耐量子計算機暗号（PQC）への暗号移行に向けた技術動向

2023年9月21日

菅野　哲
GMOサイバーセキュリティ byイエラエ株式会社

自己紹介

- 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～）

会社紹介

- 「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/

本講演の概要を確認する

・講演２　（10:45-11:30）　：　耐量子計算機暗号（PQC）への暗号移行に向けた技術動向

講師　：　菅野 哲 氏（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）

概要　：　量子コンピュータによる暗号の危殆化を見据えてPQCへ暗号移行する際の対応策の1つとして「ハイブリッドモード」が提案されています。これは、現行暗号とPQCを併用することで、いずれかの暗号方式が安全でなくなった場合やPQCに完全移行していない状況であっても安全性を維持する方法です。本講演では、ハイブリッドモードの標準化に向けた動向や、オープンソースソフトウェア（OSS）など技術面の実装状況について紹介します。

今回の講演のポイントを整理する

- 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？
  - 暗号移行とハイブリッドモードの関係は？
- 2023年現在、我々を取り巻くPQCに関する環境とは？
  - 標準化仕様、OSSなど

Agenda

- 暗号の危殆化
- 暗号移行
- 我々を取り巻く環境

Agenda

- 暗号の危殆化
- 暗号移行
- 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、**量子計算機**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）

暗号の危殆化への対処方法とは

「**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

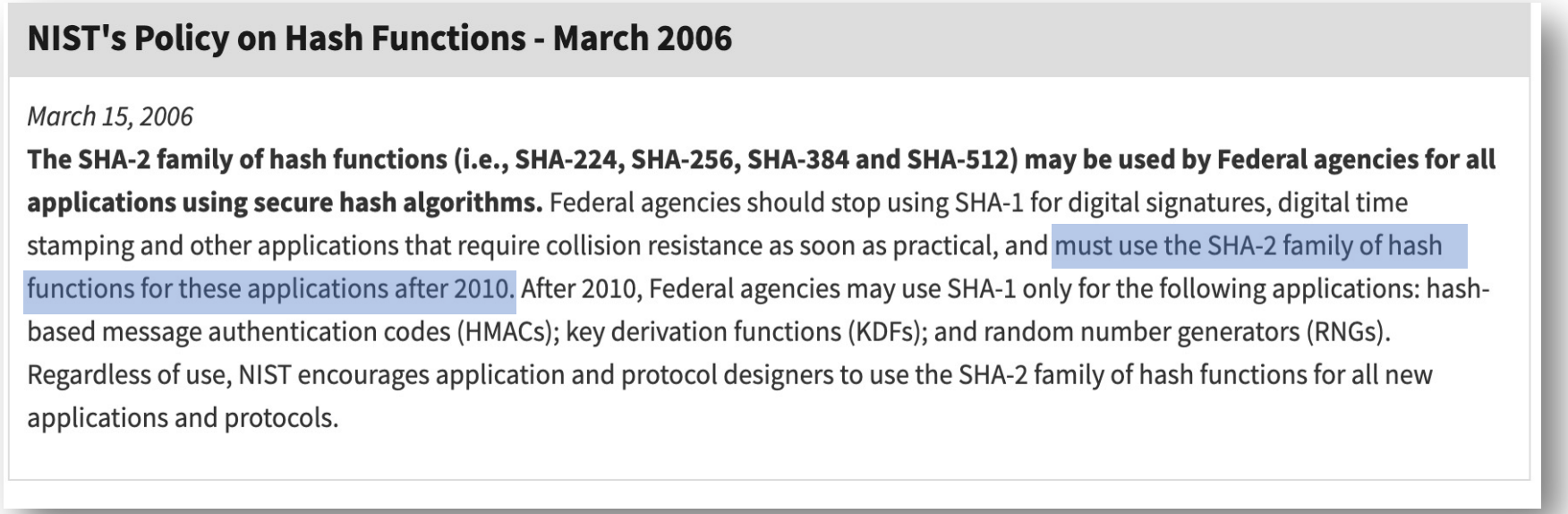
影響範囲の例：
仮想通貨、ブロックチェーン、情報家電製品、 OS、アプリケーション、ネットワーク機器、 ATM/レジスターなど

Agenda

- 暗号の危殆化
- 暗号移行
- 我々を取り巻く環境

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

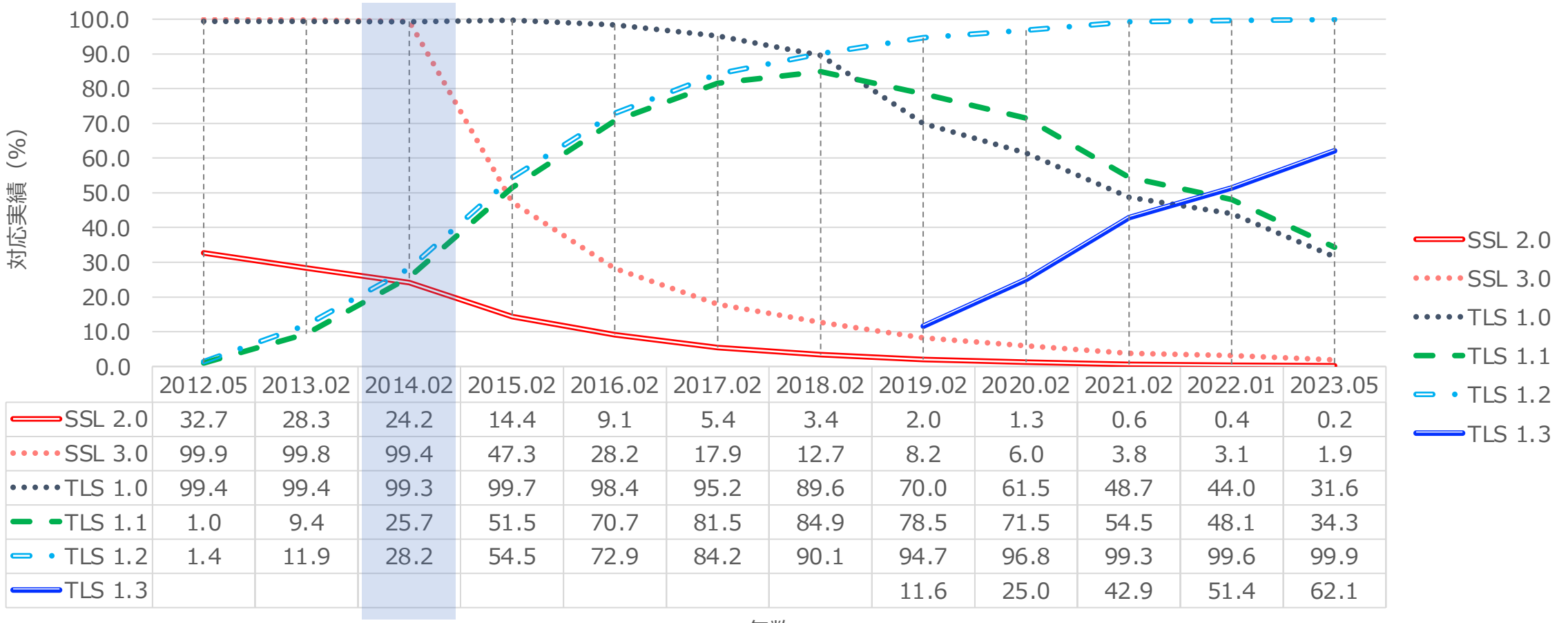
The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance 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

暗号移行の事例: TLS 1.2

- 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...

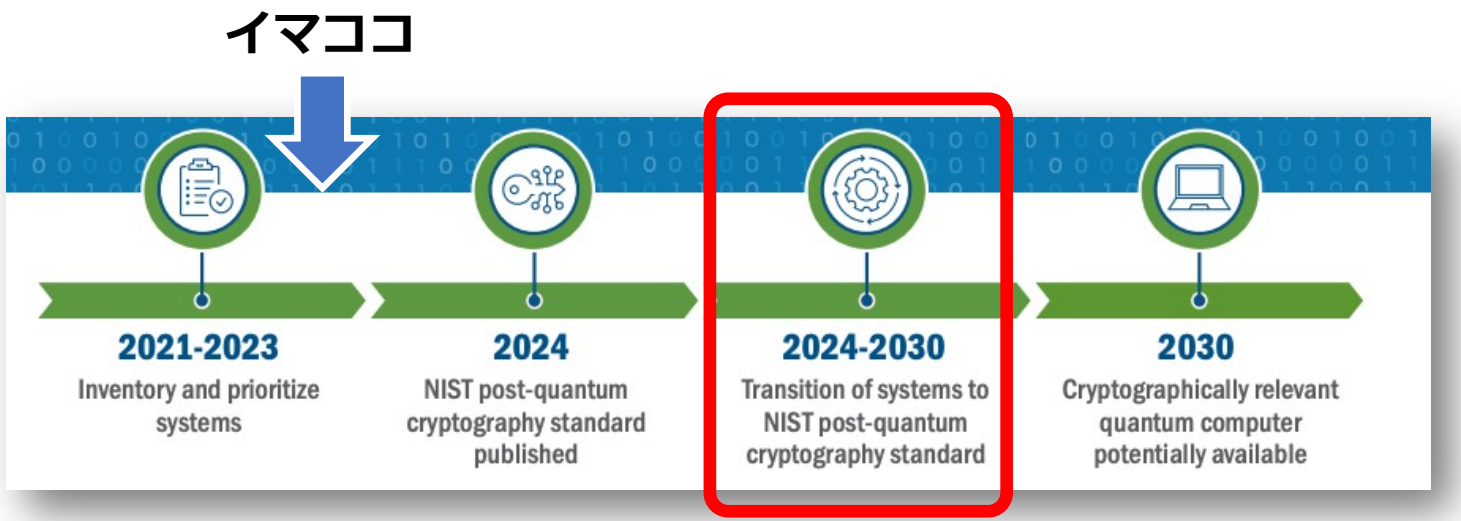


	2012.05	2013.02	2014.02	2015.02	2016.02	2017.02	2018.02	2019.02	2020.02	2021.02	2022.01	2023.05
SSL 2.0	32.7	28.3	24.2	14.4	9.1	5.4	3.4	2.0	1.3	0.6	0.4	0.2
SSL 3.0	99.9	99.8	99.4	47.3	28.2	17.9	12.7	8.2	6.0	3.8	3.1	1.9
TLS 1.0	99.4	99.4	99.3	99.7	98.4	95.2	89.6	70.0	61.5	48.7	44.0	31.6
TLS 1.1	1.0	9.4	25.7	51.5	70.7	81.5	84.9	78.5	71.5	54.5	48.1	34.3
TLS 1.2	1.4	11.9	28.2	54.5	72.9	84.2	90.1	94.7	96.8	99.3	99.6	99.9
TLS 1.3								11.6	25.0	42.9	51.4	62.1

SSL Labs Pulseのデータにより講演者がグラフ化

PQCへの移行は「暗号の2030年問題」

- 「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！！）
    - 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

NIST PQC標準化

- 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。

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**」

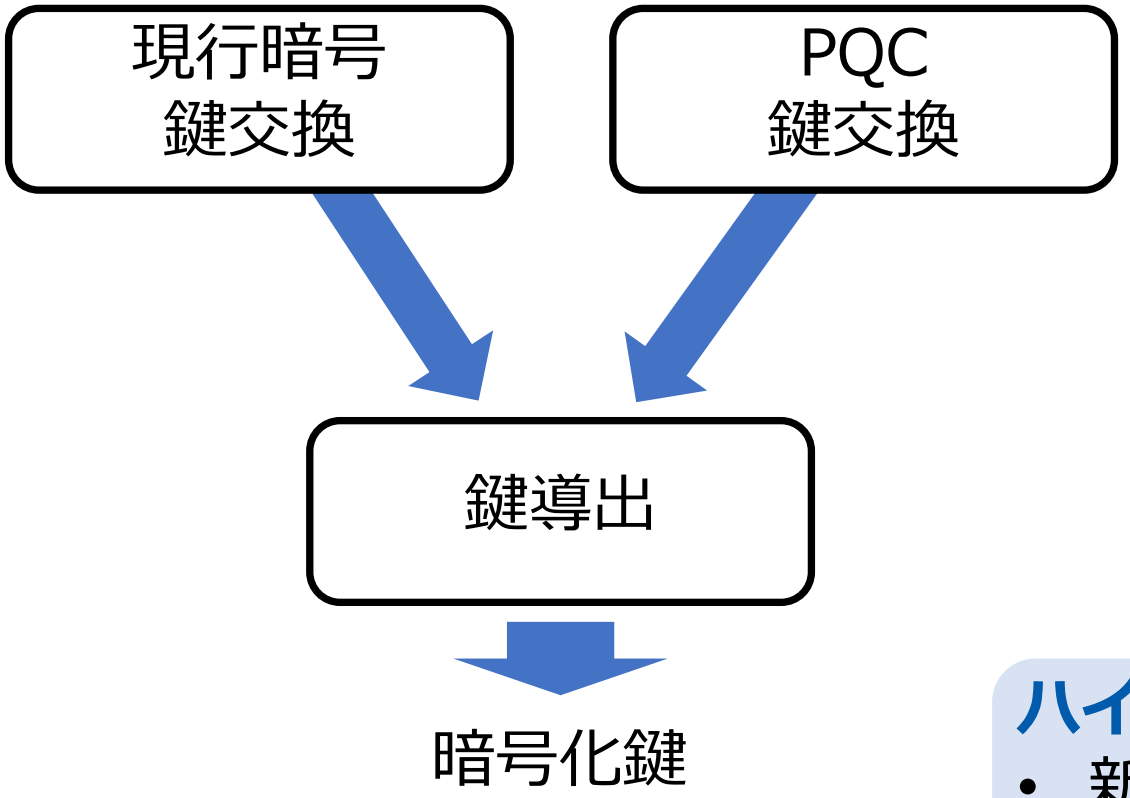
ハイブリッドモードとは

- 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

ハイブリッドモードの構成法：鍵交換

- 概念的には「現行暗号」と「PQC」をシンプルに組合わせる



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

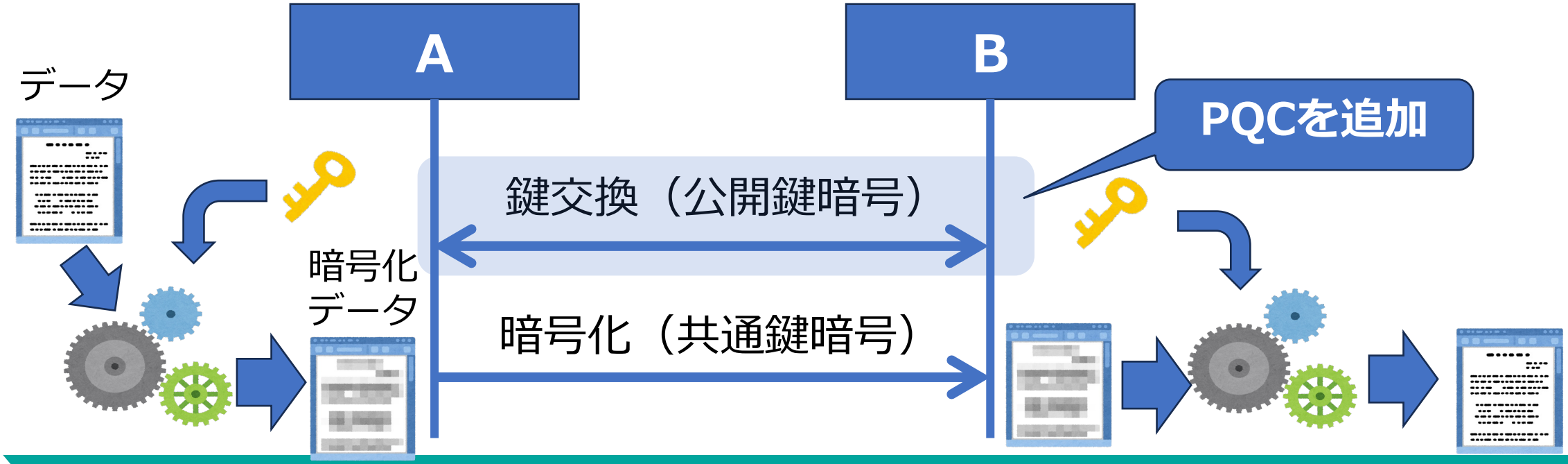
＜PQCに脆弱性が発見！＞
- PQCは機能しないが、長年利用されている現行暗号は安全なので守られる

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。

実社会でのハイブリッドモード

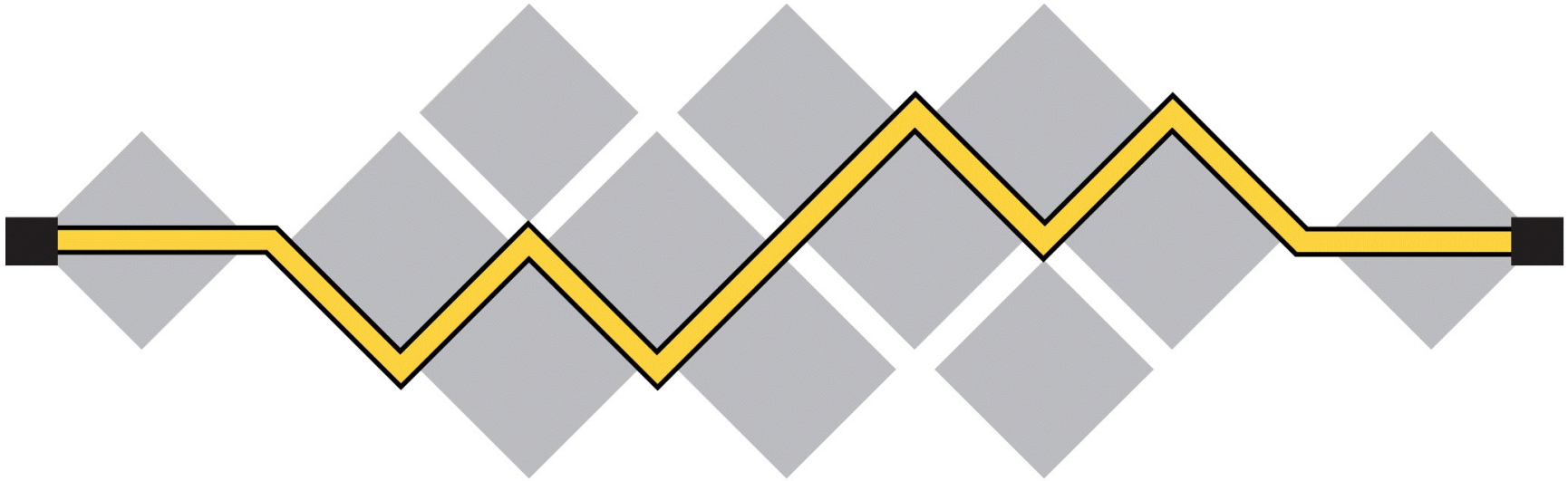
実社会での利用法は「**ハイブリッド暗号**」が主流。

- 「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



Agenda

- 暗号の危殆化
- 暗号移行
- 我々を取り巻く環境

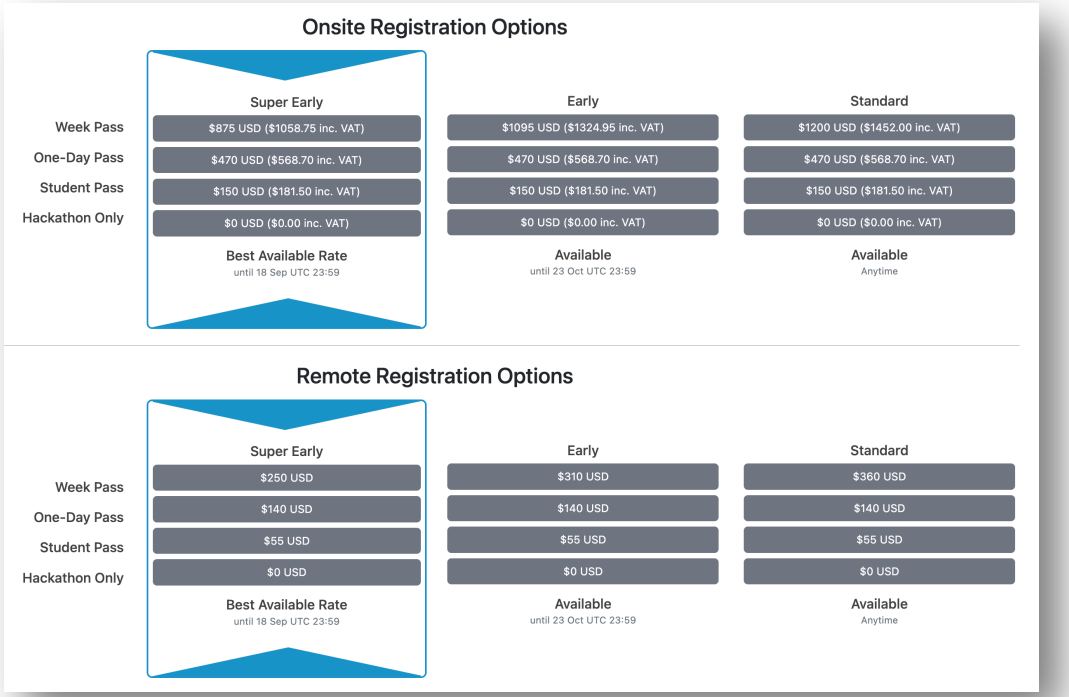


IETF®

IETF概要（1/5）

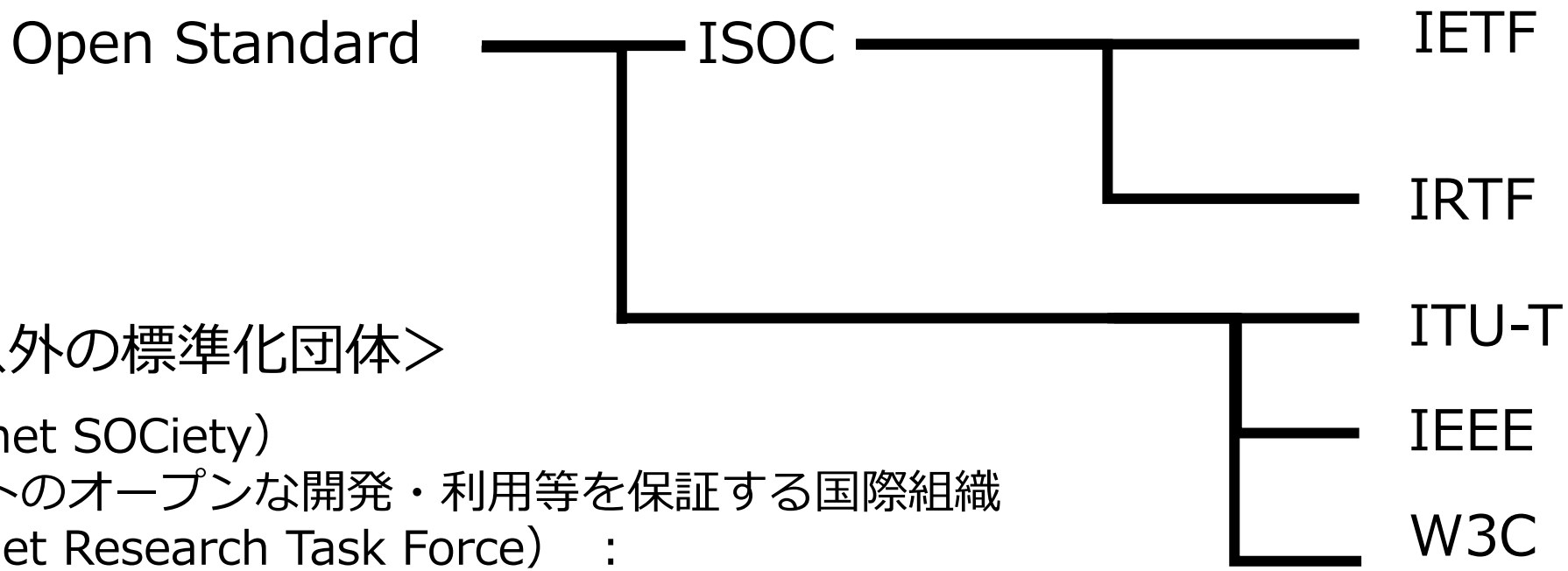
- **I**nternet **E**ngineering **T**ask **F**orce
  - **インターネットに関する技術**の国際標準を策定する組織
- 理念
  - “We reject kings, presidents and voting. We believe in ***rough consensus*** and ***running code***.” David Clark (1992)
- 生産物
  - RFC （Request for Comments）を発行
    - インターネットを技術的な側面を支えている
- 活動
  - 年3回開催（3月、7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！！



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

IETF概要（2/5）



＜IETF/IRTF以外の標準化団体＞

- ISOC （Internet SOCiety）
  インターネットのオープンな開発・利用等を保証する国際組織
- IRTF （Internet Research Task Force） ：
  インターネットの未来において重要と思われる研究を推進する組織
- ITU-T：
  国際電気通信連合において通信分野の標準化策定を担当する電気通信標準化部門
- IEEE：
  アメリカに本部を持つ電気電子技術学会
- W3C：
  World Wide Webで使用される各種技術の標準化の推進を目的に設立された団体

IETF概要（3/5）

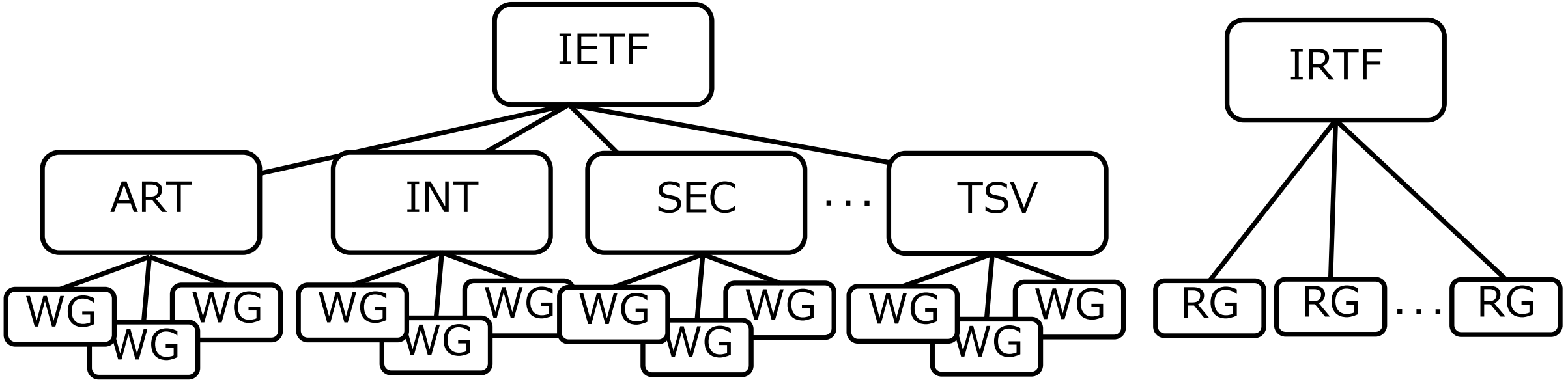
標準化スタイルはITU-Tはトップダウン、IETFはボトムアップ

トップダウン

ITU-T	IETF
Specification Oriented（まず仕様を決める）	Implementation Oriented（まずは実装をする）
Hard Specification（仕様は変わらない）	Soft Specification（仕様は変わっていく）
Quality of Service	Connectivity
Voting	Running Code & Rough Consensus
Membership	Volunteer

ボトムアップ

IETF概要（4/5）



7 Area
145 WGs
15 RGs
(2023.9現在)

- GEN （General） : 2
- ART （Applications and Real-Time） :37
- INT （Internet） : 16
- OPS （Operations and Management） : 15
- RTG （Routing） : 25
- SEC （Security） : 25
- TSV （Transport and Services） : 10
- IRTF : 15

https://datatracker.ietf.org/wg/
https://datatracker.ietf.org/rg/

IETF概要（5/5）

- IETF/IRTFで主にPQCが関係するWG/RGは以下のとおり

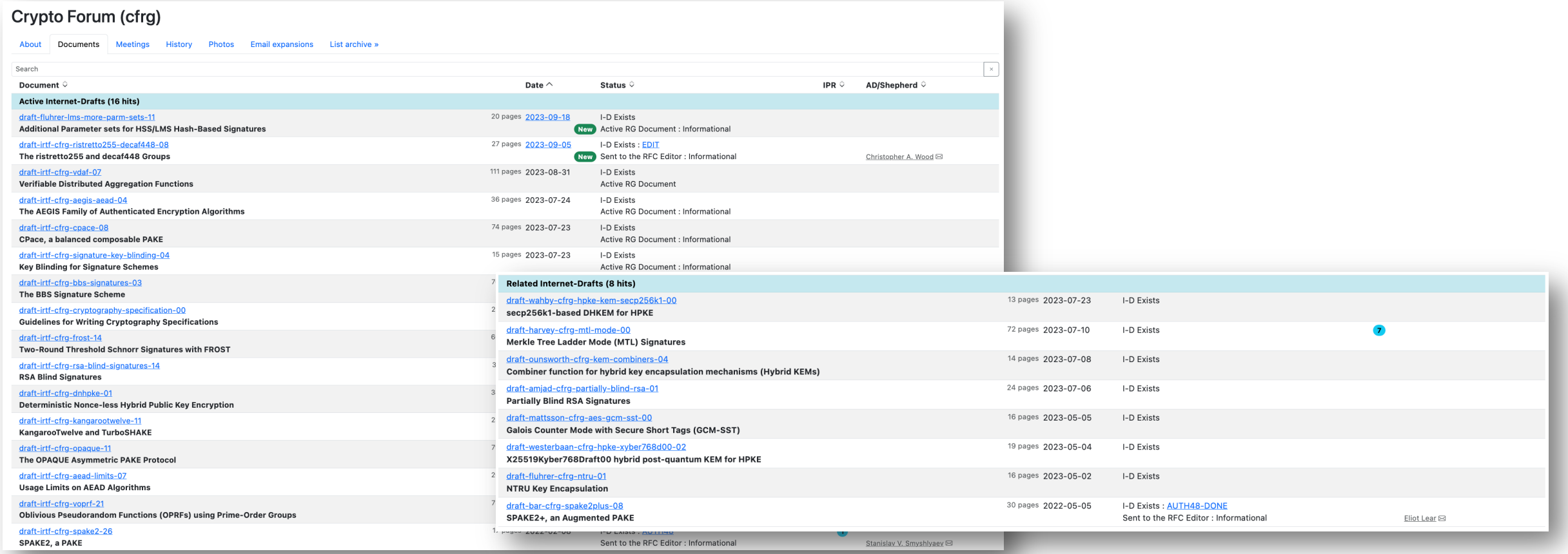
	エリア	代表的なWG
IETF	GEN	gendispatch, shmoo
	ART	httpbis, satp, uta, cbor etc.
	INT	6man, 6lo, lpwan, lwig etc.
	OPS	iotops, dnsop, v6ops etc.
	RTG	idr, manet, ospf, roll etc.
	SEC	privacypass, tls, rats, mls, lake, **pquip** etc.
	TSV	quic, tcpm etc.
IRTF		pearg, t2trg, ufmrg, **cfrg** etc.

PQC移行を検討

PQC自体を検討

cfrg (Crypto Forum)

- 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



Crypto Forum (cfrg)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

Search

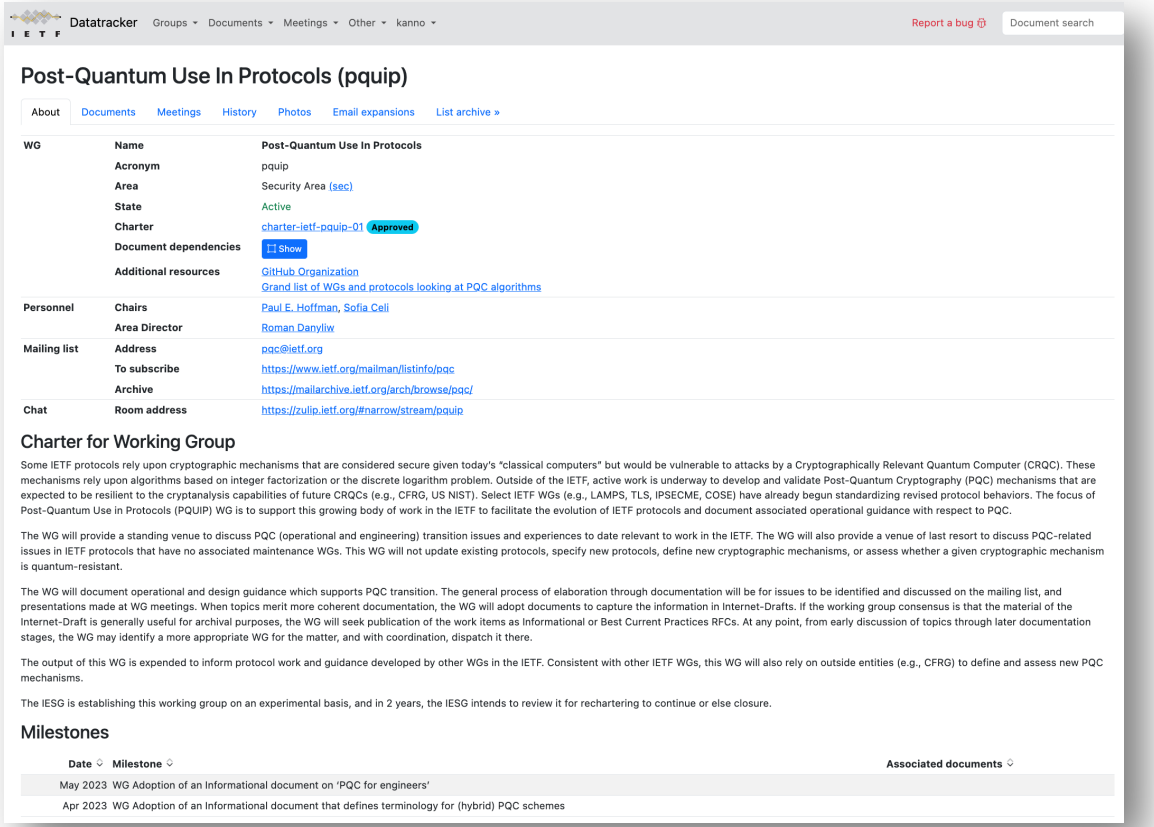
Document	Date	Status	IPR	AD/Shepherd
Active Internet-Drafts (16 hits)				
draft-fluhrer-lms-more-parm-sets-11 **Additional Parameter sets for HSS/LMS Hash-Based Signatures**	20 pages 2023-09-18 New	I-D Exists Active RG Document : Informational		
draft-irtf-cfrg-ristretto255-decaf448-08 **The ristretto255 and decaf448 Groups**	27 pages 2023-09-05 New	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-cpace-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			
draft-irtf-cfrg-cryptography-specification-00 **Guidelines for Writing Cryptography Specifications**	2			
draft-irtf-cfrg-frost-14 **Two-Round Threshold Schnorr Signatures with FROST**	6			
draft-irtf-cfrg-rsa-blind-signatures-14 **RSA Blind Signatures**	3			
draft-irtf-cfrg-dnhpke-01 **Deterministic Nonce-less Hybrid Public Key Encryption**	3			
draft-irtf-cfrg-kangarootwelve-11 **KangarooTwelve and TurboSHAKE**	2			
draft-irtf-cfrg-opaque-11 **The OPAQUE Asymmetric PAKE Protocol**	7			
draft-irtf-cfrg-aead-limits-07 **Usage Limits on AEAD Algorithms**	2			
draft-irtf-cfrg-voprf-21 **Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups**	7			
draft-irtf-cfrg-spake2-26 **SPAKE2, a PAKE**	1.	Sent to the RFC Editor : Informational		Stanislav V. Smyshlyaev

Related Internet-Drafts (8 hits)				
draft-wahby-cfrg-hpke-kem-secp256k1-00 **secp256k1-based DHKEM for HPKE**	13 pages	2023-07-23	I-D Exists	
draft-harvey-cfrg-mtl-mode-00 **Merkle Tree Ladder Mode (MTL) Signatures**	72 pages	2023-07-10	I-D Exists	7
draft-ounsworth-cfrg-kem-combiners-04 **Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)**	14 pages	2023-07-08	I-D Exists	
draft-amjad-cfrg-partially-blind-rsa-01 **Partially Blind RSA Signatures**	24 pages	2023-07-06	I-D Exists	
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-westerbaan-cfrg-hpke-xyber768d00-02 **X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE**	19 pages	2023-05-04	I-D Exists	
draft-fluhrer-cfrg-ntru-01 **NTRU Key Encapsulation**	16 pages	2023-05-02	I-D Exists	
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	Eliot Lear

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

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



Datatracker Groups Documents Meetings Other kanno Report a bug Document search

Post-Quantum Use In Protocols (pquip)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

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 Celi
	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.

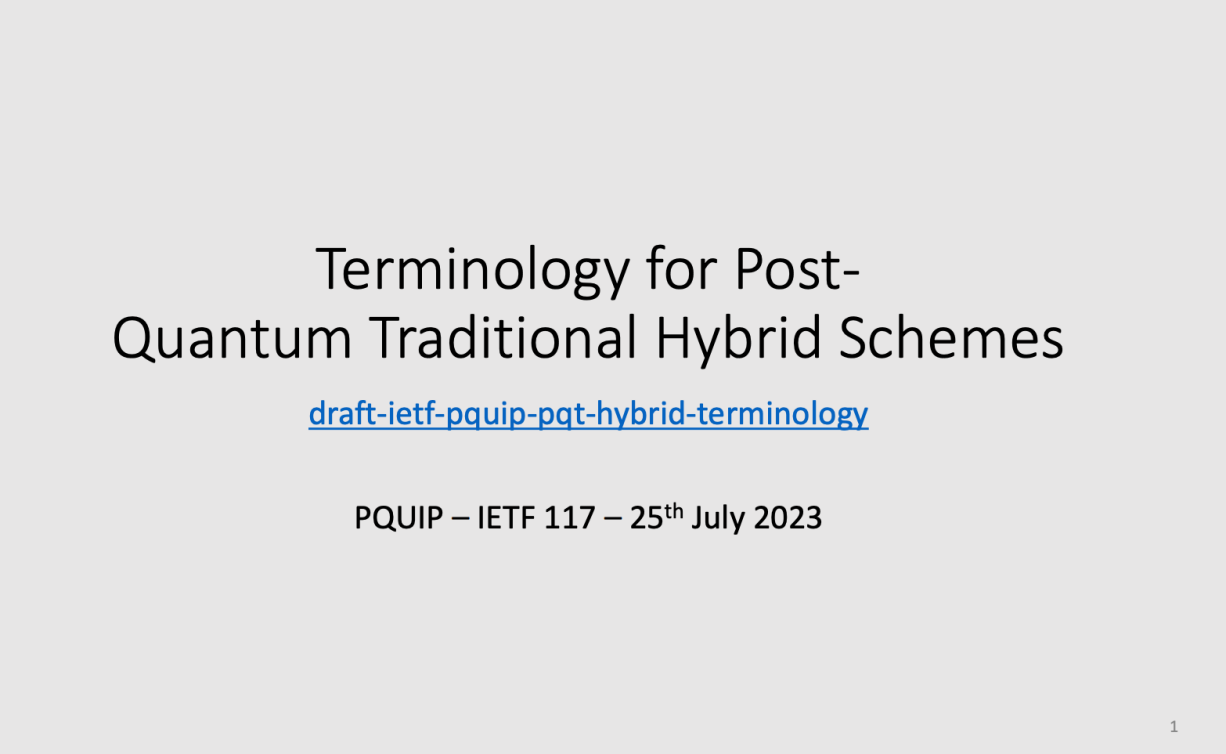
Milestones

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	

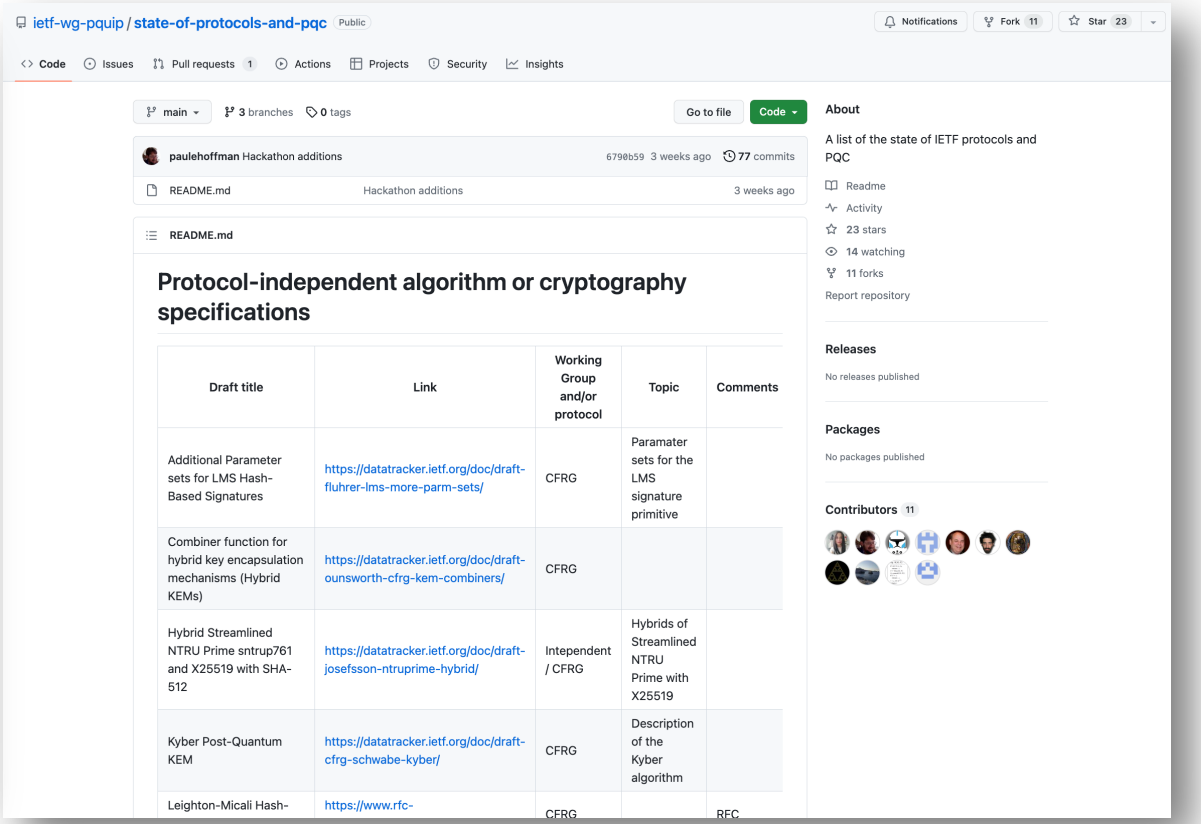
https://datatracker.ietf.org/wg/pquip/about/

pquipにおける技術動向

- IETF117（2023年7月開催）での発表をご紹介



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



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

ハイブリッドモードに関する標準化の進捗

GMO CYBER SECURITY IERAE

多くのInternet Draftは鍵交換が対象となっている

- X25519Kyber768Draft00 hybrid post-quantum key agreement
  - https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/
- Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)
  - https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/
- Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512
  - https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-hybrid/

など他多数

ハイブリッドモードに関するOSSの進捗

GMO CYBER SECURITY IERAE

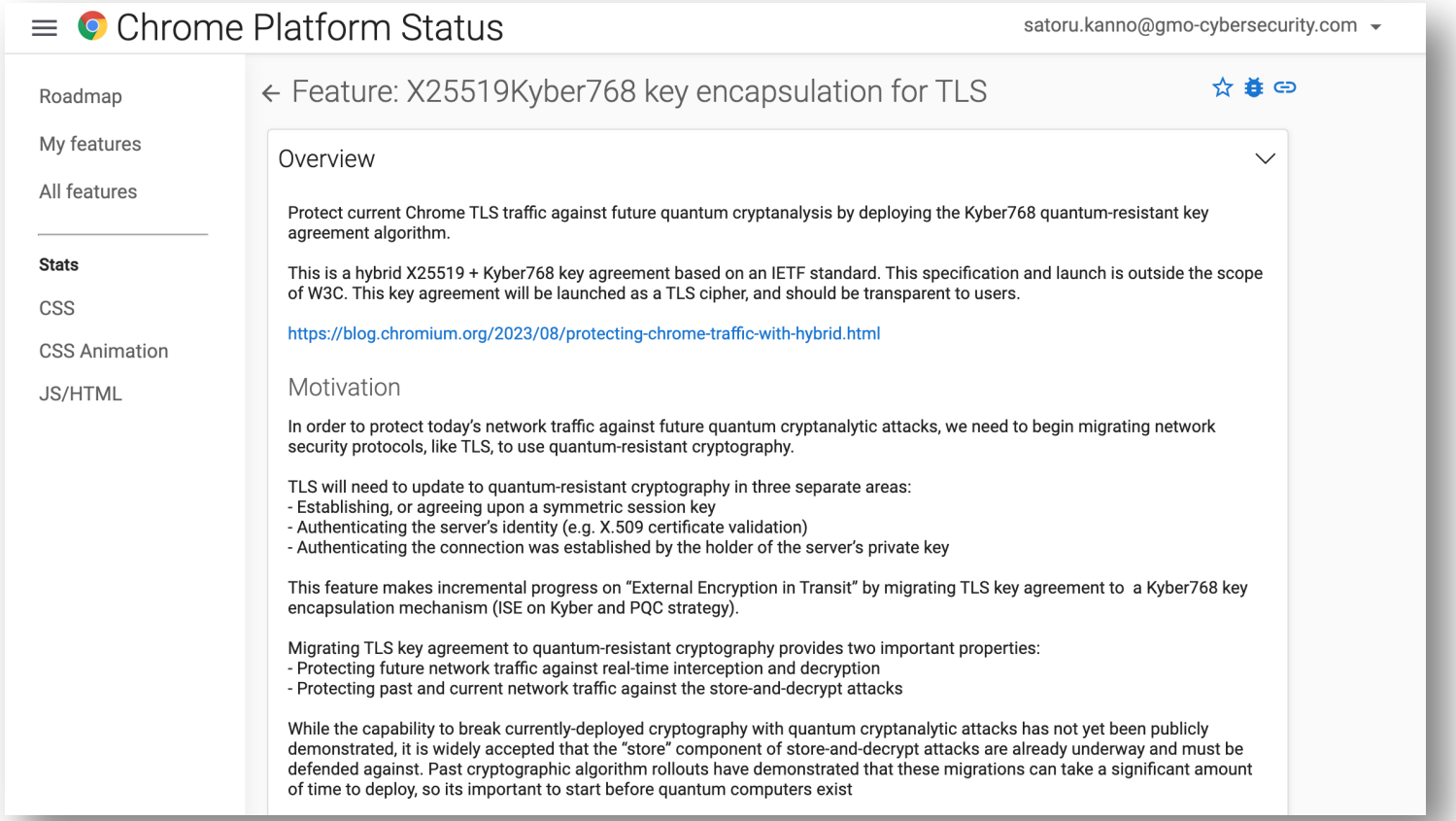
いくつかのプロジェクトが率先してOSS化を推進している

- PQClean
  - NISTのPQCプロジェクトにあるクリーンなPQC実装を提供
  - https://github.com/PQClean/PQClean
- liboqs
  - OpenSSLやOpenSSHを通じてTLSやSSHに機能提供
  - URL: https://github.com/open-quantum-safe/liboqs
- libpqcrypto
  - PQCRYPTOによって開発されたライブラリ（2018年が最終更新）
  - URL: https://libpqcrypto.org/

など他多数

身の回りにあるPQC

- Google Chrome 116（2023年8月リリース）
  - ➢ 現行暗号（X25519）とPQC（Kyber768）でハイブリッド鍵交換



https://chromestatus.com/feature/5257822742249472

- 2023年4月に発行されたInternet Draft「X25519Kyber768Draft00 hybrid post-quantum key agreement」を実装

https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/

なぜ、実社会で実証実験するのか？

実社会で前もって発生する課題を抽出し解決することができる

- 既存インターネットプロトコルへの影響
  - 例： データサイズ増加による影響
- 既存OSSへの影響
  - 例： 仕様のグレー部分の実装による挙動
- ネットワーク機器への影響
  - 例： 机上でOKでも通信できない
- PQC未対応な環境での処理
  - 例： 現行暗号へフォールバック方法

参考情報: CRYPTREC 外部評価報告書

- 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	ディジタル署名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	ディジタル署名EdDSAの構成の安全性に関する調査および評価	藤﨑 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

参考情報: 技術ブログ

- IETFにおける最新の技術動向が気になる方へ

GMO CYBER SECURITY IERAE

暗号 | 暗号 | IETF | 標準化 | PQC | 耐量子暗号 | 2030年問題 | PQUIP | CRYPTREC | ハイブリッドモード

IETFにおける耐量子暗号関連WG(PQUIP)の紹介

こんにちは、暗号のおねえさんことGMOインターネットグループ デベロッパーエキスパートの酒見(@ysakemin)です。

皆さん、好きな暗号プリミティブは何ですか？ 私は暗号プリミティブなら何でも好きでごはんが何杯も食べられちゃいます･:*+.\((°ω°))/.:+
好きな暗号プリミティブを聞きたいので教えてもらえるとうれしいです・・・！

さて、暗号技術に目を向けると社会的に見ても大きな動きがあるのは「耐量子暗号（PQC）」だと思います。これは昔懐かしい暗号移行が問題になった「暗号の2010年問題」の再来になるポテンシャルを秘めています。

そんなPQCについてインターネットの標準化を行なっているIETFでも検討されています。
そろそろ11月開催のIETF118が気になるタイミングでもありますので、今回の記事では、IETF117で開催されたIETFでのPQCに関するアレコレを検討するPQUIP(Post-Quantum Use In Protocols) WG の技術動向を報告します。

PQCが注目された背景

PQUIPの紹介に入る前に、まず、PQCがなぜ社会的に注目されているか？について紹介します。

私たちが実社会で使っている暗号技術の多くは、安全性の根拠として数学的な問題の難しさを利用しています。RSA暗号を例にすると、大きな数(2048bitなど)の素因数分解の問題を計算機で解こうとすると、現実的な時間で解くことができないので安全ですね、という考え方です。

一方で、近年の量子計算機の発展によって、難しいと考えられていた問題が現実的な計算時間で解読されてしまうリスクが指摘されています。これを受けて、脅威となる量子計算機が登場しても、将来的に解読が難しい数学的問題を使ったPQCが注目されています(※)。

- 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/

まとめ

- 暗号の危殆化
- 耐量子計算機暗号（PQC）
- 暗号移行
  - 「暗号の2010年問題」と「暗号の2030年問題」
  - 暗号移行とハイブリッドモードの関係
- 2023年現在、我々を取り巻くPQCに関する環境
  - 例としてIETFのご紹介
  - 標準化仕様、OSSなど

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