**SSRM(Supplier Security Risk Management)について**

 　キンドリルジャパン株式会社

 　購買

ソフトウェアおよび一部サービスのお取引において、弊社米国本社のセキュリティ担当部門からタイトルの冒頭に[OneTrust]とある英文のメールが送信されることがあります。

送信元アドレスは以下のとおりです。

Kyndryl Regulatory Office <KyndrylRegulatoryOffice@kyndryl.com>

これは弊社セキュリティ部門により、サイバー攻撃やサプライチェーンにおける脆弱性のリスクから弊社とお客様とを保護する目的で導入されたSSRM(Supplier Security Risk Management)というプログラムで、アンケートにご回答いただいた内容から、セキュリティ部門の専任チームによる査定をさせて頂きます。

お手数で恐縮ですが、サイバーセキュリティにかかわる将来の事故や損害から、お客様・貴社および弊社を守るための仕組みとして、趣旨ご理解のうえ、ご協力のほどよろしくお願いいたします。

アンケートには以下の二種類があります：

1. Inherent Risk Questionnaire (IRQ)

この質問票は27の質問（添付ワードファイル参照）で構成され、主に以下の観点から、ソフトウェアおよびサービスのリスクの所在を確認させて頂くものです。



* お客様・弊社のIT環境との接続（クラウドを含む）
* データの処理・管理のシステム的・地理的環境
* 製品の使用目的やお客様への提供形態
* 製品・ソリューションの開発環境、コンポーネントの入手経路
* 製品・ソリューションの目的（セキュリティ関連製品かどうか）
1. SIG Lite

この質問票は米国の認証機関である[Shared Assessments](https://sharedassessments.org/sig/)が導入しているStandardized Information Gathering（SIG）と呼ぶアンケート様式に則っており、以下のような外部機関の認証取得の確認と、SDLC（Software Development Life Cycle）上のリスク管理、Penetration Testレポートの維持など、より詳細にサイバーセキュリティ対応状況や、サプライチェーンにおける脆弱性について確認させて頂くものです。

-SOC 2 Type 2 report
-ISO / IEC certifications (e.g., 27001 and 27017) and Statement of Applicability of Controls
-Completed SIG (Standardized Information Gathering)

-CAI (Consensus Assessments Initiative) self-assessment questionnaires.

以下にその内容の例を添付します（ケースによって若干の異同があります）。



なおこのSIGは、1)のIRQへのご回答を確認させて頂いた結果、さらに詳細についてセキュリティ部門からご回答をお願いする場合にのみ、お送りするものです。

＜ご回答の注意点＞

SSRMは弊社グローバルセキュリティ組織の展開する統一プログラムで、各国のローカルサポートチームを持っておりません。従って、お送りする内容は英語になります（質問自体は各国語への変換機能あり）。恐縮ですが上記の日本語訳をご参照頂き、英語でご回答頂きますようお願いいたします。

ご回答はKyndryl Regulatory Office <KyndrylRegulatoryOffice@kyndryl.com>から送信されるメールに記載されるボタンから専用ツール（OneTrust）にログイン頂き、各質問に従ってご記入、最後に提出（Submit）ボタンを押して頂くことで完了します。メールに記載されるID：xxxxxという５桁の番号は、お問い合わせ頂く際のキー情報になりますので、控えて頂くと便利です。

なおメールにはDeadline (ご回答期限)が記載されており、期日を過ぎて提出がなされない場合には、自動的に督促メールが送信される仕組みになっています。何らかの理由で、ご回答が不要になった場合でも、送信がストップしないことがあり、大変恐縮ですがそのような場合は、弊社購買担当者までお知らせください。

＜サポート・連絡先＞

当プロセスについてのご質問、ご不明点は、貴社を担当する弊社の購買担当者までお知らせください。すぐにお答えできない場合は、弊社内のスタッフおよび本社のセキュリティ部門と連携のうえ、サポートさせて頂きます。

どうぞよろしくお願い申し上げます。

 以上