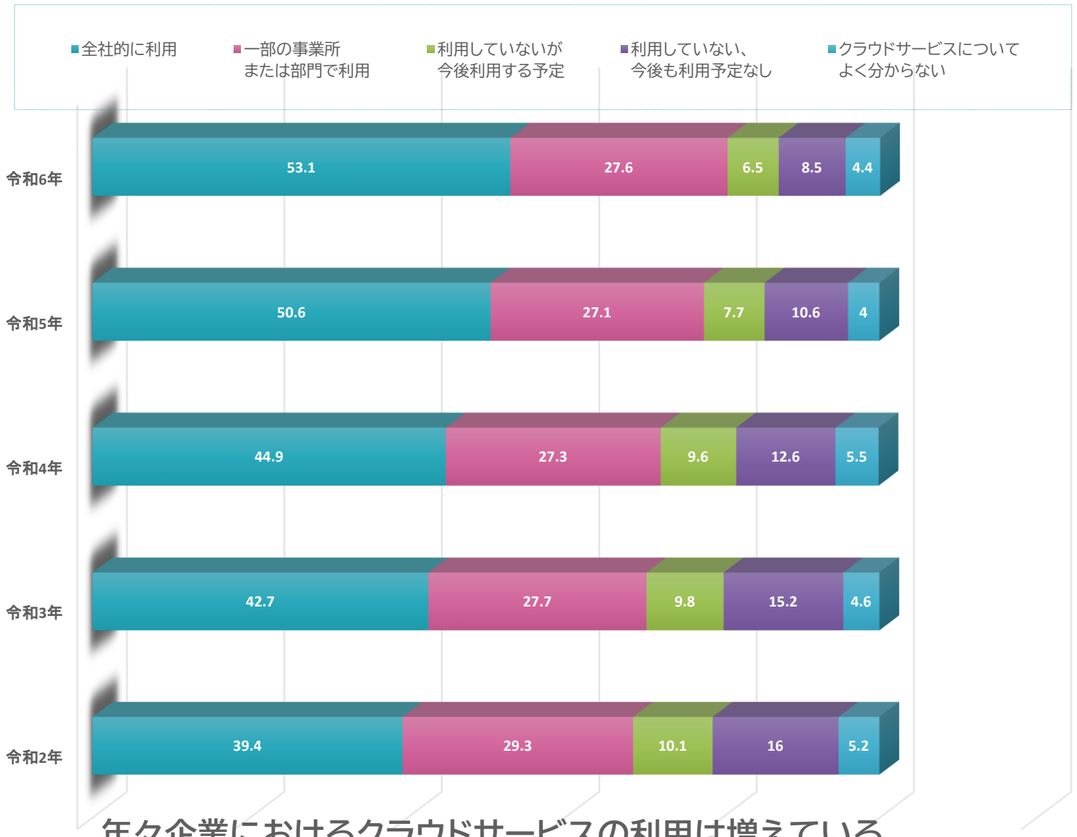
クラウド環境のセキュリティを強化する新しい方法
～CIS Benchmarks®を活用したAWS上のSaaS改善事例～

2025年11月4日

インフォテック株式会社

背景と課題

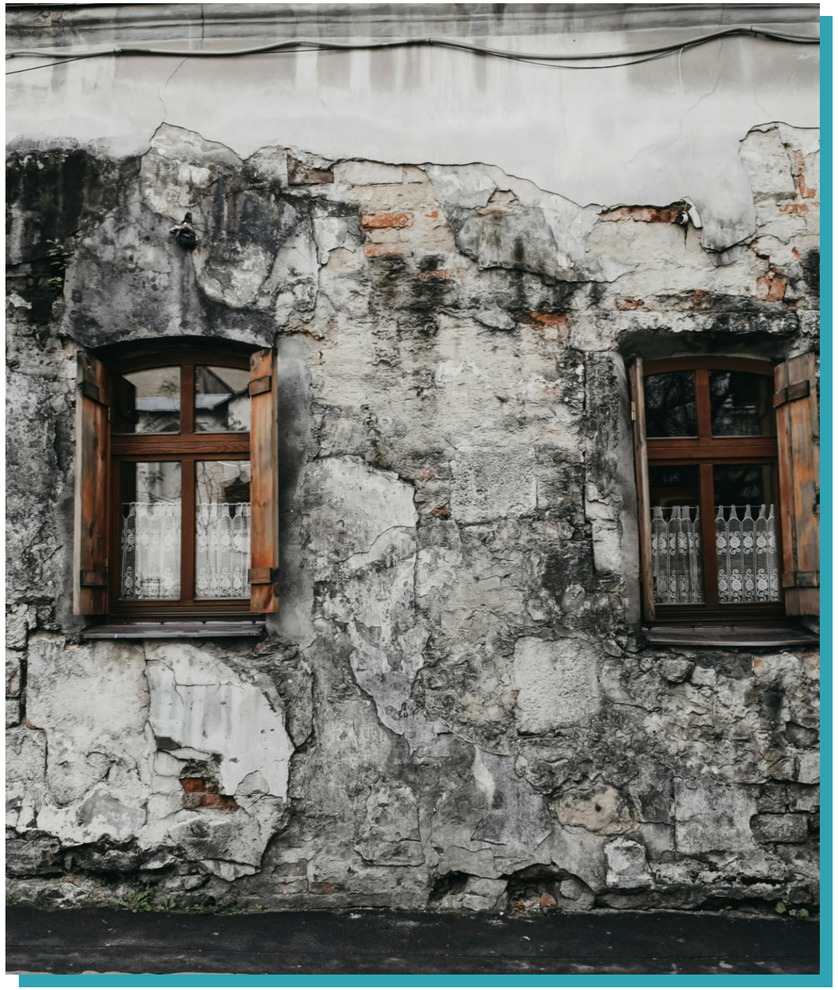
- 総務省の調査（下図）にもあるように、クラウドサービスの利用が急速に増え続けています。しかし、クラウド環境は常にインターネットに接続されているため、サイバー攻撃のリスクも高まっています。



年々企業におけるクラウドサービスの利用は増えている
（総務省 令和6年通信利用動向調査の結果（概要）をもとに作成）

- 企業が安全なサービスを提供するためには、以下のような課題に対応する必要があります。
  - 外部からの攻撃に耐えられる堅牢なシステム設計
  - 限られた人員・予算の中で効率的なセキュリティ対策
  - 安心して任せられる開発パートナーの選定

従来の対策とその課題、およびその改善方針



- 今までのセキュリティ対策は、主に「外部からの診断」に頼っていました。
  たとえば、Webアプリケーションの脆弱性診断や、疑似攻撃によるペネトレーションテストなどです。
- しかし、「内部の設定ミス」や「運用上の盲点」までは見つけにくいという課題がありました。
- そのため、当社では**CIS SecureSuite®**によるアセスメントによって改善可能かを評価することとしました。

CIS SecureSuite®とは

CIS SecureSuite®

- CIS SecureSuite®は、米国の非営利団体「Center for Internet Security®（CIS®）」が提供する、セキュリティ強化のためのツールとガイドラインのセットです。
  このメンバーシップに加入することで、企業は「CIS Benchmarks®」に基づいた設定チェックツール（CIS-CAT®Pro）や、セキュリティ対策の評価・改善に役立つリソースを利用できます。
- 当社は　CIS SecureSuite®のメンバーシップに加入しております。

CIS Benchmarks®

- CIS Benchmarks®は、世界中のセキュリティ専門家が協力して作成した、**「安全なシステム設定」のベストプラクティス集**です。
  OS、クラウドサービス、ミドルウェア、ネットワーク機器など、さまざまなIT製品に対して「どのように設定すれば安全か」を具体的に示しています。
- このガイドラインに沿って設定を見直すことで、**サイバー攻撃のリスクを大幅に減らすことができる**ため、企業のセキュリティ対策の基盤として広く活用されています。

なぜCIS Benchmarks®による内部診断が“安心”につながるのか

- 多くの企業では、セキュリティ対策として**外部診断（脆弱性診断やペネトレーションテスト）を実施しています。**
  しかし、それだけではシステム内部の設定ミスや構成の不備までは見つけることができません。

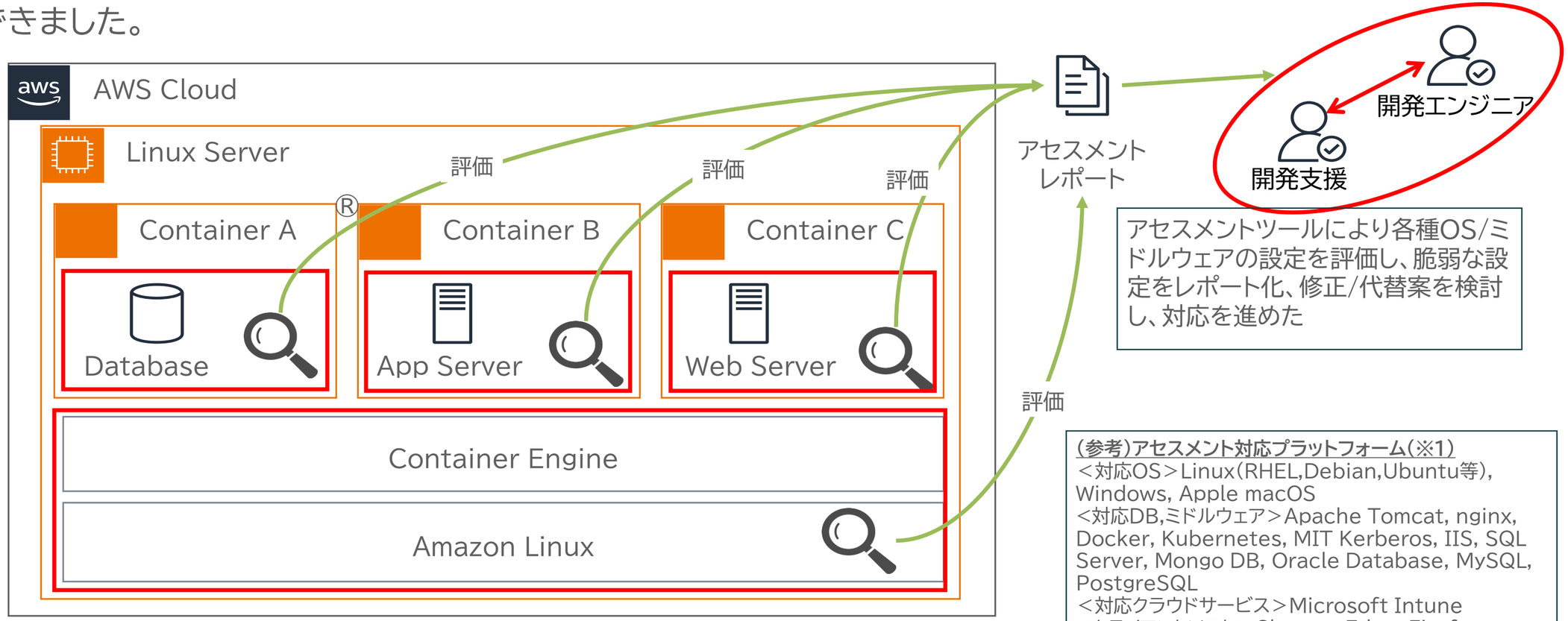
- システムの内部設定は、セキュリティ業界でスタンダードとなっているCIS Benchmarks®に基づいたアセスメントによりシステム内部の設定ミスや構成の不備を確認します。当社は、CIS SecureSuite®メンバーシップに加入しており、CIS Benchmarks®に基づく内部診断サービスを提供する、開発パートナーです。

従来の開発サービスとCIS SecureSuite®を含めた開発サービスの違い

比較観点	一般的な開発パートナー	当社
外部診断の実施	実施可能（年1回程度）	実施可能（年1回） ※継続的なチェックもご提案可能
内部診断	実施なし、あるいは限定的	CIS Benchmarks®に基づく詳細な設定診断が可能
CIS SecureSuite® メンバーシップ	未加入	加入済
改善対応	外部指摘ベース	外部・内部両面からの改善が可能

SaaS基盤のプラットフォーム脆弱性アセスメント

当社は、SaaS基盤の内部設定をCIS Benchmarks®に準拠していることをアセスメントすることにより、より強固なセキュリティ設定の改善をCIS Benchmarks®、およびCIS-CAT®Proを用いて行いました。
これによって、各種OS/ミドルウェアの設定を評価し、脆弱な設定をレポート化、修正/代替案の検討を行い、対応を進めることができました。



(参考)アセスメント対応プラットフォーム(※1)
<対応OS>Linux(RHEL,Debian,Ubuntu等), Windows, Apple macOS
<対応DB,ミドルウェア>Apache Tomcat, nginx, Docker, Kubernetes, MIT Kerberos, IIS, SQL Server, Mongo DB, Oracle Database, MySQL, PostgreSQL
<対応クラウドサービス>Microsoft Intune
<クライアントソフト>Chrome、Edge, Firefox, Microsoft Office
<その他>VMWare ESXi など
製品、及びバージョンの組み合わせで119種類

(※1) CIS Benchmarks Supported by CIS-CAT® Pro
https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/cis-benchmarks-supported-by-cis-cat-pro

成果とメリット

この取り組みにより、以下のような成果が得られました

- 外部診断だけでは見つからなかった“内部の弱点”を可視化
- システム全体の堅牢性が向上し、セキュリティインシデントのリスクを低減
- 顧客に「安心して任せられる開発体制」をアピールできるようになった

まとめ

セキュリティ対策は「外部からの診断」だけでは不十分です。
内部の設定や構成を見直すことで、より安全で信頼性の高いサービスを提供できます。

当社では、CIS Benchmarks®を活用した内部アセスメントにより、クラウド環境の安全性を高める支援を行っています。
安心して任せられる開発パートナーをお探しの方は、ぜひご相談ください。

※「CIS®」、「CIS Benchmarks®」、「CIS Controls®」、「CIS SecureSuite®」、「CIS-CAT®」は、Center for Internet Security, Inc.（CIS）の米国およびその他の国における登録商標です。本記事は、CISの商標またはサービスに関する公式な提携、認定、スポンサーシップを示すものではありません。

セキュリティは後付けでは守れない

セキュリティ対策は、システム開発の設計段階から対策することが重要です。

インフォテックが提供するセキュリティソリューションは
Security By Design x DevSecOpsをベースに構築、確かな安心をお届けします。

Security By Design

システム設計段階からセキュリティを組み込んで開発を行います

CIS Benchmarks® (*1)やCIS Controls® (*2)を活用し、設計・開発・保守におけるセキュリティの標準化と継続的な評価改善を可能とします

DevSecOps

保守フェーズではDevSecOpsに基づき、PDCAサイクルにWebアプリケーション脆弱性診断(*3)やクラウド／SaaSのセキュリティ態勢管理（CSPM(*4)・SSPM(*5)）を組み込むことで、運用の継続的な改善をご支援します

お問い合わせ・資料請求はこちらから

インフォテック株式会社HP 問い合わせ窓口
https://www.iftc.co.jp/contact/ ※「ソリューションに関するお問い合わせ」からお問い合わせください

お電話でのお問い合わせ
03-3348-0360 ※【受付時間】土日祝日を除く平日の9:00～17:30

(*1) OSやクラウドなどのITシステムに対する安全な設定方法をまとめたガイドラインで、セキュリティ強化や監査対応に活用
(*2) サイバー攻撃から組織を守るための18の優先度付きセキュリティ対策で、実践的かつ段階的な導入が可能なベストプラクティス集
(*3) スリーシェイク社の「Securify」を用いた自動診断
(*4) クラウド環境の設定ミスや脆弱性を検出・修正し、セキュリティとコンプライアンスを維持する管理ツール
(*5) SaaSアプリのセキュリティ設定を監視・管理し、データ漏洩や権限の過剰付与などのリスクを防ぐための管理ツール