平成 30 年 1 月 30 日

報道関係者各位

株式会社 bitFlyer

「bitFlyer セキュリティ・ファースト」主義、
及びセキュリティ・顧客資産保護に関する取り組みについて

当社は 2014 年の創業以来、セキュリティ・顧客資産保護を経営上の最優先課題として取り組んでまいりました。引き続き、セキュリティ・顧客資産保護を最優先し、全力で取り組むことを表明するとともに、ここに「bitFlyer セキュリティ・ファースト」主義を発表いたします。また、当社及び当社グループの取り組みの一部を紹介させていただきます。

【「bitFlyer セキュリティ・ファースト」主義】

１．当社及び当社グループは、全社一丸となり最新セキュリティ技術を導入し、お客様にご安心いただけるセキュリティ管理体制を維持し続けます。
２．当社及び当社グループは、顧客資産保護のため必要なセキュリティ対策を策定し実施します。
３．当社及び当社グループは、万が一セキュリティに関する事故等が発生した場合には、金融庁、警察庁、警視庁及び日本ブロックチェーン協会（以下、「JBA」）と連携し、速やかに適切な措置を実施するとともにその状況を当局等に報告します。
４．当社及び当社グループは、セキュリティに関する内部監査体制を構築し、セキュリティ対策の継続的な改善・見直しを実施します。
５．当社及び当社グループは、セキュリティの重要性を常に認識し、各種法令・内部規程を遵守します。

当社は、金融庁の審査を経て、2017 年 9 月に仮想通貨交換業者としての登録を終えております。仮想通貨業界のリーディングカンパニーとして、以下のチームを中心に各種法令・内部規則を遵守しております。

・金融機関、中でも特にリスクに精通した分野出身の経営陣

・CISO（Chief Information Security Officer）を中心としたサイバーセキュリティチーム

・金融機関でのコンプライアンス業務経験者によるコンプライアンスチーム

・国内大手弁護士事務所出身の弁護士、米国及び欧州の弁護士チーム

また、2017 年 11 月には当社子会社である bitFlyer USA, Inc. が米国ニューヨーク州にて BitLicense を取得、2018 年 1 月には当社子会社である bitFlyer EUROPE S.A. が欧州ルクセンブルクにて Payment Institution License を取得いたしました。当該ライセンス取得において、AML/CFT やコールドウォレットの管理等は日本で法令上求められる水準よりも厳

格な運用が求められており、当社においても当該ライセンス取得要件以上の水準にて運用を行っております。また米国の NIST800-30, ISO31000 等のガイドラインに基づいた IT Security Audit を実施しております。

JBA より 2018 年 1 月 27 日に発表があったとおり、当社は 1 月 26 日に金融庁からセキュリティに関する注意喚起を受け取っております。当社は当注意喚起において金融庁より求められた対策については既に実行いたしましたことをお知らせいたします。

また、事業における優先順位の見直しを行い、セキュリティ・顧客資産保護のための施策が最優先であることを改めて全社で意識統一・徹底いたしました。当社システム全体を対象として、今一度セキュリティの観点から点検を実施し、瑕疵のないことを確認いたしました。引き続き、不正送金を始めとするさまざまな課題に対処できるよう、全力で取り組んでまいります。

セキュリティ管理体制の整備には終わりはなく、各種不正アクセス手法の変化に応じて最新の技術を取り入れ、日々努力し続けることが要求されます。当社は上記「bitFlyer セキュリティ・ファースト」主義に基づき各種施策を行い、お客様の大切な資産を厳格に守っていくことをお約束いたします。

【当社におけるセキュリティ施策についてのご紹介】

1．仮想通貨技術に関する施策

・コールドウォレット
お客さまおよび当社が所有する金額で 80% 以上の仮想通貨は、ネットワークから隔離されたコールドウォレットに保管されています。コールドウォレットは多重の物理的セキュリティ対策により保護され、24 時間監視システムにより強固に守られております。当社では各種取扱仮想通貨に関し一定の基準を設けてコールドウォレットでの管理をしておりますが、基準のさらなる厳格化を実施する予定です。また、コールドウォレットに限らず、秘密鍵は常に暗号化されており、万が一漏洩した場合でも第三者が秘密鍵を利用することは不可能です。

・マルチシグ（マルチ・シグネチャ）
マルチシグとは送金に複数の秘密鍵を要求することができる技術のことであり、マルチシグを採用することで高セキュリティのウォレットを構築できます。マルチシグを適切に構成することで、最重要データである秘密鍵が仮に 1 つ漏洩したとしても別の秘密鍵が無ければ仮想通貨の送付ができないように設定できます。一般的に、攻撃者が 2 つ以上の異なる設計のプラットフォームに同時に侵入することは非常に困難です。当社では各種取扱仮想通貨に関し一定の基準を設けてマルチシグ化をしておりますが、基準のさらなる厳格化を実施する予定です。

・自社開発のビットコインデーモン

一般的に利用されているビットコインデーモンはソースコードが公開されているために脆弱性を突かれ攻撃されるリスクがあります。当社は自社開発のビットコインデーモンを利用することで脆弱性を突かれるリスクが低くなっています。また、自社開発のビットコインデーモンと一般的に利用されているビットコインデーモン（bitcoind）を併用し常に相互チェックしているため、当社のビットコインデーモンに万が一の不具合があった場合でもすぐに検知、修正することができます。

・暗号学的に安全な擬似乱数生成器の使用

暗号学的に安全な疑似乱数生成器（Cryptographically Secure Pseudo-Random Number Generator：CSPRNG）は、

(1)生成されたビット列からその次に生成されるビットを 50% を超える確率で推測する方法が存在しない。

(2)乱数生成器の途中の内部状態が明らかになってもそれまでに生成された過去の乱数列を再現できない。

の 2 つの条件を満たします。(1)の条件により乱数の品質が保証され、(2)の条件により乱数器の内部状態を知る者による攻撃に耐えることが保証されます。秘密鍵の生成などにこのような乱数生成器を使用することで、情報が推測されることを防止します。

・セキュリティ上問題のないコインに限った取り扱い

アルトコインの中には匿名性が高く取引が追跡できないことでマネーロンダリングに使用され問題視されているものがあります。当社は、金融庁とも協議した上で社内のエンジニアや社外の専門家の意見を交え、セキュリティ上問題ないと判断したコインのみを取り扱いしております。

２．セキュリティ技術に関する施策

・通信セキュリティ

当社はお客様の個人情報を確実にお守りする為に、お客様からの全てのデータ通信を暗号化しております。当社は大手金融機関よりも強度の高い暗号化技術をお客様との通信に使用しています（Qualys, Inc. により A+の SSL 評価を頂いております)。お客様が当社サービスに接続する際は、通信プロトコルとして TLS1.2、暗号化方式として AES_128_GCM、鍵交換メカニズムとして ECDHE_RSA を使用することができます。

・FW/WAF

FW（ファイア・ウォール）により外部のネットワークからの攻撃や不正なアクセスから常時当社ネットワークやコンピュータを防御しています。不審な URL 及び実行ファイルは自動的にブロックされます。

また、WAF（ウェブ・アプリケーション・ファイアウォール）により FW では制限できないウェブ・アプリケーションへの通信内容を検査し、不正な通信を遮断しています。また DDoS 攻撃も二重の WAF によりブロックされます。

・IP アドレス制限

IP アドレスにより接続元を判別し、利用端末・サービスへのアクセスを制限しています。予め定められた IP アドレスからのみ利用端末・サービスへアクセスさせることで、第三者によるアクセスを防止しています。不審なアクセスを試みた IP アドレスは自動的にブラックリスト化され、不正侵入を防止します。さらに国ごとにアクセスを遮断しており、特に北朝鮮は厳重警戒の対象国になっております。

・2 段階認証の推奨

当社サービスへのログイン・出金・仮想通貨の外部送付時には SMS、メールアドレス、または認証アプリによる 2 段階認証機能を設定することができます。仮想通貨の外部送付時に 2 段階認証は必須となっており、重要な機能で強固なセキュリティを担保いたします。

・ログイン履歴の管理

当社にログインするごとに、ご登録のメールアドレスへアカウント凍結リンク付ログイン確認メールを送付する設定が可能です。これは万が一第三者によるお客様アカウントへのログインがあった際に、即時にアカウント凍結ができるための仕組みです。また、ログインは全て記録され、お客様の過去のログインの履歴について IP アドレス・日時を確認することができます。

・インフラストラクチャーの管理

当社のインフラストラクチャーは最新の OS パッチが自動で適用され、自己診断機能により各サーバーのヘルスチェックが行われるなど、厳格に管理されております。また、お客様の情報は全て暗号化し保管しております。

３．顧客資産保護に関する施策

・各種保険

当社は顧客資産の安全性向上のために、下記 2 種類の損害保険を国内大手損害保険会社と契約しています。「当社へのサイバー攻撃等によって発生したビットコインの盗難、消失等に係るサイバー保険」、「二段階認証登録ユーザー様のメールアドレス・パスワード等の盗取により行われた不正な日本円出金に係る補償」。また、ビットコインをはじめとする仮想通貨決済サービスに関わる賠償責任保険についても、三井住友海上火災保険株式会社と共同開発しており、仮想通貨交換業だけでなく、仮想通貨決済等あらゆる仮想通貨サービスにおいて保険の検討・契約を行ってまいります。

・仮想通貨交換業者最大級の資本金

当社は仮想通貨交換業者として最大級の資本金をもとに、取引所の運営やそのためのセキュリティ対策等に投資を行っております。

４．社内セキュリティに関する施策

・オフィスセキュリティ

2017 年 10 月に本社を東京ミッドタウンに移転いたしました。オフィス内においては、多数の監視カメラ・24 時間常時監視システム・生体認証装置等、厳重なセキュリティシステムを導入しております。

* 画像は東京ミッドタウンオフィシャルサイトがプレス向け情報に掲載している素材を、承諾を得て使用しているものです。

・社内セキュリティ研修

当社では、すべての職員にセキュリティ研修を行っています。また、サイバーセキュリティチームにより業務上使用する端末に対して厳重なセキュリティチェックを施しております。カスタマーサポートエリアは携帯電話の持ち込み禁止、また完全に別のネットワーク設計とし個人情報を厳重に管理しております。

【当社について】

当社は、SMBC ベンチャーキャピタル、みずほキャピタル、第一生命保険、三菱 UFJ キャピタル、三井住友海上キャピタル、リクルートストラテジックパートナーズ、電通デジタルホールディングス、SBI インベストメント、GMO VenturePartners、QUICK、ベンチャーラボインベストメントなどから出資を受けている国内最大の仮想通貨・ブロックチェーン企業です。FinTech の領域において仮想通貨・ブロックチェーンの技術開発を通じたイノベーションを目指し、仮想通貨総合プラットフォーム bitFlyer の運営、およびブロックチェーンの調査・分析、プライベート・ブロックチェーン「miyabi」を活用した新サービスの研究開発を行っています。

当社コーポレートサイト：https://bitflyer.jp/

当社紹介動画：https://youtu.be/tHpT3qI0ipI

ブロックチェーン「miyabi」の特長：https://bitflyer.jp/miyabi

ブロックチェーン「miyabi」の紹介動画：https://youtu.be/SxHZI08yhZ0

【本リリースに関するお問い合わせ先】

株式会社 bitFlyer　広報担当 金光 碧

〒107-6208 東京都港区赤坂 9-7-1 ミッドタウン・タワー8F

HP：https://bitflyer.jp　Contact：https://bitflyer.jp/ContactPage