水団連定例講演会

令和４年7月26日(火)14時～

Ｗｅｂ講演会

講　演　「サイバー犯罪、サイバー攻撃の現状等について」

講　師　神奈川県警察本部生活安全部 サイバー犯罪捜査課

課長補佐　卯野　智喜　　講師

広　報　資　料
令和４年４月７日
警　　察　　庁

令和３年におけるサイバー空間をめぐる脅威の情勢等について

１　情勢概況

デジタル化の進展等に伴い、サイバー空間の公共空間化が加速する中、ランサムウェアによる被害が拡大し、市民生活に大きな影響を及ぼす事案も確認されているほか、不正アクセスによる情報流出や、サイバー攻撃事案への国家レベルの関与も明らかとなるなど、サイバー空間における脅威は極めて深刻な情勢が続いている。

２　サイバー空間の脅威情勢

○　ランサムウェアによる被害が拡大。国内の医療機関が標的となり、市民生活にまで重大な影響を及ぼす事案も確認。

○　Ｇ７各国の法執行機関等が参加する「ランサムウェアに関するＧ７高級実務者会合」が開催されるなど、世界各国において、ランサムウェア被害の防止に向けた諸対策が喫緊の課題。

○　警察庁が国内で検知したサイバー空間における探索行為等とみられるアクセスの件数は引き続き増加。大半が海外からのものであり、海外からの脅威が引き続き高まっている。

○　国内の政府機関等が外部からの不正アクセスを受け、職員の個人情報等が窃取された可能性のある事案が相次いで確認されたほか、サイバー攻撃事案の実態解明を推進する中で、国家レベルの関与が明らかとなった事例も確認。

３　警察における取組

○　サイバー事案への対処能力を強化し、諸外国と連携した脅威への対処を推進するなどの観点から、令和４年４月に警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を設置。

○　サイバー攻撃事案に関する各種捜査により、中国人民解放軍が我が国に対する各種情報収集を実行している可能性が高いことが判明。

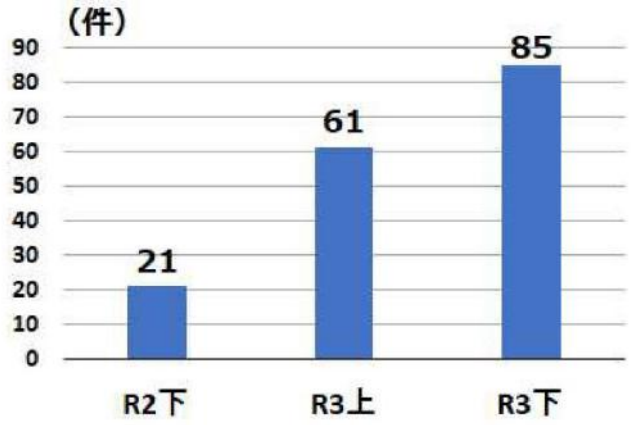
○　サイバー攻撃集団「APT40」に関し、内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携した事業者等に対する注意喚起等を実施。

○　東京オリンピック・パラリンピック競技大会について、官民が一体となったサイバー攻撃対策を実施。結果として、大会の運営に影響を及ぼすようなサイバー攻撃の発生はなかった。

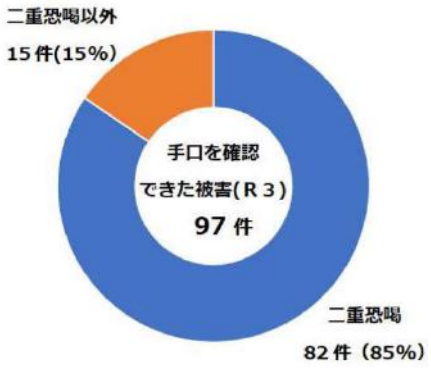
企業・団体等におけるランサムウェア被害

出典元：警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について」
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf）

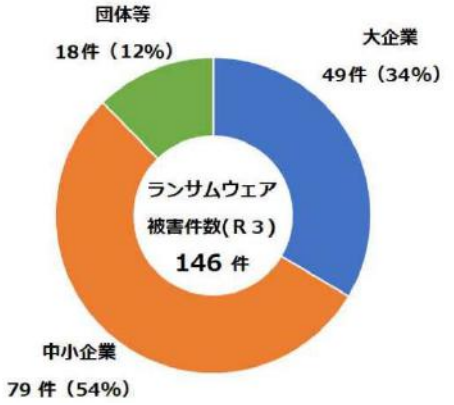
【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



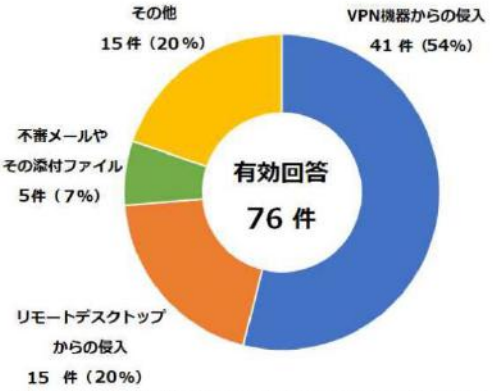
【図表２：ランサムウェア被害の手口別報告件数】



【図表４：ランサムウェア被害の被害企業・団体等の規模別報告件数



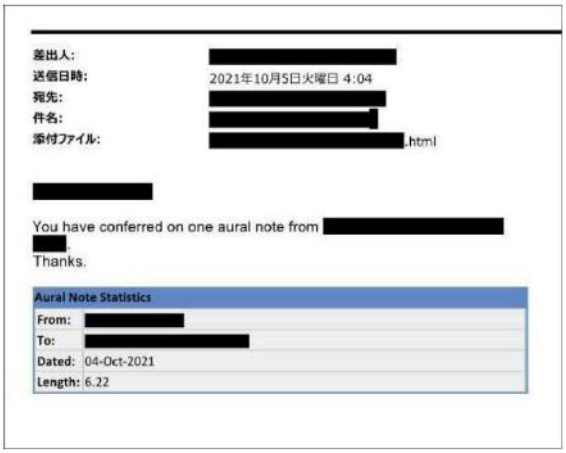
【図表７：感染経路】



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100%にならない。

半導体の製造業者に対する標的型メール攻撃

【図表22：メール文面】



【図表23：遷移後の画面】

偽（ニセ）ショッピングサイト だまされないための 7つのポイント

1 ブラウザのアドレス欄で、サイトのＵＲＬ（アドレス）などを確認

偽ショッピングサイトで見かけるURLの特徴

URLによく使われる文字列の例
「.xyz」「.online」「.fun」「.asia」「.shop」「.icu」「.top」
※これらの文字列があるからとすべてが、偽サイトという事ではありません。
正規のサイトで利用されている場合もあります。

2 相場と比べて価格が安すぎないかを確認

「掲載商品すべてが値引き」「入手困難な商品の在庫が豊富」なときは**要注意**です

3 不自然な日本語表記などがないかを確認

機械翻訳をしたような不自然な日本語表記のときには**要注意**です

不自然な表記の例

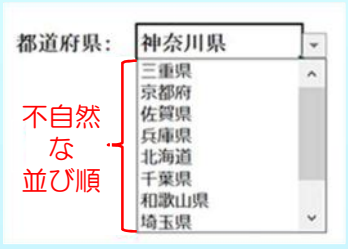
- 「三日か５日届きます」
- 振込終、超早い配達
- 休業日：365天受付

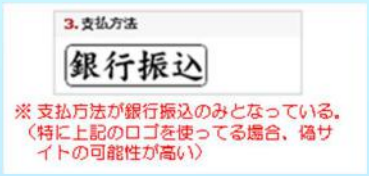
4 会社概要欄の記載を確認

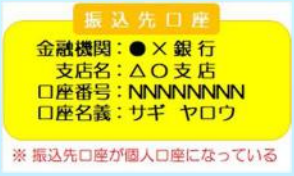
特に注意すべき点

- 電話番号が国際電話番号表記になっている（「+81-45-XXXX」）
- 電話番号の桁数が足りない（045-211-XXX）←1つ足りない？
- 連絡先にメールアドレスしか掲載されていない
- 連絡先メールアドレスにフリーメールが使われている　など

5 商品購入画面に不審な点がないかを確認







入力項目・都道府県の並び順、支払方法・振込先口座名義人など、**不審な点があります**。

6 振込む前に電話で確認

- 偽ショッピングサイトで騙されないためには、商品代金を振り込む前に**電話で確認する**ことが一番確実な対策です。
- 偽サイトの場合、**「他人」「別の会社」につながったり**、電話番号の桁数が足りずにつながらないことがあります。

7 セキュリティ対策ソフトを活用

ウイルス対策ソフトや**フィルタリングソフト**などの**セキュリティ対策ソフト**の中には、偽ショッピングサイトにアクセスしようとすると警告表示する機能を備えた製品もあります。

７つのポイントを参考に、あてはまるところがないか確認しましょう。
インターネットショッピング利用時は、購入手続前によく確認することが大切です。
もしも、被害にあってしまった時や悩んだ時は、最寄りの警察署などに相談しましょう。

神奈川県警察ホームページ 注意喚起サイト
『偽ショッピングサイトに注意!!』
https://www.police.pref.kanagawa.jp/mes/mesd7046.htm

神奈川県警察公式YouTubeはこちら

@niftyプロバイダーサービスYouTubeチャンネル
https://nif.life/sev

動画撮影協力：ニフティ株式会社
学校法人岩崎学園　情報科学専門学校

7つのポイントをわかりやすく説明した、こちらの動画もご覧ください。

神奈川県警察・株式会社ノジマ

IPA Technical Watch

2014 年 08 月 29 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：「ウェブサイト改ざんの脅威と対策」を公開
～ 付録のチェックシートで自組織のセキュリティ対策状況を把握し、“ウェブサイト改ざん”防止のために適切な対策を ～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、ウェブサイト改ざんの対策のために組織においてそれぞれの立場で求められる対策をまとめたレポート「ウェブサイト改ざんの脅威と対策」を 2014 年 08 月 29 日から IPA のウェブサイトで公開しました。

近年、ウェブサイト改ざん事故のニュースは後を絶たず、ウェブサイトを保有する組織だけでなく、閲覧者にとっても重大な脅威となっています。また、これを受け複数の専門機関等から注意喚起も出されています。

最近のウェブサイトの改ざんは閲覧者にウイルスを感染させるのが目的で、閲覧者にはウェブサイトの改ざんの有無を見た目で判別することができません。ウェブサイト改ざんの中でも、今後特に懸念されるのは標的として狙った組織が閲覧しそうなウェブサイトを改ざんし、その組織の閲覧者にウイルスを感染させる、“水飲み場型攻撃”です。これは標的型攻撃におけるウイルス感染の手口の 1 つで、標的とした組織に侵入するための足掛かりとして、今後主流になると考えられています。

そこで、本テクニカルウォッチでは、4 つのウェブサイト改ざんの手口（図 1：A、B、C、D）に対して、ウェブサイトの構築・運営者がどの工程でどのような対策を行うべきかを整理し、解説しています。また、自組織がどこまでウェブサイトのセキュリティ対策を行っているかの現状を確認し、抱える問題とリスクを認識できるチェックリストを作成しました（表 1）。例えば、経営者層に対してセキュリティ対策に必要な予算や体制を上申する上で、付録のチェックリストを利用して、現状抱えるリスクについて具体的に説明するといった活用が可能となります。

攻撃者によりウェブサイトが改ざんされ、閲覧者に被害が及んだ場合、原因究明、対策および復旧作業、信頼回復にむけた社会的な説明など、様々な対応が求められます。ウェブサイト改ざん被害が後を絶たない昨今、組織一丸となってウェブサイト改ざんの影響とその責任を認識し、「明日は我が身」という危機意識を持って対策に取り組んでいく必要があります。

本書が、組織における安全なウェブサイトの効果的な開発と運用の一助になることを期待しています。

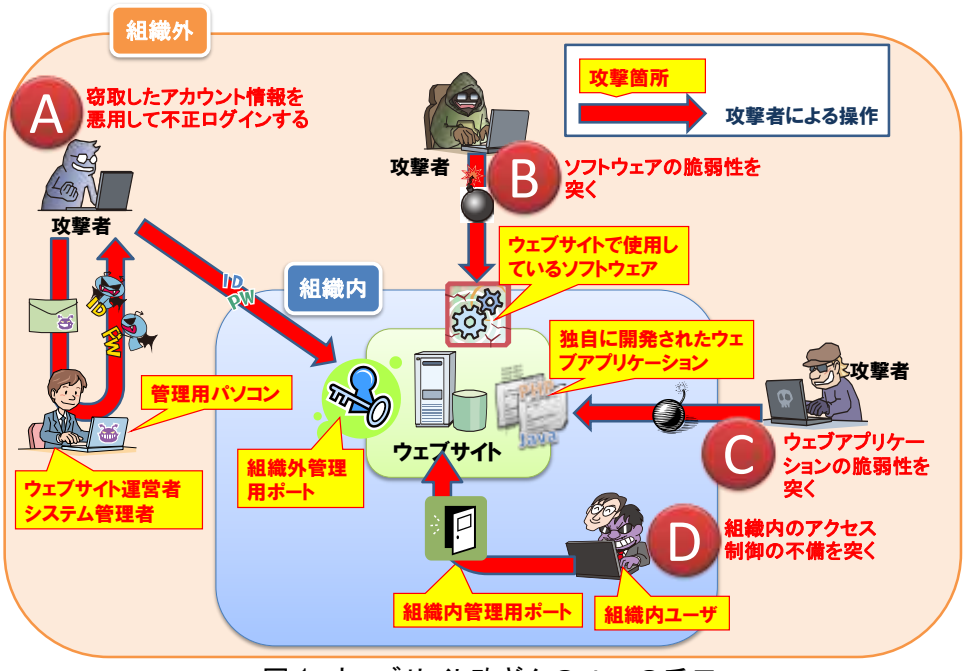


図 1 ウェブサイト改ざんの 4 つの手口

.付録：ウェブサイトセキュリティ対策状況チェックリスト

経営者層			
No	工程	概要	チェック項目
1	基本方針	セキュリティの基本方針の策定	□ セキュリティの基本方針を策定している。 □ 上記方針を職員に周知徹底している。
2	基本方針	管理体制の整備と実施策の策定	□ セキュリティ推進の体制を整備している。 □ セキュリティ推進のための手順や判断基準を策定している。
3	基本方針	セキュリティ対策の予算確保	□ セキュリティ対策に必要な予算の評価・分析を実施している。 □ 対策が必要な脅威に対する予算が確保されている。
システム管理者			
No	工程	概要	チェック項目
1	要件定義	組織外からのウェブサイト管理システムへの安全なアクセス	□ ファイアウォールによる IP アドレス制限などによりウェブサイト管理システムへのアクセスを制限している。 □ 二要素認証やワンタイムパスワードを使用している。 □ VPN 通信により通信内容を暗号化している。
2	設計	組織内の適切なアクセス制限	□ ウェブサイト管理システムへのアクセスを専用ネットワークからのみ許可している。 □ 上記が困難な場合は、二要素認証やワンタイムパスワードを導入している。
3	設計	組織外からの攻撃検知・防御	□ ウェブサイトへの攻撃を検知・防御するために、IDS、IPS、WAF を導入している。(※1)

表１　ウェブサイトセキュリティ対策状況チェックリスト（抜粋）

■本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター　関口／亀山
Tel:03-5978-7527　Fax:03-5978-7518　E-mail:vuln-inq@ipa.go.jp

サイバーセキュリティ経営ガイドライン・概要

Ⅰ．サイバーセキュリティは経営問題

○ 企業の IT の利活用は、業務の効率化による企業の収益性向上だけでなく、グローバルな競争をする上で根幹をなす企業として必須の条件となっている。さらに、IoT といった新たな価値を生み出す技術が普及しつつある中で、AI やビッグデータなども活用した、新しい製品やサービスを創造し、企業価値や国際競争力を持ったビジネスを構築していくことが企業として求められている。

○ サイバー攻撃は年々高度化、巧妙化してきており、サイバー攻撃によって純利益の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生している。さらには、攻撃の踏み台にされて外部へ攻撃をしてしまうだけでなく、国の安全保障上重要な技術情報の流出、重要インフラにおける供給停止など、国民の社会生活に重大な影響を及ぼす可能性のある攻撃も発生しており、その脅威は増大してきている。

○ 経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる可能性がある。また、国内外に関わらずサプライチェーンのセキュリティ対策の必要性も高まっており、業務を請け負う企業にあっては、国際的なビジネスに影響をもたらす可能性が出てきている。

○ また、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、IT を利活用して企業の収益を生み出す上でも重要な要素となる。**セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要**である。

○ このように、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としての**セキュリティ投資は必要不可欠かつ経営者としての責務である**。

○ 本ガイドラインは、大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたものである。

II. 経営者が認識すべき３原則

経営者は、以下の3原則を認識し、対策を進めることが重要である。

(1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

（経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施すべきである。）

(2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

（自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきである。）

(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

（平時からステークホルダー（顧客や株主など）を含めた関係者にサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。）

（詳細は後述の「２．経営者が認識すべき３原則」を参照）

III. サイバーセキュリティ経営の重要１０項目

経営者は、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に対して以下の重要10項目を指示すべきである。

指示１　：サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示２　：サイバーセキュリティリスク管理体制の構築

指示３　：サイバーセキュリティ対策のための資源（予算、人材等）確保

指示４　：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示５　：サイバーセキュリティリスクに対応するための仕組みの構築

指示６　：サイバーセキュリティ対策における PDCA サイクルの実施

指示７　：インシデント発生時の緊急対応体制の整備

指示８　：インシデントによる被害に備えた復旧体制の整備

指示９　：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

指示１０：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

（詳細は後述の「３．サイバーセキュリティ経営の重要１０項目」を参照）

あなたの会社

セパレート

してますか？

神 奈 川 県 警 察

事業者の皆様へ

誰でもできる！すぐできる！

サイバーセキュリティ対策

セパレート大作戦

～ インターネットバンキングに使うパソコンは　セパレート(分離)！～

会社のパソコンにウイルスを感染させるなどの方法で、
お金を不正に送金させる事件が発生しています！

Check Point!

そこでこんな対策

ウイルス感染のリスクのあるメールやＷｅｂ閲覧を行うパソコンと、インターネットバンキングのパソコンを**セパレート（分離）**をして使いましょう！(感染に強いタブレットなら更にGood!)

インターネットバンキング専用のタブレット

メールやＷｅｂ閲覧を行うパソコン

情報漏えいなどのリスク低減のためにも重要な情報を扱うパソコン等とインターネットを利用するパソコン等を**「セパレート」**することは有効な対策の一つです。

【神奈川県警察ホームページ】http://www.police.pref.kanagawa.jp/
(サイバー犯罪に関する情報は「暮らしの安全情報」内にあります。)

神奈川県警察

そのメール
開く 前に
まず、確かメル!!

コンピュータ・ウイルスは
メールから感染することが多い
ことを知っていますか？

神奈川県企業サイバーセキュリティ対策
官民合同プロジェクト

このプロジェクトは、サイバー空間の安全を守るため、神奈川県内の
企業、団体、学術機関、行政機関が緊密に連携して取り組んでいます。

そのメール 開く 前に まず、確かメル!!

メールに気を付けるだけで、
リスクは大きく低減します。

悪意のあるメールは
「怪しいメール」だけではなく、
「怪しくない巧妙なメール」です。

①文字化けしていませんか？
②差出人のメールアドレスは？
③ 添付ファイルは いつもの形式ですか？

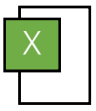
普段のメールと
何が違うの？？

差出人： 山田 太郎 〈tarou@kanagavva-sys.com〉
宛先： 横浜 港一 〈koichi@abc-company.co.jp〉

件名：お見積りの送付

横浜 港一様

いつもお世話になっております。
取り急ぎ、御依頼頂きました¶見積りを
お送りしますので御確認ください。
//
// カナガワ情報システム株式会社
// 第一営業部 山田 太郎 TEL：045-123-4545



見積り.xls

・メールを開く前に
・添付ファイルを開く前に
・ＵＲＬを開く前に

差出人等へ 確認
社内で 相談
確かメル!!

上のメールでは…
①メール本文が文字化けしている。 ➡ 「¶見積り」
②メールアドレスがおかしい。 ➡ 「kanagavva-sys.com」の「w」が「vv」
③添付されているエクセルファイルの形式が古い。 ➡ 最新のエクセルのファイル形式は「.xlsx」

※あくまでも一例です。

神奈川県警察サイバーセキュリティ対策本部

取り組みやすい サイバーセキュリティ対策

メールをきっかけとした
サイバー犯罪のリスク低減に

サイバーセキュリティ啓発動画

YouTubeで配信中

Check

テーマ

「そのメール 開く前に まず、確かメル!!」

https://www.youtube.com/watch?v=T2-KMnmQFsE

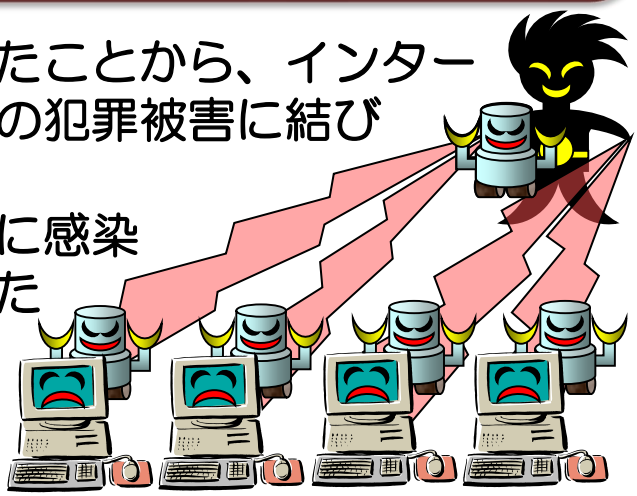
会社で役立つサイバーセキュリティ対策について、事例とともに分かりやすく解説します。

・その他、簡単に取り組めるサイバーセキュリティ対策については、こちらからご覧いただけます。
（テレワークに関する動画の紹介もあります。）
・各種会合や社内教養でもご活用下さい。

神奈川県企業サイバーセキュリティ対策官民合同プロジェクトは、神奈川県内の企業、団体、学術機関、行政機関が緊密に連携して、サイバー空間の安全を守るための取り組みをしています。

神奈川県企業サイバーセキュリティ対策官民合同プロジェクト

コンピュータウイルスなどに注意しましょう！！



パソコンがウイルスなどに感染したことから、インターネットバンキングでの不正送金などの犯罪被害に結び着くことがあります。

また、遠隔操作が可能なウイルスに感染すると、パソコンが犯罪に悪用されたり、官公庁や企業などに対するサイバー攻撃に悪用される危険性もあります。

サイバー犯罪等に巻き込まれないために、大切なパソコンをウイルスなどから守りましょう！

ウイルス感染防止対策

（様々な感染方法があるため、複合的な対策が不可欠です!! ）

1. ウイルス対策ソフトを利用し更新を行いましょう。
2. ＯＳや利用しているプログラムを最新の状態にアップデートしましょう。
3. 信頼のおけないプログラムはインストールしないようにしましょう。
4. 怪しいサイトや必要のないサイトには罠が仕掛けられていることがあるためアクセスしないようにしましょう。
5. メールの添付ファイルは安易に開けないようにしましょう。
6. ＵＳＢメモリなどの外部記憶媒体は必ずウイルスチェックをしましょう。
7. ファイアウォールなどを適切に利用しましょう。
8. 使わないときは電源を切りましょう。

スマートフォンなどにもセキュリティ対策が必要です！！

神奈川県警察サイバー犯罪捜査課
【神奈川県警察ホームページ】https://www.police.pref.kanagawa.jp/
（サイバー犯罪に関する情報は「暮らしの安全情報」内にあります。）

神奈川県警察

キミのスマホは本当に大丈夫！？

インストールする前に、安全なアプリかどうか確認していますか？

ＧＰＳをオンにしたまま、ＳＮＳやブログ等に書き込んでいませんか？

神奈川県警察マスコット
リリポちゃん

セキュリティ対策アプリは利用していますか？

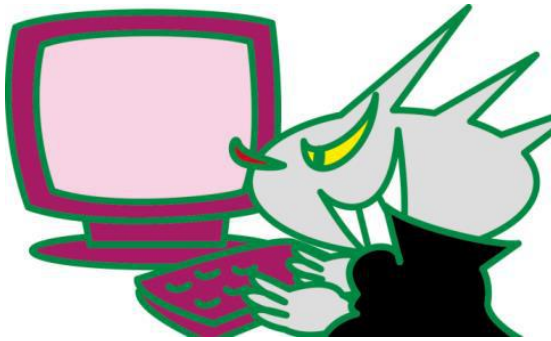
盗難・紛失に備え、セキュリティ(パスコード)ロックを設定していますか？

スマートフォンを安全に安心して利用しよう！

神奈川県警察サイバー犯罪捜査課
【神奈川県警察ホームページ】https://www.police.pref.kanagawa.jp/
（サイバー犯罪に関する情報は「暮らしの安全情報」内にあります。）

神奈川県警察

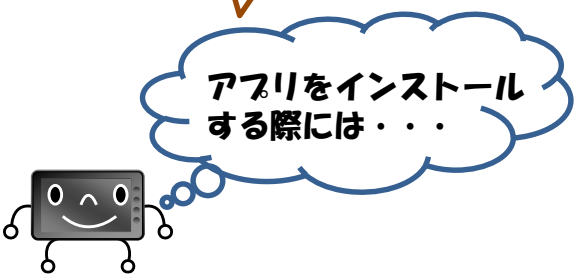
そのアプリ大丈夫！？



不用意にアプリをインストールしたことが個人情報の漏洩などのトラブルにつながることもあります。

例えば・・・

電池を長持ちさせるというアプリをインストールしたところ、スマートフォンの電話番号やメールアドレス等の個人情報を抜き取られてしまった・・・(T_T)

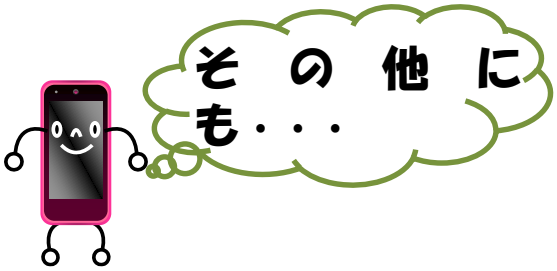


安全なアプリかどうか確認しましょう!!

□　アプリは携帯電話事業者等の信頼できるアプリストアから入手し、「提供元不明のアプリ」はインストールしない

□　インストールする際にアクセス権限を確認し、アプリの機能と関係のないものがないか注意する

また、「面白そうだな」「無料だから」等といった軽い気持ちでインストールせず、本当に必要なのか十分に考えてからインストールしましょう！



・自宅で撮った写真をブログにアップしたところ、知らない人から「△△市に住んでるんだね☺」とコメントされてしまった

・無料お宝ムービー！！" と書かれたサイトを見つけ、動画再生ボタンをクリックしたら、「会員登録されました。○日以内に○万円入金して下さい。」というメッセージが表示された(>_<)

7つのポイント

① 安易にアプリをインストールしない
② セキュリティ対策アプリを利用する
③ 不要な時はＧＰＳ機能をオフにする
④ セキュリティ(パスコード)ロックを設定する
⑤ ＯＳやアプリのアップデートをする
⑥ 不審なサイトにはアクセスしない
⑦ 改造行為(Jailbreak、root化)を行わない

みんなでスマートフォンを安全に利用しよう！！

神奈川県警察のマスコット「ピーガルくん」

神奈川県警察　サイバーセキュリティ対策本部

Cybersecurity Station

サイバー　セキュリティステーション

テーマ　Telework

テレワーク

オフィスを離れ自宅や公共のスペースなど、場所や通勤等にとらわれず働くことを可能にするテレワーク。
テレワークを実施される方は、注意すべきポイントに気を付けて、仕事上の情報漏えい等や自らの端末・機器等を守る意識を高めましょう。

★端末や機器を最新にアップデートしましょう

OSやソフト、アプリ、機器をアップデートしてセキュリティの穴をふさぎましょう。

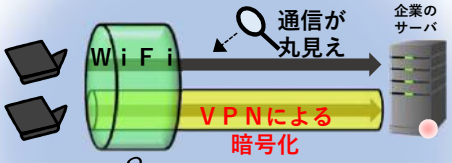
アップデートしておかなければ
受けられなくなるサポートもあるよ

★業務を装うメールや不審なメールに要注意

添付ファイルは安易に開かないように注意しましょう。メールからのリンク先は偽サイトの可能性が。安易にクリックしたり重要情報を入力したりしないようにしましょう。

★実は丸見え!?通信は暗号化して安心

公共の場所での通信は、盗聴されるリスクも高まります。VPN接続して通信路を暗号化しましょう。

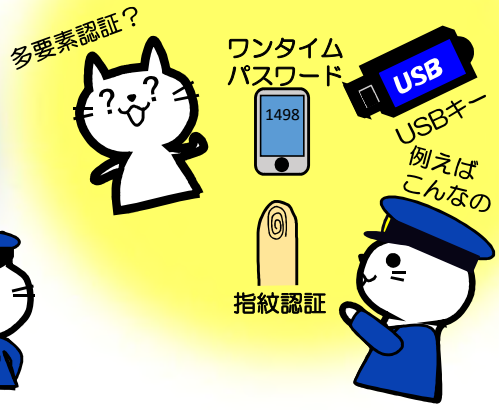


Virtual Private Network

VPNは利用者の機器からインターネット上の安全な場所にある出口サーバまで、すべての通信を暗号化しているんだ。

★複雑なパスワードや多要素認証を使いましょう

お使いになるシステムで用いるパスワードは複雑にし、貴重品のように管理しましょう。



★周りは知らない人だらけ

他者からの盗み見（ショルダーハッキング）や大声での電話会議による情報漏えいに注意しましょう。

★端末の盗難、紛失に要注意

持ち運びしやすいノートPCやスマホ、USBメモリ等は盗難、紛失のリスクも。
万が一に備えてデータは暗号化しましょう。

※このチラシは、内閣サイバーセキュリティセンター（NISC）ホームページから内容を引用、一部改変して作成しています。
NISCのホームページへは右の二次元コードか、https://www.nisc.go.jpからアクセスしてください。

テレワーク実施者の方へ

インターネットの安全・安心ハンドブック

他にも、取り組みやすいサイバーセキュリティ対策があります。
詳しくは神奈川県警察のＨＰで！

誰でもできる！すぐできる！
サイバーセキュリティ対策
セパレート大作戦

会社の
サイバーセキュリティ対策は
できていますか？

サイバーセキュリティ啓発動画

YouTube で配信中

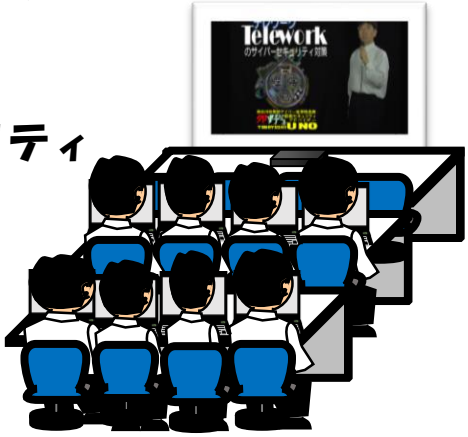
テーマ「テレワークのサイバーセキュリティ対策」

https://youtu.be/yVJfuMR1hNo

Check

会社で役立つサイバーセキュリティ対策について、サイバーセキュリティのスペシャリストがわかりやすく解説します。

- 各種会合や社内教養でもご活用下さい。
- その他、簡単に取り組めるサイバーセキュリティについては、こちらからご覧いただけます。



産 学 官

神奈川県企業サイバーセキュリティ対策官民合同プロジェクト

神奈川県企業サイバーセキュリティ対策官民合同プロジェクトは、神奈川県内の企業、団体、学術機関、行政機関が緊密に連携して、サイバー空間の安全を守るための取り組みをしています。

現実社会と同様にネット社会でも
あなたの財 産（お金や情報）が狙われています

銀行のサービスやショッピングサイトなどのパスワードを簡単なものに設定するということは、家の鍵を開けっぱなしにして外出するようなものです。

インターネットは世界中とつながっているため、いつでも、どこでも、誰でも勝手に入ることができてしまいます。

財産を守るために適切なパスワードを使いましょう

パスワードを使うときには・・・

① 英数字、記号を含めて12文字以上のできる限り長いものにする

② 名前や誕生日、簡単な英単語など推測しやすいものにしない

③ 複数のサービスやサイトで使いまわさない

※ ワンタイムパスワードなどの2段階認証機能も活用しましょう

家もネットもしっかり鍵をかけましょう

神奈川県警察本部サイバー犯罪捜査課
【神奈川県警察のホームページ】https://www.police.pref.kanagawa.jp/
サイバー犯罪に関する情報は「暮らしの安全情報」内にあります。
神奈川県警察
カチッ