Hitachi Solutions Create

HITACHI

セキュリティ診断サービスのご紹介

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

目次

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
～ 情報資産を守るための「セキュリティ診断」～

HITACHI

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	2023年(組織)	2024年(組織)	2025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	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃
3位	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等の被害	システムのぜい弱性を突いた攻撃
4位	内部不正による情報漏えい	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等
5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	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	機密情報等を狙った標的型攻撃
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組みを狙った攻撃
7位	ビジネスメール詐欺による金銭被害	ぜい弱性対策情報の公開に伴う悪用増加	地政学的リスクに起因するサイバー攻撃
8位	ぜい弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）
9位	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺
10位	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等

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

HITACHI

セキュリティ対策は十分か？

ネットワーク　サーバー　アプリケーション

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、対策は十分なのか・・・

- 対策にはどうしても「もれ」がある
- 新しいぜい弱性は大丈夫か
- 対策の費用が大きすぎ、優先度が分からない

お役に立てるのは・・・

情報資産の「**健康診断**」＝セキュリティ対策の「**現状把握**」

HITACHI

健康診断なら「セキュリティ診断」

「健康診断」にはどんな方法があるでしょうか。

- ネットワーク機器の構成や設定は大丈夫か？
- サーバー・DBなどの設定に問題はないか？パッチは最新か？
- 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。

HITACHI

「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、ぜい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れる

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

HITACHI

日立ソリューションズ・クリエイトの「セキュリティ診断」

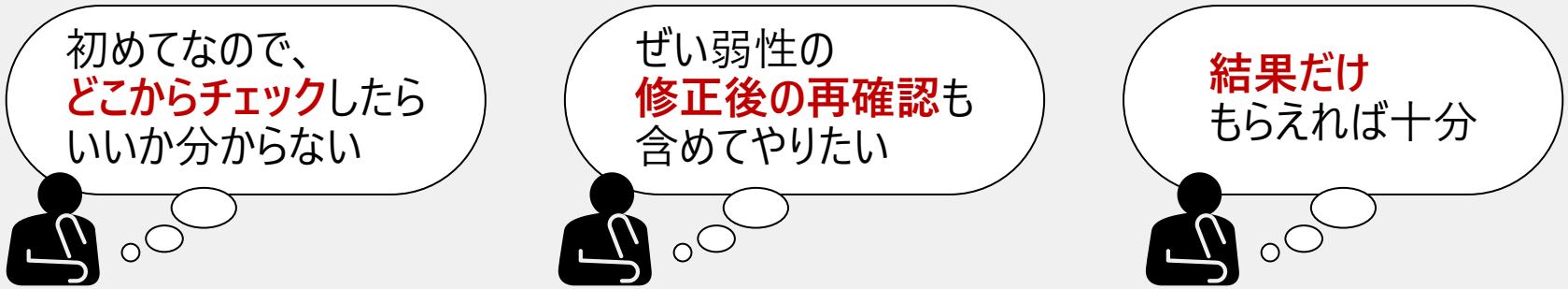
ツール＋「手動診断」

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

分かりやすい「Webアプリケーション診断結果報告書」

分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



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います。

３. セキュリティ診断サービスの概要

3 - 1 セキュリティ診断サービスの概要

HITACHI

ネットワーク型診断サービス

スタンダード プラン　プロフェッショナル 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

スタンダード プラン　プロフェッショナル 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します。

個別アプリケーション診断（ファジング診断）サービス

組み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します。
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します。

ペネトレーションテスト

お客さまのシステムを構成するサーバーやネットワークデバイスなどに対し、
攻撃者が用いる方法や技術を模倣した侵入テスト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）で実施し、セキュリティ強度を診断します。

HITACHI

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

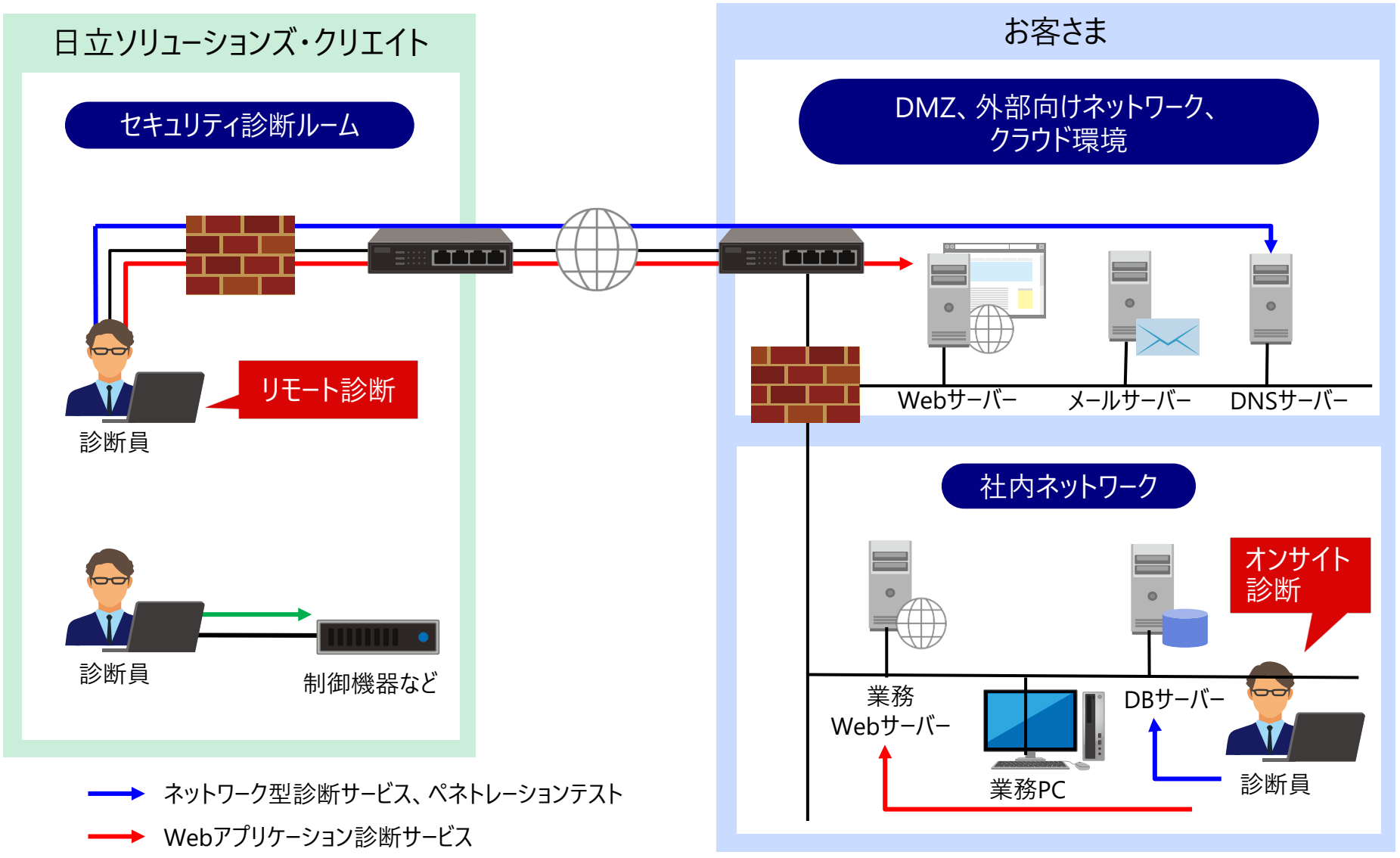
お客さまの内部ネットワークから、重要なサーバーに対して診断します。
外部クラッカーにファイアウォールを破られた場合や内部クラッカーが
存在した場合に、どのようなセキュリティリスクがあるかを予測できます。
イントラネットや、外部公開前のサーバーに対しても有効です。

**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

HITACHI



HITACHI

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。

スタンダード 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
  ※ご希望により使用不能（DoS）攻撃診断も可能
- 報告書の作成・送付

プロフェッショナル プラン

スタンダードの内容に加えて、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）

HITACHI

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		スタンダード プラン	プロフェッショナル 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	

HITACHI

Webアプリケーション検査ツールを使用し、疑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。

スタンダード プラン

- Webアプリケーション検査ツールによる疑似攻撃診断
- 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。

プロフェッショナル プラン

スタンダードの内容に加えて、以下の内容を提供します。

- 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ぜい弱性を再現手順を含めて報告書に記載

HITACHI

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		スタンダード プラン	プロフェッショナル 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	●	○
	ディレクトリリスティング	●	○
	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

4 - 1 診断結果報告書例（1）

HITACHI

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：危険度小の脆弱性のみを検出
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、管理者権限を奪わ
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
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
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せんが、できる
く改善する必要があります。

危険度小の脆弱性は、インフォメー
能性があるものです。すぐに改善する
から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。

総合評価
（5段階評価）

4　診断結果詳細

各サーバの詳細な診断結
【ネットワーク型診断】
(1)攻撃準備探査
攻撃者が実際にサー
て脆弱性をチェックする
えるため、事前にそのサ

(a)サーバ存在確認
攻撃対象のネットワ
要求(ping)が一般的に

(b)TCP サービスポートの
攻撃対象のサーバ
開不要なサービスが
張診断では、全ポート

(c)UDP サービスポートの
攻撃対象のサーバ
開不要なサービスが
張診断では、全ポート

(ご参考)UDP ポートス
UDP はコネクション
正確にスキャンできな
を送信し、サーバから
下位層の ICMP で「IC
じていることが分かり
のか、閉じているが F
したがって、弊社で
合は、ファイアウォー

(d)OS 情報の確認
OS が持つ
情報は大き
を用いて、OS

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。

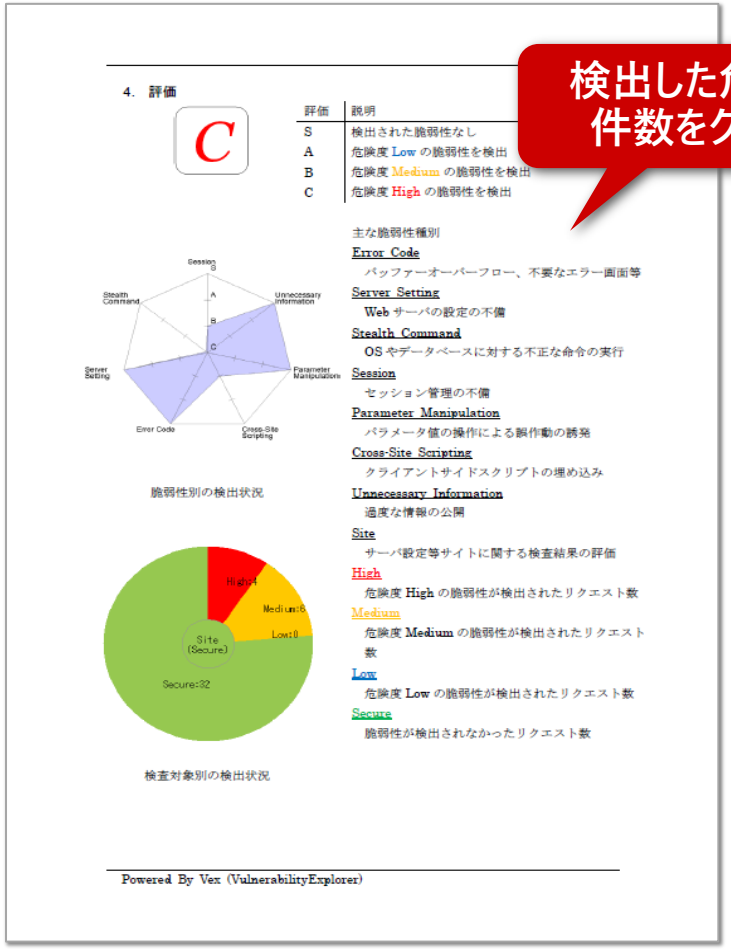
項番	1
脆弱性名	SSL/TLS プロトコルで使用される DES および Triple DES 暗号における平文のデータを取得される脆弱性
重要度	中
概要	SSL/TLS で使用される DES および Triple DES 暗号は、ブロック長が短いため、ネットワークの中継点に存在している攻撃者に暗号化通信の内容を解読される可能性があります。
修正方法	●DES および Triple DES 暗号化アルゴリズムを使用しないようにしてください。また、AES 暗号を無効化しないようにしてください。 ・<OpenSSL の場合> OpenSSL 1.1.0 以上にアップデートして下さい。 デフォルトで 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） ---------- SSLCipherSuite ALL:!SSLv2:!LOW:!EXP:!ADH:!RC4:!DES:!3DES ---------- ・<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。
参照先	●OpenSSL Blog - The SWEET32 Issue, CVE-2016-2183 https://www.openssl.org/blog/blog/2016/08/24/sweet32/ 2016-004511.html me=CVE-2016-2183 ●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
見解	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。

ぜい弱性についての詳細と
対策方法を分かりやすく解説

HITACHI

Webアプリケーション診断サービス（スタンダード 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



4. 評価

C

評価	説明
S	検出された脆弱性なし
A	危険度 Low の脆弱性を検出
B	危険度 Medium の脆弱性を検出
C	危険度 High の脆弱性を検出

脆弱性別の検出状況

検査対象別の検出状況

主な脆弱性種別

Error Code
　パッファーオーバーフロー、不要なエラー画面等

Server Setting
　Web サーバの設定の不備

Stealth Command
　OS やデータベースに対する不正な命令の実行

Session
　セッション管理の不備

Parameter Manipulation
　パラメータ値の操作による誤作動の誘発

Cross-Site Scripting
　クライアントサイドスクリプトの埋め込み

Unnecessary Information
　過度な情報の公開

Site
　サーバ設定等サイトに関する検査結果の評価

High
　危険度 High の脆弱性が検出されたリクエスト数

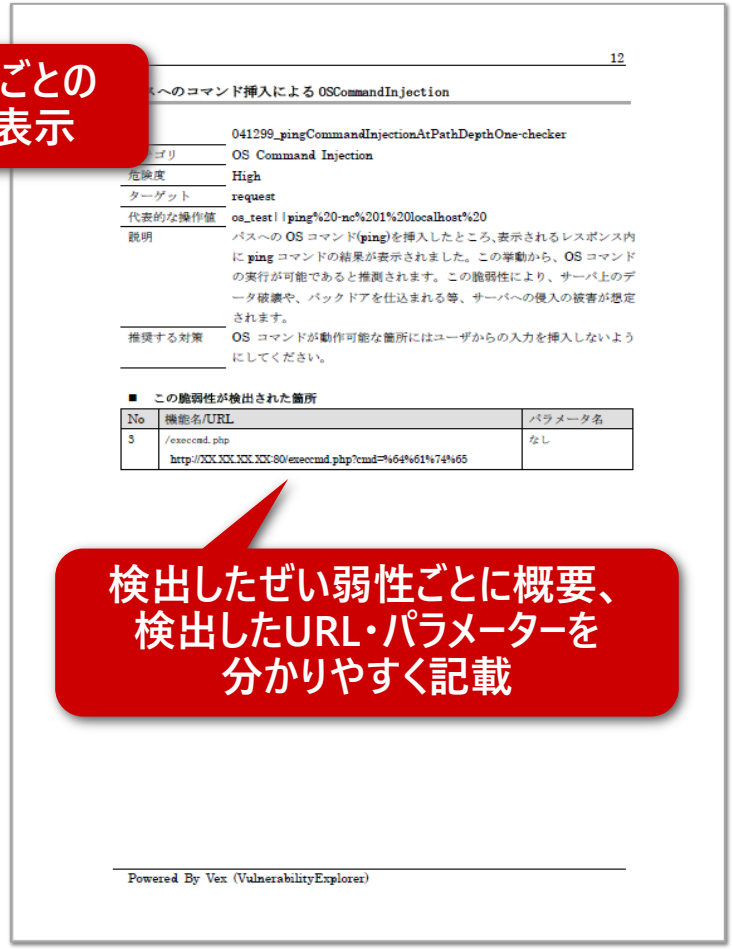
Medium
　危険度 Medium の脆弱性が検出されたリクエスト数

Low
　危険度 Low の脆弱性が検出されたリクエスト数

Secure
　脆弱性が検出されなかったリクエスト数

Powered By Vex (VulnerabilityExplorer)

検出した危険度ごとの件数をグラフで表示



12

へのコマンド挿入による OSCommandInjection

	041299_pingCommandInjectionAtPathDepthOne-checker
ゴリ	OS Command Injection
危険度	High
ターゲット	request
代表的な操作値	os_test!!ping%20-nc%201%20localhost%20
説明	パスへの OS コマンド(ping)を挿入したところ、表示されるレスポンス内に ping コマンドの結果が表示されました。この挙動から、OS コマンドの実行が可能であると推測されます。この脆弱性により、サーバ上のデータ破壊や、バックドアを仕込まれる等、サーバへの侵入の被害が想定されます。
推奨する対策	OS コマンドが動作可能な箇所にはユーザからの入力を挿入しないようにしてください。

■ この脆弱性が検出された箇所

No	機能名/URL	パラメータ名
3	/execcmd. php http://XX.XX.XX.XX:80/execcmd.php?cmd=%64%61%74%65	なし

Powered By Vex (VulnerabilityExplorer)

検出したぜい弱性ごとに概要、検出したURL・パラメーターを分かりやすく記載

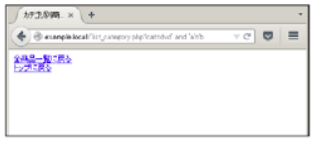
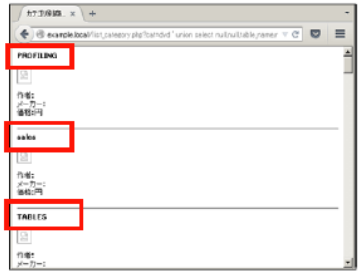
HITACHI

Webアプリケーション診断サービス（プロフェッショナル 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	パラメータ
	http://example.local/list_category.php	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=dvd」にアクセスしたと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	

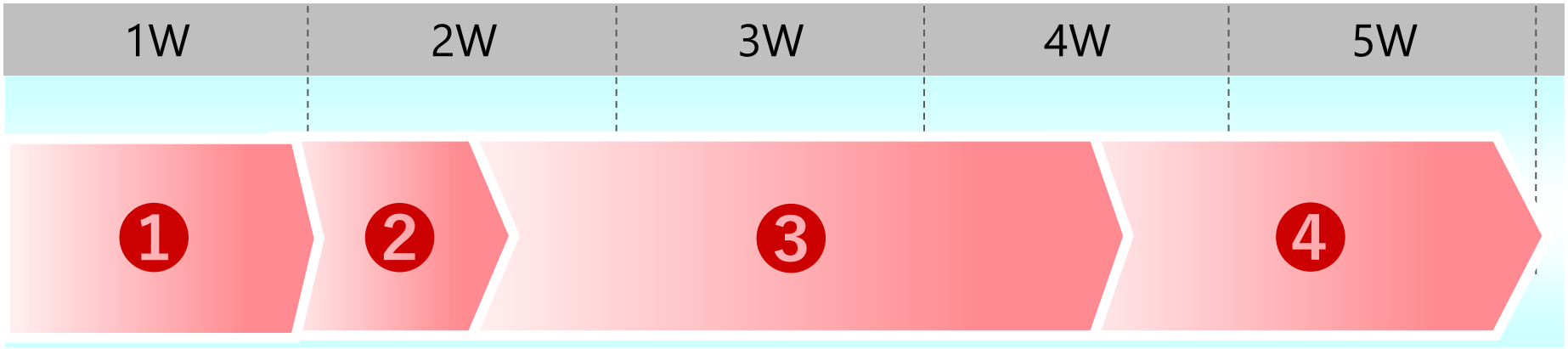
実際の攻撃手順を
分かりやすく解説

	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

HITACHI



❶ **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

❷ **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（スタンダード プラン ）・・・・・・・・・・・・・・・・・～5 IP/日
・Webアプリケーション診断（プロフェッショナル プラン）・・・・・・・・・～5遷移/日（規模によって増減）

❸ **報告書作成**（～2週間）・・・・・・・・・・・・・・・作成でき次第提出

❹ **報告会・問い合わせ対応**・・・・・・・・・・・・・・・・・・・お客さま指定場所にて実施

詳細については、別途ご相談ください

6. ご提供サービスの種別

HITACHI

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します。 本番稼働前の開発環境や、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カ月程度ごとに 同一内容で再度診断をします（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、提示します。

ご参考

ご参考 - ぜい弱性スキャナ Rapid7社 Nexpose

HITACHI

**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。**

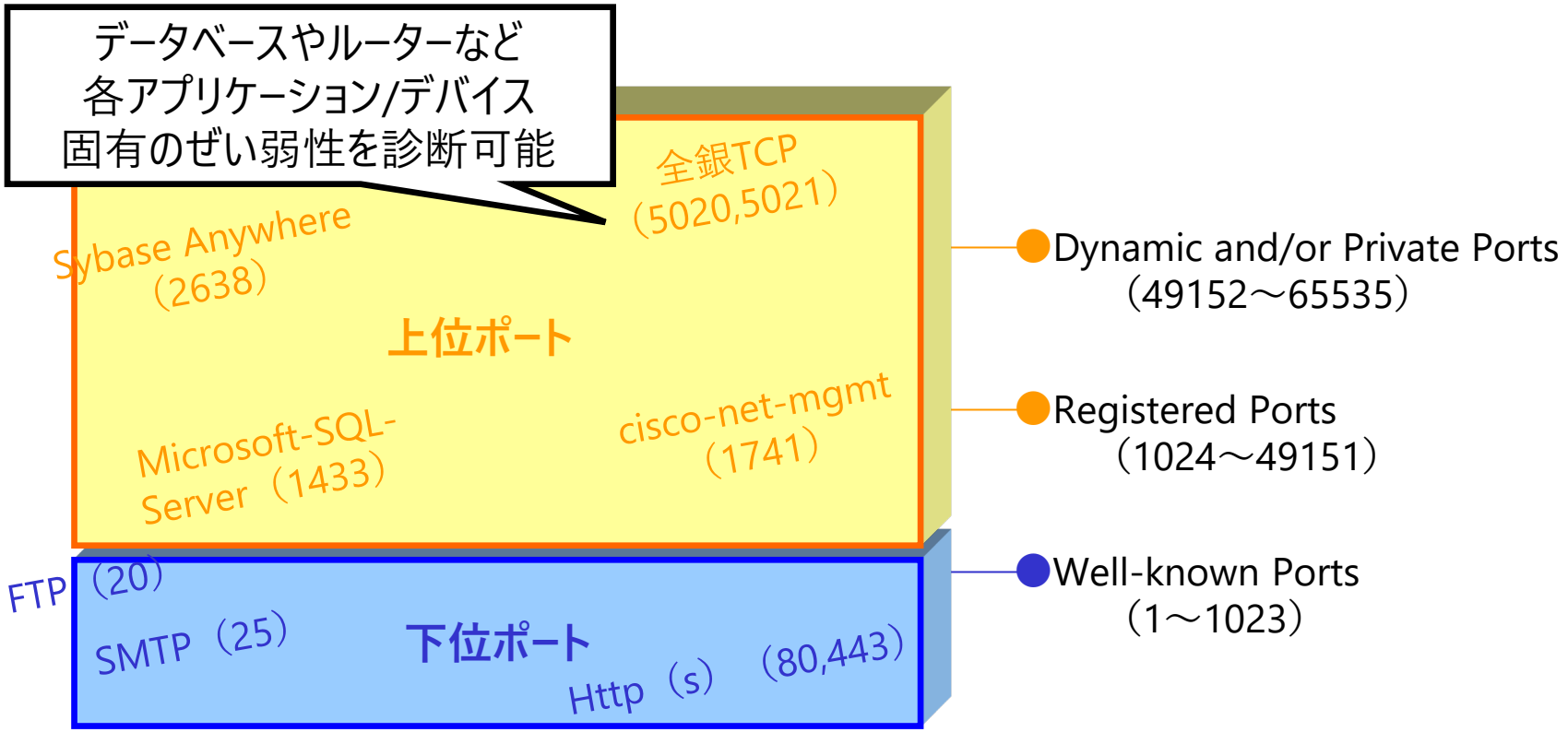
本製品には、以下のような特長があります。

- **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をはじめとした
監査用テンプレートを22種類以上所持**
- **疑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、
広範囲にわたる省庁に採用**
- **ワールドクラスのパートナーとの提携**
  （ Microsoft Corporation 、CiscoSystems 、Palo Alto Networks、REDSEAL、VMWare など）

HITACHI

上位ポートの確認

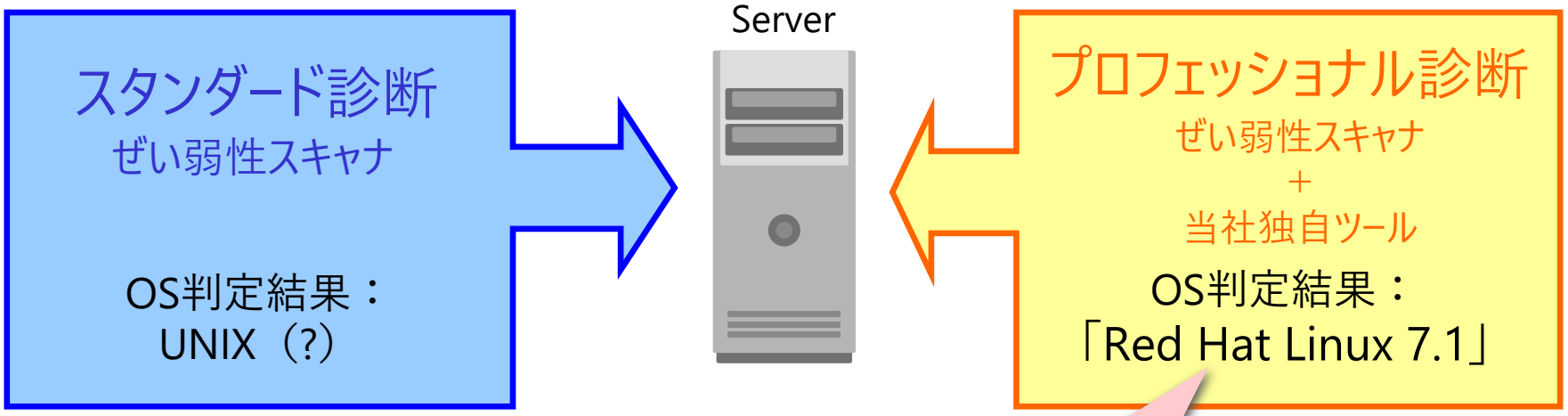
スタンダード診断、プロフェッショナル診断では、ぜい弱性スキャナやポートスキャンツールを使用し、上位ポート（1024～65535番ポート）について、疑似攻撃による診断を行います。



HITACHI

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

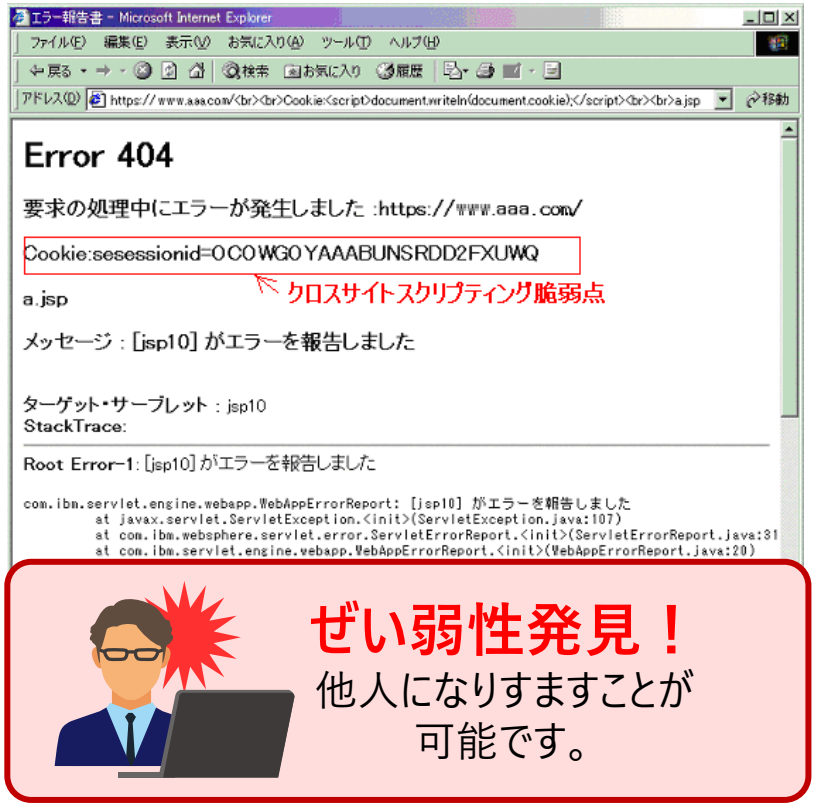
HITACHI

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



参考）クロスサイトスクリプティングに関する情報

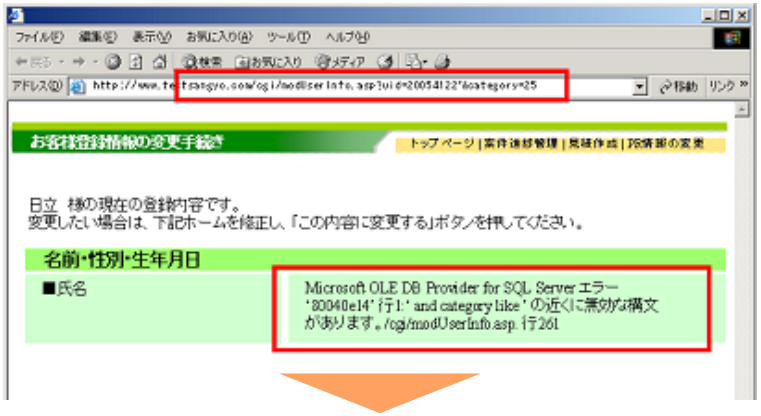
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/601.html

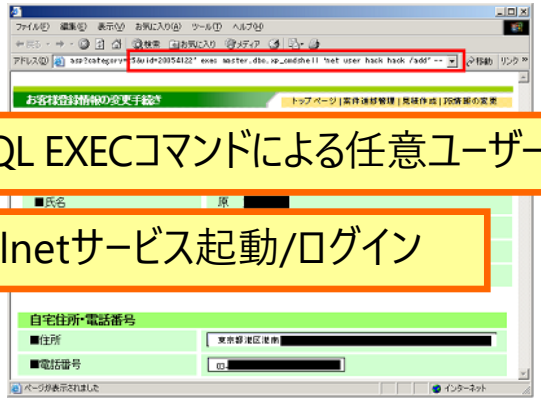
HITACHI

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、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。

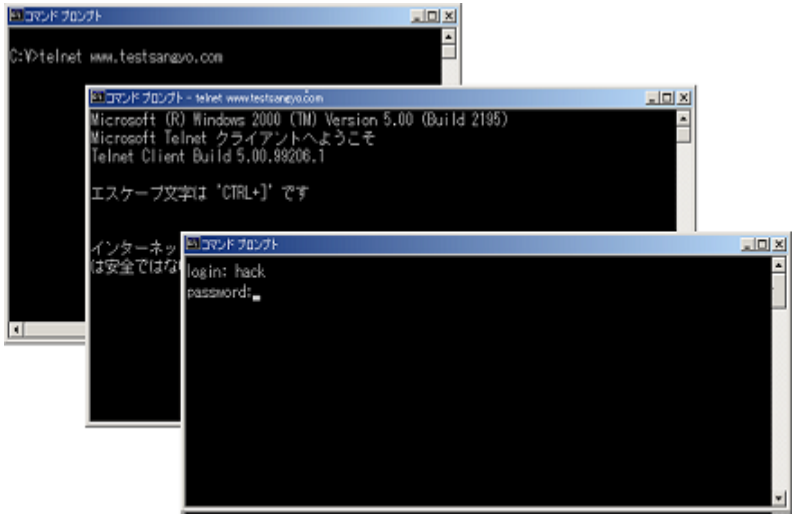
● SQLインジェクション成功





● SQL EXECコマンドによる任意ユーザー作成

● telnetサービス起動/ログイン



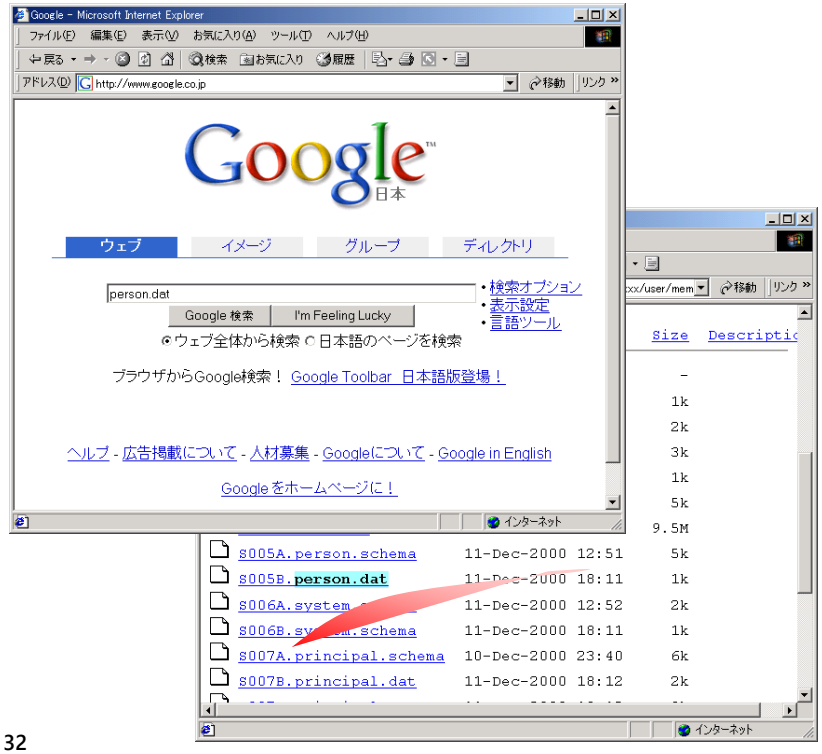
ぜい弱性発見！
重要情報の取得や
任意のコマンド実行が可能

HITACHI

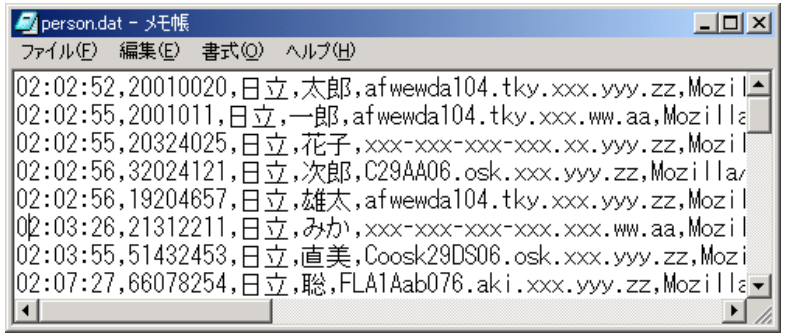
プロファイリング（類推）による顧客情報取得の試み

顧客情報が公開Web上にファイルとして存在する場合は、顧客情報の漏えいにつながります。
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



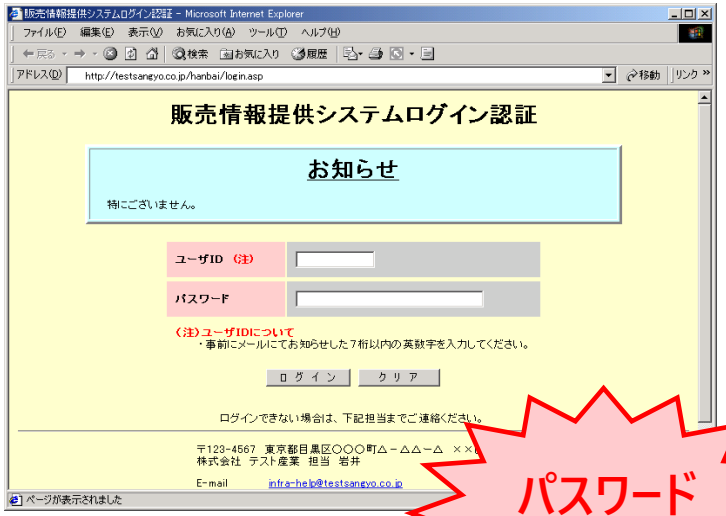
個人情報搾取！

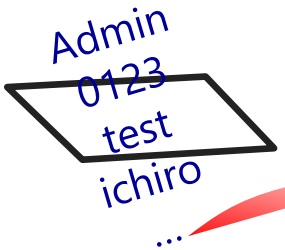
HITACHI

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、個人になりすませるか診断します。
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、
さらに別ユーザーの個人になりすませるか診断します。

● パスワード類推　ブルートフォース攻撃





パスワード
突破！

なりすまし

HITACHI

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。

表示に関する注意事項

HITACHI

■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、2025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。

HITACHI