

番号	分類	英語タイトル	日本語タイトル	IPCERTリンク [1]	概要	概要を記載した参考文献 タイトル/更新日	2015年度からの更新内容
1	Developer / Builder 向けのチェックシート	3rd Party Javascript Management Cheat Sheet	サードパーティ-Javascriptの利用におけるセキュリティ対策に関するチェックシート	—	サードパーティ-Javascriptを読み込む際の主要なリスクを3点挙げている。また、サードパーティ-Javascriptをデプロイする際のアーキテクチャ及びセキュリティ対策として考慮すべき事項について紹介している。	2016/08/30	新規追加
2		Access Control Cheat Sheet	アクセス制御に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/AccessControl.html	Webアプリケーションのアクセス制御について、種類ごとにベストプラクティス、注意点、各言語における具体的な実装手法等を紹介している。	2016/6/5	分類変更(ドラフト⇒デベロッパビルダー)
3		AJAX Security Cheat Sheet	AJAXの実装に関するチェックシート	—	AJAXを扱う際にクライアントサイド及びサーバーサイドにおいて考慮すべき事項について紹介している。	2016/02/21	新規追加
4		Authentication Cheat Sheet	Webアプリの認証に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/Authentication.html	Webアプリにおける認証機能の設計時に留意すべき事項(例: パスワードの複雑性、パスワードのセキュリティ送信手法、多要素認証の適用など)について紹介している。	2015/08/11	—
5		Bean Validation Introduction	ビーンバリデーションに関するチェックシート	—	Javaのバリデーションチェック手法の中から、ドメインモデルを採用していることから、重複作業を減らし、一貫性を保証できるビーンバリデーションについて紹介している。	2016/07/11	新規追加
6		Choosing and Using Security Questions Cheat Sheet	ユーザがパスワードを忘れた場合の措置としての秘密の質問の実装に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/ChoosingAndUsingSecurityQuestions.html	パスワードを忘れた際に利用する「秘密の質問」をWebアプリケーションに実装する際のベストプラクティスについて紹介している。	2015/07/18	—
7		Clickjacking Defense Cheat Sheet	クリックジャッキング対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/ClickjackingDefense.html	クリックジャッキングの脆弱性への対策として、(X-Frame-Options)ヘッダーの利用とフレームブレイキングスクリプトの実装について紹介している。	2015/02/11	—
8		C-Based Toolchain Hardening Cheat Sheet	C, C++, Objective-C言語における開発環境に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/c-BasedToolchainHardening.html	C, C++, Objective-C言語における開発環境において、信頼性の高い安全なコードを提供するために考慮しなければならないことを紹介している。より踏み込んだ内容については、C-Based Toolchain Hardening (https://www.owasp.org/index.php/C-Based_Toolchain_Hardening)を参照のこと。	2015/07/18	—
9		Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet	CSRF対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/cross-site-request-forgery-prevention.html	CSRFの脆弱性への対策として、トークンを利用する対策について紹介する。トークンリファレンスヘッダまたはリクエストボディを確認するといった補足的な対策を紹介している。また、ウェブアプリ利用時にはログアウトするなどユーザができる対策についても紹介している。	2015/07/18	—
10		Cryptographic Storage Cheat Sheet	保存データの暗号化に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/CryptographicStorage.html	クレジットカード情報などの機密性の高いデータを保存する際に考慮すべき事項について機密レベルで簡単に紹介している。	2015/09/04	—
11		Deserialization Cheat Sheet	デシリアライゼーションに関するチェックシート	—	デシリアライズする際にDoS攻撃や悪意のある攻撃コードが実行されることを防ぐ方法について、特にJavaに焦点を当てて紹介している。	2016/06/29	新規追加
12		DOM based XSS Prevention Cheat Sheet	DOMベースのXSS対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/DOMbasedXSSPrevention.html	XSSの脆弱性は①反射型②持続型③DOMベースの3パターンに大別されるが、本チェックシートにおいては、XSS対策に関するチェックシート(https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)では言及されていない③DOMベースのXSSの脆弱性への対策手法について紹介している。	2015/07/27	—
13		Forgot Password Cheat Sheet	ユーザがパスワードを忘れた場合の措置に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/ForgotPassword.html	ユーザがパスワードを忘れた場合の措置として、Webアプリケーションにはパスワードリセット機能の実装が必要である。本チェックシートでは、セキュアな方法でパスワードリセット機能を実装する方法について紹介している。	2015/09/15	—
14		HTML5 Security Cheat Sheet	HTML5におけるセキュリティ対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/HTML5Security.html	HTML5で新たに追加された機能に対してセキュリティ面で注意しなければならないポイント新たに追加されたセキュリティを高める機能を紹介している。	2015/09/09	—
15		HTTP Strict Transport Security Cheat Sheet	HTTP Strict Transport Security (HSTS)に関するチェックシート	—	HTTP Strict Transport Security (HSTS)について説明するとともに、HSTSによって防げる脅威やブラウザの対応状況等について紹介している。	2016/08/10	新規追加
16		Input Validation Cheat Sheet	ホワイトリストによる入力値バリデーションに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/InputValidation.html	Webアプリのセキュリティ機能として、入力値に対するバリデーションチェックがある。本チェックシートでは、ホワイトリストによるバリデーションチェックを用いて郵便番号を検証する事例を紹介している。	2015/07/18	—
17		JAAS Cheat Sheet	JAAS認証に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/JAAS.html	JAAS (Java Authentication and Authorization Services) 認証の概要とLoginModule及びCallbackHandlerについて紹介している。	2015/07/18	—
18		LDAP Injection Prevention Cheat Sheet	LDAPインジェクション対策に関するチェックシート	—	LDAPインジェクションの概要とエンコード関数やホワイトリストによるバリデーションチェック等による対策方法について紹介している。	2015/10/29	新規追加
19		Logging Cheat Sheet	Webアプリにおけるログの取得などに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/Logging.html	Webアプリにおける特にセキュリティに関するアプリケーションログについて、具体的にどういったイベントのログを取得すべきか、取得する内容の制限はかかると紹介している。合わせて、ログの取得に関して設計から運用時まで各工程において考慮すべき点について紹介している。	2015/07/18	—
20		Mass Assignment Cheat Sheet	Mass Assignment脆弱性対策に関するチェックシート	—	Mass Assignmentの脆弱性が発生してしまう原因について例を用いて説明するとともに、Data Transfer Objects (DTOs) による対策、各言語におけるホワイトリスト及びブラックリストによる対策方法について紹介している。	2016/03/10	新規追加
21		NET Security Cheat Sheet	.NETフレームワークにおけるセキュリティ対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/DoNotNETSecurity.html	.NETフレームワークを用いて開発を行う際に考慮したいセキュリティの観点について紹介している。	2015/03/29	—
22		OWASP Top Ten 2013における10の脅威への対策及びベストプラクティスに関するチェックシート	OWASP Top Ten 2013における10の脅威への対策及びベストプラクティスに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/OWASP_Top_Ten_2013.html	OWASP Top Ten 2013における10の脅威への対策方法及び当該対策が適切に実施されているかを検証するためのテスト手法(詳細はリンク先のOWASP Testing guideを参照。)について紹介している。	2015/08/24	—
23		Password Storage Cheat Sheet	パスワードなどの保持に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/PasswordStorage.html	パスワード、秘密の質問やこれらに類する重要な情報はSQLインジェクション攻撃やクエリインジェクションの攻撃により、漏洩してしまう可能性がある。そこで、本チェックシートでは、これら重要な情報を適切に保持し、漏洩リスクを低減する方法について紹介している。	2015/07/18	—
24		Pinning Cheat Sheet	公開鍵ピンニングに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/Pinning.html	証明書が公開鍵のピンニングについて説明するとともに、Android, iOS, .Net, OpenSSLにおけるピンニングの実現手法についてサンプルコード(ダウンロード可能)を用いて紹介している。詳細はCertificate and Public Key Pinningプロジェクト(https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinningを参照のこと)。	2015/07/18	—
25		Query Parameterization Cheat Sheet	クエリパラメータに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/QueryParameterization.html	SQLインジェクション対策としてのプリペAREDステートメントを利用する手法がベストプラクティスにおけるベストプラクティスである。本チェックシートでは、この手法に関するコード例を言語ごとに紹介している。	2014/11/21	—
26		Ruby on Rails Cheatsheet	Ruby on Railsにおけるセキュリティ対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/RubyOnRails.html	Railsセキュリティガイドを補完しており、Ruby on Railsの開発者のためにコマンドインジェクション、SQLインジェクション、XSSなどの脆弱性に対する基本的なセキュリティ対策を紹介している。	2015/03/09	—
27		REST Security Cheat Sheet	RESTfulなサービスの実装に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/RESTSecurity.html	RESTfulなサービスを実装する際に留意すべき作法(認証及びセッション管理、認可、入力値検証、エンコーディング、暗号化)について紹介している。	2015/07/24	—
28		Session Management Cheat Sheet	セッション管理などに関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/SessionManagement.html	Webアプリに接続するユーザを識別するためのセッションを用いてユーザ認証、セッション管理、アクセス制御を行う際に、セキュリティを高める方法について紹介している。合わせて、セッションに対する攻撃を検知する方法やWAFを用いて攻撃を防ぐといった概念についても紹介している。	2015/07/18	—
29		SAML Security Cheat Sheet	SAMLを用いたSSOの実装に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/SAMLSecurity.html	リダイレクト / POST バインディングを利用したWebブラウザにおけるSAML / SSO (Security Assertion Markup Language / Single Sign On) プロファイルについて紹介している。	2015/09/04	—
30		SQL Injection Prevention Cheat Sheet	SQLインジェクション対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/SQLInjectionPrevention.html	SQLインジェクションの対策手法として、プリペAREDステートメントの利用、ブラックリストの利用、入力値のエスケープについて具体的なコードを交えつつ紹介するとともに、保険的な対策である情報の最小化、ホワイトリストによる入力値の検証についても紹介している。	2015/07/28	—
31		Transaction Authorization Cheat Sheet	トランザクション認証に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/TransactionAuthorization.html	ワンタイムパスワードやスマートカードによるデジタル署名などを用いたトランザクション認証の適切な実装手法について紹介している。	2015/07/18	—
32		Transport Layer Protection Cheat Sheet	トランスポート層におけるセキュリティ対策に関するチェックシート	—	SSL/TLS技術の基礎を紹介している。合わせて、SSL/TLS技術を用いてサーバ認証、サーバ認証、プロトコル/暗号構成を適切に実装するためのルールを紹介している。	2015/07/28	—
33		Unvalidated Redirects and Forwards Cheat Sheet	リダイレクト及び転送機能の実装手法に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/UnvalidatedRedirectsAndForwards.html	JavaやPHPなどの各言語におけるリダイレクト及び転送機能の安全な実装手法について、危険な実装手法も交えつつ紹介している。	2015/08/21	—
34		User Privacy Protection Cheat Sheet	プライバシー権などに対する脅威の軽減手法に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/UserPrivacyProtection.html	SNSやコミュニケーションプラットフォームが提供するプライバシー権や匿名情報などの機密情報に対する脅威を軽減するためのデータの暗号化やHTTPSを用いたセキュアな通信の確立、認証方式などの基本的な手法について紹介している。	2015/07/18	—
35		Web Service Security Cheat Sheet	Webサービスにおけるセキュリティ対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/WebServiceSecurity.html	Webサービスを構築する上で考慮すべきポイント(TLSを使うなどの認証時の注意点、DDoSやブルートフォース攻撃を緩和するための対策、実施すべきバリデーション、ワイルドカードや可用性など)について紹介している。	2015/08/04	—
36		XSS (Cross Site Scripting) Prevention Cheat Sheet	XSS対策に関するチェックシート	https://pcertcc.github.io/OwaspDocuments/CheatSheet/XSSPrevention.html	反射型及び持続型のXSSに対する根本的な対策7と保険的な対策4点を紹介している。DOMベースのXSSは、DOMベースのXSS対策に関するチェックシート(https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet)を参照のこと。	2015/09/23	—

順番	分類	英語タイトル	日本語タイトル	JPCERTリンク [1]	概要	概要を記載した参考文献の更新日	2015年度からの更新内容
37		XML External Entity (XXE) Prevention Cheat Sheet	XML External Entity (XXE) 攻撃対策に関するシート	---	XMLパースを利用し、機密情報の搾取、ポートスキャン及びDoS攻撃を引き起こすXML External Entity (XXE)の概要について説明することに加え、C/C++、Java、.NET等の各言語における対策方法について紹介している。合わせてXML External Entity (XXE) Processing (https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)を参照のこと	2016/05/31	新規追加
38	Assessment / Breaker向けのシート	Attack Surface Analysis Cheat Sheet	Webアプリへの攻撃に対する脆弱性分析に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/AttackSurfaceAnalysis.html	外部からのWebアプリへの攻撃に対して、シンプラな表面分析(「サーフェイス分析」)を行うことにより、リスクを評価したうえで、Webアプリのどの部分を見直すべきか、又は脆弱性診断を行うべきかを最小限の方法で判断する手法について紹介している。	2015/07/18	---
39		XSS Filter Evasion Cheat Sheet	XSSの脆弱性を検知するのに有用な文字列に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/XSSFilterEvasion.html	XSSの脆弱性を検知するのに有用な具体的な文字列について具体的に紹介している。	2015/08/01	---
40		REST Assessment Cheat Sheet	WebサービスにおけるREST対応の詳細に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/RESTAssessment.html	WebサービスにおいてREST(Representational State Transfer)対応ができていないかを評価する観点について紹介している。	2015/07/18	---
41		Web Service Security Testing Cheat Sheet	Webサービスに対するセキュリティテストにおけるチェック観点に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/WebApplicationSecurityTesting.html	Webサービスに対するセキュリティテストにおけるチェック観点について概念レベルで紹介している。	2015/08/24	---
42	モバイルに関するシート	Android Testing Cheat Sheet	Androidアプリに対するテストに関するシート	---	Androidアプリに対するテストで確認すべき項目について、OWASP Mobile Top10(https://www.owasp.org/index.php/OWASP_Mobile_Security_Project)に掲載されているリスクと対応づけて紹介している。	2016/08/08	新規追加
43		iOS Developer Cheat Sheet	iOSアプリにおけるリスクとその対策に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/iOSDeveloper.html	iOSアプリを開発する際に留意すべきOWASP Mobile Top 10 Risk-2014(最新版は2014)に対応するリスク及びその対策について紹介している。	2015/07/18	---
44		Mobile Jailbreaking Cheat Sheet	Jailbreakingなどに関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/MobileJailbreaking.html	iOSにおけるJailbreaking、AndroidにおけるRoot化、WindowsOSにおけるunlockingに関する基礎的な事項及び各処理を実行するツールを紹介している。また、各処理を実行することによりリスクや、実行を妨げる方法について技術的、非技術的な双方の側面から紹介している。	2015/07/18	---
45	OpSec / Defender向けのシート	Virtual Patching Cheat Sheet	仮想パッチに関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/VirtualPatching.html	ソースコードを修正できない場合の副次的な対策としての仮想パッチ(WAF・IDSといったセキュリティ対策デバイス、Webサーバプラグイン、アプリケーションレイヤ/サーバ)の適切な運用に関する継続的な運用方法について紹介している。	2014/11/04	---
46	ドラフト版のシート	Application Security Architecture Cheat Sheet	[ドラフト]アプリケーションセキュリティ設計及びレビューに関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/ApplicationSecurityArchitecture.html	Webアプリのセキュリティアーキテクチャの初期設計やレビューにおける要求事項(ビジネス要求、インフラ要求、アプリ要求、セキュリティプログラム要求)に関する豆知識を紹介している。	2015/09/12	---
47		Business Logic Security Cheat Sheet	[ドラフト]ビジネスロジックの脆弱性対策に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/BusinessLogicSecurity.html	認証、認可、アクセス制御などの不備を突撃ではなく、正常な手順を踏みつつも利益を得る(例えば注文処理実行直後に注文をキャンセルした場合にシステム上で注文は不成立となるものなど)が商品価値を損ないてしまふなど、といったビジネスロジックに起因する脆弱性について紹介している。合わせて、それらの脆弱性を作り込まない方法や、脆弱性がないことを確認するテスト手法についても紹介している。	2014/06/05	---
48		Command Injection Defense Cheat Sheet	[ドラフト]コマンドインジェクション対策に関するシート	---	コマンドインジェクションの脆弱性の概要及びその対策について紹介している。 (※概要記載時点でほとんど中身が書いていないため、タイトルから推測した簡易な記載としている。)	2016/08/09	新規追加
49		Credential Stuffing Prevention Cheat Sheet	[ドラフト]パスワードリスト攻撃等のブルートフォース攻撃対策に関するシート	---	パスワードリスト攻撃等のブルートフォース攻撃対策として、多要素認証の実装、多段階認証の実装、IPアドレスの活用等の対策手法を紹介している。	2016/09/20	新規追加
50		PHP Security Cheat Sheet	[ドラフト]PHPにおけるセキュリティ対策に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/PHPSecurity.html	PHP開発者が考慮すべきセキュリティ向上のための秘訣としてSQLインジェクション、XSSなどの種々の脆弱性に対する対策、言語独自及びフレームワークにおける脆弱性に対する対策、認証・認可の実装やPHPの設定を行う上で留意する事項などについて紹介している。	2015/06/19	---
51		Regular Expression Security Cheatsheet	[ドラフト]正規表現に関するシート	---	正規表現の実装例を紹介しているGithubページ(https://github.com/attackerkan/regex-security-cheatsheet/tree/master/RegexSecurityParser)や不適切な正規表現の実装例を紹介しているGithubページ(https://github.com/attackerkan/regex-security-cheatsheet)を紹介している。	2016/10/09	新規追加
52		Secure Coding Cheat Sheet	[ドラフト]セキュアコーディングに関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/SecureCoding.html	認証、セッション管理、アクセス制御など、セキュアなシステムを開発する際に留意すべき事項について紹介している。	2015/06/22	---
53		Secure SDLC Cheat Sheet	[ドラフト]セキュアSDLCの実現に関するシート	---	組織におけるソフトウェア開発プロセスにセキュリティの観点を組み込み、OpenSAMM(http://www.opensamm.org/downloads/SAMM-1.0.pdf)における成熟度Level1を実現する方法について紹介している。	2012/12/31	---
54		Threat Modeling Cheat Sheet	[ドラフト]Webアプリに対する脅威モデリングに関するシート	---	Webアプリに対するセキュリティ上の脅威への対策方法(守るべきものの特定、攻撃者の意図、リスクの洗い出し・評価、リスクへの対応)について紹介している。	2015/08/31	---
55		Web Application Security Testing Cheat Sheet	[ドラフト]Webアプリに対してブラックボックステストを実施する際に確認すべき観点に関するシート	---	Webアプリに対してブラックボックステストを実施する際に確認すべき観点についてチェックリスト形式で紹介している。	2015/09/17	---
56		Gralis Secure Code Review Cheat Sheet	[ドラフト]Gralisにおけるコードレビューに関するシート	---	Groovy言語を使用するオープンソースのフレームワークであるGralisにおけるコードレビューの際に確認すべき事項について紹介している。	2013/01/02	---
57		iOS Application Security Testing Cheat Sheet	[ドラフト]iOSアプリに対してテストを実施する際に確認すべき観点に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/iOSApplicationSecurity.html	iOSアプリに対してテストを実施する際に確認すべき観点についてチェックリスト形式で紹介するとともに、テストに利用可能なツールについて紹介している。	2015/08/24	---
58		Key Management Cheat Sheet	[ドラフト]暗号化に利用する鍵の管理に関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/KeyManagement.html	暗号化に利用する鍵を管理する際に留意すべき事項について紹介するとともに、鍵管理におけるベストプラクティスについて紹介している。	2015/07/21	---
59		Insecure Direct Object Reference Prevention Cheat Sheet	[ドラフト]オブジェクト直接参照の危険な実装の防止に関するシート	---	オブジェクト直接参照の危険な実装の防止するための方法について紹介している。 (※概要記載時点でほとんど中身が書いていないため、タイトルから推測した簡易な記載としている。)	2014/01/21	---
60		Content Security Policy Cheat Sheet	[ドラフト]CSPに関するシート	https://jpcertcc.github.io/OWASPdocuments/CheatSheet/s/ContentSecurityPolicy.html	CSP(コンテンツセキュリティポリシー)の概要を紹介し、CSPを用いてXSSなどの脆弱性による攻撃の被害を軽減する方法を紹介している。	2015/06/09	---

[1] リンク先の日本語タイトルが左列の日本語タイトルと異なる可能性があります