脆弱性報奨金制度ルールブック

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、サイボウズ脆弱性報奨金制度（https://cybozu.co.jp/products/bug-bounty/）のページをご覧ください。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、製品ホームページをご覧ください。

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。

- サイボウズおよび、サイボウズの子会社の従業員ではないこと
- 日本語または、英語で Cy-PSIRT 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。
https://cybozu.co.jp/products/bug-bounty/pdf/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 Cy-PSIRT 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。

Web フォーム：
https://www.cybozu.com/jp/support/security.html?

メール：
productsecurity@cybozu.co.jp

3.2 対応時間

対応時間は 平日 9:00（JST）～ 17:30（JST）です。

3.3 PGP 鍵

報告者が Cy-PSIRT 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-PSIRT.asc

4. サイボウズの脆弱性情報ハンドリングポリシー

報告された脆弱性情報は、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、公開するかを定めたものです。詳細は以下の資料をご覧ください。https://cybozu.co.jp/company/security-policy/

5. 脆弱性情報の評価プロセス

5.1 評価プロセス

報告者が脆弱性情報を Cy-PSIRT 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. 「対応番号」を割り振り、報告者に連絡します。
2. 脆弱性情報を元に、脆弱性を評価します。
3. 評価結果を連絡します。

    - 評価の結果、脆弱性と認定された場合、報告者に脆弱性と認定したことを連絡します。
    - 評価の結果、脆弱性として認定されなかった場合、報告者にその旨ご連絡します。
    - 追加の情報が必要と判断された場合、報告者に再度連絡します。

4. 報告者が Cy-PSIRT に「対応完了」の連絡をし、評価プロセスが完了します。
    ※ この時点では、評価及びお支払する金額が変動する可能性がございます。
5. お支払いのご連絡時に評価およびお支払する金額を改めてご連絡します。
    ※ この時点で、お支払する金額を本確定とし、これ以降お支払い金額は変更されません。

5.2 受付順序について

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。

5.3 受付時間について

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。

5.4 評価順序について

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。

6. 報奨金

6.1 お支払金額の計算式

報奨金は、以下のルールに基づいて確定します。

No	概要	ケース	計算方法
1	最終的に認定された脆弱性か	認定された	計算式 2～8 が適用されます。
		認定された(RCE)	100 万円(固定)、6 以降が適用されます。
		対応完了後の認定取り消し	2 万円(固定)、6 以降が適用されます。 ※ 2 万円未満の報告についてはそちらの金額となります。
		認定しない	お支払いはありません。
2	基本金額	製品	CVSSv3 の基本値
		ホームページ	2 万円(固定)、6 以降が適用されます。
3	CVSSv3 基本値による係数	0.0~6.9	× 1 万円
		7.0～8.9	× 3 万円
		9.0～10.0	× 5 万円
4	脆弱性種別による係数	CVSS v3 基本値が 6.9 以下の SQL インジェクション	× 3
		それ以外	× 1
5	製品による係数	kintone cybozu.com 共通管理	× 5
		Garoon Office メールワイズ	× 2 ※ オプション製品は含まれません。
		上記以外	× 1
6	認定前の報告	1 人目	× 1
		それ以外	× 0.2
7	上限の計算	-	200 万円 ※ 製品違いで同種の脆弱性を報告いただいた場合なども含まれます。
8	支払い先による上乗せ	報告者	× 1
		寄付	× 2

6.2 報奨金獲得ルールの詳細

No	概要	報奨金	ルール
1	調査結果により複数の脆弱性が認定された	有り	報告いただいた脆弱性情報を元に複数の脆弱性をサイボウズが認定した場合、各脆弱性で報奨金を獲得できます。 この場合、報奨金の上限は 200 万円とします。
2	同一・類似の脆弱性が報告された	無し	同一製品で同一、または、類似の脆弱性情報を報告いただいた場合、 1 件の脆弱性として取り扱います。 脆弱性の評価に応じた報奨金を獲得できます。

6.2.1 同一要因とする脆弱性の例

- パラメータから入力した場合と、ハッシュから入力した場合の双方で脆弱性が顕在化する
- １つのメソッド内の別のパラメータがエスケープされておらず、脆弱性が顕在化する
- 同一のサーバーで稼働しているホームページで、環境設定に起因する脆弱性が顕在化した場合

なお、同一要因の脆弱性でも、製品が異なる場合にはこの規則を適用しないこととします。

6.2.2 類似した脆弱性の例

- 同一のロジックが別の処理で利用され、複数の箇所で脆弱性が顕在化する
- 同種のパラメータや DOM 属性などを用いる別のロジックで、脆弱性が顕在化する

なお、類似した脆弱性でも、製品が異なる場合にはこの規則を適用しないこととします。

	概要	報奨金	ルール
3	脆弱性情報が同時に報告された	有り	評価をする間に別の方から類似または、同一要因の脆弱性情報を報告いただいた場合、いずれかの脆弱性情報を脆弱性として認定します。認定された報告者は報奨金を満額で獲得でき、残りの報告者は報奨金の 20%を獲得できます。 これまでにご報告いただいた脆弱性情報について、別の方から既知の脆弱性情報をご報告いただいた場合、報奨金を獲得できません。
4	既知の脆弱性が報告された	無し	※既知の脆弱性の定義 サイボウズが脆弱性として認定してから、未公開の状態にある脆弱性情報を指します。報奨金をお支払しませんが、以下のページで謝辞を掲載します。 https://cybozu.co.jp/products/bug-bounty/specialthanks/
5	類似した脆弱性を別の方から追加で報告いただいた	有り	類似した脆弱性情報を別の方からご報告いただいた場合、既知の脆弱性情報でなければ報奨金を獲得できます。
6	公開済みの脆弱性情報を報告いただいた	無し	すでに公開されている脆弱性情報を報告いただいた場合、報奨金を獲得することが出来ません。

7	動作環境外の脆弱性が報告された	無し	動作環境ではないブラウザで再現する脆弱性を報告いただいた場合、報奨金を獲得することはできません。動作環境のブラウザについては各製品のホームページを確認してください。
8	報告された脆弱性がサイボウズ製品で改修しないと判断された	有り	一度認定された脆弱性情報が改修しないと判断された場合、改修しないと決定した時点で、認定時の評価内容に応じて報奨金を獲得できます。
9	WordPress の脆弱性が報告された	有り	サイボウズでの影響確認と改修の期間を 2 週間と定めます。以降に影響がある未知の脆弱性のみを認定し、認定時の評価内容に応じて報奨金を獲得できます。
10	製品内で利用しているサードパーティ製品の脆弱性が報告された	有り	緊急度に応じて都度システムを更新しています。更新以降に影響がある未知の脆弱性のみを認定し、 認定時の評価内容に応じて報奨金を獲得できます。

6.3 認定後の評価変更について

	概要	報奨金	ルール
11	認定した脆弱性の点数が変更になった	有り	一度認定された脆弱性情報が、調査の結果評価結果が変更された場合、変更後の評価内容に応じて報奨金を獲得できます。
12	認定した脆弱性情報が調査の結果、脆弱性ではないと判断された	有り	一度認定された脆弱性情報が、調査の結果、脆弱性ではないと判断された場合、一律 2 万円をお支払します。 なお、2 万円以下の報告についてはそちらの金額となります。
13	報告された脆弱性がサイボウズ製品で改修しないと判断された	有り	一度認定された脆弱性情報が改修しないと判断された場合、改修しないと決定した時点で、認定時の 評価内容に応じて報奨金を獲得できます。

6.4 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-PSIRT 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。

6.5 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。なお、「報奨金の獲得」と「寄付」を組み合わせることはできません。

6.5.1 サイボウズが指定する寄付先について

- Apache Software Foundation
- Linux Foundation
- 日本にある OWASP Local Chapter

寄付先のご指定が無い場合、Apache Software Foundation に寄付いたします。

6.5.2 寄付の詳細について

報告者の方から寄付する旨ご連絡を受けたのち、2 ヶ月以内に報告者の方が指定した団体にサイボウズが寄付いたします。寄付者の名義は「サイボウズ株式会社」となります。寄付が完了した時点で、報告者の方にサイボウズからご連絡いたします。税制上の優遇処置などのために、書面を発行するなどの業務はお受けできません。日本国内の方の場合、今回の寄付先は税制優遇処置をけることが出来ない団体であることを確認しております。

6.6 税金について

報告者が獲得した報奨金額が特定の金額を超える場合、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/taxes/shiraberu/taxanswer/shotoku/1900.htm
http://www.nta.go.jp/taxes/shiraberu/taxanswer/shotoku/1490.htm
また、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。
https://www.nta.go.jp/taxes/shiraberu/taxanswer/shotoku/1180.htm

7. 検証環境について

検証環境提供プログラムページをご覧ください。

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

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。
2017-07-07	ガイドラインと一本化に際し、不足情報を追記。
2018-04-09	報告規約を変更。対応時間を変更。報奨金の上限額を引き上げ。税金の詳細を簡略化。
2018-06-29	評価プロセスの追記とお支払金額の計算式を追記。