あなたの事務所は大丈夫？

神奈川県社会保険労務士会川崎北支部研修会

社労士のための情報セキュリティ対策セミナー

2023/2/7

社会保険労務士事務所フェリシアンス®
特定社会保険労務士
キャリアコンサルタント(CDA)
情報処理推進機構セキュリティプレゼンター
幸せ働き方講師®
神奈川県社労士会所属
堀川眞也

コロナ禍の中で

2020～23年テレワークが一般的に

テレワーク

ネット会議
ウェビナー

窓口閉鎖

ソーシャル
ディスタンス
(移動制限)

リモート面接

リモート
人事評価

2020年4月大企業の電子申請の義務化

https://www.nenkin.go.jp/denshibenri/index.html

我々社労士もITを駆使した業務へ

社労士事務所がIT化を進めることで
関与先へのIT化を支援し関与先の利益に貢献

ZOOMや、Teamsなどのネット会議
労働保険、社会保険の電子申請
スタッフの在宅勤務（リモートワーク）
スタッフの定着、採用のための制度

社労士事務所が使いこなすことで

関与先のIT化の支援で新たなビジネスチャンスを！

社労士のセキュリティレベル…

SRP-II認証事務所への標的型メール訓練結果


「人を大切にする企業」づくりから「人を大切にする社会」の実現へ

月刊社労士 2021 6

Labor and Social Security Attorney

連合会会長選挙　立候補者の公示

巻頭

SRPII認証事務所向け標的型メール訓練に関する報告

社労士のSDGsへの取り組み特設サイトを開設

「在籍型出向」及び「産業雇用安定助成金」に関する解説動画の配信について

2021年2月と3月にSRP-II 認定事務所の訓練希望事務所に標的型訓練メールを配信

開封率はそれぞれ

	2021/6 月刊社労士	2022/4 月刊社労士
事業所割合	41%	⇒24%
人数割合	17%	⇒ 8%

少なくとも2.5件に１件の事務所でウイルスの感染等の被害が…

社労士業界としても見過ごせない事態

●パターンA

項目名	内容
送信者名〈メールアドレス〉	全国社会保険労務士会連合会〈rengoukai@cas-go.jp〉
件名	【ご確認ください】申請手続きについての確認事項
本文	各位 平素より大変お世話になっております。 全国社会保険労務士会連合会です。 業務ご多忙のところ大変お手数ですが、2月10日に貴事務所で行っていただきました顧問先の従業員に関する申請書手続きについて、統計庁から照会事項がございました。 つきましては以下のURLのフォームより内容をご確認いただき、申請状況についてご教示をお願い申し上げます。 http://rengoukai-chosa.cas-go.jp/info/rsm/glvb/xxx
メール形式	URLリンク形式

●パターンB

項目名	内容
送信者名〈メールアドレス〉	全国社会保険労務士会連合会〈rengoukai@safegovernment.net〉
件名	【ご案内】ご自宅のWi-fi環境でのウイルス感染の危険性について
本文	皆様 平素より大変お世話になっております。 全国社会保険労務士会連合会です。 昨今、テレワークでの対応が増えているかと存じます。 ご自宅のWi-fi環境でのウイルス感染の危険性を簡単に測定できるソフトを当連合会でご用意いたしました。 詳細は以下URLでご確認ください。 http://rengoukai-service.safegovernment.net/info/rsm/glvb/xxx
メール形式	URLリンク形式

●パターンC

項目名	内容
送信者名〈メールアドレス〉	全国社会保険労務士会連合会〈rengoukai@a-mail-system-service.com〉
件名	【ご案内】社労士事務所での働き方改革の統計について
本文	各位 平素より大変お世話になっております。 全国社会保険労務士会連合会です。 この度、当会では社労士事務所の働き方改革に関する統計について一般法人ITセキュリティ組合と連携し統計を取りました。 統計結果は以下をご覧いただき、貴事務所での業務にもお役立ていただけますと幸いです。 http://rengoukaiform.mail-system-service.com/info/rsm/glvb/xxx
メール形式	URLリンク形式

本当にあった怖い話

情報漏えいはこんなところから…

・マイナンバーカードのコピーが鍵のない書棚に保管

・まだ、WINDOWS７（8.1）を使用している

・FAXでマイナンバーカードのコピーを送ってもらったら届かなかった

・パソコンの前にパスワードを書いたメモが貼ってある

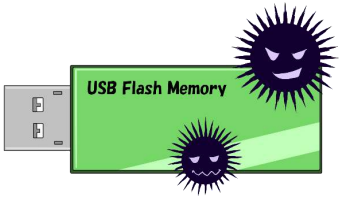
・誰がどのパソコンをもって行ったのかわからない
・業務終了後パソコンが１台足りない

・テレワーク中、カフェのフリーWi-Fiでメールの送受信をした

本当にあった怖い話

情報漏洩はこんなところから…

・家に帰ったら、パソコンが入ったカバンがなかった…



・来客者が事務所のパソコンにUSBメモリーを繋ぎ、ウィルスを移された

・何処かで、顧問先のデータが入ったUSBメモリーをなくしたようだ…

・事務所のパソコンからデータを盗まれた

・あれ～！？スマホがない！

・新幹線で仕事をしていて隣の客に画面を覗かれた

あなたの事務所でデータ漏えいが起きたら…

- たとえば…

パソコンがウイルスに感染！
持ち出したパソコンを紛失！

- **取引先の機密情報が流失！**
- **お客様の個人情報やマイナンバーが流失！**

さてどのようなことが今後起きるでしょうか…？

自己紹介

経済産業大臣認定経営革新等支援機関
社会保険労務士事務所　フェリシアンス®
株式会社　フェリシアンス®

神奈川県社労士会　横浜北支部所属
特定社会保険労務士・キャリアコンサルタント
IPA情報処理機構セキュリティプレゼンター

堀 川　眞 也　https://feliciance-sr.com/

外資系、日系のIT機器メーカー３社で、３２年の会社員を経験をした後、社会保険労務士事務所を開業。
キャリアコンサルタント＋社労士として、「従業員も経営者もずっとハッピー」を目指すコンサルティングや、就労支援のためのセミナーを行っています。

外資系会社員時代、機密情報の保管、保持、パソコンに於ける情報漏えいの防止について厳しい教育訓練を受けた経験から、情報を守るべき現場の立場で、セキュリティについてわかりやすく解説をいたします。

DVD発売中！

すぐに知っておきたい
社労士事務所のセキュリティ対応

社労士のための
情報セキュリティ規程の実務

日本法令様より

内容

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

内容

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

とられて困る情報は持っていない…？？

うちは大事務所じゃないし、取られたところで大したことはない

本当にそうでしょうか？

ビジネス情報

お客様の個人情報

取引先の情報

新製品の機密情報

従業員の個人情報

売上情報

あなたの事務所でデータ漏えいが起きたら…

- たとえば…

パソコンがウイルスに感染！
持ち出したパソコンを紛失！

- **取引先の機密情報が流失！**
- **お客様の個人情報やマイナンバーが流失！**

さてどのようなことが今後起きるでしょうか…？

（例）あなたの事務所でデータ漏えいが起きたら…

顧問先の業務を停止させ損害賠償責任を負うことに
実被害があればさらに大きな責任

マイナンバー漏えい：実被害がなかったとしても…

従業員とその家族のマイナンバーの取り直し
顧問先人事・総務部門での記録変更の作業

本人が役所での手続きのため業務中断
顧問先人事・総務部門での作業人件費が発生

顧問契約の解除・損害賠償
他の顧問先からも顧問契約の解除も

2022年より、個人情報を漏えいさせた事務所に対し報告義務が課せられます

情報を紛失・漏えいすることで被る不利益

情報セキュリティ対策を怠ることで多大な損失のリスクが

(1)金銭の損失

取引先からの損害賠償、不正アクセスによる不正送金など
業務停止による売上の減少

(2)顧客の喪失

管理責任を問われ直接の関与先から契約解除
直接関係のないお客様からも契約解除で全顧客を喪失するリスク

(3)業務の停滞

被害調査、改善実施、復旧まで業務停止
再発の防止、再教育の開始

(4)従業員への影響

スタッフのモラルの低下、復旧作業によるモチベーションの低下
最終的には離職に至る

IPA「2019年度IPA中小企業情報セキュリティ講習能力養成セミナー」より

（例）あなたの事務所でデータ漏えいが起きたら…

顧問先の業務を停止させ損害賠償責任を負うことに
実被害があればさらに大きな責任

マイナンバー漏えいで被害がなかったとしても…

従業員

取り直し

作業

事務所の存続の危機に！！

断

人件費が発生

の解除・損害賠償

顧問先からも顧問契約の解除も

2022年より、個人情報を漏えいさせた事務所に対し報告義務が課せられます

有名な漏えい事件

毎日のように繰り返される情報漏えい
今やすべての経済活動を行う企業・個人は対応が必要

- **ベネッセ　　（3504万件）**
  - 2014年　派遣社員が顧客情報を持出し名簿会社に転売

- **日本年金機構　　（125万件）**
  - 2015年　標的型攻撃メールによるウイルスに感染
  - タイトル「厚生年金基金制度の見直しについて（試案）」
    https://cybersecurity-jp.com/security-incident-case/9146

- **JTB　　（793万件）**
  - 2016年　標的型攻撃メールによるウイルスに感染

https://cybersecurity-jp.com/news

最近の漏えい事件

セキュリティに強いと思われる企業でも発生
毎日のように情報漏えい事件が発生

- **宅ファイル便　　（480万件）⇒ 2020年4月廃業**
  - 2019年1月　ウイルスに感染しメールアドレスとパスワード
- **ホンダ（米国の工場の稼働停止）**
  - 2020年6月　ランサムウエア「EKANS（エカンズ）」に感染
- **SODA「SNKRDUNK(スニーカーダンク)」(275万件)**
  - 2022年6月　不正アクセス・顧客情報流失
- **A市業務委託社員（46万人分）**
  - 2022年6月　業務再々委託先の社員がUSBメモリーを無断で持出を紛失
- **アフラック・チューリッヒ (200万件)**
  - 2023年1月　不正アクセス・顧客情報流失

http://www.security-next.com/category/cat191/cat25
https://cybersecurity-jp.com/news

クリック！毎日のように事故が発生

毎日のように情報漏えいが発生

個人情報漏洩事件・事故関連記事の一覧（1ページ目 / 全457ページ）

2023/01/18 公共料金払込票を紛失、回収袋から落下か - デイリーヤマザキ
2023/01/18 高齢者在宅サービスセンターで携帯電話を一時紛失 - 港区
2023/01/17 医療費助成受給者の個人情報含むファイルを他自治体へ誤送信 - 浦添市
2023/01/17 宮城労働局で相談事案ファイルを一時紛失 - 廃棄準備中に盗難か
2023/01/17 関西電力に新電力の顧客情報が漏洩 - 経産省が報告求める
2023/01/16 研修会申込者1人のメアドを全申込者へ誤送信 - 東京都
2023/01/16 通販サイトでクレカ情報流出、リニューアル前に判明 - 化粧品会社
2023/01/16 調査業務の委託先が個人情報含む資料を紛失 - 国交省
2023/01/16 不正アクセスで顧客情報流出の可能性 - 石油販売会社
2023/01/12 個情委、破産者情報の違法公開サイトを告発
2023/01/12 保険会社2社の業務委託先より顧客データ約200万件が流出
2023/01/12 メール誤送信でマラソン参加者のメアド流出 - 産経新聞
2023/01/11 教委認定講習の論文が所在不明に、郵送過程で - 大阪府
2023/01/11 アンケートフォームで設定ミス、個人情報が閲覧可能に - 守口市
2022/12/26 職員の複数アカウントに不正アクセス - 奈良県立医科大
2022/12/26 日経の記事クリッピングサービスにサイバー攻撃 - 個人情報が流出か
2022/12/23 生徒の個人情報含むUSBメモリを紛失 - 広島大付属福山中高
2022/12/23 業務PCが「Emotet」感染、個人情報が流出 - 保険代理店
2022/12/23 顧客情報含む業務用PCを紛失 - フジテックス

保険会社の関与先からの流失

USBの紛失
Emotet感染PCを紛失

サプライチェーン攻撃事件

サプライチェーン等への攻撃から大企業の業務が停止
下請企業・士業事務所も無防備ではすまされない

- **トヨタ自動車　（操業停止）**
  - 2022年2月　下請部品メーカーがランサムウエアに感染
  - ネットワークを切り離し、復旧までの間受発注が停止
  - トヨタの工場が一時操業停止に追い込まれる

「組織」における情報漏えいの脅威の順位

サプライチェーンを利用した攻撃により
我々社労士事務所もその標的にされる可能性あり！

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

大企業のセキュリティが強固になる中、大企業の情報収集のため、セキュリティが脆弱な中小企業のネットワークに侵入しサプライチェーン網から大企業の情報を盗み取る

企業と契約している社労士も安心できません

IPA「情報セキュリティ10大脅威2022」より
https://www.ipa.go.jp/security/vuln/10threats2022.html

最近のサイバー攻撃事件

サプライチェーン等への攻撃から大企業の業務が停止
下請企業・士業事務所も無防備ではすまされない

大企業

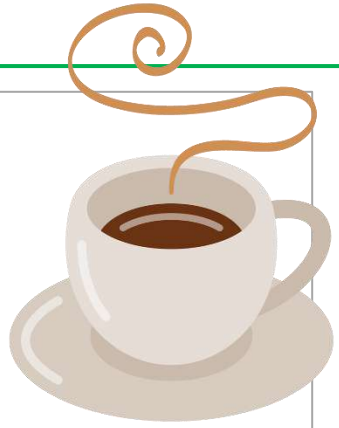
中小企業

社労士事務所

取引関係

顧問契約

コーヒーブレイク　(触れないでおきましょう…(笑))



デジタル庁

ホーム › プレスルーム › 「GビズID」利用者の個人情報の漏えいについて（2022年3月30日）

「GビズID」利用者の個人情報の漏えいについて（2022年3月30日）

デジタル庁が運用する、事業者が行政手続を行う際の共通認証サービス「GビズID」について、個人情報の漏えいが発生いたしました。関係者の方々にご迷惑をお掛けしたことを深くお詫び申し上げます。

「GビズID」利用者の個人情報の漏えいについて、別添のとおりご報告いたします。

- 個人情報の漏えいについて（PDF／385KB）

https://www.e-gov.go.jp/news/2022-03-31t1322240900_752.html

コーヒーブレイク　(触れないでおきましょう…(笑))

デジタル庁

ホーム › プレスルーム

「Gビズ
について

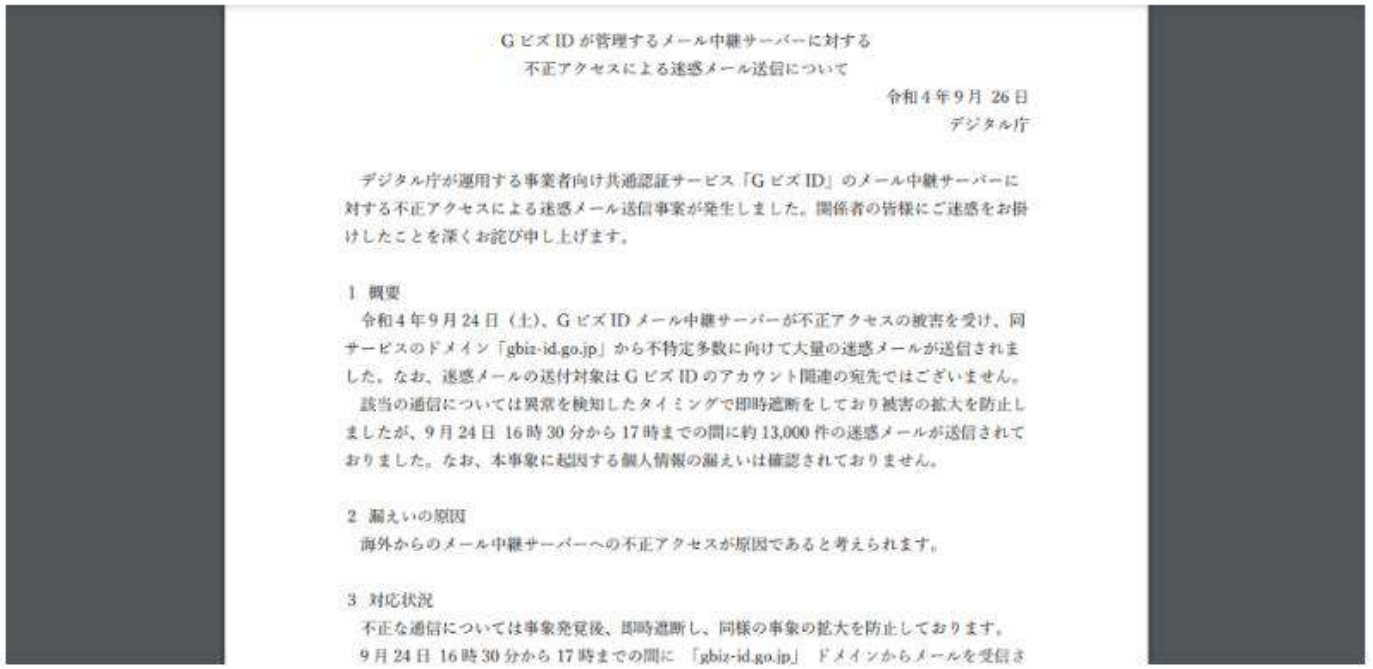
デジタル庁が運用す
情報の漏えいが発生
す。

「GビズID」利用者

- 個人情報の漏えいについて（PDF／385KB）

公開日：2022.09.29　|　最終更新日：2022.09.29

デジタル庁Gビズが不正アクセス被害、政府ドメインから不審メール



Gビズ ID が管理するメール中継サーバーに対する
不正アクセスによる迷惑メール送信について

令和4年9月26日
デジタル庁

デジタル庁が運用する事業者向け共通認証サービス「Gビズ ID」のメール中継サーバーに対する不正アクセスによる迷惑メール送信事案が発生しました。関係者の皆様にご迷惑をお掛けしたことを深くお詫び申し上げます。

1 概要
令和4年9月24日（土）、Gビズ ID メール中継サーバーが不正アクセスの被害を受け、同サービスのドメイン「gbiz-id.go.jp」から不特定多数に向けて大量の迷惑メールが送信されました。なお、迷惑メールの送付対象はGビズ IDのアカウント関連の宛先ではございません。
該当の通信については異常を検知したタイミングで即時遮断をしており被害の拡大を防止しましたが、9月24日 16時30分から17時までの間に約13,000件の迷惑メールが送信されておりました。なお、本事象に起因する個人情報の漏えいは確認されておりません。

2 漏えいの原因
海外からのメール中継サーバーへの不正アクセスが原因であると考えられます。

3 対応状況
不正な通信については事象発覚後、即時遮断し、同様の事象の拡大を防止しております。
9月24日 16時30分から17時までの間に「gbiz-id.go.jp」ドメインからメールを受信さ

画像：デジタル庁より引用

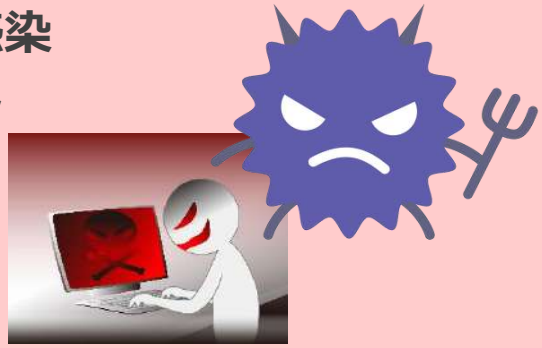
https://cybersecurity-jp.com/news/72196

https://www.e-gov.go.jp/news/2022-03-31t1322240900_752.html

情報漏えいの原因

過去の事例からも情報漏えいは人為的なミスで発生するが
意図的な抜き取りなどからも発生

- パソコンを含むIT機器
- ウイルス感染
- なりすまし
- 乗っ取り



- 人為的なミス、誤送信
- メールの宛先の選択ミス
- 一斉配信時のメールアドレスの開示
- FAX番号間違い

- 紛失、盗難
- 置き忘れ
- 紛失
- 置き引き
- 盗難

- 意図的な抜き取り(犯罪)
- データ抜き取り
- データ消去

情報漏えいの原因

過去の事例からも情報漏えいは人為的なミスで発生するが
意図的な抜き取りなどからも発生

- **パソコンを含むIT機器**
- ウイルス感染
- なりすまし
- 乗っ取り

- **人為的なミス、誤送信**
- メールの宛先の選択ミス
- 一斉配信時のメールアドレスの開示
- FAX番号間違い

- **紛失、盗難**
- 置き忘れ
- 紛失
- 置き引き
- 盗難

- **意図的な抜き取り(犯罪)**
- データ抜き取り
- データ消去

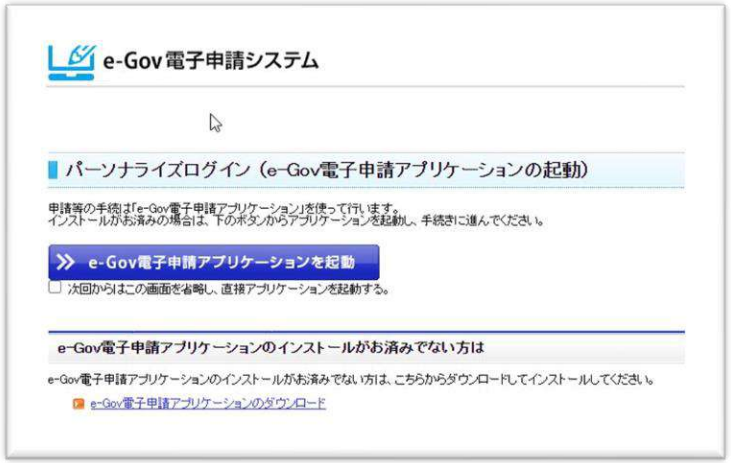
企業活動と情報機器

パソコン等情報機器なしでは今や仕事はできない…

メール　プリント　クラウド　売買

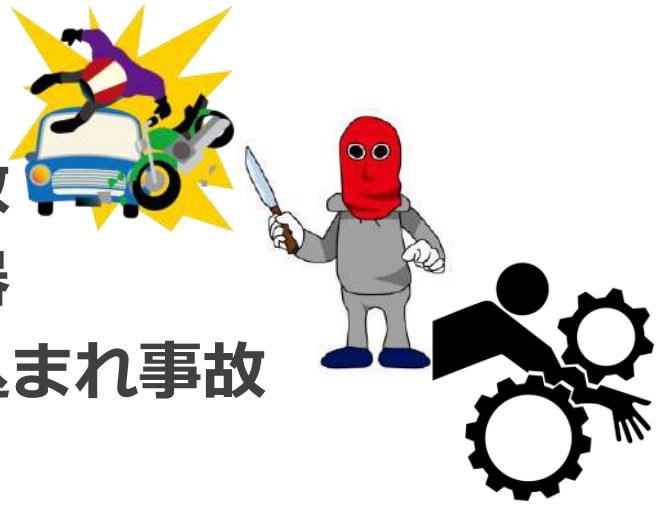
ネット会議

電子申請



情報機器（IT機器）を使う事のリスク

世の中のすべてのツールや商業活動にはリスクがあります
そのリスクを理解し情報機器を使用しましょう！



- 自動車　　便利・快適　⇒　事故
- 包丁　　料理に必須　⇒　凶器
- 製造機器　大量生産　⇒　巻込まれ事故

- パソコン　業務効率化　⇒　情報漏えい・情報消失

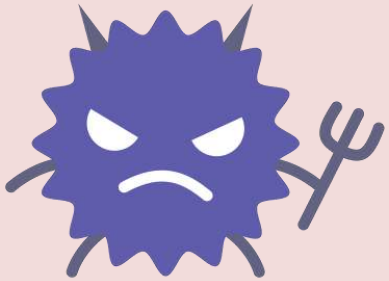
ツールは使わないことではなく、**使い方を知ることで便利になります**
場数を踏んで経験値を上げるしかありません

業務をパソコン等に依存するときの脅威

これらの脅威にさらされながらも業務を続けなければならない

データ漏えい/消失/人質

ホームページ改ざん



破壊活動（あなたが加害者に）

なりすましフィッシング

業務をパソコン等に依存するときの脅威

これらの脅威にさらされながらも業務を続けなければならない

データ漏えい/消失/人質

ホームページ改ざん

コンピューターウイルスの感染によりこれらの脅威が発生

破壊（あなたが加害者に）

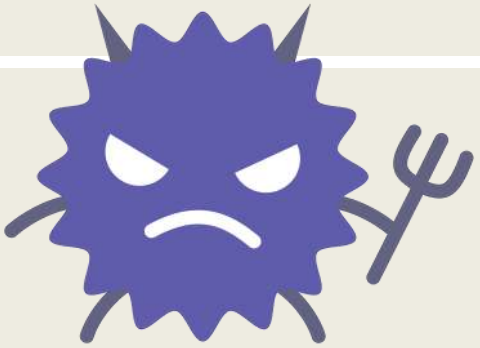
なりすましフィッシング

パスワードの管理が不十分でも！

コンピューターウイルス

悪意を持ったソフトウェアのこと
感染するとコンピューターが意図しない動作を行う

- **コンピューターウイルスとは**
  - 悪意を持った人間によって意図的に作られた不正なプログラム



- **感染したときの症状**
  - 画面上に迷惑なメッセージを出す
  - 情報を消去する
  - 個人情報を盗み取ってしまう
  - パソコンを起動できなくする（**ランサムウェア**）
  - 他のパソコンやホームページ等を攻撃する（踏み台）
  - **見た目には何も起きない事が多い**

「ランサムウェア（Ransomware）」
ランサムウェアとは、感染したパソコンをロックしたり、ファイルを暗号化したりすることによって使用不能にした後、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。身代金要求型不正プログラムとも呼ばれます。

ウイルスの感染経路

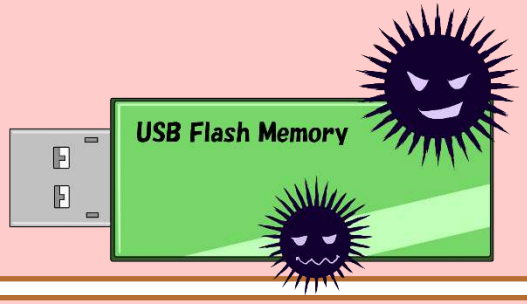
パソコン使用者が意識して感染を防ぐ以外
効果的な防御方法はない一絶対的な警戒心で

1.メール（標的型メール）

- 本文のURLをクリック
- 添付ファイル

2.各種記憶媒体からの感染

- USBメモリー、DVD、CDから

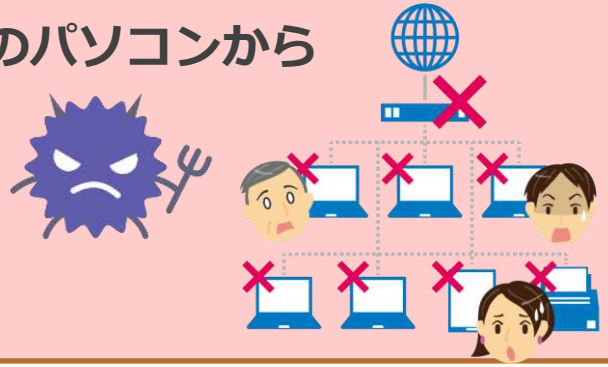


3.インターネットによる感染

- ウイルスが仕掛けられたページへのアクセス
- 動画、画像、アプリに仕込まれたもの
- セキュリティホールからの侵入（脆弱性）

4.ネットワークによる感染

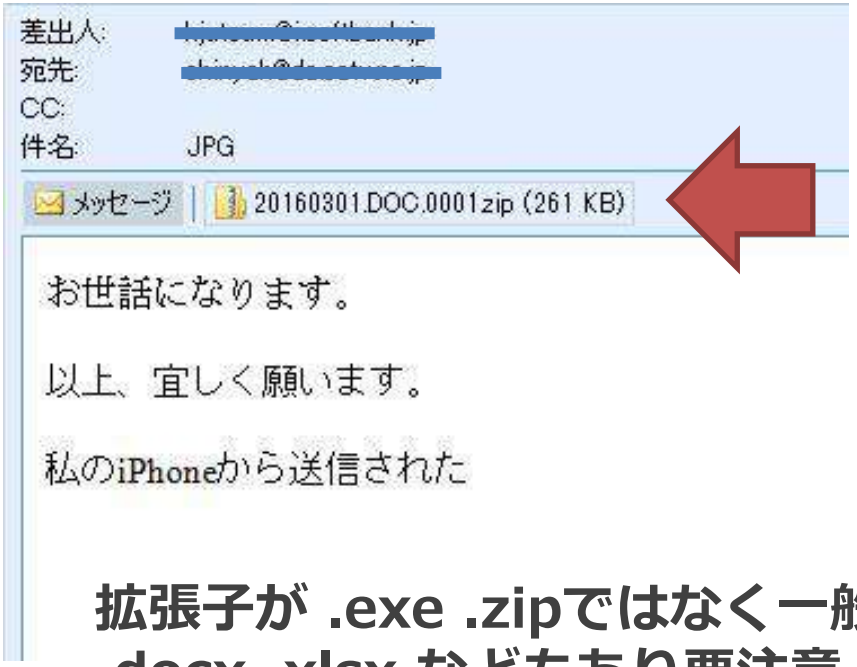
- ネットワーク上につながる他のパソコンから



1.感染経路（メール）

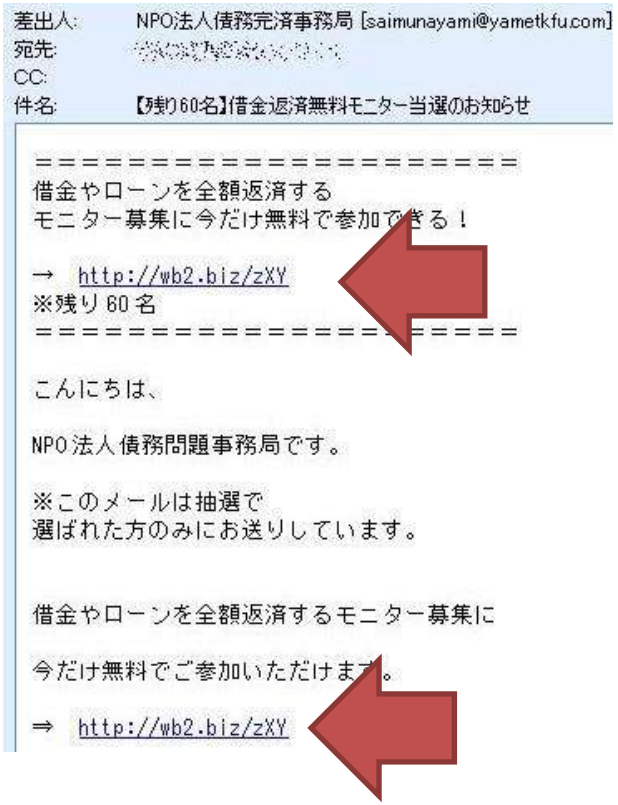
まずはクリックする前に一呼吸
知り合いからのメールでも100%の信用はしないこと

添付ファイル型



拡張子が .exe .zipではなく一般的な
.docx, xlsx などもあり要注意

リンク誘導型

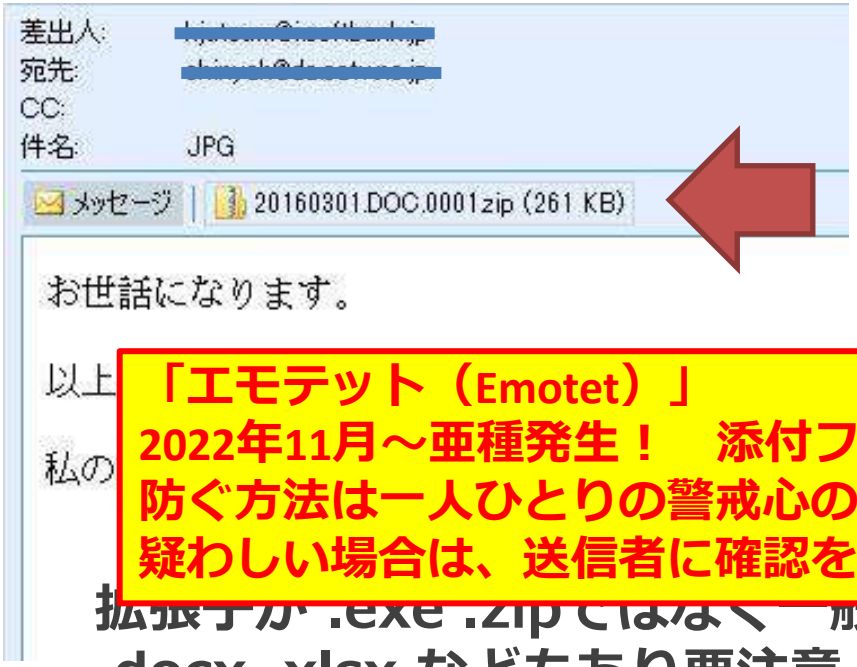


差出人が知り合いの場合やメールタイトルがそれらしいケースも

1.感染経路（メール）

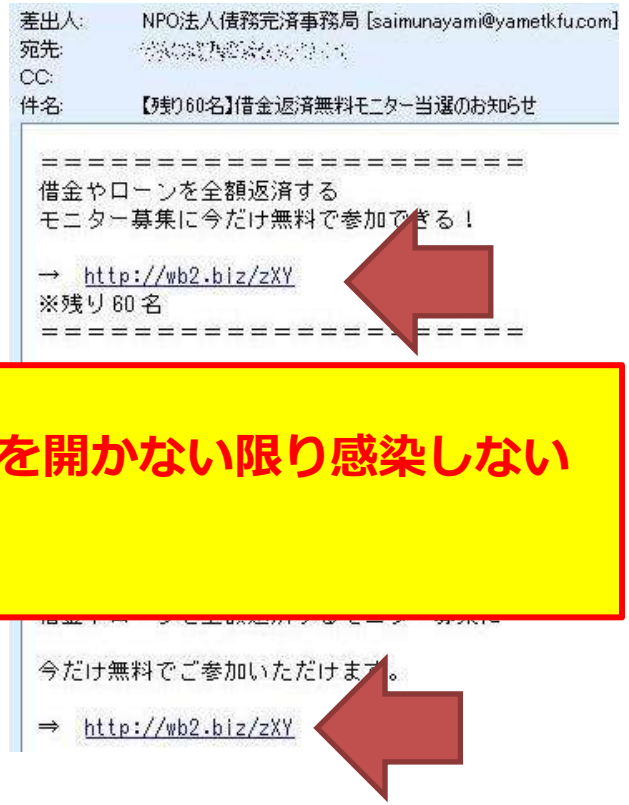
まずはクリックする前に一呼吸
知り合いからのメールでも100%の信用はしないこと

添付ファイル型



拡張子が .exe .zip ではなく一般的な .docx, xlsx などもあり要注意

リンク誘導型



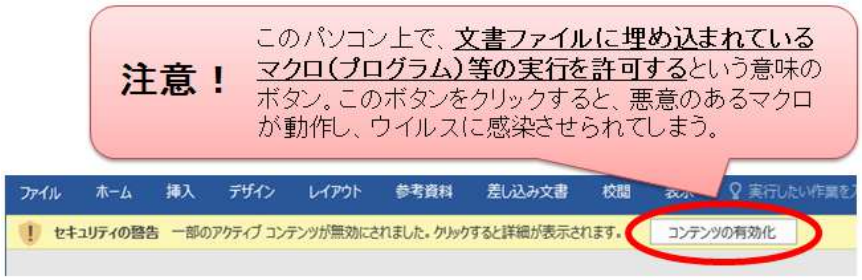
「エモテット（Emotet）」
2022年11月～亜種発生！　添付ファイルを開かない限り感染しない
防ぐ方法は一人ひとりの警戒心のみ！
疑わしい場合は、送信者に確認を！

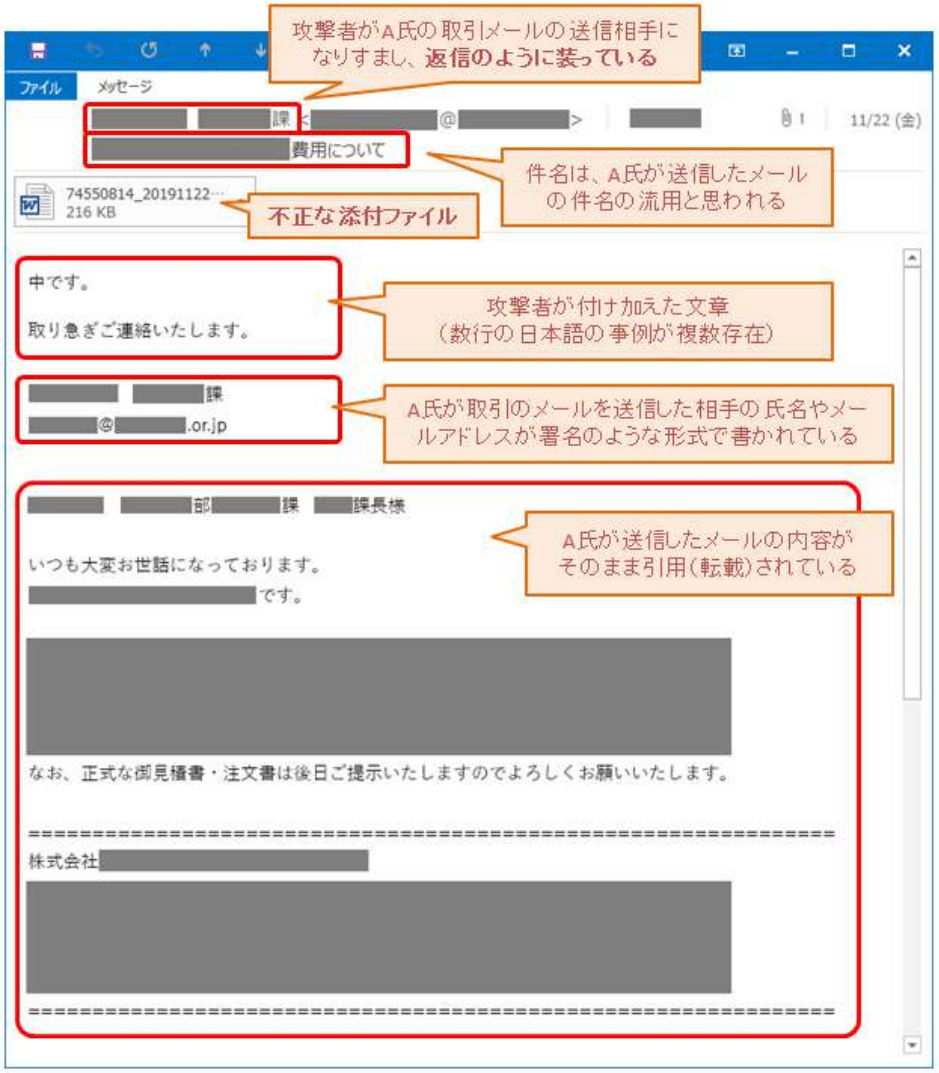
差出人が知り合いの場合やメールタイトルがそれらしいケースも

1.感染経路（メール）　Emotetが大流行

パスワード付きまたはマクロ付きファイルを開くことで感染

- 知り合いからメールが届く
- 送信者は感染者ではない場合も
- 文面もそれらしい内容
- 日本語も稚拙ではない
- 感染すると
  - 個人情報の流失
  - メール拡散
  - 他のウィルスへの感染
  - Eメール情報の搾取





https://www.ipa.go.jp/security/announce/20191202.html

警視庁Emotet 感染確認・駆除ツール使用法サイト

2023.1現在最新はV.2.3.2

Emotet感染確認ツール「EmoCheck」の実行手順

2022年に入り「Emotet（エモテット）」によるサイバー犯罪被害が激増しています。
エモテット感染を確認できる「EmoCheck」がJPCERT/CCから公開されており、一昨年公開されて以降、新しいバージョンのソフトが適宜更新されています。
本資料は「EmoCheck2.1」で手順を説明しますが、最新のもので実行しましょう。

①「EmoCheck」の入手（ダウンロード）

お使いのWebブラウザのアドレスバーに『**https://github.com/JPCERTCC/EmoCheck/releases**』と入力し、[Enter]キーを押してください

②「EmoCheck」の実行

デスクトップに表示された英文表記のページ(左図)が表示されますので、スクロールして、「**▼Assets4**」の下にある表のうち、お使いのパソコンのビット数表示がある方の実行ファイル（exeファイル）をクリックして確認を実行してください。

※ 今お使いのパソコンの種類が、x64かx86かわからないという方は、**x86**で実行してください。
仮に違っていてもパソコンが壊れる等ということはありません。

※ 今後も新しいバージョンが公開されることが予想されますので、定期的にこのページを閲覧してEmoCheckを実行するなどルール化に取り組んでください。

2022.4.4' P 1/2

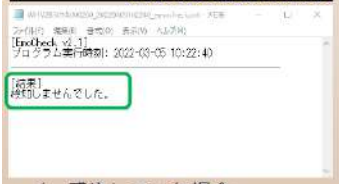
③ Emotet感染の確認

ア 感染していない場合

デスクトップ上には、左図のような黒色のウインドウが一旦立ち上がり結果が表示されます。

検索した結果は、デスクトップ上（またはEmoCheckがダウンロードされたファイル内）に新たに作成されたメモ帳（テキストファイル）にも記載されます。

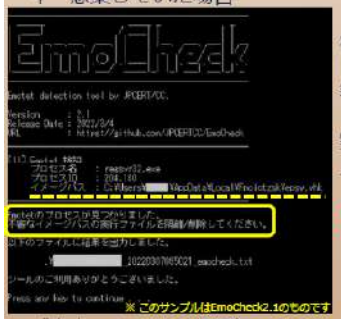
黒色の画面が瞬時に消えてしまったとしても、メモ帳に検知しなかったと表示されれば、感染していないことが確認できます。



メモ帳を開いた際、感染していなかった場合は、「**検知しませんでした。**」と表示されます。

この画面が表示された時点で、Emotetに感染していなかったことが確認できました。
一度で終わらず、定期的にEmoCheckによる確認をお勧めします。

イ 感染していた場合



感染が確認された場合には、EmoCheck実行後の黒色画面及びメモ帳に実線の囲み部分にある「**Emotetのプロセスが見つかりました。**」等と表示されます。
また、各画面の破線部分には、EmoCheckの実行によりEmotetとして認識されたものがイメージパスの項目に表示されます。

ご自身でEmotetが駆除できるようであれば、駆除作業等が詳しく書かれている「**マルウェアEmotetへの対応FAQ**（JPCERT/CC Eyes　2019/12/02）」を参照して作業を行ってください。
駆除作業に自信がない方は、ご自身(または自社)で契約しているセキュリティベンダーに連絡するか、サイバーセキュリティの相談ができる方に駆除方法等を確認しながら対応してください。
万が一、相談する先がない方は、東京都で中小企業の方に対するサイバーセキュリティ支援を行っている機関の１つである
サイバーセキュリティ相談窓口（**０３-５３２０-４７７３**）
をご活用ください。

感染再拡大に関する注意喚起も是非ご一読下さい
https://www.jpcert.or.jp/at/2022/at220006.html

JPCERT FAQ

JPCERT 注意喚起

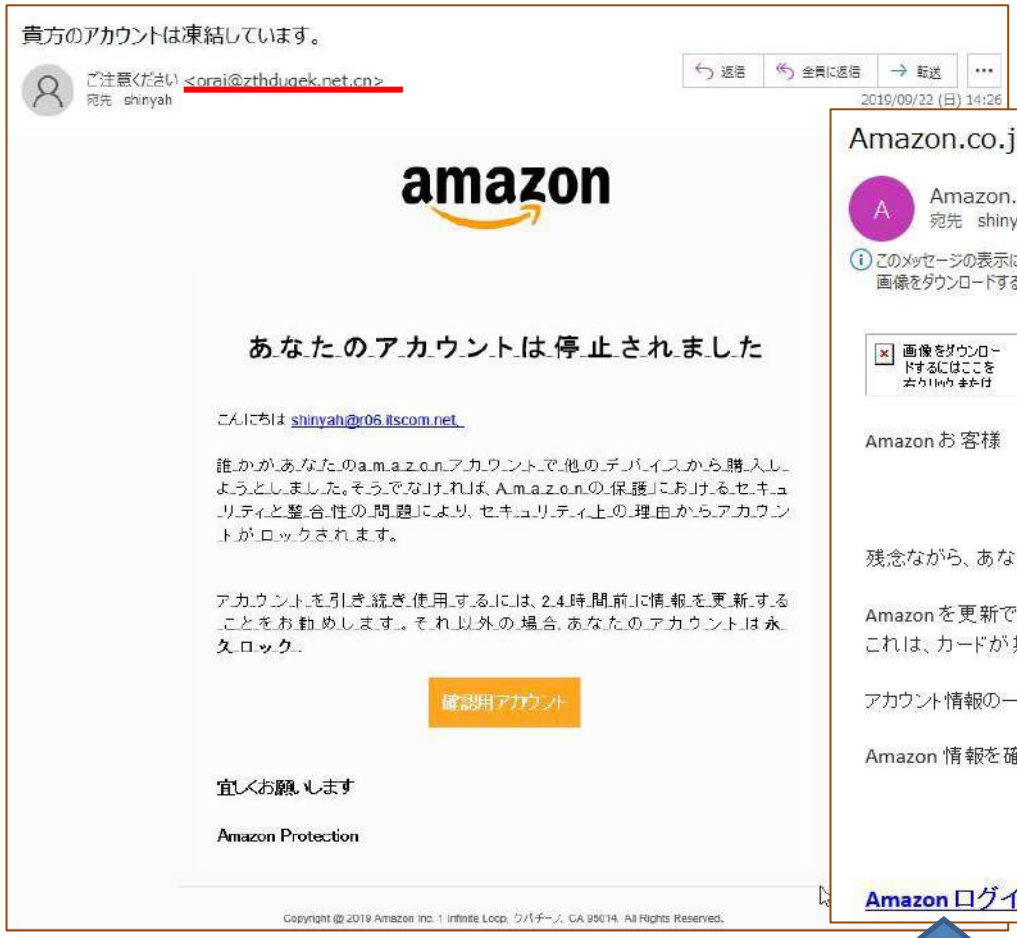
警視庁サイバーセキュリティ対策本部

2022.4.4' P 2/2

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/CS_ad.files/EmoCheck.pdf

1.感染経路（メール）　フィッシング

メールのリンクをクリックせず、ブラウザから直接確認！


貴方のアカウントは凍結しています。

ご注意ください <oraj@zthdugek.net.cn>
宛先 shinyah

返信 全員に返信 転送 …
2019/09/22 (日) 14:26

amazon

あなたのアカウントは停止されました

こんにちは shinyah@r06.itscom.net,

誰かがあなたのamazonアカウントで他のデバイスから購入しようとしました。そうでなければ、Amazonの保護におけるセキュリティと整合性の問題により、セキュリティ上の理由からアカウントがロックされます。

アカウントを引き続き使用するには、24時間前に情報を更新することをお勧めします。それ以外の場合、あなたのアカウントは永久ロック。

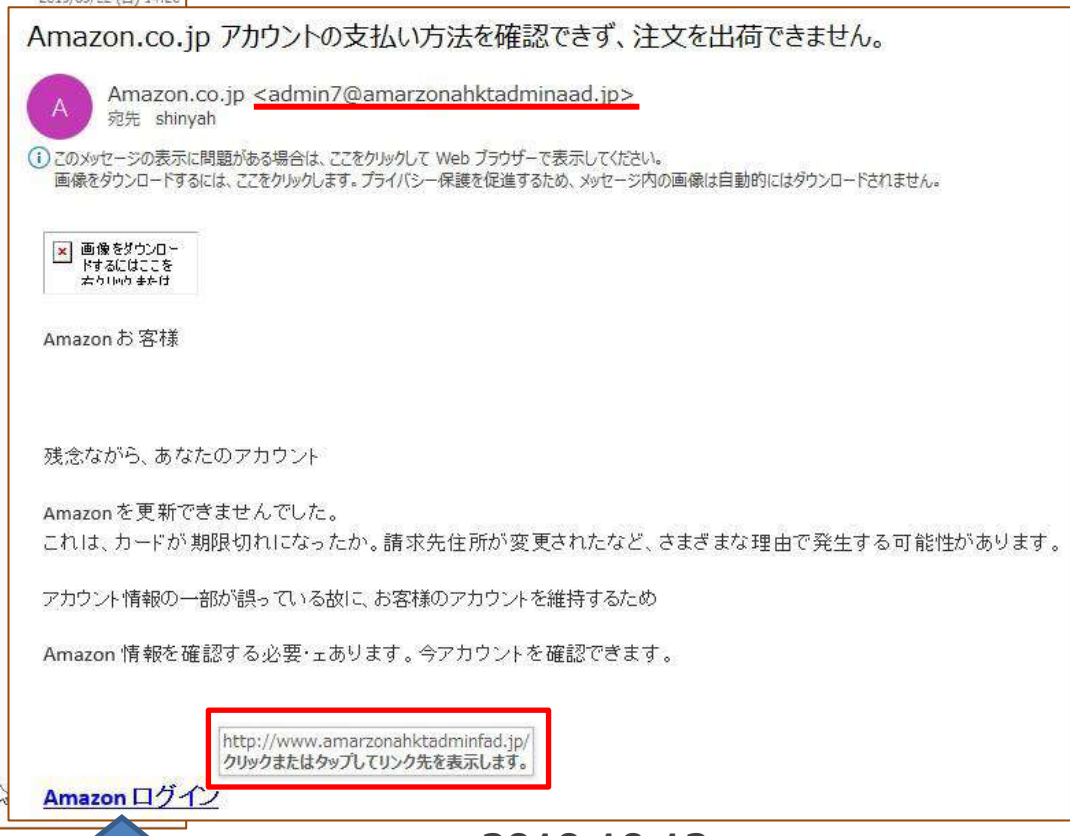
確認用アカウント

宜しくお願いします

Amazon Protection

Copyright @ 2019 Amazon Inc. 1 Infinite Loop, クパチーノ, CA 95014. All Rights Reserved.

2019.9.22
HTMLメール型


Amazon.co.jp アカウントの支払い方法を確認できず、注文を出荷できません。

A
Amazon.co.jp <admin7@amarzonahktadminaad.jp>
宛先 shinyah

このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。
画像をダウンロードするには、ここをクリックします。プライバシー保護を促進するため、メッセージ内の画像は自動的にはダウンロードされません。

画像をダウンロードするにはここを

Amazon お 客様

残念ながら、あなたのアカウント

Amazon を更新できませんでした。
これは、カードが期限切れになったか。請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため

Amazon 情報を確認する必要･ェあります。今アカウントを確認できます。

http://www.amarzonahktadminfad.jp/
クリックまたはタップしてリンク先を表示します。

Amazon ログイン

2019.10.12
テキストメール型

ここにカーソルを

2.感染経路（各種記憶媒体からの感染）

USB・SDカードスロットはパソコン内部への入口
不用意な入り口の開扉は危険

- パソコンの**USBポート**にウイルス入りの機器を接続した場合、パソコンと**接続するだけでウイルスに感染**することがある
- **「ネットに繋がないから安心」ということではない**

ウイルスを仕込んだUSBメモリーを放置し、それを拾った人がパソコンに接続し感染する等の事件が起きている事も

イラン核施設破壊工作：https://eset-info.canon-its.jp/malware_info/trend/detail/160308.html

2.感染経路（各種記憶媒体からの感染）

USBメモリー・CD・DVD・外付けHDDが感染源に
基本は外部記憶機器を接続しないこと

- USBメモリー等の機器は**信頼できるもの**を使用する
- **他人のUSBメモリーなど**を自分のパソコンに繋がせない
- 信頼できないパソコンに**自分のUSBメモリー等を使用しない**
  - ネットカフェなど誰が使用したかわからないパソコンに自分のUSBメモリー等を挿さない
  - 取引先や友人のパソコンも同様
  - ウイルスをもらってこないこと
- 定期的にウイルススキャンを実施する
  - USBメモリーも含め定期的に検診を！

ちょっと待った！！

スマホの充電をパソコンでしていませんか？

- スマホはUSBメモリーと同じ動作を行います
  （データを盗むことも可能）
- もしあなたのスマホに**パソコンに感染するウイルスが入っていたら…**

スマホは充電器で充電しましょう

事務所のパソコンと**私物のスマホの接続は禁止！**

コーヒーブレイク　　こんな所にも罠が…

空港やカフェのなどのUSB充電口を使ってはいけない！

某ファミレスの
USB充電口

旅行中、外出中スマホの電池が切れそうになったとき…
空港、カフェ等のフリー充電スペースはありがたいですね…
でも…　壁のUSBから直接充電するのはお勧めできません…
あなたの、iPhoneやスマホからデータを抜き取られたり、ウイルスを仕掛けられても責任持ちませんよ…

拾った歯ブラシで歯を磨けますか？

3.感染経路（インターネットによる感染）

業務用パソコンで業務外のネットアクセスを行わない
人的操作以外に防ぐ方法がない

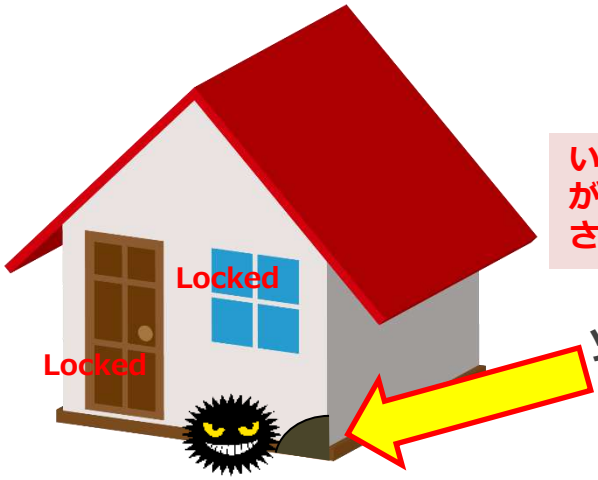
- **閲覧しただけで感染**してしまうことがある
- **出会い系サイトなどのアダルト系サイト**にアクセスしたことによるウイルス感染の被害が多く報告されている

- インターネット上の**動画や画像、フリーソフトやゲーム**に見せかけて、ダウンロードさせそのファイルを開くことにより感染する場合も

3.外部からの脆弱性攻撃

**WindowsのOSや、Microsoft Officeなどに脆弱性
外部から侵入するための抜け道が**

- **脆弱性とは**
  - **コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います**
  - **脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性があります**



いくらドアや窓に鍵を掛けても穴が空いていれば外から簡単に侵入されてしまいます

**ソフトウエアの穴
（セキュリティホール）**

**Windows7, 8.1や
Office2010など古い
ソフトを使い続けると
脆弱性を保障できない**

https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html

Windows 8.1 サポートは終了しました！

終了日　2023年1月10日

セキュリティ更新プログラムの提供
仕様変更、新機能のリクエストが終了

サポート終了後のパソコンを使い続けると

マルウェアや
ウイルスへの感染

マルウェア(Malware)とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称

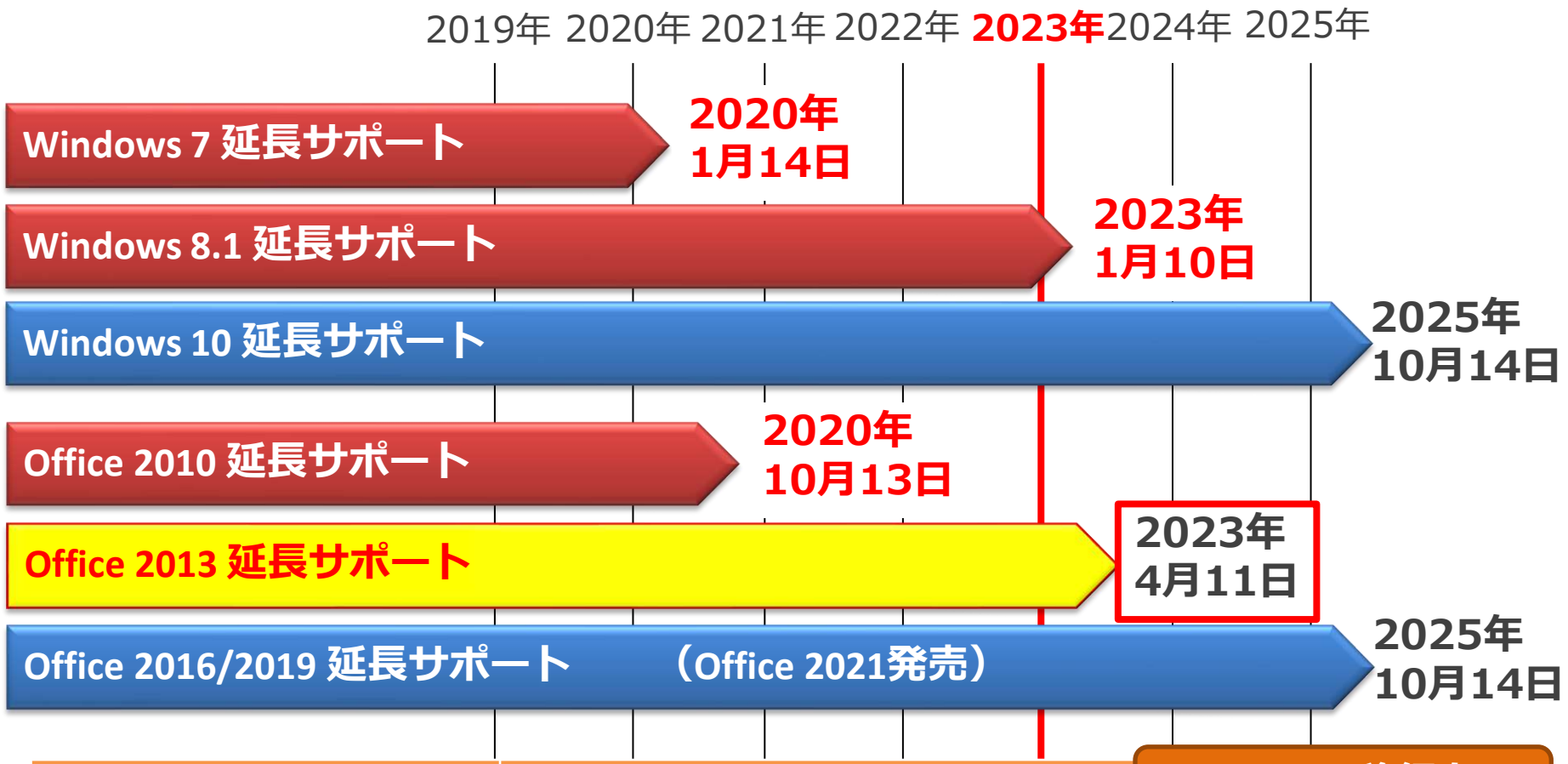
フィッシング詐欺
なりすましの被害

正規のサービスなどのふりをしたメールで偽のWebサイト（フィッシングサイト）に誘導させ、クレジットカード情報やログイン情報を盗み出す行為

個人情報の漏えい
の危険性

マルウェア(Malware)やウイルスに感染し、情報漏えいや情報の消失などが発生し、業務不能に陥る

Windows OS/MS Office サポート終了日



その他のOS / Software	延長サポート終了日
Windows 11	未定
Internet Explorer 11	2022/6/15完全終了

Edgeへ移行を

https://www.microsoft.com/ja-jp/atlife/article-windows10-portal-eos.aspx?SilentAuth=1
https://office-word-excel.com/microsoft-office-support
http://tanweb.net/2018/03/21/20199/

公文書 スタイルファイル .xsl を Edge で見る

E-gov サイトの Q&Aに Edge でのアクセス方法あり

Q. Internet Explorerのブラウザ以外で、XMLファイル形式の公文書ファイルを開く方法を教えてください。

A.

Internet Explorer以外のブラウザでは、初期設定ではスタイルシート（XSLファイル）を読み込むXMLファイル形式の公文書を開くことができませんが、次の手順により、適切に表示させることができます。

・Microsoft Edgeの場合

① 右上「メニュー」ボタンをクリックし、[設定]をクリックします。

② 「既定のブラウザ」を選択し、「Internet Explorer モードでサイトの再読み込みを許可」を有効にします。

※ ブラウザの再起動が必要となりますので、「再起動」ボタンを必ず押下してください。

③ 以上で必要な設定は完了です。

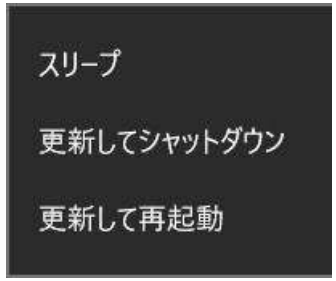
XML形式の公文書をブラウザで開いたうえで、右上「メニュー」ボタンを選択し、「その他のツール」>「Internet Explorerモードで再度読み込む」を選択すると、適切に開くことができます。

https://shinsei.e-gov.go.jp/contents/help/faq/document.html

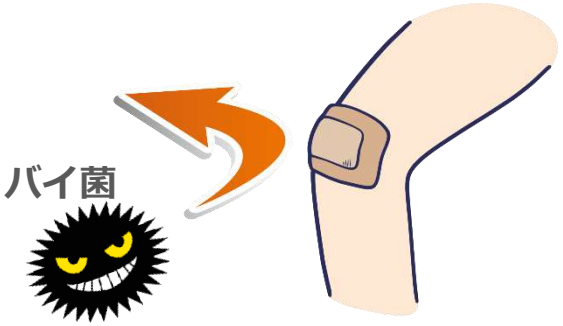
3.脆弱性を防ぐには

OSやソフトウェアメーカーからパッチソフトが供給される
そのソフトウェアを至急インストールする

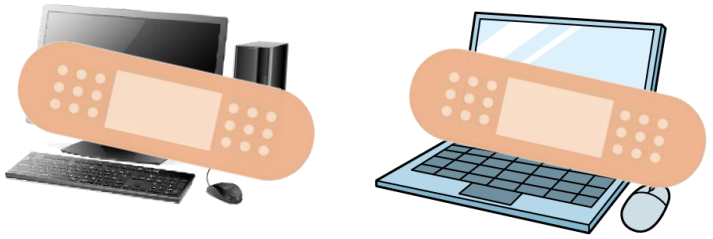
- パッチソフトとは
  - プログラムの一部分を更新してバグ修正や機能変更を行なうためのデータのこと。「修正プログラム」や「アップデート」などとも呼ばれる。



傷口に貼る絆創膏（パッチ）



脆弱性のブロック（パッチソフト）



穴を塞ぐことで外部からの侵入を防ぐ

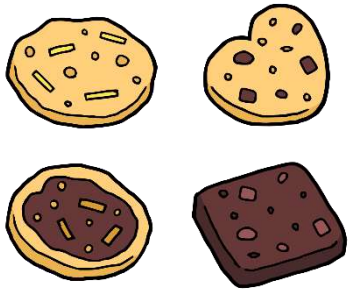
脆弱性が見つかるとパッチソフトがリリースされるがその脆弱性を突いた悪意のあるソフトも出回るため至急パッチをインストールする必要がある

コーヒーブレイク　Cookie ってなに？

ネットを見ていると画面が下の方に出ることがありませんか？

Cookie とは
あなたが閲覧したネットの履歴を残しておく機能
ID, PW, 閲覧した場所、買い物かごの内容などを記録
その他の個人情報は記録されないが…

それらのデータは、サイト管理者へも送出される
マーケティングや、広告のターゲティングにも利用



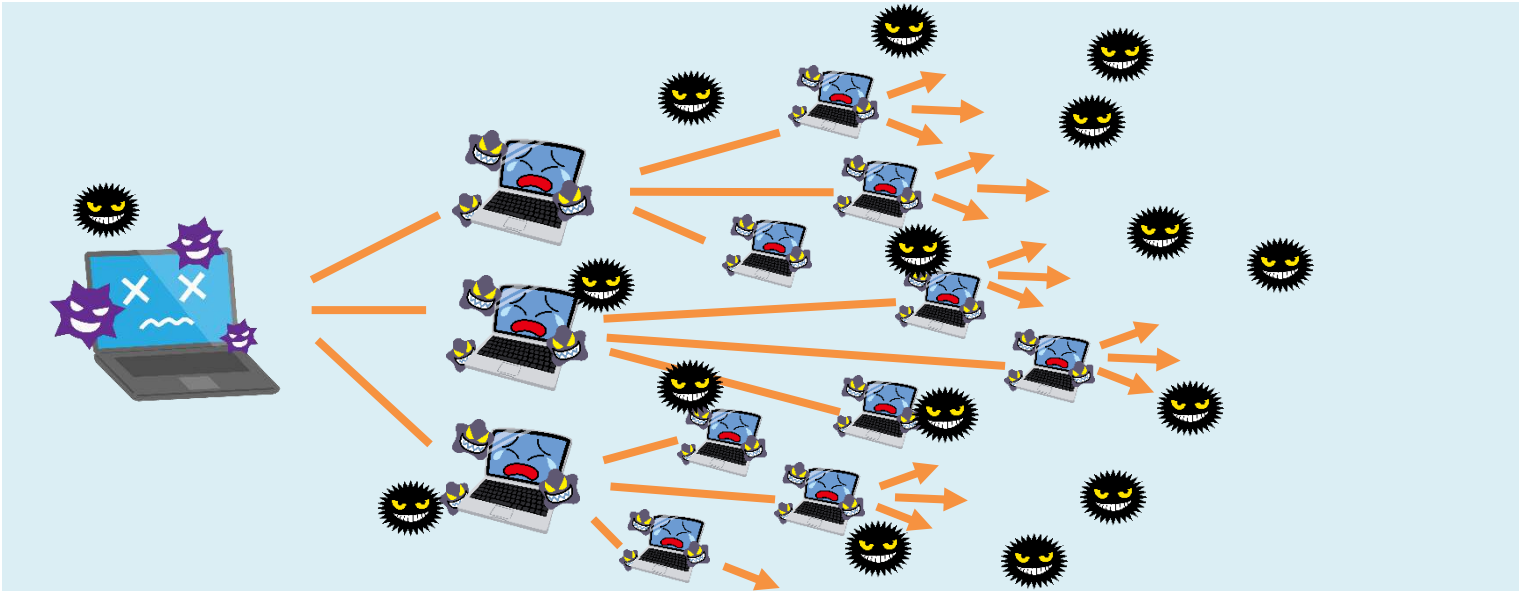
2022年の個人情報保護法改正で、cookie 利用の同意が必要となったため
同意を求める案内が表示されるようになった

同意するしないは自由
ターゲティング広告が不快なら同意しないこと

4.感染経路（ネットワークによる感染）

まずは感染させない
感染がわかれば即感染したパソコンをネットから切り離す

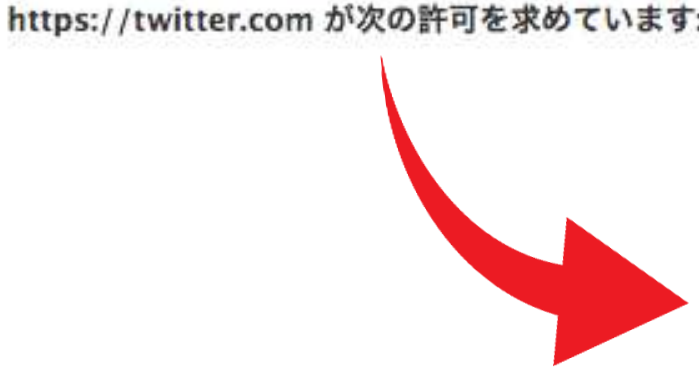
- 1台のパソコンがウイルス感染しただけでネットワーク上のパソコンに感染し、他のパソコンにまでどんどんウイルス被害が拡大してしまう。
- **社外の機器を社内のネットワーク**に接続させないこと

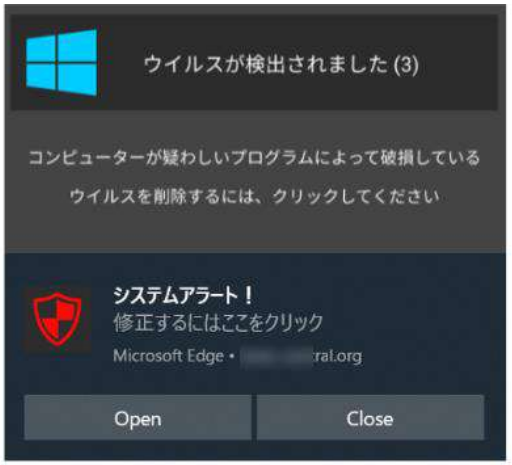


感染したPCのウイルスを完全に消去できるまでネットワークには接続しないこと

そのほか　「許可」を求められた場合

画面左上にこのような「許可」を求める
ポップアップが出た場合　⇒　「ブロック」





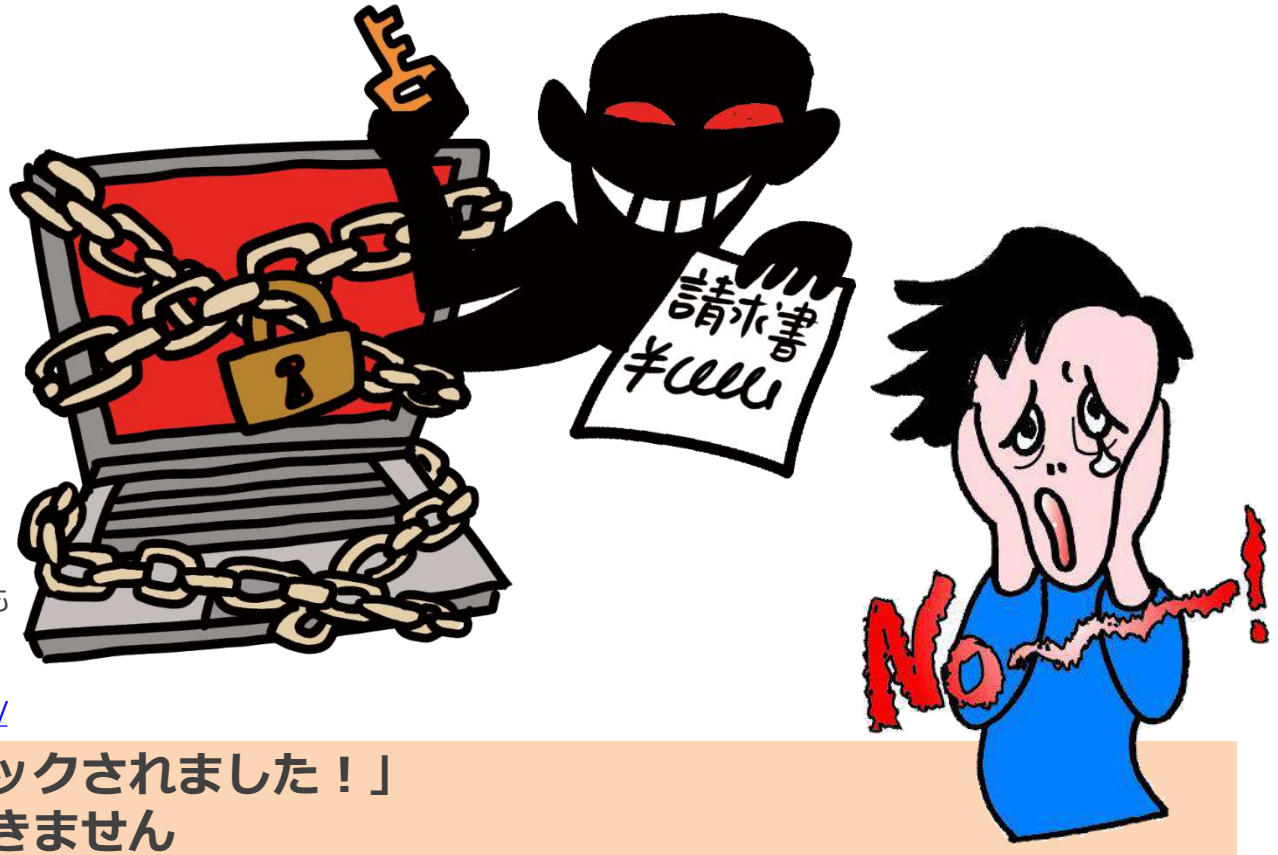
https://www.ipa.go.jp/security/anshin/mgdayori20210309.html

千葉銀行　セキュリティ対策サイト

https://www.chibabank.co.jp/myaccess/security/internet/defend/

コーヒーブレイク　ランサムウェアの被害

あなたのパソコンがロックされました！



フロリダ州のある都市の役所のパソコンがランサムウェアに感染
50万ドル（5500万円）支払ったケースも
攻撃を受けた職員は解雇処分に
(2019.7)
https://japan.zdnet.com/article/35139315/

「あなたのパソコンがロックされました！」
何をしてもパソコンが動きません
「解除する場合はこちらに電話してください 090-xxxx-xxxx」と画面に
電話はかけずに、警察「サイバー犯罪相談窓口」やIPAに連絡を！
https://www.npa.go.jp/cyber/ransom/index.html

あなたのパソコンが人質に・身代金でロック解除を誘う（お金払っても解除されない）

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
◇ウイルス防御のために
◇パスワードの管理
◇無線LANのセキュリティ
◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

ウイルス防御のために

Windows Defender またはセキュリティソフトは必須
しかし100%ではないことを理解する

- セキュリティソフトは必須
  - しかしセキュリティソフトの設定ミスなど人為的なミスで感染するケースが多い
  - 正しく設定し最新パターンファイルを取得しておくことが大切

http://thehikaku.net/security/hikaku.html

個人向けセキュリティソフト

導入後はまず全スキャン。その後自動で最新にアップデートする設定に

ソフトの期限切れにも注意してください

同時に2つ以上のセキュリティソフトを入れるのは誤作動の元

セキュリティソフトを入れても100%の除去は不可能

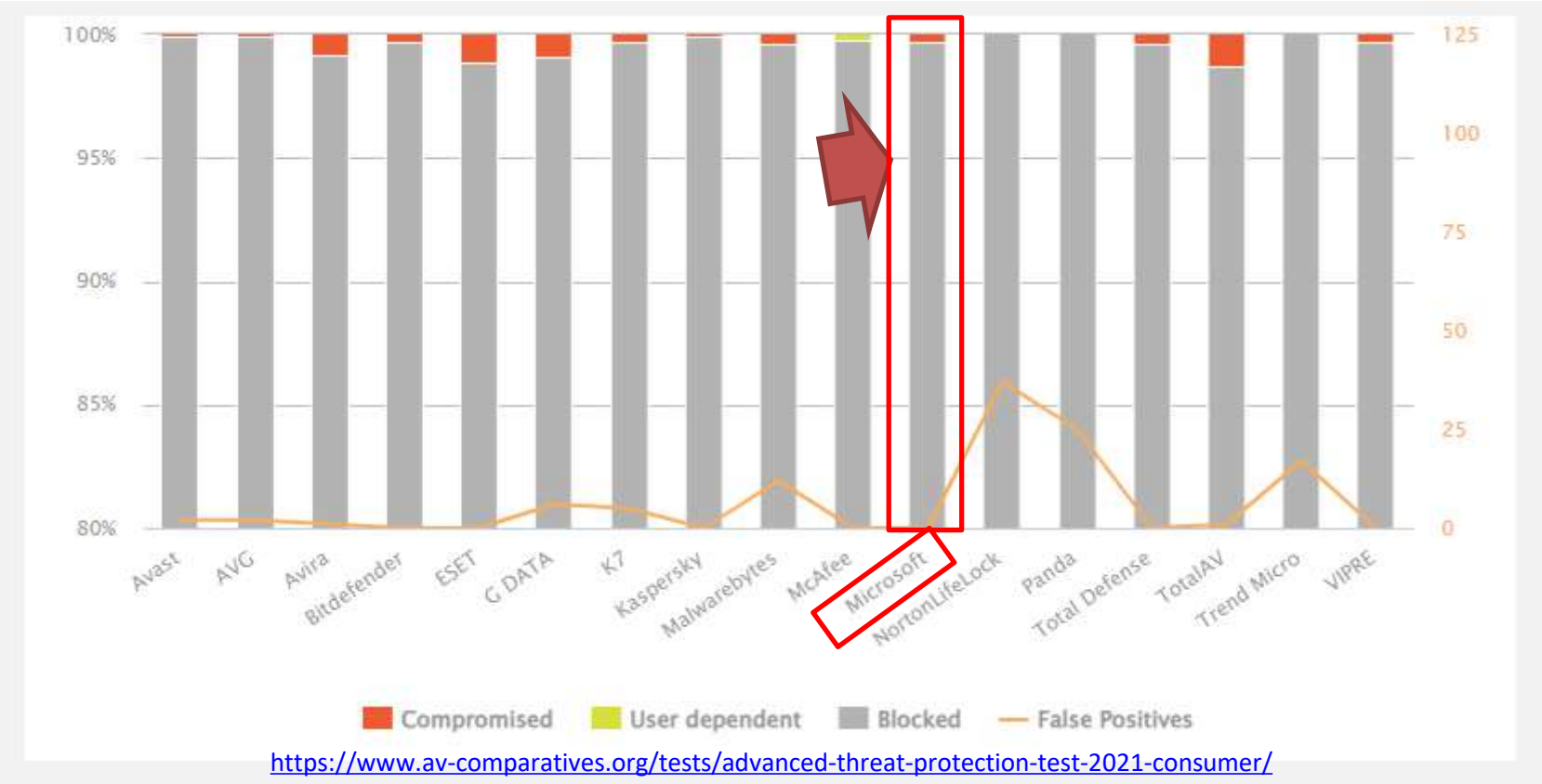
まずはウイルスに近づかないこと

https://www.ffri.jp/
https://www.shieldex.co.jp/

従来のワクチンソフトだけではなく、異常動作・無害化ソフト等も有効

ウイルス防御のために

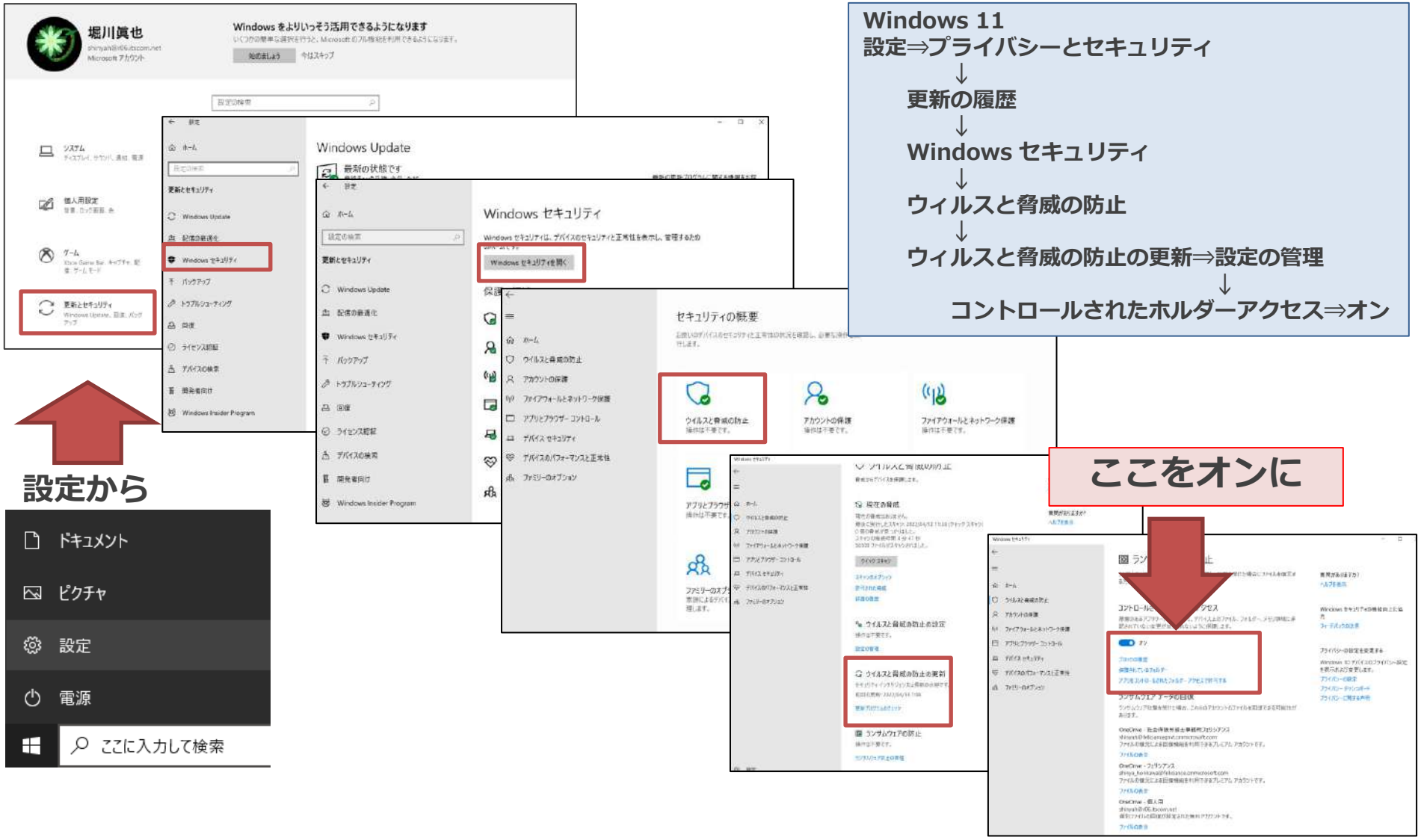
Windows 10, 11 の場合
Windows Defender でも十分な防御が可能



https://www.av-comparatives.org/tests/advanced-threat-protection-test-2021-consumer/

ネットワークバンキングを利用しない場合 Windows Defender で十分と言われている

Windows Defender での設定



Chrome を使用する場合　Microsoft Defender Browser Protection　をインストール

https://chrome.google.com/webstore/detail/microsoft-defender-browse/bkbeeeffjjeopflfhgeknacdieedcoml?hl=ja&gl=US

コーヒーブレイク

カスペルスキーは危険か？？？

ロシア製「カスペルスキー」は
近年の国際情勢から西側諸国では
使用を禁止する動きが

ニュース > 経済

露のウイルス対策ソフト「カスペルスキー」、露政府が悪用リスク…欧米で警戒強まる

2022/04/06 06:49　ウクライナ情勢　この記事をスクラップする

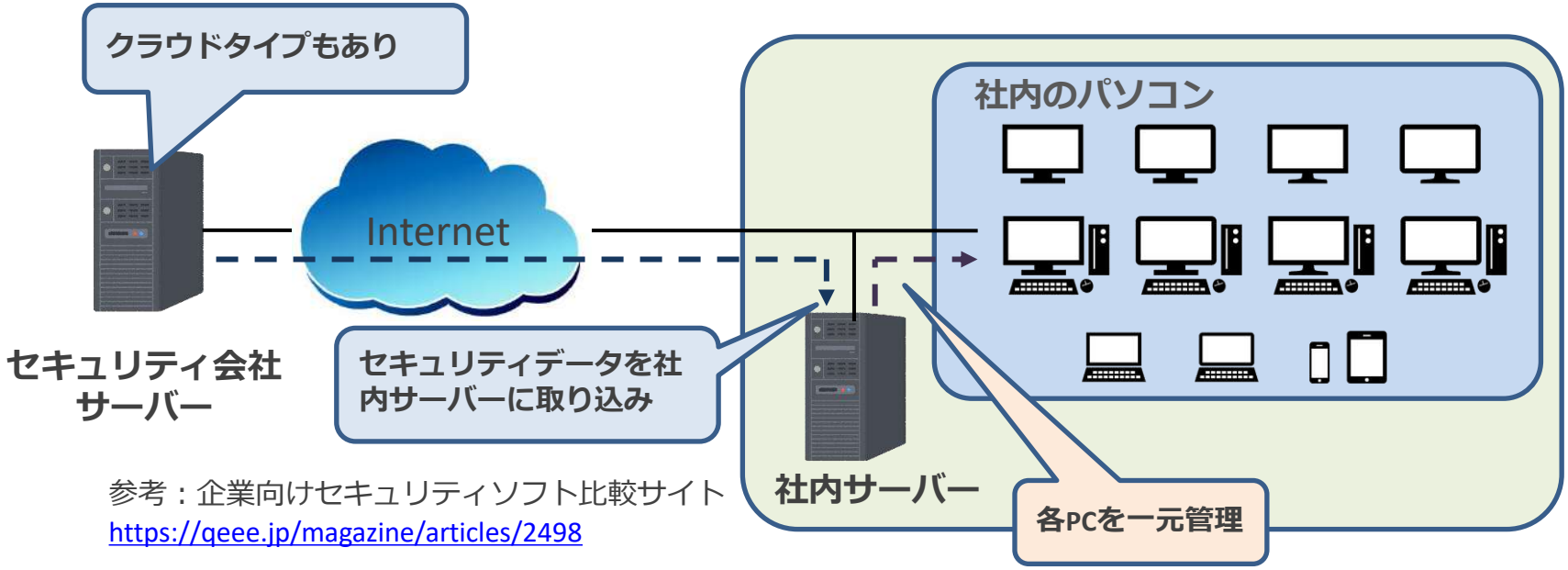
ウイルス対策ソフトを手がけるロシアの情報セキュリティー会社「カスペルスキー」への警戒感が欧米で広がっている。米政府は同社を「安全保障上の脅威がある企業」に指定し、排除の姿勢を強めたほか、ドイツ政府も同社ソフトの利用はリスクが高いと警告し、別の製品に切り替えるように呼びかけた。

https://www.yomiuri.co.jp/economy/20220406-OYT1T50044/

ウイルス防御のために

事務所のパソコンの台数が増えてくると…
すべてのパソコンを同じ条件に保つことが難しくなる

- **業務用セキュリティソフトの薦め（ESET/Symantec など）**
  - 数台のパソコンであれば個人用でもある程度カバーできるが…
  - 事務所の規模が大きくなれば総合的な対策が必要
  - 個々のPCを一元に管理・すべてのPCに同一のセキュリティを提供



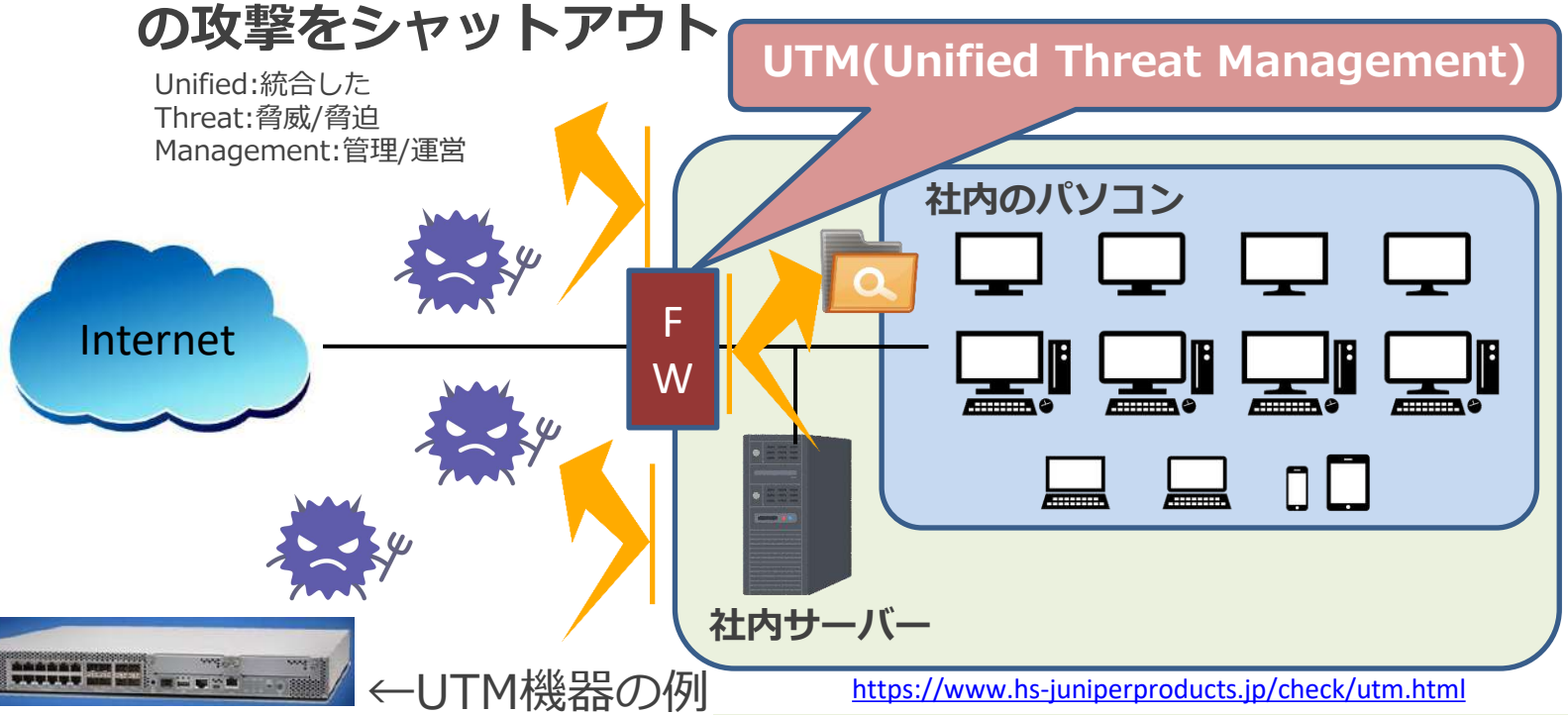
参考：企業向けセキュリティソフト比較サイト
https://qeee.jp/magazine/articles/2498

ウイルス防御のために

セキュリティソフトは水際(エンドポイント)の阻止
会社の出入口(ゲートウェイ)にも壁を設ける

- **マンションのオートロックと自宅の鍵で鉄壁の防御**
  - **インターネットの入り口にFirewall (FW) 装置(UTM)で外からの攻撃をシャットアウト**

Unified:統合した
Threat:脅威/脅迫
Management:管理/運営



←UTM機器の例

https://www.hs-juniperproducts.jp/check/utm.html

参考：https://special.oaland.jp/security/
https://www.mrb-security.jp/
5年リースで 10,000円/月程度から

Firewall (FW) 装置(UTM)でパソコンのバックドアからのデータを外に出さないことも可能

標的型メールへの対策

絶対的警戒心で！　「私は騙されない！」

パソコン使用者が注意する以外方法はない

騙されないための習慣化・訓練が必要

開く前に

- 送信者を確認

クリックする前に

- 添付ファイルを確認・差出人を確認
- 本文の内容・日本語の稚拙さなどを確認

開くべきか否かを自らで判断

いつもやりとりする人とは、あらかじめお互いのみが知る合言葉などをつける
知り合いから不審な添付メールが送られてきたときは確認するなどの対策も

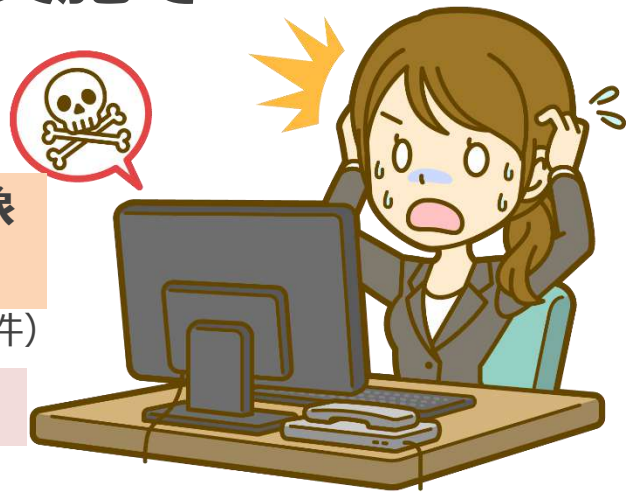
IPA対策のしおり
https://www.ipa.go.jp/security/antivirus/shiori.html

標的型メールへの対策

命を守る避難訓練と同様、訓練を行い身を守る！

標的型メール訓練の実施

経営者はもちろん、全社員（全スタッフ）にも
セキュリティ教育とメール訓練の実施で
事務所を守る！



東京都のサイバーセキュリティ対策促進助成金の対象
（上限５０万円 下限１０万円）

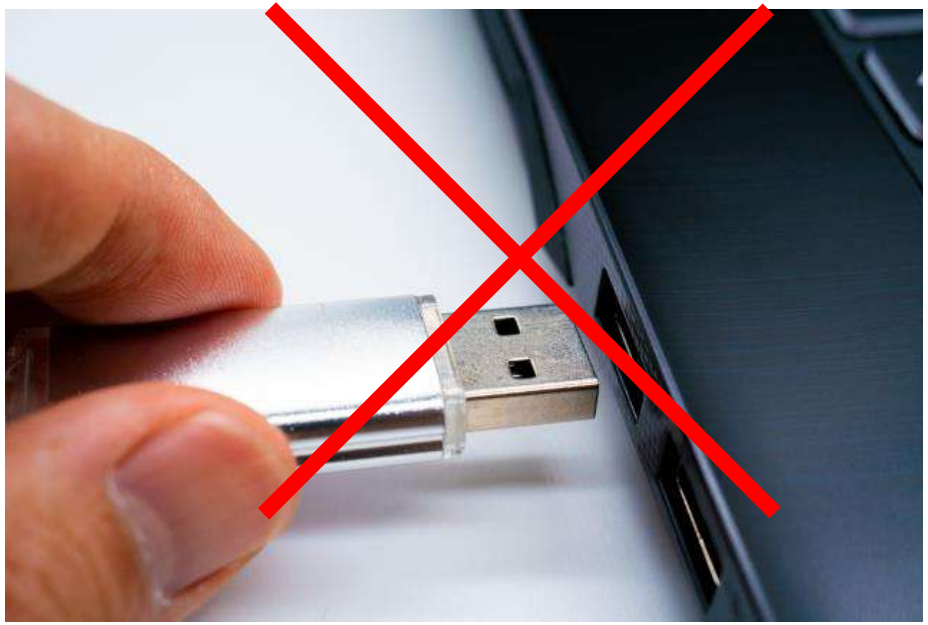
（プライバシーマーク取得していることが条件）

SRP-II登録事務所はメール訓練を受けることが可能

大塚商会の訓練サービス　(お試し無料版も用意)
https://www.otsuka-shokai.co.jp/products/security/consulting-education/aptmail-training-service/
東京都のサイバーセキュリティ対策促進助成金
https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html

各種記憶媒体からの感染の防止

USBを挿したときに自動実行しない設定にする
Windows Defenderでスキャンを



http://121ware.com/qasearch/1007/app/servlet/relatedqa?QID=018506

繋がないのが一番！

デジタル的ソーシャルディスタンスを！

見ず知らずのUSBは絶対に繋がない！

Windows10
Windowsの設定⇒デバイス⇒自動再生⇒なにもしない

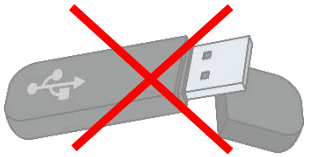
Windows11
設定⇒Bluetoothとデバイス⇒自動再生⇒全てのメディアとデバイスで自動再生を使う　オフに

https://securitynavi.jp/2074

大容量のデータの受け渡しは…

USBメモリーなどの媒体を使わず安心できるサーバー経由で

- 取引先との情報（データ）の受け渡しは…



  - USBメモリーは**原則使用しない**
  - 大容量のファイルのやりとりは外部サーバーやファイル交換サイト経由で
  - URL・パスワードの管理を！

顧問先とのデータ共有・メールの誤送信防止に ファイル交換安心君　OneDrive　Dropbox　box　メールZipper MAIL SECURITY SERVICE

コーヒーブレイク参照

  - メールで送付する場合は誤送信に注意
  - 添付ファイルにパスワードをかけて送るのは原則禁止
  - パスワードを別送する場合は、他の媒体で

脆弱性・ウイルス防御の対策　Windows Update

脆弱性が見つかるとその脆弱性に対し攻撃が始まる
OSやOfficeは自動更新の方法があるので選択しておけば安心

Windows 10 の場合

Windows 11 の場合
設定⇒Windows update⇒更新プログラムのチェック

Windows Defender のパターンアップデートも
この更新で最新となる

https://www.microsoft.com/ja-jp/safety/protect/musteps_win10.aspx

コーヒーブレイク　PPAPに注意

メールでパスワードつきファイルとPWの送信は禁止！

- 取引先との情報（データ）の受け渡しに
  - 開封パスワードをかけてZIP等で圧縮し、メールに送信
  - 次のメールで、パスワードを送信

これをPPAPと呼んでいます。
- PasswordつきZIPを送り
- Passwordを送る
- A（暗号化）
- P（Protocol）

問題点
- マルウエア（ウイルス）を発見できない可能性が増大　Emotet が通り抜ける
- 悪意のある者は、同じメールで送るZIPもPWも受信し、解読が可能
- 開封者が面倒

https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/

同じメールでパスワードを別に送っても意味が無い
送るのであれば、 Messenger や Lineなどメール以外の方法で
もしくは信頼できるクラウドサーバー経由で

コーヒーブレイク　パスワードつきファイル…

メール添付ファイルのパスワードはメリットなし

メール添付のパスワードは解読が容易		
文字列	組み合わせ	解読時間
zansin	小文字のみ	1秒未満
zansinzz	小文字のみ	20秒
202106012045	数字のみ	2分51秒
Zansin01	小文字、大文字、数字	2日6時間（見込み）
Zans!n01	小文字、大文字、数字、記号	55日13時間（見込み）

日経新聞 2021/7/12　https://www.nikkei.com/article/DGXZQOUC3074Z0Q1A630C2000000

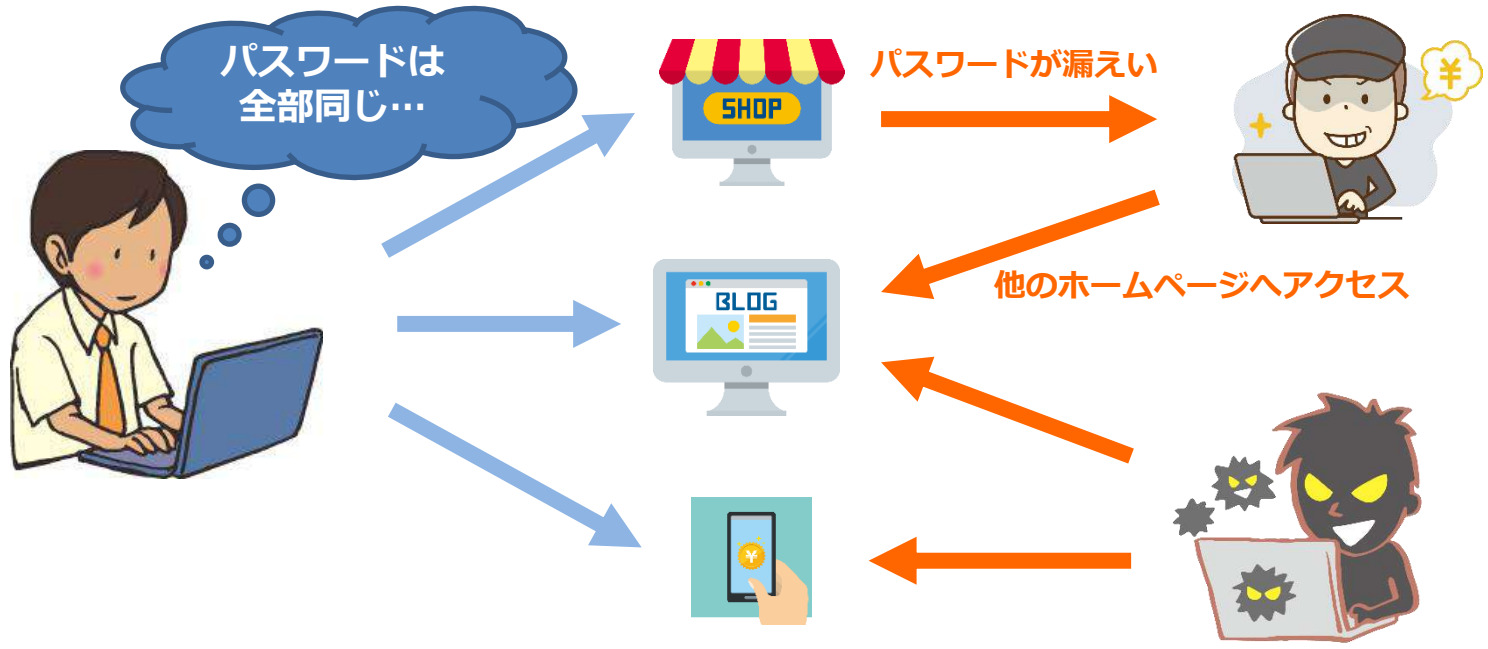
- メールに添付するファイルをパスワードをかけると、ファイル内部のウィルスをサーバーやメーラーが検知できないなどの弊害あり
- Emotet はこのパスワード付き（マクロ）添付ファイルを悪用
- メールを開く際に手間
- 追っかけてパスワードを送るのは最悪

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

パスワード漏えい

パスワードは最後の砦
不正アクセスを防止するためパスワードの重要性を！

- パスワード使い回しの危険
  - パスワードの管理が大変
    - 覚えやすいパスワード
    - 同じパスワードをたくさんの場所で使用



パスワード漏えい

パスワードの使い回しは大変危険
自分なりのパスワード作成のアルゴリズムをもつ

https://www.ipa.go.jp/chocotto/pw.html

- 悪意のある誰かがパスワードを推測できれば…
  - いくつかの思いつくパスワードを試して入力　⇒ビンゴ！

使い回しはせず、すべてのパスワードを記憶できるように

- もし何処かのサイトで自分の個人情報が漏れたら…
  - そのパスワードで他のサイトへ入ることが可能
  - それが業務上のサイトだったら…

個人のパスワード管理なら、管理アプリも選択肢

ロボフォーム
LastPass
1Password

RoboForm
LastPass

アルゴリズムの例

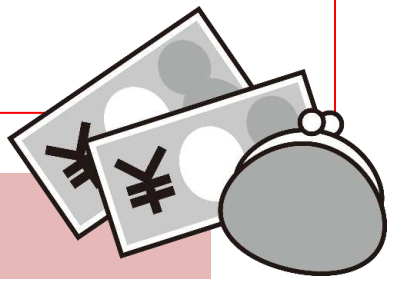
◇［ 英単語 ］＋［ 好きな日本語のローマ字 ］＋［ 英単語 ］＋［ 英単語 ］
◇[そのサイトの頭文字2～3文字]+[自分固有の単語]+[登録年月日]

ID/パスワード作成時の注意点

パスワードは最後の砦
不正アクセスを防止するためパスワードの重要性を！

- 名前や誕生日など**推測可能な情報から設定しない**
- **自分だけのアルゴリズム**を作成する（自分だけのパスワードルールを決める）
- 定期的にID/パスワードを変更する←（できれば…）
- アカウントごとに**異なるID/パスワード**を作成する
- 英字(大文字、小文字)・数字・記号など使用できる文字種すべを組み合わせ、**８ 文字以上**にする
- 辞書に載っているような単語や名前（人名、地名）を避ける
- 多段階・多要素認証を利用する
- パスワード管理ソフトを使用する

参考：https://www.hack-cafe.net/safe-password/



パスワードによる対策には費用がかかりません！！

ID/パスワード作成時の注意点

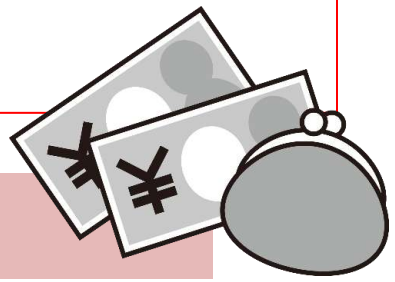
パスワードは最後の砦
不正アクセスを防止するためパスワードの重要性を！

- 名前や誕生日など**推測可能な情報から設定しない**
- **自分だけのアルゴリズム**を作成する（自分だけのパスワードルールを決める）
- 定期的にID/パスワードを変更する←（できれば
- アカウントごとに異なるID
- 英字（大
  てを
  文字にする
- 辞書に載っているような単語や名前（人名、地名）を避ける
- 多段階・多要素認証を利用する

共通パスワード、貸与アカウントは
従業員の退職と共に一斉に変更する

https://www.youtube.com/watch?v=lXh0b4KS9gE

参考：https://www.hack-cafe.net/safe-password/



パスワードによる対策には費用がかかりません！！

2019年11月25日のニュース

元勤務先のデータを消去！　退職後ID等変更せず！

2019/11/25のニュースより

業務を妨害する目的で元勤務先のパソコン内のデータを全て消去したとして、千葉県警サイバー犯罪対策課は２５日、電子計算機損壊等業務妨害の疑いで、東京都調布市多摩川の自称会社員、●を逮捕した。「社長や会社の対応に不満があり、会社の業務を妨害した」と容疑を認めているという。

逮捕容疑は３月５～６日、以前勤務していた千葉県八千代市の建設会社のパソコンに不正にアクセスし、顧客情報や契約書などの全データを消去したとしている。

●容疑者は同社のシステム管理を１人で行っており、１月の依頼退職後も会社がＩＤやパスワードを変更していなかったため、データにアクセスできた。

The SANKEI NEWSより引用
https://www.sankei.com/affairs/news/191125/afr1911250027-n1.html

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

無線LANのセキュリティ

アクセスポイント(無線ルーター）の暗号化は必須

- 社内や自宅で無線LAN(Wi-Fi)を使用している場合
  - 「WPA2」「WPA3」方式で暗号化する（「WPA」は使用不可）
  - 「AES」と「TKIP」を選べるときは「AES」を選択
  - 2019年に 「WPA3」がリリース　対応できるなら「WPA3」を
  - 「WEP」は使用不可

暗号化モード	WPA2 (WPA3)
無線の暗号化	AES

「MACアドレスフィルタ」

社内・自宅の無線LANルーターに「MACアドレスフィルタ」を設定することで、設定した機器以外の接続ができなくなりますのでよりセキュリティが強固になります

無線LANのセキュリティ

アクセスポイント(無線ルーター）の暗号化は必須

- 社内や自宅で無線LAN(Wi-Fi)を使用している場合
  - 「WPA2」「WPA3」方式で暗号化する（「WPA」は使用不可）
  - 「AES」と「TKIP」を選べるときは「AES」を選択
  - 2019年に「WPA3」がリリース　対応できるなら「WPA3」を
  - **「WEP」は使用不可**

士業事務所の電子申請や
企業のEC（ネット通販）サイトは
個人情報のやりとりを含みます
業務を行う端末と無線ルーターは
無線LANの暗号化を忘れずに！

「MACアドレスフィルタ」

事務所・自宅の無線LANルーターに「MACアドレスフィルタ」を設定することで、設定した機器以外の接続ができなくなりますのでよりセキュリティが強固になります

無線LANのセキュリティ

公衆無線LANは原則使用しない

- 公衆無線LANの利用には細心の注意
  - パソコンの「ファイル共有」機能が有効になっていないかチェックを
  - パスワードがなくても使用できる無線LANへの接続は要注意（コンビニの無線等）
  - 通信が暗号化されていないためやりとりの内容が　“まる見え”です。

参考：https://cybersecurity-jp.com/security-measures/22145

ホームページの暗号化

ID・パスワードなどのログイン情報、
クレジットカードや暗証番号といった大切な情報はSSLで

- 信頼できるウェブサイトやサーバーとの間で、インターネット上でデータを暗号化して送受信する方法（SSL：Secure Socket Layer）が有効です。
  - URLが「https」で始まっている。
  - パソコンやスマートフォンのブラウザに「鍵マーク」が表示されている。

あなたの事務所のホームページは https://で始まっていますか？

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

ＰＣ・メモリー紛失・盗難

データ漏えいの脅威はネット上だけではありません！
機器・デバイスの紛失も大きなリスクです

- パソコンをなくしたら…
  - 中のデータすべて見られる（個人情報もすべて）
  - 自動ログインパスワードオートコンプリートでサイトにアクセス可能
    - Facebook, Amazon,楽天, 銀行など自動でログインされてしまう
  - 業務に使っていたデータをすべて失うことも…
  - 最後の砦は、Windowsのログインパスワードだけ…

- USBメモリーをなくしたら
  - 中に入っていた情報が…　（業務上個人情報だと…）
  - 暗号化していなければ筒抜け…

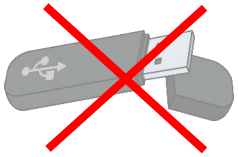
参考：
https://kensawai.com/blog/%e3%83%8e%e3%83%bc%e3%83%88%e3%83%91%e3%82%bd%e3%82%b3%e3%83%b3%e7%9b%97%e9%9b%a3-%e7%b4%9b%e5%a4%b1%e5%af%be%e7%ad%96.html

紛失の対策

転ばぬ先のつえ・考えられる対策はすべて行う
なくしてからでは打つ手が限られてしまいます。

- **持ち出すパソコンには最低限のデータのみ**
  - 個人情報や業務のデータが入ったパソコンは持ち出さない
  - ログインパスワードをかけること（しかし確実ではない）
  - 業務データは必ずバックアップを
  - 持ち出す場合パソコンそのものを暗号化する(TrueCrypt 等)
  - **Windows10/11 Pro**にする（BitLocker-HDDの暗号化搭載）
    https://www.lifehacker.jp/2014/02/140201encryption.html

- **USBメモリーの対策**
  - 暗号化ソフト付USBメモリーを使用する
  - USBメモリーは**原則使用しないこと**
  - 大容量のファイルのやりとりはファイル交換サイト、OneDrive など信頼できるサイトで



box

Dropbox

メールZipper MAIL SECURITY SERVICE

顧問先とのデータ共有・メールの誤送信防止に ファイル交換安心君

OneDrive

USBメモリー暗号化ソフト 「 USBメモリーのセキュリティ」等を使用し暗号化を（フリーソフト）https://www.vector.co.jp/soft/winnt/util/se472154.html **.**

スマホ紛失・盗難

スマホの紛失・盗難は致命的
大量の個人情報、機密情報にアクセス出来るデバイス

- スマホをなくしたら
  - 客先も含め住所録、メールのやりとりなどすべて
  - Line, Facebook, オンラインショッピング、銀行アプリ…
  - 追跡ソフトで追いかけられる場合も…（過信禁物）
  - 最低限画面ロックを！

参考：https://japan.norton.com/smartphone-lose-3112

スマホ紛失のダメージ

スマホは個人情報・個人資産の宝庫
紛失時の対応フローチャートを作り危機管理を！！

- 機能停止画面ロック
- 検索アプリで検索
- 警察へ遺失届
- 回線停止（携帯電話会社に連絡）
- Felica 機能の停止（Suica, ApplePay等非接触決済系）
- メール、SNSなど、スマホ単体でLoginできるアプリのパスワード変更
- 最終手段はリモート（遠隔）オールリセット

参考：https://japan.norton.com/smartphone-lose-3112
https://toyokeizai.net/articles/-/248099

情報セキュリティ規程でスタッフと共有

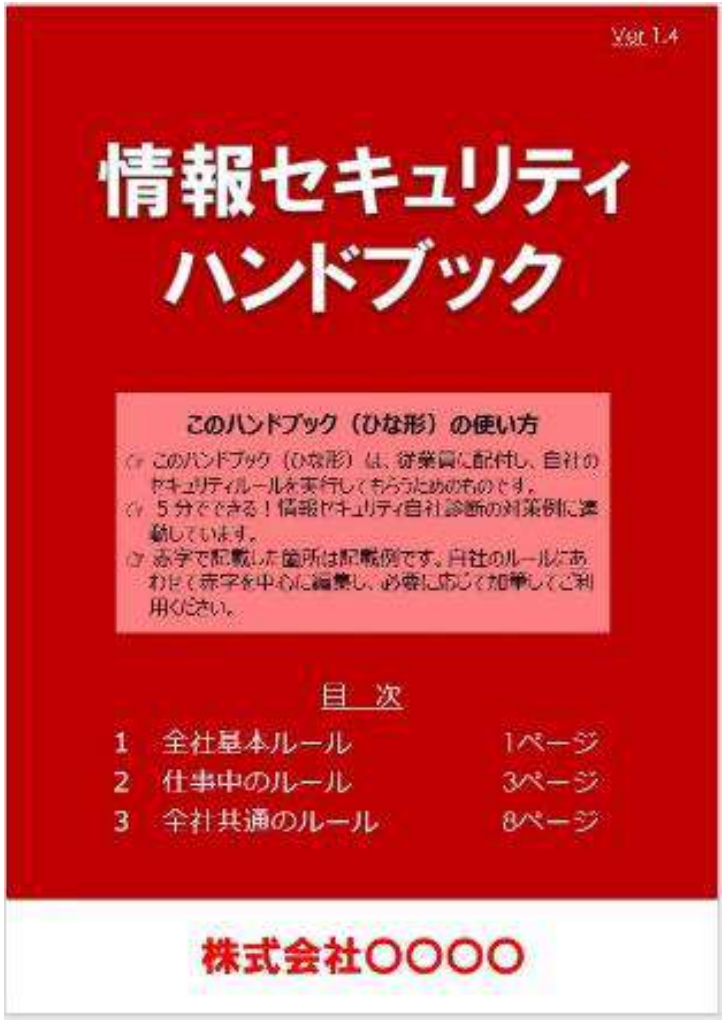
小規事務所・個人事業でも安心できません

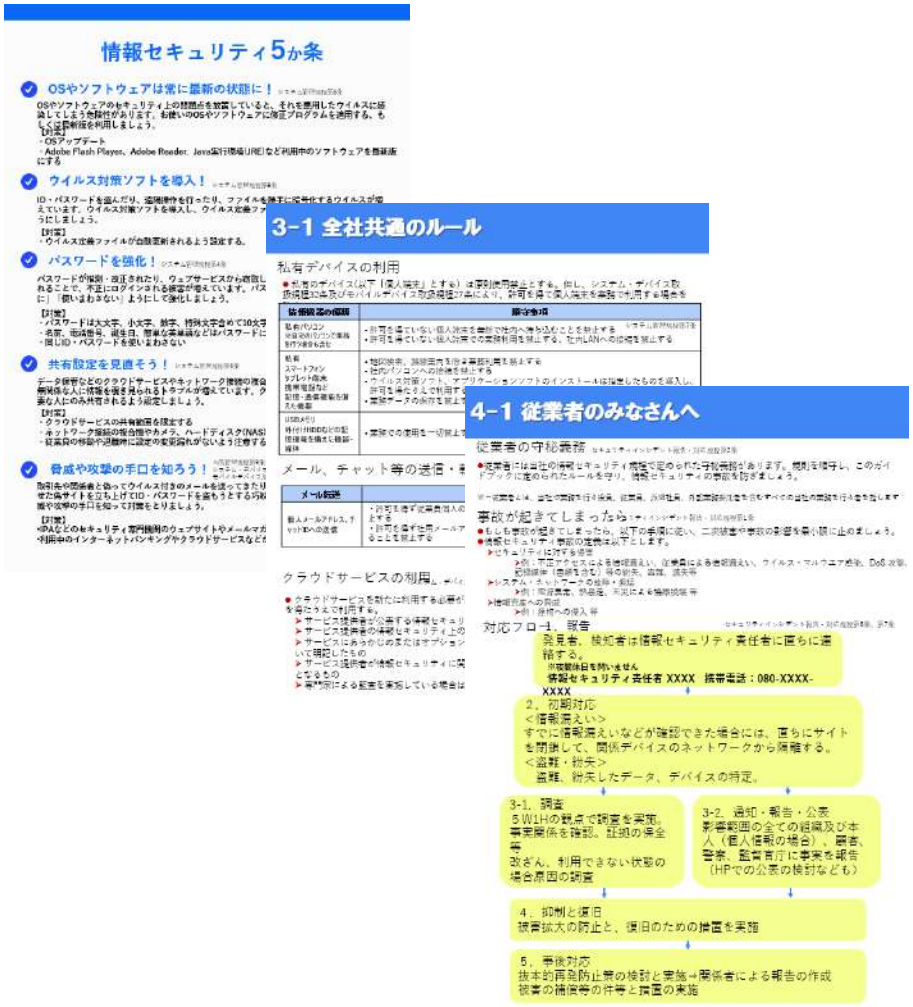
- **情報セキュリティ規程を作成する**
  - 私用で使わない
  - 個人のパソコンは事務所のネットに繋がない
  - 事務所の共有データは、サーバー・クラウドで管理する
  - アクセスできる人を制限する
  - パソコンにスマホを接続しない（スマホはUSBメモリーになります）
  - USBメモリーを使わない
  - 持出専用ノートパソコンを用意する
  - 有事の際の対処方法の明文化
  - 誓約書を準備する
  - ガイドラインを作成する
  - セキュリティ教育の実施

規程の作成・従業員への研修も行っております。お気軽にお訊ねください。
貴事務所のお客様への対応もいたします。

情報セキュリティハンドブック(ルールブック)

平易なわかりやすい言葉で全員に周知しよう





https://www.ipa.go.jp/files/000055529.pptx

クリアデスク・クリアスクリーン

帰宅時に資料や機器を机上に残さない
離席時にパソコンのモニターをロック

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

テレワークのセキュリティのポイント

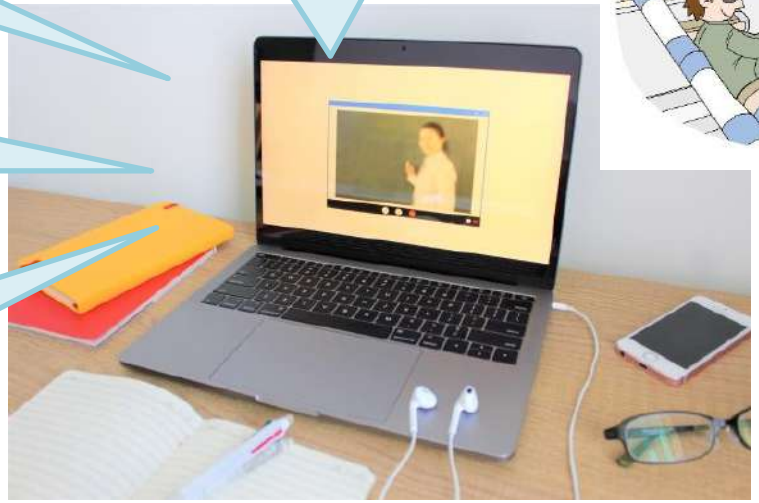
「新しい生活様式」への転換で
テレワーク（在宅勤務）の導入がスピードアップ！

大きく４つの対策を！

ルールによるセキュリティ対策
行動指針やルールの遵守、情報を取り扱う方法の教育・研修など

物理的なセキュリティ対策
防犯対策、書類や端末の収納、紛失防止、のぞき見防止

技術的なセキュリティ対策
ウィルス対策、暗号化、ログインの複雑化など

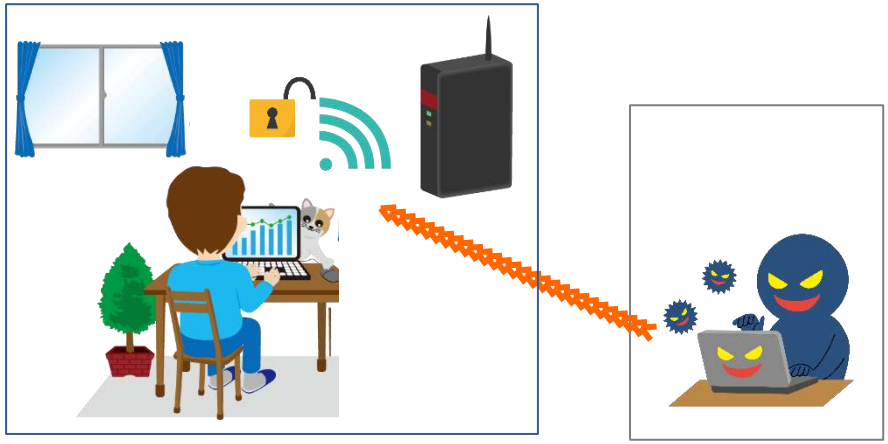


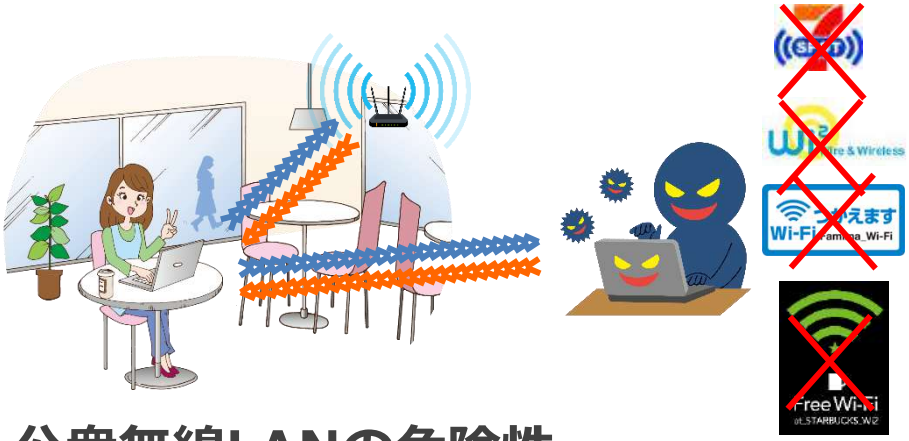
組織的なセキュリティ対策
漏えい発生時の対応手順、連絡方法の策定、安全対策のアップデート

厚労省「テレワークで始める働き方改革」より
https://roumu.com/pdf/nlb0787.pdf

テレワークのセキュリティ（ネット編）

業務で使用するすべてのネット環境の確認
自宅無線LANの暗号化を・公衆無線LANを使用しない





無線LANを暗号化しないと

- 外に漏れる電波を他人がキャッチ
- 通信の内容が漏れる可能性

公衆無線LANの危険性

- 暗号化されていないLANがある
- なりすましアクセスポイントも散見

暗号化の種類

- WPA2（3）方式で暗号化する
- WEP・WPAは使用しない

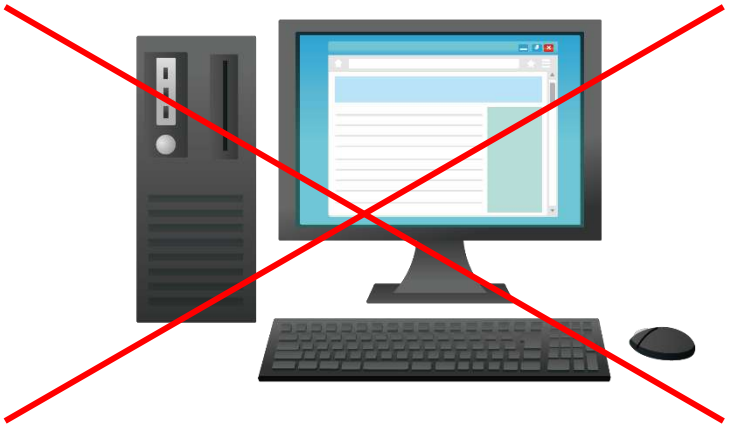
漏えい防止のために

- 公衆無線LANは使用しない
- スマホのテザリング、Wi-Fiルーターを使用

Wi-Fi ルーター　＋　格安SIM　3GB 月850円から

テレワークのセキュリティ（端末編）

パソコン・タブレットは経営者が用意
データ漏えいのリスクの最小化を



経営者が用意するパソコン

- セキュリティが社内と同等
- クラウドへのアクセスに制限
- 使用規程で使い方に制限
- 端末にデータを残さないことで紛失時の影響を最小化
- 使用ログの記録も可能

自宅のパソコンで業務

- セキュリティが個人任せ
- クラウドへのアクセス権の管理不能
- 同居家族のアクセスの可能性
- 過失も含め端末にデータが残されたときの管理ができない
  （紛失時・廃棄時のデータ漏えいの可能性）

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

顧問先、お客さまの安心のために

公的機関の認証取得
事務所の規模に合わせ各種認証の取得で安心を

全国社会保険労務士連合会　SRPII認証　(月刊社労士参照)

社会的にプライバシー保護・個人情報保護に対する意識が高まったことから、 社会保険労務士についても、顧問先等から個人情報の保護について 見える形での運用が求められるようになり、連合会が社会保険労務士独自の 個人情報の保護制度として、SRP認証制度を創設

プライバシーマーク®制度（個人情報保護）

(取得に約6ヶ月、費用は50万円～
https://upfsecurity.co.jp/seminar/)

個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です

JIS Q 15001個人情報保護（個人情報保護）

個人情報保護法・マイナンバー法の順守、業務上取り扱う個人情報の安全かつ適切な管理状況、及び、継続的改善への取り組み状況を客観的に評価するサービスです

ISMS/JIS Q 27001：2014（企業が保護すべき情報資産）http://www.tdb-net.co.jp/iso27001/

情報資産を様々な脅威から守り、リスクを軽減させるための総合的な情報セキュリティ・マネジメントシステムです

https://cybersecurity-jp.com/security-measures/11751

個人情報保護法によりすべての個人情報管理者に適用されています

http://www.soumu.go.jp/main_content/000355092.pdf

SECURITY ACTIONとは

中小企業の「自発的な情報セキュリティ対策」の宣言

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度
「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに２段階の取り組み目標を用意しています。　（情報処理推進機構 IPA）

https://www.ipa.go.jp/security/security-action/

1段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言

2段階目（二つ星）

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言

SECURITY ACTIONの手続き方法

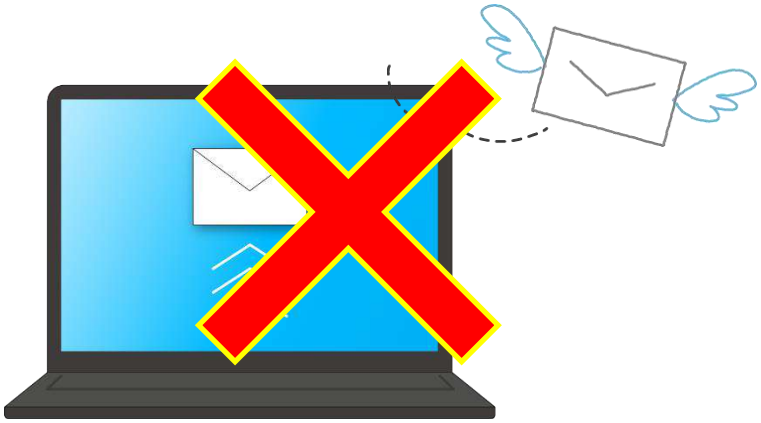
IT補助金・東京都サイバーセキュリティ対策促進助成金の支給要件にも！

https://www.it-hojo.jp/
https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html

マイナンバーをどのように受け渡しをしていますか？

誤送信が発生しても特定個人情報とならない方法など検討

メール・FAXでの受け渡しはダメ！



- 誤送信の発生を防げないこれらの方法はダメ！
- SNSでの送信もダメ！
- 端末にデータが残る方法はダメ！
- 紙での受け渡しもできれば避けたい
- **パスワード付きpdf, Zipは意味なし**
- マイナンバー共有システムの利用
- 分割送信ルールの作成

個人情報保護法改正【2022年4月施行】

個人情報の保護に関する法律等の一部を改正する法律（概要）

■平成27年改正個人情報保護法に設けられた「**いわゆる３年ごと見直し**」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施。

■自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、**今般、個人情報保護法の改正を行い、以下の措置を講ずる**こととしたもの。

改正法の内容

1．個人の権利の在り方

- **利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和**する。
- **保有個人データの開示方法**（※）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

（※）現行は、原則として、書面の交付による方法とされている。

- 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。
- ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。

- **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

3．事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

4．データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した**「仮名加工情報」を創設**し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。
- 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

5．ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

（※）命令違反：6月以下の懲役又は30万円以下の罰金
→ **1年以下の懲役又は100万円以下の罰金**
虚偽報告等：30万円以下の罰金 → **50万円以下の罰金**

- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**（法人重科）。

（※）個人と同額の罰金（50万円又は30万円以下の罰金）→ **1億円以下の罰金**

6．法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。
- 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

※　その他、本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

◇とられて困る情報は持っていない…？
◇業務をパソコン等に依存するときの脅威
◇情報漏えいさせないために
　◇ウイルス防御のために
　◇パスワードの管理
　◇無線LANのセキュリティ
　◇紛失盗難の対策
◇テレワークのセキュリティ
◇お客様・顧問先の安心のために
◇事務所を守るために

事務所を守るために

秘密情報情報・個人情報等の管理方法を定め
社員、職員全員が情報漏えいのリスクを理解し業務に当たること

情報漏えい、その他パソコンの事故・事件は

人災です

- 正しい用法、管理がなければ必ず発生します
- 発生の確率を下げるために、ツールを用意します
- 外部のセキュリティサービスの検討も
- セキュリティ対策に十分なコストの割り当てを

外部セキュリティサービスの例
https://business.ntt-east.co.jp/service/security.html

情報漏えいは人の問題

最もセキュリティが脆弱なのは”人“
あなた自身が情報漏えいに対して
知識をしっかり持っておくことが重要

最後に…社労士業界の地位向上のためにも

お客様の大切な個人情報・企業情報を扱う士業など
関与先企業のひとつ上を行く情報セキュリティを目指しましょう！

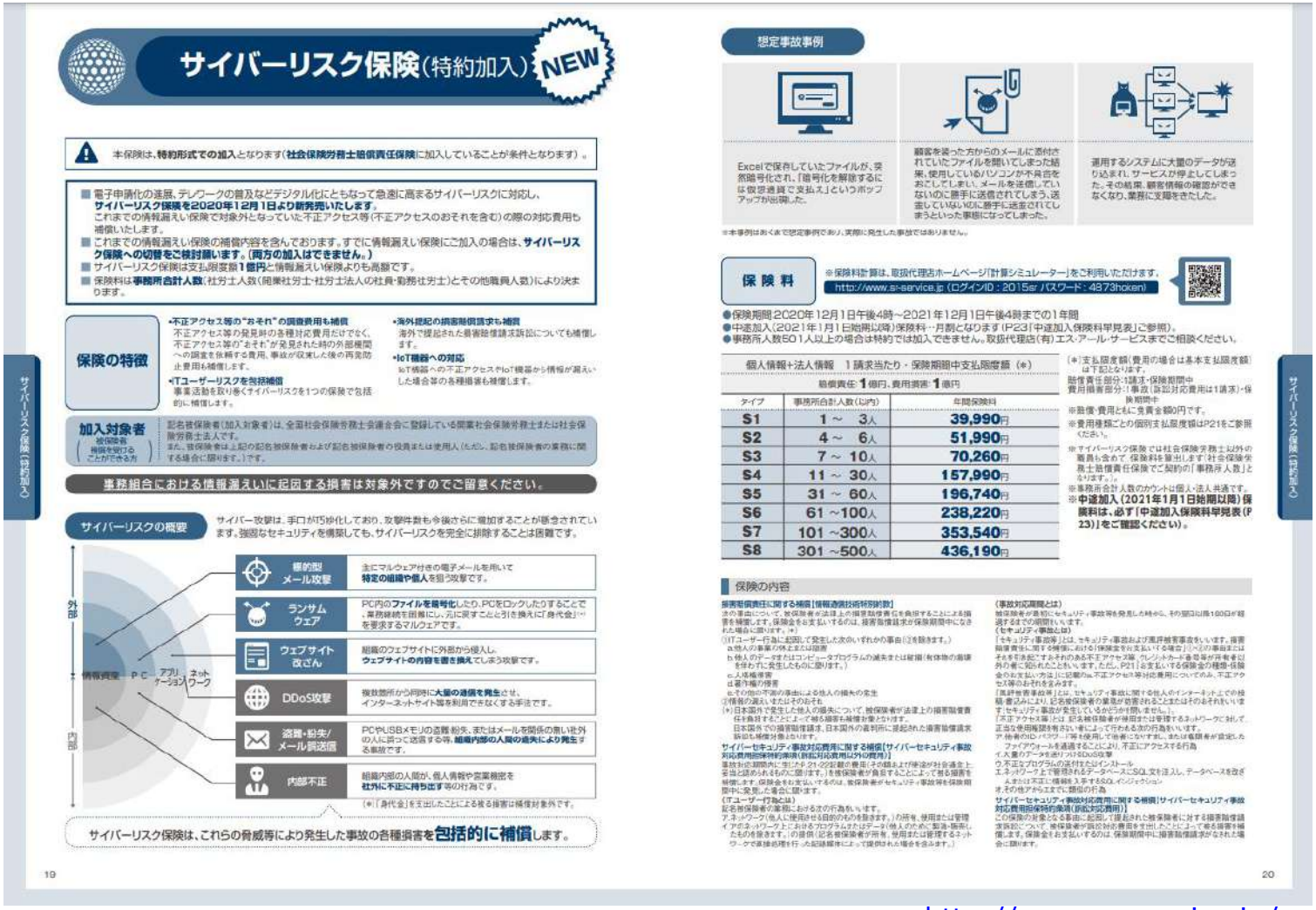
セキュリティ対策はコストです

しかし起こるべきリスクに先回りし
そのコストを払うことは
最終的に事務所を守ります

情報セキュリティの強化は社労士業界の地位向上にも結びつきます

事務所を守るために

情報漏えい保険・サイバーリスク保険への加入



サイバーリスク保険（特約加入）NEW

本保険は、**特約形式での加入**となります（**社会保険労務士賠償責任保険**に加入していることが条件となります）。

- 電子申請化の進展、テレワークの普及などデジタル化にともなって急速に高まるサイバーリスクに対応し、**サイバーリスク保険を2020年12月1日より新発売いたします。**
  これまでの情報漏えい保険で対象外となっていた不正アクセス等（不正アクセスのおそれを含む）の際の対応費用も補償いたします。
- これまでの情報漏えい保険の補償内容を含んでおります。すでに情報漏えい保険にご加入の場合は、**サイバーリスク保険への切替をご検討願います。（両方の加入はできません。）**
- サイバーリスク保険は支払限度額**1億円**と情報漏えい保険よりも高額です。
- 保険料は**事務所合計人数**（社労士人数（開業社労士・社労士法人の社員・勤務社労士）とその他職員人数）により決まります。

保険の特徴

- **不正アクセス等の"おそれ"の調査費用も補償**
  不正アクセス等の発見時の各種対応費用だけでなく、不正アクセス等の"おそれ"が発見された時の外部機関への調査を依頼する費用、事故が収束した後の再発防止費用も補償します。
- **ITユーザーリスクを包括補償**
  事業活動を取り巻くサイバーリスクを1つの保険で包括的に補償します。
- **海外提起の損害賠償請求も補償**
  海外で提起された損害賠償請求訴訟についても補償します。
- **IoT機器への対応**
  IoT機器への不正アクセスやIoT機器から情報が漏えいした場合等の各種損害も補償します。

加入対象者（被保険者 補償を受けることができる方）

記名被保険者（加入対象者）は、全国社会保険労務士会連合会に登録している開業社会保険労務士または社会保険労務士法人です。
また、被保険者は上記の記名被保険者および記名被保険者の役員または使用人（ただし、記名被保険者の業務に関する場合に限ります。）です。

事務組合における情報漏えいに起因する損害は対象外ですのでご留意ください。

サイバーリスクの概要

サイバー攻撃は、手口が巧妙化しており、攻撃件数も今後さらに増加することが懸念されています。強固なセキュリティを構築しても、サイバーリスクを完全に排除することは困難です。

標的型メール攻撃	主にマルウェア付きの電子メールを用いて**特定の組織や個人**を狙う攻撃です。
ランサムウェア	PC内の**ファイルを暗号化**したり、PCをロックしたりすることで、業務継続を困難にし、元に戻すことと引き換えに「身代金」※を要求するマルウェアです。
ウェブサイト改ざん	組織のウェブサイトに外部から侵入し、**ウェブサイトの内容を書き換え**てしまう攻撃です。
DDoS攻撃	複数箇所から同時に**大量の通信を発生**させ、インターネットサイト等を利用できなくする手法です。
盗難・紛失/メール誤送信	PCやUSBメモリの盗難・紛失、またはメールを関係の無い社外の人に誤って送信する等、**組織内部の人間の過失により発生**する事故です。
内部不正	組織内部の人間が、個人情報や営業機密を**社外に不正に持ち出す**等の行為です。

（※「身代金」を支出したことによる損害は補償対象外です。）

サイバーリスク保険は、これらの脅威等により発生した事故の各種損害を包括的に補償します。

19

想定事故事例

Excelで保存していたファイルが、突然暗号化され、「暗号化を解除するには仮想通貨で支払え」というポップアップが出現した。

顧客を装った方からのメールに添付されていたファイルを開いてしまった結果、使用しているパソコンが不具合をおこしてしまい、メールを送信していないのに勝手に送信されてしまう、送金していないのに勝手に送金されてしまうといった事態になってしまった。

運用するシステムに大量のデータが送り込まれ、サービスが停止してしまった。その結果、顧客情報の確認ができなくなり、業務に支障をきたした。

※本事例はあくまで想定事例であり、実際に発生した事故ではありません。

保険料

※保険料計算は、取扱代理店ホームページ「計算シミュレーター」をご利用いただけます。
http://www.sr-service.jp（ログインID：2015sr パスワード：4873hoken）

- 保険期間2020年12月1日午後4時～2021年12月1日午後4時までの1年間
- 中途加入（2021年1月1日始期以降）保険料…月割となります（P23「中途加入保険料早見表」ご参照）。
- 事務所人数50人以上の場合は特約では加入できません。取扱代理店（有）エス・アール・サービスまでご相談ください。

個人情報＋法人情報　1請求当たり・保険期間中支払限度額（※）
賠償責任 1億円、費用損害 1億円

タイプ	事務所合計人数（L内）	年間保険料
S1	1 ～ 3人	39,990円
S2	4 ～ 6人	51,990円
S3	7 ～ 10人	70,260円
S4	11 ～ 30人	157,990円
S5	31 ～ 60人	196,740円
S6	61 ～100人	238,220円
S7	101 ～300人	353,540円
S8	301 ～500人	436,190円

（※）支払限度額（費用の場合は基本支払限度額）は下記となります。
賠償責任部分：1請求・保険期間中
費用損害部分：1事故（非訟対応費用は1請求）・保険期間中
※賠償・費用ともに免責金額0円です。
※費用種類ごとの個別支払限度額はP21をご参照ください。
※サイバーリスク保険では社会保険労務士以外の職員も含めて 保険料を算出します（社会保険労務士賠償責任保険でご契約の「事務所人数」とならいます。）。
※事務所合計人数のカウントは個人・法人共通です。
※中途加入（2021年1月1日始期以降）保険料は、必ず「中途加入保険料早見表（P23）」をご確認ください。

保険の内容

損害賠償責任に関する補償【情報通信技術特別約款】
次の事由について、被保険者が法律上の損害賠償責任を負担することによる損害を補償します。保険金をお支払いするのは、損害賠償請求が保険期間中になされた場合に限ります。（※）
（ITユーザー行為に起因して発生した次のいずれかの事由（②を除きます。）
a.他人の事業の休止または阻害
b.他人のデータまたはコンピュータプログラムの滅失または破損（有体物の毀損を伴わずに発生したものに限ります。）
c.人格権侵害
d.著作権の侵害
e.その他の不測の事由による他人の損失の発生
②情報の漏えいまたはそのおそれ
（※）日本国外で発生した他人の損失について、被保険者が法律上の損害賠償責任を負担するごとによって被る損害を補償対象とはいたします。
日本国外での損害賠償請求、日本国外の裁判所に提起された損害賠償請求訴訟も補償対象とはいたします。

サイバーセキュリティ事故対応費用に関する補償【サイバーセキュリティ事故対応費用担保特約条項（訴訟対応費用以外の費用）】
事故対応期間内に生じた P.21-2②記載の費用（その額および使途が社会通念上妥当と認められるものに限ります。）を被保険者が負担することによって被る損害を補償します。保険金をお支払いするのは、被保険者がセキュリティ事故対応期間中に発見した場合に限ります。
（ITユーザー行為など）
記名被保険者の業務における次の行為をいいます。
ア.ネットワーク（他人に使用させる目的のものを除きます。）の将有、使用または管理
イ.アのネットワーク上におけるプログラムまたはデータ（他人のために製造・販売したものを除きます。）の提供（記名被保険者が所有、使用または管理するネットワークで直接処理を行った記録媒体によって提供された場合を含みます。）

（事故対応期間とは）
被保険者が最初にセキュリティ事故等を発見した時から、その翌日以降180日が経過するまでの期間をいいます。
（セキュリティ事故とは）
「セキュリティ事故等」とは、セキュリティ事故および風評被害事故をいいます。損害賠償責任に関する補償において保険金をお支払いする場合」とペアの事故または それを可能にするおそれのある不正アクセス等、クレジットカード番号等が所有者以外の者に知れたことをいいます。ただし、P21「お支払いする保険金の種類・保険金のお支払い方法」に記載のIoT不正アクセス等対応費用についてのみ、不正アクセスと等のおそれを含みます。
「風評被害事故等」とは、セキュリティ事故に関する他人のインターネット上での投稿・書込みにより、記名被保険者の業務が妨害されることまたはそのおそれをいいます（セキュリティ事故が発生しているかどうか問いません。）。
「不正アクセス等」とは、記名被保険者が使用または管理するネットワークに対して正当な使用権限を有さない者によって行われる次の行為をいいます。
ア.他者のID・パスワード等を使用して他者になりすまし、または権限者が設定したファイアウォールを通過することにより、不正にアクセスする行為
イ.入力データを送りつけるDoS攻撃
ウ.不正なプログラムの送付またはインストール
エ.ネットワーク上で管理されるデータベースにSQL文を注入し、データベースを改ざんまたは不正に情報を入手するSQLインジェクション
オ.その他アからエまでに類似の行為

サイバーセキュリティ事故対応費用に関する補償【サイバーセキュリティ事故対応費用担保特約条項（訴訟対応費用）】
この保険の対象となる事由に起因して提起された被保険者に対する損害賠償請求訴訟について、被保険者が訴訟対応費用を支出したことによって被る損害を補償します。保険金をお支払いするのは、保険期間中に損害賠償請求がなされた場合に限ります。

20

５分でできる自社診断シートで確認してみましょう

25問のチェック項目を回答し１００点満点を目指しましょう

お客様の情報が漏洩してしまい大ニュースに。会社の信用が急降下！

お客様にウィルス付のメールを送信してしまい、取引停止の危機！

新製品に関するデータが紛失。発売が大幅延期により売上に影響が。

100点満点だった方	入門レベルのセキュリティ対策はもう完璧です。ステップアップを検討しましょう。	「中小企業の情報セキュリティ対策ガイドライン」とその付録3を参照して、情報セキュリティ対策の強化に取り組みましょう。
70～99点だった方	ほぼ、出来ていますが、部分的に対策が不十分な点があるようです。	小さな隙間から情報が漏えいすることもあります。100点満点を目指しつつ、「中小企業の情報セキュリティ対策ガイドライン」とその付録3に取り組みましょう。
50～69点だった方	対策が行き届いていないところが目立ちます。	「5分でできる！情報セキュリティ自社診断パンフレット」で点数が低かった項目を見直し、対策を施しましょう。
49点以下だった方	いつ情報流出などの事故が起きても不思議ではありません。	「5分でできる！情報セキュリティ自社診断パンフレット」や「対策のしおり」「映像で知る情報セキュリティ」を利用して、分からなかった部分や点数が低かった項目を確認し、対策を施しましょう。

説明サイト https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html

診断シート https://www.ipa.go.jp/files/000055848.pdf

※ほとんどの対策は費用不要

最後に…　まずはここから

まずはここから、今日から始めましょう！

情報セキュリティ５ヶ条

1．OSやソフトウェアは常に最新状態にしよう！
2．ウイルス対策ソフトを導入しよう！
3．パスワードを強化しよう！
4．共有設定を見直そう！
5．脅威や攻撃の手口を知ろう！

https://www.ipa.go.jp/files/000055516.pdf

OS・ソフトの更新

1．今すぐWindows 7の即時停止を！
2．今すぐOffice 2010のアップデートを！
3．**Internet Explorerの使用停止準備を！**

そして一呼吸

1．メールを開く前に
2．添付ファイルを開く前に
3．URLをクリックする前に
4．USBを挿す前に
5．SMSを見る前に

その他参考サイト1

独立行政法人情報処理推進機構（IPA）
情報セキュリティ啓蒙全般
https://www.ipa.go.jp/security/keihatsu/features.html
日常における情報セキュリティ対策
https://www.ipa.go.jp/security/measures/everyday.html
「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル
https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html
「ここからセキュリティ」
https://www.ipa.go.jp/security/kokokara/

内閣サイバーセキュリティセンター　NISC
https://www.nisc.go.jp/

日本ネットワークセキュリティ協会　JNSA
https://www.jnsa.org/

これだけはやっておきたい！「無線LAN情報セキュリティ3つの約束」
https://www.gov-online.go.jp/useful/article/201303/1.html

中小企業情報セキュリティ.com
https://xn--dckta5b5b2j4a3878bqnb245b20icpn0jz.com/

個人情報保護委員会
https://www.ppc.go.jp/personalinfo/

マイクロソフト「自宅でコンピューターをセキュリティ保護する」
https://support.microsoft.com/ja-jp/help/4092060/windows-keep-your-computer-secure-at-home

その他参考サイト2

総務省テレワーク情報サイト
https://telework.soumu.go.jp/
https://www.soumu.go.jp/main_content/000752925.pdf（テレワークセキュリティガイドライン第5版）

総務省「国民のための情報セキュリティサイト」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

総務省「一般利用者が安心して無線LANを利用するために」
https://www.soumu.go.jp/main_content/000199322.pdf

総務省「企業等が安心して無線LANを導入・運用するために」
https://www.soumu.go.jp/main_content/000199323.pdf

「個人情報」と「特定個人情報」～正しい理解のために～（令和4年4月）
https://www.ppc.go.jp/files/pdf/tadashiirikai_kojin_tokutei.pdf

個人事務所、中小企業向けセキュリティ対策
https://www.sharingof.com/sec01.html
https://www.otsuka-shokai.co.jp/solution/keyword/security/

UTMとは
http://www.hs-juniperproducts.jp/check/utm.html

自己紹介

経済産業大臣認定経営革新等支援機関
社会保険労務士事務所 フェリシアンス®
株式会社 フェリシアンス®

代表 堀 川 眞 也 https://feliciance-sr.com/

～幸せ働き方講師®～

◇プロフィール 従業員も経営者も『ずっとハッピー』を目指します！

社会保険労務士事務所フェリシアンス代表
大阪府生まれ。外資系、日系メーカーの合計３社で、３２年の会社員経験を経て独立開業する。会社員時代、１１０回の海外出張、２２カ国を訪問、１５００日以上海外に滞在。製品設計のため６か国のメンバーと一緒にプロジェクトを行った経験から、グローバルコミュニケーションを得意とする。海外での経験を活かし、社会保険労務士として、またキャリアコンサルタントとして外国人雇用、LGBTQの就労支援、企業内の異文化理解醸成などを行う。
「幸せに働けること、働く事で幸せに」という信念のもと、すべての人が働きやすい環境作りのため奔走している。

ホメホメ英語トランプ

◇保有資格

特定社会保険労務士・医療労務コンサルタント®
国家資格キャリアコンサルタント （CDA）
２級ファイナンシャル・プランニング技能士
メンタルヘルスマネジメント検定Ⅱ種（ラインケアコース）
両立支援コーディネーター
神奈川産保センター両立支援促進員
健康経営アドバイザー・パワハラ予防士
TOEIC 815点・紙芝居型講師
「褒め言葉カード」セミナーアドバンスインストラクター
キャリア・シフトチェンジワークショップインストラクター
情報処理推進機構セキュリティプレゼンター
大型自動二輪運転免許・第2級アマチュア無線技士

日本法令 DVD
2022/12/12発売！
Amazonで購入できます

パワハラ予防士
幸せと信頼の「フェリシアンス」
～幸せ働き方講師～
褒め言葉英語カードマスターインストラクター
特定社会保険労務士・キャリアコンサルタント

代表 堀 川 眞 也
社会保険労務士事務所 フェリシアンス
株式会社 フェリシアンス 代表取締役
222-0033 横浜市港北区新横浜3-7-18 日総第18ビル508
TEL 045-594-9420 FAX 045-345-8543
✉ info@feliciance-sr.com
https://www.feliciance-sr.com/

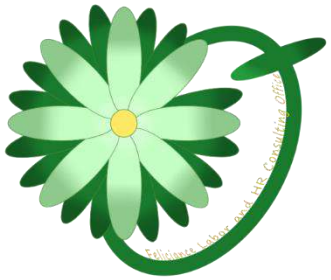
事務所名由来

フェリシアンス （Feliciance）は、フランス語で「幸せ」や「幸福」を意味する『félicité』と「信頼」や「信用」を意味する『confiance』から作られた造語です。

人生の中で仕事が占める割合は大変大きいものです。
私たちは社会保険労務士の業として、働く「よろこび」を感じていただきたい、仕事を通して幸せになって欲しいという願いがあります。
その為に私たちは皆様に愛され信頼を得るという決意を込め「フェリシアンス」と名付けました。

企業の継続や発展は人があってこそ。
その為には従業員も経営者もどちらも幸せになる必要があると思っています。
フェリシアンスは従業員も経営者も「ずっとハッピー」を目指します。

Feliciance		
felicite	félicité	幸い 幸福
confiance	confiance	信頼 信用 信任 信託



「フェリシアンス」とロゴマークは登録商標です
（登録商標第6025521号、第6025522号）

花のモチーフは「福寿草」
花言葉に『幸福を招く』や『永久の幸福』という意味があります。
24枚の花弁は、24時間と二十四節気を表し、一日、一年を積み重ね福寿草の花言葉である『永久の幸福』を意味し、色は宝石である「クロムダイオプサイド」の色をイメージしています。

このクロムダイオプサイドというのは、ダイオプサイドの中でもクロムを発色要因とするもので、元になっているダイオプサイドに『信頼』という意味が込められています。
また、すべて円の図形で花を作ったことにより、「人とのたくさんの縁が繋がっていきますように」という願いを込めました。
そして花弁の一枚を茎の上に重ねることで「Feliciance」のFを表現しています。