Vol.2019-MBL-92 No.22
Vol.2019-CDS-26 No.22
2019/8/30

SROS2における認証付き暗号の実装とパフォーマンス評価

竹本 修[1,a)]　野崎 佑典[2]　吉川 雅弥[2]

概要：Industry 4.0 の拡大に伴い，複雑化した FA システムの短期開発及びセキュアシステムの実現が求められている．産業用ロボット等に適用可能なオープンソースのプラットフォームである SROS2 は，短期開発をサポートし，AES-GCM によるセキュアな通信を保障している．一方で，AES-GCM は計算量的安全性において脆弱性が報告されており，新たに代わるセキュアな認証付き暗号とその評価が必要である．そこで，AES-GCM に代わる認証付き暗号のコンペティション CAESAR が実施され，最終ポートフォリオが決定した．本研究では，CAESAR の認証付き暗号を SROS2 に組み込むことを目的に，セキュアな SROS2 のオーバーヘッドを調査する．そして，パフォーマンス評価によって，実システムに適用可能かどうかの方針を示す．

キーワード：SROS2，認証暗号，AES-GCM，CAESAR

Implementation and Performance Evaluation of Authenticated Cryptography in SROS2

Takemoto Shu[1,a)]　Nozaki Yusuke[2]　Yoshikawa Masaya[2]

Abstract: With the expansion of Industry 4.0, realization of a short-term development of a complex FA system and a secure system is required. SROS2, an open source platform applicable to industrial robots, realizes short-term development and implements secure communication using AES-GCM. On the other hand, AES-GCM is reported to be vulnerable in computational security. Therefore, a secure encryption alternative to AES-GCM and its evaluation are needed. For these reasons, this research incorporates SROS2 with a secure certified encryption alternative to AES-GCM. This study also evaluates the performance of cryptography.

Keywords: SROS2, Authenticated cryptography, AES-GCM, CAESAR

1. はじめに

Industry 4.0 の拡大 [1] に伴い，IoT や AI が積極的にシステムに組み込まれるようになり，産業用ロボットを含む FA システムは複雑化している．また，IoT 化や産業用ロボットの遠隔操作，配線などの空間的な問題によって，従来の有線通信から無線通信へ移行 [2] し，サイバーセキュリティも重要視されるようになってきた．そのため，複雑化した FA システムの短期開発及びセキュアシステムの実現が求められている．産業用ロボット等に適用可能なオープンソースのプラットフォームである SROS2[3] は，短期開発をサポートし，AES-GCM[4], [5] によるセキュアな通信を保障している．一方で，AES-GCM は計算量的安全性において脆弱性が報告されており [6]，新たに代わるセキュアな認証付き暗号とその評価が必要である．そこで，AES-GCM に代わる認証付き暗号のコンペティション CAESAR[16] が実施され，最終ポートフォリオが決定した．SROS2 の様々なパフォーマンス評価は行われているが [7], [8], [9], [10], [11]，他の認証付き暗号への実装を見据えたパフォーマンス評価は筆者の知る限りでは行われていない．そこで本研究では，CAESAR の認証付き暗号を

[1] 名城大学大学院
Graduate School of Meijo University, Nagoya, Aichi 478–8502, Japan
[2] 名城大学
Meijo University, Nagoya, Aichi 478–8502, Japan
[a)] 193426008@ccmailg.meijo-u.ac.jp

SROS2 に実装することを目的に，実システムで問題なく動作可能かどうかパフォーマンス評価を行う．

2. SROS2

Robot Operating System (ROS) [12] はロボット開発を短期化するために開発されたオープンソースのミドルウェアである．Ubuntu Linux 上で動作し，ロボット開発における様々なライラブリやツールが用意されている．また ROS は，リアルタイム性を向上させセキュアな通信を実現するために SROS2/ROS2[3] がリリースされている．ROS2 は C++もしくは Python によって記述されるユーザアプリケーションと ROS Client Library (rcl)，ROS Interface Description Language (rosidl)，ROSMiddleware Interface (rmw)，複数の Data Distribution Service (DDS) の仕組みによって構成される（図 1）．DDS はいくつかの製品が提供されており，PrismTech の OpenSplice や eProsima の FastRTPS[13] がある．DDS はさらに，Distributed Network，Real-Time Publish/Subscribe (RTPS) Protocol，Quality of Service Policy (QoS) の仕組みを持ち，その上で各ノードがデータのやり取りを行っている．DDS のうち，DDS-Security[14]（図 2）には AES-GCM 及び AES-GMAC を用いたセキュリティ機能があり，暗号化，認証，アクセス制御，ロギングができる．暗号化及び認証は OpenSSL[15] の技術を利用して実装が行われており，図 1 の右上に示す Global Data Space に対するデータの読み書きごとに暗号化が行われている．

3. 認証付き暗号

3.1 AES-GCM

Advanced Encryotion Standard (AES) はブロック長 128-bit，鍵長 128–256bit の共通鍵暗号アルゴリズムである．AES のラウンド関数では，ラウンド鍵との加算処理，S-box を用いた置換処理，State の列ごとに演算を行う転置処理が含まれる．AES を含む暗号アルゴリズムはそのまま平文と暗号文の入出力を実装するのではなく，入力データの演算順序や暗号化前後の演算など，決められたいくつかのブロック暗号の利用モードを選択する．そのうちの一つが Galois/Counter Mode (GCM) [4], [5] である．GCM は暗号化処理だけでなく，認証機能も同時に実現できる．AES-GCM のアルゴリズムを図 3 に示す．AES-GCM ではまず，暗号化処理かつ認証を行う平文データ P と，暗号化は行わない認証データ A を 128-bit ごとのブロックに分解する．ビット数が足りない場合，0 でパディングする．また，128-bit の秘密鍵 K を暗号化し，128-bit のハッシュ値 H を生成する．初期ベクトル IV は，パディングまたはハッシュ関数 GHASH によって 128-bit のカウンタ値 Y_n を生成する．そして，128-bit の平文 $P_{\{1,2,\ldots,n\}}$ を，インクリメントしたカウント値に対して秘密鍵を用いて暗号化したものと排他的論理和演算を行うことで，暗号文 C_n とする．次に，認証データ $A_{\{1,2,\ldots,m\}}$ とハッシュ値を用いてハッシュ関数を計算，認証子を得る．最後に，認証子と暗号文を用いてハッシュ関数を計算，タグを得る．一方で，AES-GCM は認証付き暗号のデファクトスタンダードとして利用されているが，脆弱性も報告されている [6]．

3.2 CAESAR

脆弱性のある AES-GCM に代わる認証付き暗号のコンペティション CAESAR が実施され，いくつかの選考ラウンドの後，最終ポートフォリオが決定した．最終ポートフォリオでは，暗号アルゴリズムを目的ごとに最適な実装となるよう 3 種類に分け，その中で第 1 候補及び第 2 候補の暗号アルゴリズムが推薦されている．具体的には，リソースに制約があるような軽量アプリケーション，リソースの制約はない高性能アプリケーション，セキュリティを最重要視するアプリケーションの 3 種類である．これを表 1 に示す．

3.2.1 Ascon

Ascon-128a はブロック長 128-bit，鍵長 128-bit の認証付き暗号である．また，Ascon-128 の実装タイプではブロッ

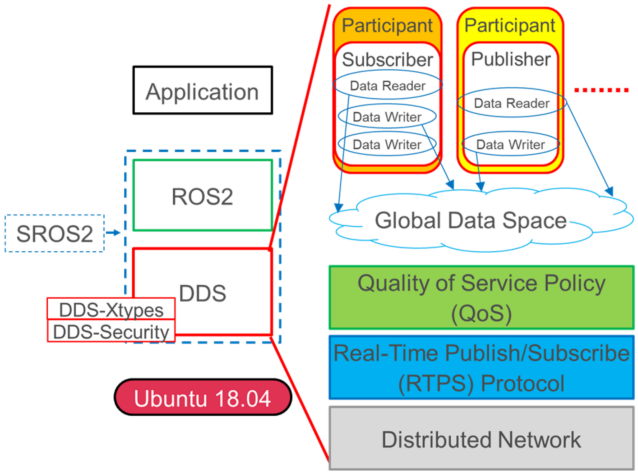

図 1 ROS2 の構造と DDS-Security

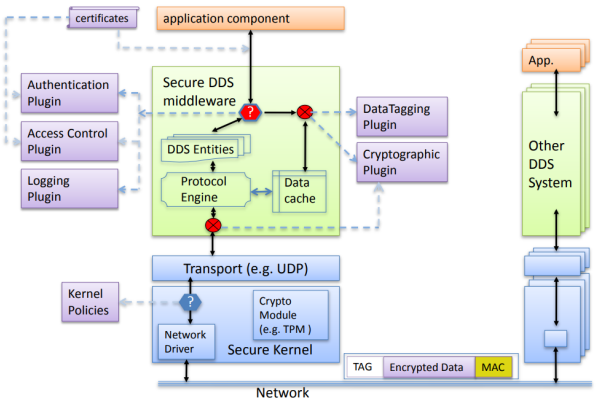

図 2 DDS-Security の詳細 2

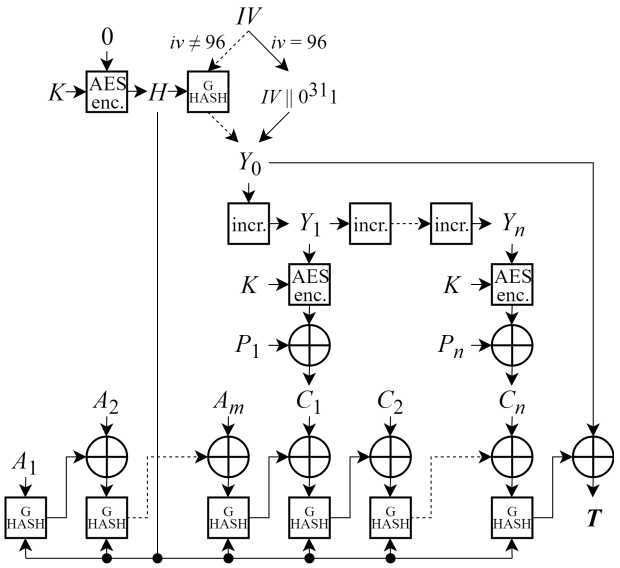

図 3 AES-GCM の暗号化・認証アルゴリズム

ク長が 64-bit となる．CAESAR コンペティションでは，最も軽量アプリケーションに特化したアルゴリズムとして評価されている．Ascon-128a のアルゴリズムを図 4 に示す．Ascon では，初期ベクトル，秘密鍵，ナンスを結合し，360-bit の State として演算を行う．複数回実行されるラウンド関数は全て共通で，初期化で 1 回，認証に s 回，暗号化に t-1 回，最終処理で 1 回実行される．具体的に，定数の加算処理，S-box による置換処理，線形拡散処理がある．

3.2.2 AEGIS

AEGIS-128 はブロック長 128-bit，鍵長 128-bit の認証付き暗号である．また，AEGIG-128L では，ブロック長や鍵長は変わらないが，演算時の State の大きさが変化する．CAESAR コンペティションでは，最も高性能アプリケーションに特化したアルゴリズムとして評価されている．AEGIS-128 のアルゴリズムを図 5 に示す．AEGIG-128 で

表 1 CAESAR の認証付き暗号

use case	1st choise	2nd choise
lightweight	Ascon	ACORN
high-performance	AEGIS-128, OCB	
defense in depth	Deoxys-II	COLM

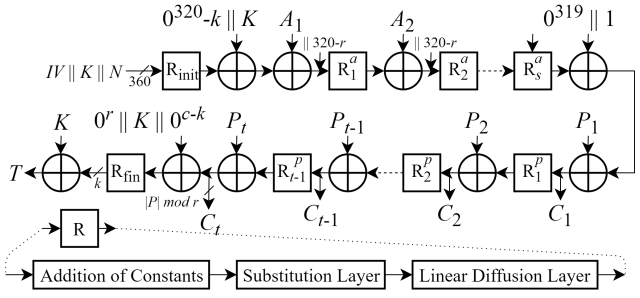

図 4 Ascon の暗号化・認証アルゴリズム

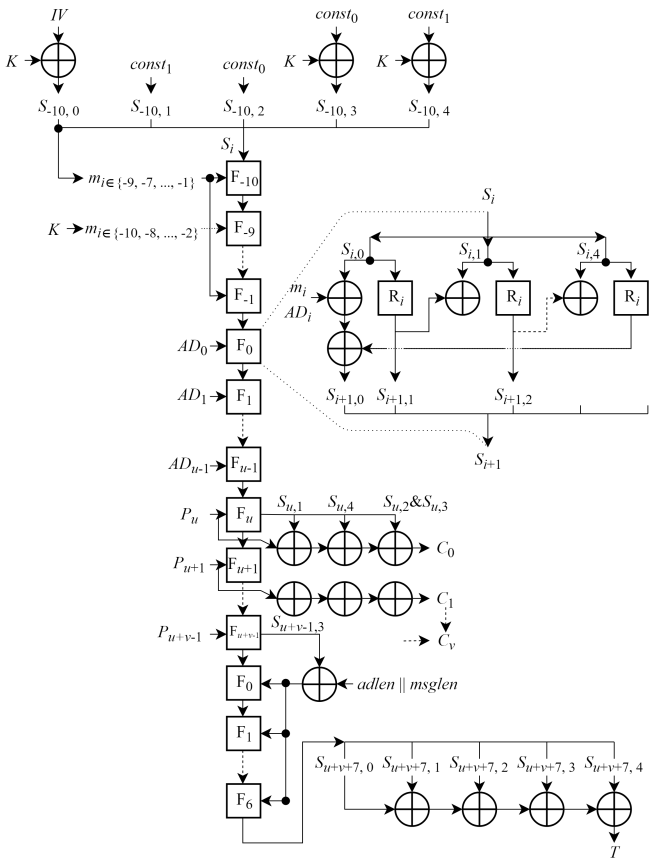

図 5 AEGIS-128 の暗号化・認証アルゴリズム

は，入力データ長に応じて，ラウンド関数を繰り返し実行する．認証データ A を 128-bit で分けたときのブロック数を u，平文を 128-bit で分けたときのブロック数を v としている．このラウンド関数は，AES の暗号化アルゴリズムを利用する．

3.2.3 Deoxys

Deoxys-II-128 はブロック長 128-bit，鍵長 128-bit の認証付き暗号である．また，Deoxys-II-256 では，鍵長が 256-bit 必要となる．CAESAR コンペティションでは，最もセキュリティ機能が優れたアルゴリズムとして評価されている．Deoxys-II-128 のアルゴリズムを図 5 に示す．Deoxys では，AES によく似たラウンド関数を用いて，認証と暗号化を実現している．

4. 評価実験

4.1 評価手法

本研究では，CAESAR の認証付き暗号のうち，第 1 候補であった Ascon，AEGIS-128，Deoxys-II について評価する．評価手法を図 7 及び以下の箇条書きに示す．

(1) SROS2 全体の処理時間を測定
(2) AES-GCM 実行部分のみの処理時間と暗号化処理回数を測定
(3) AES-GCM 実行部分以外の処理時間を測定
(4) SROS2 上に実装していない各認証付き暗号（Ascon,

Vol.2019-MBL-92 No.22
Vol.2019-CDS-26 No.22
2019/8/30

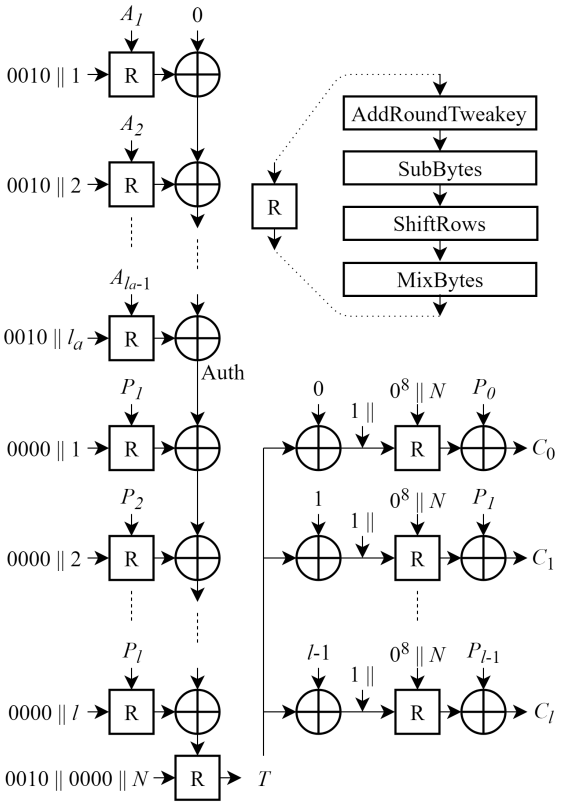

図 6 Deoxys-128-II の暗号化・認証アルゴリズム

AEGIS-128，Deoxys-II）の暗号化処理 1 回分の処理時間を測定

(5) 手順 2 の処理回数と，手順 4 の暗号化処理時間から各認証付き暗号の暗号化処理部分のみの処理時間を推測

(6) 手順 3 の非暗号化処理時間と手順 5 の暗号化処理処理時間から，各認証付き暗号時の文字列送信全体の処理時間を推測

まず手順 1 では，SROS2 の標準で実装されている AES-GCM を評価するために，16-byte の文字列を送信するプログラムを使用する．このプログラムの送信の前後で現在時刻を取得する機能を追加し，1 回の文字列送信における処理時間を測定する．これを 1 セット 100 回を 10 回行う．

次に手順 2 では，DDS-Security 内の暗号化処理のプログラムに着目し，処理時間を測定する．暗号化処理は，文字列送信中に何度も行われるため，その回数と合計の処理時間を取得する．

また手順 3 では，暗号化処理以外の処理時間を計算する．

そして手順 4 以降に，AES-GCM に代わる認証付き暗号を評価する．評価のため，SROS2 内の AES-GCM の記述を各認証付き暗号に適用するのが望ましいが，本実験では適切に実装することができなかったため，CAESAR のソフトウェア評価で用いられている SUPERCOP のプログラムの処理時間を基に，SROS2 上に実装した場合のオーバーヘッドを見積もる．具体的に手順 4 では，1 回の各認証付き暗号の SUPERCOP 処理時間を測定し，手順 5 で

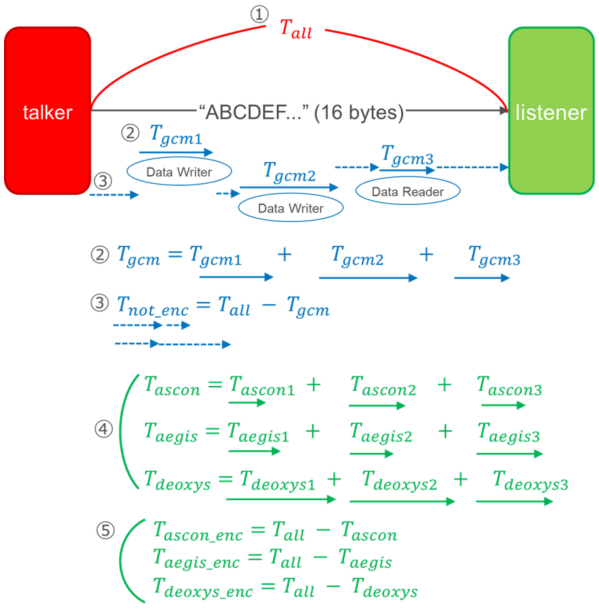

図 7 SROS2 における認証付き暗号の評価手法

AES-GCM の実行回数だけ掛け合わせ，暗号化処理に要した時間の総処理時間を見積もる．

最後に手順 6 では，各認証付き暗号の見積もった暗号化処理時間と暗号処理以外の処理時間の和を文字列送信における全体の処理時間とみなす．全体の処理時間を評価することで，AES-GCM と比較してどの程度のオーバーヘッドがあるのか，実システムに適用可能かどうかを考察する．評価実験に使用する PC とスペックを表 2 に示す．また，QoS はデフォルトの設定となっている．

4.2 評価結果

まず，図 8 に SROS2 全体の処理時間を，図 9 に AES-GCM だけの処理時間を，それらをまとめたものを表 3 に示す．表 3 より，SROS2 全体の処理時間と比較して，AES-GCM の暗号化処理の割合は約 2 割であることが分かった．また，AES-GCM 実行回数は平均で 11.28 回であり，AES-GCM 実行部分以外の処理時間は 1.530[ms] である．図 8 には一点だけはずれ値が含まれているが，これは他のアプリケーションによって PC 内に割り込み処理が生じ，SROS2 の処理時間が増加したと考えられる．

次に，各認証付き暗号の暗号化処理時間を図 10 及び表 4 に示す．

表 2 評価実験に用いた PC の詳細

型番	TOSHIBA dynabook Satellite R35/M
CPU	Intel Core i3-4005U
GPU	Intel Haswell Mobile
メモリ	4GB
OS	Ubuntu 18.04
ROS	ROS2 crystal
DDS	FastRTPS

Vol.2019-MBL-92 No.22
Vol.2019-CDS-26 No.22
2019/8/30

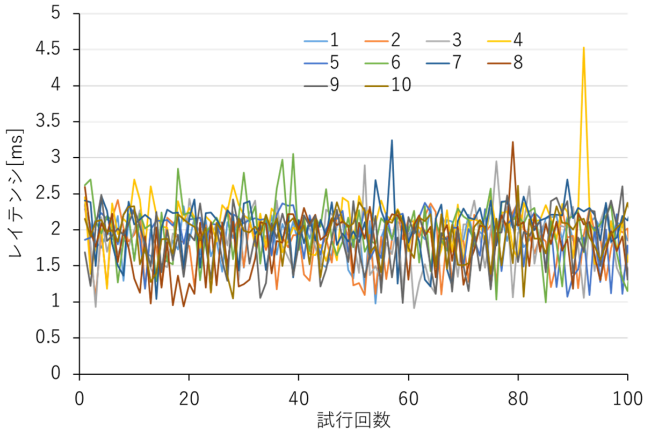

図 8　SROS2 全体の処理時間

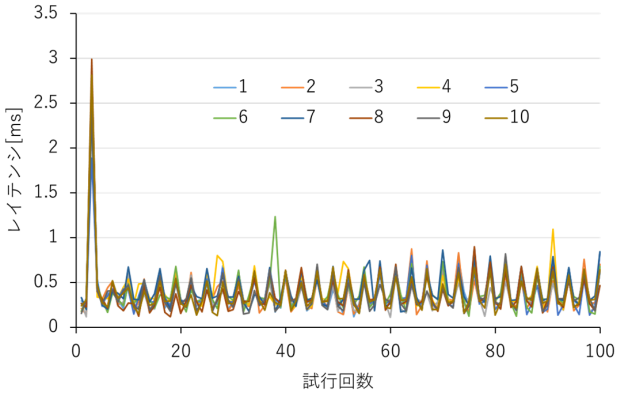

図 9　AES-GCM の処理時間

表 3　AES-GCM 実装時の処理時間

	平均値 [ms]	最大値 [ms]	最小値 [ms]
SROS2 全体	1.923	4.528	0.915
暗号処理部	0.393	2.994	0.114

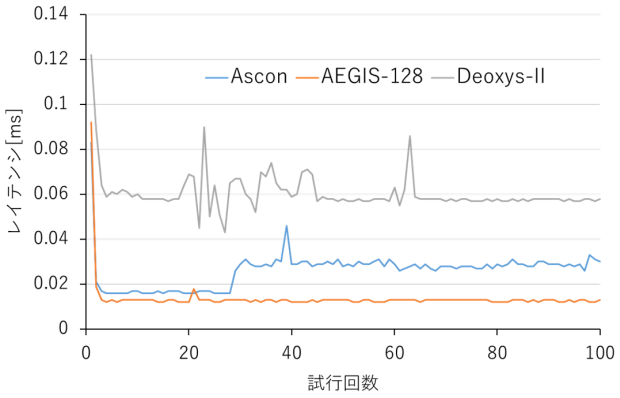

図 10　AES-GCM の処理時間

最後に，これらの結果を基に AES-GCM と各認証付き暗号の処理時間の比較を図 11 及び表 5 に示す．表 5 より，AES-GCM と比較して Ascon 及び AEGIS-128 は暗号処理の時間が短いことが分かった．従って，実際に実装した場合の SROS2 全体の処理時間も短くなると推測される．加えて，CAESAR の認証付き暗号は脆弱性が報告されていないため，SROS2 の暗号化処理及び認証には Ascon または AEGIS-128 を実装すべきである．

表 4　認証付き暗号単体の処理時間

	平均値 [ms]	最大値 [ms]	最小値 [ms]
Ascon	0.026	0.083	0.016
AEGIS-128	0.014	0.092	0.012
Deoxys-II	0.061	0.122	0.043

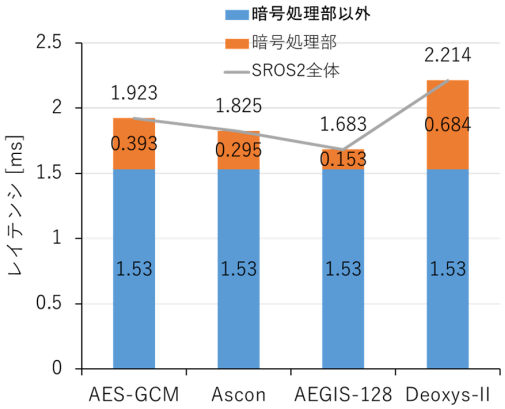

図 11　各暗号アルゴリズムの処理時間

表 5　AES-GCM と各認証付き暗号の比較

	SROS2 全体の処理時間 [ms]	暗号処理部の処理時間 [ms]
AES-GCM	1.923	0.393
Ascon	1.825	0.295
AEGIS-128	1.683	0.153
Deoxys-II	2.214	0.684

また，これらのパフォーマンス評価の結果，実システムに適用可能可能かどうかを考察する．産業用ロボットを多用する FA では，求められるレイテンシが 1ms 未満であることが文献 [20], [21] によって示されている．本実験の SROS2 処理時間は，PC のスペックに依存するものの，各認証付き暗号だけでなく AES-GCM の処理時間でも 1ms を越えてしまった．しかしながら，Ascon または AEGIS-128 ではより処理時間が短縮され，AEGIS-128 は特に暗号処理の時間が AES-GCM の半分以下となるために，SROS2 を実装する場合はこれらの認証付き暗号が適していると考えられる．

5. まとめ

本研究では，CAESAR の認証付き暗号を SROS2 に実装することを目的に，AES-GCM と比較したオーバーヘッドの評価と，実システムで動作可能かどうかの考察を行った．今後は，各認証付き暗号を SROS2 上に実装して詳細な評価を行い，パフォーマンス評価だけでなくサイドチャネル攻撃といった耐タンパ性評価についても検討する．

参考文献

[1] 総務省：第 4 次産業革命がもたらす変革，平成 29 年版情報通信白書第 1 部，pp. 106–169 (2017).
[2] 大西献：製造業ロボットにおける省配線・ワイヤレス技術の動向日本ロボット学会誌，Vol. 33，No. 5，pp. 334–337 (2015).
[3] https://github.com/ros2/sros2
[4] D. A. McGrew, J. Viega: The Security and Performance of the Galois/Counter Mode (GCM) of Operation, LNCS, Vol. 3348, pp. 343–355 (2004)
[5] M. Dworkin: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC NICT Special Publication, Vol. 800-38D, pp. 1–31 (2007).
[6] N. Ferguson: Authentication wealnesses in GCM, Comments submitted to NIST Modes of Operation Process, pp. 1–10 (2005)
[7] 亘理克好，大久保隆夫：ロボットオペレーティングシステムのセキュリティ機能に関する考察，情報処理学会研究報告，Vol. 2019，No. 1，pp. 1–7 (2019).
[8] V. DiLuoffo, W. R. Michalson, and B. Sunar: Creadential Masquerading and OpenSSL Spy: Expliring ROS 2 using DDS security, arXiv, Vol. 1904.09179v1 (2019).
[9] Y. Maruyama, S. Kato, T. Azumi: Exploring the Performance of ROS2, Proc. of EMSOFT' 16, No. 5 (2016).
[10] 小澤慶祐，本田晋也，松原豊，高田広章，加藤寿和，山本整：ROS2 と軽量 DDS の組込みシステムに対する適用性評価, 情報処理学会研究報告，Vol. 2018，No. 5，pp. 1–8 (2018).
[11] J. Kim, J. M. Smereka, C. Chung, S. Nepal, and M. Grobler, Security and Performance Considerations in ROS2:A Balancing Act, arXiv, Vol. 1809.09566v1 (2018).
[12] https://github.com/ros-infrastructure/robots.ros.org
[13] eProsima Fast RTPS Documentation, https://eprosima-fast-rtps.readthedocs.io/en/latest/index.html
[14] OBJECT MANAGEMENT GROUP: DDS Security Version 1.1, https://www.omg.org/spec/DDS-SECURITY/1.1, pp. 1–285 (2018)
[15] https://www.openssl.org/
[16] Cryptographic competitions final portfolio, https://competitions.cr.yp.to/caesar-submissions.html
[17] C. Dobrauning, M. Eichlseder, F. Mendel, and M. Schläffer: ASCON v1.2 — Submission to the CAESAR Competition —, https://competitions.cr.yp.to/round3/asconv12.pdf, pp. 1–27 (2016)
[18] H. Wu and B. Preneel: AEGIS: A Fast Authenticated Encryption Algorithm (v1.1), https://competitions.cr.yp.to/round3/aegisv11.pdf, pp. 1–32 (2016)
[19] J. Jean, I. Nikolić, T. Peyrin, and Y. Seurin: Deoxys v1.41 https://competitions.cr.yp.to/round3/deoxysv141.pdf, pp. 1–37 (2016)
[20] P. O'Farrell, A. Khadye: Latency in Factory Automation, TEXAS INSTRUMENTS Application Report, Vol. SNLA240A, pp. 1–9 (2019)
[21] G. Brown, P. Analyst, H. Reading, Ultra-Reliable Low-Latency 5G for Industrial Automation, A Heavy Reading white paper produced for Qualcomm Inc., pp. 1–11