学術情報基盤オープンフォーラム 2025

学認AAL2認証器レジストリのご支援と今後の展望のご紹介

AXIES認証基盤部会・学認合同企画セッション

2025年6月17日

NRIセキュアテクノロジーズ株式会社

サイバーエンジニアリング事業本部

DevSecOps事業部

シニアセキュリティコンサルタント　佐甲 敦彦

目　次

これまでのご支援のご紹介

これまでの国立情報学研究所様へのご支援

認証器レジストリ構築に伴う一連の手続の整備のほか、認証器審査・リスク評価・コンテンツ英訳支援も実施

支援業務とその概要		令和4年度 12月-3月	令和5年度 11月-3月	令和6年度 1月-3月	令和7年度 以降
マイルストン				▼(2月) 国立情報学研究所様によるAPAN59での活動報告	
評価基準と運用フローの策定	NIST SP800-63およびKantara KIAF1440に基づいた**学認AAL2の認証器基準**を策定しました。 認証器レジストリによる**認証器評価の運用フロー**を策定しました。	・認証器評価基準 ・運用フロー			
認証器評価、IdP・IDaaS評価、認証器運用を含めたリスク評価、基準・運用フローのアップデート	基準に従い**認証器とIdP・IDaaSの評価を実施**しました。 また、運用も考慮した**学認での認証器にまつわるリスク評価**と関連文書アップデートを実施しました。		・OTP, FIDO, クライアント証明書評価結果 ・IdP,IDaaSの評価基準、評価結果 ・リスク評価結果 ・運用フロー		
追加の認証器に関する認証器評価・運用も含めたリスク評価・認証レジストリに関するコンテンツの英訳	OTP・経路外デバイスで**新たに追加される認証器の審査とリスク評価**を実施しました。 **学認コンテンツの英訳支援**を実施しました。			・追加されるOTP, 経路外デバイスの認証器評価結果 ・リスク評価結果 ・コンテンツ英訳	
パスキーの認証器およびパスワードマネージャの学認AAL2認証器レジストリへの追加	**パスキー**の認証器評価を実施する予定です。 また、学認が**パスワードマネージャ**を取り扱うための基準や審査、リスク評価、文書整備を実施予定です。				・パスキーの認証器の審査結果 ・パスワードマネージャの基準、評価結果、各種文書

学認AAL2認証器レジストリの公開コンテンツのご紹介

学認AAL2認証器レジストリの公開コンテンツのご紹介

- 学認AAL2認証器レジストリ（https://level2.gakunin.jp/）で認証器の評価結果やリスク評価を公開しています。

本ページのコンテンツはGitHubで管理されています。

言語選択が可能です。
(Japanese/English)

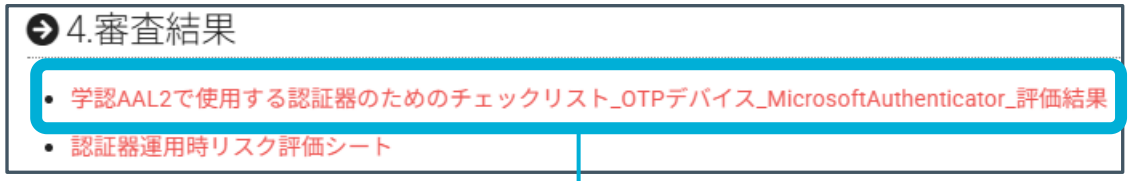
学認での運用も含めたリスク評価結果を公開しています。
今回はこちらを詳しくご説明します。

登録された認証器とその評価結果を公開しています。

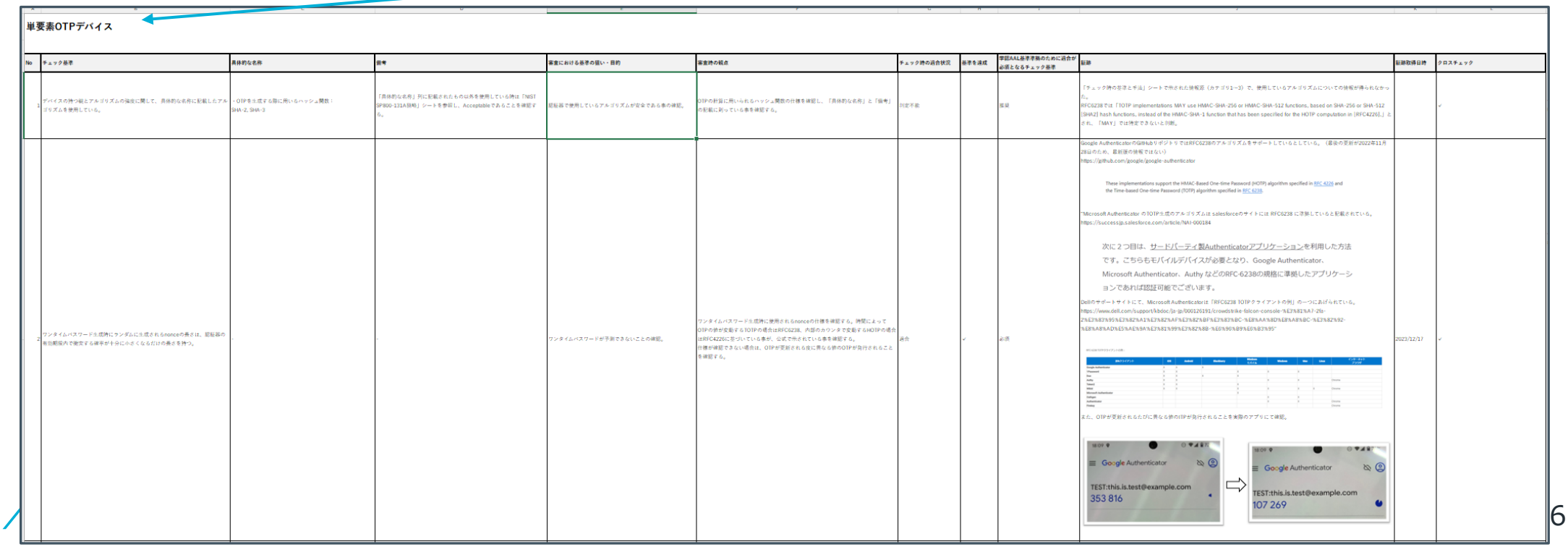
学認AAL2認証器レジストリの公開コンテンツのご紹介

認証器の「評価結果」のご紹介

登録済み認証器から認証器毎のページに遷移すると、「4.審査結果」にNIST SP800-63・Kantara KIAF1440に従った学認AAL2基準による評価結果のシートが配置されています。



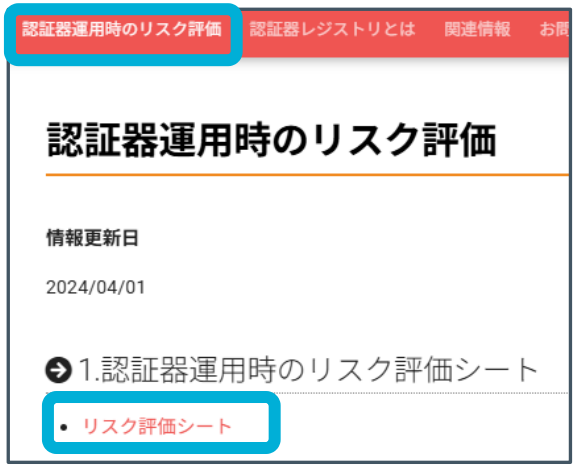
認証器評価のシート以外は、学認AAL2や評価の考え方の解説シートです。



学認AAL2認証器レジストリの公開コンテンツのご紹介

リスク評価のご紹介

「認証器運用時のリスク評価」のタブからリスク評価のページに遷移すると、学認利用の際の認証器運用にまつわるリスク評価の結果が配置されています。



対象

- **リスク評価の範囲の決定**：評価対象となる情報システムやデータの流れを可視化
- **資産の洗い出し**：対象となる情報システムの資産の洗い出し。

評価

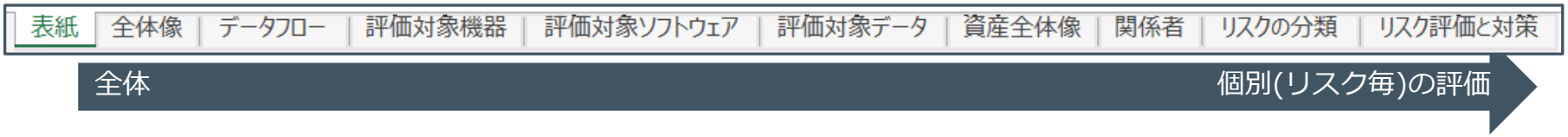
- **脅威源や脅威事象の特定**：情報システムに対する脅威源を特定し、脅威事象の特定。
- **リスクの評価**：情報システムに潜在する脅威（＝リスク）の特定。
- **リスクのレベル特定**：脅威源、脅威事象、脆弱性の組み合わせによって、リスクレベルを評価。

対応

- **リスク対策や緩和策の決定**：リスクのレベルの考察と、リスク対策の検討。

評価は、評価対象の可視化→評価→評価結果に基づく対応の検討という流れで実施しています。

これをリスク評価シートの構成に反映することで、全体→リスク毎の対策という流れにしました。

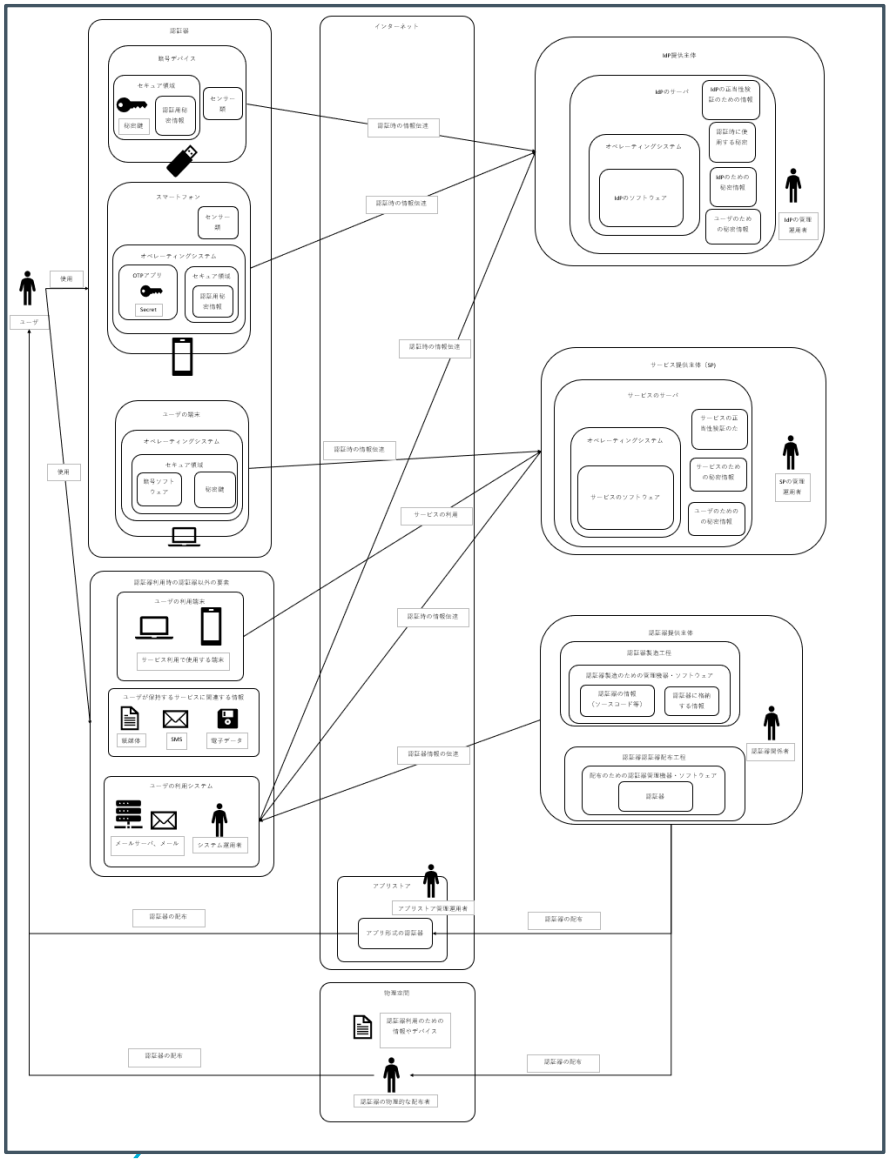


これから各シートを簡単にご説明します。

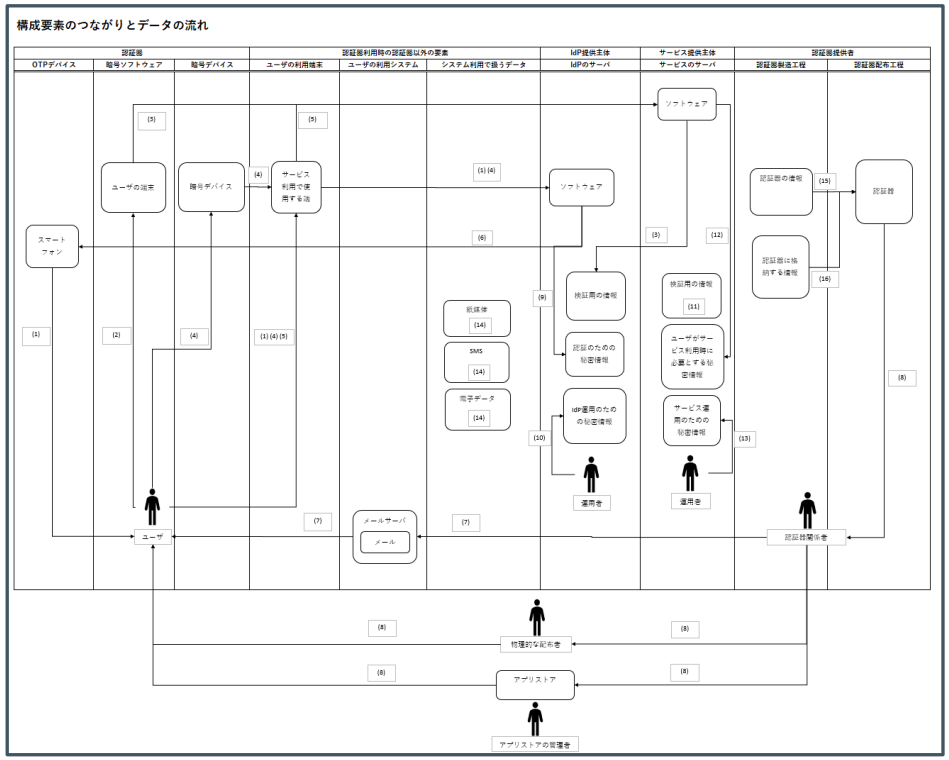
リスク評価シートのご紹介

リスク評価シートのご紹介

- 「全体像」シートでは学認で想定されるユースケースをもとに一般化した全体像を設定。



- 「データフロー」シートでは全体像の構成要素に流れるデータの観点でまとめています。



流れるデータの説明

No	説明	データ
(1)	OTP情報をユーザが取得しサービス利用で使用する端末からIdPへ送信し認証する	OTP情報
(2)	ユーザがクライアント証明書等の暗号ソフトウェアをユーザ端末へインポートする	暗号ソフトウェアと秘密鍵
(3)	暗号ソフトウェアによりサービスの利用のための認証を行い、サービスは認証局で検証する。	暗号ソフトウェア（クライアント証明書等）、暗号ソフトウェアの署名、認証局で公開されている公開鍵
(4)	暗号デバイスとユーザ間で認証する。その後、暗号デバイスがサービス利用で使用する端末と連携してIdPで認証を行う	ユーザの生体要素や記憶要素の情報、IdPで検証する暗号デバイスの署名
(5)	ユーザが端末を使ってサービスの利用する	ユーザが利用するサービスのための情報
(6)	OTP生成に使用するシークレット情報をQRコード等で提示する	OTP生成のためのシークレット情報
(7)	暗号ソフトウェアを認証器関係者から利用者へ送付する	電子的に配布される認証器
(8)	認証器（暗号デバイス、OTPデバイス）をユーザに配布する	データは流れない（認証器（暗号デバイス）が移動する）
(9)	IdPがユーザにまつわる秘密情報を参照し認証を行う	認証のための秘密情報
(10)	運用者が秘密情報を利用しIdPを運用する	IdP運用のための秘密情報
(11)	サービスを安全に提供する（通信暗号化など）ための情報	サービスの正当性検証のための情報
(12)	サービスはサービスを提供するために必要となる利用ユーザを保持する	ユーザがサービス利用時に必要とする秘密情報
(13)	運用者がサービスのための秘密情報を利用しサービスを運用する	サービス運用のための秘密情報
(14)	ユーザが保持するサービスに関連する情報	ユーザが保持するサービスに関連する情報
(15)	認証器の情報を利用して認証器を製造する	認証器のソースコードや設計図
(16)	認証器が保持するべき情報を認証器に埋め込む	認証器に格納する情報（秘密情報も含む）

リスク評価シートのご紹介

- 「評価対象機器」・「評価対象ソフトウェア」・「評価対象データ」それぞれのシートは、「全体像」「データフロー」でまとめられた要素を一覧化しています。
- 認証器の運用では、認証器の状態（登録前・運用中・廃棄後）によって想定される脅威も異なってくるため、さらに状態で分類しています。
- これらのシートで洗い出した項目一つ一つが、評価対象となります。

評価対象機器

このシートでは、「全体像」シートでまとめられたシステムの構成において、構成要素の中で物理的な媒体（例えば機器やデバイスなど）として扱われる資産をまとめている。

機器名	状態	提供元	利用方法	所在・所属	利用する者・利用する機器・利用するソフトウェア	備考
暗号デバイス	認証器登録前	-	-	-	-	認証器登録前の利用はない
	認証器運用中	認証器提供者	学認の認証時に利用	ユーザ	ユーザ	
	認証器廃棄後	-	-	-	-	認証器廃棄後の利用はない
セキュア領域	認証器登録前	-	-	-	-	認証器登録前の利用はない
	認証器運用中	認証器提供者	暗号デバイスが秘密情報保持に利用	暗号デバイス	暗号デバイス	
	認証器廃棄後	-	-	-	-	認証器廃棄後の利用はない
センサー類	認証器登録前	-	-	-	-	認証器登録前の利用はない
	認証器運用中	認証器提供者	学認の認証時に利用	暗号デバイス	ユーザ・暗号デバイス	
	認証器廃棄後	-	-	-	-	認証器廃棄後の利用はない
スマートフォン	認証器登録前	スマートフォンメーカ	私的な利用	ユーザ	ユーザ	
	認証器運用中	スマートフォンメーカ	学認の認証時に利用	ユーザ	ユーザ	
	認証器廃棄後	スマートフォンメーカ	私的な利用	ユーザ	ユーザ	
センサー類	認証器登録前	スマートフォンメーカ	学認以外の認証時に利用	スマートフォン	ユーザ・スマートフォン	
	認証器運用中	スマートフォンメーカ	学認の認証時に利用	スマートフォン	ユーザ・スマートフォン	
	認証器廃棄後	スマートフォンメーカ	学認以外の認証時に利用	スマートフォン	ユーザ・スマートフォン	
セキュア領域	認証器登録前	スマートフォンメーカ	スマートフォンの私的な利用時に利用	スマートフォン	スマートフォン	
	認証器運用中	スマートフォンメーカ	学認の認証時に利用	スマートフォン	スマートフォン	
	認証器廃棄後	スマートフォンメーカ	スマートフォンの私的な利用時に利用	スマートフォン	スマートフォン	
ユーザの端末	認証器登録前	端末メーカ	私的な利用	ユーザ	ユーザ	
	認証器運用中	端末メーカ	学認の認証時に利用	ユーザ	ユーザ	
	認証器廃棄後	端末メーカ	私的な利用	ユーザ	ユーザ	
サービス利用で使用する端末	認証器登録前	端末メーカ	学認以外のサービスで利用	ユーザ	ユーザ・サービス	
	認証器運用中	端末メーカ	サービス利用時に利用	ユーザ	ユーザ・サービス	
	認証器廃棄後	端末メーカ	学認以外のサービスで利用	ユーザ	ユーザ・サービス	
メールサーバ	認証器登録前	メールシステムベンダ	学認以外のメールの送受信に利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
	認証器運用中	メールシステムベンダ	学認に関連するメールの送受信にも利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
	認証器廃棄後	メールシステムベンダ	学認以外のメールの送受信に利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
IdPのサーバ	認証器登録前	IdPシステムベンダ	学認のサービス以外の認証で利用	IdP運用者	ユーザ、サービス	
	認証器運用中	IdPシステムベンダ	学認のサービスの認証にも利用	IdP運用者	ユーザ、サービス	
	認証器廃棄後	IdPシステムベンダ	学認のサービス以外の認証で利用	IdP運用者	ユーザ、サービス	
サービスのサーバ	認証器登録前	サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	認証器の状態によらずサービスは運営されている
	認証器運用中	サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	
	認証器廃棄後	サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	認証器の状態によらずサービスは運営されている
アプリストアのサーバ	認証器登録前	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	認証器の状態によらずアプリ形式の認証器は配布されている
	認証器運用中	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	
	認証器廃棄後	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	認証器の状態によらずアプリ形式の認証器は配布されている
認証器製造のための管理機器	認証器登録前	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	認証器の状態によらず製造は継続している
	認証器運用中	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	
	認証器廃棄後	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	認証器の状態によらず製造は継続している
配布のための認証器管理機器	認証器登録前	管理機器メーカ	認証器配布時に使用	認証器提供主体	認証器関係者、認証器の物理的な配布者	
	認証器運用中	-	-	-	-	
	認証器廃棄後	-	-	-	-	
物理的に配布される認証器デバイス	認証器登録前	認証器提供主体	認証器提供主体からユーザへ配布される	認証器の物理的な配布者	認証器提供主体、認証器の物理的な配布者、ユーザ	
	認証器運用中	-	-	-	-	
	認証器廃棄後	-	-	-	-	認証器廃棄後の利用はない

リスク評価シートのご紹介

- 「資産全体像」シート・「関係者」シートが評価対象の一覧となります。
- 認証器運用の当事者の管理責任下にないものは対象外として、評価から除外（グレーアウト）しています。

資産全体像

このシートでは、「評価対象機器」シート・「評価対象ソフトウェア」シート・「評価対象データ」シートにて抽出された、資産をまとめている。
リスク評価対象として設定されたシステムである「全体像」シート・「データフロー」シートを構成する要素が抽出されており、この資産に「関係者」シートの内容を加えた「資産・関係者」毎に「リスク評価と対策」のシートでリスク評価を実施することで、リスク評価対象システムのリスク評価を行う。
リスク評価の実施においては「認証器運用」に関連する資産を評価対象にし、「認証器運用」に関連しない資産は評価対象外とする。この判断を「リスク評価対象」列と「評価対象外理由」に記載している。
また、認証器運用の当事者でない者が責任を負っている資産は、その者の責任下で管理されているため、リスク評価の対象外としている。
認証器の運用を開始するために安全に認証器を配布する上でのリスクの評価は「認証器登録前」の状態で、認証器の運用が終了し安全に廃棄する上でのリスクの評価は「認証器廃棄後」の状態で評価する。

No	機器名	資産種別	状態	資産の内容	評価対象判断	評価対象外理由	提供元	利用方法	所在・所属	利用する者・利用する機器・利用するソフトウェア	備考
1	暗号デバイス	機器	認証器登録前	-	対象外	配布に関しては「物理的に配布される認証器デバイス」で評価	-	-	-	-	認証器登録前の利用はない
			認証器運用中	学認のサービスの認証で使用する認証器（暗号デバイス）			認証器提供者	学認のサービスの認証時に利用	ユーザ	ユーザ	
			認証器廃棄後	学認のサービスの認証で使用する認証器（暗号デバイス）			-	-	-	-	認証器廃棄後の利用はない
2	セキュア領域（暗号デバイス）	機器	認証器登録前	-	対象外	認証器運用外のため	-	-	-	-	認証器登録前の利用はない
			認証器運用中	暗号デバイスの内部でシークレット情報を保管する領域			認証器提供者	暗号デバイスが秘密情報保持に利用	暗号デバイス	暗号デバイス	
			認証器廃棄後	-	対象外	暗号デバイス自体に廃棄に関する機能なく、暗号デバイスの廃棄	-	-	-	-	認証器廃棄後の利用はない
3	センサー組（暗号デバイス）	機器	認証器登録前	-	対象外	認証器運用外のため	-	-	-	-	認証器登録前の利用はない
			認証器運用中	暗号デバイスのローカル認証で使用するためのセンサー組			認証器提供者	学認のサービスの認証時に利用	暗号デバイス	ユーザ・暗号デバイス	
			認証器廃棄後	-	対象外	認証情報が保管される資産ではないため	-	-	-	-	認証器廃棄後の利用はない
4	スマートフォン	機器	認証器登録前	ユーザが日常で利用するスマートフォン			スマートフォンメーカ	私的な利用	ユーザ	ユーザ	
			認証器運用中	学認のサービスの認証で利用する認証器アプリをインストールしたユーザのスマートフォン			スマートフォンメーカ	学認のサービスの認証時に利用	ユーザ	ユーザ	
			認証器廃棄後	認証器アプリの利用が終了した、ユーザが日常で利用するスマートフォン			スマートフォンメーカ	私的な利用	ユーザ	ユーザ	
5	センサー組（スマートフォン）	機器	認証器登録前	スマートフォンに組み込まれている、認証で使用するためのセンサー組	対象外	認証器運用外のため	スマートフォンメーカ	学認以外の認証時に利用	スマートフォン	ユーザ・スマートフォン	
			認証器運用中	スマートフォンに組み込まれている、認証で使用するためのセンサー組			スマートフォンメーカ	学認のサービスの認証時に利用	スマートフォン	ユーザ・スマートフォン	
			認証器廃棄後	スマートフォンに組み込まれている、認証で使用するためのセンサー組	対象外	認証情報が管理される資産ではないため	スマートフォンメーカ	学認以外の認証時に利用	スマートフォン	ユーザ・スマートフォン	
6	セキュア領域（スマートフォン）	機器	認証器登録前	スマートフォンやアプリがシークレット情報を管理するための領域	対象外	認証器運用外のため	スマートフォンメーカ	スマートフォンの私的な利用時に利用	スマートフォン	スマートフォン	
			認証器運用中	スマートフォンやアプリがシークレット情報を管理するための領域			スマートフォンメーカ	学認のサービスの認証時に利用	スマートフォン	スマートフォン	
			認証器廃棄後	スマートフォンやアプリがシークレット情報を管理するための領域			スマートフォンメーカ	スマートフォンの私的な利用時に利用	スマートフォン	スマートフォン	
7	ユーザの端末	機器	認証器登録前	ユーザが日常で利用する端末			端末メーカ	私的な利用	ユーザ	ユーザ	
			認証器運用中	学認のサービスの認証で利用する認証器（主に暗号ソフトウェアを想定）をインストールした端末			端末メーカ	学認のサービスの認証時に利用	ユーザ	ユーザ	
			認証器廃棄後	認証器（主に暗号ソフトウェアを想定）の利用が終了した、ユーザが日常で利用する端末			端末メーカ	私的な利用	ユーザ	ユーザ	
8	サービス利用で使用する端末	機器	認証器登録前	ユーザが学認以外のサービス利用時に使用する端末	対象外	認証器運用外のため	端末メーカ	学認以外のサービスで利用	ユーザ	ユーザ・サービス	
			認証器運用中	ユーザが学認のサービスも含め、サービス利用時に使用する端末			端末メーカ	サービス利用時に利用	ユーザ	ユーザ・サービス	
			認証器廃棄後	学認のサービス利用終了後に、引き続きユーザが学認以外のサービス利用時に使用する端末	対象外	認証器廃棄後に学認のサービス利用に関する事項はないため	端末メーカ	学認以外のサービスで利用	ユーザ	ユーザ・サービス	
9	メールサーバ	機器	認証器登録前	ユーザが日常の連絡手段として利用するメールサーバ	対象外	認証器運用外のため	メールシステムベンダ	学認以外のメールの送受信に利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
			認証器運用中	ユーザが学認のサービスの認証に関するメールも含め、連絡手段として利用するメールサーバ			メールシステムベンダ	学認に関連するメールの送受信にも利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
			認証器廃棄後	学認のサービス利用終了後に、引き続きユーザが日常の連絡手段として利用するメールサーバ	対象外	認証器運用外のため	メールシステムベンダ	学認以外のメールの送受信に利用	システム運用者	ユーザ、IdP、サービス、認証器提供主体	
10	IdPのサーバ	機器	認証器登録前	一般的なサービスの認証のために運用されているIdP			IdPシステムベンダ	学認のサービス以外の認証で利用	IdP運用者	ユーザ、サービス	
			認証器運用中	学認のサービスの認証のためにも運用されているIdP			IdPシステムベンダ	学認のサービスの認証にも利用	IdP運用者	ユーザ、サービス	
			認証器廃棄後	学認のサービスの認証での利用が終了後も、一般的なサービスの認証のために運用されているIdP			IdPシステムベンダ	学認のサービス以外の認証で利用	IdP運用者	ユーザ、サービス	
11	サービスのサーバ	機器	認証器登録前	学認の枠組みとは関連しないサービスのサーバ	対象外	学認外のサービスのため	サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	認証器の状態によらずサービスは運営されている
			認証器運用中	学認に関連するサービスのサーバ			サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	
			認証器廃棄後	学認の枠組みから離脱したサービスのサーバ			サービス開発ベンダ	サービス提供に利用	サービス運用者	ユーザ、IdP	認証器の状態によらずサービスは運営されている
12	アプリストアのサーバ	機器	認証器登録前	学認の認証のために使用される認証器アプリも配布しているアプリストアのサーバ	対象外	アプリストアのサーバの管理はアプリストアの責任範囲の為	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	認証器の状態によらずアプリ形式の認証器は配布されている
			認証器運用中	学認の認証のために使用される認証器アプリも配布しているアプリストアのサーバ	対象外	アプリストアのサーバの管理はアプリストアの責任範囲の為	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	
			認証器廃棄後	学認の認証のために使用される認証器アプリも配布しているアプリストアのサーバ	対象外	アプリストアのサーバの管理はアプリストアの責任範囲の為	アプリストア運営ベンダ	アプリ形式の認証器の配布時に利用	アプリストア管理運用者	ユーザ、認証器提供主体	認証器の状態によらずアプリ形式の認証器は配布されている
13	認証器製造のための管理機器	機器	認証器登録前	認証器を製造するために必要となる情報を管理する機器	対象外	ユーザや学認の責任範囲外のため	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	認証器の状態によらず製造は継続している
			認証器運用中	認証器を製造するために必要となる情報を管理する機器	対象外	ユーザや学認の責任範囲外のため	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	
			認証器廃棄後	認証器を製造するために必要となる情報を管理する機器	対象外	ユーザや学認の責任範囲外のため	製造機器メーカ	認証器製造時に使用	認証器提供主体	認証器関係者	認証器の状態によらず製造は継続している
14	配布のための認証器管理機器	機器	認証器登録前	認証器の配布に関する情報を管理する機器	対象外	ユーザや学認の責任範囲外のため	管理機器メーカ	認証器配布時に使用	認証器提供主体	認証器関係者、認証器の物理的な配布者	-
			認証器運用中	-	対象外	認証器運用外のため	-	-	-	-	
			認証器廃棄後	-	対象外	認証器運用外のため	-	-	-	-	
15	物理的に配布される認証器デバイス	機器	認証器登録前	配布の際に物理的な移動が発生する、移動中の認証器デバイス			認証器提供主体	認証器提供主体からユーザへ配布される	認証器の物理的な配布者	認証器提供主体、認証器の物理的な配布者、ユーザ	
			認証器運用中	-	対象外	認証器運用外のため	-	-	-	-	
			認証器廃棄後	-	対象外	認証器運用外のため	-	-	-	-	認証器廃棄後の利用はない
16	オペレーティングシステム（スマートフォ	ソフトウェア	認証器登録前	スマートフォンに搭載されているオペレーティングシステム	対象外	認証器運用外のため	オペレーティングシステムベンダ	私的な利用	スマートフォン	ユーザ、スマートフォン	
			認証器運用中	スマートフォンに搭載されているオペレーティングシステム			オペレーティングシステムベンダ	OTPアプリでの認証器利用時に利用	スマートフォン	ユーザ、スマートフォン	
			認証器廃棄後	スマートフォンに搭載されているオペレーティングシステム			オペレーティングシステムベンダ	私的な利用	スマートフォン	ユーザ、スマートフォン	
17	OTPアプリ	ソフトウェア	認証器登録前	-	対象外	認証器運用外のため	-	-	-	-	認証器登録再の利用はない
			認証器運用中	学認のサービスの認証に使用する、スマートフォンにインストールされるOTPアプリ			認証器提供主体	認証時に利用	スマートフォン	ユーザ、スマートフォン	
			認証器廃棄後	学認のサービスの認証に使用する、スマートフォンにインストールされるOTPアプリ			-	-	-	-	認証器廃棄後の利用はない

リスク評価シートのご紹介

- 評価対象に対して「リスクの分類」で挙げた9リスクを掛け合わせることで、考える必要のあるリスクが網羅的に導かれます。
- 「リスクの分類」は脅威モデリングの手法の一つであるSTRIDEのリスクに、認証器特有のリスクと考えられる「盗難や紛失」「危殆化」「誤操作」を加えています。
- 「リスク評価と対策」シートで潜在するリスクの評価とその対策をまとめています。

機器名	資産種別	状態
暗号デバイス	機器	認証器登録前
		認証器運用中
		認証器廃棄後

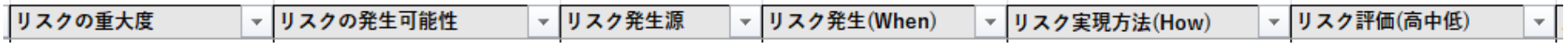
リスクの分類	説明
なりすまし	攻撃者によって正当なユーザやシステムになりすますされるリスク。
改竄	攻撃者がシステムやデータを不正に変更し、システムやデータの信頼性が損なわれるリスク。
否認	ユーザが行った行動や、システム上での特定の処理が否定され立証できないリスク。
情報漏洩	守られるべき情報が不正に露出・漏洩されるリスク。
サービス拒否	攻撃者がシステムのリソースを過負荷または妨害することにより、正当なユーザがサービスやリソースにアクセスできなくなるリスク。
権限昇格	攻撃者がシステム内で自身の権限レベルを不正に高め、通常は到達できないデータへのアクセスや実行できない処理の実行を達成されるリスク。
盗難や紛失	認証器をはじめとした機器やデバイスが、物理的に管理化に置けない状態となるリスク。
危殆化	認証器やデバイス、ソフトウェアを構成する技術が脆弱な状態であり、使用が推奨されないものとなるリスク。
誤操作	認証器やデバイス、ソフトウェアに対して想定外の操作を行う事で、不測の事態が生じるリスク。

資産・関係者	状態	リスク
暗号デバイス	認証器運用中	なりすまし
		改竄
		否認
		情報漏洩
		サービス拒否
		権限昇格
		盗難や紛失
		危殆化
		誤操作
	認証器廃棄後	なりすまし
		改竄
		否認
		情報漏洩
		サービス拒否
		権限昇格
		盗難や紛失
		危殆化
		誤操作

リスク評価シートのご紹介

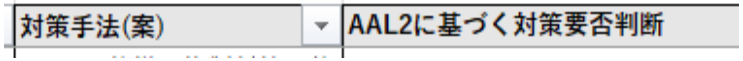
- 「リスク評価と対策」では、評価対象の資産や関係者毎に、
  - ・洗い出されたリスク

  - ・リスクの設定



  - ・リスクにまつわる情報（攻撃手法やインシデント）

  - ・対策案と学認AAL2の対策要否判断



  の内容を一覧化してまとめています。

- 今回は約740の対象を評価しました。
- 今後は、追加される認証器に関わる対象が増分として追加されていきます。

学認AAL2認証器レジストリの今後の計画

学認AAL2認証器レジストリの今後の計画

- 2025年6月現在、直近で2つの要素の追加を計画しています。
  - パスキー
  - パスワードマネージャ

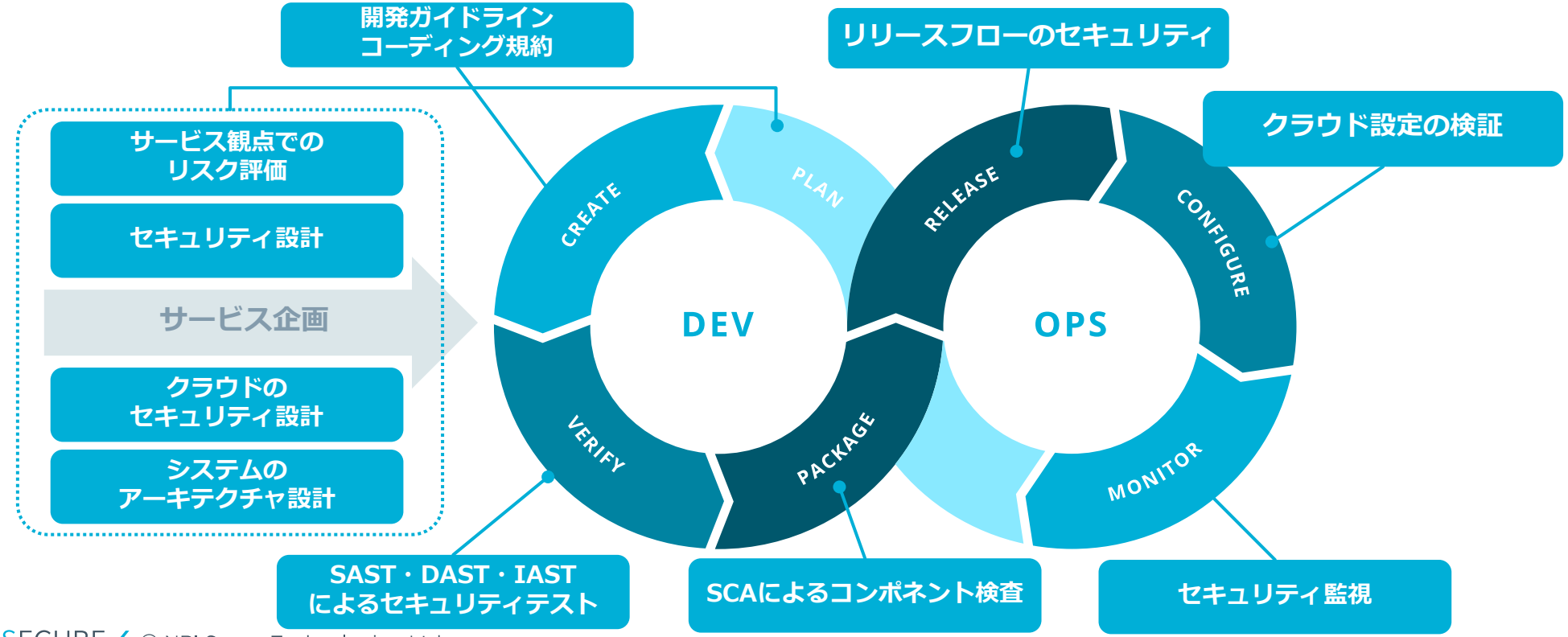
- 今後は、NIST SP800-63第4版正式版の公開にあわせてた認証器レジストリのアップデートや、パスキーの学認での位置づけについてコンテンツ追加してまいります。

- 学認AAL2認証器レジストリでは、学認参加機関のご要望にあわせて、認証器やそれに付随する要素の評価を行い、順次レジストリへ登録してまいります。
  認証器のカテゴリは網羅的に対応できておりますが、認証器の評価は時流に即して対応が必要と考えております。
  お問い合わせページ（https://level2.gakunin.jp/opt/）をご確認の上、お問い合わせください。

NRIセキュアテクノロジーズのご支援のご紹介

NRIセキュアテクノロジーズのご支援メニューのご紹介

- DevSecOpsのサイクルに合わせ「認証器」トピックで各種ご支援が可能です。
  - 認証器を用いたシステムの脅威をあらかじめ認知し設計・実装に反映 → 脅威モデリング
  - 認証器を用いた認証・認可のシステム設計に関して → 設計評価
  - 開発した認証器を用いるシステムの脆弱性の検査 → 脆弱性診断
- 各種ガイドライン整備や、開発・運用時のセキュリティ施策の導入等も非定型的にご支援可能です。
- 認証器に関する課題をお聞かせいただき、アプローチをご提案します。お問い合わせくださいませ。



NRI SECURE