{RPKI/DNSSEC/DMARC}の
ガイドラインには何が必要なのか？

三菱総合研究所

デジタル・イノベーション本部

2024/01/18

1. {RPKI/DNSSEC/DMARC}のガイドラインには何が必要なのか？

- **発表概要（日本語）**
  - 枯れた技術であるRPKI、DNSSEC、DMARCについては、現時点でも導入・運用の課題が議論され、JANOGでも毎回テーマに挙がり、議論されています。
  - このような状況を受け、総務省では、「総務省 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」を実施しています。（昨年度の関連＊1）
  - 今年度は、実証事業から得られた導入や運用で足りない情報を提供するガイドラインや手引きを作成します。
  - このセッションでは実証実験から得られた意見と有識者検討会の議論を情報共有し、作成等のガイドライン・手引きについて有識者・実証者・会場参加者でディスカッションします。

- **発表者情報（氏名・所属・連絡先メールアドレス）**
  - 小川 博久（株式会社三菱総合研究所）
  - 小俣 裕一（GMOインターネットグループ株式会社）
  - 末政 延浩（株式会社TwoFive/JPAAWG）
  - 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）
  - 高田 美紀（NTTコミュニケーションズ株式会社）

＊1:RPKIのROVを試してみた件 - JANOG52 Meeting in Nagasaki　https://www.janog.gr.jp/meeting/janog52/rov/

2. タイムテーブル

- **12分　本議論のスコープと総務省事業の説明**
  - 2分　導入・運用の課題 （RPKI/DNSSEC/DMARC）
  - 5分　ガイドラインの骨子案 （RPKI/DNSSEC/DMARC）
  - 5分　有識者の議論/実証事業者の意見 （RPKI/DNSSEC/DMARC）

- **30分　ガイドラインに関するディスカッション**
  - （10分x3技術）　　RPKI/DNSSEC/DMARCに関する意見 （有識者・実証者・会場参加者から）

  - 基本的な情報は既にあるが、何が足りない/必要なのか？
    - **導入しても問題ないですか？不正から守れるか？**
  - 運用や対処方法を説明すべきか？
    - **対処できることを実証でやった**（外部サービスもある）

- **30分　共通認識・指針に関するディスカッション**
  - （10分x3技術）　　RPKI/DNSSEC/DMARCに関する意見 （有識者・実証者・会場参加者から）

  - **RPKI：InvaildなBGP経路はドロップしましょう？**
  - **DNSSEC：SERV FAILの対処は？**
  - **DMARC：p=???は、どこまでやるべきか？**

- **3分　まとめ**

総務省事業の説明

- **4分 導入・運用の課題 （RPKI/DNSSEC/DMARC）**
- 4分 ガイドラインの骨子案 （RPKI/DNSSEC/DMARC）
- 4分 有識者の議論/実証事業者の意見 （RPKI/DNSSEC/DMARC）

1. 事業の概要（実証コース/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。

- RPKI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**

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（実証実験参加者一覧）

【①RPKI】実証実験参加者一覧

- KDDI
- QTnet
- NTT docomo
- JPNIC
- NCV
- 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
- 山陰ケーブルビジョン株式会社
- JPNIC
- at-i inc.
- NCV
- GLOBAL NET CORE
- GMO INTERNET GROUP
- 愛媛CATV
- JETINTERNET
- CATV ケーブルテレビ株式会社
- FRESIGHT WAVE

【③DMARC】実証実験参加者一覧

- iprio
- 山陰ケーブルビジョン株式会社
- JPNIC
- at-i inc.
- NCV
- ANA
- ZTV
- GMO INTERNET GROUP
- DOVA CORPORATION
- FRESIGHT WAVE

3.【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

3.【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

3.【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

参考. R5年度　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	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	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
6	石田 慶樹	日本DNSオペレーターズグループ　代表理事
7	米谷 嘉朗	日本DNSオペレーターズグループ
8	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	加瀬 正樹	JPAAWG/株式会社TwoFive
7	中村 成陽	LINEヤフー株式会社

参考. R4年度　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システムを介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

総務省事業の説明

- 4分 導入・運用の課題 （RPKI/DNSSEC/DMARC）
- 4分 ガイドラインの骨子案 （RPKI/DNSSEC/DMARC）
- 4分 有識者の議論/実証事業者の意見 （RPKI/DNSSEC/DMARC）

RPKI ガイドライン骨子案

1. ガイドラインの趣旨
1.1 本ガイドラインについて
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 推奨される実施事項

2. 技術的情報
2.1 ROA/IPアドレスの割り当てを受けた者の実施事項
2.1.1. 不正経路とIPアドレスに関する考え方
2.1.2. ROAとは
2.1.3. ROAの作成と運用管理
2.1.4. ROAの作成に関わる実施対象者
2.1.5. 例外的な処置
2.2. ROVの実施について
2.2.1. ROV/AS運用をされている者の実施事項
2.2.2. 不正経路への対策と考え方とROV
2.2.3. ROVの導入と運用方針
2.2.3.1. コストの注意
2.2.3.2. ROAキャッシュサーバ・ROVの所在
2.2.2.5. ルータ側のROV設定
2.2.2.6. ROVによる経路制御
2.2.2.7. ROVの設定
2.2.2.8. 運用上の注意と懸念点

3. RPKI以外の不正経路対策
3.1. BGPにおけるセキュリティの要素と考え方
3.2. ASパス検証の今後と運用について

4. 付録:

実証事業者からガイドライン案に求める情報　1／2

- **RPKI/ROA/ROVの仕組み**

導入は前向きに検討をしているものの、仮にROV実装の認定制度のようなものが設けられた場合は、導入の遅れにより不利益が生じてしまうことが危惧される。
また、完全に外部からの不正経路をDropさせるためには、全外部接続ルータへのROV適用が必要となるが、現実的にはかなり時間を要することが予想されるため、どの範囲まで適用できれば「ROVを実装している」と言えるのかの指標があれば、一つの目標値になると感じている。

- **脅威**

被害事例があると説得しやすいので被害事例が欲しい。

- **望ましい構成／パラメーター**

自社に合った構成を見極められるガイドラインが欲しい。

- **動作確認**

設定内容確認や監視をするためのツールの一覧などが欲しい。
正常に動作しているか確認するための安心確認方法が知りたい。

実証事業者からガイドライン案に求める情報　2／2

- **経路の監視方法を検討・導入**

メジャーな監視ツールによる監視方法について示して欲しい。

- **運用体制**

コストを算出できる構成案や、最低限必要な監視体制案が欲しい。

- **Invalid経路の扱い方**

　通信事業者としてお客様のトラフィックを疎通させる義務のある当社では、安易にInvalid経路をDropするという選択をするのが非常に難しい。一方で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Dropするのが目指すべき姿であるとの認識もあり、Invalid経路の取り扱いについて決めかねている。
　上述の理由から、ガイドライン上で推奨する動作を記載いただけると大いに参考になる。例えば「ROAはIPアドレスホルダーが正しく登録すべきものであり、InvalidをDropすることを推奨する」といったガイドラインがあれば、導入に向けた大きな助力となる。

　Invalidの内容を正しい判定か確認できる手順が欲しい。

DNSSEC ガイドライン骨子案

- **ガイドライン案の骨子案（目次案）**

1. 経営者

1. ドメイン名の役割
2. インターネット上でのサービスを提供し続けるためには名前解決が重要
3. インターネットのサービスを守る　→　ドメインを守る
4. ドメインを守るために
    1. リスク、損失などを簡潔に記述

2. リカーシブリゾルバ関係者（ISPなど）

1. 個々のリカーシブリゾルバのDNSSEC検証の有効化に関する技術的な記述
2. トラブルシュートを記述
3. 定常常務として必要な項目及び注意点など

3. 権威DNSサーバ関係者（DNSプロバイダ、ホスティング事業者など）

1. 個々の権威DNSサーバにおけるDNSSEC署名の追加に関する技術的な記述

4. ドメイン名登録・登録管理関係者（レジストラ、レジストリ、リセラー、ドメイン名登録者）

1. 鍵情報の取次、登録の実施など

ガイドライン案に求める情報　1／3

● DNSSECの仕組み

- 基本的な構造が分かりやすく載っていれば大丈夫かと思います。
- DoT / DoH と DNSSEC の違い
- 知識がない人でもDNSSECについて理解できるくらい詳しく記載してほしいと思います。

● 脅威

- 実際にあった事件、DNSSECが導入されていたことで防ぐことができた事例などがあると導入を前向きに検討できるかと思います。

● 望ましい構成／パラメーター

- 現在運用中の環境に新たに導入するケースが多いかと思われますので、追加する上で必要になる要件、現環境と衝突する可能性があるポイントなどあると導入の助けになるかと思います。
- 実際の構築例
  - ZSK / KSK の推奨される鍵長
  - ZSK / KSK 作成時に使用することを推奨される、または推奨されない暗号アルゴリズム
  - DNS Amp 攻撃など 悪用を防ぐもしくは悪用の効果を低減する設定例・対処法など（レートリミット、平時のクエリ傾向をつかんでおく、他）
- DNSSECといえばコレといった構成があるとありがたいです。そうすることで新たにDNSSECを導入する際やトラブルがあった際に事業者間で情報を共有しやすいと思います。

ガイドライン案に求める情報　2／3

● 動作確認

- 確認するポイントと実行例があり、OKであるとき、NGであるときそれぞれの結果があると分かりやすいかと思う
- 設定内容を確認するためのツールの一覧など
- 正常に動作しているか確認するためのサイトやその使い方などが記載されているとありがたい

● SERVFAILの扱いを検討

- 導入により可用性が低下することは避けたいので、可用性を維持しつつ完全性を担保する運用ノウハウが書かれていると良い
- SERVFAIL を検知した時の対処方法の例

● 監視方法を検討・導入

- 攻撃によるSERV FAILなのか運用ミスによるものなのかを識別する方法や、運用ミスの場合の取り扱いについて書かれていると良い
- 何を監視し、どんな情報を収集するべきかを前提として共有し、できれば導入ハードルの低い監視環境構築例とそれによるデータ収集例が載せられると、DNSSECそのものの敷居も低くなると思う
- どのデータを監視すべきか、どのような状態を管理者に通知すべきか
- 署名側では意図せずSERVFAILになった際にすぐに気づけるように監視が必要なため、どのような監視をするべきか参考が記載されていると良い（具体例があるとなお良い）

ガイドライン案に求める情報　3／3

● 運用体制

- 問題が起きにくいキーロールオーバーの方法が書かれていると良い
- 工程の全てをコマンド操作するような人力でのオペレーションは推奨しない、逆に可能な限り省力化すべきという方向の周知を盛り込むのが良い
- 鍵ロールオーバーの期間のデファクトスタンダード、鍵ロールオーバー時にDNSキャッシュ（TTL）で気を付けるべき事項
- DS登録などをほかの事業者に依頼していてDNSSECを1事業者では完結できない事業者もいるため、安定して運用するために望ましい運用体制を示してもらえるとありがたい
- 基本的に人の手による作業はミスが発生しうるので出来るだけ自動化するように記載したほうが良い
- 参考となる自動化ツールなども記載してあると良い

● 各種実験結果のデータ

- 負荷状況の例としてクエリ数別に大中小各種ドメインの数値があると参考になりそうかと思う

● その他

- 法的な留意点、DNS クエリログを分析するにあたって、通信の秘密などの観点から見た法的解釈（違法性が阻却されるとする解釈などの例）
- より詳細な情報を求める場合の参照先
- 関連する RFC やその翻訳物の一覧など

DMARC ガイドライン案の検討状況　骨子案

- **ガイドライン案の骨子案（目次案）**

1. はじめに

1. 目的、対象などを簡潔に記述

2. ガイドライン

1. ドメイン管理者（メール送信者）向け内容
    1. SPF、DKIMの導入
    2. DMARCの組織ドメインへの設定
    3. 利用しないドメイン名に対する設定
    4. DMARCレポートの活用
2. 再配送（中間業者）向け内容
    1. メール転送時の処理方法
    2. メーリングリストの設定
3. メール受信者向けの内容
    1. SPF、DKIM、DMARC認証
    2. 認証ドメイン名を利用した受取判断（ドメインレピュテーション）
    3. 可能であれば、フィードバックグループの仕組みの導入
    4. 可能であれば、WebmailとしてBIMI（brand mark）の表示による認証されたメール認識向上

ガイドライン案に求める情報　1／5

● DMARCの仕組み

- なぜ DMARC が必要なのか（DMARC 導入の動機付けとなるような情報）（ISP）
- DMARC を導入することで防ぐことができたと考えられる被害例等 （ISP）
- SPF/DKIMとの関係性 （ISP）
- 重要なタグに関する情報 （ISP）
- 仕組み上、正規となりすましのメールを100%区別できるわけではない点、およびSPFとDKIMのそれぞれ得意とする領域がわかりやすく書かれているとよい （ISP）
- Webの説明サイトではSPF/DKIM認証でのチェックとあるが、それ以外にも実はヘッダーFromドメインとエンペロープFromドメインの一致もチェックしていることを記述願いたい （金融機関）
- 基本的な事項について素人でもわかるような記述・補足がほしい。文字にこだわらず、絵、図、イラスト、マンガ等を活用してもよい （金融機関）

● 脅威

- DMARC でどのような攻撃を防げるのか （ISP）
- 導入にあたり顧客を納得させる材料としてどんな脅威に対抗できるかの記載が欲しい （ISP）
- こちらで用意した資料よりもガイドライン記載のものがあれば説得力が増す （ISP）

ガイドライン案に求める情報　2／5

● 望ましい構成

- レポートについて、単純なxmlファイルでは人間では解析できないので、推奨する分析ツールの記載はあった方が良い（**金融機関**）
- DMARC レポートを分析/可視化するための実装の例（**ISP**）
- 受信したメールの正当性を検証するための DMARC の実装の例（**ISP**）
- 送信側、受信側それぞれに必要なツール・設定を簡単にまとめた資料（**ISP**）

● DMARCレコードの設定

- いくつか設定できるパラメータがあるため、推奨する設定を明確に記載してあると良い（**金融機関**）
- DMARC レコードの例（**ISP**）
- 注意すべき事項（**ISP**）
- サブドメインを考慮した設定内容が書かれているとよい（ISP）
- 基本的な事項(タグの説明、最低限定義の必要なタグの明示)（**金融機関**）
- 注意を要するタグの設定内容(事例を含めて)（**金融機関**）

● 検証環境で検証結果を観測

- 検証環境の構成例（**ISP**）
- 検証結果の観測方法（重要視すべき点など）　（**ISP**）
- 検証する上でのチェックポイントが明記されているとよい　（**ISP**）

ガイドライン案に求める情報　3／5

● DMARCレポートの確認

- レポート内容から判断できること、対応すべき事項の記載があると良い（**金融機関**）
- レポートの受け取り方（**ISP**）
- RUA などの宛先とするメールアドレスの運用例（**ISP**）
- 具体的な確認内容（事例を含めて）（**金融機関**）

● DMARCレポート分析

- レポート内容から判断できること、対応すべき事項の記載があると良い（**金融機関**）
- 代表的なツールの紹介、基本的な使い方（**ISP**）
- 着目する箇所と、結果を踏まえた改善手法の提示があるとよい（**ISP**）
- DMARCレポートで見るべきポイントを記載願いたい（**金融機関**）
- 具体的な分析方法（事例を含めて）（**金融機関**）

● 偽陽性への最良な設定方法

- 判定基準の変更方法（**ISP**）
- DKIM/ARCの利用対応が進んでいないため、MLを通したメールのスパム判定率が高かったので、DMARCの範疇ではないが、このあたりを如何に対処するかノウハウがあれば教えて欲しい（**ISP**）
- 設定方法の例示がされているとよい（**ISP**）
- 具体的な設定内容（事例を含めて）（**金融機関**）

ガイドライン案に求める情報　4／5

● 運用体制

- どのような人材が必要か（**ISP**）
- どのような役割が必要か（**ISP**）
- 監視方法(何を監視すべきか、どのように監視すべきか）（**ISP**）

● DMARCポリシーの決定

- noneからの開始となると思うが、ポリシーの強度を変える際の目安や推奨等があると良い（**金融機関**）
- ポリシーを決定するまでの考え方/検討方法/検討フロー（**ISP**）
- 一般的に推奨される手順の明示（**金融機関**）
  （ex. ①SPFの設定→②DKIMの設定→③noneでのDMARC設定→④DMARCレポート分析→⑤偽陽性解消のための対応→・・・）

● DMARCポリシーの設定変更

- 利用できるツールの紹介/使い方（ISP）
- 設定変更に当たり DNS のキャッシュに関連して注意すべき点があるか（**ISP**）
- 設定変更による失敗例（**ISP**）
- DMARCレポートで見るべきポイントを記載願いたい（**金融機関**）
  ①偽陽性の具体的な解決方法
  ②ポリシー強化のタイミングやポリシー変更時の具体的な注意事項

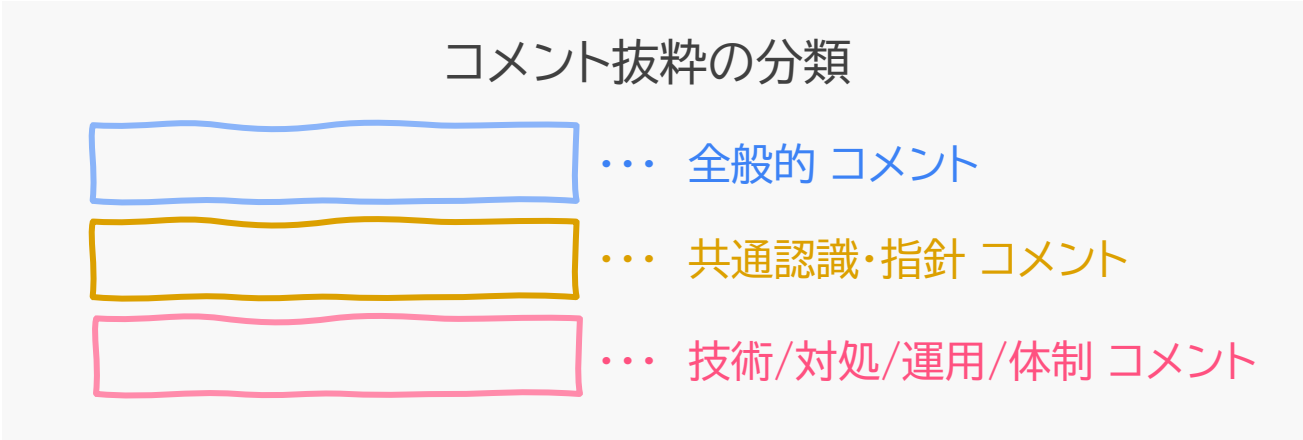
ガイドライン案に求める情報　5／5

● その他

- 主に通信の秘密に関連して違法性が阻却される行為についてその根拠、解釈の例。もしくは違法となるため実施してはいけない行為に対する説明（ISP）
  - 受信したメールのヘッダを書き換える行為の法的解釈
  - 受信したメールのデータを用いて DMARC の RUAレポートを作成する行為の法的解釈
  - 受信したメールのデータを用いて DMARC の RUFレポートを作成する行為の法的解釈
  - 作成した DMARC レポートを第三者に送信する行為の法的解釈
  - DMARC のポリシーを DNS RRで宣言する行為の法的解釈
  - DMARC レポートを受け取るために宛先となるメールアドレスを DNS レコードで宣言する行為の法的解釈（教唆に当たらないか）
  - 受信したメールを DMARC のポリシーに従って 拒否(Reject), 隔離（Quarantine）する場合の法的解釈
  - ユーザの同意を得なければ実施することが違法となる行為について、その行為を合法的に実施することを目的としてユーザから同意を得る際ににユーザへ伝えなければならない事項

付録1. ガイドラインに関するご意見・コメントの内容

- RPKI
- DNSSEC
- DMARC



1. RPKI ガイドラインに関するご意見・コメント

No	分類	コメント
1	全体	ROAキャッシュサーバに関する明文化については、より強い表現で明記すべき。「作りましょう」ではなく「作らなければならない」とするべきではないか。
2	全体	社内で議論しているが、RPKIをやる上で最終的にInvalidのものはドロップすると思っている。ガイドラインとして指針があれば上司にポリシーとして説明しやすくなると思っている。
3	全体	経営層、上司及び、支障が出たときにお客様に説明するときにガイドラインは重要であると感じる。
4	メリット・デメリット	本来のRPKIの趣旨に立ち返ると個人的には、Invalidな経路はドロップすべきと思っている。ガイドラインの中にその点を記載することは、難しい問題で各事業者のポリシーによるものがある。ドロップした時、しなかった時のメリット、デメリットは最低限書くべきと思う。
5	脅威	ROA未登録であることの脅威の説明
6	脅威	ROVを設定しないことに対する脅威の説明
7	脅威	RPKI導入により対策できる脅威と、対策できない脅威
8	Invalid経路の扱い方	経路を破棄するか優先度を下げるかなどパターンの事例があるとよい
9	Invalid経路の扱い方	dropする運用が必ずしも安全とはいえないこと
10	Invalid経路の扱いを検討	Invalid経路の扱い例(見るだけ、到達性を得つつ優先度を下げる・遅延させる、等)
11	Invalid経路の扱いを検討	こうすれば運用面でも安心してできます、という実運用例がいくつかあると良いと思いました。

1. RPKI ガイドラインに関するご意見・コメント

No	分類	コメント
12	推奨等	このガイドラインは、導入に向けて背中を押してほしい人が対象のため、強めの記述が望ましい。ROVを導入するべき、更にはInvalidな経路はDropするべき、または、することを推奨と記述して良い。
13	推奨等	Validateした後のアクションまでガイドラインに含めて作成すれば指針になると感じる。どこまで記載できるのかについて議論を進めたい。
14	推奨等	ガイドラインに「Must」「Required」と書かれてしまうと困る気がしている。多くの事業者が合意できる内容は書いてもらって問題ないと思う。推奨の意味で、「recommend」と書いていただきたい。
15	推奨等	ガイドラインに強い強制力がない方がよいと思う。
16	推奨等	当たり障りないことを書いても使われないガイドラインなるので「推奨」など書き方は難しいと思う。
17	RPKI/ROA/ROVの仕組み	RPKIの仕組みはPKIの知識が無いと深い理解が難しい部分もあり、仕組みについて図示などをしながら、分かりやすい解説が記載されることを期待します。
18	RPKI/ROA/ROVの仕組み	日本のAS運用者が実際に作業実施する対象（ROA登録先、BGPルータ設定、ROAキャッシュサーバ（自前orサービス提供利用か？）
19	経路の監視方法を検討・導入	細かい監視の導入方法はガイドラインになくていい。
20	経路の監視方法を検討・導入	ROAキャッシュで監視する項目（RTRとの接続性,VRPの数, etc）
21	経路の監視方法を検討・導入	ルータ側で監視する項目（受信した検証経路数,stateごとの数,etc）
22	経路の監視方法を検討・導入	最低限の監視、実際にここまでやっているという例があれば知りたいと思いました。
23	運用体制	障害発生時の事例を踏まえた対処方
24	運用体制	ROVするときの注意点・作法について

1. RPKI ガイドラインに関するご意見・コメント

No	分類	コメント
25	運用体制	トラブル、異常検知の事例
26	望ましい構成／パラメーター	少なくともROAキャッシュがダウンするなどROVが機能しなくなることへの考え方は示していただきたい。 ex.）経路の検証がされなくなるので一時的なROVの停止は許容できる。経路の正当性が保証されないためROVの停止は望ましくない。等
27	望ましい構成／パラメーター	ROAキャッシュサーバとBGPルータ間の適したリフレッシュタイム
28	望ましい構成／パラメーター	BGPルータでのVRPテーブル保持タイマー

2. DNSSEC ガイドラインに関するご意見・コメント

No	分類	コメント
1	経営者向け	経営者に自社のドメイン、コーポレートブランドをどう守るかという点については経営者にとっても関心の高い内容である
2	全体	ドメインのマネジメントシステムという概念の下に、ライフサイクルマネジメントを含むDNSSECや送信ドメイン認証を位置付ける考え方を説くべきと考える。
3	全体	キャッシュサーバに関して技術的な課題はほとんどなく、署名検証に失敗したときにどう対処するかが課題であり、日本の標準的な指針をガイドライン内に示してあるとよい。
4	全体	「DNSSECがあると良い。是非やってほしい。」というような一文を総務省発行のガイドラインに付け加えるだけでもある程度普及に寄与するのではないか。
5	推奨等	用途種類に関わらず、ガイドライン内でMustであると言われると事業者は身構える。一方で、Mustにしないと導入が進まないという現状もある。
6	推奨等	ガイドラインには導入推進を強気で書くとよい。ITを含めた信頼できる世界を創ると宣言している機関のメールがDNSSEC/DMARCを導入していないことにより、信頼性が欠けるということは避けるべきである。地方自治体にも努力目標として導入するとよい旨を記載するとよい。
7	推奨等	政府機関はMustという書きぶりにしたほうがよい。
8	推奨等	民間の事業者に対してはshouldやrecommendにしてほしい。
9	DNSSECの仕組み	DNSSECの仕組みは、参考書や参考ページがあるので、ガイドラインで充実させる必要はないように思う。
10	DNSSECの仕組み	基本的な構造が分かりやすく載っていれば大丈夫かと思います。自動化して運用する場合でも、あくまで構造を理解し、手動での作業手順を把握した上で取り扱うことが大事だと思うので、それは最初に念押ししても良いのかと思います。
11	SERV FAILの扱いを検討	SERV FAIL を検知した時の対処方法の例

2. DNSSEC ガイドラインに関するご意見・コメント

No	分類	コメント
12	トラブル対処	ガイドラインへの記載としては、原因を究明して正しい対処をするというのが大前提であるが、Last ResortとしてDSレコードを消すという手段もあるという程度に記載するにとどめるべきか悩ましいところである。
13	法的な留意点	DNS クエリログを分析するにあたって、通信の秘密などの観点から見た法的解釈（違法性が阻却されるとする解釈などの例）
14	運用体制	工程の全てをコマンド操作するような人力でのオペレーションは推奨しない、逆に可能な限り省力化すべきという方向の周知を盛り込むのがよいと思います。
15	各種実験結果のデータ	負荷状況の例としてクエリ数別に大中小各種ドメインの数値があると参考になりそうかと思います。
16	監視方法を検討・導入	攻撃によるSERV FAILなのか運用ミスによるものなのかを識別する方法や、運用ミスの場合の取り扱いについて書かれているとよい
17	監視方法を検討・導入	どのデータを監視すべきか
18	脅威	なにをしくじるとどんな脆弱性が発生するのかを詳しく知りたい。
19	脅威	DNSSEC を導入することで防止できたと考えられる実際の被害例
20	権威DNS	権威DNSについては、基本的には自動署名前提の内容にしていただきたい。
21	動作を確認	確認するポイントと実行例があり、OKであるとき、NGであるときそれぞれの結果があると分かりやすいかと思われます。
22	望ましい構成／パラメーター	DNS Amp 攻撃など　悪用を防ぐもしくは悪用の効果を低減する設定例・対処法など（レートリミット、平時のクエリ傾向をつかんでおく、他）
23	望ましい構成／パラメーター	著名なソフトの推奨設定の更新を伴う継続的な提供が望ましいと思います。

3. DMARC ガイドラインに関するご意見・コメント

No	分類	コメント
1	全体	ガイドラインとするなら具体的な設定手順等ではなく、目的や効果、方針といったことを記載するべきではないか。
2	メリット・利点	マルウェア対策として、積極的なDMARC導入が予防対策として必要であることを訴えるべき。
3	メリット・利点	経営者向けには導入のモチベーションを高める記述が求められるのではないか。例えば、Googleと米国Yahoo!の発表にあるように、DMARC非対応のまま大量メールを送信すると迷惑メールフォルダに隔離されるなど正規のメールが届かなくなることから、DMARC対応が求められているといった最新の動向も盛り込むことも考えられる。
4	DMARCポリシーの設定変更	偽陽性の具体的な解決方法
5	DMARCポリシーの設定変更	利用できるツールの紹介/使い方
6	DMARCポリシーの設定変更	設定変更に当たり DNS のキャッシュに関連して注意すべき点があるか
7	DMARCポリシーの設定変更	DMARC導入の効果はあるというところを示したいのでp=noneのままではなく、p=rejectを理想と考えている。
8	DMARCレコードの設定	基本的な事項（タグの説明、最低限定義の必要なタグの明示）
9	DMARCレコードの設定	サブドメインを考慮した設定内容が書かれているとよい
10	DMARCレポートの確認	レポート内容から判断できること、対応すべき事項の記載があると良いと思います。
11	DMARCレポート分析	着目する箇所と、結果を踏まえた改善手法の提示があるとよい。
12	運用体制	監視方法。（何を監視すべきか、どのように監視すべきか）