

JPNIC・JPCERT/CC セキュリティセミナー2003
守：～インシデントを未然に防ぐ～ 基調講演
2003年9月12日 後日配布版

安全なWebサイト設計の注意点

独立行政法人産業技術総合研究所
グリッド研究センター セキュアプログラミングチーム

高木 浩光

<http://staff.aist.go.jp/takagi.hiromitsu/>

本日の内容

- 「安全なWebアプリ開発30箇条の鉄則」より
 - 発注者向けに話題を絞って、詳細な実装技術よりも画面設計やSSLの話題を
- SSLの運用について追加分
 - セキュリティ欠陥とまでは言えないが、ユーザのためになすべき設計について
 - そもそもSSLとは何なのか
 - ユーザの視点から

そもそもSSLとは？

- 何のために使うのか
 - － 通信内容を秘匿するために
 - 理解されている
 - － 通信内容が改竄されていないことを確認するために
 - 理解されているか？
 - － 通信先が偽者ではないことを確認するために
 - 理解されているか？
- ユーザが理解していなければ意味がない
 - － どうして？

SSLが機能しない事態

- リンク先が https:// になっていない場合
 - これはサイト構築事業者のミス
 - そのままリンクを辿って情報送信をしたユーザは、盗聴による情報漏洩の危険にさらされる
- リンク先は https:// だが、リンク元が http:// の場合
 - これはミスでないと言えるか?
 - リンク元ページにアクセスしたとき、通信内容を改竄され、リンク先を http:// にすり替えられている可能性
 - そのままリンクを辿って情報送信したユーザは、盗聴される
 - リンク元ページも https:// にすべきか?
 - そのページのリンク元も? さらにその前も??
 - それはむちゃ

ユーザが確認するしかない

- 暗号化が必要だとユーザが感じた時点で、今見ている画面が https:// になっているかを、ユーザが目視確認するべきである
 - 全部の画面を https:// にしておくといわけにはいかないのだから
- 駄目な事例
 - パスワード送信先は https:// になっているのにパスワード入力画面が http:// になっている
 - 今見ている画面が改竄されている可能性
 - ユーザが自力でソースHTMLを見てFORM要素のACTION属性(送信先)が https:// になっているか確認すればよい?
 - それはむちゃな話だ

改竄されていないことの確認

- 重要な情報を閲覧するときの心得
 - 例: 株価情報、行政機関の発表情報などなど
 - その画面は `https://` になっているか?
 - なっていないのなら、通信路上で改竄されているか、偽サイトかも
- 重要な情報を提供するときの心得
 - 「すべての画面を `https://` にせよ」とまでは言わない
 - そうしてもよいが
 - 例: `https://www.netsecurity.ne.jp/` ここは`http`ではアクセス不可
 - 同じ画面を `https://` でもアクセスできるようにすべき
 - リンクを設けておくのは親切かもしれないが、必須ではなく、
 - ユーザが自力でアドレスバーの `http://` を `https://` に書き換えてアクセスするという習慣を身につけるべき

サーバ証明書の役割は？

- man-in-the-middle攻撃を防止する
 - － ドメイン名に対する署名
 - ドメイン名をcommon nameとする証明書に、認証局が署名を与えている
 - 認証局が証明書発行時に、署名要求者が、確かにそのドメインの所有者であることを確認して、署名する
 - その証明書に対応する秘密鍵を保持している者が提供しているサーバが、本物とみなされる
- ドメイン所有者が誰であるのかを保証する
 - － 組織名に対する署名
 - 証明書に組織名が書かれていおり、認証局が登記簿謄本などの提出を求めて本人であることを確認して署名する
 - － whoisの代替手段
 - ユーザはwhoisを使わなくともドメイン所有者を確認できる

攻撃の現実度は？

- パケット改竄の現実度は？
 - 無線LANでは？ 有線LANでは？
 - 大掛かりに書き換える必要はなく、「https」の5バイトを「http」の5バイトに差し替えるだけで攻撃は成立する
- 偽サイト提供の現実度は？
 - DNS spoofingなど
 - 偽DHCPサーバ
- 可能性の低くない状況
 - ホテルや集合住宅のLANなど

セキュアシールの意味は？

- 信頼マーク
 - 証明の確実性に対する信頼の感覚的表示
 - マークだけ見ても意味がない
 - アクセス先のサーバ証明書が別の認証局から発行されている可能性
 - ブラウザの証明書確認機能で証明書の署名者を確認した上でマークのリンク先を確認する
- 取り消されていないことの確認
 - リンク先の認証局にある確認用データの存在意義はこれだけ(か?)
- 誤った理解
 - 「〇〇社の世界最高レベルの暗号技術を使っています」
 - 「当社は〇〇社の認証を受けています」

駄目な事例

- 情報処理技術者試験センター「インターネット受験申し込み」システムの事例(2003年7月7日時点)
 - 試験センターのドメイン名は「jitec.jp」
 - ユーザはこのドメイン名に日ごろから慣れ親しみ、信頼できるドメインであると認識している(というか、そういう信頼を得ておく必要がある)
 - <http://www.jitec.jp/index.html> のページからリンクされていた「インターネット受験申し込み をクリックしてください」のリンク先は <http://www2.52school.com/jitec/guidance200302.jsp> となっていた
 - 「52school.com」って誰? サーバ証明書の内容は.....
 - CN = www2.52school.com
 - O = 52school.com
 - L = Shibuya-ku
 - S = Tokyo
 - C = JP
 - ハア?

なぜ駄目なのか

- リンク先がすり替えられている可能性がある
 - トップページは `http://` なので通信路上で改竄されている可能性がある
- ユーザがとらざるを得ない行動
 - クレジットカード番号を入力する際に、画面が `https://` になっていて、かつ、信頼できる送信先になっていることを目視確認する
 - 「52school.com」を目視確認して、何をどう納得せよというのか?
 - <https://www.jitec.jp/> に一旦アクセスしたうえで、リンク先にジャンプするという回避策をとらざるを得ない
 - jitec.jpが意図したサイトだということを確認できる
- 結論: もっと保有ドメイン名の価値を認識せよ

JNSAセキュリティセミナー in IW2002
基調講演 (2002年12月17日)
後日配布版

安全なWebアプリ開発 31箇条の鉄則

独立行政法人産業技術総合研究所
グリッド研究センター セキュアプログラミングチーム

高木 浩光

<http://staff.aist.go.jp/takagi.hiromitsu/>

Webサイトにて公開中

<http://staff.aist.go.jp/takagi.hiromitsu/#2002.12.17>

目次

- 画面設計の鉄則
 - 1.アドレスバーを隠さない 2.FRAMEを使わない 3.ブラウザの設定変更を強要しない 4.ユーザ名だけでログインさせない 5.認証キーには秘密情報を 6.パスワードを4桁数字にしない 7.認証エラーで存在を暴露しない 8.認証で秘密情報を暴露しない 9.パスワードリマインダの鉄則
- セッション実装の鉄則
 - 10.公開ディレクトリに置かない 11.全てのアクセスを認証チェック 12.アクセス許可対象者を限定する 13.URLに秘密情報を入れない 14.セッションIDを使う 15.セッションIDは予測不能に 16.状態はすべてサーバ側に持たせる 17.XSS脆弱性を排除する 18.HTMLタグの入力をさせない 19.ログアウト機能を用意する 20.際どい操作はPOSTにする 21.ログイン前にセッションID発行しない
- 万が一に備える鉄則
 - 22.Cookieの有効期限を短く 23.Cookieの有効ドメインを狭く 24.POSTによる画面推移方式を検討 25.個人情報閲覧に再度パスワードを 26.カード番号は全桁表示しない 27.パスワード変更には現パスワードを
- SSL使用時の鉄則
 - 28.自己発行証明書で運用しない 29.Cookieのsecureフラグを立てる 30.何を暗号化するかを明確に

画面設計の鉄則

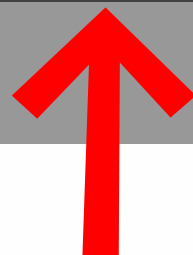
1.アドレスバーを隠さない

- ドメイン名は、ブランド名、社名に相当する、利用者から見た信頼の起点
- 隠すことに何ら意義はない
 - URL中のパラメタ部を弄られたくない?
 - 弄られるとセキュリティ上の問題が起きるシステムは、アドレスバーを隠したところで攻撃される
 - 戻るボタンを押されたくないのと同じ理由?
 - 推奨しない操作により利用者の利便性が損なわれる(セッションが途切れるなど)のは、利用者の責任
- 同じ理由で: 右クリックの無効化をしたりしない
 - 右クリックを禁止にする意義は全くない

事例: 銀行

- なぜか銀行でアドレスバーを隠すのが大流行
- 脅威
 - その銀行を装った偽ウィンドウを作られる
 - デジタルコピーは正確かつ簡単
 - どうやって被害者の画面に偽ウィンドウを出すか
 - たとえば無差別送信メールによる攻撃
 - 「こちらは〇〇銀行です。ただ今キャンペーン実施中。期間中にログインされた方には漏れなく粗品をプレゼント!」というメッセージとともに、偽のログインウィンドウを出現させるHTMLメールなど
 - 偽ウィンドウに誘ってどんな悪事を?
 - 口座番号とパスワードを入力させて盗む
 - 乱数表による第二暗証があるから振込は無理?
 - 偽ウィンドウへのアクセスを本物の銀行に中継し、振込先だけ差し替えて中継

ログイン



ログイン

店番号、口座番号、ログインパスワードを入力し、「ログイン」ボタンをクリックしてください。

.....

| | |
|------------|--------------------------|
| ■店番号 | <input type="text"/> |
| ■口座番号 | <input type="text"/> |
| ■ログインパスワード | <input type="password"/> |

.....

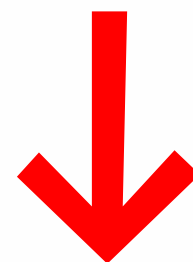
なお、店番号、口座番号をお忘れの場合は「各種お手続き」の「口座番号を忘れたかた」をご覧ください。
ログインパスワードをお忘れの場合は「各種お手続き」の「ログインパスワードを忘れたかた」をご覧ください。

キャンセル

入力内容のクリア

ログイン

**このウィンドウは本物の〇〇銀行ですか？
SSLによる暗号化はされていますか？**





会員番号

ログオンパスワード

クリア

ログオン

閉じる



**右クリックの自由まで奪っている例
プロパティでURLを確認することすらできない**

実話

- 日本のある銀行で実際にあった事例
 - 新システムの稼働と同時にアクセス集中でつながりにくくなった
 - そこで、別のサイトに臨時のログイン画面が用意された
 - 利用者にメールで以下のような連絡があった
 - ○○銀行のホームページはアクセス集中により大変つながりにくくなっております。当面、下記のURLよりログインしていただきますようお願いいたします。
- 問題点
 - これが偽のメールだったらどうする？
 - この一件で、この銀行の利用者は騙されやすくなっている
 - 本来なら次の告知をするべきところ
 - 当行から OObank.co.jp 以外のサイトへログインを促すようなご案内することは一切ございません。そのような案内のメールがお客様に届いても、それは何者かが送信した偽のメールの疑いがありますので、ご注意ください。

騙されるのは利用者の自業自得？

- 利用者に確認を怠らせる
 - 本物の銀行がURLを隠したウィンドウを出しているなら、それに見慣れた利用者は、URLの確認を怠る
 - 銀行が、確認しないことを利用者に習慣付けている
- 利用者への啓蒙も別途必要
 - アドレスバーを隠すサイトを信用しない

事例: SSLのシール

- ベリサインの「Secure Siteシール」
 - クリックしたときに現れるポップアップウィンドウで、アドレスバーを隠していた(現在は隠していない)
 - このウィンドウのURLは <https://www.verisign.co.jp/...> になっていて、それを利用者が目で確認して初めて、シールの正しい確認になる

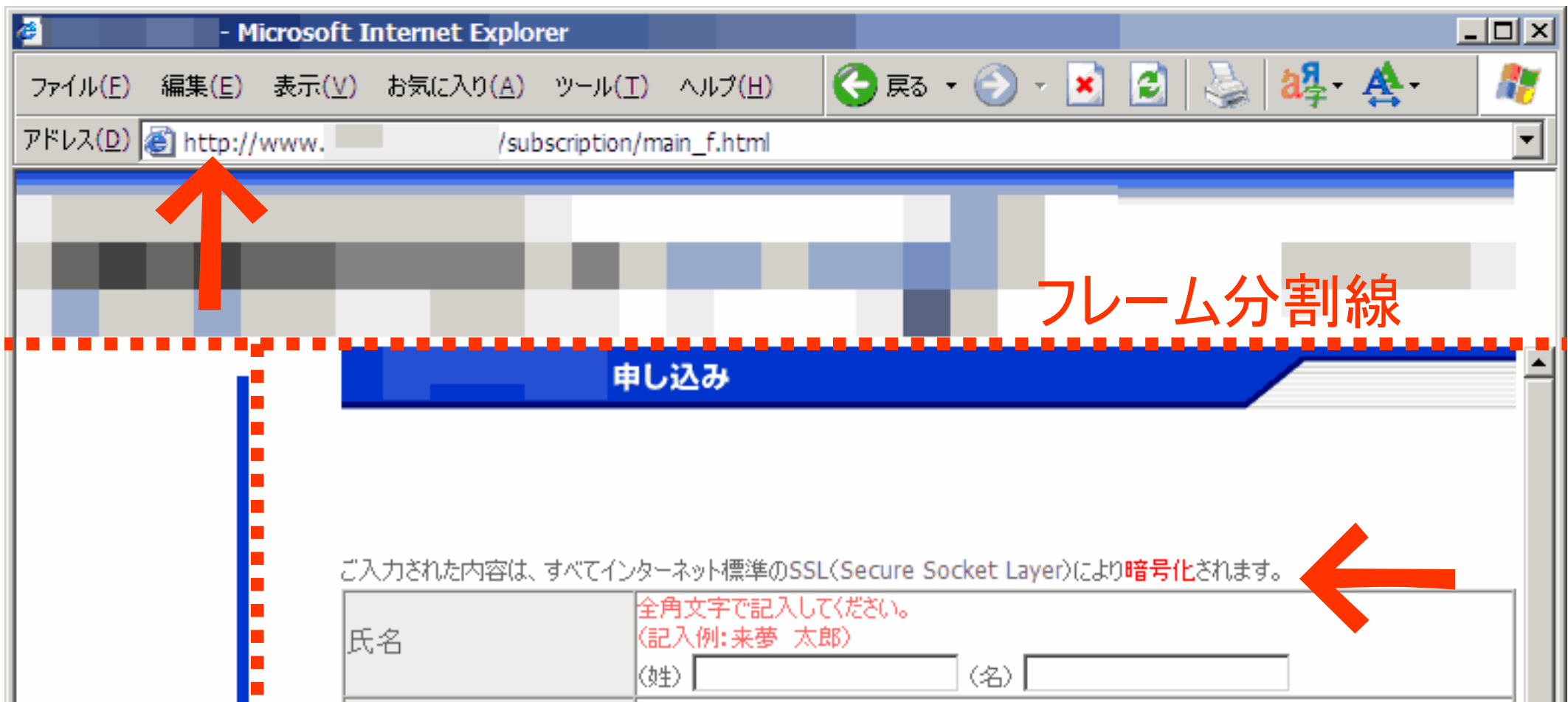


2.FRAMEを使わない

- サブフレーム中のURLを利用者が確認しにくくなる
 - 利用者に気づかれないように他のドメインに移行するのは、利用者を欺く行為
 - サブフレームでSSLを使用している場合は、その安全性を利用者が確認できない
- サブフレームのURLが他のドメインである場合に、cookieを発行できなくなる
 - IE 6のデフォルト設定では「サードパーティのcookie」として拒否されてしまう

事例: 「暗号化されます」本当?

- 親フレームのHTMLが通信路上で改竄されると、サブフレームの「申し込み」ページが http:// にすり替えられ得る
 - 「暗号化されます」と宣言したところで何の証明にもならない
 - URLがhttps:// であることを目視してはじめて確認できるもの



事例: IE 6でcookieを発行できず

- システムを直さずに、プライバシー設定を初期設定よりも緩くするようユーザーに指示することで解決しようとした
 - FRAMEでドメイン偽装をしなければ、このような設定なしにcookieを普通に利用できるにもかかわらず

農林水産省 メールマガジン - Microsoft Internet Explorer

アドレス http://www.maff.go.jp/mail/chg.html

農林水産省メールマガジン

ウェブブラウザの設定

農林水産省メールマガジンの登録解除手続きにあたっては、利用者の登録解除が不正に行われないように、ID/パスワードによる認証を行っております。その認証のセッション管理を行うためにクッキー(Cookie)を利用しております。

そのため、使用しているウェブブラウザがクッキー(Cookie)を使用するような設定になっていませんと、正常に動作しません。

クッキー(Cookie)を使用する設定を「ON」にする方法

- ・Microsoft Internet Explorer 6の場合

- 1.'ツール(T)'メニューの'インターネット オプション(O)...'を選択します。
- 2.ダイアログボックスの上段に並んでいるタブのうち'プライバシー'を選択します。
- 3.'詳細設定(V)'ボタンをクリックします。
- 4.自動Cookie処理を上書きする(O)にチェックをして『OK』ボタンを押します。
- 5.『OK』ボタンを押して、ダイアログボックスを閉じます。

3. ブラウザの設定変更を強要しない

- デフォルトより安全性の低い設定を指示するのは、利用者を危険に陥れる行為
- 事例
 - 「阪神北部広域TIKIカードコンソーシアム」が、未署名のActiveXコントロールを使わせるために、ICカード利用者に対して、IEの以下の設定を有効にするよう指示
 - 「未署名のActiveXコントロールのダウンロード」
 - 「スクリプトを実行しても安全だとマークされていないActiveXコントロールの初期化とスクリプトの実行」
 - 農林水産省メールマガジンが、FRAMEを使ったドメイン偽装画面でcookieを発行するために、IE 6のプライバシーレベルを下げる設定(cookieの受け入れを常に有効にする)を指示(前ページ)
 - 東京大学情報基盤センターが、危険性を示す警告画面を出なくする設定方法を、必要もないのに推奨



以上の手順でインストールが完了です。

(2) ICカードリーダー/ライターをご使用の方

各市町より貸与されましたICカードリーダー/ライターをご使用の方は次の手順に沿って接続を行ってください。

▼ICカードリーダー/ライタを使う為の準備

1. ICカードリーダー/ライタ本体を接続します。

1. ICカードリーダー/ライター本体とACアダプタを接続します。
2. ICカードリーダー/ライター本体とシリアルケーブルを接続します。(PC本体側はCOM1ポートに接続します。)

2. ICカードリーダー/ライターを使う時。

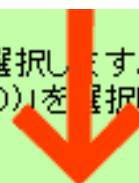
1. ICカードリーダー/ライターが上記の方法で正しく接続されていることを確認します。
2. ICカードリーダー/ライターの電源(本体背面の電源スイッチ)をONにします。
※ICカードリーダー/ライター本体の電源をPC本体の電源から供給する場合は、電源ランプ(本体上面)が緑色に点灯していることを確認してください。

3. インターネットエクスプローラーの設定(Version 5.0.2600.5512)

1. インターネットエクスプローラーのメニューの「ツール(T)」を選択します。
2. プルダウンメニューに表示される「インターネットオプション(O)」を選択します。
3. 「セキュリティ」タブを選択します。
4. 「レベルのカスタマイズ」ボタンをクリックします。
5. 下記の5項目の設定で「無効にする」になっている場合は「有効にする」又は「ダイアログを表示時する」(推奨)に変更する。
 - 「ActiveXコントロールとプラグインの実行」
 - 「スクリプトを実行しても安全だとマークされていないActiveXコントロールの初期化とスクリプトの実行」
 - 「スクリプトを実行しても安全だとマークされているActiveXコントロールのスクリプトの実行」
 - 「署名済みActiveXコントロールのダウンロード」
 - 「未署名のActiveXコントロールのダウンロード」

極めて危険な設定

ウイルス感染やデータ破壊、盗聴目的などの悪質なプログラムが自動的に起動することを許してしまう設定



証明書のインストールとブラウザの警告表示について

Active! mail を使用する際、ブラウザの設定によっては警告が何度も表示されます。以下の方法によって設定することで警告表示を減らすことができます。

警告表示は飾り?

• Internet Explorer 5.5 (Windows版) の場合

- メニューから ツール→インターネットオプション→詳細設定を選択し、セキュリティに関する項目の中で
 - サーバー証明書の取り消しを確認する(再起動が必要)
 - 発行元証明の取り消しを確認する
 - 保護つき/保護なしのサイト間を移動する場合に警告する
 - 無効なサイト証明書について警告する

の4つのチェックを外す。

- PCを再起動する。

• Netscape Navigator 4.7 (Windows版) の場合

- active! mailに初めてアクセスすると、新しいサイト証明書を受け付けるかどうか選択する窓が表示される。
- 次へ→次へ→"証明書を受け付ける(有効期限まで)"を選択→次へ→次へ→完了 と押す。
- メニューから Communicator→ツール→セキュリティ情報を選択する。
- Navigatorを選択し、警告の表示の中のチェックを外し、OKを押す。

• Netscape Navigator 6 (Windows版) の場合

- active! mailに初めてアクセスすると、新しいサイト証明書を受け付けるかどうか選択する窓が表示される。

4. ユーザ名だけでログインさせない

- 当たり前?
 - ところがどっこい、そういう事例が複数見られる
- 事例
 - JPNICがメールマガジンをはじめた当初、登録者のメールアドレスを入力するだけで、その人の住所、氏名、電話番号、性別、生年月日を閲覧、変更できた
 - メールアドレスで検索して閲覧する機能を提供するwhoisサービスとともとれるため、他人のメールアドレスを入力しても「不正アクセス」とならないおそれ
 - ある保険会社のサイトで、パスワードリマインダにユーザ名を入力すると、それだけで、登録メールアドレスが表示されるようになっていた



社団法人
日本ネットワークインフォメーションセンター

TOP ▲

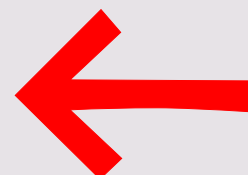
ENGLISH E

SITE MAP M

登録情報更新

電子メールアドレス:

変更



関連団体リンク ↑

入会案内 ●

お問い合わせ ✉

トピックス !

FAQ ?

FTP F

E-mail: secretariat@nic.ad.jp

[URLリンク・引用転載について](#) / [Copyright Notice](#)

Copyright (C) Japan Network Information Center. All Rights Reserved.



2001年9月3日

各位

社団法人 日本ネットワーク
インフォメーションセンター
(JP NIC:ジェービーニック)

メールマガジン登録時のセキュリティ不備について

一部報道機関において、JP NICが開始するメールマガジンサービスのシステムに第三者の個人情報を自由に閲覧できるセキュリティホールがあるという報道が行われました。

この状況は8月28日の購読登録受付開始後に発覚し、その後即座に登録受付をストップしました。続いて上記問題を解消するための対応を行い、8月31日に登録受付を再開しております。現在はそのような状況は発生しておりません。また、システム改善以前に登録された個人情報もデータベースより抹消しております。

既にご登録の皆様には、ご迷惑をおかけしましたことを深くお詫び申し上げます。

以上



5. 認証キーには秘密情報を

- パスワードのないサービス
 - 本人確認のために入力させるキーが、例えば、ユーザ番号と登録した電話番号になっているシステム
 - 実例
 - ジャストシステムのユーザ登録の変更画面
 - 注: 2003年4月2日に廃止
 - マイクロソフトのユーザ登録の変更画面
 - 旅の窓口のログイン画面
- 誰がこれを止められるのか
 - 明白に問題だと指摘できるのか
 - 程度問題であり妥当だと判断されているのかも

JUSTSYSTEM

ユーザーサービス



登録内容の変更

User IDの確認

User IDをお持ちでないお客様は、[ユーザー登録](#)をご利用ください。

User IDとご登録電話番号を入力の上、[次へ進む]をクリックしてください。

■ User ID

User IDはUser's Card(ユーザーズカード)などに印字されている10桁の番号です。

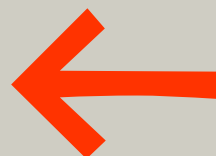
必須

※半角数字

■ ご登録電話番号

必須

(例) 03-1234-XXXX ※半角数字



次へ進む

中止

注：現在この画面は廃止されている(後述)

プライバシー情報の
取り扱い

[オンラインユーザー登録
に関するFAQ](#)

Microsoft USER Registration

製品一覧 | ダウンロード | サポート | 検索 | Worldwide |

Microsoft

Registration Home

登録について

登録ユーザー情報確認/変更

製品の登録方法

ライセンス譲渡

その他ユーザー登録のお問合せ

その他問合せ

製品購入前問合せ

アフターサービス

テクニカル

フィードバック

よくいただく質問

よくいただく質問(登録関連)

このページは、株式会社アグレックスによって運営されています。

最終更新日: 2002年 7月 17日

■ 登録ユーザー情報の確認/変更 ■

これまで購入されたマイクロソフト製品の登録情報を確認したい方
転居、電話番号変更等により個人情報が変更になった方は、こちらにお進みください。

ユーザー登録証上のユーザーID(07Xで始まる10桁の番号)と登録された電話番号により、

お客様個人情報の確認/変更ページに進むことができます。

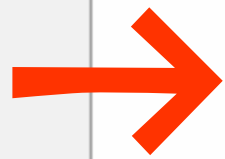
ユーザー ID 半角数字 例) 0701234567

登録電話番号 半角数字 例) 0312345678

「送信する」ボタンを押すと、登録ユーザー情報の確認/変更画面に入ります。

送信する

キャンセル



法における識別符号の定義

- 不正アクセス禁止法第二条2:

- この法律において「識別符号」とは、(中略)

- (1) 当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、
- (2) 次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
 - 1 当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
 - 2 (以下略)

警察庁担当者の見解

Q: 電話番号をパスワード代わりにするのは、不正アクセス禁止法の「識別符号」の要件を満たしていないのではないか?

A: 電話番号は(1)の条件、(2)の条件も満たさない。

会員番号は(1)の条件は満たす。

会員番号が(2)の条件を満たすかどうか:

- 「会員番号」は、一般に、アクセス管理者からみだりに第三者に知らせないように求められていると認識されるものとは考えがたく、規約等にアクセス管理者が第三者に知らせてはならないものと規定されていないならば、(2)の要件を満たさないと考えられる。したがって、
- 会員番号が、規約等にアクセス管理者が第三者に知らせてはならないものと規定されていれば、「会員番号、電話番号」は、「識別符号」に当たると考えられる。また、
- 会員番号が、規約等にアクセス管理者が第三者に知らせてはならないものと規定されていないならば、「会員番号、電話番号」は、「識別符号」に当たらないと考えられる。

この見解を紹介する意図

- 他人の会員番号と電話番号を入力してログインしても、不正アクセス禁止法違反にならないから、やってよいということではない
- 法による秩序の維持の恩恵に与れない
このようなシステム設計は不適切である

と言いたい

(規約で回避できるのかもしれないが)

補足

- ジャストシステムは、2003年4月から、パスワードを必要とする方式に切り替えた（次画面参照）
 - － なぜパスワードでなく電話番号を使ったのか（推定）
 - インターネットが登場する前からの古くからの登録ユーザについても、オンラインでサービスを利用できるようにしたかったためか
 - インターネットに登録したわけではない古くからの登録ユーザは、パスワードの登録をしていないので、既存の情報を使うしかない
 - 仮パスワードを事務局側が設定してユーザに知らせる方法もあるが、膨大な登録ユーザ全員に郵送するコストは大きすぎるのか
 - － そもそも古いユーザは自分の情報がWebで閲覧できるようになっていたことすら知らないのではないか
 - ジャストシステムは、2003年4月から、本人が希望した場合（パスワードを登録した場合）だけ閲覧できる方式に切り替えた

弊社では、登録ユーザー様の個人情報保護のため、セキュリティ強化を進めておりますが、この度、その一環として、ご登録ユーザー様向けオンラインサービス(以下、**オンライン登録サービス**)を以下のとおり変更いたします。サービスのご利用に際しましては、お客様にいくつかのお手続きを行っていただく必要があります。お手数をおかけいたしまして誠に申し訳ございませんが、趣旨ご理解のうえ、ご協力いただけますよう、お願い申し上げます。

「オンライン登録サービス」3つのポイント

1. お客様ご自身による **Web上での個人情報閲覧可否の選択**

オンライン登録サービスのご利用を希望されるかどうかを、選択していただきます。ご希望されない場合、今後、**Web上**でご登録情報へアクセスできなくなります。

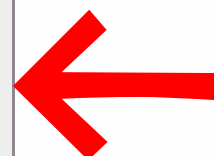
2. **本人確認方法をパスワード方式に変更**

サービスご利用の際の、ご本人様確認方法が下記の通り変更になります。

旧)お客様の **User ID** + ご登録お電話番号



新)お客様の **User ID** + お客様ご自身で設定されるパスワード
(以下、**User ID用パスワード**)



お手数ですが、**User ID用パスワードの設定**をお願い申し上げます。

※この度、設定いただくのは、お客様のユーザー基本情報(ご登録名義・電話番号・住所など)へのアクセスに必要な、**User ID用パスワード**です。
InternetDisk、Just MyShop、一本郎Web、ニコフパークなどの

6.パスワードを4桁数字にしない

- 4桁数字の暗証番号の安全性
 - ATMでの経験からそれなりに安全だと信じられている
 - 携帯電話でも4桁数字の暗証番号が使われている
 - Webとでは性質が異なるのであり、ATMや携帯電話の安全性は参考にならない
- ユーザ名の方を変化させるとロックされない
 - 認証を突破できるユーザ名と暗証番号のペアを収集できる
 - 同一ホストからの連続アクセスが制限されていても、コンピュータウィルスの力を借りて分散アクセスする攻撃や、一日数十回程度のゆっくりした攻撃があり得る
 - このリスクはインターネットならではのもの

残高照会サービス

お客様のご希望のサービスを下記より選択し、
下段の各項目を入力してください。

- 当日・前日・前月末残高照会
- 当日残高照会
- 前日残高照会
- 前月末残高照会

支店番号： (3桁)
支店番号を3桁で入力してください。

口座番号： (9桁)
預金種類2桁、口座番号7桁を続けて入力してください。
預金種類：普通預金=02・当座預金=01・納税準備預金=05・貯蓄預金=02

暗証番号： (4桁)
暗証番号を4桁で入力してください。

実行

クリア

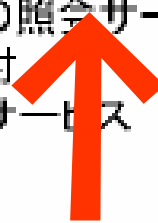


オンラインカスタマーサービス

●ご利用案内

オンラインカスタマーサービスは...をご利用中の方なら
どなたでも利用できるインターネットサービスです。

- ・ご利用料金の照会サービス
- ・各種変更受付
- ・申込書郵送サービス



申し込まなくてもこの
危険に晒される

ご利用にあたって ➡

電話番号・暗証番号を入力してください。

電話番号 (半角数字) :

例: 0901234XXXX

暗証番号 (半角数字) :



※お申し込み時にご記入いただいた4ケタの数字です。

7. 認証エラーで存在を暴露しない

- メールアドレスとパスワードを入力させるシステムで
 - 「メールアドレスが間違っています」というメッセージを出力するシステムは、指定されたメールアドレスの登録/未登録を暴露してしまう
 - 自己情報コントロール権の侵害となり得る
 - spam用アドレス収集装置を提供してしまっている
- 「ユーザ名またはパスワードが間違っています」と一律に表示すべき
- パスワードリマインダでは
 - 「メールを送信しました。到着しない場合は入力されたメールアドレスが間違っていた可能性があります」と表示すればよい

8. 認証で秘密情報を暴露しない

- 会員番号と誕生日で認証するシステム
 - 不正にログインされても利用者に害をもたらさないシステムでは妥当性がある
- パスワード認証機能はパスワード検証機能でもある
 - 会員番号と、予測年月日を入力してログインボタンを押す
 - 正解の場合と不正解の場合とで異なる結果となる
 - 大まかな年齢がわかっているならば、数千回程度の試行で判明
 - 簡単なプログラムで自動実行可能
 - 間違ってもロックされない場合



Web会員登録画面

項目を記入後、送信ボタンを押してください。



| | | | |
|--|------------------|---|-------------------------------------|
| | 会員番号 | | |
| | | | (会員番号は1999年より9桁に変わりました。新番号をご使用下さい。) |
| | 氏名 | (姓) <input style="width: 50px;" type="text"/> (名) <input style="width: 50px;" type="text"/> | |
| | | | (氏名は英字の場合も全角で入力して下さい。) |
| | 電子メールアドレス | | (パスワード返却先) |
| | 生年月日 | | (YYYY/MM/DD) |

※ Web会員として登録後、一時パスワードを発行します。
 ※ パスワードは返却先に指定されたアドレスにメールで通知されます。
 メールが届かない場合は、事務局にお問い合わせください。



[Web会員サービスストップページ ▲](#)

- 不正解の場合

 エラー

Web会員情報が間違っている、もしくは、有効な会員ではありません。



- 正解の場合

 エラー

Web会員として既に登録されています。



- 2002年9月19日に学会事務局に問題点を通知
 - 「下記の件、検討させていただきます」という返事のみ
 - 「会員番号を他人に知らせないように」などの注意はなし

9.パスワードリマインダの鉄則

- リマインダの答えを設定する箇所で、そのリスクについて説明する
 - パスワードと同様に秘密の情報にする必要があることを説明する(説明されるまで気づかないユーザがいるらしい)
- リマインダの答えを入力した後、パスワードを直接画面に表示ではなく、登録済みのメールアドレスへメールで送信するようにする
 - パスワードを生で直接送付するのではなく、パスワード変更用のセッションキー(短時間で無効化)入りURLを送付するのがベター
- リマインダの設定を拒否できるようにする

事例: 危険な質問選択肢

| | |
|---|--|
| <p>■ ユーザーID</p> <input type="text"/> | <p>IDについて ログインに必要な、あなたのIDです。「半角英数字」をお使いください。 記号は、- [マイナス] _ [アンダーバー]のみ使用可能です。</p> |
| <p>■ パスワード</p> <input type="text"/> <p>■ パスワード再入力</p> <input type="text"/> | <p>パスワードについて ログインに必要な、あなただけのパスワードです。 「半角英数字」をお使いください。 (4文字以上、10文字以内)</p> |
| <p>■ 秘密の質問</p> <p>■ 秘密の答え</p> <div data-bbox="703 1018 1279 1281"><p>1つお選びください</p><p>1つお選びください</p><p>生年月日は?</p><p>ご登録のE-mailアドレスは?</p><p>ご自宅の電話番号は?</p></div> | <p>秘密の質問と答えについて パスワードを忘れたときにお使いになる、あなたの「覚えやすい質問と答えの組合せ」を入力してください。</p> |
| <p>■ Eメールアドレス</p> <input type="text"/> | <p>Eメールアドレスについて あなたのEメールアドレスをご入力ください。</p> |

セッション実装の鉄則




10.公開ディレクトリに置かない

- 利用者から送信されたデータ(秘密とすべき情報)をCSVファイルに追記するなどの際に、ファイルの置き場所を公開ディレクトリとしない
 - CGIプログラムと同じ場所に出力先ファイルを置きたがるプログラマの心理に注意
 - 設定でアクセス制限をかけるのは危なっかしい
 - 後に別のサーバに移設した際に、設定が無効になっていたことに気づかなかったという事例が複数発生している
- 事例
 - 2002年だけで推定のべ数十万人分の個人情報漏えい事故
 - 大阪読売テレビ、小学館、高千穂交易、中央証券、TBC、YKKアーキテクチュラルプロダクツ、全日空ワールド、日本テレビエンタープライズ、日本大学通信大学院、三菱ガス化学、TVQ九州放送、砂糖を科学する会、山芳製菓、三井物産ハウステクノ、ブロックライン、アビバ、東日本ハウス、カバヤ食品、ブルドックソース、金印わさび、学習舎、名古屋国税局、東京経済大学、モバイルインターネットサービス他



Index of /cgi-bin/catalog/data

| Name | Last modified | Size | Description |
|----------------------|-------------------------------|----------------------|-----------------------------|
|----------------------|-------------------------------|----------------------|-----------------------------|

| | | | |
|--|-------------------|------|--|
|  Parent Directory | 23-Apr-2002 17:28 | - | |
|  catalog.csv | 06-Jun-2002 23:57 | 121k | |
|  catalog test.csv | 23-Apr-2002 19:12 | 3k | |

11.全てのアクセスを認証チェック

- ありがちな欠陥事例
 - － 画像ファイルに認証チェックをかけていなかった
 - 朝日新聞 2002年10月3日
学生の顔写真、認証なしで一時間閲覧可能な状態 筑波大
学生の一人がほかの学生の顔写真を閲覧できることに気づき、9月末に大学側に通報した。大学側は1日夜までに、アドレスを入れただけでは写真が表示できないようにしたという。
 - 毎日新聞 2002年7月8日
情報流出：複数の会員の写真が「ノツエ」のサイトから
閲覧した人によると、IDとパスワードを使わなくてもサーバーにアクセスでき、8日午前1時ごろには200枚以上の男女の写真を見ることができたという。
- 全てを認証チェックするのを基本とする
 - － 誰が見てもよいファイルだけチェックをスキップさせる

12. アクセス許可対象者を限定する

- 失敗事例
 - INTERNET Watch 2000年3月2日
プレイステーション・ドットコムで顧客情報流出
自分の購入状況をWebで確認できるようになっていた。その確認用WebページのURLの最後の部分の数字が、それぞれの顧客に振り分けられていたもののため、当てずっぽうで適当な数字を入力しても、他の顧客の番号と合致した場合に、その顧客の購入情報が見えてしまっていた。
- アクセス毎にセッションIDからユーザIDを取得し、それを元に必要なデータを取り出すように設計する
 - URLにユーザIDを出し、後にアクセス許可対象者チェックをするという設計は、チェック漏れを起こす

注意すべきはURLだけではない

- `<input type="hidden" name="..." value="...">`
にも注意
 - 今のところ事件として報道され発覚しているのは、URL中のIDを書き換えたアクセスによる流出ばかりだが、HTML中のhiddenなinputタグの値を書き換えてアクセスされた場合にも、同じ原因で流出が起き得る
- Cookieにも注意
 - cookieに直接ユーザ番号を入れていて(セッションID用cookieとは別に)、データ検索のキーにそれを使用している場合、ニセのcookieを送信されることで、流出が起き得る

13.URLに秘密情報を入れない

- 表示中ページのURLは、Referer機能によって、リンク先に送られる
 - URLは公開情報であると考えよ
- URLのパラメタ部は、ページ番号や商品番号など、見えてもかまわない情報(アクセス者を特定しない情報)に限定する
- 事例
 - URLにユーザ名やパスワードを含めている事例多数
 - 外部へのリンクがなくても危険な場合がある
 - https:// ページから http:// ページへのリンクがたどられたとき、Refererが暗号化されずに送信される

14.セッションIDを使う

- セッションIDを使わない方式には注意
(引数の場所: cookie、hiddenなinput)
 - ユーザIDだけを引数とする方式
 - 致命的な欠陥、認証なしと同等、ファイル丸見え並の危険性
 - ユーザIDとパスワードを直接引数とする方式
 - ユーザID+パスワードのハッシュ値を引数とする方式
 - これでもよいが、セッションIDを使う方式の方がより安全
- セッションIDを使えばよい
 - Webアプリケーションサーバが、セッションID自動発行の仕組みを持っている
- セッションIDとは?
 - 同じユーザでもログイン毎に異なるランダムな値

15.セッションIDは予測不能に

- 十分な長さ(20桁以上くらい?)
- 十分なランダム性
 - 良質な擬似乱数生成系を使用する
(下手に自作しないで既存のものを使う)
- 事例
 - 古いバージョンのWebSphereでは予測ができてしまった(某銀行は2002年初頭までそれを使っていた)
 - 連続して繰り返しログインしたときに発行されたセッションID
0001EGEAPVIAAA21QCXZAFITWSI
0001EGGBTOQAAA2VACXZAFJ4JSQ
0001EGG1NIYAAA2VCCXZAFJ4JSQ
0001EGGTY4QAAA2VECXZAFJ4JSQ
0001EGHQJQQAAA2VGCXZAFJ4JSQ

16.状態はすべてサーバ側に持たせる

- ブラウザ側にはセッションIDだけを渡す
 - サーバ側では、セッションIDをキーにそのユーザの状態を検索し、必要な情報を取り出す
- 便宜的にセッションID以外の状態情報も渡す場合
 - それがサーバに送り返されたときに、サーバ側ではその値を使用しない(書き換えられている可能性を想定する)
- 例外
 - パフォーマンス上の理由、負荷分散装置の都合、実装の簡潔化の都合で、サーバ側で毎回セッションIDから状態を検索したくない場合
 - セッションの最終段階のアクセスで、データが不当なものになっていないかチェックする

17. XSS脆弱性を排除する

- XSS (Cross-Site Scripting)脆弱性が生じないよう、全ての文字列出力で、メタ文字をエスケープするようコーディングする
 - そして、メタ文字そのものを出力する部分だけを例外的に、エスケープしないように書く
 - 後から対策するのではなく、初めからそのように書く
 - 例:
 - 「"」で括った文字列中では「"」はメタ文字なのでエスケープ
 - HTML中はそのすべての範囲において「<」「>」「&」がメタ文字なのでエスケープ

18.HTMLタグの入力をさせない

- 利用者の入力データにHTMLタグを含めることを許すシステム
 - そのようなシステムの実現はあきらめた方が賢明
 - 危険なタグをフィルタで排除するのは非常に困難
 - Hotmailに繰り返しセキュリティホールが発覚したのは、スクリプトが動いてしまうタグの書き方が無数にあり、フィルタで排除しきれなかったのが原因であり、同じ問題を抱えることになる
- 他の方法
 - 「phpBB」という掲示板システムでは、「<>」のタグに代わって「[]」を使ったマークアップ機能（「BBcode」）を用意して、安全な機能だけを提供している
 - 例: `[img]http://www.example.com/foo.jpg[/img]`
 - それでも、`[img]javascript:alert(document.cookie)[/img]`という穴があった（修正済み）

19.ログアウト機能を用意する

- ボタンが押されたら、サーバ側でそのセッションIDを無効化する
 - ブラウザ側のcookieを破棄させるだけで、サーバ側での無効化をしないサイトが見られるが、cookieがその間に盗まれていてもハイジャックされないために、サーバ側で無効化すべき

20. 際どい操作はPOSTにする

- すべての操作をGETアクションとして、セッション管理をcookieで行った場合、以下の危険性がある
 - 利用者が、ショッピングカートで発注の最終確認のページまで進んで、発注を取り止めていたときに、そのまま他のサイトに行って罾のページを踏んだ結果、発注実行のページへアクセスさせられて、買わなかったものを買わされる危険
 - 同様に、個人情報を変更しかけて、確認画面でキャンセルしたつもりが、罾のページによって変更を実行させられてしまう危険
- 最後の操作をPOSTアクションとし、hiddenなinputにセッションIDが入っていないと実行しないようにする
 - GETでは動かないようにする

21.ログイン前にセッションID発行しない

- (POST方式の場合)ログイン前に発行したセッションIDをログイン後にも使用するシステムには次の危険性がある
 - 攻撃者のサイトの罠のページに被害者がアクセスしたとき、攻撃者は自ら目的のショップにアクセスしてセッションIDを取得し、そのIDを含めたログイン画面へ被害者のブラウザをリダイレクトする
 - POST方式の場合にこれが問題となる
 - cookie方式の場合は、別のセッションIDが使用されて、XSS脆弱性がない限り他から注入されることはない

万が一に備える鉄則

22.Cookieの有効期限を短く

- セッションID用cookieの有効期限はセッション限りとする
 - － 必要もないのに保存されるcookieとしない
- セッションを越えて保存する必要のある情報を整理
 - － ユーザ名やパスワードの保存
 - － ログイン状態の保存
 - － 利用者の好みに応じた設定情報の保存
 - － アクセス追跡用ID（プライバシーポリシーでの明示が必要）
- 適切な期限でログイン毎に設定しなおす
 - － 例えば、1週間に一度でもログインがあったら、新たに1週間有効なcookieを発行する など

23.Cookieの有効ドメインを狭く

- 事例: ポータルサイトの危険性
 - 安全性が重く求められるサービス(クレジットカードを使うなど)と、危なっかしいサービス(無料ホームページ、掲示板、Webメールなど外部から書き込まれるページ)が同じドメイン上に同居している
 - cookieがドメイン全域で有効となっている
 - どこか一箇所にもXSS脆弱性があるスクリプトが動くようだと、そのcookieは盗まれてしまう
- サブドメインを使って、重要なサービスと危なっかしいサービスを隔離するべき

24.POSTによる画面推移方式を検討

- cookieは、XSS対策漏れや、ブラウザのセキュリティホールによって漏洩する可能性があり、セッションハイジャックの危険性がある
 - セッションIDをcookieに入れずに、hiddenなinputに入れて、POSTアクションで画面遷移をさせる方式にすれば安全性は高まる
 - ただし、画面設計の自由度が低下する

25. 個人情報閲覧に再度パスワードを

- セッションハイジャックされても被害を最小限に
 - 個人情報の閲覧、修正機能は稀にしか使わない機能なのだから、別途パスワード入力が必要なようにしてもよい
- セッションIDを2重化する
 - 個人情報修正画面に2度目のパスワードで入ったその中の画面のセッション管理が、外のセッションIDで行われるのでは、ハイジャック対策にならない
 - ここだけPOSTにして、hiddenなinputに2番目のセッションIDを入れておく

26.カード番号は全桁表示しない

- 登録済みクレジットカード番号の確認、変更画面で、カード番号は下位4桁だけ表示する
 - － どのカードを登録しているかさえ確認できればよいので、全桁表示する必要がない

27.パスワード変更には現パスワードを

- パスワード変更には、現在のパスワードの再入力が必要とする
 - － 同様に、リマインダの変更にも

あるいは

- 現在のパスワードをパスワード入力欄に表示しない
 - － 画面には「*****」と出ていても、HTMLソースを閲覧すれば見える

SSL使用時の鉄則

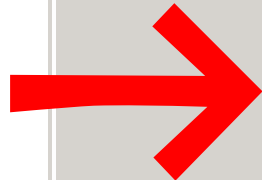
28.自己発行証明書で運用しない

- 自己発行証明書では盗聴を防げない
 - man-in-the-middle攻撃を防ぐには、サーバが本物であるかを確認する必要があり、そのためのサーバ証明書であり、ブラウザが信頼済みとしている認証局から発行したものでなくては、攻撃は防げない
- 事例
 - 多くのサイトが、誤った説明をして、安全ではないのに安全であると利用者を誤解させている

セキュリティの警告



このサイトと取り交わす情報は、ほかの人から読み取られたり変更されることはありません。しかし、このサイトのセキュリティ証明には問題があります。



このセキュリティ証明は、信頼する会社から発行されていません。証明書を表示して、この証明機関を信頼するかどうか決定してください。



このセキュリティ証明の日付は無効です。



このセキュリティ証明は、表示しようとしているページの名前と一致しません。

続行しますか？

はい(Y)

いいえ(N)

証明書の表示(O)

自前のルート認証局を運営？

- 自己発行のルート証明書をインストールさせる(すなわち認証局の運営)のは容易いことではない
 - － 安全な鍵管理体制を整え、CP(証明書発行ポリシー)とCPS(認証局運用規定)を作成して利用者に提示しなくてはならない
 - これは多大な費用を要することで、認証サービス業者からサーバ証明書を買った方が安いだらう
 - － ルート証明書を安全に配布しなくてはならない
 - 非ネット経由でフィンガープリントを示して利用者に照合させる必要があり、状況によっては非現実的
- 事例
 - － 安易にルート証明書を入れさせるサイト多数

29.Cookieのsecureフラグを立てる

- secureフラグの機能
 - デフォルト設定のcookieは、http:// と https:// のどちらにアクセスするときも、ブラウザからサーバへ送出される
 - secureフラグを立てたcookieは、https:// へのアクセスのときしか送出されない
- セッションIDを格納するcookieはsecureフラグを立てて発行する
 - そうしないと、http:// へのアクセス時に盗まれる
 - そうすると、すべてのページが https:// でないとセッション追跡できなくなる
 - すべてのページを https:// で構築する

https://とhttp://を混在させるには

- 2つのセッションIDを使う
 - http:// でも有効なcookieに1つ目のセッションID—(a)を入れ、https:// に限定したcookieに2つ目のセッションID—(b)を入れて、両者をサーバ側で対応付ける
 - パスワードが入力されたとき(この画面は https://)に発行する
 - http:// のページでは(a)のcookieでセッション追跡をし、https:// のページでは(b)のcookieでセッション追跡をする
 - (a)のcookieを盗んでも、https:// のページには入れないようにする

30.何を暗号化するかを明確に

- パフォーマンスの都合で、一部のページを http:// にするのなら、以下に留意する
 - 何の情報を暗号化で守るのかを明確にする
 - 守ると決めた情報、および、それへのアクセスに繋がるキーとなる情報が、http:// へのアクセスで流れないように設計する