DBSCからの緊急提言解説

DBSC
DataBase Security Consortium

DBSC緊急提言プロジェクト

Agenda

- 提言書について
- 1章解説
- 2章解説
- 3章解説
- 4章解説

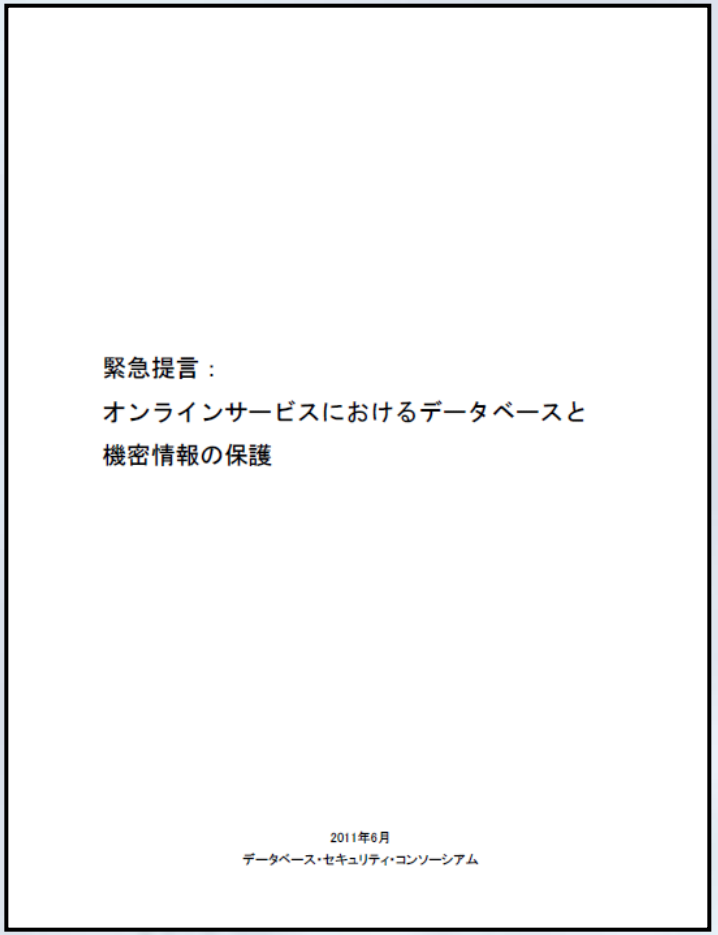
はじめに

- この提言書は2011年4月に発生したオンラインゲームサイトにおける不正アクセス・個人情報漏えい事件をうけて、同年6月に作成・公開したものです。
- したがって、2011年夏以降に明るみに出た、メールを中心とした、いわゆる「標的型」攻撃についての言及はありません。
- しかし、情報の「金庫」であるデータベースを保護しておくことが機密情報保護のために有効である点は同じであると考えられます

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

- 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。



1.1 定量化しやすい直接的被害の例

- サービスが停止することで、停止期間中のオンラインゲーム、物品・サービスの販売等による売上げと利益が失われる。
- セキュリティ専門会社等に依頼し、原因究明・解析・証拠保全などを行うコスト
- 個人情報の漏えいについては、個人（情報主体）に対する問い合わせ対応委託費用や、謝罪等の費用が必要。
- 事件発生後に改善策として多額の投資を迫られることになる。

JNSAの試算による30万人顧客情報漏洩の場合の緊急対応費用（例）

項目			費用
直接被害	逸失利益	インターネットショッピングサイト利益額（1ヶ月分）	約8,330万円
	機会損失	インターネットショッピングサイトの成長率分（1ヶ月相当）	約830万円
間接被害	業務継続費用	対策組織業務に係る人件費（1ヶ月分）	約2,000万円
		セキュリティコンサルタントの依頼費用（1ヶ月分）	約500万円
	損害賠償費用	損害賠償費用	約108万円
		弁護士費用、裁判費用	約9万円
	見舞品費用	見舞品代＋送料他（30万人分）	約2億1,000万円
	謝罪訪問費	謝罪訪問に掛かる費用（15人分）	約165万円
	広報費用	謝罪広告費（新聞5紙）	約1,000万円
		情報公開ページ作成費用（5回）	約25万円
	臨時的な対策費用	コールセンター設置費用（1ヶ月分）	約1,000万円
		問い合わせ窓口常駐人員（1ヶ月分）	約300万円
潜在化被害	影響業務	影響を受けた業務の人件費（1ヶ月分）	約3,000万円
	業務外の潜在化被害	ブランド価値の低下	＋α
		合計	約3億8,237万円

出典：日本ネットワークセキュリティ協会「2003年度 情報セキュリティインシデントに関する調査報告書 第二部」

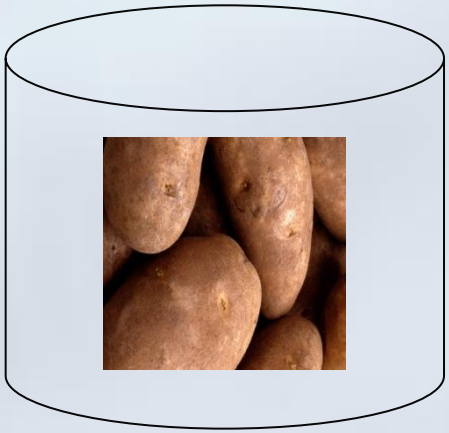
1.2 定量化が難しい間接的損害の例

- 顧客企業や個人顧客からの問い合わせ対応、広報（顧客向け、マスコミ向け等）対応にかかる内部人件費が必要となる。業務効率の低下や事件の対応、苦情対応などに関わる人的コスト（営業対応なども含む）が発生する。
- 社会的な企業イメージ・風評の問題が起きる。事件の原因となった情報保護体制への批判、事件発生後の対応に関する批判など、当該企業は多くの厳しい社会的批判にさらされることになる。またこれらに伴う株価への影響は明確な根拠がないものの、事業形態によっては大きな影響を及ぼす懸念も払拭できない。
- 事業内容・規模によっては、単一のサービスやシステムが攻撃されるだけでなく、 その後、当該企業が提供する他のサービスやシステムも次々と攻撃対象となり 「標的型攻撃」の対象となってしまう場合がある。

あるネット系企業が攻撃を受け、サイトを閉鎖している間に株価が18%程度下落した例（赤枠内が閉鎖期間）

大前提

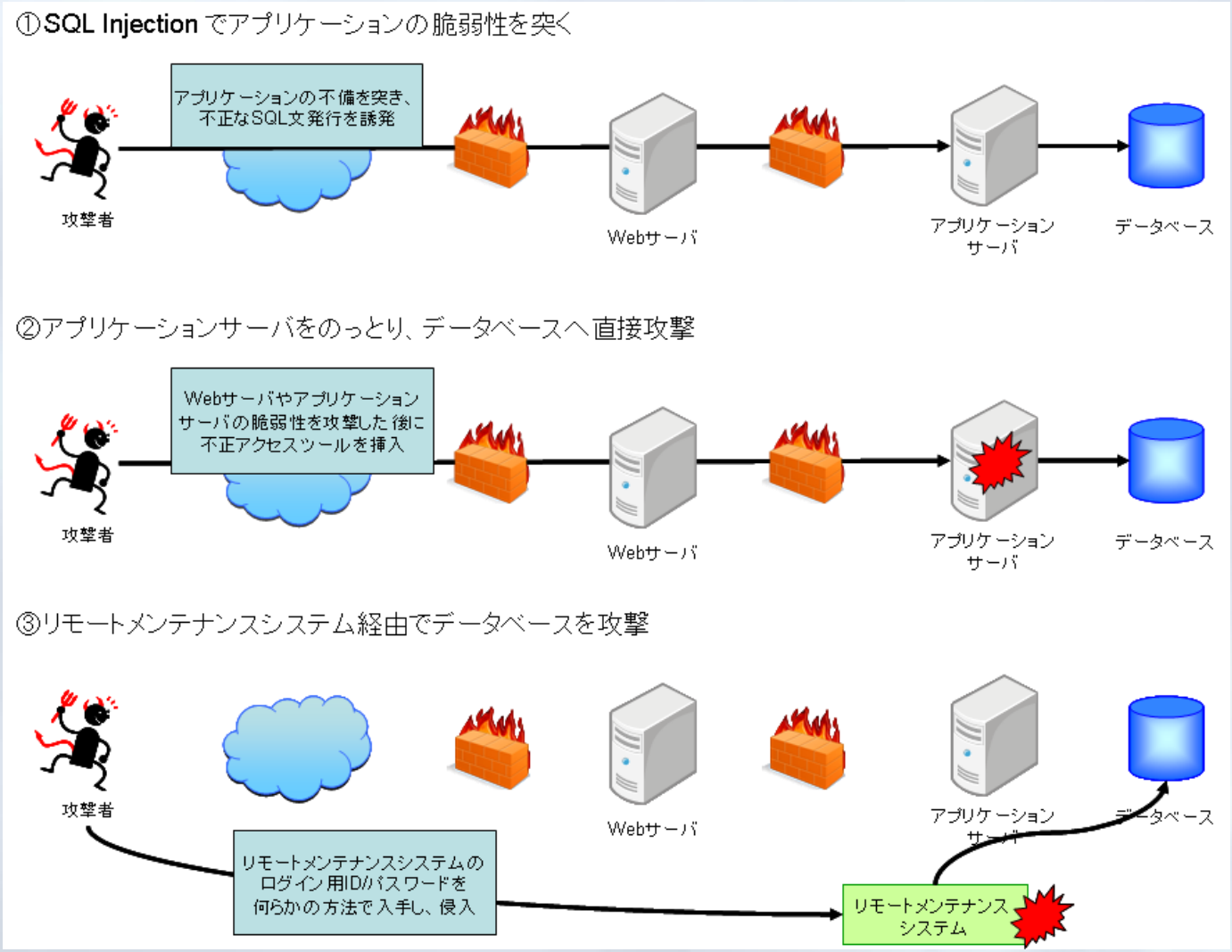
- 重要なデータ(情報)がデータベースに含まれる前提
- 以下は極端な例



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

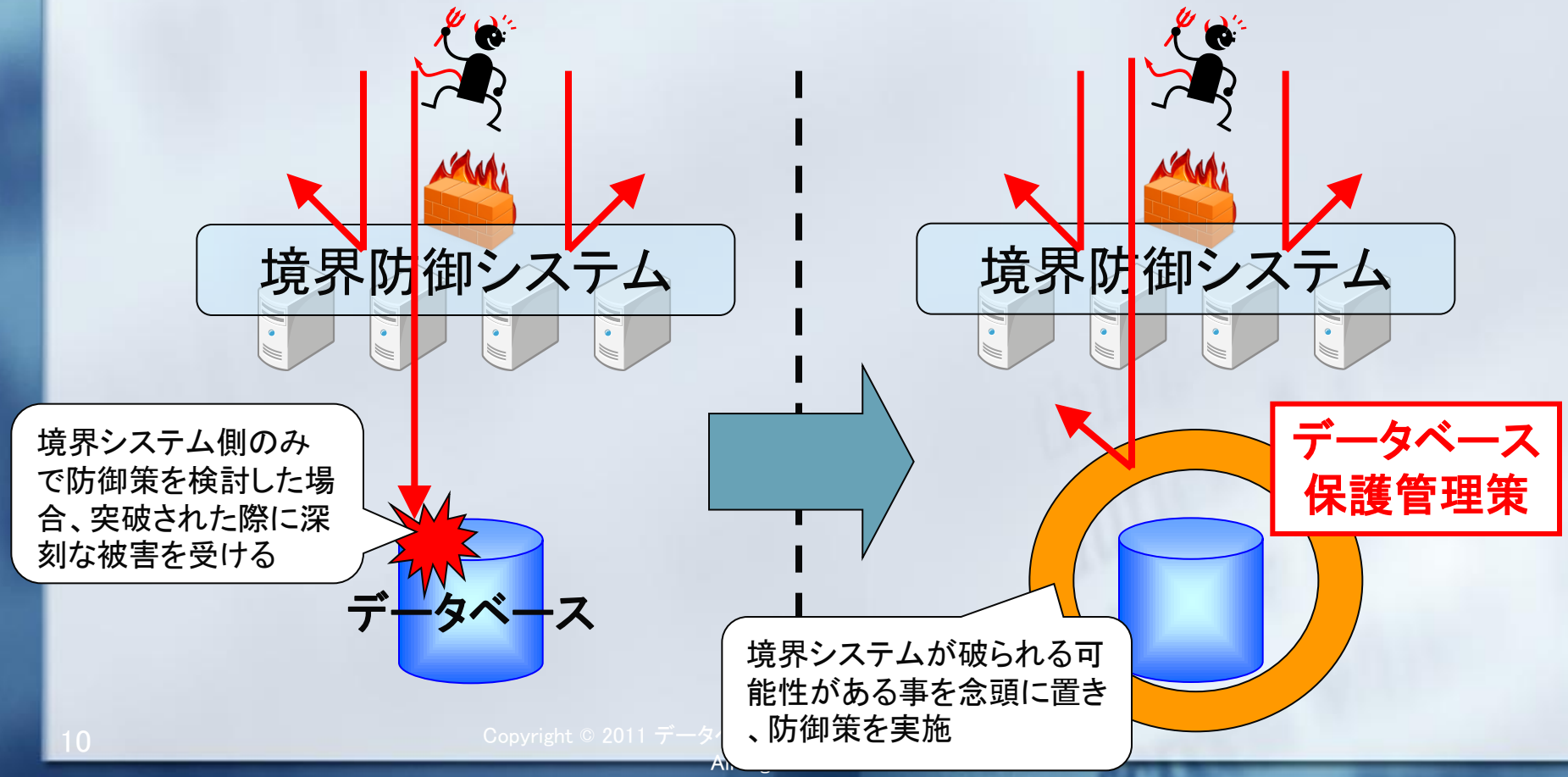
※詳細についてはセキュリティ専門企業や独立行政法人情報処理推進機構（IPA）による解説を参照下さい。

- 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

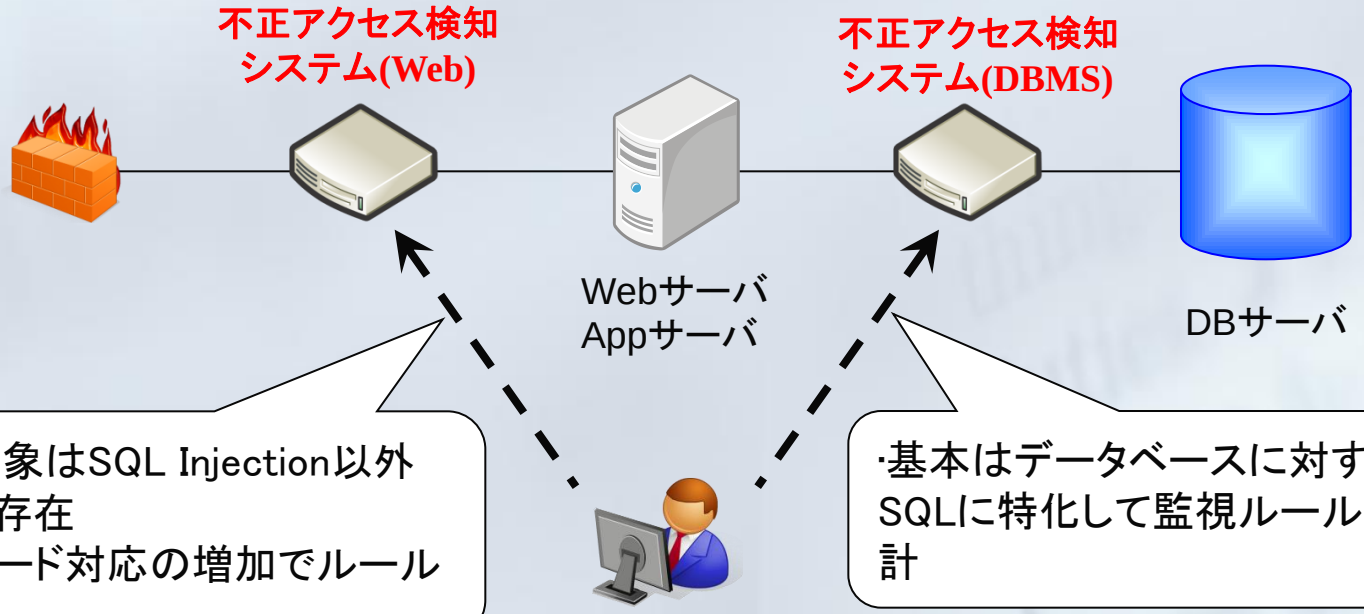
技術的に考えるべきこと

- 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



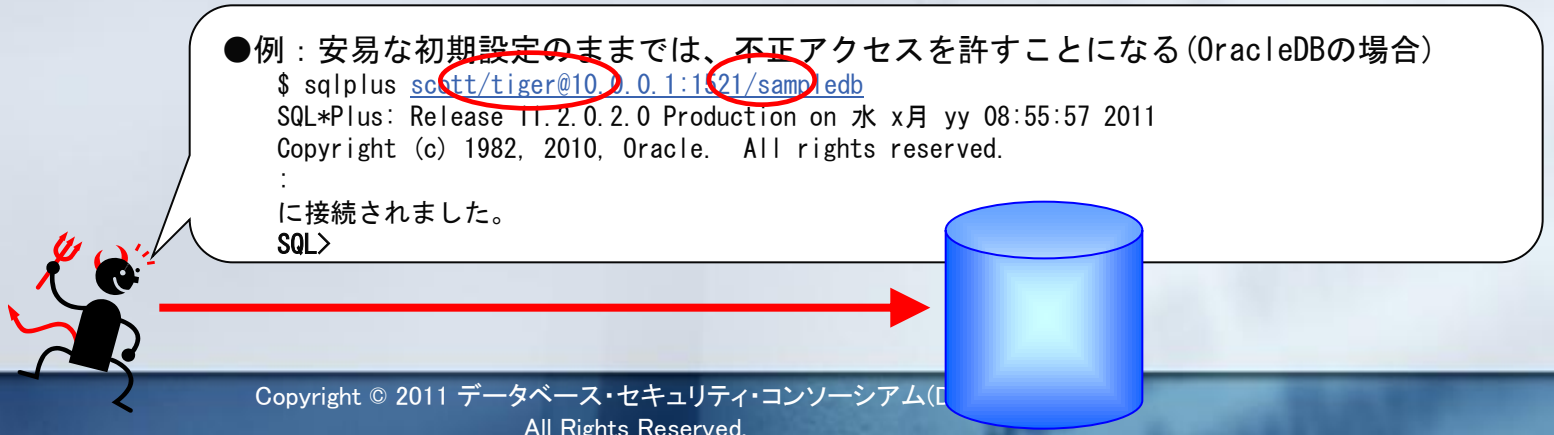
3.1 不正アクセス検知の導入

- 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



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

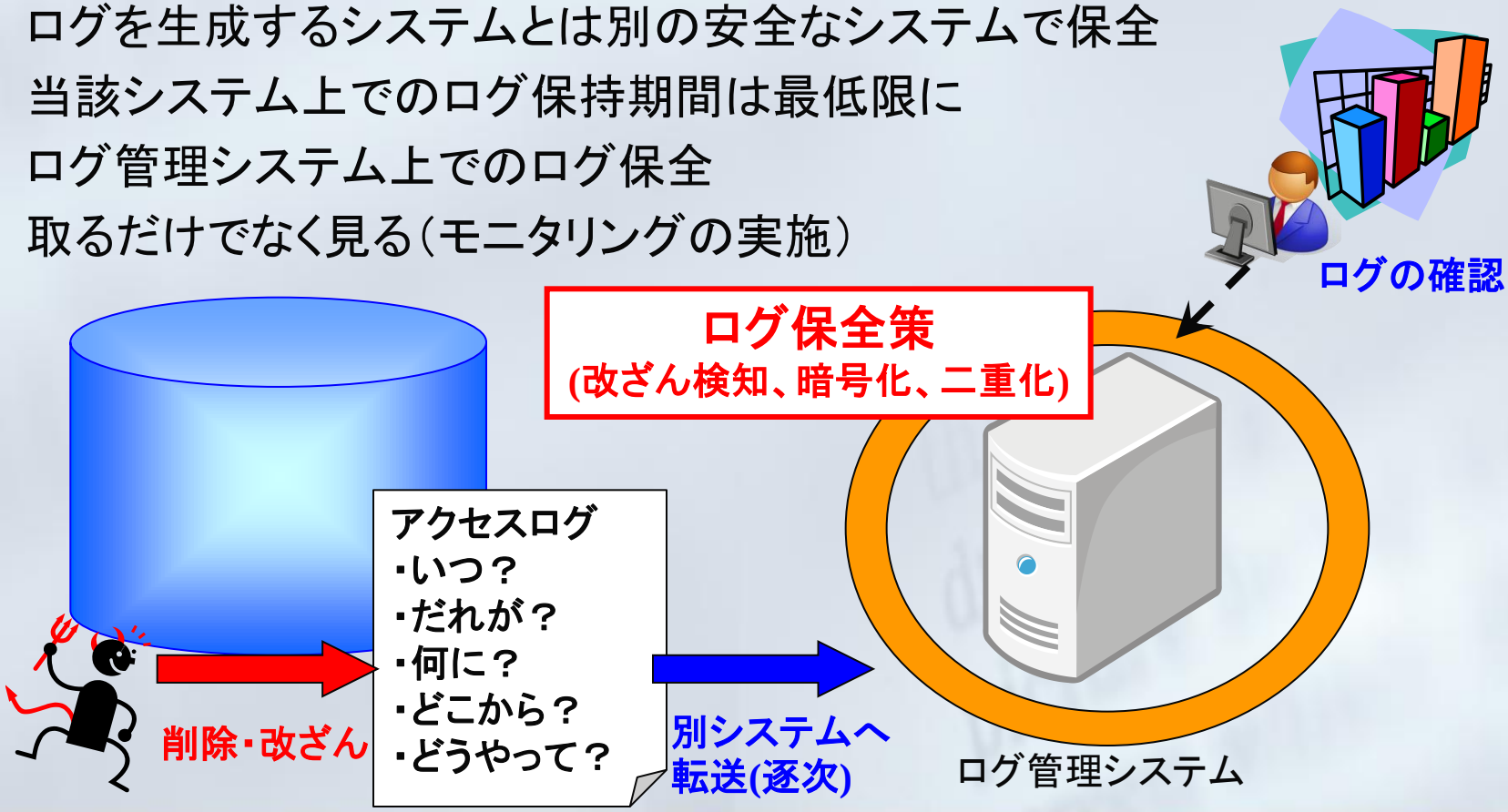


3.3 OSにまで攻撃の手が及んだ場合の対応

- 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

3.6 各種コンプライアンス対応の管理策見直し

- コンプライアンス対応実施済みの企業は多い
  - ISMS(ISO/IEC 27001)
  - 個人情報保護法(及びガイドライン)
  - 内部統制報告制度
  - FISC安全対策基準
  - PCIDSS
  - etc…
- 対応の見直しを
  - データベースに関連する管理策の見直し
  - 仕組み(マネジメントシステム)としての再考

4.1 経営リスクとしての情報セキュリティと情報保護の責任の理解

- 万一事件・事故が発生した際に、経営者が「そんなに大量の個人情報があるとは知らなかった。」「適切な対策をしていると思っていた（が、実はしていなかった）。」というような事態に陥らないことが重要である。したがって経営者のガバナンス（情報セキュリティガバナンス）という点では以下のような点について経営者自らが把握している必要がある。
  - 保有・管理している情報にはどんなものが、どれくらいの量で存在するのか。
  - 保有・管理している情報にはどの程度の機密性があるか、それらに侵害が　起きた場合、その事業インパクトはどの程度深刻か。それらはレベル分けされているか。
  - 機密性の高さと事業インパクトの大きさに見合った保護対策が適切に行われているか。
  - 保有・管理している情報の管理・保護責任者は誰か。社内でオーナーシップは明確になっているか。

4.2 情報の格納場所「金庫」としてのデータベース

- 経営資源として非常に重要な「情報」の入れ物、いわば 「金庫」に相当するのがデータベースであること。
- 金庫に鍵をかけない人がいないように、データベースに対しても適切な鍵をかける、つまり適切なセキュリティ対策が重要であること。

（経営者の方々へ）

上記は、よりよい情報保護、個人情報、クレジットカード情報などにかかわる事業リスクの最適化に役立つことを是非ご理解頂きたい。

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