資 料 1

「協会員の情報管理態勢に関するワーキング・グループ」における検討事項

平成 27 年３月４日

１．金融分野における個人情報保護ガイドライン改正対応

大手出版社の個人情報漏えい事件を受け、外部委託先の監督強化や内部管理態勢の強化（監視カメラの設置、入退室管理の強化、スマホ等の利用制限等）を求めるガイドライン改正が検討されている。

WG では、実務に与える影響を検討のうえ、金融庁への意見提出、同ガイドライン改正を踏まえた日証協規則（個人情報保護指針等）の改正等の検討を行う。

（注）自主規制規則の改善等に関する検討ワーキング・グループにおいて事前意見を取りまとめ、金融庁に送付。事務局にて金融庁に確認した。

２．パーソナルデータの活用に関する個人情報保護法改正対応　[別紙]

「個人情報」等の定義を改正のうえ、個人情報保護法が以下のとおり改正される見込みである。

・指紋・携帯番号・顧客管理番号等について、それ単体を個人情報として管理する義務
・ビックデータ（個人を特定できないように加工した大規模データ）活用の制度整備
・「機微情報」を「要配慮個人情報」と改称・範囲整理の上、第三者提供禁止の強化
・「オプトアウト方式」による利用目的の変更の際の手続き強化
・第三者提供の記録・保存義務の強化、域外適用にあたっての整理
・監督権限を消費者庁から「個人情報保護委員会」（内閣に設置する３条委員会）に移管

WG では、法令等の改正案について、実務に与える影響を検討のうえ、内閣官房への意見提出及び当該法令改正を踏まえた日証協規則（個人情報保護指針）改正等の検討を行う。

３．マイナンバーの導入等を踏まえた情報管理

マイナンバー制度が平成 27 年 10 月に交付手続き開始、平成 28 年１月から利用開始される。

マイナンバーも個人情報であることから、関係法令を踏まえ、必要に応じて日証協規則（個人情報保護指針）改正等の必要な検討を行う。

４．情報セキュリティ管理等に係る監督指針・検査マニュアル改正対応（資料３）

預金取扱金融機関における外部委託先社員による不正出金事件や大手出版社の個人情報漏えい事件を踏まえ、情報管理に関する技術的なセキュリティ対応策を求める監督指針の改正がパブリック・コメントに付されている。（２月 13 日～３月 16 日）

WG では、実務に与える影響を検討のうえ、金融庁等への意見提出及び同指針改正を踏まえ、必要に応じて日証協規則（個人情報保護指針等）の改正等の検討を行う。

（注）証券会社情報セキュリティワーキング・グループにおいて事前意見を取りまとめ、金融庁に送付。

現在、会員に対し、本協会から金融庁等に提出するパブリック・コメントの意見を募集中。

以　上

別紙

資料１

パーソナルデータの利活用に関する制度改正に係る法律案の骨子（案）

2014年　12月19日

内閣官房ＩＴ総合戦略室

パーソナルデータ関連制度担当室

１．個人情報の定義の拡充

生存する個人に関する情報であって、次のいずれかに該当する文字、番号、記号その他の符号のうち政令で定めるものが含まれるものを個人情報として新たに位置付けるものとする。

(1) 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した符号であって、当該個人を識別することができるもの（例：指紋データ及び顔認識データ）

(2) 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行される書類に付される符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は付されるもの（例：携帯電話番号、旅券番号及び運転免許証番号）

※現行法の定義：「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

１．個人情報の定義の拡充

個人情報の定義

2．適切な規律の下で個人情報等の有用性を確保するための規定の整備①

(1) 匿名加工情報（仮称）に関する規定の整備

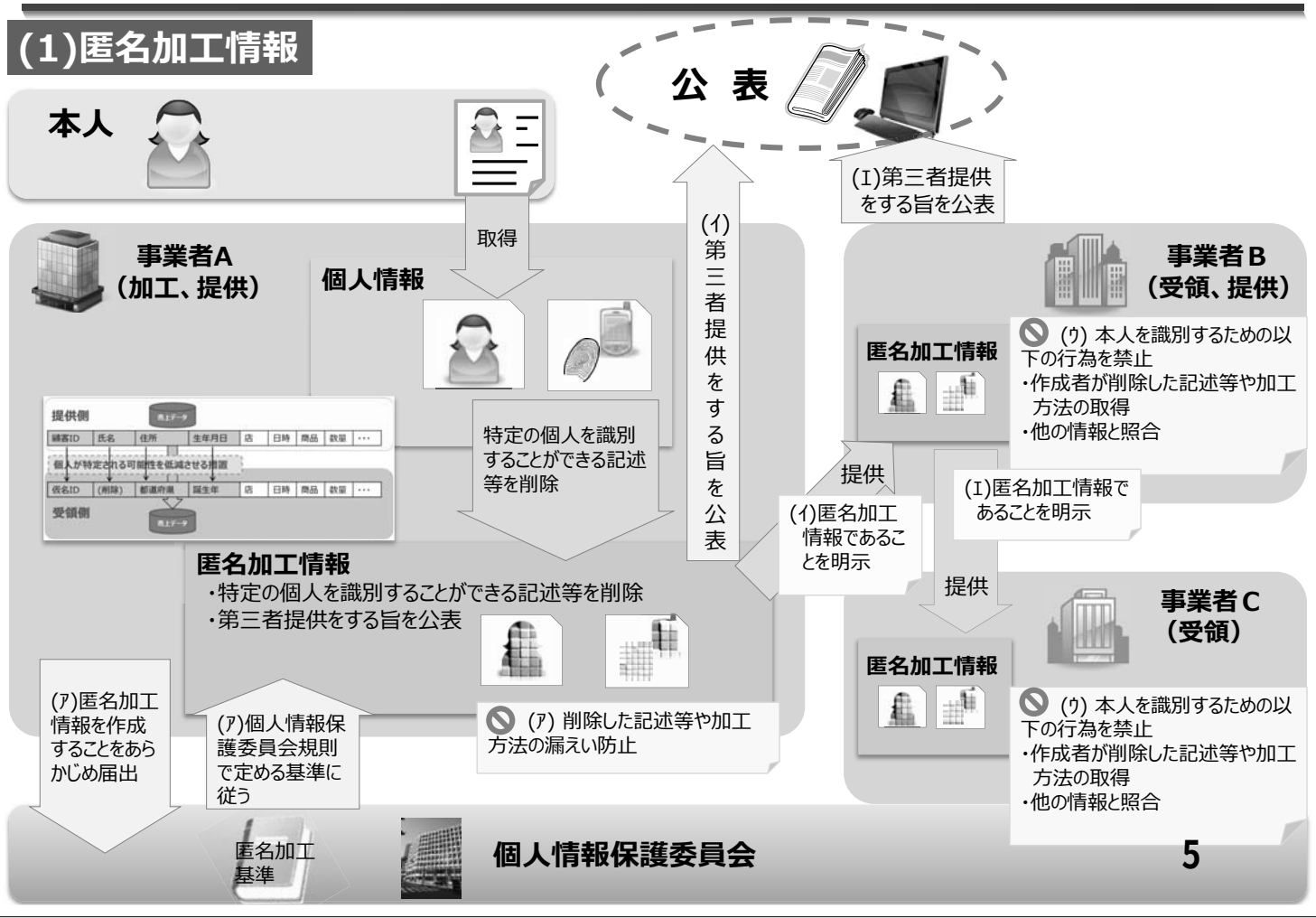
(ｱ) 第三者に提供するために匿名加工情報を作成するときは、４の個人情報保護委員会に届け出た上で、個人情報保護委員会規則で定める基準に従い、個人情報から特定の個人を識別することができる記述等の削除（他の記述等に置き換えることを含む。）をするなど、当該個人情報を復元することができないようにその加工をしなければならないこととする。また、匿名加工情報を作成した者は、削除をした記述等及び加工の方法に関する情報の漏えいを防止するために必要かつ適切な措置を講じなければならないこととする。

(ｲ) (ｱ)により匿名加工情報を作成した者が当該匿名加工情報を第三者に提供する場合には、第三者提供をする旨を公表し、提供先に匿名加工情報であることを明示しなければならないこととする。

(ｳ) (ｲ)により取得した匿名加工情報を事業の用に供する者は、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、(ｱ)の削除をした記述等及び加工の方法に関する情報を取得し、又は当該匿名加工情報を他の情報と照合してはならないこととする（(ｴ)により取得した匿名加工情報を事業の用に供する場合も同様とする）。

(ｴ) (ｲ)により取得した匿名加工情報を第三者に提供する場合には、第三者提供をする旨を公表し、提供先に匿名加工情報であることを明示しなければならないこととする（この(ｴ)により取得した匿名加工情報を第三者に提供する場合も同様とする）。

2．適切な規律の下で個人情報等の有用性を確保するための規定の整備①



2．適切な規律の下で個人情報等の有用性を確保するための規定の整備②

(2) 利用目的の制限の緩和

個人情報取扱事業者は、個人情報を取得する際に本人に利用目的を変更することがある旨を通知し、又は公表した場合において、次の事項を、個人情報保護委員会規則で定めるところにより、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、利用目的の変更をすることができることとする。

(ｱ) 変更後の利用目的
(ｲ) 変更に係る個人情報の項目
(ｳ) 本人の求めに応じて変更後の利用目的による取扱いを停止すること及び本人の求めを受け付ける方法

この場合において、個人情報保護委員会は、その内容を公表しなければならないこととする。
※本人への通知方法や本人が容易に知りうる状態が不適切な場合には、勧告・命令。

(3) 情報の利用方法からみた規制対象の縮小

利用方法からみて個人の権利利益を害するおそれが少ないもの（市販の電話帳等）は、個人情報データベース等の規制から除外する。

2．適切な規律の下で個人情報等の有用性を確保するための規定の整備②

(2)利用目的の制限の緩和

3．個人情報の保護を強化するための規定の整備①

(1) 要配慮個人情報（仮称）に関する規定の整備

本人に対する不当な差別又は偏見が生じないようにその取扱いについて特に配慮を要する記述等（例：本人の人種、信条、社会的身分、病歴、犯罪被害を受けた事実及び前科・前歴）が含まれる個人情報については、本人同意を得ない取得を原則として禁止するとともに、利用目的の制限の緩和及び本人同意を得ない第三者提供の特例の対象から除外する。

(2) 第三者提供に係る確認及び記録の作成の義務付け

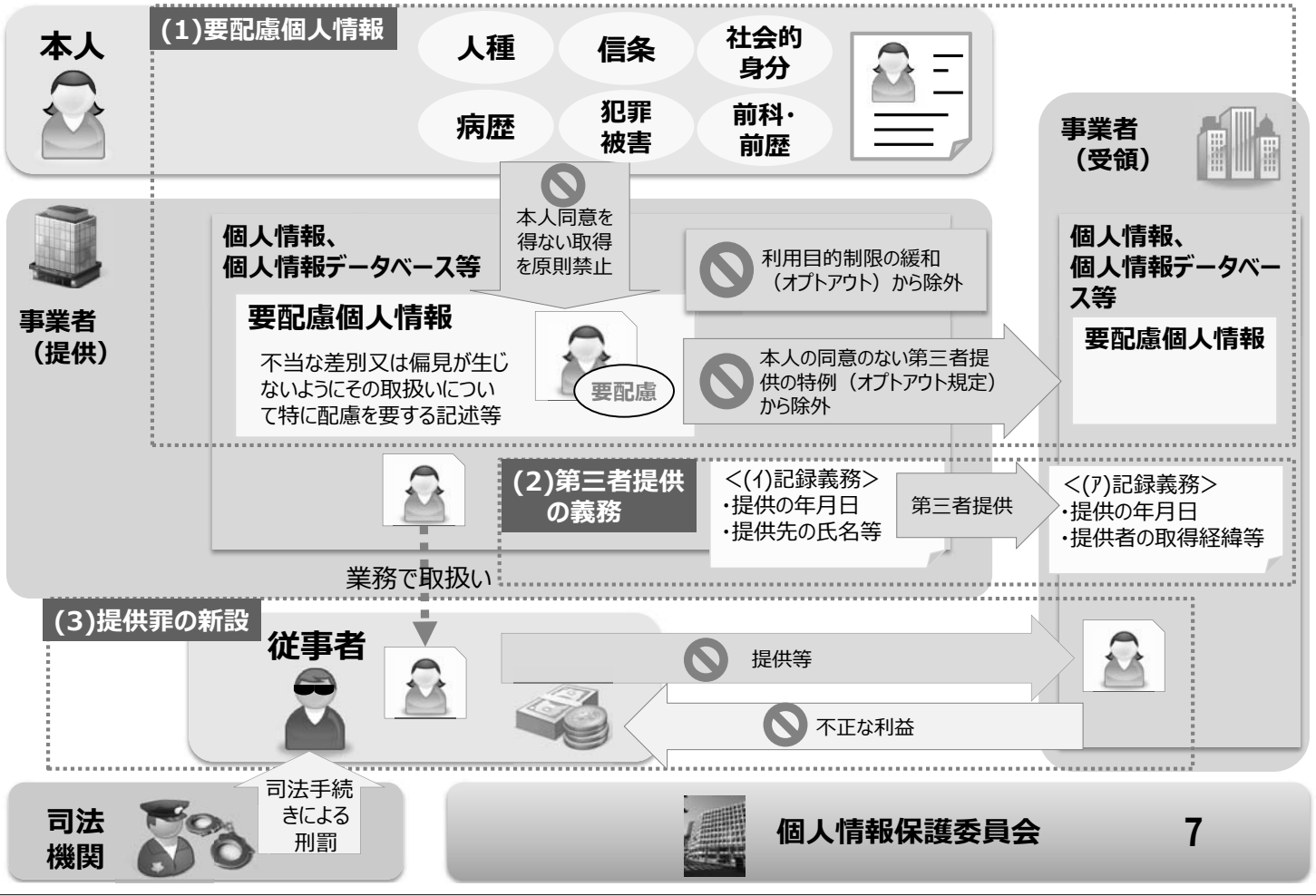
(ｱ) 個人情報取扱事業者は、個人情報データベース等の提供を受けるときは、その提供をする者が当該個人情報データベース等を取得した経緯等を確認するとともに、提供の年月日、当該確認に係る事項等の記録を作成し、一定の期間保存しなければならないこととする。

(ｲ) 個人情報取扱事業者は、個人情報データベース等の第三者提供をしたときは、提供の年月日、提供先の氏名等の記録を作成し、一定の期間保存しなければならないこととする。

(3) 不正な利益を図る目的による個人情報データベース提供罪の新設

個人情報データベース等を取り扱う事務に従事する者又は従事していた者が、その業務に関して取り扱った個人情報データベース等を不正な利益を図る目的で提供し、又は盗用する行為を処罰対象にする。

3．個人情報の保護を強化するための規定の整備①



3．個人情報の保護を強化するための規定の整備②

(4) 本人同意を得ない第三者提供への関与（オプトアウト規定の見直し）

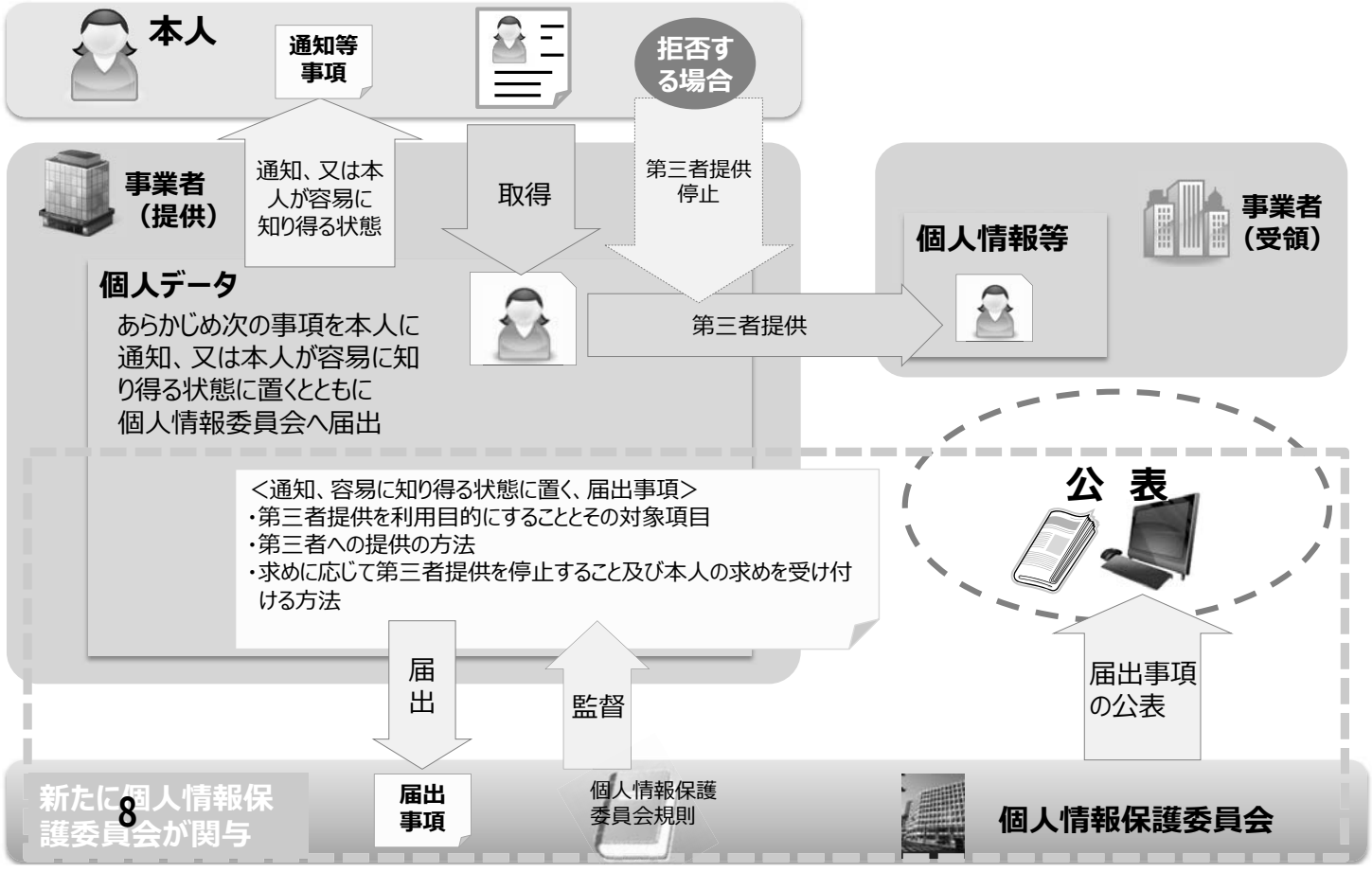
個人情報取扱事業者は、本人同意を得ない個人データの第三者提供をしようとする場合には、次の事項を、個人情報保護委員会規則で定めるところにより、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出なければならないこととする。

(ｱ) 第三者への提供を利用目的とすること
(ｲ) 第三者に提供される個人データの項目
(ｳ) 第三者への提供の方法
(ｴ) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること及び本人の求めを受け付ける方法

この場合において、個人情報保護委員会は、その内容を公表しなければならないこととする。
※本人への通知方法や本人が容易に知りうる状態が不適切な場合には、勧告・命令。

3．個人情報の保護を強化するための規定の整備②

(4)本人同意を得ない第三者提供への関与（オプトアウト規定の見直し）



3．個人情報の保護を強化するための規定の整備③

(5) 小規模事業者への対応

取り扱う個人情報が少量である場合の個人情報取扱事業者からの除外規定を削除する。

(6) 個人情報取扱事業者による努力義務への個人データの消去の追加

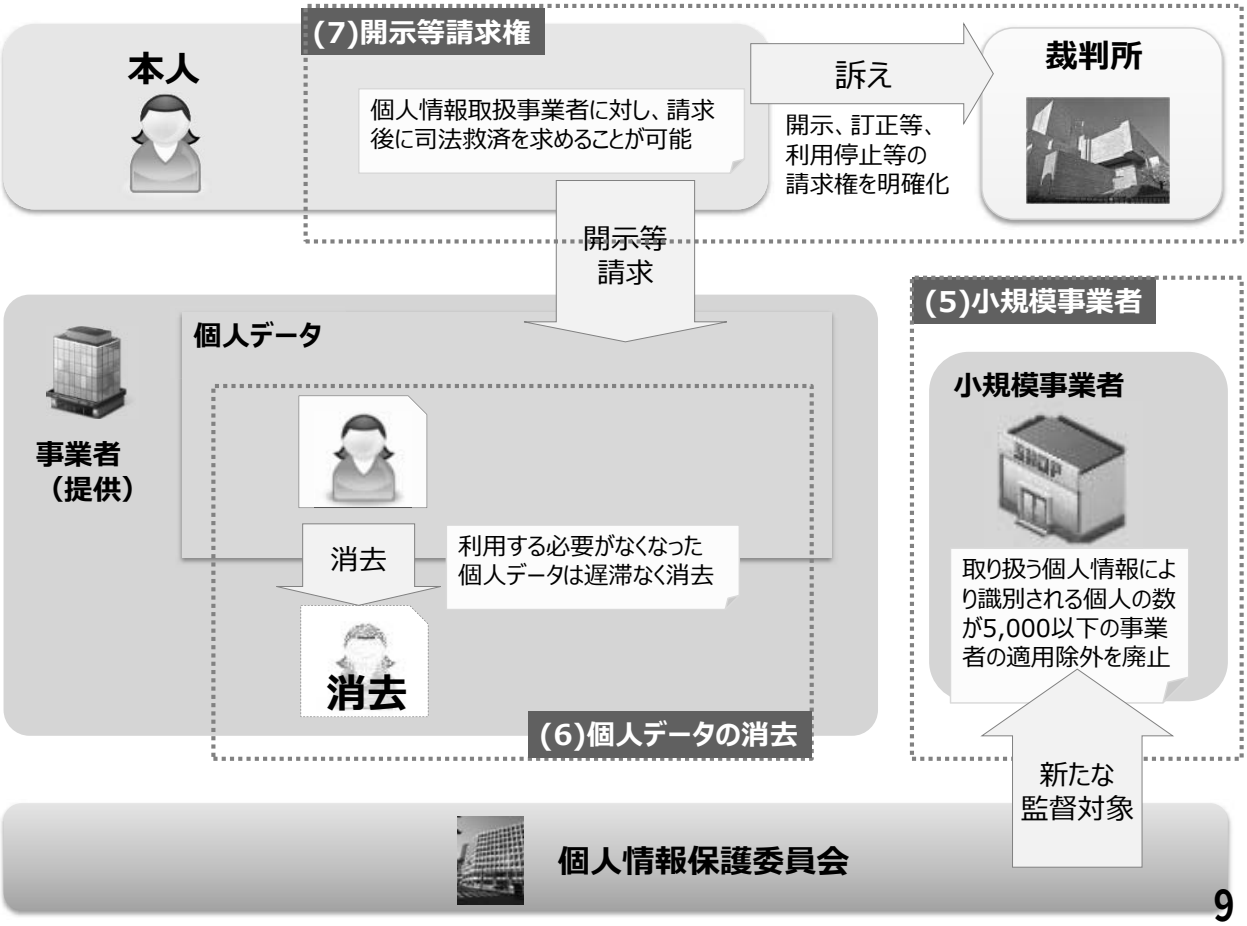
個人情報取扱事業者は、個人データを利用する必要がなくなったときは、遅滞なく当該個人データを消去するよう努めなければならないこととする。

(7) 開示等請求権の明確化

(ｱ) 個人情報の本人が、個人情報取扱事業者に対して開示、訂正等及び利用停止等の請求を行う権利を有することを明確化する。

(ｲ) 開示等の請求に係る訴えを提起する前に、個人情報取扱事業者に対して当該請求をしなければならないこととする。

3．個人情報の保護を強化するための規定の整備③



４．個人情報保護委員会の新設及びその権限に関する規定の整備 14

(1) 個人情報保護委員会の主な権限

(ｱ) 個人情報及び匿名加工情報の取扱いに関する監督等の事務をつかさどる内閣府の外局たる機関として、個人情報保護委員会を設置する（行政手続における特定の個人を識別するための番号の利用等に関する法律の監督機関である特定個人情報保護委員会を改組）。

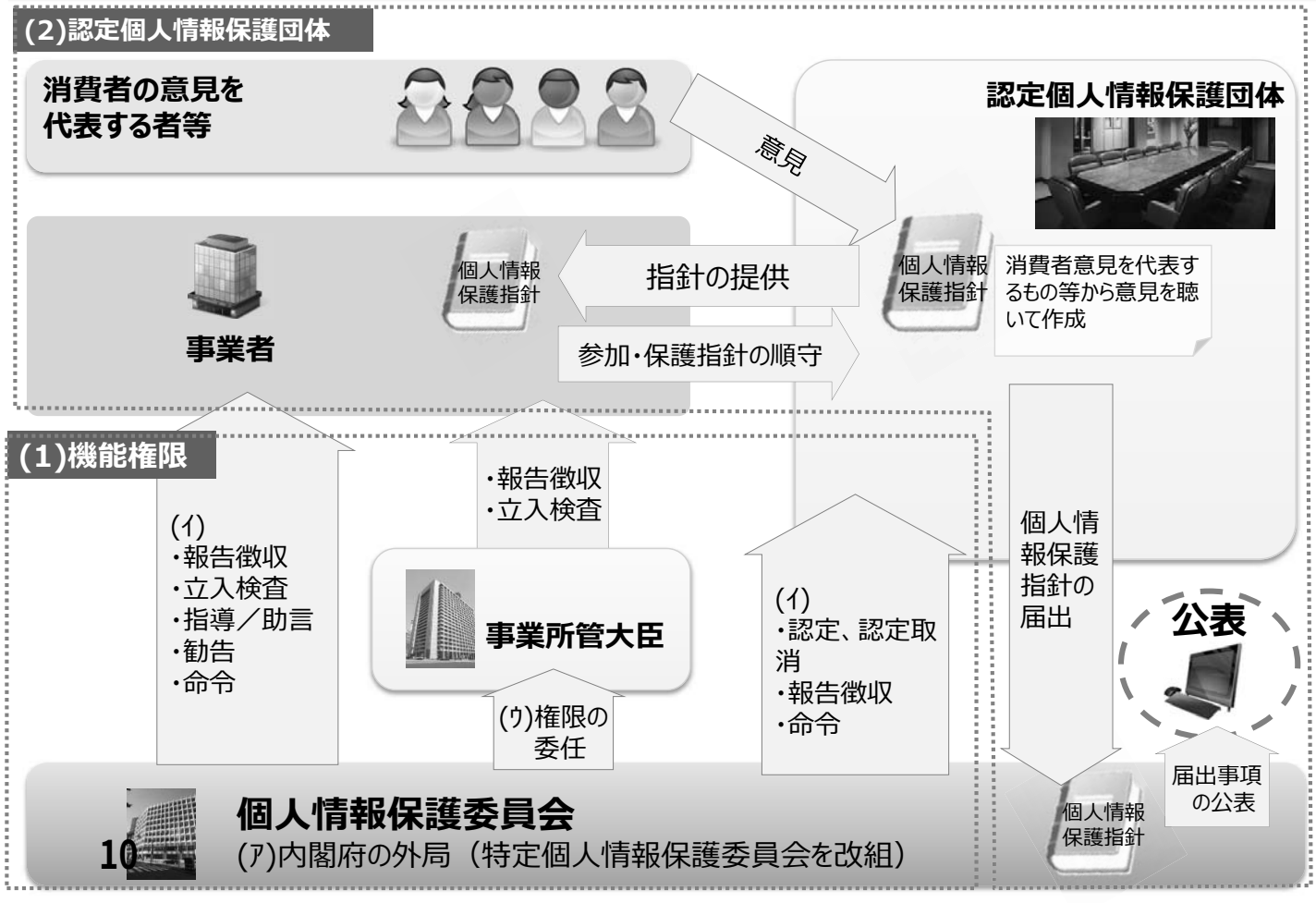
(ｲ) 個人情報保護委員会には現行の主務大臣の有する報告徴収、命令、認定個人情報保護団体の認定等の権限に加えて、立入検査の権限等を付与する。

(ｳ) 個人情報保護委員会は、個人情報取扱事業者等に対する報告徴収及び立入検査の権限を事業所管大臣等に委任することができることとする。

(2) 個人情報保護指針の作成への関与

認定個人情報保護団体が、個人情報保護指針を作成する場合には、消費者の意見を代表する者等の意見を聴くよう努め、個人情報保護委員会に届け出なければならないこととするとともに、個人情報保護委員会は、その個人情報保護指針の変更等を命じることができることとする。また、個人情報保護委員会は、その個人情報保護指針を公表しなければならないこととする。

４．個人情報保護委員会の新設及びその権限に関する規定の整備 15



5．個人情報の取扱いのグローバル化に対応するための規定の整備 16

(1) 国境を越えた個人情報の取扱いに対する適用範囲に関する規定の整備

本法は、国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報を取り扱う場合についても、個人情報保護委員会による命令に関する部分を除いて、適用することとする。

(2) 外国執行当局への情報提供に関する規定の整備

個人情報保護委員会は、本法に相当する外国の法令を執行する外国執行当局に対し、その職務の遂行に資すると認める情報の提供を行うことができることとする。

(3) 個人データの外国にある第三者への提供の制限

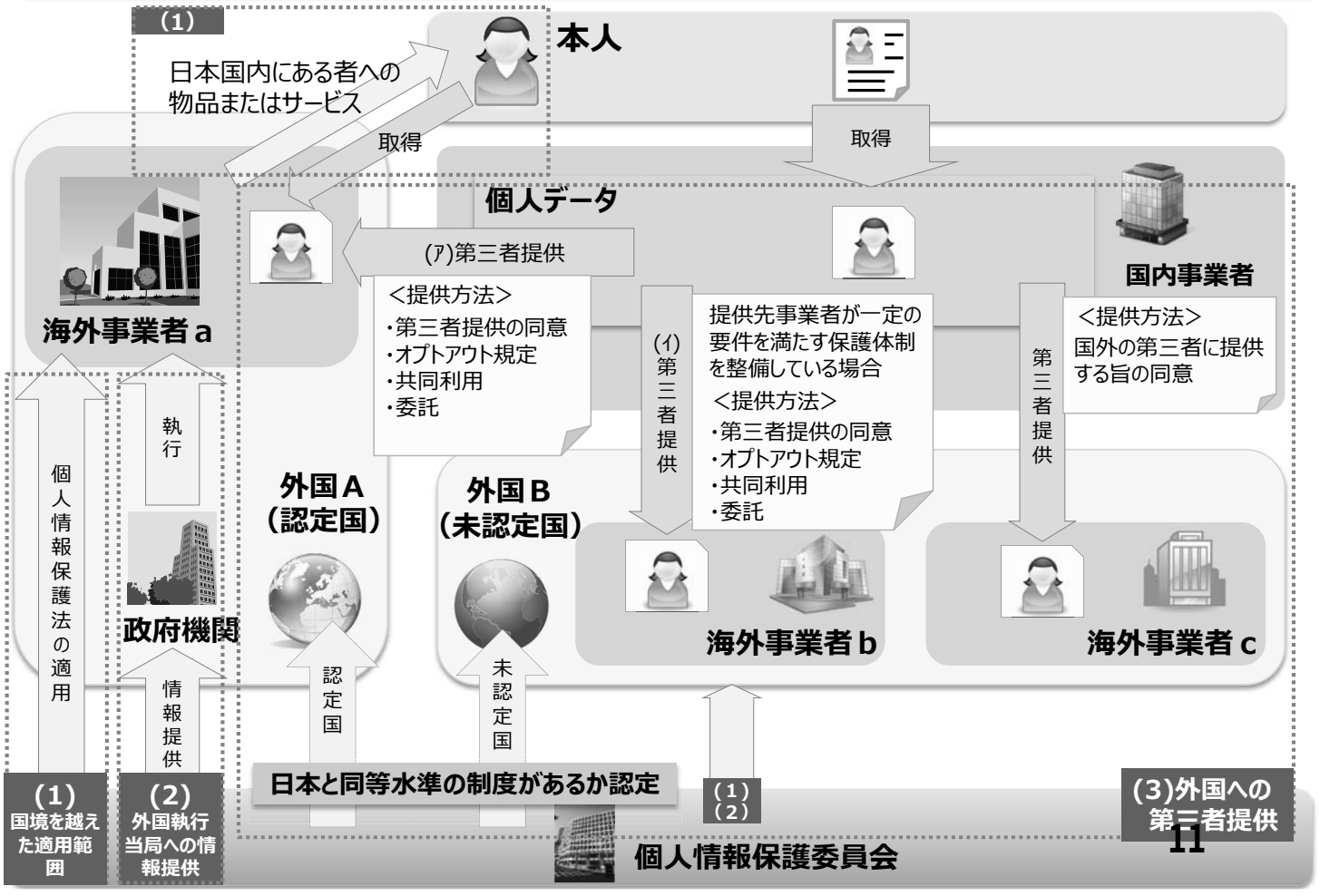
個人情報取扱事業者が個人データを外国にある第三者に提供する場合は、当該提供についての本人同意を得るか、次のいずれかの要件を満たさなければならないこととする。

(ｱ) 我が国と同等の水準にあると認められる個人情報保護の制度を有している国として個人情報保護委員会が定める国にある第三者に提供すること。

(ｲ) 当該第三者が本法の規定により個人情報取扱事業者が講じなければならないとされている措置に相当する措置を継続的に講じるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備していること。

※現行の各企業の適切な移転手続きが合法であることを明確化。

5．個人情報の取扱いのグローバル化に対応するための規定の整備 17



資料３

日本証券業協会
JSDA Japan Securities Dealers Association

日証協（企）26 第 106 号
平成 27 年 2 月 17 日

総務・企画担当者　殿

日本証券業協会
企画部長　松本昌男

「金融商品取引業者等向けの総合的な監督指針」及び「金融商品取引業者等検査マニュアル」の一部改正（案）に対する意見募集について

金融庁では、２月 13 日付けで、同庁ホームページ において、金融商品取引業者等向けの総合的な監督指針の改正案を公表し、意見募集を行っているところであります。

また、証券取引等監視委員会では、同日付けで、同委員会ホームページ において、金融商品取引業者等検査マニュアルの改正案を公表し、意見募集を行っているところであります。

本協会では、会員各社から御意見等をいただき、取りまとめの上、金融庁又は証券取引等監視委員会に提出したいと存じます。

つきましては、これらの改正案につきまして、下記のとおり、会員の皆様の御意見を募集したいと存じます（御意見等については、直接、金融庁又は証券取引等監視委員会に送付していただいても差し支えないことを、念のため申し添えます。）。

意見の提出先が異なることから、同様の意見を金融庁及び証券取引等監視委員会の両方に御提出する場合は、意見内容は同じで構いませんので、それぞれの項目に意見を御記入いただきますようお願いいたします。

なお、本協会から金融庁又は証券取引等監視委員会に提出する意見については、御提出いただいた御意見等のすべてを反映することができない場合もありますので、あらかじめ御了承ください。

記

１．意見募集締切 （本協会経由で意見を御提出される場合）
平成 27 年３月２日（月）まで

２．意見募集する監督指針等
・「金融商品取引業者等向けの総合的な監督指針」（意見の提出先：金融庁）
・「金融商品取引業者等検査マニュアル」（意見の提出先：証券取引等監視委員会）

３．提出先及び提出方法

本協会政策本部企画部あて、電子メール（kikaku@wan.jsda.or.jp）により、件名を「金融商品取引業者等向けの総合的な監督指針案等に対する意見」とし、会員名、連絡先（御担当者の部署名、氏名及び電話番号）、意見等の該当箇所及び理由を別紙様式に記入、御提出願います。

以　　上

○ 本通知に関するお問い合わせ先：政策本部企画部（TEL）03-3667-8535

平成27年2月13日
金融庁

「主要行等向けの総合的な監督指針」及び「金融検査マニュアル」等の一部改正（案）の公表について

金融庁では、「主要行等向けの総合的な監督指針」及び「金融検査マニュアル」等の一部改正（案）を別紙のとおり取りまとめましたので、公表します。

本件の概要は以下のとおりです。

1. 情報セキュリティ管理に係る監督指針等の改正

外部委託先社員等による不正出金事案等の発生を踏まえ、顧客に関する情報の厳格な管理態勢や外部委託先に対する適切な管理態勢の整備状況について、監督上の着眼点として明確化する等、所要の改正を行う。

2. サイバーセキュリティ管理に係る監督指針等の改正

サイバーセキュリティ基本法の全面施行（平成27年１月９日）、世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等を踏まえ、金融機関に求めるサイバーセキュリティ管理態勢の整備状況について、監督上の着眼点として明確化する等、所要の改正を行う。

3. インターネットバンキングに係る監督指針等の改正

インターネットバンキングに係る犯罪手口が高度化・巧妙化していること等を踏まえ、預金取扱金融機関におけるセキュリティ対策や顧客への対応について、監督上の着眼点として明確化する等、所要の改正を行う。

4. システムリスク管理態勢に係る監督指針等の改正

システムリスク管理態勢に関する着眼点・検証項目の拡充を図るため、「金融商品取引業者等向けの総合的な監督指針」「清算・振替機関等向けの総合的な監督指針」「保険検査マニュアル」について、所要の改正を行う。

具体的な内容については（別紙１～15）をご参照ください。

この案について御意見がありましたら、平成27年３月16日（月）17時00分（必着）までに、氏名（法人その他の団体にあっては名称）、職業（法人その他の団体にあっては業種）、連絡先（住所、電話番号又は電子メールアドレス）及び理由を付記の上、郵便、ファックスにより下記送付先に、お寄せください。電話による御意見は御遠慮願います。

インターネットによる御意見は、下記e-Govウェブサイトに、お寄せください。

御意見をお寄せいただいた方の氏名（法人その他の団体にあっては名称）については、開示の請求等があった場合には、御意見の内容とともに開示させていただきますので、御承知おきください。開示の際に匿名を希望される場合は、御意見の冒頭にその旨を明確に御記載ください。なお、開示に当たっては、御意見の内容に、（1）個人に関する情報であって特定の個人が識別され得る記述がある場合、又は（2）法人等の権利、競争上の地位その他正当な利益を侵害するおそれのある記述がある場合、には当該箇所を伏せさせていただくことがあります。

御意見に付記された電話番号等の個人情報は、御意見の内容に不明な点があった際に連絡・確認をさせていただく場合や御意見がどのような立場からのものかを確認させていただく場合に利用します。

なお、御意見に対しての個別の回答はいたしませんので、あらかじめ御了承ください。

インターネットによる御意見はここをクリックしてください。(e-Govへリンク)

御意見の送付先

郵便:〒100－8967
東京都千代田区霞が関３－２－１　中央合同庁舎第７号館
・(監督指針案について)　金融庁監督局総務課システムリスク担当
・(検査マニュアル案について)金融庁検査局審査課調査室
ファックス:
・(監督指針案について)　03-3506-6141
・(検査マニュアル案について)03-3506-6119
URL:http://www.fsa.go.jp/

お問い合わせ先

金融庁　Tel　03-3506-6000(代表)
・(監督指針案について)　監督局総務課(内線3853、2581)
・(検査マニュアル案について)検査局審査課(内線2592)

1. 監督指針等の改正

(別紙1)「主要行等向けの総合的な監督指針」の一部改正(新旧対照表)(PDF:150KB)

(別紙2)「中小・地域金融機関向けの総合的な監督指針」の一部改正(新旧対照表)(PDF:147KB)

(別紙3)「保険会社向けの総合的な監督指針」の一部改正(新旧対照表)(PDF:119KB)

(別紙4)「金融商品取引業者等向けの総合的な監督指針」の一部改正(新旧対照表)(PDF:122KB)

(別紙5)「信用格付業者向けの監督指針」の一部改正(新旧対照表)(PDF:32KB)

(別紙6)「貸金業者向けの総合的な監督指針」の一部改正(新旧対照表)(PDF:133KB)

(別紙7)「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)」の一部改正(新旧対照表)(PDF:170KB)

(別紙8)「事務ガイドライン(第三分冊:金融会社関係　12　電子債権記録機関関係)」の一部改正(新旧対照表)(PDF:109KB)

(別紙9)「事務ガイドライン(第三分冊:金融会社関係　13　指定信用情報機関関係)」の一部改正(新旧対照表)(PDF:111KB)

(別紙10)「事務ガイドライン(第三分冊:金融会社関係　14　資金移動業者関係)」の一部改正(新旧対照表)(PDF:170KB)

（別紙11）「清算・振替機関等向けの総合的な監督指針」の一部改正（新旧対照表）（PDF：360KB）

（別紙12）「系統金融機関向けの総合的な監督指針」の一部改正（新旧対照表）（PDF：194KB）

（別紙13）「漁協系統信用事業における総合的な監督指針」の一部改正（新旧対照表）（PDF：199KB）

2．検査マニュアルの改正

（別紙14）「金融検査マニュアル」の一部改定（新旧対照表）（PDF：231KB）

（別紙15）「保険検査マニュアル」の一部改定（新旧対照表）（PDF：346KB）

金融商品取引業者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－２－８　システムリスク管理態勢 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、システムの不備等に伴い顧客や金融商品取引業者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金融商品取引業者が損失を被るリスクをいうが、金融商品取引業者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、金融商品取引業者の情報システムは一段と高度化・複雑化し、更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や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、金融商品市場及び金融商品取引業者に対する信頼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。 （１）主な着眼点 システムリスク管理態勢の検証については、金融商品取引業者の業容に応じて、例えば以下の点に留意して検証することとする（着眼点の詳細については、必要に応じて証券検査マニュアルを参照。）。 ①　システムリスクに対する認識等 イ．　（略） （新設） （新設） ロ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。	**【本編】** Ⅲ－２－８　システムリスク管理態勢 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、システムの不備等に伴い顧客や金融商品取引業者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金融商品取引業者が損失を被るリスクをいうが、金融商品取引業者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、金融商品取引業者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や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、金融商品市場及び金融商品取引業者に対する信頼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。 （１）主な着眼点 システムリスク管理態勢の検証については、金融商品取引業者の業容に応じて、例えば以下の点に留意して検証することとする（着眼点の詳細については、必要に応じて金融商品取引業者等検査マニュアルを参照。）。 ①　システムリスクに対する認識等 イ．　（略） ロ．取締役会等は、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。 （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。 ハ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
②　（略）	②　（略）
（新設）	③　システムリスク評価 　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。
（新設）	④　情報セキュリティ管理 イ．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。 ロ．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。 ハ．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。 ニ．金融商品取引業者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 ホ．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

現　　行	改　正　後
（新設）	・記録媒体等の取扱いルール　等 ヘ．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 ト．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、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。 チ．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。 リ．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。 ヌ．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。 ⑤　サイバーセキュリティ管理 イ．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。 ロ．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 ハ．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

現　　行	改　正　後
	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） ニ．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 ホ．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。 ヘ．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。 ト．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。 ・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　等 （注）不正アクセスによる顧客口座からの不正出金を防止するための措置を講じている場合（例えば、振込先金融機関口座（出金先口座）の指定・変更手続きにおいて、顧客口座と名義が異なる出金先口座への指定・変更を認めないこととし、更に転送不要郵便により顧客の住所地に口座指定・変更手続きのための書面を送付す

現　　行	改　正　後
（新設）	るなどにより、顧客口座と名義が異なる出金先口座への振込みを防止する措置を講じている場合）は、取引のリスクに見合った対応がなされているものと考えられる。 チ．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。 ・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商品取引業者側で検知し、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 リ．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。 ヌ．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　システム企画・開発・運用管理 イ．経営戦略の一環としてシステム戦略方針を明確にした上で、中長期の開発計画を策定しているか。また、中長期の開発計画は、取締役会の承認を受けているか。 ロ．現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行っているか。 ハ．開発案件の企画・開発・移行の承認ルールが明確になっているか。 ニ．開発プロジェクトごとに責任者を定め、開発計画に基づき進捗管理されているか。 ホ．システム開発に当たっては、テスト計画を作成し、ユーザー部門も参加するなど、適切かつ十分にテストを行っているか。 ヘ．人材育成については、現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施しているか。

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
③　システム監査	⑦　システム監査
イ．システム部門から独立した内部監査部門において、システムに精通した監査要員による定期的なシステム監査が行われているか。	イ．システム部門から独立した内部監査部門において、定期的なシステム監査が行われているか。
（新設）	ロ．システム関係に精通した要員による内部監査や、システム監査人等による外部監査の活用を行っているか。
ロ．監査の対象はシステムリスクに関する業務全体をカバーしているか。	ハ．監査の対象はシステムリスクに関する業務全体をカバーしているか。
④　安全対策の整備	（削除）
イ．安全対策の基本方針が策定されているか。	
ロ．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。	
⑤　外部委託管理	⑧　外部委託管理
（新設）	イ．外部委託先（システム子会社を含む。）の選定に当たり、選定基準に基づき評価、検討の上、選定しているか。
（新設）	ロ．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、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。
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。	ハ．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。 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。
（新設）	ニ．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。
⑥　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
イ．　（略）	イ．　（略）
ロ．コンティンジェンシープランは、自社の業務の実態やシステム環境等に応じて常時見直され、実効性が維持される態勢となっているか。	ロ．コンティンジェンシープランの策定に当たっては、その内容について客観的な水準が判断できるもの（例えば「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
	書」（公益財団法人金融情報システムセンター編））を根拠としているか。
（新設）	ハ．コンティンジェンシープランの策定に当たっては、災害による緊急事態を想定するだけではなく、金融商品取引業者の内部又は外部に起因するシステム障害等も想定しているか。 　また、バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定しているか。
（新設）	ニ．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。
（新設）	ホ．コンティンジェンシープランに基づく訓練は、全社レベルで行い、外部委託先等と合同で、定期的に実施しているか。
（新設）	ヘ．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。
⑦　システム統合リスク イ．～ホ．　（略）	⑩　システム統合リスク イ．～ホ．　（略）
⑧　障害発生時の対応 イ．障害発生時に、顧客に無用の混乱を生じさせないための適切な措置を講じているか。	⑪　障害発生時の対応 イ．システム障害等が発生した場合に、顧客に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。 　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。
（新設）	ロ．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。
（新設）	ハ．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

現　　行	改　正　後
ロ．発生した障害について、原因を分析し、それに応じた再発防止策を講じているか。	か。 ニ．発生したシステム障害等について、原因を分析し、それに応じた再発防止策を講じているか。 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。
ハ．障害発生時、速やかに当局に報告する体制が整備されているか。	ホ．システム障害等が発生した場合、速やかに当局に報告する体制が整備されているか。
（２）監督手法・対応 ①・②　（略）	（２）監督手法・対応 ①・②　（略）
（３）システム障害時における対応 ①　コンピュータシステムの障害の発生を認識次第、直ちに、その事実の当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式Ⅲ－１）にて当局あ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ヵ月以内に現状について報告を行うこと。）。 なお、財務局は金融商品取引業者から報告があった場合は直ちに金融庁担当課室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、金融商品取引業者又は金融商品取引業者から業務の委託を受けた者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、金融商品取引、決済、入出金、資金繰り、財務状況把握、その他顧客利便等に影響があるもの又はそのおそれがあるもの。 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・機器が速やかに代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、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く。 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	（３）障害発生時 ①　システム障害等の発生を認識次第、直ちに、その事実の当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式Ⅲ－１）にて当局あ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ヵ月以内に現状について報告を行うこと。）。 なお、財務局は金融商品取引業者から報告があった場合は直ちに金融庁担当課室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、金融商品取引業者又は金融商品取引業者から業務の委託を受けた者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、金融商品取引、決済、入出金、資金繰り、財務状況把握、その他顧客利便等に影響があるもの又はそのおそれがあるもの。 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・機器が速やかに代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、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く。 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

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
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。 ②　（略）	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。 ②　（略）