新たな情報通信技術戦略の策定に関するパブリックコメント

～ 情報セキュリティの観点から

April 8, 2010

高度情報通信ネットワーク社会推進戦略本部より発表された新たな情報通信技術戦略（IT 戦略）骨子（案）の中では、個人情報を含む様々な行政保有の情報の集約化と、インターネット経由でのアクセスを可能にするサービスについて検討が行われている。いずれの施策も、利用者の利便性を大きく向上し、行政サービスの効率化を図る上で非常に有益である一方で、行政保有情報の機密性や個人情報の保護の重要性を考慮すると、情報セキュリティの重要性について多くの課題と留意すべき点が含まれていると考える。

本パブリックコメントでは、秘匿性の高い情報を管理するシステムが、インターネットからのアクセスを許容する際に考慮すべきセキュリティ要件についてまとめ、情報通信技術戦略骨子の策定過程での検討課題として、議論が尽くされることを期待するものである。

株式会社 Imperva Japan

Contents

要旨 3

データセキュリティの現状と課題 4

インターネットからアクセスを受ける Web サイトが抱える脅威 4

脅威の中心は、ネットワークレベルからアプリケーションレベルへ 4

パスワードのみによる保護の限界 5

内部ユーザからの脅威にさらされるデータベース 6

民間で相次ぐ情報漏洩事件とその教訓 6

重点施策１４項目とデータセキュリティ上の課題 7

Ⅰ 国民本位の電子行政の実現 7

① 行政サービスのオンライン利用に伴うセキュリティ上の課題 7

② 行政保有の統計・調査情報の公開に伴うセキュリティ上の課題 7

③ 電子政府の共通基盤としての国民 ID 制度とセキュリティ上の課題 7

Ⅱ 地域の絆の再生 8

⑥ 医療情報の電子的管理・活用とセキュリティ上の課題 8

Ⅲ 新市場の創出 8

⑬ クラウドコンピューティングサービスの競争力確保とセキュリティ上の課題 8

データセキュリティに求められるセキュリティ要件 9

情報資産を保護する上で考慮すべきセキュリティ要件 9

Web アプリケーションの保護 9

IPS でアプリレベルの防御が十分でない根拠 9

脆弱性診断のみでは不十分なわけ 11

WAF を検討する上で考慮すべき点 12

データベースの保護 12

結言 14

参考文献 14

要旨

高度情報通信ネットワーク社会推進戦略本部より発表された新たな情報通信技術戦略（IT 戦略）骨子（案）の中では、個人情報を含む様々な行政保有の情報の集約化と、インターネット経由でのアクセスを可能にするサービスについて検討が行われている。いずれの施策も、利用者の利便性を大きく向上し、行政サービスの効率化を図る上で非常に有益である一方で、行政保有情報の機密性や個人情報の保護の重要性を考慮すると、情報セキュリティの重要性について多くの課題と留意すべき点が含まれていると考える。

本パブリックコメントでは、秘匿性の高い情報を管理するシステムが、インターネットからのアクセスを許容する際に考慮すべきセキュリティ要件についてまとめ、情報通信技術戦略骨子の重点施策のうち、それらを考慮すべき項目について明らかにする。

まず、「データセキュリティの現状と課題」の章では、インターネットから個人情報を含む機密情報へのアクセスを許容する際に、Web サイトが考慮すべき外部からの脅威と、情報資産を保存するデータベースに対する内部からの脅威について述べる。外部からの脅威については、昨今はアプリケーションレベルへの攻撃が増加しており、従来のファイアウォールや IPS では十分な保護が提供できない状況になってきていることを述べる。内部からの脅威では、内部犯行による情報漏洩事件が相次いでおり、有効な内部統制システムの確立が求められる状況が続いている点について述べる。

次に、「重点施策１４項目とセキュリティ上の課題」では、前章で明らかにした内外のセキュリティ上の脅威と関連する５つの施策、① 行政サービスのオンライン利用、② 行政保有の統計・調査情報の公開、③ 電子政府の共通基盤としての国民 ID 制度、⑥ 医療情報の電子的管理・活用、⑬ クラウドコンピューティングサービスの競争力確保について、考慮すべきセキュリティ上の課題について述べる。

最後に、「データセキュリティに求められるセキュリティ要件」の章では、行政保有の情報資産を保護する上で検討すべきセキュリティ基準について、外部からの攻撃を防ぐ Web アプリケーションへの保護と、内部犯行による情報漏洩を防ぐデータベースの保護について、どのような対策を考える必要があるかを整理する。

本パブリックコメントを元に、利便性やコスト削減の追及だけではなく、内外の安全上の脅威に対して、新しい情報システムが安全対策を十分検討され、安全・安心な仕組みが提案することを強く希望するものである。

データセキュリティの現状と課題

今日、インターネットを通じてやり取りされる情報の多くがWebサイト経由で行われており、Webサイトの背後では、多くの個人情報や、金融関連情報、クレジットカード情報などの情報資産を保存するデータベースシステムが稼働している。ユーザの利便性の向上が進む一方で、これら機密情報へのアクセスが容易になったために生じる多くのセキュリティ上の課題が発生しており、ボットネットや情報資産を摂取するハッキング活動の対象は、金銭的価値の高い情報が入手できる Web アプリケーションへと推移してきている。さらに、データベースについては、内部犯行による情報漏洩の脅威にさらされており、有効な内部統制の確立が急務である。

本章では、情報資産への主要な入口となっているWebサイトが抱える安全上の脅威と、重要資産を保存するコアとなるデータベースシステムの抱えるセキュリティ上の課題についてまとめる。

インターネットからアクセスを受ける Web サイトが抱える脅威

脅威の中心は、ネットワークレベルからアプリケーションレベルへ

インターネットからアクセスを受けるWebサイトは多くの脅威にさらされており、攻撃の傾向や洗練度は日々変化している。Web アプリケーションが、金融・証券や、E コマースなどに利用が拡大するのにともない、攻撃の中心もサーバやネットワーク機器の脆弱性をつくウィルス感染活動やサービス停止攻撃(DoS/DDoS)といったネットワークレベルの攻撃から、クライアントの Web ブラウザの脆弱性や、サーバの Web アプリケーションの脆弱性をつくアプリケーションレベルへと推移してきており、2008 年は SQL インジェクションによるサイト改ざん[1]、2009 年はガンブラーウィルスによるサイト改ざんが問題になった[2]。

SQL インジェクションは、マルウェアの感染コードの埋め込みや、マルウェア配布サイトへ誘導するリンクを埋め込む感染活動に使用されるほか、個人情報やクレジットカード情報の窃取など、金銭目的のハッキングに使用される攻撃である。日本国内では、サウンドハウス、ゴルフダイジェストオンライン、トレンドマイクロ等々、2008 年中に複数のサイトで被害が報告されおり、2010 年もモンベルのサイトでクレジットカード情報漏洩事件が発生するなど、攻撃トラフィック量の減少は見られるものの[2]、引き続き警戒の必要な脅威として存在している。

SQL インジェクションという攻撃手法については 2000 年前半にはすでに知られており、安全なコードの実装方法の啓蒙活動[3]、脆弱性診断ツールによる対策や、Web アプリケーション・ファイアウォール (WAF)による防御対策が進んできているものの、相変わらず被害や脆弱性の報告が発生している状況にある[4]。特に、SQL インジェクションを効果的に防止することのできる WAF については、導入が大きく進んでいる海外でも、Forrester 社の調査[5]にあるように 30%未満の導入にとどまっていることから、国内ではさらに普及レベルが低いと想定される。相次ぐ Web サイトからのクレジットカード情報漏えい事件を受けて、クレジットカード業界では WAF の導入を加盟店に推奨しているように[6]、個人情報を取り扱う公共関連のシステムでも、同様のセキュリティ標準を検討してゆくことが必要だと考える。

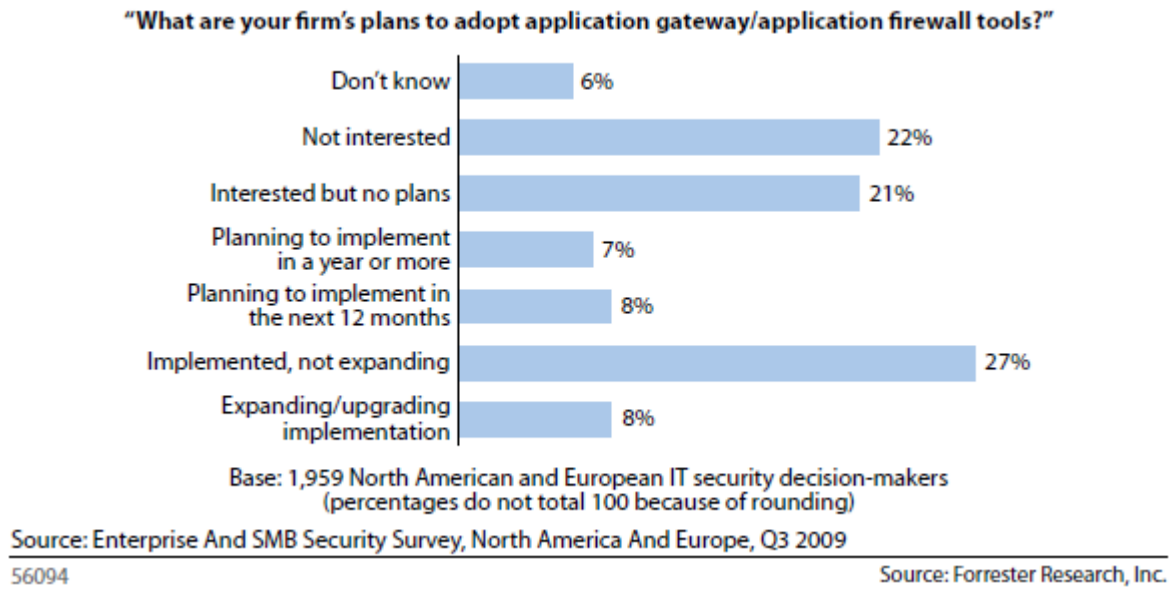

図 1 WAF 普及動向の調査結果 (Forrester [5])

パスワードのみによる保護の限界

インターネットからのアクセスにより、機密情報を取り扱うサイトは、その情報資産の重要度に合わせ様々なセキュリティ対策を盛り込んでいる。ボットネットなどのインターネット外部からの自動攻撃の多くは、様々な対策技術や運用プロセスを導入することで効果的に防止できるが、クライアント側の安全対策にセキュリティレベルが大きく左右されるものも多い。その一つがパスワードである。

ユーザが安易なパスワードを使用している場合、攻撃者に簡単に破られてしまい、個人情報の漏えいや内部からの攻撃などを引き起こす結果となる。以下は、2009 年に発生したアメリカの SNS サイト RockYou にて、ハッキングにより大量のパスワード情報が漏えいした事件をうけ、弊社が漏えいパスワードを調査した結果であり、多くのユーザが単純なパスワードを利用している状況が明らかになった。

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

図 2 漏洩パスワードの Top20 (Imperva 社調査[7])

本調査により判明した事実は、以下のとおりである。

- **30%のユーザが６文字以下のパスワードを使用**
- **50%のユーザは、氏名やスラングの単語、辞書に載っている単語、平凡なパスワード (連続した数字やキーボードの隣接した文字の組み合わせ等)を使用**

結果、多くのユーザが、ブルートフォース攻撃と呼ばれるサイバー攻撃の基本形態であるパスワード取得攻撃に対して、脆弱な状況に置かれていることが判明している。したがって、攻撃者にとって利用価値の高い行政保有の個人情報や医療関連情報を保有するシステムでは、ユーザが安全でないパスワードを利用することを前提とした対策が必要とされると考える。

内部ユーザからの脅威にさらされるデータベース

民間で相次ぐ情報漏洩事件とその教訓

2009 年は、内部犯行による個人情報漏洩事件が発生し、多額の金銭被害につながる事件が複数明らかとなった。

一つは、2009 年 5 月に明らかとなった三菱 UFJ 証券で発生した個人情報漏洩事件である。当時システム部の部長代理であった社員が、不正に取得した 148 万人の個人情報のうち約 5 万人分を売却した事件で、三菱 UFJ 証券はおわびとして顧客一人あたり一万円の商品券を配布した。最終的な損失は、逸失利益を含め約 70 億円と試算している。

もう一件は、2009 年 9 月に明らかとなったアリコジャパンからのクレジットカード情報漏洩事件である。こちらは、外部業務委託先の ID が不正使用され、32,359 件のクレジットカード情報が漏洩し、その一部で不正利用が発覚したことで事件が明るみに出た。アリコジャパンも三菱 UFJ 証券同様、クレジットカード情報の漏えいが確認された顧客に対し一人あたり一万円の商品券を、その他 11 万人に対して三千円の商品券を配布した。逸失利益を含めた最終的な損失額は 429 億円と試算されている[8]。

これら情報漏洩事件を発生させた企業では、情報漏洩のおわびに関わる損失も巨額に上るが、それ以上にブランドイメージの低下などに起因する逸失利益の影響が大きく、トラブルの損失計算式を特集した日経コンピュータ 3 月 3 日号では[8]、情報漏洩による企業価値の損失額を「トラブル報道日の企業価値×0.0225」と試算している。つまり、時価総額 100 億円規模の企業でも損失が 2 億円に及ぶことになり、内部犯行への対策が企業のリスク管理の重要な要素として浮上してきている。

過去に発生した情報漏洩事件を詳しく分析してみると、その多くは十分な監査システムが用意されておらず、不正な情報取得を監視できる状態になっていないことがわかる。また、情報資産を保有するデータベースに対するアクセス権限の管理が不十分で、不正に取得した ID や過剰なシステム権限の付与が適切に管理されていない例も散見される。日本では、これまで従業員のモラルが十分に高く、システムが性善説を前提に作られている傾向があり、職務分掌も不十分なケースが多い。昨今の経済不況に起因する経済的困窮者の出現や、コスト削減のための外部委託などにより、性悪説に基づいて強力な内部統制システムを築いてリスク管理を行うことが重要になりつつあるといえよう。

これは、公共システムについても同様のことが当てはまると考える。特に、行政保有の個人情報や医療関連情報がデータベース化された場合、情報漏洩が発生した場合の社会的影響度は、これまで発生した民間での情報漏洩と比較して非常に高いと考えられ、民間以上に内部統制およびリスク管理をシステム化して、内部犯行の発生を極限まで低下させる仕組みが必須であると考える。

重点施策１４項目とデータセキュリティ上の課題

本章では、高度情報通信ネットワーク社会推進戦略本部により発表された新たな情報通信技術戦略（IT 戦略）骨子（案）の重点施策 14 項目について、前章で明らかにしたデータセキュリティの観点から見えてくる課題に対し、検討を要する施策を列挙し、考慮すべき検討課題について述べる。

Ⅰ 国民本位の電子行政の実現

① 行政サービスのオンライン利用に伴うセキュリティ上の課題

住民票、戸籍の情報や各個人に関する行政保有情報の確認等をインターネット上で行う場合、前章で明らかにした Web ポータルに対するアプリケーションレベルの攻撃に対する備えが課題となり、また、オンラインでの利用を行う場合、情報が電子化されデータベースに蓄積されることから、データベースからの情報漏洩対策となる内部統制システムの整備が課題となる。

特に、公的個人認証サービスについては、前章で明らかにしたように、パスワードのみでの保護では不正利用のリスクを低減することができないため、パスワードのみに依拠しない公的 IC カードの普及を前提とするシステムの整備が望ましいと考える。

② 行政保有の統計・調査情報の公開に伴うセキュリティ上の課題

公開対象となるデータは、基本的に個人情報がわからない形に加工されている状態になっていると考えられるが、加工ミスや誤ってファイルを公開してしまう等の人為的ミスが入り込むことを想定すべきである。この場合、オンラインのシステムにて、個人情報の漏洩を検出かつ防止できるようなシステムの検討が必要と考える。

③ 電子政府の共通基盤としての国民 ID 制度とセキュリティ上の課題

国民 ID 制度の整備は、情報の電子化とオンライン利用を推進する上で必須となる課題である。一方で、すでに導入の進んでいる米国などで明らかなように、国民 ID は各種認証の場面で多く利用されることが想定され、ID 番号情報の保護が大きな課題となる。不正に入手した ID で容易に情報を入手できるようであれば、税、社会保障といったこれまで容易に入手できなかった情報に手が届くことになり、社会的影響は計り知れない。

したがって、国民 ID の検討を行う際は、情報漏洩に対する対策と、ID の漏洩が即個人情報漏洩につながらないような仕組みの検討が必要となると考える。

II 地域の絆の再生

⑥ 医療情報の電子的管理・活用とセキュリティ上の課題

医療情報の電子的管理や活用は、利便性向上の一方で、情報漏洩のリスクが大きい分野でもある。疾病情報は、漏洩した場合の不利益が大きく、従来の個人情報保護法以上に強力な保護が必要とされる分野と考える。米国では HIPPA により、医療従事者に対する個人情報の取り扱いについて強固な法令が課されており、日本でも医療情報の電子化にあたっては、個人情報漏洩を防止する施策が重要になると考えられる。

情報サービスの提供にあたっては、アプリケーションレベルの攻撃への対策、弱いパスワードが利用されることを前提とした認証の仕組みの整備、内部犯行による情報漏洩への対策、といったこれまで挙げた課題へのシステム的な対応は、十分に検討されるべきであろう。

III 新市場の創出

⑬ クラウドコンピューティングサービスの競争力確保とセキュリティ上の課題

具体的な取り組み例にも記述があるように、クラウドコンピューティングの分野では、いまだに確固としたセキュリティ対策が確立されていない分野である。従来の IT システムで利用可能なセキュリティ対策技術が、クラウドの内部で利用できない状況があるほか、仮想化に伴う新たな脅威の出現などもあり、今後も引き続き議論と検討、新たな技術的対策の開発が必要とされる分野である。

海外では、Cloud Security Alliance (CSA)が有識者により結成され、クラウドコンピューティングに求める安全基準についてガイドラインが発表されている[9]。我が国でも、同様の取り組みを強化し、国内の事業者が安心して利用できるためのガイドラインの整備や、安全対策における国際的なニシアチブの発揮が期待される。

データセキュリティに求められるセキュリティ要件

本章では、前章で明らかにしたデータセキュリティへの検討の必要な重点施策にてセキュリティ対策を考える際に、どのような要件を考え、セキュリティ基準を決定してゆく必要があるかについて詳細を述べる。

情報資産を保護する上で考慮すべきセキュリティ要件

これまで明らかにしてきたように、機密情報を電子化し、システムに保存する場合、主要なインタフェースとなる Web に対する外部からの脅威への備えと、情報を保持するデータベースに対する内部からの不正利用への備えの、内外両面の脅威に対する対策が必要となる。

Web アプリケーションについては、安全な Web アプリケーションを開発することはもちろんのこと、脆弱性の診断や攻撃を積極的に防御する WAF の導入などを検討すべきである。

一方の行政保有情報を保存するデータベースについては、「必要な人間が必要な情報のみにアクセスできること」を保障できる強固な職務分掌とアクセス制限の仕組みの導入、不正利用を牽制する監査、万が一の情報漏洩を検出し防御することのできるファイアウォール製品などの対策を考えてゆく必要がある。

Web アプリケーションの保護

インターネットからの攻撃を防御する手法としては、ファイアウォール、IPS、アンチウィルス対策製品、Web アプリケーション・ファイアウォール(WAF)、そしてこれらを統合する UTM などの対策機能が利用可能であり、多くの Web サイトで導入が進んでいる。

セキュリティ基準を決める過程では、当然これらの一般的なセキュリティ対策の検討が行われるものと思うが、アプリケーションレイヤに攻撃の中心が移ってきている現状を考慮すると、アプリケーションレイヤへの攻撃をどう防いでゆくかを検討することが重要である。

クレジットカード業界団体が導入した PCI コンプライアンスでは、このアプリケーションレイヤの脅威を防止するにあたって、ファイアウォールや IPS といった従来のセキュリティ対策に加えて、脆弱性診断や WAF の利用が明記されている [6]。一方で、国内では IPS 製品や簡易的なシグネチャをベースとする製品が、WAF レベルの防御機能を提供できると喧伝している傾向があり、正しい情報が伝わっていないのではと筆者は危惧している。そこで、WAF の対抗として語られることの多い、IPS や脆弱性診断のメリットとデメリットを明記し、セキュリティ基準の検討に活用いただければ幸甚である。

IPS でアプリレベルの防御が十分でない根拠

IPS のメリットは、何といっても運用の簡便さである。ベンダーがブラックリストを配布し、利用者はそれを適用するだけで主要な攻撃は防御可能である。しかし、IPS の防御機能が大きな効果を発揮するのは、あくまで Layer 4 までであり、Web アプリケーションの保護については必ずしも有効とは限らない。IPS が適さない理由を挙げると、

- **カバレージとパフォーマンス**

  Web アプリケーションレベルの攻撃は多種多様なパターンが存在するため、シグネチャだけでカバーしようとすると、膨大な数のシグネチャを用意しなければならないが、IPS が一度に有効にできるシグネチャ数には限界がある。結果、多くの製品は、非常に基本的な攻撃パターンのシグネチャしか保有していないため、簡単に回避が可能な状況にある。例えば、' or 1=1 は検出できるが、' or 2=2 は検出できない、といった具合である。

  一方で、回避攻撃に対する耐性を高めようとする場合、一般的に取る手法が正規表現となる。しかし、IPS の場合、正規表現を多用するシグネチャは、計算負荷を高める傾向にあり、多数をロードすると今度は性能劣化や遅延の増加を引き起こして、使い物にならないケースが出てくる。

- **False-Positive の多さ**

  IPS は、アプリケーションレベルの攻撃以外でも、一定量の False-Positive が避けられないソリューションではあるが、Web レベルの攻撃ではより顕著となる傾向がある。Web レベルにて SQL インジェクションを防御する場合、単純な文字列をシグネチャとしてしまうと、False-Positive が多く発生する結果につながる。例えば、SQL インジェクションの記事を書くべく、文中に ' or 1=1 を書いてブログを投稿しようとしたら、SQL Injection 攻撃としてブロックされてしまう、といった具合である。

- **回避攻撃に弱い**

  HTTP プロトコルレベルでは、様々なエンコード方式が使用される。例えば、Chunked Encoding は、メッセージを複数のブロックに分割して送信するため、リクエストの中身を検査する場合、分割されたブロックを再構築してチェックする能力が必要である。 Gzip/Deflate の圧縮転送も同様に、圧縮をデコードして、内部を解析できなければならない。URL Encoding や UTF など、文字列表記ひとつとっても記述方法はさまざまである。

  IPS の場合、L4-7 レベルのコンテンツをチェックしようとする場合、複数のパケットを組み合わせてアプリケーションレベルのメッセージを再構築し、その再構築した情報に対してシグネチャの検査を行う必要がある。ところが、多くは再構築のため一時的に保持できるパケットの数に制約が設けられており、当然、Chunked Encoding や圧縮転送への対応は弱くなる。この制約を解除することもできるが、多くの場合パフォーマンス劣化を引き起こす。

  文字エンコードについても、シグネチャでの対応はかなり難しくなる。最近の自動攻撃では、SQL インジェクションのコードが難読化される傾向が高く、防御されるとまた新たなパターンを作るといった具合に、ブラックリストでの防御が困難な状況になってきている。

以上から、アプリケーションレベルの防御に IPS のみで対応するというのは、今日のインターネット上の攻撃を防ぐ点からは十分ではないと言える。セキュリティ基準を検討する際には、十分考慮に入れるべき点であろう。

脆弱性診断のみでは不十分なわけ

続いて、Web アプリケーションへのセキュリティ対策として、利用頻度が高いサービスが脆弱性診断である。脆弱性診断による検出とアプリケーションの修正は、アプリケーションのセキュリティレベルを高める上で非常に有用である。しかし、一方で、脆弱性診断の誤った利用は、セキュリティ対策としての機能不全を起こす。

脆弱性診断については、ソースコード・レビューを含む診断サービスと、ツールを使ったブラックボックス・テストの二種類が一般的である。前者は、高い検査精度を担保できるが、一方で単価が高く、全 Web ページに適用するのは費用がかさみすぎて適用できる組織は限られる。一方、後者については、脆弱性診断ツールを使って網羅的に検査するため、ページあたりの単価は安く全 URL を対象に検査が行える。ただ、検査精度という点では、前者に大きく劣る点がネックとなる。

脆弱性診断ツールを使った場合の最大のネックは、基本的にリクエストとそのレスポンスを対にして検査を行う点である。つまり、リクエストを受けて「成功/失敗」のメッセージだけを返すような作りのアプリケーションは、基本的には自動検査できないのである。もう少し具体的に書くと、例えば、ユーザのプロパティ変更機能に SQL Injection 脆弱性があったとして、この機能は成功したか否かのみクライアントに返す構造になっているとする。この場合、SQL Injection 攻撃を実施して、他のユーザのプロパティを書き換えるリクエストを送ったとしても、メッセージの送信に成功した旨のメッセージしかアプリケーションからは返ってこない。エラー画面が返ってきたとしても、アプリケーションが作成しているエラー画面であれば、SQL Injection があったからエラーになったのか、それとも、きちんと入力値チェックをしてエラーを返したのか、ツールからは自動で判断できない。当然、脆弱性診断を行う会社は、この制約をわかっているので、検査前に制約事項を説明した上で、「可能な限り手動でのチェックを行います」とする。結果、実際に脆弱性を発見できるか否かは、検査者のスキルによるところが大きい。

したがって、ツールによる脆弱性診断は、アプリの作りによって検査精度に大きな違いが出ることになるため、ツールによる検査のみで安心かというと、そうでないケースの方が多いのが実情である。よって、脆弱性診断のみ、という運用ではなく、アプリケーションへの攻撃を積極的に防御する WAF などの防御装置を検討することが重要となる。

脆弱性診断と WAF を併用することによるメリットも非常に大きい。脆弱性診断を定期的に実施することにより、アプリケーションが抱える脆弱性を定期的にモニタできるとともに、WAF を併用することで、脆弱性を修正するまでの期間、脆弱性を保護するセキュリティポリシを実装することが可能になる。アプリケーションの修正には、多くの場合、修正のための期間と修正コードの確認のためのテスト期間の両方が必要となることから、仮想的にパッチを当てることのできる WAF が存在することにより、脆弱性がインターネットにさらされるリスクを回避しつつ、修正のための期間を自由にコントロールすることができるメリットが生まれる。

セキュリティ基準を検討する上では、脆弱性診断のメリットを生かしつつ、WAF などの外部からの攻撃を防ぐセキュリティ対策との連携を効果的に利用してゆくべきであろう。

WAF を検討する上で考慮すべき点

WAF を検討する際には、製品の持つべき能力を十分に検討する必要がある。参考になる先駆的な例として、PCI DSS が 2008 年 4 月にリリースした「補足情報: 6.6 コードの見直しとアプリケーションファイアウォールの明確化」に、WAF が持つべき能力を明記した記述がある[10]。そこで求められている要件を以下に列挙する。

- **少なくとも OWASP トップ 10 [11] で特定されている脆弱性に対する脅威に、適切に（アクティブなポリシまたはルールによって定義）対処する。**
- **Web アプリケーションへの入力を調査し、アクティブなポリシまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、アラート）する。**
- **データ漏えいの回避 - Web アプリケーションからの出力を調査し、アクティブなポリシまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、マスク、アラート）する機能が備わっている。**
- **ポジティブとネガティブの両方のセキュリティモデルの実装。**
- **HTML（Hypertext Markup Language）、DHTML（Dynamic HTML）、CSS（Cascading Style Sheets）などの Web ページコンテンツと、HTTP（Hypertext Transport Protocol）、HTTPS（Hypertext Transport Protocol over SSL）などのコンテンツの送信基盤となるプロトコルの両方を調査する（HTTPS には、SSL だけでなく、TLS による HTTP も含まれます）。**
- **Web サービスが公共のインターネットに公開されている場合は、Web サービスのメッセージの調査。**
- **Web アプリケーションとの間でのデータ転送に使用されるすべてのプロトコル（独自または標準的なもの）またはデータ構造（独自または標準的なもの）が、メッセージフローの他のポイントで調査されない場合、これらを調査する。**
- **WAF 自体を標的とした脅威を防ぐ。**
- **SSL または TLS ターミネーションに対応する。または、暗号化された送信内容を復号化してから調査できる位置に配置されている。**

上記以外にも細かい要件が記述されており、セキュリティ基準を設定する際には、同様の詳細な要件の検討が必要と考える。

データベースの保護

データベースのセキュリティ基準を検討する上で必要な検討課題について述べる。国内での検討は、データベースセキュリティコンソーシアムがリリースしている「データベースセキュリティガイドライン」[12]が詳しい。

- **機密情報の暗号化**

  漏洩した際の影響が大きい機密情報については、データを暗号化して保存することが重要となる。データベースの暗号化だけではなく、監査データや、監査の際に表示する情報についても、機密情報は暗号化やマスクが必要となる。

- **強固なアクセス制御**

自動アクセス制御の実装や、特権ユーザ ID に関するアクセス権限を最小限にとどめること、アクセス制御システムを全てのシステムコンポーネントに実装することなどを検討し、職掌に基づくアクセス権限の付与と管理職による承認といった適切な運用が考慮すべき要件として挙げられる。

- **コンポーネントにアクセスするユーザ ID の適切な運用**

内部犯行を牽制する上で重要なのが、重要資産を含むデータベースアクセスに使用する ID を一意にすること、そして職務分掌の徹底である。セキュリティ対策が不十分なデータベースでは、グループで共通のアカウントを使用しているケースなどがあり、この状況で漏洩事故が発生すると発生源の特定が困難となる。三菱 UFJ 証券の事件では、システムを運用する管理者が不正アクセスを行ったのであるが、その際に発覚を防ぐ目的で不正に作成した他の従業員のユーザ ID を使用してアクセスを行っていた。不正アクセスを行った人間が管理者であったため、防止するのは非常に困難であったと予想されるが、データベースサーバの管理と不正アクセスの監視や監査を行う人間を別々の権限とする職務分掌の徹底により、不正を未然に防ぐことは可能であったと考える。

また、2009 年に流行したガンブラーウィルスでは、Web サイトのコンテンツを管理している FTP サーバのパスワードを窃取することにより、コンテンツの改ざんが大規模に行われた。このような認証情報窃取型のウィルスは今後も増えることが予想され、データベースへのアクセスが可能なシステムに対するリモートアクセスに、パスワードだけが漏洩しても容易にアクセスを許さない二因子認証などを必要とするシステムの構築を検討する必要があろう。

- **機密情報へのアクセスの追跡および記録**

行政関連の個人情報や医療情報など、機密性の高い情報へのアクセスは全て記録に残しておく必要があり、監査の要件をセキュリティ基準に盛り込むべきである。監査は、データそのものへのアクセスに加え、監査証跡へのアクセス、管理者権限のアクセスについても要件として考慮すべきである。管理者が不正を働く場合、監査記録を削除して発覚を防ぐことが多いため、管理者の不正を防ぐ、という点で非常に重要であり、監査証跡なども容易に改ざんできない形式とする要件を検討すべきである。

また、監査証跡を取得しても、それを適切に分析し、不正な活動をいち早く検出する体制が必須である。したがって、監査証跡を効率的に実行するシステムを考慮する必要があると考える。

- **定期的な検査**

データベース製品も他のソフトウェア製品同様、脆弱性の発見と修正のリリースが繰り返されている。ファイアウォールや IPS レベルで防止できる脆弱性も多いものの、アプリケーションレベルの脆弱性も発見されており、脆弱性への対応が課題となる。したがって、データベースサーバに対する脆弱性診断など、定期的な検査を要件として考慮すべきであろう。

一方、重要施策①に示された週 7 日 24 時間サービス可能なシステムとする場合、発見された脆弱性に対するパッチの適用が課題となる。脆弱性の修正を行うパッチを適用する場合、多くのシステムでは再起動が必要となるため、サービス停止を伴うことになるが、高い稼働率を求められるシステムではこれが困難なケースが多い。

よって、Web アプリケーションにおける WAF での仮想的パッチ適用の例と同様、データベースにおいてもファイアウォール製品により脆弱性を保護するポリシを適用して攻撃を防ぎつつ、メンテナンスの時期にパッチを適用する効果的な運用が可能である。セキュリティ基準を検討する際には、このような手法も検討の価値があると考える。

結言

高度情報通信ネットワーク社会推進戦略本部より発表された新たな情報通信技術戦略（IT 戦略）骨子（案）の中では、個人情報を含む様々な行政保有の情報の集約化と、インターネット経由でのアクセスを可能にするサービスについて検討が行われている。いずれの施策も、利用者の利便性を大きく向上し、行政サービスの効率化を図る上で非常に有益である一方で、行政保有情報の機密性や個人情報の保護の重要性を考慮すると、情報セキュリティの重要性について多くの課題と留意すべき点が含まれていると考える。

そこで本パブリックコメントでは、現在のインターネット上の脅威の性質と内部犯行の脅威の増加という背景を受け、アプリケーションレベルの攻撃を防ぐ対策の必要性と、有効な内部統制システムを確立する上で非常に重要な要素となるデータベースセキュリティの要件を考慮する重要性、および検討の際に考慮すべきセキュリティ要件について述べた。

ユーザの利便性と行政の効率化とコスト削減を中心に考えるだけではなく、システムを安全に運用するためのセキュリティ要件について十分検討を行い、利用者が情報漏洩の心配なく安心して利用できる仕組みが確立されることを強く希望するものである。

参考文献

[1] 株式会社 LAC. セキュリティアラート 2009 年 6 月 9 日. (オンライン) 入手先 http://www.lac.co.jp/info/alert/alert20090609.html

[2] 株式会社 LAC. JSOC 侵入傾向分析レポート Vol.14. (オンライン) 入手先 http://www.lac.co.jp/info/jsoc_report/_vol14.html

[3] 独立行政法人 情報処理推進機構. セキュア・プログラミング講座. (オンライン) 入手先 http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

[4] 独立行政法人 情報処理推進機構. 脆弱性関連情報の届出状況. (オンライン) 入手先 http://www.ipa.go.jp/security/vuln/report/press.html

[5] Chenxi Wang, Ph.D. “Web Application Firewall: 2010 And Beyond WAF+ Finds Its Place In Firms’ Network Infrastructure”. Forrester 2010

[6] PCI Security Standard Council. “Payment Card Industry データセキュリティ基準”. (オンライン) 入手先 https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf

[7] Imperva Application Defense Center. “Consumer Password Worst Practice”. (オンライン) 入手先 http://www.imperva.com/ld/password_report.asp

[8] 「最高 1 兆円超、イメージダウンの損失」.日経コンピュータ 3 月 3 日号 (2010). Page 36-37

[9] Cloud Security Alliance. “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”. (オンライン) 入手先 http://cloudsecurityalliance.org/csaguide.pdf

[10] PCI Security Standard Council. 「補足情報: 要件 6.6 コードの見直しとアプリケーションファイアウォールの明確化」. (オンライン) 入手先 https://www.pcisecuritystandards.org/pdfs/japanese_infosupp_6_6_applicationfirewalls_codereviews.pdf

[11] Open Web Application Security Project (OWASP). “OWSP Top Ten Project”. (オンライン) 入手先 http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[12] データベース・セキュリティ・コンソーシアム. 「データベースセキュリティガイドライン第 2.0 版」(2010) (オンライン) 入手先 http://www.db-security.org/report/dbsc_guideline_ver2.0.pdf