Vol.2017-EIP-75 No.7
2017/2/17

WEB アプリケーションのセキュリティマネジメントについての考察

金根學[†1]　原田要之助[†1]

概要：近年，WEB アプリケーションのセキュリティ脆弱性対策の重要性が高まっている．インターネットを介した攻撃は日常的に行われており，その脅威（アプリケーションのセキュリティという）はますます増えている．WEB システムに対して攻撃が成功してしまう要因の一つは WEB アプリケーションの脆弱性が挙げられる．WEB アプリケーションの脆弱性とは，攻撃者が WEB アプリケーションの仕様とは異なる動作をさせることができてしまう弱点のことである．その脆弱性を足掛かりにしてシステム内部まで侵入し，情報の漏えいといった事態になるおそれがある．安全な WEB アプリケーションを開発するための対策があるにもかかわらず，WEB アプリケーションの脆弱性を利用したハッキング事件が頻繁に発生している．本稿では WEB アプリケーションセキュリティ対策についてセキュリティマネジメントの観点から考察する．

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，ISO/IEC 27000

Security management consideration about web application

GEUNHAK KIM[†1]　YONOSUKE HARADA[†1]

Abstract: In recent years, the use of the application software is not only in the IT system, is spread for the control of a wide variety of equipment and systems. In particular, the importance of the security vulnerability management on web applications is increasing. Attacks over the internet are routinely performed, the threat is more and more. The vulnerability of web application is cited in one of the factors that the attack for the system succeeds. The vulnerability of the web application　is the weakness that an attacker can be let a different behavior from the specification of. The weakness might cause accident such as leakage of information, in invading system inside, by using the weakness as a cue of the attack. In reality, hacking attacks using the vulnerability of web applications occurs frequently though there are measures for developing secure web applications. In this study, measures for web application as security management are considered.

Keywords: Web Application Security, Security Management, ISO/IEC 27000

1. はじめに

インターネットとスマートフォンの普及により，今日の日常生活では, WEB なくして暮らすのは困難な時代になった．ゲーム，EC，金融取引から IoT まで WEB は日常生活とより密接に関わるものである．

一方，それに伴うセキュリティ問題はより深刻になっている．WEB を通じた個人情報の流出だけでなく，IoT 機器を利用した WEB への DDoS 攻撃まで発生している．

Ponemon Institute は，企業のアプリケーションセキュリティ関連の業務を担当している米国内の 630 人を対象にアンケート調査を実施している．[1]

調査によると, 企業の IT 部門がアプリケーションセキュリティの運用まで含めた全体的な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．

これを解決するには，次のような活動が必要であるとしている．

- 全社的なアプリケーションセキュリティ状態の可視化をはかる活動
- 発生する可能性が最も大きくてリスクが最も高いデータセキュリティ侵害を防止するために資源を割り当てる活動
- ビジネスリスクと戦略に合わせてテストおよびトラブルシューティングのための優先順位を決める活動

すなわち，アプリケーションセキュリティとは，組織がビジネスを行う上で必要とされる WEB アプリケーションを信頼できるよう，技術レベルでのソフトウェアの脅威，攻撃，脆弱性，そして運用における対策に焦点を置いた総合的な活動である．

現在，OWASP，ISO，PCI DSS，SANS など多くの WEB のアプリケーションのセキュリティに関するガイドラインや規格が産業界などで開発され，活用されている．

本稿では，これらの標準と規定による安全な WEB アプリケーションを開発や運用するために考慮すべき事項を検討する．

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

ⓒ 2017 Information Processing Society of Japan

2. アプリケーションとアプリケーションセキュリティ

2.1 アプリケーションソフトとは

アプリケーションとは，ある特定の機能や目的のために開発・運用される「アプリケーションソフト」の略称であり，「アプリ」(app, apps)と略されることもある．また「応用ソフト」と訳されることもある．

日常的に利用される代表的なものだけでも，WEB アプリケーションは，ワープロソフトや表計算ソフト，編集ソフト，画像・動画・音楽再生ソフト（メディアプレーヤー），ゲームソフト，WEB ブラウザ，電子メールソフト，カレンダー・スケジュール管理ソフト，電卓ソフト，カメラ撮影ソフト，地図閲覧ソフトなどがある．[15]　以下，本稿では，WEB アプリケーションをアプリケーションと呼ぶ．

2.2 アプリケーションセキュリティに関する規格の調査

アプリケーションセキュリティに関する規格としては，ISO/IEC27034，OWASP，SANS アプリケーションセキュリティ調達基準，IPA のガイドラインがある（表 1 参照）．

表 1　アプリケーションセキュリティに関する規格の位置付け

標準・規格	位置付け
ISO/IEC27034	アプリケーションセキュリティ標準
OWASP ASVS	アプリケーションセキュリティ検証標準
SANS	アプリケーションセキュリティ調達基準
IPA ガイドライン	安全なウェブサイトの作り方

(1) ISO/IEC 27034[14]

まず，ISO の規格は，ISO/IEC 27034 - アプリケーションセキュリティ（2011 年）が広く用いられている．この規格では，アプリケーションが組織の中で統一的に開発・運用されるように ASC（Application Security Controls:アプリケーションセキュリティ対策）の利用について述べている．この ASC は，各ビジネスのプロセス（供給・調達，管理，監査，支援）および役割に提供され，運用のエビデンスの生成にも利用される．ISO/IEC 27034 では，ASC をライブラリとして用意して，これを開発と運用で共通的に利用することを推奨している．これを図 1 に示す．

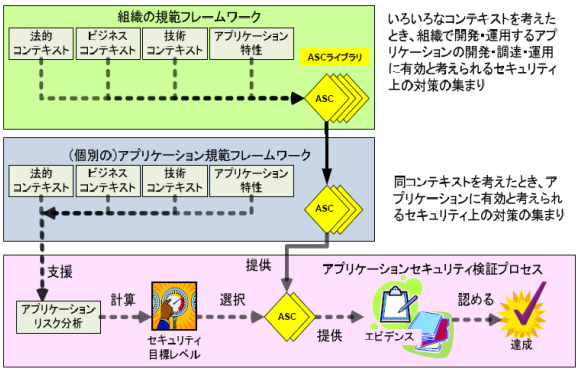

図 1　ISO/IEC 27034 の俯瞰

(2) OWASP アプリケーションセキュリティ検証標準[10]

OWASP はアプリケーションセキュリティに対して，実用的かつコスト効果の高い情報の提供を行っており，WEB システム／WEB アプリケーションセキュリティ要件書（V1.1，2013 年）や OWASP アプリケーションセキュリティ検証標準を無償で提供している．

アーキテクチャ，認証，セッション管理，アクセス制御など，アプリケーションに必要とされるセキュリティ要件を総計 19 のカテゴリに分類してまとめている．

これらのセキュリティ要件は，必ずしもすべて満たす必要はない．例えば「入力値検証はサーバ側で実装されている(5.5)」のように，すべてのアプリケーションが満たすべきセキュリティ要件がある一方で,「セキュリティログに完全性を保証する機構が備わっており許可なくログを変更できない(8.11)」のように，運用を含めた全体としての高度なセキュリティ要件もある．なお，要件書 では，次の 3 段階からなる「セキュリティ検証レベル」という運用を含めた指標を設け，個々のセキュリティ要件がどのレベルに位置付けられるかを明示しており，対策を取捨選択する際の参考になる．

- レベル 1: 全てのアプリケーションが満たすべきもの
- レベル 2: 機微なデータを扱うアプリケーションが満たすべきもの
- レベル 3: さらに高度な信頼性が求められるアプリケーションが満たすべきもの

これらのレベルをビジネスの用途に合わせて，使い分けることが求められている．

(3) SANS　アプリケーションセキュリティ調達基準[9]

SANS では，アプリケーションソフトの開発を依頼する場合に，納入前にコードの検査とセキュリティ上の弱点を調査して，不具合があった場合に，ソフトウェア作成者の責任で対処するための基準を提供している．

(4) IPA のガイドライン[7],[8]

IPA では，規格や基準の形態ではなくセキュアエンジニ

ⓒ 2017 Information Processing Society of Japan

アリングとして,脆弱性の管理,セキュリティプロトコル,セキュアプログラミング,セキュア API などの情報を提供している.
特に,アプリケーションに特化したものとして,「安全な WEB サイトの作り方(改訂第 7 版)」が挙げられる.これらは,全て開発のためのガイドラインであり,運用面については触れていない.
一方,「WEB 健康診断仕様」は,地方公共団体が運営する WEB サイトに対して,基本的な脆弱性対策ができているかをチェックするためのものとして開発された.これにより運用中の WEB アプリケーションの脆弱性が診断できる.
以上,アプリケーションセキュリティの標準は開発や設計が中心であるが,運用中の脆弱性のマネジメントについてふれられている.

3. アプリケーション運用におけるセキュリティマネジメント

アプリケーションセキュリティ対策における意見として,大久保は,アプリケーションのセキュリティを実現するためには,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[13].
これによって,アプリケーションの開発でのセキュリティの見落としが減るものと期待されるが,運用面については述べていない.
一方,小柳は,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設計に系統的に組み入れようとするアプローチを紹介して,「アプリケーションでは,新規の開発の際に脆弱性を盛り込まないようにすることだけなく,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[12].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でのマネジメントで管理することの重要性を述べている.

なお,通常の開発と運用でアプリケーション仕様とセキュリティ仕様の関係をみると,開発の場面では,アプリケーション仕様が優先されることが多い.
一般の開発では「アプリケーション仕様 ＞ セキュリティ仕様」となっていることが多い.これは,企業では,ソフトウェアの性能や機能が優先されることを指しており,セキュリティ対策など後からやれば良いという立場が多く,そのため,一般的には「アプリケーション仕様 ＞ セキュリティ仕様」が重視されていると想定される.
また,ソフトウェアのセキュリティ仕様はアプリケーション仕様の中に取り込まれている.そのため開発ではセキュリティ対策によって向上するセキュリティは他の要素(実行速度,開発環境,開発コスト,導入コストなど)とのトレードオフとなることが多い.
すなわち,セキュリティを向上させるためには他の要素のコストを削減する必要があり,一方,セキュリティ対策には費用がかかるため,他の費用とのバランスで実装するセキュリティ対策が選ばれている.そのため,本当に必要なセキュリティ対策が選ばれることは少ない.

一方,想定されるリスクを許容可能な範囲に収めるために必要なセキュリティ対策を実施するのがリスクマネジメントである.このリスクマネジメントからは,「セキュリティ仕様 ＞ アプリケーション仕様」となる逆転が発生することが起きる.
これは「許容できないリスク」がある場合には,リスクを低減するために対策せざるを得ないため,である.例えば,WEB アプリケーションの開発では,クロスサイトスクリプティングなどの対策をとらないという選択肢はとれない(これを実施しなければ,確実に外部から攻撃されるので,このようなリスクを許容することができない)ためである.
なお,これらの「許容できないリスク」は多くのシステムで項目が共通しており,既存のガイドラインなどに記載されている.しかし,開発現場では,コストとの関係でアプリケーションとして採用されないこともある.すなわち,企業などでは,まだまだ,開発に対するコストの観点から,セキュリティ対策が実施されず,「アプリケーション仕様 ＞ セキュリティ仕様」となっているため,開発では,対策されていないセキュリティのリスクが残されたままとなる.
これらのアプリケーションの開発での残存リスクに対しては,運用段階の対策でカバーせざるを得ない(上記のようなクロスサイトスクリプティングなどの未対策のケースでは,WAF などを用いて対応することになる).
このように,セキュリティが軽視されることを防ぐためには,規格やガイドラインなどを用いて開発と運用面でのバランスがとれたセキュリティ対策を考えていくことが重要である.

4. セキュリティマネジメントの規格

前章で述べてように,小柳は運用面でのセキュリティマネジメントの重要性も述べている[12].ところが,ISO/IEC27034 では,マネジメントの面からのアプリケーションセキュリティを論じていない.これは,運用面のセキュリティの規格として, ISMS 認証の要求規格の ISO/IEC27001 及び 27002 がある.そこで,本章ではセキュリティマネジメントの国際規格である ISO/IEC27001(JIS Q27001)のアプリケーションセキュリティに関する管理策

について述べる．

4.1 JIS Q 27001:2014[2]

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 2　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．ISO/IEC27034 などの規格と異なり，アプリケーションを運用の各々の段階ごとに何を確認すればよいのか，どのような手順が必要かなどが例挙され，実用的なものとなっている．さらに JIS Q 27002 の実施の手引きにおいて現場で必要となる実施の手引きが述べられている．運用面からは，IJIS Q 27001・JIS Q 27002 をベースにするのが良いと考える．

なお，以下ではこの規格の利用者について述べる．

4.2 日本の ISMS 認証取得状況

ISO27001 認証取得状況調査のうち，日本は世界で最も多く認証を取得している．

ISO が発表した ISO Survey 2015 (ISMS)の認証取得状況の結果は下記の通りである．[5]

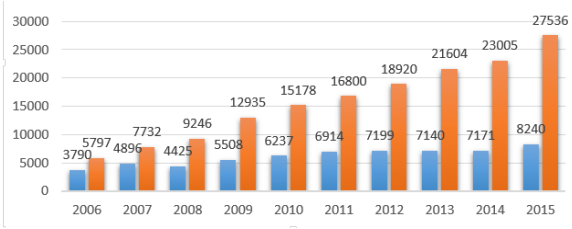

図 2　2015 年 ISMS 認証取得国 TOP 10

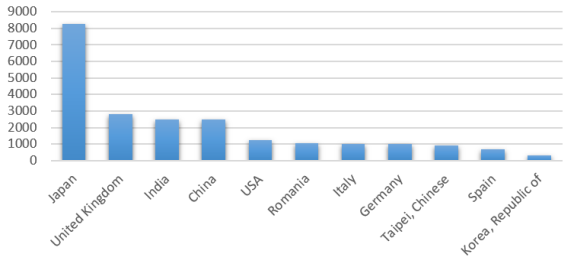

図 3　ISO/IEC 27001 取得状況比較

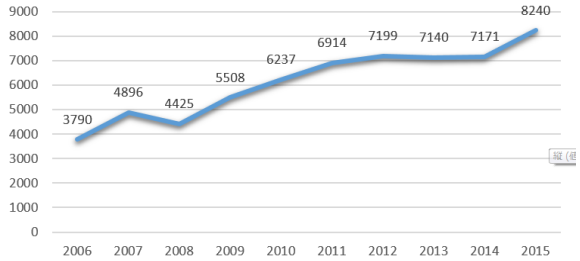

図 4　日本の ISMS 取得状況

日本における ISMS 認証の取得率は，他の国に比べて圧倒的に多いことがわかる．

すなわち，多くの組織が ISO/IEC27001 の運用のアプリケーションセキュリティ対策をベースにしていると考えられる．

5. 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

原田研究室では，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）に対して 2016 年度「情報セキュリティ調査」を実施している．その結果 544 件（12%）の回答が得られた．その中で，ウェブアプリケーションやモバイルアプリ等に関するセキュリティ対策の実施状況についても調査している．

本研究では，以下の項目について調査した．

表 3　アプリケーションセキュリティに関するアンケート項目

[Q39]. 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）	
1	CIO または CISO
2	ソフトウェア開発責任者
3	品質保証責任者
4	システム運用部門の責任者
5	不明・わからない
6	その他

[Q40]. 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．（○印はひとつだけ）	
1	全て管理できている
2	概ね管理できている
3	あまり管理できていない
4	全く管理できていない
5	不明・わからない
[Q41]. 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）	
1	独自開発
2	第三者（外注）の開発
3	パッケージソフトウェアの導入
4	その他
[Q42]. 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．（○印はひとつだけ）	
1	非常に増加している
2	増加している
3	変化はない
4	減少している
5	非常に減少している
6	不明・わからない
[Q43]. アプリケーションセキュリティのリスク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．（○はひとつだけ）	
1	ブランドの保護
2	情報漏えいの防止
3	業務の中断時間の抑制
4	その他
[Q44]. 脆弱性のあるアプリケーションのリスクへの対策として何を実施していますか．（複数選択可）	
1	開発者向けのセキュアコーディング教育の実施
2	セキュアコーディングガイドの提供
3	開発段階の脆弱性診断
4	ソースコードレベルの脆弱性検査
5	運用段階での脆弱性診断
6	外部専門会社の脆弱性診断
7	実施していない
8	その他
[Q45]. 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）	
1	十分な予算が確保できない
2	アプリケーションの脆弱性の増加
3	専門知識の不足
4	リーダーシップの不足
5	テストツールの不足
6	組織内での優先順位が低い
7	アプリケーションリリースへの抵抗感
8	その他
9	特にない

その結果を図５～図９に示す．

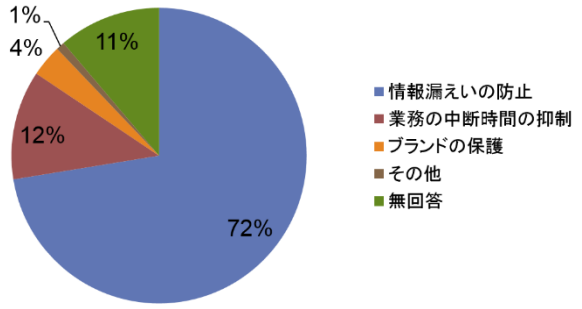

図 5　アプリケーションセキュリティにおけるリスク管理で重視　しているもの(N=544)

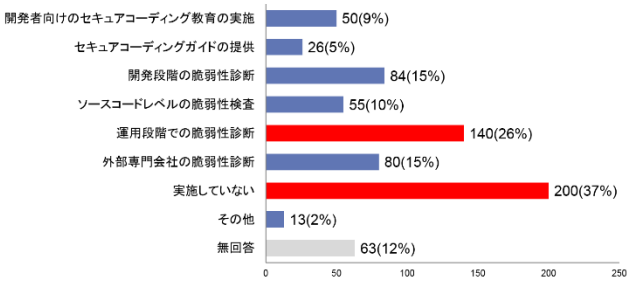

図 6　アプリケーションのリスク対策状況(N=544，複数選択)

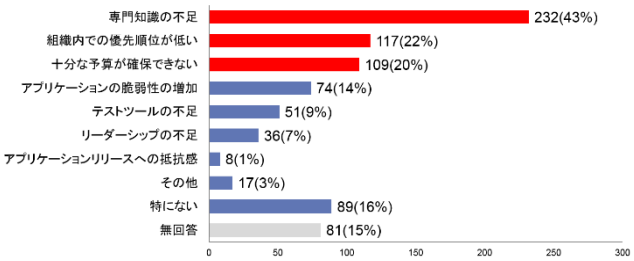

図 7　アプリケーションセキュリティのリスク管理ができない理由(N=544，複数選択)

アプリケーションセキュリティのリスク管理に関するアンケート単純集計の結果からは次のことが分かる．

- 図５からはアプリケーションセキュリティにおけるリスク管理で組織が重視しているものは，情報漏えいの防止（72%）である．
- 図６からは，開発段階から運用段階におけるアプリケーションのリスク対策は，「実施していない」が 37%を占め，「運用段階での脆弱性診断」が 26%であった．
- 図７からは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 43%，「組織内での優先順位が低い」が 22%，「十分な予算が確保できない」が 20%であった．

ⓒ 2017 Information Processing Society of Japan

図 6 からは，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 ）に分かれている．
すなわち，開発段階の対策（39%），運用段階の対策（41%），実施していない（37%）の結果が得られた．この中で開発段階と運用段階の対策がほぼ同様に重要と考えていることが分かった．

6. 今後の研究に向けて

6.1 これまでの検討状況

本稿では，まず，WEB アプリケーションのセキュリティ対策についての様々な規格や標準，先行研究などを確認した．アプリケーションセキュリティは大きく開発段階のセキュリティ対策と運用段階のセキュリティ対策が存在することがわかった．また，規格などは開発に偏っており，マネジメントについてふれているものは少ない．結局は，運用面でのアプリケーションセキュリティについては，ISMS などのマネジメント規格によらざるを得ないことが分かった．また，ISMS の管理策の中でもアプリケーションセキュリティにおける対策は，開発段階の対策と運用段階の対策が存在する．そこで，アンケートを実施して，企業の利用状況を述べた（Q44 及び図 5）．この結果からは，企業においては，開発段階の対策と運用段階の対策が同様に実施されているという傾向が見られた．
アプリケーションセキュリティ対策においては，開発段階からのアプリケーションのセキュリティ対策に重点を置かれているが，セキュリティマネジメントを通じた運用段階でのアプリケーションセキュリティ対策も重要であることが分かった．今後の研究では，あまり，検討がなされていない運用段階のセキュリティマネジメントについて検討していくことにしたい．

6.2 ポスターセッションで議論したいこと

本研究では，今後，アプリケーションセキュリティについて研究を進めるにあたり，次のことを検討している．以下について，議論したい．

- 設計・開発・導入・運用・委託の各フェーズにおけるアプリケーションセキュリティの対策について，最も重視すべきフェーズはあるのか
- 開発におけるアプリケーションセキュリティを高めれば，運用におけるアプリケーションセキュリティは減少するといえるのか．
- 運用におけるアプリケーションセキュリティのリスク対策は，十分といえるのか
- アプリケーションセキュリティのリスク対策には，専門家を増やすことや組織内での優先順位，予算の手当ができれば十分といえるのか
- 現在の ISO などのガイドラインは十分と言えるのか．また，ガイドライン間での関連性が明確でない．相互のマッピングなどが必要ではないか
- アプリケーションセキュリティの対策について，例えば，ソフトウェアのセキュリティレベルを外部機関が評価して認定するなどの制度を設けてはどうか

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] Ponemon Institute LLC, 「How to Make Application Security a Strategically Managed Discipline」, 2016 年 3 月
[2] 経済産業省, 「JIS Q27001-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
[3] 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(SP800-64 Revision 2)」, 2008, https://www.ipa.go.jp/files/000025343.pdf
[4] 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修士論文）
[5] ISO, ISO Survey 2015 (ISO 27001), http://www.iso.org/iso/iso_27001_iso_survey2015.xls
[6] 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
[7] 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
[8] IPA, 「WEB 健康診断仕様」, 2015, https://www.ipa.go.jp/files/000017319.pdf
[9] SANS, アプリケーションセキュリティ調達基準, 2009, https://software-security.sans.org/media/appseccontract/appseccontract-japanese.pdf
[10] OWASP, Application Security Verification Standard 3.0, 2015, https://www.jpcert.or.jp/securecoding/OWASP_ASVS_20160623.pdf
[11] アプリケーション・セキュリティー・リスクに鈍感な企業たち, 2016 年 5 月 16 日, https://asmarterplanet.com/jp-security/blog/2016/05/application_security_risks.html
[12] 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

ⓒ 2017 Information Processing Society of Japan

[13] 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
[14] 中尾 康二, ISO/IEC 27000 関連規格の最新動向, http://www.jnsa.org/seminar/2009/0127nsf2009/data/B1_Nakao.pdf, 2009
[15] http://e-words.jp/w/アプリケーションソフト.html “論文誌ジャーナルおよび JIP の査読のシングルブラインド制への移行について”. https://www.ipsj.or.jp/journal/info/jour_topics/topi44.html, (参照 2016-02-20).

ⓒ 2017 Information Processing Society of Japan