White Paper

embarcadero

エンタープライズデータのモバイル化

陥りやすい 5 つの落とし穴とその回避策

Stephen Ball
エンバカデロ・テクノロジーズ
EMEA テクニカル セールス コンサルタント（RAD 担当）兼
アソシエイト プロダクト マネージャー（InterBase 担当）

2014 年 6 月

エンバカデロ・テクノロジーズ

目次

要旨 1

状況分析： 背景と明らかになった教訓 1

エンタープライズデータを モバイル化する際の 5 つの落とし穴 3

落とし穴 1：「すべて」をモバイルに移行しようとする 3

この落とし穴にはまらないようにするには 4

落とし穴 2：共通のエンタープライズ メタデータを維持管理していない 4

この落とし穴にはまらないようにするには 5

落とし穴 3：ローカル データ ストレージを使用してしない 6

この落とし穴にはまらないようにするには 6

落とし穴 4：モバイルデータ ストレージがデータガバナンスや
開発のベストプラクティスに合致していないため作業量やリスクが増大する 7

この落とし穴にはまらないようにするには 8

落とし穴 5：セキュリティと暗号化を付加機能と捉え、
結果的に法的措置を受けたり、顧客を失う危険を冒している 9

この落とし穴にはまらないようにするには 9

まとめ 11

執筆者について 11

参考資料およびリンク 12

要旨

今日、多くの企業が、モバイルデバイス向けのアプリを用いることで、ビジネスプロセスの効率向上やビジネスチャンス拡大の機会を追求しています。この取り組み自体は有益ですが、同時に組織はプロジェクトを適切に管理し、失敗のリスクを最小限に抑える必要もあります。この取り組み方を誤れば、プロジェクトに計上された当初の予算をはるかにオーバーしてしまう恐れがあり、時間とコストの両面で組織にダメージを与えかねません。

技術的な観点からすれば、モバイルは新しいワークスタイルによく適合しているように見えますが、長期的観点から最良の結果を得るためには、まだいくつもの考慮すべき問題が残っています。例えば、以下のような実践上の問題やガバナンスなどに関する問題があります。

- エンタープライズアーキテクチャに対するデータガバナンス
- データ保護の順守
- オフサイトデータに伴うビジネスリスク
- デバイス上のストレージ管理とデバイスに残るキャッシュデータの管理
- 運用形態の変更に伴うリスク、信頼性に関するリスク

このレポートでは、ビジネスデータをモバイル化する際の課題をまとめ、組織が特に陥りやすい落とし穴について明らかにするとともに、エンタープライズデータのモバイル化の指針を示します。このレポートの対象読者は、CIO、マネージャー、データ管理者／データベース管理者、ソフトウェア開発者です。さらに、組織内の法務担当者にも関係します。

状況分析： 背景と明らかになった教訓

技術が採用されていく一般的なパターンによると、その技術が開発されて広く受け入れられて使われるようになるまでに、およそ 10 年という年月がかかります。Apple iOS、そして Google Android プラットフォームの普及、そしてタッチスクリーンを搭載したスマートフォンやタブレット技術の進展を見れば、この見方は正しいように思われます。最初の近代的な「タッチ」デバイスが売り出されてから、既に 7 年が経過しています。現代のモバイルデバイスは、タッチインターフェイス、位置情報サービス、カメラ、3G/4G による高速アクセスなど、既にコアとなる機能強化がなされています。携帯電話は、オペレーティングシステムで動作することにより、瞬時に起動するミニサイズのポケットコンピュータとなったのです。

旧世代の普及型モバイルデバイスは、当時のマーケットリーダーであった RIM（現 BlackBerry）が主導したものでしたが、コミュニケーション機能や強化された電子メールなど非常にすばらしい機能を提供していました。企業では、社員の生産性向上のために、このモバイルデバイスをすぐに採用しました。こ

の初期のプラットフォームは、モバイルネットワークを介してデータが利用できるようになったことで実現したものですが、これらのデバイスが利用されるようになったのは、企業での活用という需要が後押ししたものでした。

しかし、今日では携帯電話市場は成熟しており、これらのデバイスに対する需要を促進しているのは、もはや企業ではなく一般の消費者です。現在のプラットフォームでは、電子メールのような従来のビジネス機能を Facebook、Twitter、LinkedIn などのソーシャルツールと一緒に効果的にパッケージ化することで、この需要に応えています。どこからでも瞬時にアクセスできるように最適化され、操作性がよく、見た目にもリッチなアプリが数多く利用できる環境が整ってきたことで、一般消費者によるモバイルデバイスの利用はさらに拍車がかかっています。

企業においても、新たに採用する人員は PC よりもむしろスマートフォンに慣れ親しんだ世代へと変わりつつあります。この結果、BYOD（Bring Your Own Device：個人所有デバイスの業務への持ち込み）や CYOD（Choose Your Own Device：企業が認定したデバイスからの選択）が、社用モバイルハードウェアのコスト管理に役立つツール戦略として広く受け入れられるようになってきたのです。

現在のデバイスメーカーは、Blackberry の経験、特にその技術的な観点からいくつかの教訓を得ました。その中でも最も顕著なことは、アプリケーション速度や応答速度の向上に、オンデバイスデータとオフラインデータが有効であるという点です。今日では、デバイス上でこれらの機能を提供することで、顧客満足度と利用率の大幅な向上を実現しています。こうした機能は、数多くのメインストリームアプリにおける機能の開発にも浸透してきています。

おもしろいことに、Facebook はもともと HTML5 アプリケーションとして開発されました。これが再開発されて真のネイティブアプリケーションになると、ユーザーが一晩に Facebook に費やす時間は倍増しました。なぜでしょうか。ネイティブコードベースのアプリケーションははるかにリッチなユーザーエクスペリエンスを提供します。それは、一つにはローカルデータキャッシュへの直接アクセスによるものです。その結果、Facebook の使用時間数が増加し、そこに表示される広告も増加してシェアが 18%も増えたのです。

このことは、真のネイティブアプリケーションの価値を示しています。また、データキャッシュを用いることでアプリの利便性を増し、ユーザーの生産性も向上し、アプリの普及が促進されることもわかります。しかし、多くの企業にとっては、データをローカル環境に格納することにより、モバイルでのデータ セキュリティや安全なアクセスに関する課題が新たに生まれます。

最近の従業員は、モバイルデバイスでデータの入力や分析を行うことに抵抗がなくなっています。これは、「顧客向け」の業務においても「社内向け」の業務においてもいえることです。企業は、顧客とのやり取りを積極的にモバイルプラットフォームに移行するようになっており、かつては電子メールで行

ってきた業務以上の効果を得るために、従業員をどのように強化していくか、また組織の生産性向上を達成していくかといった課題に取り組むようになっているのです。

エンタープライズデータを モバイル化する際の 5 つの落とし穴

企業がモバイル環境へデータを移行する計画に着手する際に、しばしば陥りやすい落とし穴をいくつか紹介しましょう。

落とし穴 1：「すべて」をモバイルに移行しようとする

モバイル化プロジェクトの目的は、モバイル時にエンドユーザーのニーズに応える特定の機能を提供することでなければなりません。要件評価の段階で「あなたが モバイルアプリで達成したい目的は何ですか？そのためにこの機能は必要ですか？」という問いに答えることが、この目的を達成するのに不可欠ですが、しばしば見過ごされています。

モバイルで成功を勝ち取るうえで、モバイルアプリにどの機能を用意する必要があり、どの機能が重要でないかをはっきり理解することは、プロジェクトのスコープの定義や企業全体における各アプリケーションの責務を定義することよりも優先します。たとえば、データの入力と分析は企業の基幹系システムを使って実行し続ける選択もありますが、モバイルを使ってデータキャプチャの不足を補うことで作業負荷を軽減できるのであれば、その機能をモバイルで使用できるようにする価値があるといえるでしょう。モバイルを導入したとしても、データ分析の方は、引き続き基幹系システムで維持管理、実行することができます。

同様に、モバイルアプリでは通常、企業の基幹業務の一部のみを扱うので、エンタープライズデータのすべてではなく、そのサブセクションのみが必要となります。モバイルで実行する必要がある業務を決定することが、モバイルデータの要件定義に役立ちます。この定義に基づいて、関係のあるデータだけをモバイルデバイスに格納する必要があります。

モバイルデータの利用にはコストがかかります。デバイスがケーブルまたは WiFi で接続されていないと、一般的にデータ通信コストが発生します。モバイルでは、データの保存に伴うコストも発生します。使用されない余剰データの移動に伴う、隠れたコストも発生します。データの移動によって、デバイスとサーバー間のネットワークトラフィック負荷が増えるからです。これらのコストはすべて避けることができます。デバイスへのデータプッシュとデバイスからのデータプルにおいても、コストがかかるという点は同様です。データストレージが効率的な変更ログ機能を備えていなければ、データのプッシュや

プルにおけるデータ処理量が増加してしまいます。モバイルデータの変更の追跡は、アプリケーションレベルではなくデータレベルで管理すべきです。そうすれば、不注意による遺漏の可能性がなくなります。

モバイルアプリは、PC 向けのアプリケーションと比較して、用途が限定的であり、通信環境も限られています。したがって、すべてをモバイルに移行しようとすれば、目的と関係ない開発に多くの時間を割いた上に、使いにくく運用にコストのかかる、情報漏洩の可能性を持った危険なソフトウェアをリリースする結果になってしまうのです。

この落とし穴にはまらないようにするには

この落とし穴にはまらないようにするには、「あらかじめデータを可視化しておく」という取り組みが重要です。データモデリングは、モバイルプロジェクトの完了に必要な論理モデルとデータの範囲を明確にできる良い方法です。また、これによって、データに関連するコミュニケーションとリスク／影響分析が目に見えるほど向上するほか、データのあいまいさがなくなることで、データとデータを利用するビジネスコンテキストの明確化が容易になります。

シンプルなモデリング作業を行うだけでなく、モデリングに関係するチームの共同作業を支援するツールがあれば、「データの可視化」の実現に一層役に立ちます。可視化したデータを、開発者、データ管理者、データベース アーキテクト、データ利用者といったプロジェクトに関係するすべてのスタッフが共有でき、モバイル化の対象となるデータのユースケースを明確に理解できるようになるからです。

落とし穴 2：共通のエンタープライズ メタデータを維持管理していない

メタデータとは、フィールドサイズ、データ型、フィールド名などといったデータオブジェクトに対する定義です。これは、データガバナンスのベストプラクティスになくてはならないものです。全社で同じメタデータを使用すれば、オリジナルのデータ入力元からその利用先に至るまで、データの互換性が確保されます。

組織でアプリケーションを開発する際には、データ構造に関して、既にあるものを最初から作り直すという落とし穴にはまりやすく、それが次にデータソース間の非互換性を生み出します。これは、モバイルデータベースやメインのデータベースの間だけで起きる問題ではなく、同じデータベース内の複数のテーブルで使用されている同じフィールドにも起こり得る問題です。一方のテーブルの "Person Name" フィールドが 50 文字の文字列型で、もう一方が 30 文字の文字列型フィールドであるという状況を考えてみてください。このようなデータの結合では、"Person Name"が 31 文字以上あった場合にデータが失われる恐れがあり、データの整合性に関する問題が発生するリスクを抱えているといえます。

メタデータには、レコードや情報に対する業務上の論理関係についての情報も含まれています。企業では、各部門に対し、個人情報保護法やデータに関する法令に準拠するように、データの保存が正しく行われるように徹底させなければなりません。メタデータが有効であるためには、それが「現在の実システムを反映したもの」でなければなりません。実際の変更を反映していないような設計段階の青写真であったり、棚の上でほこりをかぶっているような資料であっては役に立ちません。

データの互換性が損なわれるという問題は、モバイルの導入に限ったことではありません。しかし、モバイル向けのサブデータを扱うようになれば、この問題に対処できていない組織では、一気にこれが顕在化する恐れがあります。

この落とし穴にはまらないようにするには

データの非互換性を避けるための解決策は、メタデータ ディクショナリを作成し、関係する部門からアクセスできるようにすることです。複数の開発プロジェクトで共通したデータ ドメインを使用することにより、具体的なフィールド型を用いてメタデータの定義を引き継ぐことができます（たとえば Name は 50 文字であるなど）。しかもドメインに変更があった場合でも、その変更を自動的に他のデータベースに反映させることができます。

論理モデルにドメインを作成したら、物理データベースのフィールドの定義にもそれらを使用していかなければなりません。InterBase（マルチデバイス対応の組み込み可能かつスケーラブルなリレーショナルデータベース）では、チェック制約も含んだドメインをサポートしているため、そのドメインの許容値に関するビジネスロジックが一貫して適用されます。

データディクショナリは、複数のプロジェクトチームからアクセスできるように公開し、容易に検索できるようにしておく必要があります。格納するフィールドやデータオブジェクトに関するビジネスナレッジについても、データ ディクショナリで管理しておくべきです。これらの情報をただドキュメントに記載しておくのではなく、ER/Studio TeamServer のようなツールを使用して管理すれば、容易に検索可能なデータディクショナリを構築でき、オンラインポータルや他のシステムと連携できる REST API を通じて、開発者、データ利用者、アーキテクト、管理者などが豊富なコンテキスト情報を閲覧できるようにできます。

このようなデータディクショナリがあれば、モバイル化のための開発プロジェクトは効率化できます。長期的に管理可能な一貫性のあるアーキテクチャ情報が可視化されるため、モバイルアプリで利用するデータに関して確実な情報を参照できるようになり、データの扱いに関する間違いがなくなります。

落とし穴 3：ローカルデータストレージを使用してしない

企業がモバイルデバイスを導入し従業員に利用させる主な目的は、生産性の向上と現場の従業員がより多くの能力を獲得できるようにすることです。いくつかの業務においては、たとえセキュリティ上の懸念があるとはいえ、業務で使用するデータをデバイスに保存すること、つまりローカルデータストレージを用いることは不可欠です。

現実的な観点からいえば、ライブ接続が必要なタスクはほとんどありません。たとえば、予約システムであれば、空きがあるかどうかを調べるためにライブデータフィードが必要になりますが、それ以外の部分では、オフラインデータ処理機能があれば十分である場合が多いでしょう。オフライン処理ではデータのプッシュとプルが絶えず行われるということがないので、その方が処理は高速です。もちろんデータコストも少なくなりますが、最も重要なのは、常にデータへのアクセスが可能であることです。

たとえば、営業担当者がお客様のオフィスを訪問し注文を受けようとしています。しかし、モバイルデバイスをネットワークに接続するための電波がつながりません。打ち合わせでは、前回の使用量に基づいて次の注文額を決めようということになっていましたので、これでは打ち合わせの目標を達成できません。注文を受けるには、あらためて過去の使用量データを参照して資料を作り、再訪問しなければならないでしょう。しかし、モバイルデバイスにローカル データが保存されていれば、この営業担当者は、たとえ接続できない環境であっても、お客様先で業務を完了できたことでしょう。

モバイル環境では、常にネットワークアクセスができるとは限らないため、オフライン環境でどのように生産性を落とさないかという配慮が必要になります。実際の利用シーンを想定しないで、安定したオフィスのネットワーク環境でモバイルアプリの仕様を決めてしまうと、実際には使えないシステムをリリースしてしまうことになります。

この落とし穴にはまらないようにするには

ローカルデータキャッシュ機能は、オフライン環境や貧弱なネットワーク環境でアプリの生産性を落とさない重要な技術です。これがあれば、データコストも削減でき、操作性や機能性も向上します。

レプリケーション機能が用意されていない場合には、変更しようとしているデータを捕捉するためのトリガをデータテーブルに設定することで、リモートでデータ損失を最小限に抑え、信頼性を高めることができます。これにより、データの整合性を管理しデータの変更を確実にログに記録してメインデータベースへ反映させるための開発者の作業が軽減されます。さらに、データベース全体ではなく差分だけが送信されるため、データの使用量とコストも削減できます。

落とし穴 4：モバイルデータストレージがデータガバナンスや開発のベストプラクティスに合致していないため作業量やリスクが増大する

従来のエンタープライズソフトウェアアーキテクチャは、サーバーシステムとデスクトップシステムによって構成されているのが一般的です。そして、主要なエンドユーザープラットフォーム 1 つだけを対象としている場合には、そのデータストレージの管理は比較的容易でした。しかし、モバイル化プロジェクトにおいては、複数プラットフォームに対応する必要があるだけでなく、Android のようにデバイスベンダーの実装によって異なるケースもあり、さまざまな問題が発生する恐れがあります。クライアントプラットフォームに用意されているデータストレージ機能やデータ暗号化機能に依存したアーキテクチャを採用している場合には、特に注意が必要です。

データガバナンスとソフトウェア開発に関するベストプラクティス、たとえば、PIA（Personal Impact Assessments）や ITIL（Information Technology Infrastructure Library）においては、あらかじめリスクを特定する、あるいは絶え間なく着手されるサービス改善の間にリスクを特定することで、アプリケーションのライフサイクル全体を通してリスクに対処し管理することが目的として挙げられています。

さまざまなデバイスを扱う場合のベストプラクティスと、ソフトウェアをタイムリーに提供したいという組織の要求のバランスを取るため、開発プロセスでは、開発ライフサイクル全体を通してクロスプラットフォームデータベースサポートのメリットを活用しています。選択したデータベースが、開発環境のプラットフォームとターゲットデバイスプラットフォームとで同等の機能が用意されていないと、プロジェクトリスクが増大してしまいます。そして、開発、テスト、配置、変更要求にかかる時間も多くなり、本質的なリスクが増大します。BYOD や CYOD の普及により、複数のプラットフォームを統一的にサポートしないデータベースでは、開発チームやテストチームが対処しなければならない多様性はますます増大してしまうのです。

「データ管理者」は、データ利用ポリシーとその実行/適用において中心的な役割を果たさなければなりません。データの可読性は、データのセキュリティになくてはならない部分なので、実際にはデータ層で扱うべきです。データ可読性（暗号化の実装を含む）に関するポリシーを開発者がコードを書いて管理するのは多くの場合誤りです。開発者にセキュリティ実装の管理を任せると、長期的にはミスが発生しがちで、不慮のデータ漏洩のリスクが高くなる傾向があります。変更管理もはるかに危険性が高くなり、複数のエントリポイントに同じセキュリティを実装しなければならない場合に間違いが発生する可能性が高くなります。アプリケーションに（たとえ短期間の保存であったとしても）常にデータの保存が必要で、そのデータに個人を直接または間接に特定できる情報が含まれている場合、データ可読性の管理は特に重要になります。よくある過ちは、データ管理者権限を解除したり特定しないことです。これについては、「落とし穴 5」で詳しく述べます。

この落とし穴にはまらないようにするには

モバイルプラットフォームにおけるデータベースの選択肢は、従来の PC プラットフォームをターゲットとした場合より限られています。デバイス能力の範囲内で動作可能な軽量なメモリ使用量のデータベース エンジンを用意しそれを複数デバイス向けに提供するには技術的な課題があり、さらに外部ライブラリの使用に関して一部のベンダーから制限事項が課せられているためです。限られた選択肢の中で多くのハードウェアベンダーがオープンソースのデータベース管理システム「SQLite」を同梱しています。しかし、SQLite は、ここで述べているベストプラクティスを実装する手段とはなりえません。SQLite には、暗号化が組み込まれておらず外部のアルゴリズムに依存しています。また、データ層ではなくソフトウェア層でのデータセキュリティに対応しなければなりません。したがって、ベストプラクティスを取り入れながら、データストレージに関する BYOD や CYOD の課題に取り組むには、さらに詳しい調査が必要になってしまいます。

複数プラットフォームをサポートした InterBase のような組み込み可能なデータベースを選択すれば、プラットフォーム間でデータベースの可搬性が確保でき、データの可読性ポリシーが実装されたデータ層によって、アプリケーション開発ライフサイクル全体を通してデータ管理に関連するリスクを大幅に軽減できます。これにより開発者は、セキュリティの問題ではなく UI やパフォーマンスの要件に専念できるようになります。これはまた、アウトソースリソースへのデータの移動に関する問題の解決にも役立ちます。

データの可読性ポリシーをデータ層内に実装する場合、データへのアクセスの許可と取り消しのためのセキュリティログインを別途使用して、（InterBase の SYSDSO ログインのように）データセキュリティをデータアクセス セキュリティから必ず切り離す必要があります。これは非常に重要で、ロールベースの認証と組み合わせて行われるのが理想です。これを一度データ層で行うことで、たとえ複数のプラットフォーム上に異なる言語でコーディングしたとしても、誰がどのデータを読み取れるかについてのデータポリシーは既に実装され、いつでも機能する状態になっています。これにより、コードの共通化と問題箇所が限定されることによる単純化が可能となり、開発コストとリスクを、全体的にも、変更要求があったときにも軽減することができます。

ストアドプロシージャを使ってビジネスロジックをデータベースに組み込むことができる、SQL92 に完全準拠したデータベースを活用すれば、一度テストすればどこでも使える「Test Once, Use Everywhere」が可能となり、効率化を促進できます。これにより、テスト済みのロジックを配布でき、データ層でのテストの必要性を大幅に軽減できます。その結果、あらゆるプラットフォームで市場投入までの時間を短縮し、そのコストも削減できるようになります。

セキュリティの観点からは、複数のプラットフォームにわたる共通の暗号化プロセスが必要です。詳細については、「落とし穴 5」を参照してください。

落とし穴 5：セキュリティと暗号化を付加機能と捉え、結果的に法的措置を受けたり、顧客を失う危険を冒している

セキュリティは、モバイルの世界だけでなく、どのような組織でも、アプリケーションデータについての重大な関心事です。ただし、モバイル環境ではデータ セキュリティの問題が深刻化しています。実際、多くの人々は、アプリケーションの出荷先となる地理的地域や場所に関するデータ保護法を常に意識しているわけではありません（その法律は、たとえば米国では州ごとに異なる可能性があります）。簡単にいうと、個人の特定に使用できるデータは何であれセキュリティ漏洩のおそれがあり、256 bit AES 強度暗号化によって保護すべきです（それが推奨されている場合もあれば、法律で決まっている場合もあります）。

安全でないデータはデータ漏洩のおそれがあり、法的措置や罰金を受けることになる可能性があります。しかし、現実的には、データ漏洩のコストは罰金よりも高くつきます。企業はそのような漏洩事件を起こしたあと、通常、顧客層の 3 ～ 4% を失うからです。信用調査や顧客をつなぎ止めるための予定外のディスカウントや保証など、関連するコストもさらに発生します。経営陣への影響もあります。経営陣には最終的な責任があるため、法的措置を受けるおそれがあります。

この落とし穴にはまらないようにするには

保護は最初から始めなければならない

セキュリティは、データベースの検討、開発、リリースからモバイルでの実行、管理、廃棄に至るまで、製品のライフサイクル全体を通して確立しておかなければなりません。最初から暗号化を使用しなければ、安全でない休眠データがあることになります。アプリケーション ライフサイクルのあらゆる時点で、データ損失のおそれがあるのです。

そのような事件が起こるのを何度目にしたことでしょうか。ある開発者がデータのコピーを渡され、プロトタイプアプリケーションの作成を開始します。彼は、それを自分の USB メモリに保存し、仕事に戻りますが、USB メモリからデータを削除するのを忘れたままタクシーに乗り、USB メモリをなくしてしまいます。これと似たような事件が米国であり、最終的に 170 万ドルの罰金を科せられました。同様に、移動中に携帯電話やタブレットをなくしたり盗まれたりして、データをリモートで削除できなかったり、従業員がオフィスに戻るまでデバイスがなくなったことが報告されないといったトラブルが何度発生したことでしょうか。

安全なファイルにする唯一の方法は、暗号化を使用すると共に明確なデータアクセスポリシーに従うことです。デバイスにパスワードを設定しておけば十分保護されていると考えるのは、大いなる誤解です。

ICO によって記述されたとおりに PIA（Personal Impact Assessments：個人影響評価）を作成しておくと、保護が必要な可能性がある箇所やリスクを特定し管理するのに役立つツールとなります。このトピックはこのホワイトペーパーの範囲を越えていますが、ICO では、有用な無料ガイドをオンラインで公開しています。

データ管理者に暗号化とアクセスの権限を与える

製品のライフサイクル全体を通したデータ管理者の役割はきわめて重要ですが、しばしば見過ごされたり、過小評価されがちです。データ管理者の責務には、組織で収集、保存、表示、共有するデータの範囲を定義することが含まれています。また、データ管理者には、組織がデータ利用ポリシーに必ず従うようにする最終的な責任があります。

データストレージは、データレコードの追加前に適切なアクセス権を設定して暗号化する必要があります。ある企業では、特定のスタッフが従業員のリストとその詳細情報にアクセスできるようになっていました。そのデータの 1 つが給与情報だとしたら、人事担当者だけがそのデータを参照できるようにしておかなければなりません。そのため、データ管理者はこの条件をデータ層に適用して、権限を持つ人だけが問題のデータの参照、検索、編集を行える（開発チームでさえアクセスを拒否される）ようにする必要があります。そのために、データ管理者は、企業のポリシーで規定されたとおりにデータを参照する権限をデータ層に設定する必要があります。これは、企業の管理下で行われ、ユーザー認証でサポートされる必要があります。

開発者は暗号化の実装を担当してはならない

開発者は、データ管理者の望みのものを実装してはいけません。このデータを表示するコードを開発者が忘れたり、その中にバグがあったりしたら、どうなるでしょうか。セキュリティの処理はデータ層で行われる必要があり、データが制限されている場合は、データを収集してもデフォルト値が返されるようになっていなければなりません。こうして、たとえアプリケーションが不適切に使用されても、データの安全は確保されるのです。

データ ポリシーを機能仕様に組み込むことは避ける

理由が何であれ（法律上の理由、業務上の理由、その他）、データポリシーは定期的に変わります。したがって、絶対に必要な場合やはっきりとした業務上の理由がある場合を除き、データ ポリシーをアプリケーションのコアロジックに組み込まないでください。繰り返しますが、データポリシーはデータ管理者がデータ層に実装しなければならないものです。したがって、データ層に課せられた制限事項がアプリケーションの機能に影響を及ぼさないことがきわめて重要です。これはテストの役割です。データを抽出する SQL 文を機能仕様で決定する場合には、避けられない理由がない限り、接続しているユーザーに依存したクエリーを使わないことが重要です。これは、アプリケーションが将来さまざまな場面で使用されることを想定する中、開発サイクルにおけるリスクを管理し、予期しない動作を引き起こさないようにするのに役立ちます。さらに、アプリケーションのサポートコストも最小限に抑えることができ、開発工程の単純化によって市場投入の時間短縮も可能です。

まとめ

エンタープライズアプリケーション開発は IT の世界ではかなり成熟した分野で、多くの企業がベストプラクティスを持っています。モバイル化でさまざまな課題が新たに生じますが、適切なデータベースエンジンを選択することで、このベストプラクティスを維持し、エンタープライズデータをモバイル分野にも自然と拡張できるようになります。

テストに関連するコストの管理、統合とデータ漏洩に伴うリスクの軽減、データ ポリシーの確実な順守を実現するには、テストスコープを限定することが重要です。これは言うのは簡単ですが、BYOD や CYOD ポリシーの中で実現するのは難しい課題です。これを管理する最も簡単な方法は、さまざまな構成のさまざまなプラットフォームにおけるセキュリティ設定とデータベースオプションのばらつきを避け、ベストプラクティスに準拠できる特定の組み込み可能データベース（すべてのプラットフォームで同じ動作をするもの）を使用することです。

開発に対する副作用を引き起こすことなく、データ管理者やデータ セキュリティ チームがデータアクセスを管理できるデータベース／データ層を選ぶことで、データ管理者の要件を仕様書に記載することができるようになります。その要件は、システム全体に対して有効となるため、製品のライフサイクル全体を通して安全な配置の恩恵を受けることができます。

InterBase は、暗号化サポート、マルチプラットフォーム対応、軽量な組み込みデータベース機能といった点で、上記の要件をカバーしています。InterBase だけでなく、メタデータ ガバナンスとそのデータのリアルタイム共有には、ER/Studio や ER/Studio Team Server といったツールも重要な役割を果たします。

執筆者について

Stephen Ball 氏は、英国や欧州諸国で 10 年以上にわたり、Hilton、American Express、Fitness First、Virgin Active などのさまざまな一流企業と協力して商業目的で開発チームを率いてきました。同氏は公認 IT プロフェッショナルであり、上級テクニカル セールス コンサルタント（RAD 担当）と InterBase のアソシエイト プロダクト マネージャーを務めています。InterBase は、同氏がその経歴全体を通して商業的に使用してきた製品です。EMEA 各国で定期的に講演を行っており、Twitter またはブログで連絡を取ることができます。

Twitter： @DelphiABall
ブログ： http://blogs.embarcadero.com/stephenball

参考資料およびリンク

データ保護に関する重要な定義

http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

データが格納されている可能性がある USB をなくした場合のコスト

http://www.infosecurity-magazine.com/view/26630/

データ漏洩のコストに関する報告書

https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

PIA 作成の手引き（ICO）

http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

ICO のブログ： Why encryption is important to data security（暗号化がデータ セキュリティにとって重要な理由）

http://ico.org.uk/news/blog/2013/why-encryption-is-important-to-data-security

このホワイトペーパーで言及されているエンバカデロ製品の詳細については、以下を参照してください。

ER/Studio： http://www.embarcadero.com/jp/products/er-studio
InterBase： http://www.embarcadero.com/jp/products/interbase

エンバカデロ・テクノロジーズは、1993 年にデータベースツールベンダーとして設立され、2008 年にボーランドの開発ツール部門「CodeGear」との合併によって、アプリケーション開発者とデータベース技術者が多様な環境でソフトウェアアプリケーションを設計、構築、実行するためのツールを提供する最大規模の独立系ツールベンダーとなりました。米国企業の総収入ランキング「フォーチュン 100」のうち 90 以上の企業と、世界で 300 万以上のコミュニティが、エンバカデロの Delphi®、C++Builder®といった CodeGear™製品や ER/Studio®、DBArtisan®、RapidSQL®をはじめとする DatabaseGear™製品を採用し、生産性の向上と革新的なソフトウェア開発を実現しています。エンバカデロ・テクノロジーズは、サンフランシスコに本社を置き、世界各国に支社を展開しています。詳細は、www.embarcadero.com/jp をご覧ください。