プライバシー保護データマイニング
シンポジウム　講演資料

NTT DATA
Trusted Global Innovator

「真のイノベーションには非物理的対処が欠かせない」
～高度技術の実装だけでは企業資産は守れない～

2018年 10月31日
株式会社 NTTデータ経営研究所
パートナー　金融政策コンサルティングユニット長
大野　博堂

本日のアジェンダ

金融機関における新しい技術の需要と
新たなリスクの台頭

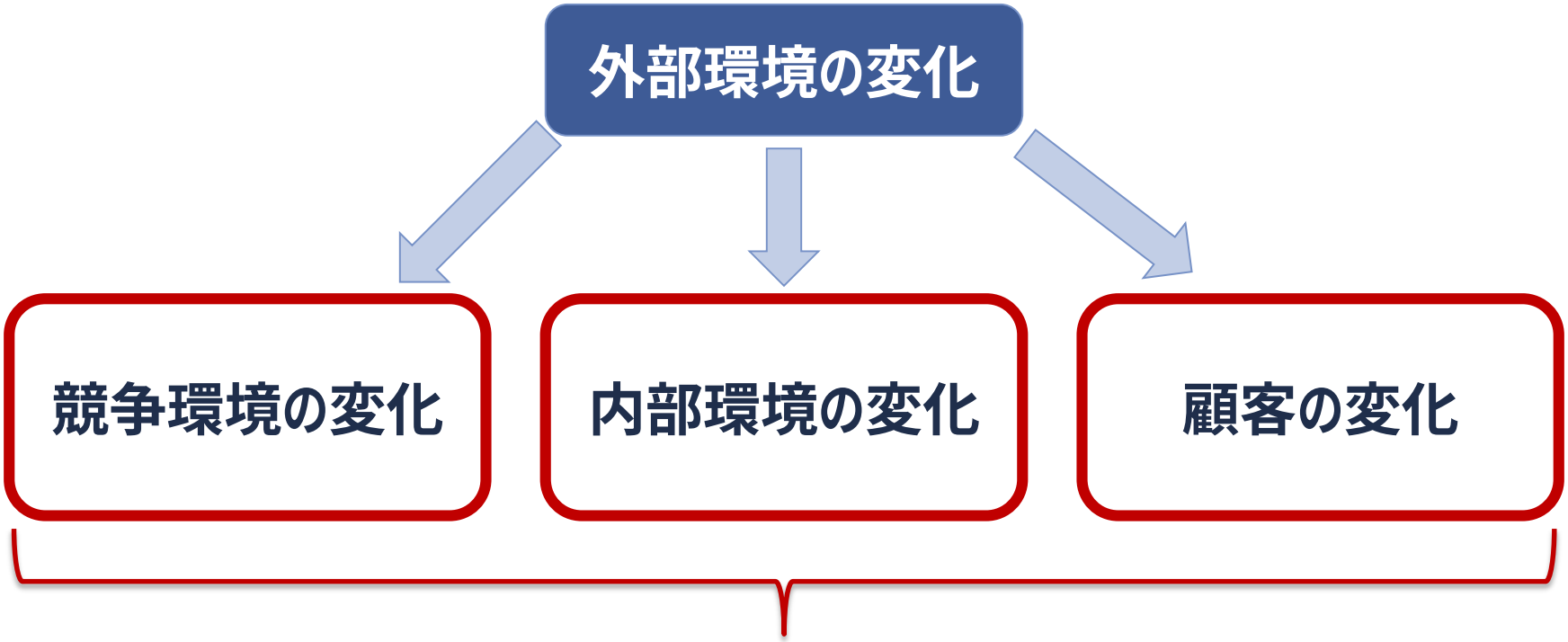
サイバーセキュリティ対策における
金融庁の金融機関への要請ポイント

当局における新たな検査体制によって加わるプレッシャー

地域金融機関においては、2つのグループに大別した検査体制を敷くとともに、顧客に主眼を置いた検査・監督指針に変更されています

	グループ① (地域トップ行)	グループ② (その他の地域金融機関)
グループの大別	ü 地域経済の活性化への貢献を目標に、金融仲介機能の発揮に重点を置くグループ	ü 将来にわたって持続可能なビジネスモデルの構築を主眼とするグループ
検査の方向性	ü 借り手企業の**事業性評価に基づく融資の動向**をチェック	ü **ニッチな分野への進出や独自のビジネス展開**などを通じ、真に顧客の利益になるようなサービスの提供を促す

ü 2グループに大別し検査を実施
ü 各行一律の金融検査マニュアルによる検査は中止
ü ただし、**サイバーセキュリティ及びFATF対応については、業態を問わず一定のチェックの視点を導入**



現状変更に迫られているのが金融機関

金融機関はこれまで、新しい技術に目をつぶっていたのか？

これまでの金融システム

- 「絶対に止めてはならない！」**との意識**
- **安全、安心を念頭に、「枯れた技術」を指向**

今、おきていること

- **「技術ありき」でベンチャーによる金融業務への新規参入が進展**
- **新規参入業者では、「安全、安心」よりも、「スピード」や「変化への対応」が**優先される傾向？

金融機関としても、新しい技術に取り組まざるを得ない状況に

フィンテック企業への依存度拡大によるリスク管理の複雑化

フィンテック企業のビジネスは顧客に近いところで展開

セキュリティ確保よりも展開スピードが優先される傾向

- ü セキュリティの考え方、セキュリティポリシーの理解、技術面での対策などについて、十分な考慮がなされない可能性

金融機関の業務部門がIT部門にかわってフィンテックを評価

- ü 金融機関のIT部門ではなく、金融機関のビジネス部門がフィンテック企業とダイレクトにビジネスを展開

フィンテック企業への依存度拡大につれ、リスク管理も複雑化

- ü フィンテック企業側のインシデントが金融システムに影響するも、金融機関のIT部門とは切り離された格好で管理

フィンテック企業に内在するリスク

ü **フィンテック企業を取り巻くリスクは、セキュリティのみではありません。経営者そのものや経営の意思決定メカニズムを含めた全体像を踏まえたリスクコントロールや監査が必要です**

対象	想定される事象
経営陣	ü 経営陣のコンプライアンス意識が希薄 ü 公私の峻別がついていない
株主・資本関係	ü 知らない間に株主が代わっていた/増えていた ü 怪しげな企業と提携していた
情報システム	ü 情報システムの運用が不安定でトラブルが多い ü 情報システムのセキュリティに課題がある
意思決定	ü 少数の幹部が複数部門を兼務で所管しており牽制機能が発揮されない ü 実は外部の第三者によって会社の意思決定が支配されていた
ビジネスモデル	ü ビジネスモデルが陳腐化する（他社が同様のビジネスを実践してしまう） ü 導入予定もしくは開発していた技術が実現されない ü 想定していた収益を確保することができない ü 第三者との間で知的所有権を巡るトラブルが発生する
リスク管理	ü そもそもリスク管理がなされていなかった/脆弱性が存在していた ü 経営層のリスク管理の意識が希薄だった

提携先企業（フィンテック企業）の定点チェックが必要

- **比較的小規模であるフィンテック企業の場合、アイディアベースで事業規模拡大が志向される傾向にあり、ガバナンスやセキュリティが劣後されている可能性があります。したがって、定期的にチェックを行い、活動実態をつぶさに捕捉・評価することが望まれます**

提携先企業の初期監査

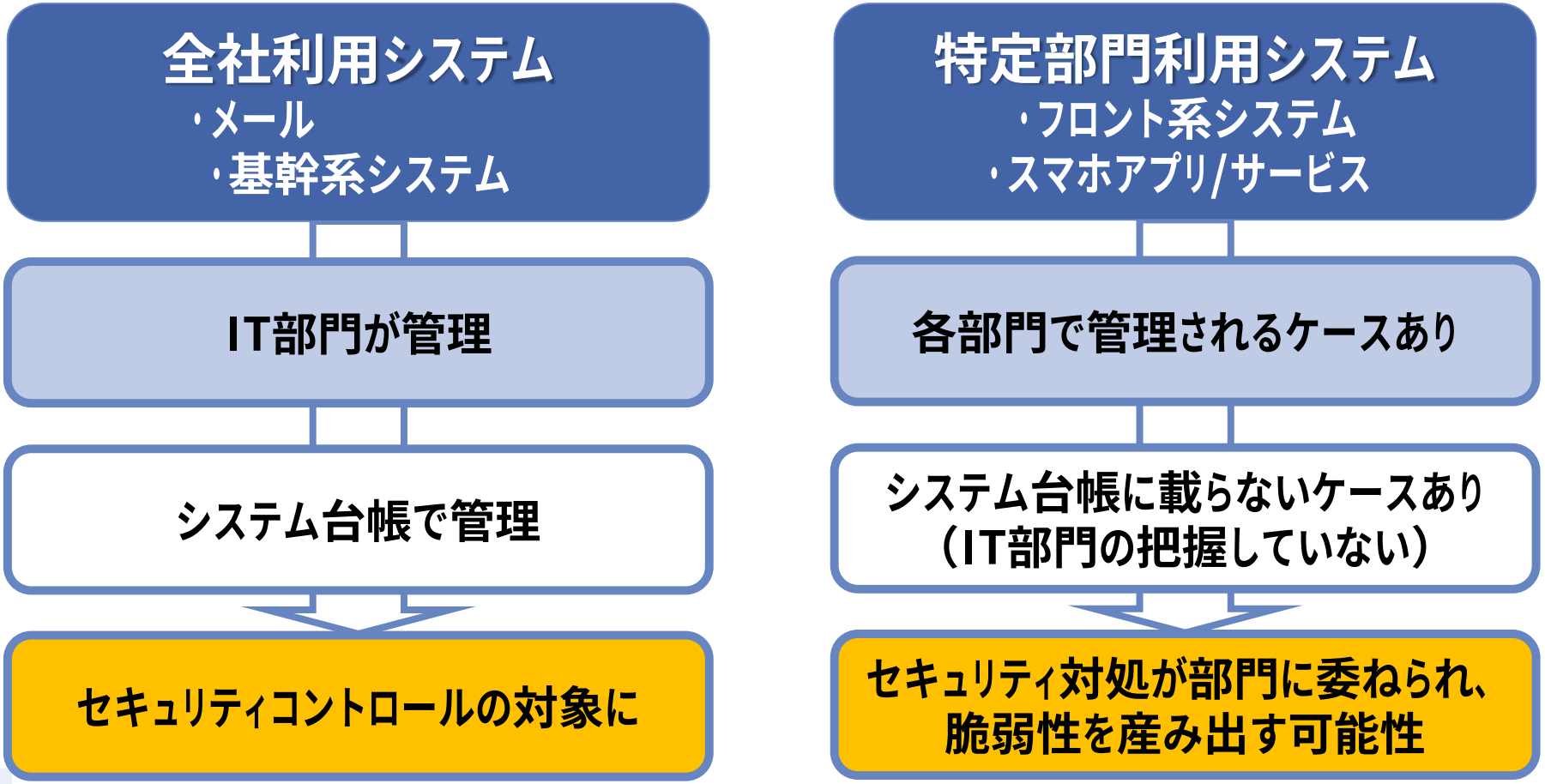
- ビジネスモデルの有意性確認
  - 技術評価
  - 事業計画の評価
- 情報システム
  - 開発状況
  - セキュリティアセスメント
- 意思決定メカニズムの状況
  - 意思決定のプロセス
  - 関連規程類の整備状況
- 兼務の状況
  - 牽制機能の実効性を検証
- 他社との資本提携・連携状況
  - 提携先企業も資本関係、株主属性などを漏れなく確認
  - 他社への再委託状況の確認

提携先企業の定点監査

- 定点観測によるリスク管理
  - 株主の変化
  - 提携先企業の変化
  - システム開発の状況変化
  - 再委託の状況変化
- セキュリティ運用状況
  - 物理的対処の状況
  - 非物理的対処の状況
- 当局レギュレーションへの準拠
  - レギュレーションへの対応状況
  - 企業の対応意識
- 規程類整備状況
  - リスク管理の手順化状況

業務部門が利用するITシステムの実態把握が必要

ü フィンテック企業との連携などにより、業務部門が他社のITシステムやサービスを利用するケースが増えつつあります。この場合、IT部門の所管外であることが多く、システム管理台帳にすら掲載されていない企業も少なくありません。セキュリティチェックも抜け落ちがちですので、早期の実態把握が必要です



新しい技術の導入に際しての当局の懸念

p 金融庁

- ü 「新しい技術やサービスの導入は進めるべき」
- ü 他方、サービスの提供元たる企業のチェックは厳格に実施すべき
- ü フィンテック企業との連携により、金融機関と顧客との間に新たなリスクファクターが生まれた

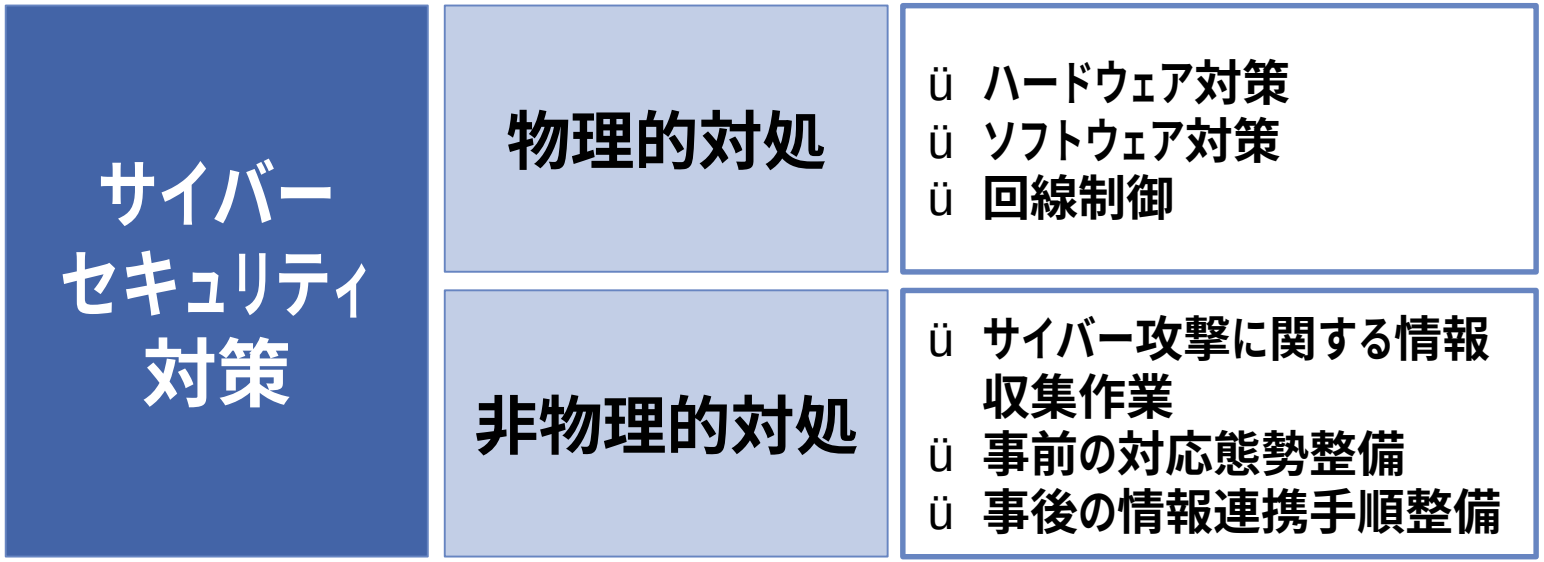
p 日本銀行

- ü 2016年3月に公表された日銀「決済システムレポート」では、フィンテック企業破綻時における決済システムへの影響が懸念される旨報告

サイバーセキュリティ対策における
金融庁の金融機関への要請ポイント

サイバーセキュリティ対策における金融庁の方針

ü **例えばサイバーセキュリティ対策において金融庁では、ハードやソフト、回線制御といった物理的対処ではなく、態勢整備や対応手順の策定などを含めた「非物理的対処」を中心に、施策を展開しています**



金融庁が定義するサイバー攻撃への対処における４つのステップ

ü **金融庁では、サイバー攻撃への対処として、金融機関に対して４つのステップで整備を進めるよう要請しています。ただし、これらを金融機関業務に実装するためには、より一層要件を整理･精緻化する必要があります**

特定

- 保護すべき対象の把握
- 経営陣によるサイバーセキュリティ管理の重要性の認識
- セキュリティ水準の定期的評価
- システム開発におけるセキュリティ管理の視点の導入

防御

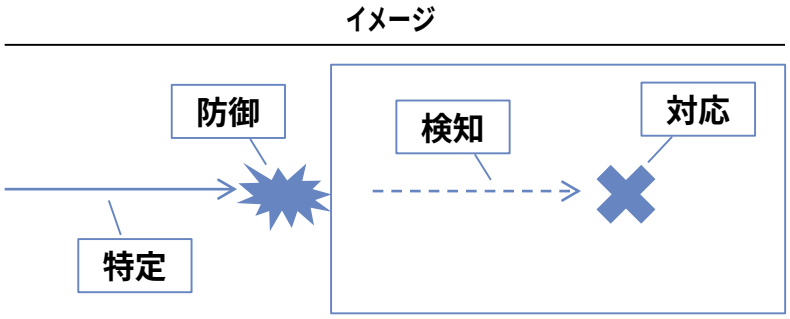
- 組織内の緊急時対応/早期警戒体制の整備
- 情報共有機関等を通じた情報収集/共有体制の整備
- 多層防御（入口対策･内部対策･出口対策）
- システムの脆弱性についての適時の対応
- CPの策定
- 業界横断的演習への参加

検知

- 通信記録（ログ）等の取得･分析を含むサイバー攻撃に対する監視

対応、復旧

- CPに沿った適切な対応



（引用元）金融庁　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について（平成27年7月）
金融庁　金融商品取引業者等向けの総合的な監督指針（平成27年9月）

金融庁が定義する取組方針（平成27年7月）の要素分解

ü **金融庁が発表した取組方針を要素分解し、背景として「何を求めているのか」を明らかにします。すると、各ステップで求めている具体的な機能が浮かび上がってきます**

特定

- 保護すべき対象把握
- 経営陣によるサイバーセキュリティ管理の重要性の認識
- セキュリティ水準の定期的評価
- システム開発におけるセキュリティ管理の視点の導入

↓

- チャネル分析
- リソース分析
- セキュリティ診断
- 技術的対処

防御

- 組織内の緊急時対応/早期警戒体制の整備
- 情報収集/共有体制の整備
- 多層防御（入口対策･内部対策･出口対策）
- システムの脆弱性についての適時の対応
- CPの策定
- 業界横断的演習参加

↓

- 態勢整備
- 情報収集
- 内部･外部連携
- 技術的対処
- 現状評価
- 対応手順策定
- 演習実施

検知

- 通信記録（ログ）等の取得･分析を含むサイバー攻撃に対する監視

↓

- 態勢整備

対応、復旧

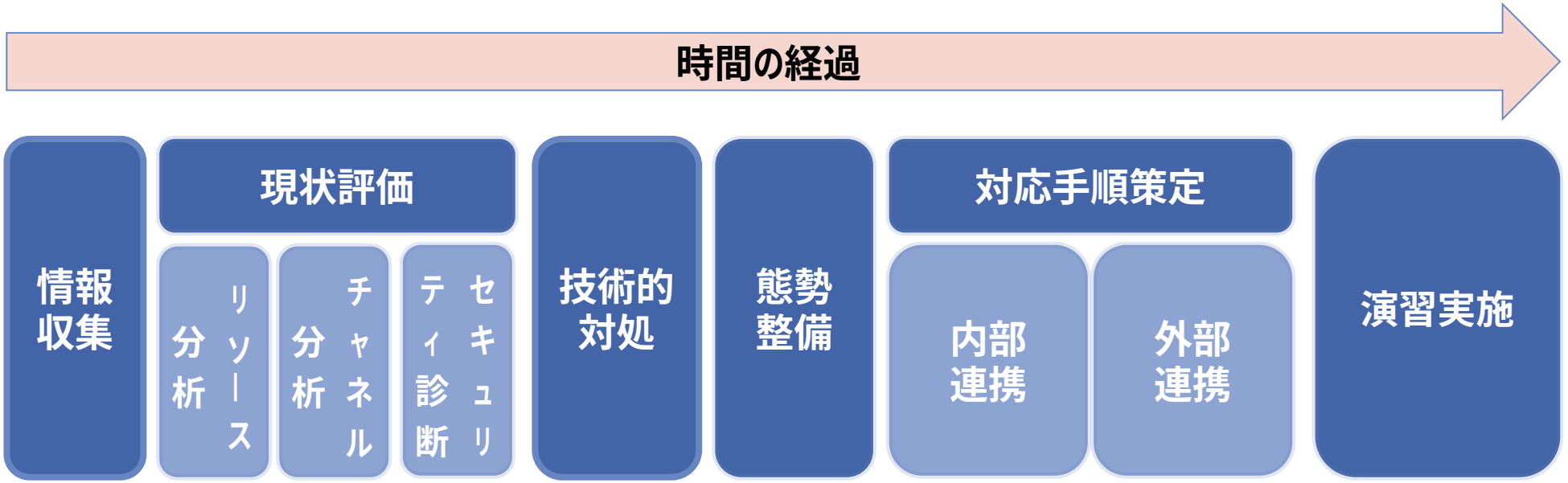
- CPに沿った適切な対応

↓

- 対応手順策定

金融庁が求める具体的な機能の構造化

ü **金融庁が「求めているであろう」と推察される具体的な機能を構造化してみると、「情報収集」「現状評価」「技術的対処」「態勢整備」「対応手順策定」「演習実施」の大きく6つに整理されます。**



マーケットでの実態としての検討スコープ

- ü ただし、マーケット動向をみると、多くが「情報収集」「セキュリティ診断」「技術的対処」にフォーカスした対応が中心となっているようです。
- ü 実際、外部事業者における支援プログラムも、金融機関へのサイバーセキュリティ関連情報提供のほか、技術的側面での支援にフォーカスされたものが中心です。
- ü 金融庁の要請に応えるためには、技術的対処のほか、初動部分の対応についても十分に検討した態勢やマニュアルを用意する必要がありますが、まだまだ検討が不足しているようです

新しい技術やサービスを導入した場合の課題

- **新しい技術やサービスの導入に際しては、それを生かすための取組が欠かせない**

  - ü 内部管理態勢の整備
  - ü 技術の提供元企業のチェック（定点観測）
  - ü サービスが途絶えた場合を想定した代替機能及び顧客対応の検討
  - ü 上記を念頭においた対応手順の策定

本日はありがとうございました

NTT DATA
Trusted Global Innovator

パートナー
金融政策コンサルティングユニット長
大野　博堂（おおのはくどう）

株式会社ＮＴＴデータ経営研究所
TEL：（03）5213-4115
FAX：（03）5560-3743
E-mail:　onoh@keieiken.co.jp
〒135-6022　東京都江東区豊洲3-3-3　豊洲センタービル22階