ORACLE

HITACHI
Inspire the Next

性能検証レポート

日立サーバ仮想化機構Virtageで実現するOracleデータベースの暗号処理高速化

高いレベルでセキュリティを確保しながら、システムのパフォーマンスをどう維持していくか――この難題に日立とオラクルが挑みました。目指したのは、日立サーバ仮想化機構Virtageによる仮想環境下でOracle Databaseを暗号化し、この暗号化に伴う処理オーバーヘッド増大＝性能低下を可能な限り抑え込むこと。そこで、インテルの新しい暗号処理用命令セットAES-NIを使用しながら性能検証を実施したところ、「セキュリティ向上に伴う性能低下」という従来のジレンマを打破する検証結果が得られました。

日立サーバ仮想化機構「Virtage」上にOracle Databaseを構築。AES-NIを利用して、セキュリティと性能を両立できるかを検証。

セキュリティに対するニーズがさらに高まっているなか、データが格納されるデータベースのセキュリティ対策も必要となりつつあります。データベースのセキュリティ対策にはさまざまなポイントがありますが、その一つに、データベースに格納されたデータの暗号化があります。データベースから情報が漏えいする原因の一つとして、データベースを構成するファイルやバックアップメディアの盗難があり、暗号化はこのような漏えいへの対策となります。

Oracle Database 11gのOracle Advanced Securityでは、Transparent Data Encryption（以下TDE）と呼ばれる、データの暗号化機能を提供。「透過的データ暗号化」という名前の通り、TDEはアプリケーションから透過的にデータの暗号化を行うことができ、アプリケーション側の作りこみや変更による追加の開発コストを必要としません。一般的に、暗号化による処理のオーバーヘッドで性能が劣化すると考えられがちですが、Oracle Database 11gのTDEでは、暗号のオーバーヘッドを大幅に低減させています。TDEには表領域暗号化と呼ばれる方式が導入され、ディスクI/O発生時にのみ暗号化することにより、処理オーバーヘッドを低減させました。さらにインテル® 社が提供するインテル® AES New Instructions（以下AES-NI）という新たな暗号処理用の命令セットを搭載したプロセッサーとOracle Database 11gのTDEを組み合わせて暗号化することで、さらなる性能向上が可能となっています。

一方、近年ではCPUのマルチコア化が進んでおり、CPUリソースを有効活用するためにサーバの仮想化技術が利用されてきています。日立の統合サービスプラットフォーム「BladeSymphony」は、複数のコアを仮想化単位に区切って論理パーティションとして使用できるLPAR方式の独自の仮想化機構「Virtage」を搭載。Virtageはハードウェアによる仮想化アシストを積極的に利用することでI/O処理の仮想化オーバーヘッドを低減し、物理サーバと同等の性能を実現しています。また、AES-NIを仮想化技術上で使用するには、その仮想化技術もAES-NIに対応している必要がありますが、インテル® Xeon® プロセッサー 5600番台以降を搭載したブレードは、Virtageの論理パーティション上でAES-NI機能をサポートしています。VirtageはOracle Real Application Clustersが動作保証されているため、Oracle Databaseの実行環境として多くの利用実績があります。

日立はVirtage上でAES-NIを利用することで、仮想化技術上でもセキュリティと性能を両立できるOracle Database環境が実現できると考えています。これを確認するため、日本オラクル社と共同で、「BladeSymphony」のサーバ仮想化機構「Virtage」上にてOracle Databaseを構築し、AES-NIを使用した性能検証を行いました。本資料ではその結果をご紹介いたします。

Virtage 環境での OLTP 処理とバッチ処理で それぞれ３パターンの性能測定を実施。

Oracle Database 11gのTDEには列暗号化と表領域暗号化の二つの方式があります。列暗号化は表の特定の列の暗号化を行い、SQLの発行のたびに暗号化／復号が行われます。これに対し、表領域暗号化は表領域全体の暗号化を行い、暗号化はディスクI/O時にのみ行われます。データの多くがバッファキャッシュ上に載っているような通常のOLTP処理では、表領域暗号化によるオーバーヘッドはあまりないと考えられます。一方、多量のI/Oが一度に発生する一括データローディングや表の全件検索処理といったバッチ処理では、表領域暗号化使用時にも処理への影響が考えられます。

OracleのTDEの表領域暗号化利用時に多量のI/Oが発生した場合でも、AES-NIを利用すれば暗号化のオーバーヘッドを抑えることができます。AES-NIには暗号化、復号処理を高速化するためのAESアルゴリズムのサブステップとして7つの命令セットが組み込まれています。4つの命令が暗号化、復号を高速化し2つの命令がキー生成、マトリクス操作を向上、そして1つの命令がキャリーなし乗算をサポートします。本命令セットをサポートするセキュリティ製品を使用することで、ソフトウェア・ベースの暗号化、復号処理で発生するCPUオーバーヘッドを最小化しつつ、高速な処理を実現することができます。

今回の検証では、Virtage環境上において、OLTP処理とバッチ処理それぞれのケースで、暗号化なし、TDEあり、TDE+AES-NIという3パターンの性能測定を実施。VirtageはBIOS設定でAES-NIのOn/Offが指定できるため、同一環境で検証しました。また検証上の留意点として、表領域暗号化はディスクI/O時に暗号化を行うという特性上、ディスクI/O自体がボトルネックになるとAES-NIの有無による性能の差違が出なくなるため、ディスク上にデータを分散配置してI/Oボトルネックにならないように構成しました。

OLTP処理には、WEBベースのオンライン受発注システムをモデル化したツールを使用しており、キャッシュヒット率が95%から100%の間で推移するようにデータサイズを調整した参照系を8割、更新系を2割に設定した負荷を80端末で10分間テストしました。

バッチ処理には、大規模テーブルに対するフルスキャン（復号）とダイレクト・パス・インサート（暗号化）をそれぞれモデル化したツールを使用。TDEは表領域暗号化を使用しているため、ディスクに読み書きする時点で暗号化・復号される点を考慮し、処理に用いるデータサイズは10GBに設定しテストしました。TDEでは表領域暗号化を使用しており、ディスクに対するアクセスで暗号化・復号されます。このため、大容量のシーケンシャル・アクセスをすることでAESの暗号演算処理のオーバーヘッドが顕著になる点を考慮し、バッチ処理に用いるデータサイズを10GBに設定しています。

◎テストパターン

次の3パターンでテストし、CPU, スループット/処理時間を比較。

■ 暗号化なし	TDE（表領域暗号化）なし。
■ TDE（AES-NI ON）	TDE（表領域暗号化）あり。BIOS上でAES-NIを有効化
■ TDE（AES-NI OFF）	TDE（表領域暗号化）あり。BIOS上でAES-NIを無効化

◎ハードウェア、ソフトウェア構成について

ハードウェア

サーバ	日立BladeSymphony BS320P5モデル インテル® Xeon® プロセッサー X5670 ×2
Virtage LPAR構成	4仮想CPU（占有モード）、8GBメモリー
ストレージ	Hitachi Adaptable Modular Storage 2300 8GB cache/controller、2TB HDD（データ領域）

ソフトウェア

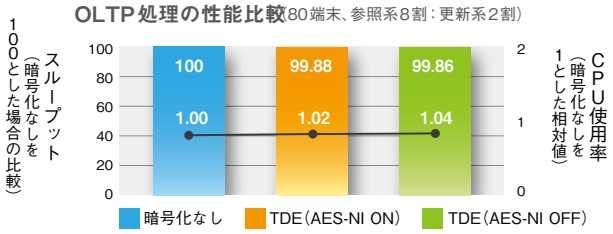
OS	RedHat Enterprise Linux 5.4（x86-64）
DB	Oracle Database Enterprise Edition（11.2.0.3）
DB Option	Oracle Advanced Security

OLTP処理、バッチ処理それぞれでセキュリティと性能の両立を確認。

AES-NIを有効にしたVirtage環境で、AES演算が高速に処理できることを実証しました。OLTP処理では暗号化なしの構成と同様の性能を得ることを確認。次にディスクI/Oが大量発生するバッチ処理では、ソフトウェアによる暗号演算と比べ、CPU使用率を抑えつつ高速に処理が行われるとともに、暗号化なしと比べても遜色のない性能が実現できることを確認できました。

OLTP処理では表領域暗号化によるパフォーマンス影響はほとんどなく、暗号化なしと同等の性能で使用できる

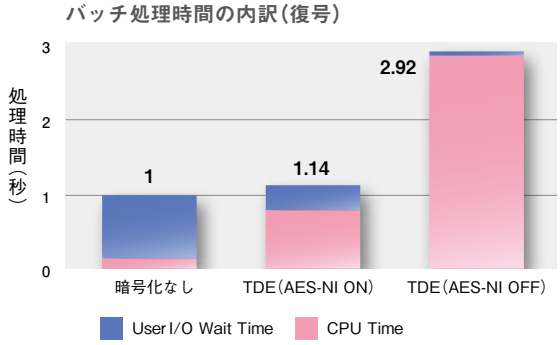
OLTP処理では多くのデータアクセスはキャッシュ上のデータに対して行われるため、表領域暗号化自体の性能オーバーヘッドは少ないという結果が得られました。
CPU使用率についてはAES-NI有効、無効に関わらず、暗号化なしとほぼ同等という結果が得られました。右のグラフがOLTP処理を実行した結果です。

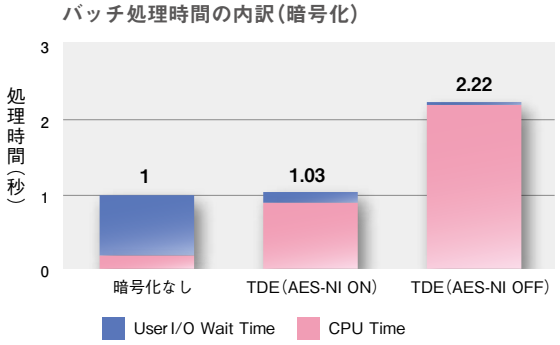


※TPSとCPU使用率はそれぞれ相対値となっています。TPSは暗号化なしを基準にしたパーセント表記、CPU使用率は暗号化なしを1とした場合の使用率の比率を示しています。

バッチ処理ではAES-NIを使用すると暗号化なしの性能を維持でき、ソフトウェア暗号化と比べ、必要なCPUパワーを大きく削減できる

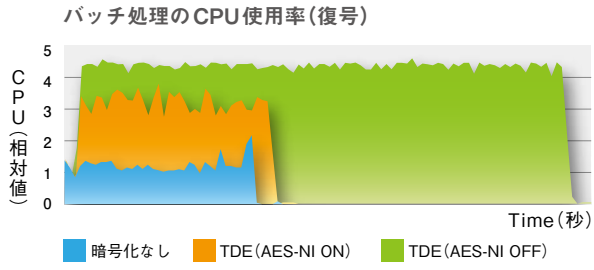
バッチ処理の比較結果は、OLTP処理時の結果と大きく異なるものとなりました。以下のグラフは10GBのデータを用いてバッチ処理を実行した結果です。復号、暗号化ともに暗号化なしとTDE（AES-NI OFF）の構成を比較した場合、復号演算処理性能の比較で2.92倍、暗号演算処理性能の比較で2.22倍の性能差が確認できました。これに対し、TDE（AES-NI ON）時の復号と暗号化処理時間は、両者ともに暗号化なしの構成とほとんど変わらず、レスポンスを損なうことなくデータの保護が実現できていることがわかります。

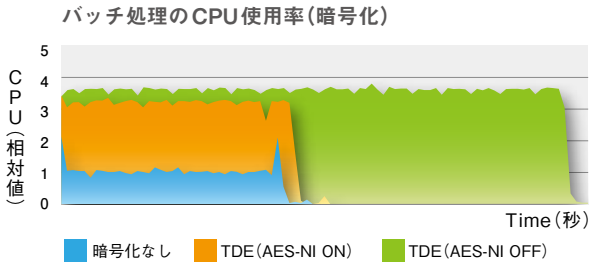




AES-NIの使用によりCPU使用率と処理時間が低減

以下のグラフは、各バッチ処理でのCPU使用率の変化を示しています。psコマンドを1秒間隔で実行し、CPU使用率を取得しました。グラフの縦軸は相対値でのCPU使用率、横軸は時間の推移を示しています。暗号化なしと比べると、大量のI/Oリクエストが発生する際に暗号化/復号処理が行われるため、TDE暗号化（AES-NI ON）のCPU使用率は高い状態になりました。しかしCPU使用率をTDE（AES-NI ON）とTDE（AES-NI OFF）時で比較したケースでは、AES-NI使用時の方が暗号/復号演算処理におけるCPU使用率を低く抑えられるという結果を得ました。単にCPU使用率の値が低いだけでなく、処理時間自体も短くなるため、右下の図のように時間積分的に見ると（図中グラフの占める面積に着目）、AES-NIによって処理に必要なCPUパワーを大きく削減できていることがわかります。余ったCPUパワーは他の論理パーティションの処理などに振り分けてサーバ集約率の向上を図ることもでき、あるいは同じハードウェアでより大きなデータベースを扱うことも可能になります。





まとめ

AES-NIとTDEの組み合わせで、Virtageの仮想化環境でもセキュリティと性能を高いレベルで両立できることを実証。

今回の検証では、TDEの表領域暗号化とAES-NIを組み合わせることによってデータベース暗号化のオーバーヘッドが極小化できることが実証できました。特に、ディスクI/Oがより多く発生するバッチ処理においては、暗号演算処理におけるCPUオーバーヘッドを低く抑え、かつ、高速化できます。さらに、Virtageによる仮想化環境で作成した論理パーティション上でもAES-NIが非常に有効であり、AES-NIとTDEを組み合わせることでVirtageの仮想化環境でもOracle Database 11gのパフォーマンスとセキュリティを両立させることが可能であることが実証できました。

仮想化環境上でTDEとAES-NIを組み合わせて使用する場合にはいくつか考慮点があります。仮想化環境上で使用する場合、その仮想化機構がAES-NIに対応している必要があります。またAES-NIはディスクI/Oがボトルネックとなる環境ではあまり効果が表れないため、I/O性能が出るようなディスク構成をとる必要があります。仮想化利用時には、その仮想化機構でディスクI/Oが阻害されないようにすることにも注意が必要となります。日立の仮想化機構Virtageは、論理パーティション上でAES-NIが有効化でき、I/Oがボトルネックにならないように構成できます。

本検証結果により、仮想化を使用した場合でもVirtageを利用することで、より少ない仮想CPUのパーティションで暗号化を使ったデータベースが利用できます。AES-NIを利用すれば、TDEの処理性能は暗号化なしの場合とほぼ遜色ありません。VirtageのようにAES-NIが利用できるプラットフォーム上ではぜひ積極的にTDEによるデータベースのセキュリティ向上をご検討ください。

［参考］用語解説

【 Oracle Advanced Security】

Oracle Advanced SecurityはOracle Database Enterprise Editionのオプションで、暗号化や厳密認証サービスとの連携によるデータベースの保護が可能になります。Oracle Advanced Securityによる暗号化では、データベースに格納されたデータだけでなく、データベースへのクエリーなどによるネットワーク上のデータやバックアップ・データに対しても、透過的に暗号化することが可能です。

【Oracle Transparent Data Encryption】

Oracle Transparent Data Encryption（以下TDE）は、Oracle Advanced Securityの1機能として、Oracle Database 11gから導入されました。TDEは表領域や表の列をデータベース側で暗号化するため堅牢性に優れており、暗号/復号処理を高速化するAES-NIとの連携が可能です。また、アプリケーションに透過的に暗号処理を実施するため、アプリケーション側の作りこみなどによる追加の開発コストを必要としません。TDEで使用される暗号化用のマスターキーは、セキュリティ強化のため、オラクルの外部セキュリティ・モジュールであるWalletに格納されます。

【 AES-NI(Advanced Encryption Standard-New Instructions) 】

インテル® AES New Instructions（インテル® AES-NI）はインテル® Xeon® プロセッサー 5600番台に搭載している暗号処理のための新しい命令セットです。

【 日立サーバ仮想化機構Virtage 】

Virtageは、統合サービスプラットフォーム「BladeSymphony」に搭載されている日立独自のサーバ仮想化機構です。日立がメインフレーム開発で培ってきた技術を生かし、論理分割方式によるサーバ仮想化を実現しています。ハードウェアによる仮想化アシストを積極的に利用することでオーバーヘッドを低減し、物理サーバと同等の信頼性を保つことができるため、大規模システムや基幹系データベースシステムにも利用できます。また、インテル® Xeon® プロセッサー 5600番台以降を搭載したブレードでは、Virtageの論理パーティション上でのAES-NI機能をサポートしています。VirtageはLinuxおよびWindows上で、Oracle Real Application Clusters の認定を受けています。

・Intel、インテル、Intelロゴ、Xeonは、アメリカ合衆国およびその他の国におけるIntel Corporationの商標です。
・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あります。
・その他記載の会社名，製品名は，それぞれの会社の商号，商標もしくは登録商標です。

製品に関する詳細・お問い合わせは下記へ

■ 製品情報サイト

日立のOracle製品情報サイト
http://www.hitachi.co.jp/oracle/

日立サーバ仮想化機構「Virtage」
http://www.hitachi.co.jp/virtage/

■ メールでのお問い合わせ

日立-オラクル Virtageソリューションセンター
OraVirtage@ml.itg.hitachi.co.jp

株式会社 日立製作所　情報・通信システム社

VEGETABLE OIL INK
本カタログは環境に配慮し、植物油インキを使用しています。

2012.3
Printed in Japan(H)