資料５－６

令和5年度
ISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査

三菱総合研究所

2024/04/05

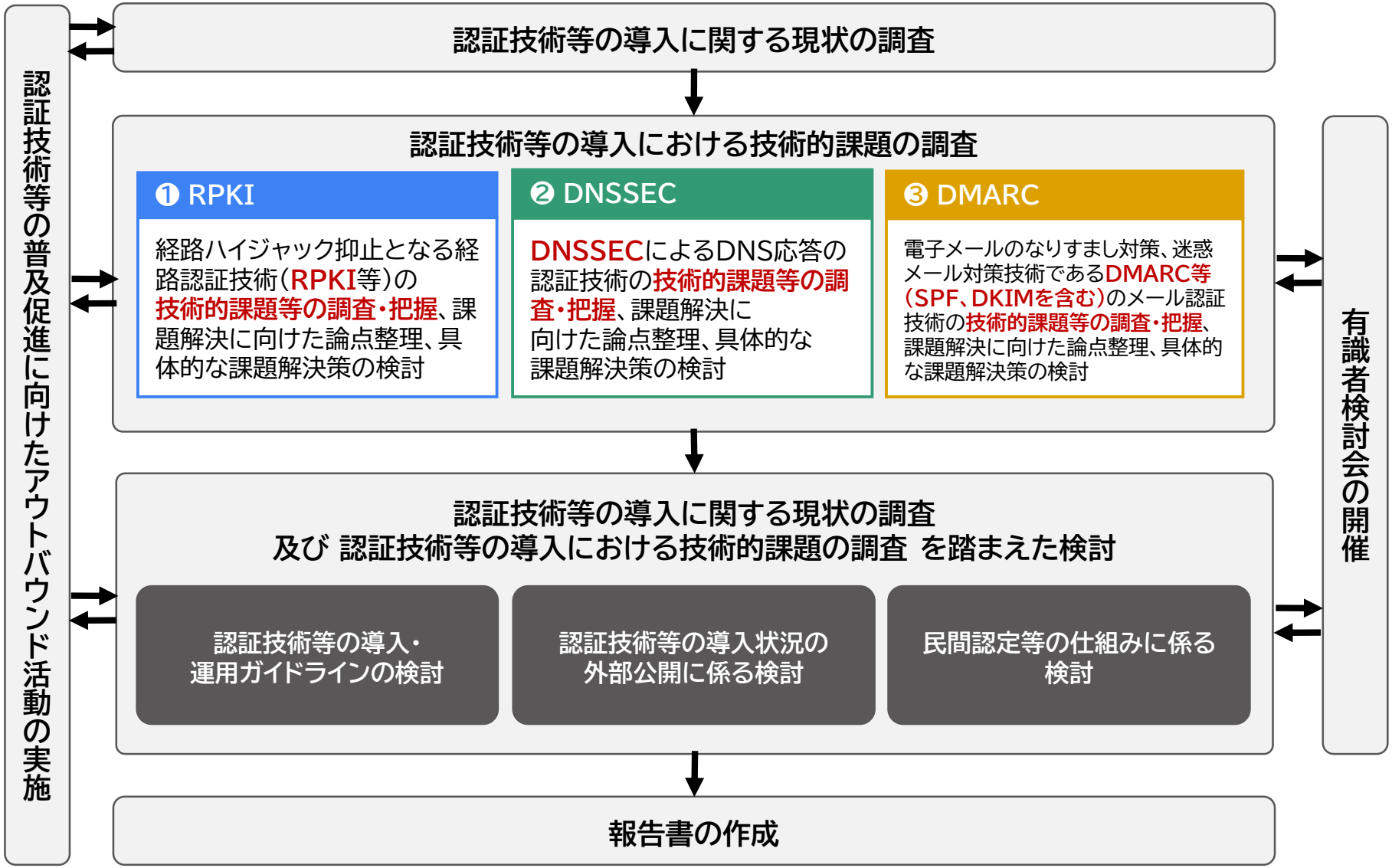
先進技術・セキュリティ事業本部

小川 博久 <hirohisa_ogawa@mri.co.jp>

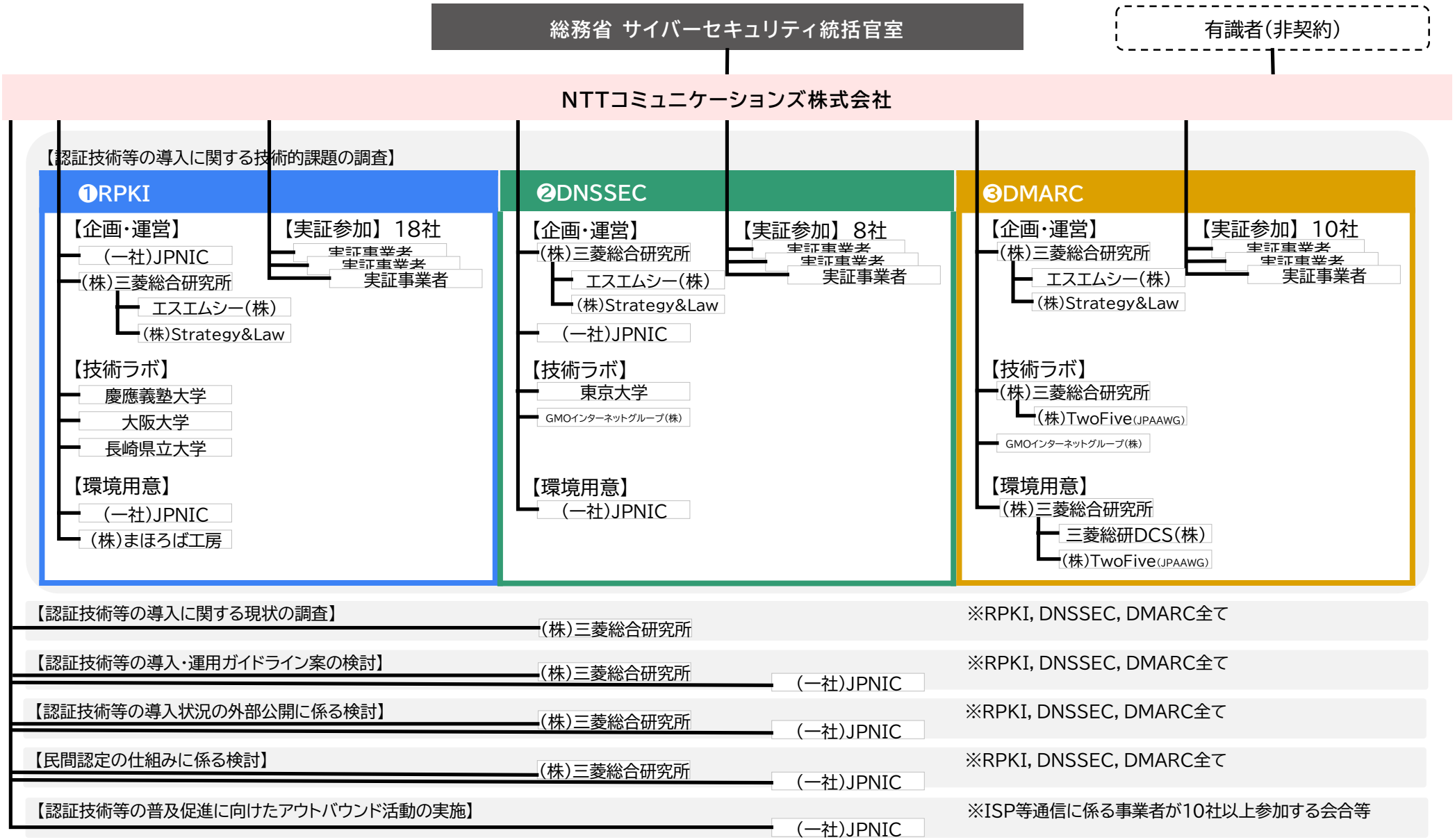
1. 本事業の全体像・体制

- 本事業の全体像
- 本事業の体制

本事業の全体像



本事業の体制

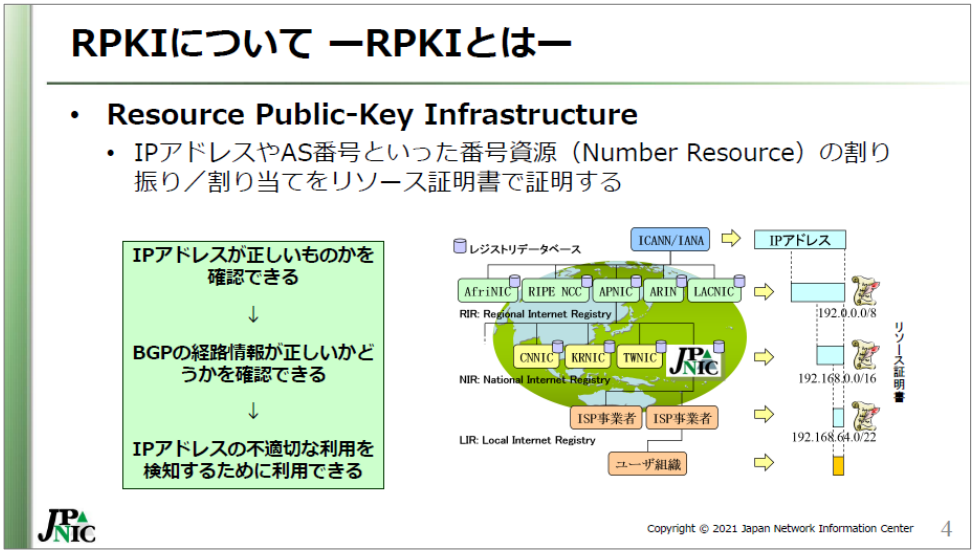


2. 認証技術の概要と普及状況

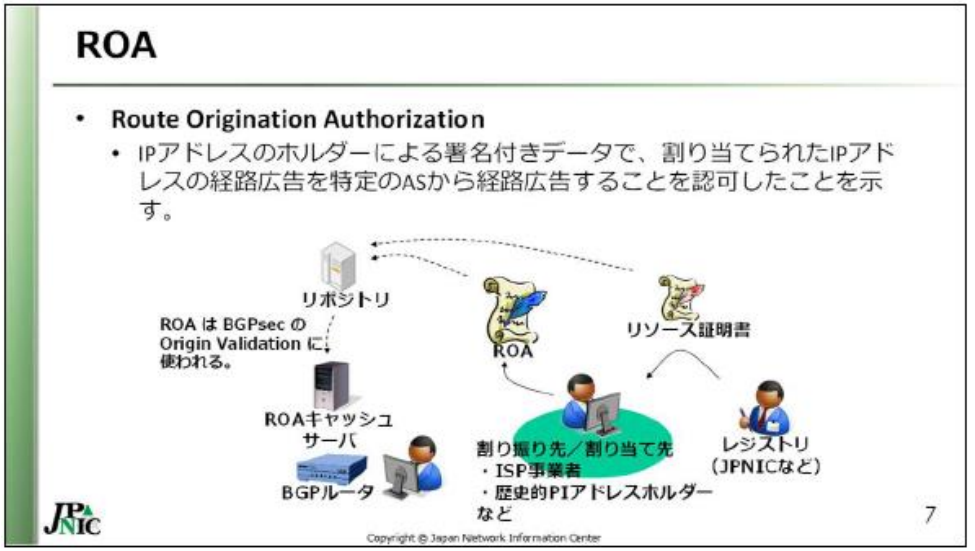
- 認証技術の概要
- 認証技術の普及状況
  - RPKI
  - DNSSEC
  - DMARC

RPKIの概要

- IPアドレスやAS番号などアドレス試験の割振り・割当てにおいては、「不正なインターネット経路制御を回避し、セキュアなインターネット経路制御を確保すること」、「 IPアドレスが正しく割り振られたものであるかどうかを確認すること」に課題があった。
- RPKI(リソースPKI – Resource Public-Key Infrastructure)は、IPアドレス等のアドレス資源管理における公開鍵認証基盤である。この基盤技術はIPアドレスなどのアドレス資源の分配について電子証明書を用いて証明するもので、**IETF*1において標準化**されている。
- 「経路ハイジャック*2抑止となる経路認証技術」とは「**ROA**(Route Origination Authorization)」と、BGP経路情報の検証である「**ROV**(Route Origin Validation)」の二つを意味しており、その導入には**「ROAの作成」と「ROVの実施」という二つの側面**がある。
- これらの技術を使い、インターネット利用者を不正な経路へ誘導されることなく、正しい経路に導くことができる。
  一方で、RPKIの**設定を誤る**とインターネットサービスを利用できなくなるといった**懸念**もある。



サイバーセキュリティタスクフォース(第30回)資料30－3の抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

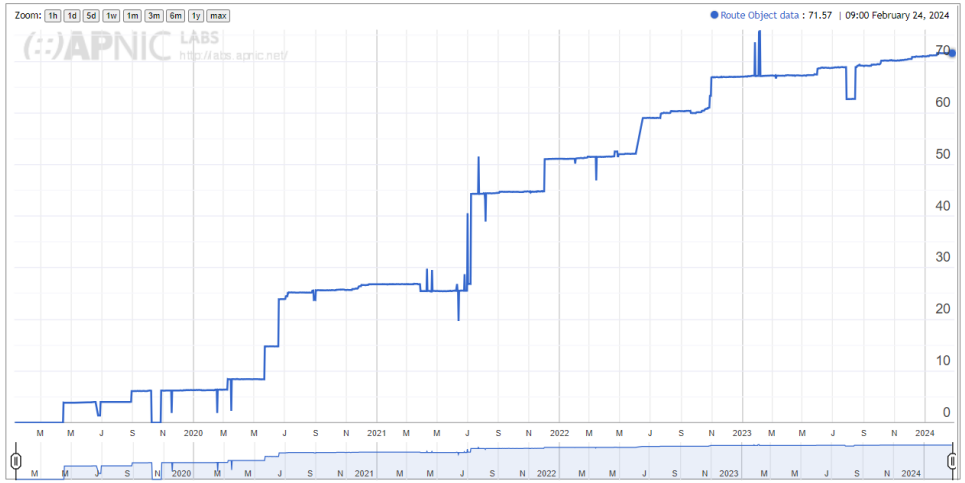


JPNIC技術セミナー「RPKI入門より」 https://www.nic.ad.jp/ja/tech/seminar/

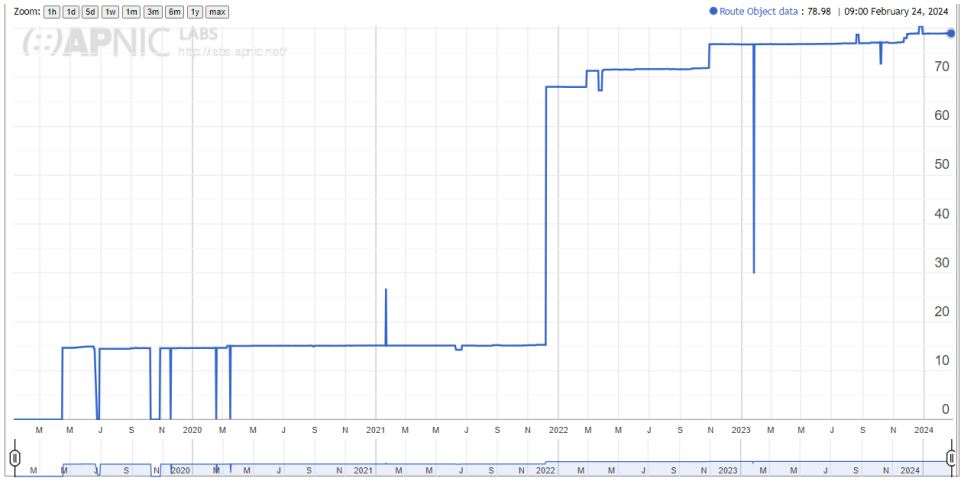
*1 IETFとは、Internet Engineering Task Forceの略称であり、インターネット技術の標準化を推進する任意団体
*2 経路はジャックとは、不正な経路情報を流すことによって経路を操作・ハイジャックする状態

RPKIの普及状況【ROA】

- 国内のIPv4[*1]アドレスを使ったBGP経路全体のうち、ROAによってカバーされていてAPNIC観測点においてValidであるものは**増加傾向にあり71.57%**に達している。また、国内のIPv6[*2]についても**増加傾向にあり78.98%**に達している。なお、上記はIPアドレス単位の普及状況であり、企業単位では一部の大手企業には普及が進んでいるものの、地域ISP等では普及が進んでいない状況がある。



IPv4 71.57%（2024年2月22日時点）



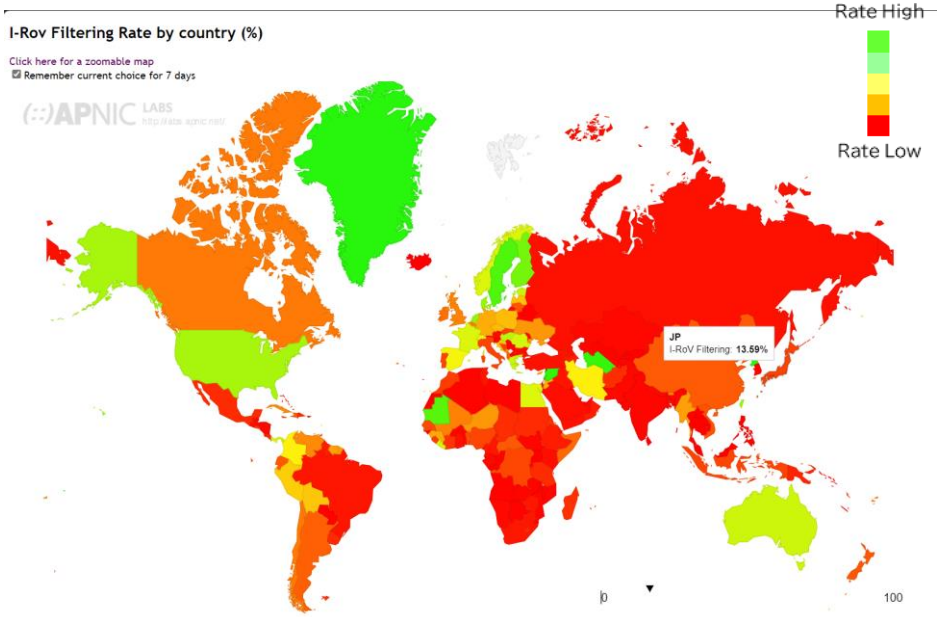
IPv6 78.98%（2024年2月22日時点）

Use of Route Object Validation for Japan (JP) https://stats.labs.apnic.net/roa/JP?o=cJPl0r1v4tadpxv&t=Address+Span&x=Valid&v=IPv4&d=Percent&l=1

*1　IPv4とは、Internet Protocol version 4の略で、インターネット上でデバイス同士を識別・通信するためのアドレス方式
*2　IPv6とは、Internet Protocol version 6の略で、IPv4に比べ、接続できるIPアドレス数や接続方式が増え、IPSec（ネットワーク上で安全な接続を設定するための一連の通信規則またはプロトコル）が必須のため、高いセキュリティを確保できるアドレス方式

RPKIの普及状況【ROV】

- APNIC Labsでは、RPKIの導入状況を公表している。
- APNICの調査によると、2024年2月時点で、**日本（JP）のValidation率は、13.59%**に留まっている。
- 米国（US）は70%台、フランス（FR）・ドイツ（DU）などの40～50%台に比して日本は圧倒的に普及率が低い。
- 日本国内のROVの導入例が少ないため不正経路の影響を小さくするために国内ISP等におけるROVの導入が課題である。

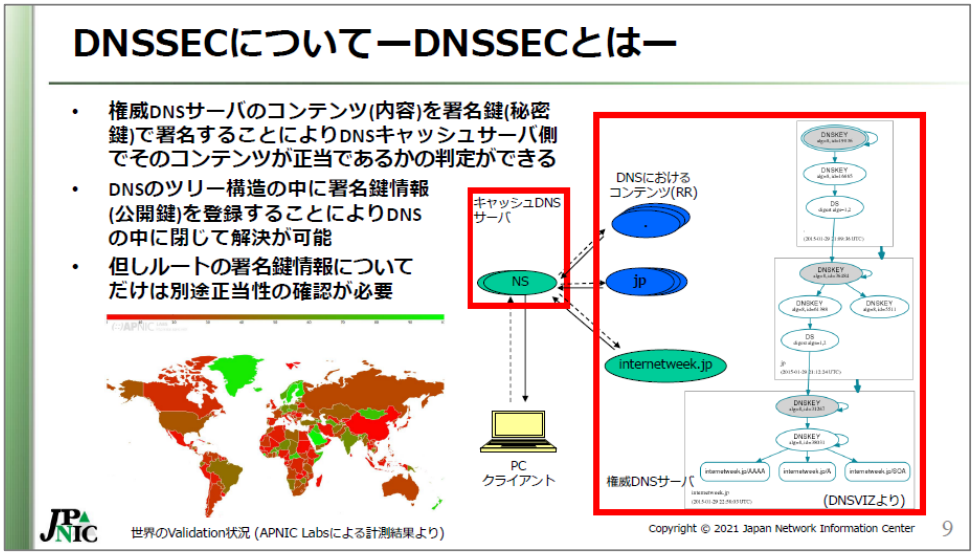


国	I-RoVフィルタリング	サンプル	重さ	加重サンプル
デンマーク,北欧,ヨーロッパ	72.41%	141,013	0.43	60,680
台湾,東アジア,アジア	70.80%	558,888	0.48	270,478
アメリカ合衆国,北アメリカ,アメリカ大陸	70.44%	6,671,366	0.4	2,700,997
ルクセンブルク,西ヨーロッパ,ヨーロッパ	69.15%	13,006	0.52	6,769
バミューダ諸島、北アメリカ、アメリカ大陸	66.60%	3,479	0.19	666
⋮				
リベリア、西アフリカ、アフリカ	58.69%	7,085	0.76	5,350
パナマ,中央アメリカ,アメリカ大陸	58.01%	32,297	0.92	29,695
フランス,西ヨーロッパ,ヨーロッパ	57.76%	670,563	0.84	562,263
ケイマン諸島、カリブ海、アメリカ大陸	57.50%	2,553	0.24	613
エジプト、北アフリカ、アフリカ	57.44%	480,376	1.25	598,652
⋮				
コロンビア,南アメリカ,アメリカ大陸	48.23%	282,682	1.31	371,706
クロアチア,南ヨーロッパ,ヨーロッパ	44.87%	38,931	0.68	26,602
ドイツ,西ヨーロッパ,ヨーロッパ	42.03%	633,349	1.17	741,543
ペルー,南アメリカ,アメリカ大陸	41.88%	200,396	0.98	196,319
ボリビア、南アメリカ、アメリカ大陸	40.56%	69,330	0.94	65,174
⋮				
ポルトガル,南ヨーロッパ,ヨーロッパ	13.90%	171,425	0.49	84,647
イタリア,南ヨーロッパ,ヨーロッパ	13.80%	572,299	0.68	391,310
日本,東アジア,アジア	13.73%	1,765,133	0.66	1,167,562
スロバキア,東ヨーロッパ,ヨーロッパ	13.36%	59,961	0.85	50,888
東ティモール,東南アジア,アジア	12.53%	1,676	2.64	4,423

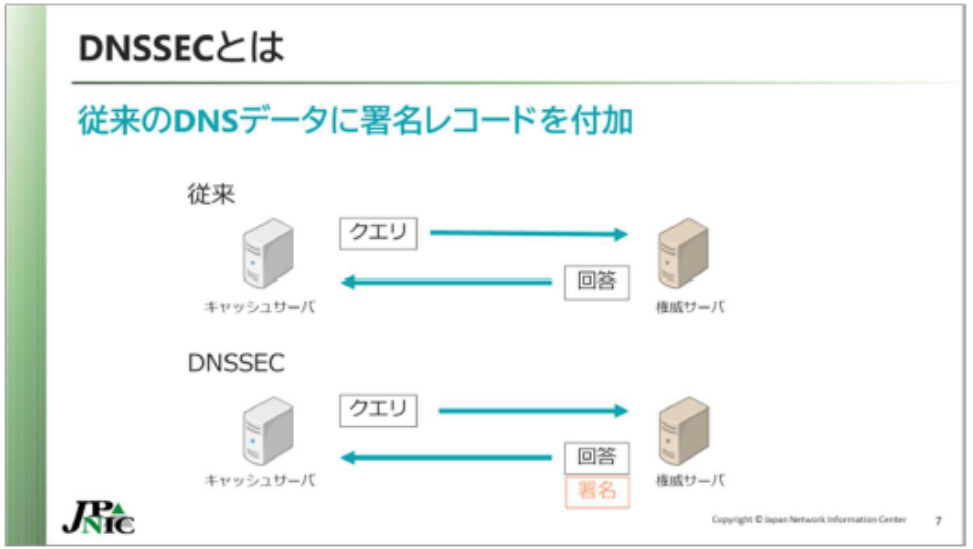
I-Rov Filtering Rate by country（%）https://stats.labs.apnic.net/rpki

DNSSECの概要

- ユーザをフィッシングサイトなどの悪意あるサイトへ誘導し情報を盗み出すことを目的とした、DNSキャッシュポイズニング*1やDNSハイジャック*2などの攻撃に対し課題があった。
- DNSSEC（DNSSECurity extensions）は、DNS の仕組みに則りつつ拡張を行ったもので、ゾーンやリソースレコードといったDNS の仕組みをそのまま使うものになっている。
- DNSSECでは、リソースレコードに電子署名を付与するため、改ざん検知が可能となる。暗号化の機能はなく、あくまでクライアント側（リカーシブリゾルバ）において**不正な情報が検知できる**ようにするものである。
- DNSSEC導入により、DNS応答の偽造による偽サイトへの誘導や情報の詐取を図るDNSキャッシュポイズニングを検知し、攻撃を防ぐことができる。一方で、DNSSECの**設定や運用を誤る**とインターネットに**接続できなくなるといった懸念**もある。



サイバーセキュリティタスクフォース（第30回）資料30－3の抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

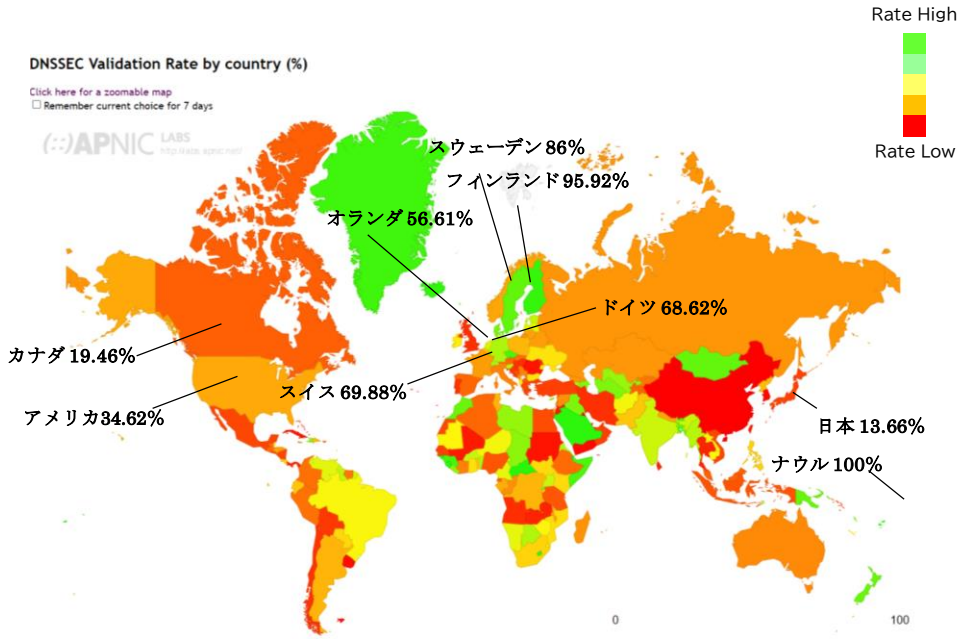


JPNIC技術セミナー「RPKI入門より」」https://www.nic.ad.jp/ja/tech/seminar/

*1　DNSキャッシュポイズニング攻撃とは、偽のDNS応答をキャッシュDNSサーバーにキャッシュさせることで偽のサイトに誘導し、ドメインの乗っ取りやフィッシングなどを図る攻撃手法
*2　DNSハイジャック攻撃とは、Webサイトのドメインを不正に操作する攻撃手法

DNSSECの普及状況

- APNIC Labsが公表するDNSSECの導入状況によると、ナウル（NR）が世界で唯一のバリデーション率100%を示しており、欧州では北欧の数値が高く、ドイツ（DE）68.62%、オランダ（NL）56.61%も比較的高い数値が見られる一方で、アメリカ（US）34.62%、カナダ（CA）19.46%と北米では低い数値を示している。
- 2024年2月29日時点で、**日本（JP）は、13.66%**に留まっている。



国	DNSSEC の検証	部分的な検証	合計検証数	サンプル	重さ	加重サンプル
ナウル、ミクロネシア、オセアニア	100.00%	0.00%	100.00%	137	3.28	448
ギニアビサウ、西アフリカ、アフリカ	99.30%	0.64%	99.95%	5,742	0.99	5,682
⟆						
フィンランド,北欧,ヨーロッパ	95.94%	1.04%	96.98%	405,007	0.77	312,608
レソト、南部アフリカ、アフリカ	95.60%	2.83%	98.43%	9,711	5.14	49,868
⟆						
ドイツ,西ヨーロッパ,ヨーロッパ	68.52%	5.08%	73.60%	3,572,780	1.26	4,508,418
マヨット、東アフリカ、アフリカ	67.97%	2.08%	70.06%	2,782	4.2	11,693
⟆						
オランダ,西ヨーロッパ,ヨーロッパ	56.73%	4.24%	60.97%	1,160,566	0.93	1,076,383
ベネズエラ 南アメリカ アメリカ大陸	56.03%	6.91%	62.94%	754,299	1.67	1,260,894
⟆						
アメリカ合衆国,北アメリカ,アメリカ大陸	34.62%	4.53%	39.15%	40,928,326	0.4	16,421,468
パレスチナ国家、西アジア、アジア	34.42%	2.40%	36.82%	142,133	1.71	243,165
⟆						
カナダ、北アメリカ、アメリカ大陸	19.59%	3.70%	23.29%	3,789,119	0.63	2,369,363
タンザニア連合共和国、東アフリカ、アフリカ	17.91%	24.93%	42.84%	304,393	2.9	882,399
⟆						
日本,東アジア,アジア	13.66%	6.59%	20.25%	8,822,643	0.8	7,098,524
アラブ首長国連邦、西アジア、アジア	13.36%	4.04%	17.40%	563,314	1.07	603,157

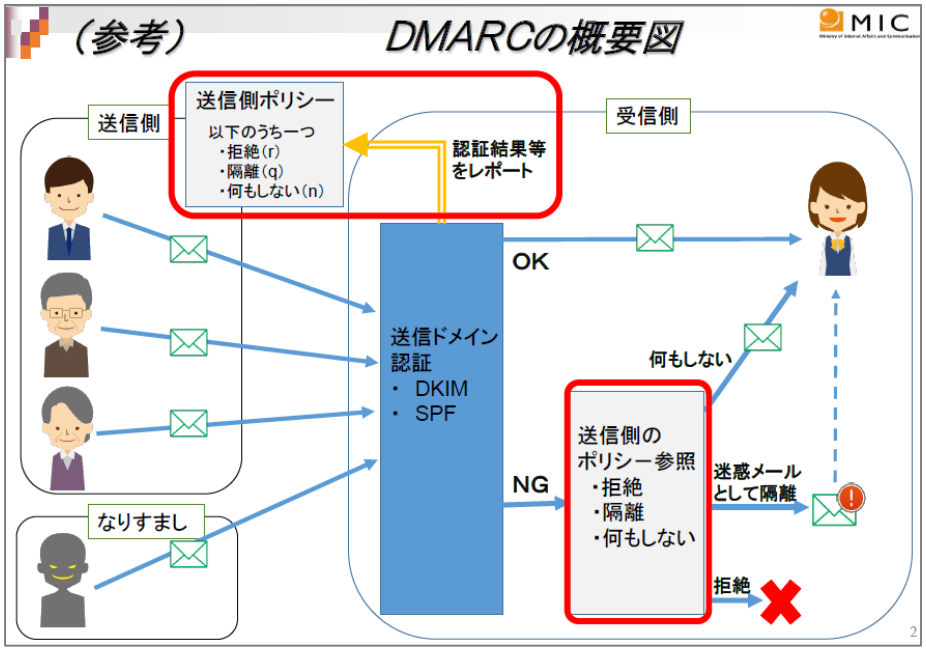
DNSSEC Validation Rate by country（%） https://stats.labs.apnic.net/dnssec
上記は、国別ドメインコードからサンプルを抽出し、DNSSECで検証できた比率であり、実際の導入状況と異なる場合がある

- なお、DNSサーバー管理には、DDoS攻撃の踏み台にならないために、オープンリゾルバー対策が必要である。

オープンリゾルバ(Open Resolver)に対する注意喚起 – JPNIC https://www.nic.ad.jp/ja/dns/openresolver/
DNSサーバーの不適切な設定「オープンリゾルバー」について | JPRS https://jprs.jp/whatsnew/topics/2013/130418.html
DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起 https://www.jpcert.or.jp/at/2013/at130022.html

DMARCの概要

- なりすまし・詐欺・サイバー攻撃など巧妙化したメールの脅威が高まっており、メールの信頼性を確保するために受信者と送信者の双方を守る対策が求められていた。
- DMARC（Domain-based Message Authentication Reporting and Conformance）は、電子メールにおける送信ドメイン認証技術*1の一つであり、RFC7489で標準化されている。
- DMARCは、「認証（IPアドレス（SPF*2）や電子署名（DKIM*3）を使って**なりすましメールかどうかを認証する技術**）」と「分析（**集計レポートする技術**）」の2つの機能を活用し、「正しいメールを届けて、なりすましメールを削除する」ことを実現するものである。 一方で、**ポリシー設定等を誤る**とメールを受信できなくなるといった**懸念**もある。



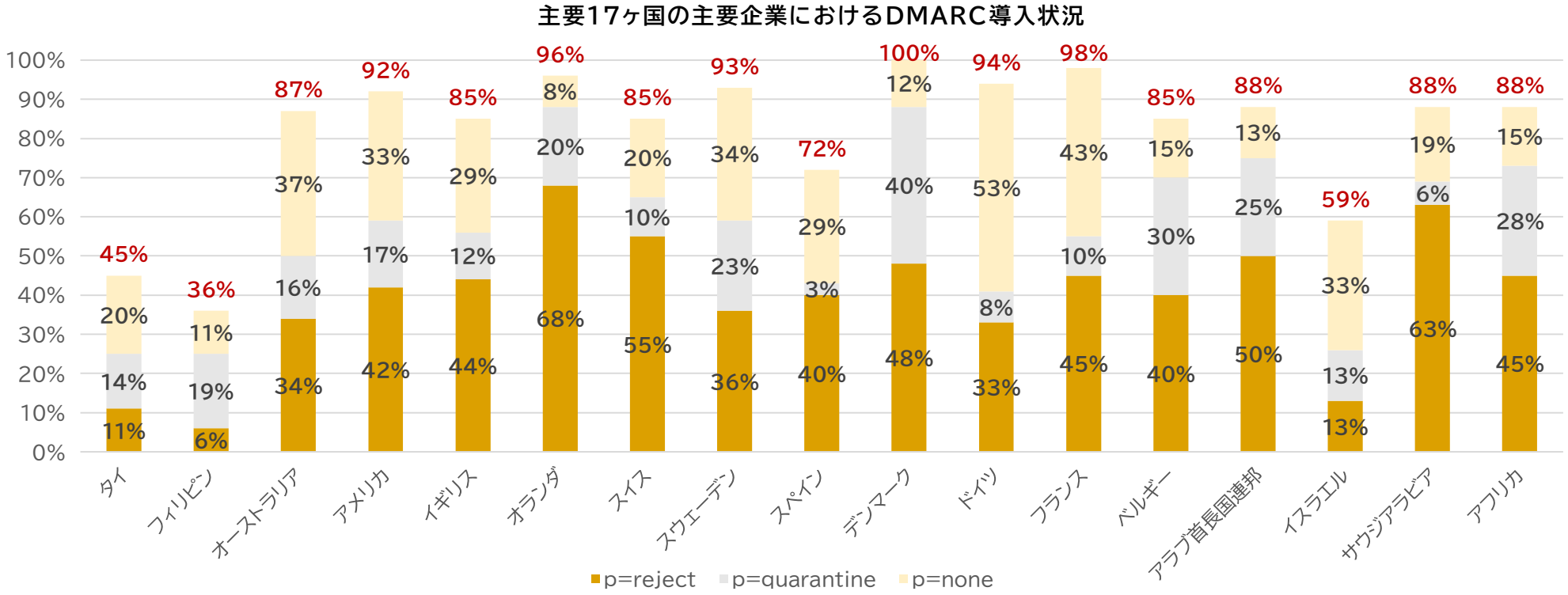
DMARC導入に関する法的な留意点　https://www.soumu.go.jp/main_content/000495390.pdf

本事業における「DMARC体験コース」コースマテリアル資料より

*1　送信ドメイン認証技術とは、SPF、DKIM、DMARCの総称で、受信したメールが正規の送信元から送られてきたかを検証できる技術
*2　SPF（Sender Policy Framework）は、電子メールの送受信において送信者のドメインの偽称を防ぎ、正当性を検証する仕組み
*3　DKIM（DomainKeys Identified Mail）は、電子メールプロバイダが認証できる方法で、組織が署名することによりメッセージ送信に責任を持つことを可能にするプロトコル

DMARCの普及状況【海外】

- 日本以外の主要17ヶ国の主要企業におけるDMARC導入状況は、2024年1月22日のプルーフポイントの調査によると、デンマークがOMXC25企業のうち100%とトップで、次いでフランスがCAC40企業のうち98%となっており、オランダはAEX企業のうち96%、ドイツはDAX40企業のうち93%、アメリカはFortune1000企業のうち92%がDMARCを導入している。

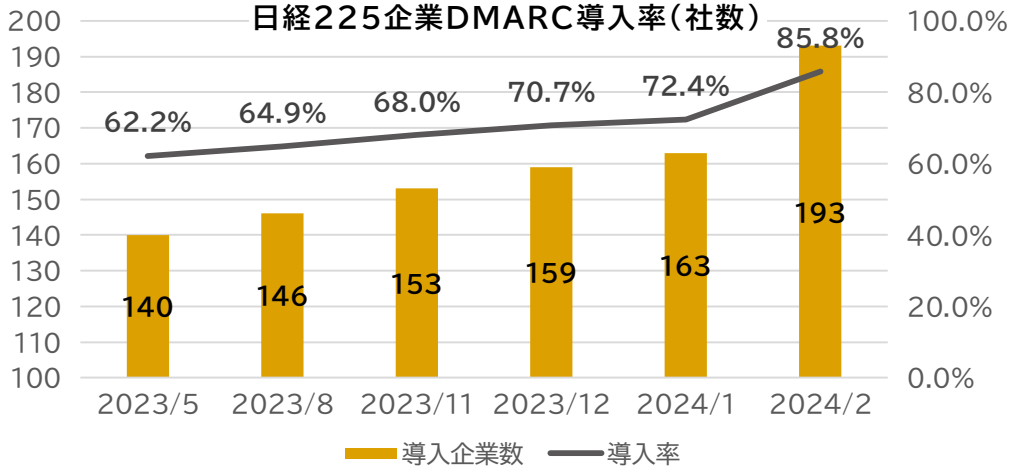


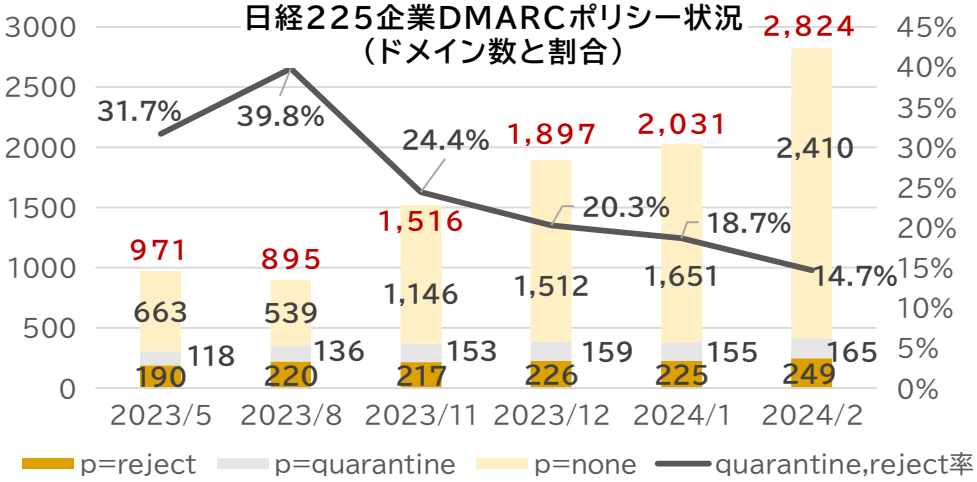
プルーフポイントの調査（2024年1月22日）を基に三菱総合研究所にて集計・作成
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/Global-DMARC-Adoption-Rate-Survey-2023

- 最も導入の進んでいないフィリピンであっても実効性のあるポリシー（拒絶（reject）と隔離（quarantine）の計）が25%となっている。

DMARCの普及状況【国内】

- 国内のDMARC導入状況については、令和5年2月の総務省・警察庁・経済産業省による要請[*1]の後、金融機関を中心にDMARC導入が進んだものの、国外に比べて低い数値を示していたが、令和6年2月よりGoogleがGmailのメール送信者ガイドラインを強化[*2]する旨を令和5年10月に発表したことに伴い導入が加速した。
- 下図（左）に示す通り、日経225企業におけるDMARCの導入率は、令和5年5月時点で140社（62.2%）だったが、令和6年2月には193社（85.8%）まで増加した。





株式会社TwoFiveの調査（2024年2月9日）を基に三菱総合研究所にて集計・作成 https://www.twofive25.com/news/20240209_dmarc_report.html

- 上図（右）に示す通り、ドメイン名ごとのDMARCポリシーを確認すると実効性のあるポリシー（拒絶（reject）と隔離（quarantine）の計）の割合は14.7%にとどまり、前述のGoogleのガイドライン強化を前に急遽対応した事業者が多く、今後ポリシーの強化が課題であると言える。
- DMARC関連技術であるSPF、DKIMについては、SPF普及率96.7%、DKIM普及率73.8%[*3]となっている。

*1 総務省 警察庁 経済産業省 クレジットカード会社等に対するフィッシング対策強化の要請 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000184.html
*2 Googleメール送信者のガイドライン https://support.google.com/a/answer/81126?sjid=4068263634946002854-AP&visit_id=638445419916825732-443438357&rd=1
*3 総務省 電気通信消費者情報コーナー ＞ 迷惑メール対策 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

3. 技術的課題の調査

- 技術調査の内容
  - RPKI
  - DNSSEC
  - DMARC
- 実証実験の規模
- 実証実験の環境

- 実証実験の結果
  - RPKI
  - DNSSEC
  - DMARC

RPKI技術調査の内容

- 令和4年度から引き続き、大学等の学術研究機関と連携し、対策技術の調査を行う技術ラボを設置・運営した。技術ラボでは、実証を通じ提起された技術課題を調査・解明するとともに、認証技術等ごとに調査を実施した。

No	調査機関	調査項目	調査結果
1	慶應義塾大学	① 国内のインターネットトポロジーにおいて不正な経路への対策を取るためのROAキャッシュサーバの展開に関する調査	ROV導入済みASに存在するInvalid経路を分析しRIRのRPKIインフラ故障により、ValidからNot foundではなく、Invalidになる現象が初めて観測された。ROAにInvalidを管理出来るかがROAの設置の可否を決める課題について考察を行った。
		② 不正な経路への対策の前提となるROAの普及に向けたデータ分析と導入施策の調査検討	ROVの導入率が低い原因に対する調査、ROVによりInvalidと判断された経路の実態と原因の解明を行った。ROA の正確な設定の重要性を確認し、Max Lengthの設定ミスが多いことを突き止めROAはそのような管理が出来る場所である必要を再確認した。
		③ RPKI Invalid 経路及びBGP 異常との関連性に関する調査	調査全体を通して、インターネットの独立性を鑑み上流のROVに頼らず下流でのROVの必要性とROAの設定及びROAセキュリティの重要性を再確認し十分な能力を持ってROAを運用すべきと提言。
2	長崎県立大学	④ ROAキャッシュサーバの実装比較に関する調査	ROAキャッシュサーバーの機能のValidatorとRPKI-RTRをソフトウエアごとに調査し各機能を比較。現時点での最良の組み合わせを導いた。また、インストール手順等を整理し公開可能な形とした。
		⑤ ROAキャッシュサーバの運用に必要なROAなどを解析できる汎用ツールの必要要件に関する調査	現状のValidatorの調査では、監視機能が不足しているため監視ツールを設計し運用者の助けとなるサンプルプログラムを作成した。
3	大阪大学	⑥ BGPセキュリティに関わるソフトウェア実績の調査	BGPのセキュリティにおいてROVによるオリジン検証のみならず、ASPAによるASパス検証はBGPの経路検証にとって今後必要になる技術と考えられるためASPAの運用にに対する課題点を実証した。

DNSSEC技術調査の内容

- 令和4年度の技術調査において、「日本におけるDNSSEC情報ポータルサイトの構築」の必要性が論じられる中、「DNS応答の正確性の検証」や「最悪のシナリオに基づいた攻撃への対策」の強化の検討が必要であるとの認識から今年度の調査内容として以下①、②を設定した。
- また、実証事業参加者以外の実態調査を目的として、以下③の調査内容とした。

No	調査機関	調査項目	調査結果
1	東京大学	①より多くの拠点における DNS応答の正確性の検証	調査期間中、リゾルバDNSサーバーにおいて明確な不正応答は確認できなかったが、年に数回のみの応答となる権威DNSサーバーの場合、注意が必要である。
2		②最悪のシナリオに基づいた 攻撃エミュレーション	受信側メールサーバに対してDNS詐称を行うことにより、本来は正式な送信者ではない攻撃者からのメールがMTA(※)で不正に認証され、SPFおよびDKIMが正しく検証されたことを示すヘッダが付加されることを確認できた。
3	GMOインターネットグループ社	③DNSSECの導入状況に 関するアンケート調査	導入3%、未導入97%という結果が判明した。未導入者は知識不足を理由としており、DNSSECの概要説明後の導入意欲変化は些少(22%)ではあるが向上した。

※MTA: Mail Transfer Agentの略でメールの配送・転送を担うソフトウェア

DMARC技術調査の内容

- 令和4年度の技術的課題の調査において、実証事業者から最も懸念された課題として挙がった「偽陽性の問題」に関する調査と、令和4年度の技術調査において、項目及び必要となる機能等を調査した「チェックサイトの構築」について具体的な開発・構築に向けた調査検討を行うこととした。
- また、DNSSEC同様、GMO-IG社による導入状況に関するアンケート調査を行った。

No	調査機関	調査項目	調査結果
1	TwoFive社（JPAAWG）	①偽陽性の問題（転送・メーリングリスト等）に関する調査	偽陽性が発生する要因のひとつであるメーリングリストの影響範囲とその回避方法を調査し、代表的なソフト・サービスにおける対応状況を調査した。
2		②チェックサイトの構築に向けた調査	チェックサイトの仕様として必要な機能を調査し、課題・懸念点を解決案とともに調査した。
3	GMOインターネットグループ社	③DMARCの導入状況に関するアンケート調査	導入18%、未導入82%という結果が判明した。未導入者は知識不足を理由としており、導入者の71.4%がrejectまたはquarantineにDMARCポリシーを強化していることが判明した。

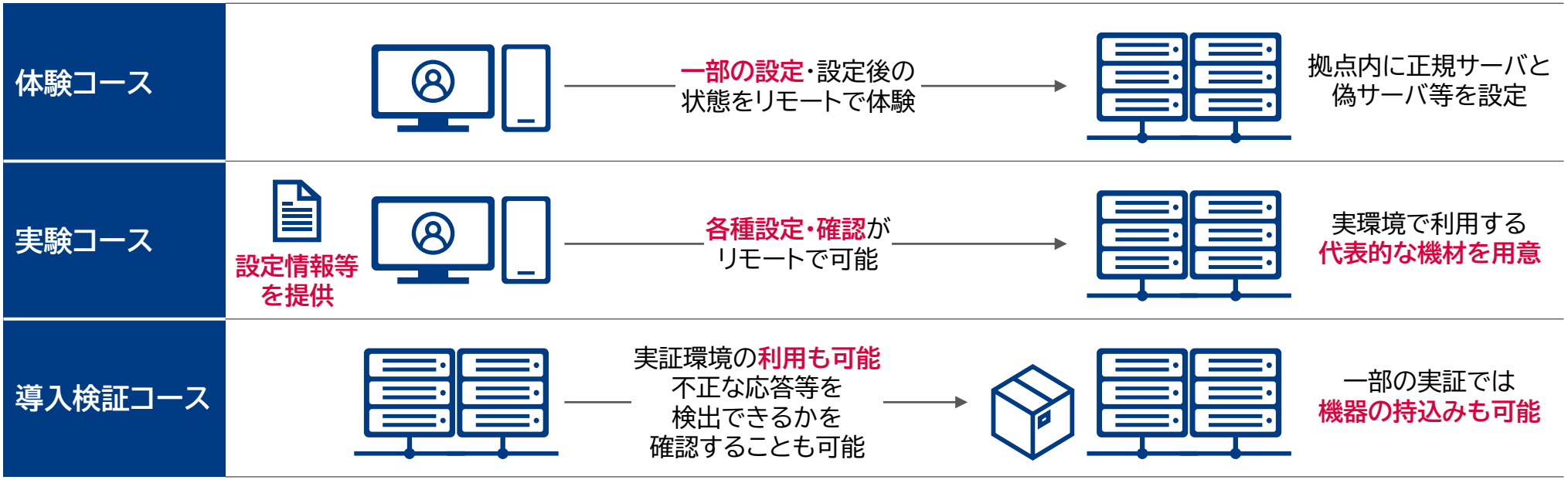
実証実験の規模

- 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

実証実験の環境

- 各実証コースの利用を想定し、実証環境を整備した。
- RPKIの仮想環境では、ネットワーク通信機材の持込みによる検証を想定し、3大学の協力の基、**慶応大学（SFC：神奈川）**、**大阪大学**、**長崎県立大学**に設置。また、検証用及び実態を体験するためフルルートを流す環境を用意。
- DNSSECの仮想環境では、正しく検証できていることを確認するために、実際に**不正なDNS応答を流せる環境**を用意。
- DMARCの仮想環境では、送信したメールのレポートの確認、受信したメールの**レポート結果等が確認できる環境**を用意。



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。

実証実験の結果　今後の課題

①RPKI

監視方法とROA運用の是非

- **監視方法の知見習得が課題**
  - -SNMPやBGPAlerterでの監視方法の知識習得が進まず、課題を残す結果となった。
- **ROAキャッシュサーバ―の運用是非**
  - -ROAキャッシュサーバ―の自社運用の是非について、IX等が提供するものを利用したい、とする意見も多く、導入検討に至っていない事業者が多い。

②DNSSEC

自動化した部分の監視方法

- **監視項目・監視方法が見えていない**
  - -KnotDNS等により自動化したことで導入障壁は下がった一方、運用上、何をどの程度監視すれば良いか、理解が進んでいない。

③DMARC

DMARCレポートの分析方法とDMARCポリシー強化の指針

- **DMARCレポートの分析方法に課題**
  - -DMARCレポートの分析ツールはコストがかかる。また、分析ノウハウがないため、外部のコンサルサービスを使用したいが、そのコストも問題である。
- **DMARCポリシー強化の指針が不明確**
  - -どうすればDMARCポリシーを強化して良いのか、その判断がつかない。

4. ガイドライン案の策定

- ガイドライン案の方向性
- ガイドライン案　目的
- ガイドライン案の対象読者
- ガイドライン案　骨子案（目次）
- ガイドライン案　特徴

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

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とライフサイクル
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 ドメイン名登録者への注意	1.2	ドメイン名の重要性
3	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

	はじめに
第1章	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)
2.1	送信側の送信ドメイン認証設定
2.2	DMARC の組織ドメイン名への設定
2.3	メールに利用しないドメイン名への設定
2.4	DMARC レポートの活用とポリシーの強化
第3章	メール配送事業者
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
第5章	メール受信者
5.1	送信ドメイン認証
5.2	認証ドメイン名の評価
5.3	フィードバック
5.4	メール受信者にわかりやすい認証結果の提示
第6章	付録

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ト　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ト　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ト　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

5. 外部公開・民間認定の検討

- 公開情報調査
- ヒアリング調査
- 実現に係る課題
- 民間認定に求める発言分布
- 利用者が公開情報を基に導入・市場で評価される仕組み

外部公開・民間認定 公開情報調査 1／3

国		ドイツ	オランダ	日本
名称		ITセキュリティラベル	Internet.nl	権威DNSサービス仕様調査
所管		The Federal Office for Information Security（BSI）	オランダ政府、業界団体、インターネットソサエティが主催するイニシアチ	日本DNSオペレーターズグループ（DNSOPS.JP）
概要		DNSSECを対象としており、技術ガイドライン「安全な電子メール転送」（BSI TR-03108）に基づいて安全な電子メール通信の比較可能性と普及を高めることが目的	電子メールプロバイダーが提供しているWebサイトで、IPv6やDNSSEC、TLS、DKIM、DMARC、SPFなどの最新のインターネット標準を使用しているかどうかをユーザーが確認可能	権威 DNS サービスについて継続した実情調査と、サービス提供の背景を知るためのサービス提供事業者の状況を把握することを目的として調査を実施 DNSSECの対応の有無などを公表
評価	評価する基準	BSI TR-03108の「安全な電子メール転送」	各セキュリティごとに仕様が定められている	DNSSECへの対応
	基準の公開	公開	仕様の内容が公開	公開されていない
	基準の確認方法	ホームページにより確認可能	ホームページにより確認可能	不可能
公表	公表単位	企業/サービス	ドメイン名	企業/サービス
	公表項目・内容	同上	ウェブサイトまたはメールのスコアがInternet.nl で 100% の場合、コミュニケーションで対応する100%バッジを使用することが許可	DNSSECへの対応の有無を完全性の項目で公表
	公表取消し	明示されていないが、公表取消しは有り得るものと思料	100%を維持できなくなった場合、公表は取り消され、バッジの使用は許可されなくなる	調査結果であるため取消しは想定されていない
	クレーム受付	E-mailにて受付	E-mailにて受付	調査結果のフィードバックを受付

外部公開・民間認定 公開情報調査　2／3

名称	プライバシーマーク（JIS Q 15001）	ISMS適合性評価制度（ISO/IEC 27001）	CC（ISO/IEC15408）	安全・安心マーク	TRUSTe（トラストイー）
概要	日本工業規格“JIS Q 15001個人情報保護マネジメントシステム-要求事項”に適合し、優れた個人情報保護の体制を取っていることを認証する制度	組織の情報セキュリティ管理に関する仕組みを、第三者（認証機関）が評価し、認証する制度	政府機関の導入の際に、認証された製品が高いセキュリティ標準を満たしていることを確保するもので、世界中の30ヵ国以上で導入	一般利用者が事業者を新たに選択する際、ユーザ対策やセキュリティ対策などが、一定基準以上であるという目安を提供するもの	インターネットに限定された個人情報保護認証制度。企業における暗号化対策、またはプライバシーポリシーの作成と公表などが正しく実施されているかどうかを審査、認証マークを取得可能
審査期間	約1.5か月	最低で3～4か月	3か月～	不明 （二次）審査は年3回	2～3か月
認証書・マーク					
認証機関	一般財団法人日本情報経済社会推進協会（JIPDEC）	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）	独立行政法人情報処理推進機構（IPA）	インターネット接続サービス安全・安心マーク推進協議会	一般社団法人日本プライバシー認証機構（JPAC）
評価機関	プライバシーマーク制度委員会の審議を経て審査機関として指定を受けた機関	ISMS-ACによって認証を受けた機関	IPAによって認定を受けた機関	ー	ー
更新/継続	有（2年間毎）	有（3年毎） 再認証審査がない期間は毎年サーベイランス審査有	有（3年ないし2年毎）	有（1年間毎）	有（1年間毎）

外部公開・民間認定 公開情報調査 3／3

国		日本	日本	日本
名称		安全・安心マーク	送信ドメイン認証実施状況	JPドメイン名の種別ごとにおける送信ドメイン認証技術の設定状況
所管		インターネット接続サービス安全・安心マーク推進協議会	一般社団法人日本データ通信協会	総務省
概要		一般利用者が事業者を新たに選択する際、ユーザ対策やセキュリティ対策などが、一定基準以上であるという目安を提供するもの。	各プロバイダ（ISP）、CATV（ケーブルテレビ）、モバイル事業者、フリーメール事業者における送信ドメイン認証の実施状況について整理したもの。 対象にDMARCが含まれる。	「jp」のドメイン名における送信ドメイン認証技術の設定状況の調査に基づく結果を公表したもの。 対象にDMARCが含まれる。
評価	評価する基準	審査点に「必須」がついている項目は、その要件を満たす必要がある。点数は、その要件を満たしている場合に与えられる推奨点数。 必須29項目、推奨119点中92点以上を獲得することでマークの使用許諾申請に合格	特になし 調査に対する回答によるのみ	特になし
	基準の公開	公開	ー	ー
	基準の確認方法	ホームページにより確認可能	ー	ー
公表	公表単位	企業/サービス	企業/サービス	JPドメイン名の種別ごとに集計した数のみ
	公表項目・内容	同上	個人向けに提供しているメールサービスの名称（インターネット接続サービスに含まれる場合は、接続サービスの名称）を表示 導入している場合には「○」、導入していない場合には「－」と表示。なお、SPFについては、SPFを導入し、かつ、ディレクティブが「 -all 」の場合には「◎」と表示	ー
	公表取消し	所定の事項に該当した場合にマークの使用許諾が取消し	取消しは想定されていない	ー
	クレーム受付	問い合わせ先を明記していない	Webフォームでの問い合わせを受付	集計数を公表しているのみであり、クレーム受付は想定されていない

外部公開・民間認定 ヒアリング調査

ヒアリング項目	日本データ通信協会	安全・安心マーク（JAIPA）
審査・公表に対する課題	■ 審査は特段やっていない認識 ■ 公開に関する課題としては、性善説で調べているため未回答であった場合、個人メールの事業を本当にやっていないかどうかは完全にはわからない	■ 公表には課題はない ■ 審査には課題がある。業界側の知識が追い付かなくなっており、評価が悪いものが出た時にどのように直すのかを理解できていない ■ 地方ではセキュリティ事案が発生しているが、気づいていない場合がある。地域のセキュリティリテラシーを上げる施策が必要
確認・公表を実施する内容・意図	■ 想定利用者は広く日本国民であろうと認識	■ 安全・安心マークの設立の背景や経験を踏まえると、DNSSECやDMARCのリストの追加や公開は実施すべき
DNSSECやDMARCについて、導入組織(ISP事業者等)のリスト作成や公開についてどのように感じるか	■ 国民の利益になるため、必要	■ DMARCとDNSSECの導入を進めるため、安全・安心マークを拡充することで対応する必要がある ■ 一方で、導入にはついては何らかの支援が必要

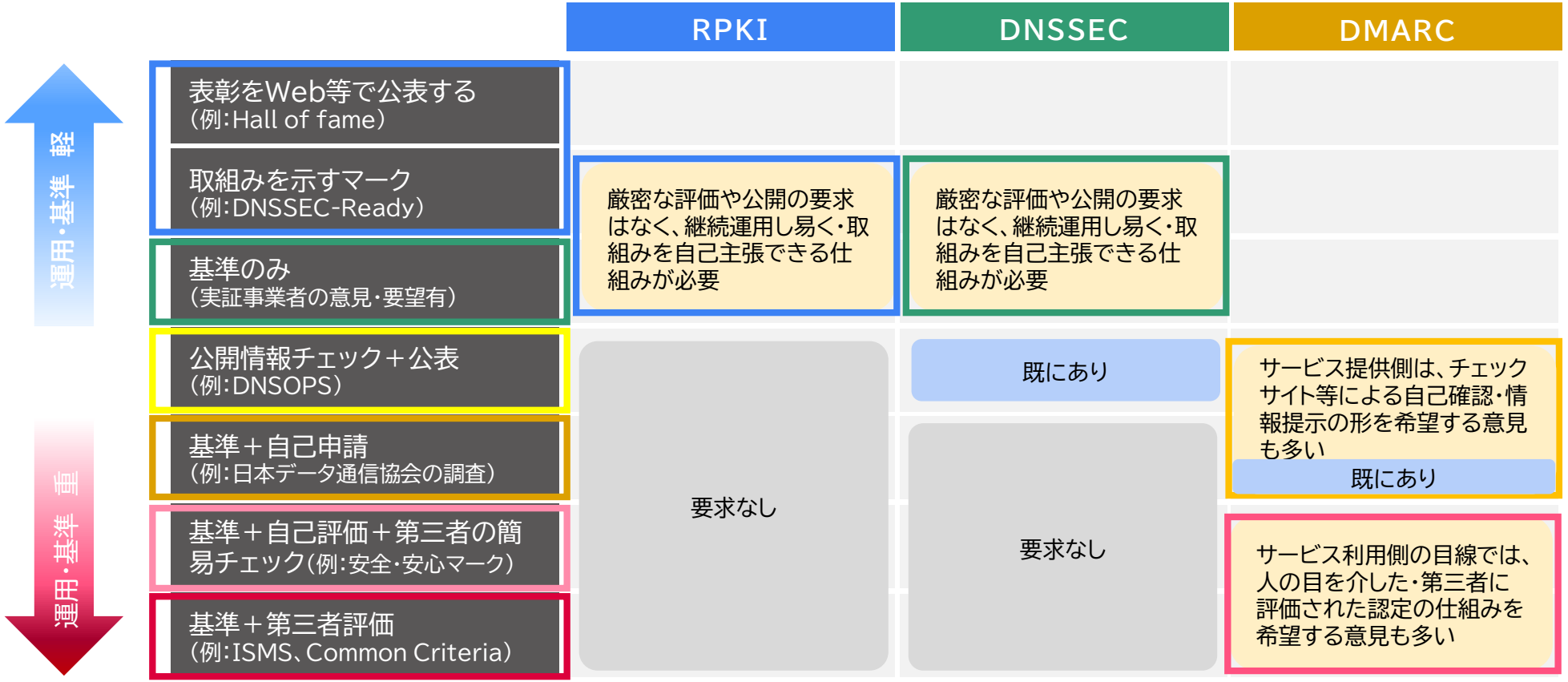
外部公開・民間認定 実現に係る課題

- 以下に、公開文献及びヒアリング調査を検討した実現に係る課題を示す

	導入状況の外部公開	民間認定等の仕組み
運用面	• 仕組みの主体/中立性が求められる • 仕組みを適切に運営していることを確認・監査することが求められる（政府の関与） • 一度、実施すると廃止することができない • 自己申請の結果を集約する場合、虚偽があってもわからない	
コスト面	• 公開データ・評価結果を定期的に確認・更新するためコスト • 公開方法・評価方法を定期的に更新するためコスト • 評価結果がよくない場合の修正方法を教えるコスト • 評価する範囲（レベル）によるコスト	
技術面	• 対象となる技術（DNSSECやDMARC）のアップデートに対応 • 評価する範囲（レベル）に対して確認する技術力 • 評価結果がよくない場合の修正方法を教える技術力が求められる	

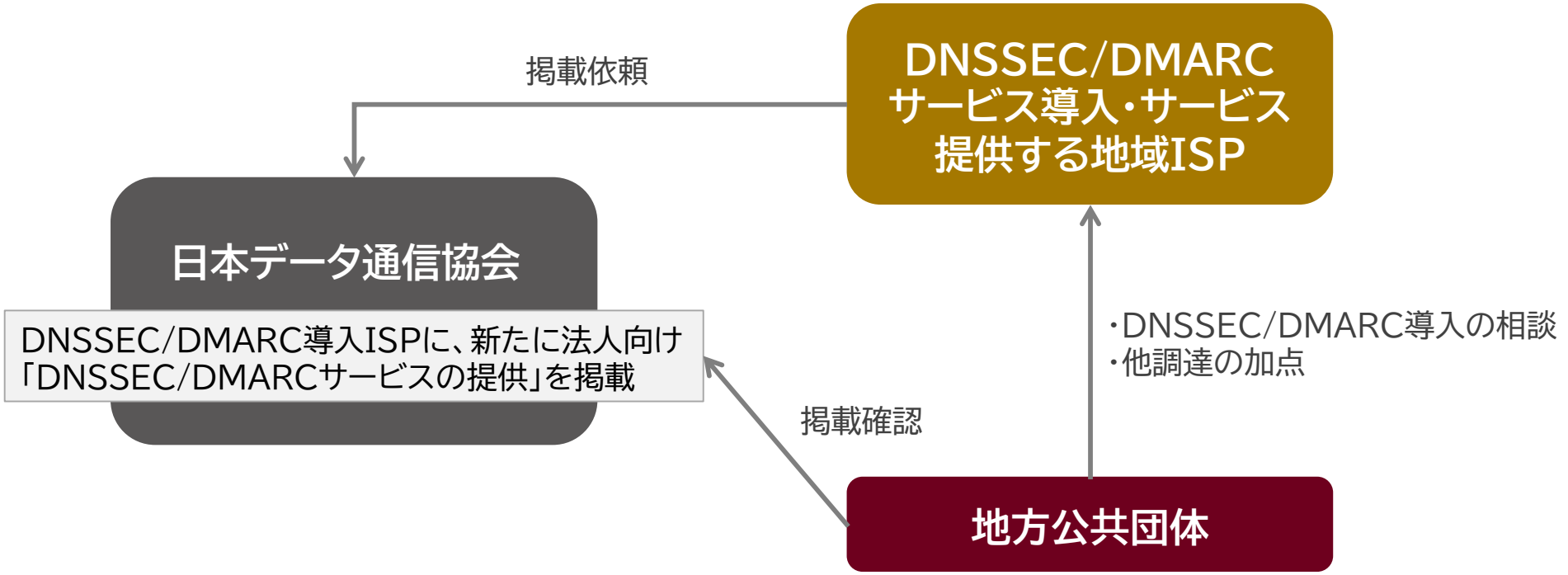
民間認定に求める発言分布

- 民間認定のパターン分析について、各認証技術等の第三回有識者検討会および情報交換会において出席した有識者ならびに実証事業者等より意見を聴取した結果、以下のような分布となった。



利用者が公開情報を基に導入・市場で評価される仕組み

- DNSSEC/DMARCを導入している地域ISPのセキュリティサービスはどこかについて、日本データ通信協会がリストを作成・公開し、地方公共団体（利用者）が確認して導入する仕組みを構築するのはどうか



根拠・動機付け
地方公共団体における 情報セキュリティポリシーに関するガイドライン（令和5年3月版）

6. アウトバウンド活動の報告

- アウトバウンド活動の実績

アウトバウンド活動の実績

- 認証技術等の普及促進に向け、ISP等通信に関わる事業者やネットワークセキュリティ関連の関係者が多く集まるイベント等において、本事業の広報を目的としたアウトバウンド活動を実施し、ガイドライン案や外部公開・民間認定の仕組み検討における意見を収集した。

No	名称	開催日	開催地	説明技術	参加人数
1	JPNIC総会	令和5年6月12日	飯田橋	RPKI DNASSEC DMARC	現地　70名＋オンライン（OL）82名 計152名
2	DNS Summer Day 2023	令和5年6月23日	オンライン/秋葉原	DNSSEC	現地 64名＋OL 229名 計293名
3	JANOG52 Nagasaki	令和5年 7月5日～7日	オンライン/長崎	RPKI	OL 不明 現地 約250-270名
4	第56回 CATVラボワークショップ	令和5年9月19日	オンライン	RPKI DNASSEC DMARC	73社150名
5	JANOG52.5	令和5年10月13日	オンライン	RPKI	OL 152名
6	JPAAWG 6th General Meeting	令和5年 11月6日～7日	オンライン/金沢	DMARC	OL 不明 現地 70名
7	Internet Week 2023	令和5年 11月15日～17日※1 11月20日～22日※2	オンライン/本郷	RPKI DNASSEC DMARC	OL 160人 ※1にて実施
8	JANOG53 in Hakata	令和6年 1月17日～19日	博多/アーカイブ配信	RPKI DNASSEC DMARC	現地 約200名

※1：オンラインWeek、※2：カンファレンスWeek

7. 実証事業の成果と今後の課題

- 実証事業の成果
- 今後の課題

実証事業の成果

- **3技術それぞれのガイドライン案を作成**
  - 技術ごとに、**実証事業者による**実証実験の結果を受けた**意見を収集**し、有識者検討会等で参加メンバーによるディスカッションを経て、**ガイドライン案を作成**できた。
  - ガイドラインは、導入メリットや導入しない場合のレピュテーションリスク等を**経営者に向けて記載**しつつ、技術者に対しては、**対象者別に章立てを構成**し、具体的な事例やトラブルシュートを含め、記載した。
- **実証実験を通じた3技術導入のための知見の提供と約80%の方から前向きな導入意識を醸成**
  - RPKI：令和4年12社、令和5年18社、DNSSEC：令和4年10社、令和5年8社、DMARC：令和4年10社、令和5年10社と、技術の導入・運用に課題を持っている多くの実証事業者に実証実験に参加いただくことで、**技術の普及促進を図る**とともに、実証事業者における導入・運用に関する**技術的知見の習得の機会を提供**し、**ガイドライン案へ記載すべき課題や知見を収集**した。
  - 3技術の導入・普及促進を図るため、基本的な内容を学習する体験コースを3技術×3回開催し、RPKI：62名（29組織）、DNSSEC：34名（19組織）、DMARC：98名（25組織以上）に参加いただくことで、**技術に関する基礎知識の習得に寄与**したほか、約80%の方々における**技術導入に向けた前向きな意識を醸成**することができたとともに、解消できなかった**課題は今後のカリキュラム・教材の改善**ポイントとする。
- **3技術の導入及び普及促進を図った多数のアウトバウンド活動を実施**
  - ISPを含むネットワークセキュリティ関連のイベント等において、本事業のアウトバウンド活動を実施。
  - 令和5年6月～令和6年1月までに、8件のアウトバウンド活動を実施したことで、**本事業の内容のアウトリーチが叶った**ほか、**ガイドライン案や外部公開・民間認定の仕組み検討における意見が収集**できた。

今後の課題

- **ガイドラインは継続的なメンテナンスが重要**
  - 技術の進歩等にあわせた技術情報のアップデート等、**継続的なメンテナンスが重要**であるとの意見が多数を占めた。
  - 中立性、継続性、専門性、妥当性・客観性、協調性、公平性の観点を考慮し、**技術ごとにメンテナンスを視野に入れた運用体制**（専門機関等に委託する等）の構築が必要である。

- **外部公開・民間認定は制度設計が重要である**
  - 技術導入状況を外部に公開する場合のメリット/デメリットを整理し、認定制度を作成するうえで、運営体制や認定項目の設定等の**軽重バランスが重要**である。

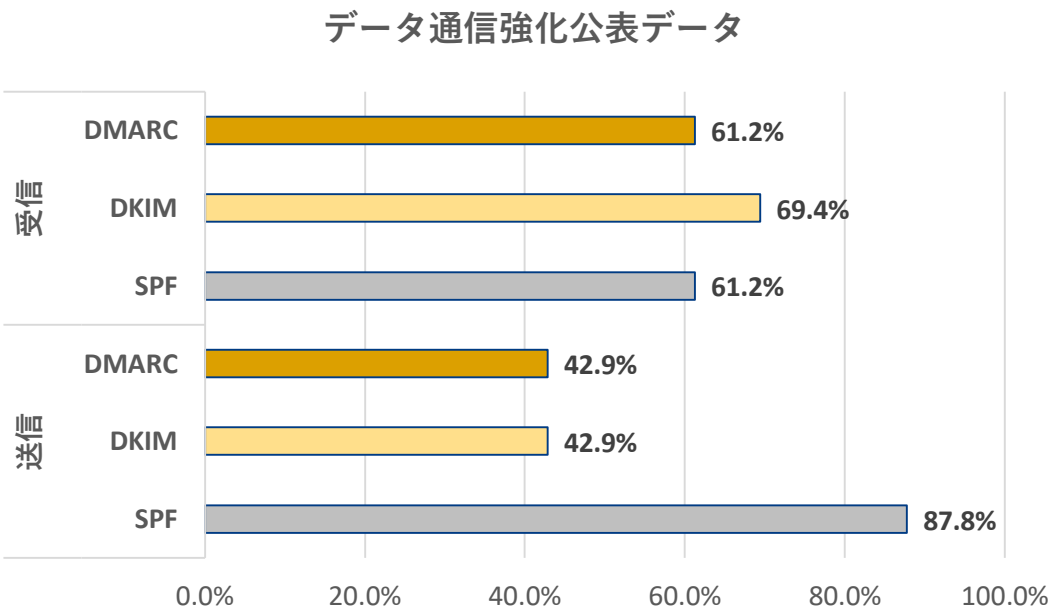
- **体験コースは継続してほしいとの意見が多い**
  - 対象者別のコース（基礎編、応用編等）を設定する等し、今後も技術の**普及啓発活動は継続してほしい**という意見が参加者からあった。
  - 一部検証項目（DNSSECの監視方法等）において、解決に至る過程で自信を持てない事業者もあったことから、**カリキュラムや教材の見直し**を行うことにより、各技術のより良い普及啓発の礎としていく必要がある。

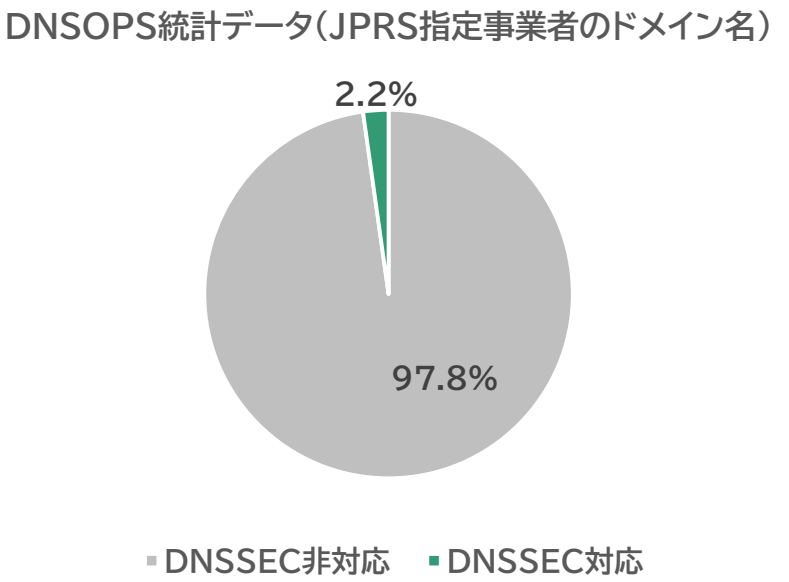
補足. 未導入組織に関する追加調査

- 補足1. 迷惑メール相談センター・ DNSOPSの公表データ
- 補足2. GMOインターネットグループのアンケート調査結果概要
- 補足3. 実証不参加の事業者に関する導入の阻害要因

補足1. 迷惑メール相談センター・ DNSOPSの公表データ

- 迷惑メール相談センターでは、ISPなどの送信ドメイン認証実施状況を公表している。送信側のSPF は87.8%と高いが、DMARCは送信側42.9%、受信側61.2%と、日経225企業が送信側70.7%であることから低い傾向である。(左図)
- DNSOPSは、DNSSEC導入状況委関する統計データを公表している。このデータには、ISPを集約したものがないため、参考として、JPRS指定事業者のドメイン名の抜粋し、集計した結果を示す。DNSSEC対応は、2.2%と低い結果である。(右図)

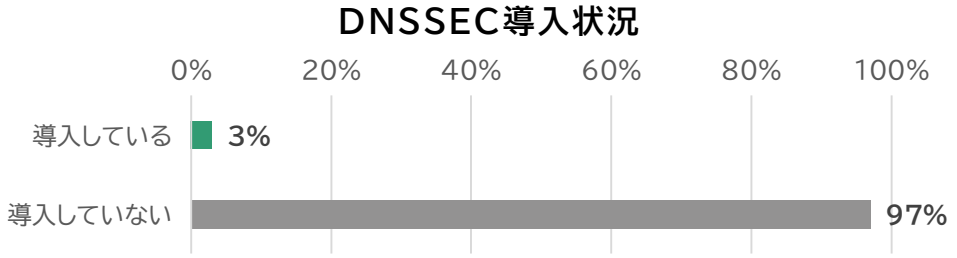


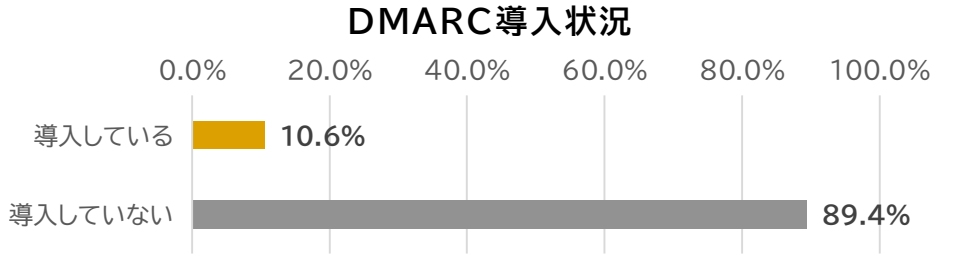


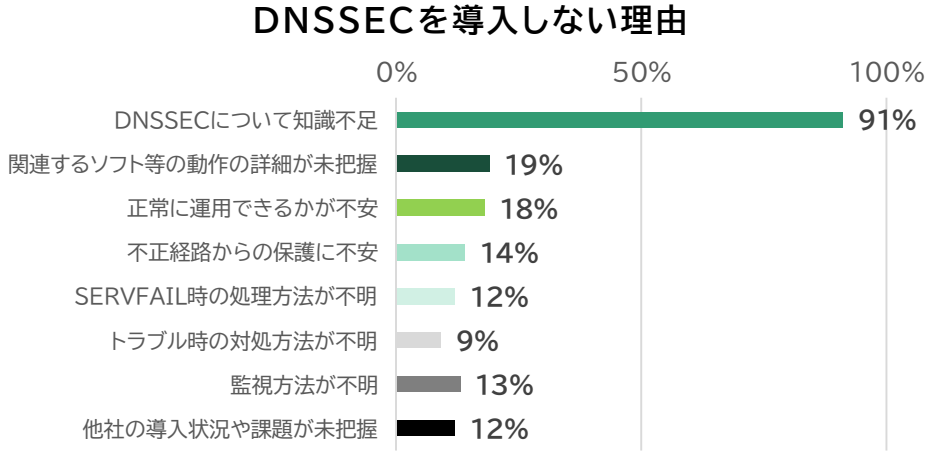
送信ドメイン認証実施状況 ｜｜ 迷惑メール相談センター https://www.dekyo.or.jp/soudan/contents/auth/index.html (2023年12月31日時点)
DNSOPS JPRS指定事業者のドメイン名 https://stats.dnsops.jp/view/jp-registrar (2024年1月31日確認)

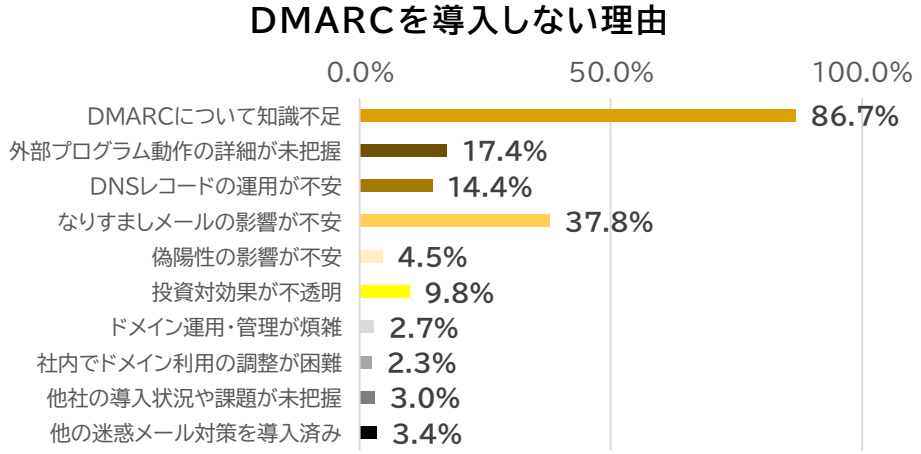
補足2. GMOインターネットグループのアンケート調査結果概要

- 2024年2月にGMO社によるDNSSECおよびDMARCの利用に関するアンケート調査を実施した。
- DNSSECの導入状況は、「導入している」との回答が3%であり、導入しない理由については、「DNSSECについての知識不足」との回答が91%を占め、技術情報の到達性を検討する必要がある。
- DMARCの導入状況は、「導入している」との回答が10.6%にとどまり、昨今のDMARC導入機運の高まりからすると低い数値となった。導入しない理由については、DNSSECと同様、知識不足を挙げる回答者が86.7%と多く、「なりすましメールの影響（なりすましメールを防げるか）が不安」にも37.8%と他の選択肢より多い回答があった。









補足3. 実証不参加の事業者に関する導入の阻害要因

(a) 関連事業課有&顧客提供有	例）DNSSEC関連事業を実施し、DNSSECを顧客に提供している/提供可能
(b) 関連事業課有&顧客提供無	例）DNSSEC関連事業を実施し、DNSSECを顧客に提供していない
(c) 関連事業課無	例）RPKI関連事業がない又はDMARCを外部事業者に依頼している

（a）関連事業有&顧客提供サービス有

1. **PKI技術が難しい:**
   - RPKI、DNSSEC等は特に、PKI（Public Key Infrastructure）技術を基にしており、特に鍵管理や鍵の更新等については、複雑であるため、一部の事業者は技術的な課題に感じている。技術的なハードルが高い場合、導入が進まない可能性がある。
2. **動いているので手を入れたくない:**
   - 3技術技術に関連したシステムが現在も安定して動作している場合、事業者はそのまま維持しようとし、新たなセキュリティ対策の導入に二の足を踏むことがある。既存の状態が維持可能であるとの認識から、新たな変更への抵抗が生じることがある。
3. **導入すると動かなくなる可能性がある:**
   - 3技術の導入にはネットワークの構成変更が伴うことがあり、これがサービスの中断や問題を引き起こす可能性がある。このため、事業者は導入に伴うリスクを恐れ、慎重になることがある。
4. **導入後に対処ができない:**
   - 3技術の導入に必要な資源や専門知識（不具合や不明な挙動への対処）が不足している場合、事業者はこれを補う手段を見つけることが難しく、導入が進まない可能性がある。

（b）関連事業有&顧客提供サービス無

1. **顧客向けのサービス提供していない事業者は優先度が下がる:**
   - 顧客との直接的な関係がない事業者は、セキュリティ対策に対する事業要求が低くなりがちである。顧客への直接的な影響がないため、対策の優先度が低くなりがちである。

（c）関連事業無

1. **顧客向けのサービス提供していない事業者よりもさらに優先度が下がる:**
   - 顧客提供せず、自社の事業としてもとの直接的な関係がない事業者は、セキュリティ対策に対する事業要求が低くなりがちである。顧客への直接的な影響がないため、対策の優先度が低くなりがちである。

(d)その他 （共通）

1. **切迫感がない:**
   - RPKI、DNSSECの導入は、DMARCの導入比べ、セキュリティインシデントや攻撃のリスクに対する意識が欠如していることや、顧客問合せや話題になっていないことも含め、事業者は切迫感を感じず、対策を先送りする可能性がある。

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3. 各認証技術体験コースの結果
- 参考4. 各認証技術実証コースの結果
- 参考5. 各認証技術ガイドライン案の概要

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

❶ 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

❷ 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

❸ 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	末政 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

❶ 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ーブ
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	ビッグローブ株式会社
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）

❷ 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ーブ
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

❸ 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ーブ
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

❶ 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

❷ 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

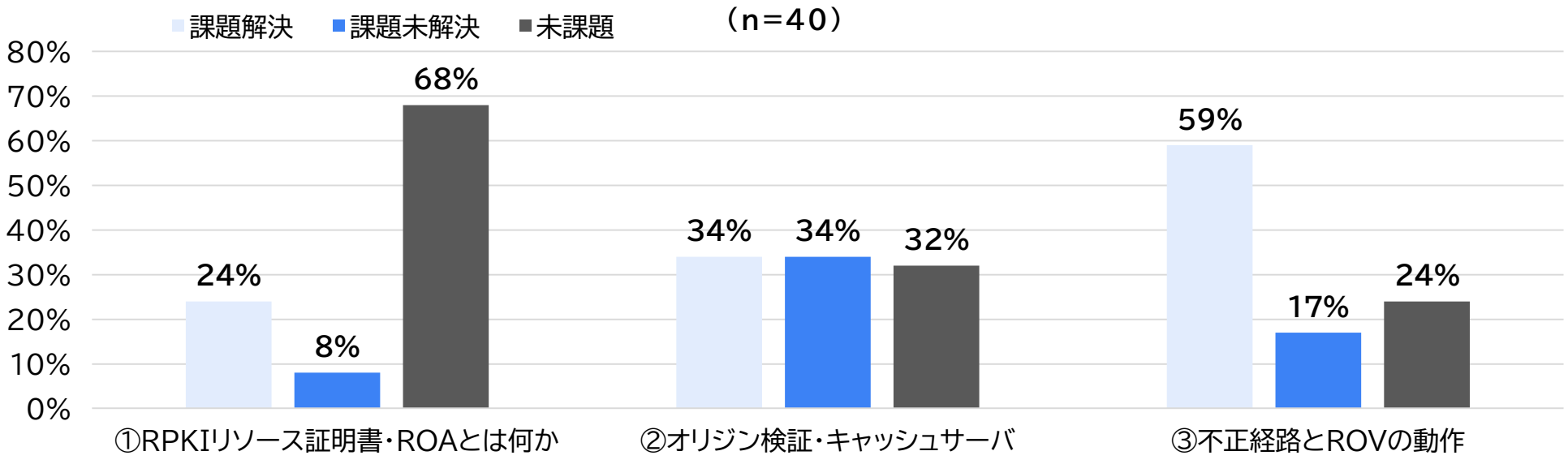
❸ DMARC｜体験コースコースマテリアル一覧

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

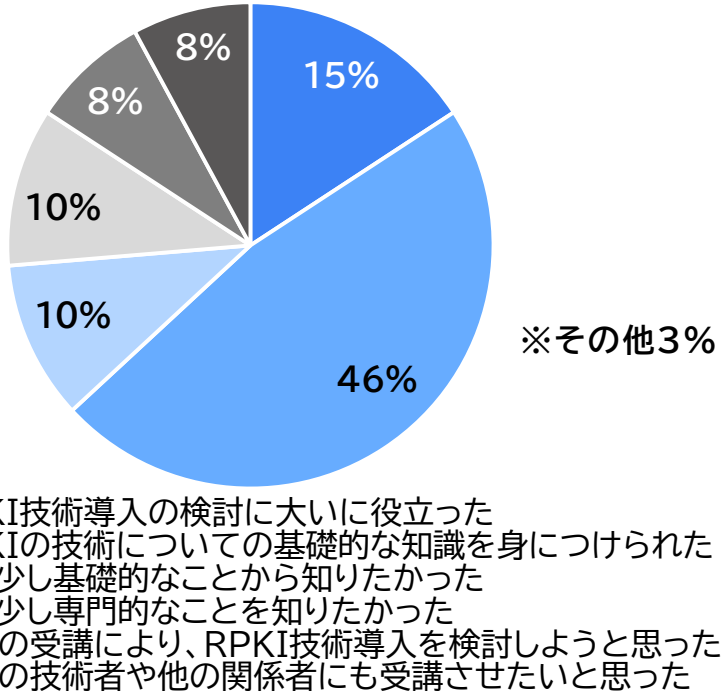
参考3. RPKI体験コースの結果 （課題・課題解消）

- より基礎的な内容である**①は約68%の参加者が受講前から理解**しており、より専門的な内容である**②は約68%、③は約76%の参加者が、参加時点で課題**として認識していた状況であった。
- ③については、**受講後に課題解消したとの回答が約59%**あったが、②については、**約34%の課題解消**に止まった。
- ROAキャッシュサーバの運用に関しては、他社依存とする意見も見られた。
- 特に第三回目の参加者には、RPKIに対する基礎的な知識を持たず、また今後の導入予定も明確にない中、参考までに参加した者もいたため、主に②の課題未解決者が多い結果の一因となった。

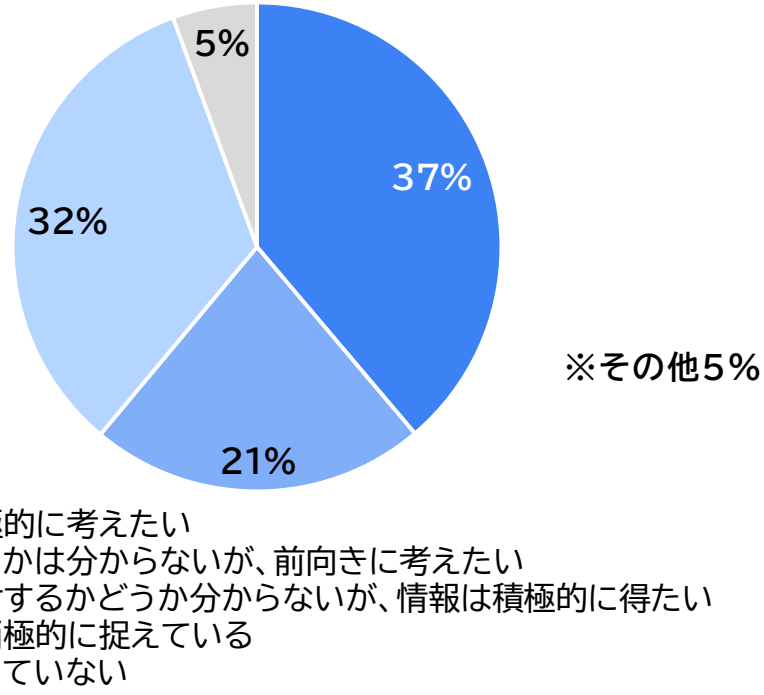


参考3. RPKI体験コースの結果（受講後の感想＆今後の導入予定）

- 「RPKIの技術について基礎的な知識が身につけられた」が約46%であり、基礎的な知識を習得するために有効である。
- また、「より基礎的」、「より専門的」なことを知りたかったという意見もそれぞれ同数あり、受講者の知見レベルの差が表れた結果となった。

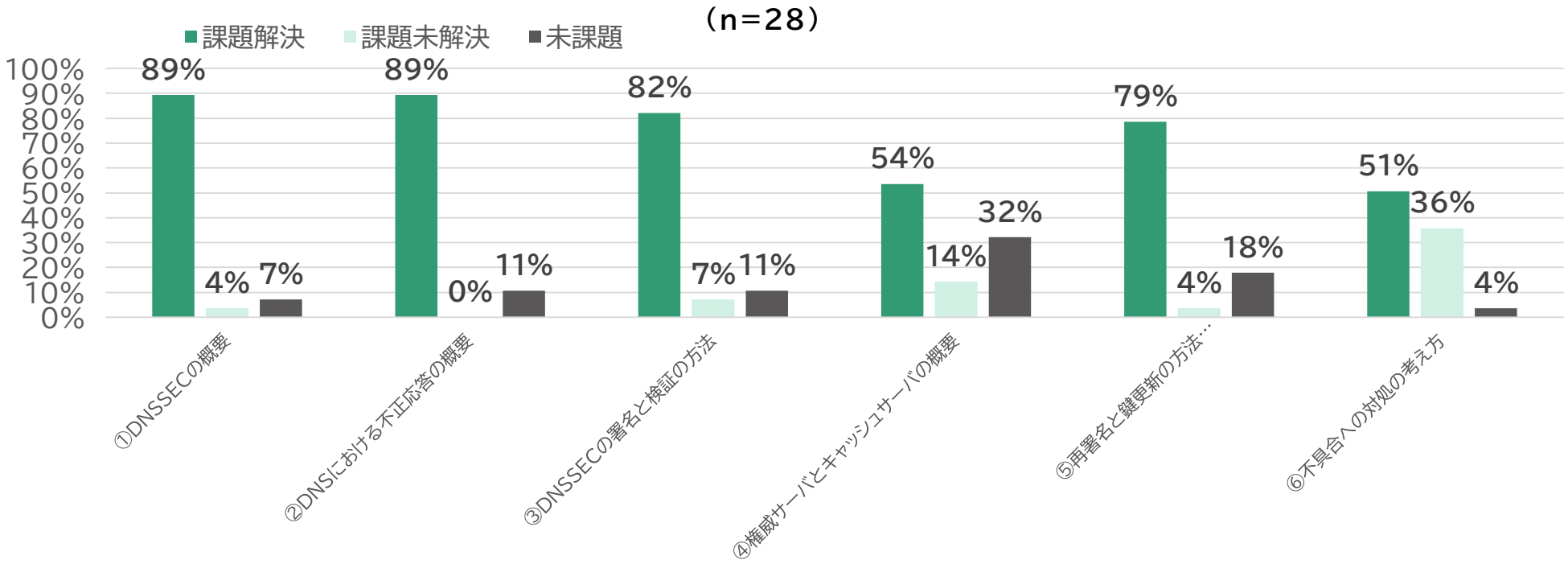


- 今後の導入意思については、「積極的に考えたい」「前向きに考えたい」とする積極的な意見の合計が約58%となった。
- 一方で、「導入は考えていない」0%、「消極的に捉えている」5%と少なく、全体的に関心度は高い。



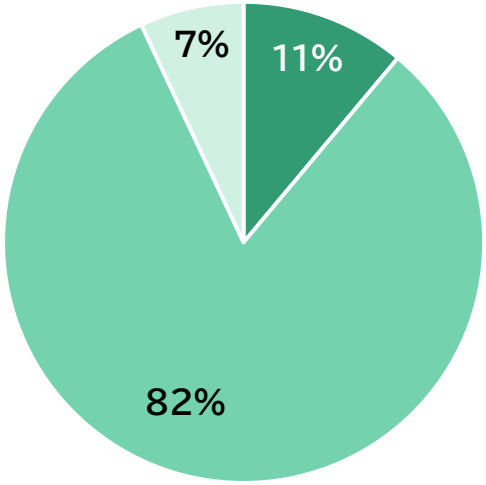
参考3. DNSSEC体験コースの結果 （課題・課題解消）

- カリキュラムの6項目いずれも、参加時に「未課題」との回答者が少なく、全般的に課題意識が高い。
- 受講後に「課題解決」したとの回答は、①～③、⑤は約80%と基礎的な内容および不正応答の概要や署名と検証の方法については課題解消できている。
- 一方、体験コースの受講だけでは課題解消できていないという回答は、④、⑥に一定数あり、他のコースの実施を推奨するなど検討する必要がある。



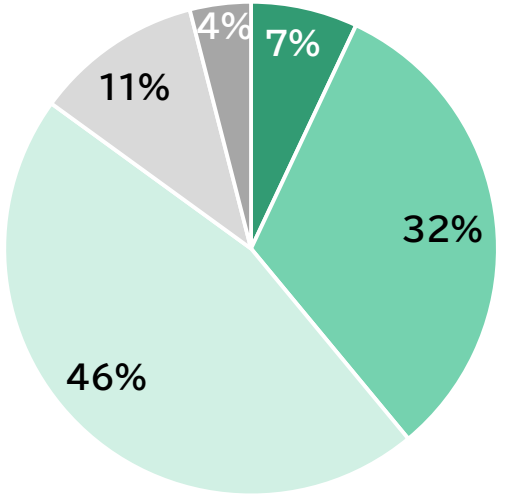
参考3. DNSSEC体験コースの結果（受講の感想＆今後の導入予定）

- 「DNSSECに技術について基礎的な知識が身につけられた」が82%であり、**基礎的な知識を習得するために有効**であり、全体的に**ポジティブな回答が多かった**。
- 一方で、7%が、「もう少し基礎的なことから知りたかった」と回答した。



- DNSSEC技術導入の検討に大いに役立った
- DNSSECの技術についての基礎的な知識を身につけられた
- もう少し基礎的なことから知りたかった
- もう少し専門的なことを知りたかった
- 今回の受講により、DNSSEC技術導入を検討しようと思った
- 自社の技術者や他の関係者にも受講させたいと思った

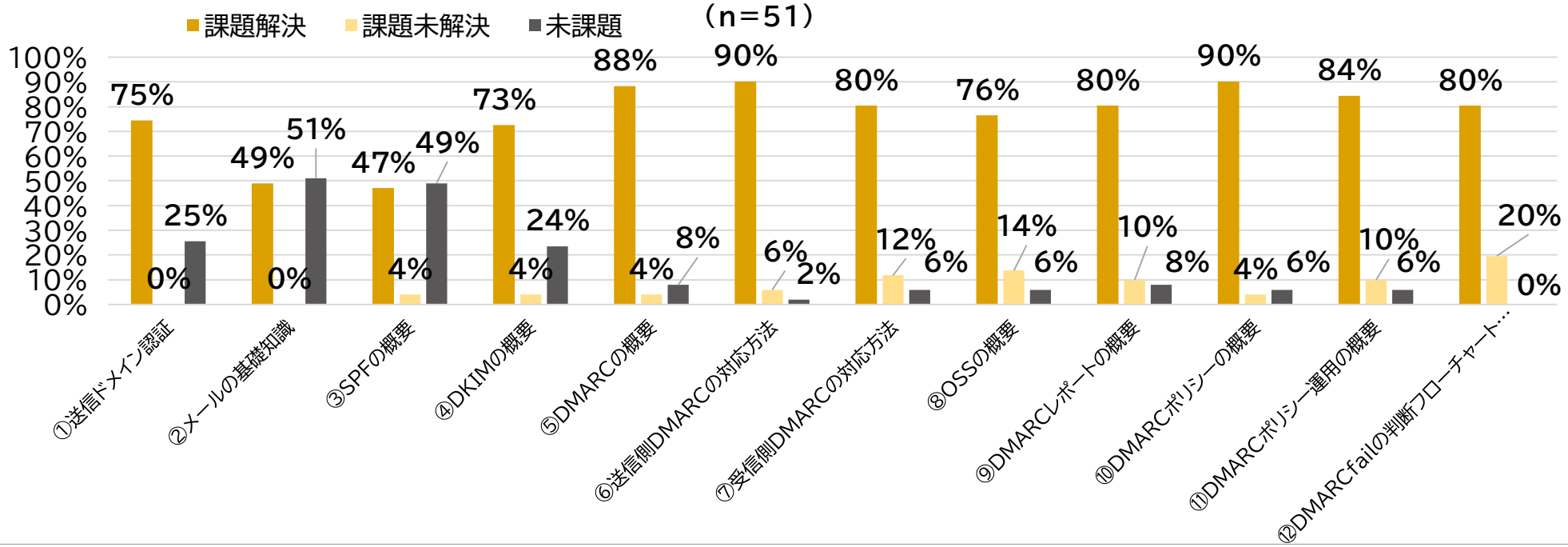
- 今後のDNSSECの導入については、**積極的な3つの回答で、合計で85%**を占めた。
- 「導入は考えていない」との回答は金融機関の外注先システム会社であり、同社における導入意思を回答したもの。**「消極的に捉えている」との回答は金融機関**からの参加者のもの。



- 導入を積極的に考えたい
- 導入に至るかは分からないが、前向きに考えたい
- 導入を検討するかどうか分からないが、情報は積極的に得たい
- 導入には消極的に捉えている
- 導入は考えていない

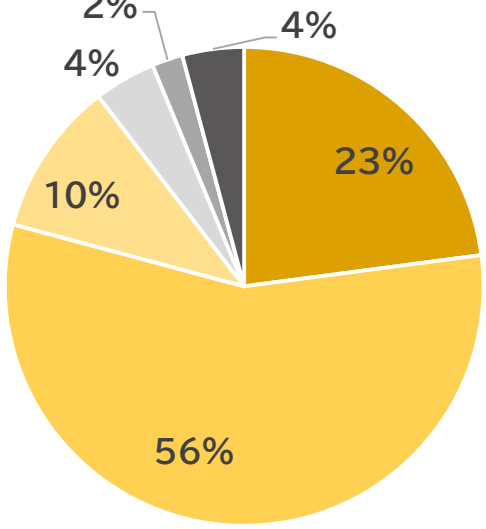
参考3. DMARC体験コースの結果 （課題・課題解消）

- 体験コースの主な内容であった12項目のち、①、④～⑫までは大半の参加者が課題解決したと回答したが、②～③は受講前から理解していた参加者も多く、未課題との回答が約半数あった。
- 未課題（受講前から理解していた等）及び体験コースの受講によって課題解決できた内容は、足し合わせると①～②は100%、③～⑥、⑩～⑪は90%超であり、基礎的な内容およびDMARCポリシーについては課題解消できている。
- 一方、体験コースの情報だけでは課題解消できていない（課題未解決）という回答は、⑦～⑨、⑫に一定数あり、他のコースの実施を推奨するなど検討する必要がある。

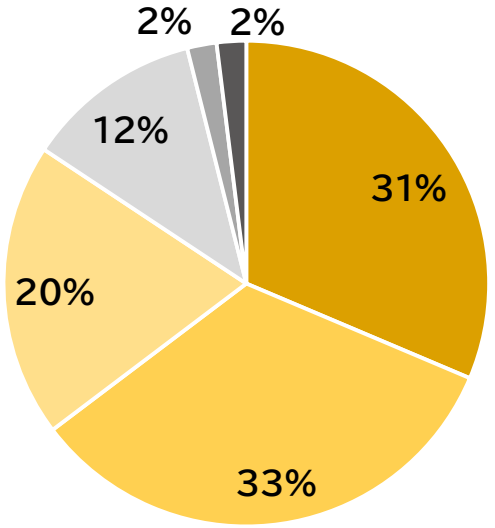


参考3. DMARC体験コースの結果（受講後の感想＆今後の導入予定）

- 「DMARC技術導入の検討に大いに役立った」と「DMARCの技術について**基礎的な知識が身につけられた**」で**79%**であり、基礎的な知識を習得するために有効である。
- また、「もう少し基礎的なことが知りたかった」との回答も10%あった。

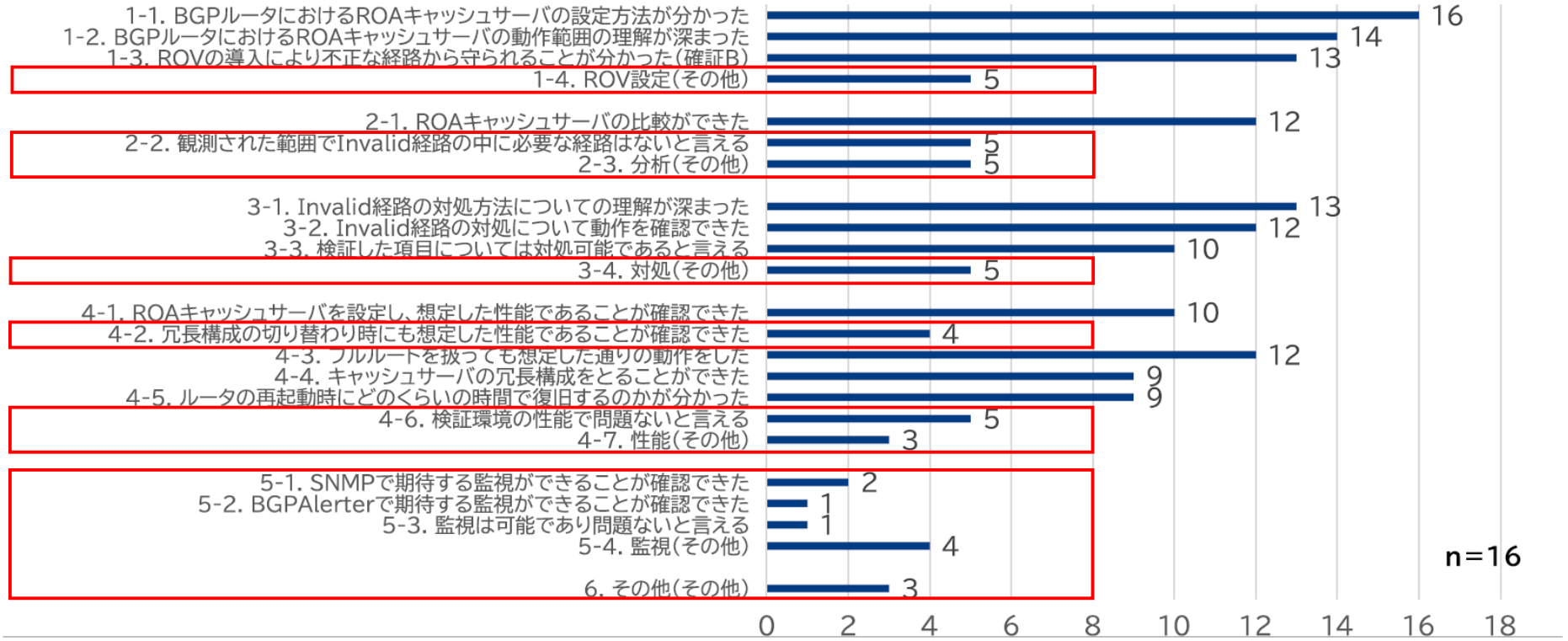


- 今後の導入予定については**前向きな意見が84%**を占め、DMARC技術の普及効果が見込めた。
- 「導入に消極的」、「導入は考えていない」はいずれも金融機関の外注先システム会社であり、同社における導入意思を回答したもの。



参考4. RPKI実証コースの結果（技術面で得られた知見）

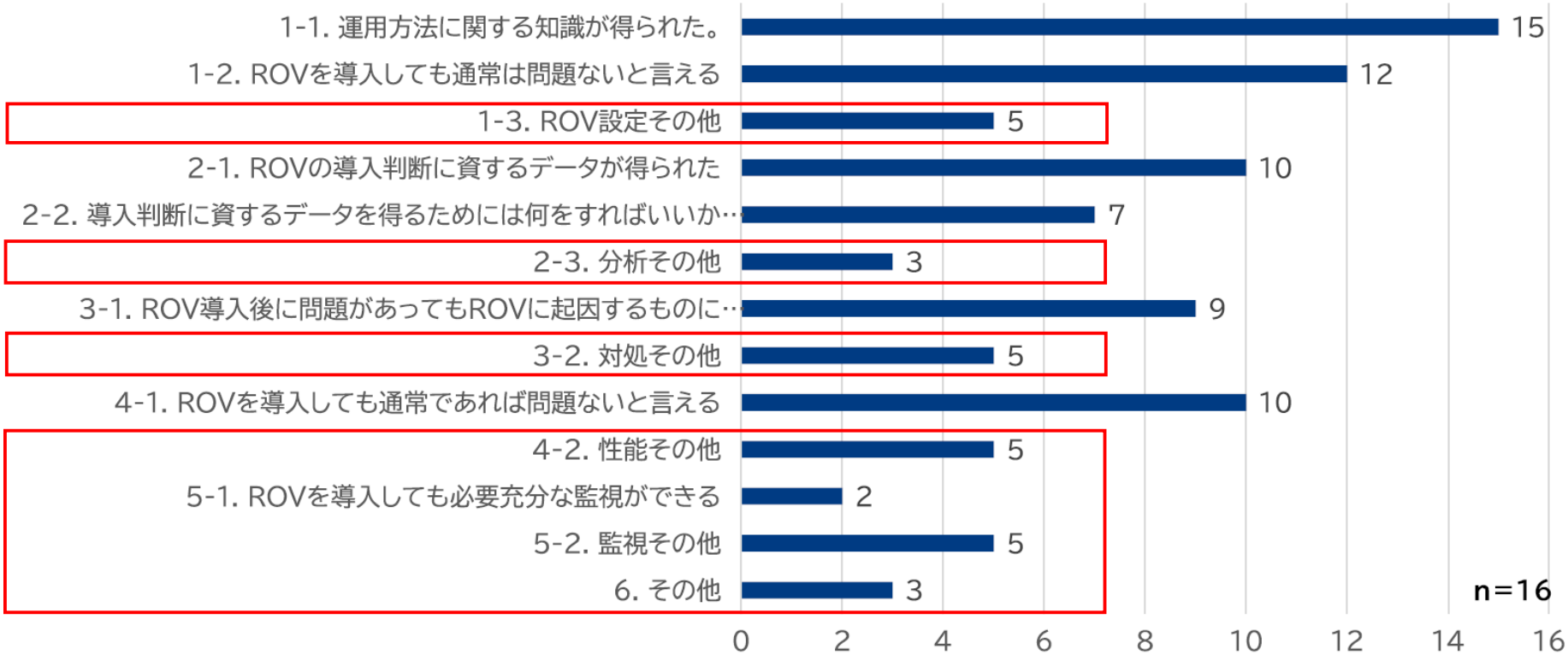
- 1-1は16社全てが知見を得られたと回答し、次いで1-2、1-3、2-1、3-1、3-2、4-3も約7割が知見を得て、Invalid経路を検知した際の確認項目を把握できたとする実証事業者もいた。
- 4-4、4-5は、昨年度より多い半数以上の実証事業者が知見を得たという回答だった。
- 少数ながら、監視関連の検証を実施した実証事業者は、いずれも知見を得たという回答だった。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考4. RPKI実証コースの結果（運用面で得られた知見）

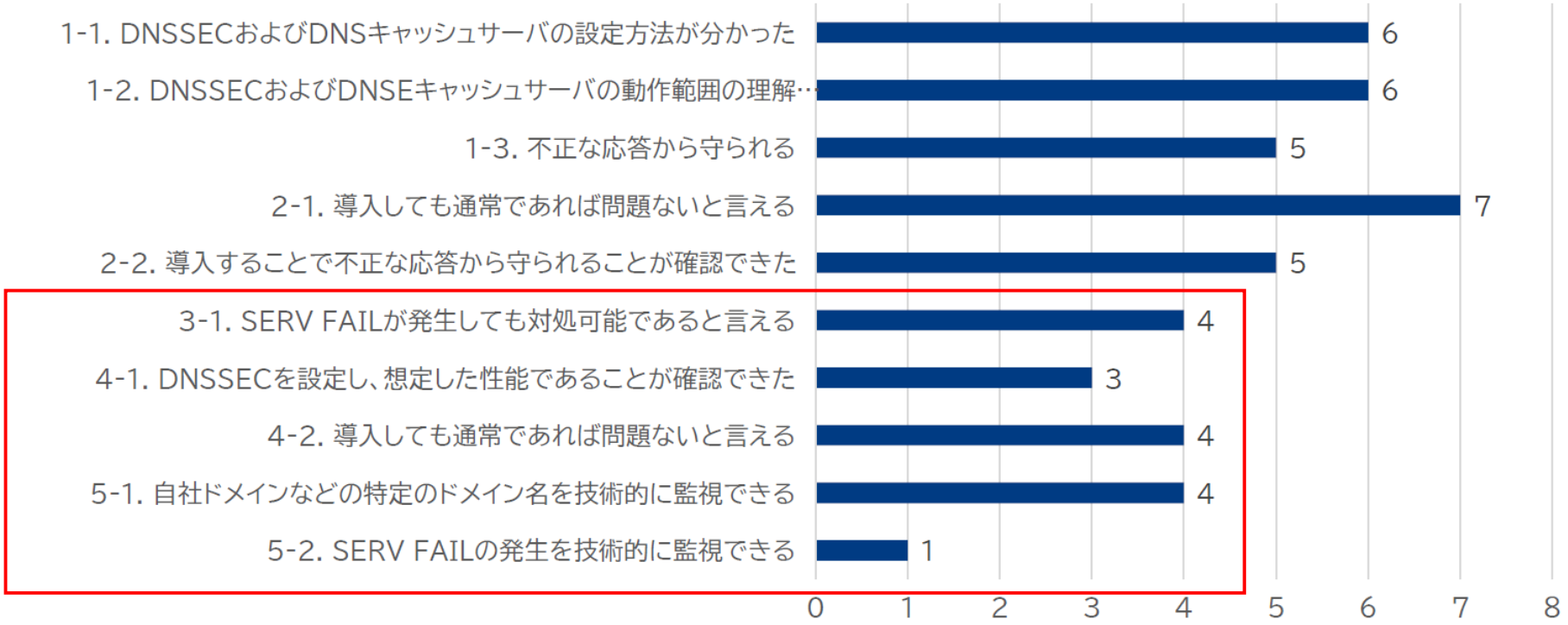
- 1-1は15社が知見を得るに至り、RPKI関連情報は少ないため役に立ったという意見もあった。
- ROVの運用は可能であると回答する一方、監視ツール等が少なく、運用中の監視について知見を得るに至らなかった実証事業者が多い。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考4. DNSSEC実証コースの結果（技術面で得られた知見）

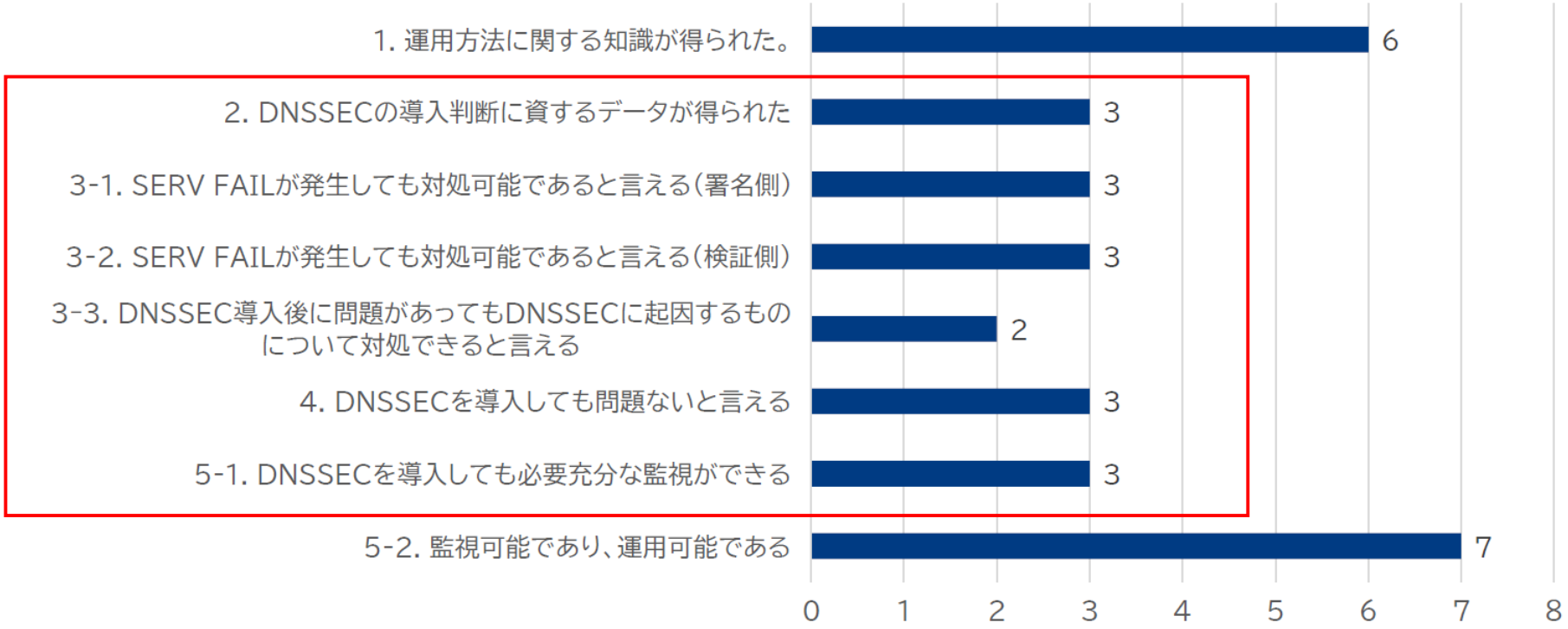
- knotDNSを活用し、導入そのもののハードルが下がったため、1-1～2-2の知見が得られたと回答した実証事業者が多かった。
- 3-1、4-2、5-1は半数の実証事業者が知見を得られたと回答した一方で、4-1、5-2については課題を残す結果となった。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考4. DNSSEC実証コースの結果（運用面で得られた知見）

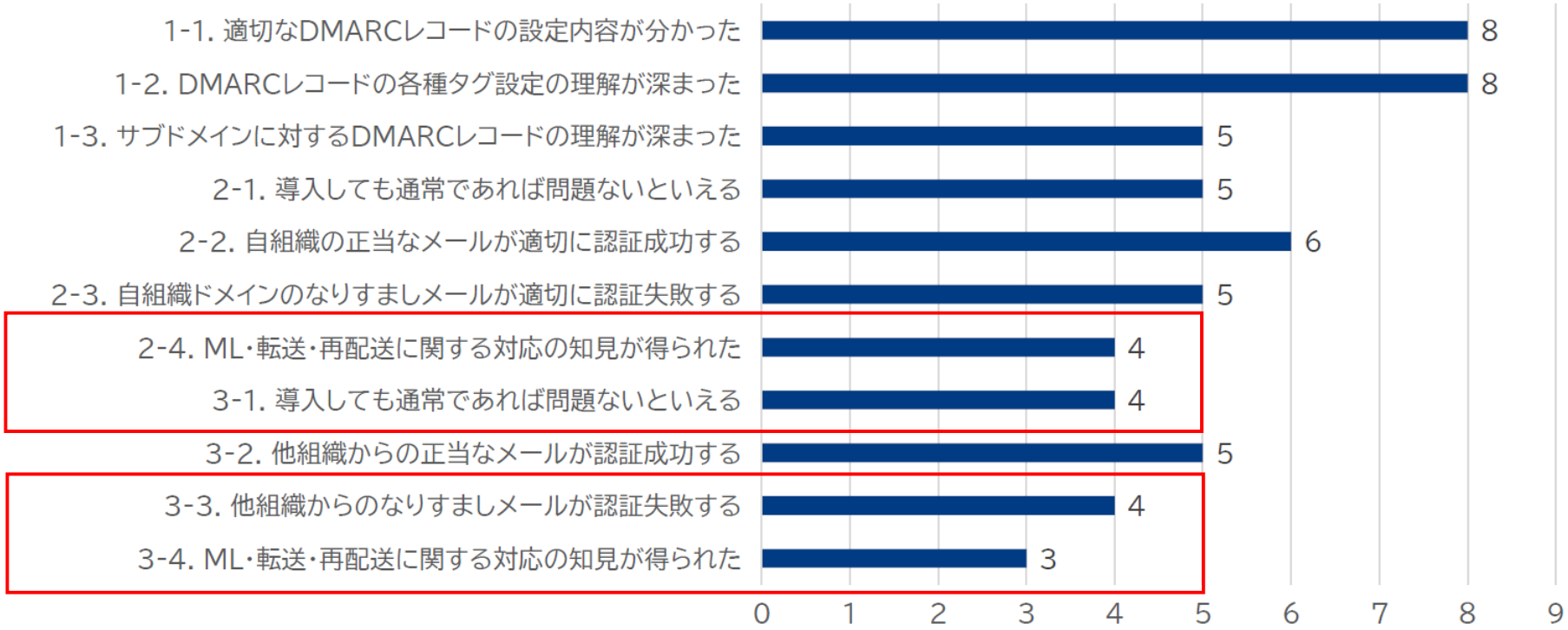
- knotDNSによって自動化される項目をどのように管理すれば良いか等、運用面では課題が残る結果となった。
- 監視が重要であるという認識は多く、グラフでは運用可能であると回答している（5-2）ものの、本当に必要充分な監視体制が整っているかについては自信がないと答える実証事業者が多数であった。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考4. DMARC実証コースの結果（技術面で得られた知見）

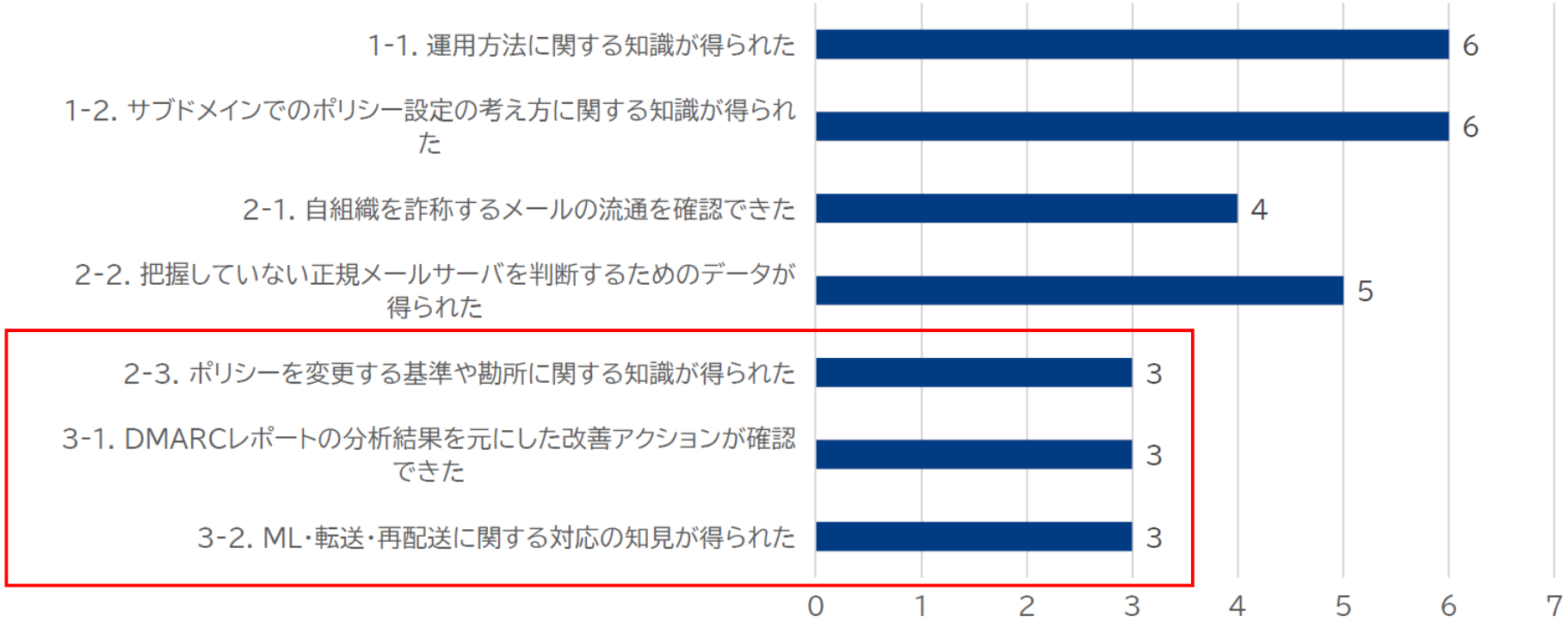
- 1-1、1-2は9社中8社が知見を得られたと回答があり、一定の効果があった。
- 2.送信メールサーバ運用については「知見が得られた」と約6割の回答があった。
- 一方で、3.受信メールサーバ運用については半数以下に止まり、3-4に至っては約7割が知見を得られていない状況のため、継続検証の必要がある。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考4. DMARC実証コースの結果（運用面で得られた知見）

- 全体的に、運用面における知見の取得には多くの課題が残る結果となった。
- 特にDMARCポリシーの変更基準や勘所については、継続検証の必要があり、専門家による診断を求める声もあった。
- 一方で、1.ポリシーやタグの調整については「知見が得られた」との回答が2/3あった。



- 「実証実験を通じ、実証事業者が知見を得た部分と知見の取得が難しかった部分を把握することができた。
- 知見の取得が難しかったと意見のあった部分は、今後の実証カリキュラム・教材の改善のポイントとしていく。

参考5. RPKIガイドライン案 概要 1／3

趣旨	
	● 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行っている組織の経営者及び技術者の方に向けたもので、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を使った対策の指針示すものとして記載。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記載。 ● 関係する立場を示し、立場に応じた項目を実施し、全体として全ての項目が実施されることを期待することとして、経営者に向けた説明として記載。 　● IPアドレスの分配を受けている全ての組織や個人 　　● **①ROAを作成する【必須事項】** 　　● **②ROAが実際のBGP経路と一致するように保つ【必須事項】** 　● インターネットに接続するASを運用している組織や個人 　　● **③ROVを行う等の処置を行う【推奨事項】**

参考5. RPKIガイドライン案 概要　2／3

技術的情報

- 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技術者に向け、不正経路と正しい経路の関係の図を示しROA技術導入効果の理解促進を図るとともに、ISPなどの相互接続時にお互いの経路情報をやり取りするために使われる経路とその広告元の組を記したROAの作成・運用の方法の指針について記載。
  - ①ROAの作成と運用管理
  - ②BGP経路とROAを一致させる手順
  - ③例外的な処置・運用上の注意
- ROAの情報を参照して経路情報が正しいかどうかを判断する仕組みであるROV導入・運用の方法の指針に対し期待される効果の評価（複数のROV実施方式別）、実証実験により得られた「三つの確証」について、技術者に向けた説明として記載。
  - 複数のROV実施方式
    - 導入方式A　ROAキャッシュサーバを自組織で構築してROVを実施する方式
    - 導入方式B　IX等で提供するROAキャッシュサーバを利用してROVを実施する方式
    - 導入方式C　ROVが行われているトランジット経路を利用する方式
    - その他の方式　パブリックキャッシュサーバを利用する方式
  - 三つの確証
    - 確証A　導入しても通常は問題ない
    - 確証B　不正から守るために役立つ
    - 確証C　不具合が起きても対処できる

参考5. RPKIガイドライン案 概要　3／3

ROA/ROV以外の不正経路対策

- RPKI（ROA/ROV）は不正経路対策として有効だが、これのみで全ての対策ができるわけではないことについて触れ、他にも考慮すべき事項や、BGP経路情報に含まれるASパス属性（AS PATH）が正しいかを検証するASパス検証の技術動向に関する参考情報について、技術者に向けた説明として記載。

リスクヘッジの事例

- ミャンマーにてロシアにあるASからの不正経路によってTwitterにアクセスできなくなったが、ROA作成によって避けられるようになった。
  - 2023年1月のJANOG51においてNTTコミュニケーションズ株式会社當間氏によるライトニングトークにおける本件事例紹介
  - ASハイジャックに対するROA作成による有効な対策の事例の一つ

参考5. DNSSECガイドライン案 概要 1／2

ドメイン名の重要性ならびに保護

- 主として、以下5点を経営者に向けた説明として記載。
  - ドメイン名は組織やサービスへの顧客からの最初の入口であり、接点となる部分であること
  - ドメイン名は組織やサービスの持つブランド力との強い関係性を有しており、安全性の高いドメイン名は顧客の信頼を獲得することができるものになり得ること
  - ドメイン名という顧客との接点に十分に注意を払うことにより提供するサービスのレピュテーションを高めることが、インターネット上でサービスを安定的に提供する上で非常に重要な要因となること
  - そのためには、ドメイン名の適切な管理と保護を行う必要があること
  - ドメインのライフサイクルマネジメントの重要性

フルリゾルバーのDNSSEC対応

- エンドユーザーが使用する端末（クライアント）からDNS問合わせを受け取り、クライアントに代わって名前解決を行うとともに、その結果をクライアントに返すという役割を持つフルリゾルバー。DNSSEC対応する際に「フルリゾルバー運用者」が行うべき事項について記載。
- 段階的に実施すべき設定・作業、トラブルシューティングの原則や方法を、運用ノウハウも添えて、技術者に向けた説明として記載。
  - 段階的に実施すべき設定・作業
    - ステップ1： DNSSEC対応・時刻同期・フラグメンテーションの回避
    - ステップ2： ソフトウェア等の対応状況の確認・性能確認と増強
    - ステップ3： 最新のトラストアンカーの確認や導入・ロギングの変更・稼動状況の確認

参考5. DNSSECガイドライン案 概要 2／2

権威DNSサーバーのDNSSEC対応

- 権威サーバーがDNSSECに対応すると追加されるリソースレコードに関し必要となる対応事項（出自の保証と不在証明）、「権威DNSサーバー運用者」及び「ドメイン名登録者」が行うべき事項について記載。
- 段階的に実施すべき設定・作業、トラブルシューティングの原則や方法を、運用ノウハウも添えて、技術者に向けた説明として記載。
  - 段階的に実施すべき設定・作業
    - ステップ1： ソフトウェア等の対応状況の確認・性能確認と増強
    - ステップ2： 鍵の保護手段の検討→署名方法の検討
    - ステップ3： 日常的な監視と確認・ログによる異常の有無の確認といった作業
    - ステップ4： 鍵の管理やロールオーバーについての対応

ドメイン名登録・登録管理関係者

- ドメイン名登録・登録管理関係者がDNSSECの有効化を選択できるようにするために、「レジストラ（指定事業者）」及び「ドメイン名登録者」が行うべき事項について記載。
- 段階的に実施すべき設定・作業を、技術者に向けた説明として記載。

リスクヘッジの事例

- DNSSECはキャッシュポイズニングによる攻撃に有効な技術であるが、現時点において、キャッシュポイズニングによる攻撃は調査研究の結果、年単位の期間で観測されていない。

参考5. DMARCガイドライン案概要　1／3

本ガイドラインについて

- 迷惑メール・なりすましメールによる被害を減らしていくため、主として以下の2点を経営者に向けた説明として記載。
  - 送信ドメイン認証などを利用してメールの受信判断を厳しくしていく動きも広がってきている現状
  - 自組織のブランドとしてのドメイン名を高めていくためにも、関連技術を含めて送信ドメイン認証技術に正しく対応していくことが今後より重要になっていくこと

ドメイン管理者

- メール送信者が用いるドメイン名に対する設定を行う、ドメイン名の管理者が行うべき事項について記載。段階的に実施すべき設定・作業を技術者に向けた説明として記載。
  - 送信側の送信ドメイン認証設定
  - 組織ドメイン名についてのDMARCレコード設定・メールに利用しないドメイン名への設定
  - DMARCレポートの活用

メール配送事業者の送信ドメイン認証設定

- メールマガジンなど多数のメール受信者へのメール送信を依頼元に代わって送信する事業者が、大量のなりすましメールなどの迷惑メール送信に加担しないよう、またメール受信側に対して、メール送信元を判断できるよう送信ドメイン認証技術を正しく設定すべきであることを、技術者に向けた説明として記載。

参考5. DMARCガイドライン案概要　2／3

メール再配送時の設定

- メール作成者によって送信されたメールが送信先のメールアドレスから別のメールにアドレスに自動的に送信されるメールを、メール再配送する（①転送メール、②メーリングリストに投稿されたメール）事業者に対して、段階的に実施すべき設定・作業を、技術者に向けた説明として記載。
  - 転送メールの設定
  - メーリングリストの設定

メール受信者

- 受信したメールが、なりすましメールであるかどうかを判断するためにメール受信時にDMARC認証を行い、DMARC などの送信ドメイン認証技術で認証できたとしてもなりすましメールでないとは限らないので、認証されたドメイン名が受け取るべきメールであるかを確認する必要があることを記載。
- メール受信側において段階的に実施すべき設定・作業を、技術者に向けた説明として記載。
  - 送信ドメイン認証
  - 認証ドメイン名の評価
  - DMARCレポートに対するフィードバック
  - メール受信者にわかりやすい認証結果を表示

参考5. DMARCガイドライン案概要　3／3

リスクヘッジの事例

- DMARC導入に向けた動きが活発化している理由として、以下の5点が挙げられる。
  - 令和5年2月に経産省/総務省/警察庁がクレジットカード会社に対して、DMARC対応を要請。
  - 令和5年7月に改訂された政府統一基準（政府機関等のサイバーセキュリティ対策のための統一基準群）において、DMARCが要件に含まるように。
  - 半導体企業や携帯端末製造会社がサプライチェーンリスク対策として、日本の取引先企業（主に化学、製造、輸送業など）にも早急なDMARC対応を求める。
  - 複数の監査法人が監査項目にDMARCを追加
  - 令和6年2月より、Google/Yahooが新スパム対策として1日5000通を超えるメールを送信する送信者にDMARC対応を義務付け
- 令和6年1月、神奈川県の公立高校入試のインターネット出願システムにおいて、Gmailのメールアドレスにのみ通知メールが届かない事象が発生。
  - 本件、当該メールシステムがGmailの要件（送信ドメイン認証に対応すること）に達しておらず、当該メールシステムからGmailあてに送られたメールがfailしたものと推察されている
  - 当該メールシステムがDMARCをはじめとする送信ドメイン認証に対応していれば発生しなかったと思われる