CubeOneのご紹介

-カラムレベルデータベース暗号化ソリューション -

eGlobal
Global Technology, Make IT easy

企業紹介

- 企業名： (株)イーグローバルシステム(eGlobal Systems Co., Ltd)
- 設立時期： 2004年10月
- 分野： ITセキュリティ / Database暗号化
- 製品名： CubeOne
- 従業員： 19名(ほとんど専門エンジニアー)
- 売上： 3年平均売上7億円
- パートナーネットワーク： 国内20社(リセラー)と海外1社

Intro I 重要個人情報

マイナンバー

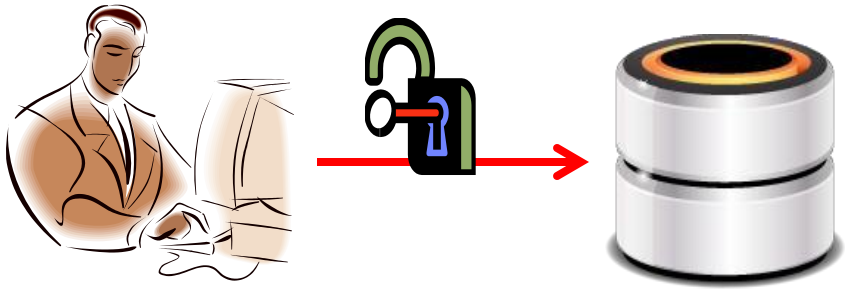
クレジットカード番号

銀行の口座番号

…、パスポートナンバー、医療記録、暗証番号など

Intro I 個人情報を保護する二通りのの方法

アクセス制限



すべき…

データベース暗号化

必ずすべき。

もしDataが漏れても被害を最低限に抑えられるため、
敏感な個人情報を保護する根本的な方法である。

Premium DBMS Encryption Solution

大容量のデータベースに適合したカラムレベル暗号化ソリューション

High Performance

- Encrypted index searching supporting
- Fast encryption/decryption performance

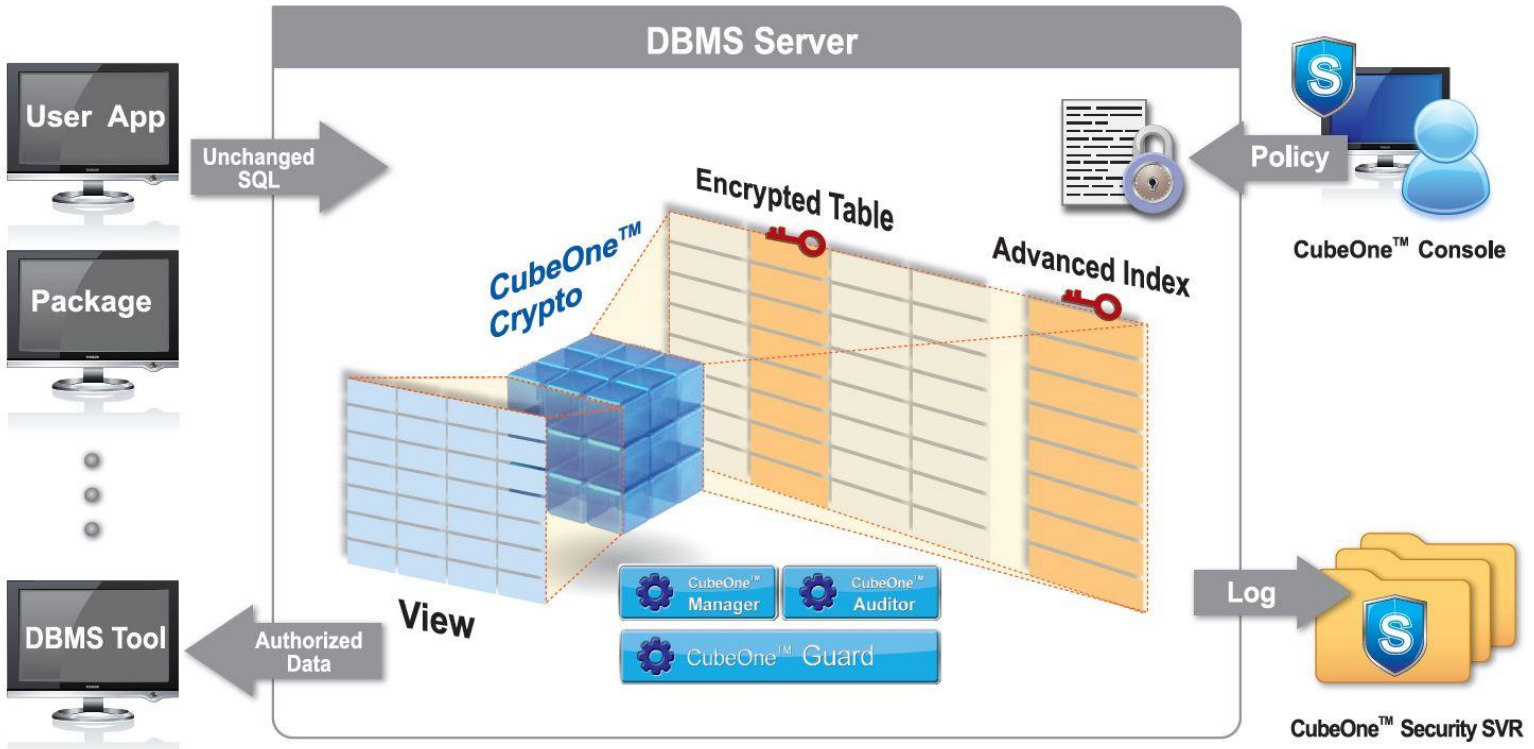
Large Capacity

- Low performance drop for the encryption application
- Simultaneous processing capability

No Downtime

- Fault-tolerance structure

I システムの概念図(Plug-in)



金融、製造、通信、公共機関などのあらゆる分野で600の顧客会社と6,500以上のサーバーに設置

1 カラムレベルの暗号化

必要なカラム、つまり重要な個人情報が入ったカラムのみ暗号化する有効な方法
(一方、テーブルスペース方式はテーブル全体を暗号化する)

CUST_NO	CUST_NAME	CARD_NO	PASSWD	REG_DATE	BONUS	COMM	GRADE_NO
1	G.M.X	XFFUJWuYDxkJPrrb8ZEb5olU3sN9OASs1upnEK8T5yE=	WXARDYWWPV	2016-01-26	0.1	1.001	4
2	Y.H.U	Z/kcJAA+S9pEA6xFz84R7UUeoaUmVToe2BNlGyH9AcU=	TTGPOVFNUB	2016-01-26	0.2	2.002	3
3	H.Q.B	wWmbZ9yCA12iaD5k7DTWiVK4k4gpJiUkKNKAvLlgrl8=	OHPDAEEYDB	2016-01-26	0.3	3.003	4
4	T.T.M	ZjWpjFRj8+iyy3brRaS2qkXPcGiKBm3APj+uQfUIpcQ=	KMVALKDKKN	2016-01-26	0.4	4.004	3
5	A.O.X	uZ4QRhYDYjpaa4DG7i8Sj0AGLxpWn3XO4NPN4cxKII4=	OUWTMYSXOM	2016-01-26	0.5	5.005	4
6	P.V.O	ft+CpqybNdgetbEtQhKQjDBv4+NW3whdizV+7SsuUbc=	OPRNEGZVDX	2016-01-26	0.6	6.006	2
7	T.D.Q	kjmELW4RpHpT5Utz8mYdVutyPE8TrtYa9yQ/ow34GR0=	ZIDSOFFYMB	2016-01-26	0.7	7.007	1
8	W.Y.C	q/zsMRnjDeOpnfpUDjmlCJ0xT2MWCi/J96A74kAkgzQ=	HPKOPGAZXQ	2016-01-26	0.8	8.008	3
9	B.R.W	pn8ir/LcOw6pTFJb1almJY2oeqSW8v8DaqfLwumquI8=	AWJSGKGXIN	2016-01-26	0.9	9.009	2
10	F.P.N	+PVdeAlmzb1SEXtQ2t8Up/ZR7P2d1Q3JK8TKfOQVaTo=	NSAAVVCWUG	2016-01-26	1	10.01	1
11	M.O.A	DDseh20iFgEpMZ3FkdnOCUWZUTUaG0vOLQGyaURhmUQ=	OGBZAQRAOP	2016-01-26	1.1	11.011	2
12	U.Y.B	cGebChMyG5KCmjfDig9YyUEa+EqkiE6gxSdCa1pXSOs=	UBHBKJMYHU	2016-01-26	1.2	12.012	2
13	B.O.N	VkVp24AMgtEZ2c5C8ULKZrth/PLJJlZpDBiM+XgnoCo=	OFEETVYZIO	2016-01-26	1.3	13.013	2
14	P.O.E	zz14UubhvnBZB5uX224yUAXzttutLLah7MJTLkhI6jU=	PDTNOTOONF	2016-01-26	1.4	14.014	4
15	S.F.Y	VVz18v66QZknzziEqGHxEZB0+wSO22wrLqEXyWYmWV8=	WJLSYZTNFD	2016-01-26	1.5	15.015	5

2 Advanced Index Search

暗号化したインデックスを使って、暗号化カラムに対する索引検索が可能

暗号化されたカラムにインデックスを作り、暗号化した後にもデータの順番をそのまま維持しているため、
全表走査(full table scan)を防ぎ、一致検索および範囲検索ができる(LIKE, BETWEEN, >, <, >=, <= など)

暗号化前

```
SQL> select *
  2  from customer
  3  where card_no = '5787-1313-8201-4786';

Execution Plan
----------------------------------------------------------
Plan hash value: 323025958

-------------------------------------------------------------------------------------------------
| Id  | Operation                    | Name                | Rows  | Bytes | Cost (%CPU)| Time     |
-------------------------------------------------------------------------------------------------
|   0 | SELECT STATEMENT             |                     |     1 |    62 |     2   (0)| 00:00:01 |
|   1 |  TABLE ACCESS BY INDEX ROWID| CUSTOMER            |     1 |    62 |     2   (0)| 00:00:01 |
|*  2 |   INDEX RANGE SCAN           | IX_CARD_NO_CUSTOMER |     1 |       |     1   (0)| 00:00:01 |
-------------------------------------------------------------------------------------------------
```

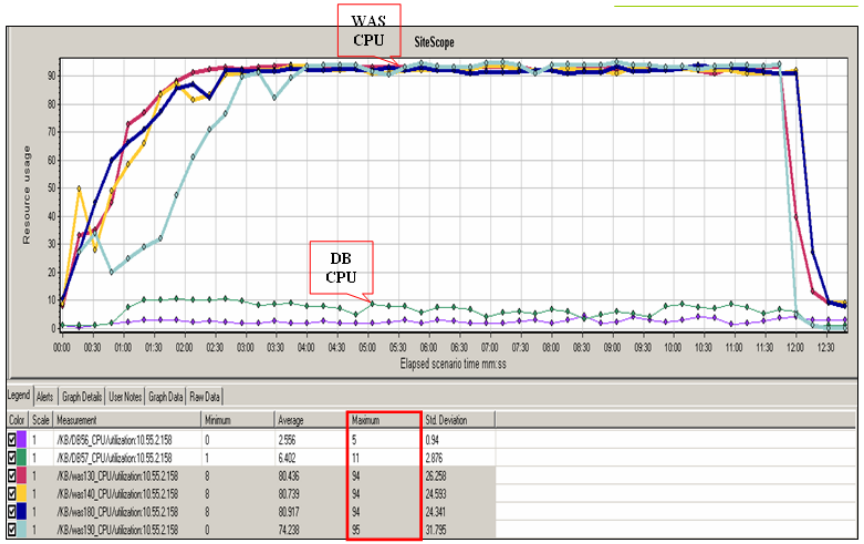
暗号化後

```
SQL> select *
  2  from customer
  3  where card_no = '5787-1313-8201-4786';

Execution Plan
----------------------------------------------------------
Plan hash value: 2860843704

-------------------------------------------------------------------------------------------------
| Id  | Operation                    | Name       | Rows  | Bytes | Cost (%CPU)| Time     |
-------------------------------------------------------------------------------------------------
|   0 | SELECT STATEMENT             |            |    10 |   620 |     5   (0)| 00:00:01 |
|   1 |  TABLE ACCESS BY INDEX ROWID| CUSTOMER#  |    10 |   620 |     5   (0)| 00:00:01 |
|*  2 |   DOMAIN INDEX               | CAR668773  |       |       |            |          |
-------------------------------------------------------------------------------------------------
```

3 高性能

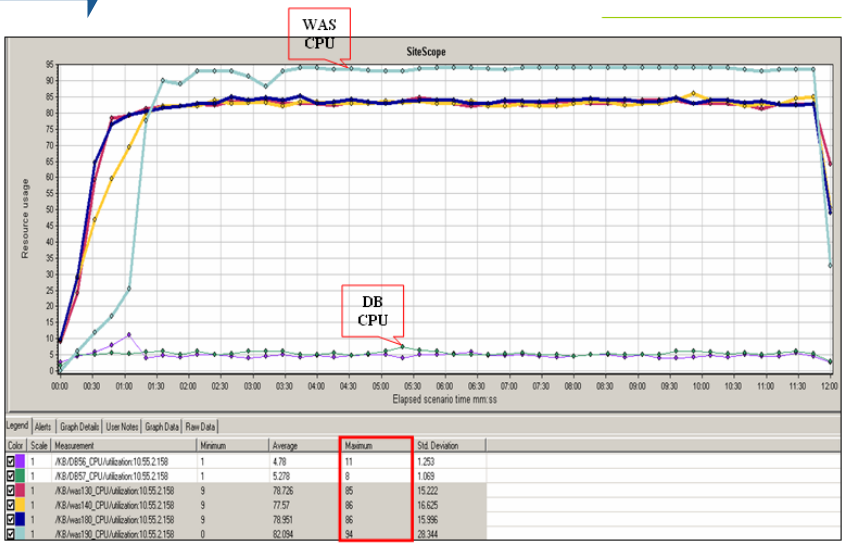
暗号化後にも性能の低下がほとんどない

暗号化前



性能低下がほとんどない
(5%以下)

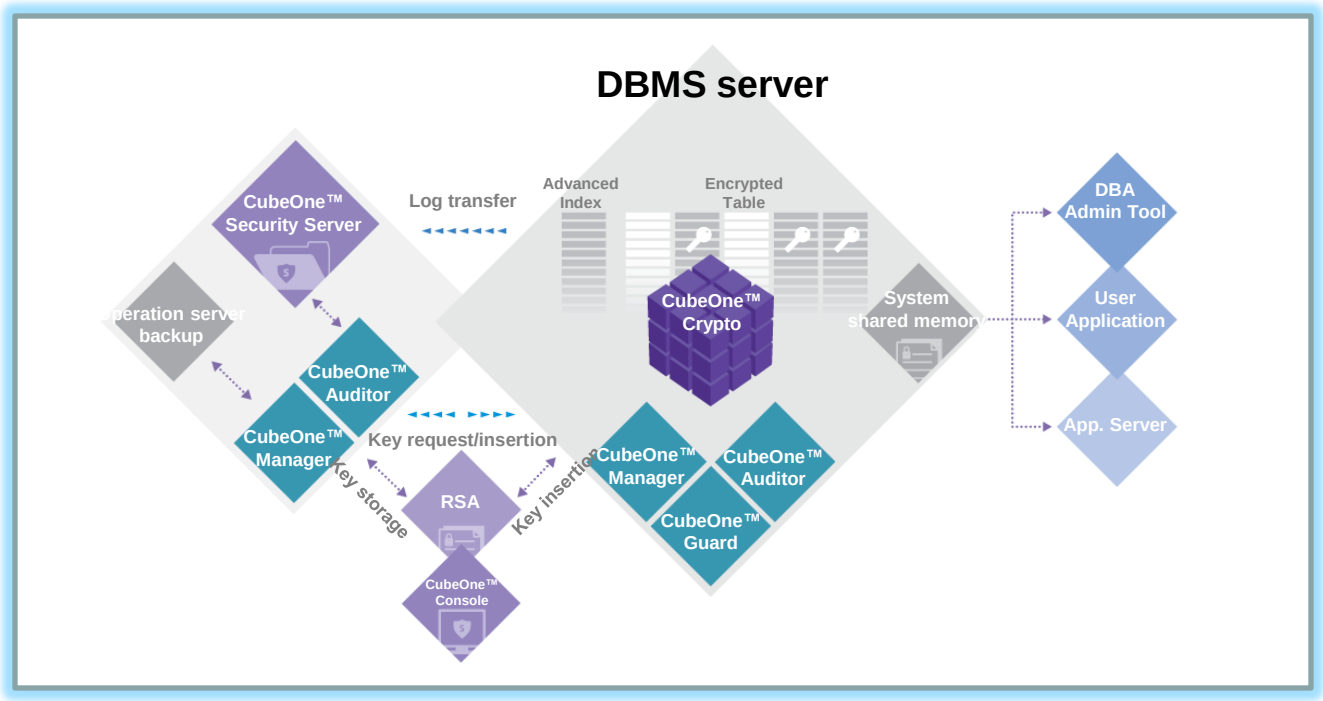
暗号化後



4 安全なキー管理

データとキーが同時に漏洩されない完璧なキー管理

暗号化・複合化キーは、別途のセキュリティサーバーで暗号化され、安全に保存される。またPKCS #11を支援するHSM / KMSに対応する。(SafeNet、Thalesなど)
運用中には暗号化・複合化キーがAPサーバーディスクやDBMSに保存されず、共有メモリーで変換された形で保存される。
サーバーが終了されるとゼロ化する。



5 権限の分離とアクセス制御

セキュリティ・マネージャのみ暗号化されたデータのアクセス制御の権限を持つ

DBAはDB管理業務の権限を持ち、セキュリティ・マネージャーから権限を付与されないと暗号化データにアクセスできない。
アクセスの制限はユーザー(workグループ) 、IP/MACアドレス、application、そしてシステムの名前などで1次管理され、使用期間、使用時間、曜日などで2次管理される。

Authorized User (SCOTT)

```
SQL> show user
USER is "SCOTT"
SQL>
SQL> select cust_no, cust_name, card_no, passwd, reg_date
  2  from demo.customer;

   CUST_NO CUST_NAME CARD_NO             PASSWD      REG_DATE
---------- --------- -------------------- ----------- -----------
         1 G.M.X     1735-9920-9865-5103  WXARDYWWPV  26-JAN-16
         2 Y.H.U     6057-0411-7315-9745  TTGPOVFNUB  26-JAN-16
         3 H.Q.B     3065-8837-1194-9681  OHPDAEEYDB  26-JAN-16
         4 T.T.M     6841-7373-9277-2465  XMVALKDKKN  26-JAN-16
         5 A.O.X     5727-9785-2585-2647  OUWTMYSXOM  26-JAN-16
         6 P.V.O     4835-5441-7045-5351  DPRNEGZVDX  26-JAN-16
         7 T.D.Q     3892-9864-6205-1946  ZIDSOFFYMB  26-JAN-16
         8 W.Y.C     3737-1084-6096-1790  HPKOPGAZXQ  26-JAN-16
         9 B.R.W     2120-7301-0494-9513  AWJSGKGXIN  26-JAN-16
        10 F.P.N     5787-1313-8201-4786  NSAAVVCWUG  26-JAN-16
```

Unauthorized User (SYSTEM)

```
SQL> show user
USER is "SYSTEM"
SQL>
SQL> select cust_no, cust_name, card_no, passwd, reg_date
  2  from demo.customer;

   CUST_NO CUST_NAME CARD_NO     PASSWD      REG_DATE
---------- --------- ----------- ----------- -----------
         1 G.M.X     Encrypted   WXARDYWWPV  26-JAN-16
         2 Y.H.U     Encrypted   TTGPOVFNUB  26-JAN-16
         3 H.Q.B     Encrypted   OHPDAEEYDB  26-JAN-16
         4 T.T.M     Encrypted   XMVALKDKKN  26-JAN-16
         5 A.O.X     Encrypted   OUWTMYSXOM  26-JAN-16
         6 P.V.O     Encrypted   DPRNEGZVDX  26-JAN-16
         7 T.D.Q     Encrypted   ZIDSOFFYMB  26-JAN-16
         8 W.Y.C     Encrypted   HPKOPGAZXQ  26-JAN-16
         9 B.R.W     Encrypted   AWJSGKGXIN  26-JAN-16
        10 F.P.N     Encrypted   NSAAVVCWUG  26-JAN-16
```

ありがとうございました。

蔡康錫(チェ･ガンソク)
副社長/海外事業部門

ks.chai@eglobalsys.co.kr
www.eglobalsys.co.kr