中小・地域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－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－３－４－１－１　意義	Ⅱ－３－４－１－１　意義
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のシステムの不備等に伴い、顧客や銀行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銀行が損失を被るリスクをいうが、銀行の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、銀行の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏えい等のリスクが大きくなっている。システムが安全かつ安定的に稼動することは決済システム及び銀行に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 他方、金融機関の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や金融機関のビジネスモデルを左右する重要課題となっており、金融機関において経営戦略を IT 戦略と一体的に考えていく必要性が増している。こうした観点から、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである「IT ガバナンス」が適切に機能することが極めて重要となっている。 また、新型コロナウイルス感染症の影響により新たな日常に移行していく中、業務継続及び生産性向上の観点から、金融機関内の連絡手段や顧客との日常的・継続的な接触手段として、情報セキュリティの確保を踏まえた上での電子メール等の情報通信基盤の整備も不可欠となる。	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のシステムの不備等に伴い、顧客や銀行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銀行が損失を被るリスクをいうが、銀行の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、銀行の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏えい等のリスクが大きくなっている。システムが安全かつ安定的に稼動することは決済システム及び銀行に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 他方、金融機関の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や金融機関のビジネスモデルを左右する重要課題となっており、金融機関において経営戦略を IT 戦略と一体的に考えていく必要性が増している。こうした観点から、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである「IT ガバナンス」が適切に機能することが極めて重要となっている。 また、新型コロナウイルス感染症の影響により新たな日常に移行していく中、業務継続及び生産性向上の観点から、金融機関内の連絡手段や顧客との日常的・継続的な接触手段として、情報セキュリティの確保を踏まえた上での電子メール等の情報通信基盤の整備も不可欠となる。
（参考）金融機関の IT ガバナンスに関する対話のための論点・プラクテ	（参考）金融機関の IT ガバナンスに関する対話のための論点・プラクテ

改正後	現行
ィスの整理第２版（令和５年６月）	ィスの整理（令和元年６月）
Ⅱ－３－４－１－２　主な着眼点	Ⅱ－３－４－１－２　主な着眼点
（１）～（４）　（略）	（１）～（４）　（略）
（５）サイバーセキュリティ管理 ①　取締役会等は、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。	（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。
（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。

改正後	現行
（削除） （削除） ②　（略）	・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 ・システムの全部又は一部の一時的停止　等 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。 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。 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。 ・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 ・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

改正後	現行
③　（略）	の利用を避けることが望ましいことに留意。 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き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）
Ⅱ－３－４－２　ＡＴＭシステムのセキュリティ対策	Ⅱ－３－４－２　ＡＴＭシステムのセキュリティ対策
Ⅱ－３－４－２－１　（略）	Ⅱ－３－４－２－１　（略）
Ⅱ－３－４－２－２　主な着眼点	Ⅱ－３－４－２－２　主な着眼点
（１）　（略）	（１）　（略）
（２）セキュリティの確保 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、自らの顧客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	（２）セキュリティの確保 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、自らの顧客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。

改正後	現行
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。 　預貯金者保護法等を踏まえ、適切な認証技術の採用、情報漏洩の防止、異常取引の早期検知等、不正払戻し防止のための措置が講じられているか。その際、顧客の負担が過重なものとならないよう配慮するとともに、互換性の確保などにより利用者利便に支障を及ぼさないよう努めているか。 　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。 （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） Ⅱ－３－５　インターネットバンキング Ⅱ－３－５－２　主な着眼点 （１）　（略） （２）セキュリティの確保 　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	預貯金者保護法等を踏まえ、適切な認証技術の採用、情報漏洩の防止、異常取引の早期検知等、不正払戻し防止のための措置が講じられているか。その際、顧客の負担が過重なものとならないよう配慮するとともに、互換性の確保などにより利用者利便に支障を及ぼさないよう努めているか。 　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」（金融情報システムセンター）などがある。 （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） Ⅱ－３－５　インターネットバンキング Ⅱ－３－５－２　主な着眼点 （１）　（略） （２）セキュリティの確保 　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

改正後	現行
顧客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、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。 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、プログラム等に沿って個人・法人等の顧客属性を勘案しつつ、「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（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。 ウェブページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。また、フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。	顧客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、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。 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、プログラム等に沿って個人・法人等の顧客属性を勘案しつつ、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（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。 ウェブページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。また、フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。
（注）情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、金融庁・警察当局から提供された犯罪手口に係る情報などを活用することが考えられる。	（注）情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、金融庁・警察当局から提供された犯罪手口に係る情報などを活用することが考えられる。
（参考） ・セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成 24 年１月、25 年 11 月、26 年５月、26 年７月等） ・インターネット・バンキングにおいて留意すべき事項について（全国銀行協会） ・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	（参考） ・セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成 24 年１月、25 年 11 月、26 年５月、26 年７月等） ・インターネット・バンキングにおいて留意すべき事項について（全国銀行協会） ・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

改正後	現行
情報システムセンター） ・情報セキュリティに関する検討会における検討資料 （３）～（４）　（略） Ⅱ－３－６　外部の決済サービス事業者等との連携 Ⅱ－３－６－２　主な着眼点 （１）　（略） （２）セキュリティの確保 ①・②　（略） ③　預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。 ④～⑨　（略） Ⅳ　銀行代理業等 Ⅳ－２　電子決済等取扱業	情報システムセンター） ・情報セキュリティに関する検討会における検討資料 （３）～（４）　（略） Ⅱ－３－６　外部の決済サービス事業者等との連携 Ⅱ－３－６－２　主な着眼点 （１）　（略） （２）セキュリティの確保 ①・②　（略） ③　預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）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） Ⅳ　銀行代理業等 Ⅳ－２　電子決済等取扱業

改正後	現行
Ⅳ－２－３　システムリスク Ⅳ－２－３－１　主な着眼点 （１）・（２）　（略） （３）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の対応 ①　Ⅱ－３－４－１－２（５）②の事例のほか、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。 イ．可変式パスワード、生体認証、電子証明書等、実効的な要素を組み合わせた多要素認証などの、固定式の ID・パスワードのみに頼らない認証方式 ロ．ログインパスワードとは別の取引用パスワードの採用（同一のパスワードの設定を不可とすること等の事項に留意すること。） また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式の見直しを行っているか。 ②　Ⅱ－３－４－１－２（５）③に加え、例えば、以下のような業務に応じた不正防止策を講じているか。 ・不正な IP アドレスからの通信の遮断・利用者に対し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導入・最新化を促す措置 ・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 ・不正が確認された ID の利用停止 ・前回ログイン（ログオフ）日時の画面への表示 ・取引時の利用者への通知　等 ③　（略）	Ⅳ－２－３　システムリスク Ⅳ－２－３－１　主な着眼点 （１）・（２）　（略） （３）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の対応 ①　Ⅱ－３－４－１－２（５）⑦の事例のほか、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。 イ．可変式パスワード、生体認証、電子証明書等、実効的な要素を組み合わせた多要素認証などの、固定式の ID・パスワードのみに頼らない認証方式 ロ．ログインパスワードとは別の取引用パスワードの採用（同一のパスワードの設定を不可とすること等の事項に留意すること。） また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式の見直しを行っているか。 ②　Ⅱ－３－４－１－２（５）⑧に加え、例えば、以下のような業務に応じた不正防止策を講じているか。 ・不正な IP アドレスからの通信の遮断・利用者に対し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導入・最新化を促す措置 ・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 ・不正が確認された ID の利用停止 ・前回ログイン（ログオフ）日時の画面への表示 ・取引時の利用者への通知　等 ③　（略）

改正後	現行
Ⅳ－３　電子決済等代行業	Ⅳ－３　電子決済等代行業
Ⅳ－３－３　システムリスク	Ⅳ－３－３　システムリスク
Ⅳ－３－３－２　主な着眼点	Ⅳ－３－３－２　主な着眼点
（１）・（２）　（略）	（１）・（２）　（略）
（３）サイバーセキュリティ管理 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。	（３）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、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

改正後	現行
	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 ・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。