

攻撃を排除し、正しくユーザーを認証・監視 - Oracle Cloudのセキュリティ・サービスの概要 -

日本オラクル株式会社
クラウド事業戦略統括
クラウドソリューション推進本部

井坂源樹

Oracle Corporation
Product Strategy Director
JAPAC

Julien Lehmann

Modern Cloud Day Tokyo

次世代クラウドが変える日本のビジネス

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。

アジェンダ

- 1 Oracle Cloud 東京リージョンがお届けする価値
- 2 Oracle Cloud Infrastructure WAFのご紹介
- 3 Oracle Identity Cloud Serviceのご紹介
- 4 デモンストレーション
- 5 最後に

Oracle Cloud 東京リージョンがお届けする価値

性能

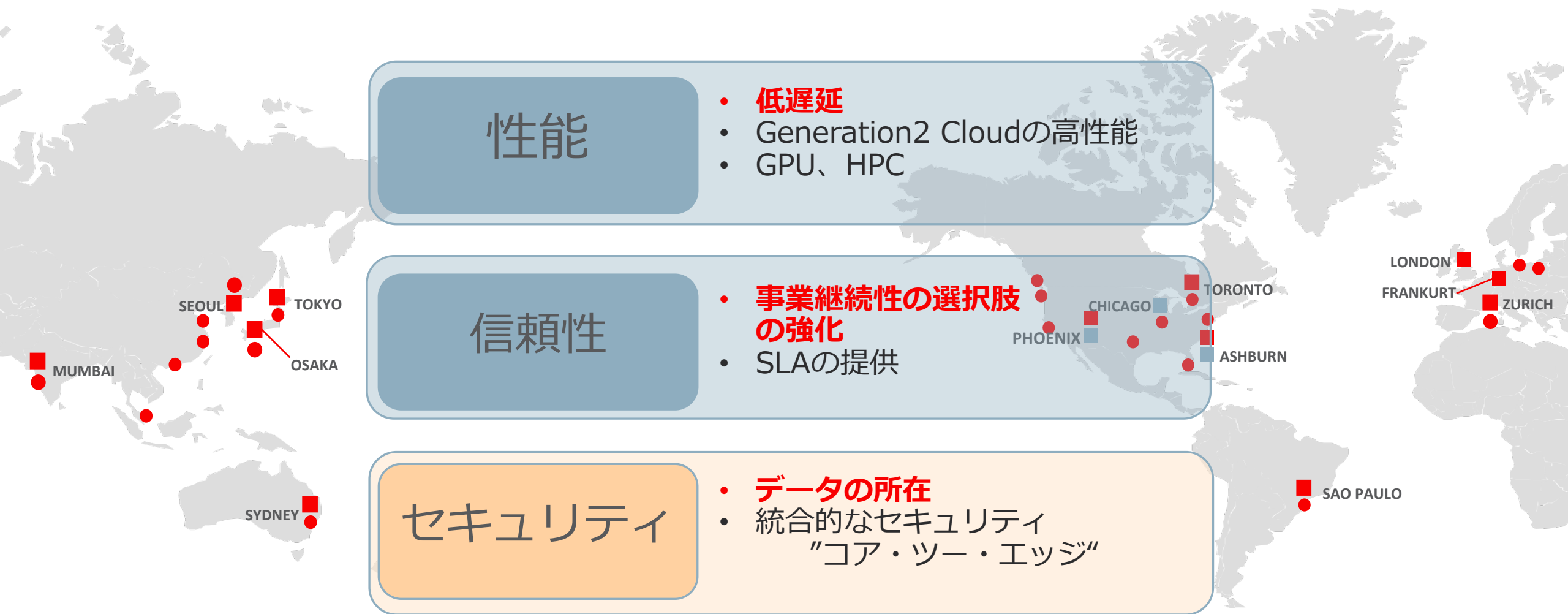
- **低遅延**
- Generation2 Cloudの高性能
- GPU、HPC

信頼性

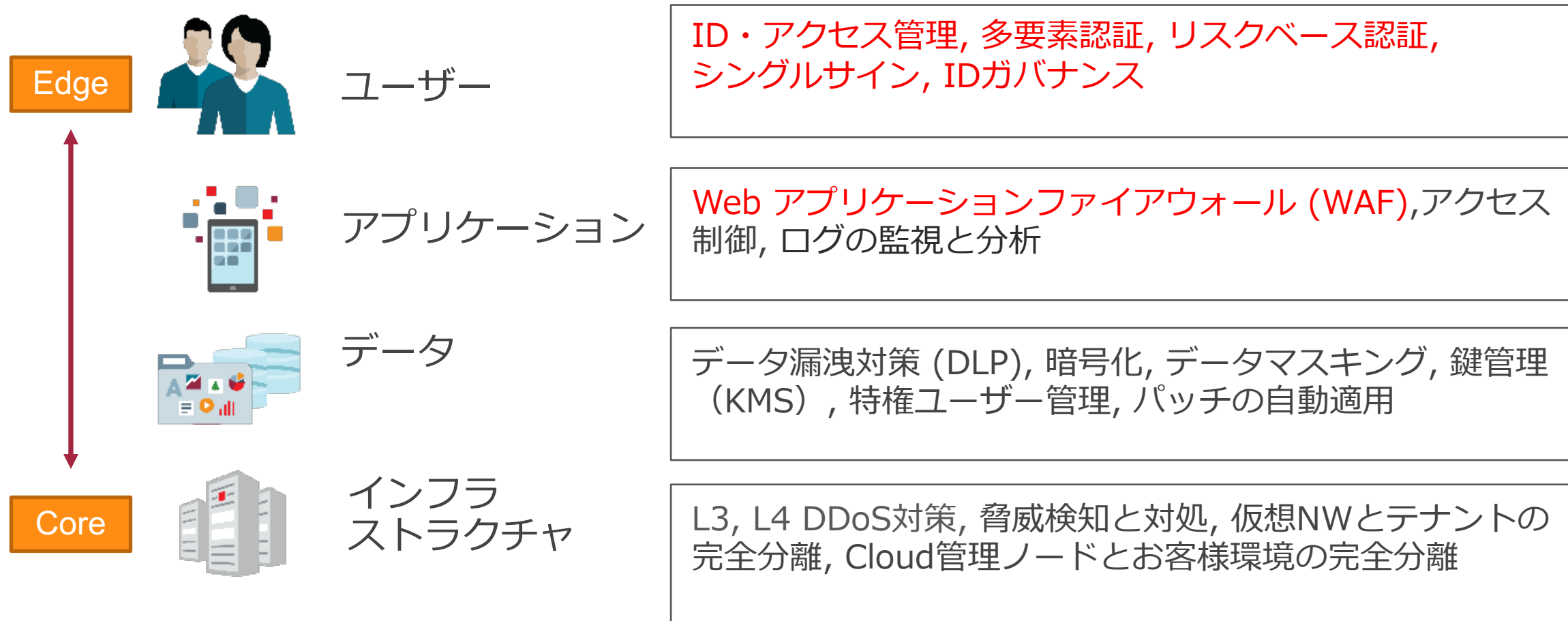
- **事業継続性の選択肢の強化**
- SLAの提供

セキュリティ

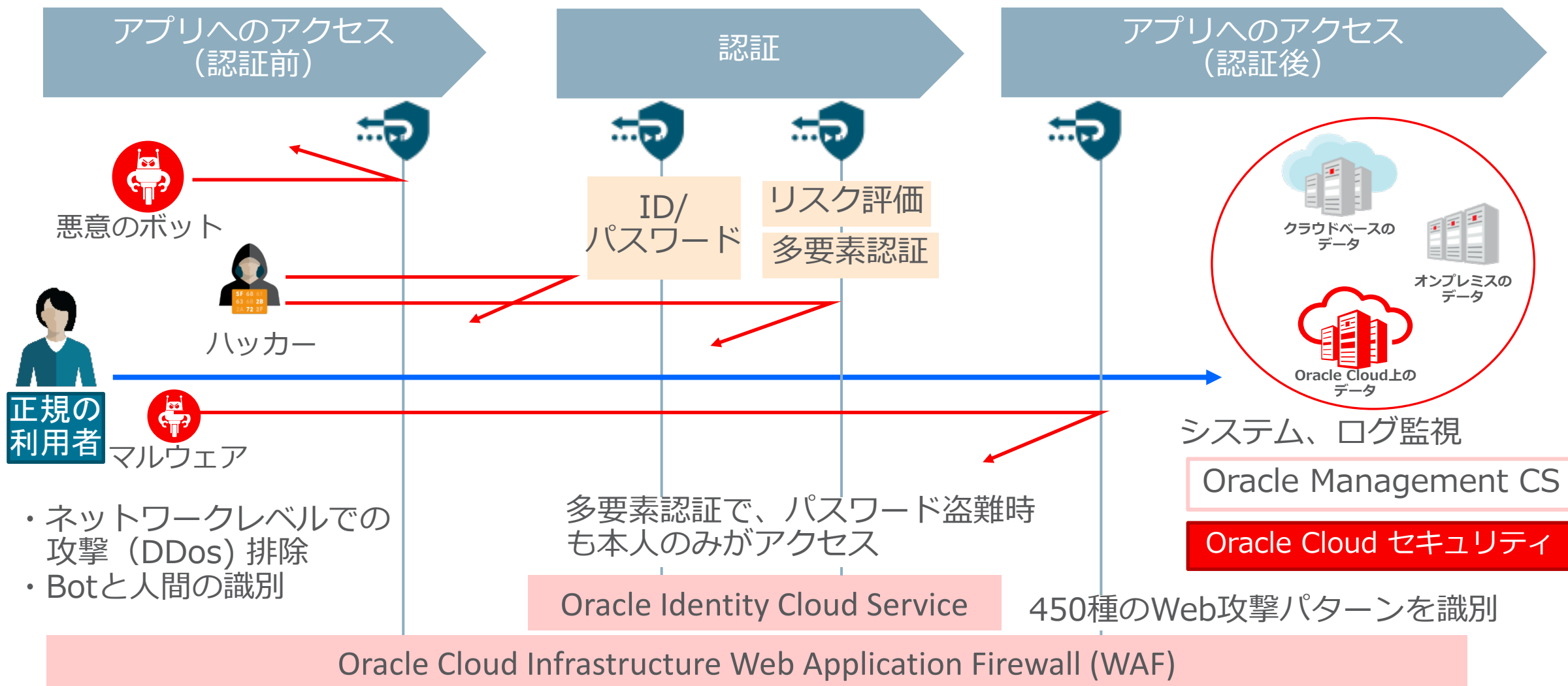
- **データの所在**
- 統合的なセキュリティ
"コア・ツー・エッジ"



Oracle Cloudのセキュリティ : Core-to-Edge Security



セッションでお伝えする事： ユーザーを中心としたセキュリティ



アジェンダ

- 1 Oracle Cloud 東京リージョンがお届けする価値
- 2 Oracle Cloud Infrastructure WAFのご紹介**
- 3 Oracle Identity Cloud Serviceのご紹介
- 4 デモンストレーション
- 5 Oracle Management Cloudのご紹介
- 6 最後に

Oracle Cloud Infrastructure Web Application Firewall (WAF)

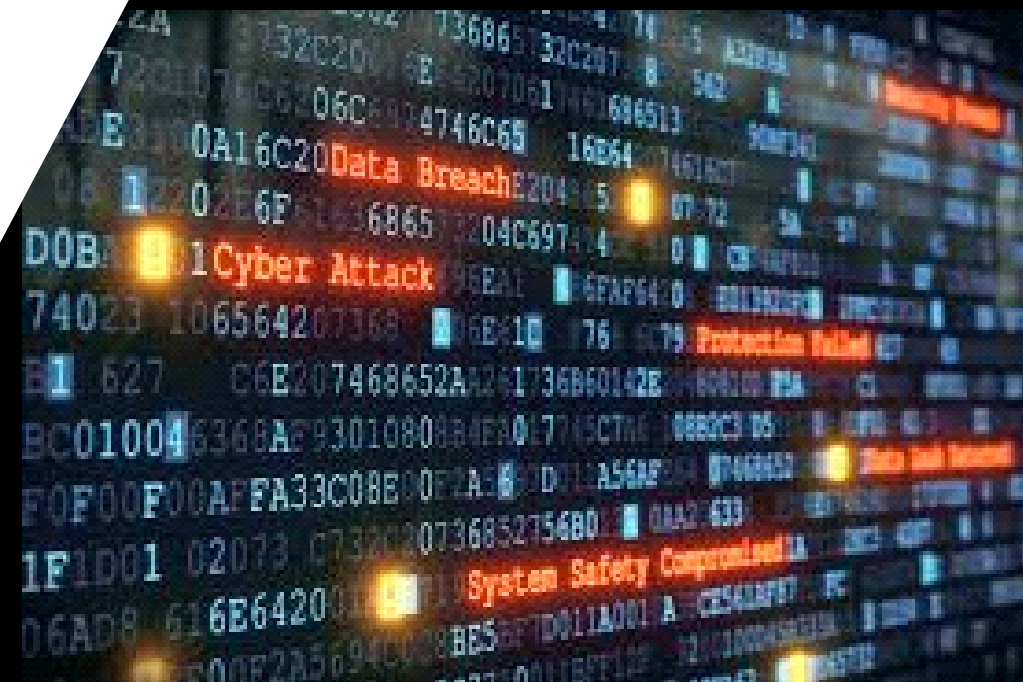
- クラウド型のWeb Application Firewall

- 任意のサイトを保護可能

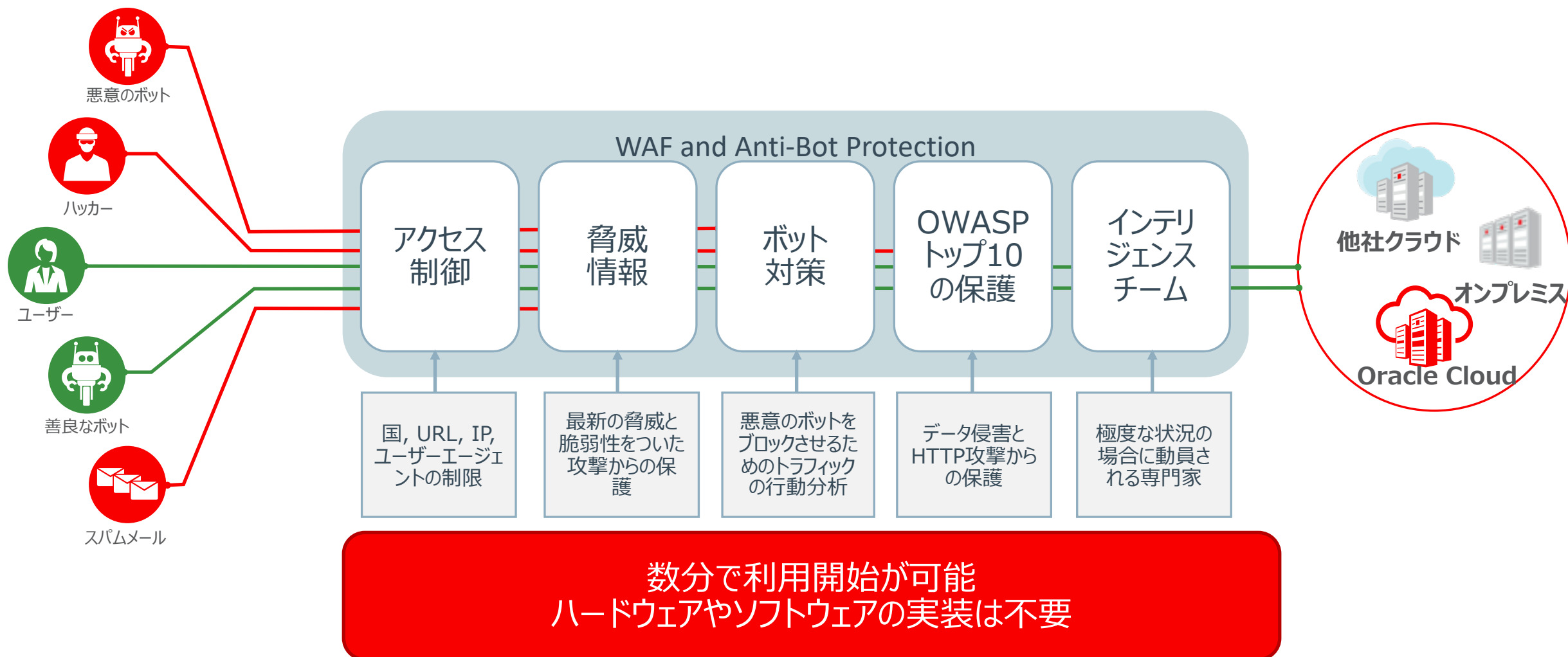
- マルチ・クラウド
- オンプレミス環境

- フルマネージド・サービス

- WAFインスタンスの作成などは不要
- 保護ルールの設定のみで利用可能

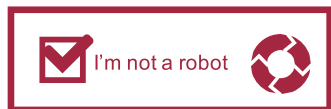


Oracle OCI WAFの機能イメージ

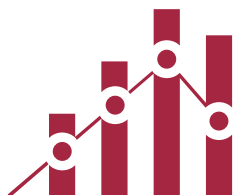


ボット攻撃の軽減策

第1世代



CAPTCHA チャレンジ



IPレート制限

第2世代



JavaScript チャレンジ



善良なボットのホワイトリスト

第3世代 – 現在



ヒューマン・インタラク
ション・チャレンジ



デバイス
フィンガープリント



高度なIPレート制限

プラットフォーム



マネージド
サービス



アクセス
コントロール



脅威情報



WAF/
アプリケーション
DDoS

始めてみましょう。

クラウド型のWAFならではの、利用までの簡潔なステップ

Step1

WAFの作成
(新規ポリシーの追加)

- ・外部公開URIの登録
- ・オリジン・サーバーURI
の登録

※VMやLBの作成は不要

Step2

DNSへの登録

WAFが生成する
CNAMEをお客様が
ご利用のDNSプロ
バイダに登録

Step3

保護ポリシーの設定

アクセスルール

ボット・マネージメント

- CAPCHA
- JavaScript Challenge
- Human Interaction

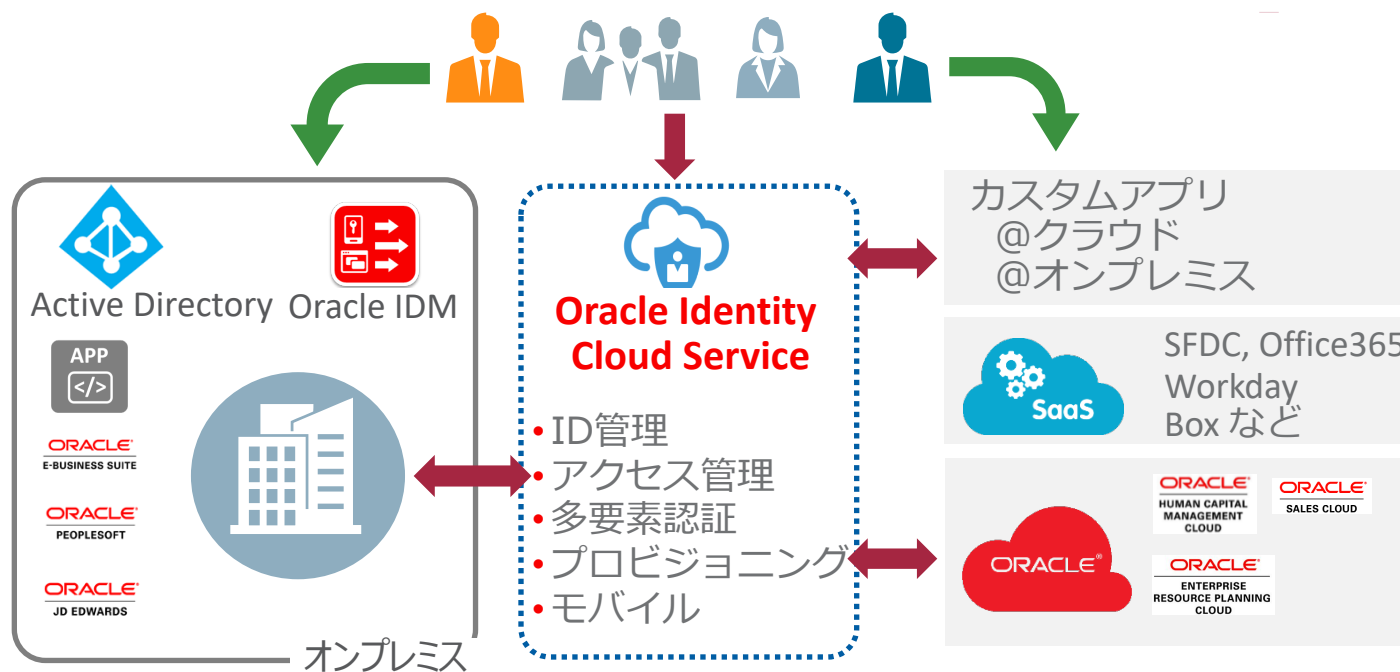
WAFルール

-推奨される保護の
有効化

アジェンダ

- 1 Oracle Cloud 東京リージョンがお届けする価値
- 2 Oracle Cloud Infrastructure WAFのご紹介
- 3 Oracle Identity Cloud Serviceのご紹介**
- 4 デモンストレーション
- 5 最後に

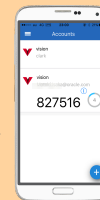
Oracle Identity Cloud Serviceの概要



SAML, OAuth2.0, OpenID Connect, SCIMなど
標準技術・標準規格を採用

標準プロトコルによる認証

- OpenID Connect、OAuth 2.0、SAML
- 各サービスはIDCSに対して認証することでシングルサインオンを実現
- Eメール、SMSを用いたワンタイムパスワードや、iPhone、Android等のモバイルアプリを提供



フルマネージド・サービス

- Oracle側でインスタンスを提供し、バージョンアップ、パッチ適用、バックアップをOracle側で実施
- SaaS型のサービスとしてご利用可能

開発柔軟性

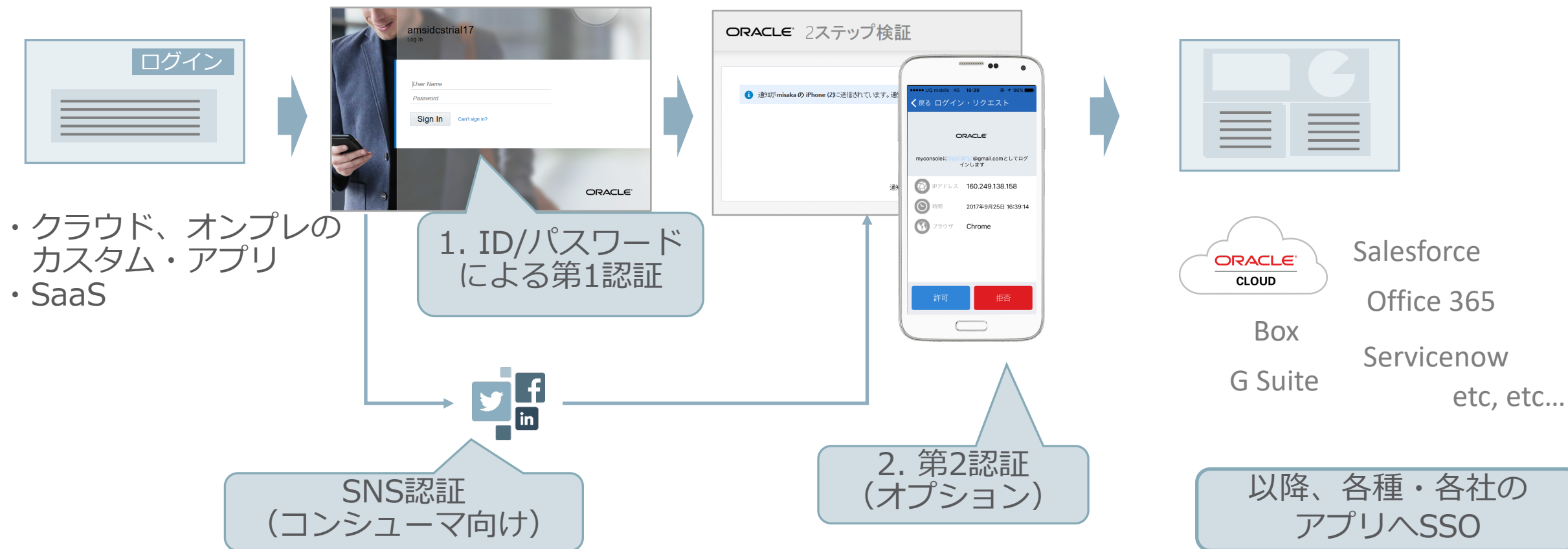
- 自由なデザインのログイン画面の開発が可能
- 要件に応じた管理画面、バッチプログラムの開発が可能

Oracle IDCSによる認証とSSOのイメージ

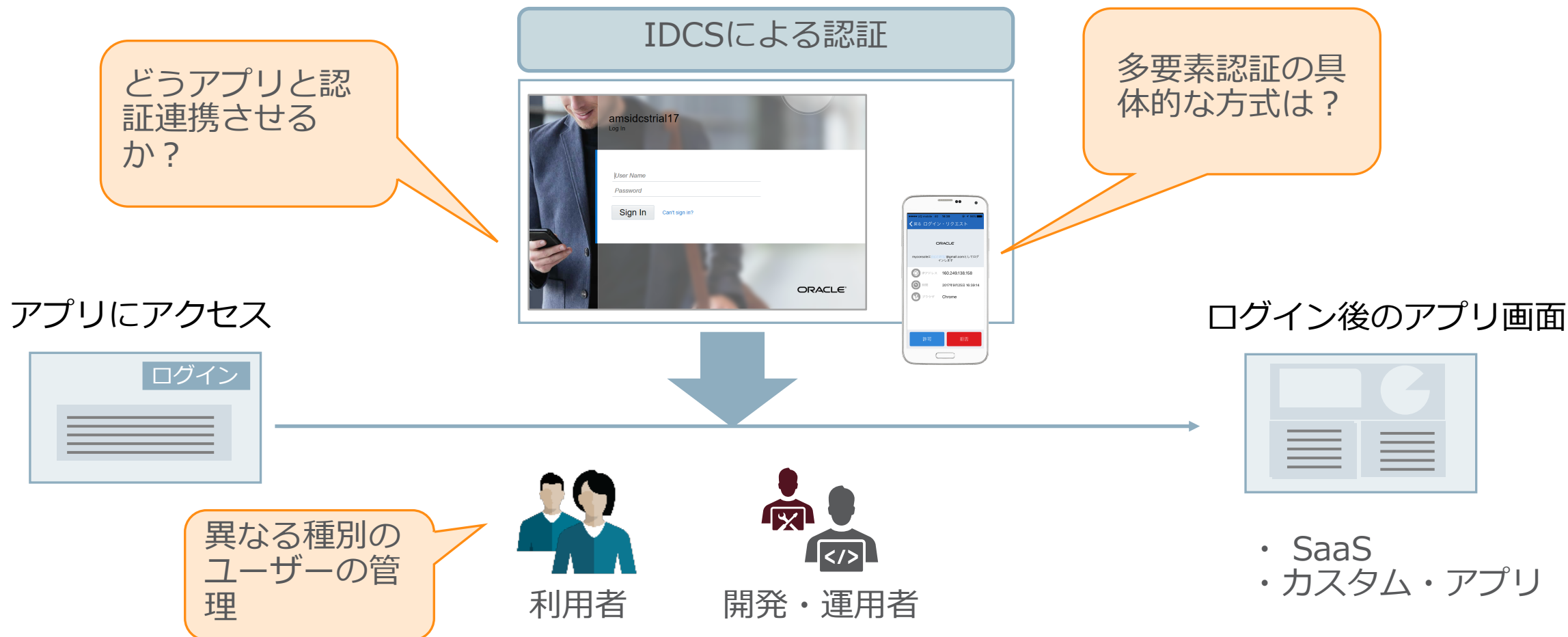
アプリにアクセス

IDCSによる認証

アプリにログイン



IDCSとの認証連携と多要素認証方式？



IDCSとの認証連携と多要素認証方式？



IDCSの提供する多様な連携方式の提供

(1) 標準フェデレーション・プロトコルによる連携

- ・ SAML 2.0
- ・ OpenID Connect 1.0, OAuth 2.0

(2) リバースプロキシ型認証

- ・ IDCS専用リバースプロキシ・サーバー

(3) Oracle Access Manager WebGateによる認証連携

- ・ 認証エージェントのOpenID Connect対応

(4) Oracle E-Business Suite用認証モジュール

EBSとの認証連携モジュールEBS Asserterを提供

・ SaaS

- ・ APサーバーのフェデレーション機能
例： WebLogic、
Java Cloud Service (JCS)

・ カスタム・アプリ

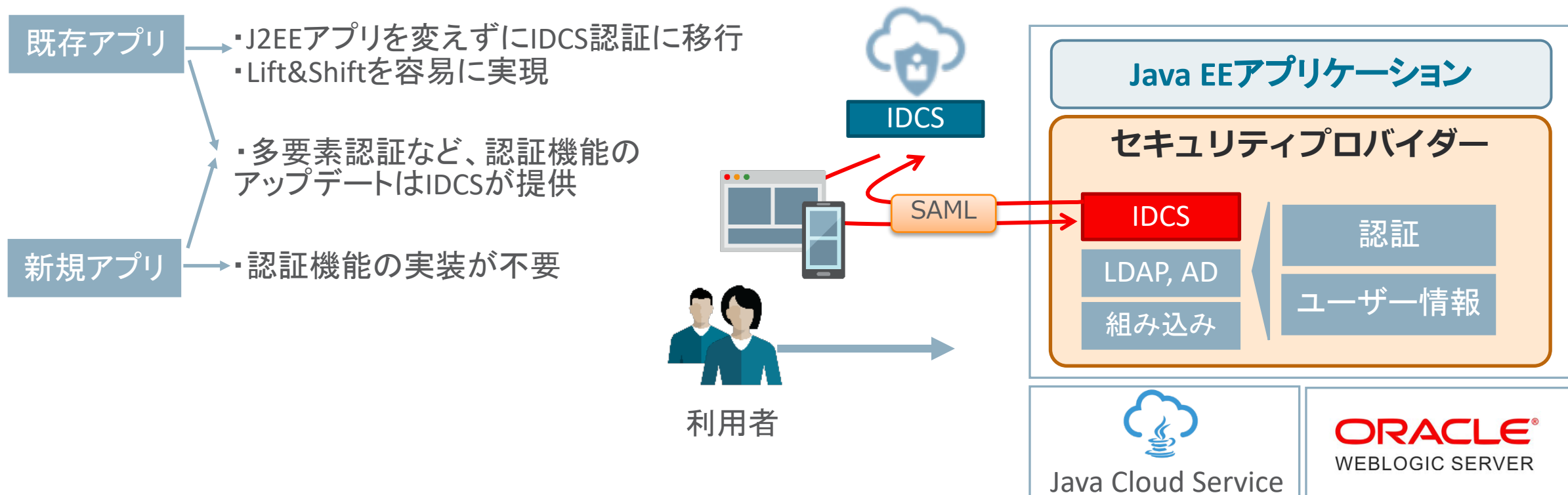
- ・ オンプレのアプリ
- ・ Lift&Shiftでクラウド移行したアプリ

- ・ すでにOracle製品をお使いのお客様向け
- ・ 認証モジュールのIDCS対応化により、
IDCSへ認証移行

WebLogic/Java Cloud ServiceアプリのIDCS認証

WebLogic/JCSのアプリの改修なしで、認証をIDCSに移行

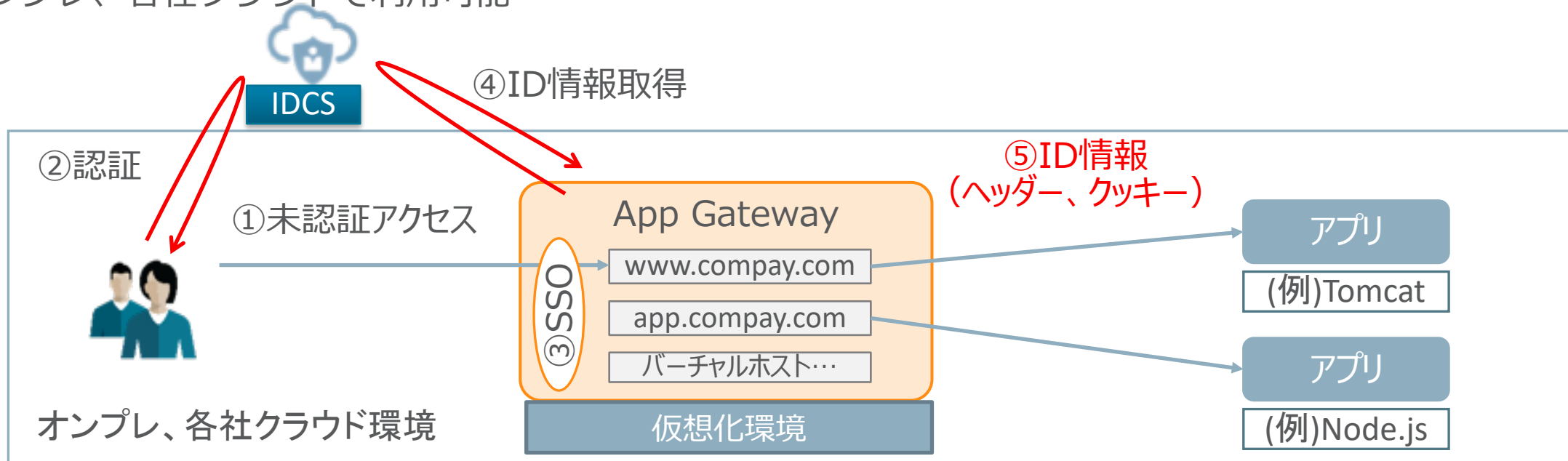
- WebLogic/JCSの標準セキュリティフレームワークがIDCSに対応済み
 - IDCSへの接続定義のみで、IDCSにより認証とIDCSで管理されるユーザー情報が取得可能



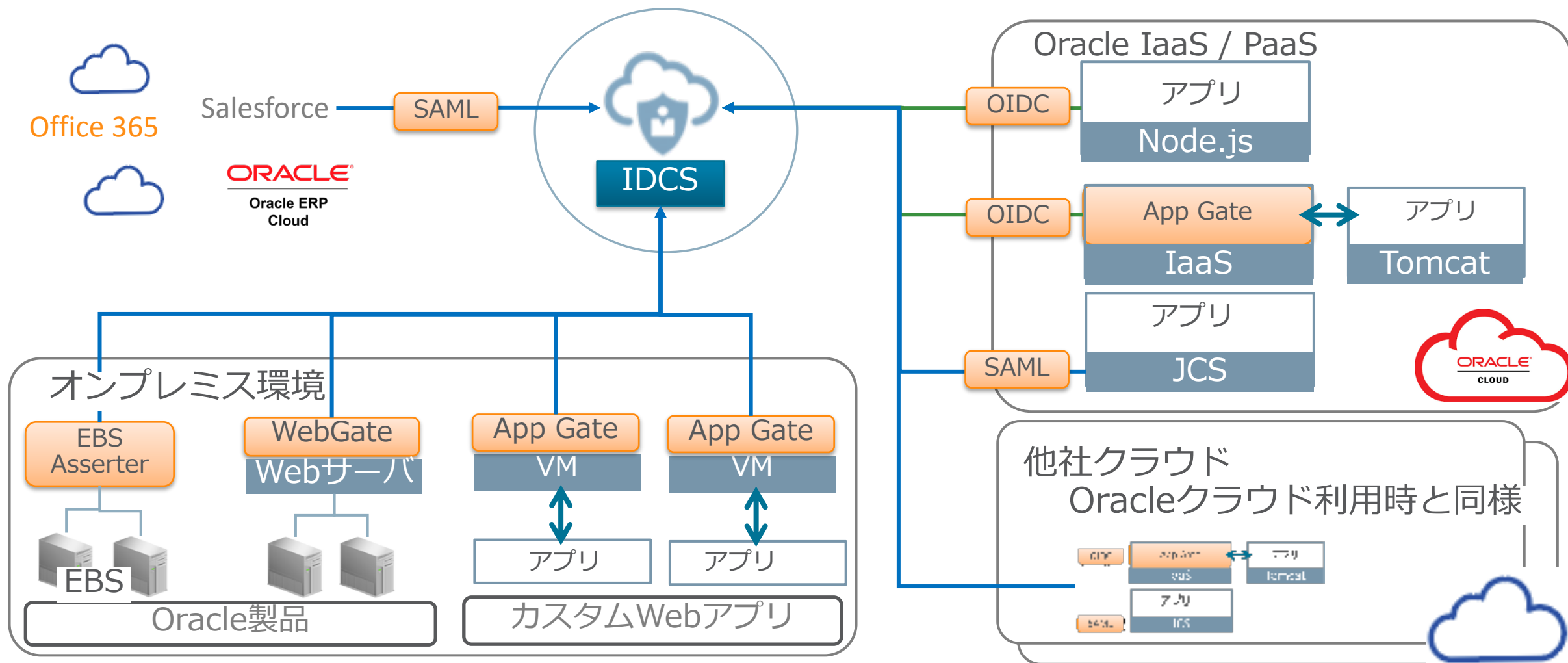
認証ゲートウェイによる連携

最小限の改修で任意のアプリケーションをIDCSと認証連携

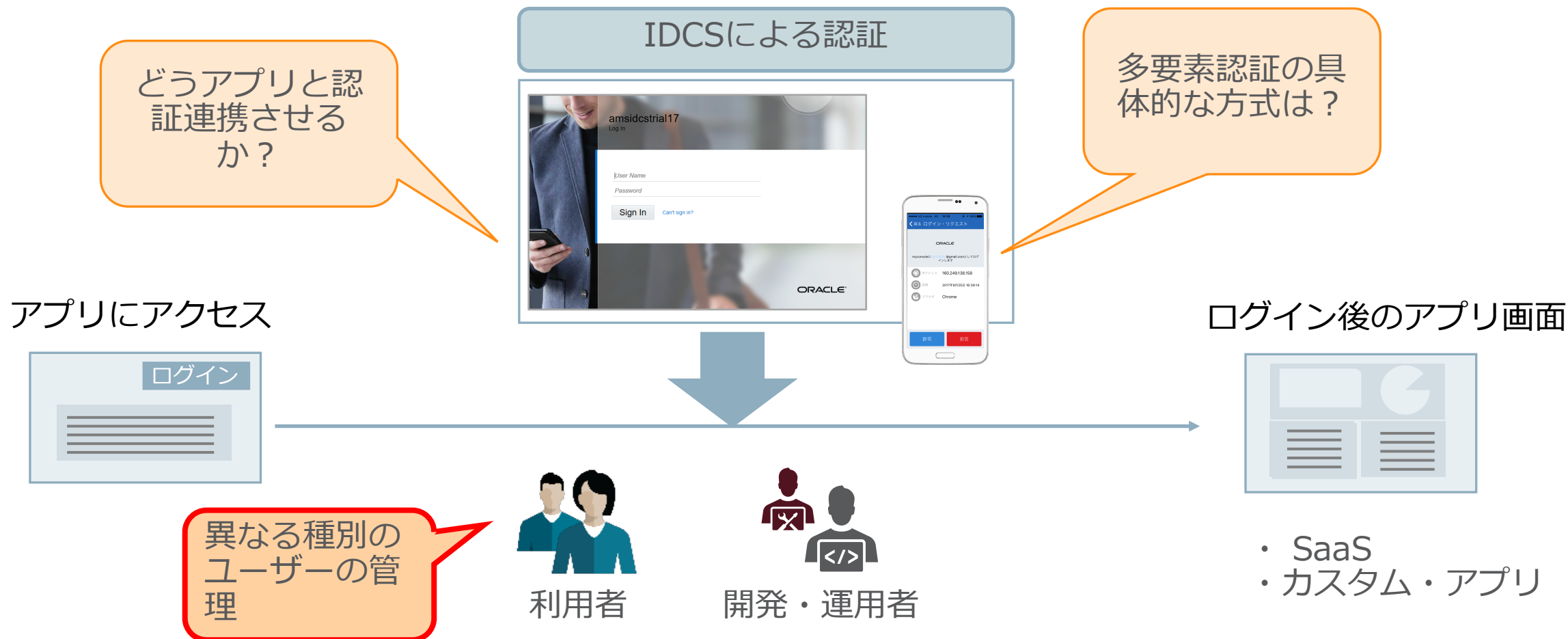
- IDCS専用の認証リバースプロキシ (App Gateway)を提供
 - セッションを管理し、ユーザー認証はIDCSで実施
- 任意のアプリケーション・サーバーとの組み合わせが可能
- オンプレ、各社クラウドで利用可能



ハイブリッド、マルチクラウド利用時の認証統合

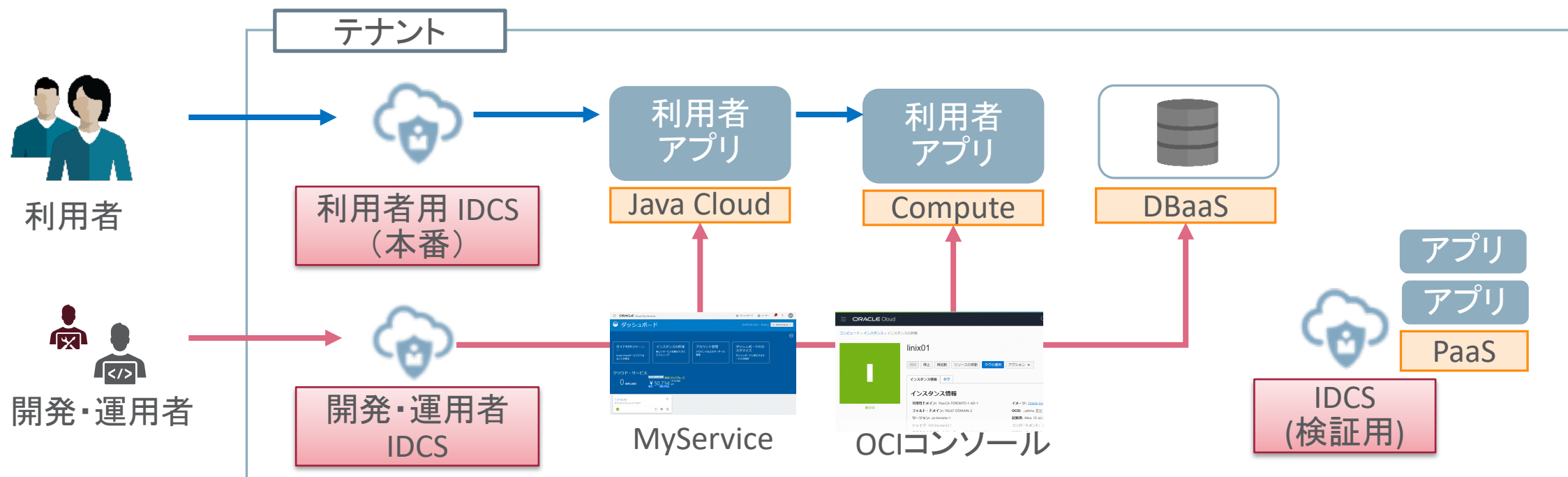


IDCSとの認証連携と多要素認証方式？

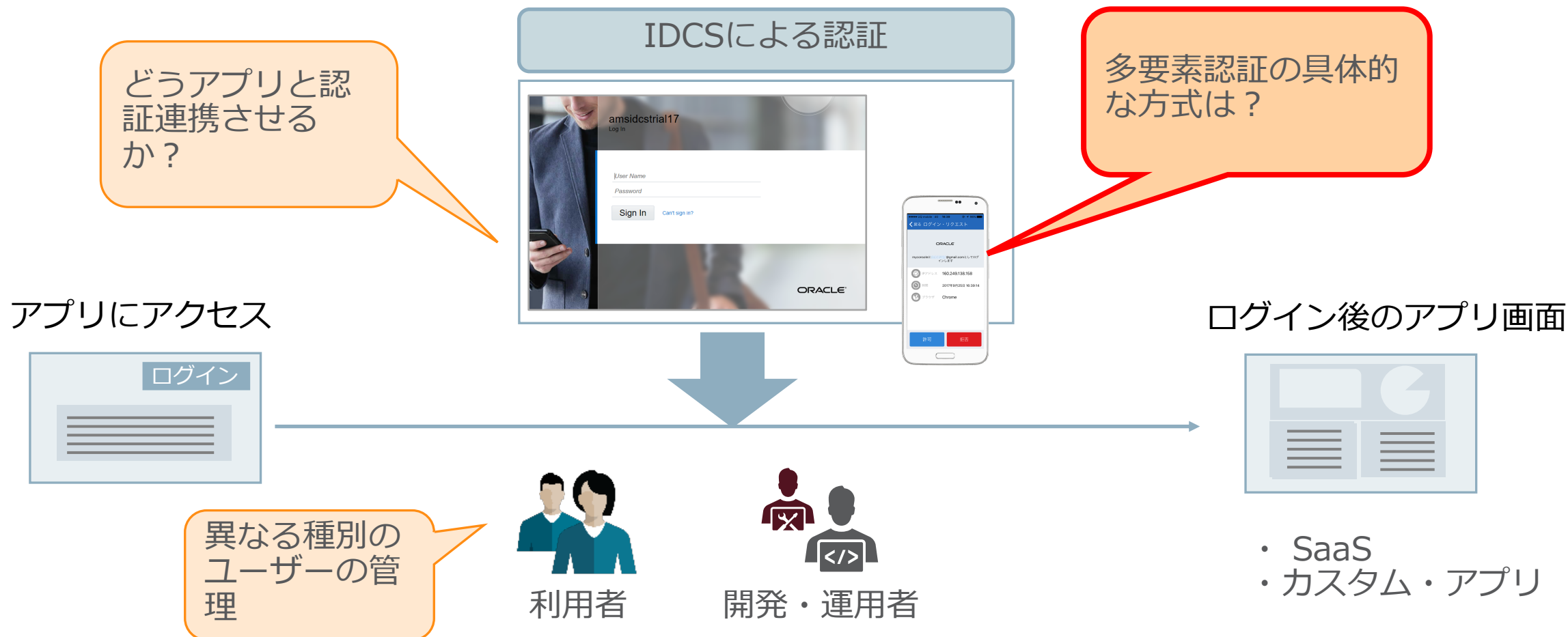


Oracle Cloudの管理者認証とアプリ・ユーザーの認証

- 独立したIDCSのインスタンスの作成が可能
 - Oracle Cloudの管理者の認証機能としてのIDCS（プライマリ・インスタンス）
 - エンド・ユーザーを管理し、認証するセカンダリ・インスタンス
 - 複数インスタンスを作成することで追加の課金なし（全体の登録ユーザー数で課金）



IDCSとの認証連携と多要素認証方式？



Oracle Cloudが提供する多要素認証

- ルールベース（設定）で認証プロセスに導入
 - アプリケーション、ユーザー・グループ、アクセス元ネットワーク
 - ログイン済み端末
 - 管理者 or 利用者
 - リスク・スコア

ワンタイムパスワード
SMS通知



ワンタイム・パスワード
モバイル・アプリ



モバイル・アプリでの 通知への応答



ワンタイムパスワード
メール

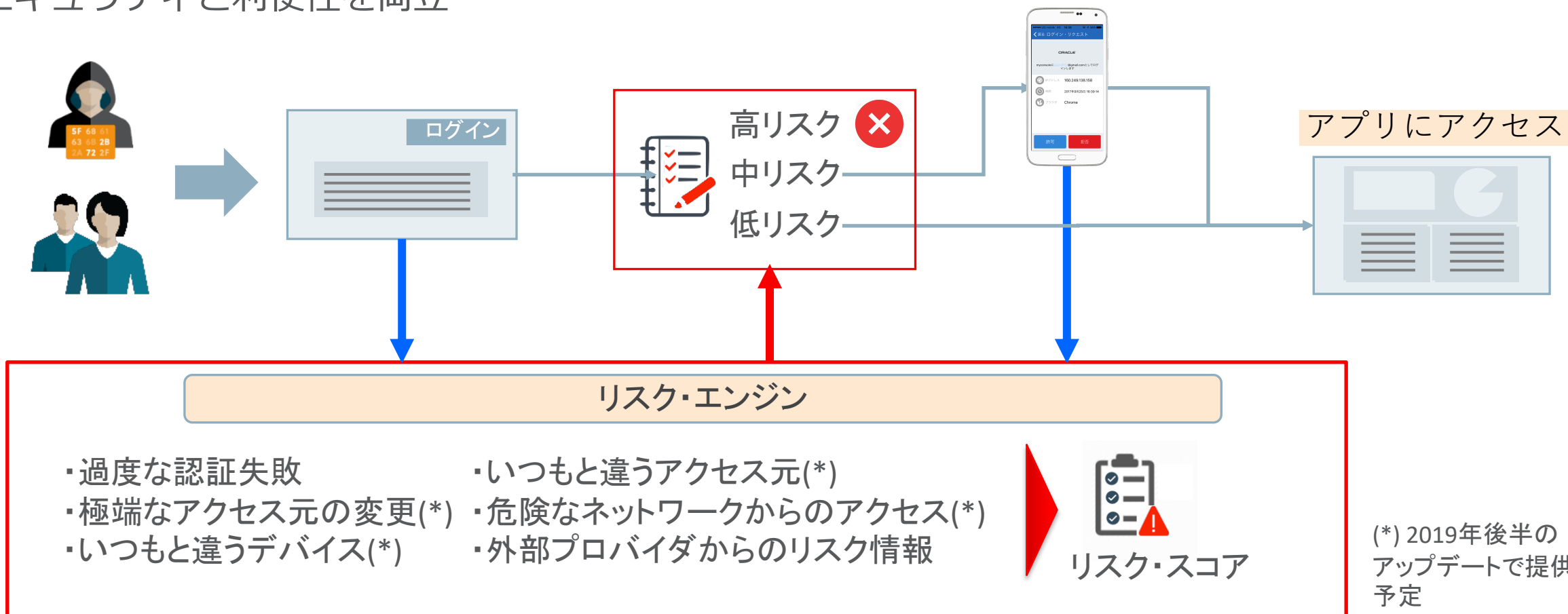


秘密の質問



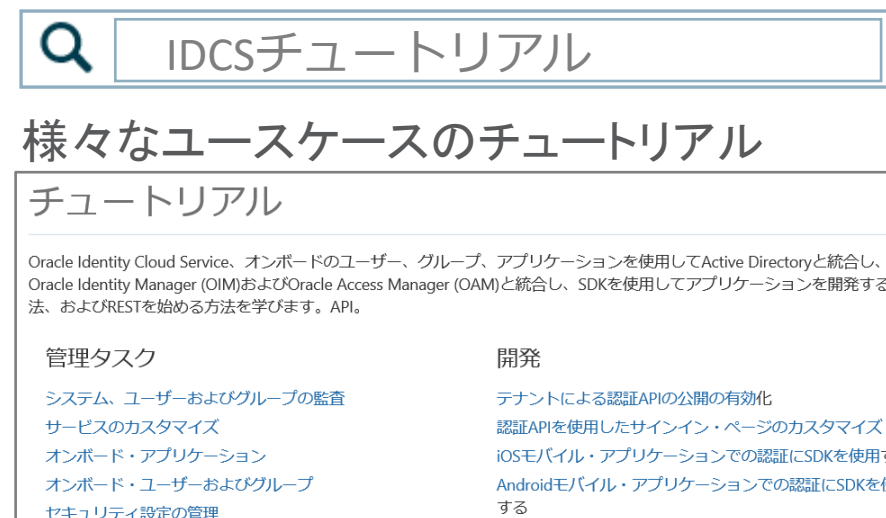
リスクベース認証 (Adaptive Security)

- アクセス条件、履歴を記録し、リスクをスコアリング。スコアに応じて認証、アクセスを制御
- セキュリティと利便性を両立



始めてみましょう。




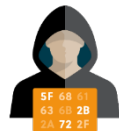
- Oracle Cloudの無料トライアルですぐ体験
 - Oracle IaaS (OCI)、PaaSの認証基盤はIDCS
 - Oracle Cloudのログインで多要素認証を体験
- IDCSを技術的に調査したい
 - カスタム・アプリとの連携方法？
 - OpenID、OpenIDってよく聞くけど？



アジェンダ

- 1 Oracle Cloud 東京リージョンがお届けする価値
- 2 Oracle Cloud Infrastructure WAFのご紹介
- 3 Oracle Identity Cloud Serviceのご紹介
- 4 デモンストレーション**
- 5 最後に

デモ内容のご紹介

1. 利用者 IDCS を利用したアプリケーションへのアクセス 
2. 管理者 IDCS 認証ポリシー設定方法 
3. 管理者 WAF 保護ポリシーの設定方法 
4. 管理者 アプリケーション攻撃のシミュレーション 

Julien Lehmann

オラクル・コーポレーション
シニア・プロダクトストラテジー・ディレクター

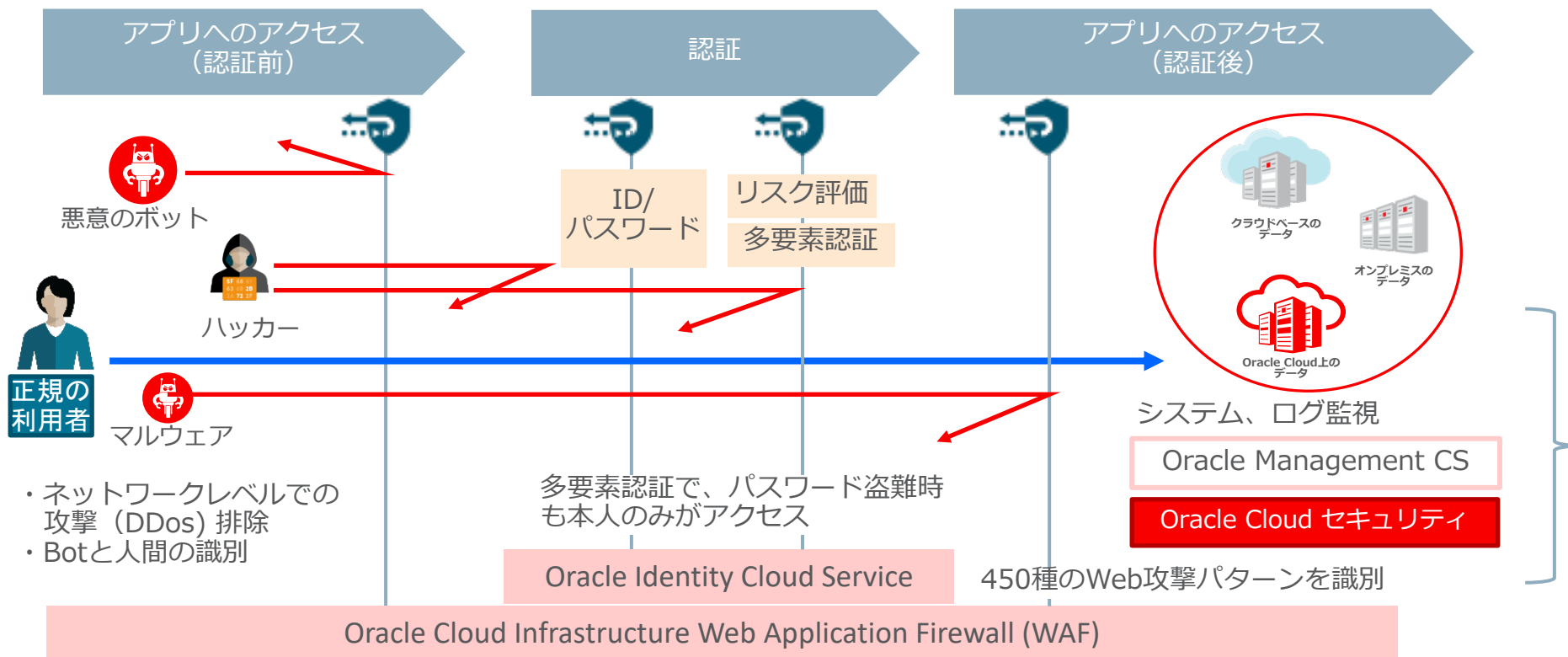
オラクル本社でOracle Cloudのセキュリティースペシャリストとして活動中。

アジェンダ

- 1 Oracle Cloud 東京リージョンがお届けする価値
- 2 Oracle Cloud Infrastructure WAFのご紹介
- 3 Oracle Identity Cloud Serviceのご紹介
- 4 デモンストレーション
- 5 最後に

最後に

- ユーザーを中心としたセキュリティと外部に対するセキュリティをご紹介
 - Oracle Identity Cloud Service
 - Oracle Cloud Infrastructure Web Application Firewall (WAF)



クラウド・セキュリティ・アドバイザリー・ボードのご案内

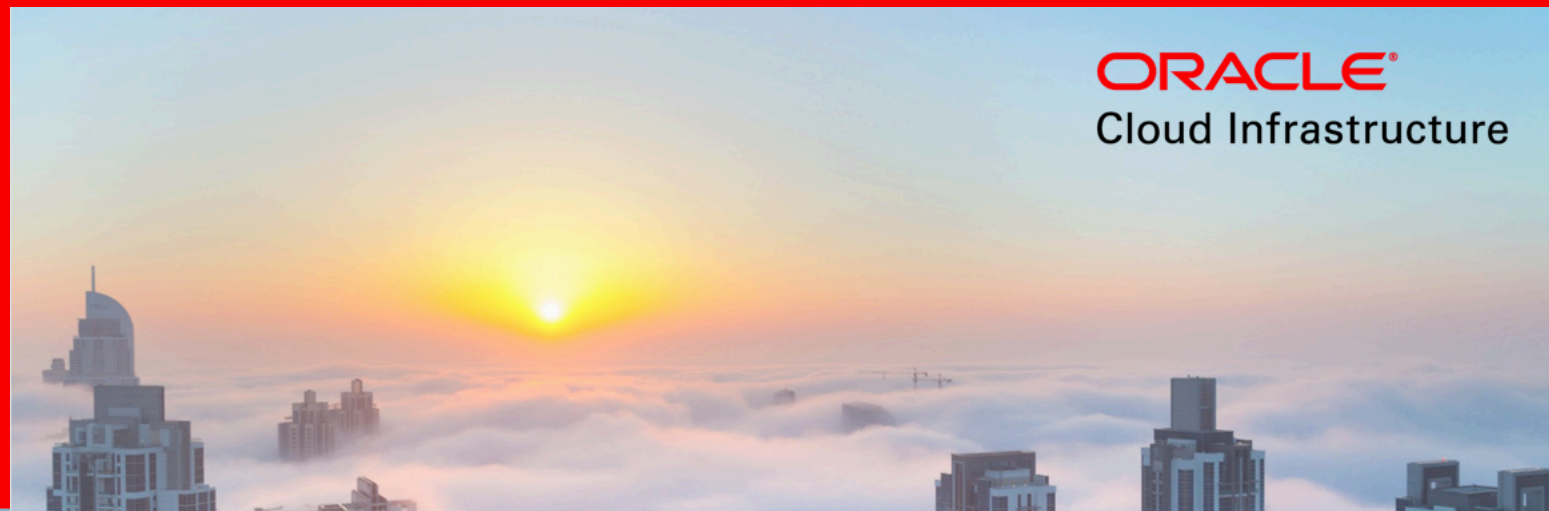
- Cloud Security Advisory Board for Japan -

- * 今後のクラウドセキュリティのあり方
- * セキュリティ・エキスパートとご参加されるお客様同士の意見交換
- * クラウド・セキュリティ施策の策定

お問合せ先:

Yuecel.Karabulut@oracle.com

Julien.Lehmann@oracle.com



関連する技術セッションのご紹介



ID・アクセス管理, 多要素認証, リスクベース認証,
シングルサイン, IDガバナンス



Web アプリケーションファイアウォール (WAF),
アクセス制御, ログの監視と分析



データ漏洩対策 (DLP), 暗号化, データマスキング, 鍵管理 (KMS), 特権ユーザー管理, パッチの自動適用 (オンライン)



DDoS対策, 脅威検知と対処, 仮想NW分離, Cloud管理ノードとお客様環境の完全分離、コンプライアンス対応

E-2

本セッション

技術

ご聴講いただきありがとうございました。

明日
15:30-
16:15

[D-7] WAF創業者が語る。3つの事例からみる

技術

脅威の実態とその対策～ボット攻撃、DDoSとの戦い方

オラクルコーポレーション Laurent Gill

本日
16:30-
17:15

[D-4] ゼロから再設計したOracle Cloudの
データ保護戦略～7つの原則とその実装

技術

オラクルコーポレーション Johnny コンスタンス

こんな時、かけこむ会社が増えています。



ビジネスプロセスを
改善したい!



今のシステムは
使いにくい!



システムコストを
下げたい!



パフォーマンスを
良くしたい!



経営分析を
したいのだが...



どんなソリューションが
あるの?



見積りはどれくらい
なんだろう?



楽に管理を
したい!

Oracle Digitalは、オラクル製品の導入をご検討いただく際の総合窓口。
電話とインターネットによる直接的なコミュニケーションで、どんなお問い合わせにもすばやく対応します。
もちろん、無償。どんなことでも、ご相談ください。



お問い合わせは電話またはWebフォーム

☎ 0120-155-096

受付時間 月～金 9:00-12:00 / 13:00-17:00
(祝日および年末年始休業日を除きます)

<http://www.oracle.com/jp/contact-us>

ORACLE®