr/15	FATF/APG	SE	HE	ME	ME	ME	SE	ME	ME	SE	ME	SE
Austria	Sep/16	FATF	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE
Bahamas	Aug/17	CFATF	LE	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE
Bahrain	Sep/18	FATF/MENAFATF	ME	SE	SE	ME	ME	SE	ME	ME	ME	ME	ME
Bangladesh	Nov/16	APG	ME	SE	ME	LE	LE	ME	LE	LE	SE	ME	SE
Barbados	Feb/18	CFATF	LE	ME	ME	ME	ME	LE	LE	LE	LE	LE	LE
Belgium	Apr/15	FATF	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME
Bhutan	Oct/16	APG	LE	ME	LE	LE	LE	LE	LE	LE	ME	LE	LE
Botswana	May/17	ESAAMLG	LE	ME	LE	LE	LE	ME	LE	LE	LE	LE	LE
Cambodia	Sep/17	APG	ME	ME	LE	LE	LE	LE	LE	LE	SE	ME	LE
Canada	Sep/16	IMF/FATF/APG	SE	SE	SE	ME	LE	ME	ME	ME	SE	SE	ME
Cayman Islands	Mar/19	CFATF	ME	ME	LE	LE	ME	LE	LE	ME	LE	ME	ME
China	Apr/19	FATF/IMF/APG/EAG	SE	ME	ME	LE	LE	ME	ME	SE	SE	LE	LE
Colombia	Nov/18	GAFILAT	SE	SE	ME	ME	ME	SE	LE	SE	LE	ME	LE
Cook Islands	Sep/18	APG	SE	SE	SE	ME	SE	ME	LE	LE	ME	SE	ME
Costa Rica	Dec/15	GAFILAT	ME	SE	ME	ME	LE	ME	ME	ME	ME	LE	LE
Cuba	Dec/15	GAFILAT	ME	ME	SE	ME	SE	ME	ME	SE	SE	SE	ME
Czech Republic	Feb/19	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	SE	SE	ME	ME
Denmark	Aug/17	FATF	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE
Dominican Republic	Sep/18	GAFILAT	ME	SE	LE	ME	ME	ME	ME	ME	SE	ME	ME
Ethiopia	Jun/15	ESAAMLG/WB	LE	ME	LE	LE	ME	LE	LE	LE	LE	LE	LE
Fiji	Nov/16	APG	ME	ME	ME	ME	LE	ME	ME	LE	LE	LE	LE
Finland	Apr/19	FATF	SE	HE	LE	ME	ME	SE	SE	ME	ME	ME	ME
Ghana	Apr/18	GIABA	ME	SE	ME	LE	LE	ME	ME	LE	LE	LE	LE
Guatemala	Feb/17	CFATF/ GAFILAT	ME	SE	ME	ME	ME	SE	SE	SE	ME	ME	ME
Honduras	Jan/17	GAFILAT	ME	SE	ME	ME	LE	ME	ME	HE	SE	ME	LE
Hungary	Sep/16	MONEYVAL	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME
Iceland	Apr/18	FATF	LE	SE	LE	LE	LE	ME	ME	ME	ME	LE	LE
Indonesia	Sep/18	APG	SE	SE	ME	ME	ME	SE	ME	SE	SE	ME	LE
Ireland	Sep/17	FATF	SE	SE	SE	ME	ME	SE	ME	ME	ME	ME	SE
Isle of Man	Dec/16	MONEYVAL	SE	SE	ME	ME	ME	LE	LE	LE	ME	ME	ME
Israel	Dec/18	FATF/MONEYVAL	SE	SE	ME	ME	SE	HE	SE	HE	HE	SE	ME
Italy	Feb/16	FATF	SE	SE	ME	ME	SE	SE	SE	SE	SE	ME	SE
Jamaica	Jan/17	CFATF	ME	ME	ME	LE	LE	ME	LE	SE	LE	LE	LE
Kyrgyzstan	Sep/18	EAG	LE	ME	ME	ME	ME	ME	ME	LE	ME	ME	ME
Latvia	Jul/18	MONEYVAL	ME	SE	ME	ME	LE	ME	ME	ME	ME	ME	LE
Lithuania	Feb/19	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME
Macao, China	Dec/17	APG	ME	SE	SE	ME	SE	SE	LE	LE	ME	SE	SE
Madagascar	Sep/18	ESAAMLG/WB	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE
Malaysia	Sep/15	APG/FATF	SE	ME	SE	ME	ME	SE	ME	ME	ME	SE	ME
Mauritania	Nov/18	MENAFATF	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE
Mauritius	Jul/18	ESAAMLG	LE	ME	LE	ME	LE	ME	ME	LE	LE	LE	LE
Mexico	Jan/18	IMF/FATF/GAFILAT	SE	SE	ME	LE	ME	ME	LE	LE	ME	SE	SE
Mongolia	Sep/17	APG	LE	ME	LE	LE	LE	LE	LE	ME	LE	LE	LE
Morocco	Jun/19	MENAFATF	ME	ME	ME	ME	LE	ME	LE	ME	SE	ME	LE
Myanmar	Sep/18	APG	LE	LE	LE	LE	LE	ME	LE	LE	LE	LE	LE
Nicaragua	Oct/17	GAFILAT	ME	ME	LE	ME	LE	ME	ME	SE	ME	ME	LE
Norway	Dec/14	FATF	ME	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME
Palau	Sep/18	APG	ME	SE	ME	ME	LE	ME	ME	ME	LE	ME	LE
Panama	Jan/18	GAFILAT	LE	ME	ME	ME	LE	LE	ME	ME	ME	SE	SE
Peru	Feb/19	GAFILAT	ME	SE	ME	ME	LE	SE	LE	ME	ME	SE	SE
Portugal	Dec/17	FATF	SE	SE	ME	ME	ME	ME	SE	ME	SE	SE	SE
Samoa	Oct/15	APG	ME	SE	LE	ME	ME	LE	LE	ME	ME	ME	LE
Saudi Arabia	Sep/18	FATF/MENAFATF	SE	ME	SE	ME	ME	ME	LE	LE	SE	SE	LE
Serbia	Jun/16	MONEYVAL	ME	ME	ME	ME	ME	ME	LE	ME	ME	LE	LE
Seychelles	Sep/18	ESAAMLG	LE	LE	LE	ME	LE	LE	LE	LE	LE	LE	LE
Singapore	Sep/16	FATF/APG	SE	SE	ME	ME	ME	SE	ME	ME	LE	ME	SE
Slovenia	Aug/17	MONEYVAL	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME
Spain	Dec/14	FATF	SE	SE	SE	ME	SE	HE	SE	SE	SE	ME	ME
Sri Lanka	Oct/15	APG	ME	LE	LE	LE	LE	LE	LE	LE	SE	LE	LE
Sweden	Apr/17	FATF	ME	HE	ME	ME	ME	ME	SE	SE	SE	ME	SE
Switzerland	Dec/16	FATF	SE	ME	ME	ME	ME	SE	SE	SE	SE	SE	SE
Tajikistan	Dec/18	EAG	SE	SE	ME	ME	ME	ME	LE	ME	SE	ME	LE
Thailand	Dec/17	APG	SE	SE	ME	LE	LE	SE	ME	SE	ME	ME	LE
Trinidad and Tobago	Jun/16	CFATF	ME	ME	ME	ME	ME	ME	LE	LE	LE	LE	LE
Tunisia	Jun/16	MENAFATF/ WB	ME	ME	LE	LE	LE	ME	ME	ME	LE	LE	LE
Uganda	Sep/16	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE
Ukraine	Jan/18	MONEYVAL	SE	ME	ME	ME	ME	SE	LE	ME	ME	ME	ME
United Kingdom	Dec/18	FATF	HE	SE	ME	ME	SE	ME	SE	SE	HE	HE	HE
United States	Dec/16	FATF/APG	SE	SE	ME	ME	LE	SE	SE	HE	HE	HE	HE
Vanuatu	Oct/15	APG	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE	LE
Zambia	Jun/19	ESAAMLG	ME	ME	ME	ME	LE	ME	ME	ME	ME	ME	LE
Zimbabwe	Jan/17	ESAAMLG	LE	LE	LE	LE	LE	LE	LE	LE	ME	ME	LE

[5] FATF Consolidated table of assessment ratingsより、2019.7.31時点までの審査結果から抜粋 <http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html>（最終閲覧日：2019.9.30）

例として、IO4で最低のLEと評価された中国に対しては以下の指摘がされている。[6]

- 金融機関は、資金洗浄・テロ資金供与対策上の義務について十分理解しているが、リスクについては十分な理解が進んでいない。リスクを軽減するために実施される措置は、概して、異なるリスク状況に見合ったものではない。
- CDDの最も重大な欠陥は、実質的支配者と継続的なデューディリジェンスの要件の非効率な実装に関連している。一部の金融機関では、取引が顧客のプロファイルに沿っているかどうかの評価に焦点を当てていない。いくつかの銀行を含む一部の金融機関は、CDDが不完全と判断された場合、組織的に取引を謝絶していない。
- オンライン融資機関は、AML/CFTの枠組みの対象となっておらず、マネロン/テロ資金供与のリスクに対する理解が進んでおらず、効果的な予防措置を講じていない。
- 金融機関のリスク評価の頑健性は、金融機関をリスクにさらす実際の脅威と対応する脆弱性を評価に反映することを確保するために、強化されるべきである。実際の脅威のより良い検出を確実にするために、継続的なデューディリジェンスが強化されるべきである。

また、下から二番目のMEと評価されたアメリカに対して、以下の指摘がされている。[7]

- 米国の金融セクターは巨大かつ複雑で、多くの金融機関が関与している。対象機関、特に銀行、証券セクター及びマネーサービス事業は、マネロン/テロ資金供与の脆弱性及び義務に対する理解を深めており、これらの脆弱性を理解、評価及び緩和するための（非常に洗練された）システム及び手続を整備している。投資顧問業者（IA）は、銀行秘密法の義務の直接の対象ではない。しかし、一部のIAは、銀行、銀行持株会社およびブローカー・ディーラーとの提携を通じて間接的にカバーされており、グループ全体でAMLルールを実施したり、アウトソーシング契約を結んだりしている。残りのセクターをカバーしていないことは、米国当局によって特定された重大な脆弱性である。
- 銀行やブローカー・ディーラーなどの金融機関は、リスク管理努力の一環として実質的支配者を特定するための措置を講じているようであるが、実質的支配者に関する義務の欠如は依然として規制の枠組みにおける大きなギャップである。
- 情報交換は活発に行われており、当局と金融セクター間、および金融機関間の米国愛国者法によって促進されている。これは米国の制度の重要な特徴である。

---

[6] FATFによる第4次対中国相互審査結果（P.113, 114）より抜粋および翻訳 <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-China-2019.pdf>（最終閲覧日：2019.9.30）

[7] FATFによる第4次対アメリカ相互審査結果（P.117, 118）より抜粋および翻訳 <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf>（最終閲覧日：2019.9.30）

このように、低評価の要素として不十分なリスク評価および不完全なCDD等が言及されており、第4次対日相互審査においても、同様の指摘がなされる可能性がある。仮に今回の審査で再度低評価となった場合、他国による日本企業との取引基準が厳格化され国際取引に支障を来たす等の恐れもあることから、業界全体でのAML/CFT水準の底上げ、および高度化に取り組んでいくことが求められている。

2.2. 証券業界に求められるAML/CFTの取組み

近年、資金洗浄やテロ資金供与に代表される金融機能を利用した不正行為等の犯罪は急増傾向にあり、証券会社を含む金融機関における重要な経営課題となっている。日本におけるAML/CFTは、犯収法や外為法の法令において基本的事項が規定されており、金融商品取引業者は犯収法上の「特定事業者」、外為法上の「金融機関等」に該当することから、これら法令の規定をその適用関係に応じて遵守する必要がある。

さらに、国際社会がテロ等の脅威に直面する中で、AML/CFTの不備を契機として外国当局より巨額の制裁金を課される事例や、取引相手である海外の金融機関等からコルレス契約の解消を求められる事例が生じるなど、AML/CFTへの目線は急速に厳しさを増している。そのような中で、2019年10月には、AML/CFTの国際協調を推進する政府間組織であるFATFによる第4次対日相互審査が実施予定であることから、本邦当局においても金融商品取引業者へAML/CFTの強化を求める機運がより一層高まっている。

こうした背景を踏まえて、各証券会社においては、AML/CFTの現時点での対応状況と金融庁等の観点から求められる水準のギャップを分析し（ギャップ分析）、改善のポイントを明らかにした上で、AML/CFTに関する組織態勢の整備、方針・規程等の社内文書の策定、ロードマップ策定等の実効性のあるAML/CFTに係る管理態勢を構築・維持していく必要がある。

AML/CFTに係る管理態勢の構築にあたっては、本邦当局は「リスクベース・アプローチ」を最重要視している。リスクベース・アプローチとは、自らが直面しているリスクを適時・適切に特定・評価し、リスクに見合った低減措置を講ずることであり、FATFの勧告等においても中心的な事項を占めているため、当然に実施していくべきミニマム・スタンダードと考えられる。したがって、各金融商品取引業者においても、その取り扱う商品・サービス、取引形態、国・地域、顧客属性等を全社的に把握してML/FTリスクを特定・評価しつつ、自らを取り巻く事業環境・経営戦略、リスクの許容度も踏まえたうえで、当該リスクに見合った低減措置を講ずることが求められる。

さらに、時々刻々と変化する国際情勢や、これに呼応して進化する他の金融機関等の対応等を踏まえて機動的にリスクに見合った措置を講ずるには、個別の問題事象への対応のみにとどまらず、フォワード・ルッキングに、態勢面の見直しの必要性も含めて幅広い検証を行い、経営陣の関与・理解の下、組織全体として実効的な管理態勢の構築を行うことが肝要である。

これら一連のAML/CFTに関する取組みの策定にあたっては、国家公安委員会が公表する「犯罪収益移転危険度調査書」のほか、 金融庁ガイドライン（2018年2月）、FATFの各種ガイドライン・諸外国のプラクティス等の内容・項目等を参照することが望ましい。

2.3. 証券業界における現状の課題

金融商品取引は、多額の資金をさまざまな商品や権利に変換することができ、利益も得られる。また、財産的価値が複雑なスキームの中で不透明な形で移転し、転々流通する権利を表章する有価証券等を通じるなどして、原資の追跡が困難になることも多い。こうした特性から、金融商品取引は犯罪による収益を生成、移転し、合法資産に統合するための有効な手段となりうる。

従来、ML/FTのリスクは、資金が国外に流出すること、正規のKYCを実施した顧客以外の第三者に資金が渡ることなどが典型例として考えられていた。従って、証券業界においては、有価証券取引に伴う資金は本人の銀行口座にのみ出金可能とすることや、非居住者との取引を一定程度制限することなどで、従来、ML/FTのリスクは高くないと考える傾向があった。しかしながら、ML/FTは、①プレースメント段階（非合法収益が口座入金され金融システムにとりこまれる）、②レイヤリング段階（送金や商品への変換・換金を繰り返すことで資金出所を不明確にする）、③インテグレーション段階（隠匿した収益を合法的に利用）などの各段階を経て行われると整理されることから、証券業務においてもその一部が実行されるなど、リスクは潜在する。この点、証券業界としては、入出金取引等に狭く限定せず、取り扱う商品・サービス、取引形態、顧客の属性、取引が行われた顧客が帰属する国・地域の情報を総合的に考慮し、部分的にでもML/FTに加担することのないよう認識することが必要である。

証券業界に共通して考えられるリスク事象として、例えば以下のような例が考えられる。

（１）仮名・借名取引などのなりすましにより、正規のKYCを実施した顧客以外が、有価証券等取引を通じて財産の増殖及び持出しを図ること

（２）何らかの手段で合理的に顧客となることで証券会社に流入した不正な資金が、市場を通じたインサイダー取引・相場操縦などの不公正取引により増殖され、持ち出されること

（３）証券化等の複雑かつ個別性の高いスキームを活用することを通じて、不適切な属性の顧客がそれを隠匿して金融取引により資金を増殖させ、持出しを図ること

（４）海外市場等での外国有価証券取引等により、資金を海外出金し、外貨資産に変換し、持出しを図ること

証券業界では、上記を参考にさらに各社の実態に応じて、個社がリスクを洗い出すことが肝要である。業界横断的なリスクの列挙とその施策の統一化は、むしろ本質的なリスクの所在への認識を鈍らせることにもつながるため、あくまで例示とし、個社での具体的分析によりリスクを認識し、リスクに応じ濃淡をつけた対策を策定するよう心がけるべきであると考える。

この点、現状での証券業界の対応状況などについて、金融庁の「マネー・ローンダリング及びテロ資金供与対策の現状と課題」（2018年8月）によれば、「全般的にはマネロン・テロ資金供与リスク管理態勢について、顧客受入時の取引時確認等を含む基本的な管理態勢の整備が定着しつつある」ものの、各業者の個別のモニタリングの中では課題が認められるケースがあると指摘されている。また、「現状としては、リスク評価書作成の取組み自体は浸透してきたものの、リスク分析の手法や深度が十分かという観点からはなお課題がある」との指摘もある。

前述のとおり、証券業界全体としてAML/CFTを高度化することが、我が国の資本市場・金融業界、ひいては国際協力に資するものと考える。証券業務固有のML/FTリスクを的確に評価し、リスクに応じた対策を策定するよう努めるものとする。

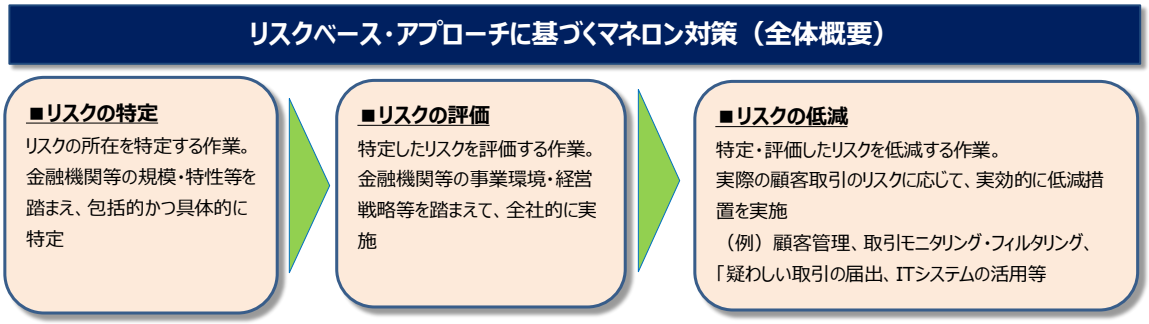
3

証券業界におけるAML/CFT

金融庁より公表されている金融庁ガイドラインでは、金融機関等に対し自らが直面しているリスクを適時・適切に特定・評価し、低減措置を講ずることが要請されている。

証券業界においても、金融庁ガイドラインに則り、各証券会社で直面しているリスクを特定・評価・低減措置を講ずるリスクベース・アプローチにより、ML/FTリスクに係る管理態勢の構築、維持を実効性をもって推進していくことが不可欠である（図3-1）。

図3-1：リスクベース・アプローチに基づくマネロン対策（全体概要）[8]



[8] 金融庁ガイドラインを基に作成

3.1. リスク特定

証券会社が各々リスクアプローチの第一段階としてML/FTリスクを特定するにあたっては、NRA（National Risk Assessment；犯罪収益移転危険度調査書）・金融庁ガイドライン・FATFの各種ガイドライン等において示されている一般的あるいは業界全体の典型例に関するリスク認識に加え、自社が提供している「商品・サービス」、「取引形態」、「国・地域」、「顧客の属性等」のカテゴリ毎に包括的かつ具体的にML/FTリスクを特定することが不可欠である。

証券業界の中でも各社のML/FTリスクは一様ではなく、自社の規模・業態等の特性に応じてリスクが異なる。例えば、取引形態が対面取引か、あるいはインターネット取引をはじめとした非対面取引かにより、リスクの状況は相違する。商品・サービスについては、リテール・ホールセールの別や国内・海外でそれぞれ取り扱う商品の個別性、現物取引・与信取引の別、現金取引の有無によりリスクの状況は相違する。顧客属性については、PEPs該当性や制裁措置対象への該当性、職業、居住地、国籍により、リスクは相違する。また、国・地域の観点では、FATFで定める高リスク国・地域とビジネス上関連するかどうかなどもリスクに影響する。

リスク特定では、社内の情報を一元的に集約し全社的な視点で分析を行うことが必要となる。AML/CFTに係る主管部門に対応を一任するのではなく、経営陣の主体的かつ積極的な関与のもと、関係する部門から必要な情報を集約し、部門毎および全社でのリスクを特定することが必要である。

リスク情報の収集については、部署ごとまたは商品ラインごとなど会社の規模・業態に合致した分類に従って行い、分類ごと、かつ「商品・サービス」、「取引形態」、「取引に係る国・地域」、「顧客の属性等」のカテゴリごとにリスクの評価や一覧ができるよう取りまとめることが望ましい。

3.2. リスク評価

証券会社は、リスク特定の後、自らのML/FTリスクについて、具体的かつ客観的な根拠に基づき評価をおこなう。

各社が提供している商品・サービスや取引形態などの特性が異なる場合、リスクの評価結果は各々相違する。

リスク評価は、特定したリスク項目について、ML/FT事案の「発生頻度」、発生した場合に自社に与える「影響度」の2要素を見積もり、一定の分類段階に基づいて評点を付すなどの手法で行う。その上で、業務分類（部署または商品ライン等）ごと、かつ「商品・サービス」、「取引チャネル」、「取引に係る国・地域」、「顧客の属性等」のカテゴリごとにマッピングまたはヒートマップ化するなどで、全社におけるリスクの所在を包括的・網羅的に認識できるよう取りまとめることが望ましい。これが、各社が定めた分類ごとの「固有リスク」の評価結果となる。

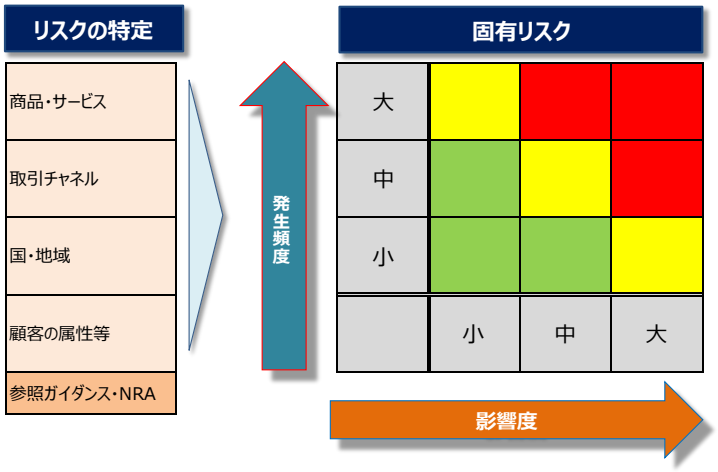
さらに、会社ですでに行われている内部統制・低減策を考慮し、評価時点での「残余リスク」の評価を行う。
リスク評価の結果は、これに基づいて個社ごとに適したAML/CFTを策定する根拠となるため、リスク対策の緊急度や経営資源の配分優先度の判断がしやすいよう、全社の状況が比較検討可能な可視化が行われることが必要である。

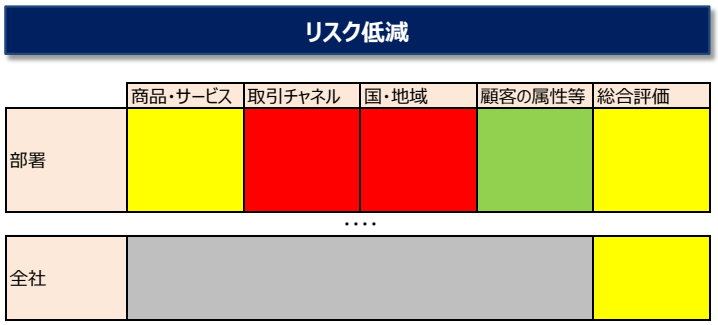
なお、リスク評価にあたっては、従来証券会社で行われている「疑わしい取引の届出実績」の分析を活用することが有用である。届出実績について対象となった顧客の属性や対象取引、発生部店ごとに分類・集計し、リスクが相対的に高い箇所を特定したり、年度ごとの傾向を把握し、固有リスクや残余リスクの評価に反映させたりするほか、直接的に低減策の検討に加えるべきである。

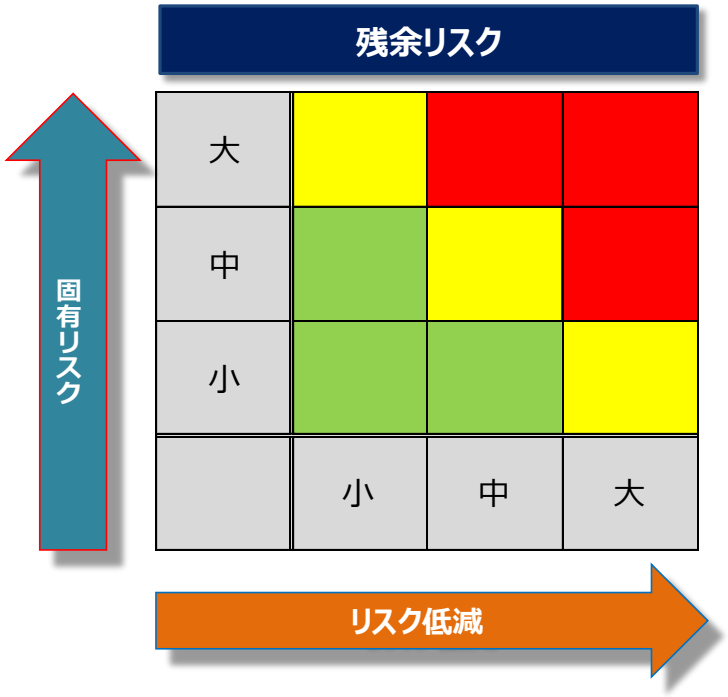
これら一連のリスク特定・評価と対応するリスク低減策等を取りまとめた「リスク評価書」は、犯収法上の「特定事業者作成書面」として活用可能なものである。リスク評価書は、これに携わった全社の部署を含めた第1線・第2線・第3線の各部署にフィードバックするほか、経営陣の承認を得ることが望ましい。

リスクの評価は定期的に見直すほか、AML/CFTに重大な影響を及ぼし得る新たな事象に備え、必要に応じ見直すことが重要である。

図3-2：リスクの特定・評価（リスク・マップ）【イメージ】





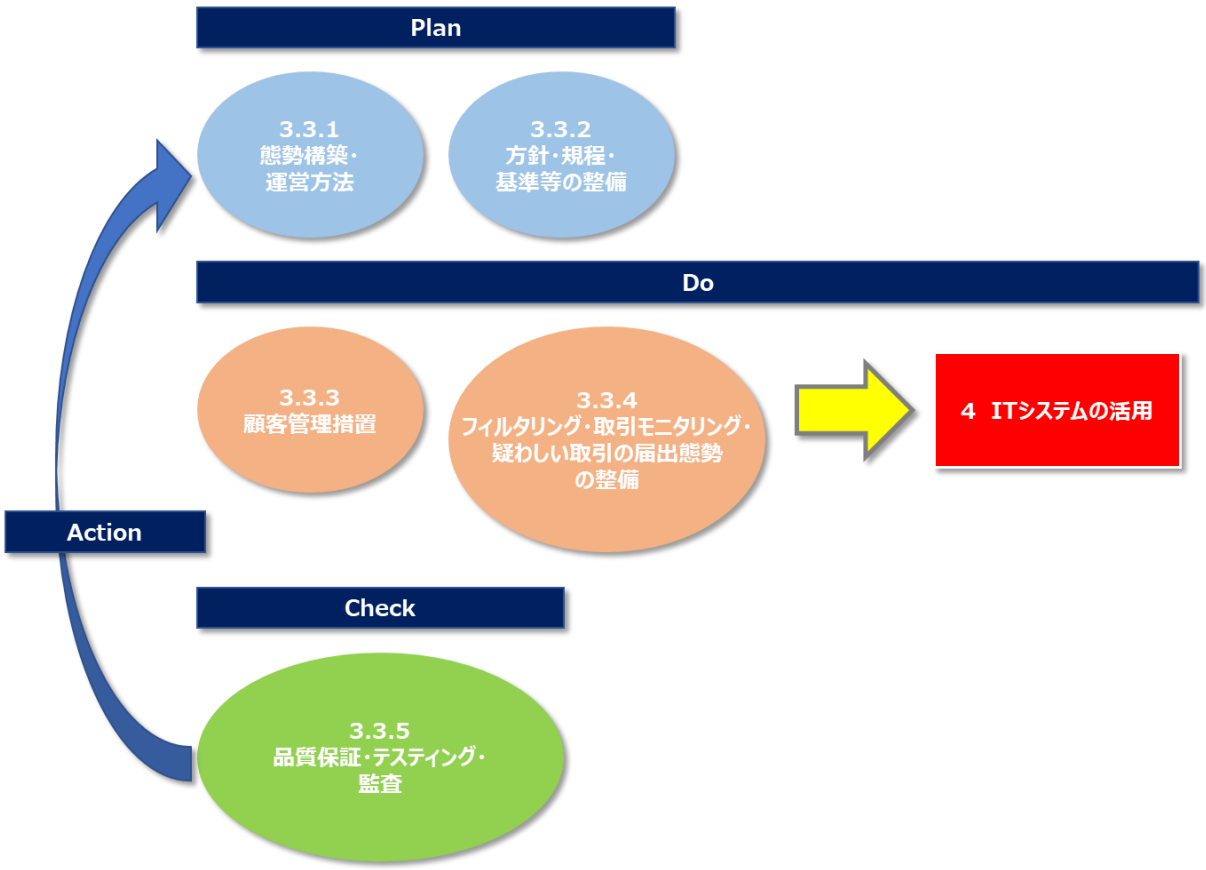


3.3. リスク低減

特定・評価されたリスクを前提としながら、リスク低減措置を具体的に定め実施する必要がある。リスク低減策においては、「態勢構築・運営方法」、「方針・規程・基準等の整備」を計画（Plan）し、「顧客管理措置」、「フィルタリング・取引モニタリング・疑わしい取引の届出態勢の整備」といったリスク低減措置を「ITシステム」も活用しながら実行（Do）し、「品質保証・テスティング・監査」によって定期的な見直し（Check）を行う。

その結果を、適宜見直しの上、次回のリスク低減措置に反映（Action）することでリスク低減措置が高度化されていく。

図3-3：リスク低減【イメージ】



3.3.1. 態勢構築・運営方法

AML/CFTの実効性の確保のためには、証券会社は取り扱う商品・サービス、取引形態、国・地域、顧客の属性等を全社的に把握してML/FTリスクを特定・評価し、自らの方針・手続・計画等を策定したうえで、当該リスクに見合った態勢を構築することが求められる。

経営陣の関与・理解

管理態勢の構築に当たっては、ML/FTリスクが経営上重大なリスクになり得るとの理解のもと、経営陣がML/FTリスクを適切に理解した上で、経営陣自身が積極的に関与し、各部門が担う役割・責任等を明確にし、トップダウンによって強固なガバナンス態勢を構築することが必要である。

三つの防衛線

証券会社においては、営業・管理・監査の各部門等が担う役割・責任を、経営陣の責任のもとで明確にして、組織的に対応を進めることが重要である。 こうした各部門等の役割・責任の明確化の観点からは、一つの方法として、各部門の担う役割等を、営業部門、コンプライアンス部門等の管理部門及び内部監査部門の機能として「三つの防衛線（three lines of defense）」の概念の下で整理することが考えられる。

顧客と直接対峙する活動を行っている営業部門や特定の商品の所管部署は、第1線としてML/FTリスクに最初に直面することからも、ML/FTリスクについて正しく理解し、自律的に営業活動・商品開発活動等に従事する。

第2線であるコンプライアンス部門やリスク管理部門等の管理部門は第1線の自律的なリスク管理に対して、独立した立場から牽制を行うと同時に、第1線を支援する役割も担う。

監査部は、第3線として経営管理態勢を客観的にモニタリングし、大局的な観点から第1線・第2線各部署や部署横断的な取組みの全体について、独立した内部監査を実施する。

グループベースの管理態勢

証券会社がグループを形成している場合には、グループ全体としてのAML/CFTに係る方針・手続・計画等を策定し、グループ全体に整合的な形で、必要に応じ傘下事業者等の業態等による違いも踏まえながら、これを実施する。

特に、海外拠点等を有する証券会社のグループにおいては、当該拠点と我が国における地理的・政治的その他の環境等の違いを踏まえつつ、グループとして一貫性のある態勢を整備することが必要となる。

具体的にはグループに共通して適用されるAML/CFTに係るグループポリシーやリスク低減プログラムを策定すること、ML/FT対策に係る内部監査計画を統一的に策定することや、グループ会社間で契約を締結し、このようなグループポリシーやリスク低減プログラムを遵守することを合意する対応も考えられる。

職員の確保、育成等

ML/FTリスクへの管理態勢の実効性は、各営業店を含む様々な部門の職員がその役割に応じた専門性・適合性等を有し、経営陣が定めた方針・手続・計画等を的確に実行することで確保されるものである。証券業界においては、こうした専門性・適合性等を有する職員を必要な役割に応じ確保・育成しながら、適切かつ継続的な研修等（関係する資格取得を含む。）を行うことにより、組織全体として、AML/CFTに係る理解を深め、専門性・適合性等を維持・向上させていくことが求められる。

こうした取り組みを通じて、第1線・第2線部署の双方について、その機能に応じたML/FTリスクに知見のある役職員を育成し、第3線の監査部門についても、さらにこうしたML/FTリスクに関する事項を監査することができる専門のナレッジの取得を促していくことが求められる。

3.3.2. 方針・規定・基準等の整備

AML/CFTの実効性の確保のためには、証券会社は、自社の方針・手続・計画等を策定したうえで、これを全社的に徹底し、有効なML/FTリスク管理態勢を構築することが求められる。

AML/CFTは経営上の重要事項であり、経営陣の積極的な関与が望まれることから、その基本方針や、顧客等の受入方針について、最上位の社内ルールとして設けることが望ましい。

その他、実務的な対応局面ごとに、必要に応じて複数の規程を設けることが想定される。例えば、実務対応上の上位規程として金融庁ガイドラインの趣旨等を汲んだ「マネー・ローンダリング及びテロ資金供与対策規程」を設けることなどが考えられる。また、すでに大半の証券会社において制定済みの「反社会的勢力対応規程」「顧客管理に関する規程」「口座開設基準」「疑わしい取引の届出基準」等との関連性を考慮しつつ、「AML/CFTの観点からの口座開設時審査・顧客フィルタリングに関するルール」「AML/CFTの観点からの取引モニタリングに関するルール」「AML/CFTの観点からの継続的顧客管理や顧客リスク格付に関するルール」などを文書化し、運用していくことが望ましい。

なお、こうした社内ルールについては、社内研修等を通じて啓蒙・教育し、全役職員が知りうる環境に掲載するなどにより周知することが望ましい。

3.3.3. 顧客管理措置

金融庁ガイドラインによれば、顧客管理とは「リスク低減措置のうち、特に個々の顧客に着目し、自らが特定・評価したリスクを前提として、個々の顧客の情報や当該顧客が行う取引の内容等を調査し、調査の結果をリスク評価の結果と照らして、講ずべき低減措置を判断・実施する一連の流れ」とされ、リスク低減措置の中でも中核的な項目と位置づけられている。

顧客等の受入に関する方針の策定

証券会社は、その規模、業態を問わず、業務の前提として顧客等に関する受入方針を定める必要がある。顧客受入方針は、AML/CFTとして自社が基本的にどのような属性の顧客を受入れるかまたは受け入れないかに関する基本方針であり、リスクが高い顧客属性の類型や対応方法の原則を取り決めたものである。

なお、証券会社におけるML/FTリスクとして、口座開設をして取引に至るいわゆる「顧客」以外にも、取引の取次ぎ先や外部委託先、金融商品仲介業者等、留意すべき先は存在する。これらについても同様に、受入等の方針を取り決めておくことが望ましい。

顧客リスク格付の導入

顧客ごとのML/FTリスクは一様ではないため、リスクが高い顧客については厳格な顧客管理を行い、リスクが低い顧客については簡素な顧客管理を行うこととするなど、顧客ごとのリスクの高低に応じてふさわしい管理措置を実施すべきである。そのためには、顧客ごとにリスクの高低を客観的に示す指標（顧客リスク格付）の導入が有効と考えられる。

顧客リスク格付は、当該顧客に該当する商品・サービス、取引形態、国・地域、属性等のリスク要素ごとに一定の評点を付すなどしたものを総合的に評価し、2段階から5段階程度の段階で付与する方法などが考えられる。

リスク要素の検討にあたっては、JAFICの「犯罪収益移転危険度調査書」をはじめ、FATF等国内外の法令・指針、ガイドライン及びプラクティスを参照の上、自社の特性を十分に考慮すべきである。

マネロン・テロ資金供与リスクの高い取引の例
・仮名・借名取引
・非対面取引
・現金取引
・反社会的勢力との取引
・非居住者との取引
・外国PEPsとの取引
・実質的支配者が不透明な法人との取引
・写真付きでない身分証を用いる顧客との取引
・要注意国・地域、マネロン・テロ資金供与対策改善継続国居住者との取引
・イラン・北朝鮮居住者との取引
・その他（金融商品仲介業者との契約等）

出所）日本証券業協会

また、顧客リスク格付にはフィルタリング及び取引モニタリングの結果を適時に反映させ、一方で顧客リスク格付に基づいてフィルタリング及び取引モニタリングの閾値を調整するなど、相互を有機的に連関させて運用することが肝要である。

顧客リスク格付の手法は例としていくつか考えられる。

（例１）リスク要素ごとのリスク値を単純合算する方式（単純合算方式）
（例２）商品・サービス、取引形態、国・地域、顧客属性といったカテゴリごとに重み付けをする
リスクウェイト方式

評価手法については、リスク要素及び評点等を定期的に見直すほか、法改正等のAML/CFTへ重大な影響を与える事象の発生時には随時見直すべきである。顧客ごとの顧客リスク格付の見直しについても、格付に応じて見直し頻度を変えるなど、顧客ごとの動態的なML/FTリスクを適時適切に反映すべきである。

顧客リスク格付に応じた顧客管理措置の実施

顧客管理（CDD）は、金融庁ガイドラインにおけるリスク低減措置の中でも中核的な項目と位置づけられている取組み事項であり、顧客ごとのリスクの高低に応じてなされるべきものとされるため、前述した顧客リスク格付に基づき、CDD、厳格な顧客管理（EDD）、簡素な顧客管理（SDD）として実施される必要がある。

顧客管理措置は、口座開設時と取引関係の継続時にそれぞれ実施方法を定めた上で行うものとする。

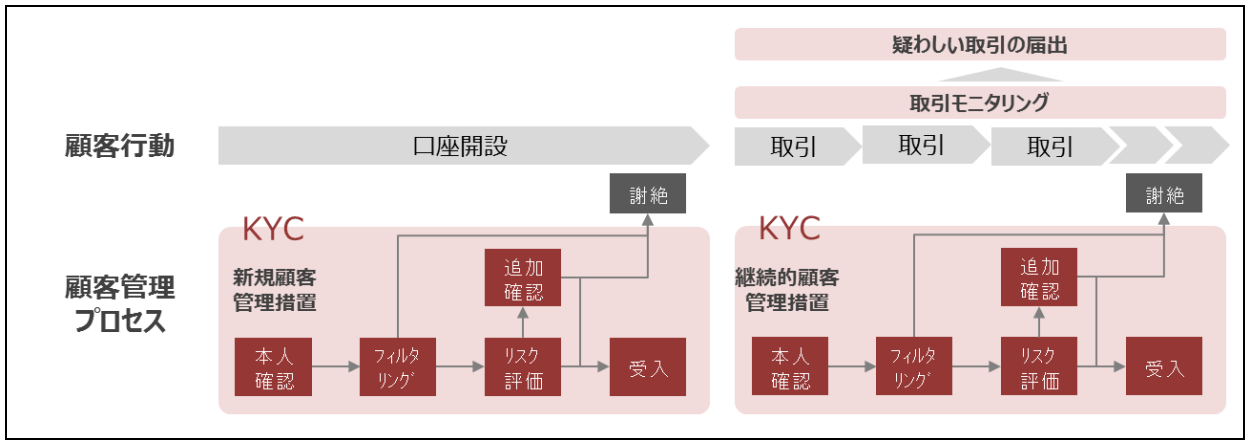
On-boarding、すなわち顧客との取引開始・口座開設に伴う一連の手続のなかで、KYCチェックはAML/CFTの観点から重要である。KYCは適切な根拠資料に基づく顧客属性の把握手続全般を指す。KYCの過程で顧客の申告等に基づく内容に疑念等がある場合には、追加で書類の提出を求めるなど、補完的手段によって審査判断を行う必要がある。

	取得すべき顧客情報の例（個人）
個人	・反社会的勢力でないことの確約に関する同意 ・氏名/マイナンバー ・国籍/住所（居住地）/連絡先 ・生年月日 ・性別 ・職業/勤務先 ・外国PEPsの該当の有無 ・投資目的（投資方針/資金の性格/運用期間） ・資産の状況（主な収入源/年収/金融資産） ・投資経験 ・取引の種類（興味のある取引） ・顧客となった動機

	取得すべき顧客情報の例（法人）
法人	・反社会的勢力でないことの確約に関する同意 ・名称/代表者名、代理人/代理人の所属部署・役職 ・業種（事業内容） ・決算期日 ・所在地/連絡先 ・実質的支配者 ・代表者及び実質的支配者の外国PEPsの該当の有無 ・投資目的（投資方針/資金の性格/運用期間） ・資産の状況（金融資産） ・投資経験 ・取引の種類（興味のある取引） ・顧客となった動機

広義のKYCには、フィルタリング、顧客リスク格付などによるリスク評価・判断が含まれる。

図3-4：KYCプロセス



出所）野村総合研究所

取引関係の継続時においては、顧客のML/FTリスクは変動しうるものであることを踏まえて、継続的な顧客管理措置として定期的な顧客情報の確認・更新（ローリング・レビュー）を実施する必要がある。実施頻度は顧客リスク格付により決定されるものとし、例えば高リスクの場合、EDDとして6ヶ月～1年に一回程度、中リスクの場合2年に一回程度、低リスクの場合、SDDとして3年～5年に一回程度などの運用が考えられる。法人の場合はさらに、代表者の変更や実質的支配者の変更がないかについても確認し、実質的支配者の変更は顧客属性の変化の端緒としてとらえ、自社が保有するフィルタリングリストと照合するなどの手続を必要に応じて実施すべく態勢を構築する。

継続的顧客管理において、顧客リスク格付に基づく厳格な顧客管理、簡素な顧客管理として実施すべき内容は以下のように例示できる。

	想定される対応
厳格な顧客管理	・統括管理者等により、顧客属性及びこれに疑念があるかどうかの確認 ・上級管理者による取引実行の承認 ・資産・収入の状況、取引の目的、職業・地位、資金調達等についてリスクに応じ追加的情報の入手 ・閾値の厳格化等の取引モニタリングの強化 ・定期的な顧客管理情報の調査頻度の増加
簡素な顧客管理	・定期的な顧客管理情報の調査頻度の緩和

出所）金融庁、日本証券業協会

3.3.4. フィルタリング・取引モニタリング・疑わしい取引の届出態勢の整備

フィルタリング

フィルタリングとは、制裁対象者等の一定のリストと証券会社自身の顧客情報を照合することにより、顧客の属性に起因するML/FTリスクを低減させる手続を言う。

財務省または金融庁から公表される制裁リストについて、通知された時及び定期的に（少なくとも年一回以上）顧客リストと照合するほか、自社の規模・業容・特性に応じて実効性のある方法で適宜実施する必要がある。海外展開するグループや、非居住者との取引を行う会社は、国内リストのみならず、海外当局等の公表するリストと照合することが望ましい。

フィルタリングリストについては制裁対象者等が適切にカバーされているかを検証し、リストの欠陥が判明または信頼性及び網羅性に対する疑義が生じた際には、フィルタリングリストの見直し、その他公知情報によるネガティブチェックなどの付加的措置を行うことが必要と考えられる。

また、既存顧客のフィルタリングの過程でリスト掲載事項に該当した場合は、速やかに取引継続可否について検討し、必要な対応を行う。併せて、速やかに当局に疑わしい取引の届出を行う。

	フィルタリングリストの一例
国内	・経済制裁措置及び対象者リスト（財務省） ・反社情報照会システム ・犯罪収益移転危険度調査書（国家公安委員会） ・外為検査ガイドライン・不備事項指摘事例集（財務省） ・外国ユーザーリスト（輸出貿易管理令）（経産省）
域外適用	・特定国籍業者リスト（米国海外資産管理局:OFAC） ・米国愛国者法 ・米国財務省金融犯罪執行機関ネットワーク ・NGOトランスペアレンシー・インターナショナル ・国内/海外外国PEPs ・その他、英国FCA、EU、世界銀行、国連安全保障理事会などのリスト

出所）野村総合研究所

また、リスクの高い顧客を的確に検知するためには、外部ベンダーの提供するネガティブニュースと顧客との照合を適宜行い、該当顧客がある場合は、ヒットしたネガティブニュースの内容に応じて、顧客リスク格付の変更措置をとるなど、実効性のある措置をとるなどの方法も考えられる。

データベースを利用しない会社については、外国PEPsの大部分を占める非居住者取引を受け付ける場合、取引時は対面で行うこととし、顧客等に申告を求める方法とインターネット等の公知情報を活用して確認する方法のいずれか、または両方を活用することで外国PEPsの該否を確認するなど、手作業により検知が可能な業務フローを構築することが望ましい。

取引モニタリング

取引モニタリングとは、ML/FTリスクがあると想定される取引の検知と、それに基づく特定の顧客や取引の排除を通じてリスクを低減させる手続のことをいい、会社ごとに一定の抽出基準や判断基準を設定し、自社にとってML/FTリスクが高い取引を適切かつ継続的に把握する。検知結果については、疑わしい取引の届出を行うとともに、個々の顧客リスク格付の精度向上のために活用する。

取引モニタリングには、手作業により検知する手続とシステムにより検知する手続がある。対面取引で営業員等が人的に判断するなどのほか、証券会社として実施している不公正取引等に関する売買審査やその他AML/CFT目的でのシステムモニタリングを通じて検知することができる。自社の規模や業容等の特性に沿った検知シナリオに基づき、口座・取引単位、顧客単位の振る舞いに着目して、疑わしい取引の疑義のある取引を含むML/FTリスクのある取引を抽出できる取引モニタリングシステムの構築が望ましい。

モニタリングのシナリオ及び閾値は、直近または過去数年分の「疑わしい取引の届出」の内容を定期的に分析するなどして適宜見直すべきであり、ITシステムを利用しない場合であってもこの方法は有用である。また、従来定めていたリスク評価及び低減措置が有効に機能しているか検証し、必要に応じて変更する上でも、過去の疑わしい取引の届出に係る分析は有効である。

取引モニタリング方法は主として以下のようなものが想定される。

想定される取引モニタリング方法の一例
・インターネット取引におけるログイン・取引実施時のアクセス元の分析
・金融商品取引業者として行っている売買審査
・金融商品取引業者として行っている定期的ななりすまし調査
・金融商品取引業者として行っている入出金及び株式等の振替のモニタリング
・マネロン・テロ資金供与対策の観点で設定したマネロン・テロ資金供与リスクのある取引シナリオによる分析

疑わしい取引の届出

営業員は取引注文を受けるに際し、顧客の属性、取引時の状況（顧客の態様、取引の内容・頻度・目的等）、自社で把握している顧客情報を総合的に勘案し、取引内容が不自然ではないかという目線で確認する。営業店の店頭における一見顧客との取引やコールセンターでの電話による受注などに際して、自社の顧客カード等に記載されたどの情報を確認すれば当該取引内容が不自然ではないかが確認できるチェックシートやFAQなどを作成して使用することが考えられる。想定外の疑わしい取引が発生した場合、直ちにマネロン等担当部署に報告がされ、担当部署から全営業店に速やかに周知される態勢を構築する必要がある。

また、疑わしい取引を的確に検知・監視・分析するために、自社のITシステムやマニュアル等を活用する態勢となっているかの確認もあわせてすべきである。

疑わしい取引の該当性を確認するにあたっては、国によるリスク評価の結果を反映した取引に係る国・地域、外国PEPsの該当性、顧客属性に照らした取引金額・回数等の取引態様その他を考慮した業務フローとなっているか確認することが考えられる。また、既存顧客との継続取引や一見取引等の取引区分の観点からも、疑わしい取引の該当性の確認・判断を適切に行うことが考えられる。

	取引区分に応じた疑わしい取引の例
既存顧客との継続取引	・取引量の急激な拡大 ・突然の代理人の設定 ・海外への転出（出国先に留意） ・不自然な売却出金 ・休眠口座における取引 ・一定期間における分割取引（見せ玉）
一見取引	・自社における取引理由が不明瞭 ・本人確認書類との不整合 ・多額の取引の申告 ・当社からの勧誘ではなく、他社から有価証券を移管し、売却のみを行い出金 ・多額の買付後、短期間で売却または他社へ移管 ・自己の投資判断ではなく、第三者からの指示による取引

出所）日本証券業協会

届出態勢については、疑わしい取引の届出の担当部署、及び疑わしい取引の疑義がある場合の対応方法等が社内に周知されており、疑わしい取引に該当またはその疑義があると認識した場合、原則即日中に担当部署に報告される態勢となっていることが求められる。

なお、疑わしい取引の届出をした顧客については、そのリスクレベルを適切に顧客リスク格付へ適切に反映し、取引の監視・制限や追加的本人確認等の措置を講ずるべきである。

3.3.5. 品質保証・テスティング・監査

社内規程や業務手順書として定めた事項が遵守されているかについて、 第1線などの該当業務・該当商品の所管部署自身がCSA等により定期的に自己評価する。

第2線は、適宜継続的に第1線での業務実施結果をモニタリングし、その到達水準が不十分な場合には指導を行うなどの業務品質維持 を行う。第2線は同様に自身の業務についてCSA等を行って業務遂行状況をチェックし、さらに定期的に業務運営状況を取締役会等の重要会議にて経営報告し、遂行すべき業務の品質を維持するとともに、相互に部署ごと及び全社的なAML/CFT管理態勢をモニタリングする。テスティング（検証）においては、AML/CFTの態勢そのものや施策の有効性について検証し、課題認識は次回のリスク評価や施策の策定に反映させる。また、テスティングの結果や課題認識は、AML/CFTに関する検証・振り返りとしてリスク管理委員会、コンプライアンス委員会、取締役会等に報告する。

第3線として独立した監査部は、必要に応じてAML/CFTに係る外部専門家を活用するなどにより、実効性のある監査を実施する。期初の監査計画等で監査部自身がリスクベース・アプローチにより監査計画を立案し、実行する。監査結果は関連部署にフィードバックするほか、取締役会に遅滞なく報告する。経営陣は課題については速やかな改善を指示し、その後の改善状況について経営報告を促す。

（空白のページ）

4

ITシステムの要件

4.1. AML/CFTにおけるITシステム

4.1.1. リスクベース・アプローチにおけるITシステムの活用

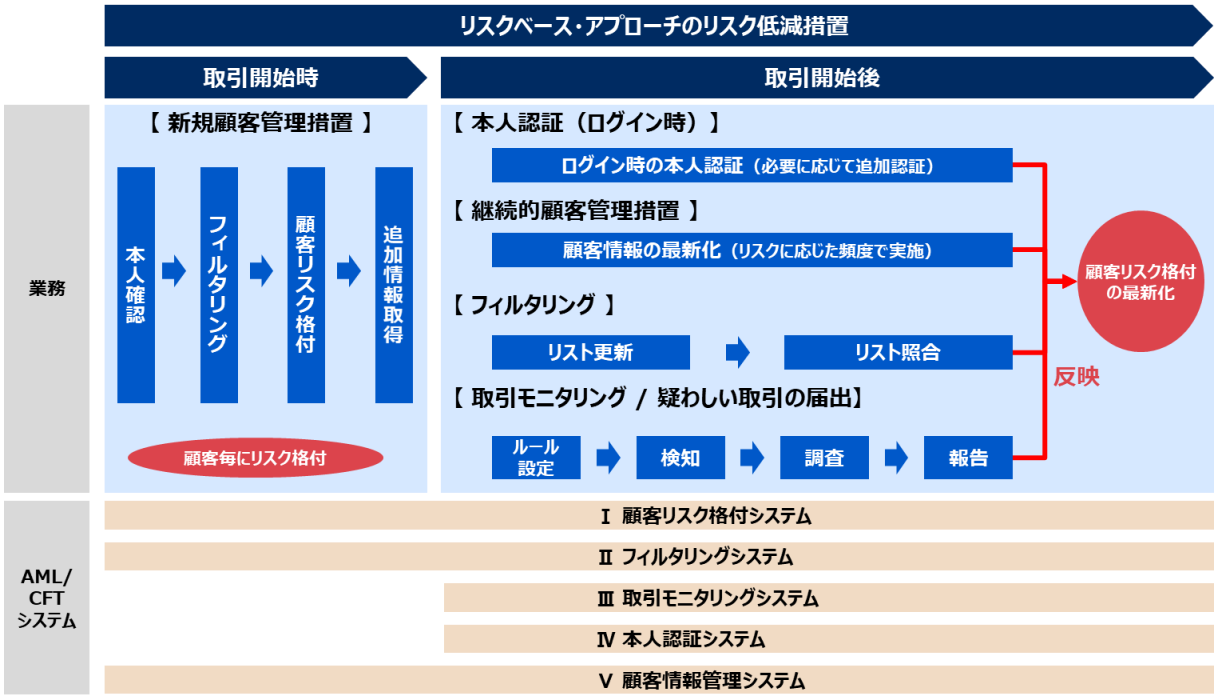
(1) ITシステムの必要性

前章までに述べた通り、AML/CFTにおけるリスクベース・アプローチとは、金融機関等が、自らのML/FTリスクを特定・評価し、これを実効的に低減するため、当該リスクに見合った対策を講ずることを指す。

リスクベース・アプローチによるAML/CFT態勢の整備にあたっては、金融庁ガイドラインにおいて、リスクベース・アプローチにおけるリスク低減措置の一つとして「ITシステム（ソフトウェアを含む。）の活用」（図4-1）が推奨されており、自らの業務規模、特性等に応じたITシステム導入の必要性や「対応が求められる事項」が列挙されている。これを受けて、多くの金融機関ではAML/CFT態勢の整備にあたり、AML/CFTシステムの活用を進めている状況にある。

AML/CFTシステムの活用において注意しなければいけないのは、単に各システムを導入すれば、AML/CFTの実効性が担保されるわけではないということである。まず、個社ごとにリスク特定・評価方針を策定したうえで、リスク低減措置にITシステムを適用することが前提となる。そして、導入後も継続的に実効性の検証を行うための仕組みを、あらかじめ計画し準備しておく必要がある。

図4-1：リスクベース・アプローチによるAML/CFT業務とITシステム



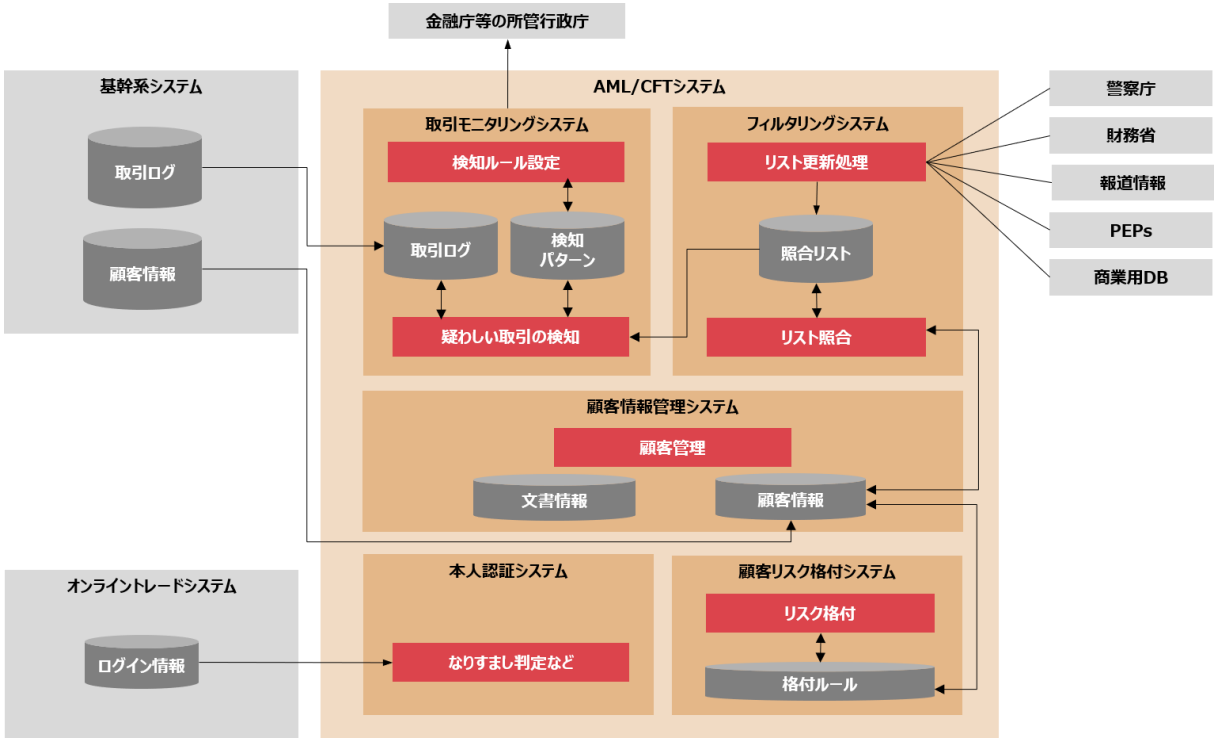
(2) 各システムの概要

図4-1で示した通り、AML/CFTシステムは、「顧客リスク格付システム」「フィルタリングシステム」「取引モニタリングシステム」「本人認証システム」「顧客情報管理システム」の5つに区分することができる。

その内、「取引モニタリングシステム」、「フィルタリングシステム」、「本人認証システム」の3つについては、証券会社の基幹系システムやオンライントレードシステム、外部システム等との連携が必要となる。

「取引モニタリングシステム」は、基幹系システムからバッチ処理等でデータを受領し、疑わしい取引の有無を分析する。「フィルタリングシステム」については、自社のフィルタリングリストの他に、警察庁の反社DBや、ダウ・ジョーンズのリスクデータベース等の商業DBと連携し、照合リストを作成することで、フィルタリング業務に利用する。また、「本人認証システム」については、オンライントレードシステム等の対顧客システムと連携し、ログイン情報を分析することで、なりすましのリスクを判定しつつ、オンラインでの本人確認を実施する（図4-2）。

図4-2：AML/CFTシステムの概要



※基幹系システム・オンライントレードシステムについては、AML/CFTシステムと連携する機能のみ記載

個々のシステムの機能と金融庁ガイドラインにおける要求事項について、表4-1～表4-5に記す。金融庁ガイドラインにおいては、ミニマム・スタンダードである「対応が求められる事項」、より堅牢なML/FTリスク管理態勢の構築に向けた提言である「対応が期待される事項」、ベスト・プラクティスを目指すにあたって参考となる「先進的な取組み事例」の3つの段階に分けて記載しているが、本書では、将来の更なる高度化要求に備えるため、記載の事項すべてを要求事項としてまとめている。

表4-1：顧客リスク格付システムの機能

機能	機能概要	金融庁ガイドラインにおける要求事項
リスク格付	商品・顧客属性情報等に基づく顧客のリスク格付を行う。 「フィルタリング」、「取引モニタリング」、「本人認証」等の結果を基に、顧客の顧客リスク格付を行う。	• 商品・サービス、取引形態、国・地域、顧客属性等についてのリスク評価の結果を総合・定量化してモデル化し、当該モデルを自社システムに組み込んで、顧客受入れ時や顧客情報変更の都度、機動的にリスク格付を付与すること 【（ⅱ）顧客管理（カスタマー・デュー・ディリジェンス：CDD）】 • 個々の顧客情報や取引情報をリアルタイムに反映するなど、リスク評価やリスク格付の結果を機動的に修正・更新できる態勢を構築すること 【（ⅵ）IT システムの活用】

表4-2：フィルタリングシステムの機能

機能	機能概要	金融庁ガイドラインにおける要求事項
リスト照合	顧客が、反社会的勢力・経済制裁対象者・PEPs等に該当していないかを、社内リスト（会社独自のイエローリスト、ブラックリスト等）・警察庁反社情報DB、および民間の外部サービス（「リフィニティブ（旧トムソン・ロイター）」・「ダウ・ジョーンズ」等） を利用し照合を行う。 ※リストについては、「3.3.4. フィルタリング・取引モニタリング・疑わしい取引の届出の整備事例」の「フィルタリングリストの一例」参照	• 送金先や輸出入品目等についての制裁リストが最新のものとなっているか検証するなど、的確な運用を図ること 【（ⅵ）IT システムの活用】 • 信頼性の高いデータベースやシステムを導入するなど、金融機関等の規模や特性等に応じた合理的な方法により、リスクが高い顧客を的確に検知する枠組みを構築すること 【（ⅱ）顧客管理（カスタマー・デュー・ディリジェンス：CDD）】

表4-3：取引モニタリングシステムの機能

機能	機能概要	金融庁ガイドラインにおける要求事項
疑わしい取引の検知（ルールベース）	疑わしい取引事例等、不正な取引に対応したルールを作成し、それに基づいた疑わしい取引の検知を行う。 ※顧客リスク格付によるリスク度に応じた閾値の設定が可能	• 自らのリスク評価を反映したシナリオ・敷居値等の抽出基準を設定するなど、自らの IT システムを取引モニタリング等のマネロン・テロ資金供与対策の有効な実施に積極的に活用すること 【（vi）IT システムの活用】 • 取引の特徴（業種・地域等）や抽出基準（シナリオ・敷居値等）別の検知件数・疑わしい取引の届出件数等について分析を行い、システム検知以外の方法で得られた情報も踏まえながら、シナリオ・敷居値等の抽出基準について改善を図ること 【（vi）IT システムの活用】
疑わしい取引の検知（プロファイルベース）	顧客や特定グループの平均的なふるまい・特性を基にプロファイルを生成し、そのプロファイルとの乖離度からリスクを特定し、疑わしい取引の検知を行う。	
ケースマネジメント	疑わしい取引の検知アラート（候補）の調査に必要な情報確認（顧客属性や取引履歴、振込先等）と調査結果管理、ならびに漏れなく調査を行うためのワークフロー管理を行う。	
疑わしい取引の届出支援	届出帳票の自動入力等により、疑わしい取引の届出の支援を行う。	
レポーティング	経営層向け報告等、各種の社内レポート作成の支援を自動入力等により行う。	

表4-4：本人認証システムの機能

機能	機能概要	金融庁ガイドラインにおける要求事項
なりすまし判定	顧客のオンライントレードシステム等へのログイン時やログイン後のふるまいを分析し、なりすましの可能性（疑い度合い）を判定する。 ※FATF高リスク国からのアクセスを検知	• 自らのリスク評価を反映したシナリオ・敷居値等の抽出基準を設定するなど、自らの IT システムを取引モニタリング等のマネロン・テロ資金供与対策の有効な実施に積極的に活用すること 【（vi）IT システムの活用】
追加の本人確認	なりすましの疑いのある場合に、追加の認証や本人確認などリスク低減措置を行う。	

表4-5：顧客管理システムの機能

機能	機能概要	金融庁ガイドラインにおける要求事項
顧客情報管理	顧客属性情報の保管、顧客からの届出等に基づく顧客DBへの登録・更新を行う。	• 確認記録・取引記録等について正確に記録するほか、IT システムを有効に活用する前提として、データを正確に把握・蓄積し、分析可能な形で整理するなど、データの適切な管理を行うこと 【（vii）データ管理（データ・ガバナンス）】 • 本人確認資料等の証跡のほか、顧客との取引・照会等の記録等、適切なマネロン・テロ資金供与対策の実施に必要な記録を保存する。【（iv）記録の保存】
書類電子化	本人確認書類の電子化および保存を行う。	

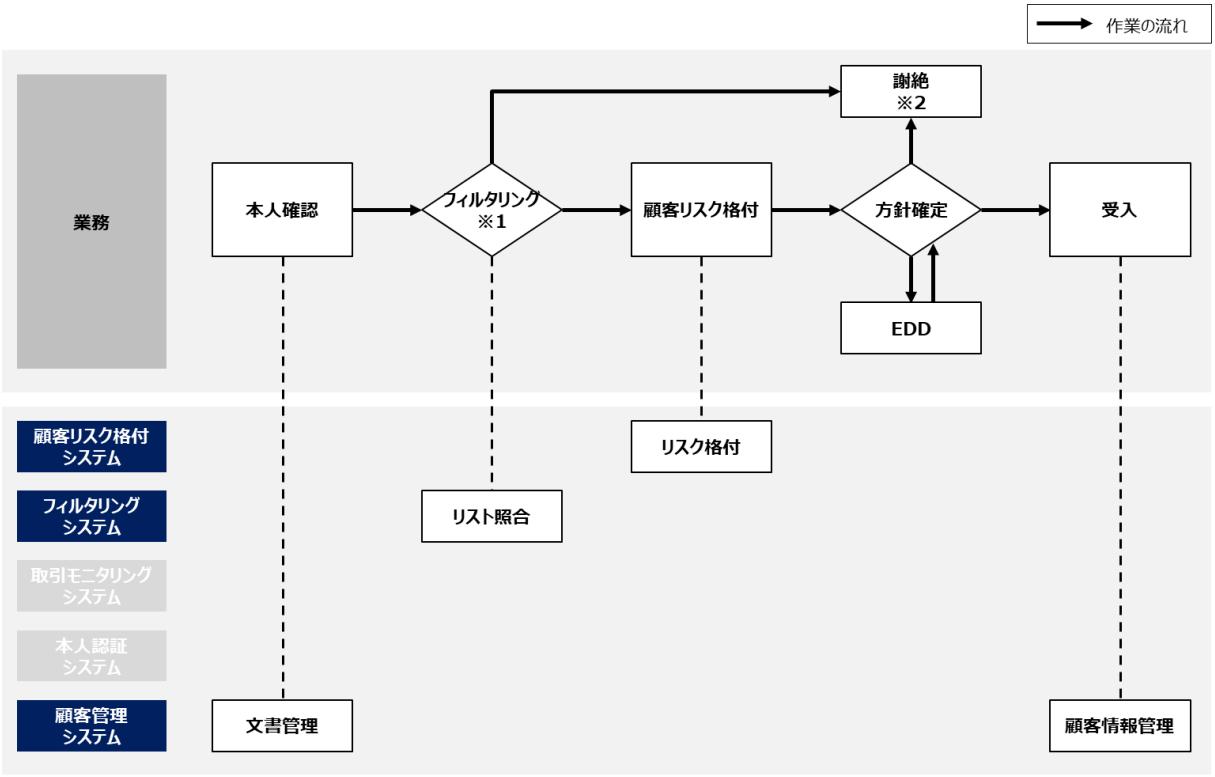
4.1.2. 各業務プロセスとITシステムの活用

図4-1で示したAML/CFTに関する５つの各業務においては、AML/CFTシステムを活用することができる。ここでは各業務のプロセスとITシステムとの関係を以下に示す。

新規顧客管理措置

まず、顧客から本人確認情報を収集し本人確認を行い、その情報を元に、「フィルタリング」「顧客リスク格付」を行う。次に、各社ごとに定められた顧客受入方針に従い、顧客受入可否を判断する。ここで、自社のリスク評価基準において「リスク高」と判断された場合、さらに踏み込んだ情報の取得・確認（EDD）を行うことで、当該顧客の受入可否の最終的な判断に繋げることが必要となる（図4-3）。

図4-3：新規顧客管理措置の業務プロセスと活用するITシステム例

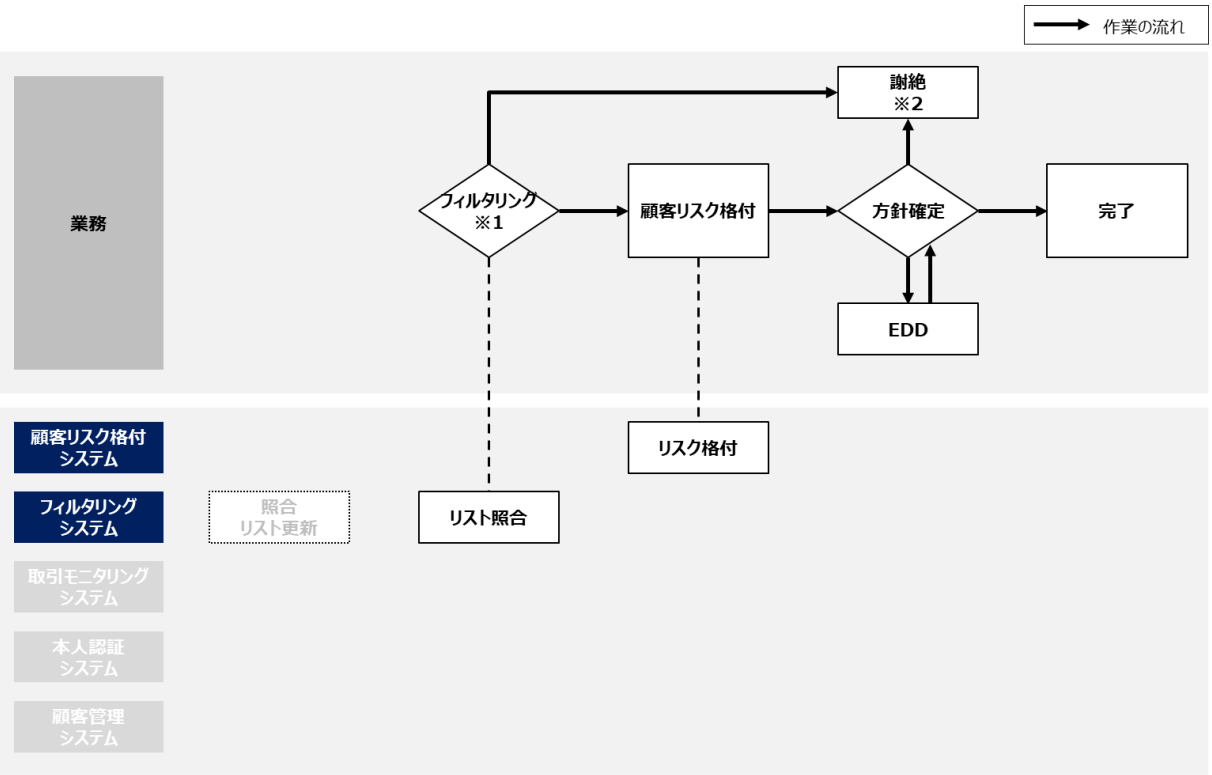


※1 リスト照合に加え、照合結果（反社に該当等）によっては謝絶の判断を行う
※2 必要に応じて、当局に疑わしい取引の届出を行う

フィルタリング

外部のフィルタリングリストと顧客から取得した顧客情報とを照合し、顧客が反社会的勢力・経済制裁対象者・PEPs等に該当していないかをチェックする。フィルタリングの過程でリスト掲載事項に該当した場合は、取引継続可否について検討し、謝絶等の対応を行う。併せて当該顧客の取引について、速やかに当局に疑わしい取引の届出を行う。最終的には、フィルタリング結果を元に改めて顧客リスク格付を実施し、顧客との取引継続可否を判断する（図4-4）。また、リスト照合結果は、顧客リスク格付の精度向上のため活用する。

図4-4：フィルタリングの業務プロセスと活用するITシステム例

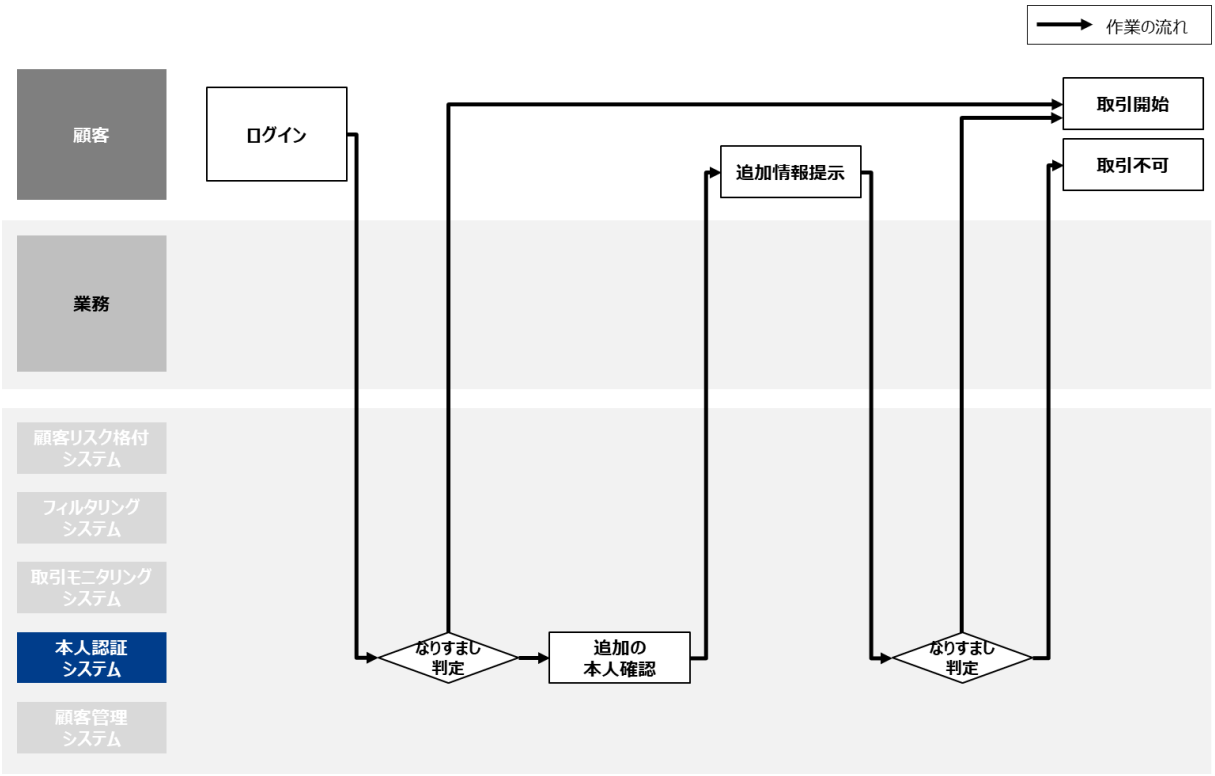


※1 リスト照合に加え、照合結果（反社に該当等）によっては謝絶の判断を行う
※2 必要に応じて、当局に疑わしい取引の届出を行う

本人認証（ログイン時）

ログイン時のブラウザやIPアドレス等のふるまいを分析し、なりすましの可能性（疑い度合い）を判定し、なりすましの疑いのある場合には、追加の本人確認を行う （図4-5）。また、なりすまし判定結果は、顧客リスク格付の精度向上のため活用する。

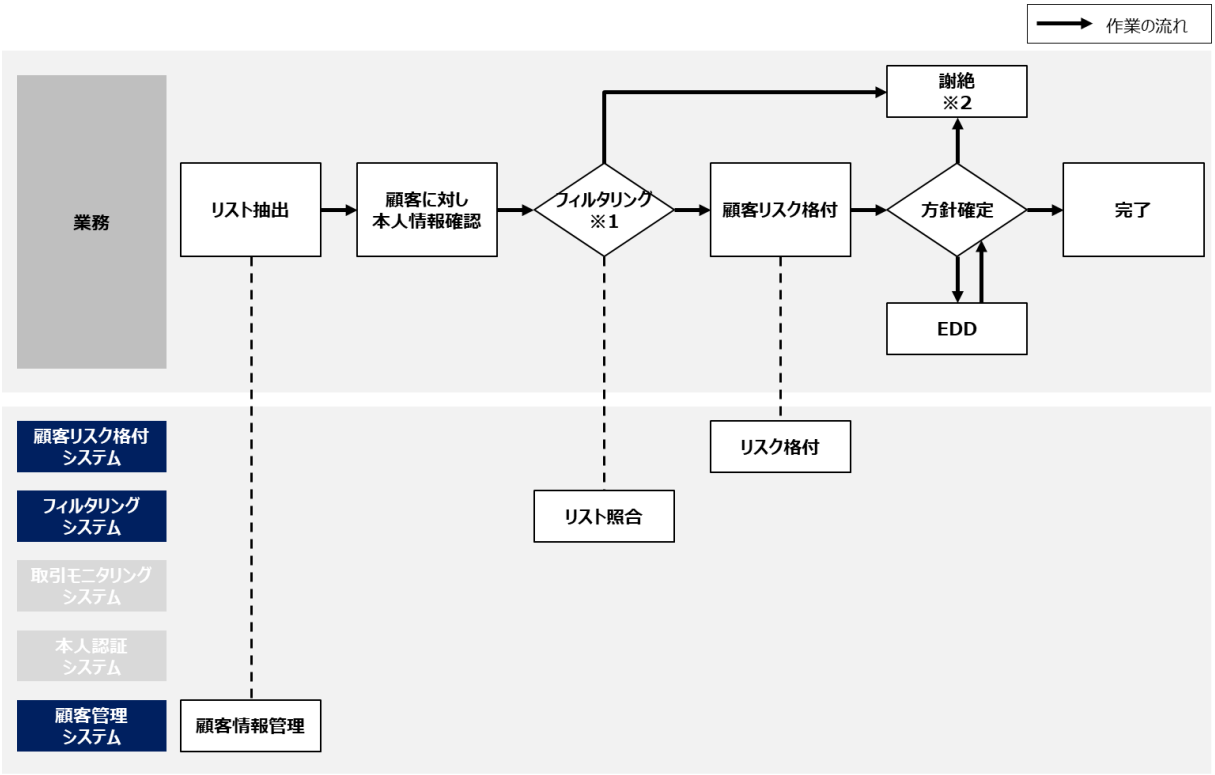
図4-5：本人認証（ログイン時）の業務プロセスと活用するITシステム例



継続的顧客管理措置

定期的（顧客のリスクに応じて決定されたタイミング）に顧客情報の確認・更新を行う。実施頻度は、顧客リスク格付により決定されることが一般的で、例えば高リスクの場合、EDDとして6ヶ月～1年に一回程度、中リスクの場合2年に一回程度、低リスクの場合、SDDとして3年～5年に一回程度などの運用が考えられる。顧客情報の確認・更新後は、「フィルタリング」および「顧客リスク格付」を実施し、顧客の取引継続可否を判断する（図4-6）。

図4-6：継続的顧客管理措置の業務プロセスと活用するITシステム例

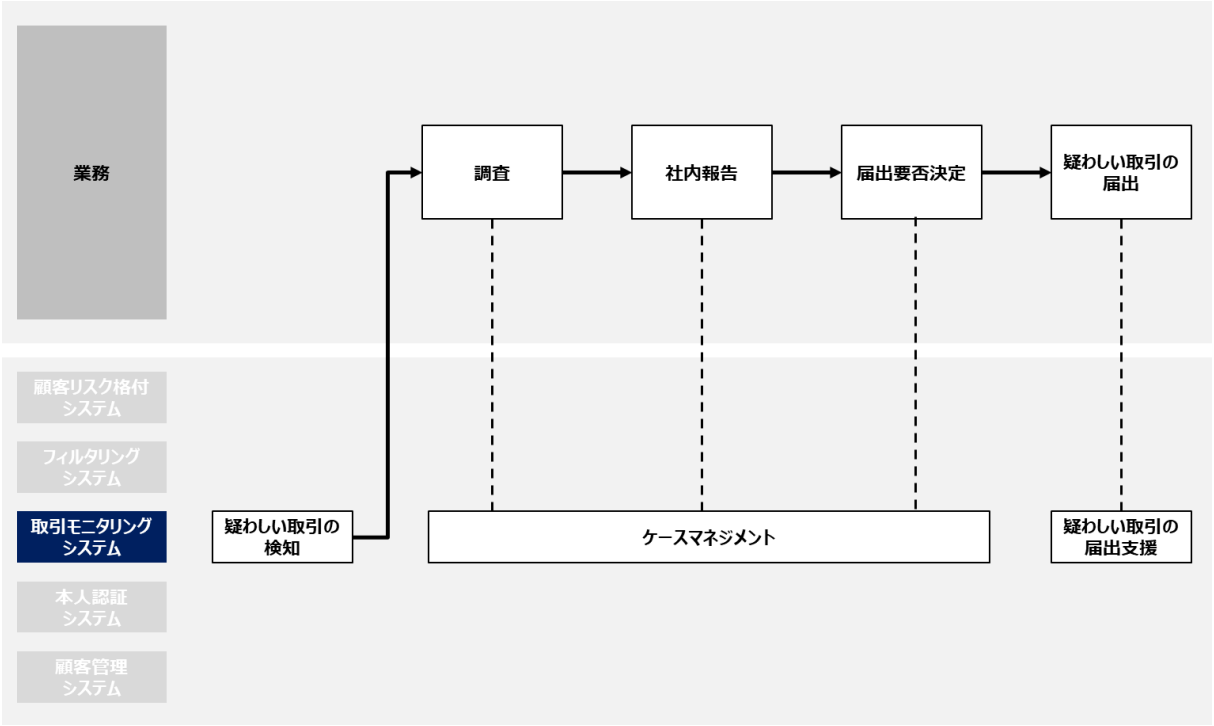


※1 リスト照合に加え、照合結果（反社に該当等）によっては謝絶の判断を行う
※2 必要に応じて、当局に疑わしい取引の届出を行う

取引モニタリング/疑わしい取引の届出

ML/FTリスクがあると想定される「疑わしい取引」の検知と当局への届出、およびそれに基づく特定の顧客や取引の排除を通じてリスクを低減させる手続のことをいい、会社ごとに一定の抽出基準や判断基準を設定し、自社にとってML/FTリスクが高い取引を適切かつ継続的に把握する。なお、取引モニタリングシステムでは、疑わしい取引の検知から疑わしい取引の届出候補の調査、社内での届出要否決定、届出までを実施する。また、疑わしい取引の届出結果は、顧客リスク格付の精度向上のため活用する。

図4-7：取引モニタリング/疑わしい取引の届出の業務プロセスと活用するITシステム例



4.2. FinTech等の活用例

金融庁ガイドラインでは、リスクの特定・評価・低減において「FinTech等の活用」について言及されており、「対応が期待される事項」として、新技術の有効性に対する積極的な検討の必要性や、AML/CFT高度化・効率化の観点から、新技術を活用する余地がないか、前向きに検討を行うことが推奨されている。

AML/CFT業務のうち、例えば、取引モニタリングであれば、システムから大量のアラートが発生するが、そうしたアラートを精査して、疑わしい取引を届けるべきか否かを最終的には金融機関の職員が判断する必要がある。このような業務は、世界中の金融機関にとって大きな負担になっており、これらを最新のテクノロジーで解決しようという取り組みが多くの金融機関で試みられている。

本節では、本WGにて想定されたユースケースをもとに活用事例を示す。

4.2.1. 新規顧客管理措置

【本人確認でのeKYCの活用】

a. 課題

現在、口座開設等における本人確認には、各社転送不要郵便・本人限定郵便を利用しているが、本人確認時のなりすましリスクや郵送コストの負担が生じている。

b. 対応策

2018年11月30日施行の犯収法施行規則の改正により、オンライン上で完結する本人確認方法（eKYC）が一部許容されることとなったことから、この実務を実現する。

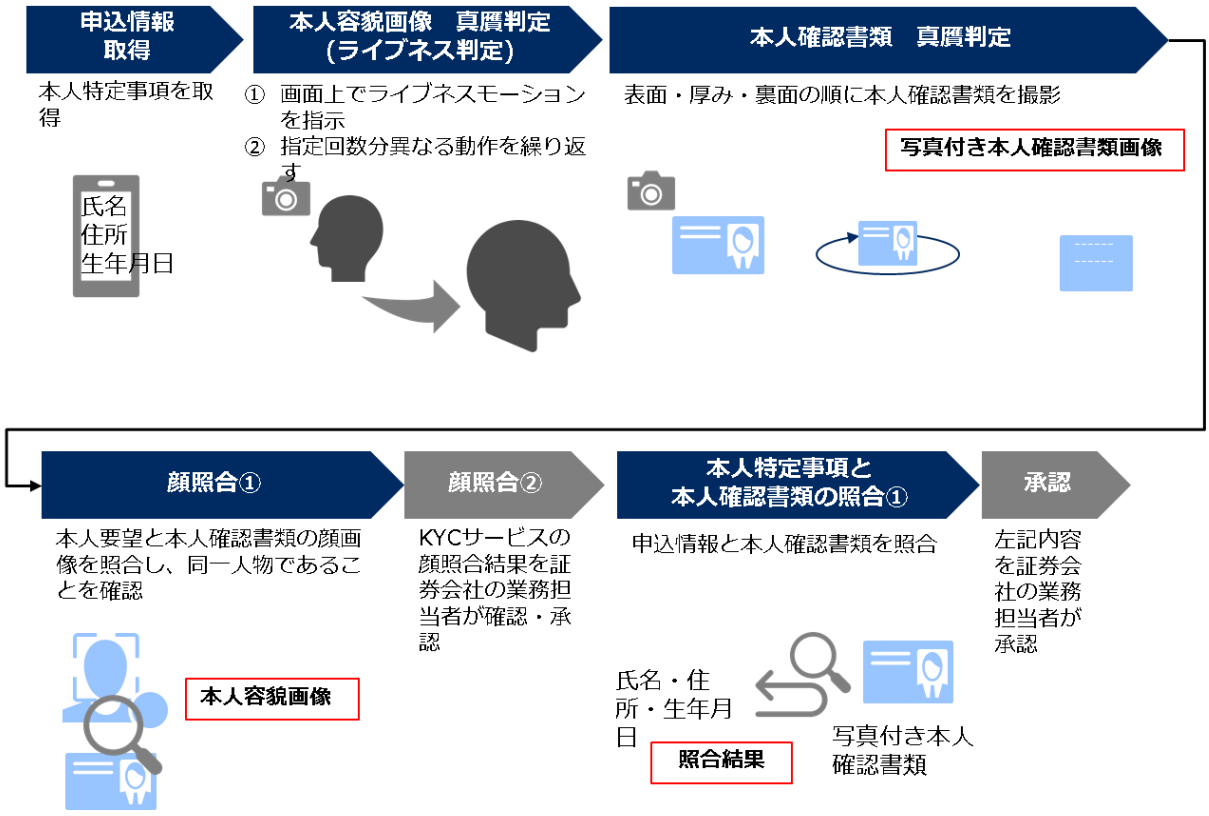
図4-8：改正犯収法施行規則にて新設された本人確認方法の概要

今般新たに認められた本人確認の方法のうち、各社で導入が進んでいる本人確認の方法（図4-9枠内）の事例を紹介する。

例1）

各社が提供するソフトウェアを使用して、顧客に撮影させた容貌及び写真付き本人確認書類の画像（本人確認書類に記載されている氏名・住居・生年月日、貼り付けられている写真を確認できるもの並びに本人確認書類の厚みやその他特徴を確認できるもの）にあたる本人確認用画像情報の送信を受ける方法【参考：犯罪による収益の移転防止に関する法律施行規則】

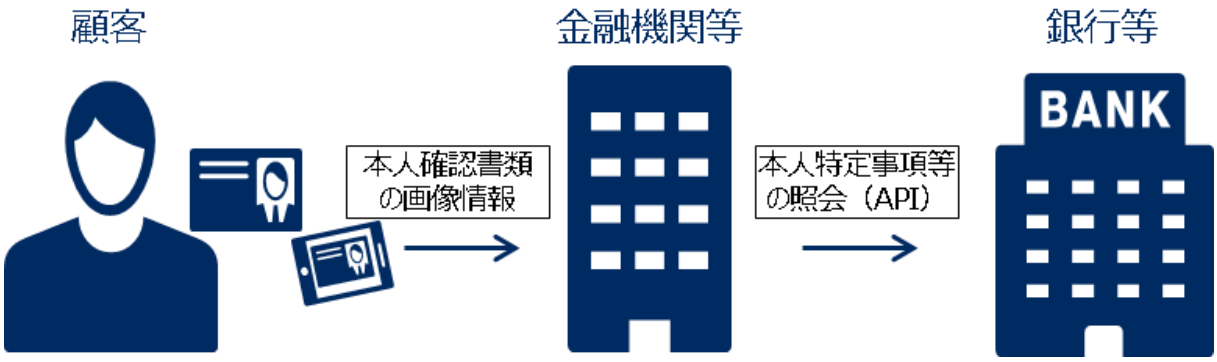
図4-9：eKYC業務フロー



例2）

各社が提供するソフトウェアを使用して、顧客に撮影させた容貌及び写真付き本人確認書類の画像（本人確認書類に記載されている氏名・住居・生年月日、貼り付けられている写真を確認できるもの並びに本人確認書類の厚みやその他特徴を確認できるもの）にあたる本人確認用画像情報の送信を受ける。又は、顧客に読み取りをさせたICチップに記録された情報（氏名・住居・生年月日）の送信を受けるとともに、他の特定事業者が氏名・住居・生年月日の確認を行い、その確認に係る確認記録を保存し、かつ、その顧客からその顧客しか知り得ない事項を確認し、確認記録に記録されている顧客と同一であることを示す申告を受けることにより、その顧客がその確認記録に記録されている顧客と同一であることを確認する方法【参考：犯罪による収益の移転防止に関する法律施行規則】

図4-10：eKYC業務フロー



c.　効果

eKYCを導入することで、本人確認をオンラインで完結させることが可能となり、下記の効果を期待できる。

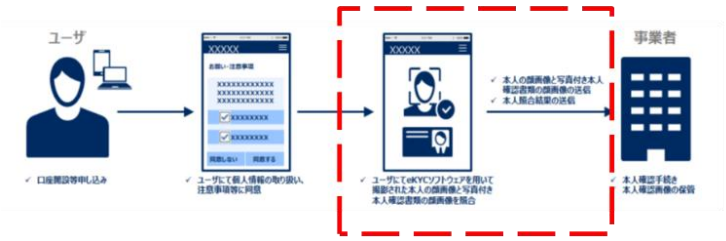
- 目視とAIにより本人確認を行うため、なりすまし防止を強化できると想定される（例1の場合）
- 転送不要郵便・本人限定郵便が不要になるため、郵送コストが減ると想定される（例1、2の場合）
- 転送不要郵便・本人限定受取郵便といった従来の本人確認と比べて、顧客の申請からサービス利用までのリードタイムが短くなると想定される（例1、2の場合）

※ご参考　～eKYCソフトウェアガイドラインについて～

本WGでは、eKYCソフトウェアを企画・開発・導入する際に参照することを想定し、証券業界として求められる要件を議論しガイドライン（Appendix ③）としてまとめた。ITベンダーの有識者にて検討した内容を中心にまとめたものであり、証券会社の個別の要件、システム構成、サービス提供形態など本ガイドラインで言及しない部分については、ITベンダーが証券会社の状況や環境を考慮して企画・開発・導入することを想定しているので、参照いただきたい。

図4-11：ガイドライン検討範囲

【検討範囲】



【章立て】

1 本ガイドラインについて
2 法令に準ずる必須要件
3 セキュリティに関わる要件
4 運用に関わる要件
5 UI/UXに関わる要件
6 本ガイドラインにおける用語の定義

【フィルタリング業務でのRPA・AIの活用】

a.　課題

CDDにおけるネガティブニュース検索の実施は、関連のない記事の除外など、完全な自動化が難しく、現場の負担となっている場合が多いと想定される。また、実施している場合でも、一連の調査は個人のスキルに依存する部分が多く、実効性が伴っていないケースも想定される。

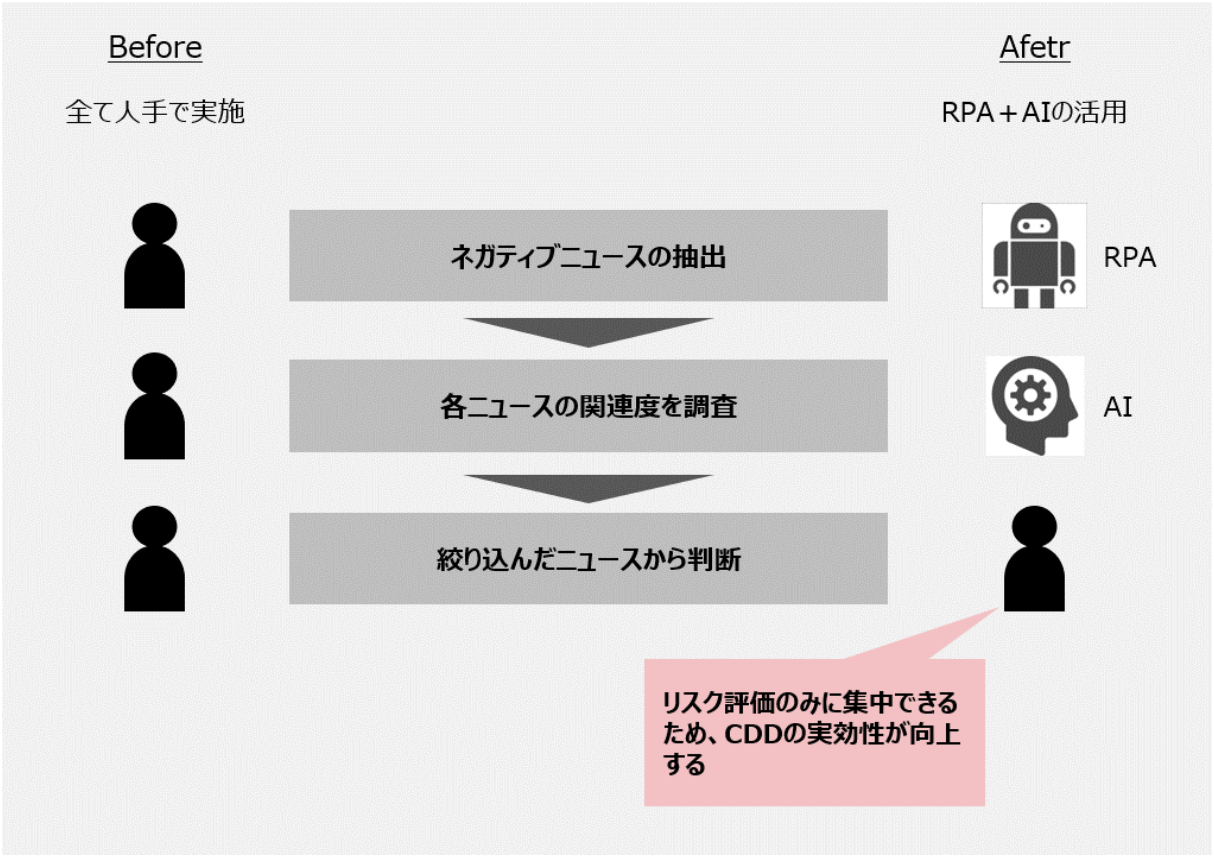
b.　対応策（例）

ネガティブニュースの抽出にRPAを活用することで、自動的に関連記事を取得する。さらに、AIを活用することで、抽出した記事の中から、関連性の高いニュースのみに絞り込む。

c.　効果

検索から絞り込みにかかっていた時間が削減できるだけでなく、担当者はすでに絞り込まれたニュースの中から、リスク判断を行うことのみに集中できるため、CDDの実効性が向上する。

図4-12：フィルタリング業務でのRPA・AIの活用事例



【顧客リスク格付業務でのAIの活用】

a. 課題

「顧客属性」や「商品」など、口座開設時に取得可能な情報のみで顧客リスクを判定した場合、高リスク顧客が特定できないケースが存在する。

b. 対応策（例）

顧客属性や商品ベースの格付に加え、①や②の方法を活用し顧客リスクを判定する。

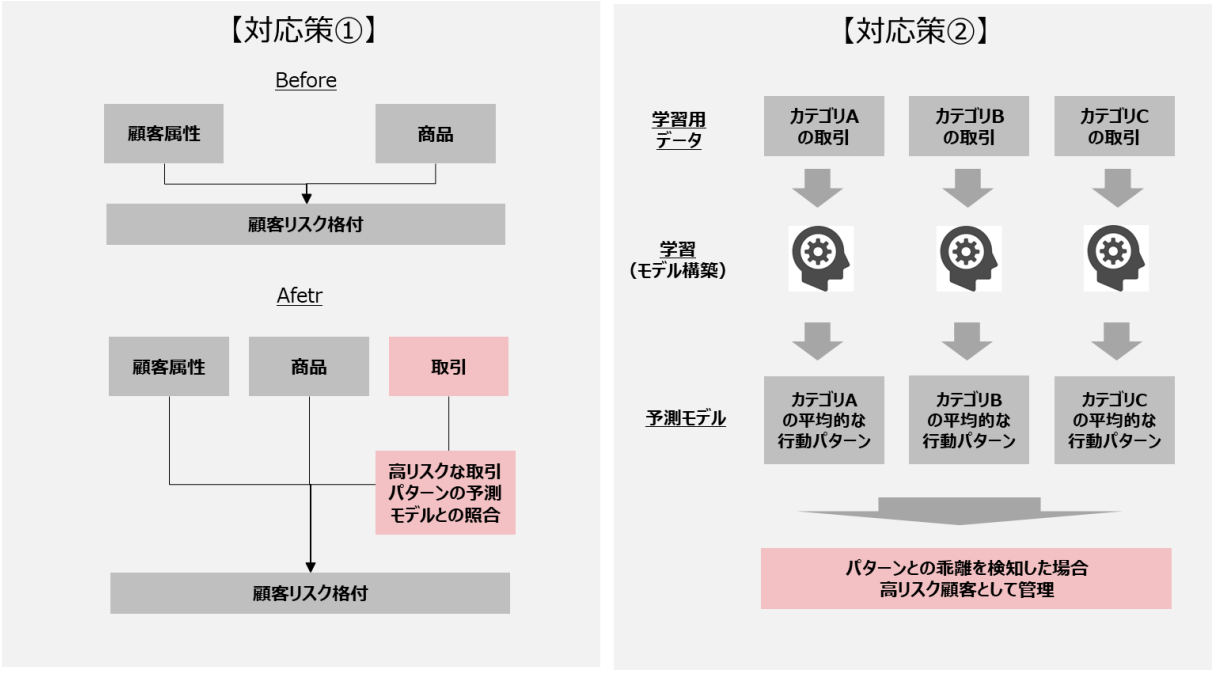
① 過去に不正判定した顧客の取引特性をAIで分析・抽出し、類似する取引パターンを持つ顧客を高リスク候補として抽出

② 職業や年齢などでカテゴライズし、そのカテゴリでの平均的な取引パターンから外れる顧客を高リスク候補として抽出

c. 効果

AIにより、取引データの分析も踏まえて顧客リスクを設定することで、顧客属性や商品といった限られた情報だけでなく、顧客の行動（取引パターン）自体を判断材料とした格付を実現することができる。

図4-13：顧客リスク格付業務でのAIの活用事例



4.2.2. 本人認証

【多要素認証の活用】

a. 課題

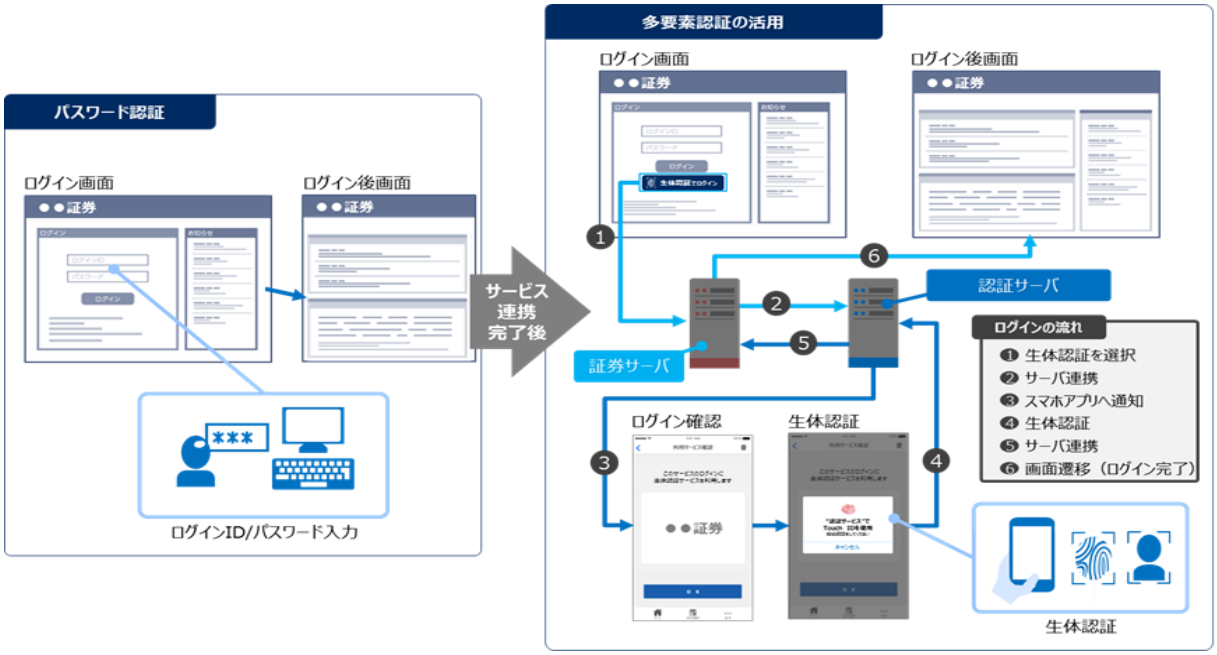
取引時にはユーザーが正当な顧客本人であることを確認することが重要である。

現在は、ログインパスワードや取引暗証番号（以降これらをパスワードと総称）など、認証を必要とする多くのシーンでパスワードを利用している。しかしながら、パスワードを安全に利用するためには忘却や紛失への対応、第三者に推測されにくくする工夫、盗難や漏えい対策など、利用者と証券会社いずれにとっても負担が大きくなっている。

b. 対策

パスワードによるログインを、スマートフォンを活用した多要素認証に置き換え本人認証を実施する。

図4-14：多要素認証の活用事例



c. 効果

多要素認証を導入することでパスワードが抱える課題を解決することができる。例えば、生体要素を認証に活用することにより忘却や紛失のリスクを軽減できることに加え、パスワード入力が不要になるなど顧客の利便性向上が期待される。所持要素は利用者自身が所持していることをもって本人であることを示すものであり、自身が所持している限り第三者に悪用される可能性は低く 、忘却のリスクも避けることができる。

また、UXの向上に加え、なりすまし防止の強化とコスト削減を実現することも可能となる。

・複数要素で認証を行うため従来の本人認証と比較しなりすまし防止に寄与する。

・パスワード忘却や紛失リスクを軽減することができるため問い合わせ対応コストが減ると想定される。

※ご参考　～本人認証ガイドラインについて～

本WGでは、証券各社の本人認証を従来よりも強化する際に参照することを想定し、証券各社がその検討や対策に取り組むための考え方を議論しガイドライン（Appendix ④）としてまとめた。このガイドラインは認証強化に取り組むための考え方を記載したものであり、具体的な対策については、ガイドラインに記載する考え方を参考に証券各社またはその関係者が状況や環境に応じて取り組むことを想定しているので、参照いただきたい。

4.2.3. 取引モニタリング/疑わしい取引の届出

【ルール設定におけるAIの活用】

a. 想定される課題

自社の取引特性に基づいた、ルールの設定ができていない。また、既存ルールの妥当性が、モニタリング担当者自身で理解できないケースが想定される。

b. 対応策（例）

「過去に疑わしい取引として判断された取引」と「正常取引」の両方をAIで学習し、①または②を実施。

① 疑わしい取引の規則性を抽出し、ルールベース検知に追加

② 疑わしい取引のモデルを構築し、プロファイルベース検知に追加

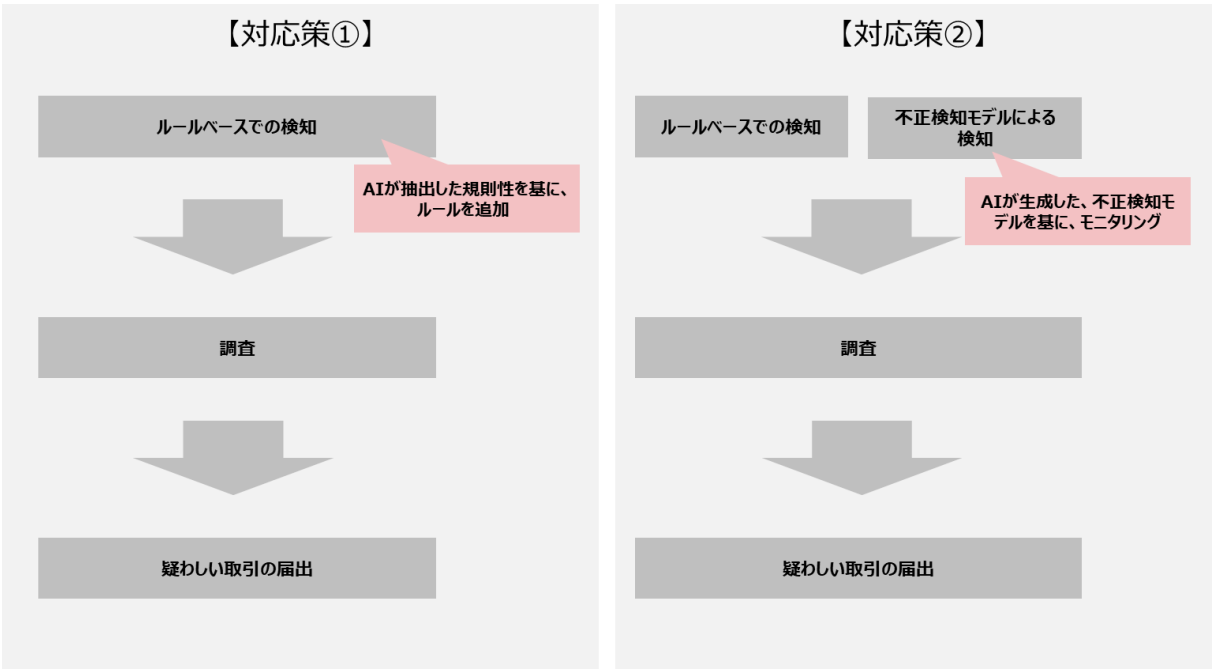
c. 効果

AIの活用によって、自社の取引データから直接ルール作成やモデル構築を実施することになるため、汎用的なモニタリングではなく、自社の取引特性を考慮したモニタリングが可能となる。また、モニタリング担当者自身も、AIの解析結果を参考にすることで、自社の取引特性の理解促進や、ルール作成のスキル向上に繋がる。

＜注意＞

本対応の実施により、対応前と比較して検知数が増加するため、業務負担が大きくなる可能性が高い。

図4-15：ルール設定におけるAIの活用事例



【調査におけるAIの活用】

a. 想定される課題

取引モニタリングシステム導入後に、大量のアラート（過剰検知）が発生することで、現場社員の業務負担が増加するケースが想定される。また、発生したアラートに対して、調査するスキルをもった専門人材の数が不足することも考えられる。

b. 対応策（例）

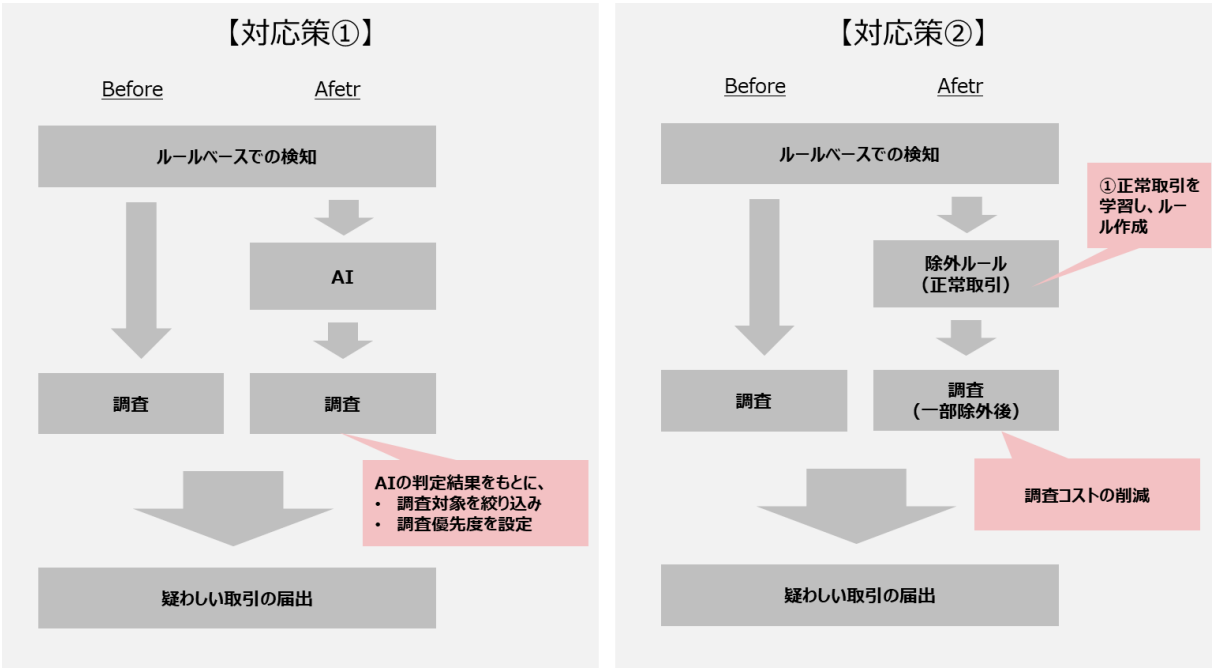
① 過去に不正判定した取引をAIで学習し、類似する取引を検知する。AI単独での運用も可能であるが、ルールベースで抽出したアラートに対してAIで絞り込むことで、よりアラートの削減効果が見込める。

② AIで正常取引の傾向を学習しその規則性を抽出することで、明らかに正常である取引をアラートから除外するためのルールを生成する。

c. 効果

AIにより、過剰検知を抑制するモデルを作成、または、規則性を抽出。これにより、検知精度（不正を逃さない）を維持しつつ、従来のルールベースと比較してアラート件数を削減する。

図4-16：調査におけるAIの活用事例



4.2.4. その他

【文書管理におけるAIの活用】

a. 課題

本人確認書類をはじめ、紙文書が画像データのまま保存されており、テキストデータとして活用できていないケースが想定される。そのため、データ活用が十分でない可能性が高い。

b. 対応策（例）

AI-OCRを活用し、画像化された文書データをテキスト化する。

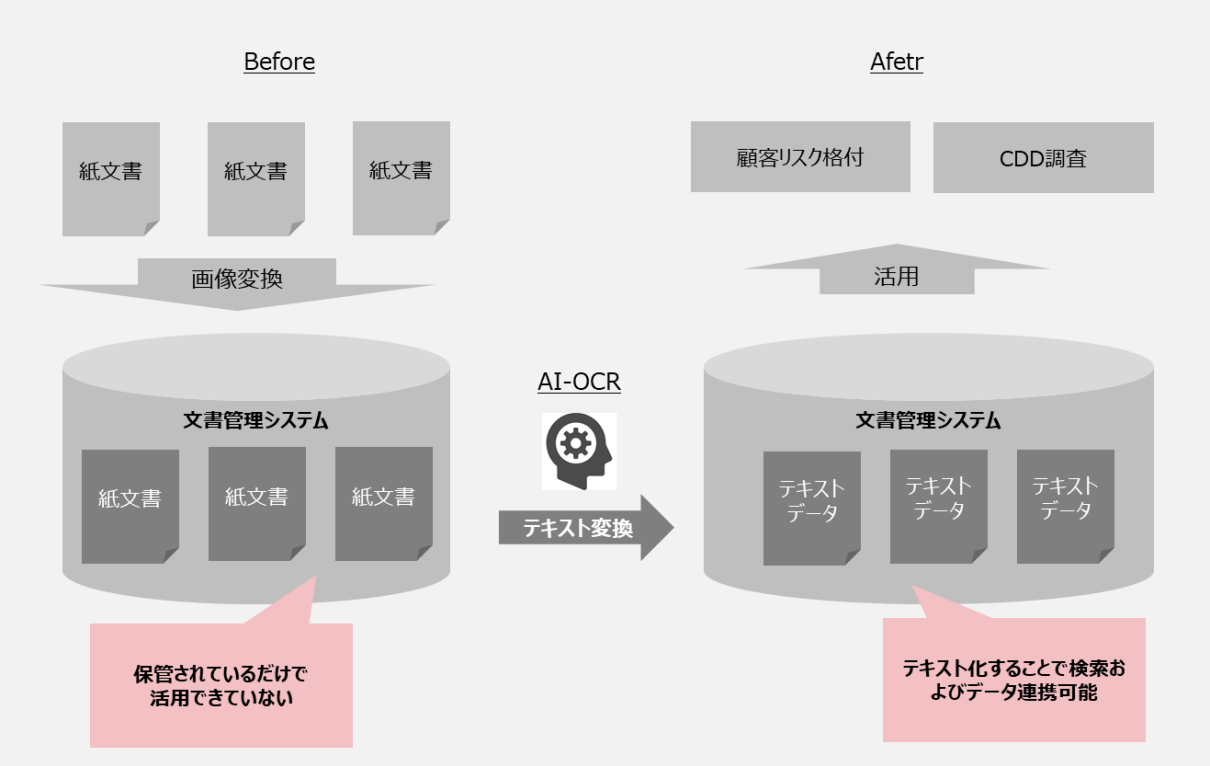
c. 効果

確認記録・取引記録等について、分析可能な形で保管できる。さらに、検索性の向上により、個人情報と紐づけた管理が容易になるため、データ・ガバナンスの向上につながる。

また、本人確認書類の有効期限切れの検知など、顧客管理プロセスに活用することも可能。

（例：免許証の有効期限切れを検知し、アラートを出す等）

図4-17：文書管理におけるAIの活用事例



（空白のページ）

5.

証券業界における

AML/CFT態勢高度化に向けた検討

5.1.検討の背景

近年、証券会社を含む金融商品取引業者においては、AML/CFTの基本的な管理態勢の整備が定着しつつあるが、顧客管理措置等の個別要件に関して、業務運営および態勢整備に課題を有する事業者が存在することが本邦当局により報告されている[9]。本WGの取り組みの中でも、規模の大きな事業者ではAML/CFTシステムの導入が進んでいる一方で、規模が小さな事業者においては十分な態勢を整備できていない実態が浮かび上がっている。

マネー・ローンダリングは、サイバー攻撃と同様に、その対策に抜け穴がある事業者を狙っておこなわれやすいという特徴がある。仮に対策が不十分な事業者の金融サービスが悪用され、例えば犯罪組織が違法に稼いだお金を有価証券に投資して売ってしまうとすると、どんな由来のお金だったかがわからなくなってしまう。そして、金融がネットワークで成り立っていることを考えると、そのような不正な経済活動に加担した責任は単に悪用された事業者にとどまらず、延いては日本の金融システム全体のレピュテーションリスクにも繋がる恐れがある。このことは、国外との金融取引禁止等の措置にまで至る可能性を秘めており、正常な経済活動の維持が困難となって、果ては国民生活にまで影響を及ぼす恐れもでてくる。よって、AML/CFTに関する規制強化の対応は、個々の事業者だけで閉じることなく業界全体で取り組むべき課題であり、継続的に強化していくことが重要である。

しかし、各金融機関は、本邦当局から求められる継続的な規制強化への対応負担がある一方で、昨今の技術革新やFinTech企業の勃興などによる急速な競争環境の変化にさらされており、相当なコスト削減を強いられている状況が考えられる。こうした背景を受け、本WGはAML/CFTを非競争領域ととらえ、十分な経営資源を投入することが難しい事業者であっても、一定のコストで一定のリスク対応水準を担保できるようにするための方策として、AML/CFTの業界全体での共通化実現を目指すこととした（AML/CFTの「共通化」）。加えて、金融システム全体としてのML/FT防御性能を強化するため、リスクベース・アプローチにおけるリスク低減措置の効率化や金融犯罪手口の複雑化への対処として、各事業者が有するインシデントや攻撃パターンなどの情報や顧客に属するデータを多くの事業者で共有することについても、あわせて検討することとした（AML/CFTの「高度化」）。これは、個々の事業者が保持する情報やデータを複数の事業者で連携することで、単独では見抜くことができないような高リスク顧客の特定、および疑わしい取引の検知等を行うなどし、取引停止や謝絶等の措置につなげることによって、より実効的なリスクの低減を目指すものである。

本章では、「AML/CFT共通化」「AML/CFT高度化」について、本WGのこれまでの議論で挙がったコンセプトとその概要をまとめるとともに、実現に向けて検討するべき論点を整理した。

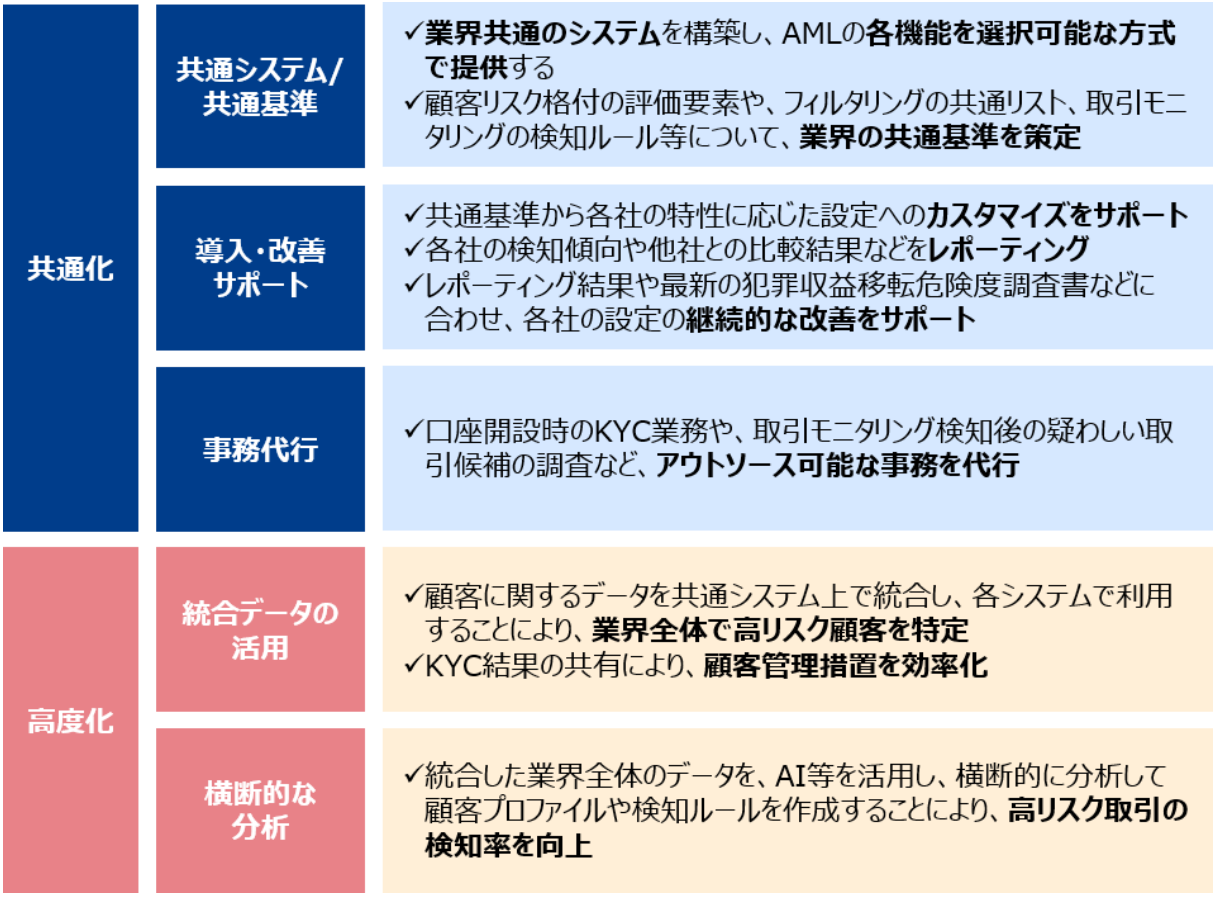
[9] 参考：金融庁「マネー・ローンダリング及びテロ資金供与対策の現状と課題」（P.22）
<https://www.fsa.go.jp/news/30/20180817amlcft/20180817amlcft-1.pdf>（最終閲覧日：2019.9.30）

5.2. コンセプト

5.2.1. AML/CFTの共通化・高度化

本WGが考えるAML/CFTの共通化・高度化について、これまでの検討と仮説を基に、目指す姿のコンセプトを図5-1にまとめた。

図5-1：AML/CFTの共通化・高度化のコンセプト



一つ目のコンセプトであるAML/CFTの「共通化」は、業界全体で当局が求める要求水準を満たすとともに、対応レベルを継続的に向上させることを目的としている。そのために、「共通システム/共通基準」、「導入・改善サポート」「事務代行」の3つのサービスを掲げ、共通システムの運営主体が証券会社に対して提供することを想定している。

「共通システム/共通基準」では、AML/CFTに必要な各種基準の策定と、業界全体で利用可能な共通システムの構築を行う。そして、4章で定義したAML/CFTにおける各システムを、共通システムを通じて提供する。「導入・改善サポート」では、各システムの導入時のカスタマイズや、継続的な改善サポートの提供を行う。「事務代行」では、共通システムのメリットを活かすために、各事業者に共通事務のアウトソーシングサービスを提供する（サービス提供方法に関する論点は 5.5.節1）に記載）。

二つ目のコンセプトであるAML/CFTの「高度化」は、個社ごとのAML/CFTでは見抜くことが難しいような、高リスク顧客の特定、および疑わしい取引の検知等を実現することを目的としている。そのために、「統合データの活用」および「横断的な分析」により、共通システムの機能向上と、サポートサービスの強化を想定している。

「統合データの活用」では、共通システムに蓄積された顧客に関するデータ（属性データ、ふるまいデータ等）を、顧客リスク格付や取引モニタリング等の個別システムのインプットとして活用し、機能向上を図る。また、「横断的な分析」では、統合データをAI等の活用によって分析することにより、疑わしい取引の検知やなりすましの検知率の向上を図る （データ統合に関する論点は 5.5.節2）に記載）。

5.2.2. 共通システムについて

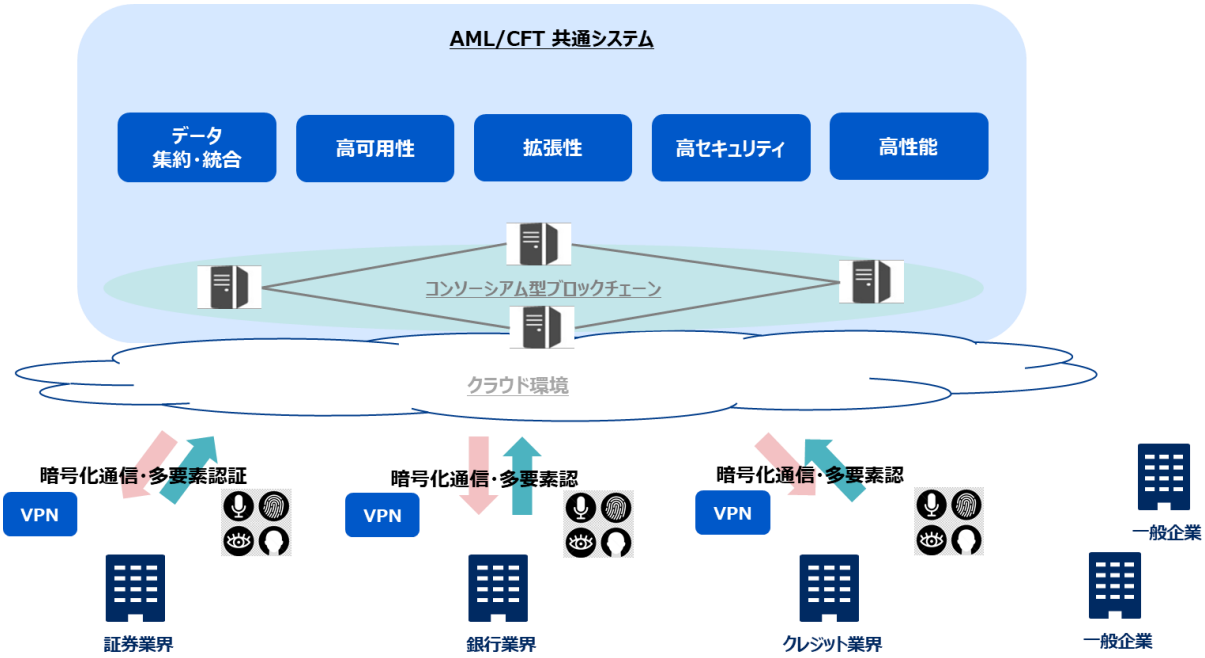
AML/CFTの「共通化」実現手段の一つである、共通システムの概要について述べる。

共通システムは、単にAML/CFTのシステムを各事業者に提供するだけでなく、業界全体のデータを集約する基盤としての役割を担う。そして、集約されたデータを最大限活用するため、AI等を活用して分析することで、各AML個別システムの機能向上や、証券各社へのサポートサービスの強化を図り、業界全体のAML/CFT水準の引き上げを実現する。

共通システムは、業界全体での利用および、統合データなどの大量データの処理を実施する基盤となるため、可用性とセキュリティに加え、それを実現するスペックも十分考慮して設計する必要がある。

また、利用事業者の増加や、当局要請や法令対応等に伴う機能変更要求に柔軟に対応するため、拡張性や運用性も十分考慮する必要がある。個別システムをマイクロサービスとして提供することの他に、クラウドの最大限の活用や、データ共有についてはブロックチェーンの活用等を考慮に入れ、長期的に陳腐化しにくいアーキテクチャーの設計が必要となる（システムに関する論点は、5.5.節2）に記載）。

図5-2：共通システムの実現イメージ



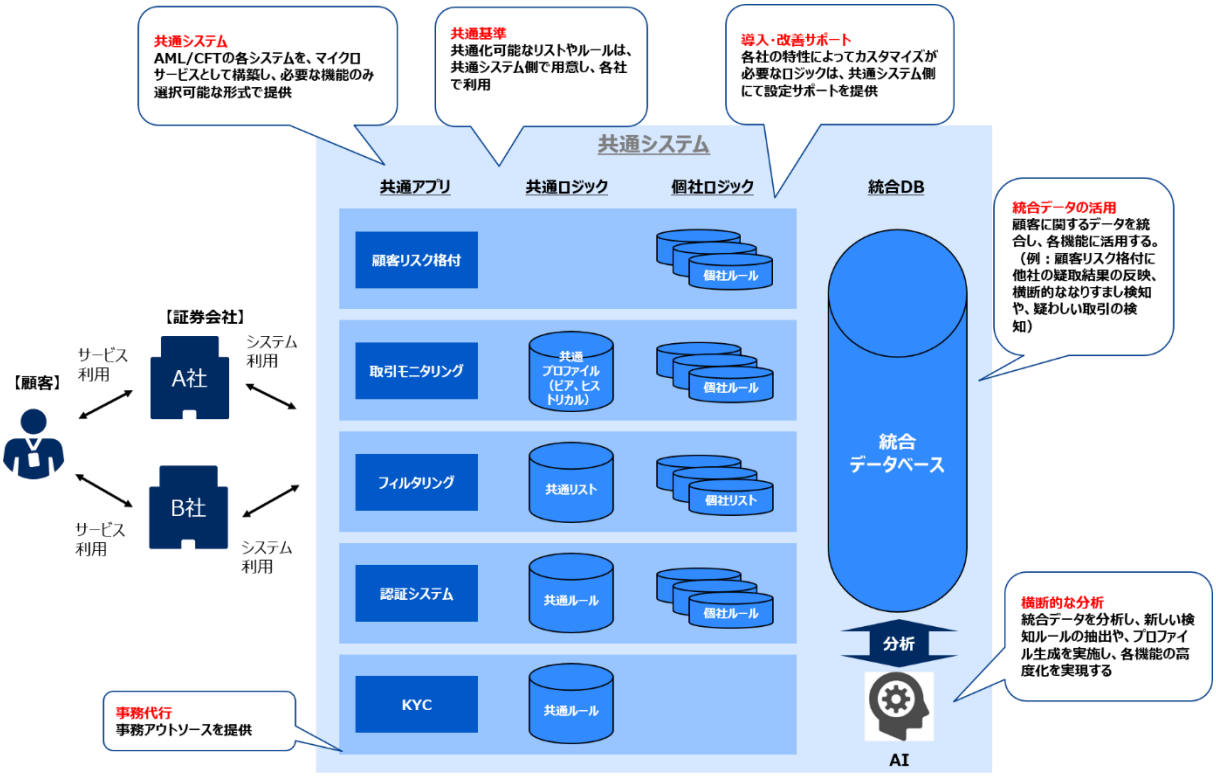
共通システムは主に、共通アプリ、共通ロジック領域（共通リストや共通ルール）、個社ロジック領域（個社でカスタマイズしたリストやルール）、統合データベースの4つで構成されている。（図5-3）。

まず、顧客リスク格付、取引モニタリング、フィルタリング、本人認証、KYCといった、AML/CFTの主な個別システムを共通システム上に用意し、各事業者での共同利用を前提とした共通アプリとして提供する。また、各機能はマイクロサービスとして構築され、証券会社側は、必要なサービスのみを契約し利用することができる。また、各個別システムに付随する業務の内、アウトソース可能なものについても、サービスとして提供する。

次に、共通アプリで利用するロジックについては、共通化可能なものは共通ロジック領域で管理し、個別カスタマイズが必要な部分については、個社ロジック領域で管理する。共通ロジック領域では、フィルタリング利用する共通リストや、取引モニタリングで利用するプロファイリングを格納する想定。また、個社ロジック領域では、顧客リスク格付のルール（リスクウェイト）、照合リスト（個社のイエロー・ブラックリスト）、取引モニタリングの検知ルール、なりすまし判定ルール等を格納する想定である。

最後に、統合データベースについては、顧客ごとに共通IDを割り当てることにより同一顧客を特定し、各事業者の顧客に関するデータを統合する想定である。そして、統合データベースを、顧客リスク格付や取引モニタリングのインプット情報として活用することにより、各機能の向上を図る。更に、統合データベースを、AI等を使用して横断的に分析することにより、疑わしい取引やなりすましを判定するための、新たなルール抽出等を行う（データ統合に関する論点は 5.5.節2）に記載）。

図5-3：共通システムの機能配置例



5.3. 「共通化」の概要と効果

共通化のコンセプトは、「共通システム/共通基準」「導入・改善サポート」「事務代行」である。
ここでは、それぞれについて、概要と効果について説明するとともに、実現に向けての論点を述べていきたい。

5.3.1. 共通システム/共通基準

「共通システム/共通基準」では、業界共通のシステムを構築し、AML/CFTの各システムを選択可能な形式で提供するとともに、顧客リスク格付の評価要素やフィルタリングの共通リスト、取引モニタリング・本人認証の標準的な検知ルールを策定する。各事業者は、共通システムより提供される共通基準を活用し、自社のリスク評価方針に沿って評価モデルやルールを設定することになる。これにより、業界として一定のAML/CFTの水準を担保しつつ、個社ごとにみれば、金融庁ガイドラインで要求されているリスクベース・アプローチによるAML/CFTが可能になると考えている。

また、業界全体でシステムを利用することにより、スケールメリットを享受でき、コスト削減が可能になるとともに、共通システム構築の取組みに関し、当局からの一定の理解を得ることにより、各事業者から当局への、AML/CFTに関する態勢およびシステム仕様の説明負荷（コミュニケーションコスト）を軽減する効果も期待される。

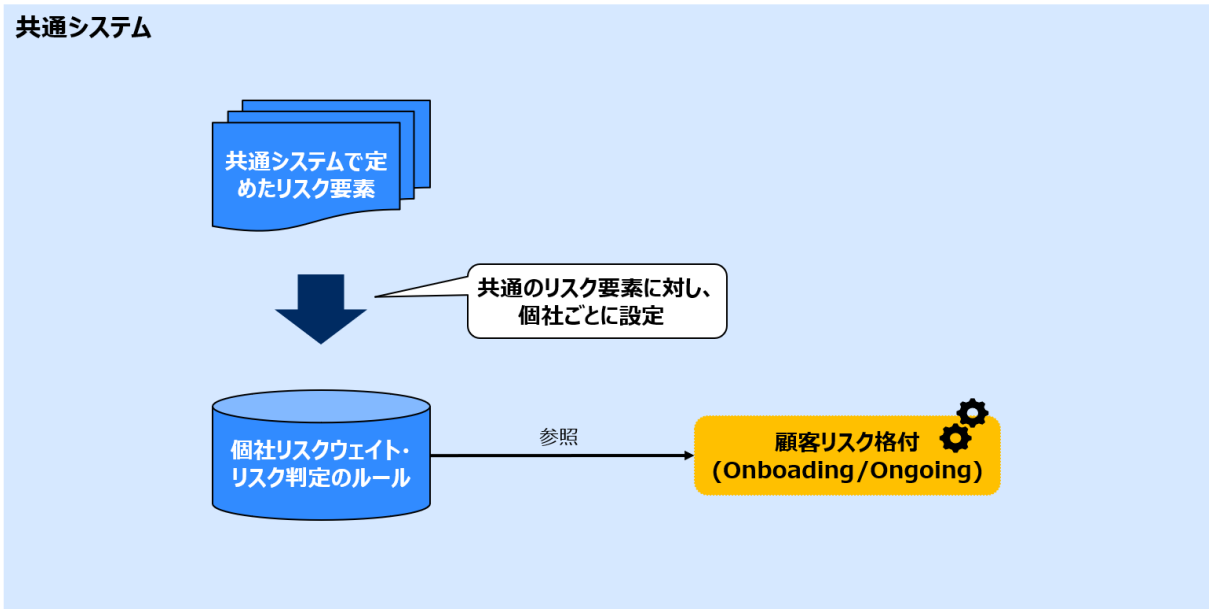
なお、共通システムを構築する前提として、共通システム上で提供する各個別システムは、その対象業務を行う上で必要な機能を網羅的に用意するため、各社で同様の重複システムを個別に用意する必要はない。しかし、共通システムを各社システムの補完的に利用することは可能である。（システムに関する論点は、5.5.節2）に記載）

ここからは、共通アプリケーションごとに、共通基準と個社カスタマイズ領域についての例を示し、今後の論点について述べていきたい。

■　顧客リスク格付

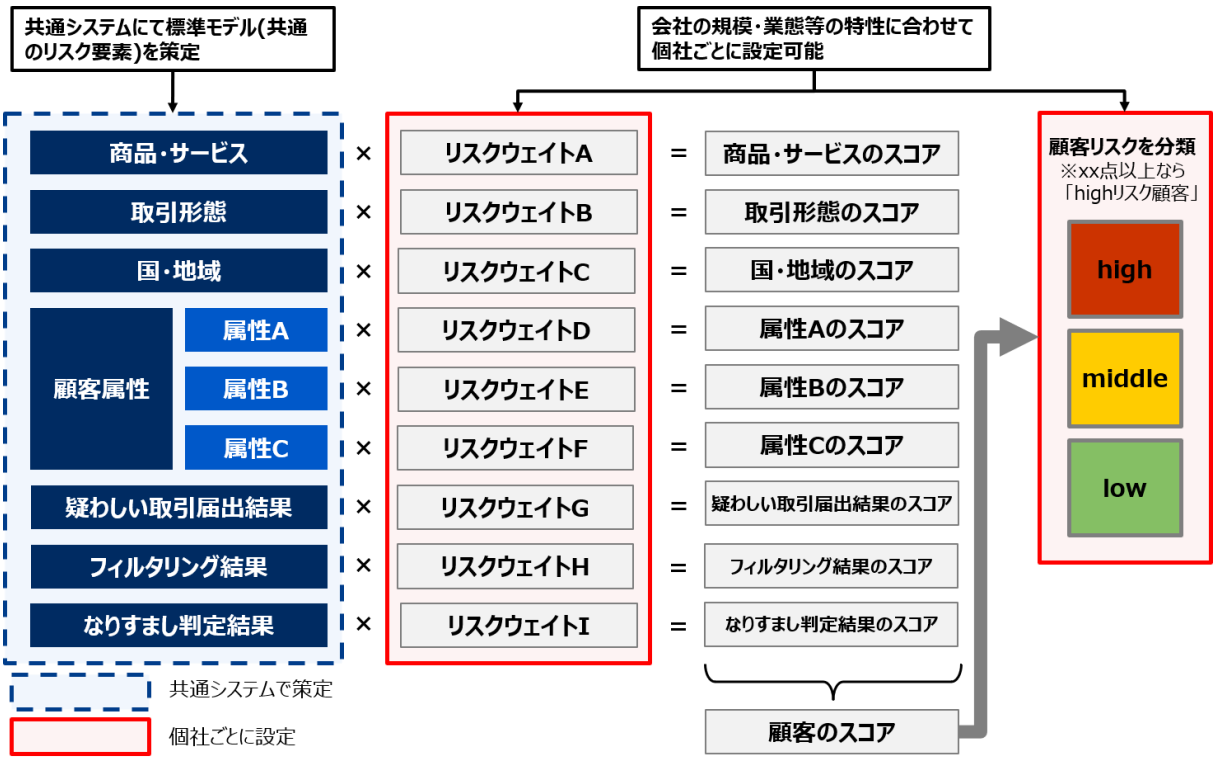
共通システム上で格付モデルのリスク要素を提供する。共通的なリスク要素に対して、個社ごとにリスクウェイトやリスク格付の判定基準（high/middle/lowの基準値）を設定する。（図5-4）。

図5-4：顧客リスク格付の評価モデル設定



具体的な格付モデルの例を図5-5に示す。左端の点線枠内が共通システムで提供する全社固定のリスク要素である。個別のリスク要素について、実線枠内にあるリスクウェイト（自社の規模や業態・特性に合わせて各事業者が決定）を掛け合わせることで、各要素のスコアを算出し、更にそれらを合計したものを顧客スコア値として利用する。また顧客スコア値を基に、顧客リスクを分類するための基準についても各事業者にて設定する。尚、共通のリスク要素については、法改正や情勢に合わせて随時更新していくことを想定している。

図5-5：顧客リスク格付のモデル（例）



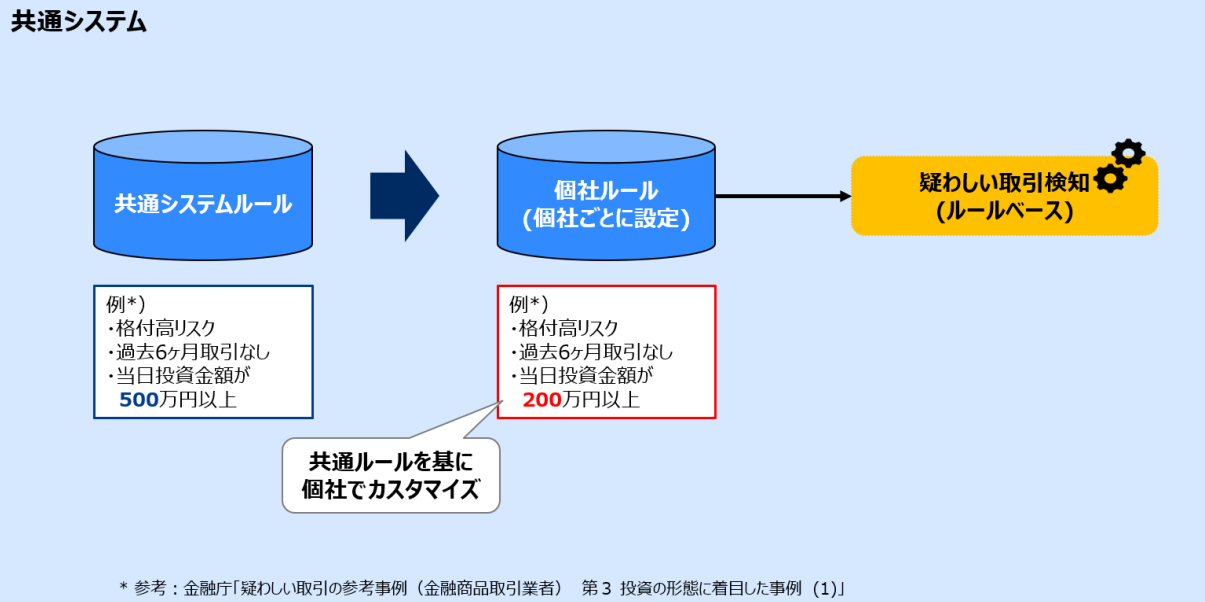
共通システムで共通のリスク要素を提供するためには、まず業界共通的なリスク要素を議論の上決定する。規模や商品ラインナップ、チャネル等が異なる会社間でリスク要素を固定することが可能なのか（論点3-1：共通基準の策定）、また、各事業者のカスタマイズはどの程度の範囲で可能とするのか（論点3-2：個社カスタマイズの許容範囲）について検討が必要である。

また、一度決めたリスク要素は、当然法改正や国内外の情勢に合わせ、見直す必要がでてくると想定される。そのため、共通的なリスク要素の更新プロセスについても検討する必要がある。（論点3-3：共通基準の更新プロセス）

■　取引モニタリング

共通システム上で疑わしい取引検出のための共通ルールを提供する。その共通ルールを基に、各事業者が顧客リスク格付と同様、自社の規模・特性に合わせてルールの内容や閾値を設定する。共通ルールとしては、例えば図5-6のように、投資の形態に着目したルール設定が考えられる。こういった共通ルールをミニマム・スタンダードとし、会社によっては投資金額を下げ、更にルールを厳しくする、といったカスタマイズを可能にする。

図5-6：取引モニタリングのルール



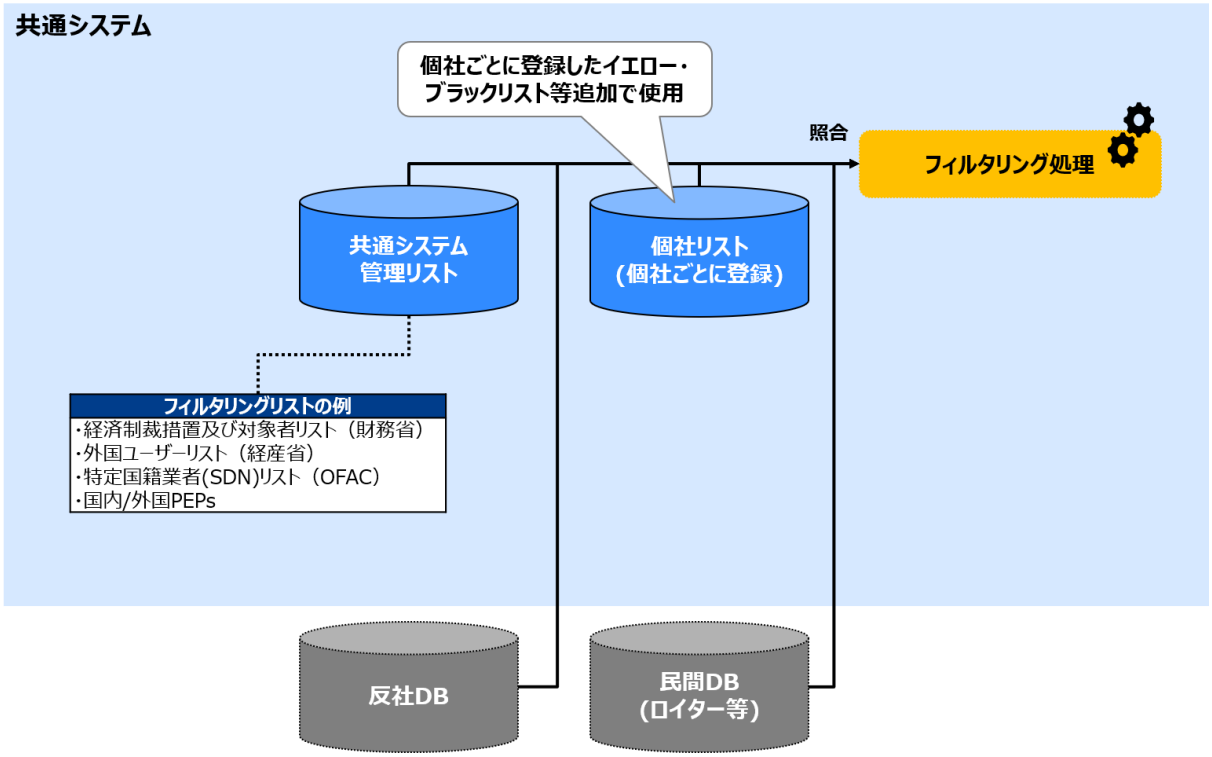
現状各事業者の取引種類は、会社の規模や特性、有するチャネルによって多種多様となっていると想定される。一言で共通ルールといっても、どのように業界全体のAML/CFT水準底上げに資するルールを作っていくのか（論点3-1：共通基準の策定）、そしてどのようなプロセスで更新をしていくのか（論点3-3：共通基準の更新プロセス）、今後検討を重ねていく必要がある。

また、個社ごとに設定するリスクウェイトやリスク「high/middle/low」の基準値について、どこまで各事業者のカスタマイズを許容するのか、についても議論が必要である。（論点3-2：個社カスタマイズの許容範囲）

■　フィルタリング

3章で定義した、当局から開示される各事業者共通的なフィルタリングリストを共通システムで作成・管理して提供する。ここは、各事業者共通的に実施していることであり、共通システムが担うこととする。それに加え、民間の商業DBおよび警察庁の反社DBへの照合も共通システムで実施する。一方で、個社で保有しているイエロー・ブラックリスト（受入留意または受入禁止顧客のリスト）は各事業者で登録を行い、他社には共有しない。

図5-7：フィルタリングのリスト



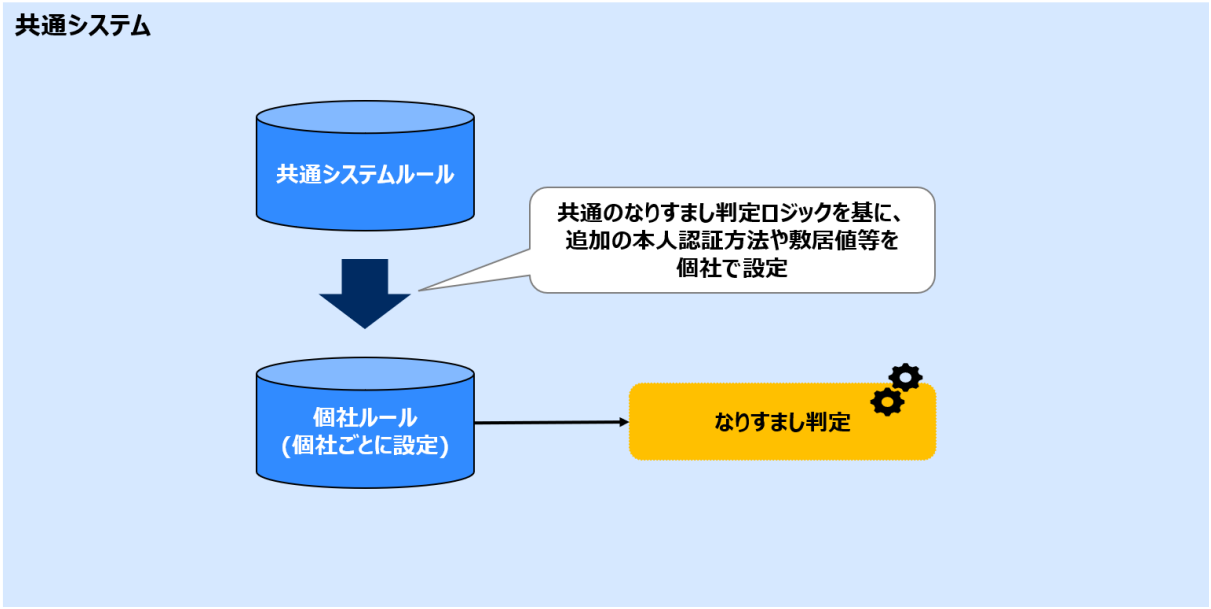
共通リストの範囲に関しては、今後議論の上決定する必要はあるが、現状各事業者がカバーしている国内・域外適用のリストを定義すれば、共通システムでの作成および管理は可能と考える。（論点3-1：共通基準の策定/3-3：共通基準の更新プロセス）

一方で、個社リストに関しては、証券会社へのヒアリングの中で、各事業者で共有できれば高リスク顧客の特定のために、有益であるというご意見があった。ここは、今後の議論で、各事業者の方針の確認および法的課題の整理が必要となると考えている。（論点3-4：個社リスト（イエロー・ブラックリスト）の共有）

■　本人認証

共通システム上で、なりすまし判定ロジックを提供する。追加の本人認証方法や閾値等は、個社ごとに設定する。

図5-8：本人認証のルール



ここでは、なりすまし判定のロジックは共通化可能か（論点3-1：共通基準の策定）、どのようなプロセスで更新をしていくのか（論点3-3：共通基準の更新プロセス）、個社ごとのカスタマイズはどうするのか（論点3-2：個社カスタマイズの許容範囲）、について今後議論していく必要がある。例えば、共通ルールでなりすましが検知された場合、どのような対応をとるのかを個社ごとのルールで決定するということが考えられる。

■　KYC

KYCについては、オフライン確認およびオンライン確認ともに、犯収法施行規則6条1項の定めに沿って、本人確認を実施するため、個社によるカスタマイズ領域はなく、全社共通部分のみの提供となる。

尚、eKYCの共通基準については、本WGにて、証券業界として求められるeKYCソフトウェアの要件をITベンダーの有識者にて検討し、その内容をガイドライン（以下eKYCガイドライン）として取りまとめている。共通システムにおいても、eKYCガイドラインに沿った機能を提供し、算出される顔照合スコアを基に、事業者の判断で本人確認OKかNGを決定する想定である。

5.3.2. 導入・改善サポート

共通基準から個社の設定へのカスタマイズについては、これまでにAML/CFTシステムの導入経験がない会社にとってみれば、自社のリスク評価書を基に、どのようなリスクウェイト、ルールを設定すればいいのか分からず、人材・ノウハウ不足により有効な設定が困難なケースもでてくると想定している。

そのため、共通システムでは、各事業者の規模・特性に応じたロジックやルールなどのカスタマイズをサポートするとともに、各事業者の検知傾向や他社との比較結果などのレポーティングを行う。また、レポーティング結果や最新の犯罪収益移転危険度調査書などに合わせて、各事業者の設定の継続的な見直しもサポートする。これにより、単にAML/CFTをシステム化するだけでなく、その中で効率的にPDCAを回すことができ、AML/CFTの有効性・実効性が向上する効果がある。

尚、サポートをしていく上で、誰が（例えばAML/CFTエキスパートやAI）、どの範囲まで、どのようにサポートをしていくのかが今後の論点となると考えられる。（論点3-5：サポートの形態と範囲）

5.3.3. 事務代行

AML/CFTに関する業務についても、共通システム側で事務代行サービスを提供する。各社の事務を集約することで、スケールメリットにより各事業者の事務コスト削減の効果があると考える。また、共通システムで担う事務代行の方針は、以下の4点とする。

1) これまで人が担ってきた事務に関しては可能な限り共通システムで実施する
2) AIやRPAを活用し自動化を推進していく
3) 各事業者判断が必要な業務（新規受入可否判断等）についてはこれまで通り個社で実施する
4) 事務代行の証跡については共通システム上に記録し、委託元の事業者からいつでも参照可能とする

事務代行の対象業務について一例を表5-1に示すが、詳細な範囲については、上記の方針に基づき、今後議論して決定していく必要がある。（論点3-6：事務代行の範囲）

表5-1：共通システムで実施する事務代行（例）

業務	説明
本人確認	口座開設時の本人確認書類の真贋確認（画像/映像を目視）を実施。
フィルタリング （リスト照合）	本人特定事項を基に、反社DBや民間DB、共通システム管理リスト、個社リスト等への照会を実施する。 ※RPA・AIで自動化が可能 ※反社DB照会代行は金融商品取引業者のライセンス取得が前提
顧客に対しての 本人情報確認	継続的顧客管理措置における顧客への確認を実施する。 （電子メール、郵送等）
EDD（追加情報取得）	EDD（追加情報取得）が必要となった際、顧客へコンタクトをとり、情報収集を実施する。（電子メール、電話、追加調査等）
疑わしい取引候補の 初期調査	検知された疑わしい取引候補について、AIを活用し、取引のリスクスコア・予想届出確率・判定理由等を提示する。
疑わしい取引の報告	疑わしい取引の届出書を作成し、届出報告を代行する。

5.4. 「高度化」の概要と効果

「高度化」では、各事業者のデータを統合し各アプリケーションで活用するとともに、統合データを横断的に分析することにより、AML/CFTの高度化を実現する。以下で「統合データの活用」と「横断的な分析」に分けて説明をしていく。

5.4.1.統合データの活用

ここでは、各事業者のデータを共通システム上で統合する。統合したデータは、顧客リスク格付、取引モニタリング、本人認証といった各アプリケーションのインプット情報として活用し、高リスク顧客や疑わしい取引の検知率を向上させる効果があると考える。

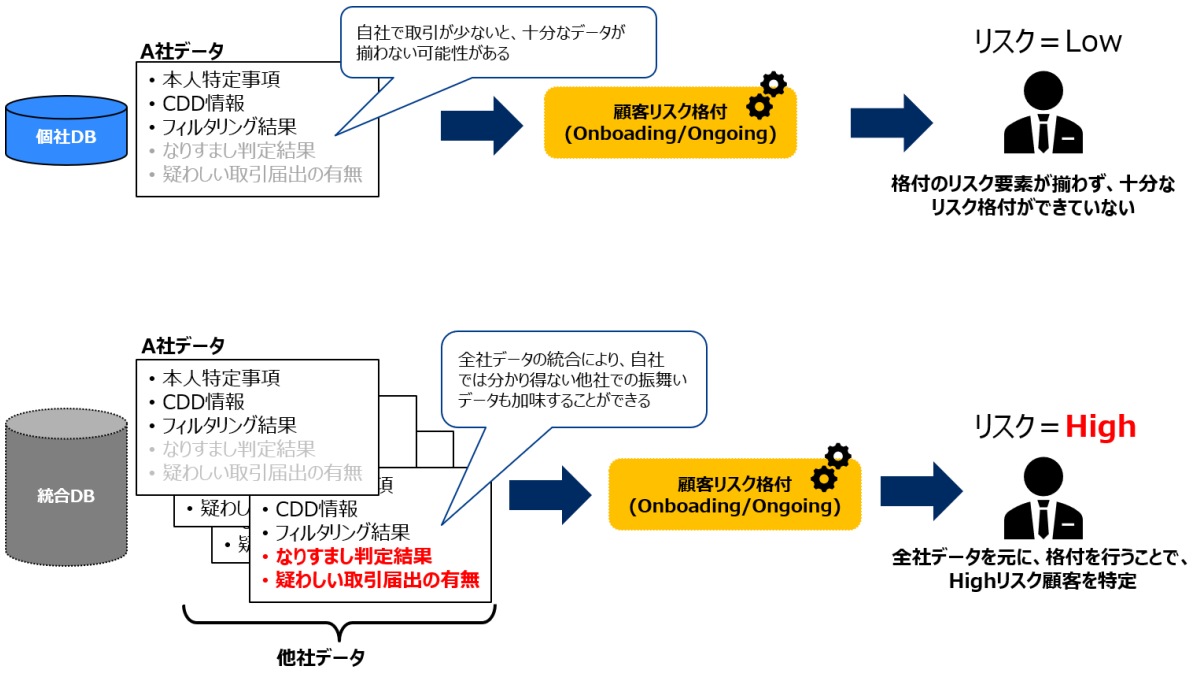
尚、データ統合における共通的な論点として、顧客の同意取得、およびデータの正確性の問題があると考えている。データを他社と共有する際には、どこかの場面で顧客からその旨の同意を取得する必要がある。（論点3-7：顧客への同意取得）また、万一統合されたデータの中に誤りがあり、例えば、そのデータを基に各事業者が顧客リスク格付を実行し、特定の顧客を金融業界から締め出すといった金融排除が発生した場合、責任の所在はどこにあるか、（論点3-8：誤データ共有時の責任の所在明確化）といったことに関しては別途検討する必要があると考えている。

以下、アプリケーションごとに、統合されたデータ活用の具体例を述べていきたい。

■　顧客リスク格付

自社で取引が少ない場合、十分なデータが揃わずリスク格付も不十分となることが想定される。そこで、全社データを統合することで、自社では分かり得ない、他社での疑わしい取引届出結果やなりすまし判定結果等も加味して、リスク格付が可能となり、結果としてリスク格付の精度が向上する。

図5-9：統合データ利用による顧客リスク格付例

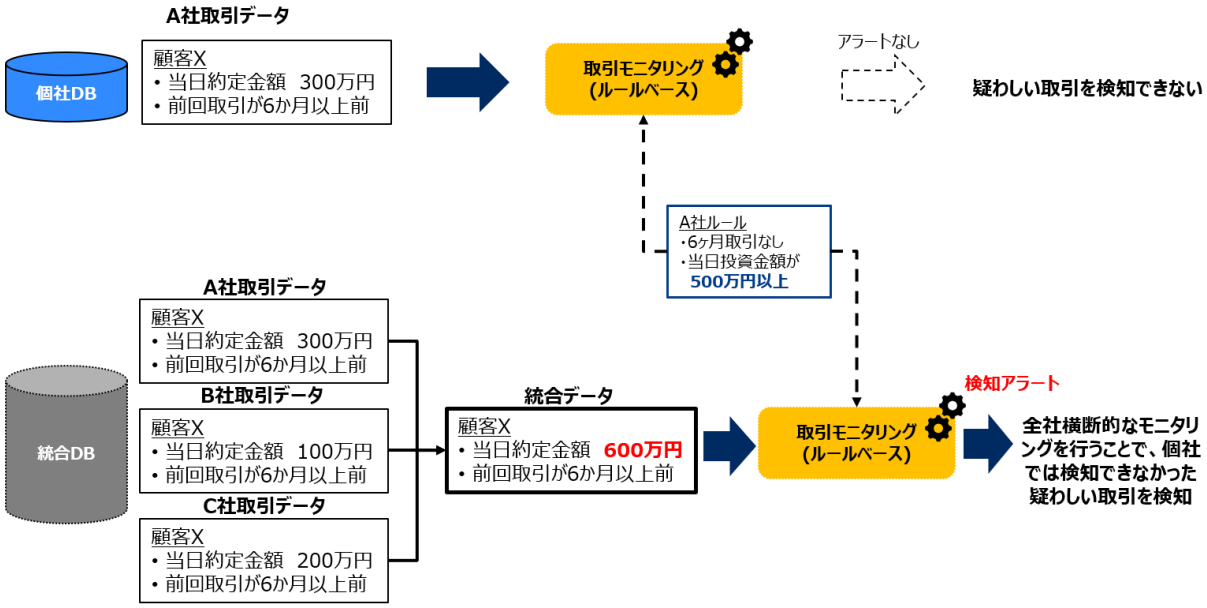


他社のデータを活用して自社の顧客リスク格付を実施する際、どこまでの情報を参照できるようにするか、は今後の論点であると考える。例えば、疑わしい取引届出であれば、届出の有無、および内容をどこまで確認できるのか、それに付随する取引データ等はどこまで参照可能なのか、もしくは参照できないようにするのか、については今後議論が必要となる。（論点3-9：他社データの参照範囲）

■　取引モニタリング

個社のルールでは閾値未満の取引金額ではあるが、複数社の取引を通算した場合は閾値を超える取引金額だったケースに備えて、各事業者の取引データを合算して疑わしい取引の検知をする、といった業界横断的なモニタリングが可能となる。結果、取引モニタリングの精度が上がり、個社では見抜けなかった疑わしい取引候補を検知することができる。

図5-10：統合データ利用による取引モニタリング例



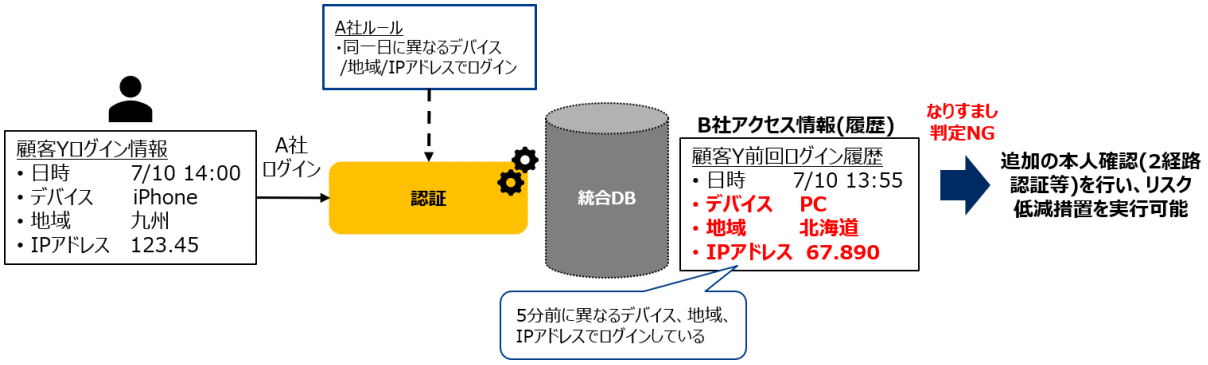
疑わしい取引の届出要否の判断、および届出理由の記載等には、活用した他社の取引データ等の参照が必要となってくる。上述の顧客リスク格付と同様に、どこまでの情報を開示するのか、は今後の論点となる。（論点3-9：他社データの参照範囲）

また、上記ケースの場合、当然疑わしい取引候補の検知アラートは、A社だけでなく、B社、C社へも同様に出されると想定される。そうなれば、疑わしい取引の届出は、全社から出されるべきなのか（その場合届出理由はどうするのか）、もしくは共通システムが代表して届出をすべきなのか、今後議論していく必要があると考える。（論点3-10：会社を跨いだ疑わしい取引の届出主体）

■　本人認証

統合データを使用することにより、例として、ある顧客がログインしようとした際に、直前にログインしている情報との差異（別のデバイス・IPアドレスで別の地域からのログイン等）を検知し、追加の本人確認を行う。複数社のアクセス情報を元にすることで、なりすまし判定の精度を向上させることが可能となる。

図5-11：統合データ利用による本人認証例



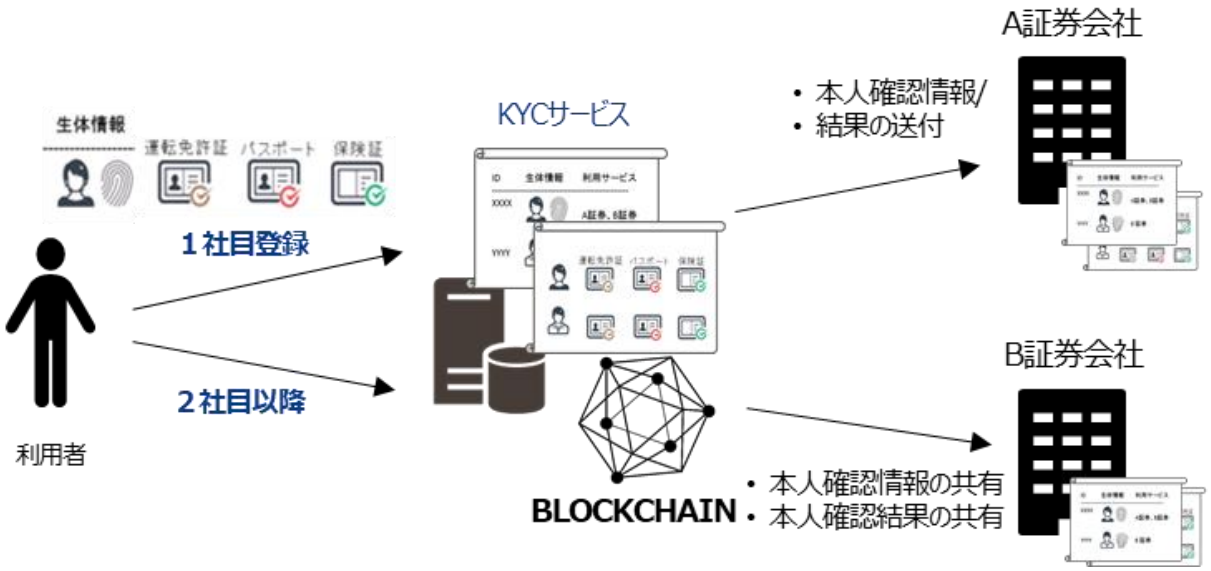
本人認証に関しても、顧客リスク格付・取引モニタリングと同様に、どこまでの情報を開示するのか、は今後の論点となる。（論点3-9：他社データの参照範囲）

■　KYC

新規顧客受入時の本人確認において、統合データベース上に存在する他社実施済の本人確認記録を参照する。本人確認における事務軽減によるコスト削減効果、および口座開設までの時間短縮による顧客CX向上の効果があると考える。

ここでのスキームは、2018年7月に公表された日本取引所グループによる「ブロックチェーン/分散型台帳技術に関する業界連携型の技術検証」の場を利用して実施した、ブロックチェーン技術を活用した業界初の顧客確認業務の実証実験が参考になると思われる。また、本WGにおいても、キックオフ当初から、図5-12に示したようなブロックチェーンを活用した本人確認情報および結果の共有について、議論を重ねてきた。

図5-12：本人確認情報･結果の共有



本人確認情報および結果の共有を実現するに当たっては、情報共有の範囲をどこまでにするか、ということが論点となる。単に、本人特定事項や、本人確認用画像情報に留めるのか、適合性の原則に関わる取得項目を含むCDD情報も共有するのか、については、今後の議論により決定する必要があると考えている。（論点3-11：KYCに関わる情報共有の範囲）

また、法的観点からみた本人確認記録の共有の可否は、犯罪収益法の施行規則13条の解釈が必要である。施行規則13条2項を参照すると、クレジットカード等に関してのみ記載がある。（施行令13条は限っていない）。また、他の特定事業者に委託する場合は、他の特定事業者自身がその後の取引時確認を全て行わなければならないという条文がある。他社の確認記録の依拠の可否は、引き続き監督官庁への確認が必要である。（論点3-12：本人確認結果の共有）

5.4.2. 横断的な分析

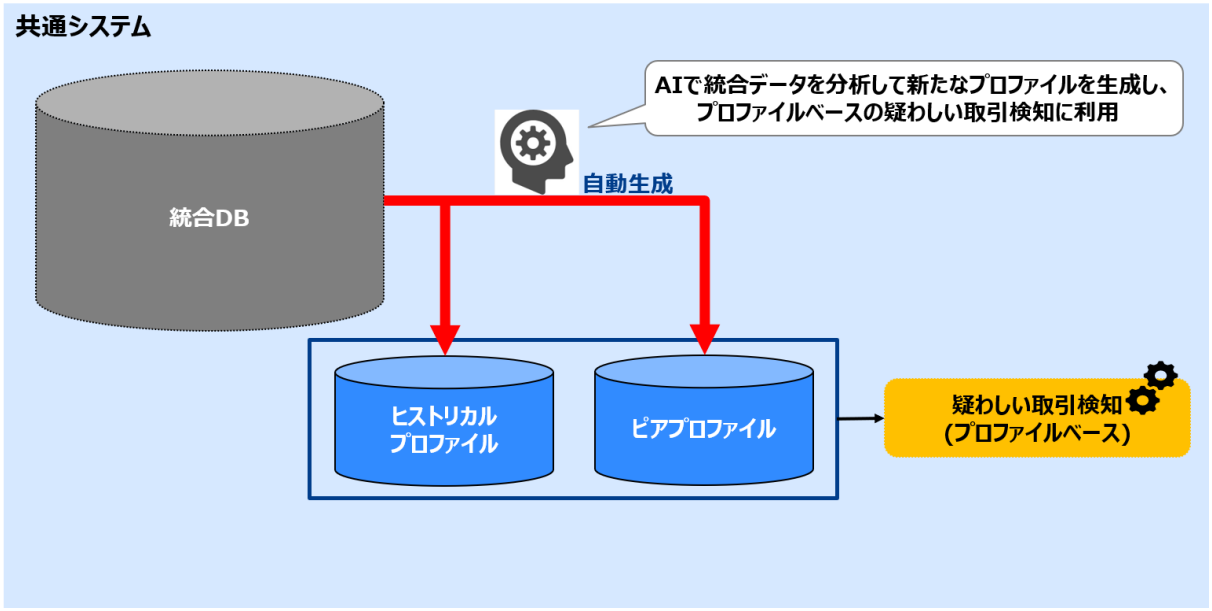
統合データ、すなわち業界全体のデータをデータベース上でAIを活用し横断的に分析することにより、顧客プロファイルや新たな検知ルールの抽出が可能と考えられる。それにより、検知精度の向上が期待できるほか、共通システムで提供する共通基準のPDCAを回すことができ、有効性・実効性の向上も期待できる。

それぞれについて、具体例を交えながら述べていきたい。

■ 取引モニタリング：プロファイル生成

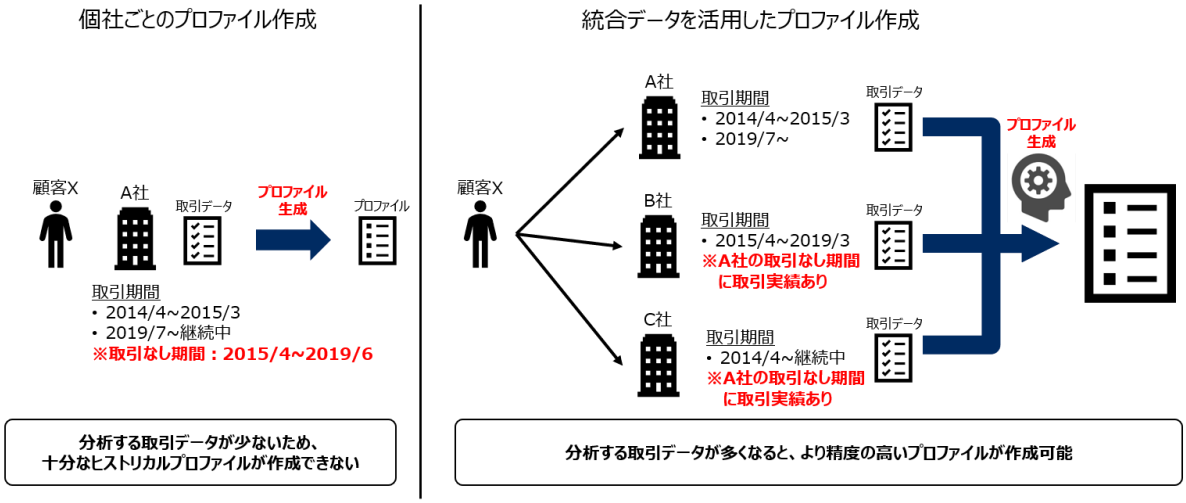
ヒストリカルプロファイルとピアプロファイルが存在し、どちらの生成にも一定以上のデータ量が必要であるとともに、データ量が多ければ多いほど、モニタリングの精度向上の可能性は高くなる。個社ではデータ量が十分ではなく、各顧客の傾向がデータ上でつかめない、またはプロファイルを生成できない、といった場合もある。そこで、統合データを、AIを活用して分析することにより、個社データよりも精度の高いプロファイルを生成することができ、結果としてモニタリング精度の向上が可能となる。

図5-13：統合データの分析による取引モニタリングのプロファイル生成



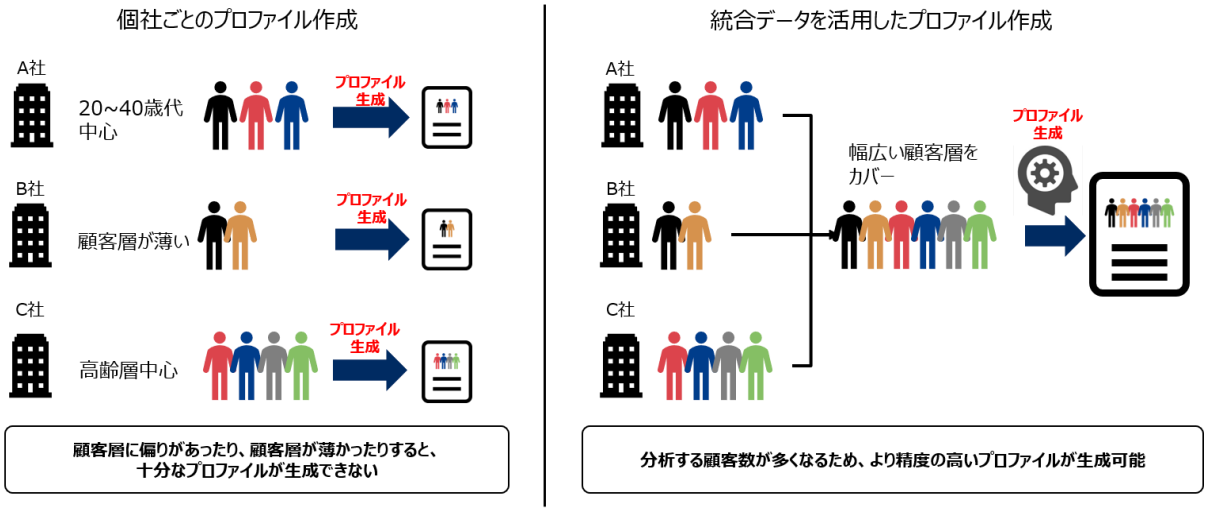
ヒストリカルプロファイルに関しては、顧客に関わるデータ量が重要となる。そのため、顧客が口座を有している会社が多ければ多いほど、データは集まりやすくなる。

図5-14：プロファイル生成のためのヒストリカルデータの統合および分析



ピアプロファイルに関しては、顧客数が重要となる。そのため、顧客数の多い会社が参画することでデータは集まりやすくなる。

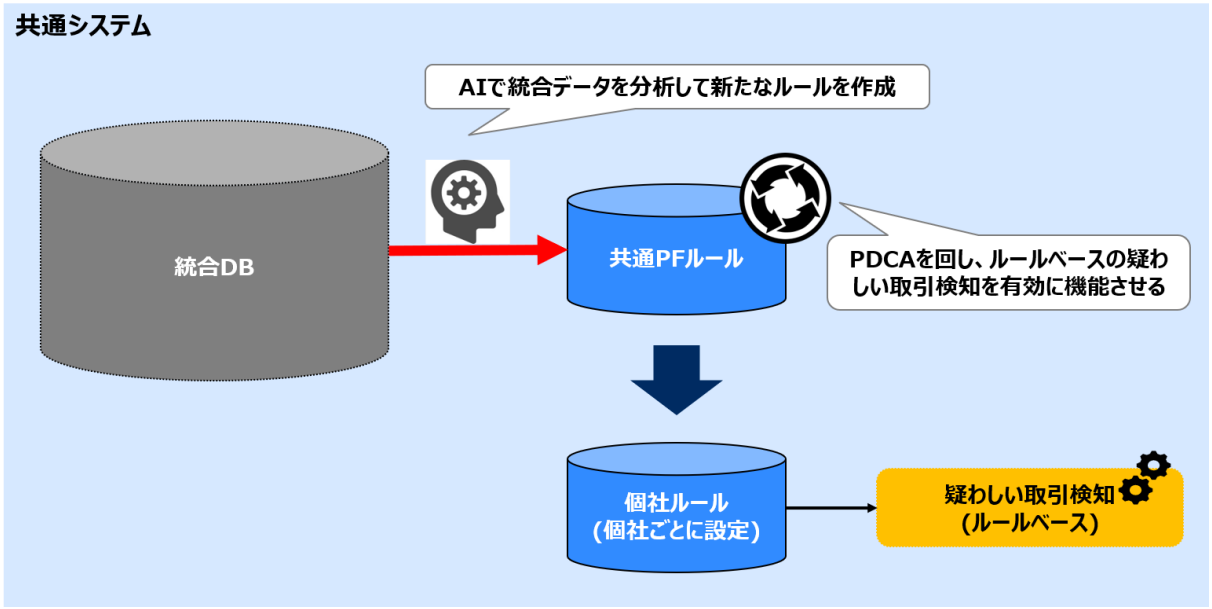
図5-15：プロファイル生成のためのピアデータの統合および分析



■　取引モニタリング：ルール抽出

AIを活用し、統合データから各事業者の疑わしい取引のパターンを学習し、規則性を抽出。その抽出結果から、新たな検知ルールを策定し、共通ルールに反映させることを想定している。その結果として、全社の取引モニタリング精度の向上が期待できる。

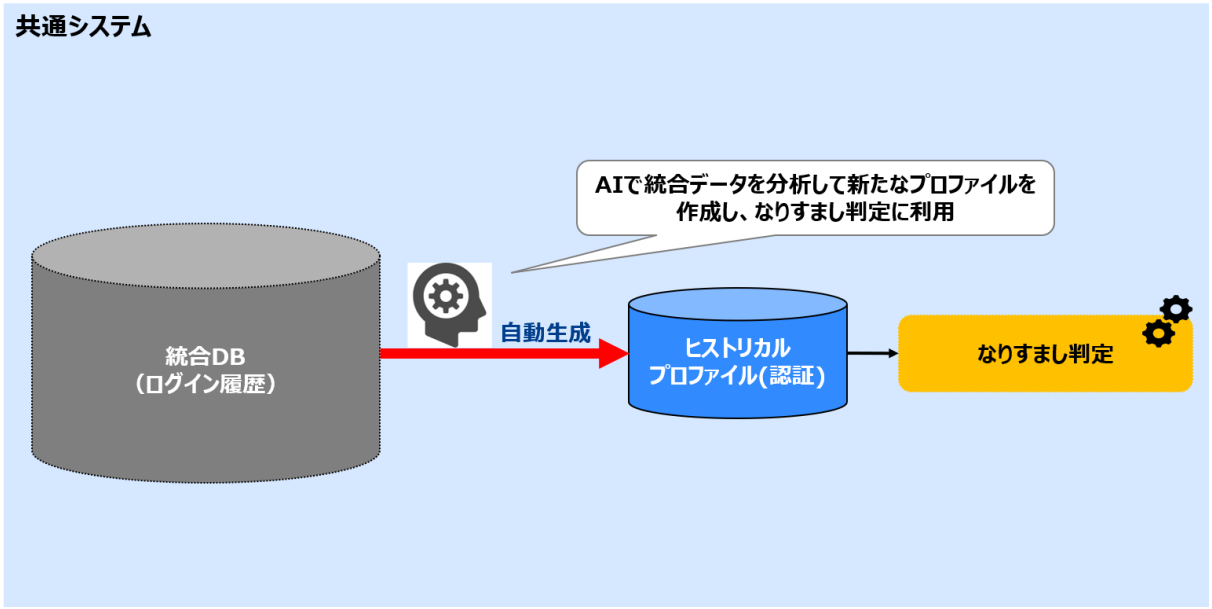
図5-16：統合データの分析による取引モニタリングのルール抽出



■　本人認証：プロファイル抽出

本人認証においては、ヒストリカルプロファイルが存在し、その生成には取引モニタリング同様に、一定以上のデータ量が必要である。そこで、各事業者のデータをした上で、AIを活用して分析することにより、本人認証の精度向上が可能となる。

図5-17：統合データの分析による本人認証のプロファイル生成



5.5. 実現に向けた論点整理

本章ではこれまで、「証券業界におけるAML/CFTの共通化、高度化」について、本WGで想定している概要と効果を述べてきた。本項では、これまでの検討の中で更なる議論が必要だと考えた点、その他今後の検討を進めるうえでの論点について整理する。

1) 「サービス提供」に関する論点

共通システムを通じた各種サービス（AML/CFTシステム、導入・改善サポート、事務代行）について、証券会社に対して誰がどのようにサービスを提供するのが望ましいのか、これまで本WGで検討してきた論点について、下表の通りまとめる。

No.	論点	詳細
1-1	提供主体	本WGでは、サービス提供主体となりうる事業体の設立の必要性について、継続的に議論している。事業形態については、意思決定の速さと中立性、事業の継続性考慮し「株式会社」または「合同会社」が候補として挙がっている。
1-2	出資者	本WGの枠組みと同様、証券会社だけでなくITベンダーも参画する想定でいる。また、必要な人材の確保については、出資企業の中から適切な人材の協力を得ることで、業務面、システム面それぞれで高度な人材を集めることが可能である。
1-3	参加金融機関	中立性を保つためには、複数の証券会社が経営に関与していることが望ましい。
1-4	サービス形態	事業体が証券会社に対して、従量課金制のサービスを提供することを想定している。また、データ統合による高度化への貢献度に応じたインセンティブ設計も必要と考えている。
1-5	権利関係	共通基準や、統合データの分析によりAIが生成したプロファイルや検知ルールについて、証券会社側と共通システム側のどちらが、著作権および所有権を保有するのか、事前の取り決めが必要となる。

2) 「システム」に関する論点

AML/CFTの共通化・高度化を実現するための共通システムの構築における、方針や実現方法について、これまで本WGで論点として挙がったものを、下表の通りまとめる。

No.	論点	詳細
2-1	クラウドの利用	国内の金融機関では、すでに基幹システム等のクラウド移行が進んでいる。また、米国では多くの機密情報を取り扱う政府機関でも、当然のようにクラウドを利用している状況である。可用性やコスト削減を実現するには、クラウド化が適していると考えている。
2-2	可用性の担保	KYCや本人認証については、顧客自身が利用するシステムとなるため、可用性が重要な要素となる。クラウドの利用により一定レベルの可用性は担保されるものの、特定のクラウド環境に依存し、そこで障害等が発生した場合、業界全体に影響を与える可能性がある。そのため、マルチクラウドの活用による冗長化を想定している。またマイクロサービスについても、各機能をコンテナ化することで、可用性と運用性を担保する想定。
2-3	セキュリティの担保	共通システムは取扱うデータ量が多く、情報漏洩時のリスクが単独企業でのそれと比較して高い。最新の入口・内部・出口対策に加え、定期的なセキュリティ診断の実施が必須である。また、各事業者間でKYC結果等の共有をするための基盤において、第三者によるデータの改ざんを防止するため、対改ざん性の高いブロックチェーン等の活用についても検討を進めている。
2-4	各社の既存AMLシステムとの連携について	共通システムの前提として、各社のAMLシステムと共存させるのではなく、共通システムのみで完結させる想定で記載している。 しかし、事業者によっては既存AMLシステムと共存させたいという要望があると想定される。そのため、共通システム上の各個別機能をAPI提供し、各社システムと連携可能な設計とする必要がある。

No.	論点	詳細
2-5	データ統合	① データ統合の手法 顧客データの統合には、複数の証券会社に口座を持つ顧客を特定し、同一顧客を紐付ける必要がある。そのための手法として、以下の２つが考えられる。 1) 各事業者の顧客マスタを対象に名寄せを実施し、同一顧客を特定したうえで、共通IDを付与 2) マイナンバー等の活用による同一顧客の特定 しかし上記の実現については、個人情報保護法の観点やマイナンバー法の観点で障壁がある。また共通ID等で管理した場合も、完全に「なりすまし」を防止するのは難しいため、ふるまいデータ等から関連性を分析し、同一顧客である可能性を分析するなどして、補完する必要がある。 ② データフォーマット 取引データについては、各事業者の基幹システムからデータを収集する必要があるが、データフォーマットが事業者間で異なると想定される。そのため、データ収集時はデータフォーマットの統一が必要となる。フォーマットを合わせた場合でも、各事業者で保有するデータ項目、粒度が異なり、真に必要な情報を揃える事が困難と想定され、補完方法等の検討が必要である。 ③ データアクセス権 データ統合の目的はAML/CFTの高度化であり、データ提供によってその会社が不利益をこうむるような事があってはならない。よって、参照可能なデータについては厳密に定義し、それを管理する仕組みの構築が必要である。現時点では、データの参照権限および、各サービスの権限設定等については、独立的な第三者による運用体制の構築を想定している。 ④ 統合データベースの論理設計 統合データベースについては、物理的に統合するパターンと、仮想的に統合するパターンが考えられる。それぞれのメリット・デメリットを整理し、今後検討していく必要がある。

3) 「業務」に関する論点

AML/CFの共通化・高度化を実現するための業務について、5章の中で論点として挙がったものを、下表の通りまとめる。

No.	論点	詳細
3-1	共通基準の策定	① 顧客リスク格付 リスク要素については業界で共通化し、リスクウェイトを個社で設定可能とする想定であるが、規模や商品ラインナップ、チャネル等が異なる会社間でリスク要素を固定することが可能なのか。 ② 取引モニタリング 入出金については、共通的なルール作成が可能と想定されるが、商品・サービスは各事業者で多種多様なため、どこまで共通的なルールを策定できるかは、検討が必要となる。 ③ フィルタリング 共通リストの範囲に関しては、今後議論の上決定する必要はあるが、現状各事業者がカバーしている国内・域外適用のリストを定義すれば、共通システムでの作成および管理は可能と考える。 ④ 本人認証 なりすまし判定ロジックについては、個社によって差異が発生しないと想定されるため、共通化可能と考える。しかし、なりすまし判定後の、追加認証の方法については、個社によってカスタマイズ可能な設定にするなどの考慮が必要。
3-2	個社カスタマイズの許容範囲	論点3-1で定めた基準から自社の設定をカスタマイズする場合、AML/CFTの底上げのためには、閾値の設定範囲については制限を設ける必要があると考える。
3-3	共通基準の更新プロセス	それぞれの基準について、更新プロセスと更新頻度を定義し、水準の維持を担保する必要がある。
3-4	個社リスト（イエロー・ブラックリスト）の共有	個人情報保護法の観点で、個社リストの共有の実現は難しい。信頼性や緊急性が高い情報については、共有化可能とするなど検討の余地はあると考える。
3-5	サポートの形態と範囲	事業体のビジネスモデルと提供価値を再定義した後、検討予定。

No.	論点	詳細
3-6	BPOの範囲	既にBPOを利用している事業者も多いため、共存できる余地があるか検討が必要。
3-7	顧客への同意取得	個人情報の共有については、事業体と証券会社及び顧客との関係性によって、必要な手続きや、留意すべき事項が異なる。 顧客に同意が必要な場合は、口座開設時などに同意を取得することが考えられるが、既存顧客全てから同意を取得するための方法については検討が必要。
3-8	誤データ共有時の責任の所在明確化	データ統合には、データの正確性が前提となる。例えば、統合データの中に誤りがあり、そのデータを基に各事業者が顧客リスク格付を実行し、特定の顧客を金融業界から締め出すといった金融排除が発生した場合、責任の所在はどこにあるか、等の懸念点を考慮に入れた上での検討が必要。
3-9	他社データの参照範囲	他社のデータを活用して自社の顧客リスク格付を実施する際、どこまでの情報を閲覧できるようにするか（例えば疑わしい取引届出結果であれば、届出の内容はどこまで確認できるのか、それに付随する素データ等はどこまで参照可能なのか、もしくは参照できないようにするのか）、個人情報保護法の観点や各事業者のポリシー等を確認したうえで、共有可能な情報の範囲の整理が必要。
3-10	会社を跨いだ疑わしい取引の届出主体	データ提供元の事業者の一方または両方が疑わしい取引の届出をすべきか、または、事業体側で届出をすべきか、当局とも連携の上検討が必要。
3-11	KYCに関わる情報共有の範囲	本人特定事項、本人確認用画像情報、CDD情報等のどこまでを共有するか。 個人情報保護法の観点に加え、3-12の通り犯罪収益移転防止法の観点でも留意が必要。また、共有する場合については、各事業者で取得する情報の種類・粒度の統一と、有効期限の定義が必要。
3-12	本人確認結果の共有	本人確認記録の共有の可否は、犯罪収益法の施行規則13条の解釈が必要である。他社の確認記録の依拠の可否は、引き続き監督官庁への確認が必要である。施行規則13条2項を参照すると、クレジットカード等に関してのみ記載がある。（施行令13条は限っていない）。施行例13条2項において、他の特定事業者に委託する場合は、他の特定事業者自身がその後の取引時確認を全て確認しなければならないという条文がある。他社の確認記録の依拠の可否は、引き続き監督官庁への確認が必要である。

5.6. 実現にむけて優先的に取り組むべき事項

5.5節では、共通システムを活用したAML/CFTの「共通化」「高度化」の実現にむけて、「サービス提供方法」「システム」「業務」の観点から論点整理をおこなった。実現にあたっては、これら論点の解決に加えて、共通化および高度化の「フィージビリティ検証」や「効果検証」の実施が必要と考えている。特に、データ統合およびAIを活用した横断的な分析については前例がないため、十分な検証を実施する必要がある。実現にむけて優先的に取り組むべき事項として、以下に2点を整理した。

1) 共通システム/共通事務のフィージビリティ検証
2) 統合データの活用・分析による高度化の効果検証

1) 共通システム/共通事務のフィージビリティ検証

現状、証券会社のAML/CFTに関するシステム化の対応状況は様々であり、システム化が対応済みの事業者もあれば、検討前の事業者も存在する。システムの共通化は、AML/CFT水準の底上げと同時に、コスト削減も目的としているが、現状の対策状況によっては、既存の投資分の回収が済んでおらず、コスト削減が実現できない事業者が存在すると想定される。共通システムが持続的に運営可能となるよう、事業モデルやプランの早期策定をおこなうとともに、業界全体でメリットを享受できる運営体制を整えることが必須である。

2) 統合データの活用・分析による高度化の効果検証

「データ統合」および「横断的な分析」による高度化については、ここまで期待される効果を記載してきたものの、あくまで仮説段階であり、フィージビリティの検証ができていない。特に検証が必要な内容は、「AIを活用した横断的な分析」の効果である。想定している主な懸念点は、以下の2点が挙げられる。

- 分析対象のデータが多すぎると全データの分析に時間がかかるため、サンプリングが必要となる。サンプリングの仕方によっては精度が出ない可能性がある。
- 単一の金融機関のデータのみでモデルを作る場合は、その金融機関の特性を学習できるが、全体のデータで学習すると１金融機関の特性は反映されず、精度が出にくい可能性がある。

（空白のページ）

6.

おわりに

本章では、5章で述べたAML/CFT態勢高度化に関して、WGでの検討を通じて得られた課題、論点を改めて振り返り、加えてAML/CFT態勢高度化にむけた新技術の活用について言及する。なお、本章はWGのプロジェクトマネージャーである日本電気株式会社（以下、「NEC」という）の担当者による見解である。

AML/CFT共通システムの検討に至る背景

FATFによる第4次対日相互審査のオンサイト審査を今秋に控える中、金融庁を含む関係当局は、金融機関が審査をスムーズに対応できるよう、強い危機意識をもって様々な施策を講じており、2018年には態勢の整備と高度化を支援するために金融庁ガイドラインを公表している。本WGは、そのような状況の中で設立されており、WG参画企業のAML/CFTに対する関心は非常に高かった。

国際社会がテロ等の脅威に直面している中、金融システムの安定性と正常な経済活動を維持し続けていくためには、日々変化するML/FTの動向にすべての金融機関等が機動的に実効性を伴って対応することが重要であり、金融庁ガイドラインに沿ったリスクベース・アプローチの導入をミニマム・スタンダードと捉え、実践していくことが必要である。AML/CFT対策に抜け穴がある事業者の存在は、金融システム全体へのレピュテーションリスクに繋がる恐れがあるため、規制強化の対応は個々の事業者だけで閉じることなく業界全体で取り組むべき課題といえる。

NECが実施した金融機関等へのヒアリング[10]の結果では、AML/CFT態勢整備状況は各事業者でまちまちであり、規模の大きい事業者ほど金融庁ガイドラインをふまえた自社対応を網羅的かつ積極的に進めている様子であった。その反面、事業者によっては、金融庁ガイドラインが求める最低限の要件を満たしてはいるものの、リスク格付けや取引モニタリング等について十分な対応がなされていないという課題認識をもつケースもあった。各事業者ともに、AML/CFT規制強化の流れに多大な負担を強いられているため、その軽減を企図し、金融庁からも一定の理解が得られる標準的な仕様を満たした業界共通的なシステムが存在する事への期待感は高い。こうした背景から、本WGではAML/CFT態勢高度化の一つの方策として、AML/CFTに関するシステムの共通化や共通基準に則った事務の代行、顧客に関するデータの集約・分析・活用をおこなうことについて検討した。この構想に対するWG参画企業の主なコメントは以下であった[11]。

- ✓ 金融庁ガイドラインが求めることを満たすには、既存のAML/CFTパッケージ等の活用で自社対応は可能。一方、低コストの業界共通的なシステムが存在することは意味がある。
- ✓ 法改正などにより、金融庁から追加対応が求められる際、業界共通的なシステムがその役割を担ってくれると嬉しい（WGのソリューションが、適宜アップデートされるのであれば意味はある）。
- ✓ データ集約・分析について、構想としては良いと感じるが、本当に価値があるのか十分な検討が必要。一方、個人情報の問題やデータフォーマット等ハードルは高そう。
- ✓ WGでの検討結果が業界標準となり、WGのソリューションがそれを満たすのであれば、価値があると思うし、現状から乗り換える余地は十分にある。金融庁も巻き込んで各社足並みを揃えれば検討の余地はある。

[10] KYC共通化WG活動の一環として、2019年4月～５月ごろ実施

[11] KYC共通化WG 第8回全体会にて報告

検討を通じて浮かび上がった課題

システム共通化は、AML/CFT規制強化への対応を業界の非競争領域と捉え、事業者単独で閉じることなく、事業者規模や業容に応じつつも、財務的に負担の大きい中小事業者も含め一定コストで一定のリスク対応水準を維持できる仕組みの構築を目指すものである。また、当該システムを基盤とした顧客に関するデータの集約・分析・活用は、事業者単独では見抜きづらい高リスク顧客や疑わしい取引の検知を実現し、より高度で実効的なAML/CFTを実現することを目指すものである。WGは、それらの実現によって、AML/CFTに係る各事業者の業務（コスト）負担軽減と規制対応水準の高度化、さらには手続き負担軽減による顧客の利便性向上を大きな目標として掲げた。

今回の検討結果から明らかになったのは、構想の実現には、サービス運営面、システム面、オペレーション面のそれぞれで、法制度観点をはじめとした様々な観点でのさらなる整理や解決すべき論点が多数存在することである。特に、顧客に関するデータの集約・分析・活用においては、要配慮情報の取り扱いについて慎重な検討を行う必要がある。図6-1に、個人情報を取り扱う際の金融機関で発生する義務と要件をまとめた。金融機関が情報を取り扱う際には、情報取得、情報保持・活用、情報提供の３つの場面で義務と満たすべき要件が発生するとされている。今回の構想では、金融機関が保持するデータの集約先としての主体が存在しており、かつデータ分析結果情報を金融機関間で共有することも検討対象となっている。構想の実現には、こうした前提条件を詳細に整理した上で、論点整理を行う必要がある。

図6-1：個人情報の取り扱いで発生する義務・要件[12]

12 金融庁等の公開情報をもとに、NECが独自作成

AML/CFTに関連する情報の共有は、不正な取引に対して複数の事業者が協力して検討・対処することを可能とするため、金融システム全体としてAML/CFTの実効性を高める意味で意義があると言える。

金融機関同士でのAML/CFTを目的とした情報共有の事例は本邦ではまだないが、本邦外における動向を図6-2にまとめた。アメリカやイギリスでは、すでに民間金融機関同士などでの情報共有の取り組みが存在しているようである。また、図 6-3に各国のAML/CFTおよび個人情報関連の規制をまとめた。民間同士の情報共有をする上では、主に個人情報関連法規との対立が問題となるが、本邦での実現に際しても関連法制度や要件をどのようにクリアしていくべきか整理が必要である。

図6-2：本邦外におけるAML/CFT関連情報共有についての動向[13]

	関連法規	情報共有主体	情報共有の経緯	共有内容
	愛国者法314(a)	公共セクターと民間金融機関	2001年より、テロ組織等を念頭に情報共有ネットワークを構築	• 10の犯罪行為の検知に有用な情報の共有 – 例）マネーロンダリング、汚職、麻薬取引、人身売買等
	愛国者法314(b)	民間金融機関同士	• 金融機関は、テロリスト・マネーロンダリング活動に関して当局に報告するため、他の金融機関に対して関連する情報の送信、受信、又は共有可能 • 2015年より、アメリカの主要銀行グループが民間の情報共有に関するパートナーシップを締結。提携する金融機関数は、2014年から2018年末時点で2倍に増加	
	The UK Circular 007/2018 on the Criminal Finances Act	公共セクター・民間金融機関同士	2018年より、民間金融機関同士の情報・不正検知レポーティングの共有開始	（詳細は明らかにされていない）
	現時点で民間同士では、情報共有はない様子			

13 公知の情報等をもとに、NECが独自作成

図 6-3：各国のAML/CFTおよび個人情報関連規制[14]

1. 非公開個人情報とは、①個人を特定する情報で、②顧客本人自身が金融機関等に提供したもの、③金融機関等が顧客との取引の際に得たもの、または④金融機関が取得したもの例）金融商品の購入やサービスを受けるために必要な個人に関する全ての情報（氏名、住所、電話番号、社会保障番号(social security number)等）、金融機関等の顧客であるという事実、顧客の口座番号や口座の残高に関する情報

14 公知の情報等をもとに、NECが独自作成

実現にむけた進め方

一方で、AML/CFT規制強化への対応は喫緊の課題である。今回検討した構想の完全な実現には、5.5節で触れたように多くの解決すべき論点があることから、短期と中長期の視点でロードマップを描き、ステップを区切って出来ることから段階的に実現していくことが現実的であると考えられる。一つの考え方としては、図6-4に示すように「システム要件の標準化」と「CDD情報の共有化」に分け、それぞれで検討を進めるアプローチがあり得る。これを前提として、たとえば、図6-5に示すように、時間軸ごとに「技術的に対応可能で、できていないこと」、「技術的に対応可能だが、リーガルな障壁があってできないこと」、「先進技術で対応可能なこと」の三つの観点に分けて課題を整理し、それぞれの時間軸で実現を目指していくことが一つの進め方となるだろう。

図6-4：システム要件の標準化とCDD情報の共有化について

「システム要件の標準化」とは

1. 業界が**共通的に参照できるAML/CFTガイドラインを制定**することで、システム標準化をおこなう（一定のリスク低減水準を担保する）
2. システムのスコープは、**AML/CFTに関する各機能システム**が対象
   ⇒ KYCフィルタリングシステム、 顧客リスク格付システム、 取引モニタリング・フィルタリングシステム
3. 事業者は個々に、マイクロサービス的に必要に応じた形で選択して利用する
4. 各個別システムに付随する業務は、運用主体がアウトソースとしてサービス提供
5. 各機能システムに必要なロジックは、運用主体が管理する「共通ロジック」と、運用主体が事業者から委託を受けて管理する「個別ロジック」からなる
   共通ロジック：業界共通化可能なもの
   ⇒ KYCフィルタリングで利用する共通リスト、取引モニタリング・フィルタリングで利用する共通プロファイリング情報（検知ルール）
   個別ロジック：各事業者でカスタマイズが必要なもの
   ⇒ 顧客リスク格付けルール（リスクウェイト）、照合リスト（個社独自のイエロー/ブラックリスト）、
   取引モニタリング検知ルール、なりすまし判定ルール
6. 各事業者は基盤側の共通ロジックを基礎として、自社のリスク評価方針に沿った個社ロジックを設定。業界としてAML/CFTの一定水準担保を図る。

「CDD情報の共有化」とは

a. 各事業者が有する**CDD情報をシステム基盤で集約**し、分析結果を共有することで、リスク低減措置を行う
b. 基盤では、各事業者共通の顧客を識別し、顧客リスク格付けや取引モニタリングに掛かる情報を集約する
   これを基盤側で分析することで、共通ロジックにフィードバックしたり、疑わしい取引やなりすまし判定の判断材料として個別ロジックに反映したりする
c. 上記手段の一つとして、**各事業者がもつCDD情報の最新性維持を基盤側で受託**する

図6-5：AML/CFT態勢高度化にむけたロードマップ（例）

実現のスパン	短期 （～１年）	中期 （１～３年）	長期 （３年～）
実現すること	**技術的に対応可能で、 できていないこと**	**技術的に対応可能だが、 リーガルな障壁があってできないこと**	**先進技術で 対応可能なこと**
具体例	・**システム要件の標準化** 業界が共通的に参照できるAML/CFTガイドラインを制定することで、システム標準化をおこなう（一定のリスク低減水準を担保する） →AML/CFTに関する各機能システム（KYCフィルタリングシステム、顧客リスク格付システム、取引モニタリング・フィルタリングシステム）の標準化をおこなう	・**システム共通化と運用主体設置** 事業者は個々に、マイクロサービス的に必要に応じた形で選択して利用。各個別システムに付随する業務は、運用主体がアウトソースとしてサービス提供 →リーガルな障壁はサンドボックスを使うなどして検証していく	・**CDD情報の共有化** リスク低減措置の高度化のため、各事業者が有するCDD情報をシステム基盤で集約し、AIなどを駆使して分析結果をセキュアに共有する →リーガルな障壁はサンドボックスを使うなどして検証していく

なお、短期的視点で見ると、実務レベルでは、ローテクではあるものの、単に仕組みを整えるだけで実効的な運用が可能となる場合もある。事業者の中には、その事業規模やリソースの制約などによって、ローテクで改善可能な部分のあぶり出しや課題抽出が上手く行われていない実態もあるという。システム要件の標準化の検討においては、「金融庁ガイドラインが求めるRBAを実現する」という観点からだけではなく、実際の現場実務レベルでの実態もきちんと踏まえながら、理想的な運用を行うために、どのような施策があり得るのか事業者同士で十分な課題の洗い出しをおこない、知見を共有することが必要と考える。この過程で、事業者単独で先行して対応可能な施策が浮かびあがることも考えられる。

AML/CFT態勢高度化にむけた新技術の活用

近年、AML/CFT規制強化への対応としてビッグデータ解析や、機械学習・ディープラーニングなどのAIを活用する“RegTech”が注目されている。金融庁ガイドラインでもリスクベース・アプローチの取組みの一環として、FinTech等の活用に言及している[15]。

> （５）FinTech 等の活用
> マネロン・テロ資金供与対策においては、取引時確認や疑わしい取引の検知・届出等の様々な局面で、AI（人工知能）、ブロックチェーン、RPA等の新技術が導入され、実効性向上に活用されている。
> こうした新技術のマネロン・テロ資金供与対策への活用は、今後も大きな進展が見込まれるところであり、金融機関等においては、当該新技術の有効性を積極的に検討し、他の金融機関等の動向や、新技術導入に係る課題の有無等も踏まえながら、マネロン・テロ資金供与対策の高度化や効率化の観点から、こうした新技術を活用する余地がないか、前向きに検討を行っていくことが期待される。

こうした注目の背景の一つとして、識者からは以下のような見解が挙げられている[16]。

> 膨大な金融トランザクションの中に潜むAML/CFTのリスクを、人海戦術で特定するのは、既に難しくなっています。やはりそこは効率性と正確性をもって自動的にリスク検知とレベル判定ができるような仕組みがないと実効性が得られません。そのためのソリューションとしてRegTechの活用は必然だと思います。
>
> 例えば、KYC（Know Your Customer）の原則を踏まえた本人確認（取引時確認）を経た後の取引モニタリングで、いつもとは違う取引先へ膨大な額の送金が行われている、小口取引の頻度が多すぎるといった判断が行えるのは、トランザクションの回数が増えるほど、その顧客の振る舞いを細かい粒度で分析し、AIなどで重み付けし、理解できるからこそです。
>
> これまでは、取得してきた情報の重み付けやパラメータ設定は、審査担当者などが時間をかけた手作業で行っていました。そこに例えばディープラーニングを適用すれば、正しい報酬系の設定により、システム自身が学習して賢くなり、より高い精度とスピードで不正な金融取引を検知して止めることができるようになります。それは顧客に対しても、取引の安全性と利便性を担保し、ファイナンシャル・インクルージョン、つまり“誰もが取り残されることなく金融サービスにアクセスでき、金融サービスの恩恵を受けられる”ようにすることで適切なサービスを維持するための突破口にもなるでしょう。テクノロジーを使ってリスクをコントロールできるRegTechは、AML/CFTの規制強化対応に非常に有効だと思います。

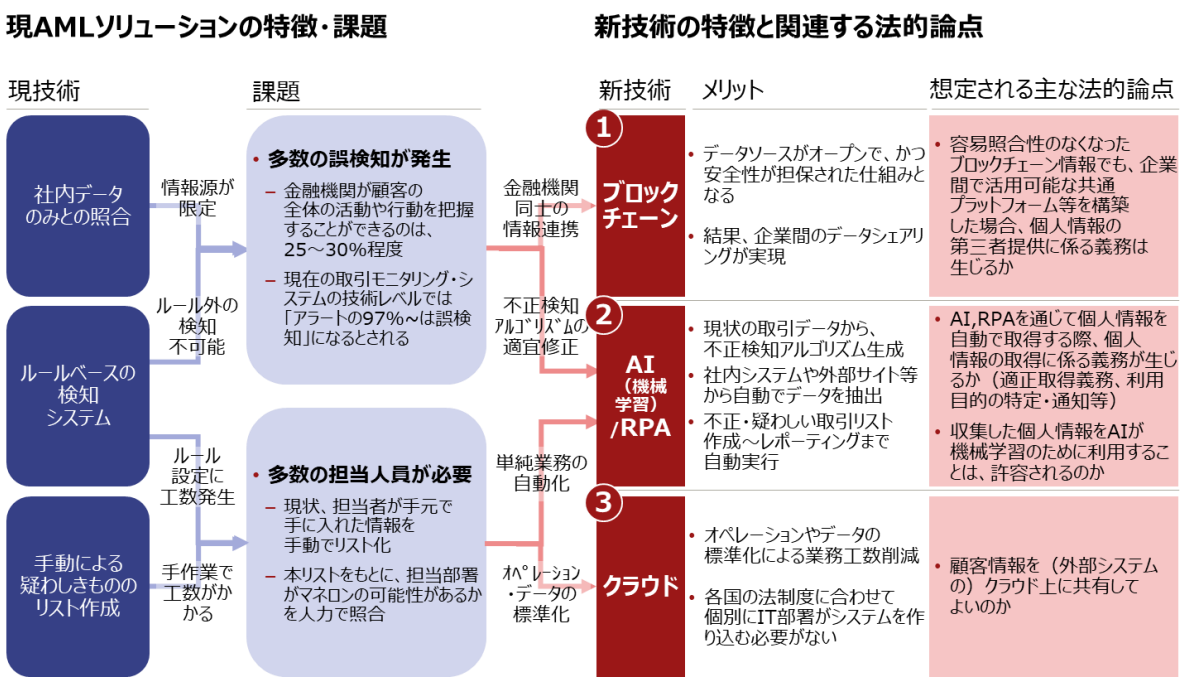
[15] 金融庁ガイドライン（P.22）より引用
<https://www.fsa.go.jp/common/law/amlcft/amlcft_guidelines.pdf>（最終閲覧日：2019.9.30）

[16] wisdom「10分で理解するFATF勧告 ～第4次対日相互審査前後に取るべき対応は～」より引用
<https://wisdom.nec.com/ja/business/2019083001/index.html>（最終閲覧日：2019.9.30）

新たな技術の活用例は、4.2節でいくつか言及した。最新のAML/CFTソリューションには、構造・非構造データを安全に管理・保管するブロックチェーンや、誤検知の防止・業務効率化を促すAI/RPA、さらに業務の標準化を実現するためクラウド等を活用するものも登場し始めている。こうした新たな技術の導入の背景にあるのは、図 6-6に示す通り、現行のAMLソリューションがもつ課題である。当然、新たな技術の導入には解決すべき法的論点もあるが、こうした技術を活用したソリューション例として、本邦外では表6-1のような取組みがすでに存在していることに注目したい。

一方、本邦で同様なソリューションを導入するにあたっては、法的要件などで整理と確認が必要な点があることから、図6-5の中長期的なスパンに相当する事例として、事例の導入効果を見極めつつ、実用化に向けた論点整理を行っていく必要がある。

図 6-6：新技術を活用するメリットと想定される法的論点[17]



17 有識者インタビュー、以下公開レポート、およびTransparency Market Research“AML Software Market”レポートをもとに作成
<https://home.kpmg/content/dam/kpmg/jp/pdf/jp-intelligent-automation-02.pdf>（最終閲覧日：2019.9.30）
<https://www.oracle.com/jp/corporate/features/pr/oracle-aml-machine-learning-blockchain/>（最終閲覧日：2019.9.30）

表6-1：本邦外における新たな技術を活用したAML/CFT取組み事例（1/2）

	ソリューション名 [ソリューション領域]	企業名 （所在国）	概要・特徴
1	Shield FC for Record Keeping/ Shield FC for Best Execution [フィルタリング/モニタリング]	Shield FC[18] （イスラエル）	**会話、音声等の非構造化データも取り込んだAI分析をすることで、従来のルールベースの検知より精度の高いサービス提供を行う** ・ 単一プラットフォームで、リスト作成、不正検知、内部コンプライアンスの全てを一括管理 ・ AI・多層分析エンジンで誤検知率減少。分析結果は即時グラフ化 ・ すべての構造化および非構造化データソースにシームレスに接続
2	Corlytics RED/ Taxonomy mapping/ RiskFusion [モニタリング（含 レポーティング）]	Corlytics[19] （イスラエル）	**規制の変化にフォーカスを当てたソリューションを展開。規制変更対応のみならず、行内の重点投資領域の分析まで行う** ・ 規制の変更をリアルタイムでトラッキングし、内部コンプライアンス・投資計画の変更を促すデータPF ・ 規制の変更、要人発言を踏まえて、規制内容をリアルタイムでマッピング ・ 規制の変化に応じて、AMLの重点投資領域の提示・投資計画を自動作成 ・ AIボットによって、規制当局のスピーチ、コンサルティングペーパー、審議中の規制案等をクラウドに保存。顧客はその内容を逐一確認可能
3	Intelligent Process Automation/ Anomaly Detection/ Automated Analytics [フィルタリング/モニタリング]	Inspirient[20] （ドイツ）	**従来のサービスとは異なり、取引開始から数分で不正検知～取引中止まで行えるスピーディーなソリューションを提供** ・ 大量の過去データ×AI分析によって、疑わしい取引中に、不正検知～取引遮断までを数分で行える ・ 疑わしい取引が開始した瞬間から数分で不正検知アラートを発する。取引終了前に取引中止が可能（分析・グラフ化は自動） ・ 過去に設定したルール＋AIの不正検知アルゴリズムで、誤検知を減少・コストを削減 ・ 専門家（AMLアナリスト、弁護士）等の知識・他のユーザーの不正検知データは毎日AIに反映
4	RegBot® [フィルタリング/モニタリング]	RegBot[21] （アイルランド）	**社内コンプライアンスのニーズの高まりを受け、行員の規制理解を高めるソリューションを開発** ・ 規制内容に関するチェックシートを適宜作成～社内共有することで、社内コンプライアンスを徹底させるソリューション ・ 弁護士、技術専門家のチームが開発した独自のアルゴリズム＋規制内容の適宜反映 ・ 不正検知の精度を高めるため、クライアント情報を自動的に取得するアプリを提供 ・ 規制要件を自動的に満たすように、レポーティング等の形式を適宜変更。規制変更箇所に関する情報を、タイムスタンプ付きの検索可能な形式で配信することで、社内コンプライアンスの徹底をサポート

18 <https://www.shieldfc.com/>（最終閲覧日：2019.9.30）

19 <https://www.corlytics.com/>（最終閲覧日：2019.9.30）

20 <https://www.inspirient.com/>（最終閲覧日：2019.9.30）

21 <https://www.regbot.net/>（最終閲覧日：2019.9.30）

表6-1：本邦外における新たな技術を活用したAML/CFT取組み事例（2/2）

	ソリューション名 [ソリューション領域]	企業名 （所在国）	概要・特徴
5	Go!vid/ Go!scan/ Go!score/ Go!checks [KYC/フィルタリング]	Algoreg[22] （ルクセンブルグ）	**過去の取引データ等に加えて、顔認証AIを活用した、精度の高い本人確認ソリューションを訴求** ・ AIビデオボットを活用したビデオセッションでの顔認証技術の導入 ・ 2,350,000のプロファイル、800,000のPEPsのデータリストと連携 ・ 100を超える言語対応が可能であり、全世界のどのエリアでも利用可能
6	Flair/ Get [KYC/フィルタリング/モニタリング]	Vadis Technologies[23] （ベルギー）	**顧客の単独のデータに拠ったリスク管理ではなく、顧客間の関係性をも加味したリスク管理が可能なソリューションを提供** ・在籍情報、過去取引等が含まれたデータベースを用いて、対象者間の関係性を調べることができる市場初の分析ツール ・3億社以上の企業に関する情報を含むさまざまなソースからデータを収集 ・個人・企業間のリンクを理解する視覚化ツール

22 <https://www.algoreg.com/gochecks_on-demand-risk-scoring-name-screening/>（最終閲覧日：2019.9.30）

23 <http://www.vadis.com/>（最終閲覧日：2019.9.30）

Appendix

WGの活動概要と活動実績および成果についてまとめる。

- WG活動概要
- WG活動実績および成果
  - ① 共通化領域の検討
  - ② 事業体の検討
  - ③ eKYCソフトウェアの要件
  - ④ 本人認証の強化に関する検討

●WG活動概要

KYC 共通化 WG について

KYC共通化WGは、証券コンソーシアムにおける3つのWGの内の一つとして、2018年8月に発足した。

本WGは、証券会社とその利用者、規制当局の各ステークホルダーがメリットを享受できる、KYC領域における共通インフラの実現のため、参加各社の意見を取り入れながら、利用者の利便性向上、証券各社の事務手続き削減に向けた共通サービスの実現を目指し、設立された（図1）。

図1：KYC共通化のコンセプト

当初のスコープ

本WGでは、KYC共通化に向け、優先的に対応すべき課題として、以下の4つを定義した（図2）。

課題1．改正犯収法対応 → オンラインで完結する本人確認の標準化
課題2．安全かつ便利なUI/UXを利用者に提供 → ログインの強化
課題3．口座開設に係る手続きや事務負担削減 → 本人確認情報・結果の共有
課題4．ハイリスク取引等の信頼性向上 → タイムリーな本人確認

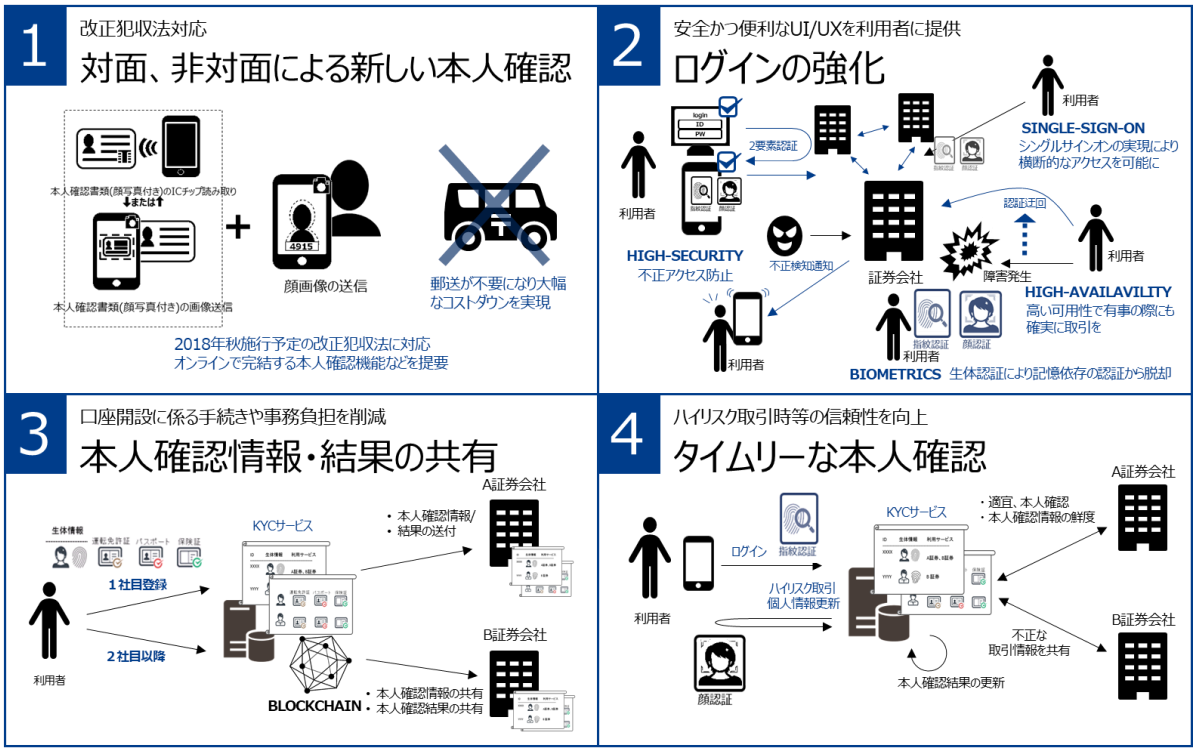
課題1については、口座開設時の本人確認業務のコスト削減および、口座開設までのリードタイム短縮による顧客の利便性向上のため、eKYCを活用した本人確認の標準化の実現を検討する。

課題2については、オンライン取引におけるセキュリティ強化と、顧客の利便性の向上の両方を実現するため、横断的なシングルサインオンの実現、2要素認証・生体認証の導入を検討する。

課題3については、業界全体のKYCの水準底上げと効率化の実現のため、JPXのPoCでも検証した、KYC結果の共有について検討する。

課題4については、リスクベース・アプローチの有効性向上のため、取引時のタイムリーな本人確認の仕組みの導入を検討する。高リスク取引の実効の前に、必要に応じて追加の本人確認を行うことで、リスク軽減を目指す。

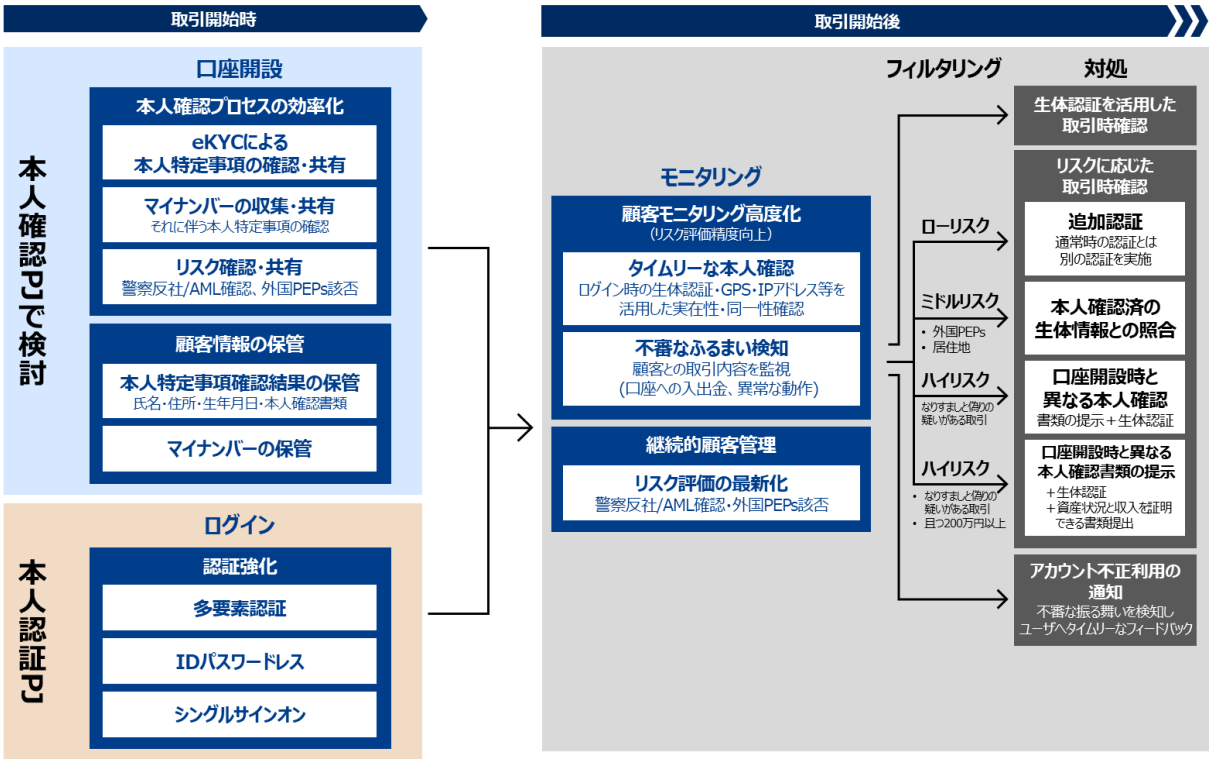
図2：KYC共通化に関する課題



プロジェクト概要

本WGは、取引開始時のKYC共通化を初期スコープとし、口座開設におけるKYC業務の共通化を検討する本人確認プロジェクト（PJ）と、オンライン取引時の本人認証の共通化を検討する本人認証PJで構成された（図3）。前者を日本電気株式会社（以下、「NEC」という）、後者をセコムトラストシステムズ株式会社（以下、「STS」という）がそれぞれプロジェクトマネージャー企業を務め、事業化に向けた検討を進めた。

図3：取引開始前後における本人確認・認証関連業務とプロジェクトスコープ



活動実績

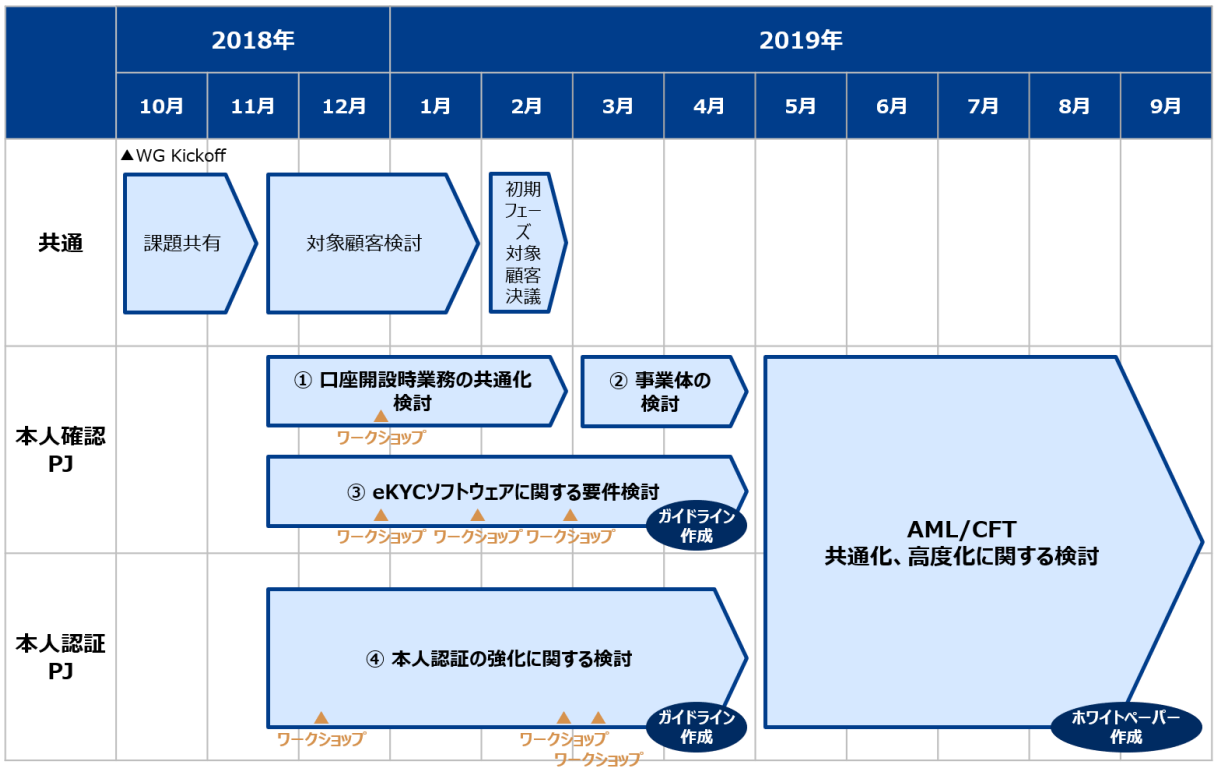
2018 年 8 月の WG 設立当初は、口座開設手続きにおける KYC 業務の一元化と証券会社間での KYC 結果情報の共有をスコープとして、事業化を前提とした議論を実施した。

本人確認PJでは、初期スコープである口座開設時の業務共通化のための検討として、共通化業務検討のワークショップを開催し、主幹事証券会社の意見を纏めながら、共通化における課題や論点の洗い出しを行った（図4①）。加えて、2018年11月の犯収法施行規則に改正の結果、オンライン完結型の本人確認方法（いわゆるeKYC）が新設されたことから、当該方法を採用する際に特定事業者が提供するソフトウェアについて、それが具備すべき要件についても検討をおこなった（図４③）。一方、本人認証PJでは、金融取引を取り巻くセキュリティの状況の変化を考慮し、証券各社の本人認証を従来よりも強化すること目指して、その対策について検討を行った（図４④）。

しかし、2019年3月の全体会にて、On-boardingに絞ってのKYC業務に特化した事業化では、利用する各社の十分なコストメリットが見いだせないとの結論に至った。これをうけて翌月より、On-boarding/On-goingを区別せず、主幹事企業でも関心の高いAML/CFT態勢の高度化を実現する業界共通的なサービスの実現にまでスコープを広げることとし活動を継続した。その結果、サービス立ち上げを視野にしつつも、まずは金融庁ガイドラインに対する業界共通的な考え方の整理と、AML/CFT態勢高度化のための方策としてシステムの共通化・共同化について検討結果をまとめ、ホワイトペーパーとして取りまとめることとなった。

本WGの発足から、ホワイトペーパーとりまとめまでの活動実績について、図4に示した。各検討の詳細については、後述の「活動の成果」で述べることとする。

図4：活動実績の全体像


2018年
2019年
10月
11月
12月
1月
2月
3月
4月
5月
6月
7月
8月
9月
共通
▲WG Kickoff
課題共有
対象顧客検討
初期フェーズ対象顧客決議
本人確認PJ
① 口座開設時業務の共通化検討
ワークショップ
② 事業体の検討
③ eKYCソフトウェアに関する要件検討
ワークショップ ワークショップ ワークショップ
ガイドライン作成
AML/CFT
共通化、高度化に関する検討
ホワイトペーパー作成
本人認証PJ
④ 本人認証の強化に関する検討
ワークショップ
ワークショップ
ワークショップ
ガイドライン作成

●WG活動成果

① 共通化領域の検討

1．概要

業界共通的な口座開設の仕組みを作ることを目的とし、eKYCを見据えた口座開設業務の共通化およびその標準策定の検討を行った。検討に際しては、主幹事証券会社参加のワークショップを開催し、共通化における論点の洗い出しを行った。

s

写真1：ワークショップの様子

2018年12月26日開催　口座開設業務共通化検討ワークショップより

2. 検討内容

ワークショップでは、口座開設業務を「フロント業務（ユーザ情報収集）」と「バック業務（その他証券会社業務）」に分け、それぞれについて非対面チャネル・個人顧客を対象という前提をおいた上で、ディスカッションを行った。

＜ディスカッション①＞フロント業務（ユーザ情報収集）

ここでは、顧客からの取得項目の例（表1）を基に、この項目における共通化の可否および共通化に際しての課題について、各社の担当者より意見を出し、その後全員でディスカッションを行った。

表1：顧客からの取得項目（例）

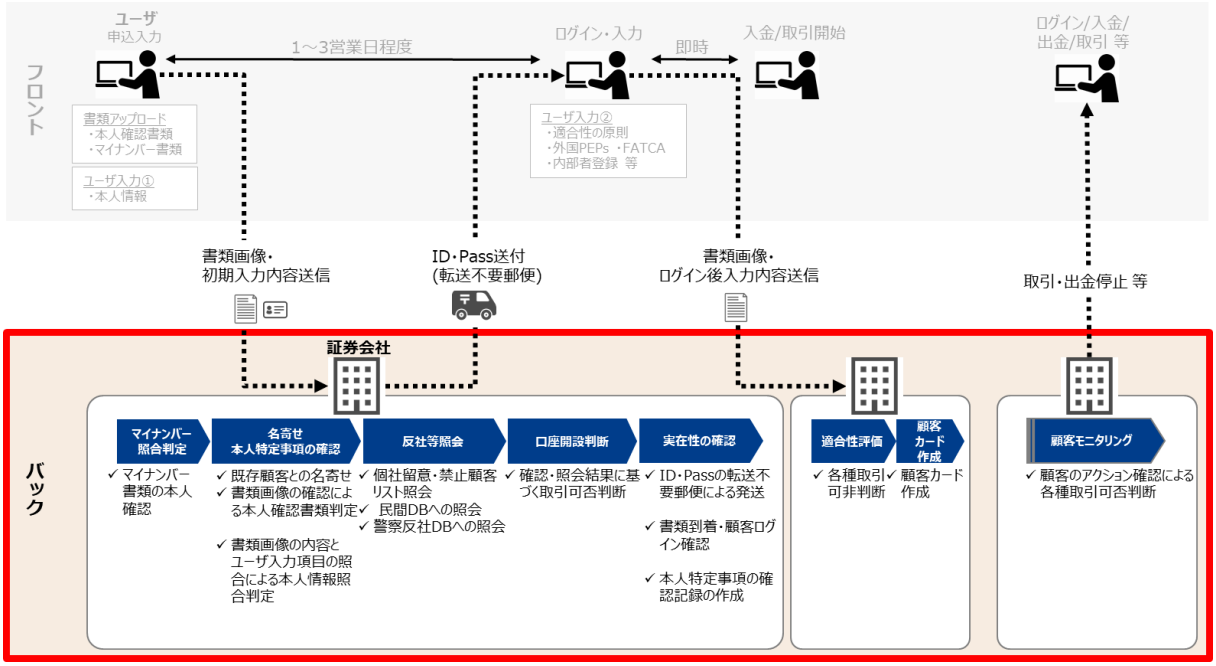
カテゴリ	項目
本人特定事項	住所・氏名・ 生年月日
その他連絡先	電話・メール
適合性の 原則 (アンケート)	職業
	投資方針
	投資目的
	投資経験
	金融資産
	年収
	主な収入源
	主たる資金の性格
	顧客となった動機
	取引の種類
	投資期間
内部者情報	世帯主との続柄
	世帯主勤務先

カテゴリ	項目
その他法律に基づく確認事項	国籍
	居住地国 (納税地)
	外国PEPs
	FATCA
	米国永住権(グリーンカード)
追加サービス	NISA口座
	iDeCo
	信用・FX 先物/オプション・金プラチナ・CDF ・銀行口座
	未成年口座 Jr.NISA口座
その他	振込先口座
	特定口座/一般口座

＜ディスカッション②＞ バック業務（その他証券会社業務）

バック業務に関しては、図5の通り、証券会社における口座開設時業務を整理したうえで、この中で共通化可能な業務、個社別の業務として残る箇所について、各社より意見を出し、その後全員でディスカッションを行った。

図5：口座開設時における証券会社の業務（例）



3. 結論

顧客からの取得項目に関しては、データフォーマットの問題と、各社で異なる情報の取得範囲について、課題および論点が多く得られた。例えば、「本人特定事項」だけでも、各社ごとに桁数や使用可能文字等が異なることで、データフォーマットにばらつきがあることが指摘された。加えて、取得情報も各社で粒度が異なったり、A社では取得していても、B社では取得していない項目があったりと、共通化への課題が多く得られる結果となった。

表2：顧客からの情報取得に関しての課題および論点（一部抜粋）

取得項目	課題・論点
本人特定事項	データフォーマットのばらつき（桁数、使用文字等）への対応
その他連絡先（電話、メール）	情報の取得範囲
適合性の原則	会社ごとに異なる区分値・取得項目への対応
内部者情報	情報の取得範囲
その他法律に基づく確認事項（PEPs等）	情報の取得範囲
追加サービス	各社異なるサービスや1社しか口座開設できないサービスの取り扱い
振込先口座・特定口座/一般口座	お客様が証券会社毎に使い分けている項目の取り扱い

証券会社業務の共通化に関しては、共通化の実現方法や共通仕様水準を課題として挙げる声が多かった。例えば、「反社等照会」の業務においては、共通化により、証券会社業務の効率化が図れるので、ぜひ対応してほしいといった前向きな意見が多く上がった一方、実現方法や経済合理性といった技術面・経済面の課題や、個社のフィルタリングリスト共有に際しての法的な課題についての意見が多く得られる結果となった。

表3：口座開設時の証券会社業務における共通化の課題と論点（一部抜粋）

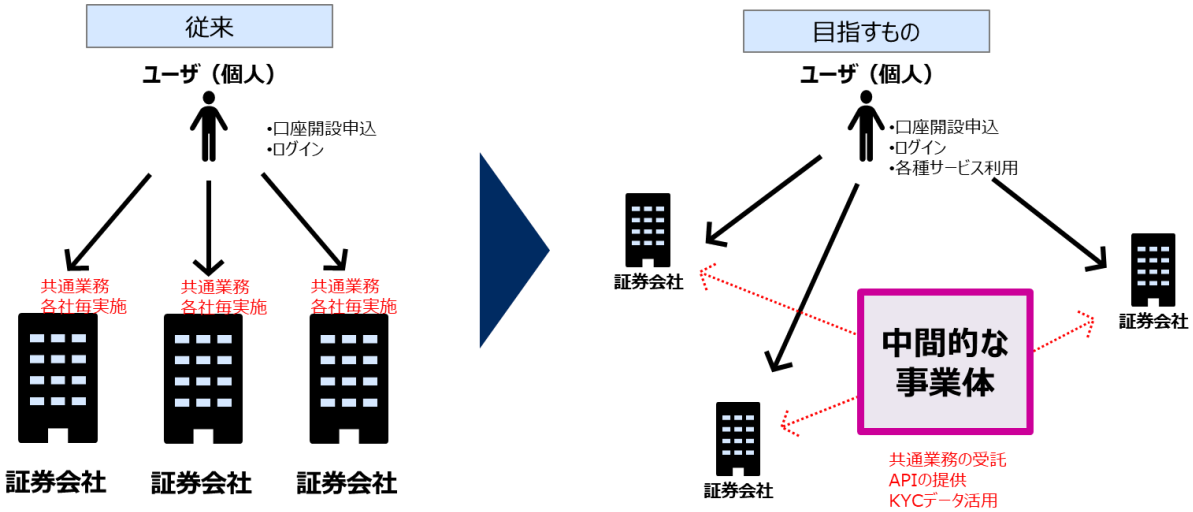
業務	課題・今後の論点
マイナンバー照合判定	実現方式/経済合理性
本人特定事項の確認	本人確認書類判定・本人照合判定の実現方式
反社等照会	チェック水準の明確化 個社イエロー・ブラックリストの共有の可否

② 事業体の検討

1．概要

本WGでは、顧客利便性の向上、証券各社の事務手続き削減を目的として、業界共通的なKYC（本人確認・認証）プロセスの標準化を検討し、それを担うソフトウェア（SW）の開発もしく選定を行うことを想定していた。標準化された共通業務を複数企業から受託し、一元的に実施するため、特定の証券会社に帰属しない、中間的な事業体の設立が必要であるとした（図6）。

図6：中間的な事業体の設立



2019年3月リーダー会にて提示

本WGで検討したサービス提供を行う事業体候補の概要・事業形態・証券会社の関わり方について簡単に示す。

2. 検討内容

（1）事業体の概要

KYC業務を標準化・効率化し、KYCプラットフォームとなり得る事業体の概要について、以下の表4に示す。

表4：事業体の概要

項目	内容
目的	• 共通事務の標準化と一元化により、証券各社の事務手続き削減する • KYCデータの一括管理と活用により、ユーザー利便性向上を図る
事業内容	証券会社が実施するKYC業務に対し、業務受託ないしAPI提供により以下を提供する ① [初期] 新規顧客を対象とする、証券口座開設に関するKYC業務 ② [将来] KYCプラットフォームを構築し、KYCデータを活用したサービスの提供
求められる特徴	**①KYCのインフラ的存在** 証券各社のKYC業務を代行するため、本事業体が業務執行不能となった場合、証券各社に与える影響が大きい。そのために、安定的かつ長期的に存続している必要がある。 **②営利目的ではない** サービス利用企業全体の事務コスト削減や、利用者の利便性向上が目的であり、事業目的以外でリスクをとる必要はない。 **③中立的な存在** 重要事項の決定について、特定の企業の意向に左右されることなく、参画企業全体で決定する必要がある。
留意事項	・金融機関のKYC業務を担う上で、必要な各種許認可の取得要否確認が必要 ・個人情報を取扱うため、各種資格が必要か（プライバシーマーク、ISOなど）

2019年3月リーダー会にて提示

（2）事業形態の選定

検討の前提として、法主体が共同事業を行う場合、内部統制や株主を含む自身のステークホルダーに対する説明責任の観点から、事業体における財産関係や経理関係を明確にする必要がある。また、事業の持続性維持の観点から、参加企業間の規律も明確にする必要がある。

加えて、財産帰属や権利義務関係の明確性や安定性を図る観点から、日本法やその実務で一般的に使用される特定の法形式を用いた事業体とすることの要請があると考えられる。

上記の前提を踏まえると、以下の3点について、日本の法律又は実務上、利用が現実的と考えられる方法を模索することが考えられる。

① 本事業体に帰属すべき財産の帰属先を、本事業体自身とすることの必要性
② 本事業体の活動に起因して負担する債務に対する加盟企業の責任の明確化
③ 特許・登記や許認可等の行政機関が管理する台帳への記録が重要な意味を持つ本事業体の法的地位について、本事業体自身が名義人となることの必要性

以上の検討結果を踏まえた上で、本WGでは、取りうる事業形態について「合同会社」「有限責任事業組合」「株式会社」の3つに絞り、メリットおよび懸念点を整理した（表5）。

表5：事業形態の選定

	合同会社	有限責任事業組合	株式会社
メリット	• 参画企業自身が事業体の運営や意思決定に携わることができる • 個別ルール等の例外規定も柔軟に策定できる • 決算報告義務や監査役設置義務がないため、株式会社と比較して、運営コストが低い	• 参画企業自身が事業体の運営や意思決定に携わることができる • 個別ルール等の例外規定も柔軟に策定できる • 決算報告義務や監査役設置義務がないため、株式会社と比較して、運営コストが低い	• 資金調達の選択肢が多い
懸念点	• 全員一致はデッドロックを招く可能性がある点*に注意	• 全員一致はデッドロックを招く可能性がある点*に注意 • 法人格ではないことによる懸念点 - 拠出した金銭や知財資産は組合に共有的に帰属するものの、実際の管理は組合員が、組合のために実施することになる - 業務上の資格は、基本的には構成員が取得する必要がある • 経済産業省が開示している資料によると、有限責任事業組合の構成員は少数のものが多く、20名を超えるものは全体の1.4%にとどまるとされている	• 個別ルール等の例外規定は、テクニックを駆使すれば可能だが、そこまでして株式会社を使う意味があるか検討を要する • 合同会社、組合と比較して、運営コストが高い

2019年3月リーダー会にて提示

＊重要事項の決議条件を全会一致とした場合、組織運営がデッドロックする恐れがある。そのため、合同会社および有限責任事業組合の場合は、定款によるカスタマイズが必要である。

（3）証券会社の関わり方

経営の中立性を確保するためには、一定数の証券会社による経営関与が必要である。証券会社の関わり方について、サービス利用・出資・業務執行の観点でパターン分けを行いそれぞれの考察結果を示す。現時点では、2または3の想定だが、詳細はサービス内容の検討と並行して議論が必要である。

表6：証券会社の関わり方

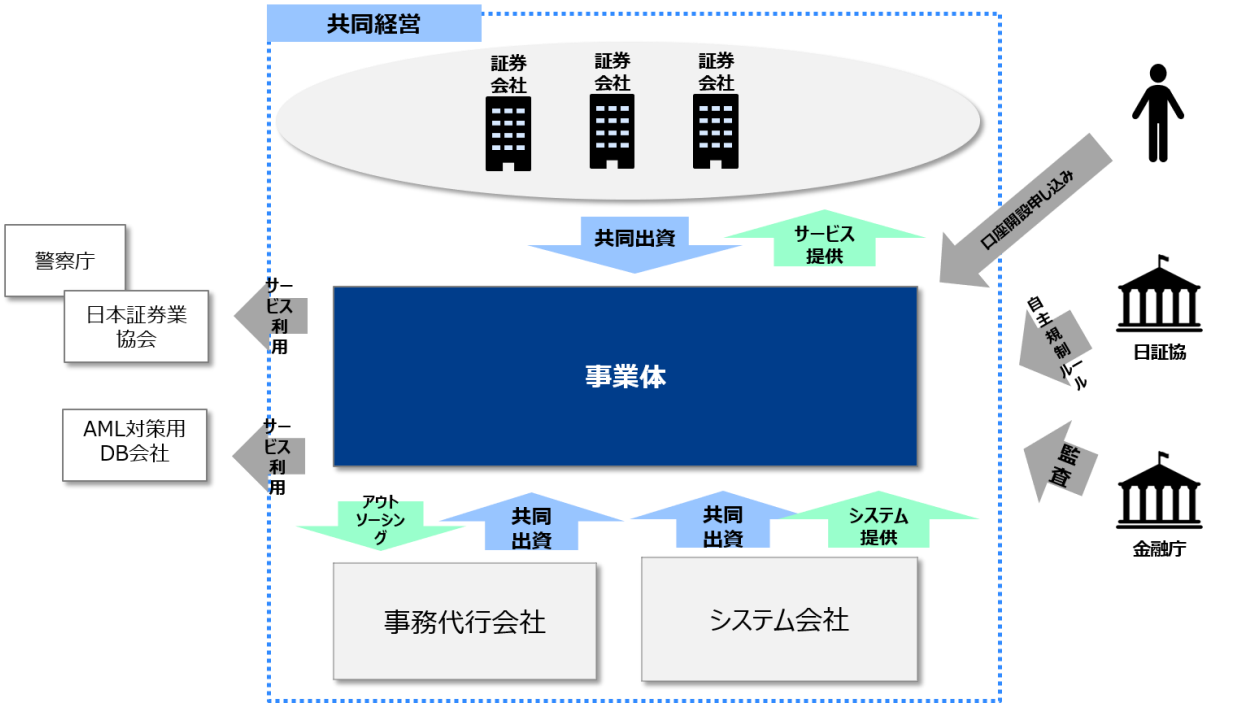
No.	サービス利用	出資	業務執行	判断	考察
1	✓			△	**全ての証券会社が本パターンを選択した場合、他の業者と差別化できず、インフラとなり得なくなる可能性が高い。**
2	✓	✓		○	**中立性を保つためには、複数の証券会社が経営に関与していることが望ましい。サービス利用企業の内、何割程度の関与が必要であるか、別途検討が必要。**
3	✓	✓	✓	○	**重要事項の決定については総会で決議するため、特定の証券会社から取締役を選出した場合も、中立性は確保できると考える。**
4	✓		✓	NG	有限責任事業組合の場合も、合同会社の場合も、出資者でなければ、運営には参加できない

2019年3月リーダー会にて提示

（4）ステークホルダーの関係

事業会社は、証券会社・システム会社・事務代行会社による共同出資で設立する。システムは外部サービスを利用し、事務作業はアウトソーシングする想定である。

図7：ステークホルダーの関係



2019年3月リーダー会にて提示

3．結論

今回の検討では、KYCサービスで想定している事業内容や、社会的な役割を踏まえたうえで、選択しうる事業形態とステークホルダーの関係について整理した。実際の事業化にあたっては、ビジネスモデルおよびサービスの詳細化検討結果を踏まえて、今回絞り込んだ「合同会社」「有限責任事業組合」「株式会社」の３つの形態の中から、最適なものを選択していくことが考えられる。

③ eKYCソフトウェアの要件検討

1. 概要

本WGでは、2018年11月の犯収法施行規則の改正（以下、「改正犯収法」という）に伴い、証券業界における本人確認の利便性の向上に資することを目的とし、非対面におけるオンライン完結型の本人確認のソフトウェア要件を検討してきた。

検討に際しては、関連ITベンダー[24]の有識者に協力を仰ぎ、ワークショップ等を開催（写真2）した上で、「eKYCソフトウェアに関するガイドライン」としてとりまとめた。ここでは、ガイドラインとしてとりまとめたeKYCソフトウェアに関する要件について、位置付け・対象範囲とともに記載する。

写真2：ワークショップの模様

2018年12月27日開　催eKYCソフトウェアに関する要件検討ワークショップより

[24] 日本電気株式会社、大日本印刷株式会社、株式会社ポラリファイ、株式会社Liquid

2. 検討内容

（1）「eKYC ソフトウェアに関する要件」の位置付け

本取組みは、証券業界として求められる eKYC ソフトウェアの要件を検討したものであり、eKYC ソフトウェアの企画・開発・導入する際に参照することを想定している。

- 記載する要件は、ITベンダーの有識者にて検討した内容を中心にまとめたものであり、証券会社の個別の要件、システム構成、サービス提供形態など言及しない部分については、各事業者が証券会社の状況や環境を考慮して企画・開発・導入することを想定している。
- eKYCソフトウェアに関する要件の遵守により、eKYCの関連法令の適合性を保証するものではない。改正犯収法を盛り込んだものではあるが、各事業者は自己の責任と負担において関連法令を調査し、これらを遵守しなければならない。

（2） 「eKYC ソフトウェアに関する要件」の対象範囲

要件検討に際しての対象範囲を下記に記載する。

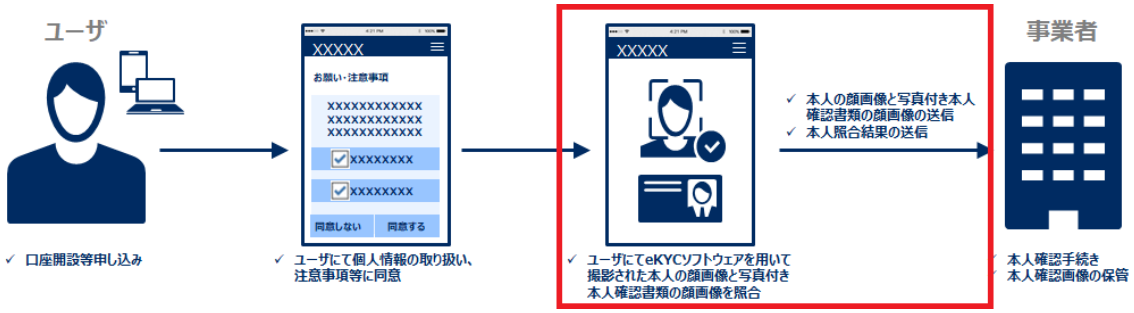
- 改正犯収法における「特定事業者が提供するソフトウェア」とする。
- 改正犯収法の第6条第1項第1号ホ・ヘ・トのうち、“ホ”「顧客等から、特定事業者が提供するソフトウェアを使用して、本人確認用画像情報の送信を受ける方法。」とする。

図8：本人確認用画像情報の送信を受ける方法[25]

[25] 出典：JAFIC「平成30年改正犯罪収益移転防止法施行規則（平成30年11月30日公布）に関する資料」

eKYCソフトウェアとして述べる範囲は下記のとおりとする。

図9：eKYCソフトウェアとして述べる範囲



3. 結論

法令、セキュリティ、運用、UI/UXの観点で、eKYCソフトウェアを企画・開発・導入・提供する際に事業者が要件として定義すべきものを「必須要件」、必須ではないが各事業者にて判断する要件を「任意要件」として記載する。

（1）セキュリティ要件

必須要件	
1	十分な実績を保有しないソフトウェアの場合、不正を検知できない可能性があるため、10万組以上の組み合わせでの測定実績が確保されること
2	事業者が本人であることを確認するのが運用上困難になるため、申請者がマスク・サングラスを着用していた場合は照合NGになること
3	不正検知及び把握のため、照合の成功・失敗履歴が事業者に通知されること
4	悪意ある攻撃を防止するため、照合を何度もトライできないこと（回数制限できること）
5	顔照合NGの際の表示メッセージが不正攻撃を助長されないものであること
6	サポート期間終了の端末・Webブラウザ・OSはセキュリティを担保できないため、サポート対象外とすること
7	端末とサーバー間のセキュリティが確保されること
任意要件	
8	本人確認書類の偽造を検知できること[26]
9	画像の加工/改ざんを検知できること[27]
10	申請時のアクセス地点を確認できること
11	申請者が申請途中で離脱した場合にデータが消されること
12	申請者が申請途中で一時保存した場合でも、一定時間が経過したあとにデータが消されること
13	実在性証明をランダムアクションで行う場合、ランダムパターンが十分準備されていること

[26] 真贋判定できる機能を備えていることを想定。eKYCソフトウェアのみで真贋判定を100%の精度で実現することは現状の技術では困難であるため、任意要件とする。

[27] 画像データのハッシュ値などで改ざんを検知することを想定。法令に準ずる必須要件項番3「申請者が撮影した画像が加工可能な状態に置くことなく事業者側に送信されること」との差異は、画像の加工/改ざんを予防するか、防止するかの違いである。

（2）運用要件

必須要件	
1	人種・性別・世代によらず照合されること
2	髭・眼鏡・化粧など日常で生じうる範囲で風貌が異なっても照合されること
3	本人確認用画像情報が一般的なファイル形式[28]で画像が保管されること
任意要件	
4	最大10年前の顔写真と照合されること
5	帽子を着用していても照合されること
6	実在性証明で使用した本人確認用画像情報が事業者にて記録・保管されること[29]
7	事業者が本人確認書類の券面の有効期限を確認できること[30]
8	撮影時の日時の情報が事業者にて記録されること
9	撮影時の場所の情報が事業者にて記録されること
10	他の証券会社と情報共有ができるようにするため、ベンダーロックされないekYCインタフェースであること
11	5Gネットワークの方向性を見据えた開発方針であること
12	本人拒否率（FRR）が1%以下であること
13	他人許容率（FAR）が0.001%以下であること

[28] 特異なファイル形式を除外することで、ベンダーロックの回避や画像情報の共有を見据える。JPEG、PNG等のファイル形式を想定している。

[29] 本人確認用画像情報の記録・保管は求められるが、実在性証明で使用した本人確認用画像情報を記録・保管する取り決めはないことを想定している。

[30] eKYCソフトウェアにAI-OCRの機能を組み込むことで券面の有効期限を確認することも可能だが、事業者の目検等による確認も想定されるため、任意要件とする。

（3） UI/UX 要件

任意要件	
1	一つの照合にかかる時間が短いこと[31]
2	eKYCにかかる時間が短いこと[32]
3	説明文を読まなくても直観的に操作できる工夫がされていること
4	申請者の手続きをサポートするメッセージが表示されること
5	利用端末に応じて申請者の手続きをサポートする音を出せること
6	利用端末に応じて申請者の手続きをサポートするバイブレーションを鳴らせること
7	申請者の手続きをサポートする音声ガイダンスを付けられること
8	事業者による目検での本人確認に支障がない距離・角度・照度で撮影されること
9	申請者が一連の流れで実在性証明できること
10	照合エラーとする条件を設定できること
11	スマートフォンやタブレット、PC等以外の専用機器を必要としないこと
12	シンプルモードがあること[33]
13	申請者の顔容貌を画面上に投影することなく申請手続きを済ませられること[34]
14	申請者による操作の手間を軽減のため、申請者が撮影ボタンを押下せずに本人確認用画像情報が撮影されること
15	撮影ステップの状況（1/5,2/5,…など）が表示されること
16	反射写り込みしている本人確認書類の券面が検知されること
17	人間以外の顔（例えば動物や絵の顔）が検知されないこと

[31] 目標値は1秒以内、ただし、通信環境・端末等に依存する。

[32] 目標値は5分以内、ただし、通信環境・端末等に依存する。当時間は規約を確認後、申請手順確認～本人確認用画像情報の撮影・本人確認用画像情報が照合されるまでを指す。

[33] 追加機能の省略、メッセージの拡大・簡素化等を想定している。

[34] 顔容貌を画面上に投影されることに難色を示すユーザーも存在すると想定している。

④本人認証の強化に関する検討

1.概要

昨今、証券サービスが利用者にとって便利で使いやすくなる一方で、新たなサイバー攻撃、不正取引手段の巧妙化、AML/CFTの厳格化など、金融取引を取り巻くセキュリティの状況も大きく変化している。そこで、本WGでは、証券各社の本人認証を従来よりも強化することを目指し、証券各社がその検討や対策に取り組むための考え方を検討した。

検討に際しては、主幹事証券会社参加のワークショップを開催し、最終的に「証券会社における本人認証ガイドライン」としてとりまとめた。ここでは、ガイドラインとして取りまとめた認証強化に関する考えた方の概要を位置付け・対象範囲と共に記載する。

2. 検討内容

（１）「証券業界における本人認証ガイドライン」の位置づけ

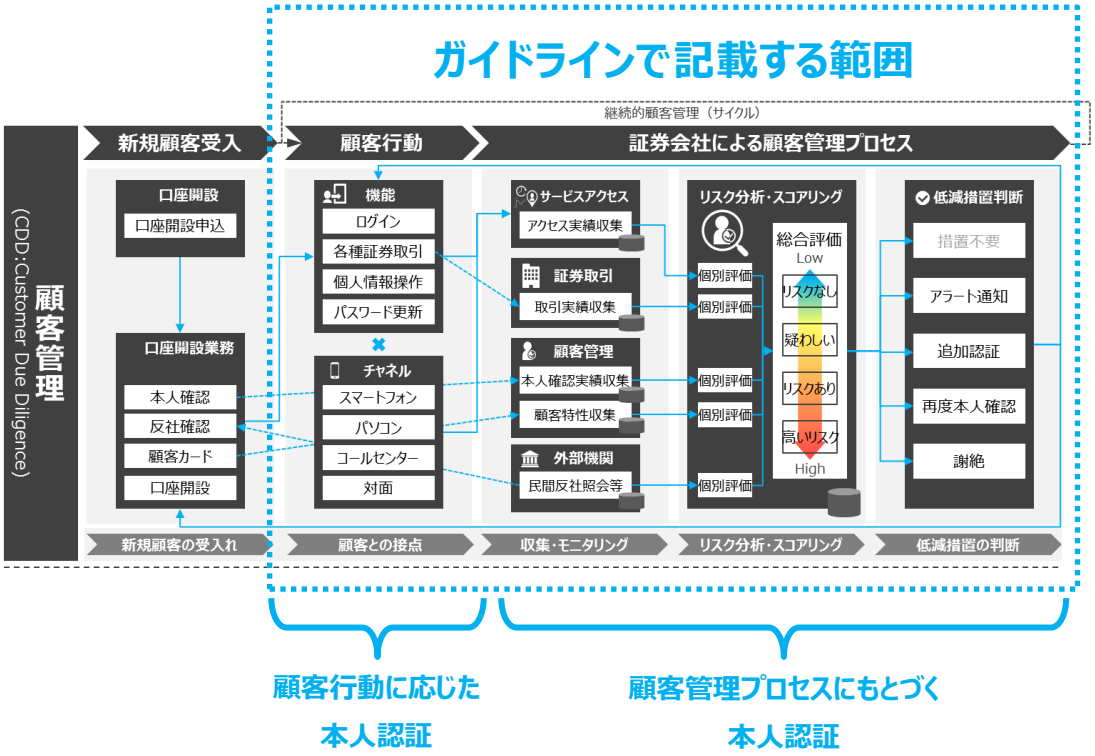
本ガイドラインの位置付けを以下に記載する。

- 本ガイドラインは、証券各社の本人認証を従来よりも強化すること目指し、証券各社がその検討や対策に取り組むための考え方をKYC共通化WGの見解としてまとめるものである。
- 本ガイドラインでは、認証強化に取り組むための考え方を記載したものであり、具体的な対策については、本ガイドラインに記載する考え方を参考に証券各社またはその関係者が状況や環境に応じて取り組むことを想定している。
- 本ガイドラインでは、認証強化に取り組むための考え方を記載しているが、本ガイドラインの考えに基づき取り組む対策は、証券サービスの安全性確保に必要な対策の全てを網羅するものではないため、本ガイドラインで言及していない事項については規制当局等が発行するドキュメントや証券各社のポリシー等も合わせて参照し、対策が行われることを想定している。
- 本ガイドラインは、認証強化に取り組むための材料を証券各社に提供するものであり、証券各社に一律に対応を求めるものではない。また、規制当局等から証券各社に求められる態勢整備の不備を明らかにするものではない。

（２）「証券業界における本人認証ガイドライン」の対象範囲

本ガイドラインでは、本人認証の範囲を整理するにあたり、金融庁ガイドラインを参照し、そこで謳われるCDDの考えと照らしながら以下の図のとおり整理を行った。

図10：ガイドラインで記載する範囲



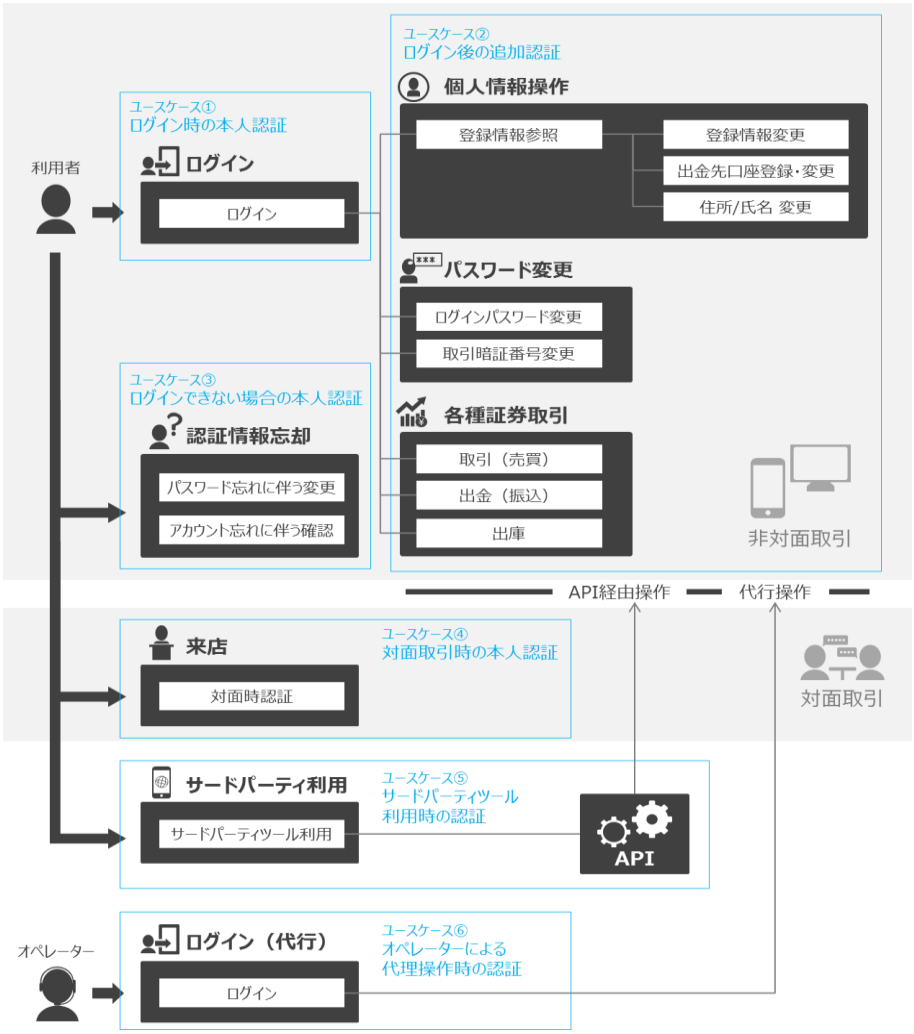
そのうち、証券会社が提供する「機能」や「チャネル」を介して利用者が証券サービスを利用する行いを「顧客行動」、顧客行動の後方で情報を収集し、リスク評価・分析・低減措置を判断・実施する行いを「証券会社による顧客管理プロセス」と整理し、現時点では「顧客行動に応じた本人認証」についてガイドラインとして取りまとめている[35]。

[35] 「顧客管理プロセスにもとづく本人認証」については今後議論していく予定である。

（３）前提とする認証サービス

本WGに参加するいくつかの証券会社からサンプリングし、証券サービスにおいて本人認証が行われるシーンを6つのユースケースに分け以下に整理した。認証時の手段としては、ログイン時に「ログインパスワード」、ログイン後の追加認証時に「取引暗証番号」を用いている。

図11：証券サービスにおける本人認証のユースケース



ユースケース	説明
① ログイン時の本人認証	利用者は、証券会社が提供する非対面サービス利用時に、ログイン認証を行う
② ログイン後の追加認証	利用者は、ログイン後に提供される各機能利用時に、適宜追加認証を行う
③ ログインできない場合の認証	利用者は、認証情報の再発行を行いたい場合、ログイン時とは異なる本人認証を行い、認証情報を復元する
④ 対面取引時の本人認証	利用者は、証券会社が提供する対面サービス利用時に、本人認証を行う
⑤ サードパーティツール利用時の認証	利用者は、サードパーティが提供するツールを経由し証券会社のサービス利用時に、本人認証を行う
⑥ オペレーターによる代理操作時の認証	オペレーターは、利用者に代わりシステムを操作する際に、本人認証を行う

3.結論

証券サービスでは、ログインパスワードや取引暗証番号（以降これらをパスワードと総称）など、認証を必要とする多くのシーンでパスワードを利用している。パスワードを用いた認証はインターネットサービスにおいて広く利用されており、証券サービスに限らず一般的な手法である。しかしながら、パスワードを安全に利用するためには忘却や紛失への対応、第三者に推測されにくくする工夫、盗難や漏えい対策など、利用者と証券会社いずれにとっても負担がかかり、これらの対応は認証強化における重要な論点である。

一方で、証券会社の特性も十分に考慮する必要がある。証券会社の取引はコンマ何秒を争うものもあり、スムーズな操作が利用者の資産に影響を及ぼす１つのファクターであるため、即時性や利便性を上げるために安全性を重視しない利用者も少なからず存在している[36]。通常、「安全・安心」、「便利・早い」はトレードオフの関係にあり、認証強化においては常にバランスに配慮することが重要である。

本ガイドラインでは、これらへの対応を考え方の基本とし、証券会社におけるそれぞれの認証シーンで最適な本人認証が行えるよう、認証強化の考え方について要点とその説明をまとめた。また要点の整理においては、認証強化の対策としてインターネット環境での利用が増えつつある「多要素認証」が、証券会社においても効果的な対策の1つになると考え、各ユースケースと照らしながらその活用における考え方などを整理している。

以下にガイドラインに記載している要点を記載する。

ユースケース	要点
① ログイン時の本人認証	要点①：多要素認証でログイン時の認証を強化する
	要点②：「生体」「所持」を加え多要素認証を行う
	要点③：チャネル全体を俯瞰した対策を行う
② ログイン後の追加認証	要点④：ログイン時の認証を踏まえて追加認証を行う
	要点⑤：リスク特性を踏まえて適切なタイミングで追加認証を行う
③ ログインできない場合の認証	要点⑥：新たな認証要素が利用できないケースに備える
④ 対面取引時の本人認証	要点⑦：対面認証時もシステム活用を検討する
⑤ サードパーティツール利用時の認証	要点⑧：APIを活用し安全なサードパーティアクセスを提供する
⑥ オペレーターによる代理操作時の認証	要点⑨：内部不正に備え代理操作時の認証を強化する

[36] 一方で利便性よりも安全性を求める声も存在している（KYC共通化WGの本人認証ワークショップにおける議論より）。

（空白のページ）

（空白のページ）

証券コンソーシアム
KYC共通化ワーキンググループ

ワーキンググループ参画幹事企業

株式会社SBI証券
株式会社だいこう証券ビジネス
カブドットコム証券株式会社
セコムトラストシステムズ株式会社
日本電子計算株式会社
日本電気株式会社
マネックス証券株式会社
みずほ証券株式会社
楽天証券株式会社
（2019.9末現在、五十音順）

■発行　2019.10.1

■ホワイトペーパーに関する連絡先
日本電気株式会社
デジタルインテグレーション本部
nec-digitaltrust@ldh.jp.nec.com