昭和36年12月15日第三種郵便物認可　平成25年2月1日発行（毎月1回1日発行）　通巻618号　ISSN　1347-6173

CIAJ JOURNAL

COMMUNICATIONS AND INFORMATION NETWORK ASSOCIATION OF JAPAN

2
2013

一般社団法人
情報通信ネットワーク産業協会
Communications and Information network Association of Japan

VoIPセキュリティの現状と今後の動向(前編)

杉岡　弘毅
(株式会社ネクストジェン ネットワーク
セキュリティ事業本部 本部長)

1. なぜ今VoIPセキュリティか

現在，日本国内ではVoIP（Voice Over IP）の利用が急速に進んでいる。総務省が発表した「電気通信サービスの加入契約数等の状況」によると，平成24年9月時点でのIP電話利用数は2982万7000件と，前年同期比10.3%のプラスを示しているのに対し，加入電話契約数（NTT東西以外にCATVによる電話や「直収電話」も含む）は前年同期比で8.9%マイナスの3432万8000件であり，国内のIP電話化を示している。また，近年の特徴として，国内で「LINE」「050 plus」といったVoIPアプリが急速に普及してきており，2005年には数百万人程度であったユーザー数は，2012年12月の時点で加入電話契約数を超える3500万人に達している。今や国民の約4割を占めるスマートフォン所有者の内，7割以上がVoIPアプリを使用する時代なのだ。

VoIPの法人利用に目を向けると，既に国内の半数以上の企業がVoIPシステム／サービスを自社の音声プラットフォームとして利用している（IDC Japan株式会社『2011年 国内ユニファイドコミュニケーション市場 企業ユーザー調査』）。また，業務効率化やコストカットの観点からBYOD（Bring Your Own Device）に対する関心が高まっているが，そのBYODには少なからずVoIPアプリの使用も含まれており，法人向けVoIPサービスの台頭も相まって，今後益々VoIPの利用割合は増加する見通しだ。

このように利用者を増やし続けるVoIPサービスだが，その脅威やリスク，セキュリティ対策については十分な認識が得られないまま使用されている。その結果として，VoIPサービスの不正利用やサービス障害，加入者情報の流出といった事件や事故が起きており，被害が一向に止まない状況となっている。

セキュリティを考える上では，一般的にリスクの評価とその対策が重要な要素となるが，本記事では特にVoIPを利用する上でのリスクを「VoIP機器がもつ脆弱性」や「外部からの脅威」という観点から解説する。なお，以降ではVoIPで使用する技術の中でも代表的なSIP（Session Initiation Protocol），およびRTP（Real-time Transport Protocol）を中心に話を進める。

2. VoIP機器の脆弱性

VoIP機器にはネットワークの境界におかれる「ゲートウェイ（以下GW）」や，ユーザー情報を

収容する「VoIP サーバー」，通話の発信・着信を行う「端末」など，色々な種類の機器がある。以降では，これらの機器に存在する脆弱性を（1）機種に依らず共通して注意すべき脆弱性，（2）機種毎に注意すべき脆弱性に分けて解説する。

□共通して注意すべき脆弱性

共通して注意すべき脆弱性として，「VoIP 機器が不具合を起こしやすいパケットに対応できない脆弱性」について紹介する。この脆弱性は，「ある特定のパターンを含むパケットを受信するとVoIP 機器が不具合を起こす」といったシンプルなものだが，機器の停止等，重大な問題を引き起こす。弊社が実施している脆弱性診断サービスにおいて，この種の問題は診断を行った機器の 8 割以上で検出されており，更に不具合を起こすパターンも 1 機器あたり平均で 3.5 パターン，多いものでは 20 パターン以上を確認している。特に端末や GW において顕著で，多くの問題が検出されている。

ここで言う問題には，機器や一部機能が停止・再起動するといったものから，処理に過大なリソースを消費する，攻撃者に機器の制御を奪われ，乗っ取られた機器が第三者に危害を加えるものまで，幅広く該当する。

先に述べた「不具合を起こしやすいパケット」には多種多様なものが該当するが，大きくは下記の 2 つに分類できる。

- SIP のプロトコル仕様（以下 SIP 仕様）に違反した不正な形式のパケット
- SIP 仕様に違反しない，不具合を起こしやすいパケット

この内，SIP 仕様に違反したパケットには，文字列として表現すべきフィールドが，ASCII 文字ではないバイナリで表現されたものや，SIP 仕様では必須とされている行が削除されたもの，逆に同じ内容の行が複数回繰り返されたもの，などが該当する。図 1 は同じ内容の行が複数回繰り返された例を示している。

```
INVITE sip:11112222@sample.com SIP/2.0
Via: SIP/2.0/UDP 192.168.0.36:5060;branch=z9hG4bK-20121220210154705
From: “88889999” <sip:88889999@sample.com>;tag=8983s
From: “88889999” <sip:88889999@sample.com>;tag=8983s
To: <sip:11112222@sample.com>
Call-ID: 20121220210138983@192.168.0.36
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:88889999@192.168.0.36:5060>
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS
Content-Type: application/sdp
Content-Length:  121

v=0
o=origin 0 0 IN IP4 192.168.0.36
s=-
c=IN IP4 192.168.0.36
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

図 1　ヘッダーの繰り返し例（From ヘッダーを 2 回繰り返し）

SIP 仕様には違反しないが不具合を起こしやすいパケットには，例えば，VoIP 端末が電話番号を扱うフィールドに 2 バイト文字が入っているものや，同フィールドに 50 文字以上の数字が入っているものなどが挙げられる。図 2 は，不具合を起こしやすいパケットの内容例として，正常なメッセージの行末に，特定の文字列が繰り返し挿

入され，1行あたりの文字列サイズが異常に大きいものを示している。

このようなメッセージは，必ずしも悪意を持った攻撃者によるものだけではなく，無線のようにパケットロスしやすい状況での再送や，携帯型端末の電源復帰状態からの処理の不整合など，さまざまな要因で発生する可能性がある。

以上のような「不具合を起こしやすいパケット」により機器が不具合を起こす原因は，主にソフトウェアの実装にある。特にコーディング時に適切に文字列型データを扱っていない，整数を型どおりに適切に処理していない，バッファメモリを保護していないなどの実装により発生する。また，SIPプロトコルの機能を拡張していく中で，セッションの状態に合わせた適切なメッセージ処理が実装できていないことや，SIPプロトコル自身が拡張される過程で，実装条件自体が明らかになっていないことも原因として挙げられる。

□機種毎に注意すべき脆弱性

• GW

GWは，主に電話網とIPネットワークとの間，または異なる電話網の間においてデータの中継の為に使用されるが，本機器のセキュリティ診断において特に多く見られた脆弱性は「SIPメッセージの偽装から起こる問題」に対する脆弱性であった。これは，SIPのリクエストやレスポンスを盗聴し，メッセージを偽装することにより，正規のシーケンスの妨害や，不正なセッションの確立を行えてしまう問題である。

この問題は，通話中に発生するSIPメッセージの正当性を確認していないことに起因していることが多い。よくある事例としては，SIPリクエストに対して認証を要求しない，または，送信元IPアドレスを確認しないというものがある。

• VoIPサーバー

VoIPサーバーとは，ここではVoIP機能を持つサーバー全体のことを指すが，主に加入者情報を有して内線電話同士や公衆回線への接続を行うPrivate Branch eXchange（以下PBX）を思い浮かべて頂ければ良い。このVoIPサーバーにおいては，「DoS攻撃によるVoIPサービスの停止，品質低下」に関する脆弱性が多く見られる。

```
INVITE sip:11112222@sample.com SIP/2.0
Via: SIP/2.0/UDP 192.168.0.36:5060;branch=z9hG4bK-20121220210154705
From: “88889999”<sip:88889999@sample.com>;tag=8983s%s%s%s%s%s%s%s%s
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
To: <sip:11112222@sample.com>
Call-ID: 20121220210138983@192.168.0.36
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:88889999@192.168.0.36:5060>
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS
Content-Type: application/sdp
Content-Length:  121

v=0
o=origin 0 0 IN IP4 192.168.0.36
s=-
c=IN IP4 192.168.0.36
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

図2　巨大ヘッダーの例（Fromを%sで256バイト分パディングする）

DoS（Denial of Service）やDDoS（Distributed Denial of Service）と呼ばれる攻撃手法は，一般的に攻撃対象に大量のパケットを送りつけるものであるが，SIPパケットを大量に送りつけるDoS攻撃が現在非常に増えており，2010年7月には警察庁からの注意喚起も出されている。一般的な企業ではファイアウォールによるネットワークの防御がなされているが，SIPパケットによるDoS攻撃は，SIPの使用ポートに対して送信されるため，正規の通信との区別を付けられず，防御が困難である。また，DoS攻撃のSIPパケットを破棄することや，処理がスタックした場合にシステムを再起動すること等は準正常系の処理として，ほとんどの機器で実装されているはずである。しかし，これらのDoS対策の処理に実装不備があり，攻撃による負荷状態でサービス低下を招いたり，攻撃中のみならず攻撃後もサービスが停止したままとなる脆弱性が存在する。

・端末

機種毎の脆弱性の紹介として最後に，端末における脆弱性について述べる。端末とは，いわゆるSIPメッセージを終端する機器のことで，IP電話機やVoIPアプリなどが当てはまる。この機器については，「不適切なIPアドレスを含むSIPメッセージに関する脆弱性」に注意しなければならない。

この脆弱性は，SIPメッセージ中に処理上問題のあるIPアドレス（ループバックアドレス，自端末のアドレスやブロードキャストアドレスなど）が設定されると，不具合が起こるというものだ。結果的に，音声パケットやレスポンスを自分自身に送信してしまうことで自己ループに陥ったり，あるいは逆に，ネットワークに所属する全サーバーや端末宛てに送信してしまうことになる。ネットワーク全体にメッセージを送信することは，放送用途などでサービス上意図された動作である場合は良いが，そうでない場合はネットワーク全体に無用に負荷をかけてしまうことになり，自己ループ同様，サービスの停止や音声の劣化を引き起こす。

このような不正メッセージにより不具合を起こす原因は，問題の端末がサービスに必要かつ十分なIPアドレスかどうかのチェックを行わない実装となっていることにある。

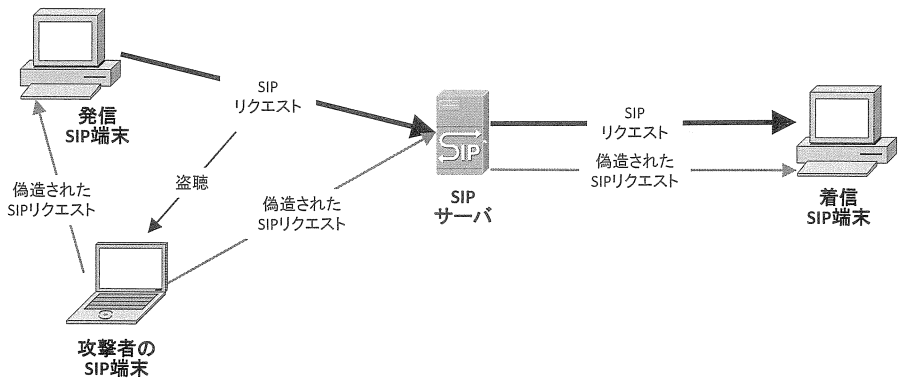

図3　盗聴と偽装

3. 脅威とリスク

□国際不正発呼

本章では，現在確認されている脅威と共に，関連するリスクについて３つ述べる。まず１つ目の脅威として，国際電話番号が発信先番号として記載されたSIPメッセージの送信が挙げられる。この脅威はGWのように「SIPメッセージの偽装から起こる問題」や「送信元IPアドレスを確認しない実装の問題」を脆弱性としてもつ機器を利用する企業にとって危惧すべきリスクだ。というのは，この脅威により，第三者が不正にVoIPサービスを利用した国際電話をかけることができてしまう。さらに，このかけ先はQ2サービスであることが多く，情報料とあわせ正規のユーザーに多大な請求がかかることが多い。

この問題は近年多発しており，最近表面化したものだけでも，表１に記載された事件が起きている。このことを受けて，2012年９月には@niftyフォン-CがIP電話の国際電話不正発信の防止策としてサントメ・プリンシペ民主共和国（アフリカ）への発信規制を行ったり，10月には日本インターネットプロバイダー協会（JAIPA）より，IP電話の不正利用に関する注意喚起がなされたりしている。

該当する機器を使用する企業や機器を作成するベンダの方々は自社のVoIP機器が本脅威に対してどの程度リスクを持っているか，確認してみるのが良いだろう。

表１　VoIP関連の事件

国際不正発呼	
ミシシッピ州デソート群庁舎が通信システムを不正利用される	2012年8月、米国ミシシッピ州デソート群庁舎の通信システムが不正利用され3時間で$23,000の割増し請求が発生。
シスコiosの脆弱性を突かれての不正利用が発覚	2012年4月、欧州のとあるスモールオフィスがCisco製call gatewayを不正使用され、後日通話料$30,000の請求が来た事で発覚。
PBX設置から7日後に不正アクセスされ6時間で約2000ドルの被害	2012年1月、SBCとIP-PBXを用いたハニーポットを置いた実験。ハニーポット設置から7日後にはUserが乗っ取られて不正通話がなされ、6時間で約2000ドルの被害にあう。不正アクセスに対してサービスプロバイダは全く気付かず、クレジットカード会社からの警告により発見
DoS/DDoS攻撃	
SIPを用いたDDoS攻撃が2週間以上継続	2012年10月、米国のCallcentric社に対して2週間以上、SIPを用いたDDoS攻撃が行われ、深刻なサービス障害が発生。
英国テロ対策室に対して電話を通したDoS攻撃	英国テロ対策室であるMI6に対して電話を通したDoS攻撃が行われた。使用されたサーバはAstarisk、SIPを用いて攻撃が行われた模様。
英BBC放送が電話を通じた高度なサイバー攻撃を受けたことを発表	2012年3月、 BBCがイラン向けに提供しているペルシャ語のサービスに対し、高度なサイバー攻撃が仕掛けられていると報じる。複数の攻撃の内、電話を使用したDoS攻撃も行われたことが示唆。
米国TelePacificのネットワークが攻撃を受けてダウン	2011年3月にDDoS攻撃を受け数日にわたってダウン。数十万ドルの被害
SIPサーバの探索	
5060/Udp宛のパケットについてJPCERT-CCが注意喚起	SIPサーバの探索と、脆弱なIDとパスワードのSIPアカウントを調査する目的として5060/UDPを対象とした不正パケットが存在すること、また、送信元である国内拠点が増加していることに言及。
Acme Packet社がSIP対象の攻撃ツールへの注意喚起	SIP攻撃ツール「SIPvicious」がバージョンアップを行った為、サーバのスキャニングやユーザ情報/パスワードの盗難を目的とした攻撃が増加することを警戒。

□ DoS/DDoS 攻撃

次の脅威としては，大量の SIP メッセージ送信，いわゆる DoS/DDoS 攻撃が挙げられる。この脅威は VoIP サーバーのような「不具合を起こしやすいパケットに対応できない問題」や「DoS 攻撃による VoIP サービスの停止，品質低下」を脆弱性としてもつ機器にとって，危惧すべきリスクだ。このリスクが表面化した例として，表 1 のような事件が起こっており，その中でも Callcentric 社になされた DoS 攻撃は，攻撃発覚後も有効な対策を取ることができず，長期間にわたり深刻なサービス障害が発生したことが報告されている。

□ SIP サーバーの探索

最後に，5060/UDP への無差別パケット送信の脅威について述べる。この脅威に関しては，2 段階に分けて攻撃が行われる。まず，VoIP サービスに使用される 5060/UDP ポートへ向けて，ランダムな IP アドレス宛のパケットを送信し，応答を確認する。その後，応答の有ったアドレス宛に様々なユーザー ID とパスワードを設定した SIP メッセージを送信し，加入者情報を奪取する。

この脅威は「送信元 IP アドレスを確認しない実装の問題」や安易なパスワードが設定されているシステムにとってリスクとなりうる。ただし，このリスクは先に紹介した 2 つのリスクと異なり，他の種類の攻撃へ波及しやすい。例えば，SIP サーバーが発見されることで DoS 攻撃の対象となったり，VoIP サービスで使用している ID とパスワードが奪取されることで，その情報が他のプロトコルサーバー（Web サーバーやメールサーバー）への攻撃や認証回避に使用される可能性がある。

4. まとめ

以上のように，VoIP の脅威は他の一般的脅威，つまり，DoS/DDoS によるサービス障害やサービスの不正利用，パスワードクラッキングによる加入者情報の流出といった脅威と同様である。しかし，その脅威がリスクとなるかを決定する脆弱性には，VoIP 独自の仕様や実装が関連しており，VoIP 独自の対策を必要とする原因となっている。この VoIP 独自の対策については，次回「VoIP セキュリティの現状と今後の動向（後編）」にて述べるので是非参考にしてほしい。

今後，VoIP の脅威も他の脅威同様，社会的・政治的な主張を伴うハッキング活動（ハクティビズム）や金銭目的の攻撃が多数を占めることが予想されるが，これは，企業にとってリスクが表面化した際に明確な金銭的被害が生じることを意味する。また，VoIP がインターネットにおけるデータ通信犯罪に使用される機会も増加しており，企業が利用する SIP サーバーが攻撃の踏み台にされたり，電話詐欺に使用されるといった事例が増えている。実際，米国連邦捜査局（FBI）は，犯罪捜査用の通信傍受機能を VoIP システムに組み込むことを課す法律を策定中だ。

国内では，特にモバイル VoIP アプリによって利用が促進される VoIP だが，今こそセキュリティに目を向け安全，安定したシステム利用，機器運用を心掛けてほしい。