第 XVIII 部

ENUM テストベッドの運用

第 18 部
ENUM テストベッドの運用

第 1 章　はじめに

ENUM ワーキンググループでは、今年度は従来の活動に追加して、迷惑電話（SPIT）に関する考察を行った。インターネット電話では、電子メールでの迷惑メール（SPAM メール）に対応する迷惑電話（SPIT）が発生しやすく、すでにいくつかの事件が起きている。

本報告書では、従来からの活動と SPIT に関する分析を以下のとおり報告する。2 章において、ETJP の活動報告と、日本における ENUM トライアル状況を報告する。3 章において、2005 年春 WIDE 合宿にて実施した ENUM 実験の報告を行う。4 章において、SPIT についての分析結果をまとめる。5 章において、SIP プロトコル的な観点から攻撃可能性と攻撃を防ぐ方法を調査し、さらに実際の機器に対し、攻撃を行えることを示した。6 章において、迷惑メールでの経験から得られる教訓について考察した。

第 2 章　ETJP/日本における ENUM トライアル状況

2.1 ETJP の状況

ENUM トライアルジャパン（ENUM Trial Japan; ETJP）は日本国内における ENUM のトライアル実施のため、JPNIC、JPRS、WIDE Project の 3 者が発起人となり、2003 年 9 月に設立した組織である。2005 年 12 月末現在で、WIDE Project を含む 46 会員が参加している。ETJP の詳細については下記の URI に詳しい。

`http://etjp.jp/`

ETJP の 2003 年 9 月から 2004 年 9 月までの活動については報告書にまとめられており、下記の URI で公開されている。

`http://etjp.jp/about/activity/20041111/ETJP_2nd_report1111.pdf`

ETJP では、トライアルを以下の 3 フェーズで実施する計画であり、2004 年 9 月までにフェーズ 1、フェーズ 2 を独自の ENUM トライアル用ドメイン名空間である 1.8.e164.jp を利用して行っている。

フェーズ 1　ENUM を用いた機器・アプリケーションの動作検証
フェーズ 2　同一組織内での ENUM を用いた通信サービスの動作検証
フェーズ 3　組織間での ENUM を用いた通信サービスの動作検証、および他国 ENUM トライアルとの連携

フェーズ 3 は日本における国際的 ENUM トライアル用ドメイン名空間である 1.8.e164.arpa の利用を必要とするため、2005 年はその環境が整うのを待つ状況であり、トライアル成果的には進捗がなかった。なお、後述のとおり 2006 年には 1.8.e164.arpa が利用できるようになる見込みである（2005 年 12 月末現在）。

2.2 日本における ENUM トライアル状況

2005 年 8 月に総務省が取りまとめた「IP 時代における電気通信番号の在り方に関する研究会」の第一次報告書において、ENUM トライアルの円滑な推進のため国際的な ENUM トライアル用ドメイン名空間である 1.8.e164.arpa 申請の必要性が明記された。当該報告書の公表に関しては、下記の URI で案内されている。

`http://www.soumu.go.jp/s-news/2005/050810_2.html`

なお、当該報告書の ENUM トライアルの推進に関する部分に対して、JPNIC、JPRS、WIDE Project が連名でパブリックコメントを提出している。

総務省は、当該報告書での ENUM トライアルに対する方針に従って 2005 年 11 月に 1.8.e164.arpa の割当委任を国際電気通信連合（ITU）に申請し、承認されている。2005 年 12 月末現在、1.8.e164.arpa の DNS は委任、運用が開始されており、2006 年には利用が開始される見込みである。

第 3 章　WIDE 2005 年春合宿における ENUM 実験報告

3.1 目的

ENUM 番号による呼び出しを前提に、以下を行う。

(1) 異なる SIP ドメイン間の相互接続確認

(2) Softphone 間の相互接続確認

(3) 上記を通じた経験の蓄積

3.2 環境

SIP サーバおよび ENUM 登録システムは、詳細は 2003 年度報告書および 2004 年度報告書で説明した、ENUM ワーキンググループが WIDE 東京 NOC に設置しているものを使用した。SIP サーバおよび ENUM 登録システムは現在でも利用可能である。

`https://www.e164.wide.ad.jp/`

SIP クライアントは、合宿参加者が各自の PC にインストールした SIP Softphone、もしくは参加者が所有していた SIP 端末を使用した。

3.3 実験方式概要

実験参加者は自身の ENUM 番号に対し ENUM 登録システムによりアプリケーション URI を登録した上で、他の実験参加者の SIP クライアントから ENUM 番号で呼び出しをしてもらい、相互接続を確認する。

3.4 実験実施結果

3.4.1 ENUM 登録状況

(1) 対象 ENUM ドメイン

3.3.4.9.e164.wide.ad.jp

(2) 対象期間

3/24 01:00 のみ調査

(3) ENUM 登録システムでアプリケーション URI を登録した参加者数

24 名

(4) 登録されたアプリケーション（プロトコル）の内訳

SIP:　18

TEL:　7

HTTP:　6

MAILTO:　8

間違い:　9

3.4.2 SIP サーバの利用状況

(1) 対象 SIP ドメイン

sip2.e164.wide.ad.jp

(2) 対象期間

3/20 04:00〜3/24 14:00

(3) Register した参加者数

17 名（37 アカウント）

(4) 呼び出し（Invite）した参加者数

17 名（394 コール、うち 35 コールは異なる SIP ドメイン間）

3.4.3 相互接続を確認したもの

(1) SIP サーバ⟷SIP サーバ

SER⟷SER

SER⟷SIP アプライアンス（Asgent 製）

(2) SIP サーバ⟷ SIP クライアント

SER ⟷ X-Lite
→ SJPhone
→ WindowsMessenger
→ SIP Communicator
→ WirelessIP-5000
→ N900iL

SIP アプライアンス⟷ WindowsMessenger
→ N900iL

(3) SIP クライアント⟷ SIP クライアント（RTP）

X-Lite	⟷	X-Lite
SJPhone	⟷	SJPhone
WindowsMessenger	⟷	WindowsMessenger
SIP Communicator	⟷	SIP Communicator
WirelessIP-5000	⟷	WirelessIP-5000
N900iL	⟷	N900iL

3.5 得られた知見

本実験を通じて以下の知見が得られた。

(1) SIP Softphone のインストールと設定はノウハウが必要であり、普及のためにはマニュアルが必要

(2) ENUM サービスのアプリケーション URI 記法は難しく、NAPTR の書き方マニュアルが必要

3.6 謝辞

SIP Softphone のインストール大会に参加してくださった 10 名の方々、ENUM 実験に参加してくださった 17 名の方々、そして SIP アプライアンスでの相互接続を確認してくださった Asgent の高石さんに深く感謝申し上げます。

3.7 参考 URI

SER（SIP Express Router）
`http://www.iptel.org/ser/`
SIP アプライアンス（Asgent）
`http://www.asgent.co.jp/Products/Applico/applico.html`
X-Lite
`http://www.xten.com/index.php?menu=X-Series`
SJPhone
`http://www.sjlabs.com/sjp.html`
WindowsMessenger
`http://www.microsoft.com/downloads/details.aspx?FamilyID=a8d9eb73-5f8c-4b9a-940f-9157a3b3d774&DisplayLang=ja`
SIP Communicator
`http://www.sip-communicator.org/`
WirelessIP-5000
`http://www.wirelessip5000.com/indexj.html`
N900iL
`http://www.docomo.biz/html/product/cordless/n900il.html`

第 4 章　SPIT の概念と分類

SPIT は、SPAM over Internet Telephony の略である。ニュースメディアでは、電子メールで発生した迷惑メール（SPAM メール）に相当する迷惑行為、つまりインターネット電話での迷惑電話を SPIT としている。

ところが、インターネット電話には迷惑行為以上の弱点も存在する可能性があり、本ワーキンググループでは、インターネット電話への Abuse（攻撃）すべてを SPIT として取り扱い、VoIP のセキュリティ全般を考察することとした。

VoIP で要求される安全な環境とは、次の項目が満たされた状態である。

- 盗聴されていない
- なりすまされていない
- 改竄されていない
- 内容に意味がある

4.1 SPIT の概念

本ワーキンググループでは、SPIT には、次の 2 つの概念を含むこととする。

- プロトコルとしては正しいが、実現手段もしくはメッセージの内容に問題があるもの（ニュース記事で取り上げられている SPIT、メールの SPAM に対応）
- プロトコルやオペレーションの視点から不正が行われているもの（Integrity、Confidentiality、Availability、Security に対する脅威）

後者に属する問題点として、プロトコルに属する問題点、実装に関する問題点があり、その中には発信者情報詐称の原因となるものや、ワン切りや DoS の原因となる問題点が存在する。

4.2 SPIT の分類（利用者の視点で）

次に、電話・VoIP サービスを使う上での脅威を洗い出し、整理を行った。最初に利用者の視点で分類した。

4.2.1 迷惑電話型（売り込み／いたずらによる被害）

- 売り込み・広告・勧誘電話
  - 発信者の種類
    - ＊人間の発信によるもの
    - ＊機械的な発信によるもの
    - ＊人工知能的な応答をするもの
  - 電話番号の収集方法
    - ＊電話帳より
    - ＊名簿流出
    - ＊網羅的発信
- ワン切り（発信者電話番号が正しい）
- 迷惑電話が多すぎて使いたいときに使えない
  - 端末から電話できない
  - 電話局の交換機・SIP サーバが落ちる

4.2.2 発信者情報詐称・つなぎかえによる詐欺

- 自 ID 虚偽使用型
  - 自分の名前の詐称
  - 料金詐欺：自分の名義で電話が使われた場合
  - callback をさせて DDoS、風評被害
- 発信者情報詐称型
  - 知人の名前の詐称
  - カード会社・銀行・公的機関などを騙った詐欺の電話
  - 使い捨て電話番号を使って勧誘など
- SIP サーバになりすます（DNS 悪用）
  - 偽 SIP サーバだが正しく振舞い、あるときダウン
  - 他の端末の代理応答のメッセージを騙ったもの
- セッションハイジャック型
  - 挨拶などによる認証後、電話線をつなぎかえ、ハイジャックして別の会話に誘導

4.2.3 通話内容の盗聴・通話の記録・個人情報漏洩型

- 盗聴、音声の記録
- トラフィック解析（電話の発着呼の記録）
- 利用者の代わりに register して、通信情報を記録
- ユーザの行動・移動情報のトレース
- 利用者の登録情報の漏洩
- UA の ID/Passwd の記録・漏洩
  →認証情報漏洩による攻撃が可能

4.2.4 電話料金に関するもの

- 料金の横領（1 円未満含む）
- 近距離通話を遠回しして課金
- 料金詐欺：自分の名義で電話が使われた場合

4.2.5 DoS 型

- 第三者による電話セッションの切断
- 電話を使えないようにする攻撃
- SIP サーバを使えなくする攻撃（SIP サーバへの DoS）
- DoS による、通話の妨害、非常通話（110 番など）の妨害
- IP 電話器の脆弱性を突いて、電話を鳴らす
- 不特定多数の電話に対して、機械的に高頻度で発呼させ続ける
- IP Phone を使って電話と無関係なサービスへの DDoS をかける
- DoS 対策の結果、知らない人からの電話が困難となる可能性
- RTP のセッションを一方的に送りつけられる

4.2.6 システム的問題

- 通話が切れない

4.2.7 他人によるなりすまし

- 認証情報漏洩などの結果、自分になりすまされて悪事を起こされる
- 料金詐欺：自分の名義で電話が使われる

4.3 原因となる脆弱性・攻撃法にもとづいた分類

次に原因となる脆弱性・攻撃法にもとづいて分類し直した。脆弱性、攻撃法は以下のものが考えられる。

- 迷惑電話型
- 認証情報漏洩によるもの
- 中間者攻撃
- From 詐称によるなりすまし、詐欺
- 想定していない DoS（大量）

4.3.1 迷惑電話型

4.2.1 と同じ。電話としては正しい使い方だが相手の都合を無視したものであり、プロトコルとしては問題がない。回避するには、発呼数の制限などにより、コストに見合わなくすることが考えられる。

4.3.2 認証情報漏洩によるもの

- 利用者のかわりに register を行い、通話し、なりすまし詐欺

認証情報が洩れにくいユーザー認証方法を用いることで解決すべきである。

4.3.3 中間者攻撃

中間者攻撃とは、ISP の根本の SIP サーバ乗っ取りや、ファイバカット、タッピング、経路情報のハイジャックなど、あるいは電話会社の共犯により、通信路上にて、通話の制御情報、あるいは通話そのものを記録したり改竄することである。中間者攻撃の場合、利用者にばれない攻撃を行うことが可能である。通信路のタッピングと SIP サーバ乗っ取りの 2 つに分類できる。

中間者攻撃や SIP サーバがハイジャックされた場合、電話が成立し、挨拶などの認証のあとで VoIP

セッションをハイジャックして別の会話に誘導するような攻撃も可能である。

基幹ネットワークでのタッピングや、SIP サーバ乗っ取りは論外としても、無線通信路などの共有ネットワークでのタッピングは考慮しておく必要がある。

4.3.3.1 中間者攻撃：通信路のタッピング

- 盗聴、音声の記録
- トラフィック解析（電話の発着呼の記録）
- ユーザの行動・移動情報のトレース
- 利用者の登録情報の漏洩
- UA の ID/Passwd の記録・漏洩（Challenge/Response 型認証のため、漏洩しにくい）
- 挨拶などによる認証後、電話線を繋ぎかえ、ハイジャックして別の会話に誘導

4.3.3.2 中間者攻撃：SIP サーバ乗っ取り

- ユーザの行動・移動情報のトレース（Register 時の IP アドレスの変化の記録）
- 利用者の登録情報の漏洩
- 登録ユーザの UA の ID/Passwd の記録・漏洩
  →認証情報漏洩による攻撃が可能
- 課金情報の操作（料金の不正）

4.3.4 発信者 ID 詐称型

SIP プロトコルを用いた VoIP サービスの電話番号は、SIP URI の一部（@の LHS）が用いられることが多く、多くの実装も SIP URI の一部を発信者 ID として表示するが、そのように取り扱うことが決められているわけではなく、すべてのサービスがそうなっているわけではない。また SIP プロトコルの From は、電子メールと同様に自己申告であり、詐称可能な場合がある。なりすまし、発信者 ID 詐称による詐欺としては以下の事項が考えられる。

- 自分の名前の詐称
- 知り合いの名前の詐称
- 料金詐欺：自分の名義で電話が使われる
- カード会社・銀行・公的機関などを騙った詐欺の電話
- callback をさせて DDoS、風評被害
- 他の端末の代理応答のメッセージを騙ったもの

4.3.5 DoS 型

4.2.5 DoS 型とほぼ一致する。SIP プロトコルを用いた VoIP サービスに対して、以下の DoS 攻撃が可能である。

DoS 攻撃の結果として、警察や被害者の通話が不可能となるので、それを組み入れた犯罪が起きる可能性がある。

また、DoS を警戒し、フィルタするような社会となると、知らない人からの電話がかかってこないような事象が発生する可能性がある。

4.3.5.1 SIP サーバへの DoS

- SIP サーバにメッセージを大量に送り、使えなくする
- register message を一斉にサーバに送りダウンさせる
- multiple register を大量に登録しておき、call が来たときに invite meesage を大量に発生させる

4.3.5.2 通信 Session への DoS

- 網羅的に CANCEL を投げ、既存の電話を切る

4.3.5.3 電話への網羅的 DoS

- 不特定多数の電話に対して、機械的に高頻度で発呼させ続ける
- 網羅的に SIP ポート 5060 へ SIP メッセージを投げる

第 5 章　SIP と IP 電話のセキュリティ状況

SIP と IP 電話に関する現在のセキュリティ対応状況について、各種プロトコルなどの技術面と実利用環境での状況の両者においての、現状の概要と、調査実験により判明した問題点などを報告する。

この文書は、ENUM ワーキンググループを中心に行われている SPIT 勉強会 2005 年活動分の、SIP と IP 電話のセキュリティ状況に関する部分の報告書である。

5.1 SIP におけるセキュリティ機能

IP 電話などで用いられている SIP（Session Initiation Protocol）[234] は、メールやウェブで用いられているプロトコルと比べて、セキュリティの

確保が非常に難しいプロトコルである。これは、Registrar への登録や複数の Proxy による転送などのしくみに加えて、UA（User Agent）がサーバにもクライアントにもなって、さらに UA 間の通信が直接行われることもあることによる。

SIP では、これらの複雑なしくみにおいて、認証、完全性、機密性といったセキュリティの実現のために、新たに 1 からセキュリティの枠組みを用意するのではなく、可能な限り、既に各分野にあるセキュリティの枠組みを利用する形をとり、その上で足りない分を新たに導入する方針をとっている。

ここでは、それらの SIP におけるセキュリティ機能について、各プロトコルの一覧とそれぞれの概要を示す。そして、認証、完全性、機密性のそれぞれのセキュリティ確保の方法についてまとめる。

5.1.1 Digest 認証

SIP では、RFC2617[88] で定められている HTTP 認証の枠組みをほぼ踏襲する形で、Challenge/Response 型である Digest 認証の枠組みを RFC3261[234] で定めている。Basic 認証については、使用が禁止されている。

UA 間、あるいは、UA と Proxy や Registrar などの間で用いられ、サーバ側は、REGISTER や INVITE などのリクエストを送ってきた UA を、ユーザ名とパスワードにより識別して認証することができ、それにより、リクエストを受け付けるかどうかなどを判断することができる。

5.1.2 TLS

SIP では、TLS（Transport Layer Security）[48] の利用を、RFC3261 で定めている。これにより、SIP 通信における認証と暗号化が可能となる。

5.1.2.1 各サーバと UA での対応の違い

Proxy/Redirect/Registrar の各サーバにおいては、TLS の実装は必須であり、相互認証も一方向認証もサポートが必須となっている。また、それら各サーバにおいては、ホスト名に対応するサブジェクトのサイト証明書を所有すべきとなっている。すなわち、これらのサーバ間での TLS 接続では、TLS のサーバ認証もクライアント認証も行える。

一方、UA は TLS を開始できることが強く推奨されている。UA が TLS サーバになることと、自分の証明書を所持することは、可能とはなっているが必須とはなっていない。これらにより、UA は主として TLS クライアントとしての利用が想定されている。

5.1.2.2 証明書の検証

TLS をサポートする場合、UA も各サーバも、受け取った相手の証明書の検証は必須となっており、このためにはルート証明書を持つことが必要となっている。つまり、UA は自分の証明書を必ずしも持たなくてもよいが、ルート証明書を所有してサーバの証明書の検証は行うことになる。

5.1.2.3 対応すべき暗号スイート

SIP において TLS が用いられるときは、AES（Advanced Encryption Standard）を用いた TLS_RSA_WITH_AES_128_CBC_SHA[36] のサポートが最低限必須であり、TLS_RSA_WITH_3DES_EDE_CBC_SHA を下位互換のためサポートすべきとなっている。

5.1.2.4 接続の継続利用

UA が各サーバにコンタクトを試みるときは、UA は TLS 接続を開始するべきとなっており、その上でリクエストなどを送る。また、UA がその TLS 接続上で、逆にリクエストを受けることも可能となっている。

そのようなケースで想定される利用形態としては、UA1 が Proxy1 と Proxy2 を介して UA2 へリクエストを送る場合、UA1 → Proxy1 → Proxy2 ← UA2 という形で矢印方向に TLS 接続することで、すべての各区間を TLS 接続にして利用することが考えられる。この場合、Proxy2 ← UA2 の部分は、UA2 が Proxy2 へ REGISTER 時に確立した TLS 接続を維持して利用することになる。

5.1.3 TLS と Digest 認証の併用

Proxy → Proxy のように Proxy 間での TLS 接続の場合は、互いにサイト証明書を所持することから、相互認証をすることが可能である。しかし、UA → Proxy のように UA から Proxy へ TLS 接続した場合は、Proxy だけしかサイト証明書を所持しない場合もあり、一方向認証しかできない。

そこで、TLS と Digest 認証が併用される。すなわち、UA が Proxy（または Registrar 等）を認証

する方法は、Proxy が TLS サーバとなってサイト証明書を用いたサーバ認証を行う。そして、Proxy が UA を認証する方法は、各 UA の個別パスワードとなる事前共有鍵によって Digest 認証を行う。

これにより、さきほどの、UA1 → Proxy1 → Proxy2 ← UA2 といった TLS 接続例では、すべての各区間において、相互認証と機密性が確保されることになる。しかし、UA1 と UA2 の間の E2E（End-to-End）で認証されてるわけではない点と、機密性と完全性も E2E で保証されるわけではない点に注意する必要がある。

5.1.4 IPsec

SIP では、その通信路において IPsec[158] の利用も可能と言及されている。TLS と異なり、必須とはなっておらず、また、SIP の枠組みには直接影響を与えない。

5.1.5 Security Mechanism Agreement

RFC3329[14] では、SIP でのネクストホップとの通信において、どのセキュリティのメカニズムを用いるかを交渉する枠組みを定めている。実際のリクエストを送る前に、OPTIONS リクエストを使って、Digest 認証か TLS か IPsec かなど、どれを用いるかの交渉決定をし、それらを用いてセキュリティを確立してから実際のリクエストのやりとりを行う。

5.1.6 S/MIME

SIP では、S/MIME[223] を用いたセキュリティ確保の方法を RFC3261 で定めている。UA は S/MIME による署名と暗号化をサポート可能としており、これに対応することで、E2E での認証ならびに機密性と完全性を提供できる。

5.1.6.1 証明書と署名

エンドユーザを特定するために使用される S/MIME で用いられる証明書は、user@domain に対応するサブジェクトを持ち、通常、From ヘッダの sip:user@domain と対応することになる。

署名が行われる場合は、ボディ部が multipart/signed[92] となり、その中に元のボディ部分と application/pkcs7-signature の分離署名の形となる。暗号化の場合は元のボディ部の代わりに application/pkcs7-mime となる。

5.1.6.2 証明書の検証

受け取った側での署名の確認は、相手の証明書の検証が必要となるので、TLS の時と同様、検証のためにルート証明書を持つ必要がある。これは、TLS 用のものを必要に応じて再利用可能であるべきであるが、S/MIME 専用のルート証明書を持つことも可能となっている。

5.1.6.3 対応すべきアルゴリズム

SIP において S/MIME が用いられるときは、署名アルゴリズムとして RSA、ダイジェストアルゴリズムとして SHA1、暗号化アルゴリズムとして AES を最低限サポート必須であることが、RFC3853[213] において指定されている。

5.1.7 Tunneling SIP

SIP のボディ部に S/MIME を適用することで、その完全性と機密性を保証することができるが、ヘッダ部には有効ではない。一方、SIP では重要な情報を含んでいるヘッダにも適用したいケースが多い。そこで、ヘッダも含めた全体を message/sip という Content-Type として導入し、それに対し S/MIME を適用することで、ヘッダを含めた SIP メッセージ全体をトンネリングする形で、その完全性と機密性を提供する方法が、RFC3261 で定められている。

この場合、SIP メッセージの転送や応答で必須となるいくつかのヘッダは、外側にも置かざるを得ないという点と、転送で用いるいくつかのヘッダは、途中の Proxy サーバが付加したり変更したりするという点に注意する必要がある。

From や To に代替の物を置くことが認められており、とくに、署名だけでなく暗号化も行う場合にはそれらの意味がある。たとえば、外側の From を sip:anonymous@domain と匿名化した場合、受け取ったものはメッセージを復号してから本物の From を取り出し、それを用いて署名を検証したり、ユーザに表示したりすることが必須となる。

5.1.8 AIB

5.1.8.1 目的と概要

message/sip を用いた SIP メッセージ全体をトンネリングする方法を、発信者の識別認証の目的のために用いようとすると、途中で Proxy により変更されるヘッダも含めて不必要なヘッダが含まれていた

り、元のボディまで必ず含まれてるなどといった、曖昧さと冗長の問題がある。そこで、その問題を解決するため、最低限必要となるヘッダのみを含む、AIB（Authenticated Identity Body）というフォーマットが、RFC3893[214] で定められている。

5.1.8.2 AIB の構成要素

INVITE の場合、From、Date、Call-ID、Contact を含むことが必須であり、To、CSeq は含むべき、その他のヘッダは含むのも可能となっている。この AIB の Content-Type は message/sipfrag であり、これは、RFC3420[263] にて、SIP メッセージの一部を表すものとして汎用的に定められている。

5.1.8.3 S/MIME での構成

AIB へ署名したものは、SIP における S/MIME の規定に従い、全体の multipart/signed の中に、AIB 部分の message/sipfrag と、その署名部分の application/pkcs7-signature から構成される。また、SDP（Session Description Protocol）[102] などの、元々の SIP ボディがある場合は、さらに全体を multipart/mixed とする。こうすることで、重要ヘッダについての完全性と認証を提供することができる。

5.1.9 SIP Identity

5.1.9.1 目的と概要

AIB などの S/MIME の枠組みにおいては、発信者認証は、発信 UA が署名をし、着信 UA が検証をするという E2E の利用形態となる。

これに対し、`draft-ietf-sip-identity`[215] において、発信 UA だけでなく、その UA を認証した Proxy が署名できるようにしたり、着信 UA だけでなく、その UA へ転送する Proxy が検証できるようにしたりする枠組みが定められており、そこでは、Identity と Identity-Info という 2 つのヘッダを導入している。

発信 UA 自身、あるいは、その UA を Digest 認証などで認証した、その UA が属するドメインの Proxy は、SIP メッセージのヘッダとボディから一定のルールで生成される文字列に対して署名したものを、Identity ヘッダとして加える。

5.1.9.2 署名

具体的には、From の SIP アドレス、To の SIP アドレス、Call-ID の値、CSeq の値、Date の値、Contact の SIP アドレス、ボディ本体を、すべての間に “|” をはさんで一つの文字列として結合し、sha1WithRSAEncryption[108] にて署名したものに対し、Base64[147] で符号化した文字列を、Identity ヘッダの値とする。また、用いられた証明書を置いた URL を Identity-Info ヘッダ内に記す。

5.1.9.3 検証

着信 UA、または、その UA が属するドメインの Proxy は、Identity ヘッダと Identity-Info ヘッダを見て、署名の検証を行うことができる。発信 UA のドメインと署名者のドメインが一致し、各ヘッダの改竄がないことが確認されることで、その発信 UA によるメッセージであることの正当性が確認できる。

5.1.10 Credential Service

ここでは、`draft-ietf-sipping-certs`[144] において導入されている、Credential Service について述べる。

5.1.10.1 導入目的

E2E での暗号化と署名は S/MIME に依存しているが、エンドユーザの証明書の取り扱いで不便な状況にある。たとえば、あるユーザが、相手にメッセージを暗号化して送付したい時、あるいは、相手からのメッセージの署名を検証したい時に、相手の証明書を入手する必要がある。また、ユーザが複数の機器を UA として用いている場合などに、別の UA 上へ自分の証明書と秘密鍵を取得してきたい場合もある。これらを解決する枠組みとして、Credential Service が導入された。

5.1.10.2 概要

この Credential Service は、証明書の登録や入手といった、すべての機能を SIP の枠組みの中で利用できるようになっており、PUBLISH リクエスト [204] で情報を登録し、RFC3265[228] で定義されているイベント通知機構を用いて、SUBSCRIBE リクエストで要求し、NOTIFY リクエストで配布する。

5.1.10.3 自分の情報の登録

ユーザは自分の証明書と暗号化した秘密鍵を、PUBLISH リクエストで Credential サーバに登録

する。このとき、通常は、REGISTER リクエストなどの時と同様に、TLS 接続した上でサーバ認証と UA の Digest 認証が行われる。

5.1.10.4 自分の情報の入手

あるユーザが、たとえば別の携帯端末を UA として利用していて、自分の証明書と秘密鍵を使うために、その UA 上へ取り出したいときは、SUBSCRIBE リクエストで要求し、NOTIFY リクエストで取得する。このときも TLS 接続してサーバ認証と UA の Digest 認証が行われる。取得した秘密鍵は自分だけが知る鍵で暗号化されているので、復号して用いることができ、Credential サーバには秘匿することができる。

5.1.10.5 他人の情報の入手

他のユーザが他人の証明書を入手したい場合も、同様に SUBSCRIBE リクエストで要求し、NOTIFY リクエストで取得する。このとき、入手した証明書の正当性の確認は、SIP Identity の枠組みを用いて行うことができる。

5.1.11 PAI (P-Asserted-Identity)

署名や証明書を用いずに、ある限定された環境で、簡易に認証情報を伝える方法が RFC3325[145] にて定められている。この方法は、RFC3324[300] で定義されている信頼ドメイン内のみで適用可能で、異なる信頼ドメイン間やインターネット全体にて適したものではない。

新たなヘッダ P-Asserted-Identity が導入されており、たとえば信頼ドメイン内のある Proxy が UA を Digest 認証などで認証すると、そのユーザ情報を P-Asserted-Identity ヘッダとして挿入し、信頼ドメイン内の他の Proxy へと転送することができる。それを受理した Proxy は、信頼ドメイン内では無条件で信頼する形となる。

5.1.12 SRTP

最後に、SIP のセキュリティ機能とは異なるが、今回対象の IP 電話に関係するものとして、RFC3711[17] で定められている SRTP（Secure RTP）を挙げる。

IP 電話では、通話セッションの確立に SIP を用い、その後の音声のやりとりには、RFC3550[247] で定められている RTP（Real-time Transport Protocol）と、その制御用の RTCP（RTP control protocol）を用いる。

RTP および RTCP 自体にはセキュリティ機能がないため、音声の盗聴や改竄などが行われる危険性がある。SRTP はその問題を低いコストで解決し、RTP パケットの完全性や RTP ペイロードの機密性などを提供する。

5.1.13 セキュリティ確保の方法

SIP におけるセキュリティ機能は、直接通信する 2 者間でのセキュリティ確保と、E2E でのセキュリティ確保の、大きく 2 つに分けられる。特に、認証においては、直接通信する相手に対する認証と、発信者 ID に対する認証に分けられる。ここでは、認証、完全性、機密性のそれぞれのセキュリティ確保についてまとめる。

5.1.13.1 認証

UA とその属するドメインの Proxy や Registrar との間では、UA に対する認証は Digest 認証で行い、サーバに対する認証は TLS で行う。この Digest 認証は、通常、発信者 ID に対する認証でもある。異なるドメインの Proxy 間では、TLS により相互認証を行う。異なるドメインの発信者 ID の認証は、SIP Identity で行う。E2E での認証は、発信者 ID に対する認証であり、SIP Identity か、AIB を用いた S/MIME にて認証が行える。

5.1.13.2 完全性

TLS を利用できる場合は、その区間では、メッセージ全体の完全性を確保できる。SIP Identity を用いれば、重要ヘッダとボディは、常に完全性を確保できる。E2E では、ヘッダ部分は AIB への署名、ボディ部は S/MIME を用いた署名で、完全性を確保できる。

5.1.13.3 機密性

TLS を利用できる場合は、その区間では、メッセージ全体の機密性を確保できる。E2E で機密性を確保したい場合は、S/MIME を用いる。

5.2 発信者認証技術

発信者認証（または送信者認証）は、なりすましを防ぐために、SPAM や SPIT 対策において重要な

セキュリティ技術である。発信者 ID の正当性を明確にすることで責任の所在をはっきりさせるとともに、詐称されている場合はそれを見抜くことが可能となる。

同じドメイン内では、少なくともドメインのサーバ側が各ユーザを知っており、各ユーザ別に事前の共有鍵を持つことで、Digest 認証等を用いることができる。一方、ドメインを越えて、異なるドメインの発信者に対する認証は、直接知らない相手に対するものになるため、さまざまな方式が提案されてきている。

ここでは、メールや SIP などの個別プロトコルを越えた全体として、発信者認証技術を 4 つの方式に大きく分類し、それぞれの概要をまとめる。

5.2.1 ユーザごとの公開鍵証明書所有方式

各ユーザが個別に自分の公開鍵証明書を持ち、メッセージを送信する際に、それを用いて発信者が署名をする方式である。この方式は、S/MIME の枠組みにより標準形式が定められている。

5.2.1.1 送信側

事前に、各ユーザが自分の属するドメインから認証を受けるなどして、user@domain に対応する公開鍵証明書の発行を受けておく必要がある。各ユーザにより署名されたメッセージは、HTTP/SMTP/SIP などで送ることができる。

5.2.1.2 受信側

発信者認証を行う受信側では、公開鍵証明書がルート証明書からたどれることを確認するとともに、その user@domain の一致と、署名を検証することで行う。これは、メッセージを受けたサーバ上でも、受信 UA でも、行うことができる。

5.2.2 ユーザ証明書の随時発行方式

各ユーザが必要となるごとに、自分が属するドメインのサーバから、ユーザ証明書の発行を受け、メッセージと共に送信する方式である。この方式は、論文 [159] において提案されている。

5.2.2.1 送信側

事前に、各ドメインがドメインの公開鍵証明書の発行を受けておく必要がある。各ドメインのサーバは、ユーザからユーザ証明書の発行リクエストが来ると、user@domain、時刻、ユーザの IP アドレスのセットに対して署名したものを、ユーザ証明書として発行する。各ユーザがメッセージを送信するときは、このユーザ証明書を添えることで、HTTP/SMTP/SIP などで送ることができる。

この方式では、各ユーザは自分の公開鍵証明書を持たなくてもよく、また、UA での署名処理はなくて、発行されたユーザ証明書を転送するだけになる。

5.2.2.2 受信側

発信者認証を行う受信側では、ユーザ証明書の中の時刻と IP アドレスと user@domain の各々の一致を確認し、署名者であるドメインの公開鍵証明書が、ルート証明書からたどれることを確認するとともに、署名を検証することで行う。これは、メッセージを受けたサーバ自身が行うこともできるし、IP アドレス情報を伝えるなどで、その先の受信 UA でも行うことができる。

5.2.3 付加署名ベースのドメイン認証方式

発信者であるユーザが属するドメインのサーバが必ず中継し、その中継サーバにおいて、ユーザの認証をした上で、署名を付加する方式である。この方式は、SIP Identity の方式で Proxy が署名する場合や、メールでの、DomainKeys[44] と DKIM（DomainKeys Identified Mail）[6] が該当する。

5.2.3.1 送信側

事前に、各ドメインがドメインの公開鍵証明書の発行を受けておく必要がある。各ドメインの中継サーバは、ユーザからのメッセージを受け取ると、ユーザの認証を行い、それが確認されると、ドメインの公開鍵証明書を用いて署名を行って、それを付加して転送する。

5.2.3.2 受信側

発信者認証を行う受信側では、各ドメインの公開鍵証明書を入手確認する必要があるが、SIP Identity の場合は Identity-Info ヘッダからたどり、DomainKeys と DKIM の場合は DNS を引くことで、その情報を入手できる。

各ドメインの署名であることが検証されると、送信ドメイン認証が行われたことになる。各ドメイン

が署名前にユーザ認証を行っているので、間接的に、発信者認証も行えたことになる。これは、メッセージを受けたサーバでも、受信 UA でも、行うことができる。

5.2.4 IP アドレスベースのドメイン認証方式

発信者であるユーザが属するドメインのサーバが必ず中継し、その中継サーバにおいて、ユーザの認証をした上で、その中継サーバの発 IP アドレスの範囲を公開しておく方式である。他の 3 つの方式と異なり、公開鍵証明書は用いられない。この方式は、Sender ID[168] や SPF（Sender Policy Framework）[309] が該当する。

5.2.4.1 送信側

各ドメインの中継サーバは、ユーザからのメッセージを受け取ると、ユーザの認証を行い、確認されれば基本的には他へ転送するのみである。ただし、その転送する際に用いる IP アドレスを、前もって DNS で公開してあるポリシーの範囲内になるように運用する必要がある。

5.2.4.2 受信側

発信者認証を行う受信側、すなわち、そのメッセージを受けたサーバは、発 IP アドレスの範囲がポリシーに従っているかどうかを検証する。そのポリシーは、送信ドメイン側の DNS を引くことで入手できる。

検証されて問題がなければ、送信ドメイン認証が行われたことになる。各ドメインが中継時にユーザ認証を行っているので、間接的に、発信者認証も行えたことになる。

5.2.5 各方式の問題点

S/MIME を用いたユーザごとの公開鍵証明書所有方式は、署名だけでなく暗号化も併用して E2E のセキュリティを提供することができるが、すべてのユーザが事前に個別に自分の公開鍵証明書を持つ必要がある点などが、普及と運用のネックとなっている。

ユーザ証明書の随時発行方式と付加署名ベースのドメイン認証方式では、各ユーザが公開鍵証明書を持たなくてよいが、ユーザが属する各ドメインがその公開鍵証明書を持つ必要がある。

IP アドレスベースのドメイン認証方式と、ユーザ証明書の随時発行方式では、それぞれ、ドメインが用いる IP アドレス、ユーザが用いている IP アドレスに依存する方式であるため、転送などでの少し難しい対応が必要となる。

付加署名ベースのドメイン認証方式と、IP アドレスベースのドメイン認証方式では、所属するドメインのサーバによる中継が必ず必要となり、また、ユーザ認証ではなくドメイン認証である。

5.3 SIP による IP 電話の NAT 越え

現時点では、まだ非常に多くの一般家庭や企業において、NAT（Network Address Translation）あるいは NAPT（Network Address Port Translation）[264] が使われている。NAT の内部のネットワークに、IP 電話機やアダプタがつながれる場合、プライベート IP アドレス [225] の割り当てを受けることになるため、外部との通信をするには、なんらかの NAT 越えのための対応が必要となる。

IPv6 または IPv4 のグローバル IP アドレスを常に使うことができれば、このような NAT 越えのための特別な対応をとる必要はもちろんないが、現実としては、多くの一般家庭の LAN が NAT の内部となっているため、セキュリティ面も含めたアーキテクチャ全体を把握しておくために、ここでは、SIP による IP 電話の NAT 越えについての概要を述べる。

5.3.1 通すべき通信

SIP による IP 電話においては、通常の DNS 解決の他に、セッション確立や制御のための SIP のパケットと、音声やりとりとその制御のための RTP と RTCP のパケットを通す必要がある。

5.3.1.1 SIP

SIP のパケットは、UDP ならびに TLS を含めた TCP の両方があり、UA はサーバにもクライアントにもなりうる。つまり、ウェブやメールの UA の場合とは異なり、UA が自分にやってくるリクエストをサーバとして受け付けられるよう、そのパケットを通すことができる必要がある。自分側のポート番号は標準の 5060 や 5061 以外に自由に自分で決めることも可能である。

5.3.1.2 RTP と RTCP

RTP のパケットは UDP であり、音声のやり取りのため双方向である。RTP のポート番号は、通常、

偶数の番号をとるべきこととなっており、それに 1 を加えた奇数の番号が RTCP のポート番号となる。

5.3.2 必要な記述情報

基本的には、自分の IP アドレス（あるいは、それに解決されるホスト名）と使用ポート番号を、SIP UA は送信するリクエストの中に記述する必要がある。

5.3.2.1 SIP ヘッダ

Via ヘッダには、このリクエストに対する応答を送ってもらう先を記述し、たとえば、Proxy を経由して応答が戻ってくる時などに、それが用いられる。Contact ヘッダには、今後のリクエストを送ってもらう先を記述し、たとえば、通信相手の UA などからリクエストが直接に送信される際に用いられる。

5.3.2.2 SDP

INVITE メッセージでの SIP ボディに記載される SDP において、自分の IP アドレスとポート番号を、記述する必要がある。これが、相手から音声の RTP/RTCP パケットを送ってもらう宛先となる。

5.3.3 NAT 環境での対応

NAT がなく、UA がグローバル IP アドレスを持つ環境においては、自分自身の IP アドレスをそのまま記述すればよく、SIP および RTP/RTCP のそれぞれで用いるポート番号も、UA 自身が開いて待ち受けるものであるため、そのまま記述すればよい。

しかし、NAT 環境において UA がプライベート IP アドレスを持つ場合に、同様にして、その自分の IP アドレスをそのまま記述し、そのメッセージがそのまま外部の Proxy や他の UA に届いたとすると、当然ながら、相手からの通信が自分に届かない結果となる。

したがって、相手に届くまでにメッセージ中のプライベート IP アドレスがグローバル IP アドレスへと置き換えられるような形で対応するか、UA がグローバル IP アドレスを何らかの方法で知って、最初からグローバル IP アドレスをメッセージ中に記述する形で対応するかの、どちらかの方法をとる必要がある。それに加えて、NAT 上を外から内へと自分のところまでパケットが通るように、なんらかの対応をする必要がある。

5.3.4 ALG と B2BUA

UA は NAT の存在を意識せずにプライベート IP アドレスを記述したまま送出し、途中で変換して対応することで、相手にはグローバル IP アドレスの記述が伝わる方法として、ALG（Application Layer Gateway）[30, 265] と、B2BUA（Back-to-Back User Agent）[234] が挙げられる。

5.3.4.1 ALG

ALG は、NAT で IP パケットの IP アドレスやポート番号が書き換えられるのと同様に、SIP や SDP の IP アドレスやポート番号を対応する形で書き換える方法である。リクエストの応答やその後のやり取りもすべて書き換えていく必要があるため、すべてを追って状態を管理するなどの複雑な対応が求められる。

5.3.4.2 B2BUA

B2BUA は、2 つの UA、すなわち役割として、UAC（User Agent Client）と UAS（User Agent Server）が背中合わせに結合されたものであり、UA から来たリクエストを UAS として受信するとともに、UAC として他の Proxy や UA などにリクエストを再生成して送信する。今回の NAT 越えの用途においては、外部と内部の境界上に位置し、内側ではプライベート IP アドレスの記述を用いたやりとりを、外側ではグローバル IP アドレスの記述を用いたやりとりを、それぞれ行う。RTP についても、外側のものと内側のものを中継することで処理を行う。

5.3.5 STUN/TURN/ICE

UA がなんらかの方法で情報を得て、はじめからグローバル IP アドレスをメッセージ中に記述して送出するのが、もうひとつの方法である。その方法のうち、NAT に関係なく、外部との通信によって、グローバル IP アドレスなどの情報を得て利用する方法として、STUN（Simple Traversal of UDP through NATs）[235]、TURN（Traversal Using Relay NAT）[232]、ICE（Interactive Connectivity Establishment）[231] が挙げられる。

5.3.5.1 STUN

STUN では、NAT の内側にいる STUN クライアントが、外部の任意の場所に設置された STUN サー

バと通信することで、外部と通信するときに使われるグローバル IP アドレスとポート番号を取得できる。したがって、STUN 対応の UA は、それらを記述して相手に伝えることができる。ただし、通信する相手に関わらず、自分の IP アドレスとポート番号に対応して、グローバル IP アドレスとポート番号が固定される Cone 型 NAT にのみ適応可能である。また、外側からやってくるリクエストが NAT を通過できるようにするために、自分が内側から外側へ UDP パケットを送信することで、その逆向きのパケットが通るようにする、いわゆる UDP hole punching にも依存し、UDP のみ適応可能である。

5.3.5.2 TURN

TURN は、それらの問題に依存せずに解決する方法であり、外部に設置された TURN サーバが、単純に UDP や TCP の中継を行う。NAT の内側にいる TURN クライアントが、TURN サーバに中継のリクエストをし、それによってグローバル IP アドレスとポート番号を得る。STUN の場合と異なり、得られた値は TURN サーバ上のもので固定であるため、STUN の方法では対応できなかった Symmetric 型 NAT に対しても適応でき、また、TCP でも UDP でも利用することができる。ただし、TURN サーバ上での中継が発生するため、負荷的な面での不利がある。

5.3.5.3 ICE

ICE は、STUN や TURN を利用した、あらゆる環境において適切に通信できるように適用可能とする NAT 越えの枠組みである。ICE においては、UA 自身の IP アドレス、STUN で取得した NAT の IP アドレス、TURN で取得した TURN サーバの IP アドレスを使い分けて、効率よい通信が可能である。

5.3.5.4 SDP での RTCP 属性

以上のような利用方法で NAT 越えを行った場合、変換後は、RTCP パケットのポート番号が、RTP パケットのポート番号と連続にならない場合や、異なる IP アドレスが割り当てられる場合もありうるため、SDP において RTCP 用の IP アドレスとポート番号を指定できるように、RFC3605[111] で拡張されている。

5.3.6 静的設定

NAT に対して設定をすることができ、かつ、グローバル IP アドレスが決まっていてわかっている場合には、静的な設定で利用することができる。

SIP および RTP/RTCP それぞれのパケットのための NAT 変換を設定し、それらに対しては外からのパケットも受け入れるように設定をする。UA 側では、そこでの指定したそれぞれのポート番号で動作するよう設定し、SIP メッセージの中ではグローバル IP アドレスを使うよう設定する。これらの静的な設定により、NAT 越えをすることができるようになる。

5.3.7 UPnP

UPnP を用いると、NAT に対しての動的な情報取得、動的な設定が可能となる。つまり、グローバル IP アドレスの取得と、使用する NAT 変換設定が動的にできる。このためには、NAT が UPnP 対応のルータである必要がある。

具体的には、まず、UPnP の SSDP（Simple Service Discovery Protocol）によって、マルチキャストでデバイス検出のための探索を行い、ルータを発見する。そのルータに対してそのデバイスのサービス情報を取得し、その情報にもとづき、まずは GetNATRSIPStatus アクションで、NAT 環境かどうかの問い合わせを行う。返答で NewNATEnabled が 1 ならば NAT 環境であり、以降はそうであると仮定する。次に、GetExternalIPAddress アクションで、グローバル IP アドレスの取得をする。返答で NewExternalIPAddress にルータの外側の IP アドレスが返ってくる。

最後に、AddPortMapping アクションで、NAT 変換の設定を行う。これは、SIP および RTP/RTCP それぞれについての NAT 変換を設定する必要がある。たとえば、SIP 用の UDP の 5060 番をそのまま内部へもマッピングしたい場合、NewExternalPort で 5060、NewProtocol で UDP、NewInternalPort で 5060、NewInternalClient で自分の持つプライベート IP アドレスを指定する。IP 電話の場合は、同様にして RTP と RTCP 用のポートも設定する。これらの設定は DeletePortMapping アクションで、消去することができる。

このように、UA と NAT ルータが共に UPnP 対応をしていると、事前に設定をすることなく、動的

に NAT 越えのための設定と情報取得ができ、UA は NAT 越えを実現することができる。

5.3.8 方式の比較と現状

あらゆる環境に柔軟に対応するには、STUN や TURN を利用した ICE をサポートするのが望ましい。しかし、現在まだ標準化の作業途中である点と、製品レベルでの対応の点から、現状では普及していない。

企業などでは、ALG や B2BUA を用いて、各自のポリシーで制御しながらファイアーウォールを通過させる方法が適している場合もあり、それらに対応した製品などが使われているケースもある。

一般家庭においては、UPnP 対応ルータの普及が進んだこともあり、UPnP を用いた NAT 越え対応が多く利用されている。そのため、IP 電話アダプタなどで UPnP のみサポートしているものが多い。

5.4 SIP を用いた IP 電話の利用

現在普及しつつある IP 電話のセキュリティ状況について、プロトコルや運用上の問題点がないかを調べてみる必要がある。そこで、一般家庭の普通のインターネット環境で利用できるものについて、国内外のいくつかの SIP を用いた IP 電話サービスに申込んで利用し調査を行った。なお、ここでは特に、PSTN（Public Switched Telephone Network）に接続され、E.164 形式 [136] の電話番号を持つ一般的な IP 電話サービスを取り扱う。

まず、IP 電話サービスを利用する際の設定情報と機器などの接続構成について述べ、さらに発着信を実際に行って、どういう情報がどう伝わるかについて、調査した結果の概要を述べる。そして、それらから判断されるセキュリティ対応状況を示す。

5.4.1 UA での設定情報

IP 電話の利用を申し込むと、ほとんどの場合、電話番号、ドメイン名、サーバ名、ユーザ名、パスワードの設定情報をもらい、それらを UA で設定することになる。

5.4.1.1 電話番号

国内の場合、ここで対象とするのは、050 で始まる電話番号である。050 番号が付与されるためには一定の通話品質を満たす必要があるため、事実上、自分がインターネット接続で用いているプロバイダに依存する形でしか、IP 電話の申し込みや利用をすることができない。

国外の IP 電話サービスを利用する場合、各国それぞれの電話番号が付与される。日本においても利用できるものは、インターネットの利用ができさえすればその IP 電話サービスの利用も可能であるため、インターネット接続で用いているプロバイダには全く依存せずに利用できる。

5.4.1.2 ドメイン名

ドメイン名は、SIP で用いるために設定される。IP 電話では多くの場合、自分の SIP URL は、与えられた電話番号が 050-xxxx-yyyy、与えられたドメイン名が example.ne.jp であるとき、sip:050xxxxyyyy@example.ne.jp としていることが多い。ただし、一部のサービスでは、SIP URL の中に電話番号を用いずに、sip:id123@example.ne.jp といった各自の SIP URL が指定されるケースもある。

5.4.1.3 サーバ名

サーバ名は、UA が REGISTER リクエストで用いる Registrar や、INVITE リクエストなどで用いる Proxy を指定するものとして設定される。ほとんどの場合では両者は同一のものが指定されるが、まれに異なることもあり、UA での設定項目も分かれていることもある。サーバのポート番号はとくに指定されることはなく、標準の 5060 が用いられる。

5.4.1.4 ユーザ名とパスワード

ユーザ名とパスワードは、Digest 認証のために用いられる。このユーザ名は、この目的専用のものとして与えられるケースが多い。これは、セキュリティ上、他と分けることでリスクを回避していると思われる。パスワードは、申し込み時に自分で指定するケースと、IP 電話サービス側から指定されるケースがある。

5.4.1.5 UA 側のポート番号

UA 側において用いる SIP および RTP/RTCP それぞれのポート番号は、IP 電話サービス側からはとくに指定されない。UA によっては設定できず固定に決められているものもあるが、それぞれのポート番号をユーザが指定できるものもある。

5.4.2 DNS の設定状況

各 IP 電話サービスで用いられているドメイン名や SIP サーバ名に対し、DNS での SIP サーバ発見や IPv6 に対応しているかの設定状況を確認した。

5.4.2.1 SIP サーバ発見

一般的に、特にサーバ名が事前に指定されていなければ、指定された自分の属するドメイン名から、DNS を引くことで、UA は RFC3263[233] の方法で Registrar や Proxy などの SIP サーバを発見することができる。

しかし、いずれのケースも、指定されたドメイン名には NAPTR レコード [178] の設定はなく、また、ドメイン名から生成される SRV レコード [98] の設定もなく、DNS を引くことでの SIP サーバ発見には対応していなかった。

5.4.2.2 IPv6 対応

指定された SIP サーバ名には、いずれも AAAA レコード [277] は設定されておらず、IPv6 による利用には対応していなかった。

5.4.3 IP 電話利用のための接続構成

IP 電話を利用するための、機器やネットワークの接続構成は、IP 対応の電話機を用いる場合と、従来からの電話機を用いる場合の、2 つにまず大きく分けられる。また、従来から用いられている普通の電話機をそのまま利用する場合は、IP 電話アダプタか、IP 電話対応ルータのいずれかが別途必要となる。

5.4.3.1 IP 電話機

IP 電話機は、電話機自体が Ethernet などのネットワークに接続できるようになっており、電話機自体が IP パケットをやり取りする。ここではとくに、SIP 対応の IP 電話機が対象となり、IP 電話機自身が SIP UA となる。既にある LAN などに接続すればよく、IP アドレスは固定設定や DHCP 設定などを通常選ぶことができる。それがプライベート IP アドレスの場合は、NAT 対応設定が必要となる。

5.4.3.2 IP 電話アダプタ

IP 電話アダプタは、普通の電話機を IP 電話で用いるためのアダプタであり、電話機を接続できるようになっている。加えて、Ethernet などに接続できるようになっており、SIP を含めた IP パケットのやり取りをし、SIP UA となる。すなわち、普通の電話機と IP 電話アダプタをセットで 1 つと見なすと、IP 電話機と同等になる。したがって、IP 電話機と同様に、既にある LAN などに接続すればよく、IP アドレスは固定設定や DHCP 設定などを通常選ぶことができる。それがプライベート IP アドレスの場合は、NAT 対応設定が必要となる。

5.4.3.3 IP 電話対応ルータ

IP 電話対応ルータは、普通のルータと IP 電話アダプタを合わせたようなものであり、ルータ自身が SIP UA も兼ね、電話機もルータに接続できるようになっている。これを用いる場合は、従来の普通のルータを置き換えて利用することになる。

5.4.4 NAT 越え対応

IP 電話機や IP 電話アダプタが、プライベート IP アドレスの割り当てを受けている場合、NAT 越えのための設定が必要となる。これは、どの IP 電話サービスを用いるかとは関係なく独立の問題であり、使用する UA やルータなどでの対応状況に依存する。

5.4.4.1 STUN の使用例

ある IP 電話機では、STUN による NAT 越えに対応していた。この場合、NAT 越えのために設定すべき項目は STUN サーバの指定だけである。この STUN サーバは外部のインターネット上の任意の場所のもので構わない。SIP および RTP/RTCP のそれぞれについて、ユーザ指定のポート番号をソースとして、STUN サーバへ Binding リクエストが投げられ、その返答として、NAT で変換されたあとのグローバル IP アドレスとポート番号が得られ、それらが記載された SIP メッセージによって NAT 越えがうまく行われていた。

5.4.4.2 UPnP の使用例

ある IP 電話アダプタでは、UPnP による NAT 越えに対応していた。この場合、NAT 越えのために設定すべき項目は、UPnP の利用選択のみである。使用するルータは、UPnP に対応したルータである必要がある。その IP 電話アダプタでは、グローバル IP アドレスの取得の後、SIP 用に 5060、RTP 用に 5090、RTCP 用に 5091 の各ポート番号を、ルータに

も同じポート番号でマッピングするよう毎回リクエストしていた。すなわち、UA 側で用いているポート番号はそれぞれ固定であり、グローバル IP アドレスでも同じポート番号が使用されることになる。それらが記載された SIP メッセージによって NAT 越えがうまく行われていた。

5.4.5 発着信

ここでは、国内のある IP 電話サービスと、国外の IP 電話サービスを利用して、IP 電話から発着信をした時に、どういう情報がどう伝わるかを把握するために、それぞれの例について概要を示す。

5.4.5.1 国内 IP 電話からの発信例

自分に割り当てられた電話番号を 050-xxxx-yyyy とし、ドメイン名を example.ne.jp とすると、INVITE リクエストにおいて、From では sip:050xxxxyyyy@example.ne.jp となっている。発信先を 090-ssss-tttt とすると、Request-URI と To では sip:090ssssttttt@example.ne.jp となっている。この INVITE リクエストは UDP 上で Digest 認証が行われている。発信先の 090-ssss-tttt の電話端末においては、発信者の電話番号 050xxxxyyyy がきちんと表示された。

SIP パケットは、指定された Proxy との間のみで行われ、Record-Route ヘッダ指定により ACK も Proxy 経由となっていた。一方、RTP パケットは、Proxy とは別の IP アドレスとなっており、ポート番号も合わせて、別の通話では変化するなど固定ではなかった。

5.4.5.2 国内 IP 電話での受信例

受信のための前提となる REGISTER リクエストによる自分の位置登録は、UDP 上で Digest 認証が行われている。他の電話（090-ssss-tttt）から電話をかけると、INVITE リクエストが来て、From では sip:090ssssttttt@プライベート IP アドレスとなり、Request-URI と To では sip:050xxxxyyyy@こちらの IP アドレスとなった。このプライベート IP アドレスは、IP 電話サービス側内部のものがそのまま漏れてきているものと思われる。From でも To でもドメイン名は使用されておらず、IP アドレスである。電話を受けた IP 電話側では、090ssssttttt がきちんと表示された。

SIP パケットは、指定された Proxy から発信されてきて、Record-Route ヘッダ指定によりすべて Proxy 経由となっていた。一方、RTP パケットは、Proxy とは別の IP アドレスとなっており、ポート番号も含めて、通話ごとにそれぞれ異なっていた。なお、同じ IP 電話サービスを利用している他の IP 電話との通信では、RTP パケットの IP アドレスは、そのまま相手の IP アドレスとなっていた。つまり、音声は直接通信が行われている。

5.4.5.3 国外 IP 電話からの発信例

国外 IP 電話サービスの IP 電話には各国それぞれの電話番号が与えられるが、ここでは米国のある IP 電話サービスを用いた例を示す。

米国の電話番号 ppp-qqq-rrrr が与えられており、ドメイン名を example.net とすると、INVITE リクエストにおいて、From では sip:pppqqqrrrr@example.net となっている。発信先を日本の電話番号 090-ssss-tttt とすると、米国から見て国外への発信であるため、日本の国番号 81 を含めて、011-81-90-ssss-tttt へと電話をかけることになる。Request-URI と To では sip:0118190ssssttttt@example.net となっている。この INVITE リクエストは UDP 上で Digest 認証が行われている。

日本の携帯電話で受けた場合は電話番号が通知不可能となったりしたが、日本のある IP 電話で受けた場合は、From にて sip:1pppqqqrrrr@domain と届き、電話機での番号表示は 1pppqqqrrrr となった。これは、米国の国番号 1 と米国での電話番号 ppp-qqq-rrrr を意味し、E.164 形式の電話番号表示となっている。

SIP パケットは、指定された Proxy との間のみで行われ、Record-Route ヘッダ指定により ACK も Proxy 経由となっていた。一方、RTP パケットは、Proxy とは別の IP アドレスとなっており、ポート番号のみ、通話ごとに変化していた。

5.4.5.4 国外 IP 電話での受信例

日本からこの電話番号へかける場合、国外宛のための 010 と、米国に国番号の 1 を加えて、010-1-ppp-qqq-rrrr と発信することになる。

日本の固定電話や携帯電話から発信してみると、たとえば、090-ssss-tttt から電話をかけた場合、From では sip:8190ssssttttt@Proxy の IP アドレス、To では sip:pppqqqrrrr@example.net、Request-URI では sip:pppqqqrrrr@自分の IP アドレス、のパケット

が届き、電話機での番号表示は 8190ssssttttとなった。これは、日本の国番号 81 と日本での電話番号 090-ssss-tttt を意味し、E.164 形式の電話番号表示となっている。

一方、日本の IP 電話から発信してみると、From において sip:asterisk@Proxy の IP アドレスとなっているパケットが届き、アルファベット表示にも対応している電話機での番号表示は asterisk となった。これは特殊な例とはいえ、他の例も含め、必ずしも電話番号通知ができているわけではないといえる。

5.4.6 セキュリティ対応状況

通信において用いられているのは UDP であり、TLS は用いられていない。そのため、UA と Proxy の間の通信において、機密性の確保、完全性の確保、Proxy に対する認証が行われていない。唯一、UA に対する認証のみが、Digest 認証によって行われている。

E2E のセキュリティの確保は全く行われておらず、Proxy を含んでそれより先の各 IP 電話サービスと、そこまでの通信路を、無条件で信頼して依存する形となっている。

とくに、かかってきた電話の電話番号、すなわち発信者 ID に対する認証は、Proxy に対する認証が行われていない以上、全く確保されていない。

また、RTP を用いた音声部分においても同様で、認証、完全性、機密性のすべてにおいてセキュリティの確保が行われていない。

つまり、全体として、なりすまし、改竄、盗聴などの危険性があるといえる。

5.5 実利用環境での攻撃実験

ここでは、現在普及しつつある一般家庭向けの IP 電話サービスを実際に利用している環境において、同様に普及している IP 電話機器と、その通信を対象として、セキュリティ状況を調べるために攻撃実験を行った。具体的には、無差別ばらまき着信攻撃、なりすまし攻撃、および、盗聴である。それぞれについて判明した脆弱性の指摘と、問題点と解決方法の概要を示す。

5.5.1 無差別ばらまき着信攻撃

この攻撃方法は、任意の位置にいる攻撃者が、ある一定の範囲を対象に、無差別にばらまく形で IP 電話をかけて着信させる、一種の SPIT 攻撃である。

5.5.1.1 対象とする識別子

攻撃対象とする識別子として、電話番号、SIP アドレス、IP アドレスが挙げられる。

電話番号は、数字だけで構成され、桁数も決まっており、この無差別ばらまき着信の対象に最もしやすい識別子である。IP 電話に限らず、従来の電話においても同様に行うことができるものであり、攻撃とは必ずしも言えないが、電話番号によるランダム調査や営業電話など、この方法の一種と考えることもできる。今回はこれを対象外とする。

SIP アドレスは、メールアドレスと同様に user@domain の形を取り、電話番号を用いない電話から、電話以外の SIP を用いたサービスまで、全てにおいて用いられる。メールにおける SPAM の場合と同様に、乱数や総当たり的に SIP アドレスを生成して用いることになる。そのため、今回はこれをとくに取り扱わない。

IP アドレスも識別子として挙げられる。SIP を用いた IP 電話の場合、着信側の UA はサーバとして振る舞い、待ち受けてリクエストを受け付ける。したがって、メールの場合と異なり、UA に対して直接攻撃が可能となりうる。つまり、IP アドレスを対象識別子として無差別にばらまく形での攻撃を、試みることができる。以降では、この方法を取り扱う。

5.5.1.2 第三者からの直接着信実験

普通に IP 電話サービスを利用している環境における、ある特定の IP アドレスを持つ IP 電話の UA に対して、インターネット上の任意の位置にいる全くの第三者が、直接、その UA に着信させることができるかどうか、すわなち、電話機を鳴らしたり、通話することができるかどうかの実験を行った。

攻撃対象となる IP 電話機には、050-xxxx-yyyy の電話番号が割り当てられており、その番号へ電話をかけると、利用している IP 電話サービスのサーバから、INVITE リクエストが送られてきて、電話機が鳴るのが正常な利用時である。ここでは、第三者が同様の INVITE リクエストを送り、その反応を調査した。

既に述べた調査結果のように、この IP 電話サービスの通常の利用時には、宛先として、sip:050xxxxyyyy@IP 電話機の IP アドレスが、指定されて来る。第三

者から、全く同じ指定をして INVITE リクエストを送信すると、電話機が鳴り、また、通話もすることができた。次に、sip:050xxxxyyyy@他の IP アドレスと、ドメイン部を変更した場合には、404 Not Found が返り、電話機を鳴らすことができなかった。最後に、sip:05000000000@IP 電話機の IP アドレスと、ユーザ部を変更してみると、今度は電話機が鳴り、また、通話もすることができた。

まとめると、攻撃対象とする IP 電話機の IP アドレスさえ指定してあれば、電話機が鳴り、また、通話もすることができることが判明した。これは、攻撃者にとっては、パケットの送り先であり常に既知の情報である。すなわち、攻撃対象に関する事前知識を持たずに、SPIT 攻撃が可能となっている。また、安価なレンタルにて全国で普及して用いられている IP 電話アダプタを使用した場合でも、同様の結果となった。

5.5.1.3 IP アドレス空間総あたり着信実験

IP 電話アダプタ、設置型 IP 電話機、携帯型 IP 電話機などがいくつか接続されたネットワークにおいて、その IP アドレス空間に対し、総当たりで無差別に INVITE リクエストをばらまいて、その反応を確認する攻撃実験を行った。Request-URI と To では、前回の実験の結果にもとづき、ドメイン部分を相手の IP アドレスに指定した。

この攻撃実験の結果、ほとんどの IP 電話機で呼び出し音を鳴らすことに成功した。つまり、無差別ばらまき着信によって、SPIT 攻撃を受けてしまう機器あるいは運用設定が非常に多いことが確認された。

呼び出し音を鳴らすことができなかった IP 電話機を調べてみると、SIP の待ち受けポート番号が、デフォルトの 5060 と異なるものに設定されていた。すなわち、この UA は、Registrar に REGISTER リクエストを送るときや、Proxy に INVITE リクエストを送るときに、自分側のポート番号として、Via や Contact ヘッダで 5060 以外を指定する形で、設定運用されていた。一方、今回の無差別ばらまき着信攻撃は、デフォルトの 5060 へのみ送ったため、この IP 電話機を鳴らすことができなかったことが判明した。

5.5.1.4 問題点と解決方法

このような第三者からの無差別ばらまき着信攻撃を受けてしまう要因として、間接的なものや特例的なものを含めて、4 つの問題点とその解決方法が挙げられる。

1 つ目は、各端末機器の UA が、自分の受け入れるべき SIP URI や電話番号を認知していないことである。実験結果にあるように、Request-URI における SIP アドレスでのドメイン部が UA の IP アドレスと一致さえしていれば、ほとんどの機器が INVITE リクエストを受け入れてしまっていた。解決方法として、自分が受けるべき SIP URI を設定認知させることができれば、今回のように IP アドレスの情報だけでは、攻撃できなくなる。

2 つ目は、SIP のリクエストを自分が受け付ける直接の通信相手を制限していないことである。これは、一般的に SIP では、UA 間の直接通信もあるため、特殊な環境を除けば、常にそのような制限をすることは難しい。しかし、UA 間の直接通信は、既に知り合った者同士でしか発生しなければ、未知の者からのリクエストについてそのような制限をすることは可能である。このとき、リクエストを自分が受け付ける直接の通信相手の制限方法としては、IP アドレスの範囲による認証や、証明書による認証などが挙げられる。

3 つ目は、2 つ目で述べた未知の者からのリクエストを判断する場合も含めて、現状では、第三者が誰であるかに関わらずリクエストを受け付けてる点である。すなわち、誰からのリクエストであるかが明確に判明すれば、ホワイトリストやブラックリストによる制限で、回避することも可能となる。このためには、発信者認証を行う必要がある。

4 つ目は、SIP の待ち受けポート番号がデフォルトのまま固定な点である。これは、必ずしも問題であるわけではないが、実験結果にもあったように、待ち受けポート番号を変更していた UA は、攻撃を免れることができた。もちろん、ポート番号も総当たりされれば攻撃を回避することはできないが、攻撃を受ける確率を下げることができるのは事実である。

5.5.2 なりすまし攻撃

この攻撃方法は、任意の位置にいる攻撃者が、自分の発信者 ID を偽って IP 電話をかけることで、相手を誤認させるという、一種の SPIT 攻撃である。

5.5.2.1 詐称した第三者からの着信実験

普通に IP 電話サービスを利用している環境における、ある特定の IP アドレスを持つ IP 電話の UA に対して、インターネット上の任意の位置にいる全くの第三者が、発信者 ID を詐称しながら、直接、その UA に着信させることができるかどうか、すなわち、嘘の電話番号を相手に表示させられるかどうかの実験を行った。

攻撃対象となる IP 電話機の環境は、第三者からの直接着信実験と同じである。同様に、第三者がそこへ直接 INVITE リクエストを送り、その反応を調査した。送信した INVITE リクエストにおいて、詐称したのは From ヘッダの SIP URI である。たとえば、sip:110@10.0.0.1 としてみると、先の実験と同様に着信した後、電話機の発信者番号表示において、110 と表示された。また、アルファベット表示が可能な IP 電話機を攻撃対象にして、sip:abc@10.0.0.1 として送信すると、abc と表示された。同様に、SIP URI をすべて表示できるものは、すべてがそのまま表示された。

まとめると、今回の実験で攻撃対象として用いられたすべての機器において、攻撃者が詐称したものが、そのまま表示されてしまう結果となった。すなわち、攻撃者は任意の電話番号、または、SIP URI を名乗って、電話をかけて通話することができ、そのような SPIT 攻撃が可能となっている。

5.5.2.2 問題点と解決方法

このような第三者からのなりすましによる攻撃を受けてしまう要因として、特殊な環境での限定例も含めて、2 つの問題点とその解決方法が挙げられる。

1 つは、発信者が名乗った発信者 ID を、そのまま信じている点である。すわなち、発信者認証をきちんと行うことで、詐称を拒絶することができる。これがなんらかの形で行えれば、最も良い解決方法である。

もう 1 つは、SIP のリクエストを自分が受け付ける直接の相手を制限していないことである。これは、一般的に SIP では、UA 間の直接通信もあるため、特殊な環境でなければ、常にそのような制限をすることは難しいが、たとえば、IP 電話サービスの利用といった限定された特殊な環境であれば、決められた Proxy 群からのリクエストしか来ない運用も十分有り得る。このとき、リクエストを自分が受け付ける直接の相手の制限方法としては、IP アドレスの範囲による認証や、証明書による認証などが挙げられる。ただし、現状のように UDP での通信の場合は、容易に発 IP アドレス自体も詐称できるため、IP アドレスの範囲による認証は好ましくない。

5.5.3 盗聴

この攻撃方法は、攻撃者がなんらかの方法で通信パケットを傍受し、誰から誰へ電話がかけられたかといった発呼情報を把握したり、その電話の音声のやりとり自体を盗聴したりする攻撃である。

5.5.3.1 発呼情報の盗聴

利用している IP 電話サービスにおいては、いずれも、SIP メッセージは UDP パケットを用いて暗号化がなされずに流れていた。そのため、それらの IP パケットを傍受できる位置に盗聴者がいた場合、流れている SIP のヘッダ情報から発呼情報をすべて把握することができた。具体的には、いつ、どの電話番号から、どの電話番号へ、発呼されたかである。

これを防ぐには、UDP ではなく TLS を用いて全体を暗号化する方法と、あるいは、S/MIME を用いた Tunneling SIP の方法で暗号化を行い、外に見えているヘッダは代替の物を置くという方法の、2 つが挙げられる。

5.5.3.2 音声の盗聴

利用している IP 電話サービスにおいては、いずれも、音声は RTP パケットがそのまま暗号化がなされずに流れていた。そのため、それらの IP パケットを傍受できる位置に盗聴者がいた場合、流れている RTP パケットから、音声のやりとりをすべて把握することができた。これを防ぐには、RTP の代わりに SRTP を用いる必要がある。

5.6 総括

最後に、ここまでのまとめと結論、および、今後の課題を示す。

5.6.1 まとめ

今回は、SIP と IP 電話のセキュリティ状況について、各種プロトコルなどの技術面と実利用環境での状況の両者において、現状の調査を行い、以下のように、各々の概要のまとめと問題指摘を行った。

最初に、SIP におけるセキュリティ機能を調査して確認し、認証、完全性、機密性といったセキュリティの確保のために、アーキテクチャとプロトコル面でどのような対応が取れるかの概要をまとめた。また、メールの SPAM 対策などでも同様に重要視されている発信者認証技術について、提案されているさまざまな方式を 4 つに大きく分類し、その比較概要をまとめた。さらに、一般家庭環境を含めて実際に避けて通れない NAT 越えへの対応について、SIP を用いた IP 電話の場合の、さまざまな手法による対応方法と比較の概要をまとめた。

次に、SIP を用いた IP 電話サービスを実際に利用し、そこで必要となる各種設定情報や、やりとりされるプロトコルの状況を確認し、実際に発信と受信を行うことで、セキュリティ対応状況などを調査した。また、そのような実利用環境における IP 電話機器とその通信に対して、無差別ばらまき着信攻撃、なりすまし攻撃、および、盗聴の実験を行い、脆弱な状況にある問題点の指摘とそれらの解決方法の概要提示を行った。

5.6.2 結論

今回は中間報告であるが、ここまでの結論としては、次のことがいえる。

まず、現在普及している IP 電話サービスの通信と IP 電話対応機器においては、使用されているプロトコル、各機器における実装、設定運用のそれぞれで、セキュリティ対応面での不備があり、攻撃実験を通して、実際にさまざまな攻撃を受けてしまう脆弱な状況にあることが判明した。

一方、アーキテクチャやプロトコル面では、セキュリティの確保のための様々な枠組みと技術が用意されており、それらをうまく組み合わせた理想的な環境を構築運用できるならば、現状の問題点を解決した形で機能させられる可能性がある。ただし、現時点では詳細検討がまだ不十分である。

5.6.3 今後の課題

今後の課題としては、次のようないくつかの事項が挙げられる。

まず、もし可能であれば、SIP による IP 電話の他のサービスやシステム、および、対応機器類について、範囲を広げてさらなる調査が望まれる。それにより、新たな問題や、他の解決方法が、見つかる可能性がある。同時に、それらの判明した脆弱性に関する正確な情報の普及なども必要である。

次に、既に出ている様々な問題を解決するための技術的な対策を、もっと具体的に運用可能な形で詳細検討していく必要がある。そして、足りない点があれば、新たに付加すべき枠組みなどの提案をしていくべきである。また、実際にそれらの実装と運用を行い、検証と評価をしていく必要がある。

第 6 章　迷惑メールから得られる教訓

IP 電話で用いられる SIP は、電子メールのプロトコルである SMTP を参考に作成されており、類似点も多い。本報告書では、迷惑メールの現状と対策を述べた後、手紙、電話、SMTP と SIP を比較し、迷惑メール対策から得られる教訓をまとめる。

6.1 迷惑電話・迷惑メールの現状と対策

電話の場合、公開されている電話帳や住所録などを使用した迷惑電話や宣伝電話は存在するが、通話にはコストがかかるため、重大な問題とはなっていない。

電子メールでは、迷惑メールは社会問題となっている。電子メールは、発信着信ともに低廉な固定料金で提供されてきた。また、機械的な発信も容易で、ほとんどコストがかからない。そのために低廉な固定料金が、悪者の迷惑メールをエンカレッジしたと考えることができる。

さらには従来の SMTP には発信者を認証する方法がないこと、またユーザ端末からメールサーバへの送信と、ドメイン名を代表するメールサーバ間のメール送信プロトコルが区別されていないことから、インターネットのすべてのホストが迷惑メールを直接送信可能であり、迷惑メールの受信者だけではなく、不正中継や、脆弱性による侵入の結果として迷惑メールの送信に荷担してしまうという被害が発生している。

多くの迷惑メールは、本来のメールサーバではない IP アドレスから、任意の発信者情報を名乗り、メールサーバに接続を行っている。メールサーバでは、明確な判断基準がない限り、すべてのメールを受け取る。

迷惑メール対策として、以下の対策がとられている。

(a) 受け取ったあとのフィルタ処理（内容をみて）
(b) 受け取り時の選別（接続元 IP アドレス、ヘッダ情報）
(c) 送信制限

また、選別処理を正しく行うため、発信者認証が実装されつつある。

発信者認証・送信制限の基本的な考え方は、ドメイン間のメール送信プロトコルと、ドメイン内のユーザが権限のあるメールサーバへ送るプロトコルを分離し、あるドメイン名のメールを SMTP で他ドメインへ送信できるのはそのドメイン名の権限を持つサーバからだけとし、受取り側では送信者の IP アドレスや署名を見て正規の送信者からの接続かどうかを判定することである。ドメイン内では、SMTP Auth などのプロトコルを用いてユーザ認証を行う。

その結果、受取り側メールサーバでは、正しい発信者情報を得ることができる。この発信者情報をもとに、さらに判定処理を行うこともできる。

6.2 迷惑メールから得られる教訓

電子メールと SIP には、

- 低廉な固定料金
- 端末・サーバ間と、サーバ・サーバ間のプロトコルが同一
- 発信者アドレスが自己申告で、認証は別方式

という特徴がある。

低廉な固定料金によるサービスは迷惑電話の原因となりうる。

また、発信者認証技術については、5 によると、提案はされているが、普及していない状況にある。

SPIT についても、迷惑メールで経験した問題が起こりうるため、迷惑メール対策での経験をよく調査し、早めに対策をたてていく必要がある。

第 7 章　まとめと今後の予定

本報告前半では、ENUM トライアルについて報告を行った。来年度には、国際的な ENUM トライアル空間である e164.arpa ドメインでのトライアルを開始する予定である。

本報告後半では、SPIT での脅威の分類と、プロトコル的な分析・機器の脆弱性の確認を行い、迷惑メールとの類似性を示した。来年度には、SPIT への対策方法を検討する予定である。さらに ENUM を運用する場合、ENUM DNS への網羅的検索により、SPIT や迷惑メールの対象となる有効な SIP URI、メールアドレスの入手が容易であるので、URI が容易に漏れる場合の SPIT・迷惑メール対策の検討を行う必要がある。