

OSC2013 Kansai@Kyoto



～ヒトの振り返り見て我が振り返り直せ～ 脆弱性事例に学ぶJavaセキュアコーディング

JPCERT/CC 情報流通対策グループ
戸田 洋三 (yozo.toda@jpcert.or.jp)

https://www.jpccert.or.jp/securecoding/materials-java-casestudies.html

4 ☆ Google

検索

最新情報を取得 (RSS | ...)

ング > Java アプリケーション脆弱性事例解説資料

Java アプリケーション脆弱性事例解説資料

最終更新: 2013-06-27

セキュアコーディングを学ぶための教材として活用していただくことを目的として、Java 言語で書かれたアプリケーションの脆弱性事例に関する解説資料を公開しています。

セキュアな Java アプリケーションの開発を目指すには、すでに知られている脆弱性の具体例を理解し、それ

公開日	タイトル	PDF	PGP 署名
2013-06-27	Apache Sling におけるサービス運用妨害(無限ループ)の脆弱性 (CVE-2012-2138)	1.52MB	PGP 署名
2013-06-27	Apache Struts2 における任意の Java メソッド実行の脆弱性 (CVE-2012-0838)	1.61MB	PGP 署名
2013-06-27	Blojsom におけるクロスサイトスクリプティングの脆弱性 (CVE-2006-4829)	1.80MB	PGP 署名
2013-06-27	MySQL Connector/J における SQL インジェクションの脆弱性 (JVN#59748723)	1.85MB	PGP 署名
2013-06-27	JBoss Application Server におけるディレクトリトラバーサル脆弱性 (CVE-2006-5750)	1.74MB	PGP 署名

Top^

6/27に公開
しました!

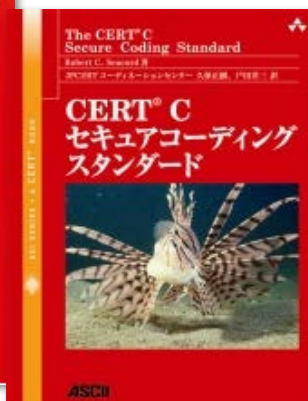
<http://www.jpccert.or.jp/securecoding/materials-java-casestudies.html>

JPCERT/CC 情報流通対策グループ 解析チーム リードアナリスト 戸田 洋三



<http://www.tomo.gr.jp/root/e9706.html>

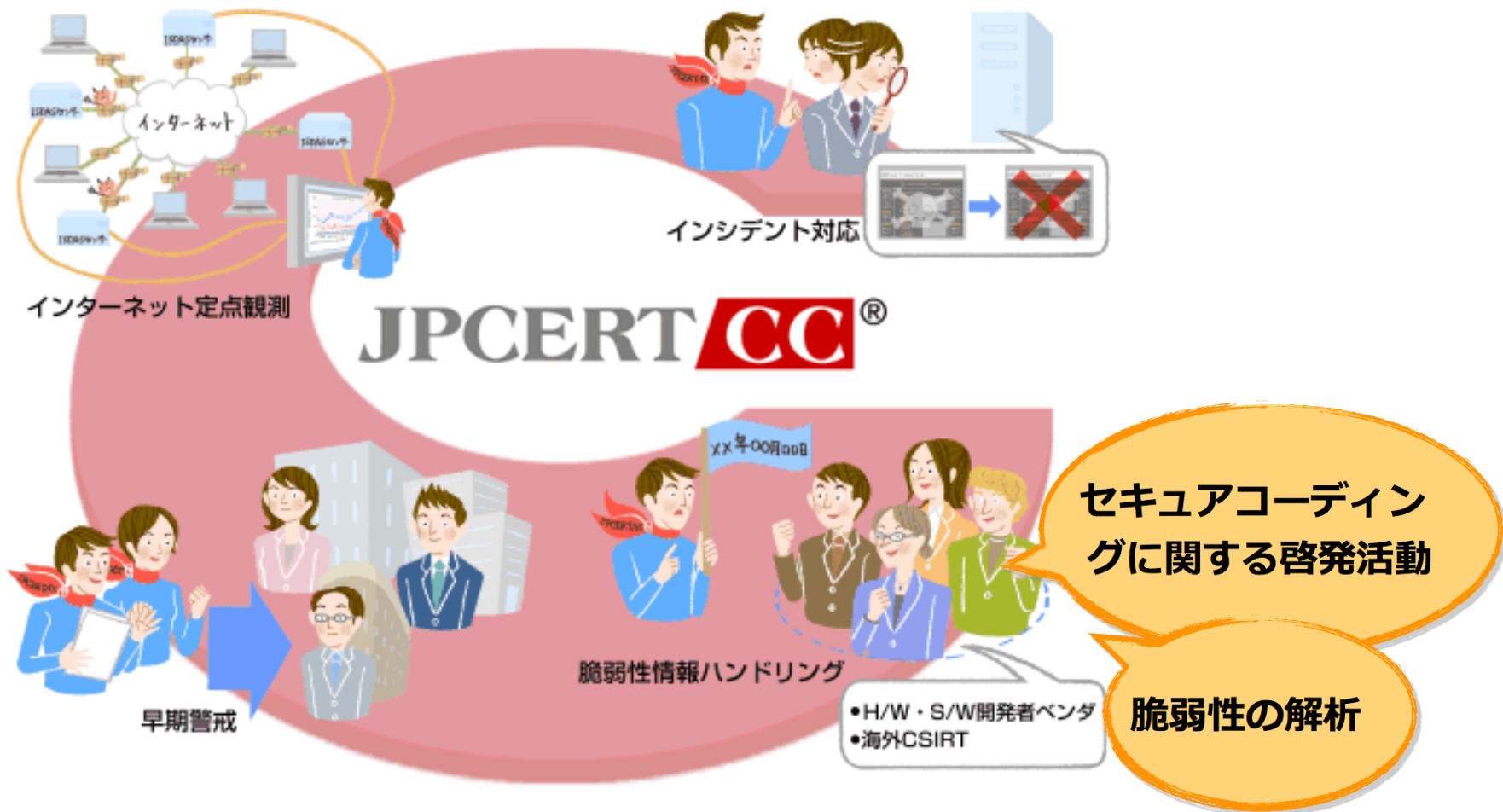
脆弱性情報分析, セキュアコーディング普及啓発活動..... に努めてます



JPCERT Coordination Center

日本における情報セキュリティ
対策活動の向上に取り組
んでいる組織

JPCERT/CCの主な活動



過去のOSC参加履歴 (セミナーを行ったもの)

- OSC2012@Fukuoka
 - Androidセキュアコーディング～安全なAndroidアプリ開発のための心得～
- OSC2011@Nagoya
 - セキュアコーディングノススメ(JAVA編)
- OSC2010@Hokkaido
 - あなたのコードにセキュアコーディングスタンダード
- OSC2009@Fukuoka
 - セキュアコーディングノススメ
- OSC2008@Tokyo/Spring
 - セキュアコーディングノススメ
- OSC2007@Fukuoka
 - セキュアコーディングノススメ
- OSC2007@Niigata
 - ソフトウェア脆弱性を取り巻く状況と対策
- OSC2007@Kansai
 - ソフトウェア脆弱性情報流通のこれまでとこれから
- OSC2005@Tokyo/Fall
 - ソフトウェア脆弱性情報流通への取り組み

本日の話題

- ✓なぜこのような資料を作ったのか
- ✓どんな資料があるの？
- ✓どんなふうに使えるの？



JAVA
DEPARTMENT

**なぜこのような資料をつくった
のか**

いまどきの脆弱性

- cve.mitre.org でキーワード検索してみました
(total CVEs: 56609)
 - arbitrary code: 12525
 - denial of service: 11741
 - XSS: 7552
 - buffer overflow: 6705
 - SQL injection: 5943
 - directory traversal: 2537

セキュアコーディングプロジェクトについて

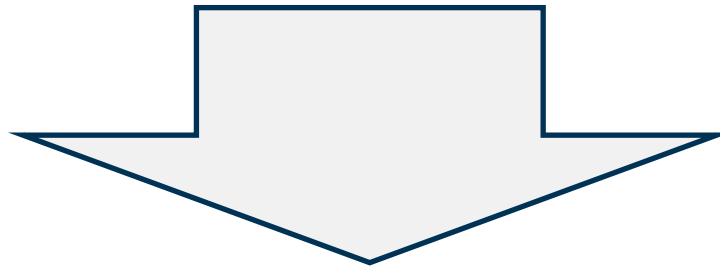
- セキュアなソフトウェア開発のための手法等の普及啓発
 - その結果として脆弱性の低減
- Web やセミナーを通じた技術情報提供

2006	書籍『C/C++セキュアコーディング』出版
2007	国内メーカー向けセキュアコーディングセミナー事業開始
2008	CERT C セキュアコーディングスタンダードWeb公開、無償セミナー等年間32回開催
2009	書籍『CERT Cセキュアコーディングスタンダード』出版、タイ、インドネシア、ベトナムにてセミナー
2010	地方セミナー、「OpenSAMM」翻訳、コードジン連載、静的解析ツール(rosechecker開発)、インド、ベトナム、フィリピン
2011	書籍『Javaセキュアコーディングスタンダード』出版・Web公開、Java/Androidのセキュアコーディングセミナー開始
2012	タイ、インドネシアでJava/Androidセキュアコーディングセミナー

セキュアコーディングの普及啓発には…

■ 具体的な事例紹介が有効

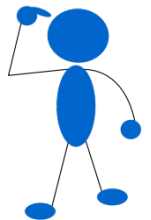
- コーディングルールの根拠
- 被害につながることを実感
- 攻撃者の視点に興味を持つ



より多くのJavaアプリの脆弱性事例と、
そこから得られる教訓を紹介する

配慮すべき(と考えた)ポイント

- 対象読者: セキュリティ方面に詳しくないJavaプログラマ
 - 興味をもって読めないネタ、理解できない技術解説はダメ
 - 専門家にしか受けられないような内容ではダメ
- 事例解説の理解し易さ、説得力
 - セキュリティ屋の言葉は使わない
 - NG: 「任意のコードが実行される可能性があります」
 - 実際の被害が分かり易く、プログラマの心を動かせること
 - 現場でいかにもやっつけてしまいそうな脆弱性は優先度高
 - 図・グラフ・表などビジュアル表現を活用する
 - 「読んで分かる」ではなく「見て分かる」ことが重要
 - 事例が偏らないようにサーバ系、webアプリ系、デスクトップ系それぞれから取り上げたい





JAVA
DEPARTMENT

どんな資料があるの？

**Apache Sling におけるサービス運用妨害
(無限ループ) の脆弱性**

Apache Struts 2 における任意の Java メソッド実行の脆弱性

Blojsom におけるクロスサイトスクリプティングの脆弱性

MySQL Connector/J における SQL インジェクションの脆弱性

JBoss Application Server におけるディレクトリトラバーサル脆弱性

Apache Sling におけるサービス運用妨害 (無限ループ) の脆弱性

- Webサイトのコンテンツ管理を目的としたオープンソースのWebフレームワーク
- コンテンツのコピー機能にサービス運用妨害 (DoS) 攻撃を受ける脆弱性
- コピー元とコピー先に同一のファイルパスを指定すると、無限ループが発生する
- 再帰的な処理であるコピー機能の実行前に、コピー対象が無限ループを起こさないことを確認する必要があった



Apache Struts 2 における任意の Java メソッド実行の脆弱性

- Java の Web アプリケーションを開発するためのオープンソースのフレームワーク
- 数値型の変数に対して文字列が送信されてきた際に発生する変換エラー処理に不備
- 送信する文字列を細工することで、任意の Java メソッドが実行可能となる
- エラー処理で扱うデータを、OGNL 式と解釈されないよう無害化する必要があった

StrutsTM

Blojsom におけるクロスサイトスクリプティングの脆弱性

- Java で書かれたブログシステム
- 入力文字列の処理に不備があり、クロスサイトスクリプティング攻撃が可能
- 処理結果(HTML形式)の出力時にHTMLエンコーディングを施すべきだった

The logo for Blojsom, featuring the word "blojsom" in a lowercase, sans-serif font. The letter "o" is replaced by a red circle with a white dot in the center, resembling an eye or a stylized letter.

MySQL Connector/J における SQL インジェクションの脆弱性

- MySQLデータベースにアクセスするためのドライバソフトウェア
- SQLクエリ文字列の処理に不備があり、SQLインジェクションが可能
- SQLのメタ文字に対するエスケープ処理を行った後で文字エンコーディングの変換を行っていた
- 最初に文字エンコーディングの変換を行うべき



JBoss Application Server におけるディレクトリトラバーサル脆弱性

- Java で書かれた web アプリを動作させるためのアプリケーションサーバ
- JMXコンソール経由のファイル操作処理にディレクトリトラバーサル脆弱性
- 引数として受け取ったパスを正規化すること、および、適切な場所を指すパスであることを検証すべきだった



Apache Sling におけるサービス運用妨害
(無限ループ) の脆弱性

Apache Struts 2 における任意の Java メ
ソッド実行の脆弱性

Blojsom は スクリプト
テイキングの脆弱性

MySQL Connector/J は
ジェクションの脆弱性

JBoss Application Server におけ
トリトラバーサル脆弱性

中身を
見てみよう!!



Apache ActiveMQ における認証不備

AtomicReferenceArray
イズ機能の脆弱性

Apache Commons ラ
SSLホスト名検証不備

Apache Axis2 に対す
Wrapping Attack

Spacewalk および Apache Tomcat におけるク
ロスサイトリクエストフォージェリの脆弱性

追加5件の
資料を現在
準備中。
乞うご期待!



JAVA
DEPARTMENT

どんなふうに使えるの？

自習用教材

- Java アプリを作れるようになったら次のステップとして
- Java セミナ資料も公開してるのでこちらもぜひ



Java セキュアコーディングセミナー資料

最終更新: 2013-06-27

これまでにJavaセキュアコーディングセミナーで使用した講義資料を公開しています。Javaアプリケーションの脆弱性事例の解説資料については[解説資料のページ](#)をご参照ください。

- オブジェクトの生成とセキュリティ
- 数値データの取扱いと入力値検査
- 入出力(File,Stream)と例外時の動作
- メソッドとセキュリティ

オブジェクトの生成とセキュリティ

クラス的设计とオブジェクトの取扱いをセキュアに行うためのポイントについて、オブジェクトの生成におけるセキュリティをテーマに解説します。

• 基礎概念のおさらい (クラス、シリアライズ、GC)

<https://www.jpccert.or.jp/securecoding/materials-java.html>

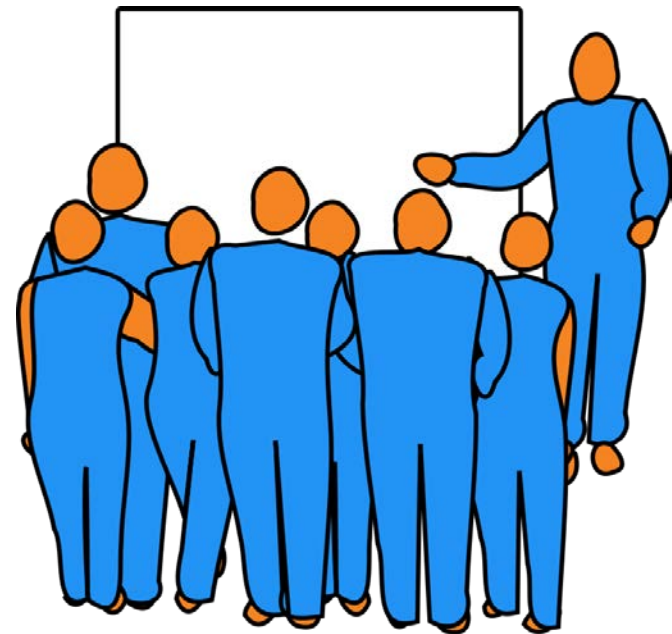
仲間内の勉強会資料

- 教材のひとつとしてどうぞ
- Java 세미나資料も活用してね
- 講師役がいちばん勉強になります



セミナーの参考資料に

- ご活用ください
- 引用や二次利用に関するお願いも確認してね



セミナーの参考資料に: 引用や二次利用について

著作権・引用や二次利用について

- 本資料の著作権はJPCERT/CCに帰属します。
- 本資料あるいはその一部を引用・転載・再配布する際は、引用元名、資料名および URL の明示をお願いします。

記載例

引用元：一般社団法人JPCERTコーディネーションセンター

Java アプリケーション脆弱性事例解説資料

Apache Sling におけるサービス運用妨害(無限ループ)の脆弱性

https://www.jpCERT.or.jp/research/materials-java-casestudies/No.1_Apache_Sling.pdf

- 本資料を引用・転載・再配布をする際は、引用先文書、時期、内容等の情報を、JPCERT コーディネーションセンター広報(office@jpcert.or.jp)までメールにてお知らせください。なお、この連絡により取得した個人情報は、別途定めるJPCERT コーディネーションセンターの「プライバシーポリシー」に則って取り扱います。

本資料の利用方法等に関するお問い合わせ

JPCERTコーディネーションセンター

広報担当

E-mail : office@jpcert.or.jp

本資料の技術的な内容に関するお問い合わせ

JPCERTコーディネーションセンター

セキュアコーディング担当

E-mail : secure-coding@jpcert.or.jp

各資料の最後のページに入れてあるよ。

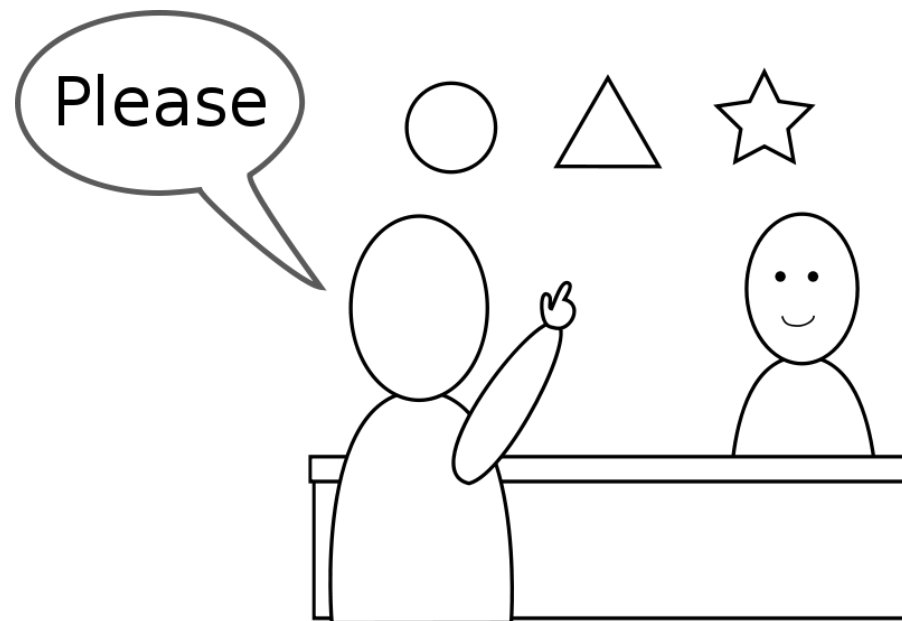


最後に...

■ご意見ちょうだい

—内容についてコメント

—どのような資料があるとうれしいですか?



付録

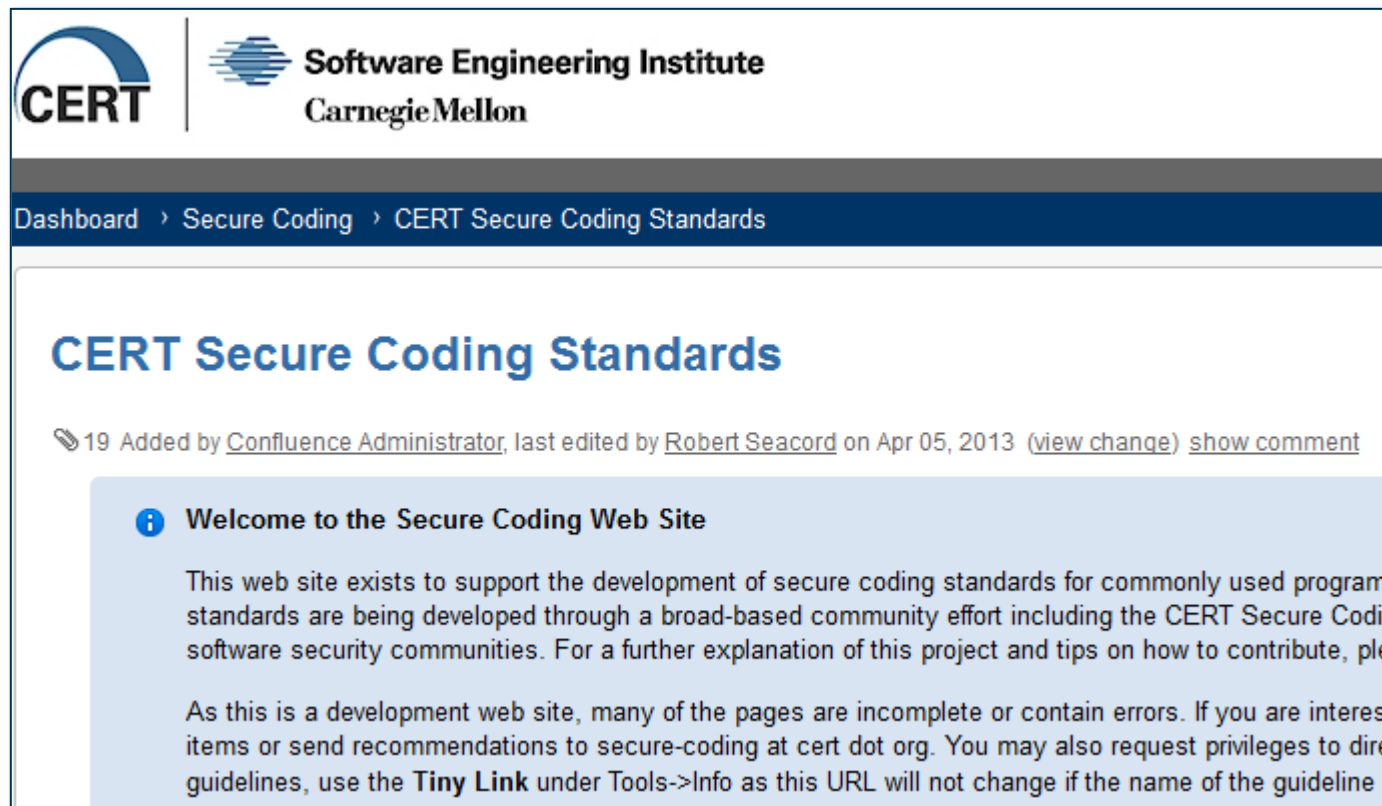
セキュアコーディングスタンダード


セキュアコーディングスタンダード

米国 CMU/SEI の the CERT Secure Coding Initiative
によるコーディングスタンダードシリーズ

<https://www.securecoding.cert.org/>


いまのところ、4種類
公開されています。




  **Software Engineering Institute**
Carnegie Mellon

Dashboard > Secure Coding > CERT Secure Coding Standards

CERT Secure Coding Standards

 19 Added by [Confluence Administrator](#), last edited by [Robert Seacord](#) on Apr 05, 2013 ([view change](#)) [show comment](#)

 **Welcome to the Secure Coding Web Site**

This web site exists to support the development of secure coding standards for commonly used program standards are being developed through a broad-based community effort including the CERT Secure Coding software security communities. For a further explanation of this project and tips on how to contribute, please see the guidelines.

As this is a development web site, many of the pages are incomplete or contain errors. If you are interested in contributing items or send recommendations to [secure-coding at cert dot org](mailto:secure-coding@cert.org). You may also request privileges to direct the development of guidelines, use the **Tiny Link** under Tools->Info as this URL will not change if the name of the guideline changes.

Cセキュアコーディングスタンダード

The CERT C Secure Coding Standard



Version 1.0 of The CERT C Secure Coding Standard is now available as a [book](#) from Addison-Wesley. This official release can be used as a fixed point of reference for the development of compliant applications and source code analysis tools.

Development of the next version of the [CERT C Secure Coding Standard](#) is being performed here on the secure coding wiki. This version is a work in progress and reflects the current thinking of the secure coding community. See [this link](#) for more information.

There is a JPCERT/CC

JPCERT/CC で日本語公開中!!

<https://www.jpccert.or.jp/sc-rules/>



電子書名: Japan Computer Emergency Response Team Coordination Center
DN: cn=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpccert.or.jp, o=Japan Computer
Emergency Response Team Coordination Center, cn=Japan Computer
Response Team Coordination Center
目録: 2011.03.29 19:30:54 +0900

C/C++ セキュアコーディングセミナー
2010年度版

CERT C セキュアコーディングスタンダード

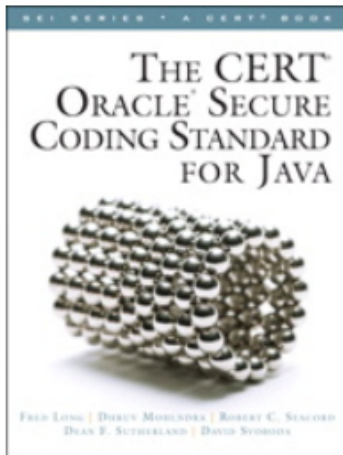
JPCERT コーディネーションセンター

CERT C セキュアコーディングスタンダード紹介

<https://www.jpccert.or.jp/research/materials.html#secure>

Java セキュアコーディングスタンダード

The CERT Oracle Secure Coding Standard for Java



Version 1.0 of *The CERT Oracle Secure Coding Standard for Java* is now available as a [book](#) from Addison-Wesley.

Development of the next version of the [The CERT Oracle Secure Coding Standard for Java](#) is being performed here on the secure coding wiki. This version is a work in progress and reflects the current thinking of the secure coding community. Subsequent official releases of this standard will be issued as dictated by the community.

Java is a multi-country effort.

There is also a partner JPCERT/CC.

JPCERT/CC で日本語公開中!!

<https://www.jpccert.or.jp/java-rules/>

オープンソースの「今」を伝える
オープンソースカンファレンス
2011 Nagoya

オープンソースカンファレンス 2011 Nagoya
セキュアコーディング/ススめ
(Java編)

2011年08月20日
戸田 洋三

JPCERT コーディネーションセンター
secure-coding@jpccert.or.jp

Copyright © 2011 JPCERT/CC. All rights reserved. JPCERT/CC®

OSC2011@Nagoya でも紹介してます
http://www.ospn.jp/osc2011-nagoya/pdf/osc2011nagoya-JPCERT_CC.pdf

セキュアコーディングスタンダード(C++, Perl)

The CERT C++ Secure Coding Standard



The [CERT C++ Secure Coding Standard](#) is under development.
contribute new guidelines to this standard.

The CERT Perl Secure Coding Standard



The [CERT Perl Secure Coding Standard](#) is under development.

“under development”
(開発中)

一般社団法人JPCERTコーディネーションセンター
(<https://www.jpccert.or.jp/>)

セキュアコーディング

(<https://www.jpccert.or.jp/securecoding/>)

お問い合わせはこちらにどうぞ…
(secure-coding@jpccert.or.jp)