

## PacketBlackHole Cloud β 版 基本仕様書

本仕様書は「PacketBlackHole Cloud β 版サービス利用規約」に基づきネットエージェント株式会社（以下、サービス提供者）という。）が提供する「PacketBlackHole Cloud β 版」（以下、「本サービス」という。）について、その内容・条件等を定めるものとする。本仕様書において用いる用語の定義は利用規約と同一とする。

### 1. サービス概要

#### (1) 本サービス内容

サービス利用者より「PacketBlackHole Probe」（以下、「PBH Probe」という。）を用いてアップロードされたパケットを解析し、サービス提供期間中、サービス利用者が Web ブラウザを介していつでも解析データを閲覧・検索可能とするサービス。サービス提供期間中、サービス利用者ごとに割り当てられた容量（100GB）分の解析データを保存可能。

#### (2) ライセンス期間

お申し込み完了後、サービス提供者より URL、ID、パスワードが発行された時点より 7 日間をライセンス期間とする。

#### (3) クラウドリソース

お申し込み以前に、本サービス記載ページ上に表示されたクラウドリソースの空き状況により、お申し込み後すぐに利用できない可能性がある。その場合、順番がまわってきたタイミングで利用可能となる。

※リソース空き状況 記載 URL

<http://www.packetblackhole.jp/pbhcloud.html>

### 2. PBH Probe 概要

WindowsOS 上で動作するパケット記録を目的としたソフトウェア。以下の動作要件を満たすクライアント PC 上にインストールすることで、インストールされた PC 上の指定されたネットワークインターフェースカード（以下、「NIC」という。）上を通過したパケットをハードディスク（以下、「HDD」という。）に蓄積することが可能。本サービスに対し、パケットをアップロードする機能を持つ。

#### (1) 動作要件

OS : WindowsXP (SP3 以上)、WindowsVista (SP3 以上)、Windows7

必要メモリ：20MB

必要 HDD 容量：5GB 以上（パケット記録領域含む）

## （2）基本動作

インストールを完了し、各種設定を行った後、パケットの取得を行うことが可能となる。通常、指定した NIC にはインストールを行った PC のパケットのみが流れるため、全社、もしくは一部のネットワークの通信全てを取得したい場合には、指定した NIC に対象となる通信が流れるよう、ミラーポート設定等を行い、その箇所に PC を接続する必要がある。

## （3）各種設定

取得したパケットの保存先の指定、パケットの破棄タイミング（容量指定）を行う。取得したパケットを本サービス上へアップロードする場合、アップロード先の指定および、配布された ID、パスワードの入力が必要となる。

## （4）パケットデータについて

PBH Prove 上のパケットデータは指定した容量まで蓄積されると、以降は古いパケットデータから順に自動的に上書きされて保存される設定か、若しくは本サービスへ向けてパケットデータのアップロードを行ったタイミングでパケットデータを破棄するという設定のどちらかとなる。上書きもしくは破棄されたパケットは完全に消失するものとする。パケットデータの消失を許容しない場合、サービス利用者が PBH Probe を利用して取得したパケットのバックアップをあらかじめとることでパケットデータの消失を防ぐものとする。

## （5）性能

パケットの取得性能については、インストール先の PC スペックおよび、取得対象となる端末あるいはネットワーク通信量により異なる。PBH Probe はパケットの取得性能値 100%を保証するものでない。

### 3. 本サービス利用可能時間帯

提供期間：365日

提供時間：24時間

※ハードウェア・システムの障害発生時、保守復旧作業時およびバージョンアップ等によるサービスの一時停止について

ハードウェア・システムの障害および保守またはシステムバージョンアップのため、サービスを一時停止する場合がある。サービスを停止する場合は、原則

サービス停止予定日の1週間前までに本サービス関連の Web ページ上へその旨を記載する。但し、緊急の停止が不可避な状況となった場合はこの限りではない。

※サービス停止記載 URL

<http://www.packetblackhole.jp/pbhcloud.html>

#### 4. 基本サービス

本サービスにて提供される機能は、以下の通りとする。

##### (1) 解析機能

本サービスにて解析可能な通信種別を記載する。但し、一部解析機能についてはサービス利用者の環境等により、期待する機能を得られない可能性がある。

##### ①メール解析機能

対象となるプロトコルにて送受信されたメールの「発信元、送信先、差出人、受取人、件名、本文、添付ファイル」の再現を行い、一覧表示する機能。日時、メールアドレスによる検索のほか件名、本文、添付ファイルに含まれる文字列による検索機能を実装。

※対象プロトコル

SMTP、POP3、IMAP4

##### ②Web 解析機能

アクセスを行った Web 通信の解析機能。アクセスを行った日時、アクセス先の URL、アクセス元 IP アドレス、アクセス先の Web コンテンツに応じたカテゴリ名などを一覧表示する機能。表示された各情報や POST 文字列を指定することで行える検索機能を実装。

※対象プロトコル

HTTP1.0、HTTP1.1 (HTTPS 暗号化通信は非対応)

##### ③Web イベント機能

解析済みの Web 通信をそのイベント内容ごとにまとめ、各イベントごとの件数を表示。表示されたイベント名をクリックすることで、対象 Web イベントに絞り込んだ Web 通信の一覧表示を行う。

※Web イベント種類

Web 検索、Web メール、ファイルアップロード、掲示板書き込み、動画

##### ④Web 画像解析

Web 通信の際にクライアント上に表示された画像データのみを表示する

機能。

#### ⑤FTP

FTP 通信の表示を行う。送信元の IP アドレスや FTP 転送されたファイルの表示、内容確認が可能。

#### ⑥メッセージ利用解析

メッセージングを利用した通信履歴を一覧表示。各履歴に付随する「msg」タブをクリックするとメッセージ内容を確認することが可能。

※対応メッセージング種類

Yahoo!、MSN、MSN Live

#### ⑦Windows ファイル共有

Windows ファイルサーバ上にあるファイルアクセスに関する通信履歴を閲覧することが可能。クライアントの IP アドレス、ファイル名などでの検索が可能。

※対応プロトコル

SMB、CIFS

#### ⑧SQL Server/Oracle

Microsoft SQL Server に関連する通信履歴を一覧表示。各履歴に付随する「qry」「res」タブをクリックすることで、それぞれクエリ内容、レスポンス内容を閲覧することが可能。

※対応プロトコル

Microsoft SQL Server : TDS7

Oracle : Net8

#### ⑨VoIP

VoIP 通信履歴の一覧表示。発信元、送信先の SIP アドレス、ドメインと通信日時が表示。各履歴に付随する「♪」マークをクリックすることで、音声ファイルの通信内容を聞く事が可能。SIP アドレスによる検索機能実装。

#### ⑩TCP 通信の記録

全 TCP 通信の記録を表示する機能。通信の送信元および宛先の IP アドレス、ポート番号、利用プロトコル、接続日時の表示を行う。ポート番号や

FTP、TELNET などの通信指定を行うことで、絞り込みが可能。パケットのトレースやパケットの情報を確認することも可能。

(2) レポート機能

解析を済みのデータを様々な角度からレポート形式で表示する機能。画面上に表示される複数の条件の中から、レポート化したい項目にチェックを入れることで必要情報のレポートを得ることが可能。

## 5. 本サービス利用時のサービスデータ取り扱いに関する仕様

(1) パケットアップロード時

パケットのアップロード時には PBH Probe を利用することで、SSL 暗号化通信によりセキュアにパケットのアップロードを行うものとする。

その他の手法によりサービス利用者が独自にパケットのアップロードを行う行為は本サービスの仕様外とする。

(2) パケット解析時

パケットの解析後、本サービス上に保存されるデータ容量はアップロードしたパケットファイルに解析データ分を加算した合計値となり、全体でアップロードしたパケットファイルの容量の約 2 倍程度の容量となる。

解析済みのデータは本サービス上でサービス利用者ごとに割り当てられた容量（デフォルト 100GB）までためることが可能。本サービス上にアップロードされたパケットおよび解析データがサービス利用者に割り当てられた HDD 容量を超えた場合、自動的に（ユーザ通知なしに）HDD 内の最も古いデータから順に上書きされる。

(3) 障害発生時

障害発生時および復旧作業時において、サービス提供者は、サービス利用者がアップロードを行ったパケットファイルおよび、障害発生以前に蓄積された解析データを保証するものではない。

(4) サービス解約時

利用規約第 10 条に準拠する。

※本項 (2) に記載される上書きされたデータ、(3) の障害発生時に本サービス上に保存されていたデータ、(4) サービス解約時まで本サービス上にアップロードされたデータは、完全に消失するものとする。パケットデータの消失を許容しない

場合、サービス利用者が **PBH Probe** を利用して取得したパケットのバックアップをあらかじめとることでパケットデータの消失を防ぐものとする。

## 6. オプションサービス

β版にオプションサービスはなし。

## 7. サポート

本サービスに関するサポート内容は以下の通りとする。

### (1) サポート窓口

ネットエージェント株式会社 サポート部

Tel : 03-5625-1244

E-mail : pbh-support@netagent.co.jp

### (2) サポート受付時間

9:00 ~ 12:00 / 13:00 ~ 17:00

※土日、祝祭日および弊社規定の休日を除く。

### (3) サポート内容

仕様通りに動作しない場合、正常な操作を行って起きたシステムの故障等に関する問い合わせを電話・E-mailにて受け付け、対応・回答するものとする。但し、サービス時間外に受け付けたメールでの問い合わせに対しては、翌営業日対応とする。

## 8. 障害時の対応について

### (1) 障害時の通知

サービス提供者が障害を確認した場合、お申し込み時の指定連絡先まで電話またはE-mailで通知する。

### (2) 障害時の復旧

障害による停止が発生した場合、サービス提供者は直ちに再起動や設定変更等で復旧を試みる。万一、サービスが再開不能な状態である場合、初期構築時の状態へ復旧を行い、サービス利用者はユーザ登録を行うこととする。

## 9. 本サービスメニュー

本サービス環境とデータ保存容量（100GB）を提供する。