脆弱性診断実施契約書

RakuCloud株式会社（以下「甲」という。）と、申し込みフォームの会社名・事業者名欄に記載された事業者（以下「乙」という。）は、乙が事業のために利用する公開Webサイト・APIの無料脆弱性診断について、次のとおり契約する。本契約は法人・事業者による事業目的の利用を対象とする。

第1条 目的と業務

甲は、双方で合意した対象及び条件の下で、脆弱性の有無、再現性及び影響を調査し、診断報告書の提出及び結果の説明を行う（以下「本診断」という。）。甲は善良な管理者の注意をもって本診断を遂行する。

第2条 申し込みと診断条件

1 申し込みフォームに入力した対象URL（最大5件）、実施可能な開始日・終了日及び各日の時間帯（日本時間）、担当者・連絡先、補足事項並びに同意記録を、本契約の個別条件とする。別紙の作成や再署名は通常要しない。

2 乙の契約締結権限を持つ担当者が本契約・秘密保持契約に同意し、対象サイトの診断許諾を明示して申し込み、申込内容が甲の受付システムに記録された時点で、両契約が成立し、本契約の範囲内の診断実施が許諾される。甲は、必要な権限・第三者許可及び安全性に疑義がない場合、入力された期間・時間帯内に診断を実施できる。申し込みと同時に自動診断を開始するものではない。

3 補足事項に条件・除外指定がある場合、権限や安全性に疑義がある場合、その他特別な事情がある場合は、甲は該当範囲の診断を開始せず乙へ確認する。標準範囲を超える行為、期間の延長又は契約条件の変更には、対象と内容が特定できる追加の書面等による合意を要する。

第3条 管理権限と第三者の許可

1 乙の申込担当者は、乙を代表して本契約及びNDAを締結する権限を持ち、かつ対象システムのアクセス管理者として本診断を許諾する権限を有すること、又は当該権限者から有効な委任・承諾を得ていることを確認する。甲から求められた場合はその証拠を提示する。単なるサイトの発注者・利用者であることのみをもって権限があるものとは扱わない。

2 ホスティング、クラウド、SaaS、制作・保守会社、共同利用基盤等の規約及び権利を確認し、必要な通知・許可を得る。甲も対象と権限の対応を合理的に確認し、管理者又は権限が明らかでない範囲は診断せず、乙へ確認する。他のテナント及び第三者が管理する基盤・システム・外部サービスは対象外とする。

第4条 診断及び侵入検証の許諾

1 乙は、入力した公開Web・APIのURLと同一オリジン（スキーム・ホスト・ポート）の該当パス及びその配下について、甲が外部から脆弱性を診断し、侵入可否を必要最小限で確認することを許諾する。診断の過程で、入力したURLと連携して動作する別ホスト・サブドメイン（APIサーバー等）が判明した場合は、乙が管理し、又は診断を許諾する権限を有するものに限り、同じ方法及び限度で対象となる場合がある。通常の利用方法と異なるリクエストや疑似攻撃による認証・認可回避の可否の確認を含むが、実データ・設定の変更や削除、コードの設置・実行、内部への展開は含まない。第三者が管理するリンク先、外部連携先その他のサービスは対象外とする。

2 前項の検証により画面、設定情報又はデータが閲覧可能となる場合がある。甲は可否を示す最小限の応答確認にとどめ、秘密情報・個人情報の探索、大量取得・複製は行わない。予定外の実データが表示された場合は

追加閲覧・取得を停止し、第8条に従う。ログイン情報の受領・使用やログイン後の業務操作は標準診断に含まない。

3 本条は無制限の侵入又は一括取得を認めるものではない。対象、期間・時間帯、深度、データ又は危険性が本契約の範囲を超える場合は一旦停止し、追加承諾を得る。

第5条 禁止行為及び追加承認

1 本契約では、意図的なサービス停止・破壊、DoS・DDoSその他の高負荷試験、実データ・設定の作成・変更・削除、大量抽出、永続的なバックドア設置、対象外システムへの展開、フィッシング及び物理侵入を許諾しない。必要な場合は、本診断とは別に法的権限と危険性を審査し、別途合意する。

2 テスト用ファイル・アカウント・データの作成・変更、コードの実行、権限昇格及び内部到達性の確認は標準診断に含まない。SSRF等を用いて対象外ネットワークやクラウド管理基盤等へアクセスしてはならない。認証情報の総当たりや、メール・SMS送信、決済・発注等の実処理を発生させる操作も行わない。

第6条 稼働への配慮と準備

1 甲は、入力された実施可能期間・各日の時間帯（日本時間）を守り、通常の閲覧と同程度の低頻度・少数同時接続による検証に限定する。応答遅延やエラー増加を認識した場合は中止する。対象URLが本番環境である場合も、本契約の限定された範囲内の診断のみを許諾する。防御機能の無効化・回避を前提とした継続試行は行わない。

2 乙は、必要なバックアップ及び復元可能性を確認し、停止困難な機能、既知の障害、除外URL・実施不可時間等の制約を補足欄に記載する。甲は制約を確認し、不明点や危険性がある場合は診断前に連絡する。復旧準備が不足する場合、危険な試験を実施しない。

3 緊急連絡先は申込担当者のメールアドレス及び入力された電話番号とし、甲への停止・撤回連絡は受付メールへの返信又はsecurity@rakucloud.ai宛てとする。監視・防御機能の変更や復旧操作が必要な場合は、担当と手順を別途確認する。

第7条 中止及び事故対応

1 乙はいつでも診断の停止又は許諾の撤回を求めることができる。甲は通知を受けたとき、又は障害、予期しない情報へのアクセス、対象外への波及、権限の疑義若しくは深刻な影響を認識したときは、該当行為を直ちに停止する。

2 甲は危険な再試行や調査の拡張を行わず、必要な証拠を最小限で保全し、緊急連絡先に遅滞なく連絡する。事故又は漏えい等のおそれの第一報は、判明事項のみでも認識から24時間以内に行う。重大な脆弱性は最終報告を待たず連絡する。

3 双方は被害抑止・復旧・原因調査に協力する。乙の環境の復旧操作は事前に定めた担当者が行い、甲は別途承認のない修復変更を行わない。再開は原因・安全性・対象範囲を確認し、乙が書面等で承認した後とする。

4 行政機関への報告、本人通知その他の法令上の義務は各当事者がその責任において判断・履行する。相手方の承認待ちを理由に法定期限を徒過してはならない。

第8条 データ取扱いと再委託

1 甲は個人情報の取得を極力避け、テストデータ又はマスキング済み証拠を優先する。予定外の実データが表示された場合は追加閲覧・取得を停止し、乙に通知して取扱いを協議する。

2 甲はNDAに従う担当者・端末・保管先のみを使用する。診断の証拠は必要最小限かつマスキング済みの情報を原則とし、報告・確認後、目的上不要となったデータを速やかに返還又は削除する。法令・現実の紛争・事故に必要な証拠保全はNDA第6条に従い別に管理する。乙は合理的な範囲で取扱状況を確認できる。再委託、国外アクセス及び外部サービスの利用はNDAの事前承認条件に従う。

第9条 報告と診断の限界

1 甲は、対象、実施日、方法の概要、発見事項、危険度、影響、必要な再現情報、推奨対策及び未実施・制限事項を記載した報告書を、診断後に申込担当者へ電子メール等で提出する。証拠に含まれる個人情報・認証情報は原則マスキングする。報告方法や日程の調整が必要な場合は連絡する。

2 本診断は合意範囲と実施時点の確認であり、全ての脆弱性の発見、将来の攻撃防止、無事故、完全な安全性又は特定の監査・認証への適合を保証しない。甲は保証しないことを理由に合意した診断や報告を省略してはならない。

第10条 費用と追加業務

1 本診断の無料提供は、同一Webサイトにつき初回1回に限る。初回の標準診断及び所定の報告・説明の対価は0円とし、有料契約の締結義務は生じない。

2 同一Webサイトに対する2回目以降の診断（再診断を含む。）は有料とする。甲は実施前に対象範囲、業務内容及び費用を見積もり、乙の事前の書面等による合意を得た後に実施する。申し込みのみをもって有料診断の発注又は費用への同意とは扱わず、乙の事前の合意なく請求しない。

3 脆弱性修正、監視、緊急対応、ソースコード監査その他本契約に含まれない業務は別途合意とし、乙の事前の書面等による合意なく請求しない。

第11条 事故のリスク確認と免責

1 乙は、甲が稼働への配慮をしても、本診断の性質上、応答遅延、負荷の増加、監視アラート、アカウントロック、サービスの一時停止、データの破損・消失、意図しない処理又は予定外の情報表示等が発生し得ることを理解する。乙は、バックアップ・停止条件等を確認し、合意したリスクの範囲で実施を許諾する。

2 甲が合意した対象・行為・時間・安全措置の範囲内で本診断を実施したことに伴い前項の事故が生じた場合、甲は、通常の過失による場合を含め、乙に生じた損害について、債務不履行、不法行為その他の請求原因を問わず賠償責任を負わない。対象には復旧費用、営業上の損失、逸失利益及び間接損害を含む。

3 前項は、甲又は甲の履行補助者・再委託先の故意若しくは重大な過失、許諾範囲外の行為、合意した安全措置又は停止義務への違反、秘密保持義務若しくは個人情報保護義務への違反により生じた損害には適用しない。また、法令上免責が認められない責任を免除するものではない。

4 本条は、甲の事故通知、被害拡大防止、調査・復旧への合理的な協力、返還・削除又は報告の義務を免除しない。免責の適用要件を満たさない損害の責任は、法令及び本契約の他の定めによる。免責の適用を甲のみの判断で確定しない。

5 本条は甲乙間の責任分担であり、第三者の請求権、刑事責任、行政上の義務又は法令違反を排除しない。第三者から請求を受けた場合、双方は速やかに通知し、事実確認と対応に協力する。

第12条 報告書等の利用と実績の掲載

1 対象データの権利は従前の権利者に留保する。甲の既存のツール、ノウハウ及び報告書の著作権は甲又は従前の権利者に留保し、乙には報告書を自己の安全対策のために利用・複製し、守秘義務を負う関係会社、保守会社、専門家、保険者等へ必要最小限で提供する権利を無償で認める。法令に基づく開示を妨げない。双方による一般公開・営業事例への利用は、次項に定める場合を除き、事前の書面等による承諾を要する。

2 乙は、本診断の完了後、甲が乙の会社名・事業者名及びロゴを、甲が脆弱性診断を提供した実績として、甲のWebサイト及び営業資料に掲載することに同意する。掲載は会社名・事業者名、ロゴ及び本診断を実施した事実に限り、診断結果、脆弱性の有無・内容、対象URLその他乙の安全性を推測させる情報は掲載しない。ロゴは乙の指定する表示方法に従う。乙は書面等による通知により以後の掲載の中止を求めることができ、甲は合理的な期間内に掲載を中止する。ただし、既に配布した資料はこの限りでない。

第13条 期間と終了

1 本契約は受付完了時から、本診断の報告及び必要な返還・削除が完了するまで有効とする。ただし、実際のアクセス許諾は入力された開始日から終了日までの各日の時間帯（日本時間）に限る。期間外、時間帯外又は撤回後のアクセスは認めない。再診断や期間延長は、対象・期間を特定して書面等で改めて合意する。

2 各当事者は相手方への書面等の通知により将来の診断を中止できる。重大な違反、安全上の問題又は必要な許可の欠如がある場合、直ちに停止・解除できる。その他の違反は相当期間を定めた是正要求後に解除できる。無料診断の中止に違約金は課さない。

第14条 終了時の措置

1 甲は、期間満了、停止又は撤回後のアクセスを行わず、承認済み手順に従ってテスト用ファイル等の撤去と変更の復元状況を乙と確認する。乙は診断用認証情報の失効・変更を行う。必要な後片付けにも新たなアクセスが必要な場合は限定的な承認を得る。

2 甲は、実施済み範囲、未実施事項、発見した重大なリスク及び残存するテスト資産を乙へ通知する。契約終了後も、秘密保持、データの返還・削除、事故対応、責任、権利、実績の掲載及び紛争解決の条項は性質上必要な限り存続する。

第15条 反社会的勢力の排除

甲乙は、自己及び役員が反社会的勢力に該当せず、これらを利用し、資金提供等を行い、又は暴力的・不当な要求をしないことを表明し、将来にわたり確約する。違反がある場合、相手方は催告なく解除できる。

第16条 通知と変更

契約及び実施許諾の申込時の承認者はフォームに記載された担当者とする。再委託及び条件変更の承認は、権限ある承認者と対象内容が特定できる電子メール、署名済み書面又は電子署名等による。緊急停止は電話等で通知でき、事後に記録を残す。

第17条 準拠法及び紛争解決

本契約には日本法を適用する。定めのない事項及び疑義は誠実に協議し、紛争について東京地方裁判所又は東京簡易裁判所を第一審の専属的合意管轄裁判所とする。一部条項が無効となっても、他の条項は可能な限り有効に存続する。

本契約は第2条のオンライン申し込みと受付完了により成立する。甲は、同意した本文・版・文書ハッシュ、申込者、受付番号・日時、対象URL、実施可能期間・時間帯及び同意の内容を保存する。乙は本書を保存できる。通常は追加の署名・押印・契約書の取り交わしを要しない。