投資信託協会講座
東京証券会館 9階会議室

サイバーセキュリティを中心とした管理態勢について

平成27年12月３日(木)10:00～11:30

証券取引等監視委員会 事務局 証券検査課
特別検査官 兼 CSIRT情報セキュリティ事案対策官
兼 金融庁 総務企画局 政策課
サイバーセキュリティ対策企画調整室　室長補佐
鈴木　博

アジェンダ

Ⅰ．金融分野におけるサイバーセキュリティ強化に向けた
取組方針の概要（平成27年７月２日公表）

Ⅱ．システムリスク及びサイバーセキュリティに係る監督指針・
検査マニュアルの改正ポイント
（平成27年４月21日公表、４月22日から適用）

Ⅲ．金融機関に求められる対応や留意点

Ⅳ．最近よくみられるサイバー・インシデントの事例

（注）本文書に記載されている内容やこれから口頭で説明する内容において、意見の部分は講師の私見等が含まれており、金融庁、証券取引等監視委員会等の見解ではありません。

Ⅰ.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（概要）

平成27年7月2日公表

金融分野のサイバーセキュリティにおける課題①

金融分野のサイバーセキュリティ強化に向けた取組みの必要性

★委員会は情報セキュリティを含めて検査を実施していました。

○ これまでも金融機関のサイバーセキュリティ管理態勢については、システムリスク管理等の一環として、監督・検査を実施。

○ 他方、下記のとおりサイバー攻撃の脅威は、今や金融システムの安定にとって重大なリスク。個々の金融機関に留まらず、業界全体のサイバーセキュリティ強化を図ることで、金融システム全体の強靭性を高めていくことが必要。

○ 昨年11月に制定されたサイバーセキュリティ基本法では、政府は、金融も含めた重要インフラ事業者のサイバーセキュリティ確保のため、政府一丸となって、施策を講じることとされている。

⇒ 金融分野へのサイバー攻撃の脅威に対抗すべく今後取り組むべき方針を整理・明確化。

金融分野のサイバーセキュリティを巡る状況

イノベーションの進展に合わせた金融分野でのインターネットの利用拡大

サイバー攻撃の高度化（手口の巧妙化、攻撃技術へのアクセスの容易化）

サイバーテロの脅威（2020年東京オリンピック・パラリンピック競技大会の開催も見据えて）

補足1：委員会過去検査指摘事例

- A証券会社

情報セキュリティ管理態勢等が不十分な状況

（金商法第40条第2号に基づく金商業等府令第123条第1項第14号）

今回検査において、当社の情報セキュリティ管理態勢等について検証したところ、

⑴サーバーの特権ID及びパスワード等に係るアクセス管理

⑵口座番号等の顧客口座情報に係るアクセス管理

⑶機微情報に係るアクセス管理

⑷役職員のユーザーIDに係る更新等の管理

⑸当社と同等の顧客情報等を保有している子会社に対する情報セキュリティ管理の指導等が不十分な状況

といった情報セキュリティ管理に係る不備が認められたほか、

⑹情報セキュリティ監査が不十分な状況

が認められた。

金融分野のサイバーセキュリティにおける課題②

金融分野のサイバーセキュリティとして対処していくスコープ

攻撃者の動機	対象	脅威		関連する既存のリスク管理態勢
社会秩序の混乱	金融機関	金融機関・金融市場インフラの機能停止	金融機関が直接サイバー空間から攻撃されるもの	業務継続（BCM） 等
			人的（故意・過失を問わない内部者）に、システムがマルウェアに感染させられ、機能停止に陥るもの	
経済目的		機密漏洩	金融機関が直接サイバー空間から攻撃されるもの	情報セキュリティ管理 等
			人的（故意・過失を問わない内部者）に、システムがマルウェアに感染させられ、サイバー空間から機密漏洩	
		不正送金等の不正取引	金融機関のコンピュータがマルウェア（注）に感染して不正送金等の不正な取引がなされるもの	顧客保護 等
	顧客		顧客のコンピュータがマルウェアに感染して、顧客の意志に反した指示が金融機関になされるものや、フィッシング詐欺等	

（注）マルウェアとは、悪意のあるソフトウェアの総称。コンピュータに感染し、不正送金や情報窃取などの遠隔操作を自動的に実行するプログラム。

★ネット証券で顧客資金の不正送金事案有り

★金融機関がDDoS攻撃を受ける事案有り

補足２：金融機関への攻撃被害事例

- 平成27年５月22日（金）11:09～12:36
  FX業者BへDDoS攻撃(Distributed Denial of Service attack
  通信量を増大させ、過負荷によって、ネットやシステムを
  ダウンさせたりして、サービス停止に追い込む攻撃）
  ５月25日（月）にFXサービスが停止したことを公表

- 平成27年６月25日（木）08:59～10:45
  ネット銀行Cのインターネットバンキングへ DDoS攻撃
  ６月29日（月）にサービス停止したことを公表

金融分野のサイバーセキュリティ強化に向けた5つの方針

基本的考え方

○　金融分野のサイバーセキュリティ対策の強化には、官民が一体となって取り組んでいくことが重要。

○　このため金融庁は、金融機関との間で、サイバーセキュリティ確保という共通目的を有しているとの理解の下、建設的な対話を日常的に重ねていくことを目指すとともに、行政当局の立場から金融分野のサイバーセキュリティ強化に貢献するため、以下の5項目に取り組んでいく。

5つの方針

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. 金融庁としての態勢構築

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

○ 金融機関等のサイバーセキュリティ管理態勢がより実効性のある優れた取組みとなるよう建設的な対話を重ねる。

○ この一環として、全ての金融業態・金融市場インフラに対してアンケートも活用した実態把握を今年中に実施し、業態ごとの課題について分析。

○ この結果は、対話等を通じて金融機関等にフィードバックし、自己点検等に繋げていく。

（参考）アンケートで確認する事項の全体像（イメージ）

		具体的な対応
・金融機関・金融インフラの機能停止 ・機密漏洩 ・不正送金等の不正取引（金融機関への攻撃）	特定	・サイバー攻撃から保護すべき対象（情報資産等）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　等
	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 ・ｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝの策定・業界横断的演習への参加　等
	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　等
	対応・復旧	・ｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝに沿った適切な対応
・不正送金等の不正取引（顧客への攻撃）	サービス提供の状況	・より安全な認証手段をはじめとする不正防止策の組合せ状況　等
	顧客への働きかけ	・顧客の利用環境のセキュリティ強化の取組み ・異常な取引等の検知・連絡　等

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

業態毎の進め方 （今事務年度は、2段階で実施）

○ フェーズ1

➢ 地銀・第二地銀、証券会社、大手以外の生損保、取引所を中心に、合計100社弱に対して実施

○ フェーズ2

➢ フェーズ1の対象数を拡大するほか、信金・信組・貸金業を中心に実施

実態把握の手法

○ 金融機関のサイバーセキュリティ対策の状況を深堀りするため、対面でのインタビュー形式で実施。なお、インタビューを効率的に進めるため、対象金融機関に対し、事前に「確認項目」への回答を依頼し、その回答を分析した上でインタビューを実施。

○「確認項目」の具体的な内容

- ✓ サイバーセキュリティに関する経営陣の取組み
- ✓ リスク管理の枠組み
- ✓ サイバーセキュリティリスクへの対応態勢
- ✓ コンティンジェンシープランの整備と実効性確保
- ✓ サイバーセキュリティに関する監査

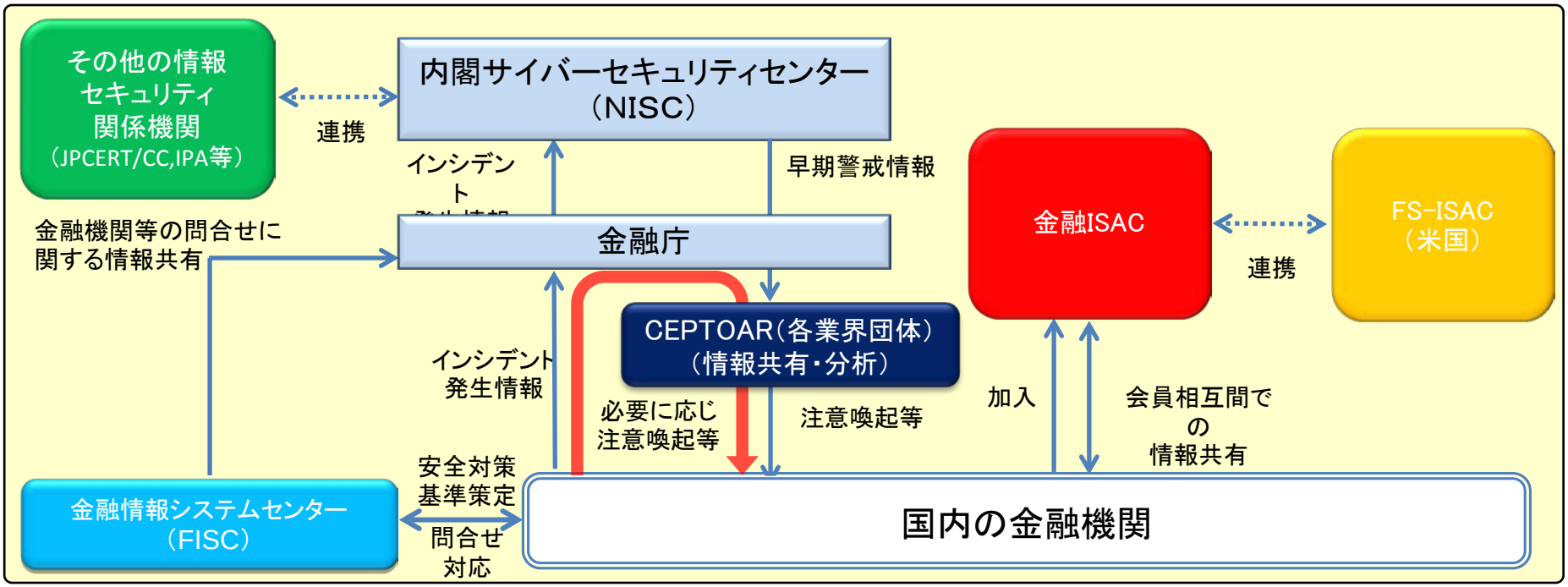
○ サイバー攻撃のいくつかのシナリオに基づく金融機関等の対応の確認（ケーススタディ）

2. 金融機関同士の情報共有の枠組みの実効性向上

○ 金融機関に対して、情報共有機関（金融ISAC等）を活用した情報収集・提供、取組み高度化（脆弱性情報の迅速な把握・防御技術の導入等）の意義について、機会を捉えて引き続き周知。

○ 業界団体等（CEPTOAR）を通じた情報提供も、NISCから発信されたものに限らず、金融庁から提供すべき情報があれば、積極的に発信。

○ 金融情報システムセンター（FISC）でも、安全対策基準を抜本強化した上で、基準の解釈に関する金融機関等からの問合せへの回答を「サイバーセキュリティ参考情報」と整理し、公表。



補足４：用語説明

	用語	説明
	CEPTOAR(セプター：Capability for Engineering of Protection, Technical Operation, Analysis and Response)	業界団体等が担っている、政府等から各金融機関へIT障害に関わる情報共有を行う機能。金融分野ではそれぞれ全銀協、日証協、生保協、損保協が該当。
	金融情報システムセンター（FISC）	金融機関、情報処理会社等により設立された、金融情報システムに係る安全基準の策定等による安全対策の推進を行う財団法人。
	一般社団法人 JPCERT コーディネーションセンター (略称：JPCERT/CC) (英文：Japan Computer Emergency Response Team Coordination Center)	インターネットを介して発生する侵入やサービス妨害等のインシデントについて、日本国内のサイトに関する報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の技術的な検討や助言などを行っている組織。2003年３月設立登記。
	IPA（独立行政法人　情報処理推進機構）	サイバー攻撃情報などの収集・評価・分析や、対策方法の実施・普及等を行う政策実施機関。
	FS－ISAC（米国） Financial Services Information Sharing and Analysis Center	1999年設立、約5,000社超の金融機関が会員のサイバーセキュリティに関する情報共有組織
	一般社団法人 金融ISAC	日本版FS－ISAC、平成26年８月設立、会員147社、準会員13社(11月17日時点）

3. 業界横断的演習の継続的な実施

○ サイバー攻撃への対応能力の向上には、演習を通じて実戦能力を涵養しつつ、対応態勢等の確認を行い、PDCAサイクルを回すことが有効。

○ そこで、海外でも行われている演習事例を参考にしつつ、当局等の関係者を含めた業界横断的演習を速やかに実施するべく、早急に具体的方法（実施主体（他省庁・関係機関との連携を含む）、演習の目的、シナリオの内容等）を検討する。

〔サイバーセキュリティ基本法（平成26年法律第104号）抜粋〕
（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）
第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

〔米国の金融分野における業界横断的演習の例〕
✓ Quantum Dawn　2
米国証券金融市場協会（SIFMA）の主催で、2013年7月に実施。対象は金融機関、証券取引所、政府関係機関等。証券市場に対する同時多発的なサイバー攻撃を想定して訓練を実施。
✓ CAPP Exercise (2014)
FS-ISACの主催で、2014年9月に実施。対象は、決済サービスを提供する金融機関。支払いプロセスに対するサイバー攻撃時の対応について訓練。

〔英国の金融分野における業界横断的演習の例〕
✓ Waking Shark　2
イングランド銀行（BOE）を中心に、2013年11月に実施。対象は金融機関、証券取引所、政府関係機関等。証券市場に対するDDoS攻撃等を想定して訓練を実施。

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

○ サイバーセキュリティ強化には、対策の実装等を行う技術担当者だけでなく、経営層及びこれを支える管理部門の職員も、セキュリティに関する意識と一定の知見を有することが望まれる。また、監督当局の担当者の質の向上も必要。そこで、平成27事務年度より以下の取組みを進める。

- ✓ 金融機関の経営層の意識向上を目的としたセミナー等の開催
- ✓ 業界団体、情報共有機関等の関係者と連携した、金融分野におけるサイバーセキュリティ人材の育成策についての検討（キャリアパス、バックグラウンドを含む適性等）。
- ✓ 金融庁における担当者の専門性向上（外部登用と内部の人材育成）

〔サイバーセキュリティ基本法（平成26年法律第104号）抜粋〕

（人材の確保等）

第二十一条　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする。

２　(略)

〔金融商品取引業者等向けの総合的な監督指針〕
Ⅲ－２－８システムリスク管理態勢（１）主な着眼点

〔主要行等向けの総合的な監督指針（抜粋）〕

Ⅲ－３－７－１－２ 主な着眼点

（１）システムリスクに対する認識等

② 代表取締役は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。

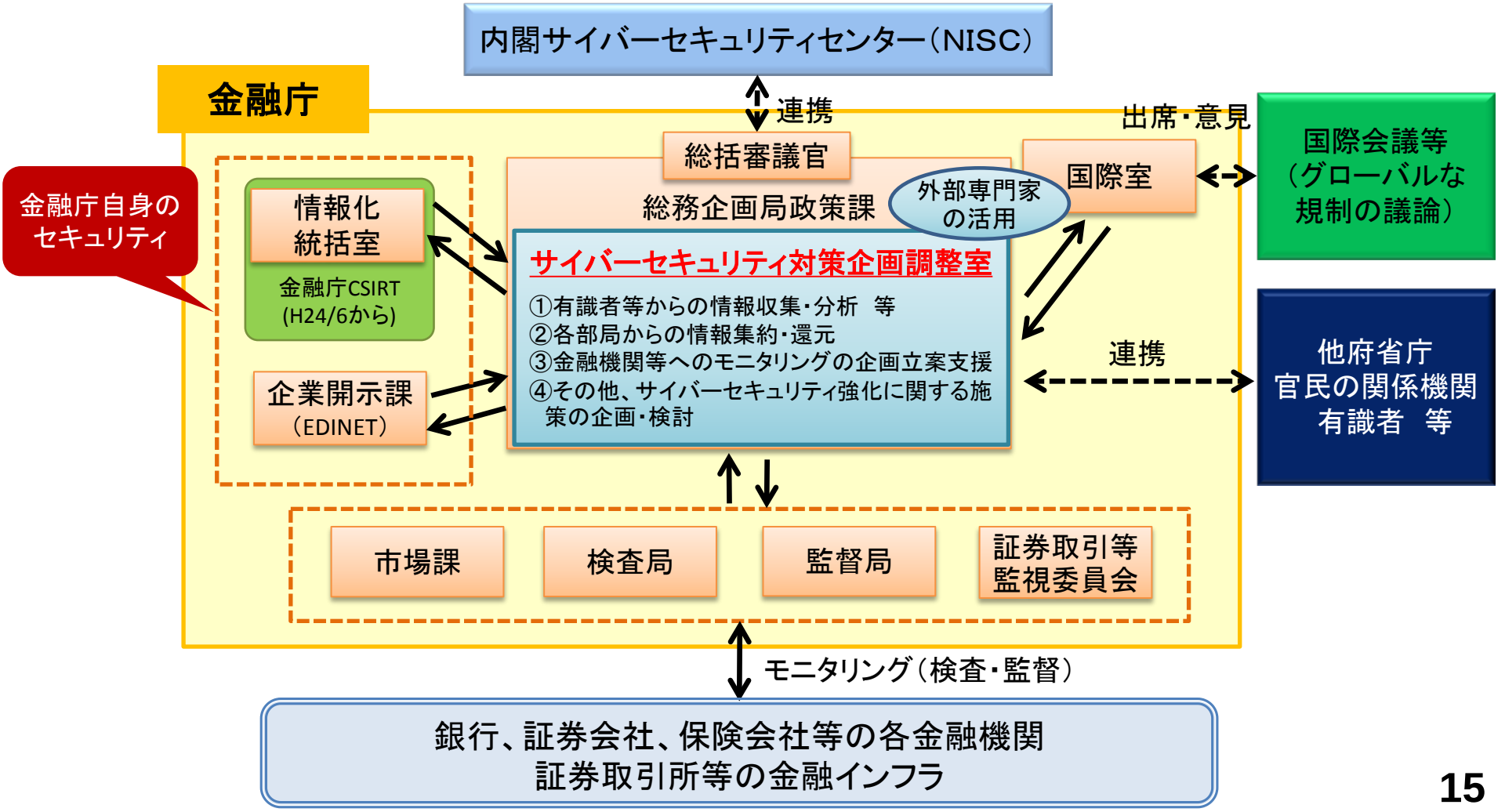
（５）サイバーセキュリティ管理

① サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

⑨ サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

5. 金融庁としての態勢構築

○ 金融システム全体におけるサイバーセキュリティを強化するため、金融庁内部において情報を一元的に集約し、外部専門家を活用しつつ知見の集積を図り、組織横断的に企画・調整を行う部署（**サイバーセキュリティ対策企画調整室**）を直ちに設置する。



参考：金融モニタリングレポート

（平成27年7月３日公表）

概要　第8章　サイバーセキュリティ管理態勢

サイバー空間を取り巻く脅威はボーダレスに進行し、急速に巧妙化。

金融機関のサイバーセキュリティ管理態勢について検証。

- ３メガバンクでは、G-SIFIs等の先進的な取組についての調査を踏まえ、管理態勢を整備。単体のみならず、グループ全体としてサイバーセキュリティ管理態勢の実効性を強化していくことが重要。
- 他の業態についても、金融機関間の情報共有を含め、管理態勢の高度化を図っていくことが重要。
- 具体的には、情報の重要度に応じた管理、多層防御（入口のみならず、システム内部、出口を含む多段階の対策の組み合わせ）、訓練による攻撃に対する初動対応の習得が重要。
- サイバー攻撃の手口は常に進化しており、経営陣の積極的な関与の下での不断の取組が必要。

Ⅱ.システムリスク及びサイバーセキュリティに係る監督指針・検査マニュアルの改正ポイント

平成27年4月21日公表

Ⅱ－１－１　システムリスクとは？

「金融商品取引業者等向けの総合的な監督指針
　Ⅲ－２－８システムリスク管理態勢」によれば、

- 「システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い顧客や金融商品取引業者が損失を被るリスクやコンピュータが不正に使用されることにより顧客や金融商品取引業者が損失を被るリスク」

→　情報セキュリティリスク・サイバーセキュリティリスクも含みます。

Ⅱ－１－２ システムリスク管理とは？

- 本日の話の範囲では、システムリスク管理とは、ITシステム及び情報セキュリティに係る狭義のリスク管理（リスクの顕在化を未然防止する）とリスク顕在化後の危機管理の両方を含めるものとします。
- システムリスク管理は、管理の枠組み（フレームワーク）と管理のプロセスの両輪を、PDCAサイクルで効果的に実践することが重要です。

Ⅱ－2. 監督指針・検査マニュアルの考え方

「金融商品取引法」第40条第2号（適合性の原則等）

業務の運営の状況が公益に反し、又は投資家の保護に支障を生ずるおそれがあるものとして内閣府令で定められる状況にあること。

↓

「金融商品取引業等に関する内閣府令」第123条第14号

金融商品取引業に係る電子情報処理組織の管理が十分でないと認められる状況。

↓

「金融商品取引業者等向けの総合的な監督指針」

Ⅲ－2－4　顧客等に関する情報管理態勢	Ⅲ－2－8　システムリスク管理態勢	Ⅲ－2－9　危機管理態勢

↓

「金融商品取引業者等検査マニュアル」

システムリスク管理態勢等

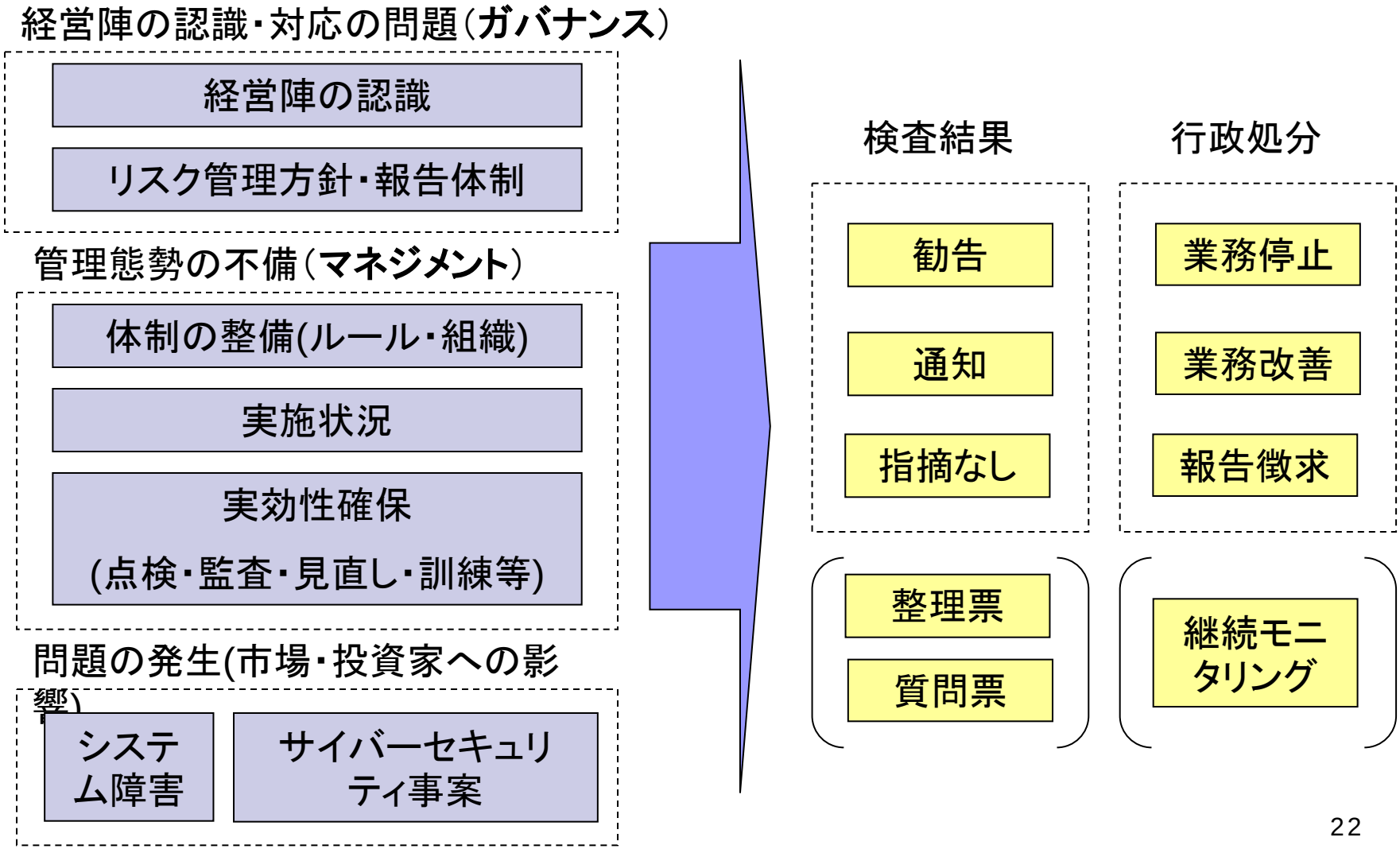
Ⅱ－2. 監督指針・検査マニュアルの考え方

監督指針Ⅲ－2－8の項目をリスク・マネジメントの観点から整理

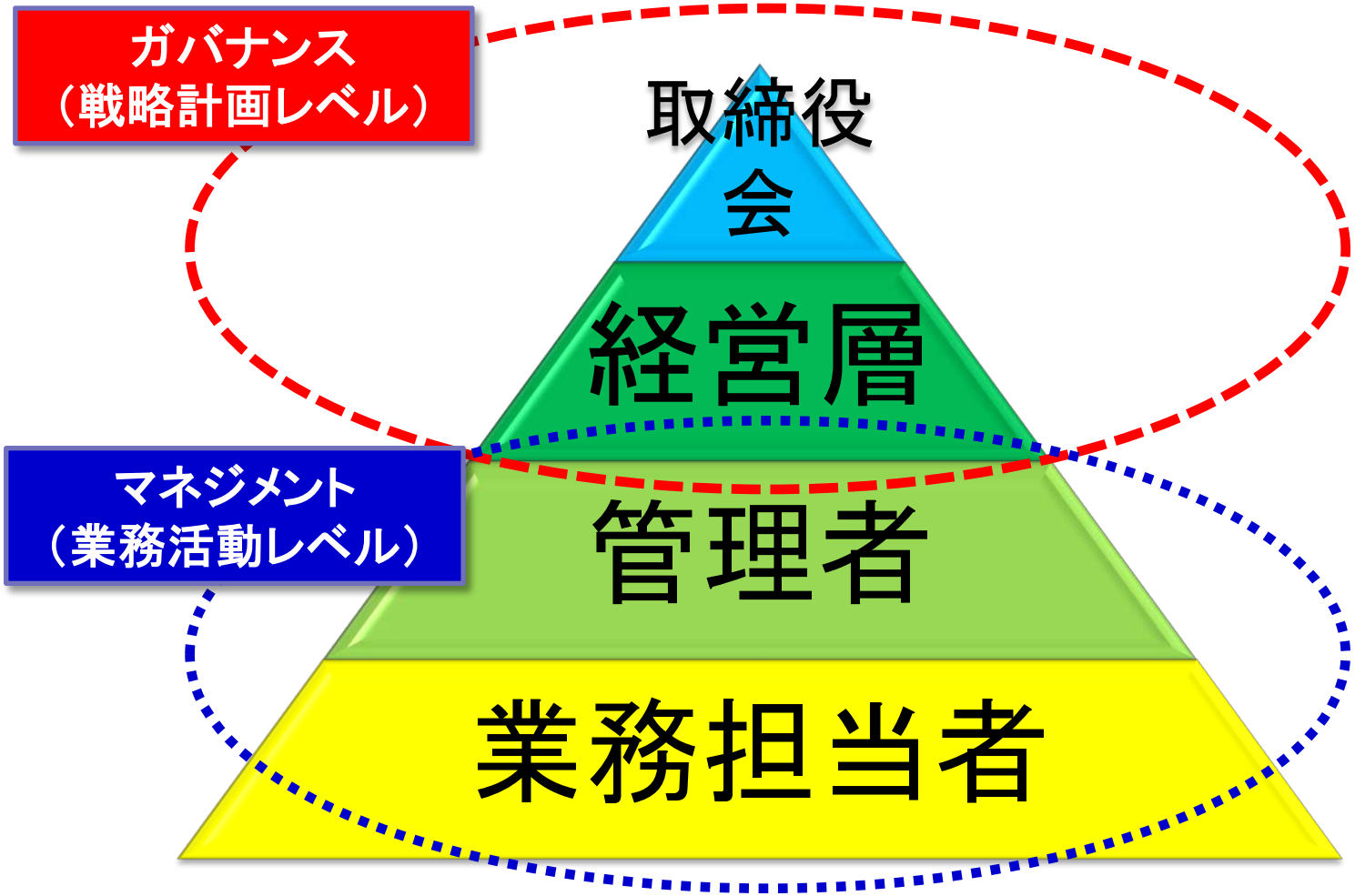
リスクマネジメント（狭義）		クライシスマネジメント
①システムリスクに対する認識		
②適切なリスク管理態勢の確立		
③システムリスク評価	障害 災害 発生	⑨コンティンジェンシープラン
④情報セキュリティ管理		⑪障害発生時の対応
⑥システム企画・開発・運用管理		
⑧外部委託管理		
⑤サイバーセキュリティ管理		
⑩システム統合リスク（プロジェクトリスク）		
⑦システム監査		

Ⅱ－2. 監督指針・検査マニュアルの考え方

～ 検査官の視点で見ると ～



補足５　ガバナンスとマネジメント



Ⅱ－3. システムリスク管理態勢の監督指針の変更点

監督指針Ⅲ－2－8(1)主な着眼点より抜粋

① システムリスクに対する認識等**(赤字は4月に改訂された部分)**

イ. 取締役会等において、システムリスクが十分認識され、全社的なリスク管理の基本方針が策定されているか。

ロ. 取締役会等は、システム障害や**サイバーセキュリティ事案(以下「システム障害等」という。)の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。**

ハ. システムリスクに関する情報が、適切に経営者に報告される体制となっているか。

(注)サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。

Ⅱ－3. システムリスク管理態勢の監督指針の変更点

監督指針Ⅲ－2－8(1)主な着眼点より抜粋

② 適切なリスク管理態勢の確立

イ. システムリスク管理の基本方針が定められ、管理態勢が構築されているか。

ロ. 具体的基準に従い管理すべきリスクの所在や種類を特定しているか。

ハ. システムリスク管理態勢は、自社の業務の実態やシステム障害等を把握・分析し、システム環境等に応じて、その障害の発生件数・規模をできる限り低下させて適切な品質を維持するような、実効性ある態勢となっているか。

③ システムリスク評価

システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。また、洗い出したリスクに対し、十分な対応策を講じているか。

Ⅱ－4. システムリスク管理態勢検査マニュアル追加点

検査マニュアルより抜粋（一部簡略化）

② サイバーセキュリティ管理態勢の整備

イ. 取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

また、例えば、以下のような管理態勢を整備しているか。

a. サイバー攻撃に対する監視体制

b. サイバー攻撃を受けた際の報告及び広報体制

c. 組織内CSIRT等の緊急時対応及び早期警戒のための体制

d. 情報共有機関等を通じた情報収集・共有体制 等

ロ. サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階の対策を組み合わせた

多層防御を講じているか。

a. 入口対策（例えば、ファイアウォールの設置、不正侵入検知システム・不正侵入防止システムの導入 等）

b. 内部対策（例えば、特権ID・パスワードの適切な管理、不要なID の削除、特定コマンドの実行監視 等）

c. 出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断 等）

Ⅱ－4. システムリスク管理態勢検査マニュアル追加点

検査マニュアルより抜粋（一部簡略化）

② サイバーセキュリティ管理態勢の整備（続き）

ハ. サイバー攻撃を受けた場合に被害の拡大を防止するための措置を講じているか。
例えば、
a. 攻撃元のIP アドレスの特定と遮断
b. DDoS 攻撃に対して自動的にアクセスを分散させる機能
c. システムの全部又は一部の一時的停止 等

ニ. システムの脆弱性について、OS の最新化やパッチの適用など必要な対策を適時に講じているか。

ホ. サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

ト. サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

チ. サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

Ⅱ－５．検査でよく見かける問題点→構築のポイント

実効性ある態勢とは、PDCAサイクルが着実に実施されていること。→　継続的な改善

×形式的にルール・プロセスが策定されていても、
　形骸化して実際に運用されていない。又は未定着。

×運用実態を検証していない。検証が不十分。

×検証していても、改善策を策定していない。

×改善策が実施されていない、フォローされていない。

×場当たり的な対策で、根本原因を解決していない。

×ルール・プロセスの改善にまで至っていない。

Ⅱ－6．Q＆A①

Q1）システムリスク管理態勢の検証は、従前どおり金融機関の業容に応じてなされるものであり、改正案で記載されている項目すべてを満たすことが求められているわけではないと考えてよいか。

A1）情報セキュリティ管理およびサイバーセキュリティ管理で示しているそれぞれの着眼点については、取り扱う業務のリスクに見合った態勢整備や対策を講じる必要があると考える。

なお、それぞれの着眼点で「たとえば」と記載されているような具体的な対策例については、例示に限定されるものではなく、例示以外の方法も含め検討し、適切な対策を講じる必要がある。監督指針等の適用にあたっては、引き続き金融機関の規模や特性を十分にふまえ、機械的・画一的な運用に陥らないよう配慮される。

一方で、情報セキュリティ、サイバーセキュリティの観点でみれば、対策の弱いところから攻撃者に狙われ、そこから金融システム全体に被害が波及するようなケースも考えられるため、着眼点として示した項目については、取り扱う業務のリスクに応じて、態勢整備や技術的対策を講じる必要がある。

Ⅱ－6．Q＆A②

Q2）「顧客の重要情報」とは具体的にどのようなものか。

A2）金融機関が責任を負うべき顧客の重要情報については、たとえば、個人情報、認証情報、電子的価値情報等が考えられるが、個々の金融機関が業務やリスクに応じて適切に定義を行う必要があると考える。一般的には、各社のセキュリティポリシーにおいて規定されているものと考える。

（参考）金融情報システムセンター（FISC）の「金融機関等におけるセキュリティポリシー策定のための手引書」

Ⅱ－6．Q＆A③

Q3）「情報共有機関等」とは、具体的にどのような機関を想定しているのか。

A3）たとえば、金融セプターや業界団体、IPA、JPCERTのほか、金融ISAC、日本シーサート協議会などが考えられる。

　サイバー攻撃の被害拡大を防止するためにも情報共有機関等を積極的に活用し、金融機関相互でタイムリーな情報共有を行うことが有益である。情報共有機関としては、前述のほか、日本サイバー犯罪対策センター（JC3）、フィッシング対策協議会等が考えられる。

Ⅱ－6．Q＆A④

Q4）「業界横断的な演習に参加」とは、具体的にどのような演習を想定しているのか。

A4）個別金融機関単独の訓練ではなく、業界内の演習や銀行、保険、証券、貸金等の垣根を越えた演習を想定している。また、すでにNISCが毎年実施している演習のように金融分野以外の重要インフラ事業者との演習も考えられる。

　欧米諸国においては、当局が関与した業界横断的な演習が実施されている。これをふまえ、当庁としても関係団体等と緊密に連携していく所存である。

　金融機関は、下記のような目的に応じて演習を重ね、実効性を確保することが重要である。

・経営層の意識改革およびトリアージ能力の向上

・連絡・報告、情報共有等、初動態勢の検証

・証拠保全、ログ解析等、技術スキルの向上　等

参照文献

- 金融分野におけるサイバーセキュリティ対策について
  http://www.fsa.go.jp/policy/cybersecurity/index.html
- 「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」の公表について

  http://www.fsa.go.jp/news/27/20150702-1.html
- 金融商品取引業者等向けの総合的な監督指針

  http://www.fsa.go.jp/common/law/index.html
- 証券検査方針・検査マニュアル

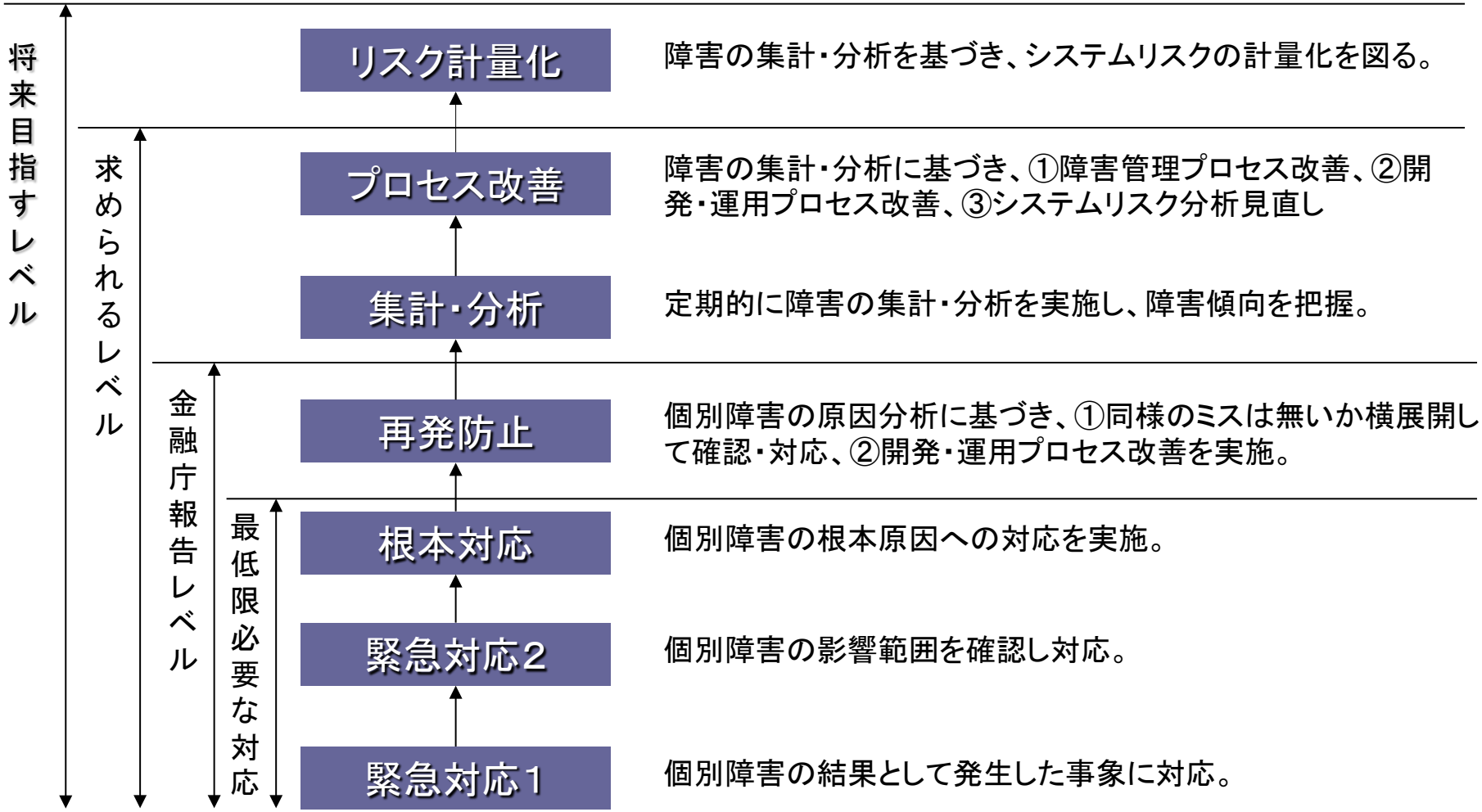
  http://www.fsa.go.jp/sesc/houshin/index.htm

補足６　Ⅲ－２－４　顧客等に関する情報管理態勢

- 顧客に関する情報は、金融商品取引の基礎をなすものであり、その適切な管理が確保されることが極めて重要である。そのうち特に、個人である顧客に関する情報については、個人情報の保護に関する法律（以下「個人情報保護法」という。）、金商業等府令、金融分野における個人情報保護に関するガイドライン（以下「保護法ガイドライン」という。）及び金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（以下「実務指針」という。）の規定に基づく適切な取扱いが確保される必要がある。
- また、金融商品取引業者は、法人関係情報（金商業等府令第１条第４項第14 号に掲げる法人関係情報をいう。以下同じ。）を入手し得る立場であることから、その厳格な管理とインサイダー取引等の不公正な取引の防止が求められる。
- 以上のように、金融商品取引業者は、顧客に関する情報及び法人関係情報（以下「顧客等に関する情報」という。）を適切に管理し得る態勢を確立することが重要である。

補足7. 障害管理

求められている障害管理とは？



SESC
"for investors, with investors"

Ⅲ．金融機関に求められる対応や留意点

Ⅲ－１．金融機関に求められる対応や留意点

一社でも対応が疎かな金融機関があっては、脅威を低減させることはできない。

（1）サイバーセキュリティは、IT部門に任せておけば良いということではなく、経営陣が先頭に立って重要性を認識し、態勢整備を図っていくことが不可欠である。

⇒ *ヒト・モノ・カネの優先順位*
⇒ *サービスの一時中断等、重要な経営判断*

（2）本年４月の監督指針等の改正においては、着眼点を理解しやすいように、できるだけ例示を入れている。これは、例示されている事項を実施すれば、それでよいということではなく、また、単なる機器の導入や組織の設置にとどまることなく、個別の着眼点の背景・趣旨を十分に理解したうえで、個別金融機関の業務やリスクに応じて、組織全体の取組みとして適切な対応を図っていくことが必要である。

（3）サイバーセキュリティへの対応は、喫緊の課題であることから、改正した監督指針等については、即日施行としており、経過期間は設けていない。金融機関は、着眼点に基づいて自己点検を行い、対応の優先付けを行ったうえで対応計画（ロードマップ）を策定するなど、経営陣の積極的な関与のもと、PDCAサイクルを回していくことが大切である。

Ⅲ－２．今すぐに取組んでいただきたいこと

サイバーインシデントは、今日にも発生する脅威

（1）保護すべき重要情報を網羅的に洗い出し、その重要度に応じた管理を適切に行っていただきたい。

⇒ *リスク認識が第一歩。*

（2）定めた管理ルールが徹底されるよう職員のセキュリティ意識向上のための教育や訓練を行っていただきたい。

⇒ *本年6月に公表された日本年金機構の事案では、管理ルールは整備されていたものの、運用が徹底されておらず、結果的に被害拡大に繋がっている。*

（3）侵入されることを前提とした対策を講じていただきたい。
特に（内部対策として）、ログの監視、特権IDの管理、パスワードポリシーの徹底、不要なアカウントの削除、セキュリティパッチの適時の適用、定期的なウィルスのフルスキャン等の実施。

⇒ *高価なソリューションを導入する前にやるべきことがある。*

（4）攻撃を検知した場合の初動を身につけていただきたい。
例えば、金融ISAC等の情報共有機関を通じた情報交換により、情報収集能力の向上を図ったり、迅速かつ適切な意思決定ができるように訓練や演習を重ねていただきたい。

⇒ *複数のサイバーセキュリティ事案をシナリオとしたコンティンジェンシープランの準備。*

SESC
"for investors, with investors"

Ⅳ. 最近よくみられるサイバー・インシデントの事例

Ⅳ－１．不審なサイトへの通信（標的型攻撃　→　情報漏えいのおそれ）

"for investors, with investors"

標的型メール攻撃、水飲み場型攻撃等により、マルウェアに感染する事案。
マルウェアに感染すると外部のウェブサーバと通信することが確認されており、場合によっては、金融機関内の内部情報が外部に送信されるおそれがあるもの。

＜速報の視点＞

速報の為、全て網羅できていなくても金融機関において把握できている範囲から報告することが重要。

① いつ、誰からの情報により当該状況を認識したか。
② 現時点で顧客への影響は発生しているか。
③ 当該感染源（PC等）は物理的な隔離は完了したか。
④ その他対策はどのような状況か（インターネット・外部メールの遮断／外部向け通信の監視等）。
⑤ 当該事象が発生している感染PC等が接続されていた、システム・ネットワーク等の構成は把握できているか。
⑥ 情報の漏えいを想定した場合、最大リスクとしてはどのような情報が流出する可能性が考えられるか。
⑦ 現在、本件対応へのリーダーシップを誰がとっているか。また、担当役員や経営トップは本件について実態を正確に把握しているか。
⑧ 関係機関への連絡連携はどこまで行っているか（当局・業界団体、警察・関係する外部委託先、その他情報共有機関など）。
⑨ セキュリティベンダーへの調査分析要請はできているか（ウィルスの種類や被害特定、或いはウィルス拡散範囲を特定するため、感染PCやネットワーク関連ログの解析依頼等）。
⑩ 最新のウィルス定義ファイルでウィルスを検出できる場合、該当PCだけでなく、全PCのフルスキャンを実施したか。

Ⅳ－２．DDoS攻撃　（ビットコインを要求する脅迫メール）

金融機関のウェブサイト等に公開されている問合せ窓口等のメールアドレスに対して、身代金を要求する脅迫メールを送りつけたうえで、デモンストレーションと称して１時間程度のDDoS攻撃を行う事案。 攻撃を受けた結果、ネットバンキングやネットトレーディング等の業務に支障が生じる例も発生。

＜留意事項＞

① 迅速に攻撃の迂回措置や、回線業者と連携してアクセス元や回線を遮断する措置等、有効な対策を講じられるよう体制を整えておく。

② DDoS攻撃のほかに、内部データの破壊、改ざん及び窃取等を行われないよう、不正アクセスについて細心の監視を行う（セキュリティ担当者の目をDDoS攻撃に向けさせ、その裏で不正侵入等の行為を行う手口も想定される）。

③ 攻撃により、ホームページにアクセスできなくなった場合にも、適切に顧客説明を行えるよう、他のアクセスツール（コールセンターやSNS等）を検討しておくことが望ましい。

脅迫メールのイメージ

【攻撃と同時に送付される１通目（全文英文）】
- 攻撃者（犯行グループ）の自己紹介。
- 24時間以内に25ビットコイン（約70万円）を支払え、さもなければ、より重大な攻撃を加える。
  ※30～50ビットコインを要求しているケースもあり。
- 現在の攻撃は、デモンストレーション攻撃として１時間で止める。
- ビットコインの購入方法や送金サイトを紹介。

【（身代金を支払わなかった場合）24時間後に送付される2通目（全文英文）】
- 昨日の予告を無視したことを指弾。
- 今から24時間以内に支払いがない場合、支払うまで攻撃を続ける。
- 支払えば、我々は二度と攻撃はしない。

さいごに

- 本日の話は、システムリスク管理態勢検査やサイバーセキュリティ実態把握作業の中で、担当者として認識した問題点や管理の事例を提示することにより、会員企業のシステムリスク管理態勢の改善やレベルアップに少しでも役立てていただければと思います。
- 当たり前の話が多いですが、当たり前のことを当たり前に行うことが実は大変であり、また、重要な事だと思います。

ご清聴ありがとうございました

情報提供は
https://www.fsa.go.jp/sesc/watch/index.html
tel:0570-00-3581
（一部のIP電話等からは03-3581-9909）

年金運用ホットラインは
http://www.fsa.go.jp/sesc/support/pension.htm
tel: 03-3506-6627

公益通報の通報・相談は
http://www.fsa.go.jp/sesc/koueki/koueki.htm
tel: 03-3581-9854