情報セキュリティ対策　チェックリスト

（宿泊施設　用）

平成 30 年３月

国土交通省総合政策局
情報政策課サイバーセキュリティ対策室

目　　　次

【はじめに】

昨今、Wi-Fi サービスの提供や、ホームページでの予約受付等の拡大により、サービス利用者にとっての利便性が急速に向上しております。その一方で、サイバー攻撃の手法は高度化・巧妙化しており、サイバーセキュリティ対策の必要性が高まっているところです。

2020 年の東京オリンピック・パラリンピック競技大会の成功に向けて、宿泊施設の事業者は、非常に重要な役割を担うことになりますので、国土交通省では事業者に対してサイバーセキュリティ対策の状況についてアンケート調査を実施し、その結果を基に、サイバーセキュリティ対策の実施に当たっての参考としていただくためのチェックリストを作成しました。

【利用方法】

(1) 事業者において、サイバーセキュリティ担当者が全体を一読し、自らが回答する部分とベンダーから回答を得るものを確認してください。

(2) ベンダーから回答を得たら、自らの回答と併せて全体を確認することで、セキュリティ対策の状況について把握してください。

(3) セキュリティ対策は、推奨対策と追加対策の 2 種類に分けてありますので、自身の組織のセキュリティ対策状況を把握し、チェックシートの実施結果から対策が不十分な項目があれば、参考情報を基に、必要な対策を検討してください。

「推奨対策」 ・・・ 組織が検討及び実施することを推奨するセキュリティ対策。
「追加対策」 ・・・ 組織が推奨対策を実施後に、さらにセキュリティ対策を強化するために、実施を検討していただきたいセキュリティ対策。

(4) チェック方法（回答方法）は、以下のとおりです。

「はい」 ・・・ 質問（チェック）に対応している場合に選択します。
「いいえ」 ・・・ 質問（チェック）に対応していない場合に選択します。
「対象外」 ・・・ 他の対策を適用することで対策を兼ねている。または、対策すべきサービスや事象などが存在しない場合に選択します。

○ 宿泊施設用 チェックリスト

1. Wi-Fi のセキュリティ対策

推奨対策（8 項目）

No	分類	対策内容	チェック項目		
1	技術的対策	暗号化（WPA2 による）の設定をしている	はい	いいえ	対象外
2		接続している端末同士が通信できないように設定している	はい	いいえ	対象外
3		アクセスログを取得・保管している	はい	いいえ	対象外
4		違法・有害情報のフィルタリング等を実施している	はい	いいえ	対象外
5		Wi-Fi 管理者パスワードを設定又は変更するなどアクセス制御を実施している	はい	いいえ	対象外
6	利用者情報保護対策	利用者への提供条件やセキュリティ対策の情報を提示している	はい	いいえ	対象外
7		利用者の個人情報を必要以上に取得しない措置を実施している	はい	いいえ	対象外
8	規程・登録	Wi-Fi の設置・運用に求められるセキュリティ対策に関する規程を作成している	はい	いいえ	対象外

❑ Wi-Fi のセキュリティ対策の参考情報

No.1 暗号化の設定について

- 安全な無線 LAN 利用の管理 【総務省】
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/08.html

No.2 端末同士の通信について

- 企業等が安心して無線 LAN を導入・運用するために 【総務省】
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_kigyoutou.pdf
- 公衆無線 LAN 版審査項目（7-3）【インターネット接続サービス安全・安心マーク推進協議会】
  https://www.isp-ss.jp/examination/item/wi-fi.php

No.3 アクセスログの取得・保管について

- 通信履歴の電磁的記録の保全要請に関するＱ＆Ａ【法務省】
  http://www.moj.go.jp/houan1/houan_houan24.html

- 公衆無線 LAN 版審査項目（3 ログ情報・利用者情報等の取り扱いについて）【インターネット接続サービス安全・安心マーク推進協議会】
  https://www.isp-ss.jp/examination/item/wi-fi.php

No.4．違法・有害情報のフィルタリング　及び　No.7 個人情報の取得　について

- 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン 【一般社団法人日本インターネットプロバイダー協会】
  https://www.jaipa.or.jp/other/mtcs/

❑ その他の Wi-Fi のセキュリティ対策の参考情報

Wi-Fi 提供者向け　セキュリティ対策の手引き 【総務省】
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf
企業等が安心して無線 LAN を導入・運用するために 【総務省】
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_kigyoutou.pdf
一般利用者が安心して無線 LAN を利用するために 【総務省】
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_ippan_riyousha.pdf
Wi-Fi 利用者向け　簡易マニュアル 【総務省】
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_Users.pdf
公衆無線 LAN 版審査項目 【インターネット接続サービス安全・安心マーク推進協議会】
https://www.isp-ss.jp/examination/item/wi-fi.php

2. ホームページのセキュリティ対策

推奨対策（25 項目）

No	分類	対策内容	チェック項目		
1	ネットワーク対策	利用しない不要なポートは閉じていることを確認している	はい	いいえ	対象外
2		ルータ機器を使った不要な通信を遮断している	はい	いいえ	対象外
3		ファイアウォールによる通信の適切なフィルタリングをしている	はい	いいえ	対象外
4		ウェブサーバ（またはウェブアプリケーション）への不正な通信の検知や遮断をしている （具体的な対策事例：WAF、IDS、IPS の導入等）	はい	いいえ	対象外
5		ネットワーク機器のログを取得・保管している	はい	いいえ	対象外
6	詳細対策	公開すべきでないファイルや Web ページがある場合、公開していないことを確認している	はい	いいえ	対象外
7		定期的なソフトウェアの脆弱性対策を実施している （具体的な対策事例：セキュリティパッチの適用等）	はい	いいえ	対象外
8		不要なエラーメッセージを送らない対策を実施している （具体的な対策事例：OS のバージョン情報を返さない（表示しない）等）	はい	いいえ	対象外
9		ウェブアプリケーションのログを取得・保管している	はい	いいえ	対象外
10	ウェブサーバ対策	メーカーサポート切れの OS やサーバソフトウェア、ミドルウェアを使用していないことを定期的（１年に１回以上）に確認している	はい	いいえ	対象外
11		不要なサービスやアプリケーションがないか定期的（１年に１回以上）確認している	はい	いいえ	対象外
12		SQL インジェクション対策を実施している	はい	いいえ	対象外
13		OS コマンド・インジェクション対策を実施している	はい	いいえ	対象外
14		ディレクトリ・トラバーサル対策を実施している	はい	いいえ	対象外
15		クロスサイト・スクリプティング対策を実施している	はい	いいえ	対象外
16		CSRF（クロスサイト・リクエスト・フォージェリ）への対策を実施している	はい	いいえ	対象外
17		セッション管理不備の対策を実施している	はい	いいえ	対象外

18		HTTP ヘッダ・インジェクションの対策を実施している	はい	いいえ	対象外
19		メールヘッダ・インジェクションの対策を実施している	はい	いいえ	対象外
20		クリックジャッキングの対策を実施している	はい	いいえ	対象外
21		バッファオーバーフローの対策を実施している	はい	いいえ	対象外
22		アクセス制御や認可制御の処理を適切に実施していることを確認している	はい	いいえ	対象外
23	証明書の利用	証明書（EV SSL）を取得し、誰がサイトの運営者であるか証明している	はい	いいえ	対象外
24	暗号化	利用者との間で送受信する予約情報を暗号化している	はい	いいえ	対象外
25	情報の取扱い・規程	利用者から必要以上に個人情報を取得しないための措置を実施している	はい	いいえ	対象外

追加対策（1 項目）

No	分類	対策内容	チェック項目		
1	外部チェック	定期的な脆弱性診断を実施している （ペネトレーションテストを含む）	はい	いいえ	対象外

❑ **ホームページのセキュリティ対策を検討するための参考情報**

安全なウェブサイトの作り方 改訂第 7 版 【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/files/000017316.pdf
セキュリティ実装 チェックリスト 【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/files/000044403.xlsx
安全な SQL の呼び出し方 【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/files/000017320.pdf
ISP 版審査項目 【インターネット接続サービス安全・安心マーク推進協議会】
https://www.isp-ss.jp/examination/item/

3. 重要システム（客室管理システム、予約システム等）のセキュリティ対策

推奨対策（9 項目）

No	分類	対策内容	チェック項目		
1	客室管理システム	客室管理システムで取り扱うデータをバックアップしている	はい	いいえ	対象外
2		客室管理システムは、ホームページと同等のセキュリティ対策を実施している	はい	いいえ	対象外
3	予約システム	予約システムは、ホームページと同等のセキュリティ対策を実施している	はい	いいえ	対象外
4	予約情報の取扱い	個人情報を含む予約情報を外部とやり取りする場合は、暗号化など情報の保護の対策を実施している	はい	いいえ	対象外
5	クラウドサービス	客室管理システム、予約システム等について、クラウドサービスを利用している場合、規約や SLA の内容を確認している	はい	いいえ	対象外
6	ネットワーク分離	客室管理システム、予約システム等は、その他の業務システムや自社の情報システムとネットワークを分離している	はい	いいえ	対象外
7	機器	客室管理システム、予約システム等のネットワークに接続する機器（パソコン、メモリカード、USB メモリ等）のウイルスチェックを実施している	はい	いいえ	対象外
8	個人情報管理	個人情報保護に関する規程を整備し、適切に管理している	はい	いいえ	対象外
9		個人情報が流出した（流出したおそれを含む）場合の報告先（所管省庁や個人情報保護委員会等を含む）のリストを作成している	はい	いいえ	対象外

❑ 客室管理システム、予約システム等のセキュリティ対策を検討するための参考情報

安全なウェブサイトの作り方 改訂第 7 版 【独立行政法人情報処理推進機構】

https://www.ipa.go.jp/files/000017316.pdf

セキュリティ実装 チェックリスト 【独立行政法人情報処理推進機構】

https://www.ipa.go.jp/files/000044403.xlsx

安全な SQL の呼び出し方 【独立行政法人情報処理推進機構】

https://www.ipa.go.jp/files/000017320.pdf

ISP 版審査項目 【インターネット接続サービス安全・安心マーク推進協議会】

https://www.isp-ss.jp/examination/item/

4. 組織のセキュリティ対策

推奨対策（15 項目）

No	分類	対策内容	チェック項目		
1	対応方針 体制構築	経営者が組織全体のセキュリティリスクに関する対応方針（セキュリティポリシー等）を策定している	はい	いいえ	対象外
2		経営会議などでセキュリティ対策予算の検討が行われ、適切な予算を確保している	はい	いいえ	対象外
3		情報セキュリティ管理の責任者（CISO 等）を設置している	はい	いいえ	対象外
4		従業員向け研修等を継続的（1 年に 1 回以上）に実施している	はい	いいえ	対象外
5	基礎的 な対策	自社で利用している PC 等の IT 機器にセキュリティパッチを適用している	はい	いいえ	対象外
6		自社で利用している PC 等の IT 機器にウイルス対策ソフトを導入している	はい	いいえ	対象外
7		自社で利用している PC 等の IT 機器に利用者用のパスワード等を設定している	はい	いいえ	対象外
8		自社で利用している PC 等の IT 機器に導入しているソフトウェアのバージョン情報等を定期的に確認している	はい	いいえ	対象外
9	委託先のセキュリティ	業務委託契約書の中にセキュリティ対策の要求事項を記載し、委託先から定期的（1 年に 1 回以上）にセキュリティ対策に関する報告を受けている	はい	いいえ	対象外
10		サイバー攻撃を想定し、委託先との緊急連絡網を作成している	はい	いいえ	対象外
11	情報収集	自社に関係しそうなセキュリティインシデントや脆弱性に関する情報を収集する仕組みを構築し、情報収集活動を実施している	はい	いいえ	対象外
12	インシデント に備えた 対策	ウイルス感染、不正アクセス等のセキュリティインシデントが発生した場合の連絡先（所管官庁等を含む）のリストを作成している	はい	いいえ	対象外
13		法令上、安全管理措置を義務づけられている情報を保存しているサーバや端末を特定している	はい	いいえ	対象外
14		サイバー攻撃を想定し、緊急時にサーバや端末をネットワークから切り離す際の実施手順を策定している	はい	いいえ	対象外
15		標的型メール訓練などサイバー攻撃に対する定期的な訓練を実施している	はい	いいえ	対象外

追加対策（2 項目）

No	分類	対策内容	チェック項目		
1	緊急時 対応体制	セキュリティインシデント対応の専門チーム （CSIRT 等）を設置または機能を整備している	はい	いいえ	対象外
2	外部監査	セキュリティに関する外部監査を実施している （情報セキュリティに関する外部監査や脆弱性診断等も含む）	はい	いいえ	対象外

❑ **組織のセキュリティ対策を検討するための参考情報**

中小企業の情報セキュリティ対策ガイドライン 【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
サイバーセキュリティ経営ガイドライン 【経済産業省】
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
サイバーセキュリティ経営ガイドライン解説書 【独立行政法人情報処理推進機構】
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

○ 用語集

用語	説明
■CISO	Chief Information Security Officer の略 最高情報セキュリティ責任者または情報セキュリティ統括担当役員
■CSIRT	Computer Security Incident Response Team の略 組織内の情報セキュリティ問題を専門に扱うインシデント対応チーム
■EV SSL	Extended Validation Secure Sockets Layer の略 EV SSL 証明書とは、より厳しい認証により、Web サイトの正当性と安全性が分かりやすく伝わる SSL サーバ証明書のこと。
■PDCA サイクル	事業活動における生産管理や品質管理等の管理業務を円滑に進める手法の一つ。 Plan-Do-Check-Act の 4 段階を繰り返すことで製品と業務を継続的に改善する。
■IDS	Intrusion Detection System の略 侵入検知システム（ネットワーク上などへの不正なアクセスの兆候を検知し、ネットワーク管理者に通報する機能を持つソフトウェアまたはハードウェア）
■IPS	Intrusion Prevention System の略 侵入防止システム（IDS の発展型で、異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能を持つソフトウェアまたはハードウェア）
■SLA	Service Level Agreement の略 サービス提供事業者と利用者の間で結ばれる品質保証のレベル（定義、範囲、内容、達成目標等）
■WAF	Web Application Firewall の略 ウェブアプリケーションファイアウォール（ウェブアプリケーションの脆弱性を狙う悪意ある通信(攻撃)から、ウェブアプリケーションを保護するるセキュリティ対策の一つ）
■WPA2	Wi-Fi Protected Access 2 の略、最も安全な無線 LAN の暗号化方式
■SQL インジェクション脆弱性	ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。
■ディレクトリトラバーサル脆弱性	ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

用語	説明
■クロスサイトスクリプティング脆弱性	ウェブアプリケーションのプログラムがHTMLページを出力する場合に、プログラムがHTMLを文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がHTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、文字列を出力する際に、文字データあるいは属性値としてのみ解釈されるように適切にエスケープを施すなど、適切な方法により、入力データの無害化を行うなどの対策方法が考えられる。
■クロスサイト・リクエスト・フォージェリ（CSRF）脆弱性	掲示板や問い合わせフォームなどを処理する Web アプリケーションに脆弱性が存在すると、それを悪用し本来拒否すべき他サイトからのリクエストを受信し処理してしまう欠陥となる場合がある。このような欠陥を解決するためには、Web アプリケーション側でサイト外からのリクエストを受信又は処理しないようにシステムを作りこむ必要があり、具体的には、予測不可能な使い捨て ID による遷移画面の識別や、確認画面によるユーザへの再認証要求などの対策が考えられる。
■クリックジャッキング脆弱性	ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。
■メールヘッダインジェクション脆弱性	ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。
■HTTP ヘッダインジェクション脆弱性	ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、

用語	説明
	HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。
■バッファオーバーフロー及び整数オーバーフロー脆弱性	ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。