事務ガイドライン（第三分冊：金融会社関係 5 前払式支払手段発行者関係）　新旧対照表

改正案	現行
Ⅱ　前払式支払手段発行者の監督上の評価項目 Ⅱ―２　利用者保護のための情報提供・相談機能等 Ⅱ－２－５　サーバ型前払式支払手段を悪用した架空請求等詐欺被害への対応 前払式支払手段には、販売店において匿名で誰でも簡単に購入して利用でき、他人に譲渡することもできるものがあり、特にサーバ型前払式支払手段については、証票等を提示又は交付しなくても、ID をインターネット上で入力して利用できるといった特性を有しているものもあり、インターネット等の通信手段を利用した非対面の取引（以下「インターネット取引」という。）の拡大に伴って決済手段として広く普及してきている。 このように利用者にとって利便性が高い決済手段として普及する一方で、その特性を悪用して、架空請求等でサーバ型前払式支払手段を購入させて ID を詐取するなどといった詐欺被害が発生している。 これらを踏まえ、架空請求等詐欺被害の発生が認められているサーバ型前払式支払手段発行者においては、被害発生状況のモニタリングや分析を通じて被害の防止及び被害回復に向けた取組みが求められている。 架空請求等詐欺被害への対応に関する監督に当たっては、例えば、以下の点に留意するものとする。 なお、字義どおりの対応がなされていない場合であっても、当該サーバ型前払式支払手段発行者の規模や特性、被害発生状況などからみて、被害の防止等の観点から、特段の問題がないと認められれば、不適切とするものではない。	Ⅱ　前払式支払手段発行者の監督上の評価項目 Ⅱ―２　利用者保護のための情報提供・相談機能等 Ⅱ－２－５ サーバ型前払式支払手段を悪用した架空請求等詐欺被害への対応 前払式支払手段には、販売店において匿名で誰でも簡単に購入して利用でき、他人に譲渡することもできるものがあり、特にサーバ型前払式支払手段については、証票等を提示又は交付しなくても、ID をインターネット上で入力して利用できるといった特性を有しているものもあり、インターネット取引の拡大に伴って決済手段として広く普及してきている。 このように利用者にとって利便性が高い決済手段として普及する一方で、その特性を悪用して、架空請求等でサーバ型前払式支払手段を購入させて ID を詐取するなどといった詐欺被害が発生している。 これらを踏まえ、架空請求等詐欺被害の発生が認められているサーバ型前払式支払手段発行者においては、被害発生状況のモニタリングや分析を通じて被害の防止及び被害回復に向けた取組みが求められている。 架空請求等詐欺被害への対応に関する監督に当たっては、例えば、以下の点に留意するものとする。 なお、字義どおりの対応がなされていない場合であっても、当該サーバ型前払式支払手段発行者の規模や特性、被害発生状況などからみて、被害の防止等の観点から、特段の問題がないと認められれば、不適切とするものではない。

改正案	現行
Ⅱ－２－５－１　（略）	Ⅱ－２－５－１　（略）
Ⅱ－２－５－２　（略）	Ⅱ－２－５－２　（略）
Ⅱ－２－６　（略）	Ⅱ－２－６　（略）
Ⅱ－２－７　（略）	Ⅱ－２－７　（略）
Ⅱ－２－８　（略）	Ⅱ－２－８　（略）
Ⅱ－２－８－１　主な着眼点	Ⅱ－２－８－１　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　リスク評価を踏まえ、連携先と協力し、利用者に係る情報を照合するほか、リスクに見合った適切かつ有効な不正防止策を講じているか。 例えば、口座振替サービスとの連携に際し、連携先の銀行等に登録された預貯金者の電話番号や住所宛てに前払式支払手段発行者における認証に必要な情報を通知する（電話番号宛てのSMS（ショートメッセージサービス）を含む）ことや、チャージ上限額を不正取引が抑止できると考えられる水準に設定するなど、適切かつ有効な不正防止策を講じているか。 （注）連携先との情報の照合に当たっては、公的個人認証を用いる場合を除き、利用者の氏名・生年月日に加え、住所や電話番号も対象項目とすることが望ましい。 また、口座振替サービスを提供している連携先の銀行等において、Ⅱ－３－１－２－２（２）に記載している認証方式が導入されていることを確認しているか。	③　リスク評価を踏まえ、連携先と協力し、利用者に係る情報を照合するほか、リスクに見合った適切かつ有効な不正防止策を講じているか。 例えば、口座振替サービスとの連携に際し、連携先の銀行等に登録された預貯金者の電話番号や住所宛てに前払式支払手段発行者における認証に必要な情報を通知する（電話番号宛てのSMS（ショートメッセージサービス）を含む）ことや、チャージ上限額を不正取引が抑止できると考えられる水準に設定するなど、適切かつ有効な不正防止策を講じているか。 （注）連携先との情報の照合に当たっては、公的個人認証を用いる場合を除き、利用者の氏名・生年月日に加え、住所や電話番号も対象項目とすることが望ましい。 また、口座振替サービスを提供している連携先の銀行等において、例えば、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やソフトウェアトークンによる可変式パスワードを用

改正案	現行
（注）前払式支払手段発行者における不正防止策は、連携先の銀行等における不正防止策の内容と重複しないものとする必要がある点に留意する。また、連携先の銀行等において、電話番号など認証に利用される情報の登録・変更に堅牢な認証方式が導入されている必要がある点に留意する。	<u>いる方法、公的個人認証等の電子証明書を用いる方法が導入されているなど、実効的な要素を組み合わせた多要素認証等の</u>認証方式が導入されていることを確認しているか。 （注）前払式支払手段発行者における不正防止策は、連携先の銀行等における不正防止策の内容と重複しないものとする必要がある点に留意する。また、連携先の銀行等において、電話番号など認証に利用される情報の登録・変更に堅牢な認証方式が導入されている必要がある点に留意する。
④～⑤　（略）	④～⑤　（略）
(3)～(5)	(3)～(5)
Ⅱ－２－８－２　（略）	Ⅱ－２－８－２　（略）
Ⅱ－２－９　（略）	Ⅱ－２－９　（略）
Ⅱ－３　事務運営	Ⅱ－３　事務運営
Ⅱ－３－１　システム<u>リスク</u>	Ⅱ－３－１　システム<u>管理</u>
<u>Ⅱ－３－１－１　システムリスク管理</u>	<u>（新設）</u>
<u>Ⅱ－３－１－１－１　意義</u>	<u>（新設）</u>
前払式支払手段の発行の業務を行うに当たっては、コンピュータシステムのダウンや誤作動等、システムの不備等により、又は、コンピュータが不正に使用されることにより利用者や前払式支払手段発行者が損失を被るリスク（以下「システムリスク」という。）が存在することを認識し、適切にシステムリスク管理を行う必要がある。	前払式支払手段の発行の業務を行うに当たっては、コンピュータシステムのダウンや誤作動等、システムの不備等により、又は、コンピュータが不正に使用されることにより利用者や前払式支払手段発行者が損失を被るリスク（以下「システムリスク」という。）が存在することを認識し、適切にシステムリスク管理を行う必要がある。
特に、IC カードを用いた前払式支払手段やサーバ型前払式支払手段については、発行者が使用するシステムに障害が発生した場合には、発行	特に、IC カードを用いた前払式支払手段やサーバ型前払式支払手段については、発行者が使用するシステムに障害が発生した場合には、発行

改正案	現行
額、回収額、未使用残高の把握ができなくなるおそれや、前払式支払手段の発行業務が継続不可能となるなど利用者に多大な損害を及ぼすおそれがあることから、特にシステムリスク管理を適切に行う必要がある。 　また、IC カードを用いた前払式支払手段やサーバ型前払式支払手段発行者の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や当該前払式支払手段発行者のビジネスモデルを左右する重要課題となっており、当該前払式支払手段発行者において経営戦略と IT 戦略を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、当該前払式支払手段発行者の規模や特性に応じて、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」を適切に機能させることが極めて重要となっている。 　以下の着眼点は IC カードを用いた前払式支払手段やサーバ型前払式支払手段の発行者を想定しているが、字義どおりの対応がなされていない場合にあっても、当該前払式支払手段発行者の規模、前払式支払手段の発行の業務におけるコンピュータシステムの占める役割などの特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。 　なお、磁気型・紙型の前払式支払手段を発行する場合にあっても、システム障害により前払式支払手段の発行の業務に支障を来たすおそれがある場合には、必要に応じたシステム管理に係る態勢整備を行う必要がある。 （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・プラクティスの整理第２版（令和５年６月）	額、回収額、未使用残高の把握ができなくなるおそれや、前払式支払手段の発行業務が継続不可能となるなど利用者に多大な損害を及ぼすおそれがあることから、特にシステムリスク管理を適切に行う必要がある。 　また、IC カードを用いた前払式支払手段やサーバ型前払式支払手段発行者の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や当該前払式支払手段発行者のビジネスモデルを左右する重要課題となっており、当該前払式支払手段発行者において経営戦略と IT 戦略を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、当該前払式支払手段発行者の規模や特性に応じて、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」を適切に機能させることが極めて重要となっている。 　以下の着眼点は IC カードを用いた前払式支払手段やサーバ型前払式支払手段の発行者を想定しているが、字義どおりの対応がなされていない場合にあっても、当該前払式支払手段発行者の規模、前払式支払手段の発行の業務におけるコンピュータシステムの占める役割などの特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。 　なお、磁気型・紙型の前払式支払手段を発行する場合にあっても、システム障害により前払式支払手段の発行の業務に支障を来たすおそれがある場合には、必要に応じたシステム管理に係る態勢整備を行う必要がある。 （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・プラクティスの整理第２版（令和５年６月）

改正案	現行
Ⅱ－３－１－１－２　主な着眼点 (1)～(4)　（略） (5)　サイバーセキュリティ管理 ①　（略） ②　インターネット取引を行う場合には、Ⅱ－３－１－２の規定に基づく適切な取扱いを確保するための態勢を整備しているか。	Ⅱ－３－１－１　主な着眼点 (1)～(4)　（略） (5)　サイバーセキュリティ管理 ①　（略） 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、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。 　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。 ・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 ・取引に利用しているパソコン・スマートデバイス等とは別の機器を用いるなど、複数経路による取引認証 ・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。） ・特定の端末のみを利用可能とする端末認証機能　等 （注）電話番号、メールアドレス、パスワードなど認証に利用される情報の登録・変更に堅牢な認証方式が導入されている必要がある点に留意する。 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には、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。

改正案	現行
	・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、連絡可能な利用者に対して速やか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
(6)　システム企画・開発・運用管理 ①～③　（略） ④　インターネット取引を行う場合には、システム設計／開発段階に関わる規程に、以下のようなセキュリティに係る事項を含めているか。 ・具体的なセキュリティ要件を明確化すること ・セキュアコーディングの実施など脆弱なポイントが生じないように対策を行うこと ・他社のシステムと連携する場合には、連携する部分を含めサービス全体を踏まえたセキュリティ設計を行うこと 等 ⑤～⑦　（略） (7)～(10)　（略）	(6)　システム企画・開発・運用管理 ①～③　（略） ④　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、システム設計／開発段階に関わる規程に、以下のようなセキュリティに係る事項を含めているか。 ・具体的なセキュリティ要件を明確化すること ・セキュアコーディングの実施など脆弱なポイントが生じないように対策を行うこと ・他社のシステムと連携する場合には、連携する部分を含めサービス全体を踏まえたセキュリティ設計を行うこと 等 ⑤～⑦　（略） (7) ～(10)　（略）
Ⅱ－３－１－１－３　監督手法・対応 (1)～(4)　（略）	Ⅱ－３－１－２　監督手法・対応 (1)～(4)　（略）

改正案	現行
Ⅱ－３－１－２　インターネット取引 Ⅱ－３－１－２－１　意義 　インターネット取引は、前払式支払手段発行者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、インターネット取引は、非対面で行われるため、異常な取引態様の確認が困難であることなどの特有のリスクを抱えている。 　前払式支払手段発行者が顧客にサービスを提供するに当たっては、顧客の財産を安全に管理することが求められる。従って、前払式支払手段発行者においては、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、インターネット取引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。 　以下の着眼点はICカードを用いた前払式支払手段やサーバ型前払式支払手段の発行者を想定しているが、字義どおりの対応がなされていない場合にあっても、当該前払式支払手段発行者の規模、前払式支払手段の発行の業務におけるコンピュータシステムの占める役割などの特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。 Ⅱ－３－１－２－２　主な着眼点 (1)　内部管理態勢の整備	（新設）

改正案	現行
インターネット等の不正アクセス・不正取引等の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、インターネット取引の健全かつ適切な業務の運営を確保するため、前払式支払手段発行者内の各部門が的確な状況認識を共有し、前払式支払手段発行者全体として取り組む態勢が整備されているか。 その際、ＪＰＣＥＲＴ／ＣＣ等の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。 (2)　セキュリティの確保 セキュリティ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。	

改正案	現行
インターネット取引に係る情報セキュリティ全般に関する方針を作成し、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、当該方針等に沿って個人・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」等も踏まえ、提供するサービスの内容に応じた適切な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。 また、フィッシング詐欺対策については、メールやSMS（ショートメッセージサービス）内にパスワード入力を促すページのURLやログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く。）、利用者に対して正規のウェブサイトのブックマークや正規のアプリからログインすることを促す、送信ドメイン認証技術の計画的な導入、フィッシングサイトの閉鎖依頼等、提供するサービスの内容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、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。 インターネット取引を行う場合には、提供するサービスの内容に応じて、以下の不正防止策を講じているか。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、認証方式等の見直しを行っているか。	

改正案	現行
・　ログイン、譲渡など、重要な操作時におけるフィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定） （注１）フィッシングに耐性のある多要素認証の実装及び必須化以降、顧客が設定に必要な機器（スマートフォン等）を所有していない等の理由でやむを得ずかかる多要素認証の設定を解除する場合には、代替的な多要素認証を提供するとともに、解除率の状況をフォローした上で、認証技術や規格の発展も勘案しながら、解除率が低くなるよう多要素の認証の方法の見直しを検討・実施することとする。 （注２）フィッシングに耐性のある多要素認証を実装及び必須化するまでの間は、代替的な多要素認証を提供するとともに、当該実装及び必須化に向けた具体的なスケジュールについて顧客に周知する必要がある。また、それまでの期間においても、振る舞い検知やログイン通知等の検知機能を強化する必要がある。 ・　顧客が身に覚えのない第三者による不正なログイン・取引・出金・出金先口座変更を早期に検知するため、電子メール等により、顧客に通知を送信する機能の提供 ・　認証に連続して失敗した場合、ログインを停止するアカウント・ロックの自動発動機能の実装及び必須化 ・　顧客のログイン時の挙動の分析による不正アクセスの検知（ログイン時の振る舞い検知）及び事後検証に資するログイン・取引時の情報の保存の実施	

改正案	現行
・　不正アクセスの評価に応じて追加の本人認証を実施するほか、当該不正が疑われるアクセスの適時遮断、不正アクセス元からのアクセスのブロック等の対応の実施 さらに、例えば、以下のような不正防止策を講じているか。 ・　取引時や他の銀行口座との連携サービス提供時におけるフィッシングに耐性のある多要素認証の提供 ・　取引金額の上限や購入可能商品の範囲を顧客が設定できる機能の提供 ・　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と仕組みの整備 （参考） ・　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） ・　フィッシング対策ガイドライン（フィッシング対策協議会） (3)　顧客対応 インターネット上での ID・パスワード等の個人情報の詐取の危険性、類推されやすいパスワードの使用の危険性（認証方式においてパスワードを利用している場合に限る。）、被害拡大の可能性等、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。	

改正案	現行
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。 不正取引による被害があった場合には、被害状況を十分に精査し、顧客の態様やその状況等を加味したうえで、顧客の被害補償を含め、被害回復に向けて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 インターネット取引が非対面取引であることを踏まえた、取引時確認等の顧客管理態勢の整備が図られているか。 インターネット取引に関し、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。 （中略）	（中略）

改正案		現行	
適否	**審　査　内　容**	**適否**	**審　査　内　容**
システムリスク（Ⅱ－３－１）		*システム管理（Ⅱ－３－１）*	
（略）	（略）	（略）	（略）
		□	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、例えば、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や複数経路による取引認証など、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。
（削除）	（削除）		
		□	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、業務に応じた不正防止策を講じているか。また、不正なログイン・異常な取引等を検知し、速やかな利用者への連絡や不正が確認された ID の停止を行う体制を整備しているか。
（略）	（略）	（略）	（略）
□	インターネット等の不正アクセス・不正取引等の犯罪行為に対する対策等について、利用時における留意事項等を顧客に説明する態勢を整備しているか。		
□	インターネット取引の健全かつ適切な業務の運営を確保するため、前払式支払手段発行者内の各部門		

改正案		現行	
	が的確な状況認識を共有し、前払式支払手段発行者全体として取り組む態勢を整備しているか。		
□	セキュリティ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。		
□	インターネット取引に係る情報セキュリティ全般に関する方針を作成し、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。		
□	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」等も踏まえ、犯罪手口の高度化・巧妙化等を考慮し、提供するサービスの内容に応じた適切なセキュリティ対策を講じているか。	（新設）	（新設）
□	インターネット取引を行う場合には、提供するサービスの内容に応じて、ログイン、譲渡など、重要な操作時におけるフィッシングに耐性のある多要素認証の実装及び必須化等の不正防止策を講じているか。		
□	インターネット取引を行う場合には、提供するサービスの内容に応じて、不正なログイン・異常な取引		

改正案		現行	
	等を検知し、速やかに利用者に連絡する体制と仕組みの整備等の不正防止策を講じているか。		
□	インターネット上での ID・パスワード等の個人情報の詐取の危険性等、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を整備しているか。		
□	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を整備しているか。	（新設）	（新設）
□	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を整備しているか。		
□	不正取引による被害があった場合には、被害状況を十分に精査し、顧客の態様やその状況等を加味したうえで、顧客の被害補償を含め、被害回復に向けて真摯な顧客対応を行う態勢を整備しているか。		
□	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しているか。		

改正案		現行	
□ □	インターネット取引が非対面取引であることを踏まえた、取引時確認等の顧客管理態勢の整備を図っているか。 インターネット取引に関し、外部委託を行っている場合、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を講じているか。		
（略）	（略）	（略）	（略）