DNS Summer Day 2023

ネットワークセキュリティ技術導入実証などの総務省の取組

令和５年６月

総務省サイバーセキュリティ統括官室
広瀬　一朗

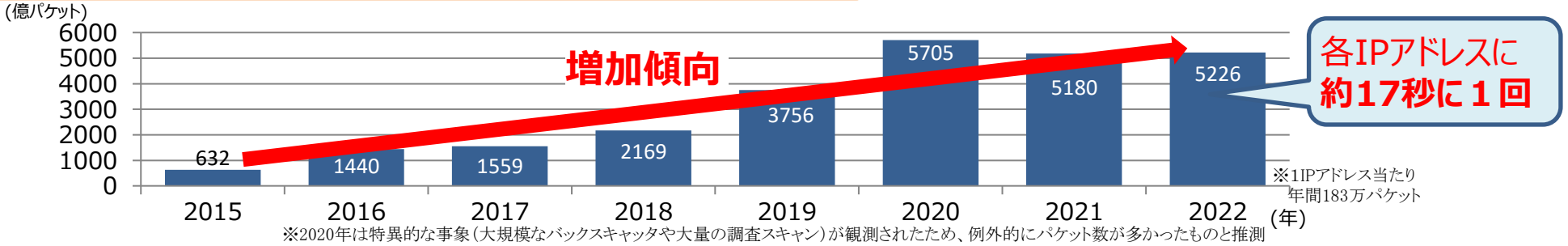
サイバーセキュリティ上の脅威の増大

- ✓ 大規模サイバー攻撃観測網※にて観測されるグローバルなサイバー攻撃関連の通信数は年々、増加傾向。

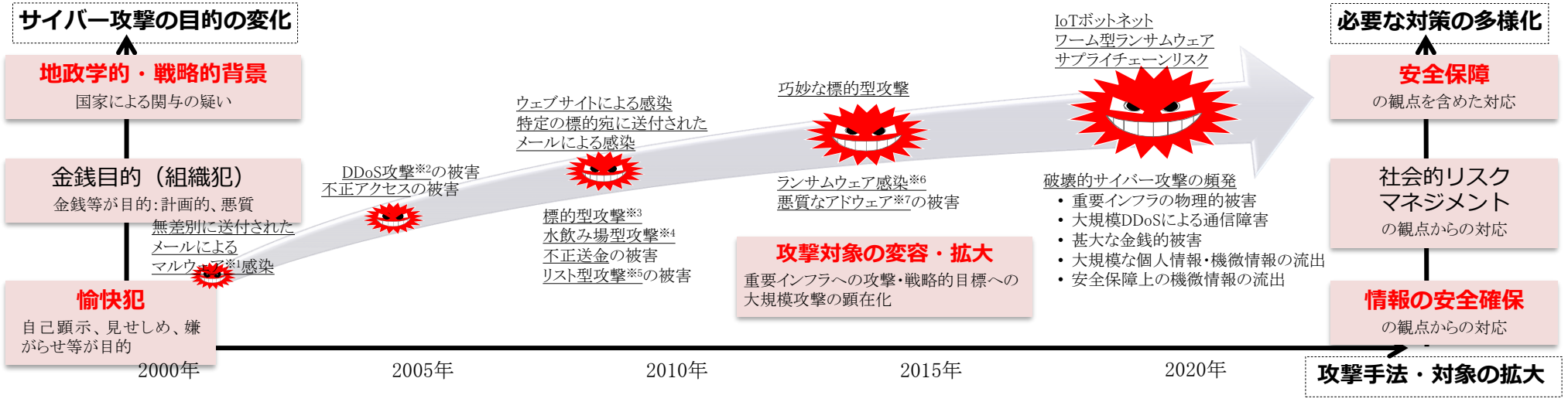
※国立研究開発法人情報通信研究機構(NICT)の未使用のIPアドレス30万個(ダークネット)を活用した観測網

- ✓ サイバー攻撃の目的の変化(愉快犯→金銭目的→地政学的・戦略的背景)や攻撃手法・対象の拡大など、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。

NICTERで１年間に観測されたサイバー攻撃関連の通信数



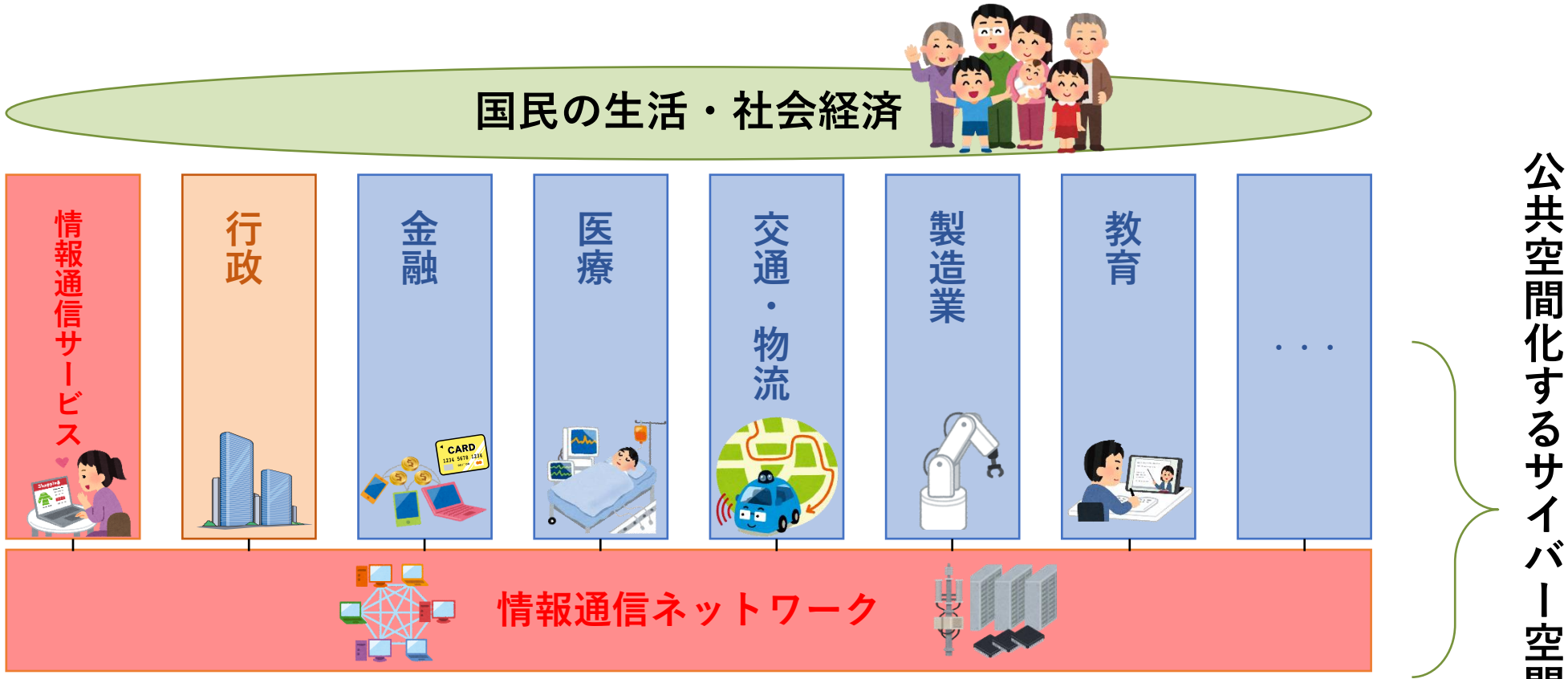
※2020年は特異的な事象(大規模なバックスキャッタや大量の調査スキャン)が観測されたため、例外的にパケット数が多かったものと推測



サイバーセキュリティと総務省の役割

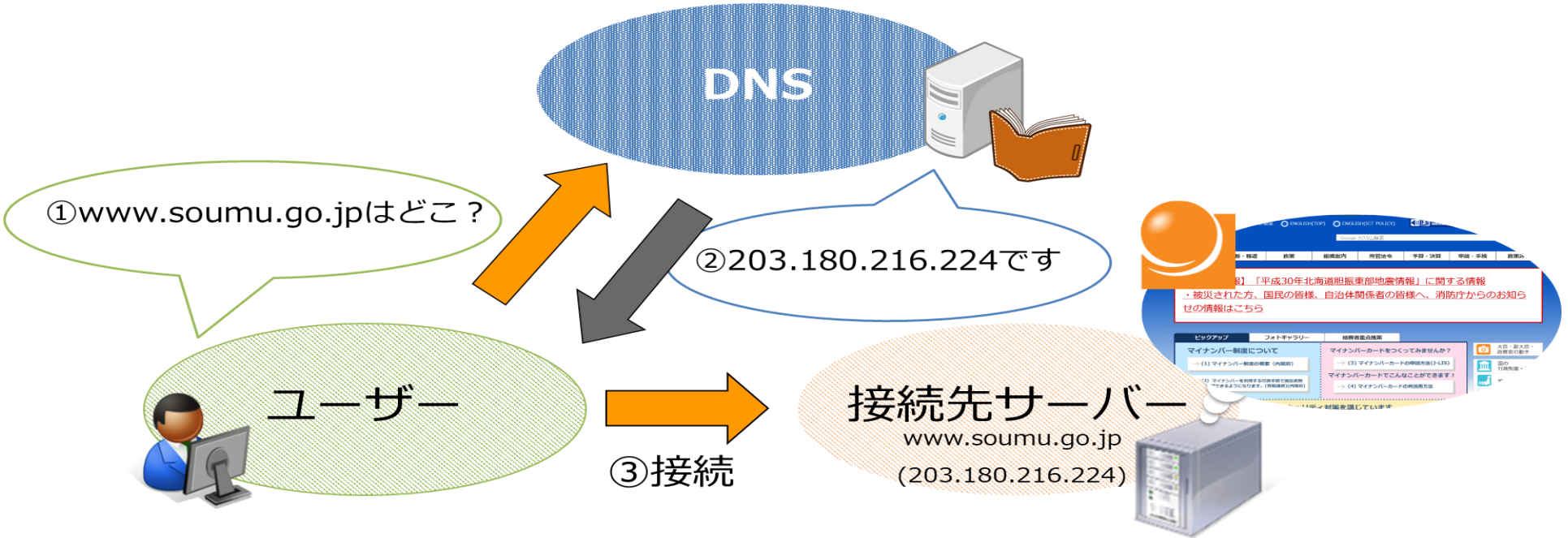
- ✓ **サイバー空間**は、あらゆる主体が利用する公共空間であり、その**根幹は情報通信ネットワーク**。
- ✓ **サイバー攻撃**等により、**情報通信ネットワークの機能停止や情報の漏えい等**が生ずれば、**国民の生活**や**我が国の経済社会**に**甚大な影響**が発生するおそれ。

⇒ 総務省の役割：社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること。



インターネットにおけるDNSの重要性

- 「インターネットの電話帳」であるDNSが正常に機能し、ドメイン名を用いた正しい相手先の指定が可能になることは、インターネットを安全に利用するための必要条件の一つ。
- DNSの正規の機能を悪用する攻撃として、DNSフラッド攻撃、DNSランダムサブドメイン攻撃、DNS キャッシュポイズニング、DNSハイジャック、DNSトンネリングなどがある。
- 最近でも、通信事業者の網内の踏み台からの大量のDNSクエリで当該事業者のDNSキャッシュサーバが応答できなくなった事例や、国内外の踏み台からの大量のランダムなサブドメインへのDNSクエリで特定の権威DNSサーバーが応答できなくなった事例がある。
- こうした攻撃への対策としては、トラヒックの監視や緩和とともに、DNSSECのようなセキュリティ技術の導入が有効。



（参考）「ICTサイバーセキュリティ総合対策2022」（令和4年8月12日公表）の概要

- 総務省では、2017年から「サイバーセキュリティタスクフォース」（座長：後藤厚宏情報セキュリティ大学院大学学長）において、情報通信分野におけるサイバーセキュリティに係る課題の整理や必要な取組の検討を実施。
- サイバーセキュリティ戦略の策定（2021年9月）、サイバー攻撃リスクの拡大等も踏まえ、パブリックコメントを経て2022年８月12日に、今後重点的に取り組むべき施策として「ICTサイバーセキュリティ総合対策2022」を取りまとめ。

１．情報通信ネットワークの安全性・信頼性の確保

- 2022年度の実証の成果を踏まえ、2023年度も電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証を継続
- 通信の秘密に配慮しつつ、電気通信事業者による、より迅速なサイバー攻撃対策を実現するため、制度改正の必要性も含めて検討
- 2年後に実施期限を迎えるNOTICE（国立研究開発法人情報通信研究機構（NICT）がパスワード設定等に不備があるIoT機器の調査等を行い、電気通信事業者を通じて利用者に注意喚起を行う）の取組の拡充及びその検討
- 情報通信分野でのSBOM（ソフトウェア部品表）の導入可能性の検討

２．サイバー攻撃への自律的な対処能力の向上

- NICTにおいて、CYNEX（サイバーセキュリティ統合知的・人材育成基盤）の2023年度の本格運用に向けた継続的な構築・運用及び産学官コミュニティの形成
- NICTが実施する実践的サイバー防御演習（CYDER）について、未受講の地方公共団体への受講の促進や、出前講習、サテライト講習の試行及びオンライン演習の演習効果向上のための改善を実施
- 2025年日本国際博覧会側からの要望を踏まえつつ、「サイバーコロッセオfor万博（仮）」の関連組織セキュリティ担当者等への実施を検討

３．国際連携の推進

- ASEANのセキュリティ人材の育成支援を実施する日ASEANサイバーセキュリティ能力構築センター（AJCCBC）について、プログラム拡充、有志国との第三者連携等の強化を図るとともに、参加者のすそ野拡大、ASEAN以外のインド太平洋地域における能力構築支援の検討
- 5Gセキュリティ等の我が国の取組について国際標準化等の可能性を継続的に検討し、国際標準化機関において発信

４．普及啓発の推進

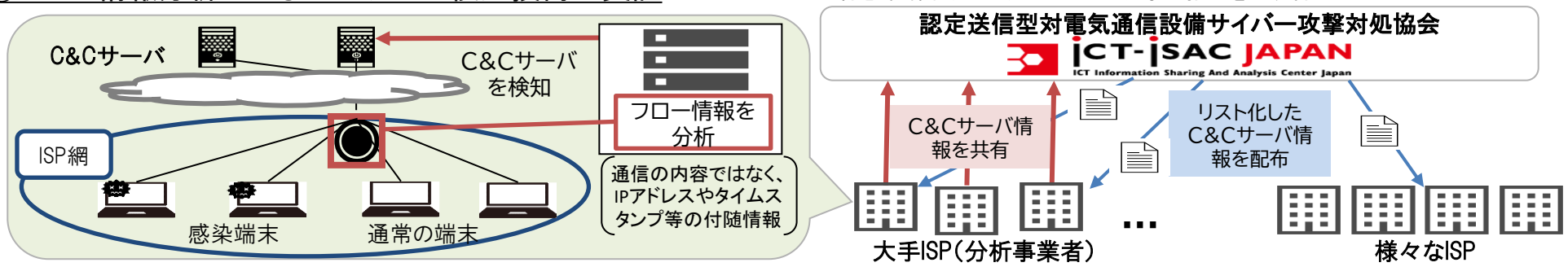
- 中小企業等へのテレワークセキュリティガイドライン・チェックリストの一層の周知や、地域SECUNITYでのインシデント対応演習の開催支援
- 2022年内に、サイバー攻撃被害を受けた組織において実務上の参考となる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を策定
- こどもや高齢者に向けたサイバーセキュリティの普及啓発の強化を検討

サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

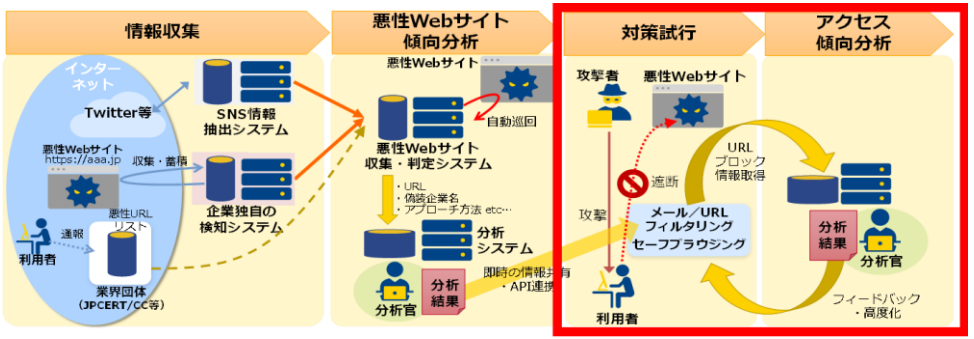
✓ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が、より効率的・積極的に対処できるようにするため、①フロー情報分析によるC&Cサーバ検知技術の実証、②悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ 対策手法の導入に係る実証等を実施。

①フロー情報分析によるC&Cサーバ検知技術の実証

※C&Cサーバ：各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

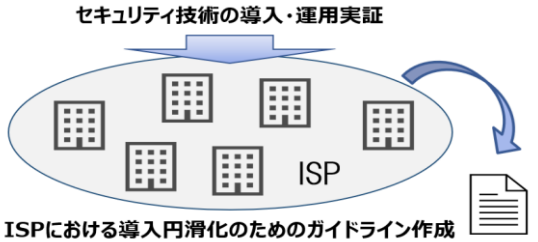


② 悪性Webサイトの検知技術・共有手法の実証



※悪性Webサイト：IDやパスワードなど個人情報の窃取に使用される、正規の金融機関等に偽装したWebサイト（フィッシングサイト） など

③ ネットワークセキュリティ対策技術の導入実証



※ ネットワークセキュリティ技術：BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC 等

サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証　R3補正18.0億円、R4補正18.0億円

（参考）IoTセキュリティ強化の取組

※NOTICE（National Operation Towards IoT Clean Environment）

➢ IoT機器（監視カメラ、ルータ等）を悪用するサイバー攻撃の深刻化への対応として、情報通信研究機構（NICT）が、**ID・パスワードに脆弱性があるIoT機器及び感染通信を出しているIoT機器**を調査し、電気通信事業者（ISP）を通じて利用者への注意喚起を行う取組を2019年より実施。

【ID・パスワードに脆弱性があるIoT機器】

※NICT法を改正し、今年度末までの５年間の時限措置として実施

情報通信研究機構(NICT)

これまでサイバー攻撃に用いられたもの	Password admin1234
同一の文字等を用いたもの	aaaaaaa 12345678

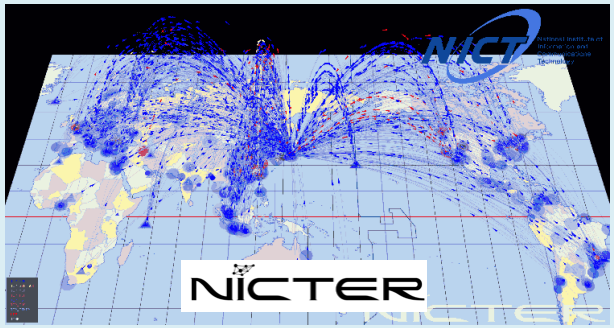
機器調査

特定アクセス行為により、ID・パスワードに脆弱性がある機器（その機器に係るIPアドレス）を特定

【感染通信を出しているIoT機器】

情報通信研究機構(NICT)

感染通信の観測



通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2023年４月）

4,685件（３月度:4,176件）
（参考）2019年度からの累積件数：87,435件

ISPへの通知件数（2023年４月）

１日平均388件（３月度:516件）
（参考）2019年度からの値：１日平均440件

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施

DNS Summer Day 2023

ISPにおけるネットワークセキュリティ技術の導入に関する調査

三菱総合研究所

デジタル・イノベーション本部

2023/06/23

Agenda

1. 事業の目的
2. 事業の概要
3. 技術概要と普及状況
4. 実証概要
5. 技術的課題の調査と促進に向けた検討

参考1. 実証実験参加者一覧 ・ 有識者会議参画メンバー

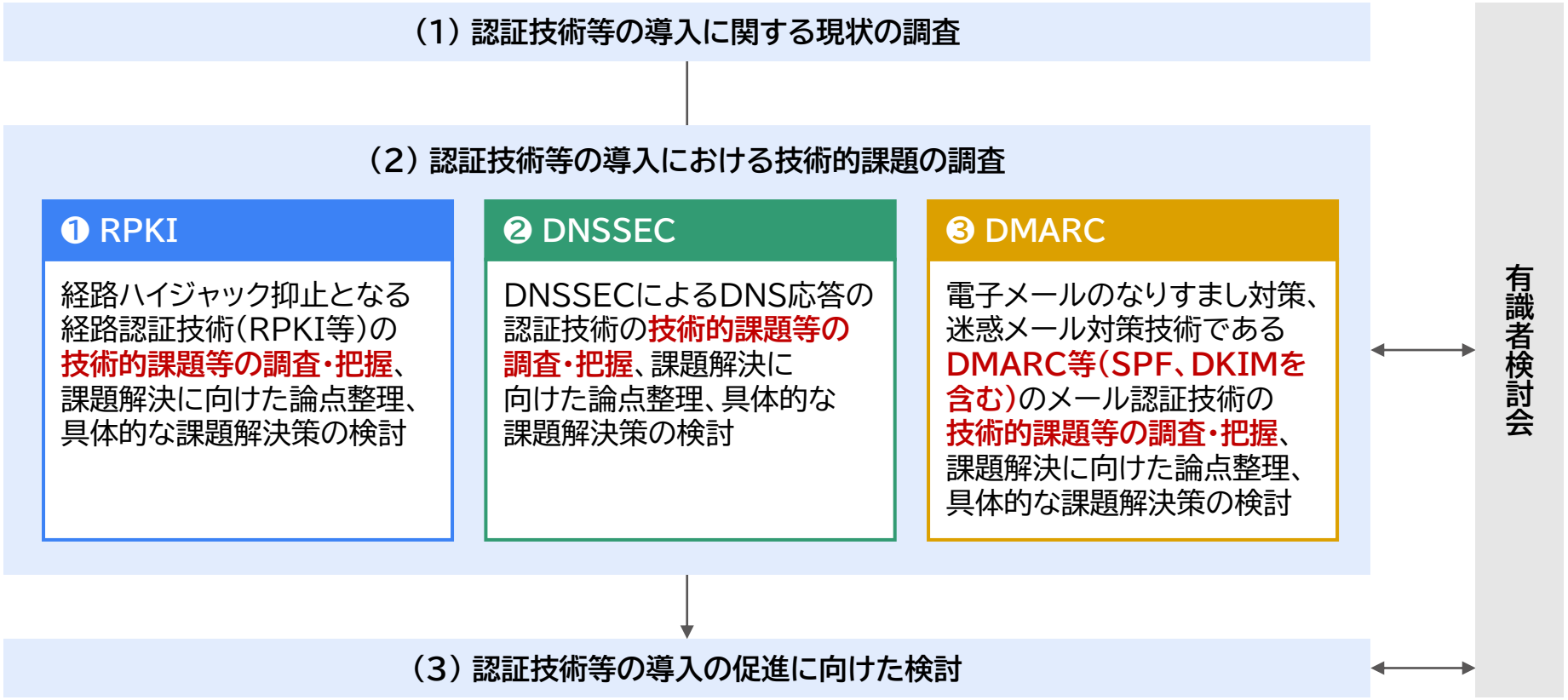
参考2. RPKI/DMARCの実施概要

1. 事業の目的

- 情報通信分野の急速な技術革新により、高度化・多様化した電気通信サービスが国民各層に広く普及・浸透し、デジタル化を支える情報通信ネットワークは、今や国民生活や経済活動の重要かつ不可欠な基盤となり、その重要性は更に一段と高まっている。一方で、2022年7月のフィッシング報告件数は、2021年7月に比べて約3倍に増加する等、**サイバー攻撃リスクが急速に拡大しており、電子メールのなりすまし、迷惑メール等の被害は継続して発生**している状況である。また、**悪意又は設定ミスによるBGPハイジャックやDNSハイジャックなどのリスク**も生じている。
- 今後、デジタル社会の実現に向けて、国民一人ひとりが安全に安心してデジタルを活用していくためには、**電気通信事業者のネットワークにおいて、各段階における適切なセキュリティ対策を講じることをはじめ、サービス提供者側から積極的なセキュリティ対策を実施**し、より安全なインターネット環境を確保していくことが今後ますます重要になる。
- **総務省では、インターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現するため、電子メールのなりすまし対策や迷惑メール対策、及び経路ハイジャックの抑止のための認証技術の普及促進を行っているが、国内ISPでの導入は一部にとどまっている。このため、これらの実装状況や技術導入の課題を把握し、導入を促すこと**が求められる。
- **本調査では、各種認証技術等（①RPKI、②DNSSEC、③DMARC）の導入を促すことを目的とし、認証技術等導入の実証を通じ、導入に係る技術的課題等を調査・把握し、課題解決に向けた論点を整理の上、具体的な課題解決策を検討する。**

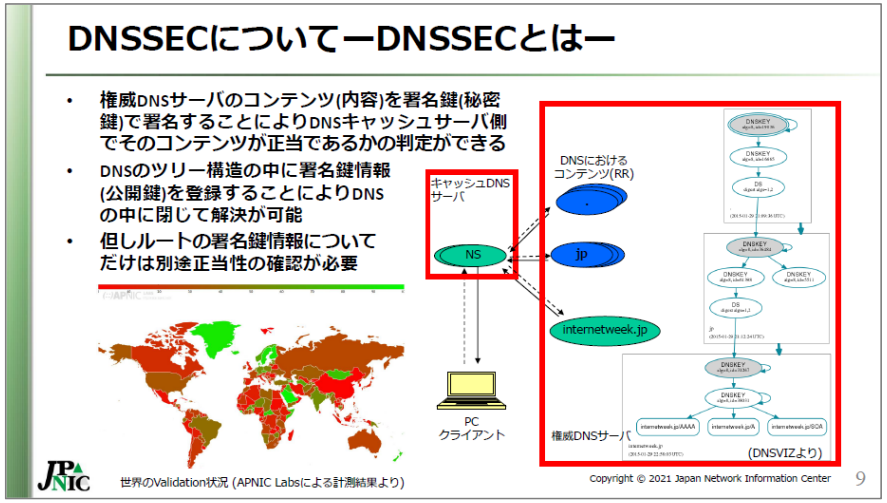
2. 事業の概要

（1）各種認証技術等（①RPKI、②DNSSEC、③DMARC）に関する**現状の調査**
（2）各種認証技術等（①RPKI、②DNSSEC、③DMARC）の導入における**技術的課題の調査**
（3）各種認証技術等（①RPKI、②DNSSEC、③DMARC）の**促進**に向けた検討

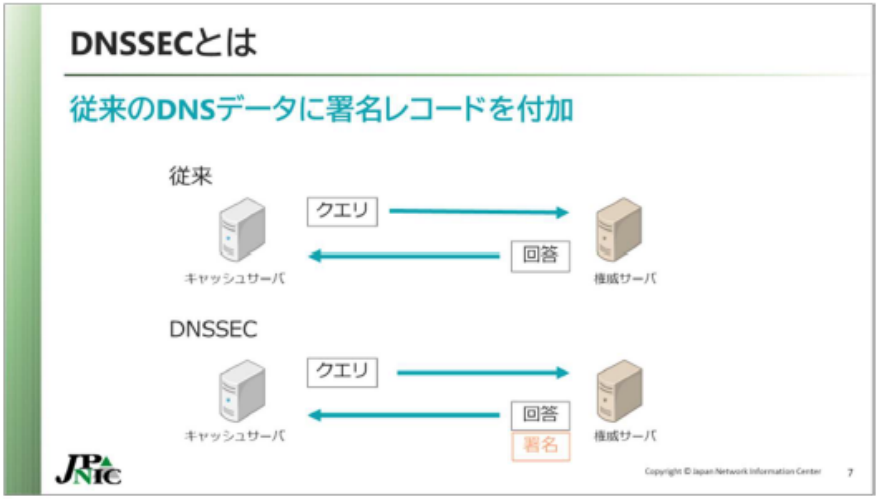


3.1. DNSSECの概要

- 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。



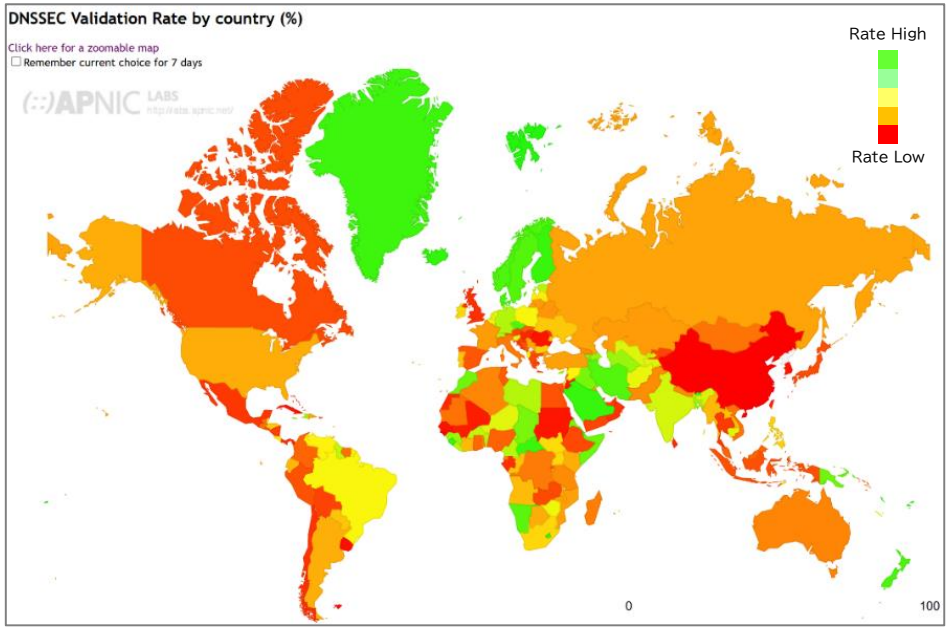
サイバーセキュリティタスクフォース（第３０回）資料３０－３の抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html



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

3.2. DNSSECの普及状況

- APNIC Labsでは、DNSSECの導入状況を公表している。
- 上位から、サウジアラビア（SA）89%、中央アフリカ共和国（CF）97% 、アイスランド（IS）96%、フィンランド（FI）95%、グリーンランド（GL）93%などの国が高いDNSSECバリデーション率を示している。
（**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）
- 2023年3月時点で、**日本（JP）は、15%**に留まっている。



DNSSEC World Map https://stats.labs.apnic.net/dnssec

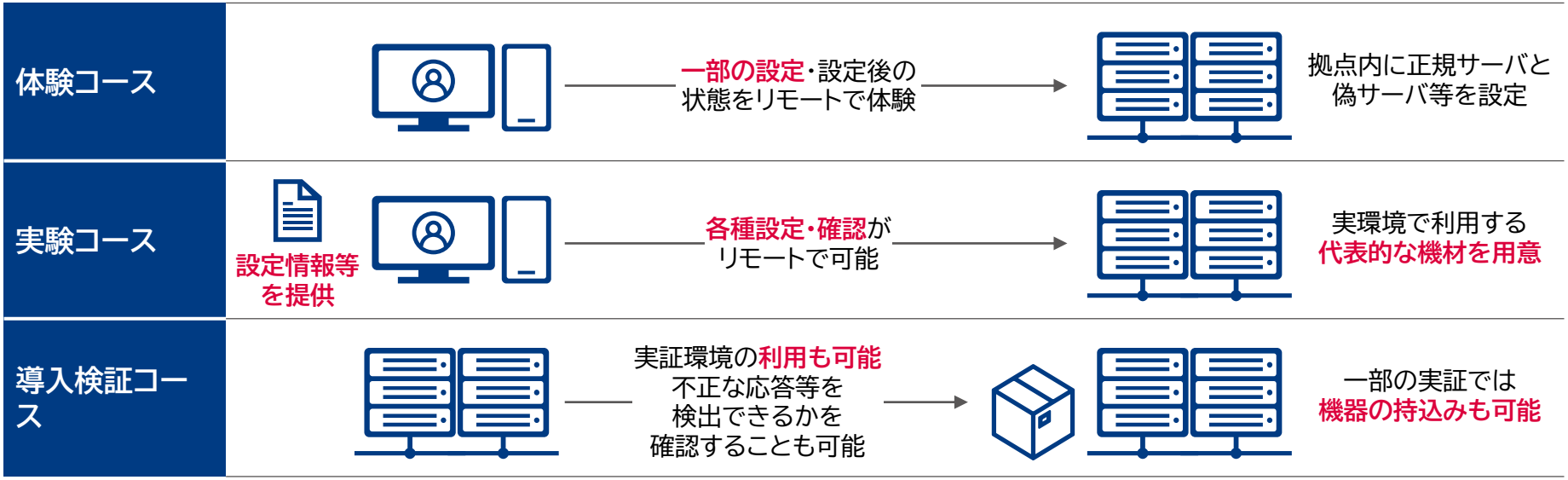
4.1. 実証規模

- 実証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22社（のべ56人）、実験コースに8社、導入検証コースに4社**
- 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15社（のべ25人）、実験コースに2社、導入検証コースに8社**
- 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、航空会社等の事業者
  - 実証参加者数：**体験コースに7社（のべ27人）、実験コースに2社、導入検証コースに8社**

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

4.2. 実証環境の整備

- 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。



4.3. 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

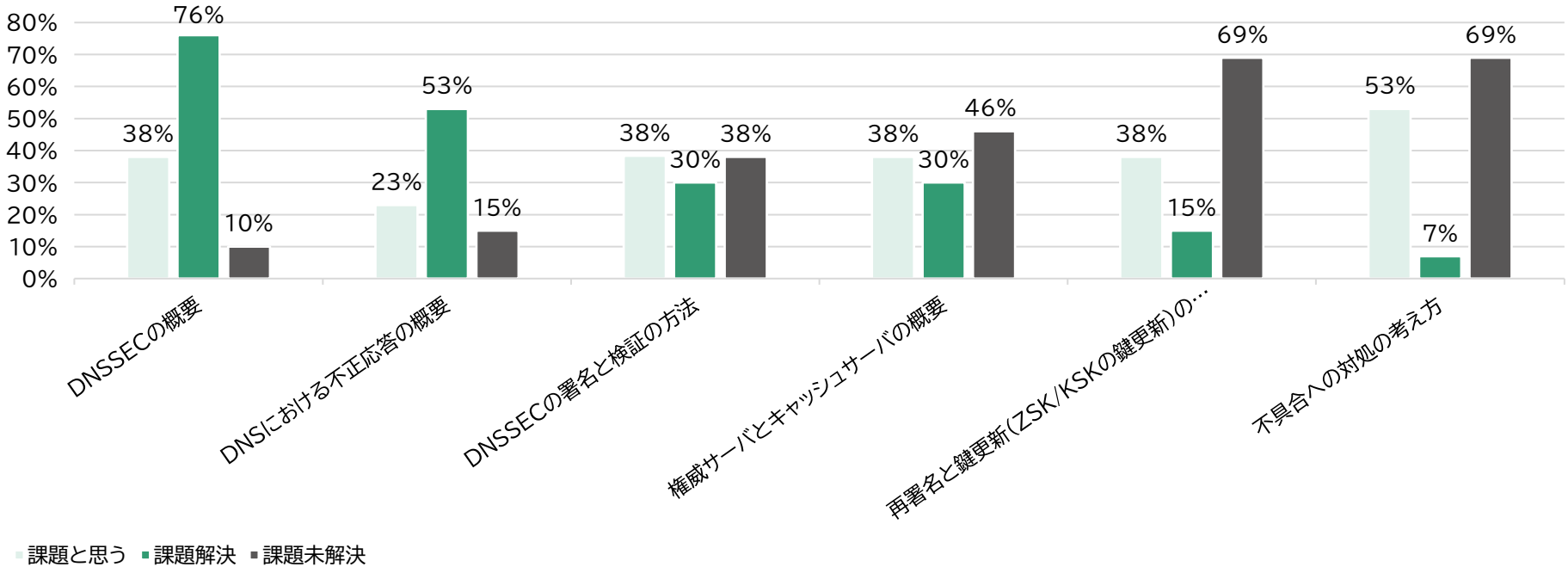
❸ DMARC｜体験コースコースマテリアル一覧

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

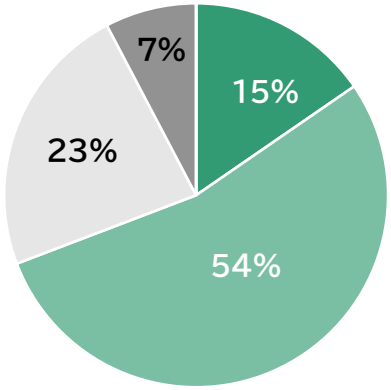
5.1. DNSSEC体験コースの結果

- 体験コースの主な想定課題については、②DNSにおける不正応答の概要を除き、①・③～⑥は半数以上であり、**想定課題が正しい結果**であった。
- また、①DNSSECの概要は、**半数以上が課題解消**できたという回答であった。
- 一方で、④権威サーバとキャッシュサーバの概要、⑤**再署名と鍵更新**、⑥**不具合への対処**の考え方は、半数以上が、課題未解消（本体験コースでは情報、体験不足）という結果であるため、**他の実験コースなどへの参加を推奨する必要**がある。



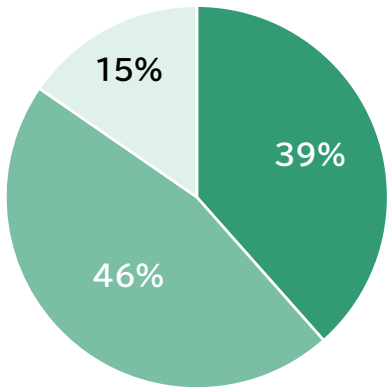
5.1. DNSSEC体験コースの結果

- 体験コースの受講の感想では、「DNSSEC技術について基礎的な知識が身につけられた」が**54%**であり、基礎的な知識を習得するために有効である。
- また、「DNSSEC技術導入の検討に大いに役立った」が15%で、この2つの回答で**69%**を占める。



- 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付けられた
- 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、「導入を積極的に考えたい」が39%、「導入に至るか分からないが、前向きに考えたい」が46%であり、**合計で85%**を占めた。
- 「導入を検討するかどうかわからないが情報は積極的に得たい」が15%であり、これらをあわせると100%となり、**DNSSEC普及の効果が見込める。**



- 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

5.2. 技術的課題の調査

- 各種認証技術等の導入における技術的課題について実証参加者よりいただいたご意見

②DNSSEC	
導入における技術的課題についての意見	● **基礎・技術** - **DNSSECの基本的な理解不足、情報不足**という課題・懸念が最も多い。 - 具体的には、**DNSSECの基本的な一連の設定（設定の準備～鍵の生成・署名～DS登録～ゾーンの編集）に関して確認したい**との意見が多い。 ● **運用・ノウハウ** - **運用に関するノウハウ、情報不足**という課題・懸念が多い。 - 具体的には、鍵交換・証明書など運用に関する意見が多い。 - また、他社の導入状況や導入に関する考え方について知りたい等の意見も有り。 ● **サービス提供・顧客視点** - DNSSEC導入によってDNSにアクセスができなくなった際の顧客の問い合わせ対応、**顧客環境での確認や顧客を安心させる材料等が欲しい**の意見も有り。

5.3. 促進に向けた検討

- 各種認証技術等の導入促進に向けた課題に対する解決策の検討

②DNSSEC	
実証事業を通じて見出された課題	● 運用に関する情報、ノウハウの要求に対する施策が必要 ＝**ガイドラインの整備**が必要 ● 鍵交換、不正応答等の具体的な実施（特に、**再署名と鍵更新の対応、不具合への対処**）に対する体験や知見取得の要求を満たす機会の創出が必要 ＝**実験環境の提供や実証作業・習得項目の創出**が必要
今後の認証技術普及の課題	● DNSSECを導入している企業・組織の取組みを評価していく施策が必要 ● DNSSECを導入している企業・組織のリスト化、公表・広報していく施策が必要
今年度の実証の課題と解決にむけた来年度の取組み	● 実運用で重要な「ロールオーバ」に関して、鍵の交換時期を通知するツールや、**鍵交換の自動化ツールなどオープンソース、サンプルコード**の紹介してほしいという意見もあった ● **SERV FAILの扱い**、不正なサイトを表示させることによるトラブル対応（顧客対応等）、**個社が判断、選択をするのが難しいため、共通認識や指標**を求める意見もあった ● DNSSEC導入による効果や**ドメインを守ることの重要性**に関する説明も重要であると有識者等の意見があった

5.4. 現状・課題・解決策と今後

- 現状・課題・解決策

	ネットワークセキュリティの技術（RPKI/DNSSEC/DMARC等送信メールドメイン認証）
現状	● **対策技術としては理解**されているが、導入に**踏み切るまでに至らず**普及していない。 ● 設定を誤ると、インターネットにおける到達性を含めて、サービスに不具合が起きる。**導入に敷居**がある。
課題	● 導入に踏み切る**根拠が必要**である。その機会を設ける。 ● **導入しても問題ないのか、不正を避けられるのか、不具合に対処できるのかに確証**を持つ。
解決策と今後	● **実際に実験して確証を得る。**（導入しても問題ない・不正を避けられる・不具合に対処できる） ● 今後、ガイドライン策定を含む活動により、基本的な理解と導入根拠が得られると考えられるが、普及への足掛かりであり**実質的普及には戦略的に取り組んでいく必要**がある。 ● ユーザが直面することになるフィッシング詐欺などの直接的な施策にあたらないが、**一つ一つの要素を押さえていく**ことがサイバー空間を支えるインターネットの分野において重要である。**要素の関係性と効果**などについて議論していきたい。

5.5. ガイドラインに必要な情報（検討中）

- 基本的な情報は、必要か？
- 設定・運用・トラブルシュートで参考になるTipsが必要
- 署名側（権威DNSサーバー）と署名検証側（フルリゾルバー）は読者が異なるので書き分けるべき

No	文献名	発行者	日付	URL
1	30分で学ぶDNSの基礎の基礎～DNSをこれから勉強する人のために～	JPRS	2014/09	https://2014/seccon/jp/dns/dns basics in 30minutes/pdf
2	初心者のためのDNS運用入門-トラブルとその解決のポイント-	JPRS	2013/07	https://dnsops/jp/event/20130719/20130719-dns-beginners-guide-mizuno-2/pdf
3	DNSSECの基礎概要	JPRS	2012/11	https://www.nic.ad.jp/ja/materials/iw/2012/proceedings/t9/t9-Funato.pdf
4	DNSSECの仕組みと現状	JPRS	2012/11	https://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-mechanisms-and-status.pdf
5	DNSSECとは	JPRS	2011	https://jprs.jp/dnssec/doc/dnssec.pdf
6	DNSSEC性能確認手順書 ver. 1.2	JPRS	2010/07	https://jprs.jp/dnssec/doc/DNSSEC-perf-co-proc-v1.2.pdf
7	DNSSEC技術実験報告書 運用設計編	JPRS	2010/12	https://jprs.jp/dnssec/doc/DNSSEC-testbed-report-odv1.0.pdf
8	DNSSEC技術実験報告書 機能・性能確認編	JPRS	2010/12	https://jprs.jp/dnssec/doc/DNSSEC-testbed-report-odv1.0.pdf
9	そこが知りたいDNSSEC	JPRS	2010/01	https://www.janog.gr.jp/meeting/janog25/doc/janog25-dnssec.pdf
10	使えます！OpenDNSSEC	JPRS	2010/07	https://jprs.jp/dnssec/doc/opendnssec.pdf
11	動かしてみましたDNSSECイントロ篇	JPRS	2010/07	https://www.janog.gr.jp/meeting/janog26/doc/post-dnssec-intro.pdf
12	動かしてみましたDNSSEC権威サーバー編	JPRS	2010/07	https://www.janog.gr.jp/meeting/janog26/doc/post-dnssec-min.pdf
13	Internet Week 2010 S10_DNSSECチュートリアル_実践編	JPRS	2010/11	https://www.nic.ad.jp/ja/materials/iw/2010/proceedings/s10/iw2010-s10-01.pdf
14	JPドメイン名におけるDNSSEC運用ステートメント（JP DPS）	JPRS	-	https://jprs.jp/doc/dnssec/jp-dps-jpn.v1.6.html
15	キャッシュDNS サーバDNSSEC導入ガイドライン	DNSSEC JAPAN	2011/01	https://dnssec.jp/wp-content/uploads/2011/03/20110207-techwg-DNSSEC-cacheserver-guideline.pdf
16	2011年度版リストガイド（DNSSEC）（cryptrec/go/jp）	独立行政法人 情報通信研究機構	2024/03	https://www/cryptrec/go/jp/report/cryptrec-tr-2001-2011/pdf
17	Secure Domain Name System (DNS) Development Guide NIST SP 800-81-2	NIST	2013/09	https://nvlpubs/nist/gov/nistpubs/SpecialPublications/NIST/SP/800-81-2/pdf
18	DNSSEC対応のために必要なこと	総務省	-	https://www.soumu.go.jp/main sosiki/joho tsusin/security previous/juyogijutsu/dnssec05.htm

参考情報1 ：実証参加者・有識者会議参画メンバー

実証実験参加者一覧

【①RPKI】実証実験参加者一覧

- KDDI
- QTnet
- NTT docomo
- J-layers, Inc.
- NCV NIKO NIKO CABLE TV
- 愛媛CATV
- ZTV
- GMO INTERNET GROUP
- CATV ケーブルテレビ株式会社
- BIGLOBE
- 中部テレコミュニケーション株式会社

【②DNSSEC】実証実験参加者一覧

- iprio イプリオ
- 山陰ケーブルビジョン株式会社 SUN-IN CABLE VISION Co., Ltd.
- J-layers, Inc.
- at-i Inc.
- NCV NIKO NIKO CABLE TV
- GLOBAL NET CORE
- GMO INTERNET GROUP
- 愛媛CATV
- JETINTERNET Network Solution & Internet Service Provider
- CATV ケーブルテレビ株式会社
- Foresight Wave INC.

【③DMARC】実証実験参加者一覧

- iprio イプリオ
- 山陰ケーブルビジョン株式会社 SUN-IN CABLE VISION Co., Ltd.
- J-layers, Inc.
- at-i Inc.
- NCV NIKO NIKO CABLE TV
- ANA
- ZTV
- GMO INTERNET GROUP
- DOVA CORPORATION
- Foresight Wave INC.

有識者会議参画メンバー

- 各種認証技術における有識者会議参画メンバー一覧

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
2	渡辺 英一郎	NTTコミュニケーションズ株式会社
3	中村 修	慶應義塾大学　環境情報学部　教授
4	豊田 安信	慶應義塾大学／WIDEプロジェクト
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 大学院情報化研究科 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	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

❷ DNSSEC｜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	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

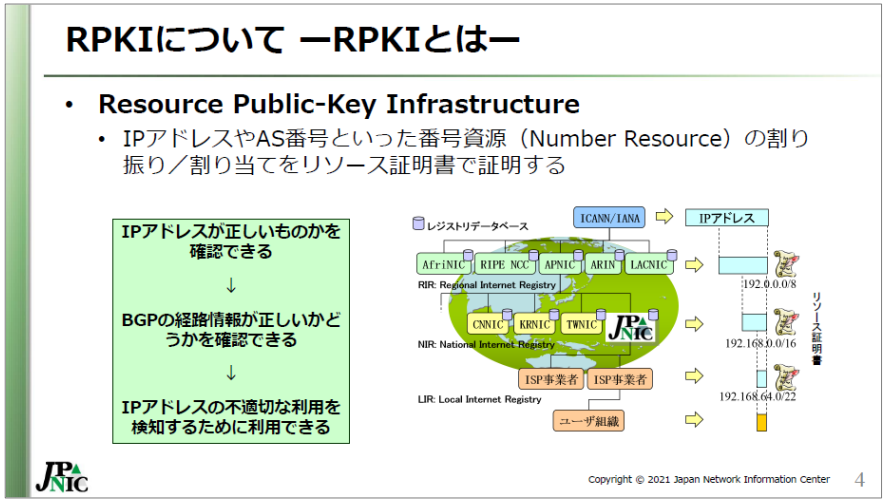
❸ DMARC｜有識者会議参画メンバー

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

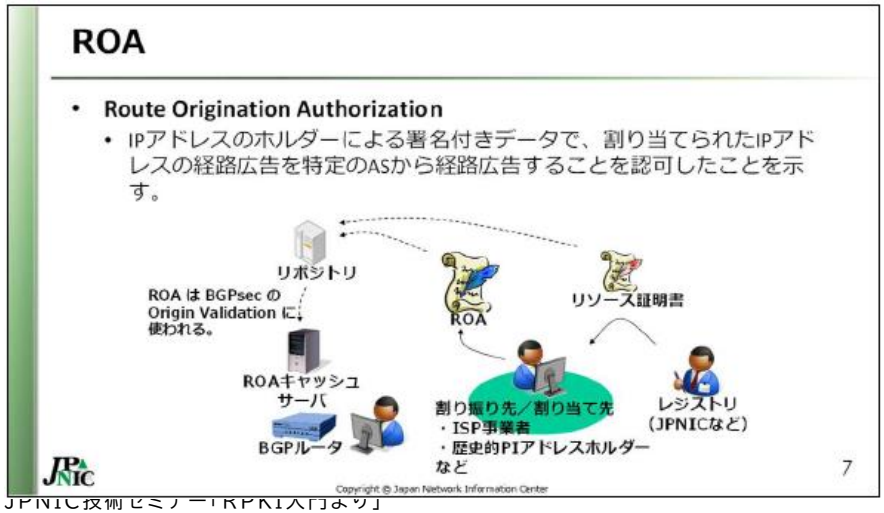
参考情報2：RPKI / DMARCの実施概要

【RPKI】認証技術の概要

- 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

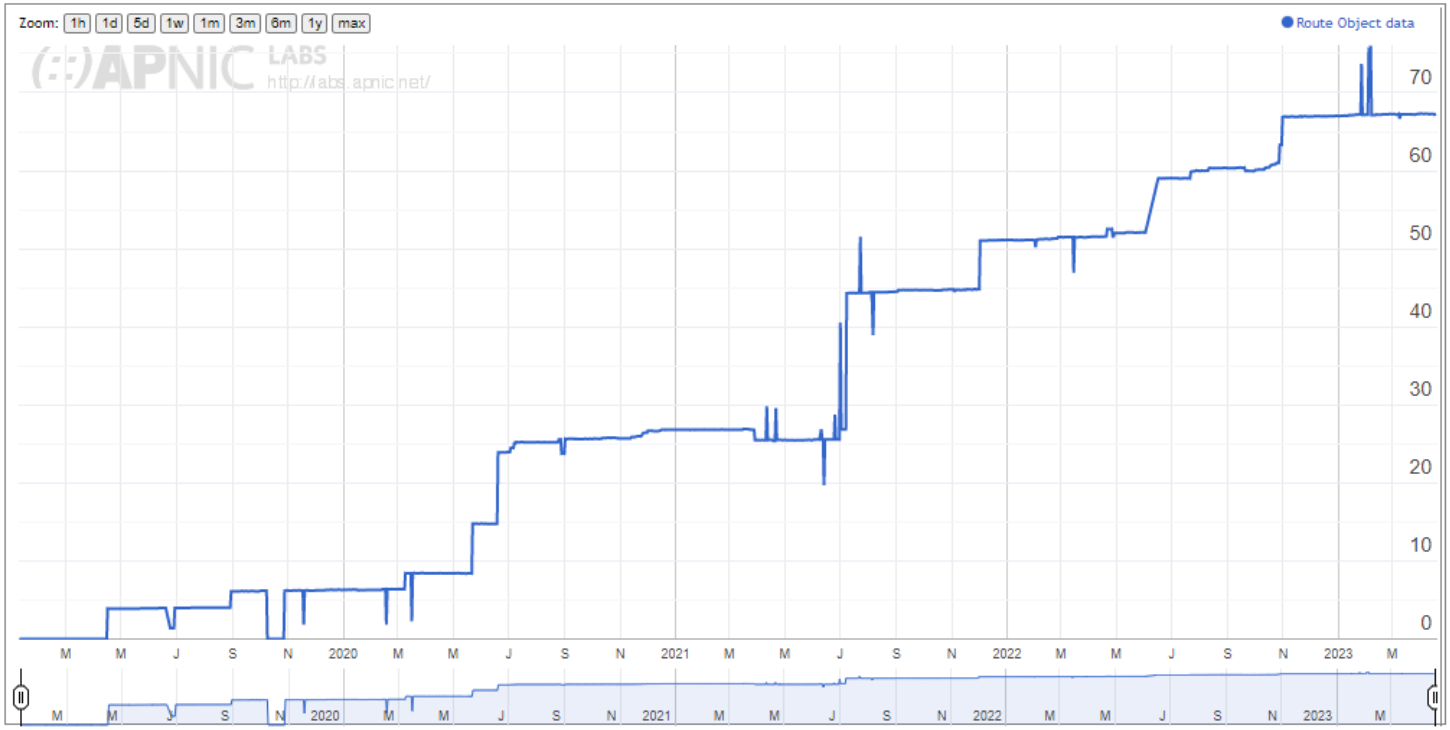


JPNIC技術セミナー「RPKI入門」より
https://www.nic.ad.jp/ja/tech/seminar/

*1 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 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のこと。

【RPKI】認証技術の普及状況

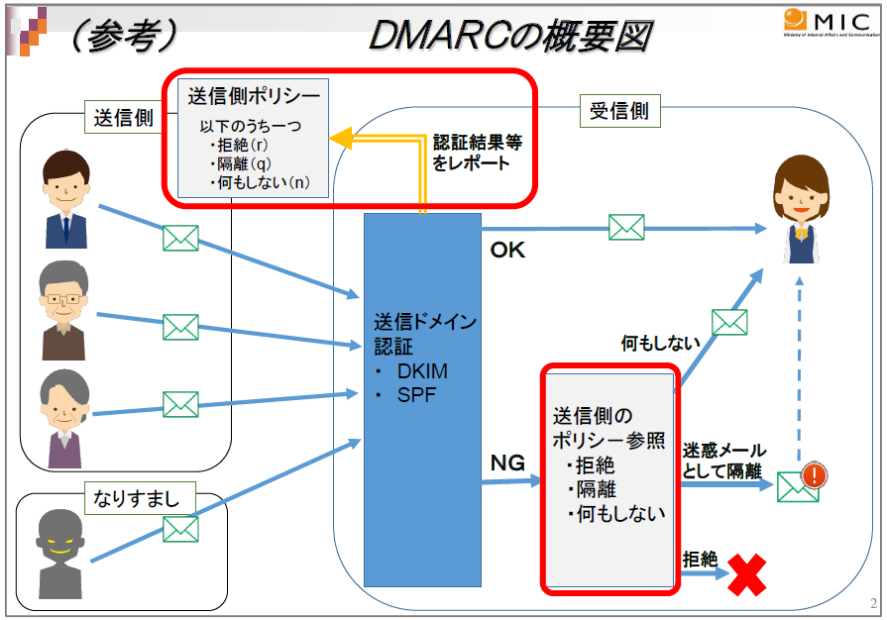
- 国内のIPv4アドレスを使ったBGP経路全体のうち、ROAによってカバーされていてAPNIC観測点においてValidであるものは**増加傾向にあり約67%**に達している。**日本国内においてはROVの導入例は少ない**ため不正経路の影響を小さくするために国内ISP等におけるROVの導入が課題である。



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

【DMARC】認証技術の概要

- 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）や電子署名（DKIM）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。

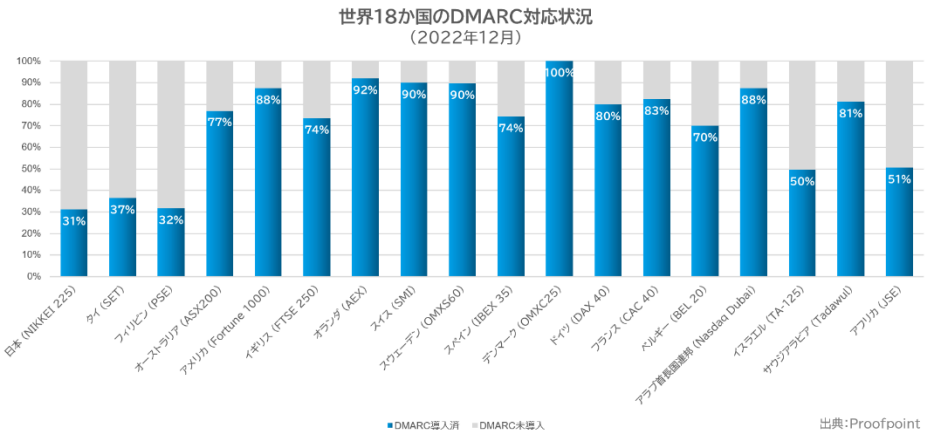


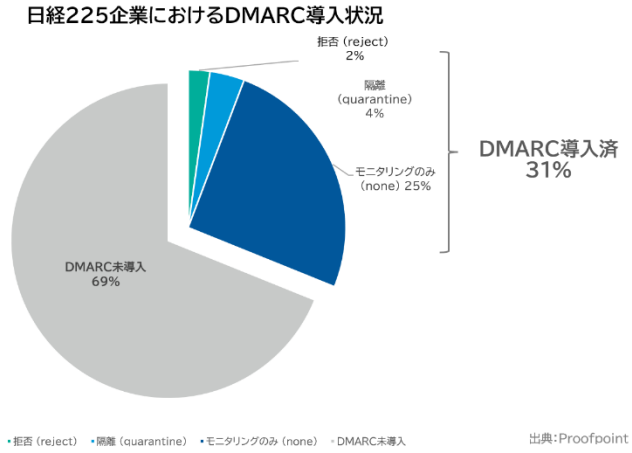
DMARC導入に関する法的な留意点
https://www.soumu.go.jp/main_content/000495390.pdf

本事業の「DMARC体験コース」より

【DMARC】認証技術の普及状況

- 2023年1月25日のプルーフポイントの調査によると、アメリカはFortune 1000企業のうち88%、オーストラリアはASX200企業のうち77%、デンマークはOMXC25企業の100%がDMARCを導入しているが、**日経255企業のDMARC対応率は31%**にとどまっている。
- さらに、DMARCポリシーを**reject（拒絶する）またはquarantine（隔離する）としている企業は併せて6%**にとどまっており、世界の主要企業に比べ、大幅に遅れている。
- DMARCに関連する技術であるSPF、DKIMについては、SPF普及率は87.9%、DKIM普及率は48.3%[*3]となっている。
- 令和5年2月1日に、総務省・経済産業省・警察庁から、クレジットカード会社等に対してDMARCの導入を始めとする**フィッシング対策強化を要請**している[*4] 。





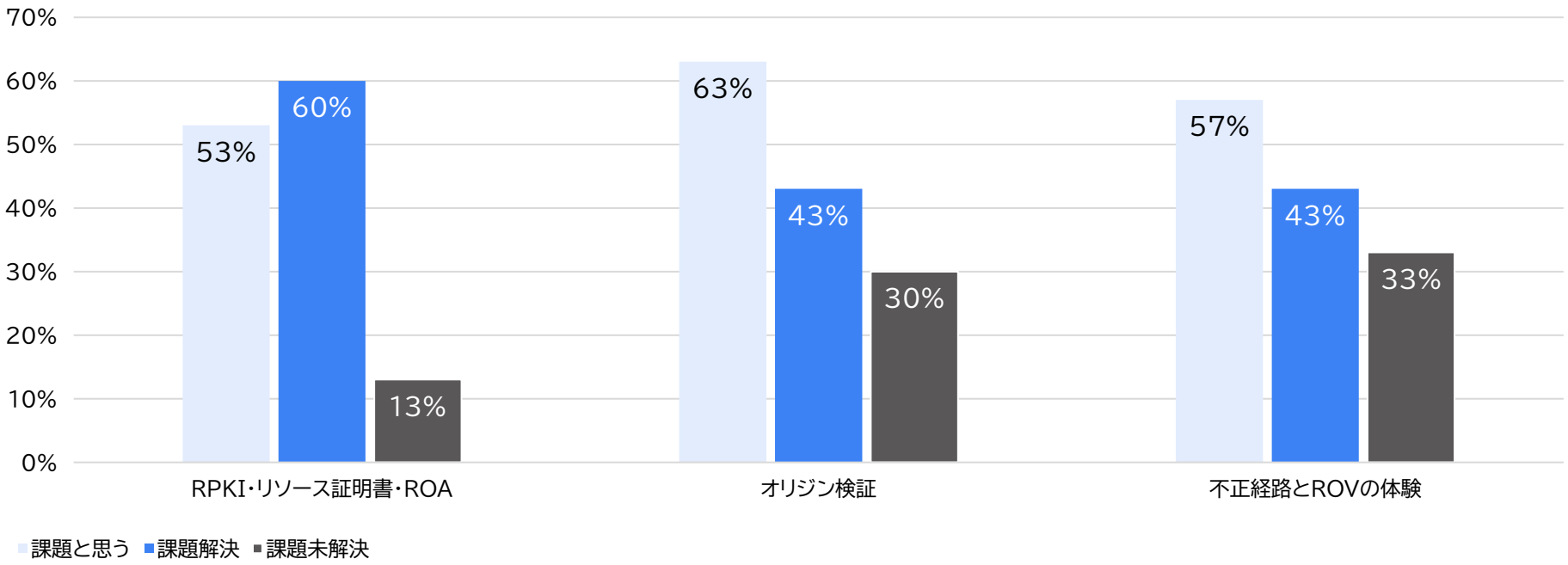
プルーフポイントの調査 2023年1月25日 https://www.proofpoint.com/jp/newsroom/press-releases/nikkei225-dmarc-implementation-rathio-2023

*3 IIJ IIR vol.47 https://www.iij.ad.jp/dev/report/iir/047/01.html （2020年4月時点 IIJの受信メールに対する割合）

*4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

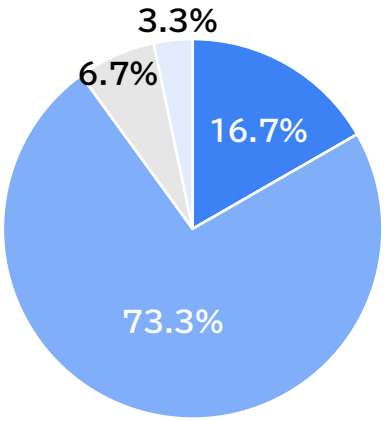
RPKI体験コースの結果

- 体験コースの主な内容である「RPKI・リソース証明書・ROA」、「オリジン検証」、「不正経路とROVの体験」は**各々53%～63%とそれぞれ課題認識が高い**。
- 体験コースの受講によって課題解消できた内容は、「RPKI・リソース証明書・ROA」は60%であり、**基礎的な内容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という回答は、「不正経路とROVの体験」が33%と高く、**他の実験コースなどの参加を推奨する必要**がある。



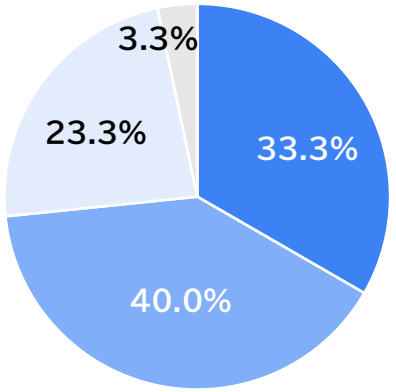
RPKI体験コースの結果

- 体験コースの受講の感想では、「RPKIに技術について**基礎的な知識が身につけられた」が73.3%**であり、基礎的な知識を習得するために有効である。
- また、「RPKI技術導入の検討に大いに役立った」が16.7%であり、上記とあわせて90%である。



- RPKI技術導入の検討に大いに役立った
- RPKI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、RPKI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RPKIの導入については、「導入を積極的に考えたい」33.3%、「導入に至るかわからないが前向きに考えたい」40%であった。
- 「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」が23.3%であり、「導入を積極的に考えたい」、「導入に至るかわからないが、**前向きに考えたい」とあわせると90%以上**と高く、**実体験はRPKI普及の効果が見込める。**



- 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

【RPKI】技術的課題の調査

- 各種認証技術等の導入における技術的課題について実証参加者よりいただいたご意見

①RPKI	
導入における技術的課題についての意見	● **基礎・技術** - **RPKI/ROA/ROVに関する基礎知識の不足、正常運用ができるのか不明**という課題・懸念が多い。 - **関連ソフトウェア・ハードウェア**（ROAキャッシュサーバ、各社ルータ、ROVサーバ、及び搭載するオープンソースソフトウェア）**の動作の詳細**が把握できていない、不正な経路から守られているのかがみえない等の課題・懸念も有り。 - **ROAキャッシュサーバの利用時の設定や設定内容の確認方法**等の課題・懸念も有り。 ● **運用・ノウハウ** - **ROAキャッシュサーバとの接続状況の変化**や**Invalid経路の分析など運用を見越した内容を確認したい**という意見も多い。 ● **サービス提供・顧客視点** - RPKIを導入することでサーバにアクセスできなくなった際の顧客の問い合わせ対応、**顧客環境での確認、顧客を安心させる材料などの課題**等の課題・懸念も多い。 - 導入に不安を感じる点として、**もし顧客への経路がInvalidになってしまった場合の対処方法**等に不安を持つという意見も有り。

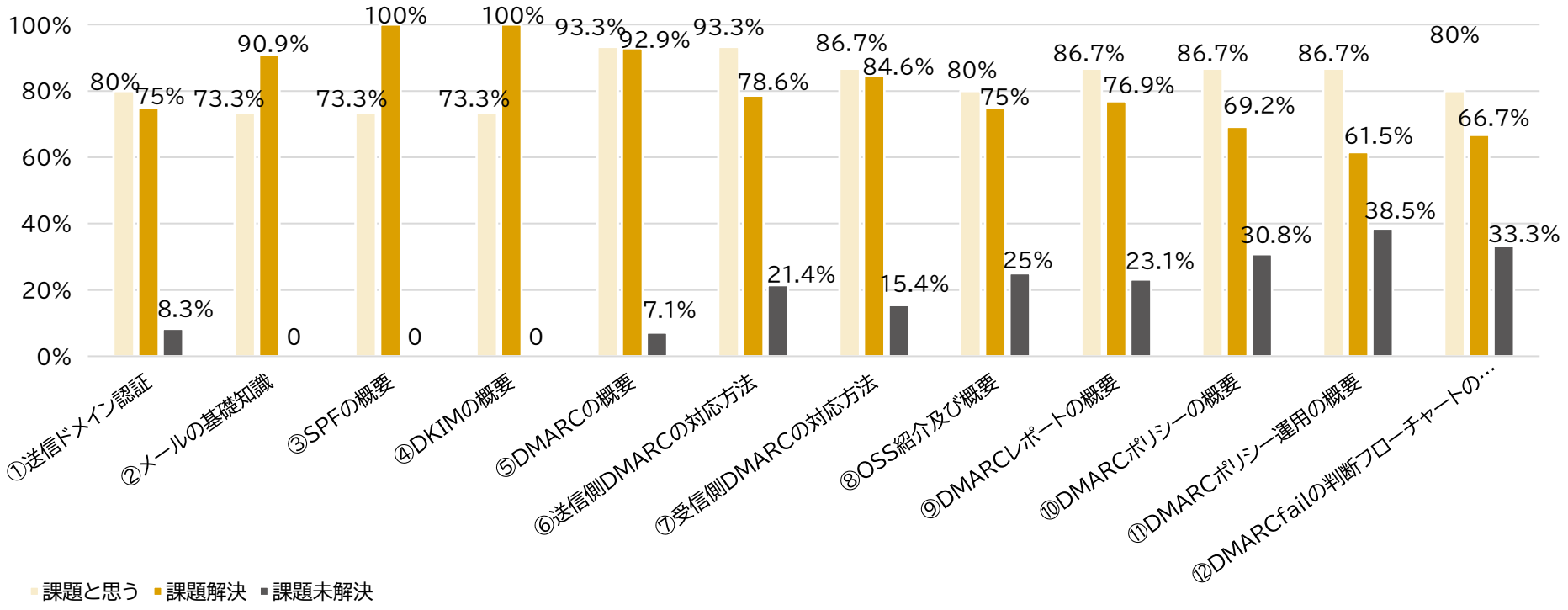
【RPKI】促進に向けた検討

- 各種認証技術等の導入促進に向けた課題に対する解決策の検討

①RPKI	
実証事業を通じて見出された課題	● 安全な設置・設定ができるガイドの要求に対する施策が必要 ＝**ガイドラインの整備**が必要 ● 不正経路の検出・対策、ROV設定・構築・運用に対する体験や知見取得の要求を満たす機会創出が必要 ＝**実験環境の提供や実証作業・習得項目**の創出が必要
今後の認証技術普及の課題	● RPKIを導入している企業・組織の**取組みを評価**していく施策が必要 ● RPKIを導入している企業・組織のリスト化、公表・広報していく施策が必要
今年度の実証の課題と解決にむけた来年度の取組み	● RPKI導入組織が各々で検証するのではなく、**パブリックなROAキャッシュサーバで検証する**要求が多いため、構築や実現に向けた検討・課題整理が必要 ● **安全に設置・設定するための**ガイドラインや手順書が求められている ● インターネット上の経路セキュリティの観点では、不正経路はドロップすることが望ましいが、invalid経路をドロップすると個社が選択をするのが難しいため、**共通認識や指標**を求められている

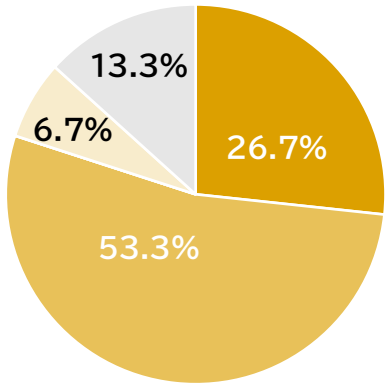
DMARC体験コースの結果

- 体験コースの主な内容であった12項目については、**各々73.3%～93.3%と課題認識が高い**。
- 体験コースの受講によって課題解消できた内容は、「SPFの概要」と「DKIMの概要」は100%、「メールの基礎知識」と「DMARCの概要」は90%超であり、**基礎的な内容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という回答は、**「DMARCポリシー運用の概要」が38.5%と最も高く**、他の**実験コース等の参加を推奨する必要**がある。



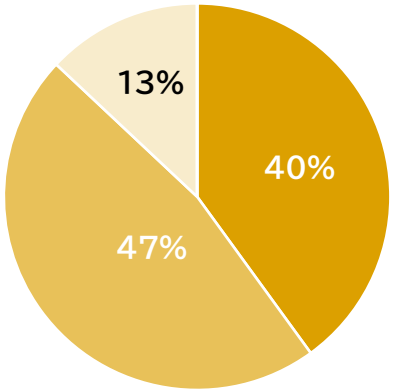
DMARC体験コースの結果

- 体験コースの受講の感想では、「DMARCに技術について基礎的な知識が身につけられた」が**53.3%**であり、基礎的な知識を習得するために有効である。
- また、「DMARC技術導入の検討に大いに役立った」が26.7%で、この2つの回答で**80%**を占める。



- DMARC技術導入の検討に大いに役立った
- DMARC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、DMARC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DMARCの導入については、「導入を積極的に考えたい」、「導入に至るか分からないが、前向きに考えたい」が合計で**87%**を占めた。
- 「導入を検討するかどうかわからないが情報は積極的に得たい」が13%であり、「導入を積極的に考えたい」、「導入に至るか分からないが、前向きに考えたい」とあわせると**100%**となり、**DMARC普及の効果が見込める。**



- 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

【DMARC】技術的課題の調査

- 各種認証技術等の導入における技術的課題について実証参加者よりいただいたご意見

③DMARC	
導入における技術的課題についての意見	● **基礎・技術** - **DMARCレコードの設定と受信メールサーバ側・レポート受信の挙動を確認**等の課題・懸念が最も多い。 ● **運用・ノウハウ** - **サブドメインが多く運用・管理が大変**という意見が多い。 - **DMARCレポートの記載情報の確認、DMARCレポートの集計・可視化、DMARCレポート分析を元にした原因の切り分けの方法**等の課題・懸念が多い。 ● **サービス提供・顧客視点** - DMARC導入で**正当なメールが届かなくなる**等の課題・懸念が多い。 - DMARC導入で**正当なメールが届かなくなる懸念を抱く顧客への対応、顧客環境での確認、顧客を安心させるための材料が欲しい**といったISP事業者ならではの意見も有り。

【DMARC】促進に向けた検討

- 各種認証技術等の導入促進に向けた課題に対する解決策の検討

③DMARC	
実証事業を通じて見出された課題	● **偽陽性（メーリングリスト・転送メールなど正規のメールが届かなくなる）への対応策・対処方法**の要求に対する施策が必要 ＝ガイドラインの整備が必要 ● **DMARCポリシーの設定、DMARCレポートの分析**等の知見取得を要求を満たす機会創出が必要 ＝実験環境の提供や実証作業・習得項目の創出が必要
今後の認証技術普及の課題	● DMARCを導入している企業・組織の取組みを評価していく施策が必要 ● DMARCを導入している企業・組織のリスト化、公表・広報していく施策が必要
今年度の実証の課題と解決にむけた 来年度の取組み	● DMARCポリシーの決定方法、判断方法、**どの段階でポリシーを高めるべきなのか**、その**指針**のようなものがガイドラインで示してほしいという意見があった ● 最も多い懸念である**偽陽性への対策、有効な設定等**をガイドラインや手順書において示してもらいたいとの意見があった