

02	目次・特集「個人情報を守るために」
08	市政「未来ポスト」～皆さんの声～
10	人事行政の運営等の状況
12	トップニュース ICOCA 対応地域が拡大します／動鳴気峡桜まつり・夜桜ライトアップを開催します ほか
18	情報ボックス 路線バス・住民バスの有料広告を募集します／一般不妊治療費を助成します ほか
24	相談日程等
26	みんなの広場
30	みんなの彩時記 見て、触れて、体験して雪あそびを満喫／ジュニア駅伝田辺市が 3 回目の優勝 ほか



今月の表紙写真

今月の表紙は、田辺警察署の金澤警部補がサイバーパトロールを行っている様子を撮影しました。日々、私たちの安全を見守ってくれています。

紙面で使用するマーク等の説明

日…日付・期間	冠…定員
時…時間	料…料金・費用
休…休館日	持…持ち物
場…場所	申…申込み・申請方法
集…集合	問…問合せ
内…内容	[消印]…消印有効
対…対象・参加資格等	[先着]…先着順

◇冠マークには、振替休日等も含まれます。
◇料金や申込み方法の記載のないものは、不要です。
◇市役所の開庁時間（申込み・問合せ等の受付を含む。）は、冠を除く日～金の 8 時 30 分～17 時 15 分です。毎週冠は、市民課・保険課・税務課の一部窓口を 19 時まで延長しています。

特集 個人情報を守るために

パソコンや携帯電話等でもインターネットを利用することは当たり前になってきています。しかし、その利用者を狙って不正に個人情報や金銭を奪おうとする人もいます。皆さんのところには、思い当たるようなメールが届いたことはありませんか。

田辺警察署生活安全刑事課
0739(23)0110

お客様の【××銀行の口座】セキュリティ強化、カード・通帳の利用停止、再開のお手続きの設定をしてください。
<http://s×××.jp>

お客様宛にお荷物のお届けに上がりましたが不在のため持ち帰りました。
配送物は以下よりご確認ください。
<http://××/大手宅配業者名>

ご利用中の●●会員アカウントへのログインが確認されました。

ログイン記録にお心当たりがない場合は、下記のリンクをクリックして、安全なサーバーを使用してアカウントにログインしてください。

[続けるにはこちらをクリック](#)

【●●】お客様の●●銀行口座に対し、第三者からの不正なアクセスを検知しました。ご確認ください。
<http://●●-ic.com>

会員登録の未納料金が発生しております。本日中にご連絡がない場合、法的手続きに移行します。
●●カスタマーセンター
03×○×○×○×○



身近に忍び寄るサイバー犯罪

そのメッセージは大丈夫？

3 ページで例を挙げているメッセージは、最近多発している『スミッシング』と呼ばれるサイバー犯罪の可能性がります。皆さんも、似たようなメッセージを見たことがあるのではないのでしょうか。

スミッシングとは、携帯電話等で使用するSMS（ショートメッセージサービス）を利用して、金融機関やショッピングサイトなどを装いメッセージを送り、不正サイトへ誘導し、ID やパスワード、クレジットカード番号、氏名、住所などの個人情報を入力させて盗む方法です。

SMS は、相手のメールアドレスが分からなくても電話番号だけで文字メッセージを送受信することが出来ます。つまり、スミッシング犯は、適当に11桁の数字を並べるだけで、いろんな方の携帯電話等にメッセージを送ることが出来るので、誰もが受け取る可能性を持っているのです。

スミッシングの被害とは

スミッシング犯は、宅配業者などを装ってメッセージを送信します。その文面には「本物の案内のような文章」と「ホームページを開くためのアドレス」が書かれています。そのアドレスを押すと、本物のホームページに似せたページが開き、メッセージ受信者は、ID やパスワード、クレジットカード番号、氏名、住所などの個人情報を入力してしまいます。スミッシング犯は、入力された情報を盗み、受信者にあらゆる被害をもたらします。

他にも、銀行を装った手口では、口座番号やパスワードを入力してしまふと、たった数分で受信者の銀行口座から不正に送金されてしまふ被害に遭うこともあります。

また、個人情報を入力させる以外にも、偽のアプリを取得させ、携帯電話等をウイルス感染させることもあります。そうすると、個人情報盗まれるだけでなく、携帯電話が遠隔操作される可能性もあり、様々な犯罪に悪用されることが予想されます。

■和歌山県警でのサイバー犯罪に関する相談件数等（カッコ内は田辺署）

		H26	H27	H28	H29	H30	R1
相談件数	詐欺・悪質商法等に関する相談 (インターネットオークション被害を除く。)	729	720	745	697	502	765
	インターネットオークションに関する相談	72	71	46	59	56	47
	名誉棄損、誹謗中傷、脅迫に関する相談	78	101	100	91	90	82
	児童の誘い出し、児童ポルノの流布等、特定の児童に関する相談	2	5	4	4	4	5
	不正アクセス、ネットワークセキュリティに関する相談	113	38	66	95	98	108
	コンピュータウイルスに関する相談	1	11	9	21	9	21
	迷惑メール、スパムメールに関する相談	112	159	138	99	126	127
	クレジットカード番号盗取等クレジットカード犯罪に関する相談	44	16	18	24	45	55
	違法有害なホームページ・掲示板等の通報、取締り要望	24	28	26	20	19	13
	プロバイダとの契約、トラブル等	9	10	8	5	3	6
	その他	133	149	208	195	155	162
	合計	1317 (107)	1308 (121)	1368 (109)	1310 (76)	1107 (53)	1391 (92)
検挙件数		46	55	56	58	92	71
検挙人数		50	47	51	58	48	42

▼実際にあった相談内容▼

インターネットショッピングで商品を購入し、指定された口座へ代金を振り込んだにも関わらず、商品が届かず、相手とも連絡が取れない。

身代金要求型ウイルス「ランサムウェア」に感染してコンピュータがロックされ、それを解除するために金銭の支払いを求められた。

掲示板サイトに個人を誹謗中傷する内容を書き込まれた。

オンラインゲームのアカウントを乗っ取られ、ゲーム内のアイテムを勝手に利用された。

ホームページにわいせつな画像が掲載されている。

メールのフィルタリング設定を行っても、アドレスが変更された大量の迷惑メールが届く。

「料金体系が安くなる」と電話で勧誘され、プロバイダを変更したが安くならない。

相談件数はほぼ横ばい

サイバー犯罪は、刑法や特別法を問わず様々な犯罪にわたることが多いため、正確な統計を出すことは難しいそうです。警察がサイバー犯罪だと認知するのは各種の相談から始まることが多いことから、相談件数をサイバー犯罪の目安としています。

近年、サイバー犯罪に関する相談件数はほぼ横ばいで推移（上表参照）していますが、サイバー犯罪は日々多様化しているため、今後増える可能性は十分に考えられます。また、左記にあるような相談は、老若男女関係なく寄せられるので、他人事だとは思わず、まずはサイバー犯罪について知ることから始めてみてはいかがでしょうか。

スミッシングだけではないサイバー犯罪

サイバー犯罪とは、コンピュータ技術や電気通信技術を悪用した犯罪で、大きく分けて次の3つの類型に分類されます。



不正アクセス禁止法に該当する行為

- ◇フィッシングや不正プログラム等により得たアカウントを用いて他人になりすまし、アクセス制御されているコンピュータを不正に使用する行為
- ◇システムの脆弱性を突いて、アクセス制御されているコンピュータを不正に使用する行為



コンピュータや電磁的記録を対象とする犯罪

- ◇コンピュータ等を不正に使用する犯罪
- ◇コンピュータウイルスに関する犯罪



実行の手段として高度情報通信ネットワークを利用する犯罪

- ◇インターネットを介してわいせつ画像の掲載や児童ポルノの販売・頒布
- ◇インターネットを介して脅迫、名誉棄損等の行為

被害に遭わないために

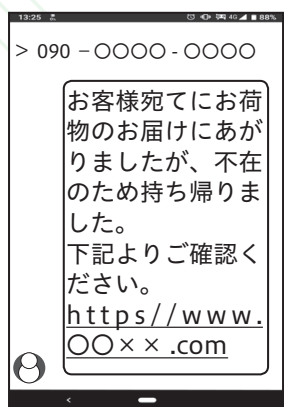
冷静な対応で被害を防ごう

被害を防ぐためには、正しい知識と冷静な対応が重要です。スミッシングへの対応を紹介しますので、実際に不審なメッセージが届いたときは、参考にしていただき、冷静に対応しましょう。

①メッセージが届いたとき

- 身に覚えのない番号や名前からのメッセージは注意しましょう。
- ※ 番号やアドレスに本物の企業名が表示されている場合もあります。
- アドレスを押す前に、本物の企業等のアドレスかどうか確認しましょう。

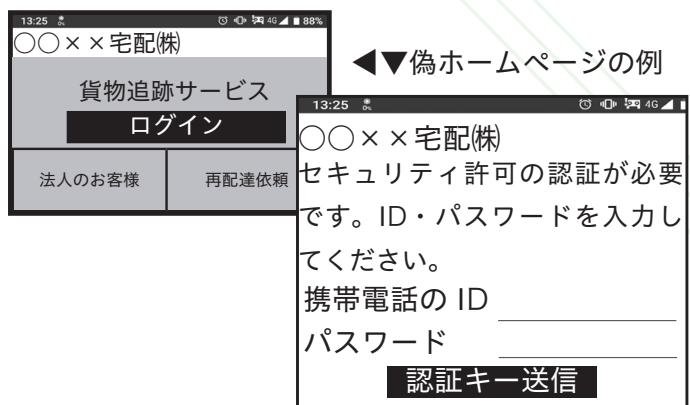
不審なメッセージの例



②アドレスを押してしまったら

- 本物によく似た偽ホームページにつながります。
- 不正アプリがダウンロードされる場合があるので、ホームページ上の「ログイン」や「次へ」などのボタンは押さずにページを閉じましょう。
- 認証を求められても、ID、パスワード、クレジットカード番号、氏名、住所などの個人情報を入力しないようにしましょう。

偽ホームページの例



サイバーセキュリティ対策5か条

～インターネットを安全に利用するために～

1. ウイルス対策ソフトを導入しよう
2. パソコン・携帯電話等のソフトウェアを最新の状態にしよう
3. ID・パスワードの使い回しは避けよう
4. 定期的にバックアップを取ろう
5. 脅威や攻撃の手口を知り、対策方法を学ぼう

③個人情報を入力してしまったら

- パスワードを入力してしまった場合は、本物のホームページからパスワードを再度変更しましょう。
- クレジットカード番号や銀行口座の情報を入力してしまった場合は、クレジット会社や銀行に電話して、クレジットカードや口座の停止手続をしましょう。



コンピュータウイルスの感染が疑われる場合や、クレジットカードが不正利用された場合は、警察に相談しましょう。

田辺警察署の取組

セキュリティ意識向上へ

田辺警察署では、昨年度から出前型のサイバーセキュリティ講演会を行っています。昨年度の企業向けの講演には延べ700名ほどの方が受講。今年度は、県内では初めての試みとなる中学生と高校生を対象とした講演を行いました。スマートフォンを偽のアプリからウイルス感染させ、遠隔操作する実演で、セキュリティ対策の重要性を体感してもらいました。



田辺高校での講演会の様子

サイバーセキュリティの講演を聞いた中・高校生にインタビューしました



田辺高校2年 溝端 大い さん

ちょうど最近、お父さんの携帯に、講演で紹介された業者さんから送られてきたメールが送られてきて、偽物か本物か見分けが付きにくいので、簡単には押さないようにしたいと思っています。

携帯に送られてくるメールをボタン一つ押ただけで遠隔操作されるようなことにつながったりするのは想像もしていなかったです。普段 SNS を使うことがありますが、個人を特定されるような写真を載せないなど気を付けています。今回の話を聞いて、より注意して使わないといけないと感じました。



田辺中学校3年 岸裏 未波 さん

いつ被害に遭うかわかりません

インターネットは、企業活動や日常生活に浸透し、とても利便性の高いものです。一方で、悪意ある者によるパソコンや携帯電話等を狙った犯罪は、年々深刻化し、犯行の手口も悪質巧妙化しています。最近では、世界的に利用されている複数の SNS で何千万人分という大規模な個人情報の流出が明らかになりました。知らない間に自分も被害に遭っていることがあるので、まずはどんな手口があるのかを知っておくことが重要です。

自分には関係がないと思う方も少なくありませんが、このようにな犯罪は身近に潜んでいます。対策としては、パスワードを適切に管理することやウイルス対策ソフトを導入することなどを心がけてください。被害に遭わないよう物理的にも意識の上でもセキュリティ対策をとることが肝心です。

田辺警察署
生活安全刑事課課長代理
奥地 隆文 警部