CIAJ セキュリティ Information

VoIP セキュリティの基礎

～IP 電話システムを安心・安全に利用するコツ～

2016 年 12 月 16 日

CIAJ 通信ネットワーク機器セキュリティ分科会

2015 年頃より、IP 電話端末を他社に不正利用され、多額の国際電話料を請求される問題[1)]が発生しています。総務省は 2015 年 6 月 12 日に IP 電話の利用者およびシステムの開発企業、事業者に対して注意喚起[2)]を発表しました。IP ネットワーク上で音声を伝送する VoIP（Voice over Internet Protocol）技術を用いた IP 電話システムや IP 電話サービスは、2000 年初頭頃より実用化されています。2010 年前後より利用者も増え、現在は利用者も 2000 万人を越え、普及期に入ったと言えるでしょう。そのため、IP 電話システムがインターネットでのセキュリティ脅威にさらされるケースが増えてきたと考えられます。IP 電話システムは、ネットワークインタフェースに IP（Internet Protocol）を使用するもののシステムの機能や形態は従来の電話端末や PBX、ボタン電話システムと変わりません。そのため、インターネットシステムでは当たり前のセキュリティ対策や運用上の留意事項が見逃されているため、不正利用などの問題が発生しているケースもあるようです。そこで、VoIP システムとして注意しなければいけない課題と対策について、基礎的なポイントを解説します。

VoIP システムの種類と構成

VoIP システムの基本構成を図 1 に示します。VoIP システムの多くは、SIP（Session Initiation Protocol）という手順に従っています。SIP では、VoIP システムに接続する IP 電話端末を SIP サーバーに登録します。登録時には、使用する電話番号と IP アドレスを対応付けます。このことにより、電話の発信をする場合に、相手先の電話番号から接続する IP 電話端末の IP アドレスを見つけることが出来ます。

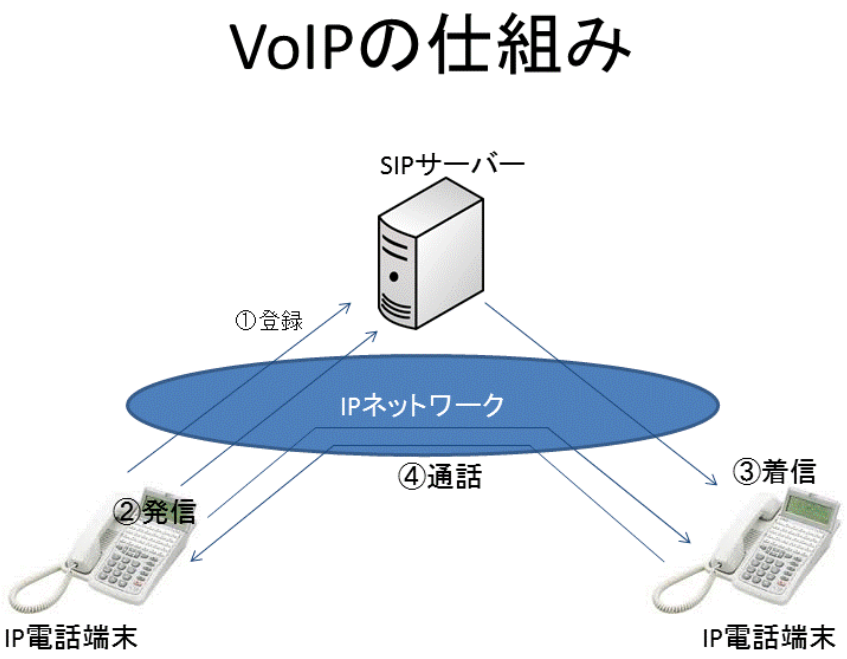


図 1

VoIP システムには、製品の特徴によりいくつもの形態があります。基本的な種類を図 2 に示します。

SIP サーバーは、汎用のサーバーに VoIP 機能をソフトウェアで実装したものです。IP 電話端末は、ルーターやスイッチを介して IP ネットワークに直接接続します。アナログ電話端末や公衆電話網への接続は、VoIP ゲートウェイを介します。

IP-PBX や IP ボタン電話は、従来の PBX やボタン電話システムに IP 電話端末を直接収容することが出来る交換システムです。

VoIP ゲートウェイは、アナログ電話端末や公衆電話網などを IP ネットワークに接続するための変換装置です。

IP 電話端末は、見た目は従来の電話機と同じですが、IP ネットワークインタフェースを有する端末です。

VoIPシステムの種類

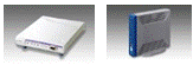
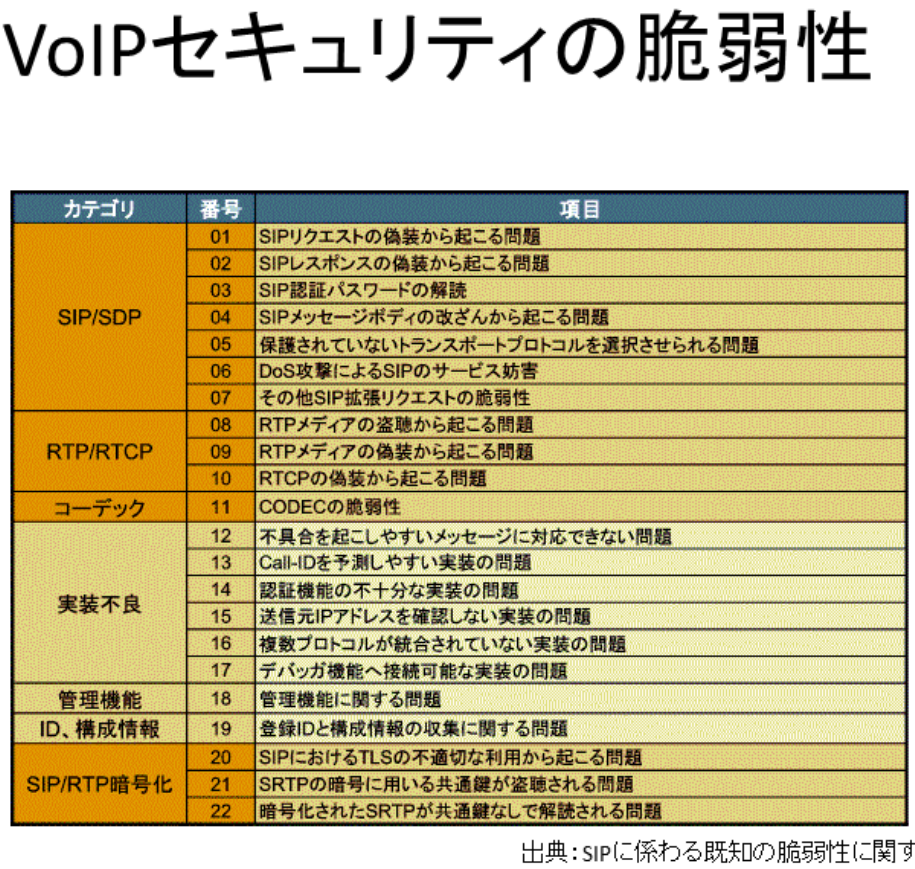
区分	システム	主な機能
VoIPサーバー	SIPサーバー 	IP電話端末の管理、端末間での呼制御を行う
	IP-PBX／ボタン電話 	IP電話端末間および公衆網との間の交換サービスを提供する
VoIP端末	VoIPゲートウェイ 	アナログ電話端末を収容し、IPネットワーク間での音声や信号の変換を行う
	IP電話端末 	IPネットワークに直接接続できる電話端末

図 2

VoIP システムのセキュリティ脅威

図 3 に情報処理推進機構（IPA）が発表している VoIP システムのセキュリティ上の脅威[3]の一覧を示します。これは、SIP というプロトコルの特徴を突いてシステムを攻撃するものです。しかし、VoIP システムを開発している方は理解できると思いますが、一般の利用者には具体的な対応方法を理解するのは困難です。



VoIPセキュリティの脆弱性

カテゴリ	番号	項目
SIP/SDP	01	SIPリクエストの偽装から起こる問題
	02	SIPレスポンスの偽装から起こる問題
	03	SIP認証パスワードの解読
	04	SIPメッセージボディの改ざんから起こる問題
	05	保護されていないトランスポートプロトコルを選択させられる問題
	06	DoS攻撃によるSIPのサービス妨害
	07	その他SIP拡張リクエストの脆弱性
RTP/RTCP	08	RTPメディアの盗聴から起こる問題
	09	RTPメディアの偽装から起こる問題
	10	RTCPの偽装から起こる問題
コーデック	11	CODECの脆弱性
実装不良	12	不具合を起こしやすいメッセージに対応できない問題
	13	Call-IDを予測しやすい実装の問題
	14	認証機能の不十分な実装の問題
	15	送信元IPアドレスを確認しない実装の問題
	16	複数プロトコルが統合されていない実装の問題
	17	デバッガ機能へ接続可能な実装の問題
管理機能	18	管理機能に関する問題
ID、構成情報	19	登録IDと構成情報の収集に関する問題
SIP/RTP暗号化	20	SIPにおけるTLSの不適切な利用から起こる問題
	21	SRTPの暗号に用いる共通鍵が盗聴される問題
	22	暗号化されたSRTPが共通鍵なしで解読される問題

出典：SIPに係わる既知の脆弱性に関する調査報告書（IPA）

図 3

そこで、図 4 に利用者視点での脅威について示します。

例えば、パスワードなど「端末情報の漏洩」により、通信内容が「盗聴」されたり、利用者の端末が「なりすまし」を受けて不正に利用され、多額の通信費が請求されるなどのことが発生します。また、「なりすまし」は利用者の番号を他者が利用することですが、これとは別に VoIP サーバーを「乗っ取り」、正しい利用者が使用できないようにするなどの脅威があります。

では、これらの脅威からどのように VoIP システムを守ったら、良いでしょうか。

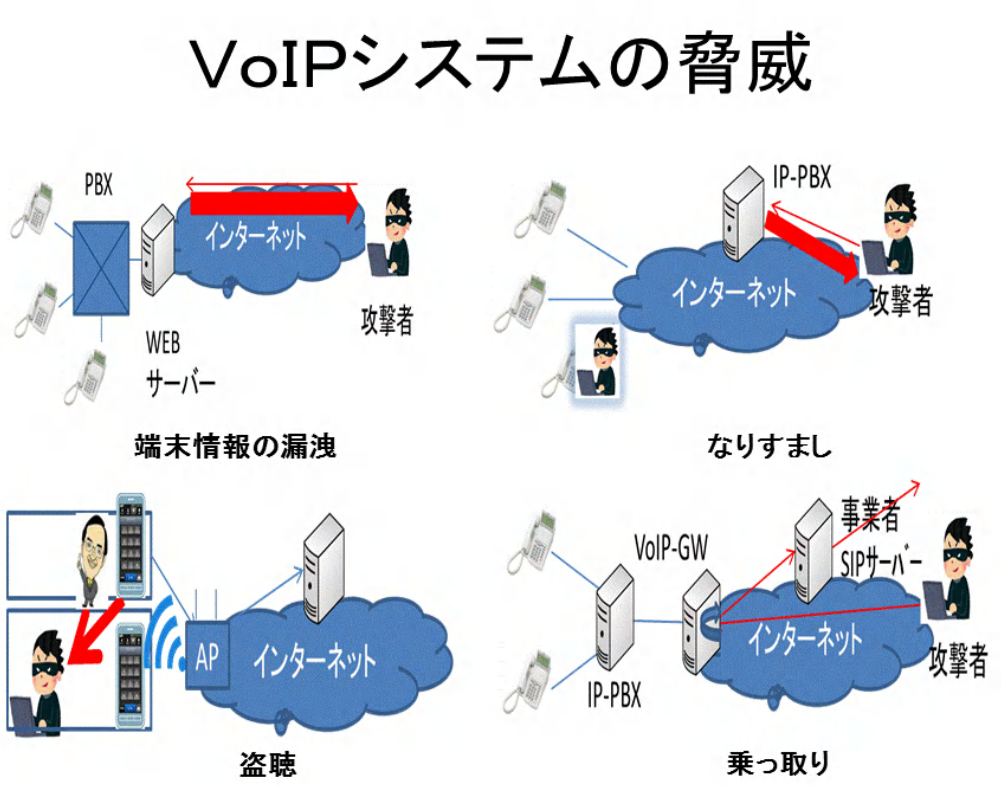


図 4

VoIP システムのセキュリティ対策

まず、「システム設定」が重要です。VoIP システムをインターネットなどの IP ネットワークに使用する際には、正しいセキュリティ設定をしましょう。企業のネットワークにおいて標準の設定条件が示されている場合は、その設定を守りましょう。また、インターネットに直接接続する場合には、使用しないポート（インターネット上のサービス機能の番号）は閉じる設定にしておくのが安全です。

一番重要なのは、「パスワード管理」です。パスワードは、VoIP サーバーの運用管理のためのものや、端末へのログインなどのために設定が必要です。パスワードを初期値のまま使用するのは危険です。初期値は製品ごとに設定されているので、製品名がわかれば、誰でも入手可能です。そこで、パスワードは利用時に変更することが必要です。以前は、パスワードは定期的に変更することを推奨するケースが一般的でした。しかし、最近では定期的なパスワード更新を盗聴するケースも出ているため、パスワードは不定期にかつ頻繁に行うことが望ましいです。

また、システムの運用者は「ログ管理」と「通話履歴管理」を行うことが必要です。

通常時からログや通話履歴を確認することで、日頃使用しない端末からのアクセスや海外発信などを発見することが可能です。

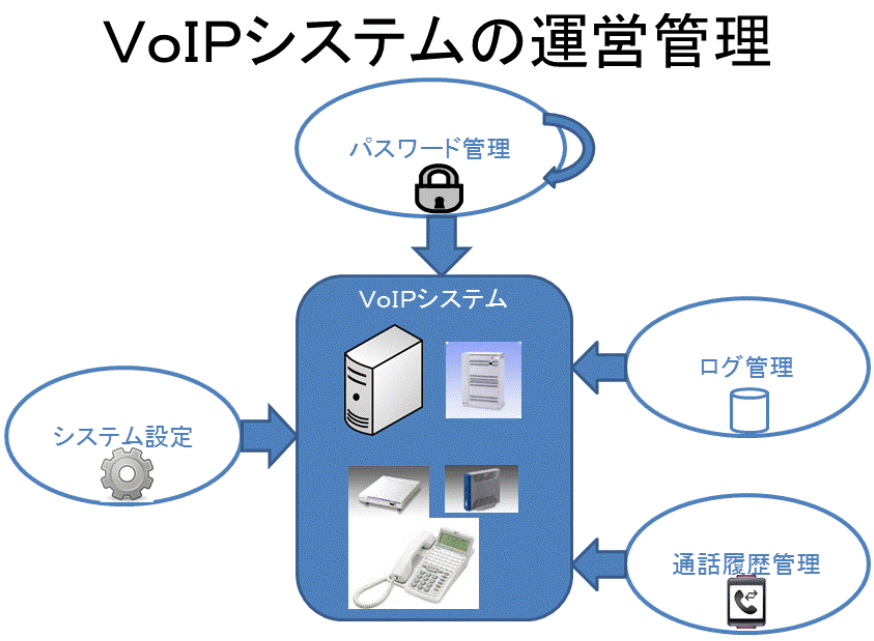


図 5

まとめ

VoIP 技術を用いた IP 電話システムは、普及期に入りセキュリティのリスクも顕在化してきています。しかし、システムの形状や機能は従来の電話システムと変わらないため、セキュリティ対策が甘くなっているケースがあります。そこで、VoIP システムのセキュリティ脅威として、「端末情報の漏洩」、「盗聴」、「なりすまし」、「乗っ取り」の例を上げました。そのための対策として、IP システムとしての「システム設定」を行った上で、不定期かつ頻繁に「パスワード設定」を行い、定期的に「ログ管理」と「通話履歴管理」を行うことが望ましいと考えられます。

IP 電話システムのセキュリティ対策については、開発ベンダや通信事業者あるいは CIAJ などの業界団体から適宜セキュリティ情報を提供しています。これらの情報を定期的に確認することをお勧めします。

著者: 千村　保文（ちむら　やすぶみ）　沖電気工業株式会社（OKI）
プロフィール
沖電気工業株式会社（OKI）　経営企画本部政策調査部　上席主幹、VoIP システムの開発に従事。ITU-T SG16 や TTC（情報通信技術委員会）などで VoIP システムの標準化活動に関与。IP 電話普及推進センタ（IPTPC）の OKI 代表。CIAJ 通信ネットワーク機器セキュリティ分科会委員。

参考文献

1) 総務省研究会資料「なりすましによる IP 電話等の不正利用について」（2015 年 7 月）
2) 総務省 IP 電話の不正利用に関する注意喚起（2015 年 6 月 12 日）
http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html
3) SIP に係わる既知の脆弱性に関する調査報告書(IP ネットワーク上のマルチメディアコミュニケーション・システムのセキュリティ品質向上のために)（2010 年 9 月、(独)情報処理推進機構セキュリティセンター)
4) ボイスオーバーIP（VoIP）アプリケーションのプロテクションプロファイル（2013 年 10 月 21 日、(独）情報処理推進機構セキュリティセンター）
5) IPTPC セキュリティデザイナ・テキスト（第 4 版）
6) なりすまし利用など、第三者による不正なＩＰ電話利用等に関して（ご注意）
http://www.ciaj.or.jp/jp/topics/topics2013/2013/08/07/10849/
7) 「ＩｏＴに対するセキュリティの考察」（日本ＩＢＭ　ＰｒｏＶＩＳＩＯＮ８１）
8) IP 電話普及推進センタ（IPTPC)「攻撃に備える！VoIP セキュリティの実践基礎知識」月刊テレコミュニケーション 2016 年 2 月号