

1. スマートフォンのセキュリティについて

1. スマートフォンのセキュリティについて 2. ソフトウェアアップデートのメリット 3. 安全なご利用に向けて

近年スマートフォンには連絡先等の個人情報だけでなく、
決済情報など多くの情報が蓄積されており、これらを標的とした悪意のある
メールや情報を外部に流出させる不正アプリ等も存在します。

例①：不審なメールやSMSから架空請求やアプリのインストールの請求

例②：個人情報(アカウント・決済情報)の流出による不正利用



上記対策としてスマートフォン・タブレットにはソフトウェアアップデートが定期的
的に提供されているので、アップデートすることでセキュリティ脆弱性の対処
を導入することができます。

2. ソフトウェアアップデートのメリット

スマートフォンを常に最新の状態にアップデートしてお使い頂くことによりセキュリティの強化だけでなく、数多くのメリットを享受できます。

① セキュリティの強化

⇒セキュリティパッチを更新することで脆弱性が対処されます。



② 固有の不具合やバグの改善

⇒端末の不具合や動作の改善が行われ、快適に利用できます。

③ 最新機能の追加/サポート対象の拡大

⇒OSのバージョンアップを行うと最新機能が追加されます。

また、OSが上がることでアプリの長期的なサポートが受けられます。

3. 安全なご利用に向けて

お客様ご自身でのセキュリティ対策

ソフトウェアアップデートの適用に加えて、お客様ご自身の使用方法やより安全なセキュリティ対策を行うことができます。

①公式マーケット以外からアプリをインストールしない

アプリには故意にウイルス機能を組み込んだ不正アプリがあり、気付かずにインストールしてしまうとウイルスに感染してしまう可能性があります。

②ウイルス対策ソフトを利用する

各携帯電話会社から提供されているウイルス対策ソフトでは、ウイルス、危険サイトなど、さまざまな脅威からスマートフォンを守る機能が利用できます。

③身に覚えのないSMSやメール、不審なサイトは開かない

悪意のある第三者によってSMSやメールにウイルスが添付されていたり、不正サイトへのアクセスを誘導されたりするおそれがあります。

④ロック設定する

端末やアプリにロックをかけておくことで紛失や盗難の際に、第三者によってすぐに悪用されるといった被害を回避することができます。また、設定の際はパスワードを使いまわさない・推測されやすいパスワードは利用しないでください。



その他のセキュリティ対策を各事業者にて掲載しておりますのでご参照下さい。

NTT Docomo : 「あんしんセキュリティ」スマホに関する脅威と対策をご紹介！ ⇒ <https://www.nttdocomo.co.jp/info/anti-phishing/>

KDDI : スマートフォンのセキュリティ対策 ⇒ <https://www.kddi.com/corporate/kddi/public/security-portal/security-sp/>

Softbank : 情報セキュリティ ⇒ <https://www.softbank.jp/corp/aboutus/governance/security/>

楽天モバイル : <https://network.mobile.rakuten.co.jp/guide/security/>