The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

商用国家安全保障アルゴリズムスイート2.0及び量子コンピュータに関するFAQ

IPAからの注意事項:

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。独立行政法人情報処理推進機構(IPA)は、本文書に記載されている情報より生じる損失又は損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。

NSAからの注意事項:

This document was created in English by the United States' National Security Agency (NSA). It has been translated by a third party and NSA has not reviewed the translation. NSA is not responsible for any errors or omissions relating to this translation. NSA has granted permission to the Japanese Information-technology promotion Agency (IPA) to use the NSA logos and related properties only in a translation which represents a faithful reproduction of the original, and for no other purpose. All other rights reserved. You can find the original English version of this document at nsa.gov.

原文書は、米国国家安全保障局(NSA)によって英語で作成されたものです。この文書は第三者(注:IPA)によって翻訳されたものであり、NSAはその翻訳を確認していません。NSAは、この翻訳に関するいかなる誤りや不作為について一切の責任を負いません。NSAは、独立行政法人情報処理推進機構(IPA)に対し、NSAのロゴ及び関連資産を、原文を忠実に再現した翻訳文においてのみ使用し、他の目的では使用しないことを許諾しています。その他の全ての権利は留保されています。この文書のオリジナルの英語版はnsa.govで見ることができます。

セクション

背景

Q: 量子コンピュータとは何か、私たちが今使っているコンピュータとどう違うのか？

A: 量子コンピュータは、現在のコンピュータで使われている通常のビットの代わりに、驚くべき振る舞いをする「量子ビット」を使用し、特定の数学的アルゴリズムを古典的コンピュータよりも指数関数的に速く効率的に実行することができる。小規模な実験室規模の量子コンピュータがすでに実現されている。

Q: 「暗号関連量子コンピュータ（CRQC: Cryptanalytically Relevant Quantum Computer）」とは何か？

A: CRQCは、「cryptographically relevant quantum computer（暗号関連量子コンピュータ）」とも表記され、現実世界の暗号システムを攻撃できる量子コンピュータのことを指す。「C」が「cryptanalytically（暗号解読的）」か「cryptographically（暗号学的）」のどちらを示しているかは書き手の好みの問題であり、この文脈ではこの2つの用語は本質的に等価である。

Q: CRQCが開発された場合、どのような脅威があるか？

A: 仮にCRQCが構築された場合、非対称鍵交換やデジタル署名に現在広く使用されている公開鍵アルゴリズムを弱体化させることが可能であり、システムに壊滅的な影響を与える可能性がある。国家安全保障システム（NSS: National Security Systems）では、国家安全保障情報の機密性、完全性、及び真正性を保護するための重要な要素として、公開鍵暗号を使用している。

Q: 「量子耐性」暗号や「耐量子計算機」暗号とは何か？

A: 「量子耐性（QR: Quantum-Resistant）」暗号や「量子安全」暗号、「耐量子計算機（PQ: Post-Quantum）」暗号は、いずれも現在のコンピュータ上で実行可能な暗号アルゴリズムのことを指す言葉であり、古典コンピュータと量子コンピュータのどちらからの暗号解読攻撃に対しても耐性があるとされる。

Q: 商用国家安全保障アルゴリズムスイート2.0（CNSA 2.0: Commercial National Security Algorithm 2.0）とは何か？

A: CNSA 2.0は、最終的にNSSでの使用が承認されたQRアルゴリズムスイートである。以下の表は、アルゴリズムとその機能、仕様、パラメータを一覧化したものである。

表：商用国家安全保障アルゴリズムスイート2.0

アルゴリズム	機能	仕様	パラメータ
Advanced Encryption Standard (AES)	情報保護のための対称ブロック暗号	FIPS PUB 197	全ての分類レベルで256ビット鍵を利用する

CRYSTALS-Kyber	鍵確立のための非対称アルゴリズム	TBD	全ての分類レベルでLevel Vパラメータを利用する
CRYSTALS-Dilithium	デジタル署名のための非対称アルゴリズム	TBD	全ての分類レベルでLevel Vパラメータを利用する
Secure Hash Algorithm (SHA)	情報の縮約表現を計算するアルゴリズム	FIPS PUB 180-4	全ての分類レベルでSHA-384又はSHA-512を利用する
Leighton-Micali Signature (LMS)	ファームウェア及びソフトウェアに対して電子的に署名を行うための非対称アルゴリズム	NIST SP 800-208	全てのパラメータが全ての分類レベルで承認されている。SHA-256/192が推奨される
Xtended Merkle Signature Scheme (XMSS)	ファームウェア及びソフトウェアに対して電子的に署名を行うための非対称アルゴリズム	NIST SP 800-208	全てのパラメータが全ての分類レベルで承認されている

CNSA 2.0

Q: CNSA 2.0をどこで使うべきか？

A: CNSA 2.0アルゴリズムは、将来の設計か現在配備済み(の製品)かに係らず、NSSにおける公的標準アルゴリズムを使用する全ての製品に要求される。Suite B又はCNSA 1.0のアルゴリズムのいずれかを使用(している全ての製品)は、CNSA 2.0の使用への移行を要求される。本FAQの「時間軸」のセクションとアドバイザリ覚書に、移行期間に関する情報がある。更なる詳細は近日中に発表する予定である。

Q: NSAは、どのようにCNSA 2.0アルゴリズムを選択したのか？

A: NSAは、米国政府の商用アルゴリズムの承認を主導する国立標準技術研究所(NIST: National Institute of Standards and Technology)が標準化のために選抜したアルゴリズムを選定した。NSAは、それらが与えられたNSSセキュリティ要件に最適な性能を提供すると考えている。

Q: NSAは、CNSA 2.0アルゴリズムがどの程度の強度を持つと考えているのか？

A: NSAは、CNSA 2.0アルゴリズムの解析を独自に実施し、米国NSSの多様なミッションを保護するための長期的な使用に適していると考えている。NSAは、特定のセキュリティ指標に対するこれらのアルゴリズムの性能に関して、特定の主張をするものではない。

Q: NSAは、CNSA 1.0に対して作成したIETF RFC[1]と同様に、CNSA 2.0に対する実装ガイダンスを作

[1] Internet Engineering Task Force Requests for Comments.

成する用意があるか？

A: NSAは、CNSA 2.0アルゴリズムに対する実装ガイダンスを提供するつもりだが、そのガイダンスをどこで公開するかは決定していない。

Q: 本ガイダンスは誰向けのものか？

A: NSAは、CNSA 2.0要件、予想される（移行）時期、及びこれに関連するFAQを広く周知することで、NSSの所有者と運用者の移行計画を支援し、NSS要件を産業界に通知する。

Q: これが配備済みの機器にも適用されるというのはどういうことか？

A: 使用中のNSSシステムであっても、承認プロセスを通じて適用除外を受けない限り、タイムリーに更新する必要がある。これは、国家安全保障に関する覚書（NSM: National Security Memorandums）8[2]及び10[3]に従っている。

Q: NSSアルゴリズム要件に適合するためにどの方針に従うべきか？

A: 高グレード機器は、CJCSN 65104[4]及びCNSSAM 01-07-NSM[5]のガイダンスに従う。商用機器は、機器の種類にもよるが、2025年から2030年の間のどこかに設定されると予想されるCNSSP 15[6]で義務付けられる移行までは、CNSA 1.0に従う。NSM-10に従い、QRアルゴリズムは、国家情報保証パートナーシップ（NIAP: National Information Assurance Partnership）が認証した場合にのみ、ミッションシステムに実装されるべきである。

Q: ハッシュベース署名について、どこでより多く知ることができるか？

A: NISTは、NIST SP 800-208[7]でステートフルハッシュベース署名を標準化した。その規格では、このトピックに関する他の技術文書への参照も提供している。NSAは、その規格で概説された特別なシナリオにおけるNSSを保護するために、例えばファームウェア及びソフトウェアに対する署名用として、連邦情報処理規格（FIPS: Federal Information Processing Standards）で認証されたハッシュベース署名を使用することを推奨する。NSAが優先するパラメータセットは、4.2節のSHA-256/192を使用したLMSである。

---

[2] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 19 January 2022

[3] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022.

[4] Chairman of the Joint Chiefs of Staff Notice 6510, Information Assurance Cryptographic Device Modernization Requirements, August 2019.

[5] Committee on National Security Systems Advisory Memorandum 01-07-NSM, Cryptographic Equipment Modernization Planning, 20 March 2022.

[6] Committee on National Security Systems Policy 15, Use of Public Standards for Secure Information Sharing.

[7] NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes

Q: なぜソフトウェア及びファームウェアに対する署名が別個にリスト化されているのか？

A: ソフトウェア及びファームウェアに対する署名のために別個のアルゴリズムを選択した理由は、3 つある:

- NISTは、SP 800-208でこれらのアルゴリズムをすでに標準化しているが、他の耐量子計算機署名はまだ標準化されていない
- この署名のユースケースは、より緊急性が高い
- この選択により、潜在的な性能問題が最小限の影響しか与えないユースケースで、暗号解読の歴史が最も長いアルゴリズムを使うことができる。特に、この用途においては、アルゴリズムの状態を追跡しなければいけない要求（つまり、これらの署名の実装においては、与えられた公開鍵がソフトウェアやファームウェアに対して署名するために何回使われたか追跡できないといけないという要求）とよく合致する

Q: なぜファームウェアに対する署名がより緊急性が高いのか？

A: 多くのファームウェアに対する署名の場合、検証アルゴリズムは容易に更新できないこともある。したがって、ファームウェアに対する署名アルゴリズムは、システムのライフサイクルにわたって、しばしばロックインされることになる。

Q: 格子ベースの鍵カプセル化メカニズム（KEMs: Key Encapsulation Mechanisms）とデジタル署名について、どこで知ることができるか？

A: NISTは、格子ベースのKEMとデジタル署名を標準化すると発表した。NISTの耐量子計算機暗号標準化のページには、標準化活動におけるこれまでの選考段階でのレポートが掲載されている。これらのレポートには、検討されている暗号の概要と多くの参考文献が含まれている。

Q: NSAが、Falconではなく、CRYSTALS-Dilithiumを選択したのはなぜか？

A: NSSに対して、NSAはNISTに同意している：Falconのほうがセキュリティに影響を及ぼす可能性のある実装上のエラーが生じやすいと思われ、CRYSTALS-Dilithiumの方が望ましい。NISTはCRYSTALS-Dilithiumの標準化を優先するつもりなので、おそらく近いうちに利用できるようになるだろう。

Q: ソリューションがSHA-384やSHA-512以外のハッシュ関数を使用している場合はどうなるか？

A: NSAは、SHA-384がNSSに十分なセキュリティを提供すると考えており、最新のCNSAスイートでもSHA-384が承認されている。設計者は性能上の理由から、しばしばSHA-512の使用を好む。SHA-512は現在CNSA 2.0でサポートされている。しかし、顧客は、SHA-512を使用することで相互運用性の問題が生じないことを確認する必要がある。一部の暗号アプリケーションでは、設計の一部として、ハッシュ値の縮退、又は他のNIST承認ハッシュ関数を使用する。このような場合、明確化のために、NSAはプロトコル固有のガイダンスを提供する場合があり、また顧客はNSAに相談することができる。しかし、他のハッシュアルゴリズムを使用することは、一般に承認されない。もっとも、新しいQRアルゴリズムでは、アルゴリズムの内部に変形SHA-3を利用している。NSAはこれに関して懸念はしていないが、現時点ではSHA-3アルゴリズムを汎用的に使用することを承認することは想定していない。

Q: CNSA 2.0実装は、どのようにNSSに対して強制されるのか？

A: 認可担当者は、NSM-10に基づき、定期的に採用状況を報告する。セキュリティのために暗号を使用する全てのシステム（ソフトウェア更新メカニズムを含む）がCNSA 2.0アルゴリズムを実装していることを確認するために利用可能なツールとリソースを使用することが重要である。いかなる違反も、NSM-10のプロセスに従って、NSAに報告しなければならない。

（移行のための）時間軸

Q: NSAは、CNSA 2.0の採用について、どのような時間軸情報を提供できるか？

A: NSAは、NSM-10で取り入れられた目標に従い、2035年までに全てのNSSに量子耐性を持たせるつもりである。商用ソリューションについて、NSAはNISTが承認した商用暗号に依拠する。NISTがCNSA 2.0に関連する標準を確定した後、NSAはCNSSP 15を更新する予定である。所定の技術について適切な標準が整備された時点で、新しい暗号（製品）開発においてはCNSA 2.0アルゴリズムを選択できるようにサポートすることが要求され、全ての適切なシステムコンポーネントがCNSA 2.0アルゴリズムを優先するように設定されるべきである。製品が成熟するにつれて、これらのコンポーネントはCNSA 2.0アルゴリズムのみを受け入れるように設定されるべきである。

製品ラインナップにより開発速度は異なるため、NSAによるガイダンスとプロテクションプロファイルのアップデート版の提供は、産業界が適切な標準を開発するのに応じて行う予定である。CNSA 1.0アルゴリズムは、現在のソリューションがCNSA 2.0モードで動作できるようになるまで、引き続き使用される予定である。移行タイミングに関するNSAの現在の見解は以下の通りである：

- ソフトウェア及びファームウェアに対する署名：直ちに移行を開始し、2025年までにCNSA 2.0をサポートし優先利用する。2030年までにCNSA 2.0を排他的に使用する
- ウェブブラウザ／サーバ、及びクラウドサービス：2025年までにCNSA 2.0をサポートし優先利用する。2033年までにCNSA 2.0を排他的に使用する[8]
- 従来のネットワーク機器（例：仮想プライベートネットワーク、ルータ）：2026年までにCNSA 2.0をサポートし優先利用する。2030年までにCNSA 2.0を排他的に使用する
- オペレーティングシステム：2027年までにCNSA 2.0をサポートし優先利用する。2033年までにCNSA 2.0を排他的に使用する
- ニッチな機器（例：制約のある機器、大規模な公開鍵基盤システム）：2030年までにCNSA 2.0をサポートし、優先利用する。2033年までにCNSA 2.0を排他的に使用する
- カスタムアプリケーション及び旧機器：2033年までに更新又は交換する

Q: 新規導入のスケジュールは？

A: NIAPと機密保持のための商用ソリューション（CSfC: Commercial Solutions for Classified）プログラムは、産業界の採用状況に合わせてプロファイルと要件を更新する。NSAは、積極的な採用のための時間軸を考えており（上記の箇条書きを参照）、産業界のサポートを要請する。

[8] プロトコル規格、製品の入手可能性、又は相互運用性の要件により、ハイブリッドソリューションが許容又は要求されたとしても、所定の日付でCNSA 2.0アルゴリズムが選択できるように義務付けられ、CNSA 1.0アルゴリズムのみの選択はもはや承認されなくなる。

Q: 配備済み機器の移行スケジュールはどうなっているか？

A: 産業界がCNSA 2.0アルゴリズムを採用するにつれ、NSAは配備済み機器のCNSA 2.0への移行を要求する。状況によっては、これはハードウェアの交換を必要とするかもしれない。NSAは、NSSの所有者と運用者が移行計画を作ることを推奨する。

Q: NIST標準が完了／確定するのはいつか？

A: この質問は、NISTに問い合わせるのが一番である。詳しくは、NISTの耐量子計算機暗号標準化プロジェクトのページを参照されたい。

Q: NSAアルゴリズム実装のためのIETF RFCが利用できるようになるのはいつか？

A: IETFや他の標準開発組織（SDO: Standards Development Organizations）は独立した組織である。NSAは、実現すべき適切なレベルのセキュリティと実装の分析が行い、適切な優先順位で、速やかにRFCや他のSDO標準に反映されることを期待している。NSAは、CNSA 2.0が標準に採用され、ベンダ製品に展開されることを推奨している。

（移行のための）準備

Q: 将来の量子耐性アルゴリズムスイートに備えるために、開発者やプログラムは何をすればよいのか？

A: AES-256、SHA-384、SHA-512、及びNIST SP 800-208に記載されているNISTハッシュベース署名は、大規模量子コンピュータによる攻撃に対して安全であると考えられている。

開発者は、これらのアルゴリズムをすぐに導入すべきである。また、NISTとNSAが選んだ他の量子耐性アルゴリズムの実装を開始し、問題を発見した場合はフィードバックを提供すべきである。NSSの所有者と運用者は、アルゴリズムの実装を研究室ネットワークでテストし、移行に備えるべきである。

Q: 量子耐性システムに移行するにはどうしたらいいか？

A: CNSA 1.0スイートは、CNSA 2.0のアルゴリズムへの商用領域での移行に際しての暫定的な戦略であり続ける。今後予定されているNSAガイダンスとNIST標準化努力に従うことが、NSSの所有者と運用者がこの移行を行うための最良の位置付けとなる。

Q: 今、商用ベンダが採用すべき量子耐性公開鍵アルゴリズムはあるのか？

A: NSAは、ベンダがソフトウェア及びファームウェアに対する署名にCNSA 2.0承認のハッシュベース署名を使用することを推奨している。NSAは、標準化完了前の、あるいはFIPS認証を受けていないCNSA 2.0アルゴリズム（ハイブリッドモードであっても）をNSSのミッションに使用することを承認しない。

しかし、NSAは、移行に備えるため、標準化完了前の、あるいはFIPS認証を受けていないCNSA 2.0アル

ゴリズムとモジュールの研究環境での限定的な使用は推奨している。

NSAは、NISTが標準化を完了した後すぐに製品を提供できるよう、ベンダがCNSA 2.0アルゴリズムの実装準備を開始するよう要請している。

CNSSP 15

Q: CNSSP 15とは何か？

A: 国家安全保障システム委員会方針15（CNSSP 15: Committee on National Security Systems Policy 15）は、他のCNSS及びNSAの文書化プロセスと連動して、NSSを保護するための商用暗号アルゴ リズムを規定している。当初は「NSAスイートB」を規定していたが、CNSSP 15 Annex Bに規定されるCNSA 1.0スイートに改訂された。NISTが標準化プロセスのラウンド3で選抜したものの標準化が完了するのに伴い、それらのアルゴリズムはCNSAアルゴリズムに含まれる予定である。CNSSの詳細はwww.cnss.govにある。

Q: CNSSP 15に何が起きるのか？

A: 2016年10月のCNSSP 15の更新では、3つの重要な変更が行われた。第一に、システムを「スイートB」規格に移行するという以前の要件を置き換え、耐量子計算機暗号標準が開発される間、より多くのアルゴリズム（すなわちCNSA）を選択できるように規定し、既存のソリューションの使用を拡張できるようにした。第二に、スイートBの2つのセキュリティレベルを統合し、全てのレベルで使用できる単一の要件とした。最後に、旧バージョンのCNSSP 15は機密情報のみに焦点を当てていたが、更新された方針は、機密情報と非機密情報の両方を含む、全てのNSSに適用されることとなった。NSAは、最近のサイバーセキュリティ勧告「商用国家安全保障アルゴリズムスイート2.0の発表」にあるように、CNSSP 15のアルゴリズムをCNSA 2.0アルゴリズムスイートに更新し、その次のバージョンでCNSA 1.0アルゴリズムを非推奨とする計画である。NSAは、その他の以前の変更点をそのまま維持し、非機密NSS及び全ての機密レベルのNSSの両方に対する単一の要件セットを作ることを計画している。

Q: CNSSP 15は、CNSSI 1253やNIST SP 800-53、RMFプロセスとどのような関係があるか？

A: CNSS指示1253[9]は、国家安全保障情報システムの管理において、NIST SP 800-39[10]及び800-53[11]に記載されるリスク管理フレームワーク（RMF: Risk Management Framework）を使用することを義務付けている。SP 800-53には、暗号に関連するセキュリティ管理（例：SC-12）が含まれている。NSSでは「NSA承認」の選択を要求している。NSAが特に明記しない限り、「NSA承認」暗号の選択には、CNSA 1.0アルゴリズム要件、及び製品の認証と運用に関する他の全ての関連NSAガイダンスが含まれる。

[9] Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems.

[10] NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

[11] NIST Special Publication 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations.

Q: より広範な政府コミュニティは、CNSSP 15の要件をどのように理解すべきか？

A: NSAはNSS要件を定めている。多くの場合、これらのシステムは、非常に高度で十分なリソースを持つ敵対者が潜在的な戦時環境において行う標的型攻撃に対して、長期間にわたって保護される必要がある。NISTは、他の政府システムのための暗号標準を制定している。NSS要件が特定のシステムに適用されるかどうかが不明な場合は、支援のためにNSAに問い合わせされたい。また、NIST SP 800-59[12]も参照されたい。

量子耐性への代替案

Q: 事前共有鍵を使用することで、量子（コンピュータによる暗号解読）の脅威を軽減することができるか？

A: 多くの商用プロトコルは、量子の脅威を軽減するために事前共有鍵を利用する選択肢を認めており、さらに事前共有鍵と非対称鍵を同じ（鍵共有）ネゴシエーション中に組み合わせることを認めているものもある。しかし、この問題は複雑である可能性がある。この選択肢を検討したい顧客は、NSAに問い合わせるか、CSfCプログラムが提供するガイダンスに従うべきである。

Q: 量子コンピュータは、公開鍵ではないアルゴリズム（つまり、対称アルゴリズム）に影響を与えるのか？

A: 量子コンピュータ技術による効果は、対称アルゴリズムに対するほうが、現在広く使われている公開鍵アルゴリズムよりもはるかに低いと一般に考えられている。公開鍵暗号は根本的な設計変更が必要だが、対称アルゴリズムは鍵長が十分大きければ安全であると考えられている。CNSA 2.0の対称アルゴリズムは、基本的にCNSA 1.0の対称アルゴリズムと同じであり、量子耐性を有している。

Q: なぜNSAは、今、量子コンピュータに関心を持つのか？量子コンピュータはまだ先の話ではないのか？

A: NSAは、CRQCがいつできるか判断できない。専門家の評価では、時期についてかなり意見が分かれている。NSSは非常に長いライフサイクルを持つことが多いため、NSAは何十年も先に使用されるシステムの要件を今日作成しなければならない。これらのシステムが保護するデータは、これらのシステムが寿命を迎えた後も、数十年にわたり暗号による保護を必要とする。量子コンピュータの分野は研究が進んでおり、NSSを保護するために、NSAがCNSA 2.0への移行のための要件を提供する行動を今しなければならないほど、進展している。

Q：量子鍵配送（QKD: Quantum Key Distribution）や量子暗号とは何か？

A: 量子暗号の分野では、量子力学の原理を利用した特殊なハードウェアを使って、機密情報の機密性を保護する。今日の最も一般的な例は、量子物理学を利用して、従来の対称アルゴリズムで使用する鍵を配送するものであり、「量子鍵配送」又は「QKD」と呼ばれている。この技術は現時点で実現しており、将来暗号アルゴリズムを攻撃しうる量子コンピュータ技術とは異なる。QKDの唯一の機能は、ユーザ間で鍵を配送することだけである。従って、QKDは暗号システムの一部分に過ぎない。

[12] NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.

Q: QKDシステムを使って、量子コンピュータから国家安全保障システムを守ることはできるか？

A: 守ることはできない。（QKDの）関連技術は科学的に非常に興味深いものであるが、一部のセキュリティ脅威にしか対応できず、NSS通信システムにも大幅なエンジニアリング的な変更が求められる。**NSAは、一般論として、QKDがNSSを保護するための実用的なセキュリティソリューションであるとは考えていない。**現時点では、NSSの所有者は、NSAに直接相談することなしに、QKDを使用又は研究するべきではない。具体的な質問については、NSSの所有者はNSAに問い合わせることができる。

Q: 量子乱数生成器（量子RNG: Random Number Generator）とは何か？

A: 量子乱数発生器は、特定の量子効果を用いて非決定論的なランダム性（を有する乱数）を生成するハードウェア乱数発生器である。特定のシナリオにおいてどのRNGが適切であるかの判断は、多くの要因に依存する。また、適切に認証／承認されたRNGはいずれも、その承認の制約内で実装されたものであれば、許容されるべきである。

機密保持のための商用ソリューション（CSfC: Commercial Solutions for Classified）と国家情報保証パートナーシップ（NIAP: National Information Assurance Partnership）

Q: NIAP／CSfCを通さずに、CNSA 1.0又はCNSA 2.0の対応製品をNSSで使用することは可能か？

A: 使用できない。CNSSP 11では、NSS上の情報を保護する目的で取得される全ての商用市販品の情報保証（IA: Information Assurance）及びIA対応情報技術製品について、NSA承認のプロセス及び該当する場合はFIPS暗号認証プログラムの要件に従って、NIAPプログラム要件に準拠しなければならないと記載されている。さらに、CNSSP 7では、適切な権限者が承認し、NSAのCSfCプログラム管理オフィスへの登録により、NSAが提供する能力パッケージに準拠していることが示されている場合に限り、そのCSfCソリューションはNSSを保護することができると記載されている。

Q: 長期間のデータ寿命を踏まえてCSfCソリューションを採用したい。量子コンピュータを持つ敵対者に対して、通信やデータの安全性を確保し続けるにはどうしたらよいか？

A: 現在のいくつかのCSfCソリューションは、長期的な量子コンピュータの脅威から保護する事前共有対称鍵を使用して実装されているかもしれない。NSAは、NIST標準と互換性の全くない実験的な耐量子計算機非対称アルゴリズムを実装するよりも、標準に準拠した方法で事前共有対称鍵を使用する方が、近未来の耐量子ソリューションとして優れていると考えている。最終的には、NSAは、商用技術開発に合わせて、CNSA 2.0アルゴリズムを実装するための能力パッケージを提供する予定である。詳細については、CSfCプログラムオフィスに問い合わせされたい。

将来の暗号アルゴリズム

Q: 暗号の他の分野（ブロックチェーン、個人情報検索、IDベース暗号など）では、どのようなアルゴリズムを使用するべきか？

A: NSAは、以下に挙げる革新的な暗号（又は他の類似の暗号革新）の潜在的なユースケースについて知

りたい。CNSSP 15は、公的標準の使用を義務付けているが、必要な場合にはNSA承認の追加の選択肢として例外を認めている。NSAとNISTのいずれもがこれらの領域の標準を作成しておらず、NSAはこれらの技術を使用するためのいかなる一般的な承認も出していない。これらのトピックの多くは、さらなる精査を必要とする新しいセキュリティ特性を含んでいる。NSSの所有者は、CNSA 1.0やCNSA 2.0、他の公表されたガイダンスが規定していない暗号を使用する前に、NSAに相談すべきである。特に、以下については、一般に承認されたソリューションがない:

- 分散台帳、又はブロックチェーン
- 個人情報検索(PIR: Private Information Retrieval)
- 個人集合交差(PSI: Private Set Intersection)
- IDベース暗号(IBE: Identity-Based Encryption)
- 属性ベース暗号(ABE: Attribute-Based Encryption)
- 同型暗号(HE: Homomorphic Encryption)
- グループ署名
- リング署名
- 検索可能暗号

Q: 新しい暗号ソリューションを持っている。どうすれば「NSA Approved」を取得できるか?

A: NSAには、機密情報を保護するために構築された、ソリューションを認証するためのプログラムがある。この認証プロセスは、特に政府の使用又は管理を目的とした開発に適用される。また、NSAは、NIAPなどの取り組みに参加し、機密保持のための商用ソリューション(CSfC)プログラムも運営しており、そのどちらについても従来の暗号標準と設計に厳格に準拠することが求められている。NSAは、商用ベンダからの製品認証の直接的な依頼の受付や、新しい暗号ソリューションの汎用的なベンダ認証の提供は行っていない。既存のプログラムが対象としているもの以上の暗号を使用する必要があるミッションであるとNSSの顧客が考える場合、NSAと直接関わり、その独自の状況を議論するべきである。

ハイブリッド(方式)

Q: ハイブリッド暗号ソリューションとは何か?

A: プロトコルにおけるハイブリッドソリューションとは、鍵合意や認証のような同じ機能を実行するために、複数のアルゴリズムを使用するものである。このソリューションは、攻撃者がシステムのセキュリティを危殆化させるために、それぞれのアルゴリズムを破ることが求められる方法でアルゴリズムを使用する。ハイブリッドソリューションは、多くの従来のアルゴリズムやQRアルゴリズムで構成することができる。「コンポーネントアルゴリズム」とは、ハイブリッドソリューションで使用される個々のアルゴリズムのことである。

Q: ハイブリッドソリューションの利用について、NSAはどのような立場をとっているか?

A: NSAは、CNSA 2.0アルゴリズムを信頼しており、NSSの開発者がセキュリティ目的でハイブリッド認証製品を使用することを要求しない。製品の入手可能性と相互運用性の要件により、ハイブリッドソリューションを採用することになるかもしれない。NSAは、いくつかの規格が、より大きなサイズを持つCRQCアルゴリ

ズムに対応するためにハイブリッド的な構造を使用する必要があることを認識しており、実装のための最良の選択肢について産業界と協力する予定である。

Q: ハイブリッドソリューションを使用すると、どんな厄介な問題が発生するか？

A: ハイブリッド方式では、設計者が追加のネゴシエーションとエラー処理を組み込む必要があるため、プロトコルに複雑さを加えることになる。ハイブリッド方式の導入は、全てのアルゴリズム及びハイブリッド化の方法が通信の全ての当事者に共通する機能でなければならないため、相互運用性に関するさらなる懸念を引き起こす。

外部で開発されている多くのハイブリッドソリューションは、厳密なQRソリューションへの移行を促進しないため、実装者は、従来のアルゴリズムが実用性を失うにつれ、ハイブリッド方式からQRへの大幅な追加移行を想定しておく必要がある。

おそらく最も重要なことは、ハイブリッドソリューションは実装をさらに複雑にするため、複雑化に伴う実装に瑕疵が発生するリスクと、暗号解読にブレークスルーが発生するリスクのバランスをとらなければならない。

セキュリティ製品の失敗は、その基礎となる暗号アルゴリズムの失敗よりも、実装や設定の誤りが原因であることが多い。したがって、限られたリソースを費やして暗号を複雑化することは、セキュリティを弱める可能性がある。

NSAがハイブリッドソリューションをサポートする場合、実装の互換性、高度な堅牢性を確保するためのエンジニアリング、及びQR専用ソリューションへの容易な移行の促進を保証するための広範な作業が必要になる。

Q: NISTの耐量子計算機暗号標準の最終版を待つ間、ハイブリッドソリューションや他の非標準のQRソリューションを使うべきか？

A: ハイブリッドソリューションや他の非標準のQRソリューションをNSSミッションシステムに使用してはならない。NSAは、研究や計画のための限定的な購入や使用は推奨するが、CNSA 2.0への移行の準備の目的のみに限定する。NSAは、CNSA 2.0アルゴリズムがNSSを十分に保護すると信頼しているため、セキュリティ目的のためにハイブリッドソリューションを必要としない。非標準のソリューションを使用することは、互換性のないソリューションを設置する大きなリスクを伴う。規定された標準（例えば、RFC 8446、RFC 8784）に従って対称鍵を含むハイブリッドソリューションを使用することは適切かもしれないが、鍵管理の複雑さから一般的に特殊なアプリケーションでの使用に限定される。

更なる情報

Q: 更なる情報はどこで得られるか？

A: CSfC固有の質問については、顧客は機密保持のための商用ソリューション（CSfC）プログラム管理オフィス（CSfC@nsa.gov）に連絡すること。

NSSユーザからのその他の具体的な質問は、電子メールでNSACryptoToday@nsa.govに、又は通常のビジネスチャネルを通じて問い合わせることができる。

承認の免責事項

本書に含まれる情報及び見解は、「現状のまま」提供され、いかなる正当化も保証も行わない。本書において、商号、商標、製造業者、その他によって参照している特定の商用製品、プロセス又はサービスを、米国政府が承認、推奨、又は優遇していることを意味するものではなく、本ガイダンスを広告又は製品推奨の目的で使用してはならない。

目的

本書は、NSAのサイバーセキュリティのミッションを推進するために作成されたものである。そのミッションには、国家安全保障システム、国防総省、及び国防産業基盤情報システムに対する脅威と脆弱性を特定して発信し、サイバーセキュリティ仕様と緩和策を開発し公表するという責任を含む。この情報は、全ての適切な利害関係者に届くように広く共有される場合がある。

お問い合わせ

サイバーセキュリティレポートに関するお問い合わせとご意見：CybersecurityReports@nsa.gov

防衛産業基盤に関するお問い合わせとサイバーセキュリティサービス：DIB_Defense@cyber.nsa.gov

メディア問い合わせ／プレスデスク：443-634-0721, MediaRelations@nsa.gov