CPMI-IOSCO Cyber Resilience Toolkit（2026年9月）に関する技術的意見

大規模サイバー侵害を前提とした金融市場インフラの取引状態の検証可能性

― 証拠保存の欠落がもたらす網羅性の問題と、検証可能性の保証条件 ―

TriStruct株式会社　｜　2026年11月3日　CPMI-IOSCO へ提出　｜　要旨と結論

要旨

サイバー侵害後の復旧に先立つ検証は、二つの根本的な課題を抱える。

第一は、対象データの真正性である。サイバー侵害によってあらゆる構成要素が侵害対象となり得る状況では、事後的に構成されるログやバックアップの照合だけでは、対象データ全体の真正性をどこまで保証できるのかが明確でなく、検証結果に推定が介在する余地が残る。

第二は、検証対象の網羅性である。ログの未発行や、業務上の確定から証拠保全までの時間的な遅延が存在する場合、侵害によって取引データやログの存在自体が失われ得る。その場合、本来存在すべき取引が痕跡を残さず失われ、残存する記録の照合だけでは、その欠落自体を検知できない可能性がある。

本稿は、既存の復旧手段の不備を指摘するものではない。高度化するサイバー侵害によって顕在化したデジタルデータの構造的課題を明らかにし、復旧前検証の信頼性をさらに高めるため、真正性と網羅性の二つの課題を提示し、その評価基準を示すことを目的とする。また、解決方法の一例として、業務上のデータ確定と証拠の生成・保全を連動させて真正性を確保する構成と、証拠の生成・保全結果の追跡によって、この全件性を検証する構成を示す。

そして、既存の復旧・照合手段を補完し、復旧判断の信頼性と検証範囲を明確にするため、真正性と網羅性に関する評価基準をCPMI-IOSCO Cyber Resilience Toolkit §3.3.2に追加することを提案する。

結論

サイバー侵害後に金融市場インフラが安全に業務を再開するには、障害時点の取引データの内容と処理状態を、信頼できる根拠から特定する必要がある。

バックアップ、取引再実行、独立照合、RT2の独立保存基盤は重要な復旧手段である。しかし、保存記録間の一致は、対象となる業務確定データの全件に証拠が対応することや、証拠が確定時点のデータ内容を表していることまで保証しない。

本稿が提案する五つの保証条件は、残った証拠の正しさだけでなく、残るべき証拠が全件存在するか、保存の失敗や結果未確定を把握できるかを評価するためのものである。既存の復旧・照合手段を補完し、真正性を立証できる範囲とできない範囲を明確にすることが、本提案の目的である。

本書は、CPMI および IOSCO の事務局に提出した意見書（英文）の、要旨と結論の日本語原稿である。TriStruct株式会社　https://tristruct.co.jp