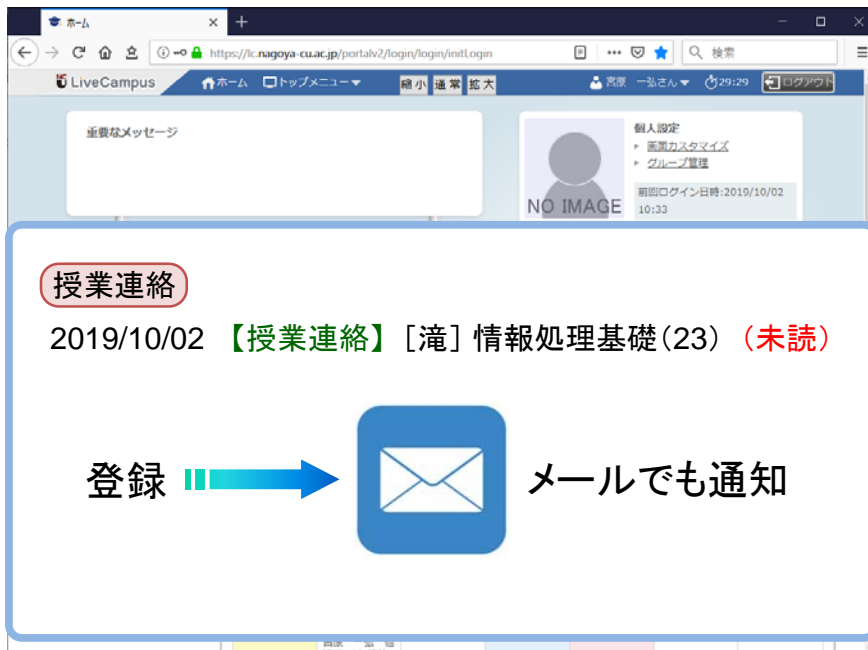


本日のキーワード0

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
2019/10/02 【授業連絡】 [滝] 情報処理基礎(23) (未読)

登録 → メールでも通知

授業連絡

2019/10/02 【授業連絡】 [滝] 情報処理基礎(23) (未読)

登録



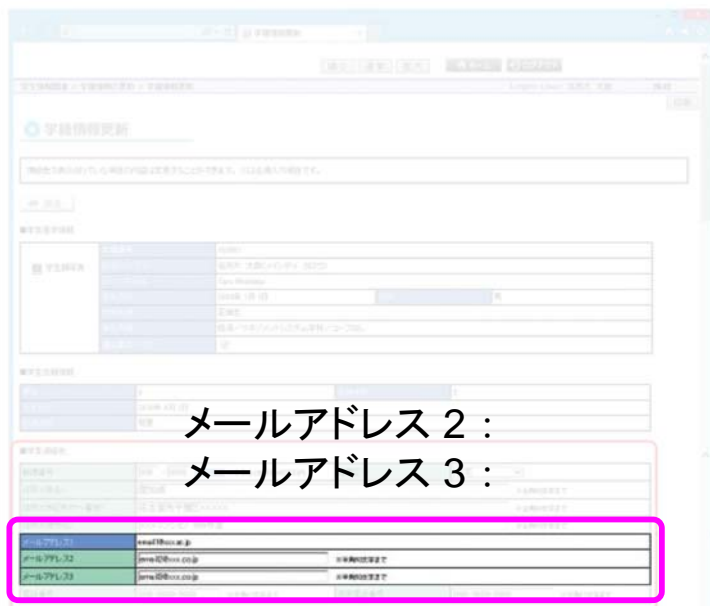
メールでも通知

メールアドレス 1 : c192599@ed.nagoya-cu.ac.jp

メールアドレス 2 : } 各自で登録
メールアドレス 3 : }

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



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

c191098 c183487 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
アカウントの種類 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 すべてのアカウントで 共通化	パスワード通知書 記載の8桁英数字	≪滝子(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 ≪松山(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		

SYSTEM GUIDE 2020 p.7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

The screenshot shows the Yahoo! JAPAN ID registration form. The following fields are highlighted with orange boxes and labels:

- ncu_nsc_miya**: Labeled "自分で決める" (I decide myself).
- pSw0Rd85**: Labeled "自分で決める" (I decide myself).
- A large yellow box at the bottom asks: "どのように保存されるのか?" (How is it saved?).

Other visible fields include: 半角英数字・記号()4~31文字, Yahoo!メールアドレス (ncu_nsc_miya@yahoo.co.jp), パスワードの安全性, パスワードを表示, 性別 (男性/女性), 秘密の質問 (父親の出身地は?), and 秘密の答え.

パスワードを設定する

ハッシュ化
(ある種の暗号化)

パスワード
pSw0Rd85



出力(ハッシュ値)

a403a4bb29c2d685
f6a196c51a019ad9



システムに保存

※ 厳密には暗号化とは異なります

ハッシュ関数

決まった手順で計算をする

あるデータ (サイズは任意) → 関数 (md5, sha1, sha256など) → 別のデータ (サイズは固定)

- ✓ 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

元データ		出力されたハッシュ値
miyahara1	md5	7c1f1de67cbdefcbe09d68033ef6535f
miyahara2	md5	30c61a05eede2d044953fe53962fda83 (16進表記)

パスワードを設定する

パスワード
pSw0Rd85



出力(ハッシュ値)

a403a4bb29c2d685
f6a196c51a019ad9



計算不可能

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

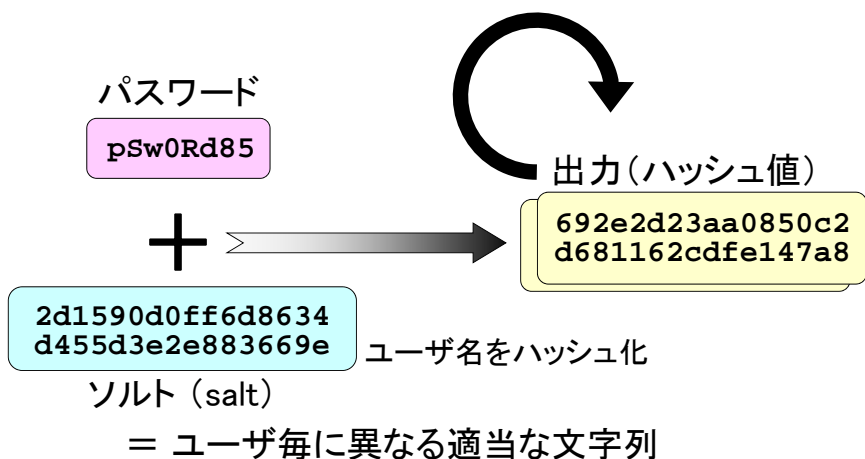
サーバ管理者が良く聞く言葉

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

- 辞書
 - 総当たり
- } → ハッシュ化 → 比較 

(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、   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?

||  すべてのパスワードが連動して変更される