2024 年 7 月 29 日

金融庁総合政策局リスク分析総括課
IT サイバー・経済安全保障監理官室 御中

一般社団法人全国銀行協会

「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対する意見について

・サイバー攻撃の被害は、地政学的な緊張の高まりなどを背景に、世界規模で増加傾向にあり、その手口は日々、高度化かつ多様化している。日本国内においても、企業や団体におけるランサムウェアの被害が、業種を問わず拡大しており、あらゆる企業において、サイバー攻撃の最新の傾向を踏まえたセキュリティ対策について検討していく必要があると認識している。とりわけ、金融機関は国民生活や経済活動を支えるインフラ事業者として、より一層強固なサイバーセキュリティ対策を講じる必要があると考えている。

・「金融分野におけるサイバーセキュリティに関するガイドライン」（以下「本ガイドライン」）では、「基本的な対応事項」及び「対応が望ましい事項」が明確化されており、いずれについても、業界で一律の対応を求めるものではなく、金融機関が、自社を取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（所謂「リスクベース・アプローチ」を採ること）が求められることに留意が必要である、とされている。

・一般社団法人 全国銀行協会（全銀協）としては、本ガイドラインは、サイバーセキュリティに関する「基本的な対応事項」と、より高度なサイバーセキュリティ態勢を構築するための参考となる「対応が望ましい事項」が示されたことで、金融機関が、自社の態勢の現状と課題を把握し、必要な改善策を計画的に実施することができるという観点において意義があり、銀行界全体のサイバーセキュリティへの対応力の底上げと態勢強化に資するものと理解している。

・こうした理解のもと、 全銀協としては、一部項目で記載されている文言の定義や、対象範囲、基準、解釈、等を明確化すること、具体例を提示することで、当協会の会員の態勢整備の一助となると考えていることから、パブリックコ

メント募集に対して、別紙のとおり意見を提出する。

以　　上

別　紙

「金融分野におけるサイバーセキュリティに関するガイドライン（案）」（パブリックコメント）に関する意見

	コメント者	コメント対象文書	コメント箇所（頁、項番等）	コメント等
1	全銀協	ガイドライン案	全般	本ガイドラインについて英語版を策定してほしい。
2	全銀協	ガイドライン案	全般	金融庁ではサイバーセキュリティセルフアセスメントの取り組みもあるが、本ガイドラインの「基本的な対応事項」と比べ求める水準感に差があり、本ガイドラインの「基本的な対応事項」が求める水準が相対的に高いように見受けられる。求める水準感がダブルスタンダード化しているようにも見え、整合性を確保してほしい。
3	全銀協	ガイドライン案	全般	「基本的な対応事項」の中には、CRI Profileなどのグローバルな評価フレームワークでは大規模な金融機関に求める内容も含まれており、「基本的な対応事項」の求める水準がグローバルスタンダードに比べても高いように見受けられる。中小金融機関を含め、対応については、時限を定めて一律の対応を求めるものではなく、各金融機関がリスクベースアプローチで対応するという理解でよいか
4	全銀協	ガイドライン案	全般	本ガイドラインにおける「経営陣」とは役員・執行役員を指し、「経営トップ」とは頭取・社長・理事長等を指すという理解で相違ないか。 サイバーセキュリティ管理態勢について経営陣の主体的な関与が求められる点は各節でも繰り返し述べられている重要事項であるため、本ガイドラインにおける定義を明確に示してはいかがか。
5	全銀協	ガイドライン案	1.1.	「対応が望ましい事項」の中には、どの金融機関にとってもかなり難度の高い取り組みも含まれている認識でいるが、その理解であっているか。金融庁として、監督・検査の中で今後どのように取り扱うことを想定しているのか。
6	全銀協	ガイドライン案	2.1.1. 基本方針、規程類 の策定等【対応が望ましい事項ｃ】	公表内容の事例のうち「サイバーセキュリティに関する責任者の知見」の記載例をお教え願いたい。 対外向けにサイバーセキュリティ経営宣言をホームページ等で常時公表する場合、責任者の変更の都度、「サイバーセキュリティに関する責任者の知見」内容を変更するものではなく、責任者の属人的な内容ではなく、役割に応じた記載をするものと考えている。
7	全銀協	ガイドライン案	2.1.1. 基本方針、規程類の策定等 ②③	②と③はいずれもサイバーセキュリティ管理態勢の整備、十分な検証・議論を求める事項だが、②は合議体、③は人物と役割を果たす責任主体の違いにフォーカスして項目が分けられているという理解で相違ないか。
8	全銀協	ガイドライン案	2.1.2. 規程等及び業務プロセスの整備 ①	規程等に含めることを求める「セキュリティ・バイ・デザイン」とは、具体的には2.3.4.3.に述べられている事項という理解で相違ないか。
9	全銀協	ガイドライン案	2.2.1.2. ハードウェア・ソフトウェア等 b	"必要に応じて、サードパーティの資産についても管理対象とする"とあるが、望ましいと考えられる管理基準や管理対象とする資産の範囲について、想定があれば例示いただきたい。 また、設定する管理基準によっては、各種法令（個人情報保護法や不正競争防止法、著作権法等）に抵触する可能性があるため、サードパーティとの契約締結時に十分に内容確認が必要であることを注記してはいかがか。
10	全銀協	ガイドライン案	2.2.1.2. ハードウェア・ソフトウェア等 d	本項目で求める事項は、 ・自機関の管理対象外となっている個人所有端末等の情報資産（個人所有のPC、スマートフォン、USBメモリ等）から自機関のネットワークにアクセスできないように制御すること、 ・自機関の管理対象端末から未承認のクラウドサービスの利用を制御すること の２点だと解釈した。この認識が合っている場合、管理対象とするか使用中止を求めるのではなく、アクセス・利用の制御対応を求めることを、より明確に表現してはいかがか。
11	全銀協	ガイドライン案	2.2.2.2. リスクの特定・評価 b	「深刻だが現実に起こりうる多様なシナリオ」について解釈が難しいため、想定されている事例があれば例示いただきたい。
12	全銀協	ガイドライン案	2.2.3. ハードウェア・ソフトウェア等の脆弱性管理 ⑥、a	サードパーティが保有するシステムとは、システム子会社やシステムベンダー、クラウドサービス事業者が自機関に提供するシステムやクラウドサービスのことではなく、サードパーティが自社で保有・使用するシステムのことで相違ないか。その場合、自機関に提供するシステムやクラウドサービスであっても「脆弱性対応状況につき非開示」とするサードパーティもあるため、自社保有システムに関してはよりその傾向が強くなり、本事項の達成が困難と推察する。 また、各種法令（不正競争防止法や著作権法等）やサードパーティと締結している契約に抵触しないよう、十分に内容確認が必要であることを注記してはいかがか。
13	全銀協	ガイドライン案	2.2.3. ハードウェア・ソフトウェア等の脆弱性管理 ⑥、a	本事項で指す「脆弱性対応の管理」とは、サードパーティにヒアリングを行い、会社として脆弱性対応に係る回答を得るという対応で充足するか。その場合、第三者保証による報告書の活用等と同様に例示してはいかがか。 全サードパーティについて、個別の保有システムを洗い出し、それぞれの脆弱性対応結果を整理するのは非現実的であり、本事項は達成困難と考えられるため。
14	全銀協	ガイドライン案	2.2.4.脆弱性診断及びペネトレーションテスト b.TLPTの定期実施、実施に際しての留意点	留意事項に見合う業者の選定やテスト水準の担保を金融機関が個別にやっていくことは難しいと思料するので、例えば、認定された業者から選定することができるような仕組みの検討をお願いしたい。
15	全銀協	ガイドライン案	2.2.5. 演習・訓練 d	「組み合わせて実施」とは、各システムに対して複数の訓練・演習等を複合的に実施することではなく、自機関として必要な訓練・演習等を複合的かつ戦略的に実施することを意図しているか。 その場合、「自機関に必要な訓練・演習等を組み合わせて実施すること」と表現してはいかがか。
16	全銀協	ガイドライン案	2.3.4.1.a.	事業者がセキュリティ・バイ・デザイン等をとりいれているかどうかについて、どのようにすれば確認できるのか、何か具体的方法で想定しているものはあるのか。
17	全銀協	ガイドライン案	2.6. サードパーティリスク管理 a. サードパーティリスク管理に係る統括部署に適切な知識等を有する人員の配置 をすること。	サードパーティリスク管理における「適切な知識等を有する人員」の適切な知識等はサイバーセキュリティに限らないと思われるが、どのような人員が望まれるか、業務経験や資格等の具体例を示していただきたい。
18	全銀協	ガイドライン案	2.3.4.3	外部委託先等がセキュリティ・バイ・デザインを実施する体制になっているかどうかについて、どのようにすれば確認できるのか、何か具体的方法で想定しているものはあるのか。
19	全銀協	ガイドライン案	2.3.4.3セキュリティ・バイ・デザイン ②外部委託先等において、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること。	各金融機関それぞれが委託先等のセキュリティ・バイ・デザインの体制を確認する場合、双方（委託先・金融機関ともに）の確認負荷が社会的コストになりうるため、公的なセキュリティ・バイ・デザインの実施体制の認定制度等の導入を検討いただきたい。斯かる認定制度があれば、金融機関は、委託先の認定状況を確認するだけでよく、また、委託先側も複数の金融機関から類似の個別照会を受けることなく、社会的コストを削減できるものと考える。
20	全銀協	ガイドライン案	2.3.4.3. セキュリティ・バイ・デザイン ②	ここでいう「外部委託先等」とは、自機関にシステムやクラウドサービスを提供するシステム子会社やシステムベンダー、クラウドサービス事業者を指しているか。その場合、「サードパーティ等において、自機関に提供するシステムやクラウドサービスを開発するに際してセキュリティ・バイ・デザインを実施できる体制になっているかを確認すること。」と表現してはいかがか。 仮にp9 注釈17の通り、「外部委託先等」が業務を委託している組織を指す場合は、業務の委託先でセキュリティ・バイ・デザインを実施するか否かは委託元の金融機関に影響を与えず、対応を求められる理由が不明瞭なため、理由を明示いただきたい。
21	全銀協	ガイドライン案	2.3.4.5	クラウド事業者は、サードパーティとして、「2.6. サードパーティリスク管理」に記載の対応が求められると思われるが、明確化の観点からその旨を記載したほうがいいのではないか。
22	全銀協	ガイドライン案	2.6.⑧	金融機関等よりも優越的な立場にあるサードパーティ等が相応に存在する中で、契約書やSLA等の文言を自社様式から頑なに変更しないケースも容易に想定される。各金融機関が円滑に進められるよう、御庁からも他省庁や他業界に対して強く働きかけをお願いしたい。