SWIFT CSCF v2026 · Control 7.3A

SWIFT CSCF v2026 Control 7.3A ペネトレーションテスト準備チェックリスト

1. 影響度に基づいてスコープを決める

- ☐ SWIFT 環境の棚卸しができている (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、およびそれに連携するバックオフィスシステム)。
- ☐ 攻撃経路が、テストのしやすさではなく、侵害された場合の影響度によって順位付けされている。
- ☐ スコープがセキュアゾーンとその信頼境界に対して定義されており、攻撃者がバックオフィスからメッセージング層へ横展開できないことをテストで証明できる。
- ☐ 3年間のシナリオサイクルにわたってテストが計画されており、アプリケーション、インフラストラクチャ、人的経路を網羅している。

2. 脅威インテリジェンスで構成する

- ☐ 金融メッセージングを標的とする攻撃者に関する最新のインテリジェンスが、テストシナリオに反映されている。
- ☐ シナリオが、一般的な脆弱性の分類ではなく、もっともらしく具体的に名前の付いた侵入経路を再現している。
- ☐ インテリジェンスの根拠が文書化されており、DORA および OSFI B-13 における脅威主導型テストとして認められる。

3. もっとも厳格な基準で実施する

- ☐ テストはシステム境界の内側と外側の両方から実施され、NYDFS Part 500 の期待事項を満たしている。
- ☐ テストは、能力があり十分に独立した者によって実施されている。
- ☐ 稼働中のシステムをテストするための実施規則、認可、安全管理策が文書化され、承認されている。
- ☐ 定められた頻度が設定および記録されており、NYDFS の年次最低要件と SWIFT のサイクルを同時に満たしている。

4. 自社の防御を測定する

- ☐ この演習は、何が発見されたかだけでなく、模擬侵入を監視機能が検知できたかどうかを測定している。
- ☐ 対応と封じ込めの実績が、検知機能と対応機能に照らして記録されている。
- ☐ 検知のギャップは、それ自体を独立した発見事項として記録している。

5. ループを閉じ、証拠を蓄える

- ☐ 発見事項は、担当者と期日を伴う追跡可能な是正サイクルに登録されている。
- ☐ 是正の完了が、単なる主張ではなく証拠で裏付けられている。
- ☐ 全記録 (スコープ、シナリオ、攻撃の経緯、発見事項、是正、検知実績) が、NIST CSF 2.0 を背骨として一度だけ保管されている。
- ☐ 単一の記録が各規制 (SWIFT 7.3A、DORA、NYDFS Part 500、OSFI B-13) にタグ付けされている。