目次

はじめに

本書の目的

本書では弊社製品で構築したシステムに関するセキュリティ対策について説明します。

一般的にセキュリティ（脆弱性）対策は次に分類されます。

各製品部分に潜むセキュリティ対策

各製品を以下のように分類します。

ミドルウェア製品

ミドルウェア製品のセキュリティ（脆弱性）対策

- OS、JDK、データベース、ブラウザなどリリースノート「システム要件」内に記載のミドルウェア

> **注意**
>
> 各ベンダーから提供される修正プログラムを必ず適用してください。

> **コラム**
>
> 「修正プログラムの適用によるintra-mart製品への影響は？」
>
> 原則、影響はないと考えられます。 脆弱性に対する修正となるため、動作仕様が変更となる事はないと考えられます。 ただし、弊社から提供するものではありませんので、修正プログラムの詳細については各ベンダー側へご確認ください。 修正プログラム適用後に問題が発生した場合は、弊社までお問合せください。

intra-mart製品（パッケージ部分）

intra-mart製品のセキュリティ（脆弱性）対策

- 製品リリース前
  IPA「安全なウェブサイトの作り方」をベースに製造
  http://www.ipa.go.jp/security/vuln/websecurity.html
  一定の水準を持ったテストの実施
- 製品リリース後
  製品リリース後、万が一、intra-mart製品に関する部分でセキュリティに関する脆弱性などが見つかった場合は、最新アップデートに対する緊急パッチ・次期アップデートにて対応します。事象に応じて、過去1年のアップデートに対するパッチ提供も検討致します。

> **注意**
>
> 弊社から提供する脆弱性修正プログラムによって、原則、動作仕様が変更になる事はありません。

弊社製品のセキュリティ（脆弱性）対応の一例

クロスサイトスクリプティング	OSコマンドインジェクション
HTTPレスポンス分割	SQLインジェクション
パラメータ改竄	強制ブラウジング
Hiddenフィールドの不正な操作	Cookieの濫用
バックドア・デバッグオプション	コンテンツ脆弱性
パス名パラメータの未チェック ／ディレクトリ・トラバーサル	CSRF （クロスサイト・リクエスト・フォージェリ）
メールヘッダ・インジェクション	HTTPヘッダ・インジェクション
セッション管理の不備	クリックジャッキング
バッファオーバーフロー	アクセス制御や認可制御の欠落

代表的な脆弱性に対するintra-martの方針（１）

- **パラメータタンパリングなどURL操作・リクエスト操作によるセキュリティ**
  intra-mart製品は、ユーザに紐付けられた権限（IM-Authz）が対象リソースへのアクセスを厳密に制限します。このため、不正なパラメータが送られた場合においても、通常は個人に割当られた情報のみが開示される仕組みです。※ただし、ユーザアプリケーション・カスタマイズアプリケーション、その他設定の漏れによるセキュリティリスクがあります。
- **クロスサイト・スクリプティング**
  通常ユーザが入力する箇所については、クロスサイト・スクリプティングを想定したサニタイジング（無害化）処理を行ったアプリケーションを作成しています。ただし、Webブラウザそのものの脆弱性に関するスクリプトなどは、対応しかねる部分があります。また、一部管理者向けの機能にて、悪意あるスクリプトが入れられてしまうリスクがあります。これらについては、アクセス権の厳密な運用によってリスク回避を行う必要があります。
- **SQLインジェクション**
  通常ユーザが入力する箇所については、SQLインジェクションを想定したサニタイジング（無害化）処理を行ったアプリケーションを作成しています。また、一部管理者向けの機能にて、悪意あるSQLが入れられてしまうリスクがあります。これらについては、アクセス権の厳密な運用によってリスク回避を行う必要があります。

代表的な脆弱性に対するintra-martの方針（２）

- **ブロークンアクセスコントロール**
  intra-mart製品は、ユーザに紐付けられた権限（IM-Authz）が対象リソースへのアクセスを厳密に制限します。このため、不正なパラメータが送られた場合においても、通常は個人に割当られた情報のみが開示される仕組みです。※ただし、ユーザアプリケーション・カスタマイズアプ

リケーション、その他設定の漏れによるセキュリティリスクがあります。

- **バッファーオーバーフロー**
  intra-mart製品は、Javaで作成されています。通常は不正なメモリ領域にアクセスさせるようなパラメータを侵入させることは困難な仕組みです。
- **セッションハイジャック・セッションポイズニング**
  セッションハイジャックについては、今現在のアーキテクチャにおいてはリスクを完全に回避することが困難です。このため、物理的なレイヤでの制御やOSでのセキュリティ強化によって、ユーザのCookieを秘匿に保っておくなどの対策が必要です。

個別に開発したアプリケーション・連携先アプリケーション

SIer開発のプログラム、連携先のERPやWebサービスのセキュリティ対策

- 弊社intra-mart製品基盤上で動作する個別に開発したアプリケーション・連携先アプリケーションについては、Sier・お客様側でセキュリティ（脆弱性）対策が別途必要です。

> **注意**
> - 製品基盤で全て担保されるものではありません。
> - 脆弱性検知ツールや、脆弱性診断サービス等のご利用をご検討ください。

> **コラム**
> 「どこまで対策を行えばよいのか？」
>
> お客様企業におけるセキュリティポリシーや、RFP（提案依頼書）に盛り込まれるセキュリティ要件、システムの用途（外部への公開有無・機密情報の取り扱いレベル・利用者の範囲）により異なります。

※以上でお困りの場合、弊社コンサルティングサービスをご利用ください。個別に開発したアプリケーション・連携先アプリケーションなど、お客様毎で最適なご提案が可能です。

サーバOS、Webサーバ等のインフラ部分の設定、管理の徹底

サーバその他、物理的なネットワークに関するセキュリティ対策
例) 暗号化通信（SSL）、VPN回線・専用回線、Firewall等のアーキテクチャ

- intra-mart製品の取り扱うセキュリティは、物理システムや通信アーキテクチャなどを除いた、アプリケーションレイヤーの一部分です。

注意

- intra-mart（製品基盤）としてのセキュリティ対策は施していますが、その上で、Firewallによるアクセス制御、SSLクライアント認証、VPN敷設、その他ウィルス対策ソフト導入などの弊社製品の範囲外については別途、対策を総じて講じる必要があります。
- インフラ等のシステム初期構築のみではなく、その後の運用も考慮したセキュリティ対策を検討する必要があります。

コラム

「どこまで対策を行えばよいのか？」

お客様企業におけるセキュリティポリシーや、RFP（提案依頼書）に盛り込まれるセキュリティ要件、システムの用途（外部への公開有無・機密情報の取り扱いレベル・利用者の範囲）により異なります。

※以上でお困りの場合は、弊社コンサルティングサービスまでご相談ください。

各製品部分に潜むセキュリティ対策

各製品を以下のように分類します。

ミドルウェア製品

ミドルウェア製品のセキュリティ（脆弱性）対策

- OS、JDK、データベース、ブラウザなどリリースノート「システム要件」内に記載のミドルウェア

> **注意**
>
> 各ベンダーから提供される修正プログラムを必ず適用してください。

> **コラム**
>
> 「修正プログラムの適用によるintra-mart製品への影響は？」
>
> 原則、影響はないと考えられます。 脆弱性に対する修正となるため、動作仕様が変更となる事はないと考えられます。 ただし、弊社から提供するものではありませんので、修正プログラムの詳細については各ベンダー側へご確認ください。 修正プログラム適用後に問題が発生した場合は、弊社までお問合せください。

intra-mart製品（パッケージ部分）

intra-mart製品のセキュリティ（脆弱性）対策

- 製品リリース前
  IPA「安全なウェブサイトの作り方」をベースに製造
  http://www.ipa.go.jp/security/vuln/websecurity.html
  一定の水準を持ったテストの実施
- 製品リリース後
  製品リリース後、万が一、intra-mart製品に関する部分でセキュリティに関する脆弱性などが見つかった場合は、最新アップデートに対する緊急パッチ・次期アップデートにて対応します。事象に応じて、過去1年のアップデートに対するパッチ提供も検討致します。

> **注意**
>
> 弊社から提供する脆弱性修正プログラムによって、原則、動作仕様が変更になる事はありません。

弊社製品のセキュリティ（脆弱性）対応の一例

クロスサイトスクリプティング	OSコマンドインジェクション

HTTPレスポンス分割	SQLインジェクション
パラメータ改竄	強制ブラウジング
Hiddenフィールドの不正な操作	Cookieの濫用
バックドア・デバッグオプション	コンテンツ脆弱性
パス名パラメータの未チェック ／ディレクトリ・トラバーサル	CSRF （クロスサイト・リクエスト・フォージェリ）
メールヘッダ・インジェクション	HTTPヘッダ・インジェクション
セッション管理の不備	クリックジャッキング
バッファオーバーフロー	アクセス制御や認可制御の欠落

代表的な脆弱性に対するintra-martの方針（１）

- **パラメータタンパリングなどURL操作・リクエスト操作によるセキュリティ**
  intra-mart製品は、ユーザに紐付けられた権限（IM-Authz）が対象リソースへのアクセスを厳密に制限します。このため、不正なパラメータが送られた場合においても、通常は個人に割当られた情報のみが開示される仕組みです。※ただし、ユーザアプリケーション・カスタマイズアプリケーション、その他設定の漏れによるセキュリティリスクがあります。
- **クロスサイト・スクリプティング**
  通常ユーザが入力する箇所については、クロスサイト・スクリプティングを想定したサニタイジング（無害化）処理を行ったアプリケーションを作成しています。ただし、Webブラウザそのものの脆弱性に関するスクリプトなどは、対応しかねる部分があります。また、一部管理者向けの機能にて、悪意あるスクリプトが入れられてしまうリスクがあります。これらについては、アクセス権の厳密な運用によってリスク回避を行う必要があります。
- **SQLインジェクション**
  通常ユーザが入力する箇所については、SQLインジェクションを想定したサニタイジング（無害化）処理を行ったアプリケーションを作成しています。また、一部管理者向けの機能にて、悪意あるSQLが入れられてしまうリスクがあります。これらについては、アクセス権の厳密な運用によってリスク回避を行う必要があります。

代表的な脆弱性に対するintra-martの方針（２）

- **ブロークンアクセスコントロール**
  intra-mart製品は、ユーザに紐付けられた権限（IM-Authz）が対象リソースへのアクセスを厳密に制限します。このため、不正なパラメータが送られた場合においても、通常は個人に割当られた情報のみが開示される仕組みです。※ただし、ユーザアプリケーション・カスタマイズアプリケーション、その他設定の漏れによるセキュリティリスクがあります。
- **バッファーオーバーフロー**
  intra-mart製品は、Javaで作成されています。通常は不正なメモリ領域にアクセスさせるようなパラメータを侵入させることは困難な仕組みです。
- **セッションハイジャック・セッションポイズニング**
  セッションハイジャックについては、今現在のアーキテクチャにおいてはリスクを完全に回避することが困難です。このため、物理的なレイヤでの制御やOSでのセキュリティ強化によって、ユーザのCookieを秘匿に保っておくなどの対策が必要です。

個別に開発したアプリケーション・連携先アプリケーション

SIer開発のプログラム、連携先のERPやWebサービスのセキュリティ対策

- 弊社intra-mart製品基盤上で動作する個別に開発したアプリケーション・連携先アプリケーションについては、Sier・お客様側でセキュリティ（脆弱性）対策が別途必要です。

> **注意**
>
> - 製品基盤で全て担保されるものではありません。
> - 脆弱性検知ツールや、脆弱性診断サービス等のご利用をご検討ください。

> **コラム**
>
> 「どこまで対策を行えばよいのか？」
>
> お客様企業におけるセキュリティポリシーや、RFP（提案依頼書）に盛り込まれるセキュリティ要件、システムの用途（外部への公開有無・機密情報の取り扱いレベル・利用者の範囲）により異なります。

※以上でお困りの場合、弊社コンサルティングサービスをご利用ください。個別に開発したアプリケーション・連携先アプリケーションなど、お客様毎で最適なご提案が可能です。

サーバOS、Webサーバ等のインフラ部分の設定、管理の徹底

サーバその他、物理的なネットワークに関するセキュリティ対策
例) 暗号化通信（SSL）、VPN回線・専用回線、Firewall等のアーキテクチャ

- intra-mart製品の取り扱うセキュリティは、物理システムや通信アーキテクチャなどを除いた、アプリケーションレイヤーの一部分です。

> **注意**
>
> - intra-mart（製品基盤）としてのセキュリティ対策は施していますが、その上で、Firewallによるアクセス制御、SSLクライアント認証、VPN敷設、その他ウィルス対策ソフト導入などの弊社製品の範囲外については別途、対策を総じて講じる必要があります。
> - インフラ等のシステム初期構築のみではなく、その後の運用も考慮したセキュリティ対策を検討する必要があります。

> **コラム**
>
> 「どこまで対策を行えばよいのか？」
>
> お客様企業におけるセキュリティポリシーや、RFP（提案依頼書）に盛り込まれるセキュリティ要件、システムの用途（外部への公開有無・機密情報の取り扱いレベル・利用者の範囲）により異なります。

※以上でお困りの場合は、弊社コンサルティングサービスまでご相談ください。