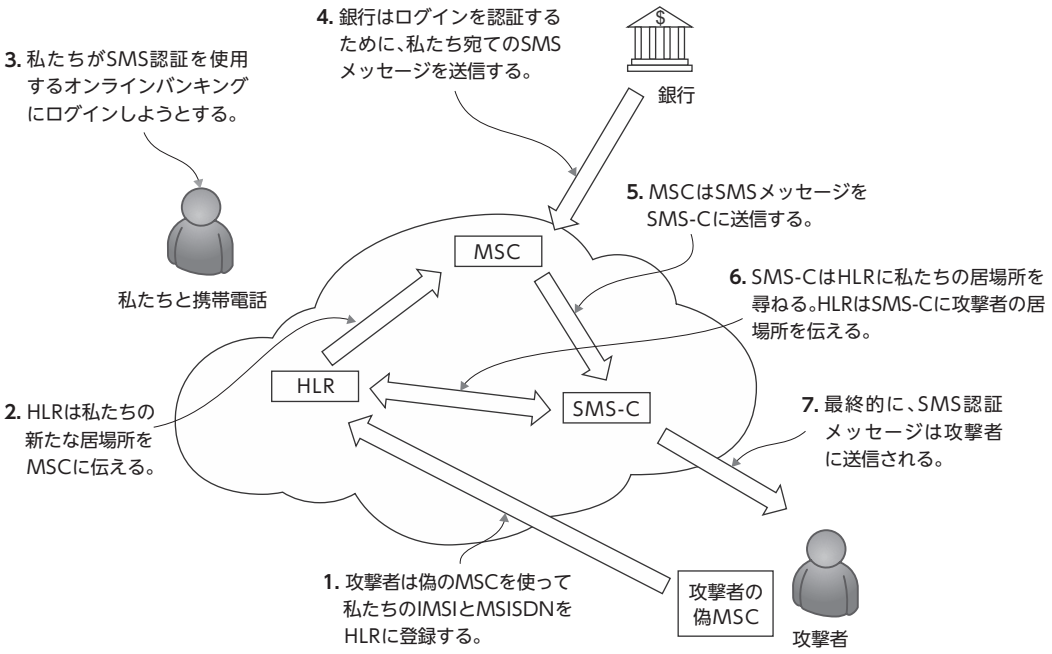

図4.21 攻撃者がSMSメッセージを傍受する方法。攻撃者はまったく同じ手法を使って、SMSメッセージを偽造し、私たちからのメッセージであるかのように見せかけることができる

この図ではさまざまなことが起きているので、一連の出来事を明確にするためにステップをリスト化してみましょう。

1. 攻撃者は偽の MSC を使って私たちの IMSI と MSISDN を HLR に登録する。
2. HLR は「私たち」の新たな居場所を MSC に伝える。
3. 私たちが SMS 認証を使用するオンラインバンキングにログインしようとする。
4. 銀行はログインを認証するために、私たち宛ての SMS メッセージを送信する。
5. MSC は SMS メッセージを SMS-C に送信する。
6. SMS-C は HLR に私たちの居場所を尋ねる。HLR は SMS-C に攻撃者の居場所を伝える。
7. 最終的に、SMS 認証メッセージは攻撃者に送信される。

繰り返しになりますが、これは非常に強力な攻撃であるうえに、必要な機器は簡単に入手できるものばかりで、Apple の新しいノート PC よりも安価です。ユーザー名とパスワードに加えた 2 段階目の認証方法として、SMS を使用するオンラインサービスがどれだけあるか考えてみてください。