令和4年度 コンプライアンス勉強会

独立行政法人情報処理推進機構(IPA)
セキュリティセンター
研究員　佐藤　裕一

情報処理推進機構(IPA)のご紹介

- 日本のIT国家戦略を技術面、人材面から支えるために設立された、経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる“**頼れるIT社会**”の実現を目指しています

IPA　検索

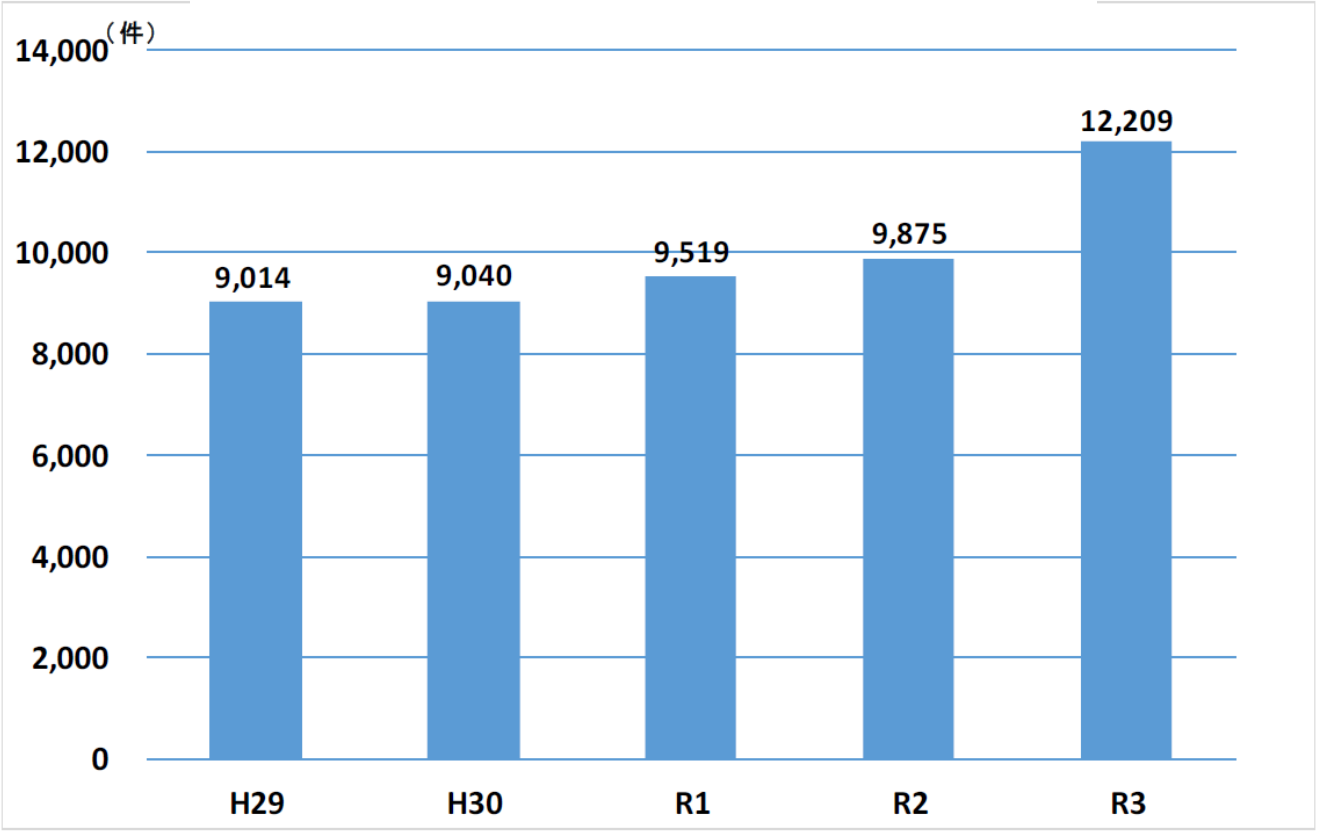
脅威にさらされている中小企業の実態

サイバー犯罪の情勢等

出典：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」

- 2022年4月、警察庁が**「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」**を公開。
- 令和3年中の**サイバー犯罪の検挙件数が12,209件と過去最高**を記録。

＜サイバー犯罪の検挙件数の推移＞



サイバー犯罪の情勢等

出典：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」

＜ダークウェブ上のリークサイト例＞

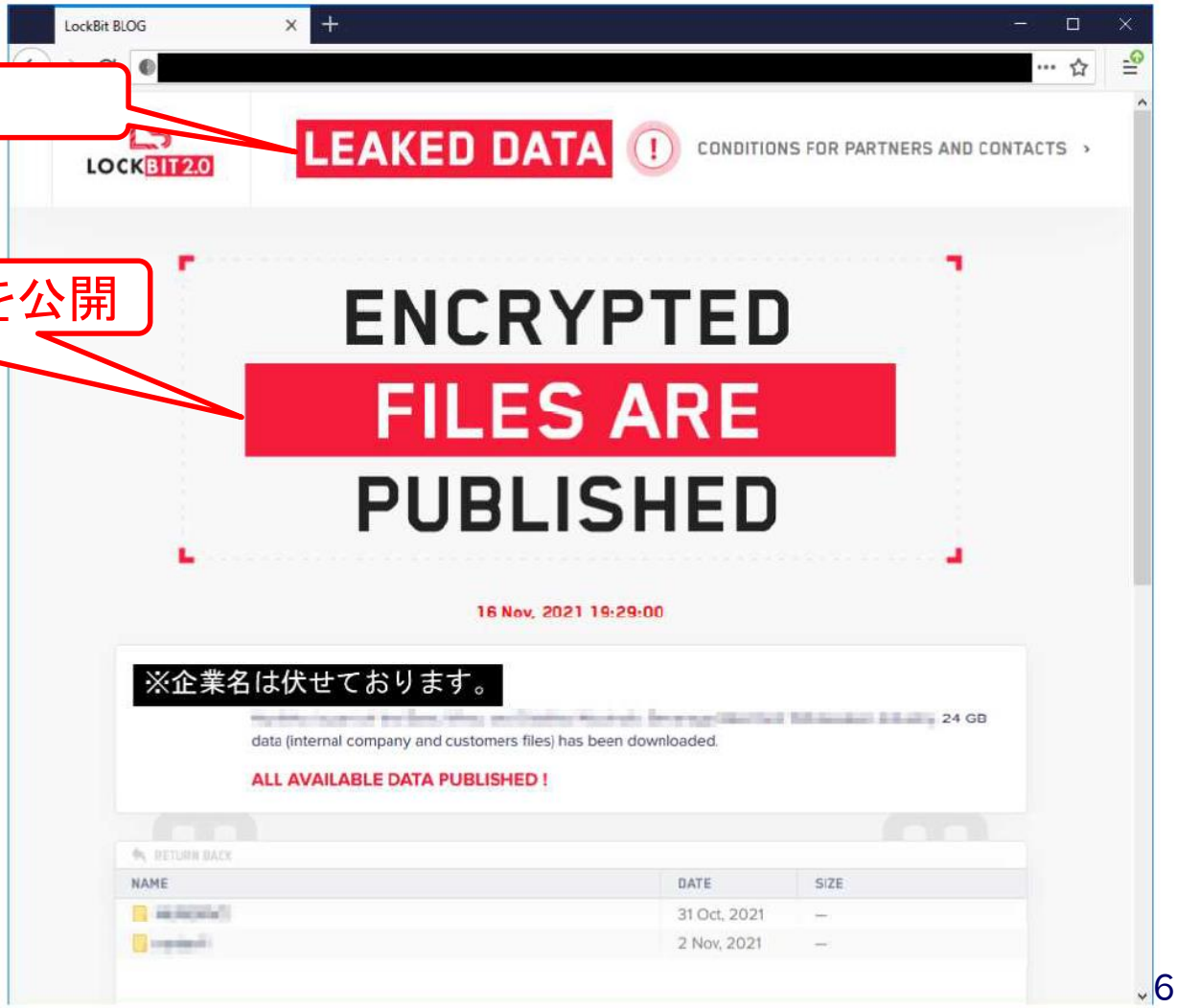
サイバー犯罪の情勢等

出典：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」

＜ダークウェブ上のリークサイト例＞

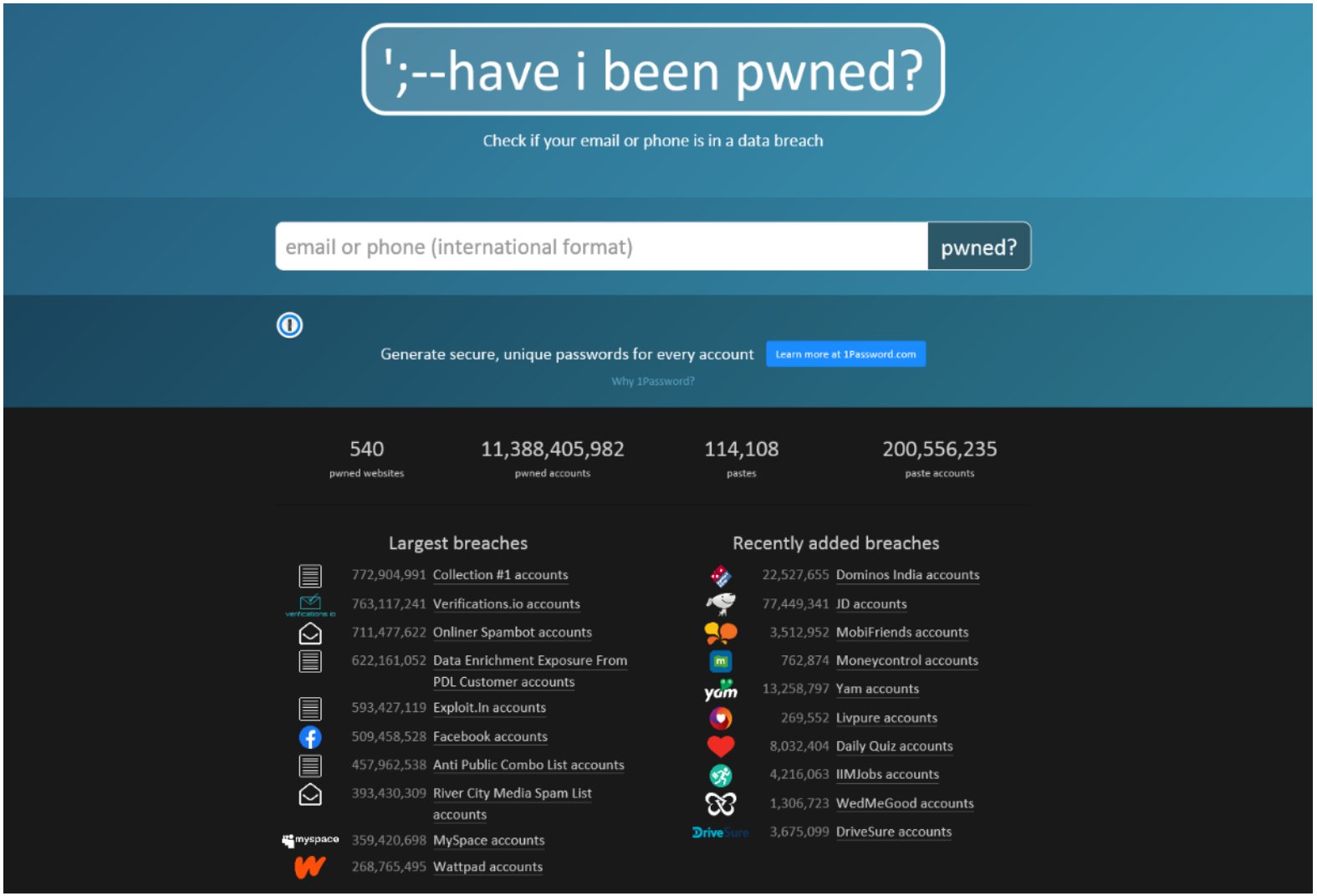
漏えいしたデータ

暗号化されたファイルを公開



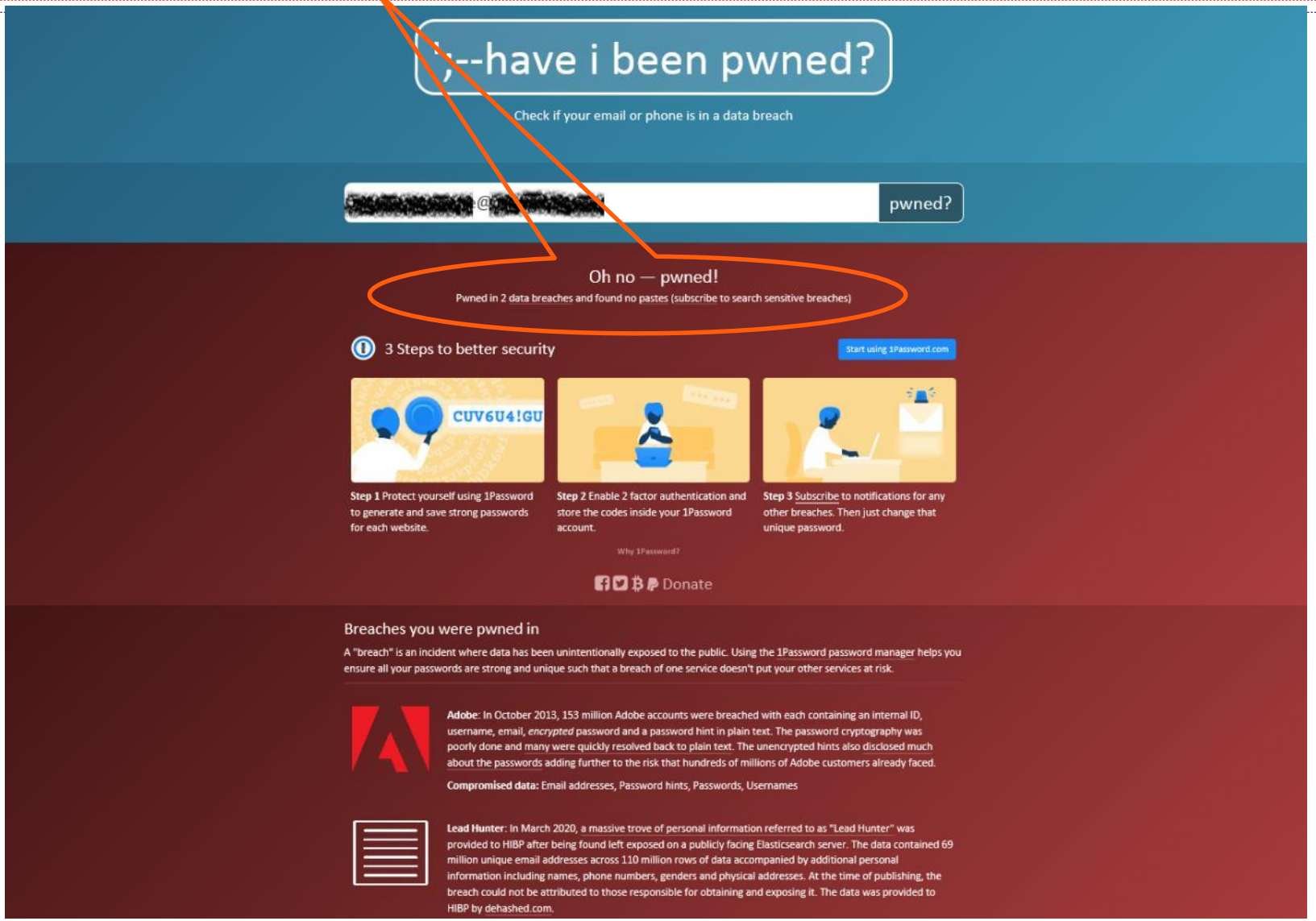
メールアドレス・パスワードが流出しているか確認できるサイト

https://haveibeenpwned.com/



Oh no – pwned!

Pwned in 2data breaches and found no pastes (subscribe to search sensitive breaches)



情報セキュリティ10大脅威2022

「情報セキュリティ10大脅威」とは？

https://www.ipa.go.jp/security/vuln/10threats2022.html?topbana

- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等からIPAが脅威候補を選出
- セキュリティ専門家や企業のシステム担当等から構成される「10大脅威選考会」が投票
- TOP10入りした脅威を「10大脅威」として脅威の概要、被害事例、対策方法等を解説

10大脅威の特徴

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人 **「個人」**

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員 **「組織」**

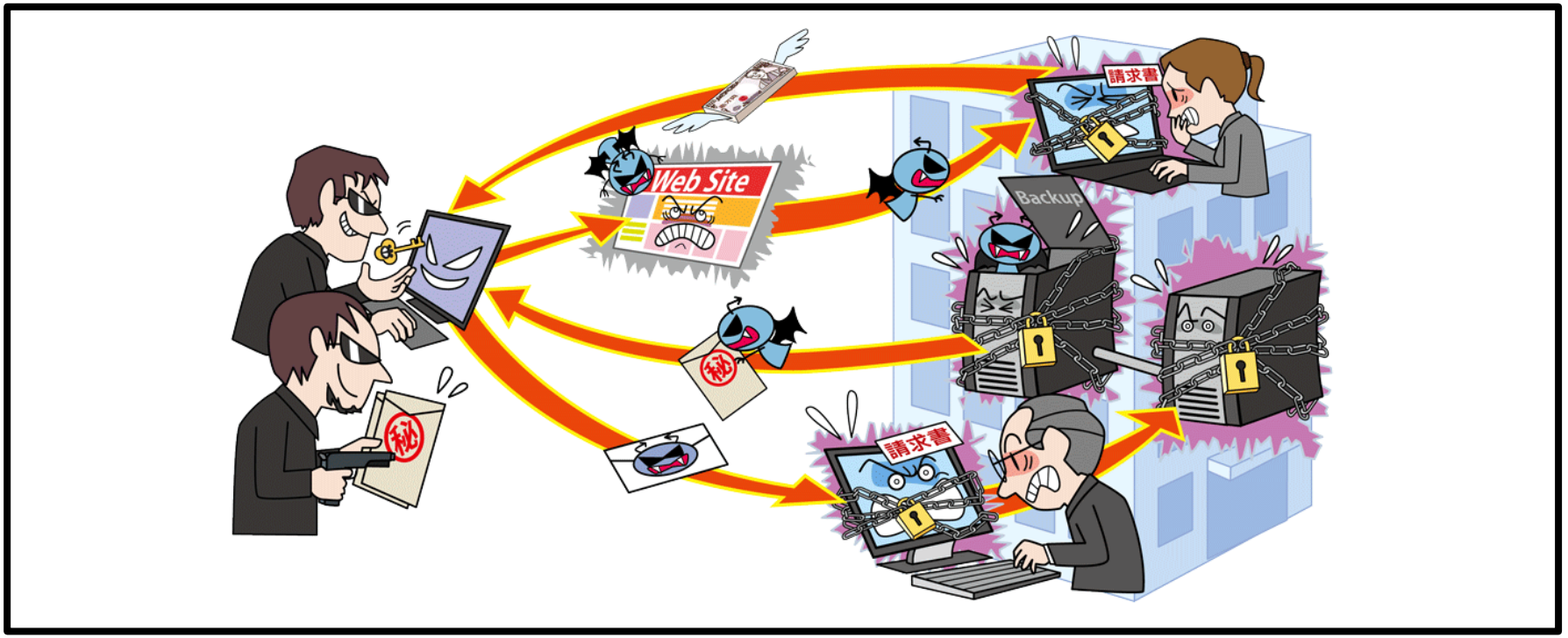
「個人」と「組織」の2つの立場で脅威を解説

情報セキュリティ10大脅威 2022 脅威ランキング

IPA

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	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	9	予期せぬIT基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～



- PC等に保存されているファイルを暗号化され使用不可に
- 復旧と引き換えに金銭を要求される
- 情報を窃取しそれを公開すると脅迫するケースも

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

● 攻撃手口

・ウイルス（ランサムウェア）に感染させて金銭を要求

- **メールを利用した手口**
  - **・不正な添付ファイルを開かせる**
  - **・メール内のリンクをクリックさせる**
- **ウェブサイトを利用した手口**
  - **・ランサムウェアをダウンロードさせるようにウェブサイトを改ざん**
  - **・当該サイトを閲覧するようにメール等で誘導**

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

攻撃手口

・ウイルス（ランサムウェア）に感染させて金銭を要求

脆弱性を悪用した手口

- ソフトウェアの**脆弱性を悪用**しウイルスを実行（感染させる）
- 攻撃ツール等を利用して**ネットワーク越しに次々と感染**させる

不正アクセスによる手口

- 管理用のRDP（リモートデスクトップ）等で**サーバーに不正アクセス**
- サーバー上で攻撃者がウイルスを実行（感染させる）

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

- **2021年の事例/傾向①**
  - **病院へのランサムウェア攻撃** (※1)

    ・2021年10月、病院のシステムがランサムウェアに感染し電子カルテや会計システムにアクセスできなくなる等の被害

    ・暗号化解除と引き換えに身代金を要求されたが応じず

    ・システム復旧まで新規患者の受け入れを中止する等の影響

    ・2022年1月、通常診療を再開

【出典】
※1 サイバー攻撃受けた徳島・半田病院 約2カ月ぶりに通常診療全面再開（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASQ145J9MQ13PTLCOOP.html

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

- **2021年の事例/傾向②**
  - **バックアップの暗号化による被害の長期化** **（※1）**
    - **製粉会社にサイバー攻撃により、ランサムウェアに感染**
    - **システムのオンラインバックアップを管理していたサーバーも暗号化**
    - **早期復旧が困難となり四半期決算報告書の提出にも影響**

【出典】
※1 2022 年 3 月期第 1 四半期報告書の提出期限延長に関する承認申請書提出のお知らせ（株式会社ニップン）
https://www.nippn.co.jp/topics/detail/_icsFiles/afieldfile/2021/08/16/20210816-1.pdf

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

● 対策

■ 経営者層

- 組織としての対応体制の確立
  - 対策の予算の確保と継続的な対策の実施
  - CIO など専門知識を持つ責任者を配置

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

● 対策

■ システム管理者、従業員

- ・被害の予防
  - －迅速、継続的に対応できる体制（CSIRT等）の構築
  - －多要素認証の設定を有効にする
  - －添付ファイルやリンクを安易にクリックしない
  - －提供元が不明なソフトウェアを実行しない
  - －機器の脆弱性対策を迅速に行う
    - －パッチ適用を迅速に行う
    - －サポート切れのOSは利用停止
  - －セキュリティ対策ツールの利用や設定見直し
    - －アプリケーション実行制限や、メールおよびウェブのフィルタリング
    - －ポリシー設定を見直し、遮断設定を極力有効にする

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

● 対策

■ システム管理者、従業員

・被害の予防

- 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と管理の強化
- 公開サーバーへの不正アクセス対策
- バックアップの取得

※3-2-1 バックアップルールを参考にバックアップを検討

※バックアップから復旧できることを定期的に確認

【1位】ランサムウェアによる被害
～社会インフラに大きな影響が出る場合も～

IPA

● 対策

■ システム管理者、従業員

・被害を受けた後の対応

－組織の方針に従い各所へ報告、相談する

※上司、CSIRT、関係組織、公的機関等

－バックアップからの復旧

－復号ツールの活用

－影響調査および原因の追究、対策の強化

－迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外ケース＞

推奨はされないが、過去には、組織の事情（暗号化されたファイルが人命に関わる場合等）により、金銭を支払ったケースもあった

電子カルテがランサムウェアに感染

NHK　Webサイト「サイカル」から

病院がサイバー攻撃を受けたとき 消えた電子カルテの衝撃

2021.11.19：#サイバーセキュリティ／#マルウエア／#医療／#ＩＴ・ネット

戸惑う医師たち。日本の地方病院が、サイバー攻撃にやられた。
Ｘ線の画像、投薬の記録、8万5000人分の患者の電子カルテが、失われてしまった。
災害と同様の非常事態宣言を発した病院。不安を隠さない患者たち。
人々の命を守る病院が、ハッカーに狙われたとき、何が起きるのか。

未明の衝撃 “電子カルテが使えない”

衆議院議員選挙の投開票日の10月31日。
未明に事件は起きていた。

およそ8000人が暮らす徳島県西部の山あいのつるぎ町。町の医療を支える町立半田病院の当直勤務に当たっていた看護師、寒川忍さんは、突然、院内のプリンターが、けたたましく動き出したことに驚いた。

はき出されてきた紙には、英文やＵＲＬが印刷されていた。

「あなたたちのデータは盗まれ、暗号化された」

病院も対策をとっていなかったわけではない。

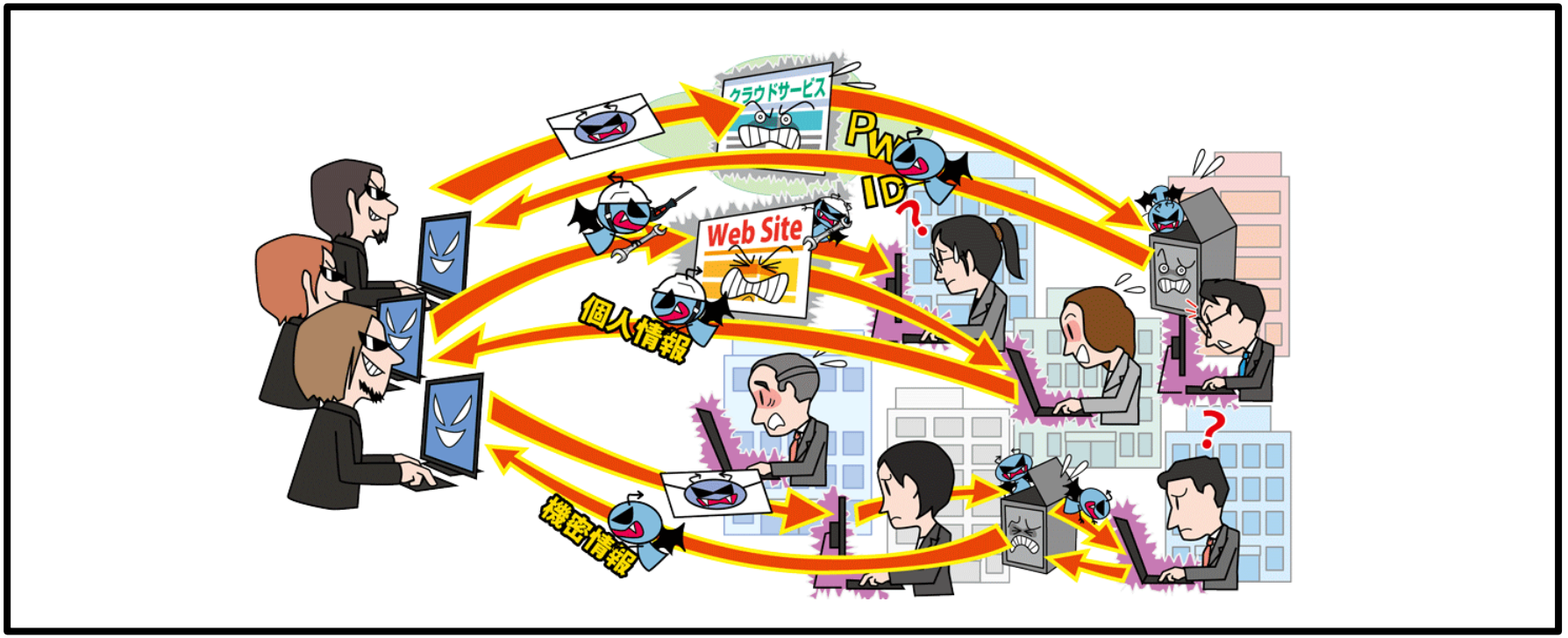
電子カルテなどのデータが失われないよう、バックアップ用のサーバーを設置していた。しかし、これもウイルスに感染してしまった。

丸笹寿也事務長は「システムを構築したときにサイバーテロまで想定していなかった」と明かす。

バックアップサーバーは、あくまで地震や水害などでメインのサーバーが壊れた場合の予備で、高い場所に設置していたが、サイバー攻撃から守る仕組みにはなっていなかった。

【2位】標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～



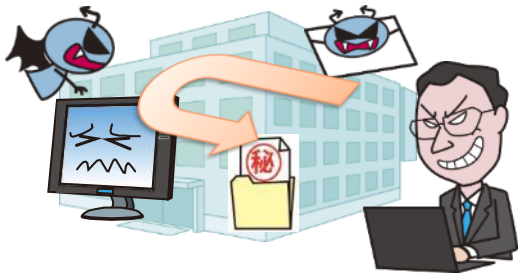
- **メール等を利用し特定組織のPCをウイルスに感染させる**
- **組織内部に潜入し長期にわたり侵害範囲を徐々に広げる**
- **組織の機密情報窃取やシステムの破壊を行う**

【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

● 攻撃手口

・メールやウェブサイトからウイルスに感染させる

- **メールを利用した手口（標的型攻撃メール）**
  - **不正な添付ファイルを開かせる**
  - **不正なウェブサイトへのリンクをクリックさせる**
- **ウェブサイトを利用した手口**
  - **標的組織が頻繁に利用するウェブサイトを調査し、当該サイトを閲覧するとウイルスに感染するように改ざん（水飲み場型攻撃）**

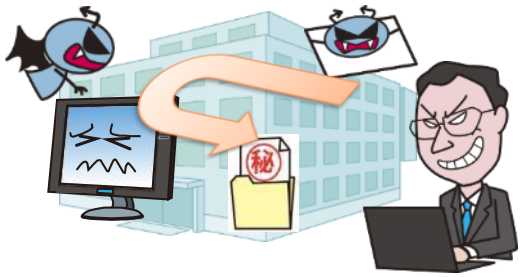


【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

● 攻撃手口

・不正アクセスして認証情報を窃取
・社内システムへ侵入しウイルスを感染させる

- **不正アクセスによる手口**
  - **組織が利用するクラウドサービスやウェブサーバー、VPNの脆弱性を悪用して不正アクセスし、認証情報等を窃取**
  - **窃取した認証情報等を悪用して正規の経路で社内システムへ侵入し、PCやサーバーをウイルスに感染させる**



【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

● 2021年の事例/傾向①

- **情報共有ツールから受託情報が外部に流出** (※1)
  - **・2021年5月、大手Sierが、自社が提供するプロジェクト情報共有ツールが不正アクセスされたことを公表**
  - **・顧客から預かっていた情報の一部が外部に流出**
  - **・本ツールは、同社やグループ会社、外部の協力企業、顧客間のシステム開発等のプロジェクト管理(開発工程やソース、タスクの管理等)に利用**

【出典】
※1 社内外で利用する「プロジェクト情報共有ツール」に不正アクセス - 富士通(Security NEXT)
https://www.security-next.com/126507

【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

2021年の事例/傾向②

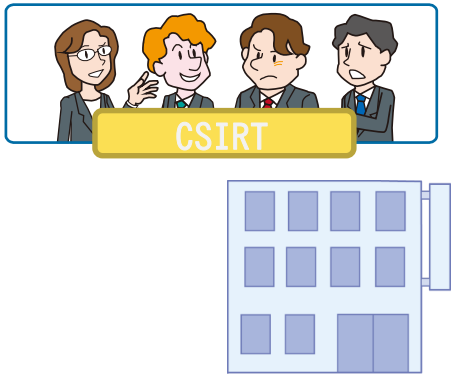
- **サイバー攻撃に関する情報共有** (※1)
  - **サイバー情報共有イニシアティブ(J-CSIP)からの報告**
  - **J-CSIP参加組織からIPAへのサイバー攻撃に関する情報提供**
  - **2021年の標的型攻撃メールとみなした情報提供は36件**

  - **2021年7月～9月の情報提供では、標的型攻撃かは判断できないが、頻繁に利用している無償イラスト素材提供サイトからダウンロードした画像ファイルにURLがリンク**
  - **不正ファイルとしてセキュリティソフトに検知**

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況 [2021年1月～3月,2021年4月～6月,2021年7月～9月,2021年10月～12月](IPA)
https://www.ipa.go.jp/security/J-CSIP/index.html

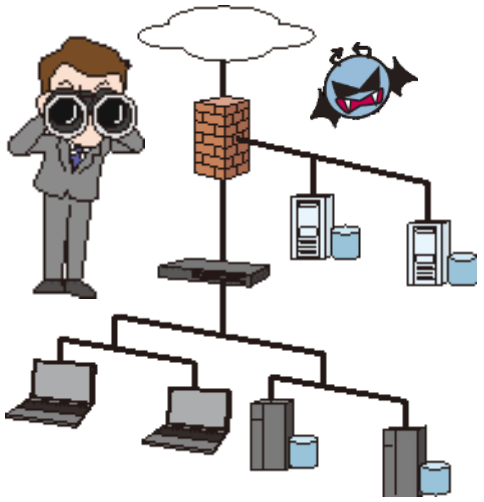
【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

- **対策**
  - **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**



【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

● 対策



• セキュリティ担当者、システム担当者

・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
- –従業員に対するセキュリティ教育の実施
- –インシデント対応の定期的な訓練を実施

※関係者やセキュリティ業者、専門家と迅速に連携できる対応方法や連絡方法を整備する

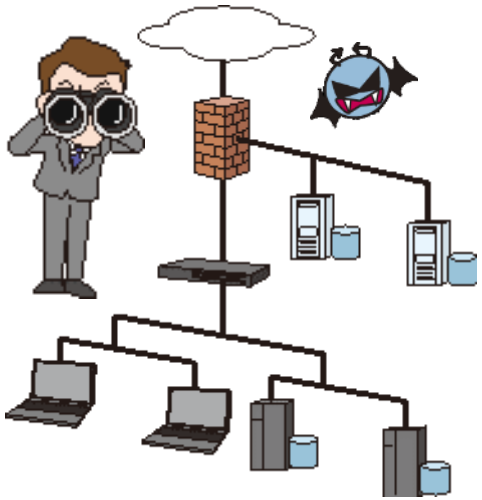
- –管理端末への継続的セキュリティパッチ適用
- –総合運用管理ツール等によるセキュリティ対策状況の把握

※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

【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

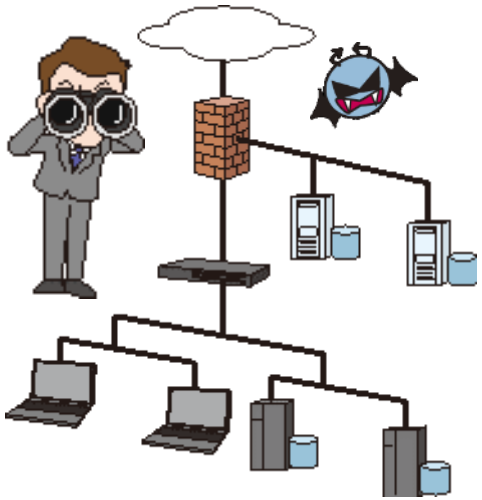
対策

- **セキュリティ担当者、システム担当者**
  - **被害の予防/対応力の向上**
    - **アプリケーション許可リストの整備**
    - **アクセス権の最小化と管理の強化**
    - **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）**
    - **取引先のセキュリティ対策実施状況の確認**
    - **海外拠点等も含めたセキュリティ対策の向上**



【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

- **対策**
  - **セキュリティ担当者、システム担当者**
    - **・被害の早期検知**
      - **－UTM、IDS/IPS、WAF、仮想パッチ等の導入**
      - **－EDR等を用いた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**



【2位】標的型攻撃による機密情報の窃取
～組織化しているサイバー攻撃～

- **対策**
  - **従業員、職員**
    - **・被害の予防（通常、組織全体で実施）**
      - **－添付ファイルやリンクを安易にクリックしない**
    - **・被害を受けた後の対応**
      - **－組織の方針に従い各所へ報告、相談する**
        - **※上司、CSIRT、関係組織、公的機関等**

中小企業の
情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン第3版

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 「クラウドサービス安全利用の手引き」を追加
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録

ガイドラインの対象

ガイドラインP.3

- 対象組織
  - 全ての業種の中小企業および小規模事業者
    （法人、個人事業主、各種団体も含む）
- 想定読者
  - 経営者と情報セキュリティ対策を実践する責任者・担当者

経営者

責任者・担当者

ガイドラインの構成

ガイドラインP.3

- 中小企業の情報セキュリティ対策の考え方や実践方法について、本編２部と付録より構成

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

第１部　経営者編

ガイドラインP.5-14

1　情報セキュリティ対策を怠ることで企業が被る不利益
2　経営者が負う責任
3　経営者は何をやらなければならないのか

経営者は何をやらなければならないのか

認識すべき「３原則」

ガイドラインP.10-11

- 経営者は、以下の３原則を認識し、対策を進める

原則１　情報セキュリティ対策は経営者のリーダーシップで進める

- 経営者は、IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

原則２　委託先の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討

原則３　関係者とは常に情報セキュリティに関するコミュニケーションをとる

- 情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、信頼関係を維持することが可能

経営者は何をやらなければならないのか
実行すべき「重要7項目の取組」

ガイドラインP.12-13

- 経営者は、以下の７項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

取組１	情報セキュリティに関する組織全体の対応方針を定める
取組２	情報セキュリティ対策のための予算や人材などを確保する
取組３	必要と考えられる対策を検討させて実行を指示する
取組４	情報セキュリティ対策に関する適宜の見直しを指示する
取組５	緊急時の対応や復旧のための体制を整備する
取組６	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組７	情報セキュリティに関する最新動向を収集する

経営者などに問われる法的責任

「中小企業の情報セキュリティ対策ガイドライン第3版」から

【表２】情報管理が不適切な場合の処罰など

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	40条 報告及び立入検査 83条 個人情報データベース等不正提供罪[3] 84条 委員会からの命令に違反 85条 委員会への虚偽の報告など 87条 両罰規定	委員会による立入検査、帳簿書類等の物件検査及び質問 1年以下の懲役又は50万円以下の罰金 6月以下の懲役又は30万円以下の罰金 30万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
マイナンバー法（番号法） 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	48条 正当な理由なく特定個人情報ファイルを提供 49条 不正な利益を図る目的で、個人番号を提供又は盗用 50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用 51条 人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得 53条 委員会からの命令に違反 54条 委員会への虚偽の報告など 55条 偽りその他不正の手段により個人番号カード等を取得 57条 両罰規定	4年以下の懲役若しくは200万円以下の罰金又は併科 3年以下の懲役若しくは150万円以下の罰金又は併科 同上 3年以下の懲役又は150万円以下の罰金 2年以下の懲役又は50万円以下の罰金 1年以下の懲役又は50万円以下の罰金 6月以下の懲役又は50万円以下の罰金 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	3条 差止請求 4条 損害賠償請求 14条 信頼回復措置請求	利益を侵害された者からの侵害の停止又は予防の請求 利益を侵害した者は損害を賠償する責任 信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	197条の2 刑事罰 207条1項2号 両罰規定 198条の2 没収・追徴 175条 課徴金	5年以下の懲役若しくは500万円以下の罰金又はこれらの併科 従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑 犯罪行為により得た財産の必要的没収・追徴 違反者の経済的利得相当額
民法	709条 不法行為による損害賠償	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う

2 **▲個人情報保護委員会**　個人情報保護委員会は公正取引委員会と同様の高い独立性を有する機関です。

3 **▲データベース等不正提供罪**　改正個人情報保護法で新設され、役員・従業者等が不正な利益を図る目的で個人情報データベース等を他者に提供等したり盗用した場合は処罰対象になります。

40

第２部　実践編

ガイドラインP.5-14

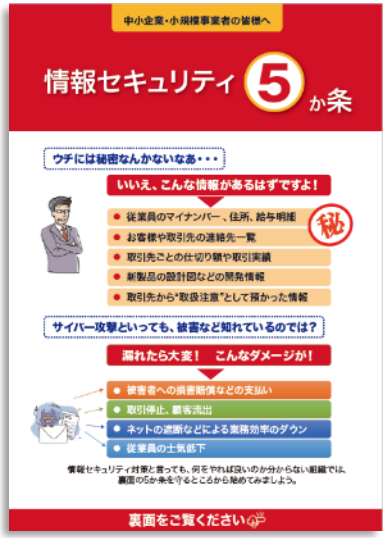
1　実践編の進め方
2　できることから始める
3　組織的な取り組みを開始する
4　本格的に取り組む
5　より強固にするための方策

第２部 実践編

ガイドラインP.15-54

● できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ５か条

SECURITY ACTION ★一つ星を宣言

Step2
組織的な取り組みを開始する

５分でできる！
情報セキュリティ自社診断

SECURITY ACTION ★★二つ星を宣言

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
より強固にするための方策

- 情報収集と共有
- ウェブサイトの情報セキュリティ
- クラウドサービスの情報セキュリティ
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

できるところから始める

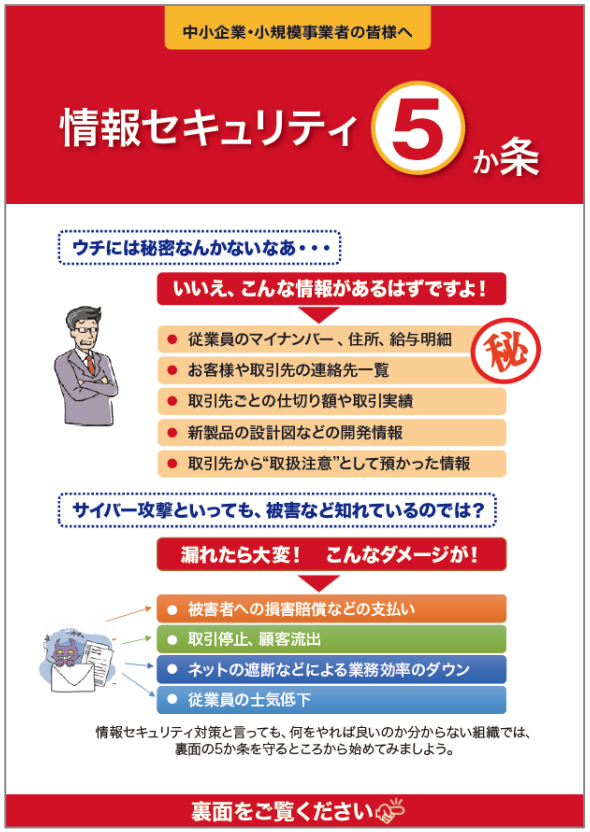
(1)情報セキュリティ５か条

- 情報セキュリティ対策と言っても、何をやれば良いのか？

情報セキュリティ **5** か条

を守るところから始めてみましょう。

1. **OSやソフトウェアは常に最新の状態にしよう！**
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！**



① ＯＳやソフトウェアは常に最新の状態に

ガイドラインP.17・付録1

- ＯＳやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。
- お使いのＯＳやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

＜対策例＞

- Windows Update(Windows OSの場合)/
  ソフトウェア・アップデート(Mac OSの場合)/
  OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/
  Java実行環境(JRE) など
  利用中のソフトウェアを最新版にする

組織的な取り組みを開始する

(2)実施状況の把握

ガイドラインP.18-19・付録3

- 自社のセキュリティ対策の実施状況を把握するために「５分でできる！情報セキュリティ自社診断」を活用
  - 25項目の設問に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる
  - 解説編の対策例を参考に、社内ルールを作成することができる
  - 付録の情報セキュリティハンドブックを活用すると従業員に対する社内ルールの周知が簡単にできる

自社診断のための25項目

IPA

ガイドラインP.18-19・付録3

- 25項目の設問に答え、自社の情報セキュリティ対策の実施状況を把握

基本的対策　5項目

脆弱性対策、ウイルス対策、パスワード強化など

従業員としての対策 13項目

標的型攻撃メール、電子メール、持ち出し、廃棄、ウェブ利用など

組織としての対策 7項目

守秘義務、インターネット利用、ルール化　など

No		診断内容
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？

５分でできる！情報セキュリティ自社診断

従業員としての対策（抜粋）

IPA

ガイドラインP.18-19・付録3

No.	診断内容	実施している	一部実施している	実施していない	わからない
1					
2					
3					
4					
5					

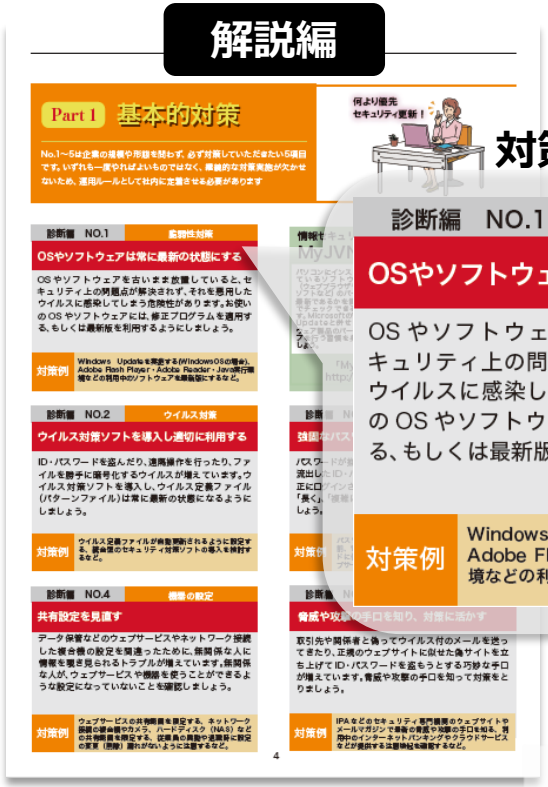
No.	診断内容	実施している	一部実施している	実施していない	わからない
6	電子メールの添付ファイルや本文中のURL リンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
7	電子メールやFAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
9	無線LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1
11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1

組織的な取り組みを開始する
対策の決定と周知

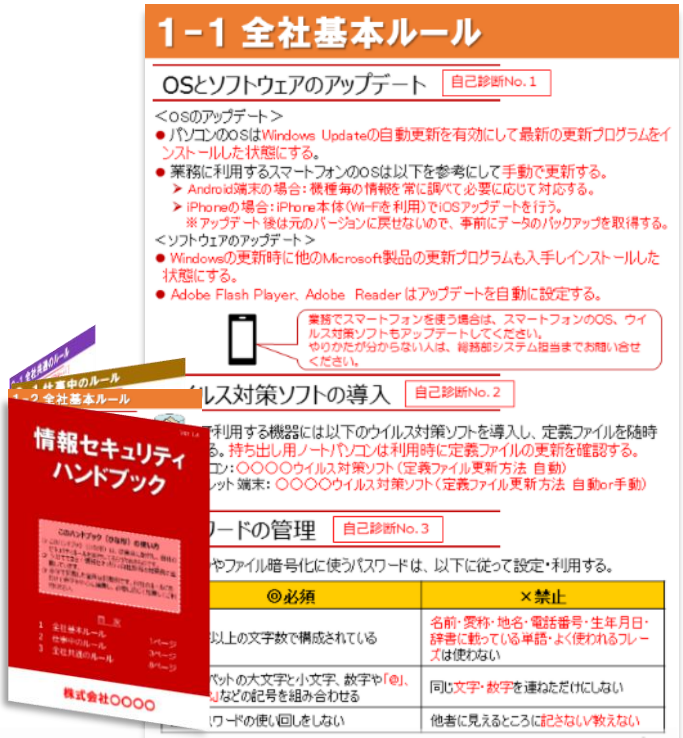
ガイドラインP.20-21・付録4

- 問題があった項目は、解説編を参考に対策を決定
- 付録「情報セキュリティハンドブック(ひな形)」を編集して社内周知

解説編



対策例を参考にして決定



情報セキュリティハンドブックを編集して周知

本格的に取り組む
情報セキュリティ規程の作成

ガイドラインP.24-25

① 対応すべきリスクの特定

※付録6「リスク分析シート」を活用

- 経営者が避けたい重大事故から、対応すべきリスクを特定
  - 外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など
  - 内部状況：経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など

本格的に取り組む

情報セキュリティ規程の作成

ガイドラインP.25・付録5

③ 規程の作成

- 「情報セキュリティ関連規程（サンプル）」を参考に、自社に適した規程にするために修正を加える
  - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

情報セキュリティ関連規程（サンプル）の概要

ガイドラインP.25・付録5

	名称	概要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等のIT インフラに関するルールを定めます。
8	システムの開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。

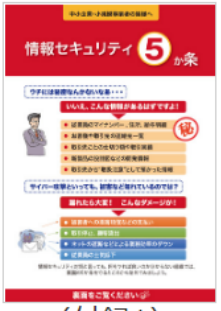
情報セキュリティ関連規程(サンプル)ダウンロード

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ガイドライン等のダウンロード

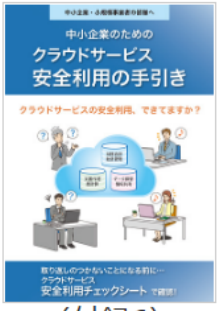
（本編）

- 本編：中小企業の情報セキュリティ対策ガイドライン第3版（全60ページ、32.56MB）
  - 付録1：情報セキュリティ5か条（全2ページ、726KB）
  - 付録2：情報セキュリティ基本方針（サンプル）（全1ページ、35KB）
  - 付録3：5分でできる！情報セキュリティ自社診断（全8ページ、1.9MB）
  - 付録4：情報セキュリティハンドブック（ひな形）（全11ページ、212KB）
  - 付録5：情報セキュリティ関連規程（サンプル）（全51ページ、179KB）
  - 付録6：クラウドサービス安全利用の手引き（全8ページ、2.8MB）
  - 付録7：リスク分析シート（全7シート、99KB）



（付録1）

（付録3）



（付録6）

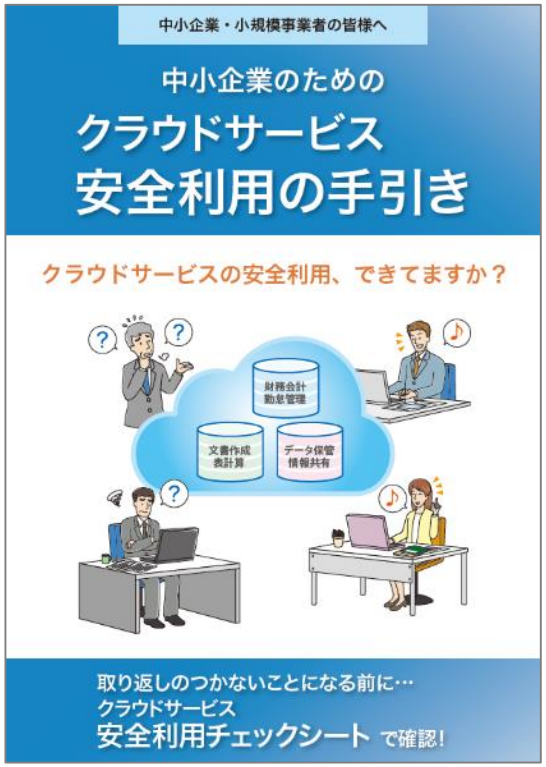
映像で知る情報セキュリティ
「ハケンが解決！情報セキュリティ規程作成のポイント」

https://www.youtube.com/watch?v=fot-PEzBZO4

中小企業のセキュリティ担当者に向けて社内の情報セキュリティ規程の作成から運用までの手順をドラマ仕立て説明します

中小企業のための
クラウドサービス安全利用の手引き

- クラウドサービスを安全に利用するためには、何をやれば良いのかを説明
  - クラウドサービス安全利用チェックシートで確認すべきことが分かる
  - 解説編で身近なサービスを例に、何を確認し、どうしたら安全に利用することができるか分かる

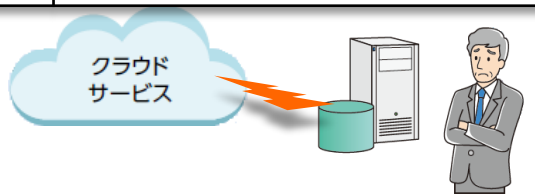


選択するときの確認ポイント（抜粋）

IPA

ガイドラインP.36・付録6

1 2	11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
3 4 5	12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
6 7	13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
8 9	14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
10	15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？



（参考）サイバーセキュリティお助け隊サービス

もしものインシデント（事故）に備えて

サイバーセキュリティお助け隊サービス制度

https://www.ipa.go.jp/security/otasuketai-pr/

- 中小企業に対するサイバー攻撃への対処として不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすものを**「サイバーセキュリティお助け隊サービス」**として登録・公表
  - **「サイバーセキュリティお助け隊サービス基準」の主な内容**

主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク及び／又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・運用できる簡単さ	**専門知識がなくても導入・運用できるような工夫**
簡易サイバー保険	突発的に発生する駆付け費用等を補償する**サイバー保険**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）** ・併用型：**これらの和に相当する価格を超えないこと** ※端末1台から契約可能であることが条件

相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性のアピール**に

・ワンパッケージのサービスとして登録

IPA

・マーク提供
・ブランド管理・普及促進

サイバーセキュリティ CSお助け隊

マーク付きの民間サービス

<サイバーセキュリティお助け隊サービス>

中小企業

【お助け隊サービス】登録サービスリスト

■ 各地域の中小企業に選択・利用可能な**「サイバーセキュリティお助け隊サービス」登録サービスリスト。**これまでに**12のサービス**が登録、今後も拡充予定。

【サイバーセキュリティお助け隊サービス　登録サービスリスト】

※2022年4月時点

	サービス名	事業者名
1	**商工会議所サイバーセキュリティお助け隊サービス**	大阪商工会議所
2	**防検サイバー**	ＭＳ＆ＡＤインターリスク総研株式会社
3	**PCセキュリティみまもりパック**	株式会社ＰＦＵ
4	**EDR運用監視サービス「ミハルとマモル」**	株式会社デジタルハーツ
5	**SOMPO SHERIFF（標準プラン）**	ＳＯＭＰＯリスクマネジメント株式会社
6	**ランサムガード**	株式会社アイティフォー
7	**オフィスSOCおうちSOC**	富士ソフト株式会社
8	**セキュリティ見守りサービス「＆セキュリティ＋」**	株式会社BCC
9	**CBM ネットワーク監視サービス**	中部事務機株式会社
10	**中部電力ミライズ サイバー対策支援サービス**	中部電力ミライズ株式会社
11	**ＣＳＰサイバーガード**	セントラル警備保障株式会社
12	**PCお助けパック　PC定期侵害調査プラン**	沖電グローバルシステムズ株式会社

【お助け隊サービス】中小企業ユーザーの主な声

＜サイバーセキュリティお助け隊サービスについて中小企業から寄せられた声＞

●自社の対策が不十分であることにより、**取引先に迷惑をおかけするわけにはいかない**ため、サイバーセキュリティお助け隊サービスの導入を決めた。

●検知・監視してくれるだけでなく**何かあった時の事後対応まで含まれる**ところがよい。セキュリティについて全く分からないので、**まとめてお任せできるところにお願いしたい**と考えていた。

●アラート通知が来るので、**防御できていることが実感でき安心**。本社のほか複数の拠点でも利用しているが**サービス利用料が安いので助かって**いる。

●**何も無いということがわかる**ことも良い点。**セキュリティレポートをストックしておくことで、報告資料としても使える**ので助かっている。

※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

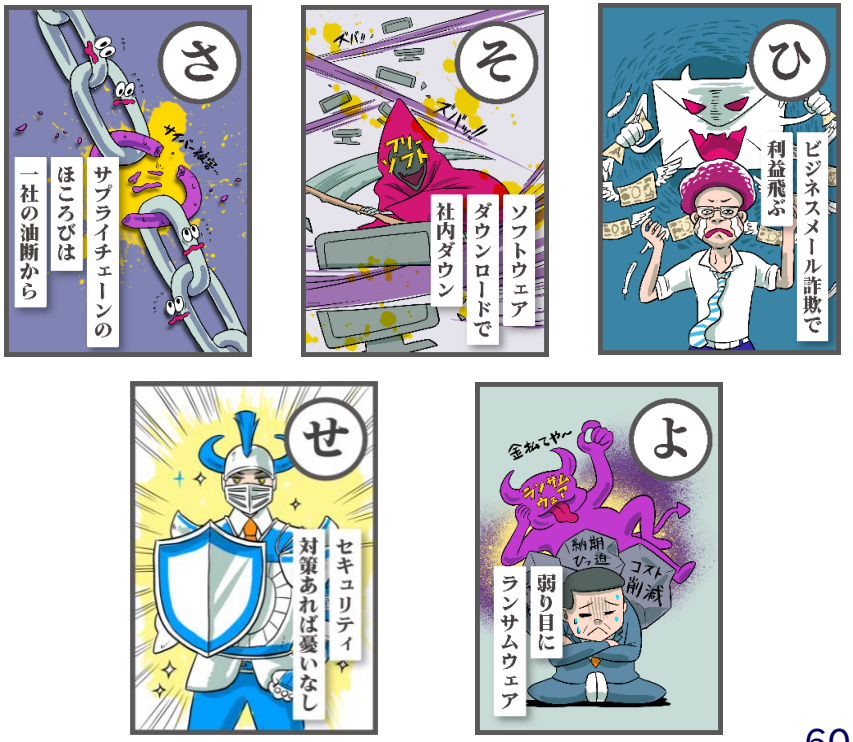
【お助け隊サービス】新ウェブサイトの公開

- 「サイバーセキュリティお助け隊サービス」の**新ウェブサイト**を公開。分かりやすく親しみやすい**動画コンテンツ**とともに登録サービスを紹介。
- また、中小企業がセキュリティ対策について考え、意識を高めるきっかけとなるようユニークな啓発コンテンツ**「サイバーセキュリティ対策かるた」**も合わせて公開。

ぜひ新ウェブサイトをご覧いただき、ご活用ください！

新ウェブサイトURL:　https://www.ipa.go.jp/security/otasuketai-pr/

<サイバーセキュリティお助け隊サービス　新ウェブサイト>



<サイバーセキュリティ対策かるた>

【お助け隊サービス】IT導入補助金との連携

■ 中小企業向け**IT導入補助金「セキュリティ対策推進枠」が新設**され、**「サイバーセキュリティお助け隊サービス」がメインツールとして補助対象**に。公募要領が**5/31**に公表。

中小企業等のサイバーセキュリティ対策の強化

（IT導入補助金の枠の新設）予算措置済み（令和元年度補正3,600億円の内数）

商務情報政策局 サイバーセキュリティ課

事業の内容

事業目的・概要

- 国際情勢の緊張などによりサイバー攻撃事案の潜在リスクが高まっていることを踏まえ、中小企業等のサイバーセキュリティ対策を強化することにより、サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることを防ぎます。
- そのため、サービス等生産性向上IT導入支援事業（IT導入補助金）について、「セキュリティ対策推進枠」を創設します。

成果目標

- 中小企業等のサイバーセキュリティ対策を強化することにより、サイバーインシデントが原因で事業継続が困難となる事態を回避するとともに、こうした被害が供給制約や価格高騰を潜在的に引き起こすリスクや中小企業等の生産性向上を阻害するリスクを低減することを目指します。
- 本事業も活用し、令和4年度までに、中小企業のセキュリティ対策機器と事後支援がセットになったサービスの利用者数を2万者以上にすることを目指します。

条件（対象者、対象行為、補助率等）

事業イメージ

- 自社サーバーの異常監視や、サイバー攻撃を受けた際の初動対応支援、被害を受けた場合の簡易保険など、中小企業等に必要な対策をワンパッケージにまとめた「サイバーセキュリティお助け隊サービス」について、最大２年間分のサービス利用料を補助することで、中小企業等のサイバーセキュリティ対策の向上を図ります。その際、サプライチェーンへの寄与度が高いなど、物資やサービスの安定供給を確保する上で重要な企業に対して優先的に支援を行います。

既定の基準を満たしたセキュリティサービスについて、独立行政法人行政法人情報処理推進機構（IPA）が、「サイバーセキュリティお助け隊サービスリスト」に掲載

サイバーセキュリティ お助け隊

	IT導入補助金「セキュリティ対策推進枠」
補助額	５万円～100万円
機能要件	独立行政法人 情報処理推進機構（IPA）が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているサービス
補助率	1／2
対象経費	サービス利用料最大２年間分

「セキュリティ対策推進枠」

「サイバーセキュリティお助け隊サービス」をメインのITツールとした申請（サイバーセキュリティお助け隊サービス単品での申請）が可能に。

※2022年8月頃申請開始予定

【参考】IT導入補助金（セキュリティ対策推進枠ページ）
https://www.it-hojo.jp/security/

15

https://www.meti.go.jp/ukraine/pdf/cybersecurity01.pdf

（参考）SECURITY ACTION制度

SECURITY ACTION 制度概要

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

- 中小企業自らが情報セキュリティ対策に取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段階の取組み目標を用意

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

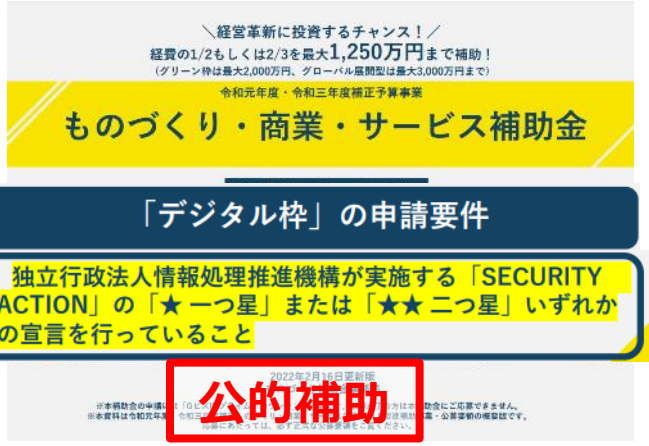
※SECURITY ACTION制度は、中小企業等自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。
各企業等の情報セキュリティ対策状況等をIPAが認定する、あるいは認証等を付与する制度ではありません

SECURITY ACTION制度のメリット

- 情報セキュリティ対策への取組みの**見える化**
  - ☞ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに 印刷することで自らの取組み姿勢をアピール
- 顧客や取引先との**信頼関係**の構築
  - ☞ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに
- **公的補助**・民間の支援を受けやすく
  - ☞ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

見える化

信頼関係



公的補助

本年度における自治体等のSA制度の活用事例

■ デジタル化やサイバーセキュリティ対策などを支援するIT導入の補助金申請の要件にするなど、各種補助金・助成金制度において**SECURITY ACTION制度を活用**。

- **IT導入補助金**【継続】
  ：中小企業庁
- **令和4年度 サイバーセキュリティ対策促進助成金**【継続】
  ：東京都中小企業振興公社
- **「情報セキュリティ基本方針 策定支援専門家派遣」事業**【継続】
  ：東京都中小企業振興公社
- **ものづくり補助金（デジタル枠）**【新規】
  ：中小企業庁
- **事業承継・引継ぎ補助金**【新規】
  ：中小企業庁
- **令和4年度 中小企業等スマートワーク促進補助金（情報セキュリティ事業）**【新規】
  ：岐阜県
- **令和4年度 堺市中小企業デジタル化促進補助金**【活用継続】
  ：大阪府堺市

SECURITY ACTION一つ星宣言による

組織的な取り組みの進め方

- **SECURITY ACTION一つ星宣言**は以下のように進めます。

情報セキュリティ5か条で対策を決定

情報セキュリティハンドブックで対策を周知

SECURITY ACTION
セキュリティ対策自己宣言

SECURITY ACTION一つ星宣言

情報セキュリティ５か条
セキュリティ対策の決定

情報セキュリティ 5 か条

1 OSやソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

対策例
- Windows Update(Windows OS の場合) /ソフトウェア・アップデート(Mac OS の場合)/OS バージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java 実行環境 (JRE) など利用中のソフトウェアを最新版にする

2 ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

対策例
- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的な機能を搭載したソフト)の導入を検討する

3 パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

対策例
- パスワードは英数字記号含めて 10 文字以上にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じ ID・パスワードをいろいろなウェブサービスで使い回さない

4 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例
- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する

5 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げて ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例
- IPA などのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

IPA 独立行政法人 情報処理推進機構 セキュリティセンター

IPA セキュリティセンターは誰もが安心、安全な暮らせる「IT 社会」を目指して、国民の皆様に情報セキュリティに関する注意喚起や対策情報・対策手段の提供、脆弱性発や相談窓口を設けるなどセキュアな社会の基盤に貢献するための活動を行っています。

E-mail:isec-info@ipa.go.jp URL:https://www.ipa.go.jp/security/

SECURITY ACTION
セキュリティ対策自己宣言

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です。「情報セキュリティ５か条」に取組むことを宣言することで、１段階目「一つ星」を使用することができます。
URL: https://www.ipa.go.jp/security/security-action/

2019.3.19 Version 1.2

1-2 全社基本ルール

アクセス制御

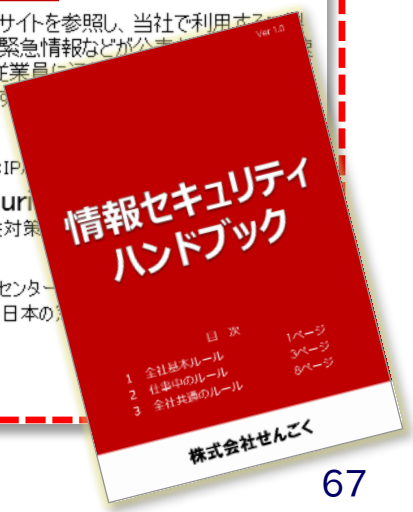
- 複数名が共有する機器には以下のようにアクセス制御を行う。
- アクセス制限の設定・変更は、総務部システム担当が行う。

機器名	アクセス制御の方法	アクセス許可対象者
ファイルサーバー	Windows Active Directory	全従業員
設計図保存用 NASサーバー	Windows Storage Server	技術部従業員
経理部複合機HDD	複合機アクセス権設定機能	社長/経理部従業員
本社無線LANルーター	Wi-Fi パスワード設定 WPA2による暗号化	全従業員

セキュリティに対する注意

- 総務部システム担当は毎週月曜日に以下のサイトを参照し、当社で利用ア… 品やサービスに関わる重要なセキュリティ情報、緊急情報などが公… やかに社長に報告し、電子メールで対策を全従業員に…
- 通知を受けた従業員は速やかに対策を実行す…

☞ 独立行政法人情報処理推進機構(略称:IP…
https://www.ipa.go.jp/securi…
☞ JVN (Japan Vulnerability Notes 脆弱性対策…
https://jvn.jp/
☞ 一般社団法人 JPCERT コーディネーションセンター
(略称: JPCERT/CC 技術的な立場における日本の…
https://www.jpcert.or.jp/



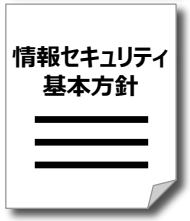
SECURITY ACTION二つ星宣言による

組織的な取り組みの進め方

- **SECURITY ACTION二つ星宣言**は以下のように進めます。

情報セキュリティ自社診断で対策を決定

情報セキュリティハンドブックで対策を周知



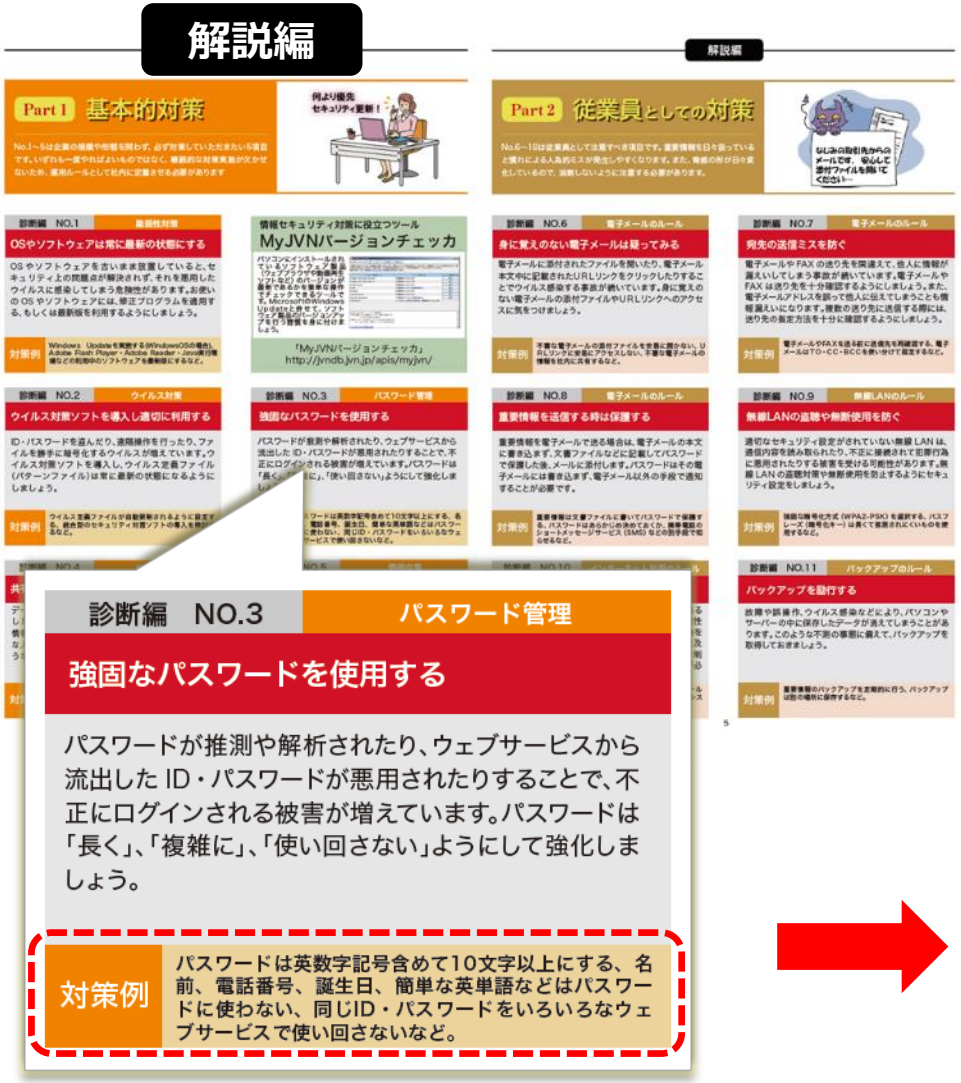
情報セキュリティ基本方針を公開

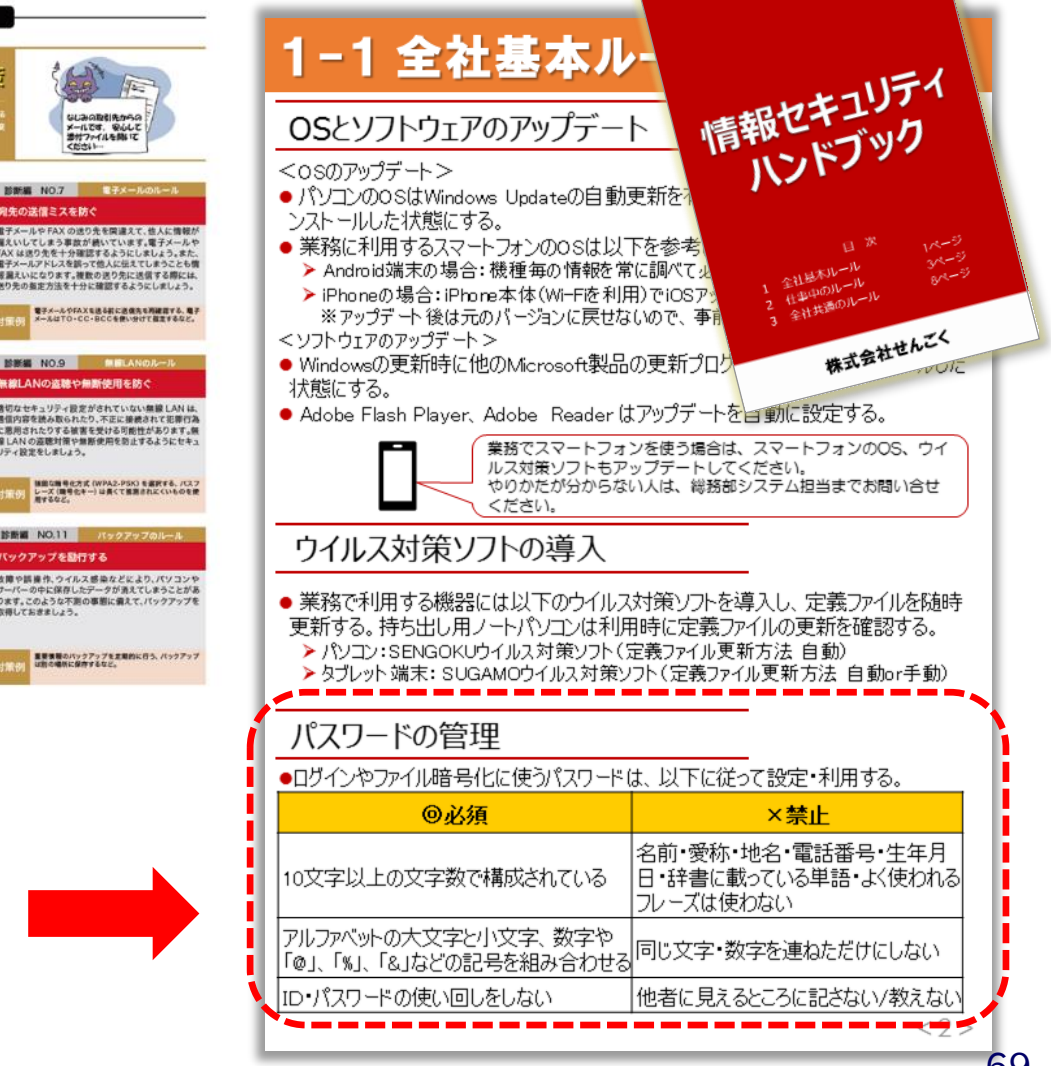
SECURITY ACTION二つ星宣言

５分でできる！情報セキュリティ自社診断
セキュリティ対策の決定

IPA

解説編

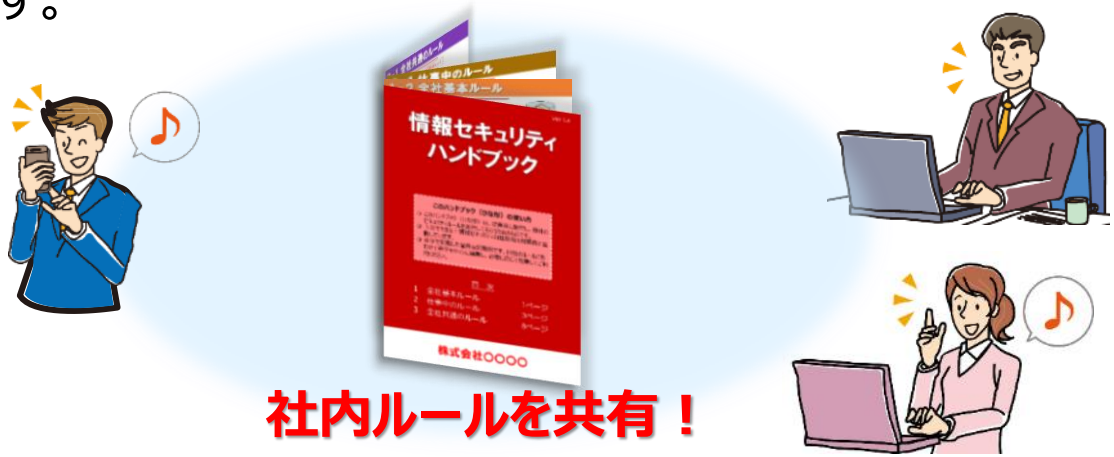




情報セキュリティハンドブック

セキュリティ対策を従業員へ周知

- 対策が決まったら、対策例と連動した「**情報セキュリティハンドブック**」※に対策を具体的に記述して、従業員に配付します。
  - 情報セキュリティハンドブックは、責任者・担当者が作成します。
  - ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。



※情報セキュリティハンドブック(ひな形)
[全社基本ルール]のページが情報セキュティ5か条に、全ページが情報セキュリティ自社診断に連動しています
https://www.ipa.go.jp/files/000055529.pptx

SECURITY ACTION二つ星宣言

情報セキュリティ基本方針の作成と周知

- 情報セキュリティに関する経営者の方針を文書で周知
- 付録「**情報セキュリティ基本方針（サンプル）**」※を参考

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

情報セキュリティ基本方針

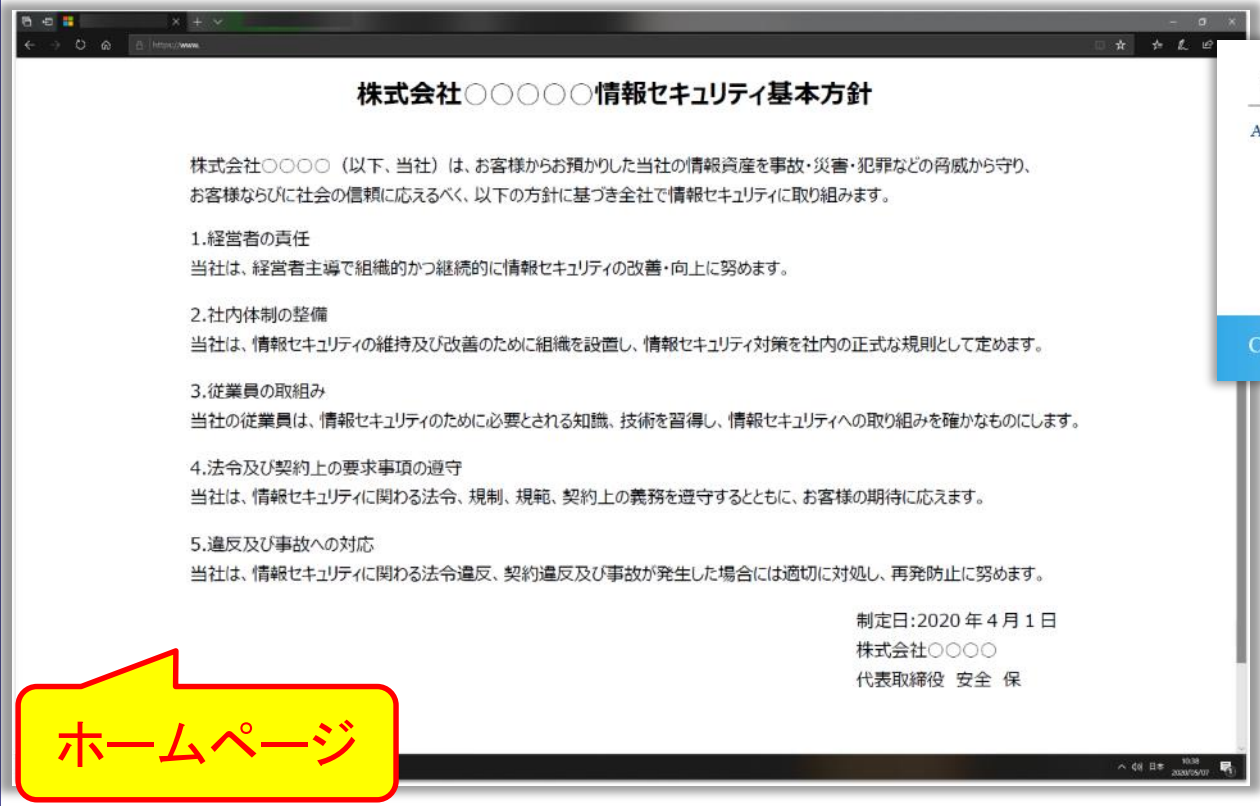
株式会社千石商会（以下、当社）は、当社の情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

※情報セキュリティ基本方針（サンプル）
https://www.ipa.go.jp/files/000072146.docx

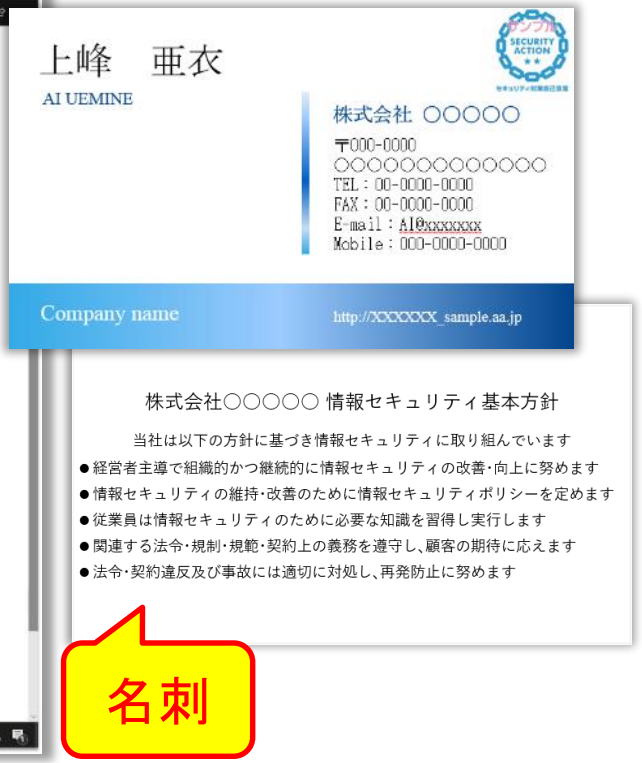
SECURITY ACTION二つ星宣言

情報セキュリティ基本方針の公開

- 情報セキュリティ基本方針をホームページ・名刺などで外部に公開して信頼を得ます※。



名刺



※二つ星では「情報セキュリティ基本方針」を定め、外部に公開します

SECURITY ACTION申込方法

1)取組み目標を決める

- 一つ星▶「情報セキュリティ5か条」を実行
- 二つ星▶「5分でできる！情報セキュリティ自社診断」で実施状況を把握し対策を決定
  「情報セキュリティ基本方針」を公開

ダウンロード：https://www.ipa.go.jp/security/security-action/mark/

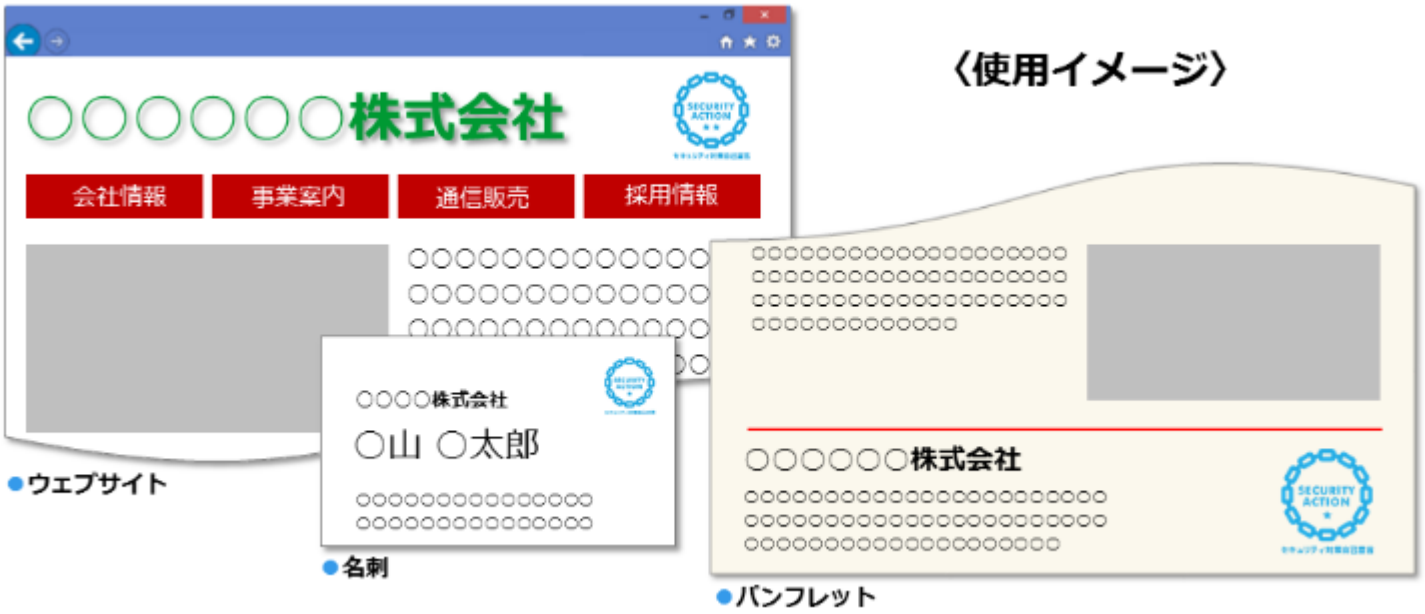
2)自己宣言する

- 使用規約に同意してロゴマークをダウンロード
- ロゴマークを表示してSECURITY ACTION自己宣言

ロゴマーク申込：https://security-shien.ipa.go.jp/security/entry/

ロゴマークの使用方法

- ロゴマークは、ポスター・パンフレット・名刺・封筒・ウェブサイト等に無償で使用でき、情報セキュリティ対策の取り組みをアピールします。



ご清聴ありがとうございました

独立行政法人 情報処理推進機構
セキュリティセンター

〒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
TEL 03-5978-7508　FAX 03-5978-7546
電子メール　isec-pr-nw@ipa.go.jp
URL　https://www.ipa.go.jp/security/