【政策ブリーフ】抜かれた資金は誰が止めるのか

―凍結を担うのは国内外の民間。だが緊急対策パッケージ 66 項目は、日本の当局がそれを求める手順も根拠も定めていない

2026 年 11 月 10 日｜一般財団法人 日本危機管理研究所｜舩山 美保｜読了目安 6 分

> **結論：侵入を止める制度と、抜かれた資金を止める制度がつながっていない。これが五つめの空白である。**

本稿は既刊「能動的サイバー防御に残る 4 つの空白」（10 月 29 日）の続編の要約版。全文と図版 5 点は本編をご覧ください。

1｜何が起きたか

11 月 4 日、フランス。 仏クレディ・ミュチュエル・アルケア（顧客 580 万人、総資産 2115 億ユーロ）が、サイバー攻撃により**自己勘定から 1 億ユーロ超**を不正送金された。顧客口座ではなく、銀行自身の資金である。

> **外部委託先のプラットフォーム**（監督の外）→ **銀行の自己勘定**（顧客口座ではない）→ **暗号資産へ交換**（規制が及びにくい）→ **民間が検知・追跡**（当局ではない）

異常を最初に指摘したのはブロックチェーン調査者 ZachXBT 氏であり、**当局ではない。** 同行のコミュニケは**資金の一部を「ブロックできた」**とし、回収は進行中とする。**誰がどの経路で止めたかは公表されていない。**

10 月、日本。 GMO インターネットの FX 自動売買用 VPS が侵入され、保存されていた取引口座のログイン情報が窃取された。金融庁は 10 月 22 日に全 FX 事業者へ緊急通知し、10 月 27 日、片山金融担当相が FX5 社からの顧客被害の報告を公表した。

入口は同じである。 監督の外にある委託先・共通基盤から入られた。

2｜監督が及ぶ先と、攻撃が入る場所はずれている

緊急対策パッケージ本文は、冒頭でこう書いた。

> 昨今の漏えい事案では…**自組織又は委託先**における基本的な対策が十分でなかった事例が多くみられる。

認識はある。だが委託先に義務を課す施策は 66 項目のどこにもない。 決定前日の 11 月 5 日、NCO は「委託先を含めたサプライチェーン全体の対策強化」を求める注意喚起を出した。ただし宛先は**委託元**であり、文末は「お願いいたします」である。



図 2：報告は第 1 層から届く。原因は第 2 層にあり、すべてを支える土台は第 3 層にある。

11 月 6 日、金融庁は「金融機関利用者へのお願い」を公表した。呼びかけの相手は**利用者**であり、求めたのは**自衛**である。

第 3 層について。 パッケージは通信事業者には「必要となる制度整備等を行う」と書いたが、クラウド事業者には「サイバー協議会への参加を促す」と書くにとどめた。施設としてのデータセンター（電源、冷却、物理防護、立地）は扱われていない。**クラウドは、サービスとしては扱われているが、施設としては扱われていない。** 2026 年 3 月の UAE では、データセンターへの攻撃で**銀行 2 行と決済アプリが障害**に陥っている（当研究所既刊「四層フレームの破綻事例と対策」。物理攻撃による事例であり、本稿は日本への物理攻撃を論じない）。金融はこの層に載っている。**総務省が通信事業者について進める「制度整備」に、クラウド・データセンターが含まれるかが直近の分岐点である。**

3｜緊急対策パッケージ（11 月 6 日決定・66 項目）の評価

四本の柱（①基本的対策、②情報収集・分析、③攻撃への対処、④被害者支援）に 66 項目。予備費**約 100 億円**（AI 点検 20 億／警察 41 億／デジタル庁 38 億）。**内訳はすべて政府側の体制強化である。** 首相は**本文の外で**サイバー対処能力強化法の改正検討を指示し、国内通信情報の利用拡大が選択肢に入った。（施策の一覧は本編第 5 章）

四つの空白は埋まったか

部分的に前進したのは④（速度）のみで、A2B 攻撃を名指ししたが API の最低基準は未着手。①（対象）は**認識のみ**で指定も義務化もなし。②（時間）は**方向が異なり**、法改正は本文外の指示で国内通信への拡大が選択肢に入った。③（手続）は**方向が逆**で、アウトリーチ・チームは「NCO から能動的に接触する」とされ、決定 2 日後の特設ページも既存窓口の一覧にとどまる。⑥（恐喝）は**未着手**で、**「身代金」「ランサムウェア」の語は一度も現れない**。（判定の根拠は本編図 3）

4｜新しい空白 ―抜かれた資金は誰が止めるのか

パッケージが止めようとしたのは**情報の流通**である（漏えい情報が載ったサイトへのアクセス抑止）。仏銀行事案で必要だったのは**資金の停止**だった。暗号資産については警察庁の資機材整備に「暗号資産追跡」の語があるが、**これは捜査能力の整備であり、連絡経路ではない。**

図4　資金を止められるのは誰か ―権限の地図

縦に機関、横に機能。右端の「即時の凍結」を担えるのは民間のみ。公的機関は一つもない

機関	事案情報の集約	監督・命令	捜査	資金の追跡	即時の凍結
国家サイバー統括室（NCO） 司令塔。無害化措置とテイクダウンの調整	○	△	×	×	×
金融庁 監督は金融事業者のみ。委託先には及ばない	○	○	×	×	×
警察庁 暗号資産追跡の資機材を整備。FFFがログを保全	○	×	○	△	×
犯罪収益移転防止対策室（日本のFIU） 疑わしい取引の届出を集約・分析。NCOとは別組織	△	×	△	○	×
暗号資産交換業者（民間） 自社を通る資金のみ。促す手順がない	×	×	×	○	△
ステーブルコイン発行体（外国の民間企業） 主要チェーン上で即時凍結が可能。要請の筋がない	×	×	×	○	○
この列に公的機関は一つもない。担うのはすべて民間である 問題は「止められる者がいない」ことではなく、日本からその民間へ要請する経路がないことである				⇢	

凡例　○担える　△限定的・任意　×担えない

テザー社の凍結実績は累計約44億ドル、2,300件超の案を支援とされる（2026年4月時点）。緊急対策パッケージは、交換業者が当局に通報する経路、当局が民間に凍結を求める経路、FIUとサイバー事案情報を接続する手順の、いずれも定めていない。これが「空白⑤ 資金」である。

出典：緊急対策パッケージ本文・施策一覧、各制度の一般的な枠組み、および報道をもとに作成。非公開の連絡経路が存在する可能性は排除できない。

図 4：「即時の凍結」の列に公的機関は一つもない。担うのはすべて民間である。

（本稿の「資金」は、攻撃によって被害者から抜かれた資金 ―被害組織自身の財産、または顧客から預かっていた資産― を指し、攻撃者の資金源ではない。「出口」はその換金先を指す。セキュリティ分野の定着語である「出口対策」＝情報の持ち出しを防ぐ対策とは、対象が異なる。）

止められる者はいる。 ステーブルコイン発行体は、自社が発行するトークンを主要チェーン上で即時に凍結できる。テザー社の実績は累計約 44 億ドル・2,300 件超とされる。ただし**外国の私企業**であり、米当局の**非公式な要請**に応じ、適法性をめぐり提訴もされている。

問題は、止められる者がいないことではない。日本の当局がその者へ要請する手順も根拠も、定まっていないことである。 空白は二種類で、一つの措置では埋まらない。国内の交換業者には**監督権限はあるが手順がない**。外国の発行体には**そもそも要請の筋がない**。

5｜提言（5 項目・新組織不要）

#	提言	検証の時点
①	**デジタル共通基盤を法改正で指定**。クラウド・データセンター・陸揚げ局を報告義務の対象に。推進法第 50 条第 1 項は対象事業を法律本文に列挙し政令に委任していないため、**この空白は緊急対策では原理的に埋められない**。首相が指示した法改正の検討に対象拡大を含める	2027 年通常国会
②	**アウトリーチ・チームに「受理と回答」機能を追加**。発動判断は政府に残し、要請元へ非公開でも結果を返す	運用要領（11 月中）
③	**アクセス抑止策と国内通信情報は、統制の設計と一体で検討**。監理委員会の体制強化を条件とし、外国関連通信の統制が働くと確かめる前の国内拡大は勧めない	法改正案の提出時
④	**資金を止める手順と根拠を、国内と国外に分けて定める**（図 4 の空白列）。**国内**＝交換業者の通報と当局の凍結要請の手順を監督上の文書に明記（登録業者への既存権限の運用として**立法を要さずに対応しうる**）、FIU とサイバー事案情報を接続。**国外**＝誰が何を根拠に発行体へ要請するかを定める（現状は米当局の非公式要請が事実上の経路）。条件は前稿の 8 基準	2027 年 3 月末
⑤	**恐喝型攻撃への方針**。身代金支払いの報告制度（豪州型：72 時間以内）、拒んだ企業への支援の定型化、事後検証の公表	2027 年通常国会

留意事項

本稿は**確定版**（表題に「（案）」を含まず、日付が令和 8 年 11 月 6 日と記載された版）で主要な引用箇所を照合した。「身代金」「ランサムウェア」の語が現れないことも確定版で確認している。ただし同義表現の可能性は排除できない。仏銀行事案の被害額と侵入経路は未確定で、本稿は当事者発言の「1 億ユーロ超」を用いた。同事案の侵入基盤がデータセンターであったことを示す公開情報はなく、本稿は断定しない。発行体の凍結実績は専門媒体の報道による。図 4 は公開情報に基づく筆者の整理で、非公開の経路が存在する可能性は排除できない。

本稿は特定の金融機関の脆弱性を評価せず、日本への物理攻撃も論じない。問いは「日本の銀行も攻撃されるか」ではなく、「**同じ入口と出口が日本にもあるか、あるとすれば誰が止めるのか**」である。

出典一覧は本編の参考資料をご参照ください。

本編：抜かれた資金は誰が止めるのか ― 一般財団法人 日本危機管理研究所

https://inst-ds.org/?p=2375

© 2026 一般財団法人 日本危機管理研究所　本資料は政策検討・引用目的での転載・配布を自由に行っていただけます。転載の際は出典（発行元・発行日）の明記をお願いいたします。