

第4回

チェック項目「防御」の解説

~リスク対応方針に基き、物理面、人的面、 技術面から防護策を実施する~

2020年9月1日 日本スマートフォンセキュリティ協会 (JSSEC) 利用部会 IoT調査・研究TF 中村 丈洋 (株式会社 SHIFT SECURITY)

IoTセキュリティチェックシート



JSSEC IoT セキュリティチェックシート 第2.1版 本チェックシートは、一般企品がNTを利用(導入)する時、セキュリティ面で発症すべきことを誘題 | | 的にまとめ、企品のIoT導入機能者や IoT機器ペンダーとの複数階、独内機能等への調金器の機構(もの 口は意味をなるなくしお店にまたを付ける事を出れても きし)への利用を保定し作成した。特にIoT等入のカギとなる「IT:依頼システム系」と「OT:整備シ ステム系」のコラボレーションによる効果的なセキュリティ対能の検討に罹用理事力い。 プロス - アロス ではたりなる 1990 C C A ②面積的なセキュリティフレームワークの採用により、利用者からの構成が制度性を完上した。 正金素の研究やは下の用金に合わせ機が開発を認めても ②位限システム (IT) 福当と発信システム (OT) 担当の人材交流・資産のための共通管理とした (RE: MOL-CAROMENE) HEURENGAATERGOATAVE - HEGES ②企品の状況やIoTの用途に合わせ検討返回を網接する目音として推議返回を研記した ■N4の文は複数的・・ビジネスへ大学な影響を考えない。 ②解抗症を追加し一般会別指導者が理解しやすくした。 第2.0種(2019年2月):MSTのサイバーセギェリティッシームワーク(CSF)をも上に利用者製の開催性を開始さ ■記載ビジネス・・他ののステータカルボーに記憶さるたる で) 会議を見たな「つながる」 本書や、松男への信用など 第2.3種(2020年2月): デュック双目の他社会体(YTSAOT)及び、選択(ITAOT)が正確な収息を検討した BNS* | National Institute of Exercises and Engineery (ASSESSMENT OF SEC.). A MARK NOT COLLS (PARAMETERS A MARK #TENANTANANTE CONSANT EI FARRECCIANA MICHONOMICANA MICHO

L	44	カテゴリー	inal unia: aradora (aventer-anesta) - arcora : arabanatikoana (eventab)	1	-	6033	CURR	A11	-1164	-	
Г			の作品が、は1000年上のかりたい場合とからない地域を映画しませ の作品が身合は「人ごと恋な考えないなど」を研究しまる					П			
			②中名の東京は「田田中代、大大名中代、松東市代のよ) を初回にする EXISTED (1772)ステムの数ののの意思を開発する	н	_	-	_	Н	_		_
	1	2002	型ルードウェブ、シアトウェブの特殊を指揮する 型品等はデータの方式を確認する	H	٠.	٠.	•	П			
	1	(ID.AM)	Bristan http://demercensieses	Н				Н			
			動きて発酵メーカー向きてシステム性機能の検索、および利用金属の検索	l			•	П			
			●CSRT/PSRTなどインシテント20回答用を用ると発表したTSRなどインシテントを実施の事業を	ш		\perp	\perp	Ш			
		ビジルス機械	を対することでは、はついてよるとなっては、またが、このでは、このでは、このでは、このでは、このでは、このでは、このでは、このでは					П			
		(ID.BE)		_	-	-		Н	_		
		ガバナンス	●sToリスク (リスクアセスメント) を認定し、確定者に適宜し扱めなか。リティがリシーの表面しをする●sTo等性 (施が多い、機能と一体、特も主しやすい、人への意象に関わるなど) を考慮する			•	•	П			
		(10.69)	● 2 屋の物形を整理し、人間を報道して配置する。 ・	_	\vdash	-	-	Н	_		
	1		●管理する運輸出作的より開発しの展示事業を検索する 機関をおかいるション・アルスの機関を開発したいる基本ではある。	•	٠.	٠.	•	П			
			DISTANCE NATIONAL DESTRONANTE DE CONTROL DE		-	-		Н			
	1		空間でポートから内容を発展する 空間空の選手に成功するリスク (第一次の名称との) を発展する	Ш	٠.	٠.	•	П			
	1		DE APPENDIX DE SETE CO	-	-	-		Н			
	識別 (ID)	l	●表示シールからのマルウェア協議を促集する	ш		•	•	Ш			
			10/ではからことで表名が記録し上記です。2007年 CUAF を確認する エリテトウェアのハードウェアの担望の不同(ミス)による外部へ大致認るは至する		•	•	•				
	50)	_		_		_			_	_	
	ent C	3 A I	回は「防御」を角	IJ	8	4			#	7	• 1
	4 M	541	四八人 「D刀和田」「今下月	生	Б.	16		7	-	· 4	
					-	•			_		
	1		SelentedDirectの内容不正常に入ります。 国内的な大型に大型(大型)が記載・他がミス(企業)をは重する				•	Н			
1	1		□ リスクラスメンシュの名式を表す。 単独を一のからのと呼吸をするのである。 □ リスクラスメンシュの名式を表す。 単独を一のためと呼吸をするのである。 □ リスクラスメンシュの名式を表す。 単独を一のためと呼吸をするのである。 □ リスクラスメンシュの名式を表す。					Н			
_	.l		GTA-USUNUEL-GENERACETS		Ľ.	Ľ.	_	Ш			
1	1	リスクマルジメ	15 (18				•				
7	1	ント記場	●第三をごとる呼音の整盤を置けている情報を示す。他で展記、1975大きとで 177データの概念により理解を開音を表示し、人名室の名	ш	\vdash			Н			
100	7	(ID.RM)	四字=身の社外機関ル=ルビはき(ルールがは(されば重める) 空をットラータの理解(インターをットや室外理会など)のルールビはき(ルー せんだ重める)	•	٠.	٠.	•	П			
	1		経過量が表現が開き、マニュアルなどに記載されているが確認する (国際基化) かな、のはのマモノ・バースに、パチェのいまだい パケアのカー・スカスと	П	_	-	_	П			
	1	1	空間のな時間の他の利用や富宝を他保持とび利用目的などを経過する	m	٠.	٠.	•	П			
	1		■マジートがた、ボーギでを指してものはアン 関係でも関係したビジネスペートテーとの「スクを指揮する ■ビジネスペートテーに関係を表示する「スクを指定する					П			
	1	#794 7. -	でクラスペートナーナル型のを立てる「ステモロエマる のどクラスペートナーナル型のを立てる「ステモロエマる		\vdash	\vdash		Ш			
1	1	ンリスクマルジ	正のではずした場合ではなりましてイマネジメントは元を記れるは、戸室する				•	Ш			
	1	4 < % (ID.SC)	#1,101年版、101アステムの日本年の日本リステット版画で G				_				
	1	(10.30)	#####################################			ı	•	П			
1	—	\vdash	CTER STORPLEWSONT TO A STORE AND A STORE A		\vdash	-	-	Н			_
	1		立め、よりもののではは着が着い着ける。 は、ははなみもりできた機能する区は、関係などは最大によったか。 はずいはなるようでは他のできたが、 はなるようでは他のできたが、 は、 は、 は、 は、 は、 は、 は、 は、 は、 は、 は、 は、 は、	•			•	ı			
	1 .		四ため」リティ対抗の不力が公の「全部を支援インターよっトに参加した。ように管理する 2016年度は、167システムの不安にサービスのボートは安全するなどは要素が他の程度を持ち ロディット・マステムのようであった。	Н	\vdash						
1			THE PART SERVICE SERVICE AND ADDRESS.	1	٠.	٠.	•	П			
1		747274	Enrithment of the control of the con	(•	•	Н			
14		7-TE, 25		1				Н			
"	防御 (PR)	ノアクセス制御	DOZKAT-KOGSBERSSSEY, SKIES (SDERKER, KPSKOSISSE) +8 KRIGISSERVISSESSESSES	П		٠.	•	П			7
7		(PRAC)	図りとベスタードを発達させいキーザと共産しない 図りとベスターに対象が大きしたはいまかりしない 対象に対象が、1972メラムには、対象のは対象はある。	Ш				Ш			
П	リスク研究の対象に基	1	20(6年度は、1670分支に対し、が東京とは意味を利用する 立って紹介が認めませます。(世界には第一人のおけた)テセと 20(月度) (本一学) のは10年度を対する(ログリスラード、ビカード、集合的はなど)					П			
M	9. 他程度、人の五. 信息をからの数		立た典を(キーザ)の問題を指摘する(ロバスラーズ、「カーズ、重要問題をと) 回かけままた(かきっかなど)の問題を使わせる(漢字語符書など) 打ち機能的とき。」(サインをは)の問題を使わせる(漢字語符書など)					Ш			
1	MORE+2	1	27、他などのなちょりティアのをかけずる の元スペッシスを持たとかけずる					П			
		\vdash	●東京をから、正式語とど表計する ●全部ケーフルはとび正から一フルカの記録と、 乗車、終年されらかまたもの配する 関係しなりを表示機能等へ表記される。	F	\vdash	\vdash	Ě	Н	_		∕
		1	●関連事業 (機能が開かるせぎ、「この様を他」(所はしたい) こと)			١.	•	П			
		実施の上分とび	・システン会会 1000 2.17 年末 2016年後後、1070 ステムの発売を1223年1223年	Н	\vdash	\vdash	\vdash	Н			
		0-200	2015年後に、1970大子の日本会社ではおりませる。 他の下級は、1970大学上の管理事情をも担保 他の下級はイカーのイン大学と自然のではは、おより利用なのはは	1		ı		ч			
1	1			r				П			
┖			このまた。					ш			

	#7#U=		111	CHEE	E033	E032	x:	PER.	- Middles
		Market and the second s				_	г		
		Market and the second s							
						_	⊢	-	
		200日では、 では、またしてはなるので、その他が哲学しまれているを紹介する はののでは、はでのできるので、ようでは、特別のではないできた様子となるかです。	•~	_		•	Н	_	
		アルアルタットフェットの成功を経過する場合は、上しば、個名の大きを用する アルアルタットフェットの概念を経過する場合は、上しば、個名の大きを用する 区ではためた。不可での概念を続けて	1				N		
	244×1		-	\vdash			L		
	7 (PR.05)	□なるよりティ対策が開発などを終え、なるようなゲートフェイを発表する。	1 1				П	·	
		34、国主で配り出き人が主任を取扱いとうにする 工芸芸をは外によるにて経験、ヒアシステムの登室工芸を設定する				•	Г		
		AND CONTRACTOR OF THE PROPERTY	П				Г		
		②開発がは完全な点式は発性性に、機能の再発・無限には必要性、表別は完全は点が可能をつきまする。 フェイン・ファイン・ファイン・ファイン・・・・・・・・・・・・・・・・・・・・・・・	1		٠.	٠.	П		
/ / [2013 MANDAM THE THE TOTAL OF THE	Н	-			т	-	
/		●ファンチートではかが明らかける。 27/37年のファンチート学院を開ける。 27/37年のファンチート学院を開発し出来する。	J I	\vdash	_	_	┖	_	
		#/00 年間のアンデートを始めていてきる。 ロアップデート時代のアップデートナッイルの入身が出か了いてデート表示を設定する。 ロアップデート時代が直接は「記述人際上のアップデートファイルの原発化など」を指数する。					П		
Person (mm)	BESSETS	②アップデート対応主義 (25人間上がアップデートファイルが記者だけだ) を指数する○アップデートする場所は下る重める②宣士にアップデートする単位にアップデート権力を呼ばれませる	ш		•		П		
	t#07etX	●富士にアップテートでも単位とアップテート組み取り出版を示されまする ●富士にアップテートの不見会があった時の第1年前を高度する 取付 アンデアト的主義のはいたい知るとなっているとなった。	ш				П		
	が上び手根	はインシアントの基本的なのでありませまする ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・					Г		
	(PRJP)	■インシデント対応を加強の対応性を申請を開催する 単定的のためのデータイックアップを重要を指する	-		٠.	٠.	П		
E. 成物至于心理医		BNATARDY - カーサウム、PCESTICE、BACなどの他は独立を展示では、かけた地域中はを重する 立本元を中心になってもなる性はなどに対する(Mattyl トウィールセン)					Н		
2022+2		□ 中心をからは同じておりませんを見るというとう。 □ 中心とどかを見かる情報をからを知ると、自己の意思と思想していたものからに思想を指する。 □ 自分がする温度が行われた経済をおり、(自己計画への意思) を検索する。	H				П		
		②は何をする全なが行われる設計はおびの(自たが終への起の)を検査する ②大規則ではどの可能が表示ってデートルが図るがある情報する 「我们は他がカフトの」では、また、一つは、アデートルができませます。	ш						
		Winterのシットウェアを開発されージョンピアップデートする ●:TGMの収入機能で展示のシットウェアピアップデートする		•	•		Г		
N I		● の下級的の使込を終す業別のシットでようにアップデートする ● 製造的には下級的シットでよう業別のページェンにアップデートする 例は有限と、はアンテムの表示の中のではないです。		Ľ.	_	_	1	_	
	∰T (PR.MA)	#1067年202、10万0万子上の他立体的自動にする 他の行政と、10万0万子上の何の行政(加工条件、金数、金属用金、可数可差など)を言葉する 4次の保存性機能を表現を確認される。		\vdash	•	•	ш	_	
		のは、日本のでは、日			۱.	١.	П		
		#INTERNATIONAL PROPERTY &		\Box		_	L		
		第3(6) 福祉的の基本のグログルをから記さる 立立版をキラー内域(セーナティの内側)が向えるもの数する 立動が表記されば(セライアビリティの付集)が向えるもの数する					П		
	207 207	□動作業をから成(リティアビリティ系統集)が開発された設定する。 □ 空気気が開発が応援、アクセス開発(セギュリティ系統集)が開発された対象する。	ш		۱.		П		
1 '	(PR.)	□ 正元が明日の時代、アクセスを取りたキュリティを作用)が取れるで記載する □ こがカタインスタンプログを記る会内でも □ のまました。 「中で表現したのなった。」	ш				М		
	TENNET C-	型点を立か、様式を整かする場合 マッシティブを発性ののできたをした。(カッシティブを見る者が重要に記事(1+3)	1-1	\perp	<u>L</u>			_	
	SANATOREL.	は、このの基本のから数金の調査をある。 の表面は、これが終れていること(2000年)のことで、単位でする ののできた。 2000年の日本	1				П		
	TRIKY	第10万元間をは全域的。				٠.	П		
	mercan.	正式では守ちの日子3 初かけ高級、はかり大手が高速を発達する。 の「大型のログゲインペント」ではかる区域の他に対しる他にする(区域とかにする主要)	_	\vdash	-	-	Н	-	
樟知 (DE)	(DEAE)	●67年経のセグラインベントリの成から国際の機能を出る機能する(国際となどが登画機) ●区域として機能するしま、個別機能する。	•				П		
954 (DE)	(DENE)	● 本本 () できない () しまい () を		⊢	-	-	₽	-	
	********	#記録シップークを認めらずシステムの異常を確認的に整合する 正確はしたが確認のログセスをレータリングしませるを取りさせばするますする ではなり、トラスタのディナース・アインをはなり、まったのからストリストの表示する。	1				П		
c → m mas ≥ m m	■数数をもまれ リング (DE.CV)	型数三したが高級にマルケェアなどが発生した。での数するを基準を増加する 図案が発生的するとはよるを認定に重要したエグリングする	-	\vdash	_	_	┖	_	
NO MARKS 17 1			ш	\vdash	\vdash	•	┖	_	
	他第7つセス (DE.DE)	25 位記した異常の原理をできまする ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	-				П		
	,,	● では、これでは、これです。これでは、これでは、これでは、これでは、これでは、これでは、これでは、これでは、		-	-	_	Н	-	
	HENE	●ビタケに発生率ある役割し、状況(200セビ)、記念(ログセビ)を応えする ●インシデントの第四級の対応手段をもとど、発生した事務にあたけた事件を通信する。			١.		П		
	(RS.RP)	●インシデントの変数に対応し返回の大変変化する ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・					П		
1 1		●第十元との対象を記述する 20インシテントを開発を開発して記載する		\Box			П		
1	25.20- 0.00	○外 車が表示できませき 毎日本の大力をようの表を含まする		\vdash	_	_			
対応 (RS)	(BS.00)	SIVインシデントの概念は万名シーカーやは発着に正確する Vンシデントの発達は万名シーカーのオポート第二ペ記号する	r.						
	,	STICHER, INTO DEPARTMENT PORTO NEED MARTS CONTROL OF THE CONTROL				•	L		
Z4:007#60		DESCRIPTION OF THE PROPERTY OF			•	•	П		
企し対応要と使達		SE(ATMESS、INTEXのテムのイベントログセとを分析し異常を構造する 下途がショウムナムトログルクテス					П		
計算を表面し、過 事態大変変変する	SHE (RS.AN)	ファスレッジック技術がどの表現したのでは会と意思を確定する。			٠.	٠.	ı	1	
		・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			•		t		
) l		● 17年後、17システムのインシテントを呼吸し、対応の計画は基する 数(基本に大き主義する		\vdash	-	-	۰	-	
1 1	他気(RSJMI)	●キットフーかを記録してルフェアの応力を禁止する ②マットェアを記録する		•	•	٠.	ı		
		「空間間を20万のアップデートを作う 8万は1個数 187の文字上のオンシデントルと学者する		\vdash	\vdash	-	-	-	
$\vdash \vdash$	ME (RSJM)	●では日本の表面に対象でも用する 対象ではない。1875のデエをかりのデントを連れる機能とは表する	r.	\vdash	\vdash	•	-	-	
	ente	●/シグラントの基本的な正言事情をもとに、機能した事故にあわせ注意事情を提供する ●正言を与いる言葉を受けた発酵を得る	ы		١.	١.	ı		
復旧 (RC)	(RCRP)	●正古からに近古無事を動す。980年9年3 ●正古が第7日七日とも980年3 ●インシデントロ素型に対応し近年60元を配止する	*		٠.	٠.	ı		
▼の公園を計画を		「ないではない。」とすシステムホインシテントから共民族とを担任する。		\vdash	\vdash	-	۰	-	
	SEE (ROJM)	●イッシデットから得た中枢を不確認とに使用する●本理のイッシデットが他のは存储が、1sTシステムで発達したいが確認する			•		ı	1	
は安存をと関係を	35.20-	●工作と言う表示した例とも用する 例がは他的にはできまるのうとデットを集を集める。		\vdash	\vdash	\vdash	-	_	
	51126- 517	○の人用をこくシャナントの中国大は完全するをの対象を担づる ・ご然のインシャントの中国大は完全するをの対象を認定する ・ごだのインシャントのドラフィテューンの中で発達した。中国国会社に登録する			ı	٠.	ı		
	(RC.CD)	●CSRT/PSRTと国際しまデータホルダーに名書する		oxdot		L	L		
AE-IIE		※ 1555C並びに製産製造者は、テェックシートなどに繋ずるいかなる重要も負うものではありませ	Á. 5	THE	200	CHEC:	£45	学べしま	f.
HE-EE	+4	※ カチェックシートに会場する意味を・サービスをは、一般に手社の意思されは意味を示す。 ※ 社内文書などに利用する場合、表行信息で認められた利用の概要のでご利用ください。また、そ	OWN	2525	297	.565	Ess.		
発行・要作権・		※ 社内文書をどじる開きる場合、悪情の意で飲められた利用の簡単符でご利用くだ多い。また、そ 同符号: 3009を引き始る「COORSEARY 日本記書人 日本スマートフォンセキュ 老代名: 一般の表述人日本スマートフォンセキュリティ協会	17	90 U	SSEC)	SINE	•		

チェック項目「防御」



- **①NIST-CSFの分類:平常時、6カテゴリー**
 - (1)アイデンティティ管理、認証/アクセス制御 (2)意識向上およびトレーニング
 - (3)データセキュリティ (4)情報を保護するためのプロセスおよび手順
 - (5)保守(6)保護技術
- ②企業のIoT推進者や管理者の視点で検討すべき点:23項目
- ❸IoT用途レベル毎の推奨項目:3つの重要度に分類
- ⁴各社の検討内容 採用理由/追加項目:検討結果の見える化
- ⑤検討主体(IT又はOT)及び、連携(ITとOT)が重要な項目を明記

NIST-CSF	(Ver.1.1)	loT-l	キュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携がI	重要]	用途レイ	ベル毎の打	推奨項目	自社の検討内容コメント			
機能	カテゴリー	ı	一般企業でIoTを利用(導入)する時に検討すべき観点 語】IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス		采用 ・採用/不採用などの理由 一部採用 ・検討のポイント 下採用 ・追加検討項目		
		① c ② c	機器の機能および用途に応じてネットワークへ接続する方針や条件を検討する 機器のインターネットへの接続が必要か否か検討する(閉域網の検討) 機器をネットワークへ接続する際には、認証および暗号化によるセキュリティ対策を実施する ドュリティ対策が不十分なIoT機器を直接インターネットに接続しないように留意する	要点	•	•	•	,			
	アイデンティ	23)lo ① 7 ② † 24)lo	機器、IoTシステムの不要なサービスやボートは停止するなど必要最小限の設定を行う フォルトで有効になっている不要な機能やサービスは無効にする ービスに必要のない不要なポートは停止する 機器への外部からの不正アクセスを防止する マイアウォールなどにより外部からのアクセス制御を行う	要点	•	•	=				
防御(PR)	ティ管理、認証 /アクセス制御 (PR.AC)	2 5)lo ①[[②第 ③[[機器、IoTシステムの管理者権限・利用者権限のIDとパスワードの設定および管理を適切に行う とパスワードを初期設定のままとせず、適切に変更(変更後の文字数、文字種別などにも留意)する 三者に知られないよう厳重に管理する とパスワードを権限のないユーザと共有しない とパスワードを他システムと使いまわししない	15	-	•	•				
リスク対応方針に き、物理面、人 対面、技術面から		26)lo ①lo ②#	機器、IoTシステムに対して適切な認証機能を利用する 機器の認証を検討する(電子証明書、IoT機器域別子など) 用者(ユーザ)の認証機能を検討する(ID/パスワード、ICカード、生体認証など) システム(クラウドなど)の認証を検討する(電子証明書など)	要点16			•	, ,			
方護策を実施する		2 j	的なセキュリティ対策を検討する 三者の入室制限など検討する 這ケーブルおよび電源ケーブルの配線は、傍受、妨害または損傷から保護する 3.クを社内利用者へ周知する	新規			-				

防御について



- ■「攻撃を防ぎリスクを軽減するための活動」をチェック
- ■防御策の策定・実施はITとOTが協力して行う
- IoTの防御は 物理的、人的、技術的 と多層的に行う
- ■「防御」は6つのカテゴリに分類される
 - ①ID管理、認証/アクセス制御
 - ②意識向上およびトレーニング
 - ③データセキュリティ
 - 4情報を保護するためのプロセスおよび手順
 - 5保守
 - 6保護技術
- ■以下、ひとつづつ見ていきましょう。

ID管理、認証/アクセス制御



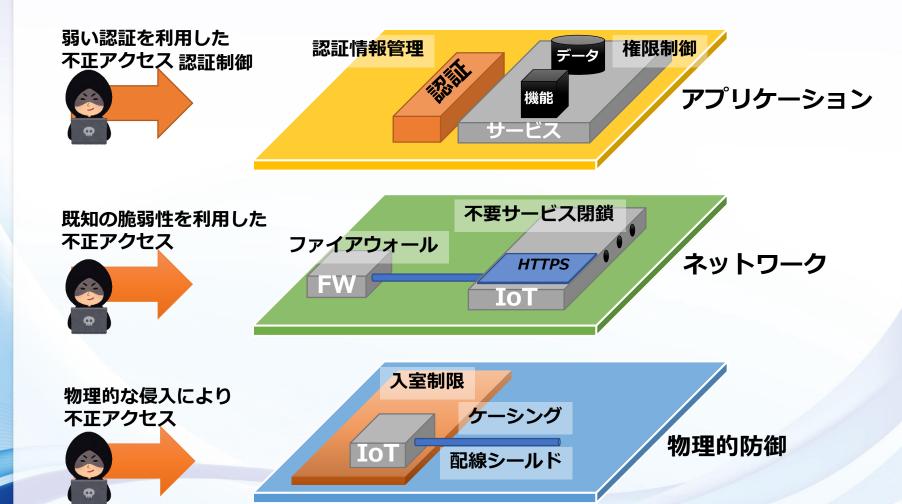
loTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が動	用途レベル毎の推奨項目			
一般企業でIoTを利用(導入)する時に検討すべき観点 【用語】IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス
22)IoT機器の機能および用途に応じてネットワークへ接続する方針や条件を検討する ①IoT機器のインターネットへの接続が必要か否か検討する(閉域網の検討) ②IoT機器をネットワークへ接続する際には、認証および暗号化によるセキュリティ対策を実施する ③セキュリティ対策が不十分なIoT機器を直接インターネットに接続しないように留意する	要点 14	•	•	•
23)IoT機器、IoTシステムの不要なサービスやボートは停止するなど必要最小限の設定を行う ①デフォルトで有効になっている不要な機能やサービスは無効にする ②サービスに必要のない不要なポートは停止する 24)IoT機器への外部からの不正アクセスを防止する ①ファイアウォールなどにより外部からのアクセス制御を行う 25)IoT機器、IoTシステムの管理者権限・利用者権限のIDとパスワードの設定および管理を適切に行う ①IDとパスワードを初期設定のままとせず、適切に変更(変更後の文字数、文字種別などにも留意)する ②第三者に知られないよう厳重に管理する ③IDとパスワードを権限のないユーザと共有しない ④IDとパスワードを他システムと使いまわししない	要点 15	•	•	=
26)IoT機器、IoTシステムに対して適切な認証機能を利用する ①IoT機器の認証を検討する(電子証明書、IoT機器識別子など) ②利用者(ユーザ)の認証機能を検討する(ID/パスワード、ICカード、生体認証など) ③IoTシステム(クラウドなど)の認証を検討する(電子証明書など)	要点16			•
27)物理的なセキュリティ対策を検討する●第三者の入室制限など検討する②通信ケーブルおよび電源ケーブルの配線は、傍受、妨害または損傷から保護する	新規			

■不正アクセスの防止策を策定・実施

- ・適切なID/パスワードの管理(No.25)
- ・認証による資産の保護(No.26)
- ・論理的(No.22, 23,24)、物理的(No.27)なアクセス制御

ID管理、認証/アクセス制御 ケーススタディ





意識向上およびトレーニング

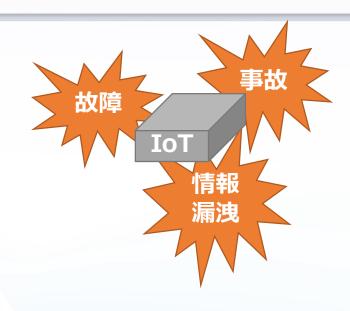


IoTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が重	用途レベル毎の推奨項目			
一般企業でIoTを利用(導入)する時に検討すべき観点	第一版要点	PoC又は	基幹	重要
【用語】IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	No.	補助的	ビジネス	ビジネス
28)リスクを社内利用者へ周知する				
●禁止事項(機器が壊れるなど、「この様な使い方はしない」こと)	要点19			
②重要な説明事項(個人情報やプライバシーに関わること、生命や重大事故につながること) ③システム全体に影響を及ぼす事項	-			
● フステム主体に影音で及ぼり事項 29)IoT機器、IoTシステムの関係者に役割を周知する	·······			
●loT機器、loTシステムの管理責任者の役割	1 1			
❷IoT機器メーカーやIoTシステム提供者の役割、および利用者の役割	要点20			
❸ IoT機器、IoTシステム運用や保守担当の役割				
◆CSIRT/PSIRT、またはインシデント対応関係部署の定義と役割(IoT機器などインシデント発生時の連携会会の関係を表のの制には、よる場合し、これがよう。	Ī			
30) 関係者の役割に従った手順をトレーニングする ① 関係者の役割に従った手順を明確にする	要点20			
②関係者の役割に従った手順をトレーニングする	20,711,20			_

- ■組織の構成員に対するセキュリティ規則の周知、意識造成とトレーニング
 - ・利用者への注意・禁止事項の周知する(No.28)
 - ・関係者(各運用担当者、管理者等)に役割を周知する(No.29)
 - ・役割に従った手順策定とトレーニングの実施(No.30)

意識向上およびトレーニング ケーススタディ





機器の誤動作が重大事故につながることも



禁止事項・注意事項 を定める インシデント発生時の役割を明確化

システム運用者、保守担当者と 情報セキュリティ部門、CSIRTの協調が重要

「定める」だけでなく「守る」活動が必要



周知徹底とトレーニング

実践してみるとルールや手順の問題点も見えてくる。 定期的なトレーニングにより担当者のセキュリティ意識を育てる。

データセキュリティ



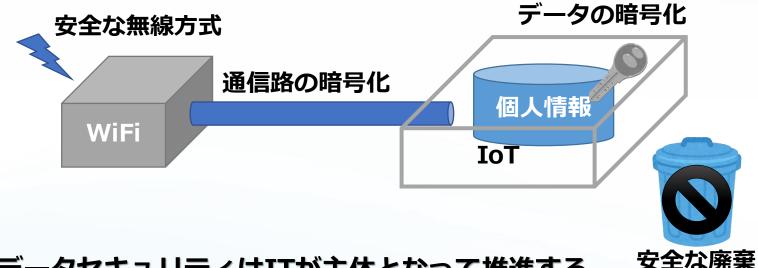
IoTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が重	用途レベル毎の推奨項目			
一般企業でIoTを利用(導入)する時に検討すべき観点 [用語] IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス
31)守るべきデータが暗号化されているか確認する ①IoT機器、IoTシステムに保管されている情報が暗号化されているか確認する	要点8			
32)IoT機器の接続、IoTシステムのゲートウェイ経由の接続などの環境に応じた暗号化を検討する ①Wi-Fiネットワークへの接続を設定する際には、より強い暗号方式を使用する ②可能な場合、有線での接続も検討する ③Telnetログインを無効にし、可能な限りSSHを利用する 33)IoT機器側でセキュリティ対策が難しい場合、別途セキュリティ製品を導入し全体でセキュリティを確保す ①セキュリティ対策が困難なIoT機器は、セキュアなゲートウェイを経由する	要点14		•	•
34) 設定情報が改ざんや変更されないようにする ①管理者以外によるIoT機器、IoTシステムの設定変更を禁止する	要点15			•
35)IoT機器の廃棄や再利用時の対策を行う ①個人情報・秘密情報を完全に消去する方法を提供者に確認する ②廃棄時は完全消去又は物理破壊、組織内再利用時には初期化、売却は完全消去が可能時のみとする ③中古など再利用する場合は、不正に改造がされていないか提供者に確認する	要点18			

- ■IT主体でデータの機密性・完全性・可用性を確保
 - ・データの暗号化(No.31)と通信路の暗号化(No.32)
 - ・機器自体での暗号化が困難な場合の代替策の検討(No.33)
 - ・管理権限の明確化(No.34)
 - ・廃棄のデータ消去と再利用時の安全確保(No.35)

データセキュリティ ケーススタディ W SMARTPHONE SECURITY ASSOCIATION



IT主体での「データ」の保護



- データセキュリティはITが主体となって推進する
- ■データや通信路の暗号化
- ■無線機器利用時の安全な方式選定 etc.

情報保護のプロセス



IoTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が重要】				性奨項目
一般企業でIoTを利用(導入)する時に検討すべき観点 [用語] IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス
36)IoT機器、IoTシステムの使用期間とサポート期間を確認する ●IoT機器、IoTシステムのサポート期限(EOL/EOSL)が提示される/されているか確認する ②アップデート可能な期間を確認する 37)IoT機器のアップデート手順を確認し策定する			•	•
①アップデート情報やアップデートファイルの入手方法やアップデート手順を確認する ②アップデート時の安全性(改ざん防止やアップデートファイルの暗号化など)を確認する ③アップデートする判断基準を定める	要点17		•	•
◆安全にアップデートする手順とアップデート後の動作確認手順を策定する⑤アップデートの不具合があった時の戻し手順を策定する38)インシデント発生時の対応計画と復旧計画を策定する				
●インシデントの基本的な対応手順を策定する②インシデント対応後の基本的な復旧手順を策定する③復旧のためのデータバックアップ計画を策定する	新規			•
39)IoT機器メーカーやIPA、JPCERT/CC、ISACなどの脆弱性情報を収集・分析と対応手順を策定する ①不具合や脆弱性などの情報を提供者に確認する(Webサイトやメールなど) ②IPAなどの機関から発信される情報を確認し、自社の構成に類似していたら提供者に影響を確認する	要点18			•
③提供者から通知が行われた脆弱性の影響(自社利用への影響)を特定する ④利用制限などの暫定対策とアップデートなど恒久対策を検討する				

■セキュリティ方針、プロセス、手順による情報の保護

- ・機器/システムの保守についての計画と手順化(No.36, 37)
- ・インシデント対応時の対応/復旧の計画策定(No.38)
- ・セキュリティ情報収集の計画(No.39)

情報保護のプロセス ケーススタディ Wisharphone Statistical Statis Statistical Statistical Statistical Statistical Statistical Sta



IoTのシステムはハードウェア以外にも様々なソフトウェアで構成される。 例)ファームウェア、OS、アプリケーション



IoTシステムの維持にはソフトウェアのアップデートが重要

- ■「いつまで」アップデートが提供されるか… エンドオブライフ=EOLを認識
 - ①「いつ」アップデートするか?
 - ■保守のタイミング・頻度を定める
 - ②「どうやって」アップデートするか?
 - ■閉環境におけるアップデート方法など、特殊な場合も生じうる

保守

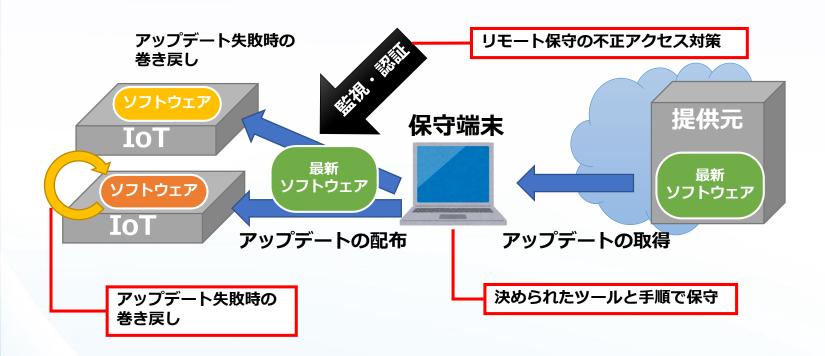


IoTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が重	用途レベル毎の推奨項目			
一般企業でIoTを利用(導入)する時に検討すべき観点 【用語】IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス
40)IoT機器のソフトウェアを最新のバージョンにアップデートする ①IoT機器の導入時点で最新のソフトウェアにアップデートする ②継続的にIoT機器のソフトウェアを最新のバージョンにアップデートする	要点15	•	•	•
41)IoT機器、IoTシステムの構成情報を最新にする	新規		■	■

- ■「情報保護のプロセス」で定めた方針にそった保守の実施
 - ・ソフトウェアの更新(No.40)
 - ・構成情報の更新(No.41)
 - ・保守作業の明確化(No.42)

保守 ケーススタディ





保護技術



IoTセキュリティチェック項目【項目No.表示例 ①:ITが主体的にOTと連携、❶:OTが主体的にITと連携、❶:ITとOTの連携が重	用途レベル毎の推奨項目			
一般企業でIoTを利用(導入)する時に検討すべき観点 【用語】IoT機器:IoTのデバイス(センサーやアクチュエータを含む)、IoTシステム:IoTに使われる情報システム(クラウドを含む)	第一版 要点 No.	PoC又は 補助的	基幹 ビジネス	重要 ビジネス
43)IoT機器の必要なログが取れるか確認する ① 故障やエラー情報(セーフティ解析用)が取れるか確認する ② 動作環境の情報(リライアビリティ解析用)が取れるか確認する ③ 攻撃や認証の情報、アクセス履歴(セキュリティ解析用)が取れるか確認する ④ ログのタイムスタンプなど時刻を合わせる ⑤ 必要なログ、保管期間などを決める ⑥ センシティブな情報のログ出力をしない(センシティブな情報を含む場合は暗号化する) 44)IoT機器の必要なログが安全に保管されるか確認する ① 不正アクセス対策がされていること(改ざん・消去対策)を確認する ② ログへのアクセス権限の設定を確認する ③ ログの暗号化を確認する ④ 保管場所を確認する	- 要点13		•	•

■前述以外のシステムを保護するための技術 ここでは主に証跡による利用者/システムの保護に着目 ・ログを収集・保管する(No.43, 44)※ IT主体

保護技術 ケーススタディ





アクセス・操作履歴やシステムエラー等を 「ログ」として保管



- ■問題の予兆を検知
- ■問題発生時の原因/影響範囲を把握

ログを取ることは有用であり、重要だが、 「個人情報」等がログに含まれる場合には扱いに注意が必要

■ 記録対象の選択、個人情報のマスキング、暗号化

次回の紹介



- ■IoTセキュリティチェックシート入門
 - ■次回は「チェック項目 検知・対応・復旧」 になります。
 - 5検知・対応・復旧
 - ■異常を検知する仕組みを構築します
 - ■被害拡大を防止し、システムを復旧するための対策を定めます

次回の受講おまちしております。

ご覧頂きありがとうございました Wishartphone Security Association





~安心・安全にIoTを活用するために~