



Guidance WG 活動報告

**CSA Japan Congress
2016.11.22.**

WGリーダー 勝見 勉



SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS ON CLOUD COMPUTING

クラウドコンピューティングのセキュリティに関する
総合的解説と基本的対策を説明したレポート

CSA-JC ガイダンスWGの活動

- Guidance 4.0 への取り組み
 - 進行中の編集作業のwatch、解析、理解
 - globalな編集のcollaborationへの参加
 - コメント、意見のfeedback
- (4.0の完成後) 日本語版の作成
 - global編集が固まるのに合わせて並行作業
 - globalリリースと日本語版の時差の短縮

Guidance V1.0

- Section I. Cloud Architecture
 - Domain 1: Cloud Computing Architectural Framework
- Section II. Governing in the Cloud
 - Domain 2: Governance and Enterprise Risk Management
 - Domain 3: Legal
 - Domain 4: Electronic Discovery
 - Domain 5: Compliance and Audit
 - Domain 6: Information Lifecycle Management
 - Domain 7: Portability and Interoperability
- Section III. Operating in the Cloud
 - Domain 8: Traditional Security, Business Continuity and Disaster Recovery
 - Domain 9: Data Center Operations
 - Domain 10: Incident Response, Notification and Remediation
 - Domain 11: Application Security
 - Domain 12: Encryption and Key Management
 - Domain 13: Identity and Access Management
 - Domain 14: Storage
 - Domain 15: Virtualization

Guidance V2.1

- **Section I. Cloud Architecture**
 - Domain 1: Cloud Computing Architectural Framework
- **Section II. Governing in the Cloud**
 - Domain 2: Governance and Enterprise Risk Management
 - Domain 3: Legal and Electronic Discovery
 - Domain 4: Compliance and Audit
 - Domain 5: Information Lifecycle Management
 - Domain 6: Portability and Interoperability
- **Section III. Operating in the Cloud**
 - Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
 - Domain 8: Data Center Operations
 - Domain 9: Incident Response, Notification, and Remediation
 - Domain 10: Application Security
 - Domain 11: Encryption and Key Management
 - Domain 12: Identity and Access Management
 - Domain 13: Virtualization

CSA: 14のセキュリティ課題(ガイダンス3.0)

“Security Guidance for Critical Areas of Focus on Cloud Computing”

第1部 Cloud Architecture クラウド・アーキテクチャ

2009.4.20.

Domain 1. Cloud Computing Architectural Framework アーキテクチャフレームワーク

第2部 Governance in the Cloud クラウドのガバナンス

Domain 2. Governance and Enterprise Risk Management ガバナンスとリスク管理

Domain 3. Legal Issues: Contracts and Electronic Discovery 法務、契約、電子的証拠
開示

Domain 4. Compliance and Audit Management コンプライアンスと監査の管理

Domain 5. Information Management and Data Security 情報管理とデータセキュリティ

Domain 6. Interoperability and Portability 相互運用性と移植可能性

第3部 Operating in the Cloud クラウドの運用

Domain 7. Traditional Security, Business Continuity and Disaster Recovery
物理的セキュリティ、事業継続、災害復旧

Domain 8. Data Center Operations データセンターの運用管理

Domain 9. Incident Response インシデント対応

Domain 10. Application Security アプリケーションセキュリティ

Domain 11. Encryption and Key Management 暗号と鍵管理

Domain 12. Identity, Entitlement, and Access Management アイデンティティ・権限・アクセス管理

Domain 13. Virtualization 仮想化

Domain 14. Security as a Service セキュリティアズアサービス



Version 3.0 日本語版



クラウドコンピューティング
のためのセキュリティガイダ
ンス V3.0

日本語版の提供について

2013年5月8日

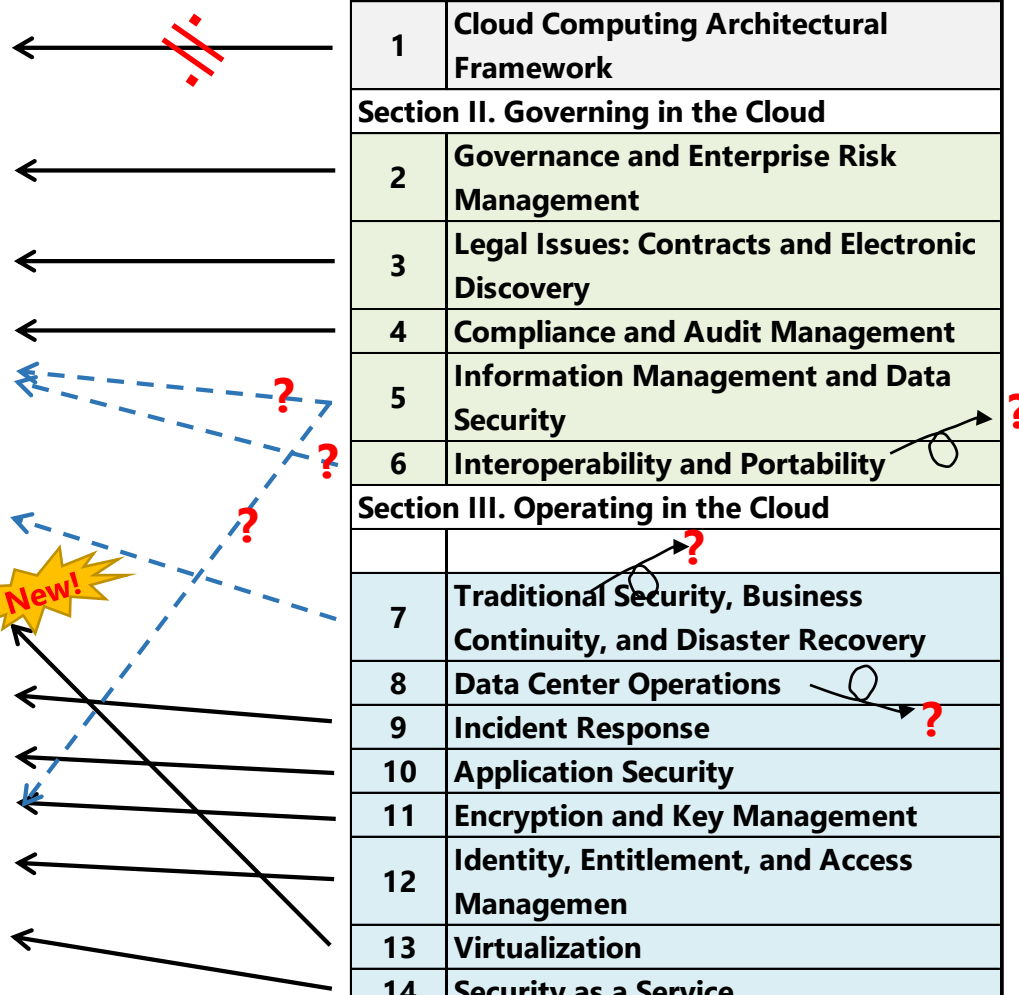
Version間Domain比較

Version 4.0		Version 3.0.1		Version 2.1		Version 1.0	
Section I. Cloud Architecture							
1	Cloud Computing Concepts and	1	Cloud Computing Architectural Framework	1	Cloud Computing Architectural Framework	1	Cloud Computing Architectural Framework
Section II. Governing in the Cloud							
2	Governance and Enterprise Risk Management	2	Governance and Enterprise Risk Management	2	Governance and Enterprise Risk Management	2	Governance and Enterprise Risk Management
3	Legal Issues, Contracts and Electronic Discovery	3	Legal Issues: Contracts and Electronic	3	Legal and Electronic Discovery	3	Legal
						4	Electronic Discovery
4	Compliance and Audit Management	4	Compliance and Audit Management	4	Compliance and Audit	5	Compliance and Audit
5	Data Governance	5	Information Management and Data Security	5	Information Lifecycle Management	6	Information Lifecycle Management
		6	Interoperability and Portability	6	Portability and Interoperability	7	Portability and Interoperability
Section III. Operating in the Cloud							
6	Management Plane and Business Continuity	7	Traditional Security, Business Continuity, and Disaster Recovery	7	Traditional Security, Business Continuity, and Disaster Recovery	8	Traditional Security, Business Continuity and Disaster Recovery
7	Infrastructure Security						
		8	Data Center Operations	8	Data Center Operations	9	Data Center Operations
9	Incident Response	9	Incident Response	9	Incident Response, Notifi-cation, and	10	Incident Response, Notifi-cation, and
10	Application Security	10	Application Security	10	Application Security	11	Application Security
11	Data Security and Encryption	11	Encryption and Key Management	11	Encryption and Key Management	12	Encryption and Key Management
12	Identity, Access, and Entitlement Management	12	Identity, Entitlement, and Access Managemen	12	Identity and Access Management	13	Identity and Access Management
						14	Storage
		13	Virtualization	13	Virtualization	15	Virtualization
13	Security as a Service	14	Security as a Service				

Guidance 4.0 のドメイン構成

Version 4.0	
Domain	Title
1	Cloud Computing Concepts and Architectures
2	Governance and Enterprise Risk Management
3	Legal Issues: Contracts and Electronic Discovery
4	Compliance and Audit Management
5	Data Governance
6	Management Plans and Business Continuity
7	Infrastructure Security
8	Virtualization and Containers
9	Incident Response, Notification and Remediation
10	Application Security
11	Data Security and Encryption
12	Identity, Entitlement, and Access Management
13	Security as a Service
14	Related Technologies

Version 3.0.1	
Domain	Title
Section I. Cloud Architecture	
1	Cloud Computing Architectural Framework
Section II. Governing in the Cloud	
2	Governance and Enterprise Risk Management
3	Legal Issues: Contracts and Electronic Discovery
4	Compliance and Audit Management
5	Information Management and Data Security
6	Interoperability and Portability
Section III. Operating in the Cloud	
7	Traditional Security, Business Continuity, and Disaster Recovery
8	Data Center Operations
9	Incident Response
10	Application Security
11	Encryption and Key Management
12	Identity, Entitlement, and Access Management
13	Virtualization
14	Security as a Service



Guidance 4.0 Domain1のざっと見

Version4

D1: Cloud Computing Concepts and Architectures

No.	Title	Contents	何が変わったか不変か
1.0	Introduction	Domain1の概要 Cloud Computingの特性 Domain1の内容 <ul style="list-style-type: none"> Defining cloud computing: 1.1.1 The cloud logical model : 1.1.2 Cloud conceptual, architectural, and reference model: 1.1.3 Cloud security and compliance scope, responsibilities, and models: 1.2 	新設
1.1	Overview	見出しだけ	
1.1.1	Defining Cloud Computing	Cloud Computingの概説、定義紹介 NIST ISO/IEC "cloud Consumer"定義 NIST SP500-292 Reference Model への言及	新しく定義に関する記述と事例紹介を執筆している。 3.0.1からの流用なし
1.1.2	Definitional Model	NISTモデル、ISO/IECモデル	3.0.1の1.2をほぼそのまま踏襲
1.1.2.1	Essential Characteristics	NISTの5特性 +ISO/IEC17788	NISTの5特性を簡潔に紹介。 3.0.1の1.4"Multi-Tenancy"は削除され、代わりにISO/IEC17788にreferする形で一言だけ触れている。
1.1.2.2	Service Models	SPIモデルの簡潔な説明 ISO/IECのXaaS(e.g. Compute, Data Storage)への言及	NISTのSPIを簡潔に紹介。 3.0.1の1.4"Multi-Tenancy"でSPIに数行ふれ、欄外に表を表示。(文内にreferなし) 3.0.1の1.5"Cloud Reference Model"でセキュリティ・責任分界点への言及を中心にほぼ丸1ページの記述があったがほとんどなくなった。
1.1.2.3	Deployment Models	Public, Community, Private, Hybrid 内部・外部、Public-Privateのmatrix図	3.0.1の1.5.1"Cloud Security Reference Model"の途中で左記matrix図を掲載。PPCH各々の説明はなし。 なお、3.0.1の1.5.1"Cloud Security Reference Model"ではJerichoモデルやISO/IEC27002 Sec6.2への言及などが続く。 3.0.1ではドメイン紹介の後の1.6で改めてDeployment modelの解説がある。節建ての統一感がない感じ。

Guidance 4.0 Domain1のざっと見

1.1.3	Reference and Architecture Models	スタックモデル ISO/IEC17788, SP500-292紹介	3.0.1ではArchitecture Modelは1.3で図を掲載の他は詳説なし。 なお、1.5.1のJerichoの後にCloud Model - Security Control Model - Compliance Modelの関連図を掲げていたが無くなった。 全体に、reference model関係はほぼ全面的に書き換えられている。
1.1.3.1	Infrastructure as a Service	スタックモデル各レイヤーの解説 システム構成図	IaaSモデルの個別解説(構成図あり) HypervisorやVM、Storage、APIなどの構成要素を用いて新たに表現
1.1.3.2	Platform as a Service	スタックモデル各レイヤーの解説 システム構成図	PaaSモデルの個別解説(構成図あり) HypervisorやVM、Storage、APIなどの構成要素を用いて新たに表現
1.1.3.3	Software as a Service	スタックモデル各レイヤーの解説 システム構成図	SaaSモデルの個別解説(構成図なし) HypervisorやVM、Storage、APIなどの構成要素を用いて新たに表現
1.1.4	Logical Model	論理構成? Infrastructure Metastructure : Mgmt Plane Components Applistructure Infostructure	クラウド論理構成モデルの新設 機能性に基づき4構成レイヤ(インフラ、メタ、アプリ、情報)に分類の上、特にメタ(プロトコル)をクラウドの特徴と言及、ただし図は各レイヤ名の羅列のみ
1.2	Cloud Security Scope, Responsibilities, and Models	見出しだけ	新設
1.2.1	Cloud Security and Compliance Scope and Responsibilities	責任構成とその分界点(provider vs consumer)	新設。V3の1.5.2と近い内容になっているが、記述は新しくなっている。
1.2.2	Cloud Security Models	Security Modelの紹介・リスト - Conceptual(Framework), Controls, Ref. Arch., Design Pattern CSA Enterprise Architecture (SABSA, ITIL, TOGAF, Jericho) CSA CCM NIST SP500-299 (CC Reference Architecture) ISO/IEC 27017	新設。新しいモデルの記述。

Guidance 4.0 Domain1のざっと見

1.2.2.1	A Simple Cloud Security Process Model	<p>Cloud Security Mangement Process Model</p> <ol style="list-style-type: none"> 1. Identify necessary security and compliance requirements, and any existing controls. 2. Select your cloud provider, service, and deployment models. 3. Define the architecture. 4. Assess the security controls. 5. Identify control gaps. 6. Design and implement controls to fill the gaps. 7. Manage changes over time. 	新設。新しいモデルの記述。
1.3	Areas of Critical Focus	Guidance全体のdomain構成	3.0.1の1.5.3 “Beyond Architecture: The Areas of Critical Focus”と対応。イントロ文は全くそのまま踏襲。
1.3.1	Governing in the Cloud	Governanceのdomains: 2, 3, 4, 5	構成としては3.0.1のTable 2a – Governance Domainsと同じ。Domainの組み立ては一部変わった。
1.3.2	Operating in the Cloud	Operationsのdomains: 6, 7, 8, 9, 10, 11, 12, 13, 14	構成としては3.0.1のTable 2b – OPerational Domainsと同じ。Domainの組み立ては一部変わった。
1.4	Recommendations	6項目: NIST、CSA Ref.Arch.、CCM、CAIQ、Security Process	3.0.1の1.7 Recommendationsと見出しは対応するが、内容は全く異なる。3.0.1では長い説明文があり、SPIごとの説明等もある。
1.5	Credits		3.0.1では1.8 Requirementsがあるが、中身は5特性の解説であり、結びの言葉も含んでいてrequirementsらしきものはない。構成としては??だったが、ごっそり削除となった。

Version 4.0 の編集プロセス

<https://github.com/cloudsecurityalliance/CSA-Guidance>

cloudsecurityalliance / CSA-Guidance

Watch 30

Code Issues 12 Pull requests 7 Projects 0 Pulse Graphs

CSA Guidance

24 commits 1 branch 0 releases

Branch: master New pull request

rmogull Adding Domain 4 outline

Images	Full first draft with diagrams
Domain 1- Cloud Computing Concepts and Architectures...	Added incident response section
Domain 10- Application Security.md	Adding domain 10 outline
Domain 11- Data Security and Encryption.md	Data security section
Domain 12- Identity, Access, and Entitlement Managemen...	Added domain 12
Domain 13- Security as a Service.md	Adding Domain 13
Domain 2- Governance and Enterprise Risk Management...	Added domain 2
Domain 3- Legal Issues, Contracts and Electronic Discover...	Adding legal domain
Domain 4- Compliance and Audit Management.md	Adding Domain 4 outline
Domain 5- Data Governance.md	Initial outline of domain 5
Domain 6- Management Plane and Business Continuity.md	Initial commit of domain 6
Domain 7- Infrastructure Security.md	adding initial domain 7 outline
Domain 9 Incident Response.md	Added incident response section
README.md	README.md typos.

誰でも参加できます

cloud security alliance

BLOG MEMBERSHIP CERTIFICATION EDUCATION RESEARCH

Cloud Security Alliance > CSA Security Guidance for Critical Areas of Focus in Cloud Computing v.4

CSA Security Guidance for Critical Areas of Focus in Cloud Computing v.4

Overview Process Domains Github Repository Working Group Page

A Stable, Secure baseline for Cloud Operations

The Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing is a practical, actionable roadmap to individuals looking to safely adopt cloud computing. Since its last revision in 2011, the cloud landscape has changed and so we want to reflect that in an updated version (which would be version 4). New CSA Guidance Domains are being added and existing ones will be updated frequently, so come back to the site to see the latest updates.

Please take your time in providing feedback. Although we have a dedicated working group, this is a community project. All feedback and edits will be managed via GitHub so that the process are open and public.

We need your feedback!

The idea is to generate a cleaner and more consistent document than possible by solely relying on working groups to do their own writing, while still reflecting the collective wisdom of the community. All feedback and edits will be managed via GitHub so that all parts of the process are open and public. You don't need to use any special command-line GitHub tools for this project. GitHub's web interface will allow you to read documents, provide feedback, and participate. But feel free to use git tools if you know how.

How to use GitHub to provide feedback

- Issues are the best way to add comments. The authors can read and respond to them directly. When leaving an issue, please list the line number for the start of any specific section you are commenting on.
- Pull requests are for edits. We can't respond to all pull requests because our only options are to ignore a pull or merge the changes. For consistency's sake, it is very hard to accept pull requests directly. All pull requests will be reviewed, some will be merged, and those we cannot directly merge will be treated as an issue/comment and closed. This is just a practical necessity, considering how many people will eventually be providing feedback.

For writing we are using the Markdown text format. If you want to edit and send pull requests you will need to learn Markdown (fortunately it's incredibly simple). GitHub renders Markdown directly, so unless you are actually editing content you won't need to learn it.

Keep all feedback public, on GitHub. This is essential for maintaining the independence and objectivity of this project. Even if you know any of the authors or CSA staff, please don't email private feedback, which will be ignored.

We will do our absolute best to respond to all feedback (with the exception of pull requests, which we will review), but depending on volume we may need to combine feedback (and we understand some feedback will be contradictory).

Contribute Now

For questions or feedback, contact research@cloudsecurityalliance.org.

<https://cloudsecurityalliance.org/guidance/>

