主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
【本編】 Ⅲ－３－７　システムリスク Ⅲ－３－７－１　システムリスク Ⅲ－３－７－１－１　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。 　特に主要行等のシステムについては、元来、機能が高度である一方、大量処理が求められていることから、規模が大きく、構成が複雑である傾向にある。加えて、累次の経営再編によりシステム構成、システム運用体制が、一層複雑化していることから、特にシステム上の諸課題に的確に対応することが求められている。仮に主要行等において、システム障害が発生した場合は、利用者の社会経済生活、企業等の経済活動、ひいては、我が国経済全体にも極めて大きな影響を及ぼすおそれがあるほか、その影響は単に一銀行の問題にとどまらず、金融システム全体に及びかねないことから、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。 （新設） （参考）　（略）	**【本編】** Ⅲ－３－７　システムリスク Ⅲ－３－７－１　システムリスク Ⅲ－３－７－１－１　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。 特に主要行等のシステムについては、元来、機能が高度である一方、大量処理が求められていることから、規模が大きく、構成が複雑である傾向にある。加えて、累次の経営再編によりシステム構成、システム運用体制が、一層複雑化していることから、特にシステム上の諸課題に的確に対応することが求められている。仮に主要行等において、システム障害やサイバーセキュリティ事案が発生した場合は、利用者の社会経済生活、企業等の経済活動、ひいては、我が国経済全体にも極めて大きな影響を及ぼすおそれがあるほか、その影響は単に一銀行の問題にとどまらず、金融システム全体に及びかねないことから、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。 （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。 （参考）　（略）

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
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 ①　（略） ②　代表取締役は、システム障害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。 ③　（略） ④　代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害発生等の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。 　また、自らが指揮を執る訓練を行い、その実効性を確保しているか。 （２）システムリスク管理態勢 ①・②　（略） ③　システムリスク管理体制の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。 　また、システムリスク管理体制は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。 （３）システムリスク評価 ①　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。 ②・③　（略） （４）安全対策 ①　安全対策の基本方針が策定されているか。	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 ①　（略） 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。 ③　（略） ④　代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。 　また、自らが指揮を執る訓練を行い、その実効性を確保しているか。 （２）システムリスク管理態勢 ①・②　（略） ③　システムリスク管理態勢の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。 　また、システムリスク管理態勢は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。 （３）システムリスク評価 ①　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。 ②・③　（略） （４）情報セキュリティ管理 ①　情報資産を適切に管理するために方針の策定、組織体制の整備、社内規程の策定、内部管理態勢の整備を図っているか。また、他社における不正・不祥事件も参考に、情報セキュリティ管理態勢の PDCA サイクルによる継続的な改善を図っているか。

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
②　定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。	②　情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、管理者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。
③　銀行以外の者が占有管理する端末機等（入出力装置等を含む。）を利用する資金移動取引については、コンピュータシステムの事故防止対策、不正使用防止対策、不正アクセス防止対策、取引者のプライバシー保護対策が施されているか。	③　コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。
（新設）	④　金融機関が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。 顧客の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。 ・通常の業務では使用しないシステム領域に格納されたデータ ・障害解析のためにシステムから出力された障害解析用データ ・ＡＴＭ（店舗外含む）等に保存されている取引ログ　等
（新設）	⑤　洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。 また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。 ・情報の暗号化、マスキングのルール ・情報を利用する際の利用ルール ・記録媒体等の取扱いルール　等
（新設）	⑥　顧客の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。 ・職員の権限に応じて必要な範囲に限定されたアクセス権限の付与 ・アクセス記録の保存、検証 ・開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制　等
（新設）	⑦　機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。 なお、「機密情報」とは、暗証番号、パスワード、クレジットカード

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
	情報等、顧客に損失が発生する可能性のある情報をいう。
（新設）	⑧　機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。
（新設）	⑨　情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。
（新設）	⑩　セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む）を行っているか。
（新設）	（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。 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 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） 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 ・システムの全部又は一部の一時的停止　等

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
	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、Ⅲ-３－８－２（２）によるセキュリティの確保を講じているか。 認証方式や不正防止策として、全国銀行協会の申し合わせ等には、以下のような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 ・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 ・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 ・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 ⑧　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。 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）システム企画・開発・運用管理 ①～⑥　（略）	（６）システム企画・開発・運用管理 ①～⑥　（略）
（６）システム監査	（７）システム監査

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
①～④　（略）	①～④　（略）
（７）外部委託管理 ①　（略） ②　外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。 ③　システムに係る外部委託業務について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。 システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。 ④　外部委託した業務について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。 また、外部委託先任せにならないように、例えば委託元として要員を配置するなどの必要な措置を講じているか。特に共同センターの内部管理、開発・運用管理の状況について、報告を受けているか。 さらに、システムの共同化等が進展する中、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。 ⑤　（略）	（８）外部委託管理 ①　（略） ②　外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。また、外部委託先の役職員が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。 ③　システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。 システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。 ④　外部委託した業務（二段階以上の委託を含む）について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか また、外部委託先任せにならないように、例えば委託元として要員を配置するなどの必要な措置を講じているか。特に共同センターの内部管理、開発・運用管理の状況について、報告を受けているか。 さらに、システムの共同化等が進展する中、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。 ⑤　（略）
（８）データ管理態勢 ①　データについて機密性等の確保のため、データ管理者を置いているか。 ②　データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。	（削除）
（９）コンティンジェンシープラン	（９）コンティンジェンシープラン

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
①～③　（略）	①～③　（略）
④　コンティンジェンシープランは、他の金融機関におけるシステム障害事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。	④　コンティンジェンシープランは、他の金融機関におけるシステム障害等の事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。
⑤　（略）	⑤　（略）
⑥　業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害が発生した場合等に、速やかに業務を継続できる態勢を整備しているか。	⑥　業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害等が発生した場合に、速やかに業務を継続できる態勢を整備しているか。
（10）障害発生時の対応	（10）障害発生時等の対応
①　システム障害が発生した場合に、顧客に対し無用の混乱を生じさせないよう、適切な措置を講じているか。 　また、システム障害の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢となっているか。	①　システム障害等が発生した場合に、顧客に対し無用の混乱を生じさせないよう、適切な措置を講じているか。 　また、システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢となっているか。
②　システム障害の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。	②　システム障害等の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。
③　経営に重大な影響を及ぼすシステム障害が発生した場合に、速やかに代表取締役をはじめとする取締役に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。 　また、必要に応じて、対策本部を立ち上げ、代表取締役等自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。	③　経営に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに代表取締役をはじめとする取締役に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。 　また、必要に応じて、対策本部を立ち上げ、代表取締役等自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。
④　システム障害の発生に備え、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。	④　システム障害等の発生に備え、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。
⑤　システム障害が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、顧客からの問い合わせに的確に対応するため、必要に応じ、コールセンターの開設等を迅速に行っているか。 　また、システム障害の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。	⑤　システム障害等が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、顧客からの問い合わせに的確に対応するため、必要に応じ、コールセンターの開設等を迅速に行っているか。 　また、システム障害等の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。
⑥　システム障害の発生原因の究明、復旧までの影響調査、改善措置、再	⑥　システム障害等の発生原因の究明、復旧までの影響調査、改善措置、

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
発防止策等を的確に講じているか。 　また、システム障害の原因等の定期的な傾向分析を行い、それに応じた対応策をとっているか。 ⑦　システム障害の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。 （注）　（略） （参考）　（略）	再発防止策等を的確に講じているか。 　また、システム障害等の原因等の定期的な傾向分析を行い、それに応じた対応策をとっているか。 ⑦　システム障害等の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。 （注）　（略） （参考）　（略）
Ⅲ－３－７－１－３　監督手法・対応	Ⅲ－３－７－１－３　監督手法・対応
（１）障害発生時 ①　一般的な対応 イ．コンピュータシステムの障害の発生を認識次第、直ちに、その事実を当局宛てに報告を求めるとともに、「障害等発生報告書」（様式・参考資料編　様式４－４５）にて当局宛て報告を求めるものとする。 　また、復旧時、原因解明時には改めてその旨報告を求めることとする。 　ただし、復旧原因の解明がされていない場合でも、１か月以内に現状についての報告を行うこととする。 （注）報告すべきシステム障害等 　その原因の如何を問わず、銀行等が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、 ａ．預金の払戻し、為替等の決済機能に遅延、停止等が生じているもの又はそのおそれがあるもの。 ｂ．資金繰り、財務状況把握等に影響があるもの又はそのおそれがあるもの。 ｃ．その他業務上、上記に類すると考えられるもの。 をいう。 　ただし、一部のシステム・機器にこれらの影響が生じても、他のシステム・機器が速やかに交替することで実質的にはこれらの影響が生じない場合（例えば、一部のＡＴＭが停止した場合であっても他の同一店舗若しくは近隣店舗ＡＴＭや窓口において対応が可能な場合。）を除く。	（１）障害発生時 ①　一般的な対応 イ．コンピュータシステムの障害やサイバーセキュリティ事案の発生を認識次第、直ちに、その事実を当局宛てに報告を求めるとともに、「障害等発生報告書」（様式・参考資料編　様式４－４５）にて当局宛て報告を求めるものとする。 　また、復旧時、原因解明時には改めてその旨報告を求めることとする。 　ただし、復旧原因の解明がされていない場合でも、１か月以内に現状についての報告を行うこととする。 （注）報告すべきシステム障害等 　その原因の如何を問わず、銀行等が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、 ａ．預金の払戻し、為替等の決済機能に遅延、停止等が生じているもの又はそのおそれがあるもの ｂ．資金繰り、財務状況把握等に影響があるもの又はそのおそれがあるもの ｃ．その他業務上、上記に類すると考えられるもの をいう。 　ただし、一部のシステム・機器にこれらの影響が生じても、他のシステム・機器が速やかに交替することで実質的にはこれらの影響が生じない場合（例えば、一部のＡＴＭが停止した場合であっても他の同一店舗若しくは近隣店舗ＡＴＭや窓口において対応が可能な場合。）を除く。

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、上記のような障害が発生する可能性が高いと認められる時は、報告を要するものとする。	なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、顧客や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。
ロ.　（略）	ロ.　（略）
②　緊急対応	②　緊急対応
特に、大規模な障害の場合や障害の原因の解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及び店頭等における顧客対応等のコンティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請し、法第24条に基づき速やかな報告を求める。	特に、大規模なシステム障害等の場合や障害の原因の解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及び店頭等における顧客対応等のコンティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請し、法第 24 条に基づき速やかな報告を求める。
さらに、大規模な障害の復旧の見通しが不確実であり、市場取引、ＡＴＭ取引・口座振替・給与振込等の決済システムに大きな影響が生じている場合には、早期に法第26条に基づく業務改善命令を発出することを検討する等の対応を行う。	さらに、大規模なシステム障害等の復旧の見通しが不確実であり、市場取引、ＡＴＭ取引・口座振替・給与振込等の決済システムに大きな影響が生じている場合には、早期に法第 26 条に基づく業務改善命令を発出することを検討する等の対応を行う。
（２）～（４）　（略）	（２）～（４）　（略）
Ⅲ－３－７－２・Ⅲ－３－７－３　（略）	Ⅲ－３－７－２・Ⅲ－３－７－３　（略）
Ⅲ－３－８ インターネットバンキング	Ⅲ－３－８ インターネットバンキング
Ⅲ－３－８－１ 意義 （略）	Ⅲ－３－８－１ 意義 （略）
Ⅲ－３－８－２ 主な着眼点	Ⅲ－３－８－２ 主な着眼点
（１）内部管理態勢の整備	（１）内部管理態勢の整備
インターネットバンキングに係る犯罪行為に対する対策等について、最優先の経営課題の一つとして位置付け、取締役会等において必要な検討を行い、セキュリティ・レベルの向上に努めているか。また、インターネットバンキングの健全かつ適切な業務の運営を確保するため、銀行内の各部門が的確な状況認識を共有し、銀行全体として取り組む態勢が	インターネットバンキングに係る犯罪行為に対する対策等について、犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、最優先の経営課題の一つとして位置付け、取締役会等において必要な検討を行い、セキュリティ・レベルの向上に努めるとともに、利用時における留意事項等を顧客に説明する態勢が整備されているか。また、インター

現　　行	改　正　後
整備されているか。	ネットバンキングの健全かつ適切な業務の運営を確保するため、銀行内の各部門が的確な状況認識を共有し、銀行全体として取り組む態勢が整備されているか。
その際、犯罪の発生状況などを踏まえ、自らの顧客や業務の特性に応じた検討を行った上で、必要な態勢の整備に努めているか。	その際、情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努めているか。
加えて、リスク分析、セキュリティ対策の策定・実施、効果の検証、対策の評価・見直しからなるいわゆるＰＤＣＡサイクルが機能しているか。	加えて、リスク分析、セキュリティ対策の策定・実施、効果の検証、対策の評価・見直しからなるいわゆるＰＤＣＡサイクルが機能しているか。
（２）セキュリティの確保	（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・種類を決定しているか。	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、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、必要に応じて見直す体制を整えているか。特に、本人認証については、個々の認証方式の各種犯罪手口に対する強度を検証した上で、個人・法人等の顧客属性を勘案し、例えば、可変式パスワードや電子証明書といった、固定式のＩＤ・パスワードのみに頼らない認証方式の導入を図るなど、取引のリスクに見合った適切な認証方式を選択しているか。	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。
ホーム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。	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）（略）	（注）　（略）
	（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」

現　　行	改　正　後
	（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（金融情報システムセンター）
（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。	・情報セキュリティに関する検討会における検討資料
（３）顧客対応 インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクについて、顧客に対する十分な説明態勢が整備されているか。 顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。 顧客からの届出を速やかに受け付ける体制が整備されているか。また、顧客への周知（公表を含む。）が必要な場合、速やかに周知できる体制が整備されているか。特に、被害にあう可能性がある顧客を特定可能な場合は、可能な限り迅速に顧客に連絡するなどして被害を最小限に抑制するための措置を講じることとしているか。 不正取引に係る損失の補償については、預貯金者保護法の趣旨を踏まえ、利用者保護を徹底する観点から、顧客対応方針等を定めるほか、真摯な顧客対応を行う態勢が整備されているか。 不正取引に関する記録を適切に保存するとともに、顧客や捜査当局から当該資料の提供などの協力を求められたときは、これに誠実に協力することとされているか。	（３）顧客対応 インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、顧客に求められるセキュリティ対策事例の周知を含めた注意喚起等が顧客に対して十分に行われる態勢が整備されているか。 顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。 顧客からの届出を速やかに受け付ける体制が整備されているか。また、顧客への周知（公表を含む。）が必要な場合、速やかにかつ顧客が容易に理解できる形で周知できる体制が整備されているか。特に、被害にあう可能性がある顧客を特定可能な場合は、可能な限り迅速に顧客に連絡するなどして被害を最小限に抑制するための措置を講じることとしているか。 不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。 不正取引に係る損失の補償については、預貯金者保護法及び全国銀行協会の申し合わせの趣旨を踏まえ、利用者保護を徹底する観点から、個人顧客及び法人顧客への対応方針等を定めるほか、真摯な顧客対応を行う態勢が整備されているか。 不正取引に関する記録を適切に保存するとともに、顧客や捜査当局から当該資料の提供などの協力を求められたときは、これに誠実に協力することとされているか。

主要行等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
（４）　（略） （参考） ・「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」（金融情報システムセンター）	（４）　（略） （参考） ・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（金融情報システムセンター） ・預金等の不正な払戻しへの対応について（平成 20 年２月 19 日：全国銀行協会） ・法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方（平成 26 年７月 17 日：全国銀行協会）
Ⅲ－３－８－３ 監督手法・対応	Ⅲ－３－８－３ 監督手法・対応
（１）　（略）	（１）　（略）
（２）　（略） （参考） ・「預金等の不正な払戻しへの対応」について（平成20 年２月19 日：全国銀行協会）	（２）　（略） （削除）