投資一任業務を行う投資運用業者の顧客情報保護と秘密保持義務 ： 米国レギュレーションS-Pによる規制を中心に

論説

投資一任業務を行う投資運用業者の顧客情報保護と秘密保持義務

――米国レギュレーション S-P による規制を中心に――

牛　丸　弘　行

はじめに
第１章　米国における投資運用業者の顧客情報保護と秘密保持義務
第２章　SEC による行政処分事例
第３章　我が国における投資運用業者の顧客情報保護と秘密保持義務
おわりに

は　じ　め　に

本稿は，投資一任業務を行う投資運用業者の顧客情報の秘密保持義務を検討する。従来，我が国において，銀行等の金融機関の法的な顧客情報の秘密保持義務に関しては，かなり，議論が進んでいる(1)。しかし，投資運用業者の顧客情報の秘密保持義務については，あまり，議論が進んでいないように思われる。そこで，米国の規制の状況を研究し，我が国の投資運用業者の顧客情報の秘密保持義務の規制の研究の参考にしたい。

米国において投資運用業者の顧客の秘密保持義務の違反は，例えば，第１に，投資運用契約から生じる信任義務違反，第２に，1940年投資顧問法（以下，「投資顧問法」という）206条違反，第３に，グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act；以下，「GLB 法」という(2)）に基

（１）　浅井弘章『個人情報保護法と金融実務（第４版）』（金融財政事情研究会，2016年）230－232頁を参照。

づいて，証券取引委員会（Securities and Exchange Commission；以下，「SEC」という）が制定した規則 Regulation S-P の違反となる場合がある。第４に，個人情報の盗取に対する規制として，Regulation S-ID が定められている。同規則は，米国において，Identity Theft Red Flags Rule（以下，Red Flags Rule という）と呼ばれている。

我が国において，投資運用業者の顧客情報の秘密保持義務の法的根拠は，次のように考えられる。第１に，投資一任契約上の義務から導きだされる(3)。投資運用業者は，顧客との間で投資一任契約を締結しており，投資一任契約上の義務に違反すれば民法644条に規定する善管注意義務に違反することになる。投資運用業者は，損害を被った顧客に対して，義務違反につき債務不履行に基づく損害賠償責任を負う場合がある。

第２に，投資運用業者の顧客情報の秘密保持義務の法的根拠は，金融商品取引法（以下，「金商法」という）の善管注意義務・忠実義務（同法42条）から導き出される。同規定に違反すれば，金商法上の行政処分の対象となるばかりでなく，投資運用業者は，金商法という業法違反の場合でも，顧客に対して，民法上の不法行為に基づく損害賠償責任を負うこともある。

（２） Pub. L. No. 106-102, 113 Stat. 1436 (1999) (codified at 15 U.S.C. §§ 6801-6827).

（３） 例えば，「金融機関の守秘義務とは，顧客との取引過程で取得した顧客に関する情報をみだりに第三者に開示しないという義務であり，法定化されていたものではなかったが，これまで各取引契約からその付随的・補充的義務として当然に負っている義務とされてきた。」と主張されている。井部千夫美・杉浦宣彦「金融取引の守秘義務についての比較法的考察―欧米の個人金融取引における守秘義務についての法制度を中心に―」金融庁金融研究研修センター 2006.4 Financial Research and Training Center discussion paper series v. 21　概要 i 頁。投資運用業者に置き換えると，顧客情報の秘密保持義務は，投資一任契約からその付随的・補充的義務として当然に負っている義務であると解される。

第３に，投資運用業者の顧客情報の秘密保持義務の法的根拠は，顧客が個人である場合には，個人情報の保護に関する法律（以下，「個人情報保護法」という）からも導きだされる。(4)

以上の３つの法的根拠のうち，特に第２の金商法から導き出される投資運用業者の顧客の秘密保持義務について，米国法の主に SEC による規制を参考にして，検討する。

第１章　米国における投資運用業者の顧客情報保護と秘密保持義務

第１節　概説

米国における投資運用業者の顧客情報の秘密保持義務の根拠として，第１に，投資運用契約から生じる信任義務がある。米国の投資顧問法研究の大家である Frankel 教授は次のように述べている。(5)「投資顧問は，多くの受任者と同様に，投資顧問として，その顧客に関して，顧客から得た情報を漏らしてはならないという義務を負っている。そして，信任関係がある期間に取得した情報に関する秘密保持義務は，信任関係の終了後にも継続する。投資顧問は，顧客に対し，効率的なサービス提供を行うために顧客の情報を必要とするが，顧客が情報の漏洩を心配することなく投資顧問に投資の相談ができることが求められ，そのために投資顧問の秘密保持義務を課すことは，必要であり，かつ，顧客の合理的な期待にも適合するものである。それ故に，投資顧問の利益のため，または他の目的のためかにかかわらず，顧客の情報を故意に漏らすことは，信任義務違反である。過失

（４）「金融商品取引業者は個人情報保護法上の個人情報取扱事業者として相応の対応を行わなければならない。」とされる。川村雄介『金融商品取引業のコンプライアンス（第４版）』（金融財政事情研究会，2008年）32－33頁。

（５） Tamar Frankel, Arthur Laby, Ann Taylor Schwing, The Regulation of Money Managers, Vol. 2, Ch. 13, 72-73 (3d ed. 2015).

によって，顧客の情報を漏らし，かつ，それにより顧客に損害を与えた投資顧問は，顧客に損害を賠償しなければならない。」

米国において投資顧問が顧客に対し受任者として信任義務を負うことは，米国の連邦最高裁判所判決[(6)]で確定されているところであるが，Frankel 教授は，投資運用業者の顧客情報の秘密保持義務の根拠をそのような信任義務から導き出されることを明言している。また，顧客情報の秘密保持義務を投資顧問に課すことは，顧客の利益ばかりでなく，顧客から詳細かつ正確な情報を入手することができ，適切な投資運用が可能になるという点において，投資顧問にとっても利益となると指摘していることは重要であると考える。

第２に，投資顧問が故意に自己または第三者の利益のために顧客情報を提供することは，投資顧問法206条に違反する詐欺的な行為となりうる[(7)]。投資顧問法206条１号は，「顧客又は顧客となろうとする者を欺罔するために手段，計画，又は技巧を用いること」と定め，同条２号は，「顧客又は顧客となろうとする者に対して詐欺又は欺瞞となる取引，慣行，又は業務に従事すること」と定めている。

投資顧問法は，顧客の情報の秘密保持の重要性を意識した規定を設けている。すなわち，同法210条ｃ項は，「本法のいかなる規定も，投資管理サービスを提供する投資顧問に対し，その顧客の個人情報，投資またはその他の事項を開示することを要求し，または委員会が投資顧問に対し，このような情報を要求する権限を付与するものと解されてはならない。ただし，本法の規定の執行を目的とする特定の手続きまたは調査のために必要または適当とされる場合は，この限りでない。」と規定する。なお，ここにいう「投資管理サービス」は，「各顧客の個人的要求に応じて，ファンドの

（６） SEC v. Capital Gains Research Bureau, Inc., 375 U.S. 180 (1963).
（７） Ibid.

投資に関して継続的な助言を提供すること」を意味している（投資顧問法202条12号）。当該規定から見て，議会は，投資運用業者がその顧客の個人情報，投資またはその他の事項の秘密を遵守する義務を有することを認識していたと主張されている[8]。

第2節　Regulation S-P による顧客の個人情報の保護

1　概説

2000年6月，SEC は GLB 法に基づき，Regulation S-P（以下，Reg. S-P とする）を採択した[9]。

投資顧問は，一般的に顧客口座の開設の手続きの一環として，顧客に関する詳細な情報を収集する。GLB 法第5編は，金融機関等を監督する行政機関が同法に基づく金融機関等による消費者の情報の適切な取扱いを実施するための規則（いわゆるプライバシー・ルール）を設けることを要求している（15 U.S.C. §6804）。GLB 法第5編は，顧客の非公開情報の安全性および秘密性を保護するために，すべての金融機関に対して，連邦によるプライバシーの保護を命ずるものである。監督機関[10]の一つである SEC は，GLB 法第5編の要求を実施するために，Reg. S-P を採択した[11]。

（8）　Ibid.

（9）　17 C.F.R. pt. 248; see Inv. Adv. Act Rel. No. 1883, 2000 SEC LEXIS 1338 (June 22, 2000) (adopting Regulation S-P).

（10）　SEC 以外の監督機関は，①貯蓄金融監督庁（Office of Thrift Supervision），②通貨監督局（Office of the Comptroller of the Currency），③連邦準備制度理事会（Federal Reserve Board），④連邦預金保険公社（Federal Deposit Insurance Corporation），⑤全米信用組合協会（National Credit Union Administration），⑥商品先物取引委員会（Commodity Futures Commission），および⑦連邦取引委員会（Federal Trade Commission）である。

（11）　米国の証券取引法の大家である Loss 教授も，著書において，秘密保

Reg. S-P は，SEC に登録している投資顧問，証券会社，投資会社に対して，その顧客から収集した情報を保護することを要求している。以下では，特に，投資顧問に対する Reg. S-P の適用について検討する。

投資顧問は，その消費者に対して，①プライバシーの政策およびその運用について通知を行うこと，②消費者に関する非公開の情報を関係者（affiliates）および特定の関係者でない第三者（non affiliates third party）に開示することができる条件を説明すること，③オプトアウト（情報授受の停止の申出[(12)]）によって関係者でない第三者に当該情報を投資顧問が開示することを防止するための手段を設けることが求められている。

Reg. S-P は，また，投資顧問に対して，顧客に関する情報および記録を保護するために，書面による政策および手続を採択することを要求している。

2004年に改正された Reg. S-P は，その適用を受ける者に対し，処分予

持の取り扱いの章で，Regulation S-P に関する規制内容を詳細に紹介しており，同規則の重要性を認識していると考えられる。10 L. Los, J. Seligman & T. Paredes, Securities Regulation ch. 13. F3 at 5135（5th ed. 2018）.

（12） 我が国の個人情報保護法第23条第２項において，個人情報取扱事業者が，第三者に提供される個人データについて，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場合であって，同項各号に掲げる事項について，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いているときは，当該個人データを第三者に提供することができるとされている。この制度は，我が国において，英語の opt out のカタカナ表示である「オプトアウト」と呼ばれている。金融庁の「金融分野における個人情報保護に関するガイドライン」においても，オプトアウトの説明を行う同ガイドラインン13条４項の表題において「４法第23条第２項（オプトアウト）について」と表示している。本文において，同制度については「情報授受の停止の申出」という日本語訳ではなく，オプトアウトと述べる。

定の情報への無断のアクセスや利用を防止するため，当該情報を保護する合理的な手段をとることを要求している。(13)

論

2　Regulation S-P の規制

（1）「消費者」と「顧客」の定義

説

Reg. S-P は，「消費者（consumers）」と「顧客（customers）」とを分けて，定義づけている。消費者と顧客の区別は，後述する Reg. S-P の定める通知義務において重要となる。

（**消費者の意義**）Reg. S-P は，個人を主として，自分自身，家族，または世帯のための金融商品または金融サービスを投資顧問から購入している，または購入した「個人」を「消費者」として定義づけている（17 C.F.R. §258.3(g)(1).）。Reg. S-P は，主として，ビジネス，商業，または農業の目的で，金融商品もしくは金融サービスを購入する会社もしくは個人に関する情報に対しては適用されない。金融上の助言サービスを求めるにあたって，投資顧問に対し，非公開の個人情報を提供する個人は，たとえ，当該個人が投資顧問と投資顧問契約を締結しない場合であっても，当該投資顧問の消費者に該当する（17 C.F.R. §258.3(j) and (k)）。

（**顧客の意義**）「顧客」というのは，金融商品または金融サービスを提供するという投資顧問との継続的な関係を有している消費者である。SEC は，ある個人が，投資顧問の顧客であるかどうかを決定するために役立つ，いくつかの例を示している。すなわち，

（ア）投資顧問が投資顧問契約を締結している相手方である個人は，投資顧問の顧客である（17 C.F.R. §248.3(k)(2)(ⅰ)(B)）。

（イ）投資顧問が個人退職金口座の証券や資産の保管人として行動してい

（13）　Inv. Adv. Act Rel. No. 2332, 2004 SEC LEXIS 2823 (Dec. 2, 2004).

るところの当該口座を保有する個人は，投資顧問の顧客である（17 C.F.R. §248.3(k)(2)(ⅰ)(D)）。

（ウ）ラップフィー口座（wrap fee account）の顧客（client）は，書面による契約がない場合においても，投資助言を提供するポートフォリオ・マネージャーの顧客である(14)。

（エ）信託の委託者または受益者は，信託の受託者として業務を行う投資顧問の消費者ではない（17 C.F.R. §248.3(g)(2)(ⅵ) and (ⅶ)）。

（オ）従業員給付制度における参加者は，当該制度のスポンサーとなっている投資顧問の消費者ではない（17 C.F.R. §248.3(g)(2)(ⅷ).）。

（カ）ミューチュアル・ファンドの株主は，当該ミューチュアル・ファンドを運用する投資顧問の消費者ではない(15)。

（キ）インターネットにおける金融上のツール（tool）（ソフトウエアをいう）を利用する個人は，そのツールを利用させている投資顧問の消費者ではない(16)。

Regulation S-P は，投資顧問に対し，その消費者および顧客に関する情報を保護することを要求している。消費者と顧客の違いは，提供しなければならない通知のタイプおよびタイミングを決定づける。消費者という文言は，広く定義づけられている。すなわち，消費者は顧客を含むより広い概念である。

---

(14) James E. Anderson, Robert G. Bangal and Marianne K. Smythe, Investment Advisers: Law & Compliance Vol. 1, 8-67 (2009).

(15) Inv. Adv. Act Rel. No. 1883, Fed. Sec. L. Rep. (CCH) ¶86,313 (June 22, 2000).

(16) Ibid.

（2）非公開の個人情報の定義[17]

Reg. S-P は，次のような非公開の個人情報のみを保護する。すなわち，①個人的に特定できる非公開の財務情報，および②一般に入手可能でない個人的に特定できる非公開の財務情報を利用することにより得られる消費者のリストと定義されている。上記①にいう「個人的に特定できる非公開の財務情報」とは，消費者が，契約の申込書または契約の中で提供する情報のような，金融商品またはサービスを得るために投資顧問に提供する情報を意味する。（17 C.F.R. §248.3(u)(1)。例として次のものが示されている（17 C.F.R. §248.3(u)(2)）。口座の残高，証券の保有持分，または購入もしくは売却した金融商品のような，金融取引から生じる情報（17 C.F.R. §248.3(u)(1)(ii) and 248.3(u)(2)(i)(B)）情報を証明するために用いられる消費者へのレポートまたはその他の外部の情報源からの情報（17 C.F.R. §248.3(u)(1)(iii) and 248.3(u)(2)(i)(G)）である。

一般に利用される情報は，非公開の個人情報の定義から除外されている。一般に利用される情報というのは，以下の情報源の一つから一般に入手可能な情報である。①公的な記録（例えば，不動産に関する記録，証券にかかる届出）（17 C.F.R. §248.3(v)(1)(i)），②広く配布されている通信媒体（例えば，電話帳，テレビもしくはラジオの番組，または新聞）（17 C.F.R. §248.3(v)(1)(ii)），③連邦，州または地方の法律によって公表が義務づけられる情報（17 C.F.R. §248.3(v)(1)(iii)）である。

Reg. S-P は，投資顧問が，前記の 3 つの情報源のうちの 1 つから情報を入手することを要求するものではない。投資顧問が，一般に入手可能であると合理的に確信していることで，十分である。当該情報が，一般に入手可能であると確信し，合理的であると評価するにあたって，投資顧問は，

（17） Loss 教授は，非公開の個人情報の定義が，特に重要であると説明されている。10 L. Loss, et. al., supra note 11, at 5135.

消費者が，情報を公的な記録に掲載していないか否かを確認しなければならない。例えば，投資顧問が，電話帳で電話番号を確認した場合，または消費者が，投資顧問に対して電話帳に電話番号が掲載されていると通知している場合には，個人の電話番号は，一般に入手可能であるという合理的な確信をもちうるものとなる（17 C.F.R.§248.3(v)(2)(ⅰ)(C)）。

（3）プライバシーの政策および運用の通知

（ⅰ）通知要件

Reg. S-P は，投資顧問に対して，プライバシーの政策および運用を適切に反映する明確かつ明白な通知を顧客に対し行うことを要求している。通知が，情報の性質および重要性に注意喚起を意図するものである場合，明確かつ明白（clear and conspicuous）であるとされている（17 C.F.R.§248.3(c)(1)）。Reg. S-P の下で，通知は，以下の場合には，情報の性質および重要性に注意を喚起しているとされている。すなわち，①簡明な文言の見出しを用いていること，②読みやすい活字体および活字の大きさを用いていること，③広い余白および十分なスペースをとっていること，④キーワードに関してボールドフェイス（肉太活字）体またはイタリック体を用いていることである。

投資顧問がそのプライバシーの政策および運用を変更した場合，変更の通知を行わなければならず，かつ，以前の通知において予想されていない方法で「関係者でない第三者」に対し非公開の個人情報が提供される前に，オプトアウトを行う新たな機会を提供しなければならない（17 C.F.R.§248.8）。

（ⅱ）当初のプライバシーの政策および運用の通知

投資顧問は，少なくとも顧客の関係（投資顧問が消費者に対して，金融

商品または金融サービスを提供する継続的な関係）を確立するまでに，顧客に対して，当初のプライバシーの政策および運用の通知（以下，当初の通知という）を行わなければならない。投資顧問は，一般的に，顧客に開示説明書（brochure）を提供する時と同時に当初の通知を行う。

投資顧問は，以下の場合は，顧客に対し，顧客に開示説明書（brochure）を提供する時と同時に行うことなく，顧客の関係を確立した後，合理的な期間内に通知を行うことができる 17 C.F.R. §248.4(e)。すなわち，①顧客が，投資顧問と顧客の関係を確立することを選択していなかった場合，②顧客の関係の確立時までに通知することが，顧客の取引を実質的に（substantially）遅らせ，かつ，顧客が後で通知を受け取ることに同意する場合，③関係者ではない証券会社や登録投資顧問が，すでに顧客の関係または消費者の関係を確立しており，投資顧問が，事前にその事実を認識していなかった場合である。

投資顧問は，新たな金融商品や金融サービスを受ける現在の顧客に通知を行うことを要求されていない。ただし，これは，顧客に対して以前に行われた通知が，新しい商品に関する投資顧問の政策および運用を適切に説明している場合に限られる（17 C.F.R. §248.4(d)）。

投資顧問は，「関係を有しない第三者」に対し消費者に関する非公開の個人情報を提供する前に，顧客でない消費者に対して，当初の通知を行わなければならない。これは，提供が特定の除外された第三者に行われたものではない場合に限られる（17 C.F.R. §248.14 and §248.15）。消費者が顧客にならなかった場合，投資顧問は，当初のプライバシーの通知も行わなくてもよい。これは，投資顧問が，消費者に関する非公開の個人情報を投資顧問と「関係を有しない第三者」に開示しない場合に限られる（17 C.F.R. §248.4(b)(2)）。

（ⅲ）年次の通知

投資顧問は，顧客の関係の継続中，年次の通知を少なくとも12カ月に1度，各顧客に送付しなければならない（17 C.F.R.§248.5）。

年次の通知は，明確かつ明白に投資顧問の現在のプライバシーの政策および運用を開示するものでなければならない。投資顧問は，投資顧問からの連絡を不要であると自ら積極的に述べる顧客に対しては，年次の通知を送る必要はない。しかしながら，通知は，顧客の請求により入手可能とされていなければならない。投資顧問は，顧客に対し，当初の通知，オプトアウトの通知および変更された通知を行うことが要求されている（17 C.F.R.§248.9(c)(1)(ⅱ)）。

（ⅳ）当初および年次の通知の内容

投資顧問の当初および年次のプライバシーの通知には，次のような情報が含まれる（17 C.F.R.§248.6(a)）。すなわち，

①投資顧問が収集する非公開の個人情報の類型

②投資顧問が提供する可能性がある非公開の個人情報の類型

③投資顧問が非公開の個人情報を提供する関係者および関係者でない第三者の類型

④投資顧問が提供する，以前に顧客であった者に関する非公開の個人情報の類型，ならびに投資顧問が当該情報を提供する関係者および関係者でない第三者の類型

⑤投資顧問が第三者のサービス提供者および共同して販売を行う者との契約に基づき提供する可能性がある非公開の個人情報の種類ならびにサービスを提供する第三者の類型

⑥関係者でない第三者への非公開の個人情報の提供からオプトアウトする消費者の権利に関する説明および消費者がオプトアウトする方法

⑦非公開の個人情報の秘密保持および安全性の保護に関する投資顧問の政策および運用に関する説明

投資顧問が情報を提供する関係者および関係者でない第三者の類型の説明においては，①金融サービスの提供者，②非金融会社，③その他の者を含めなければならない（17 C.F.R. §248.6(c)(3)）。

SEC は，関係者および第三者の種類を次のように例示している（Sample Clause A-4. 17 C.F.R. pt. 248 app. A.）。①金融サービスの提供者は，住宅金融会社，証券会社，および保険の代理人を含む。②非金融会社は，小売業者，直接販売業者，航空会社および出版社を含む。③その他の者は，非営利団体を含む。

（4）オプトアウトの制度

Reg. S-P は，オプトアウトによって，投資顧問が，消費者の非公開の個人情報を「関係を有しない第三者」に対し，提供することを防止するための合理的な機会を提供することを要求している（17 C.F.R. §248.7(a)(3)）。投資顧問は，明確かつ明白に以下のことを記載したオプトアウトに関する通知を行わなければならない（17 C.F.R. §248.7(a)(1)）。

① 投資顧問が，消費者の非公開の個人情報を「関係を有しない第三者」に対し提供し，または提供する権利を留保している旨
② 消費者は，「関係を有しない第三者」に対する提供について，オプトアウトする権利を有する旨
③ 消費者がオプトアウトするための合理的な手段

当該手段が合理的である限りにおいて，投資顧問は，消費者が特定の手段を用いてオプトアウトを行うことを消費者に要求できる（17 C.F.R. §248.7(a)(2)(iv)）。投資顧問は，消費者が通話料無料の電話番号で電話できること，またはオプトアウトするためにチェックボックスに記入し，用

紙を返送することを求めることは，合理的であるとされる。しかし，投資顧問が，消費者に自らのオプトアウトの通知を作成すること求めることは，合理的でない。

Reg. S-P は，投資顧問に対して，投資顧問がオプトアウトの指示を受け取った後，合理的に実行可能な限り速やかに，消費者の指示に応じることを要求している。SEC は，投資顧問が，消費者に対して，オプトアウトする権利を認める期間の最大限については明示していない(18)。大抵の場合，30日が，オプトアウトすることを消費者に認める合理的な期間である(19)。消費者が，オプトアウトするならば，その指示は，消費者によって取り消されるまでは有効である。消費者が，オプトアウトの通知期間中，オプトアウトを行わないならば，投資顧問は，そのプライバシーの通知に従って，消費者の非公開の個人情報を提供することができる。オプトアウトする権利を行使しない消費者は，当該権利を失うものではなく，後で，当該権利を行使することが可能である（17 C.F.R. §248.7(f)）。

共同口座（joint account）については，投資顧問は，１件のオプトアウトの通知をすれば足りる。このオプトアウトの通知は，投資顧問が，共同口座を保有するひとりの消費者によるオプトアウトの指示の取扱いについていかに処理するかを説明するものである。投資顧問は，共同口座を保有するひとりの消費者によるオプトアウトの指示を共同口座の保有者のすべてに適用されるものとして，処理することができ，また，共同口座の消費者に，個別にオプトアウトすることを認めることができる（17 C.F.R. §248.7(d)）。共同口座のひとりの消費者がオプトアウトしたとき，投資顧問は，オプトアウトしなかった共同口座の消費者に関する個人情報のみを

(18) Inv. Adv. Act Rel. No. 1883, Fed. Sec. L. Rep. (CCH) ¶86,313 (June 22, 2000).

(19) Anderson, et. al., supra note 14, at 8-73.

提供することができ，かつ，オプトアウトした消費者に関する情報，ならびにオプトアウトした消費者および共同口座の他の消費者の情報についても提供してはならない（17 C.F.R.§248.7(d)(5)(ⅲ)(C)）。

（5）通知の方法

投資顧問は，消費者が現実の通知を受領することを合理的に期待する方法により，通知を書面によって消費者に提供しなければならず，かつ，消費者が同意する場合は，電磁的方式によって，消費者に通知を行わなければならない（17 C.F.R.§248.9(a)）。投資顧問は，最初の通知および年次の通知において，オプトアウトの通知を含めることができ，または，オプトアウトの通知を別に行うこともできる。オプトアウトの通知を別に行う場合，オプトアウトの通知は，当初の通知の謄本とともに送付しなければならない（17 C.F.R.§248.7(d)(5)(ⅲ)(C)）。通知は，顧客が通知の受領を留保し，後の日において通知を受領することを認める方法で，行われなければならない（17 C.F.R.§248.7(c)）。口頭の通知は十分でない（17 C.F.R.§248.9(e)）。

Reg. S-P は，２以上の法人に共同の通知を提供することを認めている（17 C.F.R.§248.9(f)）。ただし，通知が，すべての受領者にとって正確なものであり，かつ名称により各法人を確認できなければならない。これは，同じ持株会社の子会社である関係会社にとって有益であるかもしれない[(20)]。

一般的に，投資顧問は，顧客の直近の認識している住所に対して，通知の写しを郵送すれば，顧客が現実に通知を受領したという合理的な期待をもつことができる（17 C.F.R.§248.9(b)(1)(ⅱ)）。投資顧問は，当初の通知をウェブサイトによって行うことができ，かつ，インターネットによる

(20) Anderson, et. al., supra note 14, at 8-74.

取引を行う消費者に対して，金融商品または金融サービスを購入するプロセスにおいて，必要な段階において通知の受領を要求することができる（17 C.F.R. §248.9(b)(1)(iii)）。投資顧問は，以下のような場合，金融商品または金融サービスを購入するために，投資顧問のウェブサイトを利用する消費者は，通知を受けとったと期待することができるものとされている（17 C.F.R. §248.9(b)(1)(i)）。すなわち，当該顧客が投資顧問のウェブサイトによって年次の通知を受け取ることに同意し，かつ，投資顧問が継続的にプライバシーの政策および運用の現在の通知をウェブサイトにおいて明確かつ明白に掲示している場合である。通知が，１つのスクリーン（コンピューターの画面）より長い場合，投資顧問は，もし全体の通知を閲覧するために必要であり，かつ，ウェブサイトのその他の要素が，通知から注意をそらさないのであれば，ページをスクロールダウン（ディスプレイの画面上に表示されている画面を上から下へ連続的に動かすこと。）させるため，テキストまたはビジュアルキューズ（視覚的手掛かり）を用いるべきである（17 C.F.R. §248.3(c)(2)(iii)）。

通知は，消費者がひんぱんにアクセスするスクリーンに掲示すべきであり，またそのサイトは，消費者がひんぱんにアクセスするスクリーンのサイトへの明白なリンクを含むべきであるとされている。(21)

（6）オプトアウト要件の例外

（i）サービスの供給者

Reg. S-P は，特定の法律上の例外を規定している。その例外とは，投資顧問が，一定の場合において，情報が共有される消費者に通知を提供することなく，オプトアウトする権利を提供することなく，特定の関係を有

(21) Inv. Adv. Act Rel. No. 1883, Fed. Sec. L. Rep. (CCH) ¶86,313 (June 22, 2000).

しない第三者と情報を共有することを可能としている（17 C.F.R.§248.13(a)）。すなわち，投資顧問は，消費者にオプトアウトする機会を提供することなく，関係を有しない第三者に対して，非公開情報を提供することができるのである。この例外は，投資顧問が以下のことを行った場合に認められる（17 C.F.R.§248.13(a)）。

(a) 投資顧問が，当該情報を関係を有しない第三者に提供することを説明する消費者への当初の通知を行うこと。

(b) 情報を提供する目的以外の目的のために，当該情報を提供し，かつ，用いることを禁止するという内容の契約を第三者と締結していること（17 C.F.R.§248.13(a)(1)）。

（ii）取引の処理およびサービス

投資顧問は，消費者または顧客に対して，以下のような状況において，オプトアウトする機会の通知を提供することなく，関係を有しない第三者と情報を共有することができる。

① 消費者が請求し，または授権する取引を実行し，運用し，または執行するために必要である場合。

② 消費者が授権する金融商品またはサービスの処理に関連する場合。

③ 投資顧問における消費者の口座を維持し，サービスを行うことに関係する場合。

これらの処理の例外に従って非公開の個人情報を提供する投資顧問は，消費者に通知を提供することや情報を保護するために第三者との契約を締結することを要しない（17 C.F.R.§248.14）。

（iii）消費者の指示およびその他の限定された理由

Reg. S-P は，通知およびオプトアウトの要件に関するその他の例外を

規定している。その他の例外は，消費者にオプトアウトする通知および機会を提供することなく，関係を有しない第三者と情報を共有することを次のような場合に投資顧問に認めている（17 C.F.R. §248.15）。

① 消費者の同意または指示に基づく場合
② 投資顧問の記録の秘密および安全を保護するため
③ 詐欺を防止し，授権されていない取引を防止するため
④ 連邦法，州法，その他の法を遵守するため
⑤ 消費者のために受任者または代理資格者として活動する者のため
⑥ 裁判所の手続きおよび政府の規制機関に対応するため

（7）情報の再開示および再利用

Reg. S-P は，投資顧問から非公開の個人情報を受領する関係を有しない第三者に対して，当該情報を直接にまたは関係者を通じて，投資顧問に関係を有しない者へ開示することを禁止している（17 C.F.R. §248.11）。例えば，投資顧問から，非公開の個人情報を受領するサービスの供給者は，投資顧問が，当該第三者と情報を合法的に共有できない場合，直接または間接に投資顧問と別の関係を有しない第三者およびサービスの供給者に情報を開示してはならない。一般的なルールとして，第三者は，情報を受領した投資顧問の義務を引き受けている。

投資顧問は，Reg. S-P によって，第三者が規則を遵守していることの監視を要求されていない。しかし，SEC は再利用の制限に違反した法人に対して，執行訴訟を提起することを示唆している(22)。

(22) Regulation S-P, Question 14. これは，SEC の Division of Investment Management のスタッフによる Regulation S-P に関するする質問の回答である。この回答は，ルールや規則ではなく，また，SEC の見解ではないとされている。SEC は，この回答を承認するものではなく，否認するもの

（8）口座番号情報の提供

Reg. S-P は，原則として，投資顧問が，顧客の口座番号をマーケティングの目的のために関係を有しない第三者に提供することを禁止している（17 C.F.R. §248.12(b)(1)）。例外として，SEC は，投資顧問サービスのマーケティングの目的のため，消費者調査機関（consumer reporting agency）に対して，口座番号の提供の禁止から除外している。ただし，当該機関が，口座に対して料金を請求する権限を有しない場合に限る。

SEC は，次のことを明確にしている（17 C.F.R. §248.12(c)）。すなわち，口座番号，アクセス番号，またはアクセスコードの類似の形態は，暗号化された形態の番号を含んでいないことである。ただし，投資顧問が，その受領者に対して，番号の暗号を解読する手段を提供していない場合に限りにおいてである。

（9）政策および手続の採択義務

Reg. S-P の2004年の改正は，消費者のレポート情報を廃棄する者が，廃棄された情報が当該情報に対する許可されないアクセスまたは利用から保護するために合理的な手段を講じなければならないということを明確にした[23]。同規則を採択したリリースでは，合理的な手段の例として，紙の記録については焼却，粉砕もしくはシュレッダーによる処理，または，情報が解読され，もしくは復元されることができないようにするために電子記録の破壊もしくは消去，または，適正な手続の後，同規則の定めに一致した方法で記録を破壊することを第三者と契約することがあげられている[24]。

でもないと述べられている。
https://www.sec.gov/divisions/investment/guidance/regs2qa.htm

(23) Inv. Adv. Act Rel. No. 2331, 2004 SEC LEXIS 2823 (dec. 2, 2004).

(24) Inv. Adv. Act Rel. No. 2331, 2004 SEC LEXIS 2823 (dec. 2, 2004).

第3節　Regulation S-P の運用に関する SEC の危険警告[25]

1　危険警告の趣旨

2019年4月16日，本警告（risk alert）において，SEC の法令順守検査部門が，投資顧問および証券会社のプライバシーの通知および Safeguard の政策に関する Reg. S-P および主要な SEC のルールに関係した，法令遵守の諸問題のリストを提供していた。これらの諸問題は，SEC に登録された投資顧問および証券会社に対する最近の調査において，確認されたものである。本警告における情報は，Reg. S-P の下で，投資顧問および証券会社に対し，法令に適合したプライバシーの通知およびオプトアウトの通知を提供するにあたって，支援し，かつ，顧客の記録および情報を防御するための有効な政策および手続を採用し，実行するにあたって，支援することが企図されている。

2　頻繁に生ずる Regulation S-P の法令遵守上の諸問題

法令遵守検査部門の職員（以下において「同職員」という）によって確認された，Safeguard Rule に関連して最も一般的に生じた欠陥および弱点の例は，以下のものである。

A．プライバシーの通知およびオプトアウトの通知

同職員は，当初および年次のプライバシーの通知およびオプトアウトの通知を顧客に提供していなかった複数の登録者を発見した。そのような通知が，顧客に提供されたときであっても，当該通知が必ずしも正確に登録者の政策および手続きを反映していなかった。同職員は，登録者が未公表の個人情報を関係者ではない第三者と情報共有するにあたりオプトアウト

(25)　https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf

できるという権利について顧客に通知していなかったプライバシーの通知があったことを記録している。

B．政策および手続きの欠落

同職員は，Safeguard Rule の下で要求されている書面による政策および手続きを有していなかった複数の登録者を発見した。例えば，Safeguard Rule を書き写しだけで，運営上，技術上，物理上の Safeguard に関連した政策および手続きを含んでいなかった書類しか有していない登録者を発見した。同職員は，登録者によって，記入されるべきことが予定された多くの空白の部分を含んだままの政策および手続の書面を発見した。プライバシーの通知の配布および内容について，記載していたにもかかわらず，Safeguard Rule によって要求されている政策および手続きを全く含んでいない政策を有する登録者が存在していた。

C．顧客の記録および情報を防衛するために合理的に設計されず，または実行されない政策

同職員は，（1）顧客の記録および情報の安全性および秘匿性を保証すること，（2）顧客の記録および情報の安全性または誠実性に対する予想される脅威から保護すること，かつ，（3）顧客に大きな損害または不便を結果として生じる記録および情報に対する無権限のアクセスまたは盗用から保護することを合理的に設計せず，または実行されていない書面による政策および手続を有する複数の登録者を発見した。

例えば，同職員は，以下のことを発見した。

①個人のコンピュータデバイス

個人のコンピュータデバイスにおいて，顧客の情報を防御することを合理的に企図されたとは思われない政策および手続きがある。例えば，同職

員は，登録者の従業員の個人用のパソコンに顧客の情報を定期的に記録し，保存する従業員を発見した。しかし，当該登録者の政策および手続は，これらの機器が，いかにして，適切に顧客の情報を防衛するように設計されるべきかについて，言及していなかった。

②電子通信

顧客の個人的に確認しうる情報を電子通信に含むことを言及しない政策および手続きがある。例えば，同職員は，日常的に暗号化されていない個人情報を含む e-mail を顧客に送付することを従業員に禁止する合理的に企図する政策および手続を有していかった複数の登録者を発見した。

③訓練および監視

顧客の情報が，暗号化され，パスワードで保護され，登録者が承認した方法により，送信されることを要求する政策および手続きが，合理的に企図されていなかった。なぜならば，従業員が，これらの手段に対する適切な訓練を受けておらず，かつ，政策が従業員によって適切に行われているかどうかを監視することを怠っていたためである。

④安全でないネットワーク

従業員が，顧客に個人的に確認しうる顧客情報を登録者のネットワーク以外の安全でないネットワークに送信するということを禁止していなかった政策および手続きがある。

⑤社外のベンダー

社外のベンダーに関して，登録者の政策および手続をフォローすることに失敗した。例えば，同職員は，次のような登録者を確認した。すなわち，

登録者が，その政策および手続きにおいて，社外のベンダーとの契約において顧客の個人的に確認しうる情報を秘密にするという契約を締結することを命じていたにもかかわらず，社外のベンダーに対して，契約において顧客の個人的に確認しうる情報を秘密にするということを同意することを要求していなかった。

⑥個人的に確認しうる情報の目録

登録者が，必ずしも，顧客の個人的に確認しうる情報を維持するすべてのシステムを確定していなかった政策および手続きがある。すべてのシステムの目録がなければ，登録者が，維持する顧客の確認しうる情報のカテゴリーを知らないままでいる。そのことは，合理的に企図された政策および手続を採択する登録者の能力を制限し，かつ，顧客の情報を適切に防衛する登録者の能力を制限することになりうる。

⑦事件に対応する制度

事件の対応制度を実行するための役割分担，サイバーセキュリティの事件に対応するために要求される行動，およびシステムの脆弱性の評価のような重要な分野に言及していない書面による事件の対応制度が存在する。

⑧安全ではない物理的な場所

オープンオフィスにおける鍵がかかっていないファイルのキャビネットのような安全でない物理的な場所では，保管されていた顧客の個人的に確認しうる情報がある。

⑨顧客のログインの証明

登録者の政策および手続きの下で，許可されている者以外の多くの従業

員の配布されていた顧客のログイン証明が存在する。

⑩退職した従業員

登録者の退職した従業員が，退職後も制限された顧客情報にアクセスする権利が留保されており，当該顧客情報にアクセスすることができたという事例がある。

3　結論

これらの発見された事例に対応して，登録者の多くは，同職員によって確認された諸問題を解決するためにそれぞれの政策および手続を修正した。SEC の法令順守検査部門は，登録者に対して，登録者が Reg. S-P を遵守することを確実にするため，書面化された政策および手続を調査することを奨励している。

第 4 節　Regulation S-P の改正を提案する学説[(26)]

ある論者は，SEC の最終的な目標が投資仲介業者にデータのセキュリティを真剣に運用することを促進することであり，他方，投資仲介業者に対し，それぞれの特有の必要性に応じてその解決手段を作り出す自由を提供することであると述べ，かつ，SEC が，Reg. S-P を修正し，かつ新しい執行のアプローチを採用することにより，この目標を達成できると主張している。具体的には，以下のような修正を提案している。

（1）要件

提案された Reg. S-P におけるもっとも重要な変更は，次のように，現

(26)　Gregg Moran, The SEC' Data Dilemma: Adressing a Modern Problem by Encouraging Innovation, Responsibility, and Faieness, 96 Neb. L. Rev. 482-483 (2017).

在の「合理的に企図された基準」から「忠実性の基準」に置き換えていることである。

「投資に関する仲介業者は，忠実に消費者の記録および情報の保護のための管理上，かつ，技術的，物理的な Safeguard を説明する書面による政策および手続を考慮し，かつ，採択しなければならない。これらの政策を実現するにあたって，投資を行う仲介業者は，以下のことを追求しなければならない。

①消費者の記録および情報の安全性，秘密保持を確実にすること

②消費者の記録および情報の安全または誠実性を予期される脅威または危険に対抗して，保護すること。

③結果として，顧客に生じた大きな損害または迷惑をもたらすような顧客の記録または情報に対する未授権のアクセスまたは利用から保護することである。」

なお，同修正提案において，大義を定めているが，忠実性については以下のように定めている。「忠実という文言は，消費者のデータあるいはプライバシーを保護するという目標に対する信念または目的における誠実さおよび忠実さを含む心の状態を意味する。」

（2）更新する義務

さらに，同修正提案は，「すべての投資仲介業者は，採択された政策および手続き（この項目において，説明された計画を含む）を維持するための忠実に企図された計画を採択しなければならない。」という，政策および手続きを更新する義務を定める。

（3）帳簿保管義務

修正提案は，投資仲介業者に対して政策および手続きの厳格な帳簿保管義務を課す。もし，投資仲介業者が考慮された政策を採択する場合，その記録において，情報の主要な部分を含むよう事業者に対して要求している。

第１に，記録は，その政策および手続を最初かつ最終的に採択されたものについて説明しなければならない。第２に，記録は，政策および手続の最終的な Version を採択する理由を詳細に説明しなければならない。第３に，記録はいかに投資仲介業者が履行する計画を立てているかについて，説明しなければならない。

（４）新しいルールの執行の意義

当該学説は，新しいルールの執行の意義を次のように説明している。

新しいルールは，現在の「合理的に企図された基準」から「忠実性の基準」に置き換えていることにより，投資仲介業者の政策および手続が合理的であったか否かの事後的決定を取り除き，それに代えて，投資仲介業者が良い政策および手続を開発しようとする誠実な試みを行っていたかどうかに焦点を転換している。

さらに，新たなルールの下で，幾つかの，より肯定的な結果がもたらされると述べられている。第１に，同ルールは，投資仲介業者が満たさなければならない要件を明確にすることにより，SEC が望む法令遵守のタイプを推進することになる。投資運用業者は，それぞれに特有のリスクや状況に適合した政策および手続を開発する自由が与えられるというインセンティブを持つことになる。第２に，新たなルールは，厳格な帳簿作成要件を伴っている。その要件において，投資仲介業者は，考慮したすべての政策および手続に関する記録を保存しなければならないとしている。SEC が証拠となる当該記録の審査により，投資仲介業者が忠実に行動したか否かを判断することができることになる。

第５節　米国投資顧問協会の倫理規程

１　概要

SEC は，投資顧問法204条の下で，すべての登録投資顧問に対して倫理

規定を採択することを要求する投資顧問法規則204A-1（以下，「倫理規程規則」）を制定している。倫理規程規則（a）項は書面による倫理規程において少なくとも以下の５つの事項を含めなければならないと定めている。

①業務執行基準――投資顧問の「被監督者（supervised persons）」に対して義務づける業務執行基準。かかる基準は当該投資顧問および投資顧問の被監督者の受託者責任を反映したものでなければならない。

②適用される連邦証券法の遵守――被監督者がすべての適用される連邦証券規制を遵守すること義務づける規定。

③被監督者の個人的な証券取引および持分残高の報告・審査義務――投資顧問が定期的にすべての被監督者に対し，その個人的な証券取引および持分残高を報告することを命じ，かつ審査することを命じる規定。

④被監督者の倫理規程規則違反の報告義務――被監督者に対し，倫理規程において法令順守担当主任役員がすべての倫理規程規則違反を受領すると定めるときは速やかにすべての倫理規程規則違反を法令順守担当主任役員に報告し，または倫理規程規則において別の者を指名しているときは，その者に報告することを命じる規定。

⑤被監督者による倫理規程およびその修正の謄本の提供――投資顧問に対し，被監督者の各各に倫理規程およびその修正の謄本を提供することを命じ，かつ，被監督者に対し，当該謄本の受領を承認する書面を投資顧問に提出することを命ずる規定。

2　投資顧問倫理規程ための最良の慣行（Best Practices for Investment Adviser Code of Ethics）

2004年７月２日に，SECは，投資顧問法204条の下で，すべての登録投資顧問に倫理規定を採用することを要求する投資顧問法規則204A-1を採択した。米国投資顧問協会は，同規則を遵守するために，「投資顧問倫理

規程ための最良の実務慣行（Best Practices for Investment Adviser Code of Ethics)」というガイドラインを策定し，会員に推奨している。同ガイドラインは，以下に述べるように，投資顧問法規則204A-1によって要求されている事項を反映している。

（1）まず，ガイドラインのPart 3のG項において営業行為の基準として次のように定める。

秘密保持（confidentiality）

すべての秘密保持の規定は，顧客の証券の保有の状況および財務状況に対する情報が，秘密にされなければならないという基本的な受任者としての前提から始まるべきである。

（i）投資顧問の義務

投資顧問協会は，倫理規程が，次の規定を含むことを推奨している。すなわち，投資顧問は顧客の身元，財務状況，証券保有，ならびに投資顧問によって顧客に提供される助言を含む顧客に関する全ての情報を厳格に秘密にしなければならない旨を定める規定である。

（ii）被監督者の義務

内部者取引防止のための手続きの一部として，またはその手続きの補足として，投資顧問は，顧客のため，またはその他の合法的な事業目的のために証券取引を執行するのに必要な場合を除いて，顧客に関する全ての重要な非公開の情報，顧客のために投資顧問によって行われた証券投資，予定されている証券取引に関係する情報，投資顧問の取引戦略に関する情報を投資顧問の外部の者に開示することを被監督者に禁止している。

a 保有状況の開示

ある投資顧問は，その倫理規定の中で，顧客，コンサルタントまたは将来の顧客の請求に応じて，ファンドまたは投資モデルのポートフォリオにおける持分状況を開示する時期を規制する規定を含んでいる。当該規定は，

ある顧客が，その他の顧客より早くに，そのような情報を得ることができないということを確実にし，かつ，当該情報が，投資顧問の取引戦略に影響を与えるという意味においてもはや重要でないことを確実にすることが企図されている。投資顧問は，また，コンサルタントに対して，秘密保持契約を遵守し，かつ，提供される情報に基づいて取引を行わないという合意を要求している。

（iii）internal wall

投資顧問会社の規模および性質によっては，投資顧問会社は，当該投資顧問会社の内部において，アクセスできない者に対して，顧客および証券取引に関する非公開の情報を開示するということを access person に禁止することを望む。同様に，関係会社を有する投資顧問会社は，被監督者に対して，関係会社によって雇用されている人々が，情報共有することを禁止する規定を定める。但し，例外として，合法的な営業目的の場合は除く。

（iv）物的安全性（physical security）

少数の投資顧問会社は，この倫理規定において，物的安全性を論じている。たとえば，Privacy Policy は，重要な非公開情報を含む書類が秘匿されるべきであるとする。また，そのような情報を含むコンピータファイルに対するアクセスは，制限されるべきであると述べている。

（v）Regulation S-P

少数の投資顧問会社は，秘密保持の条項の下において，Reg. S-P の Privacy Policy を相互に引用している。そのような規定は，投資顧問会社が倫理規定の中に加え，または参照する当該投資顧問会社の Private Policy を遵守することを被監督者に命じている。

Reg. S-P は，投資顧問の秘密保持の基準の一部分のみをカバーしている。Reg. S-P は，個人および個人情報のみに適用される。投資顧問の顧客の情報を秘密にするという受任者の義務は，投資顧問会社の顧客の全て

の情報に拡張されている。

（2）ガイドラインの Part 4 において，報告の要件について次のように述べている。

ある投資顧問会社は，access person に対して，その取引および持分の報告書が，秘密にされることを保証する規定を定めている。倫理規定の条項を執行するために必要な程度または，政府の機関から情報の請求に応ずるために必要な程度は除外される。

（3）ガイドラインの Part 7 では，報告の違反について次のように述べている。

倫理規定は，すべての被監督者に対し，投資顧問会社の倫理規定の違反を迅速に法令遵守担当主任役員等に報告することを要求しなければならないとしている。

投資顧問は，当該報告を法律によって認められる程度において秘密のものとして処理し，迅速かつ適切に調査することが望まれる。同様に，投資顧問が報告書を匿名で提出することを認めることができる。

第6節　個人情報窃盗の Red Flags Rules

（1）概説

2013年4月，SEC は，個人情報窃盗の Red Flags Rules（Regulation S-ID）[(27)] を採択した。

2014年早期において，SEC は，投資助言の領域におけるサイバーセキュリティに焦点を当てることを宣言した。2014年3月に，SEC は，このト

(27)　17 C.F.R. pt. 248.201: see Inv. Adv. Act Rel. No. 3582, 2013 (May 20, 2013).

ピックに関して4つのパネルの円卓会議を実施し，データの保護および個人情報窃盗の脆弱性を含む議論が行われた。SEC コンプライアンス検査局（OCIE）は，サイバーセキュリティのリスクおよび最良の業務に焦点を当てた詳細なアンケートを投資顧問に対し送付し，かつ，この分野が重要な優先事項であることを示した。

2015年4月，SEC の投資運用部局は，登録投資会社および登録投資顧問に対するサイバーセキュリティ・ガイダンスを公表した(28)。SEC のスタッフは，いかにして投資顧問がサイバーセキュリティのリスクに対応するために試みるべきかについて多くの事項を推奨した。すなわち，①脅威を管理するガバナンスの構造，センスティブ情報の目録および投資顧問の情報テクノジロジー・システムの脆弱性に対する定期的なアセスメントを行うこと，②脅威を防御し，探知し，かつ対応する戦略を構築すること，③役員および従業員に対する適切な訓練を伴う書面化された政策および手続を実行することなどである。

（2）Red Flags Rules の概要

個人情報窃盗の Red Flags Rules は，SEC に登録され，または登録されることが要求される特定の投資顧問を含む SEC の規制対象者に対して，個人情報窃盗のリスクに対応するためのプログラムを確立することを要求するルールおよびガイドラインを含んでいる。そのプログラムは，次のことを企図した政策および手続を含まなければならない。すなわち，①個人情報窃盗の red flags に関係するタイプを確認すること，② red flags の出現を探知すること，③red flags に適切に対応すること，および④個人情報窃盗のためのプログラムを定期的に更新することである。当該ルールに服する各投資顧問は，そのガイドラインを検討し，適切な部分をそのプログ

(28) IM Guidance Update No. 2015-02 (April 2015).

ラムに含めなければならない。当該ルールは，プログラムの承認（投資顧問会社の取締役会または取締役会内部の適切な委員会の承認）および運用に関する要件，ならびにサービスの提供者の訓練および監視を含んでいる。

登録投資顧問は，当該投資顧問が当該ルールにおいて定義されている「金融機関」または「債権者」であるならば，当該ルールに服する。また，当該投資顧問は，もし当該投資顧問がなんらかの「適用される口座」を維持するならば，個人情報窃盗に対するプログラムを採択しなければならない。「適用される口座」は，主として，個人，家族または家計の目的のために維持される口座を含む。それらの口座は，複数の支払または取引を許可することを企図されたものである。また，それらの口座には，顧客に対する合理的に予見されるリスク，ならびに，金融機関もしくは債権者の安全性もしくは財務の健全性に対するリスクが存在する。そのリスクは，財務上，運用上，法令遵守上，名声もしくは訴訟に関するリスクを含んでいる[(29)]。例えば，登録投資顧問は，以下のような場合には，金融機関の定義に該当し，個人情報窃盗に対するプログラムを採択することが要求される。すなわち，当該投資顧問が，個人の顧客の口座または当該投資顧問が管理するファンドの投資家の口座から第三者に対し支払うこと，もしくは取引の指図権限を有している場合，または投資顧問が個人の顧客または当該投資顧問が管理するファンドの投資家の代理人として行動する場合である。同様に，登録投資顧問は，以下のような場合には，「債権者」の定義に該当し，個人情報窃盗に対するプログラムを採択することが要求される。すなわち，もし当該投資顧問が，資本の拠出または引受けを橋渡しするために，個人のファンドもしくは口座に資金を融資する場合である。

(29)　17 C.F.R. § 248.201(b)(3).

第２章　SEC による行政処分事例

以下において７件の SEC による投資運用業者に対する行政処分事例を紹介する。

分類しておくと，①②③④は，顧客情報の漏洩事件であり，Reg. S-P の Safeguard Rule の違反事件である。⑤は，Reg. S-P のオプトアウトルールの違反事件である。⑥は，委任状勧誘に関する情報の漏洩の事件であり，⑦は顧客情報の漏洩について，Regulation S-ID が適用された事案である。

【顧客情報を保護するための合理的な書面による政策および手続きを怠った事例】

①　*In re* LPL Financial Corporation 事件(30)

本件は，登録証券会社かつ登録投資顧問である被審人 LPL 社による Reg. S-P のセーフガードの違反から生じたものである。Safeguard Rule は，証券会社および登録投資顧問に顧客の情報を保護すること要求している。LPL 社は，支店において，顧客の情報を保護するために十分な安全管理を行っておらず，2006年当初にそのことを認識していたにもかかわらず，安全性の手段を含む適切な管理を行うことに失敗していた。これにより，顧客の情報は，授権されていないアクセスの攻撃を受けやすい状態であった。2007年７月中頃から2008年９月の間，LPL 社は，授権されていない LPL 社の登録された幾人かの代理人は，顧客の口座にアクセスを行い，取引を行おうと試みた。当該コンピュータシステムにおけるセキュリティ違反を生じた。ハッキング事件において，LPL 社は，増加されたセキュリティ手段を実行することを怠り，Reg. S-P によって，要求されている政策及び手続を採択することを怠った。LPL 社は，顧客口座にお

(30)　*In re* LPL Financial Corporation, Inc., Inv. Adv. Act Rel. No. 2775, 2008 SEC LEXIS 2930 (Sept. 11, 2008).

ける違反を探索し，損害を与えた。それにも拘らず，LPL 社の失敗は，消費者情報が盗まれ，なりすまし（identity thieve）を受けやすい状態にしていた。LPL 社のセキュリティは，脆弱であった。

SEC は，LPL 社が，1934年証券取引所法15条 b 項，同法21条 c 項ならびに投資顧問法203条 e 項および同条 k 項，Reg. S-P の Rule 30(a) に違反したと認定し，LPL 社に対し27万5000ドルの民事制裁金を課した。

（本審決の分析）

投資顧問が運営していたオンラインサービスの管理が杜撰であったために顧客情報が漏洩したことが，顧客情報を保護するための合理的な書面による政策および手続きを怠ったこととなり，Reg. S-P の Rule 30(a) 違反が認定された事例である。

問題とされたのは，①登録代表者のパスワードは，ストロングパスワードという業界の基準を満たしていなかったこと。当該パスワードが，長さ，英数文字，文字のコンビネーションを満たしていなかったこと，②パスワードを一定期間後変更することを行わなかったこと，③ユーザーが，自身のパスワードを変更することが出来なかったこと。④不成功なログインの試みに関係して，自動的なロックアウトが存在しなかったこと。さらに，300人の LPL の情報テクノロジー担当の従業員は，ブランチネットのパスワードのリストにアクセスが可能であったこと。そして，多くの退職した従業員は，退職する前に，そのようなリストにアクセス出来たこと，⑤ブランチネットの不活動に関して，自動的なセッションのタイムアウトは，８時間をセットしていたが，類似のアプリケーションに対して，その他の金融機関によって用いられたものよりも長すぎたことである。

② *In re* Commonwealth Equity Services, LLP 事件(31)

本件は，登録証券会社および投資顧問である被審人である Commonwealth 社の顧客情報を保護することを意図した政策及び手続を採用することを要求する Reg. S-P の Rule 30(a) の違反によって生じたものである。関連する期間の間，Commonwealth 社は，登録代表者が，インターネットおよびトレディーング・プラットホームにおいて，顧客口座にアクセスするため用いたコンピュータにアンチウイルスソフトウェアを維持するということを推奨したが，要求していなかった。その結果，許可されないアクセスに対して，脆弱な状態におかれていた。さらに，Commonwealth 社は，コンピュータのセキュリティの手段を適切に審査さるための手続きを定めていなかった。特に，Commonwealth 社の内部監査人は，アンチウイルスソフトウェアがインストールされているか否かを確定するため，支店のコンピュータを監査しなかった。また，Commonwealth 社は，支店の監査中にカバーされていない潜在的なコンピュータセキュリティの問題について，点検する手続きを行っていなかった。あるいは，Commonwealth 社の登録代表者が，コンピュータに関連した援助を求めて，同社の情報テクノロジーヘルプデスクと接触を試みた際，当該手続きを設けていなかった。

2008年10月，許可を受けていない侵入者が，コンピュータウイルスを使用することにより，Commonwealth 社の登録代表者のログイン認証情報を取得し，それにより，同社のイントラネットにアクセスした。侵入者は，Commonwealth 社の顧客口座の代表者の368件のリストにアクセスした。そのリストは，特定の顧客の口座情報を含んでおり，侵入者は，

(31) *In re* Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network, Inv. Adv. Act Rel. No. 2929, 2009 SEC LEXIS 3363 (Sept. 29, 2009).

Commonwealth 社の清算ブローカー・ディーラーの調査の前に，かつ，将来の取引を阻止される前に，当該口座において，８つの許可されていない買付の注文を行った。Commonwealth 社は，金銭上の損害は免れたが，その懈怠は，侵入者が代表者の368の顧客口座に関係して，特定の顧客口座にアクセスすることを許した。

上述の行為の結果，被審人である Commonwealth 社は，Reg. S-P の Rule 30 に故意に違反し，取引所法15条 b 項，21条 c 項，投資顧問法203条 e 項および203条 k 項に違反したとして，SEC は，被審人に10万ドルの民事制裁金の支払いを課した。

（本審決の特徴）

本件では，ハッカーが，投資運用業者の登録代表者のログイン認証情報を獲得した。当該ハッカーは，登録代表者の特定の額を超えるキャッシュバランスのある顧客口座に対する調査を始め，顧客口座の名前，番号，類型，純資産，キャッシュバランス等の368の顧客口座のリストを作り上げ，社会保障番号の最後の四つの番号にアクセスした。当該ハッカーは，確認された368人の顧客の内，８人の口座において，１社の公開会社の普通株式に対して，授権されていない18個の買付の注文を行おうと試みた。このような侵入を許した原因は，つぎの点であった。すなわち，①投資運用業者が登録録代表者に対して，インターネットおよびトレディーング・プラットホームにおいて，顧客口座にアクセスするため用いたコンピュータにアンチウイルスソフトウェアを維持するということを推奨したが，要求していなかった。かつ，投資運用業者が，コンピュータのセキュリティの手段を適切に審査さるための手続きを定めていなかった。特に，投資運用業者の内部監査人は，アンチウイルスソフトウェアがインストールされているか否かを確定するため，支店のコンピュータを監査しなかった。また，

投資運用業者は，支店の監査中にカバーされていない潜在的なコンピュータのセキュリティの問題について，点検する手続きを行っていなかった。

論

説

③ *In re* RT Jones Capital Equities Management 事件(32)

登録投資顧問である被審人の RT Jones 社は，8400名の顧客の口座を運用しており，４億8000万ドルの資産の運用を任されていた。同社は，顧客の資産を保管していない。本件は，Reg. S-P の Rule 30(a) に違反して，顧客の記録および情報を保護することを合理的に企図した書面による政策および手続を採択することを怠った。少なくとも2009年９月から2013年７月の間，RT Jones 社は，第三者がホストとなったウェブサーバーに顧客およびその他の者の個人が特定される詳細な情報を保管していた。当該保管に関して，当該情報の安全性と秘密保持ならびに予期される脅威または許可されていないアクセスから当該情報を保護することに関する書面による政策および手続を採択していなかった。2017年７月，同社のウェブサーバーは，許可されていない侵入者によって攻撃された。当該侵入者は，アクセスする権利を獲得し，RT Jones 社の何千もの顧客に関するアクセス権と COPY 権を取得した。当該攻撃の結果，RT Jones 社の顧客を含む10万人以上の個人情報が盗まれた。

RT Jones 社は，投資顧問法203条 e 項，同条 k 項，Reg. S-P の Rule 30 (a) に違反したと認定され，75000ドルの民事制裁金の支払いを命じられた。

（本審決の特徴）

被審人は，第三者がホストとなったウェブサーバーに顧客およびその他

(32) *In re* R. T. Jones Capital, Advisers Act Rel. No. 4204, 2015 SEC LEXIS 3909 (Sept. 22, 2015).

の者の詳細な，個人が特定される情報を保管していた。当該保管に関して，当該情報の安全性と秘密保持ならびに予期される脅威または許可されていないアクセスから，当該情報を保護することに関する書面による政策及び手続を採択していなかった。その結果，ハッカーにより，数千の顧客を含む10万人以上の個人情報が，盗まれた。問題とされた点は，顧客の個人情報を保護する政策および手続において，定期的なリスク評価を行うこと，顧客の個人情報を含むウェブサーバーを保護するため FireWall を採用すること，当該サーバーに保管されている顧客の個人情報を暗号化すること，あるいは，サイバーセキュリティの事件に対応するための手続きを確立しなかったことであった。

④ *In re* Morgan Stanley Smith Barney LLC 事件(33)

被審人は，モルガンスタンレーの完全子会社であり，登録証券会社兼投資顧問である Morgan Stanley Smith Barney LLC（以下，MSSB 社という。）である。MSSB 社は，2014年，12月17日にルーティンのインターネットスウィープ（一斉点検）を通じて，データの漏洩を発見した。MSSB 社は，同社の従業員であった Galen Marsh（以下，Marsh という。）によって，生み出された特定のデータをインターネット情報と比較した後，データの漏洩の源であると確認した。2014年11月，MSSB 社は Marsh に聞き取り調査を行った。Marsh は彼の顧客の秘密情報を保管デバイスにアクセスしてダウンロードしたことを認めた。横領されたデータは，顧客のフルネーム，電話番号，住所，口座番号，口座残高および証券持分であった。Marsh はインターネットにデータを転送したことは否認した。Marsh の個人のサーバーにおいて科学捜査の分析は，第三者が個人のサーバーにハッ

(33) *In re* Morgan Stanley Smith Barney LLC., Investment Advisers Act Release No. 4415, 2016 SEC LEXIS 2142（June 8, 2016）.

キングし，Marsh がポータルからダウンロードした顧客の秘密情報を得ていたことを示していた。盗まれた情報の大部分は，仮想通貨のスピードコインを用いた支払いのために少なくとも 3 個のインターネットのサイトに掲示されていた。MSSB 社は，Safeguard Rule に違反した。なぜなら，MSSB 社の政策および手続は，限定された従業員が合法的なビジネスの必要性がある場合にのみ，顧客の秘密情報にアクセスする権限が付与されることをしていなかったこと，そのような権限付与のモジュールの有効性を監査し，かつ，検査することを行わなかったためであった。

結果として，MSSB 社は，Reg. S-P の Rule 30(a) に故意に違反し，証券取引所法15条 b 項，21条 c 項，投資顧問法203条 e 項，同条 k 項に違反したとして，100万ドルの民事制裁金を支払うよう命じられた。

（本審決の特徴）

登録証券会社兼投資顧問の従業員が当該会社の保有するポータルから顧客情報を盗み出し，当該従業員の個人のポータルにダウンロードした。その後，ハッカーにより当該従業員の個人のポータルから顧客情報を盗み出された。問題とされたのは，①被審人が，従業員に対して被審人のポータルを通じて，利用可能な報告書に関して，アクセスの制限を行っていなかったこと，②被審人が，少なくとも10年前に創設されて以来，授権されたモジュールの監査および試験を行っていなかったこと，および③被審人が，疑わしい活動の確認を行うためのポータルのユーザー活動を監視していなかったことである。

⑤ *In re* Maximillian Santos 事件(34)

登録証券会社および投資顧問の登録代表者である Santos（被審人）は，顧客の認識なくまたは同意を得ずに，少なくとも14名の顧客口座に関する秘密情報を外部の第三者と共有していた。当該第三者は，以前，本件投資顧問会社の登録代表者であった。当該第三者は，2005年に合衆国の証券取引協会の懲戒手続きの後，同社を退職した。Santos は，当該社外の第三者と口座を引き継ぎ，当該第三者と個人的または専門家としての関係を維持していた。Santos は，特定の株式の口座の持分状況，キャッシュバランス，特定の取引活動から成る情報を主として，彼の個人的 E-mail のアカウントを通して，共有していた。さらに2012年から，2013年の間に，Stantos は，個人的な E-mail のアドレスを公的なビジネス，および顧客の口座にサービスのために用いており，電話の指示を送り，株式の調査レポートおよび顧客への株式持分を含めていた。

少なくとも，2005年から，2012年まで，Stantos は，14人の顧客口座に関係する情報を社外の第三者と共有していた。証券会社によって提供される E-mail の代わりに個人的な E-mail を使用して，Santos は他の非公開情報における特定の取引活動を顧客の同意を得ずに，会社の関係しない第三者に対して，情報を送付していた。Santos が顧客の秘密情報を共有する第三者は，以前に証券会社の登録代表者として勤務していたが，NASD の仲裁人が，顧客の口座において，無断売買を行ったということを認定した後，当該証券会社を退職した。当時，Santos は，社外の第三者の口座の大部分を承継した。社外の第三者は，当該証券会社を退職した後，未公開株式の持分の取引を追求した。関連する期間の間，社外の第三者は，定期的に Stantos に対して以前の顧客の情報を要求した。

(34) *In re* Maximillian Santos, Inv. Adv. Act Rel. No. 4346, 2016 SEC LEXIS 848 (February 29, 2016).

Santos は，社外の第三者と連絡するに際して，会社の E-mail システムを用いて，第三者の名前を用いるということを避けるため，秘密の顧客情報を連絡することを含めて，自らの個人的 E-mail を慎重に用いた。証券会社が，会社のコンピュータを通じて，E-mail のアカウントのアクセスを阻止したことを知ったとき，Santos は，事務所にいる限り，携帯電話から，彼の個人的 E-mail にアクセスした。この期間中を通じて，Santos は，顧客の口座についての情報を彼の勤務先の E-mail から彼の個人的 E-mail に送付した。そして，その情報には，株式の持分状況や，少なくとも一度は，顧客のパスポートのコピー情報を含んでいた。彼の自分自身の E-mail のデータのセキュリティを防衛するに際して，彼は用心していなかった。

Reg. S-P の Rule 7(a)(1) および 10(a)(1) は，証券会社が明確かつ明白なオプトアウトの通知および情報を開示する前にオプトアウトする合理的な機会を提供していないという場合を除いて，関係のない第三者に対して，顧客の非公開の個人情報を開示することを禁止している。上記の行為の結果，Santos は，オプトアウトする権利を正確に説明した顧客への明確かつ明白な通知を怠ったにもかかわらず，顧客の非公開の個人情報を関係を有しない第三者に開示したゆえに，証券会社は，Reg. S-P の Rule 7(a)(1) および 10(a)(1) の違反を犯した。

Santos は，証券取引所法15条 b 項および21条 c 項および投資顧問法203条 f 項，投資会社法 9 条 b 項に違反したとされ，被審人の Santos は，Reg. S-P の Rule 7(a)(1) および 10(a)(1)，取引所法規則 Rule 17(a)(1) および 17(a)-4(b)(4) に違反したとされた。

（本審決の特徴）

登録証券会社兼投資運用業者の登録代表者が，顧客の了解あるいは，同

意を得ずに，少なくとも14名の顧客口座に関する秘密情報を外部の第三者と共有していた。顧客は，Reg. S-P に従った開示についてのオプトアウトの通知を与えられず，登録代表者は他の非公開情報における特定の取引活動を顧客の同意を得ずに，証券会社に関係しない第三者に対して，情報を送付していた。このことが，明確かつ明白なオプトアウトの通知および情報を開示する前にオプトアウトする合理的な機会を提供していないという場合を除いて，関係のない第三者に対して，顧客の非公開の個人情報を開示することを禁止している Reg. S-P の Rule 7(a)(1) および 10(a)(1) に違反するとされた。

【委任状のアドバイザーである投資顧問の従業員による，委任状勧誘に関する情報の漏洩の事例】

⑥ ***In re* Institutional Shareholder Services Inc. 事件**(35)

被審人である登録投資顧問 Institutional Shareholder Services Inc（以下，ISS という）は，ウェブサイト情報やポートフォリオのリスクおよびパフォーマンスの分析の手段を提供する公開会社である MSCI の完全子会社である。Form ADV Part 2A において，ISS はその助言業務をフルサービスの委任状のアドバイザーであり，機関投資家に対して，より情報が与えられた委任状の議決権の決定を行い，複雑な議決権に関する手続きを管理し，かつ，利害関係者および規制者に対して，議決権行使に関して，報告を行うということを機関投資家に支援するというフルサービスの委任状のアドバイザーとして，助言業務を説明している。2007年から2012年の間，ISS のある従業員は，委任状の勧誘者に対して，ISS の機関投資家である株主が，委任状による議決権行使に関する情報を委任状の勧誘者に提供していた。委任

(35) *In re* Institutional Shareholder Services Inc., Inv. Adv. Act Rel. No. 3611, 2013 SEC LEXIS 1527 (May 23, 2013).

状の勧誘者は，議決権行使に関する情報と引き換えに，ISS の従業員に食事，高額なコンサートおよびスポーツイベントのチケット，飛行機の搭乗券を与えていた。ISS の顧客の委任状の議決権にアクセスできる従業員は，自宅，または仕事中に ISS の議決権行使のウェブサイトにログインすることにより，当該情報を収集していた。彼の個人的な E-mail のアカウントを委任状の勧誘者に対する議決権の情報を伝えるために用いていた。

ISS は，秘密の顧客情報の開示を禁止する倫理規定を有していた。そして，従業員に対して，秘密の顧客情報を従業員の個人的利益のため，それを用いて利益を得ることを禁止していた。しかし，ISS は，特定の ISS の口座の運用者に対して，贈り物と交換に ISS の顧客の秘密情報の共有を阻止することを合理的に企図した重要な政策および手続きを確立していなかった。

ISS は，同社の株主である投資助言を行う顧客の重要かつ非公開の委任状に関する議決権行使の情報を不正使用することを防止するために企図された政策および手続を確立し，維持し，執行することを怠ったため，204A 条に違反したとされた。

SEC は ISS に対して，投資顧問法203条 e 項，同条 k 項により，同法204条に違反する行為の停止命令を発するとともに，30万ドルの民事制裁金の支払いを命じた。

（本審決の特徴）

本件では，ISS の従業員が，委任状の勧誘者に対して，秘匿すべき委任状による議決権行使に関する情報を食事，高額なコンサートおよびスポーツイベントのチケットならびに飛行機の搭乗券などの贈り物と引き換えにもらしていた。また，ISS は，同社の特定の口座の運用者に対して，贈り物と引き換えに被審人の顧客の秘密情報の共有を阻止することを合理的に

企図した重要な政策および手続きを確立し，維持し，執行することを行っていなかったと認定された。

【顧客情報の漏洩を防止できなかったとして，Regulation S-P および Regulation S-ID に違反したとされた事例】

⑦ *In re* Voya Financial Advisors, Inc. 事件[(36)]**。**

被審人は，Voya Financial Advisor Association（以下，Voya という。）であり，証券会社および投資顧問として，SEC に登録していた。また，Voya の完全子会社である VFA という会社は，1300万の顧客および110億ドルの資産を運用していた。VFA は，独立した契約者の登録代表者であり，合衆国のネットワークを通じて，投資商品やサービスを提供していた。VFA は，1000人以上の従業員および3800人の嘱託職員を雇用している。

VFA は３人の代表者の口座において，不十分なサイバーセキュリティのコントロールおよびポータルの誤った運営により，３人の代表者の口座に対して，侵入者のアクセスを防止することができなかった。侵入者たちは，VFA の契約者の代表者のユーザーネームと Password をポータルにログインするために用いた。そして，VFA の顧客の少なくとも5600人にアクセスことができた。その結果，Voya の一人の顧客の個人情報を含むドキュメントを入手した。侵入者らは，また，顧客情報を利用して，Voya.com の新しい顧客の Profile を作成するため，顧客情報を用いた。Voya.com は，侵入者ら２名の個人情報および口座情報を提供するものであった。当該攻撃の結果として，顧客の口座から，資金および証券の許可されていない取引は行われなかった。

VFA は，2009年に書面化された情報漏洩の防止計画を採択したが，顧

(36) *In re* Voya Financial Advisors, Inc., Inv. Adv. Act Rel. No. 5048, https://www.sec.gov/litigation/admin/2018/34-84288.pdf (Sept 26, 2018).

客に対するリスクの変化に対応し，情報漏洩の防止計画を調査せず，更新も行わなかった。また，従業員に対して，適切な訓練も行わなかった。さらに，当該情報漏洩の防止計画は，VFA によって調査されたコンピュータの侵入のような Red Flag に対応する合理的な政策および手続きを含んでいなかった。

上述の行為の結果，VFA は，SEC に登録されたすべての証券会社および投資顧問が，顧客の記録および情報を保護するために合理的に企図された政策および手続きの採択を要求するという Reg. S-P の30条 a 号に故意に違反した。VFA は，また，対象口座を維持，管理している証券会社および投資顧問に対して，対象口座の開設，または，現存する対象口座に関連して，情報漏洩を調査し，防止し，軽減するための書面による情報漏洩の防止計画を策定し，実行することを要求する Regulation S-ID の Rule 201 に違反した。

（本審決の特徴）

被審人は，顧客の情報を防御するための適切な企図された政策及び手続きを執行し，Regulation S-ID に対応し，情報漏洩を防止する計画に基づいて，従業員や契約者を訓練することを怠ったことにより，Reg. S-P および Regulation S-ID に違反した。当該事件は，Regulation S-ID が2013年に採択されて以来，最初の執行事例であるとされる。

Safeguard Rule は，①書面による政策及び手続きが合理的に顧客の記録および情報の秘密保持を保証するということ，②顧客の記録および情報の保全性に対する予期された危険の脅威に対して，保護すること，③いかなる顧客に対しても重大な損害および問題を結果として生じせしめるような顧客の記録または情報に対する権限が与えられていないアクセスまたは利用から，保護することを企図されなければならない。

また，Regulation S-ID は，情報漏洩の防衛計画が以下のことを行うための合理的な政策および手続きを含むことを要求している。①情報漏洩の防衛計画に対して，Regulation S-ID が対象口座のため，関連性のある Red Flag を明記し，合理的な政策および手続きを挿入すること，②情報漏洩の防止計画の中に挿入された Red Flag を認めること，③情報漏洩の防止計画に従って，Red Flag に適切に対応すること，④情報漏洩の防止計画は，情報漏洩から顧客に対するリスクの変化を反映するため，定期的に更新することを保証する。

被審人は，上述の Rule に対応して，顧客情報を保護することを怠り，顧客情報を漏洩したことで違反が認められたのであろう。

第３章　我が国における投資運用業者の顧客情報保護と秘密保持義務

第１節　投資運用業者の民法上の善管注意義務

投費運用業者は顧客の資産運用に関し，守秘義務があると解する説があり，「投資一任会社の場合には，投資一任契約上で『秘密の保持』を規定しており（投費顧問業協会の契約サンプルどおりである場合），委任者の同意を得ない場合には，第三者への顧客情報（運用資産残高やパフォーマンスを含む）の伝達はできない。ここでいう第三者には投資顧問業者の親会社も含まれ，親会社へ顧客情報を開示する場合には，委任者に事前に承諾を得ていない場合，契約違反となる。」と述べている[37]。

日本投資顧問業協会が定める投資顧問契約のサンプルにおいて[38]，秘密の保持として，「第４条　乙（投資顧問業者）は，この契約に関連して知り

（37）　河村賢治＝西山寛＝村岡佳紀『投資顧問業の法務と実務』（金融財政事情研究会，2006年）377頁。

（38）　http://www.jiaa.or.jp/profile/pdf/kisoku/jogen3-190926.pdf.

えた甲（顧客）の財産状況その他の事情については，秘密を厳守する。

2 乙は，投資助言サービスの内容を第三者に洩らし，又は甲の承諾なくして甲の投資助言サービスを第三者と共有してはならない。」と定めている。

上述のサンプルと同様の規定が投資一任契約に定めがあれば，投資運用業者が顧客情報を漏洩することは，この条項に違反する。投資運用業者が行う投資一任契約は委任契約であると解されているので(39)，このような契約違反があれば，民法644条に規定する善管注意義務に違反することになる。

なお，銀行等の金融機関は顧客に対して秘密保持義務を負うと解されているが，その根拠については次のように議論が分かれている。すなわち，①信義則説，②商慣習説，③契約説，④法人情報と個人情報を区別する見解である。また，金融機関が顧客に対して負う秘密保持義務の根拠は，金融機関と顧客との間の契約（預金契約または貸付契約）に付随する信義則上の義務（付随義務）であると解するのが，民法に関する通説的理解と整合し，妥当であるとする見解がある(40)。

私見としては，投資運用業者は，顧客と投資一任契約という委任契約を締結しており，当該契約の中で投資運用業者の顧客への秘密保持義務を明文で設けている場合には，当該秘密保持義務を善良な管理者の注意をもって履行すべきであろうし，当該契約の中で投資運用業者の顧客への秘密保持義務を明文で設けていない場合には，投資一任契約に付随する信義則上の義務（付随義務）として秘密保持義務を負うと解するのが妥当であると考える。

---

(39) 神崎克郎＝志谷匡史＝川口恭弘『金融商品取引法』（青林書院，2012年）616頁。

(40) 浅井・前掲注(1)230-231頁。

第2節　金商法上の規制

金商法42条は，投資運用業者が顧客に対して忠実義務および善管注意義務を負う旨を定めており，投資運用業者の顧客情報保護の義務は同規定からも導かれるものと解される。また，以下に述べるように，金融商品取引業者等（投資運用業者を含む）による顧客に関する情報の秘密保持義務を防止する具体的な規定として，同法40条2号がある。

1　投資運用業者の忠実義務および善管注意義務

投資運用業者の顧客情報の秘密保持義務は，金商法42条に規定する投資運用顧客に対する忠実義務および善管注意義務からも導きだされると考える。

後述する本節の2の業務に関して取得した顧客に関する情報の適正な取扱いを確保するための措置を講ずる義務に関して述べるように，金融庁は，金融商品取引業者等（投資運用業者を含む）が，顧客に対して秘密保持義務を負っていることを当然の前提にしていると推測できる。投資運用業者が秘密保持義務に違反すれば，金商法42条の投資運用顧客に対する忠実義務および善管注意義務違反となると解することができる。

2　業務に関して取得した顧客に関する情報の適正な取扱いを確保するための措置を講ずる義務（金商法40条2号の顧客情報保護に関する「内閣府令で定める状況」）

金融商品取引業者等は，業務に関して取得した顧客に関する情報の適正な取扱いを確保するための措置を講じていないと認められる状況に該当することのないように，その業務を行わなければならず，かつ，業務の運営の状況が公益に反し，または投資者の保護に支障を生ずるおそれがあるものとして内閣府令で定める状況にあることのないように，その業務を行わ

なければならない（金商法40条２号）[41]。

同条２号の「内閣府令で定める状況」とは，金融商品取引業者等に関する内閣府令（以下，「金商業府令」という）123条１項において，顧客情報保護に関するものとして，次のように具体的に列挙されている。

①その取り扱う個人である顧客に関する情報の安全管理，従業員の監督および当該情報の取扱いを委託する場合には，その委託先の監督について，当該情報の漏えい，滅失または毀損の防止を図るために必要かつ適切な措置を講じていないと認められる状況（金商業府令123条１項６号）

②その取り扱う個人である顧客に関する人種，信条，門地，本籍地，保健医療または犯罪経歴についての情報その他業務上知り得た公表されていない特別の情報を，適切な業務の運営の確保その他必要と認められる目的以外の目的のために利用しないことを確保するための措置を講じていないと認められる状況（金商業府令123条１項７号）

③金融商品取引業者等が取得した顧客の財産に関する公表されていない情報その他の特別な情報（一定のものを除く）を，事前に顧客の書面による同意を得ることなく，当該金融商品取引業者等が委託を行う登録金融機関もしくは金融商品仲介業者に提供している状況または金融商品取引業者等が委託を行った登録金融機関もしくは金融商品仲介業者から取得した顧客の財産に関する公表されていない情報その他の特別な情報（当該登録金融機関または金融商品仲介業者が当該顧客の書面による同意を得ずに提供したものに限る）を利用して有価証券の売買その他の取引等を勧誘してい

（41） 当該条文に関する詳細な研究として，神田秀樹＝黒沼悦郎＝松尾直彦編著『金融商品取引法コンメンタール２』（商事法務，2014年）355-364頁〔志谷匡史〕，黒沼悦郎＝太田洋編『論点体系 金融商品取引法２』（第一法規株式会社，2014年）148-150頁〔濃川耕平〕，黒沼悦郎『金融商品取引法』（有斐閣，2016年）528-530頁を参照。

る状況（金商業府令123条１項18号）

④登録金融機関が取得した顧客の財産に関する公表されていない情報その他の特別な情報（一定のものを除く）を，事前に顧客の書面による同意を得ることなく，委託金融商品取引業者に提供している状況または委託金融商品取引業者から取得した顧客の財産に関する公表されていない情報その他の特別な情報（当該委託金融商品取引業者が当該顧客の書面による同意を得ずに提供したものに限る）を利用して有価証券の売買その他の取引等を勧誘している状況（金商業府令123条１項24号）

3　金融商品取引業者等向けの総合的な監督指針の「Ⅲ－2－3－1 顧客情報の管理」および「Ⅲ－2－4 顧客等に関する情報の管理」

金商法40条の規定に基づき，金融庁の定める金融商品取引業者等向けの総合的な監督指針の「Ⅲ－2－3－1 顧客情報の管理」において，金融商品取引業者は，顧客の属性等および取引実態を的確に把握し得る顧客管理態勢を確立することが重要であるとし，顧客カード等を作成した上で，顧客属性等の的確な把握および顧客情報の管理の徹底を求めている(42)。

同監督指針の「Ⅲ－2－4 顧客等に関する情報の管理」では，「顧客に関する情報は，金融商品取引の基礎をなすものであり，その適切な管理が確保されることが極めて重要である。そのうち特に，個人である顧客に関する情報については，個人情報の保護に関する法律（以下「個人情報保護法」という），金商業等府令，金融分野における個人情報保護に関するガイドライン（以下「保護法ガイドライン」という）および金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（以下「実務指針」という。）の規定に基づく適切な取扱いが確保され

(42)　金融商品取引業者は，顧客について顧客カード等により知りえた情報を他に漏らしてはならない（日証協・投資勧誘規則５条２項）。

る必要がある。」と述べている。さらに，「また，金融商品取引業者は，法人関係情報（金商業府令１条４項14号に掲げる法人関係情報をいう。以下同じ）を入手し得る立場であることから，その厳格な管理とインサイダー取引等の不公正な取引の防止が求められる。」と述べている。(43)

論説

金融庁は，金融商品取引業者が顧客に関する情報および法人関係情報（以下，「顧客等に関する情報」という）を適切に管理し得る態勢を確立することが重要であると述べ，多くの留意点を上げ検証すべきであると述べている。留意事項を大きく４つに分け，それぞれ細目を述べている。

（１）顧客等に関する情報管理態勢に係る留意事項

まず，当該留意事項に関して，以下の事を検証するとしている。

情報漏えい等が発生した原因を分析し，再発防止に向けた対策が講じられているか。更に，他社における漏えい事故等を踏まえ，類似事例の再発防止のために必要な措置の検討を行っているか。

また，顧客等に関する情報管理に係る監査に従事する職員の専門性を高めるため，研修の実施等の方策を適切に講じているか。

さらに，次の６個の細目を上げている。

①経営陣は，顧客等に関する情報管理の適切性を確保する必要性及び重要性を認識し，適切性を確保するための組織体制の確立（部門間における適切な牽制の確保を含む。），社内規程の策定等，内部管理態勢の整備を図っ

(43) 法人関係情報に関しては，以前，同監督指針の改正にあたってパブリックコメントに対する金融庁の考え方の一つとして，「法人顧客情報についてまで，法定されている個人情報管理並みの水準を求める趣旨でないと理解してよいか。」というコメントに対して，金融庁は，「個人情報を含まない法人顧客情報については，個人情報保護法等の直接の適用はありませんが，顧客に関する情報は，金融取引の基礎をなすものであり，適切に管理する必要があります。」と述べていた。平成22・６・４コメントの概要及びそれに対する金融庁の考え方２頁12番参照。

ているか。

②顧客等に関する情報の取扱いについて，具体的な取扱基準を定めた上で，研修等により役職員に周知徹底を図っているか。特に，当該情報の他者への伝達については，上記の法令，保護法ガイドライン，金融分野ガイドライン，実務指針の規定等に従い手続きが行われるよう十分な検討を行った上で取扱基準を定めているか。

③顧客等に関する情報へのアクセス管理の徹底（アクセス権限を付与された本人以外が使用することの防止等），内部関係者による顧客等に関する情報の持ち出しの防止に係る対策，外部からの不正アクセスの防御等情報管理システムの堅牢化などの対策を含め，顧客等に関する情報の管理状況を適時・適切に検証できる体制となっているか。

また，特定職員に集中する権限等の分散や，幅広い権限等を有する職員への管理・牽制の強化を図る等，顧客等に関する情報を利用した不正行為を防止するための適切な措置を図っているか。

④顧客等に関する情報の取扱いを委託（脚注によれば，「委託」とは，契約の形態や種類を問わず，金融商品取引業者が他の者に顧客等に関する情報の取扱いの全部又は一部を行わせることを内容とする契約の一切を含むとする。）する場合の取るべき措置に関するものである。

⑤顧客等に関する情報の漏えい等が発生した場合に，適切に責任部署へ報告され，二次被害等の発生防止の観点から，対象となった顧客等への説明，当局への報告及び公表が迅速かつ適切に行われる体制が整備されているか。

⑥独立した内部監査部門等において，定期的又は随時に，顧客等に関する情報管理に係る幅広い業務を対象にした監査を行っているか。

（2）個人情報管理に係る留意事項

①個人である顧客に関する情報については，金商業府令123条1項6号の規定に基づきその安全管理，従業者の監督及び当該情報の取扱いを委託する場合にはその委託先の監督について，当該情報の漏えい，滅失又は毀損の防止を図るために必要かつ適切な措置として，安全管理について必要かつ適切な措置，従業者の監督について必要かつ適切な措置，委託先の監督について必要かつ適切な措置が講じられているか。

②個人である顧客に関する人種，信条，門地，本籍地，保健医療又は犯罪経歴についての情報その他の特別の非公開情報（脚注で，その他特別の非公開情報とは，以下の情報をいうとしている。(a) 労働組合への加盟に関する情報，(b) 民族に関する情報，(c) 性生活に関する情報，(d) 個人情報の保護に関する法律施行令2条4号に定める事項に関する情報，(e) 個人情報の保護に関する法律施行令2条5号に定める事項に関する情報，(f) 犯罪により害を被った事実に関する情報，(g) 社会的身分に関する情報）を，金商業府令123条1項7号の規定に基づき金融分野ガイドライン5条1項各号に列挙する場合を除き，利用しないことを確保するための措置が講じられているか。

③金融商品取引業者が，クレジットカード決済による有価証券の売買の受託等について，例外的に認められている場合において，クレジットカード情報（カード番号，有効期限等）を含む個人情報（以下「クレジットカード情報等」という。）は，情報が漏えいした場合，不正使用によるなりすまし購入など二次被害が発生する可能性が高いため，金融商品取引業者は，上記①・②に加え，特に以下の措置を講じているか。

イ．クレジットカード情報等について，利用目的その他の事情を勘案した適切な保存期間を設定し，保存場所を限定し，保存期間経過後適切かつ速やかに廃棄しているか。

ロ．業務上必要とする場合を除き，クレジットカード情報等をコンピューター画面に表示する際には，カード番号を全て表示させない等の適切な措置を講じているか。

ハ．クレジットカード情報等を保護するためのルール及びシステムが有効に機能しているかについて，定期的又は随時に点検・立入検査を行っているか。

（3）法人関係情報を利用したインサイダー取引等の不公正な取引の防止に係る留意事項

①役職員及びその関係者による，有価証券の売買その他の取引等に係る社内規則を整備し，必要に応じて見直しを行う等，適切な内部管理態勢を構築しているか。

②役職員によるインサイダー等の不公正な取引の防止に向け，職業倫理の強化，関係法令や社内規則の周知徹底等，法令遵守意識の強化に向けた取り組みを行っているか。

③法人関係情報を入手し得る立場にある，金融商品取引業者の役職員及びその関係者による有価証券の売買その他の取引等の実態把握を行い，必要に応じてその方法の見直しを行う等，適切な措置を講じているか。

以上のように，金商法40条２号においては，金融商品取引業者等は，業務に関して取得した顧客に関する情報の適正な取扱いを確保するための措置を講じていないと認められる状況に該当することのないように，その業務を行わなければならないと定め，かつ業務の運営の状況が公益に反し，または投資者の保護に支障を生ずるおそれがある状況としてものとして内閣府令で個人情報および法人顧客情報が保護されていない状況を列挙している。

さらに，金融庁は，金融商品取引業者等向けの総合的な監督指針の「Ⅲ－

2－4 顧客等に関する情報管理態勢」において，「顧客に関する情報は，金融商品取引の基礎をなすものであり，その適切な管理が確保されることが極めて重要であると述べている。このような規制状況からみれば，金商法上，金融商品取引業者等（投資運用業者を含む）が，顧客に関する情報を適切に管理すべきということは，その前提として，金融商品取引業者等は，顧客に対して秘密保持義務を負うことを命じられていると考えられる。

（4）投資運用業者の弊害防止に関する重要な留意事項

顧客情報が漏洩した際の責任の所在について，金融商品取引業者等向けの総合的な監督指針 VI－2－2－3 では，投資運用業者の弊害防止に関する重要な留意事項が，次のように示されている。

①「社内管理体制」の整備

異なる種別の業務間における弊害防止措置として，業務内容に応じた弊害発生防止に関する社内管理体制を整備するなどの適切な措置が講じられているか。

②「非公開情報管理責任者」の設置

金商業等府令147条 2 号は，投資助言業務または投資運用業に関して，非公開情報（有価証券の発行者または投資助言業務および投資運用業以外の業務に係る顧客に関するものに限る。）に基づいて，顧客の利益を図ることを目的とした助言を行い，または権利者の利益を図ることを目的とした運用を行うことを禁止している。

当該「非公開情報」について，管理責任者の選任および管理規則の制定等による情報管理措置等が整備されているとともに，当該情報の利用状況の適正な把握・検証及びその情報管理方法の見直しが行われる等，情報管理の実効性が確保されていなければならない。

上述の留意事項は，金商法の委任を受けた総合的な監督指針によって要求されるものである(44)。ゆえに，実務上，すべての投資運用業者が，非公開情報管理責任者を設置し，社内管理体制や守秘義務規定の整備を行うことが望まれる。

第３節　個人情報保護法上の規制

個人情報保護法は，個人情報を取り扱う個人情報取扱事業者に対して，遵守すべき義務を定め，個人の権利利益を保護することを目的としている（同法１条）。

個人情報取扱事業者は，個人情報データベース等を事業の用に供している者と定義づけられており（個人情報保護法２条５項），投資運用業者は，個人情報取扱事業者に該当することになる。また，個人情報とは，生存する個人に関する情報であり（同法２条１項），法人に関する情報は同法の適用対象外である。

個人情報保護法，「個人情報の保護に関する法律施行令」および「個人情報の保護に関する基本方針」（平成16年４月２日閣議決定）を受けて，金融庁は，「金融分野における個人情報の保護に関するガイドライン」（平成21年11月20日金融庁告示63号）という指針を設けている。その後，金融庁は，「金融分野における個人情報の保護に関するガイドライン」平成29年２月を設けている（平成29年２月28日金融庁告示第１号）。平成29年２月28日金融庁告示第１号では，平成21年11月20日金融庁告示63号を「通則ガイドライン」と呼んでいる。平成29年２月28日金融庁告示第１号は，第１条の目的で，本ガイドラインは，通則ガイドラインを基礎として，個人情報の保護に関する法律第６条および８条に基づき，金融分野におけ

(44)　十市崇編『金融商品取引法の諸問題』（商事法務，2012年）150頁〔上林英彦〕「証券会社等における情報共有規制」。

る個人情報について保護のための格別の措置が講じられるよう必要な措置を講じ，および当該分野における事業者が個人情報の適正な取り扱いの確保に関して行う活動を支援する具体的な検討の指針として定めるものであると規定している。

通則ガイドラインでは，金融分野における個人情報取扱事業者が個人情報の適正な取扱いの確保に関して行う活動を支援するため，金融分野における個人情報の性質および利用方法にかんがみ，事業者の講ずべき措置の適切かつ有効な実施を図るための指針として，定めたものである（同指針１条１項）。

さらに，日本投資顧問業協会は，個人情報保護法47条１項の認定を受けた認定個人情報保護団体として同項各号にかかげる業務を実施している（「会員における個人情報の適正な取扱いの確保について」（平成17年５月25日理事会決議））。日本投資顧問業協会は，「個人情報の保護に関する取扱指針」を設けている（平成17年３月23日理事会決議））。同指針は，「個人情報保護法」，「個人情報の保護に関する法律施行令」，「個人情報の保護に関する基本方針」および「金融分野における個人情報の保護に関するガイドライン」等を踏まえ，会員の行う投資運用業または投資助言・代理業における個人情報の適正な取扱いを確保するために，会員が講ずべき具体的な措置等を定めるものである（同指針１条）。

お　わ　り　に

投資運用業者は顧客から様々な顧客情報を得ている。顧客は，そのような情報が，投資一任契約の目的のために用いられることを望む。投資運用業者は，投資一任契約上，顧客に対して，忠実義務および善管注意義務を負っている。投資顧問業者が顧客の利益を無視して顧客情報を自己の利益または親会社等の第三者の利益のために用いることは，忠実義務に違反す

る。また，投資運用業者は，顧客情報の杜撰な管理により，顧客情報が漏洩された場合には，善管注意義務違反となる。投資運用業者は，契約上，顧客に対し顧客情報を保護し，かつ秘密を保持する義務を負うが，金商法上も同様の義務が課されており，同義務違反に対しては，国の監督機関が監視している。また，個人情報保護法も，個人情報の保護の観点から，顧客情報の保護を図っている。それぞれの規制の総合的な運用により，実効的な投資運用業者の顧客情報の保護が達成されることが望まれる。

＜付記＞　本研究は，公益財団法人石井記念証券研究振興財団の平成30年度の研究助成の成果である。財団の助成により，本研究が行うことができた。支援を頂いた財団の方々に，この場を借りて，御礼申し上げる。

論

説

The duty of confidentiality of Investment Advisers who Perform Investment Management Business: The Study Based on the Comparison of Japan Law with U.S. Law

Hiroyuki USHIMARU

The purpose of this article is to clarify legal problems about the duty of confidentiality of investment advisers who perform investment management business and to investigate a solution. Thereby we can protect Japanese investors. The method of the study is to compare the law of U.S. with Japan.

Japanese investment advisers have a duty of confidentiality for their clients.

This duty derives from the duty of care (Article 644 of the Civil Law), the duty of care and the duty of loyalty (Article 42 of the Financial Instruments and Exchange Law) and the Act on the Protection of Personal Information.

The SEC adopted Regulation S-P to implement the requirement of Title V of the Gramm-Leach-Biley Act. The purpose of Regulation S-P is to protect the security and confidentiality of customer's nonpublic financial information. SEC has brought many enforcement proceedings against investment advisers accompanied by the issue of confidentiality in the United States. I introduce such enforcement proceedings in order to prevent illegal business of Japanese investment advisers and to regulate such business by the regulatory authority.

The SEC adopted Investment Advisers Act rule 204A-1. This rule promulgated under Section **204A**, provides that a registered **investment adviser** must establish and enforce a written code of ethics. I propose the revision of the Financial Instruments and Exchange Law to impose investment advisers the duty to establish a written code of ethics. Such code of ethics should include the duty of confidentiality. We clear up the duty of confidentiality for protection of investors.