一般社団法人コンピュータソフトウェア協会
セキュリティ委員会
ソフトウェア出荷判定セキュリティ基準策定 WG

ソフトウェア出荷判定
セキュリティ基準チェックリスト

- 個票版 -

○本資料はソフトウェア出荷判定セキュリティ基準チェックシートの一覧表を各項番号目別に個票化したものです。

本成果物はクリエイティブ・コモンズ 表示 - 継承 4.0 国際 ライセンスの下に提供されています。
原作者のクレジット（一般社団法人コンピュータソフトウェア協会、ソフトウェア出荷判定セキュリティ基準チェックリスト-個票版-）を表示し、改変した場合には元の作品と同じCCライセンス（このライセンス）で公開することを主な条件に、営利目的での二次利用も許可されるCCライセンスです。なお、自社内でのみ利用される場合は、クレジット表示も不要です。
ライセンス証　：　https://creativecommons.org/licenses/by-sa/4.0/deed.ja
リーガルコード　：　https://creativecommons.org/licenses/by-sa/4.0/legalcode.ja

項目	Ver	日付	備考
ソフトウェア出荷判定セキュリティ基準チェックリスト-個票版-	1.0.0	2016/07/13	

No	1

対応する開発プロセス分類	ソフトウェア要件定義

対策項目
開発時の残存ファイルなど、サーバー上のデータの情報漏洩を防止する。

対策詳細
Web サーバー上にある開発関連データをドキュメントルート下に配置しない。

脅威シナリオ
データベースのダンプファイルやコンテンツのバックアップなど、Web サイトを解析する足がかりとなる情報や、個人情報などの重要な情報を誤ってドキュメントルート下に置いてしまうと、情報漏洩を招き、サーバー乗っ取りなどが発生する。

参考文献
■IPA セキュアプログラミング講座 Web アプリケーション編第 5 章暴露対策 https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄 運用障害	情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	外部からアクセス不能な一時ファイル保管場所を定義する。詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
		一時ファイル保管場所の確認テストおよび文書化	情報漏洩の有無の確認および文書化	文書の書式・保管方法の定義

No	2

対応する開発プロセス分類	ソフトウェア要件定義

対策項目

瞬間的なアクセス過多などによるサービス提供不能を防止する。

対策詳細

Web サーバーへのサービス拒否(DoS/DDoS)攻撃を対策する。
※アクセス過多による障害を招かないため
・同じ IP からのリクエスト回数を制限する。
・想定するリクエスト数に耐えられるようにする。
・対策機能を持ったルーター、ファイアウォールを導入する。

脅威シナリオ

運用上の想定を大幅に超えたアクセスへの対策を講じておかないと、サービス拒否攻撃により Web サーバーのシステムリ(CPU、メモリ、ディスク領域など)の消費を招き、Web サイトの運用障害が発生する。

参考文献

■DDoS 攻撃のソリューション(ARBOR)
http://jp.arbornetworks.com/ddos%E6%94%BB%E6%92%83%E9%98%B2%E5%BE%A1/

■DDOS 攻撃を撃退するには(Akamai)
https://www.akamai.com/jp/ja/resources/protect-against-ddos-attacks.jsp

脅威分類 ＜事象/結果＞
運用障害

脅威分類 ＜手段＞
DDoS 攻撃

機密性	完全性	可用性
–	–	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		可能な限りアプリケーションへの DDoS 攻撃を回避もしくはシステムリの枯渇を回避可能な設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
DDoS 攻撃による単体テストの実施および文書化	DDoS 攻撃による結合テストの実施および文書化	DDoS 攻撃のテストおよび文書化	DDoS 攻撃による運用障害の有無の確認、対策および文書化	文書の書式・保管方法の定義

No	3

対応する開発プロセス分類	ソフトウェア要件定義

対策項目

マスターを管理する。

対策詳細

バージョン管理システムを用いてアプリケーションのプログラムを管理する。

脅威シナリオ

プログラムのバージョン管理が適切になされないと、古いプログラムの混入を招き、過去に対策を行った脆弱性の復活が発生する。

参考文献

■チーム開発実践入門（技術評論社）
p39 理想的なプロジェクトとは（PDF）

■Git が、おもしろいほどわかる基本の使い方 33(MdN)
p12 Git を使ったバージョン管理（PDF）

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄 運用障害	脆弱性攻撃による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	－

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（運用保守）として要求する	非機能要件（運用保守）として要求する	開発環境の必須事項として定義する		
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
プログラムのマスターおよびバージョン管理実施、文書化	プログラムのマスターおよびバージョン管理実施、文書化	プログラムのマスターおよびバージョン管理実施、文書化	プログラムのマスターおよびバージョン管理実施、文書化	

No	4

対応する開発プロセス分類	ソフトウェア要件定義

対策項目

WAN 側に対して不要なポートを閉じる。

対策詳細

意図されていない WAN 側からの問い合わせ（DNS、NTP、NetBIOS-NS、ポートマッパーなど）に応答しないように既定値を変更・設定したり、イングレスフィルタリング(RFC2827/BCP38)を設定したりする。

脅威シナリオ

意図しない WAN 側からの問い合わせに応答しないように対策を講じないと、攻撃者に悪用され不正アクセスやサービス拒否（DoS，DDoS）攻撃を招き、改竄や運用障害が引き起こされる。

参考文献

■RFC2827　（IPA 独立行政法人 情報処理推進機構）
https://www.ipa.go.jp/security/rfc/RFC2827JA.html

■RFC 3704　（IPA 独立行政法人 情報処理推進機構）
https://www.ipa.go.jp/security/rfc/RFC3704JA.html

■イングレスフィルタリングとは（日本ネットワークインフォメーションセンター）
https://www.nic.ad.jp/ja/basics/terms/ingress-filtering.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
DDoS 攻撃 サービス妨害攻撃 脆弱性攻撃による権限昇格 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	システム要件の詳細設計の厳守事項として定義する。適格性確認テストの必須事項として定義する		
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
		アクセス権設定手順の確認および文書化	定期的なセキュリティの運用評価、文書化	外部応答するシステムの定義、定期的な見直し

No	5

対応する開発プロセス分類	ソフトウェア要件定義

対策項目

システム構成に合わせた脅威モデリングする。

対策詳細

システム構成とデータフローを検討することにより、どの界面でどのような脅威が発生しうるかを洗い出し、脅威リストを作成して優先度をつけ、攻撃への対策を講じる。

脅威シナリオ

脅威モデリングを実施しないと、対策の優先順位が不明確になり、危険度の高い攻撃への対策が後回しになったり、対策漏れが発生したりする。

参考文献

■IPA セキュアプログラミング講座 ＞ C/C++言語編 ＞ 脆弱性回避策とソフトウェア開発工程 ＞ 脅威モデリング
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c101.html

脅威分類 ＜事象/結果＞
全般

脅威分類 ＜手段＞
全般

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	適格性確認テストの必須事項として定義する	脅威モデリングの実施と文書化	モデリングの妥当性についての確認および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
モデリングの妥当性についての確認および文書化	モデリングの妥当性についての確認および文書化	モデリングの妥当性についての確認および文書化		

No	6

対応する開発プロセス分類	ソフトウェア 要件定義

対策項目

取引内容を第三者から保護し、当事者間だけの情報とすることを規定する。

対策詳細

コンピューター間の通信内容を SSL で暗号化したり VPN を経由するなどし通信を保護する。またユーザーは ID/パスワードで認証する。
暗号強度が低い場合は解読されるおそれがあるので、十分な強度にすることが望ましい。

脅威シナリオ

通信内容を暗号化したり、安全な通信経路を用いるなどの方法で保護しないと、通信内容の漏洩や改竄が引き起こされ、クレジットカードの不正利用や個人情報の漏洩が発生する。

参考文献

■いまさら聞けないサーバー証明書(サイバートラスト)
https://www.cybertrust.ne.jp/sureserver/basics/ssl_movie.html

■暗号技術入門第 3 版（SB クリエイティブ）
p364 第 14 章 SSL/TLS セキュアな通信のために

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄	中間者攻撃、盗聴による情報窃取

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	－

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。（通信の暗号化方式、暗号強度、秘匿方式など）		通信内容が保護されるよう詳細設計し、文書化する
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
	通信内容が保護されることを確認する結合テストの実施および文書化	通信内容が保護されることのテストおよび文書化		

No	7

対応する開発プロセス分類	方式設計

対策項目	【関連項目 No19】

認証情報を暗号化する。
この場合の認証情報とは、認証用のパスワード、マトリクス認証のパターン、生体認証用の生体情報、SOAP、REST 等で使用するアクセストークン（ID）などを指す。

対策詳細

認証用のパスワード、マトリクス認証のパターン、生体認証用の生体情報、SOAP、REST 等で使用するアクセストークン（ID）を、アプリケーション内部で保持する際は、リバースエンジニアリングや中間者攻撃に備えて、暗号化や難読化、もしくはハッシュ値で保持、保存する。また、認証情報をネットワーク、媒体などを通じて受け渡す際は、TLS1.2 による通信の暗号化を施す。
電子証明書は、秘密鍵のエクスポートを禁止し危殆化を防止する。

脅威シナリオ

認証情報の暗号化を怠ると認証情報の漏洩が起きるため、なりすましや、情報漏洩、データ改竄が発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p441 盗聴・改ざん対策（PDF）

■いまさら聞けないサーバー証明書(サイバートラスト)
https://www.cybertrust.ne.jp/sureserver/basics/ssl_movie.html

■暗号技術入門第 3 版（SB クリエイティブ）
p364 第 14 章 SSL/TLS セキュアな通信のために

■.NET で難読化を試してみる（とある技術者の劣等感）
http://ouranos.sakura.ne.jp/wordpress/2012/05/17/net%E3%81%A7%E9%9B%A3%E8%AA%AD%E5%8C%96%E3%82%92%E8%A9%A6%E3%81%97%E3%81%A6%E3%81%BF%E3%82%8B-%E7%AC%AC1%E5%9B%9E/

■不正な解析から知的財産を守る.NET アプリ「難読化」再入門 （CodeZine）
https://codezine.jp/article/detail/5444

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	暗号化方式の選定および文書化	暗号化を用いた設計の実施および文書化	暗号化を用いたる単体テストの実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
暗号化を用いた結合テストの実施および文書化	暗号化を用いたテストおよび文書化	認証情報が漏洩しないことのテストおよび文書化	認証情報への攻撃・漏洩の有無の確認、脆弱性情報の確認、対策および文書化	

No	8

対応する開発プロセス分類	方式設計

対策項目

自社製品に OSS を組み込む場合、セキュリティチェックする。

対策詳細

自社製品に組み込む OSS のセキュリティチェックを行って、その OSS が脆弱性や不正プログラムを含まないことを確認する。新規採用時のほか、その OSS のバージョンを挙げる際にもする。

脅威シナリオ

使用した OSS により意図しない不正プログラムを配布させられる可能性が存在する。また脆弱性を利用され、データの改竄、情報漏洩、なりすましなどが起こる可能性がある。

参考文献

■オープンソースソフトウェアを利用した出荷済製品のセキュリティ確保の活動（富士通）
https://www.fujitsu.com/jp/documents/about/resources/reports/securityreport/2015-securityreports/security-2015-08.pdf

■IPA テクニカルウォッチ「ウェブサイトにおける脆弱性検査手法の紹介（ソースプログラム検査編）」
http://www.ipa.go.jp/security/technicalwatch/20140306.html

■IPA MyJVN（フィルタリング条件設定）
http://jvndb.jvn.jp/apis/myjvn/mjcheck.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	開発環境の必須事項として定義する。（OSS 脆弱性情報の共有、チェック方法など）	ソフトウェアコンポーネント単位での脆弱性の回避および文書化	ソフトウェアコンポーネント単位での脆弱性の回避および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
ソフトウェアコンポーネント単位での脆弱性の回避および文書化	結合状況での脆弱性の回避および文書化	ソフトウェアコンポーネント単位および結合状態での脆弱性の有無の確認および文書化	ソフトウェアコンポーネント単位の脆弱性、結合状態での脆弱性情報の確認、対策および文書化	文書の書式・保管方法の定義

No	9

対応する開発プロセス分類	方式設計

対策項目

外部に依存するサービスの、約款・SLA が、自社が提供するソフトウェア・サービスに適合するか、障害発生時の対応を含め文書化し、自社の運用規定、約款、SLA に反映させる。

対策詳細

IaaS/PaaS/SaaS（レンタルサーバー、ホスティングサービス、ストレージサービス、バックアップサービスなどを含む)、ネットワーク回線 (閉域網、専用線、VPN、CDN などを含む)、WAF やクラウド上のセキュリティサービス（メールチェックサービス、アンチウイルスサービス）などを利用する場合は、次の項目に該当する SLA の保証値、目標値を明確化し、障害時の運用規定や顧客対応を文書化し、必要に応じて顧客に提供する約款、SLA に反映する。
・性能（オンライン応答時間、トランザクション処理完了率など）
・完全性（認証、アクセスログ、不正対策など）
・可用性（サービス稼働率・ディザスタリカバリ、バックアップの復旧時点、代替手段など）
・信頼性（平均復旧時間、監視基準、障害通知時間など）
・外部サービスのセキュリティ（公的認証、アカウント管理、暗号化、物理的監視体制、パッチの適用、パターンファイルの更新など）

システムの特性に応じて、大規模災害やシステム不具合によるシステム・データの喪失、ネットワーク切断を含めたインシデント・障害発生時の対策（責任分界点、復旧方法、役割）と、補償範囲・条件について文書化する。

脅威シナリオ

使用したサービスが意図しない停止により、自社サービスが行えず、会社の信頼を損なう可能性がある。
また、停止期間が長引くことにより大きな損害を被る可能性もある。

参考文献

■SLA の考え方 - 総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/local_support/pdf/cio_text18_t_18.pdf

■情報システムに係る政府調達へのＳＬＡガイドライン
（独立行政法人情報処理推進機構、平成 16 年）
http://www.meti.go.jp/policy/it_policy/tyoutatu/sla-guideline.pdf

脅威分類 ＜事象/結果＞
運用障害

脅威分類 ＜手段＞
サービス障害による信用あるいは金銭上の損額

機密性	完全性	可用性
外部サービスからの情報漏洩	外部サービスからの不正動作	サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	単体テスト、結合テスト、適格性確認テストの必須事項として定義する、運用障害、保守について文書化	サービス単位で性能、完全性、可用性、信頼性、セキュリティの SLA の適合、障害発生時の対応の適合について文書化	
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
単体テストの実施および文書化	結合テストの実施および文書化	適格性確認テストの実施および文書化	運用障害、保守の有無の確認、対策および文書化	文書の書式・保管方法の定義、障害発生時の顧客対応ルールの文書化

No	10

対応する開発プロセス分類	方式設計

対策項目

Web サーバーの設置方法を検討する。

対策詳細

Web サーバーをファイアウォールなどを経由して公開する。

脅威シナリオ

Web サーバーを直接外部に公開し、外部との境界にファイアウォールや Web アプリケーションファイアウォール（WAF）を設置しないと、脆弱性攻撃やサービス拒否(DoS，DDoS)攻撃を招き、データ改竄・情報漏洩・システム障害などが引き起こされます。

参考文献

■Web Application Firewall （WAF）読本(IPA)
http://www.ipa.go.jp/files/000017312.pdf

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配布、踏み台）	情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する	Web サーバー設置方法の設計および文書化	Web サーバーへの攻撃を防ぐ設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
Web サーバーへの攻撃による単体テストの実施および文書化	Web サーバーへの攻撃よる結合テストの実施の実施および文書化	Web サーバーへの攻撃によるテストの実施および文書化	Web サーバーへの攻撃による運用障害、データ改竄、情報漏洩、不正プログラム配布、サーバー乗っ取り有無の確認、対策および文書化	文書の書式・保管方法の定義

No	11

対応する開発プロセス分類	方式設計

対策項目

個人情報を扱うWebアプリケーションへの攻撃に対してWebアプリケーションファイアウォール(WAF)を実装する。

対策詳細

大規模なWebシステムや個人情報、クレジットカード情報などを扱うWebアプリケーションに対するパラメータ改竄などの攻撃に対する防御として、Webアプリケーションファイアーウォール（WAF）を実装する。
※実装の種類の選択（商用/非商用、アプライアンス/ソフトウェア/サービス）に当たっては、ソフトウェア製品の方式設計や要件を考慮するのが望ましい。
※WAFの導入は多重防御の一つの手段として考慮するのが望ましい。

脅威シナリオ

大規模なWebシステムシステムなどでは、メンテナンスが広範囲にわたり、
脆弱性のテストが不十分な受け入れが発生したり、
脆弱性情報の入手から対応を実装するまでに時間がかかる場合がある。
WAFなどの適切な脆弱性対処・検知システムを実装していないと、
対応期間中にパラメータの書き換え攻撃などによる情報漏洩やサイトの改竄といった障害が発生する恐れがある。

参考文献

■Web Application Firewall （WAF）読本（IPA）
http://www.ipa.go.jp/files/000017312.pdf

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	方式設計の厳守事項として定義する。適格性確認テストの必須事項として定義する	想定されるリスク、保守・運用体制に基づきシステムを選定する	
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
	ソフトウェアコンポーネントの脆弱性情報をもとに回避などの性能を評価し、文書化する	ソフトウェアコンポーネントの脆弱性情報をもとに回避などの性能を評価し、文書化する	脆弱性情報に基づく攻撃回避、検知などの文書化。ソフトウェアコンポーネントレベルでの脆弱性是正の評価、文書化をする	攻撃検知、回避などの傾向、統計処理および開発者への情報共有と文書化

No	12

対応する開発プロセス分類	方式設計

対策項目

プログラムやスクリプトによるクライアントからの自動データ投入や自動操作を防止する。

対策詳細

入力や操作を自動化するプログラム(スクリプト)による短時間・大量のデータ投入（記事の投稿、会員登録など）を防止する。
例としては、プログラムやスクリプトには解析が困難な画像（キャプチャ）などに記載されたデータを入力必須とする、データ投入を受けつける間隔に制限を設ける、などがある。

脅威シナリオ

会員登録や記事投稿を自動で行うスクリプトに対策を講じておかないと、短時間・大量のデータ投入を許してしまい、応答速度の低下やサービスの停止、システムダウンなどの障害が発生する。

参考文献

■ウェブサイトにキャプチャを導入する方法【reCAPTCHA の使い方】(Syncer)
https://syncer.jp/how-to-introduction-recaptcha

■reCAPTCHA: Easy on Humans, Hard on Bot
https://www.google.com/recaptcha/intro/index.html

脅威分類 ＜事象/結果＞
運用障害

脅威分類 ＜手段＞
サービス妨害（リソース消費）攻撃

機密性	完全性	可用性
–	–	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する 適格性確認テストの必須事項として定義する	自動化攻撃を防ぐ設計の実施および文書化	自動化攻撃を防ぐ設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
自動化攻撃による単体テストの実施および文書化	自動化攻撃による結合テストの実施および文書化	自動化攻撃によるテストの実施および文書化	自動反復プログラムによる不正行為による運用障害、踏み台化有無の確認、対策および文書化	文書の書式・保管方法の定義

No	13

対応する開発プロセス分類	方式設計

対策項目

障害のログを取得する。

対策詳細

障害ログを取得、保管する。ログ取得の対象範囲はソフトウェア製品(システム、サービス)の規模によるが、①ソフトウェア製品を構成する全サーバー(プロセス)、②①が動作するホストコンピューター、③システムを構成する全ネットワーク機器である。
ここで障害ログとは、エラーログともいい、ホストコンピューター(OS)、デバイス制御やシステム監視などの常駐プロセス、サーバーアプリケーション、ミドルウェアなどが、ハードウェア障害やソフトウェア障害が発生した際に、発生日時や障害事象の内容を記録したデータを指す。

脅威シナリオ

障害ログの取得を怠ると、バッファーオーバーフロー攻撃による例外発生や、監視プロセスの障害発生などが、検知できないか検知が遅れてしまい、顧客のシステムの改竄、踏み台による処理速度の低下、機密情報の漏洩などの障害が発生する。

参考文献

■インフラ/ネットワークエンジニアのためのネットワーク技術＆設計入門（SB クリエイティブ）
p381 Syslog で障害を検知する

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
DDoS 攻撃 サービス妨害攻撃 脆弱性攻撃 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	障害ログの対象とするイベントおよび記録内容の定義、ファイル構成など	障害ログ記録方式の設計および文書化	障害ログの記述仕様、ファイル構成
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
障害ログの単体テストおよび文書化	障害ログの結合テストおよび文書化	障害ログが適切に作成されることのテストおよび文書化	障害ログの定期チェック、保管	

No	14

対応する開発プロセス分類	方式設計

対策項目

ログに記載する情報を保護・制限する。

対策詳細

ログに認証情報や詳細なエラーメッセージなどを含むと、そのログ情報が攻撃側の手がかりとなり、運用障害や情報漏洩が発生するおそれがある。

脅威シナリオ

ログの内容には、機密情報（認証情報やアカウント情報など）、システムの内部情報（発生した障害の詳細なエラーメッセージ、エラー事象の詳細内容など）をそのまま含めないよう、ルールを策定・遵守する。
例としては、パスワードは記載しない、エラーについてはメッセージや事象をプログラム化して記載する、などが挙げられる。
※ルールの策定に当たっては、そもそもその情報をログに出力する必要があるか検討すべきである。また、実現方式を併せて検討するのが望ましい（エラーメッセージのプログラム体系の設計など）。
※ログ自体の暗号化も有効な対策と言える。

参考文献

■IPA コンピュータセキュリティログ管理ガイド（NIST SP800-92）
https://www.ipa.go.jp/files/000025363.pdf

■IPA セキュアプログラミング講座 C/C++言語編 ＞ 不測の事態対策 ＞ ログ記録による証跡確保とログ自体の漏えい対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c301.html

脅威分類 ＜事象/結果＞
運用障害 情報漏洩

脅威分類 ＜手段＞
DDoS 攻撃 サービス妨害攻撃 脆弱性攻撃 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計の厳守事項として定義する。適格性確認テストの必須事項として定義する	ログに記載する情報の定義および文書化	
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
		機密情報を扱うモジュール範囲の文書化、ログに機密情報を含まないことのテストおよび文書化		

No	15

対応する開発プロセス分類	方式設計

対策項目

ログのアクセス権限を設定する。

対策詳細

ログデータには、読み取り・書き込み・削除などの権限を適切に設定する。
適切に、とは、「本来その操作を許されるべきではない」役割ないし個人に、不用意に権限を与えないことである。

脅威シナリオ

ログのアクセス権限を適切に設定しておかないと、ログが盗聴され情報漏洩したり、ログが改竄あるいは削除され、システム侵入の痕跡が隠滅されてしまうことにより、顧客のシステムの改竄、機密情報漏洩などの障害が発生する。

参考文献

■IPA セキュアプログラミング講座 C/C++言語編 ＞ 不測の事態対策 ＞ ログ記録による証跡確保とログ自体の漏えい対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c301.html

脅威分類 ＜事象/結果＞
運用障害 情報漏洩

脅威分類 ＜手段＞
DDoS 攻撃 サービス妨害攻撃 脆弱性攻撃 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計の厳守事項として定義する。適格性確認テストの必須事項として定義する	ログのアクセス権限の定義および文書化	
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
		アクセス権設定手順の確認および文書化	監査ログの定期チェック、保管	

No	16

対応する開発プロセス分類	方式設計

対策項目

外部からのデータベースサーバーへのアクセスをできないようにする。

対策詳細

外部ネットワークからのデータベースサーバーへのアクセスを防ぐ。
具体的には、①Web サーバー／Web アプリケーションサーバーとデータベースサーバーとのホストの分離、②ネットワークの分離（データベースサーバーを、外部ネットワークからアクセスできないネットワークに設置する）、③ファイアウォールでデータベースサーバーへのアクセスを制限する、などがある。
Web サーバー／Web アプリケーションサーバーなどのプロセス情報やディレクトリー情報が漏洩しないようすることや、同サーバーが乗っ取られないようにすることも重要である。

脅威シナリオ

データベースサーバへの外部からのアクセスを防がないと、データベースサーバーに対する脆弱性攻撃やサービス拒否(DoS/DDoS)攻撃を招き、顧客のシステムの改竄、サービスの停止、システム障害などを引き起こす。

参考文献

■インフラ/ネットワークエンジニアのためのネットワーク技術＆設計入門（SB クリエイティブ）
p340 高可用性設計

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する	データベースへの攻撃を防ぐ設計の実施および文書化	データベースへの攻撃を防ぐ設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
データベースへの攻撃による単体テストの実施および文書化	データベースへの攻撃よる結合テストの実施および文書化	データベースへの攻撃によるテストの実施および文書化	データベースへの攻撃による情報漏洩 データ改竄・喪失の有無の確認、対策および文書化	文書の書式・保管方法の定義

No	17

対応する開発プロセス分類	方式設計

対策項目

監査ログを取得する。

対策詳細

監査ログを取得、保管する。ログ取得の対象範囲はソフトウェア製品(システム、サービス)の規模によるが、①ソフトウェア製品を構成する全サーバープロセス、②①が動作するホストコンピューター、③ソフトウェア製品を構成する全ネットワーク機器である。
ここで監査ログとは、ソフトウェア製品に対してユーザー・管理者・運用担当者・開発者が行なった操作やその内容、日時を記録したデータを指す。監査ログは定期的にチェックしなければ意味がない。また、削除/変更できてはいけない。

脅威シナリオ

監査ログの取得を怠ると、パスワード総当たり攻撃（ブルートフォース攻撃）の発生、不正侵入の発生、データの改竄、データの漏洩といった、不正な活動や異常事象に気づく事ができないか、発見が遅れ、顧客のシステムの改竄、踏み台による処理速度の低下、機密情報の漏洩などの障害が発生する。

参考文献

■IPA コンピュータセキュリティログ管理ガイド（NIST SP800-92）
https://www.ipa.go.jp/files/000025363.pdf

■IPA セキュアプログラミング講座 C/C++言語編 ＞ 不測の事態対策 ＞ ログ記録による証跡確保とログ自体の漏えい対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c301.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	監査ログの取得対象とする操作の種類および操作者の定義、ファイル構成など	監査ログ取得方法の設計および文書化	監査ログの記述仕様、ファイル構成
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
監査ログの単体テストおよび文書化	監査ログの結合テストおよび文書化	監査ログが適切に作成されることのテストおよび文書化	監査ログの定期チェック、保管	

No	18

対応する開発プロセス分類	方式設計

対策項目

ソフトウェア製品で扱うデータを暗号化する。

対策詳細

ソフトウェア製品内で扱うデータ（特に、個人を特定できる情報を含むデータ）を暗号化する。暗号の強度や暗号化の局面は、取り扱うデータの重要度を考慮するのが望ましい。
※暗号化の局面には、①ディスク上に保存するとき、②共有メモリなどグローバルなメモリ上に保持しているあいだ、などがある。ソフトウェア製品の設計を考慮して決めるのが望ましい。
※データの暗号化以前に、そもそもそのデータをソフトウェア製品内で保持する必要があるかどうかを検討するのが望ましい。

脅威シナリオ

個人を特定できるデータの暗号化を怠ると、その情報が盗聴され、または流出し、そこから顧客やユーザーへの障害、企業イメージの低下、信頼の失墜などが引き起こされる。

参考文献

■暗号サービス（MSDN）
https://msdn.microsoft.com/ja-jp/library/92f9ye3s(v=vs.110).aspx

■RedHat Enterprise Linux セキュリティガイド 第3章 暗号化
https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-Security_Guide-Encryption.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄

脅威分類 ＜手段＞
中間者攻撃 盗聴による情報窃取

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	－

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
（必要に応じて）非機能要件（セキュリティポリシー）として要求する	（必要に応じて）非機能要件（セキュリティポリシー）として要求する	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など	ソフトウェアコンポーネント単位での脆弱性情報の取得、脆弱性を回避した設計および文書化	ソフトウェアコンポーネント単位での脆弱性情報の取得、脆弱性を回避した設計および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
暗号化の単体テスト、ソフトウェアコンポーネント単位での脆弱性情報の取得、脆弱性の回避および文書化	暗号化の結合テスト、脆弱性情報の取得、脆弱性の回避および文書化	暗号化のテストおよび文書化	暗号化情報への攻撃・漏洩の有無の確認、脆弱性情報の確認、対策および文書化	

No	19

対応する開発プロセス分類	方式設計

対策項目	【関連項目 No7】
パスワードをハッシュ化する。	

対策詳細

パスワード漏洩対策のためハッシュ化や入力画面での隠蔽をする。
※出力ビット長が長い SHA-2 などの暗号学的ハッシュ関数を使用する。
※パスワードだけでなく必ずソルト（salt）を加える。この場合、加えられるソルト（salt）はパスワードごとに異なることが望ましい。
※ソルト（salt） ＋ パスワードで得られたハッシュ値をもとに、再度、ハッシュ値を求めるストレッチングを一定回数繰り返す。
A＝ハッシュ関数（ソルト（salt） ＋ パスワード） →B＝ハッシュ関数（A＋ ソルト（salt）＋ パスワード）→C＝ハッシュ関数（B＋ソルト（salt）＋パスワード）
※パスワードを強固にするため、使用できる文字種を極力限定しない、また桁数は最低でも 8 桁以上が望ましい。

脅威シナリオ

①通信経路でパスワードのハッシュ化を怠ると、通信傍受や中間者攻撃によりパスワードが窃取される。
②パスワードの暗号化の強度が低いと、レインボーテーブル攻撃や総当たり攻撃（ブルートフォース攻撃）によってハッシュ値からパスワードが解析される。
③ハッシュ値をシステム上でキャッシュすると、不正侵入によってキャッシュデータが利用される。
④入力画面でパスワードの隠蔽をしないと、ショルダーハッキングなどのソーシャルエンジニアリングによりパスワードが窃取される。
いずれのケースも、なりすましによる特権昇格、情報漏洩、データの改ざん、システムの破壊を招く。

参考文献

■暗号技術入門 第 3 版（SB クリエイティブ）
p299 パスワードを元にした暗号

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
中間者攻撃 盗聴 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
暗号化の単体テスト、ソフトウェアコンポーネント単位での脆弱性情報の取得、脆弱性の回避および文書化	暗号化の結合テスト、脆弱性情報の取得、脆弱性の回避および文書化	暗号化のテストおよび文書化	暗号化情報への攻撃・漏洩の有無の確認、脆弱性情報の確認、対策および文書化	

No	20

対応する開発プロセス分類	方式設計

対策項目

暗号の取扱いを規定する。

対策詳細

暗号の利用方針（利用、保護対象、有効期間)、アルゴリズム（アルゴリズムの種別、強度、品質)、暗号鍵の配布（意図した相手への配布)、暗号鍵の管理（紛失、盗難からの保護）を定めておく。

脅威シナリオ

通信、保管したデータの盗聴、不正な閲覧、情報の改竄や消失の可能性がある。

参考文献

■経済産業省 「スマートメーター制度検討会セキュリティ検討ワーキンググループ」報告書別添「統一的なガイドラインの標準対策要件に盛り込むべき事項」
http://www.meti.go.jp/press/2015/07/20150710001/20150710001-2.pdf

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
暗号解読 中間者攻撃 盗聴 情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
	非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など	暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
暗号化方式、暗号強度、秘匿方式、暗号化方式の脆弱性情報の共有、チェック方法など	暗号化の単体テスト、ソフトウェアコンポーネント単位での脆弱性情報の取得、脆弱性の回避および文書化	暗号化の結合テスト、脆弱性情報の取得、脆弱性の回避および文書化	暗号化のテストおよび文書化	暗号化情報への攻撃・漏洩の有無の確認、脆弱性情報の確認、対策および文書化

No	21

対応する開発プロセス分類	方式設計

対策項目

十分な強度を持つパスワードを使用する。

対策詳細

システムが内部でパスワードを用いて認証する場合、十分な強度を持つパスワードを使用することが望ましい。パスワード生成ツールなどを用い、ランダムで推測しづらいパスワードを作成するとよい。

脅威シナリオ

システムがデータ管理に用いている DB にアクセスするために安易なパスワードを用いていると、攻撃者にパスワードを推測され、DB に格納されている情報が漏洩したり、データを書き換えられるおそれがある。

参考文献

■電子認証に関するガイドライン
https://www.ipa.go.jp/files/000025342.pdf

■オンライン本人認証方式の実態調査報告書
https://www.ipa.go.jp/files/000040778.pdf

脅威分類 ＜事象/結果＞
情報漏洩 データ改竄

脅威分類 ＜手段＞
ブルートフォース攻撃 辞書攻撃 レインボーテーブルによる権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	−

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する	パスワードの強度についての要求仕様文書化	
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
		パスワードの強度についてのテストおよび文書化		文書の書式・保管方法の定義

No	22

対応する開発プロセス分類	詳細設計

対策項目

書式文字列攻撃を対策する。

対策詳細

書式文字列攻撃されると、外部から不正不正スクリプトを送り込まれ、サーバーが乗っ取られたり、サービス停止を招いたりする。
※%n 書式の使用を禁止する。
※厳密な入力検査を実施する。可能であれば、ASLR（アドレス空間レイアウトのランダム化)、データ領域でのプログラム実行防止機能を利用する。
※C11 仕様を利用する。併せて、C11 での asprintf, vasprintf、syslog, vsyslog 関数のコーディング規約と、コンパイルオプション（書式引数の警告など）の利用を規定し、実施する。

脅威シナリオ

書式文字列攻撃の対策を怠ると、入力された文字列に不正プログラムを含められ、メモリ内のデータを出力させたり、任意のアドレスにデータを書き込まれるおそれがある。これによって ID/パスワードの漏洩を招き、サーバーの乗っ取りや、情報の漏洩が発生する。また、データ、プログラムの改竄による、運用障害、不正プログラムの実行を招く。

参考文献

■IPA セキュアプログラミング講座 ＞ C/C++言語編 ＞ 著名な脆弱性対策 ＞ フォーマット文字列攻撃対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c906.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
書式文字列攻撃による権限昇格 データ改竄

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		書式文字列攻撃が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
書式文字列攻撃の単体テストおよび文書化	書式文字列攻撃の結合テストおよび文書化	書式文字列攻撃のテストおよび文書化	書式文字列攻撃、情報漏洩や運用障害などの有無の確認	文書の書式・保管方法の定義

No	23

対応する開発プロセス分類	詳細設計

対策項目

バッファーオーバーフロー攻撃を対策する。

対策詳細

バッファーオーバーフロー攻撃を受けると、入力データとして送り込まれた任意の機械語命令列を実行されるおそれがある。入力データを受け取る際には範囲外のメモリーを書き換えないように上限文字数のチェックを実施する。また CPU のデータ実行防止機能などを利用し攻撃を回避する。類似の攻撃として整数オーバーフロー攻撃がある。

脅威シナリオ

バッファーオーバーフロー攻撃への対策を怠ると、書式文字列攻撃と同様に、入力に不正プログラムを含められ、メモリー内のデータを出力させたり、任意のアドレスにデータを書き込まれるおそれがある。その結果の脅威も書式文字列攻撃と同様である。

参考文献

■IPA セキュアプログラミング講座 ＞ C/C++言語編 ＞ 著名な脆弱性対策 ＞ バッファオーバーフロー
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c901.html

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄 運用障害	バッファーオーバーフロー攻撃による権限昇格 データ改竄

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		バッファーオーバーフロー攻撃が不可能な設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
バッファーオーバーフロー攻撃の単体テストおよび文書化	バッファーオーバーフロー攻撃の結合テストおよび文書化	バッファーオーバーフロー攻撃のテストおよび文書化	バッファーオーバーフロー攻撃、情報漏洩や運用障害などの有無の確認	文書の書式・保管方法の定義

No	24

対応する開発プロセス分類	詳細設計

対策項目

シンボリックリンク攻撃を対策する。

対策詳細

シンボリックリンク攻撃を受けると、アプリケーションが読み書きする先のファイルをすり替えられてしまう。重要なファイルを読み書きする際はシンボリックリンクでないことを確認する。レースコンディションによるチェックのすり抜けにも注意する。

脅威シナリオ

シンボリックリンク攻撃への対策を怠ると、読み出すデータをすり替えられたり、書き出すデータが漏洩したりするおそれがある。これによりデータの改竄、運用障害、情報の漏洩が発生する。

参考文献

■IPA セキュアプログラミング講座 ＞ C/C++言語編 ＞ ファイル対策 ＞ シンボリックリンク攻撃対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c802.html

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 データ改竄 運用障害	シンボリックリンク攻撃による権限昇格 データ改竄

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		シンボリックリンク攻撃が不可能な設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
シンボリックリンク攻撃の単体テストおよび文書化	シンボリックリンク攻撃の結合テストおよび文書化	シンボリックリンク攻撃のテストおよび文書化	シンボリックリンク攻撃、情報漏洩や運用障害などの有無の確認	文書の書式・保管方法の定義

No	25

対応する開発プロセス分類	詳細設計

対策項目

不正な入力値による攻撃を対策する。(SQL インジェクションなど)

対策詳細

入力値をチェックしないで SQL 文の一部として用いると、意図しない SQL 文を紛れ込まされるおそれがある。ネットワークを通じて得た入力値やファイル、環境変数を使用する場合は、入力値の正当性を確認し、特殊な意味を持つ文字はエスケープする。同種の攻撃としてメールヘッダーインジェクション、HTTP ヘッダーインジェクションなどがある。

脅威シナリオ

SQL インジェクションへの対策を怠ると、入力値に紛れてデータを削除したり更新したりする SQL 文を送り込まれるおそれがある。これにより、情報漏洩、システム破壊などが発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p119 SQL 呼び出しに伴う脆弱性 （PDF エラーメッセージからの情報漏えい）

■HTTP の教科書（翔泳社）
p264 SQL インジェクション

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄	SQL インジェクションによる権限昇格 データ改竄

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		SQL インジェクションが不可能な設計の実施および文書化
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
SQL インジェクションの単体テストおよび文書化	SQL インジェクションの結合テストおよび文書化	SQL インジェクションのテストおよび文書化		文書の書式・保管方法の定義

No	26

対応する開発プロセス分類	詳細設計

対策項目

適切なセッション管理

対策詳細

・推測されにくいセッション ID を使用する。
・URL にセッション ID を埋め込まない。
・セッションフィクセーション対策する。
・セキュアな属性を付与する。

脅威シナリオ

セッション管理が適切でないとセッション ID が漏洩したり、セッション ID を強制的に使わされたりすることにより、不正にユーザーになりすまされ、情報漏洩や、改竄などの障害にあう可能性がある。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p160 推測可能なセッション ID
p164 URL 埋め込みのセッション ID
p171 セッション ID の固定化

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄	セッション乗っ取りによる権限昇格 データ改竄

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	−

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する	セッション ID の生成方法を自作しない方式を検討する	推測されないセッション ID を生成する設計の実施および文書化
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
		セッションの複雑性、URL からの漏えい、セッション固定化攻撃の確認		文書の書式・保管方法の定義

No	27

対応する開発プロセス分類	詳細設計

対策項目

サーバーサイドインクルード（SSI）インジェクションを対策する。

対策詳細

サーバーサイドインクルード（SSI）インジェクション攻撃を受けると、OS コマンドを実行され、パスワードの表示やフィッシング詐欺サイトへの誘導のおそれがある。
※SSI 機能が不要であれば、SSI 機能を無効化する。SSI の記述が含まれる場合はエラーとする。
※SSI で利用可能な機能を極力限定し、入力内容をチェックする。併せて SSI から CGI を呼び出さないように IncludesNOEXEC を有効にする。
※Indexes と FollowSymLinks の有効・無効をセキュリティ面から検討し、使用方法を決定・文書化する。

脅威シナリオ

サーバーサイドインクルード（SSI）インジェクション対策を怠ると、コマンドの不正実行によりパスワードが抜き取られ、Web サーバーが乗っ取られたり、アドレスが書き換えられて別サイトに誘導されたり、公開されていないコンテンツが読み取られるなどの情報漏洩が発生する可能性がある。
また誘導によりフィッシング詐欺や不正プログラムの配布が行われる場合もある。

参考文献

■インジェクション攻撃 OS コマンドインジェクション （ThinkIT）
https://thinkit.co.jp/cert/tech/7/5/4.htm

■SSI インジェクション（Web Application Security Consortium:脅威の分類）
http://projects.webappsec.org/f/WASC_TC-1.0.jpn.pdf

■攻撃者が”嫌う”セキュリティ対策とは何か？（yohgaki's blog）
http://blog.ohgaki.net/software-defense-attacker-hates

■安全な Web アプリケーションの作り方 （SB クリエイティブ）
p68 Web アプリケーションの機能と脆弱性の対応

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
サーバーサイドインクルード（SSI）インジェクションによる権限昇格、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		SSI インジェクション攻撃が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
SSI インジェクション攻撃の単体テストおよび文書化	SSI インジェクション攻撃の結合テストおよび文書化	SSI インジェクション攻撃のテストおよび文書化	SSI インジェクション攻撃、情報漏洩などの有無の確認	文書の書式・保管方法の定義

No	28

対応する開発プロセス分類	詳細設計

対策項目

コマンドインジェクション実行による脆弱性を対策する。

対策詳細

コマンドインジェクションを実行されると、Web サイトからの情報漏洩、改竄などのおそれがある。コマンドインジェクションの代表的なものとしては、OS コマンドインジェクション、Xpath インジェクション、LDAP インジェクションなどがある。いずれも管理者アカウントとの漏洩やバックドア設定のおそれがある。
※入力データの検査を厳重にする。
※リダイレクトやパイプなど複数コマンドを実現する記号が含まれないようにコーディング規約を定め実施する。
※XPath、LDAP の文法において全検索となるような条件を検討し、コーディング規約を定め実施する。

脅威シナリオ

コマンドインジェクションにより脆弱性をついた攻撃をされると、脆弱性の種類に応じ、運用障害・改竄（データ）・情報漏洩・改竄（システム）・消失（データ）・不正プログラム配布・踏み台・サーバー乗っ取りが可能となる。

参考文献

■インジェクション攻撃 OS コマンドインジェクション （ThinkIT）
https://thinkit.co.jp/cert/tech/7/5/4.htm

■SSI インジェクション（Web Application Security Consortium:脅威の分類）
http://projects.webappsec.org/f/WASC_TC-1.0.jpn.pdf

■攻撃者が”嫌う”セキュリティ対策とは何か？（yohgaki's blog）
http://blog.ohgaki.net/software-defense-attacker-hates

■安全な Web アプリケーションの作り方 （SB クリエイティブ）
p68 Web アプリケーションの機能と脆弱性の対応

■IPA セキュアプログラミング講座 ＞ Web アプリケーション編 ＞ 入力対策 ＞ コマンド注入攻撃対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台） 不正利用（ストレージ、CPU）

脅威分類 ＜手段＞
コマンドインジェクションによる権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		コマンドインジェクション攻撃が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
コマンドインジェクション攻撃の単体テストおよび文書化	コマンドインジェクション攻撃の結合テストおよび文書化	コマンドインジェクション攻撃のテストおよび文書化	コマンド インジェクション攻撃、運用障害や情報漏洩などの有無の確認	文書の書式・保管方法の定義

No	29

対応する開発プロセス分類	詳細設計

対策項目

Web サーバー上のアプリケーションが特定されるのを防止する。

対策詳細

Web サーバー上のアプリケーションが特定されると、種類やバージョン情報から有効な攻撃方法が特定されるおそれがある。
※最新の脆弱性対策を施す。
※組み込みの管理者アカウントの ID/パスワードを複雑かつ長いものに変更する。組み込みの管理者アカウントは無効にする。
※デフォルトで開放されるポート番号、出力されるエラーメッセージ・表示画面を変更し、種類、バージョンが特定されないようにする。
※デフォルトのゲストアカウントを無効化する。システムを利用するユーザー権限を最小限に設定する。
※デフォルトのファイアウォールの設定を見直し、必要最小限のポートのみ利用可能とする。
※デフォルトのミドルウェア、アプリケーションのオプション設定を見直し、必要最小限に設定する。
※OS、ミドルウェアごとにコーディング・テスト環境のオプション設定、セキュリティ設定、リリース時のセキュリティ設定を規定し実施する。特にテスト環境において、インターネットへ接続する場合の権限管理を厳重にするよう規約化する。

脅威シナリオ

Web サイト上で利用されているアプリケーションや、そのバージョン情報が特定されると、既知の脆弱性攻撃が可能となる。また、既知の組み込みアカウントや開放されているポート、実行可能なコマンドなどが推測され、これらを利用した攻撃を受ける。脆弱性が残存していた場合、また、管理者アカウントが乗っ取られた場合、情報漏洩、改竄、システム破壊、不正プログラム配布、外部攻撃への踏み台などのおそれがある。

参考文献

■RFC 2616　14.38 Server
Note: Revealing the specific software version of the server might allow the server machine to become more vulnerable to attacks against software that is known to contain security holes. Server implementors are encouraged to make this field a configurable option.

注意: サーバのソフトウェアバージョンを明らかにする事で、セキュリティホールを持っている事がわかっているソフトウェアを使うサーバのマシンは攻撃を受けやすくなるかもしれない。サーバの開発者は、このフィールドをオプションとして設定を変更できるようにする事が推奨される。
http://www.spencernetwork.org/reference/rfc2616-ja-HTTP1.1.txt

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p118 エラーメッセージからの情報漏えい

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台） 不正利用（ストレージ、CPU）

脅威分類 ＜手段＞
脆弱性攻撃による権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
			Web サーバー上のアプリケーション情報漏洩の有無の確認、対策および文書化	文書の書式・保管方法の定義

No	30

対応する開発プロセス分類	詳細設計

対策項目

認証システムへの不正なアクセスを防止する。

対策詳細

認証システムを適切に設定し、辞書攻撃や総当たり攻撃（ブルートフォース攻撃）の防御をしないと、情報の改竄や漏洩などのおそれがある。
※パスワードで利用できる文字種と桁数を極力制限せず、パスワードを強固にする。
※一定回数ログイン失敗した場合は、既定時間のロックアウトを行い、時間当たりの試行回数を制限する。
※ロックアウトを行った場合、不正な試行と思われる動作があった場合は、ユーザーに注意喚起の連絡を実施する。
※システムの重要性、情報漏洩の重大性を考慮して、IP アドレス制限、端末認証、二経路認証、多要素認証の導入を実施する。
※認証システムの標準規約を制定し、実施する。

脅威シナリオ

パスワード桁数や使用文字種による制限をかけないと、簡単なパスワードの設定を許し、辞書攻撃や総当たり攻撃により認証が破られ、なりすましによる情報漏洩、改竄が発生する。ログイン失敗時の再試行に回数制限や待ち時間を設けないと、これらの攻撃がさらに容易となる。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p313 パスワードに関するアプリケーション要件

■本当は怖いパスワードの話（@IT）
http://www.atmarkit.co.jp/ait/articles/1110/06/news154.html

■IPA NIST Special Publication 800-63. Version 1.0.2. 電子認証に関するガイドライン
https://www.ipa.go.jp/files/000025342.pdf

■オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議）
https://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf

脅威分類 ＜事象/結果＞
情報漏洩. 情報改竄 運用障害

脅威分類 ＜手段＞
ブルートフォース攻撃、辞書攻撃、レインボーテーブルによる権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。（桁数制限、文字種制限、再試行回数制限、再試行待ち時間など）		認証の強度が確保されるよう詳細設計し、文書化する
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
		認証仕様のテストおよび文書化	認証システムへの攻撃の有無の確認	

No	31

対応する開発プロセス分類	詳細設計

対策項目

攻撃者に手がかりを与えないように、エラーメッセージを修正する。

対策詳細

エラーメッセージの内容から、ソフトウェアコンポーネントや構成が判明し、そのコンポーネントの脆弱性をつく攻撃を受けるおそれがある。
※最新の脆弱性情報を基にシステムを修正し、万一、バージョンが漏洩しても重大事象とならないように対処しておく。
※適切に例外処理を実施するとともに、例外発生のメッセージを表示する場合は、システムが出力するメッセージをそのまま表示せず、独自のプログラム、メッセージを出力する。
※システムごとに、未処理の例外が発生した場合の対処をコーディング規約に定め、実施する。
※Web システムの場合、ServerSignature を Off にする。オリジナルのエラーページを用意する。

脅威シナリオ

ソフトウェアをデフォルト設定のまま使用すると、エラーメッセージからソフトウェアの種類やバージョンが特定され、そのソフトウェアの脆弱性や、既知のデフォルトアカウントなどを利用した攻撃を受けるおそれがある。

参考文献

■HTTP の教科書 （翔泳社）
ｐ283 不適切なエラーメッセージ処理

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p118 エラーメッセージからの情報漏えい

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
脆弱性攻撃による権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	メッセージ表示方法など		不適切な情報が表示されないよう詳細設計し、文書化する
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
不適切な情報が表示されないことを確認する結合テストの実施および文書化		テスト項目として実施する		

No	32

対応する開発プロセス分類	詳細設計

対策項目	【関連項目 No37】
ソフトウェアに起因する脆弱性攻撃対策。	

対策詳細

ソフトウェア製品のプログラムの記述方法に起因する脆弱性を排除する。(以下は対策例)
※属性値は引用符で囲む、<>“& は文字実体参照を用いエスケープを適切に施す。
　＜　→　<　、　“　→　"　など。
※入力値を許可するスキームを定め、それ以外の入力値を拒否する。
※マルチバイトの場合、1 バイト文字を受け付けない、SHIFT-JIS を使用しないなど、文字プログラムに起因する脆弱性対策を施す。
※特権昇格を防止するため、関連する情報は暗号化を施す。

脅威シナリオ

脆弱性攻撃の一例として SQL インジェクションについて示す。この攻撃への対策を講じないと意図しない SQL 文を実行され、これにより、アカウント情報の権限の範囲内で攻撃者が自由にシステムを扱うことができ、情報漏洩、システム破壊などが発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p119 SQL 呼び出しに伴う脆弱性

■HTTP の教科書（翔泳社）
p264 SQL インジェクション

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
脆弱性攻撃による権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		SQL インジェクション、クロスサイトスクリプティング（CSS、XSS）が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
SQL インジェクション、クロスサイトスクリプティング（CSS、XSS）の単体テストおよび文書化	SQL インジェクション、クロスサイトスクリプティング（CSS、XSS）の結合テストおよび文書化	SQL インジェクション、クロスサイトスクリプティング（CSS、XSS）のテストおよび文書化		文書の書式・保管方法の定義

No	33

対応する開発プロセス分類	詳細設計

対策項目

偽 Web サイトによるフィッシング詐欺を対策する。

対策詳細

フレームを利用している Web ページで、子フレームの URL を外部パラメーターから生成すると、フィッシングサイトへの誘導のおそれがある。
※フレームを極力使用しない。
※フレームを使用する場合は、子フレームの URL を外部パラメーターから生成しないなどをコーディング規約で定め、実施する。
※フレームが偽装されていないことをチェックする。
※HTTP レスポンスヘッダーに X-Frame-Options を適切な範囲に限定して出力する。

脅威シナリオ

フレームを使った Web サイトで子フレームの URL を偽装されると、ユーザーが別のサイトに誘導される。誘導された場合、ユーザーは正しいフレームか、偽のフレームかの判断が付きにくく、個人情報や ID/パスワードを窃取されてしまう。このため、なりすましによる情報の窃取やデータの改竄を招く。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p446 frame、iframe を使わない
p434 なりすまし対策

■知らぬ間にプライバシー情報の非公開設定を公開設定に変更されてしまうなどの「クリックジャッキング」に関するレポート
https://www.ipa.go.jp/files/000026479.pdf

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
誘導による情報窃取

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		適切なフレームの利用が可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
適切なフレームの利用が可能な設計の実施および文書化	適切なフレームの利用が可能な設計の実施および文書化	適切なフレームの利用が可能な設計の実施および文書化		文書の書式・保管方法の定義

No	34

対応する開発プロセス分類	詳細設計

対策項目

クロスサイトスクリプティング（CSS、XSS)を対策する。(Web アプリケーションファイアウォール（WAF）実装)

対策詳細

クロスサイトスクリプティング(CSS、XSS)とは、動的にページを生成する Web アプリケーションに外部から埋め込んだ不正スクリプトを実行させようとする攻撃である。
Web アプリケーションを作成する場合、クロスサイトスクリプティングへの対策を講じる。
最新の Web アプリケーションファイアウォール（WAF）を用いることが望ましい。

脅威シナリオ

クロスサイトスクリプティング(CSS、XSS)：
対策を講じないと Web サイトに不正スクリプトを埋め込むことができ、ユーザーが別のサイトに誘導され、マルウェア感染の障害にあったり、クレジットカードの情報を意図しない別のサーバーに送られ、カード不正使用障害などが発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p88 クロスサイト・スクリプティング

■HTTP の教科書（翔泳社）
p258 クロスサイト・スクリプティング

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄

脅威分類 ＜手段＞
クロスサイトスクリプティング （CSS、XSS）による誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	－

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		クロスサイトスクリプティング（CSS、XSS）攻撃が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
クロスサイトスクリプティング（CSS、XSS）攻撃の単体テストおよび文書化	クロスサイトスクリプティング（CSS、XSS）攻撃の結合テストおよび文書化	クロスサイトスクリプティング（CSS、XSS）攻撃のテストおよび文書化	クロスサイトスクリプティング（CSS、XSS）攻撃による改竄（データ）、不正プログラム配布、踏み台化、情報漏洩などの有無の確認	文書の書式・保管方法の定義

No	35

対応する開発プロセス分類	詳細設計

対策項目

クロスサイトリクエストフォージェリ(CSRF、XSRF)を対策する。

対策詳細

クロスサイトリクエストフォージェリ(CSRF、XSRF)とは、フォームを受け付ける Web アプリケーションに偽造リクエストを実行させようとする攻撃である。
Web アプリケーションを作成する場合、クロスサイトリクエストフォージェリへの対策を講じる。

脅威シナリオ

クロスサイトリクエストフォージェリ(CSRF、XSRF)への対策を怠ると、偽造リクエストによって Web アプリケーションの機能が不当に利用されることにより、ユーザーが意図していない書き込みが行われたり、購入意図のない商品の決済が行われたりする。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p141 クロスサイト・リクエストフォージェリ

■IPA セキュアプログラミング講座 ＞ Web アプリケーション編 ＞ セッション対策 ＞ リクエスト強要（CSRF）対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報改竄	クロスサイトリクエストフォージェリ(CSRF、XSRF)による誘導

機密性	完全性	可用性
−	情報の改竄・消去	−

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		クロスサイトリクエストフォージェリ(CSRF、XSRF)攻撃が不可能な設計の実施および文書化
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
クロスサイトリクエストフォージェリ(CSRF、XSRF)攻撃の単体テストおよび文書化	クロスサイトリクエストフォージェリ(CSRF、XSRF)攻撃の結合テストおよび文書化	クロスサイトリクエストフォージェリ(CSRF、XSRF)攻撃のテストおよび文書化	クロスサイトリクエストフォージェリ(CSRF、XSRF)攻撃による改竄（データ)、不正プログラム配布、踏み台化、情報漏洩などの有無の確認	文書の書式・保管方法の定義

No	36

対応する開発プロセス分類	詳細設計

対策項目

パスの乗り換え（ディレクトリートラバーサル）を防止する。

対策詳細

パスの乗り換え（ディレクトリートラバーサル）とは、URL を改変してアクセスすることにより、ドキュメントルートの外部にあるデータにアクセスしようとする攻撃である。
Web アプリケーションを作成する場合、パスの乗り換えへの対策を講じる。

脅威シナリオ

パスの乗り換えへの対策を怠ると、URL の改変によってサーバー上の任意のデータが読み出されたり、あるいは実行されることにより、データが改竄されたり、情報が漏洩したりする障害が発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p232 ファイルアクセスにまつわる問題

■IPA セキュアプログラミング講座 > Web アプリケーション編 > 暴露対策 > Web サーバからのファイル流出対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
パス乗り換えによる情報窃取、権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		パスの乗り換え攻撃が不可能な設計の実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
パスの乗り換え攻撃の単体テストおよび文書化	パスの乗り換え攻撃の結合テストおよび文書化	パスの乗り換え攻撃のテストおよび文書化	パスの乗り換え攻撃による改竄（データ）、不正プログラム配布、踏み台化、情報漏洩などの有無の確認	文書の書式・保管方法の定義

No	37

対応する開発プロセス分類	詳細設計

対策項目	【関連項目 No32】
アプリケーション機能の悪用を防止する。	

対策詳細

Web アプリケーションの機能は、必要かつ正当な機能であっても、悪用されることにより第三者に障害をもたらすことがある。
Web アプリケーションを作成する場合には、機能が悪用されないように対策を講じる。

脅威シナリオ

Web アプリケーションが提供する機能が不正利用されることへの対策を講じておかないと、機能の悪用により、アクセス制御機能が乗っ取られ、あるいは回避されたりする。その結果、システムが不正利用され、データの改竄その他の障害が発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p425 Web サーバーへの攻撃経路と対策

■IPA セキュアプログラミング講座 ＞Web アプリケーション編 ＞ 開発工程と脆弱性対策
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/w002_img.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 外部攻撃（不正プログラム配付、踏み台） 運用障害

脅威分類 ＜手段＞
脆弱性攻撃

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	詳細設計での厳守事項として定義する。適格性確認テストの必須事項として定義する		可能な限り脆弱性とならない設計の実施および文書化
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
既知の脆弱性攻撃による単体テストの実施および文書化	既知の脆弱性攻撃による結合テストの実施および文書化	既知の脆弱性攻撃のテストおよび文書化	既知の脆弱性攻撃によるサーバー乗っ取り、踏み台化、データ改竄の有無の確認、対策および文書化	文書の書式・保管方法の定義

No	38

対応する開発プロセス分類	詳細設計～構築

対策項目

プログラムの静的解析・動的チェック。

対策詳細

詳細設計・構築の工程において、また適格性確認テストにおける不具合の対応時に、プログラムの静的・動的解析を行い、バッファーオーバーフローなどの脆弱性を検出し、除去する。市販のプログラム解析ツールを用いることにより、静的・動的解析を効果的に実施することができる。

脅威シナリオ

プログラムを解析し、脆弱性に対策を施しておかないと、その脆弱性をついた攻撃を仕掛けられ、さまざまな脅威が発現する。

参考文献

■Coverity Security Advisor
http://www.coverity.com/

■Fortify SCA(HP Fortify Static Code Analyzer)
https://www.fortify.com/products/hpfssc/source-code-analyzer.html

■IBM Security AppScan
http://www.ibm.com/software/products/ja/appscan

■Valgrind
http://valgrind.org/

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
脆弱性攻撃による権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	開発環境の必須事項として定義する。（製品の特定など）		プログラム解析ツールでのチェックの実施および文書化
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
プログラム解析ツールでのチェックの実施および文書化	プログラム解析ツールでのチェックの実施および文書化	プログラム解析ツールでのチェックの実施および文書化		文書の書式・保管方法の定義

No	39

対応する開発プロセス分類	詳細設計～廃棄

対策項目

自社製品にマルウェアチェックする。

対策詳細

あらかじめ定めたマイルストーンでマルウェアチェックを実施する。複数のアンチウイルスソフトで最新のパターンファイルを用いることが望ましい。

脅威シナリオ

マルウェアチェックを怠ると、ソフトウェアに混入したマルウェアにより、顧客のシステムの改竄・踏み台による処理速度の低下、システムクラッシュ、情報漏洩などの障害が発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p448 マルウェア対策

■感染チェックツールのご紹介（ACTIVE）オンラインスキャンによるクロスチェック
http://www.active.go.jp/security/flow/complete.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
不正プログラムによる情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	開発環境の必須事項として定義する。（ベンダー、製品の特定、複数ベンダーの採用など）		
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
アンチウイルスソフトでのチェックの実施および文書化	アンチウイルスソフトでのチェックの実施および文書化	アンチウイルスソフトでのチェックの実施および文書化	アンチウイルスソフトでのチェックの実施および文書化	文書の書式・保管方法の定義

No	40

対応する開発プロセス分類	結合

対策項目

自社製品の第三者開発時の受入れ（バイナリ）にセキュリティチェックする。

対策詳細

第三者にプログラムを開発委託する場合、検収時にウイルスチェックを実施する。
※対策項目にバイナリとあるので、ソースプログラムをチェックしないとわからない脆弱性のチェックは実施できないはず。ここではバイナリに不正プログラムが仕込まれていないことを確認することを主眼とした。

脅威シナリオ

検収時にウイルスチェックを実施しないと、ウイルスや不正プログラムが混入することにより、自社環境がウイルスに汚染されたり、ユーザーに不正プログラムを配布するなどの障害が発生する。

参考文献

■安全な Web アプリケーションの作り方（SB クリエイティブ）
p448 マルウェア対策

■感染チェックツールのご紹介（ACTIVE）オンラインスキャンによるクロスチェック
http://www.active.go.jp/security/flow/complete.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
不正プログラムによる情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	開発環境の必須事項として定義する。（ベンダー、製品の特定、複数ベンダーの採用、外注先での管理方法など）		
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
受け入れ時のアンチウイルスソフトでのテストの実施および文書化	受け入れ時のアンチウイルスソフトでのテストの実施および文書化	受け入れ時のアンチウイルスソフトでのテストの実施および文書化	アンチウイルスソフトでのテストの実施および文書化	文書の書式・保管方法の定義

No	41

対応する開発プロセス分類	結合

対策項目

ネットワークに起因する脆弱性

対策詳細

ネットワークプロトコル、ネットワーク設定に起因する脆弱性を排除する。(以下は対策例)
※ネットワーク機器の OS、ファームウェアのバージョンおよび脆弱性を管理する。
※通信に不必要なポートはすべて遮断する。
※SSL、TLS1.0/1.1 の利用を中止し、TLS1.2 のみとする。
※リフレクション攻撃の原因となる DNS オープンリゾルバー、NTPD Monlist など、外部(Untrust)からの問い合わせに応答しないように設定する。
※ルーター、ファイアーウォールの OS、ファームウェアのバージョンを管理し、脆弱性対策を施す。特に、危殆化している暗号スイートの設定を禁止する。
※サポートの終了したブラウザ、OS はいかなる理由でも使用を許可しない。
※ネットワーク機器のインターネット側のインターフェースに uRPF (unicast reverse path forwarding)を設定する。RFC2827 (BCP 38)。

脅威シナリオ

脆弱性攻撃の一例として SSL3.0 の脆弱性 POODLE について攻撃方法を示す。この攻撃への対策を講じないと HTTPS での暗号化された cookie や機密情報を解読することができる。これにより、ユーザーのセッションの乗っ取りや情報漏洩を招くこととなる。

参考文献

■マイクロソフト セキュリティアドバイザリ SSL 3.0 の脆弱性により、情報漏えいが起こる
https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

■redhat httpd における POODLE SSLv3.0 脆弱性問題の解決方法
https://access.redhat.com/ja/solutions/1232613

■JVNDB-2013-005768 NTP の ntpd の ntp_request.c 内の monlist 機能におけるサービス運用妨害（DoS）の脆弱性
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-005768.html

■JPNIC オープンリゾルバ(Open Resolver)に対する注意喚起
https://www.nic.ad.jp/ja/dns/openresolver/

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害

脅威分類 ＜手段＞
脆弱性攻撃による権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（運用保守）として要求する	非機能要件（運用保守）として要求する			危殆化している暗号、暗号スイートの排除設計の実施および文書化
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
	ネットワーク機器、OS のネットワークに起因する脆弱性管理、結合テストの実施および文書化	ネットワーク機器、OS のネットワークに起因する脆弱性管理、運用テストの実施および文書化	ネットワーク機器、OS のネットワークに起因する脆弱性管理および文書化	文書の書式・保管方法の定義

No	42

対応する開発プロセス分類	結合

対策項目

NTP を使いシステムの時刻を維持、同期する。

対策詳細

Network 構成に応じて、NTP を適切に設定する。
外部参照時刻サーバーは、RFC-4330 に基づきホスト名(例 ntp.nict.jp など) を指定する。
外部参照時刻サーバーの過負荷とならないよう、ポーリング間隔は指定するホストが推奨する値以下とする。
時刻差が開きすぎていないか、適宜、監査する。

脅威シナリオ

サーバー、クライアント間の時刻が同期していないと、Kerberos 認証エラーを招く。また、ログの時刻の信憑性が確保できず、攻撃や障害発生の原因究明が困難となり、対処の遅れや障害の拡大を招くこととなる。

参考文献

■国立研究開発法人情報通信研究機構 日本標準時 G
http://www2.nict.go.jp/aeri/sts/tsp/PubNtp/

■インターネットマルチフィード 時刻情報提供サービス for Public
http://www.jst.mfeed.ad.jp/service/02.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 原因解明の遅延

脅威分類 ＜手段＞
中間者攻撃による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（運用保守）として要求する	非機能要件（運用保守）として要求する			
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
	受入時の実装のテスト実施と文書化	受入時の実装のテスト実施と文書化	システム時刻同期の調査および調整と文書化。	文書の書式・保管方法の定義

No	43

対応する開発プロセス分類	結合

対策項目

OS、ミドルウェアのシステムロケールを変更しテストを行う。

対策詳細

OS、ミドルウェアのシステムロケールを変更し、また、異なるコード体系のデータを入力するなどし、システムの不具合が発生しないか確認し、必要に応じて対策を施す。状況に応じて、運用条件、保守などの文書に反映する。

脅威シナリオ

特定のカルチャやロケールに依存した実装を行っている場合、利用者がカルチャやロケールを変更した際や、異なるコード体系のデータが入力された場合、不正な処理分岐や不正な表示、データ破損、ログの障害、システムやサービスの停止を招く恐れがある。

参考文献

■難読化していない Android アプリケーションは脆弱性か　（徳丸浩の日記）
http://blog.tokumaru.org/2012/02/is-obfuscation-of-android-application.html

■ロケールの影響を受ける動作（Oracle）
https://docs.oracle.com/cd/E26924_01/html/E27144/glmde.html

■言語パックとは（Microsoft）
https://technet.microsoft.com/ja-jp/library/cc766472(v=ws.10).aspx

脅威分類 ＜事象/結果＞
運用障害

脅威分類 ＜手段＞
設定変更によるサービス停止

機密性	完全性	可用性
—	ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 （コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	アプリケーションが制御できないOS、ミドルウェアのカルチャ・ロケールの意図しない変更対応、意図しないコード体系の入力について、方式設計の厳守事項として定義する。単体、結合、適格性確認テストの必須事項として定義する	意図しない変更対応を定義する。想定されるリスク、保守・運用条件に基づき、制約事項を文書化する	
構築 （単体ビルド）	結合	適格性 確認テスト	運用	支援
カルチャ、ロケールの変更、想定と異なるコード体系のデータ入力をテストし、文書化する	カルチャ、ロケールの変更、想定と異なるコード体系のデータ入力をテストし、文書化する	カルチャ、ロケールの変更、想定と異なるコード体系のデータ入力をテストし、文書化する	構築・保守・運用条件として制約事項を文書化する	

No	44

対応する開発プロセス分類	結合

対策項目

サーバー、クライアントのセキュリティポリシーを変更しテストを実施する。

対策詳細

サーバー、クライアントの暗号方式やプロトコル、通信ポート、IP アドレス、プロキシ（Proxy）、認証方式、グループポリシー（Active Directory）などを変更し、必要に応じてソフトウェアコンポーネントのダウングレード・アップグレードを行い、システムの不具合が発生しないか確認し、必要に応じて対策を施す。状況に応じて、運用条件、保守などの文書に反映する。

脅威シナリオ

想定外のセキュリティポリシーのテストを実施しないと、プロトコルや暗号のネゴシエーションにおいて、意図しない強度の低いプロトコル・暗号での接続や、想定していない経路での通信、セキュリティが担保されない認証などが発生し、システムの改竄や情報漏洩を招く。

参考文献

■Windows, Inernet Explorer セキュリティのいま（Microsoft）
http://www.jnsa.org/seminar/pki-day/2015/data/2-2_muraki.pdf

■TLS/SSL の設定（Microsoft）
https://msdn.microsoft.com/ja-jp/library/dn786418(v=ws.11).aspx

■SSL 3.0 の脆弱性により、情報漏えいが起こる
https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

脅威分類 ＜事象/結果＞	脅威分類 ＜手段＞
情報漏洩 情報改竄 運用障害	情報窃取による権限昇格

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去 ソフトウェアの不正な動作	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	暗号スイート、通信ポート、プロキシ（Proxy）、認証方式、ポリシーの意図しない変更や接続に対して、方式設計の厳守事項として定義する。単体、結合、適格性確認テストの必須事項として定義する	意図しないセキュリティポリシー変更や接続の対応を定義する。想定されるリスク、保守・運用条件に基づき、制約事項を文書化する	意図しない変更や接続の対応（強制切断、再ネゴシエーションなど）を実装する
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
セキュリティポリシーの変更を行い接続や認証のテストをし、文書化する	セキュリティポリシーの変更を行い接続や認証のテストをし、文書化する。必要に応じて、ソフトウェアコンポーネントのアップグレード、ダウングレードを行い異なるバージョンのコンポーネント間でのテストをし、文書化する	セキュリティポリシーの変更を行い接続や認証のテストをし、文書化する。必要に応じて、ソフトウェアコンポーネントのアップグレード、ダウングレードを行い異なるバージョンのコンポーネント間でのテストをし、文書化する	構築・保守・運用条件として制約事項、危殆化のおそれや情報漏洩につながる設定、操作などを文書化する	

No	45

対応する開発プロセス分類	結合後

対策項目

自社製品のインストーラーに署名を付与する。

対策詳細

アプリケーションを配布するときには、インストーラーが改竄されていないことを保証することにより、インストーラーにデジタル署名を付与する。

脅威シナリオ

インストーラーにデジタル署名を付与しないと、改竄されたインストーラーによって不正プログラムがユーザーPC にインストールされ、情報漏洩などの障害が発生する。

参考文献

■暗号技術入門 第 3 版（SB クリエイティブ）
p241 デジタル署名の利用例

■EV プログラム署名の必要性（サイバートラスト）
https://www.cybertrust.ne.jp/digicert-ev-code-signing/about-codesigning.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
不正プログラムによる情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	適格性確認テスト合格後の必須事項として定義する		
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
		合格後、署名の付与および文書化	署名の確認および文書化	署名用証明書の運用（署名方法、証明書保管、管理方法の定義）、文書の書式・保管方法の定義

No	46

対応する開発プロセス分類	適格性確認テスト後

対策項目

自社製品の SHA1、SHA2 ハッシュ値の取得。
十分な安全性をもつハッシュ方式による確認する。

対策詳細

アプリケーションを配布するときには、正当なプログラムであることを証明するために、配布パッケージの SHA1 ハッシュ値もしくは SHA2 ハッシュ値を取得して公開する。

脅威シナリオ

ダウンロード可能なプログラムを公開する場合、SHA1 ハッシュ値もしくは SHA2 ハッシュ値をあわせて公開しておかないと、悪意のある第三者が内容を不正に書き換えたパッケージを、オリジナルを装って配布することを防ぐことができず、よって不正プログラムの流通に加担させられてしまう。

参考文献

■Availability and description of the File Checksum Integrity Verifier utility（MS）
https://support.microsoft.com/en-us/kb/841290

■CRYPTREC の暗号アルゴリズム仕様書について
http://www.cryptrec.go.jp/report/c13_kentou_giji01_5.pdf

■FIPS PUB 180-4　Secure Hash Standard　(SHS)
http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
不正プログラムによる情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する	適格性確認テスト合格後の必須事項として定義する		
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
		合格後、SHA1 ハッシュ値もしくは SHA2 ハッシュ値の取得および文書化	SHA1 ハッシュ値もしくは SHA2 ハッシュ値の取得、比較および文書化	文書の書式・保管方法の定義

No	47

対応する開発プロセス分類	運用保守

対策項目

自社製品の脆弱性情報収集と修正プログラム作成・適用する。

対策詳細

アプリケーションやサービスの脆弱性について、定期的に情報収集を行い、 最新の対策方針に従って対策準備する。

脅威シナリオ

脆弱性についての情報を更新しておかないと、脆弱性が発覚したときに修正プログラム配布などの対策をスムーズに実施できず、アプリケーションやサービスを危険な状態のまま放置することになる。

参考文献

■脆弱性対策情報データベース JVN iPedia http://jvndb.jvn.jp/

■MyJVN 脆弱性対策情報収集ツール http://jvndb.jvn.jp/apis/myjvn/sysad.html

■MyJVN API とは http://jvndb.jvn.jp/apis/index.html

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
脆弱性攻撃による情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア要件定義	方式設計	詳細設計（コーディング）
非機能要件（セキュリティポリシー）として要求する	非機能要件（セキュリティポリシー）として要求する			
構築（単体ビルド）	結合	適格性確認テスト	運用	支援
			外部向けの脆弱性窓口を開設し、報告受領以後の対応プロセスを文書化	JVN などの脆弱性コーディネーションスキームに参加する

No	48

対応する開発プロセス分類	運用保守

対策項目

アプリケーションやサービスの不具合や脆弱性に対し、妥当な時間内に対策できるよう、あらかじめ保守計画を策定し、緊急時の対応についても手順を定めておく。

対策詳細

アプリケーションやサービスの不具合や脆弱性に対し、妥当な時間内に対策を講じる。
そのため、あらかじめ保守計画を策定しておく。また、緊急時の対応についても着手前に作業手順を明らかにし、作業手順に沿って実施する。作業実施後は作業履歴を文書化する。

脅威シナリオ

アプリケーションやサービスの保守計画をたてておかないと、不具合や脆弱性が放置され、攻撃により運用障害や情報漏洩などの障害が発生する。

参考文献

■IPA 「システム・リファレンス・マニュアル（ＳＲＭ)」の作成（経営目標実現のためのＩＴ課題解決へのヒント）保守・運用編
http://www.ipa.go.jp/about/jigyoseika/04fy-pro/chosa/srm/srm4.pdf
https://www.ipa.go.jp/about/jigyoseika/05fy-pro/chosa/2005-srm2.pdf

■「別表_ソフトウェアのセキュリティ」参照

脅威分類 ＜事象/結果＞
情報漏洩 情報改竄 運用障害 外部攻撃（不正プログラム配付、踏み台）

脅威分類 ＜手段＞
脆弱性攻撃による情報窃取 権限昇格 データ改竄、誘導

機密性	完全性	可用性
情報の漏洩	情報の改竄・消去	ソフトウェア、サービスの停止

ソフトウェアライフサイクルプロセス				
企画	要件定義	ソフトウェア 要件定義	方式設計	詳細設計 (コーディング)
非機能要件（運用保守）として要求する	非機能要件（運用保守）として要求する	運用時の保守計画を定義する（定期保守、緊急時の対応方法など）	適格性確認テストの必須事項として定義する	
構築 (単体ビルド)	結合	適格性 確認テスト	運用	支援
		受入時の実装のテスト実施と文書化	運用計画に沿った作業の実施と文書化	