

サイバー攻撃からDBを守る



RITSUMEIKAN

立命館大学
情報理工学部

上原哲太郎

脅威は増しこそすれ減ることはない

ITによる
業務の
効率化を

マイナンバー！
特定個人情報！

ビッグデータは
個人情報の塊

顧客情報は
宝の山だが
爆弾でもある



Under
Pressure!

なぜDBが狙われるのか

- 情報化社会とは「情報がカネになる」社会
人力を要する「泥臭い」攻撃でも
十分にペイする時代に
- DBは攻撃者にとって都合がよい標的
 - 情報が整理され集約されている場所
「ワンストップ・ソリューション」
 - 内部攻撃者にとっても外部攻撃者にとっても...



情報が金になるからこそ…

- 2014年7月 通信教育事業者個人情報漏洩
 - DB管理権限を持つ者からの内部漏洩

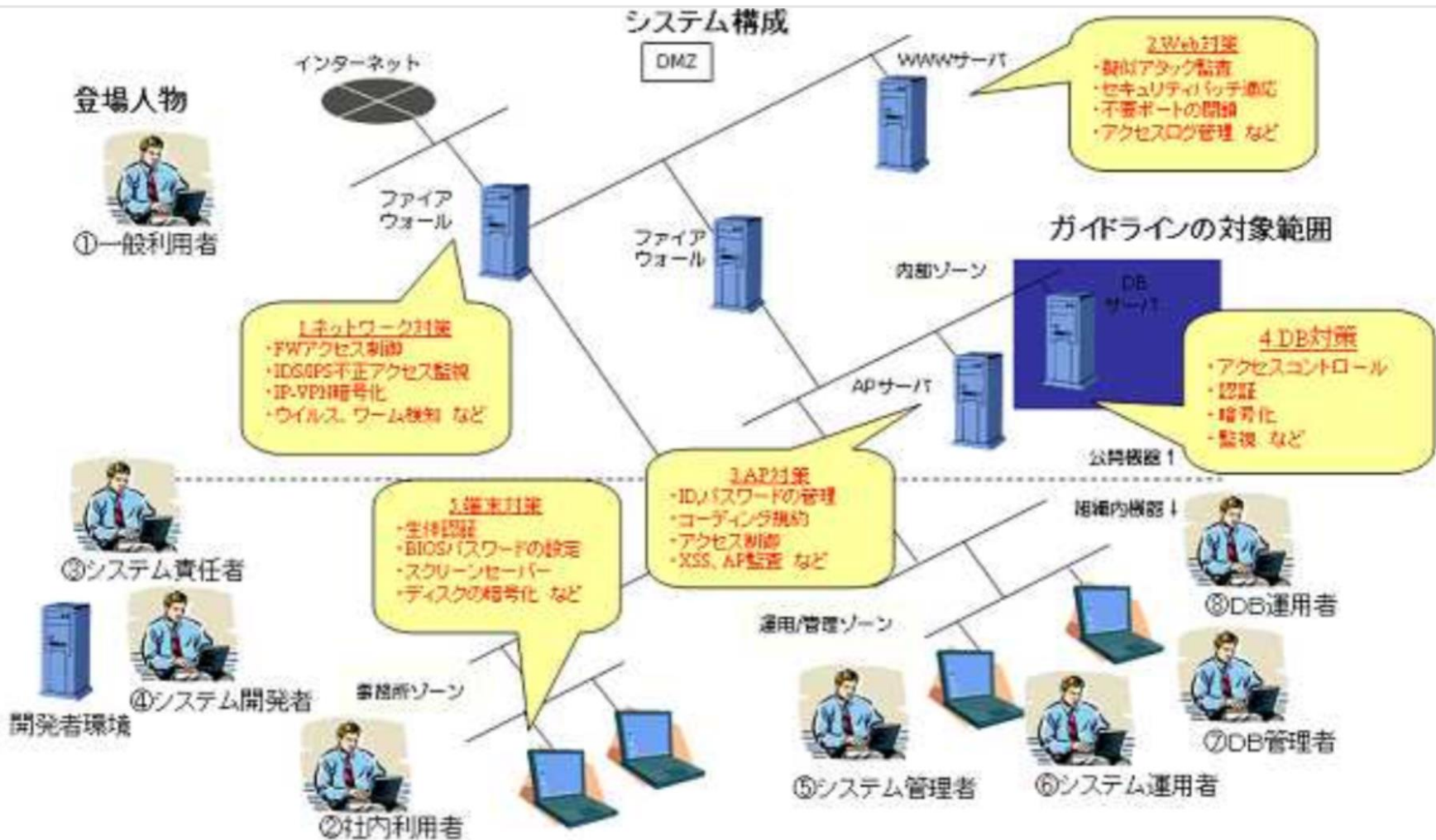
- DBSC「DBA1000人に聞きましたアンケート」
(2014年9月10日公開)
 - 「管理者でない人に
管理者権限が付与されている」 30.4%
 - 「将来、DB内の情報を売却するかも知れない」
「そう思う」3.6%+「ややそう思う」7.1%=10.8%

DBを守ることの難しさ



- DBMSはシステムの部品にすぎない
→セキュリティ対策の「銀の弾丸」がない
システムごとに固有の対策が必要
- DBMS登場時と状況は変化しているのに
新しいセキュリティモデルが確立していない
 - 相変わらず集中+権限管理モデル
 - データ分散や暗号技術の導入は五月雨的
- DBMSを使ってシステムを組む技術者が
Webの流儀に流されてゆく

データベースセキュリティガイドライン のシステム構成モデル(2009)



攻撃ベクトルはずっと変わらない・・・

- Webアプリ経由の攻撃（SQL injection等）
内部のクラサバ型AP経由の攻撃
 - アプリ自体の脆弱性対策が重要
- 不正アクセスorマルウェアで遠隔操作
→DB管理コマンドを直接発行されるなど
 - 一般的不正アクセス・マルウェア対策
- 内部不正・ソーシャル攻撃

未だに残る

この脅威が
増している

多くの脆弱性はDBMS以外にある

安全な ウェブサイトの 作り方

改訂第7版

ウェブアプリケーションのセキュリティ実装と
ウェブサイトの安全性向上のための取り組み



IPA 独立行政法人 情報処理推進機構
セキュリティセンター

2015年3月

安全な SQLの 呼び出し方

「安全なウェブサイトの作り方」別冊

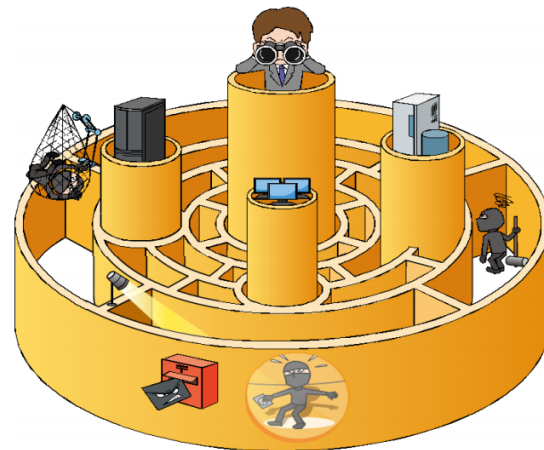


IPA 独立行政法人 情報処理推進機構
セキュリティセンター

2010年3月

「高度標的型攻撃」対策 に向けたシステム設計ガイド

～入口突破されても攻略されない内部対策を施す～



IPA 独立行政法人 情報処理推進機構
セキュリティセンター

2014年9月

IPAの各種ガイドラインがボトムライン

DBMSへの攻撃の対策・緩和策

- 周辺の脆弱性を防ぐ
 - DBMSへのアクセスが可能なAPや端末の脆弱性を防ぐ
 - 端末に遠隔操作型マルウェアが侵入するのを防ぐ
- DBMS自体へのアクセスをマネジメント
 - アカウント管理徹底・アクセス権限の最小化
 - 発行可能なSQL文の範囲を制御
 - ログ管理の徹底(内部不正抑止)
 - 暗号技術の利用
 - 開発環境の分離の徹底

データベースセキュリティガイドライン (第2版:2009発行)

第1章 はじめに.....	2
1.1 目的.....	2
1.2 本ガイドラインの前提.....	2
1.3 本ガイドラインに関する注意事項.....	2
1.4 本ガイドラインの改定にあたり.....	4
第2章 全体のセキュリティ対策における DBセキュリティの位置付け.....	5
2.1 想定システムモデル.....	5
2.2 全体のセキュリティ対策の概要.....	6
2.3 DBセキュリティの位置付け、対象範囲.....	7
2.4 DBセキュリティに関係する要素の定義.....	8
2.4.1 脅威の定義.....	8
2.4.2 登場人物の定義.....	8
2.4.3 DBに関する情報資産の定義.....	9
2.4.4 情報資産の重み付けの定義.....	9
2.4.5 手口の定義.....	10
2.4.6 不正アクションの定義.....	10
2.4.7 脅威の一覧.....	11
第3章 基本方針の策定.....	12
3.1 DBセキュリティポリシーの策定.....	12
3.1.1 重要情報の定義.....	12
3.1.2 リスク分析.....	12
3.1.3 アカウント管理ポリシー.....	13
3.1.4 ログの取得ポリシー.....	14
3.2 人的対策.....	16
3.2.1 啓発/規約.....	16
第4章 DBセキュリティ対策.....	18
4.1 防御系のセキュリティ対策.....	18
4.1.1 初期設定.....	18
4.1.2 認証.....	20
4.1.3 アクセスコントロール.....	23
4.1.4 暗号化.....	25
4.1.5 外部媒体の利用制御.....	26
4.1.6 その他.....	27
4.2 検知、追跡系のDBセキュリティ対策.....	29
4.2.1 ログの管理.....	29
4.2.2 不正アクセス検知.....	31
4.2.3 ログの分析.....	33
データベースセキュリティガイドライン執筆者(敬称略).....	34
データベースセキュリティガイドライン第2版執筆者(敬称略).....	35

- DBFWなど特殊な製品を後付けしない前提
- Oracle/MSの設定集も付録に
- 情報の格付け、アクセス権管理、ポリシー、ログによる検知など中心

DBMSに特化した対策といえは...

データベース暗号化ガイドライン

第 1.0 版

2011 年 11 月 1 日

データベース・セキュリティ・コンソーシアム

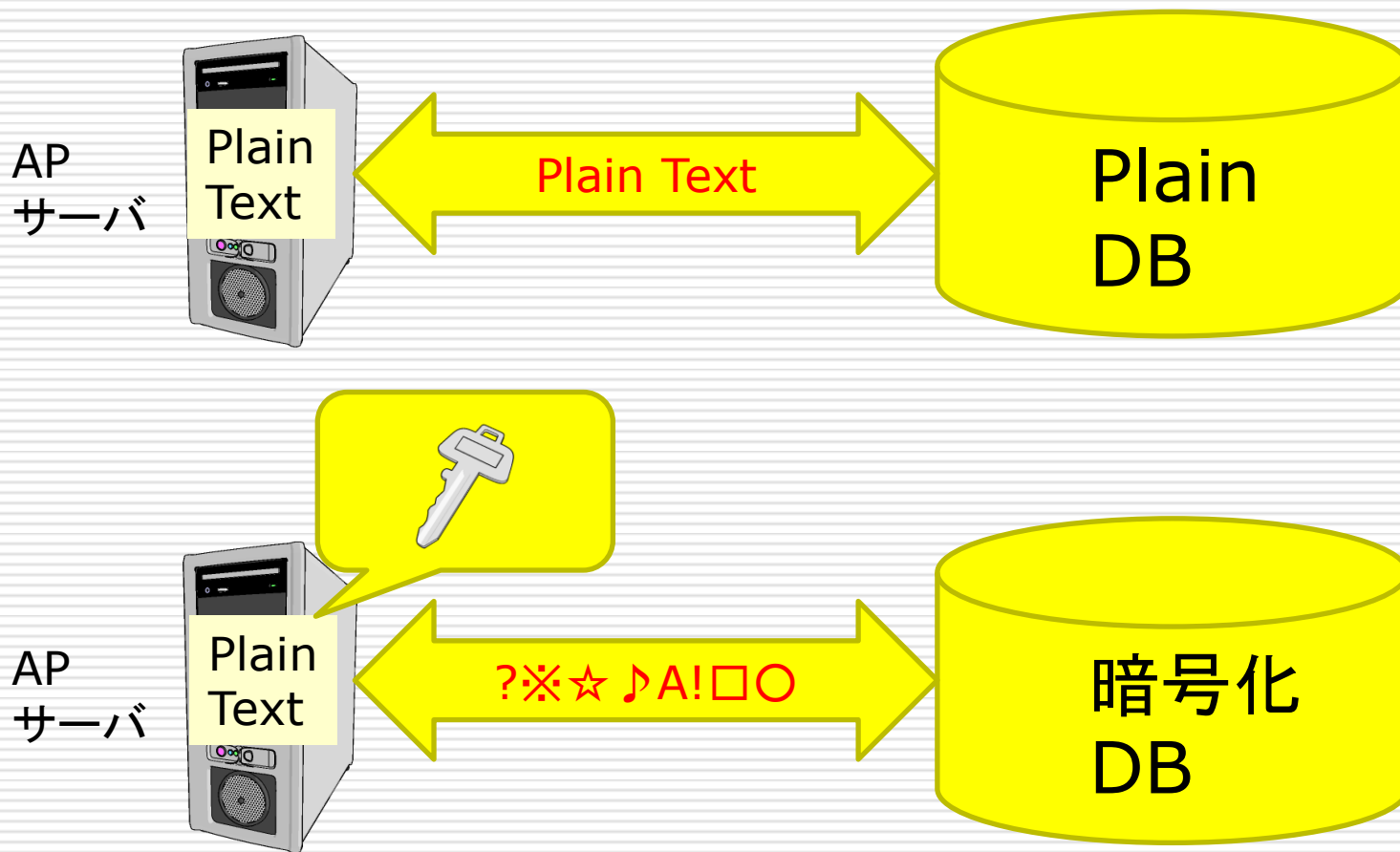
DB 暗号化 WG

- DB暗号化が有効
- DBSCガイドラインは以下に整理して解説
 - DB自体の暗号化
 - データ・テーブル・カラムバックアップ
 - 鍵管理
 - 鍵ファイル／HSM利用
 - アクセス制御
 - 世代管理
 - 通信路暗号化

暗号は「罨」が多い？

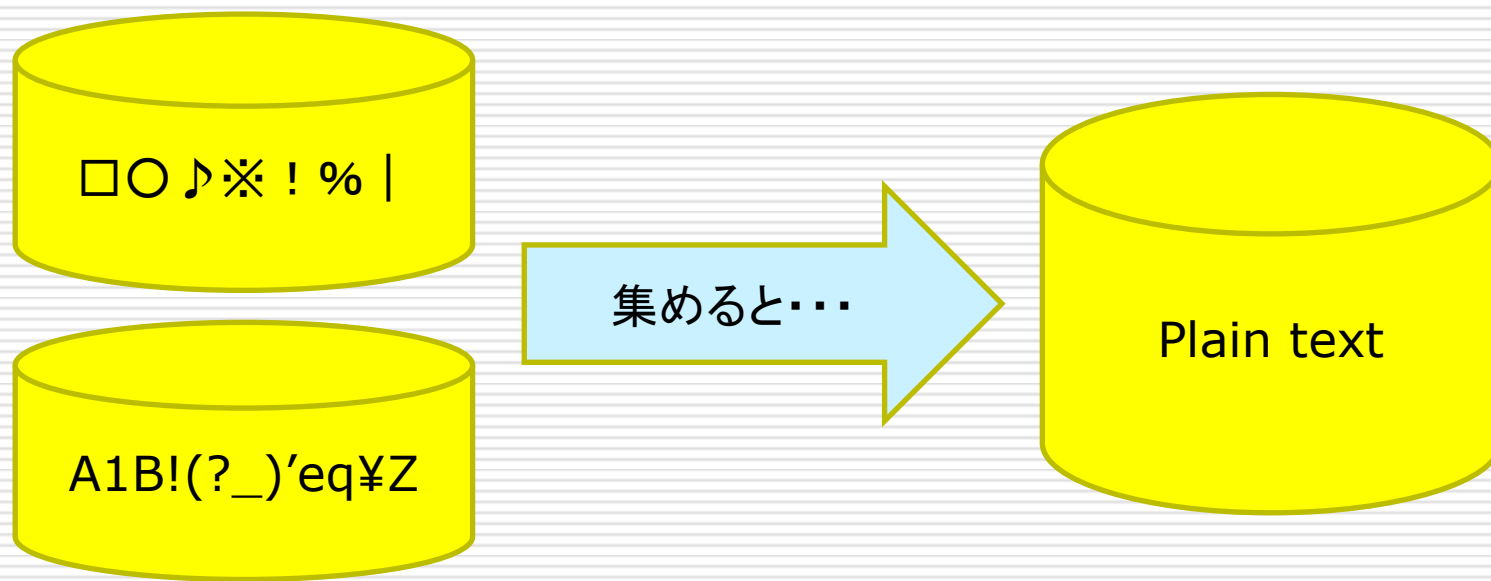
- 「暗号」のイメージするものの幅が広すぎる問題
- 「暗号」という言葉が万能に思える問題
- 独自暗号方式は安全性が担保できない問題
 - BKSA絶対禁止
- 正しい使い方が出来ていないことがある問題
 - 「パスワードの暗号化」はどうか？
- 鍵管理に穴があることが多い問題
 - コード内に埋め込みetc
- DB利用では性能とのトレードオフ問題

暗号の効果は「リスクポイントの移動」



リスクは暗号鍵に移動する＝鍵管理重要！

暗号で期待される技術：秘密分散



各分散データ単体では復元が不可能であることがポイント

欠点：処理が重い...

分散処理を強いられる弊害

暗号で期待される技術：暗号化状態処理



暗号化された状態のまま
検索や演算が出来る処理方法
準同型暗号化やマジックプロトコルなど利用

欠点：処理がとてとても重い...

可能な演算に限りがあり汎用性がない...

なのでとりあえずは...

- 「無理せず、あたりまえのことを、粛々と」
 - 結局あたりまえのことができていない例が多い
 - 脆弱性を突かれる、マルウェアに入られる
 - 脆弱性管理・権限管理はきっちりと
- 防御を完全にするばかりではなく
防御が破られたときのことをよく考えよう
 - 端末が乗っ取られたときのことを考えて権限最小化
 - ログの保護と内部犯行の備えも兼ねたログ監査
 - ネットワークの異常検知

おわりに

- こんなに時代は進んでる
 - データは増えている 活用への圧力も高い
 - なのに 守り側はあまり進歩してない...
-
- 状況は厳しいが... やれることをやろう！