マネロン等対策の現状と今後の対応について

日本金融監査協会
実務研修セミナー

2021年12月23日

尾崎　寛
金融庁総合政策局リスク分析総括課
マネーローンダリング・テロ資金対策企画室長

本資料において、出所を筆者作成とする部分、及び、筆者意見にわたる部分は、筆者の個人的見解であり、所属する組織の見解を示すものではありません。

尾崎　寛

金融庁 総合政策局 リスク分析総括課 マネーローンダリング・テロ資金供与対策企画室長

1988年東京大学経済学部卒、三井銀行入行。91年大蔵省出向（国際金融局調査課）、93年外務省出向（在ワシントンＤＣ日本大使館財務班）などを経て、2014年4月三井住友銀行欧阿中東本部中東総支配人兼ドバイ支店長、17年４月三井住友銀行総務部部付部長兼ＡＭＬ金融犯罪対応室長。同行を退職し、18年２月から現職。

ニューヨーク大学Stern School of Business(MBA)、日本証券アナリスト協会認定アナリスト(CMA)、国際公認投資アナリスト(CIIA)、日本安全保障貿易学会(CISTEC)会員、慶應義塾大学大学院システムデザイン・マネジメント研究科非常勤講師、Certified Anti-Money Laundering Specialist(CAMS)

1. マネー・ローンダリング/テロ資金供与とは何か

◆ **マネー・ローンダリング（Money Laundering：資金洗浄）**とは、一般に、犯罪によって得た収益を、その出所や真の所有者が分からないようにして、捜査機関による収益の発見や検挙を逃れようとする行為をいう。

◆ **テロへの対応**においては、未然防止が特に重要であり、テロ組織の活動を支える資金供給の遮断と資金供給ルートの解明、国際的な連携が必要なことはマネー・ローンダリング対策と同様である。

◆ これらのような行為を放置すると、犯罪による収益が、将来の犯罪活動や犯罪組織の維持・強化に使用され、組織的な犯罪及びテロリズムを助長するとともに、これを用いた事業活動への干渉が健全な経済活動に重大な悪影響を与えることから、国民生活の安全と平穏を確保するとともに、経済活動の健全な発展に寄与するため、マネー・ローンダリングを防止することが重要。

◆ 国際社会は、これまでマネー・ローンダリングを防止して摘発するための制度を工夫し発展させ、連携してこれに対抗し、我が国も、国際社会と歩調を合わせて**マネー・ローンダリング及びテロ資金供与対策**の強化を図ってきている。

出所：警察庁　平成30年犯罪収益移転防止に関する年次報告書　等

貿易決済、貿易金融は、古くから、マネー・ローンダリング等に悪用されることが多い。

⇒　Trade Based Money Laundering（TBML）

2. マネー・ローンダリングを取り巻く世界の現状

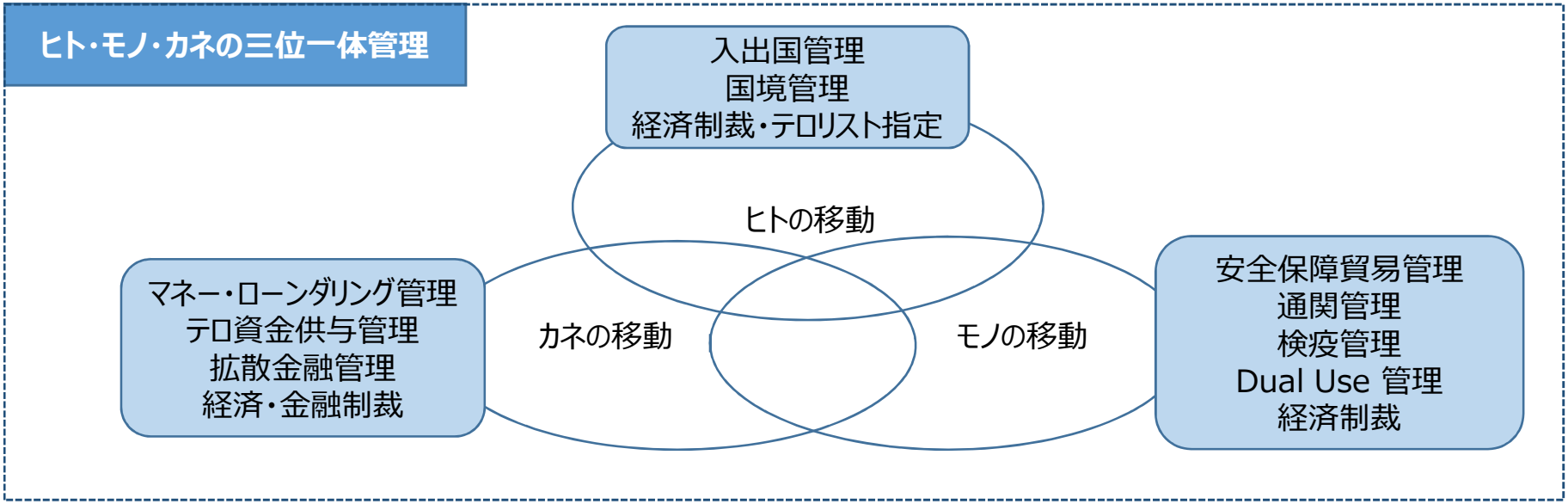
- **全世界で資金洗浄されている金額の推定**は、**世界全体のGDP（約８５兆ドル）の約２～５％**(約**１兆７千億ドル～４兆２千億ドル）**（国連薬物犯罪事務所(UNODC)による推計))
- **マネロン等対策にかかる費用**も増加。民間調査会社(LexisNexis Risk Solution)によれば、**年間全世界ベースでの費用推計額は2,139億米ドル(約24兆円)**（The True Cost of Financial Crime Compliance Report - Global Edition、2021年6月による推計）
- マネロン等体制の脆弱性や法令違反等による**行政処分の過料**も増加しており、民間データ分析会社(fenergo)によれば、全世界での、**2008年から2018年の累積で270億米ドル**。2015単年で115.2億米ドルの過料。米国当局による過料が全体の91%であり、また、73%が金融制裁違反。多くが自国当局ではなく、海外当局（特に米国）からの過料。(fenergo, Global AML/KYC/Sanctions Fines: 2008 – 2018)
- G20(G7)首脳宣言、G20(G7)財務大臣・中央銀行総裁会議においては、マネー・ローンダリング・テロ資金供与対策が、国際社会が取り組むべき重要アジェンダであることを示す旨の声明が出されている。

３．ヒト･モノ･カネの三位一体管理

◆2019年の世界貿易(財貿易、名目輸出ベース)は、前年比2.9%減の18兆5,047億ドル(ジェトロ推計値)。貿易数量も前年から減少。金額・数量双方の伸びがマイナスとなったのは2009年以来10年。

◆コロナ禍で2019年、2020年の世界貿易の拡大は足踏み状態なるも、中長期的には、グローバル経済の拡大で貿易が盛んになる中、貿易決済に関係したマネー・ロンダリング（Trade-Based Money Laundering：TBML）も増加する傾向。（そもそも、マネロンをたくらむ者は、国境をまたぐ資金決済により、捜査を遅らせる傾向があることから、TBMLも古典的な手法）

◆米国は、国土安全保障、経済安全保障の観点から、財務省、国務省、商務省、司法省等、連邦当局がヒト･モノ･カネの流れに対して三位一体で取り組んでいる。



4．金融活動作業部会（FATF）の概要

- マネロン・テロ資金供与対策のための国際基準（FATF基準）の策定・履行を担う多国間の枠組み。全加盟国・機関が承認したマンデートに基づき活動。
- FATF基準の履行を担保するため、相互審査を実施。
- 37か国・２地域機関が加盟。その他9つのFSRB型地域を加えると、FATF勧告は、世界204の国・地域に適用。

FATF：金融活動作業部会

AML/CFTの国際基準となる**FATF勧告を策定**。加盟国間で相互審査を実施。事務局はOECD内に置かれているが、運営は独立。

（FATF加盟国一覧）

アイスランド、アイルランド、アルゼンチン、イスラエル、イタリア、インド、英国、オーストリア、オランダ、カナダ、韓国、ギリシャ、豪州、サウジアラビア、シンガポール、スイス、スウェーデン、スペイン、中国、デンマーク、ドイツ、トルコ、日本、ニュージーランド、ノルウェー、フィンランド、ブラジル、フランス、米国、ベルギー、ポルトガル、香港、マレーシア、南アフリカ、メキシコ、ルクセンブルク、ロシア、欧州委員会（EC）、湾岸協力理事会（GCC）

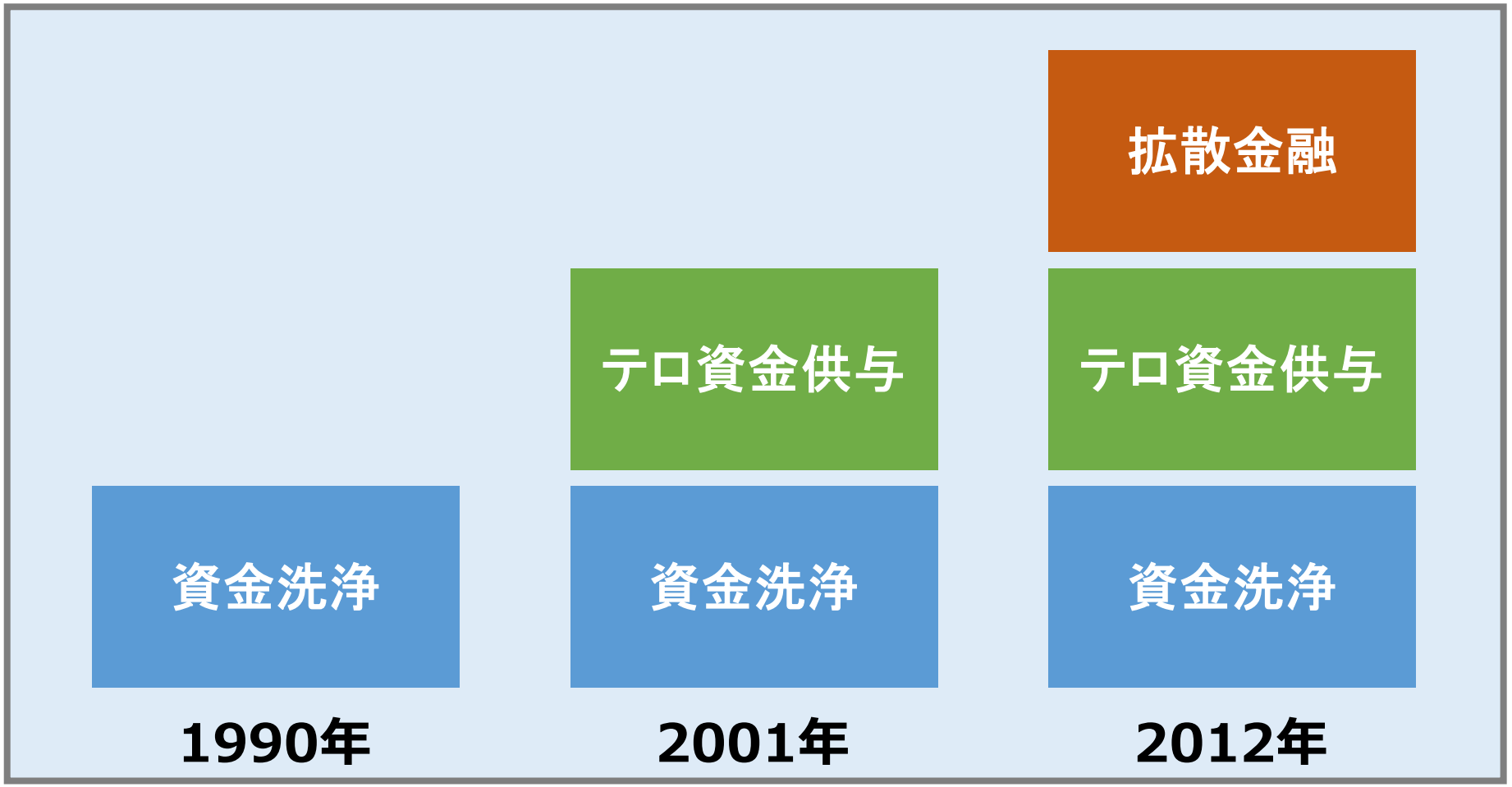
FSRB：FATF型地域体

地域ごとに存在し、**FATF勧告をベースに**加盟国間で相互審査を実施。

	参加国・地域数
①APG（アジア太平洋）	41
②CFATF（カリブ）	25
③EAG（中露を含むユーラシア）	9
④ESAAMLG（東・南アフリカ）	18
⑤GABAC（中央アフリカ）	7
⑥GAFILAT（ラテンアメリカ）	17
⑦GIABA（西アフリカ）	17
⑧MENAFATF（中東・北アフリカ）	21
⑨MONEYVAL（欧州）	33

5．FATF勧告の対応範囲

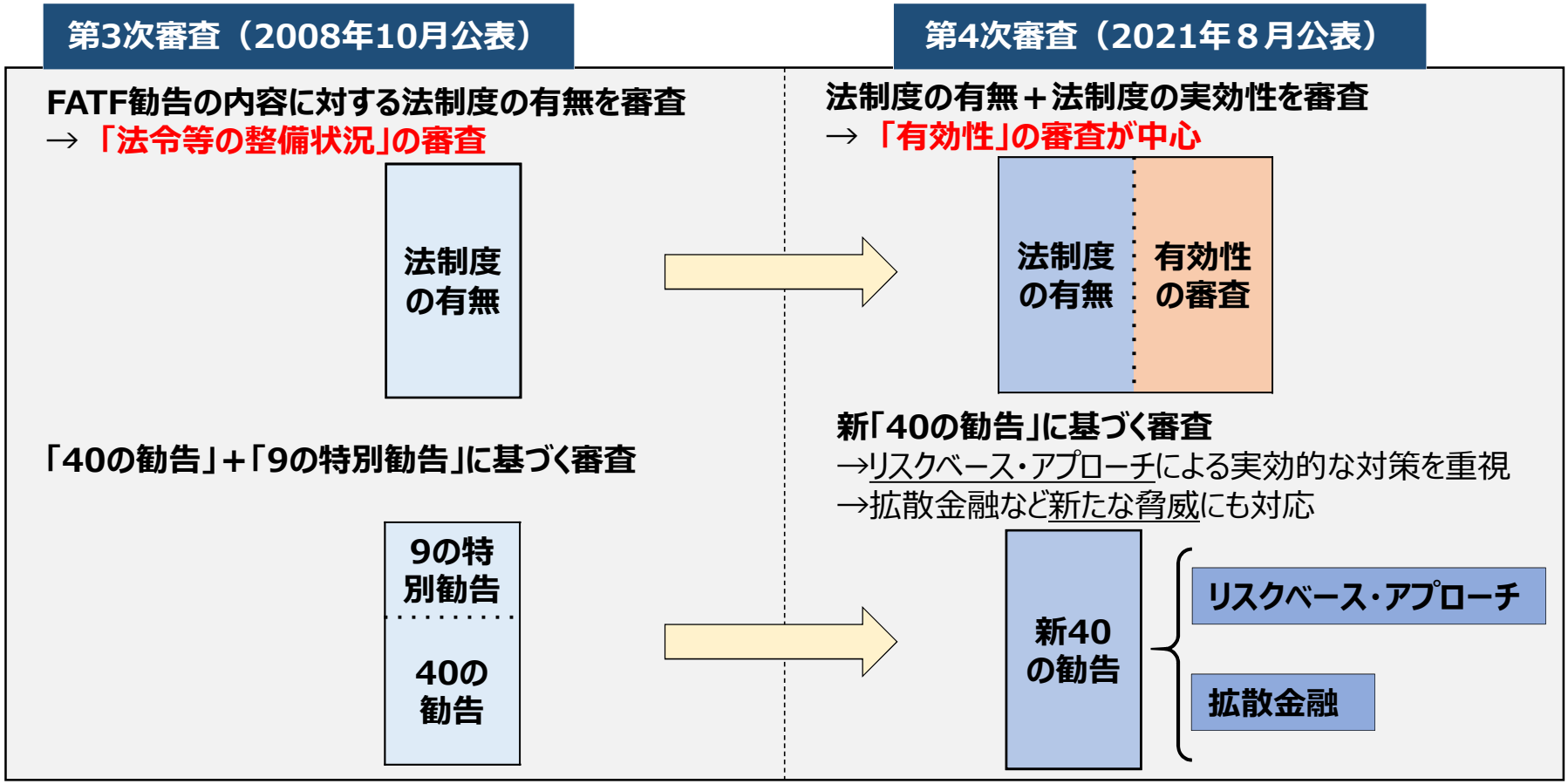
■FATF勧告の対応範囲は、時代に応じて拡大。
■現在は、2012年に策定された40の勧告が最新。



6. FATF第４次対日相互審査の経緯

2019年	**５月**	審査の開始（書面審査）
	10月～11月	オンサイト審査
2020年		審査報告書について断続的に協議　（※4月～10月はコロナで中断）
2021年	**６月**	FATF会合：審査報告書案の討議
	８月末	審査報告書の対外公表

第３次審査と第４次審査の比較



7. FATF議長のステートメント（対日相互審査部分を抜粋） 2021年6月25日公表

◆Chairman's Statement on June 25, 2021 Mutual Evaluation of Japan

- The FATF also discussed the joint FATF and Asia/Pacific Group on Money Laundering (APG) assessment of Japan's measures to combat money laundering and terrorist financing.
- The Plenary concluded that **Japan's measures to combat money laundering and terrorist financing are delivering results.**
- Japan has demonstrated good results in understanding, identifying and assessing its money laundering and terrorist financing risks, in the collection and use of financial intelligence and in the cooperation with its international partners.
- However, the country needs to prioritise efforts in certain areas, including the supervision of and preventive measures by financial institutions and designated non-financial businesses and professions, the prevention of misuse of legal persons and arrangements, and investigating and prosecuting money laundering and terrorist financing.
- The FATF will publish these reports in August, after a quality and consistency review.

日本の相互審査

- FATFとAPG（アジア・太平洋マネー・ローンダリング対策グループ）が共同で行った、日本のマネロン・テロ資金対策に関する評価について議論を行った。
- 全体会合では、**日本はマネロン・テロ資金対策の成果を上げている**と結論づけられた。
- 日本は、マネロン・テロ資金リスクを理解・特定・評価していること、金融インテリジェンスを収集及び利用していること、国際的なパートナーと協力していること、について良い結果を示している。
- しかしながら、日本は、金融機関等の監督及び予防措置、法人等の悪用防止、マネロン・テロ資金の捜査・訴追などの特定分野において優先的に取り組む必要がある。
- FATFは、審査報告書の質及び他国の報告書等との一貫性を確認したのち、当該報告書を8月に公表する予定。

（出所：FATF議長のステートメント（2021年6月25日発表）*筆者翻訳）

8. 第４次対日相互審査（TC：法令等整備状況）の結果

	内容	4次
1	リスク評価とリスクベース・アプローチ	LC
2	国内関係当局間の協力	PC
3	資金洗浄の犯罪化	LC
4	犯罪収益の没収・保全措置	LC
5	テロ資金供与の犯罪化	PC
6	テロリストの資産凍結	PC
7	大量破壊兵器の拡散に関与するものへの金融制裁	PC
8	非営利団体（NPO）の悪用防止	NC
9	金融機関秘密法が勧告実施の障害となることの防止	C
10	顧客管理措置	LC
11	本人確認・取引記録の保存義務	LC
12	PEPs（重要な公的地位を有する者）	PC
13	コルレス銀行業務	LC
14	送金サービス提供者の規制	LC
15	新技術の悪用防止	LC
16	電信送金（送金人・受取人情報の通知義務）	LC
17	顧客管理措置の第三者依存	N/A

	内容	4次
18	金融機関・グループにおける内部管理方針の整備義務、海外支店・現法への勧告の適用	LC
19	勧告履行に問題がある国・地域への対応	LC
20	金融機関における資金洗浄・テロ資金供与に関する疑わしい取引の届出	LC
21	内報禁止及び届出者の保護義務	C
22	DNFBPsにおける顧客管理措置	PC
23	DNFBPsによる疑わしい取引の届出義務	PC
24	法人の実質的支配者	PC
25	法的取極の実質的支配者	PC
26	金融機関に対する監督義務	LC
27	監督当局の権限の確保	LC
28	DNFBPsに対する監督義務	PC
29	FIUの設置義務	C
30	資金洗浄・テロ資金供与の捜査	C
31	捜査関係等資料の入手義務	LC
32	キャッシュ・クーリエ（現金運搬者）への対応	LC
33	包括的統計の整備	LC
34	ガイドラインの策定義務	LC

	内容	4次
35	義務の不履行に対する制裁措置	LC
36	国連諸文書の批准	LC
37	法律上の相互援助、国際協力	LC
38	法律上の相互援助：凍結及び没収	LC
39	犯人引渡	LC
40	国際協力（外国当局との情報交換）	LC

適

Compliant

Largely-**C**ompliant

Partially-**C**ompliant

Non-**C**ompliant

（法令等整備状況）

不適

- ✓ NC or PC = 11
- ✓ 11/40 (27.5%)

※TC（Technical Compliance）：「法令等整備状況」の審査

出所：FATFの第４次対日相互審査報告書より、筆者等が作成

（参考）第3次対日相互審査: 25/49 (51.0%)

9. 第４次対日相互審査（IO：有効性）の結果

	評価項目	評価
1	マネロン/テロ資金リスクの評価	S
2	国際協力	S
3	**金融機関等の監督**	**M**
4	**金融機関等によるマネロン/テロ資金対策**	**M**
5	法人等の悪用防止	M
6	疑わしい取引に関する情報等の活用	S

	評価項目	評価
7	マネロン罪の捜査・訴追・制裁	M
8	マネロン収益の没収	M
9	テロ資金の捜査・訴追・制裁	M
10	テロリストの資産凍結、NPOの悪用防止	M
11	大量破壊兵器拡散に関与する者の資産凍結	M

（注）対策の実施面で有効性が高いと認められる順番に、
H(High)、S(Substantial)、M(Moderate)、L(Low)と評価。

出所：FATFの第４次対日相互審査報告書より、筆者等が作成

10. IO.3（金融機関等の監督）とIO.4（金融機関等の対応）のポイント

IO.3（金融機関等の監督の有効性）

1. 金融監督当局間でリスクの理解に差はあるものの、主要なリスクに関する理解は適切である。
2. 金融庁は、金融セクターの規制・監督の主たる当局であるが、2018 年以降、リスク理解に資する関連施策を実施し、リスク理解を改善させている。
3. RBA の適用は、金融庁も含め依然として初期段階にあるものの、AML/CFT に係る監督の深度は徐々に改善しつつある。
4. 金融庁は、特定の金融機関との間で対話を行った場合、その後、緊密なフォローアップの取組を実施していることを示した。
5. 金融庁を含む金融監督当局は、金融機関に対する効果的かつ抑止力のある一連の制裁措置を活用していない。
6. 日本は、暗号資産交換業者セクターに対し、対象を絞り適時な法令及び監督対応を実施した。不備の認められる暗号資産交換業者に対して迅速かつ強固な対応を行ってきたことは認められるものの、マネロン・テロ資金供与リスクに基づく監督上の措置は改善する必要がある。
7. DNFBPs の監督当局は、マネロン・テロ資金供与リスクの理解が限定的であり、リスクベースによるAML/CFT に係る監督を実施していない。

IO.4（金融機関等の対応の有効性）

1. 大規模銀行（より高いリスクを有する金融機関として認識されているグローバルなシステム上重要な銀行（GSIB）等）を含む一定数の金融機関及び資金移動業者は、マネロン・テロ資金供与リスクについて適切な理解を有している。その他の金融機関においては、自らのマネロン・テロ資金供与リスクの理解が限定的である。
2. 金融機関がマネロン・テロ資金供与リスクについて限定的な理解しか有していない場合、金融機関のリスクベース・アプローチ（以下、RBA）の適用に直接的な影響を及ぼす。
3. このような金融機関は、最近導入・変更されAML/CFT に係る義務について十分な理解を有しておらず、これらの新しい義務を履行するための明確な期限を設定していない。
4. 指定非金融業者及び職業専門家（以下、DNFBPs）は、マネロン・テロ資金供与リスクやAML/CFT に係る義務について低いレベルの理解しか有していない。
5. 暗号資産交換業者は、暗号資産取引に関連する犯罪リスクについて一般的な知識を有し、基本的なAML/CFT に係る義務を実施している。
6. 疑わしい取引の届出の総件数（年ベース）は増加傾向にあるところ、疑わしい取引の届出の大部分は金融分野からのものであり、
7. 暗号資産交換業者の届出の実績も良いが、全体的にみて、疑わしい取引の届出は、基本的な類型や疑わしい取引の参考事例を参照して提出されている傾向がある。
8. また、特定のマネロン・テロ資金供与リスクに直面している一部のDNFBPsを含め、全てのDNFBPs が、疑わしい取引の届出義務の対象になっているわけではない。

11. 第４次相互審査の有効性検証(IO)の結果

被審査国	IO1	IO2	IO3	IO4	IO5	IO6	IO7	IO8	IO9	IO10	IO11
Norway	M	S	M	M	M	M	M	M	S	M	M
Spain	S	S	S	M	S	H	S	S	S	M	M
Australia	S	H	M	M	M	S	M	M	S	M	S
Belgium	S	S	M	M	M	S	M	M	S	M	M
Malaysia	S	M	S	M	M	S	M	M	M	S	M
Italy	S	S	M	M	S	S	S	S	S	M	S
Austria	M	S	M	M	M	L	L	M	S	M	S
Canada	S	S	S	M	L	M	M	M	S	S	M
Singapore	S	S	M	M	M	S	M	M	L	M	S
Switzerland	S	M	M	M	M	S	S	S	S	S	S
US	S	S	M	M	L	S	S	H	H	H	H
Sweden	M	H	M	M	M	M	S	S	S	M	S
Denmark	M	S	L	L	M	M	M	M	S	M	S
Ireland	S	S	S	M	M	S	M	M	M	M	S
Mexico	S	S	M	L	M	M	L	L	M	S	S
Portugal	S	S	M	M	M	M	S	M	S	S	S
Iceland	L	S	L	L	L	M	M	M	M	L	L
Bahrain	M	S	S	M	M	S	M	M	M	M	M
Saudi Arabia	S	M	S	M	M	M	L	L	S	S	L
Israel	S	S	M	M	S	H	S	H	H	S	M
UK	H	S	M	M	S	M	S	S	H	H	H
China	S	M	M	L	L	M	M	S	S	L	L
Finland	S	H	L	M	M	S	S	M	M	M	M
Greece	S	S	M	M	M	S	M	M	S	M	S
HK, China	S	S	M	M	M	S	M	S	S	S	M
Russia	S	S	M	M	S	H	M	S	H	M	M
Turkey	S	S	M	M	M	M	M	M	M	L	L
Korea	S	S	M	M	M	S	M	S	S	M	M
UAE	M	L	M	M	L	M	L	M	S	M	L
New Zealand	S	H	M	M	M	S	S	H	S	M	M
日本	S	S	M	M	M	S	M	M	M	M	M
South Africa	M	M	M	M	L	M	M	M	L	L	M

（※）評価は高い順にH>S>M>L

12. 第４次相互審査を受けたFATF加盟国の結果

通常フォローアップ国	8か国	スペイン、イタリア、ポルトガル、イスラエル、英国、ギリシャ、香港、ロシア
重点フォローアップ国	19か国	ノルウェー、オーストラリア、ベルギー、マレーシア、オーストリア、カナダ、シンガポール、スイス、米国、スウェーデン、デンマーク、アイルランド、メキシコ、サウジアラビア、中国、フィンランド、韓国、ニュージーランド、**日本**
観察対象国	2か国	アイスランド、南アフリカ

（注1）審査を実施した順番。下線付きは、審査を終了したG7国。
（注2）今後の審査予定国：フランス、ドイツ、オランダ、ルクセンブルク、インド、ブラジル、アルゼンチン

出所：FATFの第４次対日相互審査報告書より、筆者等が作成

13. FATF相互審査結果：ハイリスク･非協力国

■ 更に、一定条件*に該当した観察対象国･地域は、１年間の経過観察期間を経た後に不備事項の再審査が行われる。状況の改善が見られない国･地域は、グレイ･リスト国としてFATFから公表される。

ハイリスク･非協力国	2021年10月時点の公表国
改善に向けて政治的にコミットしているが、戦略的欠陥を有し取組が奨励される国 （モニター対象国　**グレイ･リスト国**）	トルコ、ヨルダン、マリ、アルバニア、バルバトス、ブルキナファソ、カンボジア、ケイマン諸島、ハイチ、ジャマイカ、マルタ、モロッコ、ミャンマー、ニカラグア、パキスタン、パナマ、フィリピン、セネガル、南スーダン、シリア、ウガンダ、イエメン、ジンバブエ
顕著な進展を見せていない、あるいは取組への政治的意思が欠如していることから、関連した欠陥から起こるリスクが考慮されるべき国･地域（対抗措置なし　**ブラック･リスト国**）	なし
対抗措置の適用対象国･地域 （**対抗措置あり　ブラック･リスト国**）	**北朝鮮、イラン**

*各国相互評価の結果、以下に該当する観察対象国･地域が対象

TC評価：PC･NC≧20　ＯＲ　有効性評価：M･L≧9 or L≧6 等

出所：財務省　令和元年6月14日、財務省関税･外国為替等審議会　第41回外国為替等分科会 資料、FATF公表より筆者作成

14. マネロン・テロ資金供与・拡散金融対策に関する行動計画の概要（抄）

項目	具体的な対応	期限
①リスク評価及び政策会議の設置	• 国のリスク評価書を刷新する。	2021年末
	• 「マネロン・テロ資金供与・拡散金融対策政策会議」を設置する。	実施中
②金融機関等の監督強化	• 金融機関等に対するリスクベースでの検査監督を強化する。 • マネロン等対策に関する監督ガイドラインを更新・策定する。	2022年秋
③金融機関等のリスク理解向上とリスク評価の実施	• マネロン・テロ資金供与・拡散金融対策に係る義務の周知徹底を図ることで、金融機関等のリスク理解を向上させ、適切なリスク評価を実施させる。	2022年秋
④金融機関等による継続的顧客管理の完全実施	• 取引モニタリングの強化を図るとともに、期限を設定して、継続的顧客管理などリスクベースでのマネロン・テロ資金供与・拡散金融対策の強化を図る。	2024年春
⑤取引モニタリングの共同システムの実用化	• 取引時確認、顧客管理の強化および平準化の観点から、取引スクリーニング、取引モニタリングの共同システムの実用化を図るとともに、政府広報も活用して国民の理解を促進する。	2024年春
⑥実質的支配者情報の透明性向上	• 商業登記所が株式会社の実質的支配者情報を保管し、その旨を証明する制度を開始する。（2022年１月～（予定）） • 当該情報の一元管理に向けた検討を実施する。	2022年秋
⑦資産凍結及びNPOの悪用防止	• 大量破壊兵器拡散にかかわる居住者の資産凍結を実施する法制度の整備について検討し、所要の措置を講じる。	2022年夏
	• NPOにかかるリスク評価を行い、リスクベースでモニタリングを実施する。	2022年春

15. 2021事務年度金融行政方針（令和３年8月31日公表）（抄）

６．様々なリスクへの備え

デジタル化やグローバル化が急速に進展する中で、強靭な金融システムを構築していくためには、様々なリスクへの備えが不可欠だ。

（１）マネロン・テロ資金供与・拡散金融対策の強化

技術の進化による決済手段の多様化や取引のグローバル化等が進行し、金融取引がより複雑化する中、国際的には、金融機関等に対し、リスクの変化に応じた継続的な管理態勢の高度化が求められている。海外では経営陣の交代や高額の罰金を含む処分を課せられる事例も発生するなど、マネー・ローンダリング（資金洗浄、以下「マネロン」）・テロ資金供与・拡散金融管理態勢の脆弱性が金融機関の経営に与える影響度も拡大している。

そのような環境下、FATF（金融活動作業部会）第４次対日相互審査の結果も踏まえ、引き続き関係省庁や業界団体等とも連携し、丁寧な顧客対応の促進や、顧客の実態把握に関する取組みについての利用者の理解向上を図りつつ、我が国における金融機関等のマネロン・テロ資金供与・拡散金融対策の高度化に向けた施策を着実に実行していく。

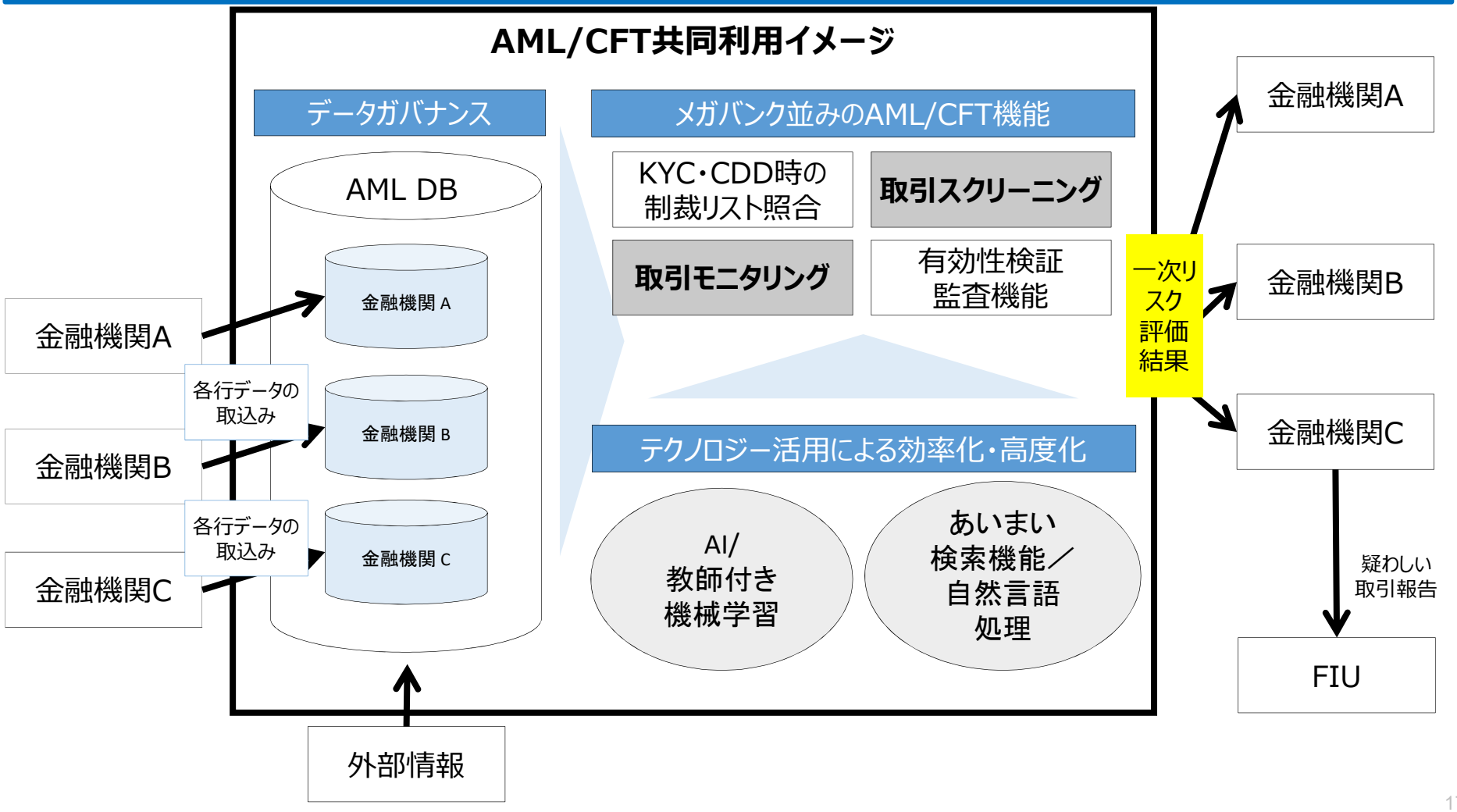
具体的には、検査要員の確保等により検査・監督体制を強化し、リスクが高いとされる業態を優先的に、リスクベースでの検査・監督を実施する。

また、マネロン・テロ資金供与・拡散金融対策の高度化・効率化のため、各金融機関等による共同システムの実用化の検討・実施に取り組む。

FATF 等における国際的な議論について、特に、「暗号資産及び暗号資産交換業者に対するリスクベースアプローチに関するガイダンス」改訂案の最終化など、金融庁が共同議長を務めるコンタクト・グループ関係の作業を中心に、主導的な役割を果たす。

16. AML/CFTシステム共同利用イメージ

- AI等を活用したAML/CFTプロセスの共同化を通じ、金融業界全体のAML/CFT態勢の有効性向上、効率化、規制の精緻化を目指す。
- 現在、全銀協を中心に実用化の検討を進めているところ。また、金融審議会資金決済WGでも議論を開始。



17. 業界団体と連携した、マネロン等対策に係る預金者・利用者への情報発信

金融庁ホームページ　抜粋

金融庁
Financial Services Agency

▼本文へ　音声読み上げ　文字サイズ 大 中 小　日本語　English

サイト内検索　Google 提供

ホーム　金融庁について　お知らせ・広報　政策・審議会等　法令・指針等　アクセスFSA（金融庁広報誌）　金融機関情報　国際関係

ホーム ＞

金融機関窓口や郵送書類等による確認手続にご協力ください

金融庁・金融機関は、金融サービスを悪用するマネー・ローンダリング・テロ資金供与・拡散金融の対策（以下、マネロン等対策）に取り組んでいます。

犯罪で得られたお金を多数の金融機関を転々とさせることで資金の出所をわからなくしたり、テロリスト等に容易にお金を送金されてしまうと、将来の犯罪活動やテロ活動を助長することになってしまいます。このため、年々複雑化・高度化するマネロン等の手口に対抗できるよう、金融機関では様々な確認手続を行うなどして、対応を進めています。犯罪組織やテロリスト等への資金の流れを止めることで犯罪やテロを未然に防止して、皆様の安心・安全な生活を守るとともに、皆様の預金や資産を守るため、ご理解とご協力をお願いいたします。

・金融機関から、お客さまの情報やお取引の目的等の定期的な確認を求められる場合がありますのでご協力をお願いいたします。

・取引の内容、状況等に応じて、過去に確認した氏名・住所・生年月日・職業等や、取引の目的等（法人の場合は、住所や事業内容、株主情報等）について、窓口や郵送書類等により再度確認を求められる場合があります。また、その際に、各種書面等の提示を求められる場合があります。

【確認を求められる事項の例】
個人の場合：氏名、住所、生年月日、職業等
　　取引の目的等
法人の場合：住所、事業内容、株主情報等、実質的支配者
　　取引の目的等

イラスト出典：政府広報オンライン

※法人の場合は、その法人を実質的に支配することが可能となる自然人（「実質的支配者（※）」と言います）も確認が求められます。

（※）実質的支配者については、「取引時確認の適正な実施について」をご確認ください

各種窓口のご案内
金融行政モニター
入札公告等
申請・届出・照会
パブリックコメント
情報公開等
利用者の方へ
採用情報

関連リンク
新着情報配信サービス
調達情報配信サービス
金融庁ソーシャルメディアアカウント

DOWNLOAD ADOBE® READER®

【参考リンク】（全国銀行協会）
TVCM・店頭動画

テレビCM用映像（30秒）

店頭用映像（2分）

関連リンク

- 金融機関におけるマネロン・テロ資金供与・拡散金融対策について

金融機関への要請等
- マネー・ローンダリング及びテロ資金供与対策に係る態勢整備の期限設定について

関係省庁等の取組
- 政府広報オンライン「金融機関などでの取引時に行う「本人確認」等にご協力ください」

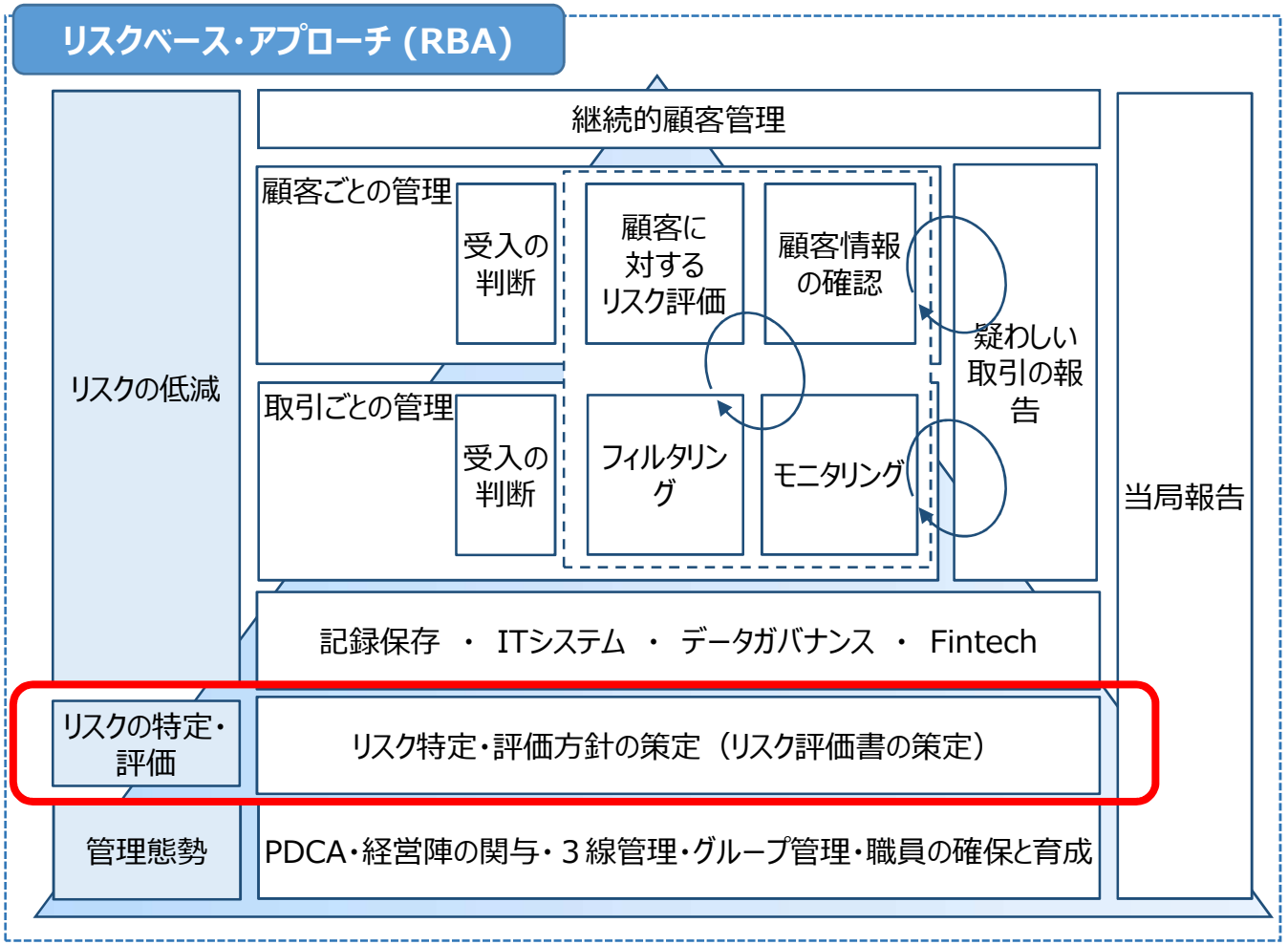
金融機関の取組
- 一般社団法人 全国銀行協会「銀行をご利用のお客さまへのお知らせ」
- 一般社団法人 全国地方銀行協会「取引時確認にご協力ください」
- 一般社団法人 第二地方銀行協会「金融機関窓口などでの取引時の情報提供にご協力ください」
- 一般社団法人 全国信用金庫協会「信用金庫をご利用のお客さまへのお知らせ」
- 一般社団法人 全国信用組合中央協会 重要なお知らせ「お取引時の確認についてのご協力のお願い」
- 一般社団法人 全国労働金庫協会「ろうきんをご利用のお客さまへのお知らせ」
- 一般社団法人 生命保険協会「取引時確認に関するお客さまへのお願い」
- 一般社団法人 日本損害保険協会「犯罪収益移転防止法に基づく「取引時確認」について」
- 日本証券業協会「証券業界におけるマネー・ローンダリング及びテロ資金供与対策への取組み」

18. 金融機関等におけるマネー・ローンダリング対策のイメージ

◆ マネロン等リスクを特定・評価の上、リスクに応じた低減措置を講ずる**「リスクベースアプローチ」**が基本である。
◆ 低減措置は、顧客毎・取引毎の管理があり、中でも、継続的顧客管理は最も重要な対策の一つである。

◆ 低減措置に基づき、疑わしい取引を届け出るとともに、届出を分析の上、低減措置も見直す必要がある。

◆ これらの対策の実施に当たっては、経営陣の関与や３線管理の構築など、管理態勢の構築が求められる。



19. 金融庁「マネロン対策ガイドライン」の策定及び改正

- 2018年2月、金融庁は、金融機関等における、**リスクベース・アプローチ**によるマネロン・テロ資金供与リスク管理態勢の構築・維持に向け、「**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**」を策定し、2019年４月、ガイドラインで求めている趣旨を明確化するために改正を実施。（１回目）
- 2021年２月、１回目の改正以降に実施したモニタリングにおいて把握した課題等を整理・反映した改正版ガイドラインを公表（2回目）。

基本的考え方

- **マネロン・テロ資金供与対策に係る基本的考え方**
  ⇒ 時々変化する国際情勢等の変化に対して、機動的かつ実効的な対応を実施するためには、自らのリスクを適時・適切に特定・評価し、リスクに見合った低減措置を講ずる**「リスクベース・アプローチ」の手法**を用いることが不可欠
- **金融機関等に求められる取組み**
  ⇒ 事業環境・経営戦略、リスクの許容度等を踏まえ、**経営陣の主体的かつ積極的な関与**の下、組織全体としてマネロン・テロ資金供与対策を高度化することが重要
- **業界団体・中央機関の役割** ⇒ 金融機関等の実効的な取組みに資する**情報・事例等の共有**、システム共同運用の促進
- **本ガイドラインの位置付け**

RBA※

- **リスクの特定**
  リスクの所在を特定する作業。金融機関等の規模・特性等を踏まえ、包括的かつ具体的に特定
- **リスクの評価**
  特定したリスクを評価する作業。金融機関等の事業環境・経営戦略等を踏まえて、全社的に実施
- **リスクの低減**
  特定・評価したリスクを低減する作業。実際の顧客や取引のリスクに応じ、実効的に低減措置を実施
  例：顧客管理、取引モニタリング・フィルタリング、疑わしい取引の届出、ITシステムの活用 等

- **海外送金等を行う場合の留意点**
- **FinTech等の活用**

管理態勢

- **マネロン・テロ資金供与対策に係るPDCA** ⇒ マネロン・テロ資金供与対策の方針・手続・計画等を策定、検証、見直し
- **経営陣の関与・理解** ⇒ マネロン・テロ資金供与対策を**経営戦略等における重要な課題**に位置付け、**適切な資源配分**
- **経営管理**
  - **第１線**：顧客と接点のある営業部門が、方針や手続等を理解して対応
  - **第２線**：担当役員等を中心に、管理部門が第１線を継続的モニタリング
  - **第３線**：マネロン・テロ資金供与対策にかかる必要な監査を実施
- **グループベースの管理態勢** ⇒ グループ全体に整合的な形でマネロン・テロ資金供与対策を実施
- **職員の確保、育成等** ⇒ 専門性・適合性等を有する職員の採用、研修による職員の理解の促進

当局

- **金融庁によるモニタリング**
- **官民連携** ⇒ 業界団体、関係省庁等との連携による情報発信や金融機関等との対話

20. FATF：11の短期的目標（Immediate Outcome）

最終目標

金融システム及び経済全体がML/TF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、安全と安定に貢献すること。

（出所：FATF公表資料より、筆者作成資料）

中間的目標		短期的目標（Immediate Outcome）	
1	政策、調整及び協力がML/TFのリスクを軽減している。	1	ML/TFリスクが理解され、適切な場合、ML/TF及び拡散金融との闘いに向けた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措置を促進している。
2	犯罪収益及びテロ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	**金融機関等が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	**金融機関等が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がML/TF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。
3	マネロン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。 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ML/TF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	マネロンが捜査され、行為者が訴追され、効果的で比例的かつ抑止的な制裁を受けている。
		8	犯罪収益及び手段が没収されている。
		9	テロ資金供与が捜査され、行為者が訴追され、効果的で比例的かつ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、移動、使用することが防止されており、NPOが濫用されていない。
		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。

21. IO. 4 金融機関及びDNFBPsにおける予防措置 主要課題(Core Issues)

4.1 **金融機関等は、自身のML/FTリスク及びAML/CFT義務をどのように理解しているか。**

4.2 金融機関等は、自身の**ML/FTリスクに見合ったリスク軽減措置**をどのように実施しているか。

4.3 金融機関等は、**顧客管理措置及び記録保存措置**（**実質的所有者情報及び継続的モニタリング**を含む）をどのように実施しているか。顧客管理措置が不十分な場合、取引は**どの程度拒絶されるのか**。

4.4 金融機関等は、**(a)PEPs、(b)ｺﾙﾚｽ銀行、(c)新しい技術、(d)電信送金、(e)テロ資金供与に関係する金融制裁、(f)FATF が特定した高リスク国**に対し、**厳格な措置又は特別な措置**をどのように適用しているか。

4.5 金融機関等は、**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**をどのように果たしているか。**内報を防ぐ現実的方策**として、どのような対策を講じているか。

4.6 金融機関等は、AML/CFTに関する義務の履行確保のための内部管理及び手続をどのように構築しているか（グループベース・グローバルベース）。

（出所：FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems）
上記は仮訳であることから、正確な内容については原文を参照のこと

22. IO. 4：金融機関及びDNFBPsにおける予防措置

a.主要課題の結論を導く情報の例

1. **金融機関等セクターに関する規模、構成、構造といった文脈的要素**（例：それぞれのカテゴリーにおいて免許を受けた又は登録された金融機関〔資金移動業者を含む〕等の数と種類。金融取引〔クロスボーダーを含む〕の種類。各セクターの相対的規模、重要性、重大性。）

2. **リスク及び一般的な法令遵守の度合に関する情報**（傾向を含む）（例：内部AML/CFTポリシー、手続、計画。傾向及びタイポロジーに関する報告。）

3. **法令遵守の不備事例**（例：実際に起こった事例＜ 特定できないもの＞ 。金融機関等の濫用に関するタイポロジー。）

4. **金融機関等による法令遵守に関する情報**（例：AML/CFTの法令遵守に係る内部検証の頻度。特定された違反の性質並びに採られた是正行動及び適用された処分。AML/CFTの研修の頻度と質。AML/CFT目的の正確かつ完全な顧客管理情報を所管当局に提出するために要する時間。不完全な顧客管理情報を理由に拒絶された口座又は取引関係。必須情報が不十分であることを理由に拒絶された電信送金）

5. **疑わしい取引の届出に関する情報やその他の国内法令によって義務付けられる情報**

   （例：疑わしい取引の届出件数及び関連する取引の価額。セクター毎の疑わしい取引の届出件数と割合。ML/FTリスク毎の疑わしい取引の届出の種類、性質、傾向。疑わしい取引の届出を行うまでに要する分析の平均時間。）

（出所：FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems）
※上記は仮訳であることから、正確な内容については原文を参照のこと

23. IO. 4：金融機関及びDNFBPsにおける予防措置

b.主要課題の結論を導く特定要素

6. より高リスクの（場合によっては、より低リスクの）顧客、ビジネス関係、取引、商品、国を特定し、取り扱うために採られている措置は何か。
7. AML/CFT措置の適用方法は、公式の金融システムの合法な使用を阻害するようなものになっていないか（De-Riskingとなっていないか）。金融包摂を促進するためにどのような措置が採られているか。
8. 顧客管理措置、厳格な措置や特定の措置は、異なるセクター/種類や個別業者のML/FTリスクに応じて、どの程度異なるのか。国際的な金融グループと国内金融機関との間で法令遵守の度合はどの程度異なるか。
9. 第三者への顧客管理措置の依存はどの程度あるか。そのコントロールは適切になされているか。
10. 金融機関とそのグループやDNFBPs は、AML/CFTの法令遵守担当部署による情報へのアクセスをどの程度確保しているか。
11. 金融機関とそのグループやDNFBPs の内部方針及び内部管理は、（i）複雑又は異常な取引、（ii）FIUへの届出が必要となり得る疑わしい取引、（iii）誤検知が疑われる取引に係る適時の検証を定めているか。届出された疑わしい取引の報告書は、疑わしい取引についてどの程度完全、正確かつ適切な情報を含んでいるか。
12. リスクを評価するほか、方針上の対応の策定・見直しを行い、また、適切なリスク低減策やシステム、そして管理態勢を講じるために、どのような措置やツールが用いられているか。
13. 上級管理者及びスタッフに対してAML/CFT方針及び管理がどのように周知されているか。AML/CFTに関する義務違反が生じた時、金融機関等はどのような是正行動を採り、処分を課しているか。
14. 金融機関等は、どの程度適切にML/FTリスク評価を文書化するとともに最新の状態に保っているか。
15. 金融機関等は、その規模、複雑性、事業内容、リスクプロファイルに見合ったAML/CFT方針及び管理を実施するにあたり、適切な資源を割いているか。
16. 疑わしい取引の検知及び届出について、金融機関等を支援するためのフィードバックが、どの程度十分に提供されているか。

（出所：FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems）
※上記は仮訳であることから、正確な内容については原文を参照のこと

24. Core Issue 4.1 自身の直面するリスク及び義務の理解

4.1 金融機関等は、自身のML/FTリスク及びAML/CFT義務をどのように理解しているか。

ポイント

（注：以下のI.O.4に関する「ポイント」は各種公表資料より筆者が作成したもの。）

- 最も重要な最初の項目は、マネロン・テロ資金供与のリスクをどのように評価し、それに伴う義務を理解しているか？という認識を問うもの。
- リスク評価は、全ての商品・サービス、取引形態、国・地域、顧客属性に着目した包括的なもので、犯罪収益移転危険度調査書等の国によるリスク評価文書を踏まえ、さらに、自らの過去に提出した疑わしい取引の届出の分析、金融犯罪の被害状況、警察からの凍結要請、捜査関係事項照会等を勘案し、評価方法と結果がリスク評価書に記載されていることが必要。
- 義務の理解は、犯罪収益移転防止法や外為法といった法令等の遵守のみならず、金融庁の「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」で求められているリスクベース・アプローチに基づく管理態勢を構築し、継続的に見直していくという義務の理解が必要。
- 具体的には、ガイドラインにおける以下の項目を実施する必要あり：
  - リスクに応じた顧客管理措置、取引モニタリング・フィルタリング（＝制裁対象者や反社等のリストとの照合）
  - 海外送金、現金取引など、リスクが高い取引の管理
  - 記録保存
  - 疑わしい取引の届出（質・量の充実とスピードの両立）と分析、態勢強化への活用
  - 方針・手続・計画等の策定・実施・検証・見直し（PDCA)の枠組みの構築
  - 経営陣への報告、経営陣の関与・理解
  - 三つの防衛線を活用した経営管理
  - グループベースの管理態勢
  - 職員の確保・育成

25. Core Issue 4.2 リスクに応じたリスク低減措置の実施状況

4.2　金融機関等は、自身のML/FTリスクに見合ったリスク低減措置をどのように実施しているか。

ポイント

- リスクに見合ったリスク低減措置は、適切なリスク評価を前提とする。顧客に着目した顧客管理、取引に着目した取引モニタリングと疑わしい取引の届出、及び、それらの記録保存の実施等が求められる。
- 取引のモニタリング
  - 外為送金取引の実行前（被仕向送金については顧客口座への入金前）のリスクに応じた確認
  - 送金関係者（送金依頼人・受取人等）の制裁対象者・反社リストとの照合（あいまい検索の活用）
  - 送金依頼人、送金内容、受取人の国・地域のリスクに応じた確認（何をどこまで確認するのか、手順を規程・マニュアルに定め、関係者に周知徹底する）
  - 事後的な取引モニタリング（外為、内為、入出金のパターン分析）
  - システムを活用した取引モニタリング等の敷居値設定をリスクに応じて変更
- 顧客管理
  - 口座開設時の本人確認（法人の場合は**実質支配者の確認を含む**）、制裁対象者・反社リストとの照合、及び顧客のリスク評価
  - 取引継続時の継続的な顧客管理、すなわち、リスクに応じた頻度での実態把握、リスク評価の見直し（リスクが高まる事象が発生した際には、直ちに見直し）

26. IO. 4.6　内部管理（グループ及びグローバル管理）の状況

4.6　金融機関等は、AML/CFTに関する義務の履行確保のための**内部管理及び手続**をどのように構築しているか（グループベース・グローバルベース）。

ポイント

- 金融機関等は、マネロン・テロ資金供与対策に関するプログラムの実施が求められなければいけないことがFATF勧告に沿って定められ、かかるプログラムには、内部の方針、管理手続等が規程化され、継続的な従業員の訓練プログラムが定められ、及び同プログラムの有効性を監視するための独立した内部監査機能が含まれていること
- 上記プログラムはリスクベース・アプローチに基づいており、役員レベルにおける責任者の任命が含まれること

※グループ会社に特定事業者が含まれる場合には、グループベースの管理態勢の構築が求められ、海外拠点がある場合には、グローバルベースの対応が求められる。例えば、グループ・グローバル全てに適用される上位規程の制定、本店によるモニタリングとグループ会社・海外拠点のリスク評価、経営陣へのこれらの報告及び監査手続も求められることになる。

勧告18．内部管理、外国の支店及び子会社

金融機関等には、資金洗浄及びテロ資金供与対策プログラムの実施が求められなければならない。金融グループは、資金洗浄及びテロ資金供与対策目的のため、グループ全体として、情報共有に関する政策及び手続きを含む資金洗浄及びテロ資金供与対策に関するプログラムの実行が求められる。

金融機関には、金融グループの資金洗浄及びテロ資金供与に対するプログラムを通じて、海外支店及び過半数の資本を所有している子会社に対し、本国のFATF 勧告の実施義務と整合的な資金洗浄及びテロ資金供与対策の措置が適用されることを確保することが求められるべきである。

27. 内部監査へ期待されること (1)

「銀行のためのコーポレートガバナンス諸原則　原則10：内部監査」
(バーゼル銀行監督委員会)

"The internal audit function should provide independent assurance to the board and should support board and senior management in promoting an effective governance process and the long-term soundness of the bank."

「内部監査機能は、取締役会に対して独立した保証（アシュアランス）を提供し、取締役会及び上級経営陣が、効果的なガバナンス・プロセスと銀行の長期的な健全性を促すことを、支援すべきである。」

「内部監査のミッション」（The Mission of Internal Audit）
内部監査人協会(The Institute of Internal Auditors)

"The mission of the internal audit function is to provide independent, objective assurance and consulting services designed to add value and improve the Institute of Internal Auditors" "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight"

「内部監査の使命は、リスクに根差した客観的な保証（アシュアランス）、助言及び洞察を提供することにより、組織体の価値を高め、保全することである。」

28. 内部監査へ期待されること (2)

「専門職的実施の国際フレームワーク」

(International Professional Practices Framework: IPPF)®

The Institute of Internal Auditors（略称 IIA:内部監査人協会）

2110 ： ガバナンス

内部監査部門は、次の事項に係る組織体のガバナンス・プロセスを評価し、ガバナンス・プロセ スの改善のための適切な提言をしなければならない。

- 戦略的意思決定および業務上の意思決定
- リスク・マネジメントおよびコントロールの監督
- 組織体における適切な倫理観と価値観の向上
- 組織体の有効な業績管理とアカウンタビリティの確保
- リスクとコントロールに関する情報の、組織体の適切な部署への伝達
- 取締役会、外部監査人、内部監査人、他のアシュアランスの提供者および経営管理者間の活動の連携と、これらの者の間での情報の伝達

2110.A1： 内部監査部門は、組織体の倫理関連の目標、プログラムおよび活動に関する、設計および実施の状況、ならびに有効性を評価しなければならない。

2110.A2： 内部監査部門は、組織体の情報技術（IT）ガバナンスが、組織体の戦略や目標を支えているかどうかを評価しなければならない。

2120：リスク・マネジメント

内部監査部門は、リスク・マネジメント・プロセスの有効性を評価し、リスク・マネジメント・ プロセスの改善に貢献しなければならない。

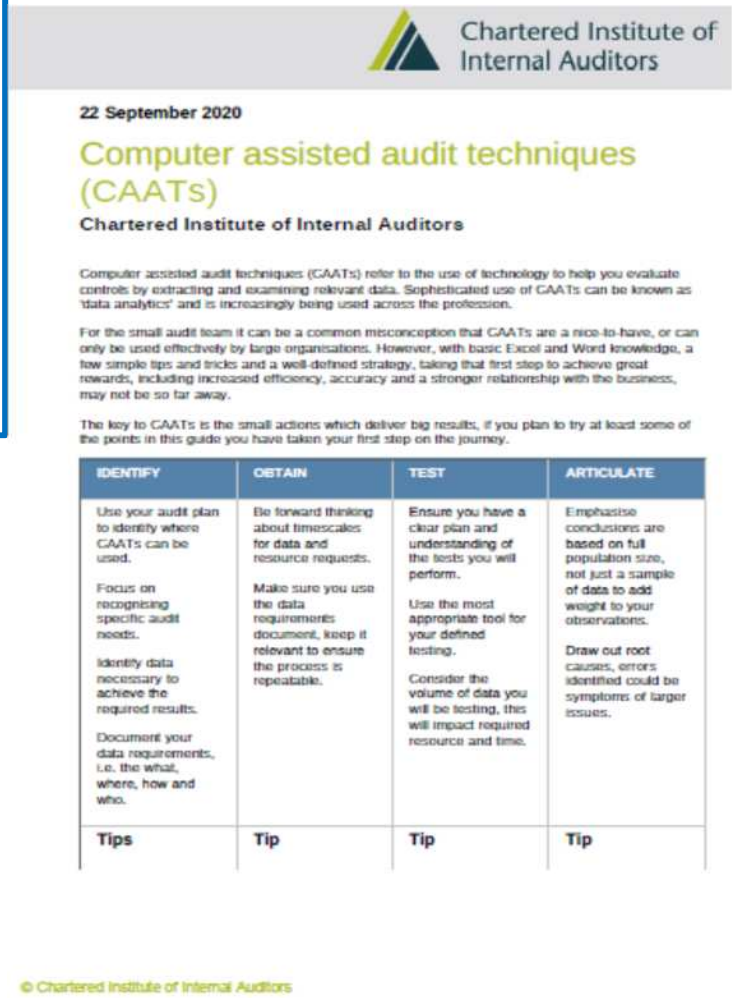
29. 内部監査へ期待されること (3)

CAAT（Computer Assisted Audit Techniques/コンピュータ支援監査技法）

- 経営資源は無限ではなく、リスクが高い分野へ重点を置いたリスクベース監査が望ましい。
- 監査の分野でも多くのデータを効率よく分析して、傾向や異常値等を識別する取り組みが有益。この観点から、CAAT（Computer Assisted Audit Techniques/コンピュータ支援監査技法）の活用が進んでいる。
- 他方で、CAATのみならず通常のサンプル監査においても、なぜその事案にその検証方法を当てはめたのか、合理的かつ客観的な説明ができることが望ましい。

（参考：私見）
業務データ量の増加に伴い、サンプルベースの監査では十分な保証や信頼度の確保が難しいという論点もある。その点、テクノロジーを活用することにより、リスクの特定・評価、コントロールの検証、証跡の確認が効率化できる可能性があり、そのようなテクノロジーを活用した内部監査は、伝統的な監査手法を実施していたときよりも、より高度な保証を提供できる可能性がある。
たとえばCAATツールを活用して、監査対象分野の事前データ分析を通じて、異常値・非定型な取引を把握し、監査対象サンプルを絞り込んだり、サンプルベースではなく全件検証を行うことが可能となってきている。
この観点から、取引モニタリングシステムの有効性検証や出すべき不自然な取引が検知漏れ、提出漏れとなっていないか、スクリーニングシステムのリスト情報に漏れがないかの独立した検証には、CAATの活用の余地があるのではないか。

（参考文献）the Chartered IIAのCAATsに関する報告書



Chartered Institute of Internal Auditors

22 September 2020

Computer assisted audit techniques (CAATs)

Chartered Institute of Internal Auditors

Computer assisted audit techniques (CAATs) refer to the use of technology to help you evaluate controls by extracting and examining relevant data. Sophisticated use of CAATs can be known as 'data analytics' and is increasingly being used across the profession.

For the small audit team it can be a common misconception that CAATs are a nice-to-have, or can only be used effectively by large organisations. However, with basic Excel and Word knowledge, a few simple tips and tricks and a well-defined strategy, taking that first step to achieve great rewards, including increased efficiency, accuracy and a stronger relationship with the business, may not be so far away.

The key to CAATs is the small actions which deliver big results, if you plan to try at least some of the points in this guide you have taken your first step on the journey.

IDENTIFY	OBTAIN	TEST	ARTICULATE
Use your audit plan to identify where CAATs can be used. Focus on recognising specific audit needs. Identify data necessary to achieve the required results. Document your data requirements, i.e. the what, where, how and who.	Be forward thinking about timescales for data and resource requests. Make sure you use the data requirements document, keep it relevant to ensure the process is repeatable.	Ensure you have a clear plan and understanding of the tests you will perform. Use the most appropriate tool for your defined testing. Consider the volume of data you will be testing, this will impact required resource and time.	Emphasise conclusions are based on full population size, not just a sample of data to add weight to your observations. Draw out root causes, errors identified could be symptoms of larger issues.
Tips	Tip	Tip	Tip

© Chartered Institute of Internal Auditors

30. AML/CFT管理における内部監査

金融庁「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」

Ⅲ－３　経営管理（三つの防衛線等）

金融機関等においては、**その業務の内容や規模等に応じ**、有効なマネロン・テロ資金供与リスク管理態勢を構築する必要があり、営業・管理・監査の各部門等が担う役割・責任を、経営陣の責任の下で明確にして、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。

以下では、金融機関等に求められるマネロン・テロ資金供与リスク管理態勢の機能を、三つの防衛線の概念の下で整理した上で「対応が求められる事項」を記載しているが、各金融機関等において、業務の特性等を踏まえ、項目によっては異なる整理の下で管理態勢等（外部へのアウトソーシングを含む。）を構築することも考えられる。その場合であっても、それぞれの管理態勢の下で、「対応が求められる事項」が目標としている効果と同等の効果を確保することが求められる。

（３）第３の防衛線

第３の防衛線（第３線）は、**内部監査部門**を指している。内部監査部門には、第１線と第２線が適切に機能をしているか、更なる高度化の余地はないかなどについて、これらと**独立した立場から、定期的に検証していくこと**が求められる。

また、内部監査部門は、**独立した立場から、全社的なマネロン・テロ資金供与対策に係る方針・手続・計画等の有効性についても定期的に検証し、必要に応じて、方針・手続・計画等の見直し、対策の高度化の必要性等を提言・指摘すること**が求められる。

31. AML/CFT管理における内部監査

「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」（Ⅲ－３（３））

【対応が求められる事項】

① 以下の事項を含む監査計画を策定し、適切に実施すること

イ. マネロン・テロ資金供与対策に係る方針・手続・計画等の適切性

ロ. 当該方針・手続・計画等を遂行する職員の専門性・適合性等

ハ. 職員に対する研修等の実効性

ニ. 営業部門における異常取引の検知状況

ホ. 検知基準の有効性等を含むITシステムの運用状況

ヘ. 検知した取引についてのリスク低減措置の実施、疑わしい取引の届出状況

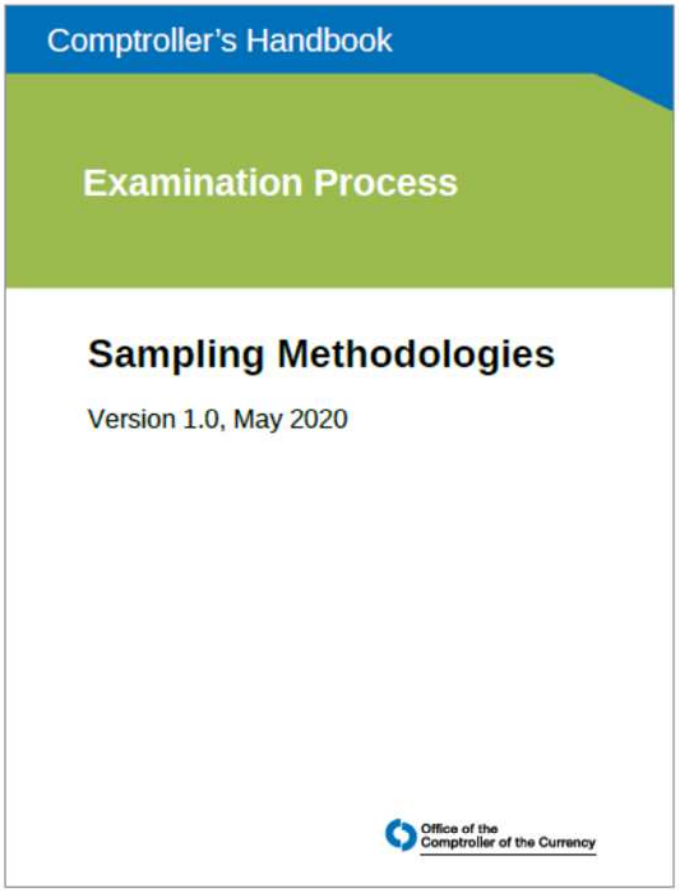
② 自らの直面するマネロン・テロ資金供与リスクに照らして、監査の対象・頻度・手法等を適切なものとすること

③ リスクが高いと判断した業務等以外についても、一律に監査対象から除外せず、頻度や深度を適切に調整して監査を行うなどの必要な対応を行うこと

④ 内部監査部門が実施した内部監査の結果を監査役及び経営陣に報告するとともに、監査結果のフォローアップや改善に向けた助言を行うこと

⑤ 内部監査部門にマネロン・テロ資金供与対策に係る適切な知識及び専門性等を有する職員を配置すること

32. サンプリング手法 The Office of the Comptroller of the Currency (OCC)



[20] Technical note: The sample size is based on the confidence level and tolerance rate using the following formula:

$$n = \frac{\ln(1 - C)}{\ln(1 - p)}$$

where

- the ln() operator denotes the natural logarithm function.
- p is the tolerance rate.
- c is the confidence level.
- n is the sample size.

Although the technical details of this calculation are not shown, it follows from standard manipulation of the binomial probability mass function.

Table 1: Sample Size Lookup Table

	Confidence level		
Tolerance rate	**90%**	**95%**	**99%**
1%	230	299	459
3%	76	99	152
5%	45	59	90
7%	32	42	64
10%	22	29	44

If the population size is less than the sample size reflected in table 1, examiners should review the entire population or consider using judgmental sampling. Examiners may consult with the Economic and Policy Analysis Division of the OCC's Economics Department to discuss other sampling methodologies.

Figure 1: Statistical Sampling Steps

33. サンプリング手法

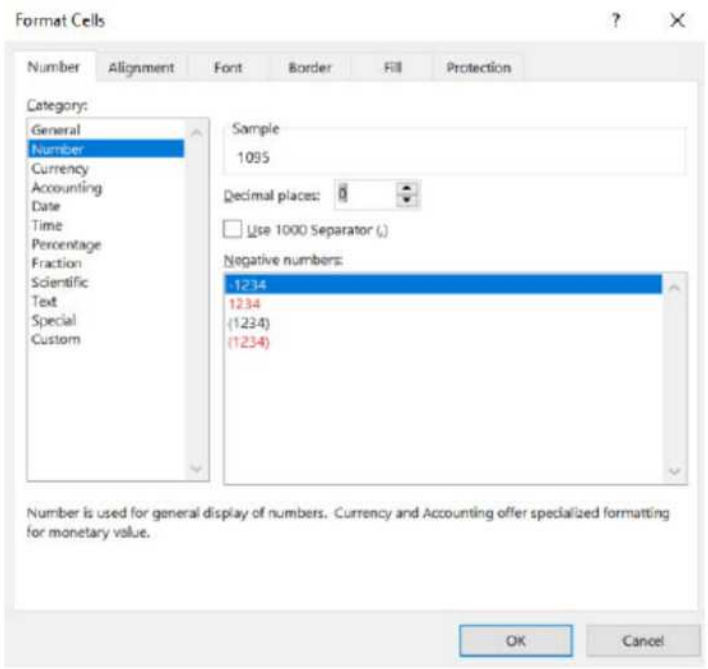
OCC Sampling Methodologies: Revised Comptroller's Handbook Booklet, May 2020

Appendix C: Generating Random Numbers Using Microsoft Excel

This appendix includes instructions and examples for generating random numbers using the =RAND() function in Microsoft Excel. The RAND() function generates random numbers between 0 and 1. The example in this appendix assumes a population size of 1,986 and a sample size of 22.

To generate whole numbers, change the formatting of the cells to use zero decimal places, as illustrated in figure 2.

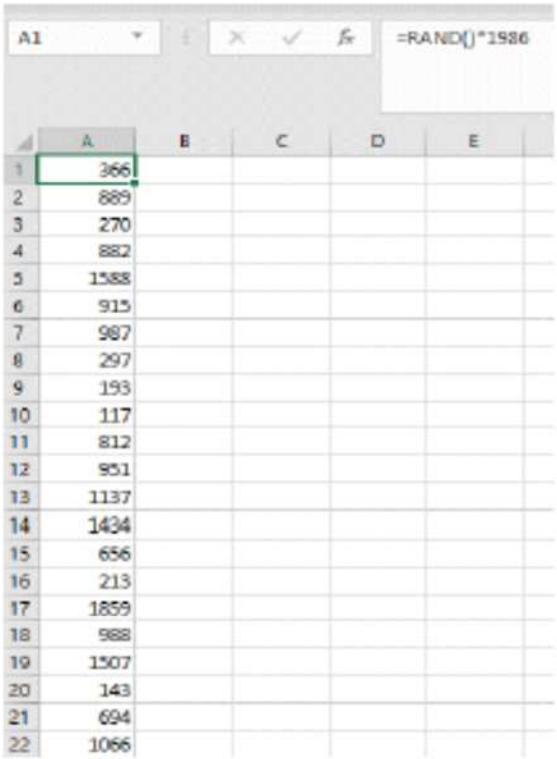
Figure 2: Format Cells Menu



To generate random numbers for a sample, enter =RAND() into a cell in Excel and multiply by the number of items in the population. Copy this formula to new rows of the spreadsheet until there are enough random numbers for the sample. An example is shown in figure 3. In this example, cell A1 is =RAND()*1986 because there are 1,986 items in the population. The examiner copied the formula to 22 rows of the spreadsheet because the sample size is 22.

Important note: Once the numbers are generated, examiners should immediately save the spreadsheet as a PDF, to preserve the generated numbers. Saving the spreadsheet in Excel format will generate a new set of random numbers each time the file is opened.

Figure 3: Excel Spreadsheet With Random Numbers



34. サンプリング手法

OCC Sampling Methodologies: Revised Comptroller's Handbook Booklet, May 2020

Appendix D: Statistical Sampling Confidence Bound Tables

Examiners use the tables in this appendix to determine the upper confidence bound on the population exception rate after testing items in a statistical sample.[28]

Table 4: Confidence Bounds for 90 Percent Confidence

Confidence level	Tolerance rate	Exceptions	Upper bound
90%	10%	0	10.00%
		1	16.56%
		2	22.42%
		3	27.89%
		4	33.10%
		5	38.12%
	7%	0	7.00%
		1	11.62%
		2	15.79%
		3	19.70%
		4	23.44%
		5	27.07%
	5%	0	5.00%
		1	8.37%
		2	11.40%
		3	14.25%
		4	16.98%
		5	19.64%
	3%	0	3.00%
		1	5.02%
		2	6.85%
		3	8.58%
		4	10.24%
		5	11.86%
	1%	0	1.00%
		1	1.68%
		2	2.30%
		3	2.88%
		4	3.45%
		5	4.00%

Table 5: Confidence Bounds for 95 Percent Confidence

Confidence level	Tolerance rate	Exceptions	Upper bound
95%	10%	0	10.00%
		1	15.34%
		2	20.16%
		3	24.61%
		4	28.84%
		5	32.89%
	7%	0	7.00%
		1	10.80%
		2	14.24%
		3	17.44%
		4	20.48%
		5	23.42%
	5%	0	5.00%
		1	7.79%
		2	10.29%
		3	12.62%
		4	14.85%
		5	17.00%
	3%	0	3.00%
		1	4.70%
		2	6.22%
		3	7.65%
		4	9.01%
		5	10.33%
	1%	0	1.00%
		1	1.58%
		2	2.09%
		3	2.57%
		4	3.04%
		5	3.48%

Table 6: Confidence Bounds for 99 Percent Confidence

Confidence level	Tolerance rate	Exceptions	Upper bound
99%	10%	0	10.00%
		1	14.16%
		2	17.77%
		3	21.07%
		4	24.18%
		5	27.14%
	7%	0	7.00%
		1	9.93%
		2	12.49%
		3	14.85%
		4	17.08%
		5	19.22%
	5%	0	5.00%
		1	7.15%
		2	9.01%
		3	10.73%
		4	12.36%
		5	13.92%
	3%	0	3.00%
		1	4.29%
		2	5.41%
		3	6.46%
		4	7.45%
		5	8.40%
	1%	0	1.00%
		1	1.44%
		2	1.82%
		3	2.17%
		4	2.51%
		5	2.83%

35. 実質的支配者リスト制度の創設（令和４年１月３１日運用開始）

- ■ 法人の実質的支配者に関する情報を把握することについては、法人の透明性を向上させ、資金洗浄等の目的による法人の悪用を防止する観点から、FATFの勧告や金融機関からの要望等、国内外の要請が高まっている。
- ■ 法務省では、こうした要請を踏まえ、法人設立後の継続的な実質的支配者の把握についての取組の一つとして、登記所が、株式会社からの申出により、その実質的支配者に関する情報を記載した書面を保管し、その写しを交付する制度を創設することとし、2022年１月３１日から運用を開始する。

36. 「金融庁マネロン・ガイドライン」の改正、「よくあるご質問（FAQ）」公表 (1)

■ 当局によるモニタリングの中で、**特にリスクの特定・評価・低減に係る重要な４項目**について、**「対応が求められる事項」に対する課題が認められた**ことを踏まえ、2021年2月、金融庁マネロン・ガイドラインを改正。

■ さらに、当該「対応が求められる事項」について、**より具体的に要請内容を明確化する**観点から、2021年3月、FAQを策定。

	リスクの特定・評価	顧客管理	取引モニタリング／フィルタリング	疑わしい取引の届出
対応が不十分な事項	○ 包括的かつ具体的検証の未実施など、**リスクの特定が不十分** ○ 自らの直面する**リスクの評価が不十分** ○ **経営陣の関与が不十分**	○ リスクの特定・評価の結果を踏まえた、**顧客リスク評価の未実施**（顧客属性や取引内容等に基づくスコアリングや格付の形式的な適用） ○ 継続的顧客管理措置の未検討・未実施 ○ **顧客リスク評価に応じた**リスク低減措置の未実施	○ 取引モニタリングにおける抽出基準（シナリオ・敷居値等）に**自らのリスク評価が未反映**。 ○ 抽出基準（シナリオ・敷居値等）の**有効性分析・改善が不十分** ○ 取引フィルタリングにおける適切な体制構築が不十分	○ 疑わしい取引該当性の判断の適切性が不十分 ○ 届出内容を踏まえ、自らの直面する**リスクの評価や顧客リスク評価、リスク低減措置への反映の未実施**
今回の改正への反映	○ リスクの特定及び評価を**区別しつつ、連動したプロセスであること**を明確化し、適切なリスクの特定及び評価を実施 ○ 疑わしい取引の届出の分析等を通じた、自らの直面するリスクの評価を実施 ○ 経営陣が**主導性**を発揮し、全ての部門が連携・協働	○ 全ての顧客について顧客リスク評価（**リスクの変化に応じた**実効的な顧客リスク評価）を実施 ○ **リスクに応じた簡素な顧客管理（SDD）**の内容を明確化 ○ **顧客リスク評価に応じた**リスク低減措置を実施（特に取引モニタリングへの適切な反映）	○ 自らのリスク評価を反映した適切な取引モニタリングにおける抽出基準の設定、及び有効性分析・改善 ○ あいまい検索機能の設定、**経済制裁対象者が指定された際の遅滞なき照合**など、リスクに応じた適切な取引フィルタリング体制を構築	○ 疑わしい取引の参考事例や自らの過去の届出事例を考慮要素に含めた、適切な疑わしい取引の届出判断の実施 ○ 届出内容を踏まえ、**顧客リスク評価を見直し**、当該リスク評価に見合った**リスク低減措置の実施**

37.「金融庁マネロン・ガイドライン」の改正、「よくあるご質問（FAQ）」公表 (2)

提携先等とサービスを提供する際の留意点

○ 金融機関等が、業務提携等を行って新商品・サービスを提供する場合、**提携先等のマネロン・テロ資金供与対策の状況について十分に確認を行わない**まま当該商品・サービスを提供している個別事例を踏まえた注意喚起

高リスク取引に対する追加的措置

○ 顧客が行おうとする取引が、**当該顧客の事業内容等を踏まえると不合理であるにもかかわらず、整合性を確認することなく、不自然な海外送金を許容している**個別事例等を踏まえ、対応が期待される事項から、対応が求められる事項に移行

海外送金

○ **コルレス先や委託元金融機関に対するリスク評価、それに応じた管理の強化の記載を充実化**

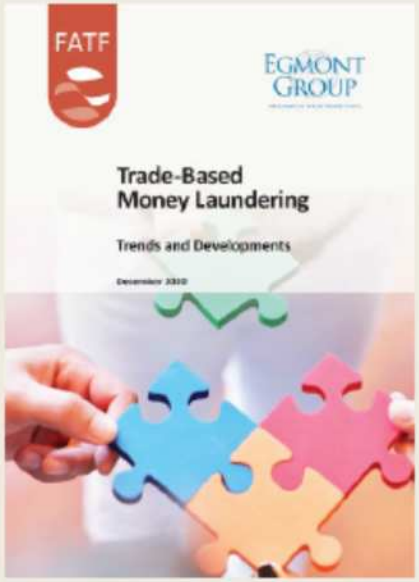
輸出入取引等に係る資金の融通及び信用の供与等

○ 輸出入取引等（いわゆる貿易金融）は、悪用の危険性、リスクに直面しており、国際社会の目線も高まっていることを踏まえ、**リスクベース・アプローチの枠組みの中で適切にリスクを特定・評価するべきことを明確化。**

38. 貿易に関するマネーロンダリング

- ◆ 貿易に関するマネロン（Trade-Based Money Laundering, TBML)は、従来より、マネロンに使用されるリスクが高く、FATFも2006年のTBMLに関するガイダンス文書、2008年にベスト・プラクティス事例集、2012年に犯罪類型（APG作成）、2020年にEgmont Groupと共同で疑わしい取引届け出参考事例を公表している。
- ◆ WEFによれば、2008年から2017年に貿易取引でマネロンや脱税に利用された金額は9兆ドルに上るとされている。(How trade-based money laundering works and its impact on world finances, World Economic Forum, 2021年6月)
- ◆ 民間ベンダーによれば、2018年以降、グローバルベースでの金融機関宛の行政処分による過料のうち、18.3億ドルがTBML関連。(Nice Actimize aml_tbml_Brochuer)

Trade-Based Money Laundering – Trends and Developments



This joint FATF-Egmont report aims to help public and private sector with the challenges of detecting trade-based money laundering. Using numerous case studies from around the FATF's Global Network, it explains the ways in which criminals exploit trade transactions to move money, rather than goods. It highlights recommendations to address the trade-based money laundering risks. These include using national risk assessments and other risk-focused material to raise awareness with the public and private sector entities involved in international trade, improving information-sharing of financial and trade data, and cooperation between authorities and private sector, including through public-private partnerships. FATF, Egmont Group (2020)

www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html

39. TBML：FATFによる疑わしい取引届出参考事例

FATFとEgmont Groupによる、疑わしい取引届出参考事例の概要(2021年3月)
“Trade-Based Money Laundering Risk Indicators, March 2021”

貿易会社や取引先の構造的な留意点や事例	貿易取引の留意点や事例	貿易書類や価格に関する留意点や事例	口座の資金移動や支払いに関する留意点や事例
• 貿易会社の株主構成が複雑、ハイリスク国に子会社を所有等 • 本社や事務所の所在地がハイリスク国 • 事務所住所が雑居ビル、私書箱等（信託会社の住所も要確認） • Web上で存在が確認できない、もしくは、実態と乖離している。 • 従業員の存在が疑われる等、営業実態が乏しい。 • 実質的支配者を隠ぺいするため、株主や役員に名義貸しが疑われる。 • 株主や経営陣に不芳情報あり。 • 活動実態に比して、従業員数が少ない。 • 休業期間が不自然に長い。 • 売上税等を払っていない。	• 貿易取引の内容が申告の業種と異なる。 • 不自然に、第三者や第三国を経由する取引。 • 通常の商流とは異なるモノの流れ。 • 貿易取引内容に比して、複雑な貿易金融スキームを用いている。 • 手数料水準が低い取引。 • 事業規模に比して多額の売買を行っている。 • 新設、もしくは、業務再開したばかりにも関わらず、多額の取引を行っている。	• 貿易書類に不整合、不自然な点がある取引。例えば、輸出者と受取人が異なる、契約と請求書の価格が異なる、取引量・個数・価格・金額に整合性無し、等。 • 取引商品の価格、手数料が市況や以前の取引に比して乖離している取引。 • 通関書類などが紛失、偽造、改ざんの恐れがある取引。 • 商流や契約条件等が、ひな型を使ったように、単純すぎる取引。 • 貿易取引の金額と、銀行間の外為決済金額が乖離している取引。 • 暫定的な輸入措置と称して、偽造書類で間髪入れずに輸出する事例。 • 複数の国を経由して戻ってくる循環取引。	• 支払い条件に関する変更を直前になって申し入れてくる取引。 • 事業規模に比して、不自然に高額や多数の取引。 • 仮名・借名口座や実態は口座名義人でない第三者が捜査している口座。 • 日中資金移動が活発で多額であるにも関わらず、日次の最終残がかが少額に収まる口座。 • フリーゾーンやオフショア地域との資金移動の活発な口座。 • 現金取引の多い口座。 • 貿易決済の入金後、少額に分散して流出する口座。 • 輸入に関する支払元が荷受人でない支払い。 • 閾値を下回る金額での入出金。 • 一時的に活発な取引。 • ラウンド・ナンバーでの支払い。 • 資金循環取引。

（FATF, Trade-Based Money Laundering Risk Indicators, March 2021より筆者作成）

40. 貿易に関するマネーロンダリング　－　金融庁マネロン・ガイドライン

Ⅱ－２　リスクの特定・評価・低減
（４）海外送金等を行う場合の留意点
（ⅱ）　輸出入取引等に係る資金の融通及び信用の供与等

輸出入取引は、国内の取引に比べ、実地確認が困難なケースもあることを悪用し、輸出入取引を仮装したり、実際の取引価格に金額を上乗せして支払うなどして犯罪による収益を移転したりすることが容易である。また、輸出入関係書類の虚偽記載等によって、軍事転用物資や違法薬物の取引等にも利用される危険性を有している。

金融機関等においては、輸出入取引等に係る資金の融通及び信用の供与等がこうしたリスクにも直面していることを踏まえながら、特有のリスクの特定・評価・低減を的確に行う必要がある。

【対応が求められる事項】
① 輸出入取引等に係る資金の融通及び信用の供与等に係るリスクの特定・評価に当たっては、輸出入取引に係る国・地域のリスクのみならず、取引等の対象となる商品、契約内容、輸送経路、利用する船舶等、取引関係者等（実質的支配者を含む）のリスクも勘案すること

【対応が期待される事項】
a. 取引対象となる商品の類型ごとにリスクの把握の鍵となる主要な指標等を整理することや、取扱いを制限する商品及び顧客の属性をリスト化することを通じて、リスクが高い取引を的確に検知すること
b. 商品の価格が市場価格に照らして差異がないか確認し、根拠なく差異が生じている場合には、追加的な情報を入手するなど、更なる実態把握等を実施すること
c. 書類受付時に通常とは異なる取引パターンであることが確認された場合、書類受付時と取引実行時に一定の時差がある場合あるいは書類受付時から取引実行時までの間に貿易書類等が修正された場合には、書類受付時のみならず、修正時及び取引実行時に、制裁リスト等と改めて照合すること
d. 輸出入取引等に係る資金の融通及び信用の供与等の管理のために、ITシステム・データベースの導入の必要性について、当該金融機関が、この分野において有しているリスクに応じて検討すること

41. TBML対策のDX、システム化とその課題

◆ グローバルでのマネロン・テロ資金供与・拡散金融リスクの増大にともなって拡大する貿易に関するマネロン等リスクへの対策として、金融機関における管理強化とシステム化検討が進んでいる。

◆ TBML対策のシステム化においては、従来型のSanction ScreeningやTransaction Monitoring い加えて、貿易金融業務の特性に起因する課題がある。

- 伝統的に、複数の関係者間（輸出入業者、運輸業者等）で紙ベースで書類を授受
- 関係者間の情報共有は相対であり、取引関係間でシームレス・リアルタイムの情報共有ができない
- 貿易書類（紙）の突合作業は、原則、人の目で行われることから、事務的負担が重い

AML/CFT/PFリスクの増大 ⇒ TBML リスクの増大

日々変化するTBMLリスク（Moving Target）

強まるGlobal・国内当局の要請

銀　行

貿易金融取引におけるマニュアルチェック負荷の増大及びサービスレベルの低下

グローバル水準に満たない対応による高リスク取引の漏出等、コンプラリスク増大

システム化検討

TBML対策のシステム化検討とその課題

1.貿易書類のDigitalizationと情報抽出

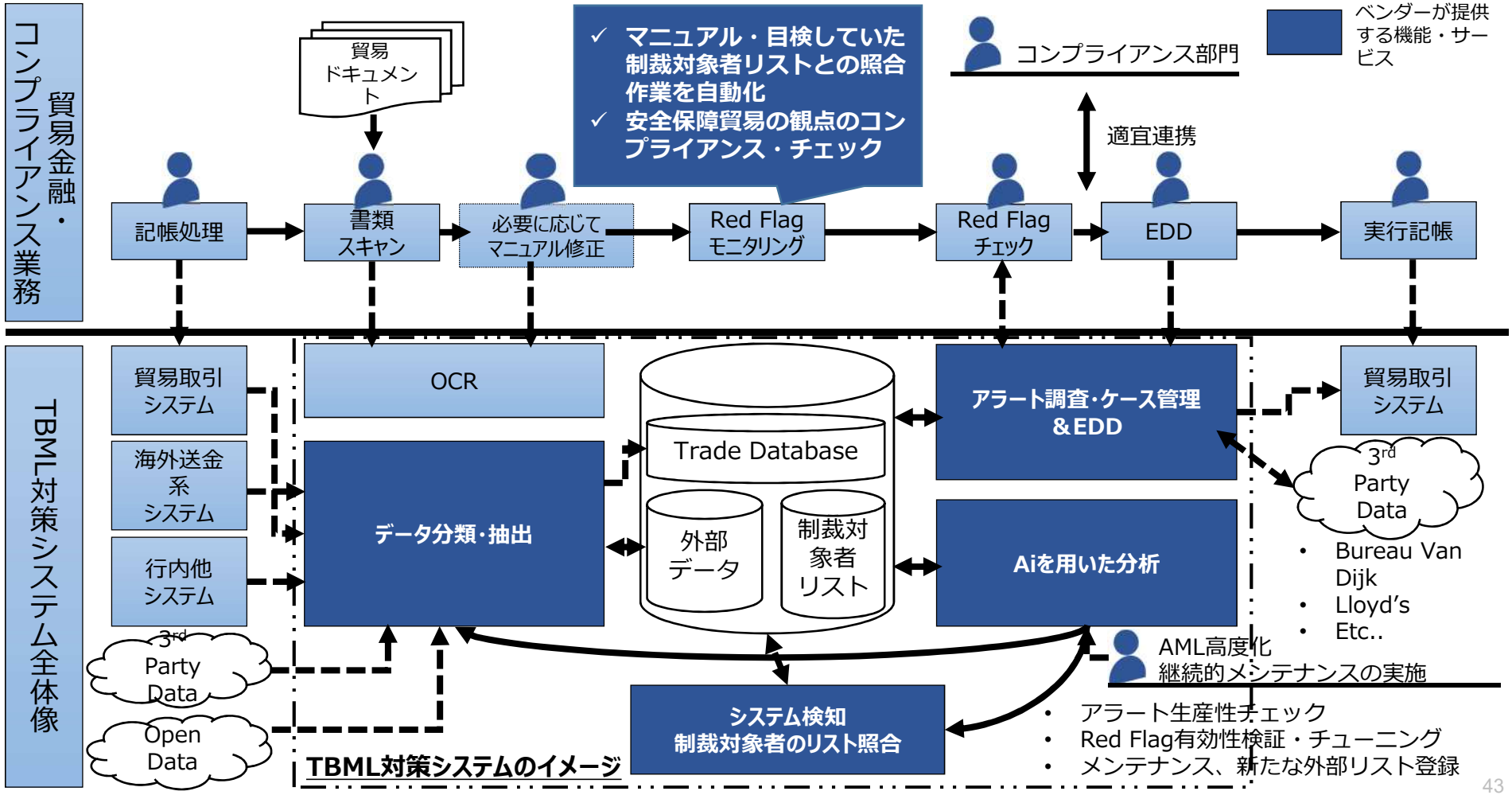
2．システムによる制裁対象者等チェック

3.多様な外部データの蓄積と活用

4.継続的なTBML対策高度化の徹底

42. TBML対策システムの全体像イメージ（例）

- 貿易及び貿易に関する資金決済は、マネーローンダリングの古典的、かつ、現在も多用される手法。
- 他方、貿易金融に関するマネロン等対策は、紙ベースの書類のマニュアル検証のプロセスが多く、効率化の余地あり。
- 検証対象文書のデジタル化（OCR）、データの分類・抽出、システム検知（スクリーニング）、調査、Aiを用いた分析、謝絶、疑わしい取引届出、継続的顧客管理等の一連の管理フローの自動化が進めば、効率性・有効性の向上が見込める。



43. 船舶ファイナンスについての適切なAML/CFT対応の必要性

現状認識

- 2017年9月に採択された国連安保理決議第2375号において、国連加盟国は北朝鮮船舶に対する又は北朝鮮船舶からの洋上での船舶間の物資の積替え（所謂「瀬取り」）を容易にし、又は関与することが禁止（国連安保理は、2017年６月、8月、9月、12月と4回北朝鮮制裁決議を採択）
- 北朝鮮関連船舶による「瀬取り」の疑いのある事案の発生は後を絶たず、2018年8月21日、米国財務省も、国連安保理決議に違反して「瀬取り」により精油製品を供給したとして、船舶6隻を米国の独自対象に追加（*1）また、2018年8月10日、韓国関税庁も、北朝鮮石炭を韓国に不正に搬入した事案に関する調査結果を発表、関与したとされる4隻に対し入港禁止措置(*2)
- 2019年3月12日、国連安全保障理事会北朝鮮制裁委員会の専門家パネルは最終報告書(*3)を公表したが、本報告書には引き続き、北朝鮮への「瀬取り」などに関与した疑いのある船舶への言及
- 2019年3月21日、米国財務省、国務省等は、北朝鮮の違法海運慣行対処に関するガイダンス（更新）(*4)を公表し、米国、オーストラリア、カナダ、フランス、イタリア、日本、英国と共に、国際海事機構（IMO)全加盟国に対し、北朝鮮の不正慣行に関する注意喚起

問題点

- 船舶自体が制裁対象者に指定される状況に鑑み、船舶金融、貿易金融、貿易に関する決済等を行う銀行、海上保険に取り組む保険会社等において、国連や関係各国の制裁措置に抵触するリスクに留意する必要あり（米国財務省・国務省等のガイダンスによれば、北朝鮮が行う不正行為は、AIS無効化、IMO番号変更、貨物・船舶文書改ざん、AIS操作 等）

対応策（案）

銀行等 （現在取り組んでいる融資対象船舶の確認等の リスク低減策の強化）	保険会社(海上保険を扱う損保) （現在取り組んでいる保険付与対象船舶の確認等の リスク低減策の強化）
● 船主、傭船者等の関係者や対象船舶の関係当局による制裁リストなどとの照合の徹底	
● AISの活用などによる対象船舶の寄港地履歴や融資/保険付保後の運行状況のモニタリングにより、対象船舶のリスクを把握し、リスクに応じた措置	
● 違法な瀬取りへの関与など国内外の制裁措置に違反する行為が確認された場合などを期限の利益喪失条項とする融資契約書/保険契約書の締結	

(*1) 米国務省発表 https://home.treasury.gov/news/press-releases/sm463
(*2) JETROホームページによる解説 https://www.jetro.go.jp/biznews/2018/08/34424635165cd7ef.html
(*3) UN Documents for DPRK (North Korea) https://www.securitycouncilreport.org/un-documents/dprk-north-korea/
(*4) US Treasury https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx

44. 米財務省による船舶に関するガイダンスの公表（2020年5月）

- 2020年5月14日、米財務省OFACが「不正な海運及び制裁回避活動に対処するためのガイダンス(Guidance to Address Illicit Shipping and Sanctions Evasion Practices)」を公表
- 主として、海運、エネルギー、金属、その他の関連産業分野で事業活動を行っている関係者に対して、最近の不正行為のパターンを説明するとともに、このような不正行為を防止するためにとるべき具体策を示しながら、関係業界に対して制裁法令遵守のための各種プログラムを見直していくべきとしている
- 国連安保理決議＝わが国外為法に基づく本邦制裁指定であるのに対し、米OFACは、国連安保理制裁決議を超えて、米国独自の判断でSDN指定を行い、かつ、その遵守義務を米国人、米国法人にのみ求めるのみならず、米国人が関与した取引については、非米国人・企業（金融以外も含む）に対して域外適用の対象としている。わが国金融機関等はGate Keeperとして、ドル取引を中心に一層充分注意を払う必要がある。

ガイダンスのポイント

- 世界の貿易の90%は、海運により行われているとの実態を踏まえ、米国が問題視している、制裁対象者による制裁回避の動きや、麻薬等の禁制品の取引、犯罪活動、テロ活動、大量破壊兵器の拡散などに効果的に対処するためには、海運、エネルギー、金属、その他の関連産業分野で事業活動を行っている関係者が現場で効果的な対策を講じることが極めて重要である旨指摘
- 付属文書で、海上保険会社、船籍管理会社等、港湾管理関係機関、海運業協会、商品の国際取引業者(商社)、サプライヤー、仲介業者、金融機関等に対して、実務上対処すべき具体的な側面をリストし、対策を促している

出所：
プレスリリース https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200514.aspx
ガイダンス https://www.treasury.gov/resource-center/sanctions/Programs/Documents/05142020_global_advisory_v1.pdf

45. 国連安保理　北朝鮮制裁委員会　専門家パネル中間報告書（2021年10月4日公表）

国連安保理北朝鮮制裁委員会専門家パネル2021年中間報告書の概要

◆ 10月4日（NY現地時間）、国連安保理北朝鮮制裁委員会専門家パネルによる2021年中間報告書が公表された。
◆ 制裁違反・回避が疑われる事例及び北朝鮮による制裁回避の詳細な手法を分析・報告。北朝鮮が、経済的に厳しい状況にあっても核・弾道ミサイル計画を継続していること、「国」境封鎖により取引量は相当程度減少しているものの、石油精製品、石炭その他の禁制品の取引は継続していること等が明らかにされている。

報告書のポイント

（1）核・弾道ミサイル関連活動

● 北朝鮮は核開発計画を継続。寧辺の軽水炉は外部工事が完成したと見られる。新たな再処理活動を開始した可能性。
● 弾道ミサイル計画の進展速度は低下しているが、3月の新型固体燃料推進式ミサイルの発射、軍事パレードでの新型の超大型大陸間弾道ミサイルの登場等、活動的。複数の加盟国が、北朝鮮は弾道ミサイルに小型核弾頭を搭載する能力があると評価。北朝鮮の貿易会社及び国防科学院は、シリア、イラン、アフリカ、東南アジア諸国等との軍需品の輸出入を行い、外貨調達と武器開発事業をめぐる協力を継続。

（2）海洋関連措置

● 2021年前半の北朝鮮への石油精製品の供給量は、例年と比較して相当程度減少しているが、年間の供給上限量は超過すると見られる。「瀬取り」は継続しているが、活動規模は低下。AIS（船舶自動識別装置）の不正操作・停泊の手口を継続。
● 北朝鮮籍船舶及び制裁違反が疑われる船舶が、寧徳・東引諸島周辺海域を航行又は帰港しているなど、中国の港湾及び領海の海域で目撃。
● 2020年に最も多く「瀬取り」が行われた海域は、2019年に続き、台湾北方沖及び揚子江河口沖。他方、2020年には、新たに露朝の「国」境付近、及び台湾南西沖でも「瀬取り」が確認。
● 2021年2～5月に、北朝鮮籍船舶等により、少なくとも41回の輸送が行われ、36万4千トンの北朝鮮産石炭が中国に不正輸出されたが、これは前年より小規模。
● 北朝鮮による第三国への漁業権の販売が継続。操業許可証、保険関連書類等の書類が第三国の漁船から発見されている。ある加盟国によれば、4～5か月の漁業権の単価は20万元（約3万1千ドル）～30万元（約4万6千ドル）。

（3）貿易、禁制品の取引、海外労働者

● 2020年の北朝鮮の貿易額は、統計上、輸出額は前年比で約33%、輸入額は同20%に減少。北朝鮮から不正輸出された主な品目は、石炭、鉱物資源、鉄、砂、繊維製品。一部エリート層向けの輸入を除き、奢侈品の輸入は事実上停止。
● 北朝鮮の海外労働者は複数の国に滞在を続け、IT、建設、電子工学、農業分野で収入を得ている。

（4）金融、サイバー

● 北朝鮮は、国際的な金融機関へのアクセスを維持。不正な金融活動は東アジア及び東南アジア諸国に集中。ある加盟国は、ロシアで6人、中国で22人、インドネシア及びシンガポールで1人ずつ、北朝鮮の銀行の海外代表が活動している旨情報提供。
● 北朝鮮は中国を拠点とする企業との合弁企業設立を継続。
● 偵察総局関連のサイバー攻撃部隊が世界各地で防衛産業への攻撃を継続。暗号通貨業界へのスピアフィッシング攻撃が継続。

46. FATF勧告の改訂（2012年）：拡散金融を追加

2021年2月、FATF第四次相互審査に向けて、第三次相互審査結果、国際情勢等よる脅威やリスクの変化を踏まえ、FATF勧告を改定：

１．現行の「40の勧告」及び「９の特別勧告」を統合

マネロン対策（40の勧告）とテロ資金供与対策（９の特別勧告）を40の勧告に統合

２．リスク・ベース・アプローチの強化

リスク・ベース・アプローチのコンセプトを明確化

３．法人・信託、電信送金システムに関する透明性の向上

法人や信託の実質所有者/支配者に関する情報、電信送金を行う際に必要な情報等について基準を厳格化し、これらの透明性を向上させた

４．マネロン・テロ資金供与対策のための当局の機能及び国際協力体制の強化

- マネロン・テロ資金供与対策に責任を持つ法執行機関及びFIU（金融情報機関）の役割と機能を明確にし、より幅広い捜査手法や権限を求めた
- 捜査当局等に求める国際協力の範囲を拡充

５．新たな脅威への対応

- 腐敗行為防止の観点から、PEPs（重要な公的地位を有する者：Politically Exposed Persons）の定義を外国人PEPsだけでなく国内PEPs等にまで拡大
- 税犯罪により生じた収益を資金洗浄する行為をマネロン罪の対象化
- 国連安保理決議の要請に沿って、大量破壊兵器の拡散に関与する者に対し、金融制裁を実施することを新たに勧告とした（勧告７）

47. 拡散金融（FATF勧告７）

勧告7. 大量破壊兵器の拡散に関する対象を特定した金融制裁

各国は、大量破壊兵器の拡散とその資金供与の防止、抑制、崩壊に関する国連安全保障理事会決議を遵守するために、標的型金融サンクションを実施する必要がある。これらの決議は、国際連合憲章 7 章に基づき、国際連合安全保障理事会によって指定された、又はその権限下にある個人又は団体の資金その他の資産を遅滞なく凍結し、直接又は間接を問わず、いかなる資金その他の資産もその者の利益のために利用できないようにすることを各国に義務付けている。

大量破壊兵器等：核兵器、軍用の化学製剤、軍用の細菌製剤、軍用の化学製剤又は細菌製剤の散布のための装置、３００ｋｍ以上運搬することができるロケット、３００ｋｍ以上運搬することができる無人航空機、部分品も含む（輸出貿易管理令）

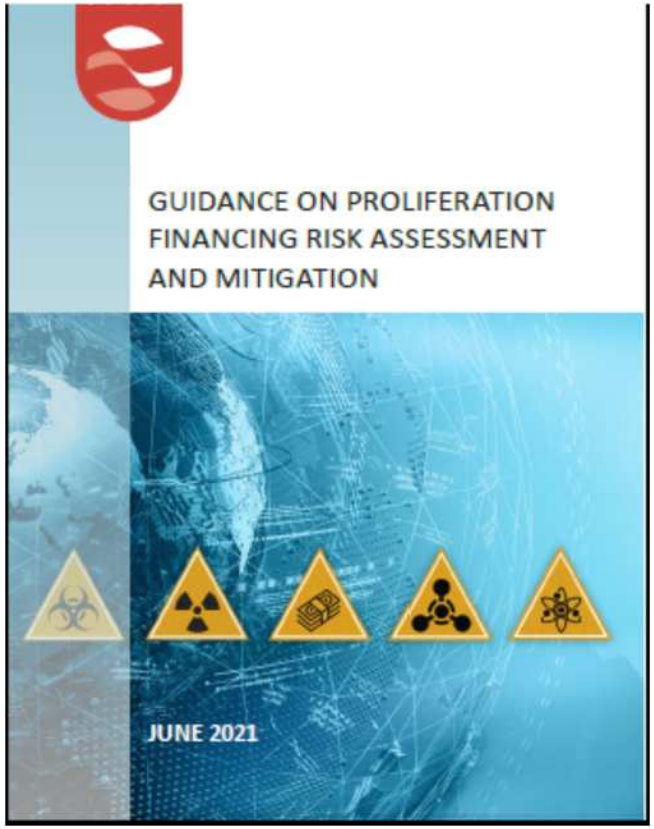
背　景　＝　イランや北朝鮮による核及び弾道ミサイル開発

【参考）　北朝鮮による核弾頭及び弾道ミサイル開発（2009年から2011年）（出所：外務省HP)

- 2009年4月，北朝鮮は弾道ミサイルを発射し，これを非難した国連安保理議長声明に反発し，軽水炉の自力建設への着手，使用済み核燃料棒の再処理，核実験及び長距離弾道ミサイル発射実験を行う旨表明。5月には核実験を実施し，それに対して採択された安保理決議第1874号に反発し，プルトニウムの兵器化，ウラン濃縮への着手を発表した。また，7月には複数発の弾道ミサイルを発射し，11月には，8,000本の使用済み核燃料棒の再処理を8月末までに成功裏に終えた旨発表した。
- 2010年に入り，北朝鮮は，六者会合への復帰のためには国連安保理決議に基づく対北朝鮮制裁の解除が必要とし，非核化措置の前に朝鮮戦争終結のための平和協定締結の協議を求めるとの立場を表明。その後，北朝鮮は韓国哨戒艦沈没事件（3月）や延坪島砲撃事件（11月）といった挑発行為を繰り返すとともに，同年11月には，訪朝した米国人科学者にウラン濃縮施設や「軽水炉」の建設現場を案内するなどしてウラン濃縮計画等を公表した。
- 2010年12月にワシントンで開催された日米韓外相会合において，日米韓は，六者会合の再開のためには，南北対話の進展と非核化を始めとする自らの約束を真剣に実施する意思を示す北朝鮮側の具体的行動が必要との立場で一致。その後，2011年7月から10月にかけて，非核化に関する南北対話及び米朝対話がそれぞれ2回にわたり実施された。

48. FATF 拡散金融のリスク評価及びリスク低減策に関するガイダンス

- ◆ 2020年10月、FATFは、勧告１（国としてのリスク評価）及びその解釈ノートを改訂し、その中で、大量破壊兵器の拡散に関与する者へのこのリスク評価を行うことを加盟国に要請
- ◆ 2021年6月、FATFは、拡散金融のリスク評価及びリスク低減策に関するガイダンスを公表



【リスク評価のポイント】

- マネロン・テロ資金供与リスクと同様、リスクを構成する要因は「脅威（threat)」、「脆弱性(vulnerability)」、「結果(consequence）」。
- 「脅威」は、制裁対象として指定された者（法人含む）に関係するセクター、商品、サービスが基になる。
- 「脆弱性」は国や民間セクターが抱える拡散金融対策の構造的な欠陥、特定のセクターにおけるリスク認識やコンプライアンス文化の低さ等に起因。
- また、民間セクターにとって、自らが扱う顧客や取引の「脆弱性」を特定することが不可欠。「結果」として、金融制裁の潜脱等が行われた場合のインパクトや危険度を評価。

【リスク低減策のポイント】

- 国によるリスク低減措置

  ①リスク評価の実施、②遅滞なき制裁を実施するための制度整備、③制裁対象者の指定に係る情報の通知、④国内協力・調整、⑤義務の履行モニタリングと罰則適用、規制強化、⑥トレーニングやガイダンス提供、等。

- 金融機関等によるリスク低減措置

  ①新規に顧客と取引を開始する際の手続きの改善、②デュー・デリジェンスの強化、③顧客データの効果的管理、④実効的な制裁スクリーニング、⑤既存のプログラムを活用した潜脱等の発見

49. 金融庁マネロン・ガイドライン

（金融庁マネロン・ガイドライン2頁）

大量破壊兵器の拡散に対する資金供与の防止のための対応も含め、外為法や国際連合安全保障理事会決議第千二百六十七号等を踏まえ我が国が実施する国際テロリストの財産の凍結等に関する特別措置法（国際テロリスト財産凍結法）をはじめとする国内外の法規制等も踏まえた態勢の構築が必要である。

FAQ４６頁

国内外の制裁に係る法規制等の遵守については、例えば、国際連合安全保障理事会（以下「国連安保理」といいます。）決議等で指定される経済制裁対象者については、外国為替及び外国貿易法第16 条及び第21 条等に基づき、同決議等を踏まえた外務省告示が発出された場合に、直ちに該当する経済制裁対象者との取引がないことを確認し、取引がある場合には資産凍結等の措置を講ずるものとされています。さらに、国際的な基準等（注）を踏まえると、外務省告示の発出前においても、国連安保理決議で経済制裁対象者が追加されたり、同対象者の情報が変更されたりした場合には、遅滞なく自らの制裁リストを更新して顧客等の氏名等と照合するとともに、制裁リストに該当する顧客等が認められる場合には、より厳格な顧客管理を行い、同名異人か本人かを見極めるなどの適切かつ慎重な対応が必要と考えています。

したがって、このような対応を確実に実施するために必要なデータベースやシステム等の整備、人材の確保、資金の手当てを、直面しているリスクに応じて実施していただくことが重要であると考えています。

なお、昨今、データ復旧等に身代金を要求するランサムウェアの感染被害が報告されています。海外ではランサムウェアの身代金がテロ資金等に悪用される可能性もあると指摘されており、米国においては、金融機関等に向けて、ランサムウェアの身代金の支払いへの関与には制裁リスクがあるという点について注意喚起の勧告も出されました。サイバー空間には国境がないことから、このような身代金の支払いに金融機関等が利用されてはならず、顧客の送金について、この種のテロ資金供与リスクがあることも留意する必要があります。

（注）FATF においては、テロ資金供与や大量破壊兵器の拡散に関する金融制裁として、国連安保理により制裁対象として指定された個人・団体が保有する資金・資産を遅滞なく凍結することを求めております。

FAQ７２頁

国際連合安全保障理事会決議等で経済制裁対象者等が指定された際には、金融機関等は、数時間、遅くとも24 時間以内に自らの制裁リストに取り込み、取引フィルタリングを行い、各金融機関等において既存顧客との差分照合が直ちに実施される態勢を求めています。

50. まとめ Takeaway

1. FATF（金融活動作業部会）第４次対日相互審査では、一定の評価は得たものの、金融機関等の監督の強化や金融機関等のリスク理解やリスク低減策への課題が示され、特に、金融機関等における、リスク理解、リスクに応じた継続的顧客管理、取引モニタリングの高度化について改善の余地があるとされた。

2. リスク理解は、RBAの大前提であり、適切なリスク理解が行われなければ、リスクに応じた対応も不十分となる恐れがある。金融機関等は、国によるリスク評価も踏まえつつ、自らの金融犯罪の被害状況や疑わしい取引届出の内容分析を踏まえ、自らが直面するマネロン等リスクについて、適切に理解する必要がある。また、リスクの特定・評価の手順についても、経営陣の承認を得た上で、文書化し、周知する必要がある。

3. 金融庁では、検査要員の確保等により検査・監督体制を強化し、預金取扱金融機関をはじめとする、リスクが高いとされる業態を優先的に、リスクベースでの検査・監督を実施し、金融庁マネロン・ガイドラインの「対応が求められる事項」に関する態勢整備状況を中心に検証を進める。金融機関等においては、2024年3月末までに体制整備の完了が求められており、FAQも活用しながら、今一度、体制整備状況について、自ら検証する必要がある。

4. 金融庁としては、全銀協とも連携し、マネロン・テロ資金供与・拡散金融対策の高度化・効率化のため、マネロン等対策の共同システムの実用化の検討・実施に取り組む。

5. また、わが国のマネロン等対策の高度化のためには、関係当局や金融機関をはじめとする特定事業者の取組と連携に加えて、金融機関等の一般利用者の理解と協力が不可欠であり、今後とも、あらゆるチャンネルを使って情報発信を行ってゆく。

（参考）貿易金融、貿易に関する送金決済におけるマネロン等対策に関する報告書など

- FATF Trade-Based Money Laundering, June 2006
- FATF Best Practices on Trade-Based Money Laundering, June 2008
- FATF-APG Typology Report on TBML, 2012
- FATF Trade-Based Money Laundering, Key Risk Indicators, March 2021
- Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking by Monetary Authority of Singapore, October 2015
- The Hong Kong Association of Banks Guidance Paper on Combating Trade-based Money Laundering, February 2016
- The Wolfsberg Group, ICC and BAFT Trade Finance Principles, 2017 (the most recent version)

【参考資料】

米国のマネロン等対策について

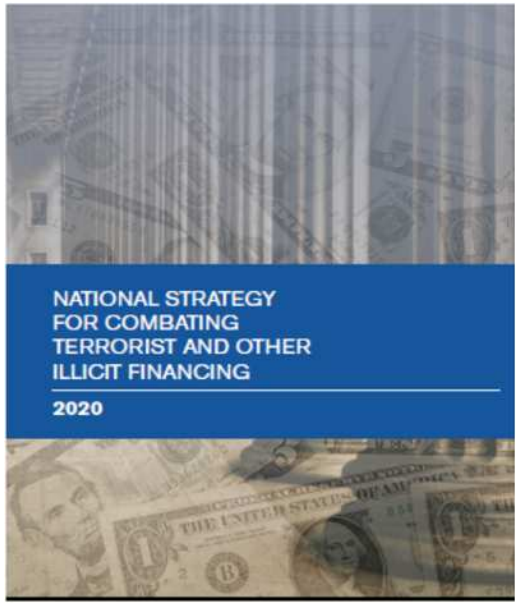
(出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

米国のマネロン等対策戦略2020 (1)

■ 2020年2 月6日、米財務省は、「マネロン等対策国家戦略 2020」（the 2020 National Strategy for Combating Terrorist and Other Illicit Financing (2020 Strategy)）を公表。2018年の戦略文書を引き継いで作成・公表されたもの。

■ 主な脅威
- ① **詐欺を含む前提犯罪と資金洗浄**
- ② **麻薬密売**
- ③ **テロ資金許与**
- ④ **拡散金融**
- ⑤ **組織犯罪**
- ⑥ **人身売買**
- ⑦ **汚職**

■ 主な脆弱性
- ① **実質的支配者の不透明性**
- ② **不動産**
- ③ **コルレス関係**
- ④ **マネロン対策の不整合性（海外）**
- ⑤ **法令遵守の脆弱性（国内）**
- ⑥ **現金**
- ⑦ **共謀(Complicit)**
- ⑧ **暗号資産**



(出所：米財務省 The 2020 National Strategy for Combating Terrorist and Other Illicit)

米国のマネロン等対策戦略2020 (2)

Objectives of an Effective AML/CFT Regime

Identify and Prioritize Illicit Finance Risks

Identify and assess illicit finance threats, vulnerabilities, and risks; develop strategies and plans to target risks; communicate to the public and private sectors and foreign partners

Prevent Illicit Finance and Protect the Financial System

Ensure well-supervised institutions limit illicit proceeds and assets from accessing the financial system and detect and report illicit finance activity that seeks to evade AML/CFT measures

Disrupt and Dismantle Illicit Finance Networks

Generate actionable financial information and intelligence so well-resourced authorities can investigate, arrest, and prosecute or otherwise disrupt illicit financiers and money launderers in priority risk areas and deprive them of their assets and proceeds

Making the U.S. AML/CFT Framework More Effective: Priorities and Supporting Actions

Increase Transparency and Close Legal Framework Gaps

1. Require Collection of Beneficial Ownership Information by the Government at Time of Company Formation and After Ownership Changes
2. Minimize the Risks of the Laundering of Illicit Proceeds Through Real Estate Purchases
3. Extend AML Program Obligations to Certain Financial Institutions and Intermediaries Currently Outside the Scope of the BSA
4. Clarify or Update our Regulatory Framework to Expand Coverage of Digital Assets

Continue to Improve the Efficiency and Effectiveness of Regulatory Framework for Financial Institutions

1. Improve the Efficiency of Existing Reporting Obligations
2. Emphasize the Risk-focused Approach to Supervision
3. Foster Responsible Innovation

Enhance the Current AML/CFT Operational Framework

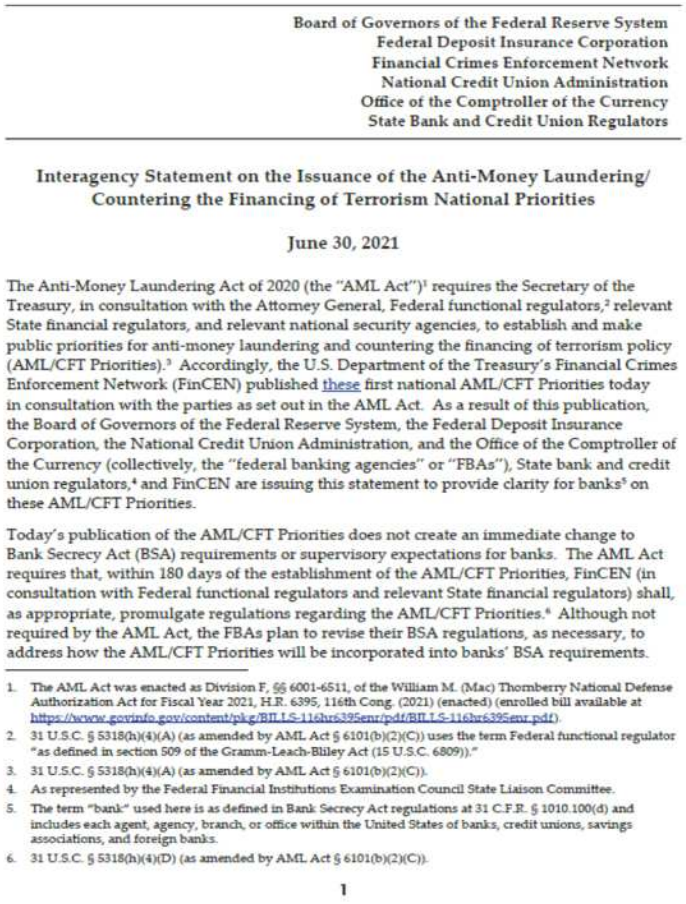
1. Improve Communication of Priority Illicit Finance Threats, Vulnerabilities and Risks
2. Expand the use of Data Analytics and Artificial Intelligence
3. Creatively and Effectively Deploy Targeted Measures to Disrupt Illicit Finance Activity
4. Enhance use of Public-Private Partnerships and Other Information Sharing
5. Support Global AML/CFT Implementation

(出所：米財務省 The 2020 National Strategy for Combating Terrorist and Other Illicit)

米国のマネロン等対策の優先事項

- 2021年6 月30日、米財務省金融犯罪取締ネットワーク（FinCEN)は、関係当局との協議に基づき、マネーロンダリングおよびテロリスト資金供与対策(AML/CFT)方針における政府全体としての優先事項を公表。
- 当優先事項は、米国の金融システムおよび国家安全保障に対する新たな脅威に対応すべく、少なくとも4年ごとに更新。

- 優先事項にはAML/CFT に関する長年にわたる懸念事項が反映されており、以下のカテゴリにおいて、金融システムを通じてマネーロンダリングされる不法収益を生み出す犯罪について記載。
  - ① **汚職** corruption
  - ② **サイバー犯罪** cybercrime, including relevant cybersecurity and virtual currency considerations
  - ③ **国内外のテロリスト資金供与** foreign and domestic terrorist financing
  - ④ **詐欺** fraud
  - ⑤ **国際犯罪組織の活動** transnational criminal organization activity
  - ⑥ **麻薬密売組織の活動** drug trafficking organization activity
  - ⑦ **人身売買および密入国斡旋** human trafficking and human smuggling
  - ⑧ **拡散金融** proliferation financing



Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency
State Bank and Credit Union Regulators

Interagency Statement on the Issuance of the Anti-Money Laundering/ Countering the Financing of Terrorism National Priorities

June 30, 2021

The Anti-Money Laundering Act of 2020 (the "AML Act")[1] requires the Secretary of the Treasury, in consultation with the Attorney General, Federal functional regulators,[2] relevant State financial regulators, and relevant national security agencies, to establish and make public priorities for anti-money laundering and countering the financing of terrorism policy (AML/CFT Priorities).[3] Accordingly, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published these first national AML/CFT Priorities today in consultation with the parties as set out in the AML Act. As a result of this publication, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the "federal banking agencies" or "FBAs"), State bank and credit union regulators,[4] and FinCEN are issuing this statement to provide clarity for banks[5] on these AML/CFT Priorities.

Today's publication of the AML/CFT Priorities does not create an immediate change to Bank Secrecy Act (BSA) requirements or supervisory expectations for banks. The AML Act requires that, within 180 days of the establishment of the AML/CFT Priorities, FinCEN (in consultation with Federal functional regulators and relevant State financial regulators) shall, as appropriate, promulgate regulations regarding the AML/CFT Priorities.[6] Although not required by the AML Act, the FBAs plan to revise their BSA regulations, as necessary, to address how the AML/CFT Priorities will be incorporated into banks' BSA requirements.

1. The AML Act was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2021) (enacted) (enrolled bill available at https://www.govinfo.gov/content/pkg/BILLS-116hr6395enr/pdf/BILLS-116hr6395enr.pdf).
2. 31 U.S.C. § 5318(h)(4)(A) (as amended by AML Act § 6101(b)(2)(C)) uses the term Federal functional regulator "as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809))."
3. 31 U.S.C. § 5318(h)(4)(A) (as amended by AML Act § 6101(b)(2)(C)).
4. As represented by the Federal Financial Institutions Examination Council State Liaison Committee.
5. The term "bank" used here is as defined in Bank Secrecy Act regulations at 31 C.F.R. § 1010.100(d) and includes each agent, agency, branch, or office within the United States of banks, credit unions, savings associations, and foreign banks.
6. 31 U.S.C. § 5318(h)(4)(D) (as amended by AML Act § 6101(b)(2)(C)).

1

米国の経済制裁の概要

- 米国政府は、包括的なものから対象を限定したものまで、様々な経済制裁を実施しており、国連安全保障理事会決議といった多数国間の合意に基づくものから、米国独自の経済制裁もある。
- 制裁は、財務省外国資産管理室（**US Department of the Treasury's Office of Foreign Assets Control・OFAC**）が主に担当している。
- 制裁の対象は、米国の国家安全保障もしくは、対外政策上の理由から問題があると考えられる特定の地域・国（例えば、クリミア、キューバ、イラン、北朝鮮、シリアなど）、政府、人（例えば、テロリスト、麻薬密売人、大量破壊兵器の拡散者）のこともあれば、特定の活動や産業分野（例えば、ロシアでの金融機関に新しい貸付（debt）や持分（equity）を提供すること、ロシアにおける非在来型石油・ガス関連事業活動を支援すること、ベネズエラ政府およびその関連企業の社債や新しい金融手段を取り扱うこと等）も含む。

- OFACの制裁の対象は、「米国人」および、米国制裁によって禁止されている取引や行動を促進するようなかたちで、米国であるいは米国人による行動を引き起こす**非米国人におよぶ**。一定の状況下、OFACの管轄対象は、米国制裁の下ブロックされ凍結される資産に加えて、物やソフトウェア、もしくは技術の輸出にも適用される。
- OFACの制裁対象者は、OFACが管理する、**特別指定国民・凍結者リスト（Specially Designated Nationals and Blocked Persons List・SDNリスト）**に掲載されている。OFACがターゲット対象者との取引などを禁止していることに関して、相手方自身がSDNリストに掲載されていない場合でも、**SDNリスト掲載者によって50%以上所有されている場合には対象となる(50%ルール)**。OFACにはまた、SDNリストより緩やかな規制の対象者のリストとして、List of Foreign Sanctions Evaders(LFSE)や、Sectoral Sanctions Identifications List(SSIL)などがある。

米国の経済制裁のリスク（域外適用）

■ OFACの管轄は、「米国人」のみならず、米国制裁によって禁止されている取引や行動を促進するかたちで米国であるいは米国人による行動を引き起こす非米国人におよぶ。例えば、ターゲットとなっている地域やターゲット対象者を含む米国外で起こった取引を支援するかたちで、米国の金融機関を通じて米国ドル建ての資金を移転する決済を非米国銀行が行った場合に、刑事および民事のペナルティーの対象になる場合がある。米国外での米国ドルを含む取引は、制裁と関係があるとみなされる。非米国人は、ターゲット地域に米国制裁の管轄に服する物、技術もしくはサービスを再輸出する場合にも、OFACの対象となる。

■ 一次的制裁（primary sanction）の下での管轄の問題としては人や活動が米国制裁の対象ではない場合でも、特定の制裁プログラム（例えば、イラン、ロシア）は、非米国人が米国の管轄のおよばないところでの一定の活動に従事することを妨げることを意図して、報復的な二次的制裁（secondary sanctions）を課すことを認めている。このような制裁は、非金銭的（non-monetary）であるが金銭的なペナルティーよりも企業の活動にとっては、より支障になる場合がある。

金融機関名	事案
ブリティッシュ・アラブ商業銀行（英国） 2019 年9月	• 英国のBritish Arab Commercial Bankは、米財務省OFACとの間で米国制裁関連法令等（スーダン）の違反で**4百万**ﾄﾞﾙの罰金を支払うことで合意。 • **同行は米国内に拠点はなく**、非米国銀行のドル口座（当方口）を経由して、2010年から2014年の間、スーダン中銀を含むスーダン法人に対し、合計72回、190百万ﾄﾞﾙの米ドル・バルク送金を行ったもの。 • **米国金融機関は経由していないものの、決済通貨がドル**であることから米国法令等の対象と看做されたもの。
SITA（国際航空情報通信機構・スイスに本部を置く非営利団体） 2020年2月	• 米財務省OFACは、スイスに本部置くSITA（国際航空情報通信機構）との間で、7.8百万ﾄﾞﾙの課徴金支払いで合意 • SITAは、航空データ通信のための専用パケット通信網の運用方式および技術基準を確立し、世界中の国家と地域の空港、管制機関および航空会社を結び、航空機の運航上必要不可欠なデータ通信技術を通じて、空の安全および定時性の確保に寄与している非営利団体 • 2013年から2018年の間、米国による制裁対象となっているシリア・アラブ航空他にデータ通信サービスを提供したこと（9,256件）が、米国法令違反と看做されたもの • 米国法人でもなく、非金融機関であるにも拘わらず、**米国制裁対象者への情報通信サービスの提供を『米国内のサーバーを経由し』、『米国製のソフトウェアを使用』して行ったということが『米国人の関与』と看做され、米国法令等の適用対象となっている**

米国による主な単独経済制裁

- イラン制裁：2018年5月、トラン政権が核合意（JCPOA)の離脱を発表以降、イラン制裁を強化。2020年9月、イランへの国連制裁（武器禁輸措置）を米国のみ独自で復活、イランとの武器取引への関与でベネズエラのニコラス・マドゥロ大統領らを制裁対象に指定、イラン国防軍需省も制裁対象
- 新疆ウイグル関連制裁：2020年7月、新疆ウイグル自自区での人権侵害で中国共産党幹部ら４人を制裁対象に指定（米国内での資産凍結）。2021年1月、米国ポンペイオ国務長官（当時）が、中国を非難する声明を公表。
- 香港関連制裁：2020年8月、香港政府の林鄭月娥（キャリー・ラム）行政長官や主要閣僚など11人を制裁対象に指定。香港における自治を脅かした疑いで、米国内の資産を凍結、米国法の管轄範囲での取引等を禁止（米国マグニツキー法による）。
- ロシア関連制裁：2021年1月、ロシア・天然ガスパイプライン関連の追加制裁を公表（2014年3月のクリミア併合以降、ロシアエネルギー関連企業への制裁を継続強化中）。
- ミャンマー（ビルマ）制裁：2021年2月10日以降、軍事クーデター後の軍部による人権弾圧で軍関係者、軍関係企業を、逐次、制裁対象に指定中。

マグニツキー法（Magnitsky Act）は、正式名称を「2012年ロシア・モルドバ・ジャクソン＝ヴァニック撤廃およびセルゲイ・マグニツキー法の説明責任法」といい、2009年にロシアの税理士セルゲイ・マグニツキーがモスクワの刑務所で死亡した事件(*)の責任者であるロシア政府関係者を処罰するとともに、ロシアに恒久的な正常貿易関係の地位を与えることを目的として、米国議会で可決され、2012年12月にオバマ大統領によって署名された超党派の法令。2016年以降、世界全体を適用範囲とするこの法令は、米国政府が人権侵害者とみなした者を制裁し、その資産を凍結し、米国への入国を禁止する権限を与えている。

(*) 2009年、ロシアの税務弁護士セルゲイ・マグニツキーは、ロシア税務当局が関与した2億3000万ドルの不正を調査した後、当局に逮捕され、モスクワの刑務所で死亡した。獄中でマグニツキーは健康を害したものの、数ヶ月間治療を拒否され、約1年間の獄中生活の後、拘束中に死亡したとされている。

米国の安全保障貿易管理

■ OFACの制裁プログラムとは別に、米国の輸出・再輸出規制もあり、両者は、並行して適用されることが多い。

■ **米国の輸出・再輸出規制**は、米国商務省産業安全保障局（US Department of Commerce's Bureau of Industry and Security・BIS）および米国国務省（US Department of State）によって公布され管理される。当局間において重複があったり、管轄を共有している場合もあるが、各当局は異なる活動をしており、そのルールは、域外適用についても異なるアプローチである。

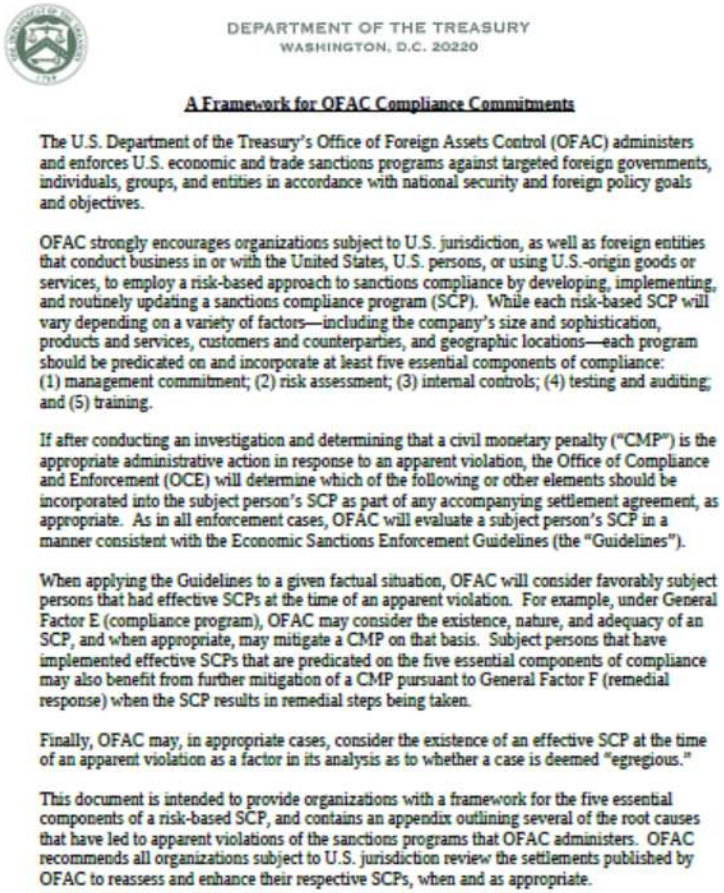
- 米国輸出・再輸出規制における管轄は、米国人か非米国人であるかを問わず、あらゆる人による米国産、矮少（de minimis）レベルを超えた米国産品を含む非米国産品、もしくは、特定の米国技術からの直接の生産物である物、ソフトウェア、技術（これらを「米国管轄に服する対象物」という）の米国からの輸出、移転、再輸出に限定される。

- 米国が独自に中国への輸出規制、投資規制などを強化しているもの：
  - 中国華為技術（ファーウェイ）への輸出管理強化：2019年5月以降、米商務省産業安全保障局がファーウエィ等の中国IT企業、軍産複合企業等の輸出規制を強化中。
  - 中国軍事関連企業への制裁：2021年1月、国防授権法（NDAA)に中国軍事関連企業の制裁対象を拡大中。

米財務省OFAC規制遵守の枠組（Framework of OFAC Compliance Commitments）

◆米国財務省の外国資産管理局（OFAC）は、2019 年5 月2日、「OFAC 規制コンプライアンスの枠組：Framework for OFAC Compliance Commitments」（OFAC規制遵守の枠組）を公表。

◆米国人・金融機関の関与のある取引は、原則、OFAC規制の対象。また、米当局は、米ドルの海外送金は、米銀を経由するか否かにかかわらず、米国人の関与があったとしてOFAC規制の対象とする立場。



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

A Framework for OFAC Compliance Commitments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities in accordance with national security and foreign policy goals and objectives.

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP). While each risk-based SCP will vary depending on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations—each program should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

If after conducting an investigation and determining that a civil monetary penalty ("CMP") is the appropriate administrative action in response to an apparent violation, the Office of Compliance and Enforcement (OCE) will determine which of the following or other elements should be incorporated into the subject person's SCP as part of any accompanying settlement agreement, as appropriate. As in all enforcement cases, OFAC will evaluate a subject person's SCP in a manner consistent with the Economic Sanctions Enforcement Guidelines (the "Guidelines").

When applying the Guidelines to a given factual situation, OFAC will consider favorably subject persons that had effective SCPs at the time of an apparent violation. For example, under General Factor E (compliance program), OFAC may consider the existence, nature, and adequacy of an SCP, and when appropriate, may mitigate a CMP on that basis. Subject persons that have implemented effective SCPs that are predicated on the five essential components of compliance may also benefit from further mitigation of a CMP pursuant to General Factor F (remedial response) when the SCP results in remedial steps being taken.

Finally, OFAC may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed "egregious."

This document is intended to provide organizations with a framework for the five essential components of a risk-based SCP, and contains an appendix outlining several of the root causes that have led to apparent violations of the sanctions programs that OFAC administers. OFAC recommends all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and enhance their respective SCPs, when and as appropriate.

◆OFAC規制遵守の枠組においては、各企業のOFAC規制コンプライアンス・プログラムは、金融機関毎のリスク要因（企業の規模、複雑さ、(sophistication)、製品・サービス、顧客・取引先並びに所在地等）によって異なるとしつつ、コンプライアンス・プログラムの**「本質的な要素」**として、以下の５項目を挙げている。

1. **経営陣のコミットメント**
2. **リスク評価**
3. **内部統制**
4. **検査及び監査**
5. **研修**

OFAC規制遵守の枠組におけるリスク評価の基本的な考え方

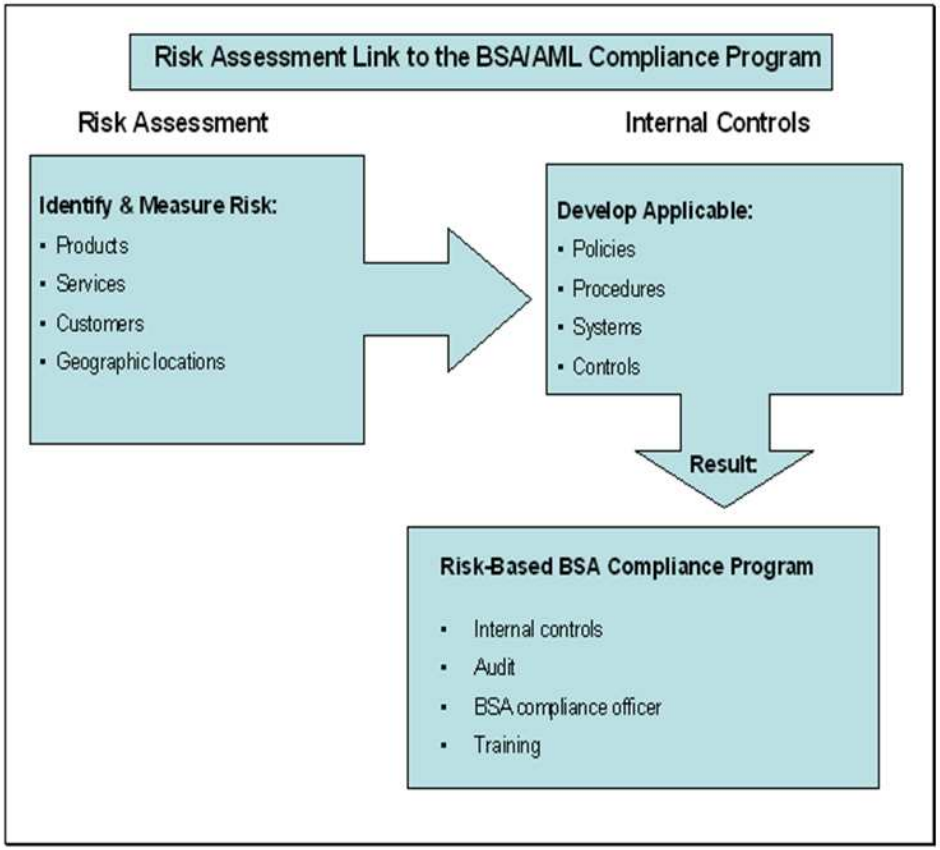
OFAC Framework	ポイント
General Aspects of an SCP: Conducting a Sanctions Risk Assessment A fundamental element of a sound SCP is the assessment of specific clients, products, services, and geographic locations in order to determine potential OFAC sanctions risk. The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls. **I. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.** **II. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.**	• 制裁コンプライアンス・プログラムは、リスク評価に基づくもの。 • 全てに適用可能なリスク評価手法は存在しないものの、リスク評価手法については、原則として「組織全体を隅から隅まで精査し、当該組織と外界とのタッチポイント（接点）を評価するもの」でなければならない。 • 評価対象は、顧客に起因するリスクに限らず、サプライチェーン、仲介者及び契約相手のほか、当該組織の製品、サービス及び取引並びに当該組織及びそのサプライチェーン、仲介者及び取引先の所在地から生じるリスクを含めた、包括的かつ網羅的なものであるべき。 • OFAC 規制リスクの評価にあたっては、何らかの関係又は取引の開始時や過程において実施したデューディリジェンスによって得られた情報を活用すべき。例えば、KYC（顧客確認）やCDD（顧客デューディリジェンス）のプロセスで取得した情報を用いて、顧客又は取引先との関係に対するリスク格付システムを活用することも有益。 • OFAC 規制リスクの評価に役立つツールとして、OFAC の「経済制裁実施ガイドライン：Economic Sanctions Enforcement Guidelines」に添付されているOFAC Risk Matrix を活用。 • リスク評価は、合併・買収の過程でも重要。合併・買収の検討プロセスに、コンプライアンス検証機能を組み込み、OFAC 規制関連の問題を確実に特定し、経営陣に報告し、合併・買収の完了前に対応できるようにすべき。 • OFAC 規制リスクを特定、分析、対応するための手法を確立したうえで、文書化することが必要。 • また、リスク評価は一回限りの作業ではなく、違反行為や違反の主要原因を究明するために「定期的、状況によっては継続的」に行うべき。

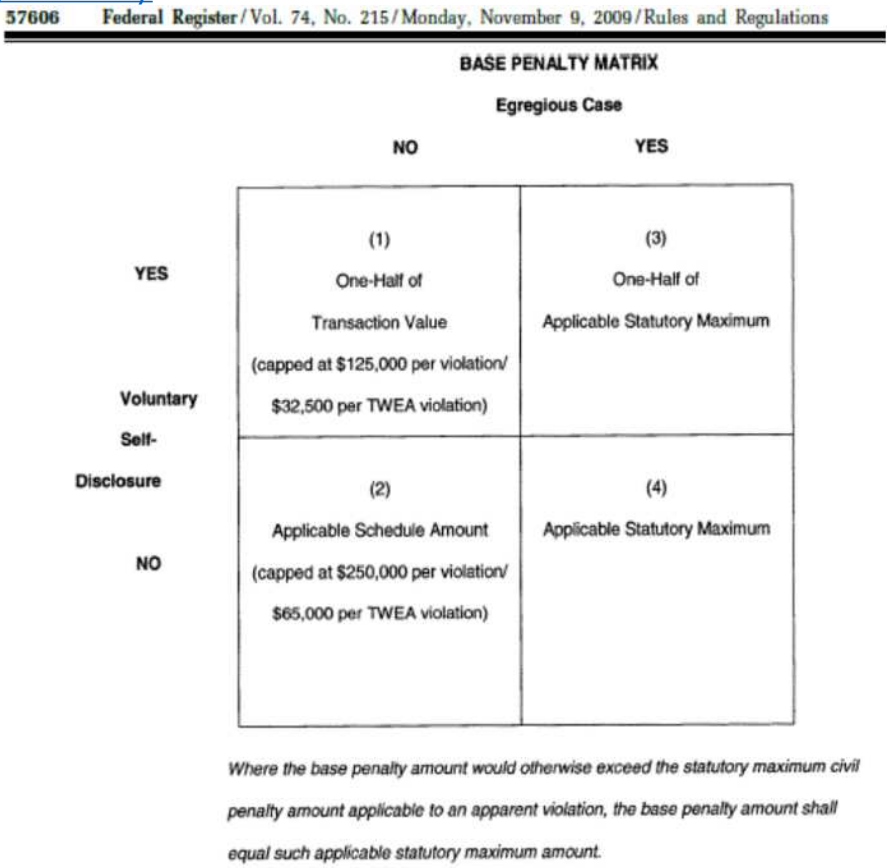
リスク評価マトリックス　および、制裁評価マトリックス

Guidance on OFAC's Enforcement and Compliance Policies

https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information

- A Framework for OFAC Compliance Commitments
- OFAC Enforcement Guidelines
- Memoranda of Understanding Between OFAC and Bank Regulators
- Memorandum of Understanding Between OFAC and the State of Delaware Department of Justice
- OFAC Office of Compliance and Enforcement Data Delivery Standards Guidance: Preferred Practices for Productions to OFAC
- Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork
- Sanctions Compliance Guidance for the Virtual Currency Industry





米財務省OFAC規制遵守の枠組（根本原因分析）

◆OFAC規制遵守の枠組では、OFAC 規制違反の**根本原因（root cause）**を10項目に分類し、その内容を具体的に記載したリストを公表し、金融機関等に注意喚起している。

1. **正式なOFAC規制コンプライアンス・プログラムが整備されていなかったこと**
2. **OFAC 規則の適用可能性に関する誤解又は認識の欠如**
3. **非米国人による取引の斡旋（Facilitation）**
4. **米国原産の製品、技術又はサービスを制裁対象者又は、制裁対象法域に輸出又は再輸出したこと**
5. **制裁対象者又は制裁対象法域が関与する取引であるにもかかわらず、米国の金融システムを利用し、又は米国の金融機関向けに、若しくは、これを経由して支払いを処理したこと**
6. **制裁をスクリーニングするソフトウェア、又は、フィルタリング・システムの機能不全**
7. **顧客／クライアントに関するデューディリジェンスが不適切であったこと**
8. **コンプライアンス機能の分散化及び制裁規則コンプライアンス・プログラムの適用における不統一**
9. **標準的でない支払慣行又は商業慣行の利用**
10. **個人の問題** ⇒ OFAC規制違反において個人の責任を問うケースもあると明記。

X. Individual Liability
In several instances, individual employees—particularly in supervisory, managerial, or executive-level positions—have played integral roles in causing or facilitating violations of the regulations administered by OFAC. […] In such circumstances, OFAC will consider using its enforcement authorities not only against the violating entities, but against the individuals as well.

米財務省経済制裁評価書（The Treasury Sanction Review）

◆10月18日、米財務省は、同省が施行している経済制裁の評価と、今後、改善すべき点も取り纏めた報告書(The Treasury 2021 Sanctions Review)を公表。

- 同報告書は、米財務省が施行している制裁法令等に限定し、その施行の現状を検討したもの。イエレン財務長官が、財務長官候補として指名され米議会による承認のための公聴会に出席した際、財務省の現在の制裁法令の施行の実情を包括的に調査し、必要とあらば改善すべき側面を見直していく旨述べたことから、財務長官就任後、同長官の指示により、Adeyemo財務副長官主導の下で、調査が行われていた。

◆財務省が施行している各種経済制裁は、米国安全保障上の政策的な効果は上げていると評価。
（*“Sanctions are a fundamentally important tool to advance our national security interests,” ... “Treasury’s sanctions review has shown that this powerful instrument continues to deliver results but also faces new challenges. We’re committed to working with partners and allies to modernize and strengthen this critical tool.”*(財務副長官))。

◆他方、国際政治・経済社会における力関係の変化や、デジタル経済の拡大、米ドルの影響力の相対的低下、米国の制裁がもたらす負の影響なども踏まえ、政策評価すべきとの問題意識もあり、今後、取り組むべき課題として以下を提示。

① 政策目的に直結した制裁とすること、

② 可能な限り共通の政策や安全保障上の利害関係を有する多国間の枠組と歩調をあわせた制裁を行うこと、

③ 制裁対象ではない他者に及ぼす経済的、政治的、人道的悪影響を最小限に食い止めるよう工夫すること、

④ 制裁の内容を明確にし、それにより影響を受ける利害関係者が理解できるよう説明すること、

⑤ 財務省の制裁関連部局が、近代的な技術や、適切な人材を活用し、その他の法令遵守を支援するためのインフラを充実させること。

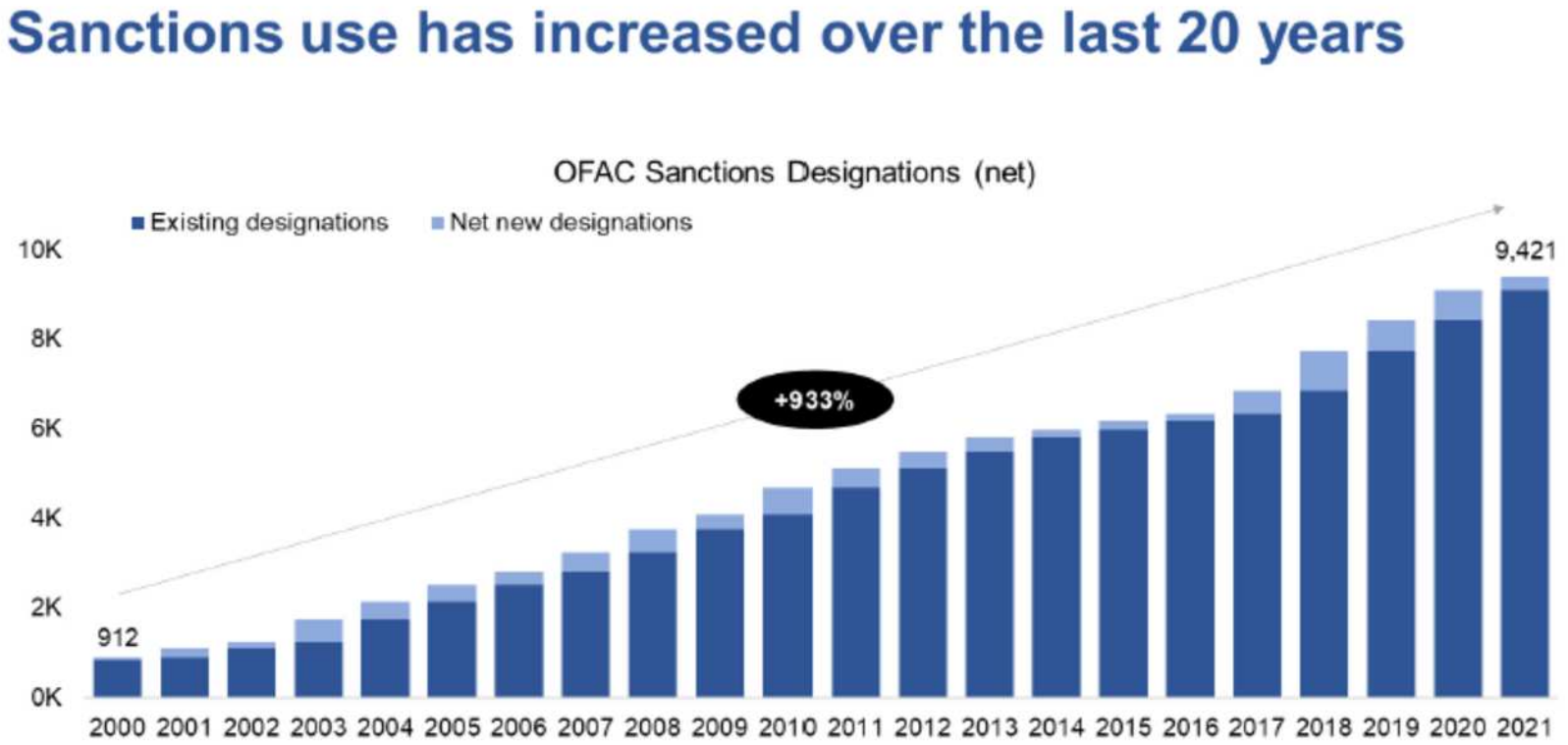
The Treasury 2021 Sanctions Review

65

米財務省経済制裁評価書（The Treasury Sanction Review）

◆米財務省経済制裁評価書(The Treasury 2021 Sanctions Review)によれば、2021年時点で、37の制裁プログラム、9,471の制裁対象者、団体、国・地域。

◆2000年から20年間で、12,000の制裁指定、3,000の指定解除が行われ、有効な制裁対象者数は**10倍**となっている。



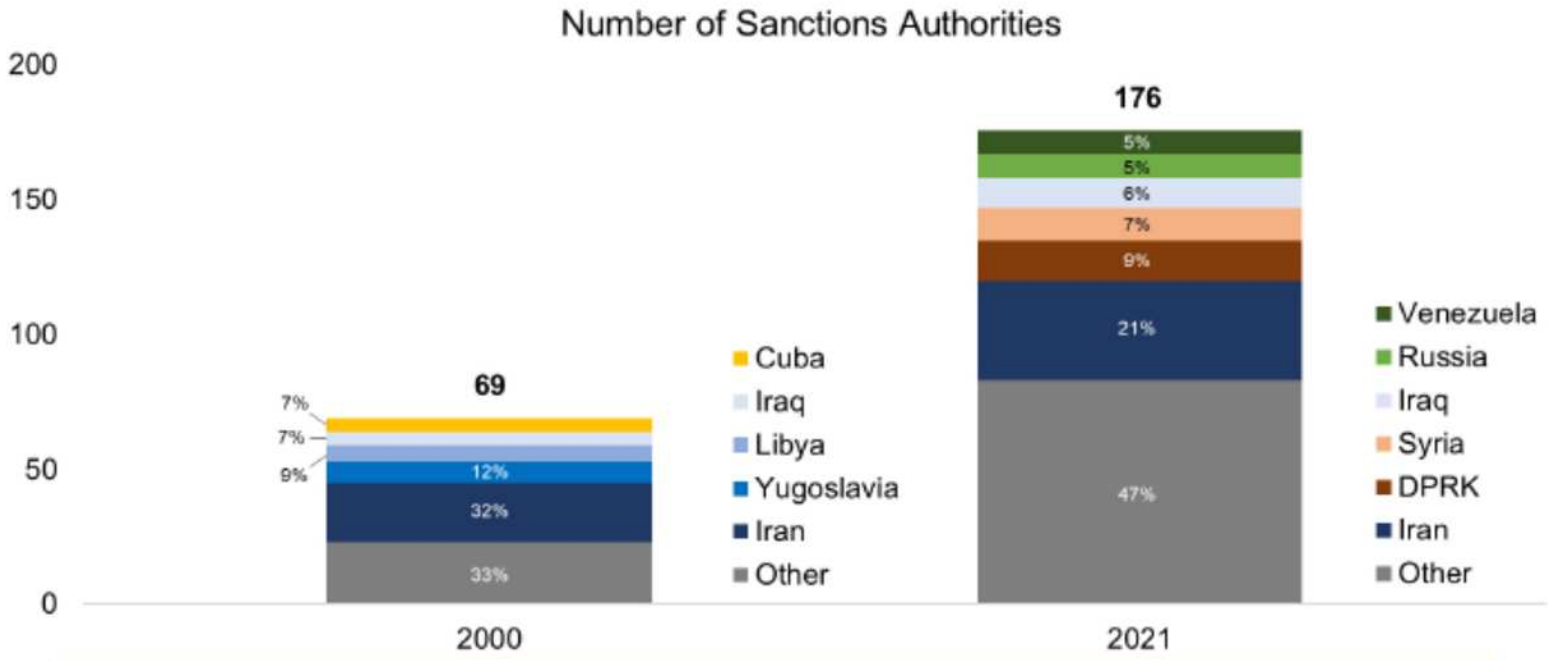
The Treasury 2021 Sanctions Review

米財務省経済制裁評価書（The Treasury Sanction Review）

◆米財務省経済制裁評価書(The Treasury 2021 Sanctions Review)によれば、国を対象とする制裁プログラム数については、2000年の69から、2021年には176に増加。

◆その他以外では、イランが引き続き最大の制裁対象国。その他の割合が増加するなど、制裁対象国は多様化。

Composition of U.S. Sanctions Programs Has Shifted



"I do seriously think we have a responsibility to use sanctions for important national security issues. But we need to think about the long-term impact on the global currency."

- Former Secretary of the Treasury Steven Mnuchin

The Treasury 2021 Sanctions Review

米国防授権法（ The National Defense Authorization Act for Fiscal Year 2021 ）

◆2021年1月1日、米国上院は、トランプ前大統領が行使した拒否権を覆し、**2021年国防授権法（the National Defense Authorization Act for Fiscal Year 2021）**を承認。予算の総額は7405億ﾄﾞﾙ（約77兆円）となり、20会計年度に比べて0.3%増え、中国への対抗を狙う政策を多く盛り込んでいる。

◆2021年国防権限法の内容は非常に多岐に渡るが、その中の立法の一つとして、マネーロンダリング等の金融犯罪のために米国におけるシェルカンパニーを利用すること等を防止するため、米国財務省に対して、米国において設立された事業体の実質的支配者（beneficial owner）を報告することを義務付ける、**企業透明法Corporate Transparency Act(CTA)が制定された**(2021年12月31日施行予定)。

https://www.congress.gov/bill/116th-congress/house-bill/6395/text

A. 中国を念頭に置いた国防の基本方針

インド太平洋地域における[中国に対する]抑止力を強化するための同地域における米軍の防衛体制及び同盟諸国との協力の強化。

B. 中国を念頭に置いた具体的対応策

米国会計監査長官による国防総省の強制労働を用いて製造された産品の調達・再販を防止するための措置に関する監査義務を規定。

米国防長官に、米国内で直接若しくは間接的に活動を行っている「中国軍事会社(Chinese military company)」を特定し、2030年12月まで毎年及び随時、報告を行うことを義務づけるもの。同趣旨の条項は1999年度の国防授権法にも含まれていたが、NDAA 2021では、対象となる「中国軍事会社」の範囲を拡大し、軍民融合に寄与している会社も含まれることとなった。

C. ロシアを念頭に置いた具体的対応策

D. その他の制裁、輸出管理等に関連する条項

トルコ政府によるロシアからのS-400(対空防衛システム)調達は、ロシア政府の防衛若しくは諜報部門に関与している者との重要な取引に対して制裁措置を科すことを規定している「制裁を通じての米国の敵対国に対抗する法(CAATSA)」のSection 231に抵触するものである旨認定し、NDAA 2021制定後30日以内に米大統領が制裁措置を科すことを義務づけるもの。

2019年欧州エネルギー安全保障保護法 のSec. 7503が規定しているNord Stream 2及びTurkstreamパイプラインプロジェクト建設に対する制裁規定の内容を改正(制裁の対象となる「パイプ敷設活動(pipe-laying activities)」の定義を拡大)し、パイプライン敷設を行っている船舶の保険、再保険サービスやパイプラインの運営に関連するテスト、点検、認証等のサービスを提供することに対しても、制裁措置の対象となる旨規定。

【参考資料】

海外当局によるマネロン等対策に関する行政処分事例

(出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

海外のマネロン等処分事例（１/9）

金融機関名	事案
HSBC （イギリス） 2012年	• 2012年7月、米国上院国土安全保障・政府問題委員会常設調査小委員会が、過去10年のHSBCの米国拠点等におけるAML/CFT態勢の不備を取り上げた報告書を公表し、公聴会で経営陣を批判。 • HSBCの拠点網を使った、メキシコの麻薬犯罪組織、イラン、ロシア関係のマネー・ローンダリングを見逃していた疑い。 • 2012年7月、HSBCメキシコ現法が27.5百万ドルの制裁金をメキシコ当局に支払、12月には、HSBCが米国当局に**19億ドル**（当時過去最高額）の罰金を支払い。 • HSBCは、関連当局との間で、AML/CFT態勢の高度化に関し合意し、実行。
スタンダード・チャータード銀行（SCB） （イギリス） 2012年	• 2012年8月、ニューヨーク州金融サービス局（NYDFS)が、SCBが過去10年にわたって意図的にイラン向け送金を隠ぺいしてきたと非難する報告書を公表。 • 2012年12月までに、二回にわたって、**総額6億67百万ドル**の罰金を支払い。 • SCBは、8月のNYDFSの報告書公表以降、株価が下落し最大時価総額の25%相当が減少。 • SCBは、関連当局との間で、AML/CFT態勢の高度化に関し合意し、実行。
BNPパリバ （フランス） 2014年	• 2014年6月、米国司法省は、BNPパリバが米国の金融制裁の対象となっていたスーダンやイランとの間で2004年から12年にかけて、ドル送金などの金融取引を続け、その事実を隠していたとして、**総額89億ドル（過去最高額）**の罰金を科し、ドル資金の決済業務の一部も最長1年間禁じると発表。 • BNPパリバは、関連当局との間で、AML/CFT態勢の高度化に関し合意し、実行。関係する幹部13名も解雇。

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

海外のマネロン等処分事例（２/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
US Bank NA （米国） 2018年2月	• 米国大手地銀（中西部）であるUS Bank及び親会社のUS Bancorp.は、マネロン管理態勢の不備で米当局（司法省、OCC、FinCEN、連銀）に合計**613百万ﾄﾞﾙ**の罰金を支払うことで合意。 • 金融犯罪に関連する送金等を行っていたにもかかわらず、疑わしい取引の届出を提出していなかったという態勢不備によるもの。
コモンウェルス銀行 （豪州） 2018年6月	• 豪大手銀行のコモンウェルス銀行(CBA)は、マネロン防止態勢の不備で豪当局に対して**7億豪ドル（約530百万米ﾄﾞﾙ）**の罰金を支払うことで合意。罰金額としては、豪州では過去最大の規模。 • 金融犯罪組織が違法薬物や銃器の闇取引で得た資金がCBAを通じて決済されていたもので、疑わしい取引届出がなされなかった等の豪法令違反事案は5万件以上。 • **CEOは、本件や本件に関する株価下落の責任を取って辞任。**
ダンスケ銀行 （デンマーク） 2018年9月	• エストニア支店で大規模なマネー・ローンダリングの舞台となっていた疑惑が深まる中で、CEOが辞任。最大**2340億ドル（約26兆3000億円）**の資金洗浄がエストニア子会社を通じて行われていた疑い（**行内第三者委員会の調査**） • デンマークとエストニアで刑事捜査が進行中。米国当局も捜査中との報道あり。
ING （オランダ） 2018年9月 2021年3月	• マネー・ローンダリング捜査を巡り、**7億7500万ユーロ（約1000億円）**を支払うことと AML/CFT管理態勢を強化することでオランダ検察当局と合意。 • 2010～16年にかけて銀行口座を資金洗浄に利用される状況を招いており、適切に顧客管理をしていなかったため、多数の顧客が同行に設けた銀行口座を犯罪活動のための資金洗浄に利用するのを許していたことが明らかになったもの。 • 2021年3月、フランスの規制当局/ACPRは、ING**の現地法人に対して、マネロン・テロ資金供与管理体制の脆弱性を理由に3百万ユーロの罰金。**PEPsなど高リスク顧客への確認不十分など。2018年9月以降、調査を行っていたもの。

海外のマネロン等処分事例（３/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
Capital One Bank （米国） 2018年10月	• 米国を中心にネットバンキング、クレジットカード事業を行うキャピタルワン・バンクは、マネロン管理態勢の不備で、米当局（OCC)との間で**100百万**ﾄﾞﾙの罰金を支払うことで合意。 • コンプライアンスに係る内部管理態勢の不備、疑わしい取引届出態勢の不備、非対面取引（ネットバンキング）のリスク評価の不備が行政処分の主な理由。
ソシエテ・ジェネラル （フランス） 2018年11月	• キューバやイランなどに対する米国の経済制裁に違反していたと認め、米当局に計**13億4000万ドル（約1500億円）**の罰金を支払うことで合意。 • 2003～13年にキューバ、イラン、スーダン、リビアなどの制裁対象国へ国際送金を繰り返していた。
ブリティッシュ・アラブ商業銀行 （英国） 2019 年9月	• 英国のBritish Arab Commercial Bankは、米財務省OFACとの間で米国制裁関連法令等（スーダン）の違反で**4百万**ﾄﾞﾙの罰金を支払うことで合意。 • **同行は米国内に拠点はなく**、非米国銀行のドル口座（当方口）を経由して、2010年から2014年の間、スーダン中銀を含むスーダン法人に対し、合計72回、190百万ﾄﾞﾙの米ドル・バルク送金を行ったもの。 • **米国金融機関は経由していないものの、決済通貨がドル**であることから米国法令等の対象と看做されたもの。
ウェストパック銀行 （豪州） 2019年11月 2020年9月	• 豪大手銀行の一つであるウェストパック銀行は、マネロン管理態勢の不備で**CEOが辞任**すると発表。海外送金に関する報告漏れや児童搾取のリスクのある先の顧客リスク評価不備等で、合計23百万件の法令等抵触事案があった模様。 • **2020年9月、13億豪ﾄﾞﾙの罰金支払いで合意（豪州では過去最高額）**。 • 2021年3月、APRA/オーストラリア規制当局は、Westpac銀行のAML/CFT違反に関する調査を終了、銀行法への違反はなし。但し、Westpacは、オペレーショナルリスク資本を10億豪ドル積み、引き続き事業全体のリスクガバナンスを向上させるための改善計画を進捗させる必要あり。

海外のマネロン等処分事例（４/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
ハルクバンク （トルコ国営銀行） 2019年10月	• 米司法省は、米国のイラン制裁逃れのための数十億ﾄﾞﾙ相当の隠ぺい工作に関与したとして、詐欺、マネロン及び制裁措置違反破り等6件の訴因からなる起訴状によって米検察当局により起訴 • 米国は、**他国の国営銀行であっても米国法令違反で「米国」において「起訴」する。**
SITA （国際航空情報通信機構・スイスに本部を置く非営利団体） 2020年2月	• 米財務省OFACは、スイスに本部置くSITA（国際航空情報通信機構）との間で、7.8百万ﾄﾞﾙの課徴金支払いで合意 • SITAは、航空データ通信のための専用パケット通信網の運用方式および技術基準を確立し、世界中の国家と地域の空港、管制機関および航空会社を結び、航空機の運航上必要不可欠なデータ通信技術を通じて、空の安全および定時性の確保に寄与している非営利団体 • 2013年から2018年の間、米国による制裁対象となっているシリア・アラブ航空他にデータ通信サービスを提供したこと（9,256件）が、米国法令違反と看做されたもの • 米国法人でもなく、非金融機関であるにも拘わらず、**米国制裁対象者への情報通信サービスの提供を『米国内のサーバーを経由し』、『米国製のソフトウェアを使用』して行ったということが『米国人の関与』と看做され、米国法令等の適用対象となっている**
コメルツバンク ロンドン支店 （ドイツ） 2020年6月	• 英FCAは、独コメルツバンク（ロンドン支店）に対し、マネロン管理態勢に関して37.8百万ポンド（50億円相当）の過料支払いを命じた • 2012年から2017年の間に、**FCAからの懸念表明(2012, 2015, 2017年）にも拘わらず、マネロン管理態勢の脆弱性及び改善のための適切な対応を取らなかったこと等**であるが、この時期にFCAがマネロン強化のガイダンスを業界に対して示していることに加えて、**「他の金融機関に複数の行政処分を発するというwarningが出ているにも拘わらず、同行は脆弱性を放置していた」**、とのこと。

海外のマネロン等処分事例（５/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
Apple, Inc. 2019年11月	• 2019年11月29日、米財務省OFACとApple, Inc.（本社：米カリフォルニア州）は、**取引スクリーニング手続きの不備**で、OFACが制裁対象者とするアプリ開発業者及びその実質的支配者と取引を行ったOFAC法令違反で、**467千ﾄﾞﾙ（約49百万円）の過料**を支払うことで合意。 • 制裁対象者について、本来であれば、「SIS d.o.o」と表記されるべきところを、誤って「SIS DOO」として登録してしまい、かつ、スクリーニング・システムが、大文字小文字の違いを検知できなかったこと、及び、実質的支配者の肩書が異なっていたことなどにより、取引開始時と継続的なチェックで漏れてしまっていたとのこと。 • Appleは、これらの違反を自主的に発見・報告し、システムも修正の上、教育研修などの再発防止策も実施済。
Amazon 2020年7月	• 2020年7月8日、米財務省OFACとAmazon Com, Inc.（本社：米ワシントン州）は、**取引スクリーニング手続の不備**により、複数のOFAC法令違反取引を行ったとして、**134,523ﾄﾞﾙ（約14百万円）**の過料を支払うことで合意。 • Amazonが2011年11月から2018年10月に掛けて、クリミア、イラン、シリアからの注文や、キューバ、イラン、北朝鮮、スーダン、シリアの外交団からの注文に応じており、低価格の消費関連商品を含む取引の総額は260千ドルであったとのこと。 • 米財務省OFACの公表文によれば、Amazonの取引スクリーニングシステムは、制裁対象国の都市名、制裁対象国の在外大使館、スペリングの習慣的な違い等を検知することが出来ていなかった模様。 • Amazonは、既に、是正措置と、内部及び第三者による制裁コンプライアンス態勢と検知システムの見直しや制裁対象国・地域のIP(Internet Protocol)の遮断措置を含む再発防止策を講じており、今後も継続的に態勢を見直すこととしている • 米財務省OFACは、「**自動化された検知システムに依存しているグローバル企業は、合理的でリスクベースの措置により、適切に顧客情報をスクリーニングし、習慣的なスペリングの違いも検知出来るようにすると共に、制裁関連法令遵守態勢の有効性と適切性について、継続的に検証を行う必要がある。**」としている。

海外のマネロン等処分事例（６/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
BitPay 米国 2021年２月	• アトランタに本社を置くBitPayが、クリミア地域、キューバ、北朝鮮、イラン、スーダン、シリアに所在すると思われる人物に（**IPアドレスや位置情報を有していたにも関わらず**）、BitPayのプラットフォーム上でデジタル通貨を利用した米国などの加盟店との取引を認めていたとして、米財務省OAFCとの間で、507,375米ドルの和解金支払に合意。 • OFACは、デジタル通貨サービス提供者も含む全ての米国人にOFACの義務が適用されることを強調。
National Westminster Bank: NatWest (旧Royal Bank of Scotland) 英国 2021年３月	• 3月16日、英金融行為監督機構（FCA）は、マネーロンダリング（資金洗浄）を防ぐ体制が不十分だったとして、英銀大手ナットウエストを刑事訴追したと発表。 • 2011年11月～16年10月の約5年間、適切な対処を怠ったと指摘。金融機関に不正利用防止の体制や運用を義務付ける英国の資金洗浄規則に基づく措置で、銀行への発動は07年の施行後で初めて。 • FCAによると、英国の法人顧客（ファウラー・オールドフィールド貴金属店（宝石・金地金取扱業者、2016年にマネロンに関与したとして事業停止））の口座をめぐる対応が訴追対象。約3億6500万ポンド（約550億円）が入金されて資金洗浄への利用が疑われたが、十分な監視や調査（EDD)をしていなかった。
Nordgas S.r.l. イタリア 2021年3月	• ガスボイラーシステム及びプリケーション用の部品を製造・販売するイタリアのNordgas, S.r.l.社が、イラン規制への違反を理由として、米財務省OFACとの間で、95万米ドルの和解金支払いに合意したと公表。 • Nordgas社は、約4年間にわたり、米国企業から調達した空気圧スイッチ27個を、イラン国内の10社に再輸出し、米国企業に間接的に商品をイランに輸出させていたとされたもの。 • 和解金のうち65万ドルは、Nordgas社の財務状況等を鑑み、コンプライアンス遵守の取組みが完了するまで保留される

海外のマネロン等処分事例（７/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
Swedbank スウェーデン 2021年５月 2020年3月	• 2021年5月、スウェーデン大手銀行のスウェドバンクは、2016年12月から2019年2月の間に同行のマネーロンダリング防止管理に不備があったとして、ナスダック・ストックホルムから4,660万スウェーデンクローナ（約6億円）の罰金を科された。 • スウェドバンクは、2020年3月にも、スウェーデン当局から、バルト諸国の子会社におけるマネロン対策に重大な欠陥があり、当局に情報を隠していたとして、既にスウェーデンで過去最高の40億クローナ（約480億円）の罰金を科されていた。 • 当該処分において、スウェドバンクは、バルト諸国でのマネロン対策に深刻かつ体系的な欠点が指摘されており、実質的支配者の確認も適切に実施されていなかった。 • 2010年から2016年にかけて、主にロシアの非居住者から年間200億ユーロに上る疑わしい取引をエストニア経由で処理していたとされる。 • スウェドバンクは、デンマークのダンスケ銀行も巻き込んだマネロンスキャンダルの詳細が2018年末から2019年にかけて明らかになり、CEOと取締役の多くが辞任。
SEB bank スウェーデン 2020年６月	• スウェーデンのセブバンクは、バルト諸国（エストニア、ラトビア、リトアニア）にある銀行の子会社でのマネロン対策不備及び、同子会社に対するガバナンスが十分でなかったとして、10億クローナ（約125億円）の罰金を科された。 • バルト諸国にある子会社は、地理的にもリスクが高く、非居住者顧客や非居住者の実質的支配者を持つ顧客など、高リスク顧客が多かったが、同顧客を背景とするコンプライアンス及びレピュテーションリスクの高まりを認識・管理しておらず、バルト諸国の子会社銀行におけるマネロン対策の中核の一部に不備があるという情報を繰り返し受け取っていたが、十分な対策を講じていなかった。 • エストニアの子会社では、2016年以前は、実質的支配者に関する情報を検索可能な形で保有していなかったことも判明。

海外のマネロン等処分事例（８/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
National Australia Bank (NAB) 豪州 2021年６月	• 豪銀大手ナショナル・オーストラリア銀行（NAB）は、マネーロンダリング（資金洗浄）防止およびテロ対策法に対する重大かつ継続的な違反の疑いで、当局の検査を受けていると発表した。 • これを受けて罰金支払いの可能性やコンプライアンス費用の増加懸念が浮上し、株価は2．６%下落した。オーストラリア金融取引報告・分析センター（AUSTRAC）は、さらなる調査を必要とする「重大な懸念事項」があったとしながらも、現時点では民事上の罰則を科すことは検討していないとした。 • 2019年12月、同行は、AUSTRACに対して、自行のAML/CFT態勢に不備があると自主的に報告していた。
Westpac, NZ ニュージーランド 2021年8月	• 8月11日、ニュージーランド準備銀行（中央銀行）は、豪銀大手ウエストパック銀行のニュージーランド（NZ）法人に対し、マネーロンダリング（資金洗浄）およびテロ対策法の報告義務を違反した取引が8000件近くあると**警告した**。 • NZ中銀は、オーストラリア当局が2019年に、児童搾取に関与した人々などの資金のやりとりを可能にしたとしてウエストパック銀行（豪）をマネロン防止法違反で訴えたのを受け、NZ国内の銀行に関する調査に着手しており、今回、調査結果を発表したもの。 • NZ中銀は、ウエストパック(NZ)内の報告システムの不備によって、報告の必要がある国際電信送金が検知・報告されなかったと指摘。報告義務を違反したのは2018年７月から19年２月の間に行われた外為送金8,000件に上った。
Bank of China, UK 英国 2021年8月	• 8月26日、米財務省OFACは、Bank of China(UK)が、過去、現在は解除されているスーダン制裁規制に違反していたとして、2,329,991米ドルの和解金支払いに合意したと発表。 • BOC(UK)は、2014年9月から2016年2月にかけて、スーダン関連取引を合計111件（40,599,184米ドル）、米国のコルレス銀行を通じて決済していた。 • 顧客から提出された取引書類にはスーダンとの関係を示す内容があったものの、顧客データベースへの登録と潜在的なリスク評価に不備あり、米銀を通じて処理したSWIFTメッセージにもスーダンの記載は含まれていなかった。

海外のマネロン等処分事例（9/9）

（出所）海外当局／金融機関等のプレスリリース、報道等の公表、公知情報から筆者が作成

金融機関名	事案
HSBC 英国 2021年12月	• 12月17日、英金融監督当局（FCA)は、HSBCのマネーロンダリング（資金洗浄）対策に不備があったとして6,395万ポンド（8,525万ドル、96億円相当）の罰金を科したと発表。 • FCAによると、2010年から2018年までの８年間で、HSBCの英国での取引モニタリング・システムに関連して深刻な脆弱性が見つかり、その背景には組織内の連携ミスやガバナンスの問題もあった。罰金は課徴金ガイドラインでは当初9,100万ポンドだったものが、HSBCが異議をとなえなかったため3割減額。 ○ 取引モニタリング・システムの問題点 ・取引モニタリング・システムのシナリオ設定が不適切 2014年までマネーロンダリングやテロ資金供与のリスクに応じたシナリオの見直しが不十分。 また2016年以降は新たに設定されたシナリオに関する適時・適切なリスク評価が実施されていなかった。 少なくとも二つの不適切なシナリオによって検知の遅延が発生した。 ・パラメーターの設定が不適切 閾値の設定や閾値とシナリオの組み合わせが不適切 サプレッションの運用が不適切 ・データの品質 不完全や不正確なデータがシステムにインプットされていた ○ 態勢面の問題 • HSBCは2012年、メキシコの麻薬カルテルの資金洗浄に関わっていた等として、米当局に罰金１９億ドルを支払ったことを受け、2012年以降、長期間にわたってマネロン等対策の業務改善に取り組んできたものの、取引モニタリング・システムについては、長期間、不適切な運用が続いていたもの。 • 今回の処分は2012年の罰金事象とは関連性はないものの、その後のマネロン等対策の改善策において、取引モニタリング・システムの運用に関しては、ガバナンスや組織的な問題により、複数の内部からの改善勧告にも拘わらず、抜本的な改善が取組まれていないかった模様。

【参考資料】

最近のFATFにおけるAML/CFT監督等に関する議論や公表物について

(Source: The FATF Home Page/Documents/等の公表資料から筆者が作成)

(1) リスクベース・アプローチによる監督に関するガイダンスの公表

1. 経緯

- FATF相互審査において、IO.3（監督）が多くの国で低評価であり、リスクベースに基づくマネロン監督の強化が重要との認識を受け作成。3月4日付で公表。
  https://www.fsa.go.jp/inter/etc/20210305.html

2. 本ガイダンスのポイント

- オンサイトかオフサイトといった監督上の形式面の違いを強調するのではなく、リスクに応じて適切な監督ツールを組み合わせ、リスク低減という監督上の成果を確実にあげることの重要性を強調。
- テクノロジーの活用にも言及。

当庁としても、本ガイダンスも踏まえ、引き続きリスクベース・アプローチに基づくマネロン監督を深化させていく。

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスの構成】

1．リスクベース監督に関するハイレベルガイダンス

(1)リスクの理解

- リスク評価の目的と射程
- リスク評価のプロセス
- リスク評価において考慮すべき情報
- リスクの理解の更新

(2)リスクベースアプローチによる監督

- 監督戦略の意義
- 監督上のアプローチの調整
- オンサイトとオフサイトの組合せによるリスクベースアプローチの強化
- 低リスク先への監督手法
- 中長期的に頑健なリスクベースアプローチの発展
- 制裁の適用
- リスクベースアプローチの実効性の計測手法
- 国内・国際協力

(3)分野横断的な問題

- SupTechの活用
- 民間セクターとのエンゲージメント
- サードパーティーの利用

2．リスクベース監督に関する共通の課題とその対処方法

(1)リスク評価に係る課題と対処方法

(2) リスクベース監督の適用に係る課題と対処方法

3．各国の事例集

(1)金融機関の監督

(2)DNFBPsの監督

(3)VASPsの監督

(4)COVID-19下での監督上の対応

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスのポイント１】

１．総論

（１）共通の監督枠組み

■ 各法域の状況とリスクを考慮に入れ、様々な監督上の枠組みが利用されている。FATFは、プロセスではなく成果に重点を置いており、監督の成果がML/TFリスクに効果的に対処し得る限り、特定の監督枠組みを規定（prescribe）しない

（２）効果的なリスクベースアプローチの特徴

■ 監督当局は、セクター・事業者のML/TFリスクを特定、評価、理解し、継続的かつ効果的にそれを低減する。当局は特に、以下の措置を講じることが期待される。

① ML/TFリスクを理解し、それを更新・発展
② 低リスク先には効率的・効果的に対応する一方で、高いML/TFリスクや新規のML/TFリスクに効果的に焦点を当てた監督戦略を策定・実施
③ 事業者に効果的なAML/CFT方針を備えさせるとともに、ガイダンスの提供、是正措置の指示、強制力の抑止的・比例的な行使により、監督先の行動に影響を及ぼす
④ 変化するリスク環境を把握し、新規のリスクを早期に発見
⑤ その機能を遂行するために必要な専門知識、権限、裁量、ツール、十分なリソースを具備
⑥ 情報共有、優先すべきリスクの特定、合同の監督活動等を通じ、他当局と協働

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスのポイント２】

２．監督上のリスク評価

- NRA（National Risk Assessment）と監督当局のリスク評価とは、相互連関。また、固有リスクの評価においては、監督当局は、NRAにより示されたリスクカテゴリ以外の利用可能な情報も考慮する必要
- リスク低減措置の評価に当たっては、監督当局は、特定のコントロールやプロセスに限らず、AML/CFT枠組み全体の有効性と健全性を評価
- AML/CFTコントロールがいかに強固であっても、固有リスクを完全に低減することはできず、残存リスクには、常にリスクアペタイトに見合ったコントロールが必要

３．リスクベースアプローチに基づく監督

（１）リスクベースの監督アプローチ

- ①監督戦略や検査計画の策定、②監督ツールの適切な組合せの選択、③監督の性質、頻度、強度、焦点の調整、を実施。監督活動のフィードバックを基にリスク評価を見直し、それに基づき上記①～③の繰り返し

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスのポイント３】

（２）監督戦略

- 監督当局は、リスクベースの監督戦略を策定し、履行
- 監督戦略では、監督先のリスクに応じた特定の監督手法を採用することにつき、その合理性を明記。監督当局は、形態や数ではなく、自らの監督活動が監督上の成果（リスクの特定・低減）に寄与するかを考慮することが必要
- 監督ツール採用にあたっての原則
  - ✓「Outcome-focused」、「Risk appropriateness」、「Efficiency」、「Dynamism and responsiveness」
- リスクに応じた監督アプローチの調整例
  - ✓ リスクに応じてオン・オフ比率を見直すなど監督上のアプローチを調整
  - ✓ 監督の焦点を調整（リスクの高い個別商品、特定のAML/CFTプロセス等）
  - ✓ 対話、検査の頻度、期間の調整
  - ✓ リスクに応じた監督の程度の調整、リソースの調整

（３）オンサイト・オフサイトの組合せによるリスクベースアプローチの強化

- 監督ツールの組み合わせにより、監督の有効性を強化する効果を相互に高め得る
- 監督当局は、必要に応じて、様々なアプローチの長所と短所を考慮しつつ、監督枠組みを評価し、その調整を検討すべき

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスのポイント４】

（４）低リスク先への対処

- 監督リソースは、高リスク先に対し優先配分されるべきであるが、監督戦略において、低リスク先へのアプローチも策定される必要
- 介入に値する情報を入手した場合、リアクティブに監督業務を遂行する能力を有する必要

（５）中長期的に頑健なリスクベースアプローチを発展させるための手法

- 監督戦略は、常に見直し・更新。監督業務の遂行から得られた経験を、監督戦略の実効性を高め、監督手法を継続的に改善・強化するために活用
- リスクベース監督上の意思決定に関し、独立性や評価の一貫性を確保するためのメカニズムを構築・実施

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

（参考）FATFによるリスクベース監督に関するガイダンス

【ガイダンスのポイント５】

（６）制裁の適用

- 監督当局は、一連の是正措置や制裁を利用できるべきであり、それらは、事業者のAML/CFTコントロールやリスク管理の不備の質・程度に基づき適用。
- 是正措置・制裁には、a.警告、b.アクションレター、c.命令、d.合意、e.行政処分、f.罰金、g. その他事業体の活動に対する制限・条件が含まれる
- 「ゼロ・トレランスアプローチ」の採用は避ける

（７）リスクベースアプローチの実効性の計測手法

- 監督当局は、自身の監督活動及びその結果を、適切に、記録・監視・分析すべき
- 監督当局は、自身の監督の効果を決定・証明するためにデータを活用すべき。データ活用により、監督先について特定された問題の件数・深刻度の時系列変化および統制の有効性レーティングの変化を特定できる。また、こうしたデータは、リソース配分や監督ツールの特定にも有益
- 監督上の措置の効果測定やSTR等を踏まえ、リスク評価を見直すべき
- リスクベースアプローチの有効性の透明性・アカウンタビリティを促進するメカニズムを具備すべき

（Source: The FATF Home Page/Documents/等の公表資料から筆者が作成）

(2) FATFにおけるクロスボーダー送金の改善プロジェクトについて

１．経緯

- 2020年２月、G20財務大臣・中央銀行総裁会議において、クロスボーダー送金改善を優先事項と設定。
- 2020年４月、金融安定理事会（FSB）は、クロスボーダー送金の現状把握と課題を特定（第一次報告書）
- 2020年７月、課題改善のための19の構成要素（Building Blocks（BB））を特定（第二次報告書）
- 2020年10月、各19BBのアクションプランやタイムラインを提示した工程表を公表（第三次報告書）
- ➢ **2021年までの工程表は野心的であるが、実現可能な項目を抽出しているとして、2021年以降の工程は「暫定的」としつつ、FSB傘下のCPC（クロスボーダー送金協調グループ）が全体調整・進捗管理を担う。また毎年工程表を見直し、G20への報告を予定。**

２．FATFにおける対応

- **FATFの担当は、BB5「AML/CFT規制の調和」。**
- BB5の目的は、国レベルでの異なるAML/CFTルールが、クロスボーダー送金に課題を与えている分野を特定し、必要なAML/CFT対策に妥協することなく対処すること。
- **FATFでは、コスト増、低スピード、アクセス制限、不透明性を引き起こしているAML/CFT要件について、以下の観点から調査を進め、改善案（基準改訂、ガイドライン策定等）を報告予定（2021年10月予定）。**

  ① FATF基準に基づくものの、各国が異なるルールを導入している部分

  ② FATF基準に基づかず、各国が導入している独自ルール

(Source: The FATF Home Page/Documents/の公表資料から筆者が作成)

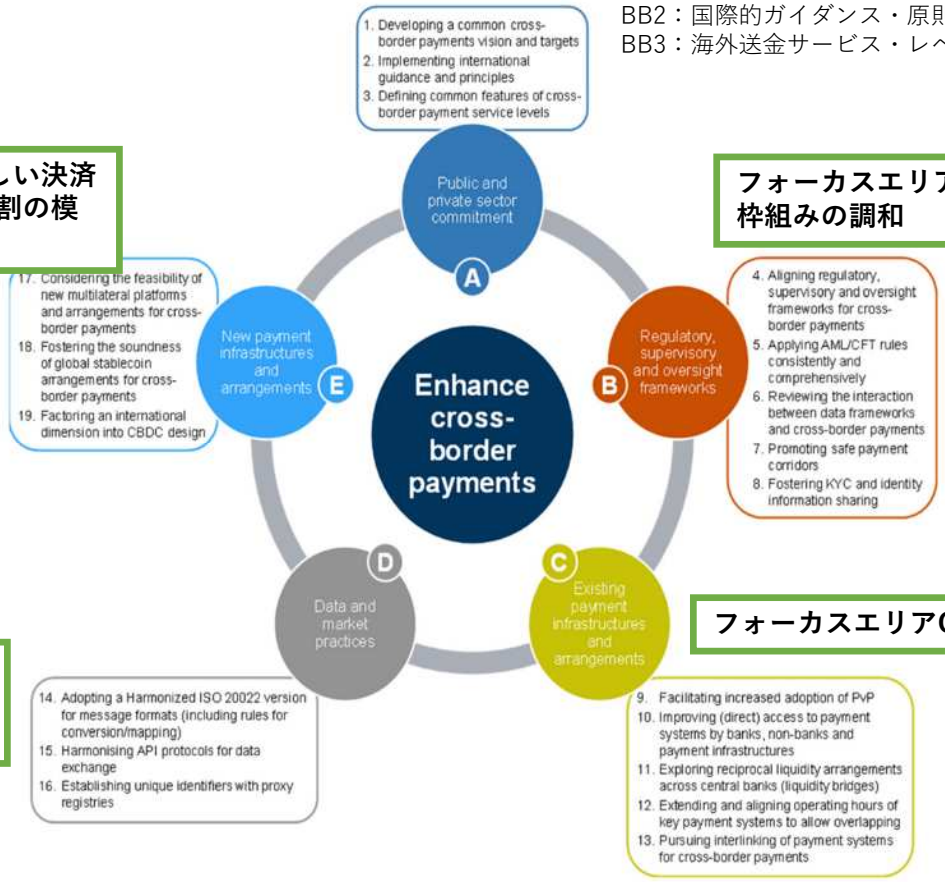
（参考）クロスボーダー送金の改善：ビルディング・ブロック［2020年7月FSB公表］

フォーカスエリアA：官民共同コミットメント構築

BB1：共通ビジョン・目標の策定
BB2：国際的ガイダンス・原則の履行
BB3：海外送金サービス・レベルの共通基準設定

フォーカスエリアE：新しい決済インフラ等の潜在的な役割の模索

BB17：新たなマルチラテラル・プラットフォームの検討
BB18：グローバルステーブルコインの健全性の育成
BB19：クロスボーダー送金に利用可能なCBDCの設計



フォーカスエリアB：規制・監督・オーバーサイト枠組みの調和

BB4：規制・監督・オーバーサイト枠組みの調整
BB5：AML/CFT規制の調和
BB6：データフレームワークの見直し
BB7：安全な送金コリドーの促進
BB8：KYC及びID情報の共有促進

フォーカスエリアC：既存の決済インフラ等の改善

BB9： PvP決済の促進
BB10：銀行・ノンバンクの決済システムへの（直接）アクセス改善
BB11：中銀間の相互的な流動性供給の模索
BB12：主要な決済システムの稼働時間延長
BB13：決済システムのインターリンクの推進

フォーカスエリアD：データの質の向上およびSTP化の促進

BB14：ISO20022の統一バージョン採用
BB15：データ交換用APIプロトコルの調和
BB16：代理レジストリを伴う固有識別子の策定

（出所）FSB「クロスボーダー送金の改善：グローバル・ロードマップの構成要素－G20向け第二次報告書」から筆者が作成

(3) AML/CFT分野におけるデジタル・トランスフォーメーションについて

1. 背　景

- FATFドイツ議長下（2020年７月～2年間）の優先課題として、 AML/CFTのデジタル・トランスフォーメーションが設定。
- 現在３つのプロジェクトが進行中。
- 当庁は①「AML/CFT分野での新技術の機会と課題」、②「データプーリング・データ分析・データ保護」の２つ※のプロジェクトチームに参画。

※　もう一つのプロジェクトは、Operational Agencies（捜査当局、FIU等）における新技術の機会と課題がテーマ。

2. プロジェクトの目的

①「AML/CFT分野での新技術の機会と課題」

⇒　官民のAML/CFT対策を効率化するための新技術の機会と課題の調査。

②「データプーリング・データ分析・データ保護」

⇒　民間セクターにおいて、データ保護を確保しつつAIやビッグデータを活用したAML/CFT規制遵守の効率性を向上

3. 成果物

FATFは、2021年7月に報告書を公表

①Opportunities and Challenges of New Technologies for AML/CFT

②Stocktake on Data Pooling, Collaborative Analytics and Data Protection

（Source: The FATF Home Page/Documents/の公表資料から筆者が作成）

① Opportunities and Challenges of New Technologies for AML/CFT

Multinational financial institutions, retail and commercial banks and internet-based firms such as Fintech take the lead when it comes to implementing new technologies.

The advantages for the private sector include:

- Better identification, understanding and management of ML/TF risks
- Process and analyse larger sets of data faster and more accurately
- Efficient digital on-boarding
- Greater auditability, accountability and overall good governance
- Reduce costs and maximise human resources to more complex areas of AML/CFT
- Improve the quality of suspicious activity report submissions

WHICH TECHNOLOGIES OFFER THE MOST POTENTIAL TO AML/CFT?

- MACHINE LEARNING
- DISTRIBUTED LEDGER TECHNOLOGY (DLT)
- NATURAL LANGUAGE PROCESSING AND SOFT COMPUTING
- Application Programming Interfaces (APIs)

(Source: The FATF Home Page/Documents/の公表資料から筆者が作成)

① Opportunities and Challenges of New Technologies for AML/CFT

MACHINE LEARNING offers the greatest advantage through its ability to learn from existing systems, reducing the need for manual input into monitoring, reducing false positives and identifying complex cases, as well as facilitating risk management.
The most useful applications of Machine Learning to AML/CFT include:

- Identification and Verification of customers through authentication AI, including biometrics, and liveness detection techniques (micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis)
- Monitoring of the business relationship and behavioural and transactional analysis by using Machine Learning algorithms to place customers with similar behaviour into cohesive groupings to monitor and alert scorings to focus on patterns of activity
- Identification and implementation of regulatory updates: Machine Learning techniques can scan and interpret big volumes of unstructured regulatory data sources on an ongoing basis to automatically identify, analyse and then shortlist it based on the institutions' requirements.
- Automated data reporting (ADR) can make granular data available in bulk to supervisors.

DISTRIBUTED LEDGER TECHNOLOGY (DLT) may improve traceability of transactions on a cross-border basis, and even global scale, making identity verification easier.
It may speed up the customer due diligence process, as consumers can authenticate themselves. They can even be automatically approved or denied through smart contracts that verify the data. DLT continue to pose challenges from an AML/CFT perspective as they are decentralized in nature and enable un-intermediated peer-to-peer transactions without any scrutiny.

（Source: The FATF Home Page/Documents/の公表資料から筆者が作成）

① Opportunities and Challenges of New Technologies for AML/CFT

NATURAL LANGUAGE PROCESSING AND SOFT COMPUTING TECHNIQUES simulates human decision-making, as a result, it can take incomplete, ambiguous, distorted, or inaccurate (fuzzy) input and produce useful outputs.

Like with all technological solutions, when they are integrated with broader monitoring systems, they should include an element of human analysis for specific alerts or areas of higher risk.

(注）自然言語処理（Natural Language Processing）とは、人間の言語（自然言語）を機械で処理し、内容を抽出する技術。一般的には、言語表記などの非構造データを、形態素解析、構文解析、意味解析、文脈解析などの処理工程を経て解析する手法。「Soft Computing Techniquesとは、ファジィ理論、ニューロコンピューティング、確率推論、カオス理論、学習理論、、知識工学などを包括し，扱いやすさ，頑健性，低コストを達成させるために寛容性の概念に基づいて，不正確性，不確実性をどこまで許容できるかを探り，問題の解決を計る新しい情報処理様式 (Lotf A. Zadeh 1991)」

Application Programming Interfaces (APIs) connect customer identification software with monitoring tools, or risk and threats identification tools with customer risk profiles. An API will generate alerts or alter risk classifications as relevant.

This can:

- Improve the interoperability between traditional banking data, moving away from siloed systems with fragmented frameworks.
- Increase automation and optimise resources and output accuracy.
- Supply an aggregated and normalized data feed, helping to build a more complete risk profile for new customers.

（Source: The FATF Home Page/Documents/の公表資料から筆者が作成）

② Stocktake on Data Pooling, Collaborative Analytics and Data Protection

- **Technology has the potential to make efforts to combat money laundering and terrorist financing faster, cheaper, and more efficient** in the ways such as; to facilitate data sharing and collaborative analysis, and help financial institutions analyse large amounts of data more efficiently and identify patterns and trends more effectively.

- **A primary reason to share or pool data is to monitor transactions.** Sharing data could also facilitate customer due diligence measures, such as institutional risk assessment, On-boarding customers, risk management of a business relationship, and identification of the beneficial owner. It can help identify and share patterns and flows, such as the identification of typologies of crime and intelligence-driven investigations.

- **An open dialogue between financial institutions AML/CFT supervisors and DPP authorities is important** to the success of initiatives using new technologies and their ultimate effective implementation. In addition, regulatory sandboxes (or innovation hubs) provide valuable opportunities to test how new technologies interact with national (or supranational) AML/CFT and DPP laws and regulations.

- **New and emerging privacy-enhancing technologies offer promising ways for private sector** collaboration while protecting information in specific use cases and in line with national and international data protection and privacy (DPP) frameworks.

(Source: The FATF Home Page/Documents/の公表資料から筆者が作成)

② Stocktake on Data Pooling, Collaborative Analytics and Data Protection - Japan's POC on Machine Learning

"Box 4.2. Japan's Proof of Concept on Machine Learning and Artificial Intelligence"

In order to facilitate data sharing consistent with DPP regulations, Japan has developed a unique proof of concept (POC) project, which includes participation from several Japanese FIs, supported by the Japan Financial Services Agency and sponsored by the New Energy and Industrial Technology Development Organisation.

This project integrates AI algorithms with instructions from each FI transaction dataset, **without sharing or pooling the data, resulting in a single AI model.** This POC aims to build an AI model to facilitate human judgement by calculating the likelihood of a true positive score for transaction monitoring and sanctions screening.

In this POC, the transaction data of individual FIs were not shared or pooled, but rather took the following two approaches:

(1) integrating the AI models themselves that learned each institutions' dataset; and
(2) tuning the AI model that had already learned the dataset of one institution to relearns another bank and continued this process to improve the accuracy of this AI model.

According to the results of this project, the Shared Transaction Monitoring and Screening System with AI has **enough potential to reduce workload, including the triage process of the detections and dealing with false positives.**

In terms of accuracy and interpretability, the results indicate that some human operations at the conventional triage process can be replaced by AI-powered judgement. If this initiative spreads to a wider range of financial industry participants, it could improve the efficiency and effectiveness of AML/CFT as a whole.

(Source: The FATF documents "STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION July 2021", FATF, "Box 4.2. Japan's Proof of Concept on Machine Learning and Artificial Intelligence")