お知らせ

2025年7月11日
SCSK株式会社

SCSKがCSPMを全社導入開始 - 全社でクラウドセキュリティを推進
～Smart One Cloud Securityを標準サービスとして適用～

SCSK株式会社(本社:東京都江東区、代表取締役　執行役員　社長:當麻　隆昭、以下　SCSK)は、パブリッククラウドのセキュリティを一元的に管理するCloud Security Posture Management (以下CSPM)の全社導入を開始しました。Palo Alto Networks社のCSPM製品であるPrisma Cloudを採用した「Smart One Cloud Security」サービスを活用し、全社のクラウドセキュリティを強力に推進します。

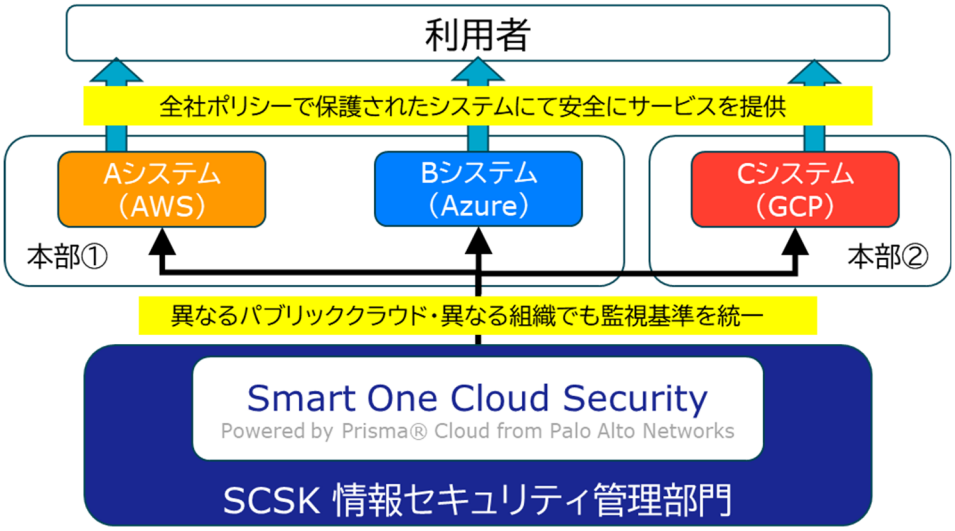
1. 背景

日本のパブリッククラウド市場は近年急成長しており、2024年には約4兆1,355億円(前年比26.1%増)となりました。また、今後も成長が続き、2029年には市場規模が約8兆8,164億円に達する見込みです。この成長の背景には、生成AIの普及やクラウドネイティブ化の進展があり、企業のデジタルビジネスへの投資拡大が市場の拡大を後押ししています※。しかし、クラウド環境はその柔軟性やスケーラビリティから、多くの企業にとって不可欠なインフラである一方、容易に利用できることから設定ミスや脆弱性が原因となる重大なセキュリティインシデントのリスクも高まっており、企業はセキュリティ強化に向けた取り組みの重要性が増しています。

※ 出典:IDC Japan「国内パブリッククラウド　サービス市場予測、 2025年～2029 年 」
https://my.idc.com/getdoc.jsp?containerId=JPJ52152425

2. 全社でクラウドセキュリティを推進

SCSKでは自社内においてもクラウド環境を活用しており、これまでも積極的にセキュリティ対策に取り組んできました。しかし、クラウド利用環境の多様化や今後のパブリッククラウドの利用拡大を踏まえると、クラウド環境に応じた個別のクラウドセキュリティ対策を一元的に管理するための体制の整備が必要と判断し、SCSKが提供するCSPMのマネージドサービス「Smart One Cloud Security」を全社の標準サービスとして推進することにしました。これにより全社でセキュリティ対策を一元的に実施することが可能となり、利用する全てのクラウドにおける一定レベル以上のセキュリティ対策を担保し、組織としてガバナンスを強化します。また、運用者が個別に実施していたセキュリティ設計や対応を標準化することにより、運用者の負荷を低減します。



図：CSPM 導入によるセキュリティ強化の概念図

初期段階では、社内利用を行っている約 300 システムへ提供を推進します。今後は適用範囲を拡大し、社内利用している環境だけでなく、SCSKがクラウドサービスとして提供している環境、構築しているお客様環境のセキュリティを向上できるよう努めます。

3. 今後の取り組み

CSPM 導入はクラウド環境のセキュリティ強化における重要なステップです。しかし、クラウドセキュリティには CSPM にとどまらず、CNAPP など多様な要素が存在します。今後は、こうした最新技術の導入を積極的に進め、クラウドセキュリティ全体のレベル向上を目指します。

また、本取り組みを社内導入にとどめることなく、従業員へのクラウドセキュリティ教育の提供、組織全体のセキュリティ意識の向上にもつなげ、セキュリティ文化の醸成を図ります。さらに、社内に限らず、お客様からお預かりするクラウド環境の構築・運用においても、より高いセキュリティ水準を実現し、安全・安心なクラウドサービスの提供を継続します。

CSPM について

CSPM はクラウド環境のセキュリティ態勢を管理し、設定ミスや脆弱な設定を検出・修正するためのソリューションです。企業のクラウド利用が拡大する中、クラウドインフラのセキュリティリスクを可視化し、コンプライアンス違反を防止します。

CNAPP について

CNAPP（Cloud Native Application Protection Platform）の略で、クラウド環境におけるアプリケーションやインフラを包括的に守るためのセキュリティプラットフォームを表します。この CNAPP は CSPM の他に以下のような要素を含んだ、包括的なセキュリティ対応の概念です。

・CWPP（Cloud Workload Protection Platform）

　仮想マシンやコンテナなど、クラウド上のワークロードを保護。

・CIEM（Cloud Infrastructure Entitlement Management）
　ユーザーやアカウントの権限を適切に管理し、過剰なアクセスを防止。
・DSPM（Data Security Posture Management）
　重要なデータの所在やリスクを可視化し、保護を強化。
・IaC スキャン（Infrastructure as Code）
　コード化されたインフラ設定のセキュリティチェック。

本件に関するお問い合わせ先

SCSK株式会社
IT インフラサービス事業グループ
基盤ソリューション事業本部 テクノロジーサービス部
Smart One Cloud Security 担当
E-mail：cloud-security-sales@scsk.jp