第 14-13-318 号
2014 年 8 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 法人向けインターネットバンキングの不正送金対策、しっかりできていますか？ 」

前月の呼びかけ[※1]でも紹介しているように、インターネットバンキングにおける不正送金被害は増加傾向にあります。また、全国銀行協会が発表したアンケート結果[※2]に基づく過去 2 年間の法人口座の不正送金被害の推移を見ると、平成 26 年に急増していることがわかります（図 1 参照）。

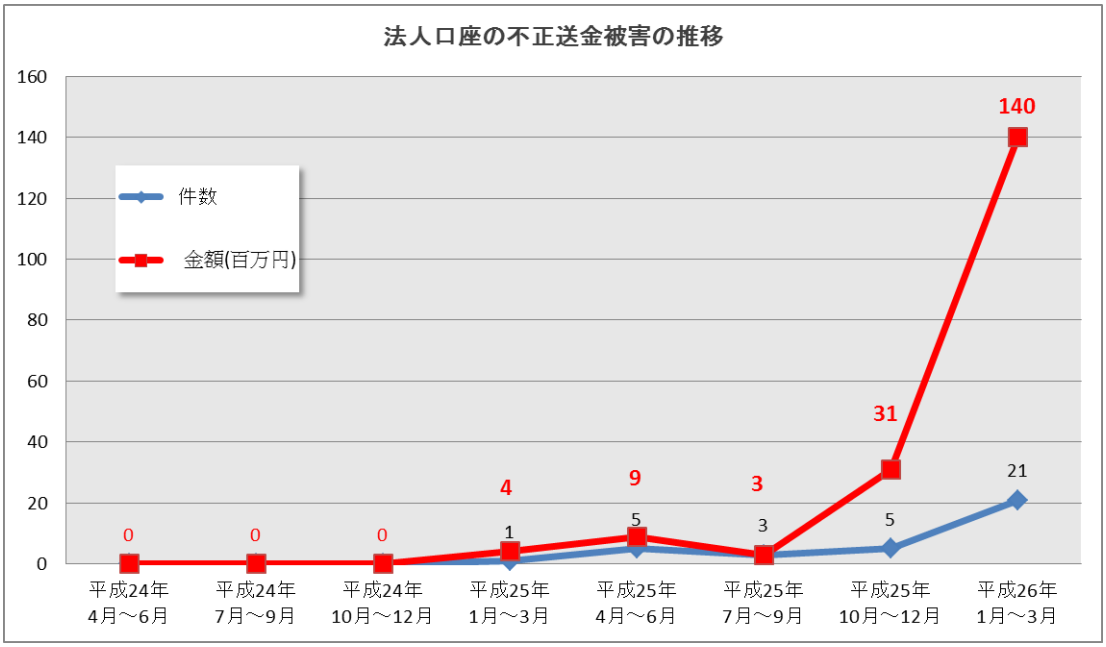

図 1：法人口座の不正送金被害の推移（過去 2 年間）

被害額急増の理由の 1 つに**電子証明書[※3]を窃取するウイルスによる新しい手口**[※4]の出現があります。

今月の呼びかけでは、法人口座を狙う不正送金の新しい手口と、その対策方法について解説します。

---

[1] 2014 年 7 月の呼びかけ：「 オンラインバンキングの正しい画面を知って、金銭被害から身を守りましょう！ 」
http://www.ipa.go.jp/security/txt/2014/07outline.html

[2] 全銀協ニュース：盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について
http://www.zenginkyo.or.jp/news/2014/05/23160000.html

[3] 公開鍵の所有者の正当性を確認できる証明書。認証局が発行する身分証明書や印鑑証明書のような電子的な証明書。
三井住友銀行：電子証明書についてもっと知りたい
http://www.smbc.co.jp/hojin/security/school/mail/column_pki.html

[4] 厳密に言うと、ウイルスは、公開鍵を含む電子証明書およびその対となる秘密鍵を窃取します。
（参考情報）トレンドマイクロ株式会社：法人ネットバンキングを狙う電子証明書窃取攻撃を解析
http://blog.trendmicro.co.jp/archives/9417

（1） 法人向けインターネットバンキングの認証方法

現在、銀行が法人向けに提供しているインターネットバンキングへのログイン時の認証方法は、概ね下記の 3 パターンに分類されます（図 2 参照）。

① ログイン ID とパスワード情報のみに基づく認証
② ブラウザに格納された電子証明書とパスワード情報に基づく認証
③ IC カード等に格納された電子証明書とパスワード情報に基づく認証

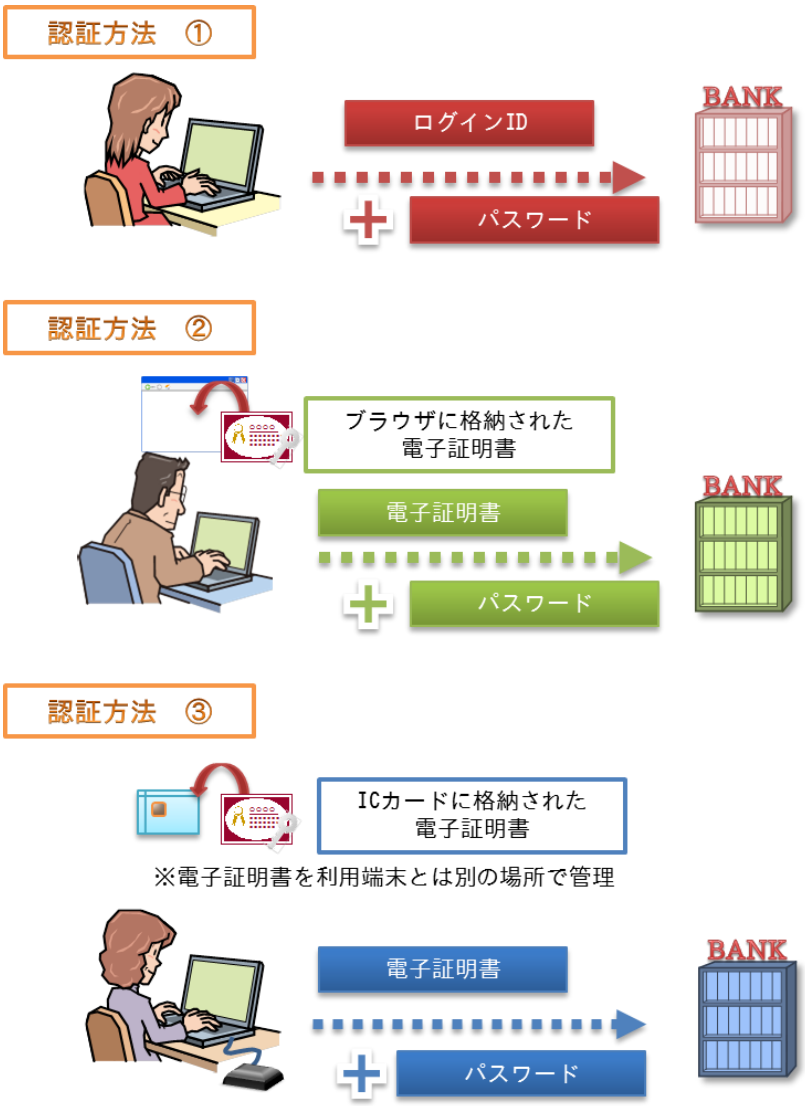

図 2：法人向けインターネットバンキングの認証方法

電子証明書はインターネットバンキングを利用する端末として正当であることを証明する“身分証明書”のような役割を担っています。そのため、別途、窃取したパスワード情報を用いて不正送金などを試みようとしても電子証明書のない他の端末では認証されず、送金ができません。このことから、上記に示す①の ID とパスワードのみの認証より、②および③の電子証明書を必要とする認証のほうが、高いセキュリティレベルが確保されていると言えます。

しかし、利用端末がウイルスに感染してしまうと**電子証明書が窃取されてしまう新しい手口が出現**しています。電子証明書が窃取されてしまうと、攻撃者が所有する端末であってもインターネットバンキングが利用可能な“正当な端末”として認識されてしまいます（図 3 参照）。

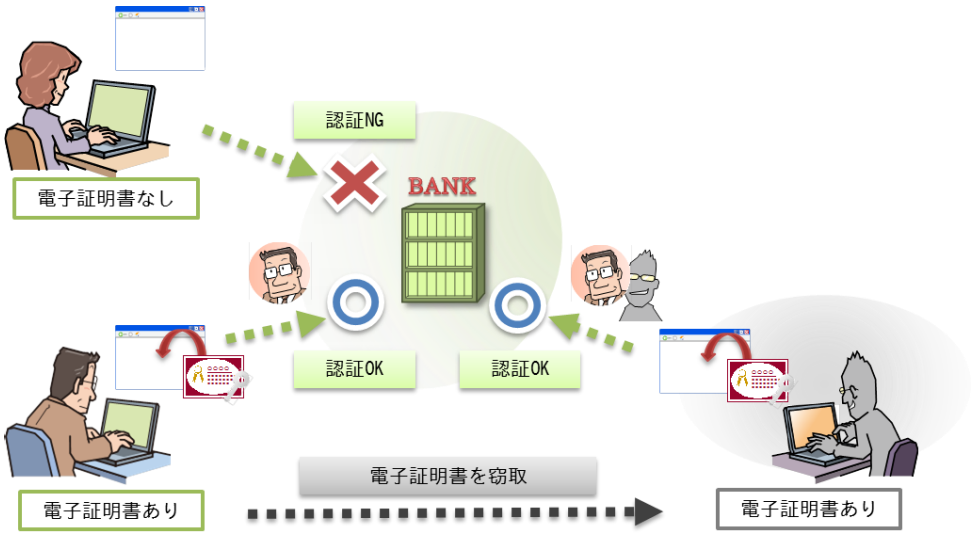

図３：電子証明書を窃取されてしまうと攻撃者が所有する端末から利用可能となる

（２） 電子証明書を窃取する手口

組織内の複数端末でインターネットバンキングを利用したい場合、それぞれの端末に電子証明書が格納されている必要があります。ブラウザに格納する電子証明書の場合、インポート※5時の設定で、エクスポート※6を「可」とすることで、現在利用している端末以外の端末に電子証明書を格納することが可能となります。

利用端末が複数あることは業務効率が高く、便利な一方で、不正送金に悪用されるリスクが高まるため、利便とリスクのトレードオフを見極める必要があります。そのため、電子証明書のエクスポート設定を原則「不可」としている銀行もあります。

最近では次のような電子証明書を窃取する新しい手口が確認されており、特に**エクスポート設定が「可」となっている場合は、気付かないうちに電子証明書を窃取されてしまう**危険性があります。

【1】エクスポート設定を「可」としてインポートした電子証明書を窃取する手口

端末がウイルスに感染していると、ウイルスが**電子証明書をエクスポートして攻撃者のサーバーに送信**します。

【2】エクスポート設定を「不可」としてインポートした電子証明書を窃取する手口

端末がウイルスに感染していると、ウイルスが**電子証明書を削除して無効**にしてしまいます。そうすると認証が行えなくなるため、利用者は電子証明書の再発行手続きを行うことになります。利用者が**再発行された電子証明書をインポートする際に、ウイルスは電子証明書をコピーし攻撃者のサーバーに送信**します。

---

[5] 自身のソフトが扱える形式に変換してファイルを「取り込む」こと
例：三菱東京 UFJ 銀行「リストア（インポート）の操作方法（InternetExplorer をご利用のお客さま）」
https://bizstation.bk.mufg.jp/info/info24/ie_import.html

[6] 他のソフトが扱える形式に変換してファイルを「書き出す」こと
例：三菱東京 UFJ 銀行「バックアップ（エクスポート）の操作方法（InternetExplorer をご利用のお客さま）」
https://bizstation.bk.mufg.jp/info/info24/ie_export.html

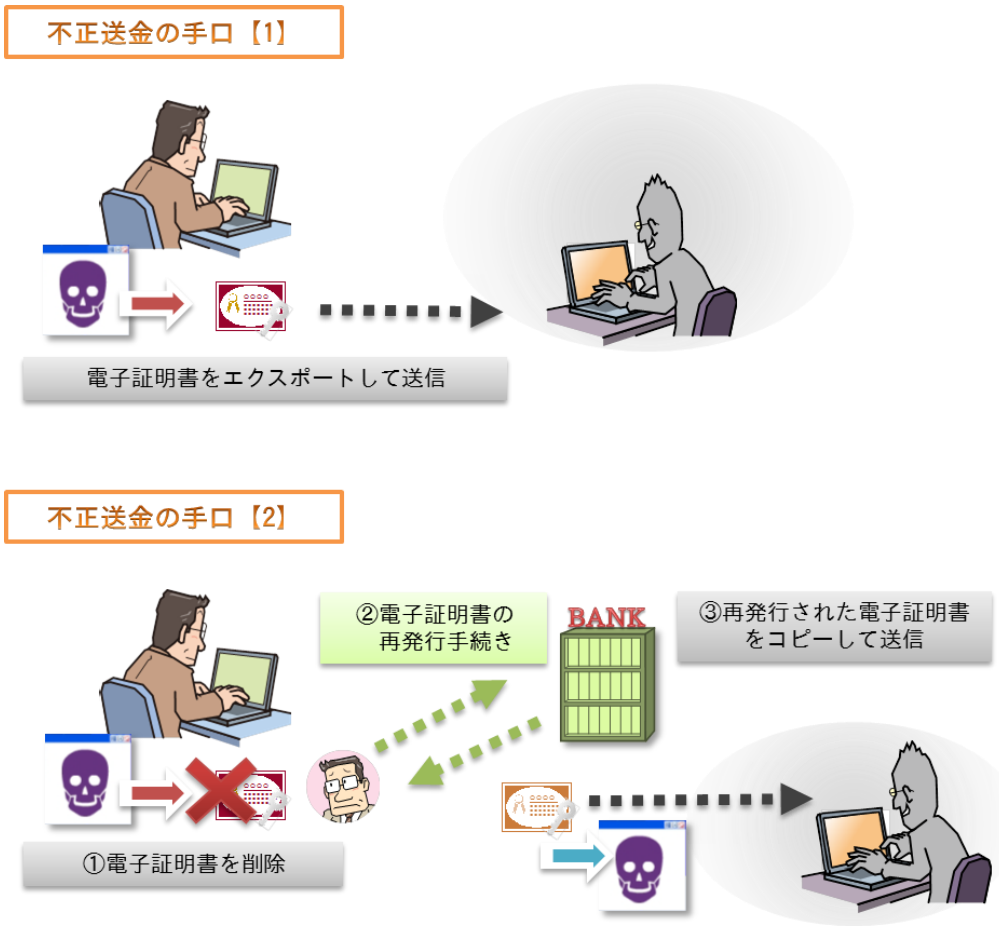

図 4：電子証明書窃取の手口

上記【1】の手口では、気が付かないうちに電子証明書が窃取されてしまう可能性があります。【2】の手口では、不自然なタイミングで電子証明書が無効となるため、この時点でウイルス感染を疑い、電子証明書の再発行手続きの前にパソコンの初期化などでウイルスを駆除することで、電子証明書の窃取を防ぐことができます。

（３） 万が一に備える対策の実施

今回の手口で IPA が推奨する対策は次の通りです。

- インターネットバンキングに利用する端末ではインターネットの利用をインターネットバンキングに限定する
- 銀行が提供する中でセキュリティレベルの高い認証方法を採用する
- 銀行が指定した正規の手順で電子証明書を利用する

ただし、前述の手口は**パソコンがウイルス感染していることが前提**のため、**パソコンをウイルスに感染させないための基本的な対策**[※7]**が最も重要**です。

このほか、全国銀行協会でも 7 月 17 日にインターネットバンキングの利用者に対して以下のような

---

[7] 2011 年 9 月の呼びかけ：「 あなたの銀行口座も狙われている！？ 」― SpyEye（スパイアイ）ウイルスに注意！ ― http://www.ipa.go.jp/security/txt/2011/09outline.html

情報セキュリティ対策※8を発表※9しています。

全国銀行協会が推奨するセキュリティ対策

・インターネットバンキングに利用する端末ではインターネットの利用をインターネットバンキングに限定する
・パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断する
・取引の申請者と承認者とで異なるパソコンを利用する
・振込や払戻し等の限度額を必要な範囲内でできるだけ低く設定する
・不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認する

法人口座は個人口座より送金限度額が大きいため、1 度の不正送金が事業存続に致命的なダメージを与える可能性があります。そのため、銀行が導入しているセキュリティ対策をよく確認し、ウイルスに感染しないための基本的な対策を行ったうえで、**全国銀行協会が提示する対策も確実に実施することが望ましい**と言えます。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／野澤
Tel:03-5978-7591 Fax:03-5978-7518
E-mail:isec-info@ipa.go.jp

8 銀行および法人のお客さまに求められるセキュリティ対策事例
http://www.zenginkyo.or.jp/news/entryitems/news260717_1.pdf

9 全銀協ニュース：法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方について
http://www.zenginkyo.or.jp/news/2014/07/17174000.html