［ディジタルエコノミー時代のサイバーセキュリティ―ディジタルトランスフォーメーション促進の基盤確立に向けて―］

⑤ フィンテックのセキュリティ

応般

岩下直行 | 京都大学

フィンテックと情報セキュリティとの関係

ここ数年，金融業界において，フィンテックという言葉が大流行している．金融庁はフィンテック相談窓口を設け，日本銀行はフィンテックセンターを創設し，大手銀行や地方銀行はフィンテック担当部署を相次いで設置した．フィンテックは一時的なバズワードの段階を乗り越え，もはや金融の一般用語として定着した感がある．

とはいえ，その意味するところは相変わらず曖昧だ．フィンテックは，「金融サービスを手掛けるベンチャービジネス」を指す言葉として普及し始めたのだが，日本の場合，伝統的金融機関が利用してきた情報技術がとても古いものであったため，それを見直して最新の技術に入れ替え，サードパーティの力を借りて顧客とのインタフェースを改善することもまた，フィンテックと呼ばれている．2017 年に相場が暴騰，社会的なブームを巻き起こし，国内で 360 万人の利用者を持つに至った仮想通貨も，広い意味のフィンテックに含まれる．新興国を中心に急拡大しているキャッシュレス決済もまた，フィンテックの一形態と解されている．

これらの共通項を拾い出せば，結局のところ，「インターネットを経由して金融サービスを改善する」という，割と普通の説明となってしまう．では，従来，伝統的金融機関が提供してきたインターネット・バンキングやインターネット証券取引と何が違うのか．それは，ベンチャーを含む新しい担い手が登場していること，UI/UX が従来のものとは大きく異なり，ユーザに新しい利便性を提供するものであることなどが特徴であろう．従来の伝統的金融機関によるインターネット取引は，伝統的な金融機関の支店店頭で提供される金融サービスをインターネットに乗せるというコンセプトであったのに対し，フィンテックは，まったく新しい利用方法を顧客に提供しようとしている．従来の金融の枠組みを越えて新たな価値を創造しようという仮想通貨の試みは，現時点で成功しているとは言いがたいが，その影響や今後の可能性は無視できない．

しかし，当然そういった変化が起これば，新たな情報セキュリティ上の脅威が発生し，新たな対策が必要となる．つまり，フィンテックのセキュリティが大切になるのである．

思えば，伝統的な金融業界は，DES 暗号の誕生当初から暗号技術の最も有力なユーザ業界であり，その後のトリプル DES，AES への乗り換えや，RSA 暗号の鍵長の伸長（512 → 1024 → 2048 bit），楕円曲線暗号の導入など，さまざまな局面で重要な判断を下してきた．しかし今や，そうした情報セキュリティ技術の変革を主導するのは，ベンチャー企業を含む IT 業界側に移ったようである．

インターネットとスマートフォンの普及は，利用者に新しい利用環境を提供し，オープンなネットワーク環境下でサービスを提供することが求められるようになった．もはや，金融業界に閉じた専用のネットワークを利用する金融取引のウェイトは低下しつつあり，インターネットとスマートフォンで完結する安価で新しい金融サービスが急速に普及している．新しいサービスは，当然新しい脅威を伴うが，インターネットやスマートフォンに利用されるセキュリティ技術が進化したこともあって，脅威を回避しつつ，利便性を最大限活用する方向でイノベー

ションが進んでいる．こうした中で，金融業務のセキュリティもまた，インターネットやスマートフォンを前提とするものに変わっていかなければならない．本稿では，こうした新しい金融であるフィンテックのセキュリティについて，その現状と課題を整理する．

銀行のオープン API 対応とセキュリティ

2017 年の銀行法改正で，オープン API（Application Programming Interface）への対応が金融機関の努力義務となった．それまで銀行が利用する情報ネットワークは，閉鎖的，閉域的な技術を前提としたものであり，その前提でセキュリティ対策も講じられてきた．しかし，フィンテックという言葉が定着する過程で，オープンなネットワークでの利用を前提として，従来の自前主義から，サードパーティの提供するシステム，サービスを上手に利用していくことが必要だという認識に，金融業界や規制当局も変わってきた．そのような対応を行う上で，銀行の API への対応は，必要不可欠なものと位置付けられ，法改正へと繋がったのである．

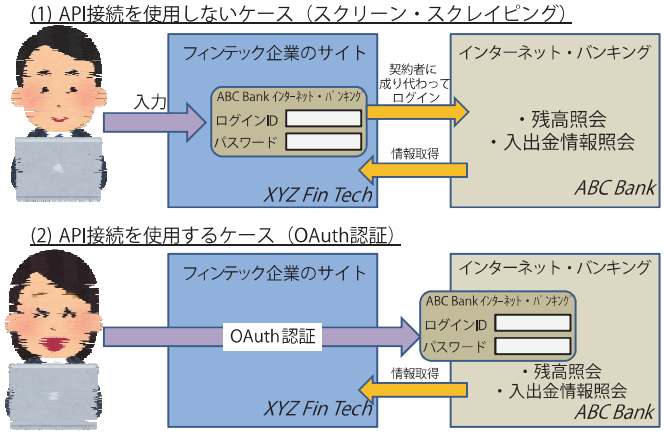
そもそも API は，現在のインターネット上で提供されている多くのサービスで実装され，我々はすでにその恩恵を受けている．たとえば，Gmail や Twitter，Facebook などのサービスは，あるサービスの利用者であることを利用して，ほかのサービスにログインすることができる仕組みを相互に持っており，それらは一般ユーザに広く利用されている．特にユーザの認証にかかる部分は OAuth 認証が使われているが，これと同じ技術を銀行のインターネット取引に採用しようというのが，オープン API 対応の柱となっている．

現在でも，PFM（個人金融資産管理）やクラウド会計などのフィンテック・サービスでは，銀行のインターネット・バンキングからの情報の取得が行われている．利用者がこのサービスを受けるためには，銀行の ID とパスワードなどの認証情報をフィンテック企業に預け，フィンテック企業が利用者に成り代わって銀行のサービスにログインする「スクリーン・スクレイピング」という手法が利用されている（図 -1 上）．

しかし，パスワードを第三者に預けることには抵抗もあり，情報漏洩のリスクもある．今後，広く銀行サービスの利用者がフィンテック企業との情報連携を進めていくためには，銀行側が API 接続に対応し，フィンテック企業からの OAuth 認証の要請に認可が与えられる仕組みとなっていくことが望ましい（図 -1 下）．

情報連携のための API を整備していけば，フィンテック企業側もシステム対応が容易となり，銀行サービスとの連携がよりスムーズに行えるようになる．こうした観点から，銀行業界とフィンテック業界の専門家が参加した全国銀行協会の WG において，銀行の API 接続に関する基本的な考え方が整理された．また，銀行法の改正により，API 接続は銀行の努力義務とされた．それにより，今後はその考え方に基づいて技術標準を整備し，実際に API 接続のためのシステム対応を行う局面に入っている．

オープン API への対応は，銀行法上は「努力義務」だから，対応するか否か，具体的にどのような情報



■図 -1　銀行とフィンテック企業との API 接続

を連携するのかは，各銀行の判断に任されることになる．とはいえ，銀行業界全体が，現在のレガシーにとらわれた状態から脱却するためには，オープンなネットワークでサードパーティのサービスを自由に受け入れられる仕組みに移行していくことが重要であり，そうした長期的ビジョンに基づいて，各銀行が対応していくことが望まれていた．

2018 年 3 月，138 先の金融機関が API 接続方針を公表した（図 -2）．82 先が，法人向けか個人向けかに限らず，参照系と更新系の双方について API を公開すると表明しており，逆にまったく対応の予定がないとした先は 9 先にとどまっている．これだけの金融機関が API 公開を表明したことの意義は大きい．今後は，API 接続の実用化を進め，顧客への利便性の向上に努めるほか，金融機関自身が利用する情報システムを，より新しい技術を受け入れるものとしていくことが必要であろう．

また，銀行が単にオープン API を利用可能としただけでは，システム対応コストの持ち出しになってしまう．新しいオープンな環境で，新しい技術を活用することで，銀行にとってどのようなビジネスが可能となるのか，フィンテック企業等との連携を通じた金融サービス向上とビジネス機会の拡大を実現していくための「ビジネスモデルの変革」が重要となる．

こうしたオープン・イノベーションとサイバーセキュリティを両立させていくことも，当然求められる．こう書くと何やら難しい課題のように聞こえるが，現在では多くの一般企業が，日々の業務の中でこの両立を実現している．銀行は長年にわたって特殊な閉鎖環境の中でビジネスを展開してきたため，オープンなネットワークへの接続を過度に恐れている面がある．サイバーセキュリティのリスクへの対応は当然必要とされることだが，すでに世の中で標準的となっている技術のメリットを享受するためにも，システムをよりオープンな環境の下で構築・運用し，生産性を高めていくことが，銀行にも要請される時代になったのだ．

API の公開といっても，現在，銀行が想定している開放度は必ずしも高いものではない．欧州における分類（図 -3）に従えば，日本の金融オープン API は，顧客に直接 API を開放する「Member 型」等ではなく，電子決済代行業者として一定の要件を満たした先のみを対象とする「Partner 型」である．

各金融機関は，詳細なチェックリスト等による事前の審査に基づいて，接続先である電子決済代行業者のセキュリティ管理体制の充足度合いを判断する仕組みである．従来の閉域型の銀行システムから一歩踏み出したにすぎないが，電子決済代行業者が提供する多様なサービスとの接続が可能となることは大きい．

仮想通貨のセキュリティを巡って

一方，同じフィンテックの重要な構成要素と位置付けられてきた仮想通貨とブロックチェーン技術に

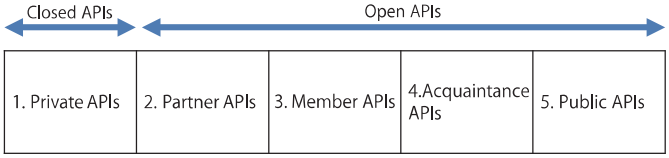
● 金融機関は改正銀行法に則り，2018年3月1日までに電子決済等代行業者との連携および協働にかかる方針（API接続方針）を公表したところ（施行日より2年以内でのオープンAPI導入にかかる体制整備の努力義務）．

▽金融機関（138先）のAPI公開見通し(※)　（2018年3月2日時点）

		個人向け		
		未定／対応予定なし	参照系のみ公開	参照系と更新系を公開
法人向け	未定／対応予定なし	9	4	20
	参照系のみ公開	0	13	3
	参照系と更新系を公開	3	4	82

（※）各金融機関の公表資料をもとに集計

（出典）日本銀行 金融高度化センター：IT を活用した金融の高度化に関するワークショップ報告書（第 3 期）（2018 年 8 月）
■図 -2　金融機関の API 公開見通し



（出典）Euro Banking Association : Understanding the business relevance of Open APIs and Open Banking for banks (May 2016)
■図 -3　API の開放度レベル

ついては，そのセキュリティが懸念される事態に陥っている．

仮想通貨とは，インターネット上で受け渡し可能であり，円やドルなどの法定通貨と交換したり，支払い手段として利用されたりする，独自の通貨単位を持つ特殊なディジタルデータのことを指す．2009年に出現したビットコインがその代表例である．ビットコインは，当初はきわめて安い価格で法定通貨と交換されていたが，2013年頃から値上がりし始め，2017年には約20倍に高騰し，注目を集めた．

2018年1月26日の午前0時，大手仮想通貨取扱業者，コインチェック社が顧客から預かっていた580億円相当の仮想通貨ネム（NEM）が何者かに不正に送金され，同社から流出する事件が起きた．同社は，10時間以上経ってから流出の事実を確認し，監督官庁である金融庁や警察に報告した．

仮想通貨の価格が大きく値上がりするとともに，仮想通貨を投資目的で購入する人の数も増加している．今回の事件の被害者，つまりコインチェック社を通じてネムを購入し，同社に預けていた顧客は26万人に上った．我が国でビットコインなどの仮想通貨に投資する人の数は，業者間の重複を調整しないベースで360万人に達する．なお，金融機関や機関投資家で仮想通貨に投資している例はほぼなく，投資しているのはほとんどが個人投資家である．

この不正流出が起こった原因はどこにあるのだろうか．報道によれば，コインチェック社は，顧客が購入した仮想通貨ネム580億円分を，インターネットに接続されたウォレットと呼ばれる装置で管理していた．仮想通貨をウォレットに入れていた，という言い方もするが，それは例え話であり，「価値のあるディジタルデータを記録媒体に書き込んでいた」わけではない．厳密にいえば，仮想通貨の実態は，インターネットにつながった世界中のコンピュータの中に書き込まれた膨大なディジタルデータ全体である．ウォレットには，その情報を書き換えるための秘密鍵が格納されていて，この秘密鍵を使って取引が行われる．

今回の盗難事件では，本来，部外者に知られてはならない秘密鍵を攻撃者に勝手に使われて，世界中のコンピュータの中の情報を書き換える指令が出された．その結果，580億円分のネムは，コインチェック社のアドレスから，犯人が用意したアドレスに送金されてしまったのだ．

つまり，今回の事件は，コインチェック社が580億円分の仮想通貨を，たった1つの秘密鍵で管理していたこと，その大事な鍵が不正に使われてしまうようなずさんな管理をしていたことが原因だった．コインチェック社は，ネム以外の仮想通貨はより厳格に管理していたという．ウォレットを複数に分けて異なる秘密鍵を格納することや，装置をインターネットに常時接続せず，必要な際にのみ，手動で接続することにより，不正に利用されるリスクを下げる対策が講じられていた．犯人は，そうした対策の講じられていなかったネムを狙って，攻撃を仕掛けてきたと考えられる．

仮想通貨の入門書には，「一人ひとりの取引情報が，世界中のシステムに書き込まれ，決して書き換えられない状態で保管されるから安全だ」という趣旨の説明が書かれている．しかし，最近は，仮想通貨の取引では交換業者に仮想通貨を預け入れるのが一般的になった．その場合，交換業者が管理するデータベースに自分のIDと残高が登録されるだけで，ブロックチェーンには何も書かれない．だから，たとえどんなにブロックチェーン技術が優れていたとしても，利用者の窓口となる交換業者が信頼できず，リスク管理やセキュリティ対策が十分でなかったなら，利用者が預けた資産は安全とはいえないのだ．

犯行当日，どのような取引が行われたのか，ネムのブロックチェーンの情報から調べてみよう（図-4）．この図において，NC3で始まるアドレスはコインチェック社が26万人の顧客から預かったネムを保管していた先であり，NC4で始まるアド

レスは，攻撃者が用意したものである．

1月26日の午前0時2分に最初の10単位のネムが送金され，その後，20分足らずの間に，523,000,000単位，約580億円相当が流出した．いまだに正体不明のこの犯人は，このアドレスからさらに別の複数のアドレスに送金し，自らが管理することになった約580億円分のネムを，少しずつインターネット上でほかの通貨と交換して資金洗浄を進め，まんまと逃げおおせてしまった．

今回の問題は，コインチェック社だけの問題ではない．仮想通貨交換業者においては，過去にも攻撃されて仮想通貨を盗まれた事例が数多く知られている．現在営業している交換業者の中にも，同じような問題を抱え，顧客からの預り資産をリスクにさらしている先がいるかもしれない．現在の仮想通貨業界は，統一的なセキュリティ基準も存在せず，経営体制やガバナンス，セキュリティ対策の充足状況に関する情報開示も行われていない．

我が国は，他国に先駆けて仮想通貨交換業者を規制する法律を施行し，業者の登録制度を運用してきた．しかし，それは資金洗浄やテロ資金調達を防止することが主眼であった．現在の仮想通貨法は，交換業者が多額の顧客資産を預かる存在であることを意識した，十分な利用者保護の仕組みを備えていない．法律制定時には想定されていなかった状況が生じている以上，それに対応した法改正を検討する必要があるだろう．業界も，信託や保険といった仕組みを活用して，自主的に被害を限定する取り組みを進めるべきである．また，セキュリティ対策の基準を制定し，ディスクロージャを徹底することにより，利用者の不安の払拭に努める必要がある．今回のような事件が再び起きないように，常に対策を最新のものとする工夫も必要である．

時刻	金額(XEM)	送金元	送金先
2018/1/26 8:26	800,000	NC3BI3DNMR2	[redacted]
2018/1/26 4:33	1,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 3:35	1,500,000	NC3BI3DNMR2	[redacted]
2018/1/26 3:29	92,250,000	[redacted]	NA6ISWNF24Y
2018/1/26 3:28	100,000,000	[redacted]	NDDZVF32WB
2018/1/26 3:18	100,000,000	[redacted]	NB4QJICLTZW
2018/1/26 3:14	100,000,000	[redacted]	NDZZJBH6JZP
2018/1/26 3:02	750,000	[redacted]	NBKLQYXFIVF
2018/1/26 3:00	50,000,000	[redacted]	NDQDXQWEIZ
2018/1/26 2:58	50,000,000	[redacted]	NA7SZ75KF6Z
2018/1/26 2:57	30,000,000	[redacted]	NCTWEIQQVIT
2018/1/26 0:21	3,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:10	20,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:09	100,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:08	100,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:07	100,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:06	100,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:04	100,000,000	NC3BI3DNMR2	[redacted]
2018/1/26 0:02	10	NC3BI3DNMR2	[redacted]

■図-4　コインチェック事件におけるネムの動き

今回の事件で誰もが不思議に思うのは，不正送金されたネムが犯人のアドレスに送金されていることは確認できるのに，それを取り戻すことができないという点である．これがもし，銀行預金であったなら，盗まれた大金がどこかの預金口座にあることが分かった時点で，当局によって差し押さえられ，最終的には盗まれた人に返還されると期待できたであろう．

ビットコインが注目され始めた当初から，その背景に特殊な思想があることが注目されてきた．それは，信頼できる中央機関を決して置かないというポリシーで，「トラストレス」と呼ばれる考え方のことだ．ビットコインは，こうした特徴を持つからこそ，法律や政治体制の違いによる国境の壁を易々と越えて，国際的な利用が可能になったと考えられる．

これに対し，信頼できる中央機関を置く従来の仕組みを「トラスト」の世界と呼ぶ．我々は，政府，中央銀行，裁判所といった信頼できる中央機関の存在を前提に構成された世界に住んでいるから，トラストレスの世界は，きわめて特殊な，危なっかしいものに見える．とはいえ，ビットコインの存在は認知され，トラストとトラストレスの両者が併存する状況が続いてきた．

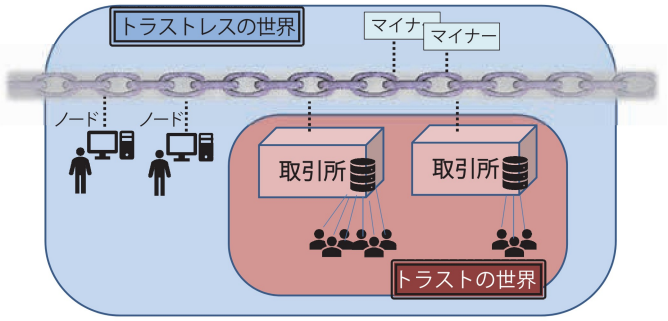
たとえば，ビットコインのノードとして直接接続しているgeekな利用者は，トラストレスの世界で生きている．しかし，自らがノードに接続することのできない素人の利用者は，取引所にビットコインを預け，取引所に依存してビットコイン取引を行っている．この場合，そうした利用者にとって，取引

所こそが「信頼できる第三者」であり，そこにトラストの構造が存在する（図 -5）．

今回流出したネムは，トラストレスの世界で盗まれ，資金洗浄された．信頼できる中央機関はなく，国家権力を含め，何者も情報を恣意的に書き換えることはできないという建前だ．今回の不正流出事件の顛末を見れば，それが両刃の剣であることが分かる．

価格が大きく上昇して注目された仮想通貨も，実はセキュリティの問題から自由ではなかった．そもそも，リスク管理が不十分で，業務改善命令を受けていることからも明らかなように，実際には安全ではない取引を行ってきたと考えられる．結局のところ，預かっている資産をまとめて盗まれてしまったという意味では，仮想通貨業者のほうがはるかに問題は深刻であった．

コインチェック事件は，仮想通貨交換業者の経営管理体制，システムリスク体制に深刻な問題が潜在していることを明らかにした．金融庁は，コインチェックを立入検査したほか，業者の経営体制を改めて詳細にチェックした．その結果，ほぼすべての主要交換業者の経営体制に問題があることが分かった．指摘された問題点の中には，顧客からの預かり資産の管理が不適切であったり，システム障害が頻発したり，マネーロンダリング・反社会的勢力対応が不十分であったりと，顧客から巨額の資金を預かっている事業者としては致命的な問題が多数指摘された．問題の解決が見込めない一部の小規模みなし事業者に対しては，正式に登録拒否処分が行われた（FSHO 社，2018 年 6 月 7 日付け）．しかし，現在の国内における仮想通貨交換業務を担っている主要業者に対しては，金融庁は，問題点を詳細に指摘するとともに，それを解消するよう厳しい業務改善命令を出した．



■図 -5 「トラストレスの中のトラスト」構造

日本の仮想通貨法では，交換業者を登録制とし，法律上はさほど厳しいルールを適用してこなかった．その基本的な考え方は，交換業者は法定通貨と仮想通貨の交換を担う者という認識があり，マネーロンダリング対策としての顧客の本人確認や取引履歴の管理が適切に実施されれば十分というものであった．仮想通貨の価格が現在ほど高くはなく，利用者数も限られていたことから，想定されていたリスクが現在とは比べ物にならないほど小さかったということもある．安全性よりもイノベーションを重視したと説明されることもあるが，そもそも交換業者が巨額の顧客資産を預かる存在とは想定されていなかった．しかし，法律制定時に想定されていた「ブロックチェーンによって安全な取引ができる」という説明は，実態とは乖離していることが徐々に明らかになってきた．

一般の利用者は元々 IT スキルがさほど高くはないので，ブロックチェーンを直接利用することは難しく，交換業者を経由して間接的に利用するしかない．その結果，交換業者がセキュリティを守る責任を負うことになる．毎月のように報道される，交換業者を狙ったサイバー攻撃による被害発生事例を見れば，交換業者のセキュリティ対策が十分ではないことは明らかである．

とはいえ，現在，我が国の仮想通貨交換業者は，延べ 360 万人の利用者を抱え，毎日数千億円もの取引を行っている．ここはどうあっても，セキュリティ対策や経営管理体制，リスク管理体制を整備して，利用者が安全に取引を行える状態とすることが，交換業者の責務であろう．

技術革新とセキュリティのバランス

以上見てきたように，フィンテックと呼ばれる金融の新しい動きは，新たなセキュリティ上の課題を生じさせており，その解決は容易ではない．

それでは，昔ながらの預金通帳と印鑑が良いのだろうか．あるいは，ネット対応せずに，レガシーシステムのままで運用していくことが望ましいのだろうか．多くの金融機関とその利用者はそうだと考え，現在でも古風な手続きを踏襲し，基盤となる情報システムも変更していない．しかし，我が国の社会全般に見られるそうした現状維持的な態度は，国全体の生産性の低下という形で弊害をもたらしている．IT による利便性，生産性の向上を重視すれば，そうした態度を未来永劫続けることはできないだろう．

フィンテックのブームを受けて，金融機関はシステムとセキュリティに対する考え方を，少しずつ変えつつある．ネット上の取引でも信頼できるものとそうでないものとをしっかり峻別することが必要だと分かってきたのだ．利用者も，キャッシュレス社会に対応していくためには，セキュリティ・リスクを敏感に察知する能力が大切だと認識しつつある．それらは，日々の実践によってのみ獲得できるものだ．だから，やはり銀行とその利用者は，早期に新しい技術に基づくシステムに移行し，インターネットとの親和性を高めていくべきなのだ．

思えば，銀行がそのシステムをレガシーのまま維持し続けて，50 年近くが経過している．そこから脱却するチャンスは何度もあったが，実現できないでいた．降って湧いたようなフィンテックのブームは，まさにこの長すぎた優柔不断の時期の終わりを告げるものだ．銀行とその利用者の奮起が期待されている．

(2018 年 9 月 4 日受付)

岩下直行　iwashita.naoyuki.7e@kyoto-u.ac.jp
1984 年, 慶大経卒業, 日銀入行. 情報技術研究センター長, 下関支店長, 金融高度化センター長, FinTech センター長を歴任. 2017 年, 日銀を退職. 京大教授に就任．金融庁参与および PwC あらた監査法人スペシャルアドバイザーを兼務.