ColdFusion セキュリティガイド

2014.12

株式会社サムライズ

このガイドの目的について

近年増加傾向にあるWebアプリケーションのセキュリティ問題。ColdFusion開発者もプログラムの作成や古いバージョンからの移行の際にコードの品質を上げる事への検討が必要な時期に差し掛かっています。

このガイドでは、ColdFusion開発者に対して、下記の３つの項目に対してセキュリティの情報を紹介します。

1. 作成するプログラム
2. セキュリティに影響する設定
3. 環境面

（参考ドキュメント：「ロックダウンガイド」）

http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf11/cf11-lockdown-guide.pdf

- ドキュメントの内容について
  - ColdFusion Administrator を介したアタッキングへの最大限の防御
  - 推奨されるColdFusion Administrator 設定
  - そのほか ColdFusion や Web サーバーで検討する設定
- ポイント
  - 最新の ColdFusion セキュリティアップデートを適用するとともに、未来への脅威に備えて /CFIDE/administrator や adminapi componentutils といった、悪用されると脅威になるフォルダに対する外部からのアクセスを遮断する

（参考ドキュメント：「セキュリティ ガイド」）

http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf11/cfml-developer-security-guide.pdf

- ドキュメントの内容について
  - 作成するColdFusionベースのアプリケーションで検討すべきセキュリティ脅威に関する解説
  - その他、ログイン設定や検証などのプログラミングに関するガイド

1.

作成するプログラム

作成するプログラムに潜むセキュリティの穴

- Webアプリケーションのアプリケーション層への攻撃方法のほとんどはColdFusionプログラムにも当てはまります。
  - ウェブサイトのパフォーマンスの低下からデータの漏えい・攻撃用プログラムの設置など、ColdFusionプログラムのセキュリティの欠陥を突いた攻撃に備える必要があります。

① SQLインジェクション

```
1  <cfif IsDefined("Url.media_id")>
2
3      <cfquery datasource="cfartgallery" name="qMedia">
4          select * from MEDIA
5          where MEDIAID=#Url.media_id#
6      </cfquery>
7      <cfdump var="#qMedia#">
8
9  <cfelse>
10     メディアIDが選択されていません<br>
11     <a href="01_sql_injection.cfm?media_id=1">メディアID 1を選択</a><br>
12     <a href="01_sql_injection.cfm?media_id=2">メディアID 2を選択</a><br>
13     <a href="01_sql_injection.cfm?media_id=3">メディアID 3を選択</a>
14 </cfif>
```

脅威

- 想定される脅威
  - 予期しないデータベースクエリが実行されて、データの改ざんや閲覧、消去が行われる
  - エラーを発生させ、画面に表示されるメッセージからデータベース構造やデータを見られる

- 想定シーン
  - データベースの処理のSQLに動的なパラメータ受け取りがある処理
    - 例えばURLパラメーターを使用した一覧⇒詳細画面へのページ遷移で
      a. 想定していない不正なSQL文やパラメーターが渡される
      b. プロシージャーを利用した内部コマンドが渡される

推奨される対策例

- 改善ポイント
  - <cfqueryparam>を使用して、プリペアドステートメントのパラメータ一変数を用いる
    - CF11以降は<cfquery>の代わりにQueryExecute関数を使う事もできる
  - 渡されてくる値が想定されたデータなのかの整合性チェックを行う（IsNumeric, IsValid 他）
  - エラーをそのまま画面に表示させない
  - データベースへ接続するユーザーの権限、ならびに、ColdFusion Administratorのデータソースの設定で制限する（後述）

② クロスサイトスクリプティング

```
1  <cfif IsDefined("Url.media_id")>
2
3      あなたは<cfoutput>#Url.media_id#</cfoutput>を選択しました
4
5  <cfelse>
6      メディアIDが選択されていません<br>
7      <a href="02_xss.cfm?media_id=1">メディアID 1を選択</a><br>
8      <a href="02_xss.cfm?media_id=2">メディアID 2を選択</a><br>
9      <a href="02_xss.cfm?media_id=3">メディアID 3を選択</a>
10 </cfif>
11
```

脅威

- 想定される脅威
  - 偽の情報や入力を表示してユーザーから不正に情報を取得する
  - Cookie情報をスクリプトを使って盗み出す。

- 想定シーン
  - ユーザーから送信されたデータを画面にそのまま表示した
  - ユーザーから送信されたデータをhiddenパラメーターなどにそのまま指定した
  - ログイン失敗などの再入力を促す画面で、直前のユーザーの入力をそのまま入力欄に指定した

推奨される対策例

- 改善ポイント
  - 入力値の表示や入力欄への指定の際に、EncodeForHTML() や HTMLEditFormatでパラメーターをエンコードする
    - EncodeForHTML関数は日本語などもエンコードされる
  - 入力値が限定できる場合は整合性をチェック（IsNumeric, IsValid）
  - <CFCookie>で発行する Cookie には HttpOnly 属性を付け、スクリプトからのアクセスを防御する
    - ColdFusion 9.0.2以降の Session Cookie には HttpOnly がデフォルトで付加されている
  - ColdFusion Administrator の スクリプトの保護の設定を有効にする
- 補足
  - 「ColdFusion Administrator の スクリプトの保護」は、文字（タグ名）一致のみチェックのため、安全対策の一つに過ぎない

③ ＣＳＲＦ（クロスサイト・リクエスト・フォージェリ）

```
<html><head></head><body>
<script type="text/javascript" >
var form = document.createElement('form');
form.action = 'http://127.0.0.1:8500/cfdemo/security/siteA/09_csrf.cfm';
form.method = 'post';
form.style.display = "none";
document.body.appendChild(form);
  var input = document.createElement('input');
  input.setAttribute('type', 'hidden');
  input.setAttribute('name', 'email');
  input.setAttribute('value', 'attackuser@hoge.com');
  form.appendChild(input);
  var input = document.createElement('input');
  input.setAttribute('type', 'hidden');
  input.setAttribute('name', 'password');
  input.setAttribute('value', 'change!!');
  form.appendChild(input);
  var input = document.createElement('input');
  input.setAttribute('type', 'hidden');
```

脅威

- 想定される脅威
  - ログイン済みのサービスに対して、自身の登録情報が不正に書き換えられ、最悪の場合ユーザーIDを乗っ取られる
  - ログイン認証が掛ったサービス（例：ランキング投稿やコメント書き込み）などが勝手に行われる
- 想定シーン
  - ユーザーがサービスにログインしたまま、攻撃者のページを（そのページへのリンクを）踏んでしまう

推奨される対策例

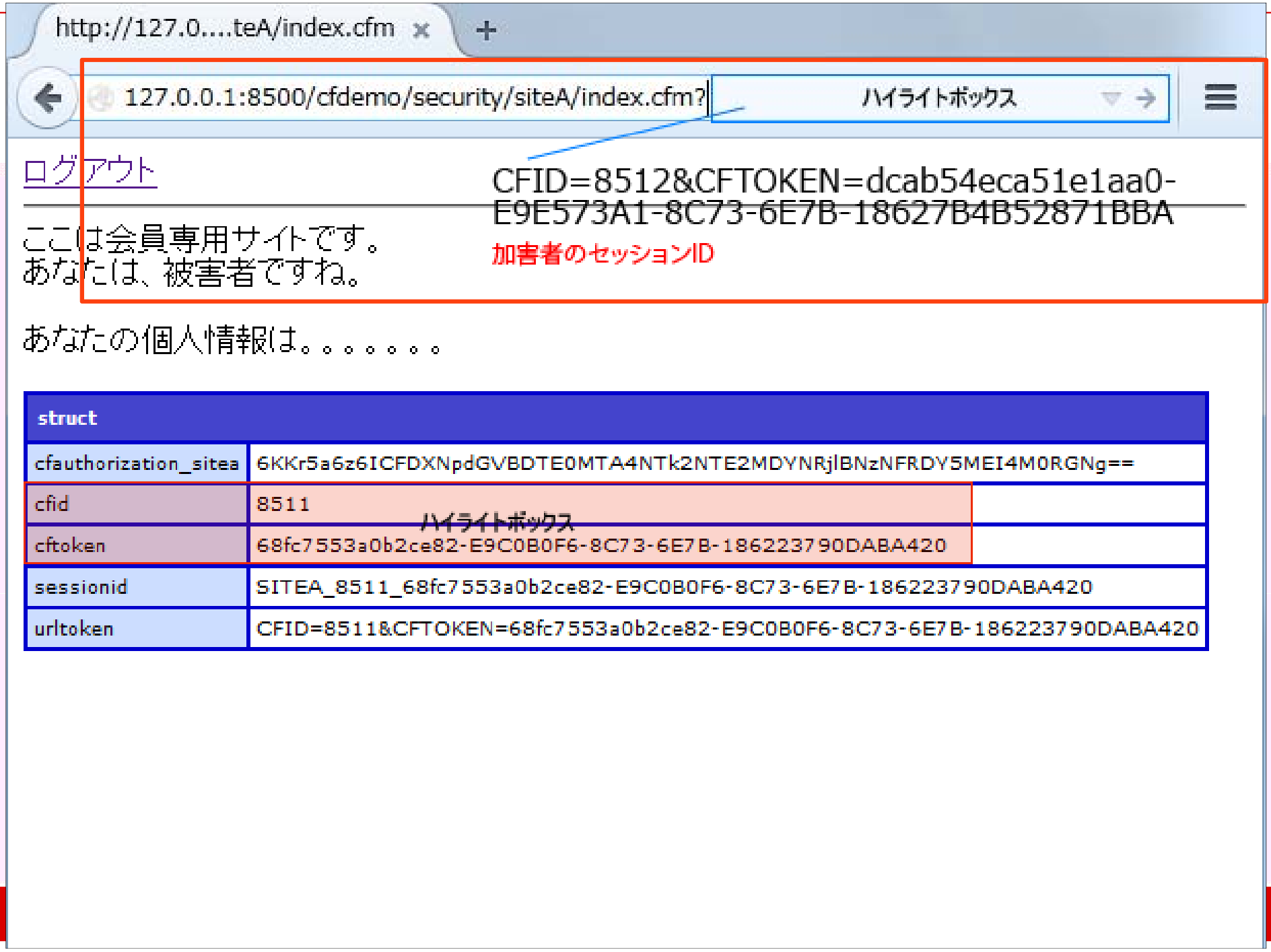
■改善ポイント

- CSRFGenerateToken、CSRFVerifyToken
  - CF9.0.2 以降で実装(9.0.0/9.0.1は最新セキュリティアップデートを適用)
- その他（ユーザーインターフェイスとの兼ね合い）
  - 特定の個人情報の表示や変更時には、二段階認証を実装
  - 変更前の確認画面の挟み込みや現在の情報を入力（現在のパスワードなど）
  - CAPTCHA, Re-CAPTCHA などの画像認証を加える

■補足

- CAPTCHA, Re-CAPTCHAなどの画像認証は、
  文字判別の難解さや、画像解析プログラムも存在する
  - ⇒ Capyパズルキャプチャ
  - ⇒ Capyアバターキャプチャ

④ セッション固定化攻撃 (Session Fixation)


http://127.0....teA/index.cfm
127.0.0.1:8500/cfdemo/security/siteA/index.cfm?
ハイライトボックス
ログアウト
CFID=8512&CFTOKEN=dcab54eca51e1aa0-E9E573A1-8C73-6E7B-18627B4B52871BBA
加害者のセッションID
ここは会員専用サイトです。
あなたは、被害者ですね。
あなたの個人情報は。。。。。。
struct
cfauthorization_sitea
6KKr5a6z6ICFDXNpdGVBDTE0MTA4NTk2NTE2MDYNRjlBNzNFRDY5MEI4M0RGNg==
cfid
8511
ハイライトボックス
cftoken
68fc7553a0b2ce82-E9C0B0F6-8C73-6E7B-186223790DABA420
sessionid
SITEA_8511_68fc7553a0b2ce82-E9C0B0F6-8C73-6E7B-186223790DABA420
urltoken
CFID=8511&CFTOKEN=68fc7553a0b2ce82-E9C0B0F6-8C73-6E7B-186223790DABA420

脅威

- 想定される脅威
  - 攻撃者のセッションIDでサービスにログインしてしまい、攻撃者に自分のサービスを利用されてしまう
    - ColdFusion は、CFIDとCFTOKENの組み合わせ、または、JSESSIONIDのどちらかでセッションを識別する
      - CFIDは連番だが、CFTOKENはランダムな値となる。CFTOKENは、UUIDを指定可能
    - ユーザーからのCookieの送信の他、URLパラメータとして渡された場合も有効である
- 想定シーン
  - ユーザーが攻撃者のセッションIDを含んだ攻撃ページを（そのページへのリンクを）踏んでしまう

推奨される対策例

- 改善ポイント（下記はすべてCF10以降）
  - ログイン処理時に SessionRotate()関数でセッションIDを強制変更
  - ログアウト処理時 SessionInvalid()関数でセッションIDを無効化
  - セッション Cookie の有効期間を変更

- 補足
  - CF10（最新セキュリティアップデートを適用したCF9）以降、サーバーで発行していないセッションIDでリクエストがあった場合は、強制的にセッションIDが書き換えられる。
    - 最新のCF11では、セッションタイムアウト時のセッションIDの取扱いに変更がある

⑤ ファイル アップロード

```
<cfif IsDefined("Form.submit")>

    <cffile action="upload" filefield="photo" destination="#ExpandPath('out/')#"
            nameconflict="overwrite">
    画像をアップロードしました。
    <br>
    <cfoutput>
        <img src="out/#cffile.SERVERFILE#">
    </cfoutput>

<cfelse>

    <cfform enctype="multipart/form-data">
        <cfinput type="file" name="photo">
        <br>
        <cfinput type="submit" name="submit" value="ファイルアップロード">
    </cfform>
</cfif>
```

脅威

- 想定される脅威
  - 想定外の実行プログラム（.cfm等）がアップロードされ、不正なプログラムが実行される
- 想定シーン
  - ファイルのアップロードを受け付けるページ
    - ブログの画像アップロードやメールフォームのファイルの添付など
  - アップロードしたファイルのチェックに不備
    - 例：クライアントから送信されるMIMEタイプのチェックしか行わない

推奨される対策例

- 改善ポイント
  - （CF10以降）<cffile action="upload" ..>は、アップロードしたファイルの先頭数バイトが読み込まれてMIMEタイプが決定される
    - 旧来の拡張子によるチェック等に戻すには、新たに追加された strict 属性を指定（strict="false"） する。その場合は別途ファイルチェックが必要。
    - 新しいチェック処理では、例えばMicrosoft Officeファイルなどのチェックの検知が環境により異なる場合もあるため、許容するファイルの種類に応じて複数の手段で検証する
      - IsImageFile、IsPDFFile、IsSpreadsheetFile、FileGetMimeTypeなど、アップロードしたファイルに対するチェックを行う
  - ファイル拡張子が想定されているものかを検証する
  - アップロードしたファイル名を動的に変更する

⑥ ファイルパス インジェクション

```
<cfparam name="Url.header" default="news.cfm" >
<cfinclude template="in/#Url.header#">
```

脅威

- 想定される脅威
  - Webページとは無関係な OSの設定ファイル・データファイル等がブラウザに表示される
  - 不正な .cfm ページがインクルード・実行され、正常な処理を阻害する
  - 他の攻撃手段と組み合わされ、攻撃者がアタックコードを含む.cfmファイルを実行する

- 想定シーン
  - URLパラメーターにファイル名が含まれている処理
    - パラメーターを使用してCSSファイルを読み込む処理
    - ファイルに対して操作を行う CFタグのパラメータ…CFHTTP, CFDIRECTORY, CFFILE, FileOpen 等ファイル・ディレクトリ操作を行うタグや関数

推奨される対策例

- 改善ポイント
  - 可能な限りパラメータにファイル名を直接指定するような実装を避ける
  - ディレクトリ・トラバーサルにつながる「..」 「../」やその他の予期しない文字を取り除く
  - ファイルを開く際は、対象のディレクトリを限定し、かつファイル名にディレクトリ名が含まれないようにする
  - ファイル名のチェック

⑦ ＨＴＴＰ・ＭＡＩＬヘッダ インジェクション

HTTP・MAILヘッダ インジェクション

- 想定される脅威
  - HTTPやSMTPでヘッダを送信する処理に、改行コードCRLF （0D, 0A）が含まれ、改行の次の情報が不正なヘッダ情報が追記され、攻撃や漏えいにつながる可能性ある
- ColdFusion側の対応
  - CF9.0.2 以降（9.0.0 / 9.0.1 は最新のセキュリティアップデートで追加）は、改行コードは強制的に削除されるようになっている
- 留意点
  - ヘッダに改行コードが含まれていると強制的に削除されるため、データが予期しない書き換えが発生しないか注意
    - <CFCookie>、<CFHeader>、<CFMailParam>に指定された値
    - クライアント変数を Cookie に保存
    - 特にデータの暗号化を行っている場合、暗号化データに改行コードがないか注意が必要となる

⑧ ハッシュ衝突攻撃 (Hash Collision Attack)

ハッシュ衝突攻撃 (Hash Collision Attack)

- 想定される脅威
  - サーバーへのパラメーターの送信(GET,POSTなど)で、複数の異なるキーが同じハッシュ値になるようなパラメータを大量に送り付け、サーバーのCPUを高負荷状態（Dos）にする
- ColdFusion側の対応
  - CF9.0.2 以降（9.0.0 / 9.0.1 は最新のセキュリティアップデートで追加）はPOSTの上限数が追加された（デフォルト100）
  - CF10 以降は、Tomcat側でも対策済みのバージョンを利用している
- 留意点
  - デフォルトのPOSTの上限数は 100なので、旧バージョンから移行する際などは、エラーにならないように適切な上限値にする

⑨ OS コマンド インジェクション

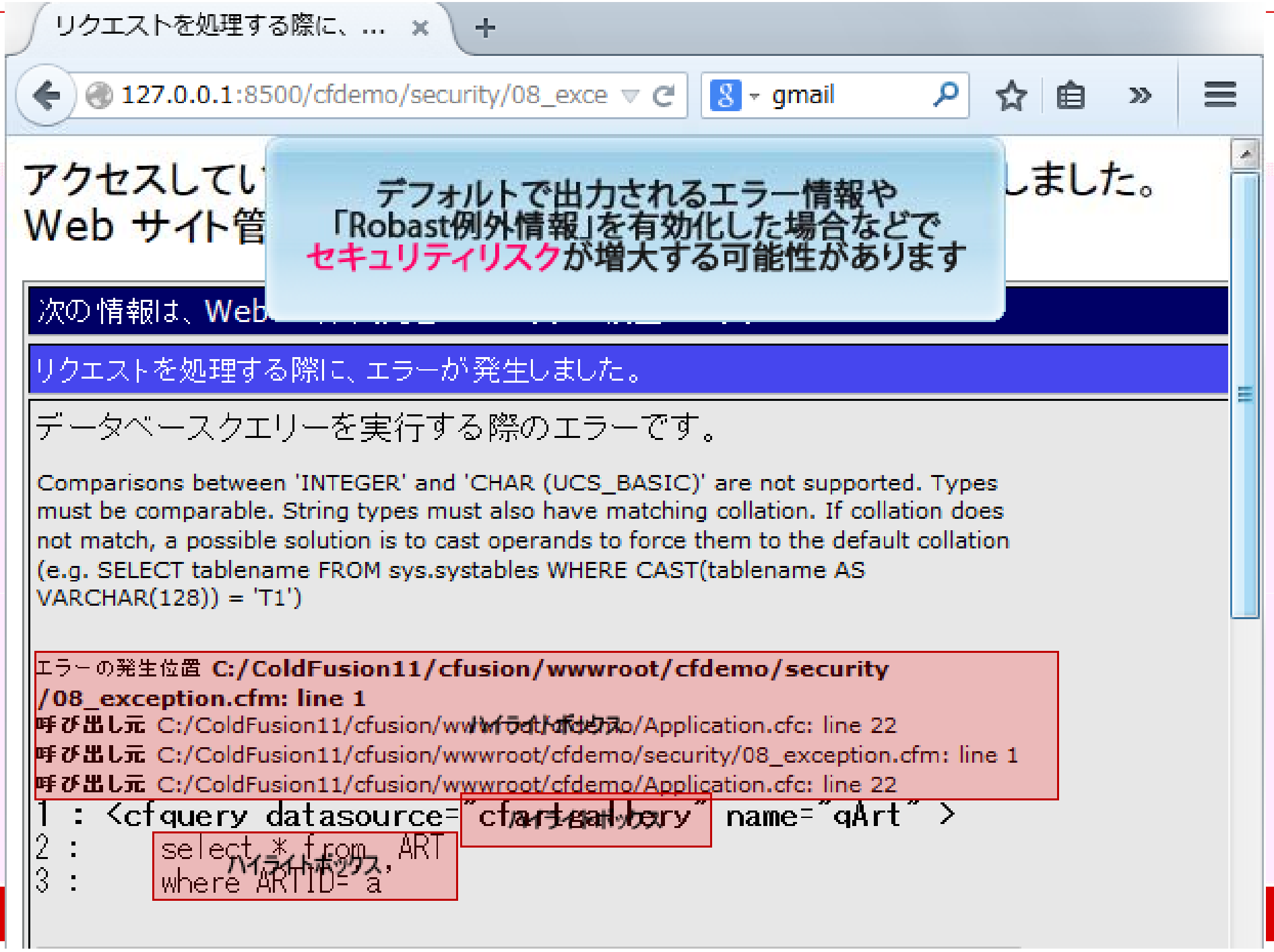
OS コマンド インジェクション

- 想定される脅威
  - 他の攻撃手段を利用して、OSのコマンドを実行するColdFusionプログラムを実行され、予期しないプログラムの実行や情報の漏えいが発生する
- ColdFusion側の対応
  - <cfexecute>や.NET呼び出しを行うページを処理する際は、動的なパラメーターの使用の有無やセキュリティ面に懸念がないかを確認する
  - Webサーバー側で不要なDLLプログラムが実行されないように注意する

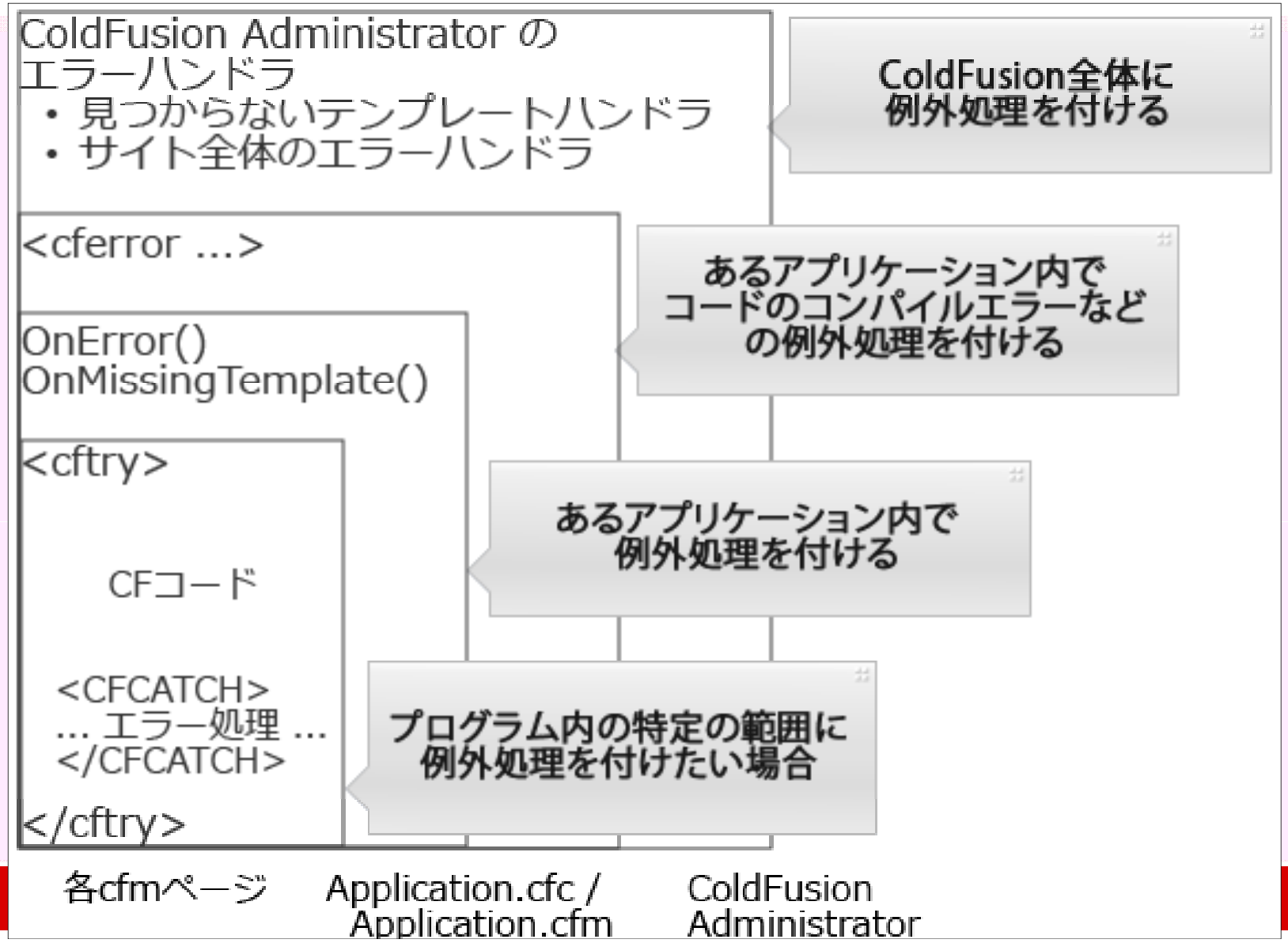
2.

セキュリティに影響する設定

例外処理


リクエストを処理する際に、...
127.0.0.1:8500/cfdemo/security/08_exce
gmail
アクセスしてい
しました。
Web サイト管
デフォルトで出力されるエラー情報や
「Robast例外情報」を有効化した場合などで
セキュリティリスクが増大する可能性があります
次の情報は、Web
リクエストを処理する際に、エラーが発生しました。
データベースクエリーを実行する際のエラーです。
Comparisons between 'INTEGER' and 'CHAR (UCS_BASIC)' are not supported. Types must be comparable. String types must also have matching collation. If collation does not match, a possible solution is to cast operands to force them to the default collation (e.g. SELECT tablename FROM sys.systables WHERE CAST(tablename AS VARCHAR(128)) = 'T1')
エラーの発生位置 C:/ColdFusion11/cfusion/wwwroot/cfdemo/security/08_exception.cfm: line 1
呼び出し元 C:/ColdFusion11/cfusion/wwwroot/cfdemo/Application.cfc: line 22
呼び出し元 C:/ColdFusion11/cfusion/wwwroot/cfdemo/security/08_exception.cfm: line 1
呼び出し元 C:/ColdFusion11/cfusion/wwwroot/cfdemo/Application.cfc: line 22
1 : <cfquery datasource="cfartgallery" name="qArt" >
2 : select * from ART
3 : where ARTID= a
ハイライトボックス
ハイライトボックス
ハイライトボックス

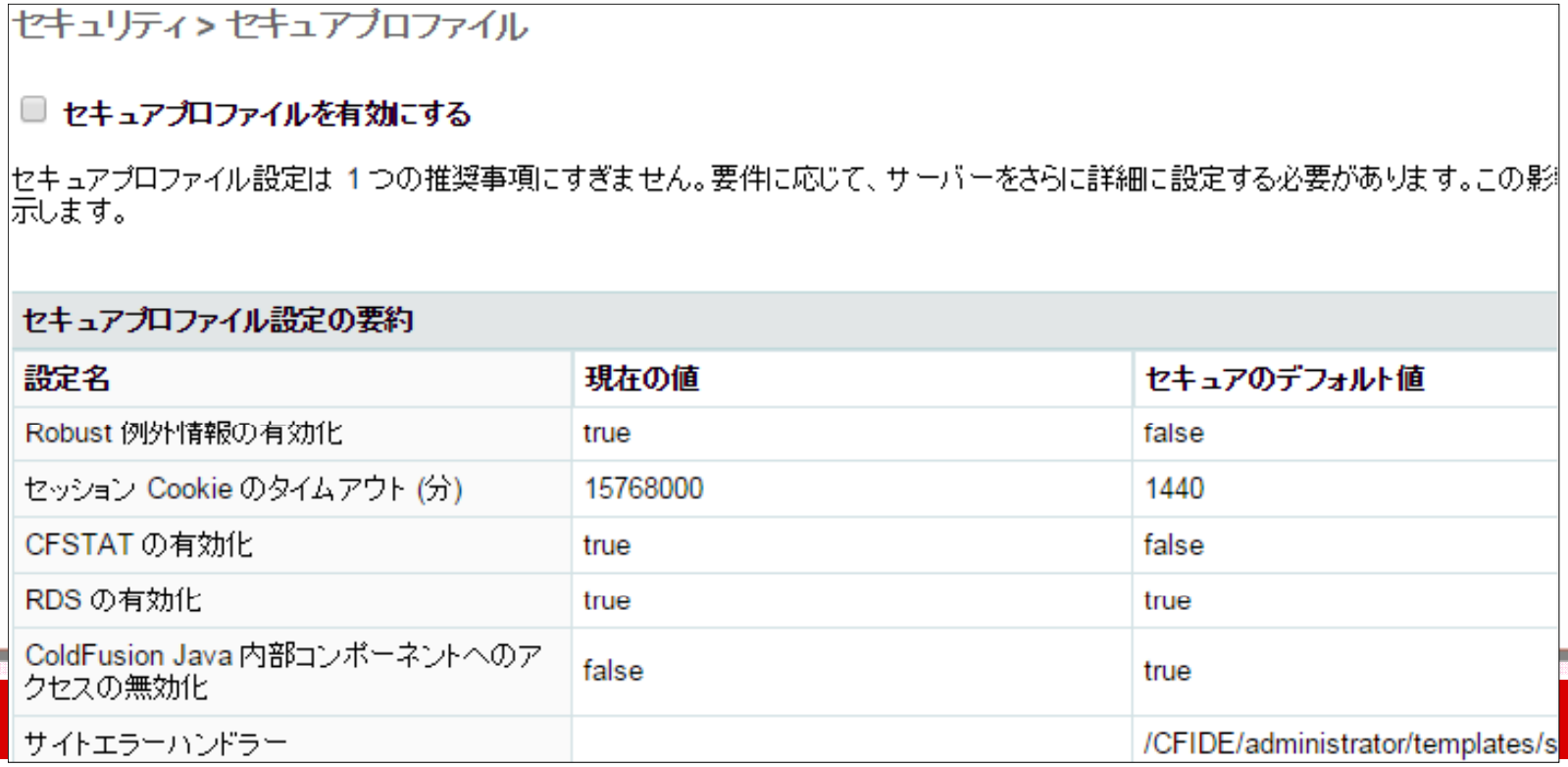
例外処理


ColdFusion Administrator の
エラーハンドラ
• 見つからないテンプレートハンドラ
• サイト全体のエラーハンドラ
ColdFusion全体に
例外処理を付ける
<cferror ...>
あるアプリケーション内で
コードのコンパイルエラーなど
の例外処理を付ける
OnError()
OnMissingTemplate()
<cftry>
CFコード
<CFCATCH>
... エラー処理 ...
</CFCATCH>
</cftry>
あるアプリケーション内で
例外処理を付ける
プログラム内の特定の範囲に
例外処理を付けたい場合
各cfmページ
Application.cfc /
Application.cfm
ColdFusion
Administrator

その他

セキュアプロファイル

- CF10以降、インストール時に本番公開に適したセキュリティ設定でインストールが可能。
  - CF11では、インストールのAdministratorでも、プロファイルを切り替える事が可能になった



セキュリティ > セキュアプロファイル

セキュアプロファイルを有効にする

セキュアプロファイル設定は 1 つの推奨事項にすぎません。要件に応じて、サーバーをさらに詳細に設定する必要があります。この影
示します。

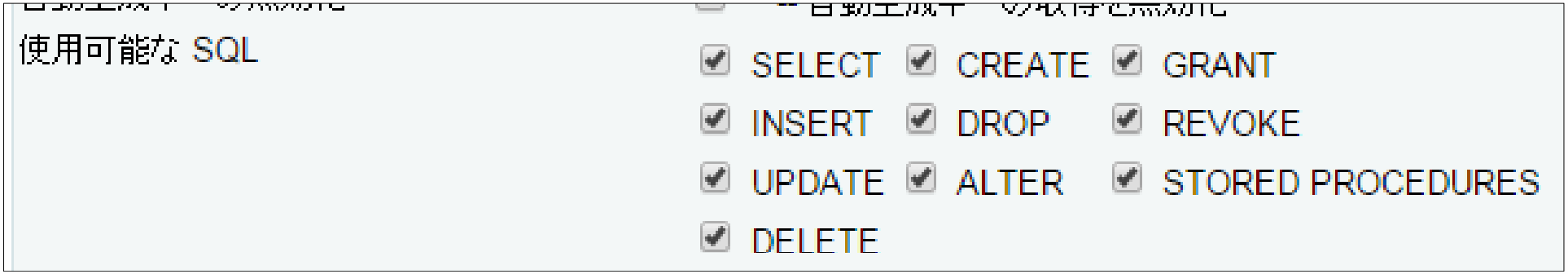
セキュアプロファイル設定の要約

設定名	現在の値	セキュアのデフォルト値
Robust 例外情報の有効化	true	false
セッション Cookie のタイムアウト (分)	15768000	1440
CFSTAT の有効化	true	false
RDS の有効化	true	true
ColdFusion Java 内部コンポーネントへのアクセスの無効化	false	true
サイトエラーハンドラー		/CFIDE/administrator/templates/s

データソース設定

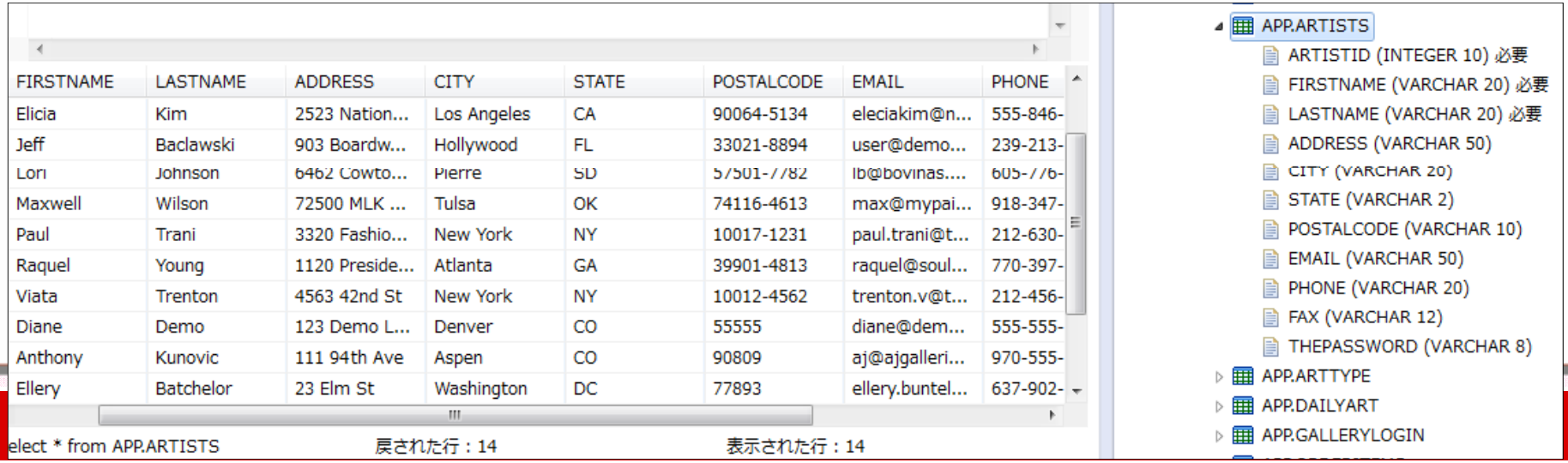
- 概要
  - データベースへの接続ユーザーの権限が適切かどうかの確認
  - 不要なSQLコマンドの実行を防ぐために、データソースの詳細

- ポイント
  - 不要なSQLコマンドの実行を防ぐために、データソースの詳細設定にある「使用可能な SQL」で必要のないコマンドを無効にする



RDSの 有効 / 無効

- 概要
  - ローカル / リモートからColdFusionに接続し、ファイルの一覧やデータソースの接続先情報にアクセスできる
- ポイント
  - 本番環境ではOFF！リモートからの不要な接続を許さない
  - 開発環境でRDSを使用する場合もAdministratorのログインパスワードとは別のパスワードを指定し、必要のない社内メンバーからの接続を防ぐ

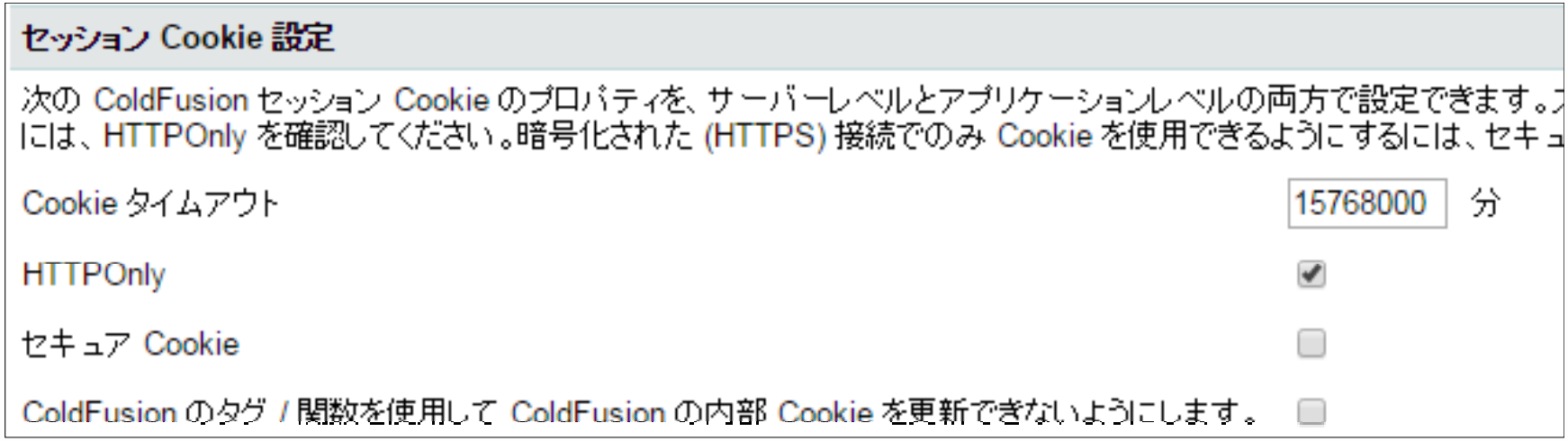


FIRSTNAME	LASTNAME	ADDRESS	CITY	STATE	POSTALCODE	EMAIL	PHONE
Elicia	Kim	2523 Nation...	Los Angeles	CA	90064-5134	eleciakim@n...	555-846-
Jeff	Baclawski	903 Boardw...	Hollywood	FL	33021-8894	user@demo...	239-213-
Lori	Johnson	6462 Cowto...	Pierre	SD	57501-7782	lb@bovinas....	605-776-
Maxwell	Wilson	72500 MLK ...	Tulsa	OK	74116-4613	max@mypai...	918-347-
Paul	Trani	3320 Fashio...	New York	NY	10017-1231	paul.trani@t...	212-630-
Raquel	Young	1120 Preside...	Atlanta	GA	39901-4813	raquel@soul...	770-397-
Viata	Trenton	4563 42nd St	New York	NY	10012-4562	trenton.v@t...	212-456-
Diane	Demo	123 Demo L...	Denver	CO	55555	diane@dem...	555-555-
Anthony	Kunovic	111 94th Ave	Aspen	CO	90809	aj@ajgalleri...	970-555-
Ellery	Batchelor	23 Elm St	Washington	DC	77893	ellery.buntel...	637-902-

elect * from APP.ARTISTS　戻された行：14　表示された行：14

セッションCookie設定

- CF10以降、セッションCookieに対するタイムアウト時間等の設定変更がAdministratorから可能になった
  - 従来からの<CFCookie>タグによる強制的なCFID, CFTOKENの上書き設定は動かなくなったため、プログラムの改修が必要
    - 下記のAdministratorの設定と同レベルの設定をプログラムで指定可



スケジュールタスク

- 概要
  - 指定された日時にColdFusionページを実行することができ、日次バッチ処理などに多用されている
  - タスクを使って.cfmファイルを書き出すような処理があった場合、ColdFusionの攻撃コードを外部から読み込み、結果を.cfmファイルとして書き出させると、その.cfmをリクエストされて攻撃される
- ポイント
  - 不必要なバッチが実行されていないか？
  - ColdFusion 10 以降、スケジュールタスクの結果をファイルに出力する際に指定できる拡張子に制限がある
    - デフォルトでは .txt / .log に制限される
    - ColdFusion 9は最新のセキュリティアップデートを当てることで同様の制限が有効となる

<CFInclude>

- ColdFusion 11より<CFInclude>タグでインクルードするファイルの内容を処理する拡張子を指定可能。
  - 例えば、.conf ファイルに<cfset>で変数をセットするようなページを作成していた場合、「conf」または「＊（デフォルト）」をセットしないと、ファイルの内容が処理されない
- ColdFusion Adminisrator または Application .cfc の This.compileextforinclude,<cfapplication>タグの compileextforinclude で拡張子をリスト形式で指定する

CFInclude タグで許可されるファイル拡張子
*
CFInclude タグ内で使用した場合にコンパイルされるファイル拡張子をカンマ区切りリストとして指定します。

Administratorへのアクセス制限

- CF10よりAdministratorへのアクセスをIPアドレスで制限
  - ただし、CF10 のアクセス制限は、セキュリティ面では不完全であり、CF11 で改良されている

*CFIDE/main/**
*CFIDE/adminapi/**
*CFIDE/administrator/**
*CFIDE/componentutils/**
*CFIDE/wizards/**
*CFIDE/servermanager/**

  - CF11では、さらに外部Webサーバーコネクタの設定でも制限が可能

アップデートの提供方法について

- **概要**
  - **ColdFusion10以降は、一部を除き ColdFusion Administrator の [サーバー更新]機能から行う**
    - セキュリティ問題を修正
    - 不具合の修正
    - ドライバやライブラリの更新 などが行われる
- **留意点**
  - **修正は累積で行われる、つまり最新のアップデートを当てると過去の修正も反映される**
    - いくつかのアップデートをスキップして最新パッチを適用する際は、過去の修正が影響した問題が発生しないかを調べる
    - Webサーバーのコネクタなど、アップデートの一部には、追加の手順が発生する場合がある

3.

環境面

（Webサーバー、JVM）

Ｗｅｂサーバー


インターネット インフォメーション サービス (IIS) マネージャー
WIN-NR32GBS32B9
ファイル(F)
表示(V)
ヘルプ(H)
接続
スタート ページ
WIN-NR32GBS32B9
アプリケーション プール
サイト
要求フィルター
フィルター規則を構成するには、この機能を使用します。
ファイル名拡張子
規則
非表示セグメント
URL
URL
アクション
/CFIDE/administrator 拒否
/CFIDE/adminapi 拒否
/CFIDE/AIR 拒否
/CFIDE/appdeployment 拒否
/CFIDE/cfclient 拒否
/CFIDE/classes 拒否
/CFIDE/componentutils 拒否
/CFIDE/debu
/CFIDE/imag
/CFIDE/multi
/CFIDE/orm
/CFIDE/portle
/CFIDE/probe
/CFIDE/sched
操作
要求フィルターには、デフォルトの設定として
/CFIDE/administrator などへのアクセス
を拒否する設定を追加します。

リモートからの脅威に備える必要性

- ColdFusion Administrator、adminAPI、 componentutils フォルダに対する遠隔（リモート）攻撃
  - 基本的にはパスワードセキュリティが掛っているが、ColdFusion Administratratorのログイン認証をバイパス（すり抜け）し、管理機能を利用して攻撃やコードの盗み見をしている脆弱性が過去にあった。
  - 未知の脆弱性にも備えるためには、それらのフォルダに対するリモートからのアドレスを遮断したい
- 最新のセキュリティアップデートと複雑なパスワードの指定だけでは、未知の脅威まで防ぐことはできない

補足

■補足

- メーカーが推奨する防御方法は、「ロックダウンガイド」に掲載されている方法となる。
  - ガイドに掲載されている方法は、実行ユーザーの変更やファイルアクセスの制限が行われてるため、プログラムの追加・改修やセキュリティアップデートのAdminsitratorからの適用に制限が生じる場合もある
- 他にもロードバランサーでのアクセス遮断、WebサーバーでのIPアドレス制限などがあるが、外部のみならず内部（ホスティング環境などの場合は接続してくるユーザー等）からの脅威を想定して、適切なWebサーバーセキュリティ設定を行うことを強く推奨する。

JVM

Java サポートについて

- （2012年9月以降）Javaサポートに関するポリシー
  - 従来）メーカーで動作を確認したJVMのバージョンのみサポート
  - 最新）製品がサポートするJavaバージョンの最新のマイナーアップバージョンもサポート対象
    - http://wwwimages.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf11/coldfusion11-support-matrix.pdf
      - All ColdFusion users can upgrade Java to the latest minor version for their ColdFusion servers. For example, ColdFusion users using jdk 1.6.0_x can upgrade to the latest jdk 1.6.0_x update. (At the time of writing, the current version is jdk 1.6.0_35.) All future JDK 1.6.0_x releases are supported.
- Java自体のセキュリティの問題が発覚した際は、深刻度に応じて最新のマイナーバージョンに切り替えることを推奨

サポートするJavaバージョン

- CF 9.0.x と CF10（旧インストーラー）には、JRE 6が同梱
  - JVMメーカーの Oracle 社では、2013年2月に無償サポートが終了
    - Javaの最新のセキュリティ問題に対する対応は、以後Oracle社が提供する有償サポートに加入する必要がある
- Java 7サポート
  - 最新の累積ホットフィックスを適用したColdFusion 9.0.x
  - ColdFusion 10 Update 8 以降
  - 2013年3月に公開された新しい ColdFusion 10 インストーラー
  - ColdFusion 11
- Java 8サポート (New!!)
  - ColdFusion 10 Update 14 – 2014年10 月公開
  - ColdFusion 11 Update 3　– 近日公開予定

お問い合わせ先

株式会社サムライズ

アドビソフトウェア事業部 ColdFusion ビジネスユニット

◆サムライズ ColdFusion公式サイト

「製品情報・製品価格・購入前FAQ・セミナー資料の配布など」

http://www.samuraiz.co.jp/coldfusion/

◆ColdFusion Associate

「ColdFusion開発会社・パッケージベンダー・技術FAQなど」

http://cfassociates.samuraiz.co.jp/

◆ColdFusionカフェテリア

「寄稿連載記事・ColdFusion入門・その他サンプルプログラムなど」

http://forum.samuraiz.co.jp/