電力業界におけるサイバー攻撃の脅威とJPCERT/CCの取り組み

2026年1月作成

一般社団法人JPCERTコーディネーションセンター
早期警戒グループ 脅威情報アナリスト　藤堂 伸勝

全体の流れ

1. JPCERT/CCの紹介

2. 電力業界におけるサイバーインシデント事例（当日限定）

3. サイバー攻撃の被害に遭った場合のインシデント対応の流れ（当日限定）

4. JPCERT/CCの取り組み

1. JPCERT/CCの紹介

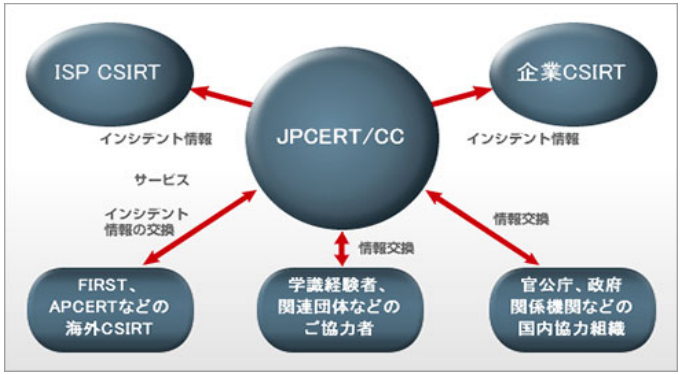
JPCERT/CCとは

■ 一般社団法人JPCERTコーディネーションセンター

Japan Computer Emergency Response Team / Coordination Center

- コンピューターセキュリティインシデントへの対応、国内外にセンサーを置いたインターネット定点観測、ソフトウェアや情報システム・制御システム機器などの脆弱性への対応など、**国内の「セキュリティ向上を推進する活動」**を実施
- **国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等のセキュリティに関わる担当者など**を主な対象として活動
- インシデント対応をはじめ国際連携が必要なオペレーションや情報連携に関し、**日本の窓口となる「CSIRT」**

  ※各国に同様の窓口CSIRTが存在
  （米国のCERT/CC、中国のCNCERT/CC、韓国のKrCERT/CC等）

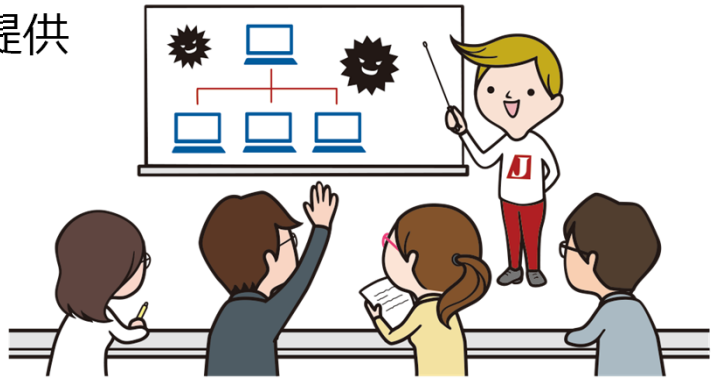


■ 「サイバー攻撃等国際連携対応調整事業」（**経済産業省委託事業**）および「被害組織から円滑に攻撃技術情報を収集する手法に関する検証業務」（**内閣官房委託事業**）を実施

JPCERT/CCの役割

■ コーディネーションセンターとしての活動

- インシデント対応
- 国内外のインシデント対応組織、関連する組織等との連携
- 国内外インシデント対応組織の立ち上げ支援・指導
- インシデントに関する事例解析
- セキュリティに関する各種情報の収集／整理／蓄積／提供
- インシデントに関する調査の受託業務
- 関連技術等の調査・研究
- 関連技術の普及・啓発、教育事業



JPCERT/CCは、非営利法人として中立的な立場から、
“インシデント”に向き合った活動を展開しています。

具体的な活動例

■ 製品の脆弱性への対応（主にPSIRT向け）

— 届けられた製品の脆弱性についての調整、脆弱性情報の公開

例）「報告者 ⇆ IPA ⇆ JPCERT/CC ⇆ 製品開発者」との調整など

■ 収集した情報の分析・発信

— インターネット上の脆弱性情報や脅威情報などを収集・分析・発信

例）注意喚起、CyberNewsFlash、WeeklyReportなど

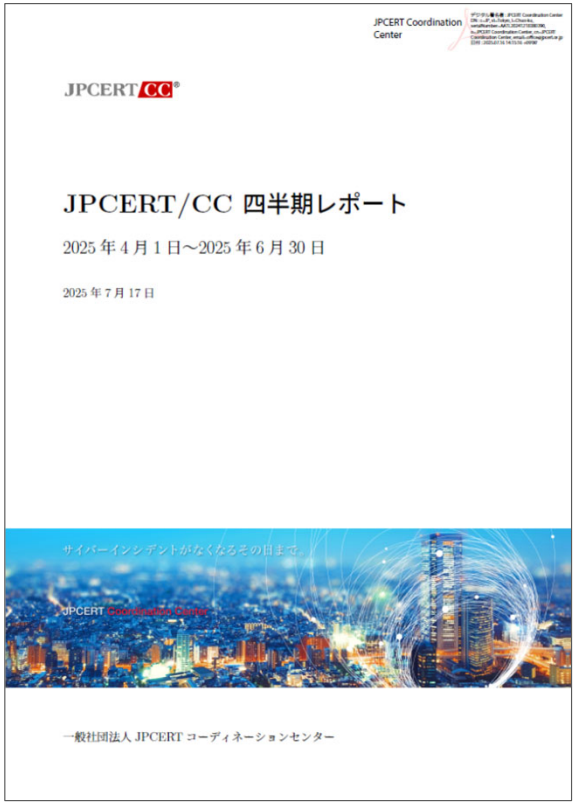
■ 発生したインシデントへの対応（主にCSIRT向け）

— インシデント初動対応への技術的な支援、助言

例）インシデントレスポンス、アーティファクト分析など

（参考）JPCERT/CC 四半期レポート

- 詳細な活動内容は『四半期レポート』で公開しています
  https://www.jpcert.or.jp/qr/index.html


JPCERT Coordination Center

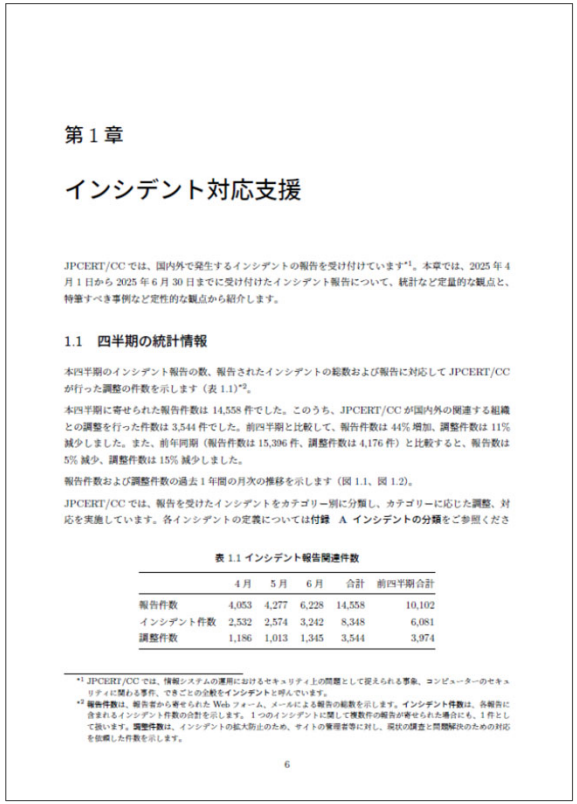
JPCERT/CC

JPCERT/CC 四半期レポート

2025 年 4 月 1 日～2025 年 6 月 30 日

2025 年 7 月 17 日

一般社団法人 JPCERT コーディネーションセンター


第 1 章

インシデント対応支援

JPCERT/CC では、国内外で発生するインシデントの報告を受け付けています*1。本章では、2025 年 4 月 1 日から 2025 年 6 月 30 日までに受け付けたインシデント報告について、統計など定量的な観点と、特筆すべき事例など定性的な観点から紹介します。

1.1 四半期の統計情報

本四半期のインシデント報告の数、報告されたインシデントの総数および報告に対応して JPCERT/CC が行った調整の件数を示します（表 1.1）*2。

本四半期に寄せられた報告件数は 14,558 件でした。このうち、JPCERT/CC が国内外の関連する組織との調整を行った件数は 3,544 件でした。前四半期と比較して、報告件数は 44% 増加、調整件数は 11% 減少しました。また、前年同期（報告件数は 15,396 件、調整件数は 4,176 件）と比較すると、報告数は 5% 減少、調整件数は 15% 減少しました。

報告件数および調整件数の過去 1 年間の月次の推移を示します（図 1.1、図 1.2）。

JPCERT/CC では、報告を受けたインシデントをカテゴリー別に分類し、カテゴリーに応じた調整、対応を実施しています。各インシデントの定義については付録 A インシデントの分類をご参照くださ

表 1.1 インシデント報告関連件数

	4 月	5 月	6 月	合計	前四半期合計
報告件数	4,053	4,277	6,228	14,558	10,102
インシデント件数	2,532	2,574	3,242	8,348	6,081
調整件数	1,186	1,013	1,345	3,544	3,974

*1 JPCERT/CC では、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピューターのセキュリティに関わる事件、できごとの全般をインシデントと呼んでいます。

*2 報告件数は、報告者から寄せられた Web フォーム、メールによる報告の総数を示します。インシデント件数は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数の報告が寄せられた場合にも、1 件として扱います。調整件数は、インシデントの拡大防止のため、サイトの管理者等に対し、脆弱の解消と問題解決のための対応を依頼した件数を示します。

6

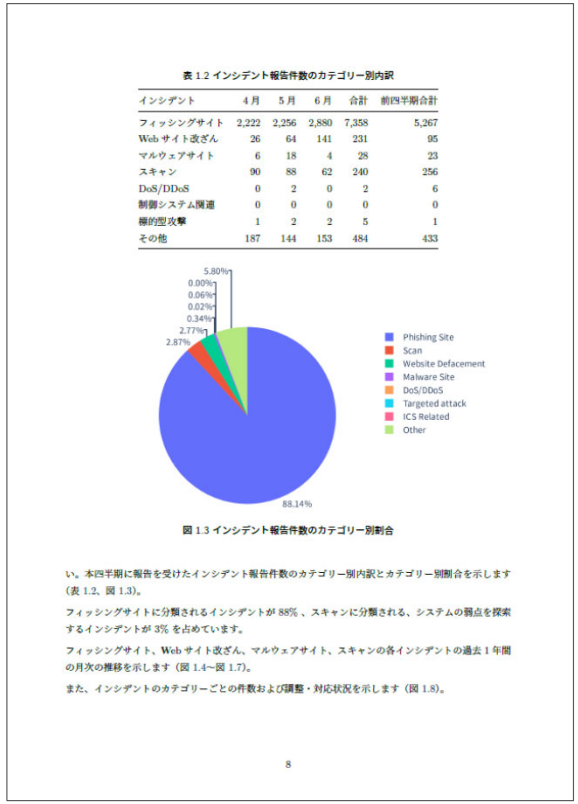


表 1.2 インシデント報告件数のカテゴリー別内訳

インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	2,222	2,256	2,880	7,358	5,267
Web サイト改ざん	26	64	141	231	95
マルウェアサイト	6	18	4	28	23
スキャン	90	88	62	240	256
DoS/DDoS	0	2	0	2	6
制御システム関連	0	0	0	0	0
標的型攻撃	1	2	2	5	1
その他	187	144	153	484	433

図 1.3 インシデント報告件数のカテゴリー別割合

い。本四半期に報告を受けたインシデント報告件数のカテゴリー別内訳とカテゴリー別割合を示します（表 1.2、図 1.3）。

フィッシングサイトに分類されるインシデントが 88%、スキャンに分類される、システムの弱点を探索するインシデントが 3% を占めています。

フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンの各インシデントの過去 1 年間の月次の推移を示します（図 1.4～図 1.7）。

また、インシデントのカテゴリーごとの件数および調整・対応状況を示します（図 1.8）。

8

JPCERT/CCに相談できること

- **インシデント初動対応支援の相談**
  - インシデント発生時の初期段階における必要な調査、対応方針の検討、被害箇所の特定方法について
- **侵入型ランサムウェア攻撃の被害相談**
  - 攻撃者によってファイルが暗号化されたり、情報がリークされた場合の初動段階での対応方法について
- **インシデント調査のセカンドオピニオン**
  - インシデント調査・対応・対策が一通り終了した後、対応に不備がないか
- **類似インシデントの問い合わせ・照会**
  - 調査・対応したインシデントに関して、類似のインシデント情報がないか
- **インシデントのアトリビューションサポート**
  - 調査・対応したインシデントに関して、攻撃主体の特定や攻撃目的、今後想定される攻撃手法について
- **高度サイバー攻撃（標的型攻撃）に関するインシデント調査の相談**
  - 高度サイバー攻撃のインシデント調査（被害範囲の特定、侵入経路の調査、攻撃アクターの特定など）
- **マルウェア感染、不正アクセスに関する相談**
  - マルウェアに感染した際の駆除方法、復旧方法について
  - サーバーへの侵入やDoS攻撃が発生した際の対処について
- **インシデント被害の公表に関する相談**
  - 発生したインシデントの公表や関係組織への連絡について
- **その他インシデントに関する各種相談**

「インシデント相談・情報提供（被害組織／保守・調査ベンダー向け）」から抜粋
https://www.jpcert.or.jp/ir/consult.html

JPCERT/CCに依頼できること

- **インシデント初動対応のサポート依頼**
  - インシデント発生時の初期段階において、必要な調査、対応方針の検討、被害箇所の特定などをサポート
- **高度サイバー攻撃（標的型攻撃）に関するインシデント調査サポート依頼**
  - 高度サイバー攻撃のインシデント調査（被害範囲の特定、侵入経路の調査、攻撃アクターの特定など）をサポート
- **改ざんされたサイトへの対応依頼**
  - サイト管理者へWebサイトが改ざんされていることを連絡し、対処を依頼
- **マルウェアを公開しているサイトへの対応依頼**
  - サイト管理者へWebサイトなどにおいてマルウェアが公開されていることを連絡し、対処を依頼
- **マルウェアが通信を行うサーバーの管理者への対応依頼**
  - サーバー管理者へ連絡し、システムの調査などを依頼
- **フィッシングサイトの閉鎖依頼**
  - サイト管理者へフィッシングサイトが公開されていることを連絡し、フィッシングサイトの停止を依頼
- **ポートスキャンを行った攻撃元IPアドレスの管理者への対応依頼**
  - 攻撃元IPアドレスの管理者へポートスキャンのログ情報などを提供し、調査、対応を依頼
- **DoS/DDoS攻撃の攻撃元IPアドレスの管理者への対応依頼**
  - 攻撃元IPアドレスの管理者へ攻撃に関するログ情報を提供し、調査、対応を依頼
- **制御システムインシデント報告・対応依頼**
  - 国内の制御システムや各種プラントが対象と考えられるセキュリティインシデントに関しての報告受け付け

「インシデント対応依頼」から抜粋 https://www.jpcert.or.jp/form/

JPCERT/CCへの相談・依頼について

■ 国からの委託事業として無償対応するもの

- 前述した相談・依頼全般
- JPCERT/CCが発信する各種情報の受信
  （メールニュース、情報共有ポータルでの情報提供など）
- 業界団体や複数企業が参加する講演・セミナー・研修・演習
  ※監査やコンサルティングなどは対象外

■ 法人の自主事業として有償対応になるもの

- 単一／個別企業内の研修・机上演習・訓練など

4. JPCERT/CCの取り組み

JPCERT/CCが配信している情報

	種別	内容	発行間隔	対象	配信方法
1	注意喚起	国内へ大きな影響を与えると考えられる「脆弱性情報」「脅威情報」などについての概要と対策などをまとめた情報	適宜	企業、一般ユーザー	Webサイト（一般に公開）
2	Weekly Report	過去1～2週間に公開された「脆弱性情報」「脅威情報」「セキュリティ情報」をサマリーとしてまとめた情報	毎週	企業、一般ユーザー	
3	CyberNewsFlash	注意喚起を発行するまでに至らない「脆弱性情報」「脅威情報」などについての概要と対策などをまとめた情報	適宜	企業、一般ユーザー	
4	早期警戒情報	国内へ大きな影響を与えたり、重要インフラ事業者へ影響を与える可能性がある「脆弱性情報」「脅威情報」などについての概要と対策などをまとめた情報	適宜	重要インフラなど	CISTA + Email
5	インディケータ情報	標的型攻撃に使用されたC2サーバーなどの情報	適宜	重要インフラなど	
6	Analyst Note	日々収集する「脆弱性情報」「脅威情報」「セキュリティ情報」のうちアナリストが重要と判断した情報	毎日	重要インフラなど	
7	リアルタイム情報	JPCERT/CCが収集している「脆弱性情報」「脅威情報」「セキュリティ情報」※リアルタイムで共有し、その日のAnalyst Noteに集約される	適宜	重要インフラなど	
8	個別通知	個別の組織に関わる情報（脆弱性を突かれてシステムが侵害されているなどの情報）	適宜	重要インフラなど	

CISTAで提供する情報のサンプル

＜取扱留意情報（GREEN）＞

JPCERT/CC 早期警戒グループ
JPCERT-EW-2023-1001
2022-10-17（新規）
2022-10-23（更新）

<<< Cisco IOS XEのWeb UIにおける権限昇格の脆弱性（CVE-2023-20198）に関する早期警戒情報 >>>

I. 概要
2023年10月16日（現地時間）、CiscoはCisco IOS XE ソフトウェアのWeb UI機能における権限昇格の脆弱性に関する情報を公開しています。同製品のWeb UI機能をインターネットまたは信頼されないネットワークに公開している場合、本脆弱性が悪用され、遠隔の認証されていない攻撃者が、特権レベル15のアクセス権を持つアカウントを作成し、当該システムを制御する可能性があります。

** 更新: 2023年10月23日追記 **********
2023年10月22日（現地時間）、Ciscoはアドバイザリを更新し、新たな脆弱性の情報と攻撃の内容に関する情報を公開しています。Ciscoは、CVE-2023-20198に加えて、新たにWeb UI機能の別コンポーネントの脆弱性にCVE-2023-20273を割り当てています。Ciscoの調査によると、攻撃者は、CVE-2023-20198を悪用してシステムに侵入し、特権レベル15のコマンドを発行して新たなローカル

早期警戒情報

取扱注意情報(AMBER)

****
情報の共有範囲
本情報は、取扱注意情報(AMBER)です。本早期警戒情報は、機密性の高い非公開情報を含むため情報の共有範囲が制限されます。共有範囲は自組織および関連組織内の必要最小限としてください。（Web サイトや公開のメーリングリストなどを使用して一般へ公開することを禁止します。）
****

[攻撃に関する情報]

JPCERT/CC では国内の組織に対して行われた標的型攻撃に関する情報を入手いたしましたので、参考までに情報をお伝えします。
以下の標的型攻撃に関する情報を参考のうえ、自システム等の確認をお勧めします。

(標的型攻撃に関する情報(JPCERT-WW-APT-201605-X))

1) 攻撃が行われた期間
2023年 1月以降

2) 攻撃に使用された通信先
example[.]com 80/TCP(HTTP)
※ 安全のため通信先の一部を、[.]に置き換えています。

インディケータ情報

Analyst Note

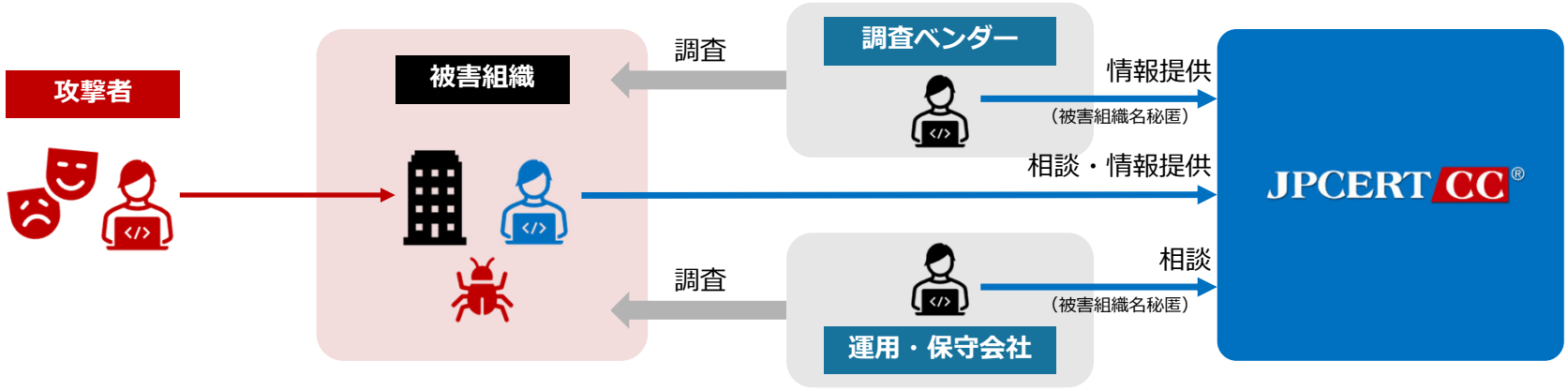
```
**********
JPCERT/CC Analyst Note - 2025/10/09
**********

目次
========
1. 本日の情報
   a.脆弱性情報
   b.脅威情報
   c.セキュリティ情報

2. JPCERT/CCからの情報

**********
本日の情報
**********

a.脆弱性情報
========================================
1. 2025-10 Security Bulletin: Juniper Security Director: Insufficient authorization for sensitive resources in web inte
 https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Juniper-Security-Director-Insufficient-authorize
# 2025年10月8日（現地時間）、Juniper Networksは本脆弱性を含む20件（Critical 2件、
# High 6件、Medium 12件）の脆弱性情報を公表しました。

2. ArcGIS Server Feature Services Security Patch
 https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-feature-services-security-patch
# 2025年10月6日（現地時間）、米Esri社が地理情報システム（GIS）ソフトウェア
# ArcGIS ServerにおけるSQLインジェクション脆弱性（CVE-2025-57870）に関する
# アドバイザリを公表しました。CVSS v4.0ベーススコアは10です。脆弱性の悪用は
# 確認されていませんが、同製品の利用者に向けて2週間以内のパッチ適用を同社は
# 推奨しています。

b.脅威情報
========================================
1. 0day .ICS attack in the wild
 https://strikeready.com/blog/0day-ics-attack-in-the-wild/
# 2025年1月に公表されたZimbra Collaboration Suiteの脆弱性
#  （CVE-2025-27915）について、悪用を分析したレポートが公開されました。
# ZimbraのWebメールを標的とし、悪意あるカレンダーファイル（拡張子.ics）を
```

JPCERT/CC情報共有会

- **CISTAに登録している組織を対象に**、年3回の情報共有会（セミナー）を開催
- 外部からの有識者による講演、JPCERT/CCのアナリストによる分析等を発表
  テーマ例：IoT、企業のセキュリティ対策とその取り組み、最新の攻撃動向、マルウェア分析結果 など
- 後日、YouTubeによる動画配信（限定公開）を実施

インシデント相談・情報提供のイメージ

- インシデント対応に関する相談や依頼は、被害組織からだけでなく、**セキュリティベンダーや運用保守会社からも受け付け**ている
  - 相談内容（例）
    - インシデント初動対応支援の相談
    - 侵入型ランサムウェア攻撃の被害相談
    - インシデント調査のセカンドオピニオン
    - 類似インシデントの問い合わせ・照会 など



制御システムセキュリティカンファレンス2026

■ 毎年「制御システムセキュリティカンファレンス」を開催

- 経済産業省とJPCERT/CCで共催
- ICSセキュリティの技術的な情報を提供
- プログラム構成の主な特徴
  - さまざまな業種のICSセキュリティの取り組みを紹介
  - ICSユーザーの対策に資する講演
  - ICSセキュリティの国際的な動向の紹介

※画像は「制御システムセキュリティカンファレンス2024」から

国内のICSステークホルダーにおけるICSセキュリティ向上を目的に企画し、**特定企業のサービスや製品等の宣伝に資する内容を扱わないように心掛け**ています

2026年の講演資料などはこちらからご確認ください
https://www.jpcert.or.jp/event/ics-conference2026.html

JPCERT/CCは、国内のインシデントをなくすことを
ミッションに掲げ、日々活動しています。
お困りごとがあれば、ぜひお気軽にご相談ください！

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

—Email：pr@jpcert.or.jp
—https://www.jpcert.or.jp/reference.html

インシデント報告

—Email：info@jpcert.or.jp
—https://www.jpcert.or.jp/form/

脆弱性に関するお問い合わせ

—Email：vultures@jpcert.or.jp
—https://jvn.jp/

■ 組織の皆さまからのお問い合わせ（国内コーディネーショングループ）

Email：dc-info@jpcert.or.jp
https://www.jpcert.or.jp/

■ CISTA登録等に関する連絡先

Email：cista-sec@jpcert.or.jp