

はじめての CNSスマホ ～ご利用時の注意点～



もくじ

はじめに

本書はCNSスマホを利用する際に注意していただきたい点をまとめました。

初めて利用する方も、今まで利用してきた方も参考にしてください。

※すべての症状をまとめた訳ではありません。CNSスマホ利用には様々な症状が発生します。

※情報の閲覧やサービスの提供を受けるにあたって、法令上の義務に従った上、お客様の責任において、ご利用いただきますようお願い致します。

- | | | |
|---|----------------|------|
| 1 | スマートフォンの保護について | P.03 |
| 2 | 紛失・盗難について | P.04 |
| 3 | 緊急速報アプリについて | P.05 |
| 4 | アプリのインストールについて | P.06 |

スマートフォンの保護について



スマートフォンを利用中に落としたり、ぶついたりした時に、故障しそうで不安なんですけど、何か対策はありますか？

スマートフォンは精密機械ですので衝撃に弱い機器です。画面も割れやすい為、取り扱いには注意が必要です。

対策として、画面保護シート、カバーケースの取り付けがおすすめです。

但し、ケースを取り付けても衝撃を与えると故障することがありますので取り扱いには注意してください。



尚、CNSではカバーケース、保護シートの取り扱いは行っていませんのでご了承ください。

各機種のカバーケース、保護シートは最寄りの家電量販店、各メーカーまたは通販等を利用頂き、ご購入をお願いいたします。



紛失・盗難について



スマートフォンを紛失してしまったり、盗難にあったときはどうしたらいいですか？
知らない人に悪用されそうで怖いので、対策案をおしえてください。

スマートフォンを紛失してしまったり、盗難にあったときにそのままにしておくと、電話帳の流出、通販等の利用、写真・動画等ファイルといった情報が悪用されることとなります。
LINEやTwitterなどのSNS等を利用し友人や会社の関係者にまで被害が及ぶ可能性があります。



そこで、対策として、

1. スマホにロックをかける
2. 情報の流出を防ぐアプリの設定が有効手段となります。

CNSでは、おすすめのアプリとしてウイルスバスターマルチデバイス版【月額420円(税別)】を提供しています。
詳しくは別途お渡しの資料をご確認ください。



緊急速報アプリについて



地震や台風が起きた時にお知らせをしてくれていたけど、CNSスマホでもお知らせしてくれるのでしょうか？

Yahoo! JAPAN 防災速報のアプリをインストールすることで、緊急速報サービスを受けることができます。地域設定を3つまで登録可能、無料で利用することができます。さらに、防犯情報や熱中症情報もみることができるのでお子様のいる方にもおすすめです。



※Yahoo! JAPAN が提供するアプリとなるため、アプリケーション及びインストール先の端末の動作保証はいたしかねます。

※CNSスマホの一部端末はETWS方式には対応していません。

アプリのインストールについて



スマートフォンでアプリをインストールする時に注意する事はありますか？
ウイルスや情報流出しないか心配です。

スマートフォンのアプリを利用した、ウイルスのインストールや情報流出は残念ながら、報告されています。
こういったアプリは不正アプリと呼ばれ、感染させるように巧妙に仕掛けられています。



不正アプリインストールでウイルスに感染した時の症例とウイルスに感染しないための対策をまとめましたので、ご確認ください。

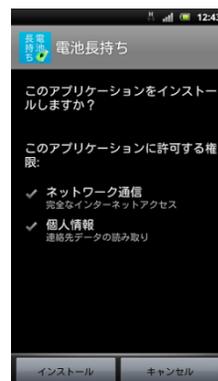
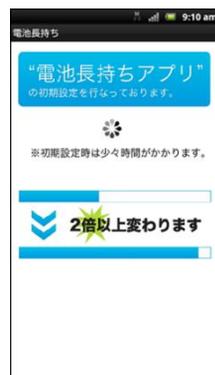


不正アプリの症例

1. 便利アプリや人気ゲームアプリに似せた情報収集不正アプリ

バッテリー節約等の便利アプリ、人気ゲームに酷似したアプリ等を利用して、電話帳情報を読み取る不正アプリです。

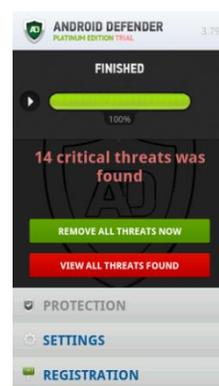
初回起動時にスマートフォン内部の情報を送信するため、初回起動後に削除を行っても送信された情報は削除されません。



2. 偽セキュリティソフトによる端末の乗っ取り

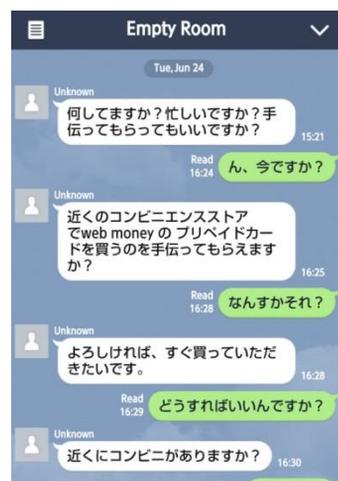
「ウイルスが見つかったので、有料版を購入してください」という表示の他、アプリストアにも登録されています。インストールすると端末がロックされ、ロック解除のための代金を要求することを目的としたものです。

代金支払い後もロック解除されない事もあります。



3. SNSアカウントの乗っ取り

一部のSNS連携アプリを認証や流出した情報を利用することによって攻撃者はアカウントを乗っ取ります。乗っ取ったアカウントで友人・知人にダイレクトメッセージを送信し、危険なURLの送信や入金依頼等を行います。



不正アプリの症例

4. 悪質な宣伝広告によりアプリ購入を強要

インターネットを閲覧中、急に画面が表示され、同時にバイブレーター機能で端末を振動させるものもあります。使用者を脅し強制的に指示に従わせることを目的とした宣伝広告です。アプリストアへ誘導等を行い、お金をだまし取る事やウイルスに感染させる事を目的としています。



上記の症例の他にも、攻撃者はスマートフォン利用者を狙っています。

感染経路としては、以下のようなものがあります。

1. スпамメールからの感染
2. SNSで紹介されたリンクからの感染
3. 検索エンジンの結果・オンライン広告からの感染
4. 公式外のサイトからダウンロードしたアプリからの感染
5. 特定サイトから自動的にダウンロードされるアプリからの感染
6. Google Play公式ストアからの感染
7. 目を離したスキに直接不正アプリをインストール

では、どのように対策を行えばいいのでしょうか？



スマートフォン不正利用の対策



不正アプリへの対策として

1. スパムメールの中に記載されているURLはタッチしないようにする
2. SNSで投稿されたメッセージの中に記載されているURLは友人・知人であっても十分注意を払う
3. Google Play公式ストア・Apple公式ストア、信頼できるサイト以外からのアプリダウンロードはしない
4. 信頼できるアプリのインストール時以外、設定画面の「提供元不明のアプリ」のインストールを許可しない
5. アプリインストール時の権限要求に注意を払う
6. アプリストアでの有料アプリ・映画・本の購入、また通販サイト利用時にクレジットカードの登録をしない。料金の支払いは、代引きやギフトカード等を利用する。
7. セキュリティソフトをインストールする
8. スクリーンロックを設定する

上記を注意しながら利用していただく事で、セキュリティレベルはかなり向上します。

また、セキュリティソフトのインストールをすることで、安心して利用していただくことができます。

CNSではウイルスバスターマルチデバイス版【月額420円(税別)】を提供しています。



CNS

株式会社ケーブルネット鈴鹿
TEL.059-388-3311 FAX.059-388-3293

0120-173734

電話受付時間 / 9:00~18:00
受付時間 / 9:30~17:30 (月~土 ※祝日を除く)

<http://www.cns-tv.co.jp>

E-mail eigyoun@cns-tv.co.jp

[ケーブルネット鈴鹿](#)

[検索](#)