資料88-3

技術基準適合認定等におけるセキュリティ基準とJC-STAR★1のセキュリティ要件・適合基準の比較における一考察

横浜国立大学
大学院環境情報研究院/先端科学高等研究院
教授　吉岡　克成

2つの観点で比較

- （セキュリティ基準・セキュリティ要件の）対象と確認方法

- 脆弱性への対応

（セキュリティ基準・セキュリティ要件の）対象と確認方法

「電気通信の機能に係る設定を変更できる端末」は、設定変更するためのアクセス制御機能が必要

○端末設備等規則（「端末設備等規則及び電気通信主任[illegible]一部を改正する省令（平成 31 年総務省令第 12 号）」による改正後）＜抜粋＞

（インターネットプロトコルを使用する専用通[illegible]設備等端末）

第三十四条の十　(1)専用通信回線設備等端末（デ[illegible]ルデータ伝送用設備に接続されるものに限る。以下この条において同じ。）であつて、(2)デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、(3)電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。以下この条において同じ。）に係る設定を変更できるものは、次の各号の条件に適合するもの又は(9)これと同等以上のものでなければならない。ただし、(4)次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。

一　(5)当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。

二　(6)前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。

三　(7)当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。

四　(8)当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

（セキュリティ基準・セキュリティ要件の）対象と確認方法

第３４条の１０　専用通信回線設備等端末（デジタルデータ伝送用設備に接続されるものに限る。以下この条において同じ。）であつて、デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。以下この条において同じ。）に係る設定を変更できるものは、次の各号の条件に適合するもの又はこれと同等以上のものでなければならない。ただし、次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。

一　当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。

二　前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。

三　当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。

四　当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

(1) 該当する欄に“○印等”を記入して下さい。
(2) 該当する項目がない場合は、（　）内に記入して下さい。

	申込機器は国際標準 ISO/IEC15408 に基づくセキュリティ認証(CC 認証)を取得しているため以下の記載を省略します。 添付資料：別紙－

1. アクセス制御機能に係る識別符号の初期状態変更を促す機能又は機器ごとに異なる識別符号が付されていることの確認

	a. 申込機器は初めて利用するときにあらかじめ設定されている識別符号(ID 及びパスワード等)の変更を促します。	別紙－　　で確認
	b. 申込機器は機器ごとに異なる識別符号(ID 及びパスワード等)が付されています。	機種ごとに異なる識別符号を付す製造工程が確認できる資料を添付 別紙－　　で確認
	c. その他（　　）	別紙－　　で確認

の機能が変更できることを確認して下さい。

端末機器の技術基準適合認定等に係るJATE様確認フォーム

左記の確認フォーム（JATE様資料）では、機器の設定を変更する際のアクセス制御について確認する手順となっているように読める

機器の設定を変更する機能は、機器の製造者（申込者）が意図的に実装するものであり、申込者は自ら実装した機能については適切な確認ができると期待される

しかし、複雑化するサプライチェーンにおいて製造者（申込者）すら把握していない通信機能が機器に存在する場合があり、それらが実際にサイバー攻撃の対象となっている。現在の確認手順でそのようなケースを発見できるか確認が必要と考える

事例：大学内の脆弱IoT機器調査

- 横浜国大内で動作する機器について網羅的な調査を実施（2021-2022）
- Telnetが動作するIoT機器116件（36モデル）を検出
- マニュアルが取得できたTelnetが動作する機器30モデルのうち、15モデルでTelnetに関する記載が全くなし．5モデルではTelnet利用目的の記載なし．
- 22モデルについて、Telnetの利用目的を問い合わたところ，5モデルは目的不明、1モデルはTelnet自体を知らないと回答．
- メーカであっても、自社製品で動作するネットワークサービス（通信機能）を完全に把握している訳ではない（チップベンダ提供のFW利用や開発の外注が背景）
- 過去に横浜国大がマルウェア感染の注意喚起を行った際、製造者が自社製品で動作するTelnetを認識していなかった事例が多く存在（ルータ等）

Device Type	Telnet or FTP	Telnet	FTP
Smart card reader	53 (2)	53 (2)	53 (2)
Printer/Multi-function printer	38 (27)	21 (16)	36 (25)
Electric current monitor	13 (2)	13 (2)	11 (1)
Display controller	11 (1)	0 (0)	11 (1)
NAS	11 (10)	1 (1)	10 (10)
Announcement broadcast system	8 (1)	0 (0)	8 (1)
Data logger	6 (2)	0 (0)	6 (2)
Earthquake early warning system	6 (2)	6 (2)	0 (0)
L2 switch	5 (2)	5 (2)	0 (0)
Wireless LAN access point	4 (2)	4 (2)	0 (0)
UPS	4 (2)	4 (2)	1 (1)
Wireless LAN controller	3 (1)	0 (0)	3 (1)
Energy monitor	3 (1)	0 (0)	3 (1)
Router	3 (1)	3 (1)	0 (0)
Network adapter for printer	2 (2)	2 (2)	2 (2)
Web camera	2 (2)	1 (1)	2 (2)
Black and white printer	2 (1)	0 (0)	2 (1)
Paperless recorder	1 (1)	0 (0)	1 (1)
HPLC controller*	1 (1)	1 (1)	0 (0)
Web conferencing system	1 (1)	1 (1)	0 (0)
Power supply Control	1 (1)	1 (1)	0 (0)
Backup storage	1 (1)	0 (0)	1 (1)
Total (IoT devices identified model No.)	179 (66)	116 (36)	150 (52)

* High-Performance Liquid Chromatography (HPLC) controller

Takayuki Sasaki, Takaya Noma, Yudai Morii, Toshiya Shimura, Michel van Eeten, Katsunari Yoshioka, and Tsutomu Matsumoto, "Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network," Proc. 45th IEEE Symposium on Security and Privacy (IEEE S&P 2024), 2024.

JC-STAR★1では

脅威に対抗するために★1で実現すべき対策

IPA

★1で考慮すべき主な4つの脅威に対し、★1の位置付けや海外制度の基準等を踏まえ、製品／製品ベンダにおいて実現すべき対策を以下のとおり選定

★1で考慮すべき主な脅威	脅威に対抗するために★1で実現すべき対策			
	製品における対策		製品ベンダにおける対策	
	カテゴリ	対策	カテゴリ	対策
1. ①弱い認証機能により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	• 容易に推測できるパスワードが設定できない仕組みを導入する • セキュアな認証の仕組みを提供する • ブルートフォースによる認証試行を防ぐ仕組みを提供する	情報提供	• セキュアな利用方法に関する情報を提供する
1. ②脆弱性の放置により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	脆弱性対策、ソフトウェアの更新	• 深刻度の高い既知の脆弱性及び主要なCWEに対する対策を行う • ソフトウェアコンポーネントがアップデート可能な仕組みを導入する	情報・問い合わせの受付、情報提供	• 製品に関する情報及び脆弱性に関する情報を提供する • セキュリティパッチの適用方法に関する情報を提供する
1. ③未使用インタフェースの有効化により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	インターフェイスへの論理アクセス	• 不要なインタフェースを無効化する		—
1. ①～③外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	データ保護	• 機器が保有する守るべき情報を保護するた…供する（①～③の脅威に共通する対策）		—
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威	データ保護	• インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装する	—	—
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威	データ保護	• 機器の利用中に機器内に保存された守るべき情報を製品本体や関連サービスを介して削除できる機能を提供する • 機器に当初から搭載されている守るべき情報を保護するための機能を提供する	情報提供	• セキュアな廃棄方法に関する情報を提供する
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威	レジリエンスの向上	• ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源OFF前の状態を提供する	—	—

不要なインターフェイスの無効化を明記しており、メーカすら認識していない脆弱サービスも発見できる可能性

JC-STAR説明会(24.11.28/12.2/12.6)

©2024 独立行政法人情報処理推進機構(IPA)

JC-STAR説明会（2024.11.28/12.2/12.6、独立行政法人情報処理推進機構（IPA）　）より

2つの観点で比較

- （セキュリティ基準・セキュリティ要件の）対象と確認方法

- **脆弱性への対応**

機器の脆弱性を狙う攻撃の増加

Year	# Occurrences	# Exploits	# Vulnerabilities
2017	46	10	8
2018	727	15	15
2019	376	26	27
2020	1,855	58	63

年を追うごとに多くの脆弱性が悪用されるようになっている

Device Category	URLhaus	Honeypot	Genealogy	Total
Router	461	1,342	610	2,413
Home security	93	219	78	390
Web application	36	38	32	106
Web server	22	10	-	32
TV	7	2	-	9
NAS	27	27	-	54
Total	646	1,638	729	3,004

- **狙われる脆弱性の8割はルータ**

推測が難しいパスワードによるアクセス制御だけでなく、脆弱性対策を行わないと機器の感染を防ぐことは困難

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

IoTマルウェア内部から発見された脆弱性攻撃機能一覧

●:All datasets
◐: two datasets
○:one dataset

Type	Vulnerability	Vuln. Published	Exploit Published	Families	Manufacturer	Target Device	U	H	G	# of Samples
RCE	CVE-2009-0545; CVE-2019-12725 *	2009-02-12; 2019-06-04	2009-02-09	Mirai	Zeroshell	Zeroshell Linux Distribution	○			2
	Netgear DGN1000 RCE	2013-06-05	2013-06-05	Mirai, Mozi, Gafgyt	Netgear	DGN1000 Netgear routers	●	●	●	107
	Linksys E-series RCE	2013-07-02	2014-02-16	Mirai, Gafgyt	Cisco	Linksys routers E-series	◐	◐		150
	Edimax EW-7438RPn-v3 RCE	2015-07-17	2015-07-17	Mirai	Edimax	EW-7438RPn-v3	○			4
	Multi-vendor CCTV/DVR RCE	2016-03-23	2016-03-23	Mirai, Mozi, Gafgyt	Multi-vendor	Multi-vendor CCTV/DVR	●	●	●	79
	NUUO NVRmini RCE	2016-08-06	2016-08-06	Mirai	NUUO	NUUO NVR	◐	◐		4
	Xfinity Gateway RCE	2016-12-02	2016-12-02	Mirai	Xfinit	Xfinity Gateway	○			3
	CVE-2017-(8221-8225) *	2017-04-25	2017-03-08	Mirai	GoAhead	GoAhead IPcam	○			3
	EnGenius IoT GCS1.4.11 RCE	2017-06-04	2017-06-04	Mirai	EnGenius	EnGenius IoT Cloud Service	◐	◐		3
	CVE-2017-14135	2017-09-04	2017-07-03	Mirai	Dream Property	Opendreambox	○			1
	CVE-2017-14127; CVE-2019-18396 *	2017-09-04; 2019-10-24	2019-11-13	Mirai	Technicolor	Technicolor TD5336	◐	◐		5
	Vacron NVR RCE	2017-10-22	2017-10-08	Mirai, Mozi	Vacron	Vacron NVR devices	●	●	●	26
	Shenzhen_TVT RCE	2018-04-03	2018-04-09	Mirai	Shenzhen TVT	Shenzhen TVT DVR/NVR/IPC	○			3
	CVE-2018-10561; CVE-2018-10562 *	2018-04-30	2018-05-03	Mirai, Mozi, Gafgyt	Dasan	GPON Home Routers	●	●	●	259
	CVE-2018-11510	2018-05-28	2018-08-15	Mirai	ASUSTOR	ASUSTOR NAS		○		1
	HomeMatic Zentrale CCU2 RCE	2018-07-18	2018-07-18	Mirai	HomeMatic	HomeMatic Zentrale CCU2	○			3
	CVE-2018-15887	2018-08-26	2018-08-02	Gafgyt	ASUS	ASUS DSL-N12E_C1		○		6
	CVE-2018-17173	2018-09-18	2019-05-06	Mirai	LG	LG Supersign EZ CMS TV	◐	◐		9
	CVE-2018-20062; CVE-2019-9082 *	2018-12-11; 2019-02-24	2019-01-14; 2020-04-16	Mirai, Singletons	ThinkPHP	v-5.0.23/5.1.31 Server	◐	◐		21
	CVE-2019-2725	2018-12-14	2019-05-08	Mirai	Oracle	Oracle WebLogic Server		○		1
	CVE-2019-7276	2019-01-31	2019-11-12	Mirai	Optergy	Optergy 2.3.0a	○			3
	CVE-2019-10655	2019-03-30	2019-03-31	Mirai	Grandstream	GAC2500; GVC3202; GXV3275-40; GXP2200 *	○			3
	CVE-2018-20841	2019-06-11	2019-01-14	Mirai	HooToo					
	Sar2HTML 3.2.1 RCE	2019-08-02	2019-08-02	Mirai	Sar2HTML					
	CVE-2020-9054	2020-02-18	2020-02-24	Mirai	Zyxel					
	Netlink GPON Router 1.0.11 RCE	2020-03-18	2020-03-18	Mirai	Netlink GPON					
	Symantec SWG 5.0.2.8 RCE	2020-04-09	2020-04-09	Mirai	Symantec	Symantec Web Gateway 5.0.2.8	◐	◐		34
	Netgear R7000 RCE	2020-06-15	2020-06-15	Mirai	Netgea	Netgear R7000	○			7
	CVE-2019-16759; CVE-2020-17496 *	2019-09-24; 2020-08-12	2020-08-12	Mirai	vBulletin 5.x	Servers using vBulletin 5.x	○			2
Backdoor	CVE-2014-2321	2014-03-10	2014-03-03	Tsunami	ZTE	ZTE F460 and F660		○		2
	Xiaongmai-based DVR/NVR/IPcam	2020-02-04	2020-02-04	Mirai, Gafgyt	Multi-vendor	DVR/NVR/IPcams		○		31

'*' indicates that this entry consists of vulnerabilities that are targeted by the same exploit code or vice versa

様々な機器の脆弱性を狙う攻撃機能がマルウェア内部から発見

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

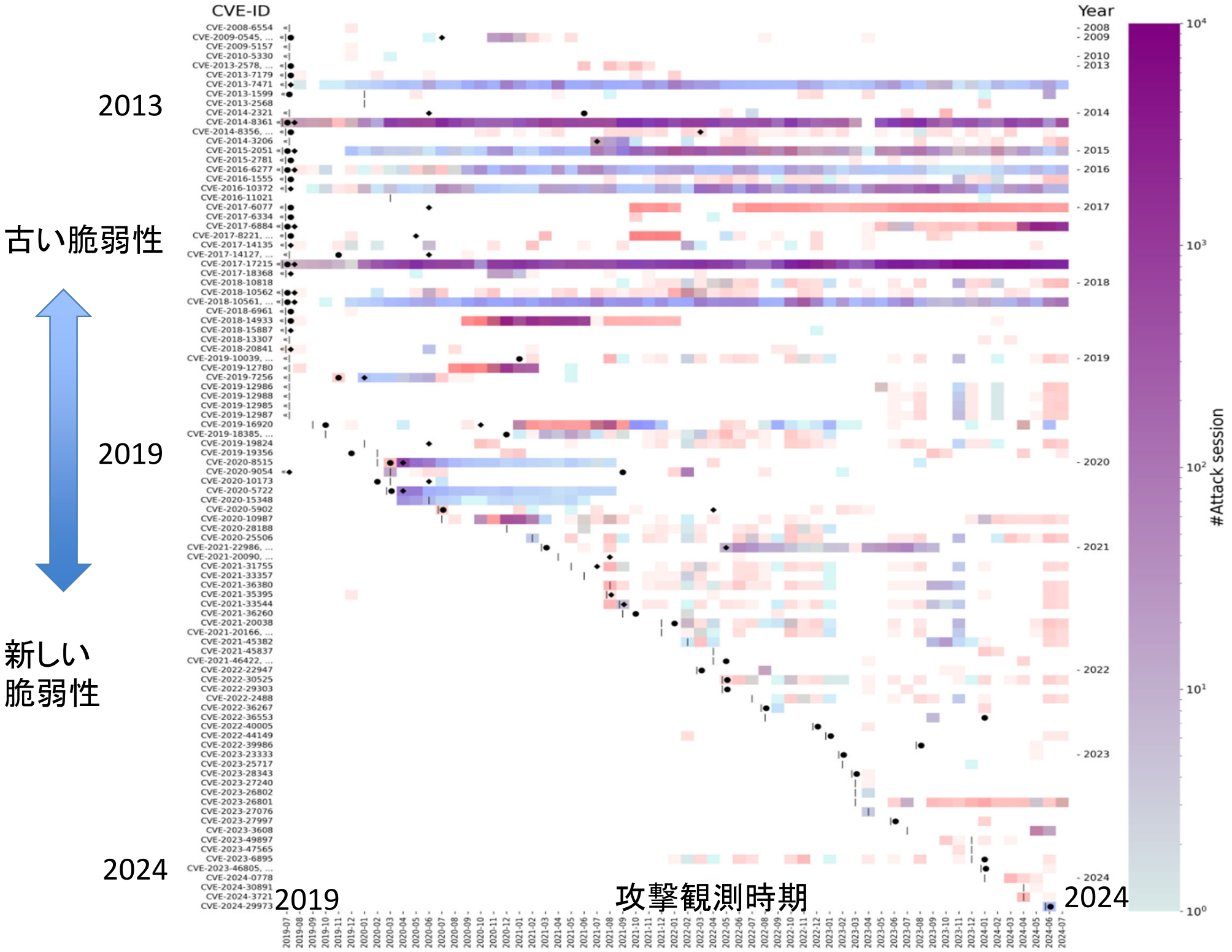
IoTマルウェア内部から発見された脆弱性攻撃機能一覧

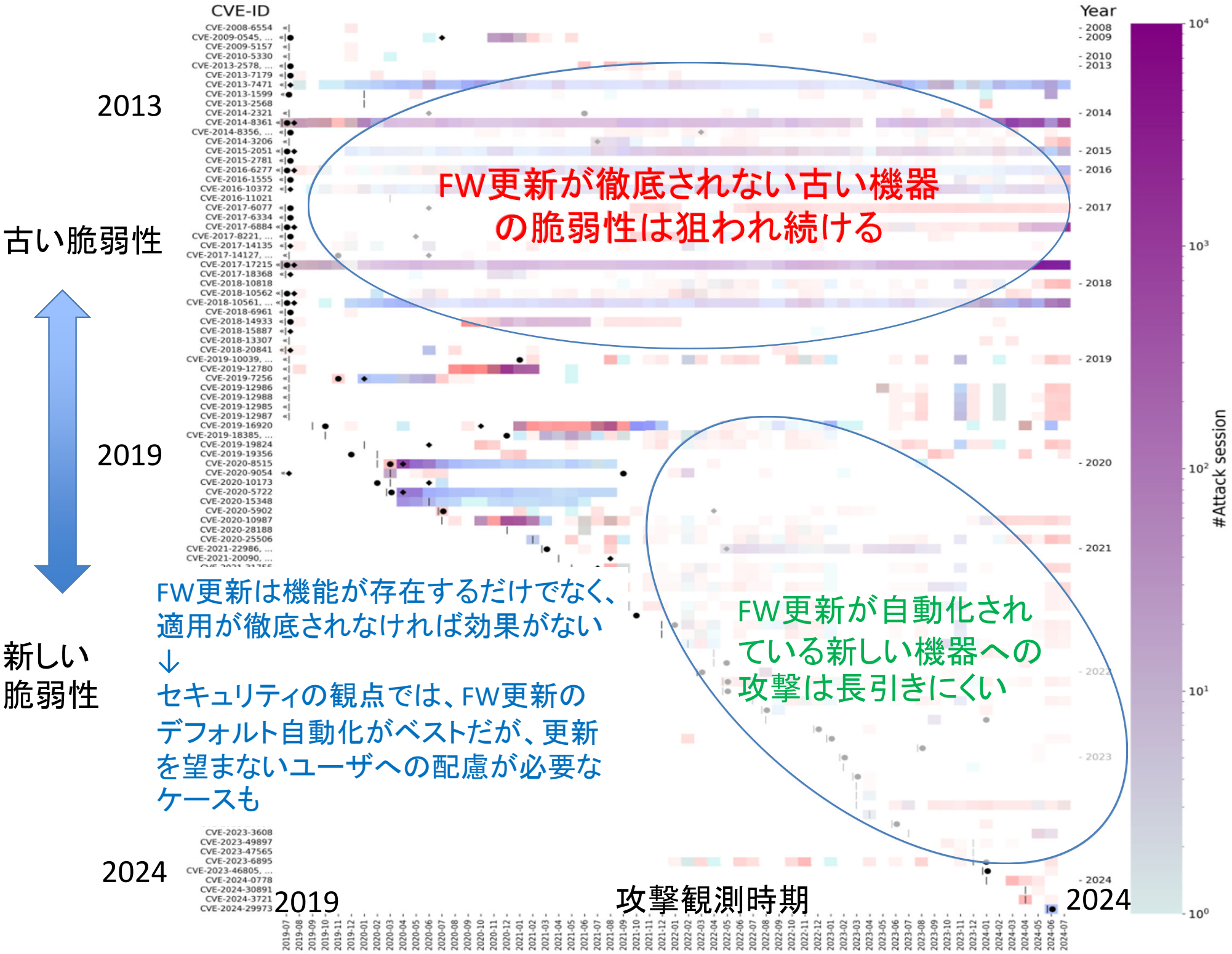
●:All datasets
◐: two datasets
○:one dataset

Type	Vulnerability	Vuln. Published	Exploit Published	Families	Manufacturer	Target Device	U	H	G	# of Samples
CMDi	CVE-2014-8361 *	2014-10-20	2015-06-01	Mirai, Mozi, Gafgyt	D-Link	D-Link Routers using Realtek SDK	●	●	●	272
	CVE-2014-9094	2014-11-26	2014-07-13	Mirai	WordPress	WordPress Plugin DZS-VideoGallery	◐		◐	35
	CVE-2015-2051	2015-02-23	2015-06-01	Mirai, Mozi, Gafgyt	D-Link	D-Link DIR-645	●	●	●	93
	AVTECH IPCam/NVR/DVR CMDi	2016-10-11	2016-10-11	Mirai	AVTECH	AVTECH IPcam/NVR/DVR	◐	◐		69
	CVE-2016-10372	2016-05-16	2016-11-08	Mirai, Mozi, Gafgyt	Zyxel	Eir D1000 Router (rebranded Zyxel)	◐	◐		78
	CVE-2016-6277	2016-07-22	2017-03-13	Mirai, Mozi, Gafgyt	Netgear	Netgear R7000 and R6400	●	●	●	41
	NUUO OS CMDi	2016-08-06	2016-08-06	Mirai	NUUO	NUUO NVRmini 2 3.0.8	○			3
	MV Power Shell CMDi	2017-02-27	2017-02-27	Mirai, Mozi	MV Power	MVPower DVR TV-7104HE 1.8.4	◐	◐		168
	CVE-2017-6884	2017-03-14	2017-04-02	Mirai	Zyxel	EMG2926 Router	◐		◐	39
	CVE-2017-18368	2019-05-02	2016-12-26	Mirai, Singletons, Gafgyt	Zyxel	Zyxel P660HN-T routers	◐	◐		77
	CVE-2017-17215	2017-12-04	2017-12-25	Mirai, Mozi, Gafgyt, Singleton	Huawei	Huawei home routers HG532	●	●	●	921
	CVE-2018-7841	2018-03-08	2019-05-14	Mirai	U.motion	U.motion software v.1.3.4	○			4
	D-Link DSL-2750B OS CMDi	2018-05-25	2018-05-25	Mirai	D-Link	D-Link DSL-2750B	●	●	●	241
	SonicWall GMS-XMLRPC CMDi	2018-08-01	2018-08-01	Mirai	SonicWall	SonicWall GMS		◐	◐	1
	CVE-2018-19276	2018-11-14	2019-12-18	Mirai	OpenMRS	OpenMRS before 2.24.0	◐	◐		5
	CVE-2019-7256	2019-01-31	2019-11-12	Mirai	Linear	Linear eMarge E3 series		○		1
	CVE-2019-12489	2019-05-30	2019-11-13	Mirai	Fastweb	Fastweb Fastgate 0.00.81	○			3
	CVE-2013-7471	2019-06-11	2013-09-17	Mirai, Mozi, Gafgyt	D-Link	D-Link DIR-645	●	●	●	29
	CVE-2019-14931	2019-08-10	2019-08-13	Mirai	Mitsubishi	Mitsubishi smartRTU& INEA ME-RTU	○			7
	CVE-2020-1956	2019-12-02	2020-06-20	Mirai	Apache	Apache Kylin 2.3.0-2.6.5,3.0.1	○			4
	CVE-2019-19824	2019-12-16	2015-07-16	Mirai	TOTOLINK	TOTOLINK Realtek SDK routers	○			7
	CVE-2020-5722	2020-01-06	2020-03-24	Mirai	Grandstream	Grandstream UCM6200 series	◐	◐		5
	CVE-2020-7209	2020-01-16	2020-05-17	Mirai	HP LinuxKI	HP LinuxKI-v6.01	○			3
	CVE-2020-10173	2020-03-05	2020-02-27	Mirai	Comtrend	Comtrend VR-3033	◐	◐		5
	CVE-2020-13786	2020-06-03	2020-06-12	Mirai	D-Link	D-Link DIR-865L Ax1.20B01	○			7
Buffer OF	CVE-2016-4429	2016-05-02	2016-05-18	Singletons	Qualcomm	Qualcomm Server	○			5
	CVE-2019-7405	2019-02-05	2019-12-16	Mirai	TP-Link	TP-Link Archer C5-v4 routers		○		4
WAF Bypass	Cloudflare WAF Bypass	2017-04-04	2016-10-25	Mirai, Gafgyt	CloudFlare	CloudFlare WAF	◐		◐	37
Brute Force	Dictionary Attack	-	-	Mirai, Mozi, Singleton, Tsunami, Gafgyt, xorddos	-	-	●	●	●	5,631
Total							59	41	16	

'*' indicates that this entry consists of vulnerabilities that are targeted by the same exploit code or vice versa

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.


CVE-ID
Year
2013
古い脆弱性
2019
新しい
脆弱性
2024
2019
攻撃観測時期
2024
#Attack session


CVE-ID
Year
#Attack session
2013
古い脆弱性
2019
新しい
脆弱性
2024
FW更新が徹底されない古い機器
の脆弱性は狙われ続ける
FW更新は機能が存在するだけでなく、
適用が徹底されなければ効果がない
↓
セキュリティの観点では、FW更新の
デフォルト自動化がベストだが、更新
を望まないユーザへの配慮が必要な
ケースも
FW更新が自動化され
ている新しい機器への
攻撃は長引きにくい
2019
攻撃観測時期
2024

JC-STAR★1では

脅威に対抗するために★1で実現すべき対策

IPA

★1で考慮すべき主な4つの脅威に対し、★1の位置付けや海外制度の基準等を踏まえ、製品／製品ベンダにおいて実現すべき対策を以下のとおり選定

★1で考慮すべき主な脅威			脅威に対抗するために★1で実現すべき対策			
			製品における対策		製品ベンダにおける対策	
			カテゴリ	対策	カテゴリ	対策
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	• 容易に推測できるパスワードが設定できない仕組みを導入する • セキュアな認証の仕組みを提供する • ブルートフォースによる認証試行を防ぐ仕組みを提供する	情報提供	• セキュアな利用方法に関する情報を提供する
	②脆弱性の放置により、		脆弱性対策、ソフトウェアの更新	• 深刻度の高い既知の脆弱性及び主要なCWEに対する対策を行う • ソフトウェアコンポーネントがアップデート可能な仕組みを導入する	情報・問い合わせの受付、情報提供	• 製品に関する情報及び脆弱性に関する情報を提供する • セキュリティパッチの適用方法に関する情報を提供する
	③未使用インタフェースの有効化により、		インターフ…への…	• 不要なインタフェースを無効化する	―	―
				…情報を保護するための機能を提…共通する対策）	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威				…送される守るべき情報を保護する…変更に対する保護対策を実装する	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	• 機器の利用中に機器内に保存された守るべき情報を製品本体や関連サービスを介して削除できる機能を提供する • 機器に当初から搭載されている守るべき情報を保護するための機能を提供する	情報提供	• セキュアな廃棄方法に関する情報を提供する
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンスの向上	• ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源OFF前の状態を提供する	―	―

脆弱性対策とソフトウェア更新を明記.
容易かつ分かりやすいアップデート手順
に関する基準が存在

JC-STAR説明会(24.11.28/12.2/12.6)

©2024 独立行政法人情報処理推進機構(IPA)

JC-STAR説明会（2024.11.28/12.2/12.6、独立行政法人情報処理推進機構（IPA）　）より

横浜国立大学　大学院環境情報研究院/先端科学高等研究院
吉岡克成，yoshioka@ynu.ac.jp
http://yoshioka.ynu.ac.jp

謝辞1：本研究は総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「電波の有効利用のためのIoTマルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含みます。
謝辞2: 本研究は国立研究開発法人情報通信研究機構委託研究革新的情報通信技術研究開発委託研究（採択番号:05201）によって実施された成果を含みます。
謝辞3：本研究は、国立研究開発法人情報通信研究機構（NICT）の委託研究（JPJ012368C08101）により得られた成果を含みます。