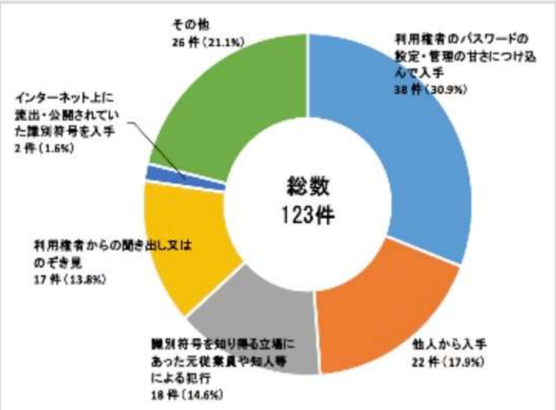
2022/2/4　樹脂製造部　北川

2022年２月１日～３月１８日は
「サイバーセキュリティ月間」です。

2022年 キャッチフレーズ
「#サイバーセキュリティは全員参加」です。

今回は安全なパスワードについて話したいと思います



不正アクセス禁止法の「識別符号窃用型」における手口（グラフ：警察庁）

警察庁が2021年上半期におけるサイバー犯罪の検挙状況を
取りまとめたものが下記の円グラフです。
検挙件数は5345件で、上半期だけで前年同期の4361件から
984件増加した状態です。

サイバー犯罪の不正アクセス禁止法違反におけるパスワードの
入手経路を見ると、「設定や管理の甘さにつけ込んで入手」が
38件でもっとも多く30.9%にのぼる。
「他人から入手（22件）」が17.9%と2番目に多い。
「パスワードを知りうる立場を悪用」が18件、
「本人より聞き出したり覗き見」したケースが17件で続く。
インターネット上に公開されているパスワードを入手した
ケースは2件だった。

安全なパスワードの作成

安全なパスワードとは、他人に推測されにくく、ツールなどの機械的な処理で割り出しにくいものを言います。

安全なパスワードの作成条件としては、以下のようなものがあります。

(1) 名前などの個人情報からは推測できないこと
(2) 英単語などをそのまま使用していないこと
(3) アルファベットと数字が混在していること
(4) 適切な長さの文字列であること
(5) 類推しやすい並び方やその安易な組合せにしないこと

インターネットなどで配布されているツールの中には、パスワードクラッカーと呼ばれる機械的に
パスワードを推測する機能を持つものがあります。
このパスワードクラッカーには、パスワードでよく使われる単語が辞書として登録されており、この辞書
に載っている単語や簡単な英数字の繰り返し（123やabc、aaaなど）を自動的に組み合わせることで、
パスワードを探し出そうとします。
このようなツールでパスワードを割り出されないようにするためには、推測しやすい文字列を使わない
ようにすることが大切です。

パスワードの保管方法

安全なパスワードの作成だけでなく、他人に知られないよう、かつ自分でも忘れてしまうことがないように管理をしましょう。
自分で忘れてしまわぬようにメモを作成した場合は、それが他人に見られることのないよう、肌身離さず持ち歩くなど、厳重に保管をするよう心がけましょう。

パスワードを複数のサービスで使い回さない（定期的な変更は不要）

また、パスワードはできる限り、複数のサービスで使い回さないようにしましょう。
あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。
もし、重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。
定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。
これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に、米国国立標準技術研究所からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです。

パスワードの活用

現在の一般的なOSのスクリーンセーバーでは、元の操作画面に復帰する際にパスワードの入力を促す設定を行うことができます。
このように設定することで、離席中に不正な利用者がそのパソコンを操作することを防ぐことができるようになります。
ただし、スクリーンセーバーが起動するには一定の時間が必要です。
さらに情報セキュリティを強化するためには、離席する際にログアウトを行い、パスワードを入力してログインしなければパソコンを操作できないようにするなど、利用者が自発的にロックする方法が有効です。

以上の事を踏まえサイバーセキュリティの被害者にならないよう
パスワードの管理を責任を持って行って下さい。