ホワイトペーパー

「3省2ガイドライン」を解明する

日本の医療情報取り扱いにおけるガイドライン

目次

シナリオ 3
3省2ガイドラインの適用対象 4

3省2ガイドラインの適用方法 5
3省2ガイドラインの詳細要件 6

3省2ガイドラインへのAcronis Cyber Protect適用 8
アクロニスのサイバーセキュリティ態勢 8

付録 A: 3省2ガイドラインの共有責任対応表 10

免責条項

本ホワイトペーパーの目的は、厚生労働省、経済産業省、総務省、3省による2つのガイドライン、通称「3省2ガイドライン」の第 2 版に関連するサイバーセキュリティのポリシー、手順、およびベストプラクティスの重要性、意味、および実装についての意見と現在の理解を提供することです。このホワイトペーパーの作成にあたっては、公式の Web サイトで公開されている日本語版の全文書を参照しました。できるだけ正確かつ詳細に情報を提供するよう努めていますが、この種の情報は時間とともに解釈の違いや改訂、補足が加えられる可能性があります。本書の著者は、読者は、原資料を精査し、法律や規制の専門家に相談した上で、独自の結論を導き出すことを推奨します。

シナリオ

日本では、Society 5.0 ビジョンやデジタル庁の改革など、政府主導の戦略によって、デジタルトランスフォーメーションの取り組みが積極的に進められています。これらの取り組みは、医療を含むさまざまな業界を最新化するために、AI 技術、クラウドコンピューティング、およびデータ相互運用を統合することに焦点を当てています。これらの技術の導入が積極的に推進されており、IT ベンダーは、日本が安全で相互接続されたテクノロジー社会に移行する過程で重要な役割を担っています。特に、医療業界は、強化された電子医療記録（EHR）管理、安全な患者データ交換、リアルタイム診断を通じて、こうした進歩から恩恵を受けています。

日本のサイバーセキュリティ戦略は、重要な業界と個人データの保護に重点を置いて、ここ数年で大きく進化しました。3省2ガイドラインは、厚生労働省、経済産業省、総務省、3省発行の2つのガイドラインから構成されており、医療情報を扱うために特別に設計された包括的なサイバーセキュリティフレームワークです。新興脅威のリスクを軽減し、リスク管理を強化し、日本の広範なサイバーセキュリティ指標に整合させるための構造化されたガイダンスを提供しています。

3省2ガイドラインは、厚生労働省、経済産業省、総務省の3省が発行する2つのセキュリティガイドラインから構成されます。

1 医療情報システムの安全性管理に関するガイドライン 第 6 版

厚生労働省発行の当該ガイドラインは、医療情報システムを安全かつ適切に運用するための指針を示したものです。

詳細

2 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 1.1 版

経済産業省、総務省発行の当該ガイドラインは、医療情報を管理するITサービスの提供事業者の安全な運用の確保に重点を置いています。

詳細

3省2ガイドラインのフレームワークは、医療データの保護に重点を置いているため、個人情報保護法と密接に関連しています。個人情報保護法は、すべての業界における一般的なデータ保護義務を定めている一方で、3省2ガイドラインは医療情報を取り扱う組織に対して、サイバーセキュリティやリスク管理に向けた具体的な対策を提供しています。

3省２ガイドラインの適用対象

個人情報保護法の規定では、データ処理に関して、個人情報取扱事業者、委託先、下請け業者という 3 つの主な役割が定義されています。これらの分類により、医療情報の取り扱いにおける責任とサイバーセキュリティ要件を整合させることで、どの組織が3省２ガイドラインを適用すべきかを判断できます。

- **個人情報取扱事業者** とは、病院や医療提供者（診療所、薬局、助産院、訪問看護ステーション、介護提供者など）などの個人データの収集と管理を担当する主な組織を指します。3省2ガイドラインにより、患者情報を保護するために包括的なサイバーセキュリティガバナンス、リスク管理ポリシー、および技術的な保護対策を実践することが求められいます。
- **委託先**とは、個人情報取扱事業者の代理として個人データを取り扱う組織または個人を指します。たとえば、患者記録を保管し管理するクラウドベースの電子カルテ（EHR）プラットフォームは、厳格なアクセス制御、暗号化ポリシー、サイバーセキュリティインシデント対応メカニズムを強化することで、３省2ガイドラインに準拠する必要があります。
- **再委託先**とは、ソフトウェア開発者、インフラプロバイダー、データプロセッサなど、サプライチェーンの下流にある第三者ベンダーを指します。患者データを直接管理していない場合でも、サプライチェーン全体で医療情報の完全性と機密性を確保するために3省2ガイドラインのセキュリティ要件に従う必要があります。

個人情報保護法の役割に基づく分類を統合することで、3省2ガイドラインにより、医療データ処理に関わる各組織が高いサイバーセキュリティ基準を遵守することを保証する体系的なコンプライアンスモデルが構築されます。3省2ガイドラインにおけるコンプライアンスの最終的な責任は、機密医療データの収集、保存、保護を直接管理し監督するため、病院や医療機関などの個人情報取扱事業者が担っています。ただし、この責任は、IT サービス提供者などの委託先と共有されます。委託先は、個人情報取扱事業者の代理としてデータ処理する際に必要となるサイバーセキュリティコントロールを実装することが求められています。同様に、再委託先は、サプライチェーン全体で医療情報の完全性を維持するために、関連するセキュリティ対策を確実に遵守する必要があります。

3省2ガイドラインの適用方法

3省２ガイドラインの適用は、日本の医療情報システムを管理する組織にとって、根本的かつ重要な段階となります。第 1 のガイドラインは、医療データを取り扱うすべての情報システムに広く適用されます。 第 2 のガイドラインは、電子カルテ（EMR）、クラウドベースの EMR サービス、オンライン医療相談システムなどの医療情報の外部保管設備サービス提供者を対象にしています。このため、このフレームワークでは、医療業界内でサイバーセキュリティのレジリエンスを強化するためのベストプラクティス、コンプライアンス要件、およびガバナンス構造が概説されています。

第 1 段階

第一段階は、医療データ処理プロセスにおける自社の立場と役割を理解することにあります。これは非常に重要です。なぜならば、その理解がなければ、コンプライアンスを主張することはできず、他の当事者が要求事項を遵守していると仮定することもできないからです。こうした理解を得るためには、次の質問に答えることが有効です。

- 貴社は医療提供者、医療機関ですか？医療データを扱うシステム提供者ですか、それとも第三者のサービス提供者ですか?
- 処理する医療データの種類と処理の目的（患者記録、診断情報、保険データ、医療機器テレメトリなど）は？
- 医療情報を保管、送信、または分析していますか？各フェーズでのセキュリティ責任はどのようになっていますか？
- 既に運用に適用している規制は何ですか（例: 個人情報保護法、医師法、または関連する経済産業省および厚生労働省のガイドライン）？
- 貴社は、情報セキュリティ管理に直接的に責任を担っていますか？それとも コンプライアンス遵守を第三者のサービスに依存していますか?

第 2 段階

取り扱うデータに対する役割を明確にしたら、3省2ガイドライン要件に対するコンプライアンスを確認する第二段階へ進むことができます。厚生労働省、経済産業省、総務省の3省では、コンプライアンスを評価するために使用できる FAQ とチェックリストを公開しています。私の個人的な提案は、「別紙２　統合前ガイドラインにおける対策項目一覧と医療情報安全管理ガイドライン6.0 版の対応表」 から始めることです。この対応表は、両方のガイドラインの要件を明確かつ包括的にリストアップし、状況に応じてコンプライアンスの主要条件としてどちらのガイドラインを選択すべきかを判断するための独自の視点を提供しています。各要件を分析する際には、医療データ管理における自社の役割にどのように適用されるかを常に念頭に置く必要があります。

第 3 段階

最後の段階は、特定したギャップを埋めることと、すべての項目がポリシーや手順に従って実行されていることを継続的に監視することです。

3省2ガイドラインの詳細要件

別紙 2 によると、要件は 3 つの大項目に分類されています。

人的・組織的

これらの管理は、組織的安全性と人的安全性に関連しています。

- **組織的安全性:** 事業継続計画（BCP）、リスク管理、規制フレームワークの遵守などのセキュリティ管理を統括する組織構造の確立、運用、文書化が含まれます。
- **人的安全性:** 機密情報の保持、セキュリティ意識向上トレーニングの実施、およびアクセス制御ポリシーの遵守を従業員に求め、不正なデータ露出を防止します。

物理的対策

データセンター、重要な IT インフラ、医療用保管設備へのアクセスを制限するために、施錠、生体認証などの物理的アクセス制御を実施するとともに、環境セキュリティ対策を講じます。

技術的対策

この大項目では、認証、認可、特権管理などのデジタルアクセス制御に加え、ログ管理、暗号化、データ漏えい防止（DLP）、脆弱性管理、侵入検知・防御システム（IDS/IPS）、継続的な脅威監視などの高度なサイバーセキュリティ対策を実施します。

特筆すべき点として、当該ガイドラインはISO/IEC 27001:2002 附属書 A の管理策分類に準拠しています。

3つの大項目全体で、3省2ガイドラインの取り組みを進めるために、次の点に重点を置くことが強く推奨されます。

1. リスクベースのセキュリティガバナンス

- 規制要件に合致するセキュリティガバナンスのフレームワークを定義します。
- 情報セキュリティ管理の役割と責任を割り当てます。
- 進化するサイバーセキュリティ脅威を評価するリスク管理プロセスを確立し、維持します。

2. アクセス制御および ID 管理

- ロールベースのアクセス制御（RBAC）と多要素認証（MFA）を実装します。
- 特権管理ポリシーを定義して、管理者のアクセスを制限します。
- システムアクセスを追跡するため、定期的なアクセスレビューおよび監査ログの確認を実施します。

3. データ保護と暗号化

- 機密医療データを転送中と保存時の両方で暗号化します。
- 機密情報の取り扱いに関するデータ分類ポリシーを導入します。
- 不正な転送を防止するために、データ損失防止（DLP）対策を実施します。

4. インシデント対応と事業継続性

- セキュリティインシデント対応計画（SIRP）を策定し、セキュリティ侵害を処理します。
- 障害発生時のシステム可用性を確保するため、災害復旧（DR）計画を策定/維持します。
- サイバーセキュリティの定期的な訓練と侵入テストを実施します。

5. 継続的な監視と脅威検出

- セキュリティインシデントおよびイベント管理（SIEM）ソリューションを導入し、リアルタイムの脅威検出を実現します。
- ワークステーションおよびモバイルデバイスの脅威を監視・軽減するため、エンドポイント検出・対応（EDR）ソリューションを導入します。
- 定期的に脆弱性診断と侵入テストを実施します。
- セキュリティの脆弱性に対応するため、パッチ管理を自動化して維持します。

6. 第三者およびベンダーリスク管理

- 第三者リスク管理（TPRM）フレームワークを確立し、外部ベンダーやサプライヤーのセキュリティリスクを評価します。
- ベンダーのオンボーディング前に、セキュリティ評価、監査、および認証（例：ISO 27001、SOC 2、NIST CSF）を要求します。
- データ保護契約（DPA）やインシデント対応義務を含む契約上のセキュリティ条項を導入します。
- 定期的な監査、コンプライアンスレビュー、脅威インテリジェンスフィードを通じて、ベンダーのセキュリティ状況を継続的に監視します。
- 第三者の担当者に対してアクセス制御の制限を適用し、最小権限アクセスの原則を確実に守ります。

一覧表にあるすべての項目が重要ですが、特にサプライチェーンセキュリティに関する 6 番目のポイントが現在における重要トピックとなっています。確立された標準に準拠していることを示すことは、サプライチェーンの両側にとって信頼を築く上で極めて重要となります。

このことが 3省2ガイドラインの適用に関して最終的な疑問を提起します。企業が本ホワイトペーパーで議論されているすべての対策を実施した後、3省2ガイドラインに準拠していることをどうすれば証明できるのでしょうか？

現在、3 省庁からの 3省2ガイドラインに対して公式の認証制度はありません」。しかし、これらのガイドラインは、国際的に認められた標準、特に ISO/IEC 27001、27017、27018 と密接に整合する形で開発されています。

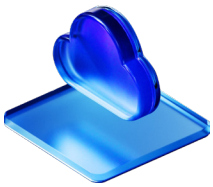
したがって、最も実践的かつ効果的で市場で認知されているアプローチは、ISO/IEC 27001 ファミリーの標準に対する資格を有し、独立し、認定された監査人から認定を取得することです。組織は 3省2ガイドライン管理を対応する ISO 管理にマッピングすることで、国際的に認められた認証フレームワークを活用しながら、コンプライアンスを確保することができます。

3省2ガイドラインへのAcronis Cyber Protect適用

Acronis Cyber Protect は、バックアップをサイバーセキュリティおよびエンドポイント管理とネイティブに統合し、3省2ガイドラインで要求されるエンドツーエンドのサイバーレジリエンスを提供します。

- **データ保護とバックアップソリューション:** 暗号化されたバックアップにより患者データを保護し、データ保持ポリシーのコンプライアンスを確保します。
- **エンドポイントセキュリティと脅威インテリジェンス:** AIセキュリティソリューションにより、医療記録をサイバー脅威から保護します。
- **インシデント対応とリカバリ:** 迅速な対応メカニズムにより、侵害を軽減し、ビジネス継続性を確保します。

コントロールと共有責任の観点から、ニーズに合わせてオンクラウドとオンプレミスのどちらの導入も可能です。



クラウド

日本政府は、クラウドの採用を積極的に支持しており、デジタル庁の創設や日本初のクラウド指針の導入からもそのことが見てとれます。

信頼できるパートナーと連携してクラウドを展開することで、3省2ガイドラインの要件を遵守し、医療データ保護のサイバーセキュリティ態勢を強化しながら、共有責任を果たすことができます。

Acronis Cyber Protect のクラウドベースの導入により、医療データに対するコスト効率の高い、管理しやすい、包括的なサイバープロテクションソリューションが提供されます。

オンプレミス

オンプレミスの導入では、企業データ、ライセンス、および IT リソースを直接管理することが優先されます。このソリューションは、拡張されたカスタマイズ、パフォーマンス、統括機能を提供するとともに、包括的なセキュリティとバックアップ機能を備えています。

Acronis Cyber Protect は、エアギャップ環境にも導入可能なため、ネットワークから完全に切り離されたシステムでも、監視、バックアップ、完全リストアを 1 クリックで実行できます。

アクロニスのサイバーセキュリティ態勢

アクロニスは、継続的なリスク評価に基づいて、人的、組織的、物理的、技術的な管理策を組み込んだ包括的な情報セキュリティおよびコンプライアンスプログラムを維持しています。

このプログラムが確実に効果を発揮するために、アクロニスは継続的な監視を実施するとともに、確立されたセキュリティ標準への準拠を検証するために内部および外部監査を行っています。このプロアクティブなアプローチにより、アクロニスはセキュリティプログラムのパフォーマンスを評価し、継続的に改善することによって新興の脅威に迅速に対応できます。

アクロニスは、ISO/IEC 27001、27017、27018、ISO 9001、および PCI-DSS の認証を取得しています。SOC 2 Type II レポートは、Acronis Trust Center で入手できます。

ACRONISトラストセンター

アクロニスは、安全なソフトウェア開発ライフサイクル（S-SDLC）に従い、初期の開発ステージからサイバーセキュリティの要素を組み込み、セキュリティバイデザインとプライバシーバイデザインのアプローチを確実に実践しています。主な特徴は以下の通りです。

- セキュアな設計と開発のためのベストプラクティスの実践。
- 脅威モデリングを使用した、セキュリティおよびプライバシーデザインのレビュー。
- CI/CD パイプラインに統合された自動静的コード解析（SAST）とセキュリティ部品表（SBOM）により、開発者にリアルタイムのセキュリティフィードバックを提供。
- 継続的なサイバーセキュリティ意識向上トレーニングにより、強固なサイバーセキュリティ文化を醸成し、新興の脅威に対してチームが警戒を維持。

Acronis Threat Research Unit（TRU）は、アクロニスのサイバーセキュリティプロフェッショナルのチームであり、マルウェア、ランサムウェア、フィッシング、持続的標的型攻撃（APT）など新興のサイバー脅威に対する詳細な調査と分析に重点を置いています。TRU の公開資料とアップデートは、TRU Security by Acronisを参照願います。

アクロニスは 2018 年から HackerOne でバグ報奨金プログラムを運用しており、セキュリティコミュニティと緊密に連携しながら、外部の研究者とも協力しています。

CVE Program のパートナーである　アクロニスは、CVE 番号付与機関（CNA）であり、当社のすべての製品に関する公開されたサイバーセキュリティ脆弱性を CVE レコードとして発行する責任を担っています。セキュリティアドバイザリとアップデートについては、Acronis Security Advisory Databaseを参照願います。

アクロニスは、自社の安全なクラウドサービスが 3省2ガイドラインを遵守していることを表明しています。このトピックに関する アクロニスのコンプライアンスについて、詳しくは、Trust Centerの3省2ガイドラインのページを参照願います。

アクロニスについて

アクロニスは、マネージドサービスプロバイダー（MSP）、中小企業（SMB）、および大企業の IT 部門向けに、ネイティブに統合されたサイバーセキュリティ、データ保護、およびエンドポイント管理を提供するグローバルなサイバープロテクション企業です。Acronis の効率性に優れたソリューションは、最小限のダウンタイムで最新のサイバー脅威を特定、防止、検出、対応、修復、リカバリし、データの完全性とビジネスの継続性を確保するように設計されています。アクロニスは、多様で分散したIT環境のニーズを満たす独自の機能により、MSP 向けに市場で最も包括的なセキュリティソリューションを提供しています。

2003 年にシンガポールで設立された、スイスの企業であるアクロニスは、全世界に 45か所の拠点を有しています。Acronis Cyber Protect Cloud は、150か国に 26 言語で提供され、2 万社を超えるサービスプロバイダーで利用されており、75 万社を超える企業を保護しています。

筆者について

Christian Nicita（ISO 27001 LA、CCSK）は、20 年以上にわたるサイバーセキュリティの経験を有し、サイバーセキュリティのガバナンス、リスク管理、コンプライアンスに関する専門家として知られています。トップクラスの企業で要職を歴任し、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 などの国際セキュリティ標準の導入を成功裏に主導しました。

アクロニスのサイバーセキュリティガバナンス、リスクおよびコンプライアンスのスペシャリストとして、セキュリティポリシーの定義、リスク軽減戦略の推進、脅威モデリングの実施、および GDPR、ENS、2G3M などの主要な規制フレームワークのコンプライアンスの確保において重要な役割を果たしています。

アプリケーションセキュリティ、侵入テスト、セキュアソフトウェア開発において深い技術的基盤を有し、セキュリティ戦略と技術実装の間のギャップを埋め、新興のサイバー脅威に対するレジリエンスを実現しています。通信、公共事業、銀行、クラウドサービスのグローバル企業にサイバーセキュリティのアドバイザリーサービスを提供し、セキュリティ態勢とコンプライアンスの準備状況を向上させています。

付録 A: 3省2ガイドラインの共有責任対応表

3省2ガイドラインの共有責任対応表は、医療データを扱う各組織ごとのサイバーセキュリティおよびコンプライアンス上の責任範囲を明確にしたものです。これにより、すべての関係者がセキュリティと規制遵守の維持における自身の役割を理解することができます。

役割	3省2ガイドラインで求められる責任
個人情報取扱事業者	包括的なサイバーセキュリティのガバナンス、リスク管理、コンプライアンスフレームワークを確立し、統括します。患者データを保護するために、暗号化、アクセスコントロール、インシデント対応などの対策を講じます。第三者がセキュリティ標準を確実に遵守するよう導きます。
委任先	個人情報取り扱い事業者に代わって医療データを処理する場合は、セキュリティコントロールを徹底して導入します。データ保護プロトコルのコンプライアンスを確保し、定期的なセキュリティ評価を実施し、堅牢なインシデント対応戦略を維持します。
再委託先	3省2ガイドラインセキュリティ要件を遵守することで、サイバーセキュリティ対策を支えます。個人情報取り扱い事業者および委託先が確立したリスク管理プロトコルに従い、データセキュリティ制御を実装し、システムの完全性を確保します。

この対応表は、医療データの取り扱いに関与するすべての組織において、責任の整合性を図り、一体的なセキュリティアプローチを推進するための参照基準となるものです。