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

2011年6月

データベース・セキュリティ・コンソーシアム

目次

はじめに

現在、企業経営の手段において IT を活用していない企業は皆無に等しく、その重要性・IT 依存度は高まる一方となっている。またネット銀行やオンラインショッピング、SNS 事業などインターネット上での事業を主とし、店舗や工場などの不動産が実在しない前提でのビジネス形態もすでに当たり前になっている。

いっぽうサーバ処理能力の向上、ネットワーク帯域や記憶装置の大容量化、スマートデバイスの台頭、デジタル家電の普及など様々な要因が重なった結果、企業が抱えるデータ（情報）の量は増加の一方をたどっている。

近年認識されているように、情報は人、物、金に加えて第 4 の経営資源に位置づけられ、企業が競争力を創出するためになくてはならないものである。この経営資源を管理・活用するための代表的な IT インフラストラクチャはデータベースである。

しかし、価値の高い情報は売買されることにより経済的利益を生み出す側面も持っているため、それらの情報を含むデータを狙って不正行為を行う人間が後を絶たない。さらに、企業には個人情報などの管理責任もあり、データを盗むことで組織にダメージを与えたいと考える人間も現れていると考えられる。つまり、データベースは攻撃の標的にされる代表的存在でもある。したがってデータベースの管理策（リスクに対する対策）も重要なテーマであるのは周知の事実であるにもかかわらず、データベースを狙われたことによる情報漏えい事件や事故は減らず、むしろ増加傾向にあるという報告もある。

これらのことから、データベースとその内部に格納される情報が経営においてより中心的存在となる現在、データベースの管理策を再考する時期に来ているのではないだろうか。従来ファイア・ウォール、IDS/IPS、Web Application Firewall（WAF）等、いわゆる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。すでに「境界防御をしっかりしていたので、データベースに対する直接攻撃は想定外だった」というのは、言い訳にできない時代に突入しているのである。

企業が各種の情報を活用し、インターネットを経由したオンラインサービスで利益を生み出しつつ、同時に重要な機密情報を保護するためには、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。そこで本コンソーシアムでは、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。

本提言をきっかけとして、情報を格納するデータベースに関わるセキュリティ対策を見直し、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に役立てて頂ければ幸甚である。

1. オンラインサービスにおけるデータベースの保護と事業リスク

インターネットを経由して提供されるオンラインサービスにおいて、データベースは顧客情報・クレジットカード情報などの機密情報を格納する場所である。したがってデータベースに格納された情報が侵害を受ける（漏えいする、改ざんされる、破壊される等）と、多くの場合サービスそのものの提供に支障をきたし、一時的なサービス停止につながる。それに伴い、当該企業に生じる損害には次のようなものが考えられる。

1.1. 定量化しやすい直接的損害の例

① 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。その規模は企業によって異なるが、数億円～数十億円といった巨額になる場合もあり得る。

② また被害を受けたシステムについて、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ことが必要になるため、それらも直接的に必要となるコストである。（一般的な企業の情報システム部門では対応するノウハウを保有しないことが多いため専門家への相談と依頼が推奨される）

③ 個人情報の漏えいについては、個人（情報主体）に対する謝罪等の費用が必要になる。いくつかの事例では、一部のサービス無償提供、商品券の配布などを行っており、漏えい規模が大きくなると、謝罪費用が巨額となる可能性がある。

④ 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。これらは本来、事前に行っておくべき投資であったとも言えるが、後になって対策を講じる場合は事前に行った場合に比べて高い費用が必要になることが多い。

1.2. 定量化が難しい間接的損害の例

① 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）対応にかかる人件費が必要となる。これらを外部委託で行う場合はその金額が定量化できるが、内部人件費の場合はそれが見えにくくなる。しかし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は内部的にも確実に発生する。

② 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。（上場直後の企業で、サービス停止中の株価が大きく下落した事例は存在する）

③ 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。

具体的なリスクの定量化・可視化の方法などについては NPO 日本ネットワークセキュリティ協会（JNSA）被害調査ワーキンググループの成果物などをご参照頂きたい。[1]

2. データベースを襲う脅威

2.1. 想定される攻撃シナリオ

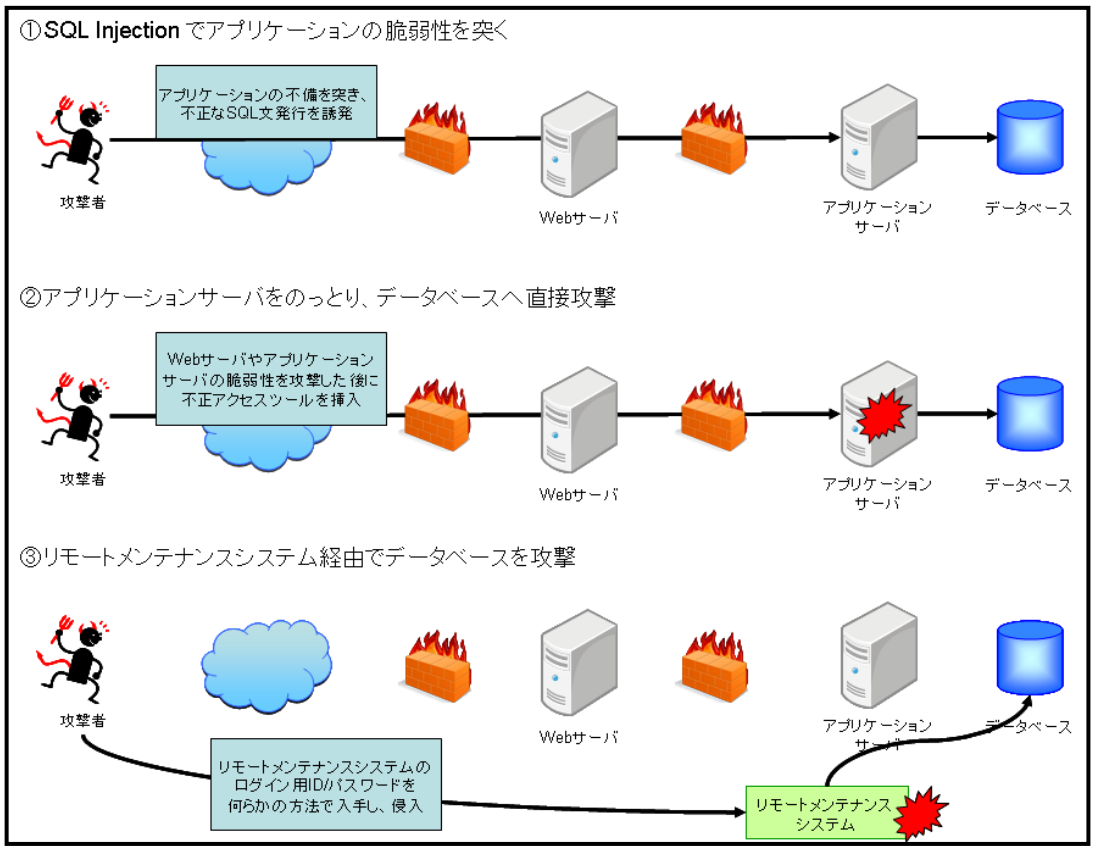
最近のシステムに対する攻撃手法を検証／想定した場合、主な攻撃シナリオは以下のようなパターンが考えられる。

① SQL Injection でアプリケーションの脆弱性を突く

② Web サーバまたはアプリケーションサーバの脆弱性を攻撃して乗っ取り、データベースへ直接攻撃を行う

③ リモートメンテナンスシステムなど内部システムからの侵入（境界防御を回避して背後から侵入する手法が増加している）

個々の手法に対する詳細は独立行政法人情報処理推進機構(IPA)やセキュリティ専門の企業による解説などを参考にして頂きたい。



データベースへの攻撃イメージ

[1] JNSA 成果物 http://www.jnsa.org/result/index.html

2.2. 最近の動向を踏まえて認識すべきこと

前述した攻撃手法自体は目新しいものではないが、最近の動向を踏まえると、以下の点を改めて認識すべきと考える。

① 攻撃技術の巧妙化と攻撃の容易化

最近のデータベースを狙った Web サーバやアプリケーションに対するサイバー攻撃は、

常に巧妙化されている。また、高度な攻撃ツールが簡単に入手可能になっており、技術的スキルが高くない人間でもサイバー攻撃が行えるようになっているため、サイバー攻撃の数自体も増加している。当然、データベースを狙う攻撃ツールも配布されており、サイバー攻撃は当たり前にやってくることを認識するべきである。

② 境界システム中心の防御手法の限界

Web サーバや Web アプリケーションなど境界システムに対する脆弱性対応は管理策として代表的なものであるが、それが効果的に機能しなくなっている。

現在のデータ量やトランザクション量では、システムを構成する Web サーバやアプリケーションサーバが数十台、場合によっては数百台の規模となり、セキュリティパッチ適用は長時間にわたる作業となる。また、アプリケーションに対する新機能の追加が多くなった結果、アプリケーション改修コストや頻度が上がる、またはビジネス上システムを停止できない等の事情から、脆弱性対応が間に合わないことがしばしばある。さらにゼロデイ攻撃[2]など、防御しにくい攻撃が増加していることも考慮する必要もある。

このような場合に境界システムに対する攻撃が成功するとデータベースへの攻撃が発生して情報漏えい等につながるため、データベース側での管理策が重要なものとなる。境界システムへの管理策が有効でない場合があること、データベース側での管理策が重要であることを認識するべきである。

③ データ量の増加速度

SNS 事業での Facebook, Twitter の記録的な成長速度に代表されるように、近年のインターネットを用いたサービス事業は急速に拡大する傾向にある。このとき、事業が抱えるデータ（情報）量も急速に増加した結果、気がついたときには莫大なデータを抱えているという状況が起こりうる。万一サイバー攻撃を受けた際の被害（データ漏えい件数）が甚大なものにならないように、現在のデータ量に注意を払いながら管理策を適用することが重要となる。

常にデータベースが管理する情報の量、質（機密性の高さ等）に注意し、現行のデータベースに対する管理策が適切か否かの検討、判断を行うべきである。

[2] ソフトウエアの脆弱性を修正するパッチが提供されるより前に、実際にその脆弱性を突いて攻撃が行われたり、悪用する不正プログラムが出現している状態

3. データベースに対する管理策を見直すための技術的提言

データベースを中心軸にすえた場合の管理策として、以下の点を見直すことを推奨する。

3.1. 不正アクセス検知の導入

不正アクセス検知は、データベースに対して不正なクエリが実行されたことを速やかに検知し、管理者への通知、不正アクセスの切断といった対処を行う仕組みである。これにより被害の規模を小さくすることが可能となる。

データベースの情報漏えいを例に挙げると、多くの場合、不正なクエリは通常アプリケーション経由では発行されないクエリを使って、機密データを保持した表へアクセスするものである。不正アクセス検知はいかに早く検知させるかが重要となる。事前に正しいアクセスと不正アクセスを定義し、ログをリアルタイムにモニタリングし、不正発見時のアクションを定義することで被害を最小限に抑えることができる。

3.2. 脆弱性管理の見直し

2.1.で述べたように、システム内の脆弱性を突いた攻撃によりサーバを乗っ取られ、そこを足がかりに情報を搾取する事例が増えている。この攻撃を防ぐためには、境界システムのみならず、バックエンドに控えたデータベースサーバにおいても OS、DBMS などに存在する脆弱性を減らす運用が必要と考える。DBMS についても常に最新のセキュリティ修正を含んだパッチを入手し、適用することを推奨する。

また、データベース構築時の初期設定に脆弱性がないか、今一度確認されることをお奨めする。初期構築の段階で散見される問題のある設定としては、デフォルト通信ポートの使用、不要なアカウントの作成、安易なパスワード管理（複雑でなく推測や総当たりが可能、開発環境と本番環境で同じものを使っている、等）などがある。

3.3. OS にまで攻撃の手が及んだ場合の対応

データベースサーバが不幸にして攻撃を受けても、データベース内の情報を漏えいさせないよう、データベースの暗号化とデータアクセスの権限分離を推奨する。データベースサーバ OS に不正アクセスを許してしまった場合（OS の root 権限を奪取された場合など）、次の 2 つの攻撃が予想される。

① データベース・ファイル、中間ファイルの盗難

② 管理者アクセス経由の機密データの漏えい

①について、データベースサーバ上の機密ファイルへの対応が必要である。具体的には、バッチの中間ファイルなど、データベース上に一時的におかれたファイルがある場合はその削除を徹底する。データベース・ファイルについては暗号化によって盗難行為を無害化する。

②については、すべての権限を持ったデータベース管理者アカウントでアクセスされた場合の

リスクである。これを回避するために、データベース管理者が機密データにアクセスできないようにするなど、データへのアクセス権限を分割することで管理者アクセスを許した場合でもリスクを低減することができる。

3.4. ログの保全管理見直し

ログは正確な被害状況の把握に欠かせないものである。ログを削除・改ざんされると被害状況を迅速・正確に報告できず、さらに企業の信用を失墜させる恐れがある。最近の攻撃手法から、ログ保全の観点で次の３点について見直しをお奨めする。

① ログは当該システム上とは別サーバに保管する
② データベース上のログ保持期間は最低限にする
③ ログを保管するサーバのアクセス制御（改ざん防止、暗号化等）を実装する

3.5. 機密データの最小化

機密データ（情報）の保護には多大なコストが発生する。しかしながら、アプリケーションの開発には、本番環境を想定したデータが必要であり、開発環境に対してもセキュリティを担保する必要がある。データのマスキングやトークナイゼーションといった処理を施し、機密データ自体を無害化することで効率的なセキュリティ対策を施すことができる。

3.6 各種コンプライアンス対応の管理策の見直し

企業は、自社の運用しているデータベースが、現在、国内外で　施行されている、各種の法制度や基準に対して、どの程度適合　しているのか、を正しく理解していることが重要である。 国内における個人情報保護法（及びガイドライン）、不正競争　防止法、内部統制報告制度、FISC、海外における、SOX、HIPPA、　PCIDSS などに関わる多くのコンプライアンス要件を満たすことが　求められ、対応している企業も多いと思うが、今一度データベースに　関連するリスクに着目して、対策の実行／見直しを行うことを推奨する。

他の技術的対策については本コンソーシアムが公開している『データベースセキュリティガイドライン 第 2.0 版』[3]などをご参照頂きたい。

[3] 『データベースセキュリティガイドライン 第 2.0 版』http://www.db-security.org/report.html

4. よりよい情報保護の実現にむけて

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

情報セキュリティを経営レベルのリスク、課題として捉えるべきであるという議論は過去 10 年近くにわたって行われてきたところであるが、我が国においては未だその成果が十分に出ているとは言い難いのが現状である。その重要性は理解されているものの、具体的な方策は現場やそれに近い人々に任され、「係長セキュリティから社長セキュリティ」という変革が求められているところである。[4]

事業が始まった時点では多くの情報を保有していなかったとしても、その事業が拡大し、進化する過程で、保有し、処理する情報量は急激に膨張していることがある。同時にその情報の中には個人情報、クレジットカード情報等に代表される機密性の高い情報が含まれていることが多い。

特に個人情報やクレジットカード情報等は、ひとたび漏えいなどの事件が起きると、漏えいした情報を悪用した詐欺やプライバシー侵害などの二次被害を引き起こすことから、当該企業自らが被害者であるだけでなく、顧客、個人（情報主体）に対してはその法的・社会的な責任を負っている。また、適切な時期・方法による情報公開や伝達、監督官庁に対する報告などの広範な社会的説明責任があることも、広く理解されている。

このような状況を踏まえて、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[5]）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。

① 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。
② 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。
③ 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。
④ 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

一般的には経営者に対して詳細な技術的理解を求めるのは困難であり、それ自体は経営の本質ではないかも知れない。しかし、多くの企業において経営戦略を実現するためのインフラとして IT システムが不可欠なものになっている現在、経営資源として非常に重要な「情報」の入れ物、

---

[4] 林紘一郎「情報セキュリティ総合科学 第２号」~係長セキュリティから社長セキュリティへ：日本的経営と情報セキュリティ~2010 年 11 月、 http://www.iisec.ac.jp/proc/vol0002/iisec_proc_002_p001.pdf
[5] 経済産業省「情報セキュリティガバナンス」http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

いわば「金庫」に相当するのがデータベースであること、そして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を行うことがよりよい情報保護と、個人情報、クレジットカード情報などにまつ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と考えている。

以上

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