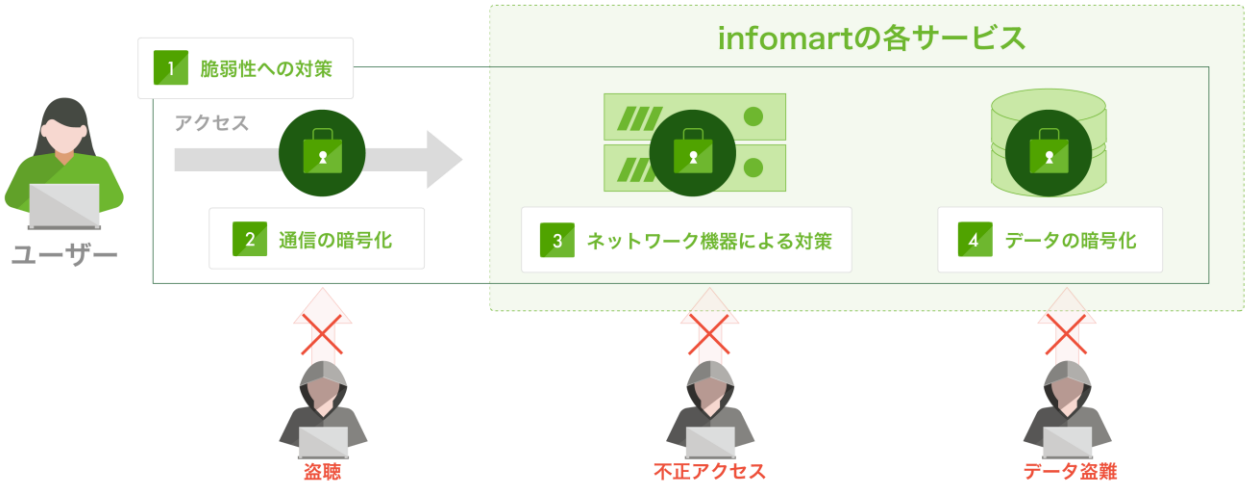
セキュリティについて

**サービスを安心・安全にご利用いただくため、
様々なセキュリティ対策を行っています。**

更新日：2025年2月12日

不正アクセス対策



1. 脆弱性への対策

infomartの各サービスでは、外部の調査機関による脆弱性診断を定期的に実施しており、新しい脆弱性の検知と対応を繰り返し行っています。

2. 通信の暗号化

ユーザとサービス間のインターネット通信は全てSSL/TLSで暗号化しています。また、Webサイトを安全にご利用いただけるよう、TLS1.1以下の暗号化通信は拒否しています。そのため、古いOSやブラウザからはアクセスができない場合があります。

3.ネットワーク機器による対策

ファイアウォール

ファイアウォールはシステムを不正なアクセスから守るための装置です。ファイアウォールにて必要最小限のポートのみを許可し、不正な探査、不正なポートスキャンに対する対策を講じています。

IPS

IPS（Intrusion Prevention System）は、侵入防止システムと呼ばれ、システムへの不正な侵入を検知し、ブロックするシステムです。

WAF

WAF（Web Application Firewall）は、Webアプリケーションの脆弱性を悪用した攻撃からWebサイトを保護するセキュリティ対策です。IPSと同様に、不正なアクセスを検知し、ブロックします。

4.データの暗号化

ストレージおよびデータベースの暗号化機能を利用し、保存される全てのデータを暗号化しています。また、パスワード等の機密データについてはシステムで暗号化してからデータ保存しています。
これらの対策により、ストレージ機器の盗難や、データへの不正アクセスが発生した場合においても、情報の漏洩を防ぎます。

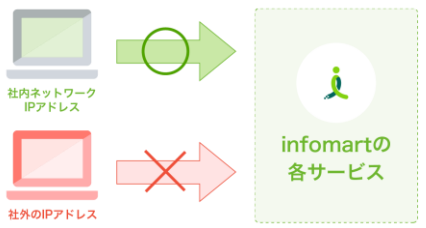
セキュリティ強化オプション

より安心に、もっと便利にBtoBプラットフォームをご利用いただけるようセキュリティ強化オプションをご用意しております。自社のセキュリティポリシーに対応したい場合などにもご活用ください。

※ご利用中のサービスにより設定できない場合があります。

不正ログイン防止

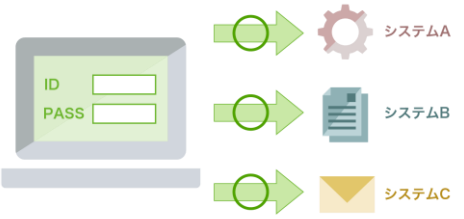
IPアドレス制限



接続元グローバルIPアドレスによる接続制限が可能です。
これによりアクセスを社内からのみに限定することが可能となり、社外からのアクセスや、攻撃者からの不正ログインを防止することができます。

ID/パスワードの一元管理

シングルサインオン



SAML、OpenIDConnectを使用したシングルサインオンに対応しています。
他サービスとID/パスワードを共有することで一元管理できるようになり、他サービスと同じセキュリティポリシーで運用することが可能になります。

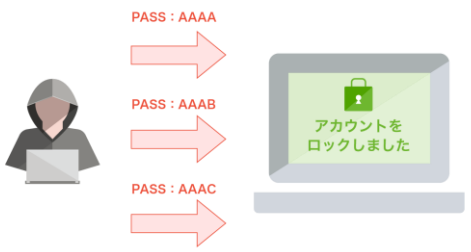
パスワード漏洩リスク軽減

パスワード有効期限

任意の日数でパスワードの有効期限を設定して、パスワードを定期的に変更することが可能です。
同じパスワードを使い続けないことで、パスワードの漏洩リスクを軽減することができます。

なりすまし防止

アカウントロック

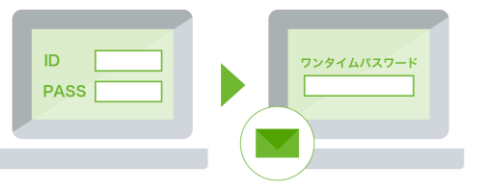


一定時間内に連続してパスワードを間違えた場合は一定時間アカウントをロックします。ロック時間やロックまでの回数については変更が可能となっています。
これにより、第三者による不正なログインを防止します。

セッションタイムアウト

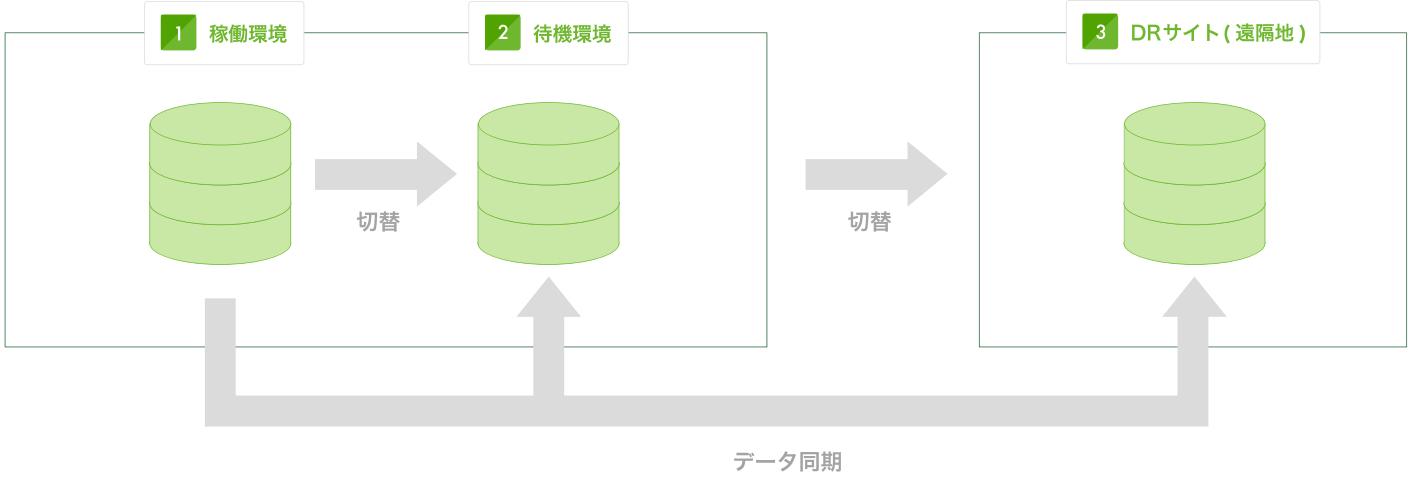
ログイン後、一定時間操作が行われなかった場合に自動ログアウトします。これにより、無関係な第三者の不正なログインを防止します。
また、セッションタイムアウトまでの時間は任意の時間に設定が可能です。

2要素認証/2段階認証



ID/パスワードでの認証後、ワンタイムパスワードによる認証を追加できます。ワンタイムパスワードはSMSやメールを利用して送信することが可能となっています。
これにより、第三者による不正なログインを防止します。

障害・災害対策



1. 稼働環境

全てのネットワーク機器やサーバ、アプリケーション、回線は冗長構成（二重化）で設計されています。この構成により、特定の機器にて故障が発生した場合でも、システムの稼働に影響しないようになっています。

2. 待機環境

稼働環境での障害発生に備え、待機環境の設置およびデータの同期を行っています。複数の機器にて同時に障害が発生し、冗長構成では対応できない状況が発生した場合には、待機環境への切り替えを行うことで、サービスの継続が可能な構成となっています。

3. DRサイト

大規模災害の発生に備え、遠隔地に災害対策環境を設置し、データの同期を行っています。震災などの大規模災害が発生した場合には、遠隔地に設置している災害対策用環境への切り替えを行うことで、サービスの継続が可能な構成となっています。

ファシリティおよび可用性対策

データセンター

BtoBプラットフォームのサーバは安全性の高いパブリッククラウドサービスで稼働し、入退室管理、監視カメラ、2要素のアクセス制御、侵入検知メカニズムなど高水準のセキュリティ対策が実施されていることを確認しています。

DDoS対策

CDN（コンテンツ・デリバリー・ネットワーク）を導入し、Webサイトのレスポンス向上を行うと同時に、DDoS攻撃への対策を行っています。

24時間監視

ハードウェア、ミドルウェア、アプリケーションなど、サービスに影響する全てのシステムについて、24時間365日監視を行っています。

定期バックアップ/遠隔地保存

毎日、定期的にバックアップを取得しており、データの確実な保全を行っています。
取得したバックアップデータは、国内遠隔地にて厳重に管理・保管しています。

第三者認証

ISMS 【ISO27001/27017】

ICMS-SR0020 / JIS Q 27001
Cloud-SR0020 / JIP-ISMS517

インフォマートでは情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO 27001」認証を取得しています。
認証番号　：ICMS-SR0020
認証規格　：JIS Q 27001:2023

また、BtoBプラットフォームの各サービスにおいて、ISMSクラウドセキュリティ認証「ISO 27017」を取得しています。
認証番号　：Cloud-SR0020
認証規格　：JIP-ISMS517-1.0

情報セキュリティ基本方針　https://corp.infomart.co.jp/security/

個人情報保護方針　https://corp.infomart.co.jp/privacy/

ISO27001/27017認証範囲　https://www.icms.co.jp/registration/2016/11/20161110-644.html

ASP・SaaS 安全・信頼性に係る情報開示認定

0190-1507

ASP・SaaS 安全・信頼性に係る情報開示認定制度により、安全・信頼性の情報開示基準を満たしているサービスに認定されております。
同制度は、総務省から公表された「ASP・SaaSの安全・信頼性に係る情報開示指針」と、「ASP・SaaSにおける情報セキュリティ対策ガイドライン」にもとづき、財団法人マルチメディア振興センターが審査・認定を行っています。

ASP・SaaS情報開示認定サイト　https://aspicjapan.org/nintei/asp-nintei/

認定公開情報　https://aspicjapan.org/nintei/0190-1507/

クラウドサービス認定プログラム

一般社団法人クラウドサービス推進機構(CSPA) の「クラウドサービス認定プログラム」に認定されています。
この制度は、クラウドを活用したIT経営の促進を目指し、中小企業の経営者が安全かつ安心して継続的に利用できるクラウドサービスを認定するプログラムになります。

一般社団法人クラウドサービス推進機構　https://smb-cloud.org/

セキュリティ資料

セキュリティホワイトペーパー

セキュリティ対策についてより詳しい情報が知りたい方は、こちらからダウンロードしてください。

https://www.infomart.co.jp/web/jp/information/securityguide/pdf/securitywhitepaper.pdf

サービスレベルチェックシート

経済産業省が発行する「クラウドサービスレベルのチェックリスト」です。

https://www.infomart.co.jp/web/jp/information/securityguide/pdf/servicelevelcheck.pdf

ASP・SaaSの安全・信頼性に係る情報開示認定資料

総務省等が定める各種ガイドラインや情報開示指針をもとにしたチェックリストです。

https://aspicjapan.org/nintei/0190-1507/

サービスレベル目標（SLO）

当社では、サービスをより安心してご利用いただくためにサービスレベル目標ガイドラインを定めています。詳しくは以下のWEBページをご参照ください。

https://www.infomart.co.jp/guideline/

商号	株式会社インフォマート（Infomart Corporation）
代表者	代表取締役社長 中島 健
事業内容	BtoB（企業間電子商取引）プラットフォームの運営
本社所在地	東京都港区海岸1-2-3 汐留芝離宮ビルディング13階
営業所	・札幌営業所（北海道札幌市中央区大通西） ・名古屋営業所（愛知県名古屋市中区錦） ・西日本営業所（大阪府大阪市西中島） ・カスタマーセンター（福岡県福岡市博多区博多駅前） ・沖縄営業所（沖縄県那覇市松尾）
設立	1998年（平成10年）2月13日
主要取引銀行	株式会社三井住友銀行（新橋法人営業部） 株式会社三菱UFJ銀行(麻布支店) 株式会社みずほ銀行(赤坂支店) 株式会社りそな銀行(虎ノ門支店)
上場市場	東京証券取引所プライム市場（証券コード2492）

本資料はWEBページでもご確認いただけます。

https://www.infomart.co.jp/security/