Oracle Direct Seminar

ORACLE

データベースの暗号高速化テクノロジーとその活用方法とは

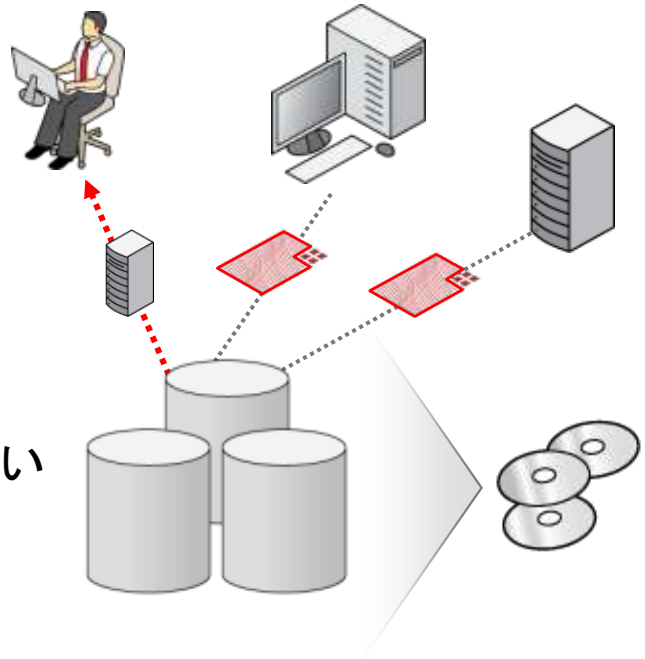
日本オラクル株式会社　テクノロジー製品事業統括本部
シニアエンジニア ,CISSP　西村克也

Oracle Direct

Oracle Direct Seminar

そもそも、データベースの暗号化は何のため？

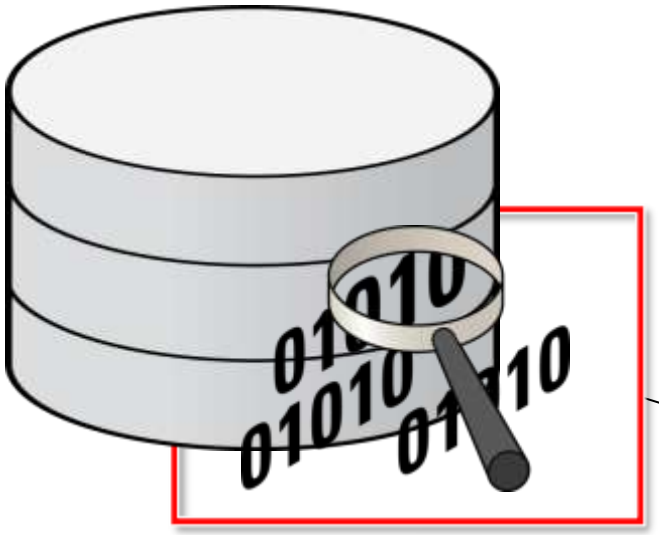
- どういった脅威があるのか？
  - データベースとの通信の**盗聴**
  - データベースに関連するファイルの**盗難**
  - バックアップメディアの**盗難・紛失**



- 暗号化するとどうなるのか？
  - パケットキャプチャしても通信内容は分からない
  - Oracleのファイルをバイナリレベルで読み取れない

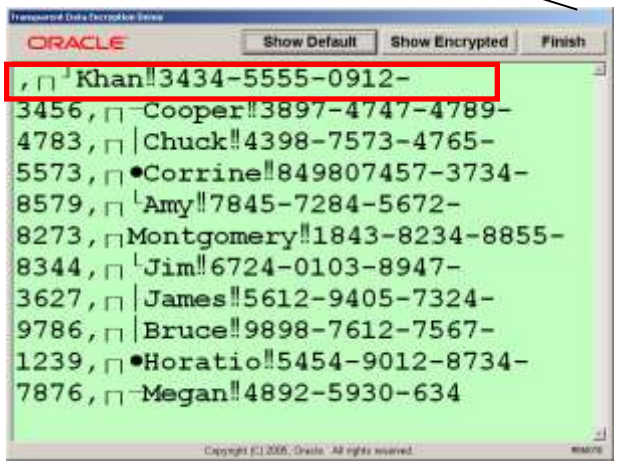
- ただし・・
  - 暗号化はデータベース・セキュリティの一部
  - 認証、アクセス制御と組み合わせることで効果倍増

データファイルを直接参照する脅威



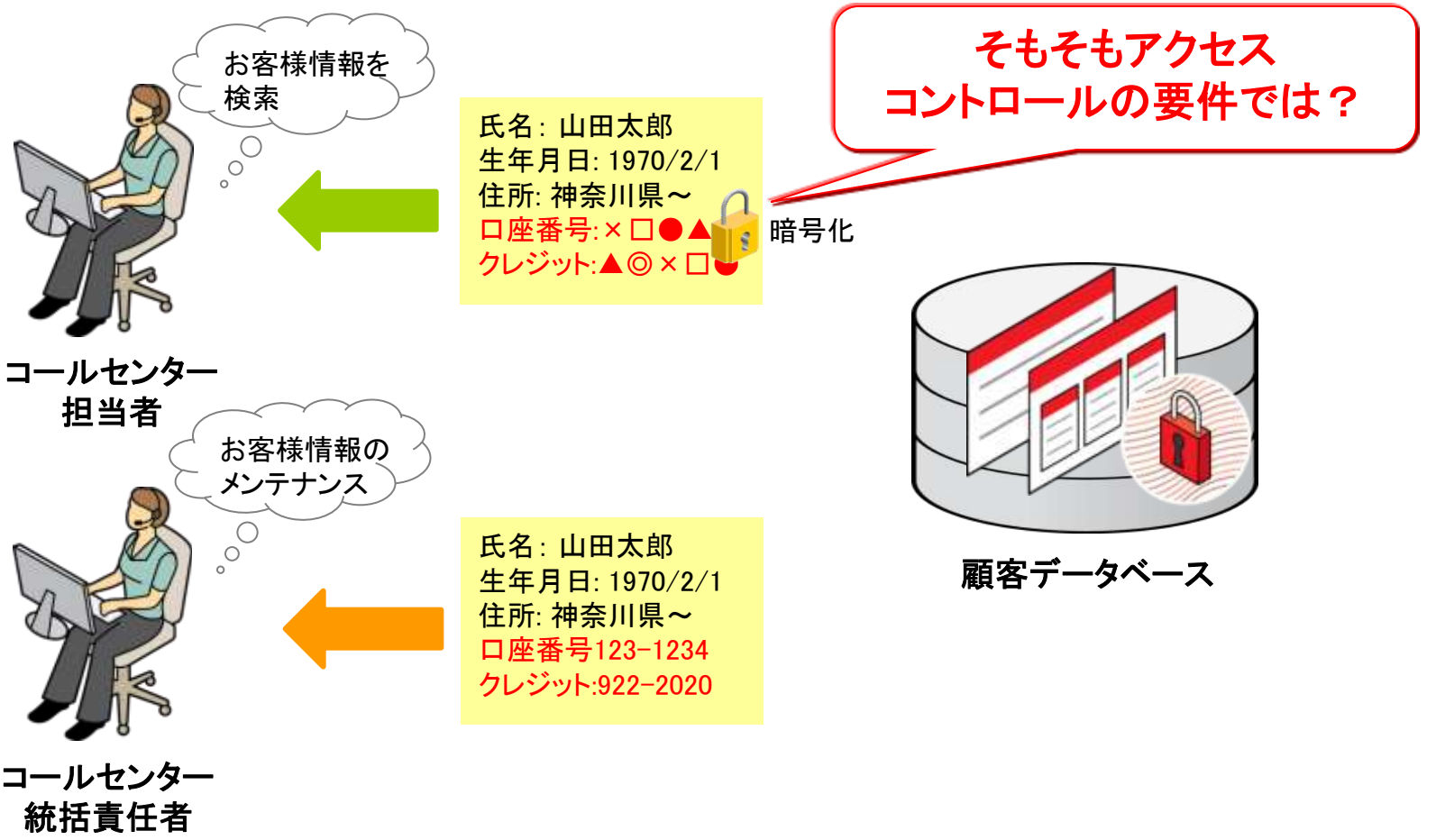
データベース上の物理ファイル
- データファイル
- Redo ログファイル
- アーカイブログファイルなど

悪意のあるユーザによって
物理ファイルを直接アクセス
クラッキングツールにより解読される！



良くある質問

- データベースを暗号化すると、ユーザに応じて暗号化されたデータが表示されるようになるんですよね？

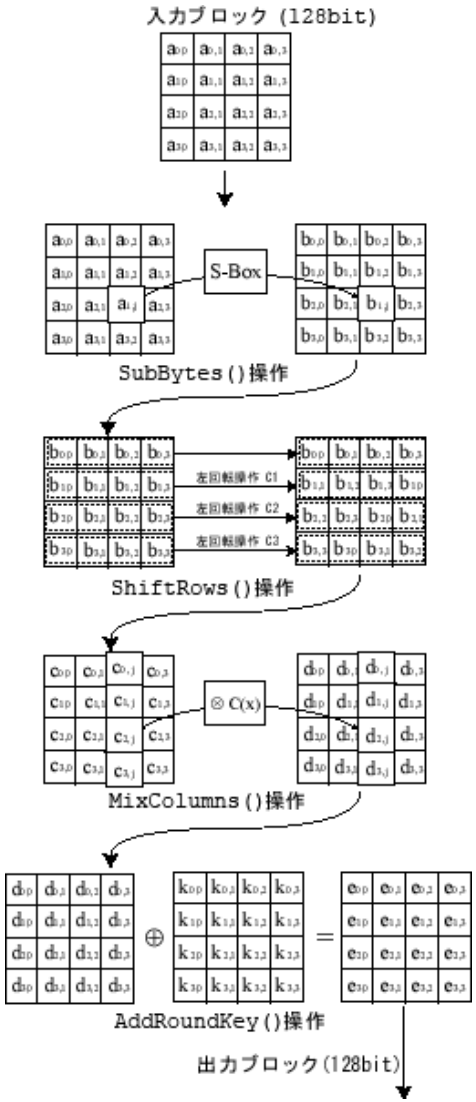


AESとは？

AESとは、アメリカ合衆国の国立標準技術研究所（NIST）が認定した共通鍵暗号化方式。
AESは、以下の事項を要求しており、公募の結果、Rijndael（ラインダール）と呼ばれるアルゴリズムがAESに選定された。

- 秘密鍵ブロック暗号であること
- 仕様と設計基準が完全に公開されていること
- DESより安全でTriple-DESより高速なこと
- ブロックサイズは128bit
- 鍵サイズは128,192,256bitをサポート
- ライセンスフリーで利用できること

AESラウンド操作概略図



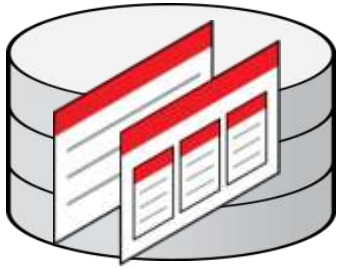
従来の格納データ暗号化機能の問題点

暗号化ツールキット（PL/SQLパッケージ）
を利用したデータの暗号化はOracle 9i以前からも可能

しかし

```
SQL> declare
  2    input_data varchar2(256) := '暗号化したい文字列';
  3    key_data raw(8) := dbms_obfuscation_toolkit.desgetkey(
  4        seed => utl_raw.cast_to_raw(rpad('abcd', 80, 'abcd')));
  5    output_data raw(256);
  6    output_data2 raw(256);
  7  begin
  8    dbms_output.put_line(input_data);
  9   dbms_obfuscation_toolkit.desencrypt(
 10      input => utl_raw.cast_to_raw(rpad(input_data, ((floor(lengthb(input_data)/8 + .9)) * 8))),
 11      key => key_data,
 12      encrypted_data => output_data);
 13    dbms_output.put_line(output_data);
 14    dbms_obfuscation_toolkit.desdecrypt(
 15      input => output_data,
 16      key => key_data,
 17      decrypted_data => output_data2);
 18    dbms_output.put_line(utl_raw.cast_to_varchar2(rtrim(output_data2)));
 19  end;
 20  /
```

暗号化ツールキットの利用

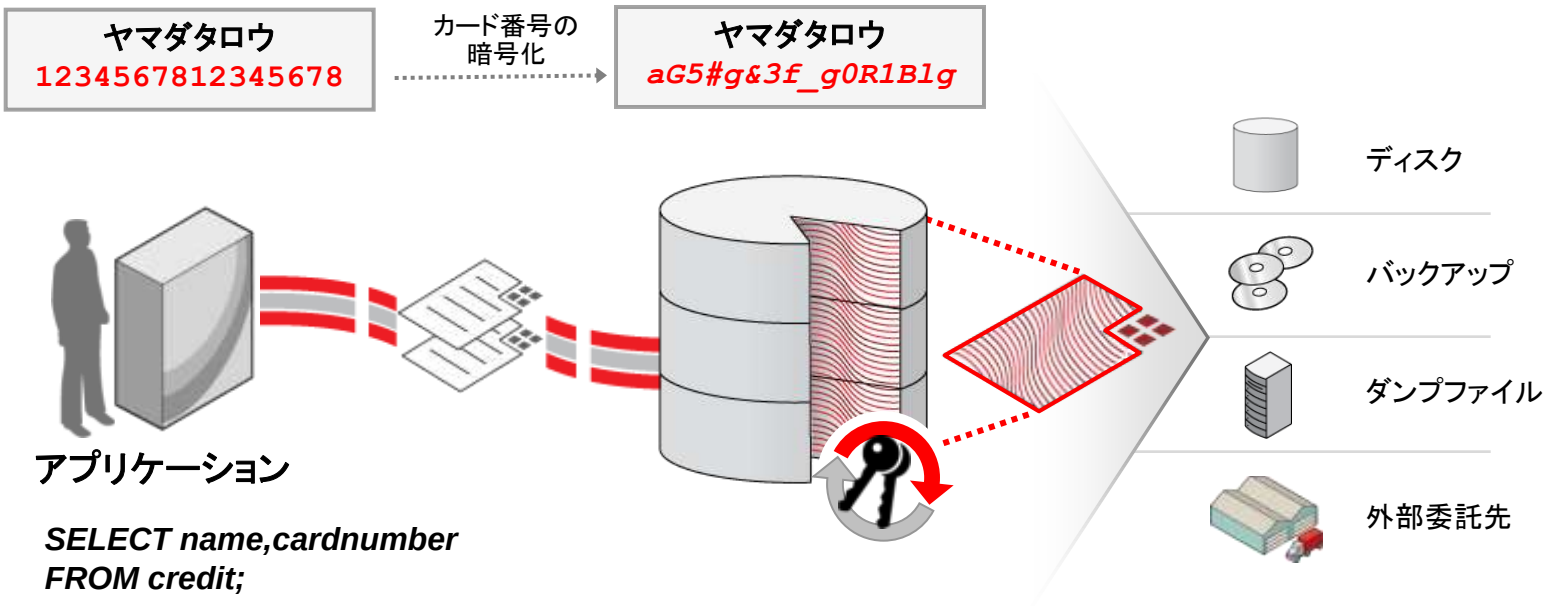


- アプリケーションの変更が必要
- パフォーマンスの劣化が大きい
- 暗号鍵管理の問題

セキュリティ要件上は求められていても、
データ暗号化の実装は困難・・

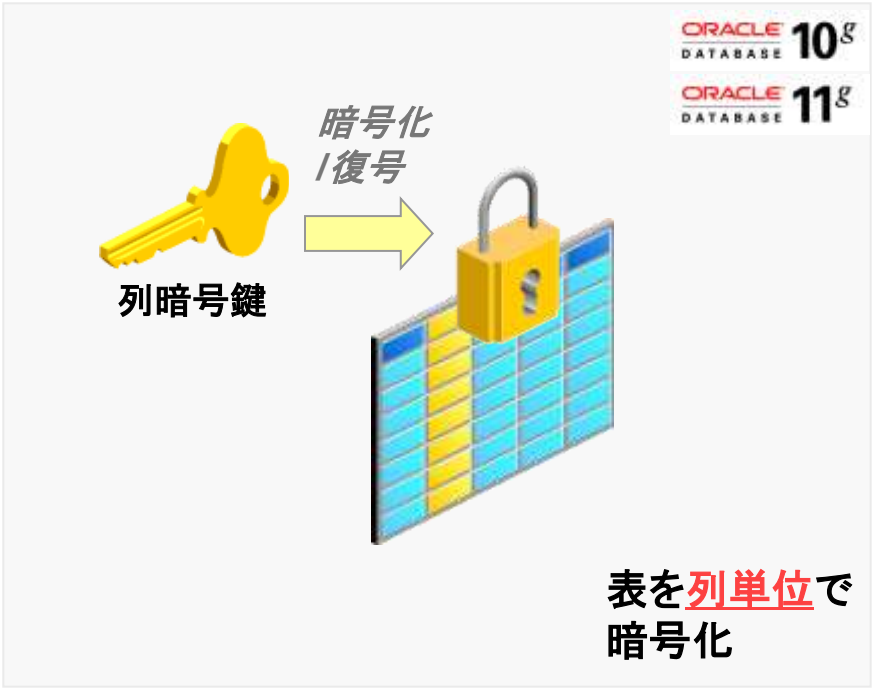
Transparent Data Encryption（TDE）

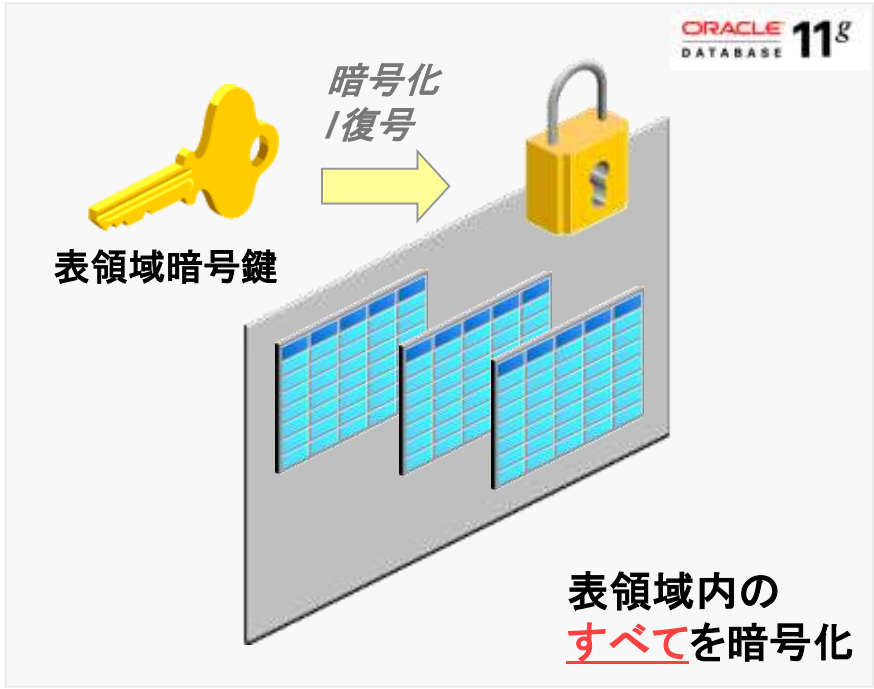
- 強力な暗号アルゴリズムを利用した暗号化を実施
  - NISTの標準共通鍵暗号方式 AES(128/192/256bit) に対応
- Oracle Wallet やHardware Security Moduleを利用した暗号鍵管理メカニズム
- アプリケーションからは透過的にデータの暗号化/復号
  - 既存のアプリケーション（SQL）を改修する必要はない



暗号化方式の種類

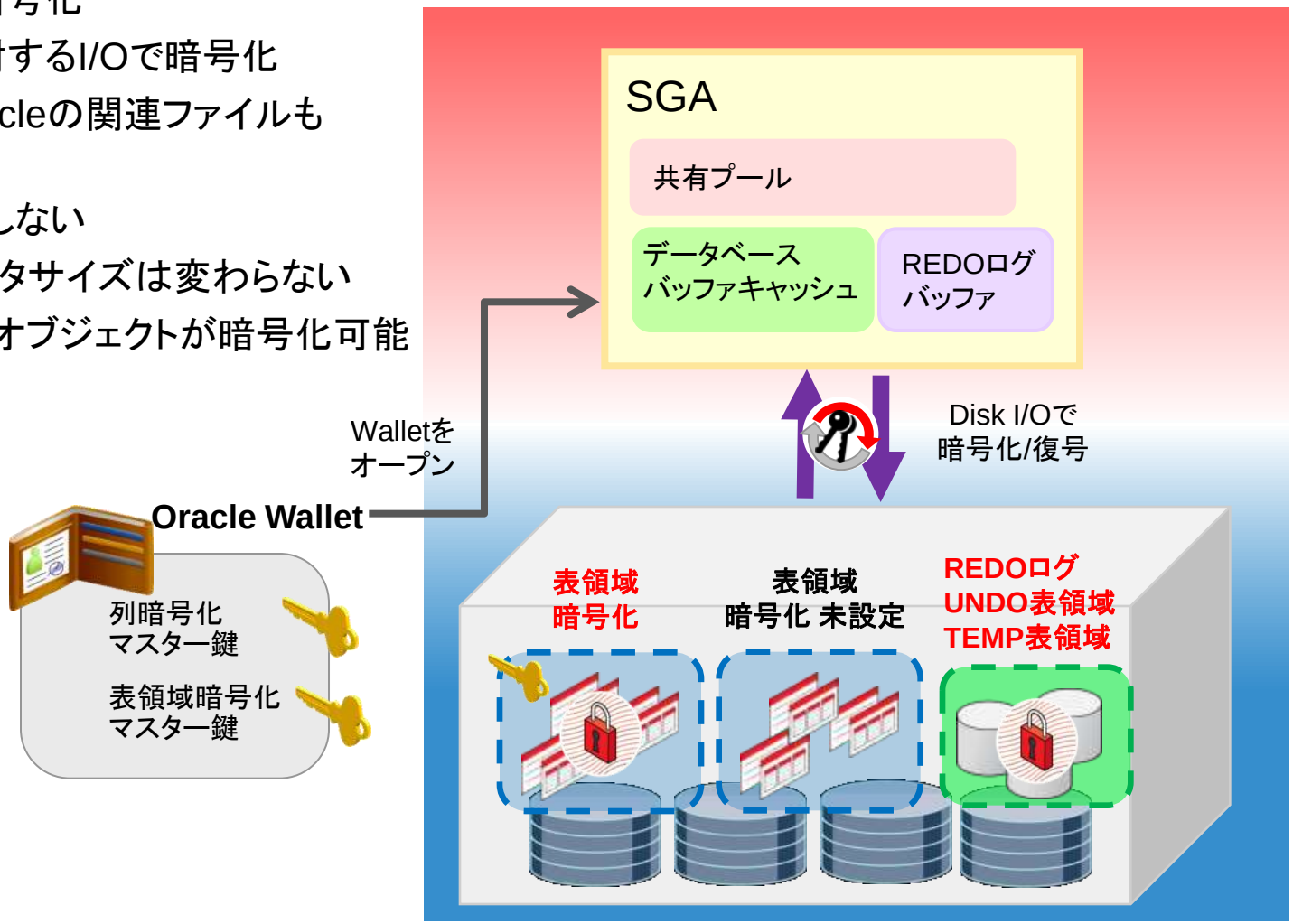
- 2種類の暗号化粒度
  - 列暗号化: 表の列ごとに暗号化を指定（10gR2～）
  - 表領域暗号化: 表領域内のすべてのデータを暗号化（11g～）





TDE 表領域暗号化(11gR1～)

- 表領域単位での暗号化
- データブロックに対するI/Oで暗号化
- 表領域以外のOracleの関連ファイルも暗号化される
- メモリ上は暗号化しない
- 暗号化してもデータサイズは変わらない
- ほとんどすべてのオブジェクトが暗号化可能(BFILEのみ不可)



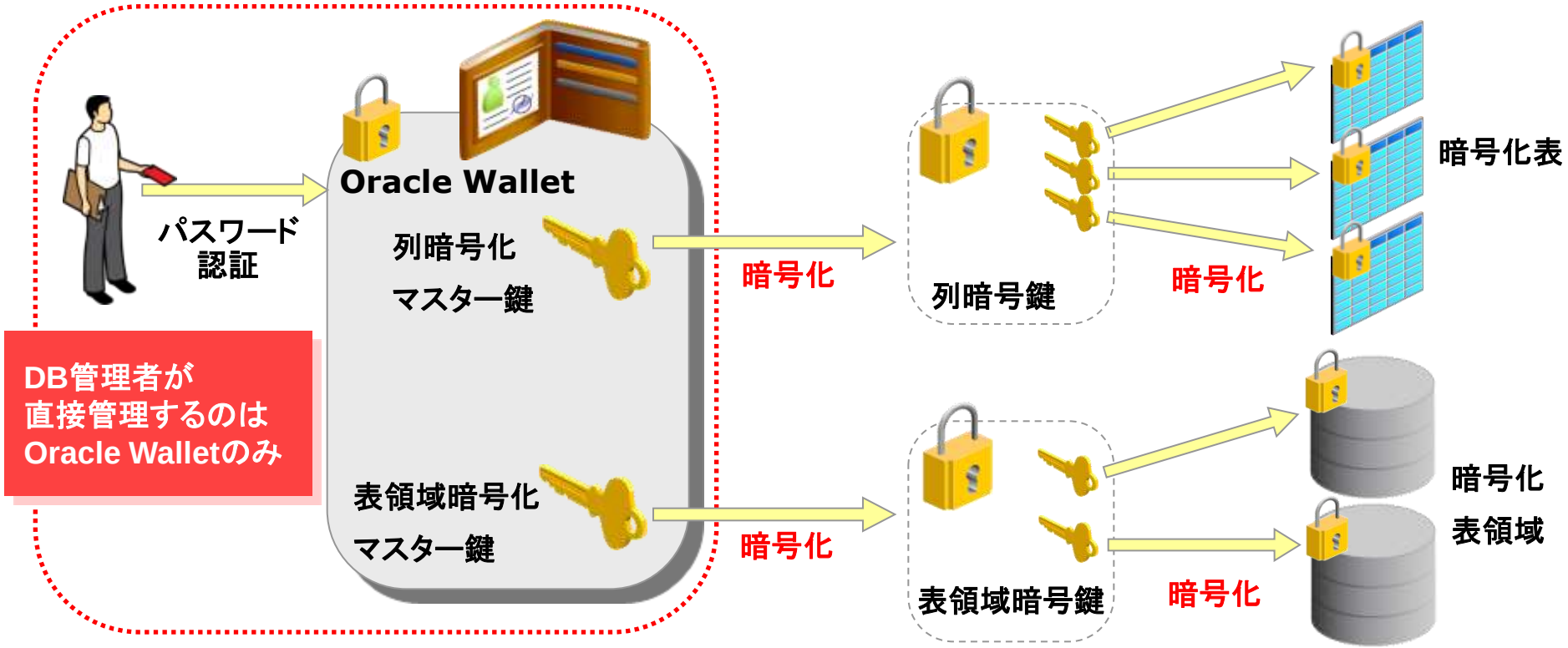
列暗号化、表領域暗号化の特徴

	列暗号化	表領域暗号化
暗号化のタイミング	行アクセス時	データ・ブロックに対する I/O発生時
暗号化アルゴリズム	3DES168, AES128 ,AES192 ,AES256	
暗号化により保護される場所	メモリ、ディスク	ディスク
データサイズ	暗号化対象データの量に比例して増加	暗号化前と変わらない
性能への影響	暗号化列へのアクセス頻度に応じて劣化	暗号化表領域のディスクI/O頻度に応じて劣化
対象オブジェクト	列のみ 暗号化列に対する索引は、 B-Tree索引の一意検索のみ可能	表領域内のすべてのオブジェクト BITMAP索引の作成やB-Tree索引の範囲検索も利用可能

許容できるセキュリティ・レベルと可用性のバランスに応じて選択

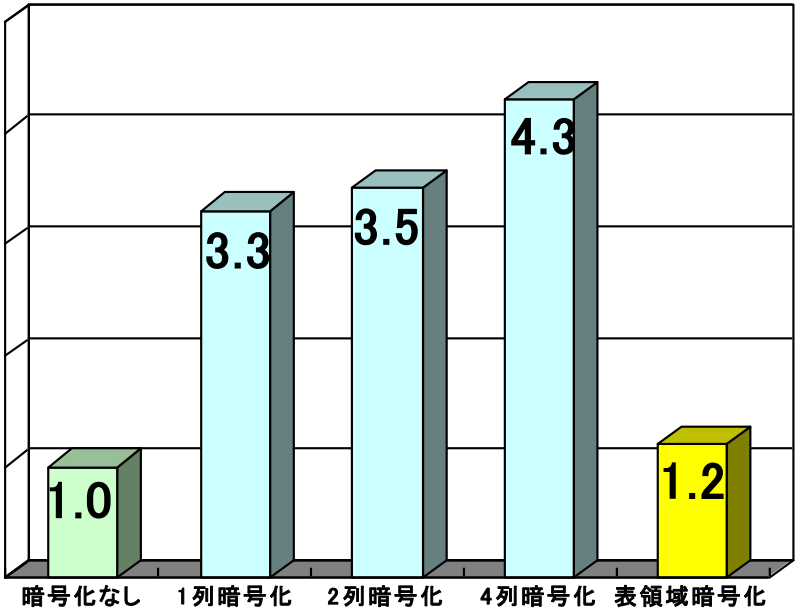
暗号鍵管理メカニズム

- TDEで利用される暗号鍵関連コンポーネント
  - Oracle Walletパスワード（1つ）
  - 列暗号化マスター鍵（1つ）、表領域暗号化マスター鍵（1つ）
  - 列暗号鍵（暗号化表ごとに1つ）、表領域暗号鍵（暗号化表領域ごとに1つ)



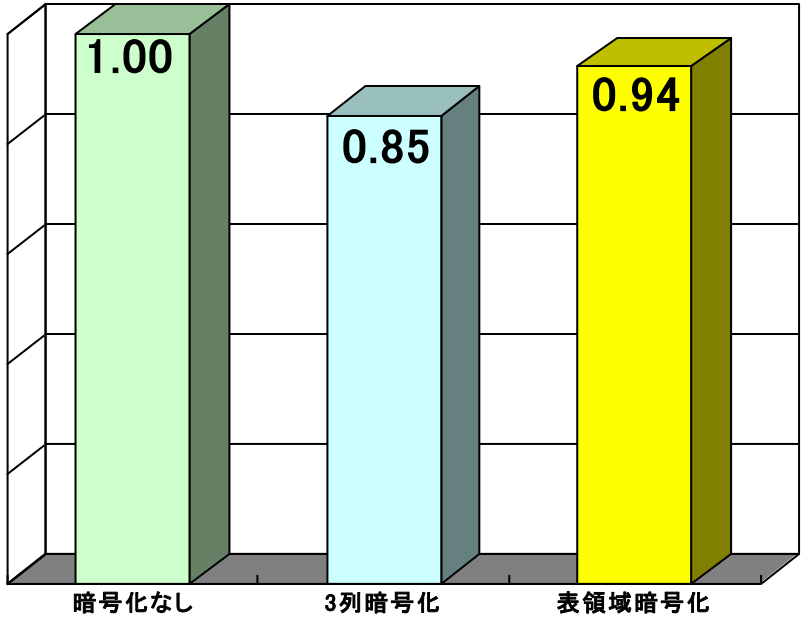
列・表領域暗号の性能の違い

- 列暗号化は暗号列数が増えるごとに処理時間に影響
- 列暗号化と比較して、表領域暗号化はバッチ処理、OLTP処理ともに性能への影響が小さい



バッチ処理に関する処理時間の比較

INSERT文を数十万回実行する処理を実行し、暗号化なしの場合を1としたときの相対処理時間を、列暗号化（1,2,4列）、表領域暗号化の場合でそれぞれ記載



OLTP処理に関するスループットの比較

TPC-Cベンチマークを実行し、暗号化なしの場合を1としたときの相対スループットを、列暗号化、表領域暗号化の場合でそれぞれ記載

AES-NIとは？

- AES-NI（Advanced Encryption Standard New Instructions）
  - Intel® Xeon® プロセッサー 5600 番台から搭載された新しい命令セット
  - 暗号化/復号処理をプロセッサー側で高速処理するアクセラレーション機能
  - AES-NIでは、6つの新しいAES命令が追加されており、これらの命令は、変換ラウンドでのAES処理を高速化できる

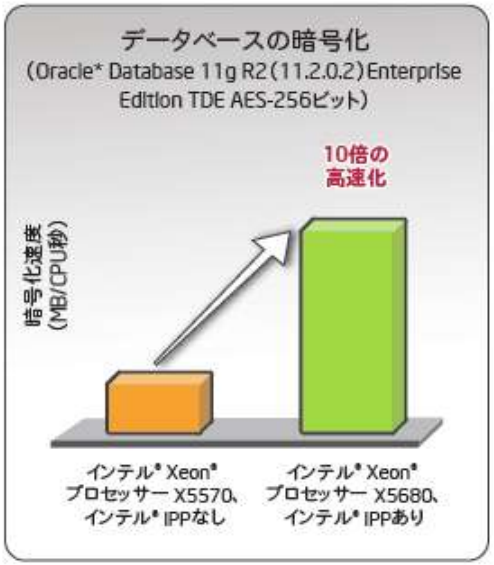
インテル® Xeon® プロセッサー X5680

- Oracle Database 11g R2 (11.2.0.2) Enterprise Edition
- TDE AES-256ビット 表領域暗号化

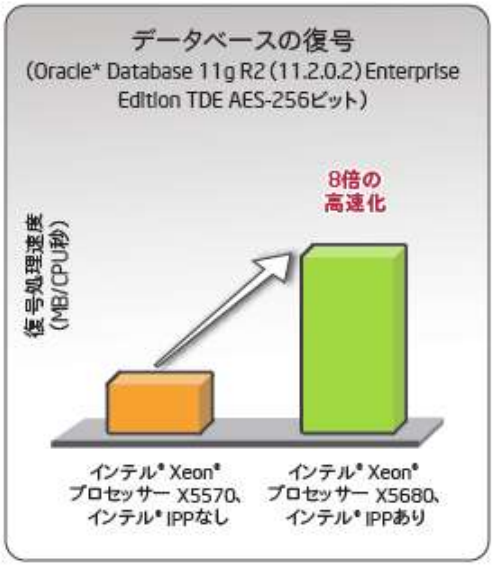
テストケース

- 100万行を空のテーブルにINSERT処理(30回)
- 510万行をテーブルからSELECT処理

暗号化 10倍高速



復号 8倍高速



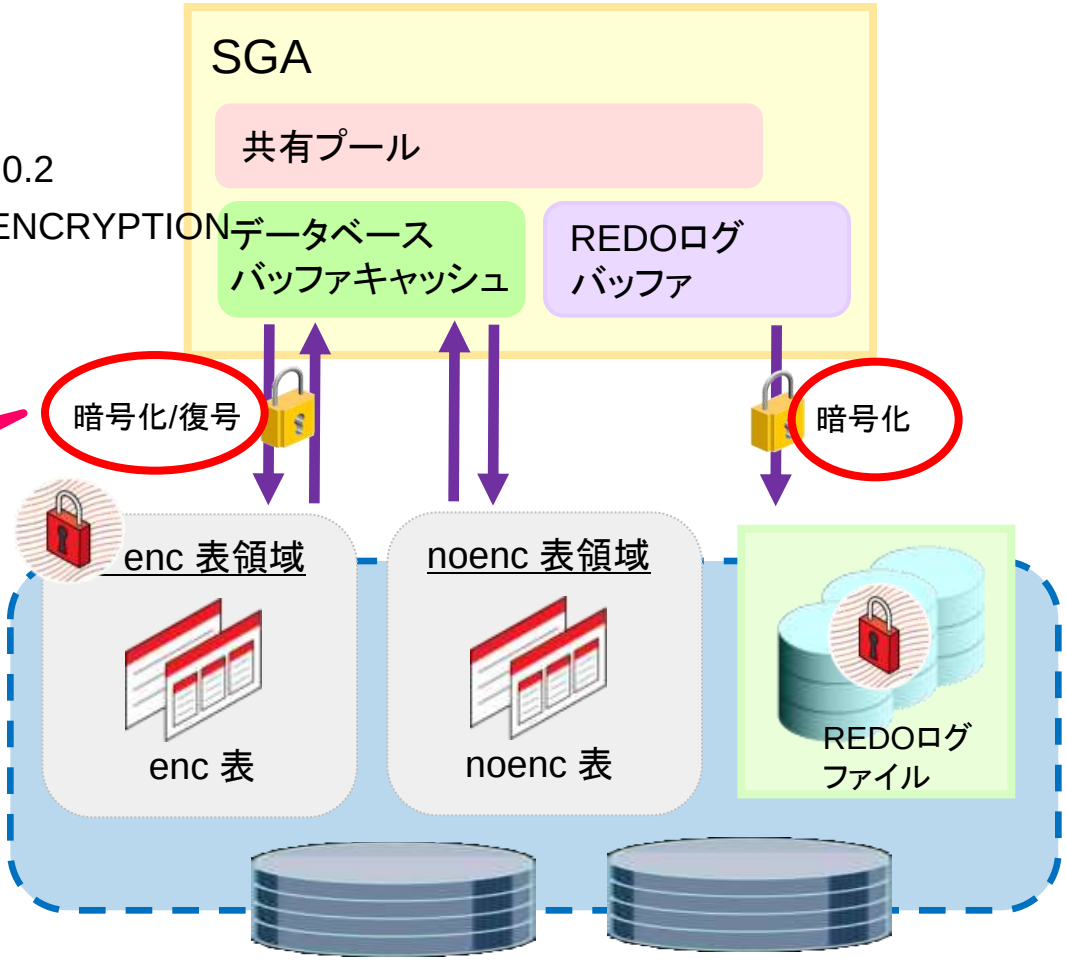
Intel White papersより引用: http://download.intel.com/jp/business/japan/pdf/323587-001JA.pdf

検証環境

- CPU:インテル(R) Xeon(R) プロセッサー 5600 6core x 2
- Memory 24GB
- Disk 300GB SATA x2
- Oracle Linux 5 x86_64
- Oracle Database Enterprise Edition 11.2.0.2
- patch(10080579) HW ACCELERATED ENCRYPTION NEEDS TO BE ENABLE BY DEFAULT
- 暗号アルゴリズムはAES256bit

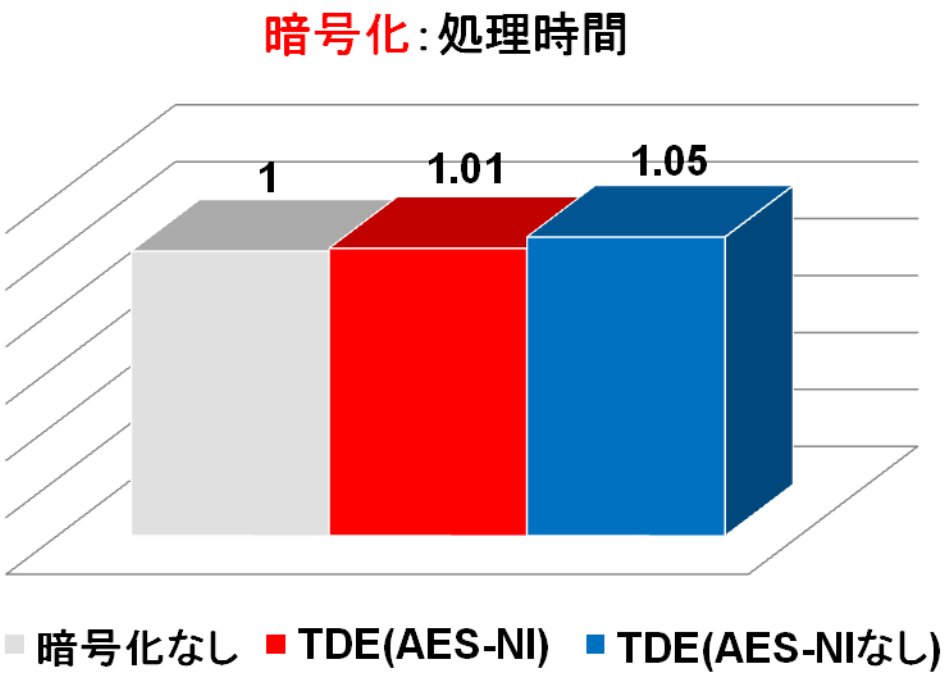
TDE 表領域暗号化では、Disk I/O のタイミングで暗号化/復号処理が実行される。

本検証では、特にこの部分に負荷をかけることで、暗号化/復号処理が性能にどう影響を与えるかを測定する



バッチ処理における暗号化性能

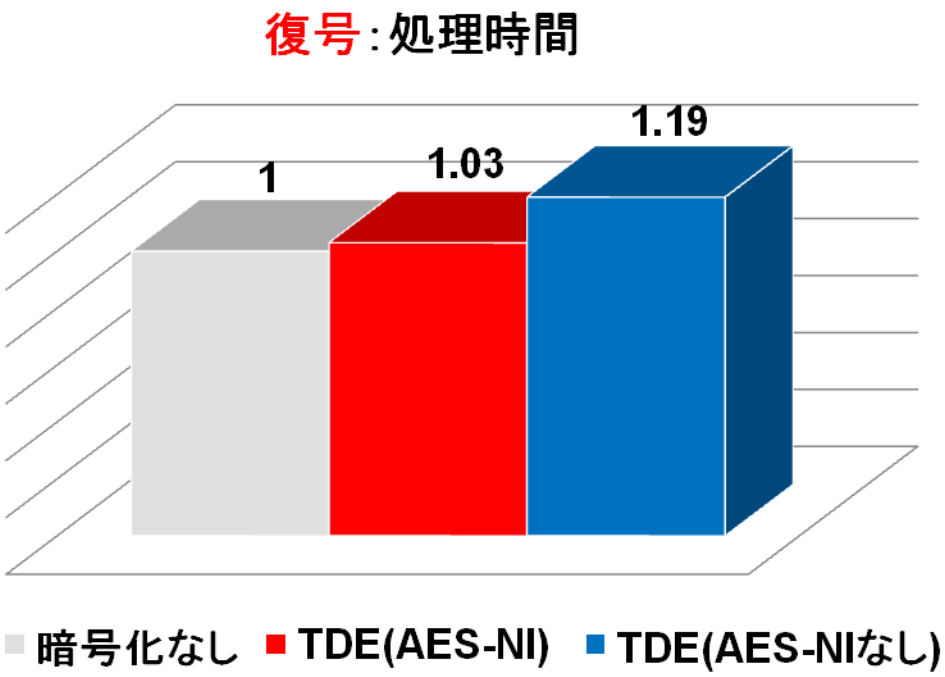
- 1 レコードあたり1MBのデータを、以下の3種類の表に100万回(1GB)のINSERT処理を行った場合の処理時間を計測
  (※ Direct Path Writeでバッファキャッシュを経由しない、暗号化なしの場合を相対処理時間と1とする)
  - 暗号化なしの表
  - TDE(表領域暗号化)に格納された表 + AES-NI をON
  - TDE(表領域暗号化)に格納された表 + AES-NIをOFF



従来のAES-NIなしの場合でも処理時間増はわずかしかし、AES-NIを使用するとほぼゼロに

バッチ処理における復号性能

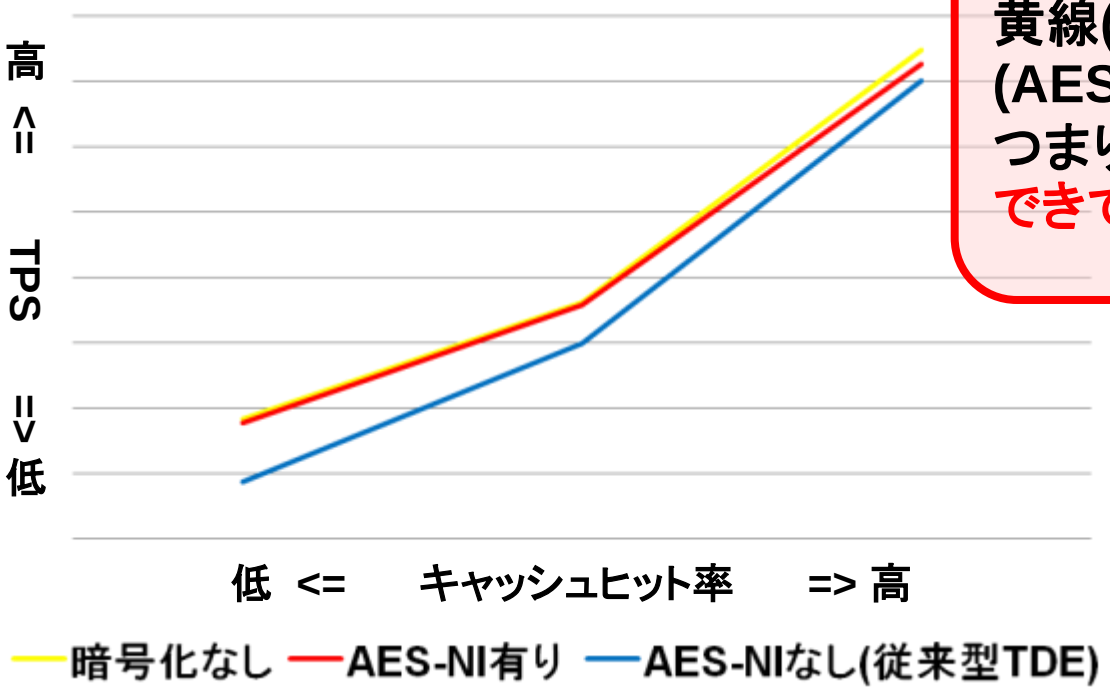
- 1GBのデータが格納されている、以下の3つの表をテーブル・フルスキャンをした場合の処理時間を計測
  (※ Direct Path Readでバッファキャッシュは使用しない、暗号化なしの場合を相対処理時間と1とする)
  - 暗号化なしの表
  - TDE(表領域暗号化)に格納された表 + AES-NI をON
  - TDE(表領域暗号化)に格納された表 + AES-NIをOFF



AES-NIなしの場合、約20%程度の処理時間増が認められたが、AES-NIありの場合、わずか3%まで短縮された

OLTP処理における暗号化/復号性能

- JpetstoreのアプリケーションをOLTP処理のトランザクションと仮定し、バッファキャッシュとDisk I/Oが同時に発生する一般的なアプリケーション(※キャッシュヒット率が高い)の場合、暗号化/復号処理がアプリケーションの性能にどう影響するかを計測
  - 検索:更新の割合=8:2
  - 40 threadで実行

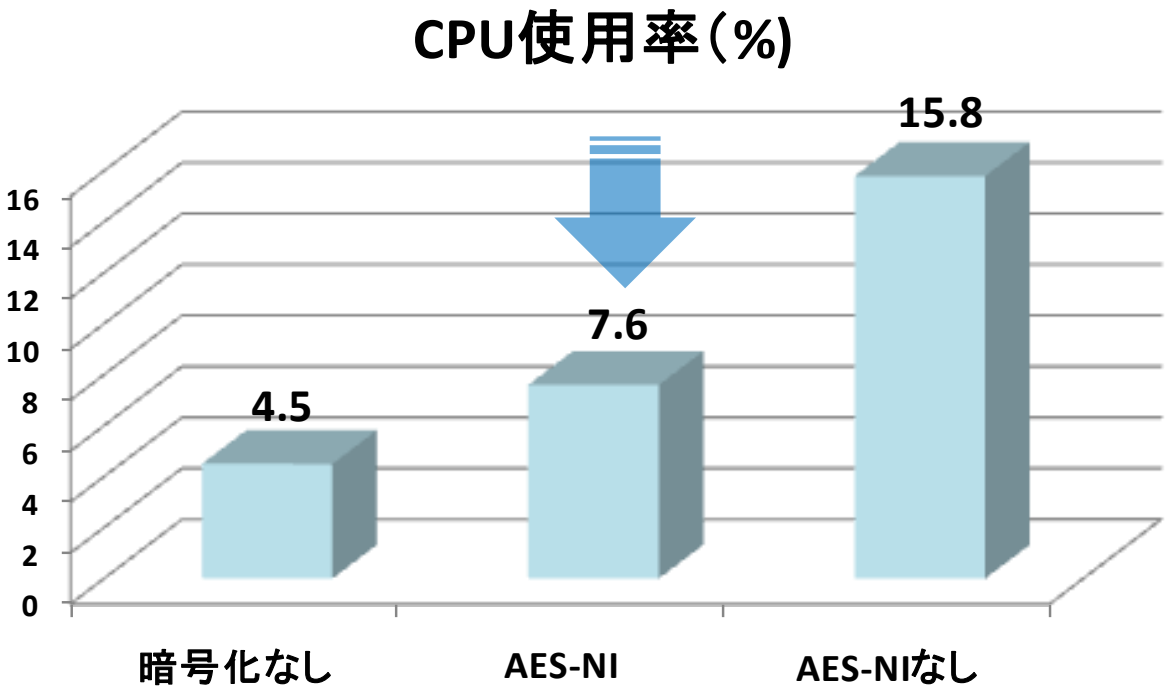


黄線(暗号化なし)と赤線(AES-NI)がほぼ同じ曲線
つまり、同等の性能を担保できているといえる

AES-NIを使用した場合のCPUへの影響

- 1GBのデータを暗号化する場合、AES-NIを使用した場合と使用しない場合、CPUの使用率にどのくらいの違いがあるかを計測

AESの演算処理をソフトウェア側で実行するより、AES-NIによるプロセッサー側で実行したほうがCPUを使用率を低く抑えられる



本セミナーのまとめ

暗号化はとにかく性能が心配	Disk I/Oが多いバッチ処理でも、高いレスポンスが要求されるOLTP処理でも、性能への影響は**限りなくゼロ**に
暗号化によるCPUやディスクのサイジングが難しい	TDE 表領域暗号化は、暗号化によるデータサイズの増加はなし、CPUも効率的に使用できるため、**特別なサイジングは不要**
どのデータを暗号化すべきなのか選別に悩む	少しでも必要と感じれば、オブジェクトを暗号化した表領域へ。さらに、よりセキュアな**データベースのフル暗号化**が現実的に

AES-NI + TDE 表領域暗号化は、限りなくゼロ・インパクトを実現する暗号化ソリューション

4月からセキュリティ講座開催中

OTN×ダイセミ　でスキルアップ!!

・一般的な技術問題解決方法などを知りたい！
・セミナ資料など技術コンテンツがほしい！

Oracle Technology Network(OTN)を御活用下さい。

http://forums.oracle.com/forums/main.jspa?categoryID=484

一般的技術問題解決にはOTN掲示版の
「データベース一般」をご活用ください

※OTN掲示版は、基本的にOracleユーザー有志からの回答となるため100%回答があるとは限りません。
ただ、過去の履歴を見ると、質問の大多数に関してなんらかの回答が書き込まれております。

http://www.oracle.com/technetwork/jp/content/index-086873-ja.html

過去のセミナ資料、動画コンテンツはOTNの
「OTNセミナー　オンデマンド コンテンツ」へ

※ダイセミ事務局にダイセミ資料を請求頂いても、お受けできない可能性がございますので予めご了承ください。
ダイセミ資料はOTNコンテンツ　オン　デマンドか、セミナ実施時間内にダウンロード頂くようお願い致します。

OTNセミナー　オンデマンド　コンテンツ

ダイセミで実施された技術コンテンツを動画で配信中!!
ダイセミのライブ感はそのままに、お好きな時間で受講頂けます。

twitter

最新情報つぶやき中

oracletechnetjp

- 人気コンテンツは？
- お勧め情報
- 公開予告　など

OTN トップページ　http://www.oracle.com/technetwork/jp/index.html
ページ左「基本リンク」>「OTN セミナー　オンデマンド」

※掲載のコンテンツ内容は予告なく変更になる可能性があります。
期間限定での配信コンテンツも含まれております。お早めにダウンロード頂くことをお勧めいたします。

Oracle エンジニアのための技術情報サイト

オラクルエンジニア通信

http://blogs.oracle.com/oracle4engineer/

twitter

最新情報つぶやき中

oracletechnetjp

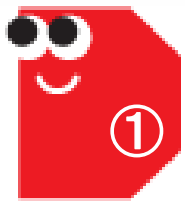
- 技術資料
  - ダイセミの過去資料や製品ホワイトペーパー、スキルアップ資料などを多様な方法で検索できます
  - キーワード検索、レベル別、カテゴリ別、製品・機能別
- コラム
  - オラクル製品に関する技術コラムを毎週お届けします
  - 決してニッチではなく、誰もが明日から使える技術の「あ、そうだったんだ！」をお届けします

こんな資料が人気です

- ✓ 6か月ぶりに資料ダウンロードランキングの首位が交代！ 新王者はOracle Database構築資料でした。
- ✓ データベースの性能管理手法について、Statspack派もEnterprise Manager派も目からウロコの技術特集公開中

オラクルエンジニア通信

Oracle Databaseの価格ご存知ですか？



問題：

Oracle Databaseの最小構成はいくらでしょうか？

ヒント：

Oracle Standard Edition Oneを

5Named User Plus(指名ユーザ) というのが最小構成です。

問題：

Real Applications Clusters(RAC) Optionはいくらでしょうか？

ヒント：

RACはOracle Database Enterprise EditionのOptionです。

答えはこちら↓ ログイン不要の簡単見積もり

ライセンス見積もりヘルプ　検索

見積もり Start!

ITプロジェクト全般に渡る無償支援サービス

Oracle Direct Conciergeサービス

■パフォーマンス診断サービス
- Webシステム　ボトルネック診断サービス　NEW
- データベースパフォーマンス　診断サービス

■移行支援サービス
- SQL Serverからの移行支援サービス
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行支援サービス
- Postgre SQLからの移行支援サービス
- Accessからの移行支援サービス
- Oracle Application ServerからWeblogicへ移行支援サービス　NEW

■システム構成診断サービス
- Oracle Database構成相談サービス
- サーバー統合支援サービス
- 仮想化アセスメントサービス
- メインフレーム資産活用相談サービス
- BI EEアセスメントサービス
- 簡易業務診断サービス

■バージョンアップ支援サービス
- Oracle Databaseバージョンアップ支援サービス
- Weblogic Serverバージョンアップ支援サービス　NEW
- Oracle Developer/2000(Froms/Reports) Webアップグレード相談サービス

オラクル社のエンジニアが 直接ご支援します
お気軽にご活用ください!

オラクル　無償支援　検索

ORACLE

1日5組限定！

製品無償評価サービス

提供シナリオー例

- データベースチューニング
- 無停止アップグレード
- アプリケーション性能・負荷検証
- Webシステム障害解析

インストールすることなく、すぐに体験いただけます

- サービスご提供までの流れ
  1. お問合せフォームより「製品評価サービス希望」と必要事項を明記し送信下さい
  2. 弊社より接続方法手順書およびハンズオン手順書を送付致します
  3. 当日は、弊社サーバー環境でインターネット越しに製品を体感頂けます

※サービスご提供には事前予約が必要です

Web問い合わせフォーム

「ダイデモ」をキーワードに検索することで申し込みホームページにアクセスできます

http://www.oracle.com/jp/direct/services/didemo-195748-ja.html

ORACLE

あなたにいちばん近いオラクル

Oracle Direct

まずはお問合せください

Oracle Direct　検索

システムの検討・構築から運用まで、ITプロジェクト全般の相談窓口としてご支援いたします。

システム構成やライセンス/購入方法などお気軽にお問い合わせ下さい。

Web問い合わせフォーム

専用お問い合わせフォームにてご相談内容を承ります。

http://www.oracle.com/jp/direct/inquiry-form-182185-ja.html

※こちらから詳細確認のお電話を差し上げる場合がありますので、ご登録されている連絡先が最新のものになっているか、ご確認下さい。

フリーダイヤル

0120－155－096

※月曜~金曜　9:00~12:00、13:00~18:00

（祝日および年末年始除く）