McAfee
An Intel Company

モバイル セキュリティを実践するための 10 の秘訣

モバイル セキュリティを実践するための 10 の秘訣

目次

回答者の 32% が携帯端末にセキュリティ ソフトウェアは不要と考えている

はじめに

携帯端末は私たちの生活に必要不可欠なものになっています。現在、世界の人口は 70 億に達しましたが、世界中で使用されている携帯電話の台数は 40 億を超えています[1]。タブレットでさえ数百万台が利用されています。これらの携帯端末の用途は通話に限らず、写真の撮影やオンライン バンキング、音楽の再生、オンライン ショッピング、ソーシャル ネットワーキングなど多岐にわたっています。多くのユーザーが個人情報や仕事のデータを携帯端末に保存しています。携帯端末は金銭的な意味でも、心理的な面でも非常に重要な存在となりました。

スマートフォンやタブレットの紛失は重大な問題です。端末に保存されている口座番号や仕事の情報など、非常に重要な情報も失うことになります。新しい機器を購入すれば良いというものではありません。にもかかわらず、多くのユーザーが携帯端末のセキュリティを重視せず、端末を無防備な状態にしています。

コンピューターに対しては、毎日様々な脅威が発生しているため、保護の必要性が十分に認識されているようです。携帯端末も同様の脅威にさらされていますが、このことは十分に理解されていません。ある調査では、回答者の 32% が携帯端末にセキュリティ ソフトウェアは必要ないと答えています[2]。

1 http://mashable.com/2011/03/23/mobile-by-the-numbers-infographic/
2 McAfee デジタル資産調査（2011 年）

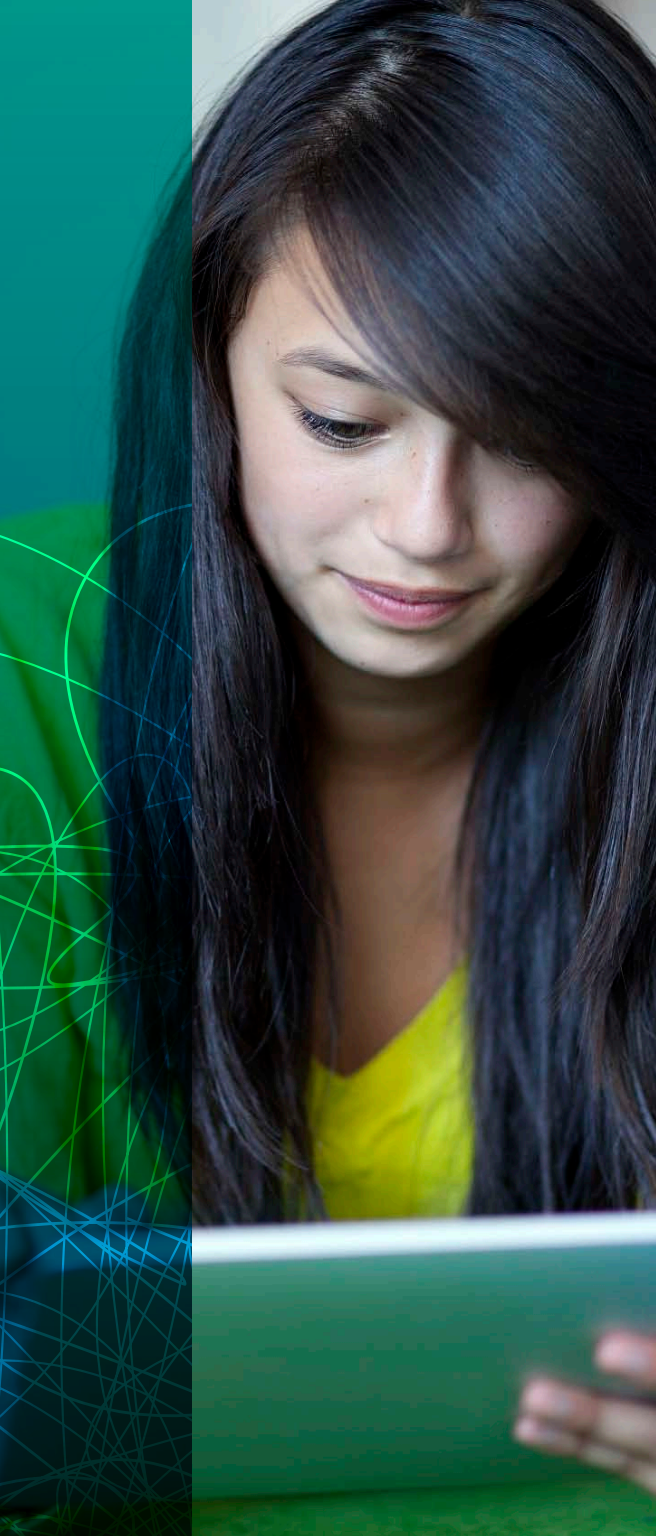
この数か月で ANDROID 端末を標的にするマルウェアが 37% も増加している

携帯端末の普及に伴い、サイバー犯罪者は携帯端末を新たな攻撃対象と見なすようになりました。Android 端末を標的にするマルウェアはこの数か月で 37% も増加しています[3]。

携帯端末を電話と同じだと考えているユーザーも少なくありませんが、実際には小型のコンピューターと同等の機能が搭載されます。しかし、携帯端末にはデスクトップ以上の脆弱性が存在します。

携帯端末のユーザーは様々なモバイルの脅威から自身を守る術を知っておく必要があります。このガイドでは、モバイル セキュリティを実践するための秘訣を紹介します。

3 McAfee 脅威レポート : 2011 年第 3 四半期



モバイルの脅威とその影響

脅威	危険性
端末の紛失または盗難	• 連絡先、カレンダー、写真など、重要な個人情報や会社情報の消失と漏えい。 • プライバシーの侵害。最悪の場合、個人情報窃盗の被害者になる。 • オンライン アカウントの不正利用 • 端末の交換費用やアカウントに対する課金（通話、携帯メールの送受信など）
フィッシング詐欺（電子メール、携帯メール、ソーシャル ネットワーキング サイトによる）	• 重要な情報（口座番号、ログイン認証情報など）の漏えい • 銀行口座からの不正な引き出し
マルウェアとスパイウェア	• 個人情報の漏えいと悪用。個人情報窃盗の被害者になる。 • 身に覚えのない使用料金の請求 • 通話やボイスメールの盗聴
QR コード	• 不正なアプリケーションのダウンロード • 個人情報の漏えいと悪用。端末が正常に動作しなくなる場合もある。
無線ネットワーク	• 安全でないネットワークへの接続。送信したデータ（パスワード、口座番号などの重要な情報）が盗まれる可能性がある。

スマートフォン ユーザーの 50% は端末をパスワードで保護していない

モバイル環境について知っておくべきデータ

携帯電話を保護する必要性を裏付けるデータをいくつか紹介しましょう。

- 携帯電話を紛失する可能性はラップトップの 15 倍。モバイル ユーザーにとって端末の紛失は最大の脅威です [4]。
- 日本では、携帯端末に保存されているデジタル資産の価値は平均で 183 万 9,395 円 [5]。デジタル メディア、仕事上の情報、個人的な情報が端末に保存されていますが、3 分の 1 以上のユーザーが端末に保護対策を講じていません。
- 2014 年までに携帯端末からのインターネット利用がデスクトップ経由を上回る [6]。これは、サイバー犯罪者や詐欺師にとって携帯端末がさらに魅力的な存在になることを意味します。
- モバイルでの商取引は 2016 年までに 310 億ドルに達する [7]。携帯端末で安全にオンライン ショッピングを行う方法を知っておかなければなりません。
- 2015 年までに携帯端末でオンライン バンキングを行うユーザーが世界中で 5 億人に達する [8]。携帯端末での安全なオンライン バンキングが最大の関心になります。
- 2010 年 6 月から 2011 年 1 月までの半年間で Android 端末を狙うモバイル マルウェアが 400% 増加 [9]。もはや安全なプラットフォームはありません。
- 回答者の 40% が財布よりも携帯端末を失くした方が被害が大きいと答えていますが [10]、多くのユーザーが携帯端末の保護を行っていません。
- 端末への不正アクセスを防ぐために端末をパスワードで保護しているスマートフォン ユーザーは 50% 未満 [11]。

4 http://www.mcafee.com/us/about/news/2011/q1/20110216-03.aspx
5 McAfee デジタル資産調査（2011 年）
6 http://mashable.com/2011/03/23/mobile-by-the-numbers-infogrpahic/
7 Forrester（2011 年）http://forrester.com/rb/Research/mobile_commerce_forecast_2011_to_2016/q/id/58616/t/2
8 Yankee Group（2011 年 6 月）
9 Juniper Networks
10 『The Rise of Smartphones and Related Security Issues』（スマートフォンの普及とセキュリティの課題）、2011 年 4 月
11 *The Wall Street Journal*、「Google Mail Hack Blamed on China」（Google Mail のハッキングは中国が攻撃元か）、2011 年 6 月

安全モバイルライフを実現するための 10 の秘訣

携帯端末は私たちの生活に不可欠なものとなり、多くのサイバー犯罪者が携帯端末に対して攻撃を仕掛けてきています。では、携帯端末を保護するために何を行えばよいのでしょうか。

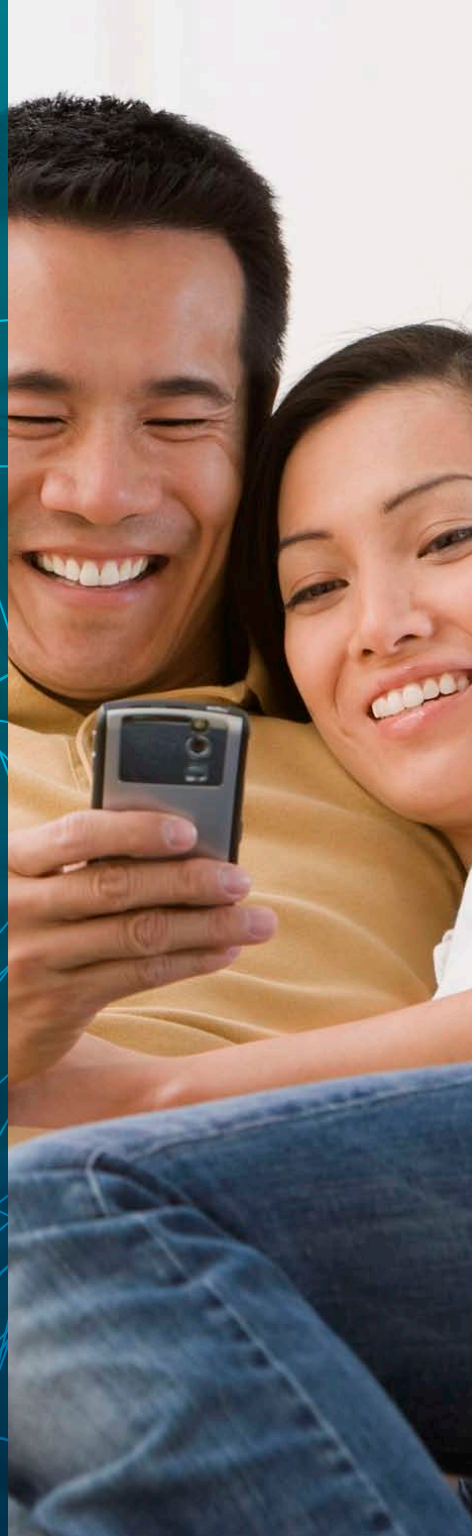
1 端末を暗証番号（PIN）またはパスワードでロックする

これにより、不正アクセスを防ぐことができます。一定の時間が経過したら端末を自動的にロックするように設定してください。

端末をパスワードで保護していても、公の場所には放置しないでください。モバイル ユーザーにとって最大の脅威は端末の紛失と盗難です。

2 信頼できる提供元以外からアプリをインストールしない

- 信頼できるストアでアプリを購入する。アプリをダウンロードする前に、アプリと発行元を十分に調べる必要があります。Android ユーザーであれば、端末のアプリケーション設定メニューで［提供元不明のアプリ］オプションの選択を解除し、マーケット以外からアプリをインストールしないようにしましょう。
- 他のユーザーのレビューと評価を確認する。安全なアプリかどうかを判断してください。
- アプリのプライバシー ポリシーを確認する。アプリがアクセスするデータの種類をチェックし、個人情報が第三者と共有されるかどうか確認してください。たとえば、ゲームアプリがアドレス帳にアクセスする場合、このようなアクセスが必要な理由について考えてください。不審な動作や好ましくない操作が実行される場合には、アプリをダウンロードしてはなりません。



3 データをバックアップする

これは比較的簡単な操作です。多くのスマートフォンやタブレットには無線でデータをバックアップする機能が搭載されています。データがなくなったり、誤って削除してしまっても、すぐに情報を携帯端末に復元できます。また、端末を紛失した場合でも、情報の復元が可能です。

4 システムを常に最新の状態にする

携帯端末の OS が更新されたら、すぐにソフトウェア更新をダウンロードして、最新のセキュリティ更新を常に使用してください。これにより、端末を常に最適な状態で使用することができます。

5 端末のハッキングを防ぐ

端末のハッキングや改ざんが行われると、端末の提供元が設定した制限が機能しなくなり、端末のセキュリティは非常に脆弱になります。端末がハッキングされると、すぐには見つからないセキュリティ ホールが作成されたり、端末に組み込まれているセキュリティ機能が回避される可能性があります。

6 オンライン バンキング サイトやショッピング サイトを閉じる場合には必ずログアウトする

- ブラウザーを終了するのではなく、サイトからログアウトする。紛失した携帯電話やタブレットからアカウントにログインされたり、端末が犯罪者の手に渡る可能性もあります。携帯端末のブラウザーやアプリにユーザー名とパスワードを保存してはなりません。
- 公共の無線接続ではオンライン バンキングやオンライン ショッピングを行わない。このようなサイトへのアクセスは、強固なセキュリティ対策が実施されているネットワークでのみ行うべきです。
- サイトの URL を再度確認する。サイトにログインしたり、重要な情報を送信する前にウェブのアドレスをもう一度確認しましょう。銀行で公式アプリを提供している場合には、アプリのダウンロードが必要になる場合もあります。

7 未使用時には無線、位置情報サービス、BLUETOOTHを無効にする

- 未使用時には無線を無効にする。接続が安全でなければ、サイバー犯罪者や窃盗者は個人情報に簡単に盗み出してしまいます。ホットスポットの使用制限も一つの方法です。自宅や職場以外では 3G または 4G のデータ接続を使用しましょう。大半の携帯電話会社は基地局と携帯端末間のトラフィックを暗号化しています。
- 位置情報サービスを使用するアプリを無効にする。携帯電話会社が端末の位置情報を保存している場合があります。このような情報が盗まれると、広告の送信に使用される可能性もあります[12]。

12 http://www.itstactical.com/digicom/privacy/data-leaks-location-based-services-and-why-you-should-be-concerned/

- 必要でない場合には Bluetooth を無効にする。端末のデフォルトの設定で他の端末との通信が有効になっている場合があります。この場合、悪意のあるユーザーが端末にアクセスしてファイルをコピーしたり、Bluetooth 経由で他の端末にアクセスする可能性があります。

8 携帯メールや電子メールで個人情報を送信しない

銀行や正規の企業からメールを受信してもすぐには信用しないでください。受信したメールに返信して個人情報を送信してはなりません。送信元の銀行や企業に直接連絡して、このようなメールを本当に送信しているかどうか確認するべきです。

携帯電話に重要な情報を保存する前に、携帯電話は紛失しやすく、盗難にあう可能性も高いことを思い出してください。端末が盗まれれば、端末に保存したパスワードや口座情報は簡単に犯罪者の手に渡ってしまいます。

9 不要なメールにあるリンクや添付ファイルをクリックしない

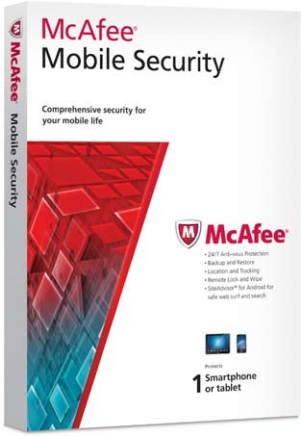
インターネットのベスト プラクティスを思い出しましょう。不要なメール（SMS と MMS）のリンクに十分に注意してください。このようなメールが届いたらすぐに削除しましょう。

短縮 URL や QR コードにも注意が必要です。危険なサイトに誘導される可能性があります。リンクに移動する前に、LongURL などの URL プレビュー サイトを利用して正規のアドレスかどうか確認してください。QR コードをスキャンする場合には、コードに埋め込まれたウェブ アドレスをプレビューできる QR リーダーを使用しましょう。また、QR コードに含まれている危険なリンクを警告するセキュリティ ソフトウェアを使用してください。

10 携帯端末用のセキュリティアプリをインストールする

既存の脅威や新たに発生する脅威に対応できるウイルス対策を携帯端末にインストールして、ソフトウェアを常に最新の状態にしてください。これにより、犯罪者やハッカーの攻撃を受けても、個人情報や端末を保護することができます。

リソース



Android、BlackBerry、Symbian **搭載のスマートフォンに対応**

モバイル セキュリティ

携帯端末に対する脅威は複雑化しています。このようなモバイル環境を保護するには McAfee Mobile Security™のように多層的な保護対策を提供するセキュリティ ソフトウェアが不可欠です。

McAfee Mobile Security の主な機能は次のとおりです。

- **ウイルス対策、スパイウェア対策、フィッシング詐欺対策を備えた完全なセキュリティ対策** — 受信メール、送信メール、携帯メール、添付ファイル、ファイルをスキャンし、不正なコードを駆除します。
- **安全な検索とオンライン ショッピング** — 携帯メール、電子メール、ソーシャル ネットワーキング サイトに含まれる不正なリンクや、ブラウザー エクスプロイト、不正な QR コードから端末とデータを保護します。
- **App Alert によるアプリの保護** — アプリがアクセスする個人データを事前に確認し、アプリを利用するかどうか判断することができます。
- **端末のロック** — 携帯端末をリモートからロックし、SIM カードを含む端末上のすべてのデータを保護し、端末とデータの悪用を防ぎます。
- **リモートからのデータの消去** — 端末上のすべてのデータ（メモリー カードのデータも含む）をリモートから消去し、プライバシーを保護します。
- **データのバックアップとリストア** — 個人情報や貴重なファイルを定期的または必要なときにバックアップできます。また、スマートフォンを紛失しても、データの消去を行う前にバックアップを行えば、新しい端末に情報をリストアすることができます。
- **位置の特定と追跡** — スマートフォンを盗まれたり、紛失しても心配はいりません。端末の現在位置を地図上に表示し、返却を求める SMS を送信したり、リモートからアラームを鳴らすこともできます。
- **通話と SMS のフィルタリング** — 迷惑メールや不要なメール、不正な電話番号を簡単にフィルタリングできます。
- **削除防止** — 犯罪者や端末を見つけた人物がマカフィーのモバイル保護対策を変更できないようにします。

McAfee Mobile Security の無料版をぜひお試しください。

要約

インターネット対応の携帯端末が爆発的に普及し、これまでには考えられなかった生産性や柔軟性が実現されています。しかし、この状況は個人情報を狙うハッカーや詐欺師にとっても非常に好ましいものとなっています。このガイドで紹介したヒントに従って保護を行うだけでなく、新たに発生する脅威に常に注意を払う必要があります。携帯端末を保護するために多くの時間や労力は必要ありません。簡単なことを実践するだけで、プライバシー、個人情報、口座情報を保護しながら便利なモバイルライフを楽しむことができます。

モバイル セキュリティの詳細については、McAfee Security Advice Center をご覧ください。

マカフィーについて

マカフィーは、インテル コーポレーション（NASDAQ: INTC）の完全子会社であり、セキュリティ・テクノロジ専業のリーディング カンパニーです。1987 年の設立以来、お客様のデジタル世界を保護するため、プロアクティブなセキュリティ ソリューションを開発し、提供しています。

マカフィーはオンラインの脅威を常時監視しています。これにより、個人のユーザーや企業は、インターネットへの接続方法や所在地に関わらず、より安全にインターネットを利用することができます。お客様の安全を確保するため、マカフィーは、新しい手法の開発に日々真摯に取り組んでいます。

http://www.mcafee.com/jp/

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

東京本社　〒 150-0043 東京都渋谷区道玄坂 1- 12- 1
渋谷マークシティウェスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480
名古屋営業所　〒 460-0002 愛知県名古屋市中区丸の内 3-20-17
中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552
西日本支店　〒 530- 0003 大阪府大阪市北区堂島 2-2-2
近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517
福岡営業所　〒 810- 0801 福岡県福岡市博多区中洲 5-3-8
アクア博多 5F
TEL 092-287-9674（代）FAX 092-287-9675