



スマートフォンへのマイナンバーカード搭載におけるデジタルセキュリティの重要性

株式会社オウルズコンサルティンググループ プリンシパル
佐藤 維亮

※2023 年 5 月 24 日付の JBpress の記事を一部変更して掲載しています。

スマートフォンユーザーを標的にしたサイバー攻撃

サイバー攻撃が飛躍的に増加している中、スマートフォンを標的にした攻撃も増加の一途を辿っている。

最近、トレンドマイクロは、大規模なサイバー犯罪組織が販売前の Android デバイスにマルウェアをプリインストールし、その数は約 890 万台にものぼると報じている。マルウェアに感染した Android スマートフォンを利用して利益を上げている「Lemon Group」の仕業だ¹。

「Lemon Group」はビッグデータ、マーケティング、広告向け事業を提供しており、マルウェアによって SMS の

¹ [「890 万台の Android デバイスにマルウェアがプリインストール、注意を」](#)、2023 年 5 月 23 日、TECH+

傍受、Facebook 関連の Cookie や WhatsApp セッションの取得、広告の挿入、サイレントインストールなどを実行でき、これにより不当に利益を得ることができるという。

さらに、Android 向けのマルウェアとして「Hook」という、感染した端末のリモートコントロールが可能となるものがある。² \$5,000/month で、ダッシュボードから感染端末をリモートコントロールできるダークサービスだ²。

スマートフォンへのマイナンバーカード機能搭載開始による期待と不安

デジタルセキュリティが益々重要となる中、2023 年 5 月 11 日には Android 向けにマイナンバーカード機能の搭載が始まった。Android にマイナンバーカードの電子証明書が格納されたことで、プラスチックのマイナンバーカードなしでマイナポータルへのログインやコンビニエンスストアでの各種証明書の交付、さらには医療機関側の対応を要するものの健康保険証としての利用などが可能となった。一層の利活用は今後に期待するところが大きい、益々活用の幅は広がっていくであろう。

一方で、例えば、上述の「Hook」マルウェアのように感染端末のリモートコントロールを受けると、第三者がマイナアプリを起動し、格納されている電子証明書を活用することで、本来であればログインできないスマートフォン所有者のマイナポータルなどにログインし、プライベートな情報を閲覧したり、詐取したりすることができてしまわないかという懸念が生じる。

直近、マイナポータルで確認できる情報として「薬剤・健診情報」や「母子健康手帳」情報などが追加された。リモートコントロールによってこれらの情報が閲覧・詐取されるリスクにも備えておかなければならない。

マイナンバーカードをめぐるトラブルとデジタルセキュリティ

マイナンバーカードの利活用はデジタル化の要であり、デジタル ID はグローバルで今後のトレンドでもある。米国では、iPhone でアリゾナ州やコロラド州、メリーランド州で運転免許証のスマートフォンへの搭載が始まった³。今後こういった動きは一層の広がりを見せるだろう。

一方で、最近、マイナンバーカードをめぐるトラブルが続いているのが現状だ。別人の医療情報を閲覧できたり、コンビニで別人の住民票を受け取ってしまったという事態が発生した。個々のトラブルの原因を追究すると、ベンダーのシステム設計の問題や健康保険組合の入力ミスによるものであったが、一見些細なミスが個人情報の流出といった大きな社内問題になりうる。将来的なサイバー攻撃などセキュリティ事案の発生につながる可能性も否定できない。また、健康保険証を廃止するに伴い、マイナンバーカードの健康保険証としての役割も重要となるが、健康保険のオンライン資格情報の誤登録が発生し、「該当資格なし」と表示される事象が生じた。「該当資格なし」と窓口で表示されてしまえば、窓口で一旦医療費全額(10割負担)をせざるを得ないという現実世界でのトラブルが発生するかもしれない。また、利活用の拡大に関して、生保協会が 22 年 12 月にマイナンバーカードやそのスマートフォン搭載に寄せる期待を調査したによれば、スマートフォンで利用できる生命保険会社のサービスの利用の可能性に 6 割の回答者が期待を寄せているが、保険会社から外部への情報ろうえいなどを懸念して利用を控える声も 4 割にのぼった。デジタル ID の活用においては、足元のデジタルセキュリティを万全に固める必要が

² [「New 'Hook' Android malware lets hackers remotely control your phone」](#)、2023 年 1 月 19 日、BLEEPINGCOMPUTER

³ [「iPhone Driver's License Feature Slow to Expand, Only Available in Three States」](#)、2023 年 3 月 6 日、MacRumors

あるだろう。

冒頭の「Lemon Group」が頒布したようなマルウェアは、一個人には防ぎようがない。さらに個人が警戒しつつも引っかけりうるものとして、情報詐取を企図したフィッシングアプリやメッセージ、身代金請求アプリなどがあり得るだろう。コロナ禍において、カナダ保健省が提供した公式の新型コロナウイルス感染症の接触確認アプリに偽装し、ユーザーを騙してアプリをインストールさせ、デバイス上のファイルを暗号化し、身代金の支払いを要求するランサムウェアが頒布された。こういった偽のアプリなどは、マイナンバーカードの利活用が拡大して行けば行くほどそのリスクが高まる。

マイナンバーカードのスマートフォン搭載で遅れを取らないために

今国会ではマイナンバーカードの番号自体の用途拡大を目的とした法改正も行われた。今後ますます、マイナンバーカードを取り巻くデジタルセキュリティの確保が重要となる。

2023年5月16日、全国消費者団体連絡会は、「今後もスマートフォンを安心して利用できるよう・・・マイナンバーカードを扱うスマートフォンのセキュリティ対策が万全なものとなるよう対策を講じる必要」があり、「サイドローディングなどスマートフォン OS のセキュリティリスクが拡大する恐れのある議論も行われていると承知していますが、政府内で緊密に連携の上、消費者をリスクに晒すことないよう、万全を期す」べき旨を関係各所に要請している。Android のマイナンバーカード搭載に加えて、iPhone も今後搭載が検討されていると報じられている。

これらの政策議論が現行のスマートフォンの OS の再設計を求めるようなことになれば、デジタルセキュリティの確保に支障が出ることで未搭載の iPhone への搭載が遅れる事態もありうるだろう。日本のデジタルセキュリティに関わる政策が矛盾しない形で慎重になされることを望みたい。

デジタルセキュリティと安全保障

近年、国家支援型のマルウェアの増加にも留意する必要が高まっている。国家主導のハッキングの主体は、北朝鮮や中国のハッカーグループやスパイウェア開発のイスラエル企業など様々だ。

成功裏に閉幕した G7 広島サミットにはウクライナのゼレンスキー大統領が来日し、必要とされる限り支援する首脳間の結束が示された。ロシア・ウクライナ戦争ではサイバー戦が重要な位置づけとなっている。デジタルセキュリティの分野においても同盟国である日米両国の一層の連携強化が望まれるだろう。

著者



株式会社オウルズコンサルティンググループ
プリンシパル
佐藤 維亮/Tadaaki, Sato

総合商社(金属資源本部所属)に新卒入社後、ローランド・ベルガー(戦略コンサルティング)、デロイト トーマツ コンサルティング、アクセンチュア、電気通信機器メーカー等を経て現職。

早稲田大学法学部、一橋大学国際公共政策大学院グローバルガバナンスコース修了。

企業向けの新規事業策定支援やデジタル戦略策定支援、中期経営計画策定支援といった事業戦略策定や組織戦略に亘る多数のプロジェクトの経験に加え、官公庁の政策立案策定プロジェクトの経験も多く担当。特にルール形成戦略立案や新市場創出関連プロジェクトに強みを持つ。

政府及び政府関連団体の技術×政策に関連するセミナー講師を複数回務めた経験を有する。

本資料は一般的な情報提供を目的とするものであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。関連する法令等の解釈を行ったものではなく、利用者が本資料を利用したことによる結果について、株式会社オウルズコンサルティンググループは一切の責任を負うものではありません。

また、書面による株式会社オウルズコンサルティンググループの事前承認なしに、第三者への配布・引用・複製を行うことはお断りしております。

株式会社オウルズコンサルティンググループ

〒106-0046 東京都港区元麻布 3-1-6

<https://www.owls-cg.com/>