サイバーセキュリティ関連情報リンク集

（第 2.0 版）

2021 年　11 月　4 日

一般社団法人情報通信ネットワーク産業協会

通信ネットワーク機器セキュリティ委員会

1．まえがき

通信ネットワーク機器セキュリティ委員会では、CIAJ 内でセキュリティに対して専門的な検討を行う組織として、会員に対してサイバーセキュリティ情報の提供を行うべく検討を行っています。2016 年サイバーセキュリティ情報として有益な情報を入手することができる HP(Home Page)について表形式にまとめた資料を公開しましたが、5 年たち、新たに公開された有益な情報を追加･更新しました。これらの HP へのアクセスにより、各種のセキュリティ関連情報が得られると同時に警報やインシデントの発生についても知ることができます。定期的なセキュリティ情報の収集のためにも有効に活用をお願いします。

2. サイバーセキュリティー関連情報

2. 1 官公庁･民間団体･企業のサイバーセキュリティ関連情報発信サイト一覧

区分	No	項目	内容	アドレス
政府省庁 関連機関	1	内閣官房 内閣サイバーセキュリティセンター(NISC)	・内閣サイバーセキュリティセンターの活動報告・情報分析 ・サイバーセキュリティ政策に関する計画立案 ・サイバーセキュリティ技術動向等の調査・研究分析 ・サイバー攻撃等に関する最新情報の収集・集約 ・標的型メール及び不正プログラムの分析 ・その他サイバー攻撃事案の調査分析 ・広報啓発活動：みんなでしっかりサイバーセキュリティ	https://www.nisc.go.jp/
	2	総務省 国民のための情報セキュリティサイト	・インターネットと情報セキュリティの知識習得、利用方法に応じた情報セキュリティ対策を講じるための基本情報を提供 ・一般利用者のセキュリティ対策と企業・組織の対策をそれぞれ分けて提示	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
	3	経済産業省 情報･セキュリティ政策 HP	・経産省 商務情報政策局 情報セキュリティ政策室による情報セキュリティ政策情報 ・政策・制度中心だが、脆弱性情報を含む	https://www.meti.go.jp/policy/netsecurity/
	4	警察庁@police	・警察庁によるインターネット定点観測データ、セキュリティ啓発情報を含む ・子供向け、一般 PC ユーザ向け、システム管理者向けに分けて学習情報を掲載 ・PC やスマホの各種ソフトのアップデート情報	http://www.npa.go.jp/cyberpolice/l
	5	IPA ((独)情報処理推進機構)	・IPA セキュリティセンター、サイバー情報共有イニシアティブ（J-CSIP、サイバーレスキュー隊 J-CRAT 等による具体的なセキュリティ対策活動 ・各種セキュリティ関連情報提供 ・セミナー開催等によるセキュリティ対策啓蒙・普及活動等の実施	https://www.ipa.go.jp/
	6	NICT ((国研)情報通信研究機構)	・サイバー攻撃に対する早期発見、分析、防御、侵入感知に関するサイバーセキュリティ技術の研究 ・サイバーセキュリティ研究所：産学との緊密な連携によりサイバーセキュリティ研究開発の世界的中核拠点を目指す ・インシデント分析センター nicter：サイバー攻撃を実時間で高精度に分析	https://www.nict.go.jp/research/cyber-security.html
海外機関･ サイト	1	NIST （米国国立標準技術研究所）	・連邦政府機関および米国業界向けのサイバーセキュリティ標準を規定 ・他にも米国 NIST の関連情報を IPAHP 内に掲載	https://www.nist.gov/ https://www.ipa.go.jp/security/publications/nist/

区分	No	項目	内容	アドレス
	2	ITU-T SG17 (ITU 電気通信標準化部門)	・情報セキュリティ関連標準化（SG17）動向	https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
	3	ISO/IEC JTC1 SC27 (国際標準化機構/国際電気標準会議)	・ISO（国際標準化機構）、IEC（国際電気標準化会議）の JTC1(第 1 合同委員会)SC27 によるセキュリティ標準化情報	https://www.iso.org/committee/45306/x/catalogue/
	4	Internet Storm Center Dshield	・インターネット定点観測データ	https://www.dshield.org/port.html
	5	SecurityFocus	・海外ニュース等、ソフトのアップデート情報、セキュリティイベント情報	https://bugtraq.securityfocus.com/
国内 民間団体	1	JPCERT/CC ((一社)JPCERT コーディネーションセンター)	・JPCERT/CC: Japan Computer Emergency Response Team Coordination Center ・セキュリティ注意情報・早期警戒、脆弱性対策 ・インターネット定点観測 ・コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信	https://www.jpcert.or.jp/
	2	(一社)日本コンピュータセキュリティインシデント対応チーム（CSIRT）協議会	・CSIRT: Computer Security Incident Response Team ・インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定等実施 ・配下に１３の WG を設置	https://www.nca.gr.jp/
	3	(一社)産業競争力懇談会 （COCN）	・安全・安心・快適を実現する空間ソリューション ・アグリ・イノベーション・コンプレックスの構築 ・安定な未利用エネルギーによる水素社会の実現 ・３次元位置情報を用いたサービスと共通基盤整備 ・IoT 時代におけるプライバシーとイノベーションの両立 ・IoT、CPS を活用したスマート建設生産システム	http://www.cocn.jp/report.html
	4	(一社)情報サービス産業協会(JISA) 「情報セキュリティ」に役立つガイドライン	・「情報セキュリティ」マネジメントシステム構築に資するガイドラインや情報セキュリティ対策ベストプラクティスなどを紹介している。	https://www.jisa.or.jp/it_info/engineering/tabid/1103/Default.aspx
国内 企業サイト	1	Kaspersky Lab	・2016 年のサイバーセキュリティ動向予測 ・ウィルスニュース、マルウェア・スパム情報	https://www.kaspersky.co.jp/about/press-releases/2015_vir10122015
	2	トレンドマイクロ	・2019 年のサイバーセキュリティ脅威予測	https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181213-01.html
	3	Symantec Security Center	・マルウェア、セキュリティリスク、脆弱性、スパム等の情報	https://www.broadcom.com/support/security-center
	4	Intel Security (McAfee)	・脅威情報, マルウェア情報	https://www.mcafee.com/enterprise/ja-jp/threat-center.html
	5	Security NEXT	・サイバーセキュリティの日刊ニュース ・政府・業界動向、マイナンバー関連情報、セキュリティメルマガ	https://www.security-next.com/category/cat179
	6	ScanNetSecurity	・海外ニュース、中国動向、脅威・脆弱性情報等	https://scan.netsecurity.ne.jp/

2．2 官公庁・民間団体発表のサイバーセキュリティ関連文書一覧

区分	No	文書	発表元	内容	アドレス
政府省庁 関連機関	1	IoT セキュリティガイドライン Ver 1.0 （2016 年 7 月）	IoT 推進コンソーシアム 総務省 経済産業省	・IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたものである。	https://www.soumu.go.jp/main_content/000428393.pdf
	2	無線 LAN のセキュリティに関するガイドライン （2020 年 5 月）	総務省サイバーセキュリティ統括官室	・無線 LAN の利用者・提供者のそれぞれに向けて、セキュリティ確保に関するガイドライン（「Wi-Fi 利用者向け 簡易マニュアル」及び「Wi-Fi 提供者向けセキュリティ対策の手引き」）である。	https://www.soumu.go.jp/main_content/000690266.pdf https://www.soumu.go.jp/main_content/000690267.pdf
	3	我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言] （2020 年1月 28 日）	サイバーセキュリティタスクフォース （総務省サイバーセキュリティ統括官室）	・本タスクフォースにおける「IoT・5G セキュリティ総合対策」の策定・公表後の議論を踏まえ、本年７月より開催される 2020 年東京大会に向けた対処として早急に取り組むべき事項を整理したものである。	https://www.soumu.go.jp/main_content/000666221.pdf
	4	IoT・5G セキュリティ総合対策 2020 （2020 年 7 月）	サイバーセキュリティタスクフォース （総務省サイバーセキュリティ統括官室）	・「IoT セキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、IoT・5G 時代にふさわしいサイバーセキュリティ政策の在り方について検討し、「IoT・5G セキュリティ総合対策」として整理、さらに状況変化に合せて改訂したものである。	https://www.soumu.go.jp/main_content/000698567.pdf
	5	ICT サイバーセキュリティ総合対策 2021 （2021 年 7 月）	サイバーセキュリティタスクフォース （総務省サイバーセキュリティ統括官室）	・「IoT・5G セキュリティ総合対策 2020」公表後、施策の進捗状況等の確認を行いつつ、社会全体のデジタル改革の推進といった状況変化を踏まえ、新たな課題への対応や施策展開の加速化を図るための検討結果を踏まえ、策定したものである。	https://www.soumu.go.jp/main_content/000761893.pdf
	6	電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第2版) （2020 年 9 月 1 日）	総務省総合通信基盤局 電気通信技術システム課	・IoT 機器のセキュリティ基準に係る技術基準適合認定について説明したものである。	https://www.soumu.go.jp/main_content/000744264.pdf
	7	サイバーセキュリティ経営ガイドライン ver 2.0 （2017 年 11 月 16 日）	経済産業省 (独法)情報処理推進機構 (IPA)	・大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたものである。	https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf https://www.meti.go.jp/policy/netsecurity/mng_guide.html
	8	産業界へのメッセージ （2020 年 4 月）	産業サイバーセキュリティ研究会 （経済産業省商務情報政策局サイバーセキュリティ課）	・大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたものである。 ・今後、更にデジタル化を推進していくことの必要性が明らかになる中、改めて IT システムや制御システムのセキュリティ対策の徹底と強化を提言している。	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf

区分	No	文書	発表元	内容	アドレス
	9	サイバー･フィジカル･セキュリティ対策フレームワーク(CPSF) (2019 年 4 月)	経済産業省商務情報政策局サイバーセキュリティ課	・産業社会の全体像を捉えたものであり、バリュークリエイションプロセスに取り組むすべての主体を適用対象としている。	https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html
	10	ビルシステムにおけるサイバー･フィジカル･セキュリティ対策ガイドライン第 1 版 (2019 年 6 月 17 日)	産業サイバーセキュリティ研究会 (経済産業省商務情報政策局サイバーセキュリティ課)	・エレベーターや空調など多くの制御系機器を有するビル分野に関して、ビルシステムに関するサイバーセキュリティの確保を目的に、そのサイバーセキュリティ対策の着眼点や具体的対策要件を体系的に整理したものである。	https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html
	11	スマートホームの安心･安全に向けたサイバー･フィジカル･セキュリティ対策ガイドライン Ver1.0 (2021 年 4 月 1 日)	産業サイバーセキュリティ研究会 (経済産業省商務情報政策局サイバーセキュリティ課)	・スマートホームにおけるサイバー・フィジカル・セキュリティ対策の考え方や各ステークホルダーが考慮すべき最低限の対策について整理したものである。フレームワークは、組織がリスクマネジメントの原則とベストプラクティスを適用し、セキュリティとレジリエンスを改善することを可能にするものである。	https://www.meti.go.jp/press/2021/04/20210401005/20210401005-1.pdf
	12	中小企業の情報セキュリティ対策ガイドライン第 3 版 (2021 年 3 月)	(独法)情報処理推進機構(IPA)	・情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたものである。	https://www.ipa.go.jp/files/000055520.pdf
海外機関	1	重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版 (2018 年 4 月 16 日)	NIST 米国国立標準技術研究所/和訳 IPA)	・本文書は、重要インフラのサイバーセキュリティリスクマネジメントを改善することを目的として、フレームワークとして作成されたものである。	(英語) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (日本語) https://www.ipa.go.jp/files/000071204.pdf
	2	NIST SP800-171 rev2 NIST SP800-207 (2020 年 2 月、8 月)	NIST 米国国立標準技術研究所/和訳 IPA)	・SP800-171 では米国政府機関が定めたセキュリティ基準を示すガイドラインである。また、SP800-207 ではシステムを設計するうえでセキュリティをどう確保するかの指針（ゼロトラストアーキテクチャ）を示している。	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
国内 民間団体	1	5GMF 白書 5G ユースケースにおけるセキュリティ第 1.0 版 (2020 年 7 月 29 日)	第 5 世代モバイル推進フォーラム(5GMF)	・５G セキュリティの標準化動向を踏まえて、①IoT、②Connected Vehicle、③Fintech について、ユースケースにおけるセキュリティの課題の抽出、新規セキュリティ機能、対応状況、具体的対策案検討結果をまとめたものである。	https://5gmf.jp/wp/wp-content/uploads/2020/07/5g-whitepaper_1.0.pdf
	2	IoT 機器セキュリティ要件 2021 年版 Ver.2.0 (2021 年 6 月 18 日)	(一社)重要生活機器連携セキュリティ協議会(CCDS)	・本ガイドラインは、つながる機器における最低限守るべき要件(対策レベル：★星一つ)を定義する。本要件は、つながる機器を用いた IoT 機器、及びシステムにおける最低限守るべき要件としての適用を想定する。	https://www.ccds.or.jp/public_document/#GR01-2021-2
	3	IoT セキュリティ評価検証ガイドライン (2017 年 6 月)	(一社)重要生活機器連携セキュリティ協議会(CCDS)	・各種団体(IPA 等)より発行されたセキュリティガイドラインの評価検証に関する項目に対して、より具体的なセキュリティの評価検証プロセスを更に掘り下げた内容である。	https://www.ccds.or.jp/public_document/#Verification_guidelines1.0

区分	No	文書	発表元	内容	アドレス
	4	IoT システム調達のためのセキュリティ要件フレームワーク（2016 年 11 月）	（一社）重要生活機器連携セキュリティ協議会（CCDS）	・ IoT システムを構成するコンポーネント毎に想定されるリスクを分類し、リスク毎に部品調達時、製造時、流通販売時や運用開始～終了時に製造者や調達者などが考慮すべき一連の対策を、セキュリティの専門家で無くても適切に把握・理解し対策を実施できるフレームワークを提示している。	https://www.ccds.or.jp/public_document/#IoT_Raising
	5	製品分野別セキュリティガイドライン スマートホーム編 Ver.1.0（2019 年 10 月）	（一社）重要生活機器連携セキュリティ協議会（CCDS）	・ スマートホームが利用されるユースケースを踏まえ、生命や財産に対する影響を考慮した検討 や、 利用者が安心・安全にサービスを利用できるような具体的なセキュリティ対策案の提示したものである。	https://www.ccds.or.jp/public_document/#guidelines-smarthome_1.0
	6	製品分野別セキュリティガイドライン 車載器編、IoT-GW 編、金融端末（ATM）編、決裁端末(POS)編 Ver2.0（2017 年 5 月）	（一社）重要生活機器連携セキュリティ協議会（CCDS）	・ 車載・IoT ゲートウェイ・金融端末（ATM）・決裁端末（POS）の４分野の製品分野別セキュリティガイドラインとなっている。	https://www.ccds.or.jp/public_document/#guidelines2.0
	7	JBMS-90（ネットワーク機能付き事務機セキュリティガイドライン Ver.1.00（2021 年 6 月）	（一社）ビジネス機器・情報システム産業協会（JBMIA）	・ ネットワーク機能付き事務機の購入者が必要とする基本的なセキュリティ要件を定義したものである。	https://hyojunka.jbmia.or.jp/hyojun2/upload-v3/archive/JBMS-90.pdf