

総合セキュリティ診断サービス FAQ

共通項目

Q1	セキュリティ診断の種類について教えてください。
A1	<p>【ネットワーク診断】 ネットワーク経由のセキュリティ診断。 診断対象機器に対して調査パケットを送信し、そのレスポンスから脆弱性を分析。 外部から確認できる脆弱性を検出したい場合に有効な診断方法です。</p> <p>【ホスト診断】 診断対象機器の内部からのセキュリティ診断。 診断対象機器上で診断用ツールを実行し、 システム内部に存在する脆弱な構成について分析。 システム内部に存在する脆弱性を検出したい場合に有効な診断方法です。</p> <p>【データベース診断】 データベースに特化したセキュリティ診断。 サーバに搭載されているデータベースに対して、 侵入検査と、監査の2種類の方法を用いて、脆弱性を分析。 データベースに特化した脆弱性を検出したい場合に有効な診断方法です。</p> <p>【Webアプリケーション診断】 Webアプリケーションに特化したセキュリティ診断。 クロスサイトスクリプティングやSQLインジェクションといった、 Webアプリケーションに特化した脆弱性を検出した場合に有効な診断方法です。</p> <p>これら診断サービスを個々に行うのではなく、総合的に全ての診断を行うことを推奨しています。</p>
Q2	診断前に必要な作業はありますか？
A2	診断対象機器のバックアップをお願いします。
Q3	診断はどのように行われますか？
A3	当社持込診断PCをお客様ネットワークに接続して行います。 また、ネットワーク診断やWebアプリケーション診断は、インターネット経由の診断も可能です。
Q4	診断中に診断対象機器で業務の継続は可能ですか？
A4	診断中は、占有させていただきます。そのため他のサービスの提供など行わないようにしてください。
Q5	誤検出とは何ですか？
A5	脆弱性ではないものが、判断を誤って脆弱性だと検出されてしまうことを言います。
Q6	誤検出は発生しますか？
A6	発生する場合がありますが、当社の診断サービスでは、誤検出が発生しやすい項目について、手動でチェックを行っています。
Q7	診断当日は立会いが必要ですか？
A7	診断当日はお客様に立ち会っていただきます。
Q8	納品物はどのようなものが渡されるのですか？
A8	診断結果報告書をお渡しします。
Q9	検出された脆弱性の対処は行っていただけますか？
A9	対処案の提示のみとなり、対処はお客様に行っていただけます。
Q10	診断結果に対するQAサポート期間はどのくらいですか？
A10	診断結果報告会から1ヶ月有効です。
Q11	セキュリティ診断後に対策を行った場合、再診断は必要ですか？
A11	診断後に行われた設定・対処が適切に行われているか確認を行うためにも、再診断を行うことを推奨します。
Q12	再診断はサービスに含まれていますか？
A12	再診断はオプションとなり、別途お見積もりとさせていただきます。
Q13	ペネトレーションテストはしていないのですか？
A13	お客様のご要望により、ペネトレーションテストを実施することが可能です。
Q14	診断予定時間内に診断が終わらない場合はどうなるのですか？
A14	診断の進捗具合から診断時間の修正、見込み時間をお客様にご報告します。 その都度、お客様と作業・時間の調整をさせていただきます。
Q15	診断時に取得した情報に対してどのような情報漏えい対策をしていますか？
A15	情報漏洩対策として、診断PCとモバイルハードディスクには、暗号化とパスワードを設定しています。また診断時に取得した情報は、入室制限のかかった部屋でアクセス制限されたファイルサーバに置かれています。



ネットワーク診断

Q1	ネットワーク診断では何をチェックできるのですか？
A1	外側から発見できる脆弱性をチェックできます。詳細については、『ネットワーク診断内容』をご参照ください。
Q2	ポートスキャンは何番までをチェックできますか？
A2	デフォルトでは、wellknownポート(1~1023番)とよく使用されるサービスをチェックします。オプションで、1~65535番までチェックすることも可能です。
Q3	診断時間はどのくらいかかりますか？
A3	環境によって変わりますが、一般的に1時間程度となります。
Q4	事前に必要な情報はありますか？
A4	以下の情報をご提供願います。 診断対象とするIPアドレス数、OS、ネットワーク図
Q5	診断後に必要な作業はありますか？
A5	診断の負荷により、診断対象機器が不安定になる可能性があるため、再起動と動作確認が必要となります。
Q6	診断可能な機器の種類を教えてください。
A6	TCP/IPで通信できる機器であれば全て診断可能です。
Q7	レポートは日本語ですか？
A7	ツールレポート、および報告書は日本語で提供いたします。

『ネットワーク診断内容』

脆弱性分類	診断内容
CGI スクリプト	/cgiIPアドレスhf cgiスクリプトのような、セキュリティ脆弱性を持つCGIスクリプトが存在するかどうかを確認します。
DoS	ICMP フラグメンテーション攻撃、Ping of Death、その他、マシンやサービスをオフラインにするなどといったサービス妨害を引き起こす、サービス妨害攻撃に対する耐性を確認します。
データベース	Oracle、MySQL、MSSQLなどデータベースアプリケーションに存在する脆弱性を調査します。
FTPサーバ	ファイル転送プロトコルに関する脆弱性を調査します。
メールサーバ	SMTP、IMAP、POP2、POP3やその他インターネットメールサーバの脆弱性を調査します。
NetBIOS	NETBIOSプロトコルの脆弱性を調査します。リモートのWindows ファイル共有内のパーミッション問題を検出します。
レジストリ	脆弱性確認に利用可能なレジストリ値の存在を確認します。
リモートアクセス	リモートアクセスエージェントの脆弱性を調査します。
RPCサービス	Remote Procedure Call (RPC) サービスの脆弱性を調査します。
SSHサーバ	Secure Shell サーバの脆弱性を調査します。
Webサーバ	WWWサーバの脆弱性を調査します。
バックドア	ポートスキャンとプロトコル判定機能によりバックドアプログラムによって稼働するオープンポートを検出します。
ユーザー	脆弱な設定が行われているユーザーを検出します。
ピアツーピア	ポートスキャンや稼働プロセスの調査によりP2Pプログラムの稼働を調査します。
スパイウェア	ポートスキャンや稼働プロセスの調査によりスパイウェアプログラムの稼働を調査します。

ホスト診断

Q1	ホスト診断では何をチェックできるのですか？
A1	OSの設定をチェックできます。詳細については、『ホスト診断内容』をご参照ください。
Q2	診断時間はどれくらいですか？
A2	診断対象機器のスペックやアカウント数によって時間は異なりますが、目安として30分程度とお考えください。
Q3	事前に必要な情報はありますか？
A3	以下の情報をご提供願います。 診断対象機器台数、OS、ネットワーク図
Q4	事前に必要な作業はありますか？
A4	特にありません。
Q5	診断時に必要な作業はありますか？
A5	管理者権限でログインをしていただきます。
Q6	サーバの設定を変更することはありますか？
A6	ありません。
Q7	診断後に必要な作業はありますか？
A7	動作確認が必要となります。(ホスト診断では再起動は必要ありません。)
Q8	レポートは日本語ですか？
A8	ツールレポート、および報告書は日本語で提供いたします。
Q9	診断可能な機器を教えてください。
A9	ホスト診断ツールのベンダサイトをご確認ください。 東芝ITサービス株式会社(対応OS)へ http://www.it-serve.co.jp/products/security/02_01.htm

【ホスト診断内容】

脆弱性分類	診断内容	OS種別	
セキュリティパッチ	最新のセキュリティパッチが適用されているかを確認します	共通	
パスワード設定	最小パスワード長	最小パスワード長がしきい値以上に設定されているかを確認します。	共通
	パスワードの有効期間	パスワードの有効期間がしきい値以下に設定されているかを確認します。	共通
	パスワードの変更禁止期間	パスワードの変更禁止期間がしきい値以上に設定されているかを確認します。	共通
	パスワードの履歴保持数	パスワードの履歴の保存数がしきい値以上に設定されているかを確認します。	共通
	パスワードが未設定のアカウント	パスワードのないアカウントの検出を試みます。	共通
	パスワードが推測可能なアカウント	簡単に推測できるパスワードを持つアカウントの検出を試みます。	共通
	パスワードを変更できないアカウント	パスワードを変更できないアカウントの検出を試みます。	Windows
	無期限のパスワードを持つアカウント	無期限パスワードを持つアカウントの検出を試みます。	Windows
	パスワードの変更警告期間	パスワードの変更警告期間がしきい値以上に設定されているかを確認します。	UNIX
	長期間パスワードが変更されていないアカウント	同じパスワードを使用しつづけているアカウントの検出を試みます。	UNIX
	パスワードロックされているアカウント	パスワードロックされているアカウントの検出を試みます。	UNIX
	アカウント設定	ユーザー権限の割り当て	ユーザー権限の割り当て状況を確認します。
管理ユーザーの変名		Administrator アカウント名が変更されているかを確認します。	Windows
ゲストユーザーの変名		Guest アカウント名が変更されているかを確認します。	Windows
アカウントのログオン時間		ログオン時間に制限のないアカウントの検出を試みます。	Windows
アカウントのログオン先		ログオンできるワークステーションに制限のないアカウントの検出を試みます。	Windows
アカウントの有効期限		有効期限のないアカウントの検出を試みます。	Windows
管理ユーザー		管理者権限を持つアカウントの検出を試みます。	共通
システムに存在するアカウントの設定		ユーザー アカウントが正しく設定されているかを確認します。(passwd ファイルの設定、ID重複の有無など)	UNIX
ホームディレクトリの設定		アカウントのホームディレクトリが正しく所有されているかを確認します。(所有者、パーミッションなど)	UNIX
特権を持つアカウント/グループ		特権を持っている可能性のあるアカウント/グループを検出します。	UNIX
ログイン設定	ログインシェルが正しく設定されているかを確認します。(所有者、パーミッション)	UNIX	
アカウントロック	アカウントロック	アカウントのロックアウトは有効に設定されているかを確認します。	Windows
	アカウントロックの回数	ロックアウト回数が適切に設定されているかを確認します。	Windows
	アカウントロックの期間	ロックアウト期間がしきい値以上に設定されているかを確認します。	Windows
	アカウントロックのリセット	ロックアウト カウンタをリセットする時間がしきい値以上に設定されているかを確認します。	Windows
	休止アカウント	休止アカウント(X日以上ログインされていないアカウント)の検出を試みます。	共通
	ログオン前のメッセージ	ログオン前のユーザーへのメッセージ通知設定を確認します。	Windows
	前回ログオンしたアカウント名	ログオン ダイアログ ボックスでユーザー名を表示しない設定になっているかを確認します。	Windows
	ログオンダイアログボックスからのシャットダウン	ログオン ダイアログ ボックスでシャットダウンできない設定になっているかを確認します。	Windows
	ログオン時間	ログオン時間をオーバーしたユーザーは強制切断される設定になっているかを確認します。	Windows
	管理ユーザーのリモートログイン	rootアカウントでのリモートログインが制限されているかを確認します。	UNIX
ネットワーク設定	ドメインの信頼関係	マシンが信頼しているドメインの検出を試みます。	Windows
	共有ディレクトリの存在	共有ディレクトリの検出を試みます。	Windows
	フルコントロール可能な共有ディレクトリ	[Everyone]グループにフルコントロールを与えている共有ディレクトリの検出を試みます。	Windows
	共有ディレクトリのアクセス権	共有ディレクトリに設定されているアクセス権の検出を試みます。	Windows
	RRASサービス	リモート アクセス サービス(RRAS)が無効に設定されているかを確認します。	Windows
	起動中のサービス	明示的にオープンされているTCP/UDPポートの検出を試みます。	共通
	sendmailの設定	sendmailが正しく設定されているかを確認します。	UNIX
	FTPの設定	FTPが正しく設定されているかを確認します。	UNIX
監査設定	FTPの無効化	TFTPが無効に設定されているかを確認します。	UNIX
	成功の監査	成功監査ポリシーの設定を確認します。	Windows
	失敗の監査	失敗監査ポリシーの設定を確認します。	Windows
	セキュリティイベントログの保持	セキュリティイベントのログ記録が上書き禁止に設定されているかを確認します。	Windows
	セキュリティイベントログのサイズ	セキュリティイベントのログのサイズがしきい値以上に設定されているかを確認します。	Windows
	イベントログの記録	イベントログ記録が有効に設定されているかを確認します。	UNIX
	プロセスアカウント	プロセス アカウントが有効に設定されているかを確認します。	UNIX
	ログインログの記録	ログインログの記録が有効に設定されているかを確認します。	UNIX
	SUコマンドの記録	SU コマンドログの記録が有効に設定されているかを確認します。	UNIX
	スタートアップ設定	インストールされているサービス	マシンにインストールされているサービスの検出を試みます。
リモートからのレジストリアクセス	リモート レジストリ アクセスが禁止に設定されているかを確認します。	Windows	
RCファイルの設定	rc スクリプト ファイルが正しく設定されているかを確認します。	UNIX	
ディスクの空き容量	ディスクの空き容量が十分かを確認します。	UNIX	
スタートアップファイル	ユーザー スタートアップ ファイルが正しく設定されているかを確認します。(パーミッション、PATH、UMASK(しきい値以上)など)	UNIX	
ホームディレクトリ配下のファイル、ディレクトリ	ユーザー ホームディレクトリ配下のファイル/ディレクトリが正しく設定されているかを確認します。(所有者、パーミッション、不審なファイルの存在など)	UNIX	

データベース診断

Q1	データベース診断では何をチェックできるのですか？
A1	データベースに特化した脆弱性をチェックできます。詳細については、『データベース診断内容』をご参照ください。
Q2	ライセンス数のカウントの仕方を教えてください。
A2	データベースインスタンス数＝ライセンス数となります。
Q3	診断時間はどのくらいですか？
A3	目安として、約1時間半程度となります。
Q4	事前に必要な情報はありますか？
A4	ユーザー名とユーザーパスワード、データベース使用のポート番号が必要になります。
Q5	事前に必要な作業はありますか？
A5	データベースのバックアップをお願いします。
Q6	診断時に必要な作業はありますか？
A6	管理者権限でログインをしていただきます。
Q7	対象となるデータベースを教えてください。
A7	データベース診断ツールベンダサイトをご確認ください。 アイディネットワークス株式会社 (AppDetectiveが対象とするシステム) へ http://www.idnetworks.co.jp/products/appsec/
Q8	データベース診断後に必要な作業はありますか？
A8	動作確認が必要となります。
Q9	レポートは日本語ですか？
A9	ツールから出力されるレポートは、英語のみとなりますが、報告書は日本語でご提供します。

『データベース診断内容』

脆弱性分類	診断内容
アカウント権限	アカウントに適切なロールや権限が設定されているか確認
パスワードポリシー	パスワードの期限や文字数などが適切に設定されているか確認
パスワード強度	デフォルトのパスワードや推測しやすいパスワードがないか確認
パスワード保護	パスワードファイルへのアクセスが制限されているか確認
アカウントロック	ログインに何回も失敗した場合にロックアウトする設定になっているか確認
テーブルのアクセス制限	テーブルに適切なアクセス制限が設定されているか確認
リソース制限	リソース制限が適切に設定されているか確認
監査	監査ログを適切に取得しているか確認
ログイン認証	通信を暗号化をするなど適切なログイン設定がされているか確認
レジストリパーミッション	Oracle関連のレジストリに適切なアクセス制限が設定されているか確認
ファイルパーミッション	Oracle関連のファイルに適切なアクセス制限が設定されているか確認
トロイの木馬	Oracleの実行ファイルが置き換えられているか確認



Webアプリケーション診断

Q1	Webアプリケーション診断で何をチェックできるのですか？
A1	クロスサイトスクリプティングやSQLインジェクションといった、Webアプリケーションに特化した脆弱性をチェックできます。詳細については、『Webアプリケーション診断内容』をご参照ください。
Q2	診断時間はどのくらいですか？
A2	目安として、1日10画面程度の診断が可能です。
Q3	事前に必要な情報はありますか？
A3	診断対象とするWebサイトの画面遷移図や操作マニュアルなどの提示をお願いします。
Q4	事前に必要な作業はありますか？
A4	診断対象機器のデータのバックアップ、診断用アカウントの準備をお願いします。
Q5	サーバ内のファイルへの書き込みは発生しますか？
A5	Webアプリケーションでファイルやデータベースへの書き込み処理を実装している場合は発生します。
Q6	診断後に必要な作業はありますか？
A6	システムのリストアと診断対象機器の動作確認が必要となります。
Q7	携帯サイトの診断は可能ですか？
A7	条件により診断可能です。別途お問い合わせください。
Q8	レポートは日本語ですか？
A8	ツールレポート、および報告書は日本語で提供いたします。
Q9	診断可能な機器を教えてください。
A9	HTTP、HTTPSを使用しているサイトであれば、全て診断可能です。

『Webアプリケーション診断内容』

脆弱性分類	脆弱性	診断内容
サーバ設定	製品の設定ミス	不要なメソッドの存在や、不適切な設定の存在を確認します。
認証	製品の既知の脆弱性	使用しているミドルウェア製品の既知の脆弱性の存在を確認します。
	認証方式	脆弱な認証方式を採用していないかを確認します。
	パスワード強度	認証で使用しているパスワードルールが適切であるかを確認します。
	権限昇格	ユーザーの権限の昇格ができないかを確認します。
セッション管理	セッション管理方式	脆弱なセッション管理方式を使用していないかを確認します。
	セッションID強度	セッションIDの強度を確認します。
暗号化	セッションのライフサイクル	セッションIDの再利用ができないことを確認します。
	通信の暗号化	重要な情報が暗号化して送信されていることを確認します。
パラメータ改竄	証明書	サーバ証明書の内容が適切であるかを確認します。
	クロスサイトスクリプティング	クロスサイトスクリプティングが実行できないかを確認します。
	コマンドインジェクション	OSコマンドを実行できないかを確認します。
	SQLインジェクション	SQLコマンドを実行できないかを確認します。
	パラメータ改竄	パラメータ値を不正に改竄した値が受け付けられないかを確認します。
	バッファオーバーフロー	大量のデータを送り込んだ場合、正常にエラー処理されるかを確認します。
	強制ブラウジング	公開されていない重要データに直接アクセスできないことを確認します。
	ディレクトリトラバーサル	相対パスを使用してディレクトリ移動できないことを確認します。
	Hiddenフィールドの改竄	Hiddenフィールドの受け渡しに起因する問題がないかを確認します。
	エラー処理	エラー処理が適切に行われ、過剰な情報をエラーメッセージに含めていないかを確認します。
その他	クロスサイトリクエストフォージェリ	クロスサイトリクエストフォージェリが実行できないかを確認します。
	クライアントのセキュリティ	クライアントのセキュリティを考慮しているかを確認します。
	ソース中のコメント	HTMLソースファイル内に過剰な情報が含まれていないかを確認します。

＜お問い合わせ＞

株式会社富士通ソーシャルサイエンスラボラトリー
1-0063 川崎市中原区小杉町1-403(武蔵小杉タワープレイス)
Tel:044-739-1251
E-mail:ssl-info@cs.jp.fujitsu.com