脆弱性報奨金制度ルールブック

内容

0. はじめに

サイボウズ株式会社脆弱性報奨金制度（以下、本制度）は、サイボウズが提供するサービスに存在するゼロデイ脆弱性を早期に発見し改修することを目的とする制度です。

本制度に基づき脆弱性を発見し、弊社に報告される方（以下、報告者）には、弊社サービスの品質向上にご協力いただいた謝礼として、報奨金をお支払いいたします。

1. 検証対象サービス

本制度の検証対象となるサービスは、以下の通りです。各サービスの最新バージョンを、本制度の対象といたします。サービスの詳細につきましては、サイボウズのホームページをご覧ください。

1.1 対象サービス一覧（cybozu.com）

cybozu.com 管理と共通設定

サイボウズ Office クラウド版

Garoon on cybozu.com

kintone（サービス本体）

メールワイズ on cybozu.com

セキュアアクセス

cybozu.com Store

サイボウズ Live

cybozu.com 運用基盤

1.2 対象サービス一覧（パッケージ製品）

サイボウズ Office

サイボウズ メールワイズ

サイボウズガルーン

サイボウズ 全文検索サーバー

1.3 対象サービス一覧（モバイルサービス）

サイボウズ KUNAI

サイボウズ リモートサービス

kintone android アプリ

kintone iPhone アプリ

サイボウズ Office 新着通知

サイボウズ Live Timeline

1.4 対象サービス一覧（周辺サービス）

Garoon API

kintone API（REST API / JavaScript API）

User API

kintone アプリストア

サイボウズ Desktop（Win 版 / Mac 版）

1.5 対象サービス一覧（ホームページ）

1.5.1 サービス紹介ホームページ

製品ホームページ（https://www.cybozu.com / https://www.kintone.com ）

kintone（https://kintone.cybozu.com）

Mailwise（https://mailwise.cybozu.com）

1.5.2 関連ホームページ

ヘルプサイト（https://help.cybozu.com / https://help.kintone.com / https://help.cybozu.cn ）

cybozu.com 稼働状況（https://status.cybozu.com / https://status.kintone.com ）

不具合情報公開サイト（https://support.cybozu.com）

Cybozu CDN（https://js.cybozu.com / https://js.kintone.com / https://js.cybozu.cn ）

2. 報告規約

以下の条件を満たした方は、本制度に基づき脆弱性情報を報告し、報奨金を獲得することができます。

- サイボウズ株式会社社員および、関連会社社員ではないこと
- 日本語または、英語で Cy-SIRT とコミュニケーションできること
- 脆弱性報奨金制度規約 に同意いただけること

脆弱性報奨金制度規約については、以下をご覧ください。

http://cybozu.co.jp/company/security/bug-bounty/terms.pdf

3. コミュニケーション

3.1 問い合わせ

本制度は、サイボウズ株式会社 CSIRT（Cy-SIRT）が運営しています。

本制度における全てのお問い合わせは、メールまたは Web フォームにて受け付けます。

それ以外の方法によるお問い合わせは受付けません。

Cy-SIRT の詳細につきましては、以下の Cy-SIRT ホームページをご覧ください。

https://www.cybozu.com/jp/features/management/cysirt.html

3.2 メールアドレス

本制度に関するお問い合わせは、以下のメールアドレスにて受け付けております。

productsecurity@cybozu.co.jp

3.3 Web フォーム

下記 Web フォームをご利用ください。

https://www.cybozu.com/jp/support/security.html

3.4 対応時間

対応時間は 平日 9:00（JST）～ 18:00（JST）です。

3.5 PGP 鍵

報告者が Cy-SIRT に連絡する際には、PGP 鍵を利用できます。

公開鍵の情報は以下をご覧ください。

https://www.cybozu.com/jp/features/management/cy-sirt.asc

4. 本制度開催期間

2017 年 3 月 1 日から 2017 年 12 月 20 日 までを開催期間といたします。

5. サイボウズの脆弱性情報ハンドリングポリシー

報告者が報告した脆弱性情報を、Cy-SIRT は原則としてサイボウズの脆弱性情報ハンドリングポリシーに沿って、受け付けます。脆弱性情報ハンドリングポリシーとは、サイボウズが提供する製品および、サービスで脆弱性が発見された場合に、どのように取り扱い、どのように公開するか定めるもので、「脆弱性対応ポリシー」と「脆弱性情報公開ポリシー」の２つで構成されます。詳細は以下の資料をご覧ください。

https://cybozu.co.jp/company/security-policy/

6. 脆弱性情報の評価プロセス

6.1 評価プロセスにおける用語集

6.1.1 対応番号

報告者が Cy-SIRT に問い合わせた際に、Cy-SIRT は全てのお問い合わせに対して「トラッキング番

号」を割り振ります。この番号を「対応番号」と呼びます。

6.1.2 受付時間

Cy-SIRT は「対応番号」を割り振ると、報告者にメールで連絡します。

このメールの送信時間を、「受付時間」と呼びます。

6.1.3 識別番号

Cy-SIRT が特定の脆弱性情報を脆弱性として認定すると、Cy-SIRT は脆弱性情報に対して「脆弱性情報識別番号」を割り振ります。この番号を「識別番号」と呼びます。

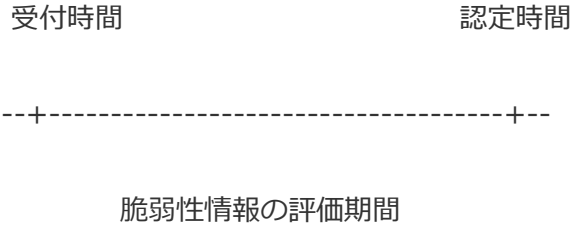
6.1.4 認定時間

Cy-SIRT は「識別番号」を割り振ると、報告者にメールで連絡します。

このメールの送信時間を、「認定時間」と呼びます。

6.1.5 脆弱性情報の評価期間

「受付時間」から、「認定時間」までの期間を「脆弱性情報の評価期間」と呼びます。



6.2 評価プロセス

報告者が脆弱性情報を Cy-SIRT に連絡した場合、以下のプロセスで脆弱性情報を評価します。

1. Cy-SIRT は「対応番号」を割り振り、報告者に連絡します。（受付時間）

2. Cy-SIRT は脆弱性情報を元に、脆弱性を評価します。

3-a. 評価の結果、脆弱性と認定された場合、Cy-SIRT が報告者に脆弱性と認定したことを連絡します。（認定時間）

3-b. 評価の結果、脆弱性として認定されなかった場合、Cy-SIRT が報告者に脆弱性として認定されなかったことを連絡します。

3-c. 追加の情報が必要と判断された場合、Cy-SIRT が報告者に再度連絡します。

4. 報告者が Cy-SIRT に「対応完了」の連絡をし、評価プロセスが完了します。

6.2.1 受付順序について

Cy-SIRT は受信したお問い合わせについて、受信したメールのタイムスタンプ順に受け付けます。

6.2.2 受付時間について

Cy-SIRT は受信したお問い合わせについて、原則として 2 営業日以内に受け付けいたします。

6.2.3 評価順序について

Cy-SIRT は原則として「対応番号」の若い順に評価を行いますが、脆弱性の報告状況などにより評価順序が入れ替わることがあります。

7. 報奨金

7.1 報奨金

報奨金とはサイボウズが提供するサービスおよび、製品の品質向上にご協力いただいた謝礼として、報告者に贈呈される賞金となります。本制度では、報告者が報告した脆弱性情報を Cy-SIRT が脆弱性として認定した時点で、報告者は報奨金を獲得する権利を有するものとします。

7.2 報奨金の金額について

7.2.1 製品・サービスの場合

報奨金は、原則として以下の計算式に基づいて設定されます。

報奨金 = CVSS v3 基本値 × 深刻度による係数（※） × ¥10,000-

※深刻度 緊急（Critical）: 5 / 重要（High）: 3 / 警告（Middle）以下 : 1

X さんが脆弱性情報 A を報告した場合を例に説明します。

Cy-SIRT が脆弱性情報 A を、CVSS 基本値「7.5 重要（High）」と評価した場合

X さんは ¥225,000（7.5 × 3 × ¥10,000）の報奨金を獲得します。

Cy-SIRT が脆弱性情報 A を、CVSS 基本値「4.0 警告（Middle）」と評価した場合

X さんは ¥40,000（4.0 × 1 × ¥10,000）の報奨金を獲得します。

7.2.2 ホームページの問題の場合

報奨金は、以下の計算式に基づいて設定されます。

報奨金 = ¥10,000-

7.2.3 報奨金の上限について

報告者から報告いただいた脆弱性情報を元に、複数の脆弱性情報を Cy-SIRT が認定した場合、

報告者が獲得できる報奨金の上限を ¥1,000,000- とします。

7.2.4 報奨金獲得ルールの詳細

報告者が獲得する報奨金の詳細な獲得ルールについては、以下の URL にある「報奨金獲得に関するガイドライン」の資料をご覧ください。

http://cybozu.co.jp/company/security/bug-bounty/guideline.pdf

7.3 報奨金の受け渡しについて

報告者が報告した脆弱性が下記の条件を満たした場合、翌月末に報奨金を現金でお振込みします。

・サイボウズが脆弱性情報を一般に公開した

・サイボウズが脆弱性情報を脆弱性として認定後、6 か月を経過時点で、脆弱性情報が公開されていない

報告者は Cy-SIRT に、振込先情報を連絡する必要があります。

なお、法人口座への入金には対応しておりません。

7.4 報奨金の寄付について

報告者は報奨金を獲得する代わりに、獲得した報奨金をサイボウズが指定する OSS コミュニティに寄付することが可能です。報告者が報奨金を寄付することを選択した場合、獲得した金額と同額をサイボウズが上乗せし、OSS コミュニティに寄付いたします。寄付に関する詳細なルールは、以下の URL にある「報奨金獲得に関するガイドライン」の資料をご覧ください。

http://cybozu.co.jp/company/security/bug-bounty/guideline.pdf

7.4.1 サイボウズが指定する寄付先について

サイボウズが指定する OSS コミュニティの詳細は、「報奨金獲得に関するガイドライン」に記載するものとします。サイボウズが寄付先を変更する場合には、「報奨金獲得に関するガイドライン」の更新履歴に記載することとします。

8. 税金について

報告者が獲得した報奨金額が 90 万円を超える場合、報告者はご自身で確定申告を行う義務が発生いたします。確定申告に関する詳細につきましては、以下の国税庁のホームページ、「No.1900　給与所得者で確定申告が必要な人」および、「No.1490　一時所得」をご覧ください。

http://www.nta.go.jp/taxanswer/shotoku/1900.htm

http://www.nta.go.jp/taxanswer/shotoku/1490.htm

報告者が獲得した報奨金額が 126 万円を超える場合、報告者は他に収入がなくても、税務上の扶養から外れることがあります。なお、健康保険の扶養に関しては、影響しません。扶養控除に関する詳細につきましては、以下の国税庁のホームページ、「No.1180　扶養控除」をご覧ください。

http://www.nta.go.jp/taxanswer/shotoku/1180.htm

9. 報告者による情報の公開について

9.1 発見した脆弱性情報について

報告者は、発見した脆弱性情報を秘密情報として取扱ってください。

サイボウズが当該脆弱性について公開するまでの期間、 第三者に対して開示、漏洩、公表等できないものとします。サイボウズが当該脆弱性について公開後は、公開情報として取り扱うことができます。

9.2 SNS などへの情報公開について

報告者は、本制度の感想等について、SNS への投稿等を含む第三者への公開を行うことができます。

ただし、前項に定める秘密情報については第三者へ公開することを禁止いたします。

9.3 賞金の授与資格のはく奪

報告者が 9.1 の規程に違反した場合および、報告規約にある条件を満たしていないことがサイボウズにて確認できた場合、報奨金の受領資格を喪失するものとします。また、報告者が報奨金を受領済みの場合は、返還に応じるものとします。

10. 検証環境について

10.1 検証環境提供プログラムについて

1.1 項にある cybozu.com 上で提供されるサービスの脆弱性を検証する環境は、サイボウズより無償で提供いたしております。詳細は以下の弊社ホームページをご覧ください。

脆弱性検証環境提供プログラムについて

https://cybozu.co.jp/products/bug-bounty/#TestingEnvironmentProgram

10.2 検証環境提供プログラムにて提供されない cybozu.com 上のサービスの検証について

cybozu.com Store および、弊社が提供する Web サイトについて脆弱性を検証することは可能です。

詳細は以下の FAQ をご覧ください。

cybozu.com サービスに対して、脆弱性検証を実施することは可能でしょうか。

http://faq.cybozu.info/alphascope/cybozu/web/cybozu.com/Detail.aspx?id=1045

10.3 パッケージ製品・モバイルサービス・周辺サービスの検証について

パッケージ製品、モバイルサービスおよび、周辺サービスつきましては、サイボウズより検証環境を提供いたしておりません。報告者がご自身で検証環境を構築いただく必要がございます。詳細な構築手順につきましては、各製品および、サービスのマニュアルをご覧ください。

11. 更新履歴

2014-06-19	初版公開。
2014-06-25	サイボウズ Live を報奨金制度の対象から削除。
2014-07-17	誤字を修正。報奨金の計算式の乗算記号を変更。ホームページの対象を詳細に記載。
2015-02-02	開催期間を修正しました。検証対象のホームページを変更。PGP 公開鍵の詳細情報を削除。誤字を修正しました。ガルーンのバージョンを変更。謝辞に関して追加。
2015-06-16	寄付に関するルールを追加。対象サービスにサイボウズ Live と cybozu.com 運用基盤を追加。
2016-02-01	報奨金の支払いルールを更新。対象サービスに サイボウズ Office 新着通知、 サイボウズ Live Timeline、Cybozu CDN、サイボウズ Desktop を追加。資料内の重複部分を削除。
2017-01-15	年度を削除。対象製品から「ネット連携サービス」を削除。開催期間を 2017 年度に変更。脆弱性情報ハンドリングポリシーの URL 変更を反映。