SWIFT CSCF v2026 / Control 7.3A

一度の試験で、多くを満たす: 横断的な法体系の演習としてのSWIFT CSCF v2026 7.3A侵入テスト

Cambridge Cyber International / 2026

SWIFT顧客セキュリティプログラムの2026年サイクルにおいて、Control 7.3A（侵入テスト）は、接続された機関に対して、回り続ける三年周期にわたって期待されるスコープと試験シナリオを定めるコミュニティ主導のガイダンスを伴っている（SWIFT 2025年）。孤立して読めば、これは満たすべきもう一つの認証項目にすぎない。より広い規制の地形に照らして読めば、それは単一の進路の証左である。すなわち、欧州連合、合衆国、カナダの各監督当局は、機関が自らの統制が単に存在するのではなく機能することを証明する手立てとして、インテリジェンス主導の、脅威に基づく試験へと収斂しつつある。本稿は、7.3A侵入テストに備える機関が、その試験を最先端の水準で一度だけ設計し、同じエビデンスを、デジタルオペレーショナルレジリエンス法（DORA）、第二次ネットワークおよび情報セキュリティ指令（NIS2）、ニューヨーク州金融サービス局のサイバーセキュリティ規制（23 NYCRR Part 500）、ならびに金融機関監督庁ガイドラインB-13に対して、合衆国国立標準技術研究所サイバーセキュリティフレームワークバージョン2.0（NIST CSF 2.0）を共通の背骨として用いながら収穫すべきだ、と論じる。

7.3Aをチェックボックスとして読むことの問題

各法体系を別個の義務として扱う接続された機関は、構造的なペナルティを支払う。それはSWIFTの侵入テストをセキュアゾーンへと狭くスコープし、別個のDORAレジリエンステストを発注し、年次試験に関するNYDFSの質問票に答え、第四の日程でカナダの監督当局向けのエビデンスを準備する。各エンゲージメントは、同じ偵察、同じ交戦規則、同じ是正サイクルを繰り返し、そのそれぞれが、次の法体系が受け入れない形のエビデンスを生み出す。代償は金銭だけではない。断片化された試験は、断片化されたリスクの像を生む。なぜなら、いかなる単一の演習も、現実の敵対者が見るように機関を見ることがないからである。すなわち、バックオフィス、オペレーターのワークステーション、メッセージングインターフェース、そしてネットワークへの接続を横断する、端から端までの像である。

ここでの論点は、いま主要な各法体系を横断して見られるようになった収斂が、断片化されたアプローチを時代遅れにする、ということである。7.3Aのガイダンス、DORAの脅威主導の試験体制、OSFIのインテリジェンス主導の期待、そしてNYDFSの年次マンデートは、四つの異なる試験ではない。それらは一つの理念の四つの監督上の表現であり、そのうち最も要求の厳しいものに合わせて設計し、その結果を共通のフレームワークに対して記録する機関は、他のものを副産物として満たすことができる。

SWIFT CSCF v2026のControl 7.3Aがいま期待するもの

Control 7.3Aは、顧客セキュリティ統制フレームワークの中で、その目的が、セキュアゾーンまたはバックオフィスの侵害につながりうる脆弱性を特定することによって、利用者のSWIFT関連インフラストラクチャの運用上のレジリエンスを検証することにある助言的統制として位置づけられている（SWIFT 2025年）。2026年の変更の実質は、新しい統制番号ではなく、試験がどうスコープされ、どのようなシナリオを網羅すべきかについてのより鋭いガイダンスである。フレームワークはいまや、三年周期にわたって演練されるべき一群の試験シナリオを明示しており、それゆえ機関は、年次で繰り返される単一の狭い外部スキャンによってこの統制を満たすことができない。期待されるのは、その周期にわたって、プログラムが、メッセージングインターフェースと関連コンポーネントのアプリケーション層の試験、セキュアゾーンとそのセグメンテーションのインフラストラクチャの試験、そして現実の侵入が悪用する人的およびオペレーターワークステーションの経路を網羅することである。

二つの設計上の帰結が続く。第一に、スコープは、都合のよいネットワーク範囲に対してではなく、セキュアゾーンとその信頼境界に対して定義されなければならない。なぜなら、この統制の目的は、攻撃者がバックオフィスからメッセージング層へとピボットできないことを証明することにあるからである。第二に、試験は、有能でかつ十分に独立した当事者によって実施されなければならず、その発見事項は、その終結それ自体がエビデンスとなる追跡された是正サイクルに供されなければならない。この統制は、あらゆるアーキテクチャ類型にとって義務的ではなく助言的であるが、それに対して自己認証する機関にとって、評価者は、スコープ、手法、発見事項、是正を、証明書ではなく一貫した記録として見ることを期待するであろう。

四つの隣接する法体系

DORAと脅威主導の侵入テスト

デジタルオペレーショナルレジリエンス法は、適用対象となるすべての金融主体に対し、その情報通信技術システムを定期的に試験することを要求し、重要な主体の部分集合に対しては、少なくとも三年ごとに脅威主導の侵入テスト（TLPT）の手段によって高度な試験を実施することを要求する（European Parliament and Council 2022a）。TLPTはインテリジェンス主導である。すなわち、稼働中の本番システムに対する管理されたレッドチーム模擬演習であり、現実の脅威アクターの戦術、技法、手順をかたどり、TIBER-EUフレームワークが欧州の参照基準となる手法のもとで実施される（European Central Bank 2018）。7.3Aの試験を、現在の脅威インテリジェンスがそのシナリオを形作る脅威主導の水準で準備する機関は、すでにDORA試験の背骨を築いており、主に正式なスコープと、指定されたTLPTを包む監督上のガバナンスにおいて異なるにすぎない。

NIS2とlex specialisの適用除外

第二次ネットワークおよび情報セキュリティ指令は、不可欠な主体および重要な主体を横断して、サイバーセキュリティのリスク管理とインシデント報告のベースラインを引き上げ、各国当局は2026年のあいだに置換から能動的な監督へと移行した（European Parliament and Council 2022b; European Commission 2025）。金融主体にとって実務上の要点は、優先順位の一つである。すなわち、DORAはlex specialisであり、NIS2の第4条は、金融セクターの規則が少なくとも同等である場合にはこれに譲る。したがって機関は、DORAを実効的なレジリエンス試験体制として扱うべきであり、同時に、共有された技術子会社のような金融の境界の外にあるグループ主体が、NIS2の内側にとどまり、同じ試験のエビデンスから便益を受けうることを認識すべきである。

合衆国: NYDFS Part 500とFFIECの期待

ニューヨーク州金融サービス局のサイバーセキュリティ規制は、各対象主体に対し、その情報システムの侵入テストを、当該主体のリスク評価に基づき、システムの境界の内側と外側の双方から、少なくとも年次で実施することを要求する（New York State Department of Financial Services 2023）。改正された規制は、ガバナンスと試験の期待をさらに引き締めた（Ropes and Gray 2026）。連邦の水準では、連邦金融機関検査協議会は固定の規則を課さないが、その情報セキュリティ手引きの中で、有資格かつ独立した当事者による侵入テストを検査官の期待であり成熟度の指標として扱う（Federal Financial Institutions Examination Council 2016）。7.3Aを高い水準で満たし、境界の内側と外側の双方から定められた頻度で試験する機関は、NYDFSの検査官とFFIECの検査がまさに期待する成果物を生み出す。

カナダ: OSFIガイドラインB-13

2024年1月1日以降施行されている金融機関監督庁ガイドラインB-13は、連邦規制下の金融機関に対し、定期的な試験を通じて脆弱性を特定することを要求し、重要な技術的足跡を持つ機関に対しては、現実的な多段階の攻撃を模擬するインテリジェンス主導の、脅威主導の侵入テストとレッドチーム演習を期待する（Office of the Superintendent of Financial Institutions 2022）。B-13は成果に基づくものであり、固定の頻度を設けないため、機関はその頻度ではなく試験の質と現実性を通じて準拠を立証する。これは、DORAおよび先鋭化された7.3Aのガイダンスが表現するのと同じインテリジェンス主導の水準であり、それがB-13を、別個の義務ではなく同じ一族のカナダの一員たらしめている。

一つの背骨: 各法体系をNIST CSF 2.0へと写像する

合衆国とカナダの双方を統治する単一の金融規制当局は存在しないため、国境をまたぐ機関は、双方で認知された中立

的な参照基準を必要とする。NISTサイバーセキュリティフレームワークバージョン2.0がその参照基準である。すなわち、任意であり、国境の両側で広く採用され、六つの機能を中心に組織されている。すなわち、統治、特定、防御、検知、対応、復旧である（National Institute of Standards and Technology 2024）。背骨として用いれば、それは機関が一つの侵入テストプログラムを記録し、その結果を、あらゆる法体系が理解する語彙で表現することを可能にする。侵入テストは、脆弱性を表面化させることによって特定に最も直接に語りかけ、機関の監視と対応が現実的な侵入を実際に捉え封じ込めるかを測定することによって、検知と対応に語りかける。統治の機能は、五つの法体系すべてが要求する交戦規則、独立性、取締役会報告を担う。表1がこの収斂を具体的にする。

表1. 一つの侵入テストプログラム、四つの法体系、一つの背骨

次元	SWIFT 7.3A v2026	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
性質	助言的統制	重要な主体に義務	義務的規則	成果に基づく期待	任意の参照基準
頻度	3年のシナリオ周期	少なくとも3年ごと	少なくとも年次	固定の頻度なし	規定なし
手法	シナリオに基づく、セキュアゾーン重視	インテリジェンス主導のレッドチーム	内側と外側、リスクに基づく	インテリジェンス主導、レッドチーム	機能と成果
独立性	有能で独立した当事者	認定されたプロバイダー	有資格の内部または外部	独立した保証	ガバナンスの成果
主要なエビデンス	スコープ、発見事項、是正	脅威シナリオ、攻撃の叙述、是正	試験報告書、是正の頻度	試験の現実性と成果	写像された成果

各行を横断して読むことが、その論旨である。すなわち、各列における最も要求の厳しい水準に試験を設計せよ。インテリジェンス主導の手法、セキュアゾーンを意識したスコープ、内側と外側の双方の網羅、独立した実行、追跡された是正であり、そうして得られる単一の記録が、五者すべてを満たすのである。

リスク主導の準備モデル

7.3Aのガイダンスは、機関が統制の名指すものの最小限を行うコンプライアンスの読みを招く。より価値があり、監督当局がますます報いる読みは、リスク主導のものである。すなわち、侵入テストは、機関の最も帰結の重い露出を表面化させ退役させるために用いる道具であり、コンプライアンスはそれをよく行うことの副産物である。

準備は、リスクとスコープのベースラインから始まる。機関は、自らのSWIFT関連の資産、すなわちセキュアゾーン、メッセージングインターフェース、オペレーターのワークステーション、ネットワークへの接続、そしてそれに供するバックオフィスのシステムを棚卸しし、試験のしやすさによってではなく、侵害の帰結によって各経路を順位付けする。これは、金銭と信頼がどこに宿るかによって定義されるスコープを生み出し、それはまた現実の敵対者が選ぶであろうスコープでもあり、B-13の帰結主導の姿勢およびNYDFSのリスクに基づく姿勢と整合する。

次に来るのは、脅威インテリジェンスによる枠付けである。金融メッセージングを標的とするアクターについての現在のインテリジェンスがシナリオを形作り、それによって試験が、汎用的なものではなく、もっともらしい侵入を演練するようにする。これが、侵入テストを脅威主導の試験へと変える段階であり、それが同じ演習をDORAとB-13のもとで信用に値するものたらしめる段階である。

しかるのちに実行は、7.3Aのガイダンスが描く三年周期にわたって各シナリオを走らせ、アプリケーション、インフラストラクチャ、人的経路を、境界の内側と外側から、独立した当事者によって、文書化された交戦規則のもとで網羅する。機関は、何が見つかったかだけでなく、自らの検知と対応が試験の発生を見たかどうかを測定する。なぜなら、その測定こそ、検知と対応の機能が要求するエビデンスだからである。

最後に、是正とエビデンスが輪を閉じる。発見事項は、その終結が記録される追跡された是正サイクルへと入り、その記録の全体、すなわちスコープ、シナリオ、攻撃の叙述、発見事項、是正、検知の性能が、NIST CSF 2.0という背骨に対して一度だけ提出され、各法体系へとタグ付けされる。この輪を完遂する機関は、一つの試験に合格したのではない。それは、再利用可能なレジリエンスのエビデンス資産を築いたのである。

当社のSWIFT
CSP評価サービスは、7.3A試験をこの水準でスコープし走らせ、PenTevaが発見事項を検証し終結まで追跡することで、そのエビデンスが四つの法体系のいずれのもとでも持ちこたえるようにする。DORAのレジリエンスモデリングがスコープに入る場合、DORA-MASTが同じエビデンスを運用上のレジリエンスの像へと運ぶ。

結論

先鋭化された7.3Aのガイダンスは、孤立したSWIFTの要件としてではなく、インテリジェンス主導の、脅威に基づく試験への世界的な運動の一つの監督上の表現として理解するのが最もよい。自らの2026年の侵入テストをその水準で設計し、帰結によってスコープし、現在の脅威インテリジェンスで枠付けし、セキュアゾーンを横断して独立に実行し、その結果を共通のフレームワークに対して記録する機関は、DORA、なお適用される場合のNIS2、NYDFS Part 500、そしてOSFI
B-13を、同じ演習から満たすことができる。侵入テストは、繰り返されるコンプライアンスの費用であることをやめ、機関が重要なリスクを見つけ退役させる道具となる。一度の試験で、多くを満たす。

頭字語

CSCF、顧客セキュリティ統制フレームワーク（SWIFT）。CSP、顧客セキュリティプログラム（SWIFT）。DORA、デジタルオペレーショナルレジリエンス法。FFIEC、連邦金融機関検査協議会。ICT、情報通信技術。NIS2、ネットワークおよび情報セキュリティ指令（第二次）。NIST
CSF、国立標準技術研究所サイバーセキュリティフレームワーク。NYDFS、ニューヨーク州金融サービス局。OSFI、金融機関監督庁。SWIFT、国際銀行間金融通信協会。TIBER-EU、脅威インテリジェンスに基づく倫理的レッドチーミング（欧州フレームワーク）。TLPT、脅威主導の侵入テスト。

References

European Central Bank (2018). TIBER-EU Framework. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Commission (2025). NIS2 Directive: transposition in EU countries. https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Parliament and Council (2022a). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj

European Parliament and Council (2022b). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Federal Financial Institutions Examination Council (2016). Information Technology Examination Handbook: Information Security. https://ithandbook.ffiec.gov/it-booklets/information-security/

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

New York State Department of Financial Services (2023). Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Part 500 (as amended). https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

Office of the Superintendent of Financial Institutions (2022). Guideline B-13: Technology and Cyber Risk Management. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Ropes and Gray (2026). NYDFS-regulated entities face stronger cybersecurity regulations. https://www.ropesgray.com/en/insights/alerts/2026/01/nydfs-regulated-entities-face-stronger-cybersecurity-regulations

SWIFT (2025). Customer Security Controls Framework v2026, Customer Security Programme. https://www.swift.com/myswift/customer-security-programme-csp