コメントの概要及びコメントに対する金融庁の考え方

凡 例

「金融庁の考え方」においては、以下の略称を用いています。

正式名称	略称
金融商品取引業者等向けの総合的な監督指針	監督指針

No.	コメントの概要	金融庁の考え方
Ⅲ－２－８－１（１）主な着眼点		
1	「インターネット取引」が「インターネット等の通信手段を利用した非対面の取引」と定義されています。ここでいう「等」の射程の範囲を具体的にご教示いただきたい。 例えば、（事業者と顧客間、又は、事業者と関連会社や外部ベンダー間の）専用回線を利用しての取引も含まれるという理解でよろしいでしょうか。 また、「非対面の取引」とは、取引相手の属性を問わないもの、すなわち、個人顧客との取引のみならず法人顧客との取引と理解しておりますが、かかる理解でよろしいでしょうか。	インターネット等の通信手段を利用した非対面による顧客口座等における有価証券の売買等であり、ＦＸ等のデリバティブ取引も含みます。 また、取引相手の属性は限定しておりません。
Ⅲ－２－８－２　インターネット取引		
2	表題が「インターネット取引」となっているので、出金や売買や出金先口座変更などは行わず、単に口座情報を閲覧するだけであれば、フィッシングに耐性のある多要素認証の実装は義務化されないということで良いのか。	単に、出金や売買や出金先口座変更の操作メニューを顧客が利用していないということではなく、このような操作そのものを行うことができない仕様ということであれば、一概に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を求めるものではありませんが、閲覧のために用いられる認証情報が不正アクセスにより流出して不正取引や不正出金に用いられること等のないよう適切に対応する必要があると考えます。 なお、フィッシングに耐性のある多要素認証の設定の解除が認められるのは、顧客が設定に必要な機器を所有していない等のやむを得ない理由がある場合のほか、システム上行うことができる操作が情報の閲覧のみであり取引を一切行うことができない場合等に限られると考えます。

Ⅲ－２－８－２－１　意義		
３	当社は有価証券取引だけではなく、FX 取引なども取り扱っているが、それぞれの取引において「異常な取引態様」とは具体的にはどのようなものが該当すると考えているのか、例示があれば示して欲しい。 「異常な取引態様」の具体例がない場合には、これらを検知する体制を整備することが難しいと考える。 また、「異常な取引態様を確認できないことなど・・・」と記載があるとおり、「異常な取引態様を確認できない」としている一方、３－２－８－２－２（２）セキュリティの確保において、「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をする」ことを求めているため、記載内容に矛盾が生じていると考える。 「異常な取引態様は確認が困難であることなど・・・」という記載に変えたほうがよいのではないか。	前段については、顧客層、取扱商品、取扱額等は各社で異なることから「異常な取引態様」を一概にお示しすることは困難ですが、各社において、顧客や取扱商品、業務の特性等に応じてリスク評価を行った上で、適切な態勢整備を講じることが重要であると考えます。 後段については、御指摘のとおり修正いたします。
４	「意義」に「一方、インターネット取引は、非対面で行われるため、異常な取引態様を確認できないことなどの特有のリスクを抱えている。」との記載があるが、この前提は誤っているため、修正すべき。 インターネット取引のほうが対面取引よりも異常な取引態様の阻止または検知は容易であり、異常な取引態様を阻止または検知できていないのは単に技術的防護策が講じられていないか、不適切というだけ。	貴重な御意見として承ります。
５	金融商品取引業者は顧客に対しサービスを提供するにあたっては善良な管理者の注意をもって、顧客の財産を安全に管理することが求められる。 ※「善良な管理者の注意をもって」を追記。金融商品取引法第 43 条「有価証券管理業務についての特則」に規定される重い注意義務の明記をお願い致します。	貴重な御意見として承ります。
６	「顧客の財産を安全に管理することが求められる。」は、これまで継続して行ってきていると思われる。今回の改正では、「従って、」以降、「金融商品取引業者においては、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」とあるが、金商業者が顧客に知識の普及を図るのは当然のことであるもの	前段について、御質問の趣旨が必ずしも明らかではありませんが、各社において、提供する商品・サービス・取引方法や顧客層に応じた情報提供、啓発及び知識の普及等を図ることは困難なことではないと考えます。 後段については、貴重な御意見として承ります。

	の、金融庁、内閣府をはじめとする政府全体で取り組むべき問題で、主体となるのは金融庁等であり、金商業者にそれを行わせるのは困難と思料するが如何か。 　また、「顧客にサービスを提供するに当たっては、」とあるが、サービスを提供する際の顧客の知識レベルは様々であることから、適合性の原則にも影響を与えるものであるため、金融商品取引法第 40 条にある「顧客の知識」に「インターネット取引に係るセキュリティ知識」を加えてはどうか。	
Ⅲ－２－８－２－２（１）　内部管理態勢の整備		
7	システムセキュリティを経営上の最重要課題と位置づけ、万一の不備による被害発生時の緊急の対応、情報開示義務、連絡・相談義務、救済検討義務を監督指針に明記していただきたい。	現行の監督指針においても、サイバーセキュリティ事案の未然防止について経営上の重大な課題として認識し態勢を整備することを求めています。 　また、本改正により、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について、最優先の経営課題の一つとして位置付け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ことを求めています。 　また、サービス利用時における顧客への注意喚起や被害発生時の真摯な顧客対応を行う態勢整備についても求めています。
8	「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」とあるが、態勢整備されている場合、幾度となく説明しても理解できない顧客が存在した場合は、理解できないことをもって取引をさせないという判断も有り得るのか。	顧客との取引を継続するか否かの判断は各社において適切に行われるべきものと考えますが、顧客にインターネット取引サービスを提供する事業者においては、サービスの利用に必要な IT リテラシーについて、顧客の意識向上に努めていくことが重要と考えます。
9	インシデント発生時及びインシデント認識時における即応態勢の整備ができているかを着眼点に明確に位置付けるべきである。 （理由） 　インシデントの予兆をいかにはやく認識して、インシデントが発生した場合には、「今ここにある危機」のために、外部事業者との連携を含めてあらゆる手段を講ずる態勢が取れているかをきちんと行政として把握しておかないと、投資家・消費者保護が徹底されないことになる。	現行の監督指針Ⅲ－２－８（１）及びⅢ－２－９においても、サイバーセキュリティ管理態勢や危機管理態勢の整備を図ることを求めています。

Ⅲ－２－８－２－２（２）　セキュリティの確保		
10	「自らの顧客や業務の特性に応じた対策を講じているか。」については取扱う商品性の特性（流動性や換価性など）も要素の一つして考慮することも可能と理解していますので、その点が判るようご配慮ください。	業務の特性には取扱う商品の特性も含まれますので、原案のとおりとさせていただきます。
11	「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。」とありますが、ここに記載される「評価・対策」は、事業者が様々なリスクの存在を総合的に勘案する趣旨のものであると認識しております。 一方、「個別の対策を場当たり的に講じるのではなく・・・」との記載がございますが、業者が評価→対策したものが、重要な対策１つだけに対応したものであった場合でも、「個別に場当たり的に対応した」ことになるのでしょうか。文脈より、そういった趣旨の内容ではないものと承知しておりますが、「個別の」という文言はなくてもよいものと考えます。	各社において仮にその時点で有効と考える対策が１つだった場合であっても、その対策で十分かどうか効果を検証し、また、その時々のセキュリティ技術水準や犯罪手法等に応じて、リスクを評価し、効果的な対策を行うことが望ましいと考えます。よって、原案のとおりとさせていただきます。
12	「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」はプリンシプルベースで策定された認識であり、監督指針上の義務をサイバーセキュリティガイドライン、不正アクセス等防止ガイドラインを参考にしながら履践することが求められているが、それらに基づいた内部管理態勢の整備やシステム導入に関する準備期間などについて、どの程度考慮をいただけるのか。 上記のガイドラインに記載の事項についての可能な限り速やかに履践するものの、監督指針の改正直後に未対応（履践できていない事項）を根拠として、直ちに業務改善命令が発出されるものではなく、各社の状況を踏まえた判断が行われるという理解でよいか。	各社の内部管理態勢の整備状況やシステム導入計画の妥当性については、顧客や業務の特性、提供するサービスの内容のほか、不正取引事案の発生状況等を総合的に勘案しながら、個別に判断します。
13	現状、一部の金融機関では顧客向けサービスの一環として、営業社員の携帯電話から URL を発行し、所定のフリーダイヤルの番号から顧客の登録メールアドレスへ SMS が送信されます。顧客に届く SMS には URL が記載されており、クリックしたのち専用のサイトに遷移し、生年月日を入力すると希望する手続きを行うことができる仕組みになっていますが、このようなシステムも規制の対象となるのでしょうか。	御理解のとおりです。 当該規定の趣旨が、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ことで、顧客がフィッシング詐欺の被害に遭うことを防ぐことであることを踏まえると、そのような顧客による手続きが可能な画面に遷移するページの URL を記載すべきではないと考えます。

	※この文面を盗用された場合や、文面のリンク先に偽の顧客専用ページ等を充てがわれた場合などは、ログイン ID やパスワードを入力してしまう恐れがあります。SMS にリンク先を貼るのではなく、信販会社が取り入れているような「Safekey 認証コード」（信販会社から顧客に送付される SMS に記載される数字の羅列）を入力するなどの、より強固な取り組み例を例示する方が良いのではないでしょうか。	
14	「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」とあるが、これは、インターネット取引サービス外であり、なおかつ顧客の口座・資産に影響を及ぼさないものは含まれないと理解してよいか。 例えば、以下のようなＵＲＬの記載は問題ないと考えてよいか。 ・WEB セミナーの申込等のために、顧客に個人情報の入力を促すページの URL が記載されたメールを送付すること ・リサーチレポートの閲覧や WEB セミナー視聴用のシステムにログインするために、顧客に ID 及びパスワード（インターネット取引サービスのログイン時に使用するものとは別のもの）の入力を促すページの URL が記載されたメールを送付すること ・キャンペーンの申込等のために、顧客にログイン ID の入力を促すページの URL が記載されたメールを送付すること（パスワード入力を伴わない場合） ・会社ウェブサイト等案内のために、ＩＤやパスワードの入力を促さない、直接アクセスできるページの URL が記載されたメールを送付すること	御理解のとおりです。
15	ログイン画面へ直接遷移をさせない URL の記載（例えば、ログインボタンを有するビジターページの URL 記載など）は問題ないとの理解で良いか。	原則として、メール配信の解除手続きなど、法令に基づき電子メールの本文に記載が義務付けられている場合などを除きメールや 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すべきではないと考えます。 また、利用者に対して、各社のウェブサイトにアクセスする際は、事前に正規のウェブサイトの URL をブックマーク登録しておきブックマークから

		アクセスしたり、正規のアプリからアクセスしたりするよう周知することが望ましいと考えます。 以上を踏まえると、ログインすることが可能な画面へ遷移するページのURLについても記載すべきではないと考えます。
16	営業やアンケートなど日常業務に必要なリンクがなくなった場合、投資家からの要望や質問を受け付けられなくなるなど、顧客本位の観点からも大きな影響が懸念されます。 不正アクセス対策は必要ですが、リンクを掲載しつつ「※フィッシング等にご懸念がある場合は、ログイン後の○○＞○○からご確認ください」と併記して注意喚起するなどの代替的措置は可能でしょうか。 あるいは、フィッシング耐性のある認証方式をデフォルトにすることで、代替的措置とすることは可能でしょうか。	今回、インターネット取引における不正取引の急増とともに、証券会社を騙る偽サイト（フィッシングサイト）の検知も急増していることを踏まえると、フィッシング対策は重要であり、原則として、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すべきではないと考えます。
17	SMSへのURL記載を禁止するのではなく、URL記載方法の指針を提示することを提案いたします。 【修正案】下記に修正。 ・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する場合は、アクセス先が識別可能なものとすること。例として、ドメイン名から利用企業を識別できるなどがある。また、短縮URLを利用する場合は、アクセスが安全なものであることを担保すること。 ・共通ショートコードの利用及び通信キャリアが公開する共通ショートコード紹介Webサイトに当該ショートコードを公開することを提案いたします。共通ショートコードは、通信キャリアが利用企業を審査しており、審査済みの専用番号で表示されるため、安心してご利用いただけます。また、通信キャリアが公開した共通ショートコード紹介Webサイトに当該共通ショートコードを公表することにより、受信者は安全な送信元の判別が可能となります。 【修正案】下記を追加。	今回、インターネット取引における不正取引の急増とともに、証券会社を騙る偽サイト（フィッシングサイト）の検知も急増していることを踏まえると、顧客側に送信元の真正性の判断を委ねるよりも、原則として、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すべきではないと考えます。

	・共通ショートコードを利用し、通信キャリアが公開したWebサイト（https://japansms.com/）に当該共通ショートコードを必ず公開し、Web サイト上又はアプリケーション上等にも公開すること。 ・ベストプラクティスとして、RCS を利用して送信元が安全であると判別できる状態とすることを提案いたします。RCS を利用することで、メッセージ画面に表示される企業ロゴや認証済み表記により送信元が安全であると受信者が判別可能となります。 【修正案】下記を追加。 ・ベストプラクティスとして、RCS（リッチコミュニケーションサービス）を利用し、メッセージ画面の認証済み表記により送信元が安全であると判別できる状態とすること。 ・メール/SMS への URL 記載を禁止する場合、代替手段を用意すべきと考えます。ベストプラクティスとして、RCS のボタンを利用することを提案いたします。本文に直接 URL を記載するのではなく、RCS メッセージ内のボタンからアクセスできる状態とし、受信者に対し、RCS のボタンから Web サイトにアクセスするよう周知を行うことで、不審な URL のクリックを抑止することが可能となります。 【修正案】下記を追加。 ・ベストプラクティスとして、パスワード入力を促すページの URL やログインリンクは、本文に直接記載するのではなく、メッセージ内のボタンからアクセスできる状態とすること。顧客に対し、RCS のボタンから Web サイトにアクセスするよう周知を行うこと。	
18	改定案では「メールや SMS 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」と記載されていますが、これは利用者保護の観点から重要である一方、実務上は正当な理由でリンクを送付するケース（パスワードリセットリンク、マジックリンク、WebOTP 対応 SMS など）も存在します。特に	フィッシングメールの内容はその時々で変化することが考えられることから、原則としてメールや 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すべきではないと考えます。

	WebOTP はブラウザ連携で正しいサイトに人の手を介さずに自動入力されるため、フィッシング耐性が高い技術です。 一方で、攻撃者は依然として利便性の高いリンク入りメッセージを送り続けることが予想されるため、一律禁止ではなく「原則禁止・適切な代替策がない場合に限定許容」とし、位置づけも「セキュリティ確保のための補足的措置」として後段に移す方が、利用者利便とセキュリティのバランスが取れると考えます。	なお、原案において、例外として「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」を提示していますので、原案のとおりとさせていただきます。
19	「法令に基づく義務を履行するために必要な場合」には、契約締結前書面及び目論見書等、金融商品取引法上の交付書面記載事項の電磁的提供を行うために、金融商品取引業等に関する内閣府令第 56 条第１項第１号ニの方法として、当該書面記載事項を掲載した自社ウェブサイトへのリンク（ＵＲＬ）等が記載されたメール等を当該顧客宛送信することも含まれるという認識でよいか。	原則として、メール配信の解除手続きなど、法令に基づきメールの本文に記載が義務付けられている場合などを除き、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すべきではないと考えます。 このため、法定書面の電磁的提供の方法としては、書面の閲覧のためにログインが必要な場合には、ログインを促すようなリンクをメッセージに記載する方法ではなく、メッセージ内本文にウェブサイト内の掲載場所を記載するなどの方法で案内することが適切と考えます。なお、ログインを伴わずに閲覧できる場合であっても、同じページ内にログインボタンが表示されるような状態は適切ではないと考えます。
20	メール等により広告を行う場合、当該メール等に自社ウェブサイトへのリンク（ＵＲＬ）等を記載し、顧客から見て一体性が認められるリンク先のページに当該金融商品の広告にあたっての法定必要表示事項が表示されていれば、メール等による広告は、広告等規制等に沿った対応であると理解している。 こうした広告等規制等に沿った取扱いについては、「法令に基づく義務を履行するために必要な場合」に含まれるという認識でよいか。	前段については御理解のとおりです。 後段については、原則として、メール配信の解除手続きなど、法令に基づきメールの本文に記載が義務付けられている場合などを除き、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すべきではないと考えます。 このため、広告に当たっての必要事項の表示については、メッセージ内本文に必要事項を記載する、ログインを伴わないページへのリンクをメッセージ内に記載するなどの方法で案内することが適切と考えます。なお、ログインを伴わずに閲覧できる場合であっても、同じページ内にログインボタンが表示されるような状態は適切ではないと考えます。

21	法令に基づく義務を履行するために必要な場合、その他の代替的手段を採り得ない場合とは、具体的にどの程度のレベルのものが求められることになるのか。	御質問の趣旨が必ずしも明らかではありませんが、メール配信の解除手続きなど、法令に基づきメールの本文に記載が義務付けられている場合などを想定しています。
22	「(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)」を削除すべき。 理由: 厳格にログインリンク付きメールを禁止すべきである。	メール配信の解除手続きなど、法令に基づきメールの本文に記載が義務付けられている場合もあるため、原案のとおりとさせていただきます。
23	フィッシング詐欺対策として、金融商品取引業者から送付されるメールマガジンの登録はオプトインにすべきである。 金融商品取引業者の中には、口座開設時等に「メールマガジンの送信を希望する」をデフォルト設定にしている者がある。これに起因して、投資家は自らの意志に反してメールマガジンを受け取ることとなる。結果として 1.セキュリティに関する重要通知の見落とし、2.金融商品取引業者を騙るフィッシングメール（投資家が契約する金融商品取引業者名を騙ったりするため）に騙されてしまう要因となる。 インターネット取引の安全性を担保するためにも、投資家のオプトアウト見落としにつけ込んで商業メールを一方的に送る仕様は禁じるべきである。	本改正により、フィッシングメール対策として、「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」を除き、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等の対策を求めております。
24	DMARC ポリシーは「reject」に設定することが必須となるのでしょうか。 また、「quarantine」に設定した場合、法令遵守上の懸念が生じるという意味でしょうか。 DMARC の進捗状況は公表する必要がありますでしょうか。	DMARC の導入に当たっては、受信側に対してなりすましメールの受信拒否を要求するポリシー(reject)での運用を行うことが望ましいと考えますが、DMARC ポリシーの切替えや進捗状況の公表に関しては、各社が適切に判断しながら行うべきものと考えます。
25	送信ドメイン認証「DMARC」のポリシーは「拒否」が必須となっていますが、「拒否」必須化となれば DKIM の公開鍵暗号は非常に長い鍵長の RSA 暗号が有力となります。DKIM で RSA 暗号以外の公開鍵暗号を設定すると、メールを受ける側も、その新しい公開鍵暗号を購入する必要があるため。現在は、いろいろ新しい公開鍵暗号を試している段階なので、とても全員が全部を購入しきれません。オープンソースだから問題ないという意見もありますが。 フィッシング対策にパスキーは高い効果がありますが OS を起動不能にする攻撃に非常に弱い。OS 起動不能は CPU のバグや OS のアップデートミスで一斉	貴重な御意見として承ります。

	に発生する場合もあり警戒すべきだと思われます。 一般人がパスキーで安全に運用することは難しいため、パスキーではオンライントレードの市場が無くなる可能性もあります。そこで各社専用の認証ハードを必須とすべきです。運用が簡単でしかも安全です。 認証専用ハードの必須化の指針を出して、メーカーが安心してハードを開発できるようにする政策を考えていただければと思います。そして次期マイナンバーカードや、DKIM アクセラレータの開発コスト低減を考えた総合的な政策となるように。認証ハードの半導体製造メーカーに株価下落のタイミングで認証専用ハードが起動しないなどの問題が起きないように抑える必要があります。 １台のハードで複数社に対応する認証ハードより、各社専用の認証ハードになれば、半導体チップの数が出るので製造コストが下がるように思います。また運用が簡単であるメリットも大きいと思われます。電卓型アイドル認証端末は電池不要のため製造コストが安く、対応年数も 10 年以上にできる可能性があり、トータルコストでは安くなります。 また７セグ文字「錦」の発明により、液晶ディスプレイを安価な７セグ液晶にできるだけでなく、液晶のドライバチップの削減効果もあります。基板の部品点数が少なくなる効果もあるので、製造コストが下がると思います。 認証ハードの音声 I/F はオプションです。実際のハードでは無くてもフィッシング耐性はあります。ただし SSL サーバ証明書をコピーされた偽サイトには効果がありません。これは音声 I/F オプションの実装で対策されます。	
26	「利用者がアクセスしているサイトが真正であることの証明確認措置」も重要ですが、人間の視認に依存する手段はフィッシング耐性が限定的です。 これも付加的対策として後段に記載し、主たる防御策は自動化・暗号化ベースのフィッシング耐性認証技術に置く方が望ましいと考えます。	「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」の具体的な方法が明らかとなるよう、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記載に修正いたします。 後段については、貴重な御意見として承ります。
27	かつて利用されていた「EV 証明書」の無効性や弊害が指摘されている中で、「真正なウェブサイトを証明する方法」で想定される方法を具体的に例示いただきたい。	御意見を踏まえ、「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」を削除し、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記載に修正いたします。
28	当社は直販をおこなっている投資信託委託業者で、ログイン時の多要素認証については、顧客が任意で選択できる仕様で導入済みである。投信直販については、今般問題となっているような口座の乗っ取り事例は該当せず同様のリスクが想定しにくい中、過度の多要素認証の導入は、顧客利便性を損なう可能性がある。 上記に加え、出金先の変更に際しては本人確認書類の提出を求めており、また出金は原則として同一名義の口座に限定していることから、不正リスクは極めて低いと考えられる。 よって一律の必須化については、業態等リスクベースに応じてなされるべきものと思料し、投資信託委託業者による投信直販における多要素認証に係る当社の上記の対応は合理的と考えられる。	今般の事案に限らず、インターネット取引においては、不正アクセスにより、真正な顧客ではない第三者等による買付けや売却といった出金時以外の場面においても顧客被害が発生する可能性があることから、本改正において、証券会社以外の金融商品取引業者等も含めて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導入を求めるものです。そのため、原案のとおりとさせていただきます。
29	第二種金融商品取引業者がインターネットを利用して、第二項有価証券の販売・勧誘を行う場合、契約の申込み・締結をインターネットで行わないもの（＝勧誘行為のみをインターネットで行うもの）、金銭の預託を受けない（＝出資者とファンドの業者が金銭を直接やり取りする）ものなどが含まれることや、第二項有価証券では中途換金の禁止や譲渡制限が付されることが多いなど、インターネットで行う業務内容や商品性によって、不正アクセス・不正取引の影響には差異が生じるものと考えられます。 監督指針改正案 3-2-8-2-2(2)における「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。」との表現は、インターネット取引を行う金融商品取引業者等に対して、同改正案で示された「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」以降の不正防止策を一律に求めるものではなく、インターネットで行う業務内容や商品性に応じて、必要・適切な不正防止策を講じることを求める趣旨であるとの理解でよろしいでしょうか。	御理解のとおりです。

30	ソーシャルレンディングでもフィッシングに耐性のある多要素認証の実装が義務化されるのか、それともサービス内容が違うので、各社で判断して良いのか。	今般の事案に限らず、インターネット取引においては、不正アクセスにより、真正な顧客ではない第三者等による操作により顧客被害が発生する可能性があることから、本改正において、証券会社以外の金融商品取引業者等も含めて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導入を求めています。
31	「フィッシングに耐性のある」を「リアルタイムフィッシングに耐性のある」に修正すべき。 理由: 一般的に多要素認証はフィッシング対策技術である。しかしリアルタイムフィッシングには破られており、実被害が多発しているのでこれを防御する趣旨を明示すべき。なお、AitM まで含めると(中間者攻撃はリアルタイムフィッシングと AitM に大別できる)過剰対策となる。利便性やコストを下げるため、現実的にはリアルタイムフィッシングに絞るべき。証券業界における大規模攻撃はリアルタイムフィッシングによるものであり、AitM は確認されていない。	フィッシングには、リアルタイムフィッシングも含まれますので、原案のとおりとさせていただきます。
32	金融庁が求めるべき多要素認証の基準の明確な定義付けを行うべき。	本改正において各社に求める多要素認証の水準は「フィッシングに耐性のある多要素認証」になるため、原案のとおりとさせていただきます。
33	用語の見直し:「多要素認証」から「高度認証」ないし「安全な顧客認証(Secure Customer Authentication)」へ 「フィッシング耐性のある」と各所で補っているので大丈夫ではあろうとは思いますが、一般に「多要素認証」という語は広義すぎ、質の低い多要素認証が機械的に採用される恐れがあります。 本案で本当に強調すべきは「フィッシング耐性」など諸種の脅威に対する耐性です。用語の置き換えや補足により、意図が明確になり、実務面での質的向上が見込まれます。	
34	現在多くの被害が発生している経路は、SMS 等を用いた多要素認証であり、単に「多要素」であることが安全性を担保するものではありません。重要なのは「フィッシング耐性」であり、認証方式の安全性を評価する際にはこの点を強調すべきです。多要素を求めるために、フィッシング耐性のより低い認証方	

	式が採用されないよう十分留意されるべきです。 【具体的な修正案 】 1. 「フィッシング耐性のある多要素認証」の表現について Ⅲ－２－８－２－２ 主な着眼点 （２）セキュリティの確保 ■修正案 「フィッシングに耐性のある多要素認証」「多要素認証」を、 「フィッシングに耐性のある強固な認証」「強固な認証」に、それぞれ修正	
35	特に、パスキー（パスワードレス認証）の導入・標準化を最優先で推進してください。 今後はパスワード単体での運用を原則禁止し、やむを得ずパスワードを残す場合は必ず 2 要素認証（2FA）を義務化すべきです。 2FA についても、SMS 認証より認証アプリやハードウェアトークン、パスキーなど、より安全性の高い手段を推奨してください。	本改正により、ログイン時などの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を求めております。
36	「ログイン、出金、出金先銀行口座の変更など重要操作時におけるフィッシング耐性のある多要素認証の必須化」は極めて重要です。しかし実務上、設定後にめんどうであるなどの理由で、顧客が自らパスワード認証へ戻す運用や、特別な取引口だけパスワード認証が残ってしまうケースが散見されます。言うまでもなく、せっかく取引に対して高度認証を設定しても、パスワード認証の口が残っていたら意味がありません。 そのため、一旦高度認証を設定したらパスワードは廃止し、ユーザーが戻せない仕組みを明示することが望まれます。 また、現行のリスクベース認証の考え方を活かし、ログイン時はパスワード・取引時はパスキーのような段階的適用も選択肢として提示すべきです。これにより、API 非提供の証券会社でも Personal Finance Manager（PFM）が利用可能であり続け、かつリスク低減が可能です。 中期的には、API 提供と高度認証の同時カットオーバーが消費者影響を最小	後段の段階的適用については、取引や出金等のログイン後の不正な操作を阻止するためにも、不正なログインをさせないことが重要であると考えます。 事業者によってはフィッシングに耐性のある多要素認証の導入をログイン時から順に操作毎に段階的に導入する場合があることも理解しますが、いずれにしても可能な限り早期に対応することが望まれます。

	化しつつ不正防止に資すると思われます。	
37	PC 用ツールでしか取引を行わないのに携帯電話等の複数経路による取引認証を一律に強要するのは利用者の利便性を損ね反対である。	本改正は「フィッシングに耐性のある多要素認証」を求めるものであり、認証を必ず複数経路により行わなければならないとしているものではありません。
38	証券会社等に求めるセキュリティと利便性のバランスは人によって異なるにも関わらず、一律にセキュリティ強化を義務付けることには反対する。 セキュリティ設定に応じて不正アクセス被害に対する補償の有無や内容に差を設けるなどしたうえで、利用者自身が設定を選択可能にするように求める。	今般の事案を踏まえると、フィッシングに耐性のある多要素認証は、一部の事業者による任意のサービスではなく、業界全体で必須化を行うことが重要と考えます。 また、セキュリティの強化により、顧客の被害防止のみならず、犯罪による不当な資金流出を遮断することにもつながります。そのため、こうした被害の未然防止等の取組みを業界全体として行うことは、業界の信頼性の向上にも資するものと考えます。
39	二要素認証の実装、利用に関しては、証券会社の自主的な判断にゆだね、努力義務にとどめるべきだと考える。利用ユーザーも、二要素認証を利用するか否かは自分で判断できることを原則としてほしい。 不正ログイン、売買、出金など、標的にされやすいような大手証券会社はすでに高度な二要素認証を導入しており、改訂せずとも、自主的に対応を行っている現状を踏まえ、一律全ての証券会社に強制するようなことは控えるべき。 二要素認証を利用しない設定にしたユーザーへの対応について、各証券会社は大きく分かりやすく、例えば「当社はこういった認証方法を提供しているがユーザーによる利用は自由で、解除も可能です。ただし、利用しない場合に不正などの被害が発生した場合、原則補償しない」などと表示する必要があります。この表示は義務化すべき。	今般の事案を踏まえると、フィッシングに耐性のある多要素認証は、一部の事業者による任意のサービスではなく、業界全体で必須化を行うことが重要と考えます。 また、セキュリティの強化により、顧客の被害防止のみならず、犯罪による不当な資金流出を遮断することにもつながります。そのため、こうした被害の未然防止等の取組みを業界全体として行うことは、業界の信頼性の向上にも資するものと考えます。 したがって、採用する認証方式を顧客の判断に委ね、それを前提に顧客対応に差異を設けることは適切ではないと考えます。
40	フィッシング耐性のある多要素認証の実装及び必須化を実施する場合、顧客へのスケジュール周知が必要であると考えるが、どの程度前から具体的なスケジュールを示せばよいか。 なお、周知の方法については、ウェブサイトでの公表や書類郵送など、各社任意の方法で実施することに問題ないか。	スケジュール周知期間については、顧客の安心のために、できる限り早期に見通しを明らかにすることが重要と考えます。 また、周知方法の如何は問いませんが、いずれの方法による場合であっても、顧客属性や取引形態等に関わらず、正しく理解できる内容により、確実に伝わる方法で行うことが重要と考えます。
41	「フィッシング耐性のある多要素認証を原則適用すること」は、顧客保護お	

	よびサイバー攻撃への備えとして妥当な方向性であります。 ただし、利用者属性やチャネル特性を踏まえると、すべての顧客に対して画一的に強制適用するには業務的制約が存在するため、原則義務化の方針には賛同しつつも、現場実装との整合性を踏まえた段階的な導入や対象範囲の優先順位付けが可能となるよう、制度上の柔軟な運用設計を認めていただくことを要望します。	システム開発等その他やむを得ない理由による場合に一定の期間を要する場合があることや顧客規模や取引チャネルに応じて段階的に導入していく場合があることは理解できますが、可能な限り早期に対応することが望まれます。
42	金融商品取引業者においては一定のシステム開発や変更が必要になるため、改正案の施行まで、或いは、施行後に十分な猶予期間を設けていただくよう、ご検討をお願いしたい。	
43	出金先口座変更時の名義一致確認や追加認証は、実効的な不正送金防止の観点で重要な措置であり、当社としてもその必要性は十分認識しています。 他方で、口座変更時の業務フローや本人確認プロセスとの整合を図るうえで、認証手段の選定・運用フローの再設計が必要となることから、制度上「導入までの設計検討・改修期間」が確保されることを希望いたします。	
44	多要素認証のデフォルト設定が要請されていますが、明確に多要素認証を望まない顧客（例：資産管理アプリを利用している一部の顧客。多要素認証の運用によりこれらのサービスの利用に支障が出る可能性がある）に対して、多要素認証を完全に解除する機能が提供することが可能でしょうか。	インターネット取引においては、提供するサービスの内容に応じた不正防止策を講じることを求めています。 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については、顧客が取引に利用する機器の都合で多要素認証が設定できないといった場合にやむを得ず解除するケースが想定されます。 御質問のように、上記のケース以外で顧客要望による例外を認めることは、顧客がそのリスクを認識していたとしても不正アクセスの隙を与えることにつながりかねず、不正ログイン・不正取引防止の観点においては、原則としてフィッシングに耐性のある多要素認証を必須化することが適切と考えます。
45	フィッシング耐性のある認証方式を採用しても、顧客が認証器を初回登録する導線や、紛失時の再登録導線において、確実な本人確認が行われなければ、攻撃を防ぐことはできません。認証器の登録・再登録については、同様にフィッシング耐性のある認証方式を利用するか、それができない場合、確実な身元	御指摘のとおり、フィッシングに耐性のある多要素認証の導入に際して、前提として、確実に本人の認証情報を登録することは重要と考えます。

	確認をした上で認証器の登録・再登録を実施するべきです。 「さらに、例えば、以下のような不正防止策を講じているか。」に、下記を追加 ・ 顧客の認証手段の設定時、再設定、もしくは解除時に、新たな認証手段と同等以上のフィッシング耐性のある認証、もしくは本人確認の実施	
46	攻撃者がパスワードログインを足掛かりに自身のパスキーを登録するリスクがあります。そのため、パスキー等の高度認証の初回登録は、公的個人認証など強い本人確認を経たセッション内でのみ許可するよう明記すべきです。	
47	フィッシングに耐性のある多要素認証の実装化及び必須化に対する本人確認強化としての追加措置として、通信キャリアが提供する認証サービス等、確実な本人確認を実施している事業者との認証連携を提案いたします。パスキー等フィッシング耐性のある認証方式を採用する際は、確実な本人確認をすることが重要です。通信キャリアが提供する認証サービスは、強固な所有物認証により、リアルタイム型フィッシング攻撃への耐性があり、安心・安全な多要素認証を実現し、パスキーでの新規/初期登録・再設定（アカウントリカバリー）等に連携活用することも可能です。 【修正案】 （注 3）として下記を追加。 （注 3）フィッシング耐性のある多要素認証の実装にあたり、確実な本人確認を実施している事業者との認証連携（通信キャリアが提供する認証サービス等）を追加的措置として導入することが望ましい。	
48	取引時等の本人確認においては、犯収法に基づいた本人確認が必須であることが前提ですが、認証器の登録時等において、確実な本人確認を行うためには、金融機関に限らず、他業種で確実な本人確認を実施している事業者との認証連携も有用です。OpenID Foundation が策定する「OpenID Connect for Identity Assurance」等の標準仕様を活用し、証跡やメタデータを含めた身元確認済情	貴重な御意見として承ります。

	報の連携を行うことで、安全性の向上が期待されます。 【具体的な修正案 】 3. 他業種との連携による本人確認の高度化 III－２－８－２－２ 主な着眼点 （２）セキュリティの確保 ■修正案 注２に加えて、注３を以下のように追加 （注３）代替的な認証手段として、デジタル庁の提供するデジタル認証アプリの利用や、民間事業者が提供する本人確認支援サービスを認証要素の一つとして利用することも検討すること。特に後者を本人確認済顧客の認証手段の１つとして利用する場合には、当該事業者が必ずしも犯罪による収益の移転防止に関する法律第二条第二項に規定する特定事業者である必要はない。さらには、当該事業者が確実に本人確認を実施していることを確認するため、OpenID Connect for Identity Assurance 等の国際的に標準化された技術仕様を用いて本人確認根拠情報の連携を行うことを検討すること。	
49	口座利用プロセス全体を見た場合、最も重要なのは入口である「ログイン時」だと考えています。ログイン時に安全な対策が講じられていれば、その後のプロセスにおける被害の可能性は大きく低減されると認識しています。 すべての段階に「フィッシング耐性のある多要素認証」を導入すると、プロジェクトの複雑さが増す一方で、防犯上の効果は限定的（コスパが低い）だと考えています。 そのため、ログイン時のみに「フィッシング耐性のある多要素認証」を導入し、出金時や出金先銀行口座の変更時などは、リスクベースの観点から OTP のような多要素認証で対応する、という運用は可能でしょうか。	何らかの事情によりログイン認証を第三者に突破された場合も想定し、ログイン後の重要な操作時にもフィッシングに耐性のある多要素認証を導入することにより、不正取引の被害を各段階で防止するための対策を講じることが重要と考えます。
50	出金時および出金先銀行口座の変更が不正取引に関わるため重要であることは明らかですが、ログイン時についてはなぜ重要な操作例として挙げられているのでしょうか。どのような脅威やリスクを想定しているのでしょうか。	ログイン後に表示される顧客情報等を全てマスキングするなど、仮に不正なログインをされた場合に備えておくことも重要ですが、取引や出金等のロ

	例えば、ログイン時にすべての個人情報等をマスキングし、出金時・出金先銀行口座の変更時にフィッシング耐性のある多要素認証を実装・必須化するとともに、マスキングを解除する際に同じ認証方式を要求すれば、本ガイドラインが想定しているリスクは解消されますか。あるいは、取引と同等に、ログインが大きなリスクという整理でしょうか。	グイン後の不正な操作を阻止するためにも、そもそも不正なログインをさせないような対策を講じることが重要と考えます。
51	電子決済等代行業者は銀行法に基づき、取得した銀行口座の情報をユーザーに提供する等の業務を行っていますが、銀行以外の金融機関（金融商品取引業者様を含む）にも機能連携を行い、複数の証券口座に跨る情報の一覧化等を行うことにより、適切な資産形成を支援するサービス等も提供しています。 電子決済等代行業者が金融機関との機能連携を行う際に、金融機関への「ログイン」時にフィッシング耐性のある認証が要求されると、いわゆるスクレイピングと呼ばれる手法での機能連携を行うことが困難となり、電子決済等代行業者の既存の業務に、大きな支障が生じることが予想されます。 まずは短期的に、参照系の（金融機関のデータの読取のみを行う）業務と、取引や出金などの重要な操作の連携が可能な更新系の業務とを分別し、後者の重要な操作に対してのみフィッシング耐性のある認証手段を導入していくことを提案いたします。なお、フィッシング耐性のあるパスキー認証は操作もスムーズであり、取引のタイミングを妨げるようなユーザー体験とはならないと考えています。 また、中長期的には金融機関（本件においては金融商品取引業者様）において API を整備していただき、そのタイミングで参照系業務での機能連携時にも、フィッシング耐性のある認証手段を導入していくという、計画的なアプローチが必要だと考えます。	証券口座や銀行口座へのログイン時には、フィッシングに耐性のある多要素認証を導入すべきと考えます。
52	顧客が記入のうえ届出印を押印し金融商品取引業者に郵送した書面に基づく取扱いは第三者による改ざんの恐れがなく、「フィッシングに耐性のある」ものと考えられます。 つきましては、出金先銀行口座の変更について、書面に基づく手続きについてもお認めいただきたい。	該当の規定は、インターネット上で手続きを行う場合に対応すべき事項を定めたものであり、書面による手続きを禁止するものではありませんが、書面での変更時においても、顧客になりすました第三者による不正な手続きが行われないよう対応する必要があります。

53	フィッシングに耐性のある方法により出金先口座の指定が行われ、かつ、ログイン時に多要素認証を行っている場合には、顧客の意図しない出金がなされることはないと思われます。 このように不正ログイン及び不正な手続きを防止できる場合には、利用者利便性を確保するために、出金時に多要素認証を行わないことをお認めいただきたい。	犯罪手口は日々高度化・巧妙化しており、ログイン時に多要素認証を行っていた場合においても「顧客の意図しない出金がなされることはない」とは言い切れないと考えられ、その他の段階においても不正な操作を阻止するために複数の対策を講じている必要があると考えます。 その点を踏まえても、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必須化は必要であると考えます。
54	「(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)」という記述は、技術的に不正確。パスキーは PKI を利用して実現される認証技術の一つの具体的な実装形態の一つであり、両者は包含関係にあります。したがって、これらを並列で例示することは、技術的な分類として適切ではありません。 現行案は「重要な操作時」の認証強化を求めていますが、これは攻撃ライフサイクルの一部にのみ着目した「点の防御」であり、本質的な対策としては不十分です。セキュリティは、一連の流れの中で継続的に確保されるべきです。 ガイドラインで「パスキー」という特定の技術名を例示することは、中小証券会社に過度なコスト負担を強いる、金融分野における日本独自技術イノベーションの機運が削がれる、他の重要なセキュリティ対策の軽視を招く危険性がある等の弊害を生む可能性があります。 以上の点を踏まえ、以下の通り修正することを提案します。 （修正案） 初回ログイン時におけるフィッシングに耐性のある多要素認証（例：PKI（公開鍵基盤）をベースとした認証）の実装を必須化（デフォルトとして設定）する。加えて、出金、出金先銀行口座の変更など重要な操作時には、セッションの正当性を検証するための継続的な監視・認証機能を実装すること。(例：リスクベース認証、振る舞い検知、デバイスフィンガープリント、PKI 技術を活用したチャレンジレスポンス方式など)	本改正においては「フィッシングに耐性のある多要素認証」の必須化を求めており、例示としていくつかの認証方法を記載していますが、具体的にどのような認証方法を採用するかは各社が判断するものと考えます。 なお、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）において、「パスキーの普及促進」が掲げられているところです。 また、本改正においては、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必須化だけでなく、ログイン時の振る舞い検知機能の実装や不正アクセスの評価に応じた追加の本人認証を実施する等の対応も求めておりますので、原案のとおりとさせていただきます。
55	改正案の「フィッシングに耐性のある多要素認証(例： パスキー, PKI ベース認証)」の、例示を削除すべき。	本改正においては、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」の必須化を求めており、例示としていくつかの認証方法を記載し

	理由：例示は事実上の強制力を持ち、同等以上の効果を持つ他技術導入を妨げる。また「PKI ベース認証」は範囲が不明瞭で混乱を招く。さらに、パスキーは厳密にはリアルタイムフィッシング耐性を有しておらず、単なるパスワード代替に過ぎない。 以下にパスキーの課題例を示す。 【リアルタイムフィッシングが可能】 WebAuthn の脆弱性がある。攻撃者が PC のログイン用 QR を偽装サイトに表示し、フィッシングメールで誘導。利用者がスマホで QR を読み取りパスキー認証すると、攻撃者 PC で即座にログインが成立する。これは典型的なリアルタイムフィッシングである。 【海外プラットフォーム依存】 FIDO UAF も導入ハードルが高く、高齢者や非スマホ利用者を排除し、金融包摂に反する。実質的に国産技術を排除し海外依存を強制することは、国防・国益・金融安定性の観点から不適切である。海外事業者従業員の属性や地政学リスクを考慮せず国民資産の鍵を「単一貸金庫」に預けることは危険である。	ていますが、具体的にどのような認証方法を採用するかは各社が判断するものと考えます。 なお、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）において、「パスキーの普及促進」が掲げられています。
56	多要素認証の実装例のパスキーとは、FIDO Alliance が策定した FIDO2 の仕様の一部であり、現在 W3C によって標準化された Web Authentication(WebAuthn)のことを指しているという理解は正しいでしょうか。 その場合、『パスキー』という表記よりも、米 CISA Implementing Phishing-Resistant MFA で説明されている『FIDO/WebAuthn authentication』の表記の方が適切だと思いました。(PKI をベースとした認証の表記に合わせるため)	本改正においては、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」の必須化を求めており、例示としていくつかの認証方法を記載していますが、具体的にどのような認証方法を採用するかは各社が判断するものと考えます。
57	多要素認証の実装例のパスキーには、複数デバイス間で同期される Synced Passkey と、特定のデバイスに紐づけられた Device-bound Passkey が存在しますが、プラットフォーマーが実装するパスキーは、Synced Passkey であり、クラウド環境等を通じて、複数デバイスで同一パスキーが同期されたり、別デバイスにパスキーを転送したりすることが可能です。そのため多要素認証でパ	

	スキーを導入使用する場合の、安全性の担保、推奨される運用方針、その他制約事項について、監督当局としての見解を示してください。	
58	多要素認証の実装例のパスキーとは、オペレーティングシステム等を提供しているプラットフォーマー（主に、Apple 社, Google 社, Microsoft 社等）が実装しているパスキーに加えて、FIDO Alliance が策定した CTAP に準拠した外部セキュリティキーを含んでいるという理解は正しいですか。	
59	多要素認証の実装に、パスキー等を導入検討する際、FIDO Alliance が策定したモバイルアプリ向けの規格 FIDO1.1 UAF (Universal Authentication Framework) も含まれているという理解は正しいですか。	
60	多要素認証の実装に、パスキー等を導入検討する際、FIDO Alliance の認定を受けている製品を採用することが望ましいと考えていますが正しいですか。	
61	ログインや出金等、複数のシーンでパスキー認証を提供する際に、ログイン用と出金用で異なる識別子によるパスキー認証を提供することが妨げられるものではないが、同一の識別子によるパスキー認証を提供するとしても、「フィッシングに耐性のある多要素認証」という趣旨からして問題とはならない理解でよいか。 また、「追加の本人認証」について、追加の本人認証は、ログイン時と同一の識別子のパスキーを提供することで問題ないか。	
62	「パスキー」 には 2 つの種類があります。「パスキー」 はデバイス間で同期する、またはデバイスに固定して紐づける（バインドする）ことができます。 ・同期パスキー：クレデンシャル・マネージャーに安全に保存され、デバイス（携帯電話、タブレット、コンピュータ）間でアクセス可能 ・デバイス固定パスキー：単一のデバイス（セキュリティキー）にバインドされ、そのデバイスとしてのみ使用可能 どちらの 「パスキー」 も利用者やサービス提供者のニーズなどに応じて、あんしんして便利にお使いいただくことができるので、補足説明として追記していただいてはいかがでしょうか？	「フィッシングに耐性のある多要素認証」の例示としていくつかの認証方法を記載していますが、具体的にどのような認証方法を採用するかは各社が判断するものと考えますので、原案のとおりとさせていただきます。
63	同じ公開鍵暗号方式を使う FIDO 認証（パスキー認証）でも同期パスキーや	貴重な御意見として承ります。

	秘密鍵を同期しないFIDO2、スマートフォンの生体認証を使うパスキー、秘密鍵を物理デバイスに保存するFIDO対応のセキュリティキー等の種類があり、それぞれでフィッシング耐性を含めたセキュリティの強度に差があります。また名称についてもパスキーという名称が使われ始めた当初は同期パスキーの事をパスキーと呼び、同期しないものをFIDO2と呼んでいましたが、現在はFIDO2でもパスキーと呼ぶ例もあり混乱しております。 仕様ごとに「パスキーType○」等の分かり易い表示に統一しメリット・デメリットを明示すべきだと考えます。 フィッシング耐性のある多要素認証という表記だけでなく、より具体的に認証方式について説明を改正案にも加えた方が良いと考えます。	
64	専用のアプリを利用しモバイル端末で完結する（一般的なブラウザから利用できない）スマホ証券サービスにおいては、端末認証を必須とすることで、「フィッシングに耐性のある多要素認証」と同等の対策を講じていると評価してよいでしょうか。 ここで言う「ログイン」はログイン後に追加の認証なしで取引・出金・登録変更などの「重要な操作」が行えるものを指し、ログイン時の認証だけでは参照しか行えないものは必ずしも含まないと考えてよいでしょうか。 必ずしも操作の都度多要素認証を行うことが求められるものではなく、一度認証をした同一セッション内で一定時間は再度の認証を行わないことも許容されると考えてよいでしょうか。	御指摘の「端末認証」の具体的な内容が必ずしも明らかではありませんが、取引チャネルが限定されている場合であってもそのログイン時においては「フィッシングに耐性のある多要素認証」による必要があると考えます。 また、「ログイン時の認証だけでは参照しか行えないもの」が意味するところが必ずしも明らかではありませんが、ログイン後に表示される個人情報等が悪用される可能性も考えられることから、ログインそのものも重要な操作と考えます。 いずれにしても、「ログイン、出金、出金先銀行口座の変更」などの重要な操作を行う際にフィッシングに耐性のある多要素認証を必須化することが重要と考えます。
65	ログイン時に多要素認証が一度正常に完了したデバイスに対して、「このデバイスを7日間記憶する」などの形で、一定期間内に多要素認証を省略できる機能の提供は可能でしょうか。	一定期間多要素認証を省略できるといった機能は、基本的には望ましくないと考えます。デバイスの乗っ取り、セッションハイジャック等のリスクを防ぐためにも、「ログイン、出金、出金先銀行口座の変更」などの重要な操作を行う際にフィッシングに耐性のある多要素認証を必須化することが重要と考えます。
66	公開鍵方式の記載の時に、例示としてマイナンバーカードを使ったJPKIを挙げることは、マイナンバーカードの利活用促進とセキュリティ向上の両者に役立つと思います。	PKI（公開鍵基盤）にはJPKIも含まれますので、原案のとおりとさせていただきます。

67	本改正案において、多要素認証の具体的な導入に際してのアクセシビリティへの配慮、特に視覚障がい等を持つ利用者がスクリーンリーダー等の支援技術を用いて円滑に利用できるための措置に関する明示的な記載が見当たらないことに懸念を表明いたします。 以下の旨を追記することを強く提案いたします。 「多要素認証の実装及び必須化に当たっては、身体的特性や技術利用環境の多様性を踏まえ、アクセシビリティに最大限配慮すること。特に、スクリーンリーダー等の支援技術を利用する者が円滑に認証操作を行えるよう、Web Content Accessibility Guidelines (WCAG) 等の国際的なガイドラインを参照し、適切なUI/UX設計及び情報提供を行うこと。 また、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代替的な多要素認証を提供する際には、アクセシビリティが確保された手段を優先的に提供すること。」	障害者への対応については、現行の監督指針Ⅲ－２－１３において、顧客保護及び利用者利便の観点も含め、障害者差別解消法及び障害者差別解消対応指針に則り適切な対応を行う、対応状況を把握・検証し対応方法の見直しを行うなどの内部管理態勢の整備を求めています。 各社においては、障害者が障害のない者と実質的に同等のサービスが享受できるよう各々の経営判断に基づき、各施策に取り組むことが望ましいと考えます。
68	改正案に「多要素認証は多様性・中立性を確保し、単一方式への依存を避けること。相互補完できる実績ある国産技術を、併用かつ選択制にすること」を明記すべきである。 「単一方式」は、金融システム全体の全滅リスクがある。またパスキーの穴を埋め、全チャネルを実績ある手法で埋め、IT弱者救済と金融包摂を実現すべきである。また国産技術により地政学的リスクを最小化すべきである。	貴重な御意見として承ります。
69	フィッシング耐性のある認証方式の導入により、Webスクレイピングを用いた家計簿ソフト等のサービス提供が困難となる可能性があります。家計簿ソフト等の利用が、顧客による強固な認証の利用を妨げないためには、金融APIへの対応が不可欠です。その際には、APIセキュリティを強化するため、OpenID Foundationが策定する「FAPI」の採用を強く推奨いたします。 【具体的な修正案 】 5. 家計簿ソフト等への影響とAPI対応の必要性	貴重な御意見として承ります。

	Ⅲ－２－８－２－２ 主な着眼点 （２）セキュリティの確保 ■修正案 注２、注３に加えて、注４を以下のように追加 （注４）顧客が電子決済等代行業者が提供する家計簿サービス等を利用している場合において、電子決済等代行業者が顧客の口座情報にアクセスする際に強固な認証手段を利用できないことによって、顧客による強固な認証手段の設定を妨げないように、オープン API を提供し、電子決済等代行業者が安全な方法で顧客の口座情報等にアクセスできる手段を講じること。また、オープン API の提供にあたっては、OpenID Foundation が策定する FAPI 等のセキュリティプロファイルを用いるなど、不正アクセスの防止に努めること。	
70	今後のさらなるセキュリティ強化とユーザー利便性の両立を図るためには、以下のような認証方式も並列的に検討可能な環境整備が重要と考えます。 ■マイナンバーカードやマイナ Wallet をトラストアンカーとしたデジタル ID を活用した本人確認 ・公的個人認証サービスを活用し、マイナンバーカードの IC チップに格納された電子証明書を用いることで、本人性の真正性・完全性を担保可能。 ・本人同意のもとで、氏名・住所・生年月日・性別といった「基本 4 情報」の提供が可能となり、本人確認プロセスの自動化・再利用が実現。 ・対面不要で高信頼な本人確認が可能となり、行政・金融・民間サービス間での相互運用性を高める基盤技術として有効。 ■分散型 ID（DID）と検証可能な資格情報（VC）を活用した認証方式 ・DID による分散型識別子と VC による属性証明を組み合わせることで、自己主権型の本人確認が可能。 ・生体認証やスマートフォンを用いた非対面 KYC、属性情報の提示・検証など、柔軟かつプライバシー保護に配慮した認証設計が可能。 ・Deepfake 対策を含む高度な本人確認技術との統合が可能であり、今後の不正	

	アクセス対策や詐欺防止にも有効。	
71	FIDO 対応のセキュリティキーは NFC 専用になりますが、タッチ決済付きのクレジットカードやマイナンバーカードのハードウェアに JAVA プログラムを載せることでセキュリティキーとして動作します。 もちろん既存のプログラムとの競合等で動作しない可能性も否定できませんが、マイナンバーカードにセキュリティキーの機能を追加できればマイナンバーカードの普及を促進できますし、クレジットカードやキャッシュカードにセキュリティキーの機能を追加することで、セキュリティキーを広く普及させることも検討をすべきだと考えます。	
72	スマートフォン以外の物理デバイスに秘密鍵を保存する FIDO 対応のセキュリティキーではパスキーハイジャックや生体ハイジャックのリスクはなく、スマートフォンの生体認証を使ったパスキー認証よりはるかに安全です。スマートフォンの生体認証を使ったパスキー認証と FIDO 対応のセキュリティキーは FIDO サーバーとの信号のやり取りは基本的に同じであり両方に対応する際の負担は大きく変わらないので、高いセキュリティが要求される場合には FIDO 対応のセキュリティキーを使った FIDO 認証を選択可能なように認証システムを構築しておくことが望ましいと考えます。	貴重な御意見として承ります。
73	パスキーハイジャック及び生体ハイジャックの対策については、どのような認証方法を採用するかにかかわらず設定を強く推奨すべきです。具体的にはアップルアカウントやグーグルアカウント等の二要素認証の設定と盗難デバイス保護機能の設定です。 また、この２つの設定が出来ないスマートフォンについては使用を推奨しないか補償対象外とすべきだと考えます。	
74	「フィッシング耐性のある多要素認証」へ移行した顧客に対して、バックエンドサーバーに保存されているパスワードなどに関する旧認証情報は削除すべきでしょうか。（そのまま保存している場合、万が一漏えいした際に、攻撃者が「フィッシング耐性のある多要素認証」未導入の他社サービスに対して不正ログインを試行できるリスクがあります。）	御理解のとおり、旧認証情報は適宜削除する必要があると考えます。

75	金融庁に対し、多要素認証（MFA）へのバランスの取れたアプローチを検討するよう推奨します。MFA 戦略は、顧客の利便性とセキュリティリスクのバランスをとる必要があります。効果的なリスク評価メカニズムを導入することで、金融機関はそれぞれのリスク許容度に基づいて、MFA 導入の適切な範囲を決定できます。この柔軟性により、業者は利便性とセキュリティのバランスを自律的に確保し、リスクに応じた MFA アプローチによって健全な競争環境を維持できます。 例えば、あるメカニズムによって同じ IP アドレスとデバイス／アプリからのログインアクティビティが確認され、その他のリスクシグナルが一定であれば、組織は短期間の一定期間内の後続のログインに対して MFA を省略することができます。 さらに、金融機関は、MFA の導入の有無に応じて、提供する補償レベルに差をつけることも検討できます。MFA にはメリットがありますが、様々なレベルの脅威に対応するために、他のリスクベースの認証アプローチも検討することが重要です。他の管轄の経験から、組織が MFA を実装すると、詐欺攻撃が進化し、悪意のある人物が顧客を操作して代理で MFA を実行させるようになることがわかっています。そのため、MFA に対するリスクベースのアプローチにより、組織はこれらのリスクを評価して対処できます。	貴重な御意見として承ります。
76	携帯電話を持っていない者にも配慮すべき。	フィッシングに耐性のある多要素認証の設定について、「顧客が必要な機器（スマートフォン等）を所有していない」等の場合には、暫定的な対応として代替的な多要素認証を提供することを求めております。
77	デフォルトでの多要素認証有効化、ならびにユーザーによる解除の制限について、強固な本人認証を実現するうえで重要な施策であると認識しています。 ただし、高齢者等の一部顧客層では操作が困難となる事例や、チャネル・デバイスごとの対応可否の差異も存在するため、「解除制限の対象範囲」や「例外的な運用」について柔軟な運用が可能となるよう、制度面での配慮（例：一時解除や代替認証の明示）をいただけると助かります。	認証の設定は顧客側の操作が必要不可欠であることを踏まえると、顧客側の物理的・技術的な理由で設定できない場合も考えられ、そのような事情でフィッシングに耐性のある多要素認証の設定を解除する場合であっても、解除率の状況をフォローし、解除率が低くなるような対策を講じる必要があります。

		いずれにしても、顧客にインターネット取引サービスを提供する事業者においては、サービスの利用に必要な IT リテラシーについて、顧客の意識向上に努めていくことが重要と考えます。
78	以下に該当する顧客は監督指針の想定する『やむを得ずかかる多要素認証の設定を解除する場合』の一類型と整理して問題ないか。 （１） IT リテラシーが著しく低い等、複雑な端末の設定や操作が困難な顧客 （２） フィッシング耐性のある多要素認証を選択するも、複数の取引端末を利用する等、必ずしもフィッシング耐性ある認証方式を利用できない顧客 （３） 高頻度取引を行うため、自身のリスクにより多要素認証の解除要請があった顧客 （４） 出金時においてのみ二要素認証の解除要請があった顧客（解除に際しては二要素認証を適用）	（１）については、認証の設定は顧客側の操作が必要不可欠であることを踏まえると、顧客側の物理的・技術的な理由で設定できない場合は「やむを得ずかかる多要素認証の設定を解除する場合」に該当する可能性がありますが、IT リテラシーが著しく低い顧客の場合は、そもそもインターネット取引を提供することの適切性についても検討いただく必要があると考えます。 仮にこのような事情で設定を解除する場合であっても、解除率の状況をフォローし、解除率が低くなるような対策を講じる必要があります。 いずれにしても、顧客にインターネット取引サービスを提供する事業者においては、サービスの利用に必要な IT リテラシーについて、顧客の意識向上に努めていくことが重要であると考えます。 また、顧客の要望による例外を認めることは、顧客がそのリスクを認識していたとしても不正アクセスの隙を与えることにつながりかねず、顧客が身に覚えがない第三者による不正なログインを早期に検知し、取引や出金等のログイン後の不正な操作を阻止するためにも、そもそも不正なログインをさせないような対策を講じることが重要と考えます。 このため、（２）～（４）については「やむを得ずかかる多要素認証の設定を解除する場合」に該当しないと考えます。
79	「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」の顧客操作のカウントから「解除率」を算出することになると考えていますが、当該ケースの顧客が 2 台のパソコンからログインを行う場合には、1(顧客)ではなく 2(解除)のカウントと考えればよいでしょうか。 また、「解除率」を算出する上での分母は、一定期間の「ログイン」数と考えてよいでしょうか。	前段については、顧客毎に算出するものと考えます。 後段については、一定期間のログインといった稼働顧客数のみでカウントするのではなく、全ての顧客数を基準に算出するものと考えます。

80	フィッシングに耐性のある多要素認証導入までの経過措置として、共通ショートコードもしくはRCSによるワンタイムパスワード等を導入し、認証強化を行うことを提案いたします。 【修正案】（注２）に「共通ショートコードやRCSによるワンタイムパスワード等を導入し、認証強化を行う。」を追加。	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、各社において代替的な多要素認証を提供することにより、被害防止に努めていただくことを求めています。
81	ログイン通知や不審な取引の即時アラートを必須とし、顧客が異常なアクセスや取引に早期に気付ける仕組みを整備してください。セッション管理（全デバイスからのログアウトやログイン履歴の確認）や、信頼できる端末・IPアドレスの登録機能も有効です。	本改正において、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を求めております。
82	ログイン履歴で提供する項目を定義・明確化すべき。	ログイン履歴で提供する項目については、顧客が自身の取引かどうかを判別できる程度の内容が求められると考えます。
83	「認証連続失敗時のアカウントロック自動発動」は、特にログイン用の識別子として、顧客番号連番利用などをしている場合、DoS攻撃による大規模アカウントロック＆コールセンター飽和攻撃に悪用され、この混乱に乗じて攻撃者がアカウント乗っ取りをすることが想定されます。 機械的な総当りには遅延応答（例：1分待機）や追加認証要求が有効であり、アカウントロックは最終手段と位置づけるべきです。	貴重な御意見として承ります。
84	現行案では、パスキー必須化までの暫定措置として振る舞い検知を推奨していますが、パスキー導入後もセッション乗っ取りや不正操作は発生し得るため、振る舞い検知や行動分析は恒久的に必須とすべきです。	本改正において、フィッシングに耐性のある多要素認証の導入後においても、「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」を求めています。
85	セキュリティの確保として行う不正防止策として、不正アクセス検知機能の導入、セッションや取引のモニタリングの強化自体をより明確に単体として位置付ける記述にすべき。また、民間外部委託事業者等の積極的な活用等を位置付ける記述にすべき。 （理由）金融庁が6月に公表した「金融分野におけるITレジリエンスに関する分析レポート」においても、「インシデントが発生していない金融機関にお	セキュリティの確保として行う不正防止策として、御指摘のような内容を含めて多層的に対策を講じることが重要だと考えます。 なお、本改正において、フィッシングに耐性のある多要素認証の導入後においても、「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」を求めています。

	いても、サイバーセキュリティを含めた IT リスク管理態勢を強化すべき」「顧客口座への不正アクセスの事案は、証券業界に限らず、金融業界の信頼を揺るがしかねない問題であり、認証やモニタリングの強化などを含め、迅速な対応が必要である。」「セッションや取引のモニタリングの強化が必要」と記述されており、金融機関全体の底上げと不正アクセス検知導入の必要性を示唆している。	
86	「不正アクセスの評価」とは、「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」及び「事後検証」を指すとの認識で相違ないか。	顧客の状況に応じたリスク評価を行うことが重要と考えており、必ずしもログイン時の挙動だけに限るものではないと考えます。
87	不正アクセスの評価に応じた追加の本人認証については、以下のような対応で十分という理解でよいか。 ・モニタリングの結果、不正アクセスが疑われるケースでは、本人に電話し不正アクセスの有無を確認。電話でのコンタクトができなかった場合はログイン規制等を実施、規制解除にはコールセンターに電話するようにメールで案内 ・コールセンターに電話があった際に、発信電話番号や氏名、住所、生年月日等により本人確認を実施の上、ログイン規制を解除、不正アクセスの有無を確認	インターネット取引サービスを提供する事業者は、顧客や業務の特性、提供するサービスの内容を踏まえながら、その時々のセキュリティ技術水準や犯罪手法等に応じて、不断にセキュリティ対策を見直していくことが重要と考えます。 そのため、個別の対策について、一概に適否を述べることは差し控えます。
88	不正防止策として、海外をアクセス元とする口座へのログインまたは取引の制限を加えるべきである。 殆どの証券会社において、非居住者による口座開設や取引を制限しているのであるから、制限されているはずの口座において、海外をアクセス元とする口座へのログインまたは取引が発生するのは論理的に矛盾している。 例外的に本人から申告があった場合（居住者のままでの一時的な海外渡航など）を除き、海外をアクセス元とする口座へのログインまたは取引による不正アクセス被害については、論理的矛盾のある口座へのログインまたは取引を看過した証券会社側の過失として扱うべきである。	貴重な御意見として承ります。
89	「他の銀行口座との連携サービス」とは、「株式等の取引時に自動で銀行口座から証券口座へリアルタイムで資金移動を行うサービス」を指しており、銀	御指摘の事例以外でも不正送金等のリスクが存在する可能性がありますので、御指摘の事例に限定することは適切ではないと考えます。

	行側の認証無しで即時に預金の移動を可能としているものという理解でよいか。 以下は「他の銀行口座との連携サービス」の対象に含まれるという理解でよいか。 ・口座振替契約を事前に締結し、都度、顧客の指示に基づいて銀行口座から証券口座へリアルタイムで資金移動を行う 以下は「他の銀行口座との連携サービス」の対象外という理解でよいか。 ・NISA の積立等のために口座振替契約を事前に締結し、月 1 回などの頻度で銀行口座から証券口座へ定期定額で入金するサービス（銀行口座での引き落としから、証券口座への反映まで数営業日かかるもの）	なお、投資信託等の定時定額購入における銀行口座から証券口座への定期的な入金サービスについては、設定変更等の重要な操作を除いては、御理解のとおりです。
90	「銀行口座との連携サービス」の具体的な定義について明確にしていただきたいです。例えば、「銀行振込を 24 時間リアルタイムでご通知」といったものも連携に該当するのでしょうか。 あるいは「証券口座の認証のみで預金引き出しが可能」なものを指していますでしょうか。	「銀行振込を 24 時間リアルタイムでご通知」の具体的な内容が明らかではありませんが、本規定の趣旨は、顧客の身に覚えのない不正な操作で資金移動が行われること及び顧客の個人情報等が漏えい（不正に閲覧）されることを防ぐものです。
91	「他の銀行口座との連携サービス」においては、証券口座単体だけでなく、連携サービス全体のセキュリティを確認した上で不正防止策の検討と対応を行うことが肝要なものと理解している。 例えば、銀行口座側で資金移動（出金）金額の上限設定を設けることができれば、取引機能の上限設定を提供していると見なされるのか。	銀行口座からの資金移動金額の上限設定と取引機能の上限設定は別のものと考えます。 なお、御理解のとおり、連携元・連携先における責任・役割分担の明確化を適切に実施することにより顧客被害の拡大防止を図ることが重要と考えます。
92	顧客からの依頼に基づいて金商業者側で設定変更を行う方法であれば、ウェブサイトからの設定に限らず、電話や対面等で設定を受付ける方法も有効な対策に含まれる理解で良いか。	事業者が顧客本人からの依頼であることの真正性を確認した上で行うという前提であれば、御理解のとおりです。
93	振る舞い検知や異常ログイン時の自動通知は、初動対応の迅速化や被害抑制の観点から極めて重要な対策であると理解しています。 一方で、AI 活用や機械学習による高精度な振る舞い検知をすぐに実装できな	システム開発等その他やむを得ない理由により、対応に一定の期間を要する場合があることは理解しますが、不正取引を防止するための対策であることから、可能な限り早期に対応することが望まれます。

	い事業者も想定されるため、段階的な導入（例：ルールベースの簡易検知からの開始）や、ベースライン水準の明示など、事業者規模やリソースに応じた実施の考え方を併せて整理いただくことを希望します。	
94	下記の文言について、追記をしていただいてはどうか。 ・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 （*セッションの切断など*）	御指摘を踏まえ、明確化の観点から修正いたします。
95	ログイン ID、PW、取引時暗証番号に関し、求める基準を明示・定義すべき。	ID、パスワード、取引暗証番号の複雑化による方法以上に強固なセキュリティ対策として、本改正において、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」を求めています。
96	メールへの「ブランドアイコンの表示」や予めの重要事項の事前案内などを明確に行う義務を明記する。	本改正においては、メールの送信ドメイン認証技術の計画的な導入等、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るよう求めています。
97	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・出金先口座変更等の、不正取引に関する情報を業界横断で連携することで、一つの取引事業者で被害を受けた顧客が、他の取引事業者で被害を受けることを防ぐことができると考えられます。OpenID Foundation の策定する仕様である Shared Signals and Events (SSE) Framework を活用することで、世界標準に準拠し、相互運用性を担保した形でリアルタイムな情報連携が促進されることが期待されます。 【具体的な修正案 】 4. 事業者間での情報連携による被害拡大防止 Ⅲ－２－８－２－２ 主な着眼点 （２）セキュリティの確保 ■修正案	貴重な御意見として承ります。

	「さらに、例えば、以下のような不正防止策を講じているか。」に、以下を追加 ・不正なログイン・異常な取引等を検知した場合に、OpenID Foundation が策定する Shared Signals and Events (SSE) Framework を用いた被害状況のリアルタイムな事業者間での情報連携等によって、当該顧客の他事業者での被害拡大の防止に努めること。	
98	今回のガイドライン改正では、下記の事項を明示していただきたく強く希望します。 A. パスキーや PKI ベースのフィッシング耐性型認証導入後も、インフォスティーラー攻撃・セッションハイジャック等のリスクが持続することを明記し、単なる認証突破防御だけでなく認証後のリスクにも対応する多層的対策を推奨すること。 B. ゼロトラスト思想に基づき、セッション状況の継続的監視、異常検知時のリスクベース再認証、デバイス・トークンの厳格なバインディング、チャレンジレスポンス検証などの先進的なセッション管理技術の導入を促すこと。 上記を追加・明示することで、本ガイドラインが国際的な基準と整合し、継続的にハッキング行為を受けやすい業界に対する被害抑止効果に大きく寄与するものと考えます。	インターネット取引サービスを提供する事業者は、顧客や業務の特性、提供するサービスの内容を踏まえながら、その時々のセキュリティ技術水準や犯罪手法等に応じて、不断にセキュリティ対策を見直していくことが重要と考えます。
99	本案ではセッションセキュリティの観点がやや薄い印象です。 Cookie 送信元のブラウザ・IP 変化検出による権限制限や、異常取引検知情報の事業者間共有（例：OpenID Shared Signals Framework の活用を米国のサイバーセキュリティー・インフラセキュリティー庁(CISA)やアメリカ国家安全保障局(NSA)は推奨しています）を記載することで、広域的な不正防止が可能になります。	貴重な御意見として承ります。
100	現状、多くの不正取引は利用者端末の脆弱性経由ですが、将来的には直接的に金融機関サーバへ不正ファイルを送り込み、制御や改ざんを試みる攻撃の増加も予想されます。利用者端末以上のセキュリティ強度を、金融機関側にも備えるべきだと考えます。	現行の監督指針においても、サイバーセキュリティ事案の未然防止について経営上の重大な課題として認識し態勢を整備することを求めています。

	そのための一案として、ディスプレー（モニター）と視覚センサ（カメラ）を用いた不可逆的な「デジタル-アナログ変換（D/A 変換）技術」を提案します。 これは、通信経路上のデジタルデータを金融機関側のモニターで一度アナログ信号化し、再度視覚センサでデジタル化して認証・取引データを一方向でやり取りする仕組みです。 実運用において、ペネトレーションテストではなく、全世界に公開された環境下で長期にわたり、通信データの盗取・改ざん・破壊が一切発生しなかった実績があり、すでに著作権保護用データベース、医療機微情報の保護、真贋証明等の分野で運用され、高い耐攻撃性が確認されています。 この技術を金融機関側の認証にも導入することで、 ゼロデーアタックやランサムウェア等の未知の不正プログラムを遮断 中間者攻撃・ブラウザ乗っ取り型攻撃（MITB）の無効化 コールドストレージ内での生体認証（顔・指紋・静脈）情報の安全な処理と保管 コールドストレージ内に保管された通信データの改ざん・盗聴防止が実現可能です。 現行案で示されたパスキーや PKI と組み合わせることで、認証・通信・データ保護の三位一体の強化が可能となり、利用者保護の実効性が大幅に高まると考えます。	また、本改正により、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応について、最優先の経営課題の一つとして位置付け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ことを求めています。
Ⅲ－２－８－２－２（３）　顧客対応		
101	利用者へのセキュリティ教育や注意喚起も継続的に実施し、実効性ある対策となるよう強く求めます。	顧客層や業務の特性、提供するサービスの内容に応じて、利用者にとってわかりやすい情報発信や注意喚起を行うことが重要と考えます。
102	注意喚起について義務化とあるが、注意喚起が業界の文化となり利用者にも根付いた段階で、脅威主体が「偽の注意喚起」をばら撒くことで、寧ろ被害者が増えることが想定される。 そもそも、メールや SMS 等による宣伝や注意喚起メールを行うべきではな	フィッシング対策の観点から、事業者においては、自らになりすました偽の注意喚起等に関する情報収集やそれらに関する注意喚起を行うことが求められると考えます。

	い。 理想としては公式アプリ内でのみ注意喚起やお知らせが行われることが理想であるが全ての利用者がアプリを使用できるとの前提には立てない場合もあるため、アプリ内通知を慣行とする流れが好ましい。	
103	証券口座乗っ取り被害の専用窓口を設け、わかりやすく表示し容易にアクセスできるよう措置する。電話連絡などを行っても受理窓口・担当不足のため何時間もつながらない。よって、「即応体制の整備」として電話架電から 15 分以内の即応体制整備基準を明記・義務づける。	各社においては、顧客の疑問や不安に迅速に対応できるよう、顧客からの相談窓口の運営を含め、規模・特性に応じた顧客対応の態勢を整備することが重要と考えており、本改正においても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等の着眼点を追加しています。
104	メール照会に関しても受け付け窓口とそのメールアドレスをわかり易く表示するとともに、原則としてメール受理のシステム確認メールも返信可能なものとすること。くわえて、即応体制の整備によりメール送信・受理から 7 日間以内に質問事項に真摯に回答することを義務づける。	
105	今回の改訂案について　証券会社の顧客対応窓口の設置・運用の詳細につき具体的に明記厳格化し義務化を明記していただきたい。	
106	今回の改正指針に遡及効がないことは理解しておりますが、その趣旨は普遍的な顧客保護の原則に基づくものです。よって、過去の対応においても本改正趣旨に則った再検討と誠実な対応を金融機関に促すようお願いする。	貴重な御意見として承ります。
107	指針制定後の被害者の補償にも言及してください。	改正後の監督指針Ⅲ－２－８－２－２（３）において、不正取引による被害が発生した場合に、補償を含む顧客対応のための態勢整備を求めています。
108	ユーザーが証券会社の指定するセキュリティ対策（パスキーや 2FA 等）を適切に実施しているかチェックできるようにし、対策していたにもかかわらず、サービス側の脆弱性や不備で被害が発生した場合は、原則として全額補償を義務付けてください。 被害額が大きい、証券会社の資金が不足している、またはユーザーの責任に転嫁して半額補償とするような運用は、利用者保護の観点から極めて不適切です。 補償体制や財源の明確化、補償条件や手続きの透明化を徹底し、誰もが安心	監督指針は監督上の着眼点や留意点等を記載するものであり、証券会社が顧客に対して行う補償の実施や手法について規定する権能はありませんが、金融庁としては、今般の証券口座の不正アクセス・不正取引事案で被害を受けた顧客への補償については、証券会社に対して、顧客の立場に立った誠実かつ公平な対応を行うよう求めています。

	して資産運用できる環境を整備してください。業界全体で補償基金を設けるなど、万が一の際にも利用者が確実に保護される仕組みも検討をお願いします。	
109	（１）監督指針本文への「補償制度一律化」条項の追加 ・「証券会社は不正アクセス等による被害発生時、販売チャネルを問わず同一の補償基準を適用せねばならない」と明記。 ※補償範囲・方式の目安を付則として示す。 ※日本証券業協会（JSDA）への加盟有無と、証券投資者保護基金への加入有無の明示・標示義務規定の書き込み。 ・被害額の全額補償を原則とし、認証欠陥やシステム不具合が原因の場合は例外なく全額補填とすること。 ・顧客の過失が軽微な場合は全額、重大な過失が認定された場合のみ一定割合減額とする詳細条件を提示。 （２）被害対応体制の標準要件化 ・監督指針に「被害発生時の初動対応体制」要件を追記。 ・初動通知（24 時間以内）や補償判断期限（30 日以内）など、具体的なサービスレベルを設定。 （３）監督官庁による実効性検証の仕組み整備 ・定期的な第三者監査や報告書提出を義務化し、補償実績の公表を促す。 ・業務改善命令の対象要件に「補償遅延・不当減額」も明記。	
110	金融機関の経営方針を理由とした責任逃れの明確な禁止 システム不備に起因すると考えられる被害についての申し出に、「取引方針・経営方針」を理由に、話し合い・調査や補償の検討を拒否する行為を、監督指針で禁止すべき。 振込の誤認や操作ミスに、分かりにくい画面表示や手続きが影響していると考えられる場合は、銀行に説明責任・補償責任があることを明記すべき。	
111	不正アクセス等による被害の補償について、「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、被害回復に向けて誠実かつ迅速に対応する」との記載では、補償の実効性や公平性の観点から不十分と考えます。 　金融商品取引業として登録された事業者には、高度なシステム安全性の確保が義務付けられており、これが担保されていなかった場合には、顧客保護の観点から明確な補償方針を定めるべきです。 　安全性確保に失敗した事業者自身が、補償の有無や範囲を判断する現在の仕組みは、顧客の立場から見て公正性を欠くおそれがあり、不適切と考えます。補償判断に関しては、より客観的かつ中立的な基準の策定が望まれます。	
112	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。被害補償については顧客に重大な過失がない限り、原状回復、全額補償で対応しているか。 ※※「被害補償については顧客に重大な過失がない限り、原状回復、全額補償で対応しているか。」を追記、米国の事例も勘案　有価証券管理業者としての原則的な補償基準を定めることをお願い致します。 　金融商品取引法第 43 条「有価証券管理業務に関する特則（金融商品取引法第四款)」にて、「金融商品取引業者等（証券業者を含む）は顧客に対し善良な管理者の注意をもつて有価証券等管理業務を行わなければならない」という義務（いわゆる受認義務）が法令上課されております。預託資産の不正取引により資産が失われたことは管理債務（責任）の不履行（民法 657 条）にあたり、金融商品取引業者は原状回復義務（民法 545 条）を負うこととなります。一部の証券会社の約款における広範な免責規定（例えば、第 3 者による不正利用でも重大な責任がない限り免責)、は金融商品取引法第 43 条遵守、消費者保護の観点から排除が必要であると考えております。	
113	「真摯な顧客対応を行う態勢の整備」に、「不正アクセスの被害について、全面的に証券会社側の免責事項とする約款を定めてはならない」という内容を含	

	めるべき。	
114	不正アクセス・不正取引事案が発生した場合の補償の有無について、監督指針では「顧客の被害補償を含めた真摯な対応」とされているが、どの程度までの補償が求められることになるのか。	
115	顧客資産は「金融機関の管理下にあるが、顧客の所有物」であることを監督指針に明記すべきである。 民法および金商法の趣旨からしても、有価証券は特定物として顧客に所有権があることは明白です。 監督指針には、「顧客資産の所有権は常に顧客に帰属し、いかなる理由によってもその所有権を侵害してはならない」旨を明記してください。	貴重な御意見として承ります。
116	不正アクセスによる資産損失に対しては、金銭補償ではなく「原状回復（現物返還）」を原則とすべきである。 現在、一部証券会社では「二分の一補償」などと称して、顧客の所有権に基づく正当な返還を拒む運用が行われています。 しかし、民法第 415 条に基づき、特定物については原状回復義務が基本原則です。 監督指針には、「不正アクセス等によって顧客資産が流出した場合、金融商品取引業者は当該資産の現物返還を原則とする」旨を明記すべきです。	
117	顧客に対して「自己責任論」による補償拒否を行う対応は禁止すべきである。 セキュリティ義務を果たさなかった金融業者が、顧客に過失があるかのように装って補償を拒否するのは不当です。 金融庁は、善管注意義務の視点から厳格な行政指導を行うべきです。	
118	金融庁の使命は、国民の財産権（基本的人権でもある）を守ることです。 私たちは「所有権に基づく正当な返還」を求めており、今後、監督指針に「原状回復原則」と「所有権尊重原則」が明記されることを強く要望いたします。	
119	今後の被害の防止策のほうに注目してしまっていて、既存の法令に基づく対応が実施されていないように思える。 被害以前に、「第三者による取引」が生じているのであるから、「犯収法に基	貴重な御意見として承ります。

	づく取引時確認（本人確認）を的確に実施」出来ていなかった訳であり、証券会社に対し犯収法違反を問う必要がある。 　証券会社の犯収法違反に起因した損害は、証券会社側の重過失によるものであるため、証券会社側が損害の全額を負うべきことも明らかであるものと考えられる。（証券会社側の法令違反の結果によって生じた損害（半額など）を、顧客に転嫁することは許されない）	
120	今般の「インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が多発したこと」の根本的原因は、「証券会社側のインターネット取引サービスにおいて、基本的なセキュリティ対策にさえ不十分な箇所があった」という、「本当に初歩的な問題」であり、「お金をかけなければいけないところ（セキュリティ）にお金をかけず、客を集めるためにお金を使ったり、セキュリティを軽視して利便性を優先させた」という、証券会社の経営者などの輩の顧客保護軽視の経営姿勢に根本的原因があるものと考えられる。 　この顧客保護軽視の経営姿勢は、「約款に証券会社側の免責を定めていれば、顧客に損害リスクを転嫁出来る」という甘い認識に由来しているものと考えられるため、「約款による証券会社側への免責の適用基準を厳格化し、証券会社側における損害補償コストを上げる（損害補償コストがセキュリティ対策コストを上回るようにする）」ことでしか改められないものと考えられるため、この点を監督指針に観点として盛り込むべきである。	貴重な御意見として承ります。
Ⅲ－２－８－２－３（１）　犯罪発生時		
121	犯罪発生時に関して、 １.「インターネット取引における不正アクセス・不正取引」とあるが、不正アクセスは確認できたものの、それが不正取引に繋がらなければ、「犯罪発生報告書」の対象外という整理でよいでしょうか。 ２.「インターネット取引における不正アクセス・不正取引」とあるが、当社における顧客口座において不正アクセスと不正取引の両方が確認できた場合に「犯罪発生報告書」を届け出るものなのか、あるいは、他社の顧客口座で不正アクセスと不正取引が確認できた取引に関連している可能性がある取引が、当	１．不正取引に至らなかった場合でも、不正アクセスを認識次第「犯罪発生報告書」を提出する必要があります。 　２．判明の端緒に関わらず、報告対象となる事案を認識次第、「犯罪発生報告書」を提出する必要があります。 　３．「犯罪発生報告書」の様式は、対象となる金融商品取引業者等に別途提示します。 　４．各事業者の所管に応じて、金融庁長官又は財務局長宛ての報告となります。

	社を介した取引でも確認ができた旨の情報を日本取引所自主規制法人等より入手した場合においても、この「犯罪発生報告書」を用いて当局報告が必要になるのでしょうか。 ３．監督指針上での記載のみならず、「犯罪発生報告書」の報告命令の枠組が別途出来るものなのかご教示ください。 ４．「当局宛て報告」というのは、財務局宛報告と理解すればいいでしょうか。 ５．既に「犯罪発生報告書」にて当局宛手報告したものについては、既に犯罪と認識し、疑わしさがないのであれば、警察庁宛ての「疑わしい取引の届け出」は不要という理解でよいでしょうか。	５．一般論として、「犯罪発生報告書」を提出することをもって「疑わしい取引の届出」の提出義務がなくなることはありません。「疑わしい取引の届出」の提出要否については、「犯罪発生報告書」と根拠となる法令が異なることから、回答を差し控えます。
122	「犯罪発生報告書」は、所定の様式はなく、報告を行う金融商品取引業者等が任意の形式により提出を行えばよろしいでしょうか。	「犯罪発生報告書」の様式は、提出対象となる金融商品取引業者等に別途提示します。
123	「犯罪発生報告書」は別紙様式集に追加されるという理解で良いか。 また、報告内容については、各証券会社との意見交換を通じ、実務上過度な負担とならない範囲の報告内容としていただきたい。例えば、不正アクセス等はその性質上、複数の被害が同時期に起きた場合、IP アドレスが異なる等の事情により、その行為者が同一であるかを特定することが困難である。一定の期間内に複数の不正アクセス等が行われた場合にはまとめて一報告することが出来る等の運用にしていただきたい。	
124	「犯罪発生報告書」について、テンプレートの提供はありますでしょうか。	
125	監督指針改正後は、インターネット取引による不正アクセス・不正取引が認識された場合、「障害発生等報告書」、「個人情報等漏えい等報告書」による報告は不要になるのでしょうか。 それとも、「犯罪発生報告書」とあわせて、「障害発生等報告書」、「個人情報等漏えい等報告書」の報告もそれぞれ必要となるのでしょうかご教示ください。	発生した事案の内容に応じて、必要な報告書をそれぞれ提出する必要があります。
126	不正取引が発生しておらず、不正アクセスのみが発生した場合でも、「犯罪発生報告書」の提出は必要となるのでしょうか。	御理解のとおりです。

その他		
127	マイナンバーの紐付けの無い口座が詐欺に使用された場合は金融機関が連帯責任を負うルールにしてください。	貴重な御意見として承ります。
128	デジタル庁が令和 5 年に開催した「本人確認ガイドラインの改定に向けた有識者会議」による検討の結果、「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」において、「本人確認」は、「身元確認」と「当人認証」から構成されると明確に定義される見込みです。当団体が 2023 年に発表した「民間事業者向けデジタル本人確認ガイドライン」においても、同様に定義しております。 本監督指針においても、本人確認と身元確認と当人認証の違いに留意され、より本監督指針の意図が明確に関係者に伝達されるように文言を見直されることを提言いたします。	貴重な御意見として承ります。
129	監督指針に沿って各金融機関がどのような態勢変更等を行ったかなどのフォローアップの実施とそれに基づいた監督指針の適宜見直しを行っていくべき。 （理由）今回の監督指針の改正で打ち出す方向性は金融取引におけるセキュリティ向上や金融犯罪の抑止のために必要であるので、この改正によりどのように各金融機関において実装され、その結果出てくる課題等は何かなどフォローアップをしっかり行い、それを踏まえ、必要に応じて監督指針も再改正するなどの政策のローリングモデルを構築すべき。	セキュリティ態勢の構築状況等についてのモニタリングは随時行っていくとともに、今後も、サイバーセキュリティ環境等の変化に伴い監督指針等の見直しは不断に行ってまいります。
130	今回の監督指針の内容や趣旨そのものを各金融機関において確実に実装させるためには、抜本的な支援措置の強化を金融庁において早急に検討するとともに、達成状況のフォローアップや必要な技術支援（必要に応じて民間知見の活用）、また、金融機関と外部民間企業との必要な連携の促進（外部ツールの積極的な活用等）などの環境整備、口座連携等に向けた工程表の作成など必要な各種政策を金融庁としてパッケージとして明らかにしたうえで政策を進めてもらいたい。 （理由）今回の監督指針の改正は、金融機関からすると、今後対応すべきことがより明確になったあるいはなるということで大変意義深いものである。それゆえに、	貴重な御意見として承ります。

	その内容や趣旨を実現するための各種措置の検討が今後大至急の課題として必要不可欠である。	
131	今回の内容については、金融商品取引業者以外の金融機関への監督指針にも反映されていることは必要であるので、今回の監督指針案では改正案が示されていない他の金融機関向けの監督指針については、改正しなくてもすでに趣旨を満たしているということなのか、併せて今回改正する必要性はないのかをあらためて検証することも必要である。 （理由）金融庁が 6 月に公表した「金融分野における IT レジリエンスに関する分析レポート」において、「顧客口座への不正アクセスの事案は、証券業界に限らず、金融業界の信頼を揺るがしかねない問題であり、認証やモニタリングの強化などを含め、迅速な対応が必要である。」とされている。セキュリティ向上の施策の対象は、証券会社だけでなく、銀行等幅広い金融機関が含まれるべきである。	金融商品取引業者以外の金融機関向けの監督指針の改正につきましては、業態毎に改正の必要性等を今後検討してまいります。
132	昨今のサイバーセキュリティレベルやインターネット取引技術の進歩を踏まえ、今後さらにインターネット取引に係る脅威が発生した場合、本改正にあたって各社が対応策を検討し取組んでいる施策が無意味なものとなり、更なる取組みを行う必要が生じた場合、本改正における施策以上の取組みと時間的猶予が必要となることが想定され、各社が各々取組むことに限界が生じる可能性もあることから、将来的には業界全体での共有システムを導入する等の考え方はあるのでしょうか。	インターネット取引サービスを提供する事業者は、顧客や業務の特性、提供するサービスの内容を踏まえながら、その時々のセキュリティ技術水準や犯罪手法等に応じて、不断にセキュリティ対策を見直していくことが重要と考えます。
133	セキュリティ対応は、基本的に脆弱性と脅威をリスクとして想定するものです。したがって、本ガイドラインでも特定のリスクを想定していると考えられます。不正アクセスがリスクであることは明らかですが、各対応項目がどのリスク要素に対処しようとしているのかを明確にしていただきたいです。現状のように対応項目だけを示すと、III-2-8 システムリスク管理態勢にもあるよう「外部環境の変化によりリスクが多様化」した際に、適切な判断ができなくなる可能性があるためです。 また、当社の業務では取り扱っていない項目や、従来の株式や債券とはリスク特性が異なる商品もあります。このような場合でも、「スタンダード」として位置づけられている項目については対応が必要なのでしょうか。	顧客にインターネット取引サービスを提供する事業者においては、各社の顧客や取扱商品、業務の特性等に応じて自らリスク評価を行った上で、適切な態勢整備を講じる責任があると考えます。 また、その時々のセキュリティ技術水準や犯罪手法等に応じて、不断にセキュリティ対策を見直していくことが重要と考えます。

134	本件の改正案では、被害側口座に係る対策のみしか言及されていない。 犯行側口座に係る対策(口座特定、口座凍結、資金回収、被害口座への資金返還)についても改正案に盛り込むべきである。	本改正において、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）、事後検証に資するログイン・取引時の情報の保存及び不正が疑われるアクセスの適時遮断を求めているほか、各社においては、不正なログイン・異常な取引等を検知する体制を整備するなどの不正防止策を講じることが望ましいと考えます。
135	本件の改正案では、被害側口座に係る対策のみしか言及されていない。 「海外の証券会社から日本の証券会社への日本株取引の取次」や「日本の証券会社から海外の証券会社への外国株取引の取次」や「日本の取引所における市場取引や清算」についても、異常な取引を検知したうえで、速やかに当該銘柄の取次や取引／清算を停止し、被害拡大や犯行者への資金流出を防ぐ対策を改正案に盛り込む必要がある。 なお、この点は、顧客保護のみならず、KYC/CFT の観点でも対策を要するものと考えられる。	
136	投資家側が果たすべき責任(投資家自身が果たすべき、自身の取引端末の管理や、フィッシングサイトに闇雲にアクセスしないこと等)についても、今後、金融商品取引法等でしっかりと示し、投資家に義務付けていくべきではないか。 昨今の不正アクセス問題は、投資家側の対応にも問題があるために発生した側面が大きいにも関わらず、その対応の責任を金商業者のみに負わせるだけでは、不正アクセス問題の根本的な解決にはつながらない。 その結果として、証券会社からの被害回復資金が、不正アクセスを受けた投資家を通じて、犯罪者側に流れ続ける構図に陥りかねないことを危惧する。	顧客にインターネット取引サービスを提供する事業者においては、サービスの利用に必要な IT リテラシーについて、顧客の意識向上に努めていくことが重要と考えます。
137	証券会社に求めるものを明確にしてください	本改正においては、インターネット取引における認証方法や不正防止策を強化するために、ログイン時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必須化等を求めております。
138	証券会社に負担を求めすぎないように （フィシング詐欺に遭った責任は各個人のセキュリティ対策の不足にあります。その対応を証券会社に負担させることに疑問です。取引手数料が上がる可能性があると困ります。）	貴重な御意見として承ります。
139	本件の改正案は、「インターネット取引サービスでの不正アクセス・不正取引(第三者による取引)の被害が多発」した主な原因について、顧客側が「証券会社のウ	貴重な御意見として承ります。

	ェブサイトを装ったフィッシングサイト等で顧客情報を窃取された」ことを前提としているが、その前提は誤っている。 　事実として、被害発生後、証券会社側のセキュリティ対策で被害件数／被害金額は激減した訳であり、被害が発生した主な原因は、顧客側の過失ではなく、証券会社側のセキュリティ対策不足（セキュリティ対策の欠陥含む）にあるということを前提とすべきである。	
140	今般、「インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が多発したこと」は、「単に、本邦の証券会社の殆どが顧客保護を軽視し、セキュリティ対策が不足していただけである」という前提認識の下で、監督行政を含め、徹底的な見直しを実施すべきである。 　海外（先進国のみならず新興国を含む）ではこれほどまでの規模での被害は生じていないのだから、「証券会社のウェブサイトを装ったフィッシングサイト等による顧客情報（ログイン ID やパスワード等）の窃取」や「インターネット取引による特有のリスク」に原因を求めるのは、監督行政や証券会社の失策を糊塗しようとしているだけの言い訳に過ぎず、本邦の証券会社に限定されたセキュリティ対策の不足が原因で、犯行の標的になったことは明らかである。	
141	「ID・パスワードは常に盗まれている」「認証後のセッション ID も常に狙われ、盗まれている」という前提に立った防御策が求められるべきだと考えます。また、ゼロトラストの原則に立って適宜検査するにしても、このブラウザという「すでに負けている戦場」では、いくら改良を重ねても、根本的な解決が可能と考えるのには無理があります。 　具体例を挙げると、フィッシング対策に大きな効果があるパスキーを導入しても、認証後のセッション ID は、他の認証手段と同じく盗まれるからです。 具体的な実行策の提案 　日本の金融セキュリティを世界に先駆けるものとするため、具体的なアクションとして、金融庁とデジタル庁が共同で、以下のテーマを掲げた技術アイディアコンテスト（稼働している製品は、まだ世の中にないはずです。あれば被害をすぐさま抑える	

	ことができているはずです）の開催を強く提案いたします。 テーマ案：「マイナンバーカードを活用し、国家レベルのハッキングに対抗できるセキュリティソリューション for 金融取引」 このようなオープンで製品開発のための賞金を提供する場を設けることで、国内外の優れた知見と技術を活かしたアイディアが製品となる可能性があるだけでなく、このアイディアに触発され新たなアイディアが創出され新たな製品として世のなかに出てくる可能性も高まります。マイナンバーカードのような IC カードを国民に配布して利用している国々は、世界中で 100 か国以上ありますので。日本以外でもビジネス展開できる可能性があります。即ち国家レベルのハッキングに対抗する製品によりユニコーン企業が生まれる可能性も出てきます。また、国民に配布する IC ID カードに限定されない（例：米国のCACカード）こともビジネスにおけるポイントです。	