第三者による脆弱性情報開示ガイドライン

本ガイドラインは、第三者がサイボウズ株式会社（以下、「サイボウズ」という）の製品およびサービスに関する脆弱性情報および検証を実施した際に知り得た挙動に関する情報（以下、「脆弱性情報等」という）を、開示、公表（以下、総称して「開示」という）をおこなう際に参照するガイドラインです。

脆弱性情報等開示に関する規約

脆弱性情報等の開示については、「サービスご利用規約」「脆弱性報奨金制度規約」の記載も併せてご参照ください。

「サービスご利用規約」制限・禁止事項

https://www.cybozu.com/jp/terms/

「脆弱性報奨金制度規約」第５条 脆弱性情報等の取扱い

https://cybozu.co.jp/products/bug-bounty/pdf/terms.pdf

脆弱性情報等の開示内容および方法

脆弱性情報等は、サイボウズから承諾を得た場合に限り、開示することができます。
承諾にあたっては、サイボウズが脆弱性情報等を精査したうえで、開示可否の判断および開示内容、開示時期の調整を行わせて頂きます。
開示をご希望の際は、以下へご連絡ください。

お問い合わせ窓口

〒103-6028 東京都中央区日本橋二丁目７番１号 東京日本橋タワー 27 階

サイボウズ株式会社　Cy-PSIRT 事務局

productsecurity@cybozu.co.jp

クラウド版特有の脆弱性情報等

クラウド版特有の脆弱性情報等については、サイボウズの承諾後、以下の開示方法に従い、開示することができます。
クラウド版特有の脆弱性情報とは、パッケージ版では発生せず、クラウド版にのみ発生する脆弱性を意味します。

例えば、クラウド版の機能がパッケージ版でも実装されており、当該脆弱性がパッケージ版でも発生する場合は、クラウド版特有の脆弱性情報等には該当しません。

開示方法

- メールアドレス・サーバー・サイト URL 等で利用する「cybozu.com」、「cybozu-dev.com」のサブドメインには例として「example」を記載する
  例：example.cybozu-dev.com
- メールアドレス・サーバー・サイト URL 等で利用する「cybozu-dev.com」、「cybozu.com」以外のドメインを例として利用する場合は、RFC2606 に沿って記載する
  例：example.com
- IP アドレスを例として利用する場合は、RFC6890 に沿って記載する
- 名前や組織・団体名には、ユーザーA といった架空の名称、またはサイボウズのデモデータの表記を利用する
  https://onlinedemo2.cybozu.info/scripts/garoon/grn.exe
  名前：佐藤 昇、松田 環奈、John Doe 等
  組織：情報システム部 等
  会社：BOZU 社 等
  - 名前や組織名・団体名の表現は実名を避ける
  - サイボウズのブランドイメージを毀損する表現、特定の個人や組織・団体を連想させる表現を用いない
- 掲載するスクリーンショットなどに上記以外の表現が含まれる場合は、黒塗りまたはモザイクによる加工を行う

パッケージ版に影響がある脆弱性情報等

パッケージ版に影響がある脆弱性情報については、原則として公開することができません。また、検証を実施した際に知り得た、脆弱性以外の情報を公開する際は、サイボウズの承諾が必要です。

サイボウズ製品の脆弱性の改修時期について

セキュリティ品質の向上には日々努めておりますが、改修による影響範囲や脆弱性の与える深刻度によっては、改修が遅れる場合がございます。

脆弱性を開示するために改修を早めてほしいといったご要望にはお応えすることができません。

その他

このガイドラインは予告なく改定することがあります。あらかじめご了承ください。