昭和36年12月15日第三種郵便物認可　平成25年3月1日発行（毎月1回1日発行）　通巻619号　ISSN　1347-6173

CIAJ JOURNAL

COMMUNICATIONS AND INFORMATION NETWORK ASSOCIATION OF JAPAN

3
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(後編)

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)

VoIPのセキュリティ対策が求められる理由

前回,「VoIPセキュリティの現状と今後の動向(前編)」では,これまで弊社のVoIP診断サービスで見てきたVoIP機器の脆弱性と共に,現在確認されている脅威やリスクについて述べた。その際,「不正な海外向け発信」,「DoS/DDoS攻撃」,「SIPサーバの探索」の3つの脅威については,実際に起こった事件と共にリスクに対する注意を記載した。本記事ではこれらの脅威に対する対策を述べたい。ただし,一口に対策と言っても,実際は対策を行うシステムの規模や対策の度合い,どのような脅威に対する対策か,誰が対策を行うのかといった点によって,取りうる対策は多岐にわたる。そこで,今回は対策を大きく「運用上の対策」と「実装上の対策」の2つのカテゴリに分け,かつ,各脅威との関連付けを行った。VoIPセキュリティを構築する上で,自身が防ごうと思う脅威について,どの対策をどれだけ採用しなければいけないのか,参考にして欲しい。

VoIPのセキュリティ対策

2.1 運用上の対策

本稿でいう運用上の対策とは,社内でVoIPシステムを運用している企業や,社外へのサービスとしてVoIPシステムを運用している企業が,その運用方法の一環として取りうる方策のことである。VoIPシステムを使用する立場の方々に,まず知っておいて欲しい。

アクセス制御

アクセス制御とは,VoIP機器に接続可能なネットワークを限定し,意図しない接続要求を未然に防ぐことである。限定とは,VoIPを使うネットワークと,それ以外のものとを分け,管理・制御することで,これには物理的に行う方法と論理的に行う方法の2種類がある。物理的方法の例としては,Ethernetスイッチの接続ポートやケーブルを,物理的にVoIP機器に対して使用されているものとは異なる機器に収容して分離・隔離することが挙げられる。また,論理的方法の例としてはEthernetのVLAN機能や,IEEE 802.1Xポート認証機能を利用して,端末認証を成功した端末だけが,特定のネットワークに接続できるように強制することが挙げられる。

注意して欲しいのはこの対策が,前回「VoIP

セキュリティの現状と今後の動向（前編）」で述べたSIP（Session Initiation Protocol）やRTP（Real-time Transport Protocol）といった高レイヤーの話ではなく，IPレイヤーやEthernetレイヤーといった低レイヤーで行う対策という点である。SIPにも，自身のパケットが送信されたIPアドレスを通知するヘッダ（Viaヘッダ）が存在するため，必ずしもアクセス制限を低レイヤーで掛ける必要はない。しかし，SIPレイヤーでアクセス制限を掛ける場合，一部のVoIP機器はIPアドレスフィルタのためにSIPメッセージを解釈しようとして，結果的に異常動作，または，スタック状態となることがある。よって，低いレイヤーでスクリーニングを行い，SIPの処理プロセスにまで意図しないメッセージを上げないことが重要である。

この対策はそもそも接続対象を限定することが可能である為，全ての脅威に対して効果が望めるが，対策の性質上，柔軟性に欠けることが欠点であり，VoIPシステムを運用していく上でその他のシステムやサービス（ウェブやメールなど）との協調方法に配慮が必要である。

IPS/IDSの使用

侵入防止システム（IPS: Intrusion Prevention System），および，侵入検知システム（IDS: Intrusion Detection System）をVoIPネットワークに対して用いることで，不正なパケットを監視することが可能である。IPS/IDSの導入により，VoIP機器が不具合を起こしやすい異常な形式のパケットやDoS/DDoSのような異常なトラフィックなど，様々なケースに対応することができる。また，この機器の利点としてウェブやメールといった他の通信への監視とVoIPの監視を同時に行えるということがある。最近は様々なプロトコルに対応したオールインワン形式の製品があるため，利用者が要求するプロトコルが全て揃った製品を見つけることも可能だろう。ただし，IPS/IDSは一般的に侵入検知という機能の関係から設置できる場所が限定される点に注意が必要だ。また，オールインワンのIPS/IDSの中にはVoIP対応となっていても，DoS/DDoS攻撃などの流量の変化しか監視できない製品がほとんどだ。そのため，どの程度VoIPに対応しており，自らが想定する利用方法に対して問題無いレベルかを見極める必要がある。

SBCの使用

セッション・ボーダー・コントローラ（SBC: Session Border Controller）とは，VoIPネットワーク間で使用されるゲートウェイで，主にIPアドレスの変換機能とポートの自動開閉機能を有する。これにより，内部ネットワーク情報の漏洩や未使用ポートの不正利用を防いでいる。また，これらに加えて，トラフィック制御によるDoS/DDoS攻撃からの防御や，不正メッセージの中継拒否も可能だ。事実，アメリカでは通信キャリアだけでなく，企業のVoIP網でも急速にSBCの導入が進んでいる。ただし，先述のIPS/IDSとは異なり，あくまでVoIPに対するセキュリティ製品であり，他のプロトコルに対するセキュリティには別途対策を講じる必要があることに注意して欲しい。

2.2 実装上の対策

次に実装上の対策であるが，こちらは主に

VoIP機器を製造するベンダに目を向けて欲しい内容である。しかし，VoIPサービスの提供者やシステム運用者も，自身の使用するVoIP機器自身にどの程度セキュリティ対策が施されているかを把握するために理解しておくべき内容である。

通信の暗号化（高レイヤー）

SIPについて言うと，TLS（transport layer security）を使用することで，SIPに関する通信を保護し，なりすましや盗聴・改ざんといった意図的な攻撃を受けるリスクを軽減することができる。SIPプロトコルの標準仕様RFC3261で標準化されている。ただし，この場合TLSセッション自身の脆弱性には留意が必要だ。

RTPに関しては，SRTP（Secure Real-time Transport Protocol）やZRTPに対応したVoIPシステムを導入することで，ネットワーク内の通話内容を秘匿することが可能だ。これにより呼の横取りや強制切断といった攻撃にも対処できる。SRTP/ZRTPはそれぞれ，RFC3711とRFC6189で標準化されている。

ただし，TLSやSRTP/ZRTPの利用は他のVoIPネットワーク間では利用できないことが多い。よって，社外との通話に通信事業者経由で接続する為に，UDPベースのSIP，および暗号化されていないRTPに変換するゲートウェイを設置することになる。

通信の暗号化（低レイヤー）

ここでは，3GPP IMS（3rd Generation Partnership Project IP Multimedia Subsystem）標準で，アクセス区間の保護方法として規定されているIPsecについて述べる。こちらは既に述べたTLSやSRTPと異なり，低レイヤーであるネットワーク層での対策だ。

IMS標準のIPsecとは，移動端末と移動端末が最初に接続するSIPサーバまでをIPsecのESPモードで保護するというものだ。ESPモードとはEncapsulating Security Payloadの略で，IPパケットの暗号化とメッセージ署名を行うことで，機密性と完全性を保護する。この対策は盗聴や中間者攻撃（man-in-the-middle attack，MITM）に有効だ。

応答を返さない

大半のVoIP機器は，不正なメッセージを受信すると，「400 Bad Request」レスポンスを返信する。しかし，自社のVoIPネットワークと外部のオープンなネットワークに置かれるGWなど，その機器が不特定多数からのリクエストを受ける可能性がある場合やDoS/DDoSのように大量のパケットを受信する場合は，不正なメッセージを受けてもレスポンスを返送しない方がよい。

レスポンスを返送しない方がよい理由は3つある。(1) リソースの枯渇を少しでも食い止めるため，(2) 攻撃者にVoIP機器の存在や機種，性能に関する情報を収集させないため，(3) レスポンスを返す途中に不具合を起こさせないためである。

以上のように，不正メッセージに対して応答しないという動作の推奨は，ITU-T（国際電気通信連合 - 電気通信標準化部門）のNGNに対する勧告「NGN release.1」のセキュリティ要求条件（Y.2701）にも謳われている。

不正なメッセージに対する試験の実施

一般にファジング(Fuzzing)や耐久試験(Torture

Test), ロバストネス・テスト(Robustness Test)と呼ばれる試験は，ソフトウェアの脆弱性検証や品質担保の為に行われる。特にファジングとは，検査対象のソフトウェアあるいは機器に対して，ファズ(fuzz)と呼ばれる異常なメッセージを次々と入力し，その応答から脆弱性を検証する試験だ。ファジングツールを使用すれば，ファズは自動的に生成され，プログラムによって無作為に入力される。開発者が想定しないような非常に長い文字列やプロトコル仕様上規制されている値などが無作為に入力されることで，人為的に予測することの難しいエラーが発見できる。このファジングをVoIP機器に対して行うことは非常に有効だ。

VoIP機器，特にSIPを利用している機器に存在する脆弱性は，大半が「不具合を起こしやすいパケットに対応できない脆弱性」だ。これは，SIPがテキストベースのためである。様々な文字列を埋め込んだSIPメッセージを送出することが簡単な一方，受診する側の機器にとっては想定外のメッセージとなり，機器の再起動やフリーズを引き起こす。ファジングを行うことでこうした脆弱性を予め無くしておくことができる。SIPについては，IPAより「SIPに係る既知の脆弱性検証ツール」が無償貸出されて（http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html）おり，ここに簡易版ながら数千のファジング項目が含まれているので，まずはこちらを利用するのが良いだろう。

ファジングを行うタイミングとしては，ベンダがVoIP機器またはソフトフェアを出荷する前が最も適当だ。ファジングにより発見された脆弱性を減らす手間について，ベンダ，ユーザ双方の立場で考えてみよう。ベンダの立場で考えると，ソフトウェアの品質の基本的な考え方として，出荷前に確認・修正する手間と，出荷後に修正・パッチを配布する手間との比較では前者の方が望ましいのは当然である。また，ユーザの立場からも，システム導入前にファジングが行われ脆弱性の有無が明らかになる場合と，導入後改めてファジングを行わなければならず，それまでは脆弱性の有無が明らかでない場合とでは，大半のユーザにとっては前者の方が望ましいはずである。

不正なメッセージに対する試験について，更に注意すべき点は，当該機器の追加開発やバージョンアップ毎に，改めて試験を実施すべきだという点である。私の経験上，脆弱性が見つかるのは，後の追加開発で盛り込まれた部分である場合が多い。

2.3 セキュリティに関する情報の収集

VoIPに限ったことではないが，セキュリティ対策を行う上では常に最新の情報を収集することが求められる。この理由として，攻撃者側，対策者側双方の視点で4つ挙げられる。(1) 悪意を持つ攻撃者は常に未発見か，もしくは発見されて間もない脆弱性に対して攻撃を行う，(2) 攻撃者が使用するツールが逐次アップデートされることで攻撃頻度が増加する，(3) 特定の脅威や攻撃には時期による流行りがあり，攻撃頻度の多寡が変化する，など攻撃者側に目を向けた理由と，(4) セキュリティ対策の方法自身が新たに作成される，という対策者側の理由だ。

(1) に関しては，逐次ベンダなどから脆弱性に関する情報が発信されているため，まずはそちらに目を向けることである。加えて，VoIPに関するイベントなどで行われる，脆弱性に関するデモンストレーションにも注意するのが良いだろ

う。ベンダよりも先にイベントによって第3者が脆弱性を明らかにすることは過去何度もあったためである。(2) については，まずどのような攻撃ツールが存在するかをリサーチする必要がある。SIP に関して言えば，SIP サーバの探索などによく使用される「SIPVicious」というツールや，ブルートフォース攻撃に利用される「Bruter」というツールがあるので参考にして欲しい。(3) については，国内の情報処理推進機構（IPA）や日本インターネットプロバイダー協会（JAIPA）などから，セキュリティ勧告や情報の通知が出されており，そちらを定期的に確認すればよい。最近では，JAIPA から 2012 年 10 月に「IP 電話の不正利用による国際通話に関する注意喚起について」という題の報道発表がなされている（http://www.jaipa.or.jp/topics/?p=530）。(4) で述べた新たなセキュリティ対策案については，例として RFC6404 が挙げられる。こちらは 2008 年頃から作成開始された内容が，2011 年 11 月に RFC として取りまとめられたものである。主に，SIP サービスプロバイダ間の通信に対するセキュリティについて記載されており，今後のセキュリティ対策に取り入れられていくと考えられる。

3. まとめ

これまで様々なセキュリティ対策を紹介してきたが，全ての方策を同時に行うことは運用的にもコスト的にも現実的ではない。結局は自分が保護したいシステムに合った方策を選択することになる。例えば，一般的な企業の場合，VoIP 以外のプロトコルについても，同時に対処可能な IDS/IPS を選択することが考えられる。また，コールセンターなどの場合は，より VoIP に適した SBC を選択するほうが妥当である。また，各々の VoIP システムにおいて，システムの仕様によっては，TLS が使用可能（あるいは，不可能）であるかもしれない。

しかし，全てのセキュリティ対策に共通していえることは，(1) 最新情報の収集が常に必要であること，(2) 定期的なシステム点検が必要であることの 2 点である。特に，(2) については，システム内に VoIP 機器を導入する前の試験はもちろんのこと，ネットワーク内のシステムや VoIP 機器が更改されるタイミングで，試験を行うことを強く推奨する。前回の「VoIP セキュリティの現状と今後の動向（前編）」でも述べたが，近年の脅威は社会的・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傾向にあり，ここから導かれる結果として，攻撃手段の高度化とリスクが表面化した際の金銭的被害の発生が考えられる。つまり，コストカットの観点から定期的なセキュリティ対策の更新を疎かにすると，ある日突然，想定以上の額の金銭的被害がおよぶ可能性がある（近年の事件については，VoIP セキュリティの現状と今後の動向（前編）の表 1 を参照されたい）。

これまで非常に安定したサービスが提供されてきた音声通信というインフラが，IP 化に伴って爆発的に利便性が高まっているのが現在の姿であるが，かつてのネットワークサービスの歴史を見てもわかるように，利便性向上による普及，このことが攻撃者の関心増加に伴いセキュリティ事故の事例も増えることは確実だ。本稿の読者の皆様には，利便性と共にセキュリティ対策にも目を向けた上で，VoIP 機器の運用・実装を行って欲しいと思う。