GDPR, COMPLIANCE FATIGUE AND CONTINUOUS ASSURANCE: LET CSA HELP YOU!

GDPR対応の重荷と継続的保証：ＣＳＡがお手伝いします!

***Daniele Catteddu**, CSA Chief Technology Officer*

AGENDA

PROBLEM STATEMENT
何が問題か

BRIEF INTRO ON THE GDPR & CSA CODE OF CONDUCT
GDPRとCSAのCOC（行動規範）の簡単な紹介

CONTINUOUS AUDITING BASED CERTIFICATION / STAR LEVEL 3
継続的監査に基づいた認証/STAR LEVEL3

MUTUAL RECOGNITION FOR SECURITY CERTIFICATION SCHEMES
セキュリティ認証スキームとの相互認証


CSA
cloud
security
alliance®

ABOUT THE CLOUD SECURITY ALLIANCE

- Global, not-for-profit organization
- Over 90,000 individual members, more than 400 corporate members, and 80+ chapters
- Building best practices and a trusted cloud ecosystem
  - Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

CSAについて

- 国際的非営利活動組織
- 個人会員9万人以上、400以上の企業会員、80以上の地域支部
- クラウドの実践規範と信頼に基づくエコシステムの構築
  - 柔軟な思考、実践的研究のスピーディな展開
  - GRC：コンプライアンスとリスク管理のバランス
  - リファレンスモデル：既存の標準を活用して構築
  - アイデンティティ：クラウドエコノミー実現の基礎
  - 相互運用性の確保
  - イノベーションの推進
  - しっかりした、広く適用できるポリシーの唱道

クラウドコンピューティングにおけるセキュリティ保証に向けた実践規範活用の促進と、クラウド利用のための教育を通じてあらゆるコンピュータ利用のセキュリティを高めるための活動への取組み

ABOUT THE CLOUD SECURITY ALLIANCE　CSAについて

- RESEARCH
  - https://cloudsecurityalliance.org/research/
- ADVISE GOVERNMENTS AND PRIVATE COMPANIES
- EDUCATION – PROFESSIONAL CERTIFICATION – TRAINING
  - https://cloudsecurityalliance.org/education/
- PROVIDER CERTIFICATION
  - https://cloudsecurityalliance.org/star/
- STANDARDS
  - https://cloudsecurityalliance.org/isc/
- EVENTS
  - https://cloudsecurityalliance.org/events/

- 研究開発
  - https://cloudsecurityalliance.org/research/
- 政府や企業に対する助言
- 教育　ー専門家の認定制度　ートレーニング
  - https://cloudsecurityalliance.org/education/
- クラウド事業者向け認証
  - https://cloudsecurityalliance.org/star/
- 標準
  - https://cloudsecurityalliance.org/isc/
- イベント
  - https://cloudsecurityalliance.org/events/

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

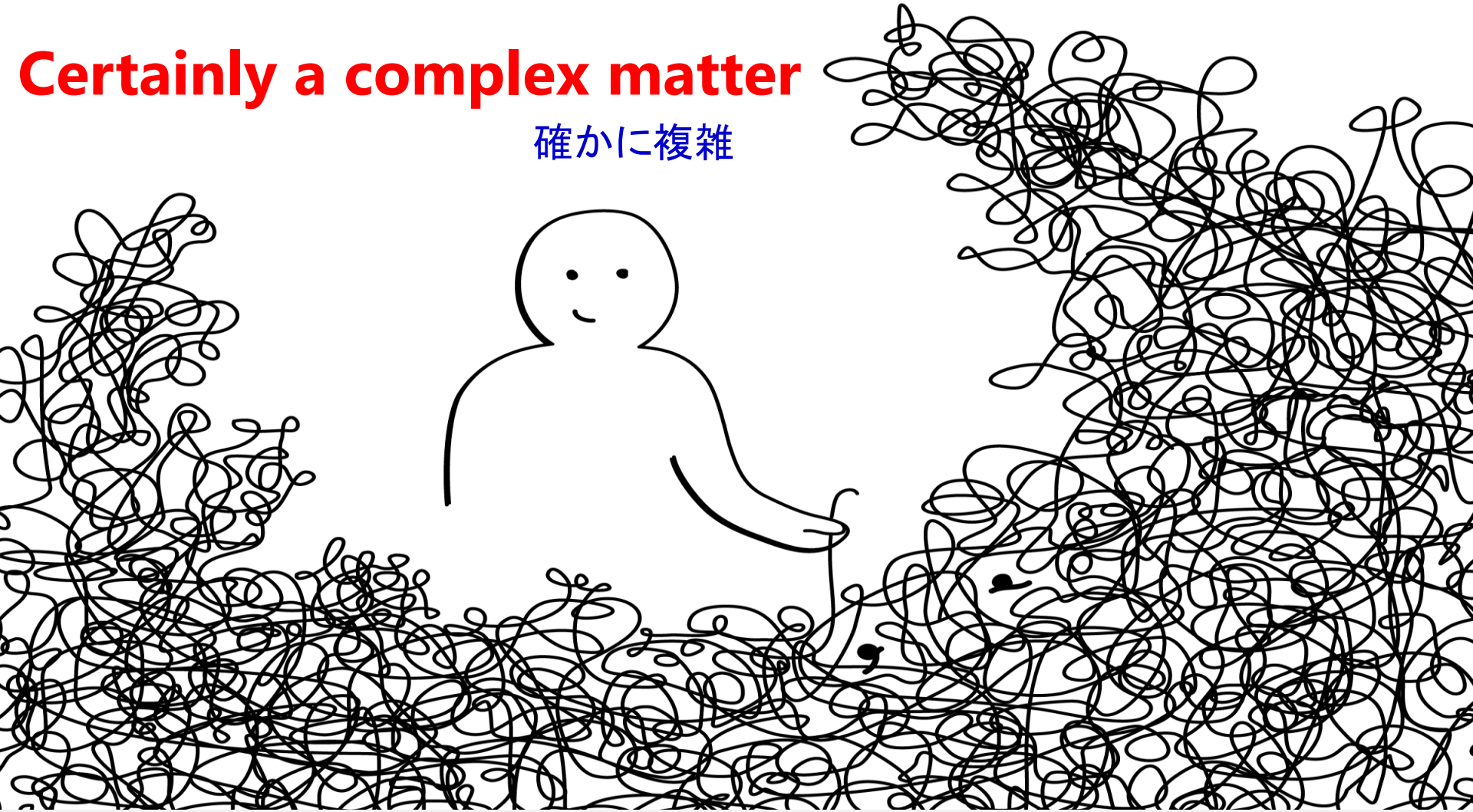
Compliance and assurance: an excessive burden?

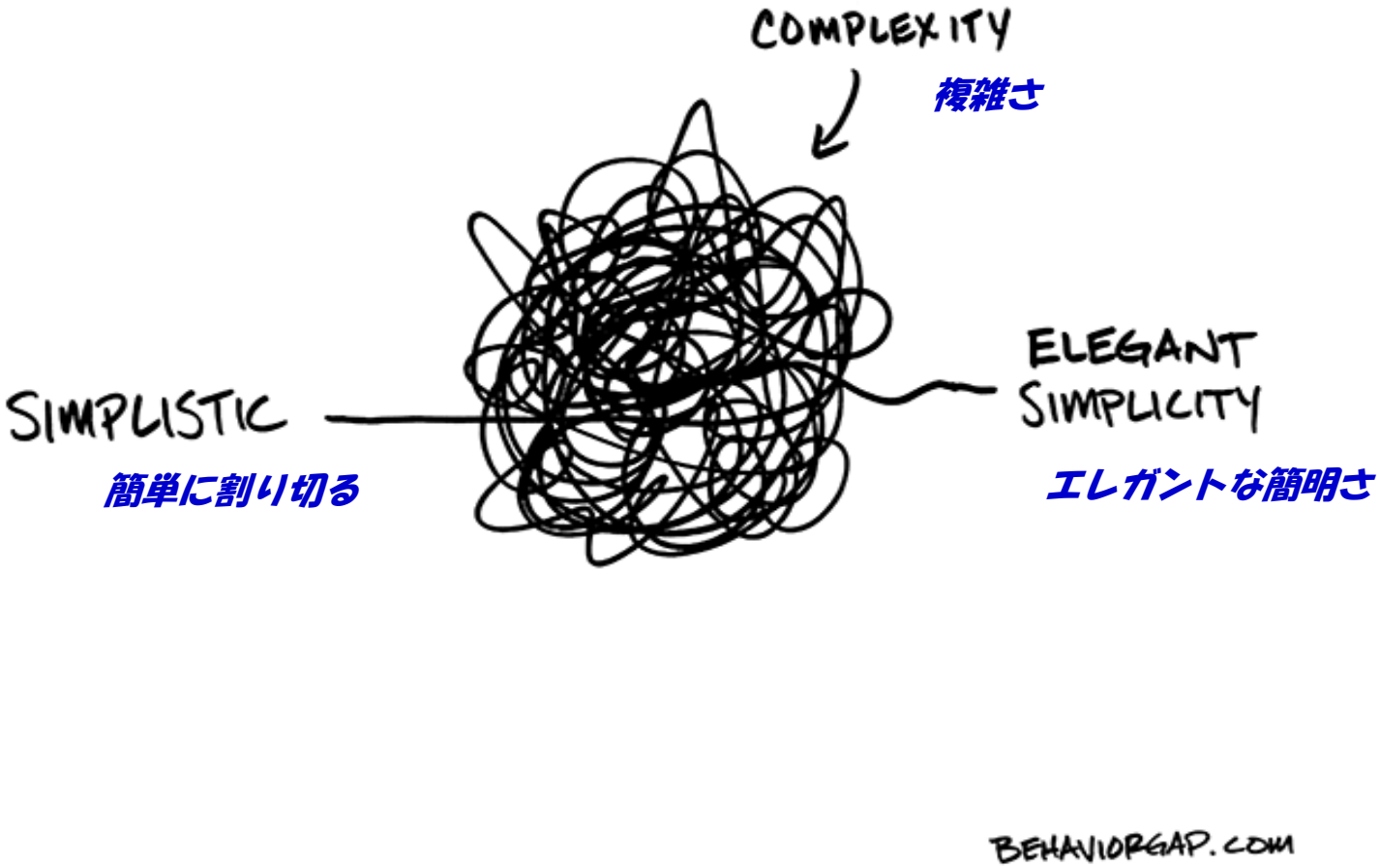
コンプライアンスと保証：重すぎる負担？

Jon Berkeley

Certainly a complex matter

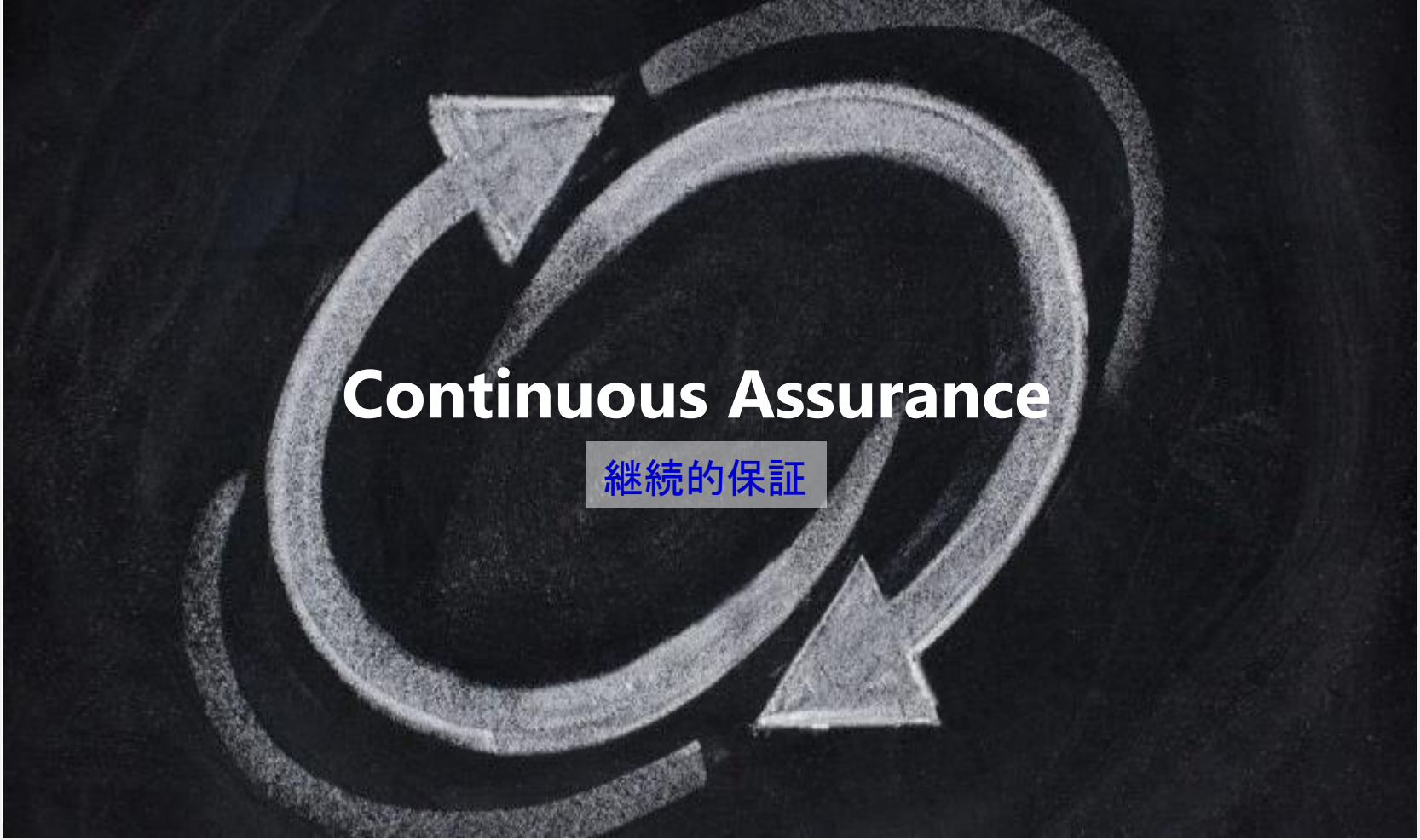
確かに複雑




COMPLEXITY
複雑さ
SIMPLISTIC
簡単に割り切る
ELEGANT
SIMPLICITY
エレガントな簡明さ
BEHAVIORGAP.COM

Proliferation of compliance schemes 順守すべき基準の増殖

Fig1. Compliance Templates Provided By Microsoft


Continuous Assurance
継続的保証


THE
GDPRrrrr
ジー
ディー
ピー
アーーー
ーーーール

GENERAL DATA PROTECTION REGULATION (GDPR)

一般データ保護規制(GDPR)

SCOPE & TIMELINE

スコープとタイムライン

Broader territorial reach than the current regime

GDPR applies where processing takes place *"in the context of the activities of an establishment of a controller or processor in the EU"*

GDPR applies to controllers outside the EU when processing activities relate to:

- **offering goods or services to data subjects in the EU**
- monitoring the behavior of data subjects in the EU

現状の枠組みよりも広範な地域を対象

GDPRは、*「EU域内のデータ管理者またはデータ処理者である存在の活動に関連して」*処理が行われる全ての場所に適用される

GDPRは処理作業が以下に関連する場合EU域外のデータ管理者に適用される:

- **EU内のデータ主体に対して商品やサービスを提供すること**
- EU域内のデータ主体の動向をモニタすること

APRIL 2016
GDPR was enacted

2016年4月
GDPR制定

MAY 2016
Text published in the OJEU, enters into force 20 days after publication

2016年5月
EU官報に文書掲載。
発行後20日で施行

MAY 25, 2018
GDPR applies throughout the EU after 2-year transition period

2018年5月25日
2年の移行期間経過後、
GDPRをEU全域に適用

GAME CHANGERS

1. Principle of Accountability & Transparency
1. 説明責任と透明性の原則
2. Data protection compliance is becoming increasingly risk-based
2. データ保護義務はより一層リスクベースに
3. Privacy by design and by default
3. プライバシーバイデザインとデフォルトプライバシー
4. Right to be forgotten and data portability
4. 忘れられる権利とデータの可搬性

世の中の流れが変わる

5. Sanctions and Enforcement
5. 制裁と強制
6. Fines and enforcement
6. 罰金と執行

- Data subjects' right to remedies:
- データ主体の救済を受ける権利
- Right to start legal action
- 法的手段開始の権利
- Joint liability of controllers and processors
- データ管理者と処理者の共同責任
- Class actions
- 集団訴訟

CODES OF CONDUCTS & CERTIFICATION

The Regulation “encourages” the use of:

- **codes of conducts** and
- **certification mechanisms**

SCOPE: to ensure **transparency** and **compliance** to the law

行動規範(Codes of Conducts)と認証

GDPRは以下のものの利用を「推奨」

- 行動規範(Codes of Conducts)
- 認証メカニズム

スコープ： 透明性と法の遵守を確実なものにすること

CSA
CODE OF CONDUCT
FOR GDPR COMPLIANCE

GDPR遵守に向けたCSAの行動規範
(Code of Conduct)

DPA'S OPINIONS ON THE PLA WORK

データ保護当局者のPLA*の成果に対する評価

CSA

*Privacy Level Agreement

I think [the PLA Outline] is a very helpful document, both for potential customers of CSPs and for CSPs themselves.

By following closely the WP29 Opinion, it ensures that both parties understand the obligations under EU law – probably the strictest requirements they will have to comply with.

Hopefully it will be accepted by CSPs that, if they want to be viewed as acceptable service providers – especially by EU-based organisations – they are going to have to be able to answer successfully the questionnaire that is annexed to the document.

BILLY HAWKES, IRISH DATA PROTECTION COMMISSIONER

「PLAの概要」はクラウド事業者とその利用者の双方にとってたいへん有用な文書だと思う

29条作業部会の意見に忠実に沿うことで、事業者利用者双方がEU法の下での義務ーおそらく彼らが従うべき最も厳しい要求事項ーを理解できるようにしている。

これがCSPに受け入れられ、利用してもよい事業者だとー特にEU内の組織にー認められるには、同書の付属質問事項に満足いく回答ができる必要があると、CSPが考えることを期待する。

アイルランドデータ保護コミッショナー Billy Hawkes

Transparency and information are key to build trust in the cloud ecosystem.

This is why the CNIL has actively contributed to the elaboration of the PLA-outline.

As it gets gradually adopted by CSPs, it will become an important building block for constructing a modern ethical and privacy-preserving framework, adequate to the challenges that face all stakeholders in the digital world.

ISABELLE FALQUE-PIERROTIN, PRESIDENT OF THE CNIL

クラウドエコシステムにおいて透明性と情報は信頼を獲得するための鍵となる

そのために、CNILはPLAの概要という力作を仕上げるのに積極的に貢献した。

CSPがこれを適用していくにしたがって、今日に見合う倫理性を備えた、プライバシー保護のためのフレームワークを構築する、重要な構成要素となり、デジタル世界の全ての参加者にとっての課題に対応するに足るものになると期待される。

CNIL*総裁　Isabelle Falque-Pierrrotin

*CNIL: フランス情報処理及び自由に関する国家委員会

CSA CODE OF CONDUCT: GOALS

CSAの行動規範(Code of Conduct): ゴール

- Provide CSPs a tool to achieve EU data protection and compliance and demonstrate it through self attestation or certification
- Provide the Cloud Customer with a tool to evaluate the level of CSP data protection compliance

- CSPがEUデータ保護遵守を達成し、それを自己評価証明または自己認証により、示すことができるための、ツールを提供すること。
- クラウド利用者が、CSPのデータ保護遵守レベルを評価するためのツールを、提供すること。

CSA CODE OF CONDUCT: SCOPE & STRUCTURE

CSAの行動規範(Code of Conduct):スコープと構成

- Structured in 2 components
  - Privacy Level Agreement (PLA) Code of Practice (CoP)
  - Governance structure and mechanisms of adherence
- Deals with the 'B2B' scenario
- Detailed list of GDPR requirements
- Strongly based on WP29 Opinions, ENISA Guidelines and ISO standards
- Considers differences between CSP-controller and CSP-processor

- 2つの要素で構成
  - プライバシーレベルアグリーメント(PLA)実践規範(CoP)
  - 統制の構造と遵守の仕組み
- B2B取引を想定
- GDPR要求事項の詳細なリスト
- 29条作業部会意見書、ENISAガイドライン、ISO基準に忠実に準拠
- データ管理者であるCSPとデータ処理者であるCSPの相違点に対する配慮

PLA CODE OF PRACTICE: REQUIREMENTS

1	CSP declaration of compliance and accountability	9	Data portability, migration, and transfer back
2	CSP relevant contacts and its role	10	Restriction of processing
3	Ways in which the data will be processed	11	Data retention, restitution, and deletion policies
4	Record keeping	12	Cooperation with the cloud customers
5	Data transfer	13	Legally required disclosure
6	Data security measures	14	Remedies for cloud customers
7	Monitoring	15	CSP insurance policy
8	Personal data breach		

PLA実践規範(Code of Practice): 要求事項

1	CSPのコンプライアンスと説明責任の言明	9	データの可搬性、移転、返送
2	CSPの連絡窓口とその役割	10	処理の制限
3	データ処理の方法	11	データの保持、制限、削除ポリシー
4	記録保持	12	クラウド利用者への協力
5	データの移送	13	法定の開示
6	データセキュリティ対策	14	利用者への救済
7	モニタリング	15	クラウド事業者の保険のポリシー
8	個人データの侵害		

PLA CODE OF PRACTICE: CONTROL SPECIFICATIONS

PLA実践規範(Code of Practice):管理策の仕様

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			WWP-1.13	*13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., ...ort production) and those conducted at the CSP's initiative (e.g., backup, di... recovery, fraud monitoring).*	Applicable	Not Applic...
			WWP-1.14	*CSPs that are **processors** provide to cloud customers*		
				14. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor (General Information - applicable to CSPs that are processors).		
			W...15	*15. Specify how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors)*	Applicable	Applicable
		2 Personal data location	WWP-2.1	*1. Specify the location(s) of all data centres or other data processing locations (by country) where personal data may be processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means).*	Applicable	Applicable
		3 Subcontractors	WWP-3.1	*1. Identify subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.*	Applicable	Applicable
			WWP-3.2	*2. Declare to cloud customers that the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.*	Not Applicable	Applicable
			WWP-3.3	*3. Declare to cloud customers that the CSP imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law;*	Not Applicable	Applicable

...WAYS IN WHICH THE ...DATA WILL BE ...PROCESSED.

要求事項

要求事項ID

管理策

管理策ID

仕様

CSPがデータ管理者

CSPがデータ処理者

適用

適用外

MECHANISMS OF ADHERENCE

遵守の仕組み

ADHERENCE MECHANISM

遵守の仕組み

The CSA CoC for GDPR Compliance contemplates 2 adherence mechanisms:

1. Self Attestation
2. Third-Party Certification

GDPR遵守のための CSA行動規範は、2つの遵守の仕組みを用意している。

1. 自己評価証明
2. 第三者認証

CSA COC SELF ASSESSMENT

- Voluntary publication on the CSA STAR Registry of the:
  - Code of Conduct Statement of Adherence
  - Self-assessment results based on the PLA Code of Practice (CoP) Template
- No review done by an independent third party
- The CSA provides the adherent Compliance Mark valid for 1 year
- Must be revised every time there's a change to the company policies or practices related to the service under assessment

CSA 行動規範 自己評価証明

- 自己申告による CSA STAR レジストリ上での公表:
  - 行動規範遵守声明
  - PLA実践規範テンプレートに基づく自己評価結果
- 第三者による独立の評価は行わない
- CSAは、申請者に、1年間有効のコンプライアンスマークを発行
- 会社のポリシーまたは評価対象のサービスに関連した実施事項に変更がある都度、更新すること

CSA COC CERTIFICATION

- The CSA CoC Certification is a component of the CSA STAR
- The assessment is done by a Qualified Auditing Partner
- The validation process aims to verify:
  - the correct implementation of CoP Requirements
  - the accuracy of information included in CoP Template.
- The CSA provides the adherent with a Compliance Mark valid for 12 months.
- Must be revised every time there's a change to the company policies or practices related to the service under assessment.

CSA 行動規範認証

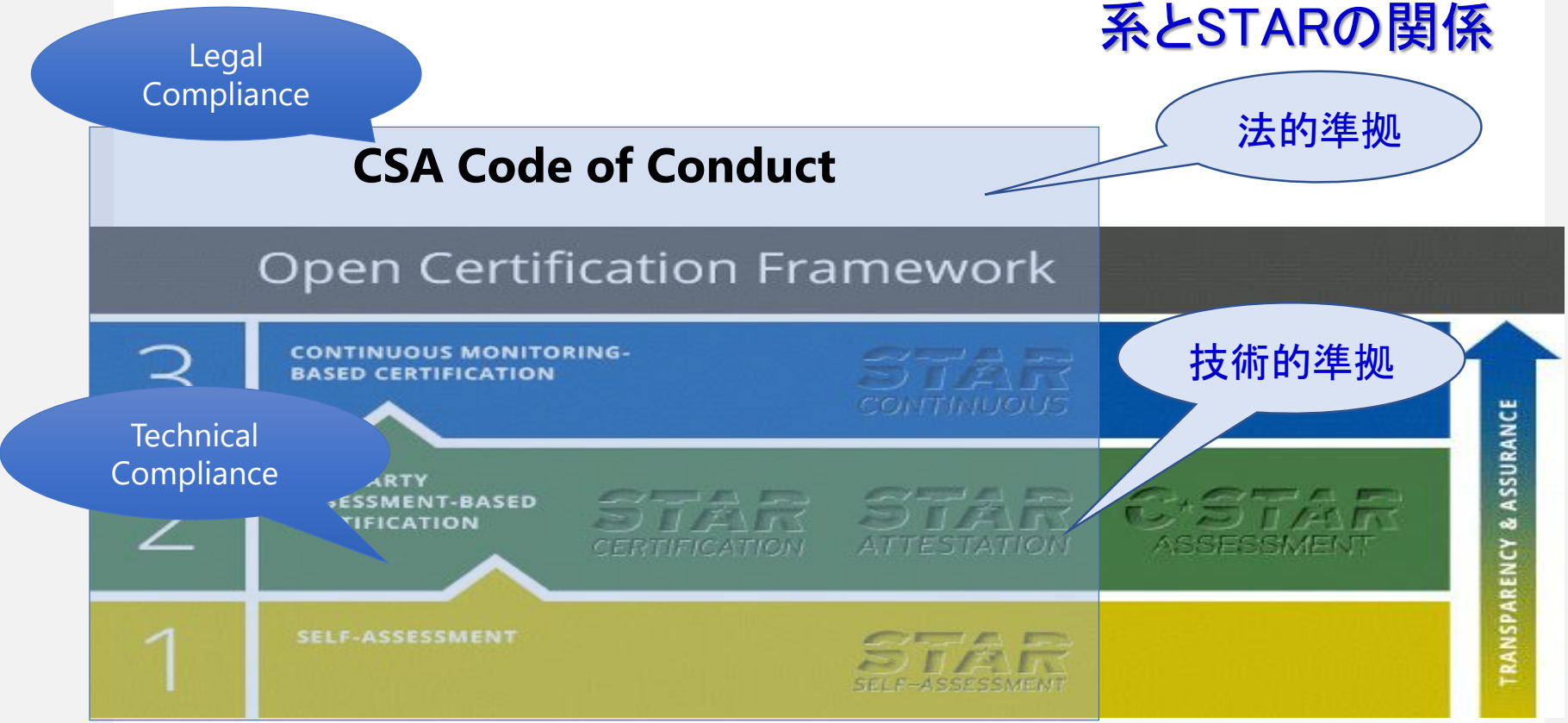
- CSA行動規範認証は CSA STAR の一部
- 評価は認定監査機関が実施
- 評価検証プロセスは以下を検証:
  - 実践規範要求事項の適正な実装
  - 実践規範テンプレートへの記載内容の正確性
- CSAは、申請者に、12ヵ月間有効のコンプライアンスマークを発行
- 会社のポリシーまたは評価対象のサービスに関連した実施事項に変更がある都度、更新すること

CSA CODE OF CONDUCT
&
THE STAR PROGRAM

CSAの行動規範(Code of Conduct)と
STARプログラム

THE PRIVACY OVERLAY

プライバシーの体系とSTARの関係



CODE OF CONDUCT & STAR PROGRAM

- The CSA CoC provides a set of legal controls for CSPs to comply with GDPR legal requirements
- The CCM provides a set of technical security controls for CSP to align with market needs and comply with legal requirements.
- The joint adoption of the CoC and CCM provides CSPs with a compliance suite for both legal and technical security requirements of GDPR.
- Adherence to CoC and CCM requirements can be demonstrated by achieving a combination of
  - STAR Certification or STAR Attestation or STAR Self Assessment and
  - CODE OF CONDUCT Certification or Self Assessment

CSA 行動規範とSTARプログラム

- CSA行動規範は、CSPがGDPRの法的要求事項を遵守するための法務面の管理策一式を提供
- CCMはCSPが市場の要求を満たし法的要求事項を遵守するための技術的セキュリティ管理策一式を提供
- 行動規範とCCMの同時適用はCSPにGDPRの法的および技術的要求事項を遵守するためのセットを提供
- 行動規範とCCMの遵守は以下のものを併せて達成することで証明可能:
  - STAR認証、STAR評価証明、STAR自己評価　のいずれか
  - 行動規範の認証または自己評価

CONTINUOUS ASSURANCE WITH STAR LEVEL 3

STAR Level 3による継続的保証

CONTINUOUS AUDITING - WHY?

Despite the wealth of certified cloud services available today, some customers in heavily regulated sectors, such as banking or health do not feel confident enough to move to the cloud.

For them, once-a-year audits applied in "traditional" certification are not enough.

Assurance should be given every month, week, day…

なぜ継続的監査が必要か？

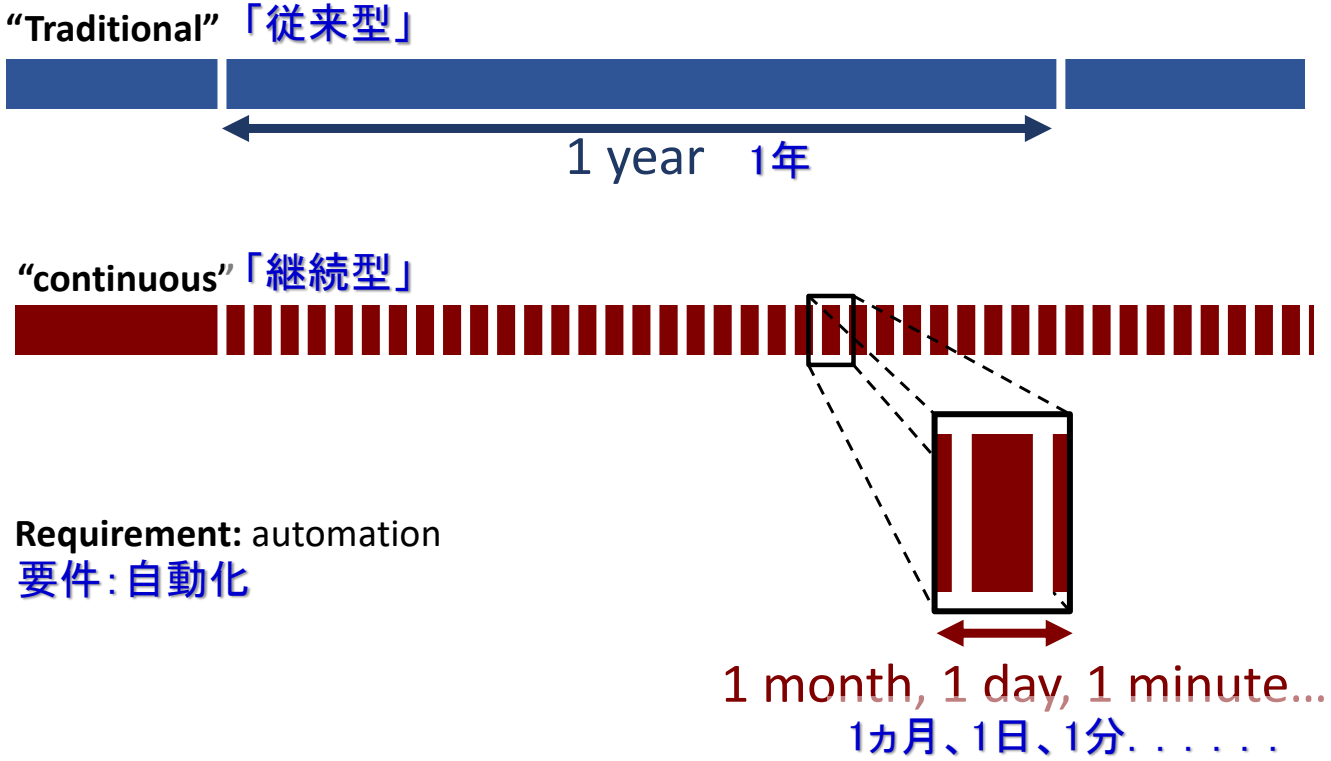
今日、認証を受けた価値あるクラウドサービスが提供されているにもかかわらず、厳しい規制のある業界、銀行や健康医療分野では、クラウドへの移行に十分確信が持てずにいる。

そのような業界では、「伝統的な」認証における、年1回の監査では不十分なのである。

保証は月単位、週単位、日単位、といった頻度で提供される必要がある。。。

“Traditional” vs “continuous audit-based” certification

「従来型」vs「継続的監査ベース」の認証



CONTINUOUS AUDITING - WHAT?

継続的監査とは？

Continuous Auditing: An on-going audit process that aims to assess Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.

継続的監査:

継続して行われる監査のプロセスで、サービス品質目標(SQO: Service Qualitative Objectives)とサービスレベル目標(SLO: Service Level Objectives)を評価するために、監査の目的に照らして必要な頻度で実施されるもの。

CONTINUOUS AUDIT-BASED CERTIFICATION

Continuous audit-based certification: The regular production of statements indicating that an information system meets a set a predefined of SLOs and SQOs, each reported at an expected frequency through continuous auditing.

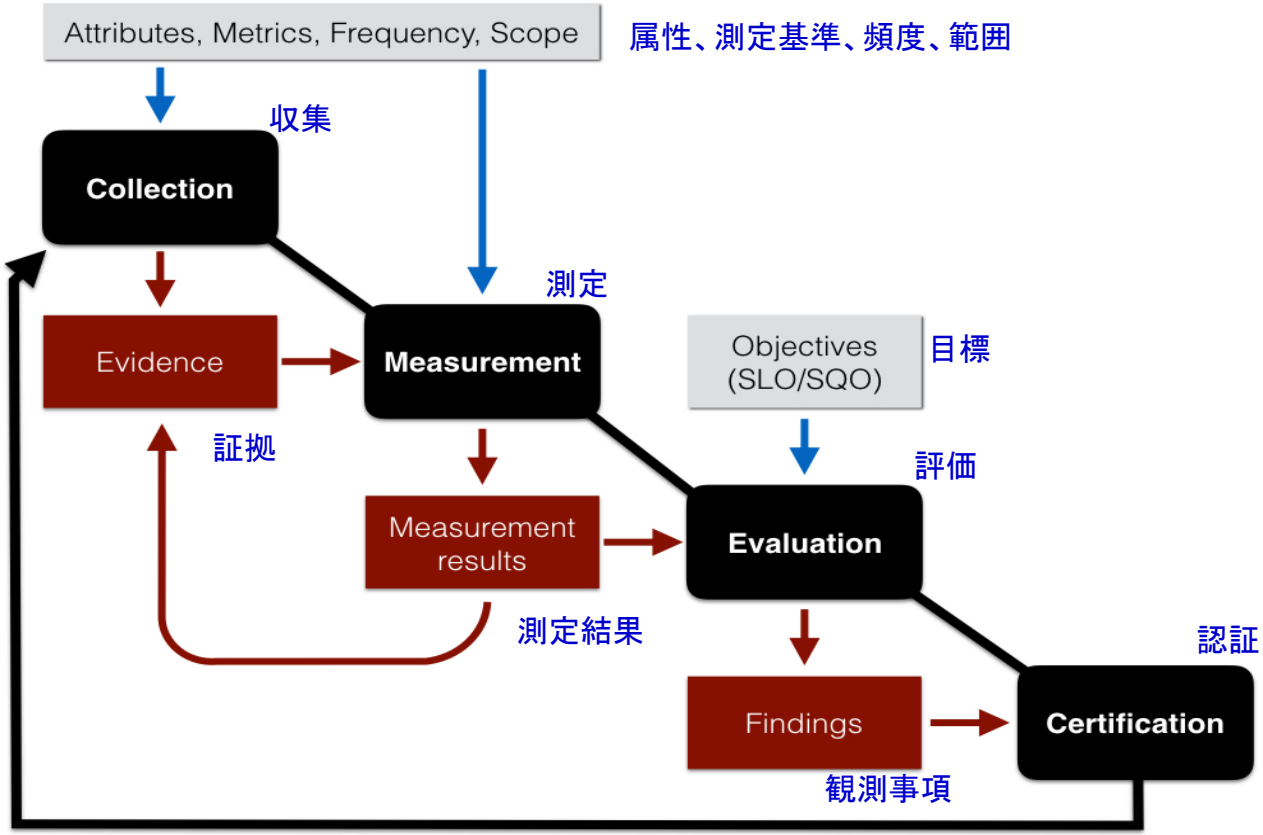
継続的監査ベースの認証

継続的監査ベースの認証:

ステートメントを定期的に発行し、対象となる情報システムが、予め設定されたSLOとSQOに適合していることを示すもので、各レポートは、継続的監査を通じて、予定された頻度で提供される。

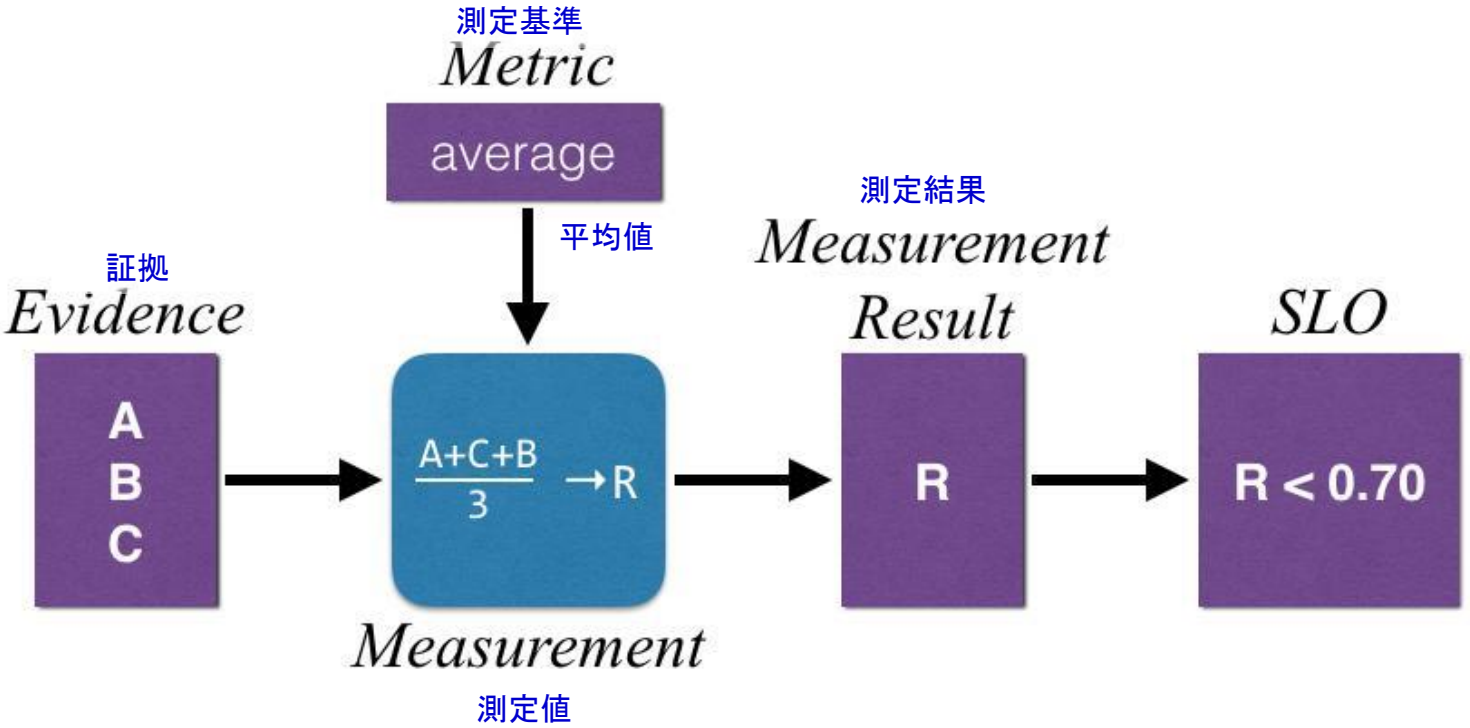
CONTINUOIUS CERTIFICATION PROCESS

継続的認証のプロセス



EVALUATION OF A SERVICE LEVEL OBJECTIVE

サービスレベル目標(SLO)の評価



3 levels of continuous audit-based certification

継続的監査ベースの認証の3つのレベル

3 **Continuous Certification**

Auditor:
- Continuous auditing
- Auditing tools/process review
- Traditional audit

継続的認証

監査主体
- 継続的監査
- 監査ツール/手順の評価
- 従来型監査

2 **Extended certification with continuous self-assessment**

Auditee:
- Continuous auditing

Auditor:
- Auditing tools/process review
- Traditional audit

継続的自己評価の拡張認証

被監査主体
- 継続的監査

監査主体
- 監査ツール/手順の評価
- 従来型監査

1 **Continuous self-assessment**

Auditee:
- Continuous auditing
- Auditing tools/process review

継続的自己評価

被監査主体
- 継続的監査
- 監査ツール/手順の評価

MUTUAL RECOGNITION OF CERTIFICATION THROUGH THE STAR PROGRAM

STARプログラムを通じた認証の相互認証

MULTIPARTY RECOGNITION FRAMEWORK

相互認証のフレームワーク

CSA is developing a multiparty recognition framework for cloud security certifications for trustful and compliant use of Cloud Computing

This work is partially done the context of the EC funded project EU-SEC

CSAでは、クラウドコンピューティングを信頼に基づき、かつ基準に準拠して活用するために、クラウドセキュリティの複数主体による認証の枠組みを開発中。

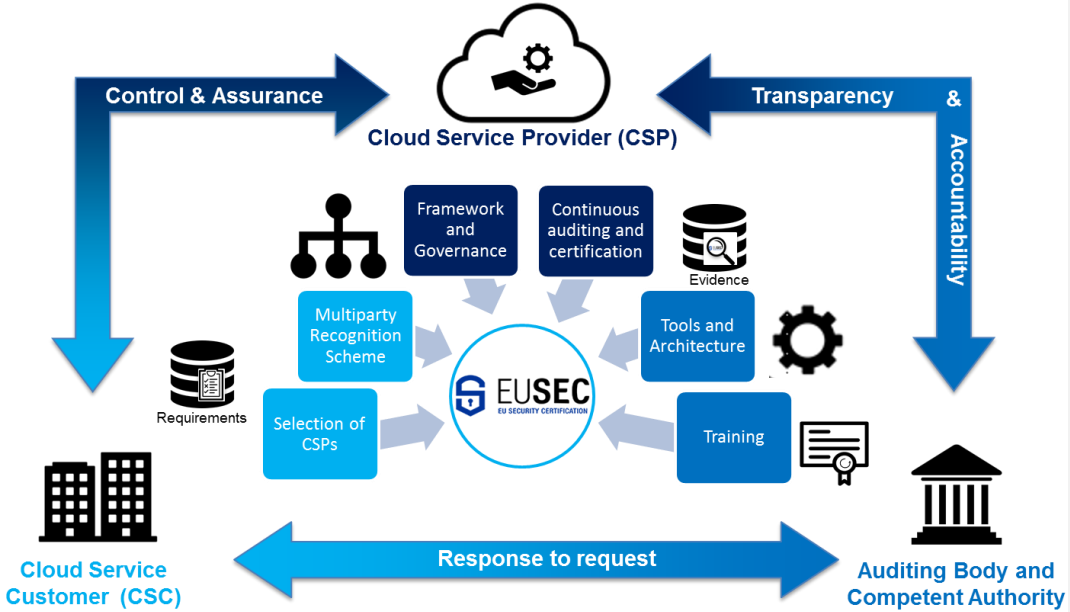
この作業の一部は、ECの資金援助によるプロジェクト「EU-SEC」の内容として完了済み。

EU-SEC – OBJECTIVES AT A GLANCE

EU-SECの開発目標の概要

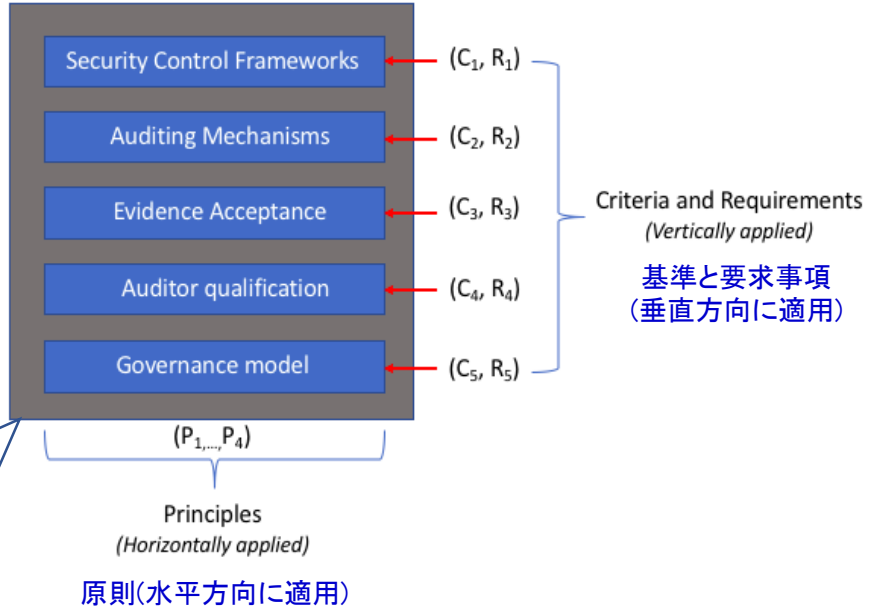
European Security Certification Framework (EU-SEC) is an innovation project with an aim to create a framework under which existing certification and assurance approaches can co-exist. It has a goal to improve the business value, effectiveness and efficiency of existing **cloud security certification schemes**.

EU-SEC (European Security Certification Framework)は革新プロジェクトで、現存する認証と保証の取り組みを共存させるための枠組みを開発することを狙いとしている。目指すところは、現存するクラウドセキュリティの認証スキームのビジネス的価値、有効性、効率性を改善することにある。



KEY CERTIFICATION SCHEME COMPONENTS
認証スキームの鍵となる構成要素

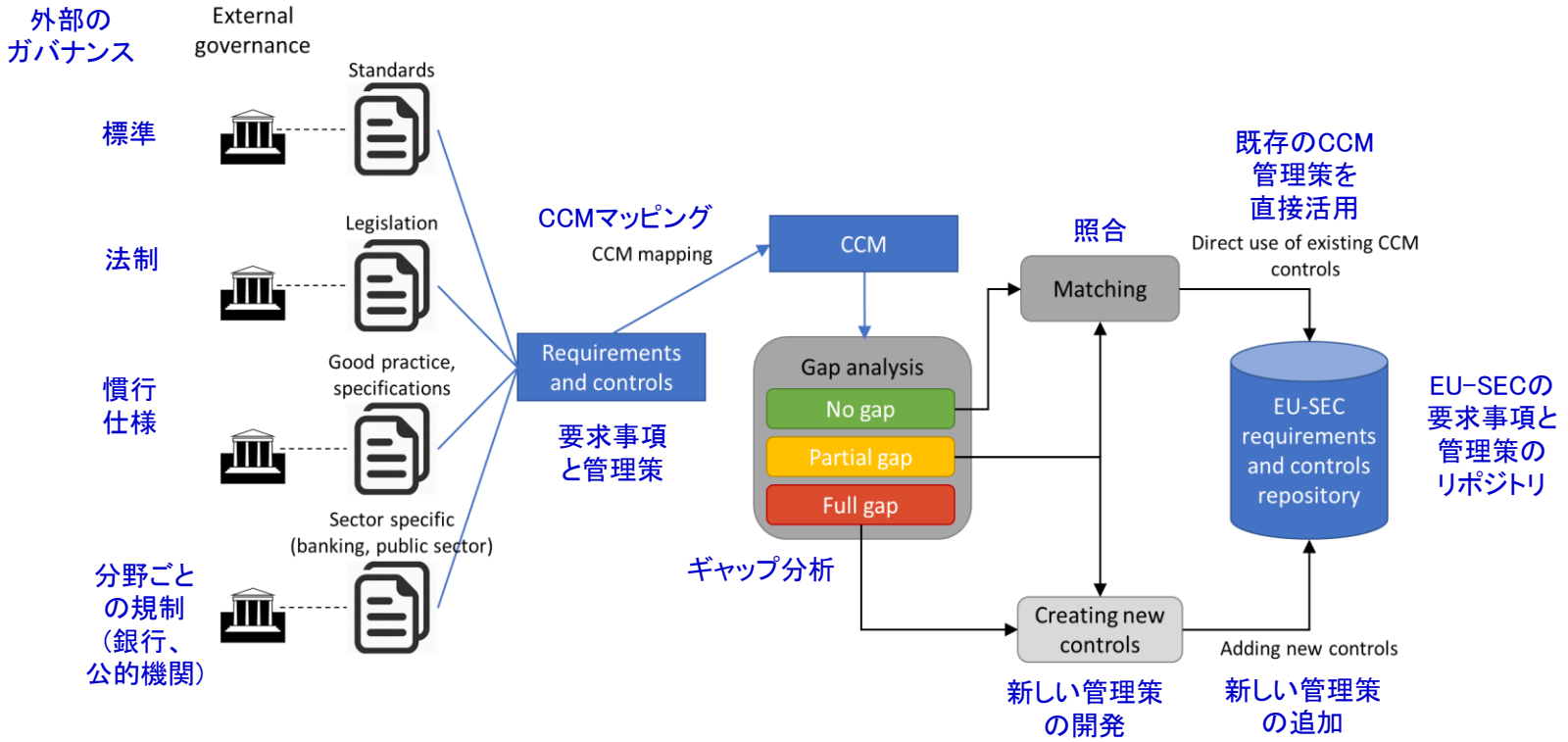
クラウドセキュリティ認証の
共通比較事項
Cloud security certification
common areas of comparison



- Security Control Frameworks — セキュリティ管理策の枠組み
- Auditing Mechanisms — 監査の仕組み
- Evidence Acceptance — 証拠の受け入れ
- Auditor qualification — 監査人の認定
- Governance model — ガバナンスモデル

THE KEY ROLE OF CCM

鍵となるCCMの役割



SUCCESS STORY SO FAR..

- German Federal Security Agency (BSI) – C5
- USA General Service Administration (GSA) - FedRAMP
- Singapore Infocomm Media Development Authority - MTCS
- Italian Digital Agency (AGID) – SaaS accreditation
- And more to come

JAPAN?

今までの成果

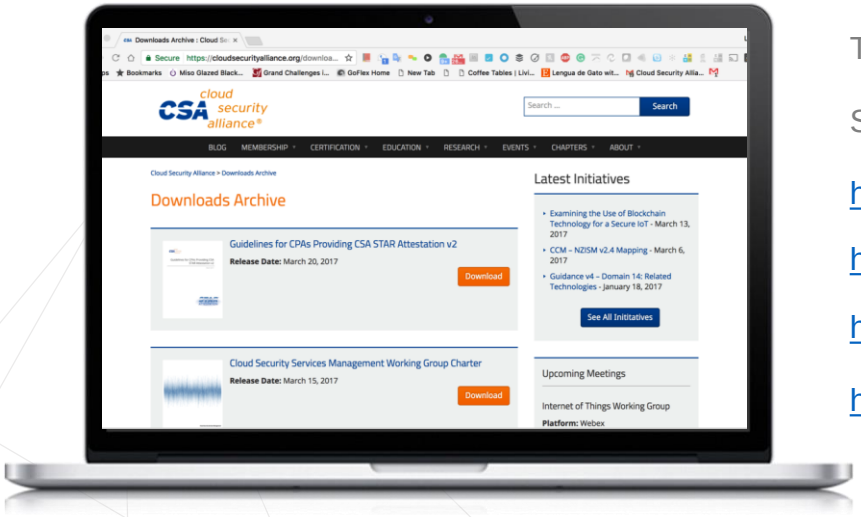
- ドイツ連邦セキュリティ局(BSI) –C5
- アメリカ行政管理局(GSA) –FedRAMP
- シンガポールIDA –MTCS
- イタリアデジタル局(AGID) –SaaS認可
- その他多数予定

日本は？

CONCLUSION

おわりに

Thank You!



Contact CSA

Email: info@cloudsecurityalliance.org

dcatteddu@cloudsecurityalliance.org

Twitter: @Cloudsa @DanieleCatteddu

Site: www.cloudsecurityalliance.org

https://cloudsecurityalliance.org/star/#_overview

https://gdpr.cloudsecurityalliance.org

https://cloudsecurityalliance.org/group/cloud-controls-matrix

http://www.sec-cert.eu