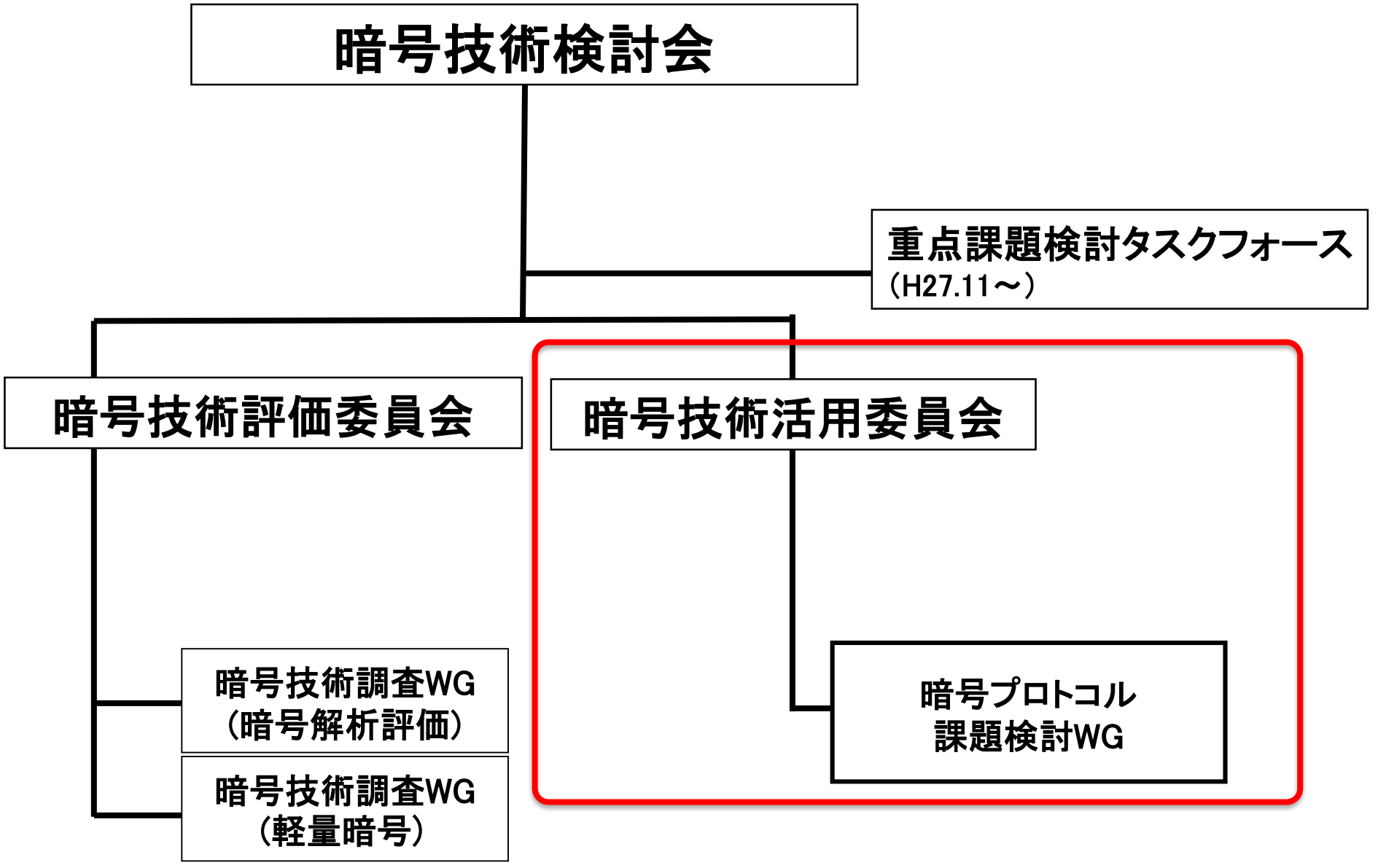
暗号プロトコル課題検討WG活動報告

2017年12月18日

暗号プロトコル課題検討WG主査
菊池 浩明
（明治大学）

2016年度CRYPTREC体制



2016年度暗号プロトコル課題検討WG委員

CRYPTREC
Cryptography Research and Evaluation Committees

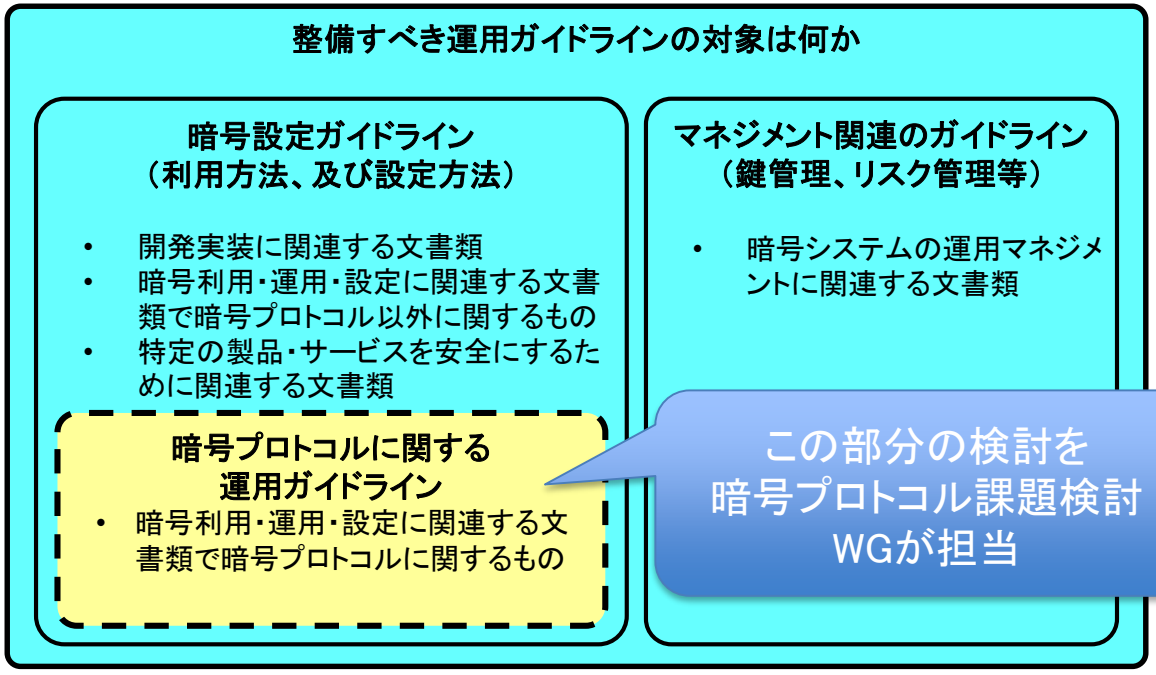
主査	菊池 浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	大泰司 章	一般財団法人日本情報経済社会推進協会　インターネットトラストセンター　企画室　室長
委員	坂根 昌一	シスコシステムズ合同会社　イノベーションセンター　エンジニア
委員	佐古 和恵	日本電気株式会社　セキュリティ研究所　技術主幹
委員	佐藤 直之	SCSK株式会社　ITマネジメント事業部門　netXデータセンター事業本部　セキュリティサービス部 シニアコンサルタント
委員	下山 武司	株式会社富士通研究所　サイバー＆データセキュリティプロジェクト　主管研究員
委員	須賀 祐治	株式会社インターネットイニシアティブ　セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	清藤 武暢	日本銀行金融研究所　情報技術研究センター
委員	村木 由梨香	日本マイクロソフト株式会社　セキュリティレスポンスチーム　セキュリティプログラムマネージャー
委員	吉田 博隆	国立研究開発法人産業技術総合研究所　情報技術研究部門サイバーフィジカルウェア研究グループ 主任研究員
委員	寺村 亮一	NRIセキュアテクノロジーズ株式会社　主任
委員	渡辺 大	株式会社日立製作所　研究開発グループ　システムイノベーションセンター　セキュリティ研究部　主任研究員

（注）2017年3月時点

2016年度暗号プロトコル課題検討WG活動内容

CRYPTREC Cryptography Research and Evaluation Committees

- CRYPTRECが「暗号プロトコル」をテーマとする「運用ガイドラインを作成」することを目標に課題を検討・整理



- WG開催概要

回	開催日時	主な議題
第1回	2016.10.27	● WG活動概要の説明、課題についての自由討議
第2回	2016.12.26	● 第1回WGでの討議を踏まえた課題の整理と更なる検討
第3回	2017. 2.10	● 報告書案の取りまとめ

運用ガイドラインの対象の検討

再掲

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会が運用ガイドラインを作成する価値がある対象は何かを明らかにする

➡ 2017年度以降、具体的な運用ガイドラインの作成に着手

■ 検討のポイント

【領域・対象】どのような用途で使う運用ガイドラインであるか

【目的】どのような目的をもった運用ガイドラインを意図したものか

【内容】運用ガイドラインに記載される内容はどのようなものか

【想定読者】その運用ガイドラインの想定読者は誰か

【必要性】なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか

【課題】 ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か（運用ガイドラインの価値を高めるための考慮ポイント）

【他組織のガイドライン等】他組織が同種のガイドラインを作っていないか／作ろうとしていないか

【関連組織】 どのような他組織と連携していくのがよいか

運用ガイドラインを作成する価値がある暗号プロトコルの対象範囲

■「種類の考え方」の整理

種類	ガイドラインの概要例	状況	代表的なプロトコル例
安全性評価に関するガイドライン	• 安全性のお墨付きをつけたプロトコル（＝CRYPTREC暗号リストのプロトコル版） • 評価されていないプロトコルに対する安全性方法 • 安全なプロトコルを設計するためのガイドライン	• 特定目的のために多くのプロトコルが提案されている • 暗号の専門家が関与しないでプロトコルが作られており、安全性評価が不十分 • 標準化を待っていられないため、先行して実装が進んでいる	OpenID Connect（銀行APIや電子請求API等で利用）,LoRa
実装・開発に関するガイドライン	• 製品の安全な実装・開発をするためのガイドライン • 安全な実装であることを検証するための基準	• この種のガイドラインがない • 各社独自の実装になっている	自動車業界で独自実装されている暗号プロトコル等
設定に関するガイドライン	• 製品に実装されている設定方法を適切に設定して安全に利用するためのガイドライン	• プロトコルレベルよりも製品レベルのほうが需要がある • 仕様が固まっている低レイヤのプロトコルであれば、運用ガイドラインが作りやすい	CIFS, RDP, SSH, IPsec, S/MIME, DKIM, DMARC, QUIC, NFC, OCSP, Active Directory, Linux, OS

具体的な検討方法

CRYPTREC
Cryptography Research and Evaluation Committees

STEP1　検討対象とする暗号プロトコルの列挙

【対象】 以下で使われる暗号プロトコルを洗い出し

Web／証明書失効管理／DNS／NW管理／鍵管理／
ユーザ管理／ユーザ認証／デバイス認証／バイオメトリクス暗号／ID連携／
無線通信／近距離通信／ICカード／
メール／リアルタイム通信／ファイル共有／ファイル転送／
リモート接続／VPN／
自動車／制御システム／仮想通貨／放送暗号

STEP2　ガイドラインを作る価値がある／必要性が高いと判断したものを抽出

特にこの3点を重視

【目的・内容】 どのような目的・内容をもったガイドラインを意図したものか

【想定読者】 そのガイドラインの想定読者は具体的に誰か

【必要性】 絞り込んだ暗号プロトコルには理由（必要性）が説明できるか

【課題】 問題となりそうな課題／注意しなければならない課題は何か

【他組織ガイドライン等】 他組織が同種のガイドラインを作っていないか

【関連組織】 どのような組織とどのように連携していくのがよいか

検討対象となりうる暗号プロトコルの列挙（1/3）

※「★」がついているプロトコルは
暗号に直接関係がないものを指す
※具体的なプロトコル名称がわからないもの
については規格やサービスの名称を示す

種類	対象	プロトコル名称
安全性評価 （暗号技術評価委員会への参考意見とする）	ID連携	OpenID Connect
	無線通信	LoRaWAN
	近距離通信	Zigbee
		Bluetooth
	仮想通貨	・Bitcoinプロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用 （証券決済/契約）
実装／開発	近距離通信	・NFC ・Felica ・ISO/IEC14443 TypeA，TypeB
	ICカード	Felica
	自動車	【車内】CAN，CAN FD，LIN，FlexRay 【車外】DSRC，ETC2.0 【ハードウェア】EVITA 【センサ】空気圧センサ，ミリ波レーダー
	制御システム	PLC SCADA

種類	対象	プロトコル名称
設定／運用	Web	QUIC
		HTTP/2★
	証明書 失効管理	・CRL ・OCSP
	DNS	・DNS ・DNSSEC（DANE,DPRIVを含む）
	NW管理	SNMP NETCONF UPnP
	鍵管理	KMIP
	ユーザ管理	・RADIUS （EAP-TLS等の利用を含む） ・PAP★ ・CHAPv2 ・IEEE802.1X
		LDAP★ （kerberos）
		・PAP★ ・CHAPv2
		TESLA
	ユーザ認証	・二要素認証

検討対象となりうる暗号プロトコルの列挙(2/3)

※「★」がついているプロトコルは
暗号に直接関係がないものを指す
※具体的なプロトコル名称がわからないもの
については規格やサービスの名称を示す

種類	対象	プロトコル名称
設定／運用	デバイス認証	・クライアント証明書 ・TPMを利用した認証
		・Apple MDM ・MS ライセンス認証 ・PUFを利用した認証
	バイオメトリクス暗号	・テンプレート保護 ・FIDO
	ID連携	・OpenID Connect ・SAML
		・OpenID Connect (HTTPS上で利用) ・代理認証
		・SAML (HTTPS上で利用) ・代理認証
	無線通信	・WEP ・WPA ・WPA2
	近距離通信	Zigbee
		Bluetooth

種類	対象	プロトコル名称
設定／運用	メール	・DKIM ・SPF★ ・DMARC★
		S/MIMEを 利用したメール送信 (メールへの署名)
		・パスワードつきZipを添付したメール送信 ・S/MIMEを利用したメール送信 (メールの暗号化) ・オンラインストレージサービス
		OpenPGPを 利用したメール送信
		・POP3 ・SMTP ・IMAP (ー/over SSL/with SASL)
		メッセージングサービス(SMS、Skype、Slack、Line、・・・)
	リアルタイム通信 (VoIP等)	・SIP★ ・RTP★ ・SRTP
	ファイル共有	・SMB ・CIFS ・WebDAV
	ファイル転送	SFTP FTPS FTP★

検討対象となりうる暗号プロトコルの列挙（3/3）

※「★」がついているプロトコルは
暗号に直接関係がないものを指す
※具体的なプロトコル名称がわからないもの
については規格やサービスの名称を示す

種類	対象	プロトコル名称
設定／運用	リモート接続	・SSH ・RDP ・telnet★
	VPN	・IPsec-VPN ・TLS-VPN
		IPsec-VPN
		TLS-VPN
	仮想通貨	・Bitcoinプロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用 （証券決済/契約）
	放送暗号	DRM ARIB W-CDMA

取りまとめ結果の例

種類	No	対象	プロトコル名称	目的	内容	想定読者	必要性	課題	他組織が発行したガイドライン等	関連組織
実装／開発	1	自動車	【車内】 CAN, CAN FD, LIN, FlexRay 【車外】 DSRC, ETC2.0 【ハードウェア】 EVITA 【センサ】 空気圧センサ、ミリ波レーダー	②	自動車の中で利用されている暗号の実装ガイドライン（検証方法含む）	自動車ベンダ、部品サプライヤ	・今後の自動運転車などを見据えた際、セキュリティに問題が発生した場合、社会的に大きな問題となることが想定されるため。	・標準化が行われている最中である。 ・規模が大きくCRYPTRECのリソースで対応できる範囲は限られる。 ・プロトコルで挙がっているものを、より細分化し優先順位を付ける必要がある。 ・自動車ベンダの協力が必要である。 ・国内では自動車工業会（JAMA）と連携するか、二人三脚で進めないと作っても受け入れられない懸念あり。 ・自動車業界は、まず欧米の評価を参考とするため、CRYPTRECがガイドラインを作成する場合には自動車業界に受け入れてもらえるような工夫が必要である。 ・DSRC,ETC2.0のセキュリティを管理するのはITS-TEAであり、ガイドラインを作成する場合、こことコンタクトする必要があるかもしれない。 ・SHE（Secure Hardware Extension）のように仕様が一般公開されないものに対してCRYPTRECがガイドラインを作るべきかは議論する必要がある。	・SAE j3061 : Cybersecurity Guidebook for Cyber-Physical Vehicle Systems ・Cybersecurity Best Practices for Modern Vehicles – NHTSA ・Automotive Cybersecurity Best Practices – Auto ISAC	・JSAE ・JasPar

取りまとめ結果

CRYPTREC Cryptography Research and Evaluation Committees

取りまとめ結果全容（全14対象）は暗号技術活用委員会に報告／「CRYPTREC Report 2016 暗号技術活用委員会報告」でも公開

種類	No.	対象	プロトコル名称	目的
安全性評価（暗号技術評価委員会への参考意見）	1	ID連携	OpenID Connect	①
	2	無線通信	LoRaWAN	①
	3	仮想通貨	・Bitcoinプロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）	①
実装／開発	1	自動車	【車内】CAN，CAN FD，LIN，FlexRay 【車外】DSRC，ETC2.0 【ハードウェア】EVITA 【センサ】空気圧センサ，ミリ波レーダー	②
	2	制御システム	・PLC ・SCADA ・BACKnet、OPC 等	① ②
設定／運用	1	ユーザ管理	・RADIUS （EAP-TLS等の利用を含む） ・PAP★ ・CHAPv2 ・IEEE802.1X	① ②
	2		LDAP★ （kerberos）	① ②

種類	No.	対象	プロトコル名称	目的
設定／運用	3	ユーザ認証	・二要素認証	① ②
	4	デバイス認証	・クライアント証明書 ・TPMを利用した認証 ・ISO/IEC9798	① ②
	5	無線通信	・WEP ・WPA ・WPA2	① ②
	6	メール	・DKIM ・SPF★ ・DMARC★	② ③
	7	メール	S/MIMEを利用したメール送信（メールへの署名）	② ③
	8		・パスワードつきZipを添付したメール送信 ・S/MIMEを利用したメール送信（メールの暗号化） ・オンラインストレージサービス	① ② ③
	9	リモート接続	・SSH ・RDP ・telnet★	① ②