

JPCERT/CC の取組みとツールの紹介

一般社団法人 JPCERT コーディネーションセンター
情報流通対策グループ 山田 秀和

- I. JPCERT/CCのこれまでの取組み
- II. JPCERT/CCのこれからの取組み
- III. 制御システム向けツールの紹介
- IV. S4
- V. まとめ

- I. JPCERT/CCのこれまでの取組み
- II. JPCERT/CCのこれからの取組み
- III. 制御システム向けツールの紹介
- IV. S4
- V. まとめ

■ 2007年の取組み



グッド・プラクティス・ガイド プロセス・制御とSCADAセキュリティ

グッド・プラクティス・ガイド プロセス・制御と SCADA セキュリティ **New**

この文書は、制御系システムの開発・設計ならびにユーザーが SCADA を使用するにあたってセキュリティ要件と仕様のガイドとなるものです。また、制御系システム開発者がオープン系システムを取り込もうとする場合の手引きにもなります。

*SCADA: Supervisory Control and Data Acquisition、遠隔制御・監視システム

- 概要
- グッド・プラクティス・ガイド プロセス・制御と SCADA セキュリティ
 - [GPG No. 1 – Understand Business Risk.pdf \(PGP署名\) \(2007-06-14\)](#)
 - [GPG No. 2 – Implement Secure Architecture.pdf \(PGP署名\) \(2007-06-14\)](#)

■ 2008年の取組み



「制御系プロトコルに関する調査研究」報告書



国内の制御システム、制御系プロトコルに関する調査報告書

2008-06-25 調査/研究の「[制御系プロトコルに関する調査研究](#)」報告書を公開しました。

2008-06-25 調査/研究の「[国内の制御系システム、制御系プロトコルに関する調査報告書](#)」(PDF:709KB) (PGP署名)を公開しました。

■ 2009年の取組み



制御システムセキュリティガイドライン、標準、及び認証への取組みに関する分析



重要社会インフラのためのプロセス制御システム (PCS) のセキュリティ強化ガイド



制御システムベンダーセキュリティ情報共有タスクフォース



制御システムセキュリティカンファレンス 2009



制御システムセキュリティ関連情報(メーリングリスト)

「制御システムセキュリティカンファレンス 2009」開催のご案内

2009年01月15日

JPCERT/CCからのお知らせ

有[®]、「制御システムベンダーセキュリティ情報共有タスクフォース」を発足 (PDF:177KB) (PGP 署名) (2009-02-19)

Japan Computer Emergency Response Team Coordination Center
JPCERT/CC
© 2009 Japan Computer Emergency Response Team Coordination Center. All rights reserved.
この文書は「JPCERT/CC」の登録商標です。お問い合わせ先: office@jpcert.or.jp

重要社会インフラのための
プロセス制御システム (PCS) の
セキュリティ強化ガイド

Japan Computer Emergency Response Team Coordination Center
JPCERT/CC
© 2009 Japan Computer Emergency Response Team Coordination Center. All rights reserved.

NCSC コーディネーションセンター
システムの保護セキュリティに関する保護共有フォーラム
the sharing concerning substantive security (SCSS) and process control

制御システムセキュリティガイドライン、標準
及び認証への取組みに関する分析

■ 2010年の取組み



推奨プラクティス: 工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発



人的セキュリティガイドライン



制御システムのサイバーセキュリティ: 多層防御戦略



制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ(OPSEC)の使用



グッド・プラクティス・ガイド パッチ管理



グッド・プラクティス・ガイド プロセス・制御とSCADAセキュリティ(改訂)



制御システムセキュリティカンファレンス2010



制御システムセキュリティ情報共有タスクフォース

■ 制御システムベンダに限らず、制御システムに携わる方を対象

■ 2011年の取組み



制御システムセキュリティカンファレンス2011



制御システムセキュリティアセスメントツール(SSAT)の提供開始



制御システムセキュリティ検討タスクフォース
インシデントレスポンス体制検討ワーキンググループ事務局

- I. JPCERT/CCのこれまでの取組み
- II. JPCERT/CCのこれからの取組み**
- III. 制御システム向けツールの紹介
- IV. S4
- V. まとめ

■ 2012年の取組み(予定)



インシデント対応に必要な技術および実態の調査



ポータルサイト



制御システムセキュリティアセスメントツール



セキュアコーディング



脆弱性情報ハンドリング



インシデント対応に必要な技術および実態の調査

日 時	3月中旬実施予定
期 間	2日間
内 容	Idaho の実地訓練から得た経験をもとに制御シミュレータ等を用いた擬似制御環境を用いて組織でのインシデント対応を行う上で必要と考えられる項目の調査等を実施
対 象	ユーザ + ベンダの2人1組
募集数	最大で10組(20人程度)

■ ポータルサイトでの情報提供

- 現在のメーリングリストでの配信も残しつつポータルサイトでの情報提供も検討中
 - メーリングリストでの配信内容見直しも
- 特定期間内に収集した制御システムセキュリティ関連の情報
- 記事へのアクセス数や反響の大きい情報を中心に分析や追跡調査などを行う予定

■ 対象者

- 制御システムベンダー
- 制御システムユーザー

■ 利用に当たって(現在検討中)

- NDA
- 組織としてのセキュリティ対応チームの確立

■ 制御システムセキュリティアセスメントツール(日本版SSAT)

- 各管理項目における現状を「見える化」する
- 問題発見や気づくためのきっかけ作り
- 設問数の100問前後

- 1/31 時点での JPCERT/CC からの直接配布数 89
- 本ツールはベンダやユーザ、業界団体がカスタマイズを加えるなどして再配布することも可能

2011年のアセスメントツール提供時

全面的にご協力をいただいたセキュリティ合同WGの皆様

- **SICE**（公益社団法人計測自動制御学会）
計測・制御ネットワーク部会セキュリティある情報共有検討WG
- **JEITA**（社団法人電子情報技術産業協会）
制御・エネルギー管理専門委員会 安全・安心システムWG
- **JEMIMA**（社団法人日本電気計測器工業会）
PA・FA計測制御委員会セキュリティ調査研究WG

また、昨年末より以下の皆様にもご協力いただき

- **業界団体、各企業ご担当者様**

日本の制御システム業界に適した形でのアップデート作業進行中

■ セキュアコーディング (C/C++ / Java)

- 出荷後のソフトウェア製品に発見される多くの脆弱性は、プログラミングエラーによって引き起こされている。



- 製品開発工程において、脆弱性につながるような欠陥を作りこまない、仮に作りこまれたとしても出荷前の検証等の段階で発見・対応につながる取り組みが必要。



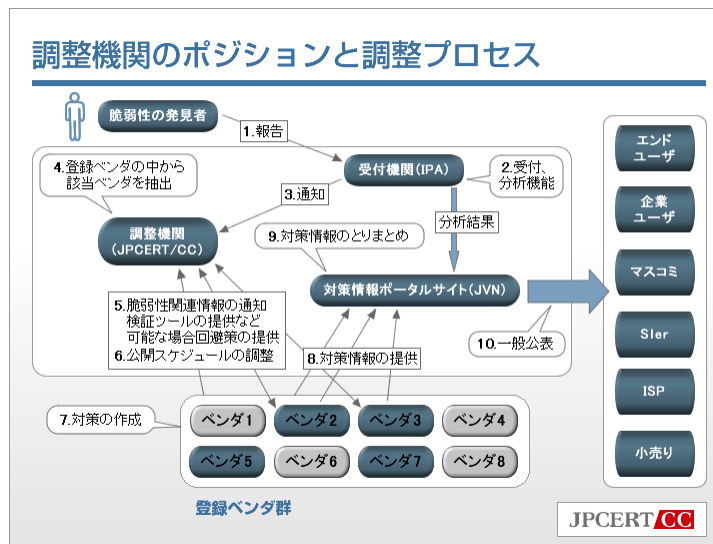
- 開発工程別、あるいは、開発プロセスを包含したよりセキュアな製品開発を実施するための幾つかの対策アプローチが存在する。



セキュアコーディング

脆弱性ハンドリング

一般公表前のソフトウェア/ハードウェアシステム等におけるセキュリティ上の欠陥に係わる情報を、適切な方法で取り扱い、製品開発者によって用意された対策情報とともに公表することによって問題解決方法を広く示し、社会における製品利用者の安全に貢献するための活動



■ 制御システム関連情報の公表例①

- JVN#98649286 (2011/11/01) <https://jvn.jp/jp/JVN98649286/>
CSWorks の LiveData Service におけるサービス運用妨害 (DoS) の脆弱性

公開日:2011/11/01 最終更新日:2011/11/02

JVN#98649286

CSWorks の LiveData Service におけるサービス運用妨害 (DoS) の脆弱性

概要

CSWorks のサーバコンポーネントの一部である LiveData Service には、サービス運用妨害 (DoS) の脆弱性が存在します。

影響を受けるシステム

- CSWorks 2.0.4115.0 およびそれ以前

詳細情報

CSWorks のサーバコンポーネントの一部である LiveData Service には、TCP パケットの処理に起因するサービス運用妨害 (DoS) の脆弱性が存在します。

想定される影響

遠隔の第三者により、サービス運用妨害 (DoS) 攻撃を受ける可能性があります。

対策方法

[アップデートする](#)

開発者が提供する情報をもとに最新版へアップデートしてください。

ベンダ情報

ベンダ [リンク](#)

CSWorks [Important: CSWorks 2.0.4115.1 security release](#)

[Release History](#)

■ CSworks 社の情報公開



CSWorks: web-based industrial automation

of CSWorks and software development

[<< PostgreSQL support | CSWorks 2.1.4385.0 released >>](#)

Important: CSWorks security release 2.0.4115.1

© 10月 27, 2011 09:23 by [Sergey Sorokin](#)

Date: October 27, 2011

Subject: DoS vulnerability in CSWorks LiveData Service

Versions: 2.0.4115.0 and earlier

Summary: Remote attackers can perform a denial of service (software crash).

Description

CSWorks LiveData Service 2.0.4115.0 and earlier allows remote attackers to cause a denial of service after sending crafted TCP packets. Isolating communication between CSWorks LiveData Service and web servers that accept requests from client applications mitigates the issue.

Patch availability

CSWorks 2.0.4115.1 has been issued as security release to correct the defect. CSWorks administrators running affected versions are advised to upgrade to 2.0.4115.1 as soon as possible. The security release can be downloaded from CSWorks web site

<http://www.controlsystemworks.com/DownloadDescription.aspx>.

Credits

The vulnerability was reported by Kuang-Chun Hung, Security Research and Service Institute - Information and Communication Security Technology Center (ICST), Taiwan R.O.C

References

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3996> (will be available after confirmation by MITRE)

<http://jvn.jp/en/jp/JVN98649286/index.html> (will be available after confirmation by JPCERT/CC)

<http://www.controlsystemworks.com/blogengine/post/CSWorks-2041151-security-release.aspx>

■ 制御システム関連情報の公表例②

- JVN#63249231 <https://jvn.jp/jp/JVN63249231/>
Cogent DataHub における HTTP ヘッダインジェクションの脆弱性
- JVN#12983784 <https://jvn.jp/jp/JVN12983784/>
Cogent DataHub におけるクロスサイトスクリプティングの脆弱性

公開日:2012/01/11 最終更新日:2012/01/12

JVN#63249231

Cogent DataHub における HTTP ヘッダインジェクションの脆弱性

概要

Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、HTTP ヘッダインジェクションの脆弱性が存在します。

影響を受けるシステム

- Cogent DataHub V7.1.2 およびそれ以前
- OPC DataHub V6.4.20 およびそれ以前
- Cascade DataHub V6.4.20 およびそれ以前

詳細情報

Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、HTTP ヘッダインジェクションの脆弱性が存在します。

想定される影響

ユーザのウェブブラウザ上で偽の情報が表示されたり、HTTP レスポンス分割攻撃を受けたりするなどの可能性があります。

対策方法

アップデートする

開発者の提供する情報をもとに、最新版にアップデートしてください。

ベンダ情報

ベンダ	リンク
Cogent Real-Time Systems Inc.	Release Notes Download Software

公開日:2012/01/11 最終更新日:2012/01/12

JVN#12983784

Cogent DataHub におけるクロスサイトスクリプティングの脆弱性

概要

Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、クロスサイトスクリプティングの脆弱性が存在します。

影響を受けるシステム

- Cogent DataHub V7.1.2 およびそれ以前
- OPC DataHub V6.4.20 およびそれ以前
- Cascade DataHub V6.4.20 およびそれ以前

詳細情報

Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、クロスサイトスクリプティングの脆弱性が存在します。

想定される影響

ユーザのウェブブラウザ上で任意のスクリプトを実行される可能性があります。

対策方法

アップデートする

開発者の提供する情報をもとに、最新版にアップデートしてください。

ベンダ情報

ベンダ	リンク
Cogent Real-Time Systems Inc.	Release Notes Download Software

■ Cogent 社の情報公開



What you can do
[Web visualization](#)
[Access remote data](#)
[Database integration](#)
[Access embedded data](#)
[Real-time trend analysis](#)
[System monitoring](#)
[Networking Excel data](#)
[Email/SMS notification](#)

Release Notes

What's new in versions 7.2.0?

This is a maintenance release that combines several improvements and bug fixes. We would like to thank all of the users who provided feedback and encourage you to continue to send feature requests and suggestions to info@coagent.ca.

[Download the new Cogent DataHub 7.2.0 release here.](#)

Version 7.2.0 - December 21, 2011

Bug

[DATAHUB-44] - Data Logging interface in Vista - item overlap.
[DATAHUB-150] - Plain-text email doesn't send special characters.
[DATAHUB-152] - Error message from Permission Editor when deleting a WebView user.
[DATAHUB-153] - DotNet API does not connect if there is no form to allow async signalling across threads.
[DATAHUB-154] - DotNet API does not produce a transition from failed to idle.
[DATAHUB-164] - Rare crash when configuring tunnel/mirror settings.
[DATAHUB-165] - OPC A&E events not reliably arriving through a tunnel, client connection not always made.
[DATAHUB-194] - DataHub emits empty string Value when a client creates a DataPoint via lookup.
[DATAHUB-197] - JVN#12983784 XSS (Cross-site scripting vulnerability).
[DATAHUB-197] - JVN#63249231 CRLF (Carriage Return and Line Feed injection vulnerability).



<http://www.cogentdatahub.com/ReleaseNotes.html>

- I. JPCERT/CCのこれまでの取組み
- II. JPCERT/CCのこれからの取組み
- III. 制御システム向けツールの紹介**
- IV. S4
- V. まとめ

■ Bandolier

- Digital Bond 社がDoEからの資金を元に作成
- 制御システムに最適なセキュリティ設定を確認するための監査ファイル(カスタマイズ可能)
- Nessus (脆弱性スキャナ) のプラグインとして提供



The screenshot shows the 'Bandolier' Analyst Report page. At the top, there are logos for Digital Bond, Pike Research, and Industrial Defender. The main heading is 'Analyst Report Trends & approaches in ICS protection'. Below this, there is a navigation bar with links like 'What's Hot', 'Bandolier', 'Portledge', 'Quickdraw SCADA IDS', and '84 Agenda'. The main content area features a 'SOLD OUT!' announcement for a training session in Miami Beach, an 'October This Month in Control System Security Podcast' link, an 'ICS Security Tool Newsletter Issue #2' link, and a video link for Dale Peterson's SCADA Research presentation. The 'Bandolier' section includes an overview and a 'How it Works' section with bullet points. At the bottom, there is an image of a Nessus Scanner laptop.

digital bond **PikeResearch** **Analyst Report** **INDUSTRIAL DEFENDER**
Cleanest Market Intelligence **Trends & approaches in ICS protection** **DOWNLOAD**

What's Hot: [Bandolier](#) [Portledge](#) [Quickdraw SCADA IDS](#) [84 Agenda](#)

SOLD OUT!
Jan 17-20 in Miami Beach
Includes Advanced Training Options
[Download the detailed agenda](#)

October This Month in Control System Security Podcast: Rios & McCorkle on HMI vulns

ICS Security Tool Newsletter Issue #2
[Subscribe to ICS Security Tool Mailing List](#)

Video: Dale Peterson's SCADA Research Presentation at OSISoft User Group

Pages

Bandolier

Digital Bond's Bandolier project helps asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. Digital Bond partners with leading ICS vendors to identify the optimal security configuration that still allows the vendor's product to operate properly. This requires access to the vendor's security experts, lead engineers and a test lab. Digital Bond then creates Bandolier Security Audit Files that work with the compliance plugin in the Nessus vulnerability scanner. Bandolier Security Audit Files are available for over twenty control system components, with more on the way.

Overview

- Defines optimal security configuration for SCADA and DCS servers and workstations
- Provides vendor-supported, customized security audit files for control system applications
- Provides a safe and effective way to audit the security of control system components

How it Works

- No client software, services, or agents are required on the control system server or workstation
- User uploads Bandolier Security Audit Files to the Nessus vulnerability scanner
- Nessus policy compliance plugins make a low impact connection to the ICS server or workstation
- Nessus uses built-in operating system functionality to compare the settings on the control system server to those defined in the Bandolier Security Audit File
- Nessus provides a report that shows whether each setting matched what is in the Bandolier Security Audit File

Nessus Scanner

制御システム向けツールの紹介

■ ツールの利用場面

ー ベンダーの皆様

- 社内の品質保証
- 受け入れテスト時



ー ユーザーの皆様

- 受け入れテスト時
- 定期的なセキュリティテスト



List of Bandolier Security Audit Files

Bandolier Security Audit Files help asset owners and vendors identify and audit optimal security configuration for control system servers and workstations. In this Department of Energy funded project, Digital Bond partners with leading control system application vendors to establish practical security configuration guidance for SCADA, DCS, and other industrial control system components. Digital Bond then creates and distributes specialized security audit files that can be used with the Nessus vulnerability scanner. Bandolier, in conjunction with Nessus, is the most widely used security tool in industrial control systems.

The Bandolier Baselines represent the O&M vendor / industry advice for the best practice security configuration that is then slightly modified for settings that will cause problems for control systems. Below are the available Bandolier Baselines.

Vendor	OS Name
Microsoft	Windows 7
Microsoft	Windows Server 2008 R2

Below is the list of Bandolier Security Audit Files and their current status.

Vendor	Application Name	Version	Operating System	Status
ABB	800A PPA Connectivity Server	5.x	Windows Server 2003	1.0
ABB	800A PPA Aspect Server	5.x	Windows Server 2003	1.0
ABB	800A PPA Historian	5.x	Windows Server 2003	1.0
ABB	800A PPA Domain Controller	5.x	Windows Server 2003	Development
ABB	800A PPA Eng/Operator Workstation	5.x	Windows XP	1.0
Alstom Grid	■ MetracPlatform (Production Server)	2.5	Windows Server 2003	1.1
Alstom Grid	■ MetracPlatform (Production Server)	2.5	Red Hat Linux 5.3	1.1
Alstom Grid	■ MetracPlatform	2.6	Windows Server	1.0

CSI Control Systems International	UCO& FOU App Server	1.0	CENTOS	1.0
CSI Control Systems International	UCO& Operator Work Station	5.2	Windows 7	1.0
CSI Control Systems International	UCO& PHM - Historian	5.2	Windows 2008 Server R2	1.0
Emerson	Orbton Engineering Workstation	3.1	Windows XP	1.0
Emerson	Orbton Operator Workstation	3.1	Windows XP	1.0
Emerson	Orbton Process Historian	3.1	Windows Server 2003	1.0
Emerson	Orbton SCADA Communication Server	3.1	Windows Server 2003	1.0
Matrox	Security Gateway Tunneler		Windows Server 2003	1.1
OSisoft	PI Enterprise Server	3.3a 3.4.4	Windows Server 2003	1.3.7
Siemens	Spectrum Power TO SCADA Host	8.2	Red Hat Linux	1.1
Siemens	Spectrum Power TO SCADA Workstation	8.2	Windows XP	1.1
Siemens	Spectrum Power TO Web Console	8.2	Windows Server 2003	1.1
SBCO	AV-S4 ICCP Server	4.0050.2	Windows Server 2003	1.1
SINO Lumin ECS	GENE SCADA	GENE	Red Hat Linux	1.1
Telnet	OMBY DNA Realtime Server	7.5	Windows Server 2003	1.1

TENABLE PRODUCTS



Nessus Product Overview

Tenable Nessus[®] vulnerability scanner is the world-leading vulnerability scanner. With more than five million downloads to-date, Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners may be distributed throughout an entire enterprise, inside DMZs and across physically separate networks.

Product Overview

- > Features
- > Nessus for Business
- > Nessus for Home
- > Upgrade to Nessus 4.4
 - > Nessus Mobile Apps
- > Nessus Auditor Bundles
- > Nessus Plugins
- > Documentation
- > Nessus FAQ
- > Sample Reports
- > Deployment Options
- > Training



Nessus 4.4 Screenshots

TENABLE PRODUCTS



SCADA Checks

The Tenable Nessus Professional Feed contains, in addition to the regular network vulnerability checks, several dozen plugins for Nessus 4 that specifically discover and test SCADA devices.

The SCADA family of plugins will readily produce vulnerability audit data that can be leveraged for a variety of NERC and other types of security audits involving process control networks. In the power industry, this can help create various lists of devices by active SCADA protocol (DCP, DNP3, etc.) as well as function or even "Area of Responsibility".

For NERC compliance, this process can help make sure the list of "Critical Cyber-Security Assets" is accurate and does not include too many hosts while ignoring others.

In addition, through funding by the Department of Energy, Digital Bond has produced a wide variety of audit policies for Nessus users to test the configurations of many different types of Unix and Windows control system software.

Both Tenable and Digital Bond have written extensively about SCADA and Control Systems auditing in their blogs:

- [Bandolier and NERC DCP](#)
- [Extending Bandolier with Other Nessus Credential Checks](#)
- [Bandolier Security Audit File Release: Matrox/DCP](#)
- [Nessus SCADA Plugins](#)

If you are an enterprise customer, you should consider applying Tenable's Unified Security Monitoring approach to NERC and control systems monitoring. We've produced a short video entitled [Auditing SCADA and Control System Networks](#) that shows how our passive, active and log analysis products can be used to monitor control system networks.

- I. JPCERT/CCのこれまでの取組み
- II. JPCERT/CCのこれからの取組み
- III. 制御システム向けツールの紹介
- IV. S4**
- V. まとめ

■ S4(Scada Security Scientific Symposium)とは












































- 2007から米国で開催されている制御システムのセキュリティに特化したカンファレンス(2011年は開催せず)
- 開催時期: 毎年1月頃(今年は2012年1月17日～20日に開催)
- 開催場所: マイアミ
- 主 催: DigitalBond

■ 過去の講演内容

- 制御システムに用いられるプロトコルに関する分析や脆弱性の公開
- 制御システムでどのようにセキュリティ対策を行うかの調査

■ Project Basecamp

－ PLC に関するセキュリティ上の問題点が無いか調査

					
Firmware					
Ladder Logic					
Backdoors					
Fuzzing					
Web			N/A	N/A	
Basic Config					
Exhaustion					
Undoc Features					

- JPCERT/CCのこれまでの取組み
- JPCERT/CCのこれからの取組み
- 制御システム向けツールの紹介
- S4 Project Basecamp
- **まとめ**

JPCERT/CC 2012年の取組み

- インシデント対応に必要な技術および実態の調査
- ポータルサイト
- 制御システムセキュリティアセスメントツール
- セキュアコーディング
- 脆弱性ハンドリング

ツールの紹介

- 制御システム向けのセキュリティツールは公開済

S4

- 制御システムのみならず、制御装置自身もターゲットに

■ 制御システムセキュリティ

連絡先: cs-security-staff@jpcert.or.jp

H P: <https://www.jpcert.or.jp/ics/>



Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

Home > 制御システムセキュリティ

検索

トップページ

情報提供

- ・ 注意喚起
- ・ 早期警戒
- ・ 脆弱性対策情報
- ・ Weekly Report
- ・ インターネット定点観測

インシデントの報告

各種登録

制御システムセキュリティ

制御システムセキュリティ

ラーニング

公開資料

イベント

プレスリリース

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

JPCERT/CC

制御システムセキュリティ

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御生活の基盤サービスを提供する重要なシステムとして利用されています。その一方で、制御系システムに関連するソフトウェアに脆弱性が

JPCERT/CC では、プロセス監視・制御システムのセキュリティに関し、国内の脆弱性関連情報調整機関として対策の促進に資する活動を

公開日	お知らせ
2011-02-28	制御システムセキュリティアセスメントツールの提供
2011-02-18	制御システムセキュリティカンファレンス 2011 の講演資料を公開
2010-05-31	「グッド・プラクティス・ガイド バッチ管理」制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用
2010-03-31	「制御システムのサイバーセキュリティ:多層防御戦略」「人的セキュリティガイドライン」「推奨プラクティス:工業用制御システム対応能力の開発」を公開しました
2009-11-24	「制御システムセキュリティガイドライン、標準及び認証への取組みに関する分析」「重要社会インフラのためのプロセス制公開しました
2009-09-18	制御システムセキュリティカンファレンス 2009 の講演資料を公開

制御システムセキュリティ情報共有コミュニティ

※タスクフォースからコミュニティに名称を変更しました。

制御システム関連製品の脆弱性情報

おすすめする読みのもの (ガイドライン・参考書など)

- ・ 制御システムセキュリティプロトコル
- ・ 制御システムセキュリティガイドライン(全版)

セキュアコーディング

連絡先 : secure-coding@jpcert.or.jp

● 書籍

- 『C/C++セキュアコーディング』
- 『CERT C セキュアコーディングスタンダード』
- 『Java セキュアコーディングスタンダード CERT/Oracle版』



● Web記事連載

- CodeZine - C/C++セキュアコーディング入門
<http://codezine.jp/article/corner/339>
- CodeZine - Javaセキュアコーディング入門
<http://codezine.jp/article/corner/437>



● その他

- CERT C Secure Coding Standard 日本語版 <http://www.jpcert.or.jp/sc-rules/>
- Java セキュアコーディングスタンダード CERT/Oracle 版 <http://www.jpcert.or.jp/java-rules/>
- Java セキュアコーディング 並行処理編
http://www.jpcert.or.jp/securecoding_materials.html#certjavacon
- OWASP「ソフトウェアセキュリティ保証成熟度モデル」
http://www.jpcert.or.jp/securecoding_materials.html#owaspsamm
- ソースコード解析ツールを活用したCERTセキュアコーディングルールの有効性評価報告書 (英語版、日本語版) <http://www.jpcert.or.jp/research/Analysistools.html>

Home

- サイト内検索
- トップページ
- 各種届出・申込
- 制御システムセキュリティ
- ラーニング
- 公開資料
- 四半期レポート
- 研究・調査レポート
- CSIRTマテリアル
- イベント
- プレスリリース
- JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務

注意喚起

深刻に影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

2009-06-10 [公開]
 2009年6月10日 Microsoft セキュリティ情報(緊急1件)に関する注意喚起

2009-06-13 [公開]
 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起

2009-06-13 [公開]
 2009年5月 Microsoft セキュリティ情報(緊急1件)に関する注意喚起

JPCERT コーディネーションセンター

過去の注意喚起

脆弱性に関する情報

ソフトウェアなどの脆弱性と対策情報をJVNより提供しています。

2009-06-19 15:00
 XOOFS マシンによる脆弱性

2009-06-19 14:32
 A51 D.O.O. 製 activeCollab におけるクロスサイトスクリプティングの脆弱性

2009-06-19 11
 Microsoft Works コンポーネントの脆弱性

2009-06-19 14:32
 Moveable Type Enterprise におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32
 Serene Bach におけるセッション ID が推測可能な脆弱性

詳しく見る

— Email : office@jpcert.or.jp

— Tel : 03-3518-4600

— Web : <http://www.jpcert.or.jp/>

Weekly Report

2009-06-12日

HTTPS FSS

セキュリティインシデント...
 フィッシングサイト...
 Webサイトの改ざん...
 マルウェア...
 不正アクセス...

発生元への「調整」を依頼したい
 インシデントを「報告」したい

ISDAS
 [インターネット定点観測]



インターネット上に配置した
 センサーにより、セキュリティ上の
 脅威となるトラフィックを観測し
 ています。

お薦めページ

セキュリティ
 対策講座



教育担当者が使える、新入社員
 などが身につけておくべきセ
 キュリティ知識などを紹介して
 います。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- CC/C+ セキュアコーディング ハーフデイキャンプ参加申し込み