

耐量子計算機暗号（PQC）のココントコ

2023年11月6日

菅野 哲

GMOサイバーセキュリティ by イエラエ株式会社

- 名前
 - 菅野 哲 (かんの さとる)
- 所属
 - GMOサイバーセキュリティ byイエラエ株式会社
 - 取締役CTO of Development
- どんなことやっていた／やっているの？
 - 学生時代
 - 暗号プロトコルの研究、セキュリティベンチャーで技術担当/営業担当
 - 社会人時代
 - 暗号ライブラリや情報セキュリティ関連システム開発
 - IETFなどでブロック暗号Camelliaに関する標準化活動
 - 外部活動
 - CRYPTREC 暗号鍵管理ガイダンスWG 委員
 - Trusted Computing Group Invited Expert (2018年10月～)

- 「誰もが犠牲にならない社会を創る」がミッション
- デジタルネイティブの時代に生きるすべての人が安全に暮らせるインターネット社会創りに貢献します。



<https://gmo-cybersecurity.com/>

現地参加のみ

16:00-16:45 A1-6

耐量子計算機暗号 (PQC) のコントコ

最近、ニュースなどで耐量子計算機暗号 (PQC) というキーワードを聞くことが増えてきたと思います。

ただでさえ取っ付きにくい暗号に関する話題なのにワンランク上の難しさを漂わせるのがPQCではないかと感じています。本セッションでは、RSAやECDSAなどに代表される現行暗号との違いやNISTが開催しているPQCコンペティションなどの技術動向をご紹介します。

本講演でどんな話のトピックスは？

- なんでPQCが必要になったの？
- 暗号アルゴリズムの安全性
 - 暗号の危殆化とは？
- 耐量子計算機暗号 (PQC) とは？
- 暗号移行とは？
 - 暗号移行というイベントは未体験なのか？
 - 2つの「暗号の2030年問題」
- IETFでのPQCに関する動向

- 暗号の危殆化
- 暗号移行を招く？！ 2つの「暗号の2030年問題」
- 我々を取り巻く環境

- 暗号の危殆化
- 暗号移行を招く？！ 2つの「暗号の2030年問題」
- 我々を取り巻く環境

暗号の危殆化とは

- 「暗号アルゴリズムへの攻撃の進歩やコンピュータの性能向上によって、**設計時に想定された「セキュリティ上の性質」がより低いコストで確保できない状態**」のこと
- 暗号を危殆化させる脅威/要因
 - 暗号解析手法（攻撃）の進歩 : 差分解読法、線形解読法など
 - 計算量的な脅威 : ムーアの法則、**量子コンピュータ**など
- 過去に危殆化した主な暗号アルゴリズム
 - ハッシュ関数（MD5）、共通鍵暗号（DES）、公開鍵暗号（RSA-512）

「**危殆化した暗号アルゴリズム**を
安全なアルゴリズムに差し替える」のみ！



実施することは明確ではあるけど・・・
「**移行コスト**」や「**社会的インパクト**」が大きい

影響範囲の例：

インターネットサービス、仮想通貨、ブロックチェーン、情報家電製品、OS、アプリケーション、ネットワーク機器など

- 細かいことをすっ飛ばして安全性のキモチを示すと・・・

情報理論的安全性

計算量的安全性



その暗号を最も効率のよいアルゴリズムで
解読した時に必要な計算量のこと

計算量的安全性って？ その1

- 暗号技術の安全の根拠となる数学的問題が「現実的な計算リソース、計算時間では解けない事実を利用」した安全性のこと
 - 無限のリソース、無限の時間があれば解読
- RSAの場合は素因数分解問題を利用

```
RSA-2048 = 2519590847565789349402718324004839857142928212620403202777713783604366202070  
7595556264018525880784406918290641249515082189298559149176184502808489120072  
8449926873928072877767359714183472702618963750149718246911650776133798590957  
0009733045974880842840179742910064245869181719511874612151517265463228221686  
9987549182422433637259085141865462043576798423387184774447920739934236584823  
8242811981638150106748104516603773060562016196762561338441436038339044149526  
3443219011465754445417842402092461651572335077870774981712577246796292638635  
6373289912154831438167899885040445364023527381951378636564391212010397122822  
120720357
```

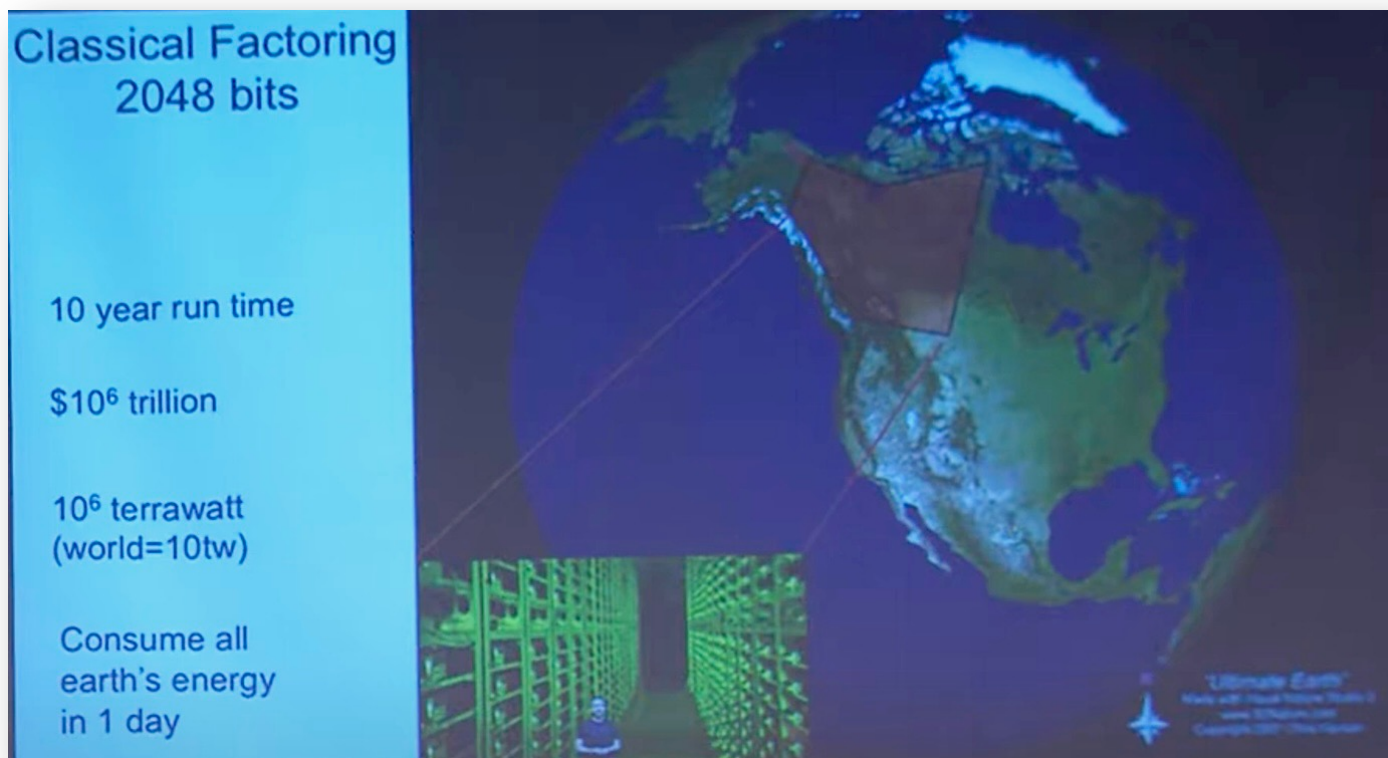
https://www.wikiwand.com/en/RSA_numbers#RSA-2048

サマーウォーズ（2009年）では
暗算で暗号解読している！

画像 削除

※ サマーウォーズで登場した仮想世界では2056桁（約6825bit）の
暗号鍵によって暗号化されている？！

Invited talk at CRYPTO 2017 by John Martinis



RSA-2048解読するには？

- 期間
 - 10年
- データセンタの敷地
 - 北米の1/4のサイズ
- 費用：
 - 10^6 兆USD
- 電力：
 - 10^6 Tワット

<https://www.youtube.com/watch?v=vOkC856dJrg>

それぞれ異なる暗号技術を同じ指標で評価

- ビットセキュリティという概念が「NIST SP800-57 “Recommendation on Key Management”」で提唱

- 異なる種類の暗号アルゴリズムに対して安全性を評価するための指標
- 「等価安全性」という表現を使っていることもある

<https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>

- ビットセキュリティはどう表されるの？

- 対象の暗号アルゴリズムへの攻撃に必要な計算量が 2^n である時、この暗号アルゴリズムの安全性は「**nビット安全性 (n-bits of security)**」とする

- 例

- 共通鍵暗号 : 秘密鍵を探索する計算量
- 公開鍵暗号 : 安全性が基づく問題（素因数分解、離散対数問題など）を解く計算量
- ハッシュ関数 : 衝突ペアを探索する計算量

• NIST SP800-57 “Recommendation on Key Management”

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
≤ 80	2TDEA	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112	3TDEA ⁶⁸	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Security Strength	Digital Signatures and Other Applications Requiring Collision Resistance	HMAC, ⁷⁰ KMAC, ⁷¹ Key Derivation Functions, ⁷² Random Bit Generation ⁷³
≤ 80	SHA-1 ⁷⁴	
112	SHA-224, SHA-512/224, SHA3-224	
128	SHA-256, SHA-512/256, SHA3-256	SHA-1, KMAC128
192	SHA-384, SHA3-384	SHA-224, SHA-512/224, SHA3-224
≥ 256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512, KMAC256

128bit安全性が求められる世界へ！

例1：オレンジ色で示された80bit以下の強度では情報を保護することは認められていません。

例2：3DESは112bit securityを持つとされていますが、そのアルゴリズムの利用は2023年まで推奨とされています。（参照：NIST SP800-131A）

- 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準
 - 前ページにある「NIST SP800-57」と同様なドキュメント

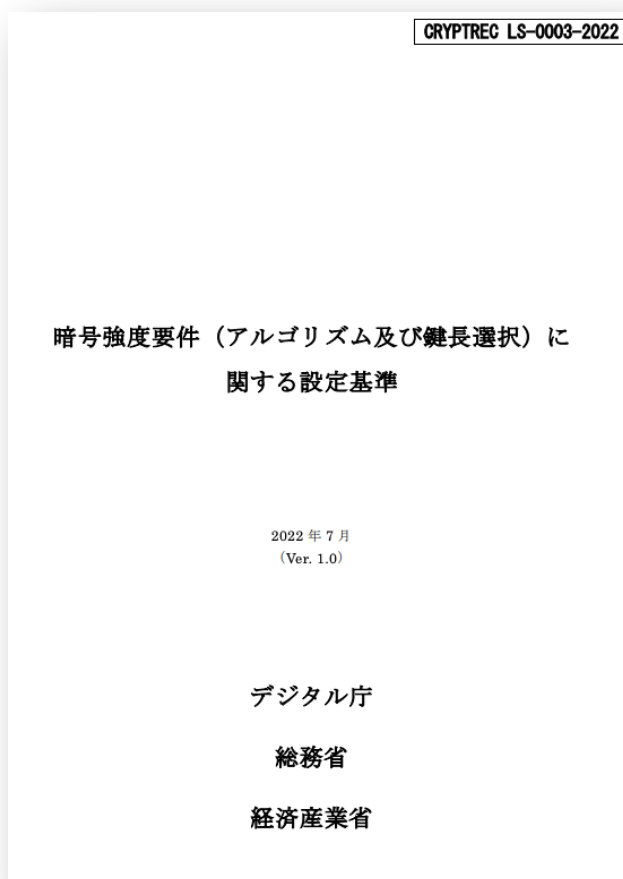


表 2 公開鍵暗号の推定セキュリティ強度

セキュリティ強度 (ビットセキュリティ)	IFC	FFC	ECC
	RSA-PSS RSASSA-PKCS1-v1.5 RSA-OAEP RSAES-PKCS1-v1_5	DSA DH	ECDSA ECDH PSEC-KEM
112	k = 2048	(L, N) = (2048, 224)	P-224 B-233 K-233
128	k = 3072	(L, N) = (3072, 256)	P-256 B-283 K-283 W-25519 Curve25519 Edwards25519
192	k = 7680	(L, N) = (7680, 384)	P-384 B-409 K-409 W-448 Curve448 Edwards448
256	k = 15360	(L, N) = (15360, 512)	P-521 B-571 K-571

※ P: curve over Prime fields (素体曲線)、B: curve over Binary fields (拡大体 (バイナリ) 曲線)、K: Koblitz-curve (コブリッツ曲線)、W: Weierstrass-curve (ワイエルシュトラス曲線)、Curve: Montgomery-curve (モンゴメリ曲線)、Edwards: Edwards-curve (エドワード曲線)

CRYPTREC暗号リストの
アルゴリズムが例示

<https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf>

現行暗号に脅威になる量子コンピュータ

- どんな量子コンピュータでも暗号の安全性に影響あるの？



答えは「**No**」！

- 具体的には「誤り訂正機能を有する大規模な量子ゲート型量子コンピュータ」が必要となる
- 別名「**CRQC**: Cryptographically Relevant Quantum Computer / 暗号解読可能な量子コンピュータ」と呼ばれる

では、CRQCによるリスクはどんなもの？

攻撃とリスク例

ハーベスト攻撃

- ・ 攻撃者が入手していた**過去**の**暗号化データを一気に解読**

デジタル署名の改ざん

- ・ 過去のデジタル署名付き文書の**信頼が喪失**する

これらのリスクが許容できないならば
暗号の更新 (=PQC) などが必要

No	暗号の種類	現行暗号例	脅威となる量子アルゴリズム	効率的に解ける問題	暗号への脅威	望ましい対策
1	共通鍵暗号	AES	Grover's Alg	データ探索問題	限定的	鍵長の伸長/ 暗号利用 モードの変更
2			Simon's Alg	周期探索問題	限定的	
3	公開鍵暗号	RSA暗号	Shor's Alg	素因数分解	非常に大きい	PQCへの移行
4		DSA/ECDSA	Shor's Alg	離散対数問題		
5		PQC	(現状) 未発見	—	現在なし	—

CRQCが実現されたら現行暗号は全てダメになるの？と気になる

- 共通鍵暗号への影響は限定的
- 公開鍵暗号への影響が大きい



この大きな影響に対策を計画する必要がある

- 暗号の危殆化
- 暗号移行を招く？！ 2つの「暗号の2030年問題」
- 我々を取り巻く環境

暗号移行：暗号の「2010年問題」とは？

- 2010年問題のきっかけ ⇨
“NIST’s Policy on Hash Functions - March 2006”

NIST's Policy on Hash Functions - March 2006

March 15, 2006

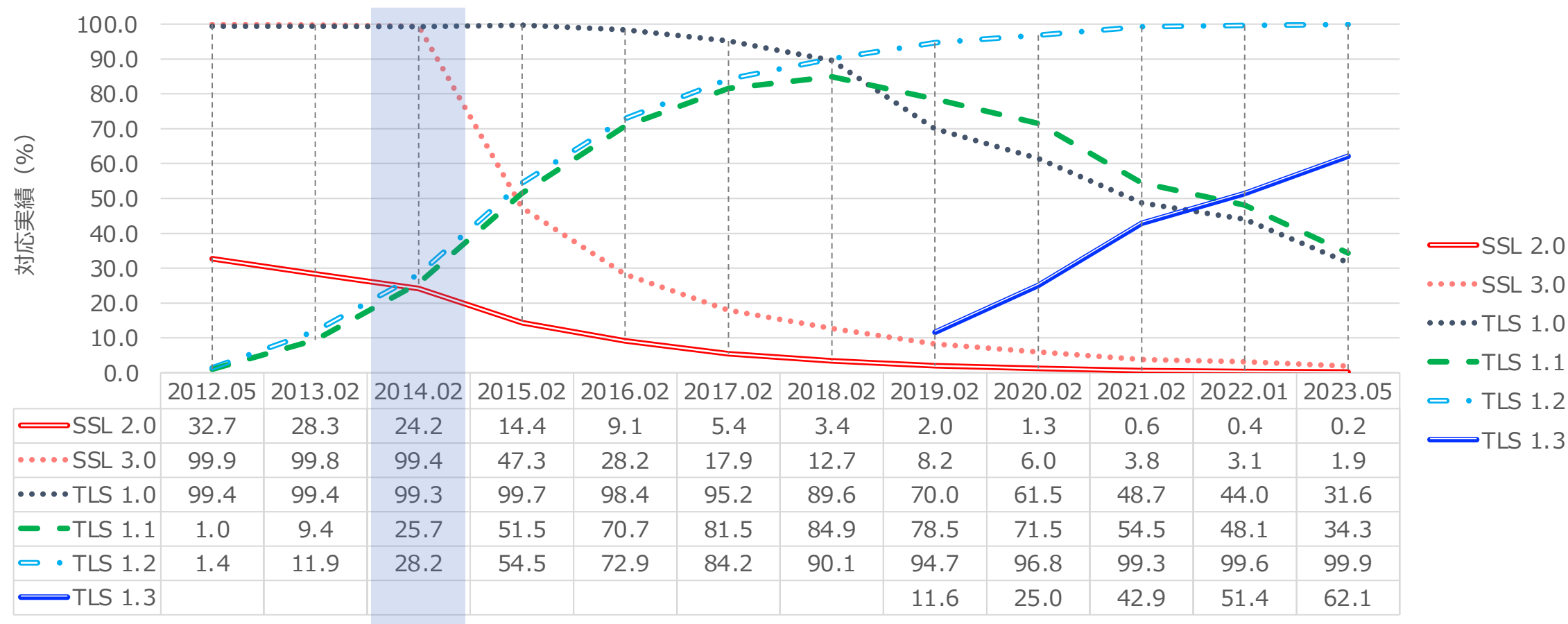
The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and **must use the SHA-2 family of hash functions for these applications after 2010.** After 2010, Federal agencies may use SHA-1 only for the following applications: hash-based message authentication codes (HMACs); key derivation functions (KDFs); and random number generators (RNGs). Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

<https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions>

「**2010年末**でSHA-1の利用停止、**SHA-2への全面移行**」という声明

※背景: SHA-1を含む複数アルゴリズムへの攻撃が公開された

- 2008年発行RFC5246「TLS1.2」に注目。2014年の利用率 ⇨ **28%**
2011年頃から様々な攻撃が公表された状況だが時間はかかった...



年数

SSL Labs Pulseのデータにより講演者がグラフ化

2つの「暗号の2030年問題」とは？

「暗号の2010年問題」の再来として、異なる移行観点で襲来！？

暗号の2030年問題の根っこ

将来的な「暗号解読の進展」や
「計算機環境の変化」を考慮し
112bit安全の移行計画

※ NIST SP 800-57 で記述

CRQCによる現行暗号への
リスクが許容できない



1つ目

128bit安全な暗号への移行



2つ目

PQCへの移行

- 128bit安全なアルゴリズム ⇨ 「RSA-3072」や「RSA-4096」
 - RSA暗号だとデータサイズが大きい・・・。
 - DKIMからの視点だと「DNSのUDPパケット(512 byte)」の制約あり
- データサイズが大きい際には「楕円曲線暗号/ECC」が活用

Internet Engineering Task Force (IETF)
Request for Comments: 8463
Updates: [6376](#)
Category: Standards Track
ISSN: 2070-1721

J. Levine
Taughannock Networks
September 2018

A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)

Abstract

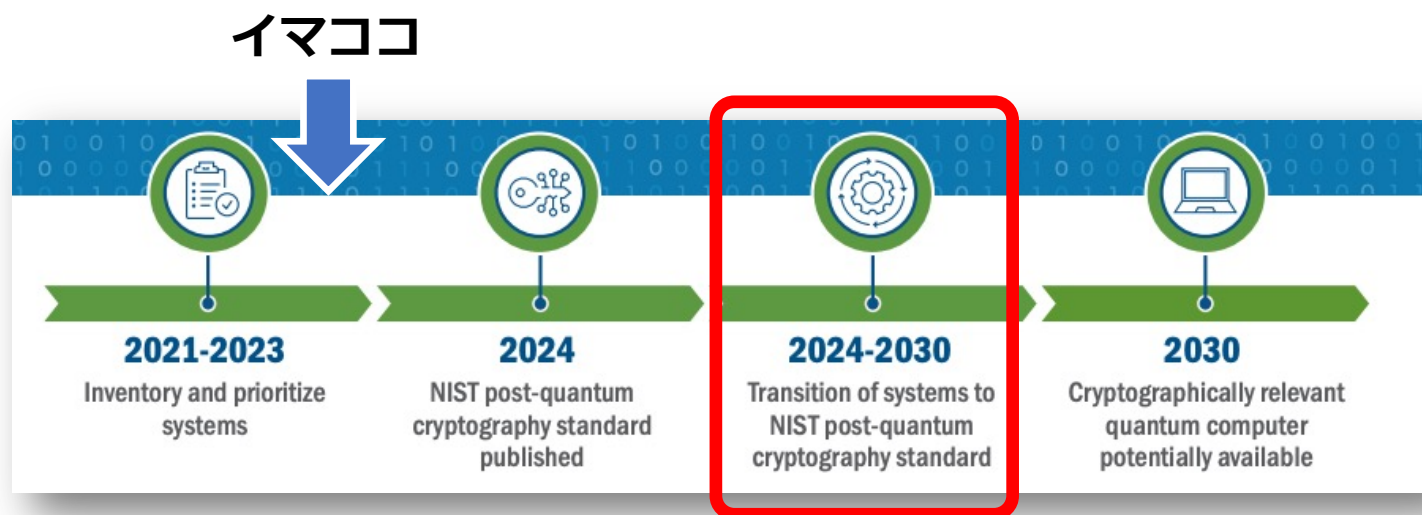
This document adds a new signing algorithm, **Ed25519-SHA256**, to "DomainKeys Identified Mail (DKIM) Signatures" ([RFC 6376](#)). DKIM verifiers are required to implement this algorithm.

EdDSA
※ ECDSAでないことに注意

<https://datatracker.ietf.org/doc/html/rfc8463>

暗号の2030年問題：PQCへの移行

- 「PQCへの暗号移行」の期日が2030年 ⇨ 「暗号の2030年問題」
- NISTが**2024年にPQCに関する標準仕様を公開**
- 2030年までに暗号移行を実行（あと6年弱！！）
 - 守るべきデータは？ 移行するシステムの順番は？ セキュリティレベルは？ など決定する必要がある



DHS 「Preparing for Post-Quantum Cryptography: Infographic」 より

https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

- 2016年にNISTがPQC標準化計画の発表を行い、2022年7月にRound 3の結果として**4つのアルゴリズムが選定**
- Round 4として標準化が見送られた4方式に対して追加評価が行われており、**少なくとも1方式は選定**される方針。

	公開鍵暗号/鍵共有	デジタル署名
選定アルゴリズム (2022年)	• CRYSTALS-KYBER	• CRYSTALS-DILITHIUM • FALCON • SPHINCS+
Round 4（追加評価）	• BIKE • Classic McEliece • HQC • SIKE	—

- 現在、上記に加えて「Additional Digital Signature Schemes - Round 1」が実施されている。

- Round4として公開鍵暗号/鍵共有は検討されているが・・・
検討中のデジタル署名候補は残っていない！ 格子ベース以外を急募

PROJECTS

PQC DIGITAL SIGNATURE SCHEMES

Post-Quantum Cryptography: Digital Signature Schemes

f t

Round 1 Additional Signatures

Official comments on the **First Round Signatures** should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the [pqc-forum Google group subscribers](#) will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

[History of Round 1 Updates](#)

Code-based Signatures

Algorithm	Algorithm Information	Submitters	Comments
CROSS Codes and Restricted Objects Signature Scheme	Specification IP Statements Zip file (11 MB) Website	Marco Baldi Alessandro Barengli Sebastian Bitzer Patrick Karl Felice Manganiello Alessio Pavoni Gerardo Pelosi Paolo Santini Jonas Schupp Freeman Slaughter Antonia Wachter-Zeh	Submit Comment View Comments

PROJECT LINKS

Overview

News & Updates

ADDITIONAL PAGES

Standardization of Additional Digital Signature Schemes

Call for Proposals

Example Files

Workshops and Timeline

Round 1 Additional Signatures

Email List (PQC Forum)

PQC Standardization: Main Project

CONTACTS

PQC Crypto Technical Inquiries

pqc-comments@nist.gov

Dr. Lily Chen

Dr. Dustin Moody

dustin.moody@nist.gov

- 現在、40方式が提案中
- 実現手段も様々！
 - 符号ベース、同型写像、多変数多項式など6種類以上

<https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures>

具体的なPQCアルゴリズムとデータサイズ

※ 128bit安全相当を実現した際のデータサイズ

カテゴリー	アルゴリズム名	利用する問題	データサイズ (byte)		
			公開鍵	秘密鍵	暗号文/署名
公開鍵暗号 /KEM	CRYSTALS-KYBER	Module-LWE問題	736	1,632	800
	BIKE	QC-MDPC符号のSDP	2,542	267	2,542
	Classic McEliece	Gappa符号のSDP	319,488	9,216	128
	HQC	Quasi-Cycle符号のSDP	2,819	2,859	5,622
デジタル署名	CRYSTALS-DILITHIUM	Module-LWE問題	1,184	2,800	2,044
	FALCON	SIS問題	897	4,097	690
	SPHINCS+	ハッシュ関数の衝突探索問題	32	64	8,080

“https://www.jstage.jst.go.jp/article/isciesci/65/2/65_60/_pdf/-char/ja”の第1表より作成

- DKIM視点では「DNSのUDPパケット (512 byte=4096bit)」の制約があるので、このまま素直に移行は厳しそう

- NISTは2023年8月24日に初版が公開済み！

UPDATES

2023

Comments Requested on Three Draft FIPS for Post-Quantum Cryptography

August 24, 2023



NIST requests comments on the initial public drafts of three Federal Information Processing Standards (FIPS):

1. FIPS 203, [Module-Lattice-Based Key-Encapsulation Mechanism Standard](#)
2. FIPS 204, [Module-Lattice-Based Digital Signature Standard](#)
3. FIPS 205, [Stateless Hash-Based Digital Signature Standard](#)

These proposed standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions to the NIST Post-Quantum Cryptography Standardization Project.

The public comment period for these three drafts is open through November 22, 2023. See the publication details (linked above) to download the drafts and for information on submitting comments.

FIPS 203 ~ 205 の3つ公開

- 暗号化/KEM
 - 格子ベース
- デジタル署名
 - 格子ベース
 - ハッシュ関数ベース

<https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography>

いきなり「PQCへの移行」実施する？

- 4つのアルゴリズムが存在するので「PQCへの完全移行」ができるのでは？ という疑問が残る

PQCの安全性

製品/実装の準備

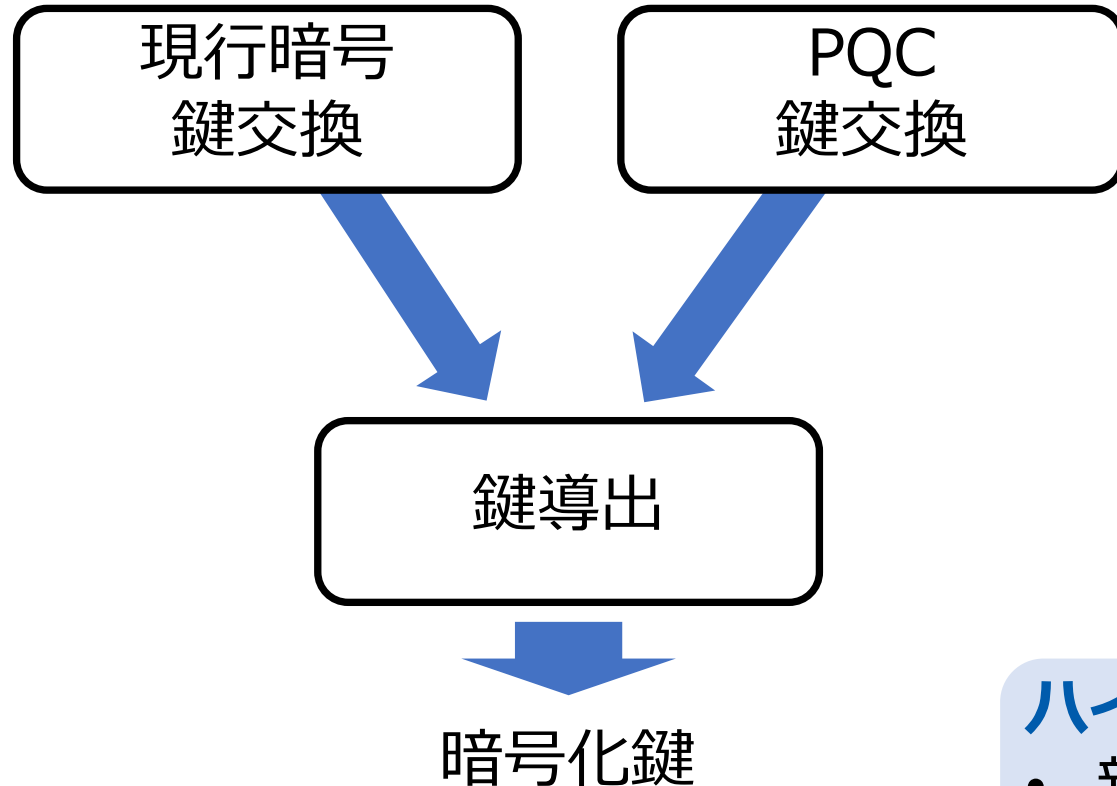
モヤモヤする点

既存環境への影響

このモヤモヤを解決するのが「**ハイブリッドモード**」

- 多くの標準化団体等でPQCへの暗号移行に関連して、ハイブリッドモードが取り上げられているが、**統一された定義は存在しない。**
- NIST
 - 「利用される**コンポーネントが一つでも壊れていない限り、期待されたセキュリティプロパティを確保**すること」と「Backwards compatibility（下位互換性）」が大事
- IETF
 - 現行暗号によって達成される安全性にPQC の性質を付与し、それぞれのアルゴリズムで独立した処理するのではなく、**どちらかが安全ではない状態になっても、いずれかのアルゴリズムによって守られることが担保**されるような構成法

- 概念的には「現行暗号」と「PQC」をシンプルに組み合わせる



例えば、次のようなケースを考える
＜量子計算機が登場！＞

- 現行暗号は解読されるが、PQCは安全なので守られる

＜PQCに脆弱性が発見！＞

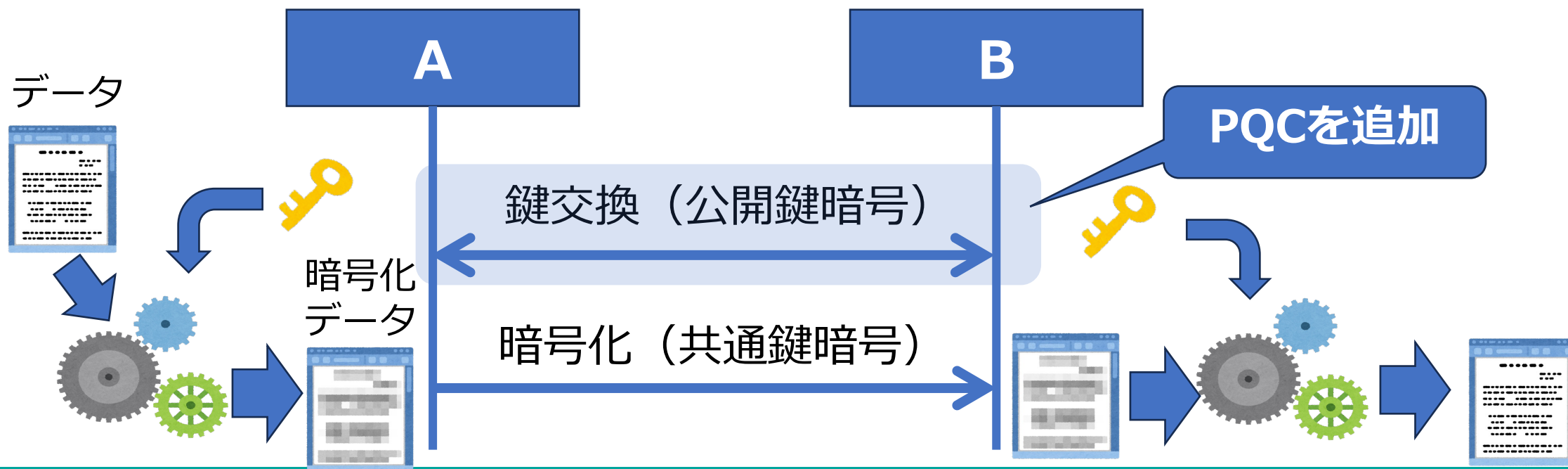
- PQCは機能しないが、長年利用されている現行暗号は安全なので守られる

ハイブリッドモードのメリット

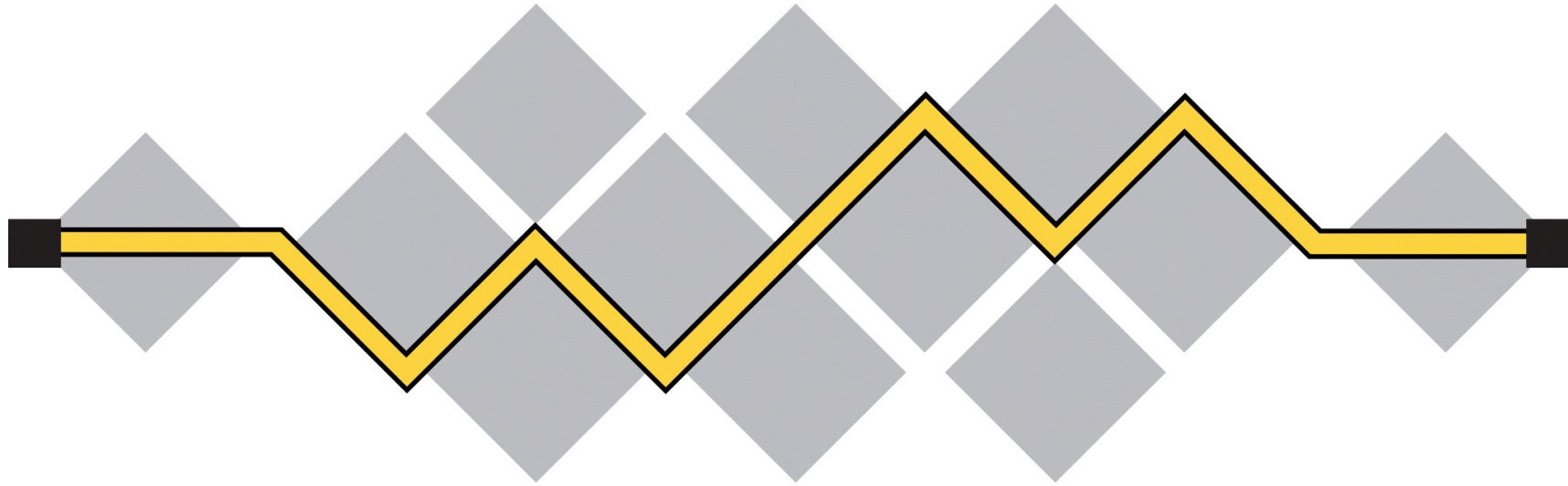
- 新技術であるPQCを実社会で運用することができ、改善を行える。

実社会での利用法は「**ハイブリッド暗号**」が主流。

- 「共通鍵暗号」と「公開鍵暗号」を組み合わせた暗号利用方法
- 構成技術の特徴は以下のとおり
 - 共通鍵暗号：処理が高速だが、安全な鍵交換（配布）が困難
 - 公開鍵暗号：処理は低速だが、鍵交換（配布）が容易
- 具体的な事例：SSL/TLS



- 暗号の危殆化
- 暗号移行を招く？！ 2つの「暗号の2030年問題」
- 我々を取り巻く環境



I E T F[®]

• Internet Engineering Task Force

• インターネットに関する技術の国際標準を策定する組織

• 理念

• “We reject kings, presidents and voting. We believe in *rough consensus* and *running code*.” David Clark (1992)

• 生産物

• RFC (Request for Comments) を発行
• インターネットを技術的な側面を支えている

• 活動

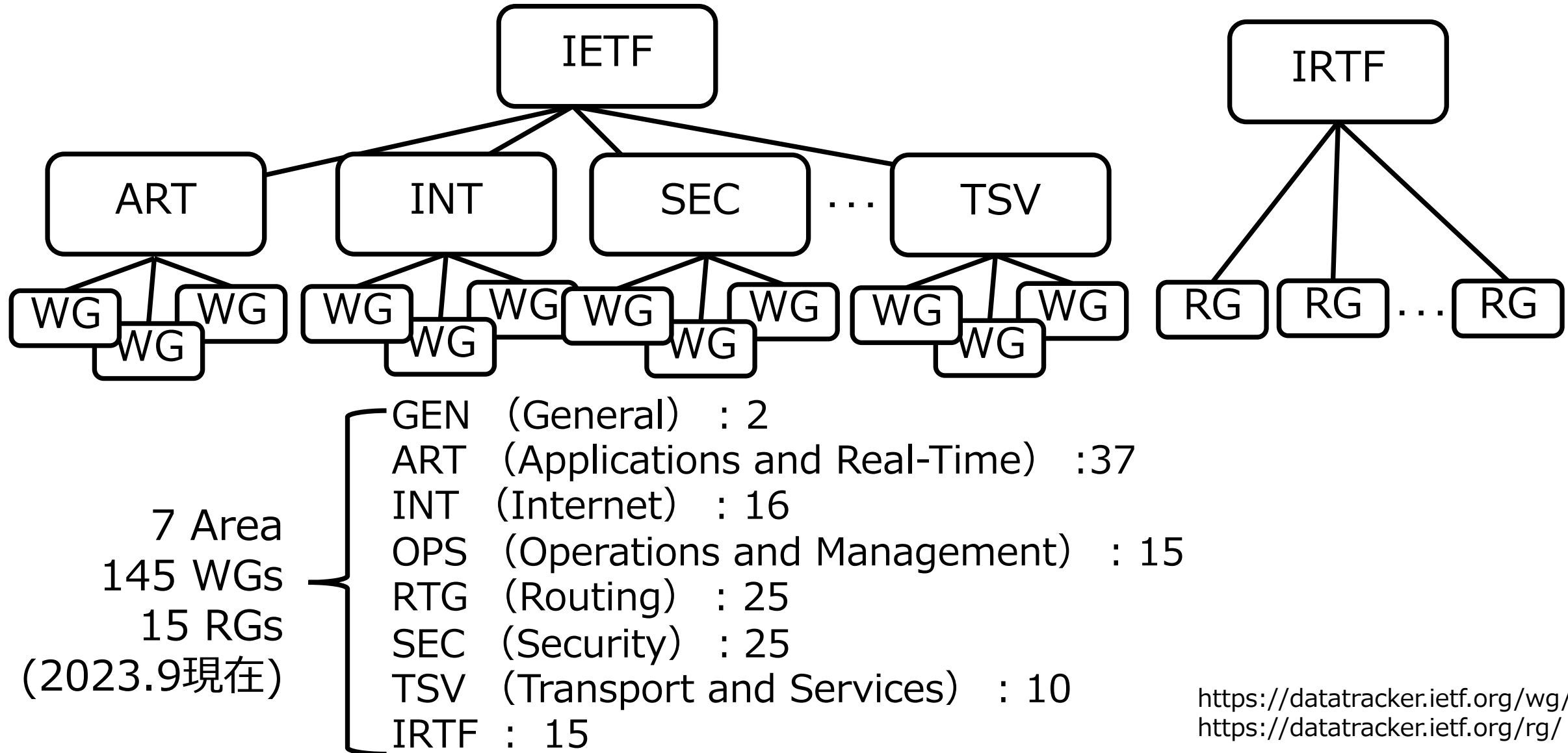
• 年3回開催 (3月、7月、11月) で1週間
• 参加者数: 1500~2000人
• 参加費: 右図参照⇒
• 参加資格: 誰でもOK

1986 年1月が
第1回!!

Onsite Registration Options			
	Super Early	Early	Standard
Week Pass	\$875 USD (\$1058.75 inc. VAT)	\$1095 USD (\$1324.95 inc. VAT)	\$1200 USD (\$1452.00 inc. VAT)
One-Day Pass	\$470 USD (\$568.70 inc. VAT)	\$470 USD (\$568.70 inc. VAT)	\$470 USD (\$568.70 inc. VAT)
Student Pass	\$150 USD (\$181.50 inc. VAT)	\$150 USD (\$181.50 inc. VAT)	\$150 USD (\$181.50 inc. VAT)
Hackathon Only	\$0 USD (\$0.00 inc. VAT)	\$0 USD (\$0.00 inc. VAT)	\$0 USD (\$0.00 inc. VAT)
	Best Available Rate until 18 Sep UTC 23:59	Available until 23 Oct UTC 23:59	Available Anytime

Remote Registration Options			
	Super Early	Early	Standard
Week Pass	\$250 USD	\$310 USD	\$360 USD
One-Day Pass	\$140 USD	\$140 USD	\$140 USD
Student Pass	\$55 USD	\$55 USD	\$55 USD
Hackathon Only	\$0 USD	\$0 USD	\$0 USD
	Best Available Rate until 18 Sep UTC 23:59	Available until 23 Oct UTC 23:59	Available Anytime

<https://registration.ietf.org/118/>



IETF概要 (3/3)

- IETF/IRTFで主にPQCが関係するWG/RGは以下のとおり

	エリア	代表的なWG
IETF	GEN	gendispatch, shmoo
	ART	httpbis, satp, uta, cbor etc.
	INT	6man, 6lo, lpwan, lwig etc.
	OPS	iotops, dnsop, v6ops etc.
	RTG	idr, manet, ospf, roll etc.
	SEC	privacypass, tls, rats, mls, lake, pquip etc.
	TSV	quic, tcpm etc.
IRTF		pearg, t2trg, ufmrg, cfrg etc.

PQC移行を検討

暗号自体を検討

pquip (Post-Quantum Use In Protocols)

- 2023年3月開始。PQC移行の問題、IETFでのPQC対応について議論
 - PQCへの移行をサポートするための運用や設計ガイドラインを作成

The screenshot shows the IETF Datatracker page for the Post-Quantum Use In Protocols (pquip) Working Group. The page includes a navigation bar with links for About, Documents, Meetings, History, Photos, Email expansions, and List archive. The main content area is divided into sections for WG information, Personnel, Mailing list, Chat, Charter for Working Group, and Milestones.

Post-Quantum Use In Protocols (pquip)		
WG	Name	Post-Quantum Use In Protocols
	Acronym	pquip
	Area	Security Area (sec)
	State	Active
	Charter	charter-ietf-pquip-01 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Grand list of WGs and protocols looking at PQC algorithms
Personnel	Chairs	Paul E. Hoffman , Sofia Ceil
	Area Director	Roman Danyliw
Mailing list	Address	pqc@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/pqc
	Archive	https://mailarchive.ietf.org/arch/browse/pqc/
Chat	Room address	https://zulip.ietf.org/#narrow/stream/pquip

Charter for Working Group

Some IETF protocols rely upon cryptographic mechanisms that are considered secure given today's "classical computers" but would be vulnerable to attacks by a Cryptographically Relevant Quantum Computer (CRQC). These mechanisms rely upon algorithms based on integer factorization or the discrete logarithm problem. Outside of the IETF, active work is underway to develop and validate Post-Quantum Cryptography (PQC) mechanisms that are expected to be resilient to the cryptanalysis capabilities of future CRQCs (e.g., CFRG, US NIST). Select IETF WGs (e.g., LAMPS, TLS, IPSECME, COSE) have already begun standardizing revised protocol behaviors. The focus of Post-Quantum Use in Protocols (PQUIP) WG is to support this growing body of work in the IETF to facilitate the evolution of IETF protocols and document associated operational guidance with respect to PQC.

The WG will provide a standing venue to discuss PQC (operational and engineering) transition issues and experiences to date relevant to work in the IETF. The WG will also provide a venue of last resort to discuss PQC-related issues in IETF protocols that have no associated maintenance WGs. This WG will not update existing protocols, specify new protocols, define new cryptographic mechanisms, or assess whether a given cryptographic mechanism is quantum-resistant.

The WG will document operational and design guidance which supports PQC transition. The general process of elaboration through documentation will be for issues to be identified and discussed on the mailing list, and presentations made at WG meetings. When topics merit more coherent documentation, the WG will adopt documents to capture the information in Internet-Drafts. If the working group consensus is that the material of the Internet-Draft is generally useful for archival purposes, the WG will seek publication of the work items as Informational or Best Current Practices RFCs. At any point, from early discussion of topics through later documentation stages, the WG may identify a more appropriate WG for the matter, and with coordination, dispatch it there.

The output of this WG is expended to inform protocol work and guidance developed by other WGs in the IETF. Consistent with other IETF WGs, this WG will also rely on outside entities (e.g., CFRG) to define and assess new PQC mechanisms.

The IESG is establishing this working group on an experimental basis, and in 2 years, the IESG intends to review it for rechartering to continue or else closure.

Milestones

Date	Milestone	Associated documents
May 2023	WG Adoption of an Informational document on "PQC for engineers"	
Apr 2023	WG Adoption of an Informational document that defines terminology for (hybrid) PQC schemes	

<https://datatracker.ietf.org/wg/pquip/about/>

- IETF117（2023年7月開催）でPQCへの移行に必要な情報が共有

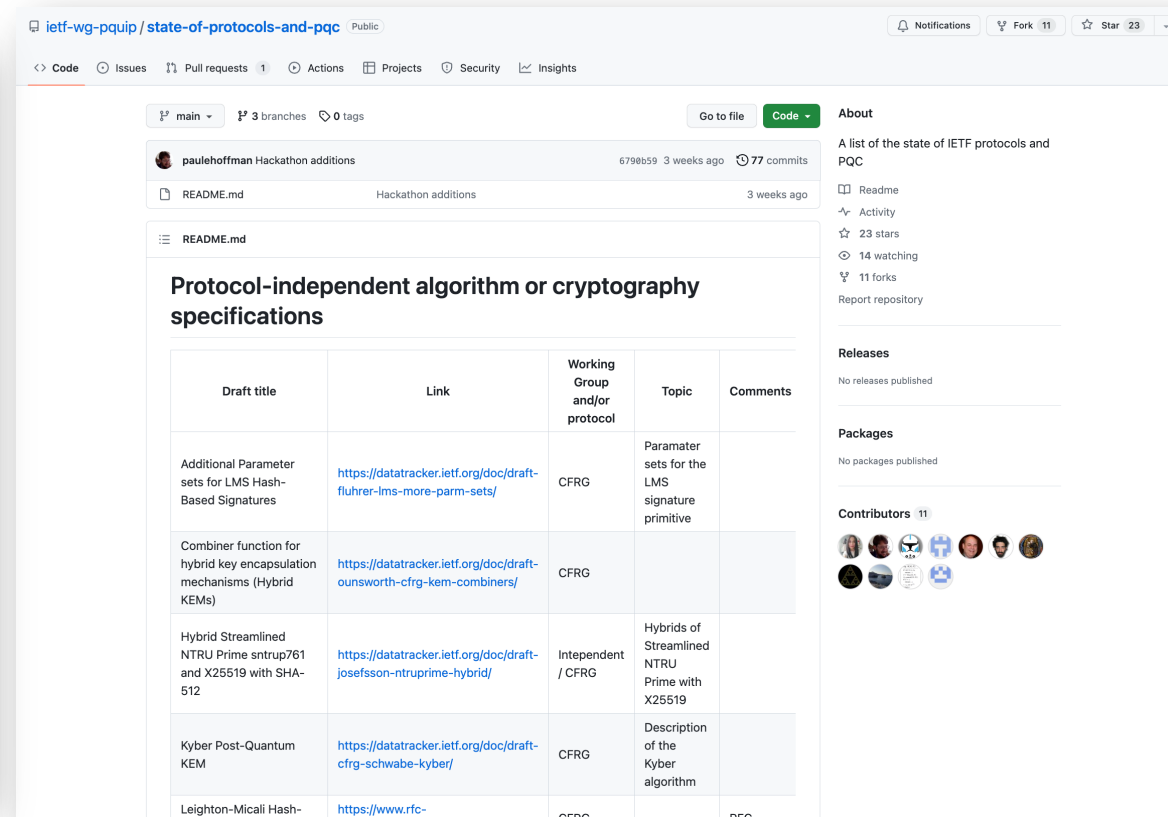
Terminology for Post-Quantum Traditional Hybrid Schemes

[draft-ietf-pquip-pqt-hybrid-terminology](https://datatracker.ietf.org/meeting/117/materials/slides-117-pquip-pqt-hybrid-terminology-00)

PQUIP – IETF 117 – 25th July 2023

1

<https://datatracker.ietf.org/meeting/117/materials/slides-117-pquip-pqt-hybrid-terminology-00>



GitHub repository: ietf-wg-pquip / state-of-protocols-and-pqc

Protocol-independent algorithm or cryptography specifications

Draft title	Link	Working Group and/or protocol	Topic	Comments
Additional Parameter sets for LMS Hash-Based Signatures	https://datatracker.ietf.org/doc/draft-fluhrer-lms-more-param-sets/	CFRG	Parameter sets for the LMS signature primitive	
Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)	https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/	CFRG		
Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512	https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-hybrid/	Independent / CFRG	Hybrids of Streamlined NTRU Prime with X25519	
Kyber Post-Quantum KEM	https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/	CFRG	Description of the Kyber algorithm	
Leighton-Micali Hash	https://www.rfc-	CFRG		REC

<https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc>

- 将来のインターネットで利用する暗号技術を検討
 - いくつかPQCに関する検討が実施

Document	Date	Status	IPR	AD/Shepherd
Active Internet-Drafts (16 hits)				
draft-fluhrer-lms-more-param-sets-11 Additional Parameter sets for HSS/LMS Hash-Based Signatures	20 pages 2023-09-18	I-D Exists Active RG Document : Informational		
draft-irtf-cfrg-ristretto255-decaf448-08 The ristretto255 and decaf448 Groups	27 pages 2023-09-05	I-D Exists : EDIT Sent to the RFC Editor : Informational		Christopher A. Wood
draft-irtf-cfrg-vdaf-07 Verifiable Distributed Aggregation Functions	111 pages 2023-08-31	I-D Exists Active RG Document		
draft-irtf-cfrg-aegis-aead-04 The AEGIS Family of Authenticated Encryption Algorithms	36 pages 2023-07-24	I-D Exists Active RG Document : Informational		
draft-irtf-cfrg-cspace-08 CPace, a balanced composable PAKE	74 pages 2023-07-23	I-D Exists Active RG Document : Informational		
draft-irtf-cfrg-signature-key-blinding-04 Key Blinding for Signature Schemes	15 pages 2023-07-23	I-D Exists Active RG Document : Informational		
draft-irtf-cfrg-bbs-signatures-03 The BBS Signature Scheme	7	Related Internet-Drafts (8 hits)		
draft-irtf-cfrg-cryptography-specification-00 Guidelines for Writing Cryptography Specifications	2	draft-wahby-cfrg-hpke-kem-secp256k1-00 secp256k1-based DHKEM for HPKE	13 pages 2023-07-23	I-D Exists
draft-irtf-cfrg-frost-14 Two-Round Threshold Schnorr Signatures with FROST	6	draft-harvey-cfrg-mtl-mode-00 Merkle Tree Ladder Mode (MTL) Signatures	72 pages 2023-07-10	I-D Exists
draft-irtf-cfrg-rsa-blind-signatures-14 RSA Blind Signatures	3	draft-ounsworth-cfrg-kem-combiners-04 Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)	14 pages 2023-07-08	I-D Exists
draft-irtf-cfrg-dnbpke-01 Deterministic Nonce-less Hybrid Public Key Encryption	3	draft-amjad-cfrg-partially-blind-rsa-01 Partially Blind RSA Signatures	24 pages 2023-07-06	I-D Exists
draft-irtf-cfrg-kangarootwelve-11 KangarooTwelve and TurboSHAKE	2	draft-mattsson-cfrg-aes-gcm-sst-00 Galois Counter Mode with Secure Short Tags (GCM-SST)	16 pages 2023-05-05	I-D Exists
draft-irtf-cfrg-opaque-11 The OPAQUE Asymmetric PAKE Protocol	7	draft-westerbaan-cfrg-hpke-xyber768d00-02 X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE	19 pages 2023-05-04	I-D Exists
draft-irtf-cfrg-aead-limits-07 Usage Limits on AEAD Algorithms	2	draft-fluhrer-cfrg-ntru-01 NTRU Key Encapsulation	16 pages 2023-05-02	I-D Exists
draft-irtf-cfrg-voprf-21 Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups	7	draft-bar-cfrg-spake2plus-08 SPAKE2+, an Augmented PAKE	30 pages 2022-05-05	I-D Exists : AUTH48-DONE Sent to the RFC Editor : Informational
draft-irtf-cfrg-spake2-26 SPAKE2, a PAKE	1	draft-irtf-cfrg-spake2-26 SPAKE2, a PAKE		Elit Lear

<https://datatracker.ietf.org/rg/cfrg/about/>

- ・ ハイブリッドモードについて詳細を把握したい方へ

2020年度暗号技術関連の調査報告

年度	報告書名	著者名	報告書文書番号
2020	デジタル署名EdDSAで使われている曲線の安全性に関する調査及び評価	安田 雅哉	CRYPTREC EX-3001-2020 
2020	デジタル署名EdDSAの構成の安全性に関する調査および評価	藤崎 英一郎	CRYPTREC EX-3002-2020 
2020	CRYPTREC Review of EdDSA	Steven D. Galbraith	CRYPTREC EX-3003-2020 
2020	ハイブリッドモードの技術動向調査	株式会社レピダム	CRYPTREC EX-3004-2020 
2020	Shorのアルゴリズム実装動向調査	高安 敦	CRYPTREC EX-3005-2020 

↑ ページトップへ戻る

- ・ ハイブリッドモードの技術動向を整理
 - 標準化動向
 - 利用可能なアルゴリズム候補
 - ハイブリッドモードの取り扱い
 - 安全性及び評価 など

https://www.cryptrec.go.jp/ex_reports.html

- PQC関連やIETFにおける最新の技術動向が気になる方へ



- GMOイエラエの技術ブログでPQC関連の技術動向は随時発信していきます！

<https://gmo-cybersecurity.com/blog/ietf117-pquip-report/>

「耐量子計算機暗号（PQC）のココントコ」として、お話しさせていただきました。

- なんでPQCが必要になったの？
- 暗号アルゴリズムの安全性
 - 暗号の危殆化とは？
- 耐量子計算機暗号（PQC）とは？
- 暗号移行とは？
 - 我々は暗号移行というイベントは未体験なのか？
 - 2つの「暗号の2030年問題」
- IETFでのPQCに関する動向

何か気になることなどあれば・・・

- E-mail
 - satoru.kanno@gmo-cybersecurity.com
- SNS
 - X (旧 Twitter)
 - <https://twitter.com/satorukanno>
 - Facebook
 - <https://www.facebook.com/satoru.kanno>

お気軽にご連絡ください！

すべての人にインターネット

GMO