JPCERT CC®

Emotet感染の確認方法と対策

2022年3月

一般社団法人JPCERTコーディネーションセンター

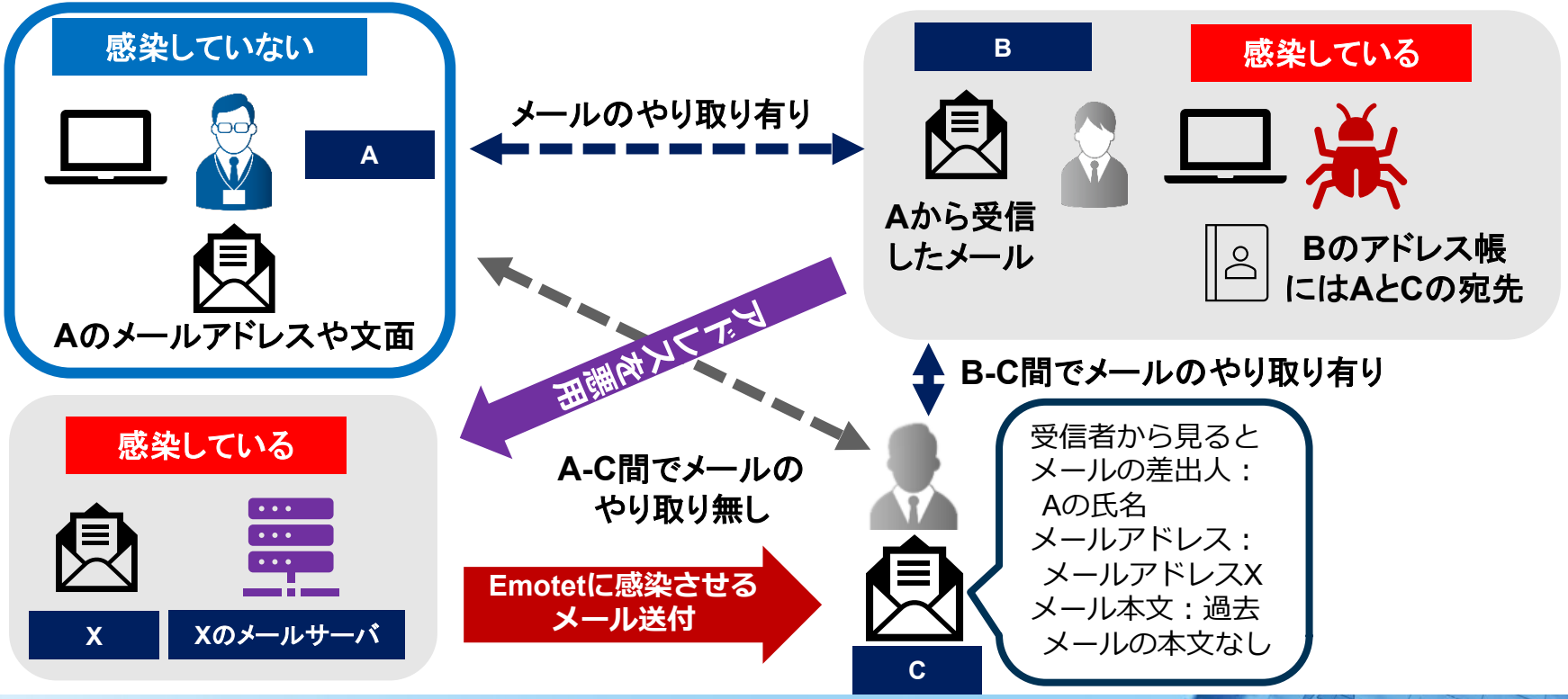
Emotetに感染してる？

1-1. Emotet感染に気づくポイント

- Emotetに感染していると起こる症状
  - 不審なファイルが添付されたメールが自分の名前で送られる
    - 過去のメール本文が引用されることもある
  - メールに添付されたパスワード付きzipやxlsmを開いたが中身はコンテンツの有効化を促す英語のみだった
    - 送信者に確認しても送った覚えがないと言われる
  - 送った覚えのないメールのエラーメールが返ってくる
  - メールサーバーの調子が悪い

1-3.Emotet感染によるなりすましメール送信

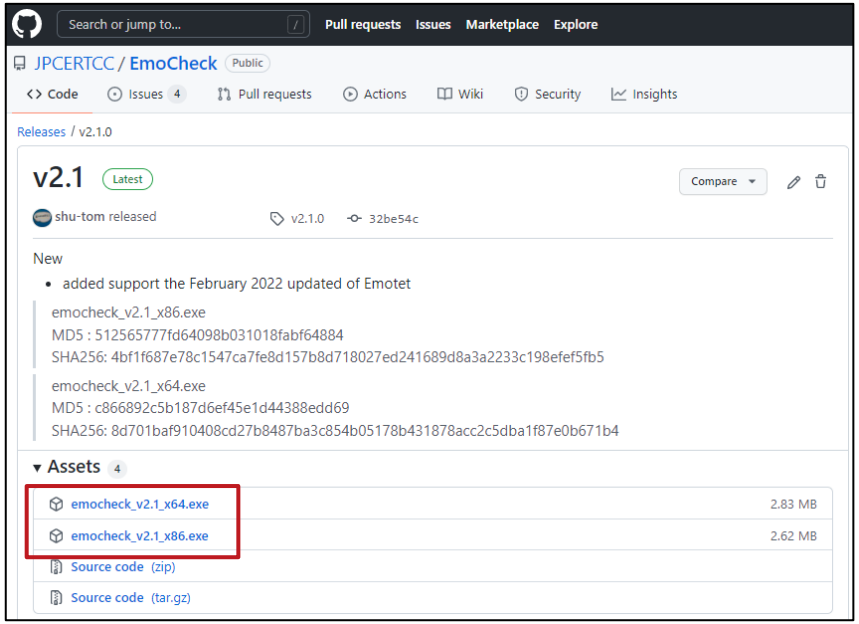
■送信元がなりすまされているケース



Emotet感染有無の確認方法

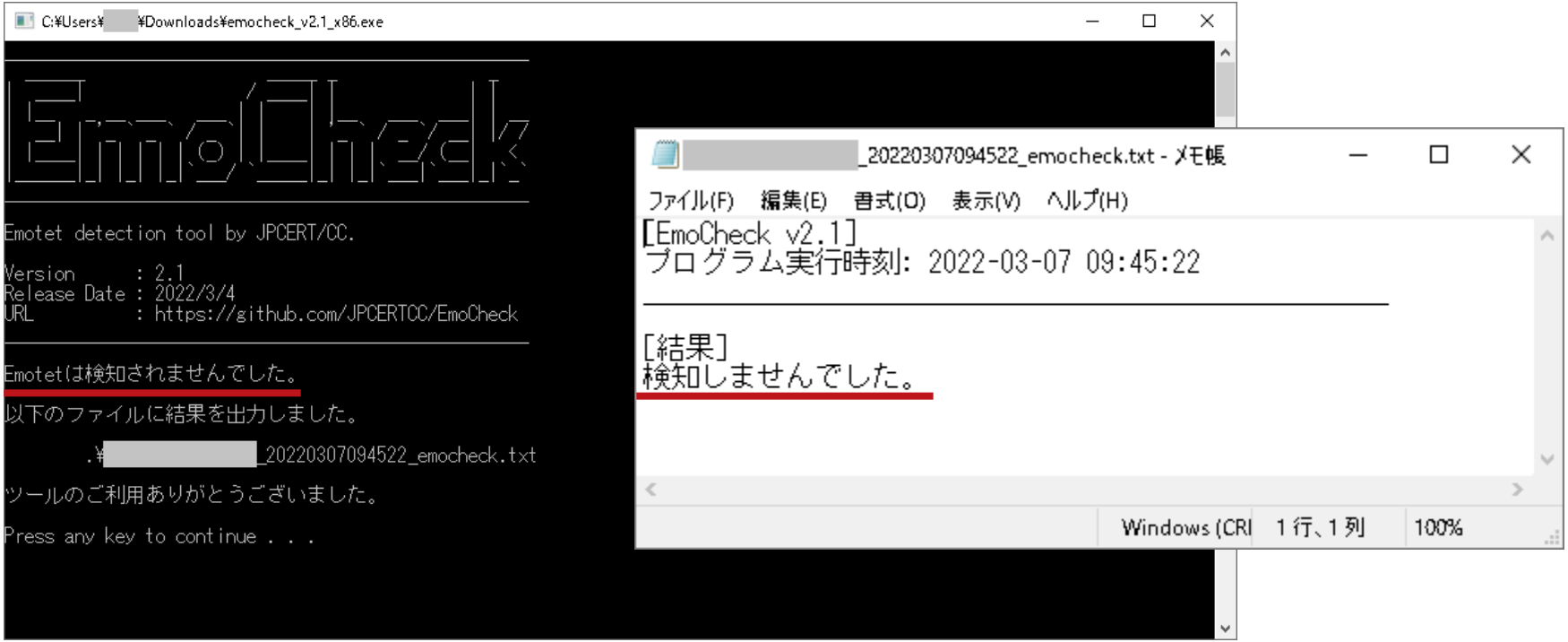
2-1. EmoCheck（エモチェック）

- Emotetの感染有無を確認するのに特化したツール
  - JPCERT/CCにて開発、githubで公開
    https://github.com/JPCERTCC/EmoCheck/releases
  - ダウンロードして端末上でダブルクリックで実行
    - x86版とx64版が存在
      不明な場合はx86版を使用
  - 感染疑いのあるユーザーで実行
  - 現時点で最新のEmotetを検出できることを確認済



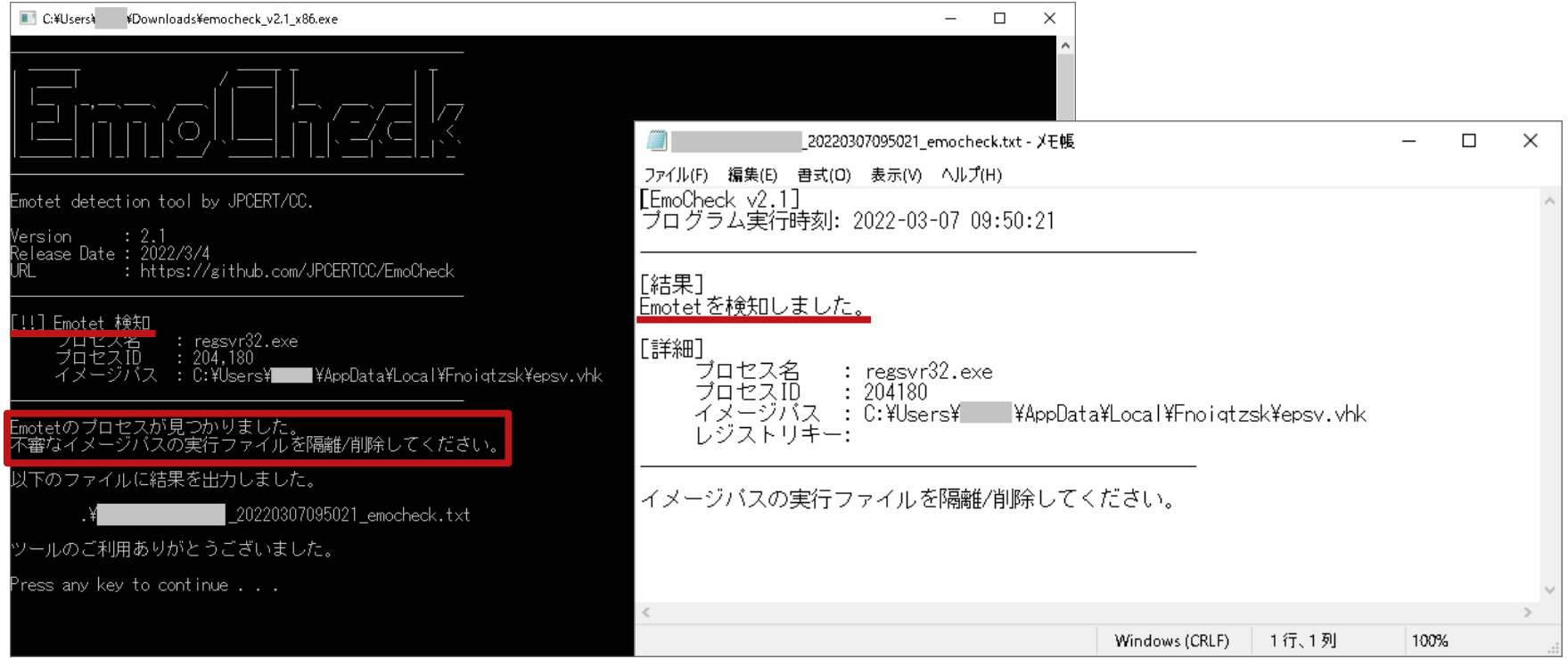
2-1. EmoCheck（エモチェック）

- Emotetを検出しなかった場合の出力



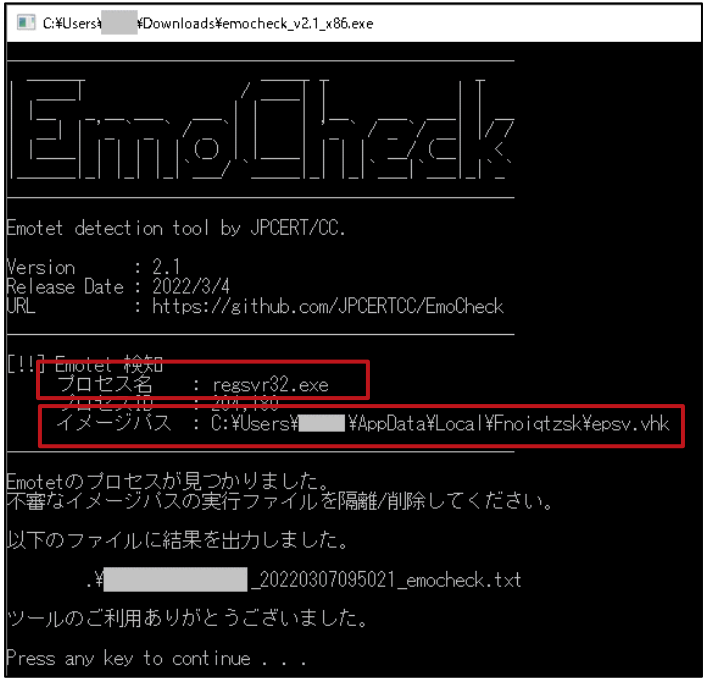
2-1. EmoCheck（エモチェック）

- Emotetを検知した場合の出力



2-1. EmoCheck（エモチェック）

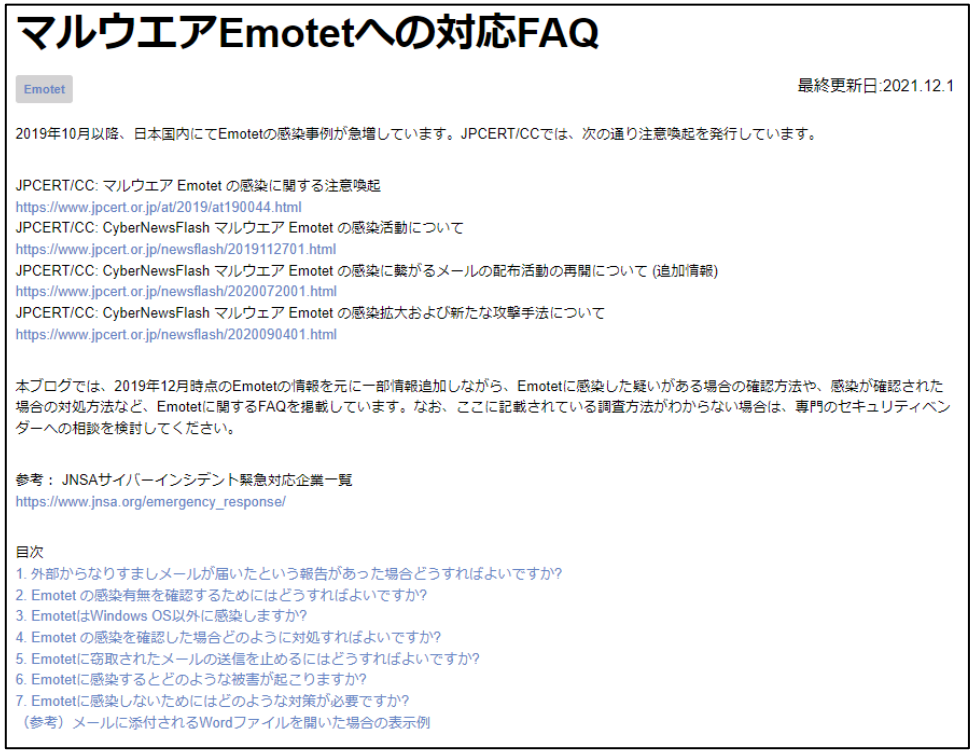
- Emotetを検知した場合の対応
  - プロセス名に表示されたプロセスをタスクマネージャーで停止する
  - イメージパスにあるファイルがEmotet本体、それを削除する
  - メールの情報も盗まれるためメールのパスワードの変更が必須
  - 他のマルウェアに追加で感染する場合もあるためウイルス対策ソフトでフルスキャンを推奨



2-2.マルウエアEmotetへの対応FAQ

- JPCERTではEmotetの対応FAQをブログで公開
  - 感染していた場合の対応手順や感染を防ぐための対策などを記載
    - Windows OSしか感染しない
    - メールの送信を止める手立てはない

  といったことも記載



マルウエアEmotetへの対応FAQ

Emotet

最終更新日:2021.12.1

2019年10月以降、日本国内にてEmotetの感染事例が急増しています。JPCERT/CCでは、次の通り注意喚起を発行しています。

JPCERT/CC: マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
https://www.jpcert.or.jp/newsflash/2020072001.html
JPCERT/CC: CyberNewsFlash マルウェア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

本ブログでは、2019年12月時点のEmotetの情報を元に一部情報追加しながら、Emotetに感染した疑いがある場合の確認方法や、感染が確認された場合の対処方法など、Emotetに関するFAQを掲載しています。なお、ここに記載されている調査方法がわからない場合は、専門のセキュリティベンダーへの相談を検討してください。

参考： JNSAサイバーインシデント緊急対応企業一覧
https://www.jnsa.org/emergency_response/

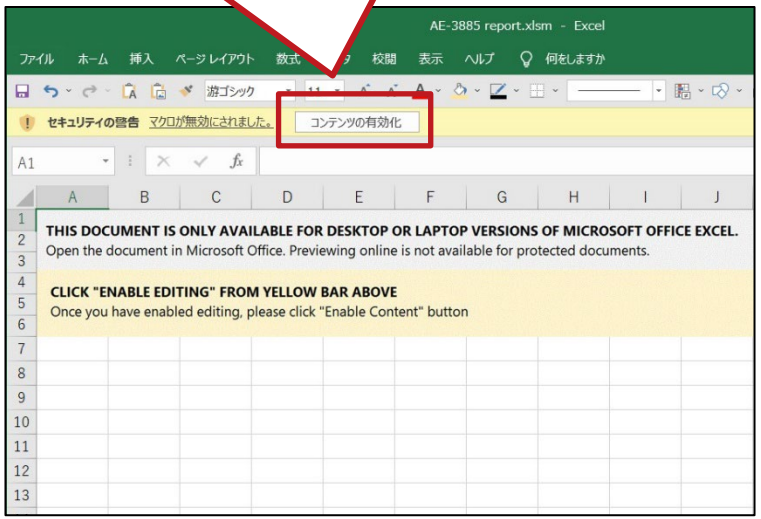
目次
1. 外部からなりすましメールが届いたという報告があった場合どうすればよいですか?
2. Emotet の感染有無を確認するためにはどうすればよいですか?
3. EmotetはWindows OS以外に感染しますか?
4. Emotet の感染を確認した場合どのように対処すればよいですか?
5. Emotetに窃取されたメールの送信を止めるにはどうすればよいですか?
6. Emotetに感染するとどのような被害が起こりますか?
7. Emotetに感染しないためにはどのような対策が必要ですか?
（参考）メールに添付されるWordファイルを開いた場合の表示例

Emotetへの対策

3-1. Emotetの感染対策

- Office製品のマクロ実行の無効化
  - ファイル→オプション→トラストセンター→設定
  - マクロを使わない組織は無効化
  - 使う場合は警告を表示して無効化

「コンテンツの有効化」を押さない。押すと感染



3-1. Emotetの感染対策

- 一般的な不審なメール対策を行う
  - メールの添付ファイル、リンクには注意する
  - Office製品の「コンテンツの有効化」は押さない
  - セキュリティ製品を導入し、定期的な確認やチューニングを行う
  - 組織内への注意喚起

- 組織の管理者向け
  - URLHaus、FeodoTrackerのIoC活用
    - EmotetのダウンロードURLやC2の情報があり、遮断に活用

参考

- マルウエアEmotetへの対応FAQ
  - https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
- JPCERTCC/EmoCheck – GitHub
  - https://github.com/JPCERTCC/EmoCheck/releases
- 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
  - https://www.ipa.go.jp/security/announce/20191202.html
- URLhaus （EmotetのダウンロードURLを掲載）
  - https://urlhaus.abuse.ch/
- Feodo Tracker （EmotetのC2サーバーを掲載）
  - https://feodotracker.abuse.ch/
- とあるEmotetの観測結果
  - https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_104_sajo-sasada_jp.pdf
- Emotet vs EmoCheck
  - https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_5_tani-kino-sajo_jp.pdf

お問合せ、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/

インシデント報告

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

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html