SNS利用時の注意事項　チェック項目

項番	分類	項目	評価内容	備考
1	A:契約事項	個人情報保護方針が関係者間で策定されているか	個人情報保護方針をSNSサービス利用主体として策定しているか。	
2			個人情報保護方針を運営ホームページ等による公開、もしくは利用する際の説明事項として公開しているか。	
3		苦情のための窓口が用意され、体制が構築されているか	SNSサービス利用主体として、利用者に対して問い合わせ体制を構築しているか。	
4			問合せ体制に対する連絡先、手段が備えられているか。	
5			利用者に対して、問い合わせ体制、連絡先、連絡手段について、運営ホームページ等による公開、もしくは利用する際の説明事項として公開しているか。	
6		患者・利用者にサービス内容や利用目的の説明を行った上で、SNSのサービスを利用しているか	サービス内容や利用目的について説明できる資料を作成しているか。	
7			利用者に対して、運営ホームページ等による公開、もしくは利用する際の説明事項として公開、もしくは個別同意をとってい	
8		サーバに蓄積された情報が目的外で利用されることはないか	SNSサービスを利用した際の蓄積された情報について、通常利用の範囲として、目的である利用者間の情報連携のためのみに利用しているか。	
9			SNSサービスを利用した際の蓄積された情報について、システムをメンテナンスするために、ログ等の情報や異常が起きた場合の事象再現のためのテスト等、SNSサービスの正常な動作のための確認に限定した利用をしているか。	
10			SNSサービスを利用した際の蓄積された情報に対する目的について明記し、運営ホームページ等による公開、もしくは利用する際の説明事項として公開しているか。	
11		ユーザに対して、実施すべき対策や運用についてきちんと示しているか	利用者に対して、利用者がSNSサービスを利用する際に、利用する端末に対する技術的セキュリティ対策について策定し	
12			利用者に対して、利用者がSNSサービスを利用する際に、実施すべき運用について策定しているか。	
13			策定している内容について、利用者に運営ホームページ等による公開、もしくは利用する際の説明事項として公開、もしくは個別説明を行っているか。	
14		責任分界点が明確になっているか	SNSサービスを利用する場合に、起こり得るリスクを検討しているか。	
15			起こり得るリスクが顕在化した場合の責任の所在が、対象や発生箇所によって明確になっているか。	
16			責任の所在について利用者に運営ホームページ等による公開、もしくは利用する際の説明事項として公開、もしくは個別説明を行っているか。	
17		利用するSNSのSLAが定めてあるか	SNSサービスの稼働時間等の稼働すべき状態（サービスレベル）について、条件を策定しているか。	
18			利用者に対し、SNSサービスのサービスレベルについて、利用契約書等で合意をとっているか。	
19		SLAの見直しが行われているか	SNSサービスのサービスレベルについて、定期的（月に1回、年に1回等）に見直しが行われているか。	
20		サービスの継続性が確保されているか	SNSサービス内に、参照すべき情報を保管する、またはサービス自体が診療、介護サービス等の行為に対して必要不可欠なものである場合、診療、介護サービス等の影響の出る範囲でサービスが停止しない、またはSNSサービス自体が終了することがないことを契約等で定められているか。	
21			仮にSNSサービス自体が終了する場合、終了する際のサービスの移行や、サービスの終了に対する十分な期間をとり、診療、介護サービス等の影響の出ないような対策が検討されて	
22	B:運用事項	プライベートSNSが利用されているか	SNSサービスが医療・介護従事者並びに診療・介護の対象となる本人や、本人に関わる家族等のみがアクセス可能とするため、ユーザになるための確認や承認が行われている。	
23			独自にSNSサービスを構築し、限られた範囲のみで利用するものとなっており、SNSサービス利用者以外はアクセスができないように制御が行われているか。	
24		利用するSNSに対して、リスク分析をした上で対応内容を策定しているか	SNSサービスに対してリスク分析を行っているか。	
25			生じると想定されるリスク内容に対して、どのような対応、対策を行うかについて策定しているか	
26		やり取りする情報の中に、個人情報や医療情報が含まれている場合のルールが定めてあるか	メッセージ等の情報の中に、個人情報や医療情報が含まれる際のセキュリティ対策について検討されているか。	
27			メッセージ等の情報の中に、個人情報や医療情報が含まれる際の運用方法について検討されているか。	
28			検討されたセキュリティ対策や運用方法についてルールとして策定されているか。	
29		SNS上で通常の業務範囲を超える事項が実施されていないか	SNSサービスを利用した際の情報について、利用者に個別同意をとらない状態で、マーケティング分析や、利用者の個人情報を利用した医療介護連携以外のサービスの提供が行われ	
30		情報の共有範囲（アクセス権）が適切に設定されているか	情報の共有範囲（アクセス権）が設定可能か。	
31			情報の共有範囲（アクセス権）について、利用者の意図しない共有範囲とならないように適切に設定されているか。	
32			情報の共有範囲（アクセス権）について、初期状態が全公開になっていないか。	
33		誰が扱っているか明確になっているか	SNSサービスの利用者について管理がされているか。	
34			SNSサービスで情報のやり取りを行う際に、誰から誰に対して情報をやり取りしているか分かるようになっているか。	
35			SNSサービスで情報のやり取りが行われたことについて、管理者等がログ等の取得により、履歴をたどれるようになってい	
36		職種に応じた情報が閲覧できるようになっているか	情報の共有範囲（アクセス権）の設定の際に、職種による共有範囲の設定が可能か。	
37		職種が特定できないことを前提とする場合、機微な情報を流さないようにルールが定めてあるか	情報の共有範囲（アクセス権）の設定の際に、職種による共有範囲の設定が可能でない場合、機微な情報を流さないようなセキュリティ対策や運用方法についてルールとして策定されて	
38		SNSサービス上、保存される情報が明確になっているか	SNSサービスで保存する情報について洗い出され、設計書、説明書等で明確になっているか。	
39		SNSを利用するための端末に関する管理ルールが定めてあり、適切に運用されているか	利用者に対して、利用者がSNSサービスを利用する際に、利用する端末に対する技術的セキュリティ対策について策定しているか。	・ユーザに対して、実施すべき対策や運用についてきちんと示しているかの項目と同項目 ・BYODの場合も含む
40			利用者に対して、利用者がSNSサービスを利用する際に、実施すべき運用について策定しているか。	・ユーザに対して、実施すべき対策や運用についてきちんと示しているかの項目と同項目 ・BYODの場合も含む
41			策定している内容について、利用者に運営ホームページ等による公開、もしくは利用する際の説明事項として公開、もしくは個別説明を行っているか。	・ユーザに対して、実施すべき対策や運用についてきちんと示しているかの項目と同項目 ・BYODの場合も含む
42		端末紛失時等の対応について定めてあるか	利用者が端末を紛失する等のリスクに備え、どのような対応、対策を行うかについて策定しているか。	・リスク分析の対応内容の一部 ・BYODの場合も含む

SNS利用時の注意事項　チェック項目

項番	分類	項目	評価内容	備考
43		何をしてはいけないか、何があったら知らせないといけないかについて定義され周知されているか	利用条件等について策定されているか。	・BYODの場合も含む
44			インシデント等の連絡すべき事項について策定しているか。	・BYODの場合も含む
45			利用条件や連絡すべき事項について、利用者に運営ホームページ等による公開、もしくは利用する際の説明事項として公開、もしくは個別説明を行っているか。	・BYODの場合も含む
46		利用ルールに対する教育が行われているか	定められた利用ルールに対して、利用者に説明が行われているか。	
47			利用ルールの利用者への説明に対して、理解した旨の証跡を取得しているか。	
48			利用ルールの利用者への説明を、定期的に実施しているか。	
49	C:技術事項	SNSを利用するためのネットワークが特定されているか	厚生労働省の「医療情報システムの安全管理に関するガイドライン」最新版の中で「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」の項に記載された事項に準拠していることを確認すること。	・独自にSNSサービスを構築している場合に注意すべき点として、ネットワーク種別の指定がされている、のアクセス先（URL、IPアドレス）が明確になっている、アクセス先が正しい接続先であることを認証している（例：サーバ証明書による認証等）等を確認する必要がある。 ・BYODの場合も含む
50		ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとられているか	厚生労働省の「医療情報システムの安全管理に関するガイドライン」最新版の中で「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」の項に記載された事項に準拠していることを確認すること。	・独自にSNSサービスを構築している場合に注意すべき点として、ネットワークについてチャネルセキュリティとしての対策が取られているかを確認する必要がある。 ・BYODの場合も含む
51			（H28/8/24の事務連絡のQ＆A改定によるTLS1.2を採用した場合） SNSサービスの通信設定として、下記項目が実施されているか確認すること。 ・SSL/TLSのバージョンをTLS1.2に限定しているか。 ・ユーザの環境にクライアント証明書を導入しTLSクライアント認証を実施しているか。 ・サーバ環境において、IPAが発行している「SSL/TLS暗号設定ガイドライン」の高セキュリティ型の基準を満たすためにチェックリストの項目を満たした設定にしているか。	・独自にSNSサービスを構築している場合に注意すべき点として、ネットワークについてチャネルセキュリティとしての対策が取られているかを確認する必要がある。 ・BYODの場合も含む
52		施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとられているか	厚生労働省の「医療情報システムの安全管理に関するガイドライン」最新版の中で「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」の項に記載された事項に準拠していることを確認すること。	・独自にSNSサービスを構築している場合に注意すべき点として、ネットワーク上を流れる情報（オブジェクト）に対し、オブジェクトセキュリティとしての対策が取られているかについて確認する必要がある。
53		セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策がとられているか	厚生労働省の「医療情報システムの安全管理に関するガイドライン」最新版の中で「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」の項に記載された事項に準拠していることを確認すること。	・独自にSNSサービスを構築している場合に注意すべき点として、なりすまし防止のための対策をとっているかを確認する必要がある。 ・BYODの場合も含む
54		利用者の識別、認証を行うために、利用する際のID/PWが設定されているか	厚生労働省の「医療情報システムの安全管理に関するガイドライン」最新版の中で「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」の項に記載された事項に準拠していることを確認すること。	・独自にSNSサービスを構築している場合に注意すべき点として、最低限ID/PWによるユーザ認証を行っているか、PWについて容易に推測されないためのルールを策定しているか等を確認する必要がある。PKI等の電子証明書による認証であれば、なお良い。
55		情報に対する暗号化が行われているか	やりとりされる情報自体に暗号化が行われているか。	・NWにおけるオブジェクトセキュリティに加えて、アプリケーションとして情報の暗号化が行われているか。
56		SNSを利用するための端末に対して、ID/PW等の利用者認証の手段が取られているか	端末を利用するために、端末に対して最低限ID/PWによるユーザ認証を行っているか。	・PKI等の電子証明書による認証、生体認証、2要素認証等であれば、なお良い。 ・BYODの場合も含む
57		情報に対するアクセス権の設定ができるようになっているか	情報の共有範囲（アクセス権）が設定可能か。	・情報の共有範囲（アクセス権）が適切に設定されているかの項目と同項目
58			情報の共有範囲（アクセス権）について、利用者の意図しない共有範囲とならないように適切に設定されているか。	・情報の共有範囲（アクセス権）が適切に設定されているかの項目と同項目
59			情報の共有範囲（アクセス権）について、初期状態が全公開になっていないか。	・情報の共有範囲（アクセス権）が適切に設定されているかの項目と同項目
60			情報の共有範囲（アクセス権）の設定の際に、職種による共有範囲の設定が可能か。	・職種に応じた情報が閲覧できるようになっているかの項目と同項目
61			情報の共有範囲（アクセス権）の設定の際に、職種による共有範囲の設定が可能でない場合、機微な情報を流さないようなセキュリティ対策や運用方法についてルールとして策定されて	・職種が特定できないことを前提とする場合、機微な情報を流さないようにルールが定めてあるかの項目と同項目
62		SNSサービスにアクセスしたことのログを取得しているか	SNSサービスの利用者について管理がされているか。	・誰が扱っているか明確になっているかの項目と同項目
63			SNSサービスにログインしたことについて、利用者が分かるような形でログが取得されているか。	
64		アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じてあるか	アクセスログに対してシステム管理者のみ、閲覧のみ可能とする対策が講じてあるか。	
65		情報を保管する場所について、医療機関等に保管する場合は厚生労働省の「医療情報システムの安全管理に関するガイドライン」の最新版、民間事業者に保管する場合は、総務省の「ASP・SaaSにおける情報セキュリティ対策ガイドライン」、「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」、経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」のそれぞれ最新版に沿った対策が取られているか	医療機関に情報を保管する場合は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」の最新版に従い、策定された運用管理規程の下、管理され、対策が取られているか。	
66			SNSサービス提供事業者が実施している場合は、SNSサービス提供事業者から各ガイドラインに沿った対策が取られていることの証跡について提出してもらっているか。	・HISPROによる「民間事業者による医療情報の外部保存及びASP・SaaSサービス」に対する評価を受けてもらい、その適合性評価結果を提出してもらうことが望ましい。
67		特に持出し端末について、通信経路として安全が守られた無線LANやキャリア網を利用した上で、暗号化通信を行うように設定されているか	持ち出し端末の場合、通信経路として安全が守られた無線LANやキャリア網を利用しているか。	・BYODの場合も、持ち出し端末としてみなす。
68			安全が守られた無線LANやキャリア網を利用する場合においてもチャネルセキュリティとしての暗号化通信の対策が取られているか。	・BYODの場合も含む
69		端末に対してウイルス等による攻撃を受けないためにウイルス対策ソフトや、不要な通信を遮断するようなファイヤーウォールソフト等を導入しているか	端末に対するセキュリティ対策方法について、ウイルス対策ソフトや不要な通信を遮断するファイヤーウォールソフト等を導入しているか。	・USBポートなどの制御、情報の持ち出し管理等が可能であるとなお良い。 ・BYODの場合も含む
70		無線LANのアクセスポイントを有する場合、利用者以外に無線LANの利用を特定できないようにしてあるか	SNSサービスを利用するための通信環境として無線LANを利用する場合、親機やサービスの設定として、SSIDがステルス設定になっているか。	・BYODの場合も含む

SNS提供事業者による技術説明・開示情報　チェックシート

1	技術説明・情報開示	非公開型であること		
2		ネットワークセキュリティのガイドライン適合性		
3		クライアント認証機能		
4		個人情報保護方針		
5		契約約款等		
6		利用者への説明資料		