Announcing the Commercial National Security Algorithm Suite 2.0

商用国家安全保障アルゴリズムスイート2.0の発表

IPAからの注意事項:

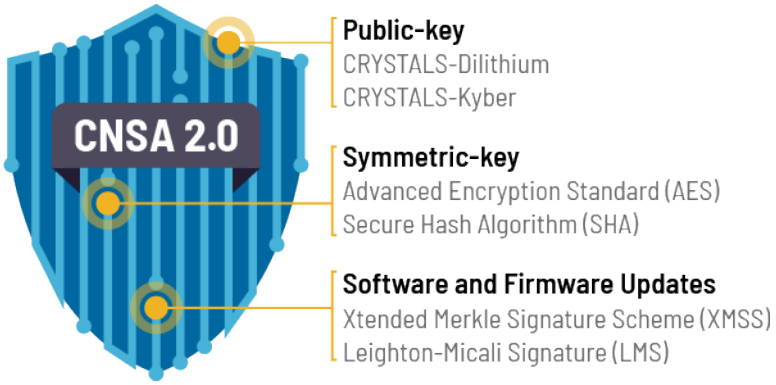
本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。独立行政法人情報処理推進機構（IPA）は、本文書に記載されている情報より生じる損失又は損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。

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。

要旨



暗号解読関連量子コンピュータ（CRQC: cryptanalytically relevant quantum computer）が将来配備された場合の防護の必要性はよく知られている。その始まりは、1990年代半ばに、CRQCによって現在使われている公開鍵暗号システムを破ることができるだろうことをPeter Shorが発見した時である。学術界や産業界、いくつかの政府による量子コンピュータ研究の継続的な進展は、量子コンピュータの展望が最終的に実現されることを示唆している。したがって、今が、国家安全保障システム（NSS: National Security Systems）と関連資産を継続的に保護するために、量子耐性（QR: quantum-resistant）アルゴリズムへの効果的な移行を計画し、準備し、予算化する時である。

この勧告は、NSSの所有者と運用者、及びベンダに対して、NSSに対するQRアルゴリズムの将来の要求事項を通知する。これらのアルゴリズム（耐量子計算機アルゴリズムとも呼ばれる）は、古典コンピュータと量子コンピュータの両方に対して安全であると分析されている。これらは、商用国家安全保障アルゴリズムスイート（Commercial National Security Algorithm Suite; CNSA 1.0と呼ばれ、現在CNSSP 15, Annex Bに記載されている）のアルゴリズムをアップデートするものである。NSAはこのアップデートをCNSAスイート2.0として参照し、今後のアップデートではバージョン番号を変更する予定である。

NSAは、NSD-42、NSM-8、NSM-10、CNSSP 11及びCNSSP 15に詳述された権限に従い、この勧告を提供する。この指示は、全ての非機密NSS及び機密NSSに含まれている、（NSAが開発したアルゴリズムとは異なる）公開鍵暗号アルゴリズムを使用する全てのNSSに適用される。国家管理者（National Manager）が承認していない、いかなる暗号アルゴリズムの使用も一般的には許可されず、（使用する場合には）アルゴリズム、実装及び用途に固有の制限免除を必要とする。CNSSP 11に従い、暗号サービスを提供するソフトウェアとハードウェアは、CNSAの適切なバージョンの要件を満たすことに加え、国家情報保証パートナーシップ（NIAP: National Information Assurance Partnership）認証又はNSA認証を必要とする。

はじめに

この勧告は、以下のセクションからなる：

- ソフトウェア及びファームウェアに対する署名のためのアルゴリズム：米国国立標準技術研究所（NIST: National Institute of Standards and Technology）は少し前に署名のためのアルゴリズムを標準化したが、この特別なユースケースのために従来と異なるアルゴリズムを使用することはCNSA 2.0では新しいことである。
- 対称鍵アルゴリズム：本セクションでは、CNSA 1.0からわずかな変更点があるだけだが、もう少しの柔軟性を持たせることができる。
- 汎用的な量子耐性公開鍵アルゴリズム：ほとんどのアプリケーションで必要とされる主流の公開鍵アルゴリズムである。標準化が完了していないため、本セクションは将来的なものである。
- 移行タイミング：CNSA 2.0への移行タイミングについて説明する
- 施行：NSSアルゴリズム要件の施行に関連する要件を要約する
- 追加ガイダンスとしてのRFC：CNSA 1.0の実装に使用された有用なInternet Engineering Task Force Requests for Comment（IETF RFC）へのリンクを提供する
- 参照表：CNSA 2.0とCNSA 1.0のアルゴリズムをリストアップした2つの表を備える

ソフトウェア及びファームウェアに対する署名のためのアルゴリズムについて

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、（他のユースケースとは）異なるアルゴリズムを選択した理由は、3 つある：

- NISTは、表 I で挙げる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

ソフトウェア及びファームウェアに対する署名に選ばれたアルゴリズムは、NIST Special Publication 800-208で規定されているものとなる。NSAは、SHA-256/192を使用したLeighton-Micaliを推奨するが、全てのNIST SP 800-208に掲載されたアルゴリズムがこのユースケースに対して承認されている。これらの署名のセキュリティを弱めることを避けるために、状態を管理し、ハードウェアで署名するような実装の必要性を含め、SP 800-208の全ての要件を満たさなければならないことに注意されたい。

NSAは、ベンダがNIST SP 800-208による署名の採用を直ちに開始することを推奨している。要件のタイムラインに関する詳細については、「移行タイミング」のセクションを参照されたい。次表は、ソフトウェア及びファームウェア（に対する署名アルゴリズム）のアップデートのためのCNSA 2.0アルゴリズムの一覧である。

表 I: ソフトウェア及びファームウェア（に対する署名アルゴリズム）のアップデートのためのCNSA 2.0アルゴリズム

アルゴリズム	機能	仕様	パラメータ
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電子的に対して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

対称鍵アルゴリズムについて

以下の表は、CNSA 1.0と比較して、SHA-512がリストに追加されたことが唯一の変更点であることを示している。

表 II: CNSA 2.0 対称鍵アルゴリズム

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
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

汎用的な量子耐性公開鍵アルゴリズムについて

NISTは、最近、耐量子計算機暗号の標準化の選抜結果を発表した。つまり、現時点では最終的な標準規格も、連邦情報処理規格（FIPS: Federal Information Processing Standard）認証された実装も存在しない。NSAは、将来のNSS要件を提供するために、今回の公開鍵アルゴリズムの選抜結果を公表する。これにより、ベンダは、これらの要件に向けて構築を開始することができ、調達担当者、NSSの所有者と運用者は要件が何であるかを知ることができる。

これが義務付けられた場合、RSA、Diffie-Hellman（DH）、楕円曲線暗号（ECDH、ECDSA）の使用は事実上非推奨となることに留意されたい。NSAは、NSSの所有者と運用者に対して、これらの要件に特別な注意を払うよう強く促す。暫定的に、CNSA 1.0への準拠が引き続き要求される。次セクションで移行タイムラインを規定する。次表は、CNSA 2.0 アルゴリズムの一覧である。

表III：CNSA 2.0量子耐性公開鍵アルゴリズム

アルゴリズム	機能	仕様	パラメータ
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

移行タイミングについて

移行タイミングは、標準化に基づく実装の普及に依存する。テクノロジーごとに異なるペースでQRアルゴリズムを採用するため、NSAは全体的な移行終了日と、今後具体的な日付を決定するためのプロセスを提供する。

NSAは、NSM-10に沿って、NSSのQRアルゴリズムへの移行が2035年までに完了することを期待している。NSAは、ベンダ、及びNSSの所有者と運用者がこの期限を守るためにあらゆる努力をすることを強く促す。実現可能な場合、NSSの所有者と運用者は、移行期間中にシステムを構成する際、CNSA 2.0アルゴリズムを優先するよう要求される。適切な場合、NSS内の商用製品のクラスではCNSA 2.0アルゴリズムの使用が義務付けられる。ただし、特殊な用途では他のアルゴリズムを許可する選択肢は留保される。

CNSA 2.0アルゴリズムの使用への一般的な移行方法は以下の通りである：

1 NIAP は、NIST標準や他の標準化団体の標準、標準準拠の暗号機器の開発に基づき、製品がCNSA 2.0アルゴリズムをサポートすることを明記したプロテクションプロファイルを公開する。

2	全ての新規機器はプロテクションプロファイル要件を満たさなければならない。旧機器は、NIAP準拠を維持するために次回の更新時に要件を満たさなければならない。	
3	認証及びテストされたソリューションが利用可能になり次第、CNSA 2.0アルゴリズムを優先的な構成の選択肢として使用することが開始される。	
4	NIAPプロテクションプロファイル要件及び更新されたNSM-10技術要件により、旧アルゴリズムのサポート廃止が決定される。	
5	その時点で、定期的に更新されない旧機器やソフトウェアは制限免除が必要となるとともに、準拠させるための計画が求められる。	

ソフトウェア及びファームウェアに対する署名の移行タイミングについて

ソフトウェア及びファームウェアに対する署名について、NSAは以下を推奨する:

1. ソフトウェア及びファームウェアに対する署名は、直ちに移行を開始する
2. 新しいソフトウェアとファームウェアでは、2025年までにCNSA 2.0署名アルゴリズムを使用する
3. 2025年までに、CNSA 1.0アルゴリズムに準拠していない配備済みのソフトウェアとファームウェアを、CNSA 2.0アルゴリズム準拠に移行する
4. 2030年までに、配備された全てのソフトウェアとファームウェアをCNSA 2.0署名準拠に移行する

NSSに対する他の要件について

NSAは、NSSに対する他のCNSA 2.0要件の実装について、以下のタイムテーブルを想定する。

- 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[1]
- 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（IoT機器など）、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

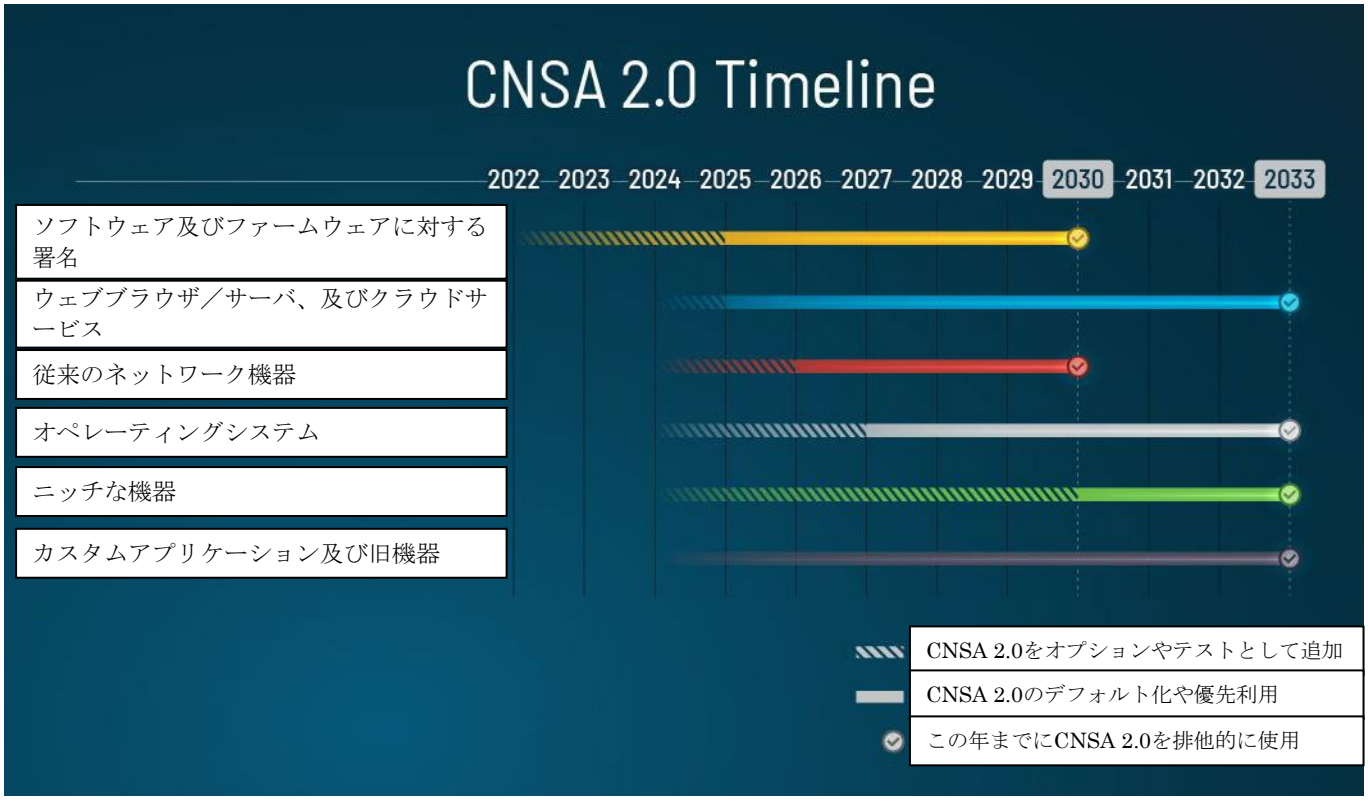


図1：移行スケジュール

施行について

NSSの所有者と運用者は、NSM-8とNSM-10の責任の一部として、CNSA 1.0とCNSA 2.0への更新の進捗を報告しなければならない。承認責任者（AOs: Approving Officials）は、セキュリティコントロール12（SC-12）

[1] 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。

を評価する際に、リスク管理フレームワーク（RMF: Risk Management Framework）プロセスの一環として準拠性を評価すべきである。さらに、承認責任者は、そのシステムのソフトウェア及びファームウェアに対する署名について、CNSA 2.0への準拠を検証する必要がある。NSSは、RMFプロセスでは「FIPS認証」に対して評価**されるべきではない**。代わりにソリューションはNSA承認されなければならない。商用製品が受け入れられるアプリケーションでは、NSAは、CNSSP 15及び他の特定の指示又はガイダンスに従って正しく構成されている限り、CNSSP 11に準拠する製品（すなわち、承認されたプロテクションプロファイルに対してNIAP認証されている製品）を一般的に承認する。

追加ガイダンスとしてのRFCについて

以下の文書は、CNSAの要件に準拠するためにソリューションを構成する方法を規定している。これらは以下の通り：

- RFC 8603 "Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile" https://datatracker.ietf.org/doc/html/rfc8603
- RFC 8755 "Using Commercial National Security Algorithm Suite Algorithms in Secure/Multipurpose Internet Mail Extensions" https://datatracker.ietf.org/doc/rfc8755/
- RFC 8756 "Commercial National Security Algorithm (CNSA) Suite Profile of Certificate Management over CMS" https://datatracker.ietf.org/doc/rfc8756/
- RFC 9151 "Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3" https://datatracker.ietf.org/doc/rfc9151/
- RFC 9206 "Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)" https://datatracker.ietf.org/doc/rfc9206/
- RFC 9212 "Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH)" https://datatracker.ietf.org/doc/rfc9212/

これらの文書は、現在CNSA 1.0に適用されている。NSAは、標準化プロセスの進行に伴い、最新のガイダンスを発表する予定である。

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

付録:参照表

以下の2つの表は、それぞれCNSA 2.0とCNSA 1.0のアルゴリズム一覧を示す。CNSA 1.0は現在の標準であり、CNSA 2.0は将来の標準である。NSAは、CNSA 2.0のソフトウェア及びファームウェアに対する署名アルゴリズムを今すぐ採用することを推奨する。

表IV: CNSA 2.0アルゴリズム

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

表V: CNSA 1.0アルゴリズム

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
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	鍵確立のための非対称アルゴリズム	NIST SP 800-56A	全ての分類レベルで曲線P-384を利用する
Elliptic Curve Digital Signature Algorithm (ECDSA)	デジタル署名のための非対称アルゴリズム	FIPS PUB 186-4	全ての分類レベルで曲線P-384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を利用する
Diffie-Hellman (DH) Key Exchange	鍵確立のための非対称アルゴリズム	IETF RFC 3526	全ての分類レベルで3072ビット以上の法サイズにする
RSA	鍵確立のための非対称アルゴリズム	FIPS SP 800-56B	全ての分類レベルで3072ビット以上の法サイズにする
RSA	デジタル署名のための非対称アルゴリズム	FIPS PUB 186-4	全ての分類レベルで3072ビット以上の法サイズにする