Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

Web アプリケーションのセキュリティマネジメント －企業の状況分析を通じた分析と提案－

金根學[†1]　原田要之助[†1]

概要：近年，Web サイトは誰もが身近に接することができるようになり，多様化，高度化され，インターネット使用者の拡大とともにその数は爆発的に増加，発展を見せている．一方，インターネットを通じた攻撃は日常的に起こっており，その脅威はますます増えつつある．特に，Web アプリケーションにおけるセキュリティリスク対策の重要性が高まっている．公開されている Web サイトは悪意ある第三者によってネットワークを通じ標的となる可能性を抱えている．また，Web アプリケーションの開発上のエラーや構成上の問題点，脆弱点に対してパッチの未適用などにより大事な情報がインターネットに流出する可能性もある．本稿では，Web アプリケーションセキュリティのあるべき姿を定義し，各組織の開発面，または運用面に関する Web アプリケーションセキュリティのリスク対策の現状をアンケート調査で把握することにより，安全な Web アプリケーションを提供するためのセキュリティマネジメントの観点から Web アプリケーションのセキュリティリスク対策について考察する．

キーワード：WEB アプリケーションセキュリティ，セキュリティマネジメント

Security management discussion of Web application security

GEUNHAK KIM[†1]　YONOSUKE HARADA[†1]

Abstract: In recent years, the Web site has become accessible to everyone, diversified and advanced, and the number has explodedly increased and expanded with the expansion of Internet users. Meanwhile, attacks through the Internet are occurring on a daily basis, and the threats are increasing more and more. In particular, the importance of countermeasures against security risks in Web applications is increasing. Published websites have the possibility of being targeted by malicious third parties through the network. Also, there is a possibility that important information leaks to the Internet due to errors in the development of the Web application, constituent problems, patches not applied to vulnerabilities, and so forth. In this paper, we define how the Web application security should be, and grasp the current status of Web application security risk countermeasures concerning development or operational aspects of each organization by questionary survey. As a result, security risk measures for web applications are considered from the viewpoint of security management to provide secure web applications.

Keywords: Web Application Security, Security Management

1. 背景

近年，デジタル環境は以前に比べ複雑になってきた．多くの人がインターネットで物を売ったり買ったり，インターネットバンキングなどの金融サービスを利用したり，余暇を楽しんだりと，様々な場面で活用している．

このようにインターネット上で動いているサービスを「Web」あるいは「Web アプリケーション」と呼んでいる．「Web アプリケーション」は Web サーバー上で実行されるソフトウェアプログラムである．OS 上で実行されている既存のデスクトップアプリケーションとは異なり，「Web アプリケーション」は Web ブラウザを介して使うことになる．インターネット上で様々なサービスを提供する Web アプリケーションはネットワークで結ばれた社会において，重要性を増している．

一方で，Web アプリケーションへのリスクは企業が深刻に憂慮すべきサイバーセキュリティ脅威の一つである．つまり Web アプリケーションそれ自身が持つ固有の脆弱性によってテロや犯罪を目的にしたサイバー攻撃にさらされている．さらにほとんどが，不特定多数のユーザーがアクセスできるように公開されているため，ハッキングなどのセキュリティ事故の攻撃対象になっている． 最近では，正規の Web アプリケーションにアクセスしただけでランサムウェアに感染したという事例があり，また Web アプリケーションが改ざんされていたこともある[1].

そのため，WEB アプリケーションの安全性を維持して改善することは，経済の成長や社会の健全な発展のために必要である．Web アプリケーションを信頼できるよう構築するには Web アプリケーションのセキュリティリスク対策（以下，「アプリケーションセキュリティ」という）を，以下述べるとおり開発時並びに運用時に，管理的かつ技術的なレベルでの対策が必要であると考える．

2. アプリケーションセキュリティのあるべき

†1 情報セキュリティ大学院大学
Institute of Information Security

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

姿

本稿では，アプリケーションセキュリティでのあるべき姿とは，アプリケーションのソフトウェア開発ライフサイクルの要件定義段階からセキュリティを考慮してセキュアコーディングを用いて開発を行う。また運用段階でアプリケーション管理，脆弱性の管理，監視，パッチの適用などの活動を行い，脆弱性に対する開発側と運用側の速やかな連携でセキュリティのリスクに対処するものと定義する．
しかし，アプリケーションセキュリティに関する調査によると，企業の IT 部門ではアプリケーションの開発から運用まで含めたアプリケーションセキュリティを全体的には可視化できていない状況であり，アプリケーションセキュリティ業務が開発と運用にバラバラに分かれて低レベルで実行されていると発表している．[2]
現実には，開発段階では多くのガイドラインが発表されているが，それらが活用されてないため，脆弱性を含んだ Web のアプリケーションが運用されていると考えられる．また，Web のアプリケーションの脆弱性が発見された場合，開発側の対応では手が回らなくなり，運用側に対応を押し付けざるを得ない状況にあるのではないかと考える．
本稿では，組織におけるアプリケーションセキュリティについて，開発面と運用面がそれぞれどのように考えているのか調査し，現状を分析して，アプリケーションのセキュリティの向上施策を提案する．

2.1 先行研究について

大久保[3]は，アプリケーションのセキュリティを実現する対策として，アプリケーションの開発時にセキュリティ工学に基づいて要求分析をすることを提案している．これによって，開発面において，セキュリティの見落としが減るものと期待される一方で，運用面での対策についても考慮する必要があると考える．
一方，小柳[4]は，ソフトウェア工学の立場からセキュリティに関する要求項目を洗い出し，それらをシステム要件として，系統的に設計に組み入れようとするアプローチを紹介している．具体的には「アプリケーションでは，新規開発の際に脆弱性を盛り込まないようにすることだけでなく，既存のシステム内の脆弱性を検出することも重要である．現在多くの Web アプリケーションが脆弱性を含んだまま利用されている．また現在発見されていない脆弱性もありうるので，運用後の脆弱性の発見・除去は必須の技術である」と述べている．
すなわち，アプリケーションの脆弱性については，設計段階だけではなく運用面でのマネジメントが重要であることを述べている．

2.2 セキュリティマネジメント規格の調査

セキュリティマネジメントに関する規格化について，ここでは ISO/IEC27001(JIS Q27001)を紹介する[5].
JIS Q 27001:2014 とは，情報セキュリティマネジメントシステムを確立し，実施・維持し，継続的に改善するための要求事項を提供するために作成されたガイドラインである．JIS Q 27001:2014 の附属書「A．14　システムの取得，開発及び保守」では，開発面と運用面でのセキュリティ対策としてセキュリティ管理策を定め，アプリケーションセキュリティの管理策を示している．

3. 組織におけるアプリケーションセキュリティの実態調査について

3.1 情報セキュリティ調査の概要

本稿では，アプリケーションセキュリティに関する実態を把握するために，アンケートによる調査を実施した．
原田研究室では 2012 年より「情報セキュリティ調査」を実施している．本稿では 2016 年 8 月に「情報セキュリティ調査」アンケートを郵送にて実施した調査結果を報告する．
対象は，日本国内のプライバシーマーク取得組織，ISMS 認証取得組織，官公庁，教育機関などから選んだ 4,800 組織(送達確認できたのは 4,704 組織)である．その結果 544 件(12%)の回答が得られた．なお，本論文においては回答の未記入および択一問題における重複回答等の無効回答は，無回答として計上している[6].
以下，アプリケーションセキュリティに関する調査を実施した結果を述べる．

3.2 アプリケーションセキュリティに関するアンケート調査

これまで日本の企業又は組織（以下，組織という）においてアプリケーションセキュリティがどう理解されているのか明らかではなかった．そこで，アンケートでは，組織におけるアプリケーションセキュリティがどう理解されているのかを調査した．その結果は下記の通りである．

3.2.1 アプリケーションリスク管理状況

組織のアプリケーションのリスク管理状況についての調査では，全体の約 66%の組織で，(全て，概ね)管理できていることが分かった（図 1）.

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

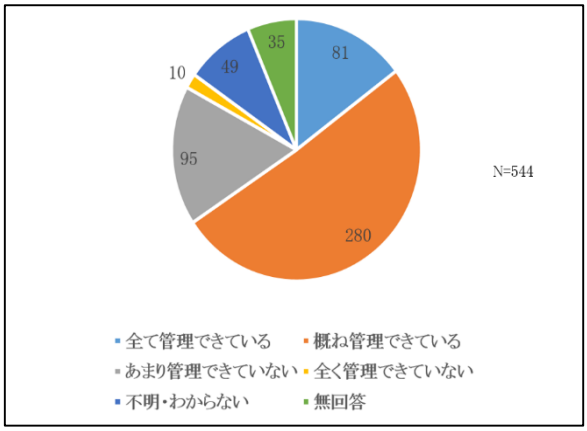

図 1 運営中のすべての Web やモバイルのアプリケーションをどの程度管理していますか．（〇印はひとつだけ）

組織ではアプリケーションのリスク管理がされていることから，組織のアプリケーションセキュリティに対する認識はあると考えられる．

3.2.2 アプリケーションリスク管理状況

一般的に，組織のアプリケーションセキュリティ管理担当はアプリケーションの開発に携わっている担当者が適任だと考えられる．

アンケート調査結果によると，アプリケーションセキュリティのリスク管理の担当者はシステム運用部門の責任者（290 件）が最も多かった．ただし，アプリケーションの開発状況について最もよく知っているソフトウェア開発責任者（102 件）や組織のセキュリティ最高責任者である，CIO または CISO（65 件）が少ないことが確認された（図 2）．

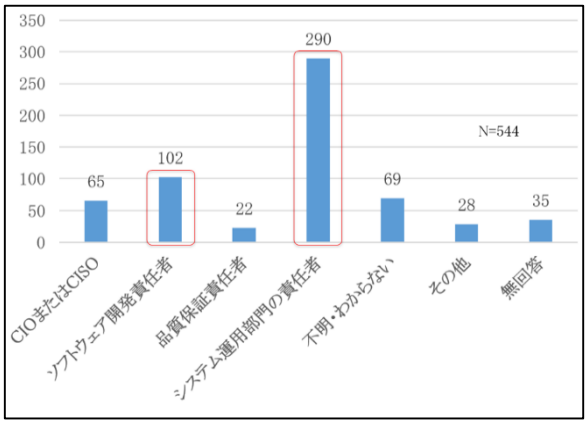

図 2 アプリケーションセキュリティのリスク管理は，誰が担当していますか．（複数選択可）

この結果では，組織のアプリケーションセキュリティのリスク管理を担当するのは開発側ではなく，運営側が担当している傾向にある．

これは，組織のアプリケーションセキュリティが開発側で対応されず，運営側に押し付けられているとも考えられる．

3.2.3 アプリケーションの開発・運営形態

アプリケーションの開発運営形態の調査では，パッケージソフトウェアの導入（312 件）の形態が最も高かった．独自開発（190 件），第三者（外注）の開発（178 件）の形態も見られた．組織では，さまざまな形でアプリケーションが開発・運営されていることが判った（図 3）．

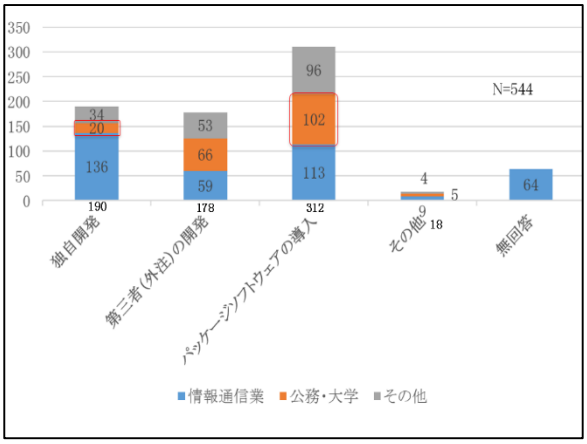

図 3 貴社のアプリケーションの開発運営形態に当てはまるものはどれですか．（複数選択可）

組織のアプリケーションの開発・運営形態はパッケージソフトウェアの導入の形態が多く，「公務・大学」では独自開発の形態に比べて最も多かった．組織では自らの開発以外にもパッケージソフトウェアも多く使っている傾向にあることが判った．

パッケージソフトウェアの導入については，今までのアプリケーションのセキュリティの対象としてはあまり考慮されなかった．パッケージソフトウェアの代表的な例としての ERP，CMS（content management system）などがあげられる．特に，CMS の場合，オープンソースのアプリケーションが多い．パッケージソフトウェアについては，今までの自らの開発するアプリケーションセキュリティだけでは対応することが難しく，別の観点のアプリケーションセキュリティのアプローチが必要であると考えられる．

3.2.4 アプリケーションセキュリティのリスク変化

アプリケーションのリスクは日々に変わっているのが現実で，組織の実務者は増加しているリスクを感じていると考えられる．

調査結果によると，アプリケーションセキュリティのリスク変化について担当者は「非常に増加している」と「増加している」の合計 36%，「変化はない」は 38%の回答であった．また，アプリケーションセキュリティのリスクの変化に対して認識していない組織も 18%の回答であった（図 4）．

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

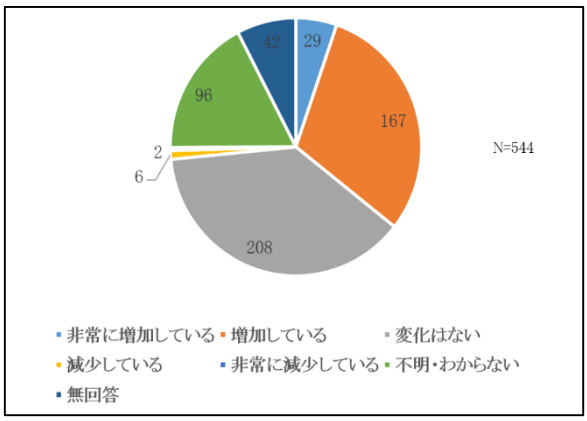

図 4 この一年でアプリケーションセキュリティのリスクに変化があったと考えていますか．（〇印はひとつだけ）

調査結果として 3 分の一の組織ではリスク変化について認識しており，気にしていることが分かった．

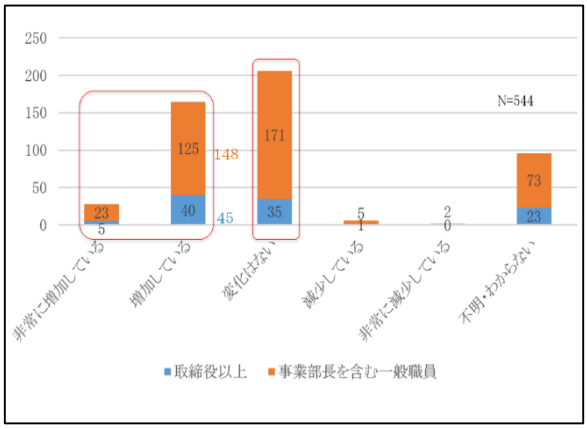

図 5 役職別分析

また，図 5 のように詳細な分析結果，取締役以上では「変化はない」（35 件）回答より「非常に増加している」と「増加している」（45 件）の回答が多く，事業部長を含む一般職員では「非常に増加している」,「増加している」（148 件）より「変化はない」（171 件）の回答の方が多かった．従って，実務者の方が経営者よりアプリケーションセキュリティのリスク変化はないという認識が若干低い傾向にある．

3.2.5 アプリケーションセキュリティの管理目的

アプリケーションセキュリティにおける管理目的で組織が最も重視しているのは，「情報漏えいの防止」（72%）である．「業務の中断時間の抑制」(12%)も少ないがアプリケーションセキュリティの管理目的として認識されている（図 6）．

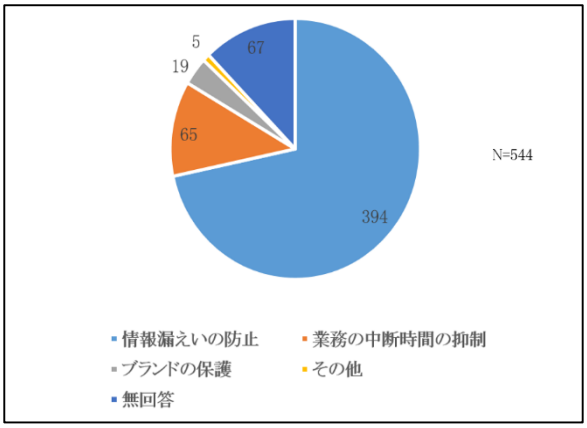

図 6 アプリケーションセキュリティの管理の目的で一番重視しているものを選択してください．（〇はひとつだけ）

3.2.6 アプリケーションセキュリティの状況

組織のアプリケーションセキュリティにおける対策は，開発段階の対策（開発者向けのセキュアコーディング教育の実施，セキュアコーディングガイドの提供，開発段階の脆弱性診断，ソースコードレベルの脆弱性検査）と，運用段階での対策（運用段階での脆弱性診断，外部専門会社の脆弱性診断 ）に分けられる．

アプリケーションセキュリティの活動として両方とも有効であるが，運用段階でアプリケーションセキュリティ活動は開発段階でのアプリケーションセキュリティの活動よりコストがかかる．

調査結果では，開発段階の対策は 215 件，運用段階の対策は 220 件,「実施していない」が 200 件を占めの結果が得られた（図 7）．

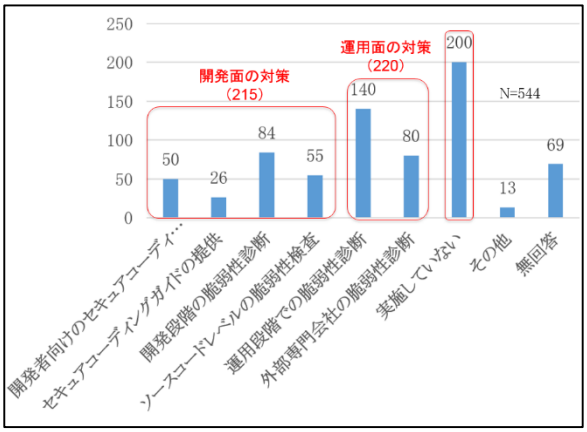

図 7 アプリケーションセキュリティ活動として何を実施していますか．（複数選択可）

より詳細を見ると，開発面において最も多かった答えは「開発段階の脆弱性診断」（84 件）で，運営面での最も多くの答えは「運用段階での脆弱性診断」（140 件）のことから，運用段階でアプリケーションセキュリティを実施している組織が多いことがわかる．従って，多くの組織では，開発

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

段階ではなく，運用段階でセキュリティ対策を実施する傾向にあると考えられる．一方,「実施していない」(200 件) と回答した組織も多く，アプリケーションセキュリティを実施していない理由についてこれから調べていきたい．

次に，アプリケーションセキュリティにおける対策状況の違いを明らかにするため，組織の業種, ISMS 認証の取得の有無による分析を行った．その結果は下記の図 8 から図 11 に示す．

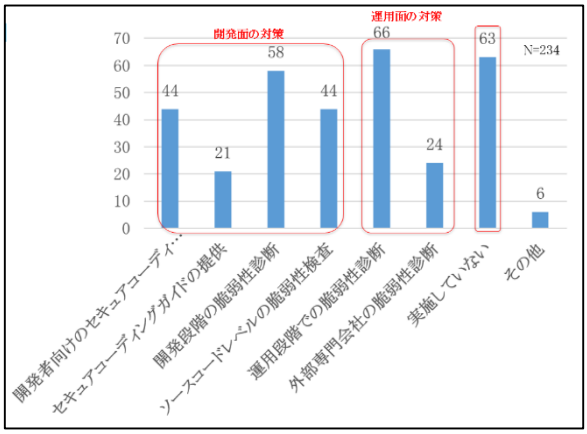

図 8 情報通信業

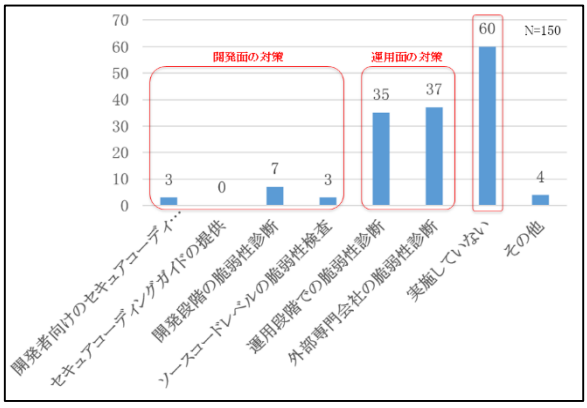

図 9 大学，公務

特に大学，公務の組織では開発段階の対策はほぼ行っていない状況であることが分かる．(図 9) これは，大学・公務の組織では前述のようにパッケージソフトウェアの導入が多いため為にあると考えられる．

次に，ISMS 認証を取得している組織を比較してみると，ISMS 認証を取得していない組織では，開発段階の対策を実施している回答がほぼない状況であることが分かる．(図 11)

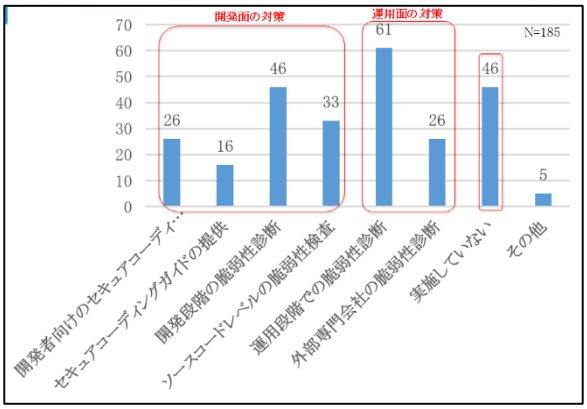

図 10 「ISMS 認証取得」組織

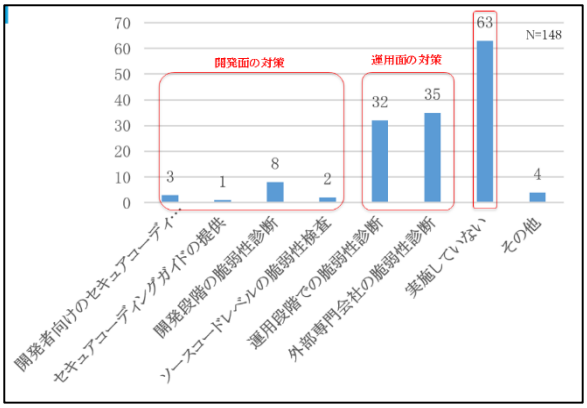

図 11 「いずれも認証取得していない」組織

ISMS 認証を取得している組織は，セキュリティ対策全般の認識が高いと思われるため，アプリケーションセキュリティにおける対策も実施していると想定される．

3.2.7 アプリケーションセキュリティのリスク管理ができない理由

アプリケーションセキュリティのリスク管理ができない理由は，「専門知識の不足」が 232 件，「組織内での優先順位が低い」が 117 件，「十分な予算が確保できない」が 109 件の順であった．(図 12)

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

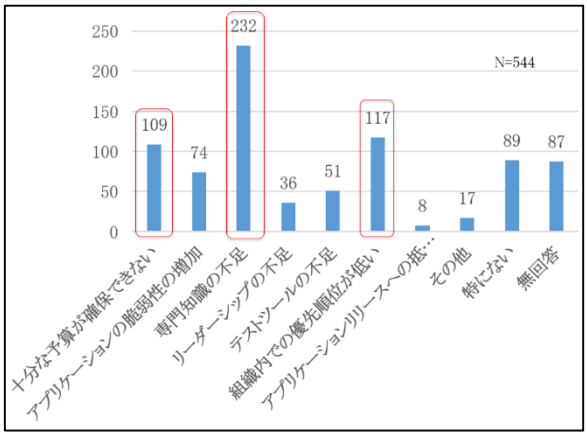

図 12 アプリケーションセキュリティのリスク管理ができない理由を選択してください．（複数選択可）

この結果により，組織のアプリケーションセキュリティ強化のためには，専門知識の確保，組織内での優先順位の向上，十分な予算が必要と考えられる．

3.3 組織におけるアプリケーションセキュリティの実態のまとめ

以上，今回の調査結果より下記の実態が分かった．

- 多くの組織ではアプリケーションを管理している
- アプリケーションセキュリティのリスク管理の担当は開発側より運用側の方が多く，対策も運用側で行われていることが多い
- 多くの組織では独自開発，第三者開発よりパッケージソフトウェアの導入が多い
- 調査対象の組織のうち，三分の一がアプリケーションセキュリティのリスクが増加していると認識している
- アプリケーションセキュリティのリスク変化に関しては，幹部より実務担当者の側の認識が低い
- アプリケーションセキュリティの管理ができない理由として，専門知識の不足，組織内での優先順位，十分な予算の確保の問題が挙げられる

4. 最後に

本来アプリケーションセキュリティについては，前述のとおり開発面と運用面の対策を考慮しなければならないと考える．しかし，企業における実態がどうなっているのかを調査してみないと対策が難しい．そこで，アプリケーションセキュリティ対策に関するアンケート調査を実施し分析した．

その結果，実際の組織の業種形態や，アプリケーションを開発し運用する開発形態によって，アプリケーションセキュリティの状況が異なることがわかった．

また，アプリケーションの開発・運用形態においては，独自開発や第三者による開発よりも，パッケージソフトウェアが多く導入されているのが現状である．これは，本来なされるべき開発セキュリティの対策がうまく適用されていないものと考えられる．したがって，パッケージソフトウェアに対して，これまでとは異なる観点でのアプリケーションセキュリティを実施する必要があると考える．

今回の調査結果を受けて，2017 年度も「情報セキュリティ調査」を実施し，より詳細なアプリケーションの開発形態や開発面と運用面のアプリケーションセキュリティの現状について調査・研究をすすめ，あるべき姿とその対策方法などを改めて提言して行く予定である．

謝辞

本論文の執筆にあたり，ご指導いただいた情報セキュリティ大学院大学の教授陣，また多くの助言をいただいた原田研究室の客員研究員及びメンバーに対して感謝の意を表します．

アンケートへの回答をいただきました組織の皆様，アンケートの封入，データ入力に多大な協力をいただいた神奈川県立麻生養護学校元石川分教室，神奈川県立相模原養護学校，神奈川県立相模原養護学校橋本分教室，神奈川県立高津養護学校川崎北分教室，神奈川県立鶴見養護学校岸根分教室，神奈川県立中原養護学校，神奈川県立みどり養護学校新栄分教室，川崎市立田島支援養護学校（五十音順）の皆様に感謝します．

参考文献

[1] IPA,「ランサムウェア感染被害に備えて定期的なバックアップを」, http://www.ipa.go.jp/security/txt/2016/01outline.html
[2] Ponemon Institute LLC,「How to Make Application Security a Strategically Managed Discipline」, 2016 年 3 月
[3] 大久保　隆夫, 企業におけるセキュリティ分析技術の実効性, 情報処理 Vol.50 No.3, 2009
[4] 小柳和子, Web アプリケーションセキュリティの最近の動向, 情報セキュリティ総合科学 No1., 2009
[5] JIPDEC,「JISQ27001-情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」,2014 年 3 月
[6] 副島ほか,“2016 年情報セキュリティ調査から見えてくる組織(民間企業・官公庁・教育機関)における現状”, 2017 年 暗号と情報セキュリティシンポジウム講演予稿集, 2A2-3
[7] 米国立標準技術研究所,「情報システム開発ライフサイクルにおけるセキュリティの考慮事項(800-64 Revision 2)」, 2008,https://www.ipa.go.jp/files/000025343.pdf
[8] 藤澤正樹,「開発環境における管理策の考察」,2006(情報セキュリティ大学大学院)
[9] Si Choon Noh, A Study of Web Application Development Method for Secure Coding Approach Based on SDLC Steps, Jouranl of Information and Security Vol12, pp. 93-99, 2012
[10] IPA,「脆弱性調査と脆弱性対策に関するレポート」,2013, https://www.ipa.go.jp/files/000032929.pdf
[11] IPA,「安全な Web サイトの作り方 改訂第 7 版」, 2015, https://www.ipa.go.jp/files/000017316.pdf
[12] IPA, セキュリティ担当者のための脆弱性対応ガイド～企業情報システムの脆弱性対策～,2011

付録

付録 A.1 JIS Q 27001:2014[2]

Vol.2017-DPS-172 No.21
Vol.2017-SPT-26 No.21
Vol.2017-EIP-78 No.21
2017/11/30

JIS Q 27001:2014 の附属書「A.14　システムの取得，開発及び保守」ではアプリケーションセキュリティに関連する１２項目の対策(管理目的及び管理策)が述べられている．ここで「A.14」の項目を開発段階と運用段階のセキュリティ対策に分類した．これを，表 2 に示す．

表 1　JIS Q 27001 の 12 項目の管理目的

段階	区分	対策
開発段階	A.14.1.1	情報セキュリティ要求事項の分析及び仕様化
	A.14.2.1	セキュリティに配慮した開発のための方針
	A.14.2.5	セキュリティに配慮したシステム構築の原則
	A.14.2.6	セキュリティに配慮した開発環境
	A.14.2.7	外部委託による開発
運用段階	A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
	A.14.1.3	アプリケーションサービスのトランザクションの保護
	A.14.2.2	システムの変更管理手順
	A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
	A.14.2.4	パッケージソフトウェアの変更に対する制限
	A.14.2.8	システムセキュリティの試験
	A.14.2.9	システムの受入れ試験

表 2 に示すように JIS Q 27001 ではマネジメントの視点から開発・運用環境におけるセキュリティ管理策を定めている．