

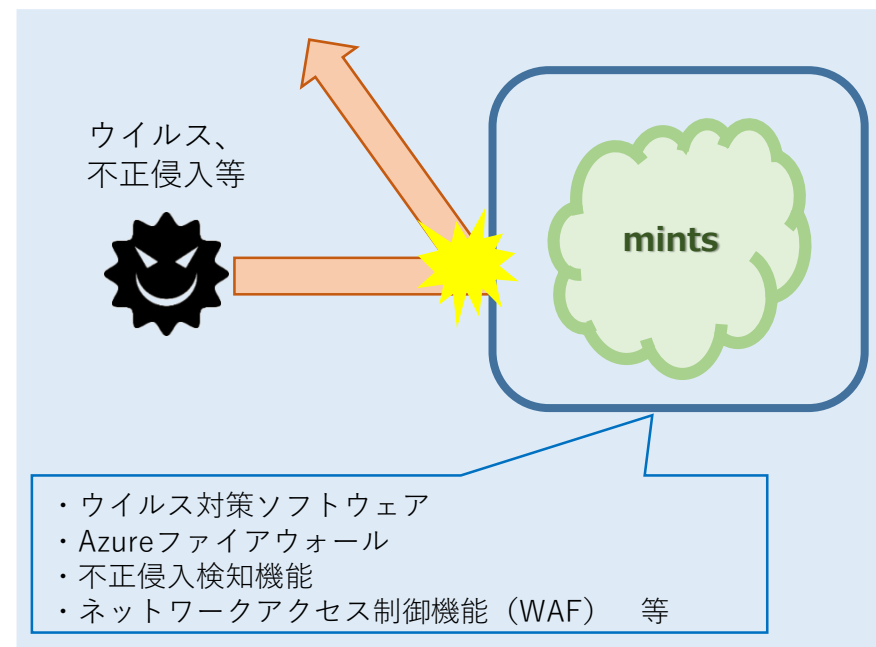
mintsセキュリティ対策の概要 ～3つのセキュリティのポイント～

令和5年2月 デジタル推進室

mintsでは、以下の高度なセキュリティ対策をとっており、安心して安全にご利用いただけます。

1 システムの安全性を確保

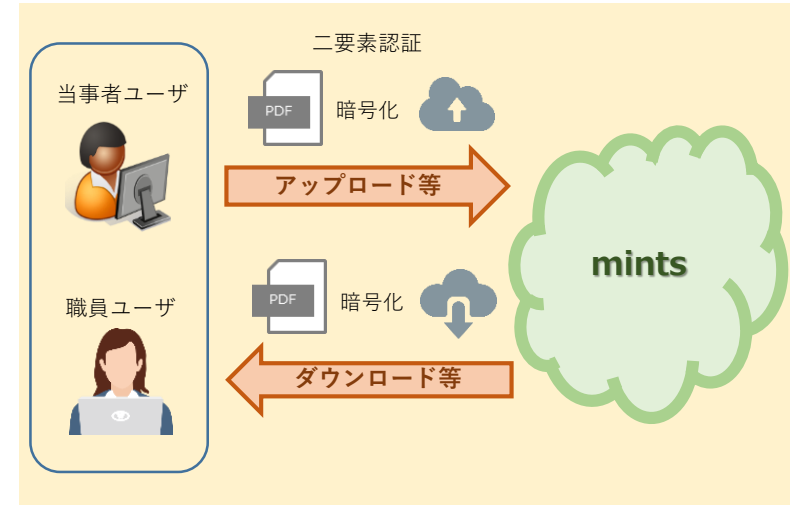
- mintsでは、政府情報システムのためのセキュリティ評価制度（ISMAP*）で安全性が評価されたクラウド・コンピューティングサービス（Microsoft Azure）*を利用しています。
- さらに、ウイルス対策ソフトウェア、Azureファイアウォール*、不正侵入検知機能*、ネットワークアクセス制御機能（WAF）*等を導入し、システムへの脅威に備えています。



*の用語の意味については3ページをご覧ください。

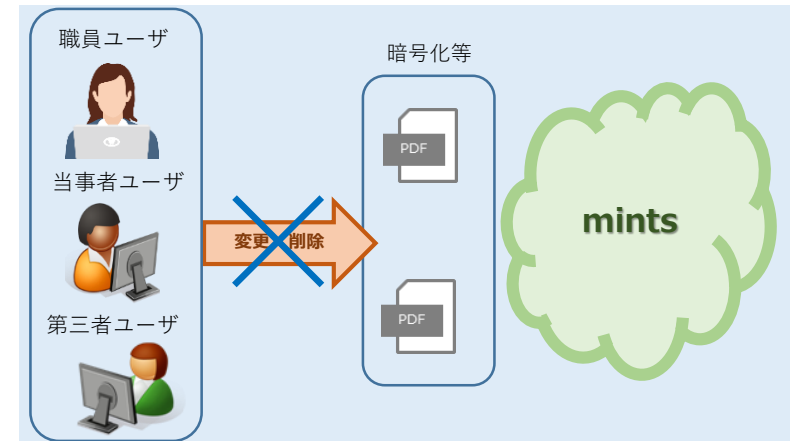
2 通信の安全性を確保

- mintsでは、第三者による盗聴や改ざんを防止するため、SSL (TLS) *暗号化技術により通信を暗号化しています。
- また、なりすまし防止として、サインイン時のパスワードは一定の複雑さ等を要求することにより安全性を向上させ、さらに、SMS認証等による二要素認証*を行っています。



3 情報の変更（改ざん）等を防止

- mintsでは、クラウド上の機能により保管データを変更（改ざん）・削除できないようにしており、また、保管データを不正に取得しても読み取れないようデータを暗号化し、情報の漏洩を防止しています。



用語集

ISMAP	ISMAP（イスマップ）とは、「Information system Security Management and Assessment Program」の略称。政府が活用するクラウドサービスのセキュリティを評価する制度である。
クラウド・コンピューティングサービス（Microsoft Azure）	インターネットを通じて、インフラやソフトウェアを提供するサービス。 Microsoft Azure（アジュール）は、Microsoft社が提供しているクラウド・コンピューティングサービス。
Azureファイアウォール	クラウド（Microsoft Azure）上に構築されたmintsに対し、不正アクセスを遮断するための機能。
不正侵入検知機能	通信を監視することでシステムへの不正なアクセスを検知し、管理者に通知する機能。 mintsでは、脆弱性攻撃等の検出と防御も行う。
ネットワークアクセス制御機能（WAF（ワフ））	WAF（Web Application Firewall）は、Webアプリケーションの脆弱性を突いた攻撃に対するセキュリティ対策の一つ。 ネットショッピングや、インターネットバンキングなど、重要なデータのやり取りが発生するWebサービスが保護対象となる。
SSL（TLS）	SSL（Secure Socket Layer）とTLS（Transport Layer Security）は、インターネット上の通信（データ）を暗号化する仕組み。 暗号化により、通信中の情報（データ）の盗聴やなりすましなどを防ぐ。
二要素認証	知識要素（ID、パスワード等）、所有要素（SMS（ショートメッセージサービス）等）、生体要素（指紋等）のうち、二つを利用した認証方法のこと。