金融財政事情研究会 「ニューバンキングセミナー」 講演資料

金融庁におけるモニタリングの方向性と期待される内部監査について

～「顧客本位の業務運営」と「サイバーセキュリティ強化」に向けて～

令和４年12月１日

金　融　庁

目次

2022事務年度　金融行政方針（2022年８月公表）

Ⅰ．経済や国民生活の安定を支え、その後の成長へと繋ぐ

- **資金繰りや経営改善・事業転換・事業再生等の事業者に寄り添った支援**を、金融機関に対して促す。
- **事業者支援能力の向上**に向け、地域金融機関のノウハウ共有や経営人材マッチングの促進などを行う。
- **経営者保証に依存しない融資慣行の確立や、事業全体に対する担保権の早期制度化**に取り組む。
- **金融機関の経営基盤の強化と健全性の確保**に向け、ガバナンスの強化や、与信・有価証券運用・外貨流動性に関するリスク管理態勢の強化を促す。
- **利用者目線に立った金融サービスの普及**に向け、複雑な金融商品の取扱いを含め、金融商品の組成・販売・管理等に関する態勢整備を促す。
- **マネロン対策等やサイバーセキュリティ、システムリスク管理態勢の強化**に向け、世界情勢等を踏まえた対応を促す。

Ⅱ．社会課題解決による新たな成長が国民に還元される金融システムを構築する

- **国民の安定的な資産形成**のため、「資産所得倍増プラン」の策定も踏まえ、 NISAの抜本的拡充や国民の金融リテラシーの向上、金融事業者による顧客本位の業務運営の確保に取り組む。
- **スタートアップなど成長企業に対する円滑な資金供給**を促すため、資本市場の機能強化に取り組む。
- **企業情報の開示**について、人的資本を含む非財務情報の充実や四半期開示の見直しに取り組む。
- **サステナブルファイナンスを推進**するため、企業と金融機関が対話をするためのガイドラインの策定やインパクト投資の促進等に取り組む。特に気候変動については、トランジションファイナンス推進のための環境整備を進める。
- **デジタル社会の実現**に向け、Web3.0やメタバース等の発展に向けた動きを金融面から推進する。
- **国際金融センターの発展**に向け、海外資産運用業者等の参入促進に向けた環境整備に引き続き取り組む。

Ⅲ. 金融行政をさらに進化させる

- **金融行政の組織力向上**のため、職員の専門性向上を図るとともに、データ活用の高度化による多面的な実態把握を推進する。
- **国内外への政策発信力の強化**のため、国際的ネットワークの強化を図るとともに、タイムリーで効果的・効率的な情報発信に取り組む。

Ⅰ．顧客本位の業務運営について

（１）顧客本位の業務運営の全体像

国民の安定的な資産形成

■ 国民が安定的な資産形成を行うためには、金融商品の販売、助言、商品開発、資産管理、運用等を行う金融事業者による顧客本位の業務運営を確保することが重要。

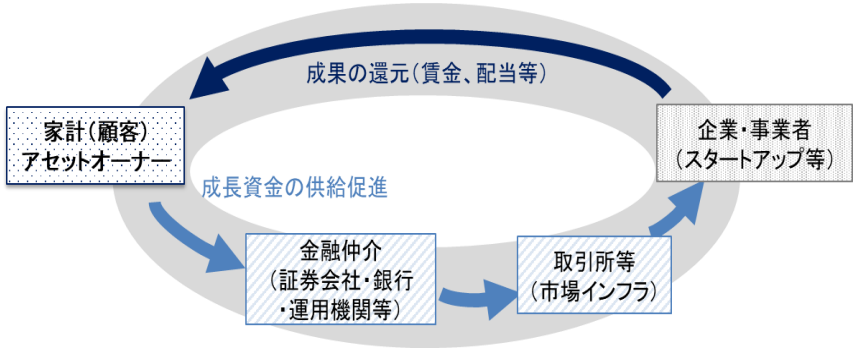
◆ 課題

- ✓ **販売会社**：リスクが分かりにくく、コストが合理的でない可能性のある商品を十分な説明なく推奨・販売
  ※仕組債
- ✓ **アセットオーナー**：運用の専門家の活用不足や運用機関の選定プロセス
- ✓ **資産運用業**：顧客の利益より販売促進を優先した金融商品の組成・管理
  ※ESG投信

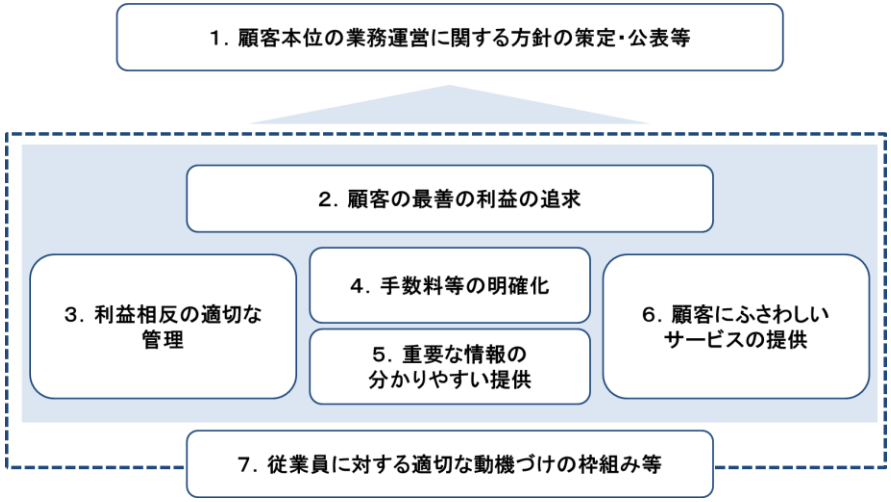
◆ 対応

- ✓ 顧客や受益者の利益を第一に考えた立場からの業務運営を求めるための制度のあり方について検討

成長資金の供給促進と成果の還元

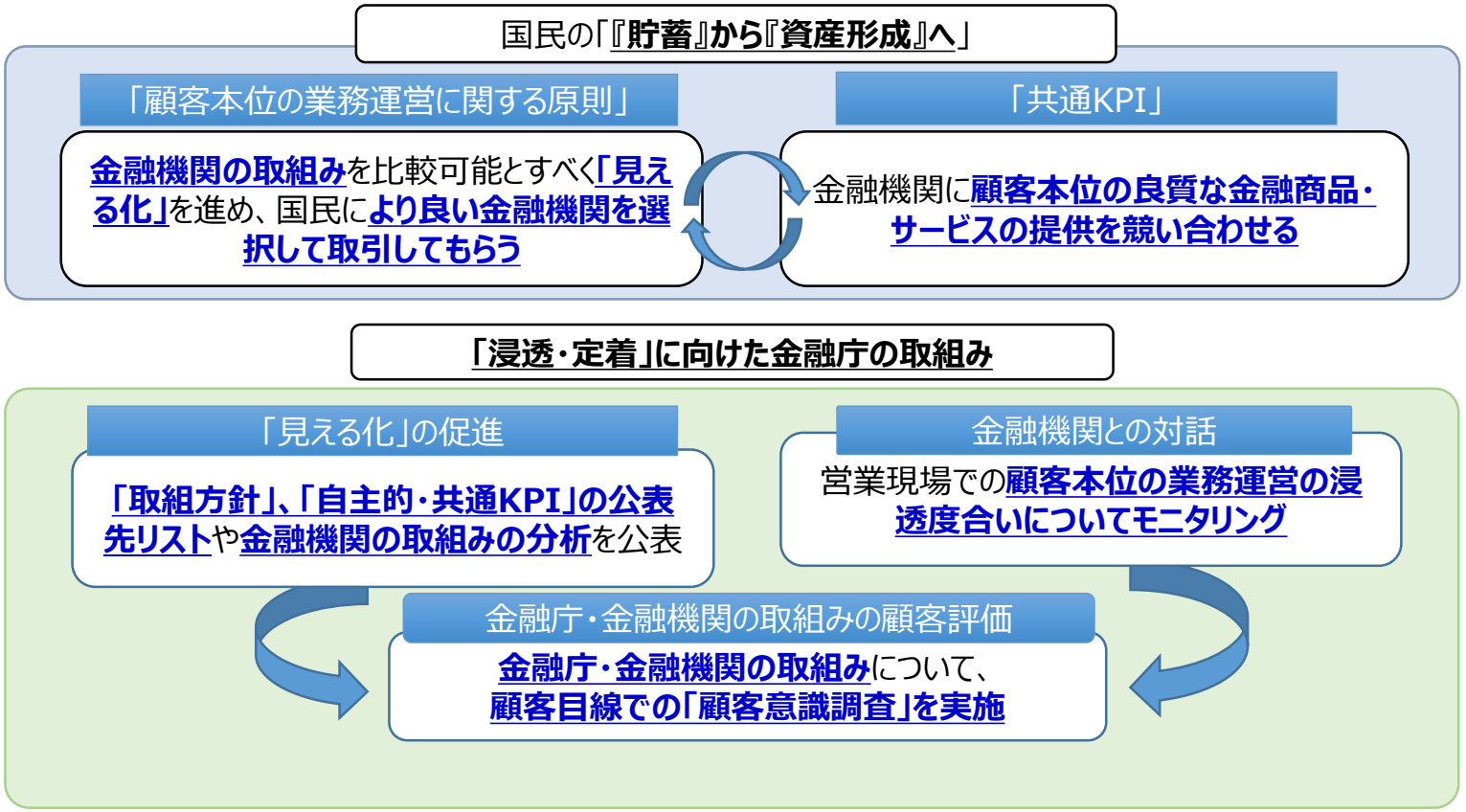


顧客本位の業務運営に関する原則



顧客本位の業務運営に係る取組みの全体像

- 安定的な資産形成には、長期・積立・分散投資が有効。これを実現するには、資産形成に適した金融商品・サービスを顧客の立場に立って提供する金融事業者を選択し、長期にわたり取り組んでいくことが重要。
- 金融事業者が顧客本位の良質な金融商品・サービスの提供を競い合うように促すべく、 2017年に「顧客本位の業務運営に関する原則」を策定し、「原則」を採択した各金融事業者の取組みの「見える化」を促進してきた。



「顧客本位の業務運営」の出発点

➢ 森元長官「日本の資産運用業界への期待」（2017年4月7日）から抜粋

- 金融庁としても、こうした決して最適とは言えない 均衡からの脱却をこれまで実現できなかったことを 、 大いに反省しなければなりません。金融庁発足以来、投資家保護は金融行政の中核に位置づけられ、・・・（中略）・・・形式的な面は改善しましたが、ビジネスの本質が顧客本位に変わったとはいえません。

- 顧客が適切な選択を行なうための条件さえ整えれば、みせかけでなく真に顧客のニーズに資する商品・サービスを提供する業者が発展するのが、業種や洋の東西を問わず成り立つ原則だと思います。安くて美味しいレストランは賑わい、まずくて高い店は淘汰されています。金融商品は、その真の価値やコストが分かりにくいですが、「見える化」への努力を行なっていく必要があります。例えば知らない土地に行ってレストランを選ぶときも、ミシュラン、ザガットや各種ウェブサイトが、良いレストランについての情報を提供してくれます。投資商品についても、同様のインフラが作られることが望ましいと考えます。

- 金融リテラシーの問題もあります。金融商品は、食事よりも 嗜好による個人差が少ないので、 各人の年齢、資産、収入などをもとに、いかなる投資や資産分散が望ましいかについての知識を持つことは、個々人が自らにあった商品・サービスを見分ける能力を向上させると思っています。 高い運用力を持つ金融機関、顧客 本位が組織に根付いた金融機関が発展し、 顧客本位を口で言うだけで具体的な行動につなげられない 金融機関が淘汰されていく市場メカニズムが 有効に 働くような環境を作っていくことが、我々の責務であり、そのため行政として最大限の努力をしていくつもりです。

Ⅰ．顧客本位の業務運営について

（２）モニタリング結果を踏まえた課題

現状認識：顧客による選択のメカニズムの実現

１．全体のポイント

（出典）令和4年版レポート

■　本資料の目的

・投資信託等の販売会社による顧客本位の業務運営に関して、主要な販売会社等における実践状況や取組方針等の開示状況等に係るモニタリング結果を整理したもの。

■　モニタリング対象先

・リスク性金融商品の預り資産残高が多い販売会社を中心に選定（主要行等10行、地域銀行26行、証券会社12社など）

■　ポイント

✓　販売会社の中には、顧客セグメントを意識した経営戦略に基づく創意工夫を実践している先がある。こうした一部の販売会社に対する顧客による選択のメカニズムは実現し始めている。

✓　一方で、販売態勢面での実践や取組方針等の「見える化」に課題が残っている販売会社も多い。背景には、顧客本位の業務運営を経営課題として取り組んでいないことが影響している可能性。

✓　仕組債のように、中長期的な資産形成を目指す一般的な顧客ニーズに即しているとは考えにくい商品・サービスが、限定した顧客に絞って販売する態勢が整っていないなど、経営レベルでの検討が必要。

２．今後のモニタリング等において重要な点について　（全体版６章参照）

■　来事務年度においては、次の観点を踏まえてモニタリング・対話等を行う。

✓　経営陣が長期的に持続可能な経営戦略を検討し、取組方針において明確化・具体化しているか。

✓　経営戦略に沿った取組が営業現場に定着し、成果が出ているか。

✓　３線管理の中で、自らのビジネスモデルの有効性や適切性を検証する態勢が取られているか。

✓　金融庁による苦情やデータの分析を踏まえたモニタリング

現状認識：対面金融機関の工夫と課題

（出典）令和4年版レポート

3．リスク性金融商品販売等にかかるビジネス概要　（全体版２章参照）

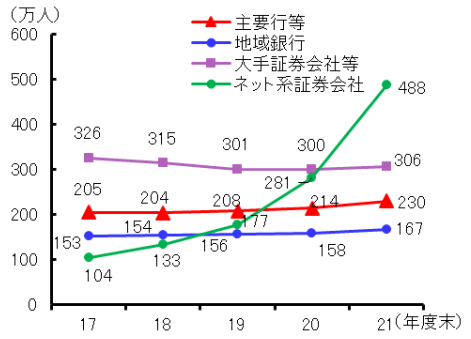
■ 経営戦略・ビジネスモデル転換等に伴う実績

- ✓ 投資信託の保有顧客数の増加など、貯蓄から資産形成への意識は一定程度広がっている。
- ✓ 販売会社の経営戦略は、①顧客セグメント毎のアプローチ明確化、②フローからストックへの転換、③銀証連携の動きが一段と明確化
- ✓ ネット系証券は低コストに基づく若年層の取り込みに奏功し、保有顧客数は顕著に増加

■ 各業態が目指す経営戦略の実現に向けた課題

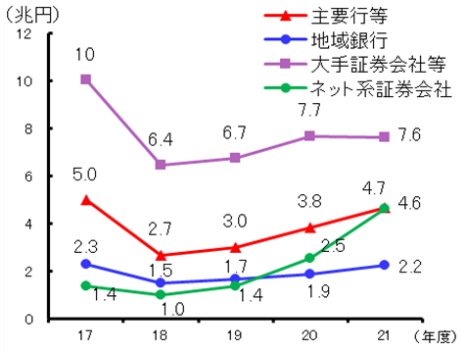
- ✓ 銀行：対面の特性を活かした経営戦略の一段の具体化・銀証連携に伴う課題への対応
- ✓ 大手証券会社：ストック収益に基づくビジネスモデルの一段の実践
- ✓ ネット系証券会社：情報提供面での工夫を通じた顧客利便性の一段の向上

【 投資信託の保有顧客数の推移 】



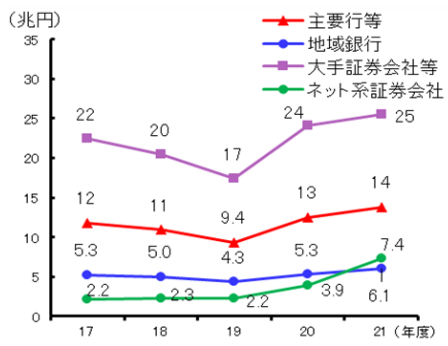
（注１）有効回答が得られた主要行等８行、地域銀行22行、大手証券会社等８社（20年度以降は経営統合により７社）、ネット系証券会社５社を集計
（注２）銀行の投資信託は、自行販売ベース
（注３）対象は、年度末時点で残高のある個人顧客
（資料）金融庁

【 投資信託の販売額の推移 】



（注１）有効回答が得られた主要行等８行、地域銀行25行、大手証券会社等８社（20年度以降は経営統合により７社）、ネット系証券会社５社を集計
（注２）銀行は、自行販売、仲介販売、紹介販売の合算ベース
（資料）金融庁

【 投資信託の預り資産残高の推移 】



（注１）有効回答が得られた主要行等８行、地域銀行24行、大手証券会社等８社（20年度以降は経営統合により７社）、ネット系証券会社５社を集計
（注２）銀行にて販売した商品は、自行販売、仲介販売の合算ベース
（資料）金融庁

投資信託等の販売会社による仕組み作り

▼ビジネスモデル構築に向けた取組み例

１．低めの手数料･大量提供

(1)広範な利用者層へネット経由で幅広い金融商品提供

- ネット系証券：口座数は著増し、積立も一定増。ノーロード化による若年層の取り込みを優先。

(2)主に資産形成層のニーズに即した商品・サービス提供

- ロボアドバイザー：ロボアドと共に投信対象を絞って提供。
- 対面の金融機関の一部：積立投信ノーロード化／土日相談。

２．高付加価値の提供(サービスの差別化)

(1)クロスセル等

- 主要行グループ：対面での富裕層対応に力点。資産形成層へはDXで対応。
- 2世代承継を想定して、各種のサービスを提供。

(2)問題解決型アドバイス（アドバイス対象を金融資産に留めない）

- 大手証券：預り資産管理に軸足を移すなか、問題解決型ビジネスモデルを指向。
- 個人向け投資助言会社を設立。アドバイスを時間ベースで提供。

(3)投資理念に基づく「長期的関係」の構築

- 直販中心：個性ある投信を絞って提供。

(４)地銀と証券会社との提携

- 業務提携、コンサル合弁会社

（参考）令和3年版レポート24頁

仕組債の課題

① 商品性の課題

- ✓ 一般的な債券と異なり、当初予定の満期時に元本で償還される可能性が必ずしも高くない
- ✓ デリバティブの知識がないと損失の見極めができず、リスクに見合ったリターンの理解がしにくい

  ⇒ 最近の市況の変動により顕在化

② 販売体制の課題

- ✓ 顧客が実質的に負担するコストが十分に開示されていない
- ✓ 顧客の「最善の利益」に資するための、真のニーズに応じた販売が行われていない可能性が高い

③ 経営陣の課題

- ✓ 仕組債を販売する金融機関の経営陣が、上記のような課題について十分に認識していなかった

仕組債に関して寄せられた苦情

相談・苦情件数

仕組債の相談・苦情件数（A）

	2019年度		2020年度		2021年度	
		（A）／（B）		（A）／（B）		（A）／（B）
相談	446	58.2%	272	46.6%	189	50.7%
苦情	226	72.9%	189	67.5%	152	61.5%
相談・苦情計	**672**	**62.5%**	**461**	**53.4%**	**341**	**55.0%**

債券の相談・苦情件数（B）

2019年度	2020年度	2021年度
766	584	373
310	280	247
1,076	864	620

（出所）日本証券業協会ホームページ「（証券・金融商品あっせん相談センター（FINMAC））あっせん、苦情、相談処理状況について（年度毎）」

紛争事例

	紛争概要（申立人の主張）	紛争解決委員の見解
①	証券会社担当者は、商品性等について詳しい説明を行うことなく、申立人に期限前償還条項付き仕組債の勧誘を行い、次々と購入させた。市況の悪化により大きな損失を被った。（60代前半女性）	家族全体の預り資産の合計の約８割を仕組債が占めていることは、適合性の観点からみて配慮が欠けていたものと考える。
②	証券会社担当者から仕組債の買付を勧誘され、詳しい説明を受けることなく商品性等を理解できないまま購入し、市況の悪化により大きな損害を被った。（80代前半男性）	申立人が承諾の上、ブラジルレアルを参照通貨とした仕組債を購入しているが、申立人は高齢であり、償還期限が10年であることや、いったんは購入を断っていることを踏まえると、被申立人には配慮が必要であった。

（出所）FINMAC紛争解決手続事例（2021年10～12月、2022年1月～3月）を元に作成。

他のリスク性金融商品の検証

➢「業界団体との意見交換会において金融庁が提起した主な論点」（令和４年９月）

４.安定的な資産形成を目指す顧客に相応しくない商品の販売について

○ 『金融行政方針』にも記載したが、一般の利用者から、安定的な資産形成を目指す顧客にはふさわしくない商品を金融機関が提案・販売しているといった相談が金融庁に寄せられている。

○ 各金融機関から提出のあったデータからも実質手数料が不透明で、顧客による適切な投資判断が困難な商品が相当程度販売されていることを確認している。

○ こうしたことは、多くの金融機関において、自らの取組方針の中で、「顧客に最善の商品の提案」や「手数料の透明化」を掲げている点と矛盾している。こうした取組方針の記述が、実際の商品の販売や手数料の開示状況と整合的なのか、金融機関において自発的に確認しているかを重点的に検証する。

○ （中略）なお、リスク性商品を幅広く取り扱っている先については、商品間の相対的な評価が課題となる。取組方針の中で、「顧客に最善の商品の提案」や「利益相反の管理」と述べている以上、当然、商品ラインナップについて相応の選別がなされ、販売の際に利益相反が起きないような態勢が構築されるべきであり、この点について重点的に検証する。

○ 最後に、こうした取組方針の実践状況の管理検証にあたっては、本部リテール部門などの第１線の現場任せにせず、経営陣や２線・３線が、その進捗状況を管理検証する態勢の構築が必要である。

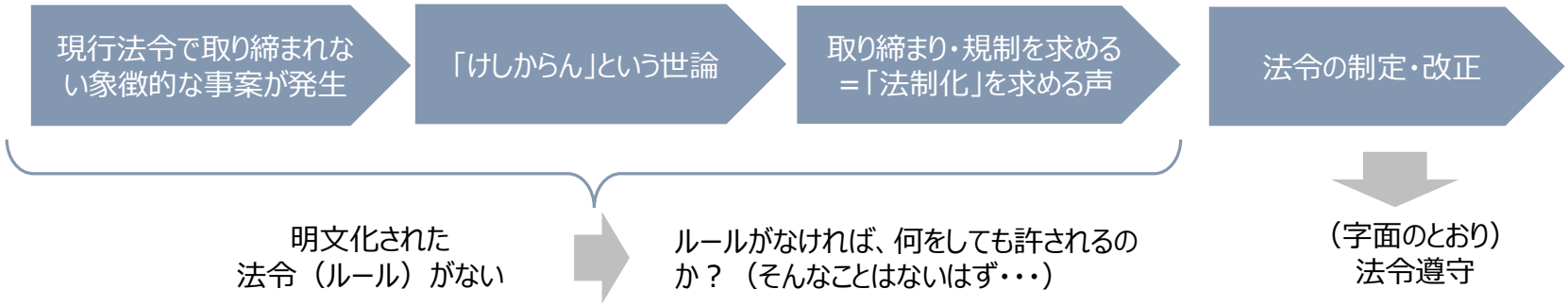
○ 現在、仕組債が問題と認識しているが、以上で挙げた問題と同様の課題は、仕組債以外の既存の商品や、今後現れる新たな商品でもありうる。金融庁が問題視した特定分野についてのみ受動的に後から対応するのではなく、むしろ金融庁に先んじて自発的に改善を図っていただきたい。

コンダクト（コンプライアンス）リスク管理の重要性

● 法令制定に至らない「社会規範」をより重要視する必要。

- 社会や時代の変化に伴い、法令制定当時に想定していなかった事象は往々にして発生。想定していなかったが故に、法令に条文として書かれていない。**結局、法令は、事案が発生する度に後追いで追加・改正されることが多い。**
- 遵守すべき法令がないことをもって、**①社会規範に悖る行為、②商慣習や市場慣行に反する行為、③利用者の視点の欠如した行為等といった社会的要請に背く行為**をとることは、信用毀損や財務的負担が生じ得るリスクとなる。

＜法令（ルール）化に至る一つのプロセス＞

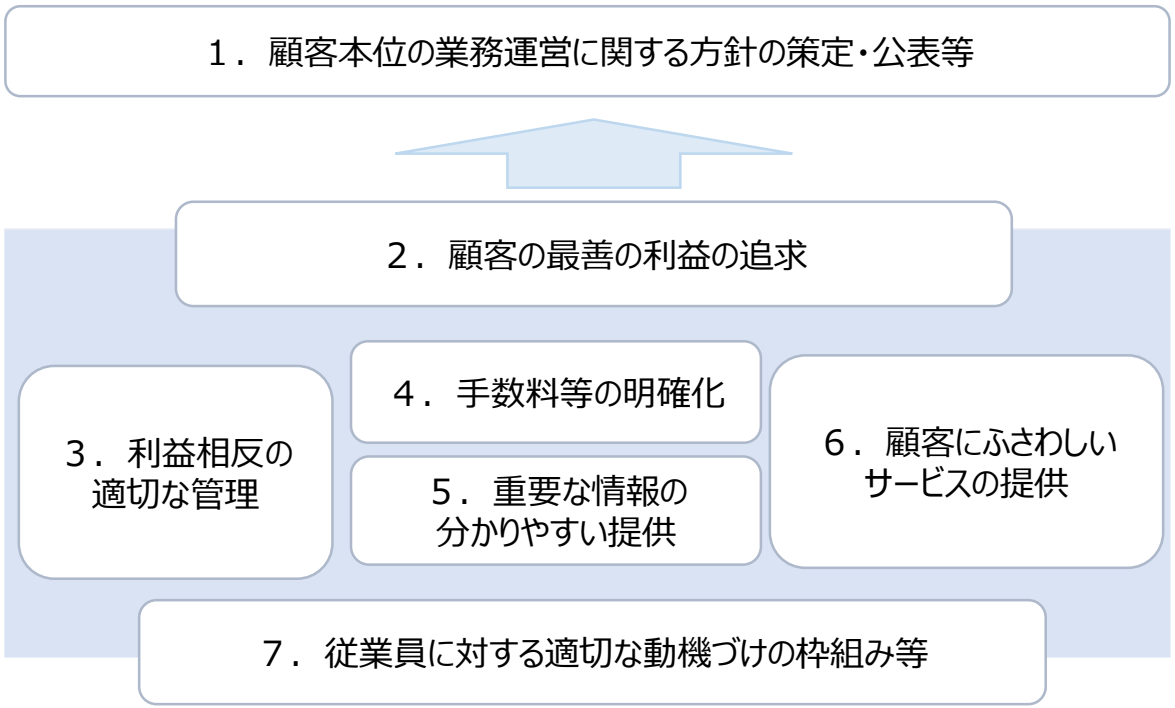


Ⅰ．顧客本位の業務運営について

（３）　顧客本位の業務運営の「見える化」

「顧客本位の業務運営に関する原則」と「見える化」

- 金融事業者は本原則を採択し、その取組みの「見える化」により、顧客がより良い金融商品・サービスを選択するメカニズムの実現を図る（プリンシプルベースのアプローチ）
- ベスト・プラクティスを目指す上で有用と考えられる原則として、金融事業者において幅広く採択されることを期待



顧客本位定着のための「見える化」

誰に「見える化」？
①顧客
②営業担当者
③経営陣
④金融監督当局

どの場面で「見える化」？
①営業現場（顧客―営業担当者）
②営業担当者と経営陣の対話
③組織の仕組み作り
④金融当局と事業者の対話

現状認識：不十分な「見える化」の活用

（出典）令和4年版レポート

５．取組の「見える化」や情報発信等の現状と課題　（全体版４章参照）

（1）「金融審議会 市場ワーキング・グループ」報告書を踏まえた金融庁の対応

① 「顧客本位の業務運営に関する原則」に示されている内容ごとに対応した取組方針等を示していることが確認できた金融事業者を「金融事業者リスト」として公表（年４回）　総数：1,164 者

② 金融事業者の取組方針等に係る比較分析　・・・ (3) 金融庁による取組方針等の比較分析と課題に記載

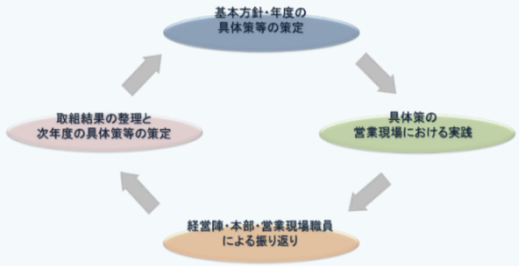
（2）金融庁による金融事業者の取組方針等の好事例の考え方

金融事業者には、以下の観点から取組方針等の記載内容に係る検証を通じて、経営陣から営業職員までが顧客に向き合う姿勢を考える契機とすることを期待

・顧客が金融事業者を選択するに当たり、分かりやすく有用な情報が示されているか。

・「原則」の趣旨・精神を自ら咀嚼した取組内容や、営業員をはじめとする従業員が、「原則」を実践するためにどのような行動をとるべきかが具体的に示されているか。

また、策定 → 実践 → 振り返り → 次年度の取組の検討といったサイクルによる定期的な見直しを期待



（3）金融庁による取組方針等の比較分析と課題

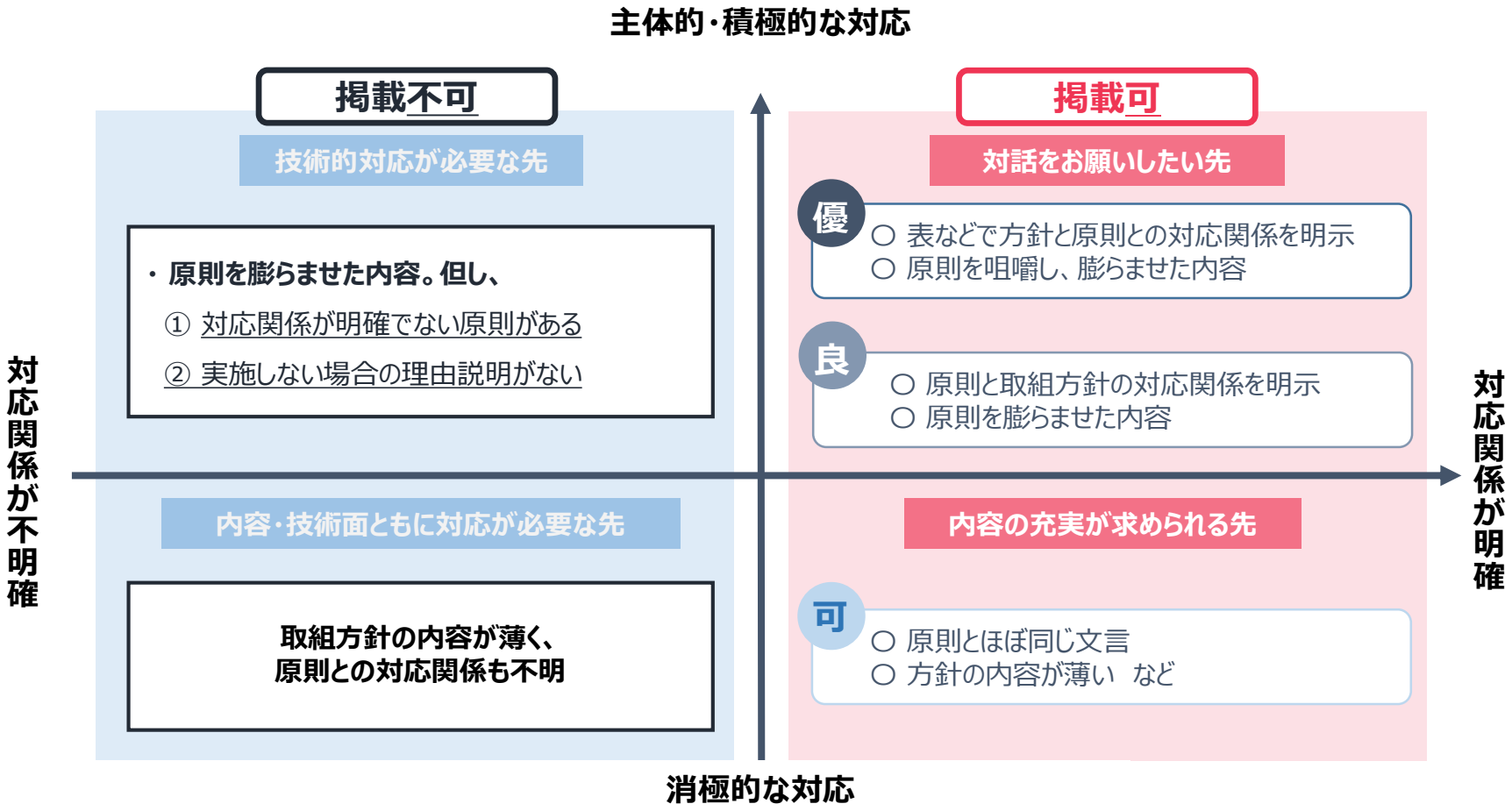
主に銀行の取組方針等について、原則２～７の項目ごとに比較分析。引き続き、具体性に欠けるなどの多くの課題が認められたため、工夫事例や期待されるレベル感を提示

（4）金融庁による一般向けの情報発信

引き続き、様々な媒体を活用し、情報発信することが重要

事業者リストの考え方

- 金融庁は金融事業者の取組方針等を本原則の項目ごとに比較できる金融事業者リストを公表
- リスト掲載に当たっては、顧客に有用な情報が提示されていることを前提とした上で、金融庁への報告が必要。令和４年より、取組方針に基づく実践結果の報告が必要



「見える化」における課題

➢ 「業界団体との意見交換会において金融庁が提起した主な論点」（令和４年９月）

３.顧客本位の業務運営に関する「金融事業者リスト」の公表について

○ （略）、金融事業者リストは、より良い取組みを行う金融事業者が顧客から選択されるメカニズムの実現を目指す観点から、原則を採択の上、原則との対応関係を明らかにした取組方針を策定し、それに基づいた取組状況を公表した金融事業者の報告を取りまとめ、９月９日に公表。

○ 一方、金融事業者からの報告や公表内容を確認したところ、原則の文言を形式的になぞるだけで「自らの取組方針とそれに対応した取組状況が十分に示されていない事例」や「取組状況を踏まえた取組方針の見直しが行われていない事例」が認められるなど、顧客本位の業務運営の重要性や「見える化」の趣旨が十分に理解されていないことが窺われた。

○ 実際、７～８月に、地域銀行との間で意見交換を行ったところ、

- 多くの先において、中期経営計画のリテールビジネス戦略と取組方針等とが整合的でない、
- ７割の先において、顧客の意見を補完し得る社外取締役を交えた議論が行われていない、
- 取組方針の内容が十分でないにも関わらず、原則と対応させるのみで十分な見直しを行っていない先も依然として少なくない。

○ 金融事業者が顧客本位の業務運営の「見える化」に取り組むことは、

- 自らの取組みの差別化を示すことができるなど、顧客を含む様々なステークホルダーに対するＰＲになる、
- 経営陣が営業職員の顧客に向き合う姿勢を検証できる、
- 営業職員が日頃の営業姿勢を見直す良い契機にもなる

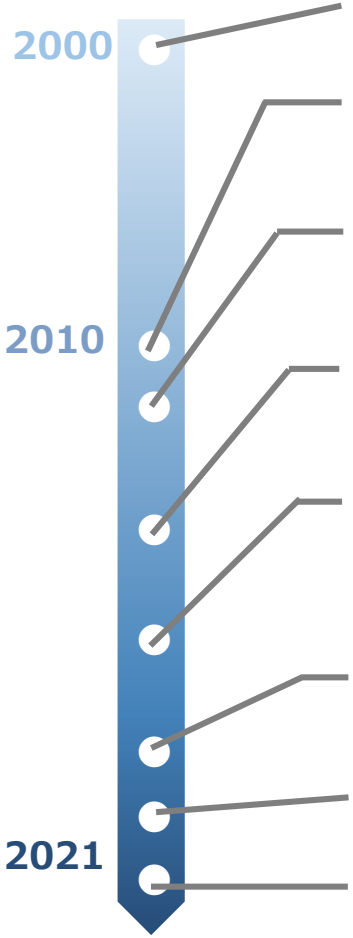
と考えられ、各社においては、その趣旨を理解の上、経営陣の十分な関与の下で、しっかりとご対応いただきたい。

Ⅱ．サイバーセキュリティについて

（１）サイバー攻撃の脅威の動向

近年の国内外の主要なサイバー攻撃

サイバー攻撃は巧妙化し、その被害は多岐に渡り（業務妨害、重要情報の窃取、金銭の獲得など）、その脅威は増大している。



2000.1　日本官公庁ウェブサイト改ざん事案
科学技術庁（当時）を始め、複数の中央省庁などのウェブサイトが改ざんされた。

2010.1　オーロラ作戦(Operation “Aurora”）の発覚
中国が関与していると疑われるハッキンググループによるInternet Explorerの脆弱性を突いたマルウェア攻撃。
金融、テクノロジ、メディア、化学など様々な分野の大企業から知的財産などを窃取した。

2010.11　イラン マルウェア「Stuxnet」による核関連施設攻撃の発覚
イランのウラン濃縮施設にある閉域ネットワーク内の遠心分離機が、USBストレージ経由にてマルウェア「Stuxnet」に感染。秘密裏に誤作動し、約1,000台が物理的に破壊された。

2016.2　バングラデシュ中央銀行における不正送金事案
バングラデシュ中央銀行が不正アクセスを受け、SWIFTシステムを通じて不正送金が行われた。
被害額は約8,100万ドル。

2017.5　ランサムウェア「WannaCry」事案
感染端末がネットワークに接続された他の端末にも感染を広げる自己増殖型のマルウェア。
日本を含む約150か国の政府機関、医療機関、企業等がデータを暗号化され身代金を要求された。

2018.1　暗号資産交換業者における不正出金事案
コインチェックが不正アクセスを受け、暗号資産NEM（約580億円相当）が不正送金された。

2020.12 大規模サプライチェーン攻撃
SolarWinds社製IT管理・監視ツール「Orion」の更新プログラムを悪用した大規模な攻撃。

2021.5　コロニアルパイプラインへのランサムウェア攻撃
コロニアルパプラインの業務全体が一時停止（５日間）し、多くのガソリンスタンドでガソリン不足が発生。

※各報道情報をもとに金融庁作成

近年の国内金融分野のサイバー脅威の動向

年月	会社名	概要	
2020/7	証券会社	顧客情報の漏洩 （氏名・生年月日・住所等）	✓ 顧客情報管理システムへの不正アクセス ✓ 個人情報4千名分が漏洩 ※運転免許証、個人番号カード等の画像データも一部流出
2020/8	商品先物業者	顧客情報の漏洩 （氏名・住所・銀行口座情報、パスワード等）	✓ Webサイトへの不正アクセス ✓ オンライントレード口座開設時の入力情報約3千件が漏洩
2020/9	証券会社	不正出金	✓ 何らかの方法で取得したログイン情報を利用してアクセス ✓ 偽装本人確認書類で作成した銀行口座を出金先に変更し、不正に出金 ✓ 被害総額は約１億円
2020/9	資金移動業者	不正出金	✓ キャッシュレス決済サービスにおける本人認証設計の不備によって不正に預貯金が引き出される ✓ 被害総額は約３千万円
2020/10	保険代理店	顧客情報の漏洩 （氏名・生年月日・住所等）	✓ データ管理システムへの不正アクセス ✓ 攻撃を受けた個人データの総数は９万件
2020/11	暗号資産交換業者	顧客情報の漏洩 （電子メールアドレス、氏名、暗号化されたパスワード等）	✓ ドメイン登録サービスに登録した情報が不正に変更されたことによる、システム・インフラへの不正アクセス ✓ 約17万件の情報が漏洩。（他に身分証明書等の本人確認書類約３万件も漏洩した可能性あり）
2020/12～	資金移動業者 銀行等	顧客情報の漏洩 （氏名・住所・電話番号等）	✓ クラウドサービスの設定不備による不正アクセス ✓ 地方自治体及び一般事業者でも発生
2021/4	証券会社	オンライン取引停止	✓ オンライントレードシステムへの不正アクセス ✓ データを暗号化され、現行システムの復旧を断念
2021/11	信用組合	HP一時利用不能	✓ サイバー攻撃により、HPの閲覧とHP経由のオンラインバンキングが利用不可
2021/12	信用金庫	HP改ざん	✓ HP改ざんにより、HPの閲覧とHP経由のオンラインバンキングが利用不可
2021/11～	保険会社	個人情報の漏洩・不正出金	✓ フィッシングサイトへ誘導する不審メールが複数の保険会社で発見 ✓ 偽装口座を使用した不正出金被害も発生
2022/8～	銀行等	不正出金	✓ フィッシングによるものとみられるインターネットバンキングに係る不正出金被害が急増

※各報道情報をもとに金融庁作成

情報処理推進機構（IPA）「情報セキュリティ10大脅威」（2022年1月）

- **組織に対する情報セキュリティへの脅威として、昨年に引き続き「ランサムウェアによる被害」が1位**
- **サプライチェーンの弱点を悪用した攻撃も昨年4位⇒今年3位と注目度が高い**

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威」 https://www.ipa.go.jp/security/vuln/10threats2022.html

事例紹介①：ランサムウェア攻撃
～コロニアルパイプラインへのランサムウェア攻撃（2021年5月）～

【コロニアルパイプラインとは】

米国最大の石油パイプラインの運営会社。テキサス州ヒューストンからニューヨーク港まで約8,800キロのパイプラインを運営（東海岸の対象地域で消費される45%の燃料を提供）

【主要な被害】

コロニアルパイプラインの業務全体が一時停止（５日間）し、多くのガソリンスタンドでガソリン不足が発生するなど、国民生活にも影響

【時系列】

5月7日(金)	• ランサムウェアによる影響をうけ業務全体を一時停止すると発表（予防措置としてパイプライン全停止）
5月10日(月)	• FBIがDarkSideと呼称されるランサムウェアギャングが今回の犯行に使われたと声明を発表 • 米大統領が、ロシア政府の関与はないが、ロシア拠点のグループが攻撃したと発言
5月13日(木)	• BloombergがColonial Pipeline社が身代金（500万ドル相当の暗号資産）を支払ったと報道 • セキュリティ研究者らが、DarkSideは米国からの圧力を理由にRaaSプログラムの活動を停止したと報告

【ランサムウェアの脅迫方法の高度化】

第1段階（従来の攻撃）：**データを暗号化**したうえ、（ビットコインなどでの）**身代金支払いを要求**（支払わないと復号鍵を渡さない）
第2段階（二重脅迫）：窃取した**機密情報を暴露すると脅す**
第3段階（三重脅迫）：**DDoS攻撃を行うと脅迫する**
第4段階（四重脅迫）：攻撃対象の企業の**顧客に連絡し、（漏洩データを公開するなどと）更に脅す**

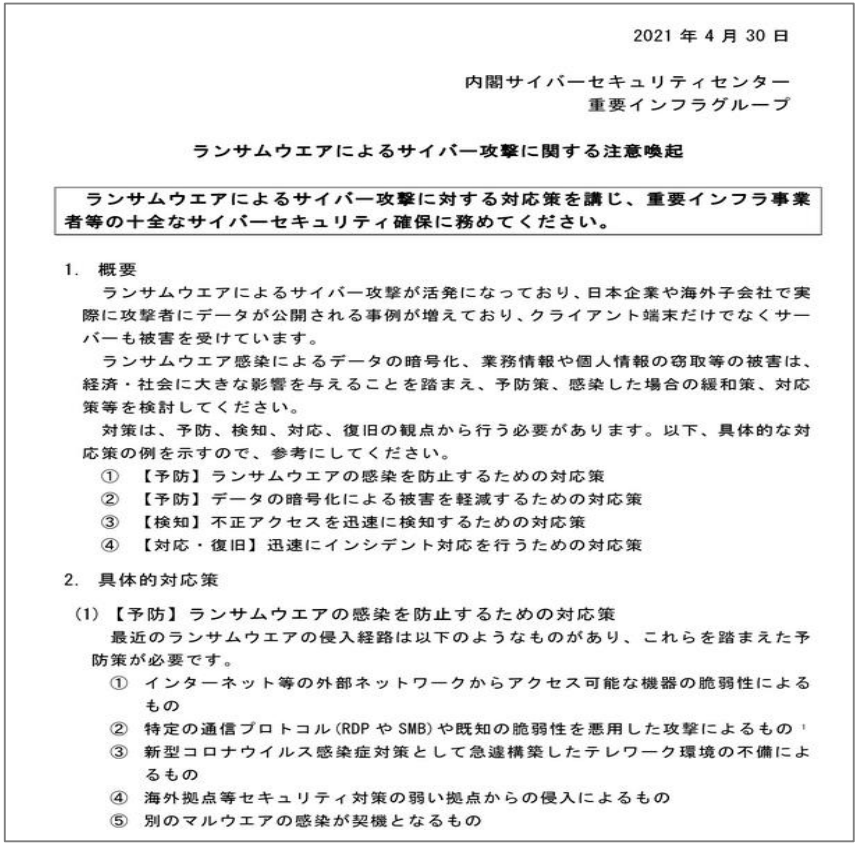
※各報道情報をもとに金融庁作成

内閣サイバーセキュリティセンター（NISC）による注意喚起

予　　防：セキュリティパッチのより迅速な適用、バックアップ、機微データの厳格管理（アクセス制御や暗号化）、復旧計画の確認

検　　知：各機器のログ監視の強化、ふるまい検知、EDR（Endpoint Detection and Response）により、PCやサーバ内で不審な挙動や痕跡がないかの常時監視

対応・復旧：データの暗号化、公開、DoS攻撃等を想定した対処態勢、BCPの策定、組織内外（業務委託先、関係省庁を含む）との連絡体制の確認



2021 年 4 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

ランサムウエアによるサイバー攻撃に関する注意喚起

ランサムウエアによるサイバー攻撃に対する対応策を講じ、重要インフラ事業者等の十全なサイバーセキュリティ確保に務めてください。

1. 概要

ランサムウエアによるサイバー攻撃が活発になっており、日本企業や海外子会社で実際に攻撃者にデータが公開される事例が増えており、クライアント端末だけでなくサーバーも被害を受けています。

ランサムウエア感染によるデータの暗号化、業務情報や個人情報の窃取等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

対策は、予防、検知、対応、復旧の観点から行う必要があります。以下、具体的な対応策の例を示すので、参考にしてください。

① 【予防】ランサムウエアの感染を防止するための対応策
② 【予防】データの暗号化による被害を軽減するための対応策
③ 【検知】不正アクセスを迅速に検知するための対応策
④ 【対応・復旧】迅速にインシデント対応を行うための対応策

2. 具体的対応策

(1) 【予防】ランサムウエアの感染を防止するための対応策

最近のランサムウエアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル（RDP や SMB）や既知の脆弱性を悪用した攻撃によるもの
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウエアの感染が契機となるもの

（記載例）

【予防】ランサムウェアの感染を防止するための対応策

最近のランサムウェアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル(RDPやSMB)や既知の脆弱性を悪用した攻撃によるもの
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウェアの感染が契機となるもの

【予防】データの暗号化による被害を軽減するための対応策

・・・（略）・・・

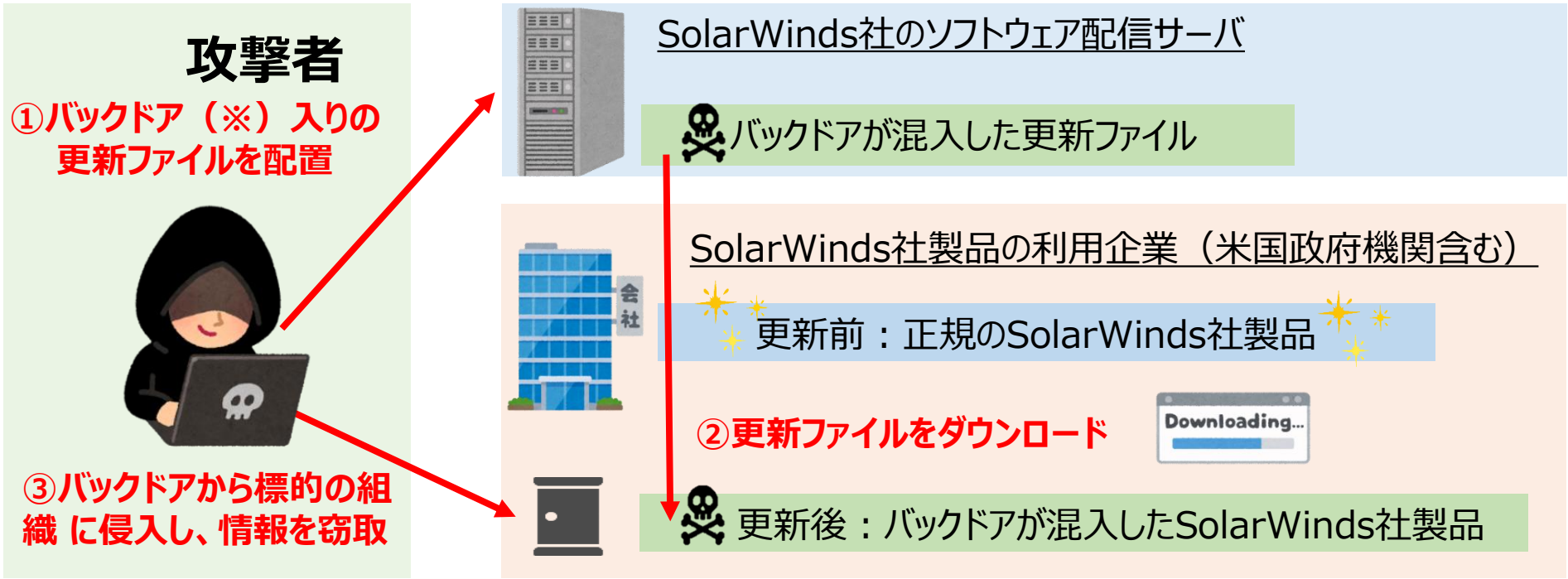
チェックポイント（抜粋）

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウェア感染時でもバックアップが保護されるように留意する。例えば、ファイルのコピーを3個取得したうえで、ファイルは異なる2種類の媒体に保存、コピーのうち、1個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する

事例紹介②：サプライチェーン攻撃
～SolarWinds社へのサプライチェーン攻撃（2020年12月）～

米国のサイバーセキュリティ企業SolarWindsは、自社製品に、バックドアが仕込まれていたと公表（2020年12月13日）

- 大手企業（米Intel等）や政府機関（米財務省等）を含め、米国を中心に世界中の組織（最大18,000組織）が情報窃取された可能性がある。
- FBI、NSA（米国家安全保障局）等が、ロシアが関与した可能性が高いと表明。



（※）バックドア：サービス利用者等に知られることなく、秘密裏に設置されたハッキング等のための侵入口のこと

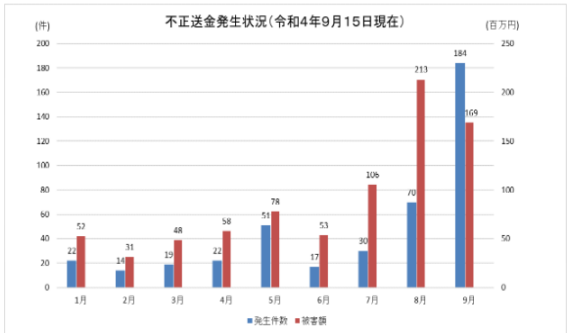
インターネットバンキングによる不正送金

- フィッシングによるものとみられる不正送金被害の急増を踏まえ、2022年9月22日に注意喚起を実施

令和４年９月22日更新
金　融　庁

インターネットバンキングによる預金の不正送金事案が多発しています。

メールやショートメッセージサービス（SMS）、メッセージツール等を用いたフィッシングと推察される手口により、インターネットバンキング利用者のＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発しています。



（出典：警察庁ウェブサイト「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」）

【主な手口】
・SMS等を用いたフィッシング手口
銀行を騙ったSMS等のフィッシングメールを通じて、インターネットバンキング利用者を銀行のフィッシングサイト（偽のログインサイト）へ誘導し、インターネットバンキングのIDやパスワード、ワンタイムパスワード等の情報を窃取して預金の不正送金を行うもの。

【主な手口】
・SMS等を用いたフィッシング手口
銀行を騙ったSMS等のフィッシングメールを通じて、インターネットバンキング利用者を銀行のフィッシングサイト（偽のログインサイト）へ誘導し、インターネットバンキングのIDやパスワード、ワンタイムパスワード等の情報を窃取して預金の不正送金を行うもの。

【被害に遭わないために】
・心当たりのないSMS等は開かない。（金融機関が、ＩＤ・パスワード等をSMS等で問い合わせることはありません。）
・金融機関のウェブサイトへのアクセスに際しては、SMS等に記載されたURLからアクセスせず、事前に正しいウェブサイトのURLをブックマーク登録しておき、ブックマークからアクセスする。または、金融機関が提供する公式アプリを利用する。
・大量のフィッシングメールが届いている場合は、迷惑メールフィルターの強度を上げて設定する。
・金融機関が推奨する多要素認証等の認証方式を利用する。
・金融機関の公式サイトでウイルス対策ソフトが無償で提供されている場合は、導入を検討する。
・パソコンのセキュリティ対策ソフトを最新版にする。
・インターネットバンキングの利用状況を通知する機能を有効にして、不審な取引（例えば、ログイン、パスワード変更、送金等）に注意する。こまめに口座残高、入出金明細を確認し、身に覚えのない取引を確認した場合は速やかに金融機関に照会する。

Ⅱ．サイバーセキュリティについて

（２）サイバーセキュリティ強化に向けた取組み

サイバーセキュリティに関する法制等

- 政府
  - 「サイバーセキュリティ基本法」（2014年11月制定、2016年4月改正、2018年12月改正）
  - 「サイバーセキュリティ戦略」（2015年9月公表、2018年7月改正、2021年9月改正）

- 金融庁
  - 監督指針等の改正（2015年4月）
    - ✓ サイバーセキュリティ管理態勢における監督上の着眼点を明確化
  - 「金融分野のサイバーセキュリティ強化に向けた取組方針」公表（2015年7月）
    - ✓ ① サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、② 金融機関同士の情報共有の枠組みの実効性向上、③ 業界横断的演習の継続的な実施、④ 金融分野のサイバーセキュリティ強化に向けた人材育成、⑤ 金融庁としての体制構築
  - 「金融分野のサイバーセキュリティ強化に向けた取組方針」のｱｯﾌﾟﾃﾞｰﾄ（2018年10月）
    - ✓ デジタライゼーションの進展、国際的な議論の進展、「2020年東京オリンピック・パラリンピック競技大会」などの新たな課題への対応方針等を明確化するため、「取組方針」をアップデート
  - 「金融分野のサイバーセキュリティ強化に向けた取組方針」のｱｯﾌﾟﾃﾞｰﾄ（Ver. 3.0）（2022年2月）

金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）

～サイバーセキュリティを確保し、安心・安全かつ利便性の高い金融サービスの実現へ～

サイバー空間の変化

- 国家の関与が疑われる**組織化・洗練化されたサイバー攻撃**や、国際的なハッカー集団等による**ランサムウェア攻撃の多発**
- デジタライゼーションの進展による**金融サービスの担い手の多様化**と、キャッシュレス決済などの**連携サービスの進展**
- クラウドサービスをはじめとした**外部委託の拡大、サプライチェーンの複雑化・グローバル化**等による**リスク管理の難度の高まり**

新たな取組方針（以下、５項目）

１．モニタリング・演習の高度化

金融機関の規模・特性やサイバーセキュリティリスクに応じて、検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証する。
共通の課題や好事例については業界団体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に

- ✓ 3メガバンクについては、**サイバー攻撃の脅威動向の変化への対応**や**海外大手金融機関における先進事例**を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する
- ✓ 地域金融機関については、**サイバーセキュリティに関する自己評価ツールを整備**し、各金融機関の自己評価結果を収集、分析、還元し、**自律的なサイバーセキュリティの高度化を促す**
- ✓ サイバー演習については、引き続き、**サイバー攻撃の脅威動向**や**他国の演習**等を踏まえて高度化を図る

２．新たなリスクへの備え

- ✓ **キャッシュレス決済サービス**の安全性を確保するため、リスクに見合った**堅牢な認証方式の導入等**を促す**（セキュリティバイデザインの実践）**
- ✓ クラウドサービスの安全な利用に向けて、**利用実態**や**安全対策**の把握を進めるとともに、**クラウドサービス事業者との対話**も実施

３．サイバーセキュリティ確保に向けた組織全体での取組み

- ✓ 経営層の積極的な関与の下、**組織全体でサイバーセキュリティの実効性**の向上を促す（セキュリティ人材の育成も含む）

４．関係機関との連携強化

- ✓ サイバー攻撃等の情報収集・分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため**関係機関（NISC、警察庁、公安調査庁、金融ISAC、海外当局等）との連携を強化**

５．経済安全保障上の対応

- ✓ 政府全体の取組みの中で、機器・システムの利用や業務委託等を通じたリスクについて適切に対応を行う

（１）モニタリング・演習の高度化

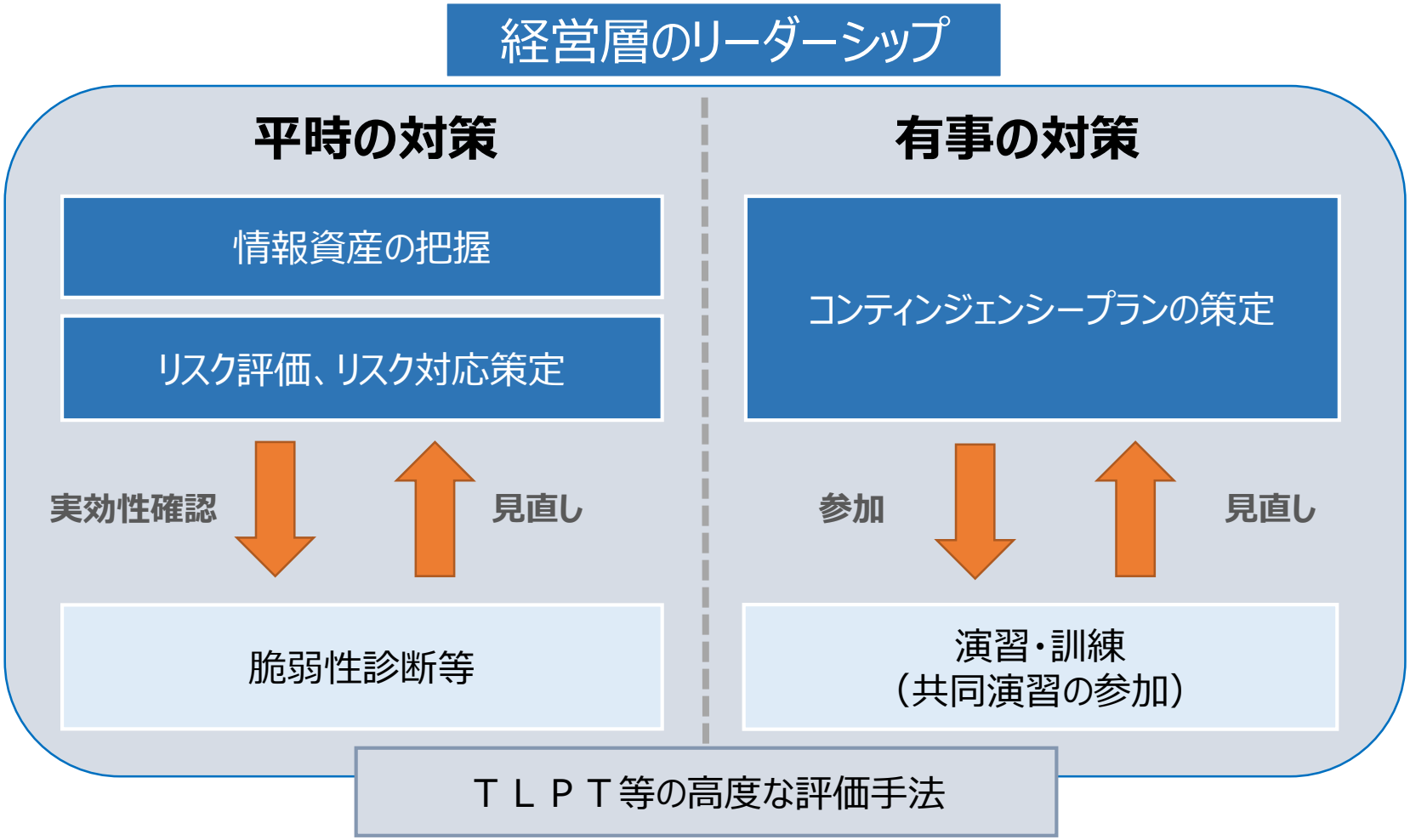
金融機関の規模・特性やサイバーセキュリティリスクに応じたモニタリングを実施

- 大手金融機関
  - ✓ 海外大手金融機関における先進的な取組事例
  - ✓ 国際的な議論の動向

- 地域金融機関
  - ✓ サイバーセキュリティ態勢の実効性の検証
  - ✓ 自己評価ツールの作成

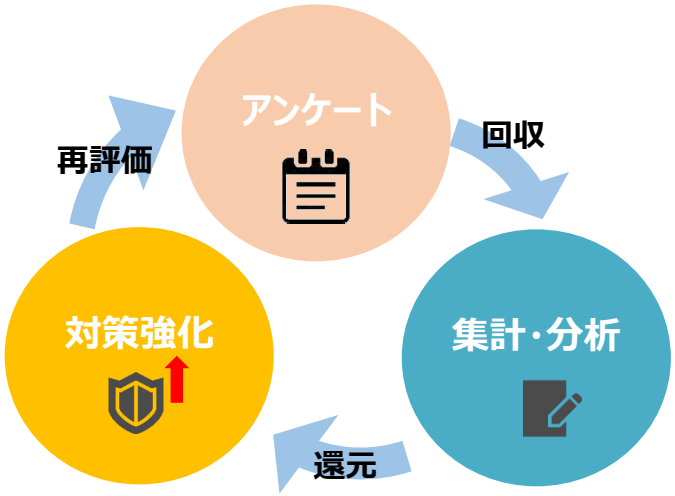
サイバーセキュリティの確保に向けて

サイバーセキュリティの確保に向けては、経営層の積極的なリーダーシップの下、①平時の対策と②有事の対策を両輪として進めていくことが重要



地域金融機関向けのサイバーセキュリティに関する自己評価ツールの作成

課題	金融機関は、それぞれの規模・特性に応じ、サイバーセキュリティ管理態勢を整備し、実効性を確保する必要があるが、これまで、他の金融機関対比での自組織の位置付けや改善すべき領域を特定するツールが必ずしも広く用いられてこなかった
目標	地域金融機関の自己評価結果を収集・分析し、その結果を還元することで、地域金融機関のサイバーセキュリティ管理の自律的な高度化を促す
方針	金融庁、日本銀行、FISCの3者共同で地域金融機関向けのサイバーセキュリティに関する自己評価ツールを整備
対象	地域金融機関（①地域銀行、②信用金庫、③信用組合）



金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅶ）

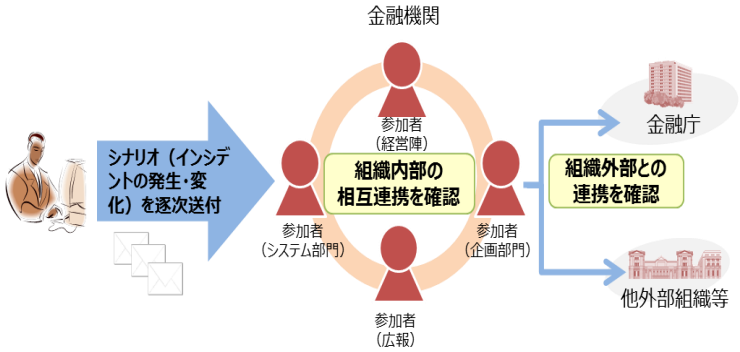
金融庁主催による７回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅶ）を実施し、約160先が参加。

インシデント発生時の顧客対応や部門間及び組織外部との連携の実効性を確認し、業界全体のインシデント対応能力の底上げを図る。

演習の特徴

- ✓ インシデント発生時における**技術的対応を含めた攻撃内容の調査等、初動対応、顧客対応、復旧対応等の業務継続**を確認
- ✓ 経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、**自職場参加方式**で実施
- ✓ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策や優良事例を示すなど、**事後評価に力点**
- ✓ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

演習スキーム



【演習シナリオの概要】

- **銀行**
  - ✓ （ブラインド方式のため非開示）
- **信金・信組・労金**
  - ✓ 顧客情報の漏えいやWebサイトの異常が発生
- **証券・FX・資金移動業者・前払式支払手段発行者**
  - ✓ ネットワーク機器の異常を端緒とした業務システム等の停止が発生
- **暗号資産交換業者**
  - ✓ 情報漏えいを端緒とした暗号資産流出が発生

（２）新たなリスクへの備え

①　キャッシュレス決済サービスにおける安全性の確保

- ✓ 金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティバイデザイン」を実践し、サービス全体の流れの中で、連携先も含めて脆弱性を洗い出し 、リスクに見合った堅牢な認証方式を導入することが重要。

②　クラウドサービスの普及等への対応

- ✓ クラウドの利点を活用しつつ、仕様・特性に伴うリスクも適切に評価し、システム稼働の安定性と顧客情報の適切な管理を確保することが重要（コンティンジェンシープランの整備や演習の実施）。

③　サイバーハイジーンの徹底（サイバー公衆衛生）

- ✓ 外部委託の拡大などにより、IT資産管理の範囲が拡大・複雑化する中、安全性の高いIT環境を維持するには、境界型セキュリティ等や特定のセキュリティ製品だけに依存することなく、サイバーハイジーンの推進が重要。

④　サイバーレジリエンスの強化

- ✓ インシデント発生時の検知、特定、対応、復旧を強化し、インシデントで業務が中断した場合も、業務や顧客への影響を許容水準内に収めることが重要。

（３）サイバーセキュリティ確保に向けた組織全体での取組み

セキュリティ確保のため、引き続き、経営層の積極的な関与とセキュリティ人材の育成を促す

①　経営層の関与

- ✓ サイバーセキュリティはIT・システム部門のみの問題ではなく、あらゆる部門、階層での対応が求められる。
- ✓ 組織全体でのサイバーセキュリティ管理の実効性を高めるため、経営層の積極的な関与、リーダーシップの発揮を促す。

②　セキュリティ人材の育成

- ✓ 人事ローテーションを前提としたうえで、各部署に必要なセキュリティ人材を育成、配置することが必要。
- ✓ 例えば、自組織で知見が不足しているセキュリティ分野を洗い出し、人材育成計画を作成、実行するほか、内部の研修だけではなく、金融ISAC等の外部の活動にも参加しやすい職場環境を整備するなど、計画的に組織全体でのセキュリティ人材の育成を図る。
- ✓ 特に、経営層の方針を踏まえ、具体的なサイバーセキュリティの立案と指揮を担う戦略マネジメント層や、研修や人材育成を担うセキュリティトレーナー、システムの開発・運用担当者については、育成に時間を要するため、計画的に取り組むことが重要である。

経営層への期待

- **サイバーセキュリティに関する方針、スタンスを表明する**
  - サイバーセキュリティに対する企業文化の醸成、意識づけ
  - 共助の枠組みへの積極的な参加の推奨
- **サイバーリスクを議題として取り上げ、十分に議論を行う**
  - サイバーリスクは経営の問題（単なるITの問題ではない）
  - サイバーセキュリティはDXの前提条件（セキュリティバイデザイン）
  - 予算・人員の適切な配分、計画的な人材育成
- **正確なリスク評価・分析に基づく経営判断を行う**
  - 国内外の脅威動向の把握
  - リスクベースの実効性あるセキュリティ対策
  - セキュリティ担当との直接のコミュニケーション
- **事案発生時の危機対応の準備**
  - 最終責任者としての自覚
  - 最悪の事態を想定した準備（演習等）

（参考）経営層の役割

経団連サイバーセキュリティ経営宣言 2.0（22年10月）

1．経営課題としての認識

- 経営者自らが最新情勢への理解を深めることを怠らず、DXを進めるうえで必須となるサイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
- 経営者自らがデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題として認識し、リーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2．経営方針の策定と意思表明

- 特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP（事業継続計画）の策定を行う。
- 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に記載するなど開示に努める。

3．社内外体制の構築・対策の実施

- 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
- 経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
- サイバーセキュリティ対策のガイドライン・フレームワークの活用や、政府によるサイバーセキュリティ対策支援活動との連携等を通じて、取引先や委託先、海外も含めたサプライチェーン対策に努める。

4．対策を講じた製品・システムやサービスの社会への普及

- 製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5．安心・安全なエコシステムの構築への貢献

- 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
- 各種情報を踏まえた対策に関して注意喚起することによって、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に寄与する。

Ⅲ．期待される内部監査について

（１）顧客本位の業務運営

- 第３線において、準拠性に止まらない監査実施の重要性が増大。

（例）・ 顧客本位の業務運営の実践に向け、法令・規定の遵守に止まらず、金融商品の販売状況（偏重や想定外の販売額）など多様な視点から、利用者視点の欠如した行為が行われていないかを監査しているか。

・ 企業文化や社会情勢等の変化を踏まえて、テーマ別監査やカルチャー監査といった形で社会規範に悖る行為が行われていないかを適時適切に監査しているか。

・ 第３線は、監査で判明した問題点の背景・真因を経営陣に適切に報告しているか。また、その問題点を踏まえて、適切な改善策を策定・実践しているかを適時適切にフォローアップしているか。

- 経営監査を含め、ビジネスモデルの有効性や適切性を検証する視点が重要。

（例）・ 顧客本位の良質なサービス提供を通じて、顧客の最善の利益を追求するとともに、長期的に持続可能な経営戦略構築の検討がなされた上で、当該検討を踏まえて取組方針が明確化・具体化されているか。

・ 経営戦略の収益計画等は、顧客本位の良質なサービスの提供に弊害のあるものとなっていないか。

・ ビジネスモデルに即した顧客の最善の利益の実現に関して、顧客本位の取組みの定着度合いや有効性を判断するのに適切な内部指標が用いられているか。

（２）サイバーセキュリティ

- 1線、2線のサイバーセキュリティに関する統制は十分かつ適切に行われているか。

（例）・ サイバーセキュリティ担当の役職・委員会が、形式的に設置されていたり、サイバーセキュリティに関する内部規定が形式的に整備されていたりすることだけではなく、こうした役職、組織、規定が有効に機能しているか。

・ 情報資産台帳は整備されているか（網羅的なものとなっているか、ソフトウェアも含まれているか、適切に更新され、管理されているか）、特権IDの管理は適切に行われているか（パスワード管理、ログ監視が行われることとなっているか、また、適切にこうした管理が行われているか）　。

- 経営層がリーダーシップを発揮し、サイバーセキュリティについて、1線・2線・3線による管理・牽制を働かせることが重要。

（例）・ 経営層は、サイバーセキュリティが監査対象に含まれているかを含め、年間監査計画の妥当性を検討し、承認しているか。

・ 監査結果は経営層に報告されているか。 経営層は、サイバーセキュリティに関する監査上の指摘事項について、改善状況が適切にフォローアップされているかを確認しているか。

・ 監査部門と外部専門家による共同監査（コソース）、システム監査人による内部監査が実施されているか。