インターネットを支える力について考える

～セキュリティ技術の普及 - RPKI/DNSSEC/DMARC を題材に ～

三菱総合研究所

先進技術・セキュリティ事業本部
小川 博久

2023/11/15

Agenda

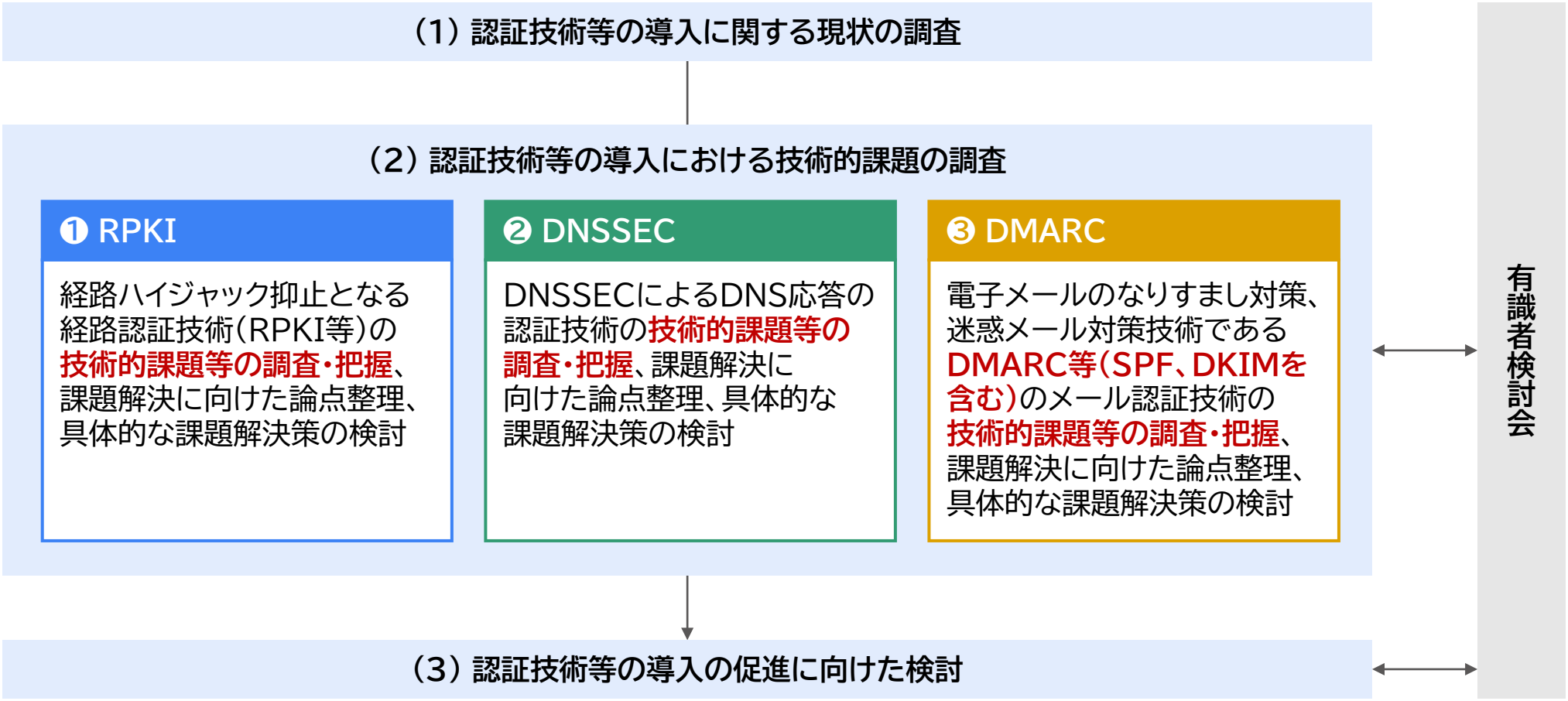
1. 事業の目的
2. 事業の概要
4. 技術的課題の調査と促進に向けた検討
5. 現状・課題・解決策と今後

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



2. 事業の概要（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

2. 事業の概要（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

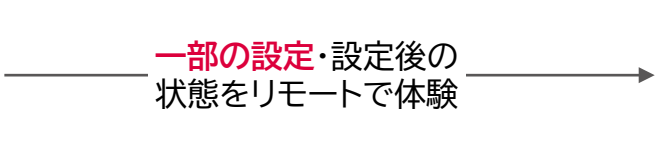
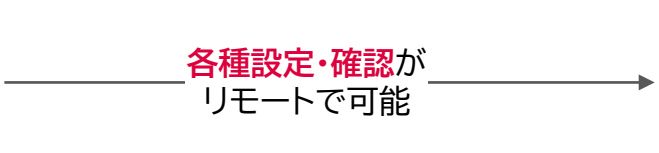
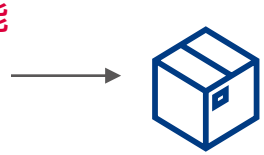
- iprio イプリオ
- 山陰ケーブルビジョン株式会社 SUN-IN CABLE VISION Co., Ltd.
- J-layers, Inc.
- at-i Inc.
- NCV NIKO NIKO CABLE TV
- GLOBAL NET CORE
- GMO INTERNET GROUP
- 愛媛CATV
- JETINTERNET Network Solution & Internet Service Provider
- CATV ケーブルテレビ株式会社
- FRESIGHT WAVE INC.

【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
- FRESIGHT WAVE INC.

2. 事業の概要（実証環境の整備：ご協力いただいた大学）

- 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。

体験コース		**一部の設定**・設定後の状態をリモートで体験 	 拠点内に正規サーバと偽サーバ等を設定
実験コース	 **設定情報等を提供** 	**各種設定・確認**がリモートで可能 	 実環境で利用する**代表的な機材を用意**
導入検証コース		実証環境の**利用も可能** 不正な応答等を検出できるかを確認することも可能 	 一部の実証では**機器の持込みも可能**

2. 事業の概要（体験コースマテリアル）

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

2. 事業の概要（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

4.【①RPKI】技術的課題と促進検討

- 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	
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** - **関連ソフトウェア・ハードウェア**（各社ルータ、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** ● **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経路の分析を見越した運用** ● **サービス提供・顧客視点** - **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**
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

4.【②DNSSEC】技術的課題と促進検討

- 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	
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 - 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）を確認したい** ● **運用・ノウハウ** - **運用に関するノウハウ、情報不足（鍵交換・証明書など）** - 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 ● **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
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

4.【③DMARC】技術的課題と促進検討

- 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	
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 ● 運用・ノウハウ - 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 - DMARCポリシーの設定、DMARCレポートの分析等の知見取得 ● 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
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

5. 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こと/議論・情報共有する場。** （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。