スミッシングの実態と対策

株式会社マクニカ
ネットワークスカンパニー　第2技術統括部
テレコムセキュリティサービス室
室長　鈴木 一実
主幹　丸山 一郎

Co.Tomorrowing
MACNICA

目 次

はじめに

本資料は、スミッシング対策に取り組む方々にとって、より広い視点と、技術的な理解につながるよう願って執筆しました。これまでのサイバーセキュリティー対策と違い、スミッシング対策には、サイバー犯罪としての視点、生活インフラとしての携帯電話・スマートフォンに関わる背景知識が必要です。また自社の情報資産を守るための IT セキュリティとは違った難しさもあります。こうしたことを踏まえ、マクニカが実施している通信インフラのセキュリティ対策支援、サイバー犯罪調査活動の知見に基づき、スミッシングの裏側を解説します。

スミッシングについて

スミッシングは、フィッシング（Phishing）行為の一種であり、SMS Phishing から生まれた造語です。携帯電話のショートメッセージサービス（Short Message Service = SMS）を使って詐欺目的のメッセージを送り、受信者を偽の Web サイトに誘導、個人情報を盗み取ります。狙われるのは主に、銀行、EC サイトのアカウント情報、電子決済やクレジットカード利用に関わる情報などです。取得した情報は、本人になりすました不正送金や不正出金、EC サイトでの商品購入、クレジット不正決済など犯罪行為に使われます。

スミッシングには、 SMS が携帯電話の加入者と紐づいていることに由来する特徴があります。それが犯罪の広がりや傾向に表れ、また、攻撃手法（騙し方）、被害者や犯罪者の特徴、対策課題にも表れています。本資料ではそこに論点を当てます。

スミッシングをとりまく被害動向

スミッシングはここ数年で大きな社会問題になりました。2022年現在、情報処理推進機構（IPA）が公開する「情報セキュリティ10大脅威　2022」において、スミッシングを含むフィッシング行為は個人向け脅威の中の第1位です。また10位までの間に、クレジットカード情報の不正利用（4位）、スマホ決済の不正利用（5位）、不正アプリによるスマートフォン利用者への被害（7位）など、フィッシング／スミッシングと関わりの深い脅威が並んでいます（図1）。

スマートフォンは生活必需品と等しくなり、個人と様々なサービスを結びつけ、経済活動のプラットフォームを形作っています。この経済圏が犯罪者にとっても現実空間と並ぶ活動領域となり、スミッシングのような大衆を狙う詐欺の横行につながっていると考えられます。

クレジットカード不正利用による被害額は年々増え続けており、日本クレジット協会によると、2021年におけるカード不正利用被害額は330.1億円（前年比30.5%増加）であり、統計上の過去最高額となりました。このうち、番号盗用被害額が311.7億円（同39.4%の増加）であり、被害額全体の94%を占めます（図2）。

後ほど述べますが、昨今のスミッシングはクレジットカード番号を狙うものが多くなっており、番号盗用被害額の大きさから見ても、スミッシングを含めたフィッシング行為は、対策すべき重要課題と言えます。

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報などの詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールや SMS などを使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワークなどのニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬ IT 基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えいなどの被害	9位

図 1.IPA「情報セキュリティ 10 大脅威 2022」より
https://www.ipa.go.jp/security/vuln/10threats2022.html

クレジットカード不正利用被害の発生状況

（単位：億円、％）

期　間	クレジットカード不正利用被害額	クレジットカード不正利用被害額の内訳					
		偽造カード被害額		番号盗用被害額		その他不正利用被害額	
		被害額	構成比	被害額	構成比	被害額	構成比
2014年(1月～12月)	114.5	19.5	17.0%	67.3	58.8%	27.7	24.2%
2015年(1月～12月)	120.9	23.1	19.1%	72.2	59.7%	25.6	21.2%
2016年(1月～12月)	142.0	30.6	21.6%	88.9	62.6%	22.5	15.8%
2017年(1月～12月)	236.4	31.7	13.4%	176.7	74.8%	28.0	11.8%
2018年(1月～12月)	235.4	16.0	6.8%	187.6	79.7%	31.8	13.5%
2019年(1月～12月)	274.1	17.8	6.5%	222.9	81.3%	33.4	12.2%
2020年(1月～12月)	253.0	8.0	3.2%	223.6	88.4%	21.4	8.5%
（1月～3月）	61.7	4.3	7.0%	49.2	79.7%	8.2	13.3%
（4月～6月）	59.1	1.2	2.0%	53.2	90.0%	4.7	8.0%
（7月～9月）	59.4	1.2	2.0%	54.1	91.1%	4.1	6.9%
（10月～12月）	72.8	1.3	1.8%	67.1	92.2%	4.4	6.0%
2021年(1月～12月)	330.1	1.5	0.5%	311.7	94.4%	16.9	5.1%
（1月～3月）	73.7	0.7	0.9%	68.7	93.2%	4.3	5.8%
（4月～6月）	81.9	0.3	0.4%	78.1	95.4%	3.5	4.2%
（7月～9月）	81.3	0.2	0.2%	77.1	94.8%	4.0	4.9%
（10月～12月）	93.2	0.3	0.3%	87.8	94.2%	5.1	5.5%

1. （一社）日本クレジット協会の調査による。
2. 調査対象は、国際ブランドカードを発行している会社を中心に、銀行系カード会社、信販会社、流通系クレジット会社、中小小売商団体等である。
3. 回答社数は41社である。なお、銀行系カード会社のＦＣ／ＢＣ各社は国内ブランド会社単位で、また日本専門店会連盟・エヌシー日商連の各単会は連盟単位で、それぞれ１社としている。
4. 集計数字は、調査票提出会社のキャッシングを含む不正利用被害額を加算合計したものであり、海外発行カード分は含まない。
5. 2014年～2016年、2017年1月～6月、2018年7月～9月及び2019年10月～2020年の集計数字は変更が生じたため、修正している。
6. 2021年より、構成比は、単位未満を四捨五入しているため、内計と計は一致しない場合がある。

〈参考1〉　クレジットカード偽造被害の国内・海外別内訳

（単位：億円、％）

期　間	クレジットカード偽造被害額	クレジットカード偽造被害額の内訳			
		国内・被害額		海外・被害額	
		被害額	構成比	被害額	構成比
2014年(1月～12月)	19.5	4.5	23.1%	15.0	76.9%
2015年(1月～12月)	23.1	5.6	24.2%	17.5	75.8%
2016年(1月～12月)	30.6	10.5	34.3%	20.1	65.7%
2017年(1月～12月)	31.7	12.8	40.4%	18.9	59.6%
2018年(1月～12月)	16.0	7.4	46.2%	8.6	53.8%
2019年(1月～12月)	17.8	6.4	36.0%	11.4	64.0%
2020年(1月～12月)	8.0	2.3	28.8%	5.7	71.3%
（1月～3月）	4.3	0.9	20.9%	3.4	79.1%
（4月～6月）	1.2	0.4	33.3%	0.8	66.7%
（7月～9月）	1.2	0.4	33.3%	0.8	66.7%
（10月～12月）	1.3	0.6	46.2%	0.7	53.8%
2021年(1月～12月)	1.5	0.8	53.3%	0.7	46.7%
（1月～3月）	0.7	0.5	71.4%	0.2	28.6%
（4月～6月）	0.3	0.1	33.3%	0.2	66.7%
（7月～9月）	0.2	0.1	50.0%	0.1	50.0%
（10月～12月）	0.3	0.1	33.3%	0.2	66.7%

〈参考2〉　クレジットカード番号盗用の国内・海外別内訳

（単位：億円、％）

期　間	クレジットカード番号盗用被害額	クレジットカード番号盗用被害額の内訳			
		国内・被害額		海外・被害額	
		被害額	構成比	被害額	構成比
2014年(1月～12月)	67.3	42.0	62.4%	25.3	37.6%
2015年(1月～12月)	72.2	45.7	63.3%	26.5	36.7%
2016年(1月～12月)	88.9	54.6	61.4%	34.3	38.6%
2017年(1月～12月)	176.7	108.0	61.1%	68.7	38.9%
2018年(1月～12月)	187.6	125.2	66.7%	62.4	33.3%
2019年(1月～12月)	222.9	152.9	68.6%	70.0	31.4%
2020年(1月～12月)	223.6	163.9	73.3%	59.7	26.7%
（1月～3月）	49.2	32.9	66.9%	16.3	33.1%
（4月～6月）	53.2	38.1	71.6%	15.1	28.4%
（7月～9月）	54.1	41.8	77.3%	12.3	22.7%
（10月～12月）	67.1	51.1	76.2%	16.0	23.8%
2021年(1月～12月)	311.7	235.2	75.5%	76.5	24.5%
（1月～3月）	68.7	53.5	77.9%	15.2	22.1%
（4月～6月）	78.1	60.9	78.0%	17.2	22.0%
（7月～9月）	77.1	55.8	72.4%	21.3	27.6%
（10月～12月）	87.8	65.0	74.0%	22.8	26.0%

図 2. 日本カード協会「クレジットカード不正利用被害の集計結果について（ニュースリリース）」より
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g_220331.pdf

スミッシング手口の全体像

実際に観測されるスミッシング手口の全体像を図3に示します。この手順は、スミッシングが顕在化して以来、根本的に変化していません。

・SMS配信～偽サイト誘導

詐欺SMSが携帯電話・スマートフォン宛に届きます。SMSにはURLが掲載されており、クリックすると偽のブランド・サイトが表示されます。手続きを進めると以下のどちらかが発生します。

① 正規の入力フォームを装った画面により、アカウント情報（ログインID,パスワード）が搾取されたり、直接的にクレジットカード番号や口座番号とセキュリティコードなどが搾取される。

② 何らかのアプリのインストールが促され、マルウェアに感染する。

・踏み台確保

マルウェア感染の主目的は、攻撃者が更なるスミッシングのためのSMS発信源（踏み台）の確保です。スミッシングで使われるマルウェアは遠隔操作機能を持っており、所望の宛先に対し、攻撃者は感染したスマートフォンを遠隔操作してSMSを送ります。本来のフィッシング行為としては、マルウェア感染は重要ではないはずですが、SMSはemailほど自由に送信する手段が無いため、発信源としての踏み台を確保していると考えられます。実際、マルウェア感染端末が発信源と思われるスミッシングが国内で多数確認されています。

・目的実行

偽サイトで搾取したID、パスワードを使い、正規サイトへ不正アクセスして金銭的なゲインを獲得します。同様に搾取したクレジットカード情報を通販サイトなどで使う不正決済も代表的な手口です。スミッシングで狙われるブランドには移り変わりがありますが、狙う情報は、銀行アカウント、ECサイトのアカウント、電子決済やクレジットカード情報などが主流です。また、搾取した情報は不正利用されるのみならず、闇市場での売却（買い取ってもらう）も目的とします。特にクレジットカード情報は狙われており、詳しくは後半で述べます。

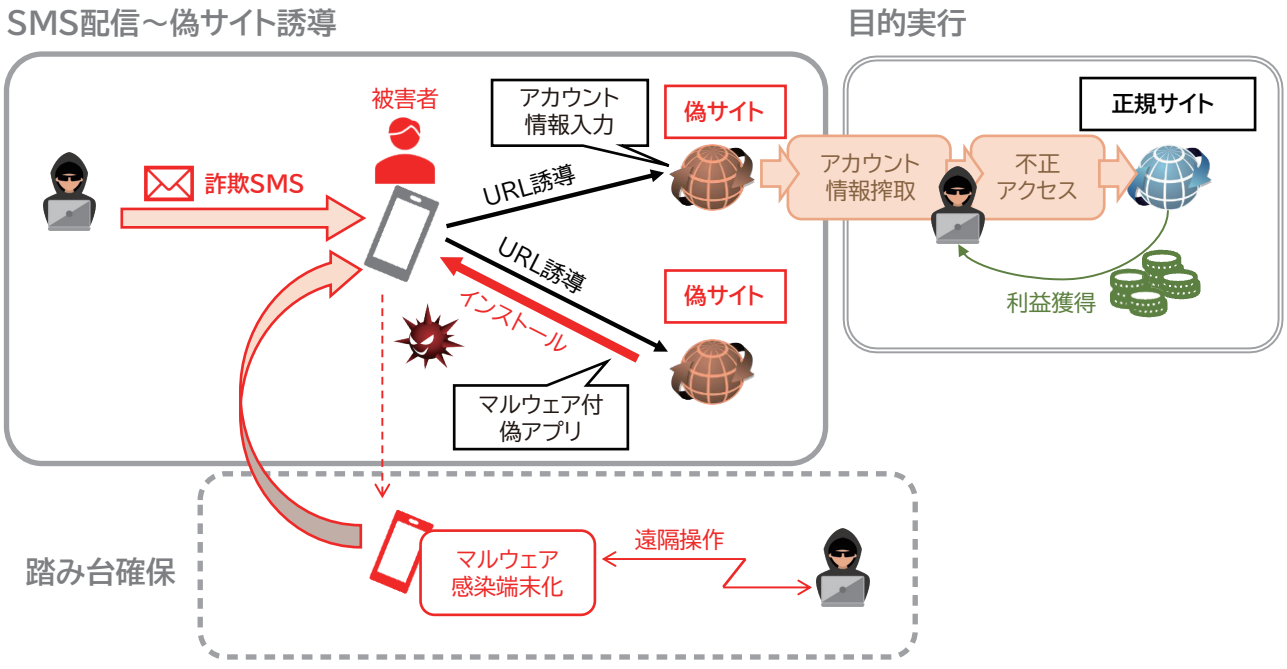

図 3. スミッシング手口の全体像

フィッシング行為におけるSMSの役割と特徴

携帯電話の基本機能として発達してきたSMSは、emailやメッセージングアプリとは違った特徴を持っており、それが詐欺の特徴に表れています。

1.SMSは日々持ち歩くスマートフォンに届く
2.宛先は特定個人と紐づいた電話番号
3.モバイルデータ通信を使わず、いつでも確実に受信される
4.反射的に開封しやすい
5.信じやすい・クリックしやすい

それぞれについて説明します。

1.SMSは日々持ち歩くスマートフォンに届く

SMS(Short Messaging Service)はGSM標準[1]として1990年代に商用化が始まり、世界中の携帯電話の基本機能として採用されました。短文のコミュニケーションツールとして欧米で広まり、日本でも2001年以降、3GでWCDMA標準を採用してから普及しました。スマートフォンが主流になっても標準機能として搭載され続けます。開発から既に30年も経つ古い技術ですが、最新の5G端末でも継続採用されており、今後も利用が続くと考えられています。

スマートフォンは生活必需品に等しい普及度合いであり、経済活動を営むほぼ全ての人が常に持ち歩いています。そこに届くSMSは、犯罪者にとって幅広い人を対象に詐欺メッセージを届け開封させる有効な手段です。

2.宛先は特定個人と紐づいた電話番号

電話番号はMSISDN[2]とも呼ばれ、通信事業者(以下「キャリア」)との回線契約により発行されます。そして実質的に、電話番号＝利用者(特定個人)として利用されています。特に携帯電話は個人が所持するため、「電話番号XXXXX＝〇〇さん」という紐づきは強固です。SMSは電話番号宛に送られるため、emailと比べて確実に狙った特定個人に届きます。この特徴は、電話による本人確認、SMSを使った多要素認証などに活用されていますが、残念ながら、スミッシング犯罪でも悪用されています。

アプリによるトークやチャットの普及、名前をタップするだけで電話発信できるなど、日常、電話番号を意識する機会は減りましたが、この「電話番号＝特定個人」という紐づきの強さは、スミッシング対策の上で理解しておく必要があります(図4)。

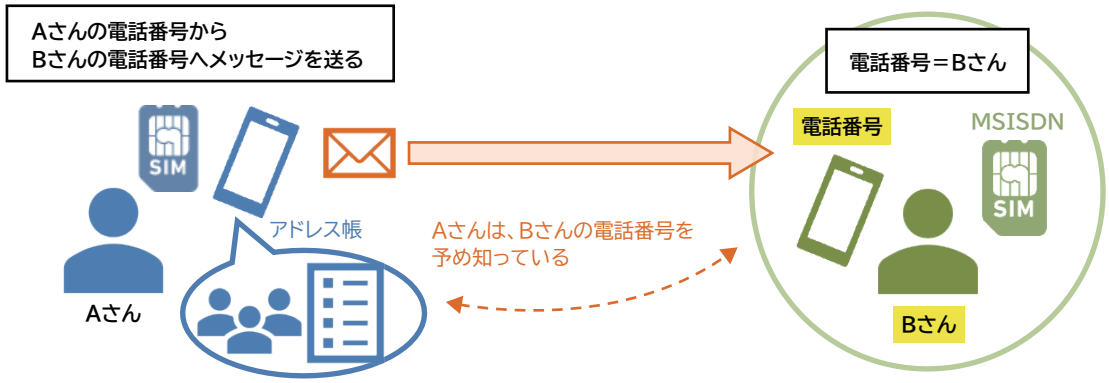

図 4. 電話番号と特定個人の紐づき

1 GSM : Global System of Mobile communications。第2世代携帯電話の標準規格の一つ。
2 MSISDN : Mobile Station International Subscriber Directory Number

3.モバイルデータ通信を使わず、いつでも確実に届く

SMSは、通常のデータ通信（いわゆるパケットプラン）を用いず、制御信号を用いて配信されます。制御信号は、携帯電話の基本的な仕組みであり、基地局を通じたキャリアネットワークへの接続・認証、通話の発着信、移動中の接続局の切り替え（ハンドオーバー）・・・などを担います。（図5）

利用者が通話やインターネットを使っていなくても、端末がキャリアネットワークと接続している間は常に制御信号がやりとりされており、SMSも常に受信する状態にあります。加えて、SMSは端末側から取りに行くのではなく、キャリアネットワーク側から送りつけるプッシュ方式で配信されます。更に制御信号はSS7/SIGTRAN[3]という標準プロトコルに載せられ、世界中の携帯電話網とつながっています。このため宛先電話番号さえ指定すれば、世界中のどこからでもSMSを届けることができます。

このようにSMSを使用すれば、電話番号と特定個人の紐づき、携帯通信の仕組みにより、送り手の好きなタイミングで、確実に、特定個人にメッセージを届けることができるのです。

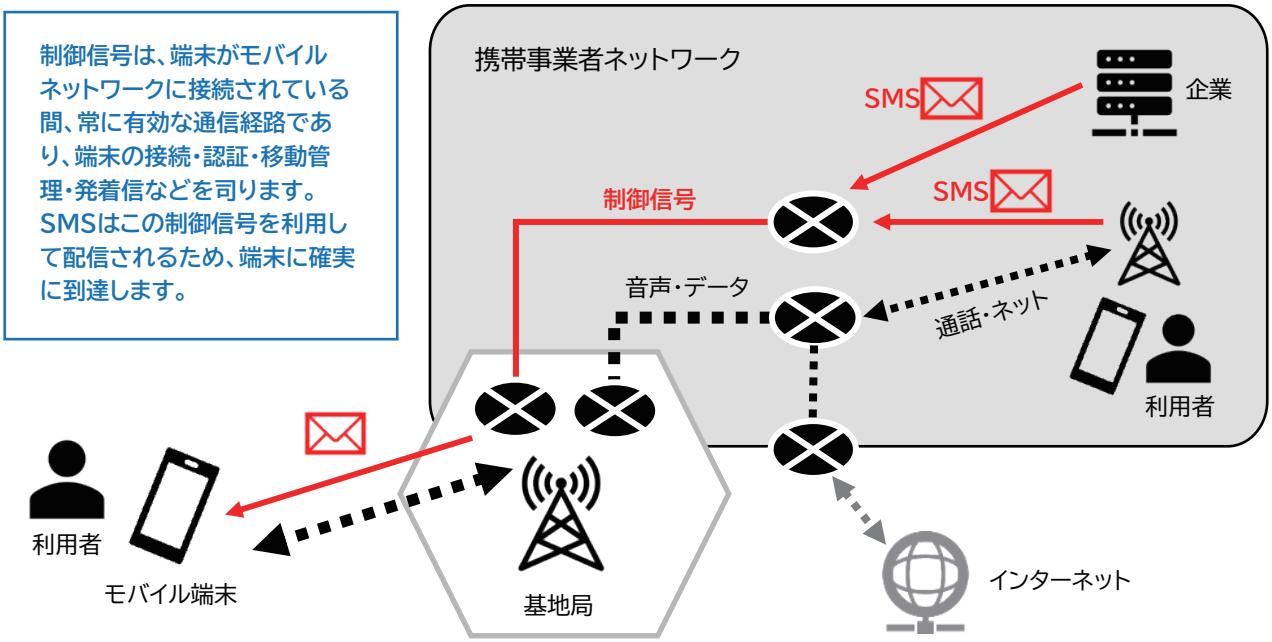

図 5.SMS はデータ通信を使わず常に送受信される

4.反射的に開封しやすい

SMSは携帯電話の基本機能であり、電話の着信同様、SMSを受信した瞬間にユーザーに分かる形で画面通知されます。

また、仕様上の文字数制約（英文160文字、和文70文字）のために短い文面しか送れません。必然的に簡潔明瞭なメッセージとなり、反射的に反応しやすくなります。

3 SS7は制御信号のための国際共通線信号方式。ITU-T勧告、ANSI/ETSI/TTCなどで規格化。SIGTRANはSS7をIP伝送できるようにしたプロトコルでありIETF標準。

5.信じやすい・見分けにくい・クリックしやすい

SMSを利用した企業・公共機関などからの正規メッセージも、文字数制約のために簡潔明瞭な文言で書かれ、短縮URL[4]も利用されます。emailでは違和感のある短さ、唐突さだとしても、SMSではありふれた表現であり、文面だけでスミッシングを疑うのは難しいです。仮に疑いの目で文面を眺めても、正規メッセージをコピーして作られる詐欺メッセージを見分けることは困難です。さらに、スミッシングも正規メッセージも、本当に伝えたい事は誘導先のWebサイトに書いてある(と感じるような文面)ということも、反射的なクリックにつながります。

	SMS	email
送信者名	送信端末の電話番号 または 任意のASCII文字列(装置発)	メールアドレス
宛先指定	受信端末の電話番号 回線契約に紐づき確実に届く	メールアドレス
送信料金	有料	無料
メッセージ形式	プレーンテキスト	自由

図 6.SMS と email の違い

4 短縮URLとは、長いURL文字列を別の短いURLに置き換える技術。ユーザーには短縮URLを提示して専用サーバーにアクセスさせ、そこから本来の長いURLにリダイレクト(転送)する。文字数制限や可読性などの観点で短縮URLが活用されている。

SMS発信源と到達経路・スミッシングへの悪用手口

SMSの発信源と到達経路には、携帯電話ネットワークならではの特徴があります。それを理解し、どのようにスミッシングに悪用されているか知ることは対策を考える上で重要です。SMS発信源・到達経路を図7に示します。スミッシングの発信源・経路も判るよう図解しました。

SMS発信源と到達経路

SMSは携帯電話の利用者同士でやりとりする他、企業広告・お知らせにも使われます。通話と同様、他のキャリアと契約している相手ともSMSを送受信でき、海外キャリアの利用者、企業からもSMSが届きます。SMSでは、キャリアが管理するネットワークとその相互接続に基づいて発信源・到達経路が定まります。技術的に以下の通り整理できます。

・自網と他網

SMS受信者「Aさん」を起点とした場合、「自網」とは、Aさんが加入している国内キャリアA社のネットワークを指します。「他網」とは、A社以外の他社のネットワークです。

SMS発信源は、自網発（例：同一キャリアの他のユーザー）と、他網発（例：他キャリアのユーザー）に分かれます。どちらから発信された場合でも、各SMSは必ず自網を通してAさんに届けられます。

・P2P／A2P

加入者端末間で相互にやりとりされるSMSを「P2P[5]」と呼びます。これに対し、広告などを目的とした加入者端末以外のアプリケーションから送るSMSを「A2P[6]」と言います[7]。P2Pは、自網内の別のユーザーから届くものと、他網のユーザーから届くものがあります。A2Pは、自網の法人接続から流入するものと、海外キャリアから流入するものがあります。

・法人接続

広告や通知などを送りたい企業がA2P　SMSを利用するための特別なインターフェースです。法人接続サービス、A2Pサービスとも呼ばれ、サーバーなどコンピュータを発信源としてSMSを送信できます。A2P　SMSを送る企業はキャリアと法人接続の個別契約を結ぶか、SMSアグリゲータ[8]のSMS配信サービスを利用します。

・国内接続

国内キャリアとの相互接続です。図5で述べた制御信号をキャリア間でやりとりし、通信相手がどこにいても通話やSMSが届くようにしています。SMSについては、基本的に他網加入者との間でP2Pのやりとりを担います。日本では、A2Pは各キャリアが個別に法人接続を持ち、国内接続を介したA2Pの他網転送は行いません（キャリア間の個別契約を除く）。

5 P2P : Person-to-Person
6 A2P : Application-to-Person
7 加入者端末から広告を送ることも可能であり、広義なA2P,P2Pの呼び分けは曖昧さを含みますが、ここでは対策検討上、技術的に区別が可能な「法人接続から送られたSMS」をA2Pと呼ぶことにします。
8 SMSアグリゲータ：A2P向けSMS配信サービスを提供する事業者。アグリゲータは国内外のキャリアと接続しており、幅広い受信者を対象にSMSを送ることが可能。

・国際接続

海外キャリアとの相互接続です。海外キャリアのユーザーとの間でSMSのやりとりを行います。P2Pのみならず A2PについてもSMSの宛先に応じて相互転送を行います。このため国際接続からは、日本のユーザーに向けたA2P が届きます。このケースを正規に利用する代表事例として、多要素認証における認証コードの通知SMSがあります。

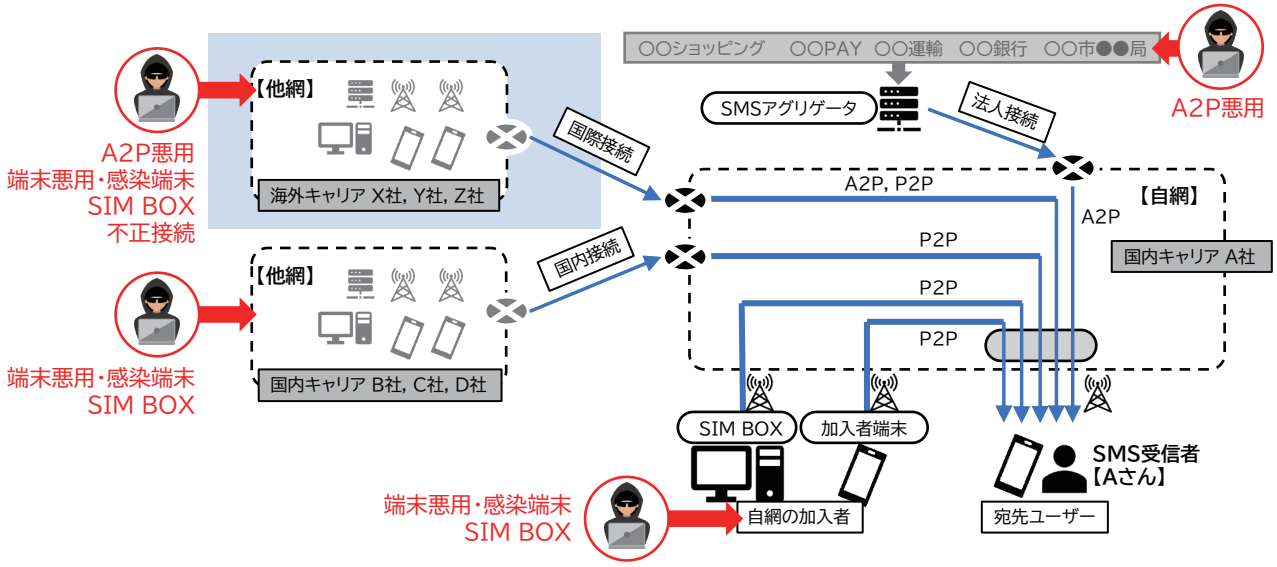

図 7.SMS の配信経路

スミッシングの送信手口

スミッシングの発信源も図7に示しています。正規のSMS送信手段はいずれもスミッシングに悪用できますが、加えて、正規の送信手段ではない、非公式／不正な手口も存在します。送信手口は以下の通りです。

・A2P悪用：コンピュータからSMSを送るための公式ルートを使う

SMSの送信方法としてコンピュータを使うと自由度が高いため、公式サービスとしてのA2Pもスミッシングに悪用される対象となります。A2Pサービス、SMSアグリゲータは、世界各国に同様の仕組みが存在し、サービス内容、自由度、質、厳格さなどは様々です。例えば、海外では、日本向けのSMSをWebサイト画面から簡単に送信できるサイトもあります。また海外のSMS配信サービスでは、SMS送信名を自由に設定できる（つまり送信者を偽装できる）ものも散見されます。

・不正接続：コンピュータからSMSを送る非公式ルートもある

非公式ルートとして、キャリアネットワークへ不正接続しSMSを送る方法があります。セキュリティ上の脅威として通信事業者間では広く知られており、GSMAセキュリティ・ガイドライン[9]にも登場します。ダークウェブで不正接続が売買されている記事もインターネット上で公開されています。

（参考：DEEP WEB）
https://www.deepweb-sites.com/dark-web-service-claimed-track-phone-read-text-messages-500-using-ss7/

またマクニカが業務支援するセキュリティ監視の中でも不正接続が疑われる挙動は国際接続上で観測されています。日本の携帯電話事業の感覚からは想像しにくいですが、運営・管理・ガバナンスの実行レベルには国・地域により大きなばらつきがあり、小規模なアマチュア局のような形態で運営することも可能です。悪意を持った不正接続の他に、保守・監視目的、あるいは設定不備などにより、不正接続に利用されかねない接続点もあり、非公式ルートを完全に塞ぐことは困難なのが現状です。

それらの不正接続点からはSS7プロトコルレベルで信号操作が可能なため、偽装SMSを自由に送信できるだけでなく、加入者情報の取得、交換機の悪用なども織り混ぜたSMS悪用が可能です。詳しくは、テレコム・シグナリング・セキュリティ[10]の範疇となるため別の機会に説明したいと思いますが、ここでは、偽装SMSを自在に送れる非公式ルートがある、という点を認識ください。

・端末悪用・感染端末からの送信

実際に携帯電話を使い、スミッシングを送ることも可能です。2通りの手法が存在しています。

1.犯罪者が所有する携帯端末からスミッシングSMSを送信する
2.マルウェア感染した携帯端末を遠隔制御してスミッシングSMSを送信する

このうち、2.マルウェア感染端末が量的にも大半を占めており、深刻な状況となっています。

・SIMボックスの利用

複数のSIMカードを差して携帯通信ネットワークに接続するためのSIMボックスと呼ばれる装置があります。4枚程度のSIMを差す小型のものや、16枚以上のSIMを差せる大型のなものがあり、それ自体が携帯端末として動作する機種や、USB接続でPCにつなぐタイプなどが販売されています。国内に設置したSIMボックスに対して、海外からインターネット経由で信号を送って携帯通信を利用することで国際ローミング課金を迂回する例が代表的ですが、スミッシングの発信にも利用されていると考えられています。SIMボックスは、国内外を問わず存在します。

9 GSMA, FS.11 : SS7 Interconnect Security Monitoring and Firewall Guidelines、他
10 モバイルネットワークのセキュリティのうち、SS7/SIGTRANなど制御プロトコルの悪用や脆弱性をついた攻撃を対象としたセキュリティ

スミッシング配信経路の識別

SMS発信源と到達経路について説明しました。これにSMS送信者名の制約を組み合わせることで、受信したスミッシング（およびSMS全般）の到達経路を識別することが可能です。経路が識別できると、後述する対策においてスミッシングと正規SMSの区別などに活かすことが出来ます。以下に説明します。

図 8. スミッシング SMS の各部の名称

SMS送信者名の制約

スミッシングを受信した際、SMS送信者名の欄にブランド名や電話番号などが表示されます（図8）。ここには通信プロトコルのTP-OA[11]フィールドに格納された値がそのまま表示されます。SMS送信者名は、一見自由なようでいて、あまり自由ではありません。制約は以下の通りです。

・プロトコル仕様

仕様上、送信者名フィールド（TP-OA）にはASCII文字列を格納できます（3GPP TS23.040 9.1.2.4 Alpha-numeric representation）。実際には以下の運用制約を受け、送信方法によって使える文字（配信できる文字）は更に限定されます。

・携帯電話からSMSを送る場合（P2Pメッセージ）

P2Pでは、自動的に発信者番号（電話番号 / MSISDN[12]）が送信者名として埋め込まれます。ユーザーが端末操作などにより任意に変更することは出来ず、SIMに記録されている電話番号が採用されます。

表記は数字に限定され、電話番号体系に従います（0-9の組み合わせで12桁以内，3GPP TS23.040参照）。このため、国内加入者発のSMSは必ず国内番号の送信者名表記となり、海外キャリアの利用者から送ると海外の番号表記になります。それ以外の電話番号表記は送信者を詐称した場合にのみ出現しますが、このパターンを携帯端末から送ることは出来ません。

11 TP-OA : Transfer Protocol - Originating Address 送信元アドレス＝送信者名のこと
12 MSISDN : Mobile Station Internatinal Subscriver Directorey Number 携帯電話の加入者識別番号＝電話番号のこと

・コンピュータなどから送る場合（A2Pメッセージ）

プロトコル仕様通り、アルファベットを含む任意のASCII文字を埋め込めます。送信者名として企業名やブランド名を使うケースが一般的ですが、使える単語や文字の種類などの運用制約は国・地域・通信事業者によって異なります。

日本国内で受信するSMSは、携帯番号以外の送信者名は全てA2Pが発信源です。アルファベットや数字を使えますが、特に、キャリアと事前合意した公式SMSだけがアルファベットの企業名（”NTT DOCOMO”など）や短縮番号・特定電話番号の使用を許可され、予め定めた公式経路（アグリゲータなど）からのみ当該SMSを送信できます。逆に、キャリアと合意していないアルファベット・記号・数列の送信者名を持つSMSは、全て国際接続から流入していることになります。

送信者名の制約を利用した経路識別

以上に基づき、送信者名によってスミッシング到達経路・主な発信源を識別することが可能です（図9）。実際に観測されたスミッシングをピンク色でマッピングしました。

送信者名の種類	国内P2Pルート（MNO内・MNO間）	国内A2Pルート（法人接続）	海外ルート（国際接続）
アルファベット		正規SMS	Amazon, SMBC, MUFGなど A2P悪用、不正接続
			正規SMS
国内電話番号	090-xxxx-xxxx 000xxxxxxx マルウェア感染端末、契約端末 SIMボックス	正規SMS	+8190xxxxxxx A2P悪用、不正接続
	正規SMS		
海外電話番号			+358xxxxxxxx, +467xxxxxxxx SIMボックス、契約端末、 不正接続、マルウェア感染端末
			正規SMS
ランダム数字		正規SMS	5～7桁のランダム数字 A2P悪用、不正接続
			正規SMS

：スミッシング　：正規SMS　：発生しない組み合わせ

図 9.SMS 送信者名とスミッシング経路の関係

国内A2Pの利用は厳格であり、スミッシングのような不正利用は困難です。A2P利用企業にとっては、自社ブランドを送信者名に持つようなスミッシングは、国内A2P発の可能性が極めて低いことを意味します。

国内では加入者番号発(P2P)のスミッシングを送ることが出来ますが、観測傾向から、その多くはマルウェア感染端末を発信源としていると考えられます。宅配業者を騙るスミッシングがその代表例です。

一方、国際接続ルートから流入するスミッシングは常に大量に観測されており、送信者名のバリエーションも豊富です。特に以下の送信者名のものが多いです。

・アルファベット
・海外の電話番号
・ランダム数字(電話番号ではない形式)

SMSアグリゲータの存在

前述の通り、A2Pの利用にはSMSアグリゲータを利用します。日本国籍のSMSアグリゲータの場合でも、実際の配信回線は海外キャリアを使うケースがあります。企業がこのSMSアグリゲータを使って国内利用者向けにSMSを配信しても、海外キャリアから国際接続を通じて日本のキャリアに流入するため、スマートフォンに表示されるSMS送信者名は、国際接続のパターンとなります(海外の電話番号やアルファベット利用など)。従って利用が厳格な国内A2Pと違い、正規の企業SMSとスミッシングとの区別は困難になります。

スミッシングの傾向と技術考察

ここまでで技術的な視点からスミッシングの配信について解説しました。この知見をもとに、実際のスミッシングの傾向を読み解きます。

手口変化の全体像

・黎明期～銀行系スミッシング

emailフィッシングが横行する中で、銀行系フィッシングは、2014年前後から騙られる銀行が増える傾向にありました。各行ともホームページなどで注意喚起を促し、ネット記事でも頻繁に取り上げられます。フィッシング対策協議会のニュースアーカイブで当時の様子を確認できます（https://www.antiphishing.jp/news/alert/）。

この時、まだSMSを使って誘導する手口は一般に認知されていませんでした。2015年、大手都市銀行の偽サイトに誘導するSMSが観測されます（図10）。これを機に表面化しますが、SMSが使われること自体が問題視され「スミッシング」として大きな話題になるのはまだ先です。

図 10.2015 年、SMS を使った銀行系フィッシングが観測された（twitter, @NaomiSuzuki_）
https://twitter.com/NaomiSuzuki_/status/601039199291060224

・2018～宅配系スミッシング

この頃から、量的、話題的にもスミッシングが顕在化します。宅配業者に成りすましたSMSにより偽サイトに誘導、個人情報の搾取に加え、不正アプリをダウンロードさせマルウェア感染させる手口です。感染端末はSMSの発信源として悪用され、この先、被害の拡大につながっていきます。

宅配系スミッシングは、初期は海外ルートから届いていました（送信者名は海外の電話番号など）。その後、感染端末が増加して国内にある端末がSMS送信の踏み台になると、国内携帯電話番号（090～など）を送信者名とするSMSが大量観測されるようになり、現在に至ります。「ご不在のためお荷物を持ち帰りました～」というSMS文面に加え、送信者名が携帯番号であることから、宅配ドライバーから送られたSMSだと思い込みやすいと言えます。多くは国内のマルウェア感染端末を発信源としますが、SIMボックスや正規端末の悪用も考えられます。

図 11.2018 年に報告された宅配系スミッシングの報告例
（フィッシング対策協議会「フィッシングに関するニュース」アーカイブより）
https://www.antiphishing.jp/news/alert/sagawa_20180810.html

・2019～キャリア系・銀行系スミッシング

2019年は、キャリア決済を騙り未納料金を請求するタイプのキャンペーンや、銀行を騙り口座情報を狙ったキャンペーンが話題となりました。SMS送信者名として”NTT DOCOMO”、”SMBC”など実在ブランド名を詐称するケースが急増します。これらアルファベット表記の送信者名は、国内では第三者が自由に使用できず、かつ詐称SMSを送信する手段が国内に無いため、国際接続から流入します。

図 12.2019 年に観測されたキャリア系・銀行系スミッシングの例

・2020～EC系・宅配系スミッシング

その後しばらく落ち着きますが、2020年末頃から再燃し、2021年から2022年にかけて過去に無いような大量のスミッシングが観測され現在に至っています。内容は大手ネット通販サイトを騙るEC系や、荷物配達の不在通知を騙る宅配系が主流です。コロナ禍によるネット通販需要の増加が背景にあると考えられます。

EC系の送信者名は、2020年頃は”Amazon”など通販ブランドそのものを詐称するケースが主流ですが、その後変化していきます（後述）。宅配系は引き続き国内の携帯電話を発信源とするSMSが支配的であり、多くは国内のマルウェア感染端末を発信源としますが、SIMボックスや正規端末の悪用も考えられます。

図 13.2020 年に報告された EC 系スミッシングの例

・2021～送信者名がランダム数列のSMSが増加

2021年からの観測傾向として、送信者名に5桁～8桁のランダムな数列を使用するパターンが急増します。SMSの文面は、以前から出回っているEC系などブランド名称を騙るものが大半であり、送信者名がアルファベット表記からランダム数列に置き換っている傾向が見られます。ブランド名を詐称する送信者名は説得性がある反面、セキュリティソフトなどでブロックされる可能性も高くなるため、毎回異なる数字を使用して防御を回避する意図があると考えられます。

電話番号の表記ルールに沿わない数列の送信者名はP2Pとして送れないためA2Pを使いますが、国内A2Pではランダムな数列を自由に使えないため、このタイプは国際接続を通って日本に流入します。

図 14. 送信者名がランダム数字の例

誘導先ドメイン名の変遷

誘導先の偽サイトで使用されるドメイン名にも変遷が見られます。2018年～2019年は、正規のブランド・サイトに似せたドメイン名や、正規ドメインに文字を追加したようなものが多く使われていました。またTLD（TopLevel Domain）には .xyz, .top, .shop なども多く用いられました。

その後スミッシングが社会問題化し、本物に似せたドメインが警戒されるようになると、正否の判別が難しい短縮URL（bit.lyなど）が増えます。さらに誘導先ドメインがテイクダウンされることを回避するため、ドメインの追跡を困難にするDDNS（ダイナミックDNS）を使用するケースも増加しました。宅配系を中心に頻出した****.duckdns.orgなどです。

電話番号に誘導するケース

本文にURLではなく電話番号を記載し、電話をかけさせる詐欺SMSもあります。いわゆる特殊詐欺に分類され、記載された番号に電話をかけてしまうと巧妙な会話に騙されて詐欺被害にいます。この種の詐欺は2018年以前から存在し現在も横行していますが、コールセンターを準備するなど組織的な対応が必要となります。新規参入にはハードルが高く、スミッシングとは異なる、従来型の特殊詐欺グループが係わっていると考えられます。

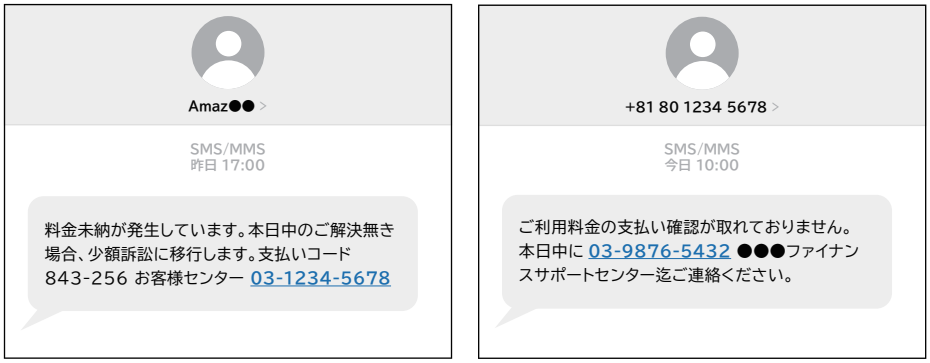

図 15. 電話番号に誘導するケース（イメージ）

13 DDNS（Dynamic Domain Name System、ダイナミックDNS）：実体サーバーのIPアドレスが変化しても公開しているドメイン名（ホスト名）との紐づけを動的に変更する仕組み／それを利用したDNSサービス。

攻撃者の変化、犯罪の裾野の広がり

スミッシングの背後には様々な攻撃者（詐欺師、フィッシャーとも言う）がいると推定できます。黎明期からある銀行系スミッシングは、対象となる銀行や地域の狙い方、認証を突破して不正出金する手口などに、知識・オペレーションレベルの高さ・組織性が見られました。また、スミッシングの手口傾向から、複数の集団がいると推定されていました。

最近はEC系、宅配系を中心に、クレジットカードや電子決済のための情報を狙うものが増えています。スミッシングの総量が増えていますが、同時に以下のようなスミッシングが散見されるようになりました。

1.偽サイトのブランドと、SMS文面のブランドが一致しない
2.SMS文面の日本語が不自然

つまり、過去から活動している攻撃者と比べて、オペレーションレベルの低い人々が参入するようになってきたことや、分業化が起こっていることが推測されます。その背景として、これから述べるような事情が関係していると考えています。

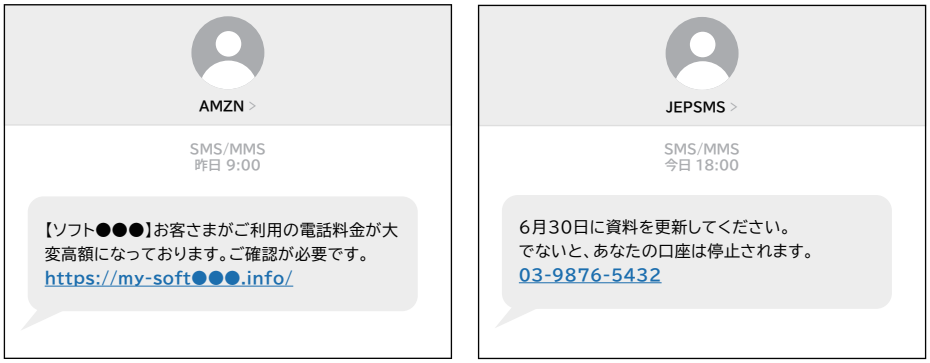

図 16. オペレーションレベルが低い例が報告されている

インターネットを流れる闇情報

スミッシングのための情報はネット上でやりとりされ、手軽に金銭を獲得する手段として広まっていることが見て取れます。過去、サイバー犯罪に関わる情報はダークWeb上で多く観測できましたが、現在、検索サイトなどから容易に辿りつけるサーフェースWebでも多くの情報が流れるようになりました。SNSやコミュニケーションアプリも利用されており、その代表例がTelegramです。

TelegramはGoogle PlayやApp Storeで入手できるチャットツールですが、匿名性の高さを特徴とする一方、犯罪や闇バイトの情報交換・勧誘に利用されていることが国内でもたびたび指摘されています。海外でも2021年9月～12月にイラン政府に成りすました大規模なSMSフィッシング・キャンペーンがあり、その際にTelegramが大きな役割を果たしたことが指摘されています。

Telegram自体の良し悪しは本題から逸れるため言及しません。どのようなコミュニケーションツールであっても、犯罪に利用される可能性があります。ここで述べたいポイントは、一般に広く利用できる手段を使い、誰でもアクセスできる場所で、犯罪に関わる（または犯罪の一旦を担うことになる）情報が流れている、という現実です。

日本がターゲット

・Telegramの調査結果から

日本を標的としたスミッシングのための情報がTelegram上でやりとりされています。関係するチャネルは多数ありますが、フィッシングハンター（@KesagataMe氏）の協力のもと、マクニカが内容を調査・確認したものだけでも17個のチャネルがありました（2021年末時点）。チャネル・オーナーが提示している宣伝文句から、そのチャネルの位置付け・性質が読み取れます。実例をいくつか抜粋します（図17）。

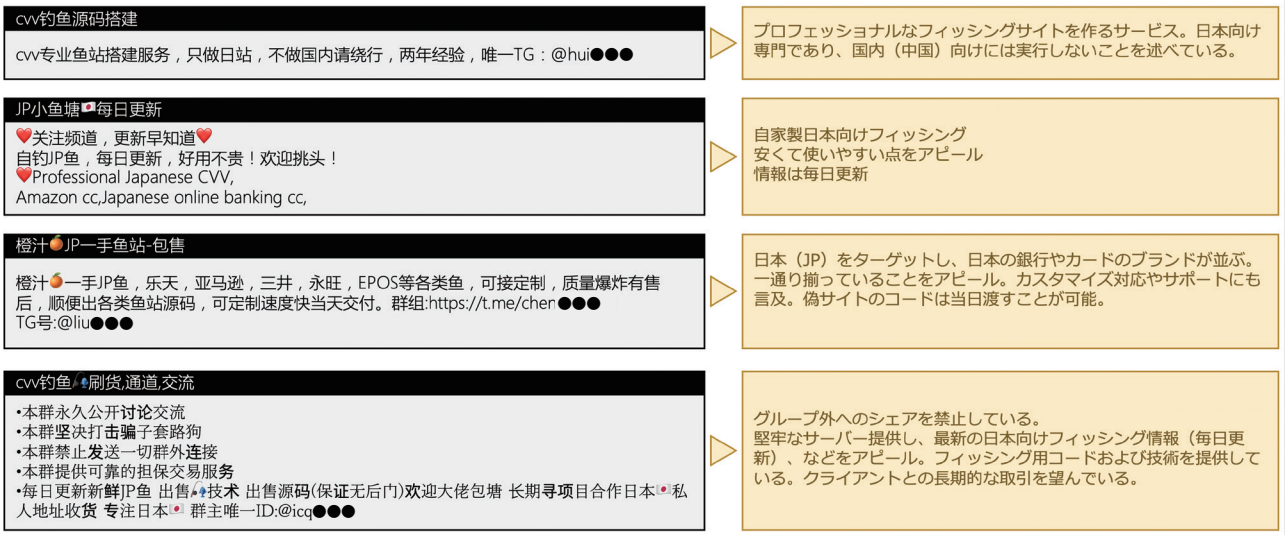

図 17. 日本をターゲットにする Telegram チャネルの例

・日本の大手ECサイト、都市銀行、カードブランドが列挙されています。
・偽サイト・ソースコードが揃っており、当日渡すことが可能。カスタマイズ対応、サポートも受けられます。
・カード情報を搾取するサイトに特化した例もあり、日本がターゲットにされています。
・情報の鮮度、低価格、クォリティなどが謳われています。

またチャネルオーナーとコンタクトする中で、以下のような情報も得ました（一部のみ掲載）。

・某大手銀行のフィッシングサイトのソースコード提供は、1000元以下の価格。
・SMSを24時間送り放題のサービス提供は100元以下。
・不正購入した製品が売れる（日本のゲーム機、APPLE製品、洋服・靴などのブランド品）。

・その他のWebサイトでは

Telegram以外にも、スミッシングに関わる情報はWebサイト上でかなりの数が流通しており、インターネット検索によって辿り着くことが可能です。例えば以下のようなものがあります。

・クレジットカード情報の販売、買取、不正利用のための情報(“Carding”と呼ばれるジャンル)。
例)『Sell cvv US-UK-US-CA-EU-ASIA-dump12 2022 FULL fresh all country』
hxxp://scandinavian-va[.]net/forums/index-
.php?/topic/12551-sell-cvv-us-uk-aus-ca-eu-asia-dump12-2022-full-fresh-all-country/

・日本の携帯電話番号リスト。鮮度の高さを主張しており、頻繁にアップデートされていると思われる。
例)『Japan Phone Number List』
hxxps://www.latestdatabase[.]com/japan-phone-number-list/

・フィッシング、Cardingのやり方を解説した動画コンテンツもある。
例)『BEST SPAMMING TUTORIAL 2021 | SMS SPAMMING 2021 | CARDING TUTORIAL 2021』
hxxps://www[.]youtube[.]com/watch?v=eza3S0pUxGg

このように、スミッシング、そこから発生するクレジットカード不正決済、商品転売など、犯罪の構成要素を実行するための情報がネット上で流れています。誰でもスミッシングに関わることでお金を稼げるため、現実世界の詐欺と同様、犯罪者のすそ野が広がっていると考えられます。

スミッシング犯罪のエコシステム

一連の調査で得た情報に基づき、スミッシング犯罪のエコシステムを図解しました（図18）。特に最近顕著なクレジットカード情報を獲るケースを例として解説します。

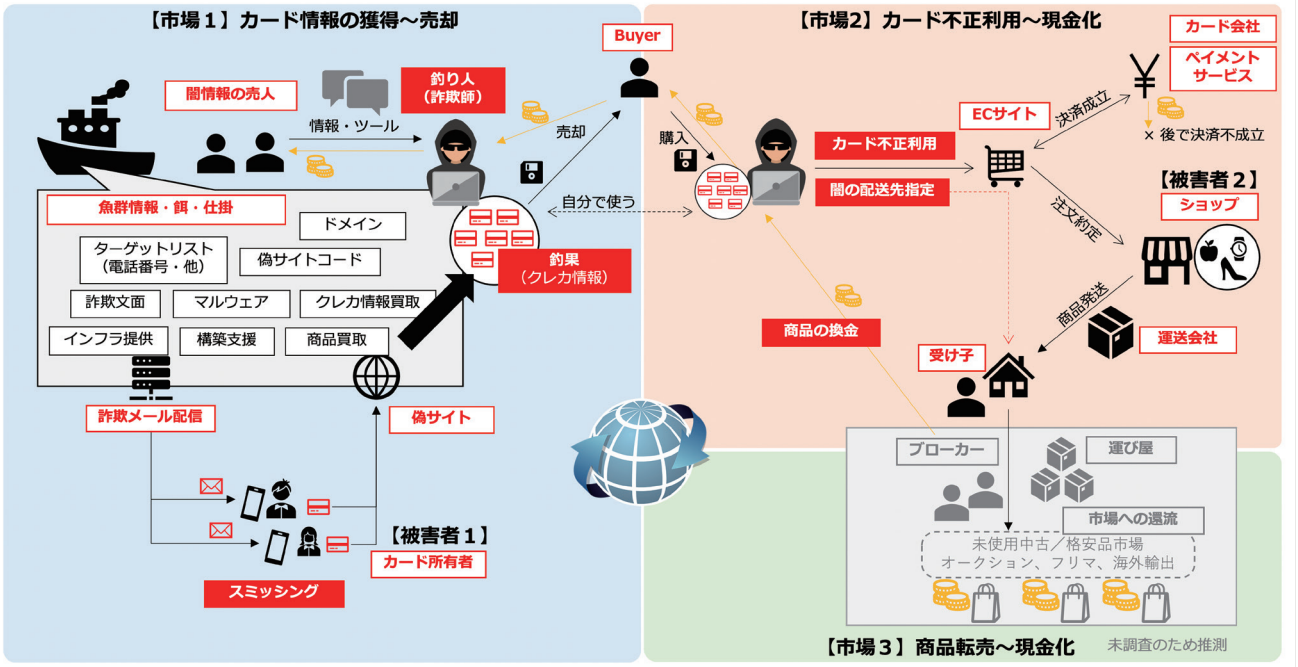

図 18. スミッシング犯罪のエコシステム

・3つの市場

エコシステムは大きく3つの市場に分解できます。

【市場1】フィッシング／スミッシングと呼ばれる詐欺手口が実行され、搾取したカード情報を金銭に変える。

【市場2】搾取したクレジットカード情報を不正利用し、購入商品を転売して金銭に変える。

【市場3】買い取った商品を消費市場などへ流通させて金銭を獲得する。

・フィッシング詐欺師

フィッシャーとも呼ばれます。銀行系スミッシングに見られるオペレーションレベルの高い集団も存在しますが、クレジットカードを狙うスミッシングでは犯罪の裾野が広がっており、お金目当てでフィッシング詐欺に参入する人が増えていることがTelegramなどの調査から読み取れます。

・スミッシングの準備

偽サイトの作り方、偽サイトのソースコード、SMS配信、カード情報の売り場、カードを不正利用して買った商品の送り先などを揃えます。これらの売買が行われる闇市場には、Telegramを始めとするコミュニケーション手段を通じてアクセスできます。

SMS配信先（ターゲット）の電話番号リストも買うことが可能です。日本の携帯電話番号リストは海外のWebサイトで販売されています。電話番号は数字なので総当たり攻撃も可能ですが、マクニカが観測した事実として総当たり送信やランダム送信は見られません。基本的に宛先はリスト情報を使っていると言えます。

・スミッシングの実行

偽サイトを立ち上げ、SMSを撒きます。ツールによりますが、ターゲットが偽サイト上で入力した情報は予め設定したメールアドレスなどに自動的に届くので、フィッシャーは待っていればカード情報が釣れます。収穫は詐欺の巧妙さと、偽サイトが発見されてテイクダウンされるまでの時間に依存しそうです。詐欺の被害者は、SMSを受信し偽サイトを通じてカード情報を盗まれた個人です【被害者1】。しかし情報を搾取されただけでは実害が発生せず、搾取されたことにも気づかないため、この段階で【被害者1】は無自覚な場合が多いと考えられます。

・情報の売買

スミッシングによって搾取したクレジットカード情報（および認証～決済に必要なクレデンシャル情報）を売却します。フィッシャーは、この段階で収入を得ます。ここで【市場1】での経済活動のゴールが達成されます。フィッシャー自ら【市場2】へ進んでカードを不正利用することも考えられます。

・クレジットカード不正利用～商品購入

フィッシングで搾取したクレジットカード情報は不正利用されます。実態としては、ECサイトでの商品購入、その後の商品の換金です。購入には搾取した他人のクレジットカードを利用するため、攻撃者は商品代金を払いません。カード情報入手にかかった費用を充分に上回るゲインが得られる商品が購入対象となります。人気のゲーム機、スマートフォン、タブレット、鞄や服飾品が示唆されていました。商品購入時、予め定めた特定住所を発送先として指定します。

・指定住所への商品発送～換金

ECサイトで決済が成立すると、ショップから商品が発送されます。送り先は、購入者ではなく、Telegramなどで得た送り先住所です。日本国内に、そうした商品の受領を専門に行う住所（受け取り拠点）がたくさんあります。通称「受け子」と呼ばれる、荷物の受け取り人がいます。摘発などによって受け取り拠点が使えなくなると、その情報もTelegram上で流れることが判っています。

商品配達が完了した後、なんらかの確認を経て商品購入者（カード不正利用犯）は代金を受け取ると考えられますが、調査中のためここまでの説明にとどめます。

なお、商品発送後にクレジットカード不正利用が判明した場合、カード利用者は保護されますが、代わりに、商品を販売したショップに対してカード会社から代金が決済されないことも問題となっています。売上ゼロで商品も失うことになります・・・【被害者2】

・商品を消費者市場へ還流する

商品は何らかの形で消費者市場に還流され、現金化していると考えられます【市場3】。マクニカでは調査対象としていない領域ですが、スミッシング以前からある、処分品、盗品、その他のルートで入手された訳あり商品を市場に還流させる仕組みと関係していると考えています。

対策アプローチ

スミッシングに関する犯罪エコシステム(図18)の理解と考察を深めることで、犯罪の全体像に沿った対策が可能になります。これまでフィッシング対策の中心は、フィッシングサイトの早期発見とテイクダウン(または、アクセスブロックによる事実上の無害化)でした。今後もこれらは有効ですが、さらに犯罪の上流・下流の対策も組み合わせ、一連の犯罪行為のチェーンを断ち切ることが肝要です。以下、考え方を述べます。

スミッシング対策フレームワーク

対策を考えるにあたり、スミッシングの流れに沿ったフレームワークを定義します(図19)。中央のアイコンは左から右に向かってスミッシング犯罪の順序を表しています。その上に並ぶ四角は、エコシステム上の企業が個別に実行できる対策を示し、下には企業が協力し合うことで実行できる対策を並べています。各対策について説明します。

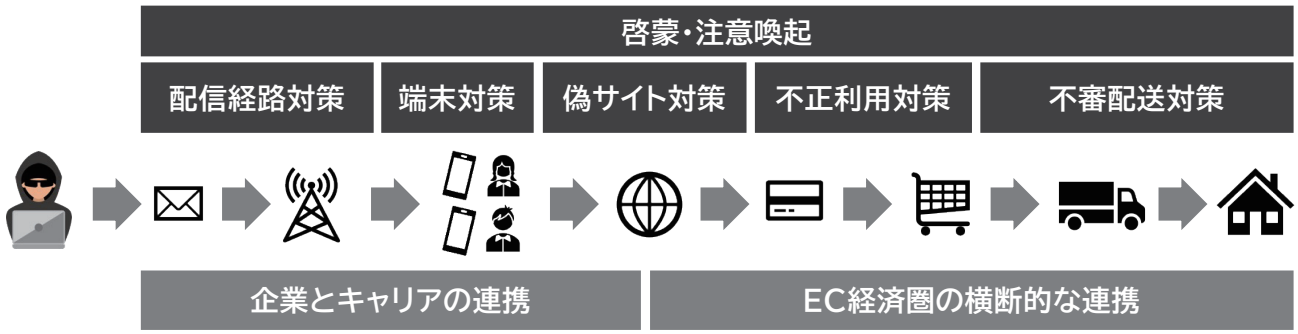

図 19. スミッシング対策フレームワーク

・配信経路対策

詐欺SMSが受信者に届かないよう、SMS配信ネットワーク側で対策します。SMSサービス利用の厳格化や、技術的にはスミッシング検知とフィルタリングが効果的です。SMS送信から受信までの経路は、通信キャリアが運営しています。このため、配信経路対策はほぼキャリアが行うことになりますが、実際には課題があります。

個人の権利・プライバシーを目的とした通信の秘密(憲法第二十一条、及び電気通信事業法)により、キャリアが配信ネットワーク側でスミッシングを区別しフィルタリングする方法が非常に限定されます。キャリア各社は、上記法律の「電気通信事業者」に明確に該当するため、安易な方法でSMSを識別・区別してスミッシングをふるい分け遮断することは出来ません。加えて、通信の到達性担保はキャリアの使命です。悪性のSMSを精度よく識別できない限り、過剰なフィルタリングによる到達性低下を招き、クレームやサービス障害につながりかねません。このように、キャリアに課せられている役割や責任を理解することが、有効な対策検討の上で大切です。

キャリア各社はスミッシングに対して高い問題意識を持っており、様々な検討・意見交換を進めてきました。キャリアの多大な努力と各省庁との協議により、昨今、出来ることが少しずつ増え始めています。国内大手キャリアではSMSファイアウォールによるフィルタリングの導入を推進中で、一部は2022年3月から適用が始まり効果を上げています。スミッシングが利用者の端末に届く前に遮断するため、適切に運用が進めば非常に効果が高い手法です。

フィルタリングの効果を高めるためには今後運用ノウハウを蓄積して行く必要があります。また誤遮断を避けて的確にフィルタできるよう精度を高めるため、正規ブランド企業、SMS利用企業、SMSアグリゲータ、キャリアが連携し対策していくことも重要です(後述)。マクニカは関係企業と一緒に配信経路対策を推進していきます。

・端末対策

端末上で実施できる対策は2つあります。

①偽サイトへの誘導対策

②マルウェア対策

現在、①はセーフブラウジングを中心とした対策が進んでいます。ドメイン名やURLから危険サイトを識別し、アクセスをブロック(および警告表示)します。危険サイトの情報は、各企業から寄せられる申請が役立っています。ドメイン不正利用(abuse)申告と合わせて企業側から情報をインプットすることが重要です。ただし、ランダム文字列を含む大量のドメイン取得～不正利用には効果が出にくいです。

また、SMS着信時に送信者名から迷惑電話／迷惑SMSを識別して警告表示するスマートフォンアプリもあります。更にSMSアプリの改良により、文中のURLへのジャンプや電話番号コールを1回の操作では出来なくしたり、リンクを無効化することも技術的には可能です。こうしたアプリ自体を普及させることに加え、機能改善、DB強化、などが有効と言えます。

②はアンチウィルスソフトや、キャリアが提供するセキュリティパックなどがあります。これらの機能向上・検知性能向上は重要です。また、利用中の端末上で行う対策だけでなく、企業側が行える対策もあります。自社の公式アプリになりすました偽アプリの配布を自動で検知するテクノロジーがあります。こうした技術を活用すれば、ブランドの信頼性を高めながらスミッシング対策(マルウェア対策)が可能です。

端末アプリを開発する視点では、マルウェアとして悪用されやすい機能(OSのAPIなど)の改善や実行権限の厳格化、アプリ配布方法やインストールの厳格化など、端末プラットフォーム側の対策も検討対象となります。ただしアプリ開発の容易性や柔軟性、アプリ市場における自由や公平性への影響など、安全性とのバランスが議論になりそうです。

・偽サイト対策

フィッシングハンター諸氏の尽力もあり、新たなパターンのスミッシングが早期発見・共有されるようになってきました。また、そこから偽サイトのテイクダウン、セーフブラウジングへの反映も迅速になりつつあります。これらは引き続き推進していくことが肝要です。

フィッシャー側は対策をかわすべく工夫しており、偽サイトのドメイン名は、短縮URL化、動的DNS(DDNS)利用、ランダム文字列を含めた大量生成など、多様化、短命化しています。これまでの発見～テイクダウン(無害化)を高速化・自動化することが重要です。既に自社ブランドを複製した偽サイト発見に取り組む企業や、テイクダウン依頼を含めて自動化に取り組む企業もあります。こうした取り組み事例・経験を活用し、より多くの企業・団体が対策推進することが望まれます。

技術的には偽サイトへのアクセスをDNSレベルでブロックすることも可能です。端末からサイトへアクセスする際、URL表記(単なる文字列)を実際のIPアドレスと結びつける仕組み(＝DNSによる名前解決)を用いますが、この時に偽サイトへのアクセスについては名前解決をしない・・・などの方法です。公共性や透明性などの点での議論が必要ですが、偽サイト誘導の対策として一考に値します。EUでは”DNS4EU”の検討が進んでおり、プライバシー保護視点に加え、DNS resolver領域でのフィルタリングなどセキュリティ対策としても期待されています。このような他国の動きも参考になりそうです。

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

・不正利用対策

犯罪者がアカウント情報やカード情報の不正利用を試みる段階で失敗させます。大きく2つに大別できます。

①不正ログイン対策

②不正行動対策（不正用アカウント作成対策なども含む）

ログイン認証の強化が進んでおり、今後も継続対応が求められます。また、近年、ふるまいベースの検知技術は刷新が進んでいます。IDやパスワードが合致していても、それ以外の要素で本人がログインした場合との違いを検出し、追加の認証を要求することも可能です。パスワードなどを用いない認証も始まっています。この分野ではユーザーエクスペリエンスとセキュリティの両立がチャレンジングなテーマであり、テクノロジー開発も続いています。そのような新しい技術の導入も検討する価値があります。

サイト上での不正行動対策も有効です。例えば、不正入手した情報を使うために犯罪者が新規アカウント作成する行為を失敗させれば犯罪の未然防止につながります。同一情報で複数アカウントが作られるケースをリスク評価したり、アカウント作成時に登録される情報と、過去の不正ユーザーとの類似性を評価することが可能です。リスク度合いに応じて本人確認を追加したり、必要に応じてアカウントを削除する・・・などの対策が検討できます。

また、なりすましログインが成功した場合でも、サイト上でのユーザーの行動から不正を検知することで対応することも可能です。完全な不正識別ができなくても、行動から不審利用者だと評価した場合に、チェックアウトや決済における手続きを厳格化する、追加の認証を要求する、などです。

このように、犯罪者が事前に予測できない要素を犯罪行為の最中に加えることで、行為を断念する可能性が高まります。こちらもサイト利用におけるユーザーの利便性や快適性とセキュリティの両立がチャレンジです。

・不審配送対策

クレジットカード不正利用によって注文した商品は、犯罪者とつながりのある宛先に出荷されます。通称「受け子」と呼ばれる受取人が商品を受け取ります。ECサイト上でそうした宛先住所が指定されるケースや、出荷後に配送先変更／転送などの手続きによって宛先指定するなどの手口があります。配達員にとって、通販の荷物が頻繁に届く、受け取る人が頻繁に変わる、誰も住んでいないように見える、など違和感を覚えるケースがあるそうです。こうした気づきから犯罪対策につなげることは可能です。2021年には郵便局が異常に気付き、邸宅侵入事件として逮捕に至ったケースもニュースになりました（朝日新聞デジタル、2021年8月7日）。

運送会社が単独で実行できることは少ないかもしれませんが、配達現場の情報を社内で共有することから始め、地域の運送会社同士や、宅配企業と郵便局との情報交換、地域の警察との相談など、対策につなげていくことが可能です。更にECサイト、ショップと連携した対策も考えられます。摘発リスクの上昇、新たな配達先の持続的確保のための犯罪コスト上昇は、抑止力となります。

・啓蒙・注意喚起

従来のITセキュリティと違い、被害に遭う方々がITの世界とつながりが無い人々が多いため、HPに記載しただけでは注意喚起が行き渡りません。いかに見てもらえる媒体に書くか、工夫が必要です。また、注意喚起の中には有効ではない主張（例：偽サイトを見分ける点の説明など）もありますが、このような理解のばらつき、対策のばらつきを減らすことも必要です。例えば、新たに自社ブランドを騙られた企業が適切な注意喚起を実行できるような、良質な事例の共有、ガイドライン化などは有効と言えます。

また、啓蒙により人々のリテラシが向上することは、中期的に犯罪抑止につながると考えています。マクニカは啓蒙・注意喚起、両方の横串を担いつつ、特に、個々の企業では届けにくい対象への啓蒙を主体的に支援していきます。

・企業とキャリアの連携

企業・団体の公式サービス、公式情報とキャリア側の配信経路対策を組み合わせることで、精度の高い識別～フィルタリングが可能です。またスミッシングで自社ブランド名や団体名が騙られたときの対策も迅速化します。そのためには以下の連携が有効です。

①自社が配信する公式SMSの「配信ルート」を国内法人ルートに限定する。または発信番号を固定する。
②自社公式SMSで使用する「SMS送信者名」を特定可能なパターンに限定し、明確化する。
③SMS文面で使用するURL全体、または、ドメイン名など出来る範囲で限定し、明確化する。
④自社SMSにURLを埋め込まない。かつそれを明言する。
⑤そもそも自社ブランドがSMSを使うかどうか明確にし、事前にキャリアと情報連携する。

アグリゲータも重要な役割を占めます。①②はアグリゲータによって出来ることに差があります。本ペーパーで述べてきたSMS配信ルートや送信者名の特徴、スミッシング送信手口をよく理解し、自社のSMS配信がどの程度スミッシングと区別可能か事前検討したり、スミッシングに使わせない工夫を施すことは大切です。

こうした連携のためには、今後、B2Bの連携窓口や連携スキームが重要になってきます。引き続きマクニカはこうした取り組みも支援していきます。

・EC経済圏の横断的な連携

犯罪者の不正利用や不正行動に関するリスク情報を、企業間やサービス間でオンラインで相互利用することも技術的には可能です。たとえば、運送会社の持つ不審な配達先の情報をECサイト側で参照できれば、購入～決済プロセスでリスク評価に加味して注文成立前にアラートを出す、認証を追加する、配達方法のオプションを制限するなど、不正取引の抑止・防止が可能かもしれません。同様に、カード決済の認証についても、ECサイト側のリスク評価をペイメントサービス側が参照して認証を追加したり、カード会社が持つリスク情報や不正取引の情報をペイメントサービスやECサイト側でユーザーのリスク評価に使うことも、技術的な観点だけならば可能と言えます。

ステークホルダーの連携・踏み込んだ協議が重要

以上は技術視点での対策アプローチです。実際に検討するには、業界規制、法規制を含めた議論と検討が必要な要素も多いと考えられます。例えば、利用者が届けている登録情報・入力情報をどこまで、どうやってセキュリティ対策に活用するか。サイト上で収集できるリアルタイムのデータで何が出来るか。これらは、そのままプライバシー問題など、セキュリティ以外の課題と結びつきます。しかし、そこで考えを止めるのではなく、出来る小さなことから合意を作っていく努力が大切と考えています。そのためには、個社で考えるだけでなく、企業間でアイデアや課題を出し合い、様々な実例を参考にしながら、踏み込んだ協議を行うこと重要です。実際、通信キャリアはそうした努力を重ねてSMSファイアウォールの導入に至りました。100%の効果を得るのは困難でも、ある程度の効果があれば、犯罪者側の実行コストが上がり、抑止力になります。

スミッシング対策はまだまだ入り口にいると言えます。これから知恵を出し合って、より効果的な対策を実現できるよう、マクニカも様々な面で協力していきます。今後、国民が安心してネットの利便性を享受できる社会になることを切に願っています。

Co.Tomorrowing

MACNICA

マクニカは、数多くの海外企業と提携し、豊富な経験や研究により培ってきたインテリジェンスを元に、最適な最先端テクノロジーを提供をする技術商社です。ラインナップはセキュリティやネットワークインフラ、AI、DX など多岐にわたり、製品の導入から運用・サポートに至るまでの万全なサービスにより、官公庁や教育機関・一般企業など数多くのお客様への導入実績を誇ります。最先端のセキュリティ商材を提供する中で独自の研究機関を有し、日本の企業に着弾したサイバー攻撃や対策をリサーチしています。
https://www.macnica.co.jp/business/security/

Co.Tomorrowing

MACNICA

株式会社マクニカ　ネットワークス カンパニー

本社　〒222-8563 神奈川県横浜市港北区新横浜1-5-5 マクニカ第2ビル
TEL.045-470-2010　FAX.045-476-2060

西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL. 06-6227-6916　FAX.06-6227-6917