認証にまつわる セキュリティの新常識 rev.2

Internet Week ショーケース in 仙台| 2019.05.31 | 東北大学片平キャンパス

勝原 達也

勝原 達也/Tatsuya Katsuhara

㈱NDIAS所属(ndias.jp)

- 経歴
  - **デジタル・アイデンティティ** ← 本日の私
    - OpenID Foundation JAPAN
    - OAuth/OpenIDに関する開発
  - Web/プラットフォーム脆弱性診断
  - IoT/OT/重要インフラセキュリティ
  - ハードウェアセキュリティ
- 現在
  - コネクテッドカーのセキュリティ
  - 車両評価Gマネージャ

認証

日本語訳が根深い問題

ウィキペディア
フリー百科事典

メインページ
コミュニティ・ポータル
最近の出来事
新しいページ
最近の更新
おまかせ表示
練習用ページ
アップロード (ウィキメディア・コモンズ)

ヘルプ

ヘルプ
井戸端
お知らせ
バグの報告
寄付
ウィキペディアに関す

認証

出典: フリー百科事典『ウィキペディア（Wikipedia）』

認証（にんしょう）とは、何かによって、対象の正当性を確認する行為を指す。

目次 [非表示]


CERTIFICATION

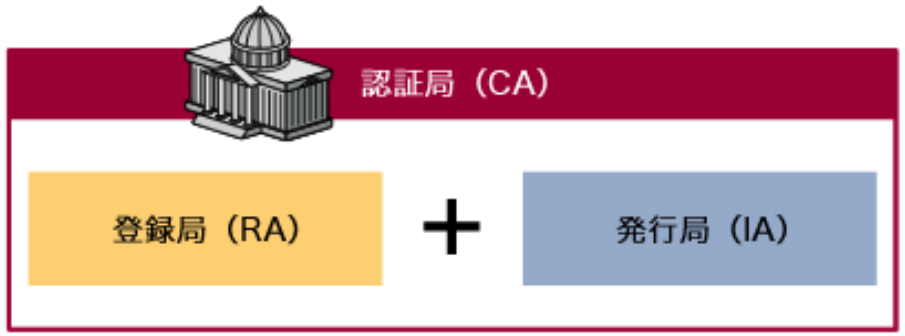

AUTHENTICATION

サポート

- FAQ
- マニュアル
- リポジトリ / 利用規約
- サポートお問い合わせ先

認証局 (CA)【Certificate Authority】

電子証明書の発行、効力停止、更新、または失効を行う権限を持つ主体。
認証局は登録局と発行局によって構成されています。



一般にCAは階層化されており、階層化することで信頼性を保ちつつ、電子証明書の運用体制に柔軟性を持たせることができます。最上位認証局は特にルート認証局(ルートCA)と呼ばれています。階層化された認証局では上位階層のCAが下位のCAに権限を与え、その認証局がまた別の(下位の)階層の認証局やユーザに権限を与えることによって電子証明書の信頼性を保持しています。この認可のプロセスの間は、一貫したポリシー(従属者の名前や階層のレベルなど)を持つように設計される必要があります。全ての階層の認証局がこれらの方針に従うことが、証明書階層の完全性を保証するのに重要となります。

SSLのご購入方法

- 新規の購入手続き
- 更新の購入手続き
- 他社からお乗換え

SSLの購入を申込む

ご購入お問い合わせ

デジサート・ジャパン・セキュリティ合同会社
TEL: 03-4578-0048
お問い合わせフォーム
見積書取得フォーム

SSL/TLS入門ガイド

- SSL/TLSの解説

https://www.geotrust.co.jp/support/glossary/ca.html

Europe

CE 0682

Apple's EU Representative
Apple Distribution International
Hollyhill, Cork, Ireland.

Japan

🅃ADF160081003
🅁003-160134

5.0 GHz (W52, W53): Indoor Use Only
総務省指定 第EC-16006号

MIC/KS

Tweets 42.1K | Following 47 | Followers 60.7M | Likes 7 | Moments 6

Donald J. Trump

@realDonaldTrump

45th President of the United States of America🇺🇸

Washington, DC

Instagram.com/realDonaldTrump

Joined March 2009

Tweet to Donald J. Trump

24 Followers you know

Tweets | Tweets & replies | Media

Donald J. Trump Retweeted

TheHillOpinion @TheHillOpinion · May 30

Shame on Robert Mueller for exceeding his role

Read the full story:
bit.ly/2QxOAnd

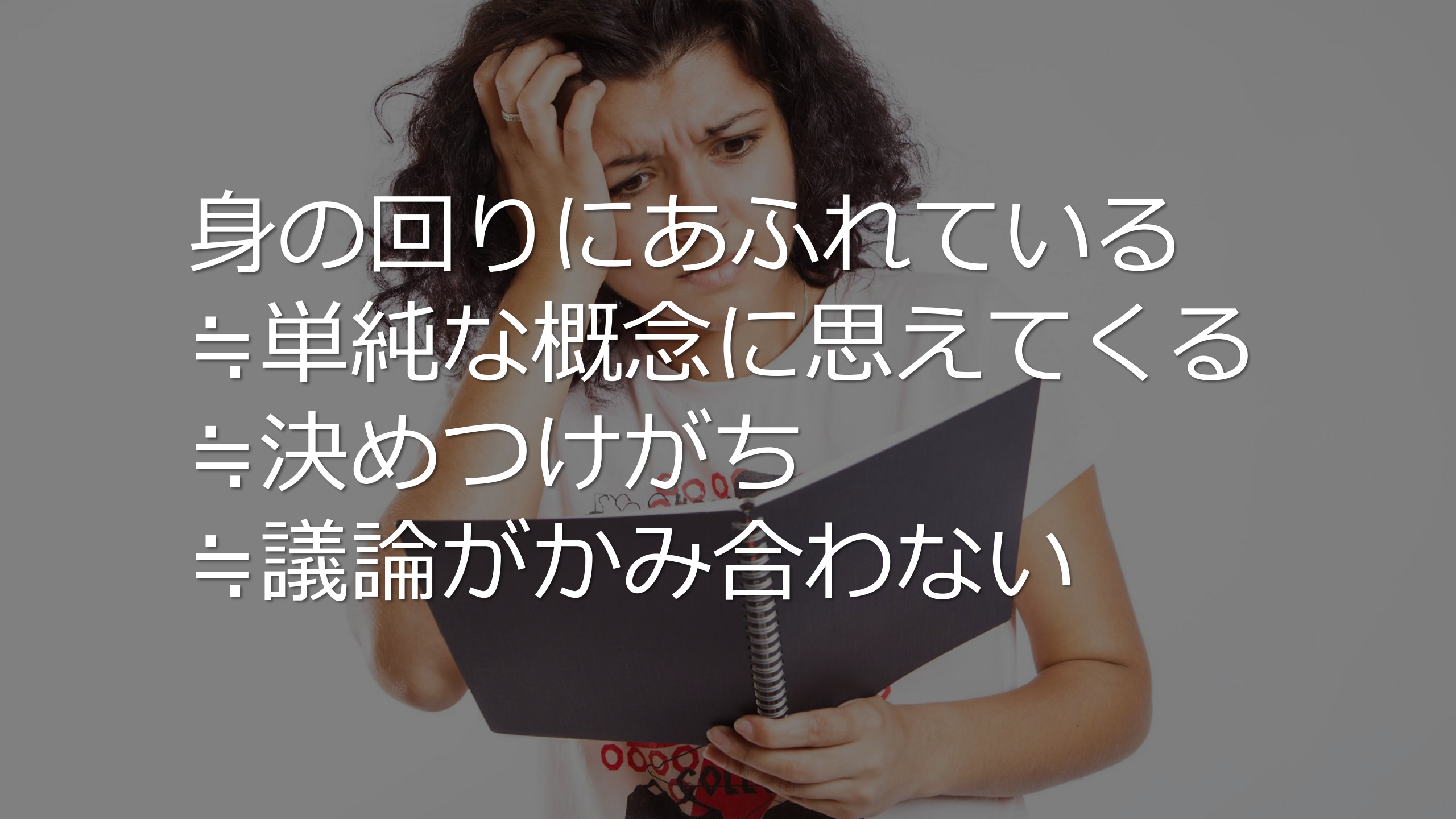
Via: @AlanDersh

Who

Cross Certification

相互認証

Mutual Authentication



身の回りにあふれている
≒単純な概念に思えてくる
≒決めつけがち
≒議論がかみ合わない

本日のテーマ
認証／Authentication

本日お伝えしたいこと

- **認証およびデジタルアイデンティティを考えるために有用な共通言語をNIST SP800-63-3の考え方を通じて知る**
- **認証にフォーカスした63Bを通じてAuthenticator種別を知る**
- **SP800-63-3の改定の過程で巻き起こった議論と、その背景にあるメッセージを考えてみる**
- **デジタルアイデンティティのセキュリティの面白さを知る**

OIDFJでの活動 兼 趣味で翻訳

https://openid-foundation-japan.github.io/800-63-3-final/

https://pages.nist.gov/800-63-3/

NIST SP800-63-3とは

- NIST SP800-63-3は**米国政府機関向け**に、デジタルアイデンティティフレームワークについて言及したガイドライン
- **日本の事業者には何ら役務が発生することはない**
- エッセンスと考え方はとても有用で、**様々な業界から参照されている**
- Fit&Gapしてリスク分析して**流用することは良いアプローチ**(なはず)

NIST SP800-63-3とは

	デジタル認証のガイドライン	登録プロセス 身元確認	認証とライフサイクル管理	フェデレーションとアサーション
興味キーワード	NIST SP800-63-3全体概要	本人確認 身元確認 窓口での対面確認 写真付き身分証明書 映像での遠隔身元審査 犯罪収益移転防止法 KYC(Known Your Customer)	パスワード認証 パスワード定期変更 秘密の質問 多要素認証 SMS認証 バイオメトリクス アカウントリカバリ	Federated Identity Single Sign On(SSO) SAML OAuth2.0 OpenID Connect Web API Authorization Identity Platform

NIST SP800-63-3とは

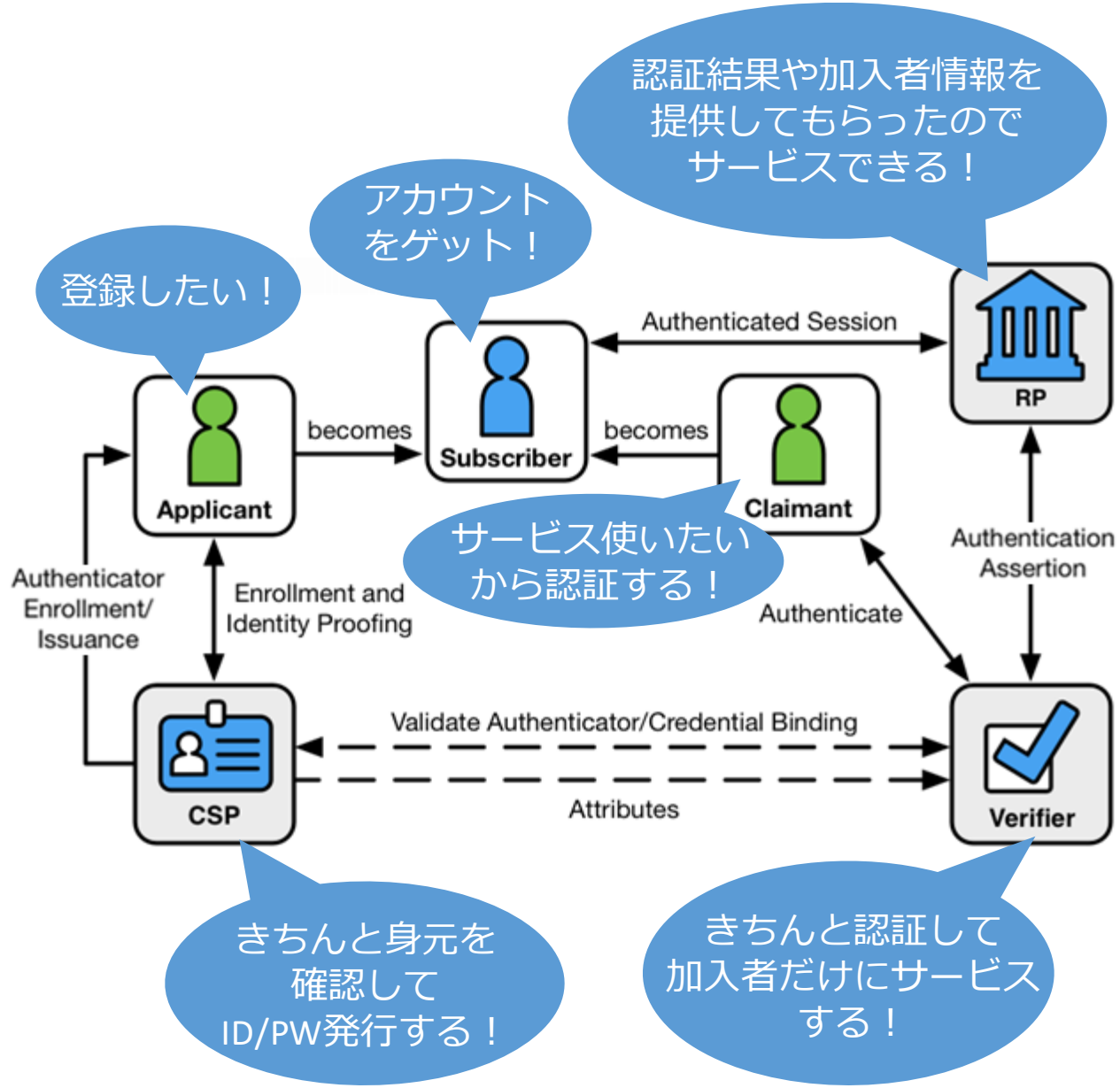
本日の対象

			例えば銀行	例えばECサイト
 SP 800-63A	**ユーザ身元確認の確からしさ**	**IAL 1-3 (Identity Assurance Level)**	2	1
 SP 800-63B	**ユーザ認証の確からしさ**	**AAL 1-3 (Authenticator Assurance Level)**	2	2
 SP 800-63C	**連携方法の確からしさ**	**FAL 1-3 (Federation Assurance Level)**	2	—

63Bもくじ

本日の対象

目次	内容
4. Authenticator Assurance Levels 5. Authenticator及びVerifierの要件 付録A ― 記憶シークレットの強度	• AAL毎の要件と、それに合致するAuthenticatorの話 • Authenticatorの種類や、備えるべき機能の話
6. Authenticatorライフサイクルの要件	• Authenticatorの発行、紛失、盗難、破棄などの要件
7. セッション管理	• セッションCookie、AccessToken、再認証など認証後のセッション維持とその保護に関わる話
8. 脅威とセキュリティに関する考慮事項 9. プライバシに関する考慮事項	• AuthenticatorやSessionに関するリスク要因および対策 • プライバシーリスクアセスメント、コントロールなどの話
10. ユーザビリティに関する考慮事項	• Authenticationのユーザビリティとビジネス影響 • Authenticatorライフサイクルを通じたユーザビリティ確保



用語

- **ユーザは文脈で区別される**
  - Applicant→Subscriber→Claimant
- **Credential Service Provider**
  - Applicant情報を確認・検証・登録
  - SubscriberへAuthenticatorを発行
- **Authentication(認証)**
  - ClaimantがSubscriberであることを、Authenticatorを用いて確認する行為
- **Verifier**
  - Authenticatorの出力を見て、Subscriberかどうかを確認する
- **Relying Party**
  - Verifierの確認結果に基づいて、認証済みセッションを開始

Authenticatorのタイプ

#	原文	和訳	認証要素 Something you ***	暗号プロトコル(鍵の所持証明)の性質があるか	HWとして認められるか
1	Memorized Secret	記憶シークレット	知識	No	No
2	Look-up Secret	ルックアップシークレット	所有	No	No
3	Out of Band Device	経路外デバイス	所有	No	No
4	SF OTP Device	単一要素OTPデバイス	所有	No	Yes/No※
5	MF OTP Device	多要素OTPデバイス	所有+知識/生体	No	Yes/No※
6	SF Cryptographic Software	単一要素暗号ソフトウェア	所有	Yes	No
7	SF Cryptographic Device	単一要素暗号デバイス	所有	Yes	Yes
8	MF Cryptographic Software	多要素暗号ソフトウェア	所有+知識/生体	Yes	No
9	MF Cryptographic Device	多要素暗号デバイス	所有+知識/生体	Yes	Yes

※「デバイス」という呼称と、HWとして認められるかが一致しないので少々トリッキー

Authenticatorのタイプ

#		Authenticatorのタイプ	内容
1		Memorized Secret 記憶シークレット	ユーザが記憶するもの。 例：パスワードやPIN ※ローカル／リモートどちらであるか問わない。
2		Look-up Secret ルックアップシークレット	Claimant（認証をしたい人）とCSP（認証情報を登録・払い出す側）の間で共有されているシークレット。 例：乱数表、Googleアカウントの二要素認証のリカバリコードのようなもの
3		Out of Band 経路外 (RESTRICTED)	セカンダリチャネルを介してVerifierと安全に通信できるようなもの。 例：SMSによるコード送信、QRコード読み取り、電話によるコード読み上げ／入力 ※今回の改定で、EメールやVoIPはセカンダリチャネルとして認められないとされた点に注意。

Authenticatorのタイプ

#		Authenticatorのタイプ	内容
4		SF OTP Device 単一要素OTPデバイス	二要素目の入力によるアクティベーションを必要とせず、所持していることで認証を実施できる。 例：パスフレーズ入力不要なOTPデバイス（物理OTPトークンや、Google Authenticatorなどスマホにインストールしたソフト含む）
5		MF OTP Device 多要素OTPデバイス	SF OTP Deviceに更に二要素目の入力によるアクティベーションを追加したもの。 例：（スマホのロック解除とは別に）Touch IDやマスタPWでアクティベートするOTPアプリ
6		SF Cryptographic Software 単一要素暗号ソフトウェア	ディスクあるいはソフト媒体に記録された一意な暗号鍵。鍵はデバイス上で最もセキュアなストレージに保存されており、アクセスコントロールが施されている。 例：端末毎のクライアント証明書（PW保護無し）
7		SF Cryptographic Device 単一要素暗号デバイス	保護された暗号鍵を用いて認証を行うハードウェアデバイス。鍵はデバイスで一意であり、エクスポートできてはいけない。 例：FIDO U2FのUSBドングル(挿すだけ)

Authenticatorのタイプ

#	Authenticatorのタイプ	内容
8	 MF Cryptographic Software 多要素暗号ソフトウェア	単一要素暗号ソフトウェアに対して、更にアクティベートするための2要素目が必要となったもの。 例：指紋認証を行うことで有効化されるクライアント証明書
9	 MF Cryptographic Device 多要素暗号デバイス	単一要素暗号デバイスに対して、更にアクティベートするための2要素目が必要となったもの。 例：パスワードまたはバイオメトリクスでアクティベートしなければ利用できないようになっているUSBトークン、指紋認証や顔認証でセキュアエレメントをアクティベートするようなFIDO対応スマホ。

注）なるべく具体例を入れていますが、NISTの基準においてFIPS140 Approvedかどうかなどが影響するため、厳密には該当しない場合があります。

AAL(Authenticator Assurance Level)

- 「Claimant＝Subscriberであること」の確認(認証)の信頼性を3段階に分類したもの
- 観点は複数あり、**同時に満たした場合**に当該レベルに適合
- 認証要素（Something you ***）は**同じ要素を2つ使っても1要素とカウント※**
- 利用する暗号アルゴリズム要件は63-3記載の「承認済み(Approved)」なものを利用

要求事項	AAL 1	AAL 2	AAL 3
許容される Authenticator タイプ	• **9タイプ全部OK（何でも良い）**	• **Authenticator単独で2要素以上** • **またはPW(知識)＋2要素目(所有,特徴)**	• **2要素以上** • **暗号鍵の所持証明要素** • **ハードウェア関与**
	• 記憶シークレット • ルックアップシークレット • 経路外 • 単一要素OTPデバイス • 多要素OTPデバイス • 単一要素暗号ソフトウェア • 単一要素暗号デバイス • 多要素暗号ソフトウェア • 多要素暗号デバイス	• 多要素OTPデバイス • 多要素暗号ソフトウェア • 多要素暗号デバイス • 記憶シークレット＋以下 　• ルックアップシークレット 　• 経路外 　• 単一要素OTPデバイス 　• 単一要素暗号ソフトウェア 　• 単一要素暗号デバイス	• 多要素暗号デバイス • 単一要素暗号デバイス＋記憶シークレット • 多要素OTPデバイス(SW/HW)＋単一要素暗号デバイス • 多要素OTPデバイス(HW)＋単一要素暗号ソフトウェア • 単一要素OTPデバイス(HW)+多要素暗号ソフトウェア • 単一要素OTPデバイス(HW)+単一暗号ソフトウェア+記憶シークレット

※単一要素を複数用いた場合の認証強度を否定するものではないが、尺度の基準を統一することが難しい。そのため「多要素」という考え方ありき。

AAL(Authenticator Assurance Level)

要求事項	AAL 1	AAL 2	AAL 3
許容される Authenticatorタイプ	• 9タイプ全部OK（何でも良い）	• Authenticator単独で2要素以上 • またはPW(知識)＋2要素目(所有,生体)	• 2要素以上 • 暗号鍵の所持証明要素 • ハードウェア関与
FIPS 140適合	Level 1 (政府機関のVerifier)	Level 1 (政府機関のAuthenticator及び Verifier)	Level 1 総合 (Verifier及び単一要素暗号デバイス) Level 2 総合 (多要素Authenticator) Level 3 物理セキュリティ (全てのAuthenticator)
再認証	30 日	12 時間または30分間活動なしの場合に、1つの認証要素を利用して再認証(任意)	12 時間または15分間活動なしの場合に、 両方の認証要素を利用して再認証(必須)
セキュリティ統制	[SP 800-53] 低い基準 (または 等価なもの)	[SP 800-53] 中度の基準 (または等価なもの)	[SP 800-53] 高い基準 (または等価なもの)
中間者攻撃耐性	必須	必須	必須
Verifierなりすまし耐性(Phishing耐性)	不要	不要	必須
Verifier改竄耐性	不要	不要	必須
リプレイ耐性	不要	必須	必須
認証意図 (AuthN Intent)	不要	推奨	必須
レコード保持ポリシ	必須	必須	必須
プライバシ統制	必須	必須	必須

読む際のコツ：要求記法および規則

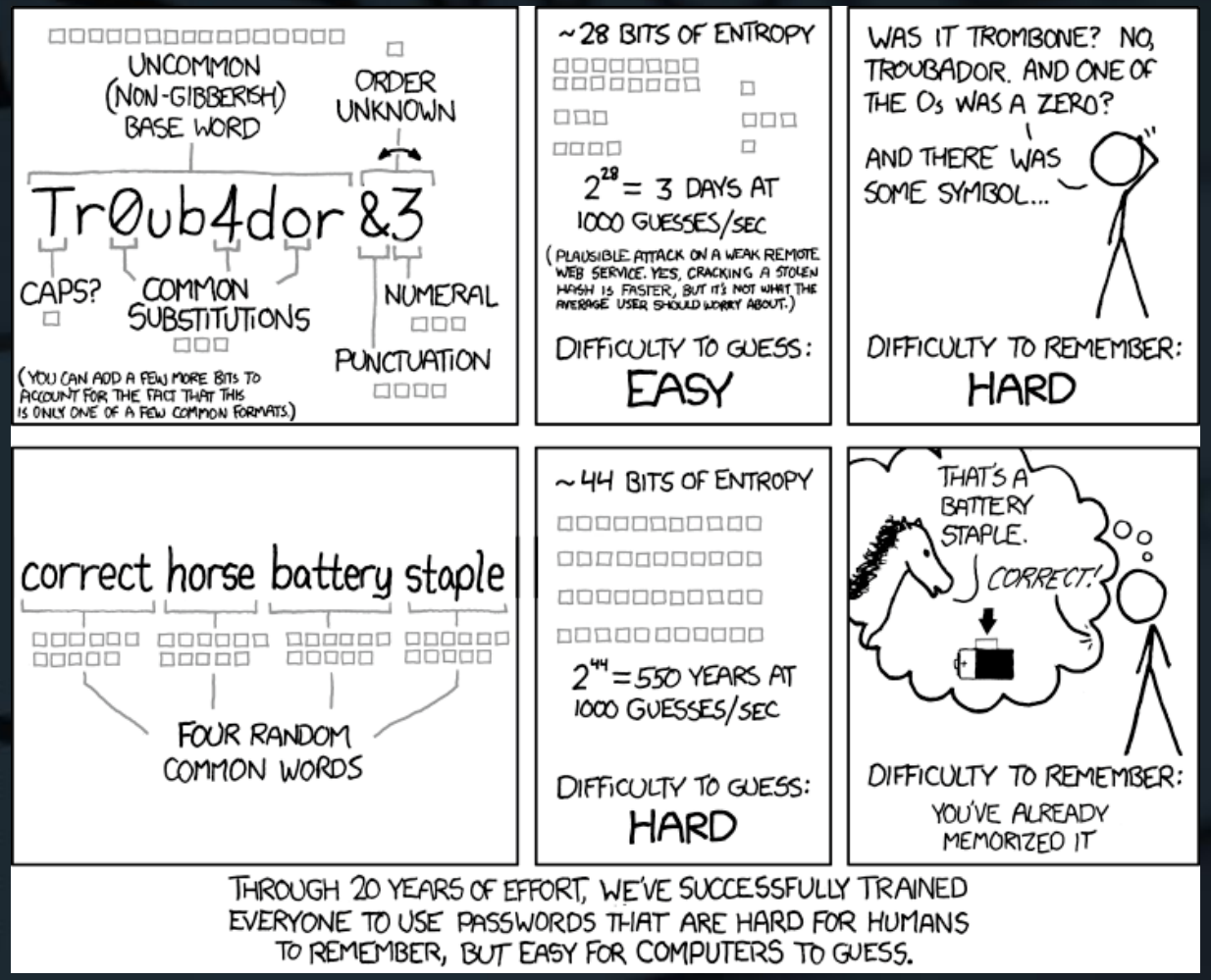
- **SHALL(するものとする)およびSHALL NOT(しないものとする)**
  - 厳密に従うことを要求しており、内容と異なってはならない。

- **SHOULD(すべきである)およびSHOULD NOT(すべきではない)**
  - いくつかある選択肢の中で特定の推奨があることを示している。
  - 他の選択肢については言及も除外もしない。
  - **行動指針を推奨するが、必須であることまでは要求しない。（微妙な表現）**

- **MAY(してもよい)およびNEED NOT(しなくてよい)**
  - 行動指針が許容できることを示す。

- **CAN(できる)およびCANNOT(できない)**
  - 物質的、物理的、偶発的であるかに関わらず 可能性や能力があること。

パスワードからパスフレーズへ



https://xkcd.com/936/

パスワードからパスフレーズへ

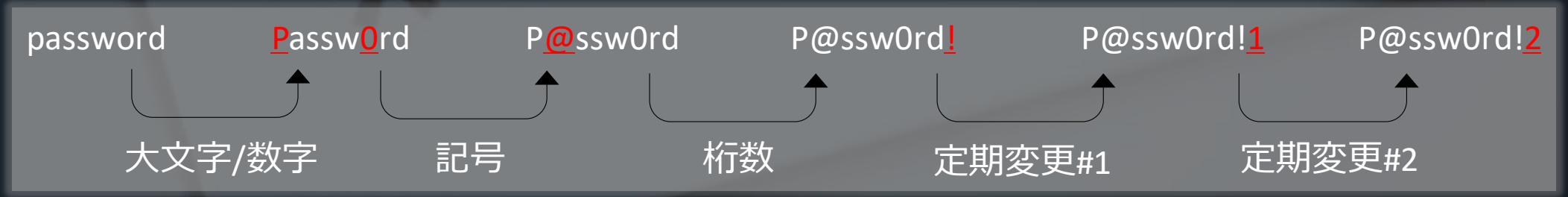
- **パスフレーズ前提**
  - 8文字以上(ランダム生成なら6文字以上)(SHALL)
  - 最低64文字(SHOULD)
  - 空白/Unicode(SHOULD)
  - 他には複雑さ要件を課さない(SHOULD)
- **リスト突合で弱いPWをはじく(SHALL)**
  - 漏洩PW、辞書、繰り返し/連番、文脈で特定
- **ペースト機能(SHOULD)**
  - パスワードマネージャ連携/使いまわし改善
- **可視化(SHOULD)**
  - ラスト1文字表示、トグルで表示/非表示など
- **パスワード強度メーター(SHOULD)**
  - (強度を正しく伝えられるかの議論あり)

パスフレーズを推奨し、桁数を伸ばす方向へ誘導することで、総合的にセキュリティ向上を図っていくというメッセージ。

パスワード定期変更を求めない方向性

「ユーザに対し定期変更を要求すべきではない」(SHOULD)
「パスワードが危殆化した可能性があれば変更強制」(SHALL)
→危殆化したことに気づくことができるかという課題も。

- 定期変更を通じてユーザは「弱いパスワード」を使うようになるので、結局は突破されがち、という考えに基づく。
  https://pages.nist.gov/800-63-FAQ/
- 米ノースカロライナ大学の研究(過去パスワードが分かれば、17%のユーザは5回以内の試行で現在パスワードが特定できる)
  https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes



完全に廃止された「秘密の質問」

- SP800-63-2では”Pre-registered Knowledge Token”と呼称。
  - Knowledge Based Authentication(KBA)とも言われる。
- SP800-63-3では記憶シークレットの一部として扱われ、**「やってはいけない」(SHALL)記憶シークレットの例**としてわざわざ記載されることになった。（例：ペットの名前）
- **「アカウントリカバリ」の難易度が増加。**
  - 生年月日（ソーシャルエンジニアリングの餌食なので問題外）
  - メールアドレス（経路外Authenticatorでは禁止だが・・・）
  - SMS（RESTRICTEDだが・・・）

地味に影響しそうな乱数表の制限追加

- **各セルの値の使い回しが禁止** (SHALL)
  - NISTは「日本的」な乱数表の利用は考慮されていない
  - 二要素認証の有効化時に発行されるような「**回復コード表**」は許容

以前
何回でもセルの値を使ってよい。

日本における乱数表イメージ
（例：キャッシュカード裏面）

	あ	い	う	え	お
A	11	12	13	14	15
B	21	22	23	24	25
C	31	32	33	34	35

今後
各セルは1回しか使えない。

バイオメトリクスの位置付け

単独でAuthenticatorとして認めないが、2要素目として補助的には利用して良い

理由はいくつか挙げられている。

- False Matching Rate(誤合致率)が低く抑えられようと、認証行為の確実性に繋がるわけではない。
- バイオメトリクスは**確率的**なもの
- 特徴点情報(テンプレート) の保護や無効化の標準不在
- バイオメトリクス特性は**シークレットではない**
  - プレゼンテーション攻撃を防ぐPADは今後必須要件になる見込み。

経路外認証は使えるが”RESTRICTED”

- ドラフト改訂の当初は、公衆交換電話網(PSTN)を使っている場合、SMSの経路外認証は非推奨になり、大盛り上がり
  - 最終的には**”RESTRICTED”という経過観察的な処遇。**

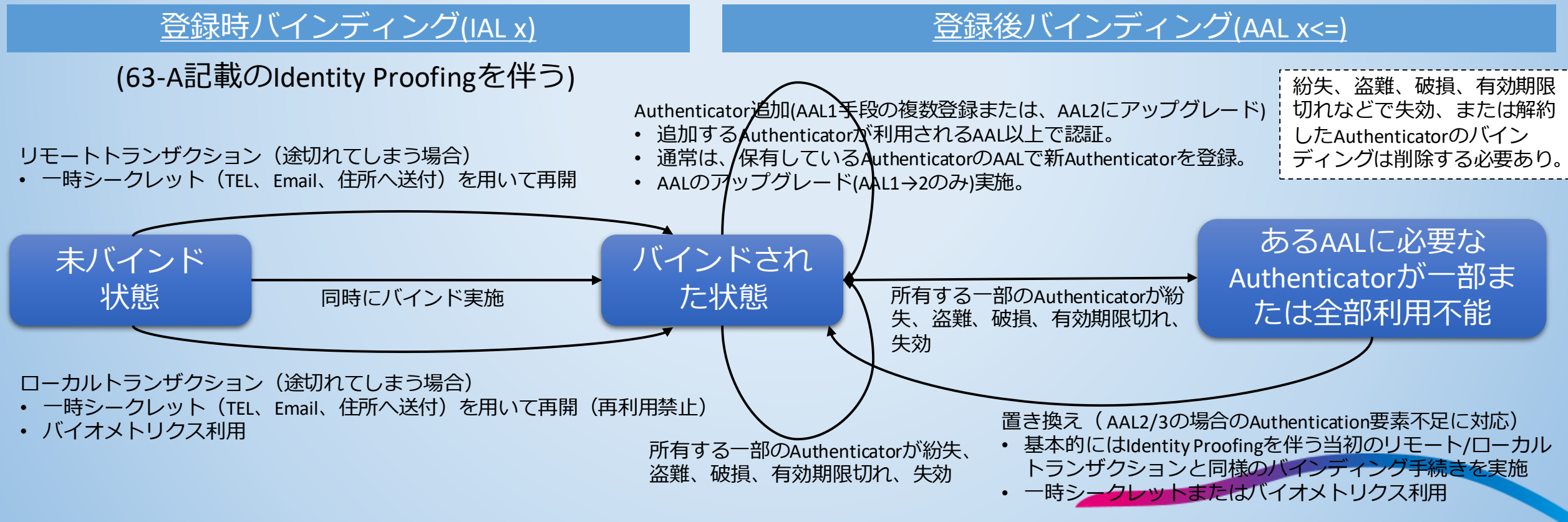
- 他にも事業者にとって重要な要件がいくつか
  - **VoIP/EメールはNG**（特定デバイスの所持証明にならない）(SHALL)
  - 事前登録済みの電話番号は**物理デバイスと結びついていること**を確認
  - **スマホのPush通知インフラ**はセカンダリチャネルとして有効

- **「アカウントリカバリ」は特別な要件が追加**
  - 電話番号の変更は新しいAuthenticatorのバインディングとみなされる。

バインディング

- Authenticatorの**登録・追加・交換・廃止**のプロセス。
- ライフサイクルを通じて、**AAL維持を意識したプロセス**が必要。

63B記載内容から作成した簡易な状態遷移例



AALを意識したアカウントリカバリは難しい

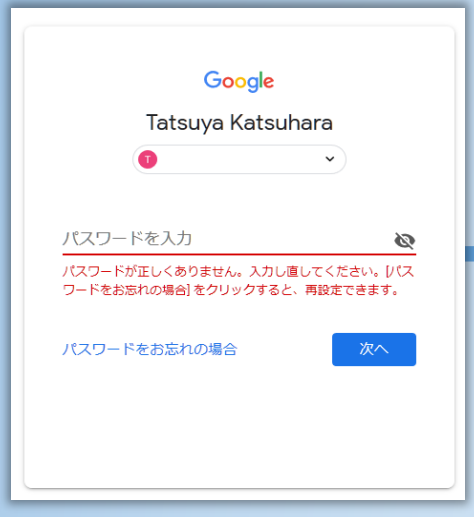
- アカウントリカバリは難しく脆弱になりがち≒狙われやすい

- パスワードを覚えていれば、2要素でのリカバリには定石あり
  - パスワード(知識)＋アカウントの回復コード(所有)
  - スマホ紛失でOTPアプリが使えない、などの問題解決

- パスワードを忘れると、2要素でのリカバリは難しい
  - 別のパスワードを事前登録・・・どうせそれも忘れる＆秘密の質問NG
  - 指紋を予め登録しておけば・・・ハードル高い

パスワード忘れのリカバリはイレギュラー

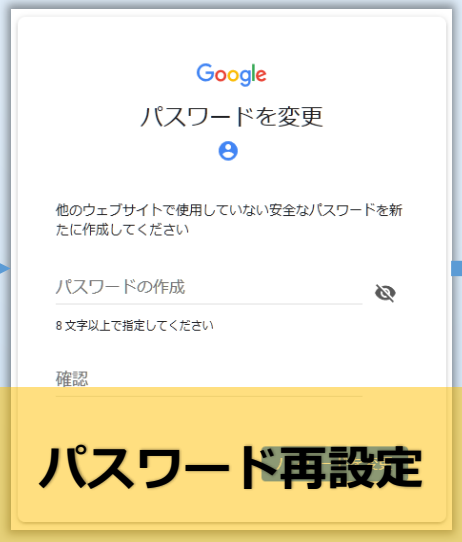
- 「物理」Authenticatorを2つ使いつつ、確認コード送付/検証(MAY)という方法が例示されているが・・・
- 2要素確保できない代わりに2物理Authenticator
- 郵送で確認コード送付(物理/経路外)＋USBキー(物理/所有)
- 本当に「物理」Authenticator使わないといけないの？



登録済みの認証要素いずれか
(FIDO, OTP, SMS, 回復コード)
※全て「所有」要素

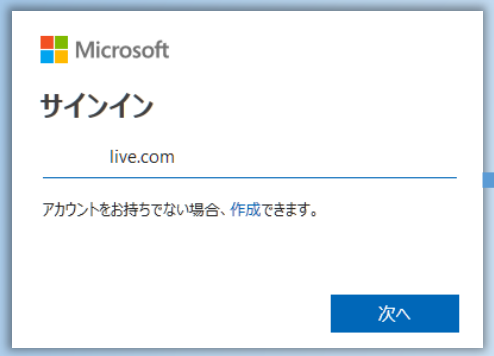
確認コードを
メールアドレスに
送信開始

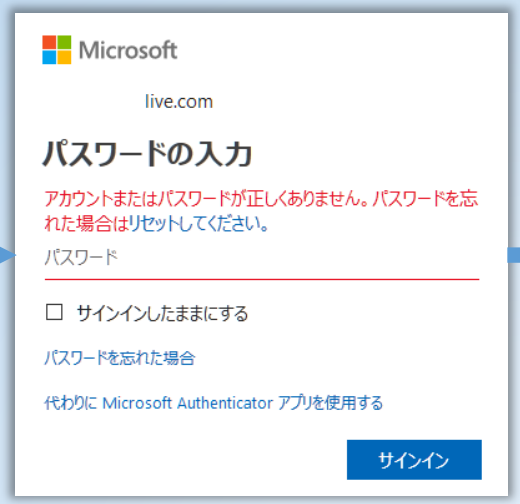
受信した
確認コードを入力

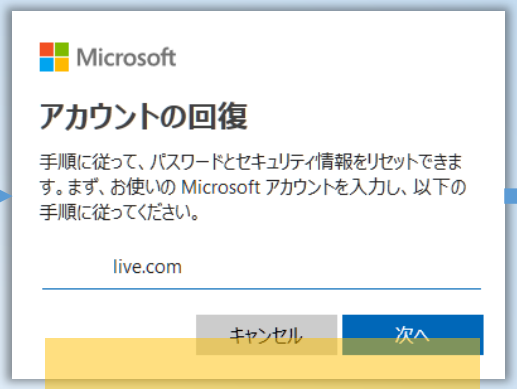


パスワード再設定

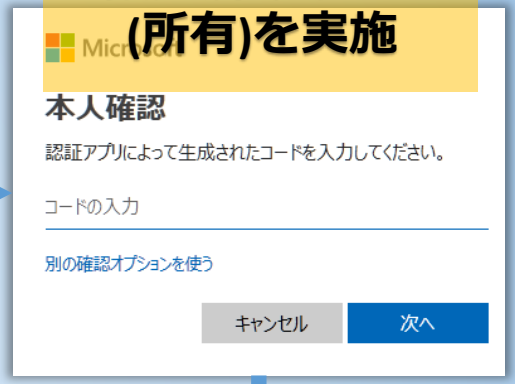
2段階認証(認証要素は1つ)で
ログイン完了





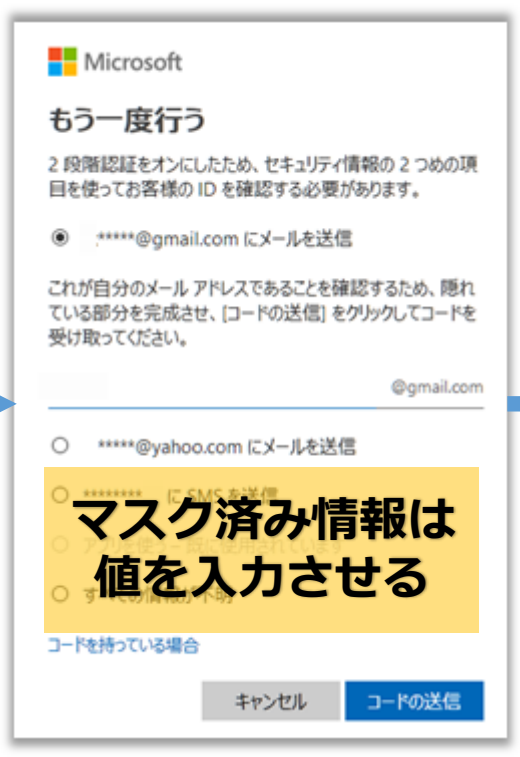


アカウントを識別



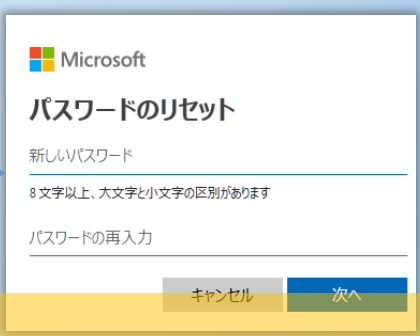
設定済みのOTP(所有)を実施

登録済みの認証要素どれか(メール、SMS, 回復コード)
※OTPは使用済み判定
※Windows Helloで生体要素が増えるかも。



マスク済み情報は値を入力させる

メールアドレス/SMSに届いた確認コードを入力



2段階認証(認証要素は1つ)でログイン完了

Eメールの取り扱いには曖昧さが残る

- Google/Microsoftでは「Eメール」での確認コード送付も活用
  - FIDOドングル、OTP、SMS、回復コード、Eメールの組み合わせ。
  - 「所有」1要素になりがちだが、2つの手段の利用はきっちり実施。

- アカウントリカバリ時の確認コード送付は根深い問題
  - 経路外AuthenticatorとしてのEメールは使えない(SHALL)としながらも「現実的には使わざるをえない」というのが、コンシューマ向けサービスでの落とし所と言えそう。
  - IAL2,3において「Identity Proofingを伴う当初のリモート/ローカルトランザクションと同様のバインディング手続きを実施」することが例示されており、Eメールによるリカバリが有効という解釈と考えられるが・・・(→バインディング参照)

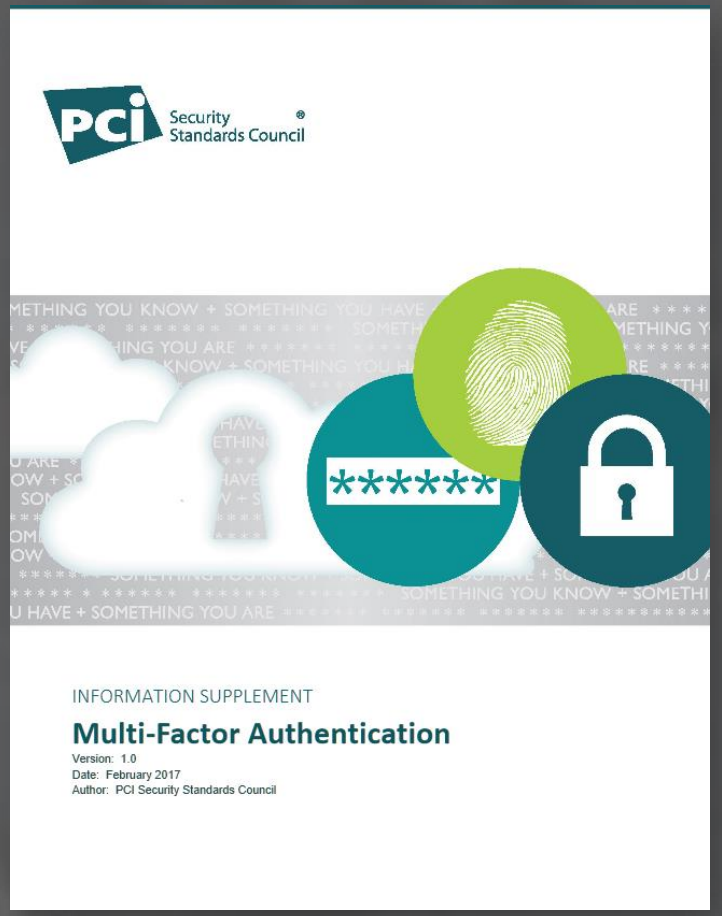
派生トピック：PCI DSS

https://www.flickr.com/photos/31176607@N05/with/34684294971/

Multi-Step vs. Multi-Factor

- アクセス許可するまえに全ての要素の認証が成功しなければならない。

- **全ての要素が提示されるまで認証の成否が分かってはならない。**

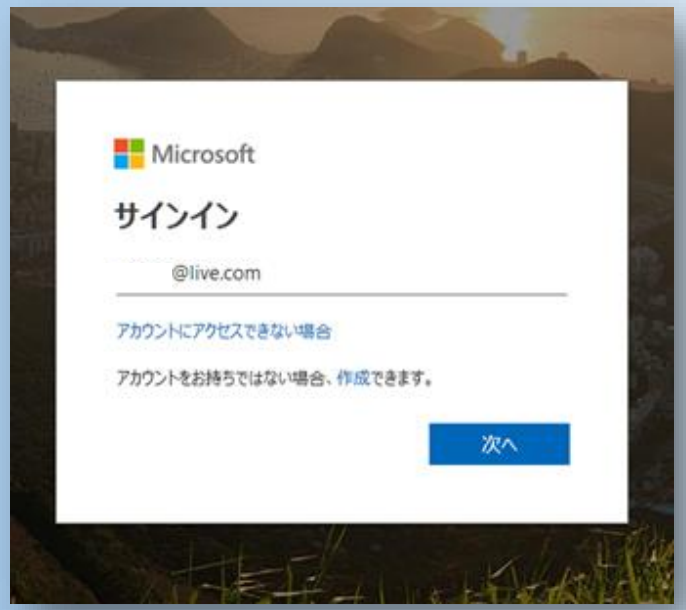


“Multi-Factor Authentication version 1.0”
https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf

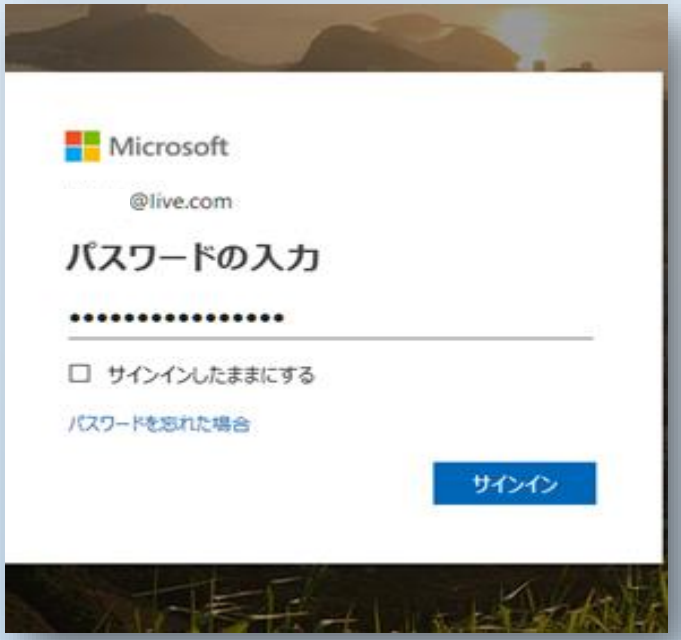
MicrosoftはNGということ?

- Multi-StepかつMulti-Factorな認証UX。
- 識別後に1要素目の認証。それが成功してから2要素目の認証。

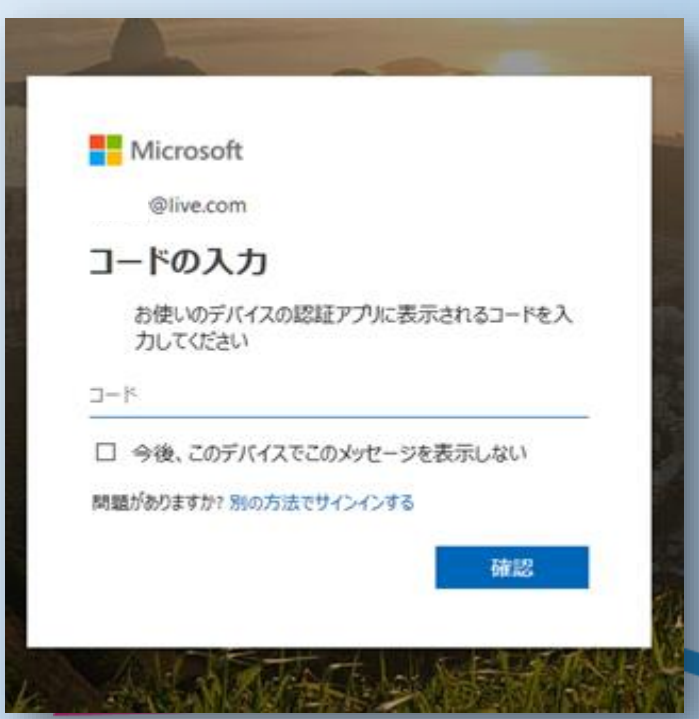
まずは識別



1次認証
(Something you know)



1要素目で認証済みの状態で
2要素目(Something you have)で2次認証



GoogleはNGということ?

- Multi-StepかつMulti-Factorな認証UX。
- 識別後に1要素目の認証。それが成功してから2要素目の認証。

まずは識別

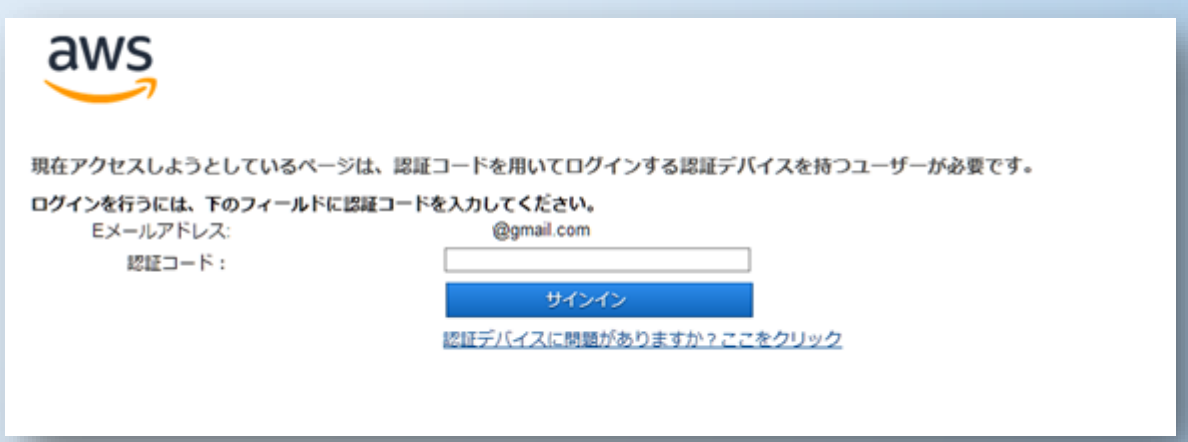
1次認証
(Something you know)

1要素目で認証済みの状態で
2要素目(Something you have)で2次認証

AWSはNGということ?

- Multi-StepかつMulti-Factorな認証UX。
- 識別後に1要素目の認証。それが成功してから2要素目の認証。

まずは識別	1次認証 (Something you know)	1要素目で認証済みの状態で 2要素目(Something you have)で2次認証



結局Multi-Step AuthenticationはOKに

- コミュニティでの質問が相次ぎ、条件付きで認められることに。

https://blog.pcisecuritystandards.org/faq-is-two-step-authentication-acceptable-for-pci-dss-requirement-8.3

- 3つの認証要素のうち最低2つを利用すること。
- ある認証メカニズムは、別のものと「独立」であること。
  - ある認証要素が別の認証要素へのアクセス許可をあたえない。
  - ある認証要素の危殆化が、別の認証要素の一貫性・機密性に影響しない。
- 「独立でない」例
- ID/PW認証後に発行された認証コードの受け取りメールアカウントに、同じID/PWを用いている場合。
  →結局ユーザ依存な側面が残っている。

PCI DSSではパスワードの定期変更が残る

- 「パスワード定期変更」については最新v3.2.1でも要件が残ったまま

- システム運用に関わる「非コンシューマ」に対しては効果ありという立場
  - 「人間のいい加減さ」を軽減して、期待した効果が得られる可能性はある

- 2020年に次期改定があるため、そのタイミングでの取り込み方に注目

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。	**8.2.4.a** システムコンポーネントのサンプルについて、システム構成設定を調べて、少なくとも 1 回は 90 日ごとにパスワード/パスフレーズを変更することを要求するようにユーザパスワードのパラメータが設定されていることを確認する。	長期間変更せずに有効なままになっているパスワード/パスフレーズは、悪意のある者がパスワード/パスフレーズを解読する行為により長い時間を与えることになります。 *注：テスト手順 8.2.4.b は事業体がサービスプロバイダを評価する場合のみの追加の手順です。*
	8.2.4.b サービスプロバイダの評価のみの追加のテスト手順。内部プロセスおよび顧客/ユーザ文書を調べて、以下を確認する。 • 非消費者の顧客ユーザパスワード/パスフレーズを定期的に変更することが要求されている • 非消費者の顧客ユーザに、いつどのような状況下でパスワード/パスフレーズを変更する必要があるかについてのガイダンスが与えられている	

派生トピック：Microsoft

遂にクライアント/サーバosポリシーも変更に

Microsoft | TechNet

Microsoft Security Guidance blog

Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903

Rate this article ★★★★★

Aaron Margosis May 23, 2019

Share 100 0 0 3

Microsoft is pleased to announce the *final* release of the security configuration baseline settings for Windows 10 version 1903 (a.k.a. "19H1"), and for Windows Server version 1903.

Download the content from the Microsoft Security Compliance Toolkit (click Download and select Windows 10 version 1903 and Windows Server Version 1903 Security Baseline.zip).

Note that Windows Server version 1903 is Server Core only and does not offer a Desktop Experience (a.k.a., "full") server installation option. In the past we have published baselines only for "full" server releases of Windows Server 2016 and 2019. Beginning with this release we intend to publish baselines for Core-only Windows Server versions as well. However, we do not intend at this time to distinguish settings in the baseline that apply only to Desktop experiences as opposed to Server Core, those settings are inert for all intents and purposes.

This new Windows Feature Update brings very few new Group Policy settings, which we list in the accompanying documentation. This baseline reconfigures only two of those. However, we have made several changes to existing settings, including some changes since the publication of this baseline that we published last month.

The changes from the Windows 10 v1809 and Windows Server 2019 baselines include:

- Enabling the new "Enable svchost.exe mitigation options" policy, which enforces stricter security on Windows services hosted in svchost.exe, including that all binaries loaded by svchost.exe must be signed by Microsoft, and that dynamically-generated code is disallowed. ***Please pay special attention to this one*** as it might cause compatibility problems with third-party code that tries to use the svchost.exe hosting process, including third-party smart-card plugins.
- Configuring the new App Privacy setting, "Let Windows apps activate with voice while the system is locked," so that users cannot interact with applications using speech while the system is locked.
- Disabling multicast name resolution (LLMNR) to mitigate server spoofing threats.
- Restricting the NetBT NodeType to P-node, disallowing the use of broadcast to register or resolve names, also to mitigate server spoofing threats. We have added a setting to the custom "MS Security Guide" ADMX to enable managing this configuration setting through Group Policy.
- Correcting an oversight in the Domain Controller baseline by adding recommended auditing settings for Kerberos authentication service.
- Dropping the password-expiration policies that require periodic password changes. This change is discussed in further detail below.
- Dropping the specific BitLocker drive encryption method and cipher strength settings. The baseline has been requiring the strongest available BitLocker encryption. We are removing that item for a few reasons. The default is 128-bit encryption, and our crypto experts tell us that there is no known danger of its being broken in the foreseeable future. On some hardware there can be noticeable

Windows 10 May 2019 Updateで変更

- Windows OSにおけるPW有効期限のデフォルトポリシは長らく42日だった。
- Office365ではNIST改定のタイミングで既に新しいパスワードベスプラに変更されていた。
- 遂にサービスとOSでのポリシーのギャップが埋まっていく。

https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/

一般的ないくつかの方法とその悪影響

以下は最もよく使われるパスワードの管理手法の一部ですが、調査ではその悪影響について警告しています。

ユーザー向けパスワードの有効期限の要件

パスワードの有効期限の要件にはメリットもありますがデメリットのほうが多くなります。これらの要件に従うと、ユーザーは互いに密接に関係している一連の単語と数字で構成される、予測可能なパスワードを選択することになるためです。このような場合、次のパスワードは前のパスワードに基づいて予測することができます。パスワードの有効期限の要件に抑制効果はありません。サイバー犯罪者は、ほとんどの場合、資格情報を侵害するとすぐに使用するためです。

長いパスワードを要求する

パスワードの長さ要件 (約 10 文字を超える) により、ユーザーの行動が予測可能で望ましくないものとなる可能性があります。たとえば、16 文字のパスワードを使用するよう求められたユーザーは、文字の長さ要件を満たすものの、推測しにくいものではない **fourfourfourfour** や **passwordpassword** などの繰り返しパターンを選ぶ可能性があります。さらに、長さ要件は、ユーザーがパスワードを書き留めたり、ドキュメントに暗号化されていないパスワードを保存するなど、他の安全でない手法を採用する機会を増やすことになります。ユーザーが一意のパスワードを考えるように、適切な 8 文字の最小長要件を維持することをお勧めします。

複数の文字セットの使用を要求する

パスワードの複雑さ要件により、キー スペースが減り、ユーザーが予測可能な方法で行動することになり、これでは元も子もありません。ほとんどのシステムでは、ある程度のパスワードの複雑さ要件を適用します。たとえば、パスワードには、次のカテゴリの 3 つすべての文字が必要となります。

- 大文字
- 小文字
- 英数字以外の文字

ほとんどのユーザーは似たようなパターンを使用します。たとえば、最初の位置が大文字、最後が記号、最後の 2 つが数字などです。サイバー犯罪者はこれを認識しているため、最も一般的な置換文字、つまり、"s" の場合は "$"、"a" の場合は "@"、"I" の場合は "1" を使用して辞書攻撃を実行します。ユーザーに大文字、小文字、数字、特殊文字の組み合わせを選択させるのは逆効果です。複雑さ要件によっては、セキュリティで保護され[illegible]ユーザーにセキュリティ レベルの低い覚えにくいパスワードを思い付かせることになります。

成功パターン

上記のものとは対照的に、パスワードに多様性を持たせる推奨事項をいくつか以下に示します。

よく使われるパスワードを禁止する

ユーザーがパスワードを作成するときに認識させる最も重要なパスワード要件は、パスワードの総当たり攻撃に対する組織の脆弱性を減らすためによく使われるパスワードの使用を禁止することです。よく使われるユーザー パスワードには、 **abdcefg**、 **password**、 **monkey** などがあります。

組織のパスワードを他の場所で再利用しないようにユーザーを教育する

組織内のユーザーに伝える最も重要なメッセージの 1 つは、組織のパスワードを他の場所で再利用しないということです。外部の Web サイトで組織のパスワードを使用すると、サイバー犯罪者がこれらのパスワードを侵害する可能性が高くなります。

多要素認証の登録を適用する

ユーザーが、代替メール アドレス、電話番号、プッシュ通知用に登録されたデバイスなどの連絡先とセキュリティ情報を更新し、セキュリティ チャレンジに応答して、セキュリティ イベントに関する通知を受け取れるようにします。更新された連絡先とセキュリティ情報は、ユーザーが万が一パスワードを忘れてしまった場合、または他のユーザーがアカウントを引き継ごうとした場合の本人確認に役立ちます。また、ログイン試行やパスワード変更など、セキュリティ イベントが発生した場合には、帯域外の通知チャネルが提供されます。

詳細については、「Office 365 ユーザー用の多要素認証を設定する」を参照してください。

リスク ベースの多要素認証を有効にする

リスク ベースの多要素認証では、Microsoft のシステムで不審な動作が検出されたときに、正当なアカウント所有者であることを確認するためにユーザーに対してチャレンジを実行することができます。

詳しく知りたい方は、 推奨される閲覧

- Do Strong Web Passwords Accomplish Anything? (強力な Web パスワードでできること)
- Password Portfolios and the Finite-Effort User (パスワード ポートフォリオとユーザーの有限労力)

このような「過渡期」をどう進むか

- **ベスプラと法令・業界等の「コンプライアンス順守」は別問題**
  - 適合基準／認定プロセスの枠組みで、新しいベストプラクティスとの差異があっても、それはそれ。

- **変化の方向性を把握して「次に打つべき手」を検討**
  - SP800-63-3の改定はシステム的な機能追加を要する要件が多い。
  - 近い将来業界が求める要件を先読みし、コスト投下ポイントを見定め。
  - 特定の変更点だけをピックアップして都合よく解釈するのはやめよう。

- **パラダイムシフトを起こすのはガイドラインではなく事業者**
  - 「効果はゼロではない」か「どんぐりの背比べ」の議論ではなく「効果が高い施策」について取り組もう。
  - 矛盾も不整合も把握したうえでリスクを踏まえて手を打てるのは、「保護すべきユーザ」に直接相対しているからこそ。

「やっぱり認証とか
デジタルアイデンティティって
面倒で地味なテーマだな」

とか思っているそこのあなた？

デジタルアイデンティティは「今」がアツい

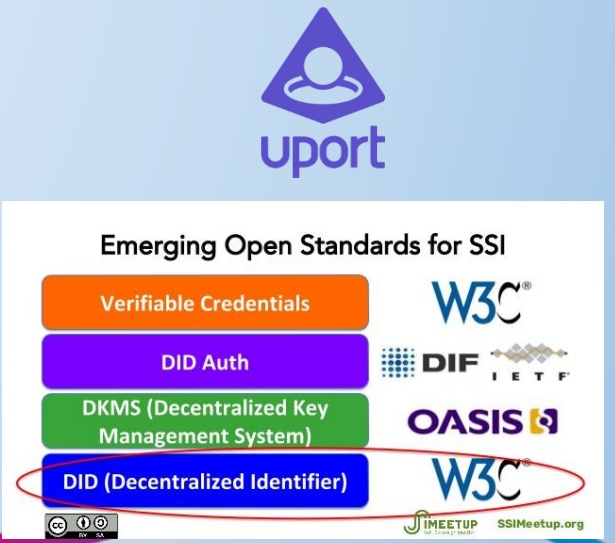
- **FIDO/WebAuthn/生体認証でパスワードレス**
  - 「なるべく」パスワードを使わない世界へ

- **金融グレードAPIを支えるOAuth2/OpenID Connect**
  - WebAPI出したので使ってください、が当たり前の世の中へ

- **リスクベース認証からコンティニュアス認証へ**
  - よりフィジカルな状態・行動に基づくログイン後のリスク判定へ

- **KYC結果の企業間でのデジタル流通(eKYC)**
  - 金融機関などIALの高い手法で実施されたKYC結果を他社に流通

- **Self-Sovereign Identity/Decentralized Identifier**
  - 自分のアイデンティティは自分で管理（ユーザセントリック）
  - あらゆるサービスに通用する自分自身の永続的な識別子



まとめ

- **デジタルアイデンティティフレームワークとして再編された NIST SP800-63-3、特に63Bの考え方を通じて共通言語を得た**
  - 63A：登録プロセスと身元確認
  - 63B：認証とライフサイクル管理（★本日フォーカス）
  - 63C：フェデレーションとアサーション
- **「パスワード認証」で一大転換**
  - パスワードからパスフレーズへ
  - パスワード定期変更は「事業者(CSP/Verifier)が採る対策として(禁止はしないが)非推奨」
  - 秘密の質問の廃止で、アカウントリカバリは複雑さを増していく
  - SMS認証は要観察
  - 生体認証は「今」は補助的なもの
- **過渡期の矛盾や解釈の曖昧さに翻弄されず、方向性を見極めよう**
  - 細部を見ると課題はあるが、進むべき方向性は示されている
  - デジタルアイデンティティはセキュリティ/UX/ビジネス全てに関係し、「今」がアツい

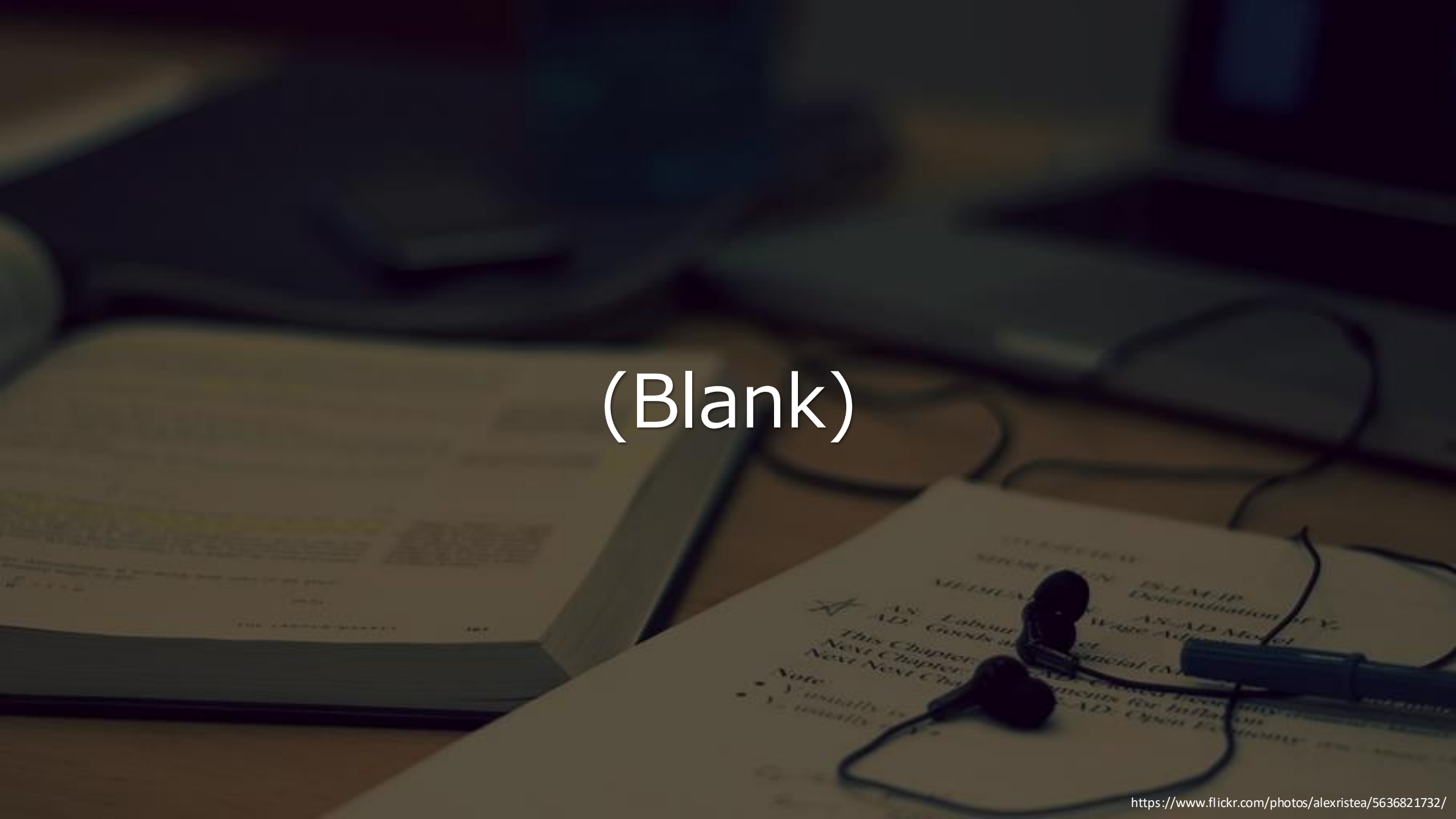
https://www.flickr.com/photos/alexristea/5636821732/

ありがとうございました

ご指摘、ご感想があればお気軽にご連絡ください

ta.katsuhara@ndias.jp, kthrtty@gmail.com

https://www.flickr.com/photos/alexristea/5636821732/



https://www.flickr.com/photos/alexristea/5636821732/