SAP® Customer Experience

SAP エグゼクティブサマリー
SAP Customer Data Cloud

情報セキュリティおよび データプライバシーの方針

THE BEST RUN SAP®

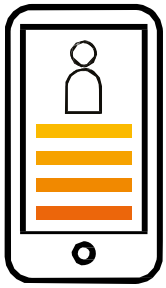
目次

SAP Customer Data Cloud の情報セキュリティおよびデータプライバシー方針の概要

企業向け顧客データ管理 サービスの大手プロバイダーとして、お客様のビジネスに貢献するためにはデータのセキュリティが重要であることを弊社は十分に認識しています。さらに、外部の顧客データ管理サービスプロバイダーと連携する際の懸念も十分に理解しています。SAP では、最高レベルのプライバシー、セキュリティシステム、ポリシー、そしてプラクティスを維持すべく全力を尽くしています。SAP のソリューションは、セキュリティとコンプライアンスの厳格な基準に従ってデータを保護しながら効率性とスケーラビリティを最大限高められるよう最適化されています。

市場をリードする SAP® Customer Data Cloud ソリューションは、各業界の慣行に従った情報セキュリティ体制を確立してきました。現在、以下のセキュリティ領域に対処する包括的なポリシーセットを提供しています。

- アクセス制御
- アプリケーション開発のセキュリティ
- 各国法的要件への遵守
- 導入および運用のセキュリティ
- エンドユーザーセキュリティ
- 人事情報セキュリティ
- インシデント対応プログラム
- IT セキュリティ管理
- ネットワークセキュリティ
- パスワード管理
- 物理的および環境のセキュリティ
- システム運用のセキュリティ



このエグゼクティブサマリーでは、SAP Customer Data Cloud ソリューションが掲げる目標を達成するために採用されている標準およびベストプラクティスの概要をご説明します

技術的および組織的対策

SAP は、お客様の個人データと機密情報における機密性、可用性、完全性を保護するために設計された情報・物理セキュリティプログラムを遵守しています。そして、このプログラムの手続きと制御の有効性について、定期的なテストおよびモニタリングを行っています。現在および将来のすべてのセキュリティの脅威に対して 100% 有効なセキュリティの手段などありません。ここで示す手段は、最小限の標準的なものに過ぎず、適宜変更され得るものです。これらの手段で十分に対応可能かどうかは、お客様の責任においてご判断ください。

物理的および環境のセキュリティ
自社の資産、従業員、情報、製品、財産、ブランド、評判を守るために、SAP はサービス提供に使用されている機器や施設に許可なく物理的にアクセスすることを禁じる、セキュリティ基準を設定しています。

SAP は、自社で所有・運営しているデータセンター、または SAP のセキュリティ要件を満たしたサードパーティのデータセンターのいずれかを利用してサービスを提供しています。

これらのデータセンターへのアクセスは、24 時間体制のアクセス制御、映像監視用テレビ (CCTV)、物理セキュリティ制御、カードアクセスといったさまざまな手段で管理されています。また、データセンターには、防火および消火設備、複数電源、UPS システム、発電機、冷却装置、空気浄化装置、ネットワークプロバイダーへの冗長接続などを装備しています。

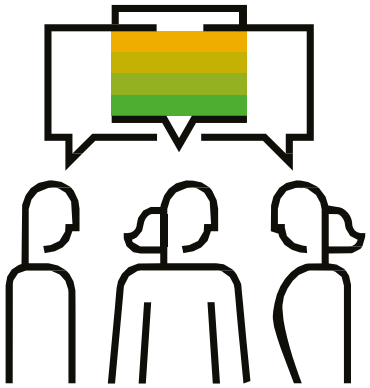
すべてのアクセスは記録され、許可されたデータセンタースタッフのみが物理マシンにアクセスでき、インフラストラクチャーやアプリケーションにアクセスするためのパスワードは共有されません。

サービス提供に関わるすべての場所において、必要なあらゆるセキュリティサービスを提供でき、SAP Customer Data Cloud 標準に準拠していることが、テストで証明されています。

米国、EU、オーストラリアのデータセンター
SAP Customer Data Cloud ソリューションは、世界中の複数の AWS (Amazon Web Services) リージョンで提供されています。

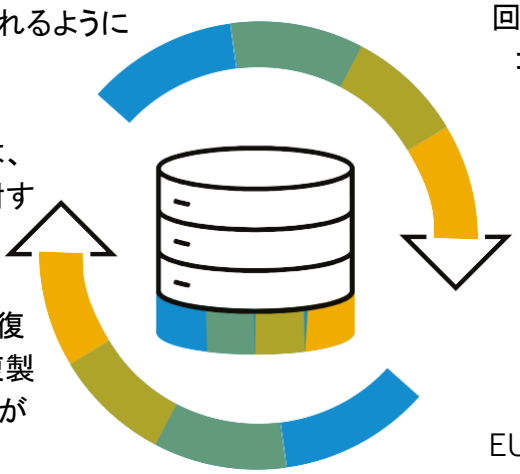
米国バージニア（アメリカ市場の場合）、アイルランド（EU 内でのデータ保存を希望するヨーロッパ企業の場合）、およびオーストラリアのシドニー（APAC 市場の場合）の AWS リージョンをご利用いただけます。

AWS のセキュリティおよびインフラストラクチャーの詳細



ロシアのデータセンター
SAP は、ロシア最大手のデータセンタープロバイダー Selectel がホストするロシアのサーバーファームを利用・運営しています。Selectel のデータセンターは、Tier 3 施設となっており、バックアップ発電機を持つ UPS と冗長 HVAC システムのほか、消火・洪水制御システムも備えています。これらのデータセンターには、24 時間体制の警備や CCTV による完全な監視を始めとする、高度なセキュリティ基準が適用されています。

中国のデータセンター
Alibaba Cloud (Aliyun) がホストする SAP Customer Data Cloud の中国データセンターは、SAP の 5 つ目のデータセンターになります。このデータセンターを使用する場合、中国に居住地を持つ顧客の場合は、顧客データが中国国内に保管しなければならないという法規制に対応し、中国のデータセンター内に顧客データが保存され、オフラインバックアップも国内に物理的に保持されるように指定することができます。



SAP Customer Data Cloud は、SAP の中国データセンターに対する完全な冗長性を提供します。顧客データは上海のプライマリデータセンターと北京の災害回復サイトとの間でリアルタイムに複製され、すべてのサーバーロールがクラスタ内で機能するため、単一障害点は存在しません。

事業継続性
災害が発生してもミッションクリティカルなサービスが完全に回復できるよう、システムコンポーネントとミッションクリティカルなビジネスプロセスを特定し、優先順位を付けてから、サービスの中断が続く可能性を減らす一連のポリシー、基準、そしてプロセスを実装しています。

それらは、以下の形で規定されています。
- 大きな災害や事故があっても中断を最小限に抑えて主要な SaaS サービスやインフラストラクチャーサービスを継続して提供できるようにするための事業継続性計画 (BCP)
- 災害から回復するために SAP が確立、実装、およびテストした一連のプロセスで構成される、BCP に含まれる災害回復計画 (DRP)

SAP のソリューションは、データセンターの機能が停止するといったまれなケースにおいても、完全な災害回復性を実現します。例えば、データを離れた場所にリアルタイムで複製したり、重要なデータをオンプレミスで転送したりすることで、ハードウェアに障害が発生した場合にもデータを失うことなく継続的にサービスを提供し、透過的に回復できるようにします。

米国では、データセンターはそれぞれまったく異なる場所に配置されています。災害回復 (DR) サイトは、実働サイトと同じコンポーネントと機能を持ち、実働サイトに変更があった場合には同様に更新されます。DR が問題なく機能して、災害への備えができているかどうかを確認するために、DR サイトのサニティーチェックを 1 時間ごとに自動的に実行しています。

EU およびオーストラリアでは、提供されるすべてのサービスについて、2 つの異なるアベイラビリティゾーンで AWS を使用しています。

アベイラビリティゾーンは両方ともアクティブで、顧客にサービスを提供しています。ロシアでは、それぞれまったく異なる場所にある、Selectel の 2 つのデータセンターを使用しています。データセンターは 2 つともアクティブで、顧客にサービスを提供しています。中国では、SAP は Alibaba Cloud にホストされた上海のプライマリデータセンターを運用しており、データは北京の DR サイトに複製されています。

障害が発生した場合にも、平均回復時間 (MTTR) を短くできることを特に重視し、多層情報漏えい防止アーキテクチャーを採用しています。すべてのデータは、2 つの地域での n+1 以上の冗長性を備えたセカンダリデータセンターのスタンバイサーバーにリアルタイムで複製されます。重要なデータはオンプレミスで複製されます。それにより、n+2 の冗長性が備わり、ハードウェアの障害が発生した場合にも、データを失うことなく迅速かつ透過的に回復できます。その他にも、ディスクスナップショットとオフラインバックアップが定期的に取られます。広範にわたる回復テストを 1 年に 2 度実施しており、お客様に以下を保証するために最新のサービスアーキテクチャーを開発しました。

- すべての層にわたる冗長性
- オンサイトおよびオフサイトのバックアップとデータ複製
- データ漏えい防止 - 30 日間
- バックアップの整合性テストとフェイルオーバーのシミュレーション
- 目標回復時間 (RTO) = 15 分間
- 目標回復地点 (RPO) = ほぼリアルタイム
- 99.9% の SLA（サービスレベル契約）順守

アプリケーション開発のセキュリティ

セキュリティの考慮事項は、製品開発プロセスのすべての段階で重要な役割を果たします。SAP Customer Data Cloud は、セキュリティ機能を製品のライフサイクルに事前対応的に統合し、製品がリリースされる前にリスクを特定して適切な軽減策を講じられるようにするためのフレームワークを備えています。以下の方法でリスクを早期に特定することで、効率的に適宜リスクを削減し、よりセキュアな製品とすることができます。

- **教育**：製品のライフサイクルに関与する主要な人物に対して、セキュリティのテクノロジーとベストプラクティスに関するトレーニングを実施して、現在の脅威の状況に対処できるようにします。
- **計画**：要件を再検討し、評価範囲について合意して、顧客および運用に関する潜在的なリスクを特定します。
- **モデリング**：サービス要件を再検討し、顧客および運用に関する潜在的なリスクを特定します。また、アプリケーションセグメントに従ったテスト計画に合意し、ネットワークトポロジーとデータフロー、さらに保護プロファイルを設計します。
- **アセスメント**：アプリケーションコードのスキャンと脆弱性の評価、およびビジネスニーズに応じたペネトレーションテストを定期的に実行します。具体的には、1OWASP の上位 10 の脆弱性に対する保護プロファイルをテストします。さらに、インターナショナルバグバウンティプログラムにより、セキュリティリサーチャーがプラットフォームの潜在的な脆弱性を継続的にテストし、責任を持って公開できるよう支援しています。
- **対処**：攻撃の傾向の変化、バウンティプログラム、および顧客からのフィードバックに従って製品の安全性を維持し、セキュリティの脅威に対処します。

また、事前にお客様と当社とで調整を図り、範囲を設定した上で、独自のペネトレーションテストを実施されることもお勧めします。SAP のソリューションチームは、SAP Customer Data Cloud 上で発見され、合意されたスケジュールに従い SAP に対して適切に公開された、実在するあらゆるセキュリティ上の脆弱性を解決すべく努めます。

保存時のセキュリティ

デフォルトでは、SAP Customer Data Cloud は、個人を特定できる情報 (PII) およびその他の保存時の機密データはすべて AES-256 の暗号化アルゴリズムを使用し、パスワードを NIST の承認済み PBKDF2 アルゴリズムでハッシュ化します。データへのアクセスの保護をさらに強化するため、SAP のソリューションでは HMAC-SHA1 を使用して要求にデジタル署名しており、API を使用する顧客は、SAP のサーバーに対する要求に同じアルゴリズムで署名する必要があります。さらに、OAuth 2.0 に完全に準拠した API アクセスも提供しています。

SAP Customer Data Cloud での管理コンソールを使用した情報へのアクセスも、2 要素認証プロセスと強力なロール・権限アーキテクチャーにより保護されており、サイト管理者はそれぞれのコンソールのユーザーが見たり使ったりできるものを詳細に管理できます。

動作に応じたセキュリティ
SAP Customer Data Cloud は、機密データをサーバー間でやり取りするときに、セキュアなチャネル (TLS) を使用します。さらに、ユーザー削除などの重要な操作を実行する REST API コールは、サーバー間の署名済み要求としてのみ許可されます。

リスク管理
SAP Customer Data Cloud ソリューションの管理チームは、情報セキュリティ要件に関する組織のニーズを特定するために必要な、強化されたリスク評価方法を定義しています。リスク評価は、適切なセキュリティ管理を実践し、情報資産がビジネスにもたらすリスクに応じてそれらの資産を管理できるようにするための基盤となります。

リスク評価プロセスの目標は以下のとおりです。
- SAP Customer Data Cloud のビジネスステークホルダーにより事業における重要な棚卸資産と見なされたものを特定する。
- データ分類レベルごとにシステムを特定する。
- リスクにさらされているものを特定する。
- ビジネスへの影響に基づいてセキュリティの側面からリスクの重大度を計算する。
- 計算されたリスクを軽減するために必要なセキュリティ管理を適用する優先度を定める。

アクセス制御
SAP の管理チームは、情報システムのあらゆるレベル（アプリケーションのソースコード、OS、データベース、およびネットワーク）で強化されたアクセス制御と認可機構を実装しています。従業員には、「最小限の権限」の原則に基づいて、それぞれのロールに応じた権限が付与されます。

システムセキュリティプラクティス
SAP のシステムセキュリティプラクティスには、サーバーとワークステーションの OS の強化、パッチ管理、監査とイベントログ、マルウェアからの保護が含まれます。重要なシステムの設定やサービスの構成や状態を自動的にセキュアに保つためのプロビジョニングシステムを導入しています。すべての管理操作は、管理者に対する 2 要素認証を使用して仮想プライベートネットワーク (VPN) 上で実行されます。

ネットワークセキュリティプラクティス
SAP Customer Data Cloud で採用されているネットワークセキュリティプラクティスには、最小限必要なポートのみを開く、ネットワークを環境（実働、開発、テスト）ごとに分離する、帯域外のセキュアなネットエワークデバイス管理インターフェースを使用する、ネットワークデバイスを強化する、といったプラクティスが含まれます。AWS 上では GuardDuty サービスを利用して、悪意のある振る舞いや許可されていない振る舞いを継続的に監視して、エコシステムに影響を及ぼす可能性のあるあらゆる脅威に関して必要な可視性が得られるようにしています。

分散型サービス拒否 (DDOS) の対応
SAP Customer Data Cloud では、想定していなかったほど極端に増えてしまったトラフィックを処理する必要がある場合に、サービスの規模を迅速に拡大できるようにするとともに、クラウドを活用した DDoS 対応サービスのプロバイダーを利用しています。AWS 上では AWS Shield を活用し、最もよく知られているインフラストラクチャー攻撃に対する包括的な可用性の保護を得られるようにしています。Alibaba データセンターについては、トラフィックの急増にも確実に対処してくれるプロバイダーを利用しています。Selectel データセンターでは、Volumetric DDOS 攻撃に対処するためにレート制限テクノロジーを利用しています。

特に DNS DoS 攻撃に関しては、2 つのプロバイダー（Dyn と AWS Route 53）を利用して、そのいずれかが攻撃されたときにも可用性を保てるようにしています。

変更管理
SAP では、適切に文書化され、まとめられた変更管理の承認および実装プロセスが用意されています。このプロセスは、サービス提供を効果的に管理し、保護するために重要なものです。

脆弱性管理
新たなセキュリティの脆弱性が日々発見されていることから、SAP は、関連するベンダーが公開したセキュリティ情報、セキュリティフォーラム、コミュニティ、新たに公開された脆弱性に関して業界の主要な企業が発したセキュリティ警告（US-CERT や Bugtraq など）の継続的な監視を始めとする情報収集プロセスを採用しています。

収集された脆弱性に関するデータはすべて識別および分類され、脆弱性を修正するための、推奨パッチ計画が関係者に通知されます。

発見された事象に対しては、以下の重大度が割り当てられます。
- **OK** – 脆弱性は発見されませんでした
- **Low** – 少なからず被害を受ける可能性はありますが、チェックされた項目に関しては脅威と見なすようなものではありません
- **Medium** – 被害を受ける可能性は中程度ありますが、脆弱性の悪用を妨げることのできる管理機能が用意されています
- **High** – 欠陥を突かれて、チェックされた項目に関して直接被害が及ぶ可能性があります
- **Critical** – チェックされた項目に関してシャットダウン、乗っ取り、または偽装を招くような欠陥が存在している、もしくはそうした欠陥が容易に生じる可能性があります

脆弱性の対応に関する SAP のデフォルトの方針は以下のとおりです。
- 極めて重大な脆弱性が発見された場合は、公開する前に修正しなければならない
- 0 日攻撃が発見された場合は、ケースバイケースで軽減策を講じるものとする

モニタリング
24 時間 365 日間、自動または手動でのモニタリングを行っています。SAP のネットワークオペレーションセンター・チームが、サービスのあらゆる側面から、各プロバイダーの API レベルに至るまでモニタリングをしています。

クラウドサービスの重要な項目については、手動で定期的（15 分ごと）にテストを実施しています。しきい値とイベントをあらかじめ定義し、それに応じてキャパシティを調整します。

インシデント管理
SAP Customer Data Cloud の情報セキュリティインシデント管理ポリシーは、インシデントを効率的かつ効果的に処理するためのガイドラインを提供しています。このポリシーは、特定のハードウェアプラットフォーム、オペレーティングシステム、およびアプリケーションを対象としない、一般的なインシデント対応のガイドラインを示しており、インシデントの検知、分析、優先順位付け、修正、および通知を中心としたものです。

インシデントが発生した場合には、顧客への通知手順に従って、影響が及ぶ顧客に通知されます。SAP は、個々のセキュリティインシデントの特性、発生源、および想定される影響に応じて、異なる方法で対処しなければならい場合もあることを理解し、承知しています。セキュリティインシデントに対処するための一般的な手順は、以下のとおりです。

- 迅速に対処する
- 情報を取集する
- 根本原因を分析する
- 要因を分類する
- 対応計画を作成する
- 計画を実行する（導入手順に沿って）
- 状況のまとめと報告
- 是正および予防措置の実施

人事管理セキュリティ

従業員は、SAP の最も重要なリソースです。SAP では、以下のことを徹底するためのポリシーと手順を確立および実装しています。

- すべての従業員が、自身の雇用条件について理解し、承知している
- 情報セキュリティのガイドラインがすべての従業員に周知されている
- 情報セキュリティ啓蒙プログラムが存在し、実施されている
- セキュリティ侵害に対処するための正式な訓練プロセスが確立されている
- 雇用の終了およびロールの変更が、管理されたセキュアな方法で実施されている

コンプライアンス

SAP Customer Data Cloud については、毎年の ISO 27001、ISO 27018、および SOC 2 Type II の認証プロセスの一環として、独立した第三者機関による監査を実施しています。この監査では、処理施設（データセンター）と運用施設（オフィス）、顧客データとプライバシー、テクノロジーとサービス、マーケティング、金融、人事データといった領域が対象となります。こうした監査は、情報資産を保護して関係者の信頼を得るための適切なセキュリティ管理方法の選択と実施を徹底することを目的としています。SAP の管理チームは、日々の活動を通じ、社内のガイドランとその他のセキュリティ業界のベストプラクティスに従って、お客様に対する情報セキュリティの管理を運用および強化しています。さらに、信頼できる組織およびソーシャルネットワークの定めた規格に従ってデータ管理の責任を確実に果たします。

- **ISO 27001:2013**（イスラエル規格機関による年 1 回の外部監査）
- **ISO 27018:2014**（イスラエル規格機関による年 1 回の外部監査）
- **SOC 2 Type II**（PwC による年 1 回の外部監査）
- **CSA STAR Level 1**（自己評価）
- 児童オンラインプライバシー保護法 (COPPA) 準拠
- 医療保険の相互運用性と説明責任に関する法令 (HIPPA) 準拠
- 一般データ保護規則 (GDPR) 対応
- 業界標準フレームワークへの適応（NIST、CIS、OWASP、SANS、その他）
- 情報収集（US-CERT、Bugtraq、バウンティプログラム、その他）

SAP は情報セキュリティの向上に積極的に取り組んでいます

適切な基準・要件に準拠することで、日々の活動における情報セキュリティのリスクを確実に特定できるようになります。特定されたリスクは、社内のリスク管理方法に従って分析および処理されます。

方針に基づくセキュリティ

設計に基づくプライバシー

信頼というミッション

各地域のプライバシー規則
SAP は複数のデータセンター（米国、ヨーロッパ、オーストラリア、中国、およびロシア）を通じて SAP Customer Data Cloud を提供することで、多国籍の顧客ベースが各地域のスレージ要件を満たせるようにしています。グローバル企業として、SAP は各地域のプライバシー規制および国際的なプライバシー規制を順守して、顧客 PII のプライバシーを保護します。SAP の管理チームは、関連するプライバシー規則と規則の改定を追跡して、SAP のソリューションやお客様に及ぼすあらゆる影響を評価し、それらに対処します。

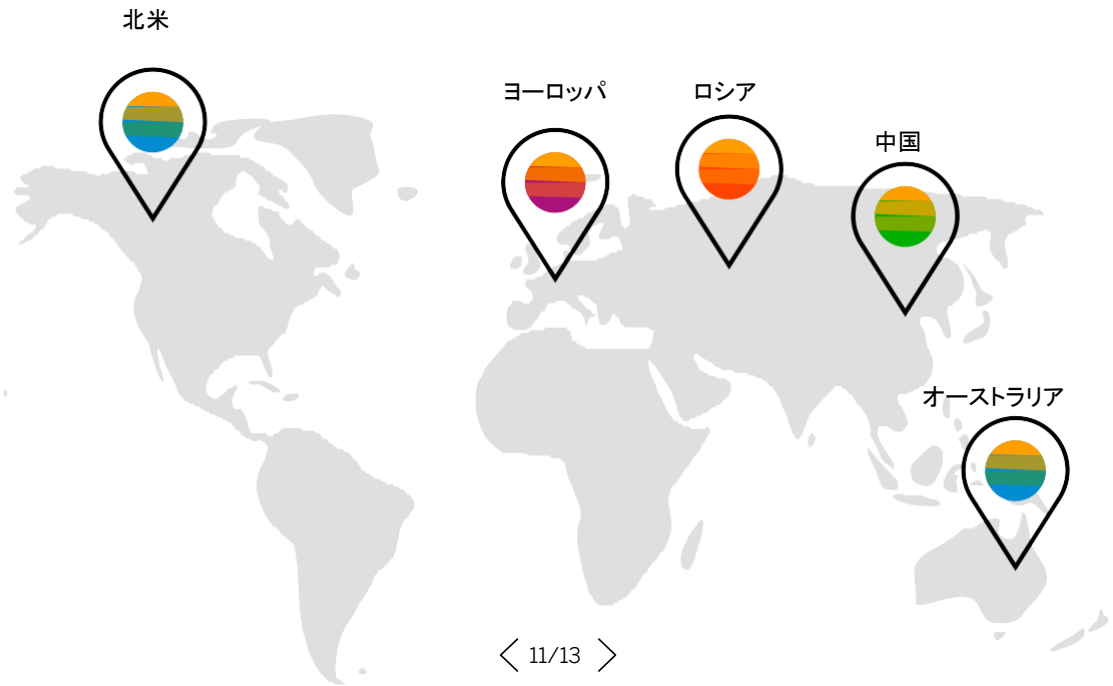
クレジットカード業界データセキュリティ基準
SAP Customer Data Cloud では、クレジットカード業界データセキュリティ基準に従い、お客様に代わってクレジットカードのデータを収集、保存、管理、または転送するようなことは一切ありません。

米国児童オンラインプライバシー保護法
（COPPA）は、最終的には消費者の責任において対応していただく必要がありますが、SAP Customer Data Cloud では、Registration-as-a-Service 機能により、Web サイトへのアクセス時に年齢確認を行い、13 歳未満の消費者個人情報を Web サイト上に保存できないようにすることで、COPPA への準拠を促進しています。消費者は、SAP Customer Data Cloud で提供されるログイン画面が表示される際に COPPA に準拠しているかを気にかける必要はありません。これは、複数の Web サイトでプロファイルを収集することはなく、内部でのレポートの作成やサービスのサポートに必要な範囲でのみクッキーを使用するからです。

ソーシャルネットワークポリシー
SAP Customer Data Cloud は、消費者がソーシャルネットワークポリシーに準拠できるようにするために、いくつかのツールを提供しています。提供されるツールには以下のものがあります。

アカウントの自動削除：ユーザーがサイトの Facebook アプリでデータアクセス権を無効にすると、そのユーザーのすべての非公開情報がサイトのデータベースから削除されます。

アカウントの自動更新：ユーザーが Facebook を使用してサイトにログインした後で Facebook のプロファイルを更新すると、サイトのデータベースでその情報が更新されるため、データを常に最新の状態に保つことができます。



プライバシー

業界をリードする SAP Customer Data Cloud ソリューションでは、顧客の個人情報を保護することを重視しており、そのために力を注いできました。SAP の製品、ポリシー、データ保護プラクティスは、「プライバシーバイデザイン」の原則に従っています。その目的は、法令を遵守するだけでなく、SAP のソリューションとビジネス慣行に対する顧客との信用と信頼を得ることです。

SAP のプライバシーポリシーおよびデータ保護プラクティスは、契約に基づき、サプライヤーやパートナーとの関係においても適用されます。取締会のメンバー、従業員、そして SAP に関連して働く人々は、それらのポリシーやプラクティスについて周知されるとともに、それに従うことが求められます。SAP のプライバシーポリシーおよびプラクティスは、SAP の信頼と誠実さ、そして品質を重んじる姿勢を反映したものであり、そうした姿勢を強化するものです。

SAP は、データ収集における透明性を高め、データの使用目的をユーザーに知らせるためのいくつかのツールを提供しています。

パーミッションに基づくソーシャルログイン
ユーザーが既存のソーシャルプロファイルを使用してサイトにログインする際に、特定のデータポイントにアクセスするためのパーミッションがあるかどうか（誕生日や所在地）を確認するためのダイアログボックスが表示され、ユーザーは共有する情報を自由に選択することができます。

ユーザーデータの制御
SAP Customer Data Cloud の登録サービスとして Registration-as-a-Service フォームを使用してユーザー登録およびログインを行う場合、サイト上にエンドユーザー用のメニューがすぐに表示され、必要に応じてサイトに保存されていたデータをダウンロードしたり、編集または削除したり、サイトのアカウントを削除したりするリクエストを出すことができます。

カスタマイズ可能な UI
セルフサービスフォームは完全にカスタマイズ可能で、お客様側で、プライバシー通知、使用条件、マーケティング用オプトイン、アカウント設定フォーム、およびその他の通知を UI に含めることができます。

管理者ロールとパーミッション
SAP Customer Data Cloud ソリューションは、内部のユーザーがアクセス可能な機能やデータを管理者が管理することのできる、強固なロールおよびパーミッションを備えています。
管理者は、ユーザーグループを作成し、アクセス権を細かく割り当てて（サイトやアプリケーションの ID ごと、サービスごと、API ごとなど）、エンドユーザーの 個人情報を確実に保護することができます。

リスクベース認証
これは、特定のログイン試行に関連するリスクのレベルを計算し、そのリスクレベルに応じた認証チャレンジをユーザーに表示する、追加のアカウントセキュリティ層です。

SAP® Customer Experience

フォローする

sap.com/crm

情報セキュリティおよびデータプライバシーの方針(19/06)

THE BEST RUN SAP®