SWIFTの不正送金事案から探るサイバーセキュリティ態勢

「人・組織」を土台としたうえで、「技術」「プロセス」の整備を

金融庁総務企画局政策課
サイバーセキュリティ対策企画調整室
室　　長　**鈴木　啓嗣**
前・課長補佐　**小林　由昌**
前・研究官　**花田　隆仁**

SWIFTのサイバーセキュリティに関する新たなガイドラインが適用され、初回の対応期限が迫っている。これは2016年に世界の複数金融機関で発生した、SWIFTを悪用し多額の資金を窃取するサイバー攻撃事案が契機となっている。本事案の発生は、日本を含む各国当局者にも衝撃を与え、国際的な金融システムの大きな脅威としてとらえられている。本稿では、本事案の概要や教訓を整理するとともに、今後SWIFTを利用する金融機関において適切な対応が求められる新ガイドラインについて解説する。

強固なセキュリティがなぜ破られたのか

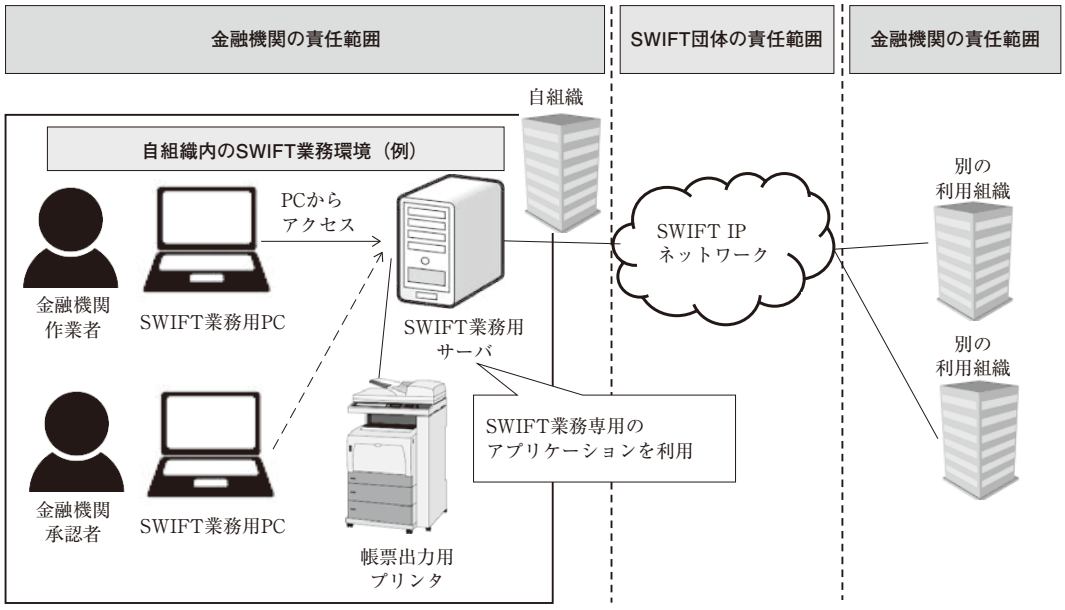
金融庁は2015年4月に監督指針を改正するとともに、同年7月にはサイバーセキュリティ対策企画調整室を設置し、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を策定・公表した。同方針に基づき、各種の取組みを推進してきている。その間、金融庁にはさまざまなサイバー攻撃事案が金融機関から報告されているが、幸いにもこれまでのところ国内の金融機関、金融市場インフラにおいて、その機能が停止・混乱するような重大な事案は発生していない。

他方、海外に目を向けると、金融分野において多数のサイバー攻撃事案が発生している。金融庁では公表・非公表を含めさまざまなサイバー攻撃事案について情報収集と分析を行っている。攻撃は日々巧妙さと執拗さを増しており、大規模な被害も発生している。その一つが本稿で扱う16年2月にバングラデシュ中央銀行（以下、「バングラデシュ中銀」）で発生した、SWIFTを悪用した8100万ドルの不正送金事案である。

SWIFTはきわめて重要な世界共通の金融インフラであり、わかりやすくいえば金融機関同士が外国送金を行う際に利用する国際金融取引のネットワークシステムである。もちろんSWIFTのセキュリティは強固に維持されている。世界各国の金融機関を結ぶネットワークは閉域網を採用しており、通信も高度に暗号化される等、何重ものセキュリティ対策が施されている。

それにもかかわらず、このような衝撃的な事案が発生したの

〔図表１〕　　ＳＷＩＦＴのシステム構成（イメージ）



（注）　SWIFT団体の責任範囲は、利用組織同士を接続する「SWIFT IPネットワーク」の部分。
　　各利用組織内のシステムにおける責任は、当該組織に帰属。
（出所）　筆者作成（図表２～４も同じ）

はなぜか。そこには、サイバーセキュリティの確保に必要な３要素のバランスが関係している。

筆者は常日ごろから金融機関との対話において、〝サイバーセキュリティの確保には、「技術」的な取組みはもちろん必要だが、「人・組織」「プロセス」に係る取組みがなにより重要である〟と伝えている。そして、〝その点は、経営から現場まで企業全体で意識して取り組むべきである〟と訴え続けている。そこで、本稿においても、事案からみえてくる３要素の関係を意識しながら解説したい。

なお、以下で記載しているバングラデシュ中銀で発生したサイバー攻撃の内容やその手口については、筆者が入手した情報をもとに解説しているが、一部推定が含まれる。また、本稿で意見にわたる部分は、筆者の個人的見解を含むため、必ずしも金融庁としての意見ではない。

国内でも250超の組織がSWIFTを利用

１９７３年に設立されたＳＷＩＦＴは、銀行等の加盟者で構成されたグローバルな協同組合で、金融メッセージングサービスを提供する民間団体（本部はベルギー）である。ＳＷＩＦＴは、利用組織に対し、利用組織間の国際金融取引に関するメッセージを、コンピュータと通信回線を利用して伝送するサービスを提供している。このサービス自体もＳＷＩＦＴと呼ばれている（両者を区別するため、以降では便宜上、サービス自体を「ＳＷＩＦＴ」、組織としてのＳＷＩＦＴを「ＳＷＩＦＴ団体」という）。

ＳＷＩＦＴのシステム構成のイメージは図表１のとおりである。利用組織同士は「ＳＷＩＦＴ ＩＰネットワーク」で接続されており、当ネットワークを経由して海外送金等の取引電文をやりとりする。

大多数の利用組織は金融機関であり、２００以上の国と地域における１万１０００以上の銀行、証券会社、市場インフラ、事業法人等が利用している。国内でも２５０以上の組織がＳＷＩＦＴを利用しており、預金取扱金融機関が多数を占めている。

SWIFT不正送金事案の教訓

また、国内金融機関等によるSWIFTの取引電文量は約1億3700万件で、全世界の2・2%を占める（2016年3月時点）。

関連する銀行の休日を狙った犯行

筆者が収集した情報をもとに、バングラデシュ中銀で生じた事案の概要と攻撃手口などを解説する。

事案の概要は次のとおりである。

●16年2月5日、バングラデシュ中銀が、ニューヨーク連邦準備銀行（以下、「ニューヨーク連銀」）に保有する口座から、複数の海外の銀行へ送金を指示するSWIFT電文を35件送信（いずれも攻撃者から作成された不正な送金指示）。

●ニューヨーク連銀は当初、電文に必要事項の記載漏れがある等の理由から、すべての送金指示の処理を拒否。

●その後、バングラデシュ中銀から修正された電文が再送されたため、ニューヨーク連銀は35件のうち、リサール商業銀行（フィリピン）の個人口座宛ての4件（合計8100万ドル）およびパン・アジア銀行（スリランカ）のNGO（のちに架空の組織と判明）口座宛ての1件（2000万ドル）の送金処理を実施。

●その結果、リサール商業銀行には全額送金が完了。他方、パン・アジア銀行への送金電文にはスペルミスなどが含まれており、経由銀行であったドイツ銀行が不審に思い送金を中断。

●ドイツ銀行がバングラデシュ中銀に対し、送金内容を確認したことをきっかけに、本件が不正送金であることが発覚。

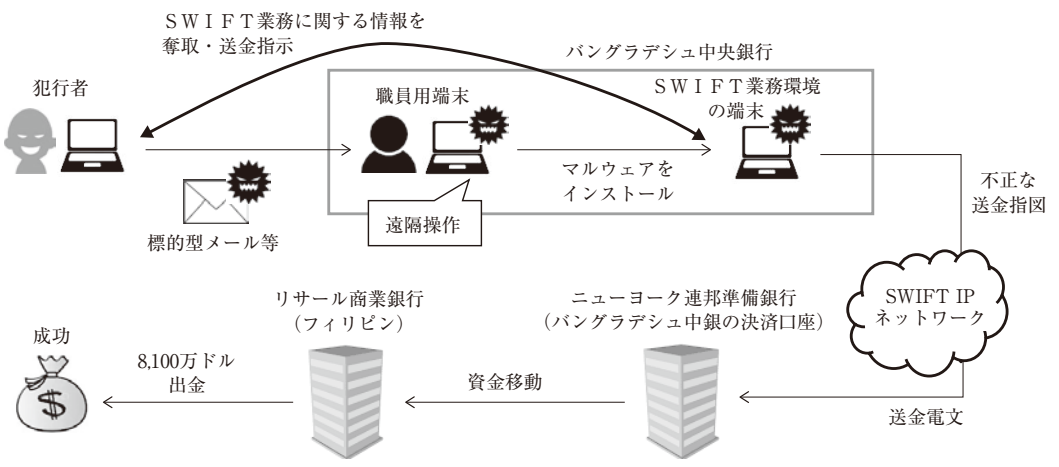
なお、送金電文が発信された同年2月5日（金）は、バングラデシュ中銀の休日であり、翌6日（土）、7日（日）はニューヨーク連銀の休日、さらに8日（月）はリサール商業銀行の休日（注）であり、攻撃者は監視が手薄となるタイミングを狙って犯行に及んでいる。

次に、本事案で用いられた攻撃は図表2のような手順で実施されたと考えられ、「侵入～調査」と「実行～痕跡の削除」の二つに大別される。

⑴ 侵入～調査

攻撃者がどのようにバングラデシュ中銀のネットワーク内に侵入したかは明らかでないが、標的型メールなどを職員に送り、インターネット接続端末にマルウェアを感染させるところからスタートしたものと考えられる。標的型メールの詳細は明らかにされていないが、事前の偵察行為やソーシャルエンジニアリングによって職員の業務に関係する内容等、メールを開かせるための巧妙な手口が用いられていたと想定される。また、当該端末とSWIFT業務環境の端末がネットワークで接続さ

〔図表2〕 SWIFT不正送金の攻撃手口の概要



〔図表３〕　攻撃手口の特徴と悪用された脆弱性

攻撃手口の特徴	➢ 内部ネットワークへ侵入後、およそ２カ月もの間、検知されることなく潜伏し続け、認証情報や電文送信手順等の観察や情報収集を実施。
	➢ 関係する複数の銀行の休日を事前に把握し監視が手薄になる日を狙った周到な犯行。
	➢ 犯行後にログを削除する等、発覚を遅らせる手法をとっている。
	➢ インサイダーによる共犯の可能性。
悪用された脆弱性	➢ SWIFT 業務環境が間接的にインターネットにつながっていた。
	➢ ネットワーク機器に安価で脆弱な中古のスイッチを利用。
	➢ インターネット接続セグメントと内部ネットワークを分離するためのファイヤーウォールが未設置。
	➢ セキュリティ対策機器が導入されていたが、導入以降、設定の見直しやアップデートが未実施。
	➢ 休日にもかかわらず SWIFT 業務環境の端末の電源が入っており電文を送信可能な状態。

れていたため、マルウェアの感染が同行ネットワーク内部にも拡大し、攻撃者はＳＷＩＦＴ業務環境までたどり着くことができたものと考えられる。

なお、攻撃者がＳＷＩＦＴ業務環境の端末まで感染を拡大できたその他の要因として、以下の点があげられる。

●ネットワーク機器に安価で脆弱な中古のスイッチを利用

●インターネット接続セグメントと内部ネットワークを分離するためのファイヤーウォールが未設置

●セキュリティ対策機器が導入されていたが、導入以降、設定の見直しやアップデートが未実施

さらに、攻撃者はＳＷＩＦＴ業務環境の端末上で日々行われる操作を入念に観察し続け、送金電文の作成や承認といった電文送信の手順ならびに操作に必要な職員の認証情報を、２カ月以上かけて盗んだといわれている。とくに、職員の認証情報については、作業者および承認者の権限等、複数の職員の情報を盗んでいたと考えられる。それだけではなく、攻撃者は電文の送信後にＳＷＩＦＴ業務環境で生成・保管されるログを削除していることから、当システムのログデータに関する仕様なども熟知していたと考えられる。

⑵実行～痕跡の削除

攻撃者は盗んだ情報を用いて、同行が通常実施するのと同様のＳＷＩＦＴ送金手続でニューヨーク連銀宛てに送金電文を送信している。この際、同行では休日にもかかわらず、ＳＷＩＦＴ業務環境の端末の電源が入ったままで、電文を送信可能な状態となっていたため、監視の手薄な休日に操作を許してしまっている。

電文送信後、攻撃者は不正の発覚を防ぐ（遅らせる）ための細工として、ＳＷＩＦＴ業務用アプリケーションの脆弱性を突いて、ＳＷＩＦＴ業務環境のデータベースのなかから当該不正送金に関するログを削除しているほか、プリンタから出力される帳票の内容を改竄している。

なお、攻撃手口のなかで、認証情報やＳＷＩＦＴ業務の手続、システムの仕様等の情報の収集に関しては、共犯の内部職員が情報提供した可能性も指摘されている。

事案の原因分析から得られる教訓

以上の内容に基づき整理すると、攻撃手口の特徴と同行が被害を許してしまったおもな要因（悪用された脆弱性）として、少なくとも図表３のポイントがあげられる。

攻撃手口の特徴から想像できるように、犯行者は、実際の送金処理を行うまでの間、マルウェアや不正なアクセスが検知されないよう慎重に潜伏し続けている。潜伏の過程では、前述した点以外にもいくつもの巧妙な手法が取り入れられたと考えられる。したがって、攻撃者には、それを実現するための相応の能

力と経験があったと推察できる。

他方で、バングラデシュ中銀のセキュリティ対策にも複数の問題がみられる。脆弱な中古スイッチの利用やファイヤーウォールの未設置が事実であるならば、内部対策が十分に機能していなかったことが想像できる。また、利用時間外であるにもかかわらずSWIFTの利用が可能な状態で端末を放置していたならば、ずさんな運用であったと考えられる。

読者のなかにはこれらを極端な事例ととらえ、「当社は対応できているので関係ない」と考える方もいるかもしれない。

しかし、重要なのは課題事例そのものではなく（もちろん、課題事例を自社に置き換えて点検することは重要）、このような事案が起きた背景や真の原因を考察し教訓とすることである。「この攻撃はわれわれには関係ない」「高機能なセキュリティ製品を導入したので心配ない」「SWIFT環境は閉域網だから安全」等の固定観念は、最も危険である。こうした固定観念によってリスクを認識・評価しようとする行為自体を放棄してしまうからである。

バングラデシュ中銀では、技術的なセキュリティ対策ができていない点があったと考えられる。また、そういった対策を有効に機能させるためのプロセスや管理ルールにも問題があったと考えられる。おそらく、高度化が著しく、変化の激しい昨今のサイバー攻撃の脅威を正しく認識することができず、自行のリスクを適正に評価することや自行の実態を正しく理解することができていなかったのではないか。

脅威やリスクを適切に把握できていない原因は「人」と「組織」にあり、その責任を負うのも「人」であり「組織」である。事実、本事案を受けてバングラデシュ中銀では経営トップである頭取が引責辞任している。セキュリティ担当者やシステム部門といった特定の人や組織だけではなく、経営陣あるいはユーザー部門等も含めたそれぞれの立場の人や組織が、役割と責任を果たしサイバーリスクを適切に認識し対処していくことが重要である。同時に、そのプロセスが適切に機能するよう継続的に見直しながら実施していくこと、ひいてはこれらの取組みを通して、サイバー攻撃に対峙していくという共通の意識が組織全体に醸成されていくことが重要である。そうでなければ、いかに優れたセキュリティ製品を導入したり、管理プロセスを整備したとしても、いずれ脅威に凌駕され、形骸化してしまうだろう。技術やプロセスは、土台となる「人・組織」がしっかりしていてこそ有効に機能すると考えられる。

SWIFT団体が策定した新たなガイドライン

今回のSWIFTが悪用された多額の不正送金は、全世界のSWIFTを利用する金融機関を不安にさせるだけでなく、各国当局やSWIFT団体自体にも大きな衝撃とシステミックリスクの可能性を示している。そのため、米国の連邦金融機関検査協議会（FFIEC）は対応の方向性について声明を出している。また、イギリス中央銀行も関係金融機関に対し対策の命令を発している。もちろん金融庁も、金融機関に対して注意喚起をし、所要の措置を講じるよう求めている。こうしたなか、だれよりも本腰を入れた対策に乗り出したのが、SWIFT団体自身である。16年5月に、利用組織のサイバーセキュリティ態勢の向上を目指し、“Customer Security Programme”を公表している。その具体的な内容は次の5点である。

① Improve information sharing amongst the global community.
（国際的なコミュニティ内における情報共有の促進）
② Enhance SWIFT related tools for customers.
（顧客に提供するSWIFT関連のツール（ソフトウェア等）の改善）
③ Enhance guidelines and provide audit frameworks.
（ガイドラインの改善と監査フレームワークの提供）
④ Support increased transaction pattern detection.
（送金パターン検知機能の普及

促進）

⑤ Enhance support by third party providers.

（サードパーティのプロバイダーによる支援の改善）

このうち、③で提示されている「ガイドラインの改善」を具体化するものとして、17年4月に「Customer Security Controls Framework」（以下、「CSF」）が策定され、すでに運用が始まっている。CSFの特徴は2点あり、1点目は利用組織が対応すべきセキュリティ上の要求項目（セキュリティコントロール）が示されたこと、2点目は、毎年1回、要求項目の遵守状況に関する自己評価（self-attestation）の実施が求められていること――である。

以下ではCSFの概要とこれらに対応する際の留意点を解説したい。

(1) 対応すべきセキュリティコントロール

CSFでは利用組織に求める27のセキュリティコントロール（安全性に関する管理項目）が提示されている。そのうち、16項目は必須項目（Mandatory

〔図表4〕 **CSFの必須項目の概要**

No	要求項目	項目の目的（抄訳）
1	SWIFT環境の保護 (SWIFT Environment Protection)	ローカルに設置されたSWIFTインフラを、社内の一般IT環境や外部環境における侵入や不正から保護すること。
2	オペレーティングシステムの特権管理 (Operating System Privileged Account Control)	オペレーティングシステム（OS）の管理者アカウントの配布と利用を制限および管理すること。
3	内部データフローのセキュリティ確保 (Internal Data Flow Security)	ローカルに設置されたSWIFT関連アプリケーション同士およびSWIFT関連アプリケーションとオペレーターPC間のデータフローの秘匿性、整合性、真正性を確保すること。
4	セキュリティの更新 (Security Updates)	ベンダーサポートを確保し、必須のソフトウェア更新を適用し、リスク評価をふまえて適時セキュリティ更新を適用することで、ローカルに設置されたSWIFTインフラ内の既知の脆弱性を最小限に抑えること。
5	システムの強化 (System Hardening)	システムを強化することでSWIFT関連コンポーネントのサイバー攻撃対象を削減すること。
6	物理的セキュリティ (Physical Security)	機密性の高い装置、作業環境、システムを導入するサイト、保管場所への不正な物理的アクセスを防止すること。
7	パスワード管理ポリシー (Password Policy)	効果的なパスワード管理ポリシーを確立することで、パスワードの一般的な攻撃手法に対して十分に耐性をもつようにすること。
8	多要素認証 (Multi-factor Authentication)	多要素認証を実装することで、単一の認証要素によるSWIFT関連システムへの侵入を防ぐこと。
9	論理アクセス制御 (Logical Access Control)	各オペレーターアカウントに必要に応じた（Need-to-know）アクセス権と最小権限のみを与え、職務の分離がなされるというセキュリティ原則を徹底すること。
10	トークン管理 (Token Management)	認証用の接続型ハードウェアトークン（利用している場合）の適切な管理、トラッキング、利用を徹底すること。
11	不正ソフトウェアの検知 (Malware Protection)	ローカルに設置されたSWIFTインフラを不正ソフトウェアから確実に保護すること。
12	ソフトウェアの整合性 (Software Integrity)	SWIFT関連アプリケーションの整合性を確保すること。
13	データベースの整合性 (Database Integrity)	SWIFTメッセージングインターフェースのデータベースの整合性を確保すること。
14	ログ取得とモニタリング (Logging and Monitoring)	ローカルのSWIFT環境内におけるセキュリティ関連のイベントを記録し、異常な行為や操作を検知すること。
15	サイバー攻撃対策 (Cyber Incident Response Planning)	サイバー攻撃対策として一貫性のある効果的なアプローチを確立すること。
16	セキュリティ教育と啓蒙 (Security Training and Awareness)	定期的にセキュリティ教育と啓蒙活動を行うことで、すべてのスタッフがセキュリティ関連の責任を認識し、果たすようにすること。

Security Controls)、残る11項目は推奨項目（Advisory Security Controls）である（必須項目の概要は図表4のとおり）。

各項目には「目的（Control Objective）」と、それを達成するための具体的な対応内容が示されている。基本的には設定された対応内容を満たすことが求められるが、その他の代替策によって「目的」を達成可能と自組織において判断できる場合には、代替策での対応も許容されている。

必須項目のなかで、とくに利用組織の対応に負荷が生じるのではないかと予想されるものは、ＩＴ投資が必要となる可能性がある「8. 多要素認証」や「14. ログ取得とモニタリング」、関係部門を巻き込んだ対応が必要となる「15. サイバー攻撃対策」などである。これらの項目を含め16項目への対応状況を速やかに確認し、未対応の場合には対応を加速する必要がある。また、現時点における必須コントロールは16項目だが、将来的には推奨項目が必須項目に格上げされる可能性も示唆されているため、このような点も考慮し計画的に準備を進めることが重要である。

(2)年次の自己評価

本年12月末までに利用者組織は自己評価の結果をＳＷＩＦＴへ提出することが求められる。評価に際しては、客観的かつ実効的な方法で実施することが重要である。そのため、評価者は各要求項目の目的・内容を十分に理解したうえで対応状況を確認するほか、内外監査などを活用し評価の客観性を担保する等、本取組みの趣旨をふまえて対応することが重要である。

提出した評価結果については他の利用組織から開示を求められる可能性があるほか、評価結果を提出しなかった組織、あるいは必須項目のなかに未対応項目がある組織については、所在国の金融当局にその旨が通知される。本取組みはあくまでＳＷＩＦＴ団体の施策であるものの、通知を受けた後の対応は、金融当局に委ねられている。そのため金融庁においてもこういった通知を受けた場合は、適切に対応していくことになる。

ただし、ＳＷＩＦＴ団体における本取組みの狙いは、対応が不十分な組織を洗い出して利用組織から排除していくことではない。取引電文をやりとりする取引先のサイバーリスクの状況を可視化することにより、利用組織が相互に安心してＳＷＩＦＴを利用できるようにすることである――とされている。

＊　＊　＊

以上、ＳＷＩＦＴへの攻撃を題材としたが、解説した内容、あるいは意見として述べたなかには、ＳＷＩＦＴに限らず、金融機関がサイバー攻撃対策を進めるうえで参考となる示唆が含まれている。

サイバー攻撃はますます高度化・巧妙化し、執拗性も増している。このような状況下でも、本邦金融機関には、適切にサイバー脅威を把握し、脆弱性へ対処することにより、被害の未然防止と最小化に向けた取組みを進めていただきたいと考えている。しかし、比較的大きな攻撃被害を受けた経験が少ない金融機関にとっては、実感として脅威をイメージしにくい部分があるかもしれない。

そのような場合には、本事案はもとより、国内外で発生しているさまざまなサイバー事案について情報収集・分析し、そこから得られる教訓に基づき、現実性のあるサイバーセキュリティの管理態勢の継続的な取組みと改善を推進していっていただきたい。

（注）金曜日はバングラデシュは休日、2月8日（月）はフィリピンの祝日であったため、それぞれ銀行も定休日。

すずき　ひろつぐ
95年大蔵省（現・財務省）入省。13年金融庁監督局総務課監督調査室課長補佐、14年金融庁監督局保険課総括課長補佐を経て、15年7月から現職。
こばやし　よしまさ
監査法人等での勤務を経て、システムリスク管理の専門家として14年金融庁入庁。15年7月からサイバーセキュリティ対策企画調整室を兼務。
はなだ　たかひと
金融機関、銀行系シンクタンクでの勤務を経て、15年金融庁入庁。