WHITE PAPER

モバイル・データのセキュリティ

はじめに

ノートPCやPDAなどのモバイル機器を使用するようになると、ビジネスに必要な情報へのアクセスがどこからでも可能になります。また、モバイル性を強化することで、LANのファイアウォールの境界を越えたデータのやりとりも可能になります。しかし、モバイル・デバイスを使用して企業のセキュアな環境の外部からアクセス制限のある重要なデータにアクセスする従業員が増えるに従って、重要なデータのアクセスや格納に使用するモバイル・デバイスの管理やセキュリティ強化方法を検討するセキュリティ戦略が必要になってきます。

このホワイトペーパーでは、モバイル・データを保護するための手順を設計・実装する際に考慮すべき点、特に、データ伝送中の傍受、ユーザの認証、データに対する不正アクセス、デバイスの紛失などのセキュリティ問題について説明します。また、セキュリティ戦略において、これらの問題にどう対処していくかについても説明します。

セキュリティとは、リスクを最小限にすることです。またセキュリティ・ソリューションとは、システムの脆弱部分の特定、処理の実行、データの保護を指します。iAnywhere Solutions のモバイル・データ・ソリューションは、下記の製品を中心にモバイルデータを保護するためのセキュリティ・インフラストラクチャを備えています。

SQL Anywhere Studio は、モバイル、組み込み、ワークグループのデータベース・アプリケーションのための、一連のテクノロジであり、パーミッション管理やユーザ認証機能、データ・ファイルの強力な暗号化、クライアント／サーバ通信の強力な暗号化などをフル装備しています。

Manage Anywhere Studio は、デスクトップPC、ノートPC、モバイル機器用のアプリケーションやハードウェアを安全に中央から管理するための完全なソリューションです。

e-BUSINESS ANYWHERE

目次

はじめに……表紙

目次 3

モバイル・データのセキュリティ 5

セキュリティ手順の実装 5

モバイル・データのセキュリティ問題の解決 7

データ伝送の保護 7

SQL Anywhere Studio でのデータ伝送の保護 7

Manage Anywhere Studio におけるデータ伝送保護 9

データ伝送のセキュリティに関するその他の問題 9

不正ユーザからの保護 9

SQL Anywhere Studio でのユーザの認証 10

Palm Computing Platform 上における Ultra Light ユーザ認証 10

Manage Anywhere Studio におけるユーザ認証 10

データへの不正アクセスの保護 11

データへの不正アクセスの防止 11

デバイス管理ソフトウェアを使用したデータへの不正アクセスの防止 12

紛失したデバイス上のデータの保護 13

デバイスに永続的に格納されているデータの保護 13

Adaptive Server Anywhere データベースの暗号化 13

Ultra Light データベースの暗号化 14

その他の手段 15

常時実行中のアプリケーションの保護 15

結論 16

付録 A: iAnywhere Solutions 製品について 17

付録 B: セキュリティに関するコンセプト 18

法的注意 23

モバイル・データのセキュリティ

今日では、携帯電話や PDA、ノートPC、その他の携帯端末の普及により、情報へのアクセスはどこからでもたいへん便利になりました。しかしながら、一方でノートPCやその他の携帯端末を企業の万全なセキュリティ環境の外に毎日持ち出すモバイルワーカーが増加したことで、これらのデバイスでの機密情報の不正使用の可能性、ファイアウォール外からの企業ネットワークへのアクセスの可能性、これらのデバイスの紛失や盗難の可能性などから考えうる潜在的なセキュリティ・リスクから、大切なデータを保護するための対策をとる必要性が高まっています。

アクセス権をもつすべてのユーザが必要なときにいつでもデータを利用できるようにすることで、データの価値というものはより高まります。また、情報へのアクセスにモバイル機器を使用して社外でデータを利用することで、ユーザの生産性は簡単に高められるという利点があります。しかしながら、モバイル・コンピューティングでは、公共のネットワークを使用して機密データを交換する必要性がある上、無線ネットワークでは、データが傍受されるというリスクもあります。また、モバイル・コンピューティングを使用している場合、企業情報にアクセスしている端末を特定するのは従来の有線ネットワーク経由よりも困難です。

iAnywhere Solutions は、このような問題をふまえ、データがどこにあってもモバイル・データを保護するためのセキュリティ・インフラストラクチャを備えたモバイル・データ・ソリューションを提供しています。

セキュリティ手順の実装

モバイル・データのセキュリティについて考えてみても、完璧なソリューションは存在しません。セキュリティとは、リスクを軽減することであり、排除することではありません。

データを保護するセキュリティ手順を確立するにあたって、考慮すべき問題がいくつかあります。回答は組織によって異なりますが、ニーズを満たす最適なセキュリティ対策は何かを理解する上で役立ちます。

解決しようとしているのはどのようなセキュリティ問題か？

モバイル・データでよく発生する問題には次の 4 つがあります。

- データ伝送の傍受
- ユーザ認証
- データへの不正アクセス
- デバイスの紛失

セキュリティ・システムの脆弱点を見つけ対処することが重要で、iAnywhere Solutions は、この4 つすべての問題に対してセキュリティ・ソリューションを提供しています。

セキュリティ問題をどのように解決するか？

脆弱点の対処には、デバイス上のデータの暗号化、データ通信の暗号化、デバイスのパスワード保護、ユーザ・ログイン・メカニズムの組み込み、デバイス・セキュリティ・ポリシーの実装などが考えられます。

実装とインフラストラクチャにかかる費用はどのくらいか？　確立されたセキュリティ手順に従った場合にかかる費用はどのくらいか？

費用を検討する際は、セキュリティ・ポリシーの実装にかかる費用とセキュリティ侵害のリスクと比較します。ここでいうリスクとは、保護対象のデータの値だけでなく、顧客からの信頼など無形のものも含まれます。つまりセキュリティ侵害が発生すると、顧客からの信頼が低下する可能性があるからです。

もう１点考慮すべきなのは、セキュリティの追加によって増加するオーバーヘッドです。たとえば、暗号化を追加するとパフォーマンスが低下することがあり、データ・ストリームを暗号化するとネットワーク経由で伝送する情報の量は増加してしまいます。

ユーザがセキュリティ手順に従うのは困難なのか？

手順に実際に従うユーザのことを考えてみると、ソリューション自体が面倒な場合、ユーザはそれを避ける方法を見つけようとします。たとえば、パスワード入力を頻繁に行わなければならない場合は、煩わしくなってパスワードを保存する方法を探そうとするかもしれません。同様に、パスワードのルールが複雑な場合 (英語の単語は使わず、大文字小文字、数字を混在させるなど) は、パスワードを覚えるのが困難になります。いずれの場合にも、ユーザはパスワードの保存方法を見つけようとする可能性があります。パスワードを書き留めたり保存した状態でデバイスが盗難に遭うよりは、単純で記憶できるパスワードを使用した方がはるかに安全です。

なぜデータが貴重なのか、なぜ特別なセキュリティ手順が実装されているのかをユーザに教育することで、確立されたセキュリティ手順に従うことがなぜ重要なのか理解してもらうのに役立ちます。

さらに、もう 1点考慮すべき重要点として、すべての形式でデータが保護されているかどうかです。例えば暗号化され、パスワードで保護されているデータベースがあるとします。そしてそのデータベース内のデータを、レポートの作成や表計算ソフトへのエクスポートにも使用しているとします。データベース内ではデータを保護するためにさまざまなセキュリティ手段が導入されていても、そのデータは別のフォームでアクセス可能になります。これが脆弱点の一例です。

モバイル・データのセキュリティ問題の解決

ここで、モバイル・データのセキュリティの 4 つの問題点であるデータ伝送の傍受、ユーザの認証、データへの不正アクセス、デバイスの紛失を、それぞれの解決策と合わせて見ていきましょう。iAnywhere Solutions は、データベース、電子メール、シンクライアント・アプリケーションのどこにデータがある場合でも、モバイル・デバイスやアクセス対象のデータの保護に役立つさまざまな製品を提供しています。

以下の項目で説明する iAnywhere Solutions 製品の詳細については、17 ページの「付録 A: iAnywhere Solutions 製品の説明」を参照してください。

データ伝送の保護

データの転送中は、開始から終了までセキュリティを確実にする必要があります。データが傍受される可能性のある場所は、シンクライアント、ブラウザベースのアプリケーション、電子メール、音声、データの同期、クライアント／サーバ通信、メッセージや警告など、多数あります。

セキュアなデータ伝送には次の機能があります。

- 機密性：通信の機密性を保ちます。
- 整合性：データを見ることができるかどうかにかかわらず、誰にもデータは変更できないようにする必要があります。
- 繰り返し不可：ストリームのレコードは、サーバに再送した場合は使用できないようにする必要があります。たとえば、金融取引の場合などは、トランザクションを再び実行できないようにする必要があります。
- 認証：通信相手が誰か必ず認識できるようにして、中間人物による攻撃を回避します。エンタープライズ・システムに接続しているクライアントが、正しいサーバと通信していることが認識でき、また、許可されているクライアントのみがサーバと通信していることも確認する必要があります。

データを保護するためには、リモート・デバイスから企業のファイアウォールの内側まで、end-to-end でデータが暗号化されていることを確実にする必要があります。

SQL Anywhere Studio でのデータ伝送の保護

SQL Anywhere Studio は、データの同期とクライアント／サーバ通信の両方に関して トランスポート・レイヤ・セキュリティ (TLS) を提供しています。トランスポート・レイヤ・セキュリティとは、セキュア接続を確立するプロトコルです。

トランスポート・レイヤ・セキュリティは、アタッカーに傍受される可能性のある公共または私設のネットワークを使用して通信を行わなければならない場合に重要です。またトランスポート・レイヤ・セキュリティを使用すると、クライアント・アプリケーションはサーバの ID を確認できます。そしてクライアントは、信頼できるサーバのみと通信できます。

トランスポート・レイヤ・セキュリティの詳細については、19 ページの「通信アーキテクチャ」を参照してください。

Adaptive Server Anywhere 8.0 では、クライアント／サーバ通信が保護するために、トランスポート・レイヤ・セキュリティを使用しています。 (図 1 参照)。

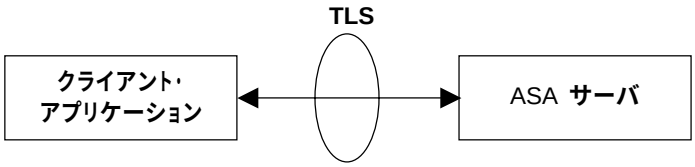

図 1: トランスポート・レイヤ・セキュリティとクライアント／サーバ通信

Mobile Link 同期では、Mobile Link 同期サーバと Adaptive Server Anywhere または Ultra Light クライアント・データベースとの間を同期データ・ストリームが送信されるときに、トランスポート・レイヤ・セキュリティを使用して、同期データ・ストリームの機密性と整合性を保護しています (図 2 参照)。

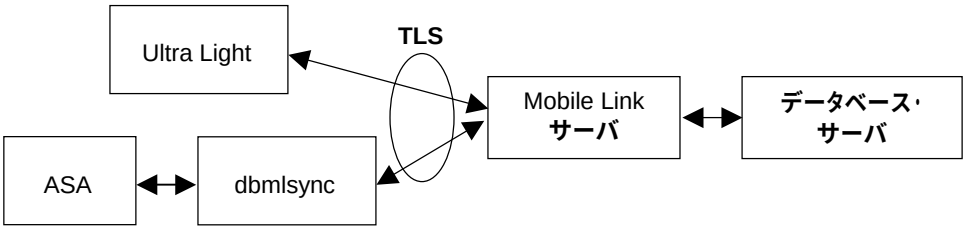

図 2: トランスポート・レイヤ・セキュリティとデータ同期

トランスポート・レイヤ・セキュリティは、デジタル証明書を利用して実装します。異なるタイプの証明書を使用し、SQL Anywhere Studio に含まれているツールを用いてさまざまな方法で証明書設定することにより、各種のセキュリティ目的を達成できます。

トランスポート・レイヤ・セキュリティは、Certicom 暗号化テクノロジとデジタル証明書を使用して実装します。このパブリック・キー暗号テクノロジでは、楕円曲線暗号方式を使用しており、トランスポート・レイヤ・セキュリティを呼び出すと、クライアントとサーバの間で送信されるすべてのメッセージが 128 ビットの暗号方式を使用して暗号化されます。

一旦証明書を作成してしまえば、Adaptive Server Anywhere クライアント／サーバ通信や Mobile Link 同期にこの証明書を使用できます。

この証明書を使用して Mobile Link 同期サーバを起動するには、暗号方式、証明書名、証明書のパスワードを、Mobile Link 同期サーバのコマンド・ラインに含めます。Adaptive Server Anywhere クライアントのパブリック証明書を指定するには、dbmlsync コマンド・ラインで指定します。Ultra Light クライアントのパブリック証明書を指定するには、Ultra Light アナライザ実行時に証明書を信頼するように指定します。

Adaptive Server Anywhere クライアント／サーバ通信に関しては、Adaptive Server Anywhere サーバを起動するときに、サーバ証明書を指定します。サーバのコマンド・ラインで強力な暗号化を使用する場

合は、サーバに対するすべての接続で TLS ハンドシェイクを実行します。このハンドシェイクはごまかしがきかず、Certicom 暗号化によって、サーバに危害を加える可能性のある無効なパケットは廃棄されます。クライアント側では、接続文字列内に暗号化パラメータを指定します。

トランスポート・レイヤ・セキュリティとデジタル証明書の詳細については、以下を参照してください。

- 19 ページの「付録 B: セキュリティ概念 」。
- SQL Anywhere Studio バージョン 8 を使用している場合は、『MobiLink Synchronization User's Guide』の「第 13 章 Transport-Layer Security」および『Adaptive Server Anywhere Database Administration Guide』の「第 13 章 Keeping Your Data Secure」の「Encrypting client/server communications」を参照してください。
- SQL Anywhere Studio バージョン 7 を使用している場合は、『Replication and Synchronization Guide』の「第 3 章 Synchronization Basics」の「Transport-layer security」を参照してください。
- 次のサイトにある『MobiLink transport-layer security and certificates』ホワイトペーパー http://my.sybase.com/detail?id=1009621。

Manage Anywhere Studio におけるデータ伝送保護

Manage Anywhere Studio には、HTTPS (HTTP over SSL 接続) を使用したリモート・クライアントと Manage Anywhere サーバ間の通信リンクを提供するインターネットベース・アーキテクチャが含まれており、Manage Anywhere サーバとリモート・クライアント間の通信はすべて暗号化されます。

データ伝送のセキュリティに関するその他の問題

多くのセキュリティ制御の責任は、電話会社、ブラウザ・プロバイダ、電子メール・プロバイダなどのサード・パーティにあります。電話会社だけが対応可能なセキュリティ問題の一例として、WAP ギャップがあります。WAP は、PDA や携帯電話で使用できる、シンクライアント Web ブラウザの 1 つの形式です。WAP/WML とインターネット／HTTP ではセキュリティ標準が異なるため、WAP ゲートウェイでは、データが復号化されて再度暗号化されます。この結果、一定の期間データが復号化された状態になります。WAP 2.0 標準では、転送中データを完全に暗号化できるよう標準のインターネット・セキュリティ・プロトコルを提供し、この問題を解決しています。

携帯電話や回線電話の通信でデータが傍受されるリスクもあります。デジタル通信はアナログ通信に比べて解読が困難とはいうものの、たとえ暗号化してもデータが安全ではない場合もあります。たとえば、売り上げ取引をすべて暗号化して転送しても、その取引について営業担当者が電話で話し合えば、データは安全とは言えません。

不正ユーザからの保護

確実に許可されているクライアントだけがサーバに接続でき、クライアントが正しいサーバに接続している必要がありますが、ハンドシェイク・プロトコルが使用できないため、メッセージ・システムでデータ伝送に正しいエンティティが関連していることを確認するのは、さらに困難です。

また、どのクライアントが何が可能なのか定義する必要があります。アプリケーションによって、特定の権利やパーミッションはユーザ・ベースで設定されています。

SQL Anywhere Studio でのユーザの認証

SQL Anywhere Studio は、ユーザを認証するために、ユーザ ID とパスワードを使用します。

- Adaptive Server Anywhere データベースに接続するときは、ユーザ ID とパスワードが必要です。データベース管理者またはアプリケーション開発者は、パスワードに最低文字数を設定できます。

- Adaptive Server Anywhere では、ユーザが不適切な情報にアクセスできないように、完全なユーザ・パーミッション管理機能を備えています。パーミッションは DBA によって、テーブルごと、カラムごと、プロシージャごと、ビューごとのいずれかで付与できます。

  また、パーミッションはグループに対して割り当てることもできます。ユーザにグループのメンバシップが割り当てられている場合は、グループ・メンバシップに従って一連のパーミッションが付与されます。

- Mobile Link クライアントが Mobile Link 同期サーバに接続するとき、クライアント (Ultra Light または Adaptive Server Anywhere) はユーザ ID とパスワードが要求されます。サーバはこの情報を使用してクライアントを識別します。

Palm Computing Platform 上における Ultra Light ユーザ認証

Ultra Light アプリケーションは通常、データベースに接続されたままになります。Ultra Light アプリケーションを開発している場合は、ユーザがアプリケーションを起動するたびにユーザの認証を行うように選択できますが、これを行うには、PilotMain ルーチンを使用してユーザとパスワードの情報のためのプロンプトを組み込む必要があります。デバイスを紛失した場合や盗難に遭った場合に備えて、アプリケーションを切り替えるときにログ・イン・プロンプトを表示すると、確実にユーザ ID とパスワードを知っているユーザだけがアプリケーションにアクセスできます。その他に可能な方法としては、使用中でないアプリケーションをユーザが保護できるメニュー項目を作成することなどがあります。

Manage Anywhere Studio におけるユーザ認証

Manage Anywhere Studio では、SQL Anywhere データベースを設定データベースとして使用して、ハードウェアやソフトウェアに関するデータ、送信済みのパッケージに関するログ情報、Manage Anywhere Studio の設定、セキュリティ設定など、さまざまな情報を格納します。設定データベースはユーザには表示されず、管理者のみが使用できます。Oracle データベースや Microsoft SQL Server データベースを設定データベースとして使用することもできます。

Manage Anywhere サーバは、リモート・クライアントで実行するファイルやコマンドから成るタスク・パッケージを使用しますが、このタスク・パッケージは、ソフトウェア、更新、アップグレードを複数のリモート・クライアントに配布する際に使用できます。また、特定の設定をリモート・デバイスに適用するイメージ・パッケージも送信できます。Manage Anywhere の自己回復テクノロジは、イメージの拡張機能です。ユーザがファイルの削除などの変更を行い、リモート・デバイス上の設定がイメージに一致しなくなると、Manage Anywhere Studio はファイルをリストアしてリモート・デバイス上でイメージを実行します。

タスク・パッケージはパスワードで保護できます。パッケージをパスワードで保護することで、パスワードを知っているユーザだけがパッケージを変更でき、パッケージを変更できるユーザを制限することで、クライアントに送信される情報の信頼性を保つことができます。さらに、情報を隠しておくために、パッケージは難読化されます。しかし、タスク・パッケージには、強力な暗号化方法はありません。

次の SQL Anywhere Studio セキュリティ・システムを使用すると、Manage Anywhere Studio でセキュリティの実装、ユーザの認証ができます。

- 管理者を認証するための、ユーザ ID とパスワード： リモート管理コンソールに接続するには、有効な SQL Anywhere ユーザ ID とパスワードが必要です。

- 管理者が Web コンソールやリモート管理コンソールにアクセスするための、適切なパーミッション： これらのコンソールへのアクセスは、Windows NT ベースの認証ポリシーを使用して制御します。また、管理者が使用できる機能のレベルを制限することもできます。

- IT 部門が Live Support を使用してユーザのマシンを制御し、ユーザの問題を診断および解決する際の、パスワード： Live Support 中のセキュリティは、ランダムに生成して暗号化したパスワードをシステムごとに確立するか、無人クライアントへのアクセスをセキュリティ保護するためのパスワードを手動で定義することによって保証されます。リモート・エージェントは、Live Support セッションが始まるまではデバイスにロードされず、これによって侵入者のアクセスが防止されます。

データへの不正アクセスの保護

場合によってはモバイル・デバイス上のサービスが、データの要求に応答することがあります。これらのサービスを不正に利用すると、デバイスのコンテンツにアクセスできてしまいます。例えばトロイの木馬をデバイス上に潜伏させ、デバイスが公開されたらトロイの木馬を使って接続を行い、データを送出させることもあり得ます。実際、この場合トロイの木馬はサービスになり得ます。現時点では、ハンドヘルド・デバイスに対するトロイの木馬はそれほど多くありませんが、インターネットに接続しているノートPCにおいて深刻な問題です。

デバイスは、データベース・サーバ、インターネット・サーバ、FTP サーバなどのインタフェースを使用して攻撃される可能性もあります。例えばCode Red ウイルスは、感染した Web サーバを経由して蔓延しました。今後無認可ソフトウェアの有無をモニタリングしたり、デバイスのシステム設定が正しいことを確認したり、オペレーティング・システムのセキュリティ更新を適用することが必要になります。

無線 LAN で使用するデバイスはファイアウォール外のものとみなし、それ相応に処理する必要があります。また、無線 LAN は、社内LANにアクセスする場合、仮想私設網 (VPN) を使用してファイアウォールの外側に設定します。

データへの不正アクセスの防止

ノートPCでは、BlackICE や ZoneAlarm などのパーソナル・ファイアウォールを使用して、データへの不正アクセスの防止に役立てることができます。またデバイス管理ソフトウェアも、中央からのセキュリティ・ポリシー実施が可能になるため、不正アクセス問題の解決に役立ちます。

デバイス管理ソフトウェアを使用したデータへの不正アクセスの防止

Manage Anywhere Studio は、次のようなタスクを実行することによってセキュリティ・ポリシーを簡単に実施できる、モバイル管理ソフトウェア・ソリューションです。

- ウィルス・スキャナへの更新の適用またはインストールとアップグレードの自動化
- 自己回復テクノロジを使用したシステム設定の保護および実施
- ハードウェアおよびソフトウェアのトラッキング

コーポレートアンチウイルス規定の自動実施

Manage Anywhere Studio では、ウイルスの修正や更新を中央から配布することにより、マシンを保護することができます。Manage Anywhere Studio を使用すると、インストールされているのがどのベンダーのアンチウイルスソフトにかかわらず、マシン上でアンチウイルス・ソフトウェアや定義ファイルの更新を実施できます。ユーザには事実上透過的なバックアップやウイルス保護スキャンをスケジュールし、自動的に実行するパッケージを設計することもできます。

そのため万が一ウイルスが社内のマシンやデバイスに侵入した場合でも、Manage Anywhere Studio が、感染しているマシンにウイルスの修正やパッチを直ちに適用し、ウイルスを駆除してそれ以上の損害を防ぎます。

またManage Anywhere の Live Support リモート・コントロール機能を使用して問題を診断し、ウイルスが原因の損害を修復することもできます。

自己回復テクノロジを使用したオペレーティング・システムおよびアプリケーションの設定

ユーザがオペレーティング・システムやアプリケーションの設定を変更する際に、マシンが不正アクセスの危機にさらされる場合もあります。そのような場合にも、Manage Anywhere Studio に含まれている状態管理およびイメージング・テクノロジを使用すると、マシンやインストールされているアプリケーションを修復できます。たとえば、Web ブラウザ内で特定のセキュリティ設定が必要な場合は、Manage Anywhere Studio を使用して、クライアント・マシンで実施する設定をそのまま含むパッケージを構築することができます。このパッケージをクライアントで実行すると、クライアントの設定は必要な設定に戻ります。これにより、セキュリティ規定をユーザが回避しようとしても、強制的に実施することができます。

中央からのセキュリティ・パッチの自動的な配布

ウイルスに関する問題は、多くの場合オペレーティング・システムまたはブラウザ設定の更新をコンピュータやデバイスに実施することで修正できます。Manage Anywhere Studio を使用すると、動的グループ検索を実行して、特定のユーザ・グループのニーズに合わせてパッケージをカスタマイズできるため、修正が必要なすべてのマシンにソフトウェアやオペレーティング・システムの更新を配布できます。ソフトウェアの配布とインストールは、中央の 1 個所から自動的に実行できます。

インストールされているソフトウェアのトラッキング

Manage Anywhere Studio を使用すると、すべてのクライアントマシンに関するインベントリ・データを収集できます。このデータを使用して、特定のソフトウェア・アプリケーションをインストールしているユーザの数や、各マシンで使用されているオペレーティング・システムの種類などの情報をまとめることができます。この情報は、ソフトウェア・ライセンスをトラッキングするときにも便利です。

Manage Anywhere Studio を使用すると、無認可のソフトウェアのスキャン、必要なソフトウェアが削除された場合の再インストール、サーバ上の設定に完全に一致するようにクライアントの設定をリストアする処理なども可能です。

標準外のソフトウェアが存在する場合、組織のセキュリティが危険にさらされる可能性があります。インターネットでのファイル共有を可能にするソフトウェア・アプリケーションは、企業の機密データに対するアクセス・ポイントを提供するおそれがあるため、組織のセキュリティにとって危険です。標準外のソフトウェアがインストールされているコンピュータまたはデバイスを検出したら、ユーザに通知した上で該当するプログラムを自動的にアンインストールするパッケージを設計し、送信することができます。

Manage Anywhere Studio は、セキュリティ・ポリシーの運用作業に伴うユーザの負担を軽減します。また、セキュリティが危険にさらされるのを防ぐために適用されているセキュリティ・ポリシーを回避することをさらに難しくすることもできます。

紛失したデバイス上のデータの保護

モバイル・デバイスのセキュリティに関するもう 1 つの考慮点は、紛失または盗難に遭ったデバイス上のデータをいかに保護するかです。対処が必要なものには、デバイスに永続的に格納されているデータと、常時実行されているアプリケーションの 2 点があります。

デバイスに永続的に格納されているデータの保護

モバイル・デバイスに格納されているデータが外部に漏れるのを防ぐための対策として、機密データの暗号化、ファイル・システム全体の暗号化 (表計算ソフトなど、データベース外でデータを使用している場合に有用) の 2 つがあります。

ハード・ディスク、永続的メモリ、取り外し可能なフラッシュ・カード (デバイスに取り付けられているかどうかにかかわらず) に格納されているデータも保護する必要があります。

iAnywhere Solutions の製品を使用すると、Adaptive Server Anywhere または Ultra Light のデータベース・ファイルを暗号化することも含めて、いくつかの方法で紛失したデバイス上のデータを保護することができます。例えばManage Anywhere Studio を使用すると、紛失したデバイス上のアクセス権に制限のあるデータを抹消する自己破壊ポリシーを実施したりすることができます。

Adaptive Server Anywhere データベースの暗号化

Adaptive Server Anywhere にはデータベース・ファイルの強力な暗号化を実装するために、2 つのアル

ゴリズムが選ばれています。1 つ目の Rijndael は、ブロック暗号化アルゴリズムで、米国の国立標準技術研究所 (National Institute of Standards and Technology、NIST) によって、ブロック暗号方式の新たな Advanced Encryption Standard (AES) として選ばれたもので、Adaptive Server Anywhere にデータベース・ファイルの強力な暗号化を実装するために使用されているもう 1 つのアルゴリズムは、Cacio が開発した MDSR です。ここでいう強力な暗号化という用語は、これらのテクノロジを Adaptive Server Anywhere の新旧バージョンに含まれている単純な暗号化と比較して説明するために使用しています。強力な暗号化とは、解読が非常に困難であることを意味しますが、強力な暗号化は、パフォーマンスにも大きな影響を与えます。

AES アルゴリズムまたは MDSR アルゴリズムのいずれかを使用するデータベース・ファイル暗号化テクノロジを採用すると、データベース・ファイルをキー (パスワード) なしで操作することができなくなります。

データベースを暗号化すると、メインのデータベース・ファイル、すべての dbspace ファイル、すべてのテンポラリ・ファイル、すべてのトランザクション・ログ・ファイルに含まれる情報にスクランブルがかけられ、ディスク・ユーティリティを使用してファイルを見ても解読できません。そのため強力な暗号化を使用すると、パフォーマンスに影響がでます。一方パフォーマンスへの影響がごくわずかの、強度の低い暗号化もあります。

強力な暗号化を使用するときは、キーをモバイル・デバイスに格納しないでください。これは、鍵を部屋の中に置いたままドアをロックしてしまうことと同じです。ただし、キーを紛失すると、データは完全にアクセス不能になります。また、キーでは大文字小文字が区別され、正しく入力しなければデータベースにアクセスできないことにも注意してください。キーは、データベースを起動したいときやデータベース上でユーティリティを使用したいときに必要です。

セキュリティをより強化するために、ユーザが暗号化キーを入力できるダイアログ・ボックスを表示するようデータベース・サーバに対して指示するオプションが使用できます。このオプションが必要なのは、暗号化キーは通常のテキストでマシンに入力するべきではないからです。

データベースの暗号化の状態を変更する場合は、データベースを再構築します。強力に暗号化されたデータベースのアンロードまたは再構築を行うには、キーがわからなければできません。

Ultra Light データベースの暗号化

Ultra Light データベース・ファイルは、AES アルゴリズムで強力に暗号化できます。

Ultra Light データベースは、初めて接続を行おうとするときに作成されます。Ultra Light データベースを暗号化するには、接続時に暗号化キーを指定すると、指定したキーを使用してデータベースが暗号化されます。その後の接続では、指定したキーが暗号化キーに対して検証され、キーが一致する場合にのみ接続が成功します。データベースに対する接続が複数ある場合は、最初の接続、つまりデータベースを起動する接続に対してのみ暗号化キーが必要です。その後データベースに接続するときは、暗号化キーは無視されます。

Ultra Light データベースを強力に暗号化するには、ULEnableStrongEncryption 関数を呼び出してから db_init() 関数を呼び出してデータベースを開きます。暗号化キーは、ULChangeEncryptionKey 関数を使用して変更できます。

強力な暗号化は、パフォーマンスに影響を与えます。Ultra Light データベースでは、データベースの難読化も使用できます。難読化を使用すると、パフォーマンスに大きな影響はありませんが、強力な暗号化ほど完璧に保護することはできません。

Palm Computing Platform 上では、アプリケーションを起動するたびに暗号化キーが必要となりますが、ULSaveEncryptionKey、ULRetrieveEncryptionKey、ULClearEncryptionKey の各関数を使用すると、キーを毎回指定する必要のないアプリケーションを作成できます。

暗号化キーは、HotSync conduit の同期でも必要です。conduit 設定ダイアログを使用すると HotSync マシンにキーを保存できますが、キーは難読化されるだけであるため、安全ではありません。

その他の手段

万が一デバイスを紛失した場合や盗難に遭った場合は、Manage Anywhere Studio を使用して、サーバから制御する自己破壊ポリシーを実施することにより、アクセス権に制限のあるデータを保護することができます。また、紛失または盗難に遭ったと認識されているデバイスがサーバに接続すると、そのデバイス上のアクセス権に制限のあるデータを破壊するパッケージをサーバから送信させることもできます。

常時実行中のアプリケーションの保護

常時実行されているアプリケーションにも、セキュリティ上のリスクにさらされています。データ格納域が保護されている場合でも、アプリケーションにキャッシュ・データが含まれている場合は、データが不正なユーザに見られているリスクがあります。アプリケーションのメモリに格納されているデータは、アクセスが比較的困難なであるものの、それでもやはり見られるおそれがあります。

アプリケーションから送信した更新が画面に表示される場合、そこに含まれるデータは、デバイスをオンにすれば誰でも見ることができてしまいます。

常にオンになっているアプリケーションを保護するためには、パスワード保護されたタイムアウトをアプリケーションに導入することができます。繰り返しになりますが、パスワードはデバイスには格納しないことが重要です。さもなくば、デバイスにアクセスできれば誰でもデータにアクセスできてしまうおそれがあります。またアプリケーションには、ユーザがパスワード保護機能を無効にしていないことを確認するコードも含めることができます。

結論

セキュリティとは、リスクを最小限にすることであり、リスクを排除することではありません。セキュリティ・ポリシーを確立するには、今解決しようとしているセキュリティ問題が何なのか特定する必要があります。iAnywhere Solutions は、多岐に渡るモバイル・データ・ソリューションを提供しており、以下のデータ保護に役立てることができます。

伝送データの保護

SQL Anywhere Studio は、TLS/SSL を使用して、データの同期およびクライアント／サーバ通信を保護しています。サーバ認証は、デジタル証明書を使用して行われます。Manage Anywhere Studio では、サーバとリモート・クライアント間で送信されるすべてのパッケージを暗号化しています。

ユーザ認証

SQL Anywhere Studio、Manage Anywhere Studio ではいずれも、ユーザ ID とパスワードを使用して、アクセス権に制限のある情報に対するアクセスが制限されています。さらに、Adaptive Server Anywhere では、ユーザが不適切な情報にアクセスできないようにするユーザ・パーミッションも使用できます。

データへの不正アクセス防止

モバイル・ノートPCの保護にはファイアウォールを使用してください。デバイス管理ソフトウェアも、データへの不正アクセスの防止に役立ちます。Manage Anywhere Studio を使用すると、ウイルス修正やパッチの適用、マシンの設定の強制実行、無認可のソフトウェアの削除を行うパッケージを送信し、リモート・クライアントを保護することが可能です。

紛失デバイス上のデータ保護

Adaptive Server Anywhere および Ultra Light のデータベースは暗号化が可能です。暗号化すると、データベースに含まれる情報にはスクランブルがかけられ、暗号化キーなしではデータベースを操作できなくなりますが、Manage Anywhere Studio には、紛失したデバイス上のデータを破壊できるメカニズムが含まれています。

モバイル・データのセキュリティ強化には多くの異なる局面があることがわかります。たった 1 つですべてを解決できる魔法のような解決法はなく、包括的なセキュリティ・インフラストラクチャが必要になります。リスクを最小限にするということは、システムの脆弱点を特定し、リスクや費用を考慮に入れた上で適切な解決法を設計し、モバイル・データを保護することです。

付録 A: iAnywhere Solutions 製品について

SQL Anywhere Studio

SQL Anywhere Studio は、分散 e-Business ソリューションの迅速な開発と展開を可能にするデータベースとエンタープライズ同期を提供する包括的なパッケージです。ワークグループ、ノートPC、ハンドヘルド・デバイス、インテリジェント機器、組み込みアプリケーション用に最適化されている SQL Anywhere Studio を使用することで、企業の e-Business の範囲をビジネス・トランザクションが発生するすべての場所に拡大することができます。

SQL Anywhere Studio の詳細については、http://www.sybase.com/detail?id=1016232 を参照してください。

Manage Anywhere Studio

Manage Anywhere Studio は、すべてのデスクトップPC、ノートPC、サーバ、ハンドヘルド・デバイスを、単一の管理コンソールを使用してどこからでも管理できる、完全なオールインワンのソリューションです。リモート・システム上のソフトウェア、データ、ファイルを配布、インストール、管理するための、簡単かつ効果的なソリューションです。Manage Anywhere Studio を使用すると、中央の IT サポート・チームは、ワークフォース全体への配布を単一の管理コンソールから管理できます。Manage Anywhere Studio は業界標準に基づいて構築されており、その使いやすく信頼性の高い、スケーラブルなプラットフォームは、各社のネットワークや設計に合わせてカスタマイズできます。

Manage Anywhere Studio の詳細については、
http://www.sybase.com/products/mobilewireless/manageanywherestudio を参照してください。

付録 B: セキュリティに関するコンセプト

SQL Anywhere Studio、Manage Anywhere Studio がいかにデータ保護に役立つかのか良く理解していただくために、ここでは、通信アーキテクチャ、セキュリティ・プロトコル、パブリック・キー暗号方式、その他の、iAnywhere Solutions 製品にセキュリティ機能を実装するときに使用するコンポーネントについて説明します。

通信アーキテクチャ

通信スタックは、信頼性の高いデータ伝送に必要なさまざまな機能を分離してしまいます。プロトコル・スタックの各レイヤは、上位のレイヤから渡された情報を単にデータとして処理し、もう一方のコンピュータ上にある同等のレイヤによる識別、解読と同じ方法で、そのデータにラベルを付けます。データを実際にワイヤや電波に乗せる役割を持つのは物理レイヤだけであり、その他すべてのレイヤは、エラーの検出、修正、暗号化など、細かく定義された機能レベルを提供します。図 3 に、典型的な通信スタックと、セキュリティの強化がいかにアーキテクチャに影響を及ぼすか示します。

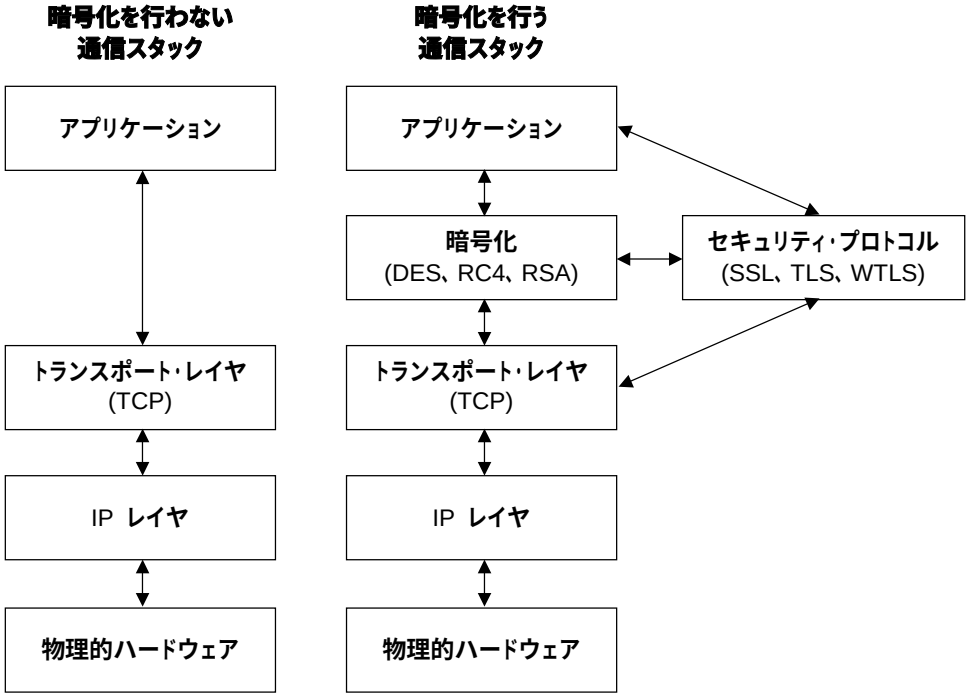

図 3: 通信スタック

あるアプリケーションで送信するデータを暗号化する必要がある場合、安全な接続を確立するためのセキュリティ・プロトコルが必要です。セキュリティ・プロトコルとは、暗号化された通信セッションを安全に確立するために必要なセキュリティ・パラメータのネゴシエーション（ハンドシェイクとも言う）です。通常、セキュリティ・プロトコルでは認証も行われます。セキュリティ・プロトコルの例として、トランスポート・レイヤ・セキュリティ（TLS）やセキュア・ソケット・レイヤ（SSL）があります。

パブリック・キー暗号方式

パブリック・キー暗号方式では、互いに関連付けられている非常に大きい 2 つの数値を組み合わせて機能する、数学的なシステムを利用しています。これらの数値はキーと呼ばれ、特定のプロパティを持ちます。キーはそれぞれ、情報の暗号化に使用できます。暗号化したメッセージは、対応するキーを使用しなければ復号化できません。

一方のキーであるパブリック・キーは、パブリック・フォーラムで発行され、パブリック・キーの所有者に送信する情報の暗号化に使用できます。この所有者は、プライベート・キーという第 2 のキーを非公開にしておきます。

パブリック・キーで暗号化したメッセージは、プライベート・キーでのみ復号化できます。パブリック・キーは公開されているため、メッセージの作成は誰でもできますが、そのメッセージを読むことができるのは、プライベート・キーの所有者だけです。また、パブリック・キーを知っていれば、プライベート・キーで暗号化されたメッセージを復号化できます。このように、プライベート・キーを使用して作成したメッセージが対応するパブリック・キーで復号化できることを確認することで、プライベート・キーの所有者は、プライベート・キーを知っていることを「証明」できます。

プライベート・キーは、パブリック・キーから容易に推測できないようにすることが不可欠です。パブリック・キーからプライベート・キーを推測する難易度は、多くの場合、暗号方式の強度とパブリック・キーのサイズ (ビット数) に対応します。プライベート・キーのもう 1 つの性質として、推測が困難でなければならないという点があります。質の高いプライベート・キーを作成するには、本当に推測不可能な乱数データにする必要があります。SQL Anywhere Studio で提供されているツールは、新しいプライベート・キーを作成するときに、オペレーティング・システムから擬似乱数データを収集します。このデータは予測不可能であるため、相手方がキーの値を推測することはできません。

パブリック・キー暗号方式を使用するアルゴリズムには、RSA、Diffie-Hellman、楕円曲線暗号 (ECC) などがあります。

デジタル証明書

デジタル証明書とは、人物またはエンティティを識別し、その人物またはエンティティのパブリック・キーのコピーを含む電子ドキュメントです。各証明書にはパブリック・キーが含まれており、このパブリック・キーで情報を暗号化することで、相手方の人物またはエンティティと誰でも安全に通信することができます。デジタル証明書は、次の情報を含む、標準化されたファイル・フォーマットに準拠します。

1 証明書所有者の名前やアドレスなどの ID 情報

2 パブリック・キー

3 有効期限

4 証明書の修正を防ぐための 1 つまたは複数のデジタル化シグニチャ

デジタル化シグニチャ

デジタル化シグニチャを使用すると、ドキュメントが変更されたかどうか判断できます。デジタル化シグニチャは、証明書の所有者が本当にその人またはその会社であることを確認する目的でも使用できます。たとえば、ABC 社から VeriSign その他の認証局が署名した証明書が届いたとすると、その認証局が信頼できるものであれば、本物の ABC 社と通信していると確信できます。

デジタル化シグニチャは、ドキュメント情報から、あるいは証明書の場合は ID 情報とパブリック・キーから、メッセージ・ダイジェストという値を計算することによって作成される暗号操作です。デジタル化シグニチャは、証明書に署名する認証局のプライベート・キーを使用してダイジェストを暗号化することによって作成されます。

メッセージ・ダイジェストとは計算されたビット値であり、ドキュメントの一部に変更があった場合に変更されるように設計されています。ダイジェストは一方向のハッシュを使用して作成されます。そのハッシュは元のドキュメントよりもかなり小さいため、ハッシュからドキュメントを再構成することはできません。

証明書のユーザは全員、メッセージ・ダイジェストの計算に使用するアルゴリズムを知っています。正しい値はプライベート・キーで暗号化され、すべての証明書ユーザがメッセージ・ダイジェストの値を計算できるため、変更箇所を検出するには単純にメッセージ・ダイジェストの値を計算し、パブリック・キーを使用してドキュメント内の値を復号化します。値が異なれば、ドキュメントが変更されたことになります。

パブリック・キー・インフラストラクチャ

パブリック・キー・インフラストラクチャ (PKI) では、認証局が証明書を作成し、認証局のプライベート・キーを使用して署名します。パブリック・キーは配布されます。たとえば、使用しているブラウザにパブリック・キーが含まれている場合は、対応するプライベート・キーで署名された証明書を持つ相手から安全な通信を受け入れることができます。

ソフトウェアは、信憑性を検証する証明書をサーバから受け取りますが、ブラウザベースの接続では、サーバ側の証明書のみが提供されます。クライアントからサーバへは、証明書を提供する必要はありません。しかしID 情報には、クライアントによって明示的に検証された内容を含める必要があります。たとえば、ブラウザの場合は IP アドレスです。

完全な PKI システムには、クライアントがサーバの ID の検証に使用できるサーバ側の証明書のほかに、サーバがクライアントの ID を検証できる、クライアントに関連する証明書もあります。

PKI システムには、考慮が必要となる管理機能もあります。たとえば、証明書が必要なすべてのクライアントおよびサーバに対して証明書を取得する方法や、プライベート・キーが危険にさらされた場合にとるべき手順 (危険にさらされているすべての証明書の取り消しリストを準備するなど) などです。

対称キー暗号方式

対称キー暗号方式では、データの暗号化と復号化の両方に同じキーを使用します。この方法の方が、パ

ブリック・キー暗号方式よりも処理がかなり速くなります。

SSL では、通信をより効率的にするために、クライアントとサーバがもう 1 つのキーを承諾して交換し、対称キー暗号方式に切り替えます。対称型の暗号方式では、データをより効率的に暗号化および復号化できるため、クライアントとサーバはこのキーと暗号方式を使用して残りの通信を行います。

ストリーム暗号方式

ストリーム暗号方式を使用している場合、プレーン・テキストで XOR したキーから、連続したランダムなストリームが作成されます。一方で、受信側は同じランダムなストリームをキーから生成して作成し、暗号化されたテキストを XOR してプレーン・テキストを得ます。ストリーム暗号方式を使用するときは、キーを再利用しないでください。複数のメッセージを同じキーで暗号化すると、アタッカーに暗号を解読するための情報をより多く与えることになるためです。ストリーム暗号方式には、RC4 や SEAL などがあります。

SSL では、セッションの最初のハンドシェイク・ネゴシエーション中に新しい対称キーが生成されます。セッションの残りの部分は、ストリーム暗号方式の意味では連続したストリームです。

ブロック暗号方式

ブロック暗号方式を使用すると、データのブロックが、同じサイズの一見無関係と思われるデータのブロックに変形されます。アルゴリズムが少し入り組んでいて、複数のブロックを同じキーで暗号化しても追加情報が提供されない設計になっているため、同じブロック暗号方式を別のブロックでも再利用できます。ブロック暗号方式には、DES、Blowfish、Twofish、AES (Rijndael)、MDSR などがあります。

ブロック暗号方式は、セッションベースの通信で通常使用されるものではありません。メッセージベースの通信で、データベース・ファイルなど、1 個所でデータを暗号化する際に使用します。

SSL セキュリティ・プロトコル

SSL は、安全なデータ伝送のためのインターネット標準です。SSL を使用すると、SSL が有効なサーバと SSL が有効なクライアントが互いに認証し合い、暗号化された接続を確立することができます。TLS は、SSL の新しいバージョンです。

SSL でセキュア接続を確立するプロセスには、次の 2 つの要素があります。

- プロトコル・ネゴシエーションのためのハンドシェイク
- データ交換のためのメッセージング定義

ハンドシェイク中に、クライアントとサーバはパブリック・キー暗号方式を使用してアルゴリズムをネゴシエートし、情報を交換します。そして互いの ID を検証するために、証明書を交換します (サーバ認証モードでは、検証が必要な証明書はサーバのみにあります)。

データを送信する前に、最大 6 個のパケットが送信されます。ハンドシェイクの一環として、クライアントとサーバの両方からランダムなバイトが送信されます。このランダムなバイトは、対称キーの生成

に使用できるほか、セッションを確実にリプレイ不能にすることもできます。これは、同じサーバに対してストリームをリプレイすると別のランダムなバイトになるためです。対称キー情報の交換には、パブリック・キー・アルゴリズムを使用します。

対称キーは、交換後、クライアントとサーバの間を行き来するすべてのパケットの暗号化に使用されます。そして、パケットを暗号化していても、パケットを修正されるのは望ましくなく、交換されるパケットの修正を防ぐため、送信メッセージにはそれぞれ署名が付けられます。

法的注意

iAnywhere、iAnywhere Solutions、iAnywhere Solutions(ロゴ)、Adaptive Server、SQL Anywhereは iAnywhere Solutions, Inc.またはSybase,Inc.とその系列会社の米国または日本における登録商標または商標です。その他の商標はすべて各社に帰属します。

Mobile Linkの技術には、Certicom,Inc.より供給を受けたコンポーネントが含まれています。これらのコンポーネントは特許によって保護されています。

本書に記載された情報、助言、推奨、ソフトウェア、文書、データ、サービス、ロゴ、商標、図版、テキスト、写真、およびその他の資料(これらすべてを"資料"と総称する)は、iAnywhere Solutions,Inc.とその供給元に帰属し、著作権や商標の法律および国際条約によって保護されています。また、これらの資料はいずれも、iAnywhere Solutions,Inc.とその供給元の知的所有権の対象となるものであり、iAnywhere Solutions,Inc.とその供給元がこれらの権利のすべてを保有するものとします。

資料のいかなる部分も、iAnywhere Solutionsの知的所有権のライセンスを付与したり、既存のライセンス契約に修正を加えることを認めるものではないものとします。

資料は無保証で提供されるものであり、いかなる保証も行われません。IAnywhere Solutionsは、資料に関するすべての陳述と保証を明示的に拒否します。これには、商業性、特定の目的への整合性、非侵害性の黙示的な保証を無制限に含みます。

IAnywhere Solutionsは、資料自体の、または資料が依拠していると思われる内容、結果、正確性、適時性、完全性に関して、いかなる理由であろうと保証や陳述を行いません。Sybaseは、資料が途切れていないこと、誤りがないこと、いかなる欠陥も修正されていることに関して保証や陳述を行いません。ここでは、「iAnywhere Solutions」とは、iAnywhere Solutions, Inc.またはSybase,Inc.とその部門、子会社、継承者、および親会社と、その従業員、パートナー、社長、代理人、および代表者と、さらに資料を提供した第三者の情報元や提供者を表します。

＊本書は、米国iAnywhere Solutions社が作成・テストしたものを日本語に翻訳したものです。

アイエニウェア・ソリューションズ株式会社
http://www.ianywhere.jp

1020369