2018年セキュリティ重大ニュース（1）

<https://securitynews.so-net.ne.jp/topics/sec_00013.html>

2018年のセキュリティニュースを振り返ると、メールを使って金銭を騙し取る攻撃が巧妙さを増していることがわかる。性的脅迫メール、災害便乗メール、詐欺メールなどが出回り、被害を受ける人が続出した。インチキ広告が蔓延し、不正アクセスによる情報流出も相次いだ。

**仮想通貨を要求するセクストーション（性的脅迫）メール出回る**

　「あなたがアダルトサイトを見ている様子を撮影した。家族や友人、同僚にばらまかれたくなければ、仮想通貨で〇〇〇ドルを支払え」と脅すメールが、9月中頃から撒布されている。海外で出回っていたセクストーション（性的脅迫）メールの日本語版だ。



　攻撃者は、メールアカウントをハッキングした、パソコンをウイルスに感染させた、ルーターの脆弱性を突いて悪質なコードを仕込んだなどと主張。あなたの行為を撮影し、（この動画を送り付けるために）メールやSNS、メッセンジャーの連絡先を盗み取ったとしているが、これらはすべて真っ赤な嘘だ。  
  
　メールの件名は「AVアラート」「あなたの心の安らぎの問題。」「すぐにお読みください！」などさまざまで、本文にも複数のパターンがある。11月下旬からは、「あなたのパスワードが侵害されました」という件名で、ボットネット経由で撒布されている。  
  
　「何てことだ！ あなたはとても面白くて揺らめいています！」「ああ、私の神、あなたのようなもの...」「あなたは大きな変態です。 無限のファンタジー！」など、機械翻訳によるおかしなフレーズがちりばめられていることも多い。  
  
　メールアカウントが本当に乗っ取られていると錯覚させる目的で、差出人（From）を［受信者自身のメールアドレス］に偽装してあったり、受信した人が実際に使用したことのあるパスワードが記載されたりしていることもある。セキュリティ関連の団体や企業などから注意喚起が行われているが、不安になってしまう方も多いようで、So-netを含めプロバイダー各社にも相談が寄せられている。  
  
**＜関連記事＞**  
・「仮想通貨を要求する日本語の脅迫メール」出回る、騙されて送金しないよう注意  
[https://security-t.blog.so-net.ne.jp/2018-09-21](https://security-t.blog.so-net.ne.jp/2018-09-21?SmRcid=SECN-BLOG20180921_00013)  
・ボットネットが大規模にばらまく悪質な迷惑メールに注意  
[https://security-t.blog.so-net.ne.jp/2018-11-30](https://security-t.blog.so-net.ne.jp/2018-11-30?SmRcid=SECN-BLOG20181130_00013)  
・仮想通貨（ビットコイン）を請求する詐欺メールに注意  
[https://security-t.blog.so-net.ne.jp/2018-11-19](https://security-t.blog.so-net.ne.jp/2018-11-19?SmRcid=SECN-BLOG20181119_00013)

**「当選詐欺」「アプリ押し売り」「サポート詐欺」などインチキ広告が蔓延**

　Webサイトに広告を配信する仕組みを利用して、悪質な広告が配信されている。　　「Googleメンバーシップ・リワード」などと称してブラウザ上に「おめでとうございます！」とメッセージを表示させ、アンケートに回答するとスマートフォンなど豪華な景品がもらえると誘う「当選詐欺」も、インチキ広告の一つだ。アンケートに答えてクレジットカード情報を登録した後に賞品としてもらえるのは、有料サービスやアプリを無料または数百円で試す権利のみだ。しかも数日後には自動的にプレミアム会員に登録されてしまい、クレジットカードから毎月、会費数千円が引き落とされることになる。Googleのほかに、Apple、au one net、Softbank、NTT、ケイ・オプティコム、amazon、日本郵便、宅急便、ヤマダ電機、ラオックスなどの名前も使われている。  
  
　「ウイルスに感染しています」「エラーが発生しました」などとブラウザに表示させて驚かす手口もある。セキュリティソフトやメンテナンスソフトといったアプリの押し売りや、電話をかけさせて有償サポートの契約を結ばせることが目的だ。国民生活センターには今年上半期に2135件の相談が寄せられており、前年同期の1601件から3割増となっている。  
  
　5月には、メッセージングサービス「Skype」のアカウントを乗っ取り、連絡先として登録されている人に、上記と同様の当選詐欺のサイトや、Mac用のユーティリティソフト「MacKeeper」のインストールを促すサイト、海外の出会い系サイトなどのリンクを送り付ける「URLスパム騒動」も発生した。  
  
**＜関連記事＞**  
・日本郵便を装うアンケートに注意、当選に見せかけ有料サイトに登録  
[http://security-t.blog.so-net.ne.jp/2018-04-03-1](http://security-t.blog.so-net.ne.jp/2018-04-03-1?SmRcid=SECN-BLOG20180403_00013)  
・「おめでとうございます！」通知に注意、賞品につられて有料会員登録  
[https://security-t.blog.so-net.ne.jp/2018-07-27](https://security-t.blog.so-net.ne.jp/2018-07-27?SmRcid=SECN-BLOG20180721_00013)  
・ネットのインチキ広告にご用心、課金サイトやアプリの罠  
[https://security-t.blog.so-net.ne.jp/2018-06-28](https://security-t.blog.so-net.ne.jp/2018-06-28?SmRcid=SECN-BLOG20180628_00013)  
・偽の警告画面に注意、ソフトウェア購入やサポート契約の相談が増加  
[https://security-t.blog.so-net.ne.jp/2018-07-19](https://security-t.blog.so-net.ne.jp/2018-07-19?SmRcid=SECN-BLOG20180719_00013)  
・ネット閲覧中の「偽セキュリティ警告」に注意――詐欺的誘導で合法的に料金徴収  
[https://security-t.blog.so-net.ne.jp/2018-11-08](https://security-t.blog.so-net.ne.jp/2018-11-08?SmRcid=SECN-BLOG20181108_00013)  
・Skype乗っ取りか、「URLスパム騒動」発生――うっかりクリックした場合の対処法  
[https://security-t.blog.so-net.ne.jp/2018-05-25](https://security-t.blog.so-net.ne.jp/2018-05-25?SmRcid=SECN-BLOG20180525_00013)

**災害に便乗する不審メールやデマ情報が拡散、偽募金サイトも**

　豪雨、台風、地震など、自然災害が猛威を振るった2018年。災害が発生したとき、インターネットは情報を受発信するために役立つが、残念なことにデマの拡散や詐欺行為にも使われてしまう。  
  
　今年も災害発生後に「〇時間後にまた大きな地震が起こる。消防署の人から聞いた」、「〇〇市はもうすぐ断水する」、「〇時間後に携帯電話が使えなくなる」、「レスキュー隊の服を着た窃盗グループが被災地に入っている」、「電車が脱線した」、「京セラドームにひびが入った」「シマウマが脱走した」などのデマが拡散。問い合わせを受けた自治体や警察、関連機関が、デマ情報に惑わされないようWebサイトやツイッターで注意を呼びかけるなどの対応をした。



　偽の募金サイトも複数回出現した。見つかったのはYahoo!基金が開設していた「平成30年7月豪雨緊急災害支援募金」のサイトをまねたフィッシングサイトで、クレジットカードの情報や、電子マネー「WebMoney」のプリペイド番号およびウォレットのアカウント情報を盗み取ろうとしていた。  
  
　「緊急災害警報」「大雨速報」などとしてURLを開かせようとする迷惑メールも多数確認された。大半は出会い系サイトへの誘導を目論むメールなのだが、11月にはマルウェア（ウイルス）感染を狙った「津波警報発表」という件名のメールがばらまかれた。差出人は気象庁とされており、対象地域はリンク先で確認するようにと本文に記載されている。リンクをクリックするとマルウェアのファイルがダウンロードされ、Windowsではこのファイルを開くと感染してしまうおそれがあった。  
  
**＜関連記事＞**  
・災害に便乗した不審メールやデマ情報が拡散、偽のネット募金サイトにも注意  
[https://security-t.blog.so-net.ne.jp/2018-09-11-1](https://security-t.blog.so-net.ne.jp/2018-09-11-1?SmRcid=SECN-BLOG20180911_00013)  
・最新フィッシング事情――LINEでアクター増殖、狙われるキャリア決済、「偽佐川急便」参戦、「偽募金サイト」稼働中  
[https://security-t.blog.so-net.ne.jp/2018-10-15](https://security-t.blog.so-net.ne.jp/2018-10-15?SmRcid=SECN-BLOG20181015_00013)  
・気象情報や災害関連情報を装う迷惑メールに注意  
<https://security-t.blog.so-net.ne.jp/2018-10-09>  
・気象庁の「津波警報発表」を装うマルウェアメールに注意  
[https://security-t.blog.so-net.ne.jp/2018-11-12](https://security-t.blog.so-net.ne.jp/2018-11-12?SmRcid=SECN-BLOG20181112_00013)

**不正アクセスによる個人情報やクレジットカード情報の流出相次ぐ**

　不正アクセスによる個人情報の流出が今年も相次いだ。流出情報の悪用も発生している。森永乳業の通販サイト（5月公表）では、サーバーの脆弱性を突かれて顧客情報約9万3000名分が流出。クレジットカード情報2万9773名分も流出し、約300件、2000万円の不正費用被害が発生した。新日本造形（11月公表）、タオル販売の伊織（10月公表）、アサヒ軽金属（8月公表）、エースコンタクト（5月公表）の件でも、カードの不正利用が確認されている。  
  
　聖教新聞社の「SOKAオンラインサイト」（10月公表）からは、顧客情報約18万1700件が流出。カード情報も2481件流出した。サーバーに不正ファイルを混入され、プログラムが改ざんされていたという。この件では、利用者がカード決済を利用しようとすると偽の画面が表示され、カード情報を入力して送信ボタンを押すとエラー画面が表示された後、本物の決済画面に遷移するという新しい手口が使われた。利用者からすると偽画面、本物の決済画面と、2回カード情報を入力することになり、偽画面で入力した内容が攻撃者に渡ってしまっている。この後に発生した上記の伊織の件でも、同じ手口が使われていた。  
  
　群馬県前橋市では、教育委員会のネットワークから、2012年度から2017年度までに在籍したすべての児童生徒と教職員、計4万7839名について、給食費のデータが流出した（4月公表）。サーバーに脆弱性があったことと、データセンター内のファイアウォールの設定に不備があったことが原因だった。流出したのは氏名、性別、生年月日、住所、電話番号、保護者氏名などの情報で、2万8209件については口座情報も含まれていた。  
  
　流出件数が10万件を超えたのは、上記SOKAオンラインサイトのほか、覆面調査サービスなどを手掛けるMS&Consultingの約57万件（5月公表）、デジタルコンテンツを販売するDLmarketの56万1625件（10月公表）、プレミアム・アウトレットの約27万件（4月公表）だった。  
  
**＜関連記事＞**  
・不正アクセスによる情報流出相次ぐ――年収含む個人情報、クレジットカード情報など  
[https://security-t.blog.so-net.ne.jp/2018-03-16](https://security-t.blog.so-net.ne.jp/2018-03-16?SmRcid=SECN-BLOG20180316_00013)  
・個人情報流出相次ぐ――市立学校の全児童生徒情報流出のおそれ（前橋市）ほか  
[https://security-t.blog.so-net.ne.jp/2018-04-13](https://security-t.blog.so-net.ne.jp/2018-04-13?SmRcid=SECN-BLOG20180413_00013)  
・不正アクセスによる情報流出相次ぐ――クレカ情報流出で不正利用被害も発生  
[https://security-t.blog.so-net.ne.jp/2018-06-12](https://security-t.blog.so-net.ne.jp/2018-06-12?SmRcid=SECN-BLOG20180612_00013)  
・「不正ログイン」で高額な不正購入や個人情報流出の被害発生――PW守る対策を  
[https://security-t.blog.so-net.ne.jp/2018-08-17](https://security-t.blog.so-net.ne.jp/2018-08-17?SmRcid=SECN-BLOG20180817_00013)  
・企業、自治体、大学などで個人情報流出が相次ぐ  
[https://security-t.blog.so-net.ne.jp/2018-10-11](https://security-t.blog.so-net.ne.jp/2018-10-11?SmRcid=SECN-BLOG20181011_00013)



**個人情報求める詐欺メール（当選通知、モニター募集など）大量観測**

　国内の企業をかたった偽の当選通知メールや、偽のモニター募集メールが、5月から6月にかけて大量に観測された。賞品またはモニター対象の製品を発送するために必要だなどとして、氏名、住所、電話番号を返信させて騙し取ろうとする詐欺メールだ。日本語としてまったくおかしなところがないメールもあったが、「おめでとうござます！」、「もれのないように詳細にご明記をして」など首をかしげたくようなフレーズが書かれたものもあった。  
  
　「動画見放題のプレミアムサービスの申し込みを受け付けた」、「有料動画サイトにて同時登録がされている」、「無料サービスから有料化へのご連絡」といった文面の詐欺メールも出回っている。身に覚えはないけれど念のために退会の処理をしておこうと考える人、あるいは前に使っていたあのサービスのことかもと思ってしまう人がターゲットだ。リンク先には、氏名、住所、電話番号を書き込む「退会フォーム」が用意されている。数年前から使われている手口で、Gmailのアドレスからメールが送られてくるという特徴がある。  
  
　こうしたメールに返信したり、入力フォームに記入して送信したりしてしまうと、個人情報をメールアドレスとセットで詐欺師に渡してしまうことになる。その後、架空請求のメールやハガキを送り付けられたり、詐欺目的の電話がかってきたりする可能性がある。  
  
**＜関連記事＞**  
・偽の「当選通知メール」に注意、多くの著名企業を名乗りばらまき  
[https://security-t.blog.so-net.ne.jp/2018-05-17](https://security-t.blog.so-net.ne.jp/2018-05-17?SmRcid=SECN-BLOG20180517_00013)  
・偽の「当選通知メール」「モニター募集メール」に注意、ばらまき継続中  
[https://security-t.blog.so-net.ne.jp/2018-06-15](https://security-t.blog.so-net.ne.jp/2018-06-15?SmRcid=SECN-BLOG20180615_00013)  
・詐欺メールに注意、「有料化のご連絡」「動画見放題サービスのお申込み」等で誘引  
[https://security-t.blog.so-net.ne.jp/2018-05-21](https://security-t.blog.so-net.ne.jp/2018-05-21?SmRcid=SECN-BLOG20180521_00013)

2018年セキュリティ重大ニュース（2）

<https://securitynews.so-net.ne.jp/topics/sec_00016.html>

2018年は国内フィッシングが過去最大の規模になり、宅配便の不在通知を装うSMSがこれまでにない規模でばらまかれ、架空請求に悩む人の相談件数も増加の一途をたどった。不正ログインによる金銭被害が相次ぎ、家庭Wi-Fiの危うさも明らかになった。どんな手口でどのような被害が起きているのか、攻撃と被害の実態を知ることで、安全対策の一歩として頂きたい。

**国内フィッシングが過去最大規模に――標的はクレカ、キャリア決済**

　実在する企業やサービスになりすまし、アカウント情報やクレジットカード情報などの情報を騙し取る国内のフィッシングが、過去最大の規模になりました。JPCERT/CCに報告された2017年のフィッシングサイトの件数は、過去最多の3306件でしたが、2018年は9月末時点で3440件と、昨年の記録を上回ってしまいました。前年同期の2454件から1.4倍に膨れあがっています。



　多発しているフィッシングのほとんどは、最終的には金銭を得ることを目的としています。2013年頃から急増したオンラインバンキングのアカウントを狙ったフィッシングは、2016年上半期でほぼ収束し、その代わりにクレジットカード情報を騙し取るフィッシングが主流になりました。楽天カードや三菱UFJニコス、クレディセゾンといったクレジットカード会社を装うフィッシングはもちろん、アップルやアマゾンを装うフィッシングもまた、クレジットカード情報を騙し取ろうとします。特にこの2ブランドは、複数の攻撃グループが、休むことなく毎日、偽サイトに誘導するメールやSMSをばらまき続けました。  
  
　2018年に新たな標的となったのが、携帯電話の通信事業者が提供する「キャリア決済サービス」です。利用した料金を月々の料金と一緒に引き落とすサービスで、対応サイトでクレジットカードと同じように利用できます。それに目を付けた攻撃グループが、2月頃からフィッシングを仕掛けるようになりました。標的は、サービスを提供するNTTドコモ、ソフトバンク、KDDI（au）の3社に加え、支払い方法にキャリア決済が設定できる、アップルのサービスも狙われました。8月以降は、宅配便の不在通知を装うSMSの誘導先にも、iPhoneユーザーのキャリア決済を狙ったフィッシングサイトが仕掛けられるようになりました。  
 **＜関連記事＞**・2018年1月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-02-23](https://security-t.blog.so-net.ne.jp/2018-02-23?SmRcid=SECN-BLOG20180420_00016)  
・2018年2月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-03-20](https://security-t.blog.so-net.ne.jp/2018-03-20?SmRcid=SECN-BLOG20180320_00016)  
・2018年3月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-04-20](https://security-t.blog.so-net.ne.jp/2018-04-20?SmRcid=SECN-BLOG20180420_00016)  
・2018年4月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-05-25-1](https://security-t.blog.so-net.ne.jp/2018-05-25-1?SmRcid=SECN-BLOG20180525_00016)  
・2018年5月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-06-22](https://security-t.blog.so-net.ne.jp/2018-06-22?SmRcid=SECN-BLOG20180622_00016)  
・2018年6月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-08-01](https://security-t.blog.so-net.ne.jp/2018-08-01?SmRcid=SECN-BLOG20180801_00016)  
・2018年7-8月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-10-15](https://security-t.blog.so-net.ne.jp/2018-10-15?SmRcid=SECN-BLOG20181015_00016)  
・2018年9月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-10-31](https://security-t.blog.so-net.ne.jp/2018-10-31?SmRcid=SECN-BLOG20181031_00016)  
・2018年10月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-11-27](https://security-t.blog.so-net.ne.jp/2018-11-27?SmRcid=SECN-BLOG20181127_00016)  
・2018年11月の国内フィッシング事情  
[https://securitynews.so-net.ne.jp/topics/sec\_00005.html](https://securitynews.so-net.ne.jp/topics/sec_00005.html?SmRcid=SECN-00005_00016)

**宅配便の不在通知装うSMS猛威――AndroidとiPhoneで異なる手口**

　宅配便の不在通知を装い、佐川急便の偽サイトへと誘導するSMS（携帯電話番号あてに短文を送るショートメッセージ）が、2017年12月から観測されるようになりました。誘導先でAndroid端末に対し、端末内の情報を窃取する偽アプリをインストールさせようとする攻撃でした。SMSは、その後も断続的にばらまかれ、2018年5月ごろから偽アプリにSMSの送受信機能が備わりました。そして7月、偽アプリがインストールされた端末が一斉に、不在通知を装うSMSを送り始めました。これまでにないおびただしい数のSMSが、不特定多数の携帯電話番号あてに送りつけられたのです。騙されて偽アプリをインストールしてしまうユーザーが相次ぎ、今度は自身の端末から不在通知SMSが送信されたり、キャリア決済を勝手に使われたりといった被害が全国から報告されました。  
  
　8月に入り偽サイトがリニューアルすると、それまで対象外だったiPhoneに対しフィッシングを仕掛けるようになりました。アクセスしてきた端末がAndroidの場合には、これまでどおり偽アプリを投下しますが、iPhoneなどのiOS端末の場合には、フィッシング用の偽サイトへと転送し、「Apple社から送られた製品はセキュリティ許可の認証が必要となります」と偽り、携帯番号とSMSで届くコードの入力を求めます。これは、アップルのサービスにユーザーのキャリア決済を登録して使い込む手口で、iTunesカードが勝手に買われる被害が発生しました。  
  
▼**SMSに書かれているURLを開くと、佐川急便の偽サイトの画面が表示され、Android端末はアプリをダウンロードしようとする（左）。iPhoneは別の偽サイトに転送され、Apple IDとパスワード（中）か電話番号と認証コード（右）を詐取しようとする。**



　一連の攻撃は、9月に落ち着きを見せましたが、10月から再び活発化し、iPhone用には、新たにApple IDとパスワードを詐取するフィッシングサイトも用意されました。12月には、ヤマト運輸をかたる同様の手口も登場しましたが短時間で終了し、その後も佐川急便を装う攻撃が相変わらず続いています。  
 **＜関連記事＞**・宅配便の不在通知を装うSMSに注意、誘導先に怪しいアプリ  
[https://security-t.blog.so-net.ne.jp/2018-01-19](https://security-t.blog.so-net.ne.jp/2018-01-19?SmRcid=SECN-BLOG20180119_00016)  
・宅配便の不在通知を装うSMSに注意、怪しいAndroidアプリを投下  
[https://security-t.blog.so-net.ne.jp/2018-04-03](https://security-t.blog.so-net.ne.jp/2018-04-03?SmRcid=SECN-BLOG20180403_00016)  
・宅配便の不在通知を装うSMS急増、誘導先でマルウェア感染のおそれ  
[https://security-t.blog.so-net.ne.jp/2018-07-23](https://security-t.blog.so-net.ne.jp/2018-07-23?SmRcid=SECN-BLOG20180723_00016)  
・止まらない不在通知SMS、不明なアプリのインストールは厳禁  
[https://security-t.blog.so-net.ne.jp/2018-08-03](https://security-t.blog.so-net.ne.jp/2018-08-03?SmRcid=SECN-BLOG20180803_00016)  
・2018年7-8月の国内フィッシング事情  
[https://security-t.blog.so-net.ne.jp/2018-10-15](https://security-t.blog.so-net.ne.jp/2018-10-15?SmRcid=SECN-BLOG20181015_00016)  
・宅配便の不在通知を装うSMSが再び増加――AndroidとiPhoneで異なる被害  
[https://security-t.blog.so-net.ne.jp/2018-12-04](https://security-t.blog.so-net.ne.jp/2018-12-04?SmRcid=SECN-BLOG20181204_00016)

**被害膨らむ「架空請求」――不安をあおりコンビニ決済など悪用**

　利用した覚えのない請求に悩む人が増えています。国民生活センターに2018年4月から9月に寄せられた相談は、前年同期の6万5315から11万8544と、約1.8倍に増加しました。通年で8万3491件から19万9537件へと大幅に増加した前年度から、さらに上昇しています。



　主な手口は、電子メール、SMS、ハガキ、封書です。電子メールは、かつてほどではありませんが、コンスタントにばらまかれています。実在する企業やサービスを名乗るものや、弁護士や債権回収業者を装うものも多く、メールに記載したリンク先で偽の訴状を見せて不安をあおる手口も使われています。携帯電話番号あてに短文を送るSMSは、メールよりもはるかに広範囲にばらまかれています。文字数制限から、「コンテンツ利用料金の精算確認が取れません。本日ご連絡なき場合には法的手続きに移行致します。」というような短文に電話番号を記載した内容です。  
  
　実在する企業を装うものでは、アマゾンが過半数を占めるほか、楽天やグーグル、DMMを装うものや実在する弁護士事務所を名乗るものもあります。かつて流だった郵便ハガキによる架空請求が前年から急増し、2018年は封書を使用したものも多発しました。ハガキや封書には、法務省の関係機関を装うものが多く、「少額消費料金未納に関する訴訟最終告知のお知らせ」などと題したものを送りつけ、訴訟取り下げの相談にのるなどと言って、記載した連絡先に電話をかけさせるように仕向けます。  
  
　手段はいろいろですが、電話をかけさせようとする手口が大半で、連絡して来た人を言葉巧みにだまし、支払う必要のない料金を騙し取ろうとします。支払い方法も様々ですが、コンビニでプリペイドカード（ギフト券）を購入させ、カード番号を連絡させて騙し取る方法や、支払番号を伝えてコンビニの端末やレジで支払うコンビニ収納（コンビニ決済）を悪用した手口がよく用いられています。  
 **＜関連記事＞**・「架空請求詐欺」被害倍増、「有料サイトの未納料金が発生しています」は無視を  
[https://security-t.blog.so-net.ne.jp/2018-02-09](https://security-t.blog.so-net.ne.jp/2018-02-09?SmRcid=SECN-BLOG20180209_00016)  
・架空請求の相談急増、国民生活センターが注意呼びかけ  
[https://security-t.blog.so-net.ne.jp/2018-04-25](https://security-t.blog.so-net.ne.jp/2018-04-25?SmRcid=SECN-BLOG20180425_00016)  
・まだまだ続く架空請求SMS、消費者庁が注意呼びかけ  
[https://security-t.blog.so-net.ne.jp/2018-07-04](https://security-t.blog.so-net.ne.jp/2018-07-04?SmRcid=SECN-BLOG20180704_00016)  
・2017年度の消費者トラブル1万件、「架空請求」「悪質ネット通販」「情報商材」など  
[https://security-t.blog.so-net.ne.jp/2018-09-11](https://security-t.blog.so-net.ne.jp/2018-09-11?SmRcid=SECN-BLOG20180911_00016)  
・あの手この手で迫る「架空請求」にご用心  
[https://security-t.blog.so-net.ne.jp/2018-11-22-1](https://security-t.blog.so-net.ne.jp/2018-11-22-1?SmRcid=SECN-BLOG20181122_00016)

**不正ログインで金銭被害――高額商品の購入やポイント消費**

　NTTドコモが運営する通販サイト「ドコモオンラインショップ」で不正ログインが行われ、高額なスマートフォン「iPhone X」を勝手に購入され、受け取り先のコンビニの店頭から持ち去られる事件が、7月から8月にかけて相次ぎました。何らかの方法で入手したIDとパスワードのリストを使ってログインを試行し、有効なアカウントに侵入する「リスト型攻撃」と見られます。約1800件のアカウントが侵入され、うち約1000件で「iPhone X」が勝手に購入されたといいます。これを受け、ドコモオンラインショップは、商品のコンビニ受取りを中止しました。



　同じリスト型攻撃で、ユーザーが貯めていたポイントが使われてしまう事件も相次ぎました。スマートフォンの公式アプリにある、ポイントカード機能が狙われたとみられます。リスト型攻撃であぶりだした侵入可能なアカウントでアプリにログインすれば、本物のカードを持っていない第三者が、アプリのポイントカード機能を使って店頭で支払いができるようになるのです。  
  
　NTTドコモの「dポイント」をはじめ「Pontaポイント」「Tポイント」などが次々に標的にされ、各社はパスワードだけではログインできないようにする「2段階認証」の必須化や、初回のアプリのカード機能利用時に、本物のカードに記載された番号などを入力させて本人様確認を行う仕組みを導入するなどの対策に追われました。  
 **＜関連記事＞**・「不正ログイン」で高額な不正購入や個人情報流出の被害発生――PW守る対策を  
[https://security-t.blog.so-net.ne.jp/2018-08-17](https://security-t.blog.so-net.ne.jp/2018-08-17?SmRcid=SECN-BLOG20180817_00016)  
・通販サイトで「高額商品略奪」発生、ユーザーにできる自衛策は？  
[https://security-t.blog.so-net.ne.jp/2018-08-24](https://security-t.blog.so-net.ne.jp/2018-08-24?SmRcid=SECN-BLOG20180824_00016)  
・コツコツ貯めたポイントが突然消失――店頭でカードアプリ不正使用相次ぐ  
[https://security-t.blog.so-net.ne.jp/2018-10-26](https://security-t.blog.so-net.ne.jp/2018-10-26?SmRcid=SECN-BLOG20181026_00016)  
・本人確認に使われるSMS認証に注意、「なりすまし」被害のおそれ  
[https://security-t.blog.so-net.ne.jp/2018-07-06](https://security-t.blog.so-net.ne.jp/2018-07-06?SmRcid=SECN-BLOG20180706_00016)  
・不正ログイン防ぐ「二段階認証」の弱点――破られる前に知っておこう  
[https://security-t.blog.so-net.ne.jp/2018-08-30](https://security-t.blog.so-net.ne.jp/2018-08-30?SmRcid=SECN-BLOG20180830_00016)  
・不正ログイン防ぐ「二段階認証」の弱点(2)――二段階目の認証が破られる3つのケース  
[https://security-t.blog.so-net.ne.jp/2018-08-31](https://security-t.blog.so-net.ne.jp/2018-08-31?SmRcid=SECN-BLOG20180831_00016)

**狙われたネットワーク機器――家庭のWi-Fiルーターが危ない**

　一般家庭を狙うサイバー攻撃は、パソコンやスマートフォンだけにとどまらず、インターネットの接続口に設置されたルーターにも魔の手を伸ばしています。



　3月中旬から、自宅のWi-FiルーターのDNS情報が書き換えられ、インターネットに接続できなかったり、不審なAndroid用アプリがダウンロードされたりするという声が聞かれるようになりました。DNS（Domain Name System）は、URLのホスト名をIPアドレスに変換する仕組みです。この情報が書き換えられたことで、ネットにアクセスしようとすると悪質なサイトに誘導され、マルウェアのダウンロードやフィッシング、仮想通貨のマイニングなどが不正に行われました。  
  
　5月には、ルーターに感染するマルウェア「VPNFilter」が報告されました。感染した機器は、外部から操られて感染活動や攻撃を仕掛ける「ボット」になってしまいます。同様のものに一昨年来からの「Mirai」というマルウェアもあり、このMirai系の亜種も相変わらず活動を続けています。  
  
　ルーター内部のソフトウェア（ファームウェア）に問題が見つかると、パソコンやスマートフォンと同じように修正プログラムが配布されます。一度設置してしまうと忘れられがちですが、インターネットの入り口で常に外部からの攻撃の矢面に立たされている存在です。欠陥があれば真っ先に狙われてしまうので、忘れずにアップデートを行うよう心掛けたいものです。  
 **＜関連記事＞**・自宅Wi-Fiで知らぬ間に「DNS情報」書き換えられ、不正アプリDLの恐れ  
[https://security-t.blog.so-net.ne.jp/2018-03-27](https://security-t.blog.so-net.ne.jp/2018-03-27?SmRcid=SECN-BLOG20180327_00016)  
・ルーターのDNS情報書き換え攻撃、標的がAndroidからiOSやPCにまで拡大  
[https://security-t.blog.so-net.ne.jp/2018-05-24](https://security-t.blog.so-net.ne.jp/2018-05-24?SmRcid=SECN-BLOG20180524_00016)  
・ネットワーク機器に感染するマルウェア「VPNFilter」に注意  
[https://security-t.blog.so-net.ne.jp/2018-06-01](https://security-t.blog.so-net.ne.jp/2018-06-01?SmRcid=SECN-BLOG20180601_00016)  
・バッファローの無線LAN親機に深刻な脆弱性、今すぐバージョン確認を  
[https://security-t.blog.so-net.ne.jp/2018-02-28](https://security-t.blog.so-net.ne.jp/2018-02-28?SmRcid=SECN-BLOG20180228_00016)  
・コレガの無線LAN親機に「深刻な脆弱性」判明、他社製品に買い替えを  
[https://security-t.blog.so-net.ne.jp/2018-03-09](https://security-t.blog.so-net.ne.jp/2018-03-09?SmRcid=SECN-BLOG20180309_00016)  
・バッファローとASUSの無線LANルーターに脆弱性、最新のファームウェアに更新を  
[https://security-t.blog.so-net.ne.jp/2018-05-17-1](https://security-t.blog.so-net.ne.jp/2018-05-17-1?SmRcid=SECN-BLOG20180517_00016)  
・NEC「Aterm」3製品に脆弱性――ファームウェアが最新版になっているか確認を  
[https://security-t.blog.so-net.ne.jp/2018-07-13](https://security-t.blog.so-net.ne.jp/2018-07-13?SmRcid=SECN-BLOG20180713_00016)