ORACLE

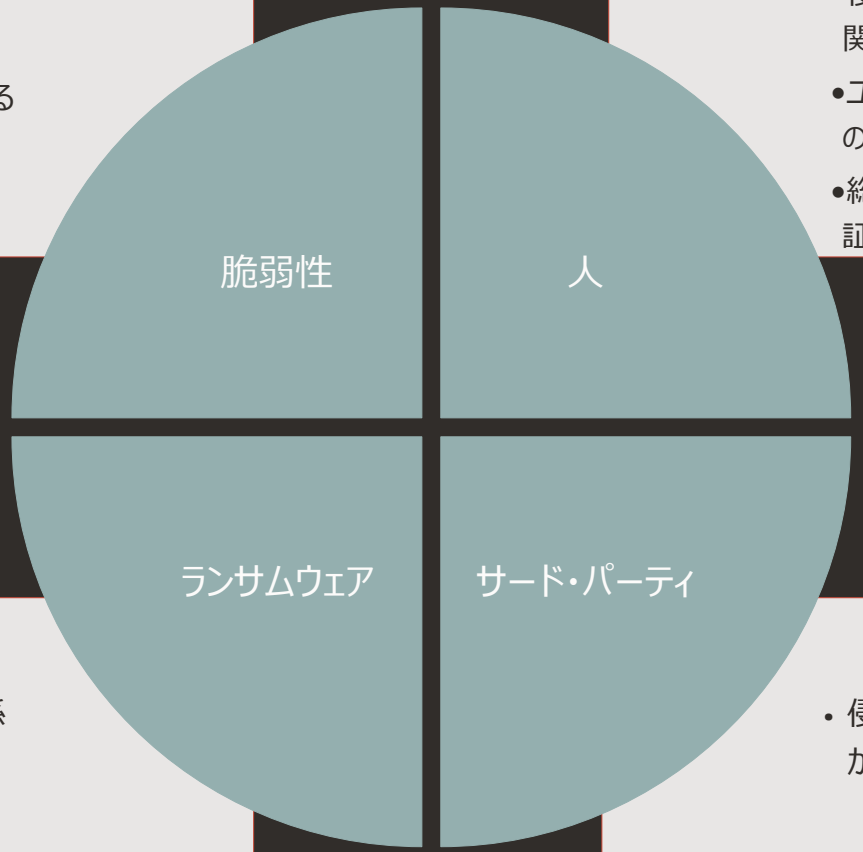
Oracle Exadata Database Machine

Maximum Security Architectureによるデータの保護

『Verizon 2024 Data Breach Investigations Report』
主要なインサイト

- 脆弱性の悪用が180 %増加
- 対応に時間がかかりすぎる：重大な問題の50 %を軽減するために55日かかる

- 侵害の68 %は悪意のない人間が関係
- ユーザーは60秒未満でフィッシングの手に陥る
- 総侵害件数の31 %は盗まれた認証情報に関係



- 侵害の32 %には恐喝が関係

- 侵害の15 %にはサード・パーティが関係

あらゆる場所で稼働するExadata

オンプレミス、ハイブリッド・クラウド、Oracle Public Cloud、マルチクラウド

Oracle Exadata Database Machine

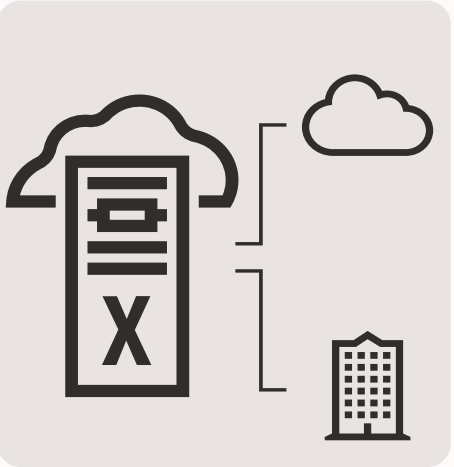
（オンプレミス）

Exadata Cloud@Customer

（ハイブリッド・クラウド）

Exadata Cloud Infrastructure

（Oracle Public Cloud）



マルチクラウド

（その他のクラウドと接続）

同じExadataテクノロジー | 100 %の互換性 | 停止時間ゼロの移行

ExadataプラットフォームがExadata DB Cloudの基盤を提供
セキュリティの概要

Exadataのセキュリティ・プラクティスと組込みセキュリティ保護は、オンプレミスのExadataに適用可能

- Exadata Cloud（ExaDB-D、ExaDB-C@C、Autonomous Database）はその利点を受け継ぎ、さらにクラウド・ソフトウェアとセキュリティ・コンプライアンスを追加

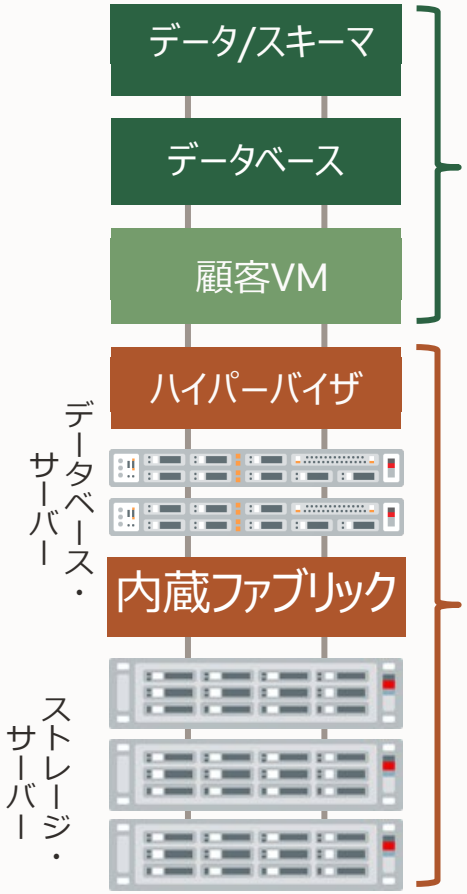
OCI上のExadata Cloudは、以下のコンプライアンス、証明書、および/または認証を取得しています

- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO 27001
- ✓ SOC 1/2/3
- ✓ C5/CSA STAR Level 2
- ✓ FedRAMP High
- ✓ DoD IL5
- ✓ UK Cyber Essentials

DB Cloud製品のセキュリティ関連の補足資料については、さらに以下を参照してください。

- https://www.oracle.com/jp/a/ocom/docs/exadata-cloud-at-customer-security-controls-ja.pdf
- https://www.oracle.com/jp/corporate/security-practices/cloud/

パブリック・クラウドでのシンプルなクラウド管理モデル



顧客はデータベース内のすべてを所有

- データ、スキーマ、暗号化鍵

顧客はデータベース・サービスをサブスクライブ

- お客様はクラウドの自動化機能（UI/API）を使用してVMとデータベースを管理
- 作成、削除、パッチ適用、バックアップ、スケール・アップ/ダウンなどが自動化
- サポートされているすべてのOracle Databaseバージョンを実行
- 顧客が顧客VMへのアクセスを制御
- 顧客は顧客VMにさらにソフトウェアをインストールして管理できる
- オラクルのスタッフには顧客VMにアクセスする権限がない

オラクルはインフラストラクチャを所有し、管理

- ハイパーバイザ、データベース・サーバーとストレージ・サーバー、ストレージ・ネットワーク
- パッチ適用、セキュリティ・スキャン、セキュリティ更新
- 監視とメンテナンス
- 顧客にはオラクルのインフラストラクチャにアクセスする権限がない

データからアイデンティティまでの統合セキュリティ

多層防御

- 透過的データ暗号（TDE）
- Data Redaction
- Data Masking
- Data Subsetting
- OCI Vault
- Oracle Database Vault
- Oracle Database Firewall
- Oracle Data Safe
- NIST SP-800-88r1準拠の消去機能

- STIG強化
- 最小パッケージ
- トークンベースのSSHアクセス

- 仮想クラウド・ネットワーク（VCN）
- Oracle Native Network Encryption
- 専用のクライアント・ネットワークとバックアップ・ネットワーク
- FastConnect

- 脆弱性スキャン
- FedRAMP
- ISO 27001
- SOC 1/2/3
- PCII-DSS
- HIPAA
- その他

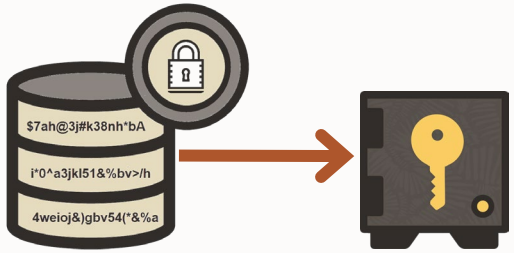
- アイデンティティおよびアクセス管理（IAM）
- フェデレーテッド・アイデンティティ・プロバイダ
- 多要素認証
- ポリシーベースのアクセス制御
- ユーザー、グループ
- コンパートメント
- インスタンス・プリンシパル
- リソース・プリンシパル

データベースの保護手法

セキュアな構成を実装

- データベース構成がポリシーに従っていることを確認
- 既知の脆弱性に対してパッチを適用
- 構成のずれを警戒

データへのアクセスを制御



- 移動中のデータと保管中のデータのどちらも暗号化
- ネットワークのスニッフィング攻撃から保護
- データ・スクレイピング攻撃（ランサムウェアなど）から保護

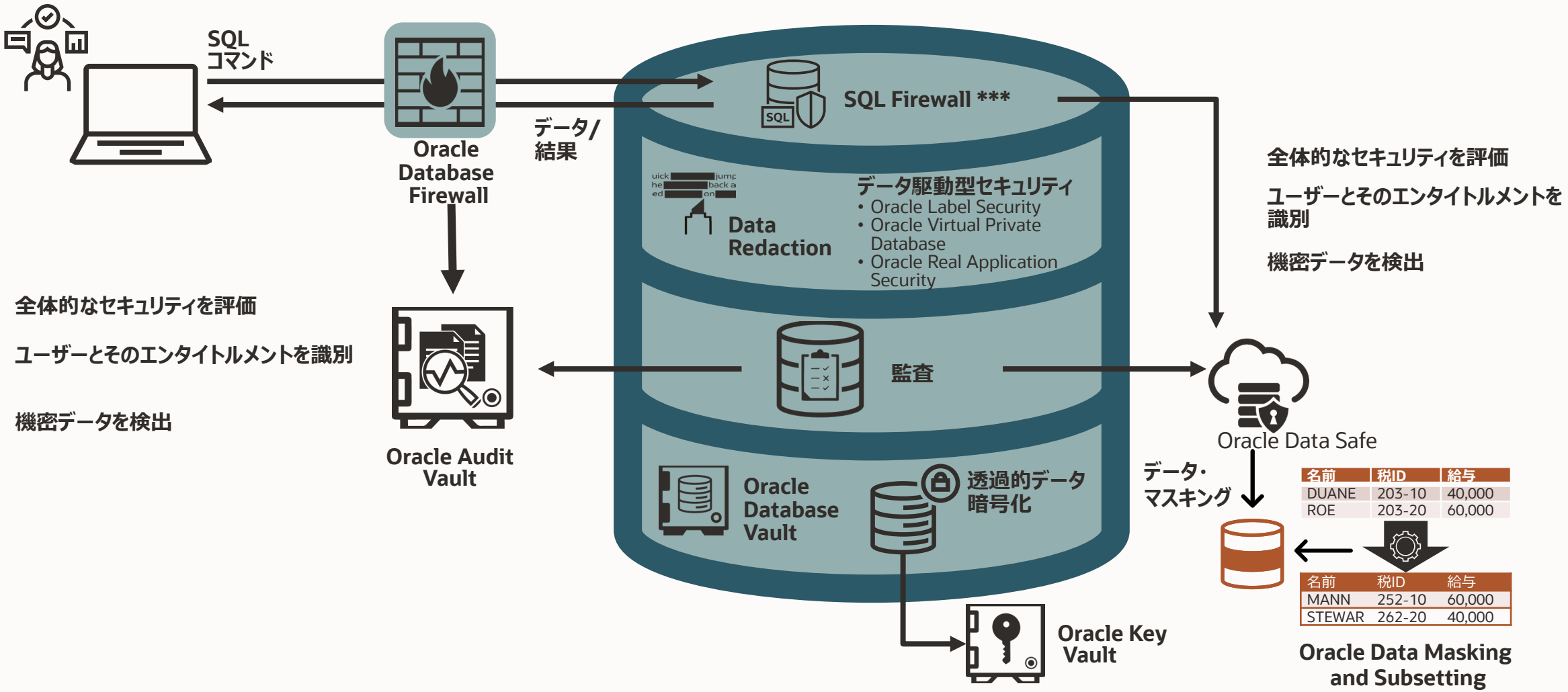
データを暗号化し、暗号化鍵を保護

- 最小限の権限付与を適用
- 特権ユーザーによるデータへのアクセスを制御
- 職務の分離を適用
- データへの信頼パスを確立して適用

データへのアクセスを監視

- ネイティブな監査機能を使用して高価値なアクティビティをキャプチャ
- ネットワークベースの監視を使用してすべてのアクティビティを検査

Oracle DatabaseのMaximum Security Architecture



*** Oracle Database 23aiでのみ使用可能

オラクルのセキュリティ・ポリシー

顧客データの機密性、完全性、可用性を保護する

- 以下のセキュリティを含む：
- 人材、ネットワークおよびシステムのアクセス制御、データ
- サプライ・チェーン管理、ラップトップPC、モバイル機器

以下の標準に準拠する

- ISO/IEC 27002:2013（旧ISO/IEC 17799:2005）
- ISO/IEC 27001:2013
- NIST

自社のポリシーとオラクルのポリシーを次のサイトにアクセスして比較できます

- https://www.oracle.com/jp/corporate/security-practices/corporate/

技術的な詳細については、『Oracle Cloud Infrastructureセキュリティ・ガイド』を参照できます

- https://docs.oracle.com/ja-jp/iaas/Content/Security/Concepts/security_guide.htm

ハードウェア、ファームウェア、サプライ・チェーンに対する攻撃の幕開け

アプリケーションとネットワーク境界を保護するだけではもはや不十分

- 攻撃はさらに高度になり、ハードウェアにより深く侵入する
- 環境はさらに複雑になり、分散している
- サーバーのサブコンポーネントは高機能になったが“ソフト”である
  - ハッカーにとってさらに好ましい標的になっている
  - 脆弱性と悪用の可能性がさらに高くなっている
- サプライ・チェーンはリスクにさらされている

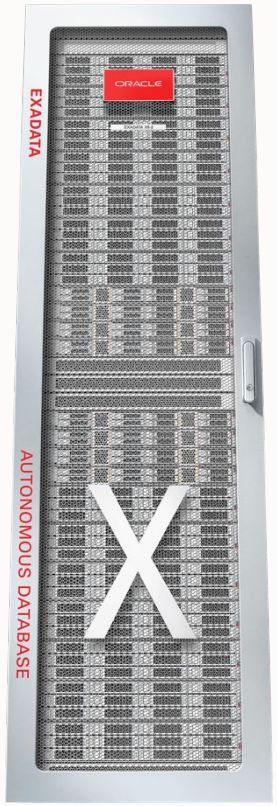
サプライ・チェーン全域に及ぶExadataのエンド・ツー・エンド・セキュリティ

オラクルのサプライ・チェーンは緊密に統合され監視されている

- コアのハードウェアとファームウェアIPの所有権はオラクルが有する
- すべての設計リリースに対しセキュリティ監査を実施する
- サプライヤーはオラクルのセキュリティ・ポリシーを理解し遵守する
- 設計データは暗号化して送信される
- システムの認定テストと検証はオラクルが管理する
- すべてのファームウェアとソフトウェアはデジタル的に署名され認定される
- システムインテグレーションはTrade Agreements Act（TAA）（貿易協定法）に準拠したセキュアな製造工程となる

Exadata Maximum Security Architecture（MSA）のビジョン

究極のパフォーマンス、可用性、セキュリティ



データベースを意識したシステム・ソフトウェア
独自のアルゴリズムでOLTP、分析、統合を大幅に向上

高可用性アーキテクチャ
組込みのOracle MAAベスト・プラクティス

エンド・ツー・エンドのセキュリティ
セキュリティの最適化、セキュリティの集中化、セキュリティの強化

Exadataセキュリティによる付加価値の概要
MSAソリューションのハイライト

- ✓ フットプリントの縮小
- ✓ アクセス制限
- ✓ 最小限の権限付与の原則
- ✓ 監査ルール
- ✓ システム強化
- ✓ ファイルの整合性の監視
- ✓ セキュリティ管理ツール
- ✓ 事前スキャン済みのフル・スタック
- ✓ マルチテナントの分離
- ✓ ブート・デバイスの保護
- ✓ 高速の暗号消去
- ✓ セキュリティ対応Linux
- ✓ メモリ保護鍵

「データベース・インスタンスのプロビジョニング、管理、チューニング、アップグレードの各プロセスを停止時間なしに、完全に自動化するOracle Autonomous Databaseは、**Oracle Databaseに保管された機密データのセキュリティとコンプライアンスを大幅に向上**するだけでなく、そのデータをOracle Cloudに移動する主張に説得力を持たせます。」

KuppingerCole Analysts

より小さいインストール・フットプリント

Exadataは依存関係がないカスタム、**ナノ**、**モノリシック**なカーネルを使用し、サイズを縮小

- デバイス・ドライバの削減
- フットプリントの縮小
- アップグレード時間の改善

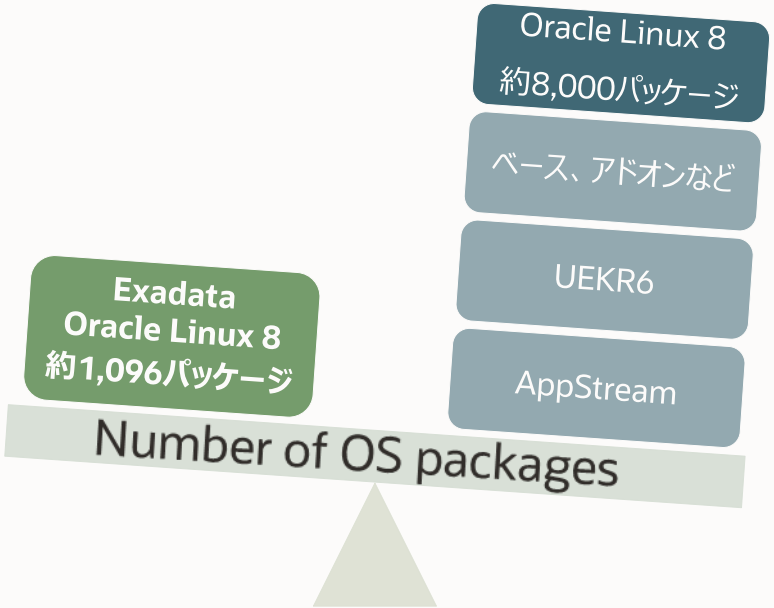
標準的なOracle Linux 8 UEKカーネル：

- kernel-uek-5.4.17-2136.324.5.3.el8uek.x86_64
- ゲスト・カーネル・サイズ：139 MB

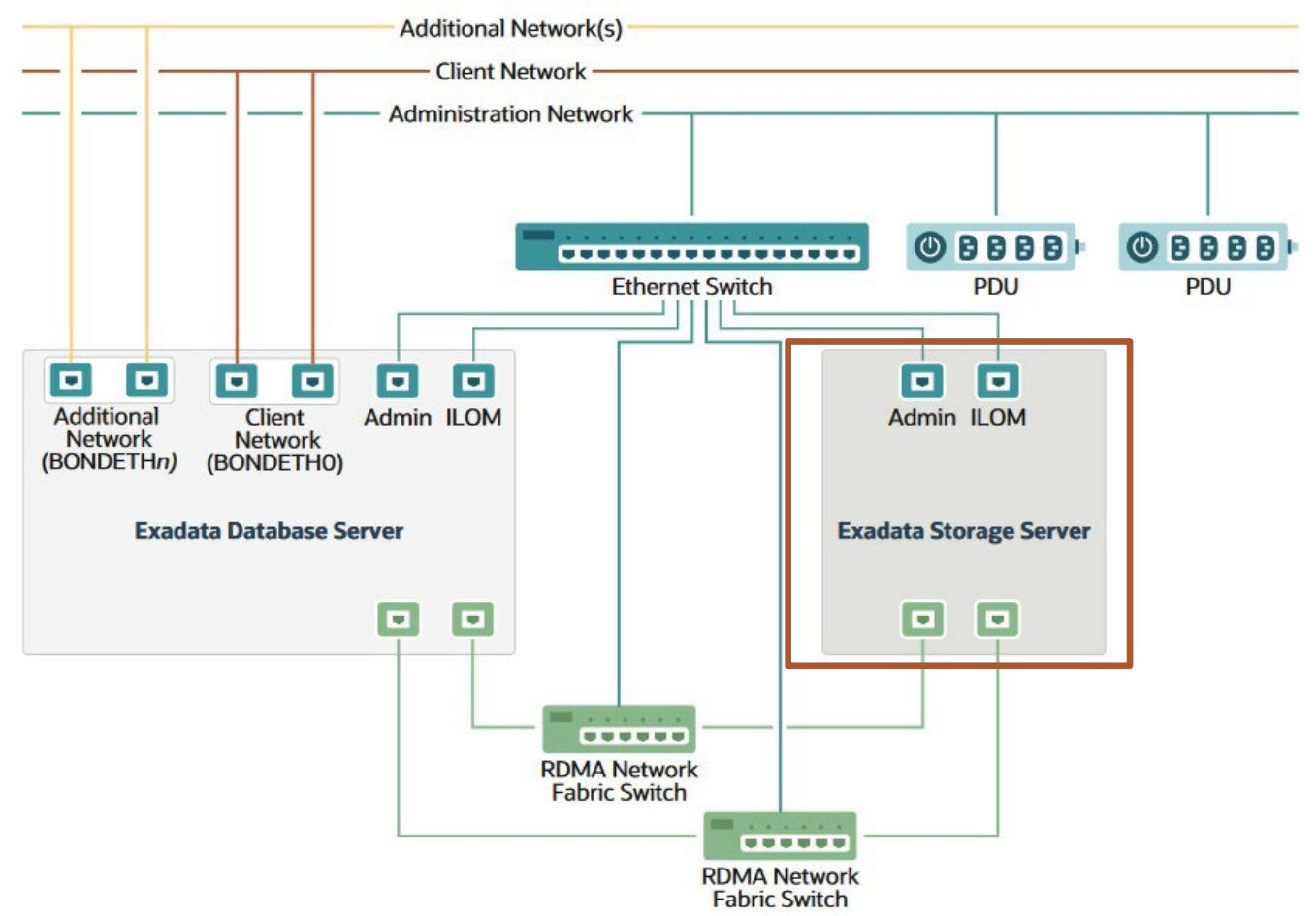
Exadata Software 24ai Oracle Linux 8 UEKカーネル：

- kernel-ueknano-5.4.17-2136.330.7.4.el8uek.x86_64
- ゲスト・カーネル・サイズ：75 MB

Exadataには、Oracleデータベースの実行に特化した必須ソフトウェア・コンポーネントのみが含まれているため、攻撃対象範囲が縮小されます



ストレージ・サーバーへのネットワーク・アクセス



- Oracle Exadata System Softwareには、各ストレージ・サーバーにファイアウォールを実装するcellwallサービスが含まれる
- SSHサーバーは、管理ネットワーク（NET0）とRDMAネットワーク・ファブリック上のみで接続リクエストに応答するように構成されています
- Exadata Storage Serverにクライアント・ネットワークへの直接接続はありません

最小限の権限付与の原則を適用

セキュリティのベスト・プラクティスでは、各プロセスがタスクの実行に必要な最小限の権限で実行されることが必要。
以下のプロセスは非特権ユーザーが実行できるようになりました。

- **Smart Scanプロセス**：Smart Scan条件評価の実行に、root権限は不要
  - cellofl ユーザーおよびcelltraceグループ
- **選択されたExaWatcherプロセス**：iostat、netstat、ps、top、およびその他の情報を収集するExaWatcherコマンドの一部が、rootユーザー権限がなくても実行できるように変更
  - exawatchユーザーおよびexawatchグループ

RESTfulサービスのアクセス制御

Oracle Exadata System Softwareには、アクセス制御を使用してHTTPおよびRESTfulインタフェースへのアクセスを制限する機能が含まれる

- IPアドレスまたはサブネット・マスクのリストを指定して、HTTP経由でのRESTfulサービスへのアクセスを制御
- 使用しない場合、RESTfulサービスを完全に無効にすることが可能

```
# lsof -i -P -n | grep LISTEN | grep java
java       <pid> dbmsvc   55u  IPv4    40193      0t0  TCP *:7879 (LISTEN)

# dbmcli -e alter dbserver httpsAccess=none
This command requires restarting MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating HTTPs access control list.
Starting MS services...
The STARTUP of MS services was successful.
DBServer successfully altered

# lsof -i -P -n | grep LISTEN | grep java
```

オペレーティング・システム・アクティビティの監視

各Exadataサーバーは、auditdを使用して、システムレベルのアクティビティを監査するように構成

- auditctlコマンドを使用して監査を管理し、レポートを生成
- auditdサービスが開始されると、augenrulesユーティリティが実行。このユーティリティは、監査ルール・ディレクトリにあるすべてのコンポーネント監査ルール・ファイルをマージし、マージされた結果を/etc/audit/audit.rulesファイル内に配置
  - Exadata固有の監査ルールは、/etc/audit/rules.d/01-exadata_audit.rulesに保管
  - 顧客のカスタム監査ルールは、/etc/audit/rules.d/20-customer_audit.rulesに保管可能

```
# auditctl -l
-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremove
xattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
…
```

システム・ログ情報（rsyslog）の暗号化

データベース・サーバーおよびストレージ・サーバー上の管理サーバー（MS）は、syslogconf属性をサポート

- syslogconf属性は、データベース・サーバーのsyslogルールを拡張
- この属性を使用して、syslogメッセージを特定のリモートsyslogdサービスに転送するように指定可能
- MS上では、転送されたメッセージは、MSのsyslog構成に応じて、ファイル、コンソール、または管理アプリケーションに送信
- これにより、さまざまなサーバーからのシステム・ログを一元化されたロギング・サーバーに集約してマイニングし、セキュリティ監査やデータ・マイニングなどを行うことが可能

証明書とsyslogconf属性を使用して、syslog情報の暗号化を構成

Oracle Exadata Deployment Assistant（OEDA）

マシンのセキュリティの再設定

初期構成時や、既存のデプロイメントに変更や追加を行う場合にDeployment Assistantを使用して設定。
新しいコンポーネントを追加したり、既存のデプロイメントを変更したりするときに、既存の構成をインポート可能。

- デプロイメント手順である、マシンのセキュリティの再設定の後に初めてホストにログインすると、rootパスワードをリセットするように求められる。
  SSH鍵ベースの認証が有効であり、パスワードベースの認証が無効になっている場合でも同様になる。

パスワードの複雑性の設定	パスワードのエージング設定	パスワードの期限切れ管理	ファイルパーミッションの設定

host_access_control – システム設定

host_access_controlコマンドを介して、デプロイメント後の利用可能な機能とセキュリティ・プランを実装

```
# /opt/oracle.cellos/host_access_control apply-defaults --strict_compliance_only
INACTIVE=0
Deny on login failure count set to 3
Account fail_interval for failed login attempts set to 900
Account unlock_time after {deny} failed login attempts set to 900
Password history set to pam_pwhistory.so 5
Password strength set to pam_pwquality.so minlen=15 minclass=4 dcredit=-1 ucredit=-1 lcredit=-
1 ocredit=-1 difok=8 maxrepeat=3 maxclassrepeat=4 local_users_only retry=3 authtok_type=
PermitRootLogin no
hard maxlogins 10
hmac-sha2-256,hmac-sha2-512 for both server and client
Password aging -M 60, -m 1, -W 7
```

host_access_control – システム設定

コマンドのサブセット

- access - User access from hosts, networks, etc.
- auditd-options - Options for auditd
- banner - Login banner management
- fips-mode - FIPS mode for openSSH
- idle-timeout - Shell and SSH client idle timeout control
- pam-auth - PAM authentication settings
- password-aging - Adjust current users' password aging
- rootssh - Root user SSH access control
- ssh-access - Allow or deny user and group SSH access
- sshciphers - SSH cipher support control
- ssh-macs - SSH supported MACs
- sudo - User privilege control through sudo

事前スキャン済みのフル・スタック

すべてのExadataリリースには、オラクルの内部スキャン・ツールで検出されたゼロデイ脆弱性に対処するセキュリティ修正と緊急修正が含まれる

- 静的/動的コード分析
- マルウェア・スキャン
- サード・パーティ・ソフトウェアのチェック
- 脆弱性スキャン
  - 『How to research Common Vulnerabilities and Exposures (CVE) for Exadata packages』（Doc ID 2256887.1）
- システム強化レビュー（STIG）
  - 『Exadata OL8 System Hardening for STIG Security Compliance』（Doc ID 2934166.1）

顧客は最新リリースにアップグレードするだけで、すぐにこれらの修正を利用できます

- 報告される問題の数は、カスタム構成に比べてはるかに減少

ExadataリリースCY2024

毎月のExadataセキュリティ・ソフトウェア更新：

- セキュリティ修正
- CVEの軽減

リリース	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
22.1.0* (OL7)	**22.1.19**	22.1.20	22.1.21	**22.1.22**	22.1.23	22.1.24	**22.1.25**	22.1.26	22.1.27	**22.1.28**	22.1.29	22.1.30
23.1.0* (OL8)	**23.1.10**	23.1.11	23.1.12	**23.1.13**	23.1.14	23.1.15	**23.1.16**	23.1.17	23.1.18	**23.1.19**	23.1.20	23.1.21
24.1.0 (OL8)					24ai	24.1.1	**24.1.2**	24.1.3	24.1.4	**24.1.5**	24.1.6	24.1.7

今後のリリースと日付については見込みにすぎません

* ソフトウェア・リリース更新は2025年に終了します

28,823

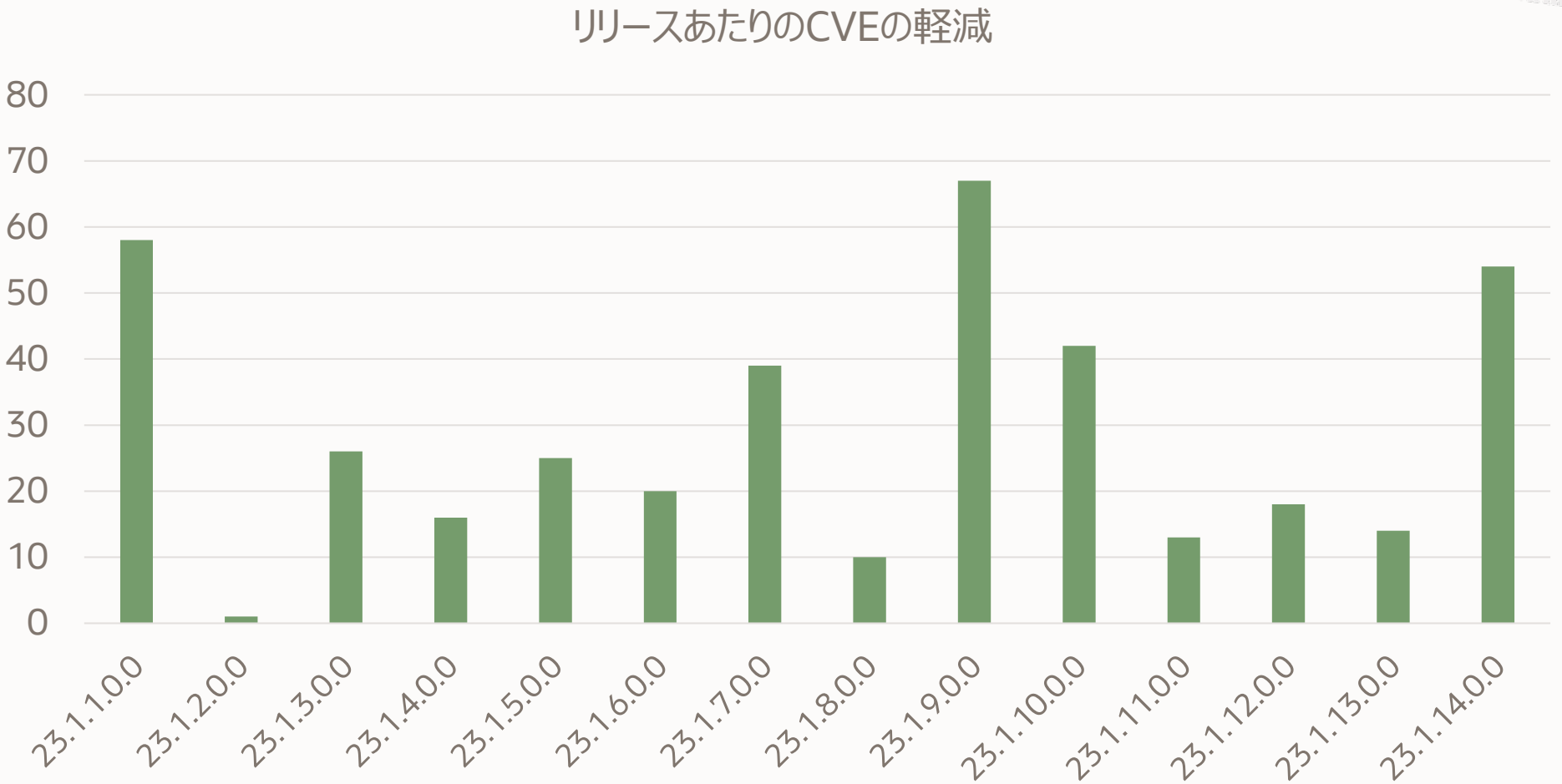
2023年に国際IT市場で発行された共通脆弱性識別子（CVE）IDの数

1日あたりでは約79件!

Exadataセキュリティによる付加価値：

- スキャン済みのイメージ
- 毎月のリリース

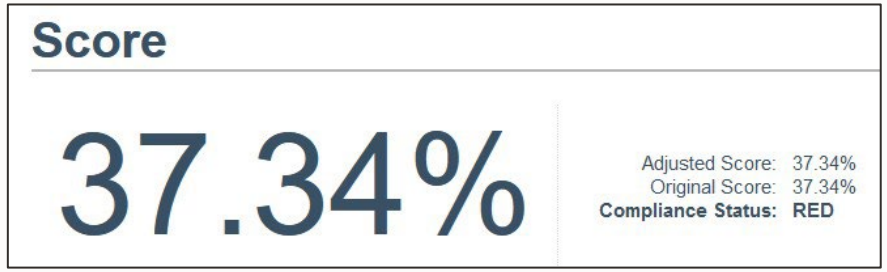
Exadata 23.1.xにおけるOracle Linux CVEの軽減



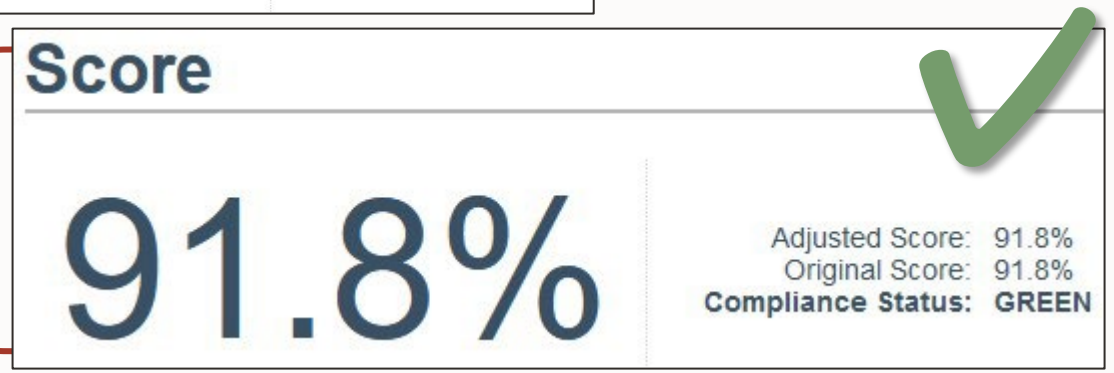
STIG SCAP Oracle Linux 8の高いベンチマーク
Exadata System Software 24aiは工場出荷時から安全

“Oracle Linux 8のセキュリティ技術導入ガイド（STIG）は、米国国防総省（DoD）情報システムのセキュリティを向上するためのツールとして公開されています”

標準のLinuxインストール



デプロイされたExadata KVMゲスト



Exadataの新規（および既存）のセキュリティ機能

セキュリティとパフォーマンスを最大化した最大限の可用性

Exadataライブ・アップデート

Exadata Software 24aiの新機能

Exadataライブ・アップデートは、RPMやkspliceなどの標準Linuxテクノロジーに基づくオンライン更新機能を使用

- 更新の特定の内容によっては、データベースの中断やサーバーの再起動をせずに更新操作が実行される場合がある。

オンラインで完了できない更新項目は、その後のサーバー再起動中に完了するようにステージングされる

- 未処理の項目は、特定の時刻、または次回の正常なサーバー再起動中に完了するようにスケジュール可能
- 未処理の項目については、無期限に延期することも選択可能

Exadataライブ・アップデートは、既存のExadataユーザーには簡単で使い慣れた操作感で使用できるExadata patchmgrユーティリティで制御可能

https://docs.oracle.com/cd/G37198_01/dbmmn/index.html

Exadataライブ・アップデート

Exadataライブ・アップデートでは、共通脆弱性評価システム（CVSS）に基づいて、セキュリティ問題に対処するための部分更新が可能。Exadataライブ・アップデートを使用する場合は、以下のオプションから選択する必要があります。

- highcvss：重大レベルのセキュリティ更新のみを実行し、CVSSスコアが7以上の脆弱性に対処
  - 高または重大レベルのセキュリティの軽減が含まれているすべての新しいパッケージ
- allcvss：セキュリティ更新のみを実行し、CVSSスコアが1以上の脆弱性に対処
  - あらゆるセキュリティの軽減（低、中、高、重大）が含まれているすべての新しいパッケージ
- full：セキュリティ関連のあらゆる更新とセキュリティ以外の他のあらゆる更新を含む、完全更新を実行
  - イメージ内のすべての新しいパッケージ

Exadataライブ・アップデート

patchmgrコマンドでExadataライブ・アップデートを実行

```
# ./patchmgr --dbnodes dbs_group --upgrade --repo <path>exadata_ol8_ 24.1.0.0.0.240517.1
_Linux-x86-64.zip --target_version 24.1.0.0.0.240517.1 --log_dir auto --live-update-target
allcvss
```

Exadata 23.1.xとライブ・アップデートからの24.1.0.0.0へのimagehistory出力は以下のようになります。

```
Version                                 : 23.1.1.0.0.230422
Exadata Live Update Version             : 24.1.0.0.0. 240517.1 (all) (CVSS 1-10) (Live Update
applied. Reboot at any time to finalize outstanding items.)
```

KVMゲストのセキュア・ブート

Exadata Software 24aiの新機能

セキュア・ブートは、システムをブートするために実行できるバイナリを制限するために使用される方法

Oracle Exadata System Softwareは、セキュア・ブートをOracle Linux KVMゲストまで拡張

- KVMゲストのセキュア・ブートは、Oracle Linux KVMのUEFIブート・フレームワークを利用して、KVMゲストをブートできるバイナリを制限し、信頼できるエンティティの暗号化署名を持つブート・ローダーのみを許可
- KVMゲストをリブートするたびに、ブート・シーケンス内のすべてのコンポーネントが検証される
- この機能により、マルウェアがブート・チェーンに埋込みコードを忍び込ませることを防止
  - ブート・セクター・マルウェアやカーネル・コードのインジェクションを防ぐことを意図
  - ハードウェアベースのコード署名

https://docs.oracle.com/cd/G37198_01/dbmsq/index.html

RESTfulサービスのリスニング・インタフェース

Exadata Software 24aiの新機能

listeningInterface 属性は、Exadata RESTfulサービスを使用してコマンドをリスニングするネットワーク・インタフェースを指定

- listeningInterface には以下の値が指定できます。ALL、NONE、またはネットワーク・インタフェースのリスト
- listeningInterface 属性は、httpsAccess属性を補完
  - listeningInterface 属性は、どのサーバー・ネットワーク・インタフェースがRESTリクエストを受け入れるかを指定し、httpsAccess属性は、リクエストのソースをExadata RESTfulサービスに制限する

```
# lsof -i -P -n | grep LISTEN | grep java
java       63902  dbmsvc   34u  IPv6    157781       0t0  TCP *:7879 (LISTEN)
# dbmcli -e alter dbserver listeningInterface=vmeth0
This command will automatically restart and redeploy MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating attribute "listeningInterface" before redeploying MS.
Starting MS services...
The STARTUP of MS services was successful.
DBServer scaqal04adm05 successfully altered
# lsof -i -P -n | grep LISTEN | grep java
java      237672  dbmsvc   34u  IPv6 308318206       0t0  TCP <ipaddress>:7879 (LISTEN)
```

https://docs.oracle.com/cd/G37198_01/dbmmn/index.html

https://docs.oracle.com/cd/G37198_01/sagug/index.html

SNMPのセキュリティ機能強化

Exadata Software 24aiの新機能

SNMP V3は、汎用サブスクライバ（type=v3）およびOracle Auto Service Request（ASR）サブスクライバ（type=v3ASR）に対してサポートおよび推奨されています。

- SNMP V1（type=v1）およびOracle ASR（type=ASR）の元のタイプ定義は引き続き使用できるが、推奨されていない
- すべてのSNMP V1（type=v1）およびOracle ASRサブスクライバ（type=ASR）に対して、管理者はSNMPコミュニティを指定する必要があります（public および private のcommunity strings は非推奨）。
- すべてのSNMP V3サブスクライバ（type=v3またはtype=v3ASR）に対して、SHA2認証プロトコルのSHA-224、SHA-256、SHA-384、SHA-512を使用可能

```
# cellcli -e alter cell snmpuser='((name=user01,authprotocol=SHA-512,authpassword=*))'
snmpUser user01 authpassword: ********
Confirm snmpUser user01 authpassword: ********
Cell <host> successfully altered
# cellcli -e alter cell snmpSubscriber='((host=localhost,port=162,type=V3,snmpUser=user01))'
snmpSubscriber ((<host>,port=162,community=public,type=asr,asrmPort=16161)) has been replaced with
((host=localhost,port=162,snmpUser=user01,type=V3)).
Cell <host> successfully altered
```

https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/index.html

Database 23aiのセキュリティ機能強化

Exadata Software 24aiの新機能

Database 23aiの以下の新機能がExadata Software 24aiで透過的に使用できるようになりました。

- AES-XTS暗号化データでのSmart Scan
  - Oracle Exadata System Softwareリリース24.1.0は、Oracle Database 23aiと連携することで、AES-XTSを使用して暗号化された表領域内のデータに対してExadata Smart Scanを透過的に有効化可能に
  - AES-XTSは、TDEが並列処理とプロセッサ・ハードウェアに組み込まれた特殊命令を利用できるExadata上で特に、セキュリティとパフォーマンスの向上を実現する。
- オンライン暗号化中のSmart Scan
  - Exadata Smart Scanは、長時間実行されるオンラインの暗号化、復号化、および鍵の再設定の操作中には、完全に有効な状態を維持。
  - 以前は、このような操作中、Exadata Smart Scanは無効になっていた。

https://docs.oracle.com/cd/G37198_01/dbmso/whats-new-oracle-exadata-system-software-release-24.1.html

Oracle Linux 8

Oracle Exadata System Software 23.1.0以降は、UEK6カーネルを含むOracle Linux 8を使用

- ストレージ・サーバー、ベアメタル・データベース・サーバー、KVMホスト/ゲスト、OVMゲスト（DomU）
  - OVM管理ドメイン（Dom0）は、UEK5カーネルのOracle Linux 7を引き続き使用
- Oracle Linux 7からOracle Linux 8へのローリング・アップグレードをサポート

Oracle Linux 8の重要なセキュリティ機能：

- さまざまなSELinuxの改善
- TLS、IPSec、SSH、DNSSec、Kerberosプロトコルに対応した暗号化ポリシー
- Diffie-Hellmanパラメータのモジュール・サイズを2048ビットに変更
- DSA公開鍵アルゴリズムをデフォルトで無効化
  - 『How to setup RSA SSH equivalence on Oracle Exadata nodes』 （Doc ID 2923095.1）
- ssh-keygenツールのデフォルトRSA鍵サイズを3072ビットに拡大

一元化されたOSユーザーの識別と認証

データベースおよびストレージ・サーバーによるサポート

- LDAP ID管理システム
- Kerberos認証
- Linuxシステム・セキュリティ・サービス・デーモン（SSSD）
  - Exadata専用のカスタム・セキュリティ・プロファイルを事前に構成
  - アップグレード後もカスタマイズを維持

アカウントの一元管理によるセキュリティの強化

- プロビジョニング/デプロビジョニング管理が容易
- パスワード管理が容易
- エンタープライズ・セキュリティ制御

参考資料：

- How to configure Kerberos and SSSD-KCM in Exadata compute nodes and cells（Doc ID 2948255.1）
- LDAP configuration example in Exadata compute nodes and storage servers using SSSD（Doc ID 3020122.1）

Security Enabled Linux（SELinux）

Linuxカーネルに対するSELinuxの機能強化では、Mandatory Access Control（強制アクセス制御（MAC））ポリシーが実装。これにより、すべてのユーザー、プログラム、プロセス、ファイル、デバイスに対してきめ細かなアクセス許可を提供するセキュリティ・ポリシーを定義可能。

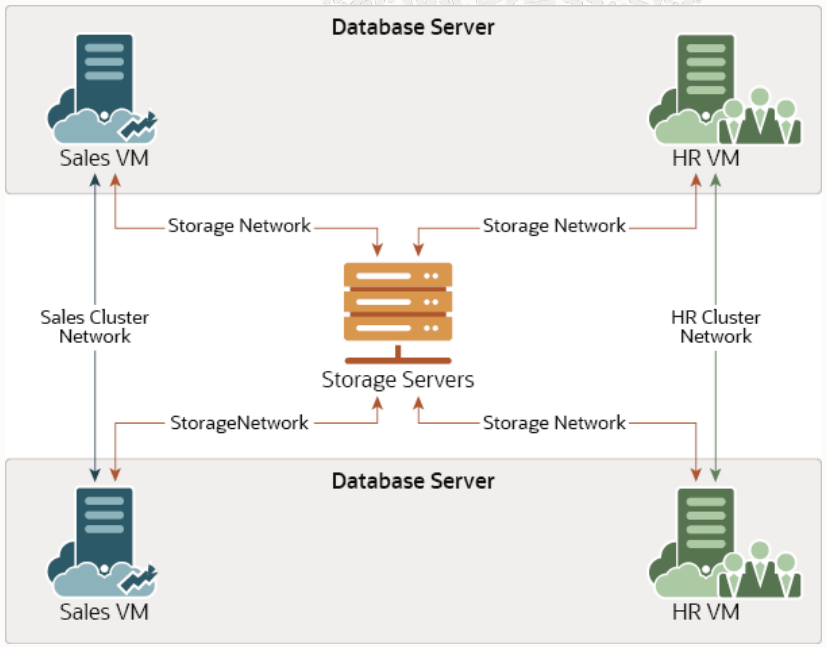
- enforcingモードに移行する前に、システムをまずpermissiveモードにして、Access Vector Cache（AVC）拒否に対処する必要があるかどうかを確認する必要がある。

```
# /opt/oracle.cellos/host_access_control selinux --help
Options:
  -h, --help        show this help message and exit
  -e, --enforcing   set the SELinux state to enforcing
  -p, --permissive  set the SELinux state to permissive
  -d, --disabled    set the SELinux state to disabled (Exadata default)
  -r, --relabel     Set the system for relabling
  -c, --config      Display the configured SELinux state
  -s, --status      Display the current SELinux status
```

RoCE環境でのExadata Secure RDMA Fabric Isolation

RoCE向けのExadata Secure Fabricシステムでは、
共有のExadata Storage Serverへのアクセスを許可しながら、
仮想マシンのネットワーク分離を実装

- 各Exadata VMクラスタにプライベート・ネットワークが割り当て
- VMは相互通信不可能
- すべてのVMは共有ストレージ・インフラストラクチャと通信可能
- ネットワーク分離のセキュリティ機能の迂回は不可能
  - すべてのパケットのネットワーク分離のセキュリティ機能はネットワーク・カードによって実施
  - ルールはハイパーバイザによって自動設定



ExadataデータベースノードのOracle Linuxカーネル/SSHにおけるFIPS 140-2

/opt/oracle.cellos/host_access_control fips-mode –enable

- カーネル設定 - 再起動が必要
  - STIGの軽減：Oracle Linuxオペレーティング・システムは、適用される連邦法、大統領令、指令、ポリシー、規制、標準に従った、デジタル署名のプロビジョニング、暗号ハッシュの生成、保管中のデータ保護が必要なデータの保護において、NIST FIPSで認められた暗号化を実装する必要がある。
  - STIGの軽減：Oracle Linuxオペレーティング・システムは、SSH通信において、FIPS 140-2で承認された暗号アルゴリズムを使用する必要がある。

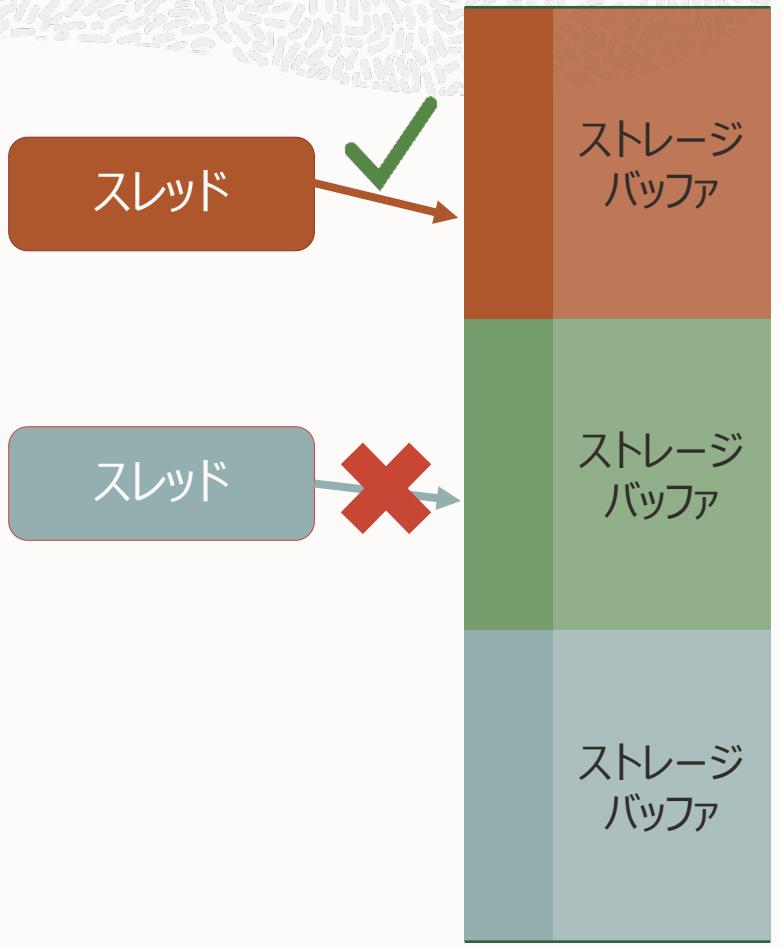
/opt/oracle.cellos/host_access_control ssh-macs –secdefaults

- SSHコントロール
  - STIGの軽減：Oracle Linuxオペレーティング・システムは、SSHデーモンが、FIPS 140-2で承認された暗号ハッシュ・アルゴリズムを使用するメッセージ認証コード（MAC）のみを使用するように構成される必要がある。

Memory Protection Keys（メモリ保護キー：MPK）を使用したストレージ・サーバー・プロセスの保護

Exadata Storage Server Softwareメモリは16色でパーティション化さ

- 色を識別するために使用される各ページ表エントリの4ビット
- 各スレッドは、一致する色の読取り/書込みおよび有効化/無効化が許可されている
- 正しい色を持たないメモリにアクセスすると、プロセスがトラップされる
- 不注意によるソフトウェアの欠陥から保護する
- 調整不要ですぐに有効にできる
- 潜在的なメモリ破損のクラスを排除する



ストレージ・サーバーにおけるその他のセキュリティ・プロセス

Oracle Linuxカーネルのセキュアなコンピューティング（seccomp）機能を使用して、発行できるシステム・コールを制限可能

- カーネルには何百ものシステム・コールがあり、そのほとんどは特定のプロセスでは不要
- seccompフィルタは、システム・コールを許可するかどうかを定義
- seccompフィルタがセル・サーバー用にインストールされており、アップグレード時にプロセスを自動的にオフロード
- システム・コールのホワイトリスト・セットは、これらのプロセスから作成することが許可
- seccompにより引数の追加検証が実行

SSHの無効化

- ストレージ・サーバーはSSHアクセスから“ロックされる”場合がある
- ExaCLIは引き続き操作の実行に使用可能
  - HTTPSおよびREST APIを使用して、サーバー上で実行されているWebサービスと通信
  - 必要に応じて、運用アクセスのために一時アクセスを有効化も可能

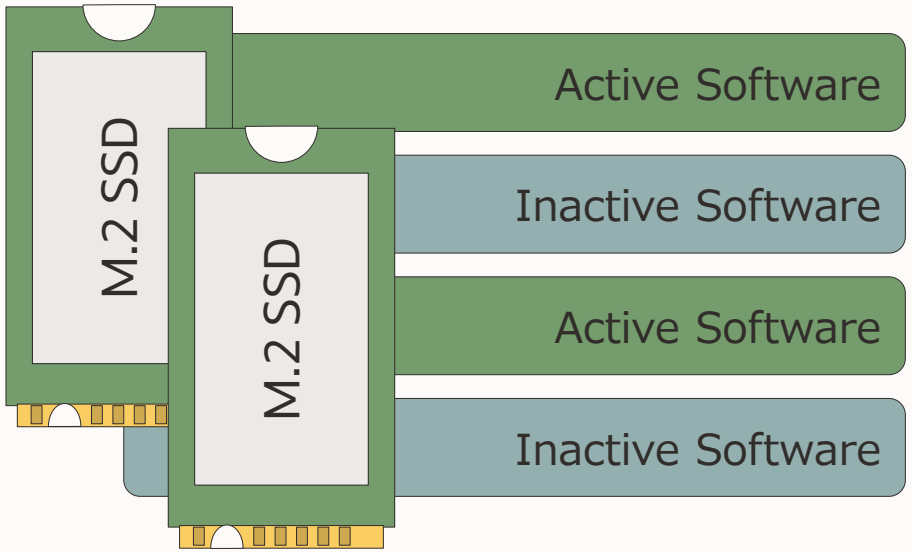
ストレージ・サーバーのパーティションへのインストール

Exadataはシステム/ソフトウェアを代替パーティションにインストール

- 新しいバージョンにアップグレードすると、ソフトウェアは非アクティブなパーティションにインストールされ、そのパーティションから起動される

アップグレードのたびに完全なOSのリフレッシュが確実に実行されるため、感染ファイルの伝播を最小限に抑えることが可能。
OSデータはデータベース・データとは別に保管

- データベースはOSが破損したとしても安全



Advanced Intrusion Detection Environment（AIDE）

Exadataシステム上のファイルへの不正アクセスを防止

- AIDEはシステム上にあるファイルのデータベースを作成し、そのデータベースを使用してファイルの整合性を確保し、システムへの侵入を検出

```
# /opt/oracle.SupportTools/exadataAIDE -status
AIDE: daily cron is currently enabled.

To add additional rules:
Edit the file /etc/aide.conf

Update the AIDE database metadata.
# /opt/oracle.SupportTools/exadataAIDE -u
```

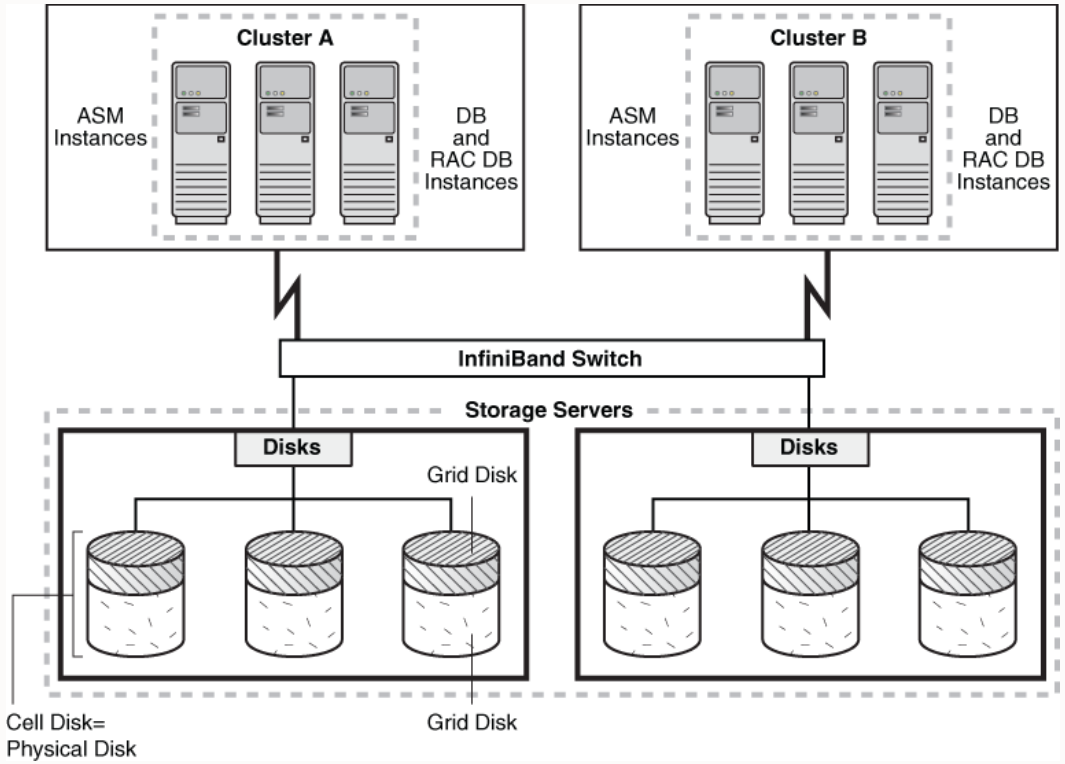
データベース・サーバーとストレージ・サーバーのセキュア・ブート

セキュア・ブートは、システムをブートするために実行できるバイナリを制限するために使用される方法

- セキュア・ブートを使用すると、システムのUEFIファームウェアは、信頼できるエンティティの暗号化署名を持つブート・ローダーの実行のみを許可
- サーバーの再起動のたびに、実行されるすべてのコンポーネントが検証される
- そのため、マルウェアがブート・チェーンに埋込みコードを忍び込ませることはできない
  - ブート・セクター・マルウェアやカーネル・コードのインジェクションを防ぐことを意図
  - ハードウェアベースのコード署名
  - UEFIファームウェア・アーキテクチャの拡張
  - UEFIファームウェアを通じての有効化または無効化が可能

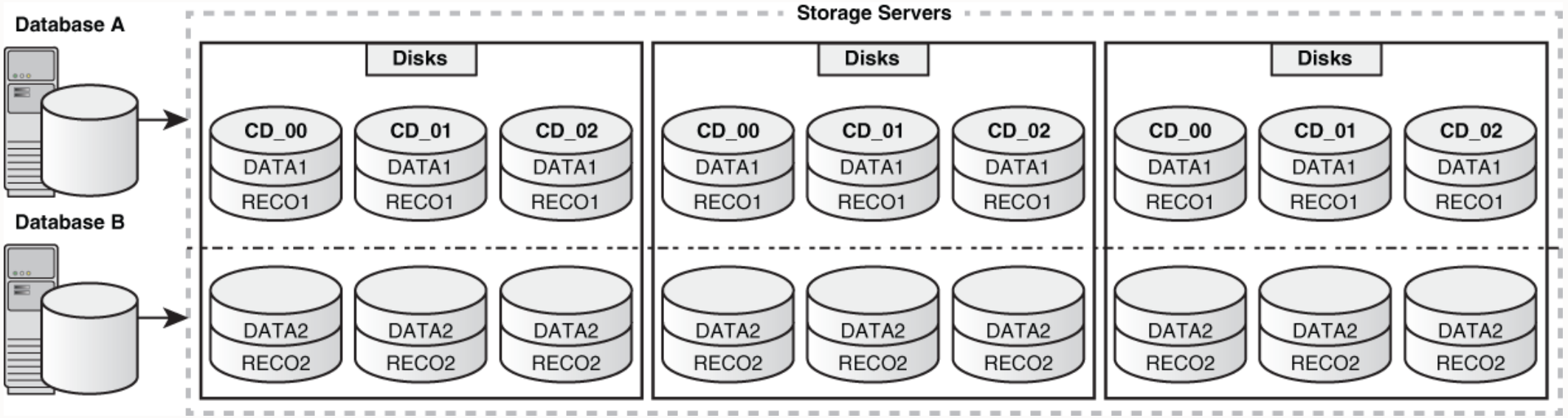
ASM-Scoped Security

Oracle ASMクラスタに関連付けられたOracle ASMディスク・グループが使用するグリッド・ディスクのみにアクセスを制限可能



DB-Scoped Security

Oracle Databaseインスタンスが特定のグリッド・ディスク一式にのみアクセスが制限される



「Oracle Exadata Cloud@Customerは、当社のデータセンターで提供されるクラウド・サービスでOracle Databaseの優れたテクノロジーを使用しており、地域創生クラウドにおける当社のデータ主権やコンプライアンスに関する要件をすべて満たしています。」

西日本電信電話株式会社（NTT西日本）
ビジネス営業本部
アドバンストアドバンストソリューション営業部名古屋支店

千田敬人氏

セキュリティのベスト・プラクティス

システムのセキュリティのレベルは、全体の中でもっとも脆弱な箇所のレベルにしかなりません

- システムの所有者が定期的なスキャンを実行して、提供された構成から一切逸脱していないことを確認する必要があります
- ソフトウェア更新を最新のものにしておくことで、最新のセキュリティ脆弱性が確実に軽減されます
- セキュアな環境の構築を支援するツールやプロセスが備えられていますが、それらは必ず使用してください

Secure Eraser

セキュアな消去ソリューションをOracle Exadata Database Machine内のすべてのコンポーネントに提供します

- 可能であればいつでも暗号消去が使用され、これはNIST SP-800-88r1標準に完全に準拠している

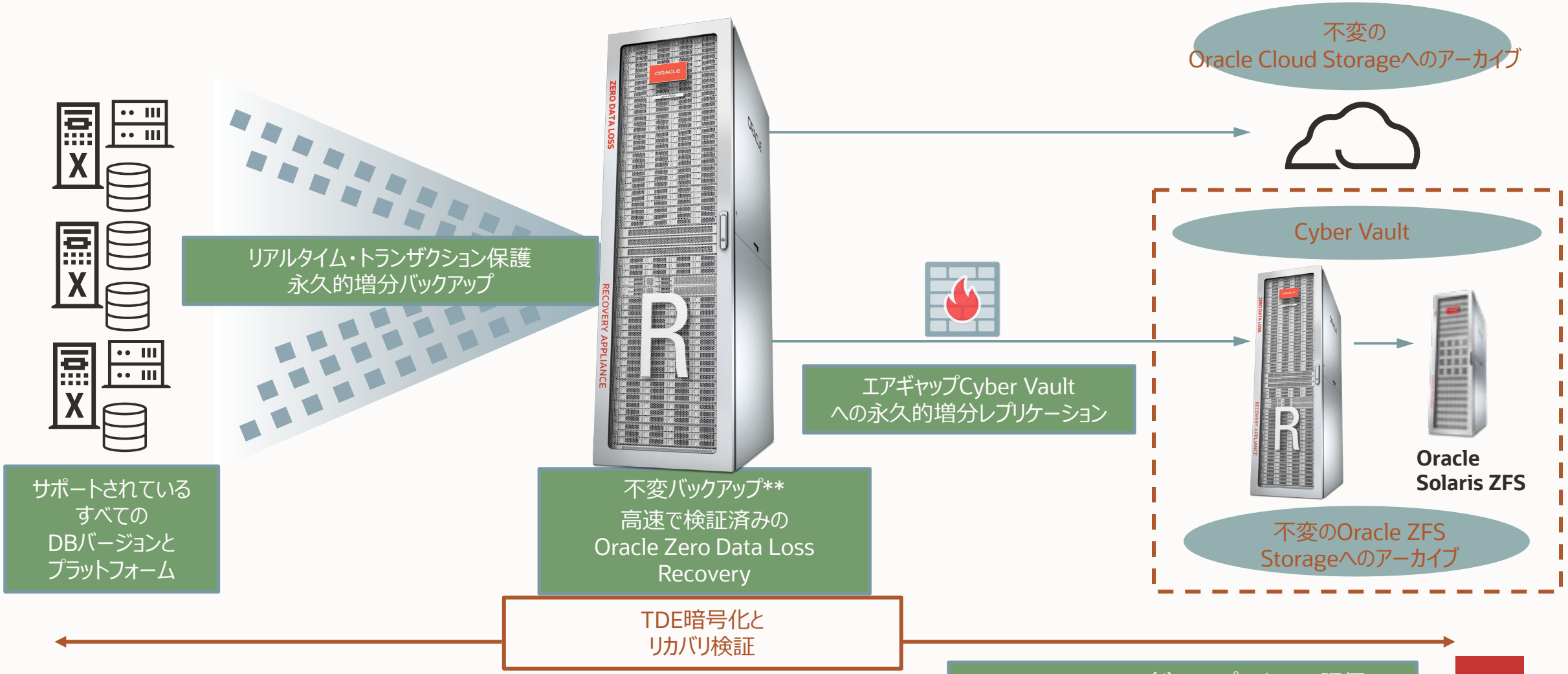
コンポーネント	モデル	消去方法
ハード・ドライブ	• Oracle Exadata Database Machine X5における8 TBハード・ドライブ • Oracle Exadata Database Machine X6以降におけるすべてのハード・ドライブ	暗号消去
ハード・ドライブ	他のすべてのハード・ドライブ	1/3/7パス消去
フラッシュ・デバイス	Oracle Exadata Database Machine X5以降におけるフラッシュ・デバイス	暗号消去
フラッシュ・デバイス	他のすべてのフラッシュ・デバイス	7パス消去
M.2デバイス	Oracle Exadata Database Machine X7-2以降	暗号消去

ランサムウェア保護

セキュリティとパフォーマンスを最大化した最大限の可用性

Recovery Appliance：エンド・ツー・エンドのデータベース保護

サイバー・リカバリ向けに設計：トランザクション保護 + レジリエンスがあるリカバリ + Cyber Vault



リストア能力の保護

リカバリのフレームワークの構築

Oracle Zero Data Loss Recovery Appliance（Oracle ZDLRA）

クラス最高のバックアップとリカバリ

- 業界トップクラスのリストア時間
- ネットワークからは見えない - ファイルシステムは非公開
- ホストはAPIコマンド・セットでOracle ZDLRAにアクセス
- エアギャップされたCyber Vaultをサポートし、さらに高いレベルの保証を実現
- アクセス管理と認可制御（職務の分離/管理者の投票）

運用効率

- 毎週の全体バックアップは不要 - 本番環境のオーバーヘッドを排除
- 永久的増分戦略による、バックアップ期間の短縮
- 影響のない継続的なデータベース・リカバリ検証をすべてのバックアップに対して実施
- きめ細かなリカバリ・ヘルス・ダッシュボードによりデータ保護に関する深い洞察を獲得

ランサムウェアに対抗できるレジリエンス

- 最適化されたバックアップにより、高速でデータ損失ゼロのリカバリを実現
- ポリシーレベルのデータベース保持ロックでバックアップを保護

Oracle Zero Data Loss Autonomous Recovery Service（Oracle ZRCV）

クラウドの簡素性

- データ損失ゼロを維持しながら大規模なデータベース保護を迅速に構成
- データベース固有のバックアップ消費メトリックを使用してコストを制御

ランサムウェアに対抗できるレジリエンス

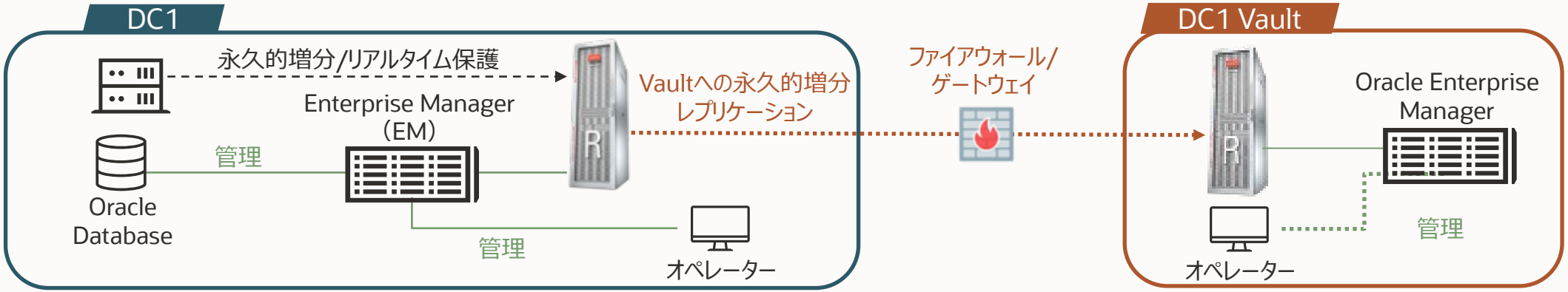
- データ盗難を防止するための自動化された強制暗号化

代替ソリューション

- Oracle Database Backup Cloud Service
- エアギャップされたオフラインのメディア（リムーバブル・ドライブなど）
- 磁気テープなどのストレージ・メディアへのオフライン・バックアップ

Recovery Appliance Cyber Vaultの構成

ランサムウェアからの保護のために、隔離されたエアギャップ・バックアップ・コピーをVaultに作成



Cyber VaultにデプロイされたRecovery Appliance – レプリケーション・トラフィックへの外部ネットワーク・アクセスを制限

- ‘エアギャップ’を作成するためにファイアウォール/ゲートウェイによって制御される、Vaultへのネットワーク接続

データベースをリアルタイムで保護 – 最新のバックアップを常にVaultにレプリケートできる状態にします

- 永久的増分レプリケーションにより、ユーザーが決定したスケジュールでVaultアプライアンスを同期する
- エアギャップが開いており、全体バックアップではなく増分変更のみをレプリケートするため、侵入の可能性が最小限に抑えられる

Vault Applianceのバックアップを個別に検証 - 転送中およびローカルのバックアップの問題を検出

アクセス制御とEnterprise Managerはゾーンごとにサイロ化されており、構成全体にアクセスできる単一のアカウントはありません

クラウドへのRecovery Applianceのアーカイブ

優れたコスト効率で長期保存とコンプライアンスを実現するバックアップ・ストレージ層

OCI Database Backup Cloud Serviceと統合されたRecovery Appliance

- オラクルが管理する無制限のクラウド・ストレージ層を活用
- 管理された環境でのテープ・ボールティング・サービスを排除

Oracle Cloudのバックアップは標準のOracle Recovery Manager（Oracle RMAN）形式を使用しており、クラウドから直接完全にリストア可能です

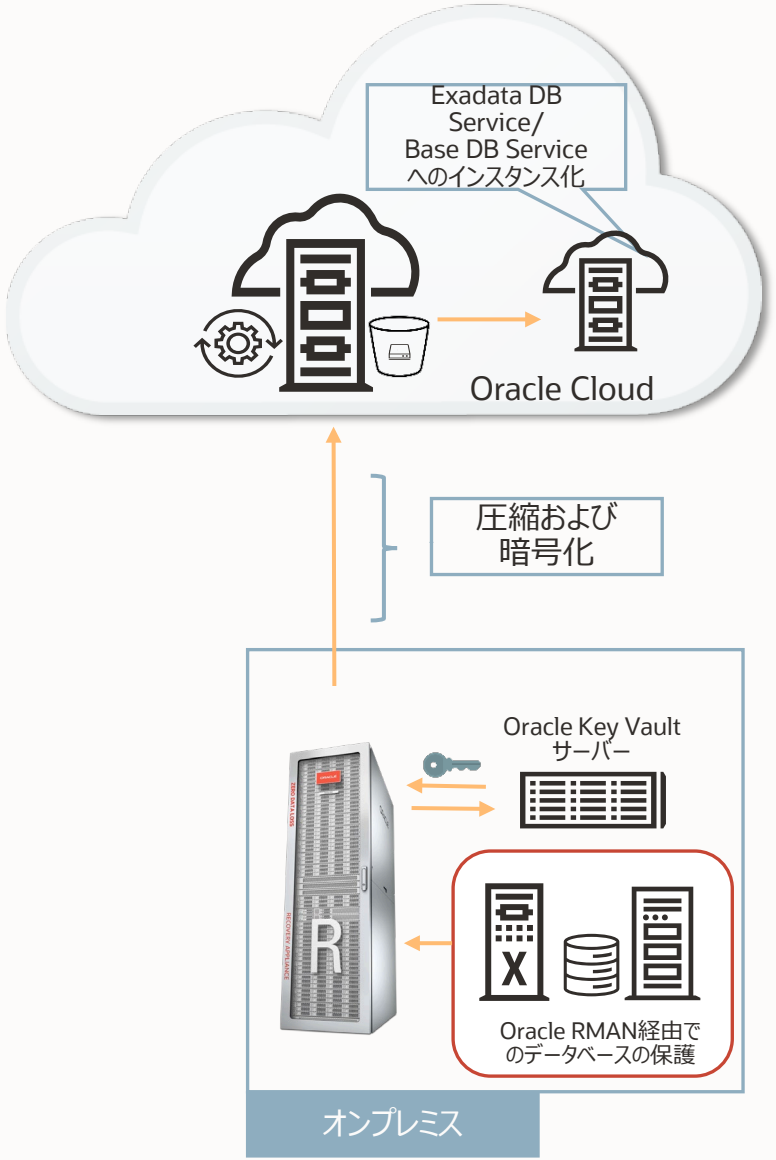
- 新しいOCIデータベースを迅速にプロビジョニング – クラウドへの移行を加速

アーカイブ・バックアップは暗号化されます

- Oracle Key Vaultを鍵管理に活用
- 保護ポリシーによりアーカイブ操作が促進され、保存期間が延長

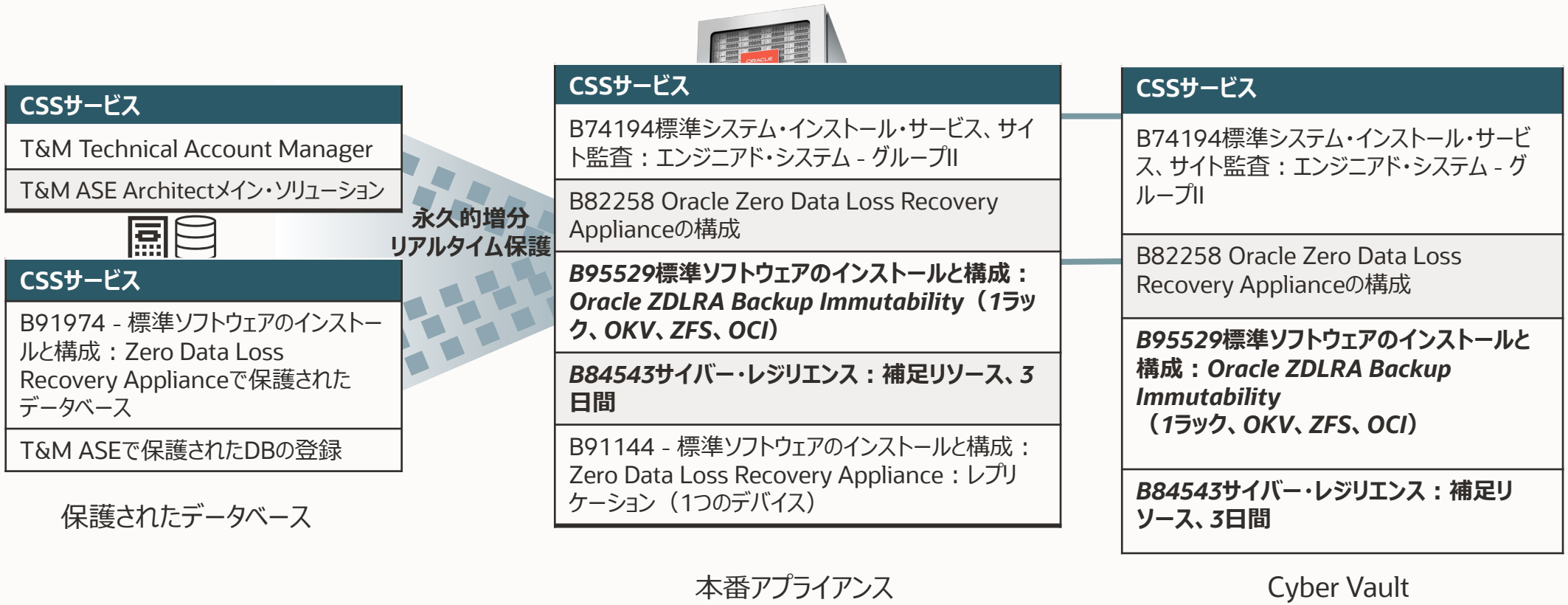
統合されたOCI規制コンプライアンス・バケットを介して不変のアーカイブ・バックアップを適用します

OCI Object Storageのアーカイブ先としてZFSもサポートします



Oracle Customer Success Services for Recovery Appliance

ランサムウェア攻撃からデータベースを防御およびリカバリするために構築



詳細情報：[Oracle ZDLRAサービス・データ・シート]

セキュリティに関する参考資料

Oracle Exadata Database Machine Security FAQ

- My Oracle Support（MOS）Note：Doc ID 2751741.1

オラクルの企業セキュリティ慣行

- https://www.oracle.com/jp/corporate/security-practices/

Critical Patch Updates, Security Alerts and Bulletins

- https://www.oracle.com/technetwork/topics/security/alerts-086861.html

オラクルの企業セキュリティ慣行

- https://blogs.oracle.com/security/

OracleのExadataドキュメント

- https://docs.oracle.com/cd/G37198_01/books.html


ORACLE