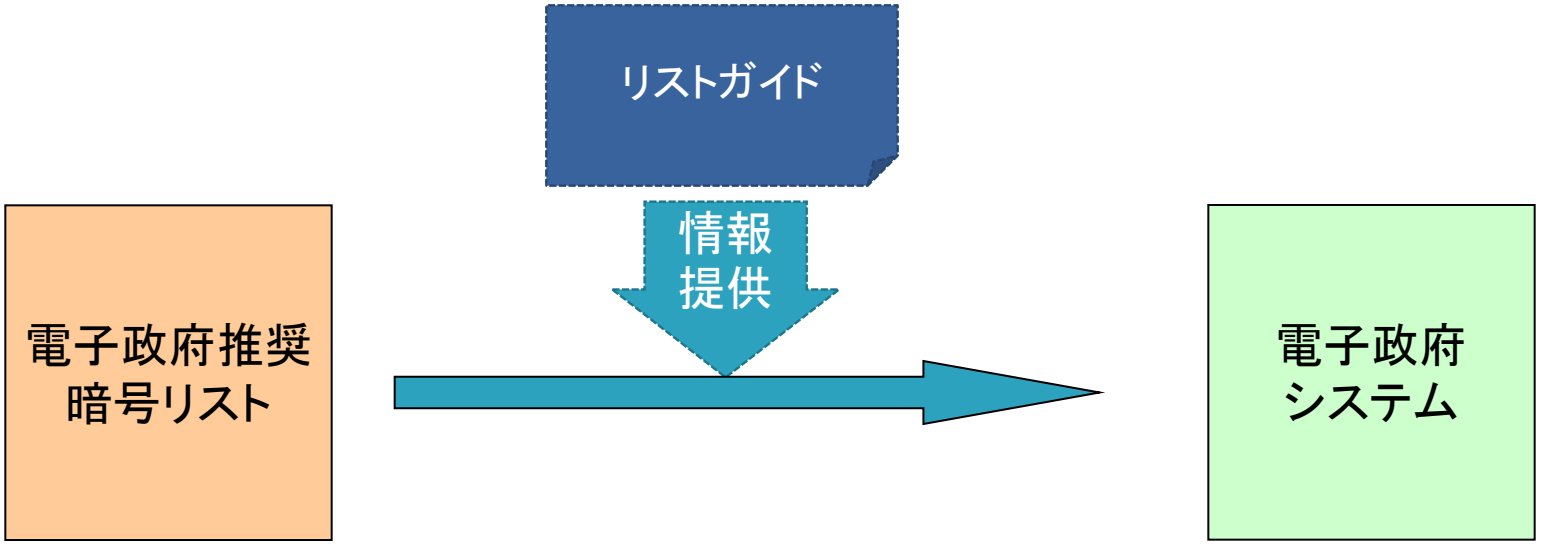
暗号技術調査WG(リストガイド)
活動報告

主査　手塚 悟
東京工科大学

1. リストガイドとは

電子政府システムの調達者及び構築者に対して，電子政府推奨暗号を利用する際に必要となる情報を提供する文書

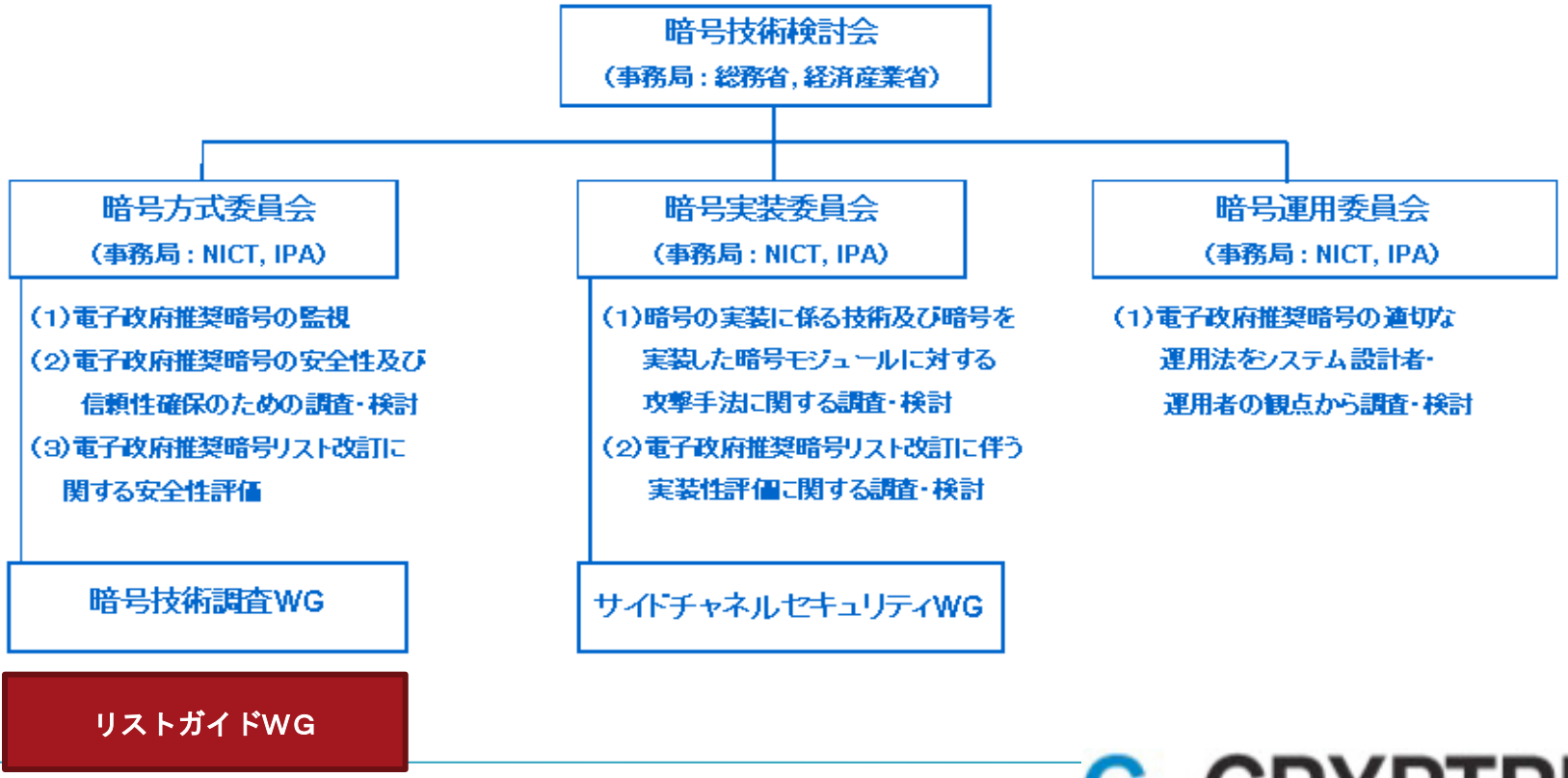


CRYPTREC
Cryptography Research and Evaluation Committees

2. リストガイドWGの位置づけ

リストガイドWGは暗号方式委員会の下に設置され、暗号システムの実装及び運用の専門家の知見を集約して暗号技術の適切な利用方法を検討し，その成果をリストガイドとして公開することを目的としている

CRYPTREC 体制図



CRYPTREC
Cryptography Research and Evaluation Committees

2. リストガイドWGの位置づけ（2）

リストガイドWG委員構成（敬称略）

【主査】

手塚 悟	東京工科大学

【委員】

岡崎 博之	日本電気株式会社
菅野 哲	NTT ソフトウェア株式会社
清本 晋作	株式会社KDDI 研究所
佐野 文彦	東芝ソリューション株式会社
花岡 悟一郎	独立行政法人産業技術総合研究所
藤城 孝宏	株式会社日立製作所
松尾 真一郎	独立行政法人情報通信研究機構
民田 雅人	株式会社日本レジストリサービス
渡辺 大	株式会社日立製作所

3. これまでの活動概要

2008年度以降，電子政府推奨暗号リストに掲載されている暗号技術の利用を促進するための検討を行い，以下の内容に関するリストガイドを作成

- 電子政府推奨暗号リストに掲載されている暗号技術の適切な利用方法及び推奨パラメータの提示
- 暗号技術の実装方法・運用方法の提示
- 電子政府推奨暗号リスト以外の先進的な暗号技術の動向調査結果

<table>
<tr><th></th><th colspan="2">推奨パラメータ</th><th>実装方法</th><th>運用方法</th><th>動向調査</th></tr>
<tr><td rowspan="8">リストガイドの名称</td><td colspan="3">電子署名</td><td rowspan="8">鍵管理</td><td>IDベース暗号</td></tr>
<tr><td colspan="3">メッセージ認証コード</td><td rowspan="7"></td><td>KDFに関する調査</td></tr>
<tr><td colspan="3">秘匿の暗号利用モード</td><td rowspan="2">一般的な暗号プロトコルに関する調査</td></tr>
<tr><td colspan="3">電子政府推奨暗号の鍵共有</td></tr>
<tr><td colspan="2">IPSec</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td colspan="2">SSL/TLS</td></tr>
<tr><td colspan="2">電子政府推奨暗号の利用方法に関するガイドブック</td></tr>
</table>

4. 今年度の活動

(1) 鍵導出関数(KDF)に関する調査

- 安全性評価の検討に向けた，安全性要件の検討及び能動的攻撃に対する評価

(2) 一般的な暗号プロトコルに関する調査

- IETF における「SSL/TLS」及び「IPsec」に関連したRFCの標準化動向の調査
- 「DNSSEC」について、鍵更新を含む鍵管理の検討を行うための事前調査として、実運用面からの課題の整理

(3) リストガイドの利用促進に係る検討

- 複数年にわたる活動を通して作成したコンテンツの利用促進策の検討

4. 今年度の活動：KDFに関する調査（1）

安全性要件の検討

- 2008年以降に発行されたNIST SP800の追加文書に関する調査を実施（下表：KDFの分類）、KDFの安全性要件を検討
  - 基本的にKDFの出力生成にハッシュ関数もしくはMACが用いられているため、KDFの安全性要件として独自に検討すべき事項はない
  - ハッシュ関数を直接用いる場合、ハッシュ関数に求められる安全性要件は一方向性と出力の一様ランダム性であり、衝突困難性は不要であることが指摘されていることを確認した

			CTR	FB	DPI	その他
直接	ハッシュ		[56a], [56b], [X9.42], [X9.63]			[SSH]
	MAC	HMAC	[108]	[108]	[108]	
		CMAC	[108]	[108]	[108]	
E-E	ハッシュ					
	MAC	HMAC	[56c]+[108]	[56c]+[108], [IKEv1,v2], [TPM]	[56c]+[108], [TLS1.0,1.1], [TLS1.2]	
		CMAC	[56c]+[108]	[56c]+[108]	[56c]+[108]	

【備考】
[SSH]：過去に生成した鍵をすべて使うログ式。
[SRTP]：AES-CTRを使用。
[TPM]：「直接」とE-Eの混合方式。

[X9.42] X9.42-2001
[X9.63] X9.63-2001

[56a] SP800-56A
[56b] SP800-56B
[56c] SP800-56C
[108] SP800-108
[132] SP800-132
[135] SP800-135rev1

4. 今年度の活動：KDFに関する調査（2）

能動的攻撃に対する評価

- 能動的攻撃に対する評価を行い，下表に示す結果を得た

仕様	評価結果
NIST SP800 56A, 56B, 56C	Other Infoの各フィールドが固定長であれば問題なし
NIST SP800 108	同上
NIST SP800 132	基本的に問題はないが、Saltの作り方において、任意入力を許容（S= purpose‖rv)しており、注意が必要（KDFの仕様対象外の可能性あり）
NIST SP800 135rev1 (IKE, TLS, SSH, SRTP, SNMP, TPM)	SRTPの仕様に問題あり
SEC1	問題なし
ANSI X9.42-2003	問題なし
PSEC-KEM	問題なし

4. 今年度の活動：一般的な暗号プロトコルに関する調査（IETF）

- IETF における「SSL/TLS」及び「IPsec」に関連したRFCの標準化動向及び電子政府推奨暗号関連の動向について調査

- 「SSL/TLS」及び「IPsec」に関連したRFCとして，数年以内にRFC化が見込まれるI-D（インターネットドラフト）の仕様を確認
  - tls：Secure Password Ciphersuites for Transport Layer Security (TLS), Standards Track等、3トラック
  - ipsecme： More Raw Public Keys for IKEv2, Informational等、2トラック
  - その他：kerberos、jose、dnsext、sidr、karp等

- 電子政府推奨暗号関係の動向として，現在，標準化が行われているI-Dの概要を確認
  - Camellia：Camellia Encryption for Kerberos 5, Standards Track等、8トラック
  - CLEFIA：CLEFIA Cipher Suites for Transport Layer Security (TLS), Informational等、3トラック
  - KCipher2：Use of KCipher-2 in Transport Layer Security, Standard等、3トラック

4. 今年度の活動：一般的な暗号プロトコルに関する調査（SRP）（1）

- IETFにおける、SRPの標準化動向と安全性について調査
- SPRの標準化動向
  - IETFにおけるSRPの位置づけについて調査（下表）

RFC番号	タイトル
2944	Telnet Authentication: SRP
2945	The SRP Authentication and Key Exchange System　(SRP-3)
3720	Internet Small Computer Systems Interface (iSCSI)
3723	Securing Block Storage Protocols over IP
3669	Guidelines for Working Groups on Intellectual Property Issues
5054	Using the Secure Remote Password (SRP) Protocol for TLS Authentication

4. 今年度の活動：一般的な暗号プロトコルに関する調査（SRP）（2）

- SRPの安全性調査
  - 証明可能安全性のフレームワークにおける安全性証明はない
  - RFCにおけるSecurity Considerationの記述
    - 鍵確認は必須である
    - セキュリティパラメータは十分に大きくする
    - パスワード推測を防ぐため、試行回数を制限
    - SHA-1の現状の衝突はプロトコル安全性への影響は少ないが、他の脆弱性が出てきたときには使わないようにすべき
- 結論
  - SRP自体のセキュリティについては、継続調査が必要
  - TLSのCipher Suiteにおいて、暗号化部分で電子政府推奨暗号リストに掲載されていないアルゴリズムの扱いを検証する必要がある

4. 今年度の活動：一般的な暗号プロトコルに関する調査（PSK）（1）

- TLS-PSK(RFC4279，RFC5489)に関する利用状況の調査及び鍵共有方式に関する安全性を検討

- TLS-PSKの利用状況：ほとんど利用されていない状況である
  - RFC 4279における利用用途の記載
    - PKIを使用したくない場合に適用可能
    - 省リソースであることが利点
  - OpenSSL 1.0.1では，normal PSK のみ実装されている（現在はTLSとDTLSでサポート）
  - GnuTLSでは、normal PSK ／ DHE_PSK ／ ECDHE_PSKが実装されている（RSA_PSKが未実装）

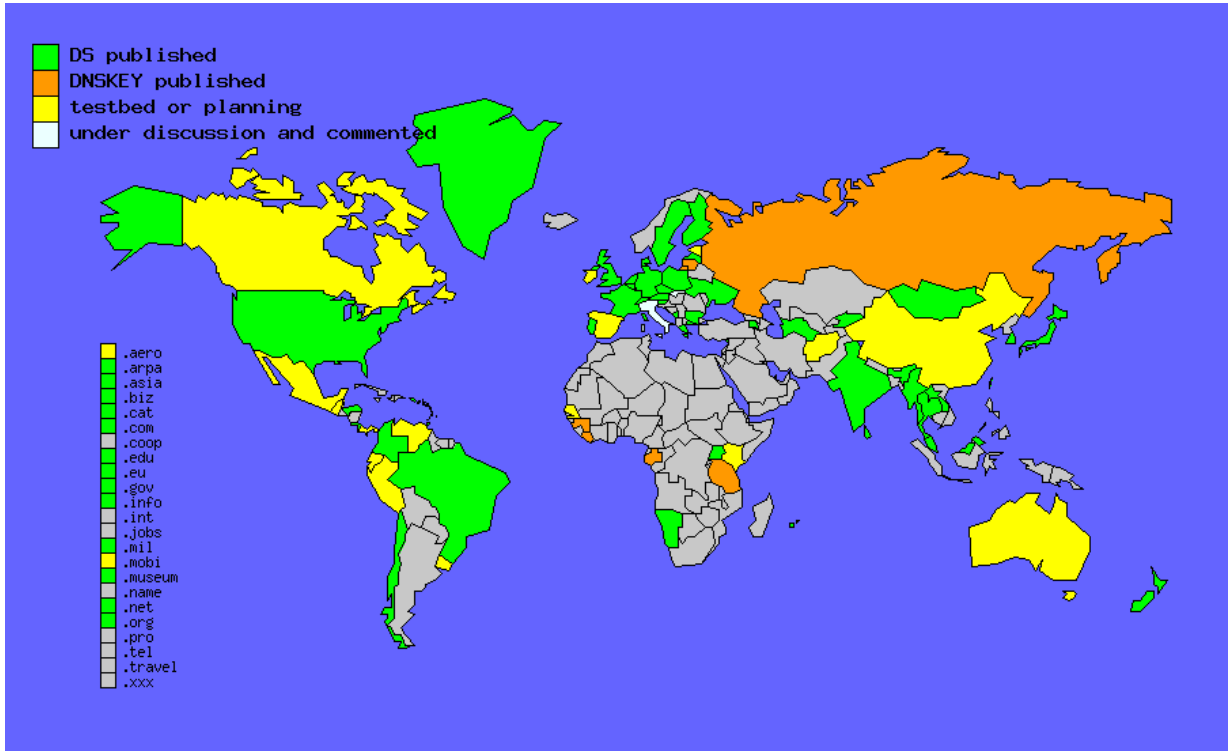
4. 今年度の活動：一般的な暗号プロトコルに関する調査（PSK）（2）

- TLS-PSKの鍵共有方式に関する安全性
  - 安全と考えられる方式（事前共有鍵が十分に大きい前提）
    - normal PSK：適切な暗号アルゴリズムとの組み合わせを用いる場合
    - RSA_PSK：適切な暗号アルゴリズムとの組み合わせを用いる場合。ただし、公開鍵証明書を参照するため、PSKの利点が小さいこともあり、opensslやGnuTLSでは実装されてない
  - 取り扱いを検討すべき方式
    - DHE_PSKおよびECDHE_PSK：ephemeralなDHおよびECDHパラメータを署名なしに使用しており、中間者攻撃が可能なため

key exchange	RFC	security	openssl-1.0.1e	gnutls-3.1.8	備考
PSK	4279	○	実装あり	実装あり	鍵長に注意
DHE_PSK	4279	×DH_anon相当	N/A	実装あり	中間者攻撃が可能
RSA_PSK	4279	○	N/A	N/A	公開鍵証明書が必要 PSKの利点が小さい
ECDHE_PSK	5489	×DH_anon相当	N/A	実装あり	中間者攻撃が可能

4. 今年度の活動：一般的な暗号プロトコルに関する調査（DNSSEC）

- DNSSECの普及状況及び運用面におけるリスク（鍵管理の課題）を整理
- DNSSECの普及状況：79のTLD(Top Lebel Domain)でDNSSEC運用(DSレコードをルートゾーンに登録済)が行われている

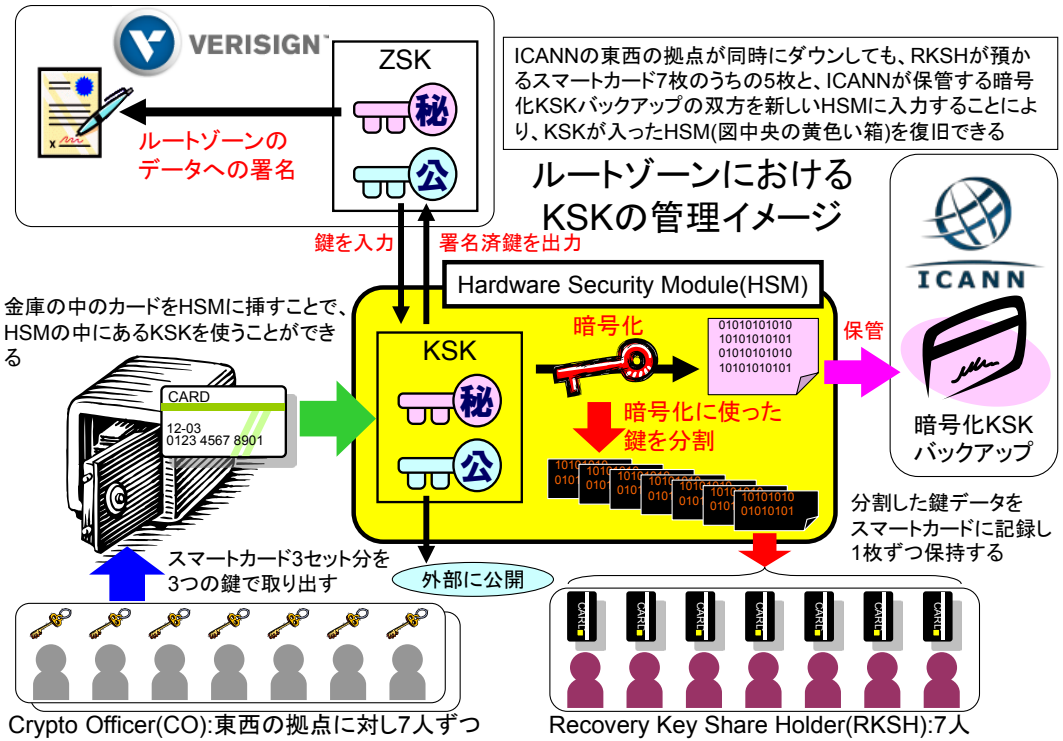


DNSSECの普及状況
出典：http://www.ohmo.to/dnssec/maps/

CRYPTREC
Cryptography Research and Evaluation Committees

4. 今年度の活動：一般的な暗号プロトコルに関する調査（DNSSEC）

- DNSSEC運用におけるリスク(鍵管理の課題)
  - 鍵や署名、手順を誤れば、正規のリソースレコードであっても署名検証に失敗し不正な情報として扱われる
  - DNSSECの運用において、「失敗が許されない運用」が要求される



4. 今年度の活動:リストガイドの利用促進に係る検討 (1)

検討の背景と検討方法

- 複数のリストガイドが作成されてきたため、今後より一層の利用を促すために、内容や運用等について検討を行う必要がある
- 利用者視点からリストガイドに関する意見を収集し、次年度以降のリストガイドの作成及び運営の指針とする

1 リストガイドに関するニーズと課題の整理

2 課題に対する提言　⇒　5. 将来に向けた展望

4. 今年度の活動：リストガイドの利用促進に係る検討（2）

ニーズ調査（委員ヒアリング）結果

- 委員へのヒアリングを行い，以下のような意見を得た

1. 内容が専門的すぎるため、想定読者を明確化するとともに一般的な用語の整理を行い、平易な内容・構成とすることが望ましい

2. 技術解説よりも、電子政府で利用可能な暗号スイートやパラメータ等を一覧化して提示することが望ましい

3. SSL/TLS等の代表的なソフトウェアについて、具体的な設定内容などを例示することが望ましい

4. 今年度の活動:リストガイドの利用促進に係る検討 (3)

課題の整理

- 既存リストガイドの位置づけ・目的
  - 現状のリストガイドには暗号実装、推奨セキュリティパラメータ、運用・鍵管理、テクニカルレポート等に関する内容が混在している
  - 想定読者がリストガイド毎に異なるため、読者がどのリストガイドを読むべきか分かりにくい

- リストガイドの情報提供体制
  - リストガイドの内容や範囲を再検討するとともに、迅速に情報提供を行うことができる体制の構築

- 情報提供機能の強化
  - リストガイドの認知度向上施策の検討

5. 将来に向けた展望：リストガイドの名称変更と目的の拡大

リストガイドの利用促進への考えられる方策を，将来に向けた展望として提言

リストガイドの名称変更

- より広範な読者の獲得等を勘案し、文書のタイトルを以下の通り修正する

CRYPTREC暗号技術利用ガイド

目的の拡大

- 民間での利用を妨げない旨を追記する

CRYPTREC暗号技術利用ガイドは、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、電子政府推奨暗号を利用する際に必要となる情報並びに推奨を示すものである。なお、電子政府以外の目的に用いることを妨げるものではない。

※参考：NIST SP800-81 “Secure Domain Name System (DNS) Deployment Guide”
This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

5. 将来に向けた展望：リストガイドの分類

リストガイドの分類

- ニーズ調査結果を踏まえ、以下の三種類のドキュメントとして整理してはどうか

CRYPTREC暗号技術利用ガイド

- 従来のリストガイドのうち、暗号実装、推奨セキュリティパラメータ、運用・鍵管理について記述したもの

CRYPTRECテクニカルレポート

- 利用ガイドの理論的・専門的な裏付けを述べたもの
- 利用ガイドには掲載されない先進的な暗号技術等の動向や技術をとりまとめたもの

CRYPTREC注意喚起レポート

- 暗号やプロトコルの監視活動において，早急に対策を要する事項が発生した場合に技術的な側面から妥当性を検討したもの

5. 将来に向けた展望：CRYPTREC暗号技術利用ガイドの分類

CRYPTREC暗号技術利用ガイドの分類

- CRYPTREC暗号技術利用ガイドを以下の3つのカテゴリに分類し、記載内容を整理することで、想定読者に適合した内容としてはどうか

カテゴリ	内容	想定読者
A 暗号実装	実装仕様、耐サイドチャネル実装などについて記載したもの	システム発注者・構築者
B 推奨セキュリティパラメータ	暗号技術・プロトコルにおける、パラメータ、ドメインパラメータ等について記述したもの	システム発注者・構築者
C 運用・鍵管理	運用・鍵管理他について記述したもの	システム運用者

【適用シナリオ1】
①システム発注者（電子政府システム発注担当官）は利用ガイドを基にシステムの発注仕様を固める
②システム構築者（ベンダー）はシステム仕様に記載されている事項に則りシステムの構築を行う
③システム運用者（ベンダー）は利用ガイド等を参考にシステムの運用を行う
【適用シナリオ2】
①システム発注者はシステム構築のためのRFPを行う
②システム構築者は利用ガイドを基に提案書の作成を行う
③システム発注者は提案書の評価において利用ガイドを利用する

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

5. 将来に向けた展望：情報提供機能の強化

情報提供機能の強化

- リストガイドの普及促進のため、リストガイドを掲載するHPを再整理する必要がある
- リストガイド公開等のタイミングで、想定ユーザである各府省庁並びにベンダ等に向けて告知を行い、認知度を向上させる必要がある

22