
# Postgresを活用した安心・安全なデータ保護とは – EPAS15の新機能 –

**Katsuji Takatsuru** | PS Manager in Japan
**Ryo Murakawa** | SE Manager in Japan & Korea

2023/3/15

# アジェンダ

- EPAS15でのアップデート内容
- セキュリティ項目
  - Transparent Data Encryption(TDE)のご紹介
  - LDAPパスワードの難読化
- お客様向けのご連絡
  - 情報ページ

# EPAS14->EPAS15への機能強化項目（今回のテーマ）

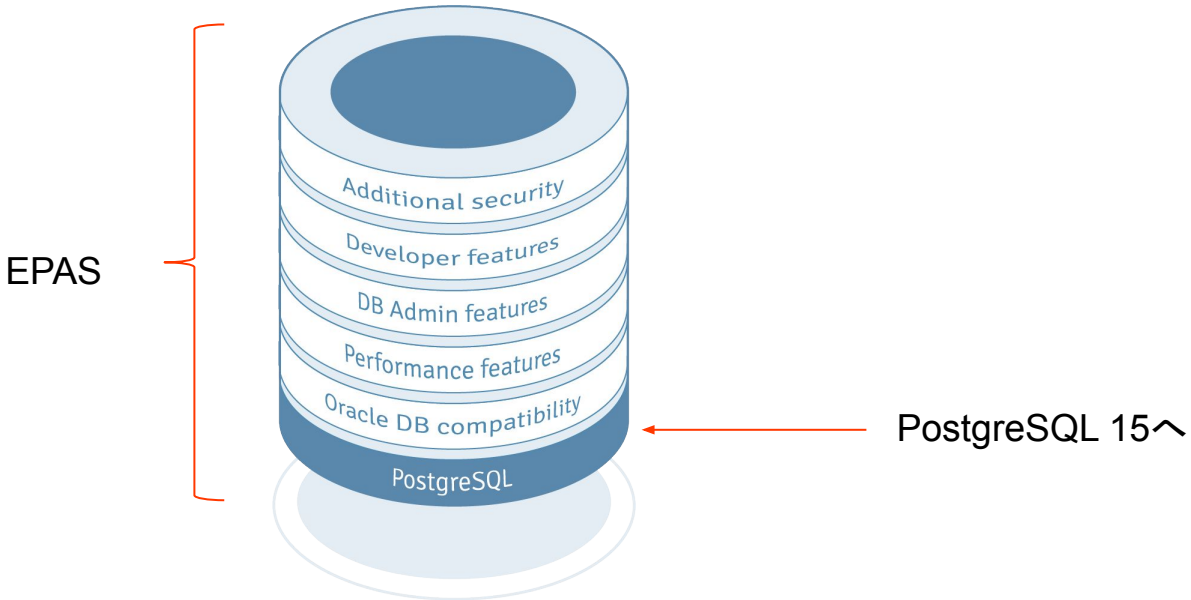
- PostgreSQL 15への対応
- 透過的なデータ暗号化(TDE)対応
- LDAPバインドパスワード難読化
  - pg_hba.confのパスワード難読化
- 非スーパーユーザがedb＊loaderを使用してデータロード可能
- SQL
  - MERGE構文
  - UPDATE ..SET ROW構文サポート
- パッケージ
  - HTP
  - HTF
  - DBMS_UTILITY(機能強化)

# EPAS15のExtension（次回のテーマ）

- 運用の改善
  - Failover slot – 論理デコードクライアントが物理レプリカのFail Over/Switch Overに従うことを許可
- Storage Extension
  - 参照データ – 正規化されたデータモデルと外部キールックアップのスケーラビリティの向上
  - 自動クラスタ、クラスタ化されたデータへの高速アクセス

# PostgreSQL 15の対応

- 2022/10/13にPostgreSQL 15がリリース
- EPAS15においても、PostgreSQL 15の拡張機能全て対応

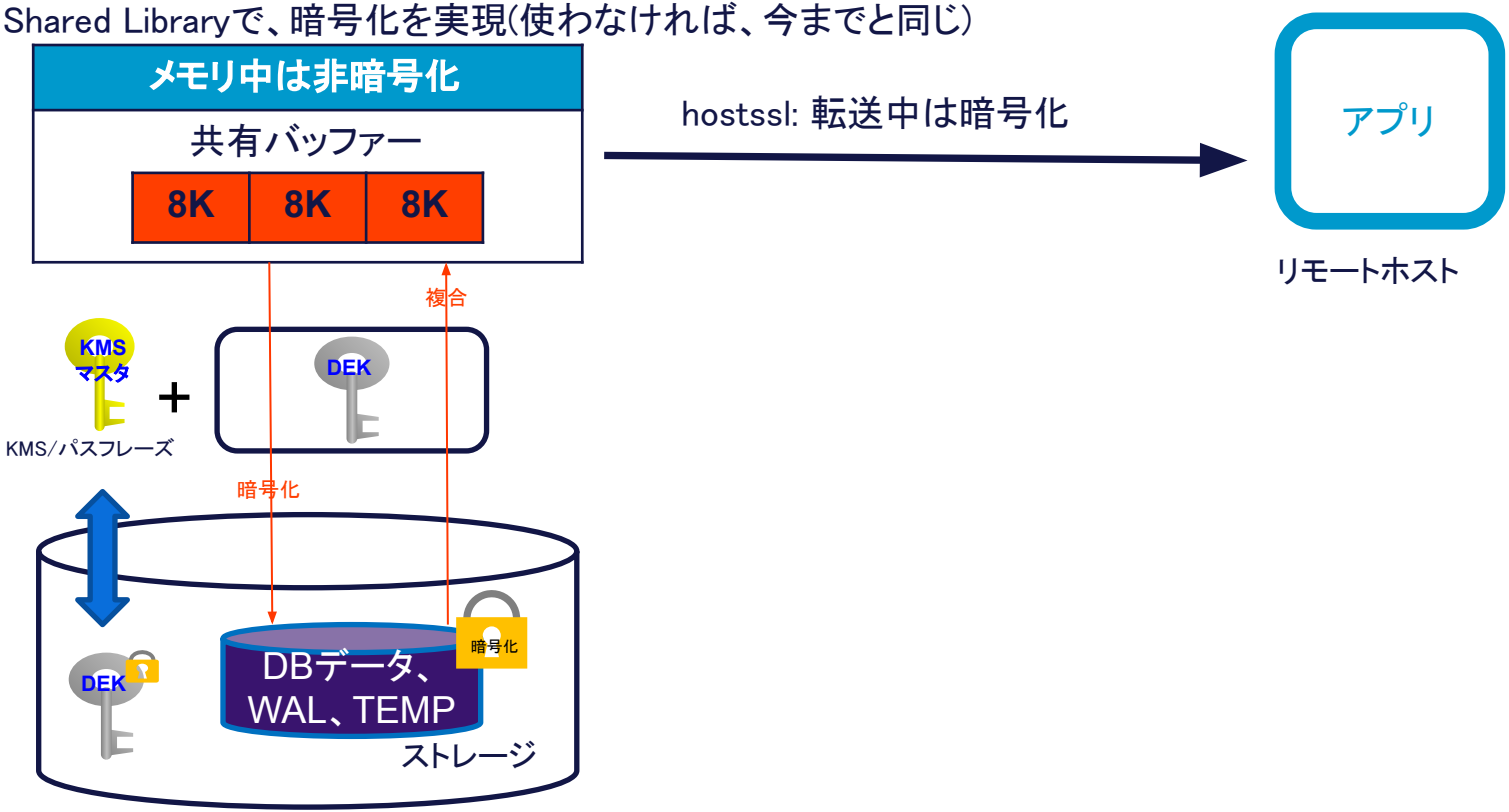


# 今までのPostgreSQLのDBの暗号化

- Filesystemに付随する機能を用いて、ディレクトリの暗号化
  - LVM暗号化、Windowsの暗号化機能を利用して。。
  - 課題
    - システムが起動すれば誰でも内容にアクセスできる
      - システム稼働中であればデータは平文
- アプリケーションからデータの書き込みの際に暗号化
  - 課題
    - 余分なコストが必要となる
    - アプリケーションの作りが複雑になる

# TDEのフロー

- TDEのフローとしては、以下のようなシンプルな形
  - Shared Libraryで、暗号化を実現(使わなければ、今までと同じ)



# TDEの構築は、オプションのみ！

- 設定するオプション
  - export PGDATAKEYWRAPCMD='openssl enc -e -aes-128-cbc -pass pass:ok -out %p'
  - export PGDATAKEYUNWRAPCMD='openssl enc -d -aes-128-cbc -pass pass:ok -in %p’
- 暗号化させるコマンド
  - /usr/edb/as15/bin/initdb --data-encryption -D /var/lib/edb/as15/data

# EPAS14->EPAS15+TDEは？

<新規で作る場合と一緒>

- 設定するオプション
  - export PGDATAKEYWRAPCMD='openssl enc -e -aes-128-cbc -pass pass:ok -out %p'
  - export PGDATAKEYUNWRAPCMD='openssl enc -d -aes-128-cbc -pass pass:ok -in %p'
- 暗号化させるコマンド
  - /usr/edb/as15/bin/initdb --data-encryption -D /var/lib/edb/as15/data
- pg_upgradeコマンドで
  - /usr/edb/as15/bin/pg_upgrade -d /var/lib/edb/as14/data -D /var/lib/edb/as15/data/ -b /usr/edb/as14/bin -B /usr/edb/as15/bin -p 5444 -P 5444 --copy-by-block

# TDEの注意点？

- キー管理をどうするか？
  - opensslは、テスト用途として用意されているという理解でいてほしい
  - ドキュメントに記載されているKey Storeとして
    - Amazon AWS Key Management Service
    - Google Cloud – Cloud Key Management Service
    - Microsoft Azure Key Vault
    - Thales CipherTrust Manager

# TDEをする前

```
edb=# \c hr;
psql (14.7.0、サーバー 14.7.0)
データベース"hr"にユーザー"enterprisedb"として接続しました。
hr=# \dt
             リレーション一覧
 スキーマ | 名前 |  タイプ  |    所有者
----------+------+----------+--------------
 public   | dept | テーブル | enterprisedb
(1 行)

hr=# select * from dept;
 deptno |   dname    |   loc
--------+------------+----------
     10 | ACCOUNTING | NEW YORK
     20 | RESEARCH   | DALLAS
(2 行)

hr=# select pg_relation_filepath('dept');
 pg_relation_filepath
----------------------
 base/16384/16385
(1 行)

hr#
```

```
[enterprisedb@tde-test 16384]$ hexdump -C 16385
00000000  00 00 00 00 70 44 73 02  00 00 00 00 20 00 98 1f  |....pDs..... ...|
00000010  00 20 04 20 00 00 00 00  c8 9f 62 00 98 9f 5a 00  |. . ......b...Z.|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001f90  00 00 00 00 00 00 00 00  e6 05 00 00 00 00 00 00  |................|
00001fa0  00 00 00 00 00 00 00 00  02 00 03 00 02 09 18 00  |................|
00001fb0  0b 00 80 14 00 13 52 45  53 45 41 52 43 48 0f 44  |......RESEARCH.D|
00001fc0  41 4c 4c 41 53 00 00 00  e5 05 00 00 00 00 00 00  |ALLAS...........|
00001fd0  00 00 00 00 00 00 00 00  01 00 03 00 02 09 18 00  |................|
00001fe0  0b 00 80 0a 00 17 41 43  43 4f 55 4e 54 49 4e 47  |......ACCOUNTING|
00001ff0  13 4e 45 57 20 59 4f 52  4b 00 00 00 00 00 00 00  |.NEW YORK.......|
00002000
[enterprisedb@tde-test 16384]$
```

# TDEをした後

```
edb=# \c hr;
psql (15.2.0、サーバー 15.2.0)
データベース"hr"にユーザー"enterprisedb"として接続しました。
hr=# \dt
              リレーション一覧
 スキーマ | 名前 |  タイプ  |    所有者
----------+------+----------+--------------
 public   | dept | テーブル | enterprisedb
(1 行)

hr=# select * from dept;
 deptno |   dname    |   loc
--------+------------+----------
     10 | ACCOUNTING | NEW YORK
     20 | RESEARCH   | DALLAS
(2 行)

hr=# select pg_relation_filepath('dept');
 pg_relation_filepath
----------------------
 base/16384/16385
(1 行)

hr=#
```

```
[enterprisedb@tde-test 16384]$ hexdump -C 16385
00000000  92 fd 63 48 8e c7 28 0e  e8 7e 03 ff c2 d0 ab d3  |..cH..(..~......|
00000010  31 8a e8 6f cd 19 76 dd  ef 0e b8 2f 38 8c 4f 59  |1..o..v..../8.OY|
00000020  41 c7 8b b8 72 18 04 c8  35 9a 89 59 fb 91 bf d0  |A...r...5..Y....|
00000030  5b fc 31 79 48 e3 5f ee  f8 06 c9 58 dd 61 77 e1  |[.1yH._....X.aw.|
00000040  aa 3f d6 5e 46 b1 2c bb  9c 98 2a 56 5d 2e 1c c6  |.?.^F.,...*V]...|
00000050  6e 85 bf db 6c 1b 50 f9  aa 8f 6b bd 47 66 ab 95  |n...l.P...k.Gf..|
00000060  a8 bf 97 40 d1 3d 04 74  07 b0 09 25 40 41 bc a9  |...@.=.t...%@A..|
00000070  cf ba 5b 03 dd e9 2d ec  3c b6 e6 65 22 b6 a0 a5  |..[...-.<..e"...|
00000080  9e 31 e3 c3 ad e6 6e d1  46 67 36 10 e1 8d 0a 82  |.1....n.Fg6.....|
00000090  a8 b0 24 3a 72 d3 e7 9b  01 ed 93 53 0d d6 56 99  |..$:r......S..V.|
000000a0  06 4e c8 b6 80 be 58 4b  ef db 53 88 ef 59 5b 71  |.N....XK..S..Y[q|
000000b0  be ca 27 aa 76 b0 36 2c  6c 09 ab 6c ec 59 96 83  |..'.v.6,l..l.Y..|
000000c0  39 2a 77 2b 8f c9 f2 d4  dd 24 d1 08 e0 70 0e eb  |9*w+.....$...p..|
000000d0  fc b1 8f 5d 62 52 45 2b  72 d3 81 8b 3b 67 70 db  |...]bRE+r...;gp.|
000000e0  41 35 98 7e 29 58 26 23  30 e0 a4 15 be 90 f5 41  |A5.~)X&#0......A|
000000f0  00 e4 72 ae 0f 83 d3 94  aa 2b 19 ac 24 36 96 17  |..r......+..$6..|
00000100  eb 71 24 7f 0d d7 15 67  e6 02 fc 45 16 b7 d5 40  |.q$....g...E...@|
00000110  98 37 80 48 73 2d ac bd  b0 8f 5d 30 bc d0 18 b2  |.7.Hs-....]0....|
00000120  53 18 e6 37 6f 52 39 fe  91 96 dd 9b 8e 87 1a ec  |S..7oR9.........|
00000130  65 6b f2 db d8 a5 36 96  e4 ca c9 8b de 7a 03 9e  |ek....6......z..|
00000140  fa e9 e3 b3 de f3 01 d3  85 07 24 5c 46 7b c3 f0  |..........$\F{..|
00000150  39 32 87 52 b6 ff e4 fa  0c a3 3e b0 b0 3f 89 8d  |92.R......>..?..|
00000160  83 53 9c 60 96 65 be e7  7f 74 c8 5e d9 a4 8d 44  |.S.`.e...t.^...D|
00000170  80 4a b6 c1 e4 02 c2 8c  8e c4 b6 5d 82 6f ce 3c  |.J.........].o.<|
00000180  79 90 9a cf 7e b9 c9 5c  4e 1c d7 61 fc 5c 10 d9  |y...~..\N..a.\..|
00000190  20 3c a2 25 11 d5 12 6a  05 c9 b8 f9 7a fb e7 51  | <.%...j....z..Q|
000001a0  c7 9f d2 e0 0f b9 30 52  5f 9e 37 38 da 0c 2d 99  |......0R_.78..-.|
000001b0  a0 bb e2 8d 96 19 8f a0  be d7 f0 41 8c 36 68 21  |...........A.6h!|
000001c0  25 eb 2a 0e 49 9b 47 ec  f6 82 43 5e 20 2f f7 54  |%.*.I.G...C^ /.T|
000001d0  69 ad 8d 39 2f 99 f3 6d  94 53 45 8a e4 1a 40 26  |i..9/..m.SE...@&|
000001e0  29 ac 17 72 1a 38 58 cd  41 fc 30 52 cb a0 99 70  |)..r.8X.A.0R...p|
000001f0  63 e4 a8 52 ca ca 4c dd  1f e2 2c f9 24 c2 73 5c  |c..R..L...,.$.s\|
00000200  85 b2 a1 2f 32 6f 31 1a  e6 d4 fd d0 9b 54 00 44  |.../2o1......T.D|
00000210  ff 38 0f b2 92 b3 7d 47  97 1c c6 0e f9 2d 31 15  |.8....}G.....-1.|
00000220  54 09 c6 fb 8d ab fd a8  de 4d 05 5d 2b 4f be da  |T........M.]+O..|
00000230  ef 93 9c 44 9d 69 59 2b  5a d9 3f 19 59 f1 e3 eb  |...D.iY+Z.?.Y...|
```

# LDAP利用の流れ

- PostgreSQLでの外部からのアクセスでRoleのLDAP認証を利用ができるようになっている。
  - LDAPの接続情報は、ファイルにアクセスできれば可能
  - PostgreSQLユーザのパスワードは、DB側に書き込まれている
    - DB側に書き込んでいるパスワードは都度変更される可能性は低い

LDAPを利用したユーザ管理の使用が進んできている

# LDAPバインドパスワードの難読化

- クライアントからLDAP認証を行う際のパスワードを難読に！

pg_hba.conf(TDEを利用しても暗号化されません )

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     trust
# IPv4 local connections:
host    all             all             0.0.0.0/0               ldap ldapserver=192.168.0.43 ldapbasedn="cn=Users,dc=suselab,dc=de" ldapbinddn="CN=bind,CN=Users,dc=s
uselab,dc=de" ldapbindpasswd="p@ssw0rd123" ldapsearchattribute="sAMAccountName"
```

```
barman@epas14-barman:~$ psql -h 192.168.0.75 -U enterprisedb edb
Password for user enterprisedb:
psql.bin (15.2.0 (Ubuntu 15.2.0-1.bionic), server 15.2.0)
Type "help" for help.

edb=#
```

ここに平文でパスワード設定することなく、hookする関数で置き換えることができるようになる

# LDAPバインドパスワードの難読化

- Hook関数に関しては、以下のサイトを参照してください

https://www.postgresql.org/message-id/attachment/142991/0001-Add-a-password-handling-hook-for-ldapbindpasswd-v2.patch

# 日本のお客様向け情報ページとお問合せ

**◆各種お問合せ**
右記QRコードのお問い合わせフォームからお願いします。
ジャパンブログのお問い合わせタブにも掲載してあります。

**◆EDBジャパンブログ: edbjapan.com**
エンタープライズDBでは日本のお客様向けに翻訳マニュアルや各種セミナー情報をジャパン・ブログにてご紹介しています。是非活用ください


EDB

# まとめ

- EPAS15の新機能
  - TDEがもたらすデータ保護
  - Ldap連携における難読化の仕組み
- 国内のお客様向け情報について

# Q&A

- TDEのKey Managementとして、KMIPを利用することができるか？
  - 使えます。
- Windows環境のおいてもEPAS15のTDE機能は使えるか?
  - 使えます
- TDEを利用した場合のパフォーマンス劣化はどのぐらいなのか？
  - EDB側で検証した結果、10%前後となっています。
- TDEで暗号化した場合、ファイルサイズが増えるのではないか？
  - ファイルサイズは増えますが、容量が2倍になるということではありません。　　どれ程増えるのかは、データに依存します。


# Thank you