
サイバーセキュリティクラウド、

耐量子計算機暗号（PQC）対応に向けた技術検証を開始

～量子コンピュータ時代を見据え、次世代のWebセキュリティ環境の実現へ～

グローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、将来的な量子コンピュータの実用化を見据え、耐量子計算機暗号（Post-Quantum Cryptography、以下「PQC」）への対応に向けた技術検証を開始したことをお知らせします。



当社では、本技術検証を通じてPQCに関する技術的な知見を蓄積し、[クラウド型WAF「攻撃遮断くん」](#)におけるPQC対応の実現を目指してまいります。

■背景：世界的に進むPQCへの移行

量子コンピュータの研究開発が世界的に進展する中、将来的に大規模な量子コンピュータが実用化された場合、現在インターネット上で広く利用されている公開鍵暗号の安全性が損なわれる可能性が指摘されています。こうした将来のリスクに備えるため、量子コンピュータによる攻撃にも耐えられるよう設計された「PQC」への移行に向けた取り組みが世界的に進んでいます。

米国国立標準技術研究所（NIST）は2024年8月、PQCに関する最初の3つの標準（FIPS 203、FIPS 204、FIPS 205）を正式に公開し、組織に対して新たな標準への移行を開始するよう推奨しています。

さらに2026年、G7サイバーセキュリティ・ワーキング・グループは、PQCへの移行準備に関するステートメントを公表。PQCへの移行を技術部門だけの課題ではなく、経営層の関与のもと、財務や調達などを含む組織横断的な取り組みとして進めることや、その第一歩として、自社システムおよびサプライチェーンを含む暗号利用状況を把握する「暗号資産の棚卸し」の重要性を示しています。

日本国内でも、金融庁が2024年に「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」を開催し、金融機関がPQCへの移行を検討する際の推奨事項や課題、留意事項について議論を行い、同年11月に報告書を公表しています。

このように、国内外でPQCの標準化や具体的な移行に向けた取り組みが進んでいます。こうした動向を踏まえ、当社では、量子コンピュータ時代においても安全なWeb環境を提供し続けることを目指し、PQC対応に向けた技術検証を開始しました。

■当社におけるPQC対応に向けた技術検証

当社は、量子コンピュータの実用化を見据え、Webサービスを支えるセキュリティ事業者として、PQCへの移行に必要な技術的な知見の蓄積と、当社サービスへの実装可能性を検証する取り組みを開始しました。

今回の技術検証では、PQCを活用したWeb通信における技術要件を整理するとともに、既存のWeb環境との互換性や通信性能への影響、当社が提供するセキュリティサービスへの適用に向けた技術的な課題などについて検証を進めます。

具体的には、以下の観点を中心に検証を予定しています。

・ RFC 10024に定義されるPQ/T（Post-Quantum／Traditional）ハイブリッド鍵合意方式に関する技術検証

- ・ 既存のWeb環境やブラウザ等との互換性の確認
- ・ 通信性能やレスポンスへの影響の検証
- ・ 当社サービスへの実装に向けた技術要件および課題の整理

本技術検証を通じて得られる知見をもとに、まずは[クラウド型WAF「攻撃遮断くん」](#)におけるPQC対応の実現を目指します。

「攻撃遮断くん」は、Webサイトへのサイバー攻撃を検知・遮断するクラウド型WAFとして、ユーザーとWebサーバー間の通信を保護しています。今後、PQCへの移行が進むことを見据え、Webセキュリティと暗号化通信の双方の観点から、将来にわたってお客様が安全にWebサービスを提供できある環境の実現を目指してまいります。

■今後について

当社は、本技術検証を通じてPQCに関する技術的な知見を蓄積するとともに、当社が提供するセキュリティサービスへのPQC適用に向けた研究・開発を進めてまいります。

その第一歩として、「攻撃遮断くん」におけるPQC対応の実現に向け、今回の技術検証で得られる知見を活用してまいります。

「攻撃遮断くん」におけるPQC対応の正式な提供時期および提供内容については、決定次第、改めてお知らせする予定です。

当社は今後も、サイバーセキュリティを取り巻く技術環境の変化を先取りし、現在のサイバー攻撃への対策だけでなく、将来の脅威も見据えたセキュリティ技術の研究・開発を通じて、安全なサイバー空間の実現に貢献してまいります。

株式会社サイバーセキュリティクラウド (<https://www.cscloud.co.jp>)

所在地 : 〒141-0021 東京都品川区上大崎3-1-1 JR東急目黒ビル13階

代表者 : 代表取締役社長 兼 CEO 小池 敏弘

設 立 : 2010年8月

「世界中の人々が安心安全に使えるサイバー空間を創造する」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使したWebアプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの1つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド プロダクトマネジメント部 担当：井田

TEL : 03-6416-9996 FAX : 03-6416-9997 E-Mail : pdm@csccloud.co.jp