PwC's Cyber Intelligence

狙われるRCS

次世代メッセージサービスが運び込んだ新しくも古い脆弱性

サイバー攻撃では情報量や対象範囲の広さの差から攻撃者が有利な状況であり、CISOなどのセキュリティ担当責任者は、より積極的なサイバー攻撃への防御戦略を策定しなければなりません。PwC's Cyber Intelligenceでは、今後のリスク要因の特定を支援するため、スレットインテリジェンスとその背景にある攻撃者の動向を解説します。

次世代のメッセージサービス、台頭の予感

企業と一般消費者の取引であるB2C（Business to Customer）のコミュニケーションにおいては現在、ショートメッセージサービス（SMS）が最も普及しているツールとされています※1。

一方で、近年このSMSの代替を目的とした高機能なサービスとして、新しいコミュニケーションツールであるRCS（Rich Communication Services）が世界的に活用され始めています。

従来のテキストメッセージのみならず、ビデオ通話やファイルの共有なども可能にするRCSの利用には電気通信事業者（通信キャリア）のサポートが必要ですが、2019年12月、米国では通信キャリアが未対応の場合でも国内でRCSを利用可能としました※2。既に英国やフランス、メキシコでは同様の仕組みで、RCSの提供が開始されています。

日本国内でも大手通信キャリア3社が『+メッセージ』としてRCSサービスを導入し、2018年の3社同時ローンチの時点から、3社間の完全な相互運用性を実現しています。

同3社は、2019年7月にユーザーが1,000万人を突破したことを発表しており※3、またある調査では、2020年の終わりまでに1,750万人にのぼり、2023年までには4,200万人を超えると予測されています※1。また、消費者は受信したRCSメッセージの85%以上を開封し、RCSメッセージからのクリックスルー率はSMSや電子メールの場合に比べて40%以上高くなっているとも言われています※1。

2019年5月以降に発売されたAndroidスマートフォンには+メッセージアプリがあらかじめインストールされており、それ以前のAndroidやiOS向けにダウンロード可能なアプリも既に展開・利用されています※4。+メッセージはレストランや携帯電話販売店の予約といった企業と消費者のコミュニケーションに活用されており、今後は金銭の授受、例えばオンラインショップの決済、電気料金など生活インフラの決済、交通系ICカードのチャージなどに利用が拡大すると考えられます。

企業はRCS公式アカウントを開設することで、アプリの追加開発なしにパーソナライズされたメッセージを消費者に送信でき、インタラクティブにやり取りをすることができます。ユーザー数の増加と高い開封率により、今後、RCS利用企業による消費者とのコミュニケーションを主軸としたビジネス展開が加速すると予想されます。

RCSの出現・台頭によって、企業と消費者とのコミュニケーションの在り方が、大きく変わり始めています。しかし同時に考慮しなければならないことがあります。B2CにおいてRCS利用企業と不特定多数の消費者との金銭のやり取りをも担うであろうRCSは、サイバー攻撃の標的とされる可能性が高いとも考えられるのです。

pwc

*1:日本におけるRCSビジネス・メッセージング（2019年12月、GSMA）
https://www.gsma.com/futurenetworks/wp-content/uploads/2019/12/1-RCS-Business-Messaging-in-Japan-single-combined-low-res-JAPANESE.pdf
※2: Sanaz Ahari Lemelson（Senior Director of Product Management at Google）の発表より
https://twitter.com/sanazahari/status/1205202155650478080?s=20
※3:「+メッセージ（プラスメッセージ）」利用者数が1,000万を突破（2019年8月9日、KDDI株式会社、株式会社NTTドコモ、ソフトバンク株式会社）
https://news.kddi.com/kddi/corporate/newsrelease/2019/08/09/3957.html
*42:「＋メッセージ」の機能を拡充-携帯電話番号だけで、企業と安心・安全にメッセージのやりとりが可能に-（2019年4月23日、株式会社NTTドコモ、KDDI株式会社、ソフトバンク株式会社）
https://www.nttdocomo.co.jp/info/news_release/2019/04/23_00.html

RCSとSMSで異なる通信方式

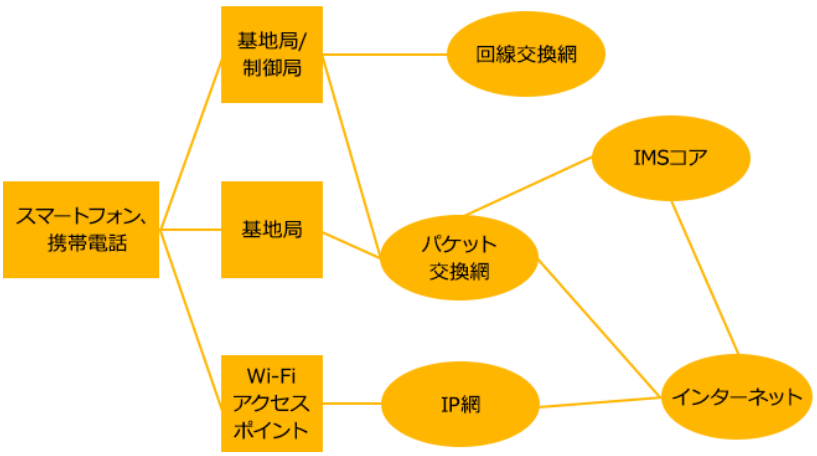
RCSがいかにしてサイバー攻撃の標的になり得るのか、その仕組みを見ていきましょう。RCSは、通信端末を電話番号で識別します。SMSと同様に送信者／受信者は通信キャリアによって事前に審査・認証されるため、安全に使用できると考えられています。

RCSとSMSで異なる部分は、通信方式です。

SMSは、通信キャリアの回線交換ネットワーク（電話に使われる方式）を通信に使用します。一方でRCSは、IMS（IP Multimedia Subsystem）を用いてIP上でHTTPとSIP（Session Initiation Protocol）により実装され、通信キャリアのパケット交換ネットワークを通信に使用します（受信者がRCSをサポートしていない場合は、SMS／MMSでの配信となります）。通信キャリアが提供する回線交換・パケット交換ネットワークで通信をしている限りは、悪意ある第三者が一般的なPC単体で通信を傍受、改ざんすることは困難で、特別な機器や専門知識・技術が必要となります。

しかし、パケット交換によるデータ通信は、自宅や外部のWi-Fiアクセスポイントに接続して行われる可能性があります。消費者の中には、通信キャリアによって制限されている月々のデータ通信量を超えないように、自宅や公共施設など、可能な場所ではWi-Fiアクセスポイントからインターネットへの接続を試みる方もいるでしょう。この場合、RCSプロトコル、アプリケーションの設計・実装次第では一般的なWi-Fiセキュリティと同様、通信の傍受、改ざんなどのリスクが生じる可能性があります。

図1.回線の全体像



セキュリティリスクが存在するWi-Fiインフラを消費者が知らずに利用する可能性

Wi-Fiインフラのサイバーリスクを消費者の観点で見た場合、大きく2種類の古典的な脅威源が存在します。

1つ目は、脆弱なWi-Fiアクセスポイントの利用です。これはオープンシステム認証、WEP（Wi-Fi Protected Access）のような脆弱な暗号化・認証方式や、事前共有鍵が事実上公知な状態で運用されているアクセスポイント（カフェなどで散見される）の利用、アクセスポイント自体がアクセス制限不備やセキュリティパッチ未適用などの脆弱な状態で運用されており、それを利用してしまうといったケースが挙げられます。

2つ目は、悪意あるWi-Fiアクセスポイントの利用です。悪意ある第三者が正規アクセスポイントを装った偽のアクセスポイントを設置し、ユーザーがだまされて当該アクセスポイントに接続してしまうケースが挙げられます。

こうしたケースでは、攻撃者によるWi-Fi通信の盗聴、改ざん、なりすましの攻撃を受ける可能性があります。対策としては、HTTPS、VPN（Virtual Private Network）の利用などが挙げられます。

しかし上述のような脅威と対策は、あくまでWi-Fiインフラを利用する消費者観点のものです。RCS利用企業は、消費者がRCSの通信にどのような通信やインフラを利用するかを選択・制限することはできません。そのため企業は、RCSを利用したサービスをプランニングする段階から、こうした脅威の全体像を踏まえてサービスを設計することが求められます。

RCS特有のセキュリティ上の懸念事項

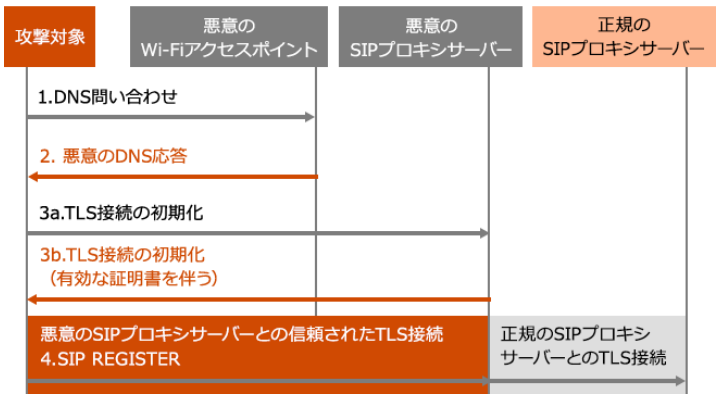
Wi-Fiインフラにセキュリティリスクが存在する場合でも、End-to-Endの強力な暗号化が施されていれば、一般的に通信を傍受されることはありません。しかしRCSでは、RCSクライアントとサーバー間でのTLSによる通信の暗号化はサポートされているものの、クライアント間でのEnd-to-Endの暗号化は提供されません。そのため、原理的にはRCSサーバーおよび経路上で中継・保存される通信データを盗聴される可能性があります。SMSでは、SMSクライアントからのデータを受信するSMSC（SMSセンター）サーバーを標的とした攻撃が報告されており※5、RCSでも今後、同様の攻撃が発生することが想定されます。

また2019年、ドイツの研究機関SRLabs※6によってRCSの実装の一例が検証され、世界的に普及するRCS対応のアプリでさえドメインと証明書の検証が十分とは言えず、DNSスプーフィングによる比較的単純な中間者攻撃によりRCSのテキスト／通話の傍受や改ざん、発信者IDのなりすましなど、RCSハイジャッキングが可能である、と指摘されました※7。

加えて、多くのネットワークではRCSの機能をアクティブにするためのプロビジョニング（SIM＜加入者を特定するためのID番号が記録されたICカード＞を利用した認証および初期設定）プロセスが十分に保護されていないため、攻撃者はSIPおよびHTTP資格情報を含むRCS構成ファイルを盗み、ユーザーアカウントを完全に乗っ取ることが可能とも指摘されています。これらは、RCSがSMSと同じ通信方式であれば問題視されなかったでしょう。しかしRCSはIP上で実装され、消費者はWi-Fiインフラを介してRCSサーバーに接続する可能性があります。この例では、Wi-Fi環境下におけるRCS通信に対して従来の攻撃手法が転用されたと言えます。

このことから、Android端末にプリインストールされるRCSがWi-Fiセキュリティ上の懸念を拡大させ、スマートフォンを利用するほぼ全ての消費者を、SMSでは心配する必要が無かった脅威に晒すことになった、との声も聞かれます。こうした事態に、SRLabsは強い懸念を示しています。

図2. 攻撃のイメージ



RCS利用企業が実施を検討すべき、セキュリティ上の問題の軽減策

SRLabsが指摘した脆弱性はあくまで実装上の問題であり、RCSを展開している各国の通信キャリア全てが同じ脆弱性を持つとは言えません。しかし、実装の問題で同じ脆弱性が発生し得るのであれば、RCS利用企業は常にこの問題を念頭に置いて、サービスを開発・展開・運用する必要があります。

SRLabsは通信キャリア向けに、ベストプラクティスとして以下のリスク軽減策を提言しています。

- SIMやセキュアエレメントを利用した認証、強力なパスワードの利用など、プロビジョニングプロセスの保護
- 送信元IPアドレス、Cookieなどに基づいたSIPセッションの検証、通信データからの機微情報の削除、アップロード制限などのRCSサービス上の対策
- 信頼できるドメイン／証明書のみ接続を許可し、信頼できる証明書の連鎖（Chain of Trust）を使用するなどの、RCSクライアント側の対策

RCSは今後も利用拡大が見込まれるため、サービスの普及と共に新たな脅威が明らかになる可能性があります。RCS利用企業は、こうした脅威動向、さらには国内の対応動向を認識した上で、RCSを利用したサービスを設計・運用していくことが重要となります。

*5:FireEye
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html
*6: Security Research Labs
https://srlabs.de/
＊7:The Future of Texting Is Far Too Easy to Hack（2019年12月4日、WIRED）
https://www.wired.com/story/rcs-texting-security/

今回のポイント

1

RCSはSMSと異なり、Wi-Fi接続を介したインターネット経由で通信される場合がある。この通信環境、RCSの実装次第では、盗聴・改ざん・なりすまし攻撃を受ける可能性がある。

2

ドイツでは、RCS実装の不備を悪用した攻撃実証が既に報告されている。

3

RCS利用企業は、脅威動向及び国内の対応動向を把握し、キャリアと連携してサービスを検討することが必要である。

執筆者

名和　利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

林　和洋

PwCコンサルティング
合同会社
パートナー

岩井　博樹

PwC Japan グループ
スレットインテリジェンス
アドバイザー

村上　純一

PwCコンサルティング
合同会社
ディレクター

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html