テーマ４　知っておきたい最新ICTトレンド

＊人工知能（AI）との向き合い方＊
　機会・リスク・実践例

＊セキュリティ対策の基本＊
　情報漏えい対策・著作権・個人情報保

「何から始めればいいの？」が
クリアになる内容です

【スライド1】

知っておきたい最新ICTトレンド
AI／セキュリティ

**＊＊知っておきたい最新ICTトレンド
～AI／セキュリティ～**

AI技術の急速な発展とサイバー攻撃の巧妙化。
この2つは表裏一体です。
適切に活用し、適切に守る。
そのための基礎知識をお伝えします。

【スライド2】AI の広がり

＊ 文書作成
＊ 画像生成
＊ 事務効率化
＊ 学習支援

3

私たちの身近にあるAI

＊ **文書作成**
- ChatGPT、Claude、Geminiなど
- 文章の下書き、要約、翻訳
- メール返信、報告書作成支援
- アイデア出し、企画のたたき台

＊ **画像生成**
- Midjourney、DALL-E、Stable Diffusion
- イラスト、写真風画像の生成
- デザイン案の作成
- プレゼン資料の素材作成

＊ **事務効率化**
- データ整理、分類
- スケジュール調整
- 議事録作成

【スライド3】AI のメリット

＊ 作業時間を大幅削減
＊ アイデア出しを支援
＊ データ分析が容易に

4

なぜ今、AIを使うべきか

* **作業時間を大幅削減**
  - 文章作成が10分の1の時間に
  - 情報収集・要約が効率的
  - 単純作業の自動化
  - 例: 議事録作成 60分→10分

* **アイデア出しを支援**
  - ブレインストーミングのパートナー
  - 多角的な視点を提供
  - 思考の整理に役立つ
  - 例: 企画案10個を数分で生成

* **データ分析が容易に**
  - 大量データの傾向把握
  - グラフ・図表の作成支援
  - 専門知識なしで分析可能

【スライド4】AI のリスク

＊ 著作権
＊ 個人情報
＊ ハルシネーション
＊ 偏った回答

5

****便利だからこそ注意が必要****

＊ ****著作権****
- AI生成物の権利は不明確
- 他人の作品に似てしまう可能性
- 商用利用には注意
- 各サービスの利用規約を確認

＊ ****個人情報****
- 入力した情報が学習データになる可能性
- 氏名、住所、電話番号を入れない
- 社内機密情報を入れない
- 例: 顧客リストをAIに貼り付けるのはNG

＊ ****ハルシネーション（幻覚）****
- もっともらしい嘘をつく
- 存在しない論文や統計を引用
- 日付や数値の誤り

【スライド5】安全に使うルール

＊ 個人情報を入れない
＊ 機密文書の扱い
＊ 情報元の確認
＊ 最終判断は人間が行う

6

組織で決めるべきガイドライン

＊ **個人情報を入れない**
- 氏名、住所、電話番号、メールアドレス
- マイナンバー、クレジットカード情報
- 顧客情報、社員情報
- 匿名化してから入力（例: A社、B氏など）

＊ **機密文書の扱い**
- 社外秘情報は入力禁止
- 公開前の情報は入力禁止
- 契約書、提案書、財務情報など
- 「公開されても問題ない情報のみ」が原則

＊ **情報元の確認**
- AIの回答を鵜呑みにしない
- 重要な情報は必ず裏取り
- 複数の情報源で確認
- 公式サイト、信頼できる文献を参照

【スライド6】セキュリティの脅威

＊ フィッシング
＊ 詐欺メール
＊ マルウェア
＊ ランサムウェア

7

巧妙化する攻撃手法

＊ **フィッシング**
- 偽のメール、偽のサイト
- 銀行、宅配業者、公的機関を装う
- リンクをクリックさせて情報を盗む
- 最近はAIを使って自然な日本語に

＊ **詐欺メール**
- 請求書を装ったメール
- 「未払い金があります」
- 「アカウントが停止されます」
- 焦らせて判断力を奪う手法

＊ **マルウェア**
- ウイルス、トロイの木馬など
- 添付ファイル、ダウンロードで感染
- 情報窃取、遠隔操作
- 気づかないうちに感染していることも

【スライド7】基本の対策

＊ 強力なパスワード
＊ バックアップ
＊ 権限管理
＊ ウイルス対策

8

****すぐに実践できるセキュリティ対策****

＊ ****強力なパスワード****
- 12文字以上
- 英大小文字、数字、記号を混在
- 同じパスワードを使い回さない
- パスワード管理ツールの活用
- 2段階認証（2FA）を必ず設定

＊ ****バックアップ****
- 重要データは3-2-1ルール
- 3つのコピー
- 2種類のメディア
- 1つはオフライン（外付けHDDなど）
- 定期的に自動バックアップ
- 復元テストも実施

＊ ****権限管理****
- 必要最小限の権限のみ付与
- 管理者権限を乱用しない

【スライド8】著作権・個人情報

＊ 無断利用の危険
＊ 画像の権利
＊ 個人データの扱い方

法律で守られている権利

* **無断利用の危険**
  - 他人の文章、画像、音楽を勝手に使用
  - 「個人利用だから」は通用しない
  - SNSへの投稿も「公開」
  - 著作権侵害で損害賠償のリスク

* **画像の権利**
  - 写真には撮影者の著作権
  - 写っている人には肖像権
  - ネットから拾った画像は使えない
  - フリー素材サイトでも利用規約を確認
  - AI生成画像も慎重に

* **個人データの扱い方**
  - 個人情報保護法の遵守
  - 本人の同意なく第三者に提供禁止

【スライド9】リスクを下げる運用

＊ 定期的な更新
＊ 管理者の明確化
＊ 情報共有の仕組みづくり

10

****組織全体でセキュリティ文化を****

＊ **定期的な更新**
- OS、ソフトウェアを最新に保つ
- 「後で」は禁物、すぐに更新
- 自動更新の設定を推奨
- 月1回は更新状況を確認
- 古いソフトは使わない

＊ **管理者の明確化**
- セキュリティ責任者を決める
- 緊急連絡網の整備
- インシデント発生時の対応手順
- 定期的な報告体制

＊ **情報共有の仕組みづくり**
- セキュリティ情報の共有
- 「怪しいメールが来た」を報告しやすく
- 定期的な勉強会・訓練
- ヒヤリハット事例の蓄積
- 失敗を責めない文化

【スライド10】AI/セキュリティ チェックリスト

* AI に個人情報を入れない運用ルール
* パスワードが安全
* 多要素認証を設定済み
* フィッシング教育がある
* バックアップが定期実施
* アップデートを怠らない
* 著作権の方針を定めている

【スライド11】ケーススタディ

＊ 実際に起きた事例
＊ どこが問題だったか
＊ 防げたポイント