Q0001

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント1：利用者やサービスが主張する本人性を確認する処理

次の説明に最も合う用語はどれか。利用者やサービスが主張する本人性を確認する処理

A. 認可
B. SAML
C. 認証
D. PAM

答え・解説

Q0001 正答：C. 認証

解説：認証は、利用者やサービスが主張する本人性を確認する処理。ほかの選択肢は目的又は適用場面が異なる。

Q0002

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント2：利用者やサービスが主張する本人性を確認する処理

認証の説明として最も適切なものはどれか。

A. 認証済み主体に許可する操作や資源を決定する処理
B. XMLを用いて認証・属性情報をサービス間で交換する仕様
C. 特権アカウントの保管、貸出し、記録、監視を行う管理
D. 利用者やサービスが主張する本人性を確認する処理

答え・解説

Q0002 正答：D. 利用者やサービスが主張する本人性を確認する処理

解説：認証の要点は「利用者やサービスが主張する本人性を確認する処理」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント3：利用者やサービスが主張する本人性を確認する処理

用語と説明の組合せとして適切なものはどれか。論点は「認証」である。

A. 認証：利用者やサービスが主張する本人性を確認する処理
B. 認可：利用者やサービスが主張する本人性を確認する処理
C. SAML：利用者やサービスが主張する本人性を確認する処理
D. PAM：利用者やサービスが主張する本人性を確認する処理

答え・解説

Q0003 正答：A. 認証：利用者やサービスが主張する本人性を確認する処理

解説：正しい組合せは「認証：利用者やサービスが主張する本人性を確認する処理」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント4：利用者やサービスが主張する本人性を確認する処理

「認証」は、利用者やサービスが主張する本人性を確認する処理。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。認証は利用者やサービスが主張する本人性を確認する処理。実務では対象、目的、前提条件を併せて確認する。

Q0005

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント5：利用者やサービスが主張する本人性を確認する処理

組織が「利用者やサービスが主張する本人性を確認する処理」ために採用すべき概念又は仕組みはどれか。

A. 認可
B. SAML
C. 認証
D. PAM

答え・解説

Q0005 正答：C. 認証
解説：この目的に対応するのは認証である。利用者やサービスが主張する本人性を確認する処理という機能・考え方を持つためである。

Q0006

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント6：利用者やサービスが主張する本人性を確認する処理

「認証」について、誤解を避けるための説明として最も適切なものはどれか。

A. 特権アカウントの保管、貸出し、記録、監視を行う管理
B. XMLを用いて認証・属性情報をサービス間で交換する仕様
C. 認証済み主体に許可する操作や資源を決定する処理
D. 利用者やサービスが主張する本人性を確認する処理

答え・解説

Q0006 正答：D. 利用者やサービスが主張する本人性を確認する処理
解説：認証は利用者やサービスが主張する本人性を確認する処理。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント7：利用者やサービスが主張する本人性を確認する処理

「認証」は、認証済み主体に許可する操作や資源を決定する処理。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述は認可の説明である。認証は利用者やサービスが主張する本人性を確認する処理。

Q0008

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント8：利用者やサービスが主張する本人性を確認する処理

次の状況で中心となる論点はどれか。「利用者やサービスが主張する本人性を確認する処理」ことが求められている。

A. SAML
B. 認証
C. PAM
D. 認可

答え・解説

Q0008 正答：B. 認証

解説：中心となる論点は認証である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

アイデンティティ・アクセス
タグ：認証
用語：認証の確認ポイント9：利用者やサービスが主張する本人性を確認する処理

「利用者やサービスが主張する本人性を確認する処理」という特徴を持つものを選べ。

A. PAM
B. SAML
C. 認証
D. 認可

答え・解説

Q0009 正答：C. 認証

解説：認証が該当する。定義は利用者やサービスが主張する本人性を確認する処理であり、他の候補とは機能が異なる。

Q0010

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント1：認証済み主体に許可する操作や資源を決定する処理

次の説明に最も合う用語はどれか。認証済み主体に許可する操作や資源を決定する処理

A. IDフェデレーション
B. OAuth 2.0
C. RBAC
D. 認可

答え・解説

Q0010 正答：D. 認可

解説：認可は、認証済み主体に許可する操作や資源を決定する処理。ほかの選択肢は目的又は適用場面が異なる。

Q0011

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント2：認証済み主体に許可する操作や資源を決定する処理

認可の説明として最も適切なものはどれか。

A. 認証済み主体に許可する操作や資源を決定する処理
B. 異なる組織やサービス間で認証結果を連携する仕組み
C. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式

答え・解説

Q0011 正答：A. 認証済み主体に許可する操作や資源を決定する処理

解説：認可の要点は「認証済み主体に許可する操作や資源を決定する処理」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0012

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント3：認証済み主体に許可する操作や資源を決定する処理

用語と説明の組合せとして適切なものはどれか。論点は「認可」である。

A. IDフェデレーション：認証済み主体に許可する操作や資源を決定する処理
B. 認可：認証済み主体に許可する操作や資源を決定する処理
C. OAuth 2.0：認証済み主体に許可する操作や資源を決定する処理
D. RBAC：認証済み主体に許可する操作や資源を決定する処理

答え・解説

Q0012 正答：B. 認可：認証済み主体に許可する操作や資源を決定する処理

解説：正しい組合せは「認可：認証済み主体に許可する操作や資源を決定する処理」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0013

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント4：認証済み主体に許可する操作や資源を決定する処理

「認可」は、認証済み主体に許可する操作や資源を決定する処理。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。認可は認証済み主体に許可する操作や資源を決定する処理。実務では対象、目的、前提条件を併せて確認する。

Q0014

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント5：認証済み主体に許可する操作や資源を決定する処理

組織が「認証済み主体に許可する操作や資源を決定する処理」ために採用すべき概念又は仕組みはどれか。

A. IDフェデレーション
B. OAuth 2.0
C. RBAC
D. 認可

答え・解説

Q0014 正答：D. 認可

解説：この目的に対応するのは認可である。認証済み主体に許可する操作や資源を決定する処理という機能・考え方を持つためである。

Q0015

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント6：認証済み主体に許可する操作や資源を決定する処理

「認可」について、誤解を避けるための説明として最も適切なものはどれか。

A. 認証済み主体に許可する操作や資源を決定する処理
B. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
C. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
D. 異なる組織やサービス間で認証結果を連携する仕組み

答え・解説

Q0015 正答：A. 認証済み主体に許可する操作や資源を決定する処理

解説：認可は認証済み主体に許可する操作や資源を決定する処理。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント7：認証済み主体に許可する操作や資源を決定する処理

「認可」は、異なる組織やサービス間で認証結果を連携する仕組み。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はIDフェデレーションの説明である。認可は認証済み主体に許可する操作や資源を決定する処理。

Q0017

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント8：認証済み主体に許可する操作や資源を決定する処理

次の状況で中心となる論点はどれか。「認証済み主体に許可する操作や資源を決定する処理」ことが求められている。

A. OAuth 2.0
B. RBAC
C. 認可
D. IDフェデレーション

答え・解説

Q0017 正答：C. 認可
解説：中心となる論点は認可である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0018

アイデンティティ・アクセス
タグ：認可
用語：認可の確認ポイント9：認証済み主体に許可する操作や資源を決定する処理

「認証済み主体に許可する操作や資源を決定する処理」という特徴を持つものを選べ。

A. RBAC
B. OAuth 2.0
C. IDフェデレーション
D. 認可

答え・解説

Q0018 正答：D. 認可
解説：認可が該当する。定義は認証済み主体に許可する操作や資源を決定する処理であり、他の候補とは機能が異なる。

Q0019

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント1：異なる組織やサービス間で認証結果を連携する仕組み

次の説明に最も合う用語はどれか。異なる組織やサービス間で認証結果を連携する仕組み

A. IDフェデレーション
B. SAML
C. OpenID Connect
D. ABAC

答え・解説

Q0019 正答：A. IDフェデレーション

解説：IDフェデレーションは、異なる組織やサービス間で認証結果を連携する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0020

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント2：異なる組織やサービス間で認証結果を連携する仕組み

IDフェデレーションの説明として最も適切なものはどれか。

A. XMLを用いて認証・属性情報をサービス間で交換する仕様
B. 異なる組織やサービス間で認証結果を連携する仕組み
C. OAuth 2.0上で利用者認証情報を連携する仕様
D. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式

答え・解説

Q0020 正答：B. 異なる組織やサービス間で認証結果を連携する仕組み

解説：IDフェデレーションの要点は「異なる組織やサービス間で認証結果を連携する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0021

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント3：異なる組織やサービス間で認証結果を連携する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「IDフェデレーション」である。

A. SAML：異なる組織やサービス間で認証結果を連携する仕組み
B. OpenID Connect：異なる組織やサービス間で認証結果を連携する仕組み
C. IDフェデレーション：異なる組織やサービス間で認証結果を連携する仕組み
D. ABAC：異なる組織やサービス間で認証結果を連携する仕組み

答え・解説

Q0021 正答：C. IDフェデレーション：異なる組織やサービス間で認証結果を連携する仕組み

解説：正しい組合せは「IDフェデレーション：異なる組織やサービス間で認証結果を連携する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0022

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント4：異なる組織やサービス間で認証結果を連携する仕組み

「IDフェデレーション」は、異なる組織やサービス間で認証結果を連携する仕組み。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。IDフェデレーションは異なる組織やサービス間で認証結果を連携する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0023

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント5：異なる組織やサービス間で認証結果を連携する仕組み

組織が「異なる組織やサービス間で認証結果を連携する仕組み」ために採用すべき概念又は仕組みはどれか。

A. IDフェデレーション
B. SAML
C. OpenID Connect
D. ABAC

答え・解説

Q0023 正答：A. IDフェデレーション

解説：この目的に対応するのはIDフェデレーションである。異なる組織やサービス間で認証結果を連携する仕組みという機能・考え方を持つためである。

Q0024

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント6：異なる組織やサービス間で認証結果を連携する仕組み

「IDフェデレーション」について、誤解を避けるための説明として最も適切なものはどれか。

A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
B. 異なる組織やサービス間で認証結果を連携する仕組み
C. OAuth 2.0上で利用者認証情報を連携する仕様
D. XMLを用いて認証・属性情報をサービス間で交換する仕様

答え・解説

Q0024 正答：B. 異なる組織やサービス間で認証結果を連携する仕組み

解説：IDフェデレーションは異なる組織やサービス間で認証結果を連携する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント7：異なる組織やサービス間で認証結果を連携する仕組み
「IDフェデレーション」は、XMLを用いて認証・属性情報をサービス間で交換する仕様。
A. ○
B. ×

答え・解説

Q0025 正答：×
解説：誤り。記述はSAMLの説明である。IDフェデレーションは異なる組織やサービス間で認証結果を連携する仕組み。

Q0026

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント8：異なる組織やサービス間で認証結果を連携する仕組み
次の状況で中心となる論点はどれか。「異なる組織やサービス間で認証結果を連携する仕組み」ことが求められている。
A. OpenID Connect
B. ABAC
C. SAML
D. IDフェデレーション

答え・解説

Q0026 正答：D. IDフェデレーション
解説：中心となる論点はIDフェデレーションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0027

アイデンティティ・アクセス
タグ：IDフェデレーション
用語：IDフェデレーションの確認ポイント9：異なる組織やサービス間で認証結果を連携する仕組み

「異なる組織やサービス間で認証結果を連携する仕組み」という特徴を持つものを選べ。

A. IDフェデレーション
B. ABAC
C. OpenID Connect
D. SAML

答え・解説

Q0027 正答：A. IDフェデレーション

解説：IDフェデレーションが該当する。定義は異なる組織やサービス間で認証結果を連携する仕組みであり、他の候補とは機能が異なる。

Q0028

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント1：XMLを用いて認証・属性情報をサービス間で交換する仕様

次の説明に最も合う用語はどれか。XMLを用いて認証・属性情報をサービス間で交換する仕様

A. OAuth 2.0
B. SAML
C. 多要素認証
D. 認証

答え・解説

Q0028 正答：B. SAML

解説：SAMLは、XMLを用いて認証・属性情報をサービス間で交換する仕様。ほかの選択肢は目的又は適用場面が異なる。

Q0029

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント2：XMLを用いて認証・属性情報をサービス間で交換する仕様

SAMLの説明として最も適切なものはどれか。

A. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
B. 異なる種類の認証要素を複数組み合わせる方式
C. XMLを用いて認証・属性情報をサービス間で交換する仕様
D. 利用者やサービスが主張する本人性を確認する処理

答え・解説

Q0029 正答：C. XMLを用いて認証・属性情報をサービス間で交換する仕様

解説：SAMLの要点は「XMLを用いて認証・属性情報をサービス間で交換する仕様」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0030

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント3：XMLを用いて認証・属性情報をサービス間で交換する仕様

用語と説明の組合せとして適切なものはどれか。論点は「SAML」である。

A. OAuth 2.0：XMLを用いて認証・属性情報をサービス間で交換する仕様
B. 多要素認証：XMLを用いて認証・属性情報をサービス間で交換する仕様
C. 認証：XMLを用いて認証・属性情報をサービス間で交換する仕様
D. SAML：XMLを用いて認証・属性情報をサービス間で交換する仕様

答え・解説

Q0030 正答：D. SAML：XMLを用いて認証・属性情報をサービス間で交換する仕様

解説：正しい組合せは「SAML：XMLを用いて認証・属性情報をサービス間で交換する仕様」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0031

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント4：XMLを用いて認証・属性情報をサービス間で交換する仕様

「SAML」は、XMLを用いて認証・属性情報をサービス間で交換する仕様。

A. ○
B. ×

答え・解説

Q0031 正答：○

解説：正しい。SAMLはXMLを用いて認証・属性情報をサービス間で交換する仕様。実務では対象、目的、前提条件を併せて確認する。

Q0032

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント5：XMLを用いて認証・属性情報をサービス間で交換する仕様

組織が「XMLを用いて認証・属性情報をサービス間で交換する仕様」ために採用すべき概念又は仕組みはどれか。

A. OAuth 2.0
B. SAML
C. 多要素認証
D. 認証

答え・解説

Q0032 正答：B. SAML

解説：この目的に対応するのはSAMLである。XMLを用いて認証・属性情報をサービス間で交換する仕様という機能・考え方を持つためである。

Q0033

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント6：XMLを用いて認証・属性情報をサービス間で交換する仕様

「SAML」について、誤解を避けるための説明として最も適切なものはどれか。

A. 利用者やサービスが主張する本人性を確認する処理
B. 異なる種類の認証要素を複数組み合わせる方式
C. XMLを用いて認証・属性情報をサービス間で交換する仕様
D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

答え・解説

Q0033 正答：C. XMLを用いて認証・属性情報をサービス間で交換する仕様

解説：SAMLはXMLを用いて認証・属性情報をサービス間で交換する仕様。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント7：XMLを用いて認証・属性情報をサービス間で交換する仕様

「SAML」は、利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はOAuth 2.0の説明である。SAMLはXMLを用いて認証・属性情報をサービス間で交換する仕様。

Q0035

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント8：XMLを用いて認証・属性情報をサービス間で交換する仕様

次の状況で中心となる論点はどれか。「XMLを用いて認証・属性情報をサービス間で交換する仕様」ことが求められている。

A. SAML
B. 多要素認証
C. 認証
D. OAuth 2.0

答え・解説

Q0035 正答：A. SAML

解説：中心となる論点はSAMLである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0036

アイデンティティ・アクセス
タグ：SAML
用語：SAMLの確認ポイント9：XMLを用いて認証・属性情報をサービス間で交換する仕様

「XMLを用いて認証・属性情報をサービス間で交換する仕様」という特徴を持つものを選べ。

A. 認証
B. SAML
C. 多要素認証
D. OAuth 2.0

答え・解説

Q0036 正答：B. SAML

解説：SAMLが該当する。定義はXMLを用いて認証・属性情報をサービス間で交換する仕様であり、他の候補とは機能が異なる。

Q0037

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント1：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

次の説明に最も合う用語はどれか。利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

A. OpenID Connect
B. PAM
C. OAuth 2.0
D. 認可

答え・解説

Q0037 正答：C. OAuth 2.0

解説：OAuth 2.0は、利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。ほかの選択肢は目的又は適用場面が異なる。

Q0038

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント2：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

OAuth 2.0の説明として最も適切なものはどれか。

A. OAuth 2.0上で利用者認証情報を連携する仕様
B. 特権アカウントの保管、貸出し、記録、監視を行う管理
C. 認証済み主体に許可する操作や資源を決定する処理
D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

答え・解説

Q0038 正答：D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

解説：OAuth 2.0の要点は「利用者のパスワードを渡さず限定権限を委任する認可フレームワーク」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0039

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント3：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

用語と説明の組合せとして適切なものはどれか。論点は「OAuth 2.0」である。

A. OAuth 2.0：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
B. OpenID Connect：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
C. PAM：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
D. 認可：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

答え・解説

Q0039 正答：A. OAuth 2.0：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

解説：正しい組合せは「OAuth 2.0：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0040

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント4：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

「OAuth 2.0」は、利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。OAuth 2.0は利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。実務では対象、目的、前提条件を併せて確認する。

Q0041

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント5：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

組織が「利用者のパスワードを渡さず限定権限を委任する認可フレームワーク」ために採用すべき概念又は仕組みはどれか。

A. OpenID Connect
B. PAM
C. OAuth 2.0
D. 認可

答え・解説

Q0041 正答：C. OAuth 2.0

解説：この目的に対応するのはOAuth 2.0である。利用者のパスワードを渡さず限定権限を委任する認可フレームワークという機能・考え方を持つためである。

Q0042

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント6：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

「OAuth 2.0」について、誤解を避けるための説明として最も適切なものはどれか。

A. 認証済み主体に許可する操作や資源を決定する処理
B. 特権アカウントの保管、貸出し、記録、監視を行う管理
C. OAuth 2.0上で利用者認証情報を連携する仕様
D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

答え・解説

Q0042 正答：D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

解説：OAuth 2.0は利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント7：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

「OAuth 2.0」は、OAuth 2.0上で利用者認証情報を連携する仕様。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はOpenID Connectの説明である。OAuth 2.0は利用者のパスワードを渡さず限定権限を委任する認可フレームワーク。

Q0044

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント8：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

次の状況で中心となる論点はどれか。「利用者のパスワードを渡さず限定権限を委任する認可フレームワーク」ことが求められている。

A. PAM
B. OAuth 2.0
C. 認可
D. OpenID Connect

答え・解説

Q0044 正答：B. OAuth 2.0

解説：中心となる論点はOAuth 2.0である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0045

アイデンティティ・アクセス
タグ：OAuth 2.0
用語：OAuth 2.0の確認ポイント9：利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

「利用者のパスワードを渡さず限定権限を委任する認可フレームワーク」という特徴を持つものを選べ。

A. 認可
B. PAM
C. OAuth 2.0
D. OpenID Connect

答え・解説

Q0045 正答：C. OAuth 2.0

解説：OAuth 2.0が該当する。定義は利用者のパスワードを渡さず限定権限を委任する認可フレームワークであり、他の候補とは機能が異なる。

Q0046

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント1：OAuth 2.0上で利用者認証情報を連携する仕様

次の説明に最も合う用語はどれか。OAuth 2.0上で利用者認証情報を連携する仕様

A. 多要素認証
B. RBAC
C. IDフェデレーション
D. OpenID Connect

答え・解説

Q0046 正答：D. OpenID Connect

解説：OpenID Connectは、OAuth 2.0上で利用者認証情報を連携する仕様。ほかの選択肢は目的又は適用場面が異なる。

Q0047

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント2：OAuth 2.0上で利用者認証情報を連携する仕様

OpenID Connectの説明として最も適切なものはどれか。

A. OAuth 2.0上で利用者認証情報を連携する仕様
B. 異なる種類の認証要素を複数組み合わせる方式
C. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
D. 異なる組織やサービス間で認証結果を連携する仕組み

答え・解説

Q0047 正答：A. OAuth 2.0上で利用者認証情報を連携する仕様

解説：OpenID Connectの要点は「OAuth 2.0上で利用者認証情報を連携する仕様」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0048

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント3：OAuth 2.0上で利用者認証情報を連携する仕様

用語と説明の組合せとして適切なものはどれか。論点は「OpenID Connect」である。

A. 多要素認証：OAuth 2.0上で利用者認証情報を連携する仕様
B. OpenID Connect：OAuth 2.0上で利用者認証情報を連携する仕様
C. RBAC：OAuth 2.0上で利用者認証情報を連携する仕様
D. IDフェデレーション：OAuth 2.0上で利用者認証情報を連携する仕様

答え・解説

Q0048 正答：B. OpenID Connect：OAuth 2.0上で利用者認証情報を連携する仕様

解説：正しい組合せは「OpenID Connect：OAuth 2.0上で利用者認証情報を連携する仕様」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0049

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント4：OAuth 2.0上で利用者認証情報を連携する仕様
「OpenID Connect」は、OAuth 2.0上で利用者認証情報を連携する仕様。

A. ○
B. ×

答え・解説

Q0049 正答：○
解説：正しい。OpenID ConnectはOAuth 2.0上で利用者認証情報を連携する仕様。実務では対象、目的、前提条件を併せて確認する。

Q0050

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント5：OAuth 2.0上で利用者認証情報を連携する仕様
組織が「OAuth 2.0上で利用者認証情報を連携する仕様」ために採用すべき概念又は仕組みはどれか。

A. 多要素認証
B. RBAC
C. IDフェデレーション
D. OpenID Connect

答え・解説

Q0050 正答：D. OpenID Connect
解説：この目的に対応するのはOpenID Connectである。OAuth 2.0上で利用者認証情報を連携する仕様という機能・考え方を持つためである。

Q0051

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント6：OAuth 2.0上で利用者認証情報を連携する仕様

「OpenID Connect」について、誤解を避けるための説明として最も適切なものはどれか。

A. OAuth 2.0上で利用者認証情報を連携する仕様
B. 異なる組織やサービス間で認証結果を連携する仕組み
C. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
D. 異なる種類の認証要素を複数組み合わせる方式

答え・解説

Q0051 正答：A. OAuth 2.0上で利用者認証情報を連携する仕様

解説：OpenID ConnectはOAuth 2.0上で利用者認証情報を連携する仕様。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント7：OAuth 2.0上で利用者認証情報を連携する仕様

「OpenID Connect」は、異なる種類の認証要素を複数組み合わせる方式。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述は多要素認証の説明である。OpenID ConnectはOAuth 2.0上で利用者認証情報を連携する仕様。

Q0053

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント8：OAuth 2.0上で利用者認証情報を連携する仕様

次の状況で中心となる論点はどれか。「OAuth 2.0上で利用者認証情報を連携する仕様」ことが求められている。

A. RBAC
B. IDフェデレーション
C. OpenID Connect
D. 多要素認証

答え・解説

Q0053 正答：C. OpenID Connect

解説：中心となる論点はOpenID Connectである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0054

アイデンティティ・アクセス
タグ：OpenID Connect
用語：OpenID Connectの確認ポイント9：OAuth 2.0上で利用者認証情報を連携する仕様

「OAuth 2.0上で利用者認証情報を連携する仕様」という特徴を持つものを選べ。

A. IDフェデレーション
B. RBAC
C. 多要素認証
D. OpenID Connect

答え・解説

Q0054 正答：D. OpenID Connect

解説：OpenID Connectが該当する。定義はOAuth 2.0上で利用者認証情報を連携する仕様であり、他の候補とは機能が異なる。

Q0055

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント1：異なる種類の認証要素を複数組み合わせる方式

次の説明に最も合う用語はどれか。異なる種類の認証要素を複数組み合わせる方式

A. 多要素認証
B. PAM
C. ABAC
D. SAML

答え・解説

Q0055 正答：A. 多要素認証

解説：多要素認証は、異なる種類の認証要素を複数組み合わせる方式。ほかの選択肢は目的又は適用場面が異なる。

Q0056

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント2：異なる種類の認証要素を複数組み合わせる方式

多要素認証の説明として最も適切なものはどれか。

A. 特権アカウントの保管、貸出し、記録、監視を行う管理
B. 異なる種類の認証要素を複数組み合わせる方式
C. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
D. XMLを用いて認証・属性情報をサービス間で交換する仕様

答え・解説

Q0056 正答：B. 異なる種類の認証要素を複数組み合わせる方式

解説：多要素認証の要点は「異なる種類の認証要素を複数組み合わせる方式」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0057

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント3：異なる種類の認証要素を複数組み合わせる方式

用語と説明の組合せとして適切なものはどれか。論点は「多要素認証」である。

A. PAM：異なる種類の認証要素を複数組み合わせる方式
B. ABAC：異なる種類の認証要素を複数組み合わせる方式
C. 多要素認証：異なる種類の認証要素を複数組み合わせる方式
D. SAML：異なる種類の認証要素を複数組み合わせる方式

答え・解説

Q0057 正答：C. 多要素認証：異なる種類の認証要素を複数組み合わせる方式

解説：正しい組合せは「多要素認証：異なる種類の認証要素を複数組み合わせる方式」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0058

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント4：異なる種類の認証要素を複数組み合わせる方式

「多要素認証」は、異なる種類の認証要素を複数組み合わせる方式。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。多要素認証は異なる種類の認証要素を複数組み合わせる方式。実務では対象、目的、前提条件を併せて確認する。

Q0059

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント5：異なる種類の認証要素を複数組み合わせる方式

組織が「異なる種類の認証要素を複数組み合わせる方式」ために採用すべき概念又は仕組みはどれか。

A. 多要素認証
B. PAM
C. ABAC
D. SAML

答え・解説

Q0059 正答：A. 多要素認証
解説：この目的に対応するのは多要素認証である。異なる種類の認証要素を複数組み合わせる方式という機能・考え方を持つためである。

Q0060

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント6：異なる種類の認証要素を複数組み合わせる方式

「多要素認証」について、誤解を避けるための説明として最も適切なものはどれか。

A. XMLを用いて認証・属性情報をサービス間で交換する仕様
B. 異なる種類の認証要素を複数組み合わせる方式
C. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
D. 特権アカウントの保管、貸出し、記録、監視を行う管理

答え・解説

Q0060 正答：B. 異なる種類の認証要素を複数組み合わせる方式
解説：多要素認証は異なる種類の認証要素を複数組み合わせる方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント7：異なる種類の認証要素を複数組み合わせる方式

「多要素認証」は、特権アカウントの保管、貸出し、記録、監視を行う管理。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はPAMの説明である。多要素認証は異なる種類の認証要素を複数組み合わせる方式。

Q0062

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント8：異なる種類の認証要素を複数組み合わせる方式

次の状況で中心となる論点はどれか。「異なる種類の認証要素を複数組み合わせる方式」ことが求められている。

A. ABAC
B. SAML
C. PAM
D. 多要素認証

答え・解説

Q0062 正答：D. 多要素認証

解説：中心となる論点は多要素認証である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0063

アイデンティティ・アクセス
タグ：多要素認証
用語：多要素認証の確認ポイント9：異なる種類の認証要素を複数組み合わせる方式
「異なる種類の認証要素を複数組み合わせる方式」という特徴を持つものを選べ。

A. 多要素認証
B. SAML
C. ABAC
D. PAM

答え・解説

Q0063 正答：A. 多要素認証
解説：多要素認証が該当する。定義は異なる種類の認証要素を複数組み合わせる方式であり、他の候補とは機能が異なる。

Q0064

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント1：特権アカウントの保管、貸出し、記録、監視を行う管理
次の説明に最も合う用語はどれか。特権アカウントの保管、貸出し、記録、監視を行う管理

A. RBAC
B. PAM
C. 認証
D. OAuth 2.0

答え・解説

Q0064 正答：B. PAM
解説：PAMは、特権アカウントの保管、貸出し、記録、監視を行う管理。ほかの選択肢は目的又は適用場面が異なる。

Q0065

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント2：特権アカウントの保管、貸出し、記録、監視を行う管理

PAMの説明として最も適切なものはどれか。

A. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
B. 利用者やサービスが主張する本人性を確認する処理
C. 特権アカウントの保管、貸出し、記録、監視を行う管理
D. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク

答え・解説

Q0065 正答：C. 特権アカウントの保管、貸出し、記録、監視を行う管理

解説：PAMの要点は「特権アカウントの保管、貸出し、記録、監視を行う管理」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0066

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント3：特権アカウントの保管、貸出し、記録、監視を行う管理

用語と説明の組合せとして適切なものはどれか。論点は「PAM」である。

A. RBAC：特権アカウントの保管、貸出し、記録、監視を行う管理
B. 認証：特権アカウントの保管、貸出し、記録、監視を行う管理
C. OAuth 2.0：特権アカウントの保管、貸出し、記録、監視を行う管理
D. PAM：特権アカウントの保管、貸出し、記録、監視を行う管理

答え・解説

Q0066 正答：D. PAM：特権アカウントの保管、貸出し、記録、監視を行う管理

解説：正しい組合せは「PAM：特権アカウントの保管、貸出し、記録、監視を行う管理」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0067

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント4：特権アカウントの保管、貸出し、記録、監視を行う管理

「PAM」は、特権アカウントの保管、貸出し、記録、監視を行う管理。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。PAMは特権アカウントの保管、貸出し、記録、監視を行う管理。実務では対象、目的、前提条件を併せて確認する。

Q0068

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント5：特権アカウントの保管、貸出し、記録、監視を行う管理

組織が「特権アカウントの保管、貸出し、記録、監視を行う管理」ために採用すべき概念又は仕組みはどれか。

A. RBAC
B. PAM
C. 認証
D. OAuth 2.0

答え・解説

Q0068 正答：B. PAM

解説：この目的に対応するのはPAMである。特権アカウントの保管、貸出し、記録、監視を行う管理という機能・考え方を持つためである。

Q0069

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント6：特権アカウントの保管、貸出し、記録、監視を行う管理

「PAM」について、誤解を避けるための説明として最も適切なものはどれか。

A. 利用者のパスワードを渡さず限定権限を委任する認可フレームワーク
B. 利用者やサービスが主張する本人性を確認する処理
C. 特権アカウントの保管、貸出し、記録、監視を行う管理
D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式

答え・解説

Q0069 正答：C. 特権アカウントの保管、貸出し、記録、監視を行う管理

解説：PAMは特権アカウントの保管、貸出し、記録、監視を行う管理。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント7：特権アカウントの保管、貸出し、記録、監視を行う管理

「PAM」は、職務上の役割に権限を割り当て利用者へ役割を付与する方式。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はRBACの説明である。PAMは特権アカウントの保管、貸出し、記録、監視を行う管理。

Q0071

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント8：特権アカウントの保管、貸出し、記録、監視を行う管理

次の状況で中心となる論点はどれか。「特権アカウントの保管、貸出し、記録、監視を行う管理」ことが求められている。

A. PAM
B. 認証
C. OAuth 2.0
D. RBAC

答え・解説

Q0071 正答：A. PAM

解説：中心となる論点はPAMである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0072

アイデンティティ・アクセス
タグ：PAM
用語：PAMの確認ポイント9：特権アカウントの保管、貸出し、記録、監視を行う管理

「特権アカウントの保管、貸出し、記録、監視を行う管理」という特徴を持つものを選べ。

A. OAuth 2.0
B. PAM
C. 認証
D. RBAC

答え・解説

Q0072 正答：B. PAM

解説：PAMが該当する。定義は特権アカウントの保管、貸出し、記録、監視を行う管理であり、他の候補とは機能が異なる。

Q0073

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント1：職務上の役割に権限を割り当て利用者へ役割を付与する方式

次の説明に最も合う用語はどれか。職務上の役割に権限を割り当て利用者へ役割を付与する方式

A. ABAC
B. 認可
C. RBAC
D. OpenID Connect

答え・解説

Q0073 正答：C. RBAC
解説：RBACは、職務上の役割に権限を割り当て利用者へ役割を付与する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0074

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント2：職務上の役割に権限を割り当て利用者へ役割を付与する方式

RBACの説明として最も適切なものはどれか。

A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
B. 認証済み主体に許可する操作や資源を決定する処理
C. OAuth 2.0上で利用者認証情報を連携する仕様
D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式

答え・解説

Q0074 正答：D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
解説：RBACの要点は「職務上の役割に権限を割り当て利用者へ役割を付与する方式」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0075

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント3：職務上の役割に権限を割り当て利用者へ役割を付与する方式

用語と説明の組合せとして適切なものはどれか。論点は「RBAC」である。

A. RBAC：職務上の役割に権限を割り当て利用者へ役割を付与する方式
B. ABAC：職務上の役割に権限を割り当て利用者へ役割を付与する方式
C. 認可：職務上の役割に権限を割り当て利用者へ役割を付与する方式
D. OpenID Connect：職務上の役割に権限を割り当て利用者へ役割を付与する方式

答え・解説

Q0075 正答：A. RBAC：職務上の役割に権限を割り当て利用者へ役割を付与する方式

解説：正しい組合せは「RBAC：職務上の役割に権限を割り当て利用者へ役割を付与する方式」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0076

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント4：職務上の役割に権限を割り当て利用者へ役割を付与する方式

「RBAC」は、職務上の役割に権限を割り当て利用者へ役割を付与する方式。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。RBACは職務上の役割に権限を割り当て利用者へ役割を付与する方式。実務では対象、目的、前提条件を併せて確認する。

Q0077

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント5：職務上の役割に権限を割り当て利用者へ役割を付与する方式

組織が「職務上の役割に権限を割り当て利用者へ役割を付与する方式」ために採用すべき概念又は仕組みはどれか。

A. ABAC
B. 認可
C. RBAC
D. OpenID Connect

答え・解説

Q0077 正答：C. RBAC
解説：この目的に対応するのはRBACである。職務上の役割に権限を割り当て利用者へ役割を付与する方式という機能・考え方を持つためである。

Q0078

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント6：職務上の役割に権限を割り当て利用者へ役割を付与する方式

「RBAC」について、誤解を避けるための説明として最も適切なものはどれか。

A. OAuth 2.0上で利用者認証情報を連携する仕様
B. 認証済み主体に許可する操作や資源を決定する処理
C. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式

答え・解説

Q0078 正答：D. 職務上の役割に権限を割り当て利用者へ役割を付与する方式
解説：RBACは職務上の役割に権限を割り当て利用者へ役割を付与する方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント7：職務上の役割に権限を割り当て利用者へ役割を付与する方式
「RBAC」は、主体・資源・環境などの属性とポリシーでアクセスを判断する方式。
A. ○
B. ×

答え・解説

Q0079 正答：×
解説：誤り。記述はABACの説明である。RBACは職務上の役割に権限を割り当て利用者へ役割を付与する方式。

Q0080

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント8：職務上の役割に権限を割り当て利用者へ役割を付与する方式
次の状況で中心となる論点はどれか。「職務上の役割に権限を割り当て利用者へ役割を付与する方式」ことが求められている。
A. 認可
B. RBAC
C. OpenID Connect
D. ABAC

答え・解説

Q0080 正答：B. RBAC
解説：中心となる論点はRBACである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0081

アイデンティティ・アクセス
タグ：RBAC
用語：RBACの確認ポイント9：職務上の役割に権限を割り当て利用者へ役割を付与する方式

「職務上の役割に権限を割り当て利用者へ役割を付与する方式」という特徴を持つものを選べ。

A. OpenID Connect
B. 認可
C. RBAC
D. ABAC

答え・解説

Q0081 正答：C. RBAC

解説：RBACが該当する。定義は職務上の役割に権限を割り当て利用者へ役割を付与する方式であり、他の候補とは機能が異なる。

Q0082

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント1：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

次の説明に最も合う用語はどれか。主体・資源・環境などの属性とポリシーでアクセスを判断する方式

A. 認証
B. IDフェデレーション
C. 多要素認証
D. ABAC

答え・解説

Q0082 正答：D. ABAC

解説：ABACは、主体・資源・環境などの属性とポリシーでアクセスを判断する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0083

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント2：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

ABACの説明として最も適切なものはどれか。

A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
B. 利用者やサービスが主張する本人性を確認する処理
C. 異なる組織やサービス間で認証結果を連携する仕組み
D. 異なる種類の認証要素を複数組み合わせる方式

答え・解説

Q0083 正答：A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式

解説：ABACの要点は「主体・資源・環境などの属性とポリシーでアクセスを判断する方式」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0084

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント3：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

用語と説明の組合せとして適切なものはどれか。論点は「ABAC」である。

A. 認証：主体・資源・環境などの属性とポリシーでアクセスを判断する方式
B. ABAC：主体・資源・環境などの属性とポリシーでアクセスを判断する方式
C. IDフェデレーション：主体・資源・環境などの属性とポリシーでアクセスを判断する方式
D. 多要素認証：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

答え・解説

Q0084 正答：B. ABAC：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

解説：正しい組合せは「ABAC：主体・資源・環境などの属性とポリシーでアクセスを判断する方式」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0085

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント4：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

「ABAC」は、主体・資源・環境などの属性とポリシーでアクセスを判断する方式。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。ABACは主体・資源・環境などの属性とポリシーでアクセスを判断する方式。実務では対象、目的、前提条件を併せて確認する。

Q0086

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント5：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

組織が「主体・資源・環境などの属性とポリシーでアクセスを判断する方式」ために採用すべき概念又は仕組みはどれか。

A. 認証
B. IDフェデレーション
C. 多要素認証
D. ABAC

答え・解説

Q0086 正答：D. ABAC

解説：この目的に対応するのはABACである。主体・資源・環境などの属性とポリシーでアクセスを判断する方式という機能・考え方を持つためである。

Q0087

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント6：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

「ABAC」について、誤解を避けるための説明として最も適切なものはどれか。

A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式
B. 異なる種類の認証要素を複数組み合わせる方式
C. 異なる組織やサービス間で認証結果を連携する仕組み
D. 利用者やサービスが主張する本人性を確認する処理

答え・解説

Q0087 正答：A. 主体・資源・環境などの属性とポリシーでアクセスを判断する方式

解説：ABACは主体・資源・環境などの属性とポリシーでアクセスを判断する方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント7：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

「ABAC」は、利用者やサービスが主張する本人性を確認する処理。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述は認証の説明である。ABACは主体・資源・環境などの属性とポリシーでアクセスを判断する方式。

Q0089

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント8：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

次の状況で中心となる論点はどれか。「主体・資源・環境などの属性とポリシーでアクセスを判断する方式」ことが求められている。

A. IDフェデレーション
B. 多要素認証
C. ABAC
D. 認証

答え・解説

Q0089 正答：C. ABAC

解説：中心となる論点はABACである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0090

アイデンティティ・アクセス
タグ：ABAC
用語：ABACの確認ポイント9：主体・資源・環境などの属性とポリシーでアクセスを判断する方式

「主体・資源・環境などの属性とポリシーでアクセスを判断する方式」という特徴を持つものを選べ。

A. 多要素認証
B. IDフェデレーション
C. 認証
D. ABAC

答え・解説

Q0090 正答：D. ABAC

解説：ABACが該当する。定義は主体・資源・環境などの属性とポリシーでアクセスを判断する方式であり、他の候補とは機能が異なる。