ORACLE

クラウドセキュリティのトレンドと求められる対策 ～ オラクルのセキュリティへの取り組み

2021年12月21日

日本オラクル株式会社
事業戦略統括 事業開発本部
大澤 清吾, CISSP

本日お伝えしたいこと

01 セキュリティ対策でのトレンドと日本が取り組むべき点

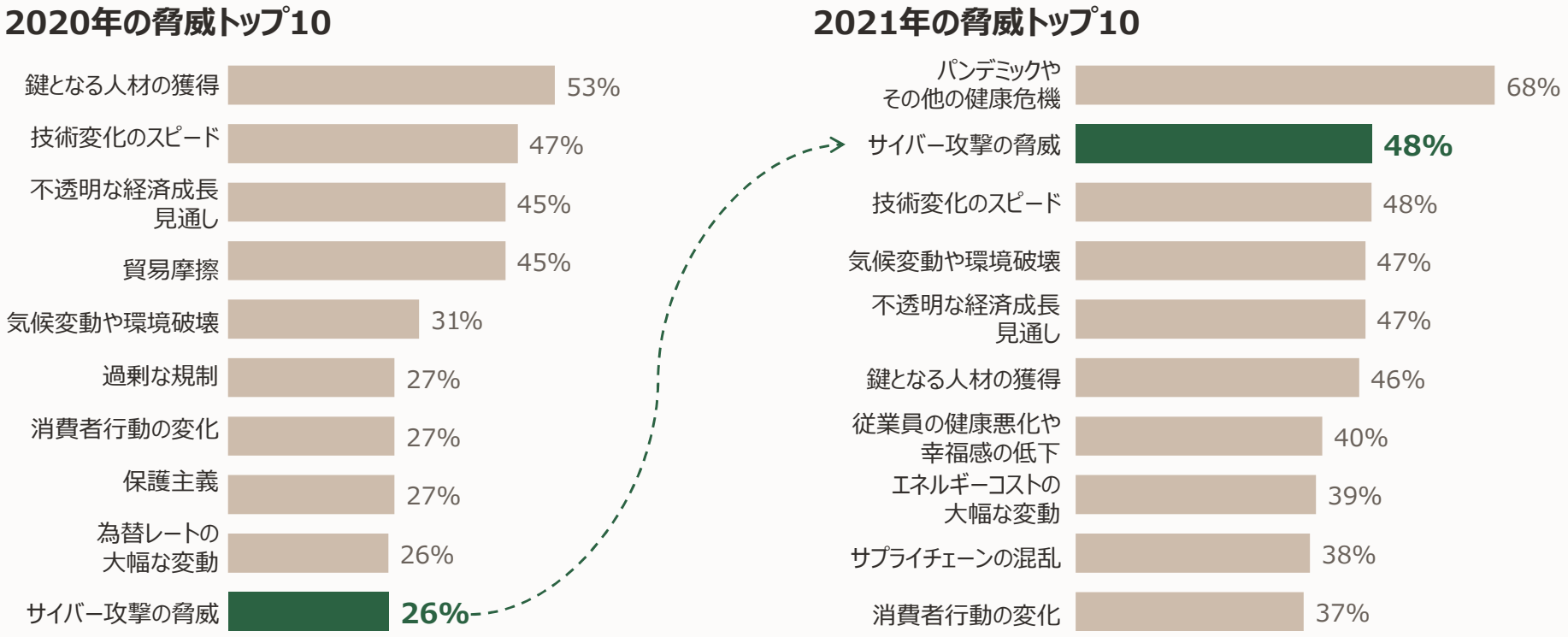
02 Oracle Cloud Infrastructureは、セキュリティは最初から組み込まれ常にオン。コンプライアンスも遵守

03 クラウドセキュリティで課題となる人的ミスを排除する自動化されたセキュリティ管理を提供

サイバー攻撃に対する経営者の懸念が高まっています

地政学的情勢が複雑化し、サイバー攻撃リスクが増大しています

貴社の成長見通しに対する潜在的な脅威（経済、政策、社会、環境、ビジネス）に関して、どの程度懸念していますか。
（「非常に懸念している」との回答のみを表示）



出所：PwC 第24回世界CEO意識調査

2020,21年：国内の情報漏洩事件(10万件以上 or 報道で大きく取り上げられたもの)

年	日付	法人・団体名	件数・人数	原因	境界防御で防げたか	漏洩内容
2021	11/30	パナソニック	詳細調査中	不正アクセス	×	同社のネットワークが不正にアクセスされ、侵入時にファイルサーバー上の一部のデータにアクセス
	11/4	ライトオン	24万7600件	不正アクセス		通販サイトへのサイバー攻撃により、同サイトと店舗会員24万7,600人分の個人情報が流出
	8/17	ニップン	詳細調査中	ランサムウェア	×	サーバー、端末が同時に暗号化され、システム起動が不可で早期復旧が困難だとして決算報告を延期
	8/6	警視庁	26万件	内部不正	×	特権IDで捜査や人事情報に不正アクセス。さらに上司のパソコンから26万件の運転免許データを削除
	8/5	村田製作所	72,460件	内部不正	×	会計システムの更新プロジェクトに携わっていた中国の再委託先の社員が、取引先情報などを不正取得
	4/1	ランドブレイン	200超の自治体	不正アクセス		自治体向けサービスのサーバーがランサムに感染し、取引先自治体の個人情報が流出した可能性
	3/31	神奈川県警	詳細調査中	内部不正	×	捜査で知り得た情報を漏らす見返りに、現金を受け取っていた可能性がある
	3/29	東急コミュニティー	約5000件	内部不正	×	元従業員が不正に顧客の氏名、住所、電話番号、マンション名、部屋番号を外部の法人へ持ち出し
	3/29	松井証券	210名/総額2億円	内部不正	×	システム開発担当企業のSEが、顧客のID、パスワード、暗証番号を不正入手
	2/12	マイナビ	21万2,816名	不正アクセス		不正ログインが発生し、サービス利用者21万2,816名分の履歴書情報が流出
	1/21	DeNA	8件	内部不正	×	カスタマーサポート業務において、お客様の個人情報を不正に使用し、カードローンの不正申し込み
	1/15	ソフトバンク	170の機密ファイル	内部不正	×	ライバル企業に転職した元社員の社外秘情報持ち出し
2020	12/8	LDH JAPAN	4万4,663件	不正アクセス		オンラインショップがサイバー攻撃を受け、クレジットカード情報4万4,663名分が流出の可能性
	12/7	PayPay	最大2007万件	不正アクセス	×	PayPayに対し、約260万の加盟店情報と従業員やパートナー企業に関する情報へ不正アクセス
	11/20	三菱電機	8,635件	不正アクセス		クラウドサービスへの攻撃により、取引先企業や個人事業主の金融口座情報について、情報が流出
	11/17	peatix Inc.	677万件	不正アクセス		イベント管理サービスの677万件の氏名,メールアドレス,パスワード等の利用者情報が流出した可能性
	11/16	カプコン	合計約35万件	不正アクセス		サイバー攻撃により、保有する顧客・従業員等の情報合計約35万件に流出の可能性があると発表
	9/8	NTTドコモ	120件/2,542万円	不正利用		ドコモ口座を悪用し、七十七銀行、東邦銀行、中国銀行など複数の銀行の口座で不正出金が発生
	7/22	みずほ総合研究所	約250万件	媒体の誤廃棄	×	顧客情報約66万9千件、顧客のサービス利用実績を記録した外部記憶媒体を誤って紛失(廃棄)
	6/15	キタムラ	最大40万件	パスワードリスト型攻撃	×	Webサイトへの不正アクセスにより、顧客情報最大40万件が流出と一部顧客でポイントの不正利用
	4/24	任天堂	約16万件	パスワードリスト型攻撃	×	「ニンテンドーネットワークID」約16万件と、一部の「ニンテンドーID」について、外部からの不正ログイン
	4/19	リジョブ	最大20万6991件	不正アクセス		テストサーバーのデータベースに2015/12/5以前に登録していた最大20万6991件の流出の可能性
	4/13	Classi	最大122万件	不正アクセス		教育機関向けSaaS「Classi」の最大122万件の利用ID・暗号化されたパスワードが流出の可能性
	1/20	三菱電機	8122件+機密情報	不正アクセス		ウイルス対策システムの脆弱性を突き、個人情報、技術・営業関連の機密情報が流出した可能性

昨今の事案

パートナー企業による不正アクセス

システム開発等を担当するパートナーSEが、2017-2019年の間に、210名分のID、パスワード、取引暗証番号などを不正入手

課題

- **システム管理担当者が顧客情報にアクセスできてしまった**
- 多要素認証が必須ではなかった

解決策

- 管理者へのアクセス制御の実現
- 厳格な本人確認:多要素認証

再委託先からの不正アクセス

会計システムの更新プロジェクトに携わっていた中国の再委託先の社員が、取引先情報など約7万件を不正に取得

課題

- **中国から個人情報にアクセスする業務を実施**
- **個人情報を伏字化していない**

解決策

- 業務委託先からのアクセス・ルートの制限
- 開発データのマスキング

システム担当による内部不正

特権IDを不正利用し、捜査情報や人事情報に不正アクセス。さらに、上司のパソコンで不正プログラムを実行し、26万件の運転免許データを削除

課題

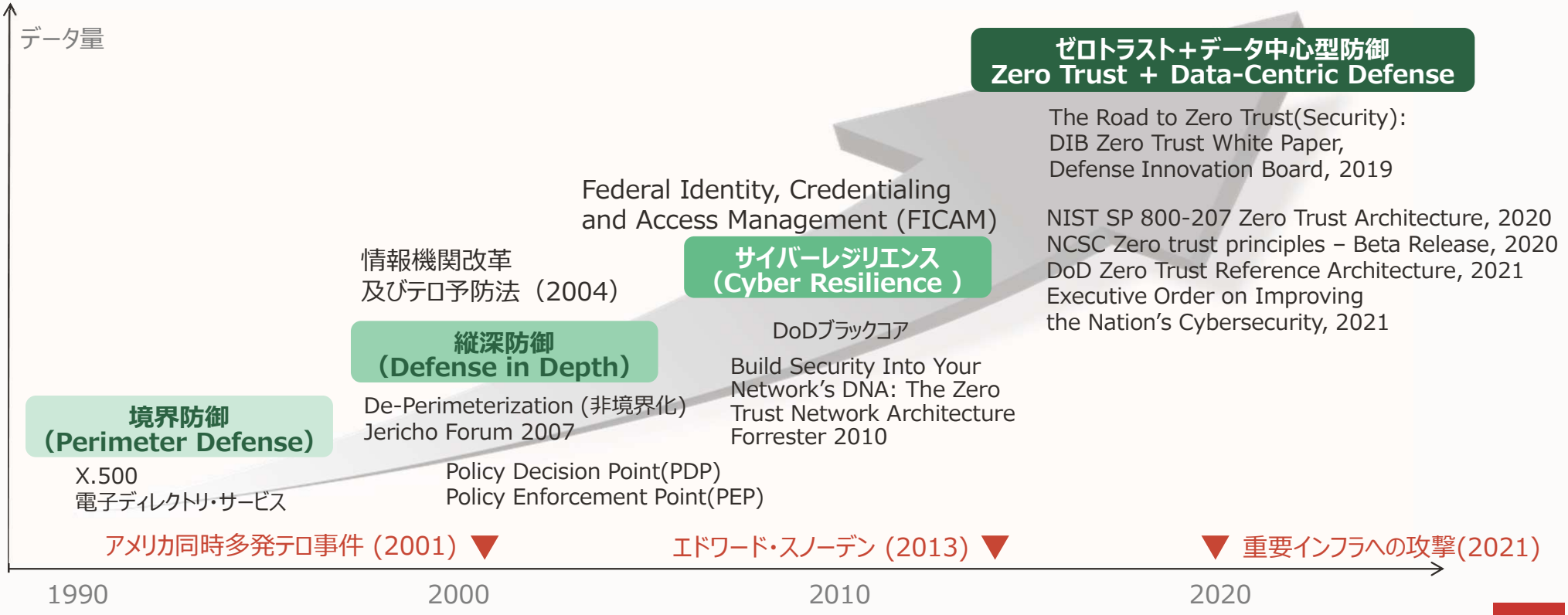
- **管理者への権限過剰付与**
- **改ざん対策**ができていなかった
- **不正な操作を検知**できなかった

解決策

- 管理者の職務分掌の実現
- データの改竄・消去の防止
- 異常操作の早期発見＆警告

米国におけるサイバーセキュリティモデルは急速に変化・発展しています

セキュリティモデルは数年毎に大波を迎え、過去の思想を塗り替えながら（過去のモデルの全否定ではなく）発展しています。
その要因としてサイバー攻撃の高度化、組織化が挙げられます。



アメリカ合衆国国防総省(DoD) ： ゼロトラストセキュリティを提供

U.S. Defense Department officials intend to complete an initial zero trust architecture by year's end to improve cybersecurity, according to Vice Adm. Nancy Norton, USN, director, Defense Information Systems Agency.

DOD to Offer Zero Trust Architecture This Year

THECYBEREDGE

July 15, 2020

By George I. Seffers

About the Author

Data-centric security marks a new paradigm.

The U.S. Defense Department by the end of the calendar year will release an initial zero trust architecture to improve cybersecurity across the department, says Vice Adm. Nanc Norton, USN, director, Defense Information Systems Agency, and commander, Joint Forc

ネットワーク中心のセキュリティモデルから**データ中心のセキュリティモデルへのこのパラダイムシフト**は、
最初にデータと重要なリソースを保護する方法に重点を置き、
次にネットワークに重点を置く

すべてを許可して例外で拒否するのではなく、**すべての[ネットワークアクセス]を拒否**して例外で許可するという
基本的な前提を変更

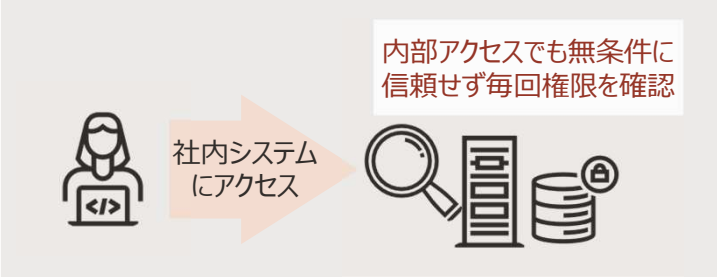
巧妙な攻撃者は私たちの**資格情報を盗み、特権に昇格し、データを盗み出し**ます。だからこそ、**データ侵害を防ぐために、ゼロトラストを採用**する

出典：https://www.afcea.org/content/dod-offer-zero-trust-architecture-year

ゼロトラスト・アーキテクチャの定義 (NIST SP 800-207)

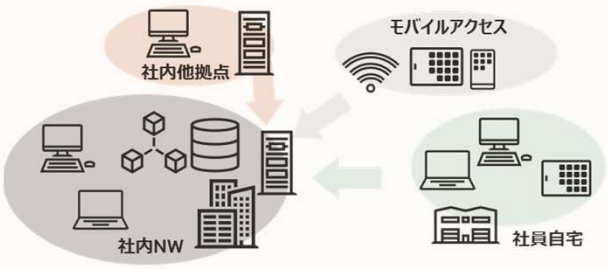
リソースにアクセスしてくるすべてのセッションを
「信頼できないもの」とみなして毎回、認証・認可の
プロセスを実施することでセキュリティを確保する方式。

- 認証：アクセス者がリソースにアクセスしてよいかを判断する
- 認可：アクセス者がアクセスしてよいリソースの範囲を判断する。



従来のネットワーク境界型のセキュリティ確保方式の代わりに出てきた概念。

業務に関わるNWの構成は年々複雑化



**一度境界を突破されると横断的に
他システムのデータも盗まれてしまう**

**内部からの不正アクセス
は防げない**

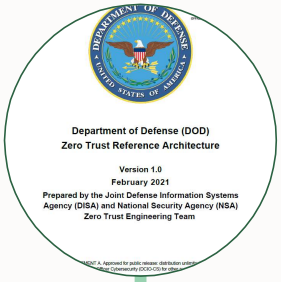
複雑化する企業NWや内部犯によるデータ漏洩等への対応を強化

出典：NIST Special Publication 800-207 https://csrc.nist.gov/publications/detail/sp/800-207/final

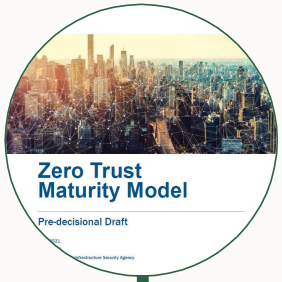
米国政府機関はゼロトラストセキュリティの具現化と適用計画を推進

米国政府機関は2024年末までにゼロトラストアーキテクチャの実装を完了

DoD Zero Trust
Reference Architecture (Draft)



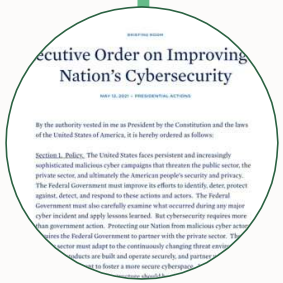
CISA Zero Trust
Maturity Model (Draft)



Moving the U.S. Government
Towards Zero Trust Cybersecurity
Principles (Draft)

2020.8 | 2021.2 | 2021.5 | 2021.6 | 2021.8 | 2021.9

NIST SP 800-207
Zero Trust Architecture



Executive Order on Improving the Nation's Cybersecurity

NCSC Zero trust principles

大統領令を発令、国家機関にサイバーセキュリティを向上する措置を指示

リアルタイムでデータ保護に集中するために、「ゼロトラストアーキテクチャ」の導入指示

データセントリックなセキュリティ・モデルの実装が必要とされています。

Sec.3. Modernizing Federal Government Cybersecurity.

60日以内に、各政府機関の長はゼロトラストアーキテクチャを実装するための計画を策定し、報告書を提出する

180日以内に、政府機関システムは多要素認証を採用し、保存中および転送中のデータに対しても暗号化を適用する

60日以内に、国家安全保証システムは大統領令のセキュリティ要件と同等またはそれ以上の要件を適用する

ゼロトラストアーキテクチャ

不正アクセスの拡大（ラテラル・ムーブメント）を制限し、異常又は不正な活動を探知し、「脅威が変化を続ける状況の中で、**リアルタイムでデータ保護に集中する**ために、インフラのすべての側面を通して、包括的なセキュリティ監視、きめ細かなリスクベースのアクセス制御、そして、システムセキュリティの自動化を組み合わせて導入する」ものです。

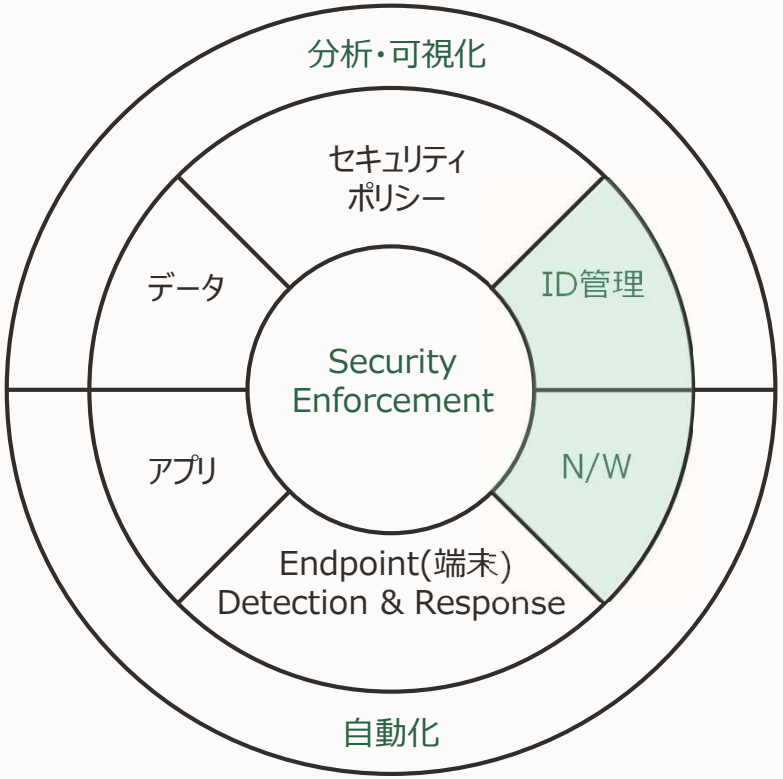
引用：Executive Order on Improving the Nation's Cybersecurity　MAY 12, 2021　PRESIDENTIAL ACTIONS

ゼロトラストの考え方

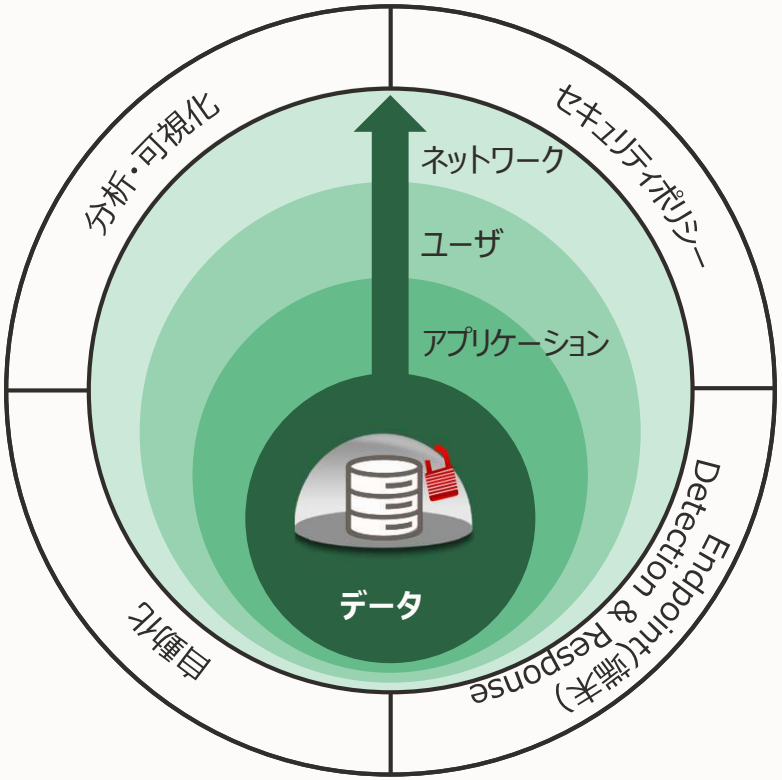
守るべき経営資源（リソース）に焦点をあてセキュリティ対策を実施することが寛容です

境界突破、内部不正を想定した対策が必要です

従来の単層式境界防御
ネットワーク中心型セキュリティモデル



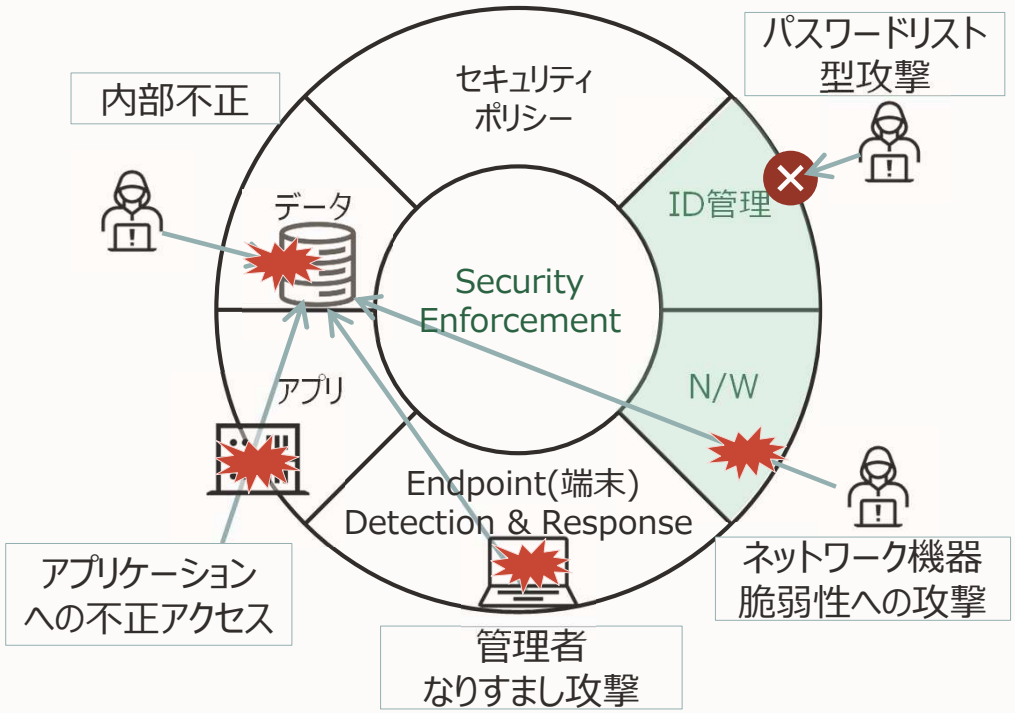
リソース防護重点型ゼロトラスト防御
データ中心型セキュリティモデル



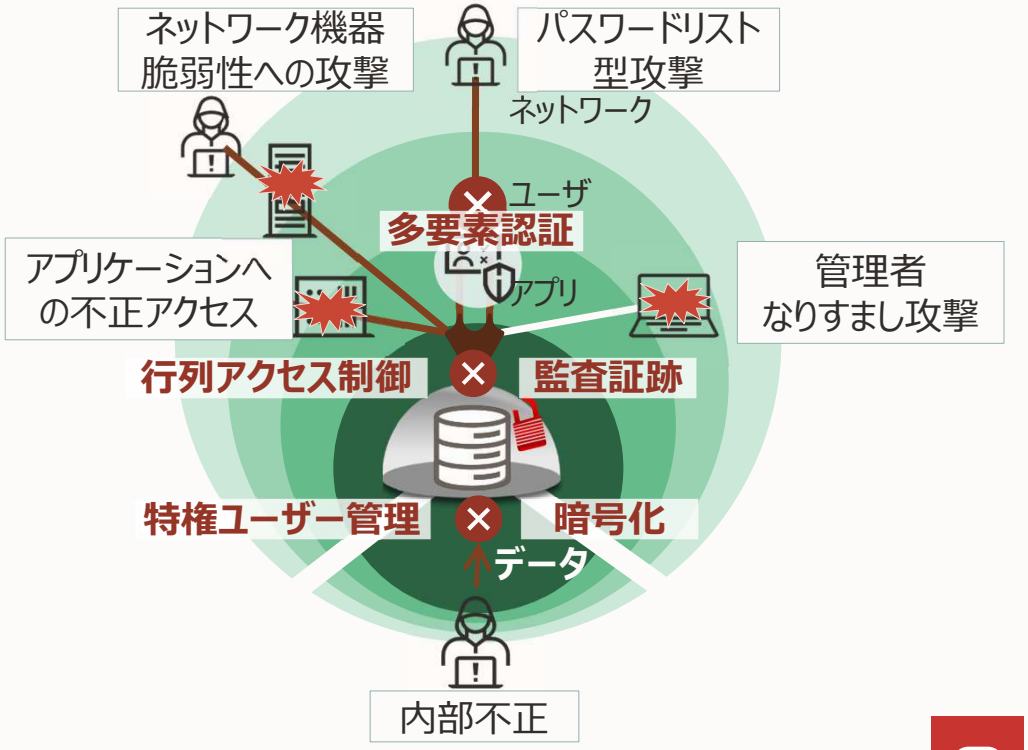
守るべき経営資源（リソース）に焦点をあてセキュリティ対策を実施することが寛容です

境界突破、内部不正を想定した対策が必要です

従来の単層式境界防御
ネットワーク中心型セキュリティモデル



リソース防護重点型ゼロトラスト防御
データ中心型セキュリティモデル



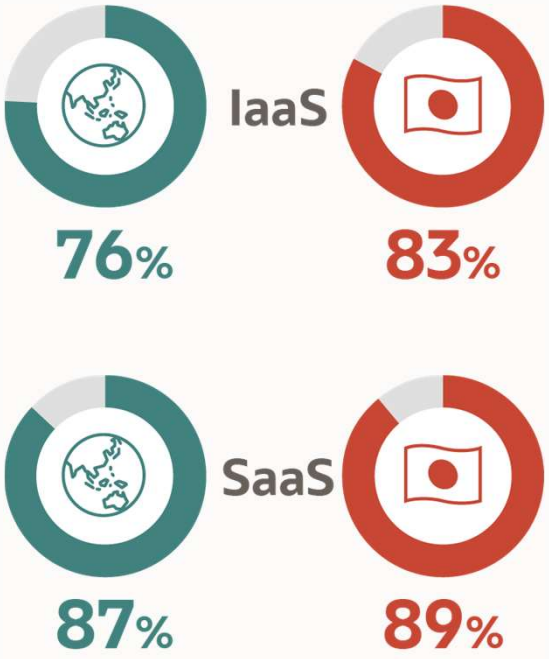
クラウドセキュリティに関する世界の動向、日本企業が抱える課題

オラクルとKPMGによるクラウドの脅威レポート 2020年

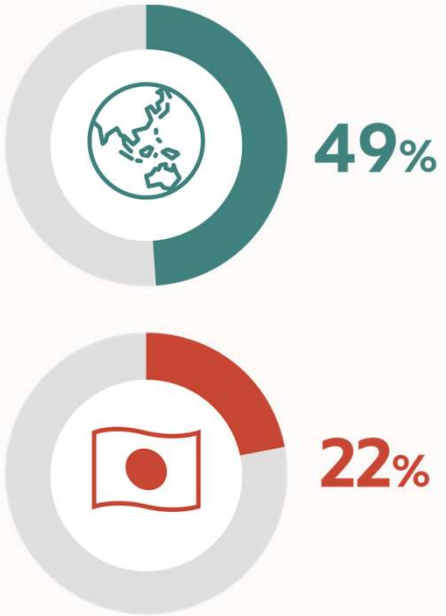
出遅れる日本企業の本格的なクラウド利用

利用は拡大しているが、日本ではクラウドサービスの限定的な利用が続いている

クラウドサービスを利用している企業



今後2年間で、半分以上のデータをクラウドに移行する予定の企業

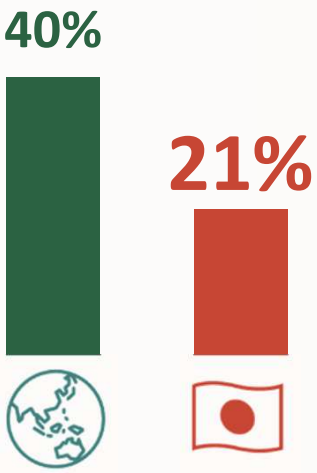


クラウドのセキュリティに対する理解は深まっておらず、グローバルと大きな開き

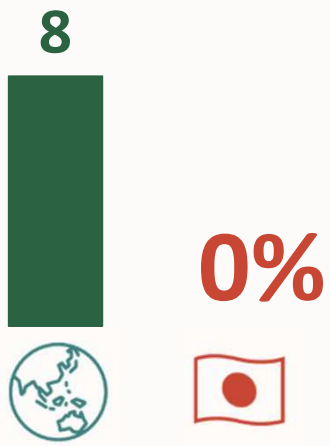
オンプレと比較して、「クラウドは十分に安全である」と認識しているか？

グローバルでの2018年から2020年の変化

2020年におけるグローバルと日本の比較



クラウドセキュリティの責任共有モデルを正しく理解しているか？



参考: クラウドサービスにおける「共有責任」モデル

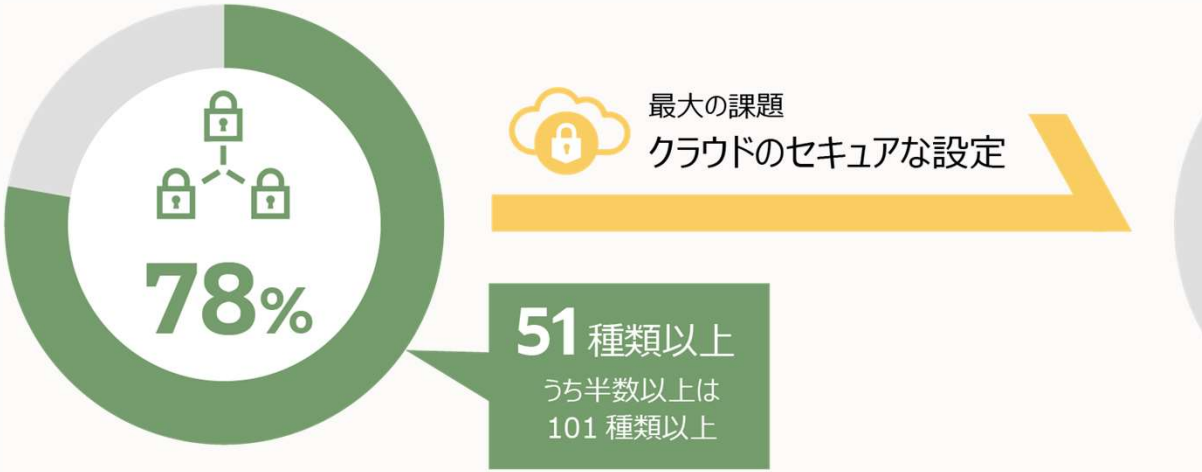
管理コンポーネント	SaaS	PaaS	IaaS
アプリケーションの構成の設定	ユーザー管理	ユーザー管理	ユーザー管理
実装したアプリケーション	クラウド事業者管理	ユーザー管理	ユーザー管理
Database, AP Server	クラウド事業者管理	クラウド事業者管理	ユーザー管理
オペレーティングシステム	クラウド事業者管理	クラウド事業者管理	ユーザー管理
ストレージ	クラウド事業者管理	クラウド事業者管理	ユーザー管理
サーバー	クラウド事業者管理	クラウド事業者管理	クラウド事業者管理
ネットワーク	クラウド事業者管理	クラウド事業者管理	クラウド事業者管理
物理筐体・建屋・電源	クラウド事業者管理	クラウド事業者管理	クラウド事業者管理

この領域の運用管理コストがポイント

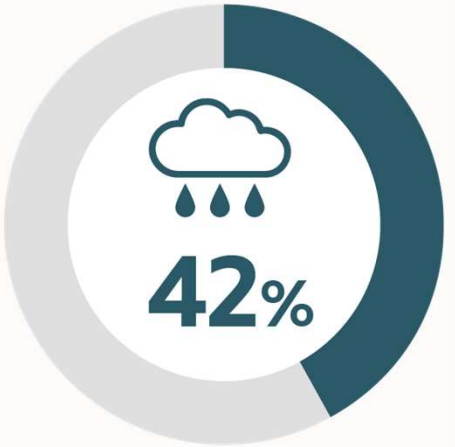
※参考 経済産業省「NISTによるクラウドコンピューティングの定義(SP 800-145)」他

ツールの多さ、場当たり的なセキュリティ・アプローチと設定ミス

利用しているサイバーセキュリティ製品



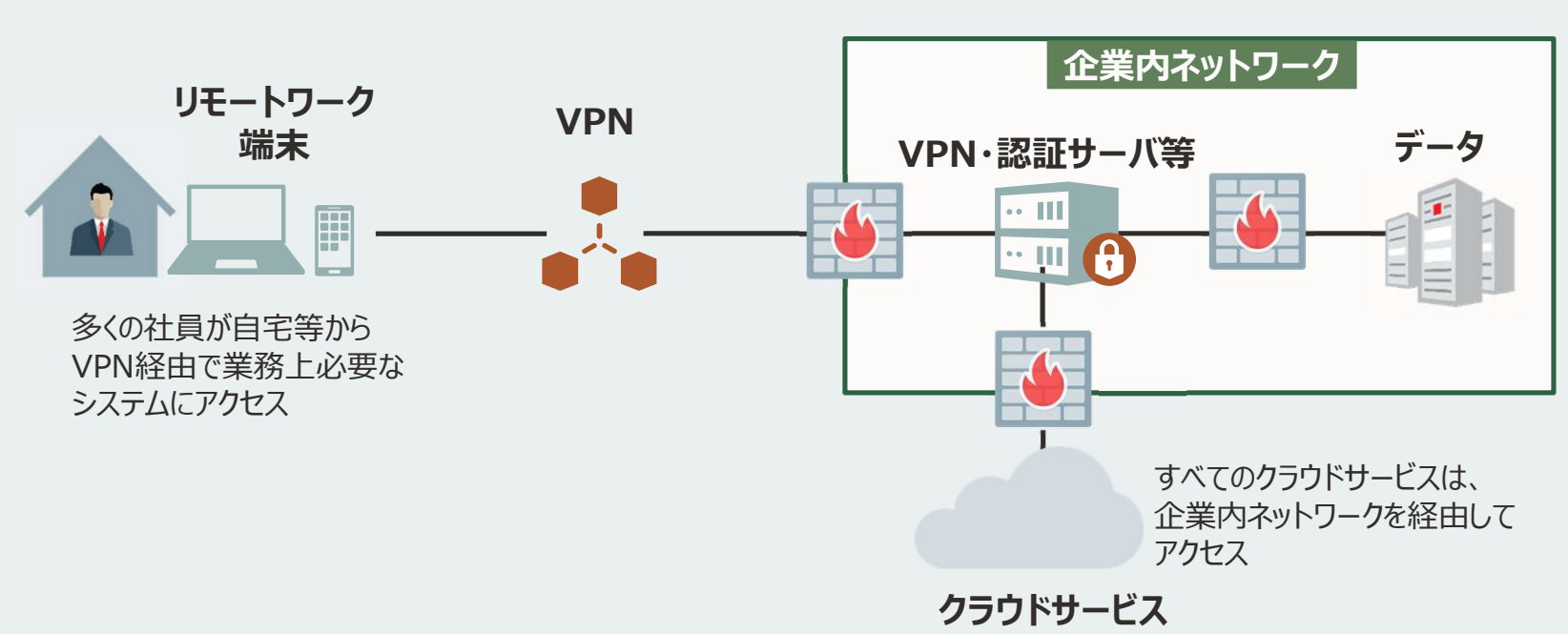
設定ミスによるデータ損失の発生



最大の課題
クラウドのセキュアな設定

リモートワーク環境整備における検討事項

リモートワークを推進すると社外からのアクセスが急増するため、社外からアクセスするために必要となる既存のネットワーク機器（VPNや認証サーバ等）がひっ迫する可能性があり、対応策の検討が求められます。



今後求められるセキュリティ対策と日本の取り組むべき点

安全なクラウドセキュリティ環境を整備するためには、ネットワークセキュリティだけでなく、
ゼロ・トラスト・セキュリティな対策が必要となります。

考慮点	ゼロトラストセキュリティの考え方	セキュリティ対策例	日本企業の状況
ネットワーク	• 通信を監視し、未許可のクラウドサービスの利用を制限	• CASB • Cloud Proxy • WAF	グローバルより注力している
デバイス	• デバイスの認証を常に実施 • 全てのデバイスの保護を徹底	• EDR、EPP • MDM	グローバルと同様
IDアクセス管理	• ID・ユーザを必ず検証 • 必要に応じて多要素認証(MFA)を実施	• IAM • PAM • MFA	**グローバルより対応が遅れている**
アプリケーション	• すべてのアクセスを制限し、不正操作を監視	• CASB、UEBA • 標的型メール対策 • SIEM、SOAR	グローバルと同様
データ	• データが漏洩・改ざんされないように保護 • 必要最小限の権限付与	• 暗号化 • アクセス制御	**グローバルより対応が遅れている**

出典: Oracle and KPMG Threat Report 2020

IDアクセス管理・データセキュリティの対応状況について：調査結果

ID・アクセス管理(IAM)で日本企業が苦労している点

① **人事イベントとの連携**
② **クラウドサービスへのIAMによる制御**
③ アプリケーション/モバイル利用の制御
④ **権限管理**
⑤ **多要素認証**

太字：グローバルとの差が多いもの

発見された設定ミス：グローバルと差が大きい TOP3

1位 過剰な権限付与
 **37%**  **45%**

2位 セキュリティグループの誤設定
 **33%**  **40%**

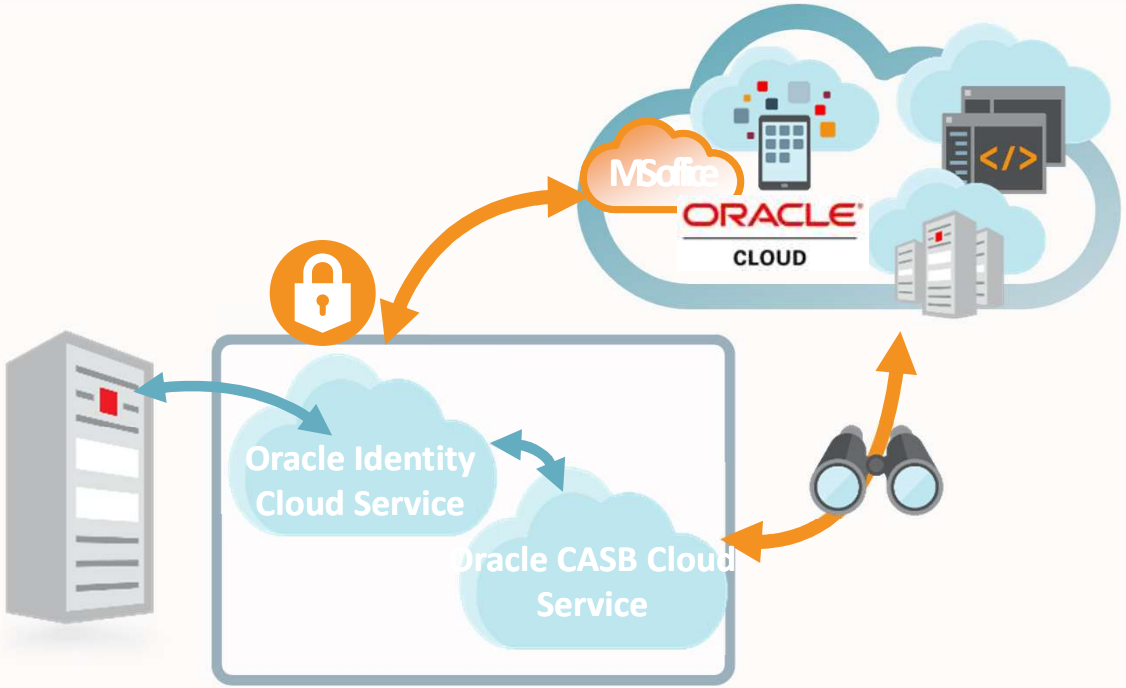
3位 機密情報が暗号化されていない
 **25%**  **32%**

IDアクセス管理・データセキュリティ対策に関して、日本企業は認証に加えて利用者に必要となる最小権限の実現と誤設定の早期検知、暗号化に課題があり、改善が必要となっています。

出典: Oracle and KPMG Threat Report 2020

顧客事例：株式会社アウトソーシング

国内外のグループ企業向けのID・アクセス管理／セキュリティ基盤



マルチクラウドでの利便性向上とセキュリティ強化

- マルチクラウドサービスのID・アクセス管理用に「**Oracle Identity Cloud Service**」を利用
- 各クラウドサービスのシステム構成の設定開始から構築完了まで**数時間で完了**
- 国内外の**利用者を特定**し、SSOによる利便性向上と多要素認証、アクセス制御、監査によりセキュリティ強化を実現
- マルチクラウドサービスの監視に「Oracle CASB Cloud Service」を採用
- 国内外のグループ企業全体のID・アクセス管理とクラウドセキュリティ監視の技術と運用を確立

紙ベースの業務を電子化することで、在宅においても業務フローを実施可能に

Oracle Identity Cloud + Process/OIC連携

	利用の目的	想定されるユースケース
1	文書のレビューや承認に関する **文書ワークフロー**	• 就業規則などの社内文書の承認・公開 • RFI/RFP などの社外向け配布文書の社内レビュー • NDA など社外からの受領文書の社内回覧・レビュー
2	複数のファイル添付が伴う **業務ワークフロー**	• 経費精算 • 国内・海外出張申請 • 営業稟議申請　ほか
3	文書+ワークフローの **ユーザーインタフェース統合**	• パートナー向け情報提供ポータル • サプライヤー向けポータル • 従業員向けポータル　ほか

外部企業との電子化フロー例

特権ユーザー管理の強化対策事例：ヤフー様

Oracle Database Vaultって本当に必要ですか？データを守るためよりもむしろメンバーを守るためにこそいるのです

谷川 耕一 [著] 2012年11月19日 00:00

ツイート 26 いいね！ 180 B! 2 g+1 2

24時間監視し監査の体制を整えるだけでは十分ではない

新たなサービスを立ち上げたいのでサーバーやデータベースが欲しいという要求があれば、社内クラウド的にITリソースを割り当てて提供する。

「個人情報を扱うデータベースについては、重要データを暗号化し、物理的にも隔離された専用のセキュアルームからしかアクセスできないようになっています。当然ながら、24時間365日しっかりと監視も行われています」と語るのは、システム統括本部 インフラ技術本部 インフラ技術2部 DBMS技術リーダーの尾崎弘宗氏。

セキュアルームからのみのアクセスで、さらには24時間の厳重な監視がなされていても、データベース管理をする立場のエンジニアであれば、データベースにアクセス可能なユーザー権限を持っている。

管理者であれば管理者権限という「特権」を持っているので、機密情報にもアクセスできるのは当たり前だろう。しかしながら、しっかりとした監視体制を敷きながら、**「管理者はアクセスできる」という事実そのものが、Yahoo!JAPANでは問題だというのだ。**

http://enterprisezine.jp/dbonline/detail/4350　記事抜粋

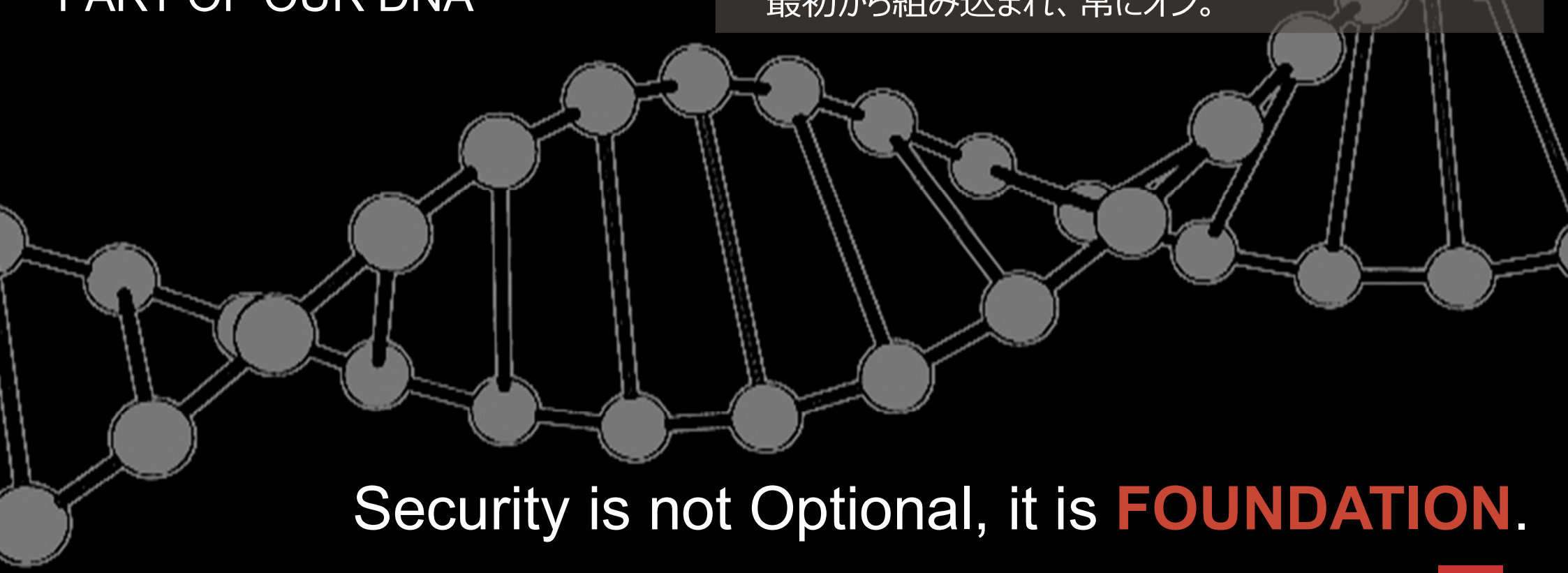
オラクルのセキュリティへの取り組み

Oracle Cloud Infrastructure

SECURITY

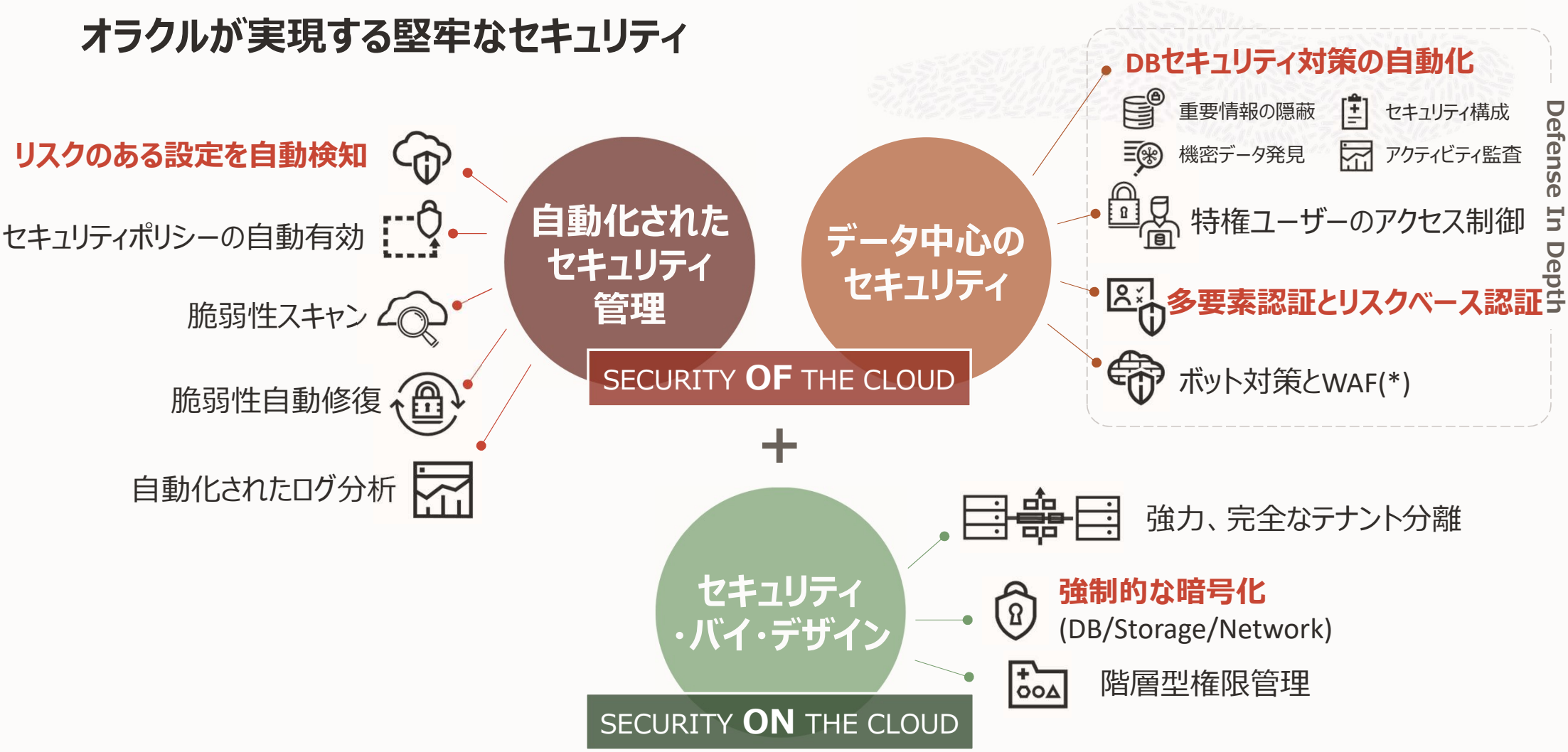
PART OF OUR DNA

- 1977 年からビジネス・スタート。最初の顧客は CIA
- 米国政府の要求に応えるセキュリティ技術を提供
- セキュリティは追加できると考えず、組み込むべきもの
- オラクルの製品とクラウド・サービスでは、セキュリティは最初から組み込まれ、常にオン。



Security is not Optional, it is **FOUNDATION**.

オラクルが実現する堅牢なセキュリティ



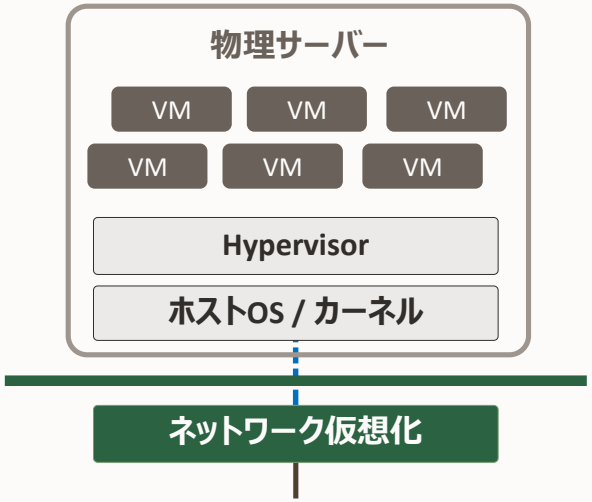
* WAF: Web Application Firewall

組み込んだ
セキュリティ

クラウドプラットフォームレベルでの環境隔離と暗号化

強力、完全なテナント分離

✓ 分離された仮想ネットワークにより情報漏洩のリスクを最小化



階層型権限管理

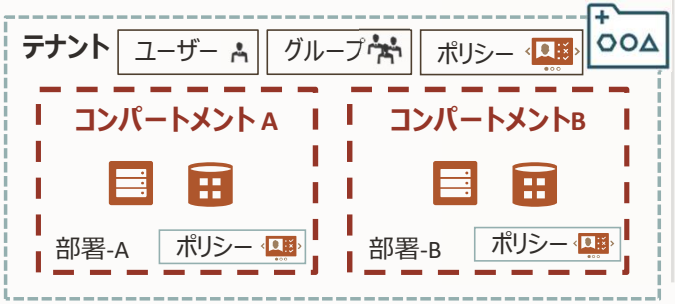
✓ 部署ごとの権限設定を実現

✓ コンパートメント間のリソースアクセスが可能、部署を跨いだシステム構築も容易

✓ コンパートメント毎のクオータ設定により　使い過ぎを抑止

「コンパートメント」モデル

部署ごとにCompartment（サブアカウント）を作成

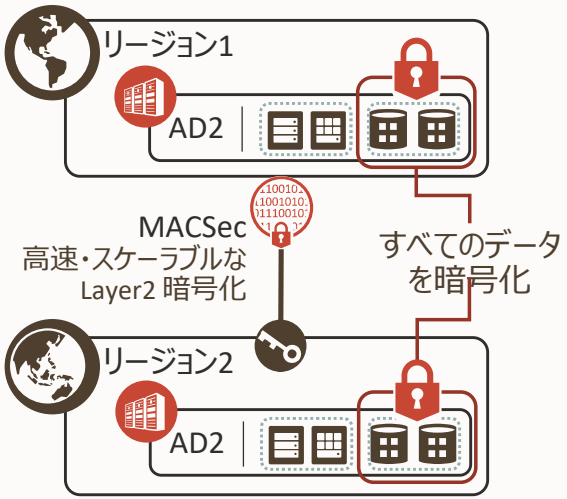


強制的な暗号化

✓ すべてのデータ・サービスはOracleがフルマネージドで暗号化

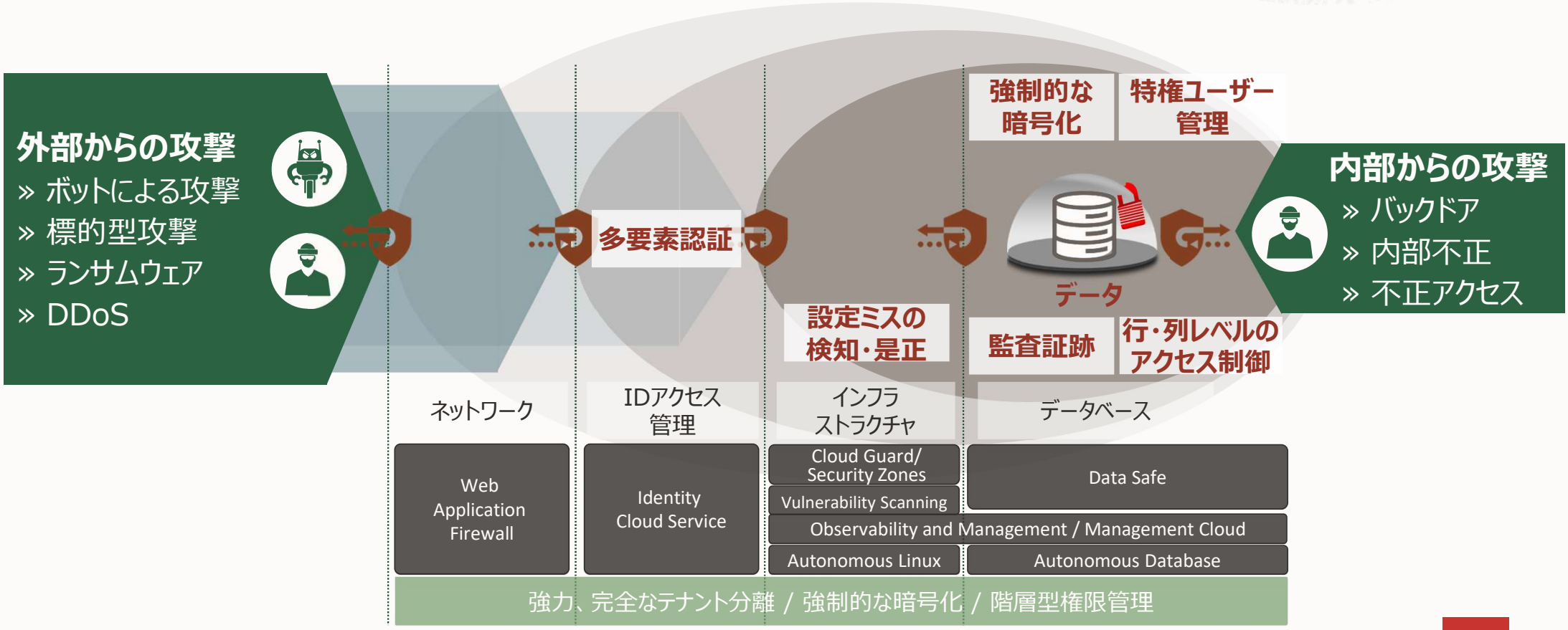
　✓ データベースファイル,ストレージ
　Block Volume, Boot Volume

✓ すべてのネットワーク通信も暗号化



推奨セキュリティ機能は基本的に全て有効化した状態で提供

常時オン

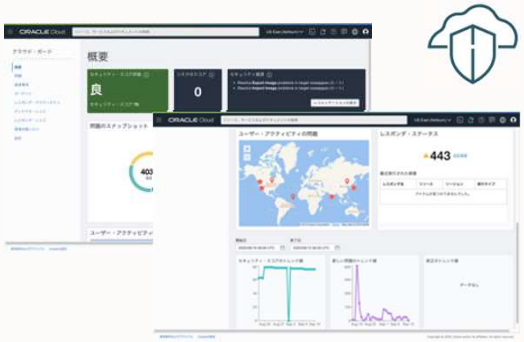


自動化されたEnd-to-Endのセキュリティで人的ミスを排除

自動化された
セキュリティ
管理

リスクのある設定を自動検知

- 構成とアクティビティを監視
- 問題の特定、脅威を検出
- 問題の是正、顧客通知



Oracle Cloud Guard

セキュリティポリシーの自動有効

- ベスト・プラクティスを強制的に適用
- 初期段階からリソースの
  セキュリティを確保

Oracle Security Zones

脆弱性自動修復

- Oracle Autonomous Databaseにおける脆弱性自動修復
- Oracle Data Safeによる
  セキュリティ・リスク軽減

自動パッチ適用
アップグレード

- セキュリティ構成評価
- ユーザーのリスク評価
- アクティビティの監査
- 機密データの発見
- データ・マスキング

Oracle Autonomous Database

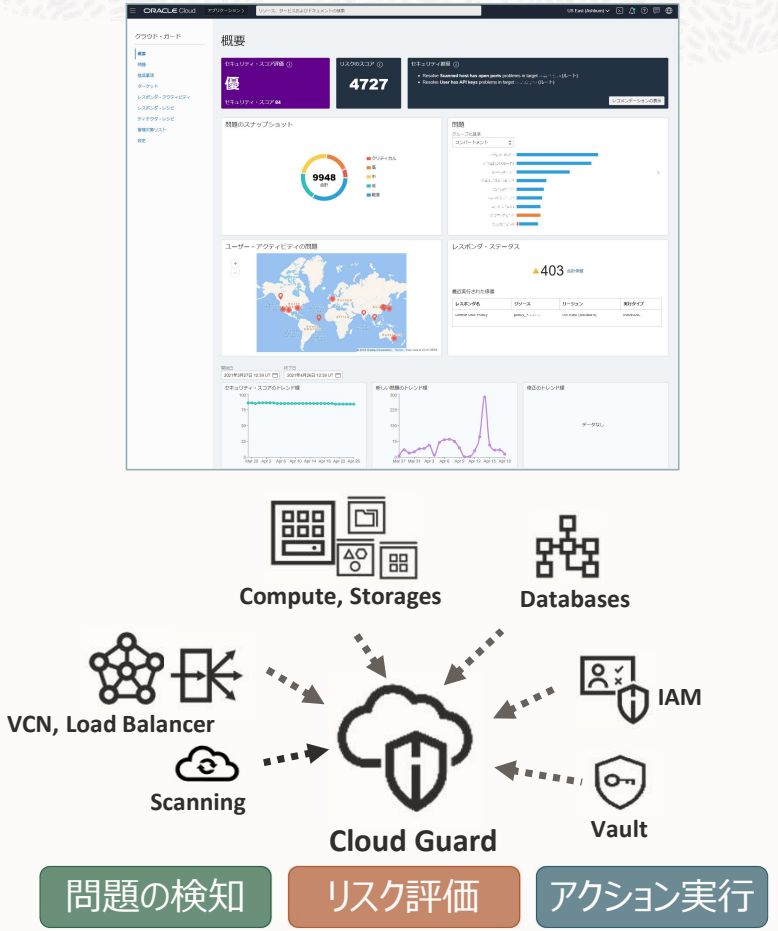
Oracle Data Safe

Oracle Cloud Guard

自動化された
セキュリティ
管理

Oracle Cloud Infrastructureの様々なサービス設定や
アクティビティを監視し、通知・是正することで安全なクラウドの 利用をサポート

- OCIの様々なサービスの設定やアクティビティを監視し、通知・アクションを実行することで安全にクラウドを運用
- 脆弱な設定やリスクの高いユーザー操作を検出ルールに基づいて常時監視
- 検出ルールはオラクル管理で自動化され、ユーザーによるメンテ ナンスの必要はなし
- 検出された問題はリスクレベルで評価し、テナント全体の健全性をスコアリング
- 検出されたリスクは、メール等で通知が可能
- 無償で提供



ワークスアプリケーションズ 様

ERPマネージド・サービスHUE Classic Cloudで「Oracle Cloud Guard」を活用し、セキュリティリスクを軽減

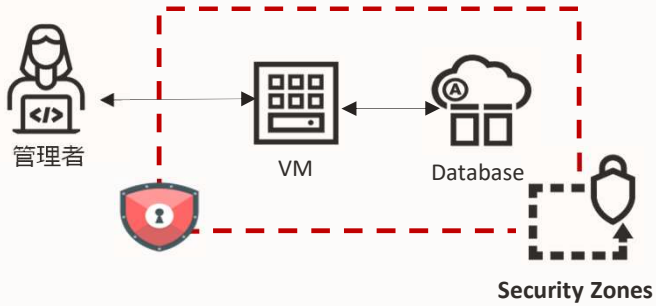
- 設定や運用上の問題によって発生するセキュリティリスクを自動検知し、インフラの安定的な運用に寄与
- 他社のクラウドサービスと比べて監視できる項目が広く、UI含め使い勝手が優れているため、効率的な運用が可能
- 「Oracle Cloud Infrastructure」は、クラウドプラットフォームレベルで環境隔離と強制的な暗号化がされており、「Oracle Cloud Guard」と組みあわせることで、お客様に安心して利用頂けるサービスを提供

自動化された
セキュリティ
管理

Oracle Maximum Security Zones

- 強固なセキュリティ・ポリシーを適用
- パブリックからのアクセスに関する制限、暗号化、リソースの移動制限など40を超えるポリシーをオラクルで管理・提供
- ポリシーに違反する操作は、定義されてセキュリティゾーン内では実行することはできない
- より高いセキュリティレベルで保護する必要があるリソースに対して、強制的にポリシーを適用し、セキュアなクラウド運用を実現

事前定義のルール
パブリックアクセス不可、
安全でないストレージなし



Oracle Cloud Infrastructureが業界初で提供した機能

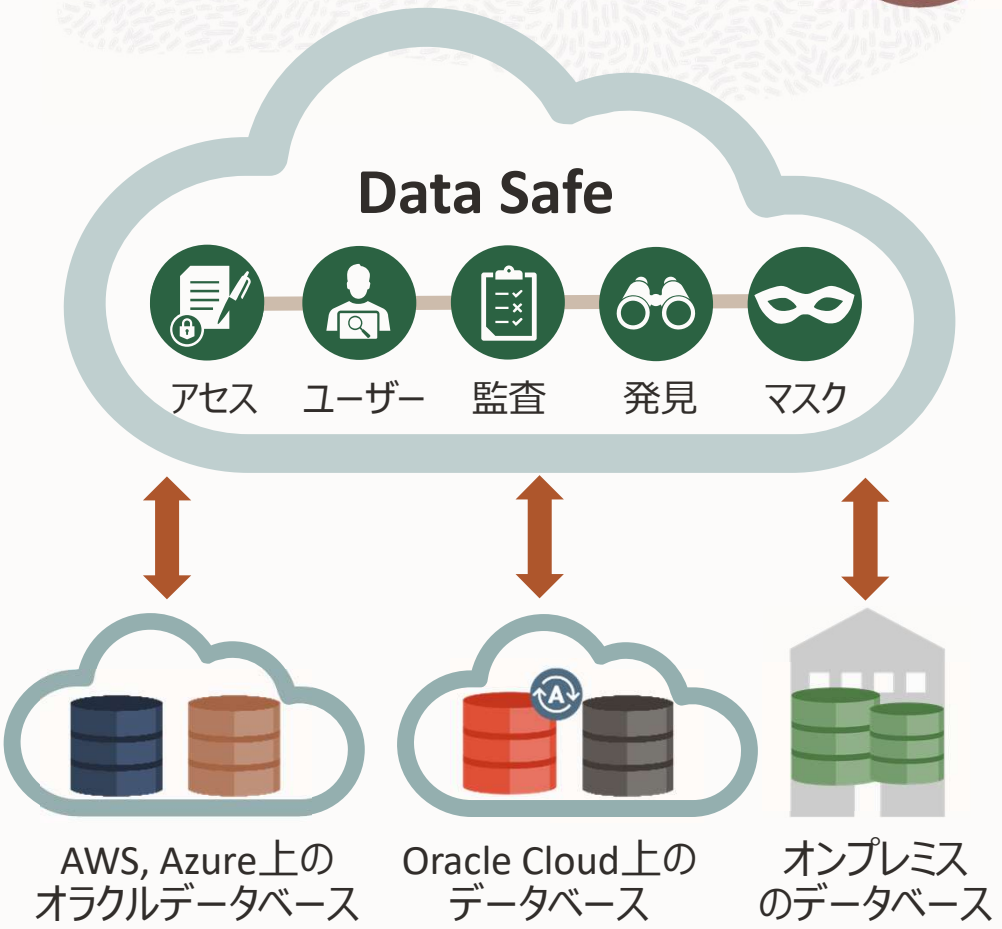
自動化された
セキュリティ
管理

Oracle Data Safe

ハイブリットクラウドで利用するデータベース をよりセキュアに

- ✓ 統合されたデータベースセキュリティ管理サービス
  1. 機密データの発見（Sensitive Data Discovery ）
  2. データ・マスキング（Data Masking）
  3. アクティビティの監査（Activity Auditing）
  4. セキュリティ構成の評価（Security Assessment）
  5. ユーザーのリスク評価（User Assessment）
- ✓ 特別なセキュリティの専門知識
- ✓ 多層防御における重要なデータ・セキュリティ対策
- ✓ 短時間でセキュリティ・リスクを軽減
- ✓ Oracle Cloud Databaseの利用でサービスを無償提供 ※1
- ✓ オンプレミス、他社クラウド上のオラクルDBへも対応
  - 24,000円 /ターゲット/月

※ 監査機能は100万レコード/月まで無償、その他の機能は無償



Oracle Cloud Infrastructure のコンプライアンス対応

代表的なもの

グローバル

27001 : 27017 : 27018

日本

(金融機関)

(政府機関)

3省3ガイドライン

(ヘルスケア)

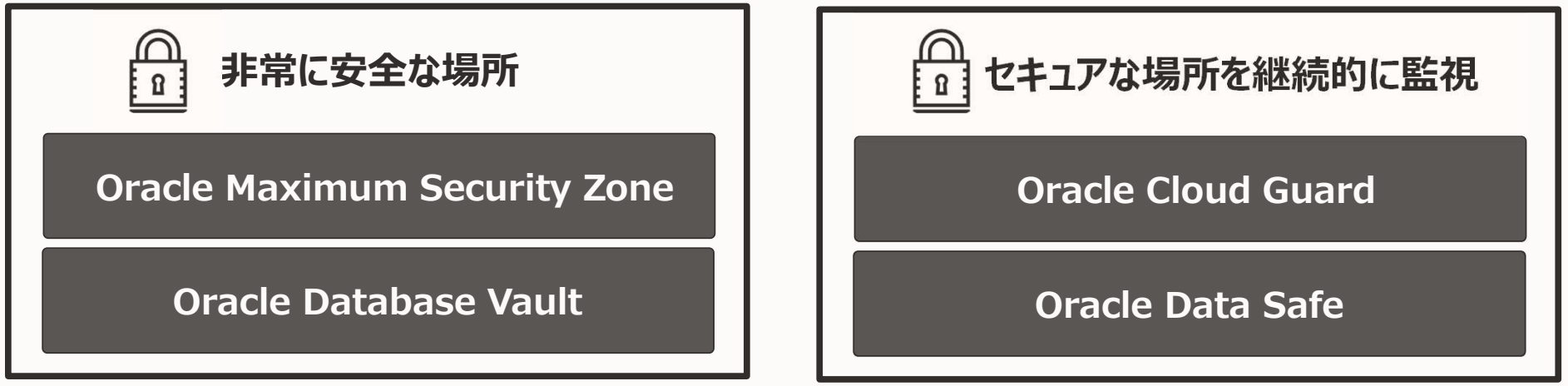
ISMAP

(政府機関)

ゼロトラスト・セキュリティに基づいた設計

Oracle Cloud Infrastructureは、接続・認証・利用は否認が前提（Default Deny）

- 許可を与えなければ何もできない：Security list、コンパートメント、ポリシーの設定等



Oracle Cloud Infrastructure
セキュリティのプロもSaaS基盤としてOCIを選択

世界最大のコンピュータ ネットワーク機器ベンダー

ハードウェアやソフトウェアセンサーから
テレメトリー情報を収集し、データを高度な
機械学習技術によって分析するSaaS
(Cisco Tetration) でOCIを採用

数千コア以上の大規模アプリケーションを
2ヶ月で稼働

インテリジェンス主導型の セキュリティ企業

なりすまし攻撃、フィッシング、スパムによる
Eメール脅威の対策を提供するSaaSで
OCIを採用

高度なリアルタイム分析をベアメタル・
インスタンスを活用することでクラウドで実現

業界をリードする サイバーセキュリティ企業

脅威の識別、調査、解決を行うクラウドベースの
SIEMソリューション(McAfee ESM Cloud)で
OCIを採用

他社クラウドに比べ1/4のコストで実現
60万データソースにおける1秒当たり
50万イベントをサポート

セキュリティ価格概要 ～ クラウド編

カテゴリ	機能	機能名	単価
セキュリティ・バイ・デザイン	強力、完全なテナント分離	Isolated Network Virtualization / Bare Meta	標準機能
	強制的な暗号化	Encryption by Default	標準機能
	階層型権限管理	Compartment	標準機能
自動化されたセキュリティ管理	リスクのある設定を自動検知	Cloud Guard	無償
	ポリシーの自動適用	Security Zones	無償
	脆弱性スキャン	Vulnerability Scanning	無償
	オンラインでのパッチ適用	Autonomous Database	無償 (*1)
	自動化されたログ分析	Logging Analytics	10GBまで無償
データ中心の多層防御	DBセキュリティ対策の自動化	Data Safe	無償～ (*2)
	特権ユーザー管理	Database Vault	DBCS HP ～ (*3)
	多要素認証、リスクベース認証	IAM Identity Domains	無償～ (*4)
	ボット対策とWAF	Web Application Firewall	無償～ (*5)

*1 Autonomous Database 利用時に無償で利用可能
*2 Oracle Cloud Databaseの利用でサービスを無償提供。監査記録の蓄積は100万レコード/ターゲット/月まで無償
*3 DBCS High Performance以上で利用可能
*4 無償で利用できるユーザー数や機能に制限あり
*5 1インスタンス、1000万インカミングリクエスト/月まで無償。価格単位：¥72 [1,000,000インカミングリクエスト/月]、¥600[インスタンス/月]

本日お伝えしたこと

01

セキュリティ対策でのトレンドと日本が取り組むべき点
- ゼロトラストは、境界防御をやりながらデータセントリックなセキュリティ対策を目指す
- 日本は境界防御に偏っているため、IDアクセス管理とデータセキュリティ対策が必要

02

Oracle Cloud Infrastructureは、セキュリティは最初から組み込まれ常にオン。コンプライアンスも遵守
- 全リージョン、全インスタンスでセキュリティバイデザインのサービスを提供
- ISMAPをはじめ、業界で求められるコンプライアンス要件に対応済み

03

人的ミスを排除する自動化されたセキュリティ管理を提供
- Cloud Guard (無償) : リスクのある設定を自動検知・修正
- Security Zones (無償):セキュリティポリシーの自動有効し、ミスの起きない環境を実現
- Data Safe (無償～): データ漏洩から保護を効率的に実現


ORACLE