



## **SAPセキュリティ & コントロールサービス** **SAP Security & Control Services**

# SAPセキュリティ & コントロール サービス

## システム導入・更改を契機としたアプリケーションインテグリティ環境の実現

### 企業を取り巻く環境の変化

企業を取り巻く環境は大きな変化を遂げており、脅威やリスクも日々高度化・多様化しています。グローバル対応、クラウド化、RPA等による自動化、ビッグデータを活用したアナリティクス導入、AI導入等、SAP導入・更改プロジェクトの難易度が上がってきている状況です。このような中、SAPシステム導入・更改プロジェクトにおいては、ガバナンス強化を目的とした統制機能の構築が求められており、アプリケーションシステムのインテグリティ環境を構築することが不可欠となっています

### アプリケーションインテグリティ環境とは

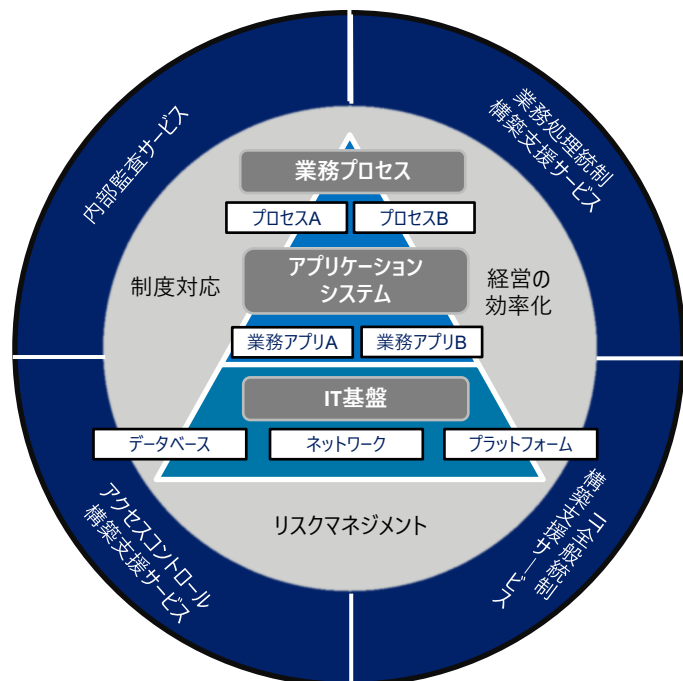
アプリケーションインテグリティ環境とは、国内外の法規制対応を踏まえ、システムセキュリティとシステム統制機能を統合的に構築することで、データに対する改竄やエラーによる誤りを防いだうえで、システムのデータを信頼することができる環境のことです

この環境下では、財務データや機微情報等の重要なデータを保護し、企業内外に正しい情報を継続的に提供することが可能になります

### アプリケーションインテグリティ環境の実現で達成できること

- ・情報セキュリティ、ガバナンス、内部統制に関する法令遵守
- ・不正・誤謬に対するリスクの軽減
- ・信頼性の高い経営管理データによる迅速な経営判断
- ・非効率な業務の改善

上記のような環境の変更に 대응すべく、アプリケーションインテグリティ環境の構築に向けて4つの領域でサービスを提供します



### アプリケーションインテグリティ環境構築に向けたサービス一覧

#### 1. 業務処理統制構築支援サービス

業務プロセスに係る内部統制を対象に、マニュアルコントロールやITコントロールの導入を支援します

#### 2. IT全般統制構築支援サービス

アプリケーションシステムのベース領域を対象に、コントロールの導入を支援します

#### 3. アクセスコントロール構築支援サービス

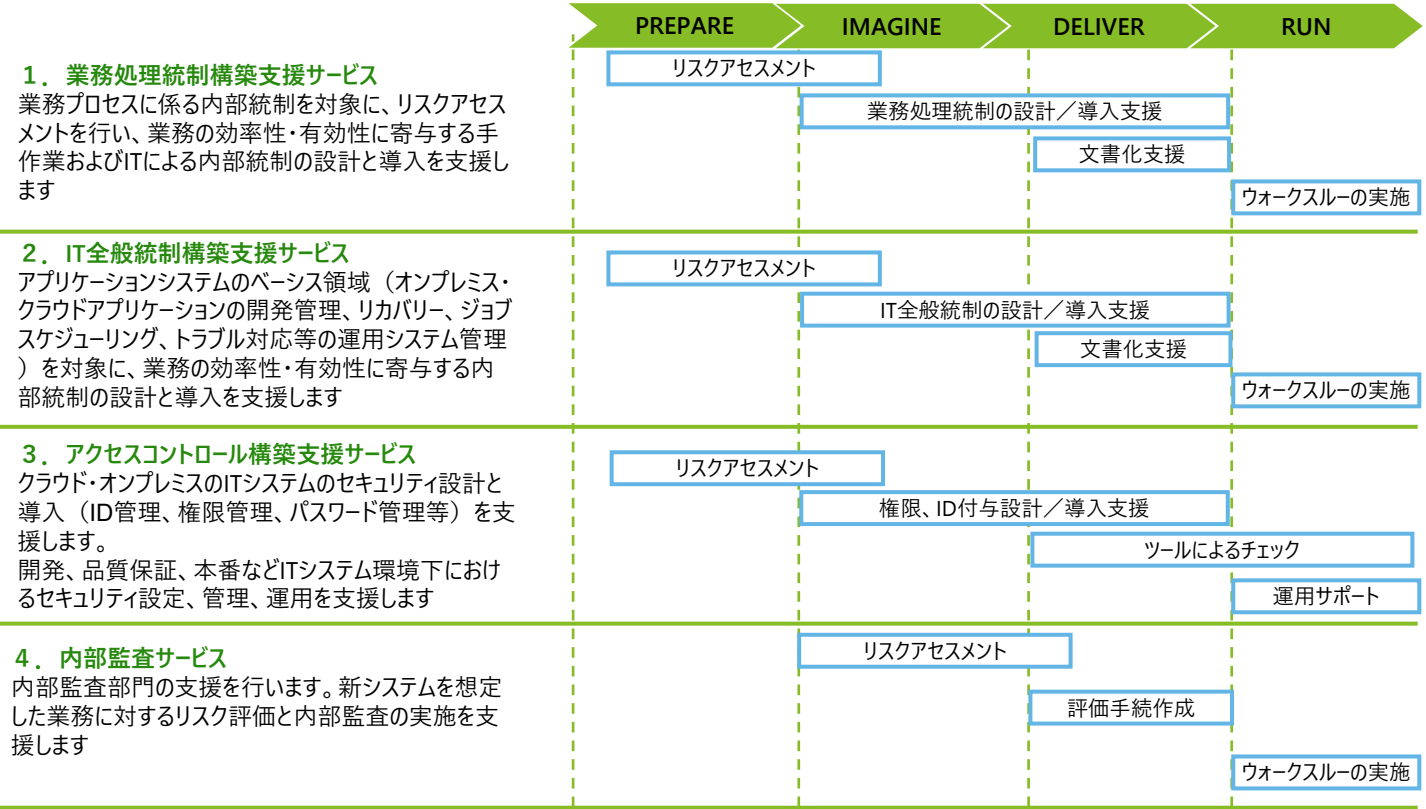
職務分掌を考慮したアクセスコントロールの導入を支援します

#### 4. 内部監査サービス

新システムにおける内部監査を支援します

**トーマツが提供するサービス**

システム導入・更改プロジェクトのフェーズである「PREPARE」「IMAGINE」「DELIVER」「RUN」それぞれに対して、デロイトの方法論を基に支援を行います



**トーマツの強み**

**① J-SOX対応の専門知見**

**J-SOX対応に関し監査法人の知見を活用したアプローチを有しています**

アプローチを活用した、効果的・効率的な構築・文書案作成を立案・実施いたします

「トーマツ内部統制報告制度対応アプローチ」「タスクリスト」

**② テクノロジーフレームワークの活用**

**デロイトの知見を集約した、IT全般統制の標準化された評価の枠組みであるテクノロジーフレームワークを有しています**

テクノロジー毎のリスク対応のリーディングプラクティスに基づいた評価手法であり、実質的なリスク領域を識別することで監査品質を向上し、標準化された手続きを実施することができます

典型的な発見事項

- 不要なユーザーIDが存在する
- 承認もしくは必要ないアクセス権が存在する
- 業務上不要となる、過大な権限が付与されている
- 適切な職務分離(SoD)が維持されていない
- パスワードが定期的に変更されないまたは、書面で管理に書面されない
- アクセスが適切にモニタリングされていない

**③ 内部統制高度化の知見**

**内部統制の高度化に多くの知見を有しています**

内部統制文書の整備、評価の過程で発見した内部統制の課題「リスクのある統制処理」「非効率/効率化の余地のある統制」「電子化の可能性」「効果的な評価」等余地がある点について、課題提起が可能です

代表的な発見事項と会社に求められる対応

発見事項	会社に求められる対応
全ての権限が実行できる権限が一般ユーザを含めたユーザに付与されている 開発検証のためのデバッグ権限が本番環境で一般ユーザに付与されている 本番環境において、プログラムを直接作成・変更を可能な設定となっている 毎週のアップデートの日付形式パスワードが変更されておらず、不正にログインされる可能性のある状態である	【暫定的対応】 ・権限過剰なユーザが存在する場合は、実際のログの抽出と監査人の監視 ・セキュリティ上リスクの高い設定値になっている場合、リスクが顕在化していないことを裏付けのログの抽出と監査人への説明 【恒久的対応】 ・権限を修正するための検討、影響調査・テスト ・セキュリティ設定を標準化するための検討、影響調査・テスト
不備が発見された場合、実際のログの抽出・監査人への説明などの暫定的対応に加え、権限・設定値の適正化の検討、影響調査などの恒久的対応も必要、会社には多くの対応が求められます。	

※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

# Deloitte. トーマツ.

## デロイト トーマツ

デロイト トーマツグループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ リスク アドバイザリー 合同会社、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ グループ 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内約30都市に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト、[www.deloitte.com/jp](http://www.deloitte.com/jp) をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。

デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オークランド、バンコク、北京、ベンガール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をバース（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、[www.deloitte.com](http://www.deloitte.com) をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（DTTL）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生し得る損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of  
**Deloitte Touche Tohmatsu Limited**

© 2025. For information, contact Deloitte Tohmatsu Group.



ISO 669126 / ISO 27001



BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください  
<http://www.bsigroup.com/clientDirectory>