（公社）医業経営コンサルタント協会継続研修

公益社団法人
日本医業経営コンサルタント協会
Japan Association of Healthservice Management Consultants

医療・介護における情報セキュリティの現状と対策

日時：平成25年12月13日（金）
10:00～12:00
場所：ホスピタルプラザ2Fセミナー室

医業経営コンサルタント・情報化認定コンサルタント
経営学博士（Ph.D.） 小野瀬　由一

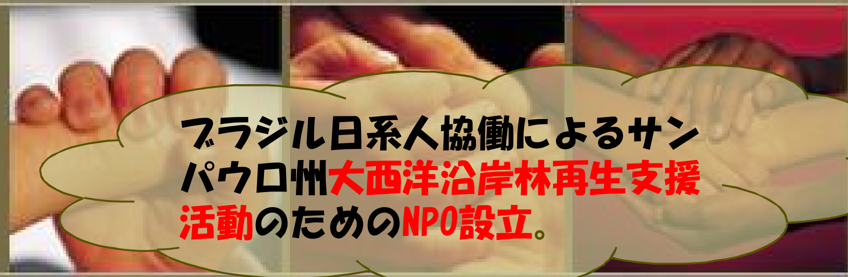
目次

0. 講師の活動紹介
1. 医療・介護関連情報セキュリティ事故の現状
2. 情報セキュリティの基礎
3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点
4. 医療情報システム安全管理ガイドラインの要点
5. 医療・介護の情報セキュリティ対策（まとめ）

◆参考資料

◆講師プロフィール

0. 講師の活動紹介①



ブラジル日系人協働によるサンパウロ州大西洋沿岸林再生支援活動のためのNPO設立。

図表0.1. NPO法人VERSTAの立上

NPO法人VERSTA(注1)のご案内 Ver.12.0

地球環境の持続可能性を高めるためには、低炭素社会の実現を図ると同時に、地球上のCO2主要吸収源である海洋と森林の保全を図ることが重要です。地球面積のわずか9%の森林が地球上のCO2吸収源の約半数を占めています。しかし、近年、特に南米の熱帯雨林の違法伐採が進み、大気中のCO2残存の増加による地球温暖化が危惧されています。

私たちNPO法人VERSTAは、熱帯雨林の再生・保全に役立つ農法として世界的な注目を集めているアグロフォレストリー(注2)の普及を支援することにより、持続可能な地球環境保全に貢献することを理念とします。

◇ビジョン

本法人は、アグロフォレストリー普及活動を支援し、CO2の吸収源である熱帯雨林の再生・保全を図ることにより持続可能な地球環境保全を目指します。

◇ミッション

本法人は、理念及びビジョンを実現するため、以下の第1事業及び第2事業により寄付金を集め、寄付金を原資に第3事業及び第4事業を行い、アグロフォレストリーの普及推進を図ります(事業の概要は裏面参照)。

第1事業　アグロフォレストリー支援チャリティライブ(AGROFORESTRY AID)事業
第2事業　アグロフォレストリーポイント(AF POINT)事業
第3事業　アグロフォレストリー支援事業
第4事業　アグロフォレストリー産地＆産品認証および森林CDM推進事業

◇コミットメント

本法人は、熱帯雨林のサスティナブルな再生・保全の重要性を世に伝承し、支援活動による継続的な熱帯雨林の再生・保全体制の整備に寄与することを責務とします。

◇会員制度

・正会員(個人)：年会費1万円。VERSTA WEB上でお名前を公表致します。
・賛助会員(法人・団体)：年会費5万円。VERSTA WEB 上で法人・団体名を公表致します。

◇お問合せ＆会員入会申込み

・お問合せ及びVERSTA会員入会申込みは下記URLの「会員制度」のフォーマットをご利用願います。

◇私たちがVERSTA活動を行なっています。

・理事長：森田 松太郎(公認会計士・日本ナレッジ・マネジメント学会理事長)
・副理事長：酒井 昭夫(㈱カフェ・ド・セントロ・ジャパン代表取締役)
・専務理事：小野瀬 由一(ICG国際コンサルタント・経営学博士)
・理事：伊藤昌輝(元ベネズエラ全権大使・ラテンアメリカ協会常務理事)
・理事：[illegible](慶応義塾大学大学院SDM研究所研究員)
・理事：大畑 聡 (元社団法人日本ショッピングセンター協会専務理事)
・理事：河田 [illegible](スクワイヤー＆サンダース法律事務所所属・ブラジル法弁護士)
・理事：[illegible]
・理事：[illegible]
・理事：[illegible](富士クラスタ株式会社代表取締役社長)
・理事：[illegible] (㈱STV-JAPAN 代表取締役社長・SMG取締役)
・理事：[illegible](外交ジャーナリスト・作家・慶応大学大学院教授)
・理事：デレオン礼子(ラテン文化サロン代表)
・理事：[illegible](㈱大洋システムテクノロジー執行取締役社長)
・理事：[illegible]
・理事：[illegible](㈱アイアック・インターナショナル取締役)
・監事役：[illegible](公認会計士・森田会計事務所)

◇ブラジル人特別顧問

・特別顧問：イシドロ山中 (元伯国農牧供給大臣特別補佐官)
・特別顧問：ゲンジ山添 (元伯国サンパウロ州森林院院長)
・特別顧問：ロドリゴ・ブランコ・ベレス (ブランコ・ベレス社長)

注1) VERSTAという名称は、ポルトガル語及びスペイン語の緑(VERDE)とサンバ等の祝祭(FESTIVAL)を合成したもので [illegible]
注2) アグロフォレストリーとは、農業(Agriculture)と林業(Forestry)の [illegible]

◇私たちはVERSTA活動を応援しています。

・慶應義塾大学大学院SDM研究所
・日系YOUTH NETWORK
・エコピープル支援協議会

◇賛助会員

・カフェ・ド・セントロ・ジャパン、富士クラスタ、STV-Japan、大洋システムテクノロジー

VERSTA
〒103-0022　東京都中央区日本橋室町3－1－10　田中ビル4F　日本ビジネスソリューション内
特定非営利活動法人VERSTA事務局　小野瀬・森田　電話：03－3270－0020
URL：http://www.versta.org/　Mail：verstaoffice@versta.org

NPO法人VERSTA支援活動の概要

◇第1事業：アグロフォレストリー支援チャリティライブ(AGROFORESTRY AID)事業

本事業は、本法人の趣旨に賛同したアーティスト＋音楽ファン＋協賛企業の協力によりチャリティライブを定期的に開催し、チャリティによる寄付金を「アグロフォレストリー(AF)基金」に積立てます。なお、AF基金は対象国の熱帯雨林等のアグロフォレストリー普及支援活動の原資として利用されます。

◇第2事業：アグロフォレストリーポイント(AFポイント)事業

本事業は、本法人と民間企業等との連携により、ポイント運営会社による「アグロフォレストリーカード」を発行しカード会員の商品・サービス購入に対し「アグロフォレストリー(AF)ポイント」を付与します.ポイントの一部または期限切れポイントを「AF基金」として積み立てます。

なお、AF基金は対象国の熱帯雨林等のアグロフォレストリー普及支援活動の原資として利用されます。

◇第3事業：アグロフォレストリー支援事業

本事業は、本法人の事業活動により積換した「AF基金」を原資にして、アグロフォレストリー活動団体に対し活動資金を提供することによりアグロフォレストリーの普及支援を図ります。

なお、アグロフォレストリー支援活動は、将来的にブラジル以外の熱帯雨林を有する国または熱帯雨林の周辺国への支援拡大を図ります。

◇第4事業：アグロフォレストリー産地＆産品認証および森林CDM推進事業

本事業は、本法人と協力企業等との提携により、アグロフォレストリー産地＆産品認証に対する日本の消費者の安心・安全の確保とブランド価値の向上を図るため、アグロフォレストリー産地＆産品認証事業に取組みます。また、アグロフォレストリー支援を通じ森林CDM推進のための条件整備に取り組みます。

◆VERSTAジュサラ椰子アグロフォレストリー支援事業が平成24年度地球環境基金助成を受けて本格的にスタートしました！

VERSTAが支援活動を準備しておりました「ブラジル連邦共和国サンパウロ州大西洋岸森林保全再生のためのジュサラ椰子(Euterpe edulis)を主成分とした小農アグロフォレストリー推進ネットワーク形成事業」が、独立行政法人環境再生保全機構(環境庁管轄)の平成24年度地球環境基金助成案件として採択されました。

これにより、VERSTAのブラジル熱帯雨林保全再生支援事業が本格的にスタートしました。

・対象地域：サンパウロ州セテバラス市

・カウンターパート組織：サンパウロ州環境局森林院・環境局森林財団・農務局農事試験場・セテバラス市・サンカルロス連邦大学・カンピナス州立大学ほか

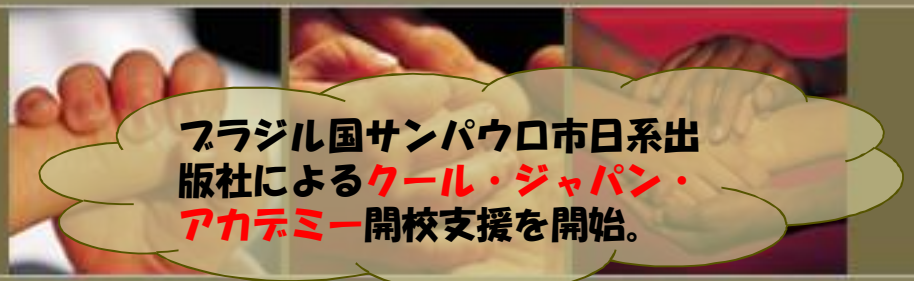
◇活動概念図

0. 講師の活動紹介②

図表0. 2. NPO法人VERSTAによるブラジル大西洋沿岸林再生・支援活動

年月	最新活動概要	年月	最新活動概要
平成23年12月	・「AF AID Vol.3」をSHIBUYA LOOP -Annexにて開催。出演アザブ・スミス他、来場者約50名	平成24年7月	・セッテ・バラース市にてVERSTAジュサラ椰子アグロフォレストリー支援共同プロジェクト会議（11日） 
平成24年4月	・VERSTAジュサラ椰子アグロフォレストリー支援事業が平成24年度地球環境基金助成対象として決定。		・サンパウロ州環境局森林院表敬訪問及び意見交換（12日） 
平成24年7月	・平成24年度VERSTAジュサラ椰子アグロフォレストリー支援事業開始。 ・グアピルブ村農業組合との意見交換（9日）  ・リオプレット村小農家との意見交換及びジュサラ椰子記念植樹（10日） 		・第15回日本まつり会場にてJICAブラジル遠藤次長と意見交換（13日） 

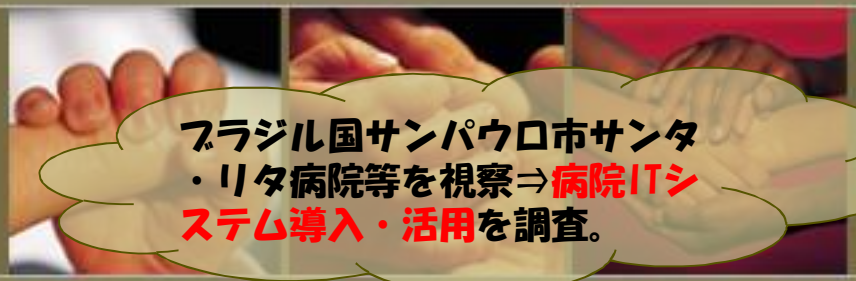
0. 講師の活動紹介③



ブラジル国サンパウロ市日系出版社による**クール・ジャパン・アカデミー**開校支援を開始。

図表0.3. ブラジルにおけるクール・ジャパン・スクール（仮称）構想支援

0. 講師の活動紹介④



ブラジル国サンパウロ市サンタ・リタ病院等を視察⇒病院ITシステム導入・活用を調査。

図表0.4.サンパウロ市「サンタ・リタ病院（2006年ブラジルベスト病院賞受賞）」

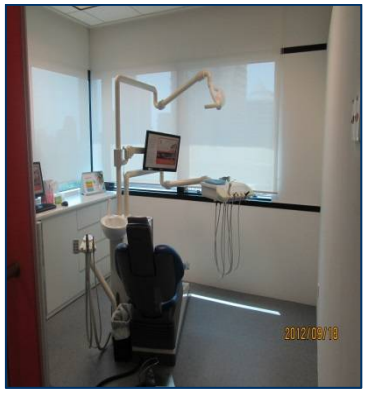
0. 講師の活動紹介⑤

2012年JAHMAC海外病院視察調査に参加⇒マレーシアとシンガポールの4病院を調査。

図表0.5. マレーシア・シンガポール医療ツーリズム視察(2012.9.17~9.19)

SIME DSRBY MEDICAL CENTER

HSC MEDICAL CENTER

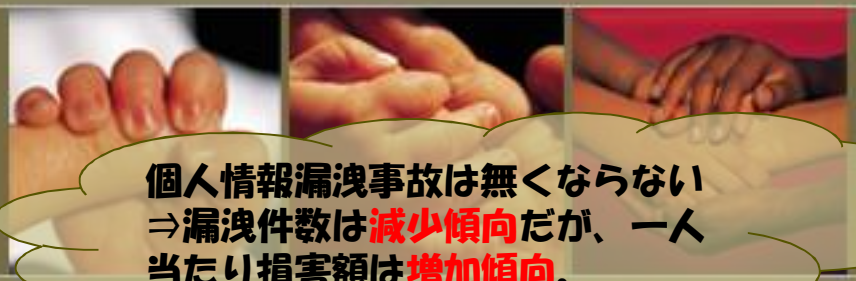


Asia Healthcare Dental Center

NATIONAL UNIVERSITY HOSPITAL

1. 医療・介護関連情報セキュリティ事故の現状

1. 個人情報セキュリティ事故の現状



個人情報漏洩事故は無くならない
⇒漏洩件数は減少傾向だが、一人当たり損害額は増加傾向。

図表1. 1. 個人情報漏洩事故の推移

項目	2010年 通年	2011年 通年	2012年 上半期
漏洩人数	557 万9316人	628万4363人	123万9626人
インシデント件数	1679件	1551件	954件
想定損害賠償総額	1215 億7600万円	1899億7379万円	347億9865万円
1件当たり平均漏洩人数	3468 人	4238人	1349人
1件当たり平均賠償額	7556万円	1億2810万円	3787万円
1人当たり平均損害賠償額	4 万3306 円	4万8533円	5万7710円

出典：NPO日本ネットワークセキュリティ協会ホームページより引用

◆NPO日本ネットワークセキュリティ協会によると、2012 年上半期（1 月1 日～6 月30 日）の日本の個人情報漏えい件数は954 件、漏えい人数は123万9626 人、被害総額は347 億9865 万円で、一件当たり漏えい人数は1349 人、一件当たり平均損害額3787 万円、一件当たり平均損害賠償額は5万7710 円と大型化傾向にある。
◆2010年から2012年の推移では、個人情報漏洩人数インシデント件数は共に減少傾向にあるものの、賠償総額は大型化傾向にあり、スマートフォンやモバイル端末の本格普及に伴い、1人当たり平均損害賠償額の増加が懸念される。

1. 医療・介護関連情報セキュリティ事故の現状

医療・福祉個人情報漏洩事故は全体4位⇒漏洩件数と漏洩人数は減少傾向だが、2012年は増加傾向。

図表1. 2. 業種別個人情報漏洩インシデント件数の推移

業種別	2010年 通年	2011年 通年	2012年 上半期
公務 〈他に分類されるものを除く〉	1位：555件 （ 57,921 人）	1位：516件 （202,791人）	1位：319件 （41,733人）
金融・保険業	2位：420 件 （993,112人）	2位：332件 （3,793,519人）	3位：171件 （603,830人）
教育・学習支援業	3位：191件 （ 134,805 人）	3位：216件 （99,271人）	2位：206件 （23,499人）
医療・福祉	4位：156 件 （ 337,549人）	4位：109件 （70,124人）	4位：69件 （68,736人）
情報通信業	5位：80件 （2,548,757人）	5位：95件 （370,909人）	6位：38件 （6,006人）
サービス業 （他に分類されないもの）	6位：58件 （520,450人）	8位：36件 （60,540人）	8位：30件 （149,430人）
卸売業・小売業	7位：55件 （341,647人）	7位：48件 （189,632人）	7位：22件 （13,898人）

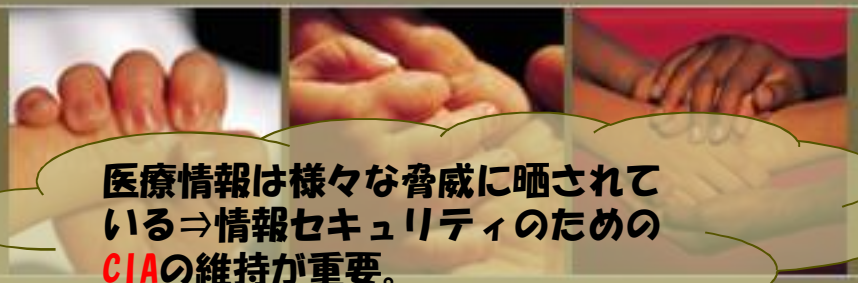
出典：NPO日本ネットワークセキュリティ協会ホームページより引用

◆同協会によると、2012 年上半期の医療・福祉分野の個人情報漏洩件数（漏洩人数）は69件（68,736人）で、漏洩件数では4位／15業種にランキングされている。
◆また、医療・福祉分野の個人情報漏洩原因は、第1位管理ミス（24.9%）、第2位誤操作（30.3%）、第3位紛失・置忘れ（18.8%）、第4位盗難（17.4%）、第5位不正な持出（5.8%）の順となっている。
◆医療・福祉分野が他の業種と比べて比較的多いのは盗難及びUSB等可搬記録媒体による漏洩であり、物理的・人的対策が求められる。

2. 情報セキュリティの基礎

2. 情報セキュリティの基礎

1）情報セキュリティのCIA



医療情報は様々な脅威に晒されている⇒情報セキュリティのためのCIAの維持が重要。

図表2. 1. 企業情報をめぐる脅威

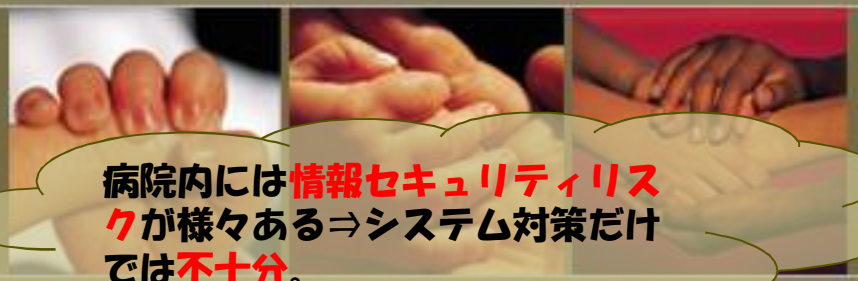
出典：NPO日本ネットワークセキュリティ協会「中小企業が知っておくべき情報セキュリティ対策（基礎編）」より引用

Plan

◆企業情報をめぐって、ICTの発展や情報記録媒体の普及に伴い、様々な脅威が存在している。
◆情報セキュリティとは、JISQ27001:2006では「情報の機密性（C）、完全性（I）及び可用性（A）を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めても良い。」と定義されている。
◆情報セキュリティの三大要件はCIAである。
・**機密性**（Confidentiality）の確保：情報資産を正当な権利を持った人だけが使用できる状態にしておくこと⇒対策：情報漏洩防止、アクセス権の設定など
・**完全性**（Integrity）の確保：情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと⇒対策：改ざん防止、検出など
・**可用性**（Availability）の確保：情報資産を、必要な時に使用できること⇒対策：電源対策、システムの二重化など

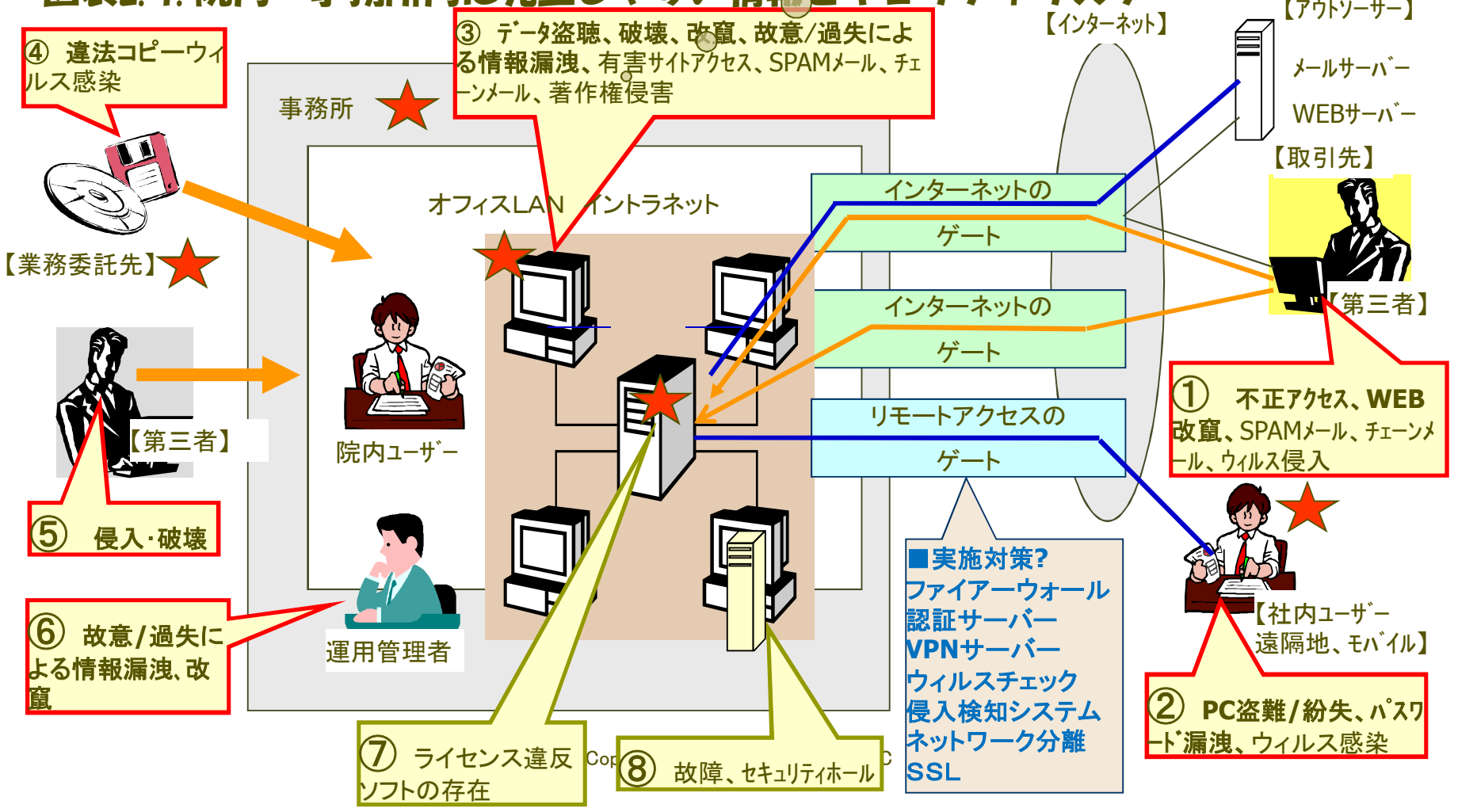
2. 情報セキュリティの基礎

2）情報セキュリティリスク



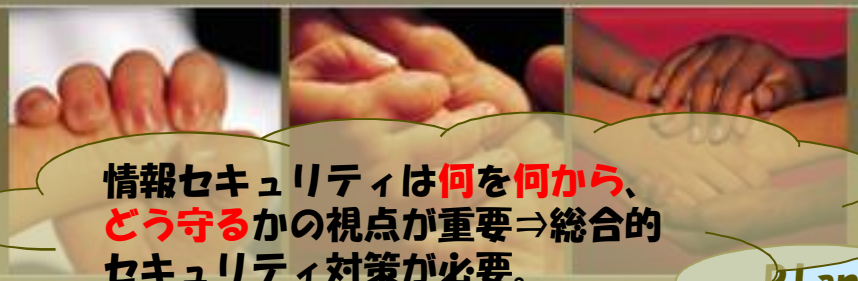
病院内には情報セキュリティリスクが様々ある⇒システム対策だけでは不十分。

図表2. 1. 院内・事務所内に発生しやすい情報セキュリティリスク



2. 情報セキュリティの基礎

3)情報セキュリティ対策の体系



情報セキュリティは何を何から、どう守るかの視点が重要⇒総合的セキュリティ対策が必要。

Plan

図表2.3.情報セキュリティ対策の体系

何を

情報資産の運用と管理

企業情報
営業・技術
個人情報
顧客・従事者
IT機器・ソフト

情報資産

脆弱性
- ビジネスプロセス
- 人
- 組織
- アプリケーション
- 建物・設備
- ネットワーク
- IT機器

リスク発生！

情報資産
漏洩・破壊
⇒信用崩壊
⇒人材流出
⇒経営体制弱体化
⇒技術資産流出
⇒設備資産破壊

どう守る

総合的なセキュリティ対策
安全管理措置

マネジメント対策
- 経営者関与
- 組織的対応
- 人的対応
- 物理的対応

技術対策
技術的対応
⇒SSL
⇒FireWall
⇒ウィルスソフト
⇒VPN・・・

● 情報セキュリティ管理システム（ISMS）の確立
⇒方針、責任権限の明確化
⇒経営全般のリスクマネジメントの確立
⇒文書管理／記録管理の徹底等

脅威

何から

①故意による**意図的脅威**
- 不正アクセス
- 紛失、破壊
- 改竄、漏洩
- 悪用
- 著作権侵害、プライバシー侵害
- コンピュータウィルス
- 中傷・スパムメール

②事故・過失による**偶発的脅威**
- ハード障害
- ネットワーク障害
- ソフトバグ
- 運用に関わる問題

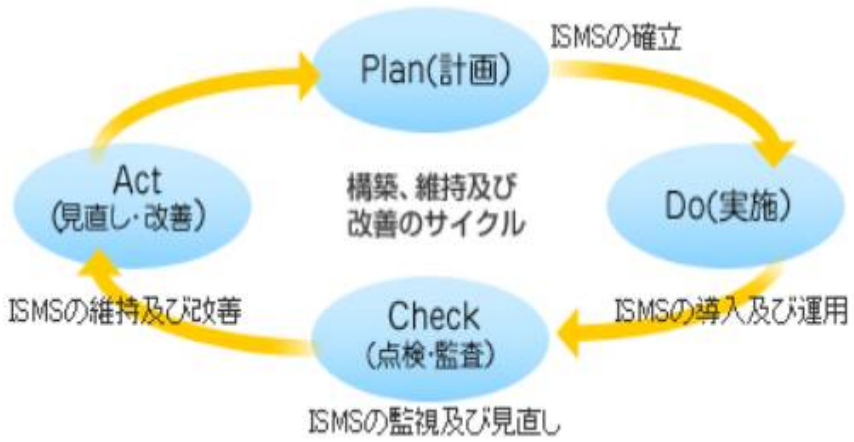
③災害等による**環境的脅威**
地震・雷・火事・水害・停電等によるシステム停止

2. 情報セキュリティの基礎

4)ISMSとPDCA

Plan

図表2.4.情報セキュリティ対策のPDCA



出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

◆情報セキュリティを体系的かつ系統立ててマネジメンする仕組みを情報セキュリティマネジメントシステム（ISMS: Information Security Management System)という。

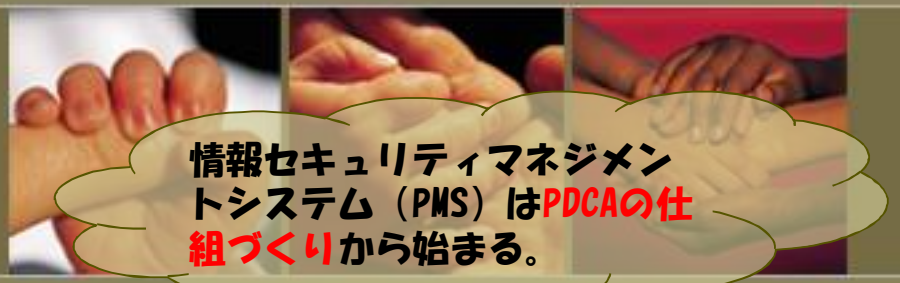
◆ISMSとは、情報セキュリティを確保、維持するための、人的、物理的、技術的、組織的な対策を含む、経営者を頂点とした組織的な取組みの仕組みである。

◆情報セキュリティマネジメントを効率よく行うための手法が、PDCA（Plan－Do－Check－Act の略）であり、品質改善や環境マネジメントでよく知られた手法で、次のステップを繰り返す。

- **Plan**：問題を整理し、目標を立て、その目標を達成するための計画を立てる。
- **Do**：目標と計画をもとに、実際の業務を行う。
- **Check**：実施した業務が計画通り行われて、当初の目標を達成しているかを確認し、評価する。
- **Act**：評価結果をもとに、業務の改善と計画の見直しを行う。

2. 情報セキュリティの基礎

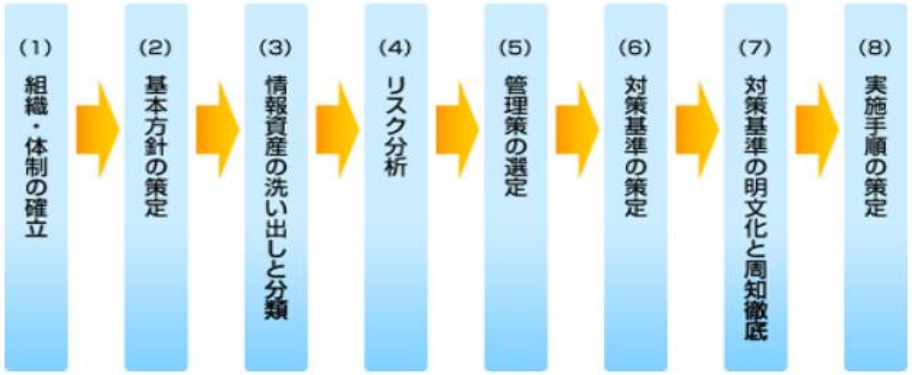
5)情報セキュリティポリシー①



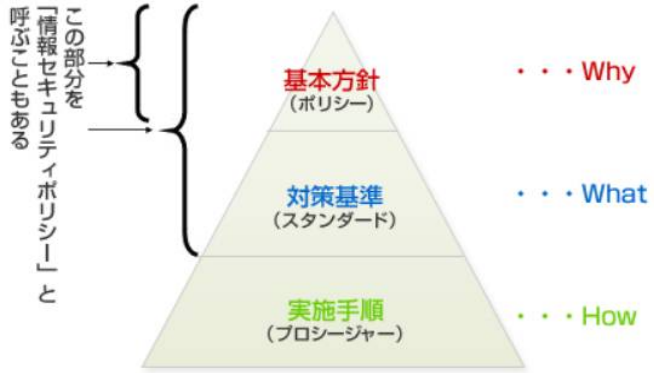
情報セキュリティマネジメントシステム（PMS）はPDCAの仕組づくりから始まる。

Plan

図表2. 5. 情報セキュリティマネジメントシステムの構築



図表2. 6. 情報セキュリティポリシーの構成



出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

◆PDCAサイクルの、P：Plan(計画)は、情報セキュリティマネジメントを確立するための計画段階にあたり、全社的な取組み方針として情報セキュリティポリシーを策定する。

◆情報セキュリティポリシーの文書構成は、特に決まりはないが、「情報セキュリティ基本方針」「情報セキュリティ対策基準」「情報セキュリティ実施手順」の3 階層の文書構成が一般的である。

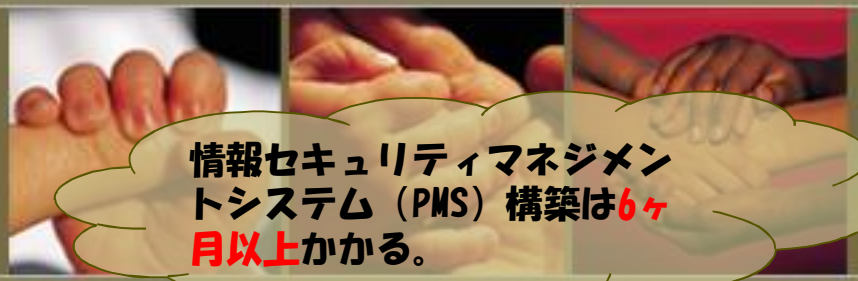
・**基本方針**：経営者が、「情報セキュリティに本格的に取り組む」という姿勢を示し、情報セキュリティの目標と、その目標を達成するために企業がとるべき行動を社内外に宣言する。

・**対策基準**：基本方針の目標を受けて、情報セキュリティ対策を行うために「What」を行うかを記述したルール集で、実際に守るべき規程をいう。

・**実施手順**：対策基準で定めた規程を実施する際に、「どのように実施するか」の「How」を記述したマニュアル的な位置づけの文書であり、詳細な手順をいう。

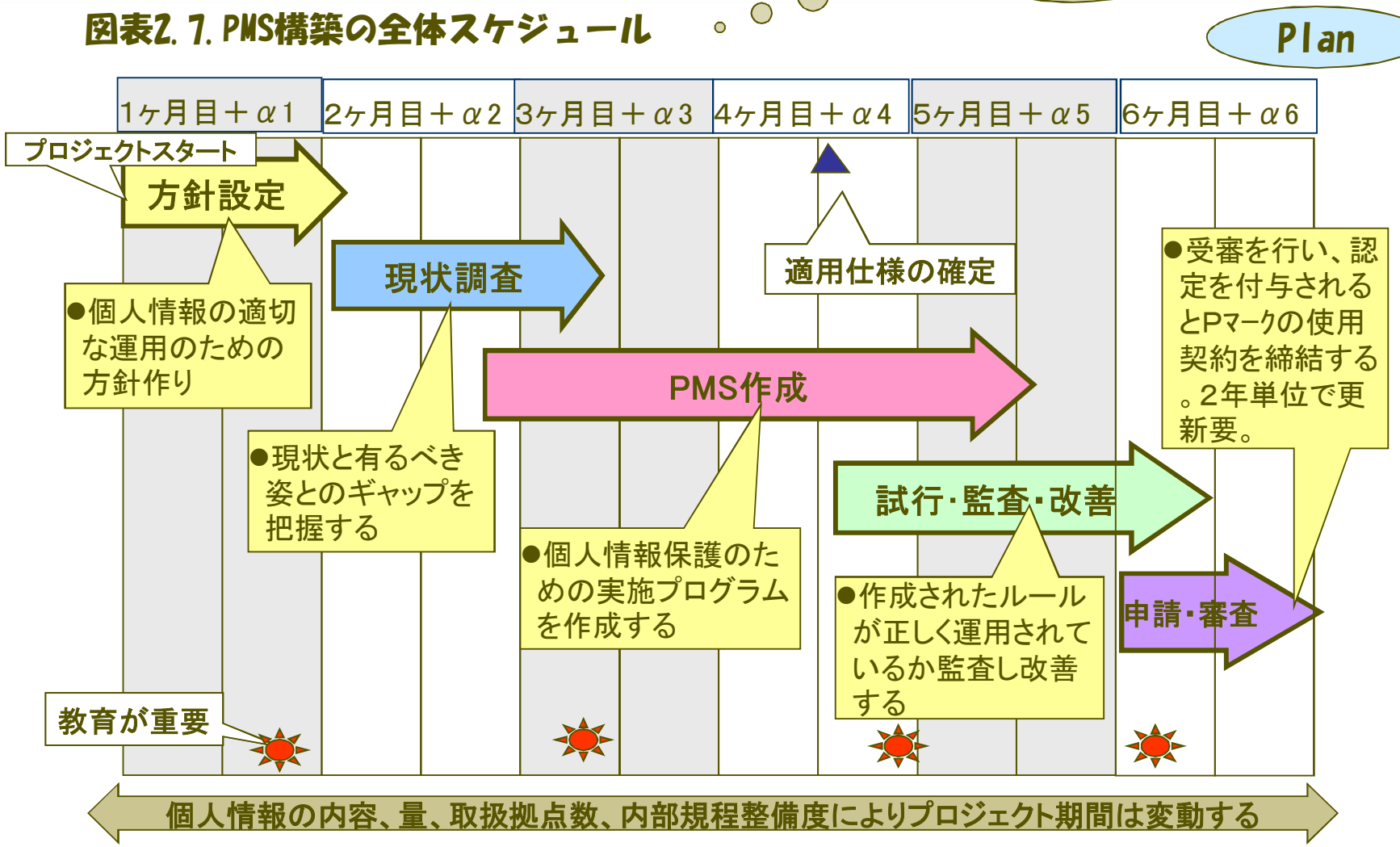
2. 情報セキュリティの基礎

5)情報セキュリティポリシー②



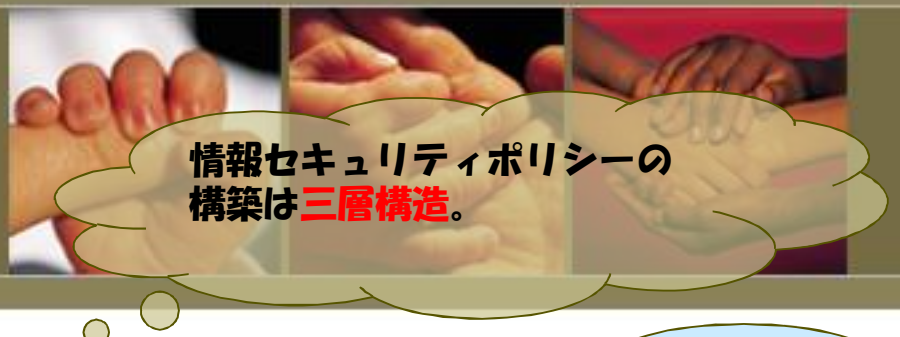
情報セキュリティマネジメントシステム（PMS）構築は6ヶ月以上かかる。

図表2.7. PMS構築の全体スケジュール



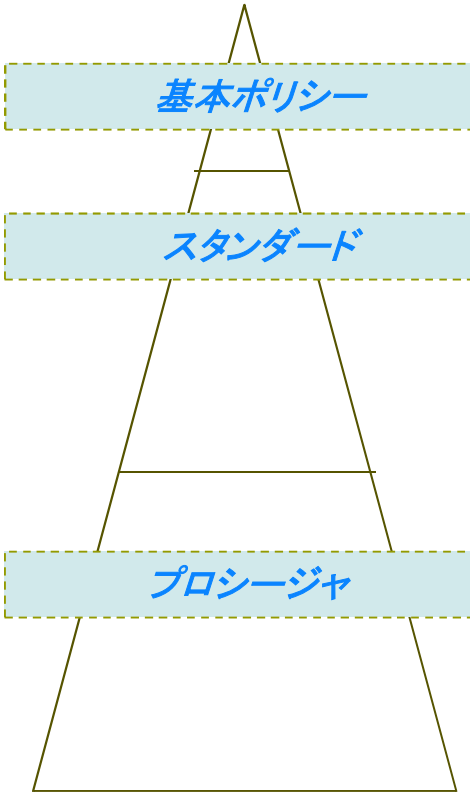
2. 情報セキュリティの基礎

5)情報セキュリティポリシー③



図表2. 8. 情報セキュリティポリシーの概要

Plan



個人情報保護 基本方針

→ プライバシーステートメント
（対外発表用）

個人情報保護 基本規程

整合 →
■既存関連規程
定款、取締役会規程、監査役会規程、文書管理規程
労働協約、就業規則、
職務権限規程、業務分掌規程、稟議規程、組織規程、経理規程、内部監査規程
各種業務規程
・・

目的、適用範囲、適用規格、
コンプライアンスプログラム
収集・利用規・提供、預託、
安全対策、維持、教育、文書、
監査、苦情・相談対応、罰則規程

個人情報保護 細則

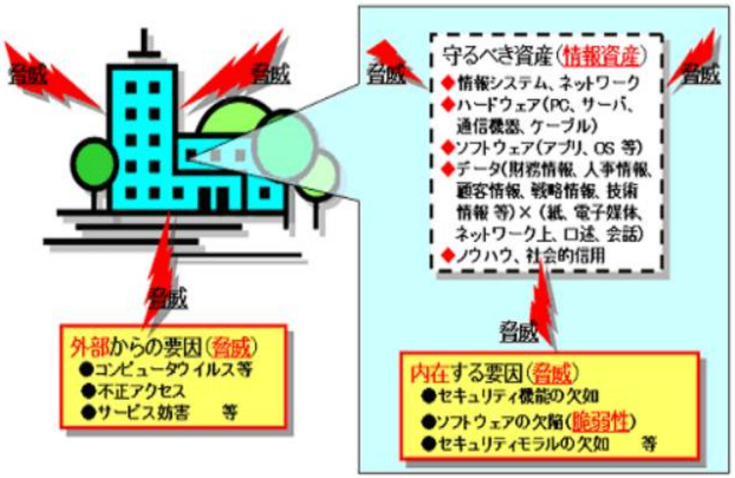
整合 →
■既存運用規程・マニュアル
各種業務マニュアル
IT資産台帳
サーバ管理規程
ウィルス対策規程
ネットワーク管理規程
バックアップ規程
・・

【共通】 共通個人情報取扱規程
個人情報　監査実施管理規程
同　教育実施管理規程
安全管理規程 、入退出管理規程
委託先管理規程
【部門別】 人事部門個人情報取扱規程
システム部門個人情報取扱規程
・・

2. 情報セキュリティの基礎
6)リスクアセスメント①

図表2.9. リスクアセスメントとは

- リスクアセスメント
  - リスク分析
    - リスク因子を特定する
    - リスクを算定する
  - リスク評価



出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

◆「リスクマネジメント－用語－規格において使用するための指針（JIS TR Q 0008:2003）」の定義によれば、リスクアセスメントとは、**リスク分析**から**リスク評価**までの全てのプロセスであり、**リスク因子**とは脅威と脆弱性を指す。

・**脅威**：システム又は組織に危害を与える**事故の潜在的原因**

・**脆弱性**：脅威によって影響を受ける**内在する弱さ**

・**リスク**：ある脅威が脆弱性を利用して**損害を与える可能性**

◆リスク分析の方法は以下の四つの方法がある。

・**ベースラインアプローチ**：既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。

・**非形式的アプローチ**：コンサルタント又は組織や担当者の経験、判断によりリスク評価する方法。

・**詳細リスク分析**：詳細なリスクアセスメントを実施し、情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスク評価する方法。

・**組合せアプローチ**：複数のアプローチの併用する方法。よく用いられるのは、(1)ベースラインアプローチと(3)詳細リスク分析の組合せて、ベースラインアプローチと詳細リスク分析の両方のメリットを享受する方法。

2. 情報セキュリティの基礎

6)リスクアセスメント②

リスクアセスメントのための
リスク分析表は以下のサンプル参照。

Plan

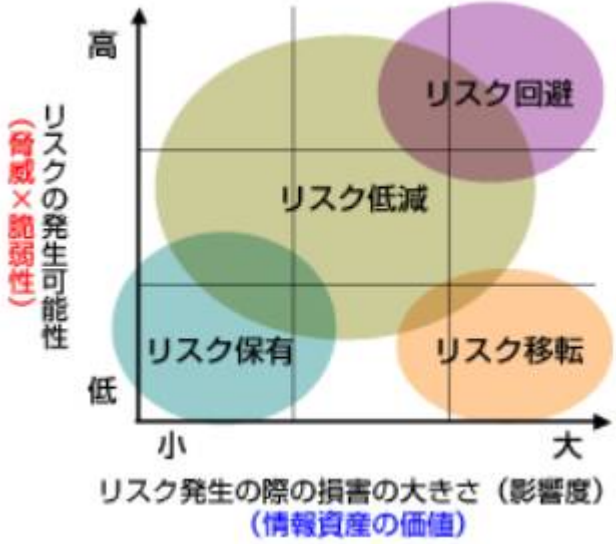
図表2. 10. リスク分析表サンプル

			リスク分析表					
	業務名:	[営業部]AIスタッフ派遣込み				作成日 2008年 5月27日	作成者:	
	個人情報:	登録スタッフエントリーデータなど[電子データ]				改定日 年 月 日	確認者:	
						最終改定日 年 月 日	改定者:	
番号	業務の流れ	リスク	対処すべきリスク	作成すべき規定マニュアル	対策としての記録(確認物)	残存リスク	対策状況	
		具体的なリスク（損害の発生する可能性）を、技術的、物理的、人的管理的側面から記載	対処方法は、技術的、物理的、人的管理的側面から記載			対策後も存在しているリスクを認識する	対策の進捗状況を記載	
1	取得・入力	①悪意のある攻撃によるデータの漏洩、滅失又は毀損。	①ＳＳＬ暗号化を導入する。 ②サーバーへセキュリティソフトを導入する。	①個人情報安全管理規程		①ハッキング。	①Fire Wall	
		②担当者の自宅PCなどでエントリーデータ送信先のアカウントを設定しメール受信することによる個人情報の漏洩。	①社員の自宅でのメール受信の禁止。 ②メール受信から10日後サーバーから削除する設定にする。	②個人情報安全管理規程				
		③						
2	移送・送信	①担当者間の情報共有のため、メール転送する際の外部への誤送信。	①アドレス登録しそれ以外に送信しない。 ②社員教育。	①個人情報安全管理規程		①操作ミスによる誤送信。	①定期的な社員教育・監査	
		②						
		③						
		④						
3	利用・加工	①エントリー者へのメール送信などの際に誤って他のエントリー者の情報を記載する。	①社員による二重チェック。 ②社員教育。	①個人情報安全管理規程		①操作ミスによる誤送信。	①定期的な社員教育・監査	
		②個人情報を表示させたまま離席し、担当者以外の者に見られる。	①スクリーンセーバーを10分に設定する。	①個人情報安全管理規程		①故意に設定変更する。	①定期的な社員教育・監査	
4	保管・廃棄	①PtoPソフトなどファイル交換ソフトによりメールデータが外部へ漏洩する。	①PtoPソフトなどファイル交換ソフトのインストールを全面禁止する。	①個人情報安全管理規程		①故意にファイル交換ソフトをインストールする。	①定期的な社員教育・監査	
		②メールを受信した担当者PCへの悪意のある攻撃によるデータの漏洩、滅失又は毀損。	①担当者PCへセキュリティソフトを導入する。	①個人情報安全管理規程		①セキュリティソフト定義の更新遅れ。	①セキュリティソフトの自動更新？	
		③						
5	委託・提供	①ウェブサーバーへの悪意ある攻撃によるデータの漏洩、滅失又は毀損。	①VPN等のセキュリティを導入する。 ②SSL暗号化を導入する。	①個人情報安全管理規程		①セキュリティホールへの攻撃。	①定期的な社員教育・監査	
		②						
		③						

2. 情報セキュリティの基礎

7)リスク対応

図表2. 11. リスクへの対応概念



出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

◆リスク対応では、リスク評価の作業で明確になったリスクに対して、どのような対処を、いつまでに行うかを明確にする。
◆リスク対応の方法には、大きく分けて「リスク低減」「リスク保有」「リスク回避」「リスク移転」の4つがある。
・リスク**低減**：脆弱性に対して情報セキュリティ対策を講じることにより、脅威発生の可能性を下げること⇒ノートPCの紛失、盗難、情報漏えいなどに備えて保存する情報を暗号化しておく、サーバ室に不正侵入できないようにバイオメトリック認証技術を利用した入退室管理を行う、従業員に対する情報セキュリティ教育を実施するなど。
・リスク**保有**：リスクのもつ影響力が小さいため、特にリスクを低減するためのセキュリティ対策を行わず、許容範囲内として受容する。
・リスク**回避**：脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ること⇒インターネットからの不正侵入の脅威に対し、外部との接続を断ち、Web上での公開を停止する場合など。
・リスク**移転**：リスクを他社などに移すこと⇒リスクが顕在化したときに備えリスク保険などで損失を充当したり、社内の情報システムの運用を他社に委託し、契約などにより不正侵入やウイルス感染の被害に対して損害賠償などの形で移転するなど。

2. 情報セキュリティの基礎

8)リスク管理策の参照

リスク管理策は、ISO17799に11管理領域と133管理策が例示されている。

Plan

図表2. 12. リスク管理策の概念

◆対策基準を一から自社で作り上げるのは大変であり、世の中にある管理策集や対策基準を参照し、それをもとに自社の実情にあわせてカスタマイズする方法が一般的。

◆よく参照される管理策集は、2000年に国際標準となったISO/IEC17799である。ISO/IEC17799 は2005年に改訂、JIS化されて、「情報技術－情報セキュリティマネジメントの実践のための規範（JIS Q 27002:2006）」(2006年5月発行)となった。ISO/IEC17799:2000には、10の管理領域と127の管理策があり、2005年に改訂されたISO/IEC17799:2005には、11の管理領域と133の管理策がある。

出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

2. 情報セキュリティの基礎

9)管理策の構築

リスク管理策は、ISO27001では133管理策が1000近くに詳細化されている。

Plan

図表2. 13. JISQ27002の管理策

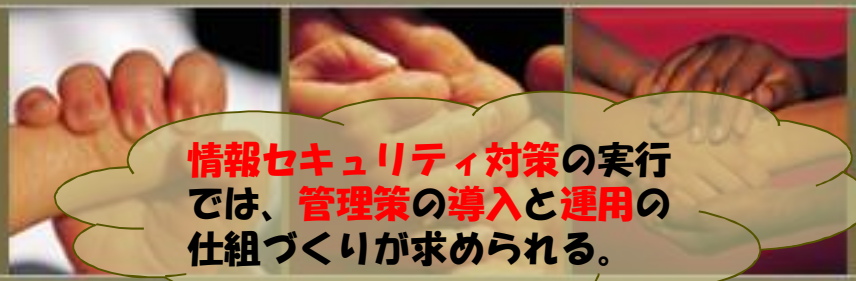
ISO/IEC 17799:2005 → JIS Q 27002		11の管理領域と133の管理策 管理策、実施の手引き、関連情報
Security policy セキュリティ基本方針	(2)	14.1 Information security aspects of business continuity management (事業継続管理における情報セキュリティの側面)
Organizing information security 情報セキュリティのための組織	(11)	14.1.1 Including information security in the business continuity management process (事業継続管理手続きへの情報セキュリティの組込み)
Asset management 資産の管理	(5)	14.1.2 Business continuity and risk assessment (事業継続及びリスクアセスメント)
Human resources security 人的資源のセキュリティ	(9)	14.1.3 Developing and implementing continuity plans including information security (情報セキュリティを組み込んだ事業継続計画の策定及び実装)
Physical & environmental security 物理的及び環境的セキュリティ	(13)	14.1.4 Business continuity planning framework (事業継続計画策定の枠組み)
Communications & operations management 通信及び運用管理	(32)	14.1.4 Testing, maintaining and re-assessing business continuity plans (事業継続計画の試験、維持及び再評価)
Access control アクセス制御	(25)	※日本語訳は暫定的な仮訳
Information systems acquisition, development and maintenance システムの取得、開発及び保守	(16)	
Information security incident management 情報セキュリティインシデントの管理	(5)	
Business continuity management 事業継続管理	(5)	
Compliance 順守	(10)	

◆管理策はcontrol(コントロール)の訳語ですので、管理策を「コントロール」と呼ぶこともある。
◆JISQ27002の133のコントロールは、さらに1000近くのサブコントロールに詳細化されている。
- セキュリティ基本方針:2管理策
- 情報セキュリティのための組織:11管理策
- 資産の管理:5管理策
- 人的資源のセキュリティ:9管理策
- 物理的及び環境的セキュリティ:13管理策
- 通信及び運用管理:32管理策
- アクセス制御:25管理策
- システムの取得、開発及び保守:16管理策
- 情報セキュリティインシデントの管理:5管理策
- 事業継続管理:5管理策
- 順守:10管理策

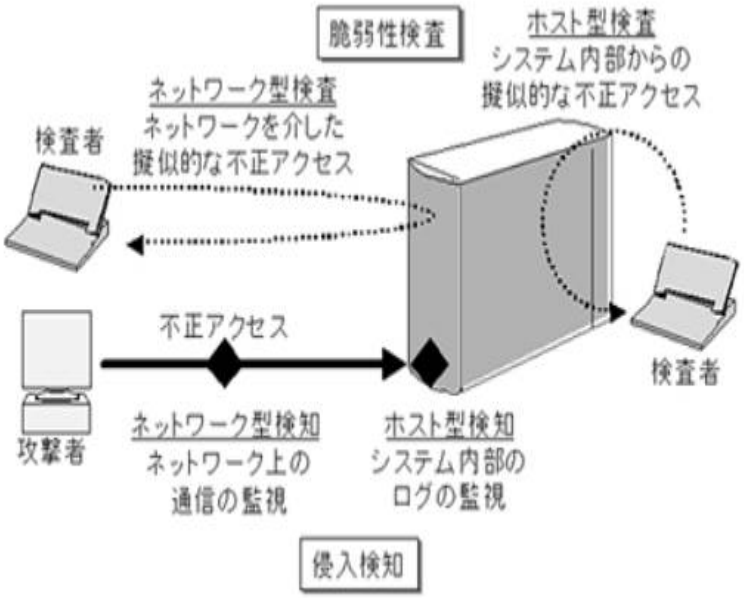
出典:独立行政法人情報処理推進機構(IPA)ホームページ「情報セキュリティマネジメントとPDCAサイクル(http://www.ipa.go.jp/security/manager/protect/pdca/index.html)」より引用

2. 情報セキュリティの基礎

10）管理策の導入と運用



図表2. 14. 情報セキュリティ監視



出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

Do

◆情報セキュリティ管理策の実行では、まず、セキュリティ対策の根本となる、システム等への情報セキュリティ対策の構築、設定を行い（導入フェーズ）、そののち、実際の運用に入る（運用フェーズ）。

・**導入フェーズ**：実際の運用に入る前に、情報セキュリティ対策の根本となる設定を行う⇒ウイルス対策ソフトやファイアウォールなどのセキュリティ装置の導入＋サーバのソフトウェアのセキュリティ脆弱性を解消するため、最新の修正プログラムの適用＋メンバーごとにアクセス権を設定し、アクセスできる情報の範囲や操作権限などを詳細に制御する。

・**運用フェーズ**：セキュリティ教育でセキュリティポリシーを周知徹底すること。その際、各人にどのような役割と責任があるかを明確にすると共に、セキュリティ対策ルールとして何が許され、何が禁止されているかを周知する⇒設定の際に最新のパッチを適用した後も、定期的にメーカやIPAのWebサイトを参照し最新パッチの適用＋セキュリティ監視として脆弱性検査や不正アクセス検知のための侵入検知＋異動した社員や退職した社員のアカウント削除やアクセスを制限する。

2. 情報セキュリティの基礎

11）情報セキュリティの評価

図表2. 15. 情報セキュリティ評価

第三者評価： 被評価者と独立の立場の専門家による客観的評価
手間、時間、費用がかかる
実施時期を決めて、計画的に行う

第一者評価：（自己評価） 情報システム部門の責任者や担当者が、導入した個々の管理策の効果や効率を自己評価する
第三者評価に比べ、手間、時間、費用が少なくて済む

第三者評価	情報セキュリティ監査 ISMS適合性評価制度 ITセキュリティ評価・認証制度 など
第一者評価 （自己評価） （セルフアセスメント）	情報セキュリティ対策ベンチマーク （IPAの情報セキュリティ対策の自己診断ツール） チェックリストによる点検 など

出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティマネジメントとPDCAサイクル（http://www.ipa.go.jp/security/manager/protect/pdca/index.html）」より引用

Check

◆情報セキュリティ対策の評価には、「自己点検」「情報セキュリティ対策ベンチマーク」、「情報セキュリティ監査」などがある。

・**自己評価**（第一者評価）：企業や組織が、自組織の現状における対策の効果や完成度を確認するために自らが行う評価⇒手間、時間、費用が少なくて済み、手軽に行える⇒チェックリストによる点検やIPA「情報セキュリティ対策ベンチマーク」が有効である。

・**第三者評価**：対策の導入や運用に関与していない、独立の立場の専門家による客観的評価⇒時間と手間と費用、事前準備がかかる⇒情報セキュリティ監査、ISMS適合性評価制度、ITセキュリティ評価・認証制度などの実施時期を決め、予算化した上で、半年に1回とか1年に1回など、計画的に行う。

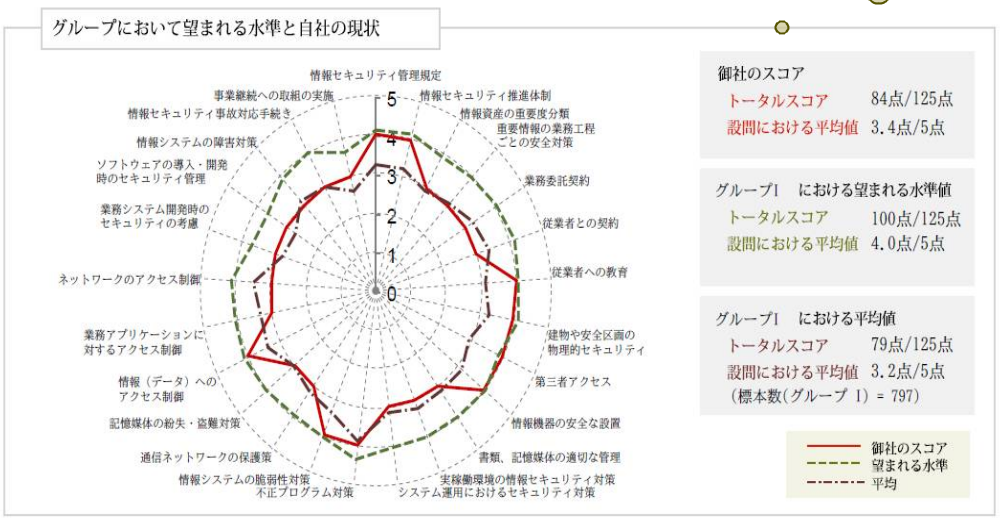
◆セキュリティ評価はPDCAのCに該当し、その種類も多く、目的や対象範囲も様々であり、自組織の現状に即し、どのような評価が必要なのかを考慮し、目的、対象、時期、評価責任者などを明確にして、全体を見通した評価計画を立てることが重要である。

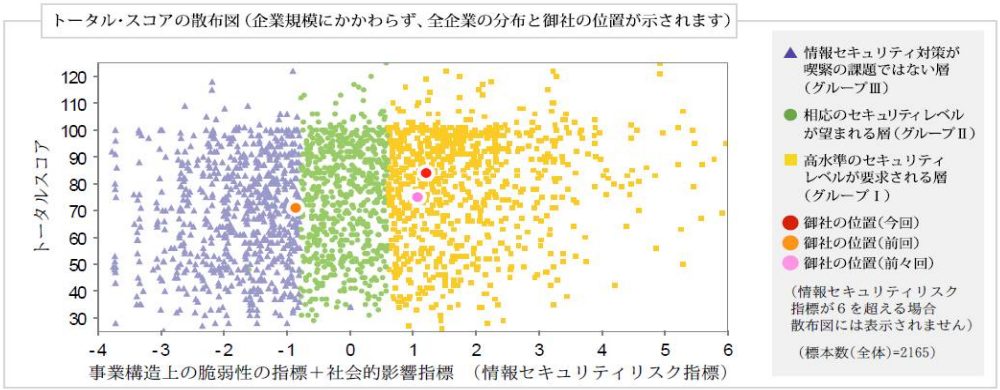
2. 情報セキュリティの基礎

12)情報セキュリティ対策ベンチマーク

情報セキュリティ対策の評価では、IPAの情報セキュリティ対策ベンチマークが有効。

図表2.16.情報セキュリティ対策診断サンプル





出典：独立行政法人情報処理推進機構（IPA）ホームページ「情報セキュリティ対策診断（http://www.ipa.go.jp/files/000011539.pdf）」より引用

Check

◆「情報セキュリティ対策ベンチマーク」は、Webページ上の質問に答えることで、何千件もの実データに基づき、望まれる水準や他社の対策状況と自社の対策状況を比較することができる公的機関が運用する無料ツールである。

◆情報セキュリティリスク指標は、従業員数、売上高、重要情報の保有数、IT 依存度などから計算される企業のかかえるリスクを表す指標である。

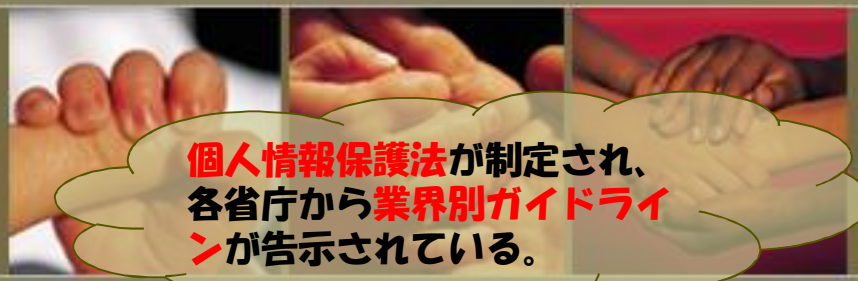
◆情報セキュリティ対策診断は、情報セキュリティ対策への取組みに関する 25 問（評価項目）の回答から対策状況のスコアが計算される。この評価項目は、ISMS 認証基準である JIS Q 27001:2006 付属書 A の管理策（133 項目）をベースに作成されている。

◆医療・介護分野のサンプル数は、教育・学習支援業を含め50件/1436件である。

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

1）個人情報保護法の要点①



個人情報保護法が制定され、
各省庁から**業界別ガイドライン**が告示されている。

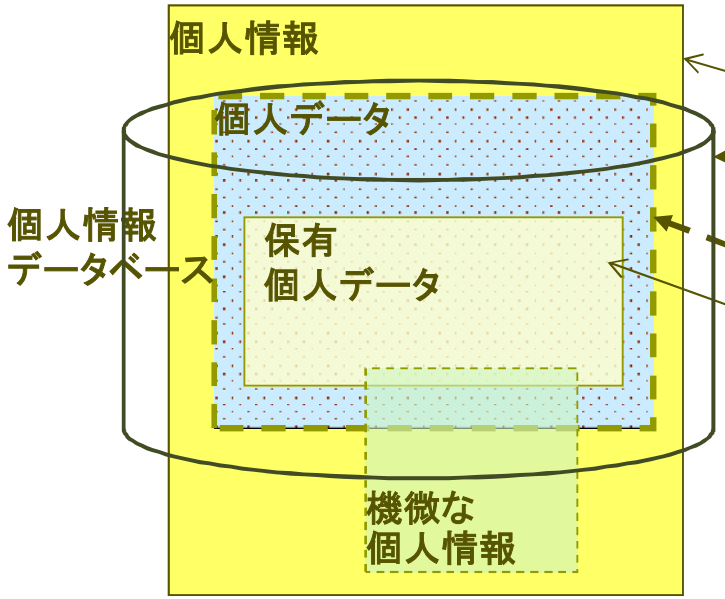
背景：高度情報通信社会の進展に伴い個人情報の利用が著しく拡大
目的：個人情報の有用性に配慮しつつ、個人の権利利益を保護すること

図表3. 1. 個人情報保護法の概要

（平成17年4月1日施行）

個人情報保護法

- 民間部門向け
  - 基本理念 → **宣言・規則**を作成・公表し、必要な措置を行なう
  - 罰則つき義務規程 → **罰則**：命令違反は**懲役6ヶ月**以下又は**罰金30万円以下**
    義務規程の適用除外：ﾒﾃﾞｨｱ、著作、学術、宗教など
- 行政機関向け
  - 公務員の罰則規程 → 正当な理由無く個人情報提供すること
    不正な利益目的で個人情報提供すること
    職務目的以外で個人情報を収集すること



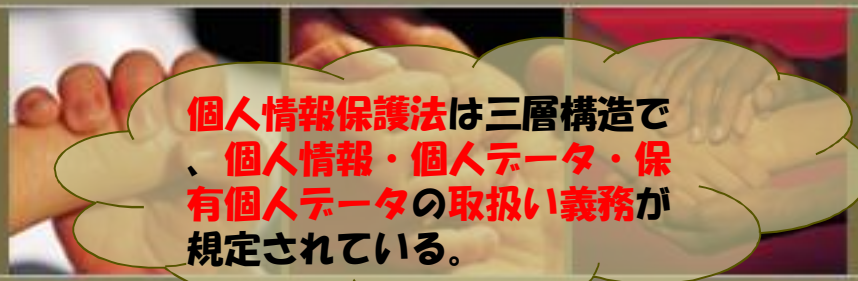
「個人情報」…生存する個人に関する情報（識別可能情報）
「個人情報データベース等」…個人情報を含む情報の集合物（検索が可能なもの。一定のマニュアル処理情報を含む）

「個人データ」…個人情報データベース等を構成する個人情報
「保有個人データ」…個人情報取扱事業者が開示、訂正等の権限を有する個人データ

「個人情報取扱事業者」…個人情報データベース等を事業の用に供している者（国、地方公共団体等のほか、取り扱う個人情報が少ない等の一定の者を除く）

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

1）個人情報保護法の要点②



個人情報保護法は三層構造で、個人情報・個人データ・保有個人データの取扱い義務が規定されている。

図表3. 2. 個人情報保護法の構造

・個人情報の適切な取り扱い(第3条)

3層構造

個人情報取扱事業者

個人情報に関する義務

個人データに関する義務

保有個人データに関する義務

・保有個人ﾃﾞｰﾀについての公表(第24条)

・開示要求対応(25)

・訂正・追加・削除要求対応(第26条)

・利用停止要求対応(第27条)

・措置の理由説明(第28条)

・開示手続明確化(29)

・手数料の合理的設定(30)

・ﾃﾞｰﾀ内容の正確性確保(第19条)

・適切な安全管理措置(第20条)

・安全管理のための従業者の監督(21)

・安全管理のための委託先の監督(第22条)

・第三者提供制限・・本人同意が必要(第23条)

・利用目的の特定と明確化(第15条)

・利用目的の制限と本人同意(第16条)

・適正な手段による取得(第17条)

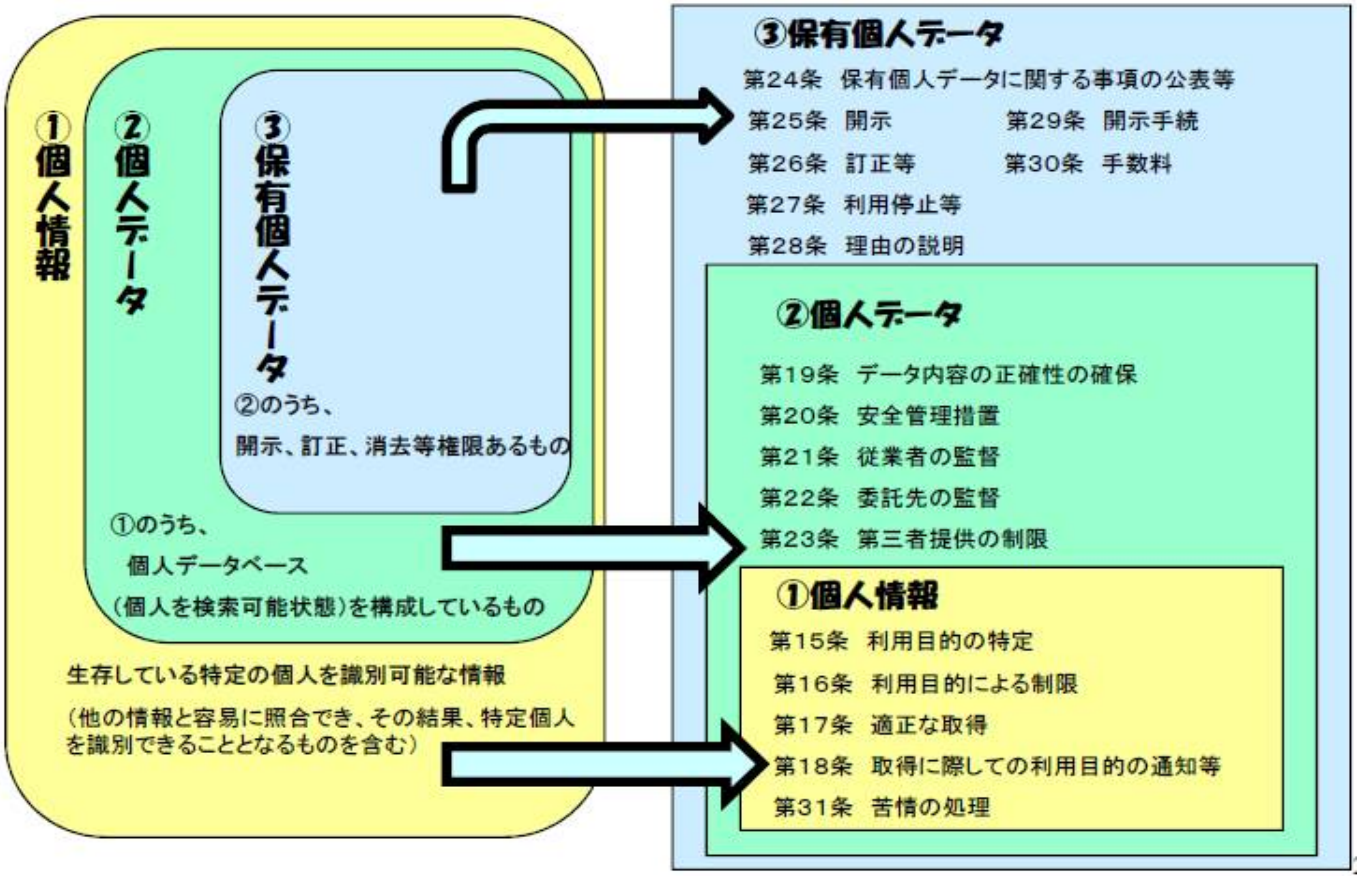
・収集時の利用目的通知・公表・明示(18)

・苦情処理対応(第31条)

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

2）個人情報保護法の義務規定

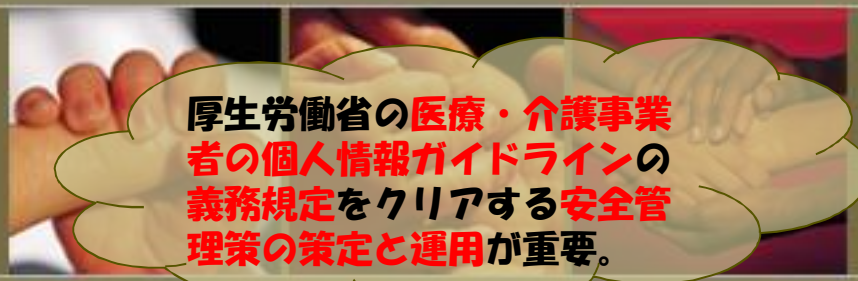
図表3. 3. 個人情報・個人データ・保有個人データに関する義務規定



出典：経済産業省商務情報政策局情報経済課「経済産業分野を対象とする個人情報保護ガイドライン等について」（平成22年3月）

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

3)医療・介護個人情報保護ガイドラインの要点



図表3. 4. 厚生労働省医療・介護事業者の個人情報保護ガイドラインの要点

	収集	保管	利用	預託	第三者提供	保有	廃棄
要求事項	●個人情報の適正な手段による取得 (第17条) ・利用目的変更時の通知・公表(18)	●個人データ内容の正確性確保(第19条) ・必要かつ適切な安全管理措置(20)	●個人情報の利用目的の特定・明確化(第15条) ・利用目的変更(15) ・利用目的の制限と本人同意(16) ・合併等事業承継による個人情報の利用制限(16) ・利用目的の制限除外要件(16) ●個人データの安全管理のための従業者の監督(21) ・個人情報取扱状況報告対応(32) ・主務大臣助言(33) ・勧告・命令(34)	●個人データの安全管理のための委託先の監督(第22条)	●個人データの第三者提供制限・・本人同意が必要(第23条) ・変更内容の事前の本人通知・知りうる状態(23) ★第三者に該当しない場合 ・処理の委託 ・予め通知した共同利用	●保有個人データについての公表(第24条) ・開示要求対応(25) ・訂正・追加・削除要求対応(26) ・利用停止要求対応(27) ・措置の理由説明(28) ・開示手続(29) ・開示手数料(30) ・苦情処理対応(31)	
発生リスク	・患者・職員情報等の不正手段による取得	・盗難 ・紛失 ・不正ｱｸｾｽ ・破壊・改竄	・意図的漏洩 ・PC等操作ミス ・悪意の無い社外持出による紛失	・患者検査情報等ﾃﾞｰﾀ授受 ・委託先からの漏洩	・患者情報の共同利用先からの漏洩	・患者情報等患者本人のなりすましによる不正アクセス	・媒体持出による漏洩 ・廃棄ミスによる流出
安全管理対策	・個人情報取扱規程 ・従業者教育と教育記録	・個人情報管理規程 ・リスク対応保管対策 ・ｾｷｭﾘﾃｨｴﾘｱ ・鍵付戸棚 ・鍵の管理 ・実施記録	・個人情報利用規程 ・従業者誓約書 ・入退出管理 ・利用者限定 ・利用PC限定 ・ｱｸｾｽ権制御 ・アクセスログ ・本人認証システム	・委託契約書締結 ・委託先監査実施 ・ﾃﾞｰﾀ授受記録	・患者情報など個人情報共同利用規程	・保有個人データ開示規程 ・保有個人データ訂正及び利用停止規程 ・保有個人データ苦情処理規程	・個人情報廃棄規程 ・ｼｭﾚｯﾀﾞｰによる廃棄 ・媒体の電子的消去

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

4）個人情報保護方針

◆「個人情報保護方針」サンプル

個人情報保護方針

当法人は、個人情報を取り扱う事業者としての法的責任及び社会的責任を認識し、以下の方針に基づき当事業所の全従業員が一体となって、利用者様の個人情報の適切な保護を実施します。

1. 個人情報の収集について

当事業所は、個人情報の利用目的をあらかじめ明確に定め、適法かつ公正な手段により、必要な範囲で個人情報を取得します。

2. 個人情報の利用・提供について

当事業所は個人情報を、あらかじめ定めた利用目的の範囲内で、業務の遂行上、必要な限りにおいて利用します。

また、当事業所は、法令で定められている場合や当事業所関連施設で共同利用する場合を除き、利用者様の同意を得ることなく、個人情報の第三者提供を致しません。

3. 個人情報の外部委託について

当事業所は個人情報の取扱いを社外に委託する場合には、適正な委託業者を選定し、個人データの漏えい、滅失又はき損を防止するために適切な監督を行います。

4. 個人情報の安全管理について

当事業者は個人データの正確性を保ち、個人データに関する不正アクセス・紛失・破壊・改ざん・漏洩等を防止するため、適正な安全管理策を講じます。

5. 個人情報保護に関する法令・規範の遵守にについて

当事業所は個人情報の取扱いにおいて、個人情報の保護に適用される法令および経済産業省のガイドライン及び日本工業規格「個人情報保護に関するマネジメントシステムの要求事項（JISQ15001）」を遵守します。

6. 個人情報保護マネジメントシステム（JISQ15001準拠）の継続的改善について

当事業所は個人情報保護マネジメントシステムを定め、これを全従業員その他関係者に周知徹底のうえ実施し、定期的にその見直しを行い継続的改善を行ないます。

2014年〇月〇日
医療法人〇〇〇〇
理事長　△□△□

3. 個人情報保護法及び医療・介護個人情報保護ガイドラインの要点

5）個人情報保護法に基づく公表事項

◆「個人情報保護法に基づく公表事項」サンプル

1. 個人情報の利用目的に関する事項
- ○個人情報取扱事業者別個人情報の利用目的

2. 保有個人データに関する事項
- ○個人情報取扱事業者別保有個人データと利用目的

3. 個人情報の第三者提供について
- ○第三者提供の例外事項

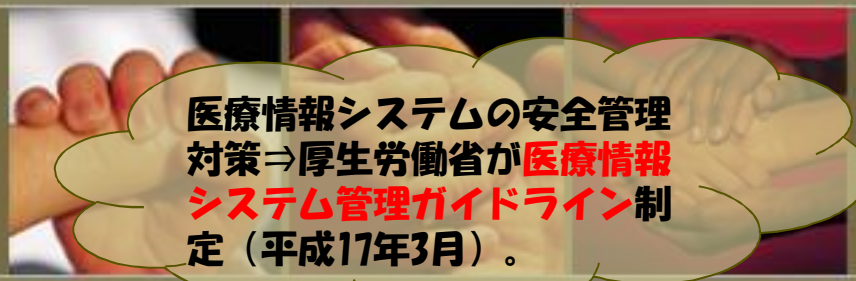
4. 保有個人データの開示請求等に応じる手続きに関する事項
- ○開示・追加・削除・利用停止等の請求の対象となる項目
- ○開示・追加・削除・利用停止等の請求先
- ○開示・追加・削除・利用停止等の請求の際の提出申請書及び様式
- ○代理人による開示・追加・削除・利用停止等の請求（申請書、委任状、同意書）
- ○開示・追加・削除・利用停止等の請求に関する手数料及び徴収方法
- ○開示・追加・削除・利用停止等の請求に関する回答方法
- ○開示・追加・削除・利用停止等の請求に関して取得した個人情報の利用目的

5. 保存期間を経過した個人情報の廃棄方法に関する事項
- ○個人情報の保存期間
- ○管轄部署への廃棄書類の回収
- ○個人情報の匿名化及び消去作業
- ○委託・回収業者による焼却

6. 苦情処理の受付窓口に関する事項
- ○電話＆FAX
- ○文書
- ○電子メール

4. 医療情報システム安全管理ガイドラインの要点

4. 医療情報システム安全管理ガイドラインの要点

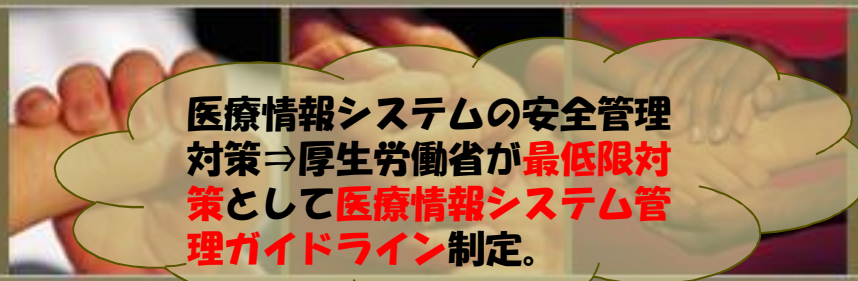


医療情報システムの安全管理対策⇒厚生労働省が医療情報システム管理ガイドライン制定（平成17年3月）。

図表4. 1. 医療情報システム安全管理ガイドラインの作成・改訂経緯

版数	日付	主な内容
第1版	平成17 年3 月	・法令保存義務の診療録及び診療諸記録の電子媒体による保存ガイドライン（紙等の媒体による外部保存を含む）及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインの作成
第2版	平成19 年3 月	・ネットワークにより「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」として取りまとめる等の改定 ・医療における災害、サイバー攻撃対策に対する指針として「6.9 災害等の非常時の対応」を新設等の改定
第3版	平成20 年3 月	・医療・健康情報を取り扱う際の「4 電子的な医療情報を扱う際の責任のあり方」を取りまとめる等の改定 ・特にモバイルで用いるネットワークの「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」要件追加等の改定
第4版	平成21 年3 月	・「医療分野における電子化された情報管理の在り方に関する事項」について全面的な改定
第4．1版	平成22 年2 月	・4 章で「4.3 例示による責任分界点の考え方の整理」に「(4)オンライン外部保存を委託する場合」を追加等の改定 ・8 章で「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」等の改定
第4．2版	平成25年10月	・平成25 年3 月調剤済み処方箋および調剤録等の外部保存改正対応 ・大規模災害時を想定した考え方について追記 ・医療情報の相互運用性と標準化について最新の技術等への対応改正

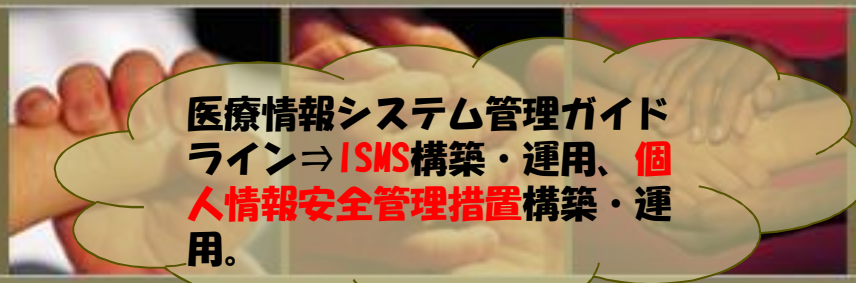
4. 医療情報システム安全管理ガイドラインの要点



図表4. 2. 医療情報システム安全管理ガイドライン（Ver. 4. 2：2013. 10改訂）の要点（その１）

	安全管理措置	ISMSの実践	組織的対策	物理的対策	技術的対策	人的対策
法的要求事項	・個人情報取扱い事業者の個人データの安全管理措置を講じる（第20条） ・委託先の管理（第22条）	・個人情報取扱い事業者の個人データの安全管理措置を講じる（第20条）				・従業員の監督（第21条）
考え方	・個人情報保護方針の策定・公表：6項目（JISQ15001：2006） ①取得・利用・提供 ②法令・指針等遵守 ③漏洩等の予防是正 ④苦情・相談対応 ⑤PMS継続改善 ⑥代表者氏名	・ISO（ISO/IEC 27001:2005）・JIS（JIS Q 17001:2006）マネジメントシステムの導入は有効 ①ミス等発見・報告 ②原因分析 ③予防・是正策	・安全管理のPDCA ①組織体制の整備 ②規程の整備と運用 ③情報資産台帳 ④評価・見直し・改善 ⑤端末外部持出規則 ⑥リモートアクセス規程 ⑦事故・違反対処	・端末・PC・媒体の物理的管理による保護 ①入退館・室管理 ②盗難・窃盗防止 ③機器・装置・媒体の盗難・紛失防止	・運用管理との併用 ①利用者識別認証 ②区分管理とアクセス権管理 ③アクセスログ ④不正ソフトウエア対策 ⑤不正アクセス	・医療情報システムに関連者の守秘義務と違反時の罰則規定 ・教育訓練
最低限ガイドライン	・個人情報保護方針の策定・公表 ・情報システム安全管理方針の策定	・個人データのリストアップ ・分類し最新状態 ・安全管理者が確認できる状態 ・リスク分析 ・脅威への対策	・情報システム運用責任者 ・来訪者の入退室管理 ・アクセス管理規程 ・委託契約 ・運用管理規程整備	・機器設置場所・媒体保存場所の施錠 ・端末設置区画の部外者立入禁止 ・個人情報管理場所の入退管理 ・PC盗難・窃視防止	・ID/PW認証 ・クリアスクリーン ・動作確認データの漏洩防止 ・アクセス権管理 ・アクセスログ ・アクセス制限 ・ウィルス対策等	・管理者による安全管理施策の実施と監督
推奨ガイドライン		・上記の記録管理		・防犯カメラ、自動侵入監視装置	・クリアスクリーン ・ファイアウオール ・PWアクセス制限等	・サーバ室等のモニタリング管理

4. 医療情報システム安全管理ガイドラインの要点



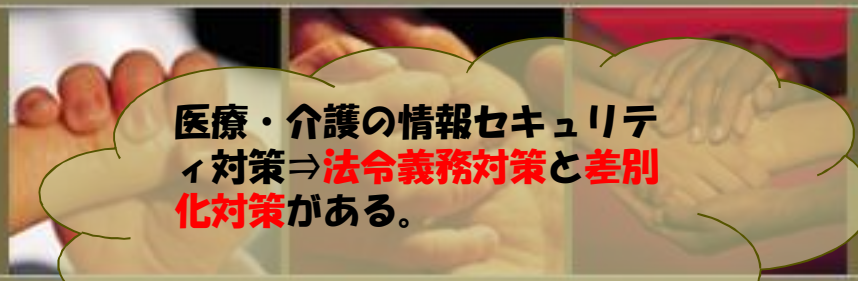
図表4. 2. 医療情報システム安全管理ガイドライン（Ver. 4. 2：2013. 10改訂）の要点（その２）

	委託管理	情報破棄	情報システム保守	情報資産持出	非常時対応	外部情報交換
法的要求事項	・委託先の管理（第22条）	・個人情報取扱い事業者の個人データの安全管理措置を講じる（第20条）				
考え方	・業務の一部を外部事業者に委託する場合は、守秘義務と監督により個人情報保護	・医療電子情報破棄の安全性確保 ・破棄手順の明確化	・可用性を維持するための定期的メンテナンス	●安全管理対策 ・ISMSの実践 ・取得情報の把握 ・リスク分析 ・医療情報管理者によるコンピュータウィルスやWinnyなどソフト管理 ・可搬媒体の盗難・紛失・置忘れ防止 ・人的安全管理対策 ・スマートフォン対策	●BCP作成と訓練 ①事前周知事項 ②BCP実行 ・方針/事象/安全・安否/影響度の確認 ③業務再開 ・人的資源/代替設備/再開・普及の両立/新たなリスク対策 ④用務回復 ⑤全面復旧→BCP改善	・送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守る ・クローズド・オープンネットワーク/モバイル接続等ケース想定による留意点を整理
最低限ガイドライン	●個人情報保護 ①守秘義務契約 ②情報システム保守作業結果の確認 ③清掃等の作業結果の定期点検 ④再委託上の対策 ・外部要員が診療録等アクセスの場合の守秘義務	・情報種別ごとに破棄手順と破棄方法の明確化 ・情報処理機器破棄の証明書 ・外部保存情報破棄の証明書 ・運用管理規程に媒体破棄を規定	・動作確認データの守秘義務と終了後の消去処理確認 ・保守要員個人のアカウント設定と作業記録 ・アカウント情報の管理 ・保守会社のアカウント管理体制の整備 ・保守会社メンテ日次管理 ・保守会社と守秘義務契約 ・保守会社の運用管理規程 ・リモートメンテのログ収集	●運用管理規程 ・リスク分析と情報・情報機器の持出 ・持出た情報・情報機器の管理方法 ・可搬媒体の盗難・紛失時の対応教育 ・情報機器・可搬媒体の台帳管理 ・情報機器の機動PW ・情報の暗号化等 ・不正アクセス防止等	●BCPの一環 ・“非常時”判断の仕組、正常復帰時の手順 ・正常復帰後の代替手段運用した間のデータ整合性を図る規約 ・非常時の情報システムの運用監査 ・サイバー攻撃で医療サービス提供体制に支障が発生する場合は、所管官庁への連絡	・ネットワーク経由のウィルス混入・改ざん防止 ・データ送信元と受信元のKPI認証など ・施設内のなりすまし防止対策 ・ネットワーク機器は安全性確認されたもの ・ファイルの暗号化 ・契約で情報通信会社等責任分界点設定等
推奨ガイドライン			・オペレーション記録ログ ・医療関係者立合い ・作業員と保守会社の守秘等	・PC窃視防止フィルタ ・複数認証の組合せ ・可搬媒体台帳管理等		・職員からの外部アクセスはVPN環境で

5. 医療・介護の情報セキュリティ対策（まとめ）

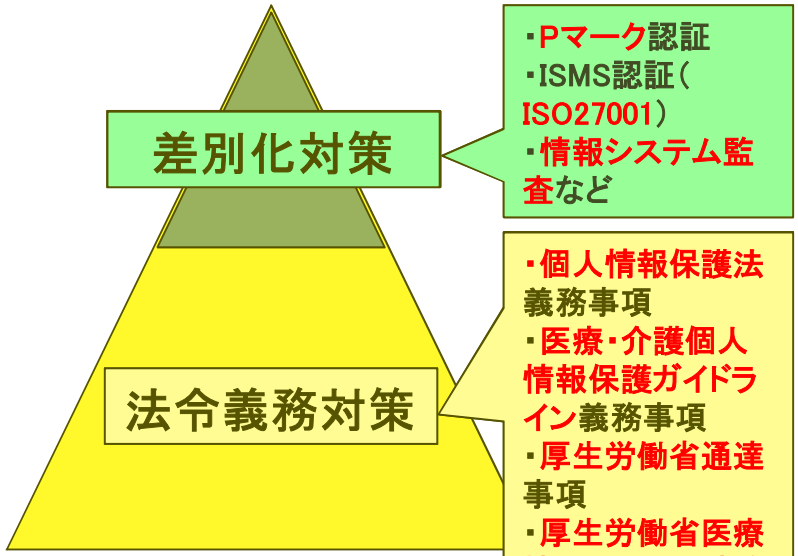
5. 医療・介護の情報セキュリティ対策（その1）

1）情報セキュリティ対策の分類



医療・介護の情報セキュリティ対策⇒法令義務対策と差別化対策がある。

図表5. 1. 医療・介護の情報セキュリティ対策の分類



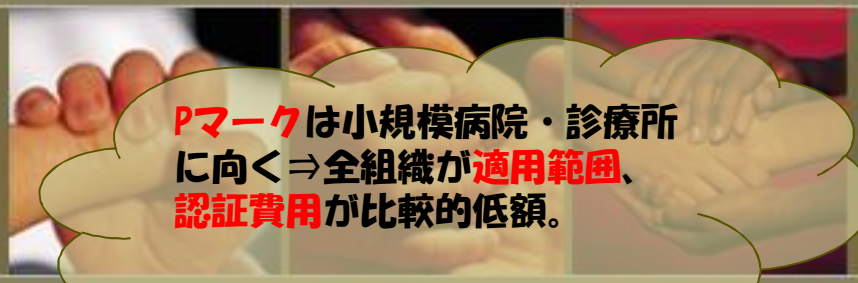
◆医療・介護分野の情報セキュリティ対策及び個人情報保護対策は、個人情報保護法などの法令義務対策とPマーク認証やISMS認証などの差別化対策がある。

・**法令義務対策**：個人情報保護法および厚生労働省ガイドラインのほか、医療分野の情報セキュリティ対策としては、厚生労働省通達「医療画像電子保存（1994）」「電子カルテの電子保存（1996）」「個人情報保護法義務事項（2005）」「厚生労働省医療・介護個人情報保護ガイドライン義務事項」「厚生労働省医療情報システム安全管理ガイドライン（2013）」などへの対応が求められる。

・**差別化対策**：認証制度として「Pマーク」「ISMS（ISO27001）」、第三者評価として「情報システム監査」などある。

5. 医療・介護の情報セキュリティ対策（その1）

2）Pマークとは



Pマークは小規模病院・診療所に向く⇒全組織が適用範囲、認証費用が比較的低額。

登録番号の構成：　Annnnnn（mm）

A・・・・・・・・指定機関を示すコードで、1桁のアルファベット。付与の申請を審査した指定機関を示す。指定の順にBから採番。Aは、付与機関が使用。

nnnnnn・・・・・・民間事業者に付与する番号で、6桁の数字。付与を受けた民間事業者に対し、指定機関コード毎に認定の順に000001から採番。更新しても変更はしない。

mm・・・・・・・・更新の回数を示し、（　）付きの2桁の数字で表す。01からはじめ更新毎に1ずつ増加する。

1.概要

個人情報の取扱いについて、適切な保護措置を講ずる体制を整備している民間事業者等に対し、その旨を示すマークとしてプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認容する制度。有効期限は2年間。以降は2年毎の更新。

2.目的

プライバシーマーク制度は、個人情報の保護に関して、下記を目的とする

①個人の意識の向上を図ること、

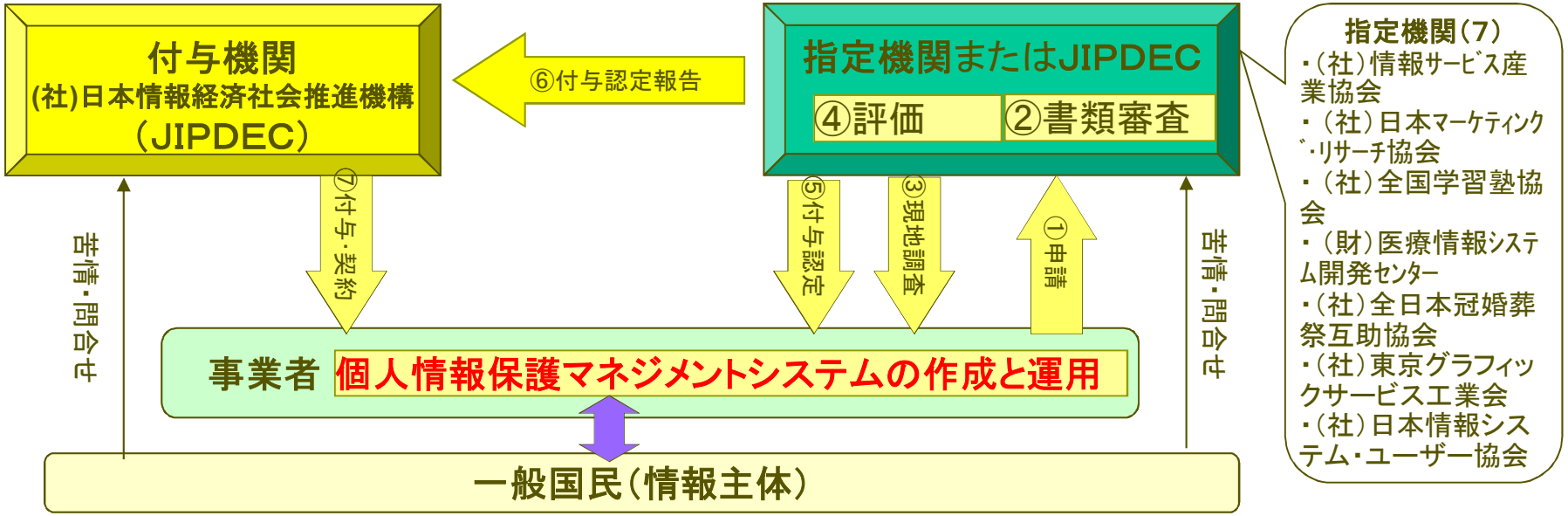
②民間事業者の個人情報の取扱いに関する適切性の判断の指標を個人に与えること、

③民間事業者に対して個人情報保護マネジメントシステム（PMS）へのインセンティブを与えること

5. 医療・介護の情報セキュリティ対策(その1)

3)Pマーク制度の概要

図表5. 2. Pマーク制度の概要 (2013. 11. 27現在13, 311社認定、 うち医療業は47社)



認定費用	小規模企業	中規模企業	大規模企業
申請手数料	50,000	50,000	50,000
現地調査料	200,000	450,000	950,000
Pマーク使用料	50,000	100,000	200,000
計	300,000	600,000	1,200,000

中規模	製造業等	卸売業	小売業	サービス業
資本金	3億円以下	1億円以下	5000万円以下	5000万円以下
従業員	300人以下	100人以下	50人以下	100人以下
小規模	20人以下	5人以下		

5. 医療・介護の情報セキュリティ対策(その1)

4)ISMS(ISO27001)とは

ISO27001（ISMS）は大病院に向く⇒適用範囲を選択できる、国際的評価を得る。

1. ISMSの目的

ISMS適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントとしての第三者適合性評価制度であり、本制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものです。

2. ISMSの認証基準(2013.11.27現在4,413社認証)

ISMSの認証基準(Ver. 2)は、英国規格BS 7799-2:2002に基づき作成したもので、本基準で使用する用語、表現については、JIS X 5080:2002(国際規格ISO/IEC 17799:2000)との互換性を確保しています。2005年のISO/IEC27001の発行に伴い、ISMS認証基準(Ver. 2)は、2006年4月よりJIS Q 27001へ移行しました。

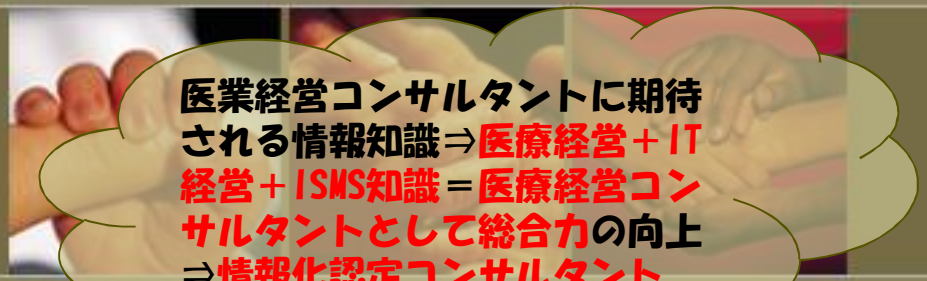
3. ISMSの適用範囲

ISMSの適用範囲は、企業情報を大量にマネジメントする企業内の部署を限定して導入を図ることが可能です。このため、ISMSはPマークに比べ大企業や事業所の多い企業に向いています。

4. 登録と維持および更新登録

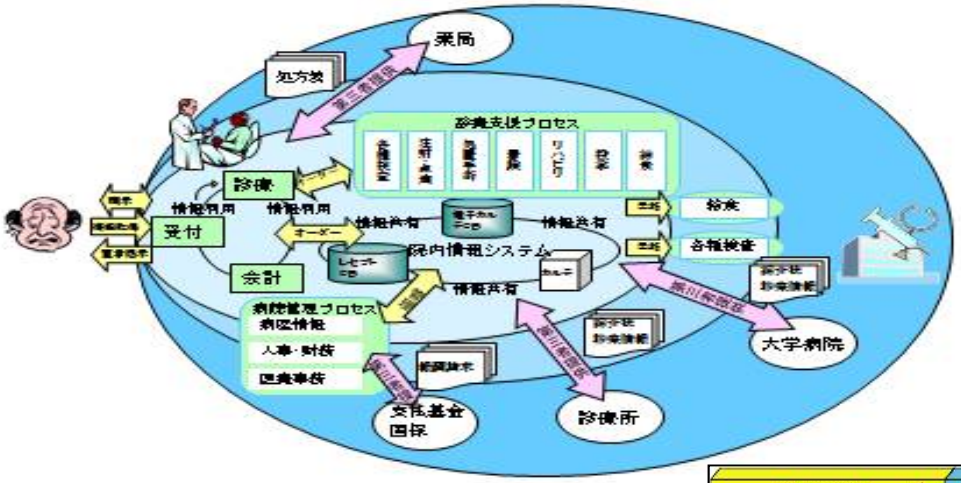
5. 医療・介護の情報セキュリティ対策（その2）

5）医業経営コンサルタントに期待されるIT知識・スキル



医業経営コンサルタントに期待される情報知識⇒医療経営＋IT経営＋ISMS知識＝医療経営コンサルタントとして総合力の向上⇒情報化認定コンサルタント。

図表5. 3. 医療経営＋IT経営＋ISMS知識・スキルによる医業経営支援



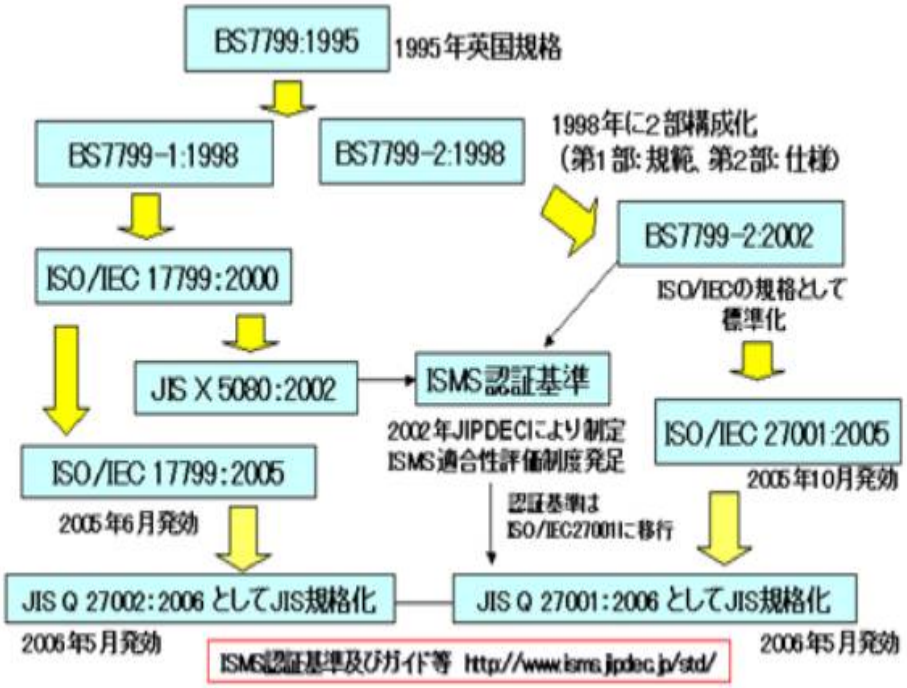
医業経営コンサルタント

◆今後の医業経営コンサルタントに期待される知識・スキルは以下である。
・医業経営知識・スキル
・IT経営知識・スキル
・情報セキュリティマネジメントシステム（ISMS）知識・スキル
◆当協会情報化認定コンサルタント資格認定特別委員会では、医業経営コンサルタントの情報化知識・スキルの向上を図るため、IT経営・情報セキュリティに関する継続研修を別途実施することを提案している。

◆参考資料

◆参考資料①

参考図表1. BS7799からISMS認証基準までの流れ

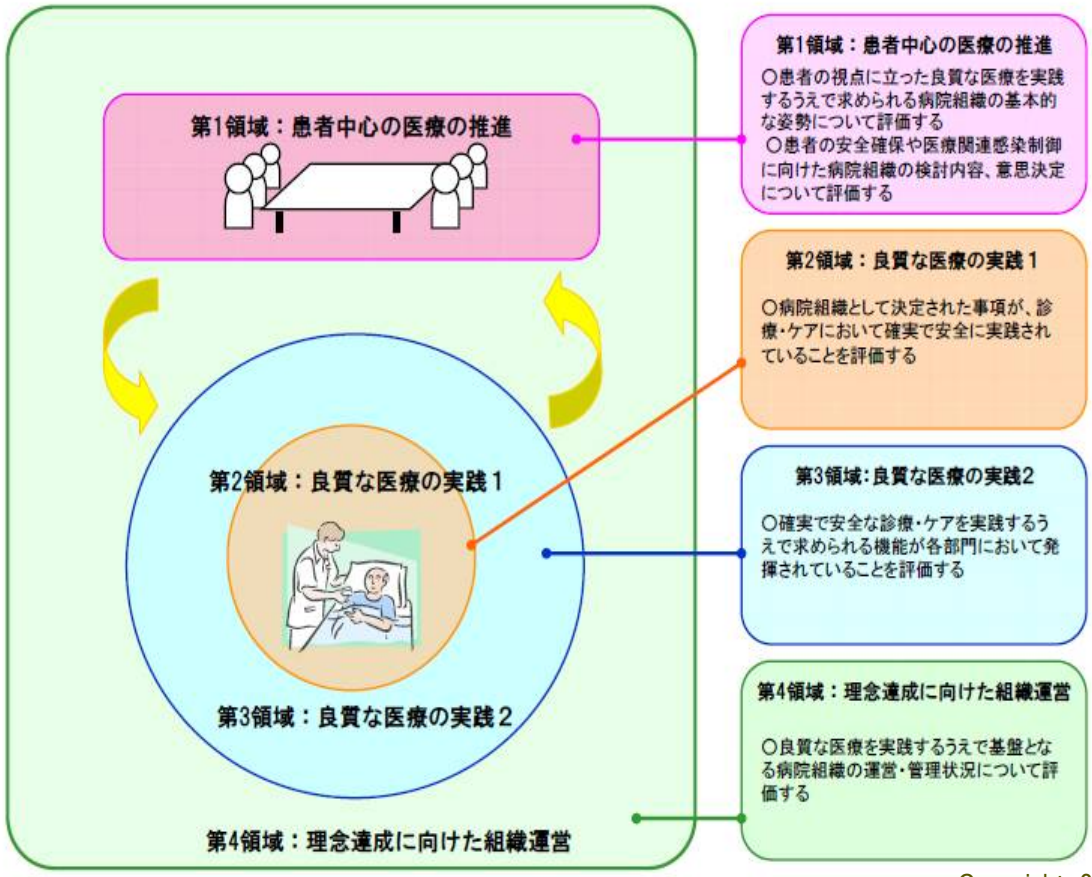


出典:独立行政法人情報処理推進機構(IPA)ホームページ「情報セキュリティマネジメントとPDCAサイクル(http://www.ipa.go.jp/security/manager/protect/pdca/index.html)」より引用

◆ISO/IEC17799は情報セキュリティ対策の管理策集、ISO/IEC27001はその管理策を適切に運用していることを認証するための規格。
◆1995年にBS7799の国際標準化が失敗に終わったが、再度国際標準化を狙い、2000年にはBS7799-1(Part1)がISO/IEC17799:2000として採用され、それに伴い英国規格もBS7799-1:2000として改正された。BS7799-2(Part2)はその後、プロセスアプローチ、PDCAサイクル、継続的改善等の考えを盛り込み、BS7799-2:2002となった。
◆日本では、ISO/IEC17799:2000はJIS X 5080:2002としてJIS化され、一方、BS7799-2:2002は、2002年4月にISMS認証基準(Ver.1.0)として制定され、この基準によるISMS適合性評価制度が稼動し始めた。その後、2003年4月にISMS認証基準(Ver.2.0)が制定された。2005年にBS7799-2:2002がISO/IEC27001:2005として国際標準化され、それがJIS Q 27001:2006としてJIS化されたのに伴い、ISMS適合性評価制度の準拠する基準はJIS Q 27001:2006に移行することになった。

◆参考資料②

参考図表2.1.病院機能評価新たな枠組み（2012年6月）



◆機能種別：病院機能に基づく5区分の導入（一般病院1（原則100床前後＋ケアミックス200床程度以上）、一般病院2（二次医療圏基幹的病院＋専門的高度医療病院）、リハビリテーション病院、慢性期病院、精神科病院）
◆評価重点：各部門における体制、規程の整備と組織的活動の評価⇒**プロセス評価**を重視
◆**評価対象領域**：対象領域と主な評価内容は参考図表2.1.参照。
◆評価項目：中項目（137項目⇒88～92項目）・小項目（352項目⇒**廃止**）
◆更新：（新規）**認定3年後状況確認**（文書審査**無料**・訪問審査有料）・5年目更新
◆評価結果：中項目5段階評価・小項目3段階評価⇒**中項目4段階評価**S（秀）・A（適切）・B（一定水準）・C（一定水準未満）

◆参考資料③

参考図表2.2.病院機能評価　機能種別評価項目
一般病院１〈３rdG：Ver1.0〉評価の視点/評価の要素

4　理念達成に向けた組織運営

4.1　病院組織の運営と管理者・幹部のリーダーシップ

4.1.4　情報管理に関する方針を明確にし、有効に活用している

【評価の視点】

○　情報の管理・活用に関する方針が明確にされ、それに基づき院内の情報が管理され、有効に活用されていることを評価する。

【評価の要素】

- 情報の管理・活用の方針
- 個々の患者の診療に関する情報の統合的な管理
- データの真正性、保存性の確保
- 情報システムの導入・活用に関する検討

◆講師プロフィール

- ***氏名***：**小野瀬　由一（おのせ　よしかず）**
- ***出身***：山形県鶴岡市（1952年生まれ）
- ***所属***：NPO法人東京ITコーディネータ副理事長、NPO法人VERSTA 専務理事、ブラジルJBC代理人
- ***学歴***：東海大学海洋学部卒、高千穂大学大学院経営学研究科博士後期課程修了
- ***学位***：高千穂大学大学院経営学博士（Ph.D.）『CSR対応型介護サービス経営革新モデルに関する研究』
- ***資格***：中小企業診断士・ITコーディネータ・**公認システム監査人・ISO27001＆ISMS審査員補**・一級販売士・イベント業務管理者・東京都福祉サービス第三者評価者、認定登録医業経営コンサルタント・情報化認定コンサルタント
- ***略歴***：大学卒業後、海洋環境計測会社、食品業界団体を経て、日本初の音楽ビジネス専門学校・大学にて、助教授・企画開発部長として音楽ビジネス・マネジメント教育と企画開発事業に従事。21世紀に入り、経営コンサルタントとして独立する一方で大学院に進学し介護経営革新モデルの研究により博士号を取得。
- その後、医療分野では**社団法人日本医業コンサルタント協会情報化（IT）特別委員**に就任し「**情報化認定コンサルタント（CIT）**」育成事業に従事した。介護分野では東京都中小企業振興公社支援専門家として「東京都ものづくり新集積形成事業」の介護製品流通アドバイスをはじめ、町田商工会議所シニア商品開発創業塾塾長に就任するほか、東京商工会議所板橋支部、埼玉県さいたま商工会議所、武蔵野商工会議所、茨城県結城商工会議所、北海道函館商工会議所、滋賀県高月町商工会、宮崎県川南町商工会などにおいてシニアビジネス、介護ビジネス関連のセミナー・創業塾の講師を担当した。
- 最近の活動としては、**社団法人日本医業コンサルタント協会企画小委員**に就任し「**医療経営者のための介護経営マニュアル**」編集委員として執筆参加した。現在は、**東京都福祉サービス第三者評価者**として、介護サービス・保育サービス等の福祉サービス第三者評価事業にも従事している。
- ***教育***：産業能率大学学習サービスセンター「ITマネジメント・エッセンス」「グローバルリーダーシップ」担当講師、拓殖大学商学部国際ビジネス学科「健康介護ビジネス論」担当講師
- ***著書***：「中小企業診断士合格50の鉄則」（法学書院）「商店街再生のデザイン」「介護ビジネス2002」「介護ビジネス2003」「介護ビジネス2004」「重点解説介護ビジネス経営革新の進め方」「介護ビジネス2005」「介護ビジネス2006」「循環資源大国ブラジルビジネス入門」「検証！介護事業の経営リスクとシステム改善～介護ビジネス2008」（以上同友館）、「ブックレットVol2.介護保険制度改正と今後の事業展開 」「介護サービスのリスクマネジメント」（第一法規）、「医療経営者のための介護経営マニュアル」（日本医療企画）ほか
- ***信条***：ポジティブ＆アクティブ＆クリエイティブ
- ***興味***：海外旅行・映画鑑賞・音楽鑑賞