	大分類 Webアプリケーションの脆弱性	中分類	小分類							
		インジェクション	SQLインジェクション	診断を実施すべき箇所	ペイロード・検出パターン '(シングルクォート)	操作を行う対象 パラメータ	診断方法 パラメータの値に検出パターンを挿入し、リクエストを送信	脆弱性がある場合の結果 DB関連のエラーが表示され		備考 DB関連のエラー (SQL
	WORDS OF THE STATE	1000000	50211112111	,	(2,2,2,2,4,1)		7 / / MEICHAN VEHICLE / / / / / / CEN	るか、正常動作と挙動が異		Syntax, SQLException,
								なる		pg_exec、ORA-5桁数字、
										ODBC Driver Managerなど)
										は画面に表示されることもあ
										れば、HTMLソースに表示さ
										れることもある
										SQLインジェクションがある
										が、エラーが画面にでない場
										合には正常時と挙動が異なる
										こともある
										ただし、この診断手法の脆弱
										性の有無については確定では
										なく、あくまで可能性を示唆
										するものである
2				すべて	1/0	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	演算が実行される(ゼロ除	文字列としてそのまま計	F
								算のエラーになる)	価される	
3				すべて	(1)「(元の値)」	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	(1)を送信して正常系の動作	左記以外	「' and 'a'='a'」の部分がSQL
					(2)「(元の値)' and 'a'='a」			を確認し、(1)と(2)を比較		文の一部として機能(演算を
					(3)「(元の値)' and 'a'='b」			して同一のレスポンスとな		実施)している場合には、
								り、(2)と(3)で異なるレス		「'a'='a'」は常に真(1)とな
								ポンスが返ってくる		り、判定結果に影響しないた
										め、SQLインジェクションが
$\vdash$	:									可能であると判断できる
4				型が数値のパラメータ	(1)「(元の値:数値)」	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	(1)を送信して正常系の動作	左記以外	「and 1=1」の部分がSQL文
					(2) 「(元の値) and 1-1」 (3) 「(二の体) 1 0」			を確認し、(1)と(2)を比較		の一部として機能(演算を実
					(3)「(元の値) and 1=0」			して同一のレスポンスとな		施)している場合には、
								り、(2)と(3)で異なるレス ポンスが返ってくる		「1=1」は常に真(1)とな り、判定結果に影響しないた
								ホン人が送ってくる		り、刊足相来に影響しないた め、SQLインジェクションが
										可能であると判断できる
6				型が数値のパラメータ	(1)「(元の値:数値)	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	(1)を送信して正常系の動作	£ RPLM	円形であると刊間できる
5				生が奴匪のバファーラ	(2)「(元の値)-0」	7.77-9	ハクターテの他に使山ハテークを押入し、リクエストを近日	を確認し、(1)と(2)を比較	ZE BEEAPF	
					(3)「(元の値)-1」			して同一のレスポンスとな		
					(3) 1(70-7)(6) 23			り、(2)と(3)で異なるレス		
								ポンスが返ってくる		
6			コマンドインジェクション	すべて	/bin/sleep 20	パラメータ	パラメータの値に輸出パターンを挿入し、リクエストを送信	レスポンスが返ってくるの	通常通りの応答速度でレ	
								が20秒遅くなる	スポンスが返ってくる	
7				すべて	;/bin/sleep 20;	パラメータ	パラメータの値に検出バターンを挿入し、リクエストを送信	レスポンスが返ってくるの		/
			CRLFインジェクション					が20秒遅くなる	スポンスが返ってくる	
8				すべて	////bin/sleep 20	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるの	通常通りの応答速度でレ	
								が20秒遅くなる	スポンスが返ってくる	
9				すべて	;ping -nc 20 127.0.0.1;	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるの	通常通りの応答速度でレ	/
								が20秒遅くなる	スポンスが返ってくる	
10				すべて	&ping -nc 20 127.0.0.1&	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるの		·
								が20秒遅くなる	スポンスが返ってくる	
11				すべて	\$(////bin/sleep 20)	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるの		·
$\Box$								が20秒遅くなる	スポンスが返ってくる	
12				レスポンスヘッダに値を出力している箇所	%0d%0aSet-Cookie:(任意の値)%3D(任意の値)%3B		パラメータの値に検出パターンを挿入し、リクエストを送信			主な診断対象はSet-Cookieや
						パラメータ			れずに検出パターンの文	C Locationヘッダフィールド
	:							ダフィールドが挿入される		
13				レスポンスヘッダに値を出力している箇所	%0d%0a%0d%0akensa		パラメータの値に検出パターンを挿入し、リクエストを送信			主な診断対象はSet-Cookieや
						パラメータ				Locationヘッダフィールド
								字列がHTTPボディ部分に	字列が表示される	
1.4				メールメッセージのヘッダに値を出力している	w0.1w0-T(が幸のメールフは・コ)	ar a	22 J. Hothi-Mill 2 H. 1 2 Mills 1 1 1 2 1 2 Mills	表示される	or m. and do do do do to	all the totals of the second of the second
14	15			メールメッセーンのヘッタに値を出力している mass	nounual0:(仕息のメールアドレス)	メールメッセージのヘッダに値を出力 しているパラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	挿入したメールアドレス宛 にメールが配送される	エラーが発生するなど、 メールが配送されない	受信可能なメールアドレスを 用意する必要がある
16			クロスサイトスクリプティング(XSS)	すべて	">'> <s>XSS</s>	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	にメールが配达される 給出パターンが適切にエス		m 応する必要がある -
10			> = A y 1 F A y y 2 / 1 2 y (ASS)	7		1.72 = 9	・・ファーフル出に使出ハラーンを押入し、リフエハドを応信	検出バターンが適切にエス ケープされずに挿入される		
								ッ ノ ご4いりに押入される	ハノ ノビ4ルに押へされ	*
16				すべて	<script>alert(1)</script>	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	検出パターンが適切にエス	⇒ 検出パターンが適切にエ	
120				7 - 7			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ケープされずに挿入される	スケープされて挿入され	ı
									5	
17	•			すべて	javascript:alert(1)	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	URI属性やjavascriptコード	javascriptスキームとし	
								等に挿入され、javascript	て有効にならない	
								スキームとして有効になる		
18	:			すべて	'+alert(1)+'	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	検出パターンが適切にエス	検出パターンが適切にコ	1
								ケープされずに挿入される	スケープされて挿入され	ι
					<u> </u>				5	
19				すべて	"onmouseover="alert(1)	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	検出パターンが適切にエス		
								ケープされずに挿入される	スケープされて挿入され	ι
Ш	:								<b></b>	
20				URL	#">'> <img onerror="alert(1)" src="x"/>	パラメータ	検出パターンをURLの最後尾に追記して、リクエストを送信	スクリプトが実行される	スクリプトが実行されな	アドレスバーのURLを直接編
									b.	集した場合はリロードが必要
										となる場合が多いことに留意
21		パストラバーサル		ファイル名を扱っている画面や機能	/////etc/hosts	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	/etc/hostsの内容が表示さ		Ŕ
					1			れる	されない	

No. 大分類	中分類 小分類	診断を実施すべき箇所	ベイロード・検出パターン	操作を行う対象	診断方法	脆弱性がある場合の結果 脆弱性がない場合	備考
22		ファイル名を扱っている画面や機能	//////etc/hosts%00	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	/etc/hostsの内容が表示さ /etc/hostsの内容が表示 れる されない	Ā
23		ファイル名を扱っている画面や機能	/////windows/win.ini	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	/windows/win.iniの内容が /windows/win.iniの内 表示される 容が表示されない	
24		ファイル名を扱っている画面や機能	////windows/win.ini%00	パラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	/windows/win.iniの内容が /windows/win.iniの内 表示される 容が表示されない	
25	XML外部エンティティ参照 (XXE)	ラクエストにXMLが含まれている箇所	元の値: <pre></pre> <pre> <pre></pre> <p< td=""><td>XMLが格勢されている箇所(パラメー ク、ファイルなど)</td><td>XMLに検出バターンを挿入し、リクエストを送信</td><td>/etc/hostsの内容が表示さ れる えれない</td><td>採定する検出パターンの foo の簡所は実装に合わせて変更 する 「OWASP Top10 2017」の 定を受けて追加(A4:XML外 部エンティティ参照:XXE)</td></p<></pre>	XMLが格勢されている箇所(パラメー ク、ファイルなど)	XMLに検出バターンを挿入し、リクエストを送信	/etc/hostsの内容が表示さ れる えれない	採定する検出パターンの foo の簡所は実装に合わせて変更 する 「OWASP Top10 2017」の 定を受けて追加(A4:XML外 部エンティティ参照:XXE)
26		リクエストにXMLが含まれている箇所	>  >-foo>&xe	XMLが格納されている箇所(パラメー タ、ファイルなど)	XMLに検出パターンを挿入し、リクエストを送信	/windows/win.iniの内容が /windows/win.iniの内容が 表示される 常が表示されない	指定する検出パターンの foo の箇所は実装に合わせて変更 する 「OWASP Top10 2017」の 定を受けて追加(A4:XML外 部エンティティ参照:XXE)
27		リクエストにXMLが含まれている箇所	プライン・ファイン・ファイン・ファイン・ファイン・ファイン・ファイン・ファイン・ファ	XMLが格納されている箇所(パラメー ク、ファイルなど)	XMLに検出パターンを挿入し、リクエストを送信	http://example.com/ に アクセスが来る にアクセスが来ない	外部Webサーバを用意し、ア クセスがログなどで確認でき るを要がある 指定する検出バターンの foo http://example.com の箇所 は実装に合わせて変更する 「OWASP Top10 2017」の 定を受けて追加 (A4:XML外 能エンティティ参照:XXE)
28	オープンリダイレクト	<b>リダイレクトが実行される画面や機能</b>	http://www.example.com/	URL、もしくはURLの一部と想定されるパラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	http://www.example.com http://www.example. にリダイレクトされる omにリダイレクトされたない	c 指定する検出パターンのURL
29		リダイレクトが実行される顕語や機能	//www.example.com/	URL、もしくはURLの一部と想定され るバラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	http://www.example.com http://www.example. にリダイレクトされる omにリダイレクトされ ない	c 指定する検出パターンのURL
30	シリアライズされたオブジェクト	\$~T	シリアライズされた値(言語によってシリアライズ形式は変わります) ■PHPの場合 「a-4:(i:0:i:13:1::s:7:"Mallory":i:2:s:4:"user"):3::3:2:"b6a8 b3bea87ie0e05022f81c88bc960':]」のような値 ■Javaの場合 (00 (小文字アール、大文字オー、数字0) から始まるBase64 文字列 H4slA (大文字エイチ、数字4、小文字エス、大文字アイ、大文字エー)から始まるBase64 文字列		検出パターンがリクエストに含まれていないか確認	検出パターンが含まれてい 検出パターンが含まれてい いない	
31	インクルードにまつわる脆弱 リモートファイルインクルージョン 性		外部サーバのスクリプトを配置したURL	ファイル名と想定されるパラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	スクリプトが読み込まれ実 行される ない	A部Webサーバを用意し、フ クリプトを配置する必要がある スクリプト例 phpinfo();sleep(15);
32	クリックジャッキング	確定処理の直前両面			レスポンス〜ッグにX-Frame-Options〜ッグフィールドが存在し、値が 「DENY」「SAMEORIGIN」(ALLOW-FROM (uri)」かを確認	X-Frame-Optionsヘッダ レスポンスヘッダにX- フィールドがない/製造 Frame-Optionsヘッダ 「DENY」 「SAMEORIGIN」 が「DENY」 「ALLOW-FROM (uri)」で「SAMEORIGIN」 はない、イスLOW-FROM (uri)」で「ALLOW-FROM (uri)」で「MALOW-FROM (uri)」で「M	
33	88年 總和回避	認証が必要な箇所		認証状態を保持しているパラメータ	認証状態を保持しているパラメータ(ex. authenticated—ueno、 userid—1234)を特定し、パラメータ値を変更して認証後のページにアク	認証後のページを指定する 認証後のページを指定す	
4		ログイン機能		パラメータ	ス 正しいアカウントとパスワードの組み合わせ以外でログインを試行	る ない 認証が成功する 認証に失敗する	<del> </del>

No. 大分類	中分割	小分類	診断を実施すべき箇所	ペイロード・輸出パターン	操作を行う対象	除断方法	脆弱性がある場合の結果	胎弱性がたい場合 備者
35 人分類	十刀飛	ログアウト機能の不備や未実装	ログアウト機能	7~7 ロード・使山バラーン	採作を行り対象	ログアウト機能が存在するかを確認	即列生がある場合の和米 ログアウト機能が存在しな	
						The state of the s	V)	8
36			ログアウト機能			認証で使っているセッションIDをメモし、ログアウト機能を実行後、メモし	認証状態でしかアクセスで	認証状態でしかアクセス ログアウト機能の実行時に
						たセッションIDを付与してログイン状態になることを確認		できない画面や機能にア セッションIDが破棄されてい
							スできる(ログイン状態に	クセスできない (ログイ) ない場合に発生する
27		過度な認証試行に対する対策不備や未実装	ロガイン操作		パラメータ	同じユーザタでパスワードを連続して10回開金えて確認	なる) アカウントロックさわかい	ン状態にならない) アカウントロックされる 試行するパスワードはパス
31		地及な認証時日に対する対象不開で未来教	1971 2 MRHG		\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	同じユーリ名でパスケートを座載して10回間座えて機能	) ガラントロック G4D4V	ワードポリシーに従うこと
								1 1171 1127 1
38		脆弱なパスワードポリシー	パスワード登録・変更	(空)	パラメータ	パスワード文字列の桁数が8文字未満、文字種が大小英字、数字の3種類が混	脆弱なパスワードが登録・	脆弱なパスワードが登
				1234567		在でない文字列を登録・変更できないことを確認	変更できる	録・変更できない
				abcdefg				
20			パスワード登録・変更	abcd123 RfM9yY8Cwk	パラメータ	パスワード文字列の桁数が8文字以上、かつ文字種が大小英字、数字の3種類	we do a section - or do than a	登録・変更できる
39			ハヘシート立脉・変更	RIMSYTOCWK	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	が混在している文字列を登録・変更できることを確認	立跡・変更できない	豆林・東丈できる
40			パスワード登録・変更		パラメータ	ユーザ名と同じパスワードが登録・変更できないことを確認	脆弱な(推測可能な)パス	脆弱な(推測可能な)パス
							ワードが設定できる	ワードが設定できない
41		復元可能なパスワード保存	パスワード登録・変更			パスワードリマインダ機能でパスワードを問い合わせて確認	登録したパスワードが返っ	パスワードリマインダ機
							てくる	能が存在しない
42			全般			設定したパスワードが、いずれかのページで表示や埋め込まれていないこと を確認	レスポンスにパスワードが 埋め込まれている	パスワードが埋め込まれていない
42		パスワードリセットの不備	パスワードリセット			を確認 パスワードリセットを実行して、再設定時に本人確認をしていることを確認	理の込まれている ユーザ本人しか受け取れな	4. 4.
		1727131111	1,000			TO TO TO TO THE WITHOUT THE WARRENCE OF THE COMMO		ない連絡先に再設定方法
							知されずにパスワードのリ	
							セットが可能	
44			パスワードリセット			パスワードリセットを実行して、ユーザ自身による新たなパスワード設定が		
						強制されることを確認	ワードが送付され、そのま	ワードを設定する
ar.	認可制御の不備		認可制御が必要な箇所		URL	権限の異なる複数のユーザで、本来権限のない機能のURLにアクセス	ま使い続けられる	アクセス権限がない情報
45	お可制御の不無		必可制御か必要な固所		URL	権限の異なる後数のユーザで、本来権限のない機能のURLにアクセス	ガクセス権限がない情報や 機能が閲覧、操作できる	
							DESIGNATION THAT CO.D.	the control of the co
46			認可制御が必要な箇所		パラメータ	登録データに紐づく値がパラメータにより指定されている場合、そのID類を	当該ユーザではアクセス権	当該ユーザではアクセス 登録データに紐づく値がパラ
						変更して当該ユーザではアクセス権限がない情報や機能へアクセス	限がない情報や機能へアク	権限がない情報や機能へ メータとして用いられている
							セスできる	アクセスできない 例:ユーザID、文書ID、注文
								番号、顧客番号など
47			認可制御が必要な箇所		パラメータ	hiddenパラメータやCookieなどの値で権限クラスを指定していると推測され	<ul><li>当該ユーザではアクセス権</li><li>限がない情報や機能が関</li></ul>	
						る場合に、値を変更、追加などを行うことで当該ユーザではアクセス権限が ない情報や機能を閲覧、操作	版かない情報や機能が周 覧、操作できる	権限がない情報や機能が られている例: 閲覧、操作できない func-admin など
48			認可制御が必要な箇所		URL			
48			認可制御が必要な箇所		URL		認証後のページを指定する ことでアクセスが可能であ	認証後のページを指定す
48						認証状態でしか表示できないページに、ログイン認証していない状態でアク セス	認証後のページを指定する ことでアクセスが可能であ る	認証後のページを指定す ることでアクセスができ ない
49			認可制御が必要な箇所 認可制御が必要な箇所	元の框:www.example.com/user1/profile.php	URL URL	認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のベージを指定す ることでアクセスができ ない 通常ユーザではアクセス
49				元の値:www.example.com/user1/profile.php 践行例:www.example.com/user2/profile.php		認証状態でしか表示できないページに、ログイン認証していない状態でアク セス	認証後のページを指定する ことでアクセスが可能であ る	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例: www.example.com/user2/profile.php		認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のベージを指定す ることでアクセスができ ない 通常ユーザではアクセス
49				試行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv		認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例: www.example.com/user2/profile.php		認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv		認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php		認証状態でしか表示できないページに、ログイン認証していない状態でアクセス 既存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変	認証後のページを指定する ことでアクセスが可能である アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49			認可制御が必要な箇所	終行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv 終行例:www.example.com/1001.csv 元の値:www.example.com/taro/index.php	URL	認証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス	認証後のページを指定する ことでアクセスが可能である る アクセス権限がない情報や 機能が閲覧、操作できる	要証後のページを指定す ることでプクセスができ ない 通常ルーザではアクセス 権限がない情報や機能へ アクセスできない
49	クロスサイトリクエストフォ	+−ジェリ(CSRF)		対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php		製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行	認証後のページを指定する ことでアウセスが可能である ろ アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない	製産級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない 1) A ~ Dが含まれてお 祭1 CAPTCHAチェックは接奨
49 50	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	認証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス	認証後のページを指定する ことでアクセスが可能である る アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている	要証券のページを指定す ることでアクセスができ ない 通常ルーザではアクセス 権限がない情報や機能へ アクセスできない 1) A~Dが含まれてお 申1 CAPTCHAチェックは振奨 り、かつ、別ユーザの飯 案ではないが、リスク板域に
49 50	クロスサイトリクエストフォ	<del>)</del> ージェ Ϳ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス ②Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行 われている確定地理において、以下のいずれかの情報が含まれているかを確 影	認証後のページを指定する ことでアクセスが可能である る アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている	製産級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない 1) A ~ Dが含まれてお 祭1 CAPTCHAチェックは接奨
49 50	クロスサイトリクエストフォ	+ージェリ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行	超級扱いページを指定する ことでアクセスが可能である ろ アクセス練限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれていない 3) スーDか含まれている 3、別ユーザの値でも主常	製造機のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 機能がない情報機能へ アクセスできない  1) AーDが含まれてお
49 50	<b>ク</b> ロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	設証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 医存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストペッダに含まれた値によって、セッション管理が行 われている確定処理において、以下のいずれかの情報が含まれているかを確 認 私利用者のパスワード	認証後のページを指定する ことでアクセスが可能である ろ アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない 2) A~Dが含まれている が、別ユーザの値でも正常 に処理が行われる 3) A~Dが含まれている	要証券のページを指定す ることでアケセルができ ない 通常ユーザではアクセス 機能がない情報や構能へ アクセスできない  1) A~Dが含まれてお り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理が行われ、なる ない ※2 Refererチェックは機災を ない ※2 Refererチェックは機災を ない ※2 Refererチェックは機災を
49	クロスサイトリクエストフォ	÷ージェリ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製能状態でしか表示できないページに、ロダイン認能していない状態でアクセス 既存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookieなどリクエストペッダに含まれた値によって、セッション管理が引 われている確定処理において、以下のいずれかの情報が含まれているかを確 認 A 利用者のパスワード B. CSRF対策トークン C. セッションID D. CAPTCHA	認証後のページを指定する ことでアクセスが可能である ろ アクセス様限がない情報や 機能が閲覧、操作できる 1)A~Dが含まれている が、別ユーザの値でも正常 に処理が行われている が、値を削削、もしてはバ フメータンと削除した場合	認証後のページを指定す ることでアケセスができ ない 遺産ユーザではアクセス 権限がない情報や構能へ アクセスできない  \$\$\text{\$\e
49 50	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 器 用 名のCSRF対ストーク C、セッションID D、CAPTCHA ②Aトのからまれている場合に、ユーザαで利用されている値をユーザβで料	超延度かページを指定する ことでアクセスが可能である。 アクセス様限がない情報や 機能が閲覧、操作できる リカーのか含まれていない 2) Aーのか含まれている が、別ユーツの低でも正常 に処理が行われる 3) Aーのか含まれている が、値を削除、もしくはパ フメータごと削除した場合 に処理が行われる	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない  1) AーDが含まれてお り、かつ、別ユーザの値 家ではないが、リスク低減に では正常に処理がわれたな ない 変 Refererチェックは構奨等 ではないが、リスク低減に ない り、たい。観やパラメー ろごと削削しても正常に 処理が行われない
49 50	クロスサイトリクエストフォ	ŧージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行列: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製鉱状態でしか表示できないページに、ロダイン認証していない状態でアクセス  版作URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 関してアクセス  ①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行 われている確定処理において、以下のいずれかの情報が含まれているかを確 認 A 利用者のパスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②A~Dが含まれている場合に、ユーザαで利用されている値をユーザβで利 用まれている値に変更してリクエストを送信し、処理が行われるか確認	超延度かページを指定する ことでアクセスが可能である 万クセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれている が、別ユーザの値でも正常 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	及延後のページを指定す ることでアケセスができ ない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない  1) A~Dが含まれてお 切、かつ、別ユーザの値、窓ではないが、リスク低域に では正常に処理が行われな など 2 Refererチェックは推奨等 ではないが、リスク低域にな カンとも開始しても正常に 処理が行われない 3) Refererチェックが行
49 50	クロスサイトリクエストフォ	÷−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 総 利用者のバスワード B、CSRF対策トーフン C、セッションID Q.AーDが含まれている場合に、ユーザαで利用されている値をユーザβで利用されている値に変更してリクエストを活信し、処理が行われる小確認 (別へのか含まれている場合に、ユーザαで利用されている値を削らしく	超延度かページを指定する ことでアクセスが可能である 万クセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれている が、別ユーザの値でも正常 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	製産機のページを指定す なことでアクセスができ ない 通常コーザではアクセス 観察ない情報機能へ アクセスできない  3) AーOが含まれてお 申1 CAPTCHAチェックは推奨 の、かつ、別ユーザの額 定ではないが、リスク転続に では正常に製造が行われな ない 次2 Refererチェックは機災案 ではないが、リスク転減にな の、かつ、値やパラメー る ンと目開放しても正常に 処理が行われない 3) Refererチェックが行 われており、正常に処理
49 50	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  版作URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行 おれている確定処理において、以下のいずれかの情報が含まれているかを確 製 A 利用者のバスワード B. CSRF対策トークン C. セッションID O. CAPではA ②Aへのが含まれている場合に、ユーザαで利用されている値をユーザβで利 用されている値に変更してリクエストを送信し、処理が行われるか確認 (③AへDが含まれている場合に、ユーザαで利用されている値をカー・サβで利 用されている値に変更してリクエストを送信し、処理が行われるか確認 (④AへDが含まれている場合に、ユーザので利用されている値を対策、もし はバラメータごと前除してリクエストを送信し、処理が行われるか確認	超延度かページを指定する ことでアクセスが可能である 万クセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれている が、別ユーザの値でも正常 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	及延後のページを指定す ることでアケセスができ ない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない  1) A~Dが含まれてお 切、かつ、別ユーザの値、窓ではないが、リスク低域に では正常に処理が行われな など 2 Refererチェックは推奨等 ではないが、リスク低域にな カンとも開始しても正常に 処理が行われない 3) Refererチェックが行
49 50	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 総 利用者のバスワード B、CSRF対策トーフン C、セッションID Q.AーDが含まれている場合に、ユーザαで利用されている値をユーザβで利用されている値に変更してリクエストを活信し、処理が行われる小確認 (別へのか含まれている場合に、ユーザαで利用されている値を削らしく	超延度かページを指定する ことでアクセスが可能である 万クセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれている が、別ユーザの値でも正常 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	製産機のページを指定す なことでアクセスができ ない 通常コーザではアクセス 観察ない情報機能へ アクセスできない  3) AーOが含まれてお 申1 CAPTCHAチェックは推奨 の、かつ、別ユーザの額 定ではないが、リスク転続に では正常に製造が行われな ない 次2 Refererチェックは機災案 ではないが、リスク転減にな の、かつ、値やパラメー る ンと目開放しても正常に 処理が行われない 3) Refererチェックが行 われており、正常に処理
50 51	クロスサイトリクエストフォ	r−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	設証状態でしか表示できないページに、ロダイン認証していない状態でアクセス  版存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストペッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 認 A利用者のパスワード B. CSR7対策トークン C. セッションリ D. CAPTCHA ②本へか浴含まれている場合に、ユーザαで利用されている値をユーザルです。 ③本のか浴含まれている場合に、ユーザαで利用されている値を利能、もしくはパラメータごと削除してリクエストを送信し、処理が行われるか確認 ③本へか浴含まれている場合に、ユーザαで利用されている値を削除、もしくはパラメータごと削除してリクエストを送信し、処理が行われるか確認 ③本へか浴含まれている場合に、ユーザαで利用されている値を削除、もしくはパラメータごと削除してリウエストを送信し、処理が行われるか確認	超越接かべージを指定する ことでアクセスが可能である ろ フクセス様限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれている が、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれている が、仮と手段 に処理が行われる 3) AーDが含まれている が、値を削除した場合 に処理が行われる 4) Refererチェックが行わ れていない	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない   第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理がわれた ない シアのからまれてお り、かつ、値やパラメー クごを削むしても正常に 別 Refererチェックは横災等 ではないが、リスク低減にな り、かつ、値やパラメー カンと前れない 別 Refererチェックが行 かれており、正常に処理 が行われない
49 50 51	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所 登録、送信などの確定処理	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級技能でしか表示できないページに、ロダイン認証していない状態でアクセス  度存URLのフォルダパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエスト〜ッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 私 利用者のパスワード B、CSRF対策トークン C、セッションID D、CAPTCHA  ②Aへのか含まれている場合は、ユーザαで利用されている値をユーザβで利用されている値に変更してリクエストを送信し、処理が行われるか確認 (②Aへのか含まれている場合が、ユーザαで利用されている値を加ました。 はパテンターダンと削除してリクエストを送信し、処理が行われるか確認 (②Aへのか含まれている場合が後、もしくはエリタのURLではない値に変更して、リクエストを送信し、処理が行われるか確認 (②Referrer を開除、もしくは正規のURLではない値に変更して、リクエストを送信し、処理が行われるか確認 CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを推測	超越接かべージを指定する ことでアクセスが可能である ろ フクセス様限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれている が、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれている が、仮と手段 に処理が行われる 3) AーDが含まれている が、値を削除した場合 に処理が行われる 4) Refererチェックが行わ れていない	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない   第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理がわれた ない シアのからまれてお り、かつ、値やパラメー クごを削むしても正常に 別 Refererチェックは横災等 ではないが、リスク低減にな り、かつ、値やパラメー カンと前れない 別 Refererチェックが行 かれており、正常に処理 が行われない
50 50	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所 登録、送信などの確定処理	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級状態でしか表示できないページに、ロダイン認証していない状態でアクセス  版作URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行 おれている確定処理において、以下のいずれかの情報が含まれているかを確 個 A 利用者のバスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②AへDが含まれている場合に、ユーザαで利用されている値をユーザβで利 用されている値に変更してリクエストを送信し、処理が行われるか確認 (③AへDが含まれている場合に、ユーザので利用されている値を判断、もしく はバラメータごと開除してリクエストを送信し、処理が行われるか確認 ②AをBriefathの解しているようと必能し、処理が行われるの確認 ②AをBriefathの解し、しては正規のURLではない値に変更して、リクエストを 送信し、処理が行われるの確認 CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数 こるRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを推測	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている に処理が行われる 3) A~Dが含まれている に処理が行われる 4) RefereFェックが行われていない な、値を削除した場合 た処理が行われる 4) RefereFェックが行われていない	製産級のページを指定す ることでアクセスができ ない。 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない り、かつ、別ユーザの値、変ではないが、リスク低域に では正常に処理が行われる 窓 2 Refererチェックは機関素 ではないが、リスク低域にな り、かつ、健やパラメー カニと開除しても正常に 処理が行われない 3) Refererチェックが行 われており、正常に処理 が行われない。 CSRF対策トークンの規 CSRF対策トークンの規 CSRF対策トークンの固定長で
50			認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョで利用されている値をユーザβで利用されている値に変更してリクエストを运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきたと、第二の上ですログインすることを適応し、MP・コーデでログインすることを適応の比較	超越後のページを指定する ことでアセスが可能である うとでアセスが可能である アクセス権限がない情報や 機能が閲覧、操作できる リカーのが含まれていない は、別ユーザの値でも正常 が、別ユーザの値でも正常 が、別ユーザの値でも正常 が、原本が行われる が、仮理が行われる 4)Refererチェックが行わ れていない と、 と、 と、 と、 と、 と、 と、 と、 と、 と、 と、 と、 と、	製産機のページを指定す ることでアクセスができ ない 通常コーザではアクセス 組織ないに特殊機能へ アクセスできない  3) A〜Oが含まれてお の、かつ、別ユーザの値 変ではないが、リスク転続に では正常に発展が計われた ない 変と Refererチェックは推奨を ではないが、リスク転続に なり、かつ、値やパラメー る っとと削除しても正常に 処理が行われない 3) Refererチェックが行 われており、正常に処理が行われない 3) Refererチェックが行 われており、正常に処理 が行われない CSRF対策トークンが固定長で 関性が何らず推薦不可 ない場合は疑う余地がある
50 50 51	クロスサイトリクエストフォ	セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級状態でしか表示できないページに、ロダイン認証していない状態でアクセス  版作URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行 おれている確定処理において、以下のいずれかの情報が含まれているかを確 個 A 利用者のバスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②AへDが含まれている場合に、ユーザαで利用されている値をユーザβで利 用されている値に変更してリクエストを送信し、処理が行われるか確認 (③AへDが含まれている場合に、ユーザので利用されている値を判断、もしく はバラメータごと開除してリクエストを送信し、処理が行われるか確認 ②AをBriefathの解しているようと必能し、処理が行われるの確認 ②AをBriefathの解し、しては正規のURLではない値に変更して、リクエストを 送信し、処理が行われるの確認 CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数 こるRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを推測	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている 以 別ユー切の信さ上下 3) AーDが含まれている が、別ユーサの信でも正常 に処理が行われる 3) AーDが含まれている が、仮を削除、もしくはバ フメータンと削除した場合 に処理が行われる 4) Refererチェックが行わ れていない していない していない していない ログイン成功前と同じセッ	型度級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 連常スーザではアクセス 機能がない情報機能へ アクセスできない  第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理が行われ ない 2) A~Dが含まれてお っ、かつ、銀や・ヴァメー のどと削除しても正常に 対策と解や・デェックは構奨室 ではないが、リスク低減にな る アクエと削除しても正常に 対策と呼ばないが、リスク低減にな の、かつ、銀や・ヴァメー のどと削除しても正常に 対策とい 3) Refererチェックが行 われており、正常に処理 が行われてが CSRF対策トータンの規 CSRF対策トークンが固定長で ログイン成功後に新しい
50 50 51			認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョで利用されている値をユーザβで利用されている値に変更してリクエストを运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきたと、第二の上ですログインすることを適応し、MP・コーデでログインすることを適応の比較	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる リカーのが含まれていない は、別ユーザの値でも正常 に処理が行われる 3) みーのか含まれている は、別エーザの値でも正常 に処理が行われる 4) 低を削除した場合 は処理が行われる 4) Refererチェックが行われていない ないない センボルカリ推測可能 ログイン成功前と同じセッション川が確核して使用さ	型産級のページを指定す ることでアクセスができない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない  1) A~Dが含まれてお の、かつ、別ユーザの紙 窓ではないが、リスク低減に では正常に処理が行われな 窓 2 Refererチェックは機関素 ではないが、リスク低減にな 3) Refererチェックに機関素 ではないが、リスク低減にな 3) Refererチェックが行 われており、正常に処理 が行われない  CSRF対策トークンの規 関性が利らず推測不可 ない場合は疑う余地がある
50 50 51		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョで利用されている値をユーザβで利用されている値に変更してリクエストを运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきたと、第二の上ですログインすることを適応し、MP・コーデでログインすることを適応の比較	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている 以 別ユー切の信さ上下 3) AーDが含まれている が、別ユーサの信でも正常 に処理が行われる 3) AーDが含まれている が、仮を削除、もしくはバ フメータンと削除した場合 に処理が行われる 4) Refererチェックが行わ れていない していない していない していない ログイン成功前と同じセッ	製産機のページを指定す ることでアクセスができ ない。 通常ユーザではアクセス 機能がない情報機能へ アクセスできない  1) AーDが含まれてお り、かつ、別ユーザの値 変ではないが、リスク低機に では正常に処理がわれた ない ではないが、リスク低機に なり、かつ、観やパラメー クごを所われない 3) Refererチェックは機関案 ではないが、リスク低機にな り、かつ、観やパラメー クごを所能しても正常に 30 Refererチェックが行 われており、正常に処理 が行われない  CSRF対策トークンの規 関性が利らず推測不可 ない場合は疑う余地がある ログイン成功機に新しい セッション/IDが操行され、古いセッション/IDが操行さ れ、古いセラッション/IDは
50 50 51 53		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL バラメータ	型級状態でしか表示できないページに、ログイン認証していない状態でアクセス  既存URLのフォルグパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付まれている確定処理において、以下のいずれかの情報が含まれているかを確  あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を列除、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのとではない値に変更して、リクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測  - エーザアカウンドことに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - ログイン成功後に新しい認証に使うセッションIDが発行されるかを確認	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる リカーのが含まれていない は、別ユーザの値でも正常 に処理が行われる 3) みーのか含まれている は、別エーザの値でも正常 に処理が行われる 4) 低を削除した場合 は処理が行われる 4) Refererチェックが行われていない ないない センボルカリ推測可能 ログイン成功前と同じセッション川が確核して使用さ	型度級のページを指定することでアクセスができない 通常ユーザではアクセス 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない  お、カーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 3) Referseチェックは機関薬 ではないが、リスク低減にな ない。 3) Referseチェックが行 われており、正常に処理 が行われない。 CSRF対策トークンの環 CSRF対策トークンが開定長で ログイン成功後に新しい セッションIDが発行され、古いセッションIDが発行され、古いセッションIDが発行され、 においセッションIDが発行され、古いセッションIDが発行され、 においセッションIDが発行され、 においセッションIDが発行され、 は、おいセッションIDが発行され、 においセッションIDが発行され、 においては、 にはいいては、 においては、 にはいいては、 においては、 にはいては、 にはいては、 にはいてはいいには、 にはいてはいいにはいいにはいいは、 にはいいてはいいにはいいには
50 50 51 52 53		セッションフィクセイション(セッション周	認可制御が必要な箇所  空縁、送信などの確定処理  CSRF対策トークンを使用している策所  ログイン機能	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス  度存URLのフォルダバス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  ②Cookiaなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョで利用されている値をユーザβで利用されている値に変更してリクエストを运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきたと、第二の上ですログインすることを適応し、MP・コーデでログインすることを適応の比較	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている い、別ユーザの信でも正常 に処理が行われる 3) AーDが含まれている が、例ユーザの信でも正常 に処理が行われる 4) Refererチェックが行わ れていない して、 と処理が行われる 4) Refererチェックが行わ れていない して、 との理が行われる 4) Refererチェックが行わ れていない して、 との理が行われる もれている もれている もれている もれている もれている もれている もれている もれている もれている もれでいる は、個を呼ばると は、 とのでは とのできまれている もれている もれている もれている もれている もれている もれでも もれでいる もれでも もれでも もれでも もれでも もれでも もれでも もれでも もれで	型度級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 連常な一ザではアクセス 機能がない情報機能へ アクセスできない  第71 A-Dが含まれてお り、かつ、別ユーザの飯 変ではないが、リスク低減に では正常に処理がわけれた ない 2) A-Dが含まれてお っ、かつ、銀や・ヴァメー のどと削除しても正常に 効果を持ちない 3) Refererチェックは構製室 ではないが、リスク低減にな る カブとが開起しても正常に 短期が行われており、正常に処理 が行われており、正常に処理 が行われており、正常に処理 が行われており、正常に処理 ない場合は疑う余地がある ログイン成功後に新しい セッションIDが場件さ
50 50 51 52		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所 ログイン機能 ログイン前に機骸情報がセッション変数に移納	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	型級状態でしか表示できないページに、ログイン認証していない状態でアクセス  既存URLのフォルグパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付まれている確定処理において、以下のいずれかの情報が含まれているかを確  あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を列除、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのとではない値に変更して、リクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測  - エーザアカウンドことに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - ログイン成功後に新しい認証に使うセッションIDが発行されるかを確認	超越機かページを指定する ことでアクセスが可能である フクセス様限がない情報や 機能が閲覧、操作できる リカーDが含まれていない ターDが含まれていなが、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれているが、値を削除、もしくはパ くが、別ユーザの値でも正常 が、原生が行われる 4) Refererチェックが行わ は、経理が行われる 4) Refererチェックが行わ はでいない でが、かり、単一のでは、 では、 では、 では、 では、 では、 では、 では、 では、 では、	型産級のページを指定す ることでアクセスができない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない  1) A~Dが含まれてお の、かつ、別ユーザの紙 変ではないが、リスク低減に では正常に処理が行われな の、かつ、銀やパラメー カンと制能しても正常に 処理が行われない 3) Refererチェックは推奨等 ではないが、リスク低減にな も 20 Refererチェックは推奨等 ではないが、リスク低減にな な 20 Refererチェックが行われない。 3) Refererチェックが行われない。 CSRF対策トークンの膜 助性が利らず推測不可 ない場合は疑う余地がある ログイン成功後に新しい セッション/Dが発行さ れ、古いセッション/Dは 微震情報人力後に新しい セッション/Dが発行さ れ、古いセッション/Dは
50 50 50 50 50 50 50 50 50 50 50 50 50 5		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所 ログイン機能 ログイン前に機骸情報がセッション変数に移納	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	型級状態でしか表示できないページに、ログイン認証していない状態でアクセス  既存URLのフォルグパス、ファイル名などから推測を行い、URLの一部を変 更してアクセス  「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付まれている確定処理において、以下のいずれかの情報が含まれているかを確  あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を列除、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのとではない値に変更して、リクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測  - エーザアカウンドことに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - 同一ユーザでログインするごとに恋途の比較 - ログイン成功後に新しい認証に使うセッションIDが発行されるかを確認	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている い、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれている が、例ユーザの値でも正常 に処理が行われる 4) Refererチェックが行わ れていない と処理が行われる 4) Refererチェックが行わ れていない センションIDが構練して使用さ はる場合 に必理が行われる もれている もれている もれている もれている もれている もれている もれている もれている もれている もれている もれている は、個を呼ばる上 に処理が行われる もれている もれている もれている もれている もれている もれている もれている もれている もれている もれでいる は、個を を は、関土 を と し に を と と と と と と と と と と と と と と と と と と	型度級のページを指定することでアクセスができない 通常ユーザではアクセス 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない  第71 A-Dが含まれており、かつ、別ユーザの値、変ではないが、リスク低域にてないでは正常に処理が打される。 20 A-Dが含まれており、かつ、観やパラメー カンと別能しても正常に 知恵が行われない 31 Refererチェックが行われており、正常に処理 が行われない 51 Refererチェックが行われており、正常に処理 が行われており、正常に処理 が行われており、正常に処理 が行われてが、リングが開発に対していまからが発行され、古いセッション川のは機能される 観微情報入り後に新しい セッション川のが発行され、古いセッション川のは機能される 観微情報入り後に新しい セッション川のは発音されています。

No. 大分類	中分類	小分類	診断を実施すべき箇所	ベイロード・検出パターン	操作を行う対象	診断方法	脆弱性がある場合の結果		備考
54		CookieのHttpOnly属性未設定	Cookie 発行処理			Set-CookieのHttpOnly属性が付与されているかを確認	レスポンスヘッダの Set-	レスポンスヘッダの	
							Cookieヘッダフィールド値		
							に"HttpOnly"属性が指定さ	フィールド値に	
							れていない	"HttpOnly"属性が指定さ れている	
5		推測可能なセッションID	セッションID発行時			セッションIDを複数集めて規則性があることを確認し、セッションIDを推測	As a common of the Hill House at the		Anna Canada Data de Estado
9		推測可能なセッションID	セッションID地行時			セッションIDを検索集のく規則性があることを確認し、セッションIDを推測 ・ユーザアカウントごとに差異の比較	でツンヨンIDに規則性かめ り推測可能		セッションIDが固定長でない 場合は疑う余地がある
						・発行時の日時による差異の比較	2 1600 2185	T1 9 7 1690 T T1	40 C (***C ) 3(2)C(2-0)-0
						<ul> <li>発行回数による差異の比較</li> </ul>			
†	情報漏洩	クエリストリング情報の漏洩	すべて			セッションIDや機微情報がURLに含まれていないか確認	URLにセッションIDや機微	URLにセッションIDや機	
							情報が含まれている	微情報が含まれていない	
							(同じスキームの) 他サイ		
							トに遷移した際に、		
							Refererヘッダで内容が漏		
67							洩する。Webサーバやプロ		
							キシーサーバにログとして		
		キャッシュからの情報漏洩	機微情報が含まれる画面			レスポンス内で適切にキャッシュ制御を行っていることを確認	残る。) レスポンスヘッダのCache-	レスポンスヘッダの	
		ヤヤッシュからの情報構改	機体情報からまれる画面			レスホンス内で適切にキャッシュ制御を行っていることを構認	Controlヘッダフィールド	Cache-Controlヘッダ	
							値に"no-store"が指定され	フィールド値に"no-	
							ていない	store"が指定されている	
58		パスワードフィールドのマスク不備	パスワード入力画面			パスワード入力に使用するinputタグのtype属性に"password"が指定されて	inputタグのtype属性が	inputタグのtype属性が	
						いることを確認	"password"ではない	"password"である	
59		画面表示上のマスク不備	全般			マスクすべき情報が画面上に表示されていないことを確認	マスクすべき情報が画面上	マスクすべき情報が画面	主なマスクすべき情報として
							に表示されている	上に表示されていない	はクレジットカード番号や
									PINコード、パスワード
60		HTTPS利用時のCookieのSecure属性未設定	E Set-Cookieヘッダフィールドがある箇所			HTTPS利用時のSet-CookieヘッダフィールドにSecure属性があることを確		レスポンスヘッダの	
						18	Cookieヘッダフィールド値 に"Secure"属性が指定され		
							こ Secure 腐性が損走され ていない	メイールト値に Secure 属性が指定されている	
61		パスワードの平文保存	パスワードリセット			パスワードリセットを実行			平文なのか可逆暗号なのかは
01		7 TOTAKIT	7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7			AND PURENT	される/メールで送られて	TTREACHAIRI (CARTY 7 G)	判断できない
							< 3		1200 1 2 3 1
62			パスワード変更画面、管理者画面			パスワード変更画面、管理者画面にアクセス	登録したパスワードが表示	表示されない	平文なのか可逆暗号なのかは
							される/inputタグに埋まっ		判断できない
							ている		
63		HTTPSの不備	全般			機微情報を取り扱うWebページ(フォームの表示、送信先共に)にアクセス	HTTPで通信している	HTTPSで通信している	
64			HTTPS箇所			HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの併用)	HTTPSだけでアクセスすべ	HTTPS以外ではアクセス	
							きページがHTTPでもアク セス可能となっている	できない	
66			HTTPS箇所			HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在)		HTTPSとHTTPのコンテ	
0.5			11111 Spa(7)			THI SEIGHE CV-S - 27 7 7 E MAD (THI CHITI SOURCE)	ツが混在している	ンツが混在していない	
66			HTTPS箇所			動作対象ブラウザで証明書を確認	ブラウザで証明書の警告が		警告が出る場合には以下のい
							出る	が出ない	ずれかに該当する可能性があ
									S .
									・自己証明書が用いられてい
67									<b></b>
									<ul><li>有効期限が切れている</li></ul>
									<ul><li>証明書のホスト名がサイト</li></ul>
									と一致してない ・推奨されない署名アルゴリ
									イ担災されない者もフルコリ ズムの利用
									<ul> <li>不適切な鍵長</li> </ul>
		不要な情報の存在	すべて			HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータベース構造に	情報が含まれている	情報が含まれていない	
ı [						などに係わる情報)」や「公開不要な情報(個人名、メールアドレス、ミド			
						ルウェアの情報、過去の公開していたコンテンツのリンク、プライベートIP			
						アドレスなど)」が含まれていることを確認			
co business a constitution of	の診 サーバソフトウェアの設定の	ディレクトリリスティング	すべて		URL	Webサーバ上の発見したディレクトリにアクセスして、ディレクトリ内の			含まれているファイルによっ
	不備	バージョン番号表示	h			ファイルが一覧表示されないかを確認	が一覧表示される	ルが一覧表示されない	てリスクは異なる
断項目   60			すべて			サーバやアプリケーション、ミドルウェア、フレームワークなどのバージョ ン番号が表示されていないかを確認	バージョン番号が表示され z	バージョン番号が表示さ れない	
		2 2 2 8 3 3 4 4			1		V		
			すべて	TRACE, TRACK	リクエストメソッド	メソッドを変更してサーバにアクヤス	TRACE, TRACK x y ~ F	TRACE. TRACK x 'V ···	
		不要なHTTPメソッド	すべて	TRACE, TRACK	リクエストメソッド	メソッドを変更してサーバにアクセス	TRACE、TRACKメソッド が機能する	TRACE、TRACKメソッ ドが機能しない	
			すべて	TRACE, TRACK OPTIONS	リクエストメソッド リクエストメソッド	メソッドを変更してサーバにアクセス メソッドを変更してサーバにアクセス	TRACE、TRACKメソッド が機能する AllowヘッダにGET、	TRACE、TRACKメソッドが機能しない Allowヘッダが存在しな	
		不要なHTTPメソッド					が機能する	ドが機能しない	
		不要なHTTPメソッド					が機能する AllowヘッダにGET、	ドが機能しない	
		不要なHTTPメソッド					が機能する AllowヘッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する (PUT、DELETE、TRACE	ドが機能しない Allowヘッダが存在しない AllowヘッダにGET、 HEAD、POST、	
		不要なHTTPメソッド					が機能する AllowヘッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する	ドが機能しない Allowヘッダが存在しない AllowヘッダにGET、 HEAD、POST、 OPTIONS以外のメソッ	
		不要なHTTPメソッド 不要なHTTPメソッド	すべて	OPTIONS	リクエストメソッド	メソッドを変更してサーバにアクセス	が機能する Allow〜ッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する (PUT、DELETE、TRACE など)	ドが機能しない Allowヘッダが存在しない AllowヘッダにGET、 HEAD、POST、 OPTIONS以外のメソッ ドが存在しない	
	公開不要な機能・ファイル・・	不要なHTTPメソッド 不要なHTTPメソッド		OPTIONS	リクエストメソッド	メソッドを変更してサーバにアクセス  メソッドを変更してサーバにアクセス  サンブルファイルや、バックアップファイルなど、アブリケーションの動作	が機能する Allow〜ッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する (PUT、DELETE、TRACE など)	ドが機能しない Allowヘッダが存在しない AllowヘッダにGET、 HEAD、POST、 OPTIONS以外のメソッ	
	公開不要な機能・ファイル・・・	不要なHTTPメソッド 不要なHTTPメソッド	すべて	OPTIONS	リクエストメソッド	メソッドを変更してサーバにアクセス	が機能する Allow〜ッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する (PUT、DELETE、TRACE など)	ドが機能しない Allowヘッダが存在しない AllowヘッダにGET、 HEAD、POST、 OPTIONS以外のメソッ ドが存在しない	