欧州セキュリティ認証制度(EUCC)と CSA STAR／CCM

イタリアのユースケースに学ぶ

2024年11月20日

日本クラウドセキュリティアライアンス
代表理事／関西支部 笹原 英司 博士(医薬学)

はじめに

The Role of CSA STAR in the Italian Cloud Strategy By CSA Italian Chapter @SECtember 2022

In the presentation, we will show the main objectives of the Italian government's cybersecurity and cloud strategy with a focus on the new National Cybersecurity Agency role and the new cloud security requirements for cloud providers in the public administration market where CSA STAR certification (level 2) is going to play a strategic role in the next years.

http://www.chapters.cloudsecurityalliance.jp/

AGENDA

- 1. EUにおけるイタリアのデジタル化動向
- 2. イタリア政府のクラウド戦略
- 3. イタリアクラウド戦略とNIS2の実装
- 4. イタリアの政府クラウド認証とCSA STAR
- 5. CSAと欧州委員会／ENISAの連携活動
- 6. STAR for AIの紹介
- 7. まとめ／Q&A

1. EUにおけるイタリアのデジタル化動向

欧州委員会「*Italy 2024 Digital Decade Country Report*」(2024年7月)

(https://digital-strategy.ec.europa.eu/en/factpages/italy-2024-digital-decade-country-report)

＜強み＞

・eヘルス：イタリアは、電子健康記録(EHR)へのアクセスにおいてEU平均(100点中79.1点)を上回る82.7点を記録しており、全地域で導入され、2023年に大きな伸(+15.9%)を記録した

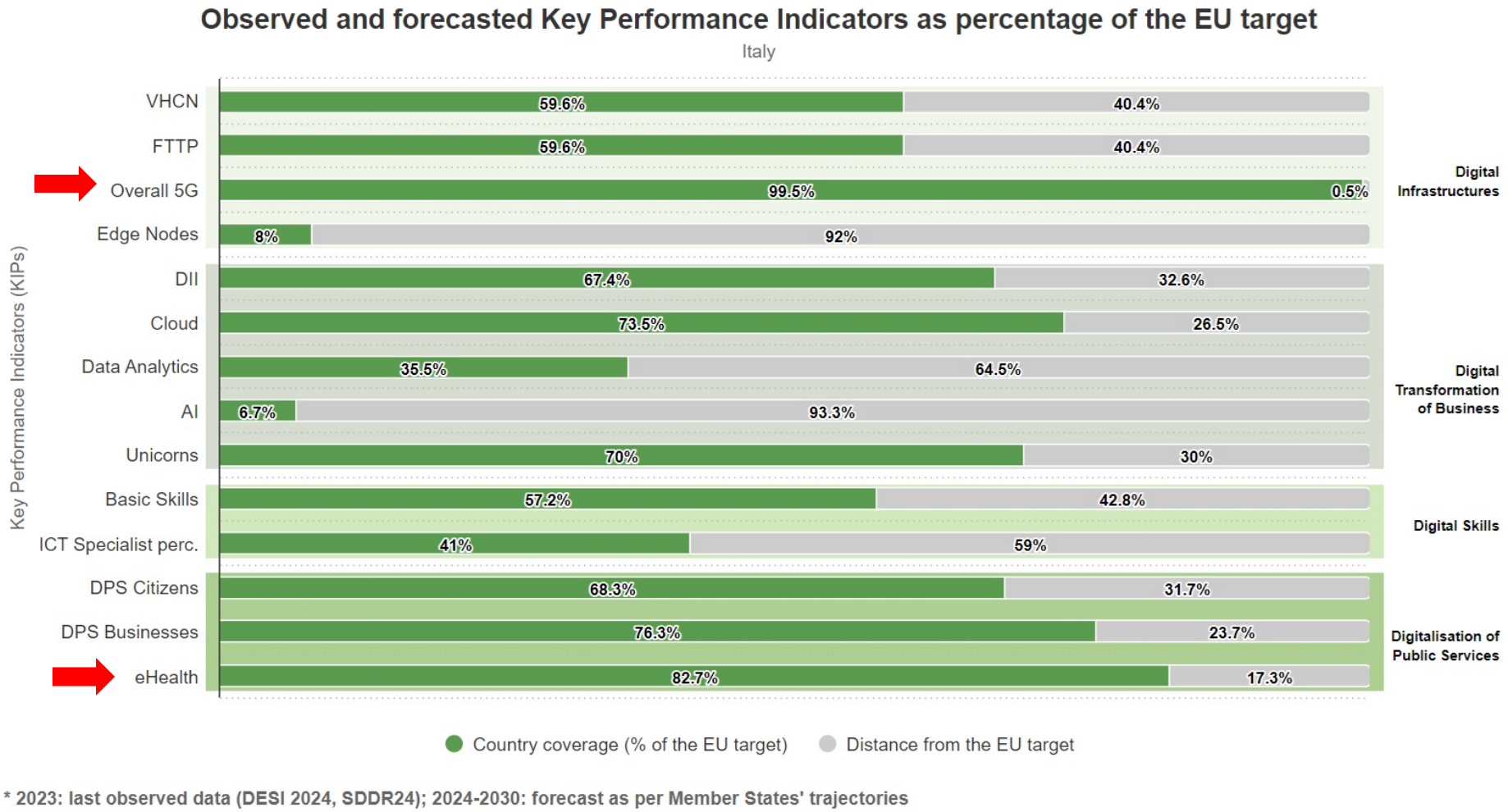
・デジタルインフラストラクチャ：現時点で、FTTPやVHCN(固定超高容量ネットワーク)の目標達成率は、EU平均を下回っているが、年々、確実に伸びている

＜弱み＞

・企業やユニコーンにおけるクラウドの採用：イタリアの企業でAIを使用しているのは5%で、EU平均(8%)を下回っている

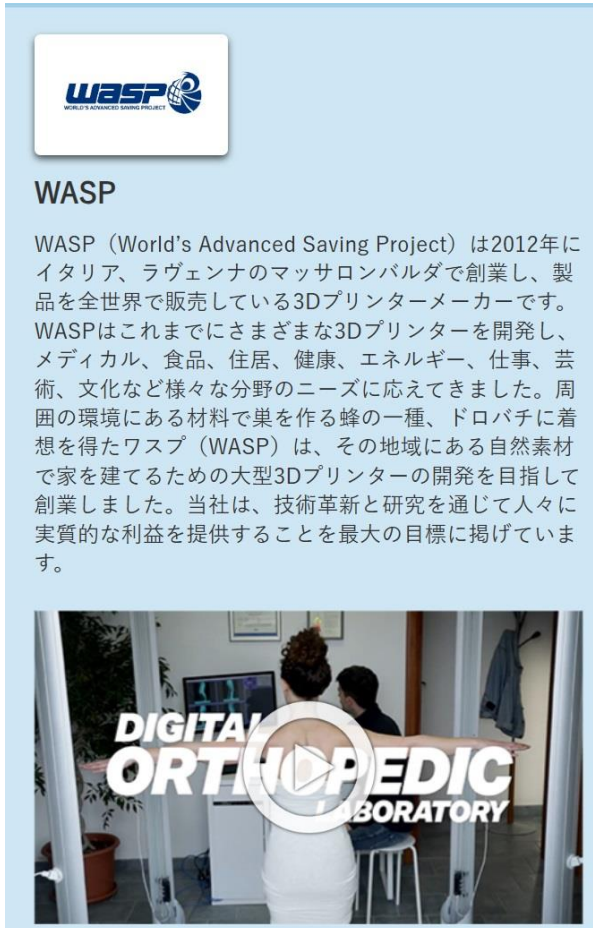
・基礎的なデジタルスキル：イタリアの人々のうち、基本的なデジタルスキルを持っているのは45.8%で、EU平均(55.6%)を下回っている

(参考)EU目標に対する重要業績評価指標の達成率



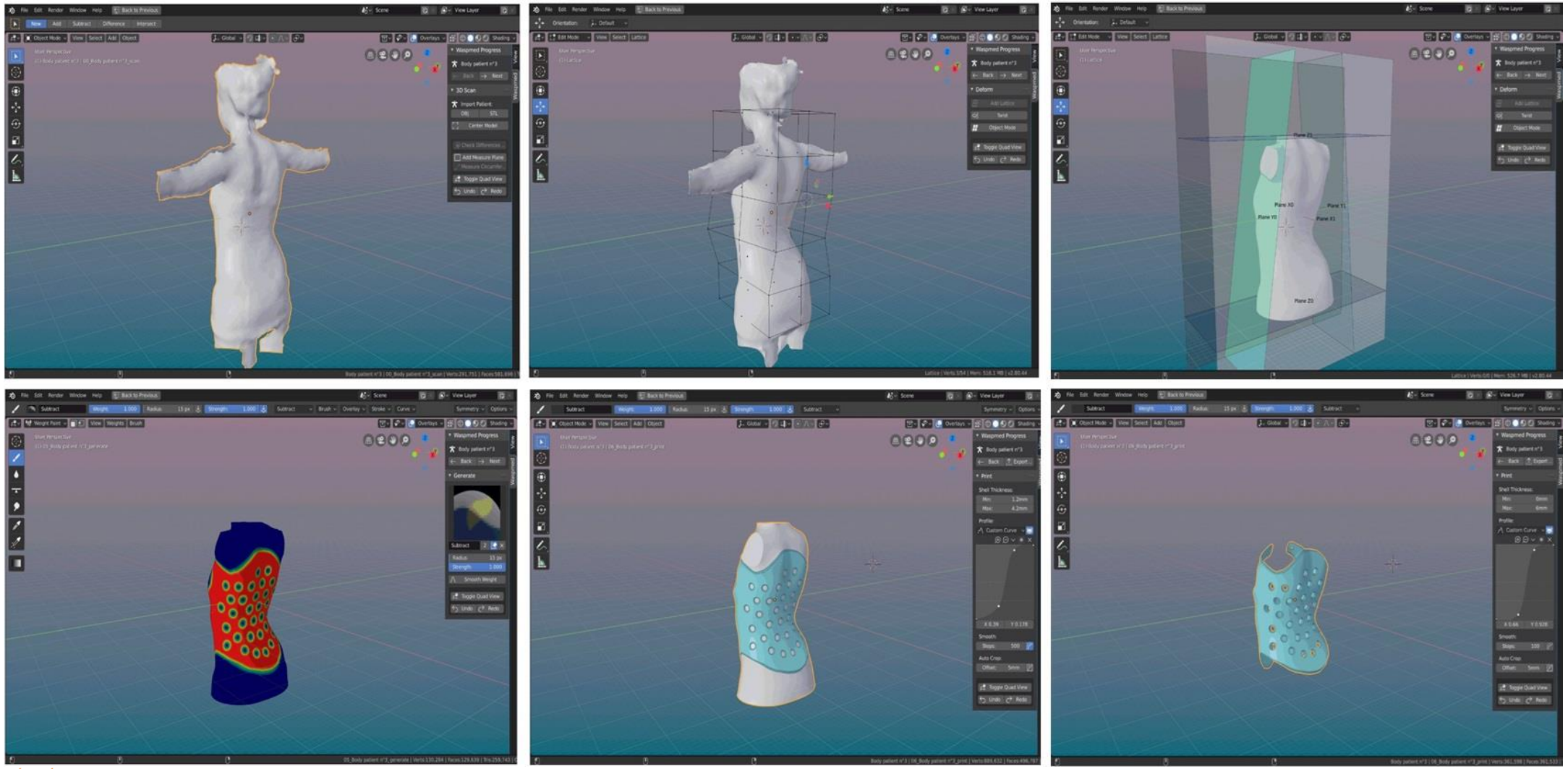
出典：European Commission「Italy 2024 Digital Decade Country Report」(2024年7月22日更新)
https://digital-strategy.ec.europa.eu/en/factpages/italy-2024-digital-decade-country-report

(参考1)イタリアのeヘルス事例:WASP s.r.l.



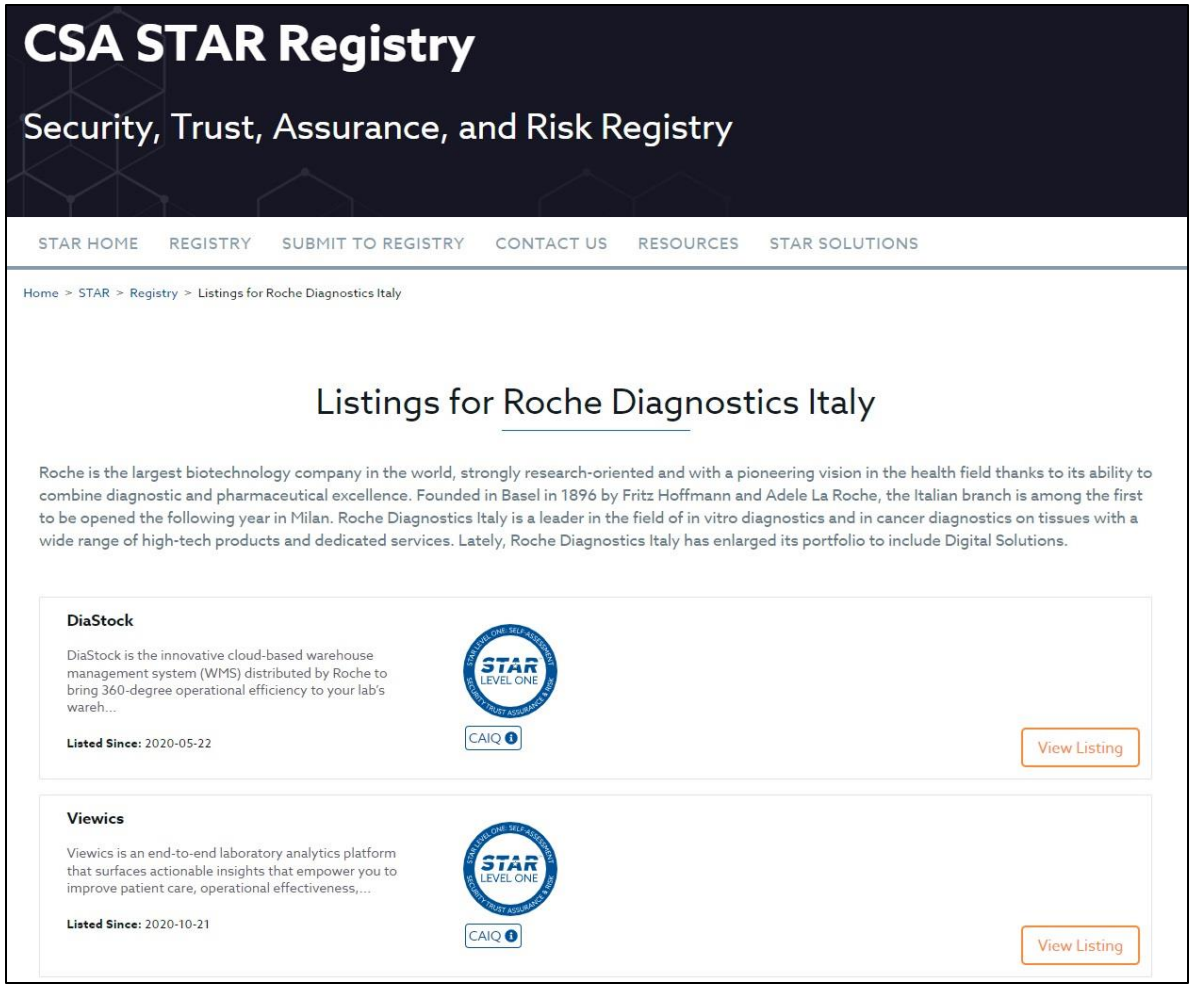
出典：Italian Trade Agency「ITALY Pavilion」(2024年10月9-11日) (https://jcd-expo.jp/ja/microsite-ITA-ja.html)

(例)整形外科向け3Dプリンタ用アドオンソフトウェア
WASP MED Add-on Blender 2.8



出典：WASP s.r.l.「The open-source 3D software for P&O now exists」(2019年7月4日)
(https://www.3dwasp.com/en/addon-blender-wasp-med/)

(参考2)イタリアのCSA STAR登録ユーザー企業事例



出典：Cloud Security Alliance「CSA STAR Registry: Listings for Roche Diagnostics Italy」(2024年11月1日時点)
https://cloudsecurityalliance.org/star/registry/roche-diagnostics-italy

2. イタリア政府のクラウド戦略

イタリア閣僚評議会議長府デジタルトランスフォーメーション局(DTD)、国家サイバーセキュリティ庁(ACN)「イタリアのクラウド戦略」(2021年9月8日)

https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/

＜構成＞

イタリアクラウド戦略の目的と柱

・クラウド戦略の目的: 行政機関におけるクラウドソリューションの実装と管理のための戦略的方向性を提供する

＜クラウドのメリット＞

・クラウドへの移行により、行政機関はデジタルサービスを提供し、プライバシー保護の原則や欧州および国内の機関の勧告に沿って、安全で効率的かつ信頼性の高い技術インフラを持つことができる
・国の戦略的な自律性、安全性およびデータに対する国内管理のための必要な保証を維持する

＜クラウド戦略の柱＞

1. EU域外のプロバイダーから独立した国家戦略ハブ(NSH)の構築
2. パブリッククラウドプロバイダーおよびそのサービスの特性やサービスレベルが、セキュリティ、信頼性、関連規制に準拠し、国家の利益に必要な要件に沿っていることを保証するための資格付与プロセス
3. 行政機関が管理するデータやサービスを分類するための方法論を開発し、それによって最も適切なクラウドソリューション(NSH または認定されたパブリッククラウド)への移行を可能にする

イタリアにおけるクラウドコンピューティングの課題

①技術的自律化:

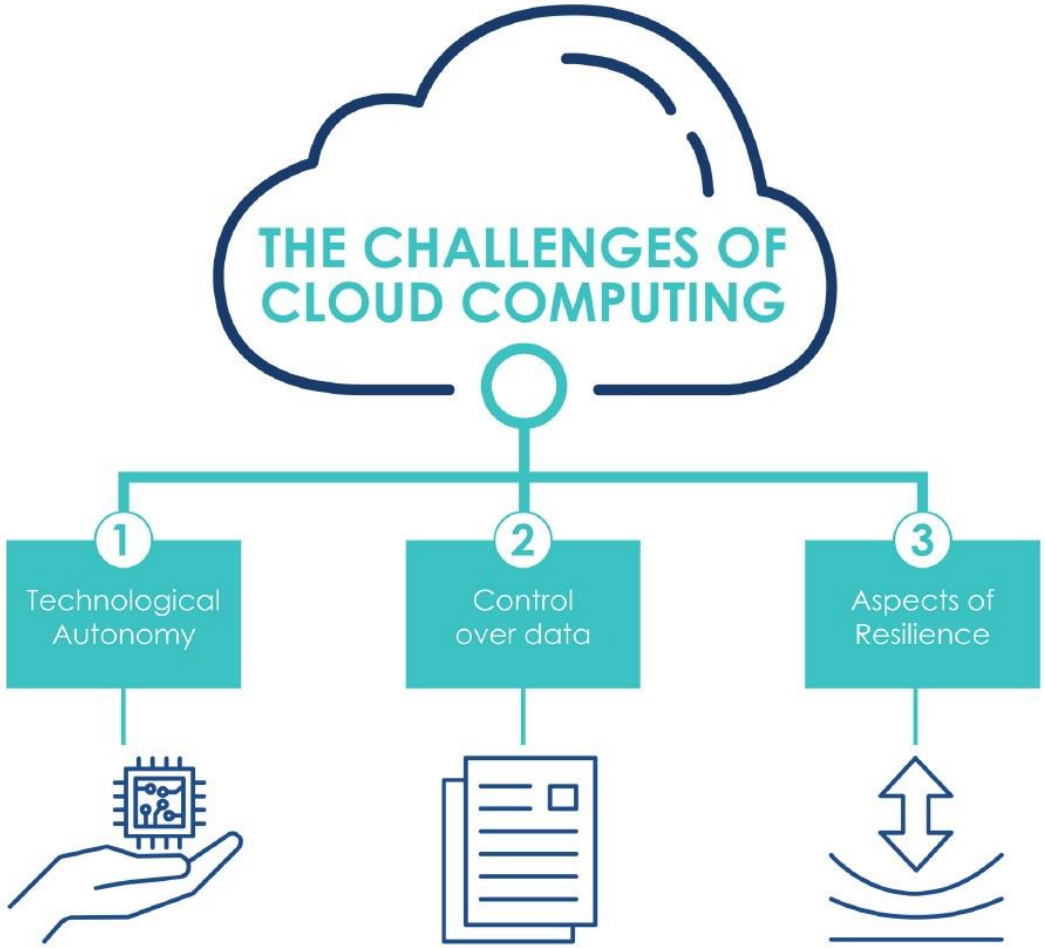
クラウドインフラにおける欧州企業の市場シェアは、非EU企業と比較して低い

②データに関する制御:

非EU諸国のプロバイダーによるクラウドサービスの運用は、国々の規制のために追加的なリスクをもたらす

③レジリエンスの観点:

行政機関のアプリケーションや国家の重要なエンティティをサポートするクラウドインフラとサービスは、適切な手続き的および技術的セキュリティ対策を採用し、冗長性と相互運用性の運用も行う必要がある



出典：Department for Digital Transformation of the Presidency of the Council of Ministers (DTN) and the National Cybersecurity Agency (ACN)「Italian Cloud Strategy」(2021年9月8日) (https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/)

イタリアクラウド戦略の概要

①データおよびサービスの分類

行政機関クラウドへの移行プロセスを標準化し、
方向付けるために、行政機関が管理するデータと
サービスを分類する体系的なプロセスを特定する

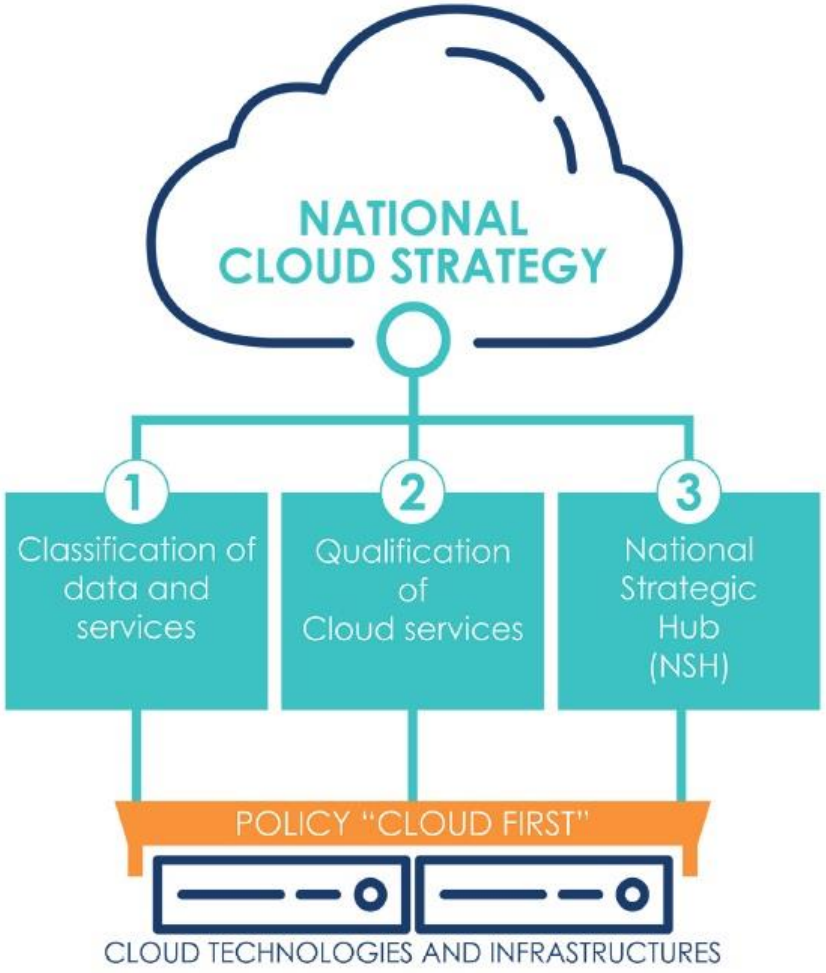
②クラウドサービスの適合性評価

＊CSA STARプログラムを参照規格の1つに採用

1.クラウドサービスの運用管理、技術的および組織的な
　標準と適用されるデータ管理対策の詳細
2.データ管理とサービス提供におけるセキュリティ要件
3.サービス提供と報告に適用される条件(例.可用性保証)

③国家戦略ハブ(NSH)

最高の信頼性、レジリエンス、独立性の保証を享受できる
クラウド技術およびインフラを行政機関に提供する



出典：Department for Digital Transformation of the Presidency of the Council of Ministers (DTN) and the National Cybersecurity Agency (ACN)
「Italian Cloud Strategy」(2021年9月8日) (https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/)

データおよびサービスの分類ポリシー

・特定の規制やセキュリティ要求事項を考慮せず、国への影響の可能性にのみ焦点を当てて、データおよびサービスを分類する

通常(Ordinary): 障害が発生しても、国家のサービスの中断や、国の経済的および社会的福祉への損害を引き起こさないデータおよびサービス

重要(Critical): 社会、健康、安全、そして国の経済的および社会的ウェルビーイングにとって重要な機能の維持に有害となる可能性のあるデータおよびサービス

戦略的(Strategic):

侵害された場合、国家の安全保障に影響を与える可能性があるデータおよびサービス

・分類プロセスの適用により、影響と適用されるクラスの分析、および適切なセキュリティおよび規制要件の特定が可能になる

・Perimetro Sicurezza Nazionale Cibernetica(PSNC)の範囲内で特定された、国家の重要な機能やサービスに関連するデータとサービスは「戦略的」に分類される

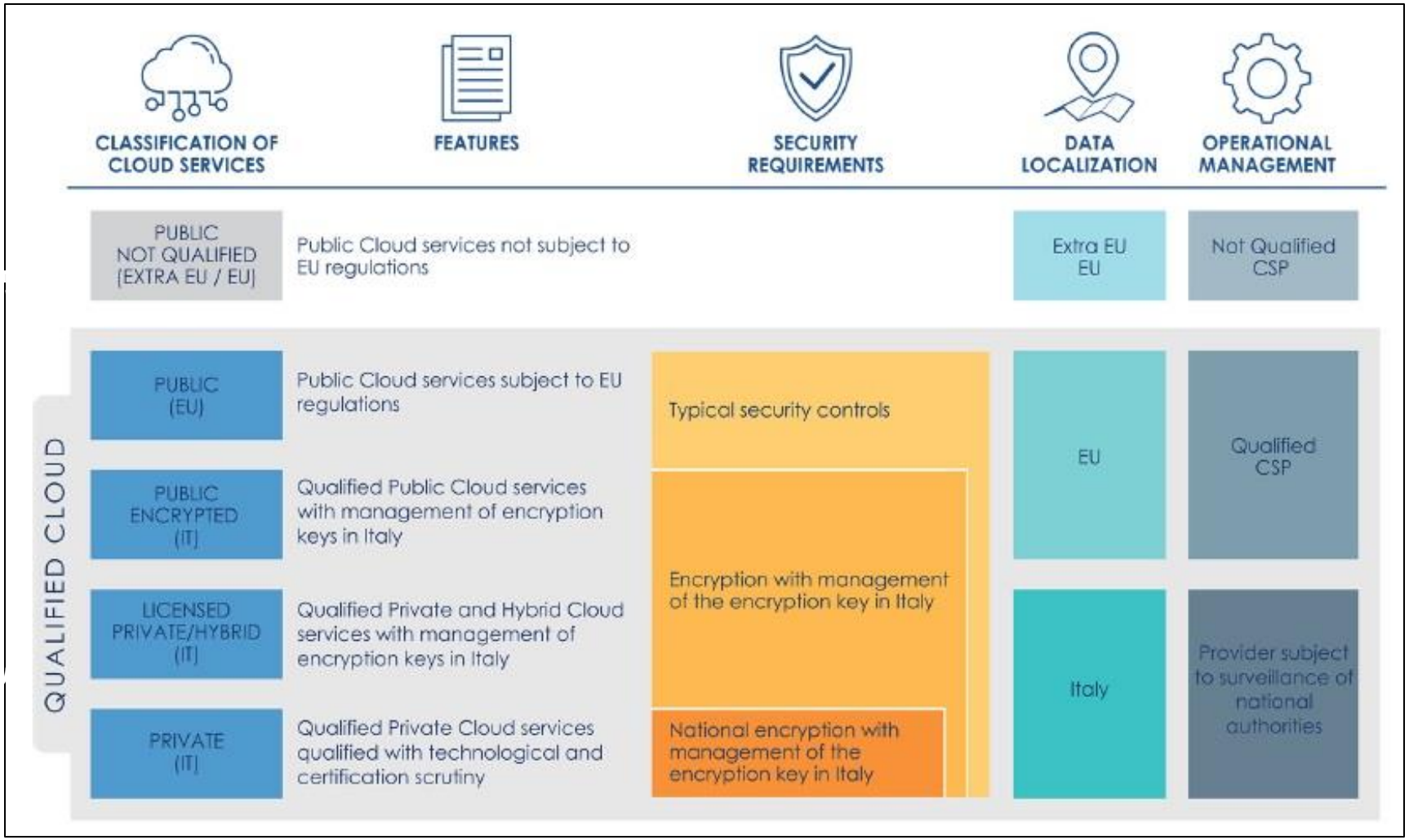
・市民の健康データは「重要」に分類される

・行政機関のWebポータルに関連するデータとサービスは「通常」に分類される

クラウドサービスの分類

・認定外のパブリッククラウド(EU域外 / EU): データおよびサービスの管理ツールがほとんど存在しない
・認定されたパブリッククラウド(EU): 関連する法律(例：GDPRおよびNIS)に準拠し、通常、CSPプロバイダーによって管理される細かい暗号化システムを使用する技術的・組織的セキュリティ要件を満たし、管理されるデータとサービスのより大きな制御を可能にする
暗号化されたパブリッククラウド(国内): オンプレミスのセキュリティメカニズムの管理を伴うパブリッククラウドに基づくソリューションの使用は、データおよびサービスの利用可能な制御レベルを大幅に向上させ、技術インフラの運用管理および制御において非EUのCSPからのより大きな独立性をもたらす
・プライベート／ハイブリッドクラウドソリューションは、主要なCSPの公共領域からの追加の隔離を可能にし、国家当局の監視およびモニタリングの下で指定されたプロバイダーによって実行される運用管理を通じて確保される
ライセンス供与されたプライベート／ハイブリッドクラウド(国内): 1つまたは複数のCSPからライセンス供与されたハイパースケーラー技術に基づくもの
認定されたプライベートクラウド(国内): 技術的精査および認証手続きによって認定された商業技術を使用して実装されたもの

クラウドサービス適合性評価の要求事項

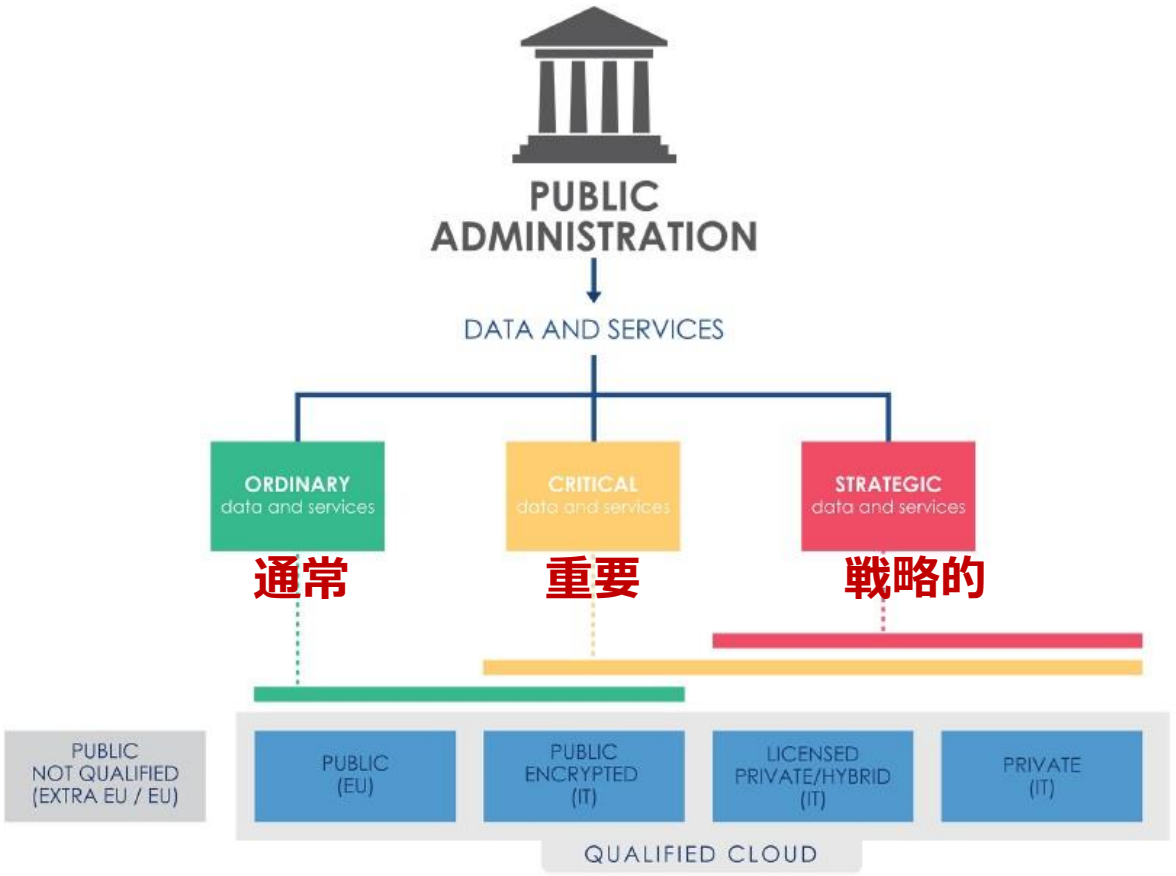


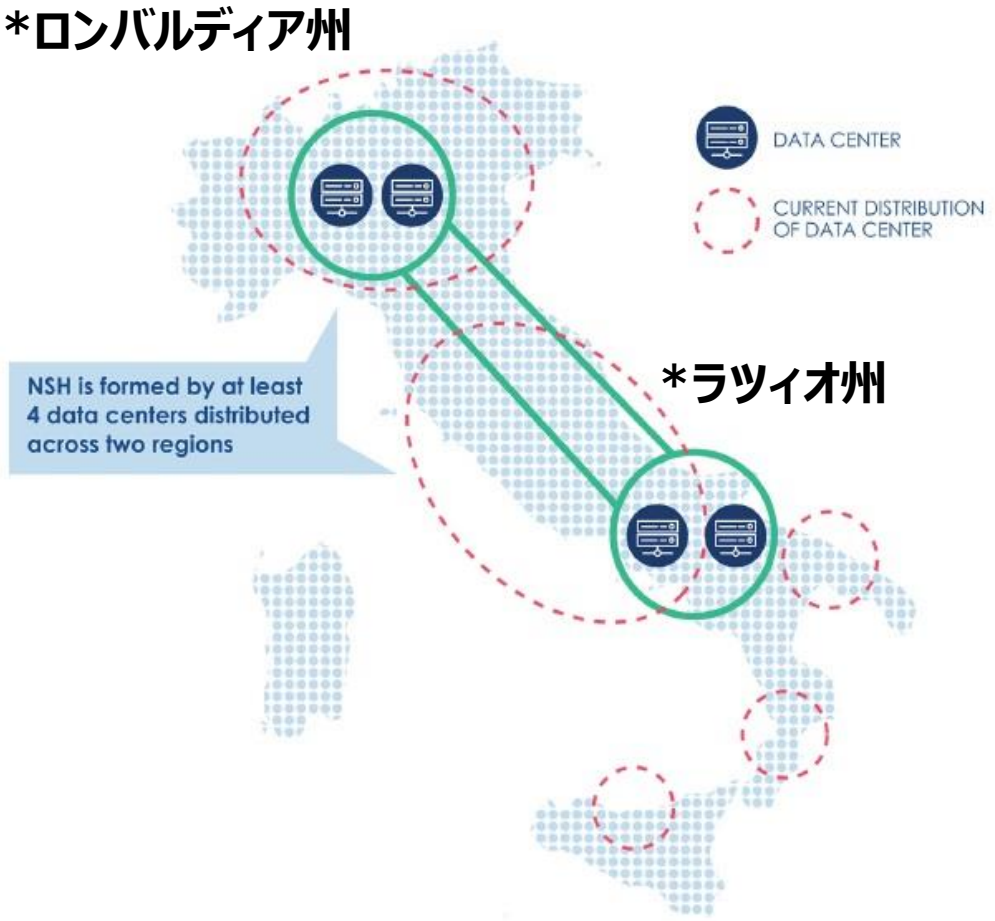
出典：Department for Digital Transformation of the Presidency of the Council of Ministers (DTN) and the National Cybersecurity Agency (ACN)「Italian Cloud Strategy」(2021年9月8日) (https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/)

国家戦略ハブ(NSH)の役割

・全国にわたる複数の行政機関にサービスを提供できる新しいITインフラ(国家戦略ハブ(NSH)) の開発により、行政機関の複数のデータセンターのセキュリティと信頼性を合理化し、強化する
・NSHは国内全域に地理的に分散され、最適なサイトに配置されることにより、十分なレベルのビジネス継続性とフォールトトレランスを確保する
・NSHの運用管理は、適切な技術的および組織的要件に基づいて、認定された国内プロバイダーに委託される
・プロバイダーは関連法令に従ってデータの管理を確保し、行政機関がクラウドサービスプロバイダーと適切な契約条件を交渉するのを支援する必要がある
・NSHは、PSNCやNISなどのセキュリティ要件に準拠することを設計上保証し、IaaSおよびPaaSクラウドサービスモデルへの移行を可能にする必要がある
・NSHは暗号化されたパブリッククラウド(国内)サービス、すなわち行政機関向けのパブリッククラウドに統合されたオンプレミスの暗号化ツールをサポートし、プライベートクラウドサービスの範囲、すなわちライセンス供与されたプライベート/ハイブリッドクラウド(国内)および認定されたプライベートクラウド(国内)を提供する
・分類および資格付与手続きに従い、NSHは、中央の行政機関や主要な地方行政機関(例：地域行政機関、地方保健当局および大都市)を支援する

国家戦略ハブ(NSH)の構造

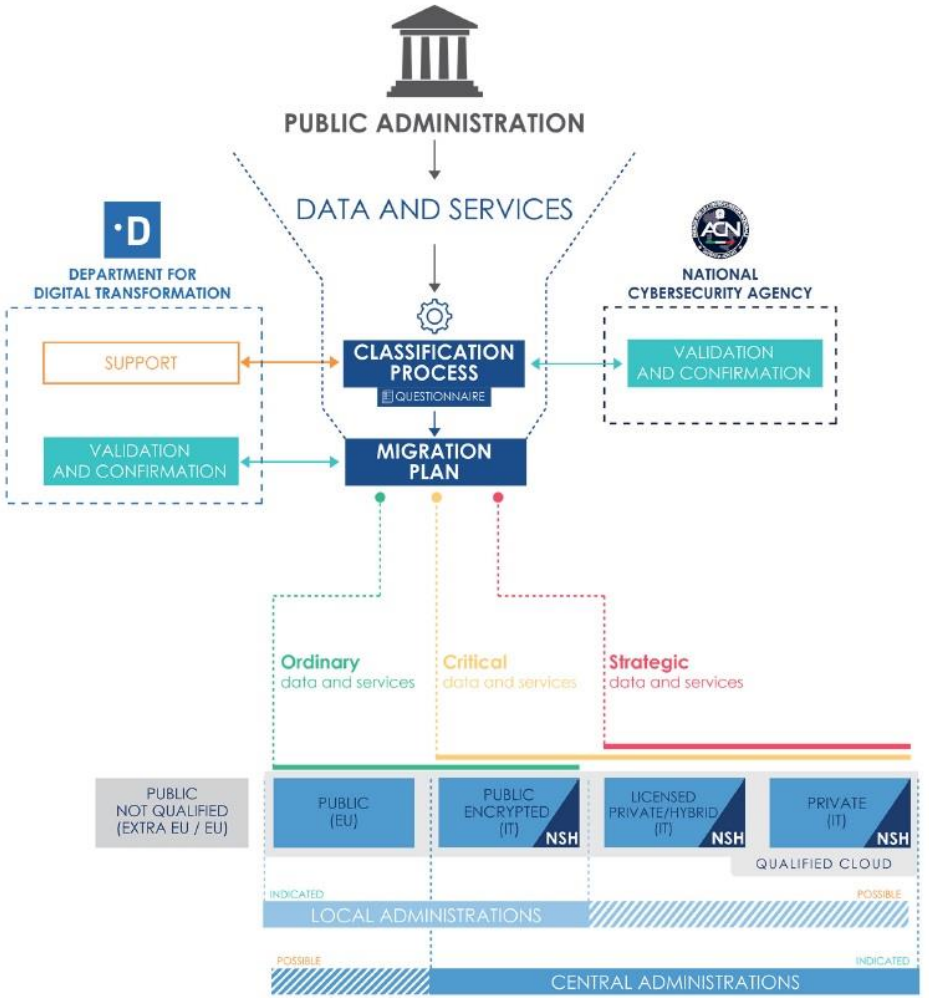




出典：Department for Digital Transformation of the Presidency of the Council of Ministers (DTN) and the National Cybersecurity Agency (ACN)「Italian Cloud Strategy」(2021年9月8日) (https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/)

行政機関のクラウドへの移行

・クラウドサービス／NSHへの移行は、すべての行政機関に対して中央集権的でスムーズかつ統一されたプロセスを通じて管理される
・移行計画は、データとサービスの分類結果に基づいて定義される
・この分類と移行計画は、適切に定義されたアンケートに基づいて定義され、国家サイバーセキュリティ庁(CAN)およびデジタルトランスフォーメーション局(DTD)によって各自のプロファイルに応じてサポートされる
・このプロセスはパブリックセクターの責任を切り離すことはできず、各行政機関が管理するデータとサービスの特定とカタログ化から始まる
・その結果、潜在的なデータ侵害、規制上の制約、およびセキュリティの影響に基づいて分類が適用される
・移行計画は、国家クラウド戦略の実施を確実にするために、省と庁によって検証され確認される



出典：Department for Digital Transformation of the Presidency of the Council of Ministers (DTN) and the National Cybersecurity Agency (ACN)「Italian Cloud Strategy」(2021年9月8日) (https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy/)

クラウド戦略の採用

・フェーズ 1:国家戦略ハブ(NSH)導入のための入札告知の発行

2021年末までに、NSH導入のための入札告知が発行される

・フェーズ 2: 調達契約の授与とNSHの実装

入札の授与は遅くとも2022年末までに行われる

＊NSH／PSNが、SOC、CERTを設置

・フェーズ 3: 行政機関の移行

遅くとも2022年末から、行政機関のNSHへの移行が開始され、2025年末までに完了する

移行フェーズでは、行政機関ICT資産調査により、構造的および/または組織的な欠陥がある、またはサービスの継続性を保証しないデータセンターとしてカテゴリBに分類される中央公共機関が優先される

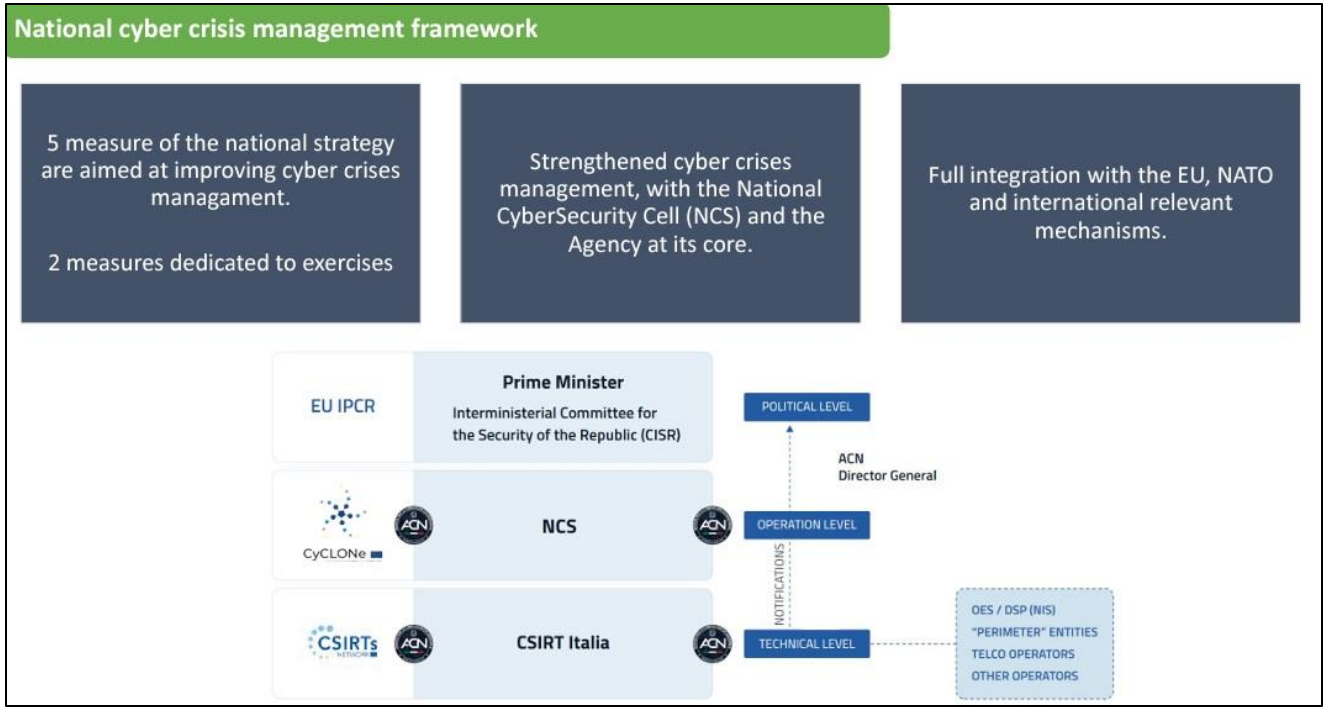
3. イタリアクラウド戦略とNIS2の実装

国家サイバーセキュリティ庁(ACN)「イタリアNIS2実装計画」(2022年1月26日)

(https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf)

サイバー危機管理フレームワーク: *ACNは傘下にCSIRT Italiaを持つ

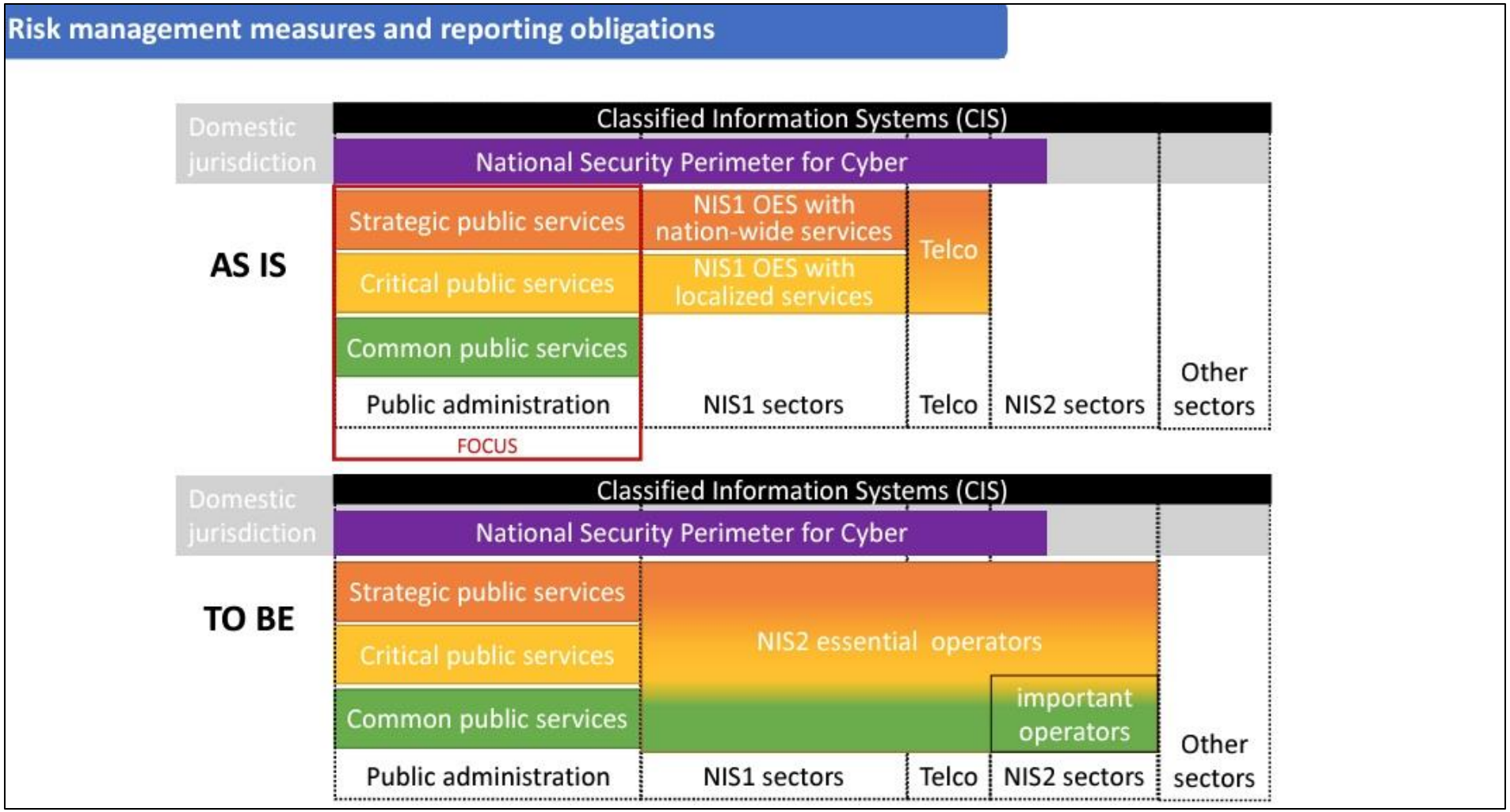
NIS2指令:
2024年
10月18日
適用開始



出典：National Cybersecurity Agency (ACN)「Italy's plans to implement NIS2 Directive」(2022年1月26日)
(https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf)

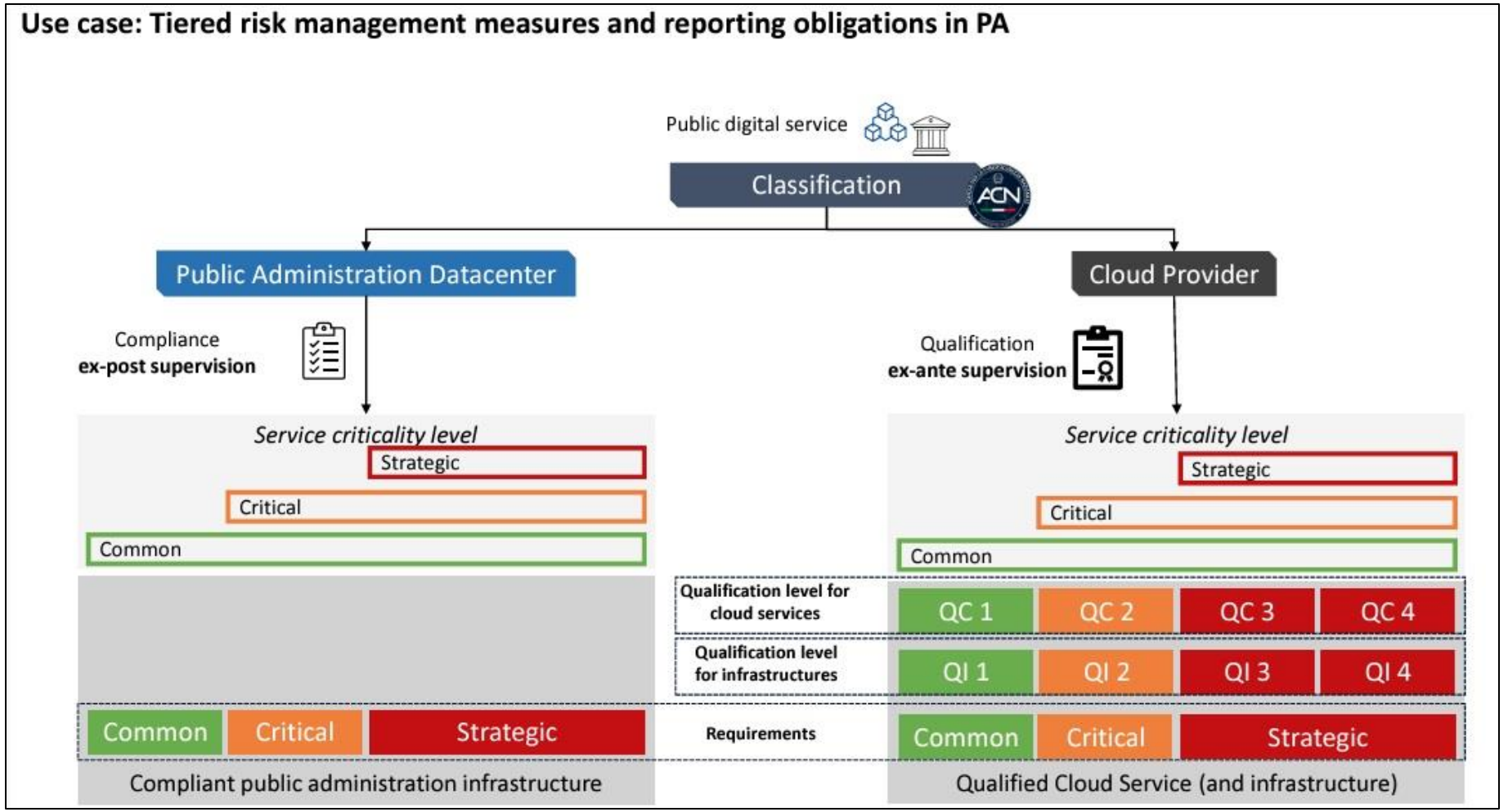
リスクマネジメント対策とレポーティングの責務

NIS2指令:
早期警告
-24時間以内
インシデント通知
-72時間以内
最終報告
-1ヶ月以内



出典：National Cybersecurity Agency (ACN)「Italy's plans to implement NIS2 Directive」(2022年1月26日)
(https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf

(事例)行政機関における多層型リスクマネジメント対策



出典：National Cybersecurity Agency (ACN)「Italy's plans to implement NIS2 Directive」(2022年1月26日)
(https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf)

4. イタリアの政府クラウド認証とCSA STAR

クラウドセキュリティアライアンス「イタリアの国家サイバーセキュリティ庁がSTARプログラムを採用」(2022年3月17日)
(https://cloudsecurityalliance.org/blog/2022/03/17/the-italian-agency-for-national-cybersecurity-embraces-the-star-program)

・イタリア国家サイバーセキュリティ庁(ACN)は、行政機関向けに提供されるクラウドサービスのセキュリティ要求事項の定義とその認証の一環として、CSAのクラウドコントロールマトリックスおよびSTARプログラムの重要な役割を再確認
・イタリア政府は、2022年1月28日、官民連携パートナーシップ(PPP)を通じた国家戦略ハブ(NSH／PSN)の創設に関する入札を発表(総額7億2330万ユーロの入札で、STARレベル2への準拠を義務付ける)
・ACNの新しい最低セキュリティ要求事項は、行政機関のデータを管理するクラウドサービス(IaaS/PaaS/SaaS)に適用される
・「重要」および「戦略的」な情報を管理するクラウドサービスに対して、STARレベル2の第三者認証の利用を規定する(従来は、SaaSサービスに対してのみSTARレベル1の自己適合宣言を要件としていた(約150社がSTARレベル1で登録))

イタリアクラウド戦略におけるCSA STARの位置付け

クラウドセキュリティアライアンス「イタリアにおけるコンプライアンス: 新しいイタリアのクラウド戦略をナビゲートする」(2023年3月30日)
(https://cloudsecurityalliance.org/blog/2023/03/30/compliance-in-italy-navigating-the-new-cloud-italy-strategy)

- イタリアクラウド戦略におけるデータおよびサービスの分類
  - 通常(Ordinary) (QC1)
  - 重要(Critical) (QC2)
  - 戦略的(Strategic) (QC3)
- イタリアの政府クラウドサービス適合性評価における最低限の要求事項
  - ISO 9001 認証
  - ISO 27001 認証(ISO 27017 および ISO 27018 を含む)
  - ISO 22301 自己適合宣言および/または認証
  - ISO 20000-1 自己適合宣言および/または認証
  - CSA STAR レベル 2 適合宣言または認証

イタリアクラウド戦略のコンプライアンス要求事項

分類	要求事項
通常 (QC1)	・ISO 9001 認証: クラウドサービスのための品質管理システム(QMS)の実装が必要 ・ISO/IEC 27001:2013 認証: 以下の拡張規格を含む情報セキュリティ管理システム(ISMS)の実装が必要: ・ISO/IEC 27017:2015 認証 ・ISO/IEC 27018:2019 認証 (上記のISO 27001要件の代替として、クラウドセキュリティアライアンス - STARレベル2認証の取得が可能)
重要 (QC2)	・QC1 のすべての要件を満たし、かつ ・ISO 22301 の自己適合宣言: 資格要件対象のクラウドサービスのための事業継続マネジメントシステム基準への準拠を宣言することが必要 ・ISO 20000-1 の自己適合宣言: 資格要件対象のクラウドサービスのためのサービスマネジメントシステム基準への準拠を宣言することが必要
戦略的 (QC3)	・QC1要件を満たし、かつ ・ISO 22301認証: 資格要件対象のクラウドサービスのための事業継続マネジメントシステムの実装が必要 ・ISO/IEC 20000-1認証: 資格要件対象のクラウドサービスのためのサービスマネジメントシステムの実装が必要 ・クラウドセキュリティアライアンスのSTARレベル2認証

5. CSAと欧州委員会／ENISAの連携活動(1)

欧州連合(EU)研究開発プログラムにおけるCSAの連携活動実績

プログラム／プロジェクト／ステータス			CSAの主な役割
FP7	HelixNebula	2014年終了	普及
FP7	CIRRUS	2014年終了	認証のベストプラクティス（グリーンペーパー）
FP7	CUMULUS	2015年終了	セキュリティ資産、継続的認証
FP7	CloudWatch	2015年終了	認証、セキュリティ基準のプロファイル
FP7	A4Cloud	2016年終了	標準化、相互運用性、責任の評価／認証
FP7	SPECS	2016年終了	標準化、開発、ツール、普及
Horizon 2020	PICSE	2016年終了	調達障壁の特定、ベストプラクティス
Horizon 2020	SLA-Ready	2016年終了	標準化、クラウドSLAマーケットプレイス
Horizon 2020	CloudWatch2	2016年終了	標準化、リスクプロファイリング
Horizon 2020	Cloud For Europe	2016年終了	仲介プラットフォーム設計、セキュリティおよびプライバシーの要求事項、認証
Horizon 2020	EU-SEC	2020年終了	欧州におけるクラウドセキュリティ認証の枠組みを策定

5. CSAと欧州委員会／ENISAの連携活動(2)

(参考)CSAジャパンSLAイノベーションWGの連携活動実績

出典：CSAジャパン「SLAイノベーションWGが「クラウドSLAの共通参照モデル／CSP評価モデル解説とデジタルヘルス分野事例の考察」を公開しました」(2018年5月21日) (https://www.cloudsecurityalliance.jp/site/?p=3650)

EUのR&D戦略「Horizon 2020」: EU-SEC

EU-SECコンソーシアム「欧州セキュリティ認証フレームワーク(EU-SEC)プロジェクト」(実施期間: 2017年1月1日～2019年12月31日)
(https://www.sec-cert.eu/)

・クラウドインフラのセキュリティを確保するための認証のスキームと評価の考え方についての欧州における枠組みを策定することをめざす
・既存のクラウドセキュリティスキーム(制度)間において、審査プロセスの一貫性も担保可能な、相互承認の枠組み創設を目的とする
・この枠組みの主な3つの柱
　相互承認の枠組み:広く知られている標準規格の共通点を特定し、それをマルチパーティ認識フレームワーク(MPRF)という明確で包括的なフレームワークの下に提示する
　継続的な審査・認証スキーム: 技術を利用して法令を遵守しない活動を継続的に監視しフラグを立てることによって、従来の認証を強化する
　プライバシー行動規範:CSAのプライバシーレベルアグリーメント(PLA)コードオブプラクティス(CoP)に基づいて、PLA行動規範を導入する

EUサイバーセキュリティ認証スキーム共通基準(EUCC)

欧州連合サイバーセキュリティ庁(ENISA)「EUが初のサイバーセキュリティ認証制度を採用」(2024年1月31日)

(https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme)

・欧州委員会が、EUサイバーセキュリティ認証スキーム共通基準(EUCC)に関する実施規則を採択したことを発表
・この結果は、ENISAが、欧州委員会の要請を受けて、業界全体およびEU加盟国の国家サイバーセキュリティ認証当局(NCCA)からの専門家で構成される特別作業グループ(AHWG)の支援を受けて起草したEUCC候補案と完全に一致する
・EUCCは、EUサイバーセキュリティ法に基づいて、EU市場におけるICT製品、サービスおよびプロセスのサイバーセキュリティレベルを向上させるために、EU全域で適用される一連の包括的なルール、技術標準要件、標準規格、および手続きを設定する
・EUCCは、17のEU加盟国(イタリア含む)ですでに使用されている実証済みのSOG-IS共通基準評価フレームワークに基づいており、製品、サービス、またはプロセスの使用に関連するリスクのレベル(事故の発生確率と影響の観点から)に基づいて、2つの保証レベルを提案している
・採択された法令で、選択された加盟国における既存の認証を引き続き活用できる移行期間を設定するとともに、EUCCの評価に関心のある適合評価機関(CAB)は、認定および通知を受けることができる
・ベンダーは、EUCCより指定された追加／更新要件に対してソリューションを評価した後、既存のSOG-IS証明書をEUCC証明書に変換できる(EUCCの下で発行された証明書はENISAによって公開される)

クラウドサービス向けサイバーセキュリティ認証スキーム(EUCS)

欧州連合サイバーセキュリティ庁(ENISA)「クラウドサービス向けサイバーセキュリティ認証スキーム(EUCS)候補草案」(2020年12月22日)*意見公募済

(https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme)

・ENISAは、欧州サイバーセキュリティ法第48条第2項に従い、欧州サイバーセキュリティ認証フレームワークの一環として、クラウドサービスに関する候補スキームの準備を行うための特別作業グループ(AHWG)を設置した
・AHWGによるレビューのための基礎資料として、クラウドサービス向けサイバーセキュリティ認証に関するEUCS候補スキームの草案を策定・公開して、意見を公募した
・EUCS候補草案の特徴:
  ・任意のスキームである
  ・スキームの証明書はEU加盟国全体で適用される
  ・IaaS、PaaS、SaaS、およびその他のクラウドサービスなど、すべての種類のクラウドサービスに適用される
  ・セキュリティ要求事項の参照セットを定義することで、クラウドサービスの信頼性を高める
  ・「基本」、「実質的」、「高」の3つの保証レベルをカバーする
  ・既存の国家レベルのスキームおよび国際標準規格に触発された新しいアプローチを提案する
  ・EU内の国家レベルのスキームからの移行パスを定義する
  ・更新可能な3年間の認証を提供する
  ・データ処理および保存場所などの透明性要求事項を含む

EUCC向け5Gセキュリティの取組

欧州連合サイバーセキュリティ庁(ENISA)「5Gセキュリティコントロールマトリックス」(2023年5月24日)

(https://www.enisa.europa.eu/publications/5g-security-controls-matrix)

・5Gネットワークのセキュリティコントロールとベストプラクティスの包括的かつ動的なマトリックスであり、EU加盟国の国家当局によるEUの5Gサイバーセキュリティツールボックスの技術的対策の実装をサポートする

CSAの「仮想化環境におけるリスク低減のためのベストプラクティス」(2015年4月)を参照

(https://cloudsecurityalliance.org/press-releases/2015/05/06/csa-launches-best-practices-for-mitigating-risks-in-virtualized-environments)

欧州連合サイバーセキュリティ庁(ENISA)「埋め込み型ユニバーサル集積回路カード(eUICC)認証に関する仕様」(2024年6月26日) ＊意見公募済

(https://certification.enisa.europa.eu/publications/specifications-related-certification-embedded-universal-integrated-circuit-card_en)

・eUICCは、一つ以上の埋め込み型加入者識別モジュール(eSIM)を含むセキュアな要素で、オペレーターやエンドユーザーにセキュアなソリューションを提供する

・ENISAは、消費者と業界の信頼をさらに向上させるために、eUICCのEUサイバーセキュリティ認証スキーム(EUCC)への適合性の認証を促進することを目指している

イタリア人工知能(AI)法案

イタリア議会上院「イタリア人工知能(AI)法案」(2024年5月20日)

(https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm)

・目的: 人間中心のアプローチに従い、AIの公平、透明、かつ責任ある利用を促進し、潜在的な経済的・社会的リスク並びに基本的権利へのリスクを監視する

　・欧州連合(EU)AI法と並行して適用され、補完する(EU AI法の定義を採用)

・目標:

　1. 公正なアルゴリズム処理: AIシステムの研究・テスト・開発・実装・適用において、個人の基本的な権利と自由、および透明性、比例性、セキュリティ、個人データの保護と機密性、正確性、非差別、ジェンダー平等とインクルージョンの原則を尊重しなければならない

　2. データの保護: AIシステムおよびモデルの開発は、利用されるセクターに応じたデータとプロセスに基づき、データが正確で信頼性があり、安全で、質が高く、適切かつ透明であることを確保しなければならない

　　・システムのライフサイクル全体でサイバーセキュリティが確保され、特定のセキュリティ対策が採用される必要がある

　3. デジタルの持続可能性: AIシステムおよびモデルの開発と実装は、人間の自律性と意思決定を確保し、害の防止、透明性、説明可能性を確保しなければならない

・所管: イタリアデジタル庁(AgID) - AIイノベーションおよび開発(AIシステムのコンプライアンス評価含む)

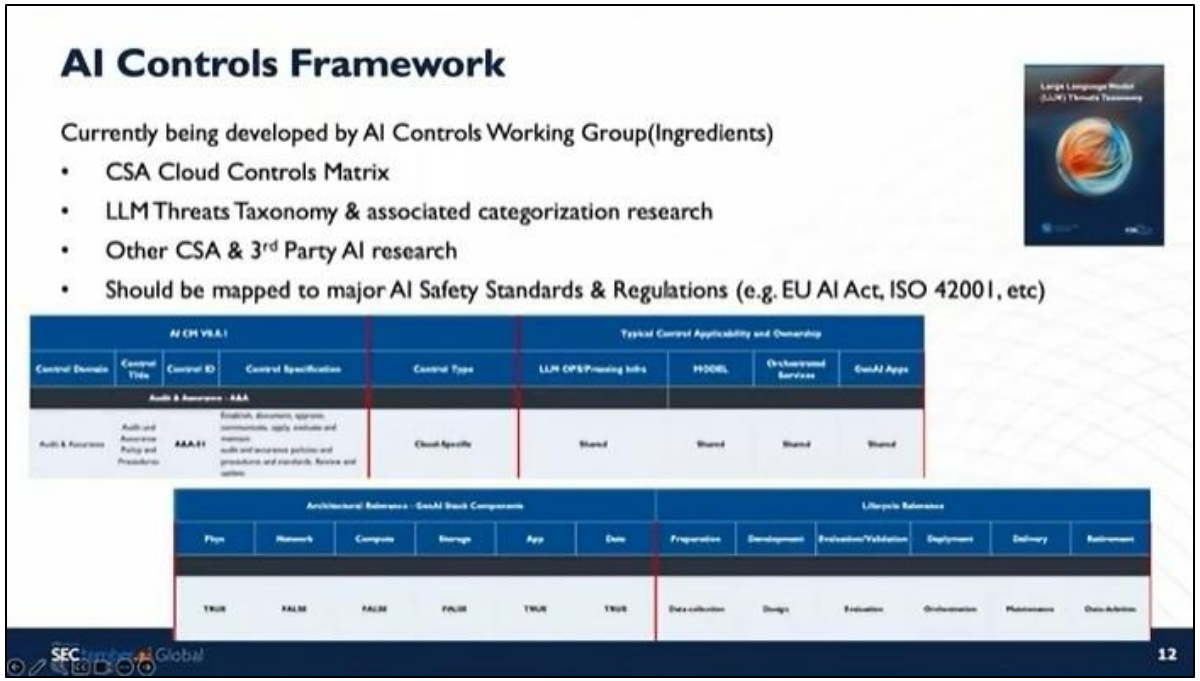
　イタリア国家サイバーセキュリティ庁(CAN) – 国家安全保障を守るためのサイバーセキュリティの監視

医療分野におけるイタリアAI法案の取扱

・医療分野でのAIの利用
　・一般的な法案の目的として、AIシステムは医療システムの改善、病気の予防および治療に貢献し、個人の権利、自由、および利益(データ保護の権利を含む)を尊重する必要がある
　・医療システムにおけるAIシステムの利用では、差別的な基準で医療サービスへのアクセスを選択したり、影響を与えたりしてはいけない
　・個人は、AIの使用および診断および治療に関する利点について情報を得る権利を持ち、意思決定に関与するロジックについて情報を取得する権利も有する
　・AIシステムは、予防、診断、治療および治療選択のプロセスを支援することを目的としており、意思決定は医療専門家の権限内に留まる必要がある
・ヘルスケア分野でAIシステムを開発するための科学研究:
　・法案は、公的および私的非営利団体が実施する科学研究に関連するデータ保護義務を簡素化することを目的としており、AIシステムの予防、診断および治療のための開発、医薬品の開発、治療およびリハビリテーション技術の開発、医療機器の製造のための科学研究目的での個人データ(健康データを含む)の処理が含まれる
　　・GDPR第9条第2項(g)に従い、目的を「重要な公益」に特定することにより、データ主体の同意を得る必要性を解除する(ビジネスおよび営利活動には適用されない)
　　・直接識別子を削除した個人データ(特別カテゴリーのデータを含む)の二次使用を、上記の「重要な公益」のための処理に対して認可する(研究が変更された場合でも、新しい同意は不要となる)

6. STAR for AIの紹介

クラウドセキュリティアライアンス「CSAのAIセーフティイニシアティブ最新情報とグローバルAIシンポジウムへの道」(2024年9月26日)
(https://www.youtube.com/watch?v=qXRoZs45n9I)



出典：Cloud Security Alliance「CSA's AI Safety Initiative Update and the Road to the Global AI Symposium」(2024年9月26日)
(https://www.youtube.com/watch?v=qXRoZs45n9I)

STAR for AIのロードマップ

・CSA AIコントロールマトリクスの作成(2024年第4四半期: 草案ピアレビュー、2025年第1四半期／第2四半期: バージョン1.0)
・AIセーフティ保証(AIコントロールフレームワーク草案版から派生したSTAR for AIを事前にサポートすることを保証するハイレベルの原則)の作成
・STAR for AI計画を告知する第1弾のプレスリリース(2024年第4四半期: AIコントロールフレームワークのピアレビューの実施、AIセーフティ保証の実施、STAR for AIロードマップ)
・CSA AIコントロールフレームワーク1.0および利用ガイダンスと初期パイロットのリリース(2025年第１四半期-第２四半期)
・認証／自己宣言スキームの明確化(2025年第2四半期-第3四半期)
・初期監査人の認定(2025年第3四半期-第4四半期)
・STAR for AIの初期監査人、教育、準備ツールを告知する第2弾のプレスリリース(2025年第3四半期-第4四半期)
・STAR for AIの立ち上げ(2025年第4四半期-2026年第1四半期)

https://www.youtube.com/watch?v=qXRoZs45n9I

7. まとめ／Q&A

Sede: Via Cesare Beruto 11,
20131 Milano, Italy
https://cloudsecurityalliance.it/
Email: info@csaitaly.it

https://www.linkedin.com/in/esasahara

https://www.facebook.com/esasahara

https://x.com/esasahara