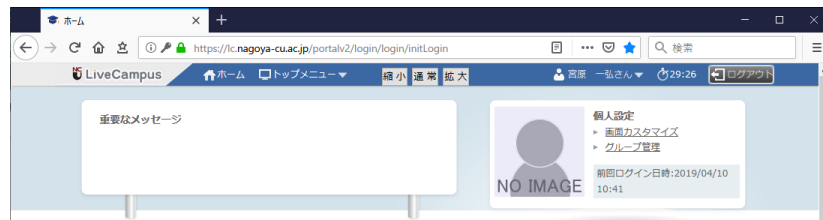


本日のキーワード0

名古屋市立大学における 情報環境

学務情報 システム経由の 連絡事項



授業連絡

2019/04/10 【授業連絡】 [滝] 情報・統計処理(11) (未読)

授業連絡

2019/04/10 【授業連絡】 [滝] 情報・統計処理(12) (未読)

授業連絡

2019/04/10 【授業連絡】 [滝] 情報・統計処理(11) (未読)

登録



メールでも通知

メールアドレス 1 : c191099@ed.nagoya-cu.ac.jp

メールアドレス 2 : }
メールアドレス 3 : } 各自で登録



誤って登録
送信エラー



本日のキーワード1

アカウント

アカウント通知書

～ 総合情報センター ～

取扱注意

総合情報センター教育システムアカウント通知書

ユーザー名：c999999

パスワード：Abcd1234

※ 下記のパソコンでログイン後「Ctrl+Alt+Delete」でパスワードの変更が可能です。

【注意事項】

- アカウントは、コンピュータや各種システムがあなたを正規の利用者として認証する手段です。パスワードを他人に知られると、あなたのデータが破壊されたり、なりすまして不正行為が行われるだけでなく、コンピュータやシステム全体に大きな被害を与えられる可能性があります。パスワードの管理は、利用者の大切な義務です。被害の度合いによっては、パスワードの管理を怠った人に損害賠償責任が生じる可能性があります。
- このパスワードは、すみやかに自分の覚えやすいものに変更し、変更後この通知書は他人に知られないよう廃棄してください。万が一、この通知書を紛失したら(他人にパスワードを知られたら)、至急総合情報センターまで連絡してください。

【総合情報センター教育システムのアカウントについて】

サービス	ユーザー名	仮パスワード	アクセス可能なパソコン
			<山の郷キャンパス> 1号館 CAL 実習室、情報処理実習室、社会調査実習室、院生室 2号館 OLI・2 教室 3号館情報処理実習室 6号館臨床系、201・202 情報処理実習室 総合情報センター山の郷分館
			<川島キャンパス> 医学部基礎教育情報処理実習室 医学部研究棟 11 階 看護学部棟 401 情報処理教室 総合情報センター川島分館
パソコンのログイン WWWサービスのログイン	c (英小文字) + 学籍番号	上記記載の8桁英数字	<田辺通キャンパス> 実習棟 CB1 教室 総合情報センター田辺通分館

アカウント



利用資格

(コンピュータの利用, ネットワークへの接続, Webサイトへのログインなど)

アカウント = ユーザ名 + パスワード

c171098
c143487
c094677
miya

Hv5%aZi4
gDVp#hDa
Bj7-uYda
t2Dh>hHp

名古屋市立大学におけるアカウント

在学中, 総合情報センターから貸与

いくつかのアカウントを 利用することになるか?

名古屋市立大学におけるアカウント

在学中，総合情報センターから貸与

サービス	ユーザー名	仮パスワード	アクセス可能なパソコン
Ⅱ アカウントの種類 Ⅱ 5 アカウント パソコンのログイン WWW サーバのログイン	c(英小文字) +学籍番号	パスワード通知書 記載の8桁英数字	<蒲子(山の畑)キャンパス> 1 号館情報処理実習室 2 号館 CAL 教室 3 号館情報処理教室 3 号館データ分析室 6 号館端末室 総合情報センター山の畑分館 <桜山(川澄)キャンパス> 医学部基礎教育棟情報処理実習室 医学部研究棟 11 階 看護学部棟 401 情報処理教室 総合情報センター川澄分館 <田辺通キャンパス> 実習棟 CBT 教室 総合情報センター田辺通分館 <北千種キャンパス> 総合情報センター北千種分館
学務情報システム (Live Campus) 図書館ポータルシステム (My Library)			学内・学外
メールの送受信 (Office365)	c(英小文字) +学籍番号 @ed. nagoya-cu.ac.jp		

すべてのアカウントで
共通化

SYSTEM GUIDE 2019 p.9より

本日のキーワード2

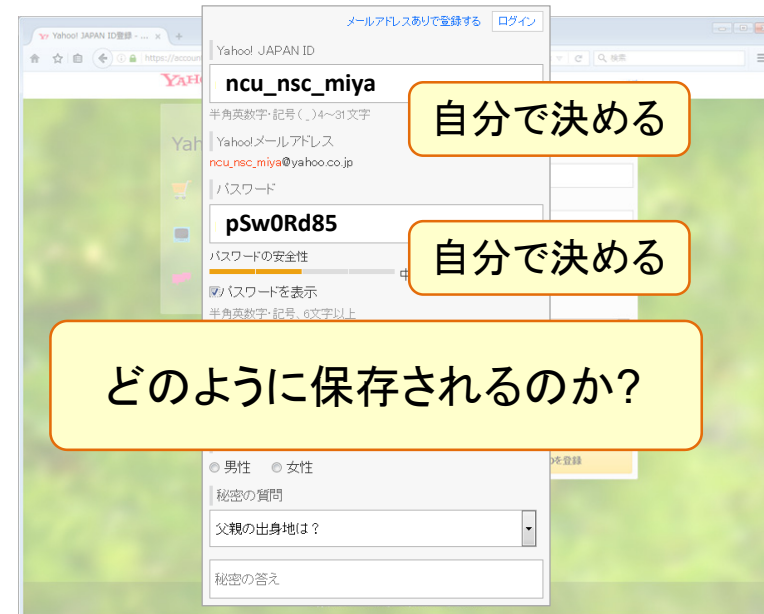
パスワード

パスワード

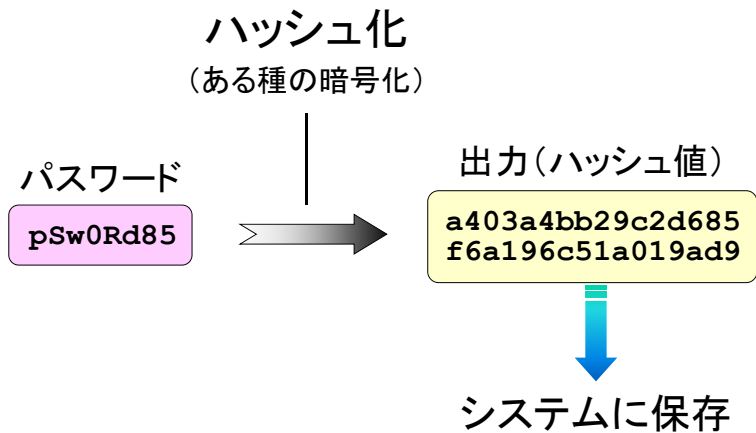
管理の重要性を認識

- (1) 人に知られてはいけない
人に教えてはいけない
- (2) 安易なパスワードをつけない
- (3) 同じパスワードの使い回しをしない

パスワードを設定する

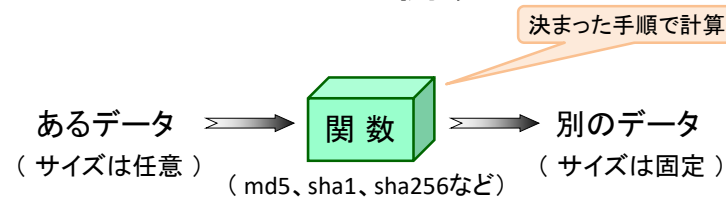


パスワードを設定する

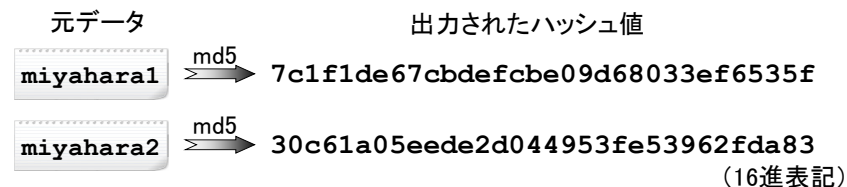


※ 厳密には暗号化とは異なります

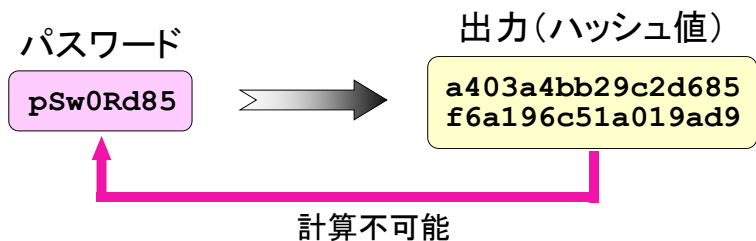
ハッシュ関数



- ✓ ハッシュ値から元データの逆計算は不可能(一方向)
- ✓ 元データをわずかでも変更すると、ハッシュ値は大きく変化
- ✓ 同一のハッシュ値を生成する別のデータは発見が困難



パスワードを設定する



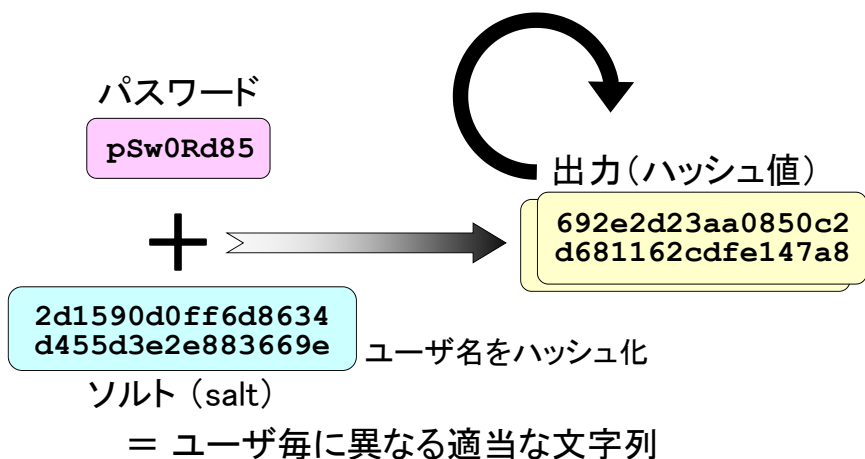
システムに保存されるのはハッシュ値
パスワードがそのまま保存されている訳ではない
本人以外、誰もパスワードを知り得ない

サーバ管理者が良く聞く言葉

パスワード忘れてしまったので
教えてもらえませんか?

返答：不可能です。

より安全なハッシュ化



パスワードアタック

(1) オンライン攻撃

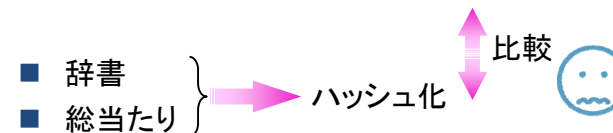
- 個人情報からの推測
- 辞書とのマッチング
- 総当たり (ブルートフォース・アタック)

→ 順に試していく → 試行回数に限界



(2) オフライン攻撃

前提：ハッシュ化されたパスワードリストの入手



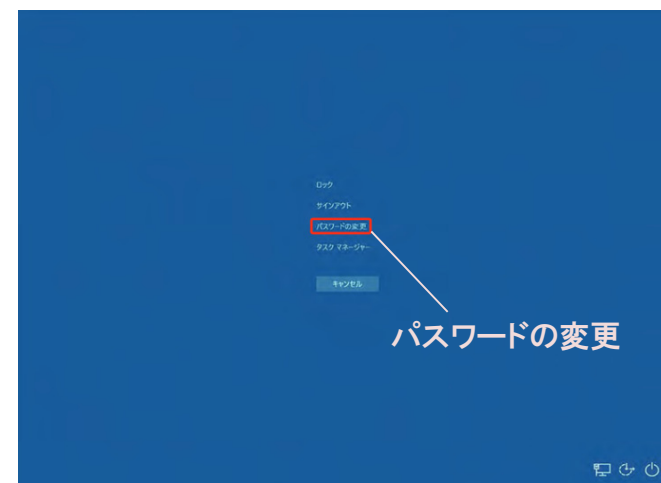
(3) ソーシャルエンジニアリング

望ましいパスワード管理

- (1) 短すぎるものは避け、ある程度の長さとする
- (2) アルファベット(大文字・小文字), 数字, 記号を混ぜる
- (3) 類推されやすいもの(個人情報など)は避ける
- (4) 定期的に変更する
- (5) メモには残さない
- (6) 他人に教えてはいけない
- (7) **使い回しをしない**

パスワードの変更

Windows ログオン中に、**Ctrl** **Alt** **Delete** キーを同時に押す



パスワードの変更



SYSTEM GUIDE 2019 p.10より

ところで…

アカウントは5つあった (アカウント = ユーザ名 + パスワード)

この操作で変更されるパスワードは、どれ?

➡ 全てのパスワードが連動して変更される

新しい認証手段

(1) ICカード



(2) 乱数表



(3) ワンタイムパスワード (トークン、カード、メール送信)

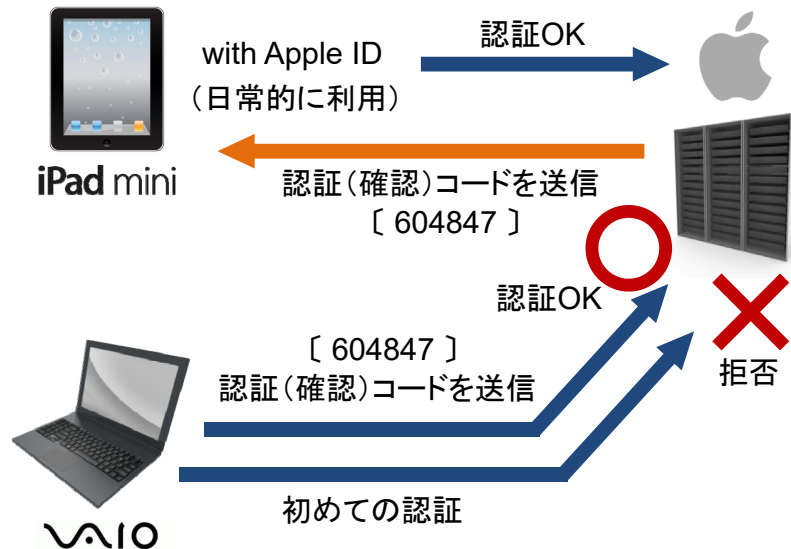
(4) バイオメトリクス

(指紋、虹彩、静脈、声紋、署名 など)



(5) 2段階認証

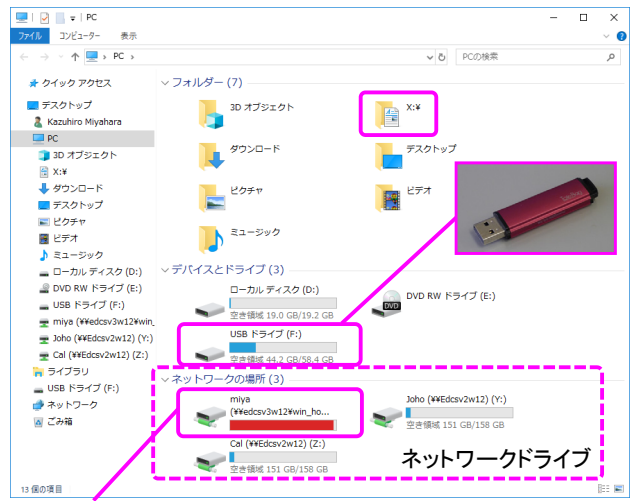
2段階認証



本日のキーワード3

ネットワーク
ドライブ
クラウド

ファイルの保存場所

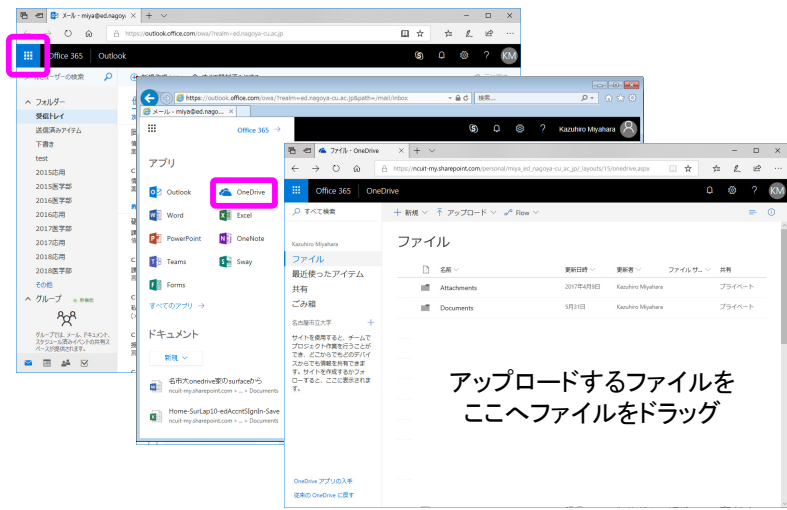


X ドライブ c191099 (¥¥edcsv3w12¥win_home)
(大学のPCのみから利用可能)

ファイルの保存場所



Office 365メールにサインイン



本日のキーワード4

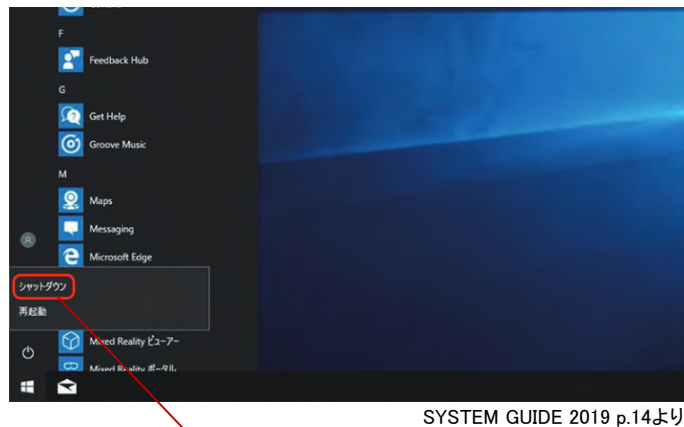
ロック シャットダウン

コンピュータのロック

一時離席時のみ



シャットダウン / ログオフ



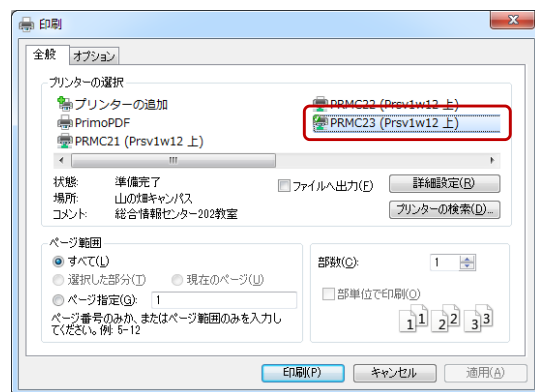
シャットダウンを選択

本日のキーワード5

プリンタ は みんなのもの

プリンタの選択

席に近いプリンタを選択



印刷 ボタンを押した後は、出力されるまで責任を持つ!

(紙詰まり、紙切れ、遠いプリンタへ出力し放置など)