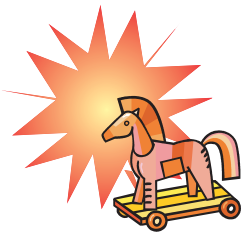


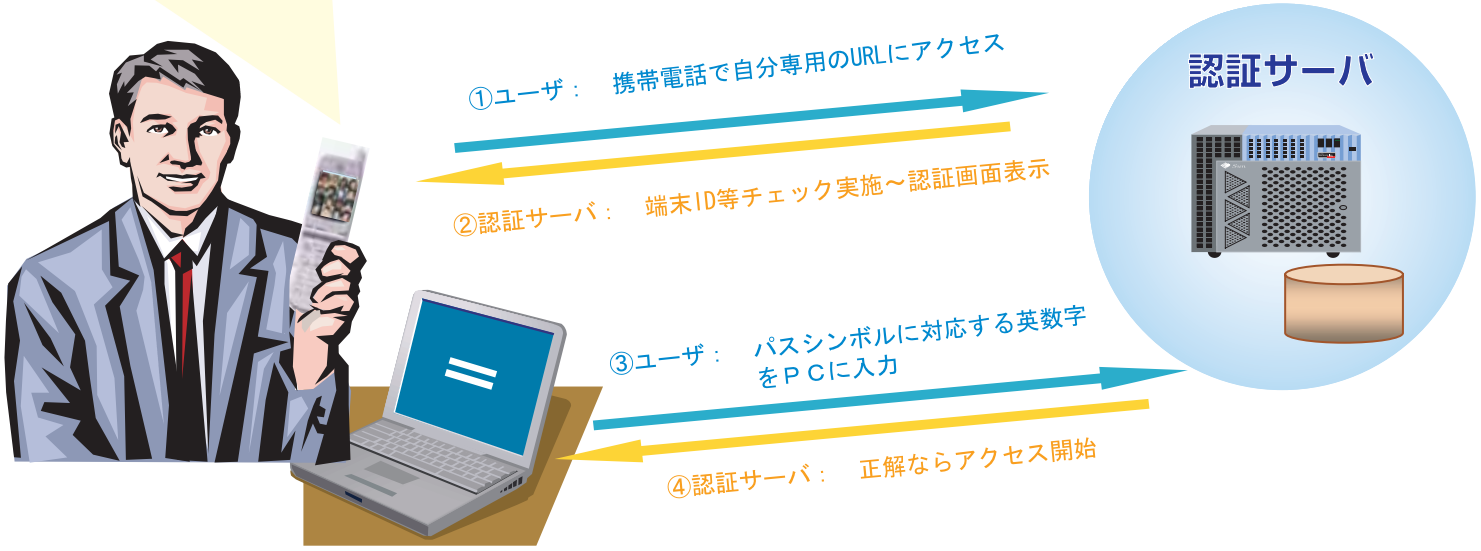
トロイの木馬型ウィルスを無力化し
本人認証情報の窃取を防ぐ

世界初

ワンタイム・ニーモニックガード

在来の使い捨てパスワード製品が窃取を防いでいるのは
『デバイス認証』情報

２経路２端末ニーモニックガードは『本人認証』情報の
ワンタイム化を実現



携帯電話に表示される認証画像の一つ一つに異なる英数字がランダムに割り振られる

➡ パスシンボル（正解の暗証画像）は毎回異なる英数字列で表現される

＝ ＰＣから入力されるワンタイム英数字列はユーザの記憶を含む本人認証情報

- 携帯電話とPCに必要なのはブラウザー搭載だけ
- ATM、PIN対応クレジットカード支払端末、入室管理にも応用可能

Mnemonic Security, Inc.

neme

Q トロイの木馬型ウィルスの脅威とは何か？　対応可能なのか？

A

大きな権限を持つユーザの本人認証情報が垂涎の的であり窃取のためにあらゆる手段を尽くそうとする人達がいます。窃取手段の中でも特に大きな脅威となるのが標的型トロイの木馬型ウィルス・スパイウェアです。狙い撃ち型・ターゲット型・スピア型とも呼ばれていますが、特定の企業や個人を標的に個別カスタマイズされたトロイの木馬を、事前に市販のウィルス駆除・スパイウェア駆除ソフトで探知できないことを確認した上であらゆる手法を使って標的の企業・個人のＰＣに潜入させるものです。このウィルスがユーザの本人認証情報を密かに送出します。

例えばセキュリティシステムの管理者の本人認証情報が盗まれるとセキュリティシステムは攻撃者の武器に転化します。機密情報管理者の本人認証情報を盗めば、資金運用担当者の場合には、防衛・治安・公共施設などインフラ組織の重要権限者では、…

駆除困難な個別カスタマイズされた標的型ウィルスであっても無力化する方法はあります。それはＰＣに入力する認証情報をワンタイム化する（使い捨てにする）ことです。本人認証情報やデバイス認証情報をワンタイム化するとトロイの木馬による本人認証情報やデバイス認証情報の盗用を防ぐことができます。

Q ２経路や２端末を使う使い捨てパスワード製品は以前からある。何が違うのか、何が新しいのか？

A

在来の機械生成型の使い捨てパスワード製品は、使い捨て乱数を生成しているデバイス（トークンや携帯電話）が本物であることの証明はできますが、今そのデバイスを保持しているのが本人なのか或いは攻撃者であるのかについては何も語りません。（本人認証としてはＩＣカード型の銀行カードやクレジットカードを暗証番号なしで運用するのと同等のセキュリティレベルです。セキュリティを重視するならば本人認証手段が別途必要となります。）

ワンタイム・ニーモニックガードで使われる使い捨て乱数は、携帯電話の画面に表示されている画像群からパスシンボル（暗証画像）を正しく視認できる本人のみが生成できるものです。ニーモニックガードが提供する高い本人認証セキュリティを犠牲にせずに盗聴やトロイの木馬を無力化できる方式です。

『デバイス認証』情報のワンタイム化製品は従来からありましたが、『本人認証』情報そのものを直接的にワンタイム化する製品はこれまで存在していませんでした。ワンタイム・ニーモニックガードは『本人認証』情報をワンタイム化する世界初の製品です。

Q 携帯電話とＰＣにプログラムを搭載しておく必要はないのか？ユーザの作業は？

A

携帯電話・ＰＣ共にブラウザーさえ搭載されていれば良く、ユーザの作業も次のように簡単です。

1. インターネットに接続されていない環境で認証画面とパスシンボル（正解の暗証画像）を認証サーバに登録し、携帯電話に受信したアクセス用ＵＲＬを登録しておきます。

2. アクセス時には携帯電話から登録ＵＲＬにアクセスすると自分の認証画面とユーザＩＤを受信します。携帯電話に表示された認証画面上でパスシンボル（正解の暗証画像）に割り振られている英数字列を認識します。その英数字列をユーザＩＤと併せて認証サーバにアクセスしているＰＣ上で入力します。

代理店

開発元

株式会社 ニーモニックセキュリティ

大阪市住吉区南住吉4丁目12番32号
（〒558-0041）
Tel:06-6608-6765　Fax:06-7494-5035
E-mail : sales@mneme.co.jp
URL : http://www.mneme.co.jp