

情報セキュリティ 10 大脅威 2020

各脅威の解説資料

本資料は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威 2020」

<https://www.ipa.go.jp/security/vuln/10threats2020.html>

目次

1. 情報セキュリティ 10 大脅威 2020	4
1.1. 情報セキュリティ 10 大脅威（個人）	7
1 位 スマホ決済の不正利用	8
2 位 フィッシングによる個人情報の詐取	10
3 位 クレジットカード情報の不正利用	12
4 位 インターネットバンキングの不正利用	14
5 位 メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	16
6 位 不正アプリによるスマートフォン利用者への被害	18
7 位 ネット上の誹謗・中傷・デマ	20
8 位 インターネット上のサービスへの不正ログイン	22
9 位 偽警告によるインターネット詐欺	24
10 位 インターネット上のサービスからの個人情報の窃取	26
1.2. 情報セキュリティ 10 大脅威（組織）	29
1 位 標的型攻撃による機密情報の窃取	30
2 位 内部不正による情報漏えい	32
3 位 ビジネスメール詐欺による金銭被害	34
4 位 サプライチェーンの弱点を悪用した攻撃	36
5 位 ランサムウェアによる被害	38
6 位 予期せぬ IT 基盤の障害に伴う業務停止	40
7 位 不注意による情報漏えい	42
8 位 インターネット上のサービスからの個人情報の窃取	44
9 位 IoT 機器の不正利用	46
10 位 サービス妨害攻撃によるサービスの停止	48

1. 情報セキュリティ 10 大脅威 2020

■「情報セキュリティ 10 大脅威 2020」

2019 年において社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づき、「情報セキュリティ 10 大脅威 2020」では、「個人」および「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2020 「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬ IT 基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT 機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

本資料で共通的に使われる用語について表 1.2 に定義を記載する。

表 1.2 情報セキュリティ 10 大脅威 2020 用語定義

用語	意味
個人	家庭等でスマートフォンや PC を利用する人
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
犯罪者	金銭や情報窃取(スーカークー行為を含む)を目的とした攻撃(犯罪)者
犯罪グループ	金銭や情報窃取を目的とした攻撃(犯罪)者集団
諜報員、産業スパイ	機密情報窃取を目的とした攻撃(犯罪)集団 国家組織の支援を受けた攻撃(犯罪)集団
ハクティビスト	社会的・政治的な主義主張を目的としたハッキング活動(ハクティビズム)を目的とした攻撃(犯罪)者集団
IoT	モノのインターネット(Internet of Things)。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み。機器自体を指す場合は、IoT 機器と呼ぶ。
CSIRT	セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。自組織に関する問題に対応する場合は、自組織 CSIRT と呼ぶ。
マイニング	PC 等を使って仮想通貨の取引に関連する情報を計算し、取引を承認する行為。計算の報酬として仮想通貨を得られる。
セクストーション	被害者のプライベートな写真や動画を入手したとして、それをばらまく等と脅迫する行為

■「情報セキュリティ 10 大脅威 2020」をお読みになる上での留意事項

① 順位に捉われず、立場や環境を考慮する

「情報セキュリティ10大脅威 2020」は、「10大脅威選考会」の投票結果に基づき順位付けして「個人」「組織」それぞれ 10 個の脅威を選定している。投票により重要度が高いと考えられるものをより上位の順位としているが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。例えば、フィーチャーフォン(ガラケー)を利用している方であれば、個人 1 位「スマホ決済の不正利用」や個人 6 位「不正アプリによるスマートフォン利用者への被害」等の対策の必要性は低くなるし、オンラインショッピング等の個人情報をメインで取り扱っている組織であれば、組織 8 位の「インターネット上のサービスからの個人情報」の窃取」を優先的に対策しなければならないだろう。そのため、**順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。**

② ランクインした脅威が全てではない

「情報セキュリティ 10 大脅威 2020」で新しくランクインした脅威もあるが、それに伴いランク外となった脅威もある。しかし、ランク外になったとしてもその脅威が無くなったわけではない。かつてランクインしていた、「ワンクリック請求等の不当請求」や「ウェブサイトの改ざん」等は、依然として攻撃が行われている状況である。そのため、**ランク外の脅威だから対策を行わなくて良いということではなく、継続しての対策が必要となる。**ランク外となった脅威の詳細や対策方法等については、過去の「情報セキュリティ 10 大脅威」を参考にしてほしい。

③ 「情報セキュリティ対策の基本」が重要

世の中には「情報セキュリティ 10 大脅威」へランクインした脅威以外にも多数の脅威が存在する。とはいえ、これらが利用する「攻撃の糸口」は似通っており、脆弱性を悪用する、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くからある基本的な手口が使われている。

詳しくは「情報セキュリティ 10 大脅威 2015」の1章で解説しているが、表 1.3 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭う可能性を低減できると考える。

表 1.3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視すべき対策を理解する

1.1. 情報セキュリティ 10 大脅威(個人)

1位 スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～



近年のスマートフォンの普及に伴い、スマートフォンを利用した決済(スマホ決済)がキャッシュレス決済の手段として利用できるようになった。その後も類似のスマホ決済サービスは次々と登場し、それらの利用者が増加している。一方、利便性の反面、アカウントに不正アクセスされたことにより、第三者のなりすましによるサービスの不正利用も確認されている。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(スマホ決済サービス利用者)
- 組織(サービス事業者・サービス利用店舗・クレジットカード会社)

<脅威と影響>

スマートフォンを利用した決済であるスマホ決済を行うサービス PayPay 等のポイント還元キャンペーンや、2019年10月の消費税率引き上げに伴う「キャッシュレス・消費者還元事業」(キャッシュレス・ポイント還元事業)が広くメディアで報道され、スマホ決済が国民に広く認知された。

スマホ決済では、スマートフォンをカードリーダーにかざしたり、決済用アプリで生成した QR コードやバーコードを店舗のバーコードリーダーに読み込ませたり、逆に店舗に置いてある QR コードを決済用アプリで読み込んで決済金額を手動で入力したりして決済する。残高をチャージするためには事

前にクレジットカード情報や銀行口座などを登録してそこからチャージすることができる。これらの情報は決済サービス毎に専用のシステムやアプリで管理されている。攻撃者に決済サービスの不備を突かれ、決済サービスに不正にログインされると、クレジットカード情報等が窃取されたり、意図しない金銭取引をされたり等の被害に遭う。

<攻撃手口>

◆ 不正アクセスによるアカウントの乗っ取り

被害者が複数のサービスで同一のパスワードを使いまわしている場合がある。攻撃者は、過去に漏えいしたパスワードをリスト化し、それをもとにログインを試みる(パスワードリスト攻撃)。不正ログインに成功すれば、なりすまして不正利用する。また、スマホ決済サービスより提供される二要素認証等のセキュリティ機能を利用していない場合、漏えいしたパスワードのみで不正ログインできるため、攻撃者に悪用されやすい。

◆ 企業で開発したスマホ決済サービスの不備の悪用

スマホ決済サービスを開発する際にセキュリティを十分に考慮していない場合、決済システムやアプリに脆弱性を作りこんでしまうおそれがある。攻撃者はその脆弱性等の不備を悪用し、利用者が意図しない決済等を行う。また、二要素認証やサービスの利用状況の通知機能等、セキュリティを強化する機能をサポートしていないスマホ決済サービスは、攻撃者に悪用されやすい。

<事例または傾向>

◆ スマホ決済サービスに不正アクセス

2019年7月、セブン・ペイが運営するバーコード決済サービス「7pay」は不正アクセスにより、登録したクレジットカードからの不正チャージやチャージした7pay残高を不正利用される等、709人、約3,800万円(2020年1月6日時点)の被害を受けた。¹不正アクセスの原因は、どこかで不正に入手したIDやパスワードを使った可能性が高いと結論づけている。セブン&アイ・ホールディングスでは、被害者への補償の他、不正アクセスに対する備えが万全ではなかったとして、サービスの廃止、役員報酬の自主返上および子会社における代表者の異動等の処分を行った。²

◆ 不正利用防止のためのガイドライン遵守要請

スマホ決済サービスで不正利用が発生した事案では、キャッシュレス推進協議会が策定した不正利用防止のための各種ガイドラインが遵守されていなかった。これを踏まえて、2019年7月、経済産業省は決済事業者等に対して、不正利用防止のための各種ガイドラインの遵守とセキュリティレベル向上に努めるよう要請した。³

<対策/対応>

個人(スマホ決済サービスの利用者)

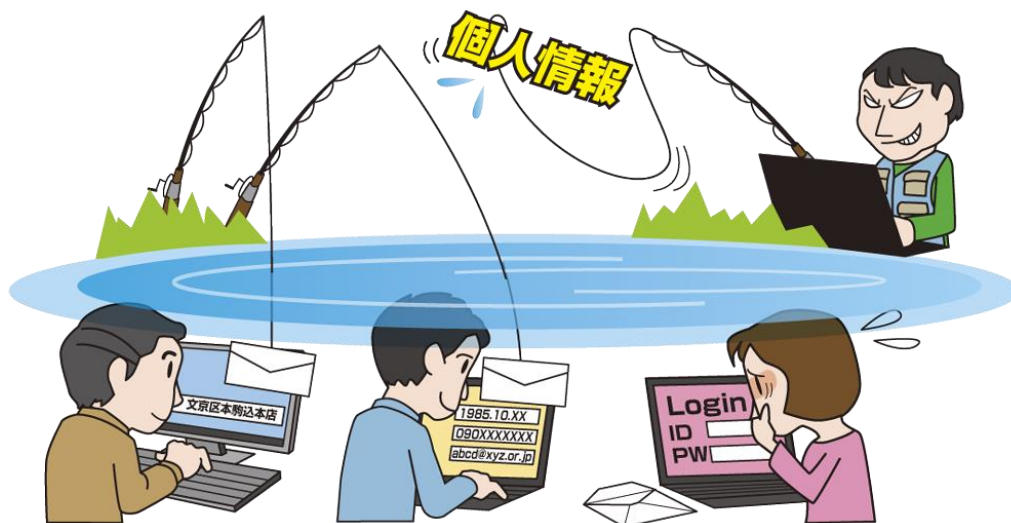
- 被害の予防
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・パスワードは長く、複雑にする
 - ・パスワードの使いまわしをしない
 - 例えばパスワードの基となるコアパスワードを作成し、その前後にサービス毎に異なる識別子を付加することでユニークなパスワードを作成することができる。⁴
 - ・パスワード管理ソフトの利用
 - ・サービスが推奨する認証方式の利用
 - 二要素認証や3Dセキュア等を利用することで、仮にパスワードが攻撃者に漏れいたとしても、不正ログインや、その後の金銭被害等につながる重要な操作を阻止できる確率を高める。⁵
 - ・不審なウェブサイトで安易に認証情報を入力しない(フィッシングに注意)
 - ・利用頻度が低いサービスや不要なサービスのアカウント削除
 - ・過剰なチャージはしない(被害額を抑える)
 - ・スマートフォンの盗難・紛失対策
 - スマートフォンを悪用されないために画面ロック等のセキュリティ対策を実施する。
- 被害の早期検知
 - ・不正なログイン履歴の確認
 - ・スマホ決済サービスの利用履歴の確認
 - ・サービス利用状況の通知機能等の利用
- 被害を受けた後の対応
 - ・パスワードの変更
 - ・クレジットカードの停止
 - ・スマホ決済サービス運営者への連絡

参考資料

1. 認定廃止のセブンペイ、払い戻し受付期限 25万人が未申請
<https://www.asahi.com/articles/ASN1B5FQKN1BULFA02C.html>
2. 「7pay(セブンペイ)」事案に関する再発防止策並びに役員報酬の自主返上および子会社における代表取締役の異動に関するお知らせ
https://www.7andi.com/library/dbps_data/material/_localhost/ja/release_pdf/2019_1010_ir01.pdf
3. コード決済サービスにおける不正アクセス事案を踏まえ、決済事業者等に対し、不正利用防止のための各種ガイドラインの徹底を求めました
<https://www.meti.go.jp/press/2019/07/20190705003/20190705008.html>
4. 不正ログイン被害の原因となるパスワードの使い回しはNG
<https://www.ipa.go.jp/security/anshin/mgdavori20160803.html>
5. 不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html

2位 フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～



フィッシング詐欺は、金融機関、ショッピングサイト等の実在する有名企業を騙るメールを送信し、偽のウェブサイト(フィッシングサイト)へ誘導することにより、銀行口座情報、クレジットカード情報、ID、パスワード、氏名等の重要な情報を詐取する詐欺である。詐取された情報を悪用されると金銭的な被害が発生することもある。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(インターネット利用者)
- 組織(インターネット利用者)

<脅威と影響>

金融機関、ショッピングサイト、宅配業者等の実在する有名企業を騙るメールが、PC やスマートフォンの利用者に届く。届いたメールの本文には、攻撃者が用意したフィッシングサイトへの URL が記載されており、巧みな言葉で URL をクリックするように誘導する。URL へアクセスすると、正規のウェブサイトを装ったフィッシングサイトになっており、クレジットカード情報、ID、パスワード、氏名等の重要な情報の入力を促す。

フィッシングサイトで重要な情報を入力すると、その情報を攻撃者に詐取される。詐取された情報は悪用され、金銭的な被害が発生する。

また、近年は、メールだけではなく、LINE や Twitter等の SNS(ソーシャル・ネットワーキング・サ

ービス)や電話番号宛にメッセージを送付する SMS(ショートメッセージサービス)を悪用したフィッシング詐欺が確認されている。

<攻撃手口>

◆ 有名企業を騙るメールを不特定多数に送信

攻撃者が、実在する有名企業のウェブサイト に似せたフィッシングサイトを作成する。そこに誘導するために、メール、SNS、SMS等を介して不特定多数の宛先に本物と信じさせる巧みな内容で送信する。騙されてフィッシングサイトに誘導された被害者に対して個人情報等の重要な情報を入力させ、不正利用目的で情報を詐取する。

◆ ワンタイムパスワード等も入力させて詐取

メール、SNS、SMS等を介してフィッシングサイトに誘導し、認証情報等を入力させる。さらに二要素認証を利用している場合は二要素認証の情報(ワンタイムパスワード等)も入力させて詐取する。そして、この詐取した情報を用いてサービスにログインして不正利用する。

＜詐取した情報の悪用例＞

- 詐取した個人情報等の重要な情報を攻撃者が情報の売買を行うダークウェブ等で販売して金銭を得る。
- 詐取した ID、パスワードを悪用してインターネットバンキング等の複数のインターネット上のサービスに不正ログインを試みる。

＜事例または傾向＞

◆ フィッシングの報告件数が増加傾向

フィッシング対策協議会によると、2019 年 12 月に寄せられたフィッシング報告件数は 8,208 件となり、1 月の 1,713 件の約 5 倍となり、増加傾向が続いている。また、金融機関を騙るフィッシングでは、11 月まで大手銀行を騙るものが主だったが、12 月は地方銀行やネット銀行等、多くの金融機関ブランドを騙るフィッシングが報告されている。¹

◆ 世界的なイベントに便乗したフィッシング詐欺

ラグビーワールドカップ人気に便乗したフィッシングサイトが確認された。無料のライブ動画配信サービスを装い、動画視聴のための会員登録と称し、メールアドレス、クレジットカード情報の入力を求める。プレミアム会員へのアップグレードまたは購入を行わない限り請求は発生しないと記載しているが、情報を入力した場合、クレジットカードの不正利用被害や、入力した情報を他のサイバー犯罪に悪用されるおそれがあった。²

◆ 琉球銀行と装い詐欺 479 万円被害

2019 年 12 月、琉球銀行を装った SMS を携帯電話に送りつけてフィッシングサイトに誘導し、インターネットバンキングの ID やパスワードを詐取する事案が発生した。個人客のユーザ ID とパスワードを使った不正送金が 5 件、総額 479 万 8,000 円の被害が確認され、琉球銀行は注意を呼び掛け、他

にも不正送金がないか調べている。³

＜対策/対応＞⁴

個人(インターネット利用者)

- 被害の予防(被害に備えた対策含む)
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・メール内の URL を安易にクリックしない
金銭や重要情報に関わるウェブサイトは、ブックマークに登録してそこからアクセスする。
 - ・受信メールやウェブサイトの十分な確認
重要なお知らせ等の緊急性を煽る内容で誘導されたウェブサイトにおいて、個人情報等の重要な情報はすぐに入力せず、サイトのドメイン名等を確認してサイトの真偽を確かめる。
- 被害の早期検知
 - ・利用するウェブサイトのログイン履歴の確認
自分のものではない IP アドレスや端末からログインした履歴がないかを確認する。
 - ・クレジットカードやインターネットバンキング等の利用明細を確認
- 被害を受けた後の対応
 - ・パスワードの変更
 - ・金融機関等への利用停止を連絡
 - ・信頼できる機関に相談
警察、国民生活センター、地域の消費生活センター等に相談する。

組織(インターネット利用者)

- 被害の予防(被害に備えた対策含む)
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・セキュリティ教育の実施
- 被害を受けた後の対応
 - ・CSIRT やシステム管理者へ連絡

参考資料

1. 2019/12 フィッシング報告状況

<https://www.antiphishing.jp/report/monthly/201912.html>

2. 【注意喚起】ラグビーワールドカップ人気に便乗したフィッシング詐欺に注意

https://is702.jp/news/3568/partner/97_t/

3. 琉球銀行と装い詐欺479万円被害 携帯にSMS届き偽サイト誘導 沖縄銀行と偽るメールも

<https://www.okinawatimes.co.jp/articles/-/512600>

4. 資料公開: 利用者向けフィッシング詐欺対策ガイドラインの改訂について

https://www.antiphishing.jp/report/guideline/consumer_guideline2019.html

3位 クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～



キャッシュレス決済の普及に伴い、クレジットカードの利用機会が増えている。さらに、スマートフォンを使った決済サービスも登場し、様々なデバイスからクレジットカードが利用されている。一方、そのクレジットカードを狙ったフィッシング詐欺、ショッピングサイトの改ざんによる偽決済画面への誘導等により、クレジットカード情報が詐取され、攻撃者によって不正利用されるという被害が発生している。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(クレジットカード利用者)
- 組織(サービス事業者、クレジットカード会社)

<脅威と影響>

近年、キャッシュレス決済の普及に加え、電子マネーやスマートフォンを使った決済方法(スマホ決済)等も登場し、クレジットカードを利用する機会が拡大している。そのクレジットカードの情報を攻撃者は狙っている。

攻撃者は、正規サイトに似せて作った偽のウェブサイト(フィッシングサイト)へクレジットカード利用者を誘導し、クレジットカード情報を詐取(フィッシング詐欺)したり、正規のショッピングサイトの決済画面を改ざんし、偽の決済画面でクレジットカード情報を入力させたりして詐取する。

クレジットカード情報が攻撃者に詐取されると、

クレジットカード利用者の知らない間に不正利用され、金銭的な被害を受けたり、クレジットカード情報をダークウェブ等で販売されたりするおそれがある。

<攻撃手口>

以下の手口でクレジットカード情報を入手し、不正利用を行う。

◆ フィッシング詐欺

メール等を使い、受信者をだましてフィッシングサイトに誘導し、クレジットカード情報等を詐取する。詳細は個人2位「フィッシングによる個人情報等の詐取」を参照。

◆ 正規の決済画面を改ざんし入力情報を詐取

ショッピングサイトの脆弱性等を悪用し、正規ウェブサイトの決済画面を改ざんする。その後、偽の決済画面に被害者を誘導し、クレジットカード情報を入力させることで、クレジットカード情報を詐取する。正規ウェブサイト上に偽の決済画面が作られているため、被害者がウェブサイトのドメイン等に気をつけていたとしても、偽の決済画面であることに気付くことが極めて困難である。

◆ 不正に取得したアカウントでなりすまし

サービスの利用者は、複数のサービスでパスワードを使いまわしていることがある。攻撃者は、他のサービスから漏えいしたパスワードを使ってログインを試みるパスワードリスト攻撃を行い、ショッピングサイト等に不正にログインする。そのショッピングサイトでクレジットカードが登録されていればそれを不正利用する。

◆ ウイルス感染

悪意のあるプログラムを含むファイルを作成し、メールに添付して送付する。メールを受信した被害者が、このファイルを開くと端末がウイルスに感染する。ウイルスに感染した端末上で決済を行うと、攻撃者にクレジットカード情報を窃取される。

<事例または傾向>

◆ 番号盗用被害の増加

日本クレジット協会が公開したクレジットカード不正利用被害の集計結果によれば、2019年の1～9月においてクレジットカード番号の盗用被害額は167億円となり、前年同期間の約132億円と比較して大幅に増加している。また、被害額全体の81.5%を番号盗用被害が占めており、その割合は年々増加している。¹

三井住友カード株式会社が実施した、クレジットカードの不正利用被害に遭った500人に対するアンケート調査では、被害者の内57.2%は自分のカードが不正利用された原因や手口を把握していないという結果となった²

◆ 不正ログインおよびカード不正利用

2019年6月13日、株式会社イオン銀行とイオンクレジットサービス株式会社は、イオンマークのカード会員向けインターネットサービスの「暮らしのマネーサイト」、およびスマホアプリの「イオンウォレット」への不正ログインおよびカード不正利用が確

認されたと発表した。

不正ログインされた可能性がある会員は1,917名、その内、カードが不正利用された会員は708名、被害総額は約2,200万円に上る。

不正ログインされた原因はパスワードリスト攻撃によるものと見られ、同社では会員に対して不正ログイン防止のための対策を呼びかけた。³

<対策/対応>

個人(利用者)

- 被害の予防
 - ・表1.3「情報セキュリティ対策の基本」を実施
 - ・パスワードの使いまわしをしない
 - ・クレジットカード会社が提供している本人認証サービス(3Dセキュア等)の利用
 - ・受信メールやウェブサイトの十分な確認
 - メールアドレスやウェブサイトのドメイン名が偽装されていないか確認する。
 - ・添付ファイルやURLを安易に開かない
 - ・信頼できるインターネットサービスの利用
 - ・普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
 - ・プリペイドカードの利用を検討
 - 不正利用被害額の範囲を限定する。
- 被害の早期検知
 - ・クレジットカードの利用明細の確認
 - ・サービス利用状況の通知機能等の利用
- 被害を受けた後の対応
 - ・該当サービスのコールセンターへの連絡
 - クレジットカード会社によっては、全額または一部補償してくれる場合がある。
 - ・クレジットカードの再発行
 - ・パスワードの変更
 - ・ウイルス感染した端末の初期化
 - ・警察への被害届の提出

参考資料

1. クレジットカード不正利用被害の集計結果について

<https://www.j-credit.or.jp/download/news20191227b.pdf>

2. 三井住友カード、クレジットカードの不正利用被害にあった500人に調査

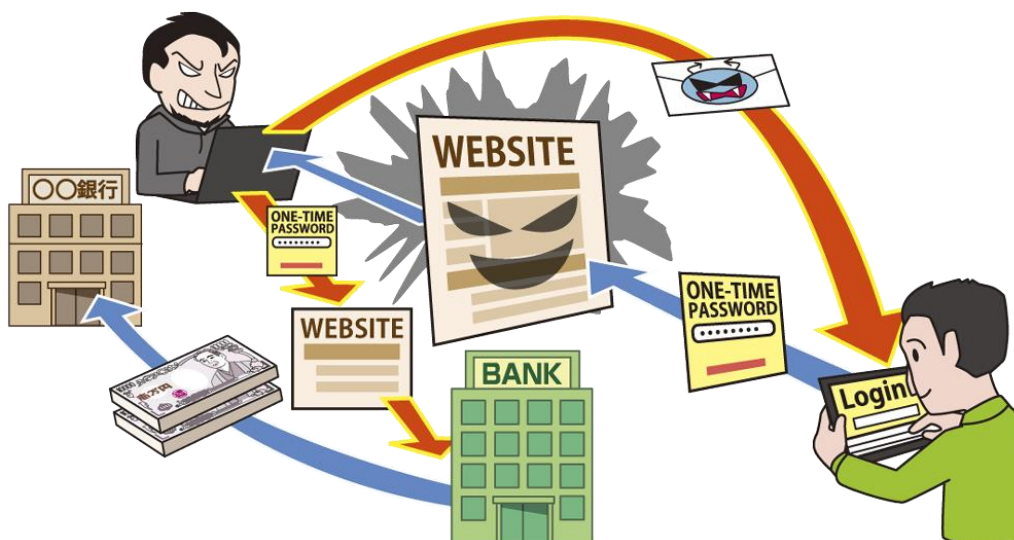
http://www.atpress.ne.jp/releases/202935/att_202935_1.pdf

3. インターネットサービス「暮らしのマネーサイト」での不正ログイン発生のお知らせおよびパスワード変更のお願いについて

https://www.aeon.co.jp/information/201906_info/index.html

4位 インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～



フィッシング詐欺やウイルス感染により、インターネットバンキングの認証情報を窃取され、攻撃者が本人になりすました不正送金や不正利用が行われている。近年はその被害が減少傾向であったが、2019年9月頃からフィッシング詐欺による不正送金被害が急増した。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(インターネットバンキング利用者)
- 組織(インターネットバンキング利用者)
- 組織(金融機関)

<脅威と影響>

偽のメールやSMS等により、攻撃者が用意した偽のウェブサイト(フィッシングサイト)へ被害者が誘導され、インターネットバンキングの認証情報を詐取(フィッシング詐欺)される。また、メールの添付ファイル等から被害者のパソコンがウイルスに感染し、インターネットバンキングの認証情報を窃取される等の攻撃が行われている。

情報を窃取された被害者は、自身のインターネットバンキングにログインされ、攻撃者が用意した口座に不正送金されることで金銭的被害を受ける。

<攻撃手口>

以下の手口でインターネットバンキングの認証情報を入手し、不正送金を行う。

◆ フィッシング詐欺

偽のメールやSMSを送信し、被害者をだましてフィッシングサイトに誘導し、インターネットバンキングの認証情報等を詐取る。また、二要素認証で使う情報(ワンタイムパスワード等)を入力させる場合もある。詳細は個人2位「フィッシングによる個人情報等の詐取」を参照。

◆ ウイルス感染

ウイルスに感染するように細工したファイルをメールに添付し、安全なファイルと誤認させファイルを開くように誘導し、ウイルスに感染させる。また、不正に改ざんされたウェブサイト被害者に閲覧させることにより、ウイルスに感染させる手口もある。

ウイルスに感染した端末でインターネットバンキングにログインしようとする、偽のログインページが表示され、そこに入力した認証情報がウイルスによって詐取される。

<事例または傾向>

◆ インターネットバンキングの不正送金が急増

警視庁によると、2019年上半期(1月～6月)のインターネットバンキングに関わる不正送金事犯の発生件数は186件、被害額は約1億7,600万円であり、前年同期の211件、約3億7,200万円に比べて減少している。しかし、2019年9月から急増し、10月の発生件数は397件、被害額は約5億1,900万円、また、11月の発生件数は573件、被害額は約7億7,600万円であり、11月の数値は2012年以降、最多の水準となっている。不正送金の多くはフィッシング詐欺によるものとみられており、金融機関を装ったフィッシングサイトへ誘導するメールやSMSが、多数確認されている。^{1,2}

また、フィッシング詐欺の手口として正規サイトのURLと誤認させるため、フィッシングサイトのURLにHTTPSから始まるものや.jpドメインが使用されているものもあり、日本サイバー犯罪対策センター(JC3)がメールに記載されたURLに安易にアクセスしないよう注意喚起を実施している。³

◆ 二要素認証を狙う攻撃が激化

インターネットバンキングの認証情報の詐取、特にワンタイムパスワード等の二要素認証の突破から不正送金を狙うと推測されるフィッシングサイトの拡大が確認されている。トレンドマイクロによると、これらフィッシングサイトのドメインは、2019年1月から8月に216件(1日当たり1件弱)を確認したが、9月は94件(1日当たり3件強)を確認しており、攻撃が激化してきたものとしている。

また、2019年8月以降に確認されたフィッシングサイトでは、JavaScriptやスタイルシートの取得URLに特徴的な文字列を含むものが確認されており、攻撃者が特定のツールキットを使用してフィッシングサイトを構築しているものと推測されている。⁴

<対策/対応>

個人(インターネットバンキング利用者)

- 被害の予防(被害に備えた対策含む)
 - ・受信メールやウェブサイトの十分な確認
 - ・添付ファイルやURLを安易にクリックしない
 - よく利用するウェブサイトは、予めブックマークに登録し、そこからアクセスする。
 - ・ファイルの拡張子を表示させる設定
 - ・普段は表示されないポップアップ画面に個人情報等は入力しない
 - ・金融機関や公的機関から公開される注意喚起等の確認
 - ・二要素認証等、金融機関が推奨する認証方式の利用
- 被害の早期検知
 - ・不審なログイン履歴の確認
 - ・口座の利用履歴の確認
 - ・サービス利用状況の通知機能等の利用
- 被害を受けた後の対応
 - ・該当サービスのコールセンターへの連絡
 - 金融機関によっては、全額または一部補償してくれる場合がある。
 - ・警察への被害届の提出
 - ・ウイルス感染した端末の初期化
 - ・パスワードの変更

参考資料

1. フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について(全銀協等と連携した注意喚起)
<https://www.npa.go.jp/cyber/policy/caution1910.html>
2. 平成30年上半期におけるサイバー空間をめぐる脅威の情勢等について[H30.9.20掲載]
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf
3. インターネットバンキングの不正送金の被害に注意
<https://www.jc3.or.jp/topics/banking/phishing.html>
4. 国内ネットバンキングの二要素認証を狙うフィッシングが激化
<https://blog.trendmicro.co.jp/archives/22696>

5位 メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～金銭を要求する脅迫・詐欺メールは無視を～



個人の秘密を家族や知人に公開すると脅迫したり、身に覚えのない有料サイトの未納料金を請求したりするメールや SMS(ショートメッセージサービス)を使った詐欺による金銭被害が発生している。公的機関を装った偽の相談窓口に誘導するといった新しい手口も確認されている。

<攻撃者>

- 犯罪グループ

<被害者>

- 個人(インターネット利用者)

<脅威と影響>

「アダルトサイトを閲覧している姿を撮影した」等の脅迫メールや有料サイトの未納金があるといった架空請求のメールを送信し、金銭を詐取しようとする攻撃が行われている。また、メールだけでなく SMS を使った同様の手口も確認されている。

脅迫・詐欺のメールの内容は虚偽のものであるが、信じてしまい不安に思ったメール受信者が金銭を支払ってしまう。また、一度金銭を支払ってしまうと、同様の脅迫や詐欺行為が何度も繰り返され、さらに被害が拡大するおそれもある。

<攻撃手口>

脅迫や架空請求によって金銭を要求する内容のメールや SMS を不特定多数に送り、金銭を詐取しようとする。指定される支払方法には仮想通貨や

電子マネーが多く見られる。また、騙す手口として以下が使われる。

◆ セクストーション(性的脅迫)

「アダルトサイトを閲覧している姿を撮影した」、「アダルト動画を見られる有料サイトを使用した料金が未納である。」等、周囲に相談しにくい性的な内容で脅す。¹

◆ 不正アクセスしているように見せかける

被害者のパスワードや住所等の個人情報をメールに記載し、あたかも被害者の PC に不正アクセスして情報を得たかのように見せかける。記載している情報は不正アクセスによるものではなく、外部のサービスから何らかの原因で漏えいした情報を使用している。

◆ 電話窓口への誘導

脅迫・詐欺のメールに問合せ窓口の電話番号を記載し、この電話番号宛に被害者から電話を掛けさせる。電話を掛けてきた被害者に対して、攻撃者は更に脅迫や催促を行う。また、電話口で公的機関を装った偽の相談窓口を紹介し、その窓口で電話を掛けさせ、信頼させた上で金銭を支払わせる。

<事例または傾向>

◆ 探偵社を装った脅迫メール

2019年8月に、探偵社の調査員を名乗った金銭を要求する脅迫メールが確認され、警察庁等が注意喚起を行った。メールは不自然な日本語で書かれており、内容としては、クライアントからの調査依頼で掴んだ貴方の秘密を家族に知られなくなったら仮想通貨で要求した額を支払うように、というものだった。警察庁は、「本文中に記載されているリンクは犯罪被害につながるものですので、クリックしないようにしてください。」と Twitter 上で注意を呼びかけている。^{2,3}

◆ 偽の消費生活センターを案内する新手口

「有料サイトの利用料金が未納である。」という内容のメール等に電話番号を記載して電話を掛けさせ、被害者を騙す手口が確認されている。2019年7月に報告された事例では、大手信販会社を騙った SMS に利用料金が未納である旨が書かれており、記載されている電話番号に電話をして心当たりがないことを伝えると、偽の消費生活センターの相談窓口を案内されるという手口が使われていた。案内された偽の相談窓口で電話をすると、請求は正しいものであり支払いに応じる必要があると指示され、実際にプリペイド型電子マネーで30万円を支払ってしまったという被害が発生している。⁴

◆ セクストーションメールを継続して確認

IPA 安心相談窓口には、2018年にセクストーションメールによる仮想通貨を要求する手口についての相談が多数寄せられたが、2019年も継続して同様の相談が寄せられた。相談件数は2018年と比べて減少し一時期は1か月に10件程度まで収束していたが、9月には76件に増えている。⁵

<対策/対応>

個人(インターネット利用者)

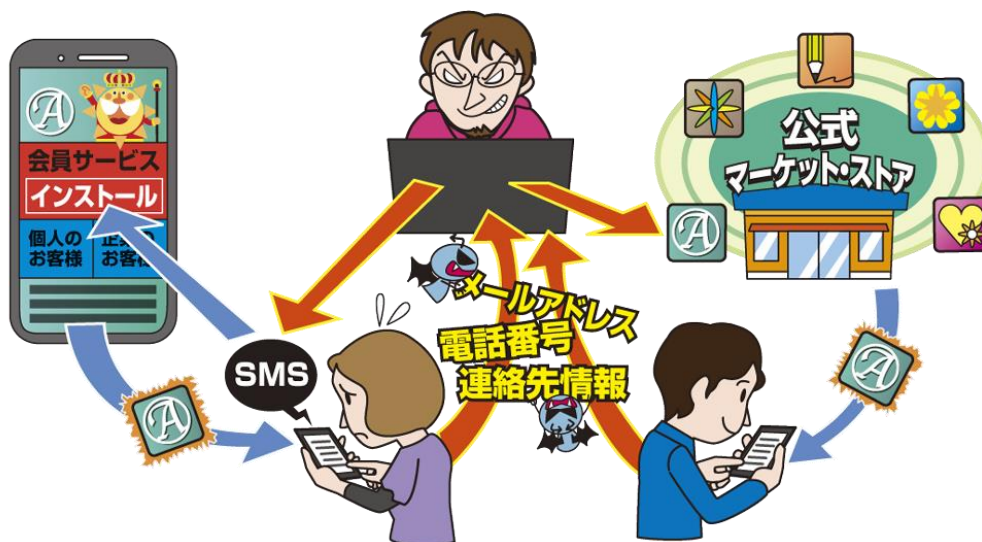
- 被害の予防(被害に備えた対策含む)
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・受信した脅迫・詐欺メールは無視する
 - 詐欺メールに、被害者のパスワード等が記載されていても、実際に不正アクセスされているわけではない。被害者のパスワード等は、別のところから漏えいしたものであると思われる。
 - ・メールに記載されている番号に電話をしない
 - 受信した脅迫や架空請求のメールについて専門機関に相談したい場合は、自分で窓口の電話番号やメールアドレスを調べるようにする。
- 被害を受けた後の対応
 - ・パスワードを変更する
 - 脅迫・詐欺メールに記載されたパスワードが自分のパスワードと一致しているのであれば、どこかからパスワードが漏えいしたおそれがあるので、早急にパスワードを変更する。
 - ・警察に相談する⁶
 - 一人で抱え込み脅迫に屈してしまうことのないように冷静に対処することが肝要。

参考資料

1. 「ハッターリだけでボロ儲け」「恥ずかしい写真」で恐喝、セクストーションスパムの手口
<https://www.itmedia.co.jp/news/articles/1901/30/news019.html>
2. 警察庁公式ツイッターアカウントによる注意喚起
https://twitter.com/npa_koho/status/1159724170894123008
3. 仕事のご健闘を祈り致します。
https://www.jc3.or.jp/topics/v_log/201908.html#d20190808
4. “ニセ”消費生活センターを案内する新手の架空請求の手口にご注意！
http://www.kokusen.go.jp/news/data/n-20190718_1.html
5. 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意
<https://www.ipa.go.jp/security/anshin/mgdayori20181010.html>
6. 都道府県警察本部のサイバー犯罪相談窓口等一覧
<https://www.npa.go.jp/cyber/soudan.html>

6位 不正アプリによるスマートフォン利用者への被害

～インストールしているのは本当に正規のアプリ？～



スマートフォン利用者が不正アプリを意図せずインストールし、スマートフォン内に保存されている重要な情報が窃取されたり、一部機能を悪用されたりする被害が確認されている。公式マーケット上に不正アプリが公開されているケースや、有名企業等になりすましたメールや SMS(ショートメッセージサービス)が届き、不正アプリのダウンロードサイトに誘導されるケースがある。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(スマートフォン利用者)

<脅威と影響>

正規のアプリに見せかけた不正アプリが公式マーケットに公開されている場合がある。また、有名な組織を装い、不正アプリのダウンロードサイトに誘導するメールや SMS 等が送信されてくる。

正規のアプリと信じて、不正アプリをスマートフォンにインストールしてしまうと、スマートフォン内に保存されている連絡先情報や通話記録、位置情報等の重要な情報が攻撃者に窃取されてしまう。また、録画や写真撮影、通話録音等のスマートフォンの機能を不正に利用される被害に遭うおそれもある。

<攻撃手口>

- ◆ 公式マーケットに不正アプリを紛れ込ませる
不正アプリを正規のアプリと見せかけて公式マーケットに公開する。利用者は公式マーケットのアプリは安全だと思い込み、安易にインストールしてしまう。
- ◆ メールや SMS 等を利用して不正アプリのダウンロードサイトへ誘導する
実在するウェブサイト似せた不正アプリのダウンロードサイトを用意し、メールや SMS 等を送信してダウンロードサイトに誘導、正規のアプリであると誤認させてインストールさせる。

<不正アプリによるスマートフォンの悪用例>

- 連絡先等の端末内の重要な情報を窃取
- 仮想通貨のマイニングに利用
- 録画・写真・通話録音機能を不正に利用
- DDoS 攻撃や悪意のある SMS の拡散などの踏み台

＜事例または傾向＞

◆ 日本郵便の不在通知を装った SMS から不正アプリのダウンロードサイトに誘導

日本郵便を装った SMS で偽サイトに誘導し、不正なアプリをダウンロードさせる手口が確認された。SMS には不在通知で荷物を持ち帰ったとする文言と URL が記載されており、Android 端末で URL にアクセスすると、「jppost.apk」という名称の不正アプリがダウンロードされるようになっていた。また、iPhone からアクセスした場合は、Apple ID の入力を求めてくる。

同社は、SMS による不在通知は行っておらず、また、ウェブサイトなどに掲載する URL において「.com」および「.top」といったトップレベルドメインは使用していないと注意を促した。¹

◆ 不正アプリを通じて電話番号を窃取され、詐欺に利用される。

2019 年 5 月、スマートフォン向け決済サービス PayPay の不正利用の詐欺容疑で逮捕者が出た。

2018 年 12 月、被害者は、佐川急便の不在通知を装う SMS を受信し、指示に従い記載されていた URL にアクセスしていた。このときに不正アプリがインストールされたおそれがある。

その後、攻撃者は被害者になりすまして PayPay に登録、その登録したアカウント上で、別ルートで入手した第三者のクレジットカードを登録した。登録を行うと、本人確認のための認証コードが登録した電話番号宛に SMS で届くようになっており、その認証コードを不正アプリによって窃取されてしまった。最終的には、攻撃者が被害者になりすまして登録したアカウントから第三者のクレジットカードが不正利用された。

攻撃者は、本被害者以外にも 3 人分のアカウントを所持しており、合計約 1,000 万円相当の商品を購入していた。²

＜対策/対応＞

個人(スマートフォン利用者)

● 被害の予防

- ・表 1.3「情報セキュリティ対策の基本」を実施
- ・アプリは公式マーケットから入手

スマートフォンの設定によっては公式マーケット以外からもアプリを入手可能だが、極力公式マーケットから入手する。ただし、公式マーケットにも不正アプリが紛れていることがあるため、レビューの評価に加え、アプリ開発者やアプリのバージョンアップ履歴等の情報を確認し、信頼できるアプリなのかを判断する。

・アクセス権限の確認

アクセス権限の確認の際に、アプリの機能に対して適切かどうか確認を行い、アプリの動作に関係がないと思われる権限が要求されている場合は、当該アプリをインストールしないことが望ましい。特にデバイス管理者になる権限を要求している場合は注意が必要である。

・アプリインストールに関する設定に注意

Android スマートフォンの設定で提供元不明のアプリのインストールを許可しない。

iPhone の設定で信頼されていないエンタープライズデベロッパを信頼しない。

・不要なアプリをインストールしない

不正アプリに限らず、正規のアプリであっても使い方を誤れば意図せず重要な情報を公開してしまうこともある。アプリの機能を理解し不要なアプリをインストールしない等の適切な利用を心がける。

● 被害を受けた後の対応

・不正アプリのアンインストール

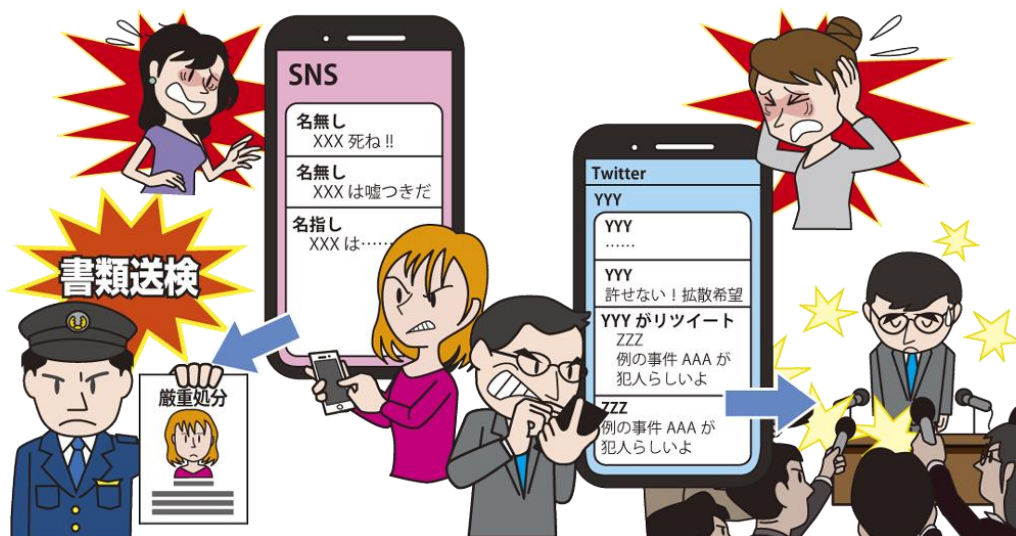
不正アプリをアンインストールする。できない場合は端末を初期化する。

参考資料

1. 当社の名前を装った迷惑メール及び架空Webサイトにご注意ください。
https://www.post.japanpost.jp/notification/notice/2019/1031_01.html
2. 宅配業者装うSMSに注意 スマホ乗っ取られ詐欺に悪用
<https://www.asahi.com/articles/ASM663JGXM66O1PE00G.html>

7位 ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～



インターネットの匿名性を利用して、特定の個人や組織に対して誹謗・中傷や根も葉もないデマを発信する事件が発生している。誹謗・中傷やデマの対象となった被害者は、精神的苦痛に苛まれる。また、既に発信されていた情報を転載した発信であっても、それが誹謗・中傷やデマであれば、転載して拡散した者も社会的責任を問われる場合がある。

<攻撃者>

- 情報モラル、情報リテラシーが低い人
- 悪意を持っている人

<被害者>

- 個人
- 組織(教育機関、公共機関、企業)

<脅威と影響>

SNS 等のサービスの普及に伴い、匿名での情報発信が容易に行えるようになっている。一方、そのサービスを利用する中で、意図的に他人への誹謗・中傷や、脅迫・犯罪予告・デマを書き込む事件が確認されている。さらに、その情報が安易に拡散され、收拾がつかなくなってしまう。

攻撃の対象が個人であれば、追い詰められて精神的苦痛に苛まれることもある。また、組織であれば、苦情電話対応や風評被害による経済的な損失を受ける等、様々な影響が出る。一方、誹謗・中傷等を発信した側も特定され、社会的責任を問われる場合がある。また、安易に拡散した人も責任を問われる対象となってしまう。

<要因>

◆ 情報モラルや自己抑制力の欠如

日常生活の中で、他者に対して恨みや妬み等から攻撃的な感情が湧いたり、また、自身の優位性や正義の誇示、ストレス発散、相手の反応を見たい等、身勝手な自己満足のための感情が湧いたりする場合がある。その際に、他者や社会に及ぼす影響を考慮せず、その感情を安易にインターネットへ発信してしまう。

◆ 個人が匿名で発信できる場の増加

昨今、様々なコミュニティサイトが存在し、個人が自由に匿名でブログや SNS、動画配信等で情報を発信することができる。一方、匿名性を利用し、普段人前では言えないことを安易に発信しやすくなっている。なお、匿名でも裁判所命令等に基づき発信者情報の開示請求を行えば身元を容易に特定できる場合が多い。

◆ 情報の真偽を確認せずに拡散

インターネット上には事実に基づかない誹謗・中傷やデマが出回ることがある。一見もつともらしく見えるため、その情報に同調し、拡散してしまう。有

用な情報を伝えたいという親切心や正義感によってデマを拡散してしまうケースもある。

＜事例または傾向＞

◆ 市議がデマを信じて拡散、名誉棄損で提訴

2019年8月に起きた煽り運転殴打事件において犯人と同乗していた女性として無関係の別の女性の名前や顔写真がインターネット上で拡散される出来事があった。その拡散されたデマ情報を信じた市議がさらに拡散した。その後、市議は拡散された女性から名誉棄損として訴えられた。市議は記者会見で非を認めて全面謝罪をし、議員を辞職している。¹

◆ 芸能人に対する誹謗・中傷で主婦書類送検

2019年6月、闘病中の女性芸能人に対して、芸能人のブログに「死ね」、「消えろ」等、誹謗・中傷する言葉を何度も書き込んだとして50代の主婦が脅迫容疑で書類送検された。取材に対して書類送検された主婦は、「みんな書いている」、「たたく人が多いのでなんとなく」、といった旨の主張をしている。²

＜対策/対応＞

個人(発信者)

- ・情報モラルや情報リテラシーの向上、法令遵守の意識の向上
- ・誹謗・中傷や公序良俗に反する投稿をしない
- 一度投稿した情報は、仮に後で削除したとしても、第三者がスクリーンショット等で保存することでインターネット上に残り続けるおそれがあることも意識する。
- ・投稿前に内容を再確認
- SNS やブログ等に投稿する内容は不特定多数の人に見られることを想定し、投稿して問

題ない内容かをしっかりと確認する。また、匿名で投稿していても、権利侵害があった場合は被害者がプロバイダーに発信者情報の開示を請求できるため、発信者の特定は可能という認識を持つ。

個人(家庭)、組織(教育機関)

- ・情報モラル、情報リテラシーの教育

自宅や学校で子供たちに情報モラルや情報リテラシーの教育を行う。さらに、トラブルの事例を伝え、悪質な行為は犯罪になりうることを理解させる。³

個人(閲覧者)

- ・情報モラルや情報リテラシーの向上、法令遵守の意識の向上
- ・安易な拡散をしない

インターネット上に流通している情報が必ずしも正しいとはかぎらないため、安易に拡散せず、一次情報やその他複数の情報元を確認し、信頼できる情報かを総合的に判断する。また、デマの拡散は、犯罪になりうることを理解する。

個人(被害者)

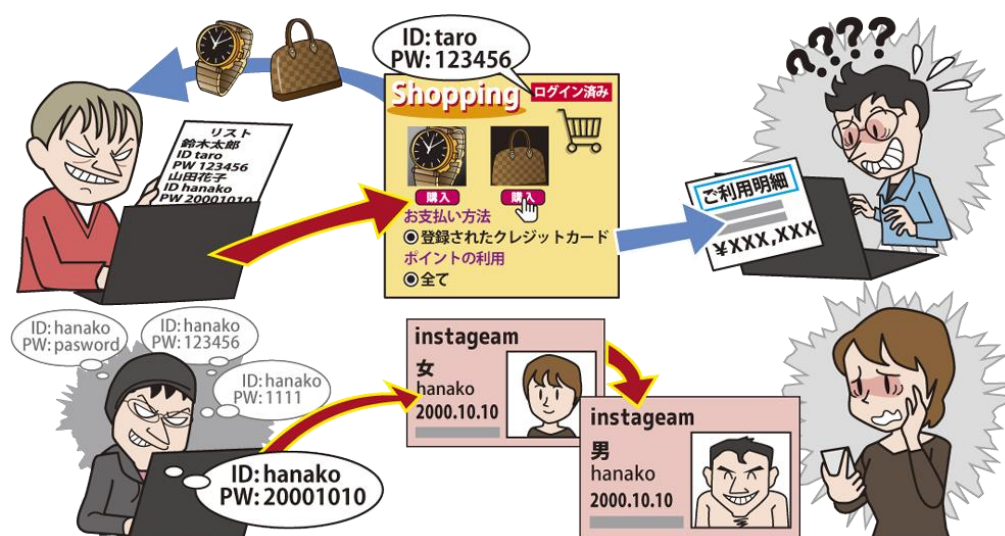
- 被害を受けた後の適切な対応
- ・冷静な対応と支援者への相談
- 一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する。⁴
- 犯罪と思われる誹謗・中傷の投稿は、警察へ被害届を提出。必要に応じて弁護士にも相談する。
- ・管理者やプロバイダーへ削除依頼
- 問題ある書き込みを削除したいときは、本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により炎上の火種になるおそれもあるため、書き込み内容の関係者等に相談して慎重に行う。

参考資料

1. あおり運転「デマ拡散」で訴えられた豊田市議、「私も被害者」と独特な持論を展開
<https://news.livedoor.com/article/detail/17382809/>
2. 堀ちえみのブログに誹謗中傷「死ね消えろ」、50代主婦が書類送検
<https://www.sanspo.com/geino/news/20190717/sca19071705030001-n1.html>
3. インターネットトラブル事例集(2018年度版)
http://www.soumu.go.jp/main_content/000590558.pdf
4. インターネット人権相談受付窓口(法務省人権擁護局)
<http://www.moj.go.jp/JINKEN/jinken113.html>

8位 インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～



インターネット上のサービスへ不正ログインされ、金銭や個人情報等の重要情報が窃取される被害が確認されている。別のサービスと同じ ID やパスワードを使いまわす利用者を狙ったパスワードリスト攻撃による不正ログインが行われている。また、不正ログインで得た情報を利用して更に被害を拡大させるおそれがある。

<攻撃者>

- 犯罪グループ
- 犯罪者(愉快犯、スーカ一等)

<被害者>

- 個人(サービス利用者)
- 組織(サービス運営者)

<脅威と影響>

インターネット上のサービスに対して不正に入手した ID やパスワードを使い、不正ログインを行う攻撃が行われている。ID やパスワードは、別のサービスから漏えいしたものを使う以外にも、被害者が使いそうなものを推測する手口もある。

不正ログインされると、サービスに応じた被害を受ける。ショッピングサイトであれば、氏名、住所、電話番号やサイトに登録しているクレジットカード情報等を窃取されたり、商品の不正購入やサイト内のポイントを盗用されたりする。また、スマートフォン等を利用したキャッシュレスの決済サービスであれば、チャージした残高を不正に利用される。さらに、LINE 等の SNS(ソーシャル・ネットワーキング・サービス)であれば、プライベートな写真やメッ

セージのやりとり等を覗き見されたり、偽の投稿をされたりする。

<攻撃手口>

◆ パスワードリスト攻撃

攻撃者が何らかの方法で事前に入手した ID とパスワードのリストを使用し、自動的に入力するプログラムなどを用いて、ログイン機能を持つインターネット上のサービスにログインを試みる。複数のサービスで ID とパスワードを使い回していると、それら全てのサービスでログインされるおそれがある。

◆ パスワード推測攻撃

使われやすいパスワードを推測し、そのパスワードでログインを試みる。また、芸能人や知人等の個人情報(氏名、誕生日等)からパスワードを推測して、ログインを試みる。

英単語(password、football)、数字の羅列(123456、111111)、キーボードの配列(qwerty、asdfgh)等を使ったパスワードは容易に推測できる。また、SNS等から個人情報やそのヒントとなる情報を入手することもある。

◆ ウイルス感染

攻撃者の用意した悪意あるウェブサイトへアクセスさせたり、メールに添付されている悪意あるファイルを開かせたりすることで、利用者の端末をウイルスに感染させる。利用者がその端末でインターネット上のサービスにログインすると、そのとき入力した ID やパスワードを攻撃者に詐取され、不正ログインに使われる。

<事例または傾向>

◆ パスワードリスト攻撃で約 46 万件の個人情報流失

株式会社ファーストリテイリングが運営するユニクロ、株式会社ジーユーの公式オンラインストアにて、2019 年 4 月 23 日から 5 月 10 日にかけてパスワードリスト攻撃が行われ、約 46 万件のアカウントに不正ログインが行われた。利用者から、「身に覚えのない登録変更通知メールが届いた」という申し出から、不正ログインが発覚した。個人情報が閲覧された可能性のある利用者にはパスワードを初期化し、個別に再設定を依頼するメールを送信し対応している。今回の攻撃は、パスワードの使いまわしによって被害が発生した可能性が高いとされており、利用者に注意を促している。¹

◆ 不正ログインによるポイントの不正利用

育児や出産に関する情報サイト「ベビータウン」「プレママタウン」において、2019 年 7 月 31 日から 8 月 6 日にかけてパスワードリスト攻撃と見られる不正ログインが確認された。この不正ログインによって、数名の会員のポイントが不正に使用され、Amazon ギフト券への交換が行われた。同社は、今回の不正アクセスは、別のサービスから流出したメールアドレスやパスワードを用いた可能性が高

いとしている。²

◆ インスタグラムの乗っ取り被害

2019 年 7 月 28 日、歌手の公式インスタグラムが不正ログインされ、乗っ取り被害に遭っていることが明らかになった。プロフィール写真が変更されたり、無関係な動画等が投稿されたりした。公式 Twitter ではフォロワーに対して、DM(ダイレクト・メッセージ)が届いた場合は本人からのものではないので注意するよう呼び掛けている。³

<対策/対応>

個人(ウェブサービス利用者)

- 被害の予防
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・添付ファイルや URL を安易にクリックしない
 - ・パスワードは長く、複雑にする
 - ・パスワードの使いまわしをしない
 - ・パスワード管理ソフトの利用
 - ・サービスが推奨する認証方式の利用
 - 二要素認証や多段階認証が提供されている場合は利用する。⁴
 - ・不審なウェブサイトで安易に認証情報を入力しない(フィッシングに注意)
 - ・利用していないサービスからの退会⁵
- 被害の早期検知
 - ・利用しているサービスのログイン履歴の確認
 - ・クレジットカードやポイント等の利用履歴の定期的な確認
- 被害を受けた後の対応
 - ・パスワードの変更
 - ・クレジットカードの停止
 - ・不正ログインされたサービスの運営者へ連絡

参考資料

1. 「リスト型アカウントハッキング(リスト型攻撃)」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて
https://www.uniqlo.com/jp/corp/pressrelease/2019/05/19051409_uniqlo.html
2. 不正ログインに関するお知らせとパスワード変更のお願い
<https://www.babytown.jp/b/info/190913-01.html>
3. PUFFY大貫亜美インスタ乗っ取り被害「対応中」
<https://www.nikkansports.com/entertainment/news/201907280000671.html>
4. 不正ログイン対策特集ページ
https://www.ipa.go.jp/security/anshin/account_security.html
5. アカウント乗っ取りによる被害を防ぐための7つのポイント
<https://www.is702.jp/special/3517/>

9位 偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～



PC やスマートフォンの利用者に対してインターネット閲覧中に、突然「ウイルスに感染しています」等の偽の警告画面（偽警告）を表示して、不要なソフトウェアをインストールおよび購入させたり、攻撃者が用意したサポート窓口で電話を掛けさせてサポート契約を結ばせたりする被害が発生している。偽警告は利用者の不安につけこむ手口であり、表示されても慌てず冷静に対応する必要がある。

<攻撃者>

- 犯罪グループ

<被害者>

- 個人（インターネット利用者等）

<脅威と影響>

インターネット閲覧中に、突然「ウイルスに感染しています」、「Windows のシステムが破損しています」等の警告画面がブラウザ上に表示されることがある。その中には根拠のない偽警告の場合があり、PC やスマートフォンの利用者は表示された偽警告を信じてしまい、警告の指示に従ってしまう。

PC 利用者であれば、不要なソフトウェアをインストールしたり、サポート契約を結ばせられたりする。スマートフォン利用者であれば、不要なアプリをインストールするように誘導される事例が多い。また、ソフトウェアの購入やサポート契約時に登録した氏名、メールアドレス、クレジットカード情報は別の詐欺等に悪用され、二次被害につながるおそれもある。

<攻撃手口>

◆ 巧みに細工が施された偽の警告画面

偽警告は様々な警告メッセージを使い、警告内容を信じさせるために実在の企業ロゴを使う場合がある。また、警告音を鳴らしたりや警告メッセージを音声で流したり、偽警告のポップアップを閉じられないようにしたりすることでさらに不安を煽る。

◆ 偽セキュリティソフトの購入を誘導

偽警告の画面からダウンロードページに誘導し、偽のセキュリティソフトをインストールさせる。最終的に有償ソフトウェアの購入へ誘導する。

◆ サポート契約詐欺

偽警告の画面に記載されているサポート窓口で電話をかけさせ、オペレーターによる遠隔操作で対策したように見せかけ、有償のサポート契約へ誘導する。サポート契約の支払い方法はクレジットカード決済や各種ギフトカード、コンビニ決済等を使う。

◆ スマホアプリのインストールへ誘導

偽警告をスマートフォンの画面に表示し、警告画面に表示された警告の解決方法として、スマホア

プリの公式マーケットからスマホアプリをインストールするように誘導する。

アプリのインストールへ誘導したことに対してのアフィリエイト収益や自動継続課金による料金請求が目的と考えられる。

<事例または傾向>

◆ 実在する製品に偽装した警告を表示

トレンドマイクロのセキュリティソフト製品での検出を偽装する偽警告が確認されている。本件では、正規ソフトウェアの知名度を悪用し、利用者信じさせて目的のソフトウェアをダウンロードおよび、インストールさせようとしている。¹

◆ 破棄されたドメインを悪用して偽警告を表示するページを公開

2019年10月、宮城県から、「東北文化の日」事業推進に関して、旧サイトのURLにアクセスすると偽警告が表示されたことが報告されている。本件では、2019年6月まで運営していたイベントサイトを閉鎖し、手放したドメインが悪用され、対象のドメインにアクセスするとWindowsセキュリティシステムが破損していると警告が表示され、悪意のあるサイトへ誘導するようになっていた。²

◆ スマートフォンでの偽警告の相談が6月から増加

IPA安心相談窓口寄せられる偽警告に関する相談の内、スマートフォンにおける偽警告の相談が2019年6月から増加している。相談の中で多かったものとしては、誘導された先でインストールさせられたアプリケーションが無料ではなく、利用料金を請求されるケースがあったとして、安心相談窓口では、注意喚起を実施し、利用者に注意を促している。手口としては、これまでと同じく利用者にアプリケーションをインストールさせるものに加え、イ

ンストールしたアプリケーションが自動継続課金であるケースも確認されている。自動継続課金のアプリケーションの場合、アプリをアンインストールするだけでは料金請求を止めることができず、別途、自動継続課金の停止手続きが必要となる。³

<対策/対応>

個人(インターネット利用者)

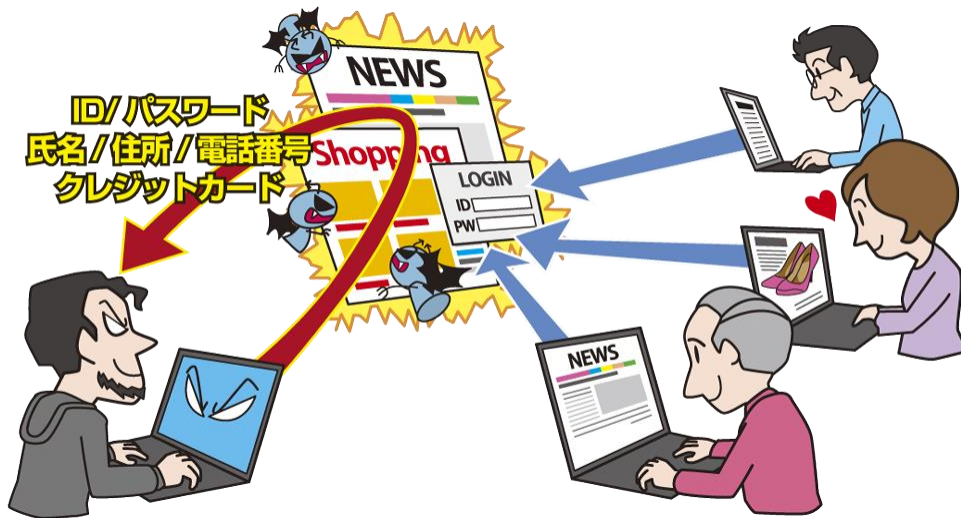
- 被害の予防(被害に備えた対策含む)
 - ・表1.3「情報セキュリティ対策の基本」を実施
 - ・偽警告が表示されても従わない
偽警告の指示に従いアプリやソフトウェアはインストールしない。また、電話は掛けない、遠隔操作は許可しない、契約には応じない。
 - ・偽警告が表示されたらブラウザを終了
 - ・ブラウザの通知機能を不用意に許可しない
偽警告の中にはブラウザの正規の通知機能を悪用するものもあるので注意する。
 - ・警告が本物か偽物かの判断は冷静に
警告画面には本物と偽物がある。警告が本物か偽物かを判断するため、OSやセキュリティソフトの仕様を把握する(正規の警告を知る)。判断が難しい場合は信頼できる周りの方に相談する。
- 被害を受けた後の対応
 - ・ソフトウェアをアンインストール
インストールしたソフトウェアをアンインストールする。できない場合は端末を初期化する。
 - ・サポート契約の解消
近くの消費生活センター⁴に相談する。
 - ・自動継続課金の停止
 - ・クレジットカード会社へ連絡

参考資料

1. トレンドマイクロ製品を詐称する「偽警告」を確認
<https://blog.trendmicro.co.jp/archives/20334>
2. 令和元年度「東北文化の日」推進事業について - 宮城県公式ウェブサイト
<https://www.pref.miyagi.jp/soshiki/syoubun/tohokubunka-2019.html>
3. IPA 安心相談だより「スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意」
<https://www.ipa.go.jp/security/anshin/mgdayori20190918.html>
4. 独立行政法人 国民生活センター 全国の消費生活センター等
<http://www.kokusen.go.jp/map/index.html>

10位 インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～



ショッピングサイト(EC サイト)等のインターネット上のサービスへ脆弱性等を悪用した不正アクセスや不正ログインが行われ、サービスに登録している個人情報等の重要な情報を窃取される被害が発生している。窃取された情報を悪用されるとクレジットカードの不正利用等の二次被害につながる。

<攻撃者>

- 犯罪グループ

<被害者>

- 個人(サービス利用者)
- 組織(サービス利用者)

<脅威と影響>

多くの企業や組織は事業としてインターネット上に様々なサービスを提供している。サービスを利用するために会員登録を行うサイトも存在し、例えばショッピングサイトであれば個人情報等の重要な情報(氏名、性別、生年月日、メールアドレス、クレジットカード情報)が登録されている。

一方、インターネット上のサービスは様々なソフトウェアから構成されている。サービス提供者がそれらのソフトウェアを適切に管理していない場合、セキュリティ上の欠陥である脆弱性を内在したままサービスを提供しているおそれがある。攻撃者にソフトウェアの脆弱性を悪用されると個人情報等の重要な情報を窃取される。

また、攻撃者にサービスを利用するための認証情報(ID とパスワード)を窃取されると、サービスに

不正ログインされ、重要な情報を窃取されるおそれがある。その結果、クレジットカードを不正利用されたり、詐欺メールを送信されたり、窃取された情報をダークウェブで売買されたり等、二次被害につながるおそれがある。

<攻撃手口>

◆ サービスの脆弱性や設定不備を悪用

攻撃者は、使用しているソフトウェアに適切なセキュリティ対策が行われていないショッピングサイト等に対して、脆弱性や設定不備を悪用して、ウェブサイト内の個人情報等の重要情報を窃取する。

また、攻撃者はウェブサイトの脆弱性を悪用してウェブサイトを改ざんする。サービスの利用者が改ざんに気づかず情報を入力してしまうと、その情報は攻撃者に窃取される。

◆ 他のサービス等から窃取した認証情報を悪用

他のサービス等から窃取した認証情報(ID とパスワード)を悪用してサービスへ不正ログインし、個人情報等の重要な情報を窃取する。詳細は個人 8 位「インターネット上のサービスへの不正ログイン」を参照。

<事例または傾向>

◆ 不正アクセスで顧客のクレジットカード情報を流出

2019年3月、ヤマダ電機が運営するオンラインストア「ヤマダウェブコム」、「ヤマダモール」が不正アクセスを受け、ペイメント(決済)アプリケーションを改ざんされた。改ざんされていた約1ヶ月の間に新規登録、変更を行った約3万7,000件のクレジットカード情報(クレジットカード番号、有効期限、セキュリティコード)が流出し、一部の利用者のクレジットカード情報が不正利用されたおそれがある。¹

◆ アンケートモニターサービスより個人情報や年収等の情報が漏えい

2019年5月、マーケティングアプリケーションズが運営するアンケートモニターサービス「アンとケイト」、「ポケットアンとケイト」において、第三者による不正アクセスを受け、氏名、メールアドレス、パスワード、生年月日、未既婚、子供の有無、年収、職業、住所、電話番号、口座番号等を含む可能性がある約77万アカウント分の情報を漏えいした。原因は、サーバーの設定上の不備を攻撃されたことで、不備は修正済みとしている。²

◆ ウェブサイトから窃取した個人情報を悪用され、当選詐欺メールが送られる

2019年12月、部品・消耗品販売サイト「象印でショッピング」が不正アクセスを受け、登録されている氏名、住所、メールアドレス等、最大約28万件の個人情報が漏えいした。不正アクセスの原因は、システムの一部の脆弱性を突かれたことによるものとしている。さらに、窃取されたメールアドレス宛にQUOカードの当選詐欺メールも送られた。詐欺メールに記載された偽サイトに誘導され、クレジットカード情報等を入力した場合は、入力した情報を攻撃者に詐取されたおそれがある。³

<対策/対応>

個人(インターネット利用者)

- 情報モラルやリテラシーの向上
 - ・不要な情報は安易に登録しない
 - ・情報漏えいに備えて、サービスを利用するための必須項目以外の情報は登録を避ける。
 - ・利用していないサービスの退会
 - ・不正ログイン対策
 - 詳細は個人8位「インターネット上のサービスへの不正ログイン」を参照。
- 被害の早期検知
 - ・クレジットカード利用明細の定期的な確認
 - ・クレジットカード情報が窃取され、不正利用された場合、被害に気づける可能性がある。
- 被害を受けた後の対応
 - ・サービス運営者への問い合わせ
 - ・クレジットカードの停止
 - クレジットカード会社へ不正利用の連絡と停止の手続きを行う。
 - ・パスワードの変更
 - サービスを継続して利用する場合はパスワードを変更する。
 - ・警察への被害届の提出

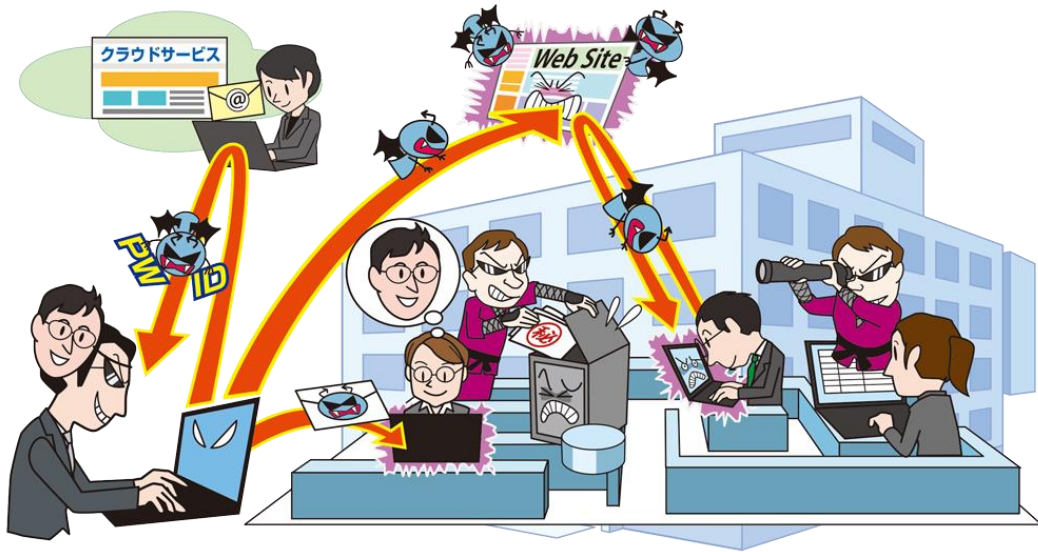
参考資料

1. 弊社が運営する「ヤマダウェブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ
<https://www.yamada-denki.jp/information/190529>
2. 不正アクセスによる会員情報流出に関するお詫びと追加ご報告
https://mkt-apps.com/news/20190628_214/index.html
3. 【重要】個人情報流出についてのお知らせ(象印でショッピング)
<https://www.zojirushi.co.jp/important/info/01.html>

1.2. 情報セキュリティ 10 大脅威(組織)

1位 標的型攻撃による機密情報の窃取

～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～



企業や民間団体そして官公庁等、特定の組織に対して、機密情報等を窃取することを目的とした標的型攻撃が発生している。2020 年初頭には、複数の防衛関連企業が不正アクセスを受けていたという報道があった。

<攻撃者>

- 諜報員、産業スパイ
- 犯罪グループ
- 犯罪者

<被害者>

- 組織(官公庁、民間団体、企業、研究機関、教育機関等)

<脅威と影響>

特定組織の機密情報等の窃取を目的とし、PC をウイルスに感染させ、組織内部へ潜入する標的型攻撃が確認されている。従業員が悪意あるメールの添付ファイルを開いたり、悪意あるウェブサイトにアクセスしたりすると、PC がウイルスに感染する。その後、感染 PC を起点に組織内部のネットワークやサーバー等を探索し、侵害範囲を拡大しながら機密情報等の窃取を行う。また、標的組織の関連組織が攻撃の踏み台にされることもあり、業種や組織の規模に関係なく狙われるおそれがある。

機密情報等が漏えいし、悪用されると、組織、企業の事業継続や国家の安全保障等に大きな影響を与えるおそれがある。

<攻撃手口>

◆ メール添付ファイル、リンクを開かせる

メール添付ファイルや本文に記載したリンク先にウイルスを仕込み、開かせることで組織の PC をウイルスに感染させる。件名や本文、添付ファイル名は業務に関連するようなものに偽装し、実在する組織の差出人名が使われる場合もある。

◆ ウェブサイトの改ざん

標的組織が頻繁に利用するウェブサイトを調査し、そのウェブサイトを閲覧すると PC がウイルスに感染するようウェブサイトを改ざんする。標的組織の従業員は当該ウェブサイトを閲覧して PC がウイルスに感染する。(水飲み場型攻撃)

◆ 不正アクセス

組織が利用するメールのクラウドサービスやウェブサーバーへ不正アクセスし、認証情報等を窃取する。その情報を使い、社内システムへのアクセス等に用いる正規の経路で組織内部へ潜入し、組織内部の PC やサーバーをウイルスに感染させる。

<事例または傾向>

◆ プラント関連業者を狙う標的型攻撃メール

サイバー情報共有イニシアティブ(J-CSIP)によると、2019年にJ-CSIP参加組織宛に届いた標的型攻撃メールとみなした情報は計282件であり、2018年の267件と比較して微増した。

2019年に確認したウイルスの中には「アイコンや拡張子の偽装」、「特定のセキュリティソフトの停止」、「特定の時間帯のみ動作を行う」、「不正接続先から特定の応答が得られないと動作を止める」等、ウイルス自身の存在、攻撃活動の露見、ウイルス解析者による解析を避けるような様々な仕掛けが施されたものも確認された。¹

◆ 委託先での標的型攻撃メールの被害

国土交通省は、保守業務の委託先の組織が標的型攻撃メールを開封し、設備関連の資料が外部に漏えいしたおそれがあることを発表した。同省は委託先の組織に対してさらなる情報の流出を防ぐ対策を行うように指示している。²

◆ 複数の企業における標的型攻撃と思われる不正アクセス報道

2020年初頭、外部からの不正アクセス事案について三菱電機が公表した。³その発覚は、2019年6月に不審な挙動が見られる社内端末が確認されたことであった。

この公表後、NECや神戸製鋼、パスコより立て続けに不正アクセス被害が公表された。⁴

<対策/対応>

組織(経営者層)

- 組織としての体制の確立
 - ・CSIRTの構築
 - ・対策予算の確保と継続的な対策の実施
 - ・セキュリティポリシーの策定

組織(セキュリティ担当者、システム管理者)

- 被害の予防/対応力の向上
 - ・情報の管理とルール策定

・サイバー攻撃に関する継続的な情報収集と情報共有

・セキュリティ教育の実施

・インシデント発生時の訓練の実施

・統合運用管理ツール等によるセキュリティ対策状況の把握

統合運用管理ツールを使い従業員や職員が利用するPCのソフトウェア更新状況を管理し、リスクの可視化を行う。

・取引先のセキュリティ対策実施状況の確認

・セキュアなシステム設計

・ネットワーク分離

・重要サーバーの要塞化(アクセス制御、暗号化等)

・海外拠点等も含めたセキュリティ対策の向上

● 被害の早期検知

・ネットワーク監視、防御

UTM・IDS/IPS・WAFなどの導入

・エンドポイントの監視、防御

● 被害を受けた後の対応

・CSIRTの運用によるインシデント対応

・影響調査および原因の追究、対策の強化

・関係者、関係機関への連絡

監督官庁、個人情報保護委員会、警察等

組織(従業員・職員)

● 情報リテラシーの向上

・セキュリティ教育の受講

メールの添付ファイルやURLを安易に開かない。Officeファイルにおいて、マクロ有効化やコンテンツ有効化のボタンを安易に押さない。被害を受けた際は迅速に連絡する。等

● 被害の予防(通常、組織全体で実施)

・表1.3「情報セキュリティ対策の基本」を実施

● 被害を受けた後の対応

・CSIRTへの連絡

参考資料

1. サイバー情報共有イニシアティブ(J-CSIP(ジェイシップ)) - 公開レポート Vol.27、28、30、31、32、33、34、35

<https://www.ipa.go.jp/security/J-CSIP/>

2. 近畿地方整備局業務受注者における情報流出の疑いについて

http://www.mlit.go.jp/report/press/kanbo08_hh_000612.html

3. 不正アクセスによる個人情報と企業機密の流出可能性について(第3報)

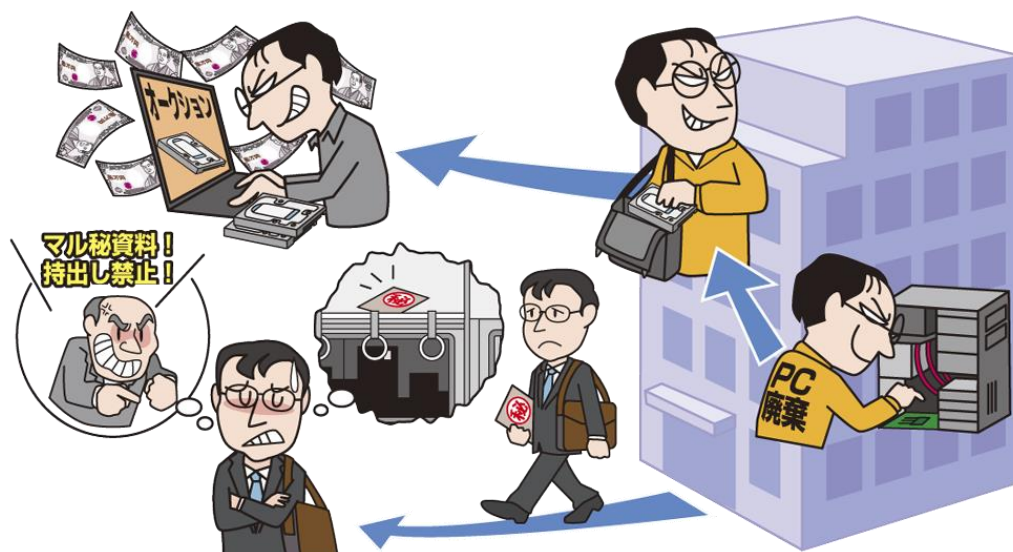
<https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf>

4. 神戸製鋼所とパスコにサイバー攻撃 防衛情報標的か

<https://www.nikkei.com/article/DGXMZO55342190W0A200C2CR8000/>

2位 内部不正による情報漏えい

～内部不正をさせない管理・監視体制を～



組織の従業員や元従業員等、組織関係者による機密情報の持ち出しや悪用等の、不正行為が発生している。また、組織の情報管理のルールを守らずに情報を持ち出し、さらにはそれを紛失し、情報漏えいにつながることもある。内部不正は、組織の社会的信用の失墜、損害賠償による経済的損失等により、組織に多大な損害を与える。

<攻撃者>

- 組織の従業員（在職者、離職者）

<被害者>

- 組織
- 個人（顧客、サービス利用者）

<脅威と影響>

組織に対する私怨や金銭目的等から、従業員や元従業員が組織の機密情報を不正に持ち出し、公開・売買することで組織に損害を与えることがある。また、従業員が自宅や外出先で仕事をするため、情報管理のルールを守らずに情報を持ち出し、その情報を紛失してしまい、情報漏えいにつながる可能性がある。

漏えいした情報の機密性や重要性、漏えい規模によっては、組織の社会的信用の失墜や、顧客等への損害賠償による経済的損失が発生する。これらは組織の競争力の弱体化等につながり、その結果、組織の根幹を揺るがすインシデントに発展するおそれがある。

<攻撃手口>

◆ アクセス権限の悪用

付与された権限を悪用し、組織の重要情報を取得する。必要以上に高いアクセス権限が付与されている場合、より多くの情報が窃取され、被害が大きくなるおそれがある。

◆ 在職中に割り当てられたアカウントの悪用

組織を離職した者が、在職中に使用していたアカウントを使って、組織内部の情報を不正に取得する。

◆ 内部情報の不正な持ち出し

組織内部の情報を、USB メモリーや HDD 等の外部記録媒体、電子メール、紙媒体、クラウドストレージ等を利用して、外部に不正に持ち出す。

<事例または傾向>

◆ 従業員が破壊処理予定の HDD を転売

情報機器の再生事業を手掛けるブロードリンクの従業員が、データ消去作業（物理破壊）前の HDD を盗み出してネットオークション等で転売し、懲戒解雇処分となった。さらに警察への被害届も

提出されている。当該 HDD は、神奈川県が契約したリース会社である富士通リースに返却したサーバーに搭載されていたものであり、HDD 内には県の内部資料や個人情報などが含まれていた。^{1,2}

◆ 委託先が個人情報を含む報告書を紛失

大阪市の自立支援センターの運営委託先が、個人情報を記載した「入所報告書」及び「退所報告書」を紛失した。個人情報を含む資料の運搬は受託事業者の車両で行う規則となっていたが、職員が鞆に入れて持ち歩き電車内に鞆ごと置き忘れ紛失した。紛失に気付いた職員が交通機関や警察に届け出たが発見には至っていない。³

◆ 元従業員が患者情報等を不正持ち出し

医療機器の製造、販売を手がけるアークレイの元従業員が、患者情報、顧客やアンケート回答者の個人情報、技術や営業に関する情報を不正に持ち出し、不正競争防止法違反（営業秘密領得）の容疑で書類送検された。患者情報は社用 PC から USB メモリー経由で私用 PC にコピーされていた。⁴

<対策/対応>⁵

組織

● 被害の予防

- ・基本方針の策定

組織全体において効率的な対策を推進するため、経営者の積極的な関与が重要である。内部不正対策は経営者の責任であることを示すとともに、最高責任者である経営者が総括責任者の任命並びに管理体制及び実施策の承認を行い、組織横断的な管理体制を構築する必要がある。

- ・重要資産の把握、体制の整備

重要資産を把握し、重要度に合わせて格付

けをした上で、重要情報の管理者を定める。

- ・重要情報の管理、保護

重要情報の利用者 ID 及びアクセス権の登録・変更・削除に関する手順を定めて運用する。従業員の異動や離職に伴い不要となった利用者 ID は直ちに削除する。利用者 ID は共用しない等を検討する。

- ・物理的管理の実施

重要情報の格納場所等への入退去を管理する。USB メモリーや HDD、PC、スマホ等の記録媒体の利用制限や持ち出し/持ち込みの管理をする。また、記録媒体を廃棄する際には適切なデータ消去の運用を実施する。

● 情報モラルの向上

- ・人的管理及びコンプライアンス教育の徹底

情報取扱ポリシーの策定や、内部不正者への懲戒処分等を規定した就業規則等の整備を行い、従業員に対する教育を定期的を実施する。その際、従業員に秘密保持誓約書等の提出を要請することも重要である。

また、離職者とは秘密保持契約等を締結し、重要情報の漏えいを防止する。

● 被害の早期検知

- ・システム操作履歴の監視

重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定期的に監視することで、早期検知に努める。

● 被害を受けた後の対応

- ・関係者、関係機関への連絡

監督官庁、個人情報保護委員会、警察等

- ・影響調査および原因の追究、対策の強化

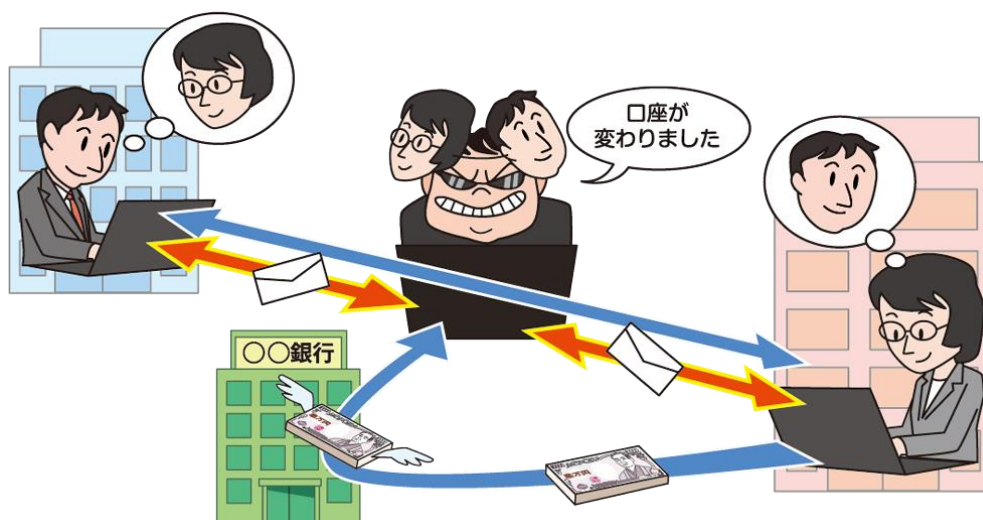
- ・内部不正者に対する適切な処罰実施

参考資料

1. (情報システム課からのお知らせ)リース契約満了により返却したハードディスクの盗難について
<https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html>
2. 当社管理下にあるハードディスク及びデータの外部流出に関するお詫び
<https://www.broadlink.co.jp/info/pdf/20191209-02-press-release.pdf>
3. 報道発表資料「自立支援センター舞洲」の管理運営等業務受託事業者における「入退所者関連資料」の紛失について
<https://www.city.osaka.lg.jp/hodoshiryo/fukushi/0000480597.html>
4. 当社元従業員の不正行為について(お詫びとご説明)
http://www.arkray.co.jp/japanese/news/press/release20190308_jp_jp.html
5. 組織における内部不正防止ガイドライン
<https://www.ipa.go.jp/security/fy24/reports/insider/>

3位 ビジネスメール詐欺による金銭被害

～この数年でメジャーなサイバーリスクへと変貌～



ビジネスメール詐欺(Business E-mail Compromise: BEC)は、海外の取引先や自社の役員等になりすまし、巧妙に細工された偽の電子メールを企業の出納担当者へ送り、攻撃者が用意した口座へ送金させる詐欺の手口である。海外だけではなく日本国内でも高額な被害が確認されている。

<攻撃者>

- 犯罪グループ

<被害者>

- 組織(企業、金銭の決裁権限を持つ責任者、金銭を取り扱う担当者)

<脅威と影響>

ビジネスメール詐欺は、国内外の取引先や自社の役員等を装ったメールで、企業の出納担当者を騙して、攻撃者が用意した口座へ送金させる詐欺である。騙すためにメール本文では、取引先や経営者を名乗り、通常の見分けづらいような内容にする。また、メールアドレスは取引先のメールアドレスを模したメールアドレスや本物のメールアドレスを使う。

受信者は偽のメールを本物のメールとして取り扱ってしまう。その結果、重要な情報を攻撃者に渡してしまったり、攻撃者が用意した口座に送金してしまったりする。

ビジネスメール詐欺は組織間での取引を装うため1回あたりの金銭被害が高額になる傾向があり、組織にとって被害に遭った際の影響が大きい。

<攻撃手口>

◆ 取引先との請求書の偽装

取引先と請求に係るやりとりをメールで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやりとりや関係している従業員の情報をなんらかの方法により入手した上で攻撃を行なっている。

◆ 経営者等へのなりすまし

企業の経営者等になりすまし、従業員に攻撃者の用意した口座へ振り込ませる。このとき、攻撃者は事前に入手した経営者や関係している従業員の情報を利用し、通常の社内メールであるかのように偽装する。

◆ 窃取メールアカウントの悪用

従業員のメールアカウントを乗っ取った上で、その従業員の取引実績のある企業の担当者へ偽の請求書等を送り付け、攻撃者の用意した口座に振り込ませる。メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気づきにくい。

◆ 社外の権威ある第三者へのなりすまし

弁護士など社外の権威ある第三者へなりすまし、企業の財務担当者等に対して、攻撃者の用意した口座へ振り込ませる。

◆ 詐欺の準備行為と思われる情報の窃取

詐欺を実行する前の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が詐欺の標的とする企業の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、企業内の他の従業員の個人情報等を窃取する。

<事例または傾向>

◆ ビジネスメール詐欺容疑、日本で逮捕者 マフィア関与か

海外企業の会社代表のメールアドレスを乗っ取り、同社の口座があるスイスの銀行へメールし、約1億1千万円を日本国内の信用金庫へ振り込ませた。警視庁は、詐欺と組織犯罪処罰法違反(犯罪収益隠匿)の容疑で日本人2人を逮捕した。¹

◆ 「新規取引」において「振込口座が偽か否かの確認を難しくさせる」手口

IPAのサイバー情報共有イニシアティブ(J-CSIP)が運用状況レポートでBECの手口を解説している。

この手口は、標的企業が新規取引先とやり取りしているところに攻撃者が介入して、偽口座を記載した見積書を「差し替え」と称して送付し、本物の見積書の破棄を依頼するものである。見積金額の変更という趣旨の偽メールで見積書の差し替えを依頼しつつも、書類上は振込口座も変更しており、振込先が偽口座に変わったことの発覚を難しくさせていた。²

<対策/対応>

組織

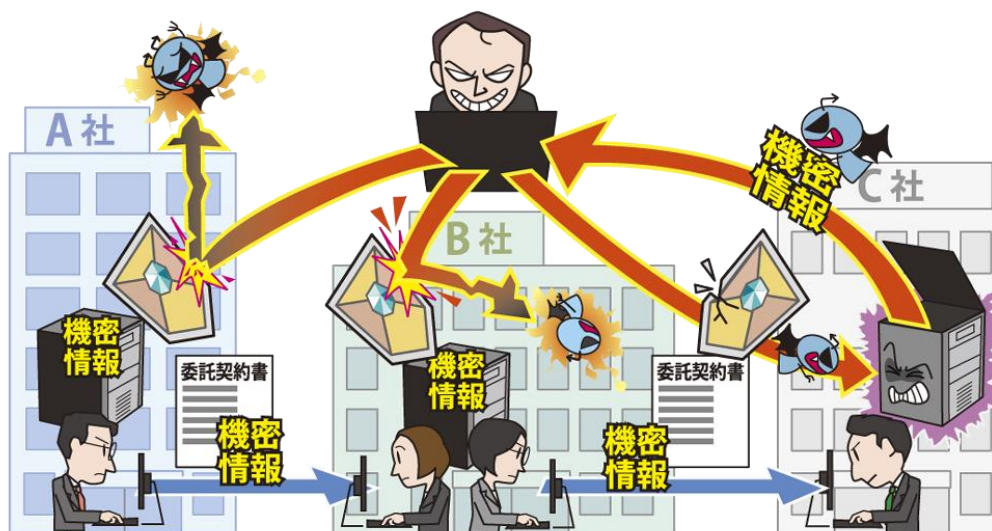
- 被害の予防(被害に備えた対策含む)
 - ・ガバナンスが機能する業務フローの構築
個人の判断や命令で取引や金銭の移動がされないルールやシステムの構築。
 - ・メールに電子署名を付与(S/MIME)
取引先との間で請求書等の重要情報をメールで取り扱う場合、S/MIMEによる電子署名の付与がなりすまし防止対策として有効である。
 - ・表1.3「情報セキュリティ対策の基本」を実施
<メールの真正性の確認>
 - ・メール以外の方法で事実確認
振込先の口座変更等がある場合、電話やFAX等の方法で取引先に確認する。また、口座の名義等を金融機関に確認する。
 - ・普段とは異なるメールに注意
普段とは異なる言い回しや、表現の誤り、送信元のメールアドレスに注意する。
 - ・判断を急がせるメールに注意
至急の対応を要求する等、担当者に真偽の判断時間を与えないようにする手口も考えられる。真偽を確認するフローを策定しておく。
<メールアカウントの適切な管理>
ビジネスメール詐欺では、攻撃や被害に遭う前に、何らかの方法でメールが盗み見られている場合があるため、パスワードの適切な管理やログイン通知機能等で不正ログイン対策を行う。
- 被害を受けた後の対応
 - ・CSIRTへの連絡
 - ・警察に相談
 - ・踏み台や詐称されている組織への連絡
 - ・影響調査および原因の追究、対策の強化

参考資料

1. ビジネスメール詐欺容疑、日本で逮捕者 マフィア関与か
<https://www.asahi.com/articles/ASM3W7529M3WUTIL06D.html>
2. サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2019年4月~6月]
<https://www.ipa.go.jp/files/000076713.pdf>

4位 サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～



原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組織群をサプライチェーンと呼ぶ。また、組織が特定の業務を外部組織に委託している場合、この外部組織もサプライチェーンの一環となる。業務委託先組織がセキュリティ対策を適切に実施していないと、業務委託元組織への攻撃の足がかりとして狙われる。昨今、業務委託先組織が攻撃され、預けていた個人情報などが漏えいする等の被害が発生している。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 組織(委託元組織、委託先組織)

発が行われないと、脆弱性を内在したソフトウェアが納品され、ソフトウェア利用者が脆弱性を突いた攻撃を受ける。

これらの攻撃で被害を受けた場合、サービス利用者への賠償対応や、組織の信用の失墜により業務継続が困難になるおそれがある。

<脅威と影響>

組織におけるウェブサイトの運営や情報システムの導入が当たり前になり、多くの組織で運用されている。しかし、ウェブサイトや情報システムの運用には設備や人材が必要であり、外部の業者に委託することもある。このような環境において、委託元組織からのガバナンスが効かない委託先組織がセキュリティ対策を適切に実施していないと、そこを攻撃者に狙われ、被害が発生する。

例えば、委託先組織に個人情報等の重要情報を扱うウェブサイトの運用管理を委託している場合、委託先が不正アクセスを受けることで、その情報が漏えいするおそれがある。また、ソフトウェア開発を委託している場合、セキュリティに配慮した開

<要因>

◆ 委託先組織のセキュリティ対策不足

サプライチェーン内にセキュリティ対策を適切に実施していない委託先組織がある。攻撃者はその弱点に対して攻撃を行い、そこから連鎖して委託元組織に被害がおよぶ。

◆ 委託先組織を適切に選定、管理していない

委託元組織が委託先組織を選定するにあたり、セキュリティ対策の実施状況等の確認を怠ると、セキュリティ対策が不十分な組織に委託することがある。また、委託後も委託先の状況を管理せずにいると、委託先組織のセキュリティ対策が不十分なままとなり、攻撃者からの攻撃を受ける。

◆ 再委託先や再々委託先の管理が難しい

委託先組織の先に再委託先組織や再々委託先組織がある場合、その管理は委託先組織が行うため、委託元にとってのセキュリティ対策管理は更に難しくなる。

<事例または傾向>

◆ 再委託先の開発環境への不正アクセスによるデータ消失

2019年11月、日本スポーツ協会の新システム開発の委託先である電通の再委託先であるスポーツITソリューションが不正なアクセスを受け、動作検証用に構築したサーバー内のデータベースからデータを削除された。開発環境のセキュリティ設定に不備があったことが原因とされている。

削除されたデータは、新システムのテスト用に加工した国体参加者データおよび公認スポーツ指導者データであり、姓名・性別・生年月日などが含まれている。

日本スポーツ協会は、データの抜き取り、流出、公開の事実は確認できていないとしている。¹

◆ IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査報告書を公開(IPA)

2019年4月、IPAは「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書を公開した。

報告書によると、IT業務委託契約の契約関連文書において、委託元の約8割が「新たな脅威が顕在化した際の対応」について責任範囲の明記をしておらず、その理由は「専門知識・スキルが不足している」が最多の79.6%であった。

責任範囲を明確にするには、契約関連文書の見直し、委託元、委託先にとっても有効であるとされている²

<対策/対応>

組織(委託元組織)

- 被害の予防
 - ・業務委託や情報管理における規則の徹底
製造においては原材料や部品の調達経路、物流経路等も考慮する。
 - ・信頼できる委託先組織の選定
委託先組織の信頼性評価や委託先への品質基準を導入する。
 - ・委託先からの納品物の検証
 - ・契約内容の確認

委託元組織と委託先組織の情報セキュリティ上の責任範囲を明確化し合意を得る。また、賠償に関する取り決めに契約に含める。

- 委託先組織の管理

委託元組織が責任をもって委託先組織のセキュリティ対策状況の実態を定期的に確認することが重要である。

- 被害を受けた後の対応
 - ・影響調査および原因の追究、対策の強化
 - ・被害への補償

組織(委託先組織)

- 被害の予防
 - ・セキュリティの認証取得
ISMS、Pマーク、SOC2など
- 被害を受けた後の対応
 - ・委託元への連絡

組織(委託先/委託元組織共通)

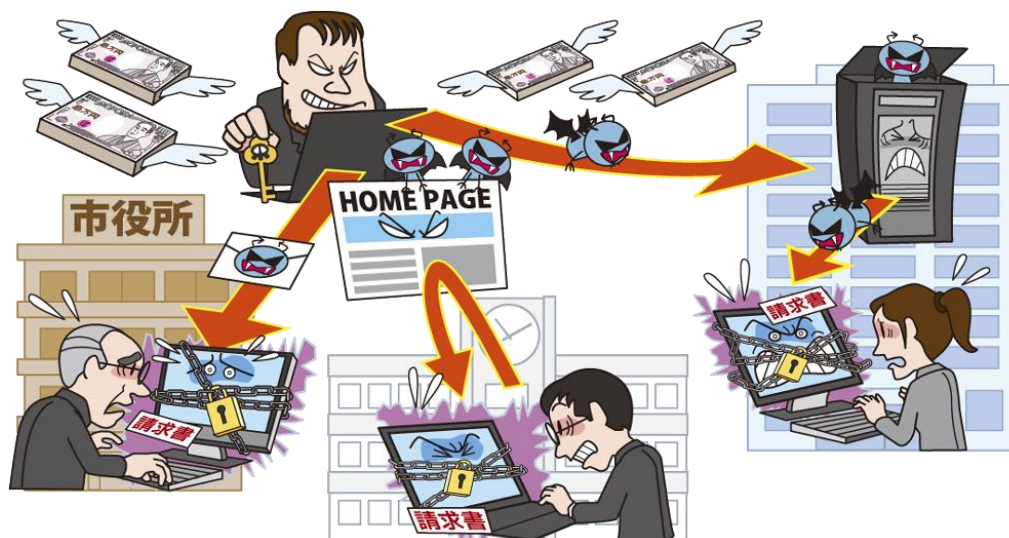
- 被害の予防
 - ・公的機関が公開しているガイドラインの活用
-「サイバーセキュリティ経営ガイドライン」³
(経済産業省/IPA)
 - 「中小企業の情報セキュリティ対策ガイドライン」⁴(IPA)

参考資料

1. 国民体育大会参加者データおよび公認スポーツ指導者データの消失について
<https://www.japan-sports.or.jp/news/tabid92.html?itemid=4065>
2. 「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について
<https://www.ipa.go.jp/security/fy30/reports/scrm/index.html>
3. 「サイバーセキュリティ経営ガイドライン」Ver2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
4. 「中小企業の情報セキュリティ対策ガイドライン」
<https://www.ipa.go.jp/files/000055520.pdf>

5位 ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～



ファイルの暗号化や画面ロック等を行うランサムウェアに感染し、PC(サーバー含む)やスマートフォンに保存されているファイルを利用できない状態にされ、復旧と引き換えに金銭を要求される被害が発生している。不特定多数に対して行う攻撃だけではなく、特定の国や組織を狙う標的型攻撃に近い攻撃も行われる。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 組織

<脅威と影響>

PC やスマートフォンの利用に制限を掛け、制限を解除するために金銭を支払え等の脅迫文を表示するランサムウェアと呼ばれるウイルスの感染が引き続き確認されている。メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用されたりすることでランサムウェアに感染する。

最近では、企業内のシステムに不正アクセスし、ファイルサーバー等から情報を盗み出した後、さらにファイルを暗号化し、ファイルの復元や窃取した情報を公開しないことと引き換えに、金銭を要求する手口が増えている。暗号化および窃取されたファイルが顧客情報や基幹システムのファイル等、組織にとって重要な情報であった場合は、業務の遂行に大きな支障が出たり、組織の信用の失墜や経済的損失につながったりするおそれがある。

組織は事業継続のために、復旧する保証も公開されない保証もないが、攻撃者の脅迫に従い金銭を支払うか否かの判断が求められる。

<攻撃手口>

◆ メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

◆ ウェブサイトから感染させる

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんしたウェブサイトや攻撃者が用意したウェブサイトを開覧させることで、ランサムウェアに感染させる。

◆ 脆弱性を悪用し、ネットワーク経由で感染させる

ソフトウェアの脆弱性が未対策のままインターネットに接続されている PC に対して、その脆弱性を悪用してインターネット経由でランサムウェアに感染させる。

◆ 公開サーバーに不正アクセスして感染させる

外部公開しているサーバーにリモートデスクトップ(RDP)等で不正ログインしランサムウェアに感

染させる。

<事例と傾向>

◆ 市立高等学校のサーバーがランサムウェアに感染、英文の脅迫ドキュメントが表示される

2019年10月、川崎市立橘高等学校が利用している校内ネットワークサーバーがランサムウェアに感染した。同校職員がネットワークサーバーにアクセスすると、Wordドキュメントが暗号化されており、画面上には感染を示唆する英文の脅迫ドキュメントが表示された。この感染により、生徒が作成した成果物等のデータが使用できなくなった。調査や二次感染防止のため、校内ネットワークでのPCの利用を禁じた。感染の原因は特定されていない。¹

◆ 日本を標的としたランサムウェア攻撃

ESETによると、2019年1月、「Love you」スパムメール攻撃が日本に標的を絞って行われ、ランサムウェア「Gandcrab」等に感染させようとしていたことが報告されている。件名には日本の女性芸能人名が使われていた。特に1月29日は攻撃の95%が日本で検出され、また、何万もの悪意のあるメールが毎時間検出されたとしている。²

◆ 脆弱性を悪用するランサムウェア「Sodin」

カスペルスキーより、Windowsの特権昇格の脆弱性(CVE-2018-8453)を悪用して感染させるランサムウェア「Sodin(別名:Sodinokibi、REvil)」が日本やドイツ、韓国、台湾、香港等で拡散したことが報告されている。³感染するとファイルが暗号化された上で任意の拡張子が設定され、利用できなくなる。PCのデスクトップには攻撃者のメッセージが表示され、金銭の支払い方法を記したテキストファイルを参照するよう誘導される。

<対策/対応>

組織(経営者層)

- 組織としての体制の確立
 - ・対策の予算の確保と継続的な対策の実施

組織(システム管理者、従業員)

- 被害の予防(BCM含む)
 - ・迅速かつ継続的に対応できる体制(CSIRT等)の構築
 - ・表1.3「情報セキュリティ対策の基本」を実施
 - ・受信メールやウェブサイトの十分な確認
 - ・添付ファイルやリンクを安易にクリックしない
 - ・不審なソフトウェアを実行しない
 - ・サポートの切れたOSの利用停止、移行
 - ・フィルタリングツール(メール、ウェブ)の活用
 - ・ネットワーク分離
 - ・共有サーバー等へのアクセス権の最小化
 - ・バックアップの取得

バックアップデータが暗号化されることを防ぐため、バックアップに使用する記録媒体はバックアップするときのみPCやサーバーに接続する。また、バックアップするデータ量が膨大な場合は、大規模バックアップに対応した外部サービス等を活用する。なお、バックアップから復旧できることを定期的を確認しておくことも重要である。

- 被害を受けた後の対応
 - ・CSIRTへの連絡
 - ・バックアップによる復旧
 - ・復号ツールの活用⁴
 - ・影響調査および原因の追究、対策の強化

<例外措置>

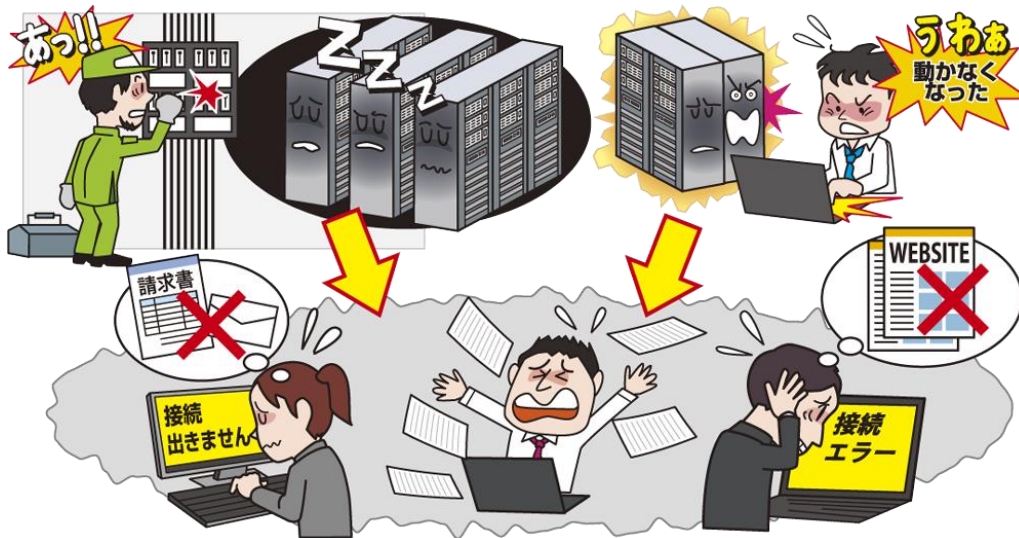
推奨はされないが、人命に関わるファイルが暗号化された場合に、金銭を支払ったケースもある。

参考資料

1. 市立高校の校内サーバがランサムウェアに感染(川崎市)
<http://www.city.kawasaki.jp/templates/press/cmsfiles/contents/0000111/111987/20191101houdou.pdf>
2. 「Love you(ラブ・ユー)」マルウェア、日本を標的にした大規模な攻撃を展開
<https://www.eset.com/jp/blog/welivesecurity/love-you-malware-makeover-massive-japan-targeted-campaign/>
3. ランサムウェア「Sodin」が日独韓台に感染集中--カスペルスキー
<https://japan.zdnet.com/article/35139470/>
4. The No More Ransom Project
<https://www.nomoreransom.org/>

6位 予期せぬ IT 基盤の障害に伴う業務停止

～ それは予告もなしに突然やってくる ～



組織がインターネット上のサービスや業務システム等で使用しているネットワークやクラウドサービス、データセンター設備等の IT 基盤に予期せぬ障害が発生し、長時間にわたり利用者や従業員に対するサービスを提供できなくなるケースがある。IT 基盤の停止は利用している組織の事業の妨げとなり、ビジネスに大きな影響を与えるおそれがある。

<当事者>

- 企業 (IT 基盤提供事業者)
- 組織 (組織内 IT 基盤設備)

<被害者>

- 個人 (IT システム利用者)
- 組織 (IT システム利用者、IT 基盤利用者)

<脅威と影響>

企業や民間団体、官公庁等多くの組織は費用面や運用負担の軽減のため、自社の機器をデータセンターに設置する場合や、クラウドの IT 基盤を利用するケースがある。利用している IT 基盤で、自然災害、データセンターの設備故障や停電、ハードウェア・ソフトウェア障害等により、予期しない障害が発生すると、IT 基盤を利用して外部に提供しているサービスや社内の業務システムが突然停止する。

それにより、組織が提供しているサービスの利用者がそのサービスを利用できなくなったり、組織の業務が停止したりする。長時間停止した場合、組織の利益減少や競争力の弱体化等、経済的損

失につながる。また、人々の日常生活にも支障が出るおそれがある。

<発生要因>

◆ 自然災害

地震や台風、洪水等の自然現象により、IT 基盤の設備や施設が被害を受け、IT 基盤に障害が発生する。

◆ 作業事故

インフラ設備のメンテナンス作業中の人為的ミスにより通信回線断や電力供給断等の事故が発生し、IT 基盤に障害が発生する。

◆ 設備障害

データセンター等、様々なサービスが稼働している施設において、空調設備等の制御システムの障害により、施設内にある機器の稼働環境 (温度や湿度等の条件) を維持できなくなり機器が停止し、IT 基盤に障害が発生する。

◆ ハードウェア・ソフトウェア障害

IT 基盤を構成する機器のハードウェアに障害が発生したり、OS やソフトウェアに不具合が発生したりすることにより、IT 基盤に障害が発生する。

＜事例または傾向＞

◆ データセンターの電源障害により約 260 社の顧客システムが停止

2019 年 11 月、QTnet が提供するデータセンターにおいて、電源設備の更新作業中に事故が発生し、電源停止(7 秒間)が起きた。その間、データセンターを利用している顧客のサーバー類の電源供給が失われ、楽天カード、福岡県庁、九州電力含む約 260 社の顧客のシステムが利用できなくなった。¹ 楽天カードでは、数日間クレジットカードやスマホ決済など消費者向けのサービスに影響が及んだ。²

◆ 自治体向け IaaS サービスにシステム障害

2019 年 12 月に日本電子計算の提供する自治体専用 IaaS サービス「Jip-Base」について障害が発生し、Jip-Base を利用する全国約 50 の自治体が影響を受けた。影響を受けた自治体では住民向けの窓口サービスや自治体の業務システムに支障が出た。復旧には時間を要し、2020 年 1 月 10 日時点の報告では全 1,318 の仮想 OS のうち、98.1%が IaaS サービスとして復旧を終えたとしている。^{3,4}

◆ 米アマゾン ウェブ サービスの大規模障害

2019 年 8 月、アマゾンのクラウドサービスである Amazon Web Services(AWS)に障害が発生した。障害が発生したのは東京に 4カ所ある AWS を提供するデータセンターのうち 1 つで、空調設備の管理システム障害により、サーバーがオーバーヒートを引き起こしてサーバーの電源が停止した。それに伴い AWS が提供する EC2 サーバーが停止

し、NTT ドコモ、PayPay、ユニクロ等の決済サービスや EC サイト含む国内の様々なサービスに影響が及んだ。⁵

◆ 台風 15 号による ATM 障害

2019 年 9 月、じぶん銀行は、ネットワーク障害により、ATM での取引ができなくなった。原因は台風 15 号により千葉県内の複数の電話局が停電し、連携している外部の決済サービスに通信が繋がらなかったためとしている。⁶

＜対策/対応＞

組織(サービス提供者)

● 被害の予防(被害に備えた対策を含む)

- ・BCM の実践(BCP 策定と運用)⁷

IT 基盤の様々なトラブルを事前に想定し、対応策を準備しておく。また、事業の継続や早期復旧を可能にするため、行動計画や復旧目標を定め、事業継続計画(BCP)を策定し、運用する。

- ・可用性の確保と維持(システム設計や監視)
システムの冗長化についても検討する。
- ・データバックアップ(復旧対策)
- ・契約や SLA 等を確認

組織は IT 基盤側との契約や SLA 等を確認しておく。IT 基盤を利用して顧客にサービスを提供する場合は、顧客との契約や SLA 等も確認しておく。

- ・被害を想定し IT 基盤側との事前の連携確認

● 被害を受けた後の対応

- ・BCP に従った対応

参考資料

1. データセンターの電源障害による停止について(障害お知らせ)
<https://www.qtnet.co.jp/info/2019/20191126.html>
2. 【完全復旧】お客様向けサービス復旧のお知らせ(株式会社QTnetの電源設備更新作業に伴う不具合)
<https://www.rakuten-card.co.jp/info/news/20191123/>
3. 「Jip-Base」の障害における復旧状況のご報告(第3報)
<https://www.jip.co.jp/news/20200110/>
4. 全国約50の自治体でWeb/電子行政サービスがダウン、自治体専用IaaS「Jip-Base」でシステム障害
<https://it.impressbm.co.jp/articles/-/18969>
5. AWS 東京リージョンで発生した大規模障害についてまとめてみた
<https://piyolog.hatenadiary.jp/entry/2019/08/23/174801>
6. じぶん銀行のATM障害が復旧、原因は台風15号による電話局の停電
<https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05945/>
7. 事業継続計画策定ガイドライン
https://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyokeizokuKeikakuSakuteiGuideline.pdf

7位 不注意による情報漏えい

～ついつい、が重大インシデントに～



組織や企業において、情報管理体制の不備や情報リテラシー不足等が原因となり、従業員が個人情報や機密情報を漏えいしてしまう事例が 2019 年も多く見られた。漏えいした情報が悪用される二次被害が発生するおそれもあるため、十分な対策が求められる。

<当事者(情報を漏えいさせた側)>

- 組織(従業員)

<被害者(情報を漏えいされた側)>

- 個人(当事者のサービス利用者等)
- 組織(当事者の取引先企業等)
- 組織(当事者自身)

<脅威と影響>

組織や企業は、個人情報や機密情報を取り扱うことがある。しかし、これらの重要情報を扱うことに対する職員や従業員の意識の低さや、体調不良等による集中力の低下により、意図せず情報漏えいしてしまうことがある。

漏えいした情報が悪用され二次被害に繋がるおそれがある他、情報漏えいを起こした組織や企業は社会的信用の失墜、経済的損失といった影響を受ける。

<要因>

◆ 従業員のセキュリティ意識の低さ

個人情報や機密情報を取り扱う従業員のセキュリティ意識が低いと、不用意な扱いをして情報漏え

いしてしまう。例えば、規則に従った手続きをしても、不注意により、そのカバンを外出先で紛失することがある。また、メールアドレスを確認した上でメールを送信したとしても、TO/CC/BCC の設定を間違えれば、メールアドレスの漏えいとなる。

◆ 情報を取り扱う際の本人の状況

体調不良や多忙等、情報を取り扱う従業員が置かれた状況から注意力散漫になり、重要資料の置き忘れやメールの誤送信等の情報漏えい事故を起こしてしまう。

◆ 組織規程および確認プロセスの不備

組織における重要情報の定義・取り扱い規程・持ち出し許可手順や作業時の確認プロセスに不備があると、規則に従っていたとしても重要情報の扱いが不適切となり、情報漏えいが起こりかねない。

<不注意による情報漏えい例>

- メール誤送信(宛先間違い、TO/CC/BCC の設定間違い、添付ファイル間違い等)
- 不適切なウェブ公開(重要情報への対処が不十分なまま公開)
- 重要情報を保存した情報端末(PC やスマート

- フォン等)・記録媒体(USB メモリー等)の紛失
- 重要書類(紙媒体)の紛失

<事例または傾向>

◆ 顧客の個人情報が保存された PC を紛失

2019年8月30日、複数の飲食店を運営するゼットンの従業員が、同社が運営する店舗に予約をした顧客の個人情報が保存された PC を、帰宅途中に立ち寄った店に置き忘れて紛失した。PC には顧客の氏名や企業名、電話番号が最大6万7,280件含まれ、そのうち最大1万475件にはメールアドレスも含まれていた。

同社では紛失が判明した後、遠隔操作で PC のログインパスワードを複雑化した上で同社へのアクセスを遮断する対応を取り、警察へ届け出た。¹

◆ BCC を TO に誤りメールアドレス流出

2019年1月18日、特許庁が実施する説明会の参加申込者のメールアドレス849件が、業務請負先であるオーエムシーから流出した。説明会のリマインドメールを送信する際、BCC 欄に入れるべき参加申込者のメールアドレスを誤って TO 欄に入れたことで、メールを受信した参加申込者が他の参加申込者のメールアドレスを見られる状態にあった。同庁は、メールを送信した申込者全員へ速やかな謝罪と当該メールの削除を依頼するようオーエムシーに指示し、今後は管理を徹底していくとしている。²

◆ 顧客情報を含む資料をネット上に誤公開

横浜農業協同組合は、顧客情報が記載された資料が2019年10月1日から12月13日までインターネット上で公開されていたことを明らかにした。資料には同組合に貯金したことがある顧客1万7,286人分の氏名や住所等の個人情報が記載されており、特定の操作により閲覧出来る状態であ

った。同組合によると、原因はウェブサイト更新作業中の操作を誤ったためと報告している。^{3,4}

<対策/対応>

組織

- 情報リテラシーや情報モラルの向上
 - ・従業員のセキュリティ意識教育
 - ・組織規程および確認プロセスの確立
 - 特定の担当者への業務集中が発生しないような体制の構築も重要である。
- 被害の予防(被害に備えた対策含む)
 - ・確認プロセスに基づく運用
 - ・情報の保護(暗号化、認証)
 - ・外部に持ち出す情報や端末の制限
 - 外部との適切なファイル送受信の運用を検討する(クラウドストレージ利用、暗号化など)
 - ・メール誤送信対策等の導入
 - ・業務用携帯端末の紛失対策機能の有効化
- 被害の早期検知
 - ・問題発生時の内部報告体制の整備
 - ・外部からの連絡窓口の設置
- 被害を受けた後の対応
 - ・被害拡大や二次被害要因の排除
 - ウェブサイトへの誤った情報公開の場合、非公開にする。また、検索サイト等への情報削除依頼を行う。
 - ・漏えいした内容や発生原因等の公表
 - ・関係者、関係機関への連絡
 - 監督官庁、個人情報保護委員会等

個人/組織(被害者)

- 被害を受けた後の対応
 - ・漏えいが発生した組織からの情報に従う
 - パスワードの変更、クレジットカードの再発行等

参考資料

1. ノートパソコン遺失による個人情報漏洩の可能性に関するお詫びとお知らせ
http://www.zetton.co.jp/company/IR/docs/ir_20190906.pdf
2. 特許庁の請負事業における個人情報の流出について
<https://www.meti.go.jp/press/2018/01/20190123005/20190123005.html>
3. 貯金者情報1.7万件含む資料をネット上に誤公開 - JA横浜
<http://www.security-next.com/110769>
4. 【重要】顧客情報流出に関するお詫びとお知らせ
https://ja-yokohama.or.jp/oshirase/20200221_01

8位 インターネット上のサービスからの個人情報の窃取

～他人事ではないウェブサイトの脆弱性～



ショッピングサイト(EC サイト)等のインターネット上のサービスへ脆弱性等を悪用した不正アクセスや不正ログインが行われ、サービスに登録している個人情報等の重要な情報を窃取される被害が発生している。窃取された情報を悪用されるとクレジットカードの不正利用等の二次被害につながる。

<攻撃者>

- 犯罪グループ
- 犯罪者

<被害者>

- 個人(インターネット上のサービス利用者)
- 組織(インターネット上のサービス利用者)

<脅威と影響>

インターネット上のサービスでは、利用者の識別やサービスの提供のため、個人情報の登録が必要である場合が多く、特に EC サイトではクレジットカード情報の登録も求められる場合がある。

インターネット上のサービスの利用には様々な個人情報の登録が必要であるが、全てのウェブサイトが常に適切に管理されているわけではなく、脆弱性が内在したまま運営されており、重要な情報が漏えいしてしまう場合がある。

インターネット上のサービスに脆弱性が存在すると、攻撃者によって登録してある情報を窃取されたり、不正に利用されたりする等の被害につながる。

また、脆弱性の種類によっては、個人情報の入力フォームを改ざんされ、利用者が入力した情報

が窃取されるといった被害の可能性がある。入力フォームの改ざんの場合、利用者が改ざんに気付くことは極めて困難である。

<攻撃手口>

- ◆ 広く共通的に使われるソフトウェアの脆弱性を悪用

インターネット上のサービスは、OS やミドルウェア等、複数のソフトウェアによって構築されている。これらのソフトウェアは、市販されているものやオープンソースソフトウェア(OSS)等が使用されることが多い。サービスで利用しているソフトウェアの脆弱性が発見されることもあり、それが広く普及しているソフトウェアであった場合は攻撃者に狙われやすく、発見された脆弱性を狙った攻撃が急速に拡大するおそれがある。

- ◆ 開発時に作りこんだウェブアプリケーションの脆弱性を悪用

インターネット上のサービスを構築する際、市販のソフトウェアや OSS のみでは構築が不可能な場合は、独自にウェブアプリケーションの開発をする場合がある。開発したウェブアプリケーションの脆

脆弱性検査等のセキュリティ対策が不十分な場合、脆弱性を作りこんでしまう場合があり、攻撃者に狙われるおそれがある。

例えば、ウェブアプリケーションが使用するデータベースを外部から不正に操作できる SQL インジェクションの脆弱性が作りこまれてしまった場合、データベースに登録された個人情報等の重要な情報が窃取されるおそれがある。

◆ 他のサービス等から入手した認証情報を悪用

他のサービス等から入手した認証情報（ID とパスワード）等を使い、サービスの利用者になりすまして不正ログインを行い、その利用者の権限でアクセスできる個人情報等の重要な情報を窃取する。

なお、不正ログインの攻撃手口については個人 8 位「インターネットサービスへの不正ログイン」を参照。

<事例または傾向>

◆ ファイル転送サービスへの不正アクセス

2019 年 1 月、オージス総研より、ファイル転送サービス「宅ふぁいる便」に対する不正アクセスがあり、480 万件以上の個人情報が漏洩したことが報告された。この被害についてのプレスリリースによれば、サーバーの脆弱性が悪用されたことで、個人情報が流出したとされている。¹

当該サービスについては、脆弱性の修正のためには大規模な改修が必要となるため、サービス終了が決定したことが告知されている。²

◆ 決済用モジュールの改ざんによる漏えい被害

掃除用品の通販サイトに不正アクセスがあったことが、2019 年 9 月に報告された。この被害では、通販サイトの脆弱性が悪用され、決済モジュールが改ざんされたことにより、顧客 34 人分のクレジットカード情報が漏洩したとされている。³

<対策/対応>

組織（インターネットサービス運営者など）

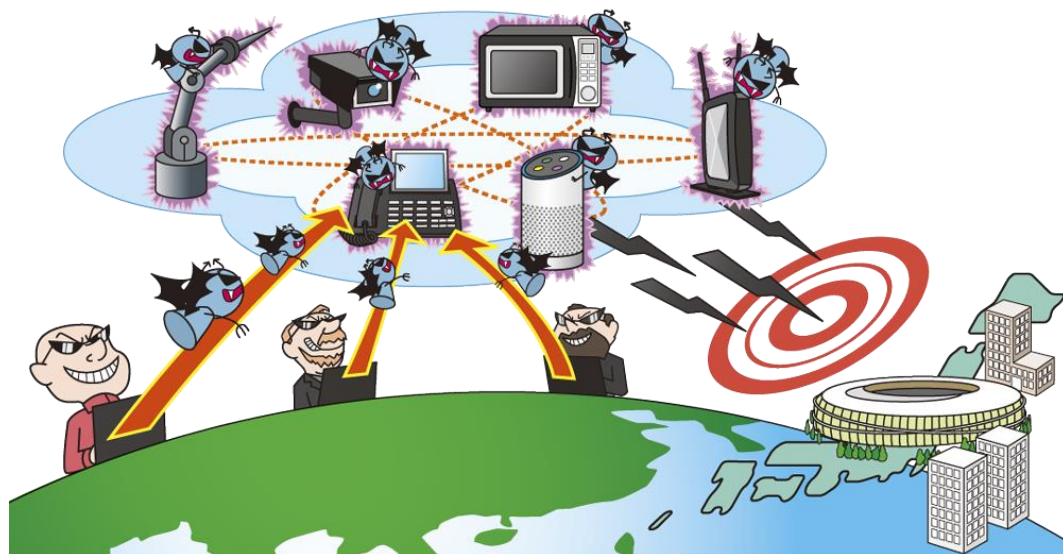
- 被害の予防
 - ・表 1.3「情報セキュリティ対策の基本」を実施
 - ・セキュリティ対策の予算・体制の確保
 - システムの導入時や保守作業時の十分な予算と体制を確保する必要がある。
 - ・セキュアなインターネット上のサービス構築
 - ・セキュア開発ライフサイクルの実践
 - ・セキュリティバイデザインの実施⁴
 - ・セキュリティ診断（ウェブアプリケーション診断、プラットフォーム診断等）の実施
 - システムの導入時や改修時に実施する。
 - また、改修がなくても定期的に診断を実施し、改善する。
 - ・WAF、IDS/IPS の導入
 - 導入後も対策情報（設定等）を定期的に更新する保守業務があることを想定すること。
 - ・利用者に対するセキュリティ機能の提供
 - 二要素認証やログイン履歴、購入履歴を確認できる機能等を提供する。
 - ・ミドルウェアやライブラリ利用状況の把握
 - コンポーネント管理表等の作成推進
- 被害の早期検知
 - ・適切なログの取得と継続的な監視
- 被害を受けた後の対応
 - ・CSIRT への連絡
 - ・セキュリティ専門企業への調査依頼
 - ・影響調査及び原因の追究、対策の強化
 - ・情報漏えいの被害者に対するすみやかな連絡と補償
 - ・漏えいした内容や発生原因等の公表
 - ・関係者、関係機関への連絡
 - 監督官庁、個人情報保護委員会、警察等

参考資料

1. 「宅ふぁいる便」サービスにおける不正アクセスについて ～お客さま情報の漏洩について（お詫びとご報告）～
<https://www.filesend.to/news20190314.html>
2. 「宅ふぁいる便」サービス終了のお知らせ（2020年1月14日）
<https://www.filesend.to/>
3. 弊社が運営する「掃除用品オンラインショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ
https://clean-shop.ec-cube.shop/user_data/news2019
4. 情報セキュリティを企画・設計段階から確保するための方策(SBD(Security by Design))
https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf

9位 IoT 機器の不正利用

～IoT 機器の普及に伴い脆弱性を悪用する攻撃が多様化、開発ベンダーは対策が急務～



ウイルスに感染させた IoT 機器を踏み台として、サービスやネットワーク、サーバーに悪影響を与える大規模な DDoS(分散型サービス妨害) 攻撃の被害が確認されている。今後も普及拡大することが予想される IoT 機器は、セキュリティ対策が必要な対象として認識しなければならない。

<攻撃者>

- 犯罪グループ
- 犯罪者(産業スパイ、愉快犯、離職者等)
- 他国家(諜報員等)

<被害者>

- 個人(IoT 機器利用者)
- 組織(企業、IoT 機器利用者)

<脅威と影響>

急速な普及を続けている IoT 機器は、「情報家電」「オフィス機器」「自動車・輸送機器」「医療機器」「産業機器」等、様々な分野において今後も高成長が見込まれている。一方、IoT 機器のメーカーは IoT 機器のリスク検討が不十分なまま製品を開発し、脆弱性を作り込んでしまうことがある。そのような IoT 機器は、インターネット越しに脆弱性を悪用されてしまう。

脆弱性を悪用されると、IoT 機器がウイルスに感染させられ、DDoS 攻撃の踏み台にされたり、搭載されている機能を不正利用されたり等の被害に遭うおそれがある。また、攻撃対象の IoT 機器が、

「産業機器」や「自動車・輸送機器」等であった場合、制御対象の誤動作、機能不全がもたらす被害は甚大になる場合がありうる。

一方、IoT 機器の利用者も、「IoT 機器を使っている」という認識や「IoT 機器はインターネットにつながっている」という意識が薄く、セキュリティパッチの適用等による IoT 機器の脆弱性対策を行っていないケースがあり、被害を拡大してしまっている。

<攻撃手口>

◆ 脆弱性を悪用した攻撃

脆弱性を悪用して、インターネット経由で IoT 機器に不正アクセスしたり、ウイルスに感染させたりする。IoT 機器がウイルスに感染後、インターネットに公開されているウェブサイト、サーバー等に DDoS 攻撃を行ったり、IoT 機器に搭載されている機能を不正利用したりする。

◆ ウイルスの感染を拡大させる

ウイルスに感染した IoT 機器は、同じ脆弱性を持つ IoT 機器がインターネット上にないかを探索する。存在した場合、その IoT 機器もウイルスに感染させ、次々と感染範囲を拡大させる。

<事例または傾向>

◆ Mirai ボットの特徴を有するアクセスの増加について

警察庁のインターネット定点観測において 2019 年 6 月中旬より Mirai の特徴を持つウイルスに感染した端末によるものと推測される宛先ポート 5500/TCP および 60001/TCP に対するアクセスの増加が観測された。ウイルスに感染した海外製デジタルビデオレコーダや Wi-Fi ストレージ製品等の脆弱性を悪用し、ウイルスの感染拡大を狙ったものと考えられる。¹

◆ 総務省、電気通信事業法に基づく端末機器の基準認証に関するガイドライン公開

総務省は、「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第 1 版)」(案)を公開した。IoT 機器の技術基準にセキュリティ対策を追加するため、端末設備等規則の一部を改正(2020 年 4 月 1 日施行)する。IoT 機器のメーカーやサービス提供者は今後「端末設備等規則」に準じたセキュリティ対策が求められる。²

◆ 「NOTICE」情報通信研究機構(NICT)は、脆弱な IoT 機器について調査結果を発表

2019 年度 第 3 四半期において、参加協力 ISP 41 社、調査対象 IP アドレス約 1.1 億の内 ID・パスワードが入力可能であったのが約 111,000 件で、ID・パスワードによりログイン可能であったのが 1,328 件であった。また、ウイルスに感染した IoT 機器の 1 日当たりの検知数は、少ない時は 60 件、多い時で 598 件であったとしている。³

<対策/対応>

組織(IoT 機器の開発者)

- 被害の予防
 - ・セキュア開発ライフサイクルの実践

- ・セキュリティバイデザインの実施⁴
- ・初期パスワード変更の強制化
- ・脆弱性の解消(セキュア・プログラミング、脆弱性検査、ソースコード検査、ファジング等)
- ・ソフトウェア更新の自動化
- ・分かりやすい取扱説明書の作成
- ・迅速なセキュリティパッチの提供
- ・利用者にとって不要な機能の無効化
- ・アクセス範囲の制限
- ・セキュリティに配慮したデフォルト設定
- ・利用者への適切な管理の呼びかけ
 - 利用者へマニュアルやウェブページ等で適切な管理を呼びかける。
- ・ソフトウェアサポート期間の明確化
 - 利用者にソフトウェアサポートの期間を伝え、サポートが切れた状態での利用について注意を促す。

組織(システム管理者・利用者)、個人

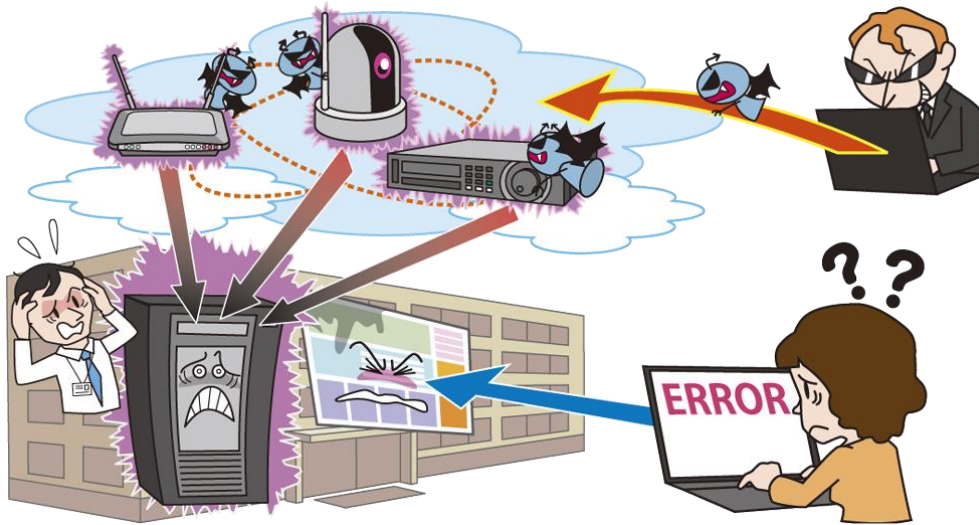
- 情報リテラシーの向上
 - ・使用前に説明書を確認
- 被害の予防
 - ・セキュリティパッチが公開されたら迅速に更新(自動更新機能を有効にする)
 - ・廃棄時は初期化
 - 廃棄時は初期化し廃棄業者等に出す場合、データ消去や秘密保持に関する契約をする。
 - ・機器の管理画面や管理ポートに対する適切なアクセス制限
 - ・不要なサービスの停止(ポートを閉じる)
- 被害を受けた後の対応
 - ・CSIRT への連絡
 - ・IoT 機器の電源オフ
 - ・IoT 機器の初期化後、「被害の予防」を実施
 - ・影響調査および原因の追究、対策の強化

参考資料

- 1.宛先ポート5500/TCP、5555/TCP 及び60001/TCP に対するMirai ボットの特徴を有するアクセスの増加について
<https://www.npa.go.jp/cyberpolice/detect/pdf/20190719.pdf>
- 2.電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)
https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000179.html
- 3.脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況(2019年度第3四半期)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html
- 4.情報セキュリティを企画・設計段階から確保するための方策(SBD(Security by Design))
https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf

10位 サービス妨害攻撃によるサービスの停止

～DDoS 攻撃の被害に遭わないために事前準備を強化する～



攻撃者に乗っ取られた複数の機器から形成されるネットワーク(ボットネット)が踏み台となり、企業や組織が提供しているインターネット上のサービスに対して大量のアクセスを一齐に仕掛け高負荷状態にさせる、もしくは回線帯域の占有によるサービスを利用不能とさせる等の DDoS (分散型サービス妨害)攻撃が行われている。標的とされた組織は、ウェブサイト等のレスポンスの遅延や、機能停止状態となり、サービスの提供に支障が出るおそれがある。

<攻撃者>

- 犯罪グループ
- 犯罪者(愉快犯等)
- ハクティビスト

<被害者>

- 組織
(インターネット上のサービスの運営者)
- 個人
(インターネット上のサービスの運営者)

<脅威と影響>

多くの組織がインターネット上で、ウェブサイト等を運営し、情報発信やサービス提供を行っている。攻撃者は、そうしたウェブサイト等に DDoS 攻撃を仕掛け、ウェブサイトアクセスしづらくすることで主義主張を誇示したり、攻撃の停止と引き換えに金銭を要求したりする。

処理能力を上回る負荷を受けたウェブサイトやサーバーは、閲覧ができなくなったり、レスポンスが遅延したりする等、サービスを正常に保つことが

できなくなるため、機会損失による損害が発生する。

<攻撃手口>

◆ DDoS 攻撃

DDoS 攻撃には、主に以下の手口が使われる。

- ボットネットの利用
IoT 機器等を悪用したボットネットに攻撃命令を出し、標的組織のウェブサイトや利用している DNS サーバー等へ大量のアクセスを行い、高負荷をかける。
- リフレクション(リフレクター)攻撃
送信元の IP アドレスを標的組織のサーバーに偽装して、多数のルーターや DNS サーバー等に問い合わせを送り、その応答を標的組織のサーバーに集中させることで高負荷をかける。DNS リフレクション攻撃や NTP リフレクション攻撃等がある。
- DNS 水責め攻撃
標的組織のドメインにランダムなサブドメイン

を付加して DNS 問い合わせをすることで、標的組織ドメイン名の権威 DNS サーバーに高負荷をかける。悪意のある問い合わせか、通常の問い合わせかの区別が付かないため、根本対策が難しい。

- DDoS 代行サービスの利用
ダークウェブ等で提供している DDoS 代行サービスを利用して攻撃する。専門的な技術や設備がなくても攻撃が行える。

<事例または傾向>

◆ DDoS に悪用される可能性ある機器は国内で約 20 万存在

A10 ネットワークスのレポートによると 2019 年 6 月時点で DDoS 攻撃に悪用されるおそれがあるボット端末およびサーバーは世界で約 1,600 万、国内で約 20 万存在すると報告されている。¹

◆ マンション向けプロバイダーで通信障害

エフビットコミュニケーションズが提供するマンション居住者向けのインターネット接続サービス「ファイバービット」では、2019 年 10 月 2 日から 21 日にかけて DDoS 攻撃を受け、一部マンションにて断続的に通信の異常が発生した。攻撃元からの通信を拒否する等の対処を行っていたが、時間経過とともに攻撃元の IP アドレスが変化し、通信障害が長期化する結果となった。同社は再発防止に向けて、共有部設置機器の順次交換や攻撃自体への対策も継続して行うとしている。²

◆ DDoS 攻撃脅迫メールで、仮想通貨を要求

ドイツのセキュリティベンダは、10 月中旬以降、複数の組織を対象に、DDoS 攻撃を示唆して仮想通貨を要求する脅迫メールが送付されていると観測しており、注意喚起を行っている。攻撃手法は DNS、NTP、CLDAP を使用したリフレクション攻

撃等を使っている。JPCERT/CC は、日本国内でも同様の事例を確認しており、このようなメールを受信しても、要求には応じず、冷静に対応を行うよう注意を促している。³

<対策/対応>

組織(ウェブサイトの運営者)

- 被害の予防
 - ・DDoS 攻撃の影響を緩和する ISP や CDN 等のサービスの利用
 - ・WAF の導入
 - ・システムの冗長化等の軽減策
 - ・ネットワークの冗長化
 - DDoS 攻撃の影響を受けない非常時用ネットワークを事前に準備する。
 - ・ウェブサイト停止時の代替サーバーの用意と告知手段の整備
- 被害を受けた後の対応
 - ・CSIRT への連絡
 - ・通信制御(攻撃元 IP アドレスからの通信をブロック等)
 - ・利用者への状況の告知
 - ・影響調査および原因の追究

組織(サービス事業者)

- 被害の予防
 - ・公開サーバーの設定の見直し(DNS サーバーや NTP サーバー等)
 - ・IoT 機器の脆弱性対策
 - IoT 機器への不正アクセスやウイルス感染でシステムを乗っ取られ、ボットネットとして悪用される。攻撃の踏み台にされないために IoT 機器のセキュリティ対策を強化する必要がある。⁴

参考資料

1. 日本国内にDDoS攻撃に悪用される可能性のあるボット/サーバーは約20万存在
<https://www.a10networks.co.jp/news/blog/ddos20a10.html>
2. インターネット通信障害のお知らせ
<http://www.fiberbit.net/news/info/2091/>
3. DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて
<https://www.jpCERT.or.jp/news/flash/2019103001.html>
4. 「IoT開発におけるセキュリティ設計の手引き」を公開
<https://www.ipa.go.jp/security/iot/iotguide.html>

10 大脅威選考会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	窪田 敏明	(株)神戸デジタル・ラボ
菅原 尚志	アクセンチュア(株)	宮崎 清隆	国際マネジメントシステム認証機構(株)
中嶋 美貴	アクセンチュア(株)	萩原 健太	(社)コンピュータソフトウェア協会
石井 彰	旭化成(株)	福森 大喜	(株)サイバーディフェンス研究所
岡田 良太郎	(株)アスタリスク・リサーチ	荒川 大	(一社)サイバーリスク情報センター
徳丸 浩	EG セキュアソリューションズ(株)	宮内 伸崇	(株)サイト
安西 真人	(株)エーアイセキュリティラボ	興石 隆	(社)JPCERT コーディネーションセンター
佐藤 直之	SCSK(株)	福本 郁哉	(社)JPCERT コーディネーションセンター
鈴木 寛明	SCSK(株)	唐沢 勇輔	Japan Digital Design(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	大久保 隆夫	情報セキュリティ大学院大学
小林 克巳	NRI セキュアテクノロジーズ(株)	東 恵寿	NPO セカンドワーク協会
芳賀 夢久	NRI セキュアテクノロジーズ(株)	金城 夏樹	(株)セキュアイノベーション
杉井 俊也	NEC フィールディング(株)	栗田 智明	(株)セキュアイノベーション
真鍋 太郎	NTT コミュニケーションズ(株)	鉢嶺 光	(株)セキュアイノベーション
北河 拓士	NTT コム ソリューションズ(株)	阿部 実洋	(株)セキュアベース
斯波 彰	NTT コム ソリューションズ(株)	薩摩 晴美	(一社)セキュリティ対策推進協議会
小林 義徳	(株)NTT データ	林 達也	(一社)セキュリティ対策推進協議会
宮本 久仁男	(株)NTT データ	持田 啓司	(一社)セキュリティ対策推進協議会
矢竹 清一郎	(株)NTT データ	澤永 敏郎	ソースネクスト(株)
池田 和生	NTTデータ先端技術(株)	勝海 直人	(株)ソニー・インタラクティブエンタテインメント
植草 祐則	NTTデータ先端技術(株)	坂本 高史	(株)ソニー・インタラクティブエンタテインメント
楯 研人	エムオーテックス(株)	相馬 基邦	(株)ソニー・インタラクティブエンタテインメント
徳毛 博幸	エムオーテックス(株)	中西 基裕	ソフトバンク(株)
間嶋 英之	エムオーテックス(株)	小島 博行	地方公共団体情報システム機構
池田 耕作	(株)オーグス総研	金城 賀真	地方公共団体情報システム機構
岡村 耕二	九州大学	鈴木 一弘	地方公共団体情報システム機構
小関 直樹	京セラコミュニケーションシステム(株)	田中 卓朗	TIS(株)
佐藤 宏昭	京セラコミュニケーションシステム(株)	三木 基司	TIS(株)
西山 健太	京セラコミュニケーションシステム(株)	大谷 毅典	DXC テクノロジー・ジャパン(株)
高崎 庸一	グローバルセキュリティエキスパート(株)	前田 隆行	DXC テクノロジー・ジャパン(株)
三木 剛	グローバルセキュリティエキスパート(株)	黒岩 亮	(株)ディー・エヌ・エー
武藤 耕也	グローバルセキュリティエキスパート(株)	松本 隆	(株)ディー・エヌ・エー
遠藤 誠	(株)ケイテック	安永 貴之	(株)ディー・エヌ・エー
新井 哲	KDDI デジタルセキュリティ(株)	内山 巧	(株)電算
岩瀬 巧	KDDI デジタルセキュリティ(株)	坂 明	(公財)東京オリンピック・パラリンピック競技大会組織委員会
町田 則文	KDDI デジタルセキュリティ(株)	石川 朝久	東京海上ホールディングス(株)
小熊 慶一郎	(株)KBIZ / (ISC)2	小島 健司	(株)東芝
保村 啓太	KPMG コンサルティング(株)	田岡 聡	(株)東芝
飯島 憂	(株)神戸デジタル・ラボ	大浪 大介	東芝インフォメーションシステムズ(株)
梅津 直弥	(株)神戸デジタル・ラボ	原田 博久	(株)Doctor Web Pacific

氏名	所属	氏名	所属
大山 水帆	戸田市役所	荒井 大輔	(株)Bridge
今 佑輔	トレンドマイクロ(株)	柳川 俊一	(株)Bridge
加藤 雅彦	長崎県立大学	今野 俊一	Broadcom Inc.
須川 賢洋	新潟大学	林 聡	Broadcom Inc.
猪股 秀樹	日本アイ・ピー・エム(株)	山内 正	Broadcom Inc.
上村 理	日本アイ・ピー・エム(株)	島田 敏宏	(株)ベリサーブ
山下 慶子	日本アイ・ピー・エム(株)	樫山 清	(株)ベリサーブ
初見 卓也	(一財)日本情報経済社会推進協会	太田 良典	弁護士ドットコム(株)
磯田 弘司	日本電気(株)	垣内 由梨香	マイクロソフトコーポレーション
谷川 哲司	日本電気(株)	増田 博史	マイクロソフトコーポレーション
淵上 真一	日本電気(株)	山室 太平	マカフィー(株)
住本 順一	日本電信電話(株)	小屋 晋吾	(株)豆蔵ホールディングス
中島 周摩	NortonLifeLock Inc.	高江洲 勲	三井物産セキュアディレクション(株)
古谷 尋	NortonLifeLock Inc.	東内 裕二	三井物産セキュアディレクション(株)
常川 直樹	パナソニック(株)	山谷 晶英	三井物産セキュアディレクション(株)
渡辺 久晃	パナソニック(株)	村野 正泰	(株)三菱総合研究所
林 薫	パロアルトネットワークス(株)	古澤 一憲	(株)三菱総合研究所
浜田 譲治	PwC コンサルティング合同会社	平田 真由美	みゅーらぼ
岩佐 功	東日本電信電話(株)	石井 崇喜	(株)ユービーセキュア
齊藤 純一郎	東日本電信電話(株)	関根 鉄平	(株)ユービーセキュア
水越 一郎	東日本電信電話(株)	八幡 美希	(株)ユービーセキュア
折田 彰	(株)日立システムズ	島田 理枝	(株)ユビテック
寺田 真敏	(株)日立製作所	松田 和宏	(株)ユビテック
古賀 洋一郎	ビッグロブ(株)	福本 佳成	楽天(株)
山口 裕也	(株)ファイブドライブ	橘 喜胤	楽天ウォレット(株)
大高 利夫	藤沢市役所	山崎 圭吾	(株)ラック
原 和宏	富士通(株)	若居 和直	(株)ラック
原田 弘和	富士通(株)	有森 貞和	(株)両備システムズ
綿口 吉郎	富士通(株)	清水 秀一郎	
坂本 拓也	(株)富士通研究所	piyokango	

著作・制作	独立行政法人情報処理推進機構(IPA)		
編集責任	土屋 正		
イラスト制作	株式会社 創樹		
執筆協力者	10 大脅威選考会		
10 大脅威執筆者	土屋 正 亀山 友彦 吉本 賢樹 熊谷 悠平 阿部 未歩	辻 宏郷 渡邊 祥樹 宇梶 宏美 佐々木 敬幸	黒谷 欣史 大友 更紗 田村 智和 佐藤 輝夫
IPA 執筆協力者	瓜生 和久 松坂 志	桑名 利幸 加賀谷 伸一郎	渡辺 貴仁

情報セキュリティ 10 大脅威 2020

各脅威の解説資料

2020 年 2 月 27 日	初 版
2020 年 3 月 10 日	第二版
2020 年 3 月 12 日	第三版
2020 年 3 月 19 日	第四版
2020 年 4 月 2 日	第五版
2021 年 5 月 26 日	第六版

[事務局・発行]

独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

<https://www.ipa.go.jp/>