資料２－２

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）

金融庁

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

○ 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）

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

<table>
<tr><th>攻撃者の動機</th><th>対象</th><th colspan="2">脅威</th><th>関連する既存のリスク管理態勢</th></tr>
<tr><td rowspan="2">社会秩序の混乱</td><td rowspan="3">金融機関</td><td rowspan="2">金融機関・金融市場インフラの機能停止</td><td>金融機関が直接サイバー空間から攻撃されるもの</td><td rowspan="2">業務継続（BCM） 等</td></tr>
<tr><td>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</td></tr>
<tr><td rowspan="4">経済目的</td><td rowspan="2">機密漏洩</td><td>金融機関が直接サイバー空間から攻撃されるもの</td><td rowspan="2">情報セキュリティ管理 等</td></tr>
<tr><td>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</td></tr>
<tr><td rowspan="2">不正送金等の不正取引</td><td>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</td><td rowspan="2">顧客保護 等</td></tr>
<tr><td>顧客</td><td>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</td></tr>
</table>

（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。

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)

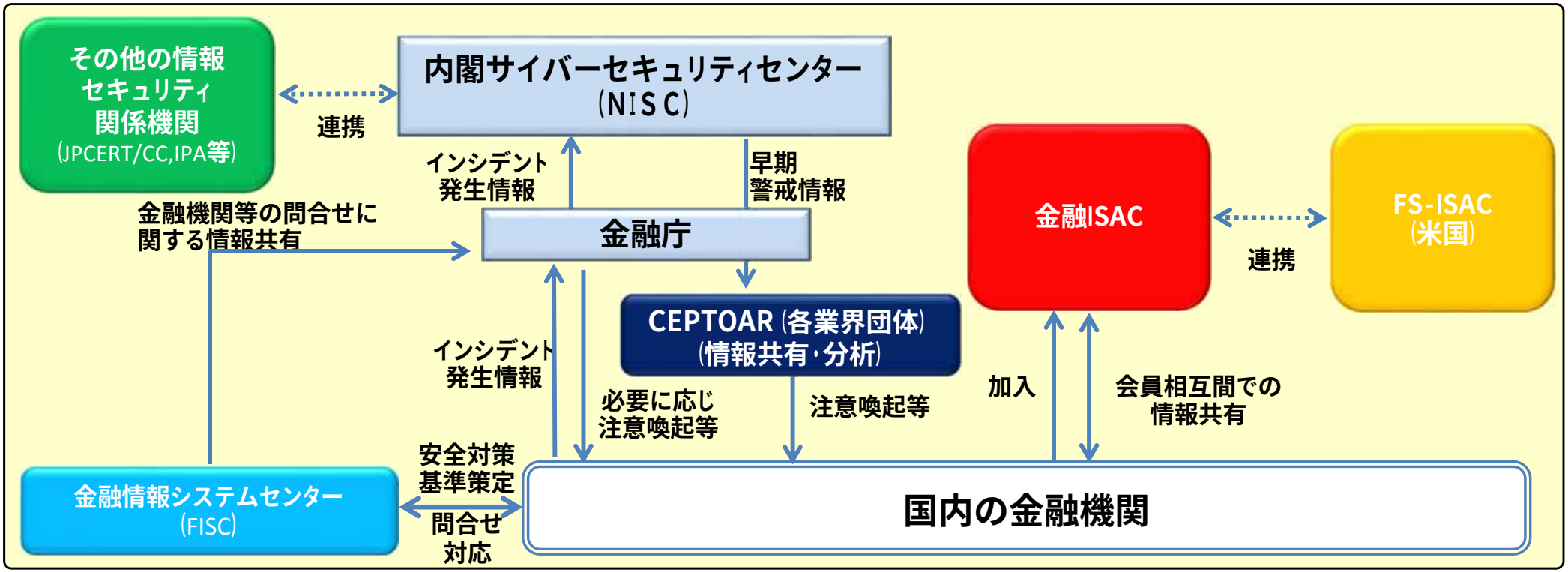
		具体的な対応
・金融機関・金融インフラの機能停止 ・機密漏洩 ・不正送金等の不正取引 (金融機関への攻撃)	特定	・サイバー攻撃から保護すべき対象 (情報資産等) の把握 ・経営陣によるサイバーセキュリティ管理の重要性の認識 ・セキュリティ水準の定期的評価 ・システム開発におけるセキュリティ管理の視点の導入　等
	防御	・組織内の緊急時対応・早期警戒体制の整備 ・情報共有機関等を通じた情報収集・共有体制の整備 ・多層防御 (入口対策・内部対策・出口対策) ・システムの脆弱性についての適時の対応 ・ｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝの策定・業界横断的演習への参加　等
	検知	・通信記録 (ログ) 等の取得・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

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。



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）

〔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。

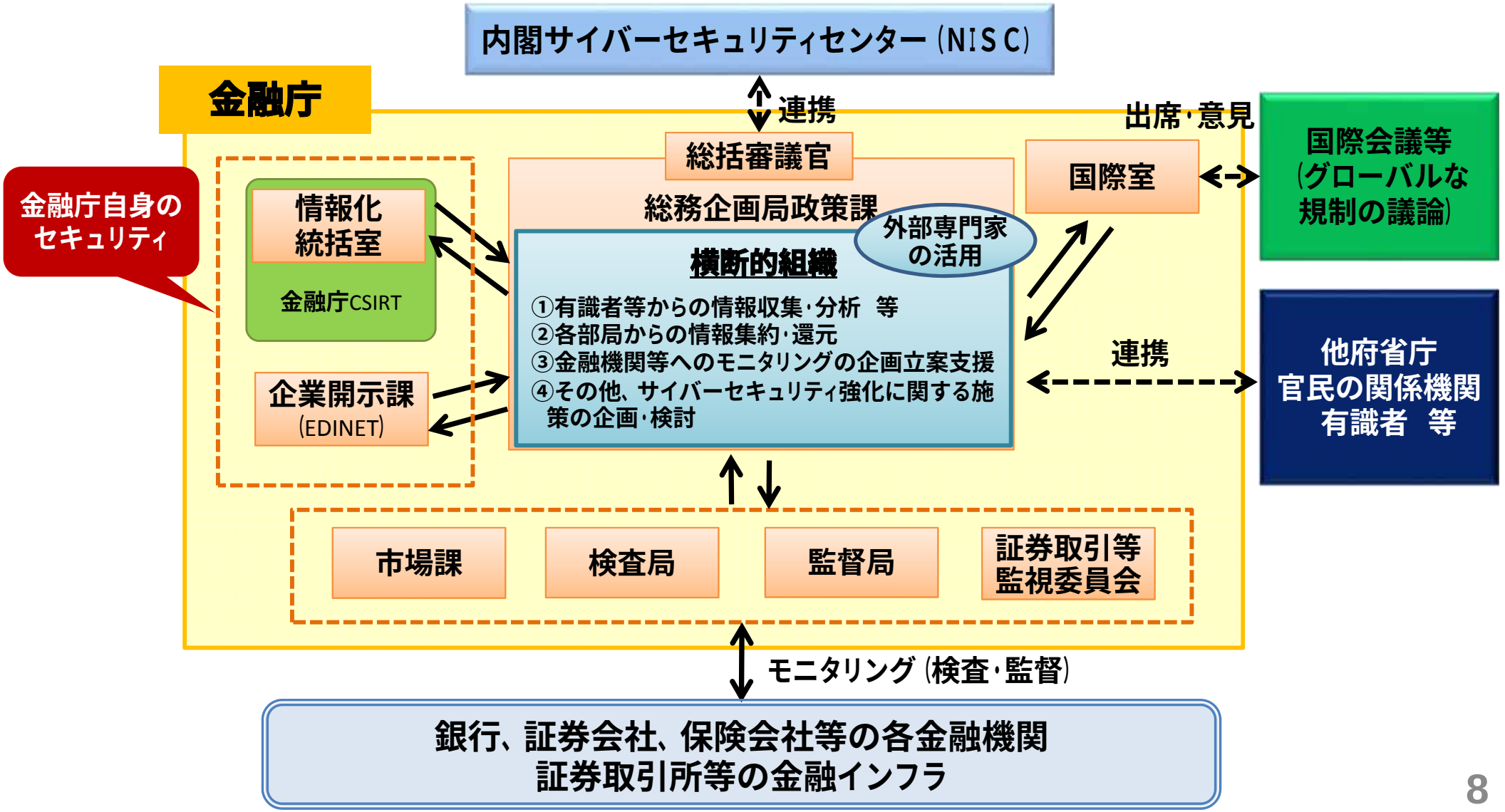
（5）サイバーセキュリティ管理

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・調整を行う部署を直ちに設置する。



(参考) サイバーセキュリティ対策企画調整室

○ 総務企画局政策課に設置された「サイバーセキュリティ対策企画調整室」が司令塔となり、サイバーセキュリティ強化に向けた金融庁内組織横断的な企画・調整を行うとともに、各局の関係部署と連携して対応にあたる。

組織図