緊急提言及びパブコメ提出に関する活動報告と新年度計画

DBSC
DataBase Security Consortium

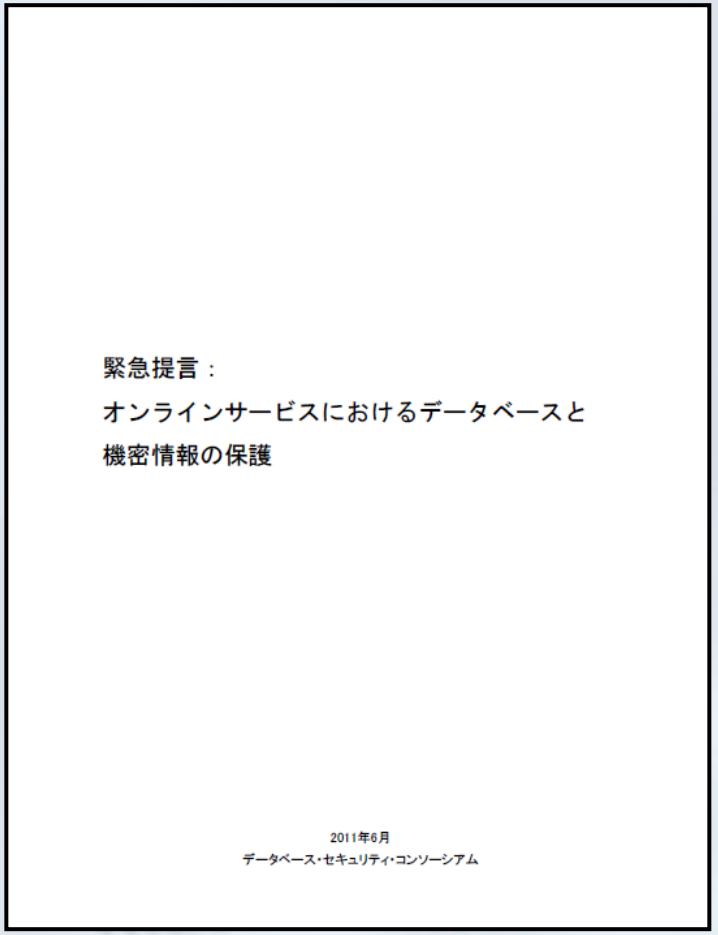
Agenda

- 緊急提言書について
- パブコメ提出について
- 新年度計画について

緊急提言：オンラインサービスにおけるデータベースと機密情報の保護

- 境界防御を中心として考えられてきたインターネット上のセキュリティ対策であるが、攻撃者がそれらを突破し、情報を格納しているデータベースそのものを攻撃することがあるという事実が、今我々の眼前に突きつけられている。
- 境界防御を乗り越えてくる攻撃者の存在を想定し、さらに進化した多層防御の仕組みを構築しなければならない。
- 最近の事件、事故の動向を踏まえた上で、改めてデータベースに対する管理策はどうするべきかを見直すための提言を行うこととした。

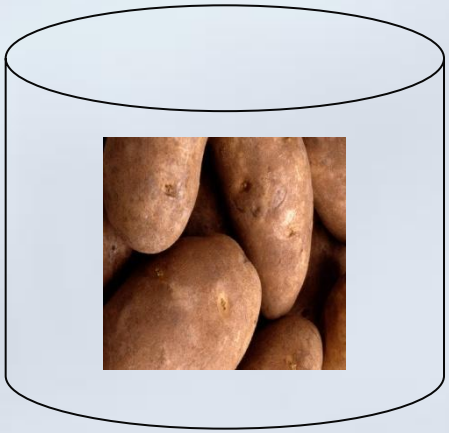
情報の活用と保護がバランスよく実現され、インターネットを通じたビジネスと経済活動の健全な発展を願っています。


緊急提言：
オンラインサービスにおけるデータベースと
機密情報の保護

2011年6月
データベース・セキュリティ・コンソーシアム

大前提

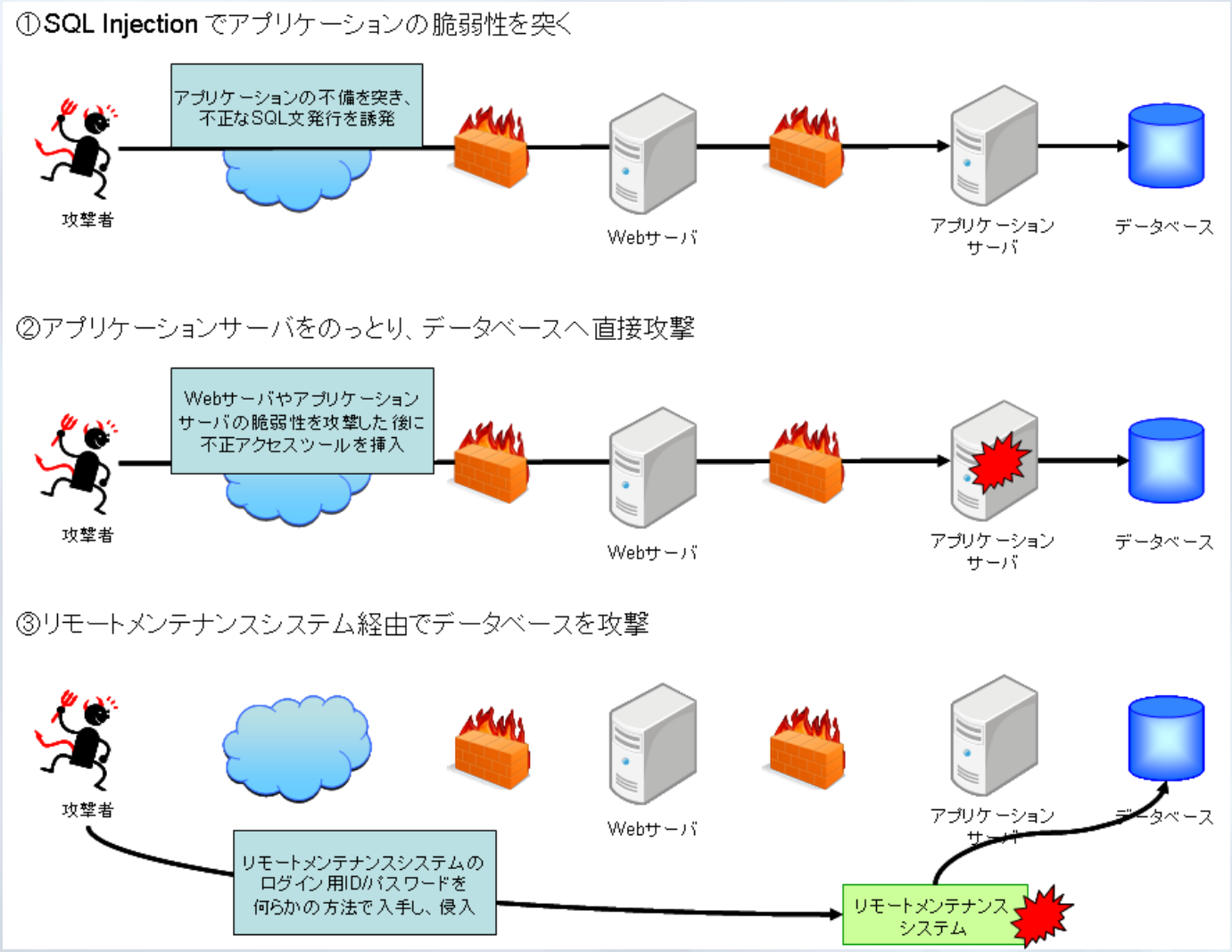
- 重要なデータ(情報)がデータベースに含まれる前提
- 以下は極端な例



じゃがいも in データベース

ダイヤ in データベース

2.1 想定される攻撃シナリオ



2.2 最近の動向を踏まえて認識すべきこと

- 攻撃に至るまでのプロセスや技術は複雑化・簡易化
  - 辞書アタックでの成りすましは当然、暗号化通信経由での攻撃も
  - 攻撃コード難読化／多様化⇒防御ツール側とのいたちごっこが発生
  - 攻撃ツールが容易に入手可能⇒誰でもスーパーハッカーに

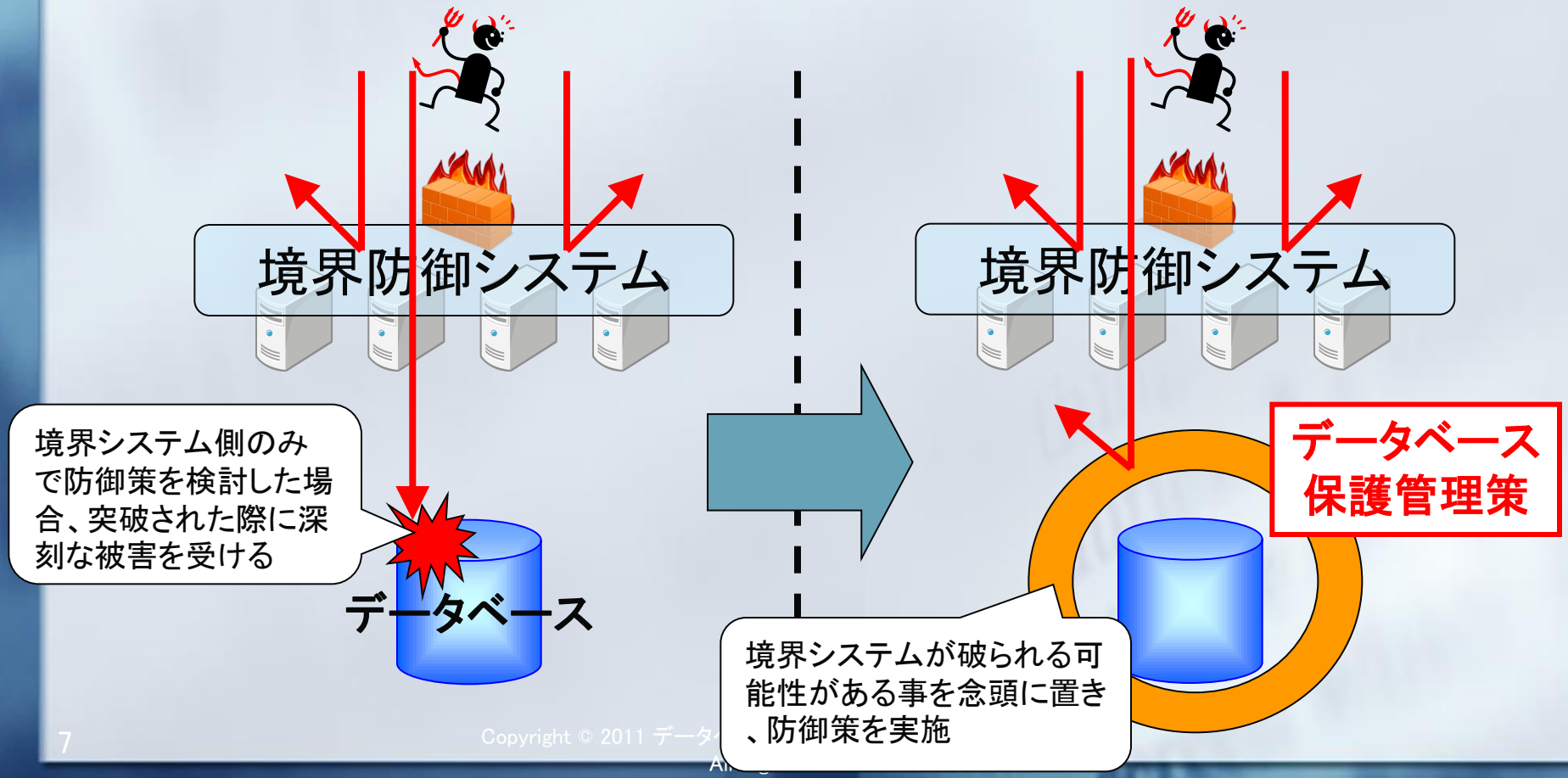
※詳細についてはセキュリティ専門企業や独立行政法人情報処理推進機構（IPA）による解説を参照下さい。

- 境界システム中心での防御の限界
  - 念のため：境界システム（Webサーバ、App サーバ）の防御も重要
  - 考える事：境界防御システムの防御機能が万全でない状態が発生する

- データ量の増加傾向
  - 事業が成長期に突入すると、サービス増強、追加が頻繁に
  - 気づいた時にはDBMSが機密データの宝庫になっている可能性も

技術的に考えるべきこと

- 境界システムでの防御策は攻撃を軽減する仕組みの一つ
- 格納庫（データベース）への安全対策も含めた多層防御へ



3.1 不正アクセス検知の導入

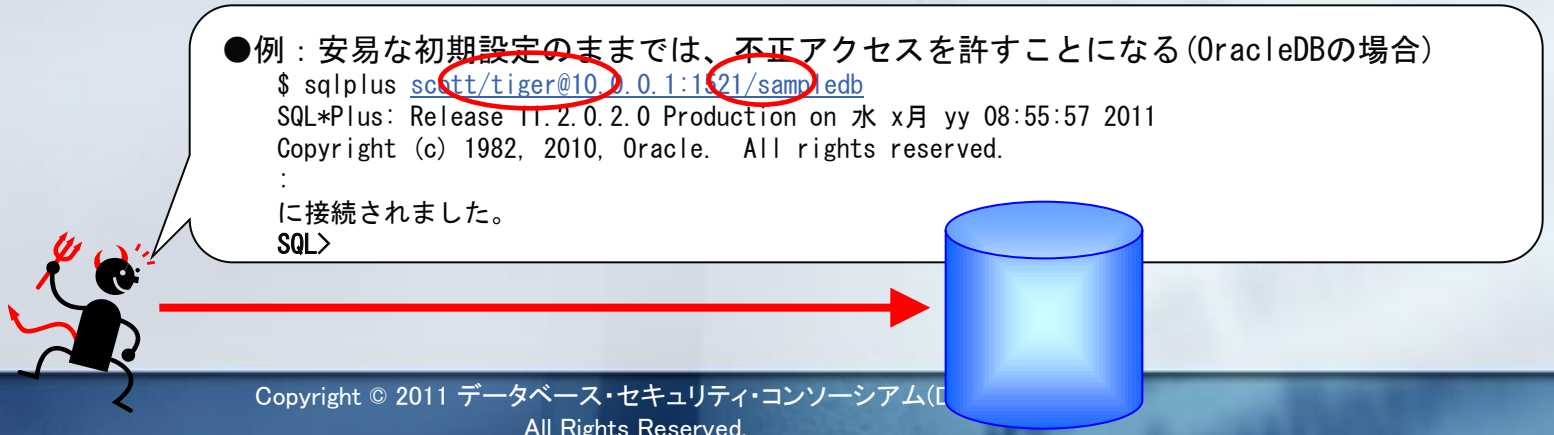
- データベースアクセスに特化した不正を検知する機構
  - データベースアクセスに特化した場合、境界システム上でのそれと比較した際に攻撃の特定が容易
    - 監視対象や必要スキルセットの単純化⇒必要スキル軽減
    - セキュリティルールの数が短くなる⇒運用負荷軽減

·監視対象はSQL Injection以外に多数存在
·攻撃コード対応の増加でルール数増加

·基本はデータベースに対するSQLに特化して監視ルールを設計

3.2 脆弱性管理の見直し

- 境界システムに対しては実施している要綱が多いと思いますが、データベースに対しても見直しを
  - 脆弱性パッチは（出来る限り）早急に適用
  - 通信ポート、接続元IPアドレスの制限
  - 必要な（最小限の）ソフトウェアモジュールのみを導入
  - 初期設定情報の排除（例：アカウント、サンプルテンプレート）
  - 不要なアカウントの排除（メンテナンス用途で作成したアカウントなど）
  - パスワードポリシ見直し（推測しにくいパスワード、定期的な変更）
  - データベース製造各社のセキュリティガイドも参照に
  - システム構築時だけでなく、継続的な対応を

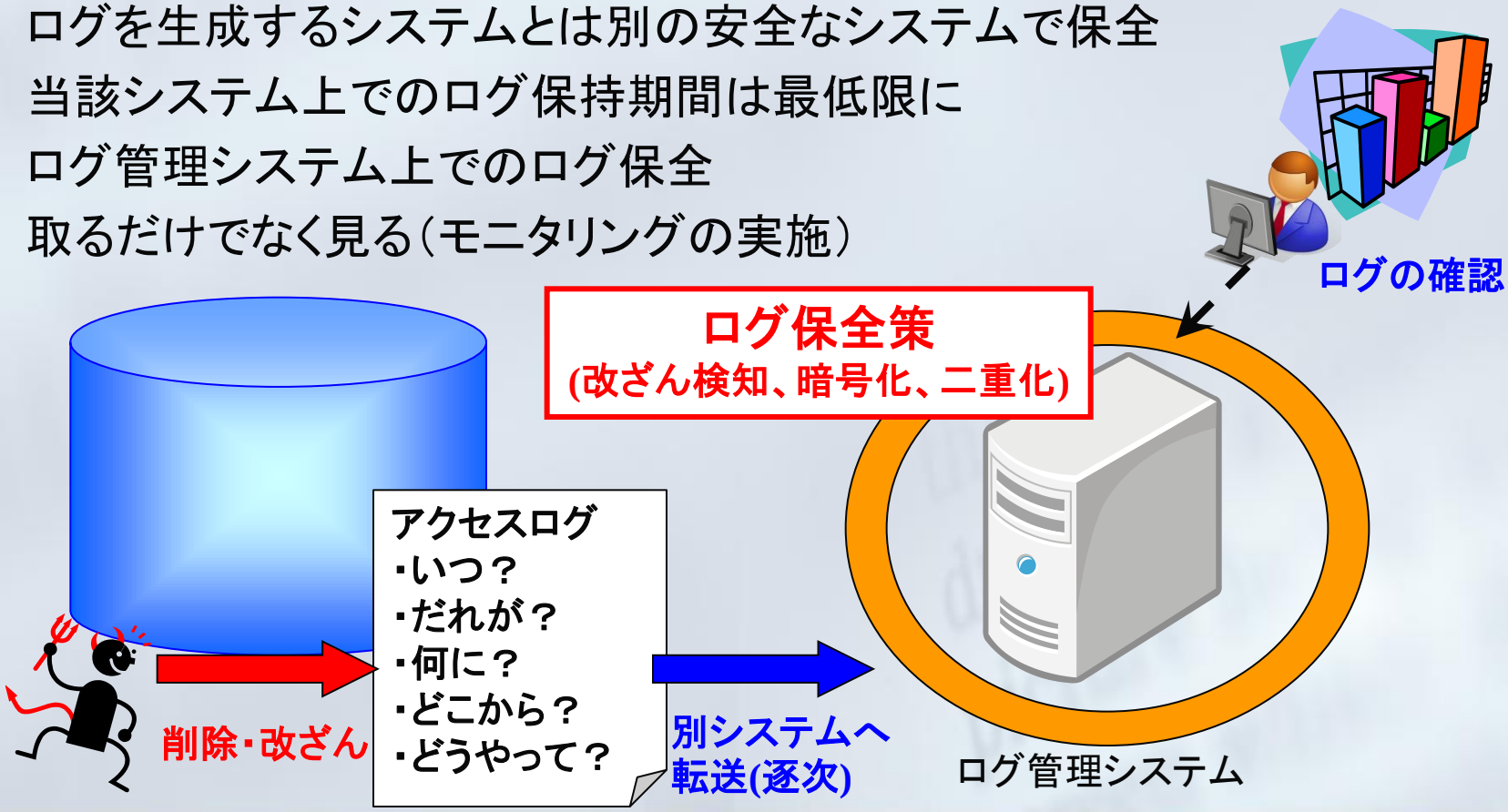


3.3 OSにまで攻撃の手が及んだ場合の対応

- OSレベルでの侵入=> DB関連ファイルの奪取
  - 暗号化(OSの権限からみて透過的だと無意味な可能性)
- データベースレベルでの侵入=>DBMS 内データ奪取
  - アプリケーションの接続情報から侵入される場合もある(OS権限を奪取しなくても侵入できる可能性)
  - 権限最小化
    - DBMS管理(システム管理)とデータアクセスの分離
    - アプリケーション用ユーザと情報を格納するオブジェクトの分離
    - 権限に応じた最小レベルのアクセス許可
  - アクセス最小化
    - 接続可能な時間帯、接続元IPアドレス・ホスト等の絞込み
  - 暗号化

3.4 ログの保全管理見直し

- 攻撃者特性：犯罪行為の足跡（ログ）を消す
- ログ保全管理見直し
  - ログを生成するシステムとは別の安全なシステムで保全
  - 当該システム上でのログ保持期間は最低限に
  - ログ管理システム上でのログ保全
  - 取るだけでなく見る（モニタリングの実施）



3.4 ログの保全管理見直し

- 攻撃者特性：犯罪行為の足跡（ログ）を消す
  - 削除するログ（例）：
    - ログイン履歴、盗難した情報へのアクセス履歴
- （ログ取得は実施の前提で）ログ保全管理見直し
  - ログを生成するシステムとは別の安全なシステムで保全
    - DBMSとは別システムへ分離、別ネットワークへ設置、要塞化など
  - 当該システム上でのログ保持期間は最低限に
    - 逐次ログ管理サーバへ転送
  - ログ管理システム上でのログ保全
    - 例：改ざん検知、暗号化、データ二重化
  - 取るだけでなく、見る事も忘れずに

3.5 機密データの最小化

- 原理原則:「余分な機密データは持たない」
  - 本番環境にのみ存在する事があるべき姿
- こんなこと、ありませんか？
  - 開発者向け環境とかテスター向け環境での本番データ利用
  - 本番環境／テスト環境の混在
  - 新旧システム入替え時に、アプリケーションは入替えを行ったが、データベース領域はそのまま残存／休止状態
- データマスキング、トークナイゼーションの検討

DBSC緊急提言プロジェクト（社名50音順）

リーダ	日本オラクル株式会社	北野 晴人
サブリーダ	伊藤忠テクノソリューションズ株式会社	伊藤 英二
	株式会社アクアシステムズ	安澤 弘子
	伊藤忠テクノソリューションズ株式会社	加藤 昇平
	株式会社インサイトテクノロジー	岸本 拓也
	タレスジャパン株式会社	上野 隆幸
	富士通株式会社	平野 秀幸
	株式会社富士通九州システムズ	片山 裕昭
	株式会社ラック	西本 逸郎
事務局	株式会社ラック	小林 香織
		須田 堅一

パブコメ提出に関する活動報告　①

- 「情報セキュリティ2011」（内閣官房情報セキュリティセンター）
  - 2011年6月21日付けでパブコメ提出
  - 内容は提言書を添付
- 「政府機関の情報セキュリティ対策のための統一基準群」平成24年度版（案）　（内閣官房情報セキュリティセンター）
  - 2012年4月2日付けでパブコメ提出
  - 「リレーショナル・データベース」の項目追加を要望
  - 導入・構築時および運用時のための遵守事項の案を作成
  - 『データベースセキュリティガイドライン 第2.0版』を推奨

パブコメ提出に関する活動報告　②

- 大規模な漏えい事件にRDBMSが関連していることを指摘

政府機関の情報セキュリティ対策のための統一管理基準」で定める要件を実現するためには、要機密情報を格納するための直接的な要素技術であるリレーショナル・データベース（RDBMS：以下同じ）をはじめとするデータベースシステムの項目を明示的に追加すべきである。

過去、国内外における機密情報に関する大規模な漏えい事件においては、その多くで当該機密情報がRDBMS内部に格納されていたことは明らかであり、個人情報等の構造化された大量の機密情報は、今後も引き続きRDBMS内で保管・管理されると考えられる。

RDBMSにおけるセキュリティ要件の多くはOS、ネットワーク、業務アプリケーションといった他のシステム構成要素と変わるところはなく、基本的には本ドキュメントの2.2.1.1～2.2.1.6に記載されている対策要素を適切に組み込むことで実現が可能である。
しかし一方でRDBMSに特徴的な留意事項も存在することや、従来OSやネットワーク上での対策に重きがおかれ、その重要性があまり考慮されないことが多く、結果として多くの重大な事故を防止できなかったことを鑑み、遵守事項を明示することが重要であると考える。これによって、今後の政府機関の情報システムの安全性に寄与することができると考えられる。

今後も根気よくアピールを続けます

新年度の計画について

- データベース、とデータベース管理者についてアンケート調査を行いたい。
  - データベースにどれくらいセキュリティ対策が実施されているか？
    - 他社のことはよくわからない。自社は比較するとどうなのだろうか？
    - セキュリティ対策全体で聞くと他の対策が見えてきて、データベースの対策が見えないことが多い。
  - データベース管理者・開発者は幸せだろうか？
    - 何でもできる権限を持っていることが多い
    - 今は管理者のモラルだけで情報が守られている？
    - 勤務時間は？待遇は？お給料は？上司は？
    - 管理者が不幸だと、内部不正の温床を作るのではないか？
  - 実態を分析し、データベースのセキュリティ状態を可視化したい。