個人情報保護・情報セキュリティ
教育テキスト

1.個人情報保護の必要性について

１.個人情報保護の必要性について

「個人情報」はプライバシーの一つであり、本人のものです。

- 個人情報が漏洩することにより、悪徳業者に渡り見知らぬ架空請求や、悪質なメールの送信等実害も発生する可能性があります。個人のプライバシーを守ることはもとより、個人情報を適切に取り扱うことは企業として当然の社会的責務なのです。
- **自分の個人情報（氏名、連絡先、学歴、健康状態、給与額等）がずさんな管理をされていて、見ず知らずの人に興味本位で見られていたり、社会に漏洩することで事件やトラブルにあったら！！という意識を持って下さい。**

個人情報は本人の持ち物であり、私共はその持ち物を預かっているに過ぎません。

２.個人情報とは？

2.個人情報とは？

個人情報保護法における個人情報の定義

生存する個人に関する情報であって、当該個人情報に含まれる氏名、生年月日その他の記述などにより特定の個人を識別することができるもの

（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）

2.個人情報とは？

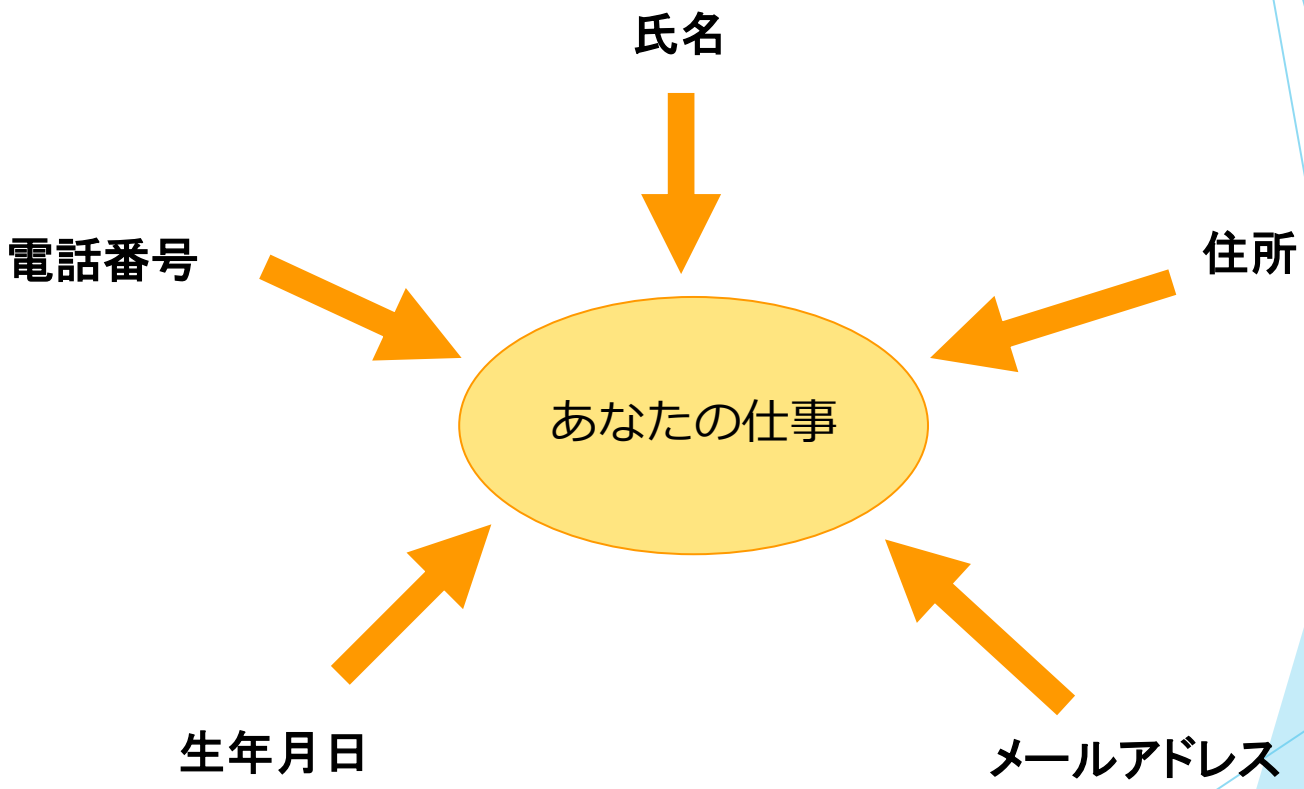
特定の個人を識別できるもの

（例）

- 氏名
- 住所
- 電話番号
- メールアドレス
- 生年月日
- 購買履歴
- ポイントカード番号
- クレジットカード番号
- Suica等の利用履歴
- カーナビなどの移動履歴

2.個人情報とは？

あなたの仕事にも個人情報が含まれている



３．情報資産とは？

3.情報資産とは？

情報資産とは？

極論を恐れずに単純に言うと「組織にとって”大事なモノ”」です。

どういう大事なものが情報資産になるかというと、次の3つの側面から考える事が出来ます。

・機密性（confidentiality）を維持する必要があるもの
・完全性（integrity）を維持する必要があるもの
・可用性（availavility）を維持する必要があるもの

・機密性とは・・・
許可されている人だけが情報にアクセスでき情報が外部に漏洩しないこと
・完全性とは・・・
情報が改ざんされたりせず整合性が取れて完全な状態であること
・可用性とは・・・
システムが安定運用されており必要なときに情報にアクセスできること

４.個人情報保護方針とは

4.個人情報保護方針とは

簡単に言うと、
「個人情報を守っていくために会社でどういったことを
　していくかを示したもの」

個人情報保護方針は、HPに掲載しておりいつでも
見ることができます

個人情報保護方針の内容
a)目的外利用をしませんという内容が書いてある
b)法令を守りますと書いてある
c)事故をした際に二度と起こらないようどう対応するか書いてある
d)苦情相談に対応しますと書いている
e)個人情報保護していくために継続して改善していくことが書いてある

5 .プライバシーマーク、ISO27001認定のメリット

5.プライバシーマーク、ISO27001認定のメリット

- **直接お客様から個人情報を預かる企業では**
  - お客様が安心して個人情報・情報資産を預けていただき、信頼されます。
  - お客様から信頼されます。
- **お取引先企業から個人情報を預かる企業では**
  - 委託、提供先企業としての選定基準をクリアできます。
  - 入札、見積りで排除されにくくなります。
  - コンプライアンス経営企業としてイメージが向上します。
- **どの企業にも共通したメリットは**
  - 社員の個人情報に対する意識が高まります。
  - リスクマネジメントが強化され、情報漏洩等のリスクが低減します。
  - 名刺やパンフレット、ホームページ上でＰマーク・ISO27001のマークが使用できます。

6 .PMSにおける役割と責任

6.PMSにおける役割と責任

個人情報保護体制上の役割	責任
代表者 角屋　守保	当社PMSの最高責任者として、管理責任者、監査責任者を指名し、PMSを実施させる。
個人情報保護管理者 平野　秀忠	当社PMSの統括責任者として、PMSの構築、維持および個人情報取扱いの管理全般について責任を負う。
個人情報保護監査責任者 平野　秀忠	内部監査について規程に従い、全部門の監査を計画、実行し、代表者に報告する。
教育責任者 平野　秀忠	個人情報保護教育について規程に従い、全従業者に対するPMS教育を計画、実行し、個人情報保護管理責任者に報告する。
特定個人情報保護管理者 平野　秀忠	安全管理規程に従い、PMS維持するための特定個人情報の管理について責任を負う。
窓口責任者 平野　秀忠	開示請求や苦情等の問合せ対応全般について責任を負う。

７.個人情報・情報資産の取り扱いによるリスク

７.個人情報・情報資産の取り扱いによるリスク

個人情報・情報資産の管理はなぜ必要なのか？

個人情報・情報資産を有効に活用して事業の拡大に活かす

お客様に安心・信頼して取引を続けていただく

自社事業の継続・発展、社会的な信頼の獲得

したがって・・・

個人情報・情報資産の漏洩等の事故は大きな社会問題に！

7.個人情報・情報資産の取り扱いによるリスク

個人情報・情報資産の取り扱いによるリスク

取扱いの各局面におけるリスク

- 漏洩（外に漏れること）
- 滅失（なくなってしまうこと）
- き損（壊れること、正確でなくなること）

結果として起こるリスク

- 関連する法令，国が定める指針その他の規範に対する違反
- 想定される経済的な不利益及び社会的な信用の失墜
- 本人への影響などのおそれ

7.個人情報・情報資産の取り扱いによるリスク

なぜこういったリスクが起こるのか？

ほとんどが規則を守らないことによる事故

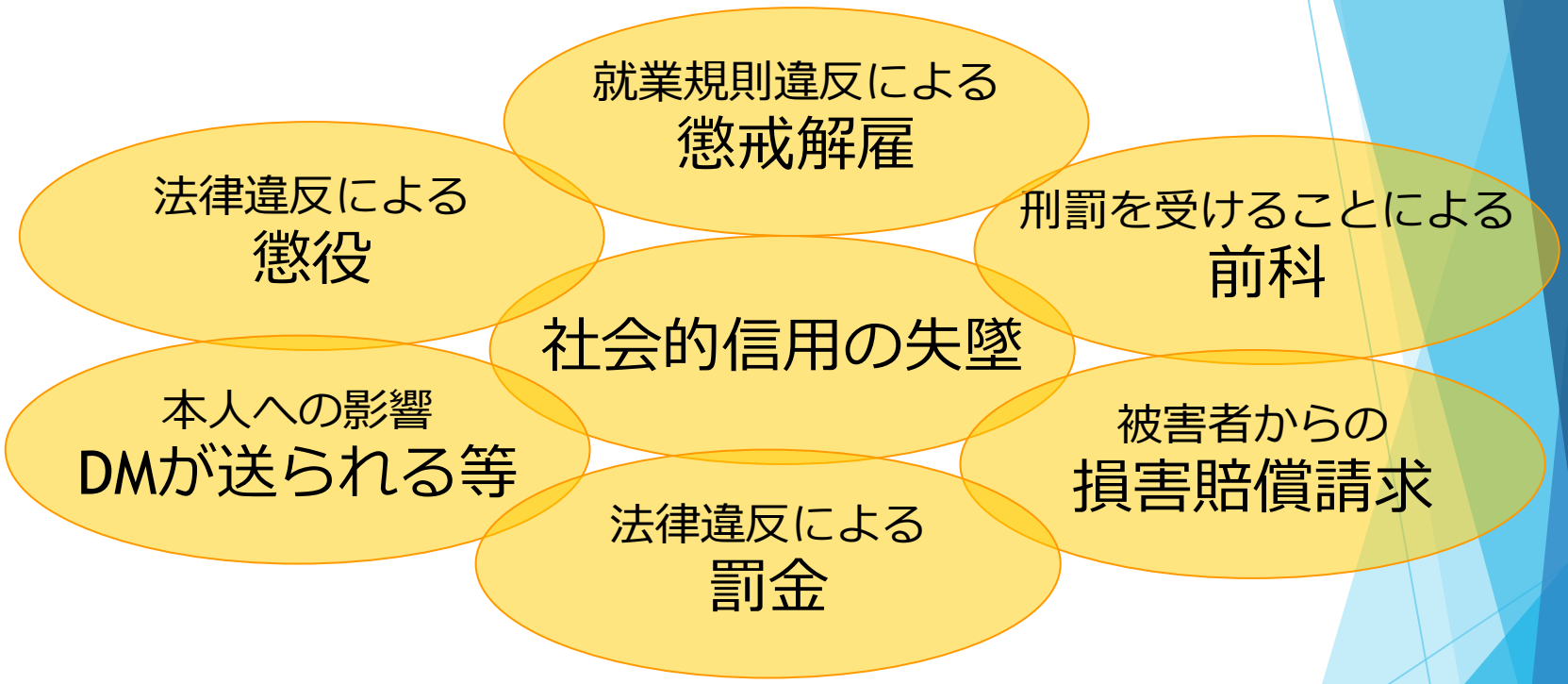
例1）仕事が間に合わないから自宅で続きをしよう、と規則を無視してノートパソコンを持ち帰り、途中で置き忘れてきてしまった。

例2）USBメモリに顧客情報を無断で写していたものをうっかり紛失してしまった。

例3）個人情報が入っているパソコンにも関わらず、ウィニー（winny）等のファイル共有ソフトをインストールして使用し、ソフトを通じて情報が流出してしまった。

７.個人情報・情報資産の取り扱いによるリスク

もし事故を起こしてしまったら？



あなたや会社にこんなことが降りかかってくるかもしれません。

7.個人情報・情報資産の取り扱いによるリスク

- 個人情報の取扱いに関する事故の傾向
  - JIPDEC公表の統計資料
    2022年度「個人情報の取扱いにおける事故報告集計結果」

直近で発生した実際の個人情報の事故事例を見てみましょう

事例 ①

酒に酔って約46万人分の個人情報記録したUSB紛失、尼崎市受託企業

兵庫県尼崎市は2022年6月23日、住民税非課税世帯に対する臨時給付金支給事業の受託事業者の関係者が、市から持ち出した全市民約46万人等が記録されたUSBメモリを外部に持ち出し、立ち寄った飲食店で酒に酔って紛失したと明らかにしました。
委託会社は2022年6月22日、受託業務のためデータ移管作業を進めようと尼崎市市政情報センターから住民基本台帳データなどを記録したUSBメモリを持ち出したとのこと。尼崎市は受託者に委託者以外の事業所でのデータ処理の許可を与えていましたが、具体的な持ち出し方法について許可を得ていなかったとしています。
情報を持ち出した社員はデータ移管作業完了後、帰宅前に飲食店に立ち寄り、酒を飲むなどの行為に及びました。しかし、帰宅の際にUSBメモリを収納したカバンの紛失を確認。
受託者より報告を受けた尼崎市は事実を公表しました。

■今後の対策

①データを外部に持ち出す際は方法について許可を得るよう徹底するよう求める
②外部持ち出しの際はセキュリティ便の活用など安全性の高い運搬方法を用いる
③個人情報保護の重要性について周知徹底する

直近で発生した実際の個人情報の事故事例を見てみましょう

事例 ②

ハードオフアプリに不正アクセス、6,186件の登録情報流出の可能性（ウイルス感染）

株式会社ハードオフコーポレーションは2022年8月13日、同社が提供する「ハードオフ公式アプリ」に対する外部からの不正アクセスがあり、ユーザーアカウント6,186件の登録情報が流出した可能性があると明らかにしました。
2022年8月9日に特定のIPアドレスから、複数のアカウントに対するログイン試行が発生しました。同社は2022年8月11日に事態を把握し、システムを緊急停止した後、全アカウントのパスワードリセットを実施するなどのセキュリティ対策を講じましたが、既に不正アクセスを受けたアカウントについて、登録情報が閲覧された可能性があるとのこと。
同社はこのため、2022年8月13日に事態を公表。被害が懸念されるユーザーについて個別に連絡を取り、事態を説明するとしています。不正アクセスの対象となっているのはEメールアドレスとログインパスワードでアプリ登録していたユーザーであるため、これらも流出した可能性があるとのことです。

■今後の対策

①安全が確認できないWebサイト上で個人情報を入力しない
②セキュリティソフトを導入・更新する
③定期的にパスワードを変更する
④「二要素認証」（2FA）が提供されている場合はできる限り使用する

直近で発生した実際の個人情報の事故事例を見てみましょう

事例 ③

テレワーク環境でマルウェア感染、社内に拡大（三菱重工）

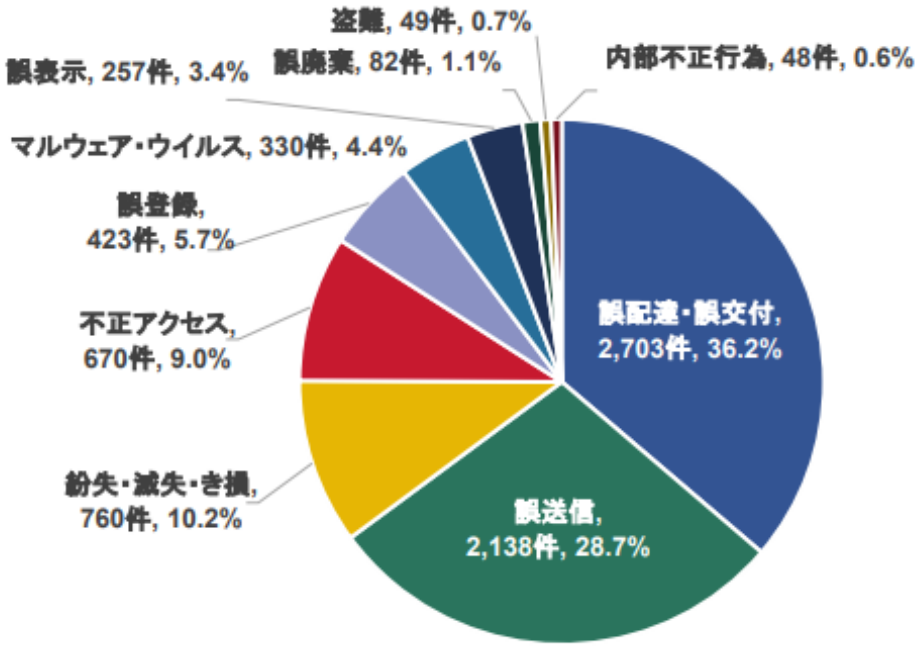
三菱重工業は、2020年4月29日にテレワークで利用した業務用端末がSNSの利用を通じて同社グループの従業員が在宅勤務を行った際、業務用モバイルパソコンから社内ネットワークを経由せずSNSを利用したところ、ソーシャルエンジニアリングによって第三者から受信、ダウンロードしたファイルからパソコンやサーバなどがマルウェアに感染し、その後外部より不正アクセスを受けて同社グループの従業員の氏名やメールアドレスなど個人情報のほか、通信パケット、サーバのログ、設定情報などが流出した。
さらに同従業員が、2020年5月7日に出社してパソコンを社内ネットワークに接続したところ、2020年5月18日よりマルウェアの感染が内部ネットワークに拡大。同地区の一部サーバにおいて、ローカル環境の特権アカウントに同じパスワードが設定されており、特権アカウントを悪用することで他機器にログインし、影響が広がったものと見られている。

■今後の対策

①特権アカウントのパスワードをすべて異なるものへ変更する
②強制的にVPN経由で社内ネットワークを経由するよう変更する
③VPN機器へ接続しない限りインターネットに接続できない仕組みを導入し社内と同等のセキュリティ対策を適用する
④多要素認証を導入し、もしID/パスワードが漏洩した場合でも容易に不正アクセスできないようにする
⑤脆弱性に関する情報を収集し、対策として配布されるセキュリティパッチの適用を徹底する

漏洩事故の分析、傾向

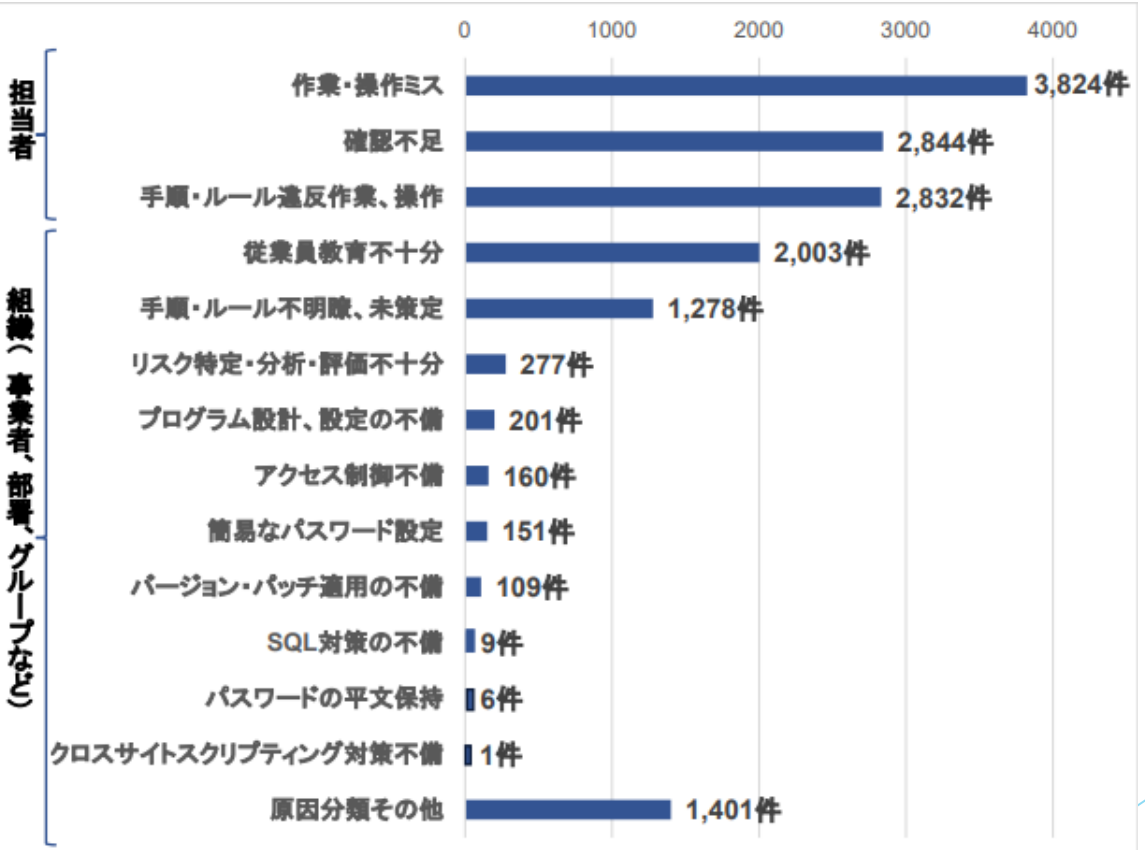
事象分類別事故報告件数



出典（リンク）：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

漏洩事故の分析、傾向

原因別集計

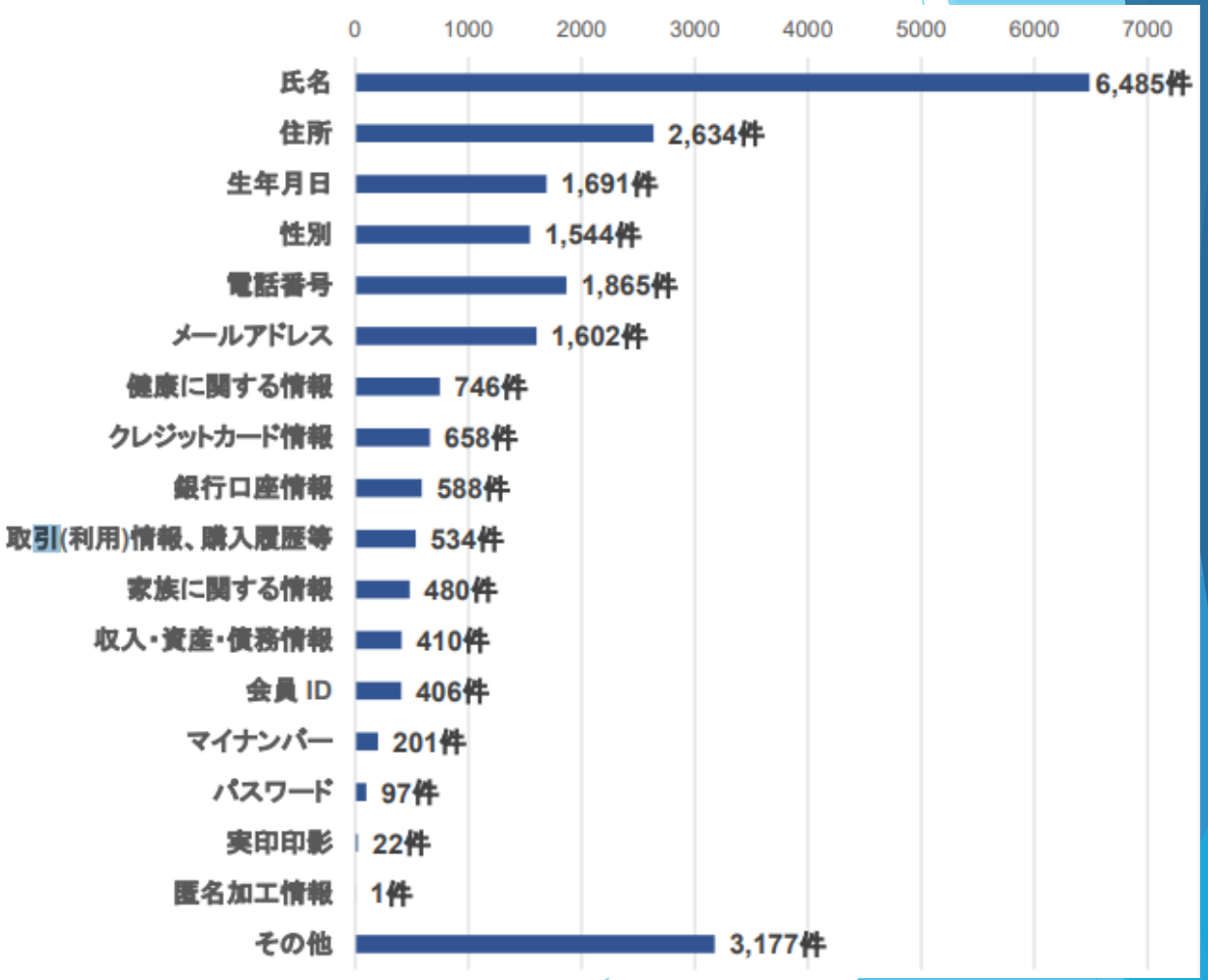


原因別には「作業・操作ミス」が3824件、続いて「確認不足」2844件、「手順・ルール違反作業」が2832件と担当者が適切な作業を実施しなかったことによる事故が多く発生した。

出典：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

漏洩事故の分析、傾向

事故報告の項目別の集計



出典：（2023年度）「個人情報の取扱いにおける事故報告集計結果」

7.個人情報・情報資産の取り扱いによるリスク

インターネットを介した事故事例と防止策例

- 事故のパターンと事例

作業ミス	ID/パスワードの漏えい	設定ミス
•A社のデータを、誤ってB社のオンラインストレージにアップロードした •Webサイト更新時、公開用フォルダに一時的に移動した個人情報が含まれるデータを削除し忘れた	•会員Cに対し、会員D用のID/パスワードをメールで送信した •E社にF社用の取引先ページのID/パスワードを送信した	•クラウド上での作業時、取引先従業員情報の非公開設定を失念した •Webサイトのアクセス制限設定を誤り、個人情報が掲載されたページが閲覧できる状態となった

- 防止策例

手順やルールの見直し	具体的な手順等の工夫	注意喚起・教育	委託先の管理
•適切な業務運営やガバナンス体制の構築、 •作業実施ルール・チェックルールの確認、見直し など	•二重チェック体制の構築 •新たな手順の導入 など	•教育方法、実施時期、内容の見直し など	•定期的なモニタリング、監査の実施 など

7.個人情報・情報資産の取り扱いによるリスク

内部不正行為による事故事例と防止策例

- 事故のパターンと事例

従業者によるもの	退職者によるもの	委託先によるもの
•人事情報を他部署の従業者が無断で持ち出した •営業担当者が顧客になりすまし、代金の払い戻しを受けた	•元社員が顧客データを持ち出し転職先での営業活動に利用した •元社員が顧客名簿を持ち出し、他の事業者に転売した	•委託先の従業者が自宅で作業するため、個人データを持ち出した •委託先従業者が委託元の社員名簿を持ち出し社員に迷惑メールを送った

- 防止策例
  - データ管理状況の見直し
  - 端末や社内システムへの接続制限
  - 退職者に係る取扱いルール見直し（秘密保持契約締結、迅速なID削除等）
  - 注意喚起・教育

7.個人情報・情報資産の取り扱いによるリスク

その他日常業務での事故事例と防止策例

- 事故のパターンと事例

口頭での漏洩	盗難・紛失
•電話での本人確認が不十分だったため、本人と誤認して別人に個人情報を教えた •誤って別人のログインID等を伝えた	•携帯電話、スマホの紛失が増加

- 防止策例
  - 対応ルール・手順の確認・見直し
  - 従業者への注意喚起・教育

８.あなたにできることは？

8.あなたにできることは？

あなたにできることは？

- 規則を守る事

- 危ないと思ったら報告する事

個人情報を漏洩しない為にできること

～規則を守ること～

ちょっとの気の緩み、これくらいならいいか…　から事故は発生します。
この教育を機会に、実際に下記の項目が守れているか確認してみましょう。

事務所編

☑一番最初に事務所についた人、最終退出者は時間等の記録を残しているか？
☑来訪者が事務所に入る場合は「来訪者記録」等を書いてもらっているか？
☑印刷したものは複合機に置いたままにせずに、すぐ回収しているか？
☑クリアデスクになっているか、名刺などを机に置いたまま離席していないか？
☑デスクに個人情報やPCのパスワードなど付箋が貼ってないか？
☑個人情報が記載されている紙をシュレッダーにかけ、廃棄しているか？

PC編

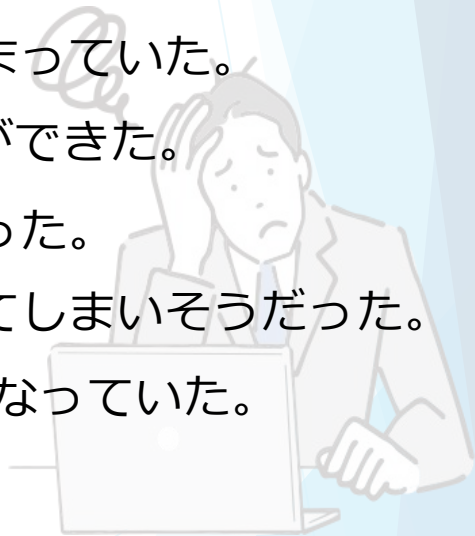
☑PCのパスワードは半角英数ルール通りに設定されているか？
☑スクリーンセーバーはルール通りにで設定されているか？
☑ウイルス対策ソフトが入っているか？
☑OSのアップデートは最新または会社から指示されているバージョンか？
☑業務に使わない、不要なアプリがダウンロードされていないか？
☑社用PCに私物のスマートフォンを接続していないか？
☑許可なく、PC、USBメモリを家に持ち帰っていないか？

個人情報を漏洩しない為にできること

～報告・連絡・相談～

事故ではないからと軽視をせず、危ないと思ったことを報告・連絡・相談を行うことで、本当に起きてはならないような、大きな漏洩事故を未然に防ぐことに繋がります。

・アドレス帳から違う人のメールアドレスを選択してしまっていた。
・FAX番号を押し間違えていたが、送信前に気づくことができた。
・電車を降りる時にノートパソコンを置き忘れそうになった。
・個人情報の書かれた紙の裏を使った後、ゴミ箱に捨ててしまいそうだった。
・メールを送る時のBCC欄とCC欄を間違えて送りそうになっていた。



9.まとめ

9.まとめ

・他人事ではなく、皆さんがお仕事される中で、**一人一人の会社の定めたルールを守ろうという意識が、情報漏洩事故を防ぐ**ことになります。

・何か疑問や、少しでも不安・怪しいと感じた事象があれば、そのままにするのではなく**すぐに上司に報告**をするようにしましょう。

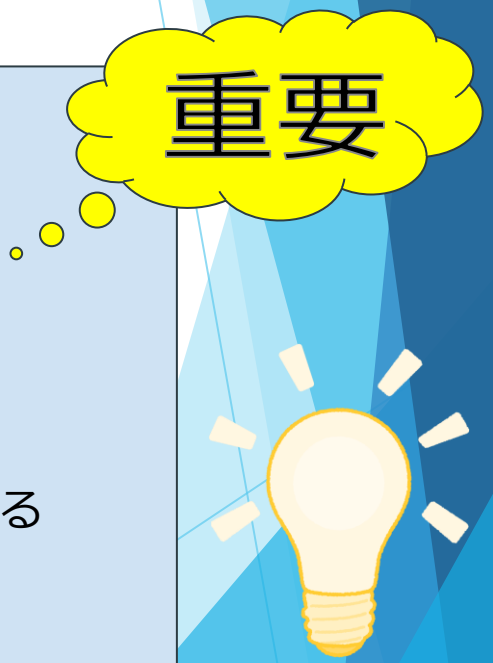
重要な4つのポイントを復習しましょう。（規格要求事項）

1．**個人情報保護方針**
　⇒個人情報を守っていくために会社で決めた指針

2．**Pマークを取得することへの重要性及び利点**
　⇒お客様が仕事を依頼する際の選定基準をクリアできる

3．**Pマークを運用するにあたり、役割及び責任**
　⇒Pマークの運用には、個人情報保護管理者等の役割を決める

4．**漏洩事故を起こした場合に予想される結果**
　⇒社会的信用の失墜、減給、解雇



補足資料

IPA情報セキュリティ10大脅威2025

情報セキュリティ10大脅威 2025 [個人]

「個人」向け脅威 （五十音順）	初選出年	10大脅威での取り扱い （2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	6年連続9回目
インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
クレジットカード情報の不正利用	2016年	10年連続10回目
スマホ決済の不正利用	2020年	6年連続6回目
偽警告によるインターネット詐欺	2020年	6年連続6回目
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
フィッシングによる個人情報等の詐取	2019年	7年連続7回目
不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続7回目
ワンクリック請求等の不当請求による金銭被害	2016年	3年連続5回目

個人の10大脅威の順位は掲載せず、五十音順で並べています。これは、順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念してのことです。

https://www.ipa.go.jp/security/10threats/10threats2025.htmlより抜粋

IPA情報セキュリティ10大脅威2025

▲ 情報セキュリティ10大脅威 2025 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）	前年順位
1	ランサム攻撃による被害	2016年	10年連続10回目	1
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目	2
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目	5、7
4	内部不正による情報漏えい等	2016年	10年連続10回目	3
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目	4
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目	9
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出	圏外
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目	圏外
9	ビジネスメール詐欺	2018年	8年連続8回目	8
10	不注意による情報漏えい等	2016年	7年連続8回目	6

https://www.ipa.go.jp/security/10threats/10threats2025.htmlより抜粋