今だから重要なセキュリティについて
～ ITC茨城セキュリティ事業のご紹介 ～

2022年11月14日

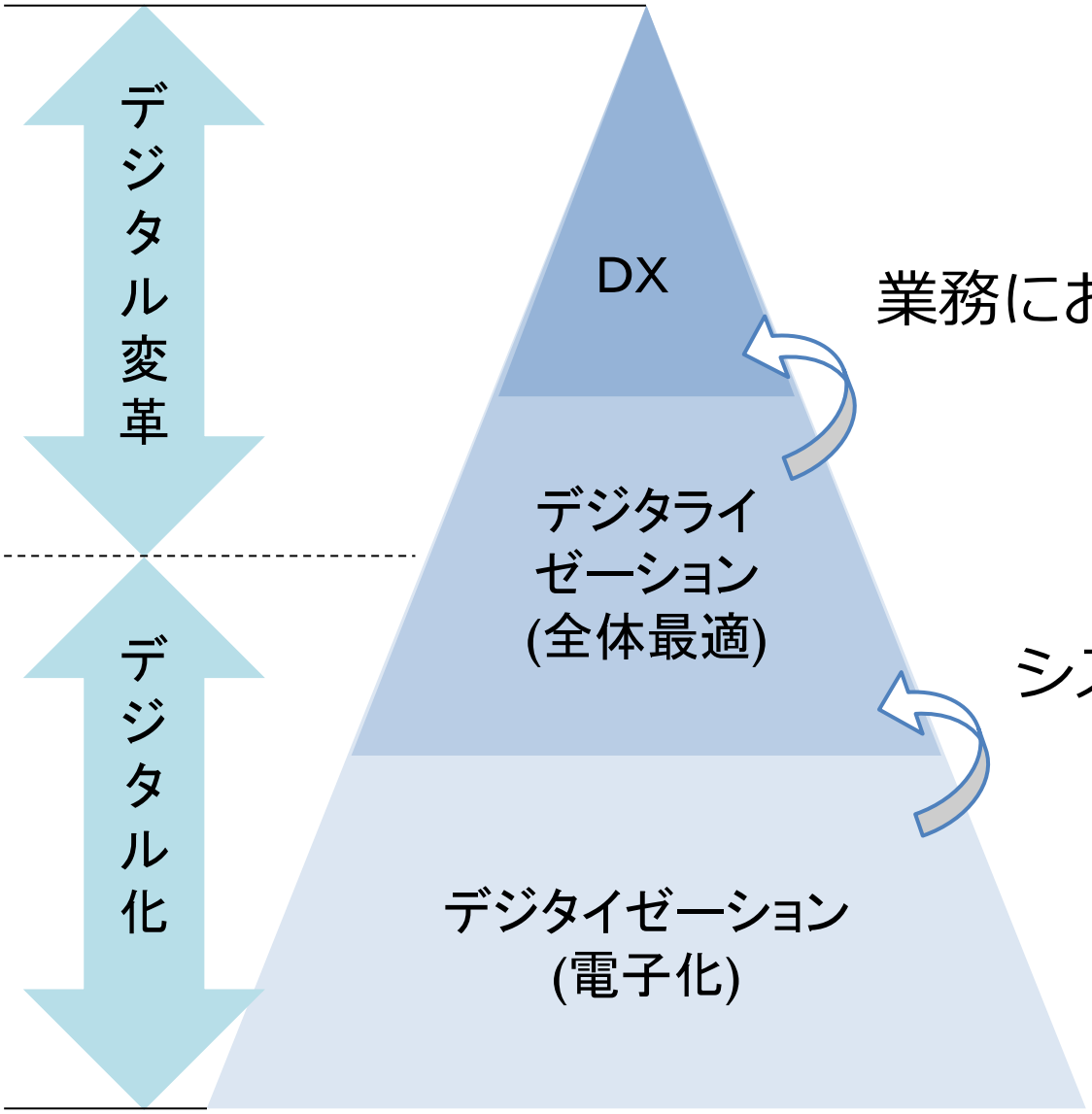
特定非営利活動法人 ITコーディネータ茨城
後藤　雅俊

DX推進におけるセキュリティ位置づけ

DX推進における実施項目	実施内容
経営ビジョン・ビジネスモデル	企業経営の方向性及び情報処理技術活用の方向性決定
戦略	企業経営及び情報処理技術の活用の具体的な方策（戦略）の決定
組織づくり・人材・企業文化に関する方策	戦略を効果的に進めるための体制の提示
ITシステム・デジタル技術活用環境の整備に関する方策	最新の情報処理技術を活用するための環境整備の方策の提示
成果と重要な成果指標	戦略の達成状況に関わる指数の決定
ガバナンスシステム	実務執行総括責任者による効果的な戦略の推進等を図るために必要な情報発信 実務執行総括責任者が主導的な役割を果たすことによる、事業者が利用する情報システムにおける課題の把握 サイバーセキュリティに関する対策の的確な策定及び実施

DX推進支援事業での実施項目

DX推進におけるセキュリティの重要性



業務におけるデジタル活用度が高まる

システム停止時のリスクが高まる

- 影響度合い
- 影響範囲

中小企業へも広がる脅威

IPA 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 2022」

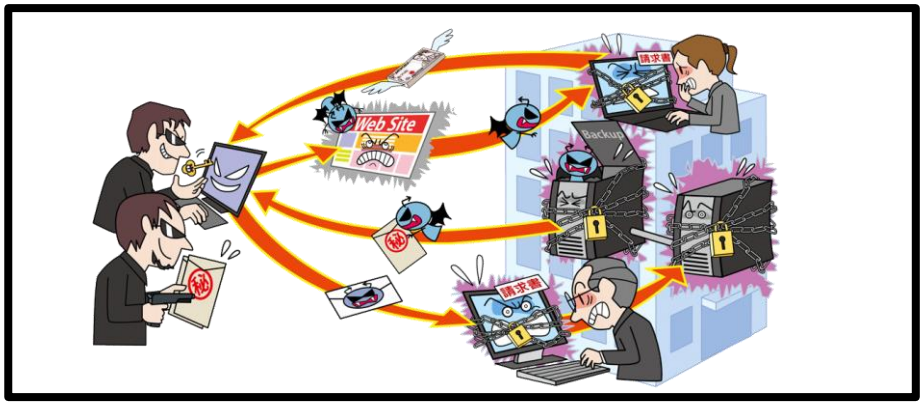
NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	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位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**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
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**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
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

＊IPA 情報セキュリティ10大脅威2022より引用

ランサムウエアによる被害

ランサムウエアは組織的犯行グループによるウィルスの一種を利用した攻撃



PCやサーバーがロックしたり、データが暗号化され利用ができなくなる。
復旧と引き換えに金銭要求をされたり、搾取された情報を公開すると脅迫するケースもある。
取引先等のメールアドレスを利用し拡散を試みることもあり、信用問題になったり、対応が長期化するなどの影響が出る。

＊IPAホームページ情報セキュリティより引用

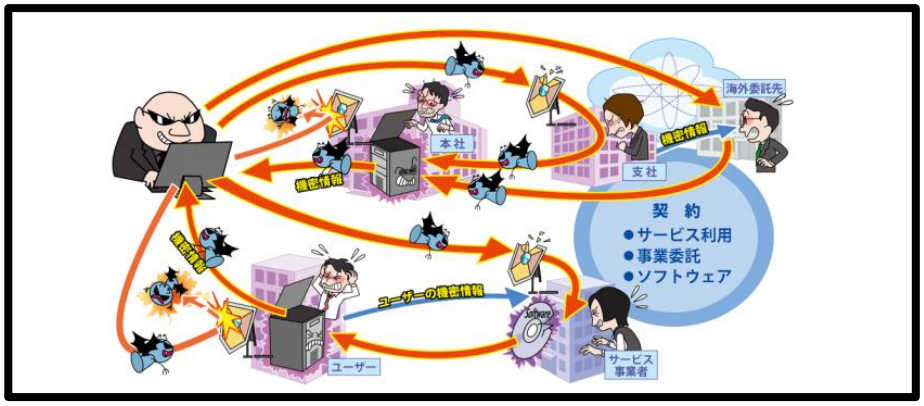
病院へのランサムウェア攻撃の事例

- 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

身代金を支払いデータを復旧したのではとの報道も…
大阪市立の医療機関でもランサムウェアの被害が発生

サプライチェーンの弱点を悪用した攻撃による被害

サプライチェーン（原材料や部品の調達、物流、販売、業務委託先等の一連の商流）において、セキュリティ対策が甘い組織が攻撃の足がかりとして狙われる



機密情報の漏えいや信用の失墜等、様々な被害が発生する。また、取引先の組織においても、自組織が被害を受けるだけでなく、取引相手にも損害を与えてしまうことで、取引相手を失ったり、場合によっては、損害賠償を求められたりするおそれがある。

＊IPAホームページ情報セキュリティより引用

自動車メーカーの事例

- 仕入れ先部品メーカーがサイバー攻撃を受けたことによる影響で国内全14工場28ラインが停止
- 仕入れ先部品メーカーの子会社のリモート接続機器の脆弱性を利用した攻撃
- 仕入れ先部品メーカーがランサムウェアに感染し全ネットワークとサーバーを停止

情報流出は確認されていない

2022年3月、県内に主要拠点がある自動車部品製造業の子会社に不正アクセスがあり情報流出の可能性あり

求められる対策①（できることから始める）

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やソフトウェアのセキュリティ上の問題点を放置していると、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。使用しているOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

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。

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窃取したID・パスワードが流用されることで、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。

4 共有設定を見直そう!

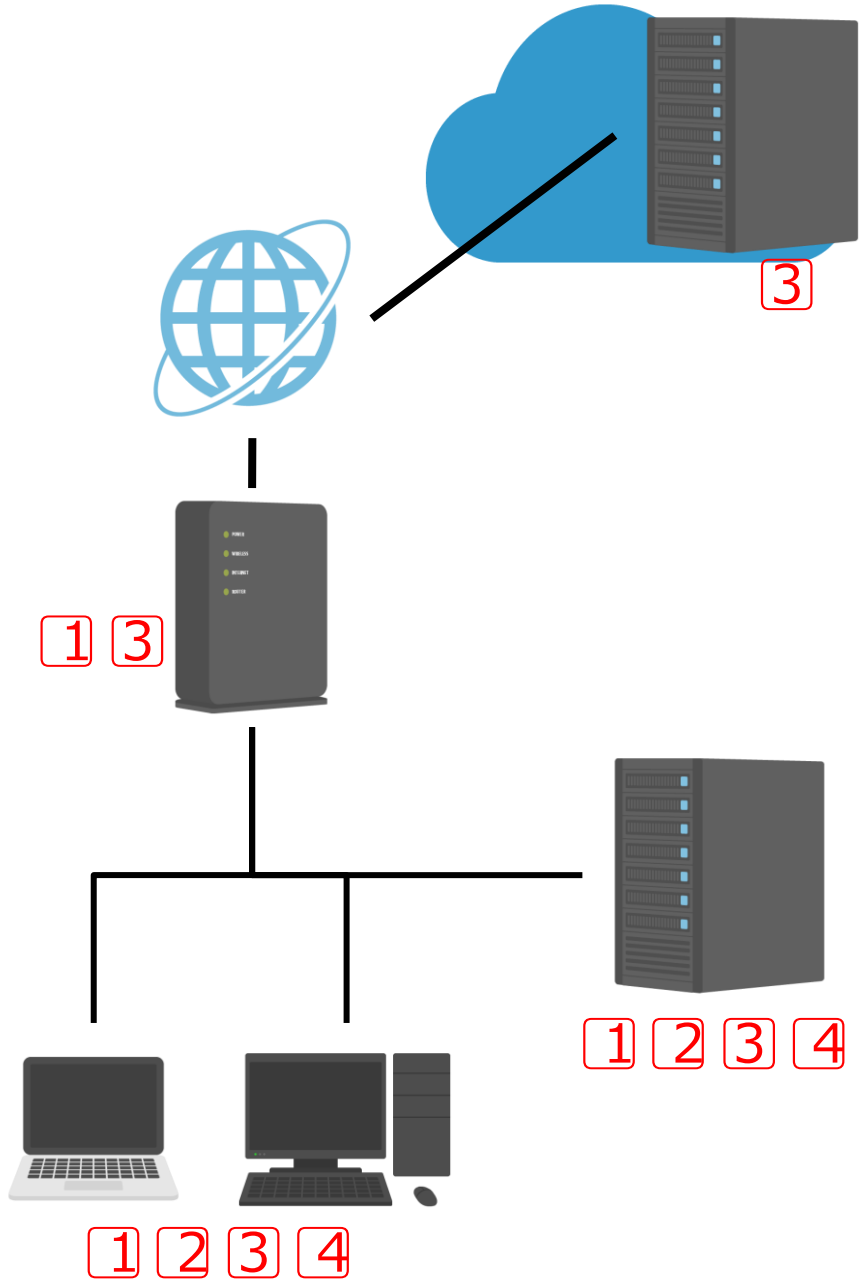
データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

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。

重要なセキュリティ情報を毎日チェックしましょう!

情報処理推進機構(IPA) 重要なセキュリティ情報一覧
https://www.ipa.go.jp/security/announce/alert.html



＊IPA情報セキュリティ5か条を引用

セキュリティ対策支援事業のご紹介

標的型攻撃やランサムウエアの被害が広がり、中小企業においてもセキュリティ対策が求められています。

ITC茨城では中小企業のセキュリティ強化支援と人材育成のための

「セキュリティ対策支援事業」を展開いたします。

①セキュリティ啓蒙セミナー

本事業の入り口です
支援機関様との連携を想定しています

②ワークショップ

自社診断

対策方法検討

対策計画策定

対策発表会

複数企業(5,6社)合同でのワークショップです
参加企業から参加費用をいただく予定です
ワークショップの詳細は次紙参照下さい

③個別コンサルティング

個別コンサルティングをご希望される企業様と
個別契約させていただきます

セキュリティ対策支援事業カリキュラム

IPA「中小企業の情報セキュリティ対策ガイドライン」に則った対策を、ワークショップ形式で行います。

自社診断	1回目、2回目：自社診断による課題抽出 5分でできる！情報セキュリティ自社診断 ネットワーク構成図等による脆弱性診断	＋ インターネットからの不正アクセス状況診断（任意）
対策方法検討	3回目、4回目：対策方法検討 課題への対策方法を検討	
対策計画策定	5回目：対策計画策定 スケジュールや体制を検討し セキュリティ対策計画書策定	
対策発表会	6回目：対策発表会	

ワークショップでのディスカッションにより、気づきや知識・経験を共有し、各自の計画書をブラッシュアップします。また、他社の実情・対策を知ることでスキルの向上を目指します。

参加企業には秘密保持の誓約をお願いします。

お問い合せ先

特定非営利活動法人　ITコーディネータ茨城

セキュリティ対策支援事業担当：後藤、根本

e-mail：goto@itc-ibaraki.com
nemoto@itc-ibaraki.com

特定非営利活動法人(NPO)

ITコーディネータ茨城