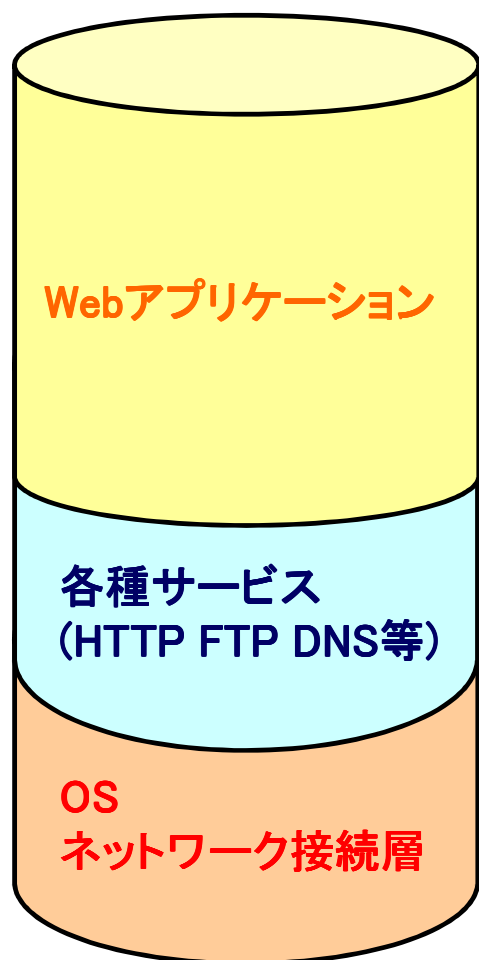


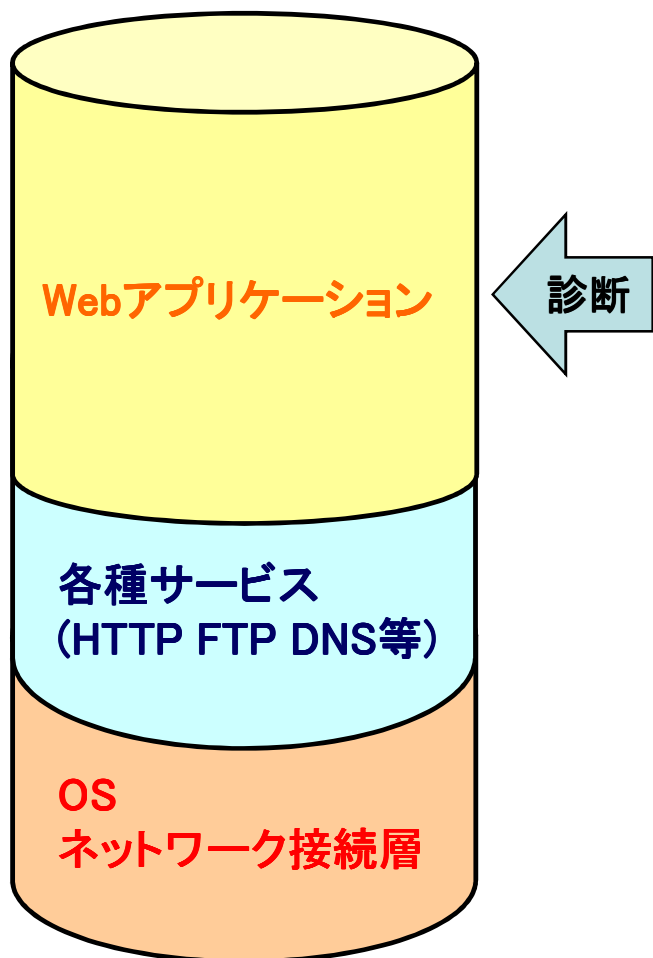
セキュリティ診断の概要



1. ネットワーク診断

- ・OSや各種サービスにおける既知の脆弱性の有無を調査する。
- ・不要なサービスが公開されていないか調査する。
- ・SSL等の通信の暗号化対策が適切か調査する。
- ・各サーバの設定が適切か調査する。

セキュリティ診断の概要



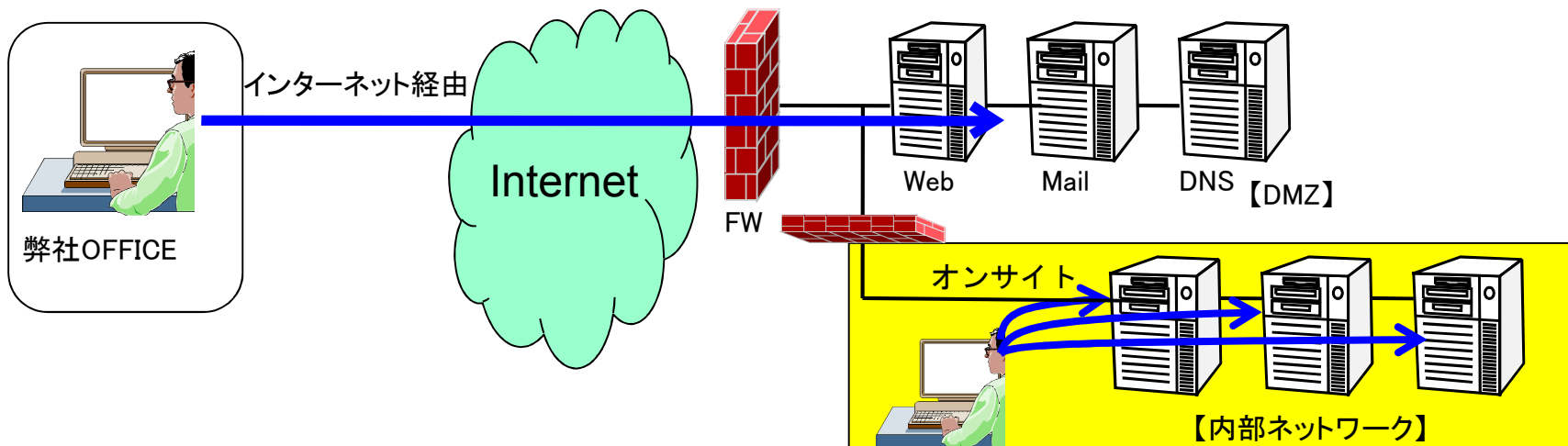
2. Webアプリケーション診断

- ・ファイアウォールでは防げないWebコンテンツ上の脆弱性の有無を調査する。

- ・OSやソフトウェアのセキュリティパッチを適用しただけでは防げない問題点を調査する。

【例】 ●Webサイトからのデータベースへの侵入
●コンテンツ書き換え
●正規ユーザへのなりすまし 等

1. ネットワーク診断の概要



No.	診断種類	診断環境	診断概要	特徴
1	脆弱性診断	インターネット経由	弊社オフィスからインターネット経由でサーバやNW機器の脆弱性を主に複数のスキャナ(商用、フリー)を利用して検出します。	インターネットからのセキュリティ侵害につながる脅威を短期間・低コストで洗い出すことを目的とする場合に有効な診断方法です。
		オンサイト	ご指定いただいた内部LANセグメントからサーバやNW機器の脆弱性を主に複数のスキャナ(商用、フリー)を利用して検出します。	内部犯行も想定し、セキュリティ侵害につながる脅威を短期間・低コストで洗い出すことを目的とする場合に有効な診断方法です。
2	ペネトレーション診断 (PCIDSS対応)	インターネット ／ オンサイト	インターネット経由及びご指定いただいた内部LANセグメントからサーバやNW機器に対して、脆弱性を検出し、その脆弱性を利用して実際の攻撃者と同様の手段で不正侵入の可否を手作業で診断し、システムの堅牢性を評価します。	ネットワーク経由で発生しうる、全てのセキュリティ侵害につながる脅威を洗い出すことを目的とした場合に有効な診断方法となります。

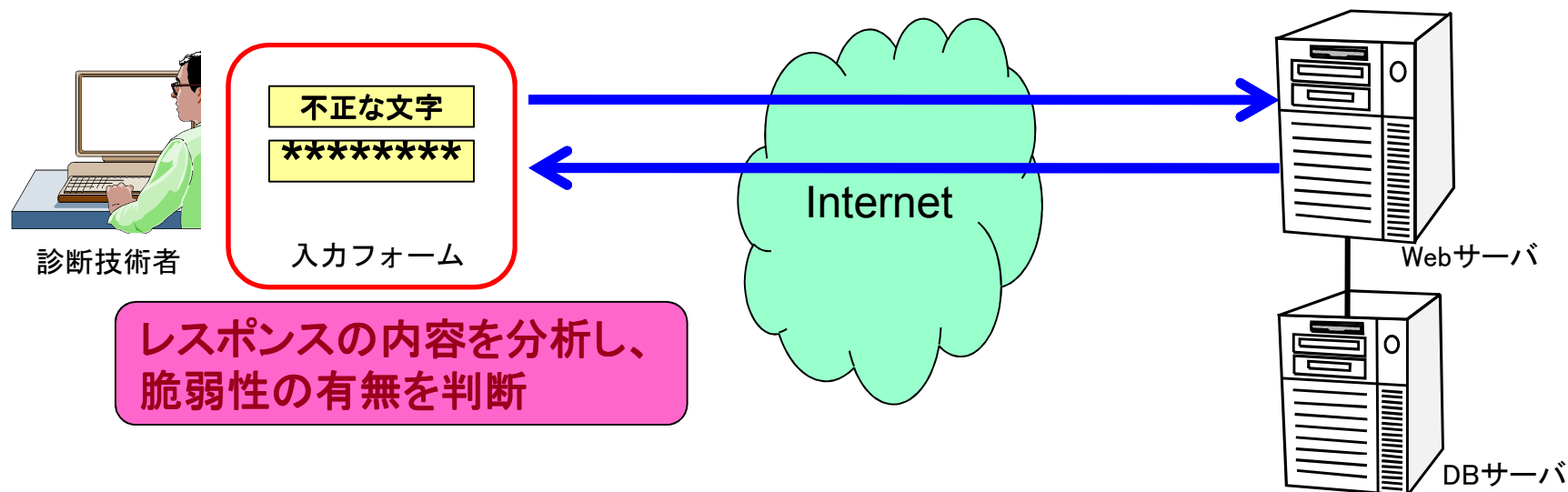
1. ネットワーク診断項目(その1)

項番	診断項目	概要	
		調査・確認事項	主な脅威
1	OSやアプリケーションソフトウェアの既知の脆弱性	OSのバージョンやセキュリティパッチの適用状況等を確認します。	既知の脆弱性を利用した任意のコマンドの実行やサービス妨害攻撃を受ける可能性があります。
2	脆弱なパスワード設定	認証を伴うサービスに対して容易に推測可能なパスワードが設定されていないか確認します。	パスワードが容易に推測可能な場合、なりすましにより不正にシステムにアクセスされる可能性があります。
3	脆弱性の知られているCGIスクリプトの存在	CGIスクリプトの存在確認及びバージョン等を確認します。	既知の脆弱性を利用した任意のコマンドの実行やサーバの内部情報を取得される可能性があります。
4	不要と思われるサービスの稼働	サービスの動作状況を確認します。	セキュリティ上不要なサービスの動作は、攻撃者に攻撃の糸口を多く与えてしまいます。
5	ワーム感染の有無	既にワームに感染していないかを確認します。	攻撃や不正侵入、サービス妨害に利用されている可能性があります。
6	稼働中のサービスからの情報取得	稼働しているサービスのバナー情報等を取得します。	動作しているプログラムの特定等により、不正侵入等の攻撃に利用される可能性があります。
7	アカウントポリシーの調査	アカウントロックアウト値などを取得し設定値の妥当性を評価します。	設定値に不備がある場合、パスワード推測攻撃が容易になったり、攻撃の成功確率が上がったりする可能性があります。
8	サービス妨害の可能性	サービス妨害攻撃を実施できる可能性があるか確認します。	提供しているサービスを停止または、アクセスすることが困難になる可能性があります。
9	サーバ設定上の問題	サーバ設定(書込権限やアクセス制御設定等)がセキュリティ的に妥当であるか確認します。	セキュリティ的に不備がある設定の場合、不正侵入等の攻撃に利用される可能性があります。 例) 書込権限に不備がある場合、任意のファイルを作成されたりする可能性があります。
10	DNSゾーン転送の可否	DNSゾーン転送を不特定のホストに許可しているか確認します。	ドメイン内に存在すると思われるホストと利用用途を容易に特定することが可能となり攻撃対象が多くなります。
11	DNS再帰的問い合わせの可否	DNS再帰的問い合わせを許可している設定か確認します。	DNS再帰的問い合わせを許可している場合、DNSサーバの不正利用や他のサーバを攻撃するDDoS攻撃に利用される可能性があります。
12	DNSダイナミックアップデートの可否	DNSレコードをアップデート可能な設定であるか確認します。	任意のレコード追加により悪意あるサイトに利用者を誘導することが可能です。

1. ネットワーク診断項目(その2)

項番	診断項目	概要	
		調査・確認事項	主な脅威
13	メール不正中継の可否	メールサーバのメール中継の設定状況を確認します。	不正中継が可能な場合、スパムメールの送信などに利用される可能性があります。
14	メールサーバによるユーザ情報漏洩問題	メールサーバでユーザに許可しているコマンドやサーバの応答等を確認します。	許可しているコマンド及びコマンドの応答結果によりシステムに登録されているユーザ情報を特定され、パスワード推測攻撃に利用される可能性があります。
15	Webサーバ上のデフォルトコンテンツの存在	システム導入時にインストールされるデフォルトコンテンツが存在するか確認します。	デフォルトコンテンツに脆弱性があった場合、それを利用した不正侵入や、攻撃に利用可能な情報を取得される可能性があります。
16	Proxy設定の不備	Proxyサーバの設定がセキュリティ的に妥当であるか確認します。	セキュリティ的に不備がある設定の場合、Proxyサーバを他のシステムを攻撃する際の踏み台として利用される可能性等があります。
17	プライベートアドレス漏洩	対象からの応答にプライベートアドレス等が含まれていないか確認します。	システムの内部ネットワーク情報が漏えいすることにより、不正侵入等の攻撃に利用される可能性があります。
18	不適切なSSL証明書の利用	SSLサーバ証明書を取得して信頼できる証明書であるか確認します。	SSLサーバ証明書に不備がある場合、サーバの实在証明ができず、利用者が悪意ある偽のサーバに誘導されても判断がつかず、利用者が誘導された偽のサーバに情報を送信してしまう可能性があります。
19	エラーメッセージによる情報漏洩	エラーメッセージが返るようなリクエストを送り、エラーメッセージにサーバ内部情報等が含まれていないか確認します。	サーバ内部情報等がふくまれている場合、取得した情報を不正侵入等の攻撃に利用される可能性があります。
20	バックドア検出 等	バックドアが既に仕込まれていないかなど様々な項目を確認します。	バックドアがある場合、既に不正にシステムを利用されている可能性があります。

2. Webアプリケーション診断の概要



【診断対象】 PCサイト、携帯サイト、スマートフォンサイト

【診断方法】 Webアプリケーションの脆弱性を網羅的に調査します。

手作業でアプリケーションの構造を考慮しながら検査を実施するため、診断ツールでは検出が困難な脆弱性の検出が可能です。

また、単に脆弱性の存在を調査するだけでなく、その脆弱性が具体的にシステムに対してどのような影響を与えるかまで検証します。

報告書は、技術者による5段階評価、総評、脆弱性及びリスク(影響度)の解説、対応策をわかりやすく画面キャプチャを取り入れて作成します。

【診断環境】 インターネット経由から診断を行います。

2. Webアプリケーション診断項目

検査項目	典型的な脆弱性	説明
ユーザ認証に関する項目	<ul style="list-style-type: none"> 脆弱なパスワードの存在 認証設定の不備 パスワードリマインダの不備 SSL証明書の妥当性 HTTPSの不備 	<p>認証を迂回して、不正にサービスを利用したり、他人になりすましてアプリケーションを利用したりすることができないか調査します。</p> <p>また、暗号化通信の有無やサーバ証明書の設定が適切に行われていることを確認します。</p>
コンテンツアクセス承認に関わる項目	<ul style="list-style-type: none"> 推測可能なセッションID アクセス制御機構の不備 セッション終了処理の不備 セッションフィクセーション 	<p>利用者毎の情報を保持する目的で使用されるセッションIDについて、なりすましによる不正アクセスや個人情報などの漏洩が発生する可能性がないか調査します。</p>
クライアントを対象とした攻撃に関する項目	<ul style="list-style-type: none"> クロスサイトスクリプティング コンテンツ詐称 	<p>アプリケーション利用者のブラウザを攻撃することで、任意のスクリプトの実行やコンテンツの詐称ができないか調査します。</p>
コマンド実行に関する項目	<ul style="list-style-type: none"> バッファオーバーフロー(内部サーバエラー含む) OSコマンドインジェクション SQLインジェクション(SQLエラーの発生含む) SSIインジェクション LDAPインジェクション 各種インジェクション 	<p>Webアプリケーションに対して、通常の使用では使用しない文字列等を入力した場合のプログラムの挙動を確認し、サービスの異常停止やOSやデータベースの不正操作、機密情報の漏えいの可能性などを調査します。</p>
情報取得に関する項目	<ul style="list-style-type: none"> サーバの設定(ディレクトリ一覧表示等) ディレクトリトラバーサル 強制ブラウザ・認証回避 不要なコンテンツの存在 コモンファイルエクステンション 	<p>WebサーバやWebアプリケーションに添付されているデフォルトページやサンプルページの有無を確認します。</p> <p>また、他のページからリンクされずにサーバ内に隠れて存在するファイルなどを探索することで、予期しない情報が露呈しないことを確認します。</p>
アプリケーション機能の悪用に関する項目	<ul style="list-style-type: none"> クロスサイトリクエストフォージェリ(CSRF) 改行コードインジェクション アップロード機能の不正利用 機能の悪用 サービス妨害 自動アクセス防止の不備 	<p>アプリケーションの構造上や機能上の弱点について、各種攻撃が可能か調査します。</p>