Ｓｋｙ脆弱性報奨金制度ルールブック

はじめに

Ｓｋｙ脆弱性報奨金制度（以下、「本制度」）は、Ｓｋｙ株式会社（以下、「Ｓｋｙ」または「弊社」）が提供する製品・サービス・Web サイトに存在するプログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥（以下、「脆弱性」）の早期発見と改修を目的とした制度です。発見または特定した本制度の対象となる製品・サービス・Web サイトの脆弱性に関する情報（以下、「脆弱性報告情報」）を本制度に沿って弊社に報告いただける方（以下、「報告者」）には、品質向上へのご協力の謝礼として報奨金をお支払いします。本制度は、弊社 Sky-SIRT（Ｓｋｙにおいて本制度を所管する Security Incident Response Team をいいます。以下同じです）が複数部門と連携して対応します。本ルールブックとＳｋｙ脆弱性報奨金制度規約（以下、「本規約」。本ルールブックと併せて「本規約等」）の内容が異なる場合には本規約が優先されます。

１．検証対象製品・サービス・Web サイト

本制度の検証対象となる製品・サービス・Web サイト（以下、「対象製品等」）は、本制度の Web サイト（https://www.skygroup.jp/security-info/bugbounty/）をご確認ください。また、製品・サービス・Web サイトの詳細は、各 Web サイトをご覧ください。

２．報告規約

報奨金を獲得できるのは本制度に沿って脆弱性を報告いただいた方であり、かつ、以下の条件を満たした方です。

- 報告時および本制度に沿って報告を行った日以前 6 か月以内（ただし、同一または類似の脆弱性についての報告を複数回行った場合には、最初に報告を行った日以前 6 か月以内）において、報告者、報告者の近親者（配偶者、子、父母、兄弟姉妹）、または世帯員がＳｋｙまたはＳｋｙのグループ会社（株式会社エッグを含む、Ｓｋｙの子会社または関連会社をいいます。以下同じです）の従業員ではないこと
- 報告時および本制度に沿って報告を行った日以前 6 か月以内（ただし、同一または類似の脆弱性についての報告を複数回行った場合には、最初に報告を行った日以前 6 か月以内）において、業務委託契約、出向契約、派遣契約等の契約形態により、Ｓｋｙまたはｓｋｙのグループ会社の業務に従事していないこと
- 過去にＳｋｙまたはＳｋｙのグループ会社で製品開発およびクラウドサービス運用関連の業務に従事していないこと
- 日本語または英語で、Sky-SIRT とコミュニケーションができること
- その他、本規約に定める参加資格を満たし、本規約に同意いただけること

本規約については、以下の Web サイトをご確認ください。
https://www.skygroup.jp/security-info/bugbounty/

３．脆弱性に関するＳｋｙへの連絡

３．１　連絡方法

本制度を利用した脆弱性に関する報告は、本制度の Web サイト内の「脆弱性連絡フォーム」で受けつけます。お問い合わせ等のご連絡は、本制度の Web サイト内の「お問い合わせフォーム」からお願いします。

脆弱性連絡フォーム：https://www.skygroup.jp/security-info/bugbounty/entry.html
お問い合わせフォーム：https://www.skygroup.jp/security-info/inquiry/

３．２　対応時間

「脆弱性連絡フォーム」および「お問い合わせフォーム」からのご連絡は、365 日 24 時間受けつけています。
原則として、「脆弱性連絡フォーム」および「お問い合わせフォーム」からのご連絡後、3 営業日以内に受領確認のご連絡をします。
ただし、年末年始等の長期休暇を挟む場合は、通常よりもお時間をいただきます。

４．脆弱性届出先の選定について

日本では 2004 年に、ソフトウェア製品および Web アプリケーションの脆弱性に関連する情報の円滑な流通と対策を図るため、官民の連携体制を目的とした「情報セキュリティ早期警戒パートナーシップ」が整備されました。それと同時に経済産業省の告示に基づき策定された「情報セキュリティ早期警戒パートナーシップガイドライン」（最新版：2019 年 5 月）が公開され、ソフトウェア製品および Web アプリケーションの脆弱性を発見した場合には、同ガイドラインに沿って、IPA（独立行政法人情報処理推進機構）に対して脆弱性関連情報を届け出ることが推奨されています。

対象製品等に存在する脆弱性を見つけられた際、IPA とＳｋｙ、どちらに届け出るかの最終的なご判断は、報告者ご自身にお任せしますが、弊社では、脆弱性への対応を速やかに開始するために本制度の「脆弱性連絡フォーム」を通して、直接Ｓｋｙへ報告いただくようお願いしています。弊社へ直接報告いただいた場合も、IPA への報告等はＳｋｙが責任を持って対応します。

５．対象製品等における脆弱性報告情報の扱いと公開について

報告された脆弱性報告情報は、Ｓｋｙの「製品・サービスの脆弱性報告情報の公開過程」に沿って取扱います。「製品・サービスの脆弱性報告情報の公開過程」は、対象製品等に脆弱性が発見された場合、どのように取扱い、公開するかを定めたものです。詳細は、以下の Web サイトをご確認ください。
https://www.skygroup.jp/security-info/notice/170404.html

６．脆弱性報告情報の対応プロセス

６．１　対応プロセス

Sky-SIRT は、報告者から報告を受けた脆弱性報告情報について、以下のプロセスで評価・対応します。

1. 「脆弱性連絡フォーム」から報告された順に受付を行い、「対応番号」を割り振り、報告者へ連絡
2. 脆弱性報告情報が対象製品等の脆弱性に該当するかを検討し、脆弱性と認定された場合は報奨金額を算出
3. 報告者へ評価結果および報奨金額を連絡
   - 脆弱性と認定されるのは、対象製品等の挙動から、弊社が脆弱性に該当すると判断した場合のみです
   - 脆弱性と認定された場合、報告者にその旨および報奨金額を連絡します
   - 脆弱性と認定されなかった場合、報告者にその旨を連絡します
   - 追加の情報が必要と判断した場合、報告者にその旨を連絡します
   - 評価および報奨金額は、対応プロセス完了までに変動する可能性があります
4. 報告者から、同一の脆弱性に関して当該報告者が調査した結果のすべてを脆弱性報告情報として受け取り、Ｓｋｙが受領の連絡を行った時点で対応プロセスが完了
   - 報奨金額は対応プロセスが完了時点で確定し、以降変更はされません。ただし、報告者が本規約等に違反した場合は報奨金の支払い決定を撤回し、または支払済みの報奨金の返還を求める等の措置を講じることがあります
   - Sky-SIRT が報奨金額とともに支払手続に関する連絡を行う際に記載する返信期日までに報告者が必要事項を返信しない場合には、当該期日を経過した時点で対応プロセスは完了したものとみなし、報奨金をお支払いすることができなくなります

６．２　受付順序

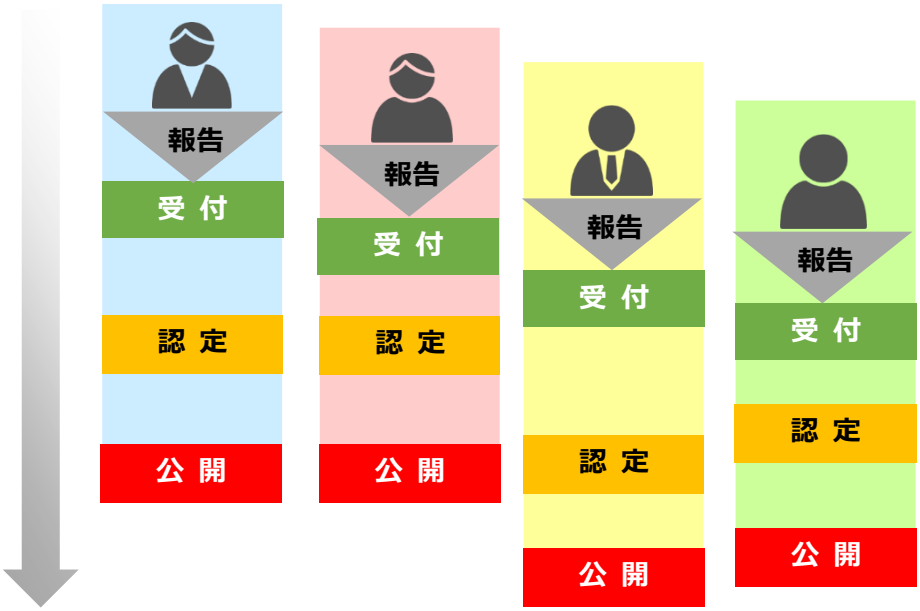
受付は、「脆弱性連絡フォーム」に登録された順に行い、対応番号が付与されます。

6．3　受領確認の連絡

原則として、「脆弱性連絡フォーム」に登録後 3 営業日以内に受領確認のご連絡をします。
「脆弱性連絡フォーム」への登録後、7 営業日を過ぎてもＳｋｙから連絡がない場合、再度「脆弱性連絡フォーム」へその旨を記載してご連絡いただきますようお願いします。

6．4　評価順序

評価は、原則として「対応番号」の早い順に行いますが、報告内容等により順番が入れ替わることがあります。また、評価および報奨金額は、対応プロセス完了まで変動する可能性があります。



7．　報告者による脆弱性報告情報の公表等について

報告者が対象製品等に関する脆弱性報告情報および検証調査を実施した際に知り得た挙動に関する一切の情報（脆弱性を発見した対象製品等の名称を含む。以下、「脆弱性報告情報等」）を公表、開示、または提供（以下「公表等」）する場合には、以下の内容に沿って対応してください。

7．1　脆弱性報告情報等の公表等に関するルール

脆弱性報告情報等の公表等については、以下の規約の記載も併せてご確認ください。

本規約第 6 条　報告者による脆弱性報告情報の公表等
https://www.skygroup.jp/security-info/assets/docs/Ｓｋｙ脆弱性報奨金制度規約.pdf

７．２　脆弱性報告情報等の公表等の内容と方法

報告者は、Ｓｋｙが事前に承諾した場合に限り、脆弱性報告情報等を公表等できます。公表等を希望する場合は、受付後のやり取りで使用するメールアドレス宛てにご連絡ください。
なお、公表等を承諾する場合にも以下のルールに従っていただきます。

- 報告者が希望する公表等の内容をＳｋｙが調整することがあります。Ｓｋｙが調整後の内容を承諾した場合は、調整後の内容に限定して公表等が認められます
- Ｓｋｙが修正プログラムを公開するまでの間は、公表等できません
- 修正プログラム公開後も、お客様による修正プログラムの適用が十分に完了されたとＳｋｙが判断するまでの間は、公表等できる内容は脆弱性を発見したことのみに限られます（脆弱性報告情報等の内容を公表等することは認められません）
  （例）私は、20××年○月△日、Ｓｋｙ製品に脆弱性があることを発見した。
- Ｓｋｙは、お客様による修正プログラムの適用が十分に完了されたと判断した場合、その旨を報告者へ連絡します。報告者は、当該連絡を受ける前までに公表等したい場合、Ｓｋｙに対しその旨とその理由を連絡し、Ｓｋｙはその裁量により当該連絡前に公表等することを特別に許可することができます
- お客様による修正プログラムの適用が十分に完了されたとＳｋｙが判断した後の公表等については、Ｓｋｙによる承諾は必要になるものの、原則として公表等の内容には特に制約を設けません

７．３　対象製品等の改修時期について

製品・サービスのセキュリティ品質向上に最善を尽くしておりますが、改修による影響範囲や脆弱性が与える深刻度によっては改修が遅れる場合があります。
脆弱性報告情報等の開示を目的として改修を早めるようご要望いただいても、お応えできません。

８．報奨金

本制度では、CVSS 値を基本的な基準として報奨金を算出します。さらに、脆弱性報告情報の重要性を考慮して加算額を算出し、それらの合計額を報奨金とします。
CVSS 値は、共通脆弱性評価システム CVSS（Common Vulnerability Scoring System)を基に、IPA が評価した値を使用しますが、CVSS 値が確定し JVN（Japan Vulnerability Notes）から公表されるまでには一定の時間がかかります。
なお、報告者から要望があった場合、Ｓｋｙが共通脆弱性評価システム CVSS を使用して独自に CVSS 値を算出し、報奨金をお支払いすることがあります。ただし、当該支払い後 JVN から公表された値との差異が発生しても、Ｓｋｙから報奨金額の補填や返還要求はしません。対応プロセスの進行中に JVN が CVSS 値を公表した場合には、JVN が公表した値を使用して計算します。

8．1　基本ルール

報奨金は、原則として以下の計算式に基づいて、CVSS v3 基本値を基本的な基準として算出します。

報奨金額　＝　（ [8.2.1 に定めるベース金額] ＋ [8.2.2 に定める加算金額] ）　× [8.2.3 に定める割合]

ただし、8.2.1、8.2.2、および 8.2.3 に定めるほかに考慮すべき事由が存在する場合、Ｓｋｙは、その裁量によって報奨金額を調整することができます。

8．2．1　ベース金額

報奨金額の算出にあたっては、以下の表に従い、CVSS v3 基本値に基づくベース金額を確定します。

CVSS v3 基本値については、IPA が公開している「共通脆弱性評価システム CVSS v3 概説」をご確認ください。
https://www.ipa.go.jp/security/vuln/CVSSv3.html

深刻度	CVSS v3 基本値	ベース金額
緊急（Critical）	9.0 ～ 10.0	CVSS v3 基本値 × 50,000 円
重要（High）	7.0 ～ 8.9	CVSS v3 基本値 × 30,000 円
警告（Medium）	4.0 ～ 6.9	CVSS v3 基本値 × 10,000 円
注意（Low）	0.1 ～ 3.9	
なし	0	報奨金なし

8．2．2 重要性による加算金額

次に、以下の分類に従って脆弱性報告情報の重要性を考慮した加算金額を確定します。
弊社は報奨金額を CVSS 値だけで判断した場合、必ずしも弊社製品・サービスをお使いのお客様への影響度合いと報奨金額の多寡が一致するわけではないものと認識しています。そこで、本制度の報奨金額の算出にあたっては、弊社のお客様への影響度合いと報奨金額を連動させ、以下の区分に該当する脆弱性に対しては、区分ごとに定めた金額を加算することとしています。ただし、ベース金額と加算金額の合計は、脆弱性 1 件につき 200 万円を上限とします。

区分	種別	加算金額（最大値）
RCE※の判定	RCE	150 万円
	RCE 以外	50 万円
脆弱性種別	SQLインジェクション	25万円
	インジェクション（SQL インジェクション以外）	10万円
	アクセス制御の不備	30万円

	入力確認の不備	25万円
	XSS	7万円
	上記以外 （報告内容によっては、Ｓｋｙが新たな種別を作成します。右記の金額は、上記以外の種別の脆弱性が報告された場合の最大値で、加算金額は作成した種別に沿って評価を行い決定します。）	30万円

※リモートからの任意のコマンドやコードの実行が可能

８．２．３ 報告された脆弱性に関するお客様への影響度と、当該区分の最大値に対する割合

さらに、報告された脆弱性に関するお客様への影響度を踏まえ、以下の区分に従い、上記 8.2.1 および 8.2.2 の合計金額（最大値）に乗じる割合を算定します。

１．製品・クラウドサービス

報告された脆弱性に関するお客様への影響度	最大値に対する割合
当該脆弱性によるお客様への被害がすでに確認され、弊社が緊急に修正プログラムを作成し公開する場合	100%
当該脆弱性によるお客様への攻撃はすでに確認されているが、お客様に被害は発生しておらず、弊社が修正プログラムを作成し、公開する場合	75%
当該脆弱性によるお客様への攻撃は確認されていないが、弊社が修正プログラムを作成し、公開する場合	50%
当該脆弱性によるお客様への攻撃は確認されず、弊社からの修正プログラムの提供を伴わない回避策の案内により当面の対処が可能な場合	25%
当該脆弱性によるお客様への攻撃は確認されず、通常のバージョンアップ時の修正で対応が可能な場合	25%
調査により、弊社が利用している他社のモジュール等に起因していると判明した、弊社が開発した部分以外の脆弱性の場合	0%

２．Ｓｋｙが公開する Web サイト

報告された脆弱性に関するお客様への影響度	最大値に対する割合
すでに Web サイト利用者の個人情報漏洩等の被害が発生し、弊社が緊急に Web サイトの停止もしくは改修、または利用者への案内の掲示等の対応を行う場合	100%
すでに Web サイト利用者の個人情報以外の漏洩等の被害が発生し、弊社が緊急に Web サイトの停止もしくは改修、または利用者への案内の掲示等の対応を行う場合	50%
Web サイトの改ざんが確認されたが、Web サイトの復旧により正常化できた場合	20%
Web サイトへの被害は確認されず、Web サイトの改修により正常化できた場合	15%

Web サイトについては CVSS 値により算出される報奨金獲得額がないため、重要性に対する加算金額に上記の割合

を乗じた金額が、原則的な報奨金額となります。

８．３．１　報奨金獲得に関する補足情報

脆弱性報告情報に関する補足情報は、以下のとおりです。

1. Ｓｋｙの調査により複数の脆弱性が認定された場合
   報告内容を基にＳｋｙが調査した結果、報告された脆弱性とは異なる脆弱性が検出された場合、報告された脆弱性に応じた報奨金は獲得できますが、その後の調査による検出分に対する報奨金は獲得できません。
2. 同一要因・類似の脆弱性が認定された場合
   同一製品・サービス・Web サイトに対して、同一要因または類似の脆弱性報告情報を報告された場合、先に報告された（対応番号の早い）脆弱性報告情報について認定を行います。報奨金は認定された報告者のみ獲得できます。
3. 既知の脆弱性が報告された場合
   すでにＳｋｙが認識している脆弱性を報告された場合、報奨金は獲得できません。
4. 動作保証外の環境での脆弱性報告情報が報告された場合
   Ｓｋｙが動作保証している環境外で発現する脆弱性報告情報を報告された場合、報奨金は獲得できません。動作環境については、各製品・サービスの Web サイトをご確認ください。
5. 製品・サービス・Web サイト内で使用しているサードパーティー製品の脆弱性報告情報が報告された場合
   Ｓｋｙが開発した部分以外の脆弱性は、Ｓｋｙが認識していない脆弱性のみについて認定し、8.2.1 に定める CVSS 値で算出される報奨金額（ベース金額）に 8.2.3 に定める割合（製品・クラウドサービスとＳｋｙが公開する Web サイトで異なります）を乗じた金額のみ獲得できます。
6. 弊社が利用する第三者が作成したモジュール等の脆弱性を報告いただいた場合、当該モジュール等に起因していると判明した、弊社が開発した部分以外の脆弱性の場合を除き、弊社製品・サービス・Web サイトの脆弱性として弊社側での対応が発生すれば、本制度の対象となります。
   ただし、以下の脆弱性は、本制度の対象には含めません。
   - Web ブラウザのリソースに起因する問題
   - 大量のデータやリクエストを必要とする Denial of Service（DoS）
   - 中間者攻撃が前提となる脆弱性

８．３．２　同一要因の脆弱性とみなす判断基準

同一要因の脆弱性と判断される例は以下のとおりですが、以下に限られません。同一要因の脆弱性と判断される場合、上記 8.3.1 の 2.を適用します。

- パラメーターとハッシュ、どちらに入力した場合も脆弱性が顕在化する場合
- 同一のサーバーで稼働している Web サイトで、環境設定に起因する脆弱性が顕在化する場合
- 同一のロジックまたは関数を利用しているなどに起因して、同一製品・サービス・Web サイト内の別の場所で脆弱性が顕在化する場合

なお、同一要因の脆弱性でも、製品・サービス・Web サイトが異なる場合には異なる脆弱性と判断されます。
ただし、脆弱性が発見されたクラウド版の機能がパッケージ版でも実装されたときに同一要因の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報告情報等には該当しません。

８．３．３　類似の脆弱性とみなす判断基準

類似の脆弱性と判断される例は以下のとおりですが、以下に限られません。類似の脆弱性と判断される場合、上記 8.3.1 の 2.を適用します。

- 同一製品等内に類似のロジックが分散していることが原因で、複数の異なる脆弱性が顕在化する場合

なお、類似の脆弱性でも、製品・サービス・Web サイトが異なる場合には異なる脆弱性と判断されます。
ただし、脆弱性が発見されたクラウド版の機能がパッケージ版でも実装されたときに同一要因の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報告情報等には該当しません。

８．４　報奨金の受け渡しについて

報奨金は、原則として、報告者が報告した脆弱性報告情報の対応プロセス完了日の翌々月末までに現金で振り込みます。

報告者は、振込先情報をＳｋｙに連絡する必要があります。振込先情報をご連絡いただけない場合、お支払いができない場合があります。また、ご連絡いただいた送金先情報に従って送金手続を行ったにもかかわらず、報告者が報奨金を受領できなかった場合も同様です。

８．５　税金について

報奨金に関する納税義務については、以下の点にご留意ください。

- 報告者が獲得した報奨金額が一定の金額を超える場合、報告者自身で確定申告を行う義務が発生する場合があります。報奨金に関する納税義務等については、報告者ご自身でご確認ください
- 報告者の所在地等によって、日本国外での納税義務が発生する場合もあります。報奨金に関する納税義務については、報告者ご自身でご確認ください
- Ｓｋｙは報奨金に関する報告者の納税義務等に関して、一切のサポートを行いません

９．検証用環境の無償貸出について

報告者への検証用環境の無償提供は、発見した脆弱性の追加調査に本番環境を使うことができない報告者が要請し、弊社が承認した場合に、弊社が承認する期間に限り行います。検証用環境の無償貸出をご希望される場合には、「脆弱性連絡フォーム」からご連絡ください。

また、弊社製品・サービスの多くが法人を対象としていることや、Web サイトの本番環境での検証が行えない事情等も考慮し、脆弱性報告情報のご報告をされていない方に対して検証環境の無償貸出を実施する機会を、定期的に設ける予定です。本制度の Web サイトで希望者を募集しますので、対象製品の入手や Web サイトでの検証が困難な方につきましては、そちらを利用ください。なお、応募多数の場合には、Ｓｋｙがその裁量により対象者を選定し、対象者にはＳｋｙからご連絡をいたします。

１０．謝辞

弊社製品・サービス・Web サイトの品質向上にご協力いただいた感謝の気持ちとしまして、本制度に沿って脆弱性を発見・報告された報告者のお名前を以下の Web サイトに掲載します（掲載を希望しない場合は、掲載しません）。「脆弱性連絡フォーム」に、報告者の公表の可否と公表時に使用するためのお名前（公表用の識別名称）を記載してください。

【品質向上にご協力いただいた皆さま】

https://www.skygroup.jp/security-info/thanks/

１１．本規約等の変更

Ｓｋｙは、事前に公表することなく、本規約等の変更を行うことがあります。

本規約等を変更する場合には、当該変更の効力発生日を定め、当該効力発生日より前に当該変更後の本規約等の内容および当該変更の効力発生日を、本制度の Web サイトで周知します。

本規約等が変更された以後に本制度に参加する場合、および、変更以前から本制度に参加していた場合であって変更の効力発生日後も継続して本制度に参加する場合は、変更後の本規約等の内容に同意したものとみなします。

本ルールブックは、日本語版を正文とし、その解釈において日本語版がほかの言語の翻訳に優先します。

更新履歴

2022 年 1 月 26 日：初版

2022 年 1 月 28 日：９項「検証用環境の無償貸出について」の貸出条件の記載に説明を追加

2022 年 2 月 14 日：８項「報奨金」の記載を修正

2022 年 2 月 14 日：９項「検証用環境の無償貸出について」の記載を修正

2022 年 3 月　2 日：本ルールブックは日本語版が正文である旨を追加