

治安情報 2012 年 第 3 四半期報告書

対象地域	フランス リヨン (及びローヌアルプ州)	在リヨン出張駐在官事務所 リヨン日本人会治安情報収集チーム	
		作成日	対象期間
調査方法 新聞 サイト	プログレ紙 仏警視庁 HP	2012 年 9 月 30 日	2012 年 7 月～9 月
集計情報の流布	未	在留邦人対象に各団体及び在リヨン出張駐在官事務所ルート	
調査項目：			

報告要旨

- I. **スリの被害に遭わないための予防策**

- II. **交通事故を装った詐欺、タイヤ破り：路上・駐車場での新しい詐欺の手口**

- III. **携帯電話：ハッカーの今後のターゲット**

I. スリの被害に遭わないための予防策

大都市観光地域では、最もスリに狙われやすいのが観光客だ。「ピックポケット」とも呼ばれるこの犯罪者たちは、被害者のポケットやカバンの中にあるものをそっと盗むプロ。たいていの場合被害者はこれに気が付かない。

この手の被害は主に外国人旅行者に多く見られる。特に公共交通機関を利用して移動する際に荷物や所持品に十分な注意が足りないためだが、スリに遭いやすい場所はそれだけではない。

特定の場所では特に警戒を

公共の場で：

- ✓ 周囲の人の動き、特にグループのスリが引き起こす偽の押し合いに注意。混乱状態で旅行者の警戒心が薄れたすきを狙います。

路上で：

- ✓ ハンドバッグやカバンが開いていないことを確認。
- ✓ 上着の内ポケットなどは、できれば閉めること。
- ✓ 財布はズボンなどの後ろポケットには入れないこと。
- ✓ 買い物袋の中に財布を入れたり、買った物の上に財布を乗せたりしないこと。

公共交通機関で：

- ✓ 地下鉄やバスの乗車・下車、エスカレーターの乗り降りの際は特に持ち物に注意。スリは、この時の混雑や押し合いを利用して犯行にでることが多い。
- ✓ 切符は自動検札を通る前に準備しておき、人前で財布を開けるのを避ける。
- ✓ 駅や空港ではスーツケース・荷物等から目を離さない。
- ✓ 自動検札では、一緒に通過しようと思知らぬ者が後ろについてきたときには財布に注意。

デパート、レストラン、劇場や美術館などで：

- ✓ スリの目を引かないように、なるべく小額紙幣で支払うか、小切手またはキャッシュカードで支払う。
- ✓ レストランでは、席の後ろのテーブルにつくスリにご用心。
- ✓ 現金やカードなどの支払い手段、身分証明書やパスポートなどの書類をクロークに置いたり、コートのポケットの中に入れてままにしておかないこと。

所持品について

現金やパスポートなど：

- ✓ ハンドバッグやショルダーバッグではなく、なるべくバナナバッグタイプのものに入れて前側に向けておく。
- ✓ リュックサックやバックパックには入れないこと。

現金：

- ✓ 大金の現金を持ち歩くことは避け、なるべく小額紙幣にする。
- ✓ 1ヶ所にまとめておかず、カバン、ポケットなどに分けて入れる。
- ✓ 現金はパスポートや免許証などの身分証明書類とは分けておく。
- ✓ コートの外ポケットやズボンの後ろポケットなどには現金や財布を入れない。

銀行カード、キャッシュカード：

- ✓ キャッシュカードの暗証番号をメモした紙を、カードが入った財布等の中に一緒に入れない。
- ✓ キャッシュカードの番号を控えて安全な場所に保管しておき、カード紛失や盗難の際にすぐ利用差し止めができるようにしておく。

携帯電話、スマートフォン

- ✓ バッグや上着の外ポケットには入れない。

(以上、仏警視庁 HP)

II. 交通事故を装った詐欺、タイヤ破り：路上・駐車場での新しい詐欺の手口

数週間前から、自動車運転手をターゲットにした新しい手口による路上犯罪が出現している。被害者の「不意をついて、困惑した状況につけ込む」新しい詐欺の手口だ。脅しの口調や自動車保険のペナルティ制度を利用したゆすりに発展することもある。

手口の例としては、「俺の車にかすただろう。目撃者もいるぞ。さあ、どうする？」といった言いがかりなどだ。車の後部がわずかに何かにぶつかったと感じた、あるいは相手の車との衝突を避けるためにハンドルを切った運転手は、何が起こったかはっきり分からず、あたふたしてしまう。ドアにちょっとした傷が付いた、バックミラーが破損したなどと言いがかりをつけ、事故が起きていないのに起きたと信じ込ませる。「偽の」事故被害者は素早く警告灯を点け、偽の自動車保険業者に電話するなど、被害者が戸惑っている間に素早く事を展開させるのも手口の特徴のひとつ。電話口の保険業者はもちろん、供述調書の作成を避けて話し合いで折り合いをつけるよう勧める。こうして被害者は、やっかいな手続きや自動車保険のペナル

ティが増えるのを避けるため、やむなく現金を渡して解決することになる。

また、別の手口の例として、ハイパーマーケットの駐車場などでのタイヤのパンクがある。被害者が店内でキャッシュカードで買い物の支払いをしているときに共犯者の1人が暗証番号を盗み見し、別の共犯者が駐車場で車のタイヤを裂く。被害者が駐車場に戻ってきてタイヤがパンクしているのを発見したところへ、詐欺師の2人がやって来て、親切を装いタイヤ交換に手を貸そうとする。被害者はこれを受け入れる。2人は全くの他人のように見えるが、1人がタイヤを交換している間にもう1人が被害者の財布を狙うというものだ。これに似たもうひとつの手口として、やはり駐車場で、1人が地図を持って道を尋ねている間にもう1人が被害者の車の中にあるものを盗む手口だ。犯人は車のボンネットの上や、特にフロントガラスの上に地図を広げ、車内が見えにくいようにする。そのすきに、共犯者が車内のシートに置かれたカバンなどを盗むケースもある。

こうした手口はやがて使い古されていくが、詐欺師の想像力もなかなか底を尽きない。

(以上プログレ紙、8月25日付)

「交通事故を装った詐欺」の手口にはまらないようにするために、このようなケースの被害に遭ったと思ったら、脅しにはのらず、できるだけ冷静に対応することが重要です。相手は現金を要求してきますが、これを絶対に受け入れず、きちんと供述証書を作成する、あるいは警察に通報する意思があるなどはっきりした態度を示すことが大切です。

III. 携帯電話：ハッカーの今後のターゲット

米ラスベガスで開催されたハッカー年次世界大会「DefCon（デフコン）」で、電子決済機能付き携帯電話の脆弱性が明らかにされた。

スマートフォン（多機能携帯電話）の登場で、さまざまな決済手段や認識手段が提供されるようになったが、これがサイバー攻撃の標的になりつつある。

リサーチャーのステファン・リドリー氏によると、携帯電話は常時つけっぱなしで、所有者の所在地を含め、ユーザーに関する大量の情報が記録されているため、ハッカーの侵入のターゲットとなる危険性が極めて高い。

その上、今後10年、電子財布としての用途が一般化することが予想される。

現在、私たちの財布には何が入っているか？ 身分証明書など、身元を識別できる書類、キャッシュカードなどの決済手段、個人情報。こうしたデータはすべて容易に携帯電話に収納することができる。今回のDefConでは、米国安全保障局

(National Security Agency, NSA) の元アナリスト、チャーリー・ミラー氏が、近距離無線通信 (NFC) のそばにセンサーを接近させて、スマートフォンに親友する方法を披露した。同氏によれば、NFC 搭載のスマートフォンを乗っ取ることも可能な場合もある。写真やアドレス帳を盗み出し、電話をかけたりすることもできる。ステッカーで隠したアンテナ装置を携帯電話に近づけることさえできれば、ハッカーはそこから侵入することが可能だという。スマートフォン対応の決済端末の近くに目立たないステッカーを貼り付けることで、買い物客の電話をハッキングすることは容易だろう。

(以上プログレ紙、7月30日付)