軽量暗号の評価指標、標準化動向に関する調査

(NIST 軽量暗号コンペティションファイナリストなど)

GMO サイバーセキュリティ by イエラエ株式会社

2022 年 12 月

エグゼクティブサマリー

本報告書では、過去に実施されていた CAESAR プロジェクトや現在評価が行われている NIST 軽量暗号コンペティション、ISO/IEC 29192 シリーズおよび CRYPTREC 暗号技術ガイドライン（軽量暗号）に対して軽量暗号に関する評価指標および標準化動向について調査・検討を実施した。

その結果として、以下のことが判明した。

- 選定アルゴリズムの側面
  - 各プロジェクト等において選定された軽量暗号アルゴリズムとして共通的なものは存在していない。
    - 各プロジェクトでターゲットとしている軽量暗号に関する技術分類（ブロック暗号、ストリーム暗号、AEAD など）が異なる点も影響しているのではないかと推測される。
  - 軽量暗号に関する各プロジェクトが様々なタイミングで実施されているので、各活動で選定されたアルゴリズム名が改良されるなどが行われている。
    - 懸念事項として、ベースとなる方式を改良した場合、名称が似通っているため同一のアルゴリズムかどうか判定しにくい状況を生み出している。
- 評価指標の側面
  - 安全性
    - 安全性評価を行う際に、アルゴリズムの考案者から設計根拠について十分な情報が出てこない場合は第三者評価が行えないと判断され、評価対象から外されるなどの事例がある
  - 性能
    - 論文等では異なる環境や測定シナリオが統一されておらず、公平な比較が実施しにくい状況となっていることが多いが、統一的な測定フレームワークなどを用いて実施することが一般化された
      - 性能評価を行う際には、AES-GCM や SHA-256 など広く世界で利用されているアルゴリズムが対象になっていた

また、本調査を行い判明したこととしては、軽量暗号を選定しているプロジェクトにおい

て選ばれた軽量暗号アルゴリズムとして共通しているものがないという結果になった。実社会での軽量暗号の利用などを想定するのであれば、ここ数年で標準化されている ISO/IEC と NIST 軽量暗号コンペティションにおいて同一の軽量暗号アルゴリズムが存在すべきであると考えられるが、異なるアルゴリズムとなっている点が興味深い。着眼点を変えると、全ての過去に選定された軽量暗号アルゴリズムは実績があると考えられるが、NIST 軽量暗号コンペティションに投稿されていない点や他プロジェクト等に投稿されたアルゴリズムを改良した方式を提案されているケースも存在している点も興味深いと言える。

目次

1. はじめに

2017 年 3 月に公開された CRYPTREC 暗号技術ガイドライン（軽量暗号）（以下、「2016 年度ガイドライン」という） [1]では、「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された共通鍵暗号技術」をスコープとし、軽量暗号の活用例、代表的な軽量暗号の性能比較、代表的な軽量暗号に関する基本情報について紹介している。しかしながら、暗号方式に対する安全性評価技術は日進月歩であり、2016 年度ガイドラインの公開から 5 年以上が経っているため、2016 年度ガイドラインには記載されていない、軽量暗号の安全性を脅かす新たな脅威が生じている可能性は十分に考えられるため、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号の安全性評価に関する動向調査を行うことを目的とし、2021 年 9 月の時点における軽量暗号に対して現実的な脅威に繋がる脆弱性が指摘されているか否かを明らかにするための報告書として「CRYPTREC 暗号技術ガイドライン（軽量暗号)」掲載の暗号方式に関する安全性評価の動向調査 [2]が公開された。

また、2019 年度量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにおいて、「CRYPTREC において、軽量暗号は CRYPTREC 暗号リストに組み込まず、別途ガイドラインという形で取り扱う」ことが決定された。この決定を踏まえて 2020 年度第 2 回暗号技術検討会において、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」について 2023 年度中を目処に更新することが承認された。そこで本報告書では、2020 年度第 2 回暗号技術検討会の承認内容を踏まえて、「NIST Lightweight コンペティション最終選考で採択された軽量暗号方式」や「軽量暗号として ISO/IEC 等で近年採録されたもしくは採録される予定の方式」に関する標準化動向について状況を整理し、今後予定されている 2023 年度の更新に向けた 2022 年度における軽量暗号方式に関する標準化動向をまとめたものである。

2. NIST 軽量暗号コンペティション

2016 年度ガイドラインの発行後、NIST*による軽量暗号コンペティション（以下、NIST 軽量暗号コンペティションとする。）[3]が開催された。この活動は軽量暗号の標準化について把握する上で重要な活動であるが、2022 年 12 月現在、Next Steps として掲載された情報のように「最終評価は 2022 年末に終了する予定である」ことが告げられていたが、選定プロセスは完了していないことを留意していただきたい。

なお、NIST 軽量暗号コンペティションの Web サイトでは、図 1 のような構成となっており、各 Round に関する情報や軽量暗号に関する Workshop に関する情報、制約のある環境下での実装性能など有益な情報へのリンクが整理されている。

* NIST の正式名称は、National Institute of Standards and Technology であり、日本語では米国立標準技術研究所と呼ばれるアメリカの政府機関である。科学技術分野における計測と標準に関する研究が行われている。
URL： https://www.nist.gov/

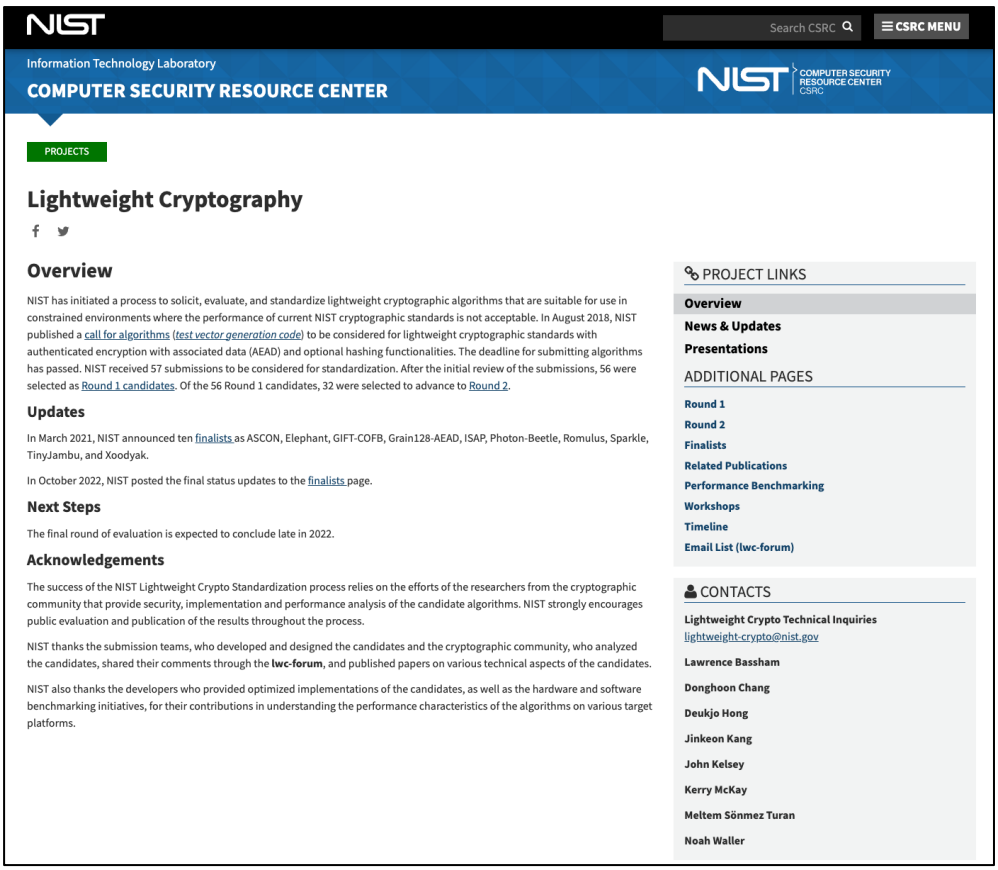

図 1　NIST 軽量暗号コンペティション

以下に、2022 年 12 月現在の NIST 軽量暗号コンペティションにおける標準化動向に関する状況を整理する。NIST 軽量暗号コンペティションでは選定プロセスにおける Round 1 から Finalist の 3 回の選定が実施されている。それぞれの選定プロセスにおいて、どのような軽量暗号アルゴリズムが提案され採択されたかについては、表 1 を参照することで全体像を把握することができるように情報整理を行なっている。

	Round1	Round2	Finalist
#	候補アルゴリズム名	候補アルゴリズム名	候補アルゴリズム名
1	ACE	ACE	ACE
2	ASCON	ASCON	ASCON
3	Bleep64	Bleep64	Bleep64
4	CiliPadi	CiliPadi	CiliPadi
5	CLAE	CLAE	CLAE
6	CLX	CLX	CLX
7	COMET	COMET	COMET
8	DryGASCON	DryGASCON	DryGASCON
9	Elephant	Elephant	Elephant
10	ESTATE	ESTATE	ESTATE
11	FlexAEAD	FlexAEAD	FlexAEAD
12	ForkAE	ForkAE	ForkAE
13	Fountain	Fountain	Fountain
14	GAGE and InGAGE	GAGE and InGAGE	GAGE and InGAGE
15	GIFT-COFB	GIFT-COFB	GIFT-COFB
16	Gimli	Gimli	Gimli
17	Grain-128AEAD	Grain-128AEAD	Grain-128AEAD
18	HERN & HERON	HERN & HERON	HERN & HERON
19	HYENA	HyENA	HyENA
20	ISAP	ISAP	ISAP
21	KNOT	KNOT	KNOT
22	LAEM	LAEM	LAEM
23	Lilliput-AE	Lilliput-AE	Lilliput-AE
24	Limdolen	Limdolen	Limdolen
25	LOTUS-AEAD and LOCUS-AEAD	LOTUS-AEAD and LOCUS-AEAD	LOTUS-AEAD and LOCUS-AEAD
26	mixFeed	mixFeed	mixFeed
27	ORANGE	ORANGE	ORANGE
28	Oribatida	Oribatida	Oribatida
29	PHOTON-Beetle	PHOTON-Beetle	PHOTON-Beetle
30	Pyjamask	Pyjamask	Pyjamask
31	Qameleon	Qameleon	Qameleon
32	Quartet	Quartet	Quartet
33	REMUS	REMUS	REMUS
34	Romulus	Romulus	Romulus
35	SAEAES	SAEAES	SAEAES
36	Saturnin	Saturnin	Saturnin
37	Shamash & Shamashash	Shamash & Shamashash	Shamash & Shamashash
38	SIMPLE	SIMPLE	SIMPLE
39	SIV-Rijndael256	SIV-Rijndael256	SIV-Rijndael256
40	SIV-TEM-PHOTON	SIV-TEM-PHOTON	SIV-TEM-PHOTON
41	SKINNY-AEAD/SKINNY-HASH	SKINNY-AEAD/SKINNY-HASH	SKINNY-AEAD/SKINNY-HASH
42	SNEIK	SNEIK	SNEIK
43	SPARKLE (SCHWAEMM and ESCH)	SPARKLE (SCHWAEMM and ESCH)	SPARKLE (SCHWAEMM and ESCH)
44	SPIX	SPIX	SPIX
45	SpoC	SpoC	SpoC
46	Spook	Spook	Spook
47	Subterranean 2.0	Subterranean 2.0	Subterranean 2.0
48	SUNDAE-GIFT	SUNDAE-GIFT	SUNDAE-GIFT
49	Sycon	Sycon	Sycon
50	Thank Goodness It's Friday (TGIF)	Thank Goodness It's Friday (TGIF)	Thank Goodness It's Friday (TGIF)
51	TinyJambu	TinyJambu	TinyJambu
52	Triad	Triad	Triad
53	TRIFLE	TRIFLE	TRIFLE
54	WAGE	WAGE	WAGE
55	Xoodyak	Xoodyak	Xoodyak
56	Yarará and Coral	Yarará and Coral	Yarará and Coral

表 1　NIST 軽量暗号コンペティション選定アルゴリズム

【Round 1】

2019 年 3 月に NIST は、NIST 軽量暗号コンペティションの Round 1 として、57 件の提出物を受け取り、“Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process”[4]で示した要件に基づき完全性と妥当性の観点から提出された軽量暗号アルゴリズムから Round 1 の候補アルゴリズムとして 56 個のアルゴリズム選定を 2019 年 4 月に行い、2019 年 8 月に Round 1 を終了した。

なお、Round 1 に関する詳細なステータスについては、“Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process”[5]を参照してほしい。

なお、Round 1 で使用された評価基準は[5]において要約されているので、概要について整理を行う。この Round での評価基準として最重要なものは、「提出された暗号アルゴリズムの安全性」と言える。軽量暗号であることを評価するために制約のある環境下での実装特性（性能とコスト）も重要な基準となっていたことがわかる。また、実装での安全性の観点からは、サイドチャネル攻撃への対策に適しているかどうかについても評価されていた。

【Round2】

NIST 軽量暗号コンペティションの Round2 は、NIST が 2019 年 8 月に 32 個の候補アルゴリズムを発表し、2021 年 3 月に Finalist を公表したことで Round2 が終了した。なお、Round2 における選定に関する詳細なステータスについては、“Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process”[6]を参照してほしい。

[6]において Round2 で使用された評価基準が要約されているので、概要について整理を行う。この Round での評価基準は、前回の Round 1 と同様の評価観点である「第三者による分析や広く理解された設計原理と安全性証明に基づく主張」および「制約のあるデバイスを用いたアプリケーションにおける候補アルゴリズムの性能（制約のある環境における候補アルゴリズムのハードウェアおよびソフトウェアの性能)」というものであり、Round を経ることにより評価基準が詳細化されたという理解をした。なお、Round 1 と同様に候補アルゴリズムのサイドチャネル耐性についても評価基準となっていた。

【Finalist】

NIST 軽量暗号コンペティションの Finalist として、2021 年 3 月に Round2 での評価を踏まえて ASCON、Elephant、GIFT-COFB、Grain-128AEAD、ISAP、PHOTON-Beetle、Romulus、SPARKLE、TinyJAMBU、および Xoodyak の 10 つのアルゴリズムを選定した。なお、前述の通り、Finalist として選定された候補アルゴリズムに対する評価

については 2022 年 12 月現在において完了していないという状況であることを再度共有する。

各 Round での候補アルゴリズムが選定されなかった理由については、NIST が公開している Status Report において示されているが、次の Round への選定に残らなかった理由について概要を整理する。

【Round 1】

- 第三者による安全性に対する評価が公開されていないことや提出資料において、安全性の主張を裏付ける情報が不十分である提案については除外された。
- 第三者評価によって、Forgery Attacks、Length-extension Attacks や Distinguishing Attacks が存在する方式が整理された。
  - なお、指摘された懸念を払拭するために設計者が提案した修正は、評価時には考慮されなかったが、実装のバグによる実用的な攻撃（例えば、Forgery Attacks）は排除の理由とはされなかった。NIST の研究者は実装の更新をチェックし、元の仕様と整合性が取れているかを確認した。

【Round 2】

- Round 1 と同様に第三者による安全性評価が行われていることや安全性の主張を裏付ける情報が十分に情報公開されていること。
- 制約のあるデバイスを使用するアプリケーションにおける性能（制約のある環境におけるハードウェアおよびソフトウェアでの性能）がよいこと。
  - さまざまな性能とコストの指標で評価・比較され、現在の NIST 標準（特に AES-GCM [7]と SHA-2 [8]）より著しく性能がよいものが選定時に優遇されていた。
- 追加検討事項として、以下の項目について評価されている。
  - Side-Channel Resistance、Nonce-Misuse Security、RUP Security、Impacts of State Recovery および Post-Quantum Security

3. 2016 年度ガイドラインに掲載されている暗号方式に関わる標準化動向

2016 年度ガイドラインで紹介されている軽量暗号方式は、ブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証コードおよび認証暗号の技術分野別に整理されている。選定基準の詳細については 2016 年度ガイドラインを参照することとするが、「執筆時点までに、主要国際学会等で発表されており、有力な攻撃法が発見されておらず、かつ十分な実装性能を持ち、リソースの限られた実装条件下で有用と考えられるアルゴリズムを選んでいる」と基準が示されており、暗号方式として最も重要である安全であることと軽量暗号方式として重要であるリソースの限られた環境での性能という側面で評価・選定されていることがわかる。以下に、2016 年度ガイドラインで選定された軽量暗号アルゴリズムリストを示す。(表 2)

ブロック暗号	CLEFIA, LED, Midori, Piccolo、PRESENT, PRINCE, SIMON, SPECK, TWINE
ストリーム暗号	ChaCha20, Enocoro, Grain v1, MICKEY 2.0, Trivium
ハッシュ関数	Keccak, PHOTON, QUARK, SPONGENT
メッセージ認証コード	SipHash
認証暗号	ACORN, Ascon, AES-JAMBU, AES-OTR, CLOC and SILC, Deoxys, Joltik, Ketje, Minalpher, OCB, PRIMATEs

表 2 2016 年度軽量暗号ガイドライン アルゴリズム一覧

また、表 2 で示した 2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムについて、NIST 軽量暗号コンペティションで選定された暗号アルゴリズムとの関係および標準化動向について調査した結果を整理する。

3.1. NIST 軽量暗号コンペティションで選定された暗号アルゴリズムとの関係

2016 年度ガイドラインでブロック暗号に分類されている 9 つの暗号アルゴリズムとの比較については表 3 で示したとおりである。結果としては、2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムは NIST 軽量暗号コンペティションで選定されたものはないという結果となった。

項番	2016年度軽量暗号ガイドラインアルゴリズム	NIST軽量暗号コンペティションとの関係
1	CLEFIA	X
2	LED	X
3	Midori	X
4	Piccolo	X
5	PRESENT	X
6	PRINCE	X
7	SIMON	X
8	SPECK	X
9	TWINE	X

表 3　2016 年度軽量暗号ガイドラインおよび NIST 軽量暗号コンペティション比較（ブロック暗号）

2016 年度ガイドラインでストリーム暗号に分類されている 5 つの暗号アルゴリズムとの比較については表 4 で示したとおりである。結果としては、2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムは NIST 軽量暗号コンペティションで選定されたものはないという結果となった。

項番	2016年度軽量暗号ガイドラインアルゴリズム	NIST軽量暗号コンペティションとの関係
1	ChaCha20	X
2	Enocoro	X
3	Grain v1	X
4	MICKEY 2.0	X
5	Trivium	X

表 4　2016 年度軽量暗号ガイドラインおよび NIST 軽量暗号コンペティション比較（ストリーム暗号）

2016 年度ガイドラインでハッシュ関数に分類されている 4 つのハッシュアルゴリズムとの比較については表 5 で示したとおりである。結果としては、2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムは NIST 軽量暗号コンペティションで選定されたものはないという結果となった。

項番	2016年度軽量暗号ガイドラインアルゴリズム	NIST軽量暗号コンペティションとの関係
1	Keccak	X
2	PHOTON	X
3	QUARK	X
4	SPONGENT	X

表 5　2016 年度軽量暗号ガイドラインおよび NIST 軽量暗号コンペティション比較（ハッシュ関数）

2016 年度ガイドラインでメッセージ認証コードに分類されている 1 つのメッセージ認証コードアルゴリズムとの比較については表 6 で示したとおりである。結果としては、2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムは NIST 軽量暗号コンペティションで選定されたものはないという結果となった。

項番	2016年度軽量暗号ガイドラインアルゴリズム	NIST軽量暗号コンペティションとの関係
1	SipHash	X

表 6　2016 年度軽量暗号ガイドラインおよび NIST 軽量暗号コンペティション比較（メッセージ認証コード）

2016 年度ガイドラインで認証暗号に分類されている 11 つの認証暗号アルゴリズムとの比較については表 7 で示したとおりである。結果としては、2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムは NIST 軽量暗号コンペティションで選定された ASCON および TinyJAMBU が該当するという結果となった。

項番	2016年度軽量暗号ガイドラインアルゴリズム	NIST軽量暗号コンペティションとの関係
1	ACORN	X
2	Ascon	Round1, Round2, Finalist
3	AES-JAMBU	Round1, Round2, Finalist ※ TinyJAMBU
4	AES-OTR	X
5	CLOC and SILC	X
6	Deoxys	X
7	Joltik	X
8	Ketje	X
9	Minalpher	X
10	OCB	X
11	PRIMATEs	X

表 7　2016 年度軽量暗号ガイドラインおよび NIST 軽量暗号コンペティション比較（認証暗号）

この比較結果を考察する前に、NIST 軽量暗号コンペティションとして公募対象[†]がどのようなものだったかを振り返ると、「AEAD (authenticated encryption with associated data)およびオプションとしてのハッシュ機能を備えた軽量暗号」となっている。これは 2016 年度ガイドラインで紹介されている軽量暗号方式が「ブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証コードおよび認証暗号」の技術分野別となっているので、両方に共通している技術分野が「ハッシュ関数」と「認証暗号」であることに依存していると考えられる。そのため、2016 年度ガイドラインで紹介されていた軽量暗号方式としては認証暗号の

[†] NIST 軽量暗号コンペティションの Web サイトに以下のような記述があるので注意が必要となる。
“NIST has initiated a process to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable for use in constrained environments where the performance of current NIST cryptographic standards is not acceptable. **In August 2018, NIST published a call for algorithms (test vector generation code) to be considered for lightweight cryptographic standards with authenticated encryption with associated data (AEAD) and optional hashing functionalities.**”

分類において ASCON と AES-JAMBU‡ のみという結果になった。

3.2. 2016 年度軽量暗号ガイドラインで選定された暗号アルゴリズムの標準化動向

2016 年度軽量暗号ガイドラインで選定されたアルゴリズムの標準化動向として、NIST 軽量暗号コンペティション以外での標準化動向について調査を行い、その結果を表 8 として示す。なお、調査方法としては、各アルゴリズム名に対して「lightweight crypto standard」のキーワードを追加して検索エンジンにより検索を行った結果であることを注意すること。

‡ 厳密には、下記資料の Chapter2 において“The TinyJAMBU mode is a small variant of the JAMBU mode which is a third-round candidate of the CAESAR competition.” として紹介されているので、同一のアルゴリズムではない。
URL: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf

#	アルゴリズム名	標準化動向
1	CLEFIA	・ISO/IEC 29192-2, Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers ・RFC6114 " The 128-Bit Blockcipher CLEFIA"
2	LED	—
3	Midori	—
4	Piccolo	—
5	PRESENT	・ISO/IEC 29192-2, Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers
6	PRINCE	—
7	SIMON	・ISO/IEC 29167-21:2018(en) Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications
8	SPECK	・ISO/IEC 29167-22:2018(en) Information technology — Automatic identification and data capture techniques — Part 22: Crypto suite SPECK security services for air interface communications
9	TWINE	—
10	ChaCha20	・RFC7539 "ChaCha20 and Poly1305 for IETF Protocols"
11	Enocoro	・ISO/IEC 29192-3:2012 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers
12	Grain v1	—
13	MICKEY 2.0	—
14	Trivium	・ISO/IEC 29192-3:2012 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers
15	Keccak	
16	PHOTON	・ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions
17	QUARK	—
18	SPONGENT	・ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions
19	SipHash	—
20	ACORN	—
21	Ascon	—
22	AES-JAMBU (TinyJambu)	—
23	AES-OTR	—
24	CLOC and SILC	—
25	Deoxys	—
26	Joltik	—
27	Ketje	—
28	Minalpher	—
29	OCB	・RFC 7253 "The OCB Authenticated-Encryption Algorithm"（ここでのOCBはOCB3のことである）
30	PRIMATEs	—

表 8　2016 年度軽量暗号ガイドラインで選定されたアルゴリズムの標準化動向

表 8 の標準化動向調査結果を踏まえると、2016 年度軽量暗号ガイドラインで選定されたアルゴリズムで標準化されたアルゴリズムは 30 個中 9 個であり、そのほとんどは、ISO/IEC で標準化されているということがわかった。なお、今回の調査では、2016 年度軽量暗号ガイドラインが作成された当時のアルゴリズムに対して標準化を行っているかどうかの調査を行なっており、そのアルゴリズムをベースとした改良方式の標準化までは行っていない

ことに注意する。例えば、Grain v1 をベースとしている Grain 128A は ISO/IEC 29167-13 にて標準化が行われている。

また、項番 8 および 9 にある SIMON と SPECK は、軽量暗号方式として ISO/IEC の標準化仕様になっていないが、自動認識・データキャプチャ技術に関する仕様で利用可能な軽量暗号方式として採択されていることも要注意である。

4. その他、軽量暗号選定に関するプロジェクト

NIST 軽量暗号コンペティションや 2016 年度軽量暗号ガイドライン以外にも、CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) [7] や FELICS (Fair Evaluation of Lightweight Cryptographic Systems) [8]というプロジェクトが存在している。ここでは、それぞれのプロジェクトについて、どのような評価指標や観点に基づいていたのか、また、プロジェクトとしてアルゴリズムを選定しているようであれば、暗号アルゴリズムについても整理を行う。

4.1. CAESAR

CAESAR プロジェクトは、認証暗号方式の設計を促進するための国際的な暗号研究者グループによって組織されたコンペティションである。なお、CAESAR は、2013 年 1 月に開催された Early Symmetric Crypto workshop でコンペティションが発表され、2019 年 2 月に最終ポートフォリオが発表された。詳細なタイムラインについては以下のとおりである。（図 2）

Timeline

- M-20, 2012.07.05–06: DIAC: Directions in Authenticated Ciphers. Stockholm.
- M-14, 2013.01.15: Competition announced at the Early Symmetric Crypto workshop in Mondorf-les-Bains; also announced online.
- M-7, 2013.08.11–13: DIAC 2013: Directions in Authenticated Ciphers 2013. Chicago.
- M0, 2014.03.15: Deadline for first-round submissions.
- M2, 2014.05.15: Deadline for first-round software.
- M5, 2014.08.23–24: DIAC 2014: Directions in Authenticated Ciphers 2014. Santa Barbara.
- M16, 2015.07.07: Announcement of second-round candidates.
- M17, 2015.08.29: Deadline for second-round tweaks.
- M18, 2015.09.15: Deadline for second-round software.
- M18, 2015.09.28–29: DIAC 2015: Directions in Authenticated Ciphers 2015. Singapore.
- M27, 2016.06.30: Deadline for Verilog/VHDL.
- M29, 2016.08.15: Announcement of third-round candidates.
- M30, 2016.09.15: Deadline for third-round tweaks.
- M30, 2016.09.26–27: DIAC 2016. Nagoya, Japan.
- M31, 2016.10.15: Deadline for third-round software.
- M40, 2017.07.15: Deadline for third-round Verilog/VHDL.
- M40, 2017.07.15: Deadline for optimized third-round software.
- M48, 2018.03.05: Announcement of finalists.
- M59: 2019.02.20: Announcement of final portfolio.

図 2　CAESAR プロジェクト（タイムライン）

最終的なポートフォリオとしては、ユースケース 1: 軽量アプリケーション（リソースに制約のある環境)、ユースケース 2: 高性能アプリケーション、ユースケース 3: 多層防御の 3 つで構成されていおり、今回の調査において対象となっているユースケース 1 において、第一候補として ASCON、第二候補として ACORN が採択されている。([9])

また、CAESAR プロジェクトにおいて評価基準が明確に示されてはいないが、AES-GCM よりも優れた利点を有し、幅広い領域で採用される認証暗号を選択することを目的[§]としている。また、ソフトウェアおよびハードウェアでの高性能を有することについて同一フレームワークを用いて測定できるような仕組み[**]を導入している。

4.2.　FELICS

FELICS は、組み込み機器向けの軽量暗号プリミティブのソフトウェア実装を公正かつ一貫して評価するために設計された、フリーでオープンソースのベンチマークフレームワークである。このフレームワークは、モジュール構造により、新しい評価基準、対象デバイス、

---

§　“CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) will identify a portfolio of authenticated ciphers that (1) offer advantages over AES-GCM and (2) are suitable for widespread adoption. Cryptographic algorithm designers are invited to submit proposals of authenticated ciphers to CAESAR. All proposals will be made public for evaluation.”

URL: https://competitions.cr.yp.to/caesar-call.html

**　“See https://bench.cr.yp.to/supercop.html for software implementations, and https://cryptography.gmu.edu/athena/index.php?id=CAESAR_source_codes for VHDL implementations.”

URL: https://competitions.cr.yp.to/caesar-submissions.html

評価シナリオを容易に統合することができ、非常に柔軟性がある。また、広く利用されている 3 つのマイコン（8-bit AVR、16-bit MSP および 32-bit ARM）で軽量暗号とストリーム暗号の性能を評価することができる 2 つのモジュールで構成されている。評価指標は、実行時間、RAM 消費量、バイナリコードサイズの 3 つとなっている。このフレームワークは暗号設計者が新しいプリミティブを公平に比較することを想定している。また、抽出された指標は組み込みエンジニアが特定のアプリケーションの要件に適する最適な暗号アルゴリズムを選択にも役立つとされている。

なお、このプロジェクトにおいては、軽量暗号を公平に評価するためのフレームワークであるため、特定の暗号アルゴリズムを選定するようなものではないと言える。

5. 軽量暗号アルゴリズムに関する評価指標および標準化動向に関する考察

これまでの調査結果を踏まえて軽量暗号アルゴリズムに関する評価指標および標準化動向について整理を行い、その整理結果を踏まえた考察を行う。

5.1. 軽量暗号アルゴリズムに関する評価指標

本調査において 2016 年度ガイドラインや NIST 軽量暗号コンペティション、CAESAR プロジェクトや FELICS などで軽量暗号を評価や選定を行う際の観点としては、安全性および実装性能であると想定される。

- 安全性に関する考え方
  - 第三者が評価対象のアルゴリズムに関する設計根拠などの情報が十分に提供されているか
  - 第三者が安全性評価を十分に行っているか
  - サイドチャネル攻撃に対する検討は行われているか
- 実装性能に関する考え方
  - 制約のある環境での性能
    - 実行時間、RAM 消費量、バイナリコードサイズ
  - ソフトウェアおよびハードウェアでの性能
  - 異なる動作環境ではなく同一の環境および評価シナリオでの公平な評価観点

安全性に関する考え方にある「第三者が評価対象のアルゴリズムに関する設計根拠などの情報が十分に提供されているか」については、NSA により提案された軽量暗号である SIMON と SPECK に関連する ISO/IEC での標準化活動の事例がある。この事例については、”An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families” [10]において詳しく時系列で標準化プロセス毎に情報が記されている。

5.2. 軽量暗号アルゴリズムに関する標準化動向

ここまで 2016 年度ガイドラインや NIST 軽量暗号コンペティションなどで選定された軽量暗号アルゴリズムを確認したが、ISO/IEC における軽量暗号関連の文書シリーズおよび共通鍵暗号関連に関する軽量暗号アルゴリズムについて、表 9 および表 10 として整理を行う。

#	タイトル
1	ISO/IEC 29192-1:2012 Information technology — Security techniques — Lightweight cryptography — Part 1: General
2	ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers
3	ISO/IEC 29192-3:2012 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers
4	ISO/IEC 29192-4:2013 Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques
5	ISO/IEC 29192-4:2013/Amd 1:2016 Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques — Amendment 1
6	ISO/IEC 29192-5:2016 Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions
7	ISO/IEC 29192-6:2019 Information technology — Lightweight cryptography — Part 6: Message authentication codes (MACs)
8	ISO/IEC 29192-7:2019 Information security — Lightweight cryptography — Part 7: Broadcast authentication protocols
9	ISO/IEC 29192-8:2022 Information security — Lightweight cryptography — Part 8: Authenticated encryption

表 9　ISO/IEC における軽量暗号関連文書

#	種別	アルゴリズム名
1	ブロック暗号	PRESENT
2		CLEFIA
3		LEA
4	ストリーム暗号	Enocoro
5		Trivium
6	ハッシュ関数	PHOTON
7		SPONGENT
8		Lesamnta-LW
9	メッセージ認証コード	LightMAC
10		Tsudik's keymode
11		Chaskey-12
12	認証暗号	Grain-128A

表 10　ISO/IEC 29192 シリーズにおける軽量暗号

これまでの調査結果を踏まえると、報告書の執筆をしている 2022 年 12 月現在で評価継続されている NIST 軽量暗号コンペティションで Finalist として残っている軽量暗号アルゴリズムと過去に検討が行われた 2016 年度ガイドラインや CAESAR プロジェクト、ISO/IEC 29129 シリーズの軽量暗号アルゴリズムを比較すると、選定アルゴリズムの品揃えにおいてあまり重複していない結果であることが判明した。この結果として考えられることとしては、2016 年度ガイドラインや CAESAR プロジェクトで選定されたアルゴリズムは、数年の月日の経過に伴う技術革新や新たな攻撃方法の考案によりアルゴリズムが入れ替わったものと考えられる。その事例としては、当時選定されていたアルゴリズムをベースに改良を行った軽量暗号アルゴリズムが NIST 軽量暗号コンペティションへの投稿されていることからも想定されると考える。また、推測になるが軽量暗号が置かれている技術領域における研究開発の進歩や制約条件のある動作環境などに関する考え方が、より明確になることで 2013 年当時に想定されていた状況と大きく異なることが発生している可能性はあるのではないかと考える。

軽量暗号アルゴリズムを標準化している団体において、選定されているアルゴリズムが異なっている点（例：ASCON、Trivium など）についても興味深い。

6. まとめ

本報告書では、過去に実施されていた CAESAR プロジェクトや現在評価が行われている NIST 軽量暗号コンペティション、ISO/IEC 29192 シリーズおよび CRYPTREC 暗号技術ガイドライン（軽量暗号）に対して軽量暗号に関する評価指標および標準化動向について調査・検討を実施した。

その結果として、以下のことが判明した。

- 選定アルゴリズムの側面
  - 各プロジェクト等において選定された軽量暗号アルゴリズムとして共通的なものは存在していない。
    - 各プロジェクトでターゲットとしている軽量暗号に関する技術分類（ブロック暗号、ストリーム暗号、AEAD など）が異なる点も影響しているのではないかと推測される。
  - 軽量暗号に関する各プロジェクトが様々なタイミングで実施されているので、各活動で選定されたアルゴリズム名が改良されるなどが行われている。
    - 懸念事項として、ベースとなる方式を改良した場合、名称が似通っているため同一のアルゴリズムかどうか判定しにくい状況を生み出している。
- 評価指標の側面
  - 安全性
    - 安全性評価を行う際に、アルゴリズムの考案者から設計根拠について十分な情報が出てこない場合は第三者評価が行えないと判断され、評価対象から外されるなどの事例がある
  - 性能
    - 論文等では異なる環境や測定シナリオが統一されておらず、公平な比較が実施しにくい状況となっていることが多いが、統一的な測定フレームワークなどを用いて実施することが一般化された
      - 性能評価を行う際には、AES-GCM や SHA-256 など広く世界で利用されているアルゴリズムが対象になっていた

また、本調査を行い判明したこととしては、軽量暗号を選定しているプロジェクトにおいて選ばれた軽量暗号アルゴリズムとして共通しているものがないという結果になった。実社会での軽量暗号の利用などを想定するのであれば、ここ数年で標準化されている ISO/IEC と NIST 軽量暗号コンペティションにおいて同一の軽量暗号アルゴリズムが存在すべきであると考えられるが、異なるアルゴリズムとなっている点が興味深い。着眼点を変えると、全ての過去に選定された軽量暗号アルゴリズムは実績があると考えられるが、NIST 軽量暗号コンペティションに投稿されていない点や他プロジェクト等に投稿されたアルゴリズムを改良した方式を提案されているケースも存在している点も興味深いと言える。

参考文献

[1] CRYPTREC 軽量暗号ワーキンググループ, “CRYPTREC 暗号技術ガイドライン（軽量暗号),” 3 2017., https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf.

[2] 伊藤竜馬, “「CRYPTREC 暗号技術ガイドライン（軽量暗号)」掲載の暗号方式に関する安全性評価の動向調査,” 2021., https://www.cryptrec.go.jp/exreport/cryptrec-ex-3101-2021.pdf.

[3] National Institute of Standards and Technology, “ Lightweight Cryptography,”, https://csrc.nist.gov/projects/lightweight-cryptography.

[4] NIST, “ Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process,” NIST.

[5] K. M. Ç. Ç. D. C. ,. L. B. Meltem Sönmez Turan, “Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process,” 10 2019., https://csrc.nist.gov/publications/detail

/nistir/8268/final.

[6] NIST, "Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process," NIST, 2021.

[7] M. Dworkin, "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," 11 2007., https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

[8] National Institute of Standards and Technology, "FIPS PUB 180-4 Secure Hash Standard (SHS)," 2015., https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[9] "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness,", https://competitions.cr.yp.to/caesar.html.

[10] "FELICS - Fair Evaluation of Lightweight Cryptographic Systems,", https://www.cryptolux.org/index.php/FELICS.

[11] “CAESAR submissions,”, https://competitions.cr.yp.to/caesar-submissions.html.

[12] T. A. &. A. Luykx, An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families, Springer.