KATABAMI Q&A

Rev. 1.1　31-May-'23

ID　CAT.　Qst　Ans

#1　tech　KATABAMI で用いる IPv6 address は、global IPv6 address でしょうか？　その場合、取得はどのように行うのでしょうか？

KATABAMI では、global IPv6 address は用いません。
KATABAMI で使用する IPv6 address は下記の2つです。
- fc00::/8
  - unique local address = fc00::/7 の 前半
- 200::/7
  - 使用されない global address（RFC1888 で NSAP に map されたが RFC4048 で非推奨となった。詳細は RFC4548 を参照）

KATABAMI では、これらの address をランダムに生成します
- 実際には、ランダムに生成したペア鍵の内、永久公開鍵からハッシュ関数を用いて生成します。
- 原理的には、重複する可能性が zero ではありませんが、128/129 bits と空間が広いため実用上の問題は無いと想定し、現状は特に管理は行っていません。

#2　tech　global IP を使用しない KATABAMI は、どのような方法で Internet 上の通信を行うのでしょうか？

KATABAMI Bridge という機能があります。
global IPv4 address を持つ node = KATABAMI Bridge を設けます。
- KATABAMI Bridge は（global IPv4 も含め）SYNCHRO が サービスとして提供することが可能です。
- 必要があれば、お客様の環境にオンプレミスで構築することも可能です。

この KATABAMI Bridge に、他の KATABAMI の node が接続する場合は、以下の手順で peer を構成することになります。
- 接続する KATABAMI の node で、
  - KATABAMI Bridfe の IPv4 address / port を指定する
  - （必要があれば）接続のための認証情報を指定する
- KATABAMI Bridge で、
  - 接続する KATABAMI の node の情報を White List に追加する

上記の設定によって、KATABAMI Bridge への接続は、IPv4 TCP or UDP で行われ、この IPv4 の session を tunnel として KATABAMI の IPv6 の通信を行います。
同じ KATABAMI Bridge に接続された KATABAMI の node は、同じネットワークに接続することになります。

#3　tech　KATABAMI を VPN的 に使うことは可能ですか？

KATABAMI には、IPv4（、必要があれば IPv6）をトンネリングする機能があります。
これを利用することで、VPN と等価な接続を行うことが可能です。

IPv4 tunneling の機能を用いた場合、そのトンネルの通信は KATABAMI でセキュアに維持されますが、
IPv4 での通信自体は、通常の IPv4 通信となり、厳密な意味での Zero Trust にはなりません。この点には注意が必要です。

#4　tech　KATABAMI を適用する場合、社内ネットワーク（LAN）を組み替える必要がありますか？

基本的には「いいえ」です。
KATABAMI の IPv6 を用いた通信と、通常の IPv4 の通信は共存可能です。
- KATABAMI を導入しても、通常通り、Web での browsing や、通常の Internet 上 のサービスへのアクセスが可能です。
- これら「通常」の通信は、KATABAMI の保護対象外です。

KATABAMI Bridge を用いて Internet を経由する場合は、KATABAMI も IPv4 を使用しますので、そのための適切な設計＆設定は必要です。
また、KATABAMI を用いて IPv4 tunneling を行う場合は、LAN との通信を行うために、適切な設計＆設定が必要です。

#5　tech　インターネットからの通信は 通信しない／させない で セキュリティを担保しているのでしょうか？

基本的には「いいえ」です。
KATABAMI Bridge を用いて、Internet を経由して KATABAMI の通信を行うことが可能です。
但し、これは、KATABAMI 非対応のサービスなどにも、セキュアな接続できるということではありません。

#21　tech　「永久秘密鍵」の安全性に依存した設計となっているが、永久秘密鍵が絶対に漏洩しないための仕組みはあるのでしょうか？

現状、この部分の対策は「不完全」です。ID、パスワードなどとは異なり、永久秘密鍵をユーザが扱うことはありません。
また、通常の運用ではユーザの目に触れない場所にファイルとして格納していますが、その配置場所を把握できれば取り出すことが可能です。
しかし、その配置場所を把握できれば取り出すことが可能です。

この部分に関しては、2つの方法で対処します（現時点では、開発中です）。
a）KATABAMI Card（指紋認証機能付き FeliCa）で永久秘密鍵を再現する（Card での認証がOKとならなければ通信は正常に行えない）
b）特許化されている大日本印刷株式会社様の暗号化手法を適用し、永久秘密鍵を秘匿する

#22　tech　仮に永久秘密鍵が漏洩してしまった場合に、即座に対象の秘密鍵を無効化する仕組み／運用があるのでしょうか？

現在の運用では、IPv6 address、永久公開鍵 を用いた WhiteList によって通信の制御を行っています（アプリケーションサーバなどのnode毎に WhiteList を設定可能）。
PCやスマホを紛失するなど漏洩リスクがあると判断される場合には、この WhiteList から当該nodeの情報を削除することで無効化可能です。

#25　tech　具体的に通信のどこからどこまでを暗号化する仕組みなのでしょうか？

node上の TUN（仮想ネットワークデバイス）から packet を送り出す時点で encode し、
対向のnode上の TUN で packet を受信した時点で decode し、payload を 対象の process（アプリケーションなど）に渡します。

#26　tech　IPv6アドレスという書き換え可能な要素を認証・承認に用いていることは問題にならないでしょうか？

IPv6 addresss は、永久公開鍵から生成します。永久秘密鍵と数学的な繋がりを持つことになります。
従って、これを改変、偽装した場合、通信は行えなくなります（安全性は担保されます）。

#27　VDP　KATABAMI VDP と UTMとの違いは何でしょう?

UTM は、ネットワークを行き来するデータを監視して、不正なデータを検出して遮断することが役割です。
KATABAMI VDP（以下、K.VDP）は、ネットワークに接続される機器や、ネットワーク自体の弱いところ（脆弱性）を見つけ出すことが役割です。
UTM が建物の人の出入りを監視する守衛さんだとします。
これに対して、K.VDP は、建物の窓が開いていないか、保管庫の鍵が掛かっているかなどをチェックして巡回する警備員さんのようなものです。

#28　VDP　KATABAMI VDP と UTMとの違いは何でしょう?

セキュリティソフト、UTM、K.VDP それぞれ役割が異なります。併用するのが望ましい運用形態です。
前述の例（#27）で説明すると、セキュリティソフトは、見つけた人を人相書きと照合し、似ていれば逮捕するおまわりさん（警官）のようなものです。

#29　VDP　KATABAMI VDP で診断した後はどのように対処になるのでしょうか？

診断結果（検出した脆弱性とその対策）を報告します。通常は月に1回の報告です。重要な脆弱性を検出した場合は速報します。
対策実施は、KATABAMI VDP サービスの対象外です。対策実施をSYNCHROにご用命頂いた場合は、別料金で対策させて頂くことも可能です。

#10　busi　KATABAMI を PC や スマートフォン に インストールする場合にライセンス料が必要でしょうか？

KATABAMI Series の多くは OSS（オープンソースソフトウェア）を利用しています。
PC、スマートフォンへのインストールに関して、ライセンス費は発生しません。

#11　tech　KATABAMI が対応している OS は？

以下の通りです。
- Ubuntu 16.04 LTS, 18.04 LTS, 20.04.x LTS, 22.04.x LTS
- Windows 10, 11、Windows Server 2016, 2019, 2022

MacOS 10.13.x, 10.14.x, 10.15.x, 11.0x, 12.x, 13.x
Android 8.1, 9, 10, 11, 12、iOS、Raspberry Pi OS
RHEL/CentOS 7.x, 8.x、Debian 9.x, 10.x、その他 linux(ex. linux 4.9.x)

#6 tech **各エンドポイントの設定をWEBなどから集約して設定可能なのでしょうか？**

現状は、単独の end point に対する WebUI のみです。
集約型の WebUI は開発中です。
この WebUI のセキュリティも重要で、KATABAMI で HTTP/HTTPS を保護する実装になります。

#7 tech **同一NWアドレスであることは、証明書等をインストールするイメージでしょうか？**

現状は、電子証明書との連携は実装していません。
クラウドサービスなどを目的として、電子証明書を併用とする機能実装を行う予定です。

#8 tech **アプライアンス以外の KATABAMI Series は、どのような提供形態になるのでしょうか？**

KATABAMI Bridge、Chat、RTC、RMS に関しては、サービス提供型 と オンプレミス構築側 の両者に対応しています。

#9 busi **KATABAMI Series の提供方法(直接販売、間接販売など)は、どのような形態になるのでしょうか？**

KATABAMI Series の内、アプライアンス製品(KATABAMI Box、VDP、PBX、AC2)に関しては、販売代理店様経由でのご提供となります。
具体的な販売代理店様に関しては、SYNCHRO まで、お問い合わせ下さい。

KATABAMI Series の内、アプライアンス製品以外に関しては、サービス提供型、オンプレミス構築型 の2種類があります。
サービス提供型 の 場合は、SYNCHRO までお問い合わせ下さい。
オンプレミス構築型に関しては、SYNCHRO または 販売代理店様 にお問い合わせ下さい。
構築形態・方法をご相談させて頂き、作業見積を行います。

#16 Chat **KATABAMI Chat は、Slack からのデータ移行は可能ですか？**

Slack からのデータ移行は(一部制約がありますが) 可能です。
※　ダイレクトメッセージとプライベートチャネルは、Slack側のセキュリティ制限のため export できないため、データ移行できません。

#17 Chat **KATABAMI Chat は、Slack との連携は可能ですか？**

KATABAMI Chat と Slack の動的な連携は難しいと思われます(実績はありません)。
※　双方の Web hook を利用して連携するという解が考えられますが、未確認です。

#19 Box **KATABAMI Box を既存ネットーワークに導入する際の留意点は？**

KATABAMI Box は、LAN に PC などと同様に設置します。
設置する LAN における IPv4 address が必要です。
Internet経由で KATABAMI のネットワークを構成する場合は、Internet に接続する default gateway の設定(IPv4) も必要です。
KATABAMI Bridge (global IPv4)への接続が、ルータ等で阻害されないことが必要です。

KATABAMI Box で IPv4 tunneling を行う場合は、対向の segment への routing を KATABAMI Box に向ける必要があります。

#12 tech **KATABAMI と Wireguard、talescale との違いは何ですか？**

Wireguard (https://www.wireguard.com/)

機能としては、Wireguard は、VPN に置換可能な技術です。
server - client model で、認証はペア鍵で行います。
認証が OK になると server から IP address が client に振り出され client はこの IP で通信します。
通信は、ネットワーク層で暗号化されます。アプリケーションは暗号化には関与する必要はありません(これは、KATABAMI と同じです)。
使用している暗号方式は、KATABAMI と同様です(暗号強度、処理性能、著作権フリー等を考慮して選定すれば、当然同じ解に行き着きます)。
OSS であるという点では、Wireguard は KATABAMI が 利用している Cjdns、Yggdrasil と同じです。

KATABAMI は、server-client modelではなく、P2P の技術です。
ここが、Wireguard や IP-Sec VPN とは決定的に違います。
server-client model は、中央集権的なシステムです。
その「中央」は「絶対」です。これを信じなければ、何も始まりません。
ということは、Zero Trust では無いのでは？と(私には)思えます。

また、KATABAMI は、ペア鍵から生成された IPv6 address を通信で用います。
アドレスと鍵に数学的な繋がりを持つことで「なりすまし」を封止することが目的です。
この方式は、そのデバイスを利用する「ヒト」ではなく、そのデバイス自体「モノ」を特定することになります。
「ヒト」中心なのか「モノ」中心なのかの違いは、大きいと思っています。
「ヒト」の認証は、上位レイヤで(一般的な認証手順)で行うことも可能ですし、生体認証なを併用することも可能です。
しかし「モノ」の認証は、そのデバイスを特定する情報が必要になります。
通常の IP address は偽装可能、なりすまし可能です。
MAC Address も、変更可能(＝偽装可能)です(スマホ等では、機器固有の MAC addess ではなく、その場で振る MAC address 機能も持っています)。
KATABAMI の 場合は、固有の IPv6 address と、それを確認する手順を持つことで、モノ自体を確実に特定できるという特性を持っています。

#13 tech talescale (https://tailscale.com/)

talescale は、SSO (Single Sign On) や IAM (Identity Access Management) と連携する機能を持っています。
大雑把には、SSO や IAM で「許可」されると、VPN server の認証が OK となり、振り出された IP address (talescale IP) で access 可能となるという仕組みです。
その VPN server を Wireguard が担うという仕組みです。

KATABAMI としては、Wireguard に対するのと同じ立ち位置です。
中央集権で良いの？　Zero Trust は「中央」は例外なの？
デバイスを特定する仕組みは必要ないの？
talescale 固有の話としては、下記もあります。
SSO や IAM が、一度、外(talescale)を流れることになるけど良いの？

#14 tech **KATABAMI と SoftEther VPN、PacketiX VPN 4.0 との違いは何ですか？**

SoftEther VPN (https://ja.softether.org/)
PacketiX VPN 4.0 (https://www.softether.jp/1-product/11-vpn)

OSS である SoftEther VPN と、その製品版である PacketiX VPN 4.0 があります。以下、SoftEther VPN としてコメントします。

単純に表すると、WireGuard よりも SoftEther VPN(以下、SEV) の方が、KATABAMI に近い部分があります。
SEV が 仮想LAN、仮想HUB と言っているのは、TUN/TAP(OS上の tunnel = 仮想LANデバイス)と等価です。
NAT traversal という機能も KATABAMI と同様ですし、処理負荷が小さいという点も

但し、使い方としては、一般的な VPN と同じです。
基本的には、ネットワーク と ネットワーク を接続するという考え方です。

使い方によっては、end-to-end での接続も可能ですが、KATABAMI の 持つ「address と key の数学的繋がり」という要素はありません。
これに対して、KATABAMI は end-to-end が基本です。
「address と key の数学的繋がり」によって、なりすましを防ぐという機能がセキュリティの基盤です。
AES-256bits を使っているところは頂けません。ARM系など Intel 以外の組み込み系への実装時に処理負荷の面で不利になります。

KATABAMI と比して有利な点を挙げます。
SSL-VPN (HTTPS)、OpenVPN、IPsec、L2TP、MS-SSTP、L2TPv3、EtherIP といった他の VPN protocol との接続があります。
既存システムとの接続性を確保するという点でメリットがあります。
もっとも、KATABAMI の 場合でも、
VPN で囲ったネットワーク上に1つ node を置けば、外部の KATABAMI の node と連接可能なので、他の VPN のネットワークとも接続できるとも言えます。
SEV の client は iOS に対応しています。どうやって、Apple のGuidelineを潜ったのか知りたいところです。

#15 tech **KATABAMI で シンクライアント のような動作は可能ですか？**

可能です。
KATABAMI は、IPv6 ベースの全てのプロトコルに対応しています。
ホスト側、クライアント側の両者に KATABAMI を install することで実現可能です。

実績がある組合せは下記の通りです。

ホスト		ゲスト	
OS	アプリ等	OS	アプリ等
Windows	－	Windows	Remote Desktop
Windows	－	MacOS	Remote Desktop
MacOS	－	MacOS	画面共有
MacOS	－	Windows	VNC client
Ubuntu	X2Go	Windows	X2Go client

専用のハードウェアなどは必要ありません。
KATABAMI は、処理パフォーマンスが高いので、画面再描画なども高速で操作上の違和感は少ない方です（一定のネットワークの帯域は必要です）。

※ 参考： NTT東日本-IPA「シン・テレワークシステム」
https://xtech.nikkei.com/atcl/nxt/column/18/00001/04192/

#18 RMS **KATABAMI RMS は、どのような機能が提供されるのでしょうか？**

KATABAMI 経由での下記のアクセス手段の提供
Remote Desktop／画面共有機能（Windows, MacOS）
SSH、HTTP/HTTPS、SMB
※ Internet 経由の場合は、KATABAMI Bridge の利用が必要となります。

#20 tech **KATABAMI Series を海外で運用することは可能ですか？**

Internet に接続可能な環境で在れば、特に日本国内に限定される機能はありません。
※ 国によっては、輸出規制などに抵触する可能性があるため、個別にご相談下さい。
暗号化方式も含め、OSS base ですので基本的には問題無いと思いますが念のために。

但し、KATABAMI PBX の外線接続機能は、日本国内の IP電話網 との接続検証しか行っていません。
※ 海外に設置した IP電話機 などでも、KATABAMI経由で 日本国内で外線接続することは問題ありません。
※ 日本国内以外での外線接続に関しては、調査・検討が必要です（場合によっては、認定などが必要となる可能性があります）。

#23 tech **OSSに依存しているため、常にOSSの最新状況と合わせて更新されるのでしょうか？**
SYNCHRO での対応は以下の通りです。
- OSS の 更新状況は定期的に watch しています。
- 更新があれば source code を download します
- code は C++、Go-lan で記述されており、walk through を行います
- 更新版の評価を行い、問題がなければ適用します。
- 必要に応じて pull request を投げるなど、コミュニティとは情報交換を行っています

#24 tech **OSSの開発がストップした場合にどのような対応を考えているのでしょうか？**
OSS の コミュニティが解散する、開発が停止するなどの場合には、SYNCHRO で、最新版のcode を基に、新しいOSへの適合、機能追加などの開発を行うことを考えています。

以下、パートナ様、販売代理店様向けです

#p1 busi **KATABAMI Series を 自社・製品やサービス などに組み込んで使用する場合、どのようなビジネス形態になるのでしょうか？**

その製品・サービスに対しての KATABAMI の付加価値として、その製品・サービスのご提供価格の 8% を SYNCHRO で申し受けさせて頂きます（レベニューシェアの形態です）。
製品・サービスの内容や、価格設定などにも依存しますので、上記のレートは個別のご相談にも応じます。

SYNCHRO は、組み込み、運用、サポートなどに対しての、技術的な支援を行います。

#p2 busi **KATABAMI の アプライアンス製品の パートナ様、販売代理店様 向けの提供価格は？**

ご契約を前提としまして、別途、ご提供価格表等をご提示します。

#p3 busi **KATABAMI Series を 自社ブランドの 製品やサービス として販売することは可能ですか？**

可能です。
ご契約を前提としまして、別途、ご提供価格表等をご提示します。