クラウドをはじめとするサービスにおける セキュリティ品質向上への取り組み

クラウドサービスをはじめとしたお客様に提供するサービスを安心安全にご利用いただくために、サービスプロバイダーは、常に変化するセキュリティ脅威に対応していく必要があります。富士通は、サービスプロバイダーとして実施すべきセキュリティ対応事項を明確化し、ガイドラインや対策基準を策定し監査しています。また、インシデントの対応を専門に実施する組織の整備、第三者評価、および情報公開にも取り組んでいます。

クラウドサービスへの対策基準による取り組み

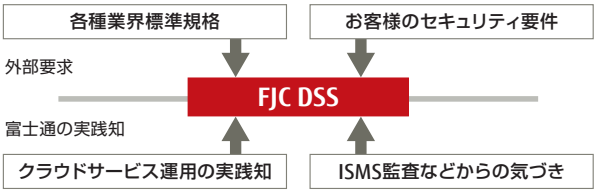
日本国内のデータセンターにおいて稼働するクラウドサービスが増加するに従い、セキュリティ面の不安やレイテンシ（遅延）問題は低減され、コスト削減・可視化、業務継続性の期待により、パブリッククラウドを第一の選択肢とする「クラウドファースト」の時代が到来しています。

経済産業省、CSA、ENISAなどの様々な団体がクラウドセキュリティガイドラインを公開しています。また、その経済産業省のガイドラインをベースとした国際標準規格であるISO/IEC 27017が2015年12月に発行されました。しかしこれらのガイドラインにおける要求事項は、クラウドサービスを活用する側が、どのセキュリティ強度の対策をとるか自由に選択できるようになっているため、クラウドサービス提供者ごとに対応レベルのばらつきが出てしまいます。

そこで富士通では、これらの外部セキュリティ要求事項と、お客様のセキュリティ要件、さらに、富士通社内の実践知から独自のセキュリティ基準である「富士通クラウドデータセキュリティスタンダード」（FJC DSS※）を策定し、富士通のクラウドサービスも含めて実践していきます。これにより、富士通が提供するクラウドサービスがばらつきなく、一定のセキュリティ品質を満たしているかを明らかにすることが可能となります。

〔※〕FJC DSS：Fujitsu Cloud Data Security Standard

FJC DSSの策定方針



ガイドラインや監査による取り組み

富士通では、お客様に提供するサービスのセキュリティ品質を確保するため、サービス開発工程とサービス運用工程で実施すべき事項を「サービスセキュリティ対応ガイドライン」としてまとめています。

各サービスを提供する部門は、このガイドラインで示した内容に基づき、セキュリティ対策を実践します。サービス開始の前には、監査部門がセキュリティ対策の実施状況を監査し、セキュリティ品質確保を担保しています。

サービス運用時には、監査部門によるセキュリティ定期監査を実施します。必要に応じて是正対応を行うことで、セキュリティ品質の確保と向上を継続的に実現しています。

富士通クラウドCERTの取り組み

クラウドをはじめとするサービスのセキュリティを専門的に扱う「富士通クラウドCERT（Computer Emergency Response Team）」は、クラウド環境を各種のセキュリティ脅威から守り、お客様のビジネスを支えるために、グローバル規模で以下のような活動を行っています。

1. 情報セキュリティ運用

お客様に安心して富士通のクラウドサービスを利用していただくために、外部からの様々な攻撃を水際で検知するモニタリングなどのセキュリティ対策を実施し、24時間365日体制で運用しています。

2. 緊急対応

インシデント発生時のプロセスを定め、万一のインシデント発生時には、事象の識別・解決・被害局所化を迅速かつ確実に実施します。

3. 情報セキュリティマネジメント

お客様の大切な情報を守るために、富士通クラウドサービスにおける「人」、「モノ」、「情報」を適切にマネジメントします。さらに、日本シーサート協議会、FIRST※などのセキュリティ関連団体に加盟し、グローバルなクラウドセキュリティの向上のために活動しています。

〔※〕FIRST：Forum of Incident Response and Security Teams

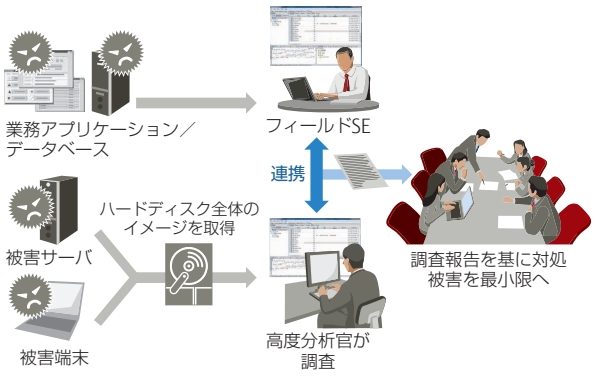
富士通クラウドCERTの活動

リアルタイム監視から侵害調査を自社で対応

自社の高度分析官によるデジタルフォレンジック技術を活用し、グローバルなマルチクラウド環境も含め、サイバー攻撃による不正アクセス、侵害状況の調査を実施しています。その際、攻撃を受けたサーバ、端末のハードディスクの情報から不正アクセスの証拠（ファイル改ざん、不正プログラム）を特定、攻撃を受ける原因となった脆弱性や不正活動による影響範囲を調査します。

また、ログや削除ファイルの復元により、不正アクセスの痕跡を見つけ出し、サイバー攻撃の全容を解明します。さらに、単なるデジタルフォレンジックに留まらず、必要に応じてフィールドSEと緊密に連携し、業務アプリケーションやデータベースも解析することにも対応しています。

侵害調査のプロセス



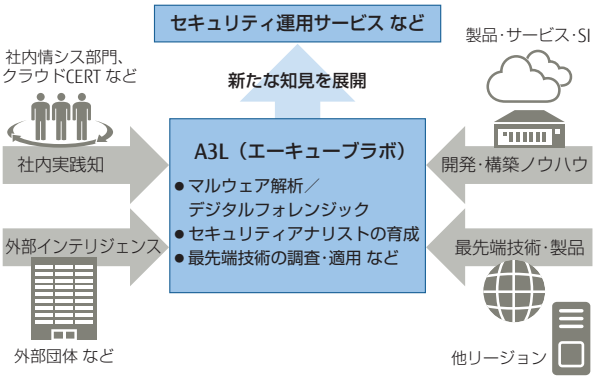
富士通グループのナレッジを集約する調査・研究施設の活用

巧妙化するサイバー攻撃への追従、高度な分析･解析技術の集約･強化を目的に「A3L（エーキューブラボ）」※を、2015年11月に新設しました。インシデントの分析・マルウェア解析と、脅威情報の活用により新たな攻撃手法を発見し、サービスへ展開することが目的です。

攻撃者の真の狙い･目的を明らかにすることで、今後発生する可能性がある攻撃に対する先回りした対策･防御を実現します。具体的には、アーティファクト分析（マルウェアや標的型メールなどの攻撃手法の分析、解析）の実施と、脅威情報（Cyber Threat Intelligence）の蓄積、共有、活用を実施しています。

〔※〕A3L：FUJITSU Advanced Artifact Analysis Laboratoryの略称。

調査・研究施設の活用



インシデント対応訓練によるセキュリティ耐性強化

運用で検出されたイベントの統計や、外部環境や攻撃手法の変化を踏まえ、運用環境の改善のために、「インシデント対応訓練」によるセキュリティ運用耐性の強化を実施しています。

インシデント対応の訓練は、実情にあった複数の想定シナリオからその場で使用するシナリオを選択し、机上演習形式で実施しています。また、インシデント対応訓練より洗い出した課題・リスクに対しては、話し合いで改善案の取りまとめを実施し、各種のインシデント対応で使用するフローやドキュメント、関連組織間の連携手順を継続的に改善しています。

インシデント対応訓練のプロセス