報道資料

SoftBank Technology

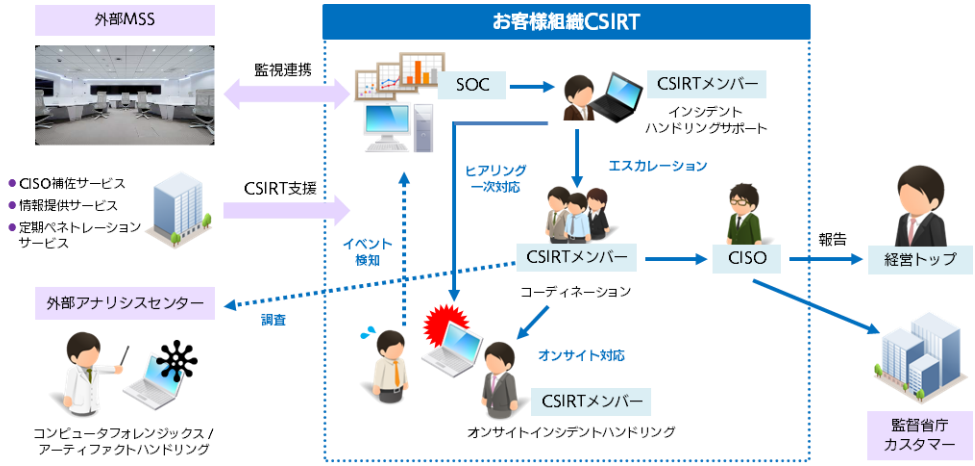
2017年10月25日

サイバー攻撃を想定した社内体制構築を支援するサービスを開始

～ 経営リスクを最小限に。侵入後の迅速な対応を目指す「CSIRT 構築支援サービス」～

ソフトバンク・テクノロジー株式会社（本社：東京都新宿区、代表取締役社長：阿多 親市、以下 SBT）は、サイバー攻撃によるセキュリティインシデントへの対応を目的とした組織内 CSIRT（シーサート※）の構築および既存 CSIRT の見直し・強化を支援する「CSIRT 構築支援サービス」を提供開始しますのでお知らせします。

（※）Computer Security Incident Response Team の略、セキュリティ上の問題を監視し、問題発生時に原因解析や影響範囲の調査を行う組織



セキュリティ対策ソフトメーカーが発表した 2016 年の脅威ブロック件数は全世界で 800 億件を超えてます。攻撃件数の増加に加えて、攻撃の内容も巧妙化・悪質化に伴い、昨今はサイバー攻撃を受けた際のサイバーレジリエンス（回復力）に主眼をおいた CSIRT 体制の構築が重要なテーマになっています。

しかし、セキュリティ・組織・仕組みなどさまざまな観点から情報を整理し、検討・構築・運用へつなげる体制の構築には、セキュリティ専門家の存在が欠かせません。また、構築後の運用も必要になります。

CSIRT 構築支援サービスは、セキュリティの専門家がお客さまの現状を分析し、ご要望に応じた CSIRT の早期立ち上げや CSIRT の強化・見直しを支援します。また、CSIRT の安定運用を支援するオプションとして、CISO の相談対応や会議体への参加、定期的に疑似的な攻撃を仕掛けて脆弱性の確認を行う他、マネージドセキュリティサービス（MSS）としてインシデント判断や復旧などのセキュリティ運用・監視まで提供します。

■ **CSIRT 構築支援サービスの詳細はこちらをご覧ください。**
https://www.softbanktech.jp/service/list/csirt/

SBT では、各種診断サービスから侵入防御ソリューションの提供に加えて、侵入後の検知や対処といったセキュリティ運用まで提供することで、お客様の情報資産保護や事業継続をワンストップでサポートいたします。

■ **SBT のセキュリティソリューションはこちらをご参照ください。**
https://www.softbanktech.jp/service/name/security/

報道関係者様向け お問い合わせ窓口	ソフトバンク・テクノロジー株式会社 コーポレートコミュニケーショングループ（皆口、吉田、與儀）
	TEL：03-6892-3063 / Email：sbt-pr@tech.softbank.co.jp