RSA

ホワイト ペーパー

CJIS準拠のための強力な認証

RSA公共部門向けソリューション

犯罪司法情報サービス（CJIS）は、FBIの最大の部門です。CJISは、自動車登録、犯罪歴、銃器追跡、指紋記録などの機密性の高い情報を一元的に格納する、全国犯罪司法情報データベースを管理しています。CJISシステムは、法執行機関、国家安全保障局、情報活動コミュニティーのパートナーに、米国および米国民を保護するために必要な情報を提供します。CJISのポリシーでは、安全が確保されていない場所からCJISシステムにアクセスするすべてのユーザーに対して高度な認証を行うことが義務付けられています。

誰が影響を受けるか？

次の条件に当てはまるすべての組織が影響を受けます。

- CJIS情報システムにアクセスする組織。連邦、州、地方の政府機関や承認済みの民間請負業者を含みます

お客様にとってのリスクは何か？

- CJISコンプライアンス基準を遵守する義務がありますか？
- モバイル データ端末またはハンドヘルド デバイスからCJISシステムにアクセスする職員がいますか？
- ノートパソコンやモバイル デバイスからCJISへのリモート ユーザー アクセスをどのように保護していますか？
- リモート ユーザー アクセス向けの強力な認証として、多要素認証（MFA）を活用していますか？
- 最小権限の原則に基づくユーザー アクセス権の付与を監査、管理、保証できますか？

CJISのアクセス要件を満たす

- FBIの犯罪司法情報サービス（CJIS）部門のセキュリティ ポリシー バージョン5.8（2019年）[1]、第5.6.2.2.1項
- このポリシーに準拠することにより、システムの機密性の高い犯罪司法情報を保護するために、ユーザーが一貫したレベルのデータ セキュリティと暗号化を維持していることが保証されます

RSA SECURID® SUITE

オンプレミス、クラウド、モバイル向けの完全なアクセス ソリューション

アイデンティティーの保証
リスクベースのコンテキスト認識認証によってセキュリティと利便性を実現

選択肢の提供
幅広い多要素認証（MFA）方式により、ますます多様化するユーザーとユースケースをサポート

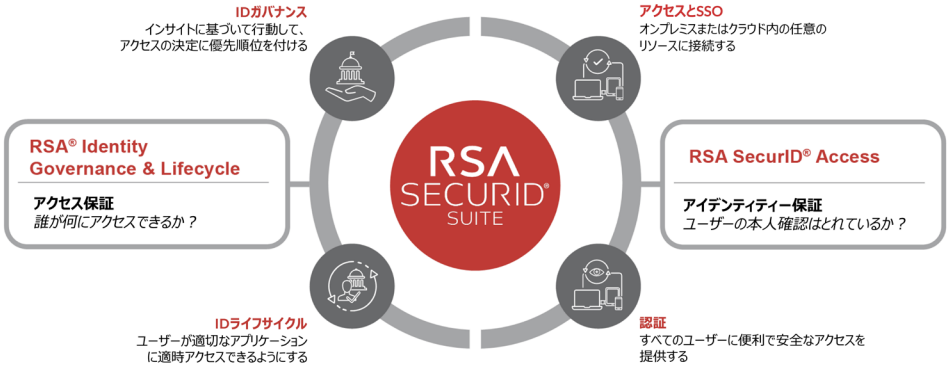
一貫性のあるアイデンティティー管理
クラウド、モバイル、オンプレミスのアプリケーション全体で一貫した可視性を提供し、アクセス ポリシーと認証ポリシーを適用

アクセス保証
誰がアクセスできるか、アクセス権が適切でポリシーおよび規制に準拠しているかどうかを把握

最小権限の原則に基づくアクセス ガバナンス
ユーザーが必要な情報にしかアクセスできないよう、最小権限の原則に基づいてアクセス権を管理

無料の試用版へのお申込み：
rsa.com/trysecurid

- CJISセキュリティ ポリシーでは、最小権限の原則に基づくアクセス制御が導入されていることを保証するために、アクセス権限を管理し、監査可能にすることも第5.5.2.1項で要求しています
- Identity Governance and Lifecycle Managementは、CJISへのアクセス権を持つユーザーを継続的に監視し、変更の監査証跡を提供するとともに、離職するユーザーまたはアクセスが不要になったユーザーのプロビジョニングを解除する上で必要となります
- コンプライアンス違反者は、CJISデータベースへのアクセス権をはく奪されたり、解雇されたり、場合によっては起訴される可能性があります



RSA SecurID Suiteは、アクセスおよびアイデンティティー保証を公共部門と民間部門の組織に提供します。組織は、誰が何にアクセスできるか、アクセス権は適切であり規則に準拠したものであるかを確認できるとともに、ユーザーがアクセスを試行したときにユーザーの本人確認を確信をもって行えるようになります。

RSA SecurID Suiteは、CJISの主要アクセス セキュリティ要件をサポートしているソリューションです。

RSAセキュア アクセス ソリューション

RSA SECURID ACCESS：

- CJISで要求されている2FAまたはMFAを提供します
- CJISで言及されている「高度な認証」方法を含んでいます
- ポリシー主導のリスクベースMFAを複数のユースケースに適用できます
  —モバイル プッシュおよびバイオメトリクス認証機能
  —ハードウェア、ソフトウェア、モバイル向けに最適化された認証システム、およびリスクベースの認証
- 認証情報を確実に保護し、許可されたユーザーにのみアクセスが許可されるようにします

公共機関および請負業者向けのアイデンティティーおよびアクセス保証

提供
業界をリードする多要素認証

保護

- 25,000以上の組織
- 5,500万人のユーザー

主要なユース ケースすべてにセキュリティを拡張

- クラウド
- モバイル
- BYOD
- Webポータル
- 従来のVPN
- その他...

アクセス制御

- その時々の状況のコンテキストまたはリスクに基づく
- アクセス権の見直しと権限の監査を自動化して、複雑性と手作業を軽減

詳細はこちら
rsa.com/ja-jp/accessthesolution

RSA IDENTITY GOVERNANCE AND LIFECYCLE：

- 最小権限の原則に基づくCJISシステムへのアクセスを管理
- 役割とポリシーに基づいてアクセス権をプロビジョニングおよびプロビジョニング解除し、監査証跡を維持
- 職務分掌のための適切なコントロールを適用

広範なリソース セットとの相互運用性を確保してミッションをサポート

RSA SECURID ACCESSは次の機能を提供します。

- 認証システムを使用した市場をリードする多要素認証であらゆるユースケースに対応
- テスト、ドキュメント化、認定が完了した、500以上のテクノロジー パートナーとのフルサポートの相互運用性に加え、さらに数千のテクノロジー パートナーとの標準ベースの相互運用性を確保
  ーCJISの最も一般的な統合機能の1つであるNetMotionの相互運用性を含みます
- 統合機能の完全なリストについては、rsa.com/ja-jp/partner/rsa-ready-programをご覧ください

RSA SECURID SUITEについて

RSA SecurID® Suiteは、デジタル環境全体のリソースへの便利でスムーズなアクセスを新世代のワークフォースに提供すると同時に、不正アクセスを防止します。このスイートは、ビジネス主導のセキュリティ ソリューションのRSAポートフォリオの一部であり、統合された可視性、自動化されたインサイト、調整されたアクションをベースにした、統合型のデジタル リスク管理アプローチを提供します。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上が成功し、革新的な変化に継続的に適応できるように支援しています。詳細はrsa.com/ja-jpをご覧ください。

1. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center