平成＊＊年＊月＊＊日

企業名
担当者名

公益財団法人 日本電信電話ユーザ協会
〒100-0011
東京都千代田区内幸町1-1-2
URL: http://www.jtua.or.jp

ホームページ・セキュリティ診断レポート

診断対象URL	http://www.exsample.com
診断実施日	平成〇〇年〇月〇〇日

実施項目	目的	対象とした脅威	結果
改ざんの検出	ホームページが不正に書き換えられていないか	外部ホームページへの不正リンク	**危険**
脆弱性の診断	ホームページに欠陥がないか	クロスサイトスクリプティング	**問題あり**
		SQLインジェクション	**安全**
		ディレクトリインデックス	**安全**

・「改ざんの検出」において、不正な書き換えが行われていることがわかり、かつ「脆弱性の診断」においても問題が見つかりました。具体的に不正な書き換えが行われているURLや問題が検出されたパラメータは別紙1でご確認ください。また、診断実施項目の説明と一般的な対策は別紙2のとおりです。

・対策実施後は、再度HPセキュリティ診断を受けて（*注）安全確保を確認し、その後も定期的に診断を受けるなど、ホームページを安全に運用するための手立てを継続していくことをおすすめします。

（＊注）「改ざんの検出」については、本診断レポートの他、診断実施日から1ケ月間の検出結果をまとめたレポートを別送しますので、その間に改ざんへの対処策を完了させれば、今回お申込みいただいたサービスメニュー内で、改善の結果を確認できます。

・本診断の診断範囲は以下のとおりであり、これらを超えたものについての結果を保証するものではありません。
1. 改ざんの検出・・・ホームページの上位階層ページから最大100ページを診断
2. 脆弱性の診断・・・(1)「クロスサイトスクリプティング」「SQLインジェクション」は、ホームページに記述されているパラメータ（入力項目）の上位階層から最大100パラメータを診断
(2)「ディレクトリインデックス」は、診断範囲内全URLを診断
・診断実施項目はすべて、診断実施日当日の実施結果です。
なお、今後改ざん検出は翌月の同一日の前日まで毎日実施し、その間に改ざん（脅威の発生）が検出された場合は、メールにてお知らせします。
さらに、診断開始日から約1ヶ月間の改ざん検出診断結果を日別に履歴としてまとめた報告書を送付します。

（別紙1）

改ざん検出結果

実施日：平成〇年〇月〇日
診断対象URL：http://www.exsample.com

以下のページをチェックし、改ざんが見つかりました。
ホームページ管理者、ホームページ制作者に連絡し、適切な対策を講じてください。
改ざん検出の結果が「検出」となっているページにはアクセスしないよう、ご注意ください。

No	URL	改ざん検出
1	https://www.example.com/sample01/	検出なし
2	https://www.example.com/sample01/back/	検出なし
3	https://www.example.com/sample01/search.php	検出なし
4	https://www.example.com/sample01/temp/	検出
5	https://www.example.com/sample01/temp/add.php	検出

脆弱性診断結果

実施日：平成〇年〇月〇日
診断対象URL：http://www.exsample.com

以下のURL内にあるパラメーターをチェックし、問題が検出されました。
ホームページ管理者、ホームページ制作者に連絡し、適切な対策を講じてください。

No	URL パラメーター	クロスサイト スクリプティング	SQL インジェクション
1	https://www.example.com/sample01/add.php		
	name	検出	検出なし
	mail	検出	検出なし
2	https://www.example.com/sample01/conf.php		
	id	検出なし	検出なし
	title	検出	検出なし
	name	検出	検出なし
	body	検出	検出なし
3	https://www.example.com/sample01/search.php		
	keyword	検出なし	検出なし
	type	検出なし	検出なし
	mode	検出なし	検出なし

診断実施項目の解説（改ざんの検出）

1. 改ざん

＜概要＞

ホームページの改ざんとは、攻撃者やコンピュータウイルス等により、ホームページの内容が不正に書き換えられてしまうことです。最近の傾向として、攻撃者がホームページを改ざんして、そのホームページを閲覧した利用者のコンピュータに、ウイルスを感染させる事件が増加しています。

＜影響＞

攻撃者が、会社のホームページの見た目を変えることなく、不正なリンクを埋め込み（下図①）、内容が書き換えられているとは知らずに会社のホームページにアクセスした利用者（下図②）を、悪意のある外部のホームページに誘導します（下図③）。利用者は、悪意のある外部のホームページにアクセスすることで、例えばパソコンが動かなくなる等のウイルス感染の被害にあう恐れがあります（下図④）。

また、ウイルス感染の被害にあった利用者のコンピュータから、個人情報が漏えいする恐れがあります。

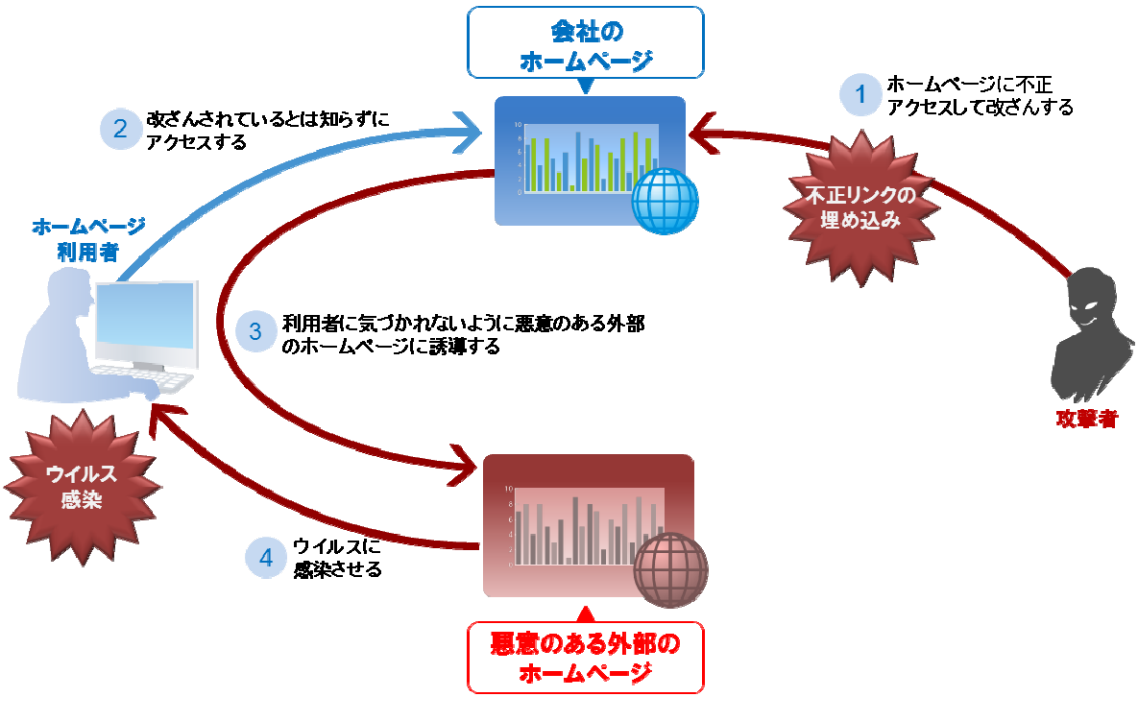
さらに、改ざんによって会社のホームページが正常に機能しなくなったり、ホームページ内の機密情報が攻撃者に漏洩する恐れもあります。

＜改ざんが見つかった場合の対策＞

一般的には「バックアップデータを使用して正常な状態に戻す」「ソフトウェアやサーバOSのセキュリティ更新や設定の見直しを行う」などの対策が知られていますが、具体的にはホームページ管理者、ホームページ制作者に連絡して状況を確認し、まずはインターネットからホームページを一時的に切り離して対応を図るなどの安全確保が求められます。

その際、本レポートで改ざんが検出されたURLにアクセスしないよう、ご注意ください。

ホームページの改ざんによる攻撃の一例



2. クロスサイトスクリプティング

＜概要＞

ホームページを閲覧している利用者のブラウザ（Internet Explorerなど）に、悪意のあるスクリプト（簡易プログラム）を送り込み、実行させてしまう脆弱性です。

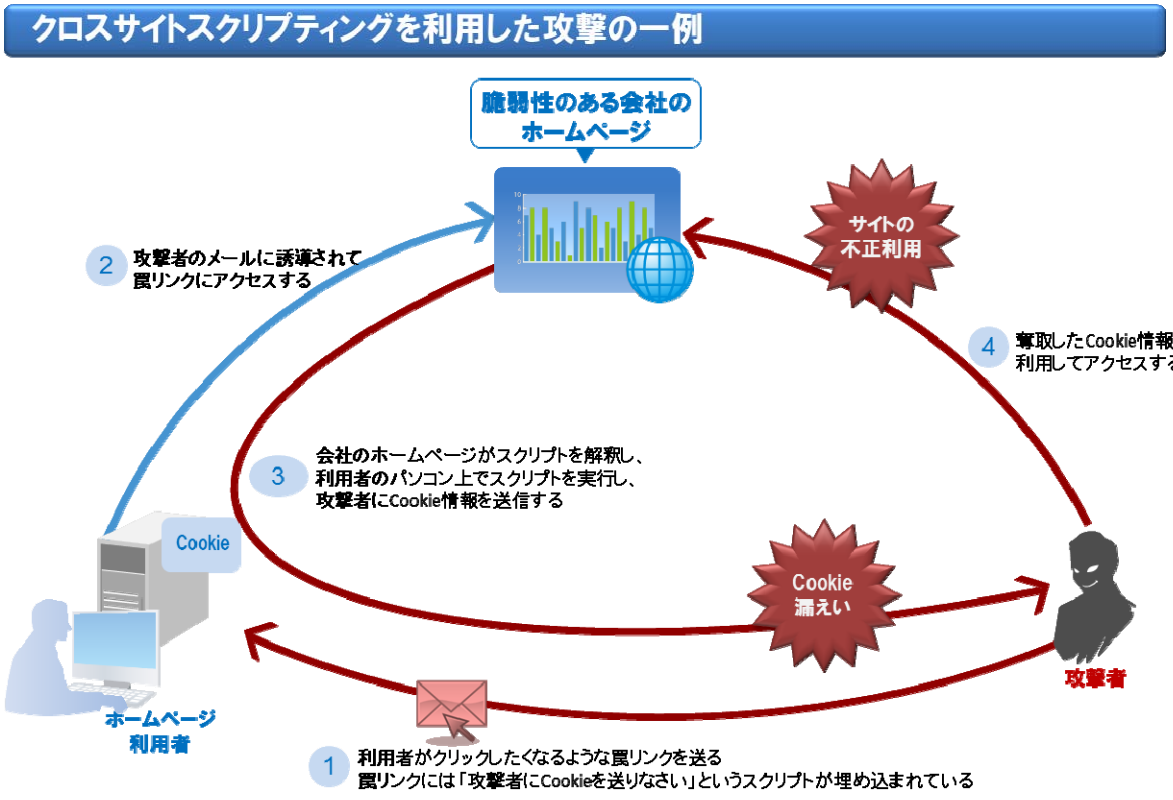
＜脆弱性を利用した攻撃の影響＞

攻撃者が、不正なスクリプトが混入できる、脆弱性のある会社のホームページへの罠リンク（悪質な偽装リンク）を作成して、利用者にメールで送信（または掲示板へ投稿）します。この罠リンクには、例えば「攻撃者にCookie（利用者を識別している情報）を送りなさい」というスクリプトが埋め込まれています（下図①）。利用者がメール（または掲示板）に記載されたURLをクリックすると（下図②）、脆弱性のある会社のホームページがこのスクリプトを解釈し、利用者のブラウザに罠リンクのページが表示された瞬間に、利用者のパソコン上でスクリプトが実行され、利用者の気づかぬうちに、パソコンにあるCookie情報が、攻撃者に送信されます（下図③）。Cookie情報を奪った攻撃者は、それを用いて正当な利用者になりすまし、脆弱性のある会社のホームページを不正に利用する恐れがあります（下図④）。

また、偽ホームページが表示されてしまうことで、利用者がフィッシング等の被害にあう恐れもあります。

＜クロスサイトスクリプティングが見つかった場合の対策＞

ホームページ管理者、ホームページ制作者に連絡して状況を確認し、対応を図ってください。



3. SQLインジェクション

＜概要＞

ホームページと連動しているデータベースにおいて、攻撃者が作成した悪意のあるSQL文（データベースを操作する言語による命令）により、データベースが操作されてしまう脆弱性です。この脆弱性が存在するホームページでは、データベース内の情報流出や改ざんが行われてしまう恐れがあります。

＜脆弱性を利用した攻撃の影響＞

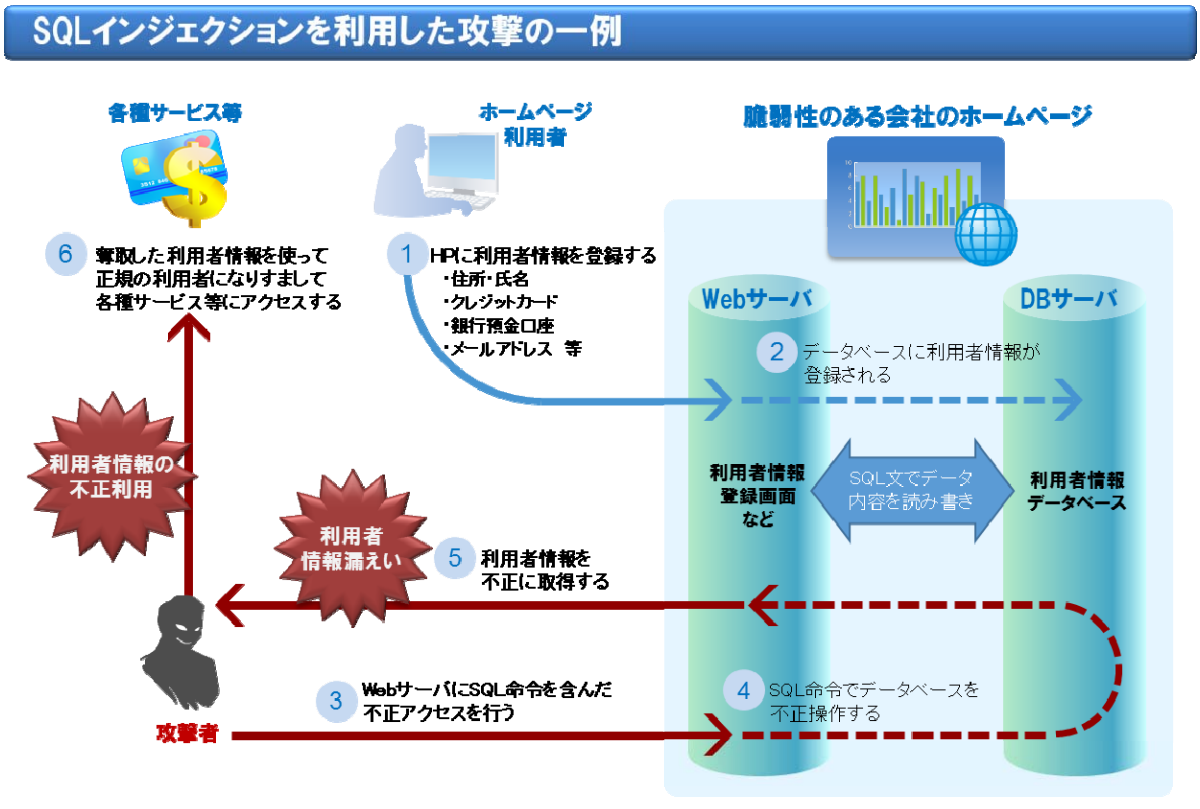
利用者がホームページに登録した情報（下図①）は、連動するデータベース内に格納されます（下図②）。攻撃者が、WebサーバにSQL文を含んだ不正アクセスを行い（下図③）、SQL文を使って不正にデータベースを操作することで（下図④）、データベースに格納された利用者情報を奪取する恐れがあります（下図⑤）。攻撃者は、不正に取得した利用者情報を悪用して利用者になりすまし、利用者に被害を与える可能性があります（下図⑥）。

またデータベース内に格納されている、ホームページ生成に用いるデータが攻撃者に改ざんされ、不正なリンクが埋め込まれることで、不正なリンクを埋め込まれた脆弱性のあるホームページを閲覧した利用者のパソコンがリンク先に誘導され、ウイルスに感染させられる恐れがあります。

さらに、ホームページのシステム構成や設定によっては、攻撃者がデータベースの基本ソフトを不正に操作したり、データベースのログイン認証を回避し、データベースにアクセスする恐れもあります。

＜SQLインジェクションが見つかった場合の対策＞

ホームページ管理者、ホームページ制作者に連絡して状況を確認し、対応を図ってください。



4. ディレクトリインデックス

＜概要＞

ホームページのコンテンツを格納するディレクトリ（フォルダ）配下のファイルが一覧表示されてしまう脆弱性です。この脆弱性が存在すると、表示されたファイル一覧上にあるファイルにアクセスされ、公開を意図していないファイルの閲覧や実行が可能となる恐れがあります。

＜脆弱性を利用した攻撃の影響＞

攻撃者は、Webサーバにあるホームページの各ページが保存されているディレクトリにアクセスし（下図①）、ディレクトリ内のファイル一覧を不正に取得します（下図②）。万が一、機密情報を含むファイルがWebサーバに保存されており、取得したファイル一覧内でその存在が明らかになった場合、攻撃者は、そのファイルにアクセスし（下図③）、Webサーバからそのファイルを盗む可能性があります（下図④）。

また、ファイル閲覧権や実行権が管理されていない実行形式ファイル（.exeファイル等）をサーバ管理者がディレクトリ配下に置いた場合、権限のない者に勝手に操作されてしまう恐れがあります。

＜ディレクトリインデックスが見つかった場合の対策＞

一般的には、インターネット上に公開するファイルを限定するような設定への変更や、サーバ構成の見直しなどの対策が知られていますが、具体的にはホームページ管理者、ホームページ制作者に連絡して状況を確認し、対応を図ってください。

ディレクトリインデックスを利用した攻撃の一例