第 23 回コラボレーション・プラットフォーム　開催レポート

「第 23 回（2022 年度上半期）コラボレーション・プラットフォーム」を開催した。

2022 年度のコラボレーション・プラットフォームは従来まで多くの方にご参集いただいたうえで開催としていた「集合型」、「Webinar 型」による開催ではなく、有識者少人数による特定テーマに関する意見交換会とした。

◆テーマ概要（１）◆

『非財務情報(サイバーセキュリティ対策)の企業開示に向けて』

企業の地球環境や気候変動への対応、またサプライチェーンにおける人権への配慮など、考慮すべき ESG （Environment, Social and Governance：環境、社会、ガバナンス）課題の範囲とその重要性が拡大してきている。特に海外においては ESG 投資への関心が高まる中、非財務情報に関する客観的な情報開示が自社を魅力ある投資先として位置付けるための手段として注目されてきている。サイバーセキュリティに対する企業の取り組みについても同様に海外での企業開示に向けた議論は活性化してきている。

一方、国内においては、政府、関連団体、セキュリティ業界等からの企業開示に向けた仕組み作り（情報セキュリティ報告書など）、啓発などは進められてきたが、一部の企業からの開示は進むも社会実装としては遅々として進んでいない。今回、投資家目線で企業開示に携わる専門家とセキュリティ業界において本件問題意識をもった有識者との間で、この課題について深掘りの意見交換を実施し、次のアクションを検討した。

◆開催概要◆

実施　：2022 年 4 月~8 月　全 8 回

開催　：オンライン

主催　：独立行政法人情報処理推進機構

◆メンバー◆

情報セキュリティ大学院大学　情報セキュリティ研究科	教授	藤本　正代　氏
株式会社野村総合研究所	上級研究員	三井　千絵　氏
PwCコンサルティング合同会社　テクノロジーコンサルティング	パートナー	丸山　満彦　氏

◆議事抜粋◆

【米国の動向】

・2022 年 3 月米国 SEC の改訂で以下を要求する動きになっている

✓インシデント遭遇 4 営業日以内での開示

✓取締役のメンバーがサイバーセキュリティの専門知識を有しているか否かの開示

・厳しい基準に見えるが米国では事前準備するのは当然という考え方がある。

・アンケート『米国取締役協会(NACD)の 2016-17 調査』では「米国経営層において強化すべき専門領域」としてサイバーセキュリティへの従事が一位(29%)となっている。

【日本の状況】

・日本では、2021 年 6 月コーポレートガバナンス・コードにおける取締役の「知識・経験・能力等の一覧を開示すべき」項目について「セキュリティ」項目を付したのは時価総額 TOP100 社のうち 3 社のみ。

・米国の経営層と日本の経営層にサイバーセキュリティリスクに対する考え方に大きなギャップがあり、日本では企業の取締役が、その責任を深く意識しているかどうかが問題。

・日本の現状としてはコーポレートガバナンス・コードに「セキュリティ」のキーワードが入った、という段階。

【投資家の方々と企業との対話に向けて】

・SEC、FRC、PRI の開示レポートを参考にするのが良い。サステナビリティ報告書が適当。投資家向けの開示資料では「経営者の責任」「体制」「ガバナンス」を記載する。「経営者のスキル・マトリックス」「リスクの認識」が重要。

・法定開示資料としての「有価証券報告書」には監査が紐づいている。投資家から企業経営者への確認項目として「有価証券報告書」に適切に記載させる等が良い。

・「SEC」「FRC」「PRI」ガイドラインの内容を情報共有し日本の経営層向けの確認項目を検討すべき。

・制度開示資料である「有価証券報告書」を第一優先にして、「コーポレートガバナンス報告書」、もしくは「サステナビリティ報告書」に何某かの記載がなされる動きに繋がれば良い。

【社会実装に向けて】

・海外の動向に遅れないことが必要。

・SEC、FRC 等の海外の動向を踏まえ、日本でのセキュリティ情報の開示を本格的にスタートしなければいけないタイミングだとの危機感がある。

・FRC が実施しているようなベストプラクティスを話し合う案がある。FRC ラボのように投資家の方々中心に開示に関する意見交換をするのが良い。参加公募型のベストプラクティスのワークショップを開催し、SEC の今回の改訂や FRC、PRI を参考にしながら企業経営者、資産運用関係者等とのディスカッションを実施するフェーズに移行するのが良い。

◆テーマ概要（２）◆

『2022 年度サプライチェーン調査を実施する視点』

IPA の昨年度調査『クラウドサービスのサプライチェーンリスクマネジメント調査』の結果を 3 月に公開した。今後の調査にあたり、視点、整理の仕方、その他参考情報などについて本業界の方々にご意見をヒアリング、意見交換を実施した(下記)。

(1)SaaS を選定するための情報開示および選定の実態（①）

(2)安全に SaaS を運用するための情報開示および利用の実態（②）

①利用者がクラウドサービスの選定時に利用する情報

②運用時に利用する情報

＜①②以外に公開されるべき情報はあるか＞

◆開催概要◆

日時　：2022 年 7 月 全 2 回

開催　：オンライン

主催　：独立行政法人情報処理推進機構

◆議事抜粋◆

【総務省の情報開示指針の動向について】

・総務省の「クラウドサービスの安全・信頼性に係る情報開示指針」に関連するガイドとしては、2007 年総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」が「クラウドサービス提供における情報セキュリティ対策ガイドライン」に統合され、その後改定され 2021 年 9 月に第 3 版が公開されている。

・第 3 版改定時に NIST SP800-53 rev.5 の要件も考慮されている。

・意見募集中の「クラウドサービスの利用・提供における適切な設定のためのガイドライン」（案）も今後情報開示指針に反映されると考えられる。

【現時点のクラウド事業者の情報開示に係る課題認識について】

・ASPIC の情報開示認定等を取得していない、新規参入事業者の情報開示の実態は不明。

・中堅以下の SaaS 事業者は、PaaS が提供するセキュリティ機能を使用していることが多い。

・民間での SaaS 調達における調達基準について実態を把握できると今後のガイド作成の参考にできる。

・IaaS、PaaS であればプロバイダが限定されるのでセキュリティ要件はほぼ統一化できる、また IaaS、PaaS 事業者はセキュリティ対策への意識が高いと想定できるので詳細リスク分析も可能。一方、SaaS 事業者は多種多様で、セキュリティ対策も様々。利用者はどうやって評価すれば良いのか、これをインタビューで調査するのが良い。

【事業者のセキュリティ対策に対する、利用者の評価方法について】

現時点、以下の評価方法があり、今年度調査を通して利用実態が見える化されるのが好ましい。

①自分でチェックリストを作成して実施する。但し実行するためには高いスキルが必要。

②フレームワークを使用する。総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」に基づく情報開示や監査の観点での基本言明に係る情報開示、海外事例では CSA が出している評価のためのフレームワークである CCM、CAIQ、CAIQ-Lite 等。

③各ベンダーが提供する CASB のなかのクラウドサービスリスク評価のスコアリングサービスを利用する。

④欧米ではプロバイダの評価、特に SaaS プロバイダの評価のサービスとして VRM、TPRM を利用する。日本でもこのサービスを提供しているベンダーが出てきており利用できるようになってきている。

⑤プロバイダが公開している情報(ホワイトペーパー)を利用する。

⑥欧米では CSA が紹介する「Security, Trust, Assurance, and Risk (STAR) Registry (STAR

Registry)」という、クラウドサービスプロバイダが自己評価した結果を公開できるサイトがあり、そのサイトを利用する。

【利用実態に係る参考情報について】

・CASB ベンダーが行っているスコアをそのまま評価している企業は実際にあり成功事例と考える。

・逆にチェックリストを独自に作って評価しようとしている会社は行き詰っている会社が多い。

・欧米の STAR Registry のサイトではプロバイダのリスト（現時点、1500 社以上）があり、そのプロバイダが提供しているクラウドサービスに対して CAIQ に基づいた自己評価結果が公表され、利用者はそれを確認している。

・欧米では、プロバイダはセキュリティ情報を積極的に公開しサービスの信頼度を差別化要素として競争している。日本の場合は“セキュリティ情報を公開するとリスクが増大する”と考える組織が多く、積極的に公開しサービスの信頼度を差別化要素とする動きに繋がらない。

・CSA でクラウドセキュリティに対する 11 の悪質な脅威というのを出している。最近では、プロバイダの脆弱性やプロバイダの問題に起因する脅威は少なくなり、脅威の原因は利用者側の設定ミスなどになってきている。

【注視すべき SaaS カテゴリーについて】

・重要インフラ/ID 管理/企業の基幹業務の BCP 関連で使われている SaaS は注視が必要。

【あるべき姿について】

・IaaS、PaaS 事業者については詳細リスク分析による評価に取り組むことで CAIQ の使用が可能になる。SaaS 事業者については CASB を導入している利用者は CASB の評価で始めつつ、CAIQ-Lite、更にそのあとで CAIQ を使った詳細リスク分析へとステップアップしていくことが望ましい。

・欧米での動向にもある通り、利用者が自由に評価結果を確認することができると同時に、市場での評価を得るためにも SaaS 事業者を含むクラウドサービス事業者からのセキュリティ情報の公開は必要と考える。

以上