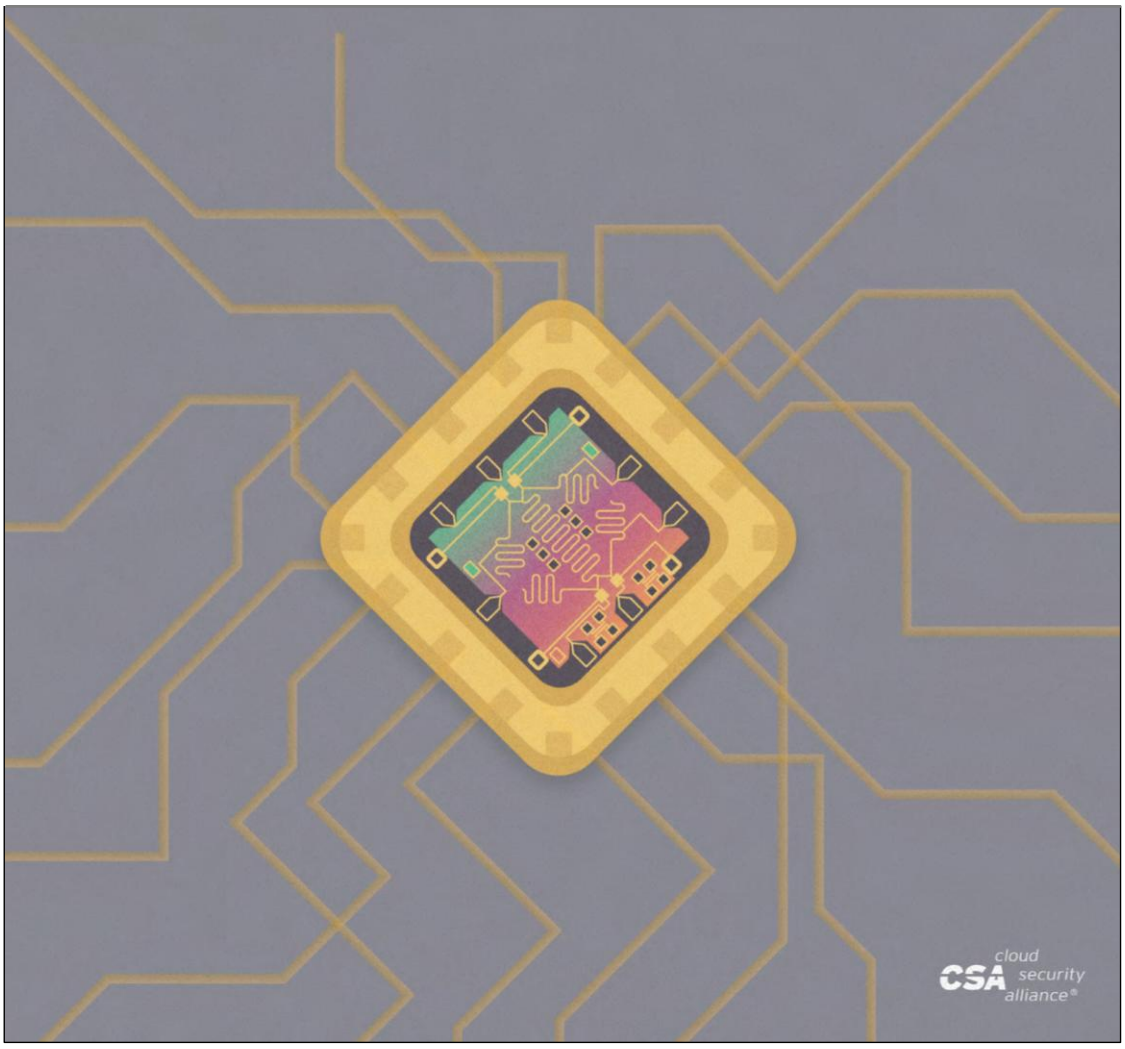
Quantum-Safe Security Glossary

耐量子セキュリティ用語集



Quantum-Safe Working Group, Cloud Security Alliance

日本クラウドセキュリティアライアンス

日本語版の提供について

本書「耐量子セキュリティ用語集」は、Cloud Security Alliance (CSA)が公開している「Quantum-Safe Security Working Group Glossary」の日本語訳です。
本書は、一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）が、CSA の許可を得て翻訳し、公開するものです。
本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。

翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性及び原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
翻訳に際して原文の誤りと推測されるものは著作者に確認の上、最小限の修正を行った上で翻訳しています。また、翻訳に際して行った判断については、脚注部に「訳注」として示しました。

この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。
変更履歴

日付	バージョン	変更内容
2017 年 4 月 24 日	日本語バージョン 1.0	

本翻訳の著作権は CSA ジャパンに帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。転載および商用利用に際しては、事前に CSA ジャパンにご相談ください。

本翻訳の原著作物の著作権は、CSA または執筆者に帰属します。CSA ジャパンはこれら権利者を代理しません。
原著作物における著作権表示と、その参考日本語訳を、以下に示します。

© 2016 Cloud Security Alliance – All Rights Reserved

You may download, store, display on your computer, view, print, and link to Quantum-Safe Security Glossary at https://cloudsecurityalliance.org/download/quantum-safe-securityglossary/, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to International Standardization Council Policies & Procedures.

すべての権利は Cloud Security Alliance に帰属します。以下の条件のもとに、ダウンロード、コンピュータディスプレイへの表示、読み取り、印刷、https://cloudsecurityalliance.org/download/quantum-safe-security-glossary/ にある「Quantum-Safe Security Glossary」へのリンクを行うことができます。

a)このレポートが個人的、参照目的かつ非商業的目的に限定して利用されること

b)このレポートを方法または内容の如何によらず修正しもしくは変更しないこと

c)このレポートの配布もしくは移転を行わないこと

d)商標、著作権その他の表示を削除しないこと

このレポートは、米国著作権法におけるフェアユース規定により認められている範囲で引用可能です。ただし、出典としてこのレポート名を明記すること。

クラウドセキュリティアライアンスの Quantum-Safe Working Group（耐量子セキュリティワーキンググループ）の常置アドレスは、https://cloudsecurityalliance.org/group/quantum-safe-security/ です。

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

謝辞

クラウドセキュリティアライアンス
Frank Guanco
Ryan Bergsma
Victor Chin
Stephen Lumpe

耐量子セキュリティワーキンググループ
Bruno Huttner, 共同リーダー
Jane Melia, 共同リーダー
Gene Carter
Ludovic Perret
Lee Wilson

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

耐量子セキュリティ(Quantum-Safe Security, QSS)ワーキンググループは鍵生成方法及び転送方法の問題を処理し、量子コンピュータに対して安全な方法を業界内で理解するのを助けるために組織された。このワーキンググループは、暗号解読の能力が向上してゆく状況の中での長期的なデータ保護に重点を置いている。

この用語集は量子コンピュータに対する安全性についての知識を高めるため、QSS ワーキンググループのメンバーが寄稿したのを集めたものであり、耐量子暗号界で使われる通常の用語を集積したものが掲載されている。このような特性を見据えて、QSS ワーキンググループではこの文書を更新し、適宜進めていく予定である。

［翻訳版における表記についての注記］

文中**青色太字**で表された単語は、本用語集の別の項で解説があるもの、及び参考文献リストの中のタグを示す。

見出し語については、略語を除いて、原語と訳語を併記した。言語の語頭の大文字・小文字については、原文に忠実にならっている。原文における規則性についてはないように見えるが、未確認である。

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

BQP	量子コンピュータによって効率的に求解可能であるクラスの問題は BQP(限られた誤差、量子、多項式時間)と呼ばれる。量子コンピュータでは確率的アルゴリズムしか実行できないので、量子コンピュータにおける BQP は古典的コンピュータにおける BPP(限られた誤差、確率的、多項式時間)に対応するものである。BQP は、誤りの確率が 1/2 より小さい多項式時間アルゴリズムで求解可能な問題の集合と定義される。もしも全てのインスタンスについて、量子コンピュータの求める解が高い確率で正しい場合に「(量子コンピュータが)問題を解く」と言う。もしもその求解が多項式時間で実行されるならば、その問題は BQP に属する。**非決定的多項式時間困難(NP 困難)**な問題は**BQP** には存在しないと考えられている。
CFS	これは、N. Courtois、N. Sendrier、及び M. Finiasz **[CSF01]**によって 2001 年に設計されたコードベースの署名方式である。
Closest Vector Problem (CVP) 最近ベクトル問題(CVP)	最近ベクトル問題は、**非決定的多項式時間困難(NP 困難)**であり、格子(Lattice)において、所与のベクトルに対して見出される最も近いベクトルを求める問題である。これは**格子ベース暗号**において発生する計算困難問題である。
Code-based cryptography コードベース暗号	**耐量子安全性暗号**の部分領域で、この中には、その安全性が線形誤り訂正符号のデコード問題の困難性に関連しているものが含まれる。
D-Wave machine D-Wave マシン	公に利用可能な最初の量子計算機(カナダの D-Wave Systems による)。この計算機は汎用量子コンピュータではなく、**量子アニーリング**を目的としたものである。
Entropy source エントロピー源	**量子乱数発生器**のようなノイズ源とヘルステスト、及びコンディショニング・コンポーネント(オプション)を組み合わせたもので、フル・エントロピーの乱数ビットを生成する**[NIST]**。
Grover's algorithm Grover のアルゴリズム	L. K. Grover **[Grover96]**にちなんで名づけられたアルゴリズム。このアルゴリズムは、**量子コンピュータ**での全数探索に量子的高速化を与えるものである。これはデータベース検索アルゴリズムとして設計されたものだが、対称暗号方式の暗号強度を半分に減らすのに利用可能である。
Hash-based cryptography ハッシュベース暗号	**耐量子安全性暗号**の部分領域で、その安全性がハッシュ関数の衝突を発見することの困難性に依拠した署名方式を言う。この署名方式は通常、ワンタイム署名方式またはフュータイム署名方式と**マークル木**を組み合わせることによって構築される。この例に Lighton-Micali 方式**[LM]**、SPHINCS **[SPHINCS]**、及び XMSS**[XMSS]**がある。
Hidden Field Equations (HFE)[1]	J. Patarin **[HFE]**によって 1996 年に提案された多変数公開鍵暗号方式(秘匿及び署名)。HFEv-**[PCG01]**は HFE のセキュアな変形法で、これは署名にのみ可能でありデータの秘匿には使用できない。

[1] 訳注: この用語は、日本においても、通常英語のまま使われているので、訳語は示さない。

©(社)日本クラウドセキュリティアライアンス 2017 All rights reserved

Information-theoretic secure 情報理論的に安全	ある暗号方式が、その安全性が純粋に情報理論から導出されるとき、その暗号は「情報理論的に安全である」という。即ち、解読者側が無限の計算能力を持っていたとしてもその暗号を破ることができないということを意味する。 情報理論的に安全な暗号方式の例には古典的ワンタイムパッド及び**量子鍵配送(QKD)**がある。
Isogeny 同種	二つの楕円曲線の間の写像の特殊な形。
Isogeny-based cryptography 同種ベース暗号	**耐量子安全性暗号**の部分領域で、その安全性が一対の楕円曲線ペアの間の未知の**同種**写像を得ることの困難性に依拠した公開鍵暗号方式を構築する。この例には D. Jao と L. De Feo **[JF]**の方式がある。
Lamport one-time signature scheme Lamport のワンタイム署名方式	**ハッシュベース**署名方式のヒントとなった方式。L. Lamport **[LamportRR]** によって提案されたこの技術には一方向性関数が必要で、最高で一つのメッセージに署名することができる。
Lattice-based cryptography 格子ベース暗号	**耐量子安全性暗号**の部分領域で、その安全性は**最近ベクトル問題(CVP)**、**Learning with Errors (LWE)[2]問題**、または**最短ベクトル問題(SVP)**に関係している。
Learning with Errors (LWE) problem Learning with Errors (LWE)問題	**格子ベース暗号**で使われる計算困難問題。この問題は O. Regev **[Reg05]**によって導入されたものであるが、この解を求めるにはノイズのある線形連立方程式を取り出すことが求められる。
McEliece encryption scheme McEliece 暗号方式	R.-J. McEliece によって 1978 年**[McE78]**に提案された**コードベース**の公開鍵暗号方式。
Merkle tree マークル木	R. Merkle **[Merkle89]** にちなんで名づけられたデータ構造で、ハッシュ木(ツリー)とも呼ばれる。これは二分木で、葉がハッシュのついたデータブロックで、他のブロックとハッシュによって結合される。このハッシュ結合が、全てのブロックが単一のハッシュで結合されるまで繰り返される。
Merkle Tree Signature Scheme マークル木(マークルツリー)署名方式	R. Merkle によって提案された**ハッシュベース署名**の代表例。この方式の原理は、葉が公開鍵/秘密鍵になったマークル木を使うことである。これによって、Lamport のワンタイム署名方式(またはその他のワンタイムまたはフューターム署名方式)を、一つでない、より多くのメッセージに署名するように拡張することができる。署名可能なメッセージ数は**マークル木**の高さに依存する。署名方式には、衝突耐性のあるハッシュ関数または原像耐性のあるハッシュ関数が必要である。
Multivariate-based cryptography	**耐量子安全性暗号**の部分領域で、その安全性が **PoSSo 問題**または**多変数二次式(MQ)問題**に関係するもの。この問題はまた、非線形方程式が二

[2] 訳注： この用語は、日本においても、通常英語のまま使われているので、訳語は示さない。

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

多変数ベースの暗号	次である場合は、MQ 問題とも呼ばれ、これも NP 困難である。
Multivariate Public-Key Cryptography (MPKC) 多変数公開鍵暗号 (MPKC)	多変数を使った公開鍵暗号方式のことを言う。
Multivariate Quadratic (MQ) problem 多変数二次(MQ)問題	**PoSSo 問題**を二次多項式に限定したもの。
Noise Source ノイズ源	非決定性乱数を生成するシステム。ノイズ源には非決定性、エントロピー生成活動**[NIST]**が含まれる。
Non-deterministic Polynomial time (NP) 非決定性多項式時間 (NP)	肯定(Yes の回答が発生すること)が決定性多項式時間で検証可能な複雑性クラスに属する決定問題。NP 困難問題を解く効率的なアルゴリズムが存在したら、全ての問題を NP で解く効率的なアルゴリズムに繋がる可能性がある。抗量子暗号(quantum-resistant cryptography)の基本的前提は、NP 困難問題のどれも決定的多項式時間では古典的設定でも量子的設定でも解くことができないということである。
Non-deterministic Polynomial time Hardness (NP-Hard) 非決定性多項式時間困難(NP 困難)	計算問題は、その(本質的な)困難性の関数で分類できる。NP 困難問題は少なくとも、**非決定性多項式時間(NP)**に属する問題で最も困難なものと同程度に困難でなければならない。
NTRU	特許取得されたオープンソースの**格子ベース暗号**で、データの暗号化と復号化に使われる。J. Hoffstein, J. Piper, J.H. Silverman **[HPS98]** によって開発された。署名方式 pqNTRUsign は同じ困難問題に基づくもので、やはり耐量子である。
Posso problem PoSSo 問題	連立非線形方程式の**非決定性多項式時間困難(NP 困難)**問題である。
Post-quantum cryptography 耐量子暗号	量子コンピュータの存在する社会にあってもなお安全な暗号方式の集合である。これには、量子鍵配送(QKD)のような量子暗号や、**格子ベース**、**コードベース**、**多項式ベース**、**ハッシュベース**、及び**同種写像ベース**などのようなアルゴリズムベースの暗号、及び AES のような対称鍵(秘密鍵)暗号が含まれる。耐量子暗号に関係する用語は、P.W. Shor による、整数の素因数分解や離散対数を解く量子多項式時間アルゴリズムの導入以降、すぐに学術論文に現われるようになった。この用語にはある種の曖昧さが残っており、一部の組織では QKD を含めていない。
Quantum annealing	古典的コンピュータを使った場合よりも速く最適化問題を解ける量子プロセス

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

量子アニーリング	である。
Quantum bit or QUbit 量子ビット、または Qubit	古典的コンピュータのビットに対応する量子の類似体。二つの準位から成り、通常|0> 及び|1>と表される。
Quantum computer 量子コンピュータ	量子力学的性質を使って計算を行うコンピュータ。量子コンピュータでは、ある種の問題については現在のコンピュータと比べて指数関数的にスピードが向上する。
Quantum-computing resistant cryptography 量子計算耐性暗号	国際標準化機構によって用いられる、耐量子暗号の変形語。
Quantum cryptography 量子暗号	その安全性が量子力学の物理法則によって保証されている暗号方式。これは、その安全性が何らかの数学的困難問題に依拠している古典的公開鍵暗号とは異なっている。
Quantum-Key Distribution 量子鍵配送(QKD)	量子鍵配送は、二つの別空間にあり、安全でない光チャネルで繋がれた者の間での、情報理論的に安全な鍵配送を実現する**量子暗号**の例である。QKD にはニつの相補的なアプローチがある:(1) 離散変数量子鍵配送(DVQKD)は単一の光子または微弱なコヒーレント状態、及び単一の光子検出器を使う。(2)連続変数量子鍵配送(CVQKD)は光のコヒーレントまたはスクイーズ状態及びホモダイン検出器を用いる。連続・離散両方のアプローチとも実験で実証されている;同じく重要なことは、両方とも情報理論的に安全であることが証明されている点である。
Quantum Random Number Generator (QNRG) 量子乱数生成器 (QRNG)	乱数を量子過程または量子システム上で行われる測定から得られる、量子ベースの**ノイズ源**。これらの測定/結果の一義性及び乱数性は、量子力学で記述される、量子起源である。QRNG の例には、光の光量子状態測定から乱数を発生する、幾つかの商用システムがある。
Quantum-resistant cryptography 抗量子暗号[3]	この用語も、量子コンピュータの存在する社会にあってもなお安全な暗号方式の集合を現わす。この用語は、米国国家安全保障局(NSA)がその「量子耐性アルゴリズムへの移行の準備的計画」において使ったものである。この用語は、耐量子暗号(post-quantum cryptography)と完全に同じものではなく、アルゴリズム技術のみを指す。また、これには**量子鍵配送(QKD)**のような物理的技術は含まないようである。
Quantum-safe cryptography 耐量子安全性暗号[4]	量子コンピュータの存在する社会にあってもなお安全な暗号方式の集合である。この用語は新しく作られたものだが、「耐量子暗号」(post-quantum cryptography)とほぼ同じ意味に使われる。更にまた、これは欧州通信規

[3] 訳注: この用語は日本語の文献では、post-quantum cryptography の同義語として紹介される程度で、殆ど見られない。しかし用語解説では post-quantum cryptography との違いに言及しているので同じ訳語では不適当なので、この文章の翻訳において、独自に別の訳語を当てはめた。

[4] 訳注: 訳注 3 と同様に、post-quantum cryptography と同じ訳語を避けるために、この文章の翻訳において、独自に

©(社)日本クラウドセキュリティアライアンス 2017 All rights reserved

	格機構(ETSI)及びクラウドセキュリティアライアンス(CSA)で使われている。
Ring-LWE (RLWE) problem Ring-LWE(RLWE)問題	解くべき問題として(ノイズのある)線形システムが構築される **Learning with Errors (LWE)**問題の一種である**[LPR]**。
Shor's algorithm Shor のアルゴリズム	1994 年に発表された P. W. Shor のアルゴリズム**[Shor]**で、整数の素因数分解と離散対数を求めることを、量子コンピュータ上で多項式時間で計算できるもの。Shor のアルゴリズムを使うことによって、今日一般に使われる非対称(公開鍵)暗号は破ることができる。
SVP	格子の中に存在する最も短いベクトルを求める最短ベクトル問題(Shortest Vector Problem)の略。この問題はユークリッドノルムについてランダム化された簡約においては**非決定性多項式時間困難(NP 困難)**である。これは**格子ベース暗号**において発生する困難問題である。
Syndrom decoding シンドローム復号	**コードベース暗号**で発生する**非決定的多項式時間困難(NP 困難)**問題。目標は線形連立方程式の制約のある解を発見することである。この解には少数の非ゼロ要素が無ければならない。
Unbalanced Oil and Vinegar (UOV)[5]	1999 年に A. Kipnis, L. Goubin, J. Patarin によって提案された**[KPG99]**多変数署名方式。

別の訳語を当てはめた。

[5] 訳注: この用語は、日本においても、通常英語のまま使われているので、訳語は示さない。

©(社)日本クラウドセキュリティアライアンス 2017 All rights reserved

参考文献

[SPHINCS] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe and Z. Wilcox-O'Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. EUROCRYPT 2015.

[XMSS] J. Buchmann, E. Dahmen, and A. Hülsing. XMSS - a Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. Post-Quantum Cryptography, 2011.
」

[CFS01] N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-Based Digital Signature Scheme, ASIACRYPT 2001.

[Grover96] Lov K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. STOC 1996.

[JF] D. Jao and L. De Feo. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, Post-Quantum Cryptography 2011.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. ANTS-998.

[KPG99] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar Signature Schemes. EUROCRYPT'99, LNCS 1592, pages 206–222. Springer, 1999.

[LamportRR] L. Lamport. Constructing Digital Signatures from a One Way Function. Technical Report SRICSL-98, SRI International Computer Science Laboratory, 1979.

[LM] F.T. Leighton and S. Micali. Large Provably Fast and Secure Digital Signature Schemes based on Secure Hash Functions. US Patent 5,432,852, July 11, 1995.

[LPR] V. Lyubashevsky, C. Peikert and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. J. ACM, 2013.

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved

[McE78] R.-J. McEliece. A Public-Key System Based on Algebraic Coding Theory, pages 114—116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[Merkle89] R. Merkle. A Certified Digital Signature. CRYPTO ’89.

[HFE] J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. EUROCRYPT’96.

[PCG01] J. Patarin, N. Courtois, and L. Goubin. QUARTZ[6]. 128-bit Long Digital Signatures. CT-RSA’01.

[Reg05] O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. STOC 2005.

[Shor] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 1997.

[NIST] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish and M. Boyle. Recommendation for the Entropy Sources Used for Random Bit Generation (Second DRAFT). NIST Special Publication 800-90B, 2016.

以上

[6] 訳注： QUARTZ はイニシャルを集めた略称なのでフルキャピタルで表記する。

©（社）日本クラウドセキュリティアライアンス 2017 All rights reserved