

DMARC/DNSSEC/RPKIガイドラインの概要

3つのガイドラインの共通構成・コンセプトの紹介

MRI 三菱総合研究所

2024/11/21

先進技術・セキュリティ事業本部

小川 博久

本資料及びDMARC以外のガイドラインは以下を参照。

総務省 | サイバーセキュリティタスクフォース | ICTサイバーセキュリティ政策分科会(第5回)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html

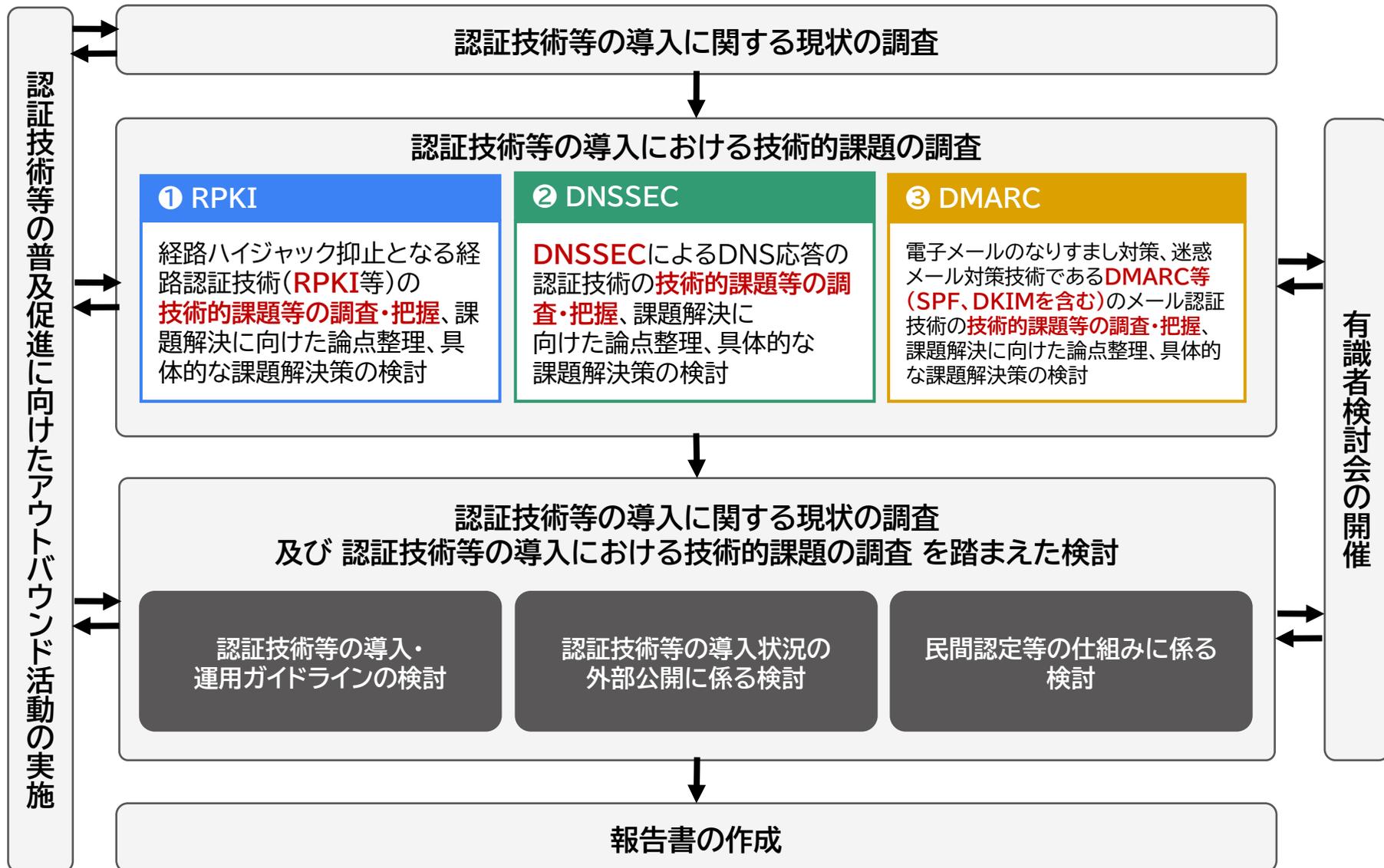
送信ドメイン認証技術DMARC導入ガイドライン 迷惑メール対策推進協議会技術ワーキンググループ

https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guideline.pdf

「RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン」公開のお知らせ - JPNIC

<https://www.nic.ad.jp/ja/topics/2024/20241113-01.html>

本事業の全体像



実証実験の規模

- 実証実験参加者の技術取得に対する要求を踏まえ、3つのコースを設け、導入における技術的課題を調査
- RPKI実証
 - 実証参加者：携帯電話サービスに関する電気通信事業者、インターネットサービスプロバイダ、電気通信事業、電力系事業者、ケーブルテレビ放送事業者、インターネットインフラ事業者、イーサネット事業者等の事業者
 - 実証参加者数：体験コースに**23組織(のべ78人)**、実験コースに**8組織**、導入検証コースに**10組織**
- DNSSEC実証
 - 実証参加者：ケーブルテレビ放送事業者、電気通信事業者・インターネットサービスプロバイダ事業者・インターネットインフラ事業者等の事業者
 - 実証参加者数：体験コースに**17組織(のべ34人)**、実験コースに**2組織**、導入検証コースに**6組織**
- DMARC実証
 - 実証参加者：ケーブルテレビ放送事業者、電気通信事業者・インターネットサービスプロバイダ事業者・インターネットインフラ事業者、金融機関等の事業者
 - 実証参加者数：体験コースに**18組織(のべ68人+現地参加30人(所属不明))**、実験コースに**3組織**、導入検証コースに**7組織**

コース名	特徴	説明
体験コース	リモート参加な体験およびディスカッションで理解を深めるコース	基本的な機能及び設定や動作を学習する技術者を対象として、座学および ハンズオン形式で技術を体験 するコース
実験コース	自組織ではない仮想環境で検証を行う組織向けのコース	基本的内容を理解しているが 導入・運用に関する課題や運用手順などのイメージ がない技術者を対象として、仮想環境などを提供して実験するコース
導入検証コース	自社に検証環境を設け、検証を行う組織向けのコース	導入・運用はイメージできているが実環境での確認する機会がない又はノウハウがない技術者を対象として、 実環境での導入を検証 するコース

実証実験の結果 得られた知見

①RPKI

基礎知識とROVの設定方法

- 基礎的な知識の習得
 - 不具合が発生した場合の**対処知識の不足**しているため障害の**即時対応が出来るか懸念が多い**との声が多かったが、実証実験を通じて、基礎的な知識を習得できた
- 設定方法の知見が得られた
 - ROVの設定方法や運用に必要な設定に対する知見が得られた

②DNSSEC

自動化による導入障壁の減少と通常運用

- 自動化により、導入障壁が下がった
 - KnotDNS等による**自動化により、導入の障壁が下がった。**
- 通常運用に必要な知見が得られた
 - 通常であれば運用上の問題もない**と言える。

③DMARC

サブドメイン管理や偽陽性対策

- サブドメインの管理方法の習得
 - サブドメインの管理方法が理解でき、サブドメインごとのDMARCポリシー設定の方法についても理解が進んだ。
- 偽陽性対策の知識習得
 - 転送やメーリングリストによって発生する偽陽性の問題の対策が理解できた。

ガイドラインの構成とコンセプト

ガイドライン案の方向性

● 実証事業の結果を受けてガイドライン案を作成

- 本ガイドライン案は、令和4年度および令和5年度における実証事業の結果を受け、実証事業者から求められる声と有識者の意見を総合して、わかりやすく・実践的なガイドラインを目指し作成した。

● 3技術ごとにガイドライン案を分けて作成

● 対象者ごとに章立てを分けて作成

- 「第一章」は、主として経営者に対し、企業が技術を導入する意義やレピュテーションリスク等について記載した。
- 「第二章」以降は、項目ごと、または対象となる技術者ごとに分けて、当該内容を記載した。

● ガイドラインとガイドブック

- 技術によっては、「ガイドライン」と「ガイドブック」の明確な線引きが難しいとの判断されるものもあったが、技術の導入及び普及促進を進める観点から、事業会社の背中を押すことを目指した「ガイドライン」として作成した。

● 今後のメンテナンスを配慮して作成

- 標準規格やRFC等を含め、技術情報のアップデートが必要になるため、アップデートを想定したドキュメント構成として作成した。(例えば、アップデートが想定される部分については、外部を参照する形とした)

ガイドライン案の特徴① 既存ガイドラインとの違い

①RPKI

既存ガイドラインとの違い

- これまで日本語版の解説はあったが、ガイドラインはなかった。特に以下を解説
 - IPアドレスの分配を受けた者が実施すべきこと 2.1節 ROA
 - AS運用をしている者が実施すべきこと 2.2節 ROV
- RPKIだけでない不正経路の対策としてBGPにおけるセキュリティ等も解説。

②DNSSEC

既存ガイドラインとの違い

- DNSSECの複雑な概念を、段階的に理解しやすいように3段階の成熟モデルを設定した。
- 成熟モデルを参考に、段階的な目標設定ができ、それぞれの段階で必要な知識やスキルが理解できる。
- 段階的な導入計画を考えられ、状況に応じた導入や運用効率策を考えることもできる。

③DMARC

既存ガイドラインとの違い

- 最低限必要な知識と設定にフォーカスした。これからDMARCの導入を考える方に向け、現時点で最低限必要な情報をわかりやすくまとめ、詳細な設定やパラメータは、送信ドメイン認証技術導入マニュアル(迷惑メール対策推進協議会発行)を参照することで、必要な対策を簡潔に確認できる。

ガイドライン案の特徴② 要求項目・対応項目の明確化

①RPKI

要求項目・対応項目の明確化

- 導入・運用の役割や担当に分け、対策をしなければいけない項目(必須)、対策することが望ましい項目(推奨)をわかりやすく示しています。
 - ROA:IPアドレスの分配を受けている組織等 必須:2項目
 - ROV:ASを運用している組織等 推奨:1項目

②DNSSEC

要求項目・対応項目の明確化

- 役割や担当別に、対策をするべき・対策を推奨する等のレベル分けし、わかりやすく示した。
 - フルリゾルバ(第2章) 22項目(Must: 4、Must not: 2、Should: 13、May: 3)
 - 権威DNS(第3章) 25項目(Must: 5、Must not: 1、Should: 15、May: 4)
 - ドメイン名登録
・登録管理関係者(第4章) 6項目(Must: 3、Must not: 0、Should: 2、May: 1)

③DMARC

要求項目・対応項目の明確化

- 役割や担当別に、対策をするべき・対策を推奨する等のレベル分けし、わかりやすく示した。
 - ドメイン管理者(第2章) 15項目(Must: 4、Should: 6、May: 5)
 - メール配送事業者(第3章) 4項目(Must: 2、Should: 2、May: 0)
 - メール再配送事業者(第4章) 7項目(Must: 5、Should: 0、May: 2)
 - メール受信者(第5章) 10項目(Must: 4、Should: 4、May: 2)

ガイドライン案の特徴③ 運用できるための三つの確証

①RPKI

運用できるための三つの確証

- RPKI技術の導入・運用ができるという確証を得る3つのポイントを示している。
 - 導入する意義・メリット ROA 2.1.5節 ROV 2.2.7節
 - 正常動作が確認できる ROA 2.1.5節 ROV 2.2.7節
 - 不具合が発生した際のトラブルシューティング ROA 2.1.5節 ROV 2.2.7節

②DNSSEC

運用できるための三つの確証

- DNSSEC技術の導入・運用ができるという確証を得る3つのポイントを示した。
 - 導入する意義・メリット フルリゾルバー：0章 権威DNSサーバー：0章
 - 正常動作が確認できる フルリゾルバー：2.7節 権威DNSサーバー：3.4節
 - 不具合が発生した際のトラブルシューティング フルリゾルバー：2.6節 権威DNSサーバー：3.5節

③DMARC

運用できるための三つの確証

- DMARC技術の導入・運用ができるという確証を得る3つのポイントを示した。
 - 導入する意義・メリット 1章
 - 正常動作が確認できる 2.1節、2.4節など
 - 不具合が発生した際のトラブルシューティング 2.4節、マニュアル※参照

※マニュアル：送信ドメイン認証技術導入マニュアル

ガイドライン案の目的

①RPKI

- 目的
- 不正な経路情報に起因する様々な不具合、および不正な経路情報を用いた犯罪等を抑止するにあたり、RPKI技術を用いた対策技術を各組織や個人において導入する判断に資する事項を示し、相互接続ネットワークであるインターネットにおける、不正な経路情報特にRPKIを使った対策技術の普及・促進を図る。

②DNSSEC

- 目的
- ドメイン名の保護は、顧客とビジネスの両方をオンライン上の様々な脅威から守るために重要であり、単に技術的な問題だけではなく、ビジネスの持続可能性と成長に直接関わる重要な課題として認識いただくとともに、ドメインを守る仕組みの一つにDNSSECがあるということを示し、対策技術の普及・促進を図る。

③DMARC

- 目的
- 迷惑メール・なりすましメールによる様々な被害を減らすため、メール送信側と受信側の双方が送信ドメイン認証技術に対応しなければ、正しくメールが届く認証機能を有したメール配送環境を実現できないことを示し、DMARC・SPF・DKIM等認証技術の導入の必要性の理解とこれら認証技術の普及・促進を図る。

ガイドライン案の対象読者

①RPKI

対象読者

- 国内のISP等、インターネットの接続性に関わる事業や技術的運用を行っている組織の経営者及び技術者の方向け

②DNSSEC

対象読者

- ドメイン名が利用可能になるまでの段階に必要な関係する組織(ドメイン名登録者・ドメイン名登録事業者・権威DNSサーバ運用者・フルリゾルバー運用者が関係する組織)の経営者及び技術者の方向け

③DMARC

対象読者

- 送信ドメイン認証技術の導入及び運用を検討している、ドメイン名の管理・メール送信事業・メール配信事業・メール受信事業に関係する組織の経営者及び技術者の方向け

RPKIガイドライン案 骨子案(目次)

● タイトル「RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン案」

経営者に対し、企業が技術を導入する意義やレピュテーションリスク等について記載

第1章	ガイドラインの趣旨
1.1	本ガイドラインの活用方法
1.2	インターネットにおける経路情報
1.3	不正な経路情報のリスクや損失
1.4	対策技術 — RPKIとROA、ROV
1.5	実施事項

対象となる技術者ごとに分けて、当該内容を実例を含めて記載

第2章	技術的情報	2.2.4	ROAキャッシュサーバの構築
2.1	ROA/IPアドレスの分配を受けた者の実施事項	2.2.5	ルータ側のROV設定
2.1.1	ROAとは	2.2.6	ROVによる経路制御の詳細
2.1.2	不正経路とIPアドレスに関する考え方	2.2.7	重要事項:ROV導入に関わる三つの確認
2.1.3	ROAの作成と運用管理	2.2.8	ROVの設定例
2.1.4	BGP経路とROAを一致させる手順	2.2.9	運用上の注意と懸念点
2.1.5	重要事項:ROAの導入に関わる三つの確認	2.3	ROA/ROV以外の不正経路対策
2.1.6	例外的な処置	2.3.1	BGPにおけるセキュリティ要素と考え方
2.2	ROV/AS運用をしている者の実施事項	2.3.2	ASパス検証の今後と運用について
2.2.1	不正経路への対策と考え方とROV		
2.2.2	ROVの導入と運用方針	第3章	付録
2.2.3	ROAキャッシュサーバ・ROVの所在		

DNSSECガイドライン案 骨子案(目次)

経営者に対し、企業が技術を導入する意義やレピュテーションリスク等について記載

序章	想定読者と用語	第1章	ドメイン名の重要性和ライフサイクル
1	想定する読者	1.1	エグゼクティブサマリ
2	各関係者が読むべき章	1.2	ドメイン名の重要性
3	ドメイン名登録者への注意 要求レベルに関する用語	1.3	ドメイン名の保護
		1.4	ドメイン名の登録とライフサイクルマネージメント
		1.5	ドメイン名を守るためのDNSSEC

対象となる技術者ごとに分けて、当該内容を実例を含めて記載

第2章	フルリゾルバーのDNSSEC対応	第3章	権威DNSサーバーのDNSSEC対応
2.1	DNSSEC対応の基礎	3.1	DNSSEC対応の基礎
2.2	DNSSEC対応の要件	3.2	DNSSEC対応の要件
2.3	導入準備	3.3	導入の準備
2.4	導入	3.4	運用
2.5	運用	3.5	トラブルシューティング
2.6	トラブルシューティング	3.6	運用ノウハウ
2.7	運用ノウハウ	3.7	参考文献
2.8	参考文献	第4章	ドメイン名登録・登録管理関係者
		4.1	レジストラ(指定事業者)
		4.2	ドメイン名登録者
		第5章	付録

DMARCガイドライン案 骨子案(目次)

経営者に対し、企業が技術を導入する意義やレピュテーションリスク等について記載

第1章	はじめに 本ガイドラインについて(経営者向け)
-----	----------------------------

対象となる技術者ごとに分けて、当該内容を実例を含めて記載

第2章	ドメイン管理者(メール送信者)	第5章	メール受信者
2.1	送信側の送信ドメイン認証設定	5.1	送信ドメイン認証
2.2	DMARC の組織ドメイン名への設定	5.2	認証ドメイン名の評価
2.3	メールに利用しないドメイン名への設定	5.3	フィードバック
2.4	DMARC レポートの活用とポリシーの強化	5.4	メール受信者にわかりやすい認証結果の提示
第3章	メール配送事業者	第6章	付録
3.1	認証ドメイン名の扱い		
第4章	メール再配送時の設定(中間事業者)		
4.1	転送メールの設定		
4.2	メーリングリストの設定		

参考

- 参考1. 有識者検討会参画メンバー一覧・実証事業参加者一覧
- 参考2. 各認証技術体験コースのコースマテリアル

参考1. 有識者検討会参画メンバー一覧

● 各種認証技術における有識者検討会参画メンバー一覧

① RPKI | 有識者会議参画メンバー

No	氏名	所属
1	蓬田 裕一	株式会社インターネットイニシアティブ(IIJ)
2	渡辺 英一郎	NTTコミュニケーションズ株式会社
3	芦田 宏之	BBIX株式会社
4	中村 修	慶應義塾大学 環境情報学部 教授
5	猪俣 敦夫	大阪大学 サイバーメディアセンター 教授
6	矢内 直人	大阪大学 大学院情報科学研究科 准教授
7	岡田 雅之	長崎県立大学 情報システム学部 情報セキュリティ学科 教授
8	服部 亜希子	シスコシステムズ合同会社
9	渡邊 貴之	ジュニパーネットワークス株式会社
10	清水 一貴	ジュニパーネットワークス株式会社
11	北内 薫	ジュニパーネットワークス株式会社
12	小川 怜	ノキアソリューションズ&ネットワークス合同会社
13	土屋 師子生	アリスタネットワークスジャパン合同会社

② DNSSEC | 有識者会議参画メンバー

No	氏名	所属
1	石田 慶樹	日本DNSオペレーターズグループ(DNSOPS)/ 株式会社JPIX
2	野々下 幸治	トレンドマイクロ株式会社
3	其田 学	株式会社インターネットイニシアティブ(IIJ)
4	永井 祐弥	GMOインターネットグループ株式会社
5	関谷 勇司	東京大学 大学院 情報理工学系研究科 教授
6	米谷 嘉朗	株式会社日本レジストリサービス ※2023/9まで
7	高田 美紀	NTTコミュニケーションズ株式会社

③ DMARC | 有識者会議参画メンバー

No	氏名	所属
1	木村 泰司	一般社団法人日本ネットワーク インフォメーションセンター(JPNIC)
2	平塚 伸世	一般社団法人JPCERTコーディネーション センター(JPCERT/CC)
3	野々下 幸治	トレンドマイクロ株式会社
4	櫻庭 秀次	JPAAWG/ 株式会社インターネットイニシアティブ(IIJ)
5	未政 延浩	JPAAWG/株式会社TwoFive
6	中村 成陽	LINEヤフー株式会社

参考1. 実証事業参加者一覧

● 各種認証技術における実証事業参加者一覧

① RPKI | 実証事業参加者一覧

No	社名
1	株式会社愛媛CATV
2	有限会社ナインレイヤーズ
3	株式会社イプリオ
4	山陰ケーブルビジョン株式会社
5	株式会社アットアイ
6	株式会社NTTドコモ
7	中部テレコミュニケーション株式会社
8	株式会社JPIX
9	KDDI株式会社
10	BBIX株式会社
11	株式会社フォーサイトウェブ
12	株式会社グローバルネットコア
13	株式会社STNet
14	ケーブルテレビ株式会社
15	株式会社オプテージ
16	ビッグロブ株式会社
17	株式会社ニューメディア
18	北海道総合通信網株式会社(HOTnet)

② DNSSEC | 実証事業参加者一覧

No	社名
1	有限会社ナインレイヤーズ
2	株式会社イプリオ
3	山陰ケーブルビジョン株式会社
4	株式会社アットアイ
5	株式会社フォーサイトウェブ
6	株式会社グローバルネットコア
7	ケーブルテレビ株式会社
8	株式会社ラック

③ DMARC | 実証事業参加者一覧

No	社名
1	株式会社イプリオ
2	株式会社アットアイ
3	株式会社フォーサイトウェブ
4	株式会社北陸銀行
5	株式会社ラック
6	JCOM株式会社
7	株式会社大分銀行
8	GMOあおぞらネット銀行株式会社
9	株式会社みんなの銀行
10	株式会社りそなホールディングス

参考2. 各認証技術体験コースのコースマテリアル

① RPKI | 体験コースコースマテリアル一覧

No	タイトル	概要
1	RPKI・リソース証明書・ROA	RPKI・リソース証明書・ROA技術内容を口頭で説明、質疑応答
2	オリジン検証	オリジン検証について口頭解説、質疑応答
3	不正経路とROVの体験	遠隔からのリモート及び、検証サイトでのハンズオン形式で自分の端末にクライアント証明書・経路証明書を導入し、実験環境に用意されたRPKIシステムを入切りして不正経路に接続されなくなることを実体験
4	ルータの設定	試験環境で普段出来ないルータ設定を変えてみる
5	ディスカッション	ハンズオンでの不明点等を会話でフォロー

② DNSSEC | 体験コースコースマテリアル一覧

No	タイトル	概要
1	レコードの整合性や信頼性を検証可能に	署名検証は応答ごとに検証することを確認するプロセスを解説
2	公開鍵暗号技術を用いた電子署名	KSK/ZSKの仕組みを解説
3	ログイン	事前に用意されたドメインと仮想環境でログインし、鍵の生成など環境設定を解説
4	鍵交換	鍵のロールオーバーのタイミングなどの解説、及び鍵交換が正しく行われなかった際にどうなるのかを解説
5	DNSの不正応答	SERV FAILを体験し、不正応答時の状態を解説

③ DMARC | 体験コースコースマテリアル一覧

No	タイトル	概要
1	送信ドメイン認証の考え方	送信ドメイン認証についての基礎知識 (SPF、DKIM等)概要を解説
2	メールの基礎知識	ヘッダ情報、エンベロープ情報によるなりすまし事例や、SPF、DKIM、DMARCの各技術の概要についてを解説
3	DMARCの対応方法	送信側、受信側それぞれにおけるDMARCの対応方法について解説
4	OSS紹介	一般的に使われるOSSとして、OpenDMARCとOpenDKIMについて紹介
5	DMARCレポート	DMARCレポートとはどういう形式で、何が分かるものなのかについて解説
6	DMARCポリシー運用	none、quarantine、rejectのそれぞれのポリシーについて解説及びポリシー強化について解説

RPKI体験コースの受講

