

セキュリティ診断サービスのご紹介



018-0053-20

本サービスは、日本セキュリティ監査協会（JASA）が審査登録を行う「情報セキュリティサービス基準審査登録制度」の登録サービスです。

株式会社 日立ソリューションズ・クリエイト

Contents

1. セキュリティ診断の3つのメリット
 2. 日立ソリューションズ・クリエイトのセキュリティ診断サービス
 3. セキュリティ診断サービスの概要
 4. 診断結果報告書例
 5. 作業スケジュール
 6. ご提供サービス種別
- ご参考 -



1. 「セキュリティ診断」 3つのメリット ～ Webサイトを守るための「セキュリティ診断」～

1-1 近年のサイバー攻撃の傾向

プラットフォーム、アプリケーションのぜい弱性を悪用したサイバー攻撃が依然として上位にある

順位	2021年(組織)	2022年(組織)	2023年(組織)
1位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取
4位	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい
5位	ビジネスメール詐欺による金銭被害	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	内部不正による情報漏えい	脆弱性対策情報の公開に伴う悪用増加	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
7位	予期せぬIT基盤の障害に伴う業務停止	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	ビジネスメール詐欺による金銭被害
8位	インターネット上のサービスへの不正ログイン	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害
10位	脆弱性対策情報の公開に伴う悪用増加	不注意による情報漏えい等の被害	犯罪のビジネス化(アンダーグラウンドサービス)

出典：独立行政法人情報処理推進機構（IPA）発行「情報セキュリティ10大脅威」より

Webサイトで検出した脆弱性の事例

セキュリティ対策を実施している大企業でも・・・

業種	資本金	検出した脆弱性	想定される最悪の被害
製造A社	100億円以上	予測されやすいパスワードにより GUIにてログイン可能	● システム破壊 ● 機密情報漏洩 ● 踏み台
金融B行	200億円以上	OSコマンドインジェクション により任意のコマンド実行、 サーバへの侵入が可能	● システム破壊 ● Webサイト改ざん ● 機密情報漏洩 ● 踏み台
運輸C社	200億円以上	メールヘッダインジェクション によりメールの第三者中継が可能	● スパムメール送信 ● 機密情報漏洩
製造D社	200億円以上	SQLインジェクション によりユーザの個人情報が閲覧可能	● Webサイト改ざん ● 機密/個人情報漏洩
情報E社	5000億円以上	ディレクトリトラバーサル により任意のファイルを閲覧可能	● 機密情報漏洩
製造F社	50億円以上	バッファオーバーフロー により未ログイン状態で遠隔操作可能	● システム破壊 ● 機密/個人情報漏洩 ● 踏み台

Webサイトのセキュリティ対策は十分か？



ネットワーク

サーバー

Web
アプリケーション

Webサイトを攻撃から守るため、多くの企業様がしっかりと対策されています

しかし、「大切なWebサイト」、対策は十分なのか・・・



- ▶ 対策にはどうしても「もれ」がある
- ▶ 新しい脆弱性は大丈夫か
- ▶ 対策の費用が大きすぎ、優先度がわからない



お役にたてるのは・・・

Webサイトの「**健康診断**」＝セキュリティ対策の「**現状把握**」

Webサイトの健康診断なら「セキュリティ診断」

Webサイトの「健康診断」にはどんな方法があるのでしょうか。



- ・ ネットワーク機器の構成や設定は大丈夫か？
- ・ サーバー・DB等の設定に問題はないか？パッチは最新か？
- ・ Webアプリケーションの設計・ソースコードに問題はないか？

心配です…



対策の
スピード感

費用

担当者の
負荷

「ホワイトハットハッカーの視点」で、
「システムの外部」からチェックできる「セキュリティ診断」が有効です。

「セキュリティ診断」 3つのメリット

メリット 1

ホワイトハットハッカー視点での網羅的なチェックができる

外部からのブラックボックステストで、脆弱性を発見できます。

メリット 2

たくさんの準備がなくても実施できる

サーバールームや、運用会社、開発ベンダーへの確認、ベンダーに支払う費用……。セキュリティ診断は外部から、スタート可能です。

メリット 3

第三者による診断結果を受け取ることができる

客観的な診断結果を基に、現状を把握できます。
診断の結果から優先度を付けての対策が可能です。

2. 日立ソリューションズ・クリエイトの セキュリティ診断サービス

2. セキュリティ診断サービスの3つの特徴

日立ソリューションズ・クリエイトの「セキュリティ診断」

ツール+「手動診断」

ツールで網羅性を確保すると共に、ツールではできない診断内容を
当社の **専任技術者（ホワイトハットハッカー）** が手動で診断します。

わかりやすい「Webアプリケーション診断結果報告書」

わかりやすく詳細な報告内容。特にWebアプリケーション診断では、**再現手順**を記載しており、
ぜい弱性の修正後の確認に便利です。

柔軟なオプション



初めてなので、
どこからチェックしたら
いいかわからない



脆弱性の
修正後の再確認も
含めてやりたい



結果だけ
もらえれば十分

さまざまなご要望に応える、手厚いオプションをご用意しております。



3. セキュリティ診断サービスの概要

ネットワーク型診断サービス

Standard プラン

Professional プラン

サーバー・ネットワークデバイスの、OS/アプリケーションに対する、セキュリティホールの有無をインターネット経由（リモート）またはお客さま先（オンサイト）で診断します。

Webアプリケーション診断サービス

Standard プラン

Professional プラン

お客さまにて作成されたWebコンテンツに対して、SQLインジェクションなどに代表されるWebアプリケーション特有のセキュリティホールの有無をネットワーク経由で診断。

個別アプリケーション診断（ファジング診断）サービス

組込み機器や制御システムを含め、個別アプリケーションの通信に存在するぜい弱性を独自ツールを使用して診断。

また、攻撃者がシステム侵入時に入口として利用するぜい弱性の有無も診断。

診断方法



リモート診断

当社よりインターネットを介して、グローバルIPアドレスを持つデバイスに対して診断します。本診断は、外部クラッカーと同じ視点で客観的に検査するため、実際に攻撃される可能性のあるセキュリティホールを検出することができます。



オンサイト診断

お客さまの内部ネットワークから、重要なサーバーに対して診断します。外部クラッカーにファイアウォールを破られた場合や内部クラッカーが存在した場合に、どのようなセキュリティリスクがあるかを予測することができます。イントラネットや、外部公開前のサーバーに対しても有効です。



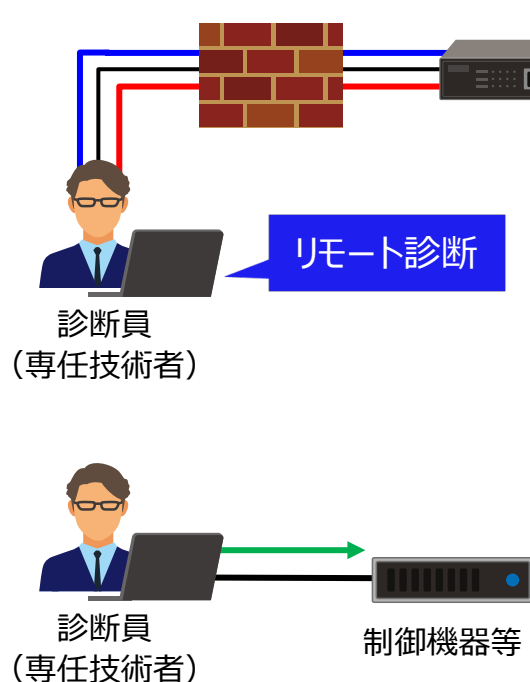
リモート & オンサイト診断

お客さまネットワーク上の同一デバイスをリモートとオンサイトの両方から診断します。より効果的な診断を実施できます。

3-3 セキュリティ診断のイメージ

日立ソリューションズ・クリエイト

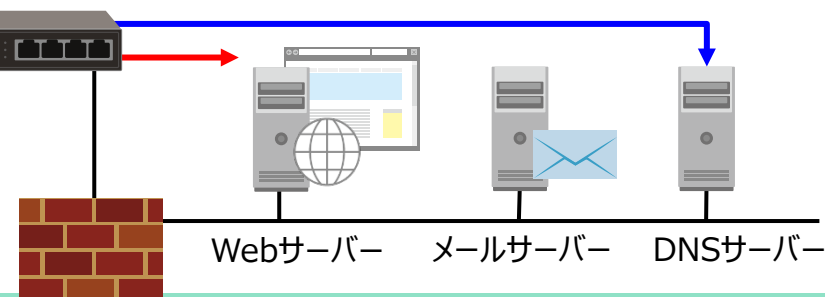
セキュリティ診断ルーム



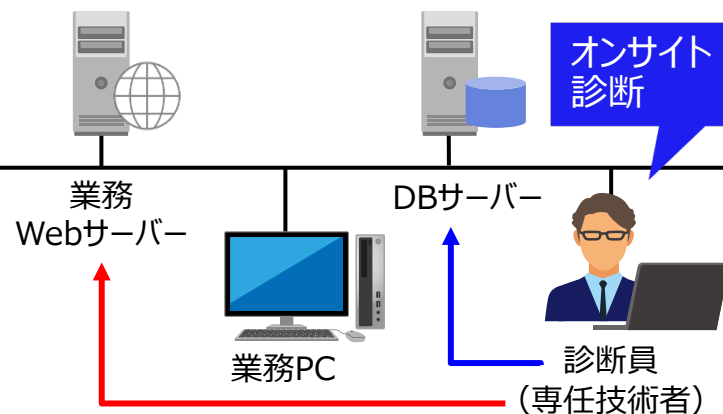
- ネットワーク型診断サービス (Network-type Diagnosis Service) - Blue arrow
- Webアプリケーション診断サービス (Web Application Diagnosis Service) - Red arrow
- 個別アプリケーション診断サービス (Individual Application Diagnosis Service) - Green arrow

お客さま

DMZ、外部向けネットワーク、クラウド環境



社内ネットワーク



商用のぜい弱性スキャンツール（Rapod7社 Nexpose）を主体とした、疑似攻撃による診断を実施します。診断内容は以下のものがあります。

Standard プラン

- サービスポートの確認（1～65535番）
- ぜい弱性スキャナツールによる通常攻撃診断
- ぜい弱性スキャナツールによる使用不能（DoS）攻撃診断
- 報告書の作成・送付

Professional プラン

Standardの内容に加えて、以下の診断を実施します。

- オープンポートに対する手動確認（OS種別／アプリケーション種別の確認）
- 危険度大のぜい弱性について速報の作成・送付
- メール診断（メールサーバーの不正中継診断・メールアカウントの類推）
- DNS診断（ゾーン転送・再帰問い合わせ）

3-4 ネットワーク型診断サービスの内容

ネットワーク型診断サービスの診断内容一覧

●：商用ツールによる診断のみ ○：商用ツール＋ホワイトハットハッカーによる手動診断

診断項目		Standard プラン	Professional プラン
標準提供	ICMP ECHO要求に対する応答の確認	●	○
	ぜい弱性スキャナ（Nexpose）による診断	●	○
	下位ポートスキャン（1～1023）	●	○
	上位ポートスキャン（1024～65535）	●	○
	OS情報の確認		○
	動作アプリケーションの確認		○
	ゾーン転送・bindバージョン照会によるDNSサーバーぜい弱性検査		○
	メールサーバーの不正中継診断・メールアカウントの類推		○
	SNMPサービスぜい弱性診断		○
	FTPサービスぜい弱性診断		○
	Webサービスぜい弱性診断		○
	その他の起動サービスのぜい弱性診断		○
オプション提供	報告会	オプション提供	
	再診断（修正後の再確認をセットでご提供）	オプション提供	
	夜間診断	オプション提供	
	休日診断	オプション提供	

Webアプリケーション検査ツールを使用し、擬似攻撃による診断を行います。
診断内容は以下のものがあります。

Standard プラン

- Webアプリケーション検査ツールによる擬似攻撃診断
- 報告書の作成・送付※

※報告書は、商用ツールが自動生成したもののご提供となります。

Professional プラン

Standardの内容に加えて、以下の診断を実施します。

- ホワイトハットハッカーによる手動診断
- 危険度大のぜい弱性について速報の作成・送付
- 手動にて発見された脆弱性を再現手順を含めて報告書に記載

Webアプリケーション診断サービスの診断内容一覧

●：商用ツールによる診断のみ ○：商用ツール＋ホワイトハットハッカーによる手動診断

診断項目		Standard プラン	Professional プラン
標準提供	クロスサイトスクリプティング	●	○
	SQLインジェクション	●	○
	OSコマンドインジェクション	●	○
	ディレクトリリストイング	●	○
	パストラバーサル	●	○
	セッションハイジャックの試み	●	○
	エラーページの検証	●	○
	認証・セッション管理	●	○
	強制ブラウジング		○
	複数のパラメータ同時改ざん		○
	Webアプリケーションのぜい弱性を利用した「なりすまし」		○
	論理的なぜい弱性（価格改ざんなど）※		○
オプション提供	報告会	オプション提供	
	画面選定ご支援	オプション提供	
	再診断（修正後の再確認をセットでご提供）	オプション提供	
	夜間診断	オプション提供	
	休日診断	オプション提供	

※ツールでは検出が困難なぜい弱性（「パラメータ名」や「アプリケーションの挙動」などから攻撃方法が考察できるぜい弱性）を診断します。

4. 診断報告書の例

ネットワーク型診断サービス

3 セキュリティ評価

御提示頂いた各診断対象のセキュリティ評価を表3-1に示します。
評価はAAA・AA・A・B・Cの5段階評価で、評価基準は以下のとおりです。

- AAA: 危険度の低い脆弱性のみを検出
- AA: 危険度中の脆弱性を検出
- A: 危険度大であるが、比較的侵入の困難な脆弱性を検出
- B: 危険度大であり、容易に侵入できる脆弱性を検出
- C: 危険度大であり、管理者権限を容易に奪える脆弱性を検出

危険度大の脆弱性は、侵入者にマシンへのアクセスを許したり、管理者権限を奪ったり、データの破壊や改ざんを許す可能性があるものです。診断対象への実際の影響度を考慮して評価をA、B、Cに細分化しています。すぐにでも改善する必要があります。

危険度中の脆弱性は、ユーザIDを奪われて、危険度大の脆弱性につながる可能性のあるものや、サービス不能攻撃によりパフォーマンスの低下を引き起こしたり、メール台にされたりする原因となるものです。危険度大ほど緊急を要しますが、できるだけ改善する必要があります。

危険度の低い脆弱性は、インフォメーション取得などの可能性があるものです。すぐに改善する必要はありませんが、順次改善する必要があります。

表3-1 セキュリティ評価

ネットワーク型診断			
項番	診断対象名	IP アドレス	セキュリティ評価
1	XX サーバ	xxx.xxx.xxx.1	AA
2	YY サーバ	xxx.xxx.xxx.2	C

本結論に至った詳細を次章以降に示します。

4 診断結果詳細

各サーバの詳細な診断結果
【ネットワーク型診断】

(1) 攻撃準備調査

攻撃者が実際にサーバに脆弱性をチェックするため、事前にそのサーバに接続を試みます。

(a) サーバ存在確認

攻撃対象のネットワーク要求(ping)が一般的に成功します。

(b) TCP サービスポートの調査

攻撃対象のサーバに開いているサービスが調査されます。本診断では、全ポートが調査されます。

(c) UDP サービスポートの調査

攻撃対象のサーバに開いているサービスが調査されます。本診断では、全ポートが調査されます。

(ご参考)UDP ポート
UDP はコネクションを確立せずに送信し、サーバから送信されたパケットが正しく届いていることが分かり、閉じていることが確認されることがあります。

(d) OS 情報の確認

OS が持つバージョン情報は、OS の脆弱性を調べる際に利用されます。

5.1.2 脆弱性診断ツールによる診断

通常診断において検出された脆弱性を以下に示します。

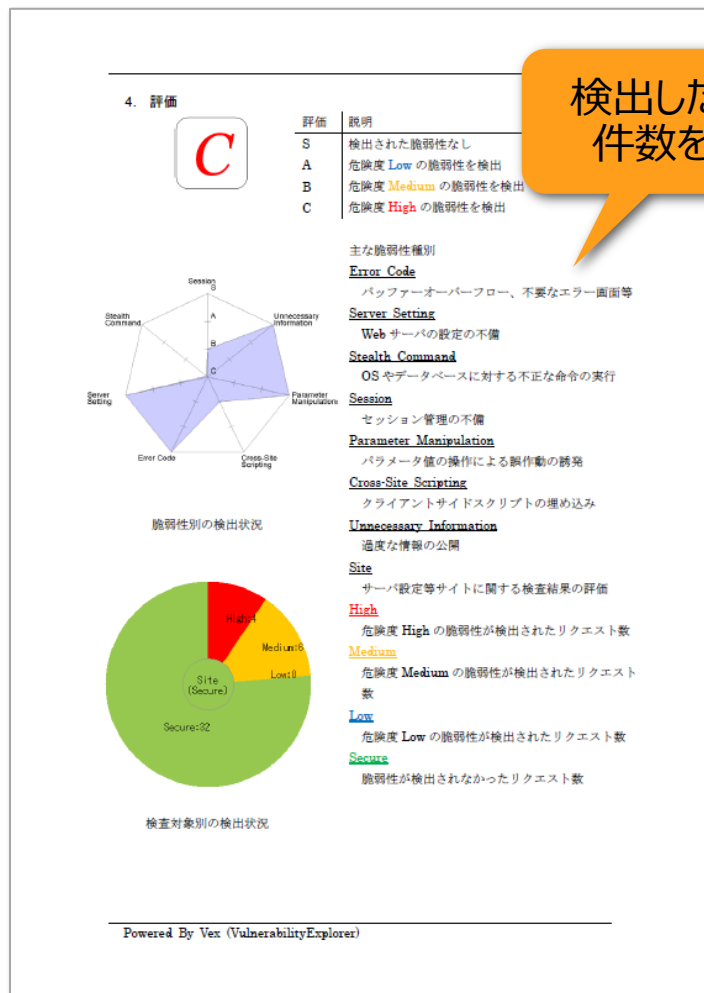
項番	1
脆弱性名	SSL/TLS プロトコルで使用する DES および Triple DES 暗号における平文のデータを取得される脆弱性
重要度	中
概要	SSL/TLS で使用される DES および Triple DES 暗号は、ブロック長が短いため、ネットワークの中継点に存在している攻撃者に暗号化通信の内容を解読される可能性があります。
修正方法	●DES および Triple DES 暗号化アルゴリズムを使用しないようにしてください。また、AES 暗号を無効化しないようにしてください。 ・〈OpenSSL の場合〉 OpenSSL 1.1.0 以上にアップデートして下さい。 デフォルトで DES および Triple DES 暗号化アルゴリズムが無効に設定されます。 ・〈Apache の場合〉 下記参照先の「SSL/TLS Strong Encryption: How-To」を参照し、DES および Triple DES 暗号化アルゴリズムを使用しないよう設定してください。 (設定例:httpd.conf) <pre>SSLCipherSuite ALL:!SSLv2:!LOW:!EXP:!ADH:!RC4:!DES:!3DES</pre> ・〈その他〉 製品開発元に問い合わせ、対策を実施することをおすすめします。 ▼OpenSSL Blog - The SSL/TLS issue, Oct 2016 - 2100 https://www.openssl.org/blog/blog/2016/08/24/sweet32/

ぜい弱性についての詳細と
対策方法をわかりやすく解説

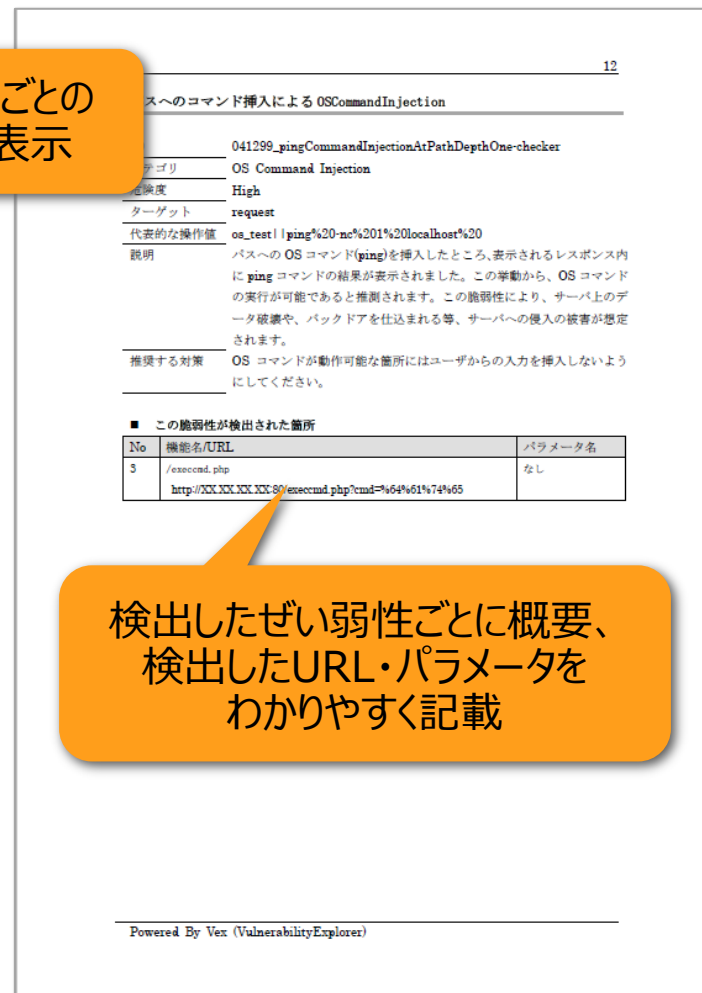
見解	●SSL/TLS Strong Encryption: How-To http://httpd.apache.org/docs/2.2/ssl/ssl_howto.html http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html 修正方法を参照し、対策することをおすすめします。対策を実施する際には利用者への影響を考慮した上で対策を検討してください。
----	---

Webアプリケーション診断サービス（Standard プラン）

Webアプリケーション検査ツールが自動生成した診断結果報告書例

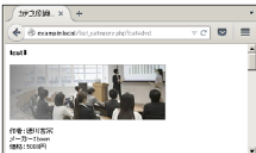


検出した危険度ごとの
件数をグラフで表示



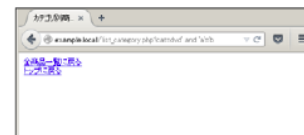
Webアプリケーション診断サービス (Professional プラン)

5.1.2.2 SQL インジェクションの脆弱性

脆弱性名	SQL インジェクションの脆弱性	
危険度	大	
概要	SQL インジェクション (SQL Injection) は Web アプリケーションに対する攻撃手法の 1 つで、SQL を使って不正にデータベースを操作することを目的としています。SQL は、データベースを操作するために一般的に使われている言語です。通常、Web サーバは利用者が Web コンテンツの入力域に入力した値をデータベースに引渡し、データベースの結果を受けて次の画面を生成します。脆弱な Web アプリケーションは、SQL を含むデータを受け取った際、その SQL を挿入した形でデータベースを呼び出してしまうため、攻撃者は、任意のテーブルを作成したり、編集、削除、もしくはユーザアカウントやパスワードなどの機密情報を入手することができます。	
対象 URL/パラメータ	URL http://example.local/list_category.php	パラメータ cat
再現方法	1) URL 「http://example.local/list_category.php?cat=dvd」のパラメータ「cat」の末尾に文字列「' and 'a'='a」を挿入してアクセスします。  2) URL 「http://example.local/list_category.php?cat=dvd」にアクセスしたときに表示される画面と同じ画面が表示されます。  3) パラメータ「cat」の末尾に文字列「' and 'a'='b」を挿入してアクセスすると、1) のときとは異なりデータが表示されません。このことから、パラメータ「cat」に設	

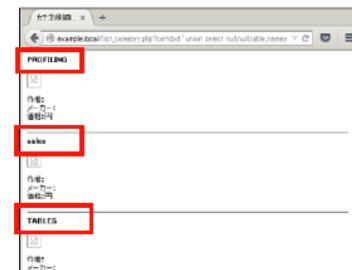
実際の攻撃手順を
わかりやすく解説

定した文字列が SQL クエリの一部として実行されていること (SQL インジェクション) が分かります。



(テーブル情報の取得)

4) パラメータ「cat」の末尾に「' union select null,null,table_name,null,null,null,(省略) from information_schema.tables order by 1 asc%23」を挿入してアクセスすると、データベースの内容 (テーブル情報) が表示されます。(下図は一部のみ)

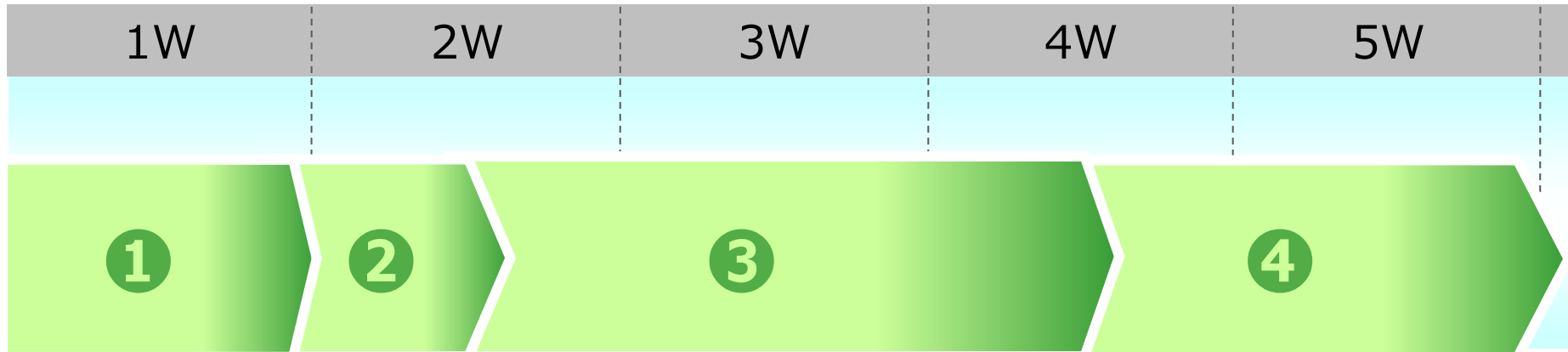


修正方法	●ユーザから受け取るデータに対して、「型・長さ・書式」などのチェックを厳しく行ってください。パラメータとして適切な値を受け取ったときのみ正常処理を行うようにしてください。
参照先	●セキュア・プログラミング講座 (IPA) http://www.ipa.go.jp/security/awareness/vendor/programmingv1/a02_01.html http://www.ipa.go.jp/security/awareness/vendor/programmingv1/a02_03.html http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/502.html
見解	SQL インジェクションにより、システム情報など重要情報の不正取得が行われる可能性があるため、早急に対策を実施してください。対策を実施する際は、今回指摘したもの



5. 作業スケジュール

5. 作業スケジュール



1 事前調査・調整（～1週間）……………診断対象についての事前調査・スケジュール調整

2 診断実施……………当社診断員によるセキュリティ診断実施

・ネットワーク型診断（Standard プラン）……………～5 IP/日

・Webアプリケーション診断（Professional プラン）……………～5遷移/日（規模によって増減）

3 報告書作成（～2週間）……………作成でき次第提出

4 報告会・問合わせ対応……………お客さま指定場所にて実施

詳細については別途ご相談いたします

6. ご提供サービスの種別

サービス体系

スポット診断	スポット的にお客さまのネットワーク、Webアプリケーションを診断いたします。 本番稼動前の開発環境や、現状のネットワークセキュリティ状況を把握したい場合にご利用いただけます。 また、 ぜい弱性修正後の再診断（オプション） も可能です。
年間継続診断	最初の診断から半年以内または3ヶ月程度毎に 同一内容で再度診断をいたします（年2回、年4回）。 定期的な診断により、セキュリティレベルが向上したかを把握可能です。 また、ネットワーク、Webコンテンツの定期改修に合わせた差分のみの診断、 ぜい弱性修正後の再診断（オプション） も可能です。

セキュリティ診断価格

セキュリティ診断 参考価格	個別見積となるため、詳細条件をお客さまとご相談の上、提示いたします。
------------------	------------------------------------



ご参考

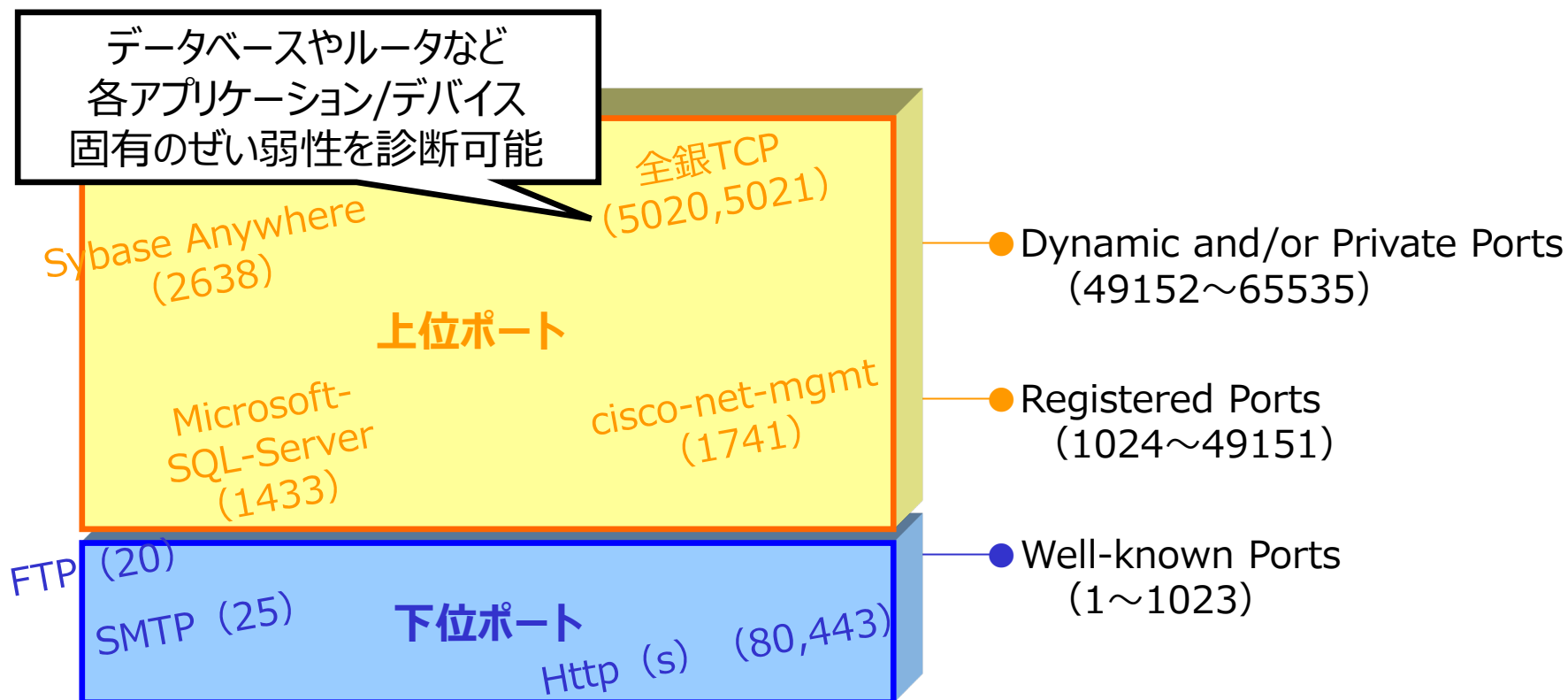
診断対象の各種ネットワーク機器／OS／ミドルウェアに対して、世の中に公開されたぜい弱性が存在するかどうかをネットワーク経由で診断するぜい弱性スキャナです。

本製品には、以下のような特長があります。

- **誤検知/検知漏れが少ない業界トップレベルの精度を実現**
 - 業界最大のぜい弱性データベース（40,000種以上のぜい弱性DB、約70万種のシグネチャ）を所持
 - 各種業界セキュリティ基準に対応した「スキャンテンプレート」により、お客さまの基準を満たすために必要な項目のみ検査可能
- **一般的なIT機器へのぜい弱性テンプレートに加え、PCI-DSSを始めとした監査用テンプレートを22種類以上所持**
- **擬似的にサービス不能攻撃を行う検査も選択可能**
- **米国連邦政府においては、民間局、請負業者から情報部や国防省まで、広範囲に渡る省庁に採用**
- **ワールドクラスのパートナーとの提携**
(Microsoft社、CISCO社、Palo Alto Networks社、 REDSEAL社、VMWare社 など)

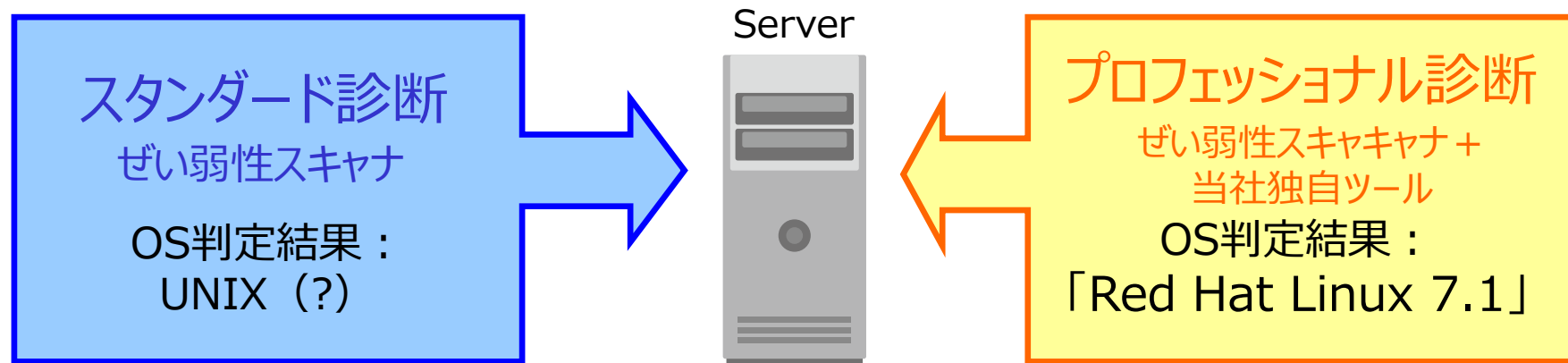
上位ポートの確認

スタンダード診断、プロフェッショナル診断では、ぜい弱性スキャナやポートスキャンツールを使用し、上位ポート（1024～65535番ポート）について、擬似攻撃による診断をおこないます。



診断対象の詳細情報取得

プロフェッショナル診断では、ぜい弱性スキャナに加え、当社独自ツールの使用やキーオペレーションにより、TCPパケットの実装の違い、応答メッセージの違いなどから、診断対象となるサーバー／デバイスのOSやアプリケーション種別、バージョンなどを判定します。



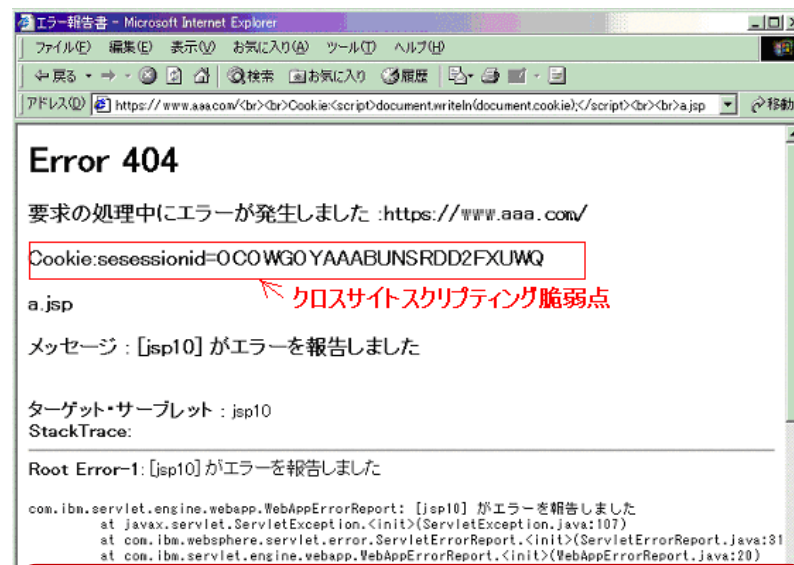
OSやアプリケーションのバージョンなど、詳細情報の判明により…
サーバー固有のぜい弱性について、診断後に的を絞った対策/設定が可能

クロスサイトスクリプティングの診断

Webアプリケーションのぜい弱性により、
攻撃者が悪意のあるスクリプトを実行できるかどうかを診断します。

クロスサイトスクリプティング

- URLへのスクリプト挿入
 - 入力エリアへのスクリプト挿入
 - POST情報（隠しエリア）へのスクリプト挿入
- …etc



ぜい弱性発見！
他人になりすますことが
可能です。

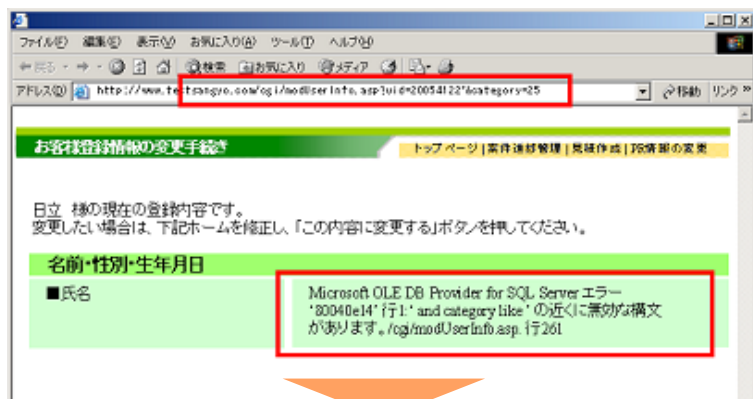
参考) クロスサイトスクリプティングに関する情報

<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/601.html>

SQLインジェクション診断

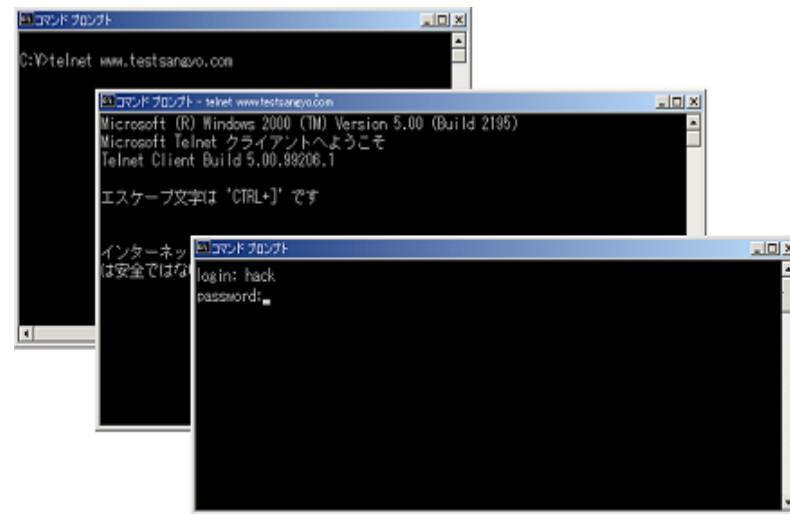
Webアプリケーションのぜい弱性により、攻撃者が任意のSQL文を実行して、重要情報を取得したり、SQL文から任意のOSコマンドを実行できるかどうかを診断します。

● SQLインジェクション成功



● SQL EXECコマンドによる任意ユーザ作成

● telnetサービス起動/ログイン



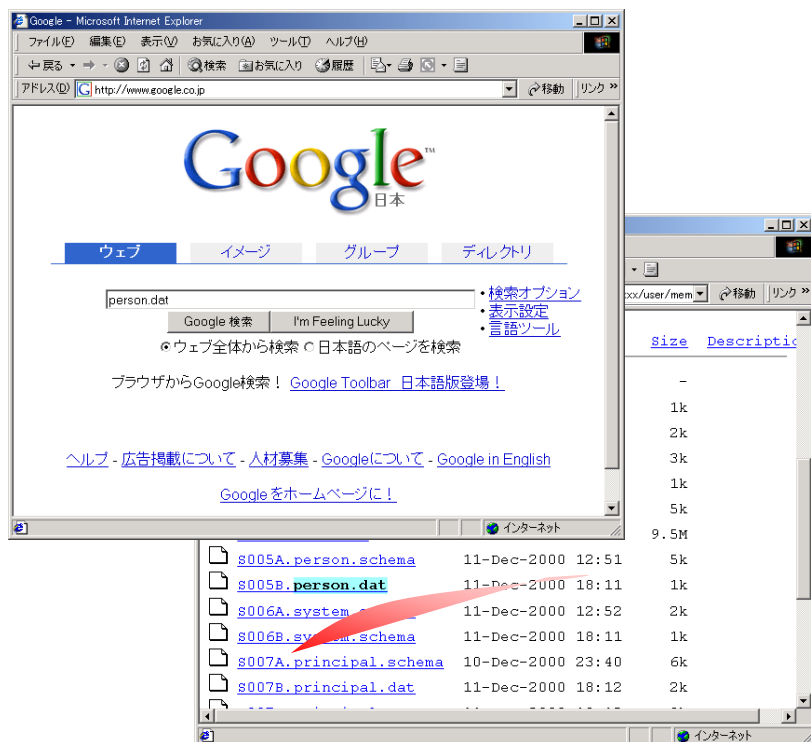
ぜい弱性発見！

重要情報の取得や
任意のコマンド実行が可能

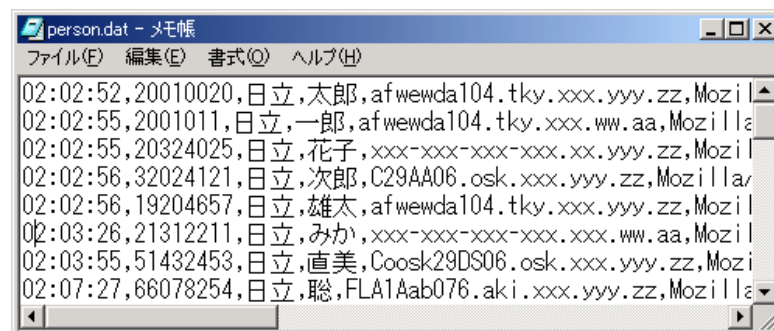
プロファイリング（類推）による顧客情報取得の試み

顧客情報が公開Web上にファイルとして存在する場合は、顧客情報の漏洩につながります。よく使用される管理ファイル名を類推し、顧客情報を取得する試みを行います。

● 顧客ファイル名類推、検索



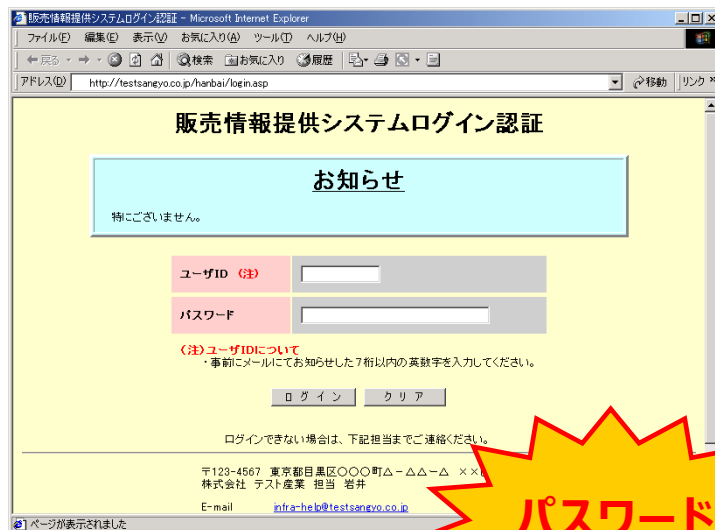
● 顧客ファイルダウンロード



Webアプリケーションのぜい弱性を利用した「なりすまし」の試み

ブルートフォース攻撃によるログインパスワードを突破し、個人になりすますことができるかを診断します。
また、URL情報やWebページ上の隠し項目に表示される内容を変更することにより、さらに別ユーザの個人になりすますことができるかを診断します。

● パスワード類推 ブルートフォース攻撃



**パスワード
突破！**

Admin
0123
test
ichiro
...



https://.../Top.cgi?user=01286002

https://.../ Top.cgi?user=01286003

日立 花子 さん おはようございます。

あなたへの依頼メール（未読）は、現在5件です。→[メールを読む](#)

案件番号	案件名	期限	ステータス
201010	〇〇電機 Webサーバ構築	04/30	見積依頼中

なりすまし

株式会社 日立ソリューションズ・クリエイト



Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

ご相談、ご依頼いただいた内容は、回答等のため、当社親会社（株式会社日立ソリューションズ）、親会社の関連会社及び株式会社日立製作所に提供（共同利用も含む）することがあります。取り扱いには十分注意し、お客様の許可なく他の目的に使用することはありません。

■他社商品名、商標などの引用に関する表示

- Linuxは、Linus Torvalds氏の日本およびその他の国における登録商標または商標です。
- Microsoft、Windowsは、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。
- Red Hatは、米国およびその他の国でRed Hat, Inc. の登録商標もしくは商標です。
- UNIXは、The Open Groupの米国ならびに他の国における登録商標です。
- nexposeは米国Rapid7の米国およびその他の国における登録商標です。
- その他記載の会社名、製品名等は、それぞれの会社の商標または登録商標です

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2023年7月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。