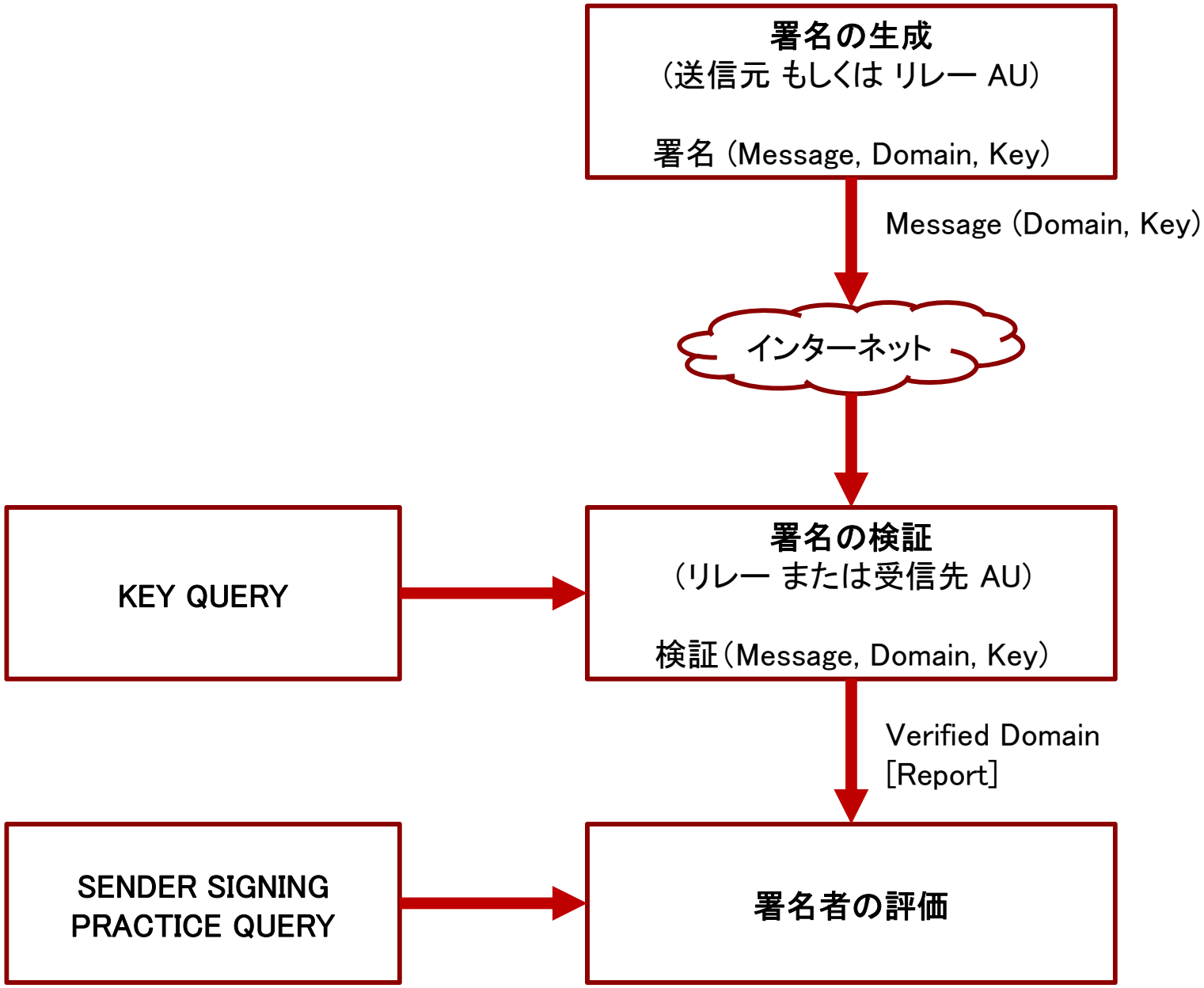
RFC 4686
Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)
概要

要約

- 電子メールに対する脅威、とりわけ DKIM で対処しようとしている脅威に関する分析を提示する。
- 以下の点について考察する。
  - 攻撃者の特質と所在
  - 彼らに何ができるのか
  - 彼らは攻撃によって何を成し遂げようとしているのか

- 管理ユニット（Administrative Unit, AU）
  - 電子メールの経路上に存在し、流通するメールを管理する部分。
  - 送信者や受信者は管理ユニットと信頼関係を結び、DKIM署名や検証を実行するために管理ユニットを介してメールの送受信を行う。

DKIMのフローチャート



攻撃者の特徴

DKIMがカバーする問題領域は幅広い攻撃者によって特徴づけられる。

レベル	タイプ	特徴

高	詐欺などの営利目的の業者	• 洗練されており、財力もある。
		• インターネット基盤への攻撃も
		  • DNSキャッシュ汚染
		  • IP routing 攻撃

中	プロの迷惑メール送信者	• インフラを保有
		  • MTA
		  • ドメイン
		  • ボットネット
		• 送信のみならずアドレスの収集も

低	だたの迷惑メール送信者	• 送信元アドレス詐称 • 将来的には署名もできるようになるだろう

攻撃者は次の情報にアクセス可能であると考えておくべき

1. 標的ドメインから送信されたメールの膨大な文例
2. 標的ドメインのビジネスの目的やビジネスモデルに関する知識
3. 標的ドメインの公開鍵とそれに結び付くDNSレコード

次のうちのいくつかを実行する能力も持ちうる

1. 複数の場所のMTAからのメールの投入
2. 任意のメールヘッダの生成
3. 支配下のドメインになり代わっての署名
4. 署名なしまたは見せかけの署名付きのメールの大量送信(DoS攻撃のため)
5. 正規に署名されたメールの再送
6. エンベロープ情報に基づくメールの転送
7. 乗っ取ったコンピュータから正規の発信者を装ってのメール送信

資金力のある営利目的の攻撃者は、さらに
以下の能力も持つと考えられる

1. IPルーティングの操作
2. キャッシュ汚染など、DNSへの影響
3. （ボットネットなどの）膨大な計算資源へのアクセス
4. 通信の傍受

攻撃者の所在

- Externally-Located Bad Actors
- Within Claimed Originator's AU
- Within Recipient's AU

もっとも基本的な不正行為は送信元アドレスの詐称であり、次の2パターンに分類される

- 任意のアドレスを詐称する場合
- 特定のアドレスを詐称する場合
  - Exploitation of Social Relationships
  - Identity-Related Fraud
  - Reputation Attacks
  - Reflection Attacks

任意のアドレスの詐称

- 真の送信者を隠すためにとられる行為
- 送信者は、攻撃者本人であることもあるが、攻撃者の支配下にあるサーバやボットネットであることも。
- SSPで全メールへの作成者署名を宣言してあれば、そのドメインの不正使用をDKIMによって軽減できる。
- しかし、攻撃者の支配下のドメインが使用されることに対しては DKIM では防げない。
  - DKIMは、そのドメインの所有者が署名したことを保証するが、署名者の正当性を保証するものではない。
- 別途、外部機関による認証や評価、自身で持つホワイトリストやブラックリストと組み合わせることによって、DKIM署名のドメインが信用できるものであるかどうかを判断できる。

特定のアドレスの詐称

攻撃の影響度と頻度の分類

この後、DKIM に対する攻撃を一覧表にまとめる際、下記のカテゴリーに分類して提示する。

■ 影響度

カテゴリー	内容
高	ドメイン全体や複数のドメインからのメールメッセージの検証に影響を及ぼす。
中	特定のユーザー、MTAからのメールメッセージの検証に影響を及ぼす。影響を及ぼす期間が限定的である場合も含む。
低	個々のメールメッセージの検証に影響するのみ。

■ 頻度

カテゴリー	内容
高	全てのメールユーザーがしばしばこの攻撃を受けると予期される。
中	たまにこの攻撃を受けると予想される。もしくは、少数のユーザーがしばしばこの攻撃を受けると予期される。
低い	攻撃は滅多にないと予期される。

署名への攻撃 (1)

dkim.jp

攻撃名	影響度	頻度
ドメインの秘密鍵の窃盗	高	低
委託された秘密鍵の窃盗	中	中
サイドチャネル攻撃による秘密鍵の回復	高	低
選択されたメッセージの再生	低	中/高
署名されたメッセージの再生	低	高
検証に対する DoS 攻撃	高	中
鍵提供サービスに対する DoS 攻撃	高	中
正規化の悪用	低	中
本文の長さ制限の悪用	中	中

署名への攻撃 (2)

攻撃名	影響度	頻度
無効な鍵の利用	中	低
鍵サーバへの侵入	高	低
鍵サービスの応答の改ざん	中	中
不正な鍵レコードや署名の発行	高	低
署名生成時の暗号の弱点	高	低
表示名の悪用	中	高
送信元のネットワーク内部の侵入されたシステム	高	中
検証探査攻撃	中	中
上位ドメインによる鍵の発行	高	低

Message Signing Practices への攻撃

攻撃名	影響度	頻度
よく似たドメイン名	高	高
国際化ドメイン名の悪用	高	高
Signing Practices に対する DoS 攻撃	中	中
複数の送信元アドレスの使用	低	中
第三者署名の悪用	中	高
Sender Signing Practices の応答の改ざん	中	中

その他の攻撃

攻撃名	影響度	頻度
Packet amplification attacks via DNS	N/A	中

これまでの議論で言明しなかったが、他にも要件が存在する。

- 鍵および SSP レコードは地理的に分散したサーバで保持するべし。
- 鍵および SSP レコードは検証側もしくは他の基盤によってキャッシュされるべし。
- 鍵レコードのキャッシュの生存期間はレコード毎に指定できるべし。
- メールメッセージ中の署名アルゴリズムIDはドメインの鍵レコードに列挙されているものであること。
- 暗号技術は日々進歩している。数年後でも耐えうる暗号アルゴリズムを使用すること。