自己紹介

貞弘　崇行（さだひろ　たかゆき）

株式会社アイピーキューブ　IAMコンサルティング部　IDコンサルタント

SIerとして主にB2E向けのMicrosoft系プラットフォーム及びアプリケーションのアカウント管理システム、オンプレミス及びクラウドへのIDフェデレーションシステム、IDaaS導入の企画、要件定義、設計、導入を担当。

最近では、B2BやB2C向けのアカウント管理、認証基盤導入の企画、要件定義等も担当。
eKYCにも関連する要求/要件を見るようになってきました。

【主な所属団体】
・日本ネットワークセキュリティ協会（JNSA）
標準化部会　デジタルアイデンティティWG

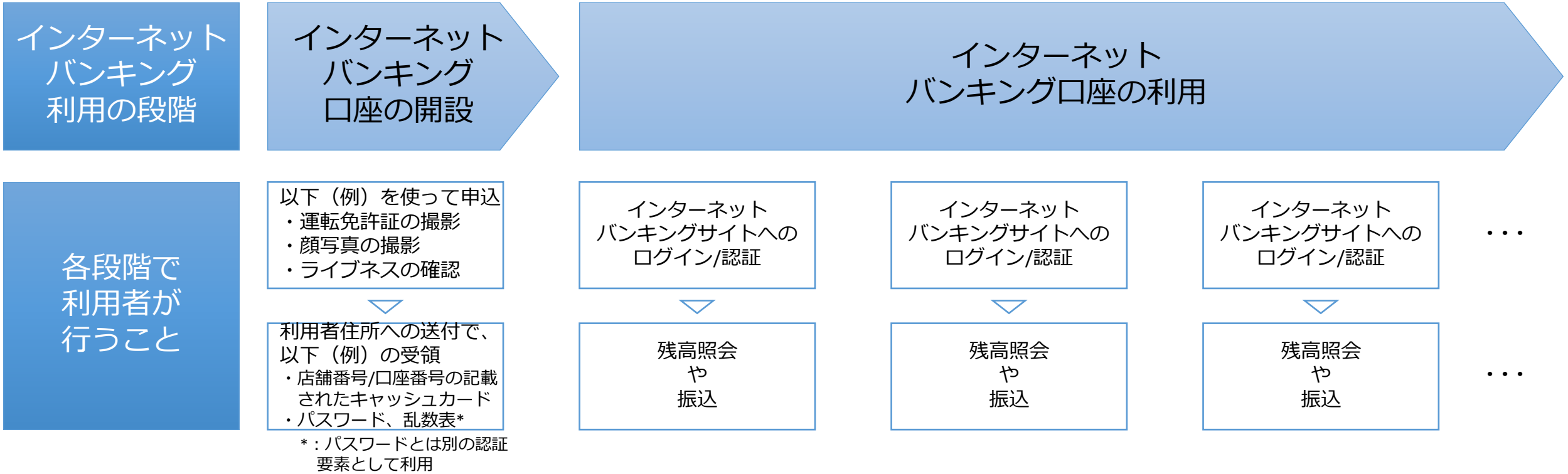
【主な活動】
・エンタープライズロール管理解説書（第3版）　主要執筆者

本資料の目的

- ID管理／本人確認（Identity proofing）に関するeKYCや認証、ID管理の標準化が関わる箇所を、インターネットバンキングを使って例示すること

- 上記例示によって、各種標準やガイドラインを適用する箇所の具体的なイメージを持っていただくこと

インターネットバンキング利用の流れ



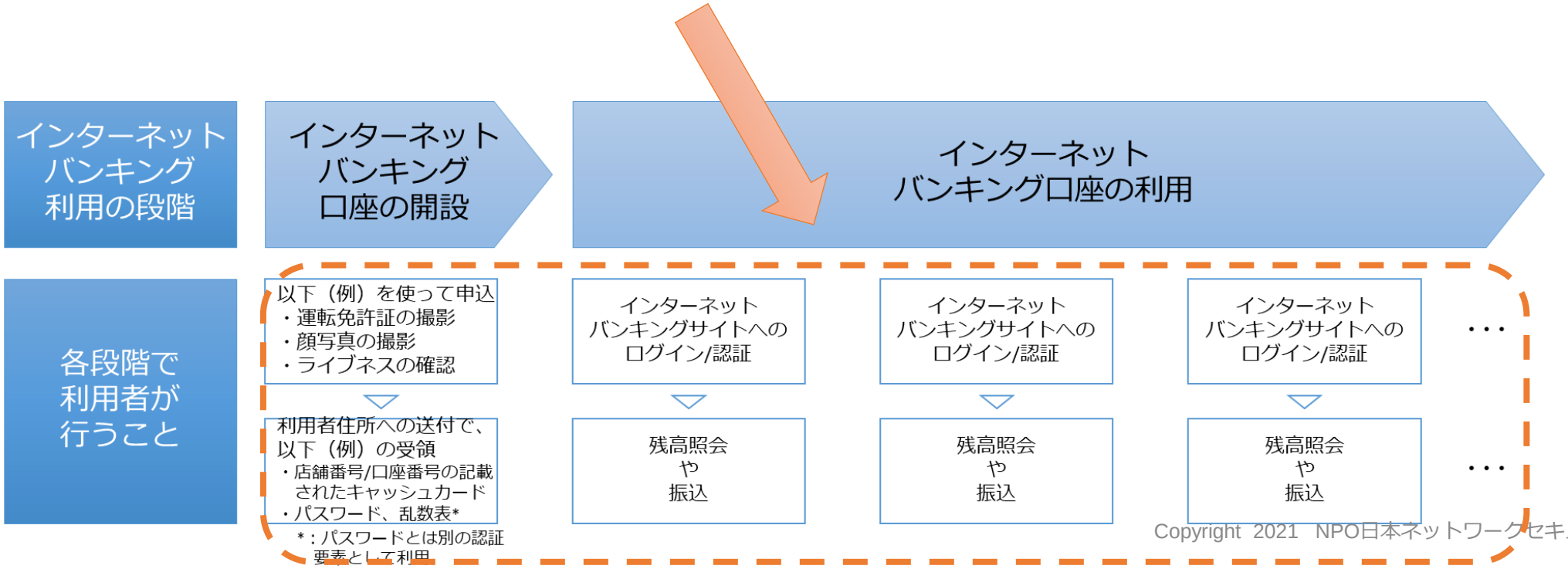
インターネットバンキング利用を支える信頼

"On the Internet, nobody knows you're a dog."

引用：On the Internet, nobody knows you're a dog
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

インターネットバンキング利用を支える信頼

- インターネットバンキング口座開設から閉鎖までの中/長期的な信頼
  - 利用者は、適切な身元確認を経ている
  - 利用者は、適切な強度を持つ認証要素を保持/利用出来る状態
  - 利用者は、口座利用者として適切な状態
    （例　自己破産していない、発行された乱数表を紛失していない）

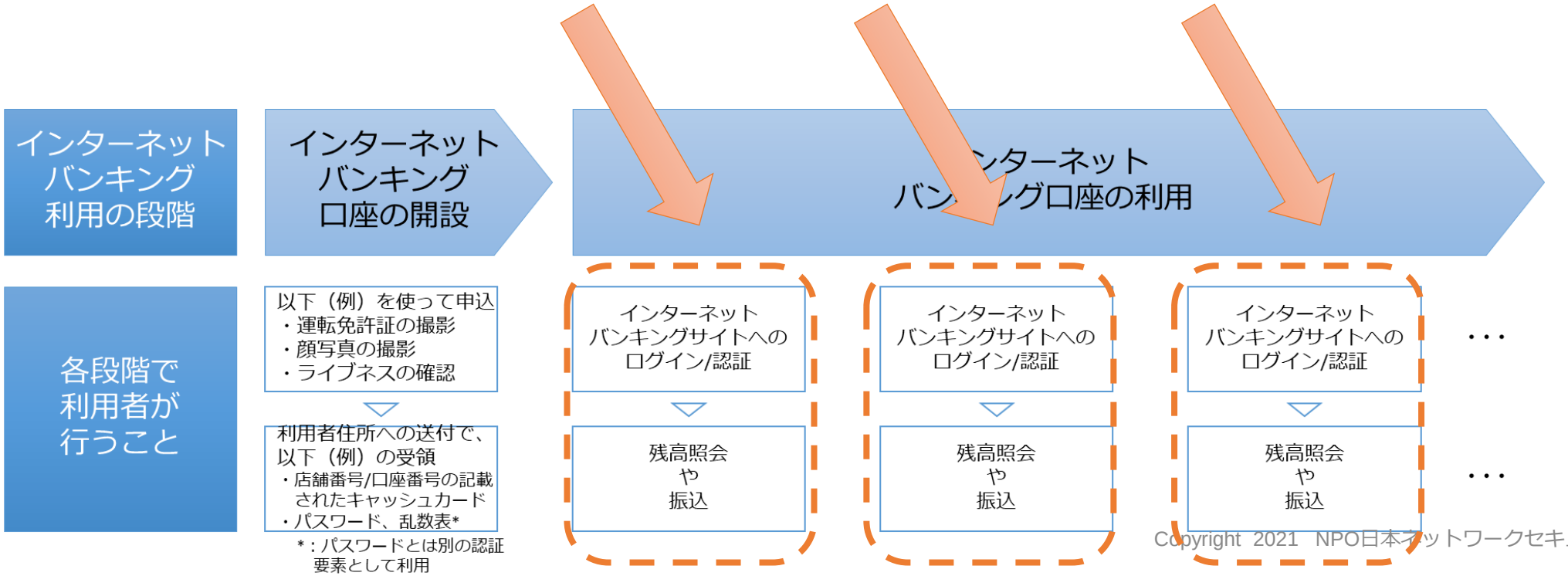


インターネットバンキング利用を支える信頼

- インターネットバンキング口座開設から閉鎖までの中/長期的な信頼
  - 利用者は、適切な身元確認を経ている
    → NIST 800-63A, 改正犯罪収益移転防止法
  - 利用者は、適切な強度を持つ認証要素を保持/利用出来る状態
    → NIST 800-63B
  - 利用者は、口座利用者として適切な状態
    （例　自己破産していない、発行された乱数表を紛失していない）
    → ISO/IEC 24760, NIST 800-63B

インターネットバンキング利用を支える信頼

- インターネットバンキングサイト利用都度の短期的な信頼
  - 利用者は、適切な強度を持つ認証要素を利用して認証した
  - 利用者は、ログイン/認証後もサイトの利用を続けている
    （例　操作の無い状態が30分以上継続していない）



インターネットバンキング利用を支える信頼

- インターネットバンキングサイト利用都度の短期的な信頼
  - 利用者は、適切な強度を持つ認証要素を利用して認証した
    → NIST 800-63B
    - 口座開設時の身元確認及び認証要素の提供と当該要素の本人との紐付けに基づく信頼
  - 利用者は、ログイン/認証後もサイトの利用を続けている
    （例　操作の無い状態が30分以上継続していない）
    - 利用者が何らかの操作を行う度に認証すれば確実だが、利便性は著しく低下
    - 一度認証したら、一定の条件で認証された状態を維持
      （振込の実行等、意思/意図を確認する場合は、都度認証を行う）
    - 一般的には再認証までは時間の経過（認証時点から、無操作状態になってから、など）
      → NIST 800-63B, PSD2
    - （参考）
      - 離席を検知して、デバイスをロック（Windows 10）
      - サイト上での操作をスコアリングして、マルウェア等を検知

（参考）時間の経過について

- NIST 800-63B（4.1.3, 4.2.3, 4.3.3）
  - 再認証を求めるまでの時間

	AAL1	AAL2	AAL3
操作の有無にかかわらず	30日	12時間	12時間
操作が無い	指定無し	30分	15分

- PSD2 – Regulatory Technical Standards（Article 4.3.(d)）
  - 認証後、操作が無い場合に許容される最長時間は5分間

引用
NIST 800-63B：https://pages.nist.gov/800-63-3/sp800-63b.html
PSD2 – RTS：2017-02-15 BoS Final report on the draft RTS on SCA and CSC under PSD2.docx (europa.eu)