第４回重点課題検討タスクフォース

日時：平成 29 年 2 月 22 日(水) 15:00～17:00
場所：経済産業省 本館１階西共用会議室

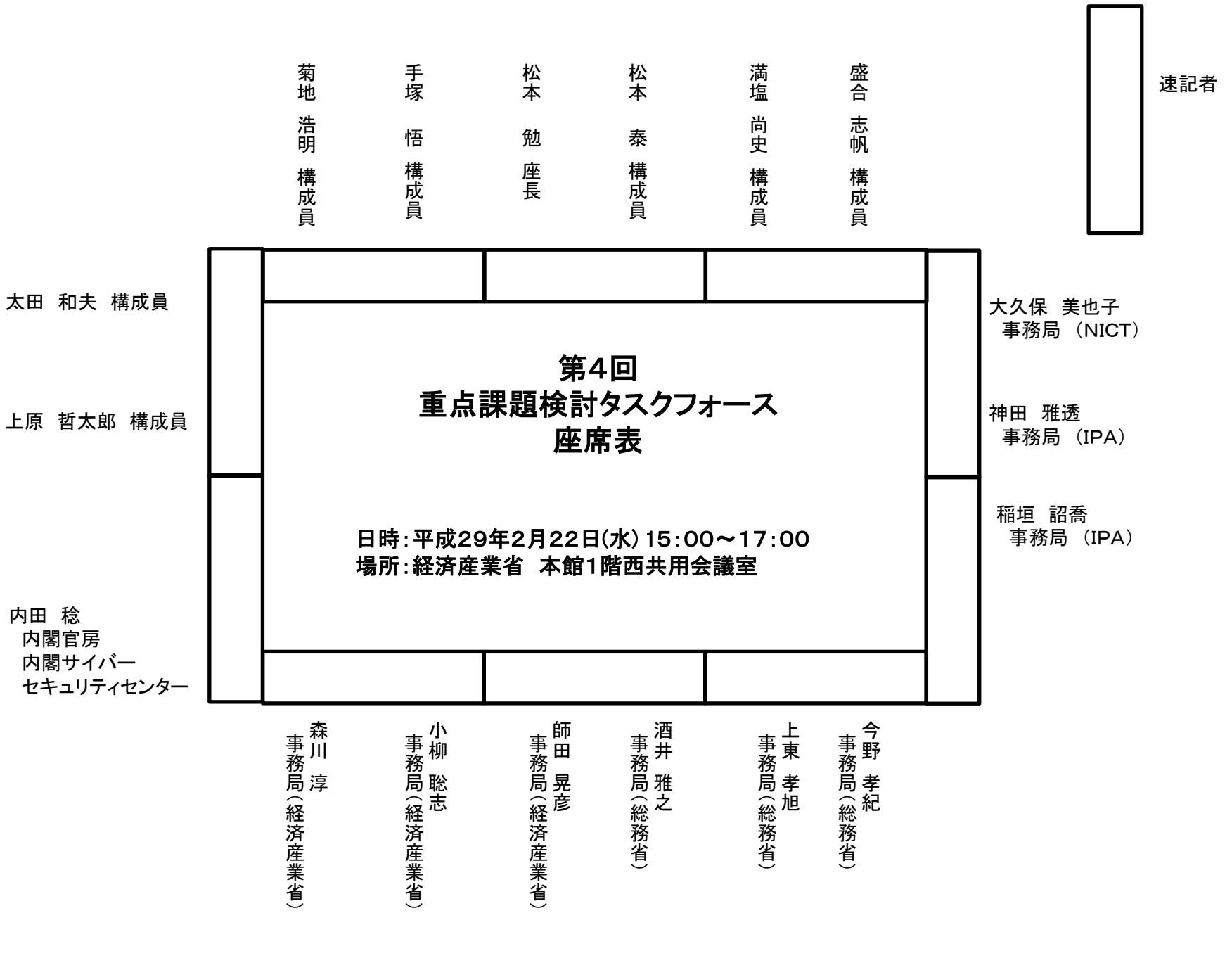
議　事　次　第

１．開　会（資料確認等）

２．議　事
(1) 「重点課題検討タスクフォース」開催要綱について
(2) CRYPTREC 今後の体制について
(3) 文書番号体系について
(4) その他

３．閉　会

（資料番号）	（資　料　名）
資料１	CRYPTREC の今後の体制（案）について
資料２	文書番号体系（案）について
参考資料１	「重点課題検討タスクフォース」開催要綱
参考資料２	委員名簿


速記者
盛合　志帆　構成員
満塩　尚史　構成員
松本　泰　構成員
松本　勉　座長
手塚　悟　構成員
菊地　浩明　構成員
太田　和夫　構成員
上原　哲太郎　構成員
内田　稔
内閣官房
内閣サイバー
セキュリティセンター
大久保　美也子
事務局（NICT）
神田　雅透
事務局（IPA）
稲垣　詔喬
事務局（IPA）
第4回
重点課題検討タスクフォース
座席表
日時：平成29年2月22日(水) 15：00～17：00
場所：経済産業省　本館1階西共用会議室
今野　孝紀
事務局（総務省）
上東　孝旭
事務局（総務省）
酒井　雅之
事務局（総務省）
師田　晃彦
事務局（経済産業省）
小柳　聡志
事務局（経済産業省）
森川　淳
事務局（経済産業省）
出入口

資料 1-1

CRYPTREC の今後の体制（案）について

［背景］

CRYPTREC には、これまで取り組んできた暗号アルゴリズムのセキュリティ（安全性）確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ（安全性）確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供といった貢献が求められている。

2015 年度の CRYPTREC においては、暗号技術に対する社会ニーズの変化や、社会情勢の変化を踏まえ、柔軟な活動を図るため、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等に係る活動の在り方の見直しを議論するため、暗号技術検討会の下に「CRYPTREC の在り方に関する検討グループ」（H27.6～H27.8）を設置、議論するとともに、当該検討グループでの議論を継続的に行うため、「CRYPTREC 重点課題検討タスクフォース」（H27.11～）を暗号技術検討会の直下に設置し、議論を行った。

2015 年度、重点課題検討タスクフォースにおいて主に(1) CRYPTREC 暗号技術活用委員会の今後の活動に向けて、(2) 暗号アルゴリズムの脆弱性に関する情報発信フローについて、(3) 暗号プロトコルのセキュリティ確保に向けた活動について議論した。

2015 年度 第 3 回重点課題検討タスクフォースにおいて、2016 年度の主な課題として以下が挙げられた。

① 文書体系の在り方について
② 政府統一基準に向けた新たな CRYPTREC 成果物
③ 新たな社会ニーズを見据えた新規活動
④ 情報システム全体のセキュリティ確保を意識した他団体との連携
⑤ その他

［今後］

①については CRYPTREC 成果物の区分の仕方・構成、読者、CRYPTREC が扱うべき範囲等を今回のタスクフォースにて議論を行い、暗号技術検討会に報告・審議を頂く。

②、③については、政府統一基準等から参照されやすい文書の作成やプライバシー保護のような社会ニーズを見据えた検討等の新たな取り組みについて、今後どのように議論を進めていくかを NISC との相談を含め、事務局 4 者で整理する。その後、整理した内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移して検討を行う。

④については、今後他団体との連携を必要とする対象のタスクが明確になった段階で、タスクの内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移し、具体的な連携方法について検討を行う。⑤については CRYPTREC としてどう取り組むか議論が必要なテーマに関する検討であるが、昨年度、例として挙がった ChaCha20 の安全性評価の必要性については、今年度、暗号技術評価委員会にて議論され、安全性評価が実施されている。

以上をもって、重点課題検討タスクフォースのミッションを終了とする。（今後、暗号技術検討会やその下の両委員会にまたがる検討事項が出てきた場合には、適宜 4 者事務局打合せで調整のうえ、必要に応じて暗号技術検討会やその下の両委員会に付議する。）

なお、暗号技術検討会は、現状の活動状況を踏まえて、フェーストゥフェースでの開催は年１回を基本とするが、メールベースの審議や報告などをタイムリーに行う体制を整えるなどの施策を通じて、検討会としてのアクティビティが低下しないように、活動の効率化を図る。
※リスト改定等の大きな動きがある時は適宜開催するものとし、年次活動計画のなかで開催回数を明示

［審議事項］

1. 重点課題検討タスクフォースの廃止

   重点課題検討タスクフォースのミッション終了に伴い、同タスクフォースを廃止することとしたい。

2. 今後の暗号技術検討会の審議や報告の進め方

   今後の暗号技術検討会の審議や報告の進め方について、事務局から以下を提案する。

   暗号技術検討会活動の効率化の観点から、従来、年度の第一回暗号技術検討会で行われてきた年度計画等の審議をメールベースで行うこととし、年度末に開催される第二回暗号技術検討会においては、従来どおりご参集いただくこととしたい。

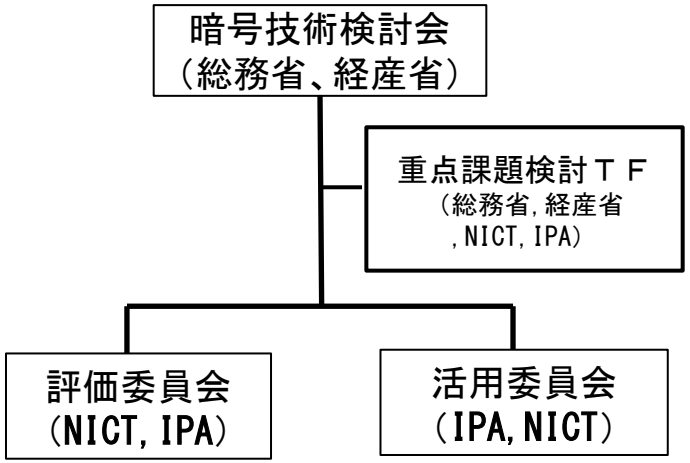
以上

CRYPTREC今後の体制（案）について

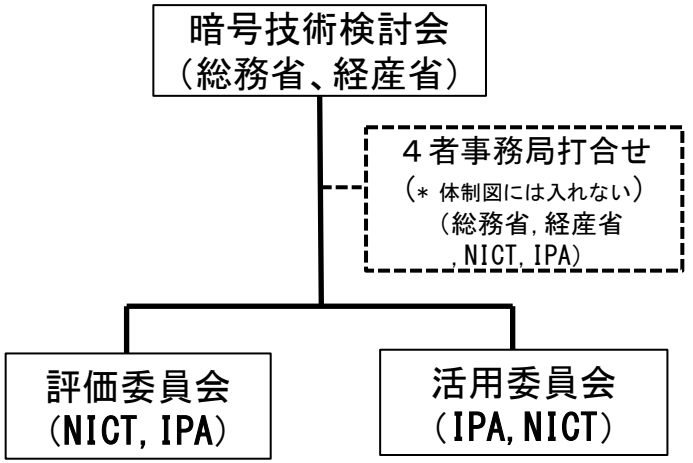
資料1-2

■重点課題検討タスクフォースのミッション終了に伴い、当該タスクフォースを廃止する。
（今後、検討会や両委員会にまたがる検討事項が出てきた場合には、適宜4者事務局打合せで調整のうえ、必要に応じて検討会や両委員会に付議する。）

Before



After



資料 2

文書番号体系について（案）

文書番号体系の確立を目指して(1/3)

【論点(1)】

現在はCRYPTREC文書に付番されていないが、今後は文書番号から内容(の位置づけ)がわかるように文書管理を行うのはどうか

- 統一的な番号体系を採用し文書番号を付与する
- 一度付与された連番は文書の改訂では変更しない
  - 管理情報(「改訂年度情報」か「バージョン情報」)で管理

2013年度のリストガイドWG検討結果をベースにした文書番号体系イメージ:

＜文書番号＞ ::= (CRYPTREC) ＜カテゴリ＞"-"＜連番＞("-"＜管理情報＞)

例 (CRYPTREC) CL - 001 - 2012 ⇔ 2012年度発行のCRYPTREC暗号リスト
(CRYPTREC) CR - 001 - 2015 ⇔ 2015年度発行の暗号技術検討会報告書
(CRYPTREC) OG - 001 - 1.1 ⇔ SSL/TLS暗号設定ガイドライン ver 1.1

【参考】

	カテゴリ		連番		管理情報	
•	FIPS		xxx	-	yyy	⇒ 米国連邦強制規格
•	(NIST) SP800	-	xxx		rev.	⇒ NISTが自ら作ったガイドライン
•	(NIST) SP1800	-	xxx			⇒ NCCoEプロジェクトで作ったガイドライン
•	NISTIR		xxx			⇒ NIST内部用のレポート

CRYPTREC文書

CRYPTREC活動に関連して作られた文書類のうち、CRYPTRECが著作権を有する、以下の条件のいずれかを満たすものを「CRYPTREC文書」という

※便宜上、CRYPTRECには、総務省、経産省、暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、各WGを含む

- CRYPTREC暗号リスト
- CRYPTRECが報告書またはガイドラインとして公開するもの
- CRYPTRECが公表する注意喚起レポート

- CRYPTREC暗号リスト掲載の各暗号アルゴリズムの仕様書

上記の定義からは外れるがCRYPTREC文書に含めたほうがよいか

【参考】

CRYPTREC文書に該当しない代表的な文書類

- 外部評価レポート（外部評価者が作成した技術報告書）
- 委員会資料（議事録を含む）

文書番号体系の確立を目指して(2/3)

【論点(2)】

内容(の位置づけ)を識別するためには、どのようなCRYPTREC文書分類を採用するのがよいか

【案1】分かりやすいように表記数をできるだけ集約

#	CRYPTREC文書分類例	該当する既存のCRYPTREC文書例	表記名イメージ(参考)
ア	CRYPTREC暗号リスト	CRYPTREC暗号リスト CRYPTREC暗号の仕様書	CL
イ	年次報告書	年次報告書	CR
ウ	早期に公開する注意喚起	注意喚起レポート	NR
エ	技術報告書	調査WG報告書、暗号技術ガイドライン、 推奨セキュリティパラメータ設定	TR
オ	運用ガイドライン	暗号運用ガイドライン	OG

【案2】現在のCRYPTRECホームページでの表記に準拠

#	CRYPTREC文書分類例	該当する既存のCRYPTREC文書例	表記名イメージ(参考)
カ	CRYPTREC暗号リスト	CRYPTREC暗号リスト	CL
キ	仕様書	CRYPTREC暗号の仕様書	SP
ク	年次報告書	年次報告書	CR
ケ	早期に公開する注意喚起	注意喚起レポート	NR
コ	技術ガイドライン	暗号技術ガイドライン、推奨セキュリティパラメータ設定	TG
サ	調査報告書	調査WG報告書	TR
シ	運用ガイドライン	暗号運用ガイドライン	OG

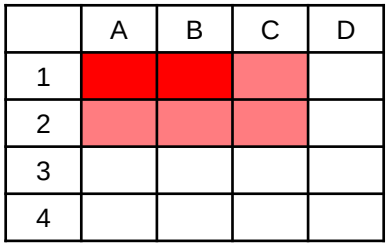
文書番号体系の確立を目指して(3/3)

【論点（3）】

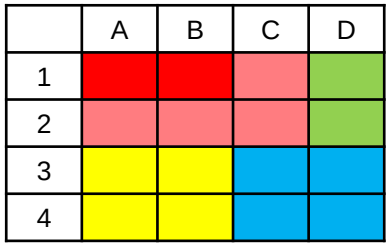
文書管理の対象範囲と作業主体の違いをどのように考えるか

- 「文書作成段階での作成主体」や「文書アップデート段階での作業主体」の違いが分かるような表記名をカテゴリ識別に含めるのがよいか
- どのような表記名がよいか。何段階ぐらいにするのがよいか

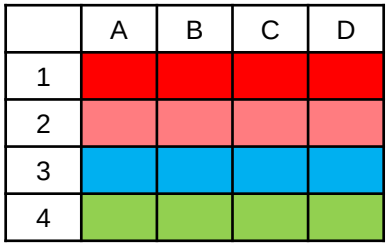
CRYPTRECの成果物の範囲と区分の考え方(3/3)を参考例としてのイメージ



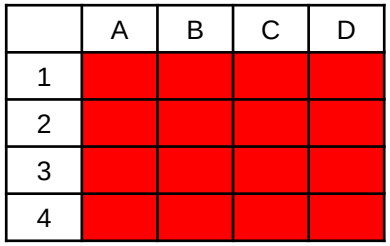
イメージ1
今までのCRYPTREC文書の範囲を踏襲
○ 文書の品質を確保できる
○ 表記について考える必要がない
× 文書の個数を大きく増やすことは困難



イメージ3
作業主体の違いを正確に反映して付番
○ 作業主体の違いを反映できる
○ 文書の個数を大きく増やせる可能性がある
× アップデートの作業主体が最初は決まらない可能性がある
× 種類が多すぎると分かりづらい



イメージ2
文書作成段階での作成主体をベースに付番
○ 作成段階での作成主体の違いを反映できる
○ 文書の個数を大きく増やせる可能性がある
× アップデート段階の作業主体の違いは反映されない
× 種類が多すぎると分かりづらい



イメージ4
文書の対象範囲を広げるが、作業主体の違いは考えない
○ 表記について考える必要がない
○ 文書の個数を大きく増やせる可能性がある
× 作業主体の違いが表現されない
× 文書の品質が異なる可能性がある

CRYPTREC文書の範囲と区分の考え方(1/3)

【作成段階】

※便宜上、CRYPTRECには、総務省、経産省、暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、各WGを含む

#			作成方法	過去の文書例
1	CRYPTREC内で完結する文書	CRYPTREC主導で作成	CRYPTREC内部に閉じて作成	CRYPTREC文書に該当する全文書
2			アウトソーシングで作成させた内容をベースに、CRYPTRECとしての文書を作成 ※WG設置は想定しない	なし
3	CRYPTREC内で完結しない文書		他組織と共同で文書を作成 ※両組織で発行されることを想定 ※主体は他組織。CRYPTRECはサポート	なし
4		他組織主導で作成	他組織が作成した文書をベースに、（できるかぎり少ない変更で）CRYPTRECとしての文書を作成	なし

CRYPTREC文書の範囲と区分の考え方(2/3)

【アップデート段階】

※「アップデート」とは、文書に記載されている内容の質自体に関わる記述をいずれ改訂することを**当初から意図**しており、かつそれを**実行**することを意味する。また、アップデート後は、前バージョンの文書は廃止（アーカイブ）される。
したがって、いわゆる「記述内容の正誤修正」、「作成時点で改訂を意図していない文書」はここでの「アップデート」には含まない

※ 便宜上、CRYPTRECには、総務省、経産省、暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、各WGを含む

#		作業方法	過去の文書例
A	CRYPTREC内で完結するアップデート	発行後は原則アップデートしない	年次報告書
B		CRYPTREC内部に閉じてアップデートを実施	CRYPTREC暗号リスト 解析計算量評価
C		アウトソーシングで検討させた内容をベースに、CRYPTRECとしてのアップデートを実施 ※WG設置は想定しない	なし
D	CRYPTREC内で完結しないアップデート	他組織がアップデートした内容をベースに、CRYPTRECとしてのアップデートを実施 ※WG設置は想定しない	なし

CRYPTREC文書の範囲と区分の考え方(3/3)

■ 今後予想される文書の区分

作成段階の違い ＼ アップデート段階の違い			CRYPTREC主導でのアップデート			他組織主導のアップデート
			A	B	C	D
			原則アップデートなし	完全自前でアップデートを実施	アウトソーシングベースでのアップデートを実施	他組織がアップデートした内容をベースのアップデートを実施
CRYPTREC主導	1	CRYPTRECが完全自前で作成	• 年次報告書	• CRYPTREC暗号リスト • 解析計算量評価		
CRYPTREC主導	2	アウトソーシングベースで成果物を作成			今後の暗号運用ガイドラインとしてはこのあたりを想定	
CRYPTREC主導	3	他組織と共同で成果物を作成				
他組織主導	4	他組織が作成した成果物をベースに作成				

参考：NIST文書類作成の関連組織

NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC: GO
CONTACT SITE MAP
Computer Security Division
Computer Security Resource Center

PUBLICATIONS

NIST publishes standards, guidelines, recommendations and research on computer/cyber/information security and privacy using the following NIST technical series. Publication drafts are available for public comment

- Federal Information Processing Standards (FIPS): security standards;
- NIST Special Publications (SPs): security and privacy guidelines, recommendations and reference materials. These include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy;
- NIST Interagency or Internal Reports (NISTIRs): reports of research findings and background information for FIPS and SPs; and
- Information Technology Laboratory (ITL) Bulletins: monthly overviews of NIST's security and privacy publications, programs and projects.

Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

National Checklist Program Repository

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search CVE and CCE Vulnerability Database

(Advanced Search)
Keyword search: Search

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
NIST National Institute of Standards and Technology U.S. Department of Commerce

Projects

Overview

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available and open source technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, end-to-end reference designs that are broadly applicable and repeatable.

Use Cases Versus Building Blocks

The center works on use cases, which are sector-specific cybersecurity problems, and building blocks, which address technology gaps affecting multiple sectors.

Final Products

When a project is completed, the NCCoE facilitates rapid, widespread adoption of secure technologies by publishing NIST Cybersecurity Practice Guides (Special Publication series 1800), which include all of the information and instructions needed to deploy a reference design.

Partners

The NCCoE has joined with a variety of U.S. companies through a formal initiative called the National Cybersecurity Excellence Partnership (NCEP). These partners have pledged to provide hardware, software and expertise to our mutual efforts to advance the rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, companies may designate guest researchers to work at the center in person or remotely.

We are pleased to work with:

Akamai, ca technologies, cisco, FireEye, hp, HYTRUST, IDW, intel, JUNIPER, Lookout, Lumeta, McAfee, Microsoft, NEXTLABS, paloalto, Ping, Pulse Secure, redhat, RSA, splunk>, Symantec, tripwire, VANGUARD, VENAFI

参考：NIST文書類での予想分類例(1)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
①	**政府統一基準から参照**される文書	• **（必須）FIPS** • **（ガイドライン）Special Publication (SP)**
②	攻撃の内容（影響範囲・対処方法等）を**早期に公開し、注意喚起**することを目的とした文書	• なし（あえていえばNews／Announcement）
③	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめた文書	• **NIST Internal/Interagency Report (NISTIR)** NISTIR7427 6th Annual PKI R&D Workshop "Applications-Driven PKI" Proceedings NISTIR7539 Symmetric Key Injection onto Smart Cards NISTIR7896 Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition
④	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめた文書	• **FIPS Appendix／change notice** FIPS186-4 Appendix D: Recommended Elliptic Curves for Federal Government Use • **NIST SP800シリーズ** SP800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications SP800-107 Recommendation for Applications Using Approved Hash Algorithms SP800-108 Recommendation for Key Derivation Using Pseudorandom Functions
⑤	委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめた文書	• **NIST SP800シリーズ** SP800-133 Recommendation for Cryptographic Key Generation SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations SP800-77 Guide to IPsec VPNs SP800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i SP800-111 Guide to Storage Encryption Technologies for End User Devices
⑥	委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**文書	• **NIST SP800シリーズ** SP800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach SP800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans SP800-114 User's Guide to Securing External Devices for Telework and Remote Access SP800-128 Guide for Security-Focused Configuration Management of Information Systems SP800-130 A Framework for Designing Cryptographic Key Management Systems SP800-152 A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

参考：NIST文書類での予想分類例(2)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
⑦	委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめた報告書	• **NIST Internal/Interagency Report (NIST IR)** NISTIR7816 2011 Computer Security Division Annual Report NISTIR7956 Cryptographic Key Management Issues & Challenges in Cloud Services NISTIR7966 Security of Automated Access Management Using Secure Shell (SSH) NISTIR8014 Considerations for Identity Management in Public Safety Mobile Networks • **NIST SP800シリーズ** SP800-145 The NIST Definition of Cloud Computing SP800-176 2014 Computer Security Division Annual Report • **White paper（NIST NCCoE Program）** DATA INTEGRITY - Reducing the impact of an attack
⑧	実用性を向上させるための**具体的な設定方法を紹介**した文書	• **SP800シリーズ（National Checklist Program）** SP800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers • **SP1800シリーズ（NIST NCCoE Program）** SP1800-1 Securing Electronic Health Records on Mobile Devices (DRAFT) SP1800-5 IT Asset Management (DRAFT)
⑨	**外部機関が作成・公表**する同系列の文書へのリンク	• **National Vulnerability Database (NVD)**

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

FIPS

13. Waiver Procedure: The Federal Information Security Management Act (FISMA) does not allow for waivers to a FIPS that is made mandatory by the Secretary of Commerce.

SP

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

参考：CRYPTRECシンポジウム2013公開資料（抜粋）

5. 将来に向けた展望：文書番号体系の確立とCRYPTREC暗号リストの改定に伴う修正

文書番号体系の確立

- リストガイドを参照しやすくするため、統一的な番号体系を採用し文書番号を付与する

＜文書番号＞::=＜略称＞”-”＜カテゴリ＞”-”＜連番＞
例：CUG-A-003

- 一度付与された連番は，文書の改訂では変更しない
- 改訂における考え方
  - 改訂年度などの情報を入れる（ISO方式）⇒　例：CUG-A-003-2013
  - バージョンを文書に付与する（NIST SP800方式）⇒　例：CUG-A-003 Rev.1

CRYPTREC暗号リスト改定に伴う修正

- CRYPTREC暗号リストの改訂に伴い、これまでに作成したリストガイドを修正する
  - 新しい体系（電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リスト）に対応した内容の追記

参考資料１

「重点課題検討タスクフォース」開催要綱

１　名　称

本検討会は「重点課題検討タスクフォース」（以下「タスクフォース」という。）と称する。

２　開催の趣旨・目的

暗号技術を取り巻く環境やサイバーセキュリティ基本法（平成 26 年法律第 104 号）の施行といった社会情勢の変化に鑑み、今後の情報システム全体のセキュリティ基盤の為に必要となる CRYPTREC の活動の方向性の議論を行い、今後 CRYPTREC が取り扱うべき暗号に係る技術分野の選定や情報発信の在り方等を決定し、トップダウン的な意志決定も出来る体制の構築を目的として開催する。

３　検討事項

（１）CRYPTREC のミッション検討

・政府統一基準への新たな成果物
・暗号プロトコルレベルのセキュリティ確保に向けた活動
・新たな社会ニーズを見据えた新規活動
・他団体との連携
・情報発信フローの整備

（２）上記に基づいた CRYPTREC 次年度活動計画方針案検討

４　構成等

（１）タスクフォースの構成は、別紙のとおりとする。
（２）タスクフォースには、座長１名を置く。
（３）座長は、構成員の互選により定める。
（４）座長は、タスクフォース構成員の中から顧問及び座長代理を指名できる。
（５）構成員の任期は委嘱時に定めるものとし、再任を妨げないものとする。

５　運　営

（１）座長は、タスクフォースの議事を掌握する。
（２）座長が、緊急の理由によりやむを得ず不在となった場合、座長代理が座長に代わり議事を掌握する。
（３）関係する政府機関等で、座長が特に認めたものについては、オブザーバとしてタスクフォースに出席することができる。
（４）座長が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。

（５）座長は、タスクフォースが調査する事項について特に専門的な調査を行う必要があると認めるときは、委員会等を置くことができる。
（６）座長は、必要があると認めるときは電子メールによる審議を行うことができる。なお、この審議を行った場合は、次のタスクフォースにおいて当該審議の結果を報告するものとする。
（７）その他タスクフォースの運営に関し必要な事項は、座長が定めるところによる。

６　議事の公開

タスクフォースは非公開とするが、タスクフォースで使用した資料及びタスクフォースの議事概要については、次の場合を除き、公開する。
（１）公開することにより当事者又は第三者の権利、利益や公共の利益を害するおそれがあると座長が認める場合
（２）その他、非公開とすることが必要と座長が認める場合

７　スケジュール

タスクフォースは、年度内に１回以上開催する。

８　庶　務

タスクフォースの庶務は、総務省情報流通行政局情報セキュリティ対策室、経済産業省商務情報政策局サイバーセキュリティ課、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構において処理する。

参考資料２

重点課題検討タスクフォース　構成員・オブザーバ名簿

2017.2.22 現在

（構成員）

上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
太田　和夫	電気通信大学大学院　情報理工学研究科 総合情報学専攻（セキュリティ情報学コース）　教授
菊池　浩明	明治大学　　教授
手塚　　悟	慶應義塾大学大学院　政策・メディア研究科　特任教授
時田　俊雄	独立行政法人情報処理推進機構　セキュリティセンター暗号グループ グループリーダー
松本　　勉	横浜国立大学　大学院環境情報研究院　教授
松本　　泰	セコム株式会社　IS 研究所　マネージャー
満塩　尚史	内閣官房情報通信技術（IT）総合戦略室　政府 CIO 補佐官
盛合　志帆	独立行政法人情報通信研究機構　サイバーセキュリティ研究所 セキュリティ基盤研究室　室長

（オブザーバ）

内田　　稔	内閣官房情報セキュリティセンター　政府機関総合対策グループ

（五十音順、敬称略）