医療機関等における情報セキュリティ等の留意点

2024年１月

（一財）日本情報経済社会推進協会
常務理事　坂下哲也

自己紹介

■ （一財）日本情報経済社会推進協会（**JIPDEC**）　常務理事
【所管】電子情報利活用研究部・認定個人情報保護団体
- 芝浦工業大学　情報通信工学科　非常勤講師（通信システム設計論）

■ 日頃やっている業務
- ➢ 電子情報の保護と利用に関する基盤整備の企画・推進
  - G空間（地理空間情報）、IoT（Internet of Things）、ブロックチェーン（分散型台帳技術）、PDS（Personal Data Store）、デジタル・トランスフォーメーションなど
- ➢ データの利用やプライバシー保護に関する制度研究など

■ 政府委員等
- ➢ 静岡県デジタル戦略顧問
- ➢ 浦安市CIO補佐官
- ➢ 準天頂衛星システム事業推進委員会委員
- ➢ 国立研究法人審議会臨時委員（JAXA部会　部会長）
- ➢ 内閣府消費者委員会デジタル化に伴う消費者問題ワーキング・グループ委員
- ➢ ISO／TC211（地理空間情報）、TC307（ブロックチェーン）、TC321（EC）、TC324（シェアリングエコノミー）委員など

■ 最近の著作
- ➢ 「「信託」から見た「情報銀行」の取り組み」（『信託フォーラム　vol.19』商事法務、2023年4月）など。

■ その他
- ➢ （一社）JcoMaaS理事、（一社）ピープルアナリティクス＆HRテクノロジー協会理事　など。

はじめに

- 今日、このセミナーを受講されている皆さんは、手元にスマートフォンを持っていらっしゃると思います。
- その画面の右上には「  」の電波状況のマークが出ていると思います。

- インターネットが社会基盤となり、私達は常に「繋がっている」状態になりました。仕事でも、プライベートでも、チャットでやり取りをしたり、Web会議を行ったり、受発注を行ったり、お金の送金など便利になりました。
- 一方で、「繋がっている」状態において、セキュリティにも気を配らなくてはならなくなりました。
- 医療機関や薬局では、多くの個人情報や医療情報、処方箋などの機微情報も扱っています。
- それらの情報が漏えいなどの事故を起こした場合には、患者への被害だけではなく、事故を起こした法人に対する社会からの批判などの影響も発生します。
- 今日の講義ではセキュリティについて、どのように留意をしていくのかという点について解説をしていきます。
- 受講される皆様の対策の参考になれば幸いです。

本講義のアジェンダ

- 医療機関等で発生した事故について、どのような影響が出たのか振り返りましょう。
- どのような事故が懸念されるのか整理しましょう。
- その上で、どのように留意をしていくのか手順などを確認しましょう。

医療機関等で発生した事故の例

サイバー攻撃によるシステム障害の例

■ 経緯

時期	事象	備考
2022年10月31日	ランサムウェアの攻撃により、大規模システム障害発生。 ⇒救急受入、予定手術、初診受付などが停止。 （被害内容） ・基幹システム（電子カルテ、医事会計、看護支援等） ・部門システム（検体検査、放射線情報、給食管理等） ・連携医療機器（検査、画像、調剤などの機器約67種類） ・サーバ約100台、端末約2200台、プリンタ約400台	厚生労働省では初動対応支援チームが対応を開始。（以降、11月6日まで支援）
11月4日	予定手術一部再開	
11月10日	バックアップデータによる復元	3次救急の受入れ再開
11月17日	バックアップデータの参照環境を救急外来に設置	2次救急の受入れ再開
11月28日	同参照環境を手術室に設置	予定手術枠の拡充を実施
12月12日	電子カルテなどの基幹システムの運用再開	
12月22日	電子カルテ運用を全面再開	入院・外来対応復旧
2023年1月11日	部門システムを概ね再開（攻撃を受けてから2か月以上）	診療体制全面復旧

（参考：大阪急性期・総合医療センター　情報セキュリティインシデント調査委員会報告書について　2023年3月）

どのような影響が出たか

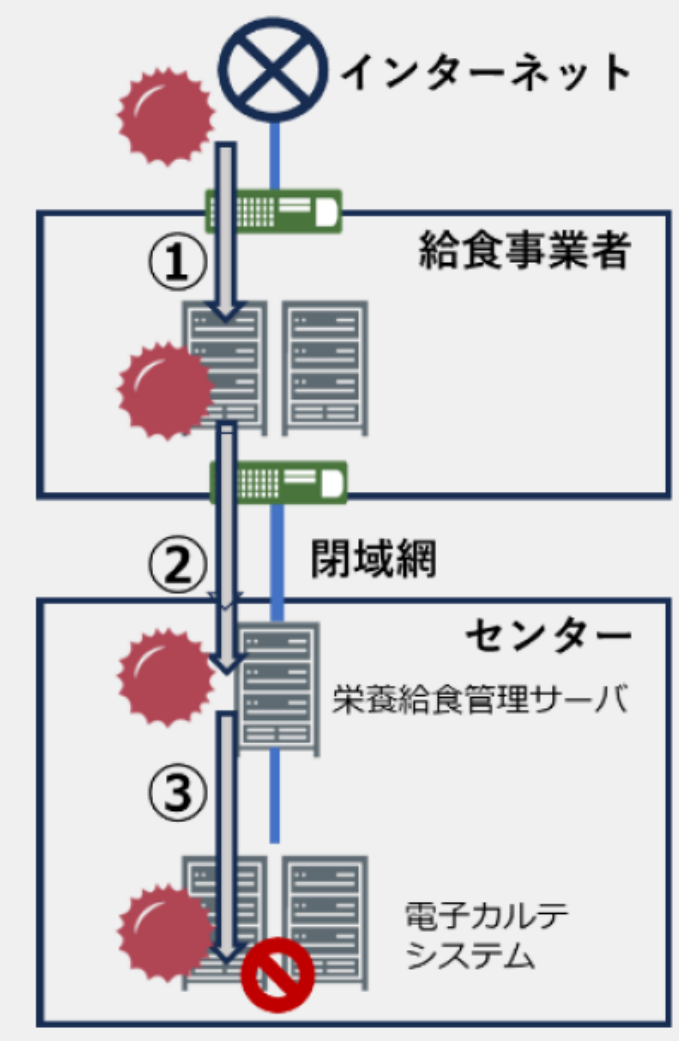
- 基幹システムサーバ内のデータの大部分がランサムウェアによる攻撃を受け、暗号化されてしまったため、診療活動に多大な影響が出た。
- 基幹システムサーバの再稼働には43日、全体の診療システムの復旧には73日を要した。
- 調査復旧に数億円、診療制限に伴う逸失利益として十数億円以上が見込まれる。（報告書では精査中と記述。）

	2021年11月と2022年11月の比	2021年12月と2022年12月の比
新入院患者数	**33%**	**55%**
延べ入院患者数	53%	56%
初診患者数	**18%**	**43%**
延べ外来患者数	62%	70%
中央手術室手術件数	**28%**	**39%**
救急車搬入件数	**13%**	**67%**
入院診療行為額	**47%**	**57%**
外来診療行為額	**56%**	**65%**

（参考：大阪急性期・総合医療センター　情報セキュリティインシデント調査委員会報告書について　2023年3月）

攻撃の手口

■ 病院と契約する給食事業者が攻撃を受け、事業者と閉域網で接続するセンターの栄養給食管理サーバに不正アクセスし、そこを踏み台として、病院の電子カルテシステムを攻撃。



①給食事業者との通信の境界となっているネットワークから内部へ侵入し、拡散。
（設置されていたVPN機器（離れた拠点間を仮想的な専用線でつないで通信できるようにする機器）に脆弱性があった。）
⇒繋がる環境では取引先の通信環境も管理しなくてはならない。

②閉域網（限られた利用者のみが利用可能な広域通信網、物理的または論理的にインターネットに接続していないネットワーク）のため、境界の防御は一般的にされていない。

③栄養給食管理サーバを踏み台にして、センター内ネットワークに侵入し、電子カルテシステムを攻撃。
⇒システムのユーザ全てに管理者権限を与えていたために、感染範囲が拡大。

（参考：大阪急性期・総合医療センター　情報セキュリティインシデント調査委員会報告書について　2023年3月）

サイバー攻撃や事故によって漏洩が懸念される場合の対応

漏えい等報告等の義務化

■ 漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、委員会への報告及び本人への通知の義務化。（個人情報保護法）

報　告

漏えい等報告の義務化の対象事案
（委員会規則で定める要件）

- **要配慮個人情報の漏えい等**
- **財産的被害のおそれがある漏えい等**
- **不正の目的によるおそれがある漏えい等**
- **1,000件を超える漏えい等**

これらの類型は件数に関わりなく対象

※各類型につき、漏えい等の「おそれ」がある事案も対象。

通　知

事故が起きた場合の対応

■ 漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、個人情報保護委員会への報告及び本人への通知を義務化。

類型	事例
要配慮個人情報の漏えい等	従業員の健康診断等の結果を含む個人データが漏えいした場合
財産的被害のおそれがある漏えい等	送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合
不正の目的によるおそれがある漏えい等	不正アクセスにより個人データが漏えいした場合
1,000件を超える漏えい等	システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合

	時間的制限	報告内容
速報	報告対象の事態を知ってから「速やかに」（個別の事案によるものの、当該事態を知った時点から概ね3～5日以内）	報告をしようとする時点において把握している内容
確報	報告対象の事態を知ってから30日以内（不正の目的によるおそれがある漏えい等の場合は60日以内）	全ての報告事項（合理的努力を尽くしても、全ての事項を報告できない場合は、判明次第、報告を追加）

	考えられる具体例
本人へ通知が困難	● 保有する個人データの中に本人の連絡先が含まれていない ● 連絡先が古いために通知を行う時点で本人へ連絡ができない等。
代替措置	● 事案の公表 ● 問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにする等。

どのような脅威があるのか

情報セキュリティ10大脅威

■ （独）情報処理推進機構（IPA）では、『情報セキュリティ10大脅威 2023』を公開し、セキュリティ対策を呼び掛け。

法人10大インシデント	解説
ランサムウェアによる被害	2023年11月市民病院では、財務会計システムのサーバがランサムウェアに感染し、取引先事業者に関する情報が流出した可能性を発表。
サプライチェーンの弱点を利用した攻撃	セキュリティ対策が弱い取引先企業を狙い、そこから本丸である企業に侵入する手口
標的型攻撃メールによる情報の窃取	2020年標的型攻撃として報告されたものは3978件
内部不正による情報の漏洩	被害が大きい事が特徴
テレワークを狙った攻撃	家庭のWiFiに侵入する攻撃が増加
修正プログラムの公開直前を狙う攻撃	ゼロデイ攻撃という手法 例えばウィルス対策ソフトのパターンファイルが更新される前に侵入等
ビジネスメール詐欺	手口がより巧妙に。
公開された脆弱性情報を利用した攻撃	ネットワーク型カメラにアクセスされ店内映像が漏洩した等
不注意による情報漏洩	**もっとも事故報告が多いもの**
ビジネス化している犯罪による被害	アンダーグラウンドサービスと言われ、昨今増加している。

（公開URL：https://www.ipa.go.jp/security/10threats/10threats2023.html）

テレワークを狙った攻撃

■ **2023年4月5日　警視庁は「家庭用ルーターの不正利用に関する注意喚起について」を公開。**

- 一般家庭で利用されているルーターを、サイバー攻撃者が外部から不正に操作して搭載機能を有効化するもの。
  - 一度設定を変更されると従来の対策のみでは不正な状態は解消されず、永続的に不正利用可能な状態となってしまう。

■ チェックするポイント

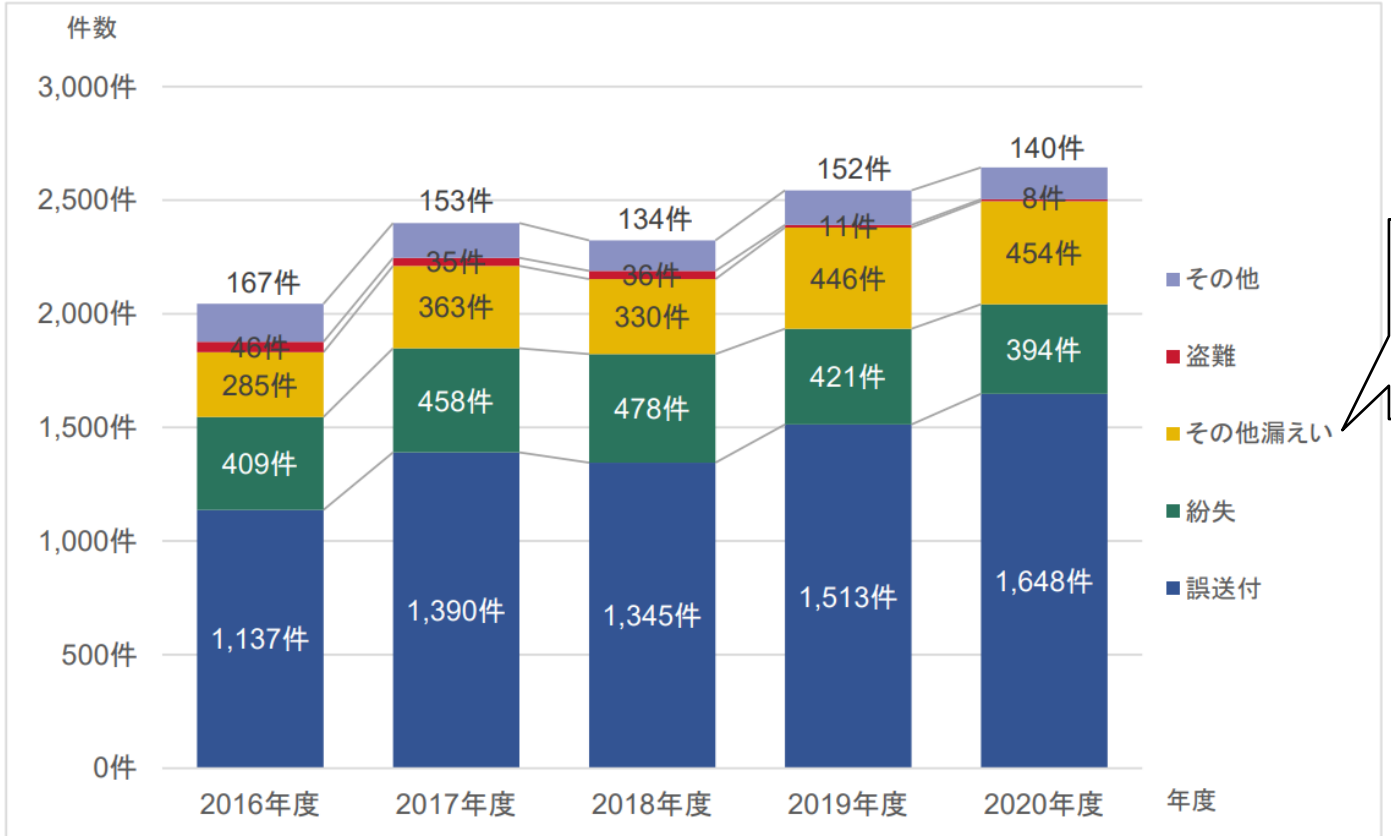
- 暗号化方式は**「WPA3」**に設定することを推奨。
- 初期設定の単純なIDやパスワードは変更する。
- 常に最新のファームウェアを使用する。
  - サポートが終了したルーターは買い替えを検討する。
- **見覚えのない設定変更がなされていないか定期的に確認する。**
  - ルーターの管理画面で以下を確認
    - 見覚えのない「VPN機能設定」や「DDNS機能設定」、「インターネット（外部）からルーターの管理画面への接続設定」の有効化がされていないか。
    - VPN機能設定に見覚えのないVPNアカウントが追加されていないか。
  - 対応
    - 見覚えのない設定があった場合、ルーターの初期化を行い、ファームウェアを最新に更新した上、ルーターのパスワードを複雑なものに変更。

（図の出典：警視庁）

（警視庁リーフレット：https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.files/leaflet.pdf）

不注意による情報漏えい

- 当協会認定個人情報保護団体事務局に報告される事故は年間1500件から2000件で推移。
- **最も多い事故が「誤交付・誤送付・誤送信」で6～7割を占める。**
- 近年は、**外部からの攻撃・セキュリティの脆弱性・システムのバクなど**により数千件以上の個人情報が流出・漏洩するケースも増加・。



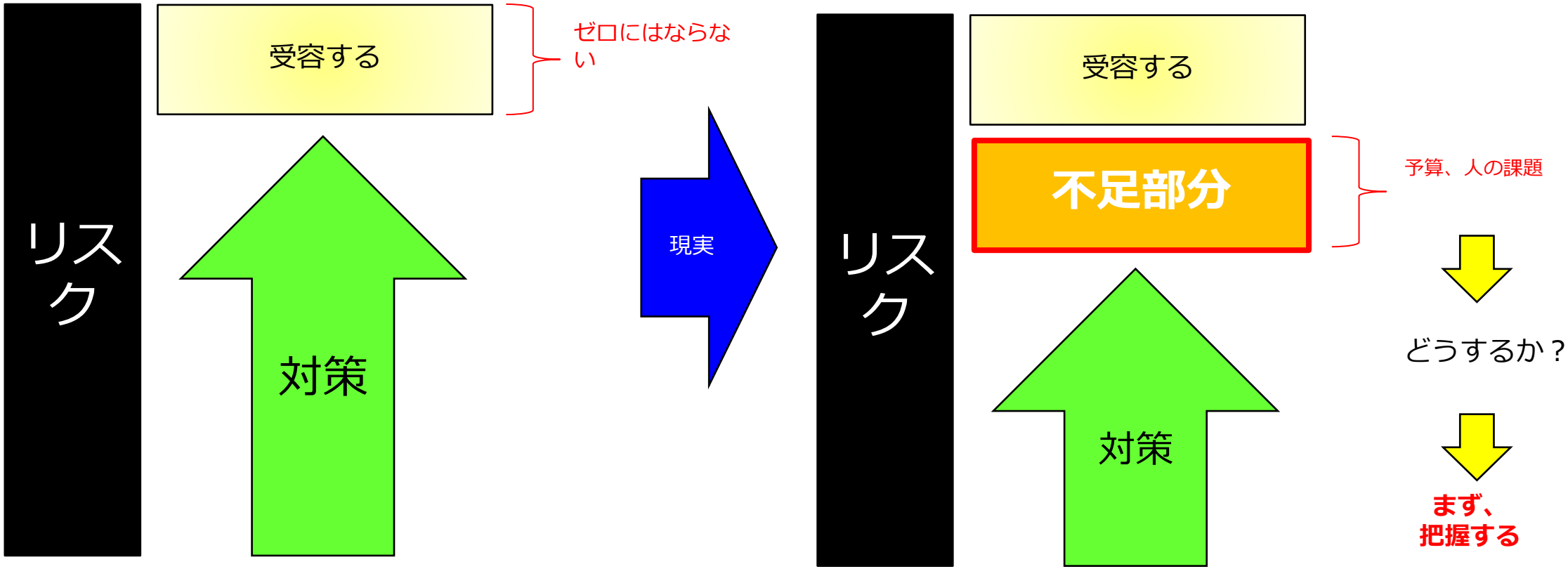
ウィルス感染、不正アクセス、プログラムの設計ミスなど。

（出典：JIPDEC「個人情報の取扱いにおける事故報告集計結果」、2022年10月）

対策の考え方

リスクの対処方法

- リスクを事前に確認することが必要。
- リスクの対処方法
  - 受容する　＝　認める
  - **転嫁する　＝　影響や責任の一部または全部を第三者に託す。（マネジメントシステムの運用）**
  - 回避する　＝　対策を打つ



プライバシーマークとISMSの違い

- **ISMS**は『ISO/IEC27000シリーズ』に基づいて、**情報セキュリティ・マネジメントシステムの適合性を評価**するもの。
  - リスクアセスメントに基づいて、情報セキュリティマネジメントシステムが計画・実施・点検・改善が行われているかを審査。
  - 情報セキュリティは、全社ということではなく、システムやデータなど様々な対象になるため、**情報資産として認証を取得する事業者が指定し、それを扱う組織（部署、機械など）を対象に認証**。

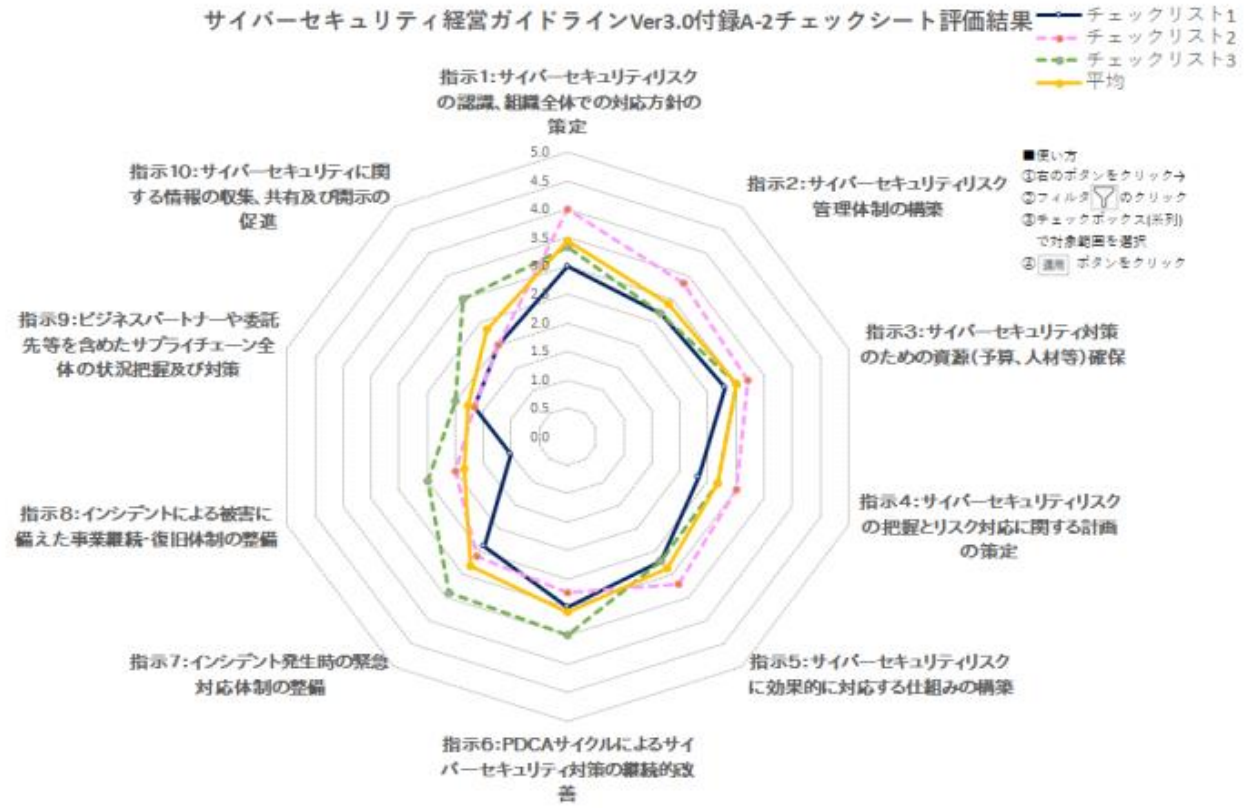
- **プライバシーマーク制度**は、個人情報を保護するために作られた『JIS Q 15001（個人情報保護マネジメントシステムの要求事項』を元に、当協会が提供している認証サービス。
  - **個人情報について“取得・保管・利用・提供・廃棄”のプロセスに求められる“個人情報・個人データ・保有個人データ“などの要件が遵守されていることを認証。**
  - 個人情報の保護が目的のため、この認証によって**『当社は個人情報の保護について個人情報保護法に求められている以上の十分な対策を取っている』**ことを示す。
  - また、個人情報保護法は企業単位にかかる法律であるため、**全社で同一の個人情報保護のマネジメントを行っていることを表している**。

まずはここから

■ 自社の状況を知る

➢ **サイバーセキュリティ経営可視化ツール（IPA：独立行政法人情報処理推進機構）**

- 小規模の企業でも利用できる。
- 弱い部分が可視化されたら、「サイバーセキュリティ経営ガイドライン」（同）の「サイバーセキュリティ経営の重要10項目」の項目と照らして対策を検討。



図．可視化結果のレーダーチャート表示例

（公開サイト：https://www.ipa.go.jp/security/economics/checktool.html）

安全管理措置の4要素

■ セキュリティ対策という狭域な視点だけはなく、安全管理措置という全体的な視点で考えることが必要。

項目	内容	ポイント
組織的対策	取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について個人データの取扱規程を策定し、整備運用し、その実施状況を確認等。 （連絡手順、広報対応手順など）	**やる人とやる事を明確にする。**
人的対策	・個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施 ・個人データについての秘密保持に関する事項を就業規則に記載等。	**研修などを通じて言い続ける。**
技術的対策	情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等。	**リスク分析の中で、組織的・人的対策では対応できない範囲を絞る。**
物理的対策	入退室管理、廃棄証明をもらう等。	

支援策の例

中小企業向けサイバーセキュリティ対策の支援例

- 2022年10月28日、公正取引委員会は、中小企業に対するサイバーセキュリティ対策の支援と取引先への対策支援・要請に係る関連法令の適用を整理。
- 取引先の中小企業へのサイバーセキュリティ対策の要請は、ただちに独占禁止法・下請法の問題とはならないとした。
  - ただし、相応のコスト負担を上位の取引先が行わない場合は問題となる。
- 整理の内容を発表し、支援策も提示。
  - **サイバーセキュリティお助け隊サービス**
    - 中小企業等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提供する事業者を、IPAが登録・公表。
    - 対象
      - **見守り**（24 時間監視し挙動や問題のある攻撃を検知）
      - **駆付け**（問題が発生したときに地域の IT 事業者等が駆付け対応）
      - **保険**（簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストを補償）
  - 利用料はIT導入補助金の対象。

サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて（概要）

令和４年10月28日
経済産業省
公正取引委員会

【背　景】

- 昨今、サイバーセキュリティ対策が不十分な**中小企業がサイバー攻撃に狙われ、サプライチェーン全体に問題が波及**する事態が発生。
- 令和４年４月、「原油価格・物価高騰等に関する関係閣僚会議」（内閣総理大臣、内閣官房長官、関係大臣、公正取引委員会委員長が出席）において、**コロナ禍における「原油価格・物価高騰等総合緊急対策」**を決定。

「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のないよう、**中小企業等におけるサイバーセキュリティ対策を支援**するとともに、**取引先への対策の支援・要請に係る関係法令の適用関係について整理**を行う。」

【内　容】

- 発注者側となる事業者は、以下を参考に、サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築を目指していただきたい。

①サイバーセキュリティ対策に関する支援策

- **サイバーセキュリティお助け隊サービス**（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サービスをワンパッケージで提供）の利用促進
- **セキュリティアクション**（中小企業がセキュリティ対策に取り組むことを宣言）の推進
- **中小企業の情報セキュリティ対策ガイドライン**（中小企業を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき方針、対策を実践する際の手順や手法をまとめたもの）の活用
- **パートナーシップ構築宣言**（発注側企業が取引先との間でパートナーシップを構築することを宣言）の中で、取引先にサイバーセキュリティ対策の助言・支援を行うことを取組例として記載

②サイバーセキュリティ対策の要請に係る独占禁止法・下請法の考え方

- サイバーセキュリティ対策の必要性が高まる中、**サプライチェーン全体のセキュリティ対策強化は重要**な取組。サイバーセキュリティ対策を要請すること自体が直ちに問題となるものではない。
- ただし、要請の方法や内容によっては、問題となることもあるため、そのようなケースを例示。

＜問題となるケースの例＞

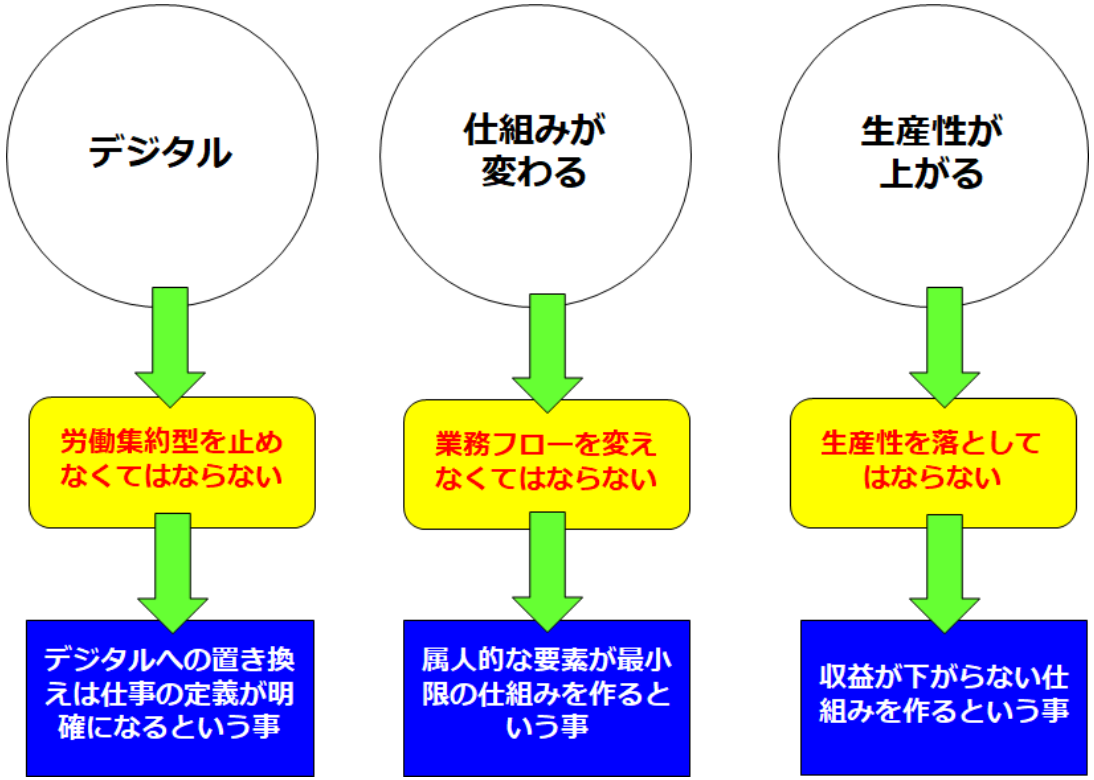
①取引上の地位が優越している事業者が、サイバーセキュリティ対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合

②取引上の地位が優越している事業者が、新たなセキュリティサービスを利用する必要がないにもかかわらず、自己の指定する事業者が提供するより高価なセキュリティサービスの利用を要請し、当該事業者から利用させる場合

（公開URL：https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html）

まとめ

- 紙で処理をする場合、①紙の情報は複製に人手がかかる（書き写す、入力する）、②紙の情報は一元的に把握するには手間がかかる（ファイルに綴る）、③紙の情報は閲覧記録が残らないので、プライバシーが保護されたか分からないなどの問題があります。
- これをデジタル化すると、①複製の手間がなくなり、②一元管理が効率化され、③閲覧記録も残るようにする事ができます。
- 受講されている企業の皆様にはDX（デジタルトランスフォーメーション；従来の業務フローを見直し、やり方を変える事）の取組みも進めておられると思います。その中で、セキュリティや個人情報の扱いについても、現状をしっかり点検し、合理的な仕組みを構築して頂きたいと思います。
- 但し、セキュリティは自己責任のみで全て実行できるものではありません。組織経営者、システム開発者・管理者、利用者、技術や法制度などの専門家などがそれぞれの立場から、知恵を出し合い、実現するものです。
そのことを忘れずに、「今できる最善の策」を打ちましょう。



ありがとうございました。