Japan Computer
Emergency Response
Team Coordination
Center

JPCERT CC®

ICS向け JPCERT/CC提供サービスのご紹介

一般社団法人 JPCERTコーディネーションセンター

ICSR（Industrial Control System Security Response Group）
制御システムセキュリティ対策グループ
宮地 利雄・山田 秀和・功刀 ゆみ・長田 貢

ICS関連で JPCERT/CCが提供するサービスの概要

JPCERT CC®

CERTの立場から事後対策を中心とするサービスを提供

未然防止対策

1) 国際標準化の推進
2) テストベッドの構築
3) 評価・認証スキームの構築

事後対策

4) インシデント対応体制の構築

- ICS用製品の脆弱性関連情報の調整
- ICSインシデント報告の受付
- ICSインシデントや脅威情報の提供

共通対策

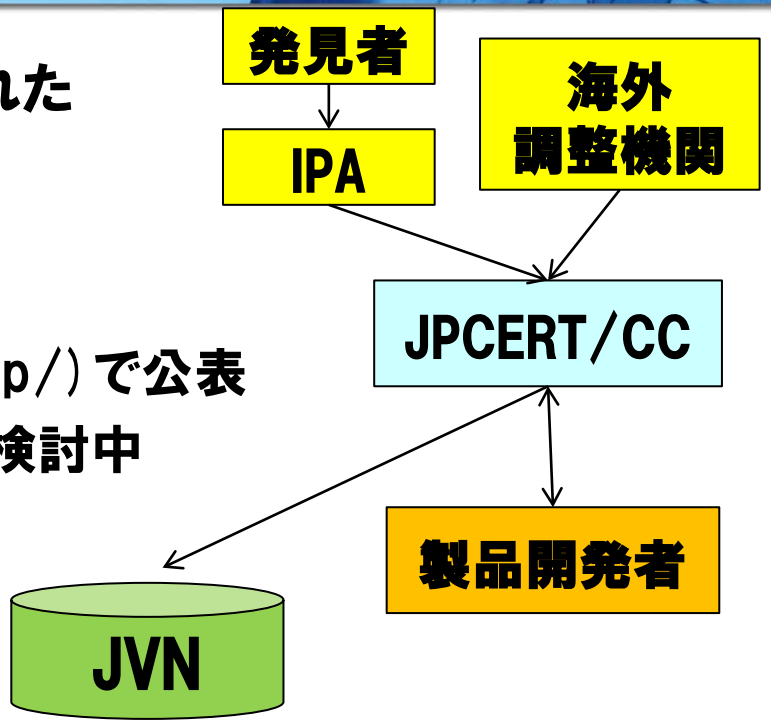
5) 人材育成，ユーザ企業への普及啓発の推進

- 対策への気付きのためのツールの提供

製品に潜在する脆弱性を減らすためのサービス

JPCERT CC®

- 発見者や海外の調整機関から報告された製品の脆弱性関連情報を当該製品の開発者に通知
  - IT系製品の脆弱性情報は脆弱性情報ポータルJVN（https://jvn.jp/）で公表
  - ICS製品に関する取扱方法を研究会で検討中



- セキュア・コーディング
  - 対象プログラミング言語
    - C/C++
    - Java
  - 技術資料を含む詳細：https://www.jpcert.or.jp/securecoding.html
  - 講師派遣（有償サービス）

ICSインシデントや脅威情報の提供

- ICSインシデントへの効果的な対応に必要な情報を収集して提供
  1. ICSセキュリティ関連ニュース
     - ICSセキュリティに関連する注目すべきニュース
  2. ICS脅威事例
     - インシデント事例や公にされたシステム脆弱性など
  3. 米国ICS-CERTの公開情報
     - 新しく発行されたアドバイザリ，アラートなど
  4. JPCERT/CCからのお知らせ

- 月刊ニュースレターの形式でメール配信中
  - 2011年度の隔月刊から月刊化
- ConPas（ICSセキュリティ情報ポータル）にバック・ナンバーを含め掲載予定

ICSインシデントや脅威情報の購読方法

- 月刊のニュースレター
  - ICSセキュリティ関連のニュースや話題情報を月刊で配信
  - 購読の申込みはJPCERT/CCホームページ
    → 制御システムセキュリティ
    → 制御システムセキュリティ情報共有コミュニティ

（ICS関連を含む情報セキュリティ関連情報）

- 早期警戒情報
  - 重要インフラ事業者が対象
  - 詳細は
    http://www.jpcert.or.jp/wwinfo/
  - 購読の申込みは
    ww-info@jpcert.or.jp（早期警戒情報登録受付窓口）

インシデント情報報告の受付

報告受付の目的

- 他の利用者への注意喚起を通じた類似インシデントの防止
- インシデント対応の中で必要な分析・調整業務の依頼を受ける
- 日本におけるICSインシデントの状況と動向を掌握する

想定される報告の内容例

- インターネットから直接にアクセス可能なICS機器を見つけた
- ICSが未知のマルウェアに感染し，そのマルウェアについて動作などを分析してほしい
- 自社のICSがサイバー攻撃を受けていると疑われる状況にあり，類似例の有無その他の情報が欲しい，あるいは相談にのって欲しい
- 自社等で発生したサイバー・インシデントに関する情報を，匿名化した上で提供することで，他の利用者の参考に供したい

ICSインシデント情報報告の方法

- 報告は次のいずれかの方法で:
  - 電話
  - Fax
  - 電子メール
  - Webフォーム
    (JPCERT/CCホームページ)

- 2013年1月下旬から
  ICSのためのWebフォームを
  開設

続いて各担当者から詳しくご説明します

JPCERT CC®

- **制御システム関係者向けインシデント対応トレーニング**
  - サイバー・インシデントへの対応の初歩を学ぶ
  - 座学＋擬似マシンを使った実地（ハンズ・オン）訓練
- **制御システム・セキュリティ評価ツール**
  - セキュリティ対策へのきっかけを掴むための気付き支援ツール
- **ConPas提供サービスのご説明**
  - 制御システム関係者向け情報ポータル・サービス
  - パスワード保護アカウント

制御システム関係者向けインシデント対応トレーニング

制御システム関係者向けインシデント対応トレーニング

JPCERT CC®

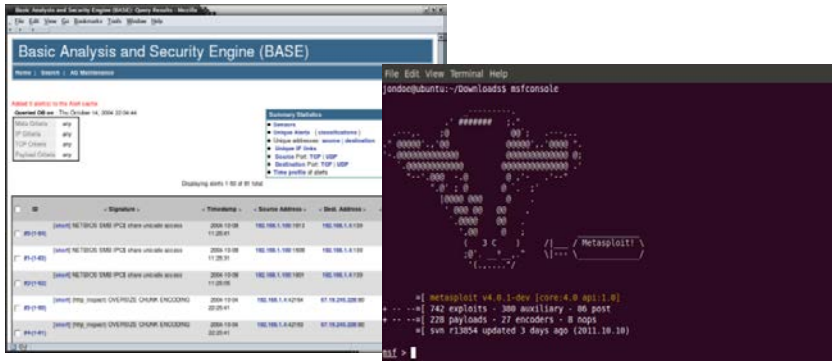
開催概要

- 期間：2日間
  - 2013年2月　大阪
  - 2013年3月　東京 2回
- 費用：無料
- 対象：制御システムユーザ企業、ベンダ企業、研究者の方
- 人数：最大10組（20名程度）

擬似的なネットワーク環境において、
制御システムシミュレータを用いた
トレーニングを実施

トレーニング内容

- セキュリティ基礎
- 制御システムセキュリティ基礎
- 攻撃の流れを知る
- 防御策を考える
- ハンズオン（攻撃・調査）
- セキュリティ対策の検討、実施、発表、効果測定

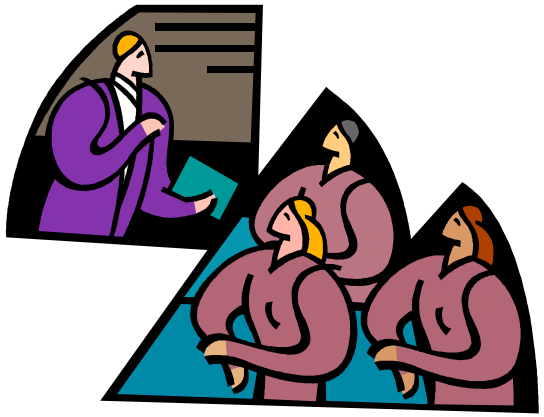


制御システム関係者向けインシデント対応トレーニング

JPCERT CC®

トレーニングを受けた方の声

- ✓ 意識の変化。対策の具体例を知った。
- ✓ 事前に準備をしておく必要があることが分かった。
- ✓ 発生時の対応のイメージが今まで無かった。
- ✓ 攻撃を受けた場合、いち早く察知する能力が必要と感じた。
- ✓ どういう観点をもって、防御すればよいのか学べたから。
- ✓ 本当に完全に防御可能なのか。
- ✓ 守る側は、非常に大変。攻撃者の立場で考える必要がある。
- ✓ 防御がこれほど難しいとは思わなかった。
- ✓ 非常に多岐にわたる知識が必要と分かったため。
- ✓ 意外とその気になれば、簡単に攻撃できる。
- ✓ 攻撃はかなり容易にできる。内容が具体的で理解しやすかった。
- ✓ セキュリティの重要性を認識できたから。



制御システム関係者向けトレーニングに関するお問合わせ

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
Email：icsr@jpcert.or.jp

J-CLICS
(Check List for Industrial Control Systems of Japan)

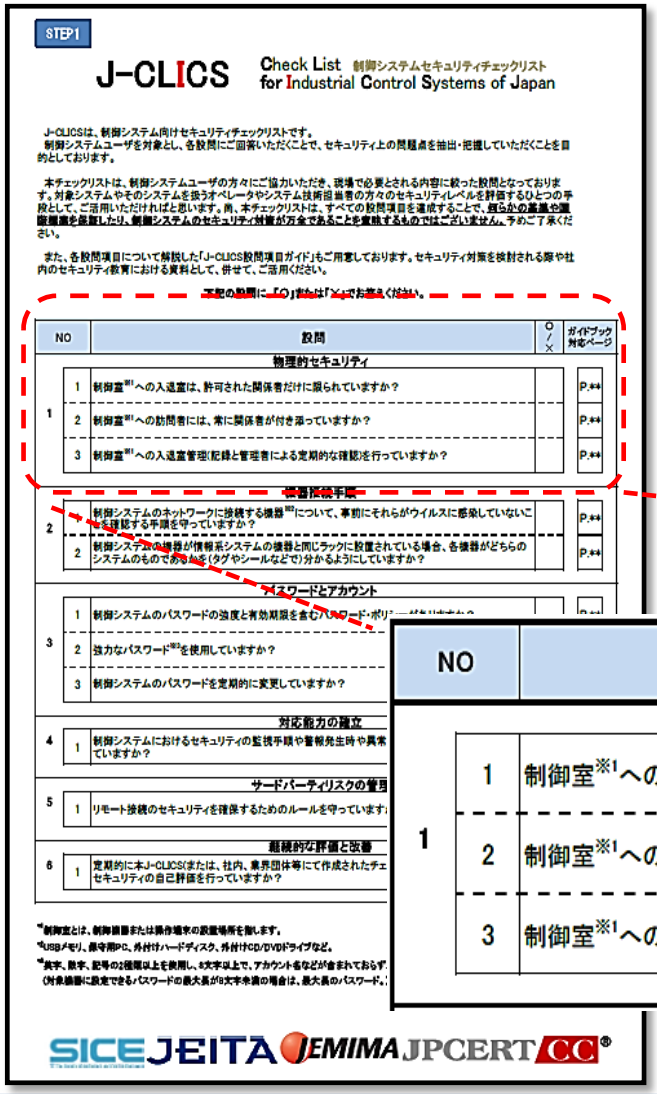
J-CLICSとは

- J-CLICSとは：
  - SSATをもとにした、制御システム向けセキュリティ自己評価ツール
  - チェックリストと補足ガイド
  - 制御システム部門全体で取組むSTEP1と各担当者で取組むSTEP2

- 目的：
  - 制御システムやその管理体制の現状の「可視化」
  - セキュリティに対する意識の向上
  - セキュリティ対策に取組むためのきっかけ作り

- 入手方法：
  - JPCERT/CCホームページよりお申し込み、後日メールにて提供
  - 2013年2月より、順次公開予定

J-CLICSチェックリスト


STEP1

J-CLICS Check List 制御システムセキュリティチェックリスト for Industrial Control Systems of Japan

J-CLICSは、制御システム向けセキュリティチェックリストです。
制御システムユーザを対象とし、各設問にご回答いただくことで、セキュリティ上の問題点を抽出・把握していただくことを目的としております。

本チェックリストは、制御システムユーザの方々にご協力いただき、現場で必要とされる内容に絞った設問となっております。対象システムやそのシステムを扱うオペレータやシステム技術担当者の方々のセキュリティレベルを評価するひとつの手段として、ご活用いただければと思います。尚、本チェックリストは、すべての設問項目を達成することで、何らかの脆弱や潜在問題点を発見したり、制御システムのセキュリティ対策が万全であることを意味するものではございません。予めご了承ください。

また、各設問項目について解説した「J-CLICS設問項目ガイド」もご用意しております。セキュリティ対策を検討される際や社内のセキュリティ教育における資料として、併せて、ご活用ください。

下記の設問に「○」または「×」でお答えください。

NO		設問	○/×	ガイドブック対応ページ
1	物理的セキュリティ			
	1	制御室※1への入退室は、許可された関係者だけに限られていますか？		P.**
	2	制御室※1への訪問者には、常に関係者が付き添っていますか？		P.**
	3	制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.**
2	情報機器の設定手順			
	1	制御システムのネットワークに接続する機器※2について、事前にそれらがウイルスに感染していないことを確認する手順を守っていますか？		P.**
	2	制御システムの機器が情報系システムの機器と同じラックに設置されている場合、各機器がどちらのシステムのものであるかを(タグやシールなどで)分かるようにしていますか？		P.**
3	パスワードとアカウント			
	1	制御システムのパスワードの強度と有効期限を含むパスワード・ポリシーを守っていますか？		P.**
	2	強力なパスワード※3を使用していますか？		P.**
	3	制御システムのパスワードを定期的に変更していますか？		P.**
4	対応能力の確立			
	1	制御システムにおけるセキュリティの監視手順や警報発生時や異常時の対応手順を守っていますか？		P.**
5	サードパーティリスクの管理			
	1	リモート接続のセキュリティを確保するためのルールを守っていますか？		P.**
6	継続的な評価と改善			
	1	定期的に本J-CLICS(または、社内、業界団体等にて作成されたチェックリスト)を用いてセキュリティの自己評価を行っていますか？		P.**

※制御室とは、制御機器または操作端末の設置場所を指します。
※USBメモリ、録音用PC、外付けハードディスク、外付けCD/DVDドライブなど。
※英字、数字、記号の2種類以上を使用し、8文字以上で、アカウント名などが含まれておらず、(対象機器に設定できるパスワードの最大長が8文字未満の場合は、最大長のパスワード。)

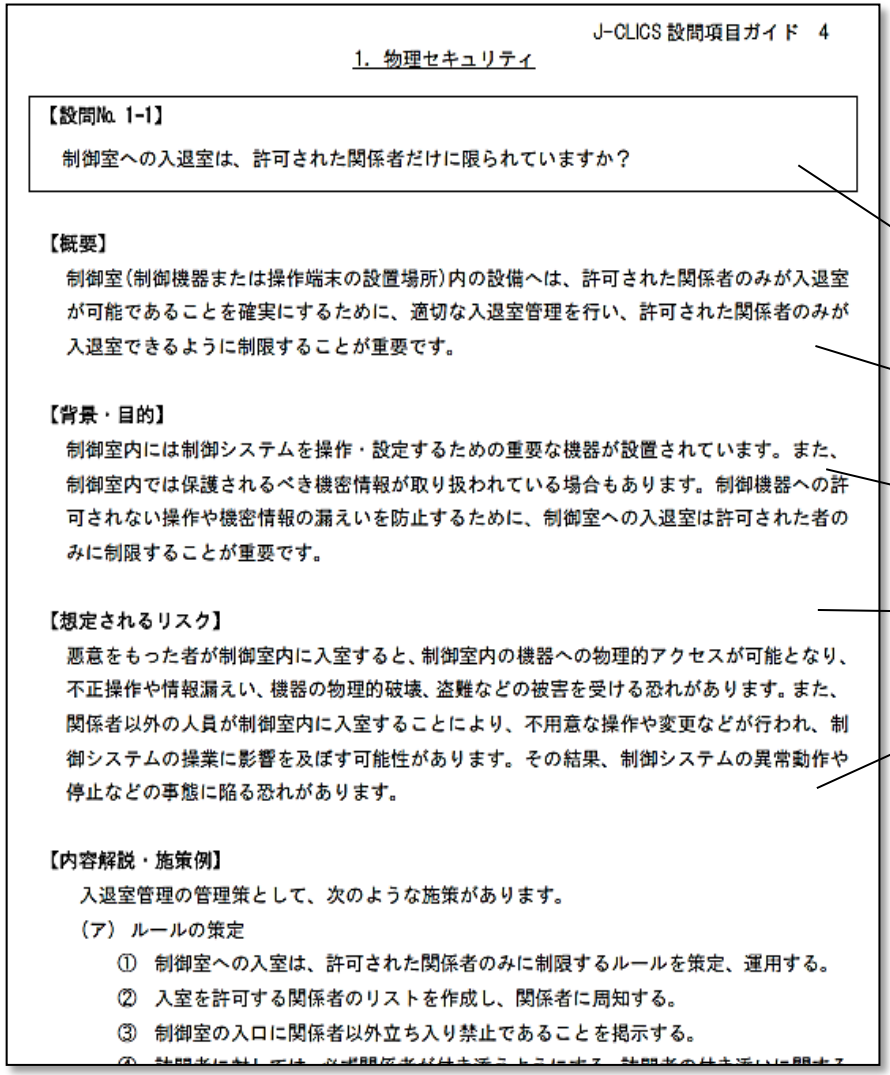
SICE JEITA JEMIMA JPCERT/CC

- 現場で必要とされるセキュリティ施策
- ○×形式による回答方法

チェックリストで、
セキュリティ上の問題点の抽出と把握を!

NO	設問	○/×	ガイドブック対応ページ
1	物理的セキュリティ		
1	制御室※1への入退室は、許可された関係者だけに限られていますか？		P.**
2	制御室※1への訪問者には、常に関係者が付き添っていますか？		P.**
3	制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.**

J-CLICS設問項目ガイド



J-CLICS 設問項目ガイド　4

1. 物理セキュリティ

【設問No. 1-1】

制御室への入退室は、許可された関係者だけに限られていますか？

【概要】

制御室(制御機器または操作端末の設置場所)内の設備へは、許可された関係者のみが入退室が可能であることを確実にするために、適切な入退室管理を行い、許可された関係者のみが入退室できるように制限することが重要です。

【背景・目的】

制御室内には制御システムを操作・設定するための重要な機器が設置されています。また、制御室内では保護されるべき機密情報が取り扱われている場合もあります。制御機器への許可されない操作や機密情報の漏えいを防止するために、制御室への入退室は許可された者のみに制限することが重要です。

【想定されるリスク】

悪意をもった者が制御室内に入室すると、制御室内の機器への物理的アクセスが可能となり、不正操作や情報漏えい、機器の物理的破壊、盗難などの被害を受ける恐れがあります。また、関係者以外の人員が制御室内に入室することにより、不用意な操作や変更などが行われ、制御システムの操業に影響を及ぼす可能性があります。その結果、制御システムの異常動作や停止などの事態に陥る恐れがあります。

【内容解説・施策例】

入退室管理の管理策として、次のような施策があります。

（ア）ルールの策定

① 制御室への入室は、許可された関係者のみに制限するルールを策定、運用する。

② 入室を許可する関係者のリストを作成し、関係者に周知する。

③ 制御室の入口に関係者以外立ち入り禁止であることを掲示する。

- チェックリストの補足文書
- 「何のために何をすべきか」を分かりやすく解説

【設問】

【概要】

【背景・目的】

【想定されるリスク】

【内容解説・施策例】

設問項目ガイドで、
対策の検討や教育を!

STEP1とSTEP2

STEP1

- **制御システムに携わる方すべて**を対象とする
- 物理セキュリティやパスワードなど、基礎的なセキュリティ項目
- 6分野11項目

STEP2

- **制御システムの技術担当者や管理者**を対象とする
- システム監視やウイルス対策など、より技術的なセキュリティ項目
- 10分野10項目

- まずはセキュリティの現状を確認してみたいという方　→　STEP1
  その後、STEP2　を入手し、段階的にセキュリティ意識の強化を

- セキュリティ全般を確認する必要のある方　→　STEP1 & STEP2
  網羅的にセキュリティ意識の強化を

J-CLICS作成にご協力いただいた方々

- SICE/JEITA/JEMIMAセキュリティ合同WGの皆さま
  - 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）
    制御システム専門委員会 セキュリティWG
  - JEMIMA（社団法人日本電子計測器工業会）
    PA・FA計測制御委員会セキュリティ調査研究WG
- ユーザー企業ご担当者さま

ConPaS
(Control Systems Security Partners Site)

ConPaSって？

ConPaS

Control Systems Security Partners Site

JPCERT/CC ICSR（制御システムセキュリティ対策グループ）が
2013年3月上旬からサービス提供開始を予定している
制御システムセキュリティ関係者向け情報共有サイト です。

※本サイトは無料でご利用いただけますが、
ご利用に事前の会員登録が必要です。

ご利用いただける方々

制御システムに関係する方々

- ベンダ
- システムインテグレータ（エンジニアリング）
- アセットオーナ
- セキュリティベンダ
- 学術関係者
- 関連団体,組織
- 政府,公共団体

会員登録 → 登録済みユーザとしてログイン可能

未登録 → ログイン不可

※情報の性質上、制御システム関係者以外は利用できません。ご了承ください。

情報共有コミュニティが変わる

JPCERT/CC ICSRから提供している制御システムセキュリティ情報

JPCERT CC®

ICSR

（制御システムセキュリティ対策グループ）

制御システムセキュリティ関連情報

月刊NewsLetter

定期的に情報取得

ConPaS　情報共有サイト

随時情報取得が可能

※画面は開発中のものです。

3月からNewsLetterとConPaSで制御システムセキュリティ情報をご提供します。

※月刊NewsLetterによる情報提供も続行します。

ConPaSで提供予定のコンテンツ

- 情報
  - 国内外の制御システムセキュリティ動向
  - 制御システムセキュリティ関連カンファレンスやトレーニングの情報
- 資料
  - ICS-CERT Advisory & Alert (邦訳) アーカイブ
  - セキュリティチェックツールなどのツール類
  - 各種ガイドライン
  - JPCERT/CC発行のレポート
  - カンファレンスやセミナーでの講演資料
  - NewsLetter (制御システムセキュリティ関連情報) バックナンバー

提供予定コンテンツ概要（提供情報）

- RSSフィードを利用し、国内外のサイトから制御システムセキュリティに関する最新動向についての情報を収集・提供します。

※画像はイメージです。

- その他、ICSRが実施するトレーニングやセミナー等についての情報も掲載します。

※画面は開発中のものです。

提供予定コンテンツ概要
（ICS-CERT Advisory&Alert邦訳アーカイブ）

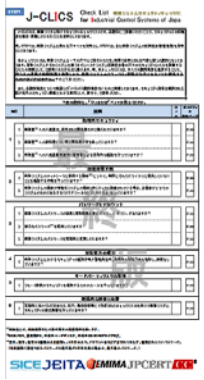
- ICS-CERTから公開されている Advisory & Alert を邦訳し、公開年月別、発生ベンダー別等にアーカイブしていきます。
- 邦訳したAdvisory＆Alertをアーカイブすることで、類似の脆弱性や脅威情報を検索する、などの用途にお役立ていただけます。
- 最終的には全件のアーカイブを目標に、まずは2012年度に公開されたものの邦訳とアーカイブの作業を進めています。

提供予定コンテンツ概要(ツール類)

- 日本版S-SATおよびJ-CLICSなどのセキュリティチェックツールをダウンロードしてご利用いただけます。
- これまで日本版S-SATをご利用いただくためには、JPCERT/CCへご連絡いただき、お送りした後ご利用いただいておりましたが、ConPaSサービス開始後は当該手続が不要となり、必要な際にすぐダウンロードしてご利用いただけるようになります。
- また、今後ほかのツールやマニュアル等についても公開を検討しています。

日本版SSAT

J-CLICS



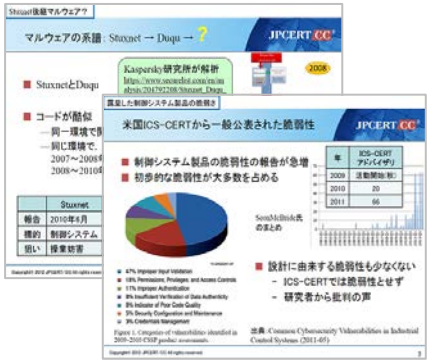
※J-CLICSの画像は開発中のものです。

提供予定コンテンツ概要(その他の資料)

- その他、今後JPCERT/CC　ICSRで作成・翻訳を行う制御システムに関する各種ガイドラインや報告書、講演資料などを閲覧またはダウンロードいただけまいただけます。
- また、現在JPCERT/CCの制御システムWebページでご提供している制御システムに関する資料について、分類の関係で配置場所が判りにくいものが出てきたため、資料の種別ごとに分類を行いConPaS上でご提供いたします。

ガイドライン

報告書

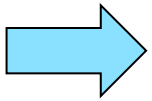


講演資料

NewsLetterバックナンバー

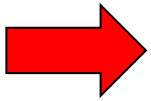
会員登録の手続き

- 制御システムセキュリティ情報共有コミュニティにご登録済の方



手続方法について1月号以降のNewsLetter
（制御システムセキュリティ関連情報）でお知らせいたします。

- 制御システムセキュリティ情報共有コミュニティに未登録の方



JPCERT/CC Webの制御システムセキュリティページ記載の
連絡先まで、制御システムセキュリティ情報共有コミュニティ
登録希望のメールをお送りください。

※フリーメールのメールアドレスでは登録できません。
登録希望のメールは必ず所属組織のドメインの
メールアドレスでメールをお送りください。

ご静聴ありがとうございました

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
Email：icsr@jpcert.or.jp