主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
Ⅲ－３－６－２　ＡＴＭシステムのセキュリティ対策	Ⅲ－３－６－２　ＡＴＭシステムのセキュリティ対策
Ⅲ－３－６－２－１ 意義	Ⅲ－３－６－２－１　意義
利用者ニーズの重視と利用者保護ルールの徹底を図る観点から、その時々の犯罪技術や各行の顧客特性を踏まえながら、キャッシュカード偽造等の犯罪行為に対するＡＴＭシステム全般のセキュリティを確保することが重要である。	ＡＴＭシステムは、簡便・迅速に各種サービスを提供するものであり、顧客にとって利便性が高く、広く活用されている。一方で、ＡＴＭシステムを通じた取引は、非対面で行われるため、異常な取引態様を確認できないことなどの特有のリスクを抱えている。 金融機関が顧客にサービスを提供するにあたっては、顧客の財産を安全に管理することが求められる。従って、利用者利便を確保しつつ、利用者保護の徹底を図る観点から、金融機関にはＡＴＭシステムの情報セキュリティ対策を十分に講じることが要請される。この点、預貯金者保護法（注）は、偽造・盗難キャッシュカード等による預貯金の不正払戻しを未然に防止するため、必要な情報システムの整備を講じること、及び、顧客に対する情報提供、啓発及び知識の普及を銀行等の責務として規定している。
特に、各金融機関のＡＴＭシステムは、統合ＡＴＭスイッチングサービスを通じて相互に接続していることから、仮にセキュリティ対策が脆弱なＡＴＭシステムを放置している金融機関が存在した場合、他の金融機関に対する影響が及ぶこととなるため、「金融機関等コンピュータシステムの安全対策基準」（金融情報システムセンター）等を参照しながら、適切なセキュリティ対策を講ずることが必要である。	また、金融機関のＡＴＭシステムは、統合ＡＴＭスイッチングサービスを通じて他の金融機関と相互に接続していることから、仮にセキュリティ対策が脆弱なＡＴＭシステムを放置している金融機関が存在した場合、他の金融機関に対する影響が及ぶことにも留意し、セキュリティ対策を講じる必要がある。 （注）偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻等からの預貯金者の保護等に関する法律（平成 17 年８月 10 日公布、平成 18 年２月 10 日施行）
Ⅲ－３－６－２－２ 主な着眼点	Ⅲ－３－６－２－２　主な着眼点

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
（１）犯罪技術の巧妙化等の情勢の変化を踏まえ、キャッシュカード偽造等の犯罪行為に対する対策等について、銀行が取り組むべき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。さらに、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。	（１）内部管理態勢の整備 犯罪技術の巧妙化等の情勢の変化を踏まえ、キャッシュカード偽造等の犯罪行為に対する対策等について、銀行が取り組むべき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、ＡＴＭシステムに係る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。 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。 （参考）情報セキュリティに関する検討会で示されたＰＤＣＡサイクル ① 金融機関側に起因するリスクの把握（内部管理態勢の整備状況、システム開発の体制、システムの特性、システムの外部委託の状況等） ② ＡＴＭ利用に関するリスクの把握（取引限度額、利用可能時間、ＡＴＭの設置環境、周辺地域における犯罪発生状況等） ③ 上記リスク特性を踏まえ、どのような犯罪手口・リスクに対処すべきかの優先順位付け ④ 対策の実施 ⑤ 対策の効果の検証、改善
（２）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。	（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

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
認証技術の開発、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、預金者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。また、国際的な業務展開を行っている金融機関については、国際的なセキュリティトレンドに沿った対策を念頭におきながら、必要な検討を行っているか。	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。 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。また、国際的な業務展開を行っている銀行については、国際的なセキュリティトレンドに沿った対策を念頭におきながら、必要な検討を行っているか。 （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」（金融情報システムセンター）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）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。スキミングの可能性、暗証番号及びカードの盗取の危険性、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（ＡＴＭ利用限度額等）、不必要に多くのカードを保有することによる管理上の問題等、キャッシュカード利用に伴う様々なリスクについて、顧客に対する十分な説明体制が整備されているか。	（３）顧客対応 スキミングの可能性、暗証番号及びカードの盗取の危険性、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、ＡＴＭ利用限度額の設定等）、不必要に多くのカードを保有することによる管理上の問題等、キャッシュカード利用に伴う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。

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」に基づき、不正払戻しに係る損失の補償に係る規程等を整備するに当たっては、可能な限り明確かつ具体的な内容とするよう努めるとともに、その内容を顧客に対して十分説明・周知する態勢が整備されているか。 ① 犯罪予防策等に係る自行の対応も踏まえつつ、被害発生後の顧客に対する対応や捜査当局に対する協力に関する対応方針、基準等について、必要な検討を行っているか。 ② 被害が発生した場合の補償のあり方について、約款、顧客対応方針等において、統一的な対応を定めているか。また、専門の顧客対応窓口を設けるなどにより、適切かつ迅速な顧客対応を行う態勢が整備されているか。顧客に対して情報提供等の協力を求めるに当たっては、顧客の年齢、心身の状況等に十分配慮がなされることとされているか。 不正払戻し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。	不正払戻しに係る損失の補償に関する規程等は、預貯金者保護法に基づき、可能な限り明確かつ具体的な内容となっているか。また、その内容を顧客に対して十分説明・周知する態勢が整備されているか。 ① 犯罪予防策等に係る自行の対応も踏まえつつ、被害発生後の顧客に対する対応や捜査当局に対する協力に関する対応方針、基準等について、必要な検討を行っているか。 ② 被害が発生した場合の補償のあり方について、約款、顧客対応方針等において、統一的な対応を定めているか。 ③ 専門の顧客対応窓口を設けるなどにより、適切かつ迅速な顧客対応を行う態勢が整備されているか。顧客に対して情報提供等の協力を求めるに当たっては、顧客の年齢、心身の状況等に十分配慮することとされているか。 不正払戻し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。
（注）ＡＴＭシステムに関し、外部委託がなされている場合であっても必要なセキュリティ対策が講じられているか。	（４）ＡＴＭシステムの運用・管理を外部委託している場合の対策 ＡＴＭシステムに関し、外部委託がなされている場合、外部委託に係るリスクを検討し、必要なセキュリティ対策が講じられているか。
Ⅲ－３－６－２－３ 監督手法・対応	Ⅲ－３－６－２－３　監督手法・対応
（新設）	（１）犯罪発生時 偽造キャッシュカード及び盗難キャッシュカードによる不正払戻しを認識次第、速やかに「犯罪発生報告書」にて当局宛て報告を求めるものとする。 （２）問題認識時

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
被害が発生した場合は、必要に応じ、法第24 条に基づき報告を求める。その上で、犯罪防止策や被害発生後の対応について、必要な検討がなされず、被害が多発するなどの事態が生じた場合など、利用者保護の観点から問題があると認められる場合には、法第26 条に基づく業務改善命令等を行うものとする。	検査結果、犯罪発生報告書等により、銀行のＡＴＭシステムのセキュリティ対策及び犯罪対策に係る管理態勢に問題があると認められる場合には、必要に応じ、法第 24 条に基づき追加の報告を求める。その上で、犯罪防止策や被害発生後の対応について、必要な検討がなされず、あるいは被害が多発するなどの事態が生じた場合など、利用者保護の観点から問題があると認められる場合には、法第 26 条に基づき業務改善命令を発出する等の対応を行うものとする。
（注）ＡＴＭシステムに関し、外部委託がなされている場合において、そのセキュリティに関し、適切な業務運営が懸念される場合などには、必要に応じて、Ⅲ－３－３－４－３の対応を行うものとする。	（注）ＡＴＭシステムに関し、外部委託がなされている場合は、必要に応じて、Ⅲ－３－３－４－３の対応を行うものとする。
（参考）「偽造キャッシュカード問題に関するスタディグループ最終報告書」（平成17 年６月24 日：偽造キャッシュカード問題に関するスタディグループ） 「偽造・盗難キャッシュカードに関する預金者保護の申し合わせ」（平成17 年10 月６日：全国銀行協会）	（参考） ・「偽造キャッシュカード問題に関するスタディグループ最終報告書」（平成 17 年６月 24 日：偽造キャッシュカード問題に関するスタディグループ） ・「偽造・盗難キャッシュカードに関する預金者保護の申し合わせ」（平成 17 年 10 月６日：全国銀行協会） ・「金融機関の防犯基準」（警察庁） ・「全銀協ＩＣキャッシュカード標準仕様」（全国銀行協会）
Ⅲ－３－６－３　金融機関相互のシステム・ネットワークの利用 （略）	Ⅲ－３－６－３　金融機関相互のシステム・ネットワークの利用 （略）
Ⅲ－３－７　インターネットバンキング	Ⅲ－３－７　インターネットバンキング
Ⅲ－３－７－１　意義	Ⅲ－３－７－１　意義

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
情報通信技術の進展により、インターネットは、銀行にとっては低コストのサービス提供を可能とする一方、利用者にとっては利便性の高い取引ツールとなり得るものである。 したがって、銀行は、インターネットバンキングが非対面取引であることを踏まえた、内部管理態勢を確立することが重要である。	インターネットは、金融機関にとっては低コストのサービス提供を可能とするものであるとともに、利用者にとっては利便性の高い取引ツールとなり得るものである。一方、インターネットを通じた取引は、非対面で行われるため、異常な取引態様を確認できないことなどの特有のリスクを抱えている。 金融機関が顧客にサービスを提供するにあたっては、顧客の財産を安全に管理することが求められる。従って、金融機関においては、利用者利便を確保しつつ、利用者保護の徹底を図る観点から、インターネットバンキングに係るセキュリティ対策を十分に講じるとともに、顧客に対する情報提供、啓発及び知識の普及を図ることが重要である。
Ⅲ－３－７－２ 主な着眼点	Ⅲ－３－７－２　主な着眼点
（１）内部管理体制の整備	（１）内部管理態勢の整備
① 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の社内規則等を定めているか。 ② 利用者からの問合せ等のための窓口を設け、これをホームページ等で分かりやすく明示しているか。 ③ 通信技術の進展に伴い、取引の安全性を確保する観点から、不正防止策に係る技術的な問題について、適切に検討を行う体制が整備されているか。	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。 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

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
	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。
① 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係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。 ② 取引の安全性の確保等の観点から、適切な不正防止策を講じているか。 ③ 不正取引については、その実態の把握に努め、その防止策のあり方を検討し、必要な措置を講じているか。	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、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。 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。
	（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」（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）利用者保護の確保 ① 利用者に対し、暗証番号等は推測されやすい番号を避ける等の注意喚起を行っているか。 ② 利用者が取引内容を確認できる手段を講じているか。 ③ 不正取引については、利用者保護のあり方を検討し、必要な措置を講じているか。	（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

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
	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、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。
（４）その他 ①インターネットバンキングが非対面取引であることを踏まえた、本人確認等の顧客管理体制の整備が図られているか。 ② 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。 ③ 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）インターネットバンキングに係る外部委託に関する監督上の主な着眼点は、Ⅲ－３－３－４－２を準用することとする。	（４）その他 　インターネットバンキングが非対面取引であることを踏まえた、本人確認等の顧客管理態勢の整備が図られているか。 　インターネットバンキングに関し、外部委託がなされている場合、外部委託に係るリスクを検討し、必要なセキュリティ対策が講じられているか。
（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 平成14 年４月） 「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） ・「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

主要行等向けの総合的な監督指針　新旧対照表

（別紙２）

現　　行	改　正　案
	報システムセンター）
Ⅲ－３－７－３ 監督手法・対応	Ⅲ－３－７－３　監督手法・対応
（新設）	（１）犯罪発生時 インターネットバンキングによる不正取引を認識次第、速やかに「犯罪発生報告書」にて当局宛て報告を求めるものとする。
検査結果等により、銀行のインターネットバンキングに係る健全かつ適切な業務の運営に疑義が生じた場合には、必要に応じ、法第24 条に基づき報告を求め、重大な問題があると認められる場合には、法第26 条に基づき業務改善命令を発出する等の対応を行うものとする。	（２）問題認識時 検査結果、犯罪発生報告書等により、銀行のインターネットバンキングに係る健全かつ適切な業務の運営に疑義が生じた場合には、必要に応じ、法第 24 条に基づき追加の報告を求める。その上で、犯罪防止策や被害発生後の対応について、必要な検討がなされず、被害が多発するなどの事態が生じた場合など、利用者保護の観点から問題があると認められる場合には、法第 26 条に基づき業務改善命令を発出する等の対応を行うものとする。
（注）インターネットバンキングに係る外部委託について、外部委託先における適切な業務運営が懸念される場合などには、必要に応じて、Ⅲ－３－３－４－３の対応を行うものとする。	（注）インターネットバンキングに関し、外部委託がなされている場合は、必要に応じて、Ⅲ－３－３－４－３の対応を行うものとする。