第18回 迷惑メール対策カンファレンス × JPAAWG
A9 パネルディスカッション

A9 Panel Discussion

Internet Initiative Japan

トピック2: パスワードの定期変更問題

Topic 2: Periodic password changes issue

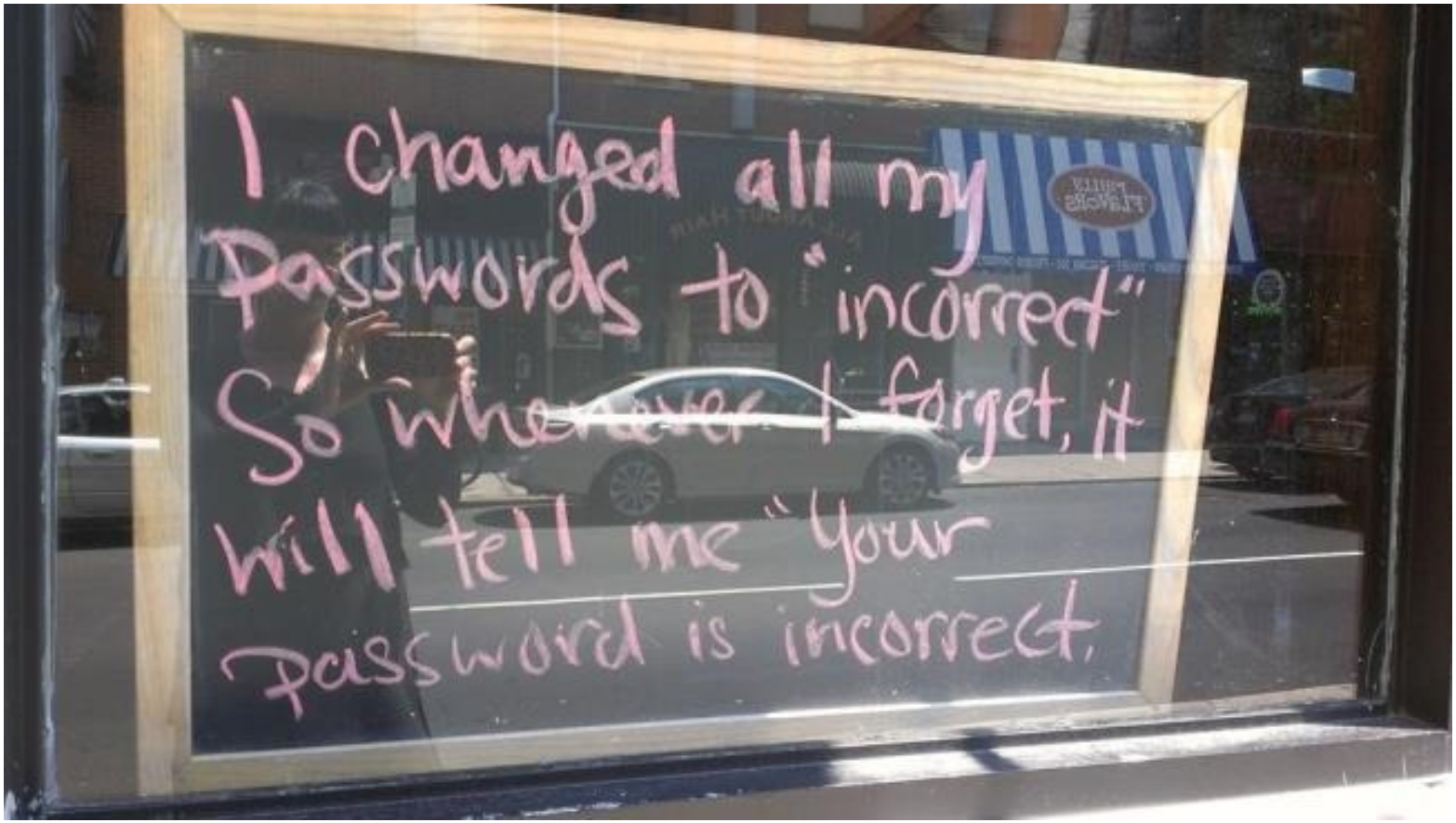
株式会社インターネットイニシアティブ (IIJ)
ネットワーク本部 アプリケーションサービス部
古賀 勇 (Isamu Koga)

Ongoing Innovation

議論に入るまえに

みなさんの社内システム、パスワードは定期変更必須ですか？

Is it nessesary to change the password periodically for your system that you use?

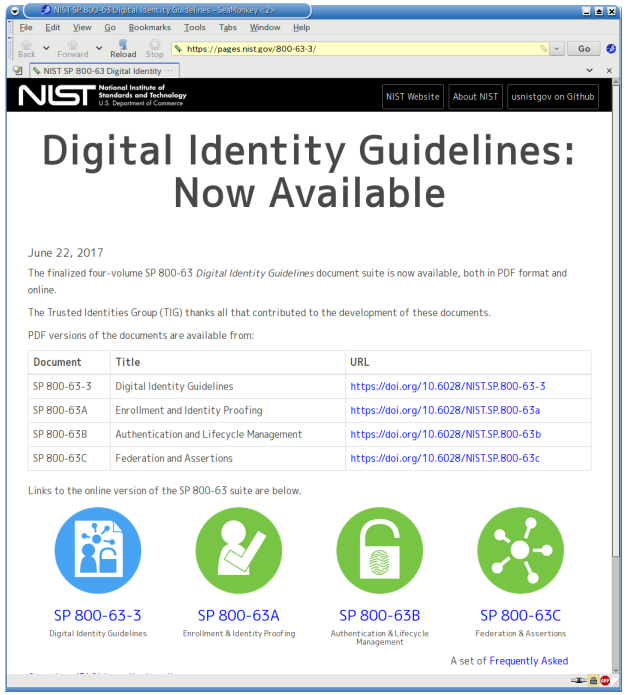


https://www.howtogeek.com/187645/htg-explains-should-you-regularly-change-your-passwords/

アメリカ国立標準技術研究所 (NIST)

- NIST SP800-63: Digital Identity Guidelines
  - https://pages.nist.gov/800-63-3/
  - 2017/06 に認証に関するガイドラインを発行

- 認証管理のありかたが明記されたことに注目を浴びる
  - NIST SP800-63B: Authentication and Lifecycle Management
  - 5.1.1.2 Memorized Secret Verifiers
  - メディアで「パスワード定期変更不要」と大きく報じられる



大きく報道された NIST の原文はココ
NIST sentence point of which it has been widely reported by mass media

5.1.1.2 Memorized Secret Verifiers (抜粋)

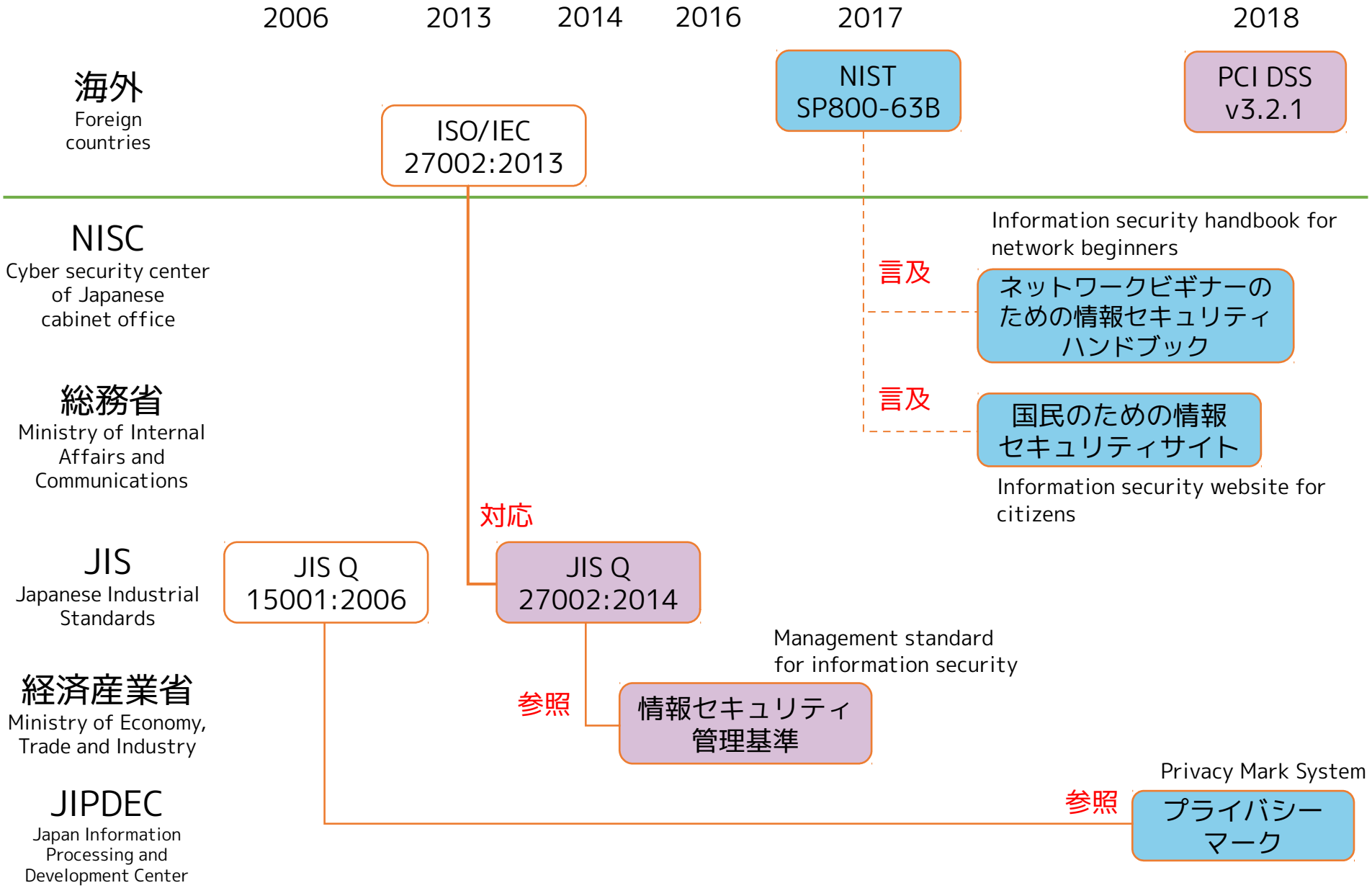
Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

- 生成ルールを強制しないのが望ましい（SHOULD NOT）
- 変更タイミングを強制しないのが望ましい（SHOULD NOT）
- しかし、盗用された証拠がある場合は変更を強制すべき（SHALL）

パスワードの定期変更にまつわる文献
Standards concerning periodic password changes

組織	表現	文書	最終更新日
内閣サイバーセキュリティセンター (NISC)	パスワードの定期変更は必要なし。流出時は速やかに変更する。	ネットワークビギナーのための情報セキュリティハンドブック https://www.nisc.go.jp/security-site/handbook/	2017/12
総務省 (Ministry of Internal Affairs and Communications)	定期的な変更不要…(略)…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。	国民のための情報セキュリティサイト http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html	2018/03
経済産業省 (Ministry of Economy, Trade and Industry)	9.4.3.5 パスワードの管理システムでは、パスワードは、定期的に及び必要に応じて変更させるようにする。	情報セキュリティ管理基準 http://www.meti.go.jp/policy/netsecurity/is-kansa/	2018/03
JIS (Japanese Industrial Standards)	e)パスワードは，定期的に及び必要に応じて変更させるようにする。	JIS Q 27002:2014 報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範 http://www.jisc.go.jp/	2014/03
プライバシーマーク (Privacy Mark System)	漏えいしたパスワードは、速やかに変更することを求めている。	JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン 第2版 https://privacymark.jp/system/guideline/outline.html	2018/04
PCI DSS (Payment Card Industry Data Security Standard)	8.2.4 ユーザパスワード/パスフレーズは、少なくとも1回は90日ごと変更する。	PCI DSS v3.2.1 https://ja.pcisecuritystandards.org/minisite/env2/	2018/05

パスワードの定期変更にまつわる規定・参照元
Regulations and references regarding periodic password changes



他にも色々書いてある
Source text from NIST (abstract)

5.1.1.1 Memorized Secret Authenticators

Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed.

- ユーザが設定する場合は最低 8 文字とすべき (SHALL)
- 管理者がランダムに設定する場合は最低 6 文字とすべき (SHALL)
  全部数字でも良い (MAY)
- 過去悪用されたものだった場合は別の文字列にすべき (SHALL)
- 他に複雑さを要求するのは望ましくない (No ～ SHOULD)

ただし
However,

報道された 5.1.1.2 章には続きがある
The chapter 5.1.1.2 which was reported continues ...

5.1.1.2 Memorized Secret Verifiers (cont.)

Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to:

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’).
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account as described in Section 5.2.2.

(abbr.)

Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets.

(abbr.)

The salt SHALL be at least 32 bits in length and be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

報道された 5.1.1.2 章には続きがある
The chapter 5.1.1.2 which was reported continues ... (abstract)

5.1.1.2 Memorized Secret Verifiers (続き・一部抜粋)

- 認証前にヒントを与えるべきでない (SHALL NOT)
- 秘密の質問に関する特定の情報を与えるべきでない (SHALL NOT)
- よく使われる言葉・想定される言葉のリストと比較し、以下のようなものは制限すべき（SHALL）
  - 過去盗用されたもの
  - 辞書に載っている単語
  - 繰り返しに連続性のあるもの
  - サービス名など特定の名称・ユーザ名・それらに似た言葉
- 認証失敗回数による制限を実装すべき（SHALL）
- コピー & ペーストを許可することが望ましい（SHOULD）
- オフライン攻撃に備えるため salt は、最低 32 ビットで一方向ハッシュ化すべき（SHALL）

...などなど、他にも様々なシステムへの要求が前提として書いてある

ディスカッションテーマ 1
Discussion 1

- 社内システムや所属している組織でパスワード定期変更を止める動きはありますか?
  Are there any moves to stop periodic password changes in internal systems or organizations that belong to?

ディスカッションテーマ 2
Discussion 2

- そもそもパスワードを定期的に変更したほうが良い根拠とは?
  At all, why is it necessary that you change the password periodically?

ディスカッションテーマ 3
Discussion 3

- 二要素認証対応への課題とは?
  What is a concern about two-factor authentication?

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――――――――――――――― IIJはいつもはじまりであり、未来です。

Ongoing Innovation