長崎県 CSIRT 活動表明文書

（バージョン 1.03　　2023 年 5 月 1 日）

CSIRT 活動表明文章

目 次

1　文書情報（Document Information）

（1）最終更新日（Date of Last Update）

バージョン 1.01（作成日：2022 年 4 月 1 日）
バージョン 1.02（作成日：2023 年 4 月 1 日）
バージョン 1.03（作成日：2023 年 5 月 1 日）

（2）通知の他の配布リスト（Distribution List for Notifications）

CSIRT 活動表明文章が変更となった場合には、長崎県ホームページにて報告する。

（3）本文書の場所（Locations where this Document May Be Found）

長崎県ホームページにて報告する。

2　連絡先情報（Contact Information）

（1）チーム名（Name of the Team）

長崎県 CSIRT

（2）所在地（Address）

〒850-8570　長崎県長崎市尾上町３－１
長崎県総務部スマート県庁推進課
長崎県 CSIRT 事務局

（3）時間帯（Time Zone）

JST（日本標準時）

（4）電話番号（Telephone Number）

095-895-2233

（5）ファクシミリ番号（Facsimile Number）

非公開

（6）他の音声通信手段（Other Telecommunication）

なし

（7）電子メールアドレス（Electonic Mail Address）

非公開（電子メールによる受付は別途報告窓口による）

（8）チームメンバー（Team Members）

統括情報セキュリティ責任者
総務部スマート県庁推進課総括課長補佐

（9）受付時間（Reception Hours）

報告窓口　24 時間 365 日
電話受付　9:00-17:00 JST（土日祭日、年末年始を除く）

3　憲章（Charter）

（1）ミッションステートメント（Mission Statement）

長崎県の情報セキュリティインシデントに迅速かつ適切な対応を行うため、緊急即応体制として長崎県 CSIRT を設置する。

（2）サービス対象者（Constituency）

長崎県 CSIRT は長崎県庁の行政機関を対象とする。

（3）権限（Authority）

長崎県 CSIRT は長崎県最高情報セキュリティ責任者の下、情報セキュリティ委員会、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ担当者およびシステム管理者と連携して活動する。

4　ポリシー（Policies）

（1）インシデントの種類（Type of Incident and Level of Support）

長崎県 CSIRT が対応する基本的なインシデントの種類を以下のとおりとする。

1．不正アクセス：第三者より管理者が意図しないアクセスを受ける。
以下の内容も、不正アクセスに分類する。
・内部不正によるアクセス：悪意を持つ県職員等内部の利用者が、許可されていないアクセスを行う。

2．マルウェア感染：悪意のあるソフトウェア（コンピュータウイルス、ワーム等を含む）に感染する。
以下の内容も、マルウェア感染に分類する。
　・ランサムウェア：感染したコンピュータのファイルを暗号化したり、コンピュータを使用できない状況にしたりし、金銭を要求される。
　・標的型攻撃：特定の組織を標的にしたサイバー攻撃で、一連の攻撃ステップ（侵入、情報収集、情報送出）により情報を窃取される。

3．Web 改ざん：脆弱性攻撃や、不正アクセスにより Web サイトのコンテンツを変更・削除される。

4．DoS,DDoS：回線帯域やコンピュータリソースに負荷がかかり、サービス運用を妨害される。

5．アカウント不正利用：アカウント情報が第三者により不正に利用される。

6．インターネットを利用した金銭詐欺：インターネットを利用した詐欺により金銭を詐取される。以下の内容も、インターネットを利用した金銭詐欺に分類する。
　・ビジネスメール詐欺：巧妙に細工した電子メールのやりとりにより担当者を騙し、攻撃者の用意した口座へ送金させられる。

7．迷惑メール送信：長崎県が管理するメールサーバから迷惑メールが送信される。

8．情報漏えい：個人情報もしくは機密情報を窃取される。
以下の内容も、情報漏えいに分類する。
　・フィッシング：利用者は正規サイトを装った不正サイト（フィッシングサイト）へ誘導され、ID/パスワード等を詐取される。
　・内部不正による情報漏えい：悪意を持つ県職員等内部の利用者が情報を外部へ持ち出す。
　・電子メール誤送信：悪意のない県職員等正規利用者による電子メールの送信先設定誤り、誤ったファイルの添付等による電子メール送信で情報漏えいが発生する。
　・文書の誤発送：悪意のない県職員等による郵便物の宛名間違え、誤った文書の送付等により情報漏えいが発生する。

9．情報資産の盗難・紛失：物理的な情報資産（コンピュータ、ハードディスク、USB メモリ、CD-ROM、印刷物等）を盗難され、もしくは紛失する。

なお、上記に該当しないインシデントであっても、インシデント対応支援要請がある場合には、必要に応じてインシデントを直接対応する部署に対して支援を行う。

(2) 協力、連携、情報開示 (Co-operation, Interaction and Disclosure of Information)

長崎県 CSIRT が他組織やコミュニティと相互に協力し、活動し、あるいは情報を開示するにあたっては、該当する対外的な各組織に応じて各々以下のとおり対応する。

・総務省との連携に関するポリシーは、機密情報に関する事前の取り決めの範囲内で、対応および情報の開示を行う。

・市町との連携に関するポリシーは、機密情報に関する事前の取り決めの範囲内で、対応および情報の開示を行う。

・他組織(JPCERT,IPA など)との連携に関するポリシーは、機密情報に関する事前の取り決めの範囲内で、対応および情報の開示を行う。

・警察機関への情報提供に関するポリシーは、機密情報に関する事前の取り決めに関わらず、警察機関が調査目的のために要求する情報を含め、全面的に協力する。

・報道機関に対するポリシーは、広報部門のポリシーに準じる。

(3) コミュニケーションと本人認証 (Communication and Authentication)

機密情報を含むセキュリティインシデントに関する情報を送付する場合には、メールを用い、本文には記載せず暗号化添付ファイル等適切なセキュリティ対策を施した方法にて送付すること。

5　サービス（Serveices）

インシデント対応（Incident Response）

インシデント対応に必要な技術情報のハンドリングをすることにより、サービス対象者のインシデント対応を支援する。

a　インシデントトリアージ（Incident Triage）

報告されたインシデントの発生状況を確認し、インシデントか否かの判断、重要度および優先順位等を決定する。

b　インシデントコーディネーション（Incident Coordination）

・外部に公開する必要があると判断したインシデントについては、外部機関と協力し情報を公開する。
・長崎県 CSIRT のみで対応できないインシデントについては、他の組織に協力を仰ぎ、必要に応じて、警察機関に連絡する。

c　インシデント解決（Incident Resolution）

発生したインシデントに対し、封じ込め・根絶を行い、インシデントの対応活動の活動履歴を残し、再発防止策の検討を行う。

6　インシデント報告フォーム（Incident Reporting Forms）

長崎県 CSIRT に対するインシデント報告は、以下のフォームより行う。
https://apply.e-tumo.jp/pref-nagasaki-u/offer/userLoginDispNon.action?tempSeq=1444&accessFrom=

また、上記のインシデント報告フォームが使用できない場合は、以下の電話番号で受付を行う。
095-895-2233

＜記入事項＞
■報告者情報
お名前
お電話番号
メールアドレス

7　免責事項（Disclaimers）

本文書、または本文書に含まれる情報を利用することで、直接・間接的に生じた損失に関し、長崎県 CSIRT は一切責任を負わないものとする。