＜　重点領域　＞

株式会社ニーモニックセキュリティ
２００８年5月３０日

最近のセキュリティ動向を踏まえ、次の４分野を当社技術のメリットが際立つ重点領域とみなします。

Ａ　モバイル端末の情報流出防止
Ｂ　リモートアクセスの情報漏洩改竄の防止
Ｃ　最重要情報の持ち出し防止
Ｄ　パスワード窃取を図るトロイの木馬の無力化

以下に当社から提供できるソリューションについて述べます。(ページ番号は技術製品紹介スライドの該当ページを示します。)

Ａ　モバイル端末の情報流出防止：　様々な選択肢を提供できます。

１．　ＰＣログオン認証(紹介スライドＰ１３)：　Ｃドライブに『ニーモニックガード Windows2000/XP 版』をインストールする方式とＵＳＢキー搭載『パスシンボルロッカー・ＰＣログオン』を使用する方式の２つの方法がありますが、どちらも多桁 Windows パスワードと連携するものです。どちらのケースでもディスク抜き取りへの対抗策として Windows に備わっているフォルダー暗号化機能を使うことをお勧めしています。

注意点としては、両製品ともに Windows のレジストリーを変更しますので、同じくレジストリーを変更するソフトが搭載されている場合にはインストールができないことがあります。

『パスシンボルロッカー・ＰＣログオン』ではＵＳＢキーの保持が前提になりますので２要素認証の長所（攻撃者は記憶情報とキーの両方を盗まねばならない）と短所（ユーザはキーを置き忘れると仕事にならない）の両方を併せ持つことになります。

＊　Windows パスワードの脆弱性（LMハッシュ保存問題）及び Windows パスワードとニーモニックガードとの関係につきましてはそれぞれ文末注１・２に、またオフィス環境で有効であった在来技術がモバイル環境では有効性を失うことについて文末注３に説明しています。

２．　『パスシンボルロッカー・セキュアストレージ』(紹介スライドＰ１５)：　ＰＣは持ち出さず外部メモリーのみを持ち出す場合に加えて、ＰＣを持ち出す場合にもデータはＰＣには保管せず本製品に保管して持ち出すという運用方法もあります。(他のソフトが Windows のレジストリーを変更していてニーモニックガードでの Windows ログオン認証ができない場合にも、このような方法をお勧めできます。)

３．　『クリプトニーモ』(紹介スライドＰ１６)：　常態では暗号鍵を存在させず暗号化・復号時にはニーモニック認証データから動的に暗号鍵を生成する暗号ソフトをＰＣ上あるいは外部メモリー上で運用する製品「クリプトニーモ」はモバイル環境で本領を発揮します。

応用製品にはハギワラシステコムの『パスワードロッカー・パスシンボル』があります。文字パスワードを通過して始めてドライブ内にアクセスできるＵＳＢメモリー上で、更に個々の機密ファイル・フォルダーを「クリプトニーモ」によって暗号化するものです。使用場面は『パスワードロッカー・セキュアストレージ』と同じです。

４．　スマートフォン・ログオン認証（紹介スライドＰ１４）：　業務に利用される携帯電話からの情報流出の懸念があれば『ニーモニックガード・WM』搭載可能なスマートフォンの使用をお勧めします。

なお、汎用携帯電話に搭載された業務アプリの利用者認証をＪａｖａないし Ｂｒｅｗ上で動作するニーモニックガードで行うことは可能であり実例もあります。

　汎用携帯電話のロック機能用のニーモニックガード搭載は未だ先のことになりそうです。ＡＴＭでの静脈認証装置の普及は銀行業界での暗証番号の位置づけを如実に示す証とみなせるのですが。

Ｂ　リモートアクセス時の情報漏洩改竄の防止

１．　『パスシンボルロッカー・ウェブ自動ログイン』（紹介スライドＰ１５）：　シンクライアント方式が注目を集めていますが、シンクライアント端末自体は情報を持たなくてもサーバとの通信ができる限りは本人認証が弱いと情報の流出を防げず、特に改竄の脅威は深刻です。本製品をお使いいただくと現行のパスワード認証システムに変更を加えることなくセキュリティを大きく向上させることができます。

覚える必要のない１００ビット級以上の多桁パスワードを本製品に登録しておきます。端末上での成りすまし攻撃は画面とキーボードを占拠しているニーモニックガードが防ぎ、ネット上での総当り攻撃は１００ビット以上という数学的強度で防ぎます。覚える必要のないパスワードを運用するので頻繁に変更してもユーザの負担はほとんど増えません。

ニーモニック認証画面に文字マトリックスを用意すればユーザは苦労して覚えた無機質パスワードを使い続けることもできます。このケースでも端末上での攻撃は画面とキーボードを握っているニーモニックガードが防ぎ、自動化できるネット上での総当り攻撃に対しては１００ビット以上のパスワードで防ぐことになりますので、同じ文字パスワードを使っていても直接入力する在来方式に比べればより高いセキュリティを実現できます。

なお、携帯電話やＵＳＢ端子のないモバイル端末についてはニーモニック認証をサーバ側で行うウェブアクセス認証版（Ｐ１９）をご提案します。ＮＴＴコミュニケーションズでの運用実績のある基本モデルに加えて、今後は「Ｆｌａｓｈ」を組みこみ携帯電話の機種の違いを乗り越えた汎用サービスの提供も進めます。

Ｃ　有権限者による意図的情報持ち出しと改竄の防止

１．　『権限分散クリプトニーモ』（紹介スライドＰ１８）：　常態では存在しない暗号鍵を１０人の登録オペレータの中の３人が共同で作業して復元する方式のため有権限者でも一人では情報を持ち出せません。どんなに価値のある情報を扱っていても誘惑・ストレス・脅迫を心配する必要はなくなります。

これまで複数ユーザの共同作業を要求するような面倒なソリューションは民間での需要は殆どないだろうと言われてきましたが、潮目は変わってきたようです。ヤマトシステム開発では暗号鍵の分割保持を実行しているとの情報が以下のサイトから得られます。
　http://itpro.nikkeibp.co.jp/article/OPINION/20080408/298307/?P=2

また、最近あちこちで目にするデータ分割保管の考え方を延長すれば自然にオペレータ権限の分割つまり権限分散に行き着きますから、『権限分散クリプトニーモ』運用の煩雑さを厭わないような土壌が既にできつつあると考えています。

どこまでを最重要情報と見なすかは企業・組織ごとに異なるでしょうが、全般に適用可能な共通基準はあります。それは外部から守秘義務を負って預かった情報はその性格・質・量を問わずすべて最重要情報に属します。どんなに価値あるものでも社内で生まれた情報の流出・改竄であれば社内で処理を完結させることも可能でしょうが、外部から守秘義務を負って預かった情報を社内の有権限者に意図的に持ち出されることを許せば企業・組織の存続にさえ関わります。

Ｄ　パスワード窃取を図るトロイの木馬の無力化

１．　『ワンタイム・ニーモニックガード』（紹介スライドＰ２１）：　これまでのデバイス認証情報を使い捨てにするだけのいわゆる“ワンタイムパスワード”製品とは異なり本人認証情報そのものを使い捨てにすることにより重要権限者のパスワード窃取を図るトロイの木馬を無力化します。

「ネット時代のスパイ活動、発信源は中国にあり　－　サイバー攻撃が激増、標的は政府機関や防衛関連企業」　http://business.nikkeibp.co.jp/article/world/20080418/153470/
というスピアフィッシングの脅威を取り上げたBusinessWeekの記事を日経ＢＰネット版が紹介しています。

言うまでもなく攻撃者に取得されると一番大きなダメージが予測されるもの、それは大きな権限を持った人物のパスワードです。防衛・治安・行政・インフラ系企業とのつながりある人達のパスワード窃取を防ぐのは喫緊の課題の一つと考えられます。

喫緊の課題であるＣ１とＤ１については文末注４もご参照ください。

注１　　Windows パスワードの脆弱性　（LMハッシュ保存がデフォルトでON）

Windows のログオン用パスワードは１４桁までと１５桁からでは扱いが異なります。１４桁までにはLMハッシュ保存という脆弱な手法が使われ、１５桁以上にはLMハッシュ保存が行われません。LMハッシュがONとなっているＰＣの１４桁までのパスワードはネットで簡単に入手可能なパスワードクラッキングソフトを使うと短時間で破られてしまいます。

問題なのは Windows ＰＣのセキュリティを崩壊させるLMハッシュ保存がデフォルトではONであることがハッカー集団や犯罪予備軍の間ではよく知られている一方で、マイクロソフトがこの情報を積極的に開示しないこともあって一般の善良なＰＣユーザはそのことを知らないままだということです。LMハッシュをＯＦＦにしてクラッキングソフトを無力化できることを知っており実際に実行できるのは極めて限られたWindows 専門家のみ(際立ってセキュリティ意識が高いと言われている大手ＩＴ企業のセキュリティ責任者ですら知らない人が多い）という状況が続いています。

LMハッシュでは１４桁のパスワードを７桁ごとに分割してからハッシュをします。１４桁の大文字小文字まじり英数字は８０ビットですが、これを７桁ごとに分割するとそれぞれが４０ビットで、２つを足しても１ビット増えるだけです。ただ、多くの人は８０ビットは４０ビットの２倍だろうといった認識をしているようです。４０ビットのパスワードを総当りして平均１秒で解けるコンピュータが仮に手元にあるとしても８０ビットに当たると平均で１兆秒かかることになります。４０ビットと８０ビットはそのくらい違うのですが。

ともあれ、１５桁以上のパスワードではLMハッシュ保存は機能せずセキュリティ崩壊は起こりませんので、当社では１５桁～３２桁のパスワードをニーモニックガードＰＣログオン版で管理運用する方法を薦めています。

注2　『ニーモニックガードＰＣログオン版』でのニーモニックガードと Windows パスワードの関係は次のようになっています。

Ａ　管理者は

Windows パスワードとして出来れば３２桁までの無機質ランダムな英数字記号列を登録し、管理簿に記載して安全な場所に厳重に保管しておきます。ユーザがニーモニックガードの認証データを登録したところで Windows パスワード入力を要求されるので、管理者が管理簿を参照して入力して、ＰＣをユーザに返します。

ユーザが突然退職したような場合には、管理者は管理簿のパスワードを使ってセーフモードで Windows を立ち上げてニーモニックガードのアンインストールを行い、新たなユーザ用に再インストールを行います。

Ｂ　ユーザは

ニーモニックガードのパスシンボルとして（既に長期記憶となっている＝覚えてしまっている）昔の懐かしい思い出につながる画像を登録しておくだけで、パスワードを覚える必要はありません。パニック状態になっても使いこなせます。

Ｃ　不正取得者は

１．Windows 立ち上げの前にニーモニックガードの通過を要求され、他人推定エラー回数あるいは総エラー回数が事前に設定された値に達するとそれ以後の認証作業継続を拒否されます。

２．自動プログラムでの総当りを試みることは可能ですが、Windows パスワードとして最大３２桁のランダム英数字記号列を登録してあれば我々の生きている間に破られる確率はゼロに近いといえます。

以上をまとめると次のようになります。
・不正取得者がニーモニックガードのエラー判定をすり抜けて認証を通過できる確率はゼロに近く、
・自動プログラムによる総当り攻撃で破られる確率もゼロに近く、
・パスワード管理上の追加負担はありません。
　＋
・　『異常事態通報シンボル機能』を活かせば強要による情報流出・不法取引・サボタージュのリスクを大きく軽減できます。

＊　異常事態通報シンボル機能：　モバイル環境では、オフィスでは考える必要のなかった新たな脅威にも備えなければなりません。その一つは単独行動時に起こりえる第三者による強要・脅迫です。唯々諾々と応じてしまえば大きな被害を承知していながらも端末の悪用ないし機密情報の奪取を許してしまうことになり、かといって応じなければ危害を加えられる怖れがあります。このような状況を想定してニーモニックガードにはオプション機能として異常事態通報シンボルを活用できるようになっています。

パスシンボル（暗証画像）の登録個数は自由ですから、脅迫者はユーザが５個或いは８個選択するのを目視していても、その情報からは異常事態通報シンボルも選択されたかどうかは判断できません。つまり、ユーザは脅迫者には知られることなくパスシンボルに加えて異常事態通報シンボルを入力することができます。認証処理完了時に事前に指定していたフォルダーを自動的に強制削除するようにしておけば、脅迫者がＰＣの中を探してもユーザが守りたい機密情報を見つけることはできません。機密情報に似て非なる情報を見るだけです。

こうした情報は速やかに攻撃予備軍に届きます。他にもっと狙いやすい獲物があるのに敢えて異常事態通報機能を備えたニーモニックガードで守られたＰＣを狙おうという攻撃者は多くはないでしょう。盗用・情報流出・不法取引・サボタージュのリスクを極小化し、ユーザの不安・ストレスを軽減します。

注3　オフィス環境　ＶＳ　モバイル環境

	オフィス	モバイル
・物理的警備	可	不可
・同僚の環視・監視カメラ	可	不可
・管理者の支援	可	不可
・端末盗難・紛失リスク	小	大
・脅迫・強要リスク	小	大

モバイルで使えるものは、よりリスクの低いオフィスでも使えるとは言える。

しかし、オフィスで使えるからと言って、よりリスクの高いモバイルでも使えるは言えない。

＜オフィス：　端末は机に張り付いている　管理者に頼れる＞

1．離席する時に手帳を持ち歩く　→　ＰＣの近くに手帳はない
　→　『難解パスワードの手帳管理』でそれなりの安全性を確保
（携帯電話・ＩＣカード・ＵＳＢキーなどの照合用所持物でも同様）

2．生体照合で本人拒否発生　→　上位権限者による救済でセキュリティ維持

＜モバイル：　端末はユーザ個人に張り付いている　頼れる管理者はいない＞

1．端末と手帳・照合用所持物が
　・離れてしまうと仕事にならない
　・離れなければ一緒に盗まれる可能性が高い

2．生体照合の本人拒否時に頼れる上位権限者はいない
　・救済用に脆弱パスワードを併用すると他人排除力は脆弱パスワード単独使用より更に低下
　・本人拒否を起こさない閾値での運用は他人排除力なし

注4　「一番大事なことは最後にじっくりと」と考えるのは災害対策とセキュリティでは不適当

最高機密の暗号化保護などの高度なソリューションについては、アクセス管理の整備などセキュリティ体制全般の見直しを行った後で時間をかけてじっくりと検討するのが望ましいといった考え方が強いようです。これは妥当なものでしょうか？

洪水の危険が迫っています。乳幼児や家宝を先ずは高いところに避難させておいてそれから家の周りに土嚢を積むことを考えますか、それとも乳幼児や家宝は一階に置きっ放しのままで先ず家の周りの土嚢積みを終わらせてしまおうと考えますか？　筆者ならば迷うことなく前者を選択します。

情報の保護も同じでしょう。外部から守秘義務を負って預かっているデータなど、この情報が流出したら、特に権限を与えてある社員に持ち出されたりでもしたら、大変なことになるといった最高度の機密情報を今手に入る最良の手段で保護して最悪の事態に対する手当てを先ずは終えておき、それからじっくりと時間をかけて全般的なセキュリティ体制の整備を進めるのが望ましいと考えます。

以上