一般社団法人 サルビアねっと協議会

サルビアねっとを安心してご利用いただくための セキュリティの取り組み

サルビアねっと協議会（以下、当協議会）は、参加施設の皆様に安心してサルビアねっとをご利用いただくため、システムの構築・運用・保守を担当する株式会社ヘルスケアリレイションズ（以下、ベンダー）と連携し、情報セキュリティの確保を最優先事項の一つとして取り組んでいます。

本ページでは、ベンダーから当協議会へ報告されたセキュリティ対策の状況（2026年11月5日付報告）と、ご利用施設の皆様へのお願いをご案内します。これから参加をご検討の施設の皆様も、ご判断の参考としてご覧ください。

要点 ― 先にお伝えしたいこと

- 最近報道されているPHPの脆弱性について、サルビアねっとのシステム（CoEsse・CoEsseCA）はPHPを使用していないため、**影響はありません**。
- システムは、国のガイドライン（3省2ガイドライン）に準拠し、暗号化された接続、Webからの攻撃への防御、ネットワークごとに分離された専用環境での情報管理など、多層的な対策を実施しています。
- より安全なご利用のため、参加施設の皆様にも、ID・パスワードの管理など3点のお願いをしています（本ページ後半をご覧ください）。

1．背景 ― なぜ、いまご案内するのか

医療機関を狙ったサイバー攻撃や、PHP等のソフトウェアの脆弱性に関する報道が続いています。サルビアねっとがお預かりするのは、患者様・利用者様の医療・介護情報とプライバシーに関わる大切な情報です。

このような状況を踏まえ、当協議会はベンダーからセキュリティ対策の現状について改めて報告を受け、その内容を参加施設の皆様、および参加をご検討中の皆様へ公開することといたしました。

2．PHPの脆弱性に関する報道について

最近、Webサイトなどで広く使われているプログラミング言語「PHP」の脆弱性と、それを悪用した不正アクセスに関する情報が公表されています。

サルビアねっとに適用しているベンダーのシステム（CoEsse・CoEsseCA）は、PHPを使用していないため、本脆弱性による影響はございません。引き続き安心してご利用ください。

なお、ベンダーでは今後も新たな脆弱性情報を継続的に確認し、必要な対策を速やかに実施していくとの報告を受けています。

3．セキュリティ対策の取り組み

お預かりしている医療・介護情報や、患者様・利用者様のプライバシーを保護するため、以下の対策を実施しています。

（1）国のガイドライン（3省2ガイドライン）に準拠したシステム

サルビアねっとでは、厚生労働省・経済産業省・総務省が定めるガイドラインに準拠したセキュリティ対策を実施しています。医療情報を取り扱うシステムに求められる国の基準に沿った運用は、参加をご検討の施設様にとっても、院内・施設内の規程整備や説明の際の根拠となります。

（2）IPsec-VPNによる暗号化された接続

サルビアねっとのクラウドと各連携施設（病院・診療所・調剤薬局・介護施設・訪問看護ステーション等）との間の通信には、IPsec-VPNを適用しています。通信内容は暗号化された経路でやり取りされるため、途中で第三者に読み取られるリスクを低減しています。



図1　施設との通信は、暗号化された専用の経路（IPsec-VPN）で行っています

（3）Webアプリケーションファイアウォール（WAF）による防御

住民の皆様がWebからの同意取得で利用するシステム「CoEsseCA」には、AWS WAFを導入し、不正な通信やサイバー攻撃を遮断する対策を実施しています。特に、海外IPからのアクセス制限をかけるなど、インターネット側からの入口（インバウンド）に対する制御を実施しています。



図2　インターネットからの入口（CoEsseCA）では、WAFが不審な通信を遮断します

（4）ネットワークごとに分離された専用環境での情報管理

患者様・利用者様の基本情報や医療・介護情報は、Amazon Web Services（AWS）上に、地域医療連携ネットワークごとに独立して構築した専用のネットワーク環境（VPC）で管理しています。サルビアねっとの情報がほかのネットワークの情報と混在することはなく、外部の環境とも分離されているため、万一いずれかの環境で問題が生じても、影響がほかに広がりにくい構成としています。

※ここでいう「分離」は、ネットワークごとの環境の分け方を指すもので、データセンターの所在地を示すものではありません。



図3　サルビアねっとの情報は、ほかのネットワークとは分離された専用環境で管理しています

（5）継続的な脆弱性管理と対策の強化

システムで使用しているソフトウェアのバージョンを一元管理し、新たな脆弱性が判明した際に、影響範囲を速やかに把握できる体制づくりを進めています。あわせて、システム基盤の継続的な更新や、二要素認証の順次導入など、対策の強化を計画的に進めています。

※二要素認証などの新たなセキュリティ機能を追加する際は、設定方法とあわせて、参加施設の皆様へ改めてご案内いたします。

4．ご利用施設の皆様へのお願い

サイバー攻撃の多くは、ID・パスワードの不適切な管理や、更新されていない端末を入口として発生しています。システム側の対策とあわせて、各施設様での運用について、以下のご確認をお願いいたします。これは、これから参加される施設様に、参加後に日々の運用としてお願いする内容でもあります。

お願い	具体的な内容
1．ID・パスワードの適切な管理	使い回しや複数人での共有は避けてください。英数字・記号を組み合わせた、推測されにくいパスワードを設定してください（13文字以上を推奨）。
2．ウイルス対策ソフトとOSの最新化	サルビアねっとをご利用になる端末のウイルス対策ソフトおよびOSは、常に最新の状態に保ってください。
3．USBメモリ等の外部記録媒体の利用	サルビアねっとをご利用になる端末でUSBメモリ等の外部記録媒体を利用する場合は、事前にウイルスチェックを実施し、問題ないことを確認のうえご利用ください。

5．不審な連絡の見分け方（フィッシング詐欺への対策）

昨今、実在するサービスを装ったフィッシング詐欺（偽メール・偽SMS）が増加しています。安全を守るため、以下の運用を徹底しています。

> **ベンダーから、メールやSMSで、お客様のパスワード等を直接入力・返信いただくようお願いすることは、一切ございません。**

当協議会事務局やサルビアねっとを名乗る連絡であっても、パスワードの入力・返信を求めるものには応じないでください。

6．万が一、不審な挙動に気づいた場合

アカウントに不審なログインがあった場合や、サルビアねっと等を装った不審な連絡を受け取った場合は、速やかにパスワードを変更のうえ、下記窓口までご連絡ください。

お問い合わせ・不正利用通報窓口
一般社団法人 サルビアねっと協議会
電話：045-900-3090（9:00〜17:00／月曜日〜金曜日・祝日を除く）

7．参加をご検討中の施設様へ ― よくあるご質問

Q．国のガイドラインに対応していますか？

A．はい。いわゆる「3省2ガイドライン」に準拠した対策を実施しています（詳しくは本文「3．セキュリティ対策の取り組み」をご覧ください）。ガイドラインの出典は以下のとおりです。

出典：厚生労働省「医療情報システムの安全管理に関するガイドライン 第7.0版」（令和8年6月）https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html ／ 総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン 第2.0版」（令和7年3月改定）https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html

Q．施設とシステムの間の通信は安全ですか？

A．IPsec-VPNによる暗号化された経路で情報をやり取りしています。

Q．患者情報はどこで、どのように管理されますか？

A．AWS上に、地域医療連携ネットワークごとに独立して構築した専用ネットワーク環境（VPC）で管理し、ほかのネットワークや外部環境とは分離しています。また、データはAWSの国内データセンターで管理しており、国外に保存されることはありません。

Q．話題になっているPHPの脆弱性の影響はありますか？

A．ありません。サルビアねっとのシステム（CoEsse・CoEsseCA）はPHPを使用していません。

Q．参加施設側では、どのような準備や運用が必要ですか？

A．ID・パスワードの適切な管理、端末のウイルス対策ソフト・OSの最新化、USBメモリ等を使う際の事前ウイルスチェックをお願いしています。詳しくは本ページ「4．ご利用施設の皆様へのお願い」をご覧ください。

Q．セキュリティ対策は、今後も強化されますか？

A．ベンダーにおいて、ソフトウェアのバージョンの一元管理による脆弱性管理、システム基盤の継続的な更新、二要素認証の順次導入などを、計画的に進めています。新たな機能を追加する際は、改めてご案内いたします。

今後も、安心・安全にご利用いただける環境の維持・向上に努めてまいります。引き続きサルビアねっとをよろしくお願い申し上げます。

一般社団法人 サルビアねっと協議会 事務局

※本資料は、株式会社ヘルスケアリレイションズからの2026年11月5日付の報告をもとに作成しています。