Technology Reports

SMS　フィッシング　セキュリティ

SMSを用いたフィッシングを防止する検知・防御技術概要

ネットワーク開発部　岩井 遼太（いわい りょうた）　原田 翔（はらだ しょう）
久保 耀介（くぼ ようすけ）

近年，SMSから偽のウェブページにアクセスするよう仕向けられ，情報を盗み取られるフィッシングの被害が拡大している．手口も多様化，巧妙化しており，フィッシングSMSと受信者が気付くことも容易ではなくなりつつある．そこでドコモは，ユーザがSMSを受信する前にそれがフィッシングSMSかどうかを判定し，フィッシングSMSであればユーザへ送信する前に破棄することで被害を防止するシステムを開発した．本稿ではその技術概要を解説する．

1. まえがき

近年，実在する有名企業やサービスからのメッセージを装ったSMS*1（以下，フィッシングSMS）により，偽のウェブページへ誘導させられ，ユーザ情報やクレジットカード情報を盗み取られる，あるいはマルウェアを端末にダウンロードさせられるなどのSMSを用いたフィッシング被害が拡大している．偽のサイトに誘導する手口も巧妙化しており，宅配業者の不在通知を装ったメッセージや，携帯電話料金の未払い通知を装ったメッセージなど，本文やウェブサイトを見ただけでは，実際に利用しているサービスのサイトであるか，あるいはフィッシングサイトであるかの区別をすることが極めて困難なケースも存在し，被害規模も拡大している状況にある．そこでドコモでは，ユーザが希望する場合において，SMSを受信する前にフィッシングSMSかどうかをドコモにて自動判定し，フィッシングSMSである場合は，ユーザへ送信する前に該当のSMSをドコモネットワーク内で破棄することで，フィッシングSMSの被害を防止するフィッシングSMS検出・防御システムを開発した．本稿では，その技術概要について解説する．

*1　SMS：主に移動端末同士でテキストベースの短い文章を送受信するサービス．

2. フィッシングSMS検知・防御システムのアーキテクチャ概要

2.1 ネットワーク構成

ネットワークの全体構成を**図1**に示す．ドコモは，独自のフィッシングSMSに関するDBをもち，フィッシングSMSであるかどうかを判定する機能を具備するシステムであるSMSI（SMS Inspector）*2を新たに構築した．また，SMSの中継・蓄積・配信を行う役割をもつSMS-GMSC（Gateway Mobile Switching Center）/SMS-Router*3にSMSIと接続するための新規のインタフェースを設けることで，従来のSMS処理を行うネットワーク基盤とSMSIとの連携を行う．SMS-GMSC/SMS-Routerは，全国のドコモ拠点をつなぐ専用ネットワークであるドコモIPルータ網を介して，SMSIと接続する．なお，全国のドコモ設備を監視するシステムであるドコモO&M（Operation & Maintenance）システムとSMSIに関してもドコモIPルータ網を介して接続を行い，装置監視および運用・制御を行う．

2.2 基本制御方式

フィッシングSMS対策機能の処理を含む，SMS制御に関する処理シーケンスを**図2**に示す．SMS標準で規定される処理［1］に対して，新たにフィッシングSMSに関する判定および破棄の処理を追加し，それらを基本制御方式にて実装している．まず，SMS-GMSC/SMS-RouterはSMSをユーザへ送信する前に，加入者情報を参照し危険SMS拒否設定の利用有無を確認する（図2②）．なお，危険SMS拒否設定の利用有無の確認は，既存機能である加入者情報の収集／応答とともに行うよう実装しており，処理にかかる時間は既存のSMS送信とほとんど変わらない．危険SMS拒否設定利用が有効である場合は，SMSに含まれるヘッダ情報や本文情報などを用いて，フィッシングSMS検知問合せメッセージを作成しSMSIへ送信する（図2③）．なお，SMS-GMSC/SMS-RouterはSMSそのものをSMSIへ送信

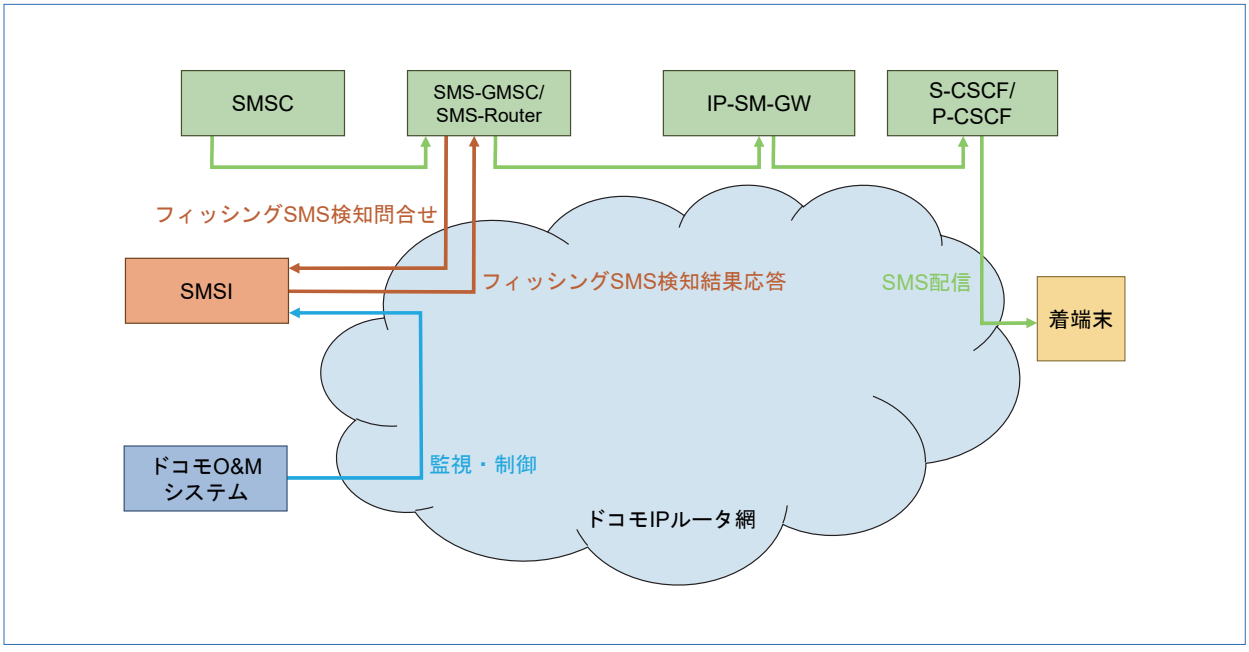

図1　ネットワーク構成

＊2　SMSI：独自のデータベースを用いたフィッシングSMS判定処理を行う装置．

＊3　SMS-GMSC/SMS-Router：SMSセンタサーバとSMS送受信ユーザの在圏交換機との間にあり，信号のルーティングを担う装置．

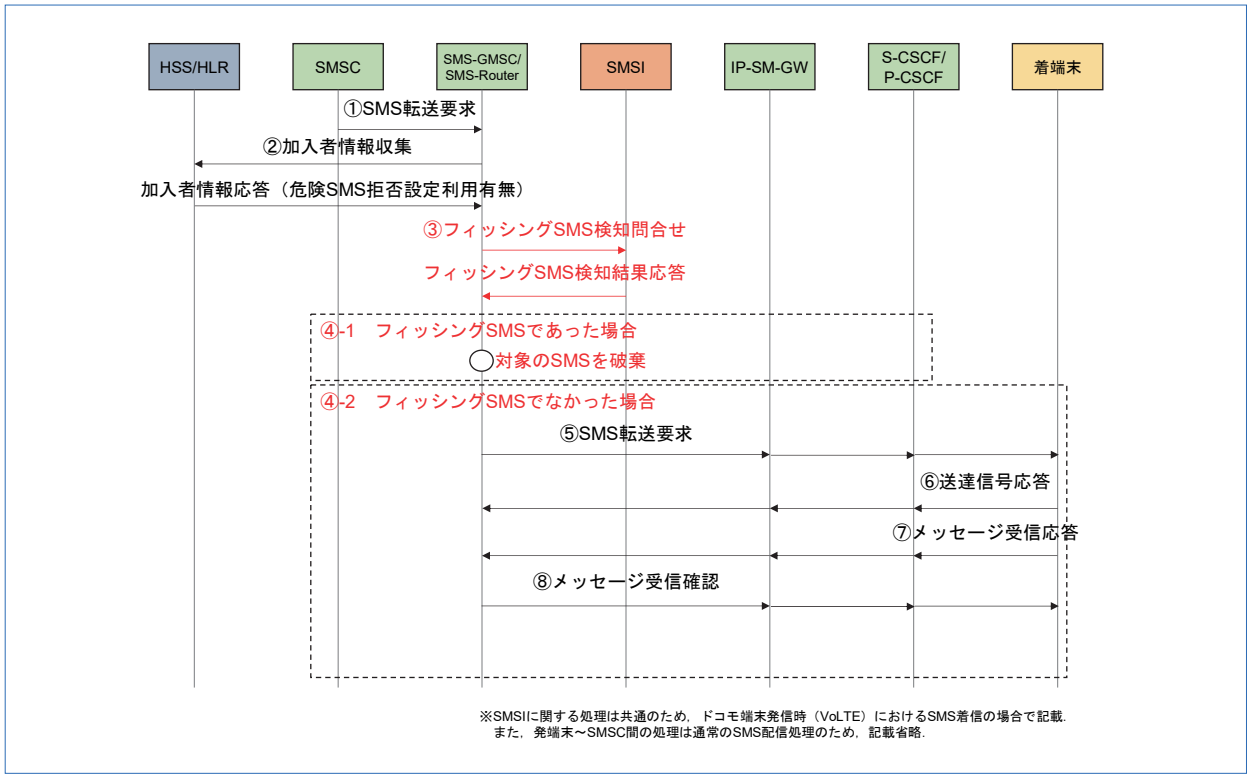

図2　SMS制御処理シーケンス

するのではなく，SMSメッセージのプロトコル変換によりフィッシングSMSであるかどうかの判定のリクエストメッセージを生成し，送信する．SMSIは，全国に設置された各SMS-GMSC/SMS-Routerからのフィッシング SMS検知問合せメッセージに対して，独自のデータベースを用いたフィッシングSMS判定処理を実行し，フィッシングSMSである，あるいはフィッシングSMSではない，という判定処理結果を，フィッシングSMS検知結果応答メッセージとして問合せ元のSMS-GMSC/SMS-Routerに送信する．フィッシングSMS検知結果応答メッセージを受信したSMS-GMSC/SMS-Routerは，該当のSMSがフィッシングSMSであった場合は破棄を（図2④-1），フィッシングSMSでない場合は，従来のSMS制御処理に基づき，配信を実行する（図2④-2）．なお，SMSI異常動作時にSMS配信不可となることの無いよう，SMS-GMSC/SMS-RouterはSMSIアクセス不可時の処理機能を実装している．本機能はSMSIからの応答がない場合，あるいは，SMSIからのフィッシングSMS検知結果応答メッセージの内容が適切でない場合は，保守者へ通知するとともに，一時的にフィッシングSMS検知問合せメッセージの送信を停止し，従来どおりSMS配信を実施する．さらに，SMS-GMSC/SMS-Router側で信頼できるSMSメッセージとして定義されたSMSに関しては，SMSIへの問合せを省略することができる機能を具備している．信頼できるSMSメッセージかどうかの判定では，SMSの複数のパラメータにさまざまな判定ロジックを組み合わせて行うことで，細やかな制御が可能となり，SMSIの負荷を50％以上軽減するなど，SMSIの判定処理の高速化および負荷軽減を実現している．

2.3 フィッシングSMS判定処理更新手法

SMSIはフィッシングSMSに関する独自のデータベースを保持しており，複数の判定手法により各SMSがフィッシングSMSかどうかを判定している．データベースには大量のデータがあり，あらゆるフィッシングSMSに対応しているものの，フィッシングの手口は社会のトレンドなどを取り込み，常に変化しており，多様化・巧妙化を続けているため，それに追随してデータベースを更新する必要がある．しかしデータに誤りがあると，フィッシングSMSを見逃すなどの不具合が発生する恐れがあり，データベース更新の前にそのデータが妥当か検証する必要がある．そこでドコモでは，複数のチャネルから収集した新規のフィッシングSMS情報に対して，データベースへの反映を実施する前に，その妥当性を評価するための手段を保持している．新規のフィッシングSMS情報に関する評価手法を**図3**に示す．複数のチャネルから収集したフィッシングSMS情報（フィッシングSMSそのものや，フィッシングサイトのURL情報など）を基に，試験SMSIの検知ルールDBおよびシミュレータのテストデータをそれぞれ同時に更新する（図3①）．なお，このシミュレータはSMS-GMSC/SMS-RouterからSMSIへのフィッシングSMS検知問合せメッセージを作成，送信する機能，およびSMSIからのフィッシングSMS検知結果応答メッセージが想定される結果であるかを評価する機能を具備している．更新されたテストデータは試験SMSIを通して判定処理され，シミュレータは既存のフィッシングSMSと追加したフィッシングSMSの判定処理の評価を行い（図3②），適切な結果が得られた場合に，実際にユーザのSMSに対して判定処理を実施している商用SMSIのデータベースへの適用を実行する（図3③）．ドコモでは，本評価手法を自動化する専用のシステムを独自に開発・構築しており，本自動化システムにより最小の工数・期間で試験を実施することができ，これにより新規手口発生時にも速やかに対応することが可能である．

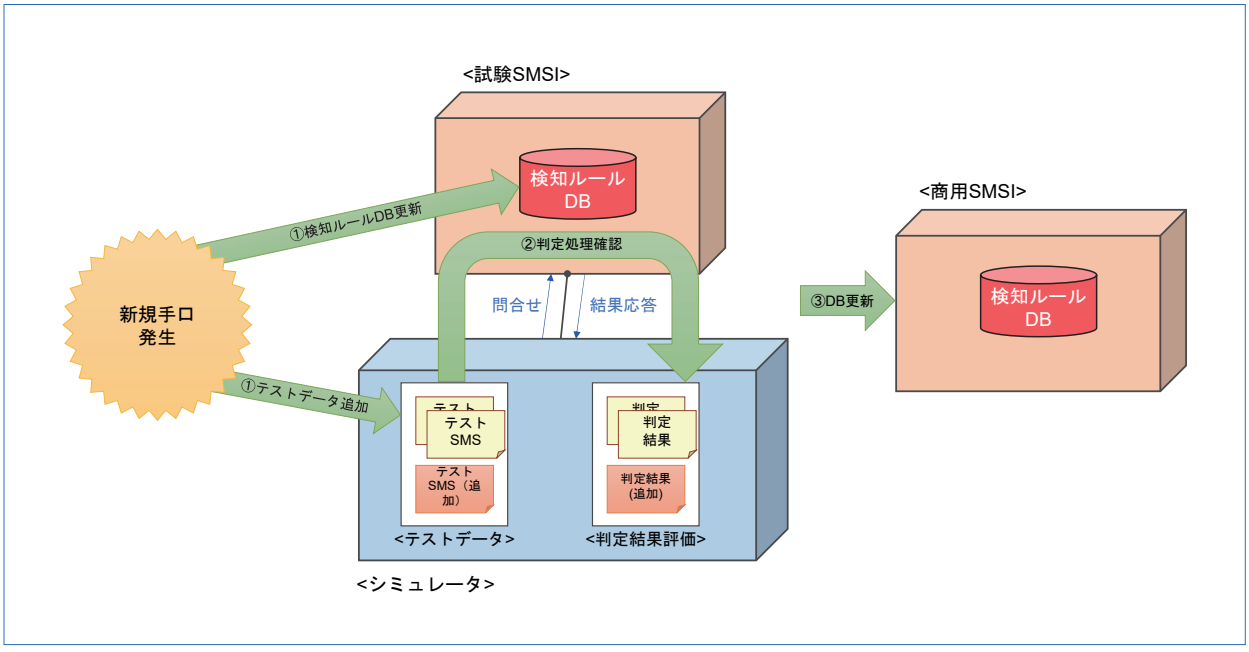

図3　新規フィッシングSMS情報に対する評価手法

3. あとがき

本稿では，フィッシングSMSをネットワーク内で判定し，フィッシングSMSである場合は破棄をすることのできるフィッシングSMS検知・防御システムに関する技術概要を解説した．ドコモは情報通信業界や官公庁，金融機関などと合同でフィッシングSMS被害者削減に向けたスミッシング*4対策ワークショップを定期的に開催しており，社会全体でのフィッシングSMS対策に取り組むとともに，今後も新規フィッシングSMS情報の収集に関する関連技術との連携や新規手口に対する対策技術の高度化，フィッシングSMS判定精度の強化などを通じて，継続的にフィッシングSMS対策を実施していきたい．

文　献

[1] 3GPP TS23.040 V17.1.0：“Technical realization of the Short Message Service (SMS),” Jun. 2021.

*4　スミッシング：SMSを用いたフィッシング詐欺のこと．