プロジェクト名：　　IT セキュリティ対策プロジェクト

組織内 CSIRT 構築

CSIRT 記述書

（バージョン 1.6　　2019 年 4 月 1 日）

担当部署	作成者
総務部　IT セキュリティ対策室長	木内　健二

CSIRT 記述書（Description）

目　次

1　文書情報（Document Information）

（1）最終更新日（Date of Last Update）

✧　バージョン　0.1（作成日：2017 年 4 月 27 日）
✧　バージョン　1.0（更新日：2017 年 4 月 27 日）
✧　バージョン　1.1（更新日：2018 年 4 月　5 日）
✧　バージョン　1.2（更新日：2018 年 6 月　1 日）
✧　バージョン　1.3（更新日：2018 年 9 月 14 日）
✧　バージョン　1.4（更新日：2018 年 10 月　4 日）
✧　バージョン　1.5（更新日：2019 年 2 月　1 日）
✧　バージョン　1.6（更新日：2019 年 4 月　1 日）

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

✧　CSIRT 記述書が変更となった場合には、弊社ホームページにて報告します。

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

✧　現在のバージョンの記述書は、弊社ホームページで公開されています。
　　JTB ホームページ（https://www.jtbcorp.jp/jp/）

2　連絡先情報（Contact Information）

（1）　チーム名（Name of the Team）

✧　正式名称：JTB-CSIRT Team（ジェイティービーシーサートチーム）

✧　略称：JTB-CSIRT

（2）　所在地（Address）

✧　東京都品川区東品川二丁目 3 番 11 号　JTB ビル
株式会社 JTB　総務部 IT セキュリティ対策室

（3）時間帯（Time Zone）

✧　東京／日本（GMT＋0900）

（4）電話番号（Telephone Number）

✧　＋81 3 5796 5839（“JTB-CSIRT”と尋ねてください）

（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）

✧　上記の電話以外の音声通信回線は用意されていません。

（7）チームメンバー（Team Members）

✧　JTB-CSIRT Team 代表者　木内健二（IT セキュリティ対策室長）

✧　メンバー　迫田肇 IT セキュリティ対策担当副主幹、杉野宏彰担当部長、椎野紘平担当マネージャー、末木理美担当

（8）業務時間（Operating Hours）

✧　09：30－18：00（GMT＋09:00）（土日祝日を除く、平日のみ）

（9）　顧客連絡先（Points of Customer Contact）

✧　JTB-CSIRT Team に対する連絡は電話にてお願いします。
JTB-CSIRT Team（＋81 3 5796 5839）

✧　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頂く場合には、別途メールアドレスをお知らせいたします。

✧　日本語のみ対応しております。

3　憲章（Charter）

(1)　ミッションステートメント（Mission Statement）

✧ 弊社及び連結決算会社の従業員に対し、コンピュータセキュリティインシデントによる被害が軽減されるための環境および仕組みの構築への支援をする。
✧ 弊社及び連結決済会社の従業員に対し、インシデントが発生した場合の対応の支援をする。

(2)　サービス対象者（Constituency）

✧ 弊社及び連結決算対象会社の従業員

(3) スポンサーシップと提携（Sponsorship and/or Affiliation）

✧ JTB-CSIRT Team は株式会社 JTB の予算で活動をしています。

(4) 権限（Authority）

✧ JTB-CSIRT Team は株式会社 JTB の統制の中で活動します。
✧ JTB-CSIRT Team のメンバーは、インシデント対応のために弊社及び連結決算会社の管理者（担当者）と協力して活動を行います。
✧ JTB-CSIRT Team のメンバーは、JTB グループのセキュリティポリシーの策定に深く関わっています。

4　ポリシー（Policies）

(1)　インシデントの種類とサポートレベル（Type of Incident and Level of Support）

✧ JTB-CSIRT Team で対応可能なインシデントの種類とその対応レベルは以下の通りです。
- マルウェア感染
- 外部からの攻撃（DDoS など）等

✧ JTB-CSIRT Team がインシデントを直接対応することはありません。弊社及び連結決算会社の管理者（担当者）、或いはインシデントを直接対応する各部署に対してサポートをします。
✧ JTB-CSIRT Team は JTB グループ内にて様々なインシデントの発生の未然防止の努力として、様々な技術情報や最新セキュリティ動向に関する情報を提供していきます。

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

✧ 他社のインシデント対応チームとの連携に関するポリシーは、機密情報の取り扱いに関する事前の取り決めの範囲内で、JTB-CSIRT Team は情報をゆだねます。
✧ 警察機関への情報提供に関するポリシーは、機密情報の取り扱い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をする情報を含め、JTB-CSIRT Team は全面的に協力します。
✧ 報道機関に対するポリシーは、弊社の管理部門のポリシーを活用します。

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

✧ 機微な情報を取り扱う場合は、メールではなく弊社指定のサービスを利用すること。
✧ 社内情報共有の仕組みを活用して、最新のセキュリティ動向および関連する技術情報の提供をします。

5　サービス（Serveices）

(1) インシデント対応（Incident Response）

✧ JTB-CSIRT Team は、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、管理者（担当者）、ネットワーク管理者のインシデント対応を支援します。

(1)-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が、本当に発生しているかどうか調査をします。
インシデントの影響範囲を見積もります。

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

✧ インシデントの原因に基づき、関係するところに連絡をします。
✧ 必要により、管理部門を通して警察に通知をします。
✧ 必要により、他の CSIRT に報告をします。
✧ 必要により、全ユーザに対する告知文を作成します。

(1)-c　インシデント解決（Incident Resolution）

✧ パッチの適用などにより、脆弱性を取り除きます。
✧ 証拠の収集をします。

(2)　予防的活動（Proactive Activities）

✧ 社内情報共有の仕組みを活用して、最新のセキュリティ動向および関連する技術情報の提供をします。

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

✧ JTB-CSIRT に対するインシデント報告は、以下の電話番号までご報告ください。
JTB-CSIRT Team（＋81 3 5796 5839）

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、JTB-CSIRT Team は一切責任を負わないものとします。