オープンAPIにおけるセキュリティ対策及び利用者保護に関する基本的な考え方
【 中間的な整理(案) 】

2017年1月20日
オープンAPIのあり方に関する検討会

2017 年 1 月 20 日
オープン API のあり方に関する検討会
（事務局：一般社団法人全国銀行協会）

オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方

※ なお、セキュリティ原則及び利用者保護原則は、現時点の関係法令に基づいて整理したものであり、関係法令の改正等が行われた場合には当該法令に準拠した対応等が必要になることに留意すること。

Ⅰ. 背景

- 近年、金融機関と FinTech 企業等との連携を通じた金融サービスの高度化に向けたツールとして、銀行システムへの接続仕様を他の事業者等に公開する“オープン API[1]”への注目が高まっている。わが国銀行界においても、現在、多数の銀行がオープン API の活用可能性について検討を開始しているところ。
- 諸外国においては、英国“Open Banking Standard”をはじめ、API 仕様の標準化に関する検討、API の活用を促進していく上での課題への対応、利用者保護を図りつつオープン API を推進していくために必要な法整備について、官民連携した取組みが進展している。
- こうした状況を踏まえ、当検討会は、わが国金融サービスの高度化、利用者利便の向上等を実現するためのオープン API 活用促進に向けた、官民連携のイニシアティブの一環として、銀行分野のオープン API（バンキング API）におけるセキュリティ対策及び利用者保護に関する基本的な考え方を取り纏めた。
- 本文書に記載した原則は、銀行界、IT 事業者、FinTech 企業、学者、弁護士、消費者団体、金融庁等の幅広い関係者をメンバーとして議論した結果としての「規範」と位置付けられるものであり、当検討会は、オープン API に取り組む関係者において本原則が十分に尊重されることを期待する。

Ⅱ. 基本的な考え方

- IT の進展が金融業のあり方を大きく変容させていくことが見込まれる中で、オープン・イノベーションは、今後の金融機関における基本的な戦略の一つである。
- オープン API は、他の事業者等とのオープンネットワーク上でのセキュアなデータ連携を可能とする技術であるが、単なるデータ連携上の意義

[1] 明確な定義はないが、一般に API（Application Programming Interface）とは、「あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様等」を指し、このうち、サードパーティ（他の企業等）からアクセス可能な API が「オープン API」と呼ばれている。

を超えて、他の事業者等と金融機関が協働して、それぞれの保有する情報やサービスを組み合わせ、あるいはお互いに知恵を絞り、オープン・イノベーションを実現していくためのキー・テクノロジーの一つと位置づけられる。

- 金融分野におけるオープン API の活用は、現在、世界的にみても初期的な段階にあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者保護は、オープン API を活用したサービスに対する利用者の信頼を確保し、オープン API の普及、活用促進・円滑化を図る上で、重要な論点である。
- オープン API では、利用者からの申請・同意に基づいて行われるとはいえ、銀行が保有する秘匿性の高い顧客情報が FinTech 企業等の他の事業者等（以下、「API 接続先」）に提供され当該 API 接続先において蓄積・保存されるほか、銀行が決済指図等を利用者ではなく API 接続先を経由して受け取ることになる。それゆえ、オープン API に取り組むにあたっては、関係者において十分なセキュリティ対策、利用者保護が図られることが必要となる。
- 他方、API 接続先に対して、銀行と同水準のセキュリティ対策、利用者保護策を徒に求めれば、API 接続先と銀行の協働・連携による利便性の高い革新的なサービスの提供や金融サービスの高度化、イノベーションに向けた取組みが阻害され、利用者がテクノロジーの進展の恩恵を受ける機会を失うおそれがある。
- こうした認識の下、当検討会では、API の機能[2]や連携するデータの種類・秘匿性等に応じたリスクベース・アプローチに基づいて、利用者利便と利用者保護のバランスを踏まえた、銀行分野のオープン API（バンキング API）におけるセキュリティ対策及び利用者保護に関する基本的な考え方を取り纏めた。
- 取り纏めにあたっては、イノベーションを阻害しないよう留意するとともに、銀行、API 接続先双方に対して対応水準の目安を示すことで、銀行による API 接続先に対する過度に保守的なセキュリティ対策の要求や、セキュリティ上の懸念から生じる銀行側のオープン API への取組みに対する躊躇といった課題を解消し、銀行と FinTech 企業等の協調・連携の円滑化に資するものとすることを意識した。
- なお、上述の通り、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、さまざまなビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本文書では、様々なビジネスモデルやサービスに共通すると思われる主なリスクに対応したセキュリティ対策及び利用者保護策に焦点をあてて取り纏めている。
- 具体的なセキュリティ対策及び利用者保護策については、各銀行のポリシーや、個別のビジネス、各サービスのリスク、API 接続先の態様等に応じて個々に判断されるものであり、利用者保護の観点から、関係当事者において本文書の趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本文書では挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。
- 以下では、オープン API において想定される主なリスクを整理した上で、セキュリティ原則及び利用者保護原則を示す[3、4]。

---

[2] 例えば、更新系 API において、決済指図上限が定められていない場合、不正送金によって利用者に大きな損害が生じる可能性がある。

[3] 以下では、API 接続先が銀行の銀行代理業者又は外部委託先に該当しない場合について記載。銀行代理業者又は外部委託先に該当する場合は、銀行法に基づく利

Ⅲ．オープン API の主なリスク

・　オープン API では、金融機関のシステムに新たな通信路を設けて他の企業等を経由した新たなサービスを利用者（預金者）に提供することになるため、当該通信路を悪用したデータの漏洩・改竄や不正取引等が生じるリスクがある。これらオープン API において想定される主なリスクを列挙すれば、以下の通り。

１．セキュリティ上の脅威とリスク

(1) API 接続先への外部からの不正アクセスに起因して生じるリスク

・　API 接続先のログイン ID／パスワード等が何らかの原因で漏洩し、第三者によって、API 接続先が不正にアクセスされるリスク
・　API 接続先のシステムが第三者から攻撃を受けて、API 接続先のサービス機能の停止や、API 接続先からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

(2) 銀行への外部からの不正アクセスに起因して生じるリスク

・　トークン[5]の発行を管理する銀行側の API 連携システムが第三者によって不正に認証され、トークンが不正に取得されるリスク
・　トークンの流出や偽造等により、銀行からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

(3) 銀行、API 接続先、利用者の間の通信に起因して生じるリスク

・　ルータ等の通信経路へのハッキング、無線通信等の傍受等により、情報流出、情報改竄／消失、不正送金等が発生するリスク
・　API 接続先のプログラム不備等により、銀行のシステムがダウンするリスク
・　銀行のオープン API の通信路に不必要に大量のデータが送信され、銀行側システムの負荷が増加し、他の銀行サービスにも影響が生じるリスク

(4) 内部の役職員の不正により生じるリスク

・　内部の役職員が、利用者の情報を不正に利用（転売、私的利用を含む）するリスク

用者保護規定が適用されることに留意。

[4] なお、セキュリティ原則及び利用者保護原則の各規定の語尾の趣旨は以下の通り。
- 「しなければならない」： 社会規範として強く求められる対応を意味する。
- 「必要である」： 銀行及び API 接続先がオープン API を活用するにあたってのベストプラクティスとして期待される対応を意味する。
- 「努めなければならない」： その状態になるよう努力が期待される対応を意味する。
- 「考えられる」： 銀行又は API 接続先が任意に選択可能な対応を意味する。
- 「期待される」： 対象となる機関や団体に対する当検討会の期待を意味する。

[5] OAuth2.0 において、銀行と他の企業等のアプリケーションを連携するための認証情報を保持した「許可証」。（以下同じ）

・　内部の役職員が、トークンを不正に使用して、口座残高情報の不正取得や不正決済指図を行うリスク

２．API 接続先のサービスに関連する利用者保護上のリスク

(1) API 接続先に起因するリスク

・　API 接続先の事業内容や社会的信用に疑義があり、API を利用したサービスによって、利用者に被害や混乱が生じるリスク
・　API 接続先の利用者保護態勢、経済的信用、資力等に疑義があり、利用者が十分な保護を受けられないリスク
・　API 接続先が利用者との緊急時の連絡方法を有しておらず、十分な顧客保護対応ができないリスク

(2) インターネットを利用した取引特有のリスク

・　利用者が、誰に何の権限を与えているのか、それにどのようなリスクがあるのか、API 接続先に取得される情報の利用目的は何かなどについて、十分に理解しないまま、API を活用したサービスを利用するリスク
・　トラブルが発生した場合に、利用者がどこに問い合わせたら良いかわからなくなるリスク
・　十分な説明、表示を尽くしても、利用者がよく読まずに手続きを行うリスク

(3) 銀行又は API 接続先のシステムに起因するリスク

・　API 接続先のシステムにおいて不具合、バグ等が発生し、銀行から提供された情報が正しく表示されないリスク
・　API 接続先と銀行間の通信経路に起因する障害により、利用者・API 接続先と銀行の間に取引の齟齬が発生するリスク

Ⅳ．セキュリティ原則

(1) API 接続先の適格性

（事前審査）

・　銀行は、他の事業者等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である[6]。
・　セキュリティに関連した適格性の審査にあたっては、少なくとも以下の点について API 接続先に確認することが必要である[7]。
　- セキュリティ原則の充足状況
　- 過去に発生したセキュリティ関連の不祥事案と改善状況

[6] 情報セキュリティ以外の適格性については、「Ⅴ.利用者保護原則」の「(1)API 接続先の適格性」を参照。
[7] API 接続先が ASP やクラウドサービスを利用している場合には、API 接続先から必要な開示が行われる必要があることに留意する。

- 利用者の属性や取引のリスクに応じた、継続的なセキュリティ対策の高度化に向けた態勢やリソースの有無

・ 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。

・ なお、API 接続先が任意に定めたセキュリティポリシーやセキュリティ関連文書、API 接続先が取得した情報セキュリティ関連の認証（ISO27001、TRUSTe、等）は、上記の適格性の審査にあたっての参考になると考えられる。

・ 複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される[8]。

・ なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や、銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる[9]。

（モニタリング）

・ 銀行は、API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的に又は必要に応じて確認することが必要である[10]。

・ モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、個別に判断されると考えられる。

・ 銀行は、API 接続にあたって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、必要に応じた立入検査等、情報セキュリティ対策の大幅な変更を行う場合の対応、等）を予め取り決めておくことが必要である。

・ 銀行は、API 接続先の情報セキュリティに関連した適格性に懸念があると判断した場合には、API 接続先に対して改善を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[11]。

・ なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる[12]。

---

[8] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。

[9] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

[10] API 接続先が定期的な情報セキュリティ関連の外部監査を受けている場合には、それらの結果を活用すること等も考えられる。

[11] 但し、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。

[12] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

(2) 外部からの不正アクセス対策

・ 以下は、アクセス権限の認可に OAuth2.0[13]、認証プロトコルに OpenID Connect1.0[14]を実装するシステムを前提とした記載。なお、同等の又はより強固な認可・認証が可能な他のプロトコル（新たなテクノロジーを含む）の採用を妨げるものではない[15]。

（アクセス権限の付与に係る認証）

・ 銀行は、公表情報又は匿名加工情報を提供する場合を除き、API 接続先に対するアクセス権限の付与（OAuth2.0 においては「認可」と呼ばれる）を利用者の申請に基づき行うこととし、その際、利用者の本人認証を行わなければならない。

・ 認証方式は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度とすることが必要である[16]。例えば、決済指図の権限を付与する場合には、残高・入出金明細を取得する権限を付与する場合と比較してより強固な認証方式とする等。

・ 認証方式の選択にあたっては、当該銀行において採用されている他のオープンネットワークを利用した取引チャネル（例：インターネット・バンキング）の認証方式の水準が一つの目安となり得るが、以下の点にも留意が必要である。
  - 個々の取引に係る認証ではなく、アクセス権限の認可に係る認証であること
  - API を通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不正アクセスリスクに応じた認証強度とする必要があること

・ 当該銀行において採用されている他のオープンネットワークを利用した取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には（例：インターネット・バンキング契約のない利用者を対象として暗証番号認証を許容する場合等）、不正アクセスリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。例えば、店頭手続・郵送確認等を併用する、資金移動上限を少額に制限する、トークンの有効期限を短期とする、不正使用発生時の補償を予め定める、等。

・ その他の留意点については、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-8／Ⅱ-3-5：インターネット・バンキング）や「預金等受入金融機関に係る検査マニュアル」（別紙２-Ⅲ-1-(5)インターネットを利用した取引の管理）、金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準」、全銀協の「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」等を参考にすることが考えられる。

（アクセス権限／トークンの管理）

・ 銀行は、API 接続先に付与するアクセス権限（OAuth2.0 においては「トークン」が発行される）の管理について、以下の点に留意することが必要である。

---

[13] アクセス権限の認可を行うためのシステムフローに関する規格。一般向けに公開されており、API 開発者は誰でも参照することが可能。IETF（Internet Engineering Task Force：インターネットで利用される技術の標準化を策定する組織）が管理・運営。
[14] 複数の API 接続先を利用する場合に、１つの ID で認証を実現できるようにする仕組みのこと。
[15] 仕様の標準化に関連する論点については、本年度内を目途とする報告書の取り纏めまでに考え方を整理する予定。
[16] 各銀行の判断に基づき、利用者保護の観点から、強固な認証方式を一律に採用することも妨げない。

- 付与するアクセス権限は、API 接続先が提供するサービスに必要な範囲に限定すること
  （利用者からの申請／同意があったとしても、不必要なアクセス権限を API 接続先に付与しないこと）
- API 接続先に発行するトークンには、利用者属性やアクセス権限の内容とそのリスク、利用者の利便性等を踏まえた適切な有効期限を設定すること
- トークンには暗号化や接続元の制限等の十分な強度の偽造・盗用対策を講じること
- 不正アクセス等を検知、または発生した場合に速やかにアクセス権限の制限、停止、取消が可能な仕組みとすること

・ 銀行は、アクセス権限やトークンを管理するシステムに堅牢なセキュリティ対策を講じなければならない。また、API 接続先に対しても、トークンの適切な管理とセキュリティ対策を求めなければならない。

（個々の取引に係る認証）

・ 利用者からの個々の取引指図（残高・入出金明細取得指図、決済指図、等）は、利用者が API 接続先のシステムにアクセスする際に API 接続先において行われる認証[17]と、銀行が個々の取引指図を API 接続先から受け付ける際に銀行において行われる認証の、二段階の認証を経て処理される。

・ 利用者保護や不正アクセス／情報流出防止の観点からは、上記いずれの認証方式とも、利用者の口座保有銀行において採用されている他のオープンネットワークを利用した取引チャネルにおける個々の取引に係る指図の認証方式と同水準以上の強度とすることが原則であると考えられる。

・ 例えば、法人利用者の口座保有銀行のインターネット・バンキングにおいて残高・入出金明細の確認に可変式パスワードや電子証明書等の固定式の ID・パスワードのみに頼らない認証方式が採用されている場合、API 接続先、銀行の双方において同水準以上の強度の認証方式を採用することが原則となる[18]。

・ 他方で、強固な認証方式の中には利用者に手続負担が大きいものや API 接続先の対応に大きな投資が必要なものもあるため、原則的な考え方を一律に適用すれば、利用者利便の大幅な低下や、利便性の高いサービスのフィージビリティが確保できなくなるおそれがあると考えられる。

・ このため、他の利用者保護策や不正アクセス／情報流出対策を組み合わせることで、利用者利便を確保しつつ、個人・法人等の利用者の属性や認証する取引のリスク等に見合った利用者保護の徹底を図っていくことも考えられる。組み合わせる他の利用者保護策や不正アクセス／情報流出対策としては、例えば以下の対策が考えられる。

（例）・ 資金移動指図に係る銀行側の認証方式をトークン認証に加えて帯域外認証も組合せ、その都度利用者を銀行側で直接認証する
・ 生体認証や端末認証、複数経路認証等、一定の認証強度を確保しつつ、利便性が確保される認証方式を採用する
・ 資金移動が行われた場合には、銀行又は API 接続先から利用者に対して電子メール等で通知する

---

[17] 但し、API 接続先が NFC（Near field radio communication：近距離無線通信）技術を用いた物理媒体による決済サービスを提供する場合等については、API 接続先における個々の取引に係る認証は、物理媒体の所持・使用を以て行われることがある。

[18] 逆に、例えば、API 接続先の認証強度がインターネット・バンキング等と比較して劣後する場合、認証強度が脆弱な API 接続先が集中的に狙われて情報流出等が発生するリスクが高まることになる。

- 利用者がアクセス可能な端末をセキュリティが確保された特定の端末や特定の種類の端末に限定する
- 利用者と API 接続先間又は API 接続先と銀行間あるいはその両方の通信方式を閉域ネットワークとする
- トークンの有効期限を短期に設定する（例えば、１回限りとする、１ヵ月から数カ月で失効させる等）
- 提供する情報の範囲や期間を制限する
- 資金移動上限を少額に制限する（例えば、１回あたりの資金移動上限を X 円、かつ簡易な認証方式に基づく資金移動の累積上限を Y 円とする）
- 資金移動先口座を強固な認証手続によって登録された口座に限定する
- 資金移動先口座を同一銀行内の本人口座に限定する
- サービスを利用可能な利用者の属性を制限する（例えば、一定の属性要件を満たす個人に限る、法人に限る、系列企業や従業員に限る、等）
- 不正送金、情報漏洩が発生した場合に銀行又は API 接続先が利用者に対して被害額を補償する [19]
- 利便性が高まる半面、認証強度が低下することによるリスクについて利用者の十分な理解と同意を得た上でサービスを提供する
- 銀行が利用者からの決済指図を API 接続先を経由せずに直接受け付ける [20]

- なお、上記の例を組み合わせれば即座に認証強度を引き下げることが可能になるわけではなく、採用する認証方式と上記の利用者保護策を組み合わせた後においても、個人・法人等の利用者の属性や認証する取引のリスクに見合った利用者保護が十分に確保されることが必要である。

（通信方式）

- 通信方式としてオープンネットワークを使用する場合、第三者による盗取等を防止する観点から、TLS を使用して保護することが必要である。

（システムの堅牢性）

- 銀行は、顧客情報について、商慣習又は信義則に基づく私法上の義務として守秘義務を負うほか、銀行法（13 条の 3 の 2：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／II-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル」（別紙２）、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」、全国銀行個人情報保護協議会が定める「個人情報保護指針」・「個人データの安全管理措置等に関する指針」等に基づき、顧客の利益が不当に害されることのないよう、当該業務に関する情報を適正に管理し、かつ、当該業務の実施状況を適切に監視するための体制の整備その他必要な措置を講じることが求められている。また、態勢が不十分な場合は、銀行法に基づく業務改善命令等の対象となる。

- 銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API では、外部委託と

[19] 但し、資金移動上限を定めない場合、被害は補償されても、反社会的勢力等に巨額の資金が盗取される可能性がある点には留意が必要。
[20] 現在、W3C（World Wide Web Consortium：ウェブ上で使用される各種技術の標準化を推進する非営利団体）において標準仕様の検討が進められている Payment Request API では、決済指図が API 接続先のサーバを経由せず、利用者の使用端末から直接銀行に送信される仕組みが検討されている。

異なり、銀行から API 接続先への情報提供は利用者からの申請／同意に基づくものであることや高い堅牢性が求められる銀行システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。

- API 接続先が確保すべき安全管理措置の水準は、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。
- API 接続先が確保すべき安全管理措置の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。但し、最低限、以下の措置については API 接続先においても必要である。
  - ウィルス対策ソフトの導入
  - 機密性の高い情報（例：API 接続先のログインパスワードやクライアント証明書、トークン、等）の暗号化
  - ファイアーウォール等のサイバー攻撃に対する多層防御の導入
  - サーバ変更監視（改ざん検知）、ネットワーク監視
  - 公開サーバ脆弱性対策
  - API 実行ログ（ユーザー、操作、結果、等）取得、保管
  - 情報喪失等に備えたバックアップ等の対策
- なお、API 接続先に、顧客の同意を得て銀行が提供する個人情報（個人データ）の個人情報保護法上の取扱は、個別のスキームに応じて個々に判断されるべきものではあるが、原則的には銀行は API 接続先に対して、個人情報委託先の監督義務（同法第 22 条）を負っていないと解するのが適当と考えられる。

（不正検知・監視機能）

- 不正検知・監視機能は、不正アクセス被害の発生やその拡大を未然に防止する上で重要な機能の一つである。
- 銀行については、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」において、データ改竄、不正アクセス、不正な取引、異常取引の検知・監視等に関する枠組みが定められている。
- 但し、オープン API においては、利用者の IP アドレスや認証失敗回数等の不正検知に活用される情報を銀行が直接入手できなくなるため、取引のリスクに応じて、銀行が必要とする場合には、API 接続先から銀行に不正検知に必要な情報が提供される仕組みを構築することが必要である。
- API 接続先についても、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、情報セキュリティ関連機関において、不正検知・監視機能の要否やその水準等についての考え方や留意点の整理が行われることが期待される。

(3) 内部からの不正アクセス対策

- 外部からの不正アクセス対策は、内部からの不正アクセスに対して効果を発揮しない場合がある。それゆえ、銀行、API 接続先の双方において内部からの不正アクセス対策が講じられることが必要である。

（銀行における内部不正対策）

- 銀行については、銀行法（13 条の３の２：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／Ⅱ-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル」（別紙２）、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」等において、内部からの不正アクセス防止に関する枠組みが定められている。また、態勢が不十分な場合は、銀行法に基づく業務改善命令等の対象となる。

（API 接続先における内部不正対策）

- 銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出（役職員による私的な閲覧・利用、転売を含む）防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API は、銀行システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。
- API 接続先が確保すべき内部不正アクセス対策の水準は、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。
- API 接続先が確保すべき内部不正アクセス対策の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。但し、最低限、以下の措置については API 接続先においても必要である。
  - 役職員に対するシステムアクセス権限の適切な設定・運用
  - アクセスログの記録保存、定期的な査閲
  - 役職員に対する教育・研修の実施
  - サーバルームの監視、認証、入退出管理 [21]
  - 重要な機密情報・顧客情報の媒体（USB）等へのデータのコピー制限、禁止
  - 重要な機密情報・顧客情報のデータの持出、削除、廃棄管理

(4) 不正アクセス発生時の対応

（システム設計・仕様）

- 銀行及び API 接続先は、不正アクセスが判明した場合に被害発生やその拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことができるシステム設計・仕様としなければならない。

[21] クラウドサービスを利用している場合においては、安全対策基準「クラウドサービスの利用」に定めるところに拠る。

・ 銀行及び API 接続先は、不審な資金移動等についての利用者からの照会への対応や、不正アクセス発生時の原因調査、必要な対策の検討を行うため、適切なアクセスログの記録及び保存を行わなければならない。

（情報連携、対策協議）

・ 不正アクセス発生時には、速やかに銀行と API 接続先の間で情報連携を行うとともに、原因調査や必要な対策の協議等を協力して行っていくことが必要である[22]。必要な対応については、銀行と API 接続先との間で予め取り決めて明確化しておくことが必要である。

(5) セキュリティ対策の継続的な改善・見直し、高度化

・ サイバー攻撃やサイバー犯罪の手口は年々巧妙化している上、オープン API を活用した金融サービスの提供は世界的にみても現状、初期段階にある。そのため、銀行及び API 接続先は、自社のみならず他社での不正アクセス事例等を踏まえ、セキュリティ対策の継続的な改善・見直し、高度化を図っていくことが必要である。

・ セキュリティ対策の改善・見直し、高度化に向けては、銀行及び API 接続先は、協力して取り組むことが重要と考えられる。

Ⅴ. 利用者保護原則

(1) API 接続先の適格性

（事前審査）

・ 銀行は、他の事業者等との API 接続に先立ち、利用者保護等の観点から、API 接続先の適格性を審査することが必要である[23]。

・ 適格性の審査にあたっては、少なくとも以下の点について API 接続先に確認することが必要である。
  - グループ会社を含めた事業内容、兼業内容
  - 反社会的勢力との関係の有無を含む社会的信用、組織ガバナンス
  - 法令遵守態勢
  - 利用者保護態勢[24]
  - 利用者保護原則の充足状況
  - 過去に発生した利用者保護関連の不祥事案と改善状況
  - 利用者の属性や取引のリスクに応じた、継続的な利用者保護策の高度化に向けた態勢やリソースの有無

---

[22] その他の不正アクセス発生時の対応については、「Ⅴ.利用者保護原則」の「(4)被害発生・拡大の未然防止」を参照。
[23] 情報セキュリティ関連の適格性については、「Ⅳ.セキュリティ原則」の「(1)API 接続先の適格性」を参照。
[24] 特に顧客情報の適切な取扱・管理態勢や、取得情報の利用目的の適切性、利用約款の適切性（過度な免責規定等、利用者保護に著しく欠ける条項の有無）、について確認する。

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が定めた社内規定等は、上記の適格性の審査にあたっての参考になると考えられる。
- 複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される[25]。
- なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や、銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる[26]。

（モニタリング）

- 銀行は、API 接続先の適格性について、API 接続後も定期的に又は必要に応じて確認することが必要である。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、個別に判断されると考えられる。
- 銀行は、API 接続にあたって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、API 接続先に提出を求める情報、API 接続先が大幅な態勢見直しや業務停止等を行う場合の対応、等）を予め取り決めておくことが必要である。
- 銀行は、API 接続先の利用者保護態勢等に関する適格性に懸念があると判断した場合には API 接続先に対して改善を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[27]。
- なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる[28]。

（その他の留意点）

- API 接続先において API 接続を通じて提供する金融サービスに関して利用者保護に欠ける不祥事案等が発生した場合、銀行と API 接続先との関

---

[25] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。
[26] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。
[27] 但し、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。
[28] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

係、利用者からの見え方等によっては、銀行側も社会的な批判を浴びる等のレピュテーションリスクが生じる可能性に留意が必要である。

- API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ銀行側も自行サービスの提供を取り止めて、預金者に対して API 接続先のサービスの利用を推奨する場合は、形式上、銀行と API 接続先の間に外部委託契約が締結されていなくとも、その実態において同視され、銀行法に基づく外部委託規制の対象となる可能性があることに留意が必要である。
- API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ利用者の大部分が当該 API 接続先のサービスの利用に依拠する場合は、API 接続先のシステム障害や業務停止等によって、利用者が金融サービスを利用できなくなり、混乱が生じるおそれがあることに留意が必要である。
- 事前の取決めにおいて、API 接続先における障害等によって銀行の業務に影響が生じるおそれがある場合には、ただちに銀行に連絡するよう定めておくことが必要である。なお、その他の障害等の報告要否やタイミングについても、予め取り決めておく必要があることに留意する。
- API 接続先もしくは銀行の都合によるサービス停止を行う際は、一定期間の事前通知期間を設定することが必要である。

(2) 説明・表示、同意取得

（重要な情報の表示、同意取得）

- インターネットを利用した取引は、基本的に画面に表示される情報に基づいて利用者の判断・同意が行われ、また、必要な情報を表示しても、利用者が十分に確認せずに、手続きを進める可能性がある。
- そのため、銀行及び API 接続先は、利用者の判断・同意に必要な情報を単に提供・表示するに止まらず、わかりやすく画面表示するとともに、誤認・誤解を招く表現を避け、また、利用者に重要な判断・同意を求めるものについては注意喚起プロセスを設けることや、利用者のシステム操作による同意を求めること等、利用者保護に十分配慮した表示方法、画面構成とすることに努めなければならない。
- 銀行は、トークン発行にあたって、少なくとも以下の点について、わかりやすく画面表示の上、利用者の同意を求めることが必要である。
  - アクセス権限を付与する API 接続先の名称
  - API 連携するサービス等の名称
  - 付与する権限の内容・範囲
  - 付与する権限の有効期限[29]
  - 付与した権限の削除、解除方法
  - その他注意喚起が必要な事項
- API 接続先は、サービス提供にあたって、少なくとも以下の点について、わかりやすく画面表示の上、利用者の同意を求めることが必要である。
  - 個人情報保護法に基づく取得した情報の利用目的、共有範囲（第三者提供の有無）
  - 取得した情報の削除に関する事項

[29] リフレッシュトークンを発行する場合には同トークンによって延長される最大の有効期限。

- サービス利用上の制限
- その他注意喚起が必要な事項

（リスク等に関する表示）

- API 接続先は、提供するサービスに関して生じる主なリスクの適切な表示に努めなければならない。
- API 接続先は、サービス提供時間帯又は停止時間帯、休日・休業等のサービス提供上の制約について適切な表示に努めなければならない。

（利用者の誤認防止）

- 以下の点については、特に利用者の誤認や誤解が生じるおそれがあることに留意し、適切に表示することに努めなければならない。
  - API 接続先が提供するサービスは銀行が提供するサービスとは異なること
  - 銀行と API 接続先の関係、それぞれの役割（特に API 接続先が銀行代理業者又は銀行の外部委託先でないこと）
  - 決済指図取引と他のサービスの区別
  - 銀行と API 接続先の画面の区別
- なお、銀行は、API 接続先が虚偽又は意図的に誤認を招く表示を行っていることが判明した場合には、API 接続先に対して是正を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消、関係当局への通報等の必要な措置を講じなければならない。

（その他の表示）

- 銀行及び API 接続先は、利用者からの相談・照会、苦情、問合せがあった場合の役割分担、業務フロー等を、予め取り決めておくことが必要である。
- 銀行及び API 接続先は、上記の取決め内容を踏まえ、利用者からの相談・照会、苦情、問合せに対応するための連絡先を表示することが必要である。
- API 接続先は、商号、代表者、住所、連絡先等について表示することが必要である。
- API 接続先は、電磁的方法による決算公示を選択している場合、会社法に基づく決算公告についても表示することが必要である。

(3) 不正アクセスの未然防止

- API 接続先は、不正アクセスを未然に防止する観点から、例えば以下の点について、利用者に注意喚起することに努めなければならない。
  - API 接続先のログインパスワード等は、銀行サービスに利用しているパスワード等と異なるものを設定すること
  - API 接続先のログインパスワード等は、類推されやすいものを避けること、適切な管理に努め第三者に貸与、開示しないこと、定期的に変更すること
  - セキュリティ対策ソフトを導入すること
- API 接続先は、利用者に対して、API 接続先のパスワード等の紛失、漏洩や不正アクセスの懸念がある場合には、ただちに API 接続先に対して連絡するよう求めておくことが必要である。

(4) 被害発生・拡大の未然防止

（初動対応）

- 銀行又は API 接続先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことが必要である。
- 銀行と API 接続先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、一方で API に関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を銀行と API 接続先間において予め取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。
- API 接続先が複数の銀行と接続している場合において、他の銀行においても同様の事案が発生するおそれがある場合には、API 接続先は、当該他の銀行に対してもただちに連絡し、被害拡大を未然に防止することに努めなければならない。

（利用者への連絡）

- 被害が発生した利用者への連絡や、被害が広範な利用者に及ぶ可能性がある場合に利用者にただちに十分な注意喚起（例えば、ただちにパスワード等の変更を求める等）ができるよう、API 接続先は、利用者との連絡手段を予め確保しておくことが必要である。
- 利用者に届出・登録を求める連絡手段の範囲については、提供するサービスの内容や取引のリスクに応じて、個別に判断されると考えられる。
- 銀行は、API 接続先が利用者との十分な連絡手段を予め確保することができない場合、被害発生時に、銀行が API 接続先に代わって利用者に対し連絡、注意喚起する必要が生じる可能性に留意することが必要である。

(5) 利用者に対する責任・補償 [30]

- オープン API では、取引指図の処理・実行に API 接続先と銀行の双方が関与するため、情報流出や不正送金、システム上の不具合等により利用者に損害が発生した場合、利用者に対する責任の所在や、対応窓口・主体等が不明確になるおそれがある。
- 当事者の民事上の最終的な損害賠償責任を司法の判断に委ねた場合、速やかな被害回復、補償等が図られず、利用者保護に欠けるおそれがある [31]。

（当事者間における事前の取決め）

- 銀行及び API 接続先は、利用者に対して速やかな被害回復、補償等を図る観点から、不正アクセスや情報流出、不正送金、システム上の不具合

[30] 2016 年 12 月 27 日付で公表された金融審議会・金融制度ワーキンググループ報告書では、「金融機関は（中略）業者との間で締結する契約において顧客に生じた損失の分担を定め、公表することとする」（報告書８頁参照）とされており、当該記述を踏まえ、本節は、利用者の保護を適切に確保していくための銀行及び API 接続先と顧客との間の損失分担ルールのあり方について検討したもの。

[31] なお、本節における記述は、API 接続先及び銀行が利用者保護の観点から自主的に行うことが期待される取組みであり、それぞれの利用者に対する最終的な法的責任を加重又は軽減するものではない。

等が発生した場合の対応窓口や、利用者に損害が生じた場合の補償・返金方法（含む、その主体）[32]、補償範囲について、予め取り決めておかなければならない[33]。なお、利用者に対して双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行ってはならない[34]。

- API 接続先及び銀行は、予め取り決めた利用者に対する補償・返金方法とその補償範囲（免責事由も含む）について、API 接続先及び銀行は、ウェブサイト等において利用者が常時確認できるよう表示するとともに、API 接続先が利用者と利用契約を締結する際にわかりやすく画面表示する等により、利用者が補償・返金を求める際の対応窓口やその方法について十分認識できるよう努めなければならない。

（補償内容・範囲に関する考え方）

- API を利用したサービスによる預金等の不正な払戻しについて、銀行及び API 接続先に過失がない場合でも、利用者が個人であって利用者自身の責任によらずに被害に遭われた場合については、上記事前の取決めに基づいて銀行又は API 接続先から補償を行うことが必要である。なお、利用者に重大な過失又は過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担にすることも含め、個別に判断されることが必要である。
- 法人の利用者については、個人の利用者と比較して、セキュリティ対策等への対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、サービス提供者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人の利用者に対する補償については、利用者が行っていたセキュリティ対策や不正利用被害の防止に関する状況、法人の属性やセキュリティ対策への対応力等の点を考慮して、個別に判断されることが必要である。
- 銀行及び API 接続先は、API を活用したサービスの形態や利用者の属性等に鑑みて、上記と異なる補償内容・範囲とすることに合理的な理由がある場合であって、かつ利用者に不測の損害が生じないよう、かかる補償内容・範囲について利用者に適切に説明又は表示した場合に限り、補償内容・範囲を個別に定めることができる。

（API 接続先が補償・返金責任を負う場合の留意点）

- 銀行と API 接続先との間の取決めに基づき API 接続先が利用者に対して補償・返金責任を負う場合、銀行は、API 接続先の利用者に対する補償・返金に係る態勢や資力等が利用者保護に欠けるおそれがないかに留意の上、API 接続の是非を判断するとともに、それらの状況について定期的に又は必要に応じて確認することが必要である。
- 銀行は、API 接続先の補償・返金の態勢や資力等が利用者保護に欠けるおそれがあると判断した場合、API 接続先に対して態勢の見直しや責任財産の充実、責任保険への加入を求め、API 接続先においてそれが困難な場合は API 接続しない（あるいは接続の停止又は取消を検討する）等の

[32] 利用者への補償・返金後の、銀行と API 接続先の間の内部分担（求償）についても、別途予め取り決めておくことが望ましい。
[33] 銀行及び API 接続先が利用者に対して連帯して責任を負うこととする場合でも、利用者からみて対応窓口・主体等がわかりにくくなるおそれがあることから、任意の一次的な補償・返金方法（含む、その主体）等について、予め取り決めておくことが望ましい。
[34] その前提として、銀行は、API 接続先の利用約款について、消費者契約法等を踏まえ、不相当に API 接続先の責任を限定する条項が定められていないかを精査することが必要である。

対応を行うことが必要である。

- API 接続先の利用約款等において API 接続先の免責事由が過大に定められている等（例えば、過失責任も負わない等[35]）、実質的に利用者に対する補償・返金責任が果たされないおそれがある場合、消費者契約法等を踏まえ、見直しを求めることが必要である。

Ⅵ. その他

（公表情報の取扱）

- 店舗・ATM の所在地等、銀行のウェブサイト等においてログイン等の手続きを要さずに取得可能な公表情報（以下、「公表情報」）を API 接続先に提供する場合は、上述の記載にかかわらず、以下の取扱とすることが考えられる。
  - 銀行と API 接続先との通信経路において改竄が行われることを防止する観点から、銀行と API 接続先との通信方式は、セキュリティ原則「(2) 外部からの不正アクセス対策」に定める通信方式に拠るものとする。
  - API 接続先は、システム上の不具合や外部又は内部からの攻撃による改竄等によって、銀行に利用者からの問い合わせが行われる可能性のある事態が発生した場合には、ただちに関係銀行に対し連絡するよう努めなければならない。
  - 銀行は、API の利用約款等において、不具合発生時等の責任について予め定めておくことが望ましい。
  - 銀行は、公表情報を提供する API のアクセス量を銀行側でコントロールできない場合には、システムキャパシティの超過が原因で不具合が発生するリスクに留意するものとする。

（API 接続先の API 接続先の取扱）

- 銀行は、API 接続先との間で「API 接続先の API 接続先」（以下、「API 連鎖接続先[36]」）の取扱について予め取り決めておくことが必要である。
- これには、例えば、API 接続先と同様に取扱う（銀行が API 連鎖接続先と直接契約を締結）、API の連鎖接続について銀行の承諾又は銀行への事前通知を条件とする、連鎖接続を許容する条件を双方協議の上予め定める、API 接続先の責任と管理の下で連鎖接続を許容する等、様々な方法が考えられる[37]。
- いずれの方法による場合であっても、API 連鎖接続先において、本原則の趣旨を踏まえて、十分なセキュリティ対策と利用者保護が図られていることが重要である。

---

[35] なお、事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項や、当該事業者、その代表者又はその使用する者の故意又は重大な過失による事業者の債務不履行により消費者に生じた損害を賠償する責任の一部を免除する条項等は、消費者契約法（第８条乃至第１０条）に基づきそもそも無効とされる。

[36] 銀行に対する API 接続先からの取引指図が、API 接続先と API 接続する他の事業者等の取引指図に基づいて行われる場合における、当該他の事業者等をいう。

[37] API 連鎖接続先の取扱は、例えば、取引のリスクに応じて参照系 API と更新系 API との間や、API 連鎖接続先が API 接続先と同一グループに属するか否かによって異なる取扱とすることも考えられる。

・　なお、API 接続先が有する自社の情報を同接続先の API を通じて他の事業者等に提供することは、API の連鎖には該当しないが、個人情報保護法等に基づき適切な利用者保護が図られる必要があることに留意する。

（業界・企業横断的なセキュリティ対策に関する取組み）

・　関係者においては、業界・企業横断的な不正アクセス事案やセキュリティ関連対策の情報共有の枠組みについて、セキュリティ関連団体等との連携を含め、引き続き検討していくことが期待される。

・　関係者においては、本原則を必要に応じて見直し・改訂していくことが必要である。なお、事務局における改訂要否の検討等の参考とするため、本原則についてご意見がある方は、末尾に掲示した意見提出先までご連絡いただきたい。

（バンキング API 以外の API における本原則の活用）

・　当検討会は、銀行以外の事業者がオープン API を提供する場合においても、本文書で定めたセキュリティ原則・利用者保護原則が、当該事業者におけるセキュリティ対策、利用者保護態勢を整備する上で、参考になることを期待する。

以　上

【本原則に対する意見提出先】

open-api＠zenginkyo.or.jp
（事務局：一般社団法人　全国銀行協会）