セキュリティクリアランス制度への対応について

MedCSC 情報保護・アクセス適格性確認内規

項目	内容
文書番号	MedCSC-SC-2026-01
分類	TLP:AMBER+STRICT（内部限り。必要性のある役職員・委託者・関係者に限定）
版	第 1.0 版（2026 年 5 月 30 日更新）
施行日	2026 年 6 月 3 日（理事会承認日として運用開始予定）
所管	理事会／事務局／情報保護責任者
適用対象	理事、監事、職員、事務局、外部委託者、ボランティア、会員・共同研究者その他 MedCSC 情報を取り扱う者

重要な位置付け
本内規は、政府が付与する公的なセキュリティクリアランスを MedCSC が独自に付与するものではない。MedCSC 内部における情報保護、アクセス制御、委託・共同研究・会員連携時の信頼確保を目的とする「内部アクセス適格性確認」の規程である。
政府、行政機関、委託元又は共同研究先から、法令・契約・ガイドラインに基づくより厳格な取扱いを求められる場合は、それらを優先する。

改定要旨

2023 年 8 月版の検討文書は、制度準備段階における簡易な論点整理であった。本版では、2026 年時点の MedCSC の活動内容、公益社団法人化に向けたガバナンス、サイバー脅威情報共有、HCARE シリーズ、医療機関インシデント訓練、政府・会員・共同研究先との連携を前提に、正式な内規として実運用できる水準まで更新した。

特に、従前文書に含まれていた「米国基準に基づく案」は、そのままでは日本法上の個人情報保護・差別防止・目的外利用防止の観点で不十分であるため、本版では日本の特定秘密保護制度の適性評価項目を参照しつつ、MedCSC の民間団体としての権限範囲に合わせて、本人同意、必要最小限、目的限定、苦情・再審査の仕組みを明文化した。

主な更新点	内容
制度の位置付けを明確化	MedCSC は政府 SC を付与しない。内部のアクセス適格性確認制度として、Need-to-Know、最小権限、TLP、契約上の守秘義務を組み合わせて運用する。
情報区分を整備	公開情報、内部情報、TLP:GREEN、TLP:AMBER、TLP:AMBER+STRICT、TLP:RED、MedCSC 重要管理情報（MCI）を整理した。
適格性確認を人権・個人情報保護に適合	本人同意、目的限定、必要最小限、センシティブ情報の原則不取得、不服申立て、記録管理を明文化した。
システム・物理環境を対象化	人的確認だけでなく、クラウド、端末、ログ、AI 利用、印刷、保管、会議、委託先を含めた統制を定義した。
実装計画を追加	30 日、60 日、90 日、180 日の導入ロードマップを明記し、理事会で管理できる形にした。

第 1 章　総則

第 1 条（目的）

本内規は、一般社団法人医療サイバーセキュリティ協議会（以下「当協議会」又は「MedCSC」という。）が、医療機関、医療情報ベンダー、医療機器ベンダー、行政機関、会員、共同研究先その他の関係者から取得し、又は生成する機微なサイバーセキュリティ関連情報を適切に保護するため、情報区分、アクセス適格性確認、物理・システム管理、委託管理、インシデント対応及び違反時措置を定めるものである。

本内規の最終目的は、医療を利用する患者の安全と安心を守り、医療機関等におけるサイバーセキュリティリスクを実効的に低減するための信頼基盤を確立することにある。

第 2 条（基本原則）

1. Need-to-Know：役職、地位、会員資格又は理事資格のみをもって情報アクセスを認めない。業務上の必要性がある範囲に限定する。
2. 最小権限：情報、システム、会議、保存領域、AI ツール及び印刷物へのアクセス権は、目的達成に必要な最小限とする。
3. 本人同意と目的限定：適格性確認において個人情報を取得する場合は、原則として本人の同意を得て、利用目的を明示し、目的外利用を禁止する。
4. 契約・法令優先：行政機関、委託元、共同研究先又は会員企業が定める秘密保持義務、情報区分、再委託制限、ログ保存、報告義務がある場合は、それらを優先する。

5. TLP と正式な秘密指定の峻別：TLP は共有範囲を示す実務ラベルであり、政府による秘密指定又は法定のクリアランスそのものではない。
6. 患者安全・公共利益の尊重：情報保護は、医療提供体制の維持、患者安全、国民保護、重要インフラ防護のために行う。過度な秘密化により必要な防御情報共有を妨げてはならない。

第 3 条（適用範囲）

本内規は、当協議会の理事、監事、顧問、職員、事務局、外部委託者、ボランティア、会員の担当者、共同研究者、講師、受講者、訓練参加者、システム開発者、クラウド運用者その他当協議会の管理対象情報にアクセスする者に適用する。

対象情報には、紙媒体、電子ファイル、電子メール、チャット、会議録、録音・録画、ログ、ソースコード、設定情報、脆弱性情報、AI プロンプト・出力、HCARE 評価結果、インシデント訓練記録、契約書、会員情報、個人情報、医療機関のセキュリティ態勢に関する情報を含む。

第 4 条（用語の定義）

用語	定義
政府 SC	政府又は行政機関が、法令に基づき、特定の秘密情報又は重要情報にアクセスする者について適性評価等を行い、アクセスを認める制度。MedCSC が独自に付与するものではない。
内部アクセス適格性確認（MAE）	MedCSC の管理対象情報にアクセスする者について、本人同意、守秘義務、役割、教育受講、利益相反、情報取扱実績等を確認し、内部アクセス権を付与・維持・停止する手続。
MCI（MedCSC Controlled Information）	MedCSC が独自に管理する重要情報。サイバー脅威情報、医療機関の弱点、HCARE 評価結果、インシデント訓練資料、未公開の政策提言、会員機密、個人情報等を含む。
TLP	Traffic Light Protocol。情報の共有可能範囲を示すラベル。TLP:RED、TLP:AMBER、TLP:GREEN、TLP:CLEAR 等を用いる。
MCI 取扱システム	MCI を保存、処理、送信、分析又はバックアップするクラウド、端末、SaaS、AI 環境、リポジトリ、ログ基盤その他の情報システム。
MCI 取扱区域	MCI を閲覧、印刷、保管、議論又は廃棄する会議室、事務局区画、保管庫、イベント会場、オンライン会議室等。

第 2 章　情報区分と取扱い

第 5 条（情報区分）

当協議会は、情報の性質、開示範囲、漏えい時の影響、契約上の制約に応じて、次の区分を用いる。区分は情報作成者又は情報オーナーが設定し、必要に応じて情報保護責任者が見直す。

区分	例	共有範囲	主な管理策
PUBLIC / TLP:CLEAR	Web 公開資料、公開済み活動報告、公開セミナー告知	制限なし。ただし著作権・引用条件に従う。	公開前レビュー、個人情報・機密情報の除去
INTERNAL	理事会準備資料、事務局手順、未公開の事業計画案	MedCSC 内部及び業務上必要な委託先	アクセス制御、社外転送制限、最新版管理
TLP:GREEN	業界啓発用の脅威傾向、一般化した教訓	定義された医療サイバーコミュニティ内。公開 Web 掲載は禁止。	出典確認、再共有条件の明示
TLP:AMBER	医療機関支援に必要な限定情報、会員向け注意喚起	受領組織内及び必要性のある顧客・支援対象に限定	Need-to-Know、転送時の TLP 明示
TLP:AMBER+STRICT	会員機密、HCARE 評価結果、訓練シナリオ、未公開契約情	受領組織内の必要者に限定。外部再共有不可。	MAE-2 以上、MFA、ログ、暗号化、印刷制限

区分	例	共有範囲	主な管理策
	報		
TLP:RED / MCI-Restricted	実インシデントの詳細、未修正脆弱性、認証情報、攻撃手順、政府・契約上の高度機密	明示された受領者のみ。原則再共有不可。	MAE-3 以上、個別承認、保管場所限定、会議録・録画の原則禁止
法令・契約指定情報	行政機関又は委託元が指定する特定秘密、重要経済安保情報、契約上の秘密情報等	法令・契約・行政機関の指示に従う。	MedCSC 内規ではなく、当該法令・契約の統制を優先

第 6 条（ラベリング及び保存）

7. MCI を含む文書、メール、チャット、会議招集、共有フォルダ、資料名には、可能な限り情報区分を明示する。
8. TLP 表示を用いる文書は、ヘッダー又はフッターに TLP ラベルを表示し、共有範囲を本文又は送付文で明示する。
9. MCI-Restricted は、個人端末、私用クラウド、個人メール、個人 SNS、許可されていない生成 AI、無承認のファイル転送サービスに保存又は入力してはならない。
10. 共有リンクは、原則として組織アカウント限定、期限付き、ダウンロード制限又は閲覧限定とし、アクセスログを取得できる方法を優先する。

第 7 条（情報オーナー）

各プロジェクト、WG、訓練、共同研究、会員支援、政策提言、HCARE 評価、システム開発について、担当理事又は事務局長は情報オーナーを定める。情報オーナーは、情報区分、共有範囲、保管場所、保存期間、廃棄方法、再共有可否を決定し、アクセス権の棚卸を行う。

第 3 章　内部アクセス適格性確認（MAE）

第 8 条（MAE の段階）

区分	対象情報・権限	必要条件	承認者
MAE-0	公開情報、公開イベント資料	利用規約・著作権の遵守	不要
MAE-1	内部情報、一般的な事務局資料、TLP:GREEN	守秘義務への同意、組織アカウント、基本教育	事務局長又は担当理事
MAE-2	TLP:AMBER、TLP:AMBER+STRICT、会員機密、HCARE 評価、医療機関支援資料	NDA、利益相反確認、情報取扱教育、MFA、業務上必要性の確認	担当理事及び情報保護責任者
MAE-3	TLP:RED、MCI-Restricted、実インシデント詳細、未修正脆弱性、認証情報、政府・防衛・重要インフラ関連の高感度資料	MAE-2 条件に加え、個別案件ごとの必要性、追加誓約、アクセスログ、期間限定権限、理事会又は代表理事承認	理事会又は代表理事
Gov-SC / Contract-SC	行政機関又は契約元が指定する法定・契約上の秘密情報	行政機関・契約元の制度、適性評価、施設・システム要件に従う	行政機関・契約元

第 9 条（適格性確認の対象）

MAE-2 以上の情報にアクセスする者は、内部アクセス適格性確認を受けなければならない。理事、監事、顧問、会員代表、講師、委託者であっても、当該情報への業務上の必要性及び本内規への同意が確認されない限り、アクセスを認めない。

第 10 条（確認項目）

MedCSC 内部で実施する確認は、本人の同意を前提に、業務上必要な範囲に限定する。日本の特定秘密保護制度における適性評価項目を参考にしつつ、民間団体である MedCSC の権限範囲に合わせ、原則として自己申告、契約書、研修受講記録、アクセスログ、業務実績、利益相反確認を中心とする。

確認領域	確認内容	運用上の注意
本人・所属確認	氏名、所属、役割、連絡先、契約又は参加根拠、組織アカウント	本人確認資料の写しは必要最小限とし、不要になったら廃棄する。
守秘義務・教育	NDA 締結、本内規同意、情報区分・TLP・インシデント報告教育の受講	教育未受講者には MAE-2 以上を付与しない。
利益相反・外部活動	競合事業、委託関係、外部役職、会員企業との利害関係、研究費・報酬関係	利益相反はアクセス禁止のためではなく、開示・管理・回避策設定のために確認する。
外国からの不当な影響リスク	外国政府・軍・国有企業等との契約、資金、指揮命令、機密保持義務の競合可能性	国籍、出身、思想信条による差別的取扱いをしてはならない。具体的な利害・義務・リスクに限定する。
犯罪・懲戒・情報取扱非違	情報漏えい、無断持出し、不正アクセス、守秘義務違反、懲戒歴に関する自己申告	詳細確認は業務必要性と本人同意に限定し、法令・雇用慣行に反する照会を行わない。
経済的リスク	重大な利益相反、反社会的勢力との関係、金銭的脆弱性が情報漏えいリスクを生む場合の自己申告	信用情報の取得は原則行わない。契約上又は法令上必要な場合のみ、本人同意と最小限で実施する。
IT 利用状況	MFA 設定、端末管理、パスワード管理、許可外クラウド・生成 AI 利用の有無、ログ遵守	監視は業務アカウント・業務端末・業務システムに限定する。私的領域への過度な介入を禁止する。

第 11 条（取得してはならない情報・慎重取扱情報）

11. 思想信条、政治的意見、宗教、労働組合活動、性的指向・性自認、家族構成、出身地、民族、疾病・障害・精神疾患に関する詳細情報は、法令又は契約上明確に必要な場合を除き、内部適格性確認の評価項目として取得してはならない。
12. 健康情報、精神疾患、薬物・アルコールに関する情報は、法令又は契約上必要で、かつ本人同意があり、業務上の安全・情報保護リスクとの合理的関連性がある場合に限り、必要最小限で取り扱う。
13. 家族、同居人、交友関係に関する調査は、MedCSC 内部の MAE では原則として行わない。行政機関又は契約元の法定制度で求められる場合は、当該制度に従う。

第 12 条（手続）

手順	内容	期限・記録
申請	情報オーナー又は担当理事が、対象者、必要な情報区分、目的、期間を記載して申請する。	アクセス開始前
本人同意	対象者に利用目的、確認項目、保存期間、苦情窓口、不同意時の取扱いを説明し、同意を取得する。	同意書又は電子記録で保存
確認	NDA、教育、利益相反、IT 要件、必要性、役割を確認する。MAE-3 は追加誓約と個別承認を行う。	確認票を保存
承認	承認者がアクセス範囲、期間、保管場所、再共有可否を決定する。	アクセス管理台帳に記録
付与	システム管理者が最小権限でアカウント・グループ・フォルダ権限を付与する。	付与ログを保存
棚卸	情報オーナーは、MAE-2 以上について少なくとも四半期ごとにアクセス権を棚卸する。	棚卸記録を保存
停止・取消	役割変更、契約終了、違反、必要性消滅、本人申出、リスク顕在化時は速やかに停止する。	停止理由と実施日時を記録

第 13 条（有効期間）

MAE-1 及び MAE-2 の有効期間は原則 1 年とする。MAE-3 は案件ごとに最長 6 か月を上限とし、継続する場合は再承認を要する。役割変更、所属変更、委託終了、退会、プロジェクト終了、情報漏えい又は重大な規程違反が発生した場合は、有効期間中であっても見直す。

第 4 章　物理・システム・AI 利用の管理

第 14 条（MCI 取扱区域）

14. MCI-Restricted を扱う会議又は作業は、参加者を事前登録し、無関係者の入室・傍聴・画面閲覧を防止する。
15. 紙資料は配布番号を付し、会議終了時に回収又は返却確認を行う。保管する場合は施錠可能なキャビネット等に保管する。
16. オンライン会議では、待機室、参加者認証、録画禁止、画面共有制限、チャット保存の可否を設定する。
17. イベント、セミナー、訓練会場では、公開可能資料と内部資料を分離し、会場掲示、投影、配布物に情報区分を明示する。

第 15 条（MCI 取扱システム）

統制領域	必須要件
アカウント	組織管理アカウントを原則とし、MFA を必須とする。共有アカウントは禁止する。
端末	OS・ブラウザ・EDR 等を最新化し、画面ロック、ディスク暗号化、管理者権限制限を行う。
保存	許可されたクラウド又はリポジトリに保存し、個人クラウド・個人メール・私用チャットへの保存を禁止する。
送信	共有リンクは受領者限定、期限設定、必要に応じたダウンロード禁止を用いる。暗号化ファイル送付時はパスワード別送を最低限とし、可能な限りアクセス制御型共有に置き換える。
ログ	MAE-2 以上の情報を扱うシステムでは、アクセス、ダウンロード、共有、削除、権限変更のログを取得し、必要期間保存する。
バックアップ	MCI を含むバックアップにも同等のアクセス制御と保存期間を適用する。
脆弱性管理	MCI 取扱システムは、定期的なパッチ適用、設定確認、不要アカウント削除を行う。

第 16 条（生成 AI・AI 分析基盤の利用）

HCARE シリーズ、インシデントシミュレータ、BigQuery データレイクハウス、生成 AI、ログ分析、要約支援、文書作成支援等の AI 利用においては、入力データ、プロンプト、出力、学習・保存設定、外部送信先を管理対象とする。

18. MCI-Restricted、未修正脆弱性、認証情報、実インシデントの詳細、会員・医療機関の未公開情報を、承認されていない外部生成 AI サービスに入力してはならない。
19. AI 利用時は、可能な限り匿名化、仮名化、要約化、秘匿化を行い、医療機関名、担当者名、IP アドレス、認証情報、契約金額、未公開の弱点を直接入力しない。
20. AI 出力は、誤情報、過度な断定、機密情報の混入、攻撃手順の過剰具体化をレビューしてから共有する。
21. AI 環境のログ保存、学習利用設定、データ保持設定、国外移転、再委託先について、契約又は設定で確認する。

第 5 章　外部提供、委託、共同研究、会員連携

第 17 条（外部提供の原則）

MCI を外部に提供する場合は、情報オーナーが、提供目的、受領者、情報区分、TLP、再共有可否、保存期間、削除義務、インシデント時の連絡方法を明示する。TLP:AMBER+STRICT 及び TLP:RED の外部提供は、原則として情報保護責任者又は担当理事の事前承認を要する。

第 18 条（契約条項）

MAE-2 以上の情報を外部委託者、共同研究先、会員企業、講師、開発者、クラウド事業者等に提供する場合は、少なくとも次の事項を契約書、覚書、NDA 又は発注書に含める。

- 秘密情報及び MCI の定義、TLP 表示の遵守
- 利用目的の限定及び目的外利用の禁止
- 再委託・第三者提供の制限及び事前承認
- アクセス者の限定、教育、NDA、ログ管理
- MFA、暗号化、バックアップ、廃棄、返却
- インシデント又は漏えい疑義発見時の速やかな報告
- 契約終了時の返却・削除・証明
- 監査・説明・是正要求への協力
- 違反時の損害賠償、契約解除、アクセス停止

第 19 条（会員・共同研究先との情報共有）

当協議会は、医療業界全体の防御力向上のため、必要な範囲でサイバー脅威情報、教訓、訓練成果、HCARE 評価結果の一般化情報を共有する。ただし、特定の医療機関、患者、会員企業、製品、脆弱性、インシデントを識別できる情報は、情報オーナーの承認、受領者の Need-to-Know、契約上の根拠がある場合に限り共有する。

第 6 章　インシデント対応と違反時措置

第 20 条（報告義務）

MCI の紛失、誤送信、無断閲覧、無断ダウンロード、権限誤設定、私用クラウド保存、認証情報漏えい、フィッシング被害、端末紛失、生成 AI への不適切入力、契約先からの漏えい疑義を発見した者は、速やかに情報保護責任者又は事務局長へ報告しなければならない。

初動の目安
重大性が判断できない場合でも、まず報告する。報告遅延は二次被害を拡大させるため、責任追及よりも早期封じ込めを優先する。医療機関、行政機関、委託元、会員企業への通知要否は、契約・法令・影響範囲を確認して理事会又は情報保護責任者が判断する。

第 21 条（初動対応）

段階	対応
検知・報告	発見者は、何が、いつ、どこで、誰に、どの範囲で影響した可能性があるかを報告する。証拠

段階	対応
	を消さない。
封じ込め	共有リンク停止、権限停止、パスワード変更、トークン失効、端末隔離、誤送信先への削除依頼等を実施する。
影響評価	情報区分、個人情報・会員機密・医療機関機密の有無、契約上の通知義務、法令上の報告義務を確認する。
通知・報告	必要に応じて、理事会、監事、委託元、共同研究先、会員、個人情報保護委員会、行政機関、警察等への報告を行う。
再発防止	権限設定、教育、運用手順、契約条項、システム設定を見直す。

第 22 条（違反時措置）

本内規又は契約上の秘密保持義務に違反した者に対しては、違反の態様、故意・過失、影響範囲、再発可能性を踏まえ、次の措置を単独又は組み合わせて行う。

- 注意、再教育、誓約書の再提出
- アクセス権の一時停止又は取消
- プロジェクト、WG、訓練、会議からの除外
- 委託契約又は会員契約の停止・解除
- 損害賠償請求、原状回復、削除証明の要求
- 法令違反又は犯罪が疑われる場合の関係機関への相談・通報

第 7 章　個人情報保護、苦情・再審査、記録管理

第 23 条（個人情報保護）

適格性確認により取得した個人情報は、アクセス適格性の確認、権限管理、教育管理、インシデント対応、契約履行、法令・契約上必要な説明のためにのみ利用する。目的外利用、不要な第三者提供、過剰な保存、評価対象者への不利益な取扱いを禁止する。

個人情報の取得、利用、保管、削除、第三者提供、委託、漏えい時対応については、個人情報保護法、個人情報保護委員会のガイドライン、契約、MedCSC の個人情報保護方針に従う。

第 24 条（苦情・再審査）

適格性確認の結果、アクセス範囲、停止・取消、確認内容又は個人情報の取扱いについて不服がある者は、事務局長又は情報保護責任者に対して再審査を申し出ることができる。MAE-3 に関する再審査は、理事長、担当理事、監事又は理事会が必要な範囲で確認する。

第 25 条（記録管理）

記録	保存期間の目安	管理者
MAE 申請・承認記録	権限終了後 3 年	情報保護責任者／事務局
NDA・同意書	契約終了後 5 年又は法令・契約の定める期間	事務局
教育受講記録	最終受講から 3 年	事務局
アクセスログ	少なくとも 1 年。MCI-Restricted は必要に応じて 3 年	システム管理者
インシデント記録	解決後 5 年	情報保護責任者
棚卸記録	3 年	情報オーナー

第 8 章　運用体制と導入計画

第 26 条（責任体制）

役割	責任
理事会	本内規の承認、重大インシデント対応、MAE-3 の承認、例外承認、定期レビューを行う。
理事長	情報保護に関する最終責任者として、理事会の方針に基づき業務執行を統括する。
情報保護責任者	本内規の運用、教育、アクセス審査、インシデント初動、台帳管理、委託先確認を統括する。
事務局長	日常運用、NDA、教育記録、会員・委託者の管理、台帳更新を行う。
情報オーナー	個別情報の区分、共有範囲、保存期間、アクセス申請、棚卸、廃棄を管理する。
システム管理者	アカウント、MFA、ログ、共有リンク、バックアップ、端末・クラウド設定を管理する。
監事	必要に応じて、重要な情報保護統制、決算・事業報告に関連する内部統制の状況を確認する。

第 27 条（導入ロードマップ）

期限	実施事項	成果物
施行後 30 日以内	情報保護責任者、情報オーナー、MCI 取扱システム管理者を指名する。	責任者一覧、連絡先、暫定台帳
施行後 60 日以内	既存資料、共有フォルダ、クラウド、AI 利用、会員資料、HCARE 資料を棚卸し、情報区分を付与する。	情報資産台帳、アクセス権一覧
施行後 90 日以内	MAE-2 以上の対象者に NDA 再確認、教育、MFA 確認、アクセス権再付与を行う。	MAE 台帳、教育記録、権限棚卸記録
施行後 180 日以内	インシデント机上演習、委託先確認、生成 AI 利用レビュー、理事会への運用報告を行う。	演習記録、改善計画、理事会報告
以後毎年度	内規、アクセス権、教育、委託先、インシデント、法令・契約要求を見直す。	年次レビュー報告、改定履歴

第 28 条（例外管理）

業務上やむを得ず本内規の定めと異なる方法で MCI を取り扱う必要がある場合は、情報オーナーが理由、期間、代替統制、影響範囲を記録し、情報保護責任者又は理事会の承認を得る。緊急時に事後承認となった場合も、速やかに記録し、再発防止策を定める。

第 29 条（改定）

本内規は、法令、政府制度、契約要件、TLP 標準、個人情報保護法制、医療サイバーセキュリティに関するガイドライン、MedCSC の定款・事業計画、HCARE シリーズの運用状況に変更があった場合、又は重大インシデントが発生した場合に、理事会の承認を経て改定する。

附則

22. 本内規は、2026 年 6 月 3 日から施行する。ただし、理事会承認日が異なる場合は、理事会承認日を施行日とする。
23. 2023 年 8 月の検討文書は、本内規の施行をもって廃止し、本内規に統合する。
24. 本内規の施行前に付与されたアクセス権は、施行後 90 日以内に本内規に基づき再確認する。

別紙 1　内部アクセス適格性確認票（MAE）

項目	記載欄
申請日	
対象者氏名・所属	
役割・参加プロジェクト	
必要な MAE 区分	MAE-1 / MAE-2 / MAE-3 / Gov-SC・Contract-SC
アクセス対象情報	
利用目的・期間	
NDA・同意書	締結済 / 未締結 / 不要（理由：　　）
情報取扱教育	受講済（年月日：　　） / 未受講
MFA・端末要件	確認済 / 未確認
利益相反・外部活動	なし / あり（管理策：　　）
追加条件	印刷禁止 / ダウンロード禁止 / 期間限定 / ログ確認 / その他
申請者	
承認者	
承認日・有効期限	

別紙 2　MCI インシデント一次報告様式

項目	記載欄
報告者・連絡先	
発見日時	
発生又は疑義の内容	誤送信 / 権限設定ミス / 紛失 / 端末紛失 / 不正アクセス / 生成 AI 入力 / その他
対象情報区分	INTERNAL / TLP:GREEN / TLP:AMBER / TLP:AMBER+STRICT / TLP:RED / MCI-Restricted / 不明
関係する相手先	医療機関 / 会員 / 委託先 / 行政機関 / 個人 / その他
含まれる可能性のある情報	個人情報 / 医療機関情報 / 会員機密 / 脆弱性情報 / 認証情報 / 契約情報 / その他
初動対応	共有停止 / 権限停止 / パスワード変更 / 削除依頼 / 端末隔離 / 未実施
外部通知の要否	要 / 不要 / 判断中
添付・証跡	
情報保護責任者判断	

別紙 3　参考資料

区分	資料名・位置付け
MedCSC 内部資料	2023 年 8 月版「セキュリティクリアランス制度への対応についての準備（内規）」
MedCSC 定款	令和 7 年度定款改定案。目的・事業、社員・会員、理事会、議事録、資産・会計、公告等のガバナンス根拠。
政府資料	内閣官房「Overview: Act on the Protection of Specially Designated Secrets (SDS)」適性評価、取扱者制限、罰則等の制度概要。
政府法令	特定秘密の保護に関する法律、重要経済安保情報の保護及び活用に関する法律、個人情報の保護に関する法律。
標準	FIRST Traffic Light Protocol (TLP) Version 2.0。TLP は共有範囲の表示であり、正式な秘密指定制度ではない。
監督機関資料	個人情報保護委員会「個人情報保護法等」「法令・ガイドライン等」「漏えい等の対応」。
医療サイバー運用文脈	HCARE 2.0、インシデントシミュレータ、JNSA 医療 IT WG、京都大学連携、厚生労働省関連事業へのアドバイザリー等。

別紙 4　改定履歴

日付	版	内容
2023 年 8 月	検討版	政府 SC 制度への対応準備として論点整理。
2026 年 5 月 30 日	第 1.0 版	法令・標準・MedCSC 現行事業に整合し、情報区分、MAE、TLP、物理・システム管理、AI 利用、委託、インシデント、個人情報保護、導入計画を含む正式内規案として全面改定。

承認欄

承認区分	氏名・役職	承認日	署名又は確認記録
作成	事務局／情報保護責任者		
確認	監事又は担当理事		
承認	理事会		

ファイル名 : MedCSC_セキュリティクリアランス制度対応内規_2026 最新版.docx
フォルダー : /Users/katsu/Library/Containers/com.microsoft.Word/Data/Documents
テンプレート : /Users/katsu/Library/Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
表題 : MedCSC セキュリティクリアランス制度対応内規 2026 最新版
副題 : Security clearance, information protection, internal access eligibility
作成者 : Medical Cyber Security Council / ChatGPT assisted draft
キーワード : MedCSC, SC, MAE, TLP, MCI, 情報保護
説明 : generated by python-docx
作成日時 : 2013/12/24 8:15:00
変更回数 : 3
最終保存日時 : 2026/05/30 18:44:00
最終保存者 : Katsuaki SUZUKI
編集時間 : 1 分
最終印刷日時 : 2026/05/30 18:44:00
最終印刷時のカウント
ページ数 : 11
単語数 : 9,933
文字数 : 1,710 (約)