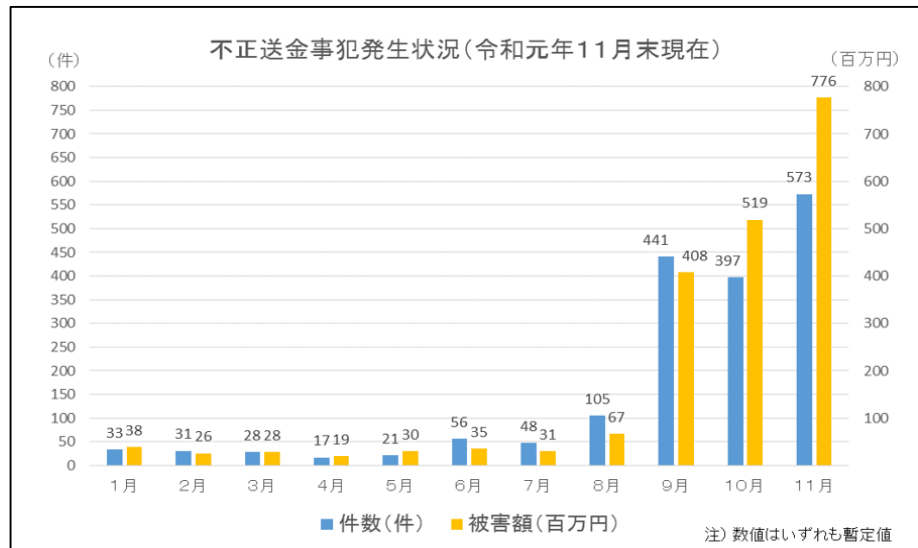
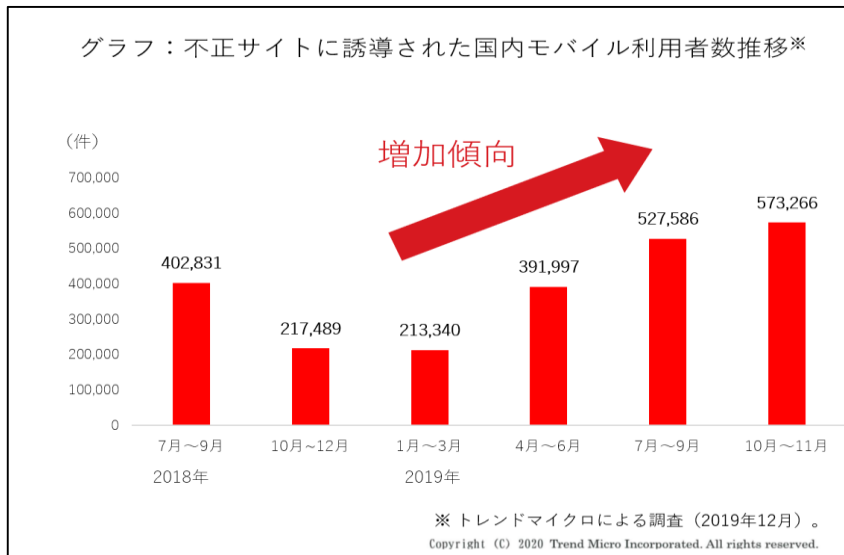


1. SMSにおけるフィッシング被害状況

- ・ 2019年は前年に続き、増加傾向
- ・ 銀行系不正送金、携帯電話キャリア決済被害の急増



SMSフィッシング被害報告件数（フィッシング対策協議会提供）

2019年	6月	7月	8月	9月	10月	11月	12月
銀行	2	0	4	11	68	63	12
クレジットカード	0	1	0	0	2	2	0
物販・EC	5	3	0	2	3	1	1
物流	8	25	16	5	6	19	20
携帯キャリア	3	5	0	0	0	0	0
計	18	34	20	18	79	85	33

警視庁発表

2. SMSにおけるフィッシング被害状況（続）

- ・ 2020年もSMSによる被害報告多数
- ・ フィッシング対策協議会の報告窓口への報告数も増加（月次報告書）

:: フィッシングに関するニュース

緊急情報 ▶▶▶ 緊急情報一覧

- ▶ 2020年07月22日 BTCBOX をかたるフィッシング (2020/07/22)
- ▶ 2020年07月09日 宅配便の不在通知を装うフィッシング (2020/07/09)
- ▶ 2020年07月08日 セブン銀行をかたるフィッシング (2020/07/08)
- ▶ 2020年06月25日 楽天をかたるフィッシング (2020/06/25)
- ▶ 2020年06月25日 [更新] au をかたるフィッシング (2020/06/25)

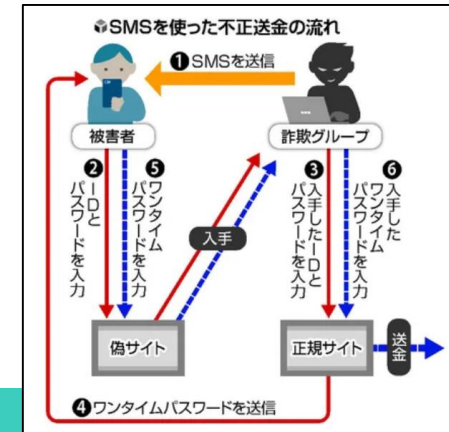
ニュース記事集 ▶▶▶ ニュース記事集一覧

- ▶ 2020年05月29日 ネット不正送金急増 4 か月被害 144 件 過去の年間最多上回る 2020/05/23 (読売新聞)
- ▶ 2020年04月02日 他人のドコモ ID 盗みゲーム機など購入 詐欺容疑で中国人 5 人逮捕 福岡県警 2020/04/01 (毎日新聞)
- ▶ 2020年03月09日 ソフトバンク、送信元が偽装された SMS への注意を呼びかけ 2020/03/05 (ケータイ Watch)
- ▶ 2020年03月03日 LINE、約 4000 人が不正ログイン被害 -- フィッシング詐欺に悪用、乗っ取りの可能性も 2020/02/28 (CNET Japan)
- ▶ 2020年02月07日 「新型コロナウイルス問題でマスク無料送付」 フィッシング詐欺に注意 2020/02/07 (熊本日日新聞社)

お荷物のお届けにあがりましたが不在の為持ち帰りました。ご確認ください。<http://.duckdns.org>

【セブン銀行】お客様の口座のご利用を一時利用停止しております。詳細は下記URLをご確認ください：<https://sevenb.com>

愛知県内のSMSによる被害が4月末で既に過去の年間最多件数を更新



3. SMSにおけるフィッシング被害状況 (続)

ドコモを装ったSMSで「異常ログインの可能性がある」「電話料金が高額になっている」などと虚偽メッセージを送信

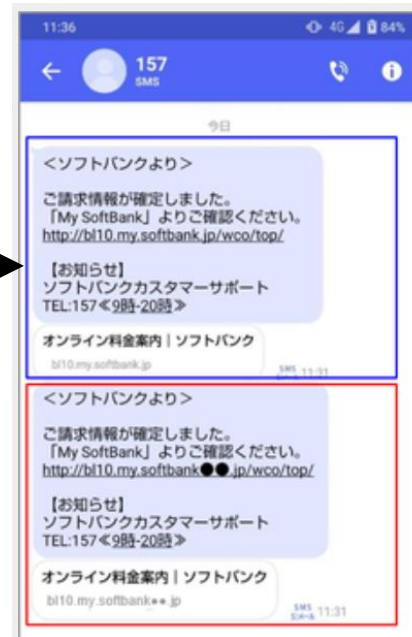
:: フィッシングに関するニュース

緊急情報 ▶ 緊急情報一覧

- ▶ 2020年07月22日 BTCBOX をかたるフィッシング (2020/07/22)
- ▶ 2020年07月09日 宅配便の不在通知を装うフィッシング (2020/07/09)
- ▶ 2020年07月08日 セブン銀行をかたるフィッシング (2020/07/08)
- ▶ 2020年06月25日 楽天をかたるフィッシング (2020/06/25)
- ▶ 2020年06月25日 [更新] auをかたるフィッシング (2020/06/25)

ニュース記事集 ▶ ニュース記事集一覧

- ▶ 2020年05月29日 ネット不正送金急増 4 か月被害 144 件 過去の年間最多上回る 2020/05/23 (読売新聞)
- ▶ 2020年04月02日 他人のドコモ ID 盗みゲーム機など購入 詐欺容疑で中国人 5 人逮捕 福岡県警 2020/04/01 (毎日新聞)
- ▶ 2020年03月09日 ソフトバンク、送信元が偽装された SMS への注意を呼びかけ 2020/03/05 (ケータイ Watch)
- ▶ 2020年03月03日 LINE、約 4000 人が不正ログイン被害 -- フィッシング詐欺に悪用、乗っ取りの可能性も 2020/02/28 (CNET Japan)
- ▶ 2020年02月07日 「新型コロナウイルス問題でマスク無料送付」 フィッシング詐欺に注意 2020/02/07 (熊本日日新聞社)



←差出人から送信された
正規のSMS

←差出人を偽装した
詐欺のSMS

フィッシングサイト
のURLになっている

送信元が偽装されたSMSは、チャット形式で受信する場合、同じスレッド内（画面）に偽装されたSMSが表示される。

4. フィッシング被害が報告されたSMS送信元

- 悪用された送信元番号は、国際網（偽装可能）、携帯SIM利用

フィッシング被害が報告されたSMS送信元
(2019年6～12月：フィッシング対策協議会提供)

種別	発信元電話番号	報告件数
国際網	国際電話番号 (+国番号から始まる)	93
国際網	アルファベット文字列	52
国際網	電話番号以外の数字	2
国内携帯	携帯電話番号 (090 等から始まる)	128
	番号不明	41
総計		316

携帯SIM利用の場合は下記両方の可能性

手作業での送信 (前頁写真)

システムへのSIM組込 (次頁)

偽装の事例、国内網と国際網の違い等の詳細資料
(携帯電話から下記に音声発信後、URLをSMSで送付)

050-5371-9990 (要番号通知)

5. フィッシングに関わる携帯SIM利用の新たな配信形態

- ・携帯キャリアとの正規契約なく、SIMカードをシステム内に組込（SIMファーム）
- ・SMSの企業利用の前提となる事前審査ができないため、携帯キャリアは提供阻止に向けた対策を実施
- ・利用企業のリスク：①送信元共用によるフィッシング、②サービス安定提供



詳細資料（音声発信後、URLをSMSで送付） **050-5371-9990**