情報通信ネットワーク産業協会
Communications and Information network Association of Japan

海外サイバーセキュリティ
標準調査
法令/法規制調査
【概要編】

2023年3月

通信ネットワーク機器セキュリティ委員会

はじめに

サイバー攻撃の狡猾化と被害の甚大化、産業のDX化によりセキュリティに対する要求は益々強まるとともに広範化してます。当委員会では、通信ネットワークのセキュリティに起因する問題を未然に防ぐことを目的に情報および通信ネットワークのセキュリティの動向を収集し、会員企業や社会に対して発信するとともに、関係省庁に対し業界意見を集約、意見発信しています。

この度、2021年度および2022年度における活動成果のひとつとして、海外のサイバーセキュリティに関わる標準および法令／法規制の調査を公開する運びとなりました。調査に当たっては、欧米を対象とした以下を調査しました。

⑴ 標準調査
　NIST、ITU-T SG17、ISO/IEC JTC1 SC27、3GPPの４つの組織のサイバーセキュリティ関連の標準
⑵ 法令／法規制調査
　主要なサイバーセキュリティおよびプライバシーに関わる法令／法規制

調査資料は、2022年10月時点の調査結果に基づき、以下の2部構成としました。
欧米の最新のサイバーセキュリティに関わる情報収集の一助となれば幸いです。

・海外サイバーセキュリティ標準調査、法令／法規制調査【概要編】
・海外サイバーセキュリティ標準調査、法令／法規制調査【詳細編】

目次 (1/2)

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

海外サイバーセキュリティ標準調査説明資料

【NIST】
- NIST概要
- NIST発行規格・ガイドライン(セキュリティ関連)
- NIST発行規格の調査方針
- NIST発行規格・ガイドライン掲載サイト

【ITU-T SG17】
- ITU-T SG17概要
- ITU-T SG17発行規格
- ITU-T SG17発行規格の調査方針
- ITU-T SG17掲載サイト

【ISO/IEC JTC1 SC27】
- ISO/IEC JTC1/SC27概要
- ISO/IEC JTC1/SC27発行規格
- ISO/IEC JTC1/SC27発行規格
- ISO/IEC JTC1/SC27発行規格掲載サイト

【3GPP】
- 3GPP SA WG3概要
- 3GPP SA WG3 発行規格
- 3GPP SA WG3 発行規格の調査方針
- 3GPP SA WG3 発行規格掲載サイト

目次 (2/2)

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

海外サイバーセキュリティ法令/法規制調査説明資料

【欧州・北米】

- 海外サイバーセキュリティおよび個人情報保護に関わる法律、規則等の調査方針
- 欧州サイバーセキュリティ認証スキーム
- 日本の個人情報保護法の基本対応とGDPRにおける強化点
- 北米サイバーセキュリティフレームワーク
- カルフォルニア州消費者プライバシー法施行に関する動向(概要)
- カルフォルニア州消費者プライバシー法施行に関する動向(影響)

海外サイバーセキュリティ標準調査説明資料
【NIST】

NIST概要

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関

◆ NISTの組織

NIST内には、情報技術に関する研究を行っているITL（Information Technology Laboratory）がある。

ITLは情報技術に関して6つの分野（Security, Information Access, Mathematics and Computational Science, Software Testing, Networking Research, Statistical Engineering）の研究を行っている

ITLの中でコンピュータセキュリティに関して研究を行い各種文書を発行しているのがCSD（Computer Security Division）と呼ばれ、FIPSやSP800シリーズの文書を発行している。

https://www.ipa.go.jp/security/publications/nist/nist_publications.html

NIST発行規格・ガイドライン(セキュリティ関連)

セキュリティに関する標準、ガイドライン、技術仕様、レポート、ホワイトペーパー等を発行

大分類	中分類	概要
FIPS		連邦情報処理規格：セキュリティ標準
SP (Special Publication)	SP 800 (Computer Security)	ガイドライン、技術仕様書、推奨事項、参考資料など：複数のサブシリーズから構成
	SP 1800 (Cybersecurity Practice Guide)	
	SP 500 (Information Technology)	
IR(NISTIR)		NISTの内部または省庁間レポート
CSWP		FIPS、SP、IRとして発行されていない一般的なホワイトペーパー、サイバーセキュリティやプライバシー関連の公式文書。
ITL Bulletin		NISTのセキュリティおよびプライバシーに関する出版物、プログラム、プロジェクトの月次報告

※ ITL Bulletinは月次報告のため今回調査対象としない

NIST発行規格の調査方針

FIPS、SP、IRおよび、「Publications」のページに掲載されていない NIST Cyber Security Frameworkのうち、下記基準で選定したものを調査対象とする。

◆ 選定基準

選定項目	選定内容
規格の発行日	原則、2015年1月以降発行のもの
文書の種類	ガイドラインやフレームワーク。年次報告書やワークショップ記録は対象としない
技術分野	IoT、通信（5G）、ネットワーク、暗号技術　関連のもの
活用状況	ー
その他	ー

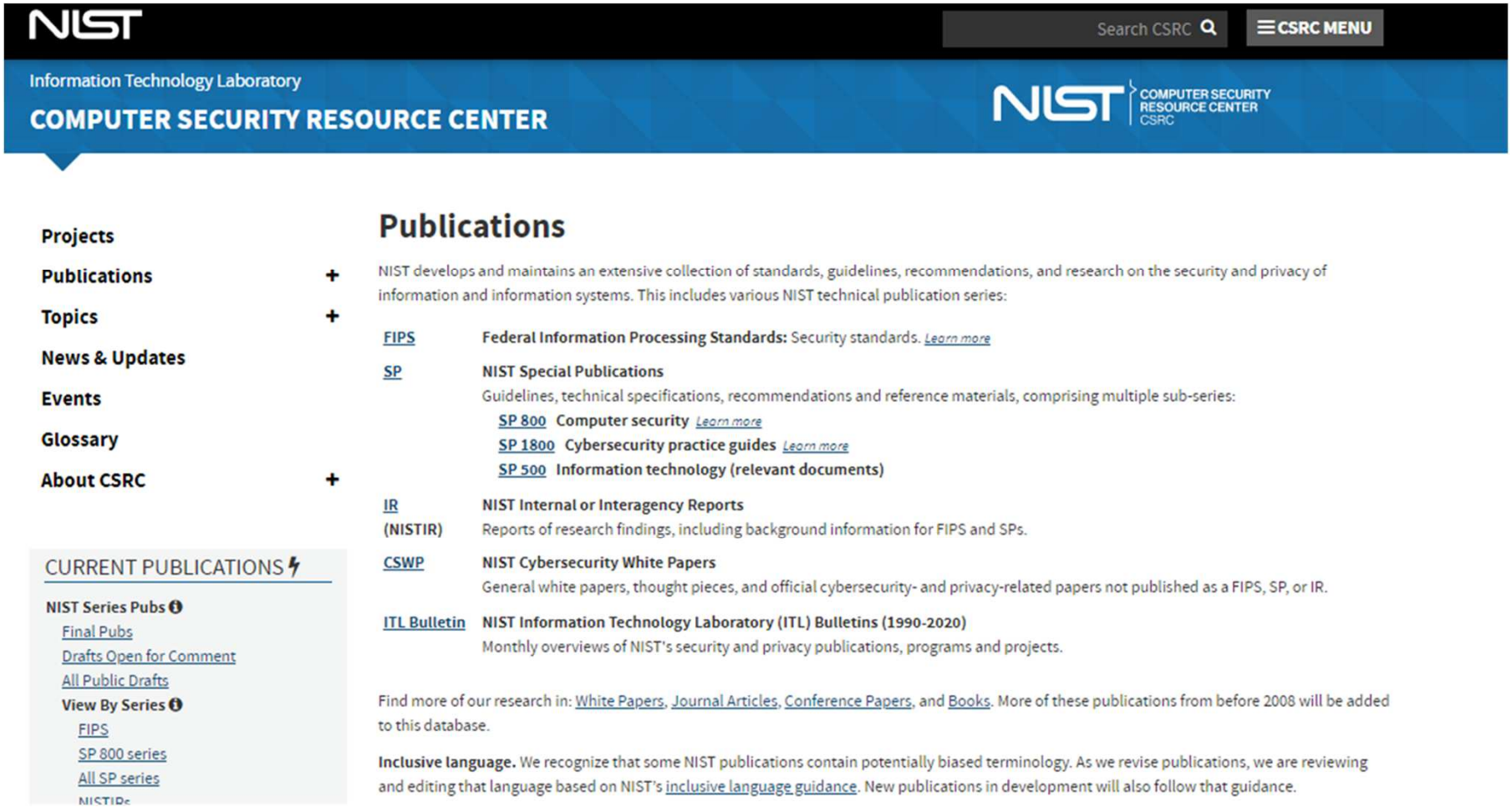
◆ 調査対象

COMPUTER SECURITY RESOURCE CENTERのPublicationsの項目のうち次のものを調査対象の全体とする。（https://csrc.nist.gov/publications）

分類	絞り込み前		絞り込み後	
FIPS	11件	518件	7件	165件
SP	235件		71件	
NISTIR	242件		58件	
CSWP	29件		28件	
Cybersecurity Framework Version 1.1 https://nist.gov/cyberframework	1件		1件	

NIST発行規格・ガイドライン掲載サイト

◆ NISTのセキュリティ関連の標準・ガイドライン情報
NISTのセキュリティ関連の情報はNISTのホームページの「COMPUTER SECURITY RESOURCE CENTER(https://csrc.nist.gov/)」にまとめられており、その中の「Publications(https://csrc.nist.gov/publications)」の項目に、NIST発行のセキュリティ関連標準・ガイドラインの情報が記載されている。



海外サイバーセキュリティ標準調査説明資料
【ITU-T SG17】

ITU-T SG17概要

国際標準化を行うITU-Tにおいて、情報セキュリティに関する標準化を担当する研究委員会(SG)

	SG17:Security 体制
WP1/17	**セキュリティ戦略と調整**
WP2/17	**5G、IoT、ITSセキュリティ**
WP3/17	**サイバーセキュリティと管理**
WP4/17	**サービスとアプリケーションのセキュリティ**
WP5/17	**セキュリティ基盤技術**

ITU-T SG17発行規格

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

SG17は、サイバーセキュリティ、セキュリティ管理、セキュリティアーキテクチャとフレームワーク、スパム対策、ID管理、個人を特定できる情報の保護、データ保護の運用面、オープンID信頼フレームワークに取り組んでいます。

No.	番号	制定日時	掲載URL	ステータス	概要
1	ITU-T X.805	2003/10/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=7024&lang=en	In force	通信ネットワーク事業者および企業に、セキュリティの観点からエンドツーエンドのアーキテクチャ記述を詳述する機能を提供します。企業がネットワークを見る方法を変更する仕様を定義し、ネットワーク内のすべての脆弱性を特定して軽減できるようにします。
2	ITU-T X.1051	2016/4/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=12845&lang=en	In force	電気通信組織における情報セキュリティ制御の実装をサポートし、機密性、完全性、可用性を含むベースライン情報セキュリティ管理要件を満たすためのガイドラインを提供します。
3	ITU-T X.1254	2020/9/3	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14260&lang=en	In force	エンティティのデジタル ID の検証をサポートするエンティティ認証保証フレームワークを提供します。この保証は、オンラインの信頼、セキュリティ、アクセス制御の中心にあります。この推奨事項では、デジタル ID に対する信頼を確立するための 3 種類の保証 (ID 保証、認証保証、およびフェデレーション保証) が特定されています。
4	ITU-T X.1141	2006/6/13	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=8844&lang=en	In force	セキュリティー情報を交換するための XML ベースのフレームワークであるセキュリティー・アサーション・マークアップ言語 (SAML 2.0) が定義されています。これは、サブジェクトに関するアサーションの形式で表されます。ここで、サブジェクトは、あるセキュリティー・ドメインで ID を持つエンティティー (人間またはコンピューターのいずれか) です。
5	ITU-T X.1231	2008/4/18	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=9333&lang=en	In force	スパムに対抗するための技術的戦略
6	ITU-T X.1361	2018/9/7	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13607&lang=en	In force	セキュリティゲートウェイを使用してIoT環境におけるセキュリティの脅威に対抗する機能
7	ITU-T X.1601	2015/10/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=12613&lang=en	In force	クラウドコンピューティングのためのセキュリティフレームワーク
8	ITU-T X.1085	2016/10/14	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13060&lang=en	In force	ITU-T X.509デジタル証明書の所有権を確認するためのテレバイオメトリック認証スキーム
9	ITU-T X.1712	2021/10/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14805&lang=en	In force	量子鍵配布ネットワークの鍵管理の設計、実装、運用に関連する考慮事項を提供しています
10	TU-T X.1371	2020/5/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14090&lang=en	In force	コネクテッドカーに対するセキュリティ脅威の分析
11	ITU-T X.1400	2020/10/29	https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14449&lang=en	In force	分散元帳技術の用語と定義のベースラインセット

ITU-T SG17発行規格の調査方針

ITU-T SG17が発行している国際標準のうち、下記基準で選定したものを調査対象とする。

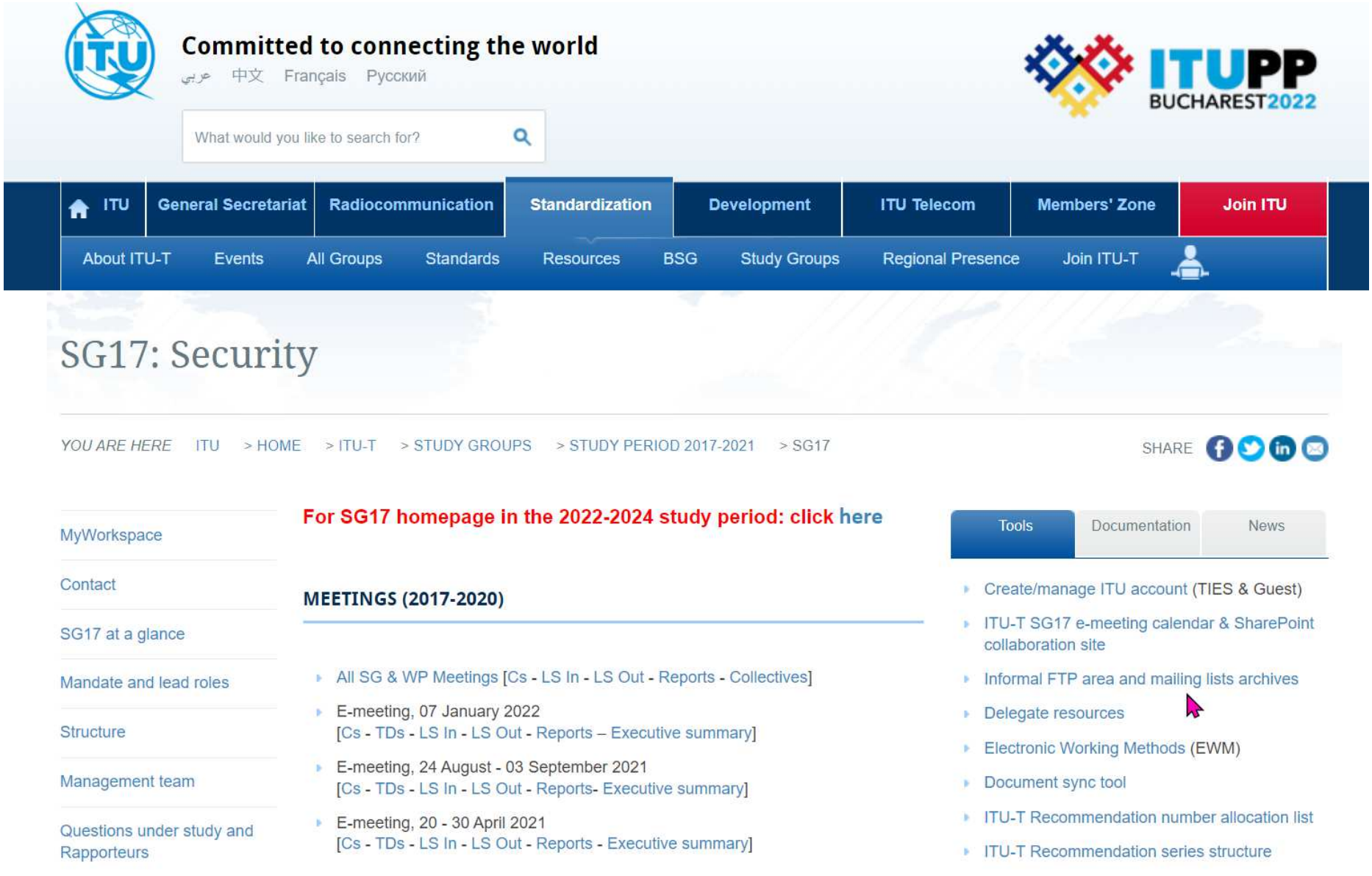
◆ 選定基準

選定項目	選定内容
規格の発行日	原則、2000年以降発行のもの
文書の種類	標準化段階のうち、in force(勧告)の段階の規格
技術分野	サイバーセキュリティ、セキュリティ管理、セキュリティアーキテクチャとフレームワーク、スパム対策、ID管理、個人を特定できる情報の保護、データ保護の運用面、オープンID信頼フレームワークのもの
活用状況	開発途上国のセキュリティ実務者に特に価値のあるガイダンスを提供している。
その他	情報通信技術(ICT)の利用における信頼とセキュリティを構築するための作業は、より安全なネットワークインフラストラクチャ、サービス、およびアプリケーションを促進するために引き続き強化されている。

（出典）https://www.itu.int/en/ITU-T/about/groups/2022-2024/Pages/sg17.aspx

ITU-T SG17 掲載サイト

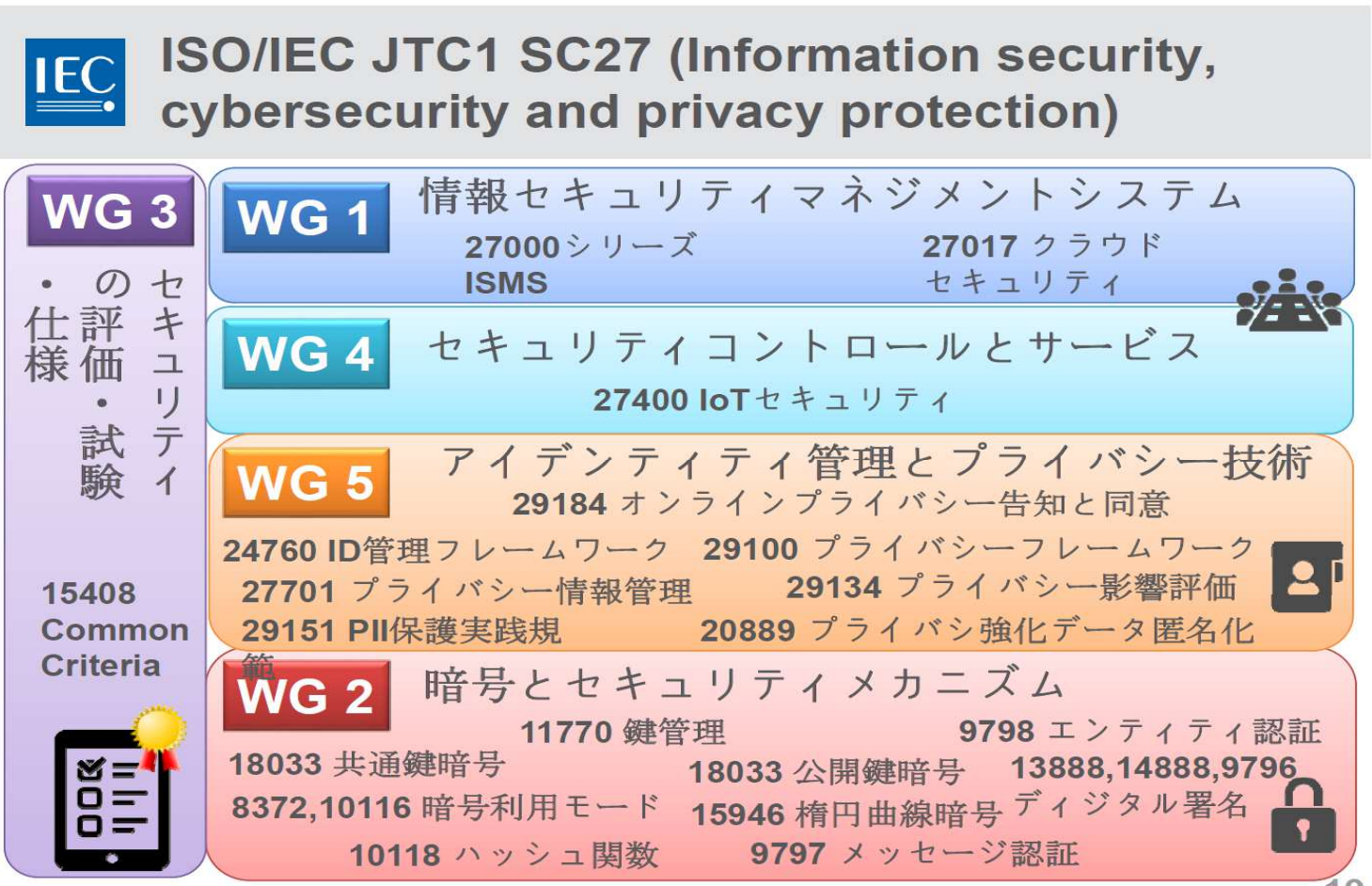
◆ ITU-T SG17ホームページ
https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx



海外サイバーセキュリティ標準調査説明資料
【ISO/IEC JTC1 SC27】

ISO/IEC JTC1/SC27概要

国際標準化を行うISOとIECの合同委員会（ISO/IEC JTC 1）において、情報セキュリティに関する標準化を担当する副委員会(SC)



情報セキュリティに関する国際標準化特別講演会 一般財団法人日本規格協会/IEC 活動推進会議/一般社団法人国際標準化協議会（2021年1月28日）
「IEC、ISO/IEC JTC1 SC 27等における情報セキュリティ標準化状況」（国立研究開発法人産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　古原 和邦 様）より転載

ISO/IEC JTC1/SC27発行規格

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

セキュリティマネジメントシステム、セキュリティに関するクラウド、IoT、プライバシー、鍵管理、セキュリティ評価などについて規格化されている。

項番	タイトル	WG
1	ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls	WG1
2	ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	WG1
3	ISO/IEC TR 27103: 2018　Information technology — Security techniques — Cybersecurity and ISO and IEC Standards	WG1
4	ISO/IEC TS 27100:2020　Information technology -- Cybersecurity -- Overview and concepts	WG1
5	ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components	WG3
6	ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components	WG3
7	ISO/IEC 29147:2018 Information technology -- Security techniques -- Vulnerability disclosure	WG3
8	ISO/IEC 30111:2019 Information technology -- Security techniques -- Vulnerability handling processes	WG3
9	ISO/IEC 27400:2022　Cybersecurity -- IoT security and privacy -- Guidelines	WG4
10	ISO/IEC 27701:2019　Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines	WG5
11	ISO/IEC 29100:2011　Information technology -- Security techniques -- Privacy framework	WG5
12*	ISO/IEC CD 27402.2　Cybersecurity — IoT security and privacy — Device baseline requirements	WG4
13*	ISO/IEC CD 27403 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	WG4

ISO/IEC JTC1/SC27発行規格の調査方針

SC27が発行している国際標準のうち、下記基準で選定したものを調査対象とする。

◆ 選定基準

選定項目	選定内容
規格の発行日	原則、2015年1月以降発行のもの
文書の種類	標準化段階のうち、CD(委員会原案)以上の段階の規格
技術分野	IoT、クラウド、暗号、クラウド、プライバシー、マネジメントシステム関連のもの
活用状況	省庁の調達や認証制度で用いられている
その他	セキュリティ要件が列挙されている

ISO/IEC JTC1/SC27発行規格掲載サイト

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

◆ ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection
https://www.iso.org/committee/45306.html

Standards About us News Taking part Store Search

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

About

Secretariat: DIN
Committee Manager: Mr Sobhi Mahmoud

Chairperson (until end 2024): Mr Dr Andreas Wolf

ISO Technical Programme Manager [TPM]: Mr Hakim Mkinsi
ISO Editorial Manager [EM]: Ms Isabel Veronica Nelson

Creation date: 1989

Quick links

Work programme
Drafts and new work items

Working area
Working documents (user account required)

ISO Electronic applications
IT Tools that help support the standards development process

Scope

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas

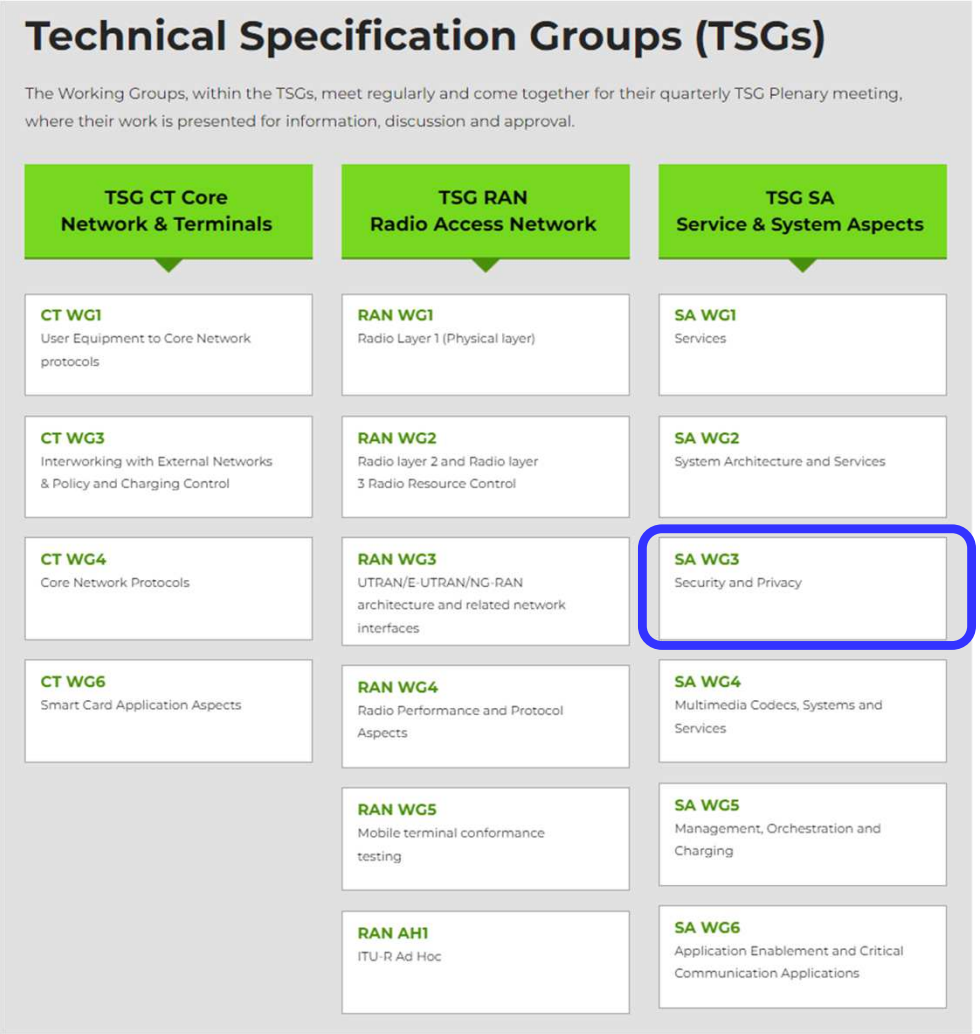
海外サイバーセキュリティ標準調査説明資料
【3GPP】

3GPP SA WG3概要

3GPPは、7つの電気通信標準化組織（ARIB、ATIS、CCSA、ETSI、TSDSI、TTA、TTC）を統合し、技術レポートと標準仕様を作成

◆第3世代パートナーシッププロジェクト（3GPP）は、無線アクセス、コアネットワーク、サービス機能などの**セルラー通信技術を対象**としています。

◆3GPP TSG SA WG3（SA3）で、**セキュリティとプライバシー**のためのアーキテクチャやプロトコルの要件や仕様定義を行っている。



出典）https://www.3gpp.org/3gpp-groups

3GPP SA WG3 発行規格

3GPP TSG SA WG3（SA3）では、**セキュリティとプライバシー**のためのアーキテクチャやプロトコルの要件や規格の定義を行っている。

- 対象となるシリーズ
  - 22 series ：サービス概要
  - 33 series ：セキュリティ概要
  - 35 series ：セキュリティアルゴリズム

Subject of specification series	3G and beyond / GSM (R99 and later)
Requirements	21 series
Service aspects ("stage 1")	22 series
Technical realization ("stage 2")	23 series
Signalling protocols ("stage 3") - user equipment to network	24 series
Radio aspects	25 series
CODECs	26 series
Data	27 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series
Programme management	30 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series
OAM&P and Charging	32 series
Access requirements and test specifications	
Security aspects	33 series
UE and (U)SIM test specifications	34 series
Security algorithms [5]	35 series
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series
Multiple radio access technology aspects	37 series
Radio technology beyond LTE	38 series

出典) https://www.3gpp.org/specifications-technologies/specifications-by-series

3GPP SA WG3 発行規格の調査方針

3GPP SA WG3が発行している技術仕様のうち、下記基準で選定したものをリストアップした

◆ 選定基準

選定項目	選定内容
仕様の発行日	なし
文書の種類	技術仕様　（ドラフト版を除く）
技術分野	LTE、5Gを対象とするもの
活用状況	セルラー通信技術でのセキュリティとプライバシーの技術仕様として活用されている
その他	ステータスが「Under change control」の物を「発行済み」と記載

3GPP SA WG3 発行規格掲載サイト

https://www.3gpp.org/dynareport?code=TSG-WG--S3.htm

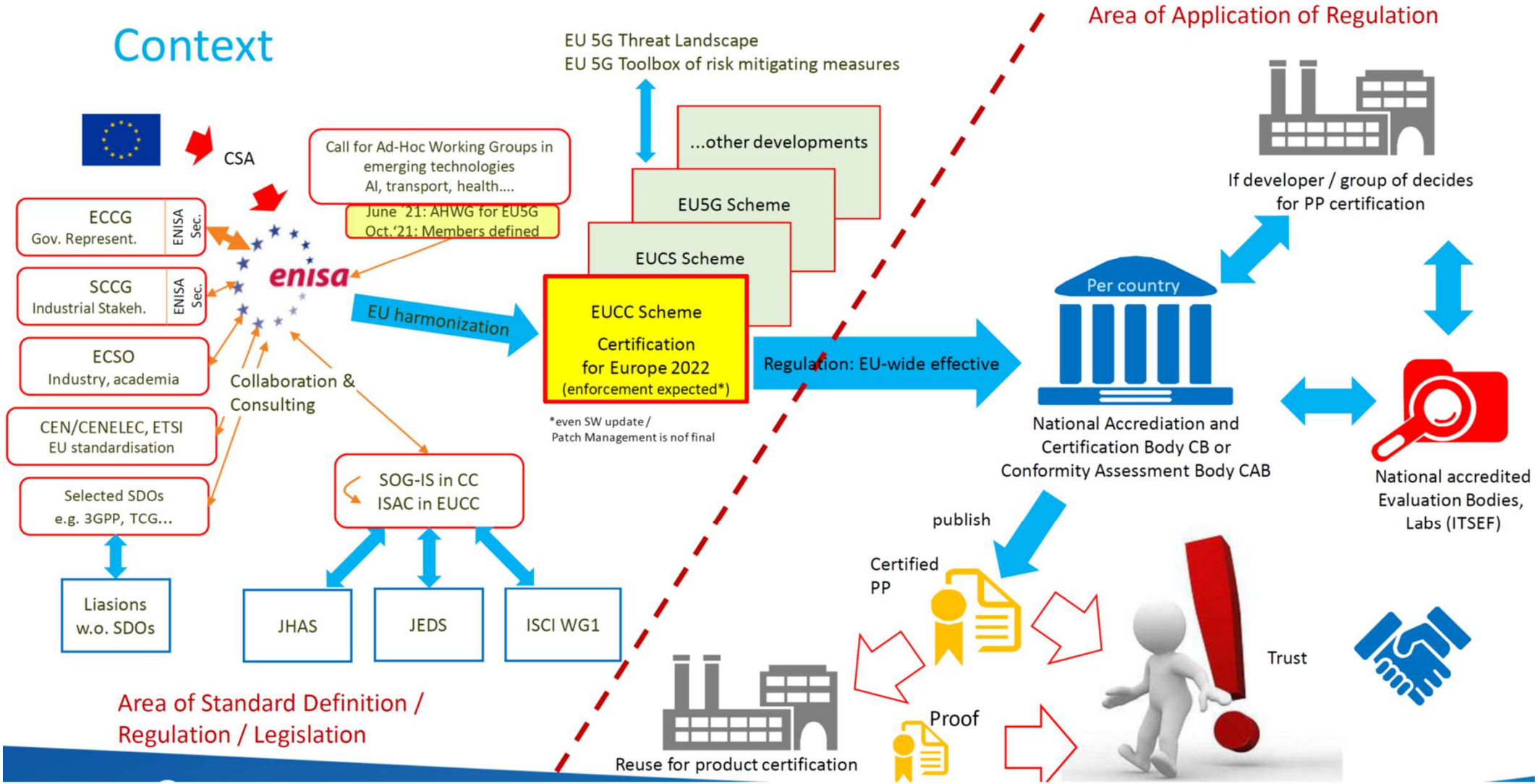
海外サイバーセキュリティ法令/法規制調査説明資料
【欧州・北米】

海外サイバーセキュリティおよび個人情報保護に関わる法律、規則等の調査方針

調査方針の項目	内容
調査対象国	北米、欧州
文書の種類	サイバーセキュリティおよび個人情報保護関連の 法令、指令、規則、法案
文書のステータス	発効済み、法制化中、改訂中
調査時期	2022年10月
主な情報収集元	①経産省　商務情報政策局 ②IPA（Information technology Promotion Agency） ③JCIC (Japan Cybersecurity Innovation Committee) ④JETRO（Japan External Trade Organization） ⑤その他インターネット記事

欧州サイバーセキュリティ認証スキーム

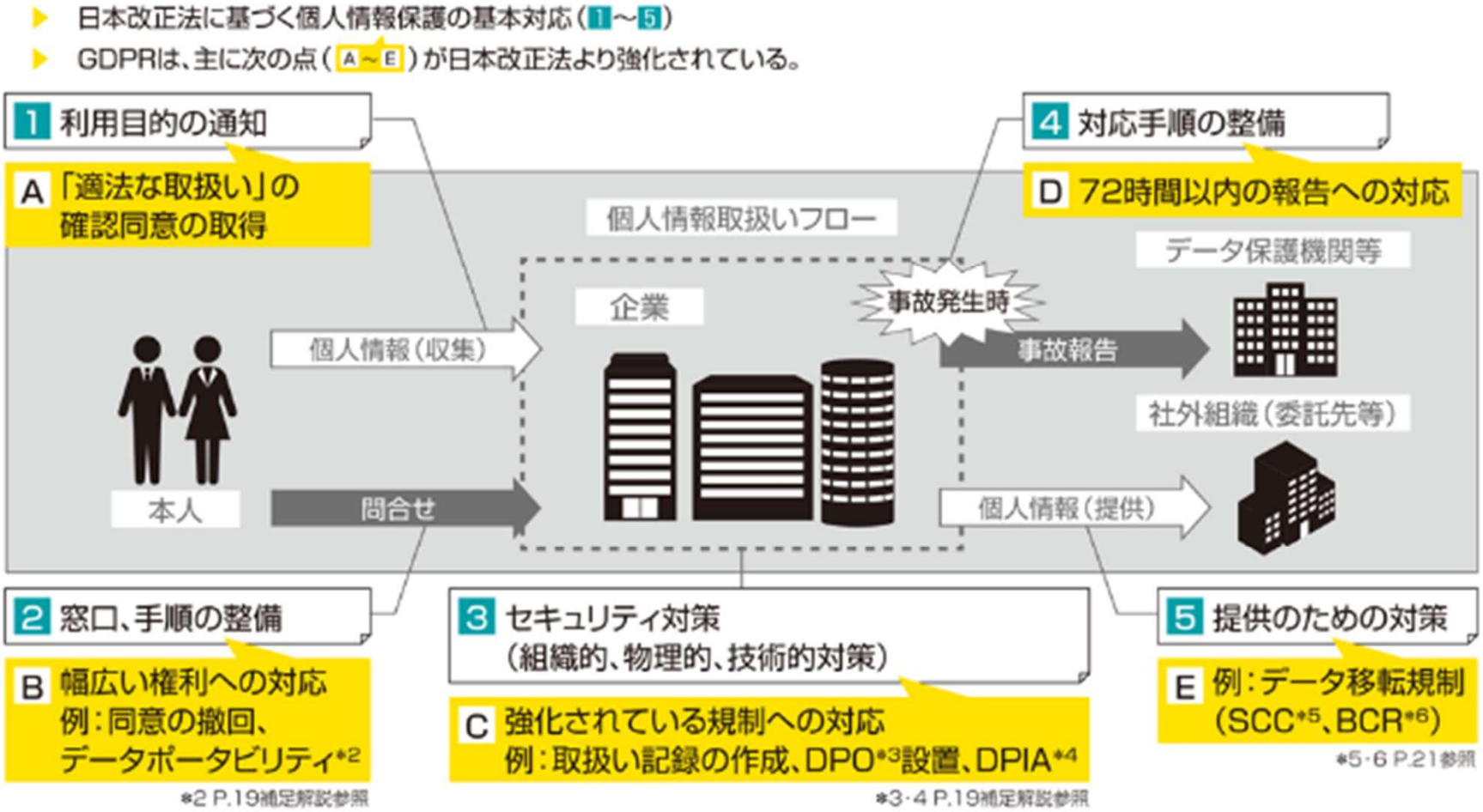
◆ 欧州連合サイバーセキュリティ庁（ENISA)にて各国の政府、産業界、学術機関および標準化機関等と連携してEU加盟国を対象としたサイバーセキュリティ関連法案を作成し、欧州各国は必要に応じて対応する自国の法案を策定。



出典：5GAA 2021-10-26 Virtual WG7資料

日本の個人情報保護法の基本対応とGDPRにおける強化点

◆ 経済協力開発機構（OECD）が、個人データ取扱に関するガイドラインとして、公表した原則（OECD8原則）が、現在も世界的に個人情報保護法制の基本理念とされている。GDPR及び日本改正法もそのコンセプトを踏襲しているが、GDPRには、日本改正法に比べて強化されている点がある。個人情報保護のための基本的な対応とGDPRにおける強化点（黄色吹き出し箇所）を下図に示す。



出典：GDPRの概要と日本企業への影響、EYアドバイザリー・アンド・コンサルティング株式会社 熊谷真知子、2020年

北米サイバーセキュリティフレームワーク

- NISTは、セキュリティに配慮したソフトウェア開発手法を既存の標準やガイドライン等を参照する形でSecure Software Development Framework (SSDF)として整理（2020年4月に最終版を公開）。
- SSDFでは、各手法を「組織構築」「ソフトウェア保護」「セキュアなソフトウェア」「脆弱性対応」の4つに分類の上、何をすべきか（Practice-Taskの2階層）、事例、参照文書について体系化。

【 SSDFにおける各手法の分類】

分類	分類（英語名）	概要	手法例	備考
組織構築	Prepare the Organization（PO）	人材、処理能力、技術等のソフトウェア開発リソース確保	• ソフトウェア開発におけるセキュリティ要件を定義 • 各役割と責任の実装	• PSの中でSBOMの作成と維持について言及あり • 参照文書（Reference）は、ISO、BSA、NIST CSF 等
ソフトウェア保護	Protect the Software（PS）	ソフトウェアの全てのコンポーネントを改ざんや不正アクセスから保護	• 全ての形式のコードを改ざんや不正アクセスから保護	
セキュアなソフトウェア	Produce Well-Secured Software（PW）	ソフトウェアリリース時のセキュリティに関する脆弱性を最小化	• ソフトウェアデザインにおけるセキュリティ要件への合致とリスク低減	
脆弱性対応	Respond to Vulnerabilities（RV）	ソフトウェアセキュリティの脆弱性の認識、適切な対応、将来にわたる予防策	• 継続的な脆弱性の特定・確認 • 脆弱性の評価・優先付け・修正	

出典：令和３年３月経産省 サイバーセキュリティに関連する海外の動き

カルフォルニア州消費者プライバシー法施行に関する動向(概要)

情報通信ネットワーク産業協会
Communications and Information network Association of Japan

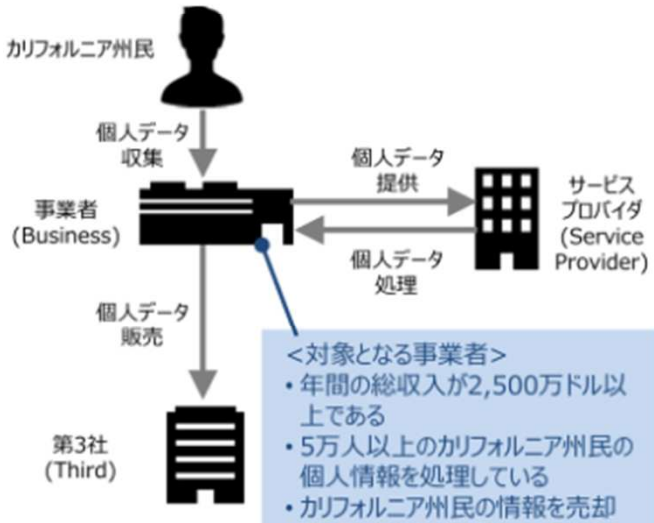
- 個人データに関する問題をきっかけに、米国カリフォルニア州にて2020年1月1日に「カリフォルニア州消費者プライバシー法」が施行された。
- 消費者データのプライバシー規制については、バーモント州（2018年12月施行）、ネバダ州（2019年10月施行）、メイン州（2020年7月施行）等でも制定されている。

背景

- **カリフォルニア州で通称「Shine the Light」法施行（2005年）**「Shine the Light」法とは、企業がマーケティングを目的として第三者と共有する個人情報の内容を請求する権利を、年1回に限りカリフォルニア州の居住者に付与するものである。
- **ケンブリッジ・アナリティカ問題（2018年）**2018年3月、Facebookから大量の個人データが流出したことが発覚した際、コンサルティング会社であるケンブリッジ・アナリティカ社がそれらを集め、2016年米大統領選などに使っていたことが明らかとなった。

動向の概要

- 2020年1月1日に、カルフォルニア州はプライバシー権及び消費者保護の強化を目的として、カリフォルニア州消費者プライバシー法を施行した。
- カリフォルニア州消費者プライバシー法では、一定の条件を満たしたカリフォルニア州民の個人情報を収集する事業者を対象としており、消費者に対して以下に示す5つの権利を認めた。



消費者の5つの権利

No	内容
1	企業が収集した個人情報のカテゴリー、情報源、情報の用途および収集した情報の開示先など、**企業のデータ収集の運用について開示請求する権利**
2	消費者による請求から過去12カ月の間にその消費者について収集した具体的な**個人情報のコピーを受け取る権利**
3	**本人の個人情報を削除してもらう権利**（ただし、例外有）
4	企業のデータ売却の運用について知り、その消費者の**個人情報を第三者に売却しないよう求める権利**（いわゆるオプトアウト）
5	消費者らがカリフォルニア州プライバシー法により付与された新たな権利を行使したことに基づいて**差別されない権利**

(出所) JETRO"施行が迫る「カリフォルニア州消費者プライバシー法」（米国）"（2019/6/6）等を参考に作成

出典：令和３年３月経産省 サイバーセキュリティに関連する海外の動き

カルフォルニア州消費者プライバシー法施行に関する動向(影響)

- カルフォルニア州消費者プライバシー法施行により、企業は個人情報取扱いに関する義務を負った。またこれらの義務を遵守できなかった場合のペナルティも定められており、企業は対応が必要となる。

事業者に課せられる義務

セキュリティ対策の実施
(第1798.150条)

- 個人情報を保護するための合理的なセキュリティ手順と慣行を実装する義務が事業者に課された。この義務について、事業者は身元の偽装や、個人情報への不正なアクセスまたは削除を防ぐ合理的なセキュリティ措置を実行しなければならないとされている。

開示請求等への対応
(第 1798.100 条,規則第 999.313 条)

- 企業として法令を順守するため主に以下の内容に対応する必要があるとされた。
  - ◆ 請求している消費者の本人確認をする手順を実施すること
  - ◆ 45日以内に情報開示するために社内で個人情報を特定・発見することができるようにすること
  - ◆ 特定の情報開示を電子的に行う方法を開発すること 等

義務に違反した事業者へのペナルティ等

消費者により提起される民事訴訟
(第1798.150条)

- 暗号化されておらず、かつ修正されていない個人情報が、不正アクセス、流出、窃取又は開示の対象となった場合、当該消費者は、以下のいずれかについて民事訴訟を提起することができるとされた。
  - ◆ 違反1件について消費者一人当たりで100ドル以上750ドル以下の、又は実損害の、いずれか大きい額の損害を回収するため
  - ◆ 差止命令による救済又は宣言的救済
  - ◆ 裁判所が適切と判断するその他の救済

開示請求への対応不足による罰金
(第1798.155条)

- 消費者からの情報開示請求に対して1件あたり最大2,500ドルの罰金（故意だと認定される場合には最大7,500ドル）を科せられる可能性がある。

請求に対して45日以内に事業者は情報を開示する必要があるが、不遵守を通知されてから30日以内に対応がされていないと判断された場合、罰金が科される可能性がある。

<日本企業への影響>
今後、日本企業・組織が米国国内においてビジネスを行っていく上では、説明責任の一環として、例えば「**カルフォルニア州消費者プライバシー法の適用を受けるか否か**」、（受ける場合）「**どのようにカルフォルニア州消費者プライバシー法を遵守しているか**」、（受けない場合）「**なぜカルフォルニア州消費者プライバシー法の適用を受けないと判断をしたか**」について、説明できるように準備する必要がある。

（出所） JETRO "施行が迫る「カリフォルニア州消費者プライバシー法」（米国）"(2019/6/6)、"カリフォルニア州消費者プライバシー法(CCPA)実務ハンドブック"（2019/12/25）等を参考に作成

出典：令和３年３月経産省 サイバーセキュリティに関連する海外の動き

海外サイバーセキュリティ
標準調査
法令/法規制調査
【概要編】

一般社団法人　情報通信ネットワーク産業協会
〒103-0026　東京都中央区日本橋兜町 21 番 7 号
兜町ユニ・スクエア 6 階
電　話　03-5962-3451
FAX　03-5962-3455