# システムリスク管理におけるデータベース技術

**Database Technologies for System Risk Management**

**原嶋　秀次**　　**鈴木　裕之**

■ HARASHIMA Shuji　■ SUZUKI Hiroyuki

**Eメール，情報共有など組織における活動基盤の中で，情報システムは欠かせないものとなっている。このような状況において，情報システムのリスクは組織のリスクの大きな部分を占めるようになりつつある。情報システムのリスクには，物理的破壊や障害のリスク，不正アクセスなどのサイバー攻撃のリスク，運用によってプライバシーが流出するなどのリスクがあり，これらに対する対策技術の一つとして，データベースセキュリティがある。**

**東芝は，データベースセキュリティの構成要素である推論制御を用いた，運用に伴うリスク低減を実現するシステム構築手法を開発中である。**

Information systems play an important role in many organizations, supporting their activities including e-mail exchange and file sharing. Risk management for information systems is therefore a subject of prime importance. Risks in an information system include physical destruction of the system, unauthorized access to the system, and unexpected information disclosure caused by careless operation of the system. Database security can be used to minimize these types of risks.

Toshiba is developing a system integration method that reduces operation risks, applying inference control.

## 1　まえがき

情報システムは，組織における活動基盤として，その利用は普及・定着している。このような状況において，情報システムのリスクは組織のリスクそのものになりつつあると言ってよい。障害が発生した場合の影響は，企業活動への影響のみならず大きな社会的影響を及ぼすことさえある。“ITに関する非常時対策をとっていない企業が，壊滅的な被害を受けた場合，5年以内に40％の確率で倒産[*1)]や，“米国で個人情報に関する訴訟で企業が支払った賠償金額は，過去2年間で8,500万ドル[*2)]などの報告もあり，リスク対策は極めて重要である。

ここでは，情報システムのリスクについて考察し，対策技術を概観する。なかでも、データベースセキュリティについて注目し，その応用として東芝が取り組んでいる，推論制御のシステムへの適用方法について述べる。

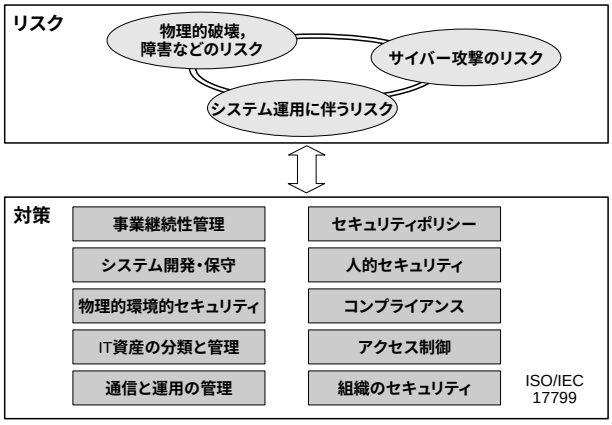


**図1．情報システムのリスクとその対策** ― 情報システムのリスクには，物理的リスク，サイバーリスク，運用に伴うリスクがあり，ISO/IEC17799などに示される情報セキュリティの様々な視点から適切な対策をとることが必要である。

**Risks in information systems and measures to be taken**

## 2　情報システムのリスク

ここでは，情報システムのリスクとリスク対策全般について概観する。

### 2.1　リスクの種類

当社が考える情報システム(以下，システムと略記)のリスクとその対策を**図1**に示す。対策にあたっては，ISO/IEC17799[(3)](ISO：国際標準化機構，IEC：国際電気標準会議)に示されたように，様々な観点からの検討が必要である。

物理的破壊や障害リスク(以下，物理的リスクと呼ぶ)は，システム障害による機能停止やデータの喪失，地震や火災などの災害，テロなどによる物理的破壊などを指す。

災害やテロなどは，他のリスクに比べて発生の可能性は低いと思われるが，万一発生した場合には，大きな被害となる

ことが多い。

サイバー攻撃のリスクは，システムへの不正侵入，不正使用，データの改ざんや成りすましなど多くがある。ハードウェアからソフトウェアまで多くの対策技術・製品が提供されているが，手口，対策技術ともに変化しており，継続的な対策が必要である。

運用に伴うリスクは，システム運用により個人や組織への不利益を発生させてしまうもので，システムによる公開情報からプライバシーや機密情報が推測されてしまうなどがある。

### 2.2 対策技術

物理的リスクに対しては，運用を継続させる仕組みが基本となり，業務継続性[4]として検討されている。リスクの分析・評価→対策方針の決定→運用体制→システム対策→教育・訓練といった手順をとる。保護すべき対象はデータとシステムの機能であり，データの保護に対してはバックアップ技術が，機能の継続に対してはHA（High Availability）やクラスタリングなどの技術が使われる。近年では，ストレージエリアネットワーク（SAN）を利用した，広域リアルタイムリプリケーションが可能となり，データの保護については大きな進展を見た[5]。

サイバー攻撃のリスクに対しては，情報の漏えいを防ぎつつ，正しいユーザーに設定された範囲内の操作を行わせることが対策の基本となる。セキュリティポリシーの作成→システム対策→監視といった手順をとる。ユーザー管理，アクセス制御，暗号化，ファイアウォール・・・というふうに，多くの関連技術が研究・開発され，実用化されている。これらの技術はセキュリティポリシー作成サービス，セキュリティ診断サービス，セキュリティ監視システム構築サービスのようなパッケージとして提供される場合が多い。当社ではセキュリティポリシー作成支援サービスを提供している。

運用に伴うリスクに対しては，システムの運用が個人や組織に悪影響を与えないよう，設計と運用の方法をチェックし，必要な機能を取り込むことが対策の基本となる。体系的な対策方法が確立しているわけではないが，影響の分析・評価→システム対策→監視といった手順になる。関連技術としては，データベースセキュリティがある。

このように，リスクに応じた様々な対策方法と対応技術が存在する。これらを，それぞれの情報システムの役割や環境に応じて適用することになるが，ISO/IEC17799やISO/IEC15408[6]で定められているように，総合的な対策が求められるようになってきている。例えば，バックアップデータからの情報漏えいを防ぐための対策として暗号化やアクセス制御を用いる，といったものである。また，例えば物理的リスクへの対応を考える際に，保守作業の際の運用を継続する仕組みとしておくことで，システムの可用性を高めることができ，積極的な効果を出すことが可能となる。

## 3 データベースセキュリティ

ここでは，当社が中心テーマとして取り組んでいるデータベースセキュリティ[7]について述べる。ごく一部の例外を除いて，ほとんどの情報システムは意味的なデータベースを持っており，それらはマスタデータや取引データなど，重要なものであることが多い。

データベースに対しても，物理的破壊のリスク，サイバー攻撃のリスク，運用に伴うリスクが存在する。特にデータベースに特徴的なのは，次のようなものである。

⑴ データベースへの不正アクセス
⑵ データの一貫性の破壊
⑶ 機密データの読出しと公開エリアへの不正書込み
⑷ 公開データから非公開データの推論など

一方，対策としては，ユーザー認証とアクセス制御，一貫性管理，マルチレベルプロテクション，追跡と監査などが考えられる。これらを実現するデータベースセキュリティ技術として，アクセス制御，フロー制御，推論制御がある。全体のイメージを**図2**に示す。

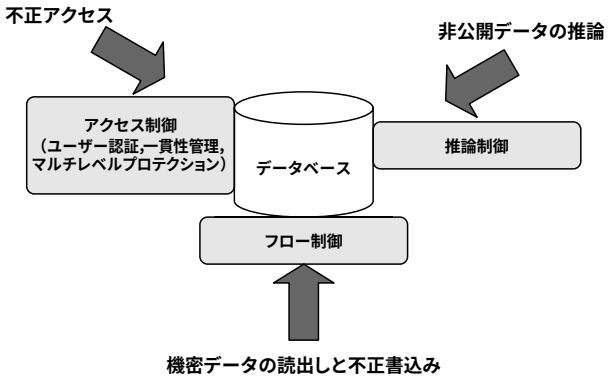


**図2．データベースセキュリティ概要** ― データベースのリスクである不正アクセス，機密情報の流出，非公開データの推論の三つに対して，それぞれ対策技術が研究・開発されており，システムでの活用が期待される。
**Overview of database security**

アクセス制御は，ユーザーの認証，データの読出しと書込み，テーブルの作成と削除など，一般的なアクセス制限が基本となる。これらは通常，リレーショナルデータベースなどのデータベース管理システム（DBMS）で提供されているが，他のシステムコンポーネントを含めた統合的なアクセス制御が必要となることが多く，その場合にはディレクトリサーバ[8]を利用することになる[9]。また，機密情報の取扱いが必要な場合には，ユーザーとデータ双方に順位付けを行い，一定の組合せのみを許可するというマルチレベルプロテクションが使われる。

フロー制御とは，機密情報へのアクセスを許可されたユー

ザーが機密情報を読み出して、アクセス権限のないユーザーがアクセス可能なエリアに書込みを行うことにより，機密情報が漏えいしてしまうことを防止する仕組みである。権限の大きなユーザーは，権限の低いユーザーエリアへの書込みができないようにするのがフロー制御の基本である。

推論制御とは，公開情報や，ユーザーがあらかじめ持っている情報によって，非公開情報が簡単に推定できてしまうことを防ぐ仕組みである。公開情報の提供方法を制限して，このような情報漏えいを防ぐ，例えば，統計情報の公開にあたって，母集合の要素数が一定以下なら公開しない，特定の値を持ったデータは他の状況にかかわらず公開しない，などの方法が提案されている。

推論者があらかじめ持っている情報の量や質によって，同じ情報から推論可能な範囲は大きく異なるため，完全な防止は困難である。しかし，様々な個人情報や機密情報が情報システムで扱われ，ひとたびそれが漏れればインターネットにより瞬く間に広がってしまう状況において，推論防止への配慮は，システムの構築・運用者にとってもっとも重要な課題の一つであると言える。

## 4 推論防止を考慮したシステム構築方法

上述したように，情報システムには様々なリスクが存在し，それぞれの対策技術が研究・開発されている。システムを実際に構築・運用するには，システムの目的を考慮し，これらの適切な利用や運用を行うことが必要である。当社は，このような観点で，リスク対策技術を具体的にどのようにシステム設計に取り込むかについて，その方法を検討している。ここでは，推論制御に関する研究について述べる。

### 4.1 システムの想定

住民情報の公開を想定する。地方自治体による公開や，マーケティング会社によるデータ提供などのケースが相当する。住民のプライバシー保護は絶対条件となるから，統計情報を公開対象とするのが妥当であろう。具体的には，地域別の住民数や収入分布などが考えられる。これに対して，次のような推論が想定される。

⑴ 特定地区において，非常に高い年収，例えば8,000万円以上の人の数を検索し，地域内の立派な住宅と関連付けて，その住人の年収を推測

⑵ 興味のある人物に関する特徴的な事がら，例えば引っ越したばかり，などを利用して地区ごとの転入者数を検索し，住んでいる地域を推定

### 4.2 構築手順

前節のケースで述べたようなプライバシー情報の推論を防ぐために，情報の公開にあたって対策が必要となる。統計データベースの推論防止には様々な技術があり，システム構築・運用にそれらを適切に組み込む手順が必要である。当社が検討中の手順を以下と**図3**に示す。

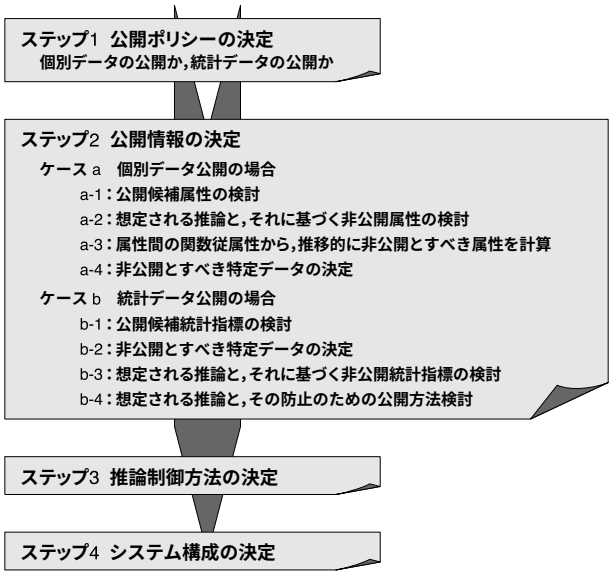


**図3．推論防止を考慮したシステム構築手順** ― 公開ポリシー，公開情報を決定したうえで，推論制御の方式及びシステム構成を決定する。
**System design steps for inference control**

ステップ1　仕様検討のステップで，公開情報を個別情報とするか統計情報とするかを検討する。前節で想定したケースでは，統計情報の公開であったが，企業の事故や不正などが行われていないことを示すための活動情報の公開といったケースでは，個別データの公開が必要であろう。

ステップ2　公開する情報を決定する。個別データの公開では，公開すべき属性（項目）と非公開とすべき項目を決める。例えば，医療機関の実績情報では，患者の名前やそれを推定することが容易な日時や場所などは非公開とする。また，非公開とする特定データも決める。前節の例で，引っ越してきたばかりという事実や，極端に高い年収といった事実が推論に使われていることがわかる。このように，推論に有効な値を特定データと呼ぶ。統計データの公開の場合は，公開する統計指標を決め，それに対して考えられる推論を検討し，非公開にするか対策を施したうえで公開するかを決める。

ステップ3　ステップ2の検討結果を受けて推論制御の方法を決める。前節の想定ケースでは，データベースのデータの件数をn，公開基準をkとしたとき，次のような方法が考えられる。

⒜ 検索結果がk未満又はn－k以上なら非表示とする。

⒝ 母集団（地区）を動的に変更し，検索結果がk以上で，かつn－k以下となるようにする。

(c)　公開基準であるkそのものが推定されることを防ぐために，kより大きな数に動的に変える。

ステップ4　　実装レベルのシステム構成を決めて，システムの構築に移る。システム構成の概要を**図4**に示す。

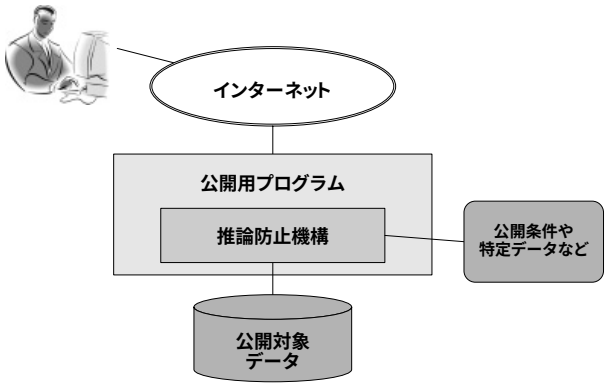


**図4．システム構成例** ― 公開条件として設定された内容に基づき，推論防止機能が公開情報の内容やアクセスを制限する。
**Example of system configuration for information disclosure**

推論防止には監視が効果的であるが，これにはユーザーの認証など，システム全体の枠組みの変更が必要であり，今後の課題である。

## 5　あとがき

ここでは，まずシステムのリスクとその対策技術について概要を述べ，その後，具体的技術としてのデータベースセキュリティについて触れ，システム構築への応用方法について述べた。

冒頭で述べたように，安全な情報化社会を実現するにはシステムのリスク対策は不可欠である。ここで述べた個々の対策技術は，比較的長く研究・開発されてきている。そして，今まさに，通常のシステム構築においてこれらを適切に取り込む段階である。ここでは推論制御について，システムへの取込み手法を紹介したが，様々な組合せや要件への対応が必要であり，今後順次紹介していきたい。

また，利用者の認証や追跡と，提供情報の無制限な拡散を防ぐ手段の併用など，情報流通全体の仕組みのなかでの検討も必要であり[10), (11)]，積極的な提案を行っていきたい。

## 文　献


(1)　栗原　潔．“ZDNetエンタープライズ：Gartner Column：第14回”．ZDNet．<http://www.zdnet.co.jp/enterprise/0109/17/01091788.html>，(参照2003-04-16)．
(2)　アラン・F・ウェスティン．先手の個人情報保護はビジネスチャンスだ．日経ビジネス．2003年2月24日号(通算1180号)，2003，p.182.
(3)　中尾康二，ほか．JIS X 5080:2002　情報セキュリティマネジメントガイド．東京，日本規格協会，2002，285p.
(4)　駒津公一，ほか．ビジネスコンティニュイティ技術．東芝レビュー．**57**，12，2002，p.56－59.
(5)　喜連川優編著．ストレージネットワーキング．東京，オーム社，2002，227p.
(6)　田渕浩樹．国際セキュリティ標準 ISO/IEC 15408入門．東京，オーム社，2001，309p.
(7)　Silvana Castano, et.al. Database Security. New York, ACM Press Books, 1995, 456p.
(8)　大山　実，ほか．X.500 ディレクトリ入門　第2版．東京，東京電機大学出版局，2001，183p.
(9)　小林智恵子，ほか．Webtopシステムにおけるデータベースアクセスのセキュリティ実現　－LDAPによるユーザ管理の一応用－．電子情報通信学会技術研究報告．DE2000-55，2000，p.109－114.
(10)　本村憲史，ほか．ネットワーク上での情報統合に対するプライバシー保護．情報処理学会論文誌．**41**，11，2000，p.2985－3000.
(11)　牧野京子．インフォメーションハイディングの社会的側面．情報処理学会誌．**44**，3，2003，p.260－264.



**原嶋　秀次**　HARASHIMA Shuji
ソフトウェア技術センター　技術開発第二担当参事。
データベースシステムの研究・開発に従事。情報処理学会，電子情報通信学会，ACM会員。
Software Engineering Center

**鈴木　裕之**　SUZUKI Hiroyuki
e-ソリューション社 SI技術開発センター　SI技術担当主務。
各種プラットフォーム構築・ネットワーク設計業務に従事。
Systems Integration Technology Center