Case Study

THALES

CYBERSECURITY

Asana Group：CipherTrustとITソリューションパートナーHINTAGによる医療データの保護と暗号化

cpl.thalesgroup.com

THALES

CYBERSECURITY

企業概要

2002年に設立された「Asana Gruppe AG」は、ルンゲルン病院とメンツィンゲン病院という2つの運営株式会社の持株会社です。2004年7月1日には、メンツィンゲンにある高齢者向け居住・介護施設「Falkenstein Asana AG」も、運営株式会社かつ完全子会社としてAsana Group AGに統合されました。

課題

アールガウ州の医療データの保護と暗号化

専門医不足と医療費の高騰により、アールガウ州の病院は大きなプレッシャーにさらされています。一方で運営会社としてのAsana Groupは、収入水準を維持しながら患者に高品質なサービスと一流の医療を提供し続ける必要があります。同時に、デジタル化がもたらす機会を活用し、増え続けるデータ量に対応できる効率的なプロセスとスリムな管理体制を整備することも求められています。Asana Groupはこれらの課題を、メンツィンゲンとルンゲルンの2つの病院に勤務する650名の従業員が中核的価値である患者ケアに専念できるようにするための解決策が必要でした。

デジタル化戦略の一環として、Asana Groupは2023年にクラウド型コラボレーションソリューションへ移行しました。これにより、同僚同士で迅速かつスムーズに予定を調整したり、他の人の意見を求めたりするための情報交換が可能になります。Asana Groupは、Microsoft Azure上でホストされるMicrosoft Office 365を採用しました。しかし、クラウド経由でのデータ交換には、いくつかのコンプライアンス課題に対処する必要があり、特にスイスの「データ保護影響評価（Datenschutzfolgeabschätzung）」が大きな課題となりました。「データ分類の手段がないことは、以前から現在まで続く課題です。どのデータがクラウドに送られているのか把握できていません。そのため、個人データがクラウドにアップロードされる可能性を想定せざるを得ず、アールガウ州との間でデータ保護影響評価に関する合意書を締結する必要がありました」と、Asana GroupのIT責任者であるエイドリアン・ザイラー氏は説明します。

さらに、コンプライアンスだけでなくセキュリティも重要な課題でした。「Microsoftはクラウド上のデータを暗号化するための標準ツールを提供していますが、暗号化に使用される鍵は私たちの手元にはありません。いざという時に自社データを完全に管理できず、Microsoftが要求に応じて復号鍵を提供するかどうかも不明です」と、ザイラー氏はセキュリティ上の課題を説明します。

Asana Groupのこの取り組みは時流に沿ったもので、チューリッヒ州でも自治体行政機関に対し、Microsoft Azure上のMicrosoft 365についてデュアルキー暗号化ソリューションの使用を義務付けています。「1つの鍵はMicrosoftが保持し、もう1つは自治体が保持します。自治体は自らの鍵を完全に管理できます」とザイラー氏は述べています。

ASANA Gruppe

hintag
Gesundheitswesen sicher digitalisiert

業種
ヘルスケア

所在地
スイス・ルンゲルン

ウェブサイト
asana.ch

導入

CipherTrustによるBYOK（Bring Your Own Key：独自の鍵の持ち込み）暗号化と医療データ向けセキュリティ

Microsoftの暗号化サービスに依存するのではなく、データセキュリティを強化したいとザイラー氏は考えていました。特に、アールガウ州とのデータ保護影響評価（Datenschutzfolgeabschätzung）におけるコンプライアンス上の理由からです。「綿密な協議を経て、2024年初頭にセキュリティ層を追加しました。ただしプロジェクト開始前に、Asanaの経営陣と取締役会の合意を得ることが重要でした」とザイラー氏は述べています。「プロジェクトは4月に開始され、遅延なく5月に完了しました」

CipherTrust Data Security Platformは、お客様がデータを保護するための幅広いデータセキュリティユースケースのサポートを提供します。CipherTrust Cloud Key Management（CCKM）コネクタにより、お客様はクラウド上のデータを暗号化する鍵を自ら管理できるようになります。Microsoft Azureは保存データの暗号化と鍵管理を提供していますが、データ保護要件ではお客様自身が鍵を保管し管理することが求められます。Microsoft Azureの「BYOK（独自の鍵の持ち込み）」サービスはこの要件を満たし、お客様による鍵管理を実現します。お客様が鍵を管理することで、暗号鍵の分離、生成、所有、管理（失効を含む）が可能となります。

BYOK（独自の鍵の持ち込み）は、組織が独自の暗号鍵を使用してクラウドサービスに保存されたデータを保護できるようにするセキュリティモデルであり、データ保護に対する管理権限を強化します。CCKMは、Asana GroupがMicrosoft Azureに保存されたクラウドデータを自社の鍵で管理できるよう、BYOK機能を提供します。この堅牢なアーキテクチャは、非構造化ファイルと構造化データベースを保護します。「これにより、データ保護規制の対象となるデータがクラウドに保存された場合でも、完全に自社の管理下に置かれます。すべてのデータはBYOK暗号化によって高い安全性を確保しており、量子安全な暗号化が利用可能になった際にはすぐに移行できる準備が整っています。多くの人は、従来の暗号化ソリューションが量子時代に対応していないことを認識していません」とザイラー氏は述べています。

結果

Microsoft Azureのデータにアクセスする際もMicrosoft 365はシームレスにパフォーマンスを発揮

同社は特に、タレスソリューションによる暗号化がMicrosoftアプリケーションでのデータアクセス時にパフォーマンスの低下を引き起こさなかったことに満足しています。CipherTrustソリューションの導入後も、ユーザーは顕著な差異を感じることなくシームレスなパフォーマンスを体験しており、Microsoft 365を介したアプリケーションやデータの作業を従来どおり継続しています。Microsoft 365によるコラボレーションは、プロジェクト作業の実現と加速において重要な役割を果たしており、効率性やスピードを損なうことなくデジタル空間でのチームワークを大幅に向上させています。

Microsoft 365 コラボレーションソリューションにより、Asanaの従業員は管理部門でも病院でも、より効率的に共同作業を行えるようになりました。BYOKアプローチにより、タレスCipherTrustソリューションは、Asanaがデータ保護規制に準拠し、BYOK暗号化によって第三者のアクセスからデータを保護することを支援しました。「HINT AGとタレスとの連携はシームレスでした。プロジェクトは成功し、計画どおりに進みました」と、ザイラー氏は述べています。

> 「すべてのデータはBYOK暗号化によって高い安全性を確保しており、量子安全な暗号化が利用可能になった際にはすぐに移行できる準備が整っています」
>
> **– アドリアン・ザイラー氏、Asana Group IT責任者**

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。決断の瞬間のための、確実なテクノロジー。

お問い合わせ先 – 連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-us をご覧ください。