

情報セキュリティ 10 大脅威 2018

IPA 情報処理推進機構（2018年4月27日発表版より）

本日付けで、情報処理推進機構より、1月30日にプレスリリースされた内容の図入り説明が発表されました。現在の脅威のイメージも記載されており、非常に役立つとの考えから記載内容を抜き出してファイルにさせていただきました。

皆様でのセキュリティ脅威にかんする確認に役立てばと思っております。

記載に関しては、殆ど変更しておりませんが、原文の確認は下記のアドレスで可能です。

<https://www.ipa.go.jp/security/vuln/10threats2018.html>

また、80頁程のIPA情報処理機構様が作成頂いたより詳しい文書も下記のアドレスでダウンロードが可能です。

<https://www.ipa.go.jp/files/000065376.pdf>

次頁以降の内容を確認頂いた上で、気になる脅威から確認頂けると宜しいかと思えます。

皆様の業務上にて、セキュリティ事故が発生せず順調な業務遂行が出来る事を願っております。

SWM (Support to Worlds Member)

夢ある明日を貴方と共に

石川光信

<https://www.wswm.jp>

■「情報セキュリティ 10 大脅威 2018」

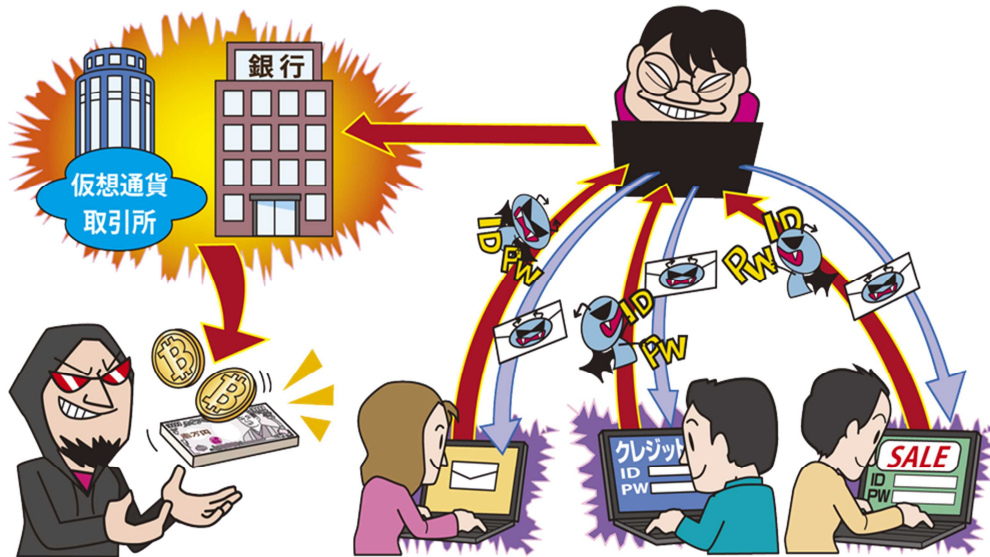
昨年順位	個人	順位	組織	昨年順位
1 位	インターネットバンキングやクレジットカード情報等の不正利用	1 位	標的型攻撃による被害	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺による被害	ランク外
3 位	スマートフォンやスマートフォンアプリを狙った攻撃	4 位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	脅威に対応するためのセキュリティ人材の不足	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告によるインターネット詐欺	10 位	犯罪のビジネス化 (アンダーグラウンドサービス)	9 位

「情報セキュリティ 10 大脅威 2018」の概要

10 大脅威選考会メンバーの投票により選出した「個人」と「組織」の 10 大脅威の順位と概要は下記になります。

<個人>

第 1 位 インターネットバンキングやクレジットカード情報の不正利用



ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が攻撃者に窃取され、不正送金や不正利用が行われている。2017 年は、インターネットバンキングの被害件数と被害額は減少傾向だが、新たに仮想通貨利用者を狙った攻撃が確認されている。

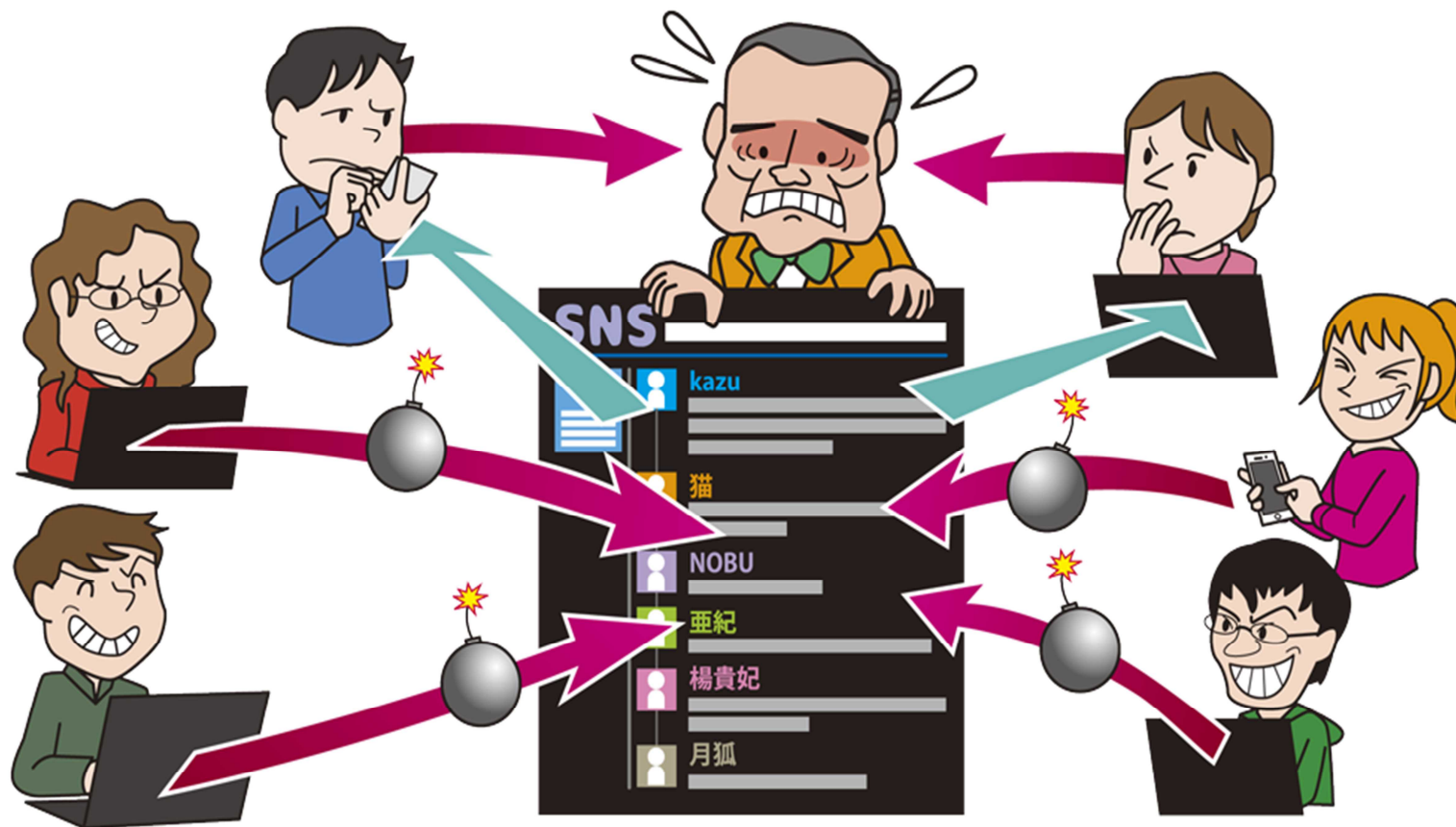
なお、1 月 30 日にプレスリリースした「[情報セキュリティ 10 大脅威 2018](https://www.ipa.go.jp/about/press/20180130.html) <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「インターネットバンキングやクレジットカード情報の不正利用」としていましたが、検討の結果、本タイトルに変更しました。

第2位 ランサムウェアによる被害



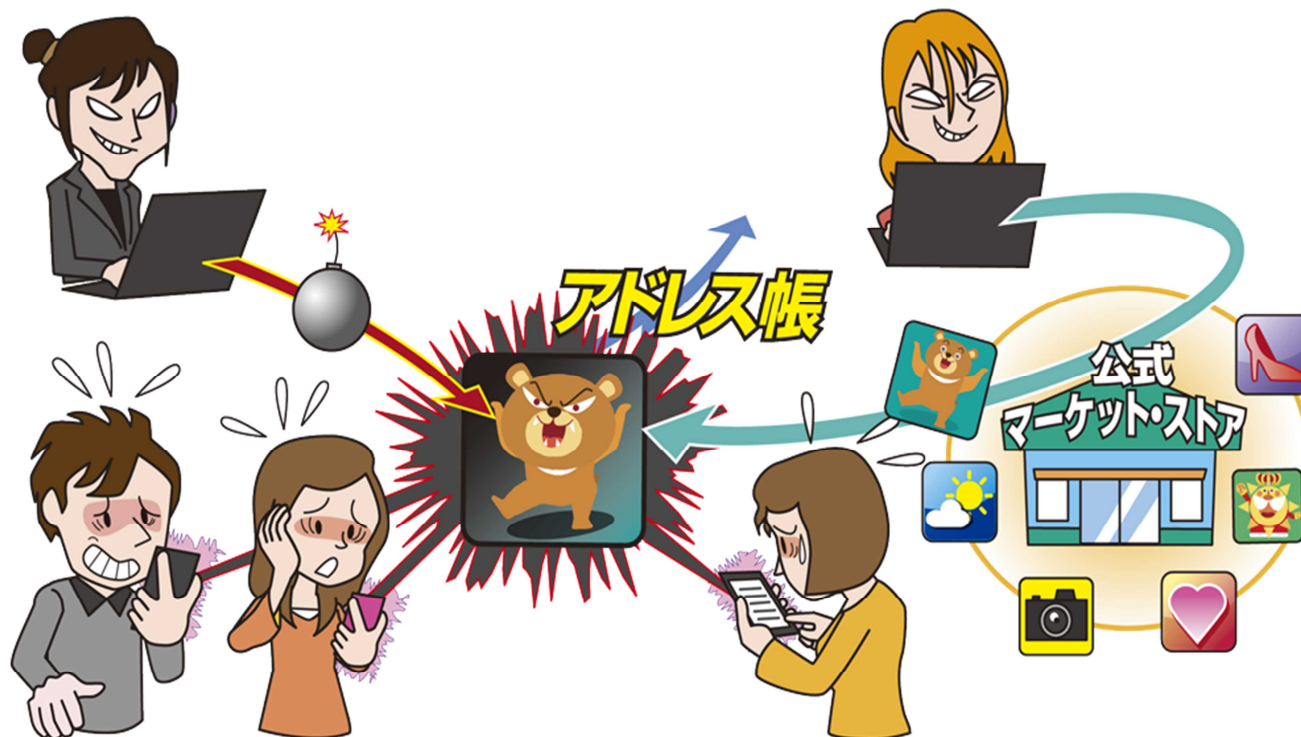
ランサムウェアとは、PC やスマートフォンにあるファイルの暗号化や画面ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルスである。そのランサムウェアに感染する被害が引き続き発生している。さらに、ランサムウェアに感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付け HDD に保存されているファイルも暗号化されるおそれがある。2017 年には、OS の脆弱性を悪用し、ネットワークを介して感染台数を増やすランサムウェアも登場した。

第3位 ネット上の誹謗・中傷



コミュニティサイト（ブログ、SNS、掲示板等）上で、個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。コミュニティサイトへの書き込みは、匿名性や手軽さから安易に投稿されてしまう傾向にある。また、SNSを使った犯罪は社会的な問題となっており、2017年は殺人事件にまで発展した事例もあった。

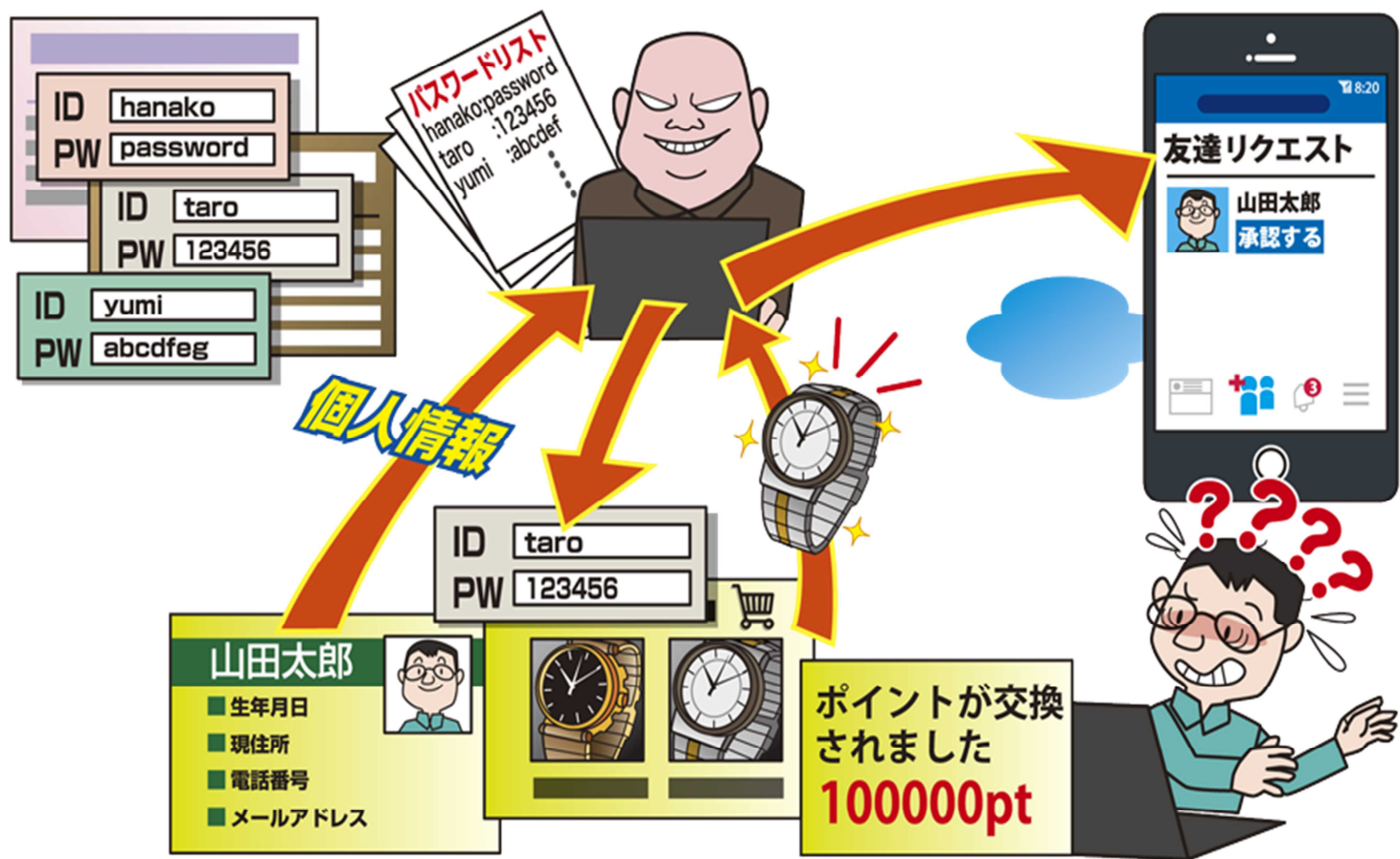
第4位 スマートフォンやスマートフォンアプリを狙った攻撃



公式マーケット等に公開されている不正アプリをスマートフォン利用者がインストールしてしまうことで、スマートフォン内の重要な情報を窃取されたり、不正に操作される被害が確認されている。また、データの暗号化等を行うランサムウェアの機能を持つアプリに加えて、2017年は個人情報を開示すると脅すランサムウェアの機能を持つアプリも確認されている。

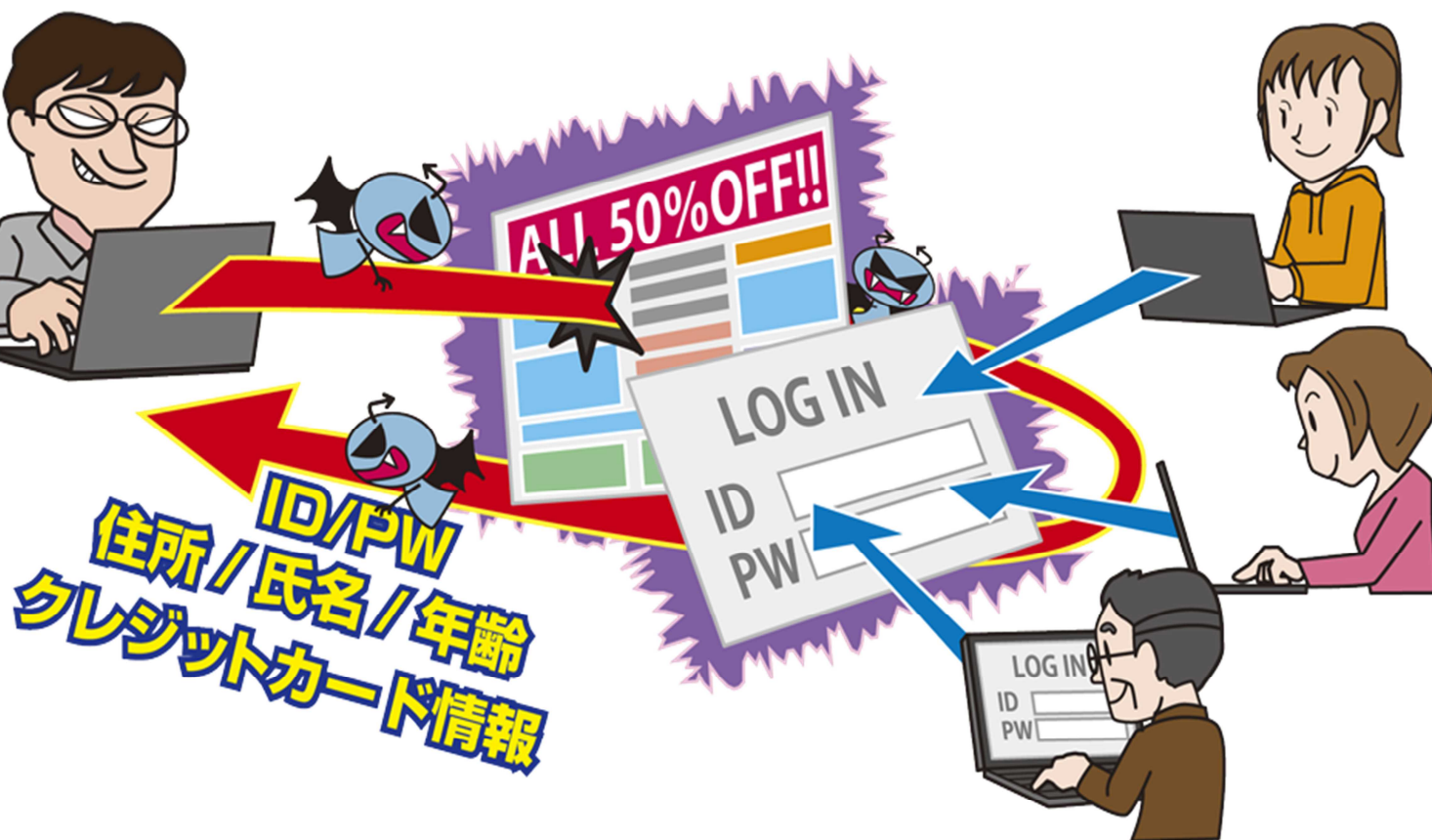
なお、1月30日にプレスリリースした「[情報セキュリティ 10 大脅威 2018](https://www.ipa.go.jp/about/press/20180130.html) <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「スマートフォンやスマートフォンアプリを狙った攻撃の可能性」としていましたが、検討の結果、本タイトルに変更しました。

第5位 ウェブサービスへの不正ログイン



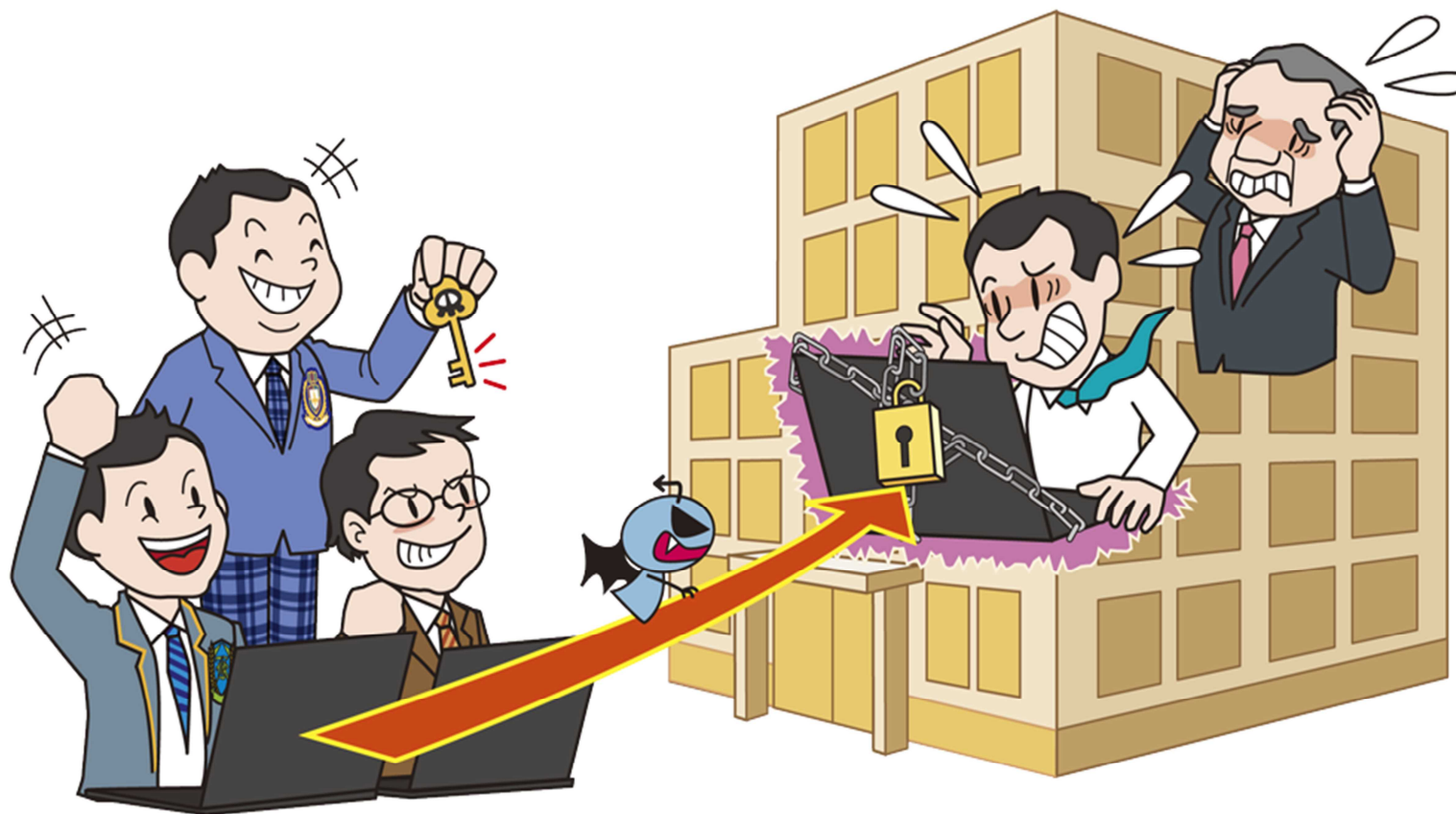
ウェブサービスに不正ログインされ、金銭的な被害や個人情報が窃取される等の被害が確認されている。2017年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃により行われている。インターネットには多数のウェブサービスが存在しており、ウェブサービスの利用者が推測されやすいパスワードの使用やパスワードの使いまわしをしている場合、不正ログインが行われてしまう。

第6位 ウェブサービスからの個人情報の窃取



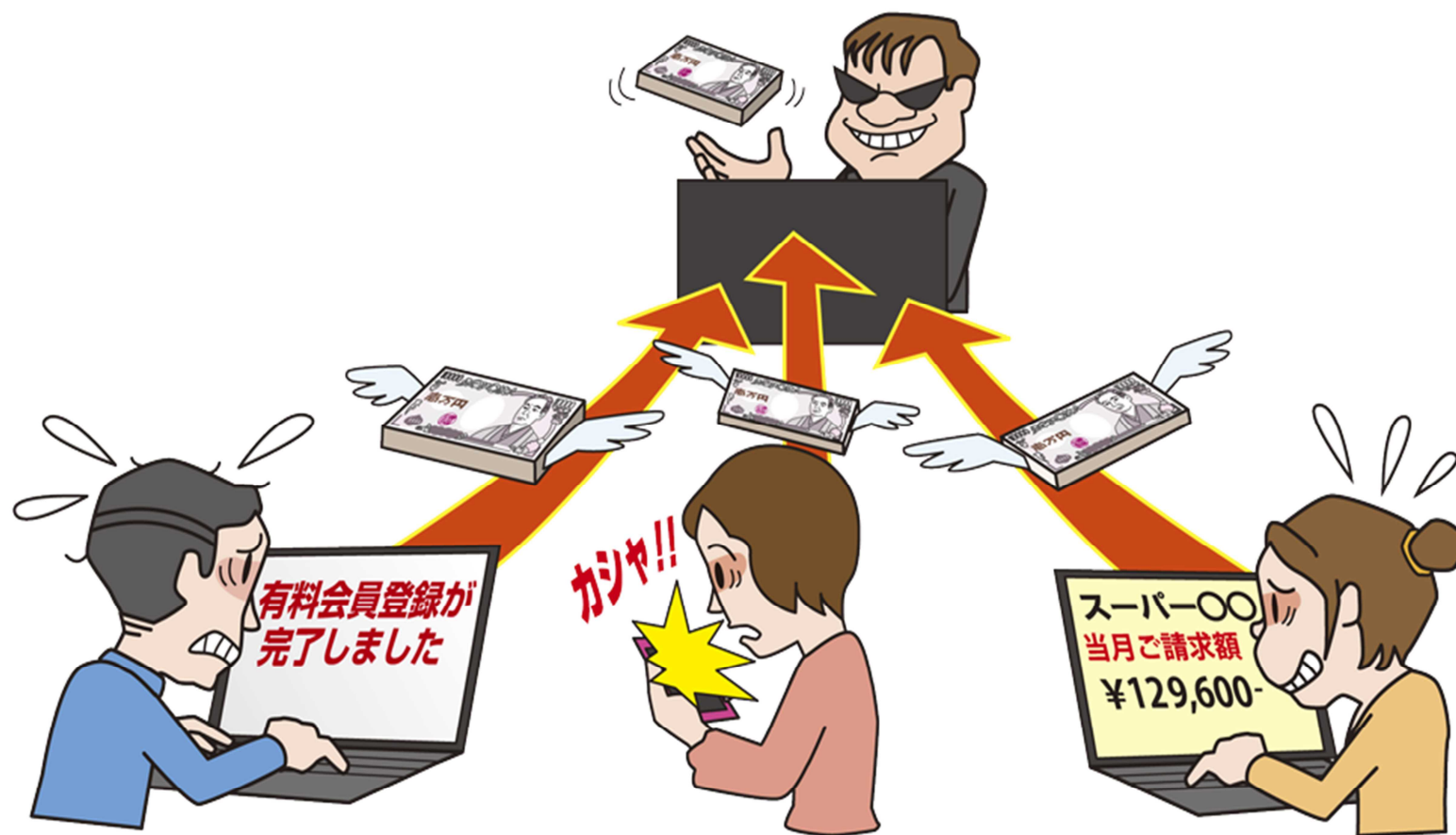
2017年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービスに登録した個人情報やクレジットカード情報を窃取される事件が多発している。窃取した情報を悪用されると不審メールを送信されたり、クレジットカード情報を不正利用されるおそれがある。

第7位 情報モラル欠如に伴う犯罪の低年齢化



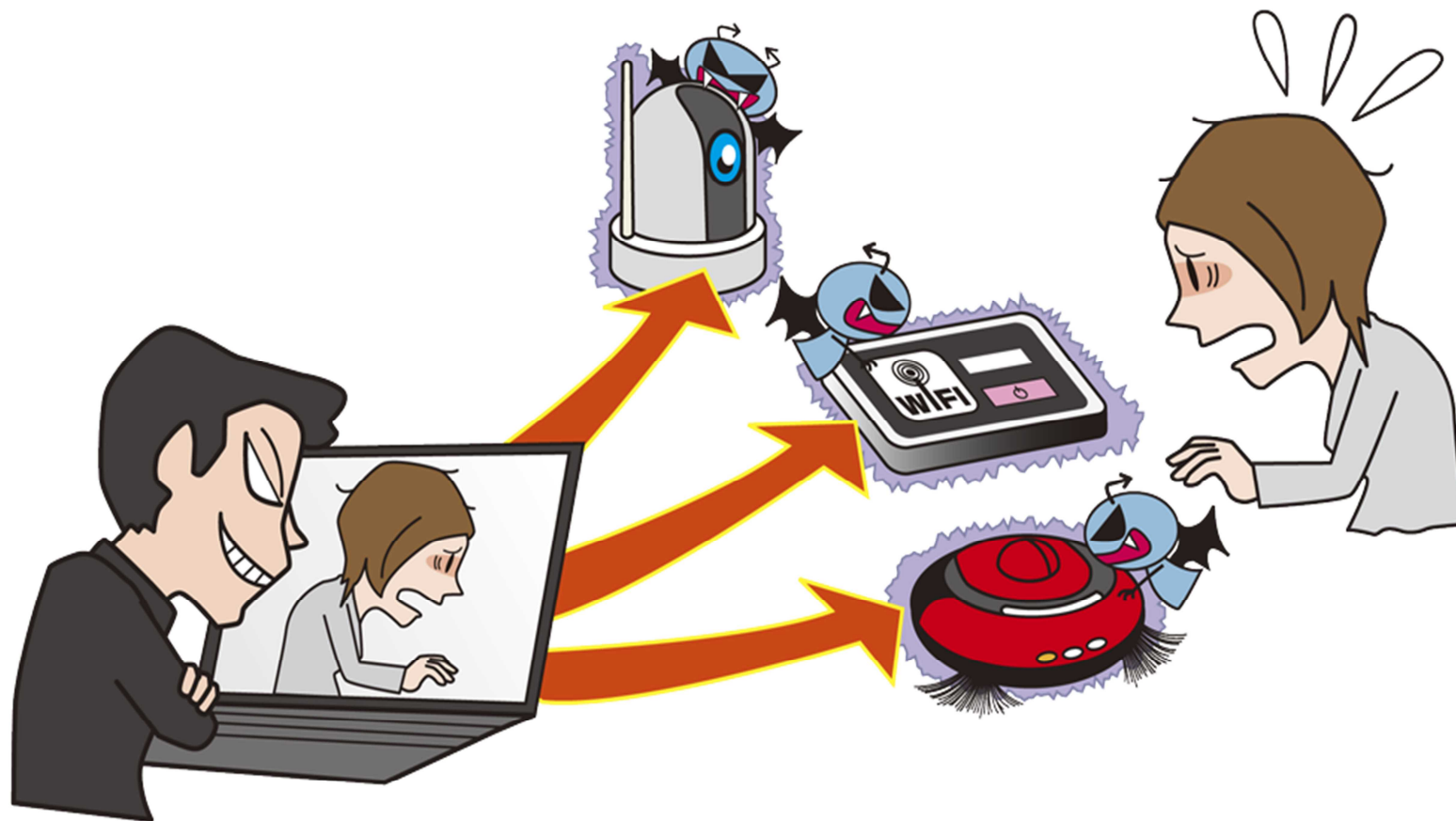
2017 年も未成年者がサイバー犯罪の加害者として逮捕、補導される事件が確認されている。サイバー犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手・利用できるようになったことで、情報モラルの欠如した未成年者が、サイバー犯罪に手を染めやすくなっている。また、未成年者の PC やスマートフォンの所持も当たり前となってきたが、教員や親の監視が行き届きにくい。

第8位 ワンクリック請求等の不当請求



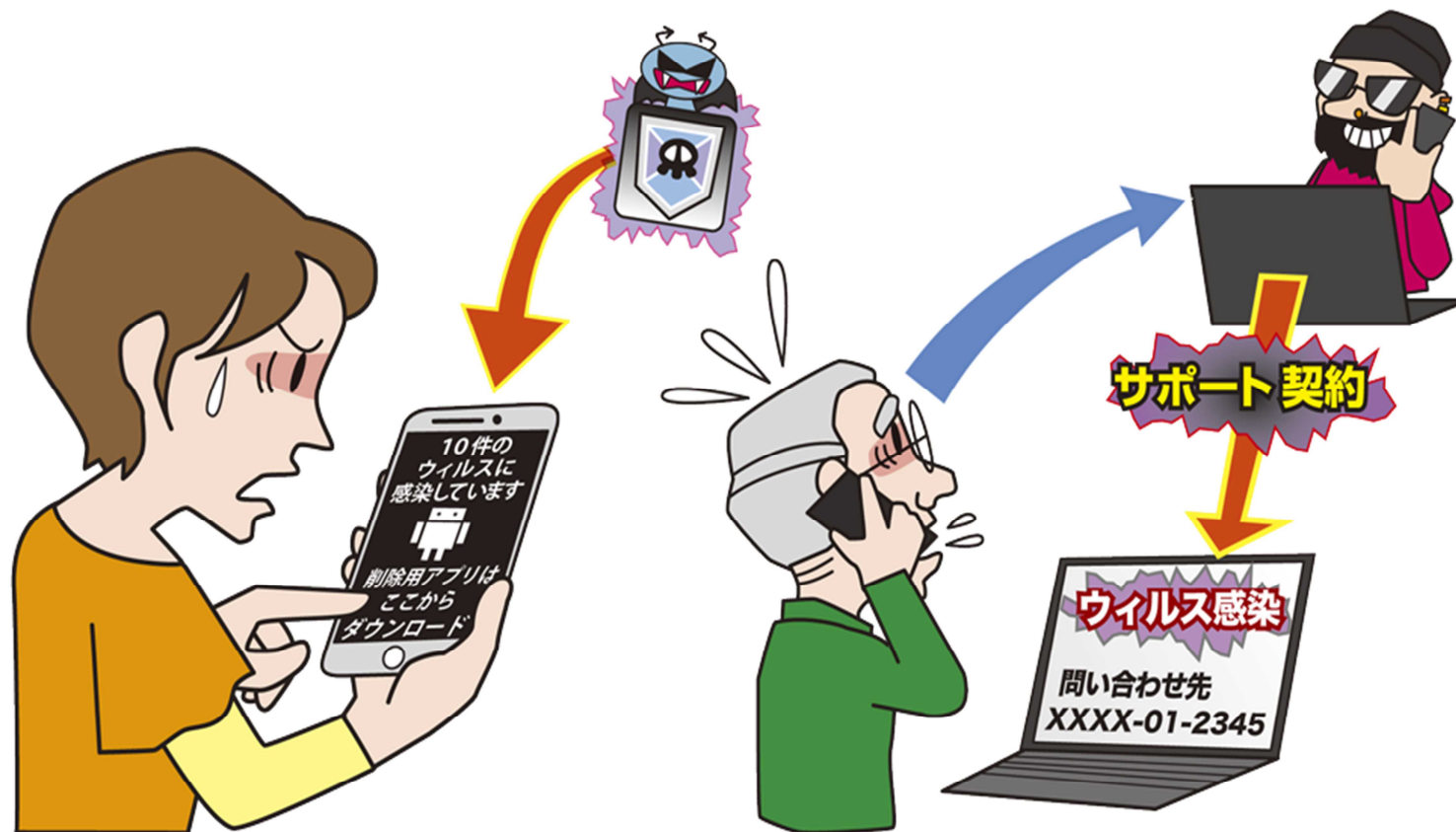
PC やスマートフォンを利用中にアダルトサイトの請求画面が表示され、金銭を不当に請求されるワンクリック請求の被害が依然として発生している。1 度のクリックによる請求だけでなく、複数回のクリックをさせることで、請求の正当性を主張されて不当請求されてしまう被害も確認されている。

第9位 IoT 機器の不適切な管理



昨今、インターネットに接続されている機器である IoT 機器の利用が進んでいる。一方、利用者は IoT 機器がインターネットに接続されていることを意識せずに利用しており、セキュリティ対策等の適切な管理が行われていないことがある。管理を怠っている IoT 機器が狙われ、室内の覗き見や攻撃の踏み台にされるといった被害が出ている。

第 10 位 偽警告によるインターネット詐欺

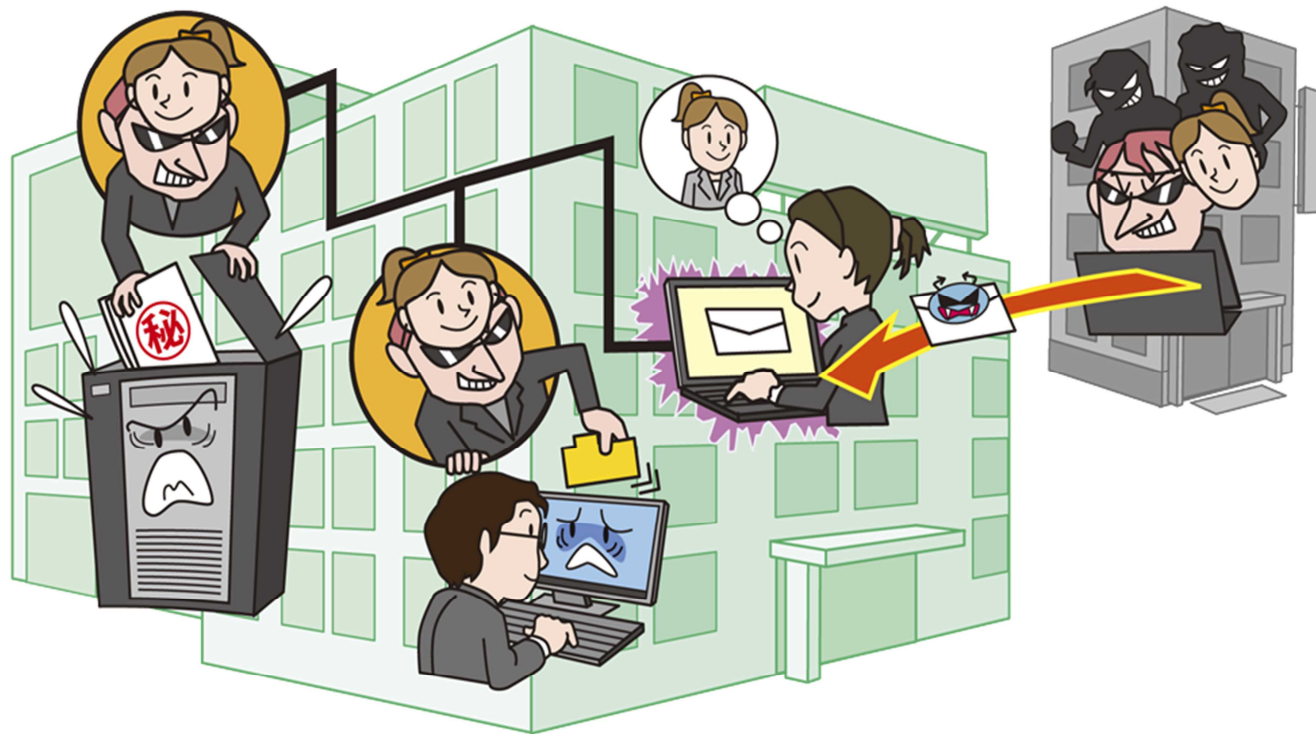


PC やスマートフォンでウェブサイトを開覧中に、突然「ウイルスに感染している」等の偽警告を表示し、利用者の不安を煽り、偽警告に記載された操作を行わせ、金銭的な被害や個人情報等を窃取される被害が発生している。偽警告は本物の警告と誤認されるように巧妙な細工が施されており、被害者は信じて指示に従ってしまう。

なお、1 月 30 日にプレスリリースした「[情報セキュリティ 10 大脅威 2018](https://www.ipa.go.jp/about/press/20180130.html) <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「偽警告」としていましたが、検討の結果、本タイトルに変更しました。

<組織>

第1位 標的型攻撃による被害



企業や民間団体や官公庁等、特定の組織を狙う、標的型攻撃が引き続き発生している。メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせて、PCをウイルスに感染させる。その後、組織内の別のPCやサーバーに感染を拡大され、最終的に業務上の重要情報や個人情報が窃取される。さらに、金銭目的な場合は、入手した情報を転売等されるおそれもある。

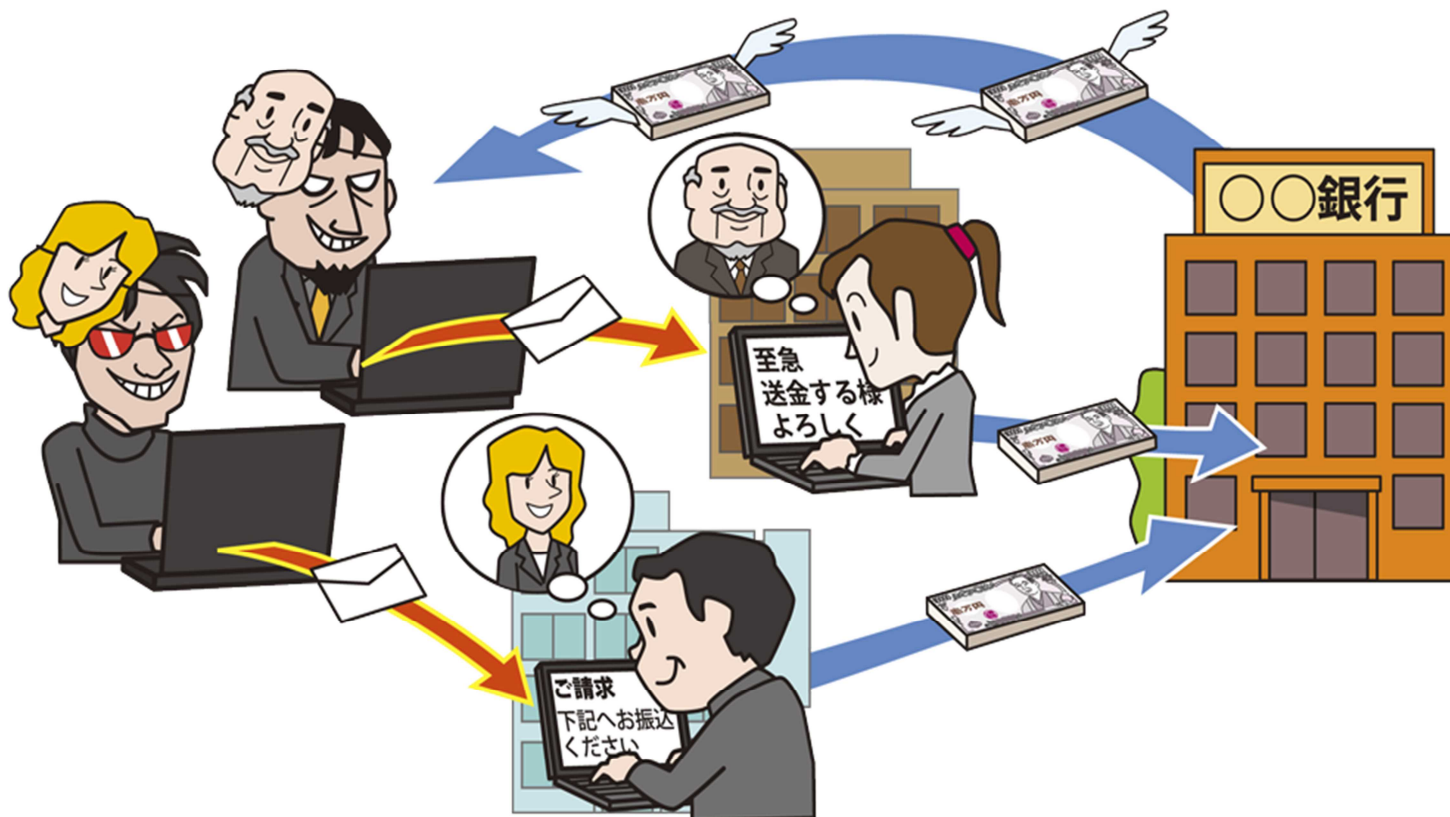
なお、1月30日にプレスリリースした「[情報セキュリティ 10大脅威 2018](https://www.ipa.go.jp/about/press/20180130.html) <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「標的型攻撃による情報流出」としていましたが、検討の結果、本タイトルに変更しました。

第2位 ランサムウェアによる被害



ランサムウェアとは、PC やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルスである。そのランサムウェアに感染する被害が引き続き発生している。さらに、ランサムウェアに感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付け HDD に保存されているファイルも暗号化されるおそれがある。組織内のファイルが広範囲で暗号化された場合、事業継続にも大きな支障が生じる。また、2017 年は、OS の脆弱性を悪用し、ランサムウェアに感染した端末が接続しているネットワークを介して感染台数を増やすランサムウェアも登場した。

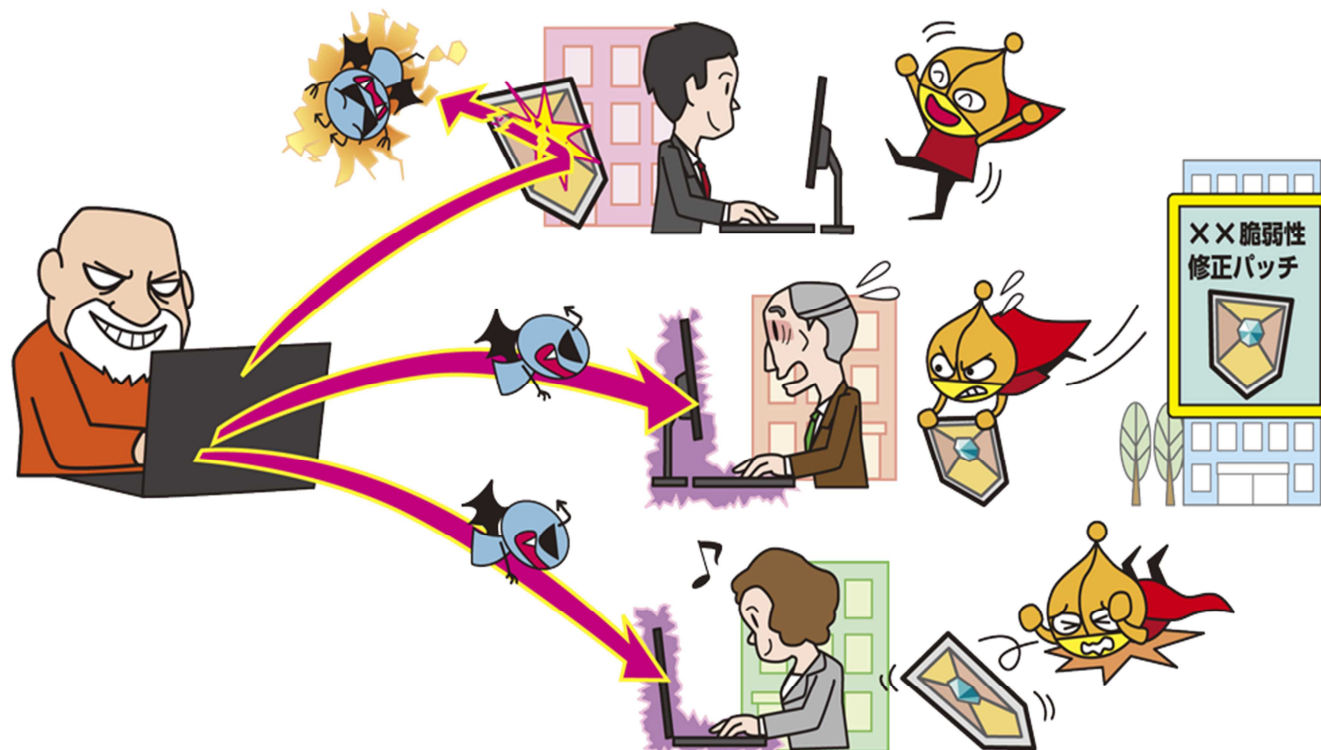
第3位 ビジネスメール詐欺による被害



「ビジネスメール詐欺」(Business E-mail Compromise : BEC)は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。以前は主に海外の組織が被害に遭ってきたが、2016年以降、国内企業でも被害が確認されている。

なお、1月30日にプレスリリースした「[情報セキュリティ 10大脅威 2018](https://www.ipa.go.jp/about/press/20180130.html) <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「ビジネスメール詐欺」としていましたが、検討の結果、本タイトルに変更しました。

第4位 脆弱性対策情報の公開に伴う悪用増加



ソフトウェア製品の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。一方、その情報を攻撃者に悪用され、当該ソフトウェア製品を利用した対策前のシステムを狙う攻撃が行われている。また、近年では脆弱性情報の公開後、その脆弱性を悪用した攻撃が本格化するまでの時間が一層短くなっている傾向がある。なお、脆弱性対策情報の公開前に攻撃が行われる場合もある。

なお、1月30日にプレスリリースした「**情報セキュリティ 10 大脅威 2018** <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加」としていましたが、検討の結果、本タイトルに変更しました。

第5位 脅威に対応するためのセキュリティ人材の不足



情報セキュリティにおける脅威は増大の一途を辿っており、毎年のように新たな脅威が出てきている。これらの脅威に対応するためには情報セキュリティの知識や技術を有するセキュリティ人材が求められる。しかし、需要に対するセキュリティ人材の人数が不足しており、また、セキュリティ人材がいたとしても組織は確保するための十分な予算がなく、確保できていないケースもある。セキュリティ人材の不足により、様々な脅威への対応や対策が十分に行えず、被害を拡大してしまうおそれがある。

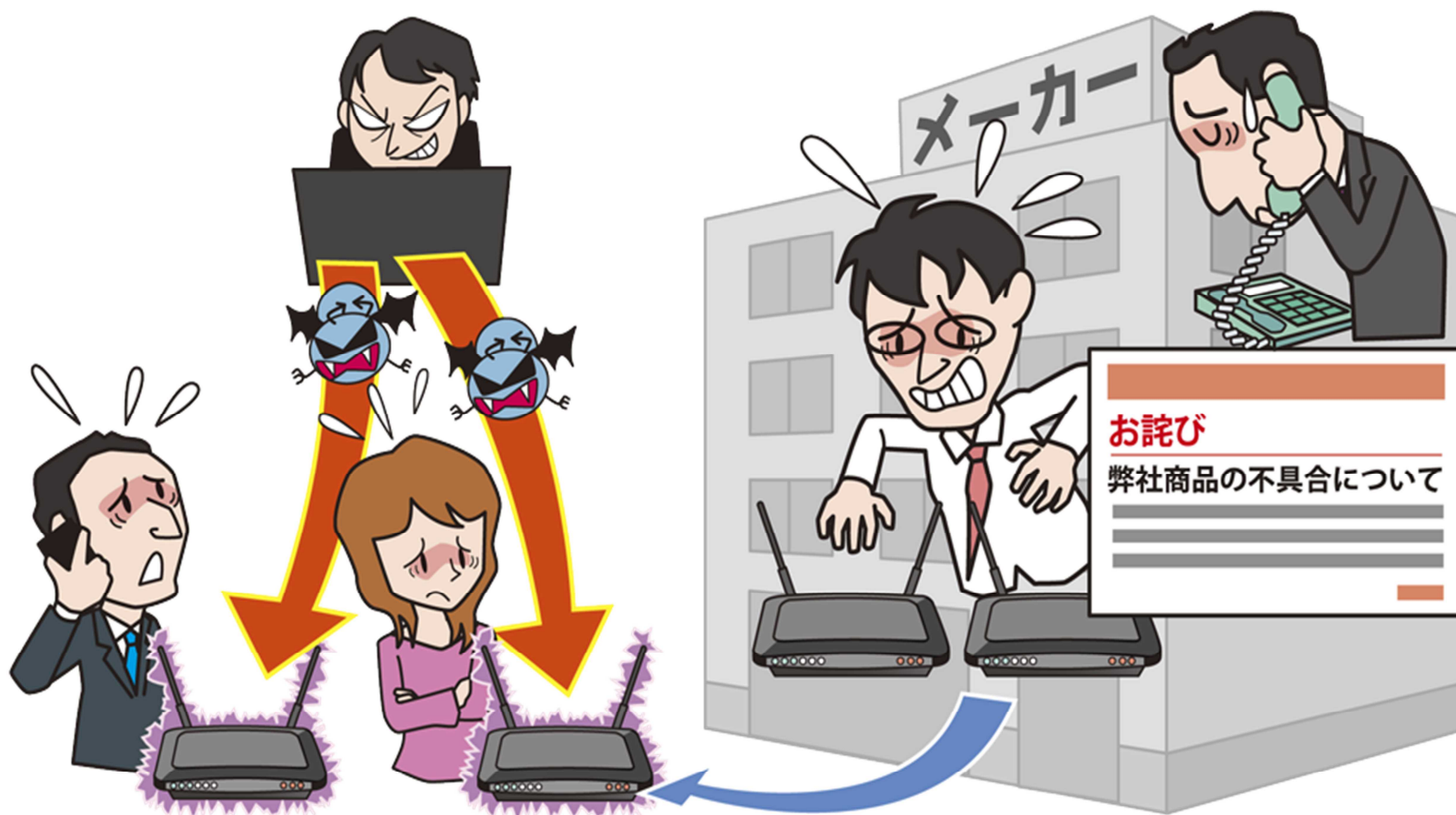
なお、1月30日にプレスリリースした「**情報セキュリティ 10大脅威 2018** <https://www.ipa.go.jp/about/press/20180130.html>」を決定では、タイトルを「セキュリティ人材の不足」としていましたが、検討の結果、本タイトルに変更しました。

第6位 ウェブサービスからの個人情報の窃取



2017年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。それらの情報を窃取されると、攻撃者により顧客や利用者の個人情報を悪用した不審なメールを送信されたり、クレジットカードを不正利用されるおそれがある。

第7位 IoT 機器の脆弱性の顕在化



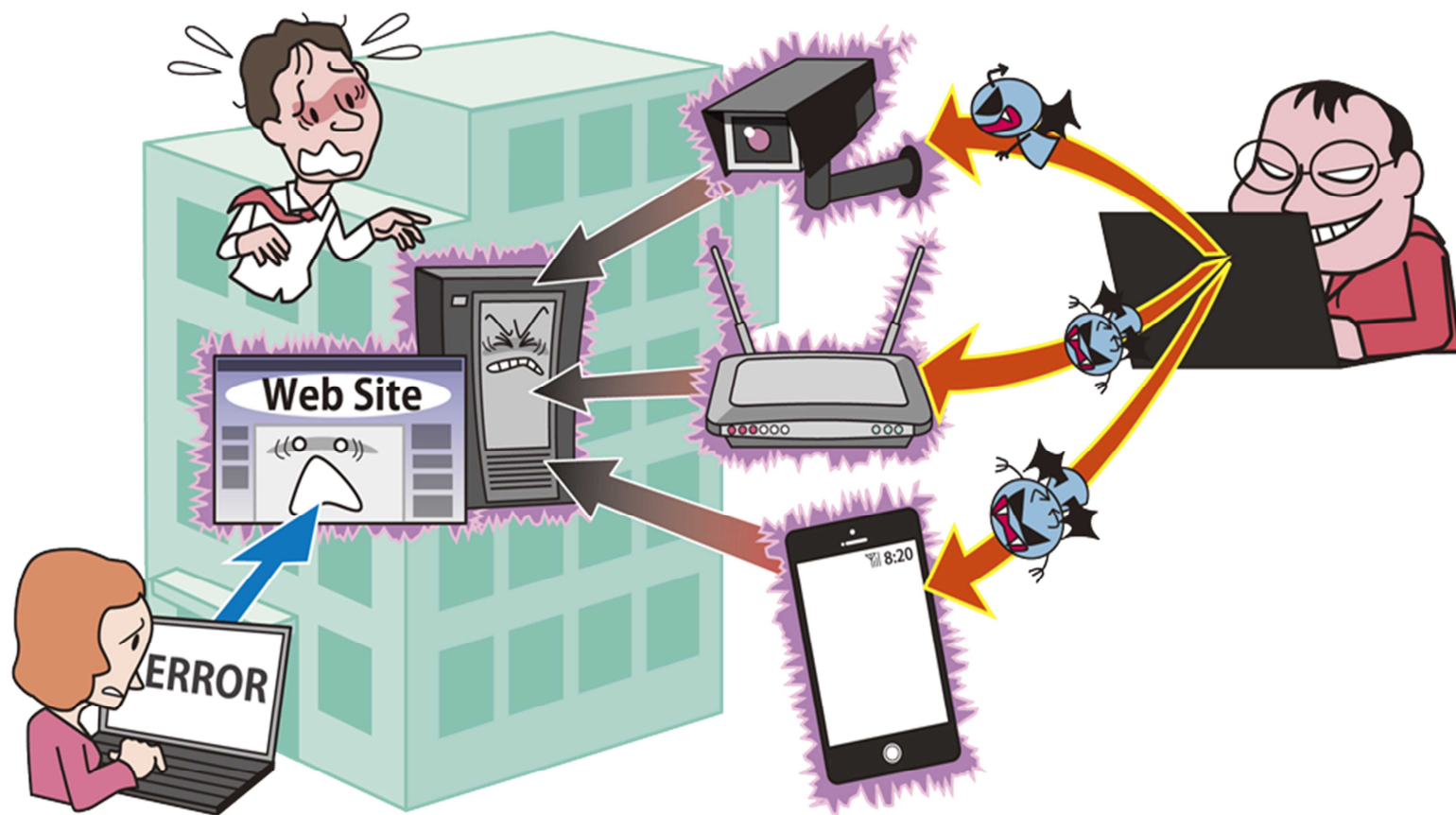
2016年に引き続き、IoT機器の脆弱性を悪用しウイルスに感染させることで、インターネット上のサービスやサーバーに対して、大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。また、国内で発売されているIoT機器において脆弱性が発見されており、機器を乗っ取られる、または撮影機能等を悪用して個人情報等を窃取されるといった危険性があることが公表されている。

第8位 内部不正による情報漏えい



組織内部の従業員や元従業員により、私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。また、組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、さらにその情報を紛失し、情報漏えいにつながることもある。内部不正が発覚した場合、組織は、被害把握や原因追求等の対応に追われ、また社会的信用の失墜等にもつながる。

第9位 サービス妨害攻撃によるサービスの停止



ウイルスに感染し、ボット化した機器から DDoS（分散型サービス妨害）攻撃が行われている。それにより、ウェブサイトや DNS サーバーが高負荷状態となり、利用者がアクセスできなくなる被害が確認されている。2017 年は公式のマーケットに公開されたスマートフォンアプリがボット化し、DDoS 攻撃が行われた被害が確認されている。

第10位 犯罪のビジネス化（アンダーグラウンドサービス）



犯罪に使用するためのサービスやツール、ID やパスワードの情報がアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。

プレス発表

プレスリリース全文 (PDF ファイル 236KB) <https://www.ipa.go.jp/files/000063831.pdf>

以上