

令和7年度医療情報セキュリティ研修 及び  
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

## 【初学者等向け研修】 SNSセキュリティ管理コース

# 誰もがしっかり管理すべき個人情報と SNSの業務利用に関するセキュリティ

2025年10月16日  
一般社団法人ソフトウェア協会

## 目次

- ◆ 個人情報の管理について
  - ・ 個人情報保護法とは
  - ・ 情報漏えい時に必要な対応
- ◆ SNSの適切な利用について
  - ・ 実際のSNSによる漏えい事例
  - ・ 承認されていないITの利用

## 目的

- ◆ 個人情報の取り扱いに関する基本的なルールを正しく理解し、個人情報の管理を自分事として考えられるようになること
- ◆ SNSを利用する際に、安易な投稿ややり取りが情報漏えいにつながる危険があることを理解し、安全で適切な利用を意識できるようになること

## 個人情報の管理について

## 実際の情報漏えい事例

### ■ 国分生協病院

#### 鹿児島県の国分生協病院、ランサムウェア攻撃受け診療記録PDFの一部アクセスできず

鹿児島県鹿児島市にある国分生協病院は2024年2月4日、ランサムウェア（身代金要求型ウイルス）によるサイバー攻撃を受け、「画像管理サーバー」に障害が発生していると発表した。ファイルの一部が暗号化されアクセスできなくなっている。現時点で個人情報漏えいは確認されていない。

同月2月27日深夜から画像管理サーバーの正常な運用ができなくなっている。具体的には同サーバー内の、診療記録のPDFファイルの一部が暗号化されアクセスできない状態だ。詳細は現在調査中とした。同病院によると被害の範囲は、保守目的のインターネット接続回線を介し、接点となる院内設置ネットワーク機器で、認証なしで外部から病院のコンピューターにリモートデスクトップ接続が可能に設定が存在したことだ。また、画像管理サーバーにはウイルス対策ソフトが設定されていなかった。

現在、電子カルテや医療会計などは正常稼働しているという。予的外傷と入院患者については電子カルテで対応し、検査と一般外来は受け入れを制限しながら診療している。病院全体でインターネット接続を停止しており、現時点で再接入や再攻撃はないという。被害者から身代金の具体的な要求はなく、支払いや交渉はしない方針だ。

出典：日経XTECH (<https://xtech.nikkei.com/atcl/nxt/news/24/00350/>)

#### 概要

2024年2月、国分生協病院がランサムウェア攻撃を受け、画像管理サーバーに障害が発生。

画像管理サーバー内の診療記録のPDFファイルの一部が暗号化され、「**対応が必要な事態**」に該当することから、**個人情報保護委員会への報告**を行いました。

## 実際の情報漏えい事例

### ■ 岡山県精神科医療センター

#### 岡山県精神科医療センター、ランサムウェアで最大約4万人分の患者情報流出の恐れ

岡山県精神科医療センターは2024年6月11日、3月に公表したランサムウェア攻撃による総合情報システムの障害で、最大約4万人分の患者情報が流出した可能性があることを発表した。6月7日に岡山県本部で、同センターの保有する患者情報の流出を確認したという。

流出した可能性があるのは、総合情報システムで職員が業務で作成した資料を保存していた共有フォルダ内の情報という。最大約4万人分の、患者の氏名や性別、生年月日、病歴などのほか、精神科医の診療録などが含まれるとしている。

岡山県精神科医療センターは2024年5月19日午後4時ごろから同センターと診療所の電子カルテを含む総合情報システムがダウンし、翌20日までに県や県警、厚生労働省に連絡。同月21日にランサムウェアとみられるサイバー攻撃が原因だと特定したと公表していた。22日には個人情報保護委員会に報告した。

同センターは「電子カルテのセキュリティ対策への管理監督が十分でなかったためにこのような事態を招き、これまでお断りいただいた皆様を憂慮することになった」と患者や家族らへの謝罪を公表している。

出典：日経XTECH (<https://xtech.nikkei.com/atcl/nxt/news/24/00969/>)

## 実際の情報漏えい事例

#### 概要

2024年5月、岡山県精神科医療センターがランサムウェア攻撃を受け、電子カルテを含む総合情報システムに障害が発生しました。

この被害により、総合情報システム内の共有フォルダに保存していた**最大約4万人分の患者情報が流出し、個人情報保護委員会への報告**を行いました。

## 漏えいの可能性がある情報

2つの医療機関で漏えいした情報は何かを見てみましょう。

### ■ 国分生協病院

- **患者の医療画像**（X線、CT、MRI等）
- **患者の個人情報**（氏名、診療内容、診断結果等）

### ■ 岡山県精神科医療センター

- **患者の個人情報**（氏名、住所、生年月日、病名等を含む最大40,000人分）
- **病棟会議の議事録等**（医療スタッフ間の議論内容や患者対応に関する記録）

このような情報が漏えいした可能性があったため、**個人情報保護委員会への報告**を行いました。

## 医療機関で情報漏えいが起こった場合の影響

情報漏えいが起こった場合にどのような影響があるのでしょうか。

### 患者への影響

- 要配慮個人情報の漏えい
- 不利益や差別の可能性
- 病院への不信感

### 医療機関への影響

- 信用の損失
- 診療の停止や医業収入の減少
- 法的・行政的リスク

### 職員への影響

- 過度な労働
- 精神的な負担
- 職場への影響

# 個人情報保護法とは

## 個人情報保護法とは

個人情報保護法とは、**個人情報の有用性に配慮しながら、個人の権利・利益を保護することを目的とした法律**で、個人情報を扱うすべての事業者が対象となります。

### 個人情報の定義

- 特定の個人を識別できるもの（氏名・生年月日・身体データ 等）
- 個人識別符号が含まれるもの

#### 特定の個人を識別できるもの



#### 個人の身体データ



#### 個人識別符号が含まれるもの



中でも、特に慎重な取り扱いが求められる情報があります。➡

## 特定個人情報とは

特定個人情報とは、**マイナンバー（個人番号）を含む個人情報**のことです。

### 特定個人情報に該当する情報

- 個人番号（マイナンバー）
- 個人番号と紐づいた氏名、住所、生年月日などの情報

### 特定個人情報と個人情報の主な違い

項目	特定個人情報	個人情報、個人データ
利用目的	「税・社会保障・災害対策」限定	利用制限なし
不要時の情報の取り扱い	所管法令で定められている保存期間を経過した場合には、できるだけ速やかに廃棄または削除しなければならない	遅滞なく消去するよう努めること
第三者提供	第三者提供可能な場合が限定	第三者提供可能（本人の同意あり）

<https://www.ppc.go.jp/legal/policy/>

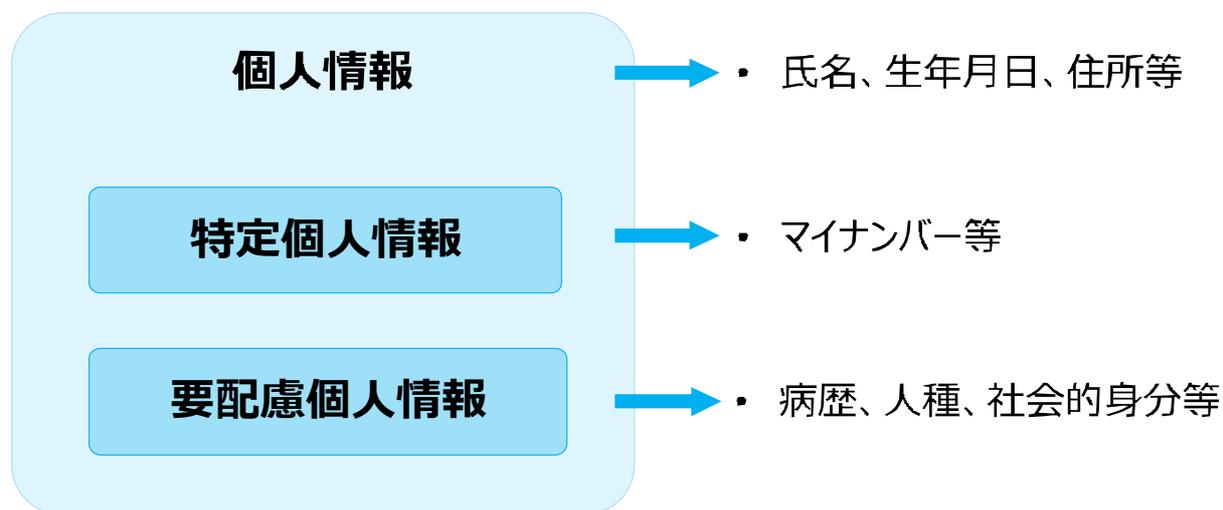
## 要配慮個人情報とは

要配慮個人情報とは、**他人に公開されることにより、本人が不当な差別、偏見などの不利益を被らないよう、取り扱いに特に配慮すべき情報**のことです。

例	医療機関でよく扱う情報例
<ul style="list-style-type: none"> <li>• 社会的身分</li> <li>• 病歴</li> <li>• 身体・知的・精神障害</li> <li>• 人種・民族</li> <li>• 犯罪歴</li> <li>• 健康診断等の検査結果</li> <li>• 調剤情報</li> </ul> <p>など</p>	<ul style="list-style-type: none"> <li>• <b>病歴、診療記録</b> → 健康状態が漏れると、差別や偏見の原因になるため</li> <li>• <b>障害に関する情報</b> → 社会的な偏見や不利益につながりやすいため</li> <li>• <b>妊娠・出産・不妊治療などの情報</b> → 個人のライフイベントに直結し、プライバシーへの影響が大きい</li> <li>• <b>遺伝情報</b> → 将来の病気リスクや家族情報を推測され、不利益を受けやすいため</li> </ul> <p><b>医療機関では、このような「差別・偏見・社会的不利益」に直結する情報を特に慎重に扱う必要があります。</b></p>

## それぞれの位置づけ

個人情報、特定個人情報、要配慮個人情報の位置づけはこのとおりです。



## 情報漏えい時に必要な対応

## 漏えいした（可能性がある）場合に必要な対応

個人情報が漏えいした場合には、どのような対応が必要なのでしょうか？

▼個人情報保護委員会によると

個人データの漏えい等が発生し、**個人の権利利益を害するおそれがある場合**は…

**個人情報保護委員会  
への報告**

+

**本人への通知**

が必要となります。

以前まで

- ・ 個人情報保護委員会への報告 → **努力義務**
- ・ 本人への通知 → **推奨**

令和4年の個人情報保護法改正後

- ・ **どちらも義務化**

## 個人情報と個人データの違い

なぜ「個人データ」と表現されているのでしょうか？

### 個人情報



- ・ 氏名
- ・ 住所
- ・ 電話番号

### 個人データ



- ・ 整理・検索できる
- ・ 名前、住所、電話番号
- ・ 名簿やデータベース



個人情報 = 人を特定できる情報そのもの  
個人データ = その中で「整理・検索できる状態」にした情報

報告が必要なのは、  
「影響が大きい、組織的に管理している情報」

### 例

- ・ 患者に関するメモ書きが1枚、棚の中から無くなった  
→ **個人情報の漏えい（報告義務なし）**
- ・ 電子カルテのデータベースが外部に流出した  
→ **個人データの漏えい（報告義務あり）**

## 個人情報漏えいした（可能性がある）場合に必要な対応

それぞれのルールについて見ていきましょう。

### 個人情報保護委員会 への報告

#### 報告期限

- **速報**（新規）  
発覚した日から**3～5日**以内
- **確報**（続報）  
発覚した日から**30日**以内  
※不正アクセス等のおそれがある場合は  
60日以内

### 本人への通知

#### 通知方法の例

- **文書の郵送**
- **電子メールの送信**  
※通知が困難な場合は、次の代替措置も可能
  - ホームページ等での公表
  - 問い合わせ窓口の設置

## 個人情報漏えいした（可能性がある）場合に必要な対応

「個人の権利利益を害するおそれがある場合」に該当する事態はどのようなものでしょうか。

	事態	例
1	要配慮個人情報が含まれる事態	患者の診療情報などを含む個人データを保存したUSBメモリを紛失した場合
2	財産的被害が生じるおそれがある事態	送金・決済機能のあるサービスのログインID・パスワードを含む個人データが漏えいした場合
3	不正の目的をもって行われた漏えい等が発生した事態	ランサムウェア等により、個人データが暗号化され復元できなくなった場合
4	1,000人を超える漏えい等が発生した事態	メール送信時に、メールアドレスを誤ってCC欄に入力し、1000人以上に一斉送信した場合

## 個人情報が漏えいした（可能性がある）場合に必要な対応

「個人の権利利益を害するおそれがある場合」に該当する事態はどのようなものでしょうか。

	事態	例
1	要配慮個人情報が含まれる事態	患者の診療情報などを含む個人データを保存したUSBメモリを紛失した場合
2	財産的被害が生じるおそれがある事態	送金・決済機能のあるサービスのログインID・パスワードを含む個人データが漏えいした場合
3	不正の目的をもって行われた漏えい等が発生した事態	ランサムウェア等により、個人データが暗号化され復元できなくなった場合
4	1,000人を超える漏えい等が発生した事態	メール送信時に、メールアドレスを誤ってCC欄に入力し、1000人以上に一斉送信した場合

**1～3は、1件でも漏えいした可能性がある場合は対応が必要になります。**

## SNSの適切な利用について

SNS利用

個人情報の管理

きちんとルールを守って  
利用しているか？



どのような危険があるか  
意識できているか？

## SNS利用におけるリスク

患者情報の漏えい

医療機関の信用低下

法的責任の発生

職員本人への不利益

SNSに投稿した写真や文章には、患者の名前や病状などが含まれることがあります。たとえ直接名前を書いていなくても、状況や特徴から患者が推測されることがあります。



今日から入院してる  
〇〇病の患者さん、  
まさかの同じ年だった〜

職員の投稿は、個人のもので「病院の姿勢」として受け止められやすいです。不適切な発言や軽率な投稿は、患者や地域社会からの信頼を失うおそれがあります。



## SNS利用におけるリスク

患者情報の漏えい

医療機関の信用低下

法的責任の発生

職員本人への不利益

SNSでの情報公開が、個人情報保護法等の法律に違反し、行政指導や処分を受ける可能性や、裁判や損害賠償に発展することもあります。



不用意な投稿は就業規則に違反してしまう場合があります。たとえ匿名でも、投稿内容から本人が特定され、社会的信用や職業的立場を失う危険があります。

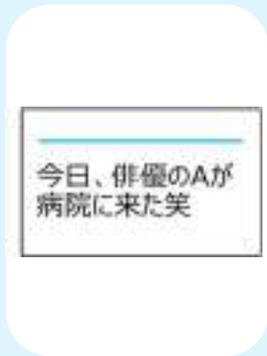


## どのように情報が漏えいするのか？

SNSにおいて、どのような使い方で情報が漏えいするのでしょうか？



写真や動画に患者情報が映り込む



患者の病状や来院事実を記載する

## どのように情報が漏えいするのか？

SNSにおいて、どのような使い方で情報が漏えいするのでしょうか？



**愚痴やエピソード投稿で個人が特定される**



**勤務先を公開したうえで投稿する**

## これって投稿して大丈夫？

どのような投稿が問題なのかを判断できますか？

今日忙しすぎた・・・  
仲間のおかげで何とか乗り切れた > <



**OK**

特定の名前や病院名などを特定できる情報がなければ問題なし

〇〇市の事故で救急外来やばすぎる



**NG**

患者数や出来事を特定でき、地域や病院の対応状況が漏れる可能性

## これって投稿して大丈夫？

どのような投稿が問題なのかを判断できますか？

今日、あのモデルが皮膚科に来て、まさかの自分が対応しちゃった！きれいだった～



**NG**

名前を伏せていても、病院や診療科で特定される可能性

夜勤明けであまりにも眠い……



**OK**

業務内容や患者情報に触れていないので問題なし

## (参考) 守秘義務について

医療資格を持つ職員

資格を持たない職員

個人情報保護法

資格関連法令

就業規則・雇用契約

## (参考) 守秘義務について

医療資格を持つ職員は、法律により患者の個人情報適切に取り扱うことを定められています。

### 刑法第134条第1項

「業務上知り得た秘密を漏らしてはならない」

→医師、薬剤師、助産師等に適用

### 保健師助産師看護師法第42条の2

「正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない」

→保健師、看護師、准看護師に適用

資格名	根拠法
医師	刑法第134条第1項
歯科医師	刑法第134条第1項
薬剤師	刑法第134条第1項
保健師	保健師助産師看護師法第42条の2
看護師	保健師助産師看護師法第42条の2
准看護師	保健師助産師看護師法第42条の2
理学療法士	理学療法士及び作業療法士法第16条
歯科衛生士	歯科衛生士法第13条の5
...	

守秘義務は「約束」ではなく、法律で定められた「責任」です。

## (参考) 守秘義務について

医療資格を持たない職員も、一般的に就業規則や雇用契約で守秘義務が規定されています。

### ■ 就業規則・雇用契約の例

第x条 職員は業務上知り得た秘密を他に漏らしてはならない。  
ただし、法令に基づく証人又は鑑定人等として、理事長の許可を受けた場合はこの限りではない。

2 前項の規定は、退職又は解雇された後においても適用する。

第x条 職員は、次に掲げる行為をしてはならない。  
・職務上知り得た秘密を他に漏らすこと。

参考 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス  
[https://www.ppc.go.jp/personalinfo/legal/iryokaigo\\_guidance/](https://www.ppc.go.jp/personalinfo/legal/iryokaigo_guidance/)

医療職と同等の守秘義務が規定されているため、責任を持つ必要があります。

## (参考) 守秘義務について

過去にこんな事例がありました。



2020年3月、名古屋大学大学院医学系研究科の学生が、名古屋大学医学部付属病院の患者2名の電子カルテ写真（氏名や入院診療科名等を含む）等をSNSに投稿し、情報漏えいとなりました。

学生が研修等により院内に入ることがある際には、**法的な制限があることを理解していない**場合があるため、注意が必要です。

引用：読売新聞 (<https://www.asahi.com/articles/ASS6K1Q9KS6KOIPE00JM.html>)

## 実際のSNSによる漏えい事例

# SNS利用に関する実際の事例 1

## ◆ 仙台市立病院



引用：NHK (<https://www3.nhk.or.jp/news/sendai/20240524/6000027637.html>)

概要

投稿理由

影響

病院の対応

概要

2024年5月、仙台市立病院に勤務する管理栄養士が、スマートフォンで撮影した患者1名のカルテ画像を自身のInstagramに投稿し、情報漏えいが発覚。投稿は約1か月間外部から閲覧可能になっていました。

# SNS利用に関する実際の事例 1

事例の詳細をシナリオでご紹介します。

1. ある日、管理栄養士の佐藤さんは、休憩中に患者の電子カルテを私用のスマートフォンで撮影しました。

2. 佐藤さんは、撮影した電子カルテの画像を、私用のInstagramアカウントに「業務メモ」として投稿。

3. 約1か月後、外部のSNS利用者が佐藤さんの投稿を発見し、病院に連絡。問題が発覚しました。

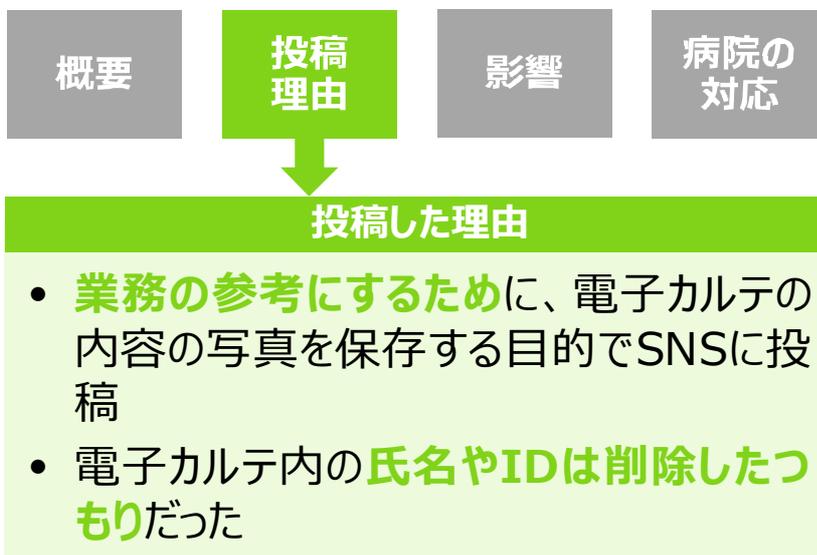
4. 佐藤さんはすぐに投稿を削除しましたが、1か月の間、外部から患者の個人情報が見られる状態になっていました。

# SNS利用に関する実際の事例 1

## ◆ 仙台市立病院



引用：NHK (<https://www3.nhk.or.jp/lnews/sendai/20240524/6000027637.html>)

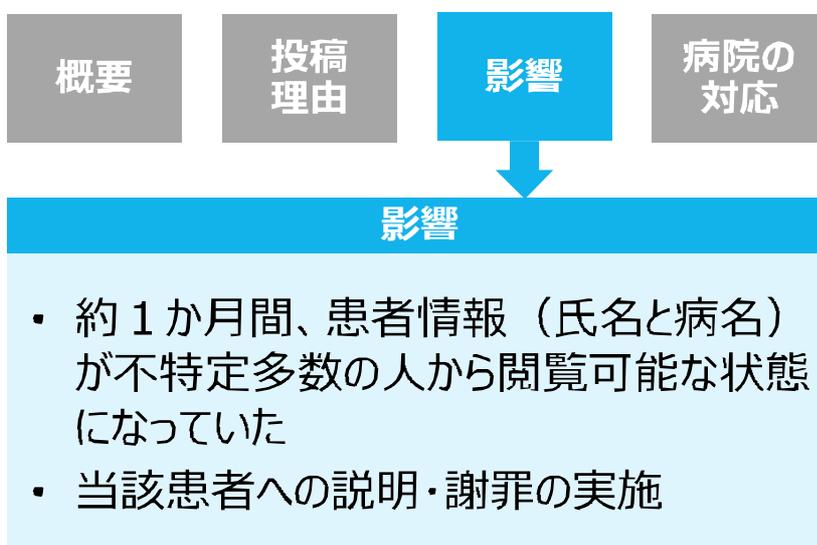


# SNS利用に関する実際の事例 1

## ◆ 仙台市立病院



引用：NHK (<https://www3.nhk.or.jp/lnews/sendai/20240524/6000027637.html>)





## SNS利用に関する実際の事例 2

事例の詳細をシナリオでご紹介します。

1.

佐藤さんは、ある皮膚の病気を患い、X病院に通院しています。カルテには詳細なデータが記録されていました。

2.

ある日、X病院の小児科医である山田さんが、佐藤さんのカルテを不正に閲覧。LINEで佐藤さんの娘に送信しました。

3.

佐藤さんは娘に病気の事実を伝えていなかったため、山田さんの情報共有が原因で、娘に知られることとなりました。

4.

その後、佐藤さんは、守秘義務違反・プライバシーの侵害を主張し、病院と山田さんに損害賠償を請求しました。

## SNS利用に関する実際の事例 2

### ◆ 堺市立総合医療センター

カルテ漏洩で損害賠償へ 70代女性 堺市医療センターと医師

堺市立総合医療センター（堺市堺区）の女性小児科医が、医師士会審判官にも関わらず医療関係者の個人情報を知り、勝手に画像（顔写真）したために裁判的損害を受けたとして、医療センターと医師の70代女性が、センターの運営法人と医師を相手取り、計330万円の損害賠償を求め訴訟を大法院地裁に起こすことが24日、分かった。24日には開廷する。

裁判によると、女性は画像が撮れるといった意味が解れる「肉撮り」を敷いた。平成29年12月23日、同センターの診療科へ通った。小児科医は、自分の職務と関係がないと関わらず、女性の病状や治療経過の記録を盗んだと主張。女性の娘がLINEで一斉的に語り分け、女子情報も勝手に漏らしたという。女性は病気が起ると考え、病院の事実を伝えていなかった。

彼女と小児科医の縁は、ゆるい「ママ友」関係だったが、画像漏洩は縁戚になっていた。

当該で被告側は、当該医の行為は、守秘義務の範囲や個人情報の取扱いとされた病院の管理方針に反すると認め、小児科医を相手とする訴訟面にも被害者側が主張した。

引用：産経ニュース (<https://www.sankei.com/article/20210224-5FHIXDMPJMMNCLHTL4AIHVZU4/>)



### 背景

小児科医の女性医師と被害者の娘は、かつての「ママ友」で、この時は疎遠になっていましたが、連絡先を持っており、医師が勝手に被害女性の病状等を娘に連絡しました。

## SNS利用に関する実際の事例 2

### ◆ 堺市立総合医療センター



引用：産経ニュース (<https://www.sankei.com/article/20201224-5FHIXDMPJMMNCLHTL4AIHVZU4/>)



### 裁判の結果

被害女性は精神的な苦痛を受けたため、330万円の損害賠償を求め、裁判の結果約5万5千円の支払いが命じられました。  
(情報閲覧は一度のみ、漏えい相手が被害者の娘だったためこの額になりました)

## SNS利用に関する実際の事例 2

### ◆ 堺市立総合医療センター



引用：産経ニュース (<https://www.sankei.com/article/20201224-5FHIXDMPJMMNCLHTL4AIHVZU4/>)



### 学び

- たとえ家族等の知人でも、本人の同意なしに情報を伝えてはいけない
- 場合によっては慰謝料が発生する可能性も

# SNS利用に関する実際の事例 3

## ◆ 千葉大学附属病院



引用：NHK (<https://www3.nhk.or.jp/shutoken-news/20250108/1000112859.html>)



**概要**

2025年1月、看護師とみられる人物の「X」での投稿が話題となりました。内容は、患者に不適切な処置をしたことや、職員・患者への愚痴等で、千葉大学附属病院の関係者による投稿ではないかと指摘されました。

# SNS利用に関する実際の事例 3

事例の詳細をシナリオでご紹介します。

1. 看護師の田中さんは、勤務中の出来事や日々の勤務への愚痴をSNS上に呟こうとしています。

2. 田中さんは、匿名アカウントでSNSに投稿。公開範囲を限定しておらず、不特定多数の人に見られる状態でした。

3. 投稿内容は、患者への不満や不適切な行為の記述が含まれており、たちまちSNS上で話題になりました。

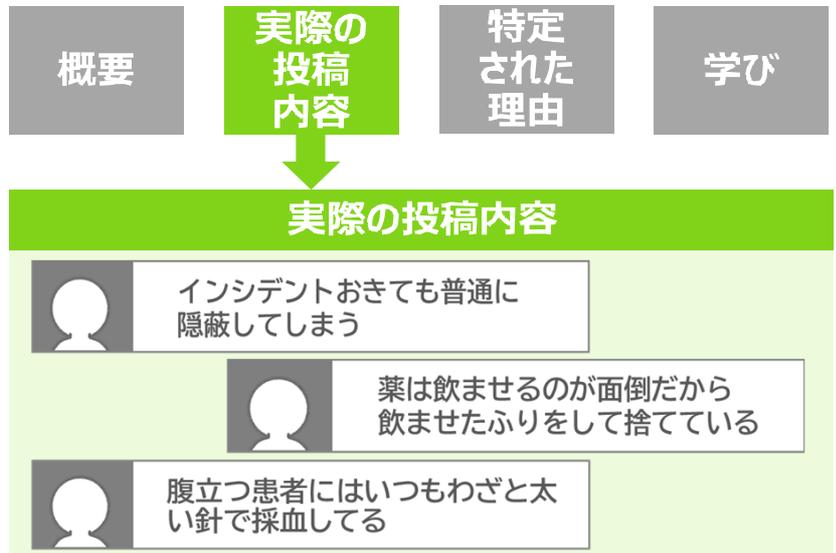
4. 投稿は拡散され、その内容から田中さんの正体、勤務する病院まで特定され、大問題になりました。

# SNS利用に関する実際の事例 3

## ◆ 千葉大学附属病院



引用：NHK (<https://www3.nhk.or.jp/shutoken-news/20250108/1000112859.html>)

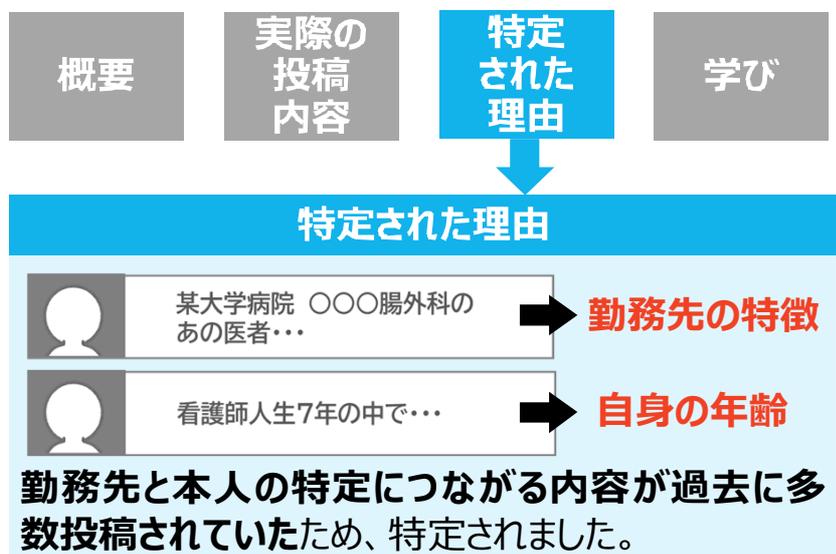


# SNS利用に関する実際の事例 3

## ◆ 千葉大学附属病院



引用：NHK (<https://www3.nhk.or.jp/shutoken-news/20250108/1000112859.html>)

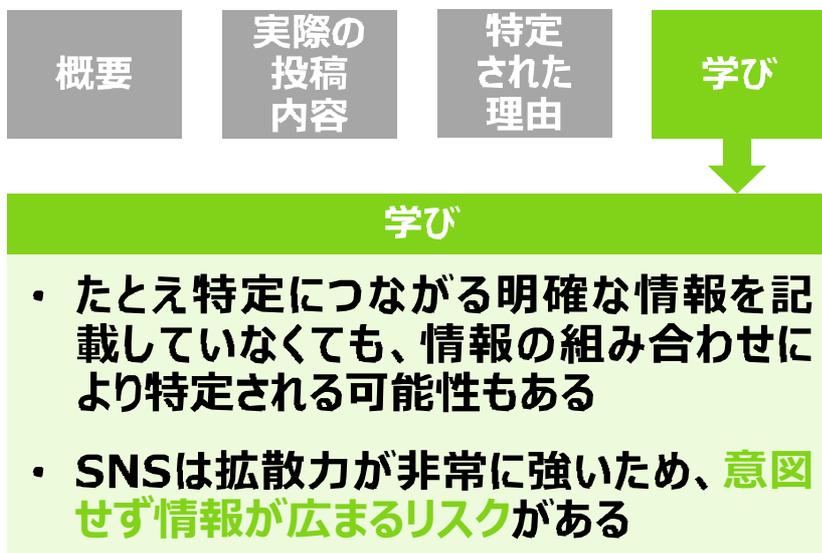


## SNS利用に関する実際の事例 3

### ◆ 千葉大学附属病院



引用：NHK (<https://www3.nhk.or.jp/shutoken-news/20250108/1000112859.html>)



## 承認されていないITの利用

## シャドーITとは

業務外で私的にSNSを利用し、情報漏えいが発生するケースだけでなく、**業務内で、承認されていないSNSや外部サービスを利用してしまいうケース**にも注意が必要です。

### シャドーIT

組織が把握していないIT機器やアプリ、サービスを、職員が勝手に**業務内で**利用すること。  
例：個人の端末、個人のLINEやGmail、無料のファイル共有サービス等

#### 本来



#### シャドーIT



## シャドーITの事例

### ◆ つがる西北五広域連合

**カルテ流出 看護師4人が関与**

つがる西北五広域連合の医療機関から新型コロナウイルス感染症患者の電子カルテデータが外部に流出した際、報道は24日、流出に関与したのは感染症患者の病状の検閲記録に勤務する4人の看護師だったと明らかにした。右記書の内容は正確であることが、事後は関与の経路に応じて明らかになる方針。4人のうち、少なくとも外部の2人に情報が漏れたことも分かった。

同連合の付帯医療情報管理担当委員副委員長・副委員長と中泊型地域医療支援センターが発表で明らかにし、改めて患者や家族と連絡先に謝罪した。

カルテは新型ウイルスで陽性と確認された20代男性のもので、無料通信アプリのLINEと「ライン」に画像が流出。個人を特定できる内容ではなかったものの、病状の検査項目や検査結果が読み取れる状態だった。

同連合は専門医情報センターの担当で発祥を把握、内部で調査取り調べを進めた結果、A〜Dの4看護師が分かった。4人の性別、年代などについては、特定を避けるためとして公表していない。

調査結果によると、Aは感染記録のある患者が入居するに当たり、外来担当看護師の電子カルテの一部の印刷物を引き取った。Aはその一部を携帯電話で撮影し、翌日勤務の日にLINE、LINEでその画像を関係者一人ひとりに画像を伝付、さらに、関係者でなくても印刷物を持ってある関係者から情報が流出したと推定。中泊の対応を関係者としてLINEで関係者に伝付した。この関係が別の関係者にも伝付していた。

それから、Cからも中泊型病棟のLINEが送られたが、Dがこれに気づき、関係者より連絡がストップ。ただしDは上層への報告を怠っていた。

引用：陸奥新報 (<https://mutsushimpo.com/news/hbbe11ye/>)

概要	事例のイメージ	共有の理由	学び
----	---------	-------	----

**概要**

2020年3月、つがる西北五広域連合の医療機関に勤める看護師が、患者の電子カルテの印刷物をLINEで共有。流出に関与したのは4人の看護師で、少なくとも外部の2人にも情報が漏えいしました。

# シャドーITの事例

## ◆ つがる西北五広域連合

**カルテ流出 看護群4人が関与**

つがる西北五広域連合の医療機関から新型コロナウイルス感染症患者の電子カルテデータが外部に流出した疑いで、同連合は24日、関与が疑われたのは感染症患者情報等の感染経路等に勤務する4人の看護士だと明らかにした。公文書の不審的な処理であることが、半年は関与の経路に応じて追跡調査する方針。4人のほか、少なくとも外部の2人に情報が漏れたことも分かった。

同連合の市町村保健医療情報推進委員会副委員長・調査委員長と中泊市立病院院長が記者会見で明らかにし、改めて患者や家族と謝罪表明に謝罪した。

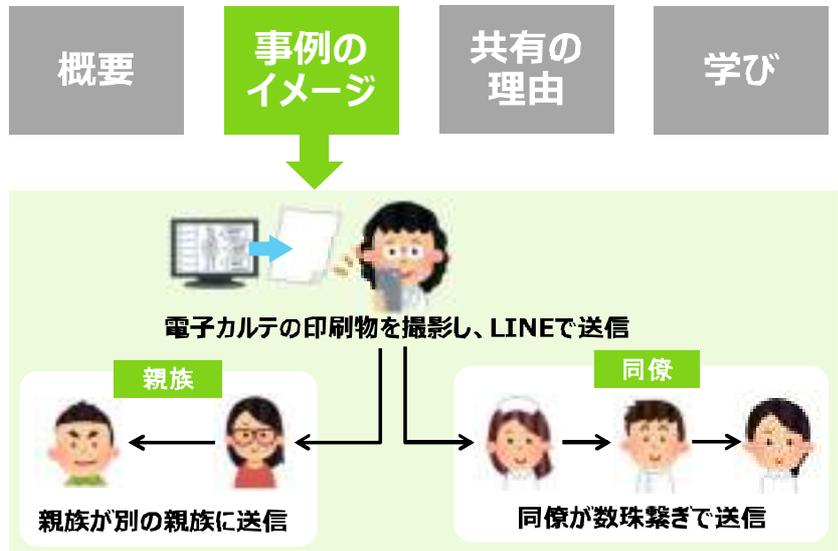
カルテは新型ウイルスで陽性と確認された20代男性のもので、無料通信アプリのLINEと「ライン」に画像が流出。個人を特定できる内容ではなかったものの、身元の検査項目や検査結果が読み取れる状態だった。

同連合は専門医情報センターの協力で発祥に事実を調査、内訳を聞き取り調査を進めた結果、A〜Dの4看護士が関与した。4人の性別、年代などについては、特定を断ったためとして公表していない。

調査結果によると、Aは感染経路のある患者が入院するに当たり、外来科と検査科の電子カルテの一部に印刷物を引き取り、Aはその一部を携帯電話で撮影し、翌日同科の者に渡し、1ヶ月までの検体を送る一環と名を偽装を反付、さらに、同科検体でできなくなる検体で待機のある同科検体の結果が不明になると考え、本来の対応を偽装ととらして1ヶ月で検体3人に送った。この検体が別の検体2人にも送られていた。

BからD、Cからの不正アクセスは1ヶ月が区別されたが、Dがこれに押し、恐めるよう仕掛け伝達をストップ。ただしDはとも同への報告を怠っていた。

引用：陸奥新報 (<https://mutsushimpo.com/news/hbbe1iye/>)



# シャドーITの事例

## ◆ つがる西北五広域連合

**カルテ流出 看護群4人が関与**

つがる西北五広域連合の医療機関から新型コロナウイルス感染症患者の電子カルテデータが外部に流出した疑いで、同連合は24日、関与が疑われたのは感染症患者情報等の感染経路等に勤務する4人の看護士だと明らかにした。公文書の不審的な処理であることが、半年は関与の経路に応じて追跡調査する方針。4人のほか、少なくとも外部の2人に情報が漏れたことも分かった。

同連合の市町村保健医療情報推進委員会副委員長・調査委員長と中泊市立病院院長が記者会見で明らかにし、改めて患者や家族と謝罪表明に謝罪した。

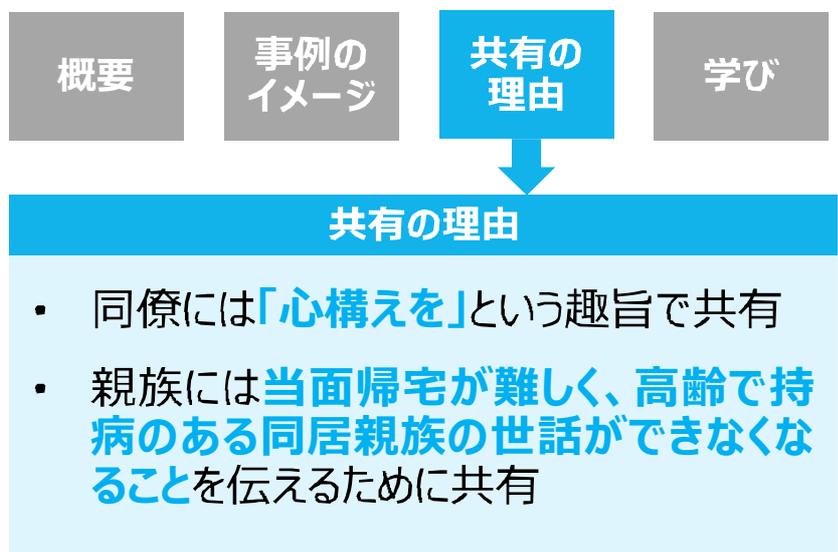
カルテは新型ウイルスで陽性と確認された20代男性のもので、無料通信アプリのLINEと「ライン」に画像が流出。個人を特定できる内容ではなかったものの、身元の検査項目や検査結果が読み取れる状態だった。

同連合は専門医情報センターの協力で発祥に事実を調査、内訳を聞き取り調査を進めた結果、A〜Dの4看護士が関与した。4人の性別、年代などについては、特定を断ったためとして公表していない。

調査結果によると、Aは感染経路のある患者が入院するに当たり、外来科と検査科の電子カルテの一部に印刷物を引き取り、Aはその一部を携帯電話で撮影し、翌日同科の者に渡し、1ヶ月までの検体を送る一環と名を偽装を反付、さらに、同科検体でできなくなる検体で待機のある同科検体の結果が不明になると考え、本来の対応を偽装ととらして1ヶ月で検体3人に送った。この検体が別の検体2人にも送られていた。

BからD、Cからの不正アクセスは1ヶ月が区別されたが、Dがこれに押し、恐めるよう仕掛け伝達をストップ。ただしDはとも同への報告を怠っていた。

引用：陸奥新報 (<https://mutsushimpo.com/news/hbbe1iye/>)



# シャドーITの事例

## ◆ つがる西北五広域連合

**カルテ流出 看護婦4人が関与**



つがる西北五広域連合の医療機関から看護婦30名くらいが感染患者の電子カルテ画像が外部に流出した際、報道は24日、関与が疑われたのは感染症患者画像の感染経路等に勤務する4人の看護婦だと明らかになった。公文書の不審的な処理などから、今度は関与の経路に応じて警察送付する方針。4人のほか、少なくとも外部の2人に情報が行ったことも分かった。

同連合の市町村保健医療情報担当委員会委員長・副委員長と中込弘次地区連合長が早急対策を明らかにし、改めて患者や家族と連絡調整に動いた。

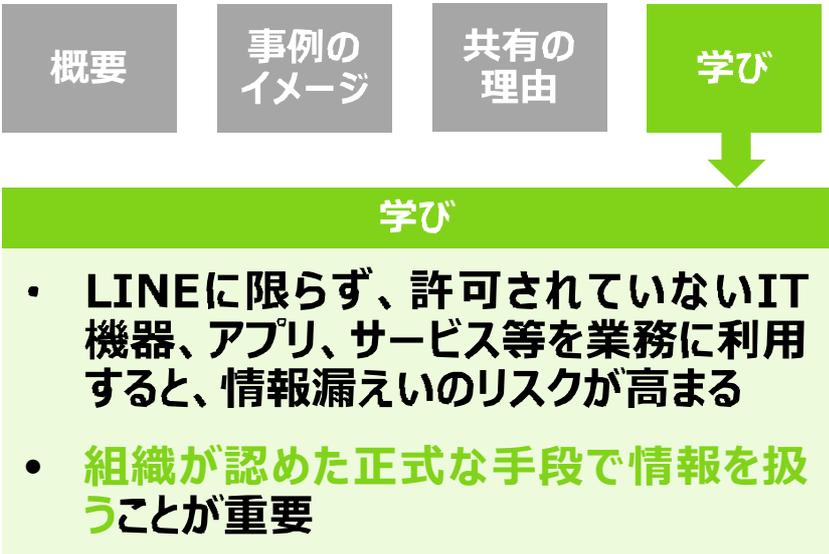
カルテは紙型ファイルで開封と確認されたところ代男性のもので、無料通信アプリのLINEと「ライン」に画像が流出。個人を特定できる内容ではなかったものの、具体的な検査項目や検査結果が読み取れる状態だった。

同連合は専門医情報センターの協力を得て、内閣府と連携し、内閣府から調査を求めた結果、A〜Dの4看護婦が関与した。4人の関与、年代などについては、特定を断れるためとして公表していない。

調査結果によると、Aは感染経路のある患者が入院するに当たり、外来医と連携してカルテを1枚ずつ一部に印刷物を印刷していた。Aはその一部を携帯電話で撮影し、翌日社員の手に渡し、LINEなどで送信を求めた一文とともに画像を送付。さらに、画像保存できなくなる直前で携帯で所持する医療機関の情報が不明瞭になると考え、画像の対応を画像とともにLINEなどで検索したに違いない。この機嫌が別の検索手段にも関係していた。

それから、Cからのにも送付確認がLINEで返されたが、Dがこれに対し、早めるよう依頼し伝達がストップ。ただしDはその後への発信を断っていた。

引用：陸奥新報 (<https://mutsushimpo.com/news/hbbe11ye/>)



# シャドーITの問題点

なぜシャドーITが問題なのでしょう？

**業務で利用するIT機器やサービスを組織が把握・管理できないため**



- **情報漏えいに気づけない**
- **セキュリティ対策が適用されない**
- **漏えい時の追跡・原因調査ができない**

**許可なしにアプリやサービスを業務で利用しないよう、注意しましょう**

## パブリックSNSの利用について

たとえ病院の許可がある場合でも、**パブリックSNSの業務利用は不適切**です。

パブリックSNS（公開型）	プライベートSNS（非公開型）
<ul style="list-style-type: none"> <li>誰でも利用でき、情報が広く公開されるタイプのSNS</li> </ul> 例：Instagram、Facebook、LINE 等	<ul style="list-style-type: none"> <li>組織が契約・管理し、利用者や閲覧範囲が制限されたSNS</li> </ul> 例：LINE WORKS、Microsoft Teams 等



### どんなリスクがある？

- ・ 情報が意図せずとも公開される
- ・ 患者情報や業務情報の漏えい
- ・ 病院の印象・信用の低下

## パブリックSNSの利用について

### 医療情報システムの安全管理に関するガイドライン第6.0版 Q&A

(<https://www.mhlw.go.jp/content/10808000/001145860.pdf>)

〈概Q-8〉SNS等のWebサービスを利用して医療情報をやり取りする場合、考慮すべきことはあるか。

- A SNS（Social Networking Service）等のWebサービスを利用して患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要があります。特に、SNS の場合、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNSを利用する際に気を付けるべき事項」を参考に、適切な対策を講じてください。

HISPROが公表する「医療情報連携において、SNSを利用する際に気を付けるべき事項」を参考に、適切な対策を講じる

### 医療情報連携において、SNSを利用する際に気を付けるべき事項

([https://hispro.or.jp/open/pdf/SNS\\_RiyouchiCheckJikou\\_20160126.pdf](https://hispro.or.jp/open/pdf/SNS_RiyouchiCheckJikou_20160126.pdf))

#### 2.2.1 パブリックSNS（公開型）

パブリックSNSは一般の利用者で利用できるものが多く、Facebook、Google+、LINE等に代表される。サービスの多くは無料で利用でき、アカウントを作成し、そのアカウントでメッセージやデータのやり取りが行われたり、情報を開示したりしている。情報に対して、利用者によるアクセスコントロールが可能になっているサービスもあるが、基本的にはインターネット上に全公開することが可能になっているものが多く、患者や家族等の自分自身の情報ではない機微な情報を連携させるためのツールとしては不適切である。また、無料で提供されることが多いため、利用規約としてSNSサービス上を流通している情報について、運営会社も分析等が可能な規約になっているサービスも存在し、注意が必要である。

パブリックSNSは公開範囲の制御が不十分で、運営会社による情報利用のおそれもあるため、**医療機関の業務での利用は不適切**である。

**パブリックSNSは、患者や家族等、自身の情報ではない機微な情報を扱うには不適切**です。

## (参考) プライベートSNSの選択基準

業務では、プライベートSNSの利用が適切です。

### プライベートSNSを選ぶ際の基準

#### ① アクセスできる人が限られていること

特定の医療関係の有資格者や家族等、信頼できる人だけがアクセスできる仕組みを持つサービスを選びましょう。

#### ② 国内の安全な環境でデータが守られていること

データセンターが日本国内にあり、通信経路や保存時のデータが暗号化されるサービスを選びましょう。

#### ③ 信頼できる第三者の認証を受けていること

ISO/IEC 27001やISO/IEC 27018等の公的なセキュリティ規格を取得しているサービスを選びましょう。

※パブリックSNSを業務利用している場合、上長や情報システム部門に相談し、運用の見直しを検討してください。

## SNSを適切に利用するために

SNS利用時にはどのような点に注意すればよいでしょうか？

### 1. 投稿前に内容を確認する

SNSを利用する際は、むやみに投稿するのではなく、本当に投稿して良い内容か、情報漏えいにならないか？を意識して確認する習慣をつけましょう。



### 2. 発信する場所・相手を意識する

たとえ自分がSNSに投稿しなくても、例えば家族や友人に何気なく話した情報を、SNSに投稿される可能性もあります。情報を発信する場所や相手は、常に意識しましょう。



## SNSを適切に利用するために

SNS利用時にはどのような点に注意すればよいでしょうか？

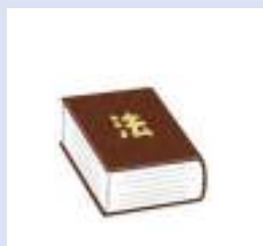
### 3. 医療現場で特定につながる情報を理解する

病院では、例えば病室の場所や受診日等の情報でも、組み合わせ次第で個人を特定できることがあります。どのような情報が特定につながってしまうのか、情報の内容を正しく理解しましょう。



### 4. 法的なリスクを理解する

医療機関で情報漏えいが発生すると、個人情報保護法や守秘義務違反に問われる可能性があります。医療従事者としての信頼を守るためにも法的な責任を理解しましょう。



## SNSを適切に利用するために

SNS利用時にはどのような点に注意すればよいでしょうか？

### 5. SNSのプライバシー設定を見直す

無意識にSNSに情報を書き込んでしまった場合に備え、公開範囲等のプライバシー設定を見直しましょう。（たとえ公開範囲が友人限定でも、患者情報は書き込んではいけません。）



### 6. 業務用と私用アカウントを分けることを検討する

業務用と私用のアカウントを分けることで、情報の混同や誤解を防げます。完全に分けることが難しい場合には、すべての投稿内容に責任を持ちましょう。



# まとめ

## まとめ（個人情報の管理）

### ● 個人情報

- ✓ 氏名や生年月日、身体データ等、特定の個人を識別できるもの
- ✓ 個人識別符号が含まれるもの

### ● 特定個人情報

- ✓ 個人番号（マイナンバー）および個人番号と紐づいた氏名や生年月日等の情報

### ● 要配慮個人情報

- ✓ 人種、信条、病歴等、差別や不利益につながるおそれがあるため、特に慎重な取り扱いが求められる個人情報

- 情報漏えいがあった（可能性がある）場合は、個人情報保護委員会への報告と、本人への通知が必要

### ● 報告が必要なケース

- ✓ 要配慮個人情報が含まれる
- ✓ 財産的被害のおそれがある
- ✓ 不正の目的をもって行われた漏えい等

※ 1件でも漏えいすれば報告が必要

- ✓ 1,000人を超える漏えい等

## まとめ (SNS利用)

### ● SNS利用におけるリスク

- ✓ 患者情報の漏えい
- ✓ 医療機関の信用低下
- ✓ 法的責任の発生
- ✓ 職員本人への不利益

### ● 守秘義務

- ✓ 医療資格を持つ人は、個人情報適切に扱うことが法的な義務
- ✓ 医療資格を持たない人も就業規則や雇用契約で守秘義務が課せられている

### ● シャドーITとは、組織が把握していないIT機器やアプリ・サービスを、**職員が勝手に業務内で利用すること**

- 業務で使用するものを組織が把握・管理できない = **情報漏えいに気づけない、セキュリティ対策を実施できない、漏えい時の追跡や原因調査ができない**
- 業務で利用するITは必ず**正式な手続き**を通し、組織全体で安全な情報管理を心がける

### ● SNS利用時に注意すべきこと

- ✓ 投稿前に内容をよく確認する
- ✓ SNSに限らず、情報を発信する場所や相手を意識する
- ✓ どのような情報が個人の特定につながるのかを理解する
- ✓ 法的なリスク（個人情報保護法や守秘義務違反）を理解する
- ✓ プライバシー設定を見直す
- ✓ 可能な場合は業務・私用アカウントを使い分ける