

暗号化 for SQL Server

概要

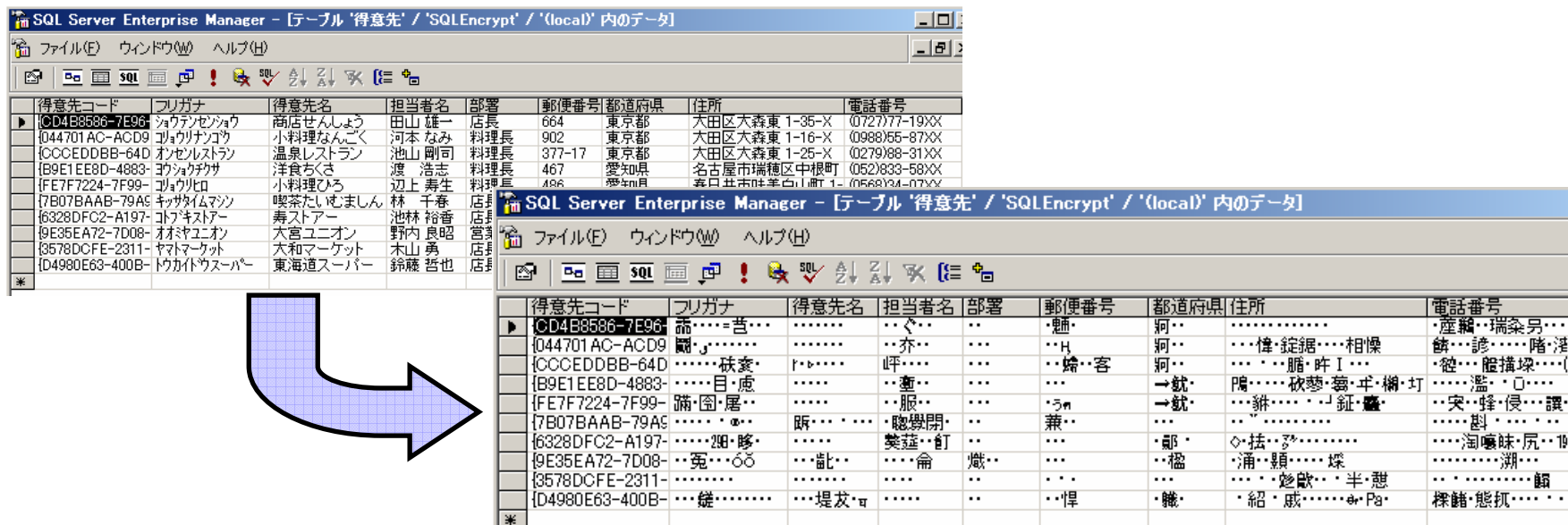
株式会社エイ・エヌ・テイ

暗号化 for SQL Server とは

- 情報漏洩問題に対するピンポイントソリューション
 - Microsoft SQL Server 2000データベースに特化
- SQL Server ネイティブ対応
 - 拡張ストアドプロシージャとして暗号化エンジンを実装
 - 高速
 - 通常のSQL文にて容易に実装可能
- 強力かつ柔軟な暗号化
 - カラム単位の暗号化指定
 - 用途に応じた2つのエディション
 - スタンダード版
 - ANT独自開発の暗号エンジンを搭載。ハッシュ暗号化エンジンを採用、暗号化したデータでも部分一致などの柔軟な検索が可能。
 - C4版
 - 株式会社シーフォーテクノロジー社製の暗号エンジンを搭載。カオス理論にもとづく高い乱数性が保証された高速で強度な暗号化を実現。

目的

- 機密データの暗号化により、顧客情報の流出を防ぎます
 - データベースに格納されるデータそのものを暗号化します
 - 正規のアプリケーション以外 (SQLツールやAccessなど) からアタックしてもデータが見えません
 - SQL Serverの物理ファイルが流出しても、暗号キーが盗まれない限り解読できません



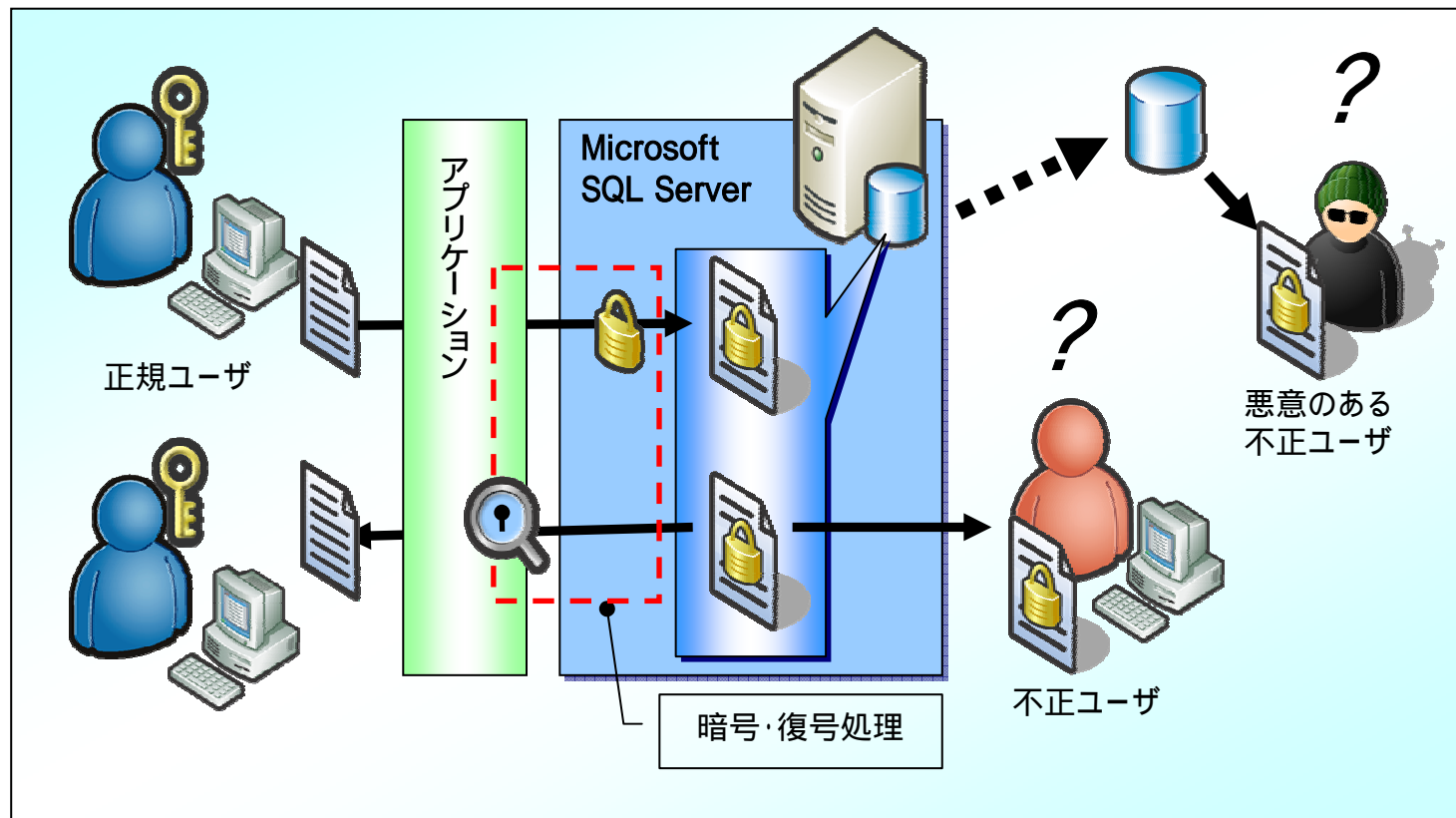
SQL Server Enterprise Manager - [テーブル '得意先' / 'SQLEncrypt' / '(local)' 内のデータ]

得意先コード	フリガナ	得意先名	担当者名	部署	郵便番号	都道府県	住所	電話番号
CD4B8586-7E96	ツウテンショウ	商店せんしょう	田山 雄一	店長	664	東京都	大田区大森東 1-35-X	(072)777-19XX
044701AC-ACD9	ツウリナゴウ	小料理なんごく	河本 なみ	料理長	902	東京都	大田区大森東 1-16-X	(0988)65-87XX
CCCEDDBB-64D	オンセルストラ	温泉レストラン	池山 剛司	料理長	377-17	東京都	大田区大森東 1-25-X	(0279)88-31XX
B9E1EE8D-4883	ツウカチカ	洋食ちくさ	渡 浩志	料理長	467	愛知県	名古屋市長瀬区中根町	(052)833-58XX
FE7F7224-7F99	ツウカヒロ	小料理ひろ	边上 寿生	料理長	486	愛知県	春日井市味平白川町 1-	(0563)34-07XX
7B07BAAB-79A9	キツカタイムツ	喫茶たしゅましん	林 千春	店長				
6328DFC2-A197	トバキスター	寿スター	池林 裕香	店長				
9E35EA72-7D08	オオキユニオン	大宮ユニオン	野内 良昭	営業				
3578DCFE-2311	ヤママーケット	大和マーケット	木山 勇	店長				
D4980E63-400B	トウカイウスーパー	東海道スーパー	鈴藤 哲也	店長				

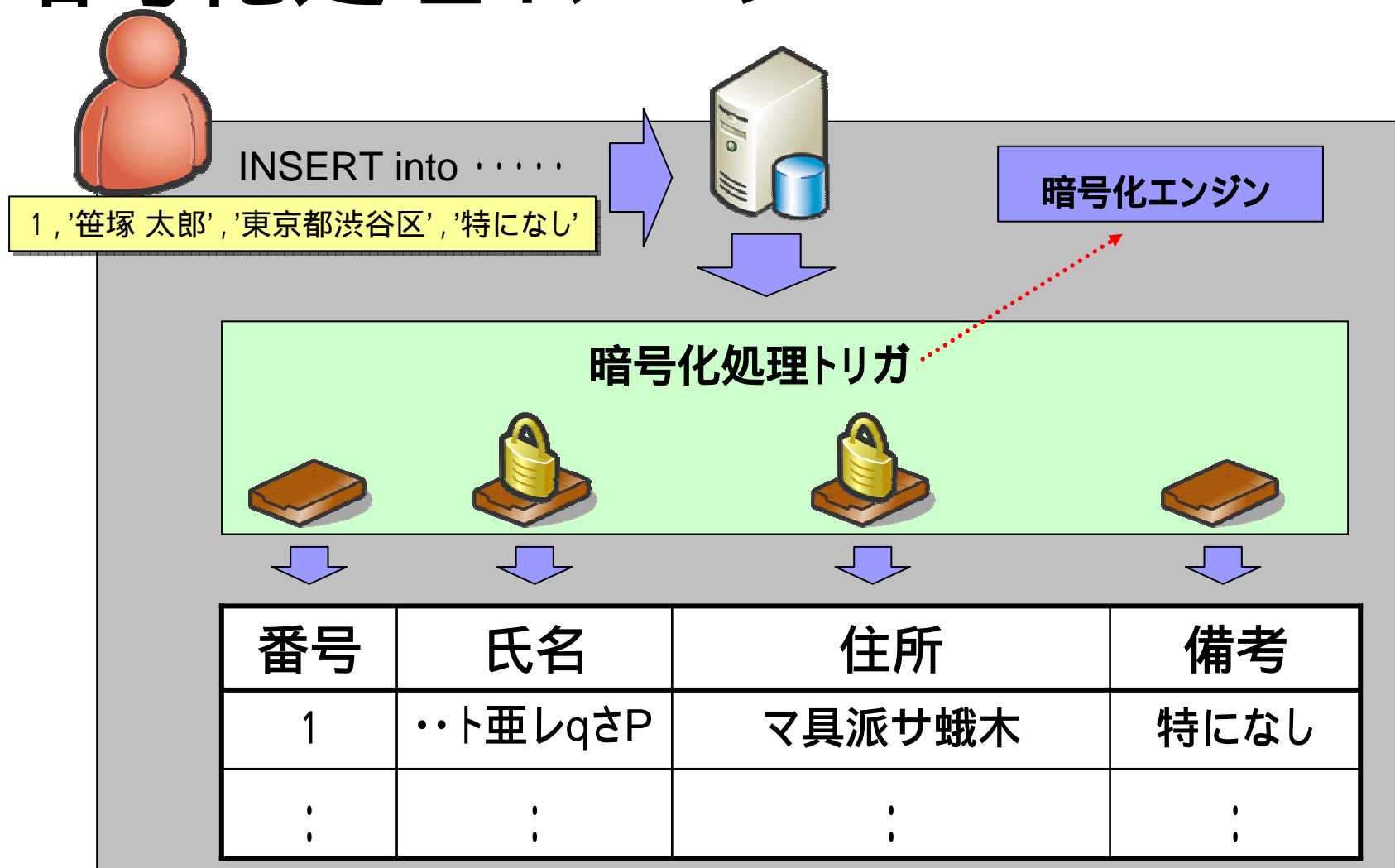
SQL Server Enterprise Manager - [テーブル '得意先' / 'SQLEncrypt' / '(local)' 内のデータ]

得意先コード	フリガナ	得意先名	担当者名	部署	郵便番号	都道府県	住所	電話番号
CD4B8586-7E96	商.....告...	河..
044701AC-ACD9	商.....	河..
CCCEDDBB-64D	河..
B9E1EE8D-4883	一.....
FE7F7224-7F99	一.....
7B07BAAB-79A9
6328DFC2-A197
9E35EA72-7D08
3578DCFE-2311
D4980E63-400B

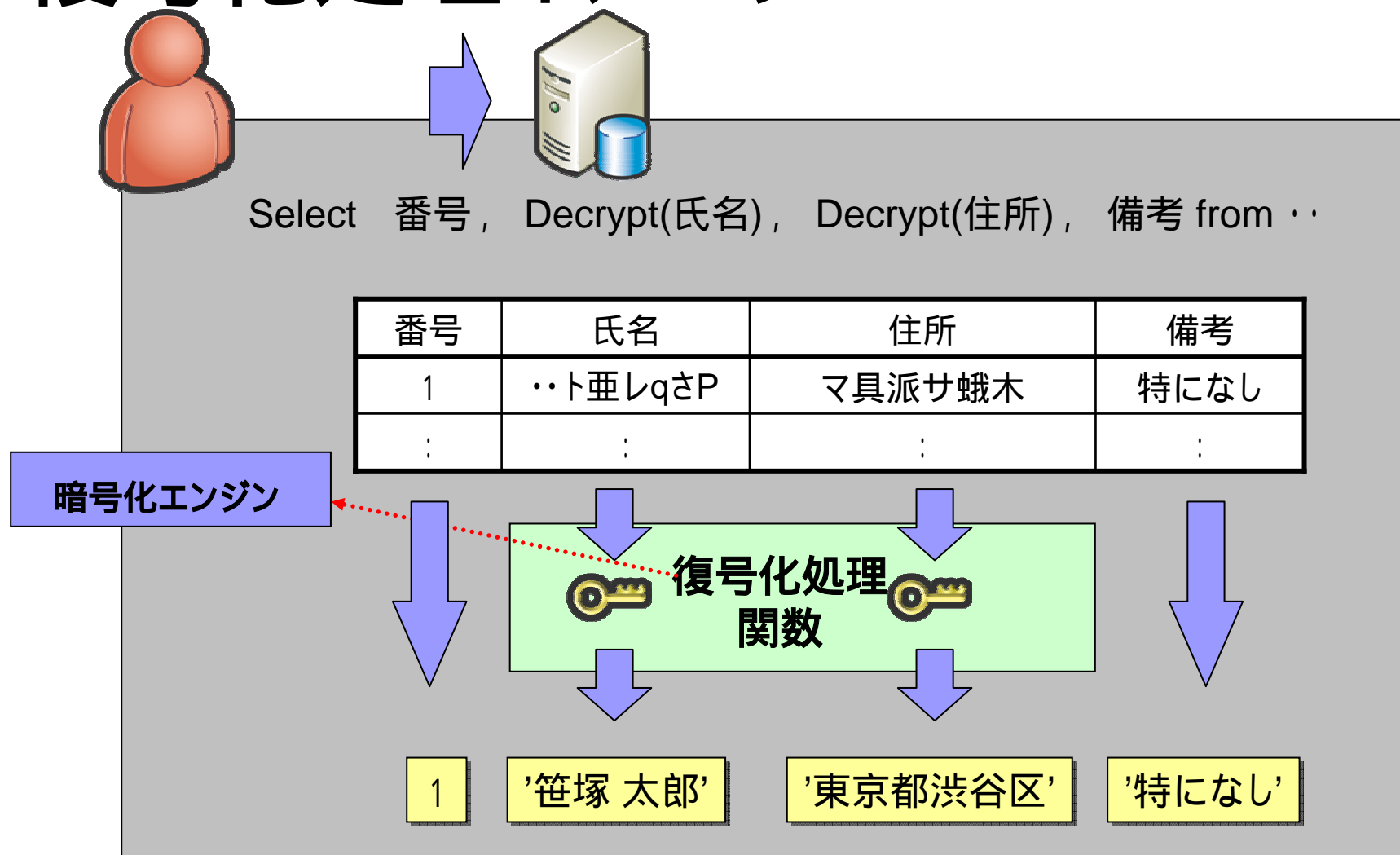
目的 (概念図)



暗号化処理イメージ

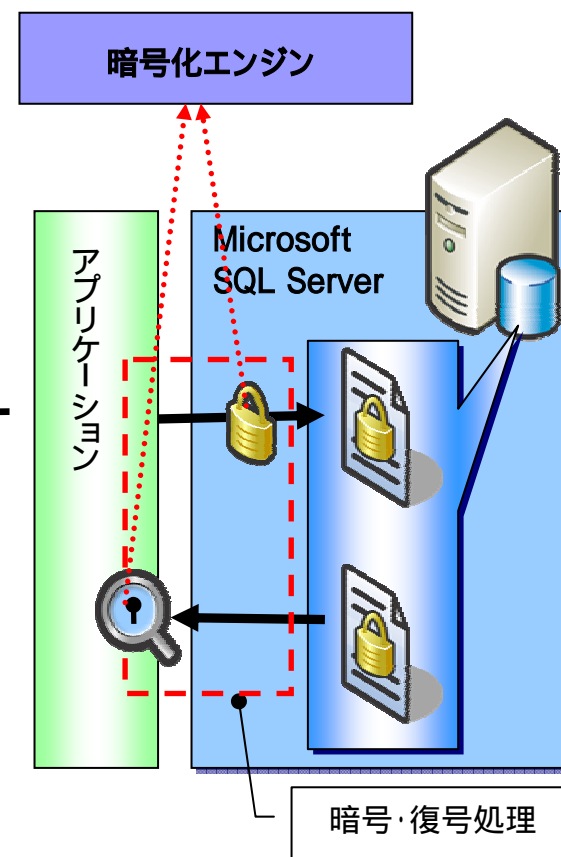


復号化処理イメージ



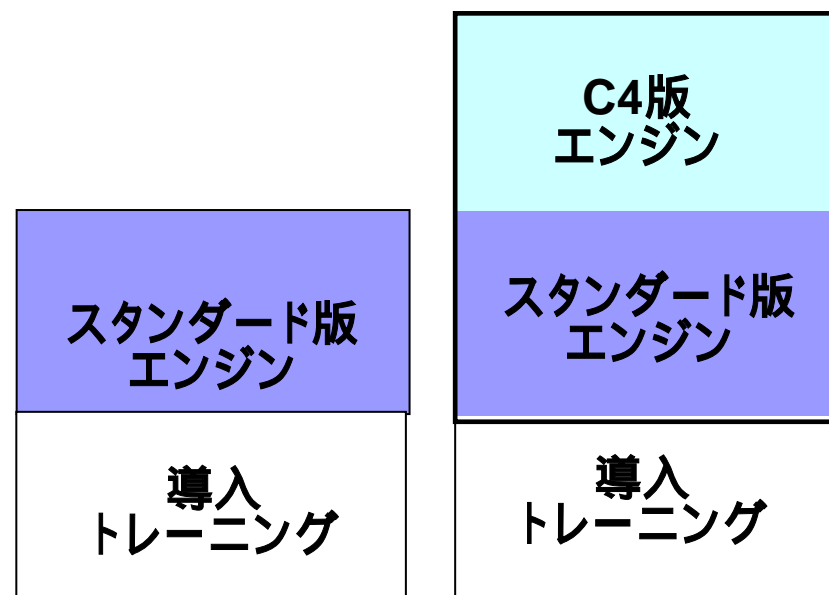
暗号化/復号化の実装手順

1. 暗号化すべきデータ列を決定します
 - 例:「顧客」テーブルの「会社名」「住所」「ご担当者」「メールアドレス」列
2. 暗号化をセットアップします
 - 「暗号化 for SQL Server」をインストールします
 - 暗号化キー登録を初期化します
3. データベースに暗号化を導入します
 - 既存データを暗号化します
 - 既存システムへ導入する場合に必要です
 - 対象テーブルにトリガを実装します
4. アプリケーションに復号化を導入します
 - SELECT文に復号化関数を追加します
5. 結果をテストします
 - アプリケーションにて入出力、および検索結果をテストします



商品構成

- 「暗号化 for SQL Server」CD
 - 暗号化エンジン
 - 暗号化強度に応じた2オプション
 - ドキュメント
 - インストールガイド
 - ユーザーズガイド(拡張ストアドプロシージャリファレンス)
- SQL Server 技術者向け導入トレーニング
 - 初回のみ
 - 弊社エンジニアによる半日トレーニング
 - 実装するためのチュートリアルプログラムおよび導入ガイド
 - サンプルコード



スタンダード版
¥ 1,000,000

C4版
¥ 1,380,000

* 同一ユーザへの2つ目のオーダーからはトレーニングなしでエンジンだけの販売が可能。
(追加ライセンス)

スタンダード版 VS C4版

エンジン	暗号化強度	性能	検索可否	結果の類似性
スタンダードエンジン	抑止効果として十分	非常に高速	前方一致、後方一致 完全一致が可能	全体
C4エンジン 標準モード	非常に高い	高速	前方一致、完全一致が可能 後方一致は不可能	先頭部分のみ
C4エンジン 強化モード	解読は不可能	高速	X 完全一致のみ可能	なし

* スタンダード版はスタンダードエンジンのみ使用できます

* C4版はすべてのエンジンを使用でき、カラム単位で選択することができます

導入トレーニング

■ 半日オンサイトトレーニング

□ 目的

- 御社技術者が暗号化を実装できる

□ 対象

- 御社SQL Server技術者(1回あたり最大5名様まで)

- SQL Server機能(トリガ、ユーザー定義関数)、およびT-SQLの基礎知識が前提

□ 教材

- 弊社オリジナルテキストおよびチュートリアルプログラムを使用

□ 購入形態

- 初回製品購入時に同梱
- 追加開催については別途ご相談承ります

オプションメニュー

■ 導入コンサルティング

□ 目的

■ 複雑なデータベース環境における導入方式設計支援

- データ型変換(スキーマ変更)、複数システムの連携するデータベース、レプリケーション環境、バッチによるデータ転送環境、高度な暗号化キー運用、アプリケーション分析、など

□ 実施形態

- 週次定例ミーティングを開催ください(1回2~4時間程度)
- 課題の抽出および解決案をご提示いたします

□ 購入形態

- ¥1,000,000 / 月より月次ご契約とさせていただきます
- 納品物: QAシート

(参考) 制限事項

- アプリケーションを修正することができない場合、原則として適用することができません。
- 暗号キーを損失した場合は暗号データを復号することはできません。
- 暗号化対象列のデータ型は nvarchar/nchar/varbinary/binary をサポートします。既存データがそれ以外の場合、データ型の変更が必要になります。
- 暗号化対象列の照合順序は JAPANESE_BIN にしてください (照合順序は列ごとに指定できます)。
- 暗号化対象の SQL Server インスタンスにおいて、「Windows NT ファイバー」機能を使用することはできません。
- 暗号化/復号化関数を利用するオブジェクトはスキーマバインディングできません。