3DEXPERIENCEプラットフォーム クラウド セキュリティ＆プライバシー

ホワイトペーパー

目次

はじめに

当社の方針

クラウド コンピューティングは、ビジネス手法におけるパラダイム シフトと言えます。組織はアプリケーションを実行し、データを管理し、業務をクラウドに移行することで、クラウドがもたらすスピードとシンプルさというメリットを獲得します。さらに、専門プロバイダーによるメンテナンス、ITサービス、セキュリティによる運営上の有効性からもメリットを得られます。

ダッソー・システムズは、2012年の**3D**EXPERIENCE®プラットフォームのサービス開始以来、クラウドをベースとするサービスを提供してきました。安全性、柔軟性、拡張性に優れたクラウド リソースからクライアントがメリットを得られるように、**3D**EXPERIENCE Cloudプラットフォームを始めとする完全なクラウドベースのエコシステムを構築しました。当社の使命は、ソリューションのあらゆる側面で信用と信頼を確保し、クライアントをサポートすることです。

リスク管理に対するアプローチは、多面的かつ事前対策的です。ベスト プラクティスをベースとし、業務全般にわたってセキュリティ上の脅威が発生しないかを予測できるように配慮しています。当社は、ISO/IEC 27001:2017およびISO/IEC 27701:2019に準拠し、定期的な監査が必須となる情報セキュリティ プライバシー管理システム（ISPMS）を導入しています。このISPMSは、機密性、完全性、可用性、説明責任という4つのコア バリューをベースとしています。

本ホワイトペーパーは、ダッソー・システムズの**3D**EXPERIENCEにおけるセキュリティおよびコンプライアンスへのアプローチを解説するものです。当社の顧客は、このクラウドベースのプラットフォームを介して、アプリケーションやデータ ストレージ、さらに拡張可能なコンピューティング リソースにアクセスしています。本ホワイトペーパーでは、クラウド セキュリティ、プライバシー、コンプライアンスの主な取り組みについて説明します。

当社の情報セキュリティとプライバシーに関するミッション ステートメント

ダッソー・システムズの情報セキュリティとプライバシーに関するミッション ステートメントは以下の通りです[1]。

3DEXPERIENCEプラットフォームSaaS（サービスとしてのプラットフォーム）における情報セキュリティ リスクの影響度とともに、個人を特定できる情報（PII）を管理することで、情報の機密性、完全性、可用性を継続的に改善し、以下の保護対策を強化します。

- 顧客の知的財産とユーザー データ、そこに含まれるPII
- ダッソー・システムズの評判と知的財産
- クラウドの可用性と回復力
- 該当するサイバーセキュリティおよびデータ保護規制や基準への準拠

このミッション ステートメントは、文書化された情報として従業員に支給され、要請に応じて関係者にも提示されます。

免責事項

本書の内容は、2022年3月時点の**3D**EXPERIENCE Cloudプラットフォームのセキュリティ、プライバシー、品質、コンプライアンスの取り組みをまとめたものです。本書に記載された取り組みは、ダッソー・システムズの裁量で変更される場合があります。本書で「当社」、「当社の」と記述する場合は、ダッソー・システムズを意味します。

1.これはISO 27001の情報セキュリティとプライバシー ポリシーに準じるものです。

ダッソー・システムズ：セキュリティとプライバシーを重視する組織

3DEXPERIENCEプラットフォームSaaSのサイバーセキュリティおよびプライバシー ガバナンス

ダッソー・システムズR&Dは、一元的に管理される**3D**EXPERIENCEプラットフォームSaaS向けの情報セキュリティ プライバシー管理システム（ISPMS）を実践しています。ISPMSは、SGS国際認定サービス（SGS-ICS）により、ISO/IEC 27001:2017およびISO/IEC 27701:2019認定を取得しています。認定の範囲には以下が含まれます。

1. **3D**EXPERIENCEプラットフォームSaaSの設計、開発、デリバリー、展開、クラウド運営。
2. ダッソー・システムズが以下の役割を果たす場合のデータプライバシー管理：
   - a. **3D**EXPERIENCEプラットフォームSaaSに伴って提供される個人データを取り扱うコントローラ（管理者）。
   - b. 顧客の管理下にあり、**3D**EXPERIENCEプラットフォームSaaSで処理されるPIIのプロセッサ（処理者）。

ダッソー・システムズのISPMSは、ダッソー・システムズR&D執行委員会が統括し、R&D執行委員会の管理レビューの対象となります。ISPMSは、定評ある品質管理システム（QMS）をベースとして構築されます。このQMSは、**3D**EXPERIENCEプラットフォーム上で稼動し、SGS-ICSによりISO 9001:2015認定を取得しています。

QMSとISPMSは、セキュア ソフトウェア開発ライフサイクル（セキュアSDLC）手法に基づく多くの基本プロセスやサポート プロセスを共有します。ISPMSには、情報セキュリティとデータ保護に特化した追加のリスクベース プロセスも含まれます。

すべてのISPMSプロセスとコントロールは、ダッソー・システムズR&D **3D**EXPERIENCEコンプライアンス監査プログラムにより、コンプライアンスと有効性が継続的に評価されます。その評価で明らかになった是正措置と継続的な改善は、**3D**EXPERIENCEプラットフォームで追跡されます。

監査条件は、ISO 9001、ISO 27001、ISO 27701管理システムとコントロール要件がベースとなります。ダッソー・システムズはPIIコントローラとPIIプロセッサの両方の役割を果たすため、すべてのISO 27001 Annex AのコントロールとISO 27701 Annex AおよびBのコントロールは、管理システムの範囲に含まれます（11ページの「データ保護とプライバシー」を参照）。

ISPMSは、**3D**EXPERIENCEプラットフォームの情報セキュリティとプライバシーに関するミッション ステートメント（ポリシー ステートメント）と年次目標によりサポートされます。目標をベースに、測定可能な目標値と主要業績評価指標（KPI）を策定し、それらを業務チームが監視します。サイバーセキュリティおよびデータ保護目標の適合性は、ダッソー・システムズの年間計画プロセスの一部として定期的に見直されます。

セキュリティ、プライバシー、コンプライアンス担当者

R&D執行委員会

ダッソー・システムズR&D執行委員会は、データ保護要件とプライバシーを担当するダッソー・システムズの相談役（General Counsel）のサポートを受けながら、**3D**EXPERIENCE情報セキュリティ プライバシー管理システム（ISPMS）の有効性について最終的な責任を負います。R&D執行委員会は、以下のようなさまざまな手段を通じて、ISPMSや顧客の期待に積極的に取り組みます。

- 情報セキュリティ プライバシー ポリシーと年次目標を組織の戦略的な方向性と一致させる
- ISPMS要件を組織のビジネス プロセスに確実に統合する
- ISPMSに必要なリソースを確保する
- ISPMSの重要性を伝達する
- ISPMSが目的とする成果を達成できるようにする
- ISPMSの有効性に貢献するように人員を導き、サポートする
- ISPMSプロセスと運用の継続的な改善を促進する

サイバーセキュリティ、データ プライバシー、コンプライアンス チーム

ダッソー・システムズは、それぞれの役職またはロールに割り当てられる使命、説明、成果物、KPI、ロール プロファイル、スキルを定義するエンタープライズ ロール モデルを維持しています。

最高情報セキュリティ責任者（CISO）とセキュリティ リーダーのチームは、ダッソー・システムズの情報セキュリティ プログラムの導入について全体的な責任を負います。チームは責任を持って、情報セキュリティ ポリシー、基準、ガイドライン、手順をグローバル レベルで確立、維持、適用します。

ダッソー・システムズR&Dのサイバーセキュリティおよびデータ プライバシー チームの責務は、ISO 27001およびISO 27701の要件に従い、**3D**EXPERIENCE ISPMSを計画、導入、維持し、継続的に改善することです。さらに、ISPMSへのコンプライアンスと有効性を監視し、基準ガバナンス会議の中で執行役員に監視結果を報告します。

グループ企業の個人情報保護担当者（DPO）は、ダッソー・システムズにPII保護に関する情報を提供して助言することで、ベスト プラクティスを確実に適用して説明責任を果たし、ダッソー・システムズの持続的な成長をサポートします。グループ企業のDPOは、データ保護監督当局の特権的な対話者として、ISPMSのコンプライアンスと有効性をダッソー・システムズの相談役に報告します。

R&Dコンプライアンスおよびリスク チームは、ダッソー・システムズの社内プロセスと業界認定（ISO 9001、ISO 27001、ISO 27701など）への準拠を評価するために、社内コンプライアンス監査プログラムを実践します。監査所見とその是正および予防行動計画（CAPA）は、プラットフォーム内で管理されます。

グループ企業の社内監査チームは、全社レベルの社内監査プログラムを通じて、ダッソー・システムズの社内コントロール評価（ICE）フレームワークのコンプライアンスと有効性を定義し、評価します。社内コントロール フレームワークは、一般コントロールおよび情報テクノロジー一般コントロール（ITGC）の確立と検証を通じて、リスク緩和に貢献します。

全従業員を対象としたオンボーディングとトレーニング

ダッソー・システムズに入社した従業員は、ダッソー・システムズの行動規範、IT憲章、データ保護ポリシーに同意する必要があります。新たに入社したすべての従業員は、セキュリティやプライバシーをテーマとする、以下のような倫理およびコンプライアンス関連の必須のトレーニングを受講します。

- データ セキュリティに対する脅威の阻止。
- 物理的なデータとワークステーションのセキュリティ確保、クリーン デスク ポリシー。
- 個人データの保護と機密性。
- 倫理的なビジネス活動、汚職・腐敗行為防止および競争法の原則。
- インシデント管理、潜在的な脅威の認識と報告。

当社は、組織全体でセキュリティとプライバシーの認知を継続的に高めます。

テレワークにおけるセキュリティ

リモート ワークの場合、ダッソー・システムズの従業員は、VPNを介してのみ、データ、アプリケーション、プラットフォーム ユーティリティにアクセスできます。これは、会社所有と個人所有の両方のデバイスに適用されます。個人所有のデバイスについては、登録・承認済みで、VPNアクセスを持つデバイスのみが許可されます。

当社のクラウド セキュリティを支えるパートナー

当社は、3DS Outscaleなどのクラウド インフラ（IaaS）プロバイダーと密接に連携し、業務全体でセキュリティとコンプライアンスを確保します。IaaSプロバイダーには、その他の条件とともに、ISO 27001認定の取得が求められます。

当社のセキュリティ基準

当社のサイバーセキュリティに対するアプローチは、最も信頼できる業界基準に基づいています。独立したサイバーセキュリティ専門家が積極的に連携し、ソフトウェア プロバイダー向けのグローバルな基準を確立しています。OWASP、NIST、ISO/IECという3つの専門家団体は、ベスト プラクティス、要件、コントロール、テストとともに、リスクの軽減と脆弱性の緩和に役立つ他のツールを用いて、当社のサイバーセキュリティおよびプライバシーチームを導きます。

OWASP：OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASPは、組織がセキュリティの高いアプリケーションを開発・維持できるようにする専門団体です。OWASP Foundationは、優れた情報源として、アプリケーション セキュリティに関する最先端の研究成果、防止フレームワーク、重要な情報を提供します。

グローバルなアライアンスの支援を得て、OWASPは以下の情報を提供します。

- アプリケーション セキュリティ ツール、基準、手法
- セキュアなコード開発、セキュリティ コード レビュー、アプリケーション セキュリティ テストのためのリソース
- 標準的なセキュリティ コントロールとライブラリ

OWASPの主な出版物は以下の通りです。

- Top 10 Web Application Security Risks（Webアプリケーションのセキュリティ リスク トップ10）
- Secure Coding Practices（セキュアなコーディングの実践方法）
- Code Review Guide（コード レビュー ガイド）
- Application Security Verification Standard（アプリケーション セキュリティ検証基準）

NIST：アメリカ国立標準技術研究所[2]

NISTは、卓越した情報源として、エレクトロニクス、ソフトウェア、その他のテクノロジーに関する重要な測定ソリューションと公平な基準を提供します。NIST Special Publication（SP）800-53では、情報システムや組織向けのセキュリティ コントロールとプライバシー コントロールを定義しています。

NIST SP 800-53は、組織運営とアセット、個人、その他のエンティティを「敵対的攻撃、人的なミス、自然災害、構造的な不具合、海外の情報エンティティ、プライバシー リスクなど、さまざまな脅威やリスクから守る」ために設計されています。これらのコントロールは、機能性と保証の両側面からセキュリティとプライバシーに対処します。

ISO/IEC：国際標準化組織と国際電気標準会議[3]

ISO/IECは、ITおよび通信技術の標準化を促進する合同技術委員会です。当社の**3D**EXPERIENCEプラットフォームSaaS向けのISPMSは、ISO/IEC 27001:2017およびISO/IEC 27701:2019認定を、QMSはISO 9001:2015認定を、いずれもSGS-ICSにより取得しています（4ページの「**3D**EXPERIENCEプラットフォームSaaSのサイバーセキュリティおよびプライバシー ガバナンス」を参照）。

ISO 9001では、組織が以下の作業を進める場合の品質管理システムの要件を規定しています。

a. 顧客要件と該当する法律および規制要件を満たす製品およびサービスを一貫して提供する能力を示す必要がある場合。

b. システムの改善プロセスや、顧客要件と該当する法律および規制要件の確実な遵守を含む、効果的なシステムのアプリケーションを通じて顧客満足度を高めたい場合。

当社の品質管理システム（QMS）は、**3D**EXPERIENCEプラットフォームの設計、開発、デリバリー、展開、クラウド運用、サポートで使用するプロセスに基づいています。多くのアプリケーション セキュリティの実践方法は、QMSに組み込まれています。

ISO/IEC 27001では、情報セキュリティ管理システム（ISMS）の確立、実装、維持、継続的な改善のための要件を規定します。ISO/IEC 27001 Annex Aでは、パブリック ネットワークでのアプリケーション サービスのセキュリティ確保、アプリケーション セキュリティ トランザクションの保護、安全な開発ポリシーの適用、ソフトウェア パッケージへの変更制限、セキュアなシステム エンジニアリング原則による遵守など、あらゆる場面で想定されるコントロールを規定します。

ISO/IEC 27701では、組織の環境内でのプライバシー管理のためにISO/IEC 27001およびISO/IEC 27002を補足する形で、プライバシー情報管理システム（PIMS）の確立、実装、維持、継続的な改善のための要件を規定し、ガイダンスを提供します。この標準は、PII処理の責務と説明責任を負うPIIコントローラとPIIプロセッサに対するガイダンスとなります。Annex Aでは、PIIコントローラ向けのコントロール目標とコントロールを規定し、Annex Bでは、PIIプロセッサ向けのコントロール目標とコントロールを規定します。

1.詳細：www.owasp.org
2.詳細：csrc.nist.gov
3.詳細：iso.org/isoiec-27001-information-security

主なセキュリティ機能

認証と承認

3DEXPERIENCE Cloudプラットフォームの認証および承認メカニズムでは、**3D** Passportを使用しています。これは、ユーザーがすべてのロール、アプリ、サービスに安全にアクセスするためのパーソナライズされたログイン機能です。管理者は、パスワードの強度、期限等のユーザー認証ポリシーを保守し、パスワードをアンロックする際の総当たり攻撃を検出するためのパターンを構成できます。

3D Passport機能

データ プライバシー

オンライン ソリューションのすべてのユーザーは、**3D** Passportを作成する際に、ダッソー・システムズのプライバシー ポリシーにアクセスし、それに同意することを求められます。ユーザーは、Webフォームからリクエストを送ることで、ダッソー・システムズのポリシーとプロセスに従って権利を行使できます。

また、企業が自社のプライバシー ポリシーを提示してユーザーに同意を求める場合もあります。この場合は、プラットフォームの管理者がプラットフォーム管理ダッシュボードを通じてそのプライバシー ポリシーをアップロードします。

シングル サイン オン(SSO)

3D Passportは、認証・承認データを標準形式で交換することで、**3D**EXPERIENCE Cloudプラットフォーム上のすべてのアプリでシームレスなサイン オンを可能にしています。

多要素認証(MFA)

プラットフォーム上で多要素認証機能を活用することで、高いレベルのセキュリティを実現できます。たとえば、管理者によるMFAの構成後、ユーザーはモバイル アプリを使用して、パスワードとともに入力するコードを生成し、セキュリティを強化できます。

アクセス コントロール

アクセス コントロールは、クラウド コンピューティング環境でリソースにアクセスし、表示して、使用できるユーザーを管理します。これらの承認により、顧客データのセキュリティを確保し、**3D**EXPERIENCE Cloudプラットフォーム内で顧客のコンプライアンスおよび認証プロセスを完結できます。

暗号化

包括的なHTTPS/TLS暗号化プロトコルを使用して完全性と機密性を保護し、転送中のデータのセキュリティを保ちます。

高可用性とDDoS防御

すべてのサービスは、高可用性、高性能、負荷分散プロキシ サービスで保護されます。このサービスには、DDoS(分散型サービス妨害)攻撃の防御機能とブラックリスト機能が統合されています。

運営上のセキュリティ

当社のクラウド運営

当社のクラウド ソリューションは、3つの階層構造で構築・運営されます。脅威を特定して監視を進め、業界標準を用いてリスクを検討・優先順位付けすることで、すべての階層で監査対策を実施します。

サービスとしてのソフトウェア（SaaS）

最上位の階層は、サービスとしてのソフトウェア（SaaS）またはアプリケーション層です。この階層で、**3D**EXPERIENCE Cloudプラットフォームのユーザーはアプリにアクセスして使用します。

サービスとしてのプラットフォーム（PaaS）

中間層は、サービスとしてのプラットフォーム（PaaS）またはプラットフォーム層です。この階層で、**3D**EXPERIENCEプラットフォームは構築・運営されます。この階層により、インフラ プロバイダーとの関係を安全に管理し、SaaS層がやり取りするデータベースを保管できます。

PaaSチームは、**3D**EXPERIENCE Cloudプラットフォームを構成する設定、オペレーティング システム、構造、仮想リソースを決定し、クラウド インフラ プロバイダーからの情報の受領方法を指定します。

SaaSおよびPaaS層での重要なリスク緩和戦略としては、認証、ロールベースのアクセス コントロール、暗号化、監視と監査、DASTとSAST、ミドルウェアのハードニング、サーバーのハードニング、SSL/TLSチェックなどがあります。

サービスとしてのインフラ（IaaS）

サービスとしてのインフラ（IaaS）またはインフラ層は、クラウド コンピューティング リソースが配置される層です。仮想化機能を提供し、バックアップと災害復旧サービスを提供します。

この階層により、ダッソー・システムズとその顧客は拡張性を得ることができます。さらに、追加の処理能力とオンデマンドのストレージ容量も確保できます。

主要なクラウド プロバイダーには、ダッソー・システムズのグループ会社である3DS Outscale、Amazon Web Servicesなどがあります。

責任分担モデル

クラウド プロバイダーとクラウド ユーザーは、クラウド コンピューティング モデルで責任を分担することで、オンライン サービス向けに最高レベルのセキュリティとコンプライアンスを確保できます両者は、クラウド セキュリティの異なる側面の責任を分担します。

- クラウド プロバイダーは、クラウド インフラのセキュリティを担当します。
- プラットフォーム プロバイダー（ダッソー・システムズ）は、セキュリティ構成、管理、運営を担当します。
- 顧客は、管理者/テナント管理を含むアプリケーション層でのセキュリティを担当します。
- 当社は、CSA（クラウド セキュリティ アライアンス）とNISTのガイドラインとともに、クラウド プロバイダーのベスト プラクティスに従ってセキュリティのベスト プラクティスを適用し、クラウド環境を強固にして運営します。

詳細については、Outscaleのベスト プラクティスを参照してください。

可用性に関するSLA（サービス レベル契約）

当社が目指すのは、オンライン サービスが（i）計画的にサービスを停止している場合、または（ii）顧客の要請により停止している場合を除き、99.5%以上のオンライン サービスの可用性を達成することです。

詳細については、オンライン サービスのサービス レベル契約を参照してください。

脆弱性管理

脆弱性の継続的な監視および緩和対策の一環として、当社はリスクを特定、分析、評価するための包括的なリスク アセスメントを適用し、NIST SP 800-53、ISO/IEC 27001、ISO/IEC 27701に基づいてリスク処理コントロールを選択しています。

NISTのベスト プラクティスをベースとした多層的な脆弱性管理システムを導入し、社内外のシステムを統合して脆弱性を特定、テスト、管理します。脆弱性管理システムの主な要素となるのが、ネットワークおよび脆弱性スキャナーの使用です。修正を必要としている脆弱性が特定された場合、ログとして記録し、深刻度に応じて優先順位を決定して、修正が完了するまで追跡します。

OWASPのベスト プラクティスをベースとするコントロールに加えて、静的コード分析（SAST）、動的分析（DAST）、徹底的な手動侵入テストを使用し、潜在的な脅威に対抗する新たなセキュリティ対策を継続的に追加します。

脅威の検知方法

次のような脅威検知方法を使用しています。

マルウェアの防止

当社は、不正なソフトウェアの使用を禁止し、機器の正しい使用方法について従業員にトレーニングを実施しています。技術的なコントロールを用いて悪質なコードを特定し、従業員の認知を高めるトレーニングも実施しています。さらに、マルウェア インシデントの発生時に、効率的かつ速やかに対応するための手順も確立しています。

監視

当社は、コントロールの効果とともに、ミドルウェア、ネットワーク、OSアクセス、OSなど、すべてのクラウド層でのセキュリティ イベントを監視します。自動監視により、運営および機能的なパフォーマンスに関するリアルタイム データも得られます。

インシデント管理

当社は、体系的なアプローチを取って、セキュリティおよびプライバシー インシデントを特定、分類、記録、伝達しています。すべてのインシデントは、分類スケールに基づいてコンタクト ポイントで評価され、確立されたインシデント管理およびデータ侵害プロセスに従って処理されます。

アプリケーション層の脆弱性管理

セキュアなクラウドSaaSおよびPaaSを運営するには、脆弱性を継続的に特定して緩和する必要があります。これは情報テクノロジーや通信テクノロジーでは一般的な手法です。セキュア ソフトウェア開発ライフサイクル（セキュアSDLC）の一環として、複数の主要指標を統合してソフトウェアの脆弱性を特定し、既存のセキュリティ コントロールを検証しています。こうした指標には、開発のさまざまな段階での静的および動的スキャンや、広範囲にわたる手動侵入テストなどがあります。

静的アプリケーション セキュリティ テスト（SAST）

SASTは、開発プロセス中にソース コードを自動的に評価し、コードをセキュアSDLCの次の段階に渡す前に問題を修正します。当社は、GartnerがリードするSASTプロバイダーと連携しています。

動的アプリケーション セキュリティ テスト（DAST）

DASTは、フロントエンドを通じてプラットフォームを自動的に評価し、アーキテクチャ的な弱点や潜在的なセキュリティ脆弱性の有無を検証します。当社のDASTは、業界大手のセキュリティ ツールを使用して実行されます。

手動侵入テスト

認定された第三者のセキュリティ プロフェッショナルが、**3D**EXPERIENCE Cloudプラットフォームや特定のアプリセットにシミュレーションとして手動で攻撃を仕掛けて、セキュリティ体制を確認します。

部門横断型品質エンジニアリング テスト

当社の独立した品質エンジニアリング チームは、定期的に脅威シナリオを実行することで、セキュリティ検証プロセスに貢献しています。このチームの幅広い製品知識と主要なセキュリティ概念に対する理解は、セキュリティ検証および確認のための追加の階層として機能します。

ミドルウェア、ネットワーク、オペレーティング システムの脆弱性管理

当社は、複数の脆弱性チェックと権限に基づくスキャニングを使用して、インターネットに接続するアセットを特定し、Gartnerがリードする脆弱性スキャナーを使用して、ネットワークやアセットに潜む欠陥をすばやく効率的に明らかにします。

パッチ管理

当社は、機能面およびセキュリティ面のパッチも含めて、定期的にソフトウェア アップデートを適用します。SLAで明記しているように、計画的なサービス停止を定期的に行います。さらに、パッチ管理およびインシデント管理プロセスでは、緊急セキュリティ パッチも想定しています。この緊急パッチは数時間以内に適用できますが、計画にないサービス停止を伴います。

セキュリティ監視とインシデント管理

当社の包括的なセキュリティ監視およびインシデント管理システムは、セキュリティ脅威をリアルタイムで特定し、分析して、対応します。脆弱性を特定して修正するとともに、セキュリティ インシデントに速やかに対応するという二面的なアプローチを採用しています。

セキュリティ監視

ログとイベントを集約し、SIEM（セキュリティ、インシデント、イベント管理）ソリューションを介して分析を進め、専任のSOC（セキュリティ オペレーション センター）チームが24時間体制で監視します。当社のSIEMプラットフォームは、データを一元的に収集し、高度な相関エンジンを使用してセキュリティ イベントを未然に特定します。さらに、大量のセキュリティ ログデータを分析して悪意のある試みを特定します。

3DEXPERIENCE Cloudプラットフォームの監督・監視サービスでは、クラウド層全体の多数の指標を考慮し、機能性、パフォーマンス、セキュリティを監視します。

インシデント対応プロセス

SOCチームは、SIEMソリューションがインシデントの性質に基づいて特定したリスクを継続的に監視・評価します。当社は、NIST SP 800-61ガイドラインに沿ったインシデント管理手順に従って、リスク評価に基づきインシデントを直ちに処理します。これは、封じ込め、根絶、回復、通知という主要フェーズに含まれます。

パッチ管理プロセスの一環として、緊急パッチを数時間以内に適用します（「パッチ管理」を参照）。

ビジネス復旧計画（BCP）と災害復旧計画（DRP）

ビジネス復旧計画（BCP）と災害復旧計画（DRP）は、クラウドベースのあらゆるソフトウェア プロビジョニングにおいて重要です。当社のBCPでは、損失イベントの発生時に、コンピューティング サービス、ソフトウェア サービス、コネクタおよびデータを復旧し、完全に機能を回復できるように計画します。当社のDRPでは、大規模なイベントの発生時に、損失範囲を制限するか無効にするための手順を計画します。

以下のように、BCP/DRP関連の業界ベスト プラクティスを活用しています。

1.顧客データのバックアップと回復のための一貫した計画を維持し、大災害の発生時には、すべての計画要素にアクセスできるようにする。

2.重要なデータのコピーを、メインのデータ センターから離れた、実稼動地域以外の場所で保管する。

3.BCP/DRPを最新の状態に保ち、実稼動環境の変化を考慮する。

4.BCP/DRPを年1回実施する。

5.負荷分散やフェイルオーバー システムなど、仮想化機能を利用してサービス中断を最小限に抑える。

当社は、積極的な目標復旧時間（RTO）と目標復旧ポイント（RPO）を設定し、あらゆるシナリオで顧客のビジネス継続性を確保することを目指します。

データのバックアップと回復

サービス レベル契約を満たすために、当社は顧客およびユーザー データを毎日バックアップし、そのバックアップをSLAの規定に従って保管します。継続的なホットおよびコールド バックアップを実施し、ダウンタイムを最小限に抑えながら、データ保護を可能な限り強化します。

3DEXPERIENCE Cloudプラットフォームの顧客データは、SLAで明記している指定期間内は、継続的に取得できます。

詳細については、オンライン サービスのサービス レベル契約を参照してください。

データ保護とプライバシー

当社のクラウド ソリューションは、顧客とユーザーのプライバシーを尊重して構築されています。ヨーロッパ一般データ保護規則2016/679（GDPR）など、関連する法律や基準に従って、すべてのPIIを安全に保管して処理するように高い基準を設定しています。

コントローラ

GDPRで定義されるコントローラは、情報の保管期間、PIIを最小限に抑えるためのコンプライアンス、要請に応じたデータの取り扱いなど、個人データを処理するためのポリシーと手順を判断する必要があります。ダッソー・システムズは、社内のビジネス プロセスや情報システムに関連するPIIを処理する際に、コントローラの役割を果たします。

ダッソー・システムズのSaaSソリューションの顧客は、ソリューションに保管されるPIIの取り扱いについて責任を負うため、コントローラの役割を果たします。

GDPRや他のデータ保護法は、プライバシーの権利を拡大し、個人が自分のPIIを管理できるようにすることで、その地域の居住者の基本的な権利を強化することを目指しています。世界中に進出しているダッソー・システムズは、GDPRとともに、ダッソー・システムズの参入地域で規定されているその他のデータ保護法を遵守します。GDPRと各国の法律は、3ds.comで入手できるダッソー・システムズのプライバシー ポリシーで確認できます。

3DEXPERIENCE Cloudプラットフォームでは、ダッソー・システムズは、以下の場合にコントローラの役割を果たします。

- **3D** Passport（プライベート クラウド ソリューションを除く）
- **3D** Passport（3ds.comを通じて個人が作成したもの）
- **3D**EXPERIENCEのパブリック コミュニティ（ダッソー・システムズのパブリック プラットフォームで利用可能）
- ダッソー・システムズ カスタマー サポート
- **3D**EXPERIENCE Marketplace

GDPRとともに、その他の各地域のデータ保護法や規制は、各地域のダッソー・システムズ データ保護担当者によって監視され、各地域のプロセスと手順に従って適用されます。

3D Passportは、ユーザーごとに作成される認証プロファイルです。**3D** Passport内でのPIIの処理は、ダッソー・システムズの責任で行います。**3D** Passportに関連するPIIは、規制要件によるいくつかの例外を除き、ヨーロッパで保管されます。

プロセッサ

ダッソー・システムズがクラウドベースのサービス（**3D**EXPERIENCE Cloudプラットフォームなど）を提供する場合、ダッソー・システムズは、処理と保管を委託されたPIIのプロセッサの役割を果たします。この役割の場合、ダッソー・システムズは両者で合意した契約に従ってPIIを処理します。

ダッソー・システムズは、以下の場合に、GDPRで規定されるプロセッサの役割を果たします。

- ダッソー・システムズのクラウドサービス（プライベートおよびパブリック）を顧客やビジネス パートナーに提供する場合
- クラウド サービス用の**3D** Passportを提供する場合

プロセッサとして行動する場合、プラットフォーム データは第三者のIaaSプロバイダー（3DS OutscaleやAmazon Web Servicesなど）が各地域のデータセンターに保管します。

まとめ

ダッソー・システムズは、セキュリティとプライバシーを業務の中心に据えています。当社のサイバーセキュリティおよびデータ保護対策は、定評ある業界標準をベースとし、トレーニング、設計要件、セキュリティ コントロール、プライバシー対策、第三者による監査とテストを通じて体系的に運用されています。当社は、セキュリティおよびプライバシー対策を革新と先進の精神で継続的に改善し、お客様をできるだけ最善の方法でサポートしたいと考えています。

ダッソー・システムズの**3D**エクスペリエンス・プラットフォームでは、11の業界を対象に各ブランド製品を強力に統合し、各業界で必要とされるさまざまなインダストリー・ソリューション・エクスペリエンスを提供しています。

ダッソー・システムズは、**3D**エクスペリエンス企業として、人々の進歩を促す役割を担います。当社は持続可能なイノベーションの実現に向けて、企業や人々が利用する3Dのバーチャル コラボレーション環境を提供しています。当社のお客様は、**3D**エクスペリエンス・プラットフォームとアプリケーションを使って現実世界の「バーチャル エクスペリエンス ツイン」を生み出し、さらなるイノベーション、学び、生産活動を追求しています。

ダッソー・システムズの約2万人の従業員は、140カ国以上、あらゆる規模、業種の27万社以上のお客様に価値を提供します。より詳細な情報は、**www.3ds.com**（英語）、**www.3ds.com/ja**（日本語）をご参照ください。

3DEXPERIENCE®

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

本社
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

アメリカ大陸
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
USA

アジア - 太平洋
ダッソー・システムズ株式会社
〒141-6020
東京都品川区大崎 2-1-1
ThinkPark Tower