RFC 5585
DomainKeys Identified Mail (DKIM)
Service Overview 要約

RFC 5585 要約

- **RFC 5585**
  DomainKeys Identified Mail (DKIM) Service Overview

- DomainKeys Identified Mail とは？

  ✓ ドメインレベルのデジタル署名認証フレームワーク
  ✓ 公開鍵暗号を使い、キーサーバ技術として、DNSを利用
  ✓ 送信元の組織の確認、および、メッセージの内容が改ざんされていないことの確認が可能
  ✓ DKIMの認証によるメールのなりすましの防止により、スパムとフィッシングのグローバルなコントロールを支援

RFC 5585 要約

- **RFC 5585の内容、対象、前提知識**

項目	説明
内容	・DKIMのスコープ ・DKIMの経緯 ・DKIMの活用とゴール ・DKIMの機能 ・DKIMのサービスアーキテクチャ
対象読者	DKIMの適用、開発、設置を行うエンジニアの方
前提知識	・電子メールのバックグラウンド ・ネットワークセキュリティ技術 ・ネットワークサービス
説明の対象	・DKIMのアーキテクチャ、機能
説明の対象外	・DKIMの運用での課題 ・DKIMが利用するサービス ・DKIMを使って実装されるサービスの詳細、運用ポリシー、その評価

RFC 5585要約

- **DKIMのスコープ**

DKIMのスコープ	DKIMはドメイン名を識別子（署名ドメイン識別子、以下、SDID）として利用
	ドメイン名をDKIM-Signatureヘッダーフィールドのd=タグに設定
	SDIDの所有者がメッセージに対する責任、説明責任を持つ
	メッセージの作成者、メッセージの取扱い者、メッセージを作成代行をするサービス提供者が署名を生成
	DKIM署名のないメールは、DKIMの定義前と同じように処理
	メッセージの正当性の判定のみに限定したサービス
	フィルタリングサービスやドメインの評価といった、より大きなコンテキストでの利用も想定

DKIM署名	署名時と確認時のデータの整合性を証明し、このタイミング以外で内容の認証・確認はしない
	署名者の振る舞いについての主張しない
	署名の確認成功のために受信者に対して特定の指示をしない
	署名確認後の保護を提供しない
	すでに確認された署名を持つメッセージの再送（あるいはリプレイ）に対する保護はしない

RFC 5585要約

- DKIMの経緯

既存の技術	【送信ドメイン認証技術】 – SPF – Sender ID	【インターネットメールの署名技術】 – Privacy Enhanced Mail (PEM) – Pretty Good Privacy (PGP) – MIME Object Security Services (MOSS) – Secure MIME (S/MIME)
課題	▲IPアドレスを利用するため、機能面、運用面でセキュリティの問題あり	◎PGPとS/MIMEは大きなユーザベースを獲得 ×ユビキタス(遍在性)という観点では未達成
課題への対応	ドメイン名を使えば良い	PGP、S/MIMEにドメイン認証の仕組みを取り入れれば良いが、技術的に困難

既存の暗号化の部品を再利用して
新サービスを作成

DomainKeys Identified Mail (DKIM)

① 公開鍵の管理スキームの鍵中心のアプローチ
② 公開鍵の管理にDNSを利用
③ 新たなインフラの展開を要求せず、既存のDNSに情報レコードを追加することで、鍵管理機能を提供

RFC 5585要約

- DKIMの活用とゴール

活用
「合法的なメールを識別するための基盤」、「メッセージとSDIDの関連付け」を提供
署名の確認に成功した場合、署名者に関する情報をスパム、スプーフィング、フィッシング、あるいは、他の好ましくない動作を制限するサービスの一部として使うことが可能
送信者の身元の確認
信頼性評価の入力情報としての活用
メッセージの正当性の証明

ゴール	
機能面	メッセージの保証に、ドメインレベルの粒度を利用
	局所的な実装に対応
	コアとなる検証の仕組み、および、派生した利用の明確な区別
	電子メールを送信するユーザの匿名性を保持
運用面	検証の失敗を署名なしと同じように扱う
	インクリメンタルな成果を得られるように、インクリメンタルな適用を許す
	要求されるインフラの量を最小化
	適用時に幅広い選択肢を提供

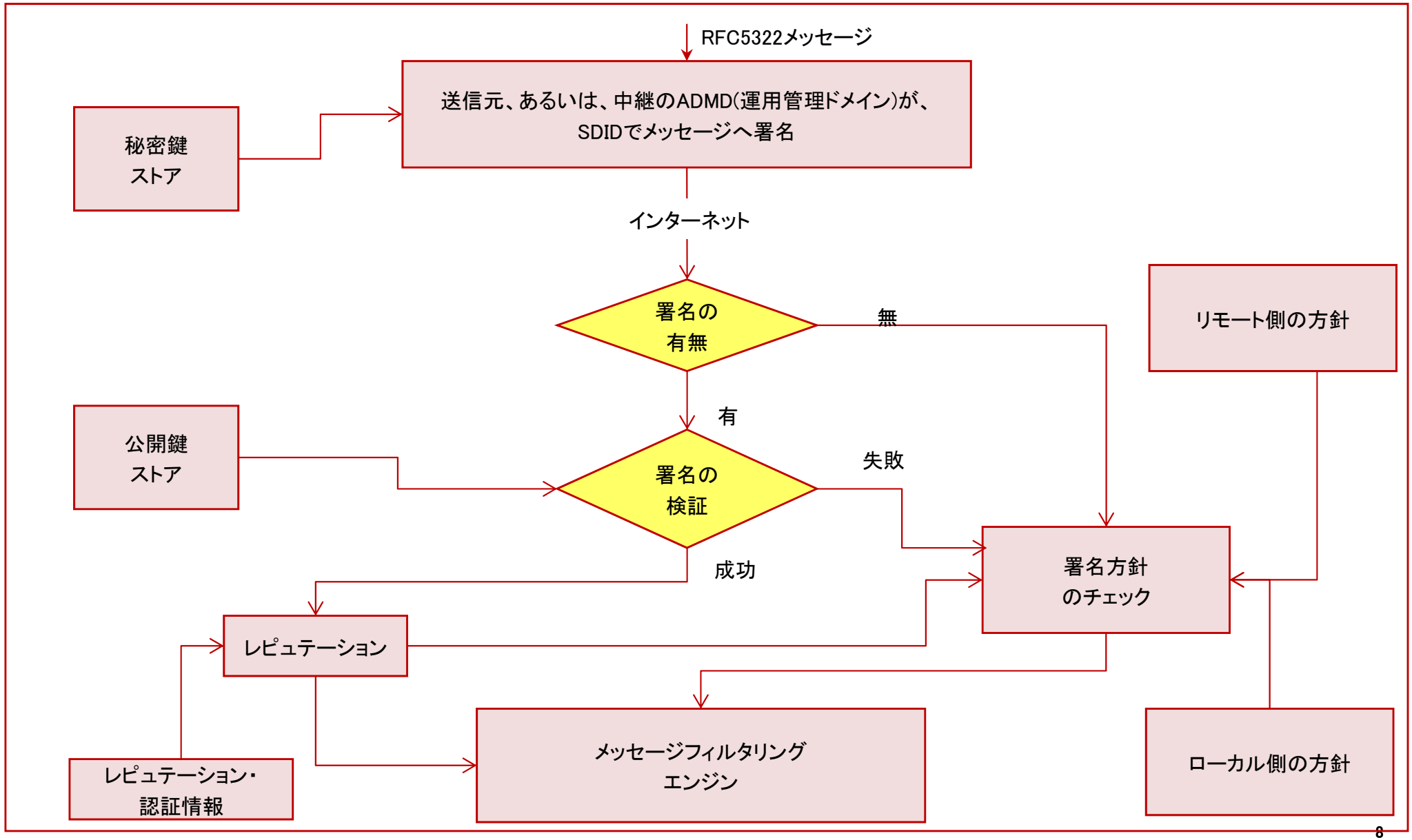
RFC 5585要約

- DKIMの機能

処理	説明
署名の作成	1) SDIDの選択
	2) 署名の作成 2-1) 選択されたヘッダフィールドのハッシュ、メッセージボディのハッシュを生成 2-2) 他の署名パラメータと共に、秘密鍵を用いてハッシュをエンコード
	3) DKIM-Signature:ヘッダを使ってメールに署名情報を追加
署名の検証	1) DKIM-Signature:ヘッダからドメイン、セレクタを取得
	2) セレクタの情報を用いて、DNSから公開鍵を取得
	3) 署名を検証
セレクタ	1つのSDIDで、複数の秘密鍵(複数の署名者)を利用できるようにするためのパラメータ DKIM-Signature:ヘッダの中で、独立したパラメータとして設定
署名の検証者	メッセージ受信者の運用管理ドメインのエージェントが署名検証を実施 メッセージの発信元が、対応するSDIDの秘密鍵を所有している団体かどうかを確認
サブドメインの評価	同一組織で複数の種類の評価を受けたい場合、異なるサブドメインを使うことで対応可能 たとえば、transaction.example.comと、newsletter.excample.com あるいは、productA.example.comと、productB.exmaple.com など

RFC 5585要約

- DKIMのサービスアーキテクチャ



RFC 5585要約

- DKIMのサービスアーキテクチャ（続き）

作成と検証	説明
メッセージへ署名	鍵ストアから取得した秘密鍵を使って、運用管理ドメイン（以下、ADMD）内で権限を与えられたモジュールにより行われる 送信元のADMDのMUA、MSA、あるいはMTAが実行
署名の検証	鍵ストアから取得した公開鍵を使用して、受信側の運用管理ドメイン（以下、ADMD）内の権限を与えられたモジュールにより行われる。受信側のMTA、MDA、あるいはMUAが実行 〇署名の検証が成功すると、署名者の評価のため、レピュテーション情報がメッセージフィルタリングシステムへ渡される 〇署名検証に失敗、あるいは、メッセージの作成者のドメインを使った署名がないとき、メッセージの作成者に関係する署名の方針情報を、リモート、かつ/あるいはローカルから取得し、この情報がメッセージフィルタリングシステムへと渡される

情報の管理	
さまざまなテーブル、サービスを外部情報の管理に利用	
鍵ストア	DKIMは公開/秘密鍵(非対称)暗号を利用 署名には秘密鍵を使い、検証には、DNSへ問い合わせて取得した公開鍵を利用。 セレクタとSDIDの組み合わせごとに公開鍵をDNSに登録
レピュテーションと認証	メッセージの署名に対し、メッセージの配布あるいは、表示判定に、 関連するドメインのレピュテーションを確認することができる ※DKIMではこの評価サービスは提供しない
署名方針(ADSP)	メッセージの送信者のドメインにおけるADSPを公開

RFC 5585要約

- DKIMのサービスアーキテクチャ（続き）

処理	説明
署名の作成	署名は、SDIDに関連付けられた秘密鍵を利用し、メッセージの中継経路上のADMDあるいはメッセージを作成するADMDのコンポーネントにより行われる
署名の検証	メッセージのリレーあるいはメッセージの配布の経路に沿った機能コンポーネントにより行われる
検証不可メッセージ、未署名メッセージ	メッセージ作成者の情報が権限なしで使われているかを判断するため、公開されている署名方針の問い合わせをすることが可能
署名の評価	評価結果の一般的な利用方法は、フィルタリングエンジンへの入力としての利用 （フィルタリングの詳細はDKIMの範囲外）
ADMD内でのDKIMの処理	DKIMを実装する一般的な場所 〇部門、あるいは、境界のMTAのような、作成側の組織の外向けのサービス 〇受信側の組織のインバウンドサービスのインフラ内 作成者あるいは受信側のMUAでも実装できるが、管理とサポートのコストが大きくなるため、期待できない