変更履歴

※版数は法改正でメジャーアップ、軽微な修正はマイナーアップ

No.	版数	変更日	変更者	変更箇所	変更内容
1	1.0	2021/5/6	事務局	---	初版
2	1.1	2022/4/5	石本	1.2	法施行日の表現を変更、個人情報取扱事業者であることの説明（吹き出し）を削除し、文章も是正。
3	1.1	2022/4/5	石本	1.2.2	監督権限を主務大臣から個人情報保護委員会へ変更。
4	1.1	2022/4/5	石本	1.2.2	罰則の変更
5	1.1	2022/4/5	石本	5.5	「2017年度情報セキュリティインシデントに関する調査報告書」の内容を2018年度版に更新
6	1.1	2022/4/5	石本	6.1	Pマーク更新回数修正
7	2.0	2022/4/5	石本	1.1	保有個人データの6カ月以内に消去する場合は対象外となる文を削除
8	2.1	2022/12/16	石本	2.3	誤字修正
9	2.1	2022/12/16	石本	6.5	「Mail」を「メール」に変更
10	2.2	2024/5/23	石本	–	年度更新（表紙の年度やPマーク更新回数）

No.	版数	変更日	変更者	変更箇所	変更内容
11	2.3	2024/6/18	石本	---	体制図を更新
12	2.4	2025/2/17	石本	–	年度更新（表紙の年度やPマーク更新回数）
13	2.5	2025/2/17	石本		個人情報漏えい事故の事例　③の内容を更新
14	2.6	2025/3/7	石本		7.1 個別事案①の内容を更新 個別事案の採番し直しと出向社員による漏洩事故追加
15	2.7	2025/3/18	石本		体制図を更新

個人情報保護
学習テキスト

2025年　プライバシー定期教育

版数　：2.7
作成日：2025/04/01
作成　：個人情報保護教育担当者
監修　：CSIRT

本教育の目的

1. 個人情報とは・・・
2. 個人情報保護マネジメントシステム
3. PMSに適合することの重要性と利点の認識
4. PMSに適合することの役割と責任の認識
5. PMSに違反した際に予想される結果
6. 個人情報に関する当社の取り組みの理解
7. 各社員が守るべきルール
8. テレワーク(在宅勤務)について
9. まとめ

1. 個人情報とは・・・

1. 個人情報とは・・・

この章では、個人情報保護法について、パートナー会社社員や受託案件で取り扱う個人情報、ひいては私たちの個人情報を守る為に、法が企業に求めていることを学ぶ。

1.1 個人情報保護法で守られる個人情報とは

＜個人情報＞

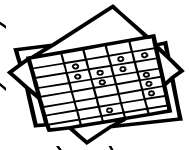
・その情報から特定の個人を識別できる生存者の情報。
（他のものと照合することで容易に識別できるものを含む）
・個人識別符号が含まれるもの（指紋認識データ等）
・要配慮個人情報
（本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪被害の事実）
ex.・住所　・氏名　・社員番号　・E-Mailアドレス → 名刺の情報も個人情報

＜個人データ＞

個人情報データベース等を構成している個人情報であり、容易に検索できるよう、体系化したもの
※紙媒体、電子媒体問わない
ex.・システムテストのために預った顧客の実データ
・提供を受けたメーリングリスト
・電話帳、住宅地図データなど

＜保有個人データ＞

個人情報取扱事業者が、開示、内容の訂正、追加、削除、また第3者への提供の停止を行う権限を持つ個人データ。
ex.・名刺を50音別に纏めたもの
・アンケートで収集した顧客情報の一覧資料



これを取扱っている個人情報取扱事業者の責任が重いとして、責任に応じた管理が要求されている。

1.2 個人情報保護法とは

個人情報保護法

基本理念＝情報取扱いの基本的考え方
（個人情報を取扱う全ての者が個人情報の保護の為に自ら努力すべき事項）
2003年5月30日一部施行

<個人情報の適正な取扱い>
個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきもの
であることにかんがみ、その適正な取扱いが図られなければならない。

義務規定＝個人情報取扱事業者が守るべき
必要最小限の規定（勧告・罰則対象）
2005年4月全面施行→2017年5月改正法施行

「個人情報取扱事業者」

コンピュータ技研は個人情報取扱事業者に該当する。

1.2.1 個人情報保護法の成立

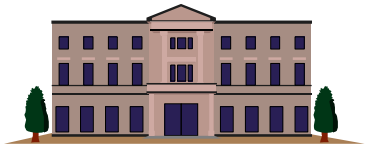
個人情報の利用に関して

2003年以前は

民間企業は原則として、自主規制に委ねられていた

個人情報が自由に取得・利用されていた

現在



2003年5月
個人情報保護法が成立

2005年4月
全面施行

2015年9月
個人情報保護法改正成立・公布

2017年5月
改正法全面施行

法により規制される

1.2.2 個人情報保護法「義務規定」

義務規定＝個人情報取扱事業者が守るべき必要最小限の規定
（勧告・罰則対象）情報の種別により義務の範囲が異なる

個人情報

(1) 利用目的の特定
(2) 利用目的による制限
(3) 適正な取得
(4) 利用目的の通知等
(5) 個人情報取扱事業者による苦情の処理

個人データ

(6) データ内容の正確性の確保
(7) 安全管理措置
(8) 従業者の監督
(9) 委託先の監督
(10) 第三者提供の制限
(11) 外国にある第三者への提供の制限
(12) 第三者提供に係る記録の作成等
(13) 第三者提供を受ける際の確認等

保有個人データ

(14) 保有個人ﾃﾞｰﾀに関する事項の公表等
(15) 開示
(16) 訂正等
(17) 利用停止等
(18) 理由の説明
(19) 開示等の求めに応じる手続き
(20) 手数料

※罰則：個人情報保護委員会の勧告、命令に従わない場合、1年以下の懲役又は100万円以下の罰金
法人には1億円以下の罰金が科される

2. 個人情報保護マネジメントシステム

2. 個人情報保護マネジメントシステム

この章では、個人情報保護に関するJIS規格であるJISQ15001と、そのJISQ15001を遵守していると認められた企業に使用が許可されるプライバシーマークについて学ぶ。

2.1 JISQ15001とは

（正式名称：個人情報保護マネジメントシステム　要求事項）

個人情報保護法が成立する以前の1999年に個人情報保護に関する遵守規定がJIS規格化されている。

→2017年12月にJISQ15001:2017として大幅改定

↑

法律より厳しい規定

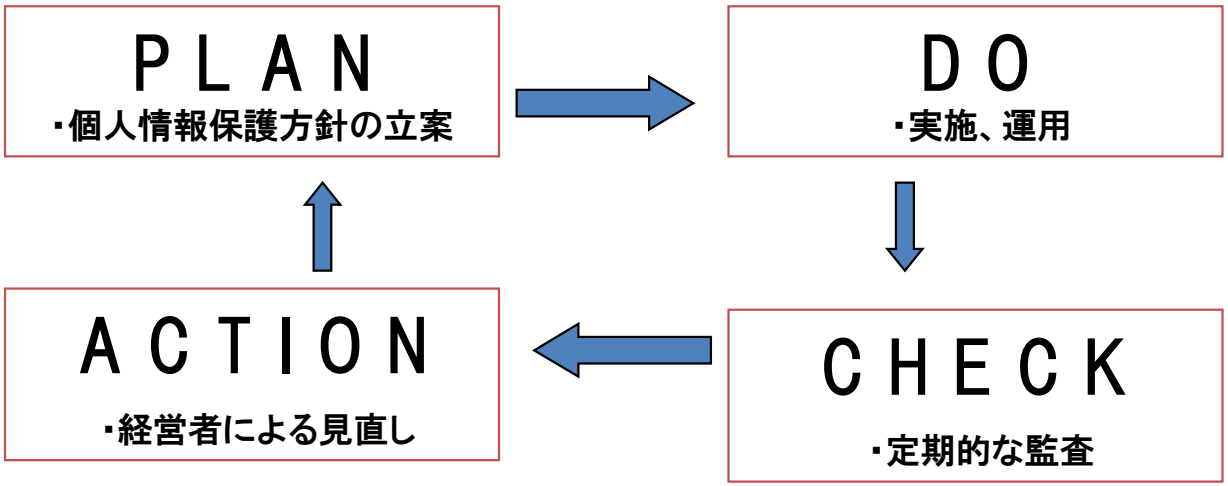
↓

コンピュータ技研はJIS規格遵守の証である「プライバシーマーク」の使用を許可されている企業

2.2 JISQ15001の特徴

【JISQ15001の主な特徴】

(1)PDCAサイクルをスパイラル的に回すことで継続的に管理レベルが向上する仕組み(図参照)



(2)個人情報保護法だけでなく、他の法律や方針、規範、倫理、手続等を含めて遵守する体制を構築する仕組み

⇒個人情報保護マネジメントシステム

(3)個人情報保護法との親和性が高い

(JISQ15001を遵守することで、法律も守ることができる)

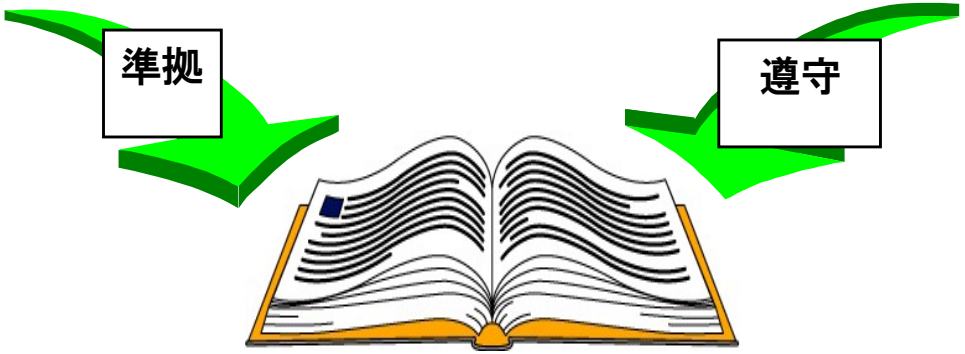
2.3　個人情報保護マネジメントシステムとは

- 個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含む体制を構築する仕組み（マネジメントシステム）
- 自社の業務の中で具体的に「どのように個人情報保護を実践するか」について書かれたもの。このようなルールを文書で定めることにより、担当者が代わっても個人情報保護の体制を維持することができる。

個人情報保護マネジメントシステムに適合することの重要性
- 高度情報化社会の健全な発展と適切な消費者保護を促す
- 個人情報の適切な利用と保護を促す

JIS Q15001
個人情報保護マネジメントシステムの要求事項

個人情報保護関連法



（自社の）
個人情報保護マネジメントシステム

2.4 プライバシーマーク

- （財）日本情報処理開発協会（JIPDEC）が推進する個人情報保護の認定制度
- JIS Q 15001準拠（法律より厳しい規定）
- 個人情報における信頼の証
- 2年毎に継続更新

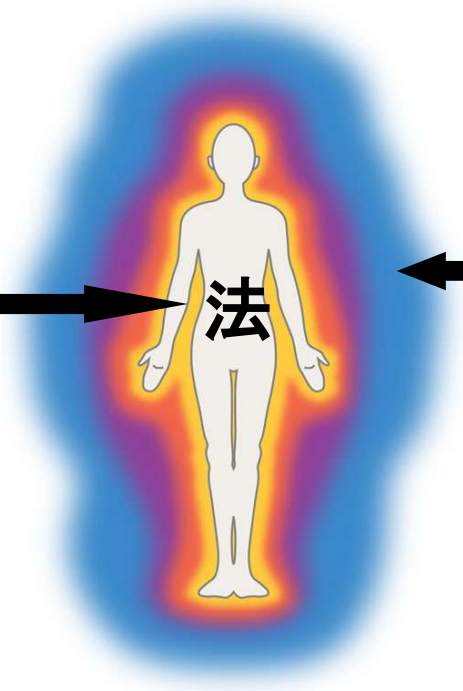
メリット
- 顧客からの信頼
  ⇒受注条件となり得る
- 消費者(個人)からの信頼
- 個人情報保護法への対応基盤

責任
事業者としての社会責任が重くなる

JISQ 15001による個人情報の定義

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他記述、又は個人別に付された番号、記号その他の符号、画像若しくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む）。

法律は、
「生存者の情報」



JISQ15001

JIS規格の方がより
広い範囲をさしている

3. PMSに適合することの重要性と利点の認識

3. PMSに適合することの重要性と利点の認識

この章では、現在における個人情報に対する法律に則った取組の必要性、及び、PMSに適合することの重要性と、プライバシーマークの認定を受けるメリット、及び、個人情報保護マネジメントシステムに適合するメリットを考える。

3. PMSに適合することの重要性と利点の認識

法規制が無かった時代

特に意識なく、自由に集め自由に利用していた。

現在（法規制後）

法律に則った利用が求められ、個人情報漏えいは処罰の対象となる。また社会的な信用度の失墜につながる。

PMSに適合することで、個人情報の保護対策を行う。

3. PMSに適合することの重要性と利点の認識

プライバシーマークの認定を受けるメリットと

個人情報保護マネジメントシステムに適合するメリット

- 個人情報を適切に扱っていることを、
  取引先や消費者にアピールできる。

- PMSを構築・運用することにより、
  個人情報を漏洩するリスクを極めて低下
  させることができる。

4. PMSに適合することの役割と責任の認識

4. PMSに適合することの役割と責任の認識

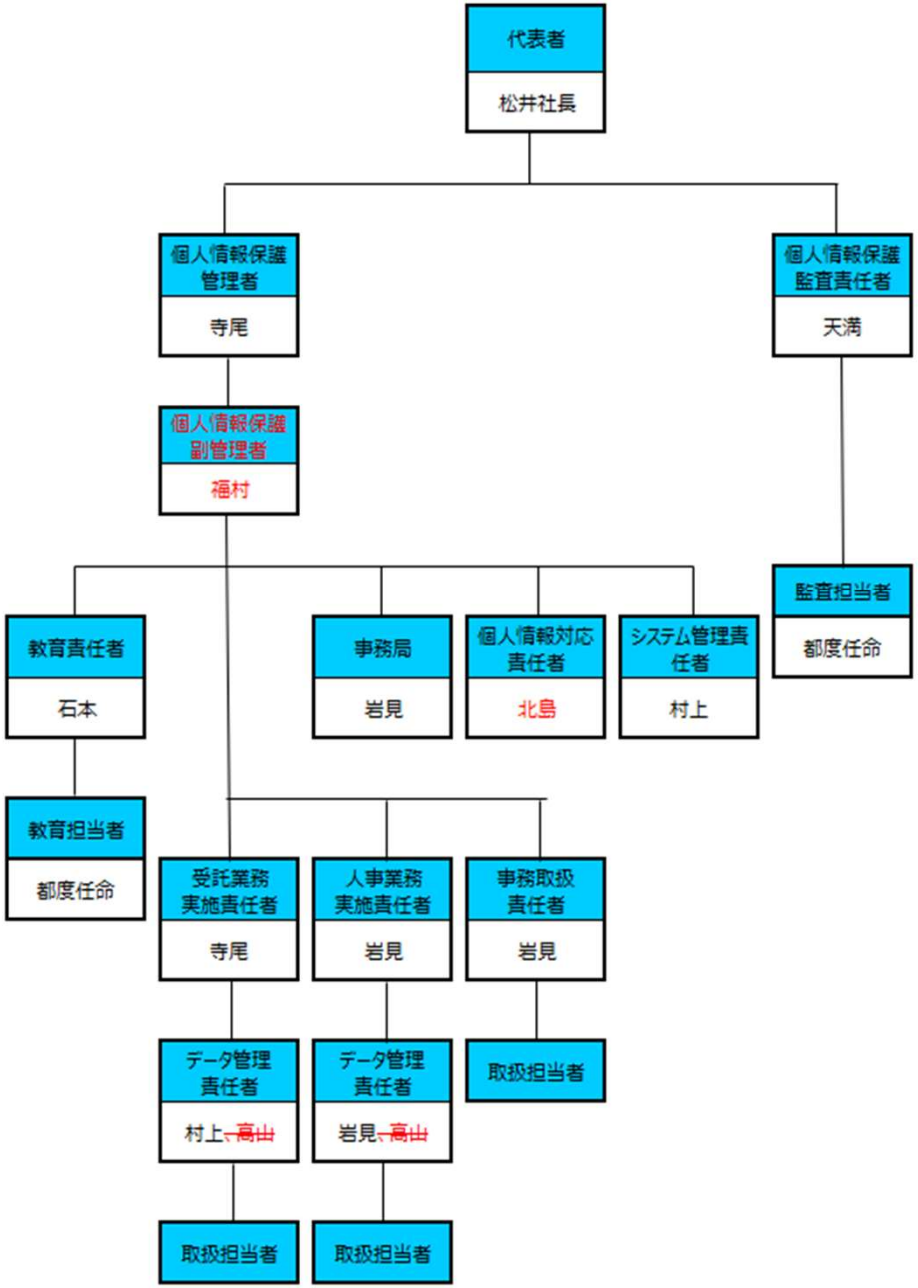
情報サービス事業者の代表者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ改善するために不可欠な資源を用意しなければならない。

情報サービス事業者の代表者は、個人情報保護マネジメントシステムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、従業者に周知しなければならない。

4. PMSに適合することの役割と責任の認識

別紙－1　　2024/10/17　版数：1.2

個人情報保護に係わる組織体制図



左記の組織体制を基に役割・権限・責任を明確化したうえで、PMSに対して組織的に運用を行う。

5. PMSに違反した際に予想される結果

5. PMSに違反した際に予想される結果

この章では、個人情報の漏えい事故などを紹介し、
なぜ個人情報保護が必要なのか、
という背景を説明し、合わせてPMSに適合することの
役割と責任、違反した際の結果について学習する。

5. PMSに違反した際に予想される結果

こんな経験がありませんか？

〇〇さんのお宅ですか？

お宅には5年生になられる娘さんがいらっしゃいますよね。

中学の受験をお考えでしたら、是非うちの塾で受験対策を・・・。

塾の営業

はて？

なぜ5年生の娘がいることを知っているのだろう？

個人情報は、本人の知らない所でも、取得、利用されている。

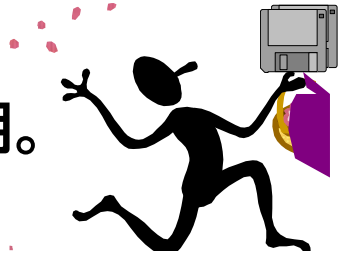
5.1　個人情報漏えい事故の事例　①

【大手通信教育会社の顧客リスト漏えい】(2014年)

＜事故内容＞

会員から「不審なメールが来る」との連絡により、

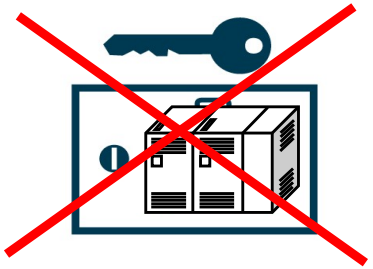
会員2070万件(世帯)の個人情報が社外へ流出したことが判明。



＜主な原因＞

・業務に従事するSEのモラルの低さ。(確信犯)

・会員情報へアクセス可能な人が多かったこと。



＜損害＞

・「お客様問い合わせ窓口」を設置し、顧客からの問い合わせに全件対応。

・金銭的な補償、及び、お詫び状の発送や情報流出の調査を実施。

過去最大級の損害

260億円 の支出

5.2　個人情報漏えい事故の事例　②

【H銀行：従業員の無断持ち出しで紛失(2011年10月】

＜事故内容＞

従業員が自宅で作業するため無断で内部資料を持ち出し**帰宅途中で紛失**。

顧客情報は氏名・住所・勤務先のほか決算データや融資額、預金残高など。

＜主な原因＞

個人情報データの取扱管理全般、無断持ち出し

5.3　個人情報漏えい事故の事例　③

【保険・金融商品販売：従業員の無断持ち出しで紛失（2024年8月】

＜事故内容＞

Ａ社からの出向社員2名が当企業が保持するＡ社以外の
保険契約者情報をＡ社に漏えい

件数　　：3万5千件

流出内容：契約者名や住所、電話番号、保険料や契約先など

＜主な原因＞

出向社員による不正持ち出し

個人情報データの取扱管理全般

5.4 個人情報漏えい事故の事例（その他）

頻繁に発生！

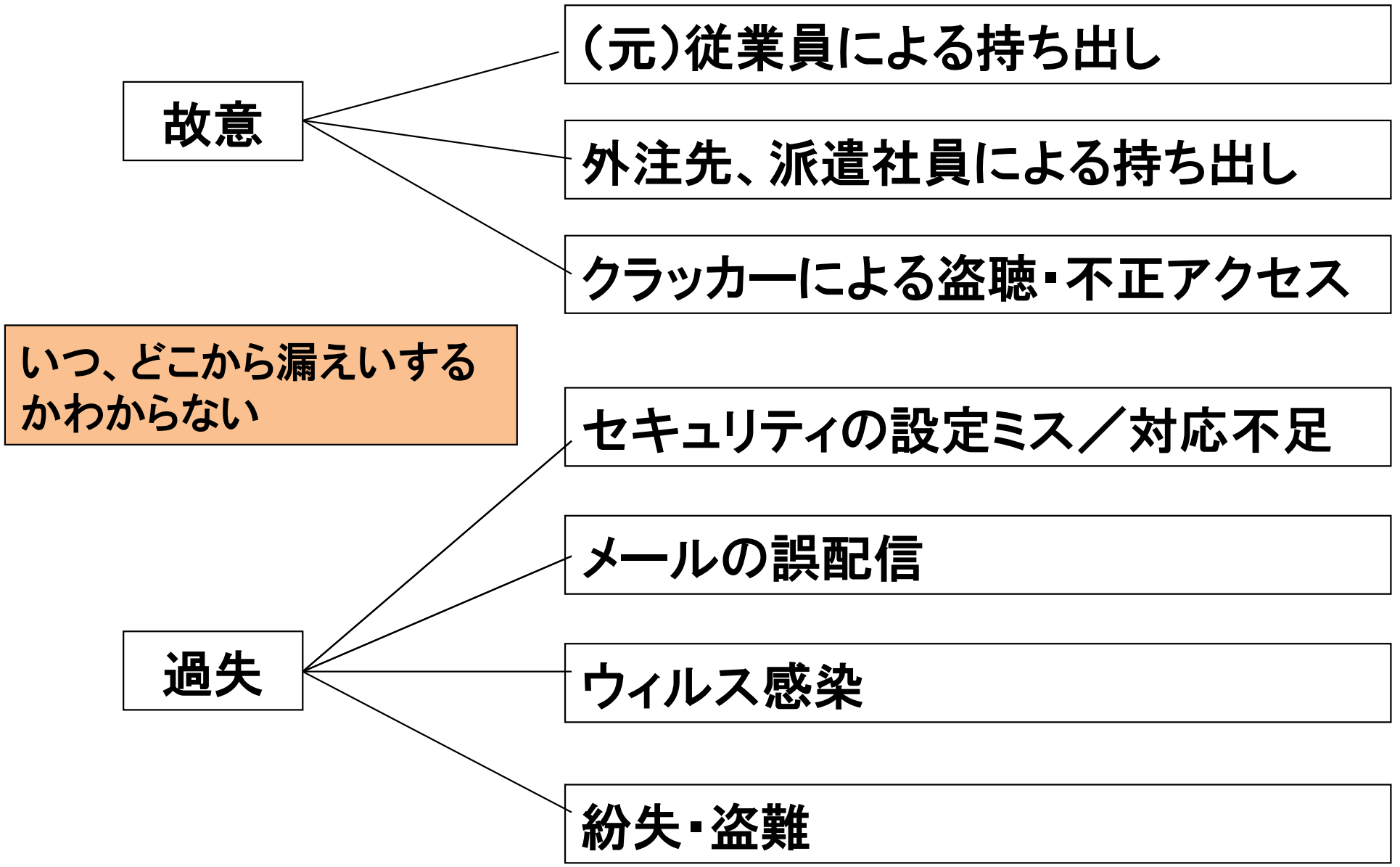
漏えい事故！！

あまりニュースで取り上げられていないが、

実はこんなに発生している！！

日付	法人・団体名	件数・人数	漏洩原因	漏洩内容・詳細・二次被害（悪用）など
2025/1/27	株式会社ハンズ	12万1,886件	不正アクセス	株式会社ハンズは、同社が展開する雑貨通販アプリ「ハンズクラブアプリ」に対し、第三者による不正なアクセスが確認されたと発表した。不正アクセスの影響により、登録している一部ユーザーの個人情報12万1,886件について、漏えいの可能性が生じている。
2025/1/10	株式会社東急モールズデベロップメント	1,082件	誤送信	株式会社東急モールズデベロップメントは、同社が一部業務を委託している事業者が電子メールを誤送信し、同社元従業員等を含む従業員の個人情報1,082件を外部漏洩したと発表した。
2024/12/25	大阪医科薬科大学病院	5,031件	USBメモリ紛失	大阪医科薬科大学病院は、緩和ケアセンター執務室内にて患者の個人情報を記録したUSBメモリを紛失したと発表。紛失したUSBメモリには、氏名や年齢、病名など5,031名の情報が記録されていた。
2024/11/8	ウエルシア薬局株式会社	4万736件	サポート詐欺	公式通販サイト「ウエルシアドットコム」担当従業員のサポート詐欺被害に伴い、ユーザー3万9,805名や関係会社の従業員931名の個人情報漏えい懸念を公表。
2024/10/16	株式会社八十二銀行 株式会社長野銀行	10万6,000件	情報誤漏えい	株式会社八十二銀行と株式会社長野銀行は、業務提携契約に関連して両社に出向していたアコム株式会社の従業員が、両社の保有する個人顧客の情報合計約10万6,000件をアコム社に漏えいしていたと発表した。
2024/10/15	日本駐車場開発株式会社	5,078件	PC紛失	日本駐車場開発株式会社は、同社に所属する従業員が駐車場契約者等の契約者情報合計5,078件が記録されたノートパソコンを紛失したと発表。

5.5　個人情報漏えいの原因



5.6　個人情報漏えいの社会的影響

・信用失墜
・多額の損害賠償金
・調査・データベース再構築等の対策に掛かる費用・時間的損害
・上場企業の場合は株価下落
・業務停止等による実被害

想定損害賠償額

1件当り平均　6億3767万円

（平均　1万3334人分　漏えい）

※NPO日本ネットワークセキュリティ協会発行「2018年度情報セキュリティインシデントに関する調査報告書」より

会社存亡の危機!

5.7　個人情報漏えいの社員に対する責任

個人情報漏えいが発生した場合、社会的な企業の責任が問われることはもちろんのこと、

漏えいした原因によっては、社員個人の責任が問われることもある。

社員一人一人がPMSに対して常に意識し、

個人情報保護に取り組む必要がある。

6. 個人情報に関する当社の取り組みの理解

6. 個人情報に関する当社の取り組みの理解

この章では、コンピュータ技研における
個人情報保護の取組みについて学ぶ。

6.1　プライバシーマーク取得

株式会社コンピュータ技研は、財団法人日本情報処理開発協会より、個人情報の適切な取扱いを行う事業者に付与されるプライバシーマークの付与認定を受けています。

・2004年6月から取組み開始

・2005年6月7日に
財)日本情報処理開発協(JIPDEC)より認証(2年間有効)

・更新取得中(現在11回更新)

↑　コンピュータ技研　許諾番号

コンピュータ技研は
個人情報を適切に取り扱う事業者という証

6.2 個人情報保護方針

- 株式会社コンピュータ技研は、IT情報処理関連業務において質の高いサービスを提供することにより、お客様の信頼にお応えすると共に、業務の適正な運営と健全な業績の伸長を通じて広く社会の発展に貢献することを経営理念としております。個人情報を安全に保管・管理し、次に掲げた事項を常に念頭に置き、個人情報保護に万全を尽くしてまいります。

- 個人情報の取扱いについて規定を定め、また、組織体制を整備し、個人情報の適切な保護に努めております。
個人情報を取得させていただく場合は以下にあげる内容をお知らせしたうえで、事業の内容と規模を考慮して必要な範囲で個人情報を取得させていただきます。

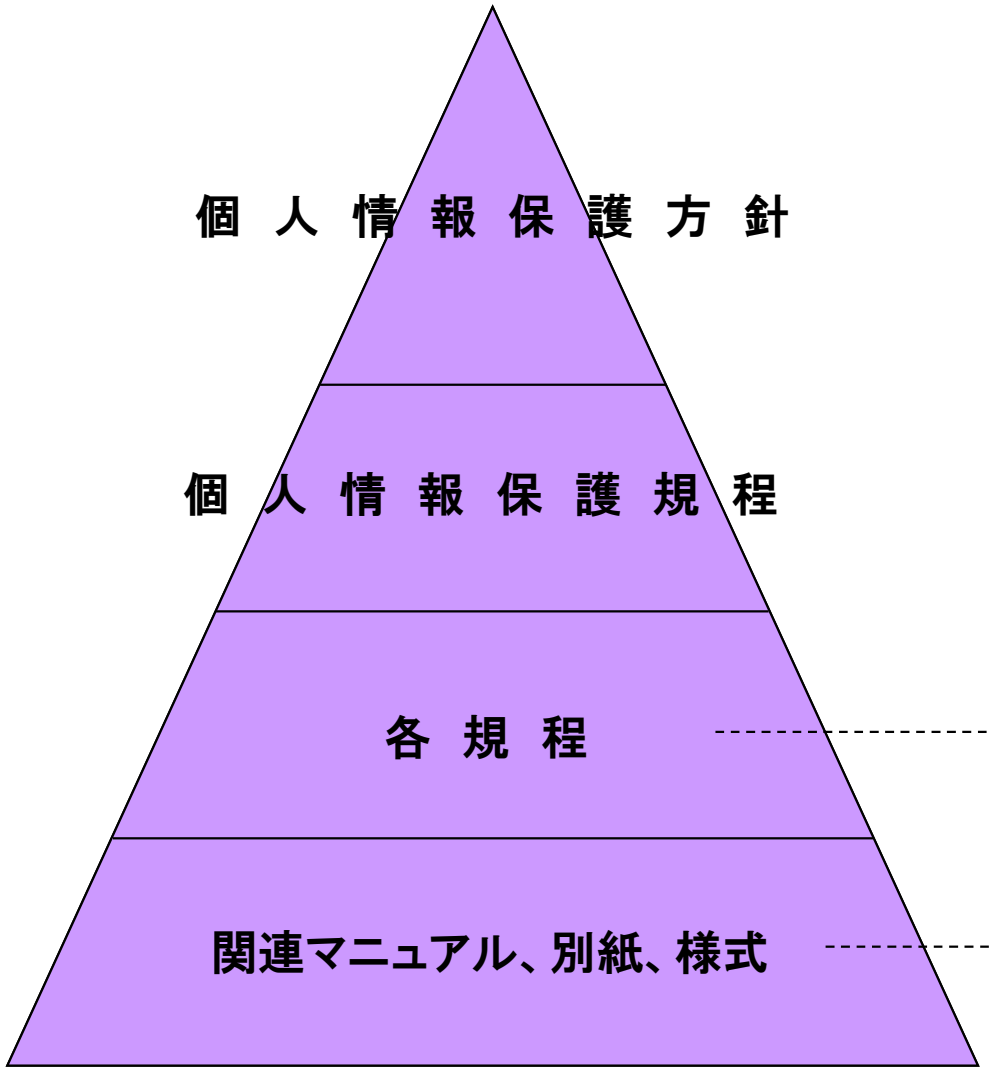
  ①事業者の氏名
  ②個人情報保護管理者の氏名
  ③利用目的
  ④提供の有無と提供する個人情報の項目
  ⑤委託の有無
  ⑥当社の個人情報相談窓口
  ⑦個人情報を与えることの任意性と与えなかった場合に生じる結果

  当社Webサイトにも掲載

- 当社は、個人情報を利用目的の達成に必要な範囲を超えた取り扱い（以下「目的外利用」といいます）をすることはないとともに、適切な方法で管理し、本人の承諾なく第三者に開示・提供することはありません。
当社は、委託元よりお預かりした個人情報は、厳正なる管理を行い契約の範囲内で利用します。また、当社が、個人情報の処理を外部へ委託する場合には、委託先の個人情報保護の水準を確認し、漏えい等を行わないよう契約により義務づけ、適切な管理を実施させていただきます。
個人情報は、正確かつ最新の状態に保ち、目的外利用、個人情報の漏えい、滅失又はき損の防止及び是正の措置を講じております。
当社は、個人情報の取扱いに関する本人からの苦情及び相談等の問い合わせに対し、誠実かつ迅速に対応いたします。
当社が保有する個人情報に関して適用される法令、国が定める指針その他の規範を遵守するとともに、上記各項における取り組み及び保護活動を、維持、改善してまいります。

6.3 個人情報保護マネジメントシステム

個人情報保護マネジメントシステム(PMS)の関連規定と文書体系



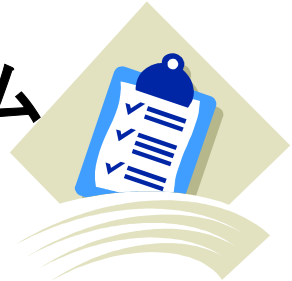
PMSの関連規定と文書体系を遵守した上でコンピュータ技研はPMSの運用を行っています。

監査規程や教育規程など、個人情報保護規程に基づき必要な催促を規定したもの

PMS運用にあたり活用される業務マニュアルや運用で用いられる各様式、別紙など

6.4 個人情報保全内部監査の実施

- 全部署に対し、個人情報保護マネジメントシステムに基づく監査を実施



項　目	実　施　要　領
実施時期	1回/年 全部署に対し、内部監査を実施する。
監査要領	全体の監査計画に基づき、各部毎に監査計画書を作成し、実施。 監査結果を監査責任者に報告する。
改善	監査結果により問題点や対応策等がある場合、各部管理責任者に対し、是正処置報告書により改善の徹底を図る。

6.5 個人情報保護のための一人一人の取組み

個人情報の 取得	・不必要な個人情報を取込まない ・特定の機微な情報の取得は原則不可 ・個人情報を業務上取り込むことが予想されたら、 上長・責任者に早めに報告・相談
個人情報の 利用	・個人情報の「目的」を逸脱する使用は不可 ・取扱基準があれば、それに従う （名刺も、電子情報化したら業務登録が必要）
個人情報の 保管・管理	・個人情報を机上に放置しない ・コピー原則不可・社外に持ち出さない ・原則手渡し（宅配便不可） （メールで送信する場合はHengeなどのセキュアな手段で） ・ID、パスワードによる管理 （HDDのパスワード保護／画面のロック）
個人情報の 廃棄	・紙媒体は、シュレッダー ・電子情報は、再読できないよう消去

7. 各社員が守るべきルール

7. 各社員が守るべきルール

この章では、個別にコンピュータ技研における
個人情報保護についてのルールを学ぶ。

7.1 個別事案①

・業務中、画面や資料が閲覧可能な状態で長時間離籍しない。
→離席中に業務上重要な情報等が不特定多数に閲覧されることを防ぐため、ロック画面にするか資料の収納を行うこと。

・やむなく印刷した資料は、不要となった時点で、速やかにシュレッダーを行い廃棄すること。
→保存する必要がある場合は、ファイリングを行い、ルールに則った管理を行うこと。
（裏紙使用や、ごみ箱への廃棄は禁止）

・社給、個人用に関わらず、スマホや携帯電話にお客様情報を登録する際は、フルネームや会社名で登録せず、個人を特定できないように登録を行うこと。（頭文字や、略字等）

7.1 個別事案②

・顧客先ルールの遵守。
→顧客ルールマニュアルを熟読し理解し、徹底すること。

・貸出PCの取り扱い方法。
→フリーソフトのインストールやダウンロードを許可なく
行わない。（貸与物は顧客の資産という側面でも禁止）

・業務上取得した情報の持出し。
→原則禁止。やむを得ない場合、必ず上長の許可を取り、
取扱ルールを順守すること。

7.1 個別事案③

・独断的な判断を行わない。
→顧客ルールから逸脱する行為と思われる場合、必ず上長に確認する。個人的な考えで判断を行わない。

→たとえその行為により効率が上がるとしても勝手な判断は行わない。

許可なくルールから逸脱した行為を行った場合、責任は全て自分で受けることになる。

8. テレワーク(在宅勤務)について

8. テレワーク(在宅勤務)について

2020年以降、新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いたテレワーク環境が急速に普及。社員等を出社させずに事業継続を図る動きが進んでいる。

この章では、このような環境で働く在宅勤務者に向けたセキュリティ上の注意事項を学ぶ。

8.1 テレワーク(在宅勤務)時の注意事項

テレワーク（在宅勤務）時の注意事項を以下に記す。

（１）作業を始めるにあたって

- 自宅での通信環境に関して、最新のセキュリティパッチを適用する
- ルータはメーカのサイトを確認のうえ、最新のファームウェアを適用する
- ウェブ会議のサービス等を新たに使い始める際は、事前にサービス等の初期設定の内容を確認する。特にセキュリティ機能は積極的に活用する

（２）作業を行うにあたって

- テレワークで使用するパソコン等は、他人と共有して使わない
- 公共の場所で作業を行う場合は、ソーシャルハッキングや声もれに注意する
- 公衆Wi-Fiは、意図しない共有や信頼性の問題があるため利用しない


セキュリティ対策 として、詳細を次項以降に記載します。
内容を確認し、セキュリティ対策を厳として対応してください。

8.2 セキュリティ対策

セキュリティ対策の詳細①

・修正プログラムの適用

利用する機器のOS、ルータやスイッチ等のファームウェア、
各種ソフトウェアに修正プログラムを適宜適用し、
最新のバージョンに更新、維持する。

・セキュリティソフトの導入および定義ファイルの最新化

利用する機器等にセキュリティソフトを導入するとともに、
セキュリティソフトの定義ファイルが常に最新の状態になるように設定し、
最新の状態になっているか定期的に確認する。

・パスワードの適切な設定と管理

システム管理等で使用するパスワードは可能な範囲で
複雑な長い文字列を設定する。

8.2 セキュリティ対策

セキュリティ対策の詳細②

・不審なメールに注意

日々届くメールには、ウイルスが添付されていたり、
悪意のあるサイトへ誘導するURLが記載されていたり
といった可能性があるため、不用意にファイルを開いたり、
URLをクリックしない。
そのようなメールを受信した場合は、ただちに管理者へ報告する。

・USBメモリ等の取り扱いの注意

ウイルス感染の可能性があるため、安全性が担保されていないUSBメモリ等の
外部記憶媒体はパソコンに接続しない。

・ソフトウェアをインストールする際の注意

貸与された機器等へ、ソフトウェア（フリーソフト等）を
インターネットからダウンロード、インストールする場合は、
システム管理者に事前に許可をとる。

セキュリティ対策の詳細③

・社内ネットワークへの機器接続ルールの遵守

ウイルス感染したPCや外部記憶媒体を
社内ネットワークに接続することで、ウイルスをネットワーク内に
拡散してしまうおそれがあるため、個人所有のPCや外部記憶媒体等を
社内ネットワークに接続する必要がある場合は、
システム管理者に許可を取ってから接続する。

・パソコン等の画面ロック機能の設定

第三者に見られたり、操作されたりしないようパソコンやスマートフォン等には
画面ロックを設定する。
また、席を離れる際パソコンは画面ロックをかけ、
スマートフォンは放置しないようにする。

9. まとめ

9. まとめ

- 個人情報保護は社会人としての常識
- パートナー社員の個人情報、同僚の個人情報は
  自分の個人情報と同じだけ大切
- 「規則」や「体制」の整備は所詮仕掛け
  各人のコンプライアンス・マインドの向上が重要
- 対象者：社員及びパートナー社員