2016 年 7 月 6 日

報道関係各位

伊藤忠テクノソリューションズ株式会社
東京都千代田区霞が関 3-2-5 霞が関ビル
代表取締役社長　菊地　哲

CSIRT の構築・運用を支援するセキュリティサービスを開始

インシデントの予防と対応の両面から総合的に支援

伊藤忠テクノソリューションズ株式会社（代表取締役社長：菊地　哲、本社：東京都千代田区、以下：CTC）は、サイバー攻撃に伴うセキュリティ・インシデント（事案）に対応するための、「CSIRT（Computer Security Incident Response Team）」と呼ばれる組織について、企業内での立ち上げから運用まで総合的に支援する「CSIRT 構築・運用支援サービス」を本日から提供します。標的型攻撃への対策の強化やセキュリティの専門家を必要とする企業にサービス展開し、3 年間で 20 社への導入を目指します。

近年、特定の企業や団体を狙った標的型攻撃を含めてサイバー攻撃は高度化、巧妙化しており、検知されたインシデントを早期に対応して被害を最小限に抑える専門組織 CSIRT を設置する企業が増加しています。しかし、CSIRT にはインシデントの分析や対策の立案・推進ができる高度なセキュリティ人材を確保する必要があり、セキュリティ強化を目指す企業の課題となっています。

CTCが今回開始するサービスは、長年のセキュリティサービス提供でのノウハウに基づき CSIRT の構築・運用を支援するものです。セキュリティについて現状を評価する「CSIRT アセスメントサービス」と CSIRT の計画策定を支援する「CSIRT プランニングサービス」、専門性が高い業務をCTCのエンジニアが代行する「CSIRT 運用支援サービス」で構成されます。

CSIRT アセスメントサービスは、システムや情報資産の確認やオンサイトでの調査によって、セキュリティリスクの洗い出しを行い、CSIRT プランニングサービスでは、お客様の要件に応じた CSIRT の計画策定を支援します。

また、CSIRT 運用支援サービスは、インシデントの予防と対応の両面を支援するものです。予防面では脆弱性調査や脅威情報の収集、サイバー攻撃への演習、セキュリティルールの見直しなどを通してセキュリティレベルの維持・向上に貢献します。対応面では、システムを 24 時間 365 日遠隔監視する「CTCセキュリティ・オペレーション・センター（以下：CTC-SOC）」と連携したインシデントの高度な調査・分析や、復旧支援により早期解決につなげ、再発防止策の提供も行います。

CTCは既に、セキュリティの検査・監査・コンサルティング、お客様企業ごとのセキュリティシステムの構築、CTC-SOC を活用した遠隔運用サービス「CTCマネージド・セキュリティ・サービス（以下：CTC-MSS）」を含めたトータルなセキュリティサービスを提供しています。

今後は、CTCの組織内 CSIRT で蓄積したセキュリティの情報も活用し、「CSIRT 構築・運用支援サービス」を拡充することで、お客様のセキュリティ強化に貢献していきます。

＜CSIRT 運用支援サービス 運用業務メニュー＞

CSIRT 業務分類	業務概要
システムリスクマネジメント（予防策）	
システム堅牢化	システムの脆弱性を継続的に特定し修正します。また、セキュリティ製品の導入・運用により、横行するサイバー攻撃からシステムを保護します。
情報収集・分析	情報セキュリティリスクをもたらす脅威や脆弱性の情報を収集・分析し必要な対策を検討し、情報セキュリティの最新動向を調査します。
規程・教育	情報セキュリティに関するルールを策定・運用し、組織構成員に対する情報セキュリティ教育や訓練により、組織のセキュリティレベルを維持・向上します。
インシデントハンドリング（対応策）	
検知・連絡受付	セキュリティ製品によるシステムの監視や、外部からの通報・連絡の受付けにより、情報セキュリティ事故の可能性があるイベントを認知します。
トリアージ	セキュリティイベントの一次調査を実施し、組織への影響やリスクレベルを判定し、セキュリティ・インシデントとしての対応の必要性を判断します。
インシデント レスポンス	各種ログやマルウェア検体の調査により、セキュリティ・インシデントによる被害とその影響範囲を特定し、被害を受けたシステムを迅速に復旧します。また、原因を特定し対策を講じます。

以上

＜本件に関するお問い合わせ先＞
伊藤忠テクノソリューションズ株式会社
広報部
TEL：03-6203-4100／E-mail：press@ctc-g.co.jp