情報セキュリティ対策　チェックリスト

（鉄道事業者　用）

令和３年４月　第２版

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

チェックリスト（鉄道事業者用）

【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いる一方で、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ます。

本チェックリストにつきましては、平成３０年３月に初版を公表しておりますが、改めて事業者へサイバーセキュリティ対策の状況についてのアンケート調査を実施し、その結果を基に見直しを行い、第２版として作成しました。

各事業者の環境に応じたセキュリティ対策をとるための参考として活用されることを期待します。

【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、標準対策と望ましい対策の２種類に分けてあるので、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。

標準対策　・・・　組織が検討及び実施することが必要と考えられる以下のようなセキュリティ対策。

1）メジャーなセキュリティ規程（ISMS等）に記載されている

2）独立行政法人情報処理推進機構（IPA）が毎年発表している「セキュリティの10大脅威」等での近年の脅威を防ぐ主要な対策

3）共通脆弱性評価システム CVSS （ Common Vulnerability Scoring System）で高以上(CVSS基準値7以上)、Webアプリケーション脆弱性診断ツールとしてIPAが推奨しているOWASP ZAPでのリスク高、ネットワーク脆弱性診断ツールとしてグローバルで使用されているNessusで高に設定されている対策

望ましい対策　・・・標準対策ではないが、セキュリティ対策を強化するために検討及び実施することが望まし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。

（５）ネットワーク環境提供リスクと外部チェックの有効性

Wi-Fiなどの無線LANの環境や、顧客向けなどのWebアプリケーション環境を提供するためには高度なセキュリティ対策が施されていないと大きなリスクになります。必要なセキュリティ対策が採られているかは外部チェックで確認することができます。

1) ネットワーク環境提供のセキュリティリスク

① Wi-Fi環境

Wi-Fiが提供する個々人が使用するネットワークには外部の人が入れない仕組みがありますが、その仕組みが弱いと侵入を許すことになり、通信内容が窃取され、標的型攻撃など様々な攻撃にさらされることになります。

② Webアプリケーション環境

Webアプリケーションにおけるセキュリティ上の弱点があると、攻撃によってその機能や性能が損なわれる原因となります。また、Webサイト運営者の不適切な運用により、個人情報等の適切な管理がなされていないと、情報の流出を招くことになります。

2) 外部チェックの有効性

外部チェックは専門知識を持ち、資格要件を備えた者が行う「情報セキュリティ外部監査」という形態で有効性が確保されます。

① 専門知識

外部からの攻撃と同じ手段で擬似的に検証し、隠れた脆弱性を脆弱性データベースと比較して発見します。そして脆弱性が発見された場合はその対処方法を示します。

② 資格要件

国が「情報セキュリティサービス基準」を設けており(https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html)、その審査登録制度に適合した脆弱性診断サービスを行う事業者が日本セキュリティ監査協会情報セキュリティサービス基準審査登録委員会のHP(https://sss-erc.org/vulnerability)に掲載されています。

1. Wi-Fi のセキュリティ対策

標準対策（6 項目）

No	分類	対策内容	チェック項目			備考
1	技術的対策	暗号化（WPA2/WPA3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をしている	はい	いいえ	対象外	
3		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	
4	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	
5		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		
6	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	

望ましい対策（3 項目）

No	分類	対策内容	チェック項目			備考
1	技術的対策	アクセスログを取得・保管している	はい	いいえ	対象外	
2		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	
3	外部チェック	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外部のチェック（外部監査等）を受けている	はい	いいえ	対象外	

❑ Wi-Fi のセキュリティ対策を検討するための参考情報

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

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】

https://www.soumu.go.jp/main_content/000199323.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

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

違法・有害情報のフィルタリング 及び 個人情報の取得 について

電気通信事業者におけるサイバー攻撃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】
https://www.soumu.go.jp/main_content/000690267.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】
https://www.soumu.go.jp/main_content/000199323.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】
https://www.soumu.go.jp/main_content/000199322.pdf

Wi-Fi 利用者向け 簡易マニュアル【総務省】
https://www.soumu.go.jp/main_content/000690266.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

標準対策（16 項目）

No	分類	対策内容	チェック項目			備考
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	SaaSなどサービス自体の提供を受ける場合は対象外
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	SaaSなどサービス自体の提供を受ける場合は対象外
4		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	SaaSなどサービス自体の提供を受ける場合は対象外
5	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	
6		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	
7		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	
8		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	SaaSなどサービス自体の提供を受ける場合は対象外
9	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	SaaSなどサービス自体の提供を受ける場合は対象外
10		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	
11		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	
12		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	
13		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	
14		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	
15	証明書の利用	証明書（EV SSL）を取得し、サイトの運営者が誰であるか証明している	はい	いいえ	対象外	
16	情報の取扱い・規定	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		

望ましい対策（9 項目）

No	分類	対策内容	チェック項目			備考
1	ネットワーク対策	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	
2	ウェブサーバ対策	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）に確認している	はい	いいえ	対象外	
3		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	
4		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	
5		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	
6		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	
7		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	
8		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	
9	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 【独立行政法人情報処理推進機構（IPA）】
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（IPA）】
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（IPA）】
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. 組織のセキュリティ対策

標準対策（13 項目）

No	分類	対策内容	チェック項目			備考
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		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	
3		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	
4	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	
5		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	
6		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	
7		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	
8	委託先のセキュリティ	サイバー攻撃を想定した、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	
9	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	
10	インシデントに備えた対策	ウイルス感染や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	
11		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	
12		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	
13	運用・見直し・PDCA	セキュリティリスクや脅威への対策の定期的（1年に1回以上）な見直し（PDCAサイクルの実施）を行っている	はい	いいえ	対象外	

望ましい対策（8 項目）

No	分類	対策内容	チェック項目			備考
1	計画・資源確保	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	
2		顧客向けの予約システムとその他の業務システムのネットワークを分離している	はい	いいえ	対象外	
3		自社向けの業務システムとその他の業務システムのネットワークを分離している	はい	いいえ	対象外	
4		予約システム・業務システムに関連するシステムとその他の業務システムのネットワークを分離している	はい	いいえ	対象外	
5	委託先のセキュリティ	業務委託契約書内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	
6	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	
7	インシデントに備えた対策	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	
8	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（IPA）】
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（IPA）】
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

４．顧客向けの予約システムのセキュリティ対策

標準対策（14 項目）

No	分類	対策内容	チェック項目			備考
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	SaaSなどサービス自体の提供を受ける場合は対象外
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	SaaSなどサービス自体の提供を受ける場合は対象外
4		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	SaaSなどサービス自体の提供を受ける場合は対象外
5	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	
6		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	
7		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	
8		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	SaaSなどサービス自体の提供を受ける場合は対象外
9	証明書の利用	証明書（EV SSL）を取得し、サイトの運営者が誰であるか証明している	はい	いいえ	対象外	
10	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		
11	機器・ネットワーク	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	
12	クラウドサービス	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	
13	個人情報管理	個人情報保護に関する規程を整備して適切に管理している	はい	いいえ		
14		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	

望ましい対策（3 項目）

No	分類	対策内容	チェック項目			備考
1	ネットワーク対策	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	
2	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	
3	機器・ネットワーク	自社の情報システムと顧客向け予約システムのネットワークを分離している	はい	いいえ	対象外	

❑ **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 【独立行政法人情報処理推進機構（IPA）】
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（IPA）】
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（IPA）】
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/

５．重要システム（列車運行管理などの自社向けの業務システムや予約･業務システムに関連するシステム等）のセキュリティ対策

標準対策（13 項目）

No	分類	対策内容	チェック項目			備考
1	バックアップ	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	ネットワーク管理	ネットワークの出入り口を記載したネットワーク図を作成している	はい	いいえ	対象外	
3		重要システムを構成する機器以外からネットワーク接続できないようにMACアドレス等によるアクセス管理を実施している	はい	いいえ	対象外	
4		重要システムを構成する機器からのインターネットアクセスをブロックする仕組みがある（例：ゲートウェイやファイアウォールの設置等）	はい	いいえ	対象外	
5	構成管理	システム構成やネットワーク構成の管理（構成変更の確認を含む）を実施している	はい	いいえ	対象外	
6		システム構成やネットワーク構成の閲覧は、関係者以外できないように制限している	はい	いいえ	対象外	
7	機器管理	重要システムに接続できる機器（パソコンやメモリカード、USB メモリ等）を制限し、管理している	はい	いいえ	対象外	
8		重要システムに接続する機器（パソコンやメモリカード、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	
9		操作ログ（セキュリティに関するログを含む）を取得し、保管している	はい	いいえ	対象外	
10		操作ログの削除は、管理者権限に限定している	はい	いいえ	対象外	
11	リモートメンテナンス	遠隔地からの保守（リモートメンテナンス）は、決められた通信経路（IP アドレスを限定する等）で行われ、かつ保守担当の認証を実施している	はい	いいえ	対象外	
12	脆弱性対策	システムを構成しているソフトウェアの定期的な脆弱性対策を実施している	はい	いいえ	対象外	
13	規程	セキュリティ対策の規程を作成している	はい	いいえ	対象外	

望ましい対策（5 項目）

No	分類	対策内容	チェック項目			備考
1	機器管理	重要システムの管理端末と操作端末を別にしている	はい	いいえ	対象外	
2	ネットワーク管理	自社の情報システムと重要システムのネットワークを分離している	はい	いいえ	対象外	
3		電力系、空調系ネットワーク等と重要システムのネットワークを分離している	はい	いいえ	対象外	
4	リモートメンテナンス	外部サービスを受ける際に、持ち込み機材について、許可を与える等の管理をしている	はい	いいえ	対象外	
5	脆弱性情報の共有	同業種間での脅威情報や脆弱性情報などの情報共有を実施している	はい	いいえ	対象外	

❑ **重要システムのセキュリティ対策を検討するための参考情報**

国土交通省所管重要インフラにおける情報セキュリティ確保に係るガイドライン【国土交通省】
http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

制御システムセキュリティ運用ガイドライン【一般社団法人日本電気制御機器工業会】
http://www.neca.or.jp/wp-content/uploads/control_system_security_guideline2017.pdf

○ 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。
■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）
■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。
■SaaS	Software as a Serviceの略 ソフトウェアを利用者側に導入するのではなく、サービス提供事業者が提供するソフトウェアを、インターネット等のネットワーク経由で、利用者が利用する形態
■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セキュリティ対策の一つ）
■WPA3	Wi-Fi Protected Access 3 の略 無線LANの暗号化規格であるWPA、WPA 2 のセキュリティをより強固にした規格
■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。
■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「same origin」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。
■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。
■アクセス制御欠如と認可処理欠如の脆弱性	ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりすまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。
■OS コマンド・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OS のコマンドを操作する必要がある場合に、プログラムがOS のシェルのコマンドラインを用いてコマンド呼出しを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コマンドライン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、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンド・インジェクション脆弱性」と呼ばれている。OS コマンド・インジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない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。

■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。
■セッション管理の脆弱性	ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッションID が推測可能な値となっている場合、セッションID を URL パラメータに格納している場合、TLS（SSL）を使用しているセッションの管理に用いるcookie にsecure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的擬似乱数生成器（CSPRNG）で生成する十分な長さの文字列をセッションID として推測困難なものとし、secure 属性のセットされたcookie にこれを格納することでセッションID の漏えいを防ぐ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、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。
■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。