系統金融機関向けの総合的な監督指針　新旧対照表

改正後	現行
Ⅱ　系統金融機関監督上の評価項目	Ⅱ　系統金融機関監督上の評価項目
Ⅱ－３　業務の適切性	Ⅱ－３　業務の適切性
Ⅱ－３－４　システムリスク	Ⅱ－３－４　システムリスク
Ⅱ－３－４－１　システムリスク	Ⅱ－３－４－１　システムリスク
Ⅱ－３－４－１－２　主な着眼点【共通】	Ⅱ－３－４－１－２　主な着眼点【共通】
(1)～(4)　（略）	(1)～(4)　（略）
(5) サイバーセキュリティ管理	(5) サイバーセキュリティ管理
①　経営管理委員会又は理事会等は、サイバーセキュリティの重要性を認識し、「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」を踏まえ、必要な態勢を整備しているか。	①　サイバーセキュリティについて、経営管理委員会又は理事会等は、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。
（削除）	②　サイバーセキュリティについて、組織態勢の整備、内部規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。 ・サイバー攻撃に対する監視態勢 ・サイバー攻撃を受けた際の報告及び広報態勢 ・組織内 CSIRT（Computer Security Incident Response Team）の設置 ・情報共有機関等を通じた情報収集・共有体制　等
（削除）	③　サイバー攻撃に備え、次のような入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。 ・入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入　等）

改正後	現行
	・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）
	・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）
（削除）	④　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に、以下のような措置を講じているか。
	・攻撃元の IP アドレスの特定と遮断
	・自動的にアクセスを分散させる機能
	・システムの全部又は一部の一時的停止　等
（削除）	⑤　システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。
（削除）	⑥　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。
②　インターネット等の通信手段を利用した非対面の取引を行う場合には、Ⅱ―３－５－２（２）又はⅡ－３－６－２（２）によるセキュリティの確保を講じているか。	⑦　インターネット等の通信手段を利用した非対面の取引を行う場合には、Ⅱ-３－５－２（２）又はⅡ－３－６－２（２）によるセキュリティの確保を講じているか。
なお、全国銀行協会の申し合わせ等には、以下のような実効的な認証方式や不正防止策を用いたセキュリティ対策事例が記載されている。	なお、全国銀行協会の申し合わせ等には、以下のような実効的な認証方式や不正防止策を用いたセキュリティ対策事例が記載されている。
・可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式	・可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式
・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証	・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証

改正後	現行
・ハードウェアトークン等でトランザクション署名を行うトランザクション認証 ・電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用 ・取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供 ・利用者のパソコンのウィルス感染状況を系統金融機関側で検知し、警告を発するソフトの導入 ・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備　等 （注）キャッシュカード暗証番号のような組み合わせの数が僅少な情報を記憶要素として用いる認証方式は、インターネット上での利用を避けることが望ましいことに留意。	・ハードウェアトークン等でトランザクション署名を行うトランザクション認証 ・電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用 ・取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供 ・利用者のパソコンのウィルス感染状況を系統金融機関側で検知し、警告を発するソフトの導入 ・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備　等 （注）キャッシュカード暗証番号のような組み合わせの数が僅少な情報を記憶要素として用いる認証方式は、インターネット上での利用を避けることが望ましいことに留意。
③　（略）	⑧　インターネットバンキング等の不正利用を防止するため、電話番号やメールアドレスなど預貯金者への通知や本人認証の際に利用される情報について、不正な登録・変更が行われないよう適切な手続が定められているか。
（削除）	⑨　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。
（削除）	⑩　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。
(6)～(10)　（略）	(6)～(10)　（略）

改正後	現行
Ⅱ－３－４－２　ＡＴＭシステムのセキュリティ対策 Ⅱ－３－４－２－２　主な着眼点【共通】 (1)　（略） (2) セキュリティの確保 ①　キャッシュカードやＡＴＭシステムについて、そのセキュリティ・レベルを一定の基準に基づき評価するとともに、当該評価を踏まえ、一定のセキュリティ・レベルを維持するために体制・技術、両面での検討を行い、適切な対策を講じているか。その際、情報セキュリティに関する検討会の検討内容等を踏まえ、体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの利用者や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。セキュリティの確保に当たっては、「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」も参照すること。 ②　（略） ③　高リスクの高額取引をＡＴＭシステムにおいて行っている場合、それに見合ったセキュリティ対策を講じているか。特に脆弱性が指摘される磁気カードについては、そのセキュリティを補強するための方策を検討しているか。 （参考１）セキュリティに関する基準としては、「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」のほか、「金融機関等コンピュータシステムの安全対策基準・解説書」（金融情報システムセンター）などがある。	Ⅱ－３－４－２　ＡＴＭシステムのセキュリティ対策 Ⅱ－３－４－２－２　主な着眼点【共通】 (1)　（略） (2) セキュリティの確保 ①　キャッシュカードやＡＴＭシステムについて、そのセキュリティ・レベルを一定の基準に基づき評価するとともに、当該評価を踏まえ、一定のセキュリティ・レベルを維持するために体制・技術、両面での検討を行い、適切な対策を講じているか。その際、情報セキュリティに関する検討会の検討内容等を踏まえ、体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの利用者や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。 ②　（略） ③　高リスクの高額取引をＡＴＭシステムにおいて行っている場合、それに見合ったセキュリティ対策を講じているか。特に脆弱性が指摘される磁気カードについては、そのセキュリティを補強するための方策を検討しているか。 （参考１）セキュリティに関する基準としては、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター編）などがある。

改正後	現行
（参考２）リスクの把握に当たって参考となるものとしては、情報セキュリティに関する検討会における検討資料がある。	（参考２）リスクの把握に当たって参考となるものとしては、情報セキュリティに関する検討会における検討資料がある。
(3)・(4)　（略）	(3)・(4)　（略）
Ⅱ－３－５　インターネットバンキング	Ⅱ－３－５　インターネットバンキング
Ⅱ－３－５－２　主な着眼点【共通】	Ⅱ－３－５－２　主な着眼点【共通】
(1)　（略）	(1)　（略）
(2) セキュリティの確保	(2) セキュリティの確保
①　（略）	①　（略）
②　インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。 　また、当該プログラム等に沿って個人・法人等の利用者属性を勘案しつつ、「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」や一般社団法人全国銀行協会の申し合わせ等も踏まえ、取引のリスクに見合ったセキュリティ対策を講じているか。 　その際、犯罪手口の高度化・巧妙化等（暗号通信を行う二者の間に第三者が割り込み、盗聴や介入する「中間者攻撃」やウェブ上で不正操作をし、送金を行う「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。	②　インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。 　また、当該プログラム等に沿って個人・法人等の利用者属性を勘案しつつ、一般社団法人全国銀行協会の申し合わせ等も踏まえ、取引のリスクに見合ったセキュリティ対策を講じているか。 　その際、犯罪手口の高度化・巧妙化等（暗号通信を行う二者の間に第三者が割り込み、盗聴や介入する「中間者攻撃」やウェブ上で不正操作をし、送金を行う「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。
③　（略）	③　（略）
(3)・(4)　（略）	(3)・(4)　（略）
Ⅱ－３－６ 外部の決済サービス事業者等との連携【共通】	Ⅱ－３－６ 外部の決済サービス事業者等との連携【共通】

改正後	現行
Ⅱ－３－６－２ 主な着眼点	Ⅱ－３－６－２ 主な着眼点
(1) （略）	(1) （略）
(2) セキュリティの確保	(2) セキュリティの確保
①・② （略）	①・② （略）
③ 預貯金口座との連携を行う際に、固定式の ID・パスワードによる本人認証に加えて、ハードウェアトークン・ソフトウェアトークンによる可変式パスワードを用いる方法や公的個人認証を用いる方法などで本人認証を実施するなど、実効的な要素を組み合わせた多要素認証等の導入により預貯金者へのなりすましを阻止する対策を導入しているか。	③ 預貯金口座との連携を行う際に、固定式の ID・パスワードによる本人認証に加えて、ハードウェアトークン・ソフトウェアトークンによる可変式パスワードを用いる方法や公的個人認証を用いる方法などで本人認証を実施するなど、実効的な要素を組み合わせた多要素認証等の導入により預貯金者へのなりすましを阻止する対策を導入しているか。
（注）実効的な認証方式についてはⅡ－３－４－１－２（５）②を参照。なお、実効的な認証方式などのセキュリティ対策は、情報通信技術の進展により様々な方式が新たに開発されていることから、定期的又は必要に応じて見直しを行う必要があることに留意。	（注）実効的な認証方式についてはⅡ－３－４－１－２（５）⑦を参照。なお、実効的な認証方式などのセキュリティ対策は、情報通信技術の進展により様々な方式が新たに開発されていることから、定期的又は必要に応じて見直しを行う必要があることに留意。
④～⑨ （略）	④～⑨ （略）
(3) （略）	(3) （略）
Ⅵ 特定信用事業電子決済等代行業及び農林中央金庫電子決済等代行業	Ⅵ 特定信用事業電子決済等代行業及び農林中央金庫電子決済等代行業
Ⅵ－３ システムリスク	Ⅵ－３ システムリスク
Ⅵ－３－２ 主な着眼点	Ⅵ－３－２ 主な着眼点
(1)・(2) （略）	(1)・(2) （略）
(3) サイバーセキュリティ管理	(3) サイバーセキュリティ管理

改正後	現行
経営上責任を負う立場の者は、サイバーセキュリティの重要性を認識し、「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」を踏まえ、必要な態勢を整備しているか。	① サイバーセキュリティについて、経営上責任を負う立場の者は、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。
（削除）	② サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。 ・サイバー攻撃に対する監視体制 ・サイバー攻撃を受けた際の報告及び広報体制 ・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制 ・情報共有機関等を通じた情報収集・共有体制　等
（削除）	③ 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サイバーセキュリティ対策を組み合わせた多層防御を講じているか。 ・入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入　等） ・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） ・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）
（削除）	④ 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に、以下のような措置を講じているか。 ・攻撃元の IP アドレスの特定と遮断 ・DDoS 攻撃に対して自動的にアクセスを分散させる機能

改正後	現行
	・システムの全部又は一部の一時的停止　等
（削除）	⑤　システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。
（削除）	⑥　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。
（削除）	⑦　サイバー攻撃を想定したコンティンジェンシープラン（緊急時対応計画）を策定し、訓練や見直しを実施し、高度化を図っているか。
(4)・(5)　（略）	(4)・(5)　（略）

附　則

この通知の改正は、令和６年 10 月４日から適用する。