サイバーセキュリティ対策の必要性について

高性能ＡＩ悪用の危険性

※　イラストはイメージです。

クロード・ミュトスなどの高性能ＡＩは、その活用によってサイバー対処能力の向上が期待できる一方で

悪用されることで**攻撃のスピード**や**規模が大幅に増加**するなど**悪用リスク**への懸念が高まっております。

（以下略）

※　出典　R8.5.19 総務省記者会見記事

高性能 AI の特徴 → サイバー攻撃に悪用されやすい。

高性能 AI の特徴として、リバースエンジニアリング能力によるソフトウェアの脆弱性検索に秀でている一方、脆弱性の修正作業には向かない点が挙げられます。

製造とは逆のプロセスをたどり、既存のソフトウェアの構造や設計等を明らかにする手法

何が脅威なのか？ → お金を払えば誰でも使える可能性がある。

高性能 AI を安全保障の対象として公開制限とするか、有料サービスとしてオープン利用とするかは、各国の事情によるため、その将来性は依然として不透明なままです。

※　WannaCry 感染画面イメージ

いつ頃が危ない？ → 2027 年中盤から 2028 年前半以降

中華系 AI を例に考察すると、近い将来、ミュトス級の高性能モデルが開発されると予測しています。※ Ｃｙｂｅｒ Ｇｙｍ、ＡＩＳＩ基準値から予測

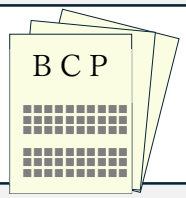
大規模なサイバー攻撃は起きる？ → 起き得ます。

150 カ国 23 万台以上の Windows コンピュータに感染したワーム型ランサムウェア

2017 年５月に起きた『WannaCry（ワナクライ）』による世界的被害の様に、多くのコンピュータに共通する致命的な脆弱性があると、大規模な攻撃が行われる可能性が払拭できません。

最重要な対策

事業継続計画（BCP）～平常時において有事の備えを行うこと～



サイバー攻撃を完全に防ぐことは困難です。攻撃を受けてシステムが止まる前提で、被害を最小限に抑えながら事業を継続化させることが最も重要です。

平常時に何ができるかを考えましょう。

本資料に関する問い合わせ先（サイバーセキュリティ対策の必要性について）
北海道警察本部生活安全部サイバー局サイバー企画課 対策・官民連携係
TEL：011-251-0110（内線 3742）

サイバー攻撃への備えはできていますか？
「SECURITY ACTION」から始めましょう！

サイバー攻撃は、どの企業にも起こりうるリスクです。
できることから始めて、取引先やお客様の信頼を守り、事業を継続しましょう。

セキュリティアクション SECURITY ACTIONとは？

▼公式サイトはこちらから▼

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

中小企業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。「何から始めればよいかわからない」という方は、この制度を活用し、まず自社の対策状況を確認することから始めましょう。このチラシで紹介する基本的な対策を実践し、サイバー攻撃に備えましょう。

まずは、情報セキュリティ６か条に取り組む！ SECURITY ACTION　一つ星

【情報セキュリテイ６か条】

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 バックアップを取ろう！
⑥ 脅威や攻撃の手口を知ろう！

すぐに取り組める基本の対策です。できているところから実践しましょう！

GET!

次に ① 情報セキュリティ自社診断を実施！ ② 情報セキュリティ基本方針を策定！ SECURITY ACTION　二つ星

これが重要！必ず自社の状態を知ろう！

５分でできる！情報セキュリティ自社診断

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

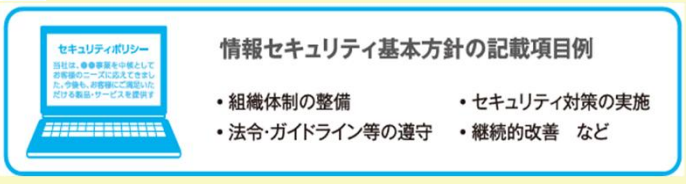
- 基本的対策　6項目
  - 脆弱性対策、ウイルス対策、パスワード強化など
- 従業員としての対策 11項目
  - 標的型攻撃メール、電子メール、持ち出し、廃棄、ウェブ利用など
- 組織としての対策 8項目
  - 守秘義務、インターネット利用、ルール化　など

▼診断シートこちらから▼

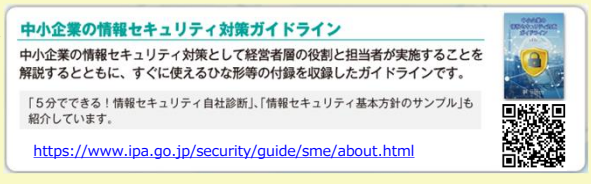
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_3.pdf

GET!

情報セキュリティ基本方針を策定し、外部へ公開



基本方針サンプルをガイドラインの付録としてご用意しています！



【参考】さらにセキュリティ対策を進めたい企業様へ【新たに始まります】

①サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）

経済産業省では、サプライチェーンを構成する企業が実施すべきセキュリティ対策をまとめた「サプライチェーン強化に向けたセキュリティ対策評価制度」の制度創設に向けた取組を進めています。この制度は、取引先ごとに異なるセキュリティ要件を共通の★基準で"見える化"することを目的としています。令和8年度末頃の施行を目指しています。

②サイバーセキュリティお助け隊サービス（新類型） 実証事業について

この実証事業では、IPAが認定したサービス提供事業者様が、中小企業の皆様にセキュリティサービスを提供し、「サイバーセキュリティお助け隊サービス」（新類型）として必要な要件の検証を行います。実証事業に参加すると、組織的対策を含むセキュリティ対策を無料※で実施、SCS評価制度の★取得の支援等を受けられます。※SCS評価制度の対策の範囲で、実証期間中（最大で1年程度）に限ります。

本資料に関する問い合わせ先（SECURITY ACTIONについて）
経済産業省北海道経済産業局地域経済部 製造･情報産業課
TEL：011-709-2311（内線2571）
Mail：bzl-hokkaido-seizojoho@meti.go.jp