Penta SECURITY

お客様が暗号化に迷う５つの理由とデータ保護対策

データ保護のトータル・セキュリティ・ソリューション、D'Amo

ペンタセキュリティシステムズ株式会社| 2011.07.

誠に申し訳ございませんが、本ドキュメントの最初から3ページ目まではアニメーション効果がきいておりまして、一部削除させて頂きました。

削除された内容としては、
１．多発している個人情報漏えい事件の例
２．それによって、企業として払わなければならないコスト
３．クレジットカード会社の個人情報漏えいに対する罰金規定
になります。

弊社の資料にて暗号化に関する有益な情報が得られたら嬉しいかと思っております。
それから、非常に強力な暗号化機能を提供している弊社の製品であるD’Amoに注目をして頂ければと思っております。

引き続き、宜しくお願い申し上げます。

ペンタセキュリティシステムズ株式会社
テクニカルサポートマネージャー 陳 貞喜

Penta SECURITY

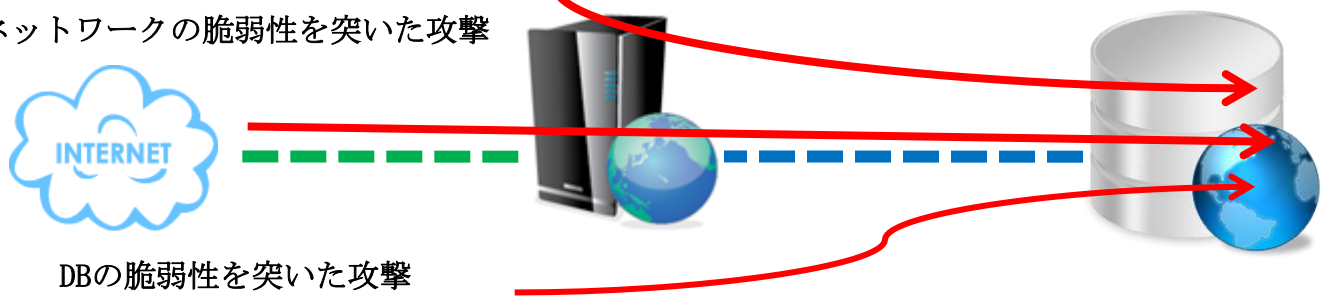
システム管理者及び運用者からの情報漏えい

業務システム開発者及び外注開発者からの情報漏えい

移動保存媒体やバックアップデータからの情報漏えい

Webサーバを経由したDB攻撃
(Ex. SQL Injection)

OSやネットワークの脆弱性を突いた攻撃



DBの脆弱性を突いた攻撃

なぜ、
お客様は暗号化に迷ってしまうのでしょうか？

暗号化に迷う５つの理由

各分野のお客様がデータ暗号化の必要性については強く感じているものの、暗号化システム導入の直前にまで迷う理由を５つ挙げます。

- 暗号化作業中、DBサービス停止が心配
- 暗号化後パフォーマンス低下が心配
- 暗号化鍵の紛失によるデータ復旧が心配
- 震災など自然災害にて暗号化データの復旧が心配
- 暗号化による他のシステムの影響が心配

ペンタセキュリティのD’Amoは、
このような５つの暗号化への心配からお客様を解放します。

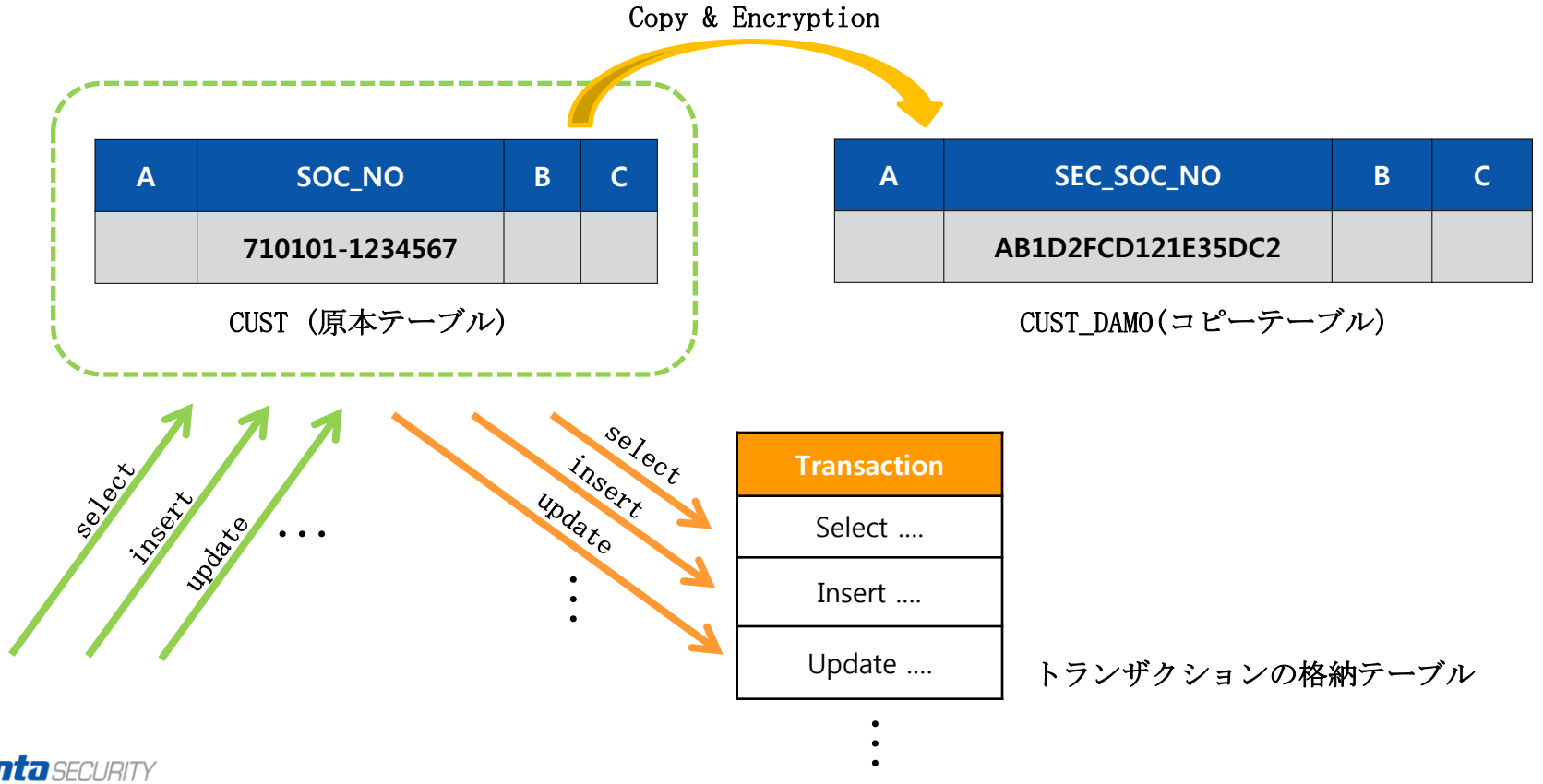
暗号化作業中、DBサービス停止が心配１

D’Amoは、サービスに影響なく暗号化を行います。(1/2)

- ❑ サービス中の暗号化

  コピーテーブルを生成し暗号化作業の際にサービスに影響を及ぼさない方法です。

- ❑ サービス中の暗号化第1段階(コピーテーブルを生成し暗号化)
  - コピーテーブルを生成し、暗号化作業を行います。
  - 第1段階にて対象テーブルの全トランザクション(Insert、Update、Deleteなど)は別途格納され、第2段階の「サービス転換」にて全て反映されます。

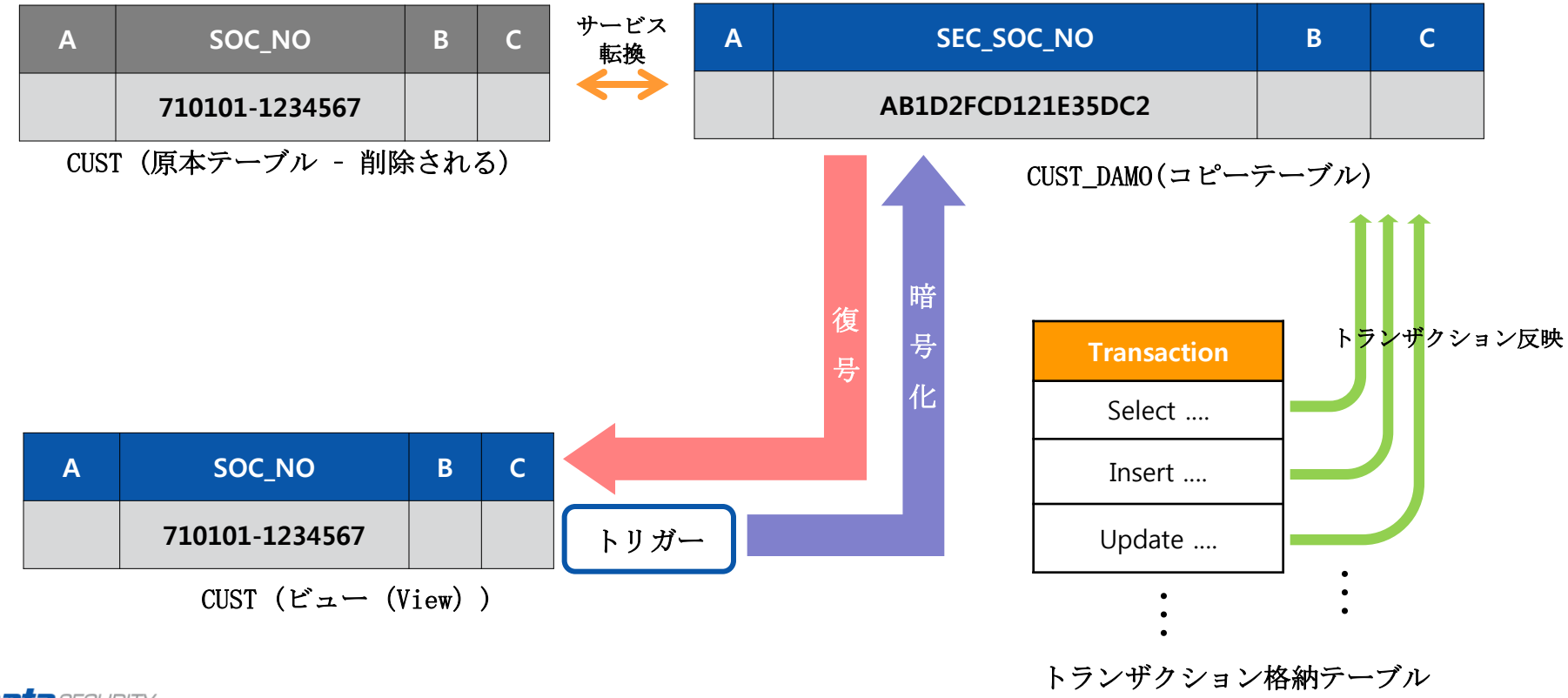


暗号化作業中、DBサービス停止が心配２

D’Amoは、サービスに影響なく暗号化を行います。(2/2)

❑ サービス中の暗号化第２段階(サービス転換)

- 原本テーブルと暗号化されたコピーテーブルのサービスを転換します。
- 転換の際には第１段階にてコピーテーブルに格納されているトランザクションを採用します。
- サービス転換が完了されると原本テーブルは削除され原本テーブルと同じスキーマの「ビュー（View）」が生成されます。
- サービス転換の際に発生するトランザクションは格納されないため、トランザクションの殆どない時間帯（夜）に同作業を行うよう推奨致します。

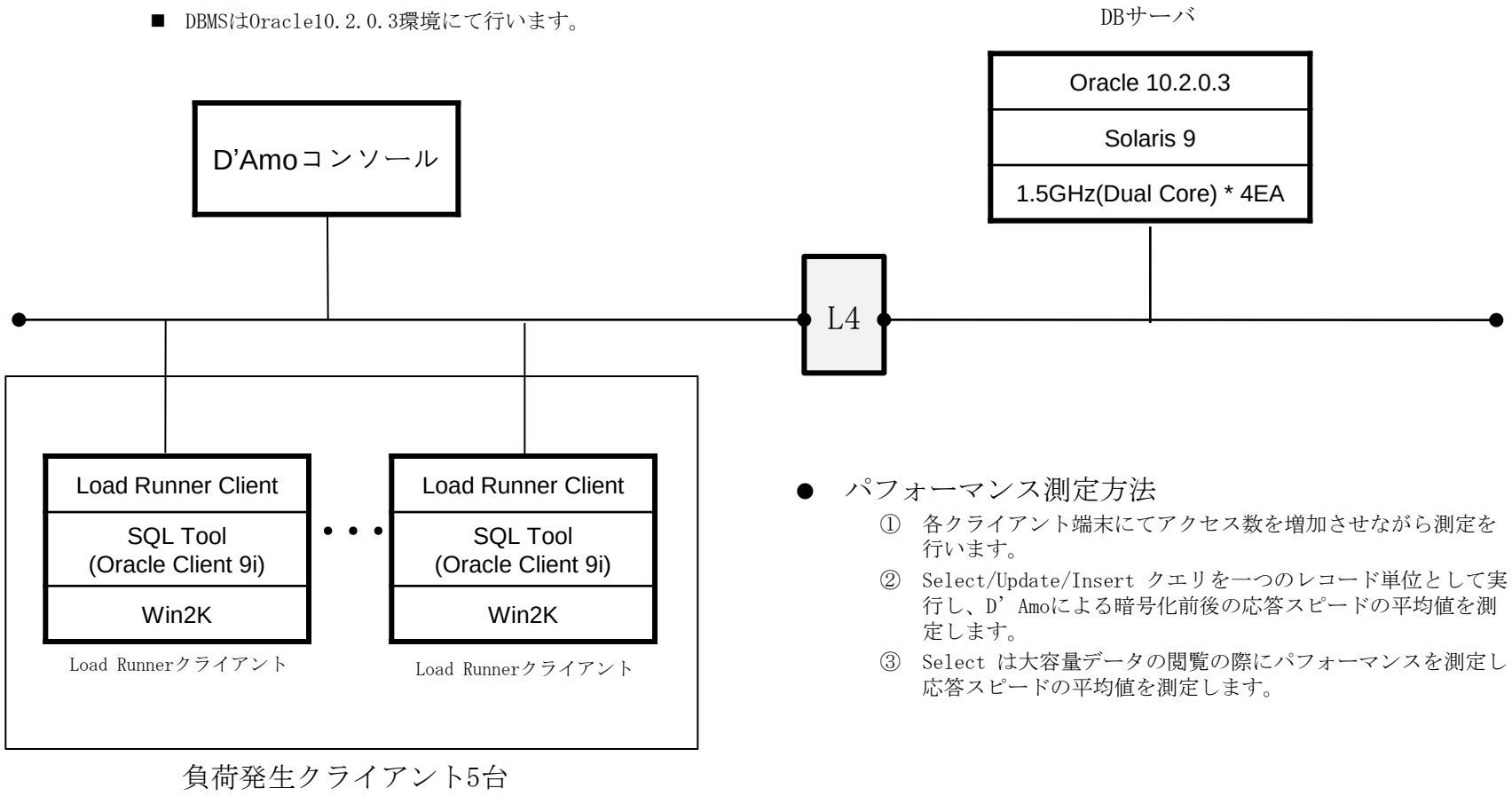


暗号化後パフォーマンス低下が心配１

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(1/8)

❑ パフォーマンス測定の環境情報

- D’Amoの運用中である韓国の代表的な銀行の環境を基準とします。
- パフォーマンス測定環境
  - サーバとクライアントが切り分けされる2-Tier方式にて行います。
  - クライアントPCの５台にて「Load Runner 8.1」をインストールします。
  - DBMSはOracle10.2.0.3環境にて行います。

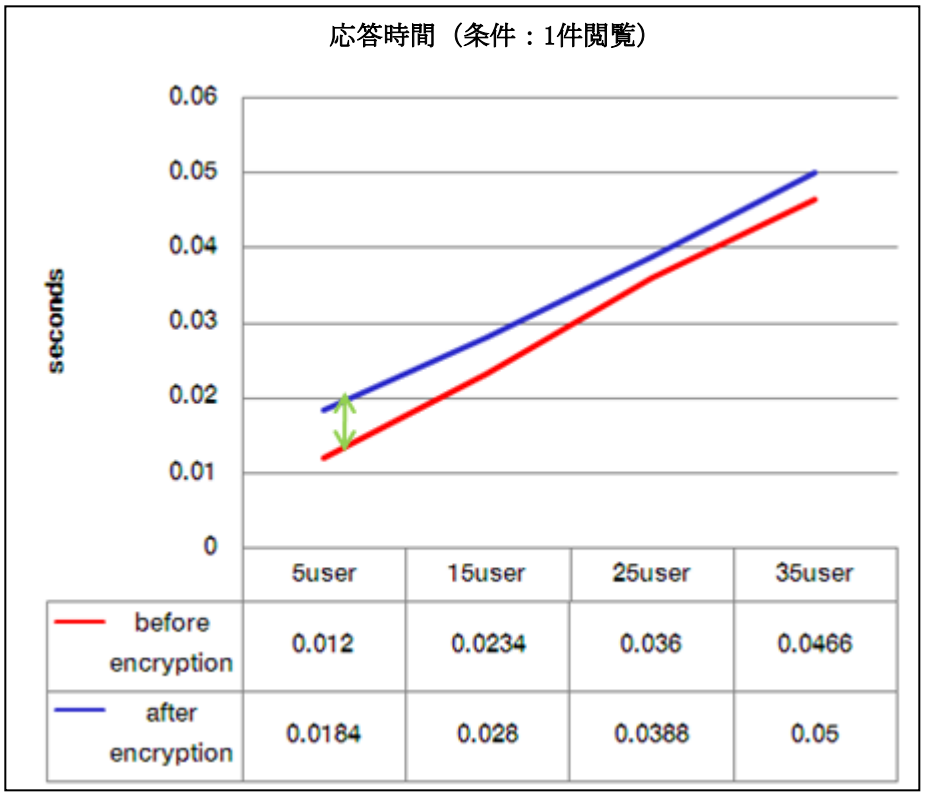


- パフォーマンス測定方法
  - ① 各クライアント端末にてアクセス数を増加させながら測定を行います。
  - ② Select/Update/Insert クエリを一つのレコード単位として実行し、D’Amoによる暗号化前後の応答スピードの平均値を測定します。
  - ③ Select は大容量データの閲覧の際にパフォーマンスを測定し応答スピードの平均値を測定します。

暗号化後パフォーマンス低下が心配２

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(2/8)

- ❑ 応答時間（条件：１件閲覧）
  - ● クエリ条件
    - ■ 条件節にインデックスカラム(ROLECODE)を含む
    - ■ SELECT ID、NAME、ROLECODE FROM TABLE02 WHERE ID = :1 AND ROLECODE = :2



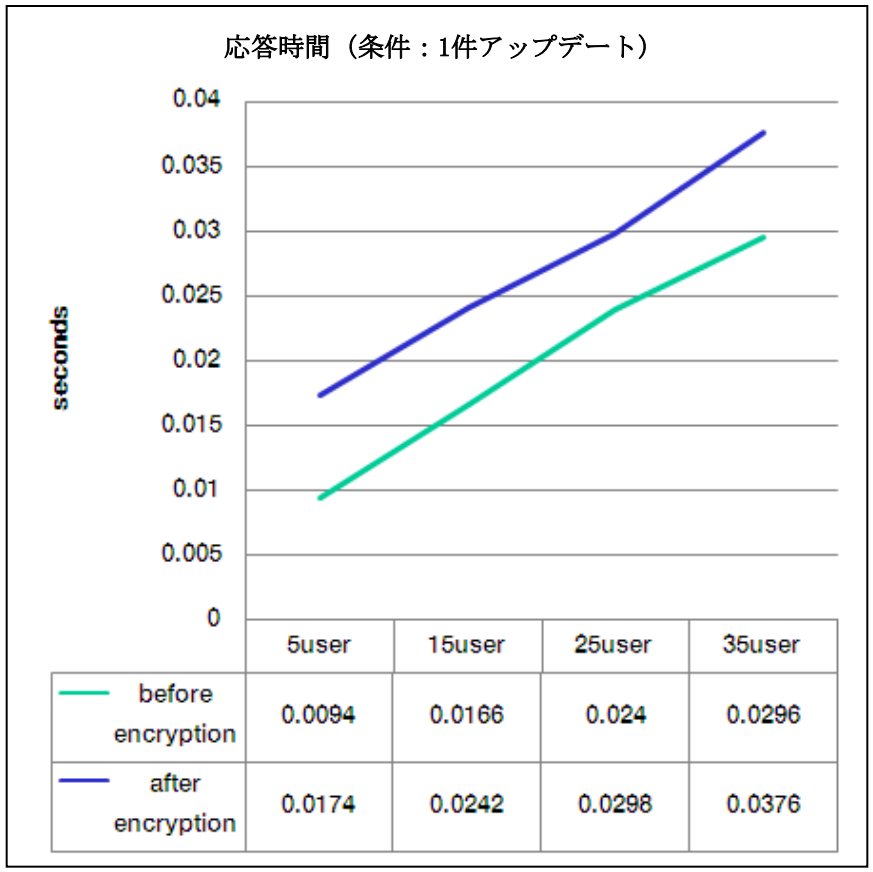
	5user	15user	25user	35user
before encryption	0.012	0.0234	0.036	0.0466
after encryption	0.0184	0.026	0.0388	0.05

暗号化前後の応答時間は平均0.03~0.06秒の範囲内の差があります。

暗号化後パフォーマンス低下が心配３

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(3/8)

- 応答時間（条件：１件アップデート）
  - クエリ条件
    - UPDATE TABLE02 set **NAME** = :1 where ID = :2

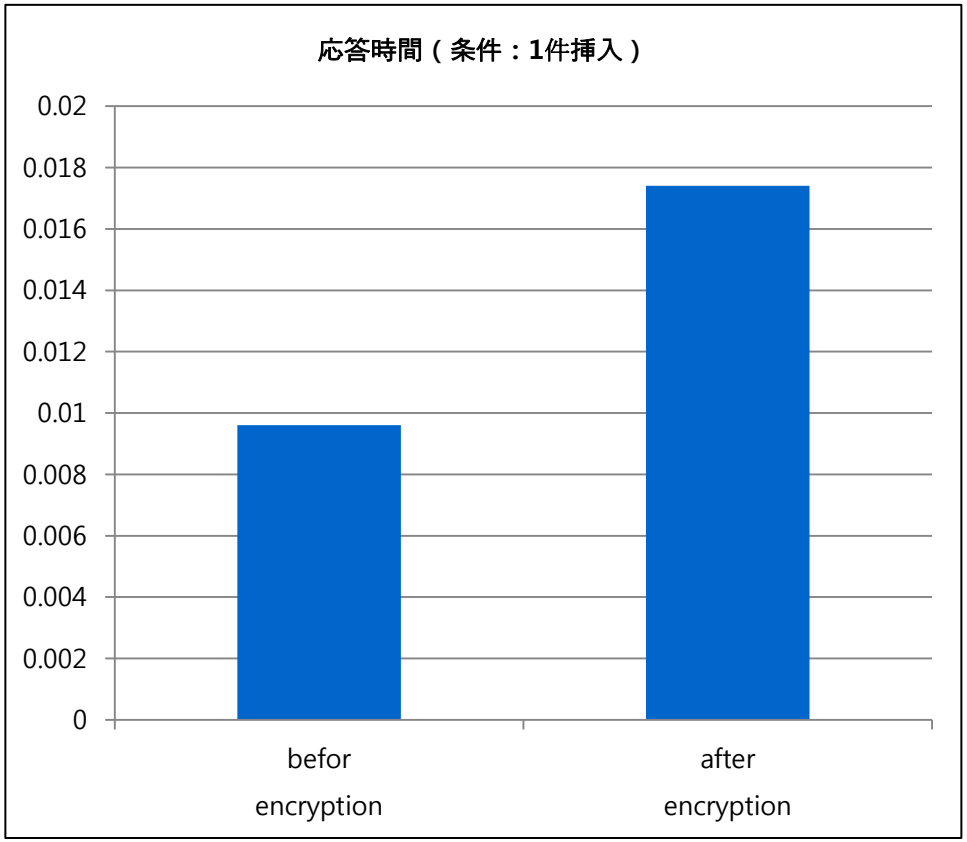


暗号化前後の応答時間は平均0.005~0.008秒の範囲内の差があります。

暗号化後パフォーマンス低下が心配４

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(4/8)

- 応答時間（条件：１件挿入（INSERT））
  - クエリ条件
    - INSERT INTO TABLE02 (ID, **ROLECODE**, **NAME**) VALUES (:1, :2, :3)

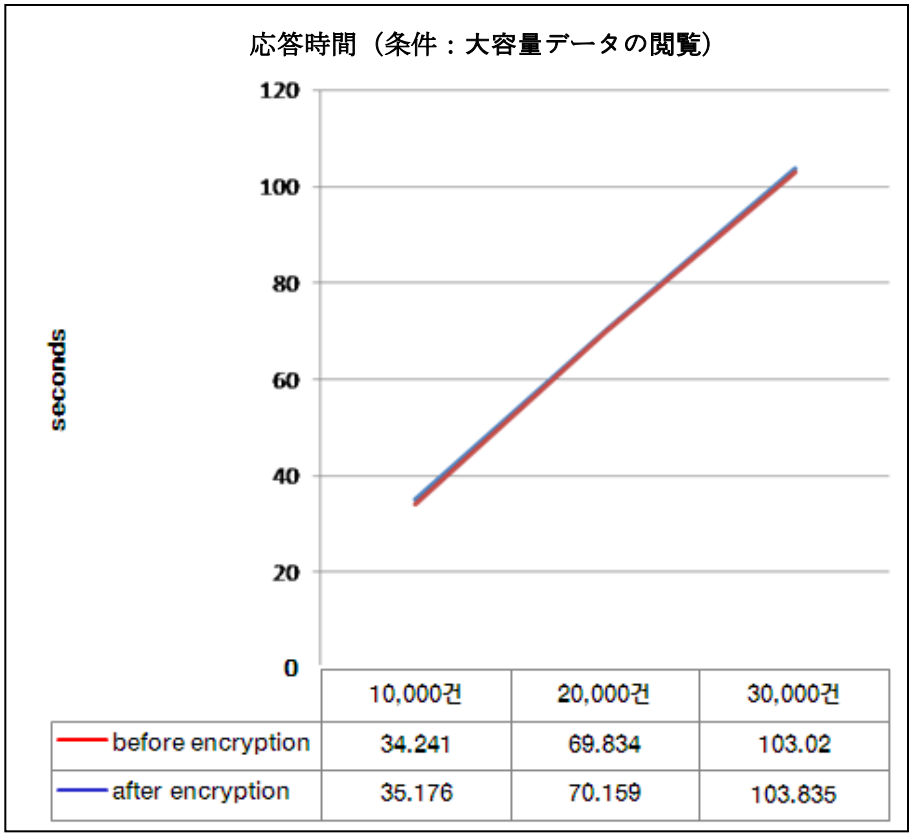


暗号化前後の応答時間は平均0.007秒の範囲内の差があります。

暗号化後パフォーマンス低下が心配５

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(5/8)

- 応答時間（条件：大容量データの閲覧）
  - クエリ条件
    - SELECT TDT, ID, **ROLECODE**, **NAME** FROM TABLE02 WHERE ID BETWEEN :1 AND :2



暗号化前後の応答時間は平均3%の範囲内の差があります。

暗号化後パフォーマンス低下が心配６

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(6/8)

❑ パフォーマンス測定結果

- 暗号化前後のパフォーマンスは殆ど差はなく維持されていることが分かります。

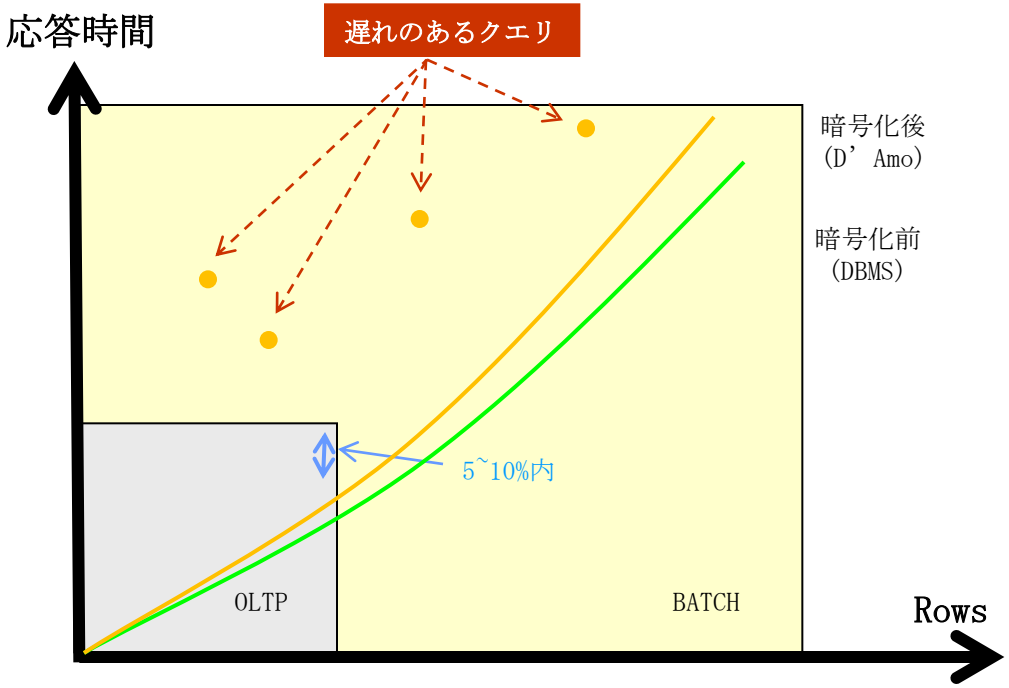
クエリ条件（応答時間）	測定結果（暗号化後平均値）
１件閲覧	0.03~0.06秒
1件アップデート	0.005~0.008秒
1件挿入	0.007秒
大容量データの閲覧	3%

暗号化後パフォーマンス低下が心配？

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(7/8)

❑ クエリチューニング（最適化作業）

- パフォーマンス測定の結果から一般クエリの場合、暗号化前後のパフォーマンス低下が殆ど見られませんが、一部のクエリは応答時間の遅れが発生することがあります。
- 主に暗号化データを「Full-Scan」をしたクエリの場合、全データにアクセスする度に暗号化・復号のプロセスを行うため、応答時間の遅れがあります。
- D’Amoでは、クエリチューニング（最適化作業）を行い、アクセスをする度に暗号化・復号が行われずに暗号化データを直接読み込むように修正をするため、パフォーマンス低下を最小限にすることができます。



一般クエリは5~10%内サービスされるため、パフォーマンス低下は殆ど見られません。

＊遅れのあるクエリとは、Full-Scanクエリを意味します。

暗号化後パフォーマンス低下が心配８

D’Amoは、パフォーマンス低下を最小限にする暗号化を行います。(8/8)

❑ クエリチューニング（最適化作業）例

- 原本テーブル(CUST)ではない暗号化テーブル(CUST_DAMO)にて平文データ(SOC_NO)ではない暗号化データ(SEC_SOC_NO)を読み込みをし、最終結果値のみ復号の関数(DAMO.DEC_VARCHAR)を実行することによって、検索の途中では復号のプロセスが行われないようにします。（最終結果値のみ復号を行います。）
- Inline Sub-Queryの結果の10万件のうち、最終結果値20件

```
SELECT A.SOC_NO FROM (SELECT C, SOC_NO FROM CUST) A, CUST_DEP B
 WHERE A.C = B.C;
```

10万件のデータに対しSub-Queryを実行すると、10万件の復号が行われます。

```
SELECT DAMO.DEC_VARCHAR ('OWNER', 'CUST', 'SOC_NO', A.SEC_SOC_NO)
FROM (SELECT C, SEC_SOC_NO FROM CUST_DAMO) A, CUST_DEP B
 WHERE A.C = B.C;
```

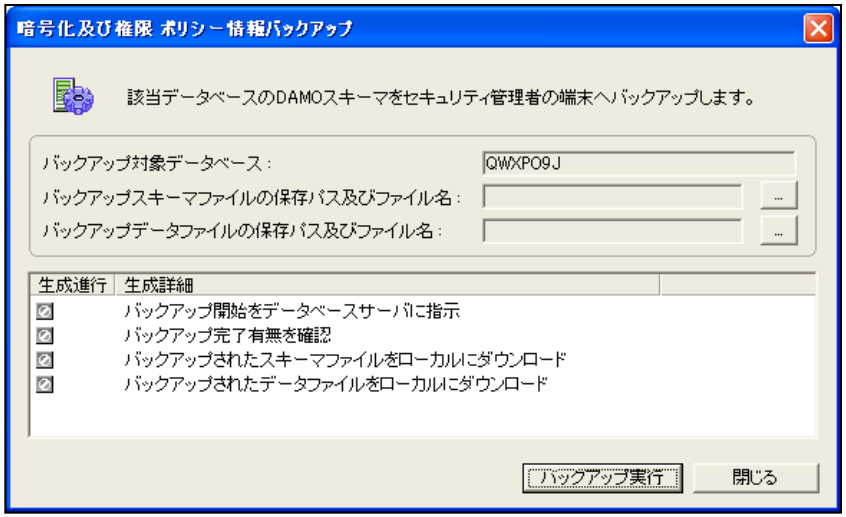
10万件のデータは暗号化データにて直接読み込み、最終結果値の20件のみ復号関数を採用します。

- 暗号化を行うと、殆どのクエリはパフォーマンス低下が見られませんが、 暗号化データに対しFull Scanをする一部のクエリは応答時間に遅れができてしまうことがありますので、D’Amoではクエリチューニング（最適化作業）によって暗号化前とパフォーマンス差のないようにします。

暗号化鍵の紛失によるデータ復旧が心配

鍵管理の必要性

- 鍵は暗号化データと直結されているため、第３者に漏洩されるとセキュリティ的に危険な状況になります。
- 鍵はセキュリティ管理者のみによって発行及び管理されなければなりません。セキュリティ管理者が鍵を紛失すると、暗号化データの復号及び障害時データ復旧が不可になります。
- 鍵の紛失に対応するため、必ず鍵のバックアップなどを行っておくように推奨致します。
- **鍵バックアップ**
  - サイト鍵及びDB鍵のバックアップ: 鍵ファイルをバックアップし管理
  - カラム鍵(暗号化鍵)ぼバックアップ: カラム鍵の情報を格納しているSecure DBをバックアップ、D’Amoコンソールの「セキュリティポリシーのバックアップ」メニューにて行います。

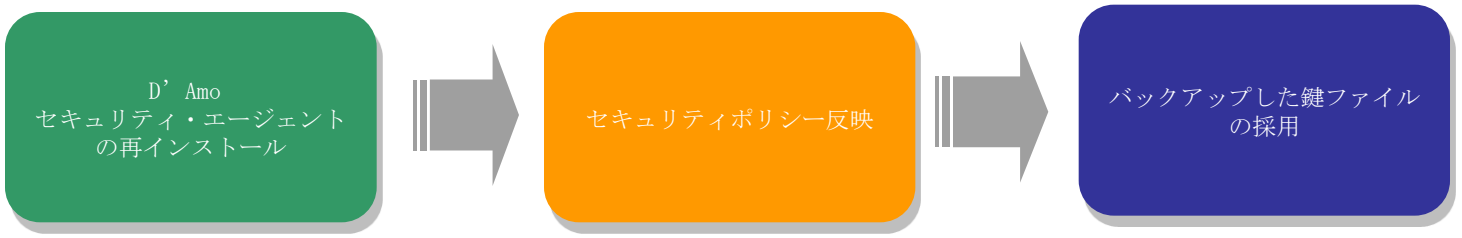


震災など自然災害にて暗号化データの復旧が心配

鍵管理及びセキュリティ・エージェントによる復旧

- 震災対策として鍵バックアップ及びセキュリティポリシーバックアップが正常に行われていると暗号化データは復旧することができます。

- 復旧プロセス
  - サイト鍵、コンソール鍵、DB鍵はバックアップした鍵を採用します。
  - D’Amoのセキュリティ・エージェントのインストール後、バックアップしておいたセキュリティポリシーにより既存環境を構築します。
  - 鍵及びセキュリティポリシーのバックアップファイルにより、既存の環境が構築された時点にて暗号化データの復号及び新規暗号化が可能になります。
  - データ暗号化は、国際標準方式(暗号化アルゴリズム、ブロック暗号化方式、初期化ベクトルなどを採用）であり、鍵のみ正常にバックアップされていると、セキュリティ・エージェントのバージョンとは関係なくデータ復旧ができます。



D’Amo復旧プロセス

暗号化による他のシステムの影響が心配１

環境ヒアリングにより暗号化の影響を事前分析

- CPU、メモリ使用率、暗号化対象になるデータ、連動サービスなどを事前に確認する環境ヒアリングを行い、暗号化後の影響を分析し導入を行います。

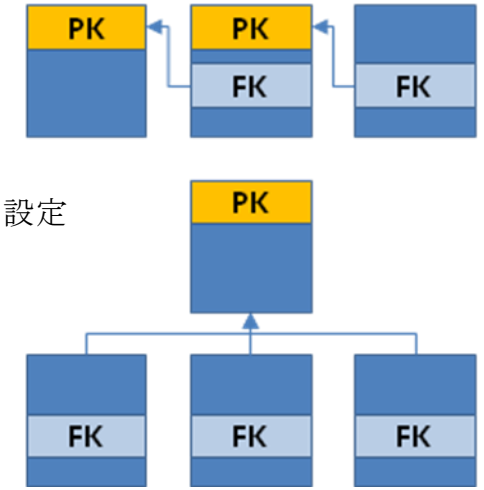
COLUMN ENCRYPTION INFORMATION		
QUESTION		ANSWER
Columns to be encrypted	Target information to be encrypted	
	Table size and the number of rows containing the columns to be encrypted	Size : The # of Rows :
Whether trigger exists in the table containing encrypted column	(If trigger exists, please also answer whether encrypted column is in the trigger body or not.)	
Whether columns – even though not encrypted - with default setting exist in the table containing encrypted column	(Please also answer if it's ok to change the condition of the column with default setting to 'not null'.)	
Whether the table containing encrypted column is used with 'materialized view'	(If yes, please also answer how many number of DBMS are related to MVIEW.)	
Whether the column to be encrypted uses Index or PK-FK	(If it uses PK, please also answer how many tables are related as FK.)	
Whether the table containing encrypted column is included in clustering?		
Whether the DB Service is duplicated	(In RAC environment, two D'Amo packages are needed.)	
Whether XA connection is used	(XA connection is a DB connection to be used for 2-phase commit.)	
Whether the DB service is working in archive mode		

環境ヒアリングシート

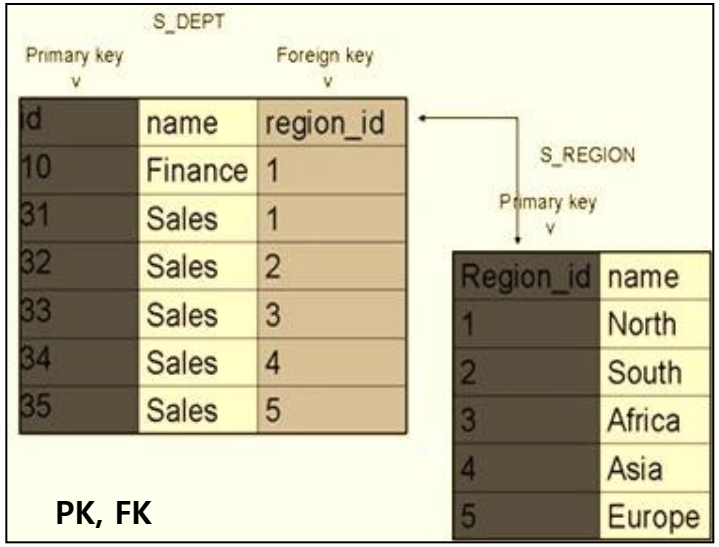
暗号化による他のシステムの影響が心配２

Key export及びimportによる同様な設定にて暗号化

- 暗号化データがPK-FKなどにて連動されている場合、連動されている全てのデータを暗号化しなければなりません。
- Primary Key (PK)
  - Primary keyとは、テーブルにて各レコードが重複されず雄一な値を持つよう設定されているカラムです。
- Foreign Key (FK)
  - Foreign keyとは、primary keyを参照にするカラムです。
- PK-FKカラムの暗号化
  - Primary KeyとForeign Keyは、お互いデータを連動し採用しているため、片方の暗号化の際には連動されている残りの片方も暗号化をしなければなりません。
  - 同じデータの暗号化値は同じ値を持つよう、同じ値に対する同じ暗号化値を持つ初期化ベクトル（Fixed）を採用し暗号化しなければなりません。



PK-FK 関係



PK, FK

Penta SECURITY

暗号化について、お客様を迷わせない、

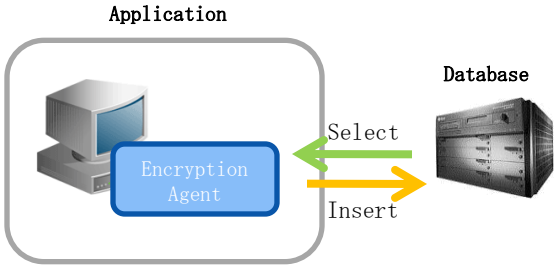
D’Amoは、
データ保護のトータル・セキュリティ・ソリューションです。

DB暗号化の方式

DB暗号化の方式は、大きくAPI、Plug-In、TDEの３つがあります。

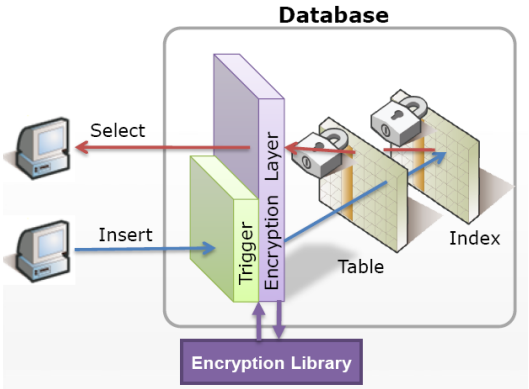
API

- アプリケーションにて暗号化を実行
- DBにこだわらず暗号化可
- 暗号化対象関連の全クエリを修正しなければならない
- アクセス制御と監査機能なし



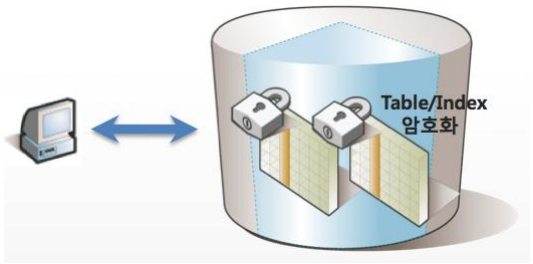
Plug-In

- DBにPlug-Inタイプで暗号化モジュールをインストール
- アプリケーションと別に動作してあるため、クエリ修正は最小限
- 暗号化カラムのインデックスに対応
- 暗号化、アクセス制御、監査のトータルセキュリティサービスを提供



TDE

- DBエンジン中に暗号化機能が実装
- アクセス制御及び監査機能に対応するためには別途パッケージが必要
- トータルセキュリティに難しく、直感的ではない

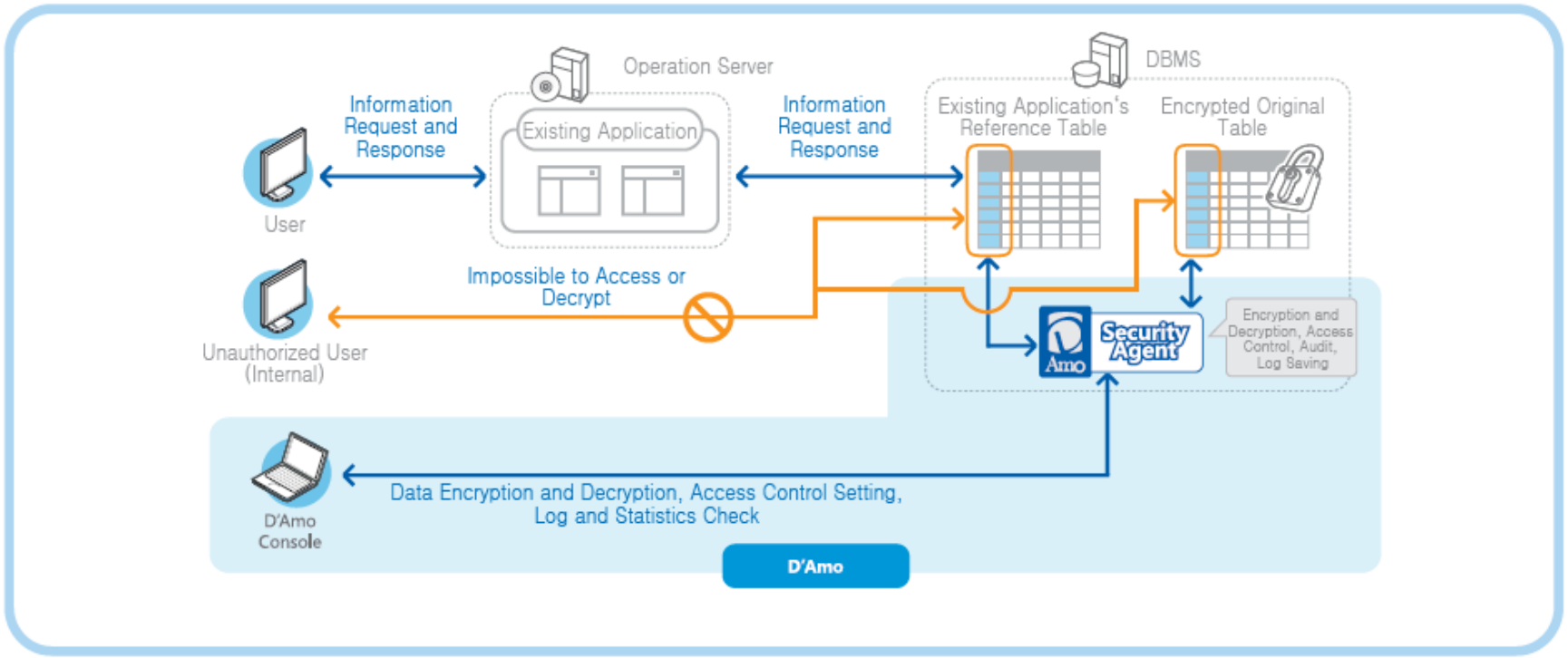


ペンタセキュリティのD'Amoは、
暗号化、アクセス制御、監査のトータルセキュリティソリューションを提供致します。

D'Amoの暗号化仕組み

D' Amo構成

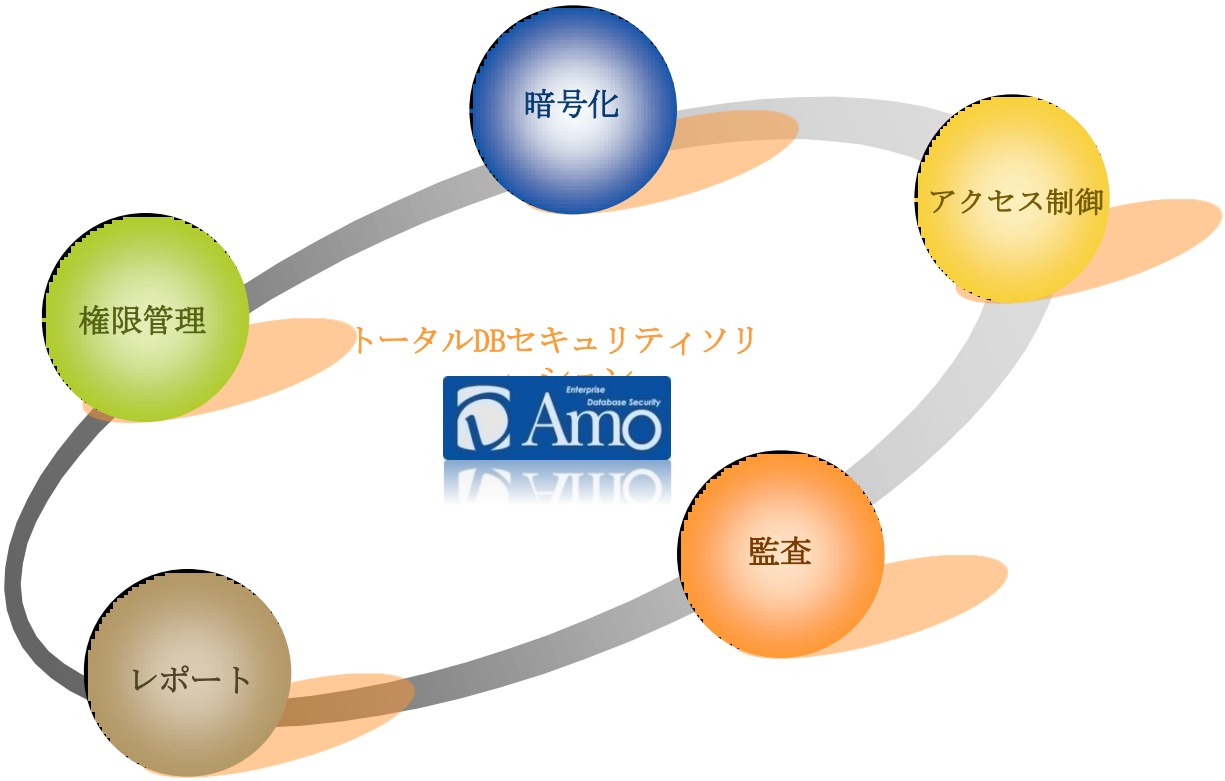
- D' Amoは、D' AmoコンソールとD' Amoセキュリティ・エージェントにて構成されております。
- D' Amoコンソールは、GUI基盤の管理ツールによってユーザが直感的に暗号化・復号、アクセス制御の設定、ログ及び統計情報の確認をすることができます。
- D' Amoセキュリティ・エージェント(SA)は、plug-in方式にてDBにインストールされ暗号化・復号、アクセス制御、監査、ログ記録などを実行します。



トータルセキュリティソリューション、D’Amo

完璧なデータ保護のためのトータルセキュリティソリューション、D’Amo

- D’Amoは、暗号化だけではなく、アクセス制御及び監査の機能をトータルで提供する、根本的なDBセキュリティソリューションです。
- 2004年韓国にてリリースされた以来、国内約80%のマーケットシェアとなり、韓国DB暗号化市場1に誇るトータルソリューションです。



韓国本社
韓国ソウル市永登浦区汝矣島25-11 韓進海運ビル20階
TEL : 82-2-780-7728 FAX : 82-2-786-5281
www.pentasecurity.com
Penta Security Systems Inc.

日本本社
東京都港区赤坂3-2-8アセンド赤坂3階
TEL: 81-3-5573-8191 FAX: 81-3-5573-8193
www.pentasecurity.co.jp
Penta Security Systems K.K.