セールスフォースのための重要なコントロールの実装

組織がセールスフォース アプリケーションに安全に移行するには

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for the Enterprise Resource Planning Working Group is https://cloudsecurityalliance.org/working-groups/enterprise-resource-planning.

Acknowledgments

Lead Authors:

Frederik Weidemann
Sergio Abraham
Juan Perez-Etchegoyen

Reviewers:

Ivan Djordjevic

CSA Global Staff:

Shamun Mahmud

The Enterprise Resource Planning (ERP) WG seeks to develop best practices to enable organizations that run their business on large ERP implementations, such as SAP or Oracle applications, to securely migrate to and operate in cloud environments. Every ERP deployment is something that is unique to each organization. In most cases, organizations spend months, if not years, customizing their SAP or Oracle implementations and also spend a significant amount of money with third-party contractors to complete implementations. This makes standard security measures more difficult to implement due to the differences of each deployment. The complexity of these large implementations, combined with the criticality of data and processes housed in these applications, necessitates the establishment of industry best practices to provide security guidelines for companies migrating to the cloud, in order to protect the organizations' critical infrastructure.

日本語版提供に際しての告知及び注意事項

本書「セールスフォースのための重要なコントロールの実装」は、Cloud Security Alliance (CSA)が公開している「Critical Controls Implementation for Salesforce」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2021年07月09日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。

(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3. 本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する(組織内の利用者に順守させることを含む)ようにしなければなりません。

(3) 本書をダウンロードした者は、CSA ジャパンからの文書(電子メールを含む)による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSA ジャパンからの文書(電子メールを含む)による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. 原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「セールスフォースのための重要なコントロールの実装」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

井上　淳
太田　吏城
小野　貴博
佐藤　智典
神保　冬和子
鈴木　伸
高尾　美由紀
福井　将樹
松浦　一郎　CISSP, CISM, CDPSE
満田　淳
諸角　昌宏
山下　亮一
渡邉　浩一郎　CISA,CISSP

目次

はじめに

本書は、Salesforce をクラウドで展開する際に、どのようなセキュリティの変更が必要かを組織が判断するのに役立ちます。なお、本ドキュメントでは中核となるSalesforceプラットフォームの使用に焦点を当てます。Salesforce は大きな拡張性を持っています。

このドキュメントの対象者は、Salesforce を新規導入する利用者、並びに、基本的なセキュリティを実現したい既存のSalesforceの利用者です。

本ドキュメントの使用方法

本ドキュメントは、Salesforce におけるセキュリティ運用のベストプラクティスを推進するためのリファレンスです。Salesforce セキュリティガイドなど、Salesforce（およびSalesforceを提供するベンダー）のドキュメントや具体的な指示を置き替えるものではありません（訳注：日本語版Salesforce セキュリティガイドはこちらを参照）。

特に、本ドキュメントは、クラウドセキュリティアライアンス（CSA）の Enterprise Resource Planning（ERP）ワーキンググループの継続的な議論とともに使用することを想定しています。関連するリソースについては、ERP ワーキンググループのサイトを参照してください。

このドキュメントに記載されているSalesforceプラットフォームに対する20個のコントロールはそれぞれ、基準となったCSAの包括的なTop 20 Critical Controls for Cloud Enterprise Resource Planning Customersに直接対応します。

各コントロールは2つのパートで定義されます:

- **コントロールの実装**：コントロールの実装では、コントロールの根拠を定義します。情報技術（IT）のリーダーと情報セキュリティおよびコンプライアンスの専門家は、各コントロールを理解し、それらをIT運用、セキュリティ、コンプライアンスに対する包括的なコントロールに対応付けることができます。
- **チェックリスト**：各コントロールを実装するために、具体的な要件や手順のチェックリストが示されています。データベース管理者（DBA）およびシステム管理者は、このセクションを使用してコントロールを実装できます。

このドキュメントでは、RFC2119で定義されているように、MUST、MUST NOT、SHOULD、SHOULD NOT、MAYという単語を使用します。MUSTは、チェックリストの項目が絶対的な要件であることを意味します。SHOULD は、推奨事項に従わない背景やその影響を含む理由が文書化されている場合を除き、その項目を実装することが推奨されていることを意味します。MAY は、純粋に任意の項目を定義しています。

本書を最大限に活用するためには、読者はCSAのCloud Controls Matrix（CCM）およびセキュリティ強化のためのCenter for Internet Security’s (CIS) Benchmarksに精通している必要があります。

コントロールの実装

ドメイン	Salesforce
コントロールID	**USR01 - セキュアな認証**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceで有効化された認証メカニズムは、アプリケーションユーザになりすますことができないようにセキュアに構成する必要があります。このためのベストプラクティスは、シングルサインオン、強固なパスワードポリシー、および認証プロセス中に強固な2つめの要素を使用することです。
チェックリスト／優先順位に基づくステップ	次の属性を認証プロセスに適用することを推奨します： 1. 強固な2つめの要素を使用した多要素認証を実施しなければなりません。弱い要素の例としては、メールやSMSがあります。強固な要素の例は、TOTPまたはSalesforce Authenticatorです。 2. エンドユーザ、テクニカルユーザ、外部ユーザを含むすべてのユーザに対して、強固なパスワードポリシーを実施する必要があります。これは、組織全体の強固なポリシーを有効にすることによって実現されます。[設定]に移動し、[クイック検索]項目で[パスワードポリシー]を選択します。プロファイルレベルでパスワードポリシーに個別のしきい値を定義することができます（例:外部ユーザなど）。 3. 可能であれば、シングルサインオンを有効にすべきです。 4. **セキュリティの向上：** • システム管理者などの高い権限を有するユーザの場合、パスワードは非常に厳しく複雑な要件に従う必要があります。 • 攻撃対象面を減らすために、使用されているすべてのプロファイルに対してログイン時のIPアドレスの制限と営業時間を設定する必要があります。

リファレンス

- Salesforce Trailblazer Community | Salesforce Multi-Factor Authentication FAQ
- Salesforce Trailblazer Community | Set Password Policies
- Salesforce Trailhead | Secure Your Users' Identity
- Salesforce Trailblazer Community | View and Edit Password Policies in Profiles
- Salesforce Security Guide | Authenticate Users

ドメイン	Salesforce
コントロールID	**USR02 - ユーザアカウント管理**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	ユーザアカウント管理は、適切なユーザだけがアクセスできることを保証するために最も重要です。このコントロールが目的としていることは、ビジネス情報への未認可なアクセスを防止するために、Salesforce 組織内に存在するユーザアカウントが適切に管理され統治されていることを確実にすることです。
チェックリスト／優先順位に基づくステップ	1. テストおよび開発の目的で非本番用のサンドボックスを作成する際、本番ユーザアカウントを変更して非アクティブ化しなければなりません。 2. ユーザ管理は、全社的なアイデンティティ管理システムを使用して一元化すべきです。 3. 未使用のユーザアカウントは無効にしなければなりません。ユーザアカウントを凍結しても良いです。その場合、レコードの割り当ては変更されず、ライセンスは解放されません。 4. ユーザアカウントは削除できないため、法的要件がある場合はデータを匿名化する必要があります。
リファレンス •	Salesforce Trailblazer Community | Deactivate Users • Salesforce Trailblazer Community | Considerations for Deactivating Users • Salesforce Trailblazer Community | Data Protection and Privacy • Salesforce Trailblazer Community | Identity Connect • Salesforce Trailblazer Community | Manage Salesforce User Identities with SCIM • Salesforce Trailblazer Community | Let Users Scramble Their User Data • Salesforce Apex Reference Guide | UserManagement Class

ドメイン	Salesforce
コントロールID	**USR03 - ロールベースのアクセスコントロール**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceの権限管理には、ロールベースのアクセスコントロール（RBAC）を使用すべきです。Salesforce は、ユーザに割り当てるプロファイルに同一の認可をバンドルし、同じ機能領域または技術領域のユーザに付与することによって、RBACの機能をサポートします。さらに、権限セットを使用して割り当てを行うこともできます。 Salesforce オブジェクトへのアクセスは、一般的にオブジェクト権限を使用して定義できます。さらに、項目ごとに制限を加えることもできます。そして、個々のレコードへのアクセスは、共有ルールを使用して定義できます。さらに、レコードへのアクセスは、ロールに基づく階層構造を用いて制御することができます。ロールは、特定のSalesforceオブジェクトのレコードへのアクセスの許可を継承させるために機能します。そのため、ロールは他のシステムとは異なる振る舞いをします。一般的に、プロファイルと権限のセットは、他のITシステムでロールと呼ばれるものと同等です。 Salesforceを継続的に監視し、ユーザが日々の業務に必要な最小限の適切な権限のみを持つようにする必要があります。これが最小権限の原則です。 この制御を実施する上で最も重要なことは、ユーザ、権限、役割、責任の変更管理プロセスを検査することです（例：従業員の役職が変わり、権限を変更する必要がある場合）。人事異動でポジションが変わった場合のプロセスを確立する必要があります。入社や解雇を監視し、適切な対応を取る必要があります。他のアプリケーションと同様に、この種の変更が適切に制御されていない場合、異なる権限セットやプロファイルが積み重なった権限により、ユーザが強力な権限を持つようになる可能性があります。

チェックリスト／優先順位に基づくステップ	1. 権限の割り当ては、"最小権限の原則"に従い、対象となるユーザに必要な権限のみを割り当てなければなりません。 2. "administrators can login as any user"機能をコントロールする必要があります。この機能は、管理者が任意のユーザとしてログインし、ユーザの同意を得ることなく、そのユーザになりすますことができます。 3. "login as any user"機能の使用状況は、設定および設定変更履歴の分析により自動的に監視すべきです（訳注：Audit Trailの訳は一般的には監査証跡ですが、Salesforceでは設定変更履歴という訳語を当てています）。 4. 最小権限の原則に従ったアサインを確認し、職務分掌との矛盾が起こらないように権限を割り当てます。
リファレンス	• Salesforce Security Guide | Give Users Access to Data • Salesforce Trailblazer Community | Controlling Access Using Hierarchies

ドメイン	Salesforce
コントロールID	**USR04 - 緊急アクセス**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	緊急アクセスは、システム障害やエラーが発生した場合、あるいは通常の業務過程でも病欠、休暇、解雇など担当者不在の結果として従業員に付与されます。緊急時のアクセスを許可すると、通常は禁止されている権限が与えられることが多く、適切に管理されなければならない追加のリスクにさらされます。 1. 誰が、いつ、どこで、どのように、何ができるのかを説明する緊急時アクセスポリシーを定義します。緊急アクセスの管理、アクセス許可、監視、終了、報告、および監査の対応責任を定めます。緊急アクセスの許可は、リスクベースで、職務分掌と最小特権を考慮しなければなりません。 2. 以下の観点を含むポリシーを定義する必要があります： • 管理：緊急アクセスの手続きを管理するのは誰か？ • アクセス権の付与：誰がどのような行動を承認するのか？ • アクセス監視：何が、いつ、誰に、どのように報告されるのか？ • アクセス終了：誰が承認するのか？ • アクセスの報告と監査：何を、いつ、誰に、どのように？
チェックリスト／優先順位に基づくステップ	**1. 全体** • 要求された緊急アクセスのためのアクセス要件を決定します。 • すべての緊急アクセス活動にサービスリクエスト（チケット）を要求します。承認ワークフローを活用し、有効性を監査します。 • 緊急アクセスの対象となるアプリケーションおよび支援テクノロジ内のアカウントを特定します。

- 緊急時に使用するアカウントについては、長くて複雑なパスワードを使用し、password safeの使用を強制します。複雑なパスワードと企業のpassword safeの両方が使用されていることを確認します。
- 監査ログのストリーミング（設定変更履歴やログイン履歴）を設定して監査ログをSIEMに流して相関をとり、サービスリクエストやpassword safeの動きを伴わないアカウントの緊急使用を特定します。トランザクションログへのアクセスには、追加の商用ライセンスが必要です。緊急ユーザへのアクセスは、端末の発信IPアドレスに対してログイン制限をかけるべきです。
- すべての緊急アクセス活動に対する定期的な報告と監査手順を実施します。

2. **セキュリティ強化**
   - 緊急ユーザのパスワードを安全に受け渡すためには、サービスリクエスト（チケット）を参照すべきです。サービスリクエストが、パスワードを受け取る人と同じ人に割り当てられていることを確認します。

リファレンス

- Salesforce Trailblazer Community | Monitor Login History
- Salesforce Trailblazer Community | Enable Event Monitoring
- Salesforce Trailblazer Community | Require Users to Log In with SSO

ドメイン	Salesforce
コントロールID	**USR05 - 職務分掌**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	職務分掌（SOD）とは、ある一つのプロセスの最初から最後までを、特定の人がコントロールしてはならないという考えをサポートするコントロールの原則です。このコントロールは、利益相反、不正、誤りおよび悪意のある行為の防止を目的としています。どのプロセスにおいても、アクションの作成と承認のような、互換性を持たない複数のタスクを実行する職能を持つ人はいないはずです。例えば、不正な配送や出荷を隠蔽するために架空の注文を作成できることは許されません。SODは、タスクや従業員の柔軟性とセキュリティを両立させる必要があります。 SODマトリクスを用いて、ERPの中で職務分掌を実装できます。このマトリクスは、内部および外部の監査人によってレビューされ、承認される必要があります。さらに、アクセスは電子的に要求され、システムによるSODの検証が必要です。SOD検証されたリクエストは、レビュー、承認およびアクティベーションのために適切な担当者に転送されますが、検証が失敗した場合はフラグが立てられ、報告、解決のために返却される必要があります。システムはトランザクションの使用状況を継続的に監視し、ユーザが互換性のないトランザクションを実行するたびに、自動的にレポートが生成される必要があります。 サービスモデルに係わらず、適切な職務分掌の保証は、常に利用者の責任になります。
チェックリスト／優先順位に基づくステップ	1. SODのコンフリクトは、SODマトリクスを使用して文書化されなければなりません。 2. パーミッションが割り当てられる際には、予防的なSODのチェックが実行される必要があります。 3. 割り当てられた権限を持つすべてのユーザに対し、SODの不備が継続的に監視される必要があります。 4. 機微性の高いトランザクションの使用状況を監視し。警告やレポートを行います。

リファレンス	• Salesforce Trailblazer Community - Administrators and Separation of Duties

ドメイン	Salesforce
コントロールID	**USR06 – セキュアなユーザプロビジョニング/デプロビジョニング**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforce組織内で技術的および機能的なユーザをプロビジョニングすることは、運用の観点から重要なセキュリティコントロールです。このプロビジョニング・プロセスでは、次の事項を確実に行う必要があります: 1. ユーザの作成には、正当なビジネス上の理由と要件があります。 2. ユーザは適切な組織の中に作成されます。 3. このアカウントには責任者が割当てられます。 4. ユーザの権限(認可)は、最小権限の原則に基づいて割り当てられます。 5. 当該アカウントに適用可能な場合には、定義された有効期間があります。 管理されていないアカウントや休眠状態のアカウントが悪用され、認可されていない方法でシステムにアクセスされる可能性があります。そのため、ユーザアカウントのデプロビジョニングが適切に管理される必要があります。
チェックリスト／優先順位に基づくステップ	1. ユーザのプロビジョニングとデプロビジョニングは、適切に管理され、企業ポリシーにおいて文書化される必要があります。ISO/IEC 27001、NIST Cybersecurity Framework、PCI DSS(Payment Card Industry Data Security Standard)などの、関連するコンプライアンス要件が満たされている必要があります。 2. 権限を付与する際には、最小権限の原則が実施される必要があります。各ユーザには、そのビジネス活動に必要な権限のみが割り当てられる必要があります。 3. 活動していないアカウントに関して、当該組織を監視します。

リファレンス

- Salesforce Trailblazer Community | Security Center Metrics, User and Profile Metrics
- Salesforce Trailblazer Community | Identity Connect
- Salesforce Trailblazer Community | Manage Salesforce User Identities with SCIM

ドメイン	Salesforce
コントロールID	**USR07 - アカウントセキュリティ**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	特にオンプレミスのアプリケーションをSalesforce Cloudへ移行している場合、Salesforceのユーザアカウントのセキュリティは最も重要です。侵害された有効な認証情報を用いたとしても、攻撃者にとってSalesforce組織へ侵入することが困難になるように、ログインプロセスが開発されるべきです。 さらに、Salesforceの組織には、適切な標準を参照して、セッション管理のメカニズムを実装すべきです。 Salesforceを使う組織は、以下を確実にすべきです： 1. 多要素認証を有効にします。 2. 複雑さより長さを優先したパスワードルールを有効にします。 3. ユーザのログイン行動を分析し、普段と異なる場所や時間でのログインを検出します。また、他のユーザアクティビティと関連付けます。（例：CASBプロバイダや条件付きアクセスが提供するデータ） 4. 適切にSSOを実装します。 5. ERPシステムへのアクセスを特定のネットワークに限定します。 6. セッショントークンが動的であり、十分にランダムで、暗号化され、かつ有効期限付きであることを確実にします。 7. ユーザーアクティビティやトランザクションの監査ログを有効にします（管理者を含め、読取専用とします）。
チェックリスト／優先順位に基づくステップ	1. ユーザの認証情報を保護するため、クライアントとサーバの間を暗号化します。 2. すべてのユーザに対して、多要素認証を強制する必要があります。

	3. 多要素認証がサポートされないところでは、代替するコントロールを整備する必要があります(IPアドレスの制限など)。 4. ログインのログを中央ログサーバに送信します。 5. SIEM製品を使って、中央ログサーバを監視します。
リファレンス	• Center for Internet Security | CIS Controls • NCSC | Cloud Security Guidance • Salesforce Security Guide • NIST | Special Publication 800-63B Digital Identity Guidelines

ドメイン	Salesforce
コントロールID	**APP01 – セキュアランドスケープ**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceの重要性から、アプリケーションは通常、多層環境に配置され、その開発とテストは専用のシステムにおいて実施されます。ランドスケープ全体に影響を与えるリスクは、（セキュアな設定、分離、インタフェース、アクセスの観点において）本番環境の完全性とセキュリティを変えてしまう可能性があります。 本番環境への未認可のアクセスが許可されないことを確実にするため、ランドスケープ全体に渡って、プロセスを実装しなければなりません。これらには次のものが含まれます： • 企業をまたぐシステム／プラットフォームにおいて、アクセスや認可に関わるリスクを予防します。 • 役割と責任が明確に定義されていることを確認します。 • ランドスケープ全体にわたる特権昇格を回避するために、全ての環境で同じレベルのセキュリティが実装されていることを確実にします。 サービスモデルに関係なく、この管理は常に利用者の責任です。
チェックリスト／優先順位に基づくステップ	1. Salesforceのすべての範囲内のガバナンスポリシーとコントロールのインベントリを作成します。 2. ポリシーおよび関連するコントロールの所有権（チーム）を決定します。 3. 現在のポリシーの有効性を評価します。 4. 新しいコンプライアンス要件に適応できるように定期的なレビューと更新のプロセスを設定します。 5. 可能な場合、自動制御を実装すべきです。
リファレンス	該当なし

ドメイン	Salesforce
コントロールID	**APP02 - セキュアベースラインコンフィグレーション**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforce環境は複雑で、いくつかの異なるソリューションで構成される可能性があります。これらのコンポーネントは相互に密接に相互作用することが可能で、広範囲にカスタマイズできると共に構成可能となっています。Salesforceプラットフォームの拡張性は魅力的な利点である一方、構成可能なオプションのかなりの割合がセキュリティに重大な影響を及ぼします。それゆえ、セキュリティプロセスのベストプラクティスは以下のものを含みます: 1. すべてのコンポーネントとテクノロジのベースラインを定義します。 2. ベースラインを実施します。 3. 可能な場合、ベースラインの実施と監視を自動化します。 4. レビューと更新の手順を設定します。
チェックリスト／優先順位に基づくステップ	1. セキュアなベースラインポリシーを定義すべきです。 2. ベースラインポリシーは、次のもので構成されるべきです: • セキュリティ構成 • 認証 • 認可と重要な権限 • インタフェース（転送中のデータ） • 資産保護（保存時） • ネットワーク要件 • ロギング • 監視 • カスタム開発（例：APEX） • セキュリティパッチポリシー • 変更管理 • 適用される規制順守要件 • 監査および不正防止手順 • セキュリティガバナンスフレームワーク

	• リスク管理手順 • 運用上のセキュリティ手順 • データ分類/カテゴリ
リファレンス	• NIST Computer Security Resource Center | NIST Risk Management Framework SP 800-53 Revision 5.1: CM-6(1) • Salesforce Trailhead | Use Health Check to Scan Your Security Configurations

ドメイン	Salesforce
コントロールID	**APP03 - セキュリティの脆弱性**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceは、リリースバージョン（以前は「クリティカルアップデート」と呼ばれていました）を通じてコードのセキュリティの脆弱性を修正するパッチを定期的に提供しています。インフラストラクチャはSalesforceによって利用者向けに維持されますが、アプリケーションレベルでは、セキュリティ拡張を有効化する前に利用者がタスクを実行する必要がある場合があります。Salesforceは、変更点、組織に対する影響、およびいつまでに準備手順を行う必要があるかを、利用者に通知します。セキュリティ強化をオプトアウトすることはできませんが、必要な準備手順が欠落していると、組織に影響を与える状態で、新しいバージョンがアクティブ化されてしまう可能性があります。
チェックリスト／優先順位に基づくステップ	1. セキュリティアラートとリリースアップデートのために、継続的な脆弱性管理プロセスを設定する必要があります。 2. 各変更は、サンドボックス組織でテストする必要があります。 3. オフピーク時に本番環境でセキュリティ拡張機能をアクティブ化することをお勧めします。
リファレンス •	Salesforce Trailblazer Community | Release Updates • Salesforce Trailblazer Community | Keep Up with Security Alerts • Salesforce Trailblazer Community | Manage Security Contacts for Your Organization • Salesforce Trailblazer Community | Manage Your Notification Preferences in the Salesforce Help Portal

ドメイン	Salesforce
コントロールID	**APP04 - セキュアな通信**
テクノロジースタック	アプリケーション、ネットワーク
バージョン	すべて
コントロールの実装	Salesforce環境では、インターネットブラウザ（HTTP）、モバイルアプリケーション、APIアクセスなど、アプリケーションと通信する方法は複数あります。転送中のすべてのデータは、暗号化を使用して保護する必要があります。
チェックリスト／優先順位に基づくステップ	**アプリケーション** 1. 転送中のすべてのデータは、暗号化を使用して保護する必要があります。これには、内部通信と外部通信の両方が含まれます。 2. 発信APEXコールアウトはhttpsを使用する必要があります。 3. 外部に接続されたアプリケーションに向かって流れるデータ（AppExchangeやインタフェースなどを介して）も同様に保護する必要があります。例：Salesforceは、暗号化されていないFTPを介したアクセスを許可していません。 4. 外部に接続されたアプリケーションに向かって流れるデータ（AppExchangeやインタフェースなどを介して）も同様に保護する必要があります。例：Salesforceは、暗号化されていないFTPを介したアクセスを許可していません。 備考: 5. 暗号スイートと暗号化の設定はSalesforceによって処理されます。
リファレンス •	NIST Computer Security Resource Center | NIST Risk Management Framework SP 800-53 Revision 5.1: CM-6(1) • Salesforce Trailblazer Community | Allow Only Secure Connections to Your Domain with HSTS Preloading

ドメイン	Salesforce
コントロールID	**APP05 – 変更管理コントロール**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	不正なアクセスにより意図しない変更が本番システムに実装されないよう、組織の全てのSalesforceコンポーネントに適切な変更管理が実施されるようにしなければなりません。計画的な変更を行うためには、スコープの定義と影響評価が必要です。公開前にメタデータとカスタムコーディングによる変更についてテストしなければなりません。
チェックリスト／優先順位に基づくステップ	1. 変更は必ずサンドボックスでテストしなければならない。 2. 変更は必ずセキュリティレビューの対象としなければならない。 3. 変更はバージョン管理システム（GIT等）を用い追跡できるようにしなければならない。 4. 変更は配備前にUAT（訳注：ユーザ受入テスト）の対象としなければならない。 5. 本番環境への配備はバージョン管理システムで承認された成果物に基づき実施されなければならない。 6. 変更は組織内に周知されなければならない。 7. 開発担当者のみが変更を実施できるよう、本番環境ではアクセス制限をしなければならない。 8. 定期的に実行されるコピープロセス（訳注：Cloneの訳はクローンですが、SalesforceではProductionからSandboxへの組織の複製について「コピー」の訳語を当てています）を用い、テストのための実稼働前ステージング用サンドボックスを作成しなければならない。 9. セキュリティ対応のために本番環境にて手動で変更した場合は、バージョン管理システムで保持されている最新設定に自動的に戻さなければならない。
リファレンス	• Salesforce | Best Practices for Salesforce Change Management • Salesforce Trailhead | Architect Journey: Development Lifecycle and Deployment • Salesforce Trailhead | Determine Which Application Lifecycle Management Model Is Right for You • Salesforce Dreamforce To You 2020 | Sandbox Best Practices for Developers

ドメイン	Salesforce
コントロールID	**APP06 - セキュアな機能拡張**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	SalesforceはAppExchangeマーケットプレイスで利用可能なアプリケーションを用いたり、APEXを用いたカスタム開発により大幅に機能拡張することができます。 AppExchangeマーケットプレイスで提供されるアプリケーションは、セキュリティレビューに合格しなければなりません。このレビューは自動化されていますが、Salesforceはパートナーが手動テストを実施することも提案しており、これは、AppExchangeで提供されているアプリケーションがSalesforceプラットフォームと同じセキュリティ基準を満たしていることを暗黙に意味するものでないことを示しています。自動化されたレビューだけでは、手動で実施するのが適切なセキュリティチェックが行われていない可能性があります。例えば、設計ミス、論理エラー、法的要件を満たしていない等が想定されます。 同様にSalesforce利用者は、カスタムAPEXコーディングを使用するときに、セキュア開発のベストプラクティスが満たされていることを確認しなければなりません。
チェックリスト／優先順位に基づくステップ	1. セキュアな開発、およびコーディングガイドライン文書を作成し実施すること。 2. 全ての開発された成果物のための必須となるレビュープロセスを含むセキュアなソフトウェア開発ライフサイクルを確立すること。 3. 全てのソフトウェア開発では、バージョン管理システムを用いること。 4. 外部アプリケーションの場合、セキュリティとコンプライアンス要件が満たされていることを確認するためのリスクアセスメントを実施しなければならない。 5. 外部アプリケーション導入には、常に管理者権限が必要となる。権限は、最小権限の原則に従い導入後に適切に設定すること。

リファレンス

- Salesforce ISVforce Guide | How Does AppExchange Security Review Work?
- Salesforce Apex Developer Guide | Apex Security and Sharing
- Salesforce Apex Developer Guide | Security Tips for Apex and Visualforce Development
- Salesforce Trailblazer Community | Monitor Setup Changes with Setup Audit Trail

ドメイン	Salesforce
コントロールID	**INT01 - セキュアな統合と アプリケーションプログラミングインターフェイス**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceを外部アプリケーションやデータソースと広範囲に統合することは、これらのシステムがサポートするプロセスの性質上、よく行われています。 一般的なSalesforce環境では、異なるソリューションや異なる環境間のインターフェースや接続が存在します。セキュリティが不適切な場合、これらの統合は悪用されやすく、本番環境の情報やデータのリスクが容易に損なわれる可能性があります。 Salesforceインタフェースの管理では、以下のような点を考慮する必要があります: 1. 資産管理 2. すべてのインタフェースの継続的なセキュリティモニタリング
チェックリスト／優先順位に基づくステップ	1. 交換されるデータの種類や、プロトコル、ユーザ、ビジネスオーナー、権限、暗号化の詳細など、接続の技術的な詳細を含む、すべてのインタフェースのインベントリを維持します。 2. インタフェースのセキュリティ監視のための継続的なプロセスを設定します。 • 幅広く信頼し合える関係や他人が利用できるユーザ名やパスワードを使用するような、セキュアではないプロビジョニングのインタフェースを使用しないようにしてください。ベストプラクティスは、各インタフェースに1つのテクニカルユーザアカウント（サービスアカウント）を割り当てることです。

	• 最小権限の原則を常に適用し、さまざまなインタフェースでテクニカルユーザに付与される特権を定義します。 • インタフェースを経由するすべての通信を暗号化します。 • 開発システムに永続的な認証情報やアクセストークンがある場合は、セキュリティの低いシステム（開発システム等）からセキュリティの高いシステム（本番システム等）へのインタフェースを確立すべきではありません。 • インタフェースの設定にシークレットが使用されている場合（API鍵、パスワード、証明書など）、それらのシークレットを管理するための適切な管理プロセスを確立します（必要に応じて維持／変更／ローテーションします）。 • 使われなくなったインタフェースや統合を検出し、削除します。
 リファレンス	• Center for Internet Security | The 18 CIS Controls • Salesforce Integration Patterns and Practices | Integration Patterns Overview

ドメイン	Salesforce
コントロールID	**DAT01 - 継続的な監視**
テクノロジースタック	継続的な監視
バージョン	すべて
コントロールの実装	複数のアプリケーションやサービスが複雑に絡み合ったバンドルがSalesforceで提供されています。Salesforce内で起こっていることを理解するためには、さまざまなログプロバイダを分析し、ライセンスを取得する必要があります。これらのソースを効果的に活用するためには、セキュリティ情報およびイベント管理（SIEM）システムに供給される必要があります。アラートを設定し、インシデント対応プロセスで処理する必要があります。 さらに、トランザクションセキュリティポリシーを利用して、緊急ユーザがログオンしたときなど、特定の条件が満たされたときにアラートを実行することができます。可能であれば、リアルタイムイベントをインターセプトし、適切なアクションを適用するようにポリシーを構成してください（下記「トランザクション・セキュリティの強化」を参照）。
チェックリスト／優先順位に基づくステップ	1. アプリケーションのロギングと監査を有効にすること。以下のイベントを対象にする必要があります： • アクセスおよび失敗したログインは、「ログイン履歴」に最大6ヶ月間記録されます。イベントマネージャで保存を有効にすると、さらにログインフォレンジックが可能になります。さらに、ログアウトイベントは、イベントマネージャを使用して追跡することができます（以下「リアルタイムイベントモニタリング」および「イベントモニタリングの有効化」を参照）。 • メタデータの設定変更は、「設定変更履歴」で追跡されます。サインオン監査が「フォームレベル」に設定されていることを確認し、ユーザーがどのprofessional formにアクセスしたかを追跡し、記録します。また、このログが集中ログソリューションに転送されていることを確認してください。

2. アプリケーションのロギングと監査を有効にすること。以下のイベントを対象とします：

    - 追加のトランザクションログは、別途ライセンスを取得すれば利用可能です。以下、イベントタイプを提供しています（詳細は、下記「リアルタイムイベントモニタリング データストリーミングとストレージ」を参照）：
        - API Anomaly Event
        - API Event
        - Bulk API Result Event
        - Concurrent Long Running Apex Error Event
        - Credential Stuffing Event
        - Identity Provider Event
        - Identity Verification Event
        - Lightning URI Event
        - List View Event
        - Login Event
        - LoginAs Event
        - Logout Event
        - Report Anomaly Event
        - Report Event
        - Session Hijacking Event
        - URI Event

3. 個々のビジネスログの要件については、リストに定義されたSalesforceおよびカスタムオブジェクトに対する変更を追跡し、項目履歴管理を評価する必要があります。
4. すべてのログが転送される集中型ロギングソリューションを使用する必要があります。
5. 可能であればSIEMツールを使用して、ログを自動的に確認するプロセスを導入し、タイムリーな対応を可能にする。
6. インシデント対応プロセスを導入し、インシデントが確認された場合、適切なチームがインシデントの抑制に関与します。

リファレンス

- Salesforce Trailblazer Community | Enable Login Forensics
- Salesforce Trailblazer Community | Monitor Setup Changes with Setup Audit Trail
- Salesforce Trailblazer Community | Field History Tracking
- Salesforce Trailblazer Community | Enhanced Transaction Security
- Salesforce Trailblazer Community | Real-Time Event Monitoring
- Salesforce Trailblazer Community | Enable Event Monitoring
- Salesforce Trailblazer Community | Real-Time Event Monitoring Data Streaming
- Salesforce Trailblazer Community | Real-Time Event Monitoring Data Storage

ドメイン	Salesforce
コントロールID	**DAT02 - データ分離**
テクノロジースタック	データベース
バージョン	すべて
コントロールの実装	Salesforceの実装はサンドボックス、開発、品質保証、本番といった多様な役割をもった複数の環境で構成されています。環境全体のセキュリティは、本番システムでホストされているデータのセキュリティにとって最も重要です。 同様に、組織には、いかなる場所にデータが存在する場合においてもデータを保護する受託者責任が存在します。 一般的に、開発用などのリスクの低い環境へのアクセスによって、機微データが危険にさらされてはなりません。つまり、可能な限り（異なるアクセス制御を行い）本番環境と非本番環境を分離し、非本番環境の機密情報がマスキング、スクランブル、リダクテッドなどにより適切に保護されていない限り、これらの環境も同じレベルと基準で保護するべきです。
チェックリスト／優先順位に基づくステップ	1. 本番データは、いかなる場所に存在する場合であっても法的に保護されなければなりません。本番データを非本番システムにコピーする場合、データは本番システムと同様に扱われ、保護されなければなりません。カスタムソリューションは、PIIデータのマスキング、スクランブル、またはリダクションにも使用できます。例：すべての個人データがテストシステムにコピーされ、このテストシステムは本番システムと同様に扱われます。 データ分類は、Salesforceの項目に機微レベルを割り当てるために使用することができます。これは、ユーザのデータへのアクセスレベルや、データを本番環境からサンドボックス環境に移行する前のマスキング戦略に関する意思決定の指針となります（以下の参考文献を参照）。

2. テスト、開発、サポートなどの目的で本番環境のコピーを作成する場合、コピーされた本番環境ですべてのユーザアカウントを変更または無効とすべきです。
3. テスト環境でのみ使用する責任（ロール）は、本番環境では無効としなければなりません。サポートや開発用のロールは、一般的に、本番環境で許されないほど、広範な権限で作られます。
4. 本番環境と非本番環境間のインタフェースは存在すべきではありません。インタフェースはケースバイケースの検証の際に使用することが可能で、その場合には全てのコンプライアンス要件を満たさなければなりません（例：暗号化と最小権限の原則）。インタフェースは本番環境から非本番環境の方向（データのプッシュ）に限って使用すべきで、非本番環境から本番環境の方向（データのプル）には行うべきではありません。

リファレンス

- Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies
- Salesforce Security Guide | Give Users Access to Data
- Salesforce Trailblazer Community | Secure Your Sandbox Data with Salesforce Data Mask

ドメイン	Salesforce
コントロールID	**DAT03 - データの暗号化**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceによって保存され処理されるビジネスデータは極めて重要なコンポーネントです。既定のルールとポリシーによれば、保存された機微な情報は、暗号化され、認可されないアクセスを防ぐために分類されなければなりません。 Salesforce Shieldは、プラットフォームの暗号化、完全なイベントモニタリング、データ変更を追跡する項目の監査を含む、データ保護の追加レイヤを提供します。金融機関やヘルスケア企業のように機微な情報を扱う企業では、Shieldがコンプライアンス要件を満たすかどうかを確認するために検証することが望まれます。 ビジネスデータについては、保存中または他の場所に保管している場合とも、データ分類に基づいて暗号化すべきです。
チェックリスト／優先順位に基づくステップ	1. 全てのビジネスデータは分類され、所有者が指定されていなければなりません（参照：下記の参考情報にあるClassify Sensitive Data） 2. データは企業のコンプライアンス要件に従って暗号化すべきです。
リファレンス	• Salesforce | Salesforce Shield • Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies • Salesforce Trailhead | Secure Your Apps with Salesforce Shield • Salesforce Trailblazer Community | Strengthen Your Data's Security with Shield Platform Encryption

ドメイン	Salesforce Business Processes
コントロールID	**BUS01 - ビジネス資産、データ、プロセスのインベントリ**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceアプリケーションに保存され、処理されるビジネスデータの保護は、ビジネスアプリケーションを大規模に運用する上で最も困難な部分の一つです。各アプリケーションがサポートしているデータとプロセスを適切なレベルで可視化することが重要です。これらのコンポーネントの明確なインベントリを持つことは、組織のどこに重要な資産（crown jewels）があるかを理解し、それらのコンポーネントに適切なガバナンスとコントロールを提供するための出発点となります。 アプリケーション、データ、およびプロセスのインベントリは、ビジネスプロセスに関する信頼できる唯一の情報源として機能するよう実装される必要があります。
チェックリスト／優先順位に基づくステップ	1. ITIL構成管理データベース（CMDB）のような、信頼できる唯一の情報源（インベントリ／リポジトリ）が存在することを確認します。 2. 本番および本番以外のSalesforce環境を構成、サポートする全ての技術とコンポーネントを特定し、徹底的に文書化する。Service Cloud、Marketing　Cloud等のその他アプリケーションとの重要な関係を盛り込みます。 3. 全てSalesforceアプリケーションとサポートする技術に対してサービスレベルアグリーメントが定義されていることを確認します。 4. 各Salesforce環境について、機密データ保護要件を含むリスク管理スコアカードが利用可能であることを確認します（以下参照先の「Classify Sensitive Data」を参照）。
リファレンス	• ISO 27001:2013 | A.8.1 - Asset Management • Salesforce Trailblazer Community | Classify Sensitive Data to Support Data Management Policies

ドメイン	Salesforce Business Processes
コントロールID	**BUS02 – ビジネスプロセスコントロール**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforce は重要なビジネスプロセスをサポートします。 既存の権限や昇格した特権を悪用した不正行為が実行されないためにコントロールが導入されなければなりません。
チェックリスト／優先順位に基づくステップ	1. ビジネスプロセスオーナーと共に、Salesforce内の各重要なビジネスプロセスにおける重要なステップを特定する必要があります。 2. 各プロセスについて、組織の不正防止プログラムのすべての要件を満たす必要があります。
リファレンス	該当なし

ドメイン	Salesforce Business Processes
コントロールID	**BUS03 - 継続的なコンプライアンス**
テクノロジースタック	アプリケーション
バージョン	すべて
コントロールの実装	Salesforceがサポートするデータやプロセスの性質上、データやプロセスに適用される規制や、組織が属する業界の規制に対して、一定のコンプライアンスレベルを維持することが重要です。 継続的なコンプライアンスを確実にし、集中化された視野で、コントロールの有効性をリアルタイムに監視するプロセスを実装します。 さらに、Salesforceが提供するサービスのセキュリティやコンプラアンスに関する、Salesforceの公式ドキュメントを参照し、コンプライアンスコントロールのフレームワークに組み込むべきです（参考資料の、Certifications, Standards, and RegulationsとTrust and Compliance Documentationを参照）。
チェックリスト／優先順位に基づくステップ	1. Salesforceのアプリケーションに影響する、すべてのコンプライアンス、規制基準、および、契約による合意事項を特定する必要があります。 2. 必須とされる重要なコントロールを特定する必要があります。 3. 監査を含む、ガバナンスフレームワークを確立する必要があります。 4. コントロールの有効性を24時間365日評価できる、自動化されたテスト手順を確立すべきです。 5. 検出時にすぐに対応するため、アラート通知のメカニズムを実装すべきです。
リファレンス	• Salesforce | Certifications, Standards and Regulations • Salesforce | Trust and Compliance Documentation • Wikipedia | Continuous Monitoring • Wikipedia | Continuous Auditing • Wikipedia | Regulatory Compliance