



新ワーキンググループ 【DB暗号化WG】ご紹介

DB暗号化WGリーダー
サイファーゲート株式会社
彦田 雅之
hikota@ciphergate.co.jp

DB暗号化WGのねらいと活動内容 - その1

【 DB暗号化が必要とされる外的要因・内的要因を分析・考察 】

WGが発足した時代背景を考える

- セキュリティに関する様々なガイドラインにてDB暗号化の必要性が求められ、企業側は実装を強く求められ始めている。
 - 米国カリフォルニア州法 SB1386
 - 厚生労働省 医療情報システムの安全管理に関するガイドライン
 - 内閣官房情報セキュリティセンター 政府機関の情報セキュリティ対策のための統一基準
 - 金融情報システムセンター (FISC)
 - コンピュータシステムの安全対策基準・解説書 第7版
 - 金融庁 保険検査マニュアル 顧客保護等管理態勢の確認検査用チェックリスト
 - PCIDSS (Payment Card Industry Data Security Standard)
 - 金融庁 金融検査マニュアル 顧客保護等管理態勢の確認検査用チェックリスト
 - 農林水産省 共済事業検査マニュアル 利用者情報管理態勢の確認検査用チェックリスト
 - 経済産業省 個人情報保護に関する法律についての経済産業分野を対象とするガイドライン
 - 総務省公開 ASP・SaaSにおける情報セキュリティ対策ガイドライン(案)
- DBから直接情報漏洩が起こった場合は対象となる件数が膨大となる。



DB暗号化に関するエンドユーザーの悩み

- 暗号化対象となるDBは膨大で多岐に渡るが、どこから手をつけて、どこまでやればいいのか？
- DBのパフォーマンスへの影響は大丈夫なのだろうか？
- バッチ系システムの処理は問題無いのだろうか？
- データ移行のチャンスは年1回しかないが、上手くいくだろうか？
- 既存システムのDBを暗号化するに際して、アプリケーションの修正は必要なのだろうか？
- 実際にDBを暗号化した場合に、具体的にどういった情報漏洩の可能性をなくすことができるのだろうか？

などなど

DB暗号化WGのねらいと活動内容 - その2

【 DB暗号化を実施・運用する際の技術的ポイントを整理 】

DB暗号化に関する実践的ノウハウを普及させる

- データベース暗号化の定義と歴史
- データベース暗号化を実施する際の留意点
 - 暗号化設計
 - データベースサーバーのパフォーマンスへの考慮
 - 既存のデータベースを暗号化する際のデータ移行
 - 鍵の管理
 - 運用設計
- データベース暗号化手法比較
 - 客観的視点でメリットと課題を比較
- 現状の課題の洗い出しと今後の方向性