日本金融監査協会
展望セミナー　講演資料

NTT DATA
Trusted Global Innovator

コロナ禍における緊急時対応

2020年10月13日
株式会社NTTデータ経営研究所
大野　博堂

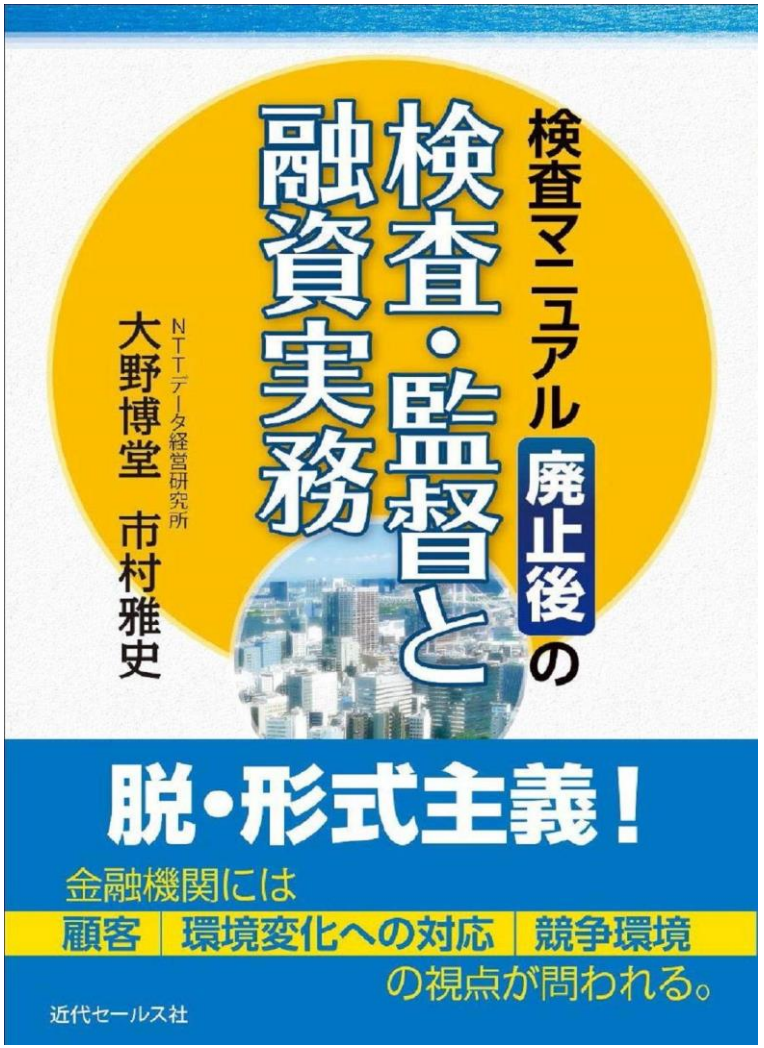
自己紹介

大野　博堂（おおの　はくどう）

平成5年　　NTTデータ　金融システム事業本部
平成10年　大蔵省大臣官房総合政策課
（金融再生関連法対応、金融市場分析を担当）
平成12年　NTTデータ　金融システム事業本部
平成18年　NTTデータ経営研究所　金融政策コンサルティングユニット
（中央省庁、金融機関、自治体向け調査・研究・コンサルティングを担当）

（著書）「マイナンバー義務的対応&利活用ガイド」（2015　金融財政事情研究会）
「サイバーセキュリティとBCPの実務」（2016　金融財政事情研究会）
「AIが変える2025年の銀行業務」（2018　近代セールス社）
「地域金融機関のためのRAF構築」（2020　金融財政事情研究会）
「検査マニュアル廃止後の検査監督と融資の実務」（2020　近代セールス）
（連載）WEBサイト**「Fintech Journal」**にて**「大野博堂の金融最前線」**を連載中

近著のご紹介



本日のアジェンダ

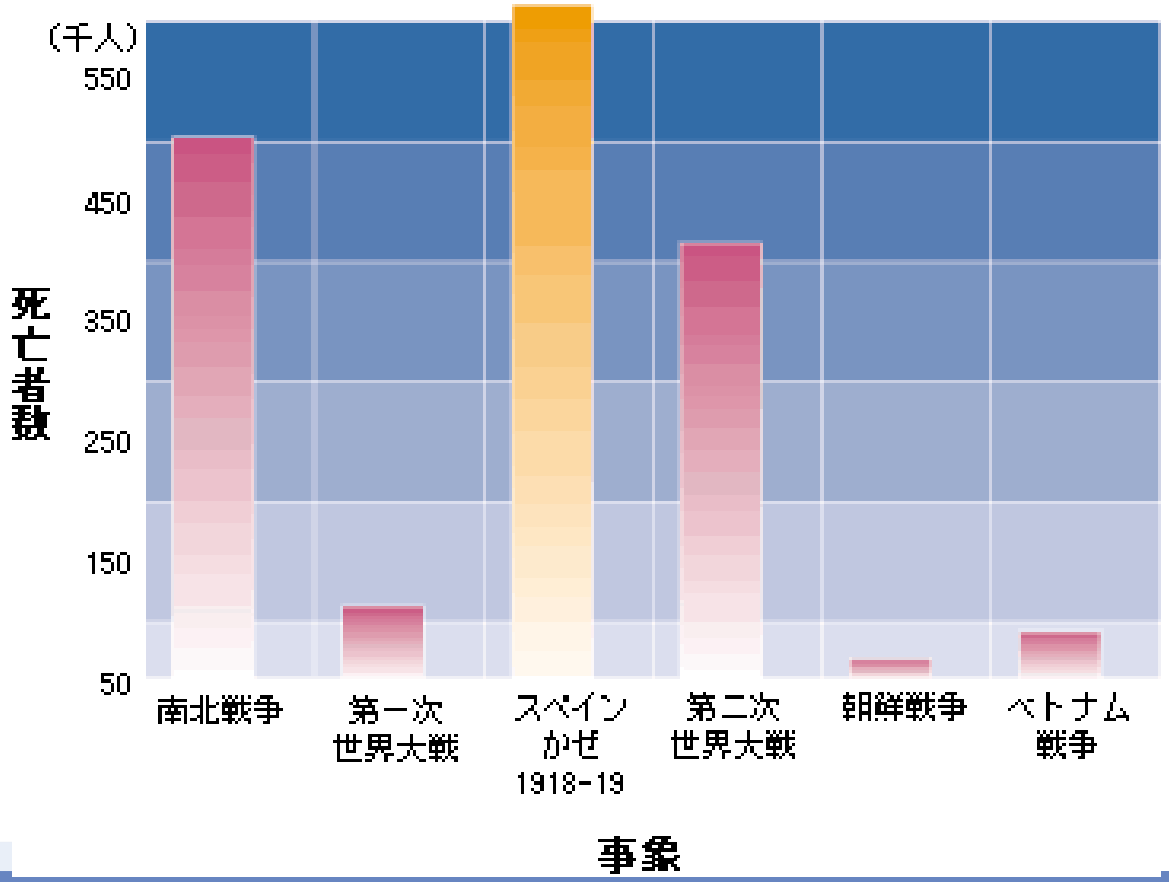
次なる波に備えた「必須・重要業務」の点検、テレワーク対応

コロナ禍で増加するサイバー犯罪への対応

次なる波に備えた
「必須・重要業務」の点検、テレワーク対応

1918年のスペイン風邪における被害

過去の感染症の大規模流行としては、1918年のスペイン風邪（スペイン・インフルエンザ）があります。世界では人口の25～30%が罹患し、4000万人が死亡したと推計されており、日本では当時の人口の半数にあたる2300万人が感染し、39万人が死亡しています



スペイン風邪が全世界的に流行するまでには8ヶ月を要した

航空機などの交通網が発達し、ボーダーレスに人が行き交う現代では、世界のどこで発生しても、短期間に蔓延する可能性が高い

パンデミック・警報フェーズの定義

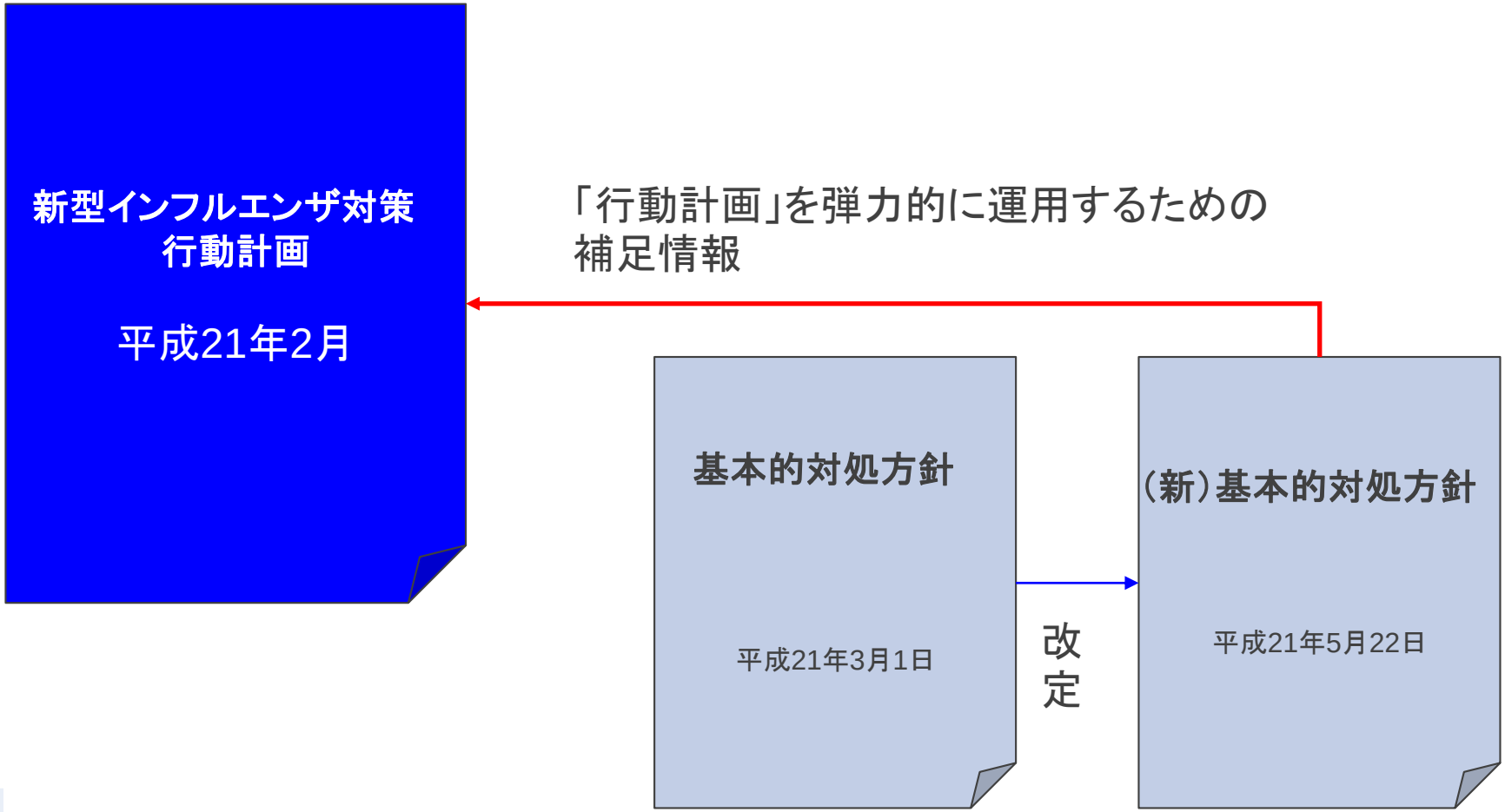
WHO（世界保健機関）ではパンデミックを大きく6段階で区分し、それぞれ定義付けを行っています。なお、このフェーズ分けは、「感染地域の拡がり」を示すスケールです

発生事象	定義	WHO指定フェーズ	
（平時）	ヒト感染のリスクは低い	1	プレ・パンデミック期
動物間に、新しい亜型ウィルスが存在するが、ヒト感染はない	ヒト感染のリスクがより高い	2	パンデミック・アラート期
新しい亜型ウィルスによるヒト感染発生	ヒトーヒト感染は無いか、または極めて限定されている	3	
	ヒトーヒト感染が増加している	4	
	ヒトーヒト感染が集団規模で発生している（世界6地域のうち、1地域の複数国で感染）	5	
	ヒトーヒト感染が大流行している（世界6地域のうち、複数地域で感染）	6	パンデミック期

図表：国立感染症研究所HPを参考に、㈱NTTデータ経営研究所が作成

我が国における新型インフルエンザ対策の構造

我が国では、過去から新型インフルエンザに関するガイドラインが用意されていました。
そのため、新型コロナウィルス流行に際しても、比較的早期に対策に着手できたものとみられます



毒性の差異を踏まえた二系統の対策

平成21年2月に策定された国の「行動計画」と、同年5月にこれを補足する目的で策定された「基本的対処方針」（新対処方針）によって、我が国の新型インフルエンザ発生時における対策としては、ウィルスの毒性の強弱を踏まえ、二系統の対策が用意されることとなりました。

	「行動計画」 （平成21年2月）	「基本的対処方針」（新対処方針） （平成21年5月）
ウィルスのタイプ	H5N1	H1N1
感染力	強い	強い
毒性タイプ	**強毒性**	**弱毒性**
外出・集会	自粛を要請	自粛を要請しない
企業への要請	企業の不要・普及の業務の縮小・停止、職場での感染防止対策の要請。	事業自粛の要請を行わない。ただし、事業運営において感染機会を減らすための工夫を検討するよう要請。

我が国における感染症法上の分類

新型コロナウィルスは、現在のところ二類感染症として政府は捉えています。

なお、インフルエンザ」の場合、強毒性タイプと弱毒性タイプでは、感染症としての分類が異なっています

分類	対象となる主な感染症
一類感染症	エボラ出血熱、クリミア・コンゴ出血熱、ペスト、ラッサ熱
二類感染症	結核、ジフテリア、鳥インフルエンザ（H5N1）、新型コロナウィルス
三類感染症	コレラ、赤痢、出血性大腸菌
四類感染症	黄熱、鳥インフルエンザ（H5N1を除く）、狂犬病、デング熱
五類感染症	季節性インフルエンザ（鳥インフルエンザ及び新型インフルエンザを除く）、梅毒、風疹、手足口病、日本脳炎

一類及び二類は、「法で定める強制措置」の対象となる

現在、政府は新型コロナウィルスについて、感染症法における分類を、第二分類から第五分類へと変更することを検討中

通常の風邪と同様の取扱となる可能性

日本銀行による金融機関向けのパンデミック対策ガイドライン

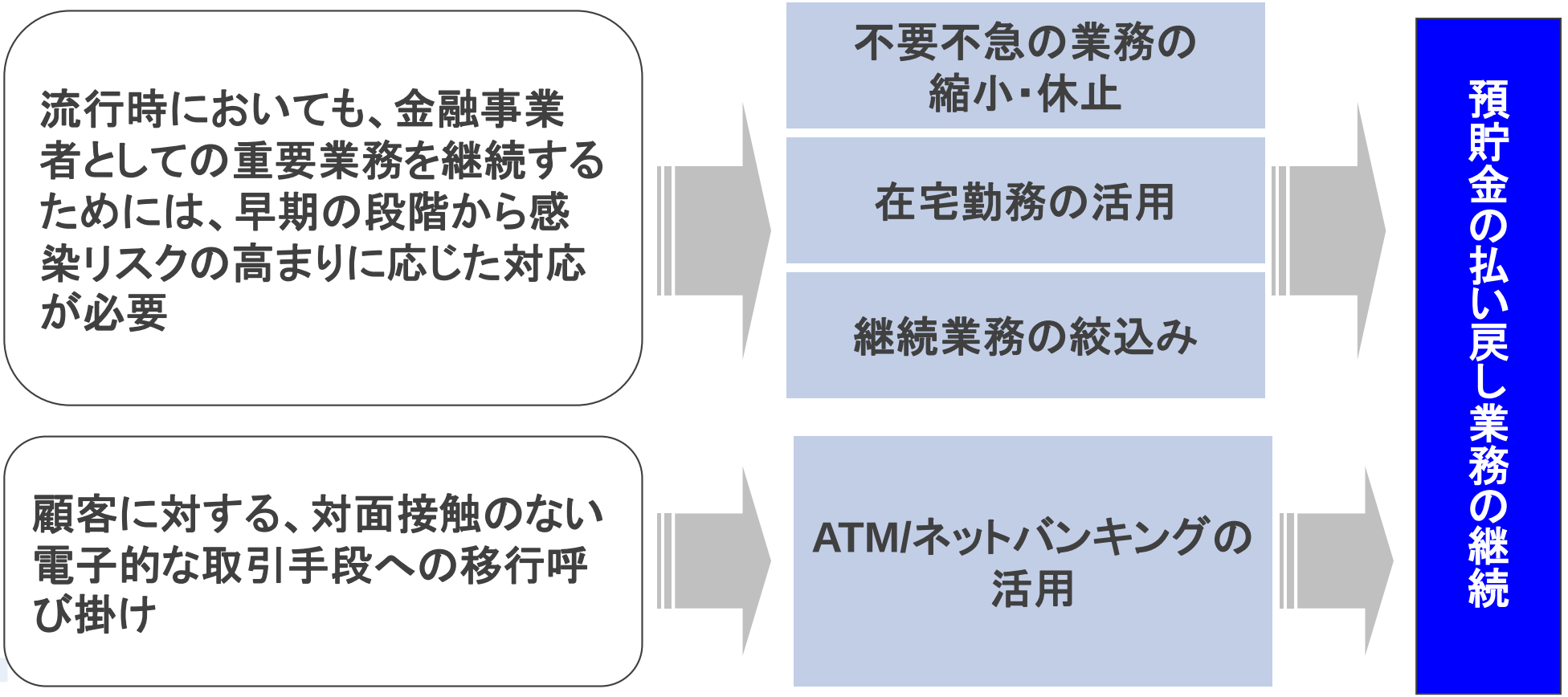
日本銀行では、2008年3月、金融機関に対し、パンデミックへの対応策としての手引きを配布しています。その中では、具体的な取組事例として5つの手順が挙げられています。

手順	推奨策
段階的な対策強化	WHOの感染拡大フェーズ等を参考に、局面を分類し、各フェーズにおいて決定実施すべき事項を策定すること
危機管理体制面での追加対応	一般的なBCPに追加する形で、特別な危機管理体制を構築すること ①関与部署の拡大 ②モニタリング体制の構築
感染拡大前の事前対応策	①衛生・予防面の強化 ②勤務面での特別措置 ③衛生医療用品の備蓄 ④システム面での準備対応
染拡大時の業務継続具体的手段	継続対象の業務を吟味し、感染リスクの少ない業務継続手法の準備 ①在宅勤務 ②スプリット・オペレーション（業務を二つ以上のチームに分けて遂行）
研修及び訓練	一般的なBCPとは異なるシナリオに基づく、特別の研修や訓練の実施 ①新型インフルエンザに対する正確な知識の社員への周知 ②クロストレーニングによる訓練（一人の社員が複数の業務を遂行）

出典：日本銀行「金融機関における新型インフルエンザ対策の整備について」を参考にNTTデータ経営研究所が作成

日銀ガイドラインからみたパンデミック対策の基本的考え方

ガイドラインの内容を確認すると、継続すべき最低限の業務を「預貯金の払い戻し」に絞り込んだうえで、業務を縮小・休止し、従業員に対しては在宅勤務の活用を、利用者に対しては、非対面取引（ATMやネットバンキング）の活用を促すよう求めていることがわかります



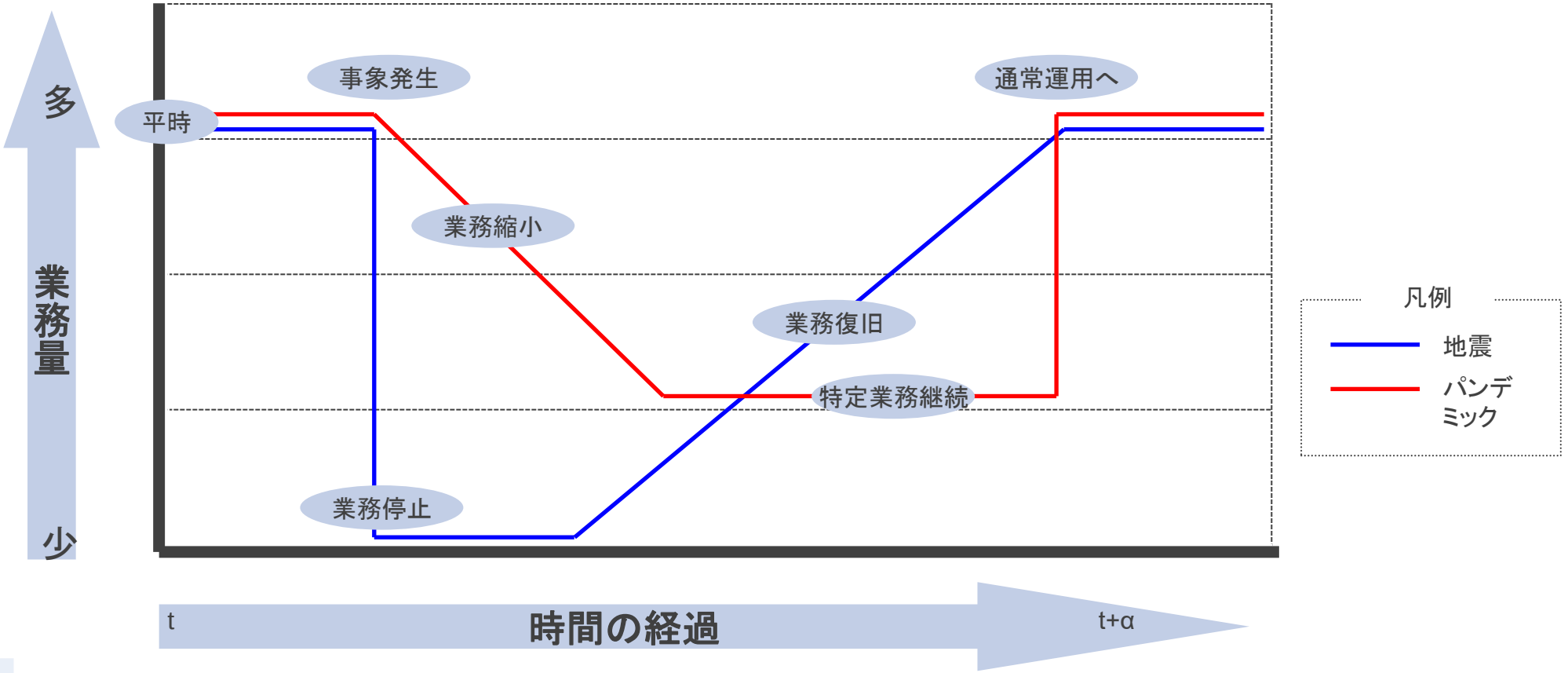
地震を想定したBCPと、パンデミックリスクを想定したBCPの差異

従来のBCPとは異なり、パンデミックリスクを想定したBCPでは、事前にリスクの予兆を察知できる可能性が残されており、対策も峻別して策定する必要があります。

	地震を想定したBCP	パンデミックを想定したBCP
予兆	予兆がなく被災する可能性が高い	事前に予兆を察知することが出来る場合が多い
システムへの影響シナリオ	物理的にシステムに影響を及ぼす可能性がある、もしくは、社会インフラが停止し（停電など）、システムの運用に影響を与える可能性がある	システムに直接的な影響はなくとも、人的被災を受け、間接的にシステム運用が困難になる可能性がある
リスクの継続期間	短期間で終焉する	長期間に亘って継続する
被害規模の把握	短期間で把握が可能な場合が多い	時間の経過とともに被害が拡大する可能性が高い
事業継続の段階的イメージ	想定リスク発生時に、オペレーションが停止し、時間の経過とともに、段階的に復旧し、平時の運用体制に戻る	想定リスク発生後、時間の経過とともに、コア業務を除いたオペレーションが段階的に停止し、リスク沈静後、平時に戻る。

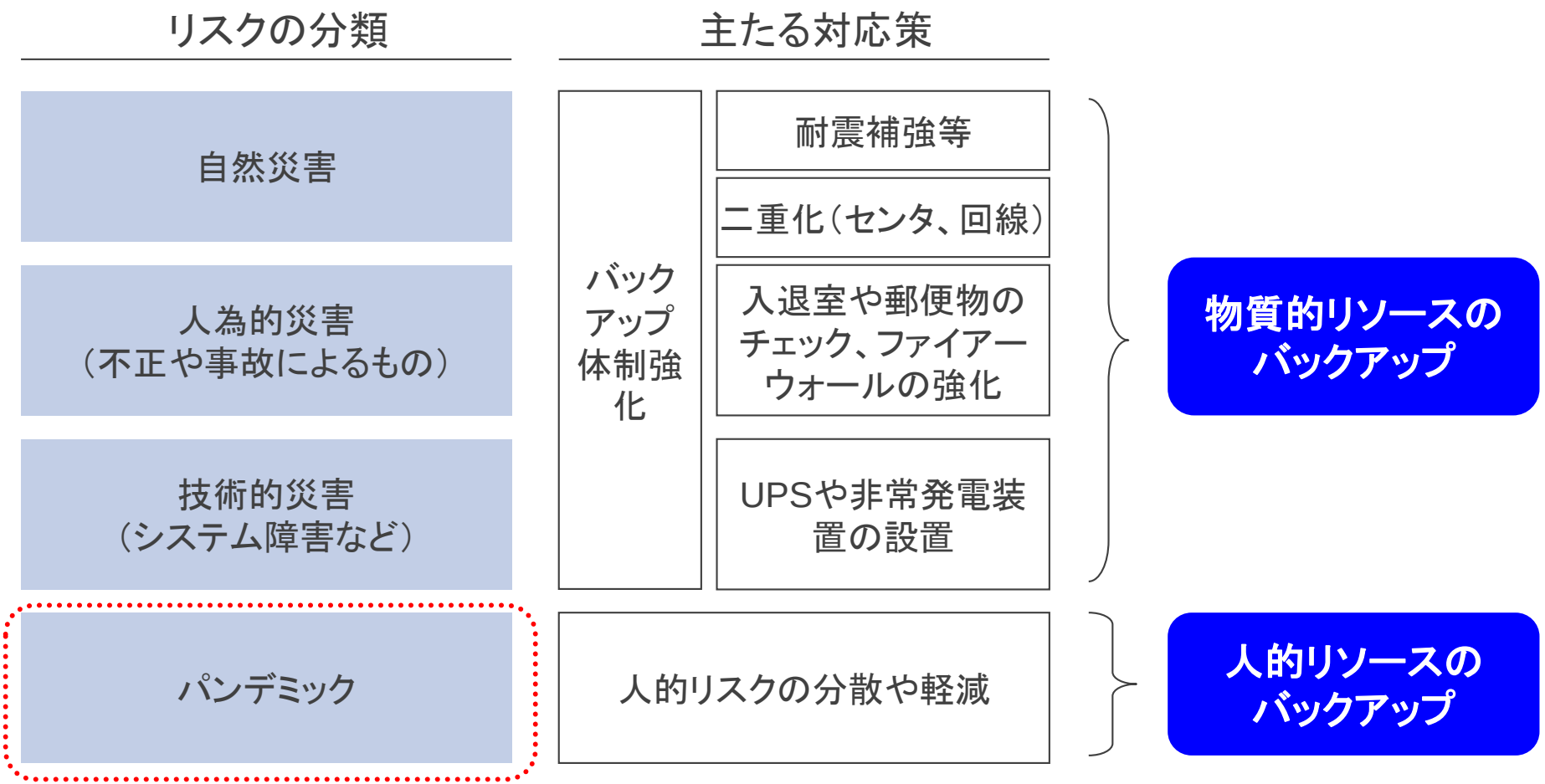
事象発生から通常運用への移行イメージの差異

大地震などの自然災害と、パンデミックとでは、事象発生から通常運用への復帰に至る過程が大幅に異なることがわかります



事業継続計画としてのパンデミック対策の特異点

- **他の災害との差異に着目したうえで、人的リソースのバックアップを中心とした対策を検討することが肝要です**



憂慮すべき事象と、対策立案の方向性

得られた示唆等も踏まえ、有事の際に実効性を高める対策の検討を進めることが肝要です

有事における表面的な事象	ポイント	対策の方向性
休業社員の多発	バックアップ要員の確保	俗人的なスキルの棚卸、暗黙知となっている手順のドキュメント化、教育の実施
	育児中の（主に）女性社員の就業支援策	在宅勤務を実現する環境の整備
事業所単位での業務停滞や閉鎖	事業所における顧客対応の支援	コールセンターの活用等による事業所における顧客対応のバックアップ
事業所間/社員間でのコミュニケーションの遮断	コミュニケーションツールの導入や連絡手続きのルール化	衛星携帯電話、テレビ会議システム、社員安否確認システムの活用
意思決定の遅延	意思決定者の順位付け	意思決定者を順位付けし、上位者に事故ある場合の意思決定メカニズムを確立

社内外にわたる人員不足を見越した事前準備

- 新型感染症流行時、人的リソースが不足することを前提とした事前準備を行うことが重要です

限られた人員の下でも継続すべき事業（重要事業）の選定

（不要・不急の事業の特定）

重要事業について、高い欠勤率での事業継続方法の検討

事業継続レベル（通常の稼働率の何割を確保するか）の検討

サプライチェーンからの物品、サービスの供給継続の可能性の検証

流行時の対応方針にかかるステークホルダーとの事前協議

名古屋銀行におけるパンデミック時の業務継続に向けた体制

	新型インフルエンザ発生段階（行内定義による）			
	第一段階	第二段階	第三段階	第四段階
	海外発生期	国内発生期	感染拡大 ～ 蔓延期	小康期
営業店	通常通り	営業継続（主要店）		
店内ATM	通常通り			
店外ATM	通常通り	一部稼動	休止	
必須業務	通常通り		縮小して継続	
重要業務	通常通り	縮小	休止	縮小、一部再開

資料：名古屋銀行公表資料を基にNTTデータ経営研究所が作成

名古屋銀行におけるパンデミック時の業務区分

業務区分	定義	業務
必須業務	国内での感染が拡大しても、継続させる業務 （状況に応じては、業務量を縮小）	預金取引（ATM）、事業性貸付（実行、審査）、個人ローン（実行、審査）、内国為替（ATM、IB）、手形交換、給与関連等
重要業務	国内での感染初期段階において、業務範囲を縮小させつつも継続させるものの、感染拡大時には休止する業務。	預金取引（店頭）、事業性貸付（契約変更）、個人ローン（契約変更）、内国為替（店頭）、投資信託等

店頭業務は大幅縮小するが、店内ATM、貸付の実行は死守

コロナ禍で増加するサイバー犯罪への対応

増加するサイバー攻撃

□自宅のルーター攻撃が大規模に発生
（テレワーク環境がターゲット）

□ 金融機関と顧客との間でサービスを提供するフィンテック事業者をターゲットとした攻撃が増加

□ 国内初の大規模なマイナンバー窃取事案の発生
（FX事業者）

テレワーク実施に際しての留意事項

テレワーク実施に際しては、通信環境の点検が欠かせません

□公衆Wi-Fiを利用した社内システムへの接続はしない
（ホテルや喫茶店などが提供する環境は要注意）

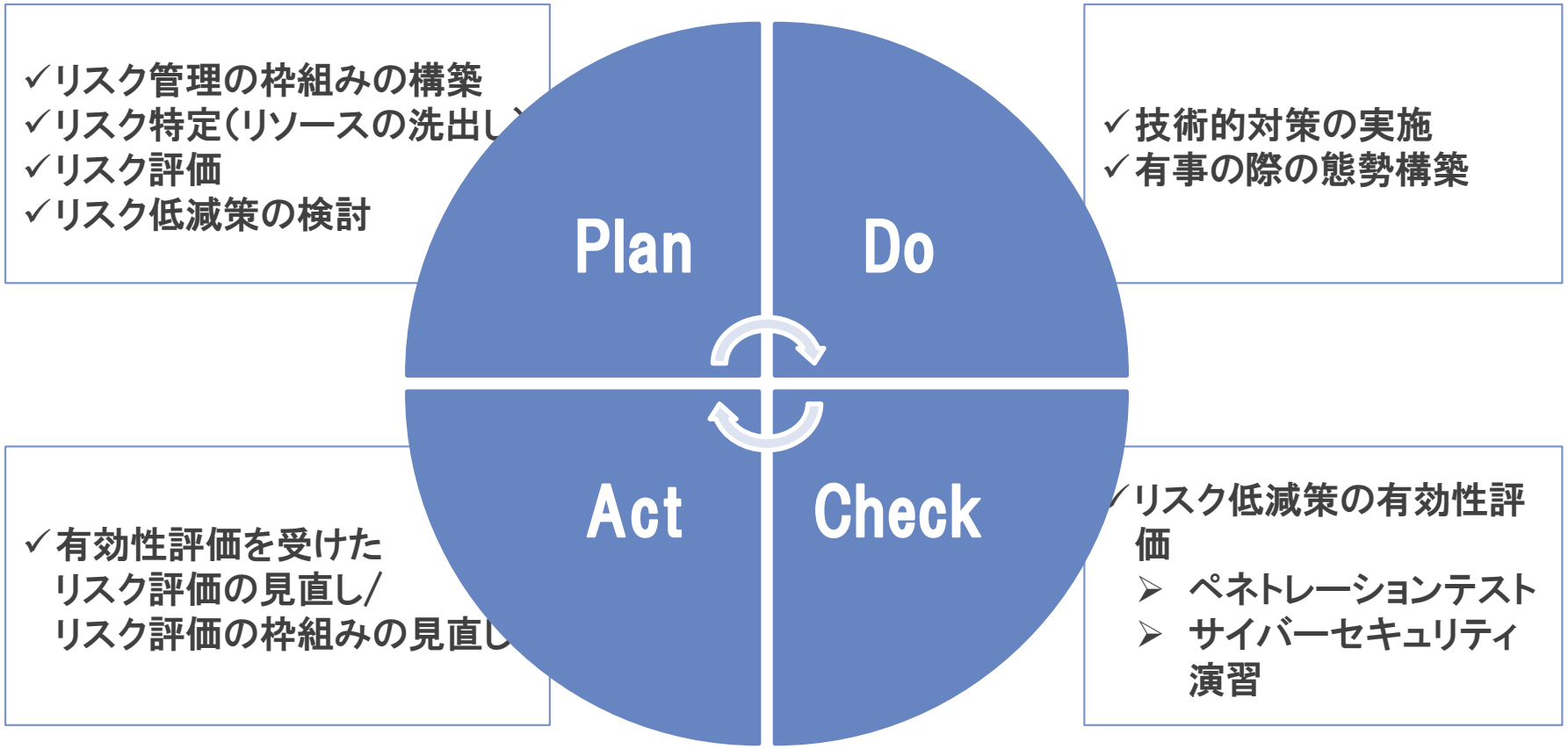
□利用するウェブ会議システムは安全か？
（特定のウェブ会議システムには脆弱性も）

□FAT端末の利用は極力避ける
（シンクライアント端末の利用を前提）

サイバーセキュリティにおけるPDCAサイクルの概観

金融庁が要請しているとおり、サイバーセキュリティにおいては、リスクベースドアプローチを念頭に、PDCAサイクルを自社で構築することが求められます。今回はサイバーセキュリティの態勢構築に向けた一連の流れを解説します。

サイバーセキュリティにおけるPDCAサイクルのイメージ



「PLAN」では４つのステップでリスク評価が必要です。

リスク管理の枠組みの構築

Point
- ✓ 経営陣の関与
- ✓ 組織体制の整備

リスクの特定

Point
- ✓ 自社のリソースを網羅的に洗出し

リスク評価

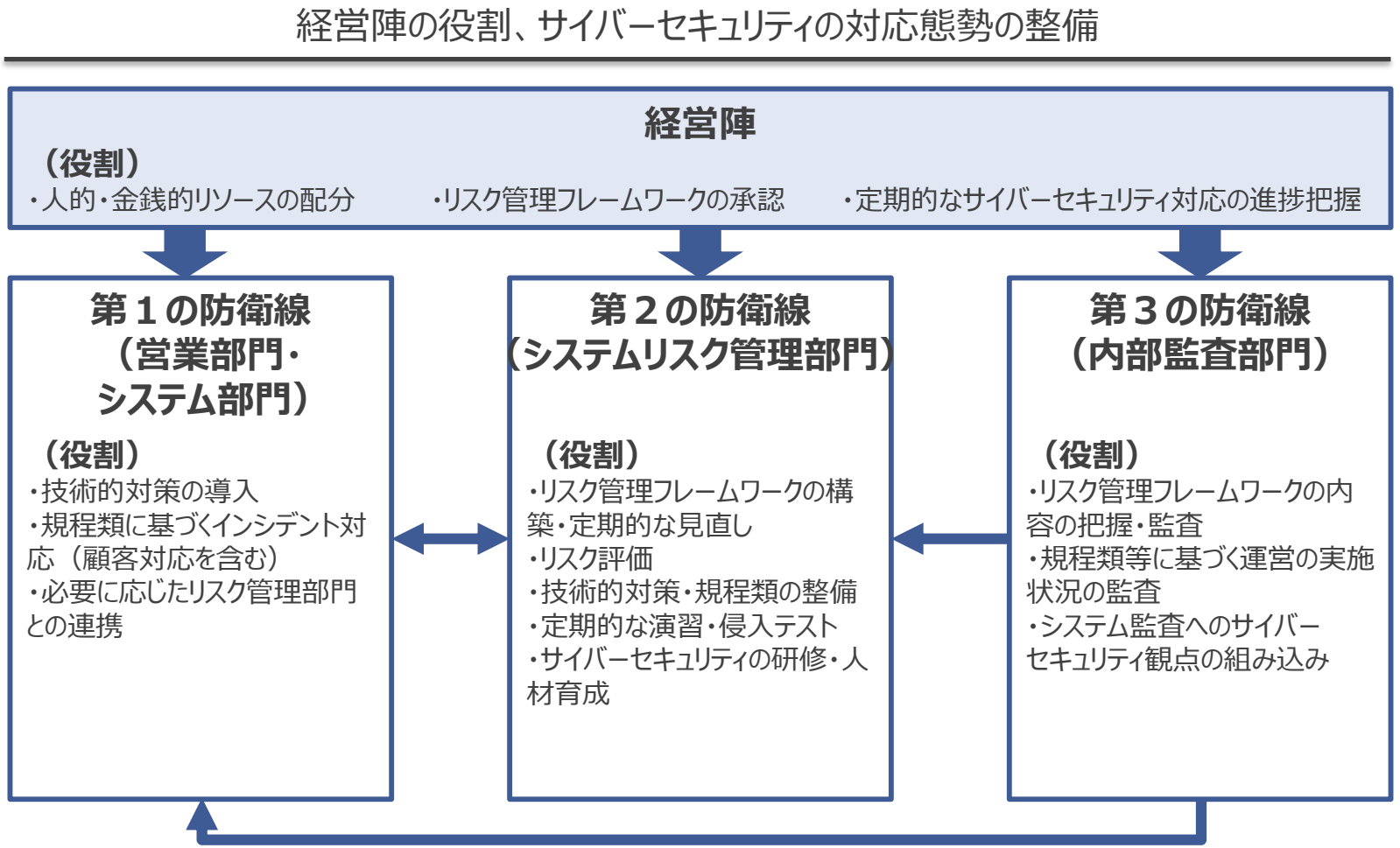
Point
- ✓ 内部に加え、外部の脅威情報を活用したリスク評価
- ✓ 外部委託先も評価

リスク低減策の検討

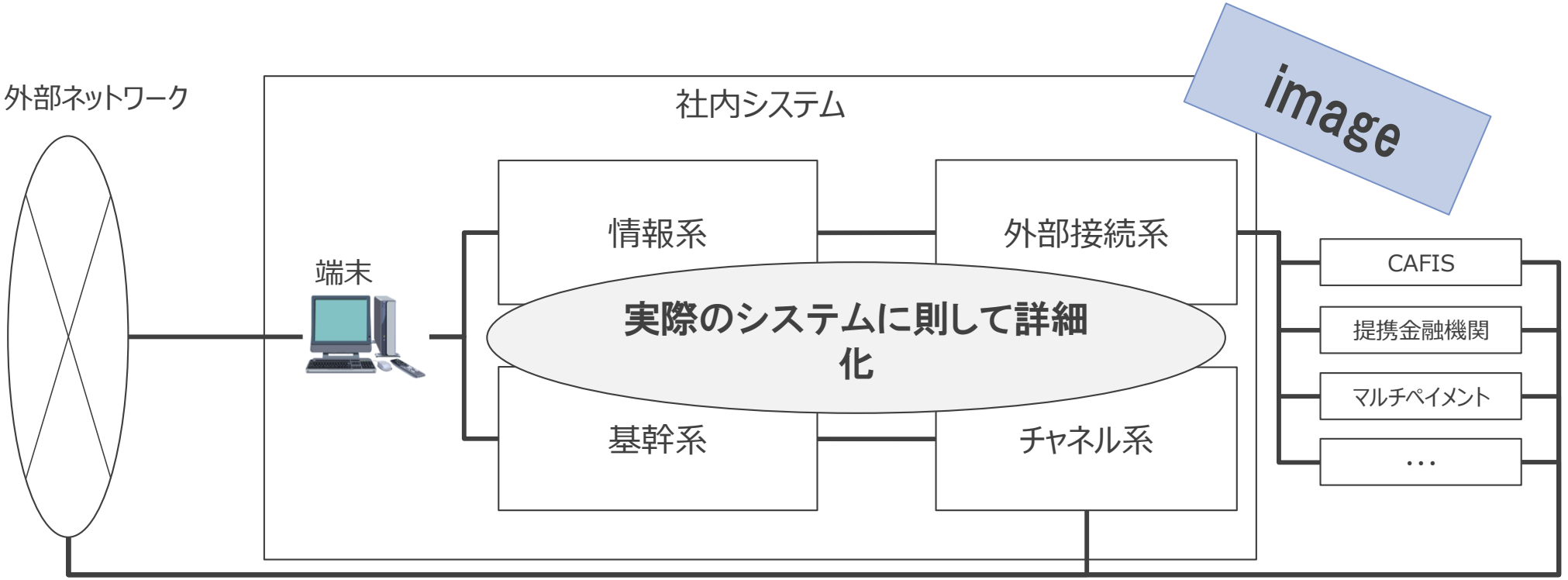
Point
- ✓ リスク評価の結果優先度の高いと判断した対象をまずは検討

PLAN～リスク管理の枠組みの構築～
サイバーセキュリティにおける３線管理（Three Lines of Defense）

リスク管理の枠組みの構築では、３線管理による牽制機能を意識した仕組みの構築が求められます。また経営陣はこうした全てのプロセスを監督することが求められます。



リスクの特定においては、自社のITリソースを漏れなく抽出することが求められます。情報資産管理台帳、システム構成図といったサイバーセキュリティリスク管理の基礎となるシステムリスク管理態勢の整備が欠かせません



情報資産管理台帳、システム構成図の作成は必須要件
⇒システムリスク管理の枠組みのうえにサイバーセキュリティリスク管理が成り立っている

リスクの評価～外部情報の収集～

金融庁では、サイバー攻撃は日々高度化・巧妙化するという考えから、外部機関等を活用した情報収集を行うよう求めています。ここでは金融ISACを除く脅威情報の提供先を示しています。
こうした外部機関の情報を分析することが求められます。

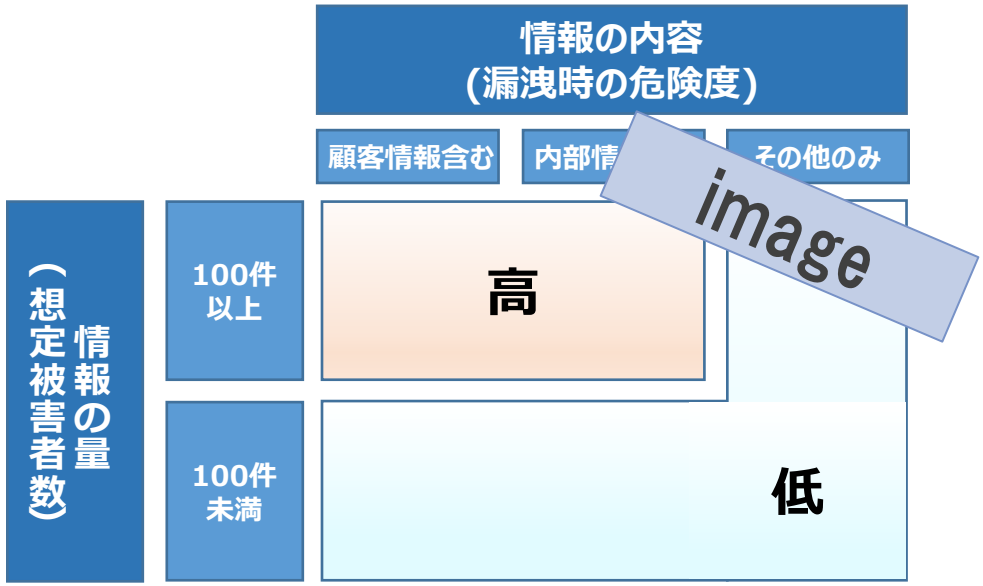
	収集先名	収集対象とする脅威情報	URL等
1	独立行政法人 情報処理推進機構 （IPA）	・各種の重要なセキュリティ情報 ・セキュリティに係る各種の調査報告書 ・セキュリティ対策	https://www.ipa.go.jp/
2	JPCERT/CC	・インシデント対応 ・注意喚起 ・インターネット定点観測システムの運用 ・脆弱性情報	http://www.jpcert.or.jp/
3	フィッシング対策協議会	・フィッシングサイト・フィッシングメールの情報収集 分析・共有	・https://www.antiphishing.jp/
4	日本サイバー 犯罪対策センター （JC3）	・サイバー犯罪の情報・知識・経験・ノウハウ ・サイバー犯罪の脅威情報、犯罪者の追跡・特定	https://www.jc3.or.jp/index.html

他の業態ではCEPTOARを設立し、金融庁が提供する注意喚起情報を共有する枠組みを構築

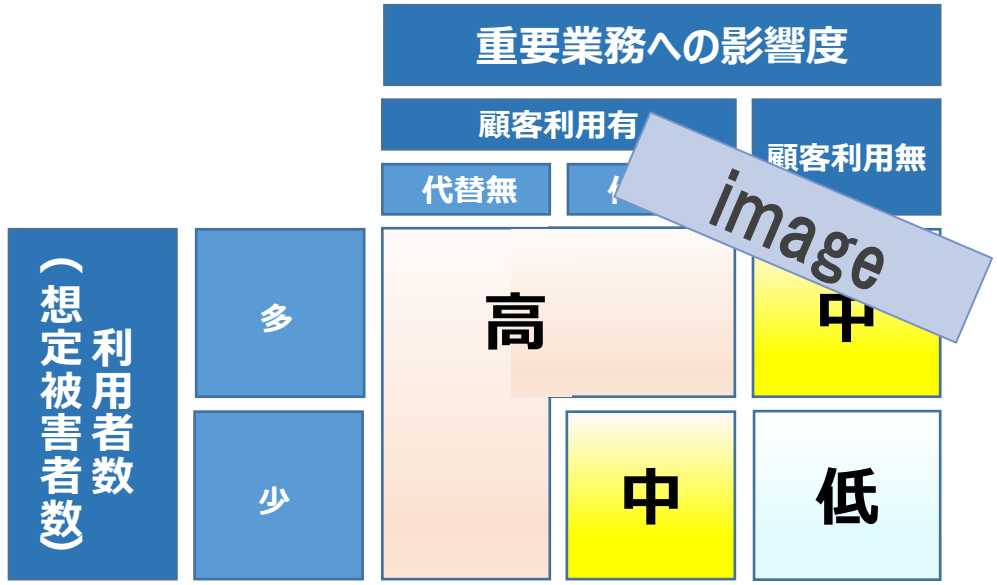
リスクの評価～内部の評価（ITリソース）～

リスク評価では、サイバー攻撃の被害を想定した、情報窃取、サービスへの影響等の評価軸を定め、自社のITリソースの対応優先度を付与することが求められます。またリスク評価は評価者に寄らない評価基準を定めておくことが望ましいと考えます。

情報窃取の評価



顧客サービスへの影響の評価



評価の視点は評価者によらない評価基準を設けておく必要

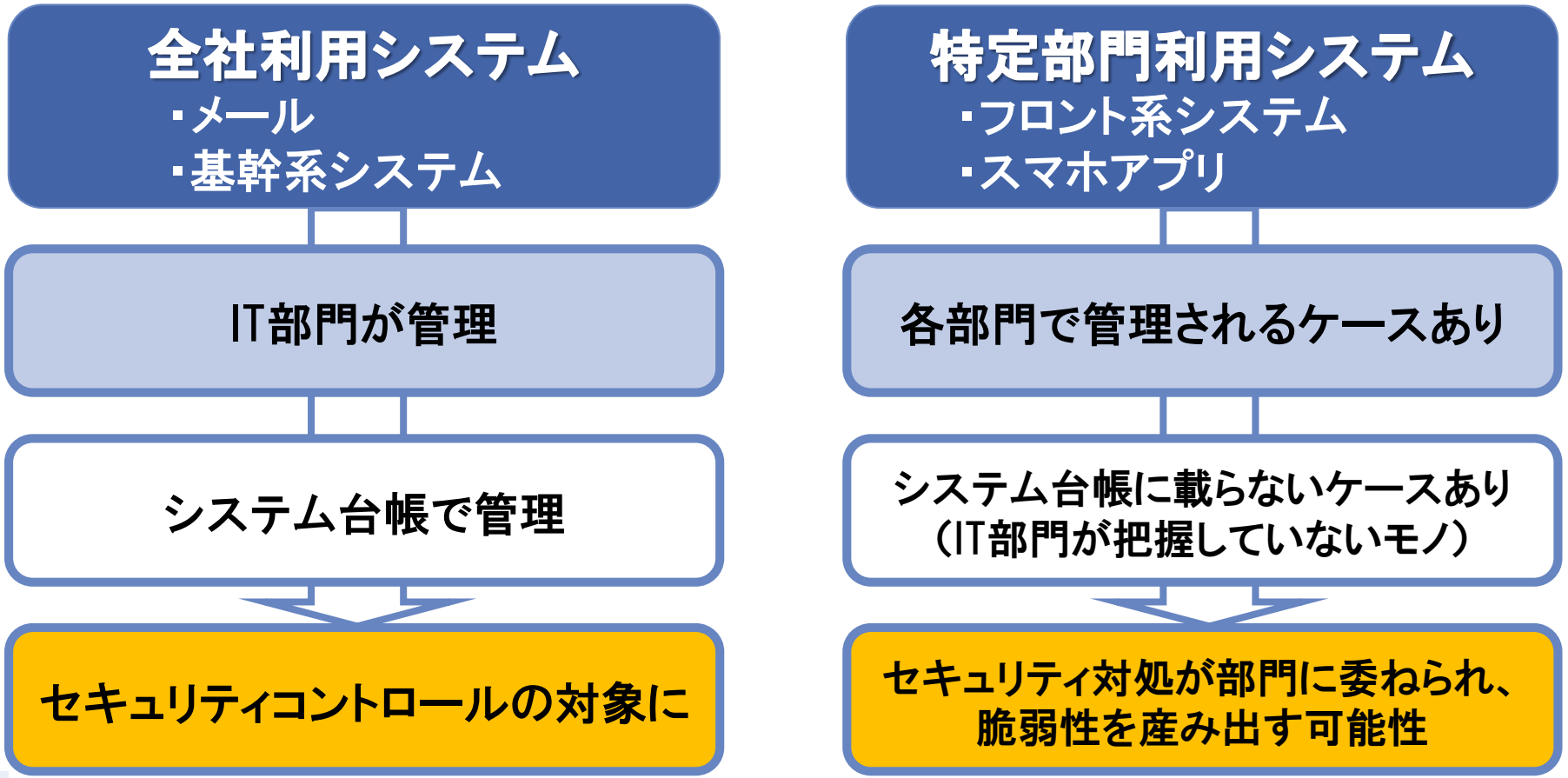
リスクの評価～サードパーティーリスク～

最近では、自社のシステムでの構築ではなく、外部のサービスの利用や接続等、外部委託先との連携が一般化してきています。こうしたことから、サードパーティーリスクといった概念を考慮する必要があり、単に外部委託先のサービスの評価にとどまらない視点での委託先管理が求められています。

対象	想定される事象
経営陣	✓ 経営陣のコンプライアンス意識が希薄 ✓ 公私の峻別がついていない
株主・資本関係	✓ 知らない間に株主が代わっていた/増えていた ✓ 怪しげな企業と提携していた
情報システム	✓ 情報システムの運用が不安定でトラブルが多い ✓ 情報システムのセキュリティに課題がある
意思決定	✓ 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 ✓ 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	✓ 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） ✓ 導入予定もしくは開発していた技術が実現されない ✓ 想定していた収益を確保することができない ✓ 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	✓ 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 ✓ 経営層のリスク管理の意識が希薄だった

シャドーIT（システム部門が管理していないITサービス）の増加

業務部門が外部のサービスを独自に利活用することで、システム部門が把握しにくいシステム構成となっている場合（シャドーIT）もあります。この場合、システム部門の所管外であることが多く、情報資産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。



口今年度より、中央省庁における委託先管理が厳格化

- 委託先事業者そのもののチェック
- 委託先事業者の経営者、作業従事者のチェック
- 重要なシステムの開発事業者のチェック

サードパーティーリスクの点検項目

提携当初のチェックに加え、経営様態が短期間に変わる可能性を念頭に、定期的な監査を行うことが必要となります。まずは、最低限必要な相手先企業の情報収集が欠かせません。

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

リスク評価の結果、重要度が高いと判断されたシステムについてはリスク低減策を検討する必要があります。リスク低減策は大きく、技術的対策の視点、態勢構築の視点に分かれます。

技術的対策の視点

- 脅威情報から不足する対策はないか
- ITリソースの評価結果で重要度が高いITシステムに不足する対策はないか
- 外部委託先は健全にリスクをコントロールできているか

態勢構築の視点

- 経営陣が関与する管理の枠組みを構築できているか
- リスク評価の枠組みは規程に定められているか
- 万が一攻撃を受けた場合を想定した、インシデント対応は規程に定められているか

技術的対策の検討

技術的対策の検討では、金融庁の監督指針にもあるとおり、「入口対策」、「内部対策」、「出口対策」の視点が求められます。「内部対策」では、見落としがちである内部犯行の視点も考慮しておく必要があります。

入口対策

- ✓ 外部との接点について、不正侵入を防ぐ仕組みが導入されているか

内部対策

- ✓ 内部で攻撃が拡散することを防ぐ仕組みが導入されているか
- ✓ **内部犯行を想定した対策**を講じているか
  （サイバー攻撃の事例をみると、人間系が入口となるケースが多い）

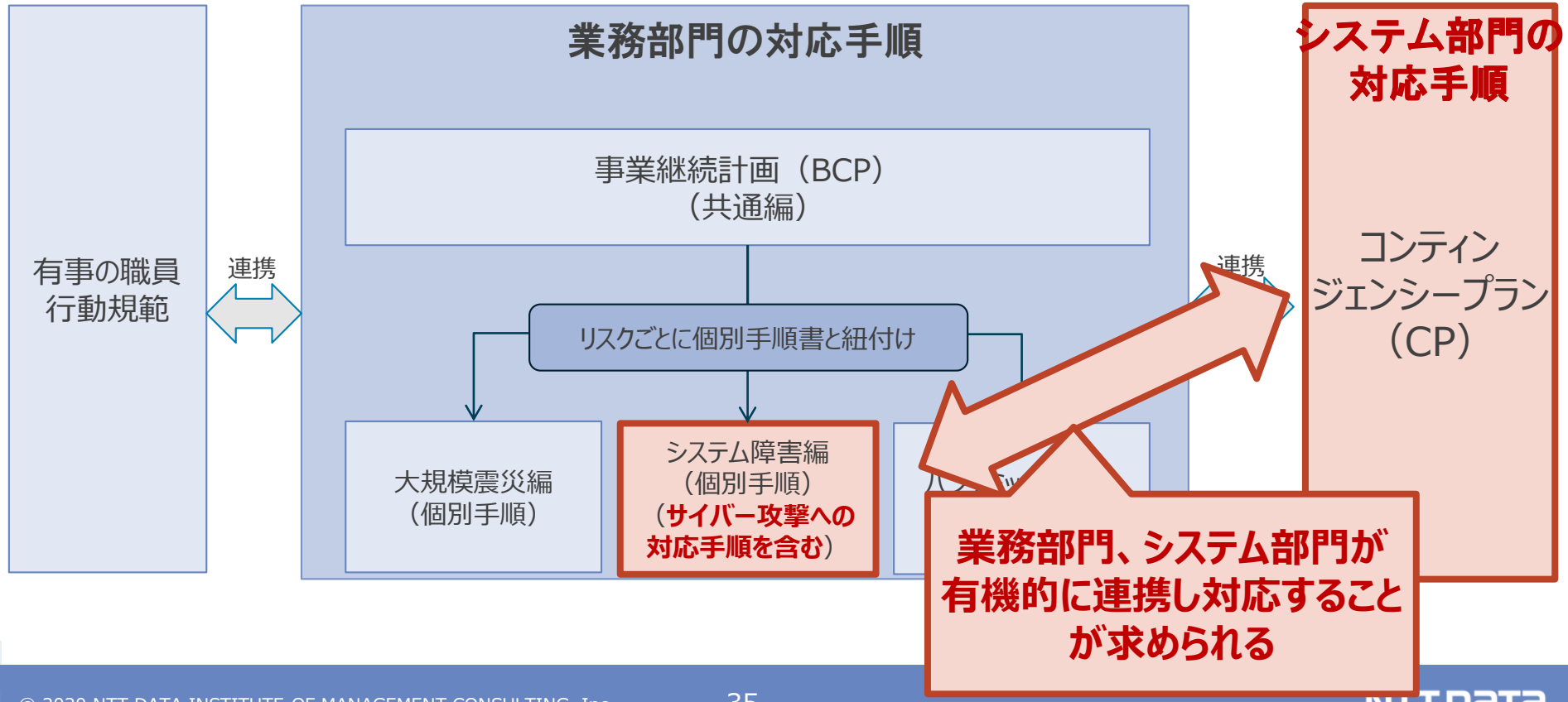
出口対策

- ✓ 外部へのデータ流出を防ぐため、監視する仕組みが導入されているか

コンティンジェンシープランの策定

態勢構築では、万が一サイバー攻撃を受けた場合を考慮し、コンティンジェンシープランにサイバーセキュリティの対応マニュアルを追加しておく必要があります。また、システム部門の対応手順にとどまらず、業務部門との連携が必要であることも考慮すべきです。

BCPとコンティンジェンシープランの関係



コンティンジェンシープラン（サイバーセキュリティ）の策定（1/2）

コンティンジェンシープラン策定の際の視点を整理しています。

	対象	観点	内容
対応手順策定に関する視点	1. 基本方針の作成	• インシデントの想定状況	• 様々なインシデントを想定し、リスクの大きくなりそうなものに焦点を当て、対策を検討しているか
		• 対策本部の立上げ手順	• 対策本部の立上げ手順を策定しているか
		• 対策本部の要員確保	• 対策本部のメンバー、参集ルールを策定しているか
	2. 有事の際の有効性確保に向けた手順の可視化	• BCPの実効性	• 対応手順の有効性を高めているか
	3. BCMの実装状況	• 教育・訓練の実施状況	• コンティンジェンシープランの定着化に向けた教育・訓練の計画を立てているか
		• 対応手順の更新プロセス	• コンティンジェンシープランそのものの見直しを検討できているか

コンティンジェンシープラン（サイバーセキュリティ）の策定（2/2）

特にインシデント対応手順では、システムの対処手順にとどまらず内部・外部としかるべきタイミングで連携できる手順となっているかも考慮すべきポイントです。

	対象	観点	内容
有事のサイバーセキュリティ対応に関する視点	1. 態勢整備	• インシデントの想定	• 複数のインシデントを想定し、判断基準・対応手順が整備されているか
		• 態勢構築	• 攻撃予告を受けた場合の態勢構築、内部での検知・外部からの報告を受けての態勢構築について定義されているか
		• 暫定対処	• 複数のインシデントに応じた暫定対処方法について定義されているか
	2. 攻撃対応手順	• 内部連携	• 対応の中心となる主体からの内部連携方法が定義されているか
		• 外部連携	• 対応の中心となる主体からの外部連携方法が定義されているか
	3. CPへの移行	• 復旧手順(CP)への移行	• サイバー攻撃により個別システムの障害が生じた場合を想定し、個別システム別の復旧手順書とサイバーセキュリティに関する手順書との棲み分けが定義できているか

コンティンジェンシープランによくみられる問題点

弊社では金融機関のコンティンジェンシープランのアセスメントサービスを行っています。コンティンジェンシープランによくみられる問題点を整理しました。

手順が詳細化されておらず実効性が乏しい	✓ インシデント対応の作業概要は記載されているものの、**詳細な手順が記載されておらず、実際に利用可能な手順となっていない**
顧客への対応が意識されていない	✓ **業務部門との連携が意識されておらず**、単にシステムの暫定対処、復旧対処のみを記載している
誰がやるのかが分からない	✓ 対応手順としては記載されているものの、対応者が不明確であり、実際に利用可能な手順となっていない（**内容によっては経営陣の判断を伴うことを意識**）
定期的に見直されていない	✓ 新サービスを導入したにもかかわらず、**対応手順が更新されておらず、実際の対応とは乖離**している

技術的対策の妥当性・十分性を評価するために、脆弱性診断、ペネトレーションテスト、TLPT等の手段があります。
特に実際に攻撃を仕掛けるTLPTについては、FISCより手引書が出ていますので、次ページ以降で概要を解説します。

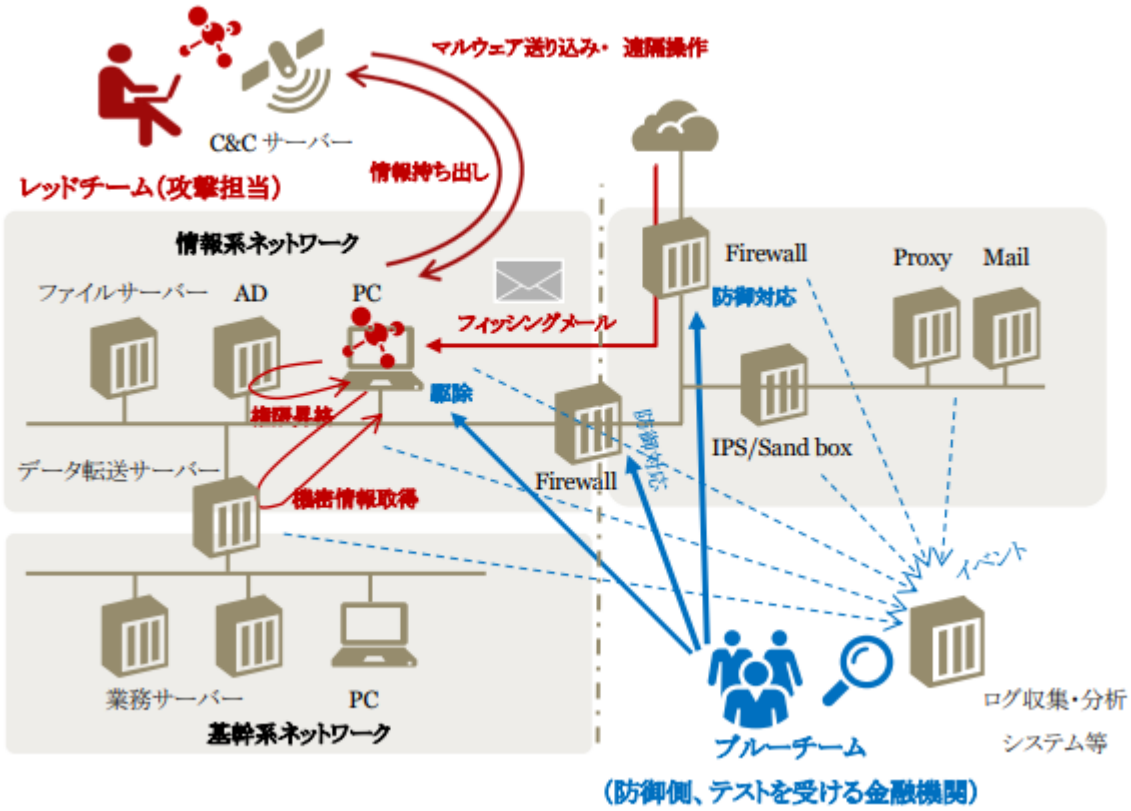
種類	対応内容	個社の関与	ITベンダーの関与
脆弱性診断	✓ OS、ミドルウェアに脆弱性を持つ(パッチ未適用)ソフトがないかを診断	×	○
ペネトレーションテスト	✓ システムに侵入を試み、システムの脆弱性がないかをテスト	×	○
脅威ベースのペネトレーションテスト(TLPT)	✓ 脅威情報を基に実際にシステムに攻撃を仕掛け、防御、インシデントレスポンス等を実施	○	○

(出所)FISC「金融機関等におけるTLPT実施にあたっての手引書」を基にNTTデータ経営研究所にて作成

ペネトレーションテスト～TLPT（脅威ベースのペネトレーションテスト）～（1/2）

TLPTは、レッドチーム（攻撃側）、ブルーチーム（防御側）に分かれてペネトレーションテストを行うもので、ブルーチームは攻撃箇所を含むシナリオが開示されていない状況で、検知、インシデントレスポンス（システム対応が中心）を実施するものです。

図 2-1 脅威ベースペネトレーションテストのイメージ



（出所）金融庁「諸外国の『脅威ベースのペネトレーションテスト（TLPT）』に関する報告書」

ペネトレーションテスト～TLPT（脅威ベースのペネトレーションテスト）～（2/2）

FISCの手引書を確認すると、TLPTは実際のシステムの脆弱性を確認できるとともに、技術的な対処の一部訓練が可能です。ただし、あくまでシステム部門の対処にフォーカスしているとご理解ください（**業務部門や顧客対応の手順については確認できない**）。

		金融機関	サービス提供者
工程1	計画(準備)	➢ TLPT予算確保、PJT発足 ➢ TLPTのスコープ(対象システム)検討 ➢ サービス提供者の選定	
工程2	シナリオ構築	➢ 攻撃によるリスクの検証	➢ 脅威情報の分析 ➢ 攻撃シナリオの検討 ➢ 攻撃によるリスクの検証
工程3	テスト実施	➢ テスト実施(ブルーチーム) ➢ テスト結果報告受領	➢ テスト計画の作成 ➢ テスト実施(レッドチーム) ➢ テスト結果報告書作成
工程4	評価・改善計画の策定	➢ テスト結果による課題の導出 ➢ 技術的対処の改善計画の策定・承認	

(出所)FISC「金融機関等におけるTLPT実施にあたっての手引書」を基にNTTデータ経営研究所にて作成

サイバーセキュリティ演習は規程類の実効性を確認することを目的に実施します。金融庁のDeltaWallは「情報連携テスト」と「オープンテスト」「ブラインドテスト」を組み合わせています。

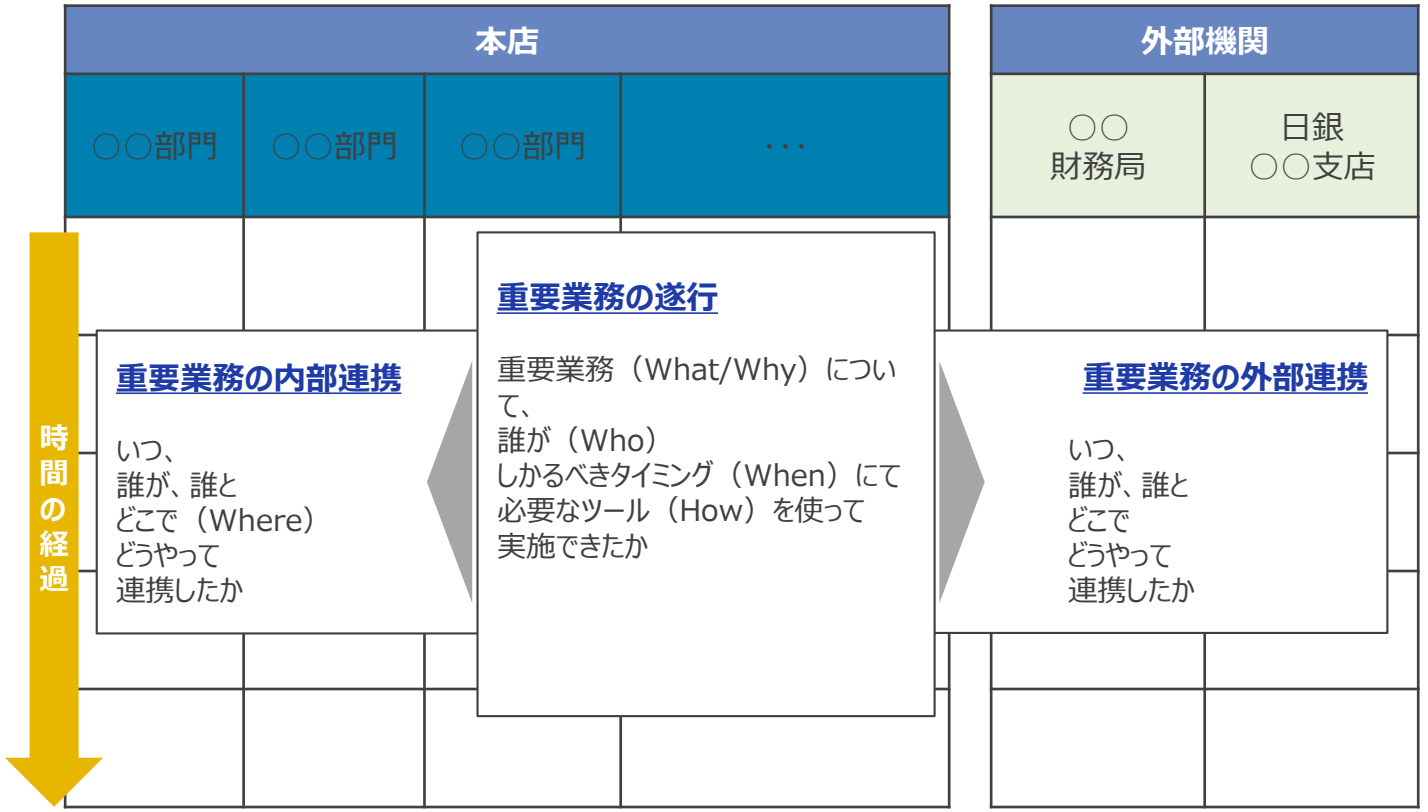
種別	目的
ドキュメントウォークスルー（内部組織のみ）	✓CP関連ドキュメントを内部関係者で読み合わせ、隠れた瑕疵を抽出する ✓関係者間での有事対応の意識合わせを実施する
ドキュメントウォークスルー（外部組織を含む）	✓外部組織を交え、隠れた瑕疵を抽出する ✓外部組織との間で、有事対応の意識合わせを実施する
情報連携テスト	✓関係者間でのツール（電話、メール、電子掲示板、その他）を用いた連絡訓練を実施し、伝達時間や連携ツールの在り方などを確認する
オープンテスト（内部組織のみ）	✓用意されたシナリオに基づき、内部関係者のみに限定し、実地訓練を実施する
オープンテスト（外部組織を含む）	✓用意されたシナリオに基づき、外部組織を交えて、実地訓練を実施する
ブラインドテスト（内部組織のみ）	✓事前にシナリオを開示することなく、内部組織のみに限定し、実地訓練を実施する（訓練目的、訓練日時などのみを開示）
ブラインドテスト（外部組織を含む）	✓事前にシナリオを開示することなく、外部組織も交え、実地訓練を実施する（訓練目的、訓練日時などのみを開示）

演習では、マニュアルに規定されている業務が抜け漏れなく、正しいカウンターパートに対して適切に実行されているか、をチェックした上で、そのプロセス及び結果における改善すべき点の有無を確認致します。
以下では実際の評価ポイントを簡略化して紹介しています。

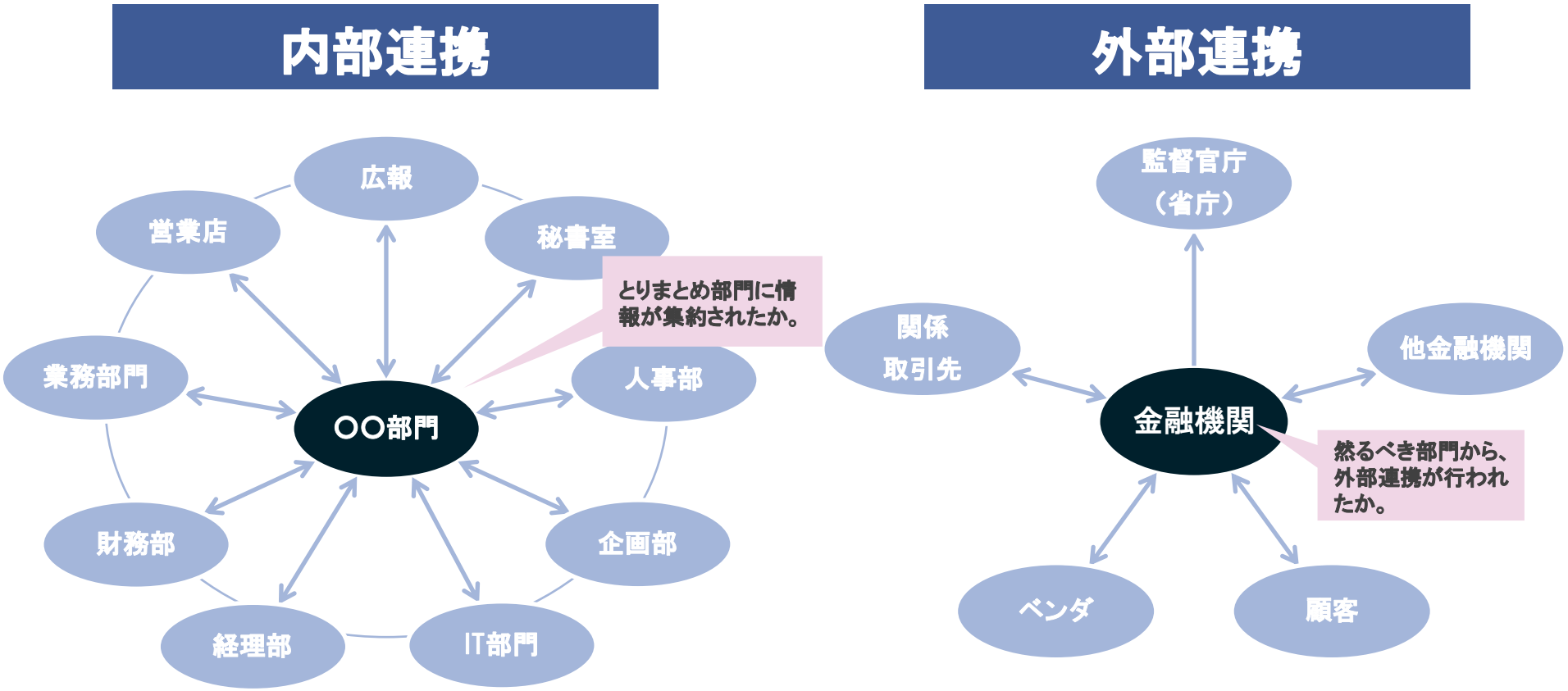
評価の視点

評価視点	確認項目
①重要業務の遂行	✓共通の重要業務が円滑に実施されているか ✓各部個別の重要業務が円滑に実施されているか
②重要業務の内外連携	✓連携先は明確か ✓連携のタイミングに齟齬はないか

確認ポイント



初動対応やその後の業務継続まで、状況の把握が必要不可欠となります。演習においては、「適切なタイミングに、適切なツールを用いて、内外連携を行えたか」をチェックします。



サイバーセキュリティ演習～演習でよくみられる問題点～（1/2）

サイバーセキュリティ演習では、手順に記載されていないことから、実施されない問題点が散見されます。一次情報の点検、攻撃を受けた場合の影響評価、攻撃に関する情報収集、必要な外部機関との連携、等が見落とされています。

一次情報の点検が未実施	✓ 予告や攻撃の情報を受けた場合、一次情報の点検が必要です（単なるイタズラか否かの見極め）
もしものケースを想定した影響評価がなされていない	✓ 攻撃予告であったとしても、実際に攻撃を受けた場合を想定したうえで、リソース・業務・顧客に与える影響を評価する必要があります
攻撃に関する情報収集がなされていない	✓ 攻撃が及ぼす被害や攻撃の特徴について、外部機関を活用して情報収集することが求められます
外部機関やステークホルダーとの連携が検討されていない	✓ 実際に攻撃を受けた場合を想定したうえで、ITベンダーを含めた外部機関・ステークホルダーとの連携を強化しておくことが望まれます

サイバーセキュリティ演習～演習でよくみられる問題点～（2/2）

また各作業フェーズにおいて求められるはずの経営陣の関与がみられないケースも認められます。
併せて、顧客への影響を評価のうえ、対外情報発信も含めた顧客対応を実践する必要があります。

攻撃状況の継続的な監視がなされていない	✓ 攻撃は一度で止むとは限りませんので、他のシステムにも攻撃対象が拡大することを念頭に、監視態勢を強化する必要があります
経営陣の関与が「みえない」	✓ 場合によっては有事対応手続きである「BCPの発動」へとシフトする可能性があるはずです。これを念頭に、経営陣への情報エスカレーションを契機とした各作業フェーズにおける経営陣の関与を明確化する必要があります
影響度評価がなされていない	✓ 攻撃が、顧客・業務・その他のリソースにいかなる影響を与えるのか？といった視点での評価作業が求められます
顧客対応が実施されていない	✓ 顧客に対し、どのような情報を提供すべきか、本店及び営業店ごとに、あるいは対外情報発信のあり方も含めて検討・実施する必要があります

ペネトレーションテスト、サイバーセキュリティ演習の結果から見えた課題を、改善計画として取りまとめることが肝要です。また併せてリスク評価の枠組みに問題がないかも点検しておく必要があります。最後に改善計画を経営陣に承認を得ることがPDCAサイクルの構築には不可欠です。

有効性評価の結果を受けた課題

【ペネトレーションテスト】
不足する技術的対策　等

【サイバーセキュリティ演習】
不足する対応手順　等

改善計画の策定

【視点1】
✓ 技術的対策の追加対応

【視点2】
✓ コンティンジェンシープランの改善

【視点3】
✓ そもそもリスク評価の枠組みに問題ないか

年間計画等に整理し、経営陣に承認を得る（リソースの獲得）

サイバーセキュリティに関する内部監査

３線管理の考えに基づき、内部監査部門は、サイバーセキュリティに関する視点を評価することが求められます。

内部監査の視点（イメージ）

リスク評価に関する視点	✓ リスク評価の枠組みに経営陣が関与・承認しているか ✓ 内部リソース、外部脅威情報を網羅的に評価しているか ✓ 外部委託先のリスクを評価しているか ✓ リスク低減策に漏れはないか
リスク低減策に関する視点	✓ 予算・人的リソースに不足がないか ✓ 技術的対策、規程類の整備に関する計画は経営陣に承認されているか ✓ 計画通りに対策を実行しているか
有効性評価に関する視点	✓ ペネトレーションテストを定期的に実施しているか ✓ サイバーセキュリティ演習を定期的に実施しているか
改善に関する視点	✓ ペネトレーションテスト、サイバーセキュリティ演習の結果から浮き彫りとなった課題への対応を整理しているか ✓ リスク評価の枠組みは有効性を担保できているか ✓ 改善計画をまとめ、経営陣に承認されているか

金融庁では、自助・共助・公助の観点についてサイバーセキュリティ対策検討時から重要視しています。特に共助の観点は、業態独自の対応も可能であり、こうした取組を検討いただくことも個社の支援には有効と考えます。

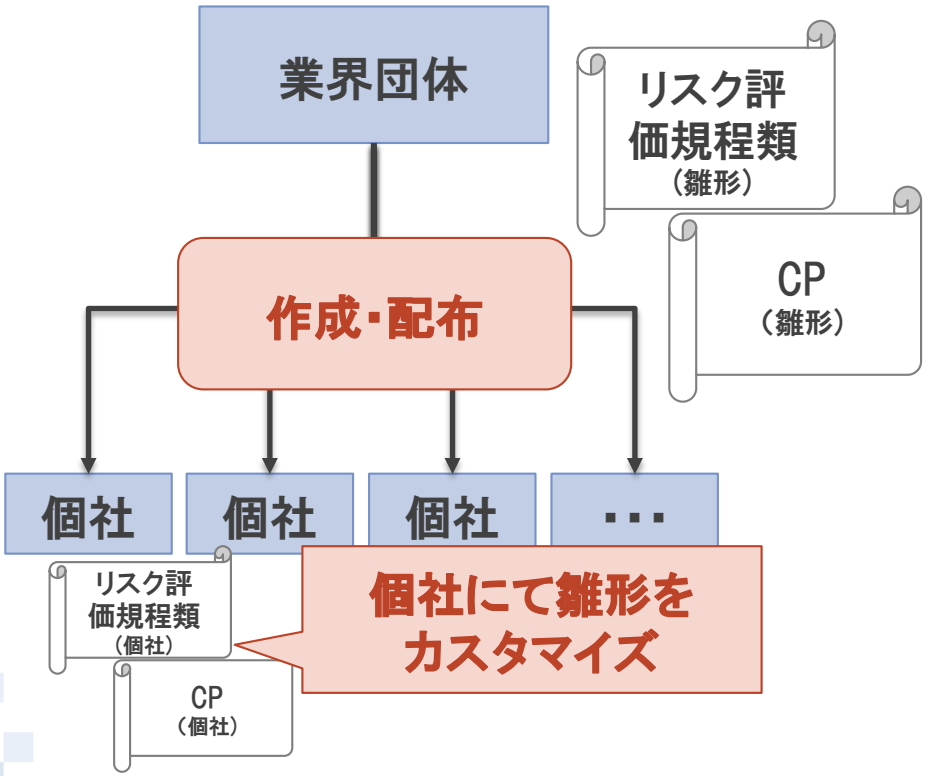
共助により対応可能なテーマ

PLAN	□ リスク評価関連規程類の雛形の配布	事例をご紹介
	□ 脅威情報の提供	
	□ 外部委託先管理手順の雛形の配布	
DO	□ コンティンジェンシープランの雛形の配布	事例をご紹介
	□ 既に作成済みのコンティンジェンシープランのアセスメント	
CHECK	□ 業態内のサイバーセキュリティ演習の実施	事例をご紹介
ACT	（個社の対応のため、なし）	

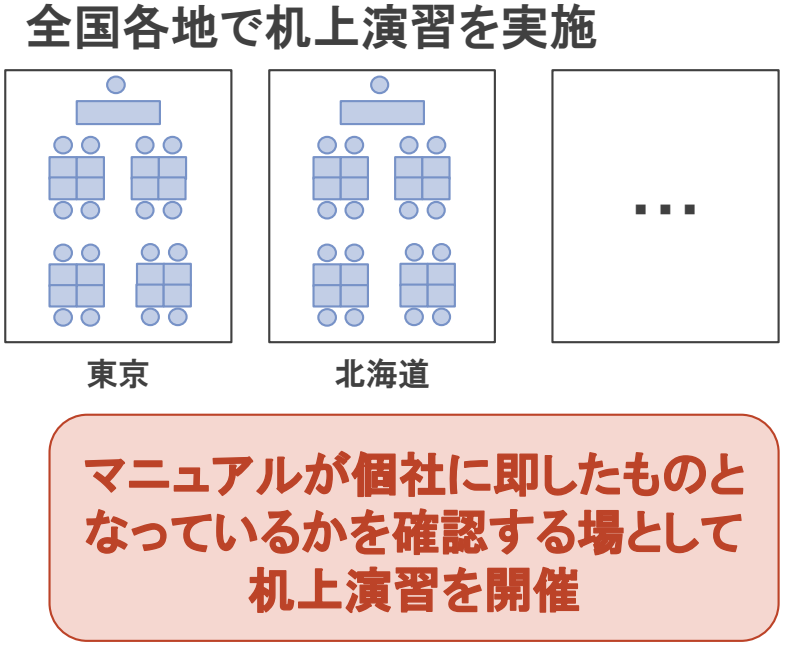
共助に向けた対応～事例①業界雛形のマニュアル配布、机上演習の実施～

信用組合業界では、システムが共同化されている特性を踏まえ、リスク評価手順、コンティンジェンシープランの業界雛形を作成し、個社の負担を軽減しています。
また雛形を受けて、個社が適切にカスタマイズできているかを個社が確認できるよう、机上演習を実施し、マニュアルの実効性向上に向けた取り組みを並行して行っています。

雛形のマニュアル配布



机上演習



業態での対応
共助に向けた対応～事例②業態内演習の実施～

金融庁は定期的な演習の参加を呼び掛けているものの、DeltaWallの参加可能企業は少ない状況です。こうしたことから、信用金庫業界では、業界団体が主催の演習を実施しています。

日本金融通信社
ニッキン

ニッキン記事DB(過去6ヶ月分の記事)

2018年11月23日号09面_信金界、サイバー攻撃対策強化、130信金がSSCと演習、各地区協会で勉強会も

信用金庫界がサイバーセキュリティー対策を強化する。130信金が参加し、しんきん情報システムセンター（SSC）と2019年1月下旬―2月上旬にサイバー攻撃を想定した演習を実施する。また、全国の地区協会単位でマニュアル整備などの勉強会を開催する。サイバー攻撃が複雑化するなか、対応をより高度化するのが狙い。

金融庁は、2016年から地域金融機関を対象にサイバーセキュリティー対策についてヒアリングを実施。2年が経過し、取り組みが進展している信金は増える一方で対策未着手や停滞状態の小規模信金もあり、対応にばらつきがみられた。金融庁の追加ヒアリング時に「経営陣の関与が少なく役員の役割や責任が不明確」「リスク評価の方法が不十分」と指摘を受けた信金もあった。

このため、全国信用金庫協会（佐藤浩二会長＝多摩信用金庫会長）は、サイバーセキュリティーリスクをコーポレートリスクとして捉え、経営陣がリーダーシップを発揮して対策を講じるように各信金に要請。サイバーインシデント対応マニュアルやリスク評価シートの参考例も示した。

年明けに実施する演習は、対策が遅れている信金の課題を見つけ出すことも狙いの一つ。SSCは、演習後に明確になった課題に対して個別信金をフォローする方針。

全国の地区信用金庫協会は、サイバーインシデントマニュアルの整備やリスク評価の実施を目的とした勉強会を開催する。

（出所）ニッキン2018年11月23号記事

本日はありがとうございました

NTT DATA
変える力を、ともに生み出す。

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（おぉのはくどう）

株式会社ＮＴＴデータ経営研究所

TEL：（03）5213-4115
FAX：（03）5560-3743
E-mail:　onoh@nttdata-strategy.com
〒102-0093　東京都千代田区平河町2-7-9　JA共済ビル10階

NTT DATA

Trusted Global Innovator