社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＤＤ－62（12）
2007／7／27

内部統制を実現するためのデータベース・セキュリティ技術
－モニタリングからコントロールへ－

松永 豊† 大場 みち子‡

†東京エレクトロン デバイス株式会社 〒163-1034 東京都新宿区西新宿 3-7-1
‡株式会社日立製作所 ソフトウェア事業部 新分野事業推進室
〒244-8555 横浜市戸塚区戸塚町 5030 番地
E-mail: †matsu@kabuki.tel.co.jp, ‡michiko.oba.cq@hitachi.com

あらまし 情報漏洩の防止や規制遵守の要請により、データベース内の情報アクセスや変更に関するセキュリティ管理が必要になってきている。ところが、データベースへのアクセスを記録する監査機能が成熟してきたのに比べて、不正な流出や改竄を未然に防止する手だては普及していない。そこでデータベースのアクセス制御や不正操作の検知、暗号化など、利用可能な技術を調査し、特徴を分析した。その上で各セキュリティ技術のさまざまなセキュリティ要件に対する適合性を検討した。

キーワード 内部統制，データベース，セキュリティ，アクセス制御，暗号化，監査

Database Security Technologies for Internal Control
－Evolution from Monitoring to Control－

Yutaka MATSUNAGA† Michiko OBA‡

† Corporate Planning Dept., Tokyo Electron Device Ltd. 3-7-1 Nishi-Shinjuku, Shinjuku-ku, Tokyo, 163-1034 Japan
‡ Hitachi Ltd. Software Division, Emerging Business Development
5030 Totsuka-cho, Totsuka-ku, Yokohama-shi, Kanagawa 244-8555, Japan
E-mail: †matsu@kabuki.tel.co.jp, ‡michiko.oba.cq@hitachi.com

Abstract As the requirements for preventing information leakage and for regulation compliance are getting critical, the security management capability of the information access and modification in database systems is becoming necessity. However, compared with relatively established auditing functionality to log the database acccess, mechanism to prevent the information leakage and unauthorized modification is still not widely deployed. In this research, a variety of the available security technologies including access control, detection of unauthorized operation, and encryption are investigated and analyzed. Then we evaluated the technologies against the different security requirements for the best solution.

Keyword Internal Control, Database, Security, Access Control, Encryption, Audit

1. はじめに

データベースに保存される情報は、企業や政府機関など組織のあらゆる活動にかかわっているため、さまざまな観点からセキュリティの確保が必要になる。

近年多発している情報漏洩事件は、インターネットに不用意に露出したデータへの不正アクセスから、比較的安全と考えられてきたバックエンドのデータベースからのデータ流出へと傾向が変化してきている。それに伴い、漏洩規模の拡大と直接的金銭的被害が目立つようになり、データ保護の重要性が急激に高まっている。一方、米国企業改革法や日本の個人情報保護法などから始まった規制強化による内部統制の分野では、情報漏洩や経営不祥事などの対応強化も影響して、IT統制、特にデータ利用方法も含めたシステムの安全性を要求するようになっている。

こうした統制の対象となるべきデータが大量に保管されるデータベースには、当然高度なセキュリティ対策が求められることになるが、従来、データベースのセキュリティ技術としては、アクセス状況を記録する監査機能が重要視されてきた。筆者らもデータベース監査機能の重要性と課題に注目した検討を行い、報告してきた[1]。ただし情報漏洩の防止や厳格な内部統制の適用のためには、監査だけでなく不正あるいは誤ったデータの利用や変更を未然に防止することが求められる。残念ながら従来の監査機能を中心としたセキュリティ技術では、こうした要求に応えられない。つまり、従来モニタリング(監視)を重視してきたデー

タベースのセキュリティ分野にコントロール(制御)の機能を導入することが求められている。

事実最近になってデータベースの利用をコントロールするための技術が新たに登場しており、運用環境での利用も始まっている。企業改革法やVisaのCISPなど規制遵守の動きで先行している米国では、既に監査において、データベースに対するより高いセキュリティが求められている[2]。

今までいわば素通しだったデータベースへのアクセスをリアルタイムで検査し、ポリシーに違反するものを遮断するわけで、利用技術は発展途上といえるが、今後重要なデータベースを構築する際には避けて通れなくなるだろう。

本稿では、データベースへのアクセスに対してコントロールが求められる背景と必要となる要件を検討した上で、登場してきている複数のデータベース・セキュリティ技術を分析し、各種要件にそれぞれ適合する技術と実装上の留意点を述べる。

2. データベース・セキュリティが求められる背景

データベース・セキュリティに対する要求は、主に情報漏洩防止と規制遵守が原動力となっている。

2.1. 情報漏洩防止のためのデータベース・セキュリティ

情報漏洩事故は従来、インターネットを通じて外部に露出している資源、例えばWebサーバなどへの攻撃によるものが多かったが、データベースへの直接アクセスによる大量の漏洩事故が増加している。

2006年5月に発覚した国内通信会社の個人情報400万件の漏洩事故では、顧客情報を管理するサーバから、開発保守用のパソコンを通じてデータが引き出された[3]。また、2007年2月にはクレジットカード会社などから業務委託を受けていたデータ処理会社より800万件以上ともいわれる個人情報が流出したが、業務委託先社員が電算処理室内で情報を不正にコピーしていた[4]。また、米国では2007年1月に小売業のシステムから合計4500万件以上におよぶ顧客情報の流出が発覚し、この際はネットワークに不正侵入してきたハッカーが内部のサーバからデータを持ち出したといわれている[5]。

これらの事例では、保護されているはずの内部システムから情報が流出した点以外にも共通点がある。一つは、情報の流出自体は最近ではなく、最も古い例では2001年から継続して行われていたこと。さらにいずれも外部からの情報で漏洩が発覚し、後者2件ではクレジットカード不正利用の被害が既に発生していたこと。これらのことによって、データベースを保護する技術および、情報の流出が起こった際に迅速にその事実を検知できる仕組みの必要性が浮かび上がった。

2.2. 規制遵守がデータベースに求めるセキュリティ要件

各種の法令や規制で要求される内部統制においても、データベースに対するセキュリティが重要な役割を果たしている。

金融庁が公開している内部統制の実施基準では、システムの安全性の確保として、「データ、システム、ソフトウェア等の不正使用、改竄、破壊等を防止する」ために、適切なアクセス管理等が必要な旨、規定されている[6]。

2003年に制定された個人情報保護法では個人データ防止など安全管理のために必要かつ適切な措置を講じなければならないことを規定している[7]。ただしその後の漏洩事故の頻発に伴って、2006年に経済産業省より注意喚起が行われ、データベースへの不正アクセスの除去[8]が明記されるようになっている。

またクレジットカード業界の大手企業が共同で策定しているPCI DSS規制では、Webアプリケーションとデータベースの保護を具体的に求めている[9]。

3. データベースに対する脅威

内部統制で求められる安全性の確保について、データベースへのアクセスに対しては次のような脅威が存在する[10]。セキュリティ対策を考える際には、これらの脅威を除外あるいは軽減することが目標になる。

3.1. 必要以上に設定されたアクセス権の濫用

全ユーザについて正確なアクセス権設定を維持することは容易ではなく、画一的な緩いアクセス権設定となっている場合が多い。このため、あるユーザが、本来アクセスできるべきでないデータに対してもアクセスできてしまう状況が存在する。こうして期せずして得たアクセス権を濫用することにより、不正なアクセスが発生する。

この脅威を防止するためには、詳細なアクセス権設定を行う必要があるが、ある程度以上大規模なシステムでは、手作業による管理が現実的ではなくなってしまう。そうした場合はアクセス権の自動判断と設定・管理の仕組みを取り入れる必要がある。

3.2. 適切に設定されたアクセス権の濫用

ユーザ対データの関係においてアクセス権が適切に設定されている場合でも、不正な情報の持ち出しや改竄があり得る。例えば、適切な端末以外からのアクセスによる情報の複写、必要以上の大量アクセス(顧客

対応窓口の要員が顧客リストを全件引き出すなど)といったケースがある。

データ先以外の要素によるアクセス制御、例えばアクセス元、アクセス件数、曜日や時間などの制御により、こうした危険性を低減できる。

3.3. 特権の不正取得

正規のユーザが通常与えられていない特権を取得することによって適切でないデータアクセスを行う。これはシステムやデータベース管理システム(DBMS)に存在する脆弱性を利用することなどによって行われる。 脆弱性の除去(パッチなどによる)と、侵入検知/防御技術が必要になる。

3.4. 通信傍受によるデータ不正取得

クライアントからデータベースに対する通信を傍受することにより、データが持ち出される場合がある。これを回避するためには、通信路を暗号化する必要がある。

3.5. DB への不正接続 (なりすまし、ハッキング)

もともとアクセス権を持たないユーザが、不正な方法によってデータベースに接続することがある。主にDBMS やアプリケーションの脆弱性を利用して行われる。 対策としては、脆弱性の除去、侵入検知技術の利用がある。

3.6. アプリケーションを介した不正アクセス

データベースに直接アクセスする代わりにアプリケーションを経由して攻撃する手法が存在する。特にWeb アプリケーションは広く露出している場合が多く、狙われやすい。 広く知られた Web アプリケーションの攻撃手法として SQL インジェクションがある。

こうした攻撃に対処するには、データベースだけでなくアプリケーションの保護も必要になる。

3.7. オンライン記憶媒体の持ち出し

データベースが保存されているハードディスクなどの媒体が持ち出される場合がある。こうした脅威には、サーバ室やラックなどの物理的セキュリティと、ディスクの暗号化が対策として挙げられる。

3.8. バックアップ媒体の不正取得

復旧用のバックアップデータを納めた磁気テープなどの媒体が紛失、盗難などにより流出する場合がある。 この対策には、バックアップ媒体の暗号化技術が既に普及している。

4. データベース・セキュリティの技術

これまでのべたような新たな要求に直面し、さまざまな脅威に対抗するためのセキュリティ技術も進化してきている。

4.1. アクセス制御

最も基本的で、DBMS の機能としても提供されているのがアクセス制御で、全てのデータベースで何らかの実装が行われている。

ただしポリシー管理が難しく、充分な粒度のアクセス制御を実装するのは簡単ではない。 具体的には、アクセス制御のポリシーは、ユーザごとに対象テーブル、操作の種類、アクセス元、曜日や時間帯などの項目について、実行の可否を定義する必要がある。 初期定義もさることながら、ユーザの移動やアプリケーションの変更に伴う管理が莫大な工数を要求する場合があり、注意が必要となる。

4.2. 監査ログ

データベースに対するモニタリングとして中心的な監査ログの取得も、技術としては従来から提供されていた。

注意点としてはサーバに与える負荷や、必要な情報が記録されないといった問題点が存在するが、監査技術の進歩により解決されてきている[1]。 具体的には主に、

- ユーザ名の特定
- 詳細なアクセス制御
- セキュリティ機能の迂回防止
- ログデータの管理

といった点に注意を払う必要がある

4.3. データベース・ファイアウォール

モニタリング技術を拡張してコントロールまで可能にしたのがデータベース・ファイアウォール(DB ファイアウォール)あるいはデータベース・セキュリティ・ゲートウェイ(DSG)[11]と呼ばれる技術分野で、近年急速に充実してきている。データベースへのアクセスをリアルタイムで監視し、不正なアクセスを発見して通知あるいは遮断する。構造としては一般的なネットワーク・ファイアウォールに似ているが、従来 DBMS で行われてきたアクセス制御と、IPS (Intrusion Prevention System、侵入防御装置)の機能をネットワーク上で提供する。

データベース・ファイアウォールでもポリシー定義が問題になる。 不正なアクセスの定義が、データベース定義やアプリケーション、ユーザの役割など多数の要因に左右されるため、この定義(ポリシー)の策定と

管理が運用のポイントとなる。

4.4. 暗号化

情報の不正な参照、漏洩などに効果が期待されているのが暗号化技術で、さまざまな形態がある。 従来、通信路の暗号化は比較的広く行われてきた。最近の情報保護の要求により、保存状態や運搬可能な媒体上のデータに対する暗号化が行われている。この種の取り組みの一つとしてデータベース内の暗号化がある。データベース内にある特定のテーブルやカラムを暗号化し、正規の経路によるアクセス以外では判読できないようにする。

さらにバックアップ媒体の紛失や盗難に対応するために、バックアップに限定した暗号化技術も登場している。

暗号化にかかわる注意点としては鍵管理がある。暗号化に使用した鍵を安全に保管し、正当なユーザにのみ復号用の鍵を提供する仕組みが必要になる。

また、データベース内のデータを暗号化する場合には、追加で注意するべき点がある[12]。

- 性能 – 暗号処理は、サーバの性能に大きな負担となる。
- データの互換性 – 暗号化によってデータのサイズが変わることにより、データベースへの格納に問題が出る場合がある。
- 検索 – 暗号化したままでは検索が行えないため、暗号化データのインデックス管理、復号してからの検索処理など、対応が必要になる。
- 権限の分離 – データベース管理者が暗号鍵の管理も兼ねる場合、セキュリティ上大きなリスクとなる。

そして暗号化は暗号化の対象について、さまざまなレベルでの実装が提供されていることも考慮が必要になる。 保護の要件と環境によって、適切な暗号化対象と技術を選択する。図 にデータベース周辺で提供される暗号化技術の形態と暗号化対象を示す。

このように、ほとんどの暗号化対象において、ソフトウェアかアプライアンス(ハードウェア)を選択可能な状況にある。 アプライアンスは暗号化対象ごとに、専用の機能を提供していることが多い。 一般に、アプライアンスは性能と導入の手軽さ、暗号鍵管理の安全性、大規模システムにおける一元管理などに優れ、ソフトウェアは導入コストやインストールの柔軟性が特徴で比較的小さなシステムに向く。

4.5. 脆弱性検査

特権の不正取得やサーバへの不正接続などを回避するため、悪用の可能性がある脆弱性をサーバや

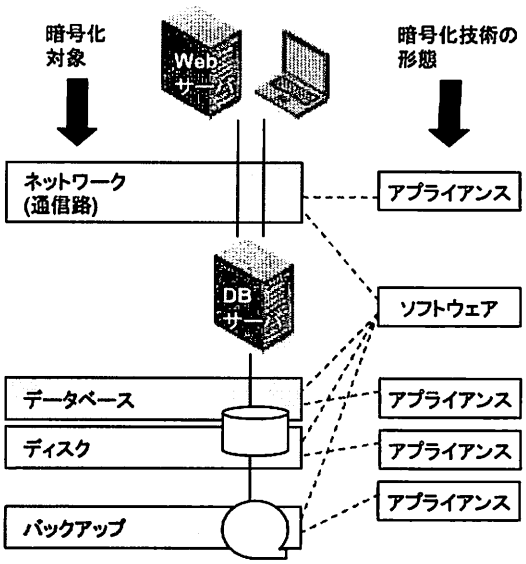

図 1 暗号化技術の形態と暗号化対象

DBMS から排除しておく必要がある。排除自体はパッチの適用や設定の強化によって行うが、新たに発見されるものも含めて脆弱性が存在しないことを確かめるために、脆弱性の検査を行う。 従来は手作業による確認が主だったが、自動的、定期的に検査を行う技術が発達してきている。

データベースの脆弱性検査は、パッチで修正するような類の脆弱性以外に、例えばディフォルトのアカウントやプロシージャがオープンになっていないか、といった設定面での検査も必要になる。 また、DBMS の種類やバージョンによって異なる検査が必要になる。したがって、検査のツールは、対象の DBMS に依存する包括的な検査項目を網羅している必要がある。

また、脆弱性の情報は拡大するものであり、アプリケーションやデータベースの変更によって状況が変わることもあるので、検査項目が頻繁に更新されることも重要な要素となる。

4.6. プロファイリング / DAM

アクセス制御やデータベース・ファイアウォールなど、コントロールを行う技術では不正を判断するためのポリシー定義が重要になる。 また、リアルタイムではないアクセス監査でも、異常な挙動があったかどうか、を判断するためには、正常なアクセスを定義することが必要で、結局システムやユーザ、環境に依存したルールの運用が重要になる。こうした正しいアクセスの定義と不正アクセスの検知に使われるのが、プロファイリングあるいは DAM (Database Activity Monitoring, データベース挙動監視)といわれる技術で、

ここ2年ほどで実装例が出てきた。

通常のアクセスパターンを学習してプロファイリングし、その内容により正しいアクセスを自動定義する。 そのプロファイルから乖離したアクセスは不正、あるいは不審とみなし、通知あるいは遮断を行う。 このことにより、不正アクセスの未然防止の大きな障害となっていたポリシー管理を自動化することができ、データ・セキュリティ関連で最も有望な新分野の一つだと評価されている[13]。

プロファイリングの注意点としては、自動生成したプロファイル情報に誤りが無いとは言いきれないため、プロファイルの導入時および運用中の定期的な確認とチューニングが必要になる。

4.7. WAF

アプリケーションを介した不正アクセスからの防御には、アプリケーションに対するセキュリティ対策が必要になる。 特にインターネットに露出する Web アプリケーションは、SQL インジェクションなど、データベースへの不正アクセスを目的にした手法によって狙われやすい。 さらに Web 2.0 といった新たなアプリケーション開発手法の普及によって攻撃も多様化しており、防御方法も新たな対応が求められている[14]。

経済産業省の個人情報に関する注意喚起でも、データベースの保護の前提として、情報システムの外部との接点となるウェブサイトの脆弱性の悪用を防止することが必要であると指摘されている[8]。

こうしたアプリケーションの保護には、専用のセキュリティ技術が必要であり、WAF (Web Application Firewall)とよばれる製品分野として実装されている。 Web を使った3階層システムで個人情報などを扱う場合には必須の技術となっている。

5. データベース・セキュリティ機能の実装形態

データベース・セキュリティの技術はそれぞれさまざまな形で実装されているが、システムへの導入形態によって、4種に分けられる。

1. DBMS 付属機能 – DBMS 自身が提供する機能。アクセス制御、監査、暗号化などがある。
2. ホスト・ベースのツール – データベース・サーバに専用のソフトウェアを導入する。
3. ネットワーク上監視型 – ネットワーク上で通信を監視する。
4. ネットワーク・ゲートウェイ – ネットワークにインラインで設置し、通信の検査および遮断を行う。

これら導入形態により、サーバへの影響や導入・運用における手間やコストが異なってくる。

表 1 データベース・セキュリティの導入形態

	1 DBMS 付属機能	2 ホスト・ベース	3 & 4 ネットワーク
権限の分離	できない	できない	できる
サーバ負荷	高	中	無し
DBMS 互換性	種類が限定	要注意	問題なし
導入コスト	低	高	高
運用コスト	低	高	低

ただし、これらの性格は技術の種類にも依存する。例えば、暗号化の実装は、DBMS 付属の機能を利用しても、導入コストが高くなることが多い。

6. 個別の脅威に対する各技術の適合性

以上のことから、2章で説明したデータベースに対する脅威への対策として、適用すべきデータベース・セキュリティ技術の対応を検討した。その結果を表 2 にまとめる。

表 2 脅威に対するセキュリティ技術の対応

	アクセス制御	監査ログ	DB ファイアウォール	暗号化 *5	脆弱性検査	プロファイリング	WAF
必要以上に設定されたアクセス権の濫用	○	*1	○			*3	
適切に設定されたアクセス権の濫用		*1	○			*3	
特権の不正取得	○	*1	○		○	*3	
通信傍受				○			
DB への不正接続（なりすまし、ハッキング）		*1	○	△ *2	○	*3	
アプリケーションを介した不正アクセス		*1	△ *4		○	*3	○
オンライン記憶媒体の持ち出し				○			
バックアップ媒体の不正取得				○			

ただし、*1～*5 は以下の通りである。

*1. 監査ログは脅威への直接の対策にはならないが、規制遵守に必要な証跡、定期的な監査による事故の発見、事故発生時の調査、悪意のある

ユーザへの抑止効果、などのために必要。

*2. 暗号化は、データベース内のカラム単位で詳細な暗号化ポリシーを設定している場合に、一部の不正接続に対して効果が期待できる。

*3. プロファイリングは直接の対策にはならないが、アクセス制御やファイアウォールのポリシー管理に連携させることにより、アクセス権の濫用など、通常では検知できない攻撃の発見、回避を実現できる。

*4. DBファイアウォールはWAFと連携することにより、アプリケーションを介した不正アクセスの検知精度を向上できる。

*5. 暗号化は、暗号化の対象により具体的な技術が異なる。

また、それぞれのセキュリティ技術適用上の留意点を表 3にまとめる。

表 3 セキュリティ技術と留意点

セキュリティ技術	導入時の留意点
アクセス制御	ポリシー管理、 運用コスト
監査ログ	充分な情報の取得、 処理負荷
DBファイアウォール	ポリシー管理、 導入コスト
暗号化	鍵管理、 互換性、 導入コスト、 処理負荷
脆弱性検査	検査項目
プロファイリング	チューニング
WAF	ポリシー管理、 導入コスト、 性能

7. 結論

データベース・セキュリティに対する要件をまとめ、それらに応えるための技術を調査、分析した。その結果、新たに登場してきているものも含めてさまざまな技術を組み合わせることにより、各種脅威に対する対策を適用できることがわかった。データベース・セキュリティの技術は、内部統制で必要とされるモニタリングの段階からコントロールの段階へと進化しているといえる。

今後、これら個別のセキュリティ技術を統合的に運用する手法や、大規模システムにおける運用性、拡張性などについて、一層の検討が必要になってくると考えられる。

文 献

[1] 松永豊, 大場みち子, "Webシステムにおけるデータベース監査ログの課題と解決法, " 情報処理学会デジタルドキュメント, IPSJ-DD06058012, Nov. 2006.

[2] Phebe Waterfield, "Security Begins at the Database Level, " Yankee Group DecisionNote, Oct. 2005.

[3] 榊原 康, "【KDDI情報漏えい続報】「アクセス・ログは1年間しか保存していなかった」, 日経BP ITpro, Jun.13, 2006

[4] "DNPの個人情報漏洩事件で新たな被害明らかに - のべ43社分863万件に," Security Next, Mar.12, 2007.

[5] "盗まれた個人情報は過去最大規模, " IDGジャパン Computerworld, Mar.30, 2007. http://www.computerworld.jp/news/sec/61549.html

[6] "財務報告に係る内部統制の評価及び監査に関する実施基準－ 公開草案－, " 企業会計審議会内部統制部会 III-4.-(2)-②-ロ-c, Nov.21, 2006.

[7] "個人情報の保護に関する法律, " 平成15年5月30日法律第57号, 第二十条, May 2003.

[8] "個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起, " 経済産業省, Feb. 2006. http://www.meti.go.jp/policy/it_policy/privacy/kanki.htm

[9] "PCI Data Security Standard Ver.1.1, " PCI Security Standards Council, Sept.2006. https://www.pcisecuritystandards.org/tech/index.htm

[10] Amichai Shulman, "Top Ten Database Security Threats, " Imperva Whitepaper, Sept. 2006.

[11] Robert Westervelt, "Database security undermined by protocol loopholes, lax defenses", SearchSecurity.com, Mar.06, 2007. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1246341,00.html

[12] Noel Yuhanna, "Database Encryption Solutions, Q3 2005, " The Forrester Wave, Aug. 2005.

[13] Rich Mogull, "Involuntary Data Security Case Studies, " Gartner Security Summit 2007, C8, Jun. 2007.

[14] 松永豊, 大場みち子, "Web技術を悪用する攻撃に対するサーバ側セキュリティ要件, " 情報処理学会 デジタルドキュメント, IPSJ-DD06058012, Jul. 2006.