SYNOPSYS®
Silicon to Software™

JNSA標準化部会ビギナーズセミナー 「IoTセキュリティ標準化の動向を知る」

松岡正人@日本シノプシス合同会社
IoT セキュリティWG リーダー

IoTセキュリティWGについて

活動履歴

- コンシューマ向けIoT セキュリティガイド
  - https://www.jnsa.org/result/iot/2016.html
- IoTセキュリティセミナー
  - 2016/10/26
    IoTの未来とセキュリティの課題
  - 2017/3/1
    IoTセキュリティワークショップ
  - 2018/2/26
    IoT機器を守るために何を学ばなければならないか？
  - 2019/2/1
    Society5.0で実現する社会におけるIoTとAI、そしてセキュリティはどうなるか？
  - 2019/12/20
    IoTとAIが当たり前になる時代のセキュリティはどうなるのか？
- IoTセキュリティガイド 標準／ガイドライン ハンドブック　2017年度版
  - https://www.jnsa.org/result/iot/2018.html
- IoTセキュリティチェックリスト（JPCERT/CC）
  - https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

現在は、IoTの開発者を招いた勉強会や欧米の関連規制の情報収集や分析など、オンラインで活動中

※活動を牽引してくれるメンバー絶賛募集中

IoT Security WG Report 2016

はじめに

近い将来、多数のIoT製品が相互に接続され通信しあって生活や社会のインフラとして機能するようになります。そして、従来のITでは実現できなかった、個人の行動や状況にあわせたきめ細かい情報処理と最適制御が実現します。

それにともなって、セキュリティはIoTの重要な要素となります。しかし現状では、セキュリティの実現と実践を一般の利用者に任せるのは困難です。このため、IoT製品やシステム、サービスを提供する事業者の側が利用者のセキュリティ対策を設計時から作り込み、利用者に情報提供する必要があります。

このようなIoTセキュリティの課題を踏まえ、2014年に本WGは活動を開始しました。コンポーネントベンダーやシステムインテグレータ、サービス提供事業者などを交えて情報収集や議論を行った上で、IoTに関連するさまざまな仕様や規格、技術ドキュメント類を俯瞰し、それらをどのように整理するべきかを議論しました。そして、実際のIoTの利用形態を分析し、IoT利用者を守るためにIoT製品やシステム、サービスを提供する事業者が考慮しなければならない事柄を「コンシューマ向けIoT　セキュリティガイド」としてまとめました。

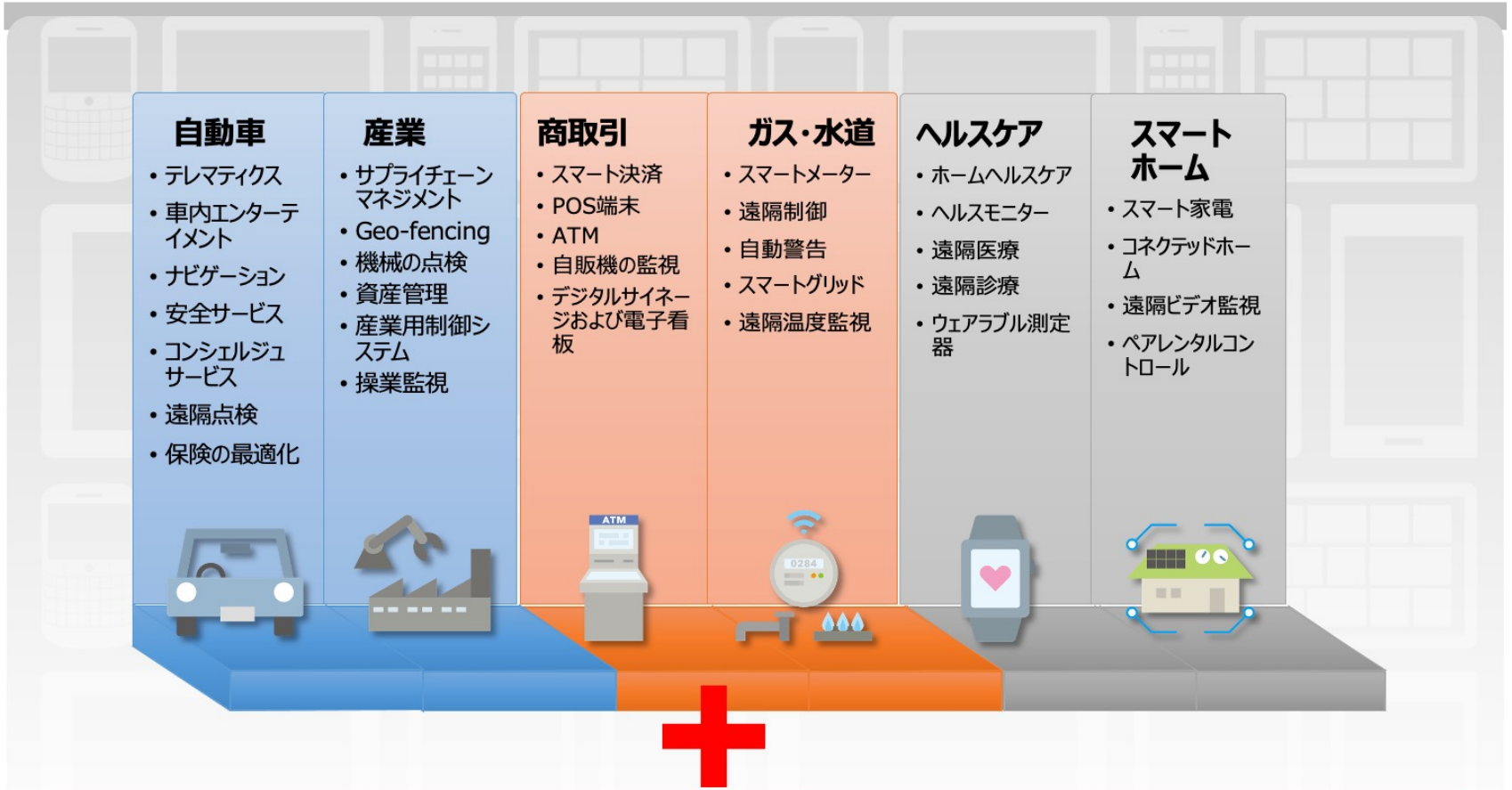
このガイドがIoTのセキュリティ向上の一助となれば幸いです。

IoT Security WG メンバー一同

インフラ/産業から個人へ

*Internetにつながる機器はより身近に

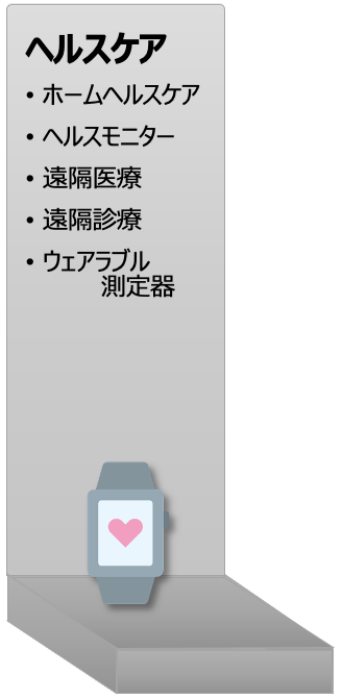
JNSA



個人用マイコンボード(RaspberryPi など)、ネットワーク玩具 など

消費者向けと企業向け

- 代表的な区分として、これら六つの分野を挙げるが、各分野ごとに提供されるサービスや商品によって「消費者向け」のものと「企業向け（あるいは事業者、自治体などの組織）」の二つがある
- ヘルスケアであればウェアラブル端末（個人が身につけて利用するもの）は「消費者向け」であるが、自治体や特定の医療機関が住民や患者に対して提供し、健康状態を遠隔で把握するためのウェアラブル端末（たとえば携帯型の心電記録装置）は個人が使用するものの、その所有者や目的からは「病院・自治体向け」というのが適切である
- 心電記録装置であれば病院によって提供される遠隔診断というサービス、健康促進やライフログの記録が目的であれば活動量の記録サービスを利用するためにウェアラブル機器を利用することになる



JPCERT/CCによるIoTセキュリティチェックリスト

セキュリティの専門家でなくても必要な機能をチェックできる虎の巻

- JPCERT/CC では、IoT システム/IoT デバイスの開発者がチェックすべきことと、利用者がチェックすべきことをまとめた IoT セキュリティチェックリストを作成、安全に運用するために実装しておきたい 39 のセキュリティの機能をそれが必要な背景とともに一覧表を提供
- 本チェックリストを使うことで、 IoT システムのセキュリティを担保する上で必要な機能が備わっているかどうかの判断と更なる検討項目の洗い出しを手早く行う事が出来る
- チェックリストは、用途に応じてカスタマイズをしてご利用いただけるよう、Excelファイルも提供

https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

IoTの課題

規制と現実

GDPR規制とIoT（ネットワーク化された機器）

IoT化された機器が増えることで個人情報やデータ漏洩のリスクは増大している

- GDPRは機器に対するセキュリティ対策を規定していないが、個人情報取扱規程に準ずる必要がある
- Global Privacy Enforcement Networkの調査では300台以上の機器から以下の課題が見つかった（2016年）
  - 59% は個人情報の取得、使用、開示の説明が不適当
  - 68% はデータ格納の説明が不適当
  - 72% はデータの消去方法の説明が不適当
  - 38% はプライバシーの懸念についての問い合わせ先が示されていない
- 違反した場合の制裁金
  - 1000 万ユーロ以下、または、 直前の会計年度の全世界の売上総額の2%以下の金額のいずれか高額の方
  - https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

https://eugdprcompliant.com/internet-of-things-era-of-gdpr/

EUによる製品開発品質にまで踏み込んだ規制

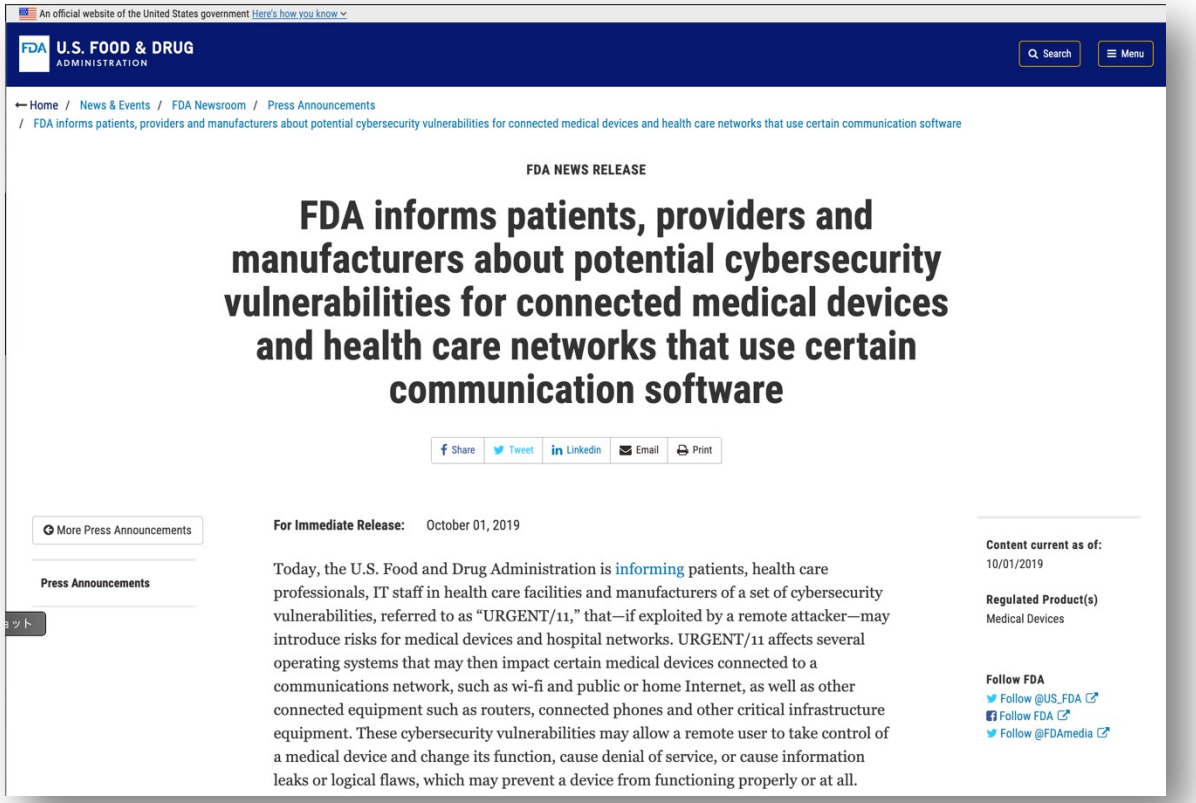
メーカーがソフトとハードのセキュリティを担保するための取り組みを推進

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

- 2022/9/15に公開された「Cyber Resilience Act」法案
- 製造業者が、設計および開発段階からライフサイクル全体を通じて、デジタル要素を備えた製品のセキュリティ向上を保証
- 一貫したサイバーセキュリティ フレームワークの確保と、ハードウェアおよびソフトウェア メーカーのコンプライアンスを促進
- 企業や消費者がデジタル要素を備えた製品を安全に使用できるように

URGENT/11

医療機器にも大きな影響、FDA（米国食品医薬品局）が警告



An official website of the United States government Here's how you know

U.S. FOOD & DRUG ADMINISTRATION

Search Menu

Home / News & Events / FDA Newsroom / Press Announcements

/ FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software

FDA NEWS RELEASE

FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software

Share Tweet LinkedIn Email Print

More Press Announcements

Press Announcements

For Immediate Release: October 01, 2019

Today, the U.S. Food and Drug Administration is informing patients, health care professionals, IT staff in health care facilities and manufacturers of a set of cybersecurity vulnerabilities, referred to as "URGENT/11," that—if exploited by a remote attacker—may introduce risks for medical devices and hospital networks. URGENT/11 affects several operating systems that may then impact certain medical devices connected to a communications network, such as wi-fi and public or home Internet, as well as other connected equipment such as routers, connected phones and other critical infrastructure equipment. These cybersecurity vulnerabilities may allow a remote user to take control of a medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent a device from functioning properly or at all.

Content current as of:
10/01/2019

Regulated Product(s)
Medical Devices

Follow FDA
Follow @US_FDA
Follow FDA
Follow @FDAmedia

- 影響のあった組み込みOS
  - VxWorks (by Wind River)
  - Operating System Embedded (OSE) (by ENEA)
  - INTEGRITY (by GreenHills)
  - ThreadX (by Microsoft)
  - ITRON (by TRON)
  - ZebOS (by IP Infusion)
- CVE一覧
  - CVE-2019-12256、CVE-2019-12255、CVE-2019-12260、CVE-2019-12261、CVE-2019-12263、CVE-2019-12257
  - CVE-2019-12258、CVE-2019-12262、CVE-2019-12264、 CVE-2019-12259、CVE-2019-12265

https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities

AMNESIA:33

米国Forescout社が発見したTCP/IPスタックの複数の脆弱性

公開日：2020/12/09　最終更新日：2021/01/22

JVNVU#96491057
複数の組み込み TCP/IP スタックにメモリ管理の不備に起因する複数の脆弱性

概要
複数の組み込み TCP/IP スタックの実装に、メモリ管理の不備に起因する複数の脆弱性が発見されました。これら一連の脆弱性は「AMNESIA:33」と呼称されています。

影響を受けるシステム
組み込み TCP/IP スタックとして以下を使用している製品

- uIP Version 1.0 およびそれ以前
  - uIP は開発が終了しています
- Contiki-OS (uIP) Version 3.0 およびそれ以前
  - Contiki-OS は開発が終了しています
- Contiki-NG (uIP) Version 4.5 およびそれ以前
- picoTCP Version 1.7.0 およびそれ以前
  - picoTCP は開発が終了しています
- picoTCP-NG Version 2.0.0 およびそれ以前
- FNET Version 4.6.3
- Nut/Net Version 5.1 およびそれ以前

詳細情報
リアルタイム OS や IoT 製品をはじめとした多くの製品で使用されている複数の組み込み TCP/IP スタックで、メモリ管理の不備に起因する複数の脆弱性が発見されました。
脆弱性の深刻度や影響範囲は製品によって異なります。詳細については、一連の脆弱性を発見した Forescout が提供する情報を

- 想定される影響
  - 遠隔の第三者によって、サービス運用妨害 (DoS) や任意のコードの実行が行われたり、機微な情報が漏えいしたりする可能性がある
- 対象となるシステムやソフトウェア
  - リアルタイム OS や IoT 製品をはじめとした多くの製品で使用されている複数の組み込み TCP/IP スタックで、メモリ管理の不備に起因する複数の脆弱性
  - 詳細については、一連の脆弱性を発見した Forescout が提供する情報を確認が必要
  - 本脆弱性の検出ツールも公開されている

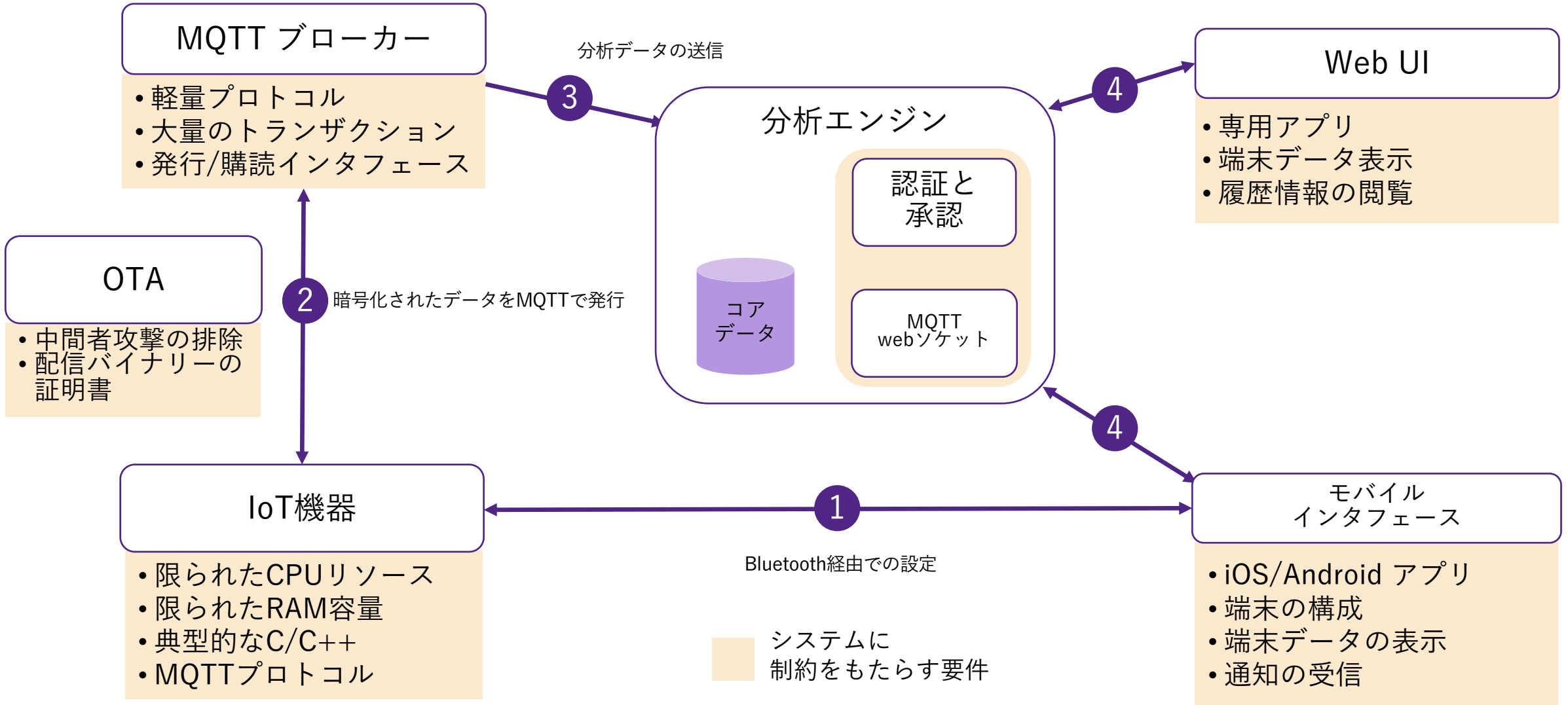
https://jvn.jp/vu/JVNVU96491057/

IoTシステム全体のセキュリティを考える

どのように強固なセキュリティにもリスクはつきもの
ラズパイのような機器は手軽で便利ですが
使い方を間違うのは「人」の問題？

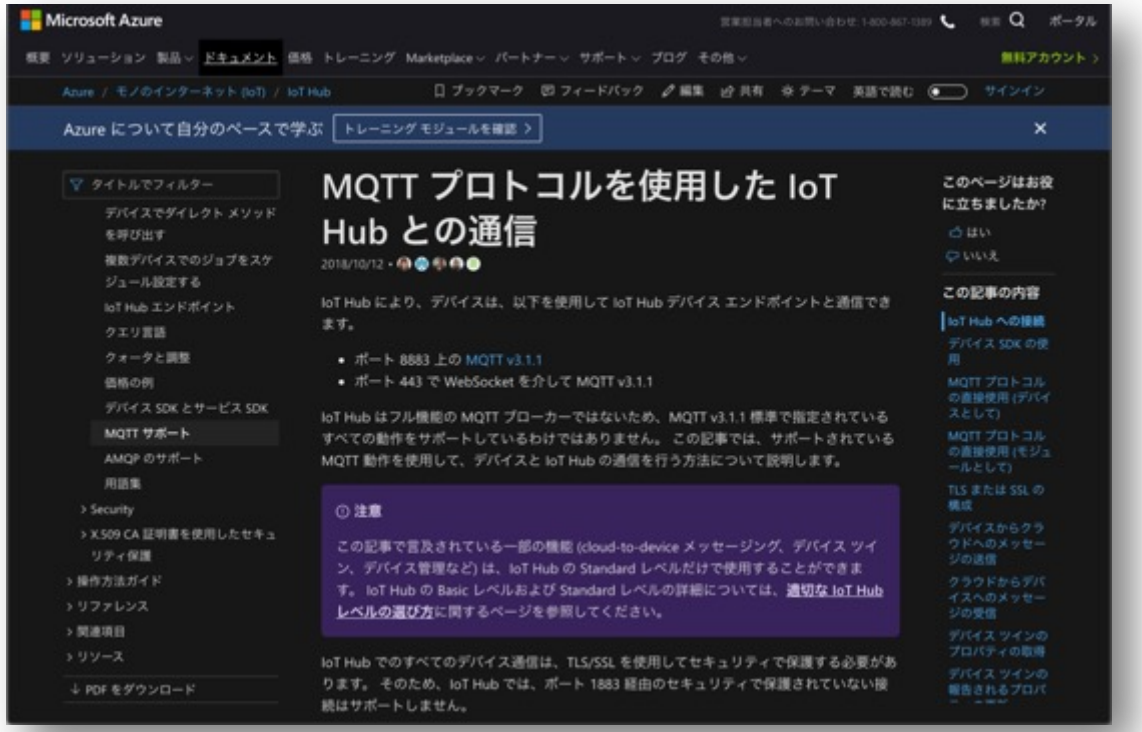
現代のアプリケーションは構成が非常に複雑

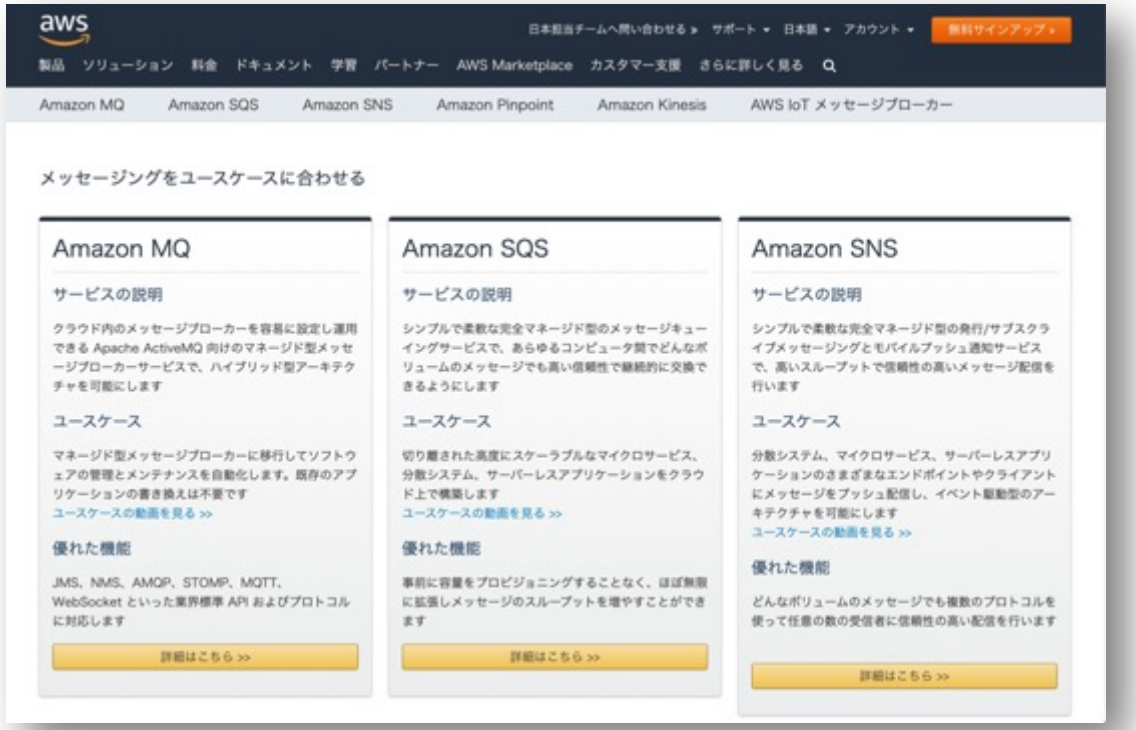
ありがちなIoTシステムの例



たとえば、MQTTはどんなところで使われているか？

Azure IoT HUB, Amazon MQなどの各種デバイス接続サービス



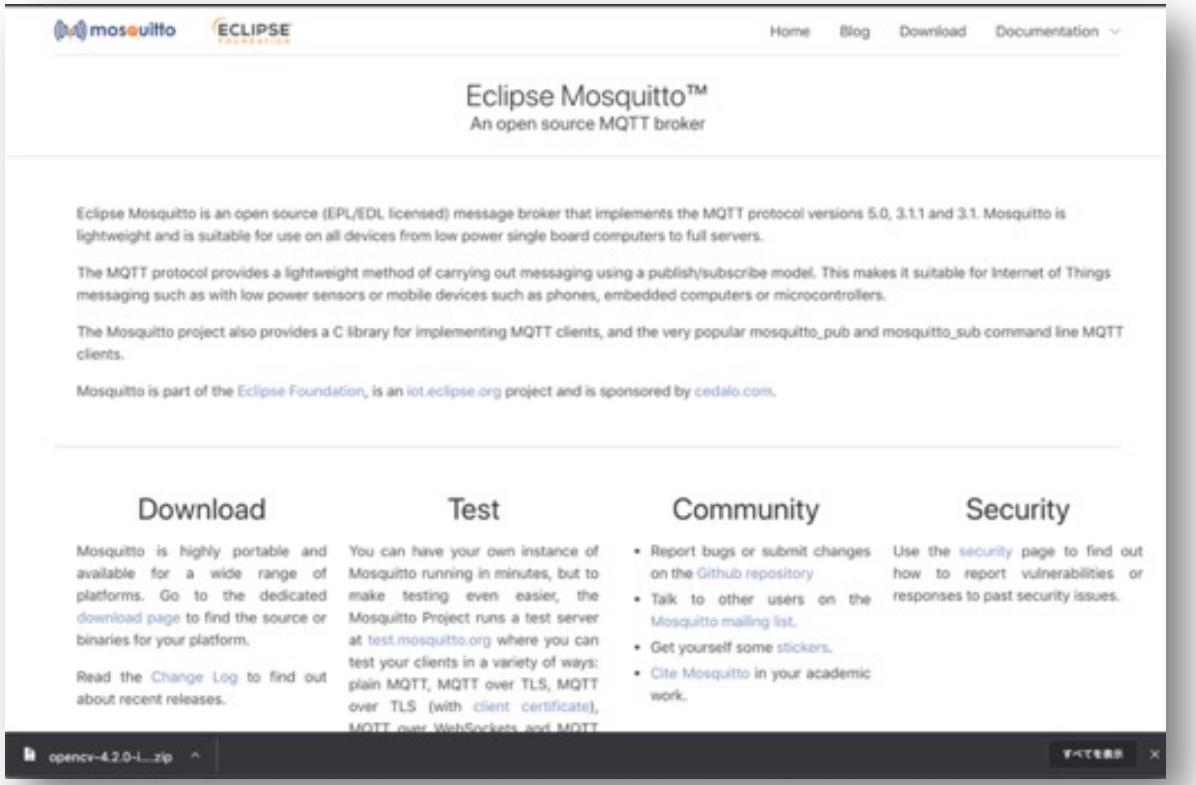


https://docs.microsoft.com/ja-jp/azure/iot-hub/iot-hub-mqtt-support

https://aws.amazon.com/jp/messaging/

Mosquitto (MQTT)

MosquittoはオープンソースのMQTTのライブラリ

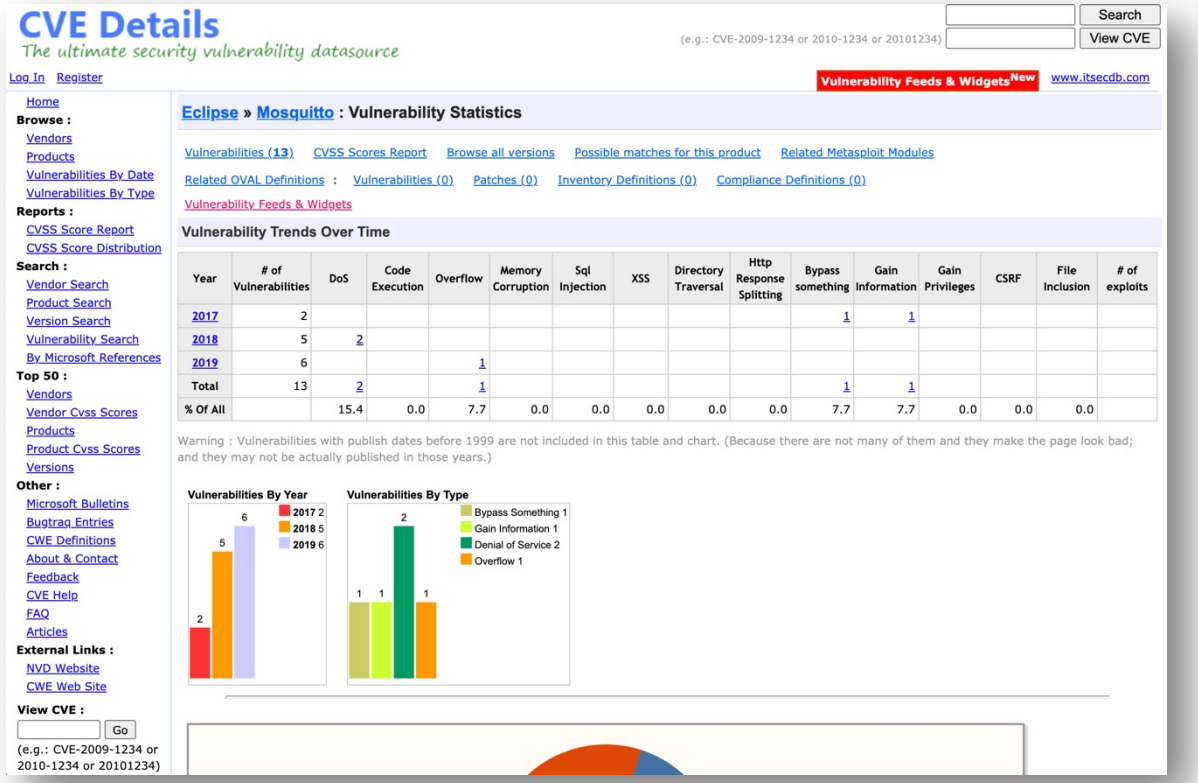


- MQTT:Message Queue Telemetry TransportはIBMが開発したTCP/IPベースの非同期通信プロトコル
- 当初は油田のパイプラインに設置されたセンサーとホストとの通信を衛星回線で実現するために開発された
- 2014年にOASISにより標準化
- IoT機器とサーバーとの通信に多く利用されている
- メッセージはパブリシャーとサブスクライバーとの間で行われ、TLSによる暗号化も可能

https://mosquitto.org/

Mosquittoの既知の脆弱性をCVEデータベースで確認

主な脆弱性とバージョン



CVE Details
The ultimate security vulnerability datasource

Search
View CVE
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register
Vulnerability Feeds & Widgets New
www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Eclipse » Mosquitto : Vulnerability Statistics

Vulnerabilities (13) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (0) Patches (0) Inventory Definitions (0) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2017	2									1	1				
2018	5	2													
2019	6			1											
Total	13	2		1						1	1				
% Of All		15.4	0.0	7.7	0.0	0.0	0.0	0.0	0.0	7.7	7.7	0.0	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year
2017 2
2018 5
2019 6

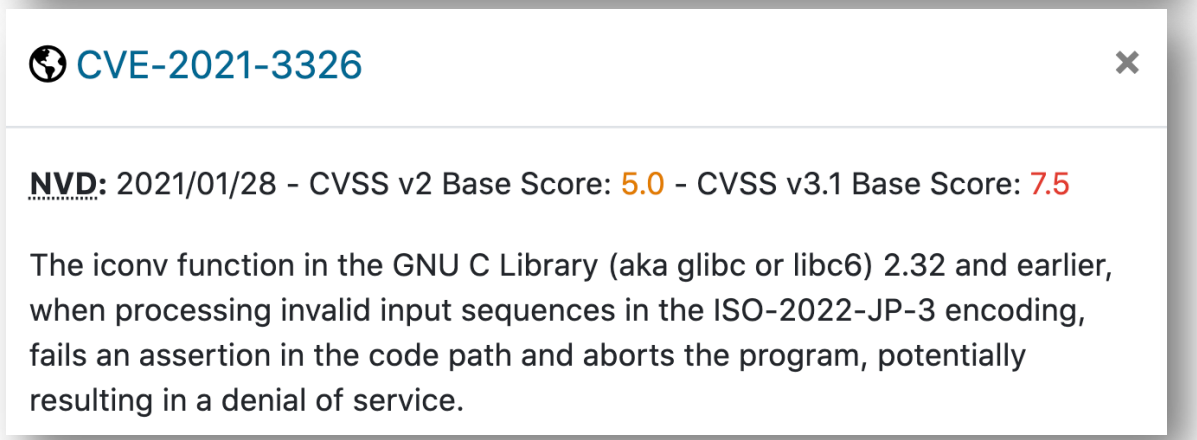
Vulnerabilities By Type
Bypass Something 1
Gain Information 1
Denial of Service 2
Overflow 1

- CVE-2017-7654
  - 1.4.15以前のバージョンでDoSの脆弱性
- CVE-2019-11779
  - 1.5～1.6.5のバージョンではスタック・オーバーフローの脆弱性
- 最新版は2.0

https://www.cvedetails.com/product/45945/Eclipse-Mosquitto.html?vendor_id=10410

そもそもラズパイのOSには脆弱性がある

2021-01-11-raspios-buster-armhf-lite.zip

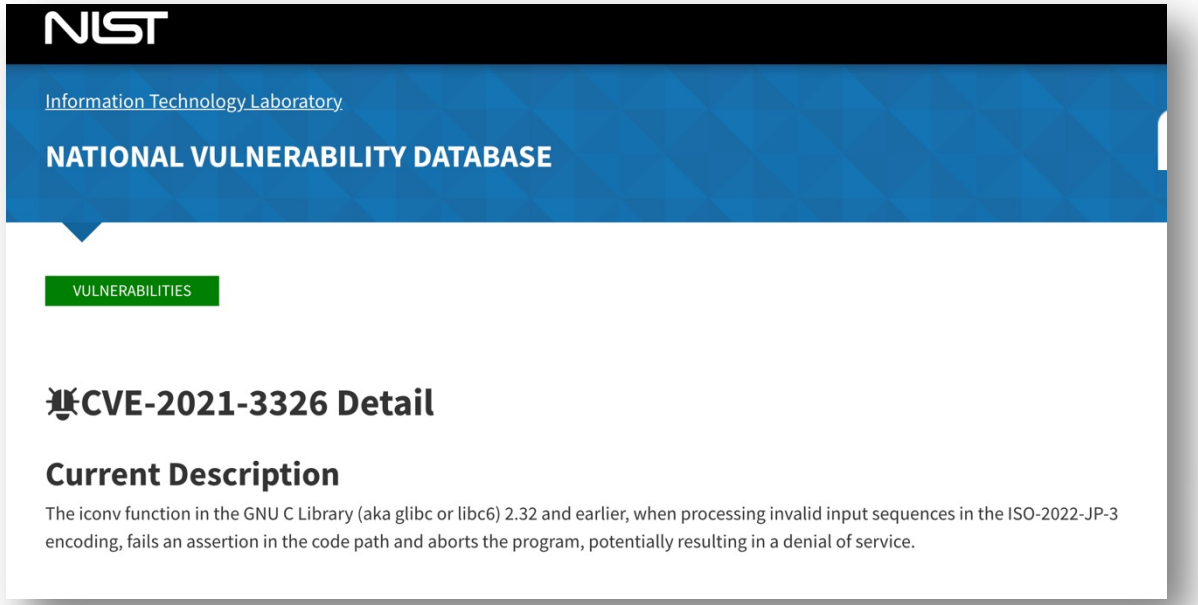


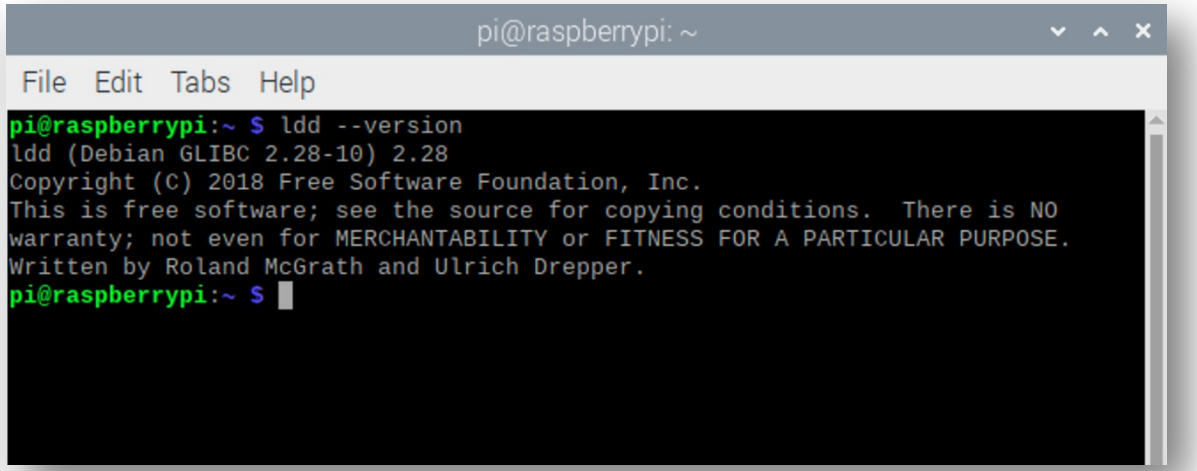
- Raspberry pi OSをスキャンしてみる https://www.raspberrypi.org/software/operating-systems/#raspberry-pi-os-32-bit
- Raspberry Pi OS Lite
  - Release date: January 11th 2021
  - Kernel version: 5.4
- 脆弱なコンポーネント数：411
- 脆弱性「高」：268
- 新しい脆弱性、CVE-2021-3326も含まれていることがわかる

CVE-2021-3326 “日本語処理の脆弱性”

サービス拒否へ陥るおそれ

- 「GNU C Library 2.32」および以前のバージョンに、関数「iconv」で「ISO-2022-JP-3」の処理を失敗してプログラムが中断し、サービス拒否へ陥るおそれがある脆弱性
- Raspberry Piのターミナル上にて”ldd --version”コマンドで確認すると、“glibc 2.28”となっており「 CVE-2021-3326 」の対象であることが確認できる





https://nvd.nist.gov/vuln/detail/CVE-2021-3326

Raspberry Piによるデータ漏洩事例（2018年）

NASA、ジェット推進研究所の定期監査レポートより

ZDNet Japan　海外発　デジタル変革　CIO　ITインフラ　セキュリティ　クライ

ZDNet Japan › セキュリティ

NASAが2018年にハッキング被害で情報流出--無許可で接続された「Raspberry Pi」標的

Catalin Cimpanu（Special to ZDNet.com）翻訳校正：編集部　2019-06-24 11:44

シェア 141　ツイート　B! 3　noteで書く　Pocket 22

PR　企業ITのあるべき姿"DXのためのセキュリティ"とは何か

PR　導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載

米航空宇宙局（NASA）の監察総監室（OIG）が先週発表した報告書によると、2018年4月にハッカーがNASAのネットワークに侵入し、火星探査ミッションに関連する約500MBのデータを盗んだという。

- 事象
  - 2018年4月に500MBのデータが盗まれたことが発覚
  - さらに、宇宙船やIISとの通信用ネットワークの「DSN」に侵入された
  - そのため、IISなどを DSNから切断しなくてはならなかった
- 原因
  - 2018年4月のサイバー攻撃の原因は「未承認のラズパイ」が研究所のネットワークに繋がっており、容易にアクセス権を奪われたため

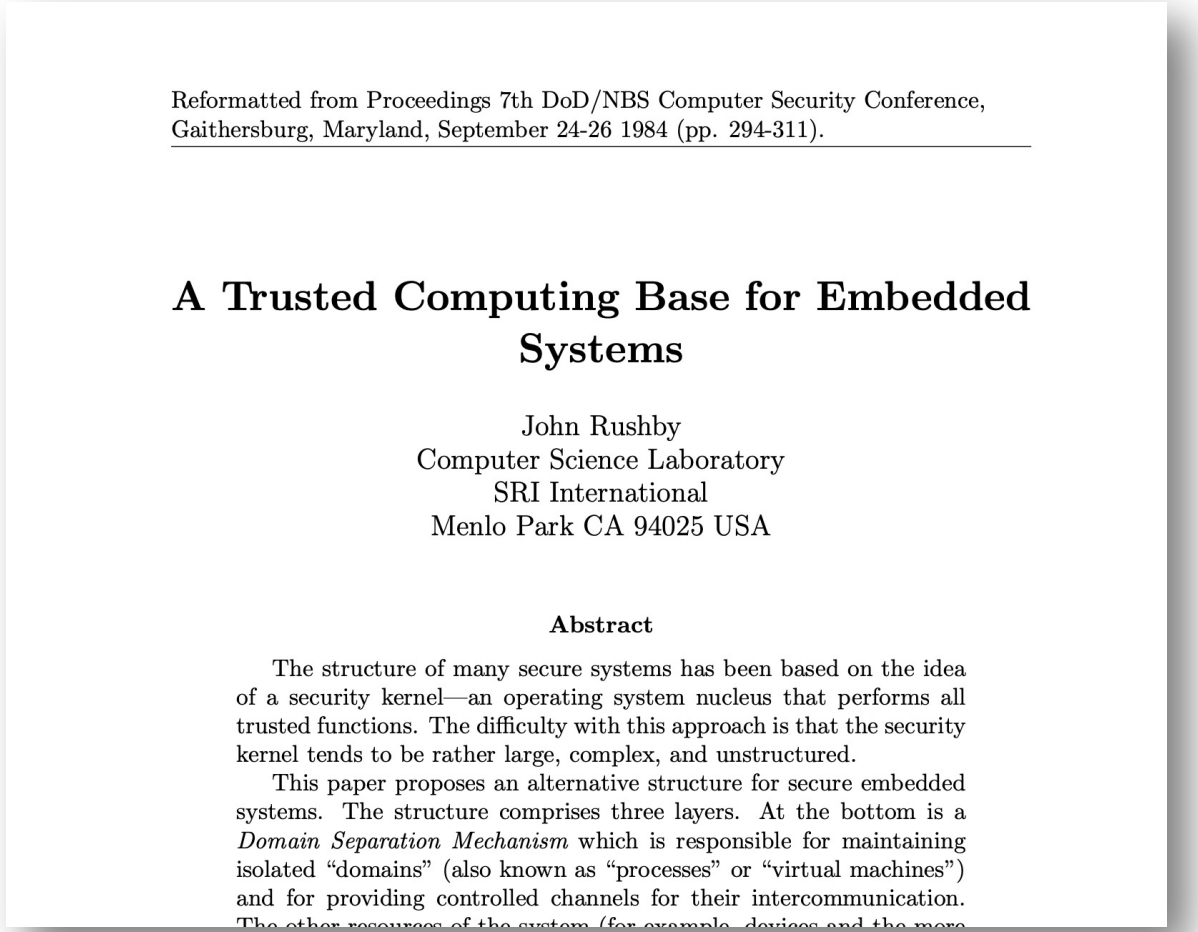
https://japan.zdnet.com/article/35138895/

OSのドメイン分離で機器をセキュアに

1984年、ASL InstitutionのJohn Rushbyの論文 “A Trusted Computing Base for Embedded Systems” が始まりと言われている

OSはセキュリティドメインの分離でセキュアに

複数の組み込みOSでセキュリティドメイン分離を実装



Reformatted from Proceedings 7th DoD/NBS Computer Security Conference, Gaithersburg, Maryland, September 24-26 1984 (pp. 294-311).

A Trusted Computing Base for Embedded Systems

John Rushby
Computer Science Laboratory
SRI International
Menlo Park CA 94025 USA

Abstract

The structure of many secure systems has been based on the idea of a security kernel—an operating system nucleus that performs all trusted functions. The difficulty with this approach is that the security kernel tends to be rather large, complex, and unstructured.

This paper proposes an alternative structure for secure embedded systems. The structure comprises three layers. At the bottom is a *Domain Separation Mechanism* which is responsible for maintaining isolated "domains" (also known as "processes" or "virtual machines") and for providing controlled channels for their intercommunication. The other resources of the system (for example, devices and the more

1984年、John Rushby が ”A Trusted Computing Base for Embedded Systems”でセキュリティドメイン分離を提唱、MILSに反映される

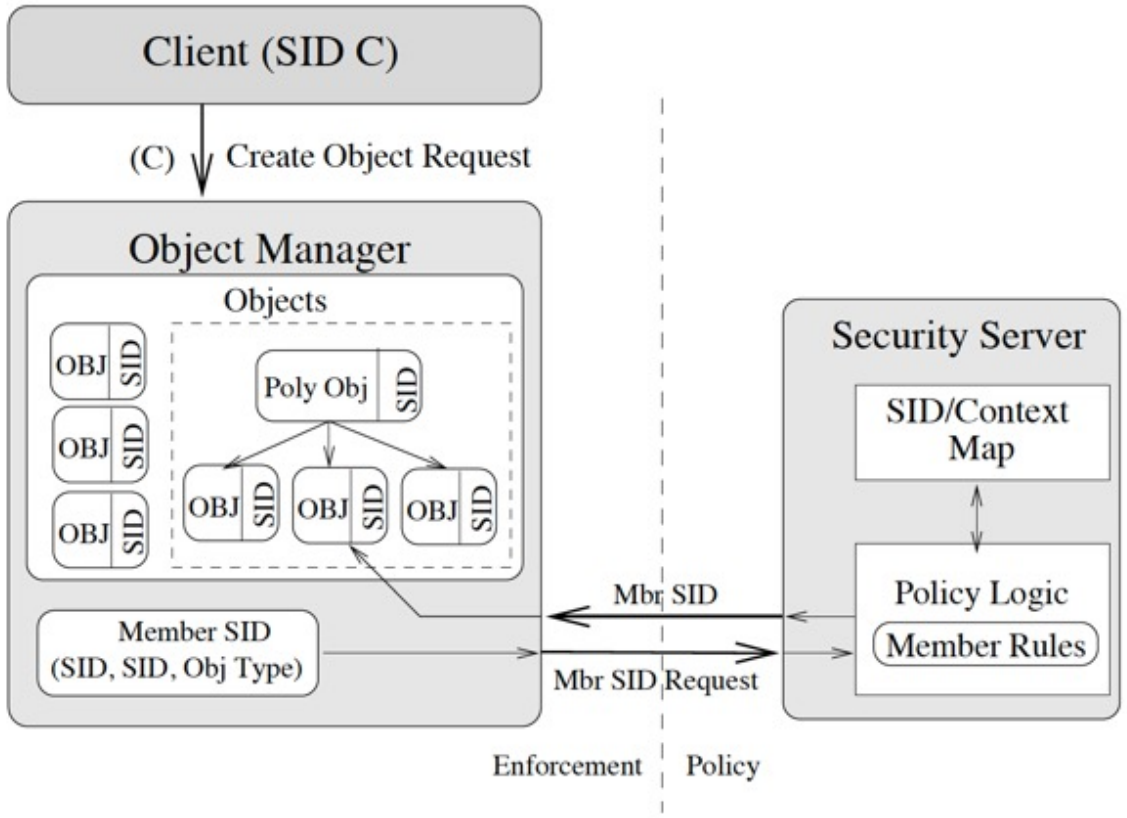
下記は代表的な商用セキュアOS、多くはMILS（米軍の調達基準、MIL規格とも）などの規格に対応

- Green Hills Software社、INTEGRITY https://www.ghs.com/products/rtos/integrity.html
- Wind River社、VxWorks https://www.windriver.com/products/vxworks/
- SYSGO社、PikeOS https://www.sysgo.com/products/pikeos-hypervisor/
- Kaspersky社、KasperskyOS https://os.kaspersky.com/

http://www.csl.sri.com/users/rushby/papers/ncsc84-tcb.pdf

セキュリティドメインの分離とは？

Flask セキュリティアーキテクチャによるセキュアなアクセス制御の実証



- SE Linuxの参照アーキテクチャで、1993年のT. Fine と S. E. Minearによる研究 “Assuring Distributed Trusted Mach” から出発してユタ大のFluxが参画し、 DTOS(Distributed Trusted Operating System)プロジェクトを経て、 1999年の“The Flask Security Architecture: System Support for Diverse Security Policies”に至る

- セキュリティポリシーの異なるドメインを、カーネル内のセキュアなプロセスに分離したSecurity Serverによってアクセス制御を行い、セキュアなOSを実現するためのアーキテクチャとして考えられた

http://www.cs.utah.edu/flux/flask/

ドメイン分離でできることとできないこと

- **できること**
  - あらかじめ定義されたポリシーに基づいてアクセス制御が行われるため、カーネル上で動作するプロセス（アプリやドライバーなど）同士の相互作用（プロセス間通信）で定義されていない相互作用はすべて弾かれるため、マルウェアなどが侵入しても他のプロセスにアクセスできない。

- **できないこと**
  - 厳しい「ポリシー」によるアクセス制御が機能しても、脆弱で危険なプログラムコードが含まれていないことを保証するわけでは無く、第三者による改竄の可能性もある

RoT(信頼の基点)でよりセキュアに

Root of Trust（信頼の基点)は現時点での最適解、しかし課題もある

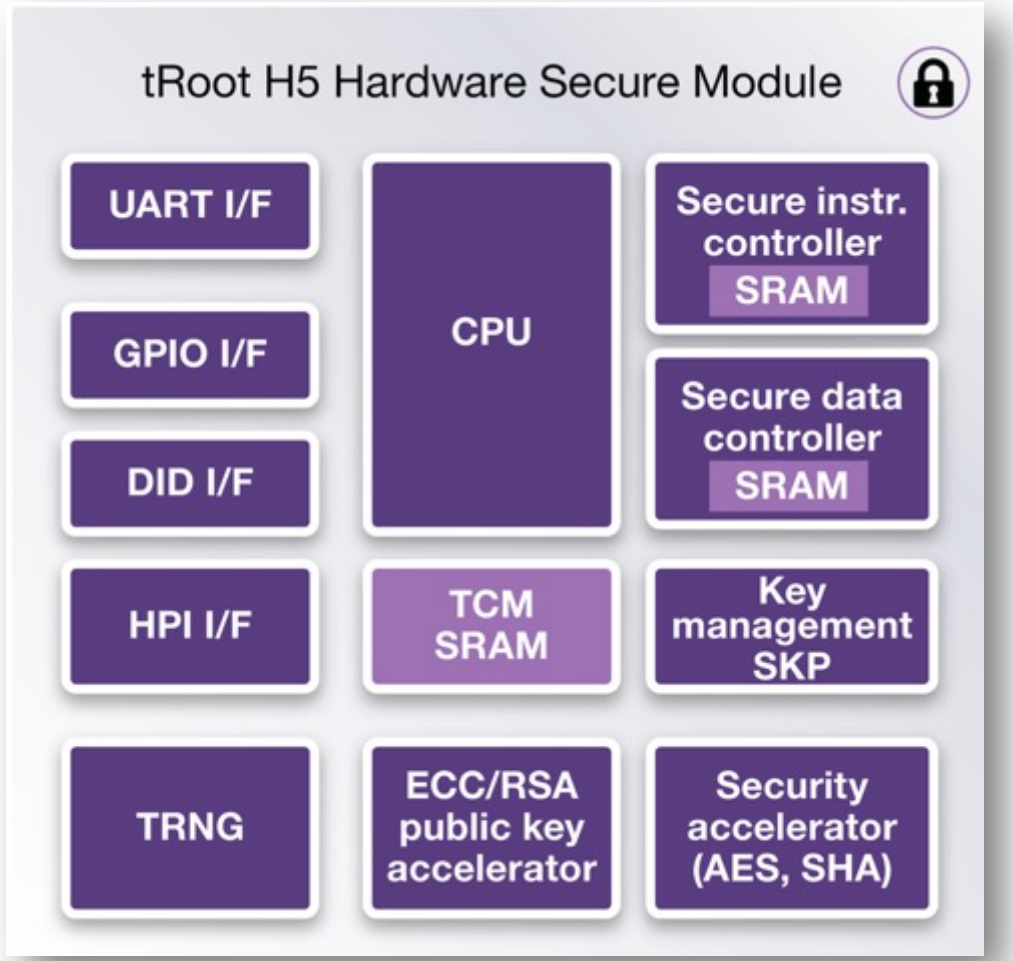
Root of Trustってなんだっけ？

- 改竄の困難なハードウェア（半導体）を用いて信頼できるブートローダー、OS、アプリケーションを順次起動する基点。

- Microsoft社の Azure Sphere MCU(＋Pluton)、Google社のTitan、Infineon社のOptiga TPM、ARM社のTrustZoneなどがあり、これらは半導体と組み込まれたファームウェアなどとセットで提供される。
- https://docs.microsoft.com/ja-jp/azure-sphere/product-overview/what-is-azure-sphere
- https://cloud.google.com/blog/ja/products/gcp/titan-in-depth-security-in-plaintext
- https://www.infineon.com/cms/jp/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/
- https://developer.arm.com/ip-products/security-ip/trustzone

ハードウェア Root of Trust 構成例

~ DesignWare tRoot H5 HSM (Hardware Secure Module) ~



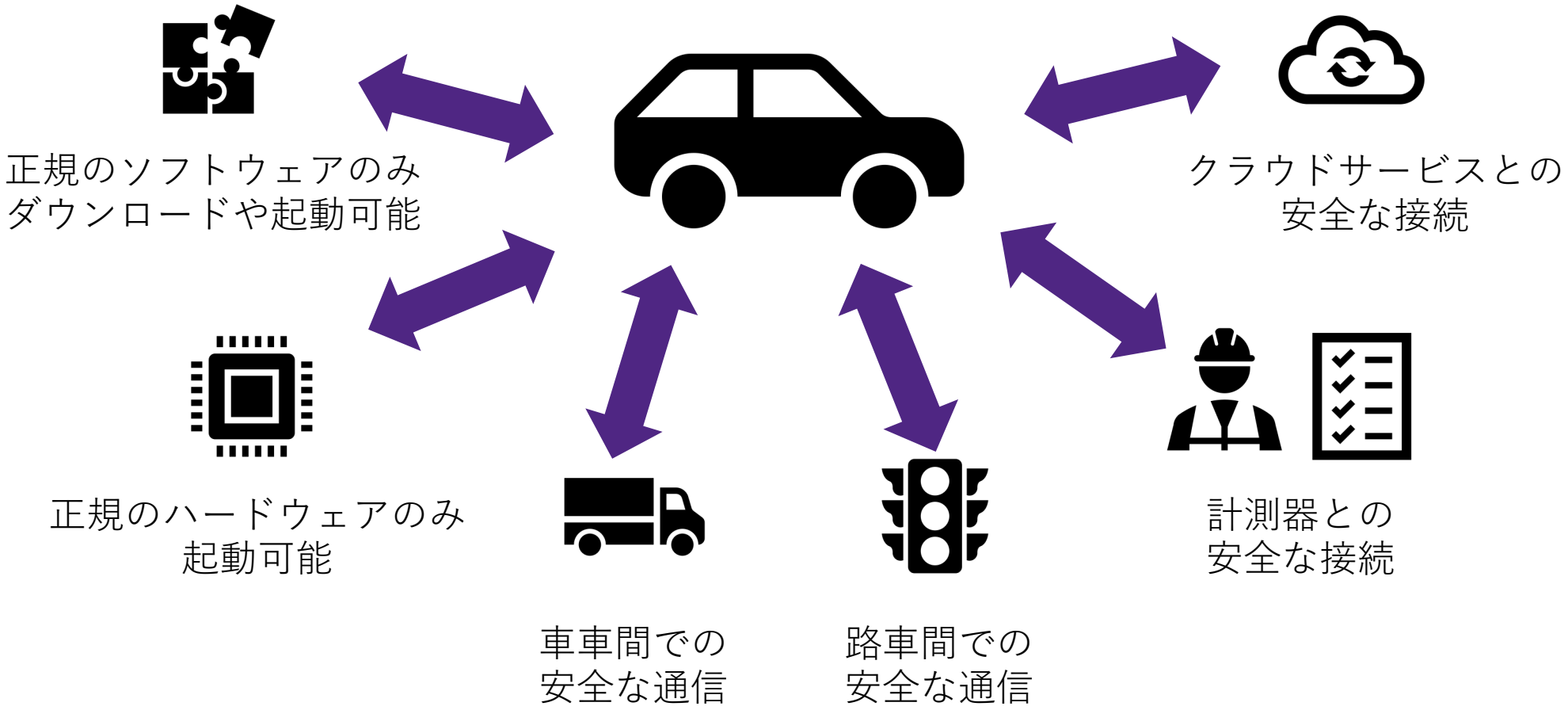
https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html

ハードウェアRoTを構成する主なコンポーネント

- 安全な監視
  - 電源投入時から SoC上のコンポーネント間の通信を監視し、問題があればホストに通知
- 安全な検証と認証
  - 暗号化されたプログラムコードやデータの真正性を保証し、起動時のブートコードなどを検証する
- 記憶域の保護
  - 非暗号化データをデバイス固有の暗号鍵を使って暗号化
- 通信の保護
  - HMAC (Hash-based Message Authentication Code)による鍵交換や認証
- 鍵の管理
  - 秘密鍵を格納し、アプリケーションからの要求に対しては間接アクセスのみを提供

アクセスを証明書で管理する

より包括的なセキュリティ対策を実現するためには「証明書」が必要



Microsoft Azure Sphereの例

- 例えば、Microsoft Azure Sphere ではRoot of Trustによるプラットフォームが正規のソフトウェアで起動し、動作するための仕組みを提供するだけでなく、証明書を使った管理の仕組みを組み込むことで、以下を実現。
  - 正規のアプリケーション、ネットワーク接続、周辺機器との接続を保証
  - Over The Airでの遠隔更新を安全に実現
  - ハードウェアファイアウォールによるデータやアプリケーションを侵害や改竄から保護
  - 障害発生の通知と管理を安全に実現
- https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

Root of Trustでできることとできないこと

- **できること**
  - ボード上のファームウェア（UEFIなど）をロードして、ストレージ上のブートセクターにアクセスして「ブートローダー」を起動。OSイメージをロードしてOSを起動し、改竄などを検知することができる。

- **できないこと**
  - 信頼された「ファームウェア」、「ブートローダー」、「OS」に、脆弱で危険なプログラムコードが含まれていないことを保証するわけでは無い。

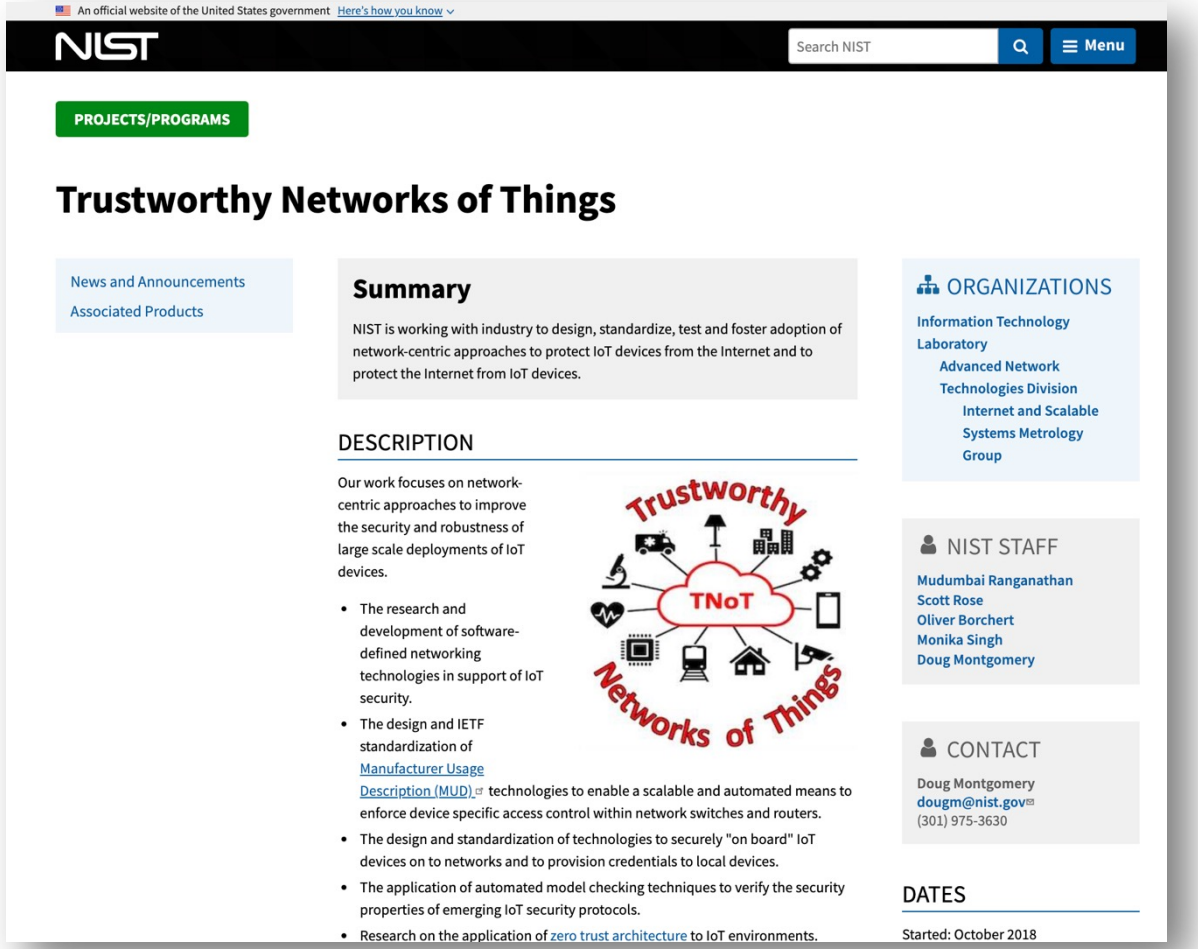
⇧は開発者の仕事です

米国の取り組みを眺めてみる

IoTのセキュリティリスクを低減するために
効果のある標準や規格を策定する
そのための様々な試み

米国(NIST)はどうしているか？

プロジェクト“TNoT”が進行中



https://www.nist.gov/programs-projects/trustworthy-networks-things

業界と協力して、IoT機器をインターネットから保護し、インターネットをIoT機器から保護するためのネットワーク中心のアプローチの設計、標準化、テスト、および採用の促進に取り組んでいる

成果：

- MUD（Manufacturer Usage Description Specification）＝RFC 8520
  - https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1709.html
- 制約のあるIoT環境の信頼できるインフラ構築のためのDNS-based Authentication of Named Entities (DANE)の研究
- ゼロトラスト・アーキテクチャ（ZTA）に基づいたアプリケーションのIoT環境のための研究

ZTAもMUDも”アクセス制御”

前出のFlaskアーキテクチャによるドメイン分離もアクセス制御

NIST SP 800-207 ZERO TRUST ARCHITECTURE

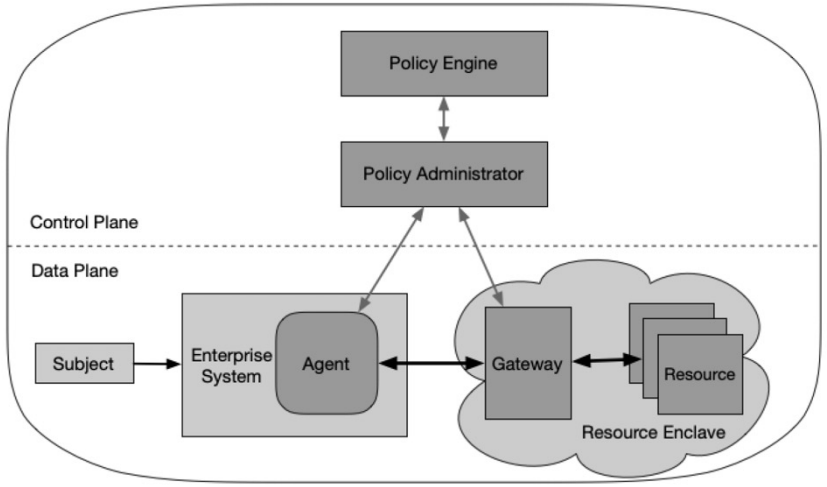


Figure 4: Enclave Gateway Model

https://csrc.nist.gov/publications/detail/sp/800-207/final

What is MUD?

To answer the above three questions, Cisco has been working on a solution known as Manufacturer Usage Description (MUD) to arm IoT security with you.

The key idea of MUD is to facilitate device visibility and segmentation by allowing your network administrators to effortlessly identify the type of IoT device and define the corresponding appropriate behaviors for that device. To do this accurately, we are introducing a participant to the conversation: the manufacturer. IoT manufacturers are able to disclose to us what their devices are, and what network policies they need for the devices to correctly function. This whitelist statement is something that customers can use to deploy access policies in their own networks without any guesswork.

As shown in Figure 1, an IoT device first sends out a pre-embedded MUD-URL to the network devices (e.g. switch & AAA server), through which the MUD-URL will be received by the MUD controller (software). According to the specific MUD-URL, a matching MUD file will be provided from the MUD file server and translated into policy format through the MUD controller, to then enforce the access control list to the device.

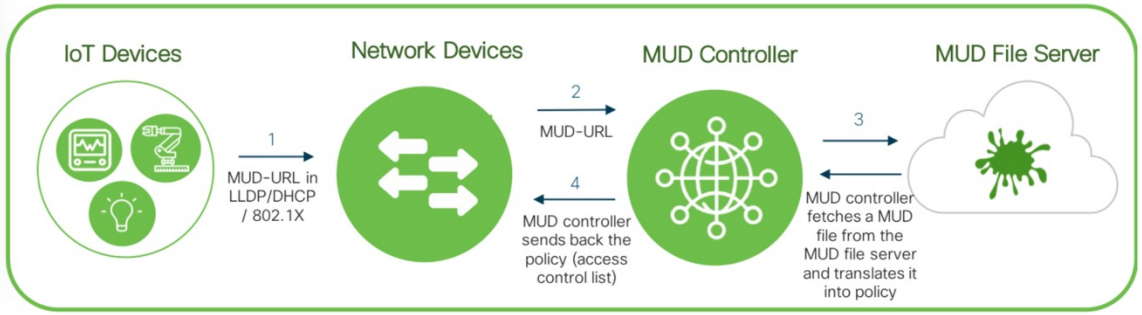


Figure 1: MUD Architecture Flow

https://blogs.cisco.com/security/mud-is-officially-approved-by-ietf-as-an-internet-standard-and-cisco-is-launching-mud1-0-to-protect-your-iot-devices

EO 14028 ” Improving the Nation's Cybersecurity”

2021年5月12日発行のEO（Executive Order /大統領令）の構成

- Sec.2：情報共有の推進
  - 政府組織間、契約ベンダー含む
- Sec. 3：最新のセキュリティ対策
  - プライバシー保護、ZTAの推進など
- Sec.4：サプライチェーンの向上
  - ソフトウェアの透明性の向上
  - SBOM、ASTなどの活用
- Sec.5：Cyber Safety Review Boardの設置
  - インシデントおよび対処についての評価など
- Sec.6：プレイブック
  - サイバーセキュリティおよびインシデント
  - NISTのガイダンスを集約するなど

など

https://www.synopsys.com/blogs/software-security/ja-jp/biden-cybersecurity-executive-order/

https://www.federalregister.gov/presidential-documents/executive-orders/joe-biden/2021

ソフトウェアの複雑さを管理するため、SBOMが必要

サプライチェーンで問題が発生したら？➔ソフトウェアの透明性が不足している。

	ソフトウェアに対する視点		
リスク	提供者 のベネフィット	選択者 のベネフィット	運用者 のベネフィット
コスト	計画外で予定外の作業を減らす	より精度の高いTCOの実現	より効果的な管理
セキュリティリスク	既知の脆弱性を回避	デュー・デリジェンスを容易に	速やかに特定して解決。特定のソフトウェアへの影響とその範囲を知る
ライセンスリスク	ライセンスと関連するリスクをを定量化して管理	デュー・デリジェンスを容易に	より効果的で正確なライセンス要求への対処
コンプライアンスリスク	リスク評価を容易に。ライフサイクルの早期にコンプライアンス要件を特定	より正確なデュー・ジェリエンす、ライフサイクルの早期に問題を捕える	簡素化されたプロセス
高度な保証	成果物、ソースコード、使用するプロセスのアサーションを作成	コンポーネントについて、情報に基づいて攻撃に強い選択	変化する敵対的な状況下で主張を検証

透明性を改善するためのポイント

- 来歴（Provenance）
  - SBOMの来歴は、ソフトウェアを構成するすべての構成コンポーネントの管理過程に関する情報を持ち、作成者とコンポーネントが取得された場所に関する情報を含みます
- 血統（Pedigree）
  - SBOMの血統は、集まったすべてのコンポーネントと、それらが集まったプロセスに関する情報です。これには、コンパイラオプションなど、コンポーネント以外の詳細を含めることができます
- 完全性（Integrity）
  - SBOMの完全性は、暗号化技術を使用して、SBOMが作成者によって作成されてから変更されていないことを示すか、変更があった場合は他のSBOM作成者による変更を示します

https://www.ntia.gov/SBOM

エコシステムにおけるソフトウェアの“公衆衛生”の向上

ソフトウェアの安全性を管理・流通させる仕組み「SBOM」で実現する

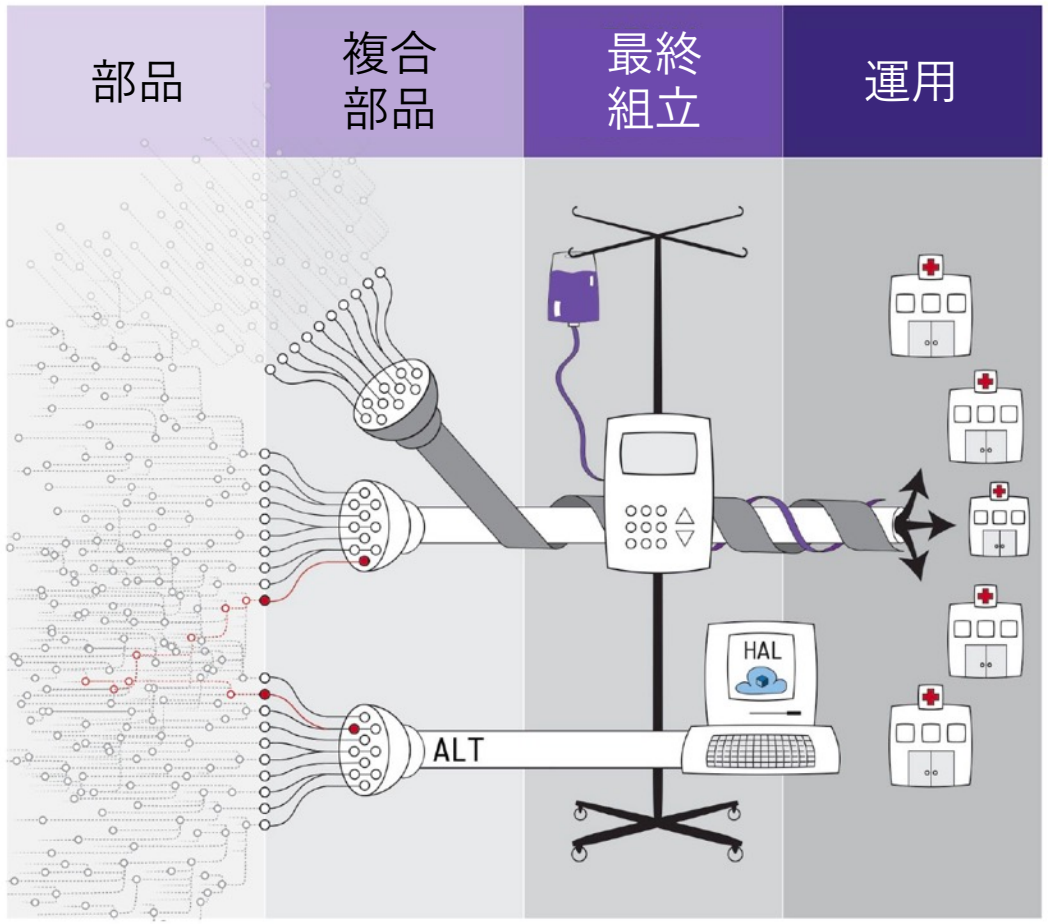


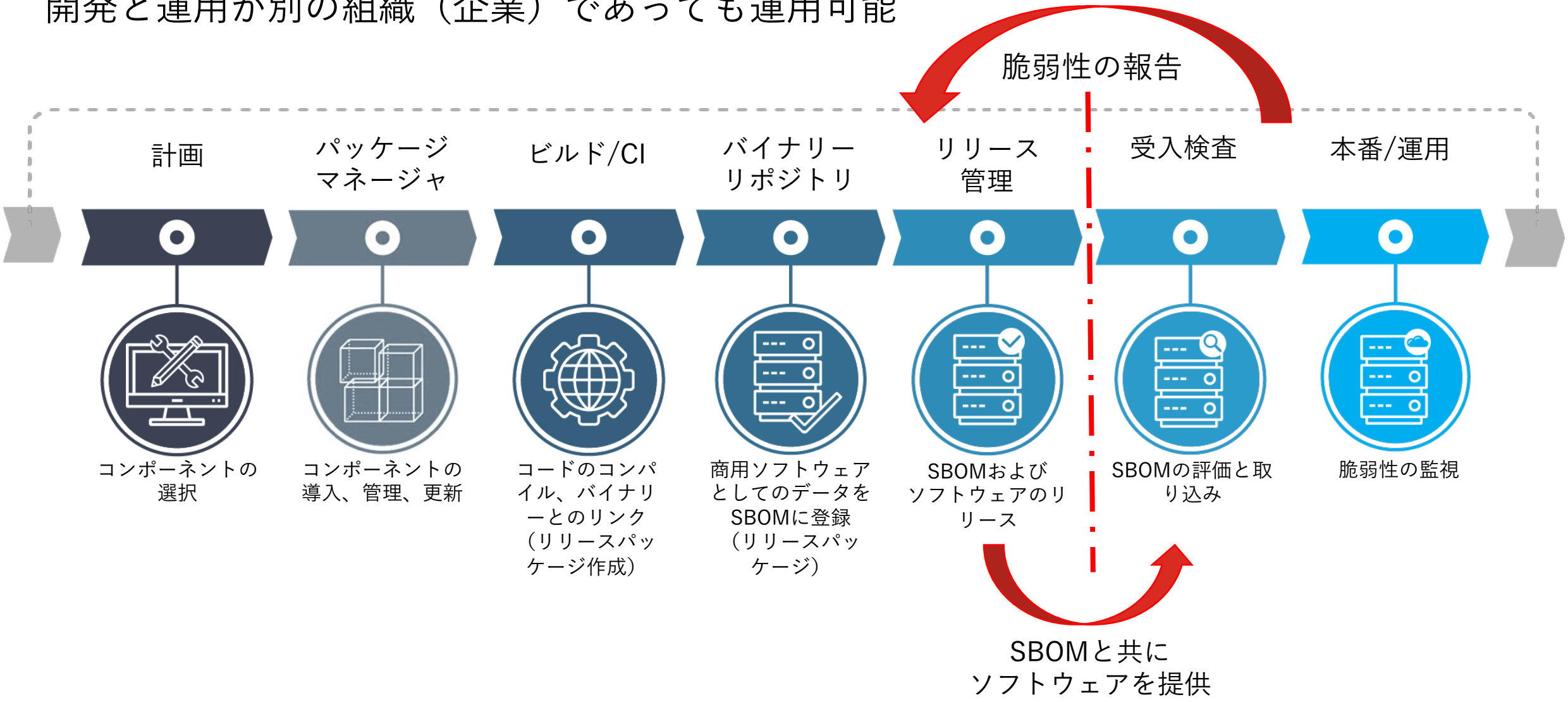
Figure 1: Software Supply Chain Ecosystem

https://www.ntia.gov/SBOM

- SBOMは特定のチーム、役割、または組織へのメリットだけでなく、エコシステム全体の重要なメリットを提供
- 集団予防接種が「集団免疫」を獲得することで他の予防接種を受けていない子供を保護するのと同様、サプライチェーン内の保護を強化
- より広範な生態系レベルの変化が起こることで、サプライチェーン内の「公衆衛生」が向上

SDLC全体でのコンポーネントの管理

開発と運用が別の組織（企業）であっても運用可能



SSDF(Secure Software Development Framework)の更新

NIST SP 800-218（1.0は2020/4 公開）

NIST

Search CSRC

CSRC ME

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS

SP 800-218

Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

Date Published: February 2022

Supersedes: White Paper (04/23/2020)

Author(s)

Murugiah Souppaya (NIST), Karen Scarfone (Scarfone Cybersecurity), Donna Dodson

Abstract

Few software development life cycle (SDLC) models explicitly address software security in detail, so secure software development practices usually need to be added to each SDLC model to ensure that the software being developed is well-secured. This document recommends the Secure Software Development Framework (SSDF) – a core set of high-level secure software development practices that can be integrated into each SDLC implementation. Following these practices should help software producers reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Because the framework provides a common vocabulary for secure software development, software purchasers and consumers can also use it to foster communications with suppliers in acquisition processes and other management activities.

Keywords

secure software development; Secure Software Development Framework (SSDF); secure software development practices; software acquisition; software development; software development life cycle (SDLC); software security

DOCUMENTATION

Publication:

SP 800-218 (DOI)

Local Download

Supplemental Material:

SP 800-218 Table in Excel (xls)

Delta from April 2020 paper (word)

Delta from September 2021 public draft (word)

SSDF Project homepage (other)

Executive Order 14028, Improving the Nation's Cybersecurity (web)

Related NIST Publications:

White Paper

Document History:

09/30/21: SP 800-218 (Draft)

02/03/22: SP 800-218 (Final)

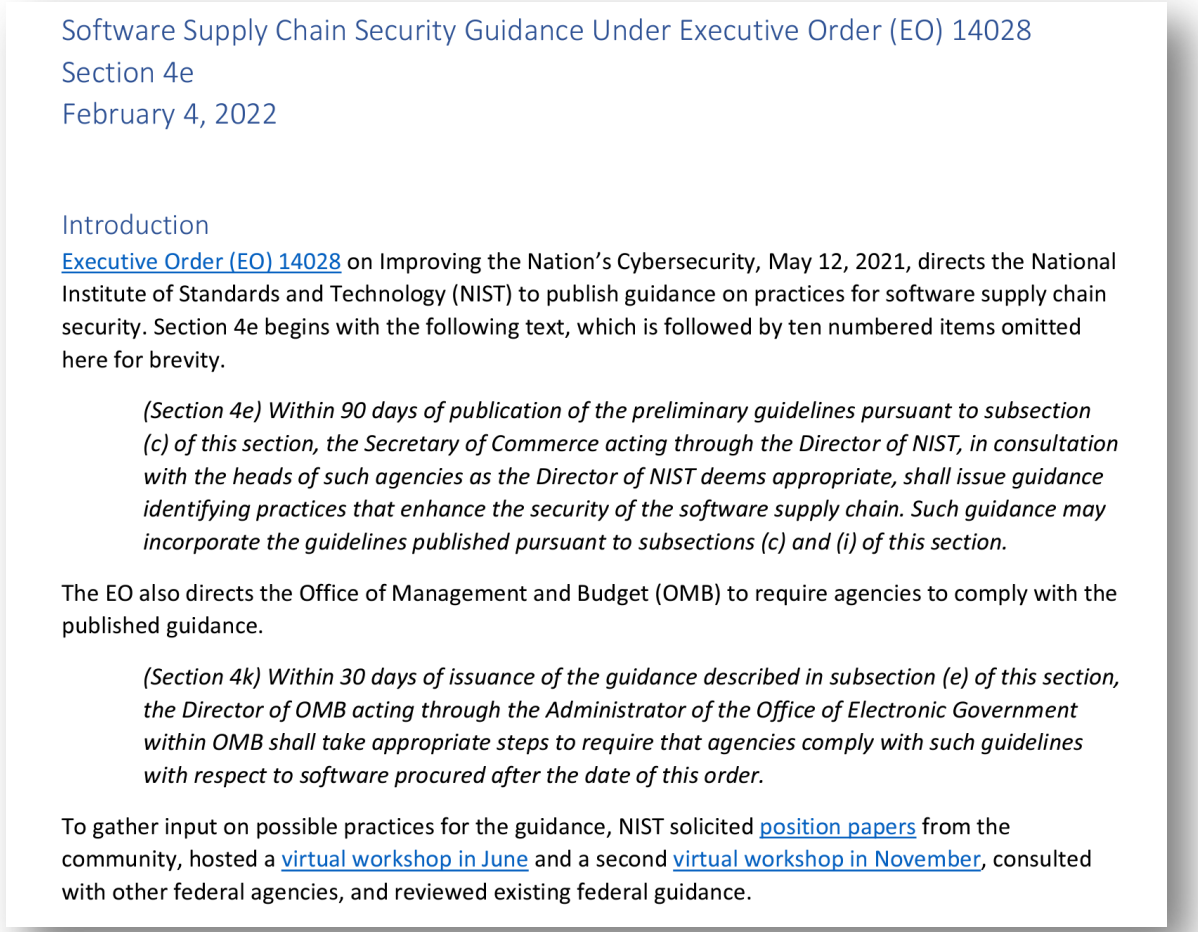
TOPICS

https://csrc.nist.gov/publications/detail/sp/800-218/final

- 2022/2/3、ver 1.1 最終版公開
- EO14208の各章の記述をSSDFに割り当てる
- 組織毎のSDLCの実装に合わせて統合可能な、高度に安全なソフトウェア開発プラクティスのコアセットを提供する
- SSDFに倣うことで、以下を実現する
  - 脆弱性の数を減らす
  - 未知の、または未対処の脆弱性の悪用による潜在的な影響を軽減する
  - 脆弱性の根本原因に対処して将来の再発を防ぐ

NIST Software Supply Chain Security Guidance

Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e



Software Supply Chain Security Guidance Under Executive Order (EO) 14028
Section 4e
February 4, 2022

Introduction

Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, May 12, 2021, directs the National Institute of Standards and Technology (NIST) to publish guidance on practices for software supply chain security. Section 4e begins with the following text, which is followed by ten numbered items omitted here for brevity.

> *(Section 4e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section.*

The EO also directs the Office of Management and Budget (OMB) to require agencies to comply with the published guidance.

> *(Section 4k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.*

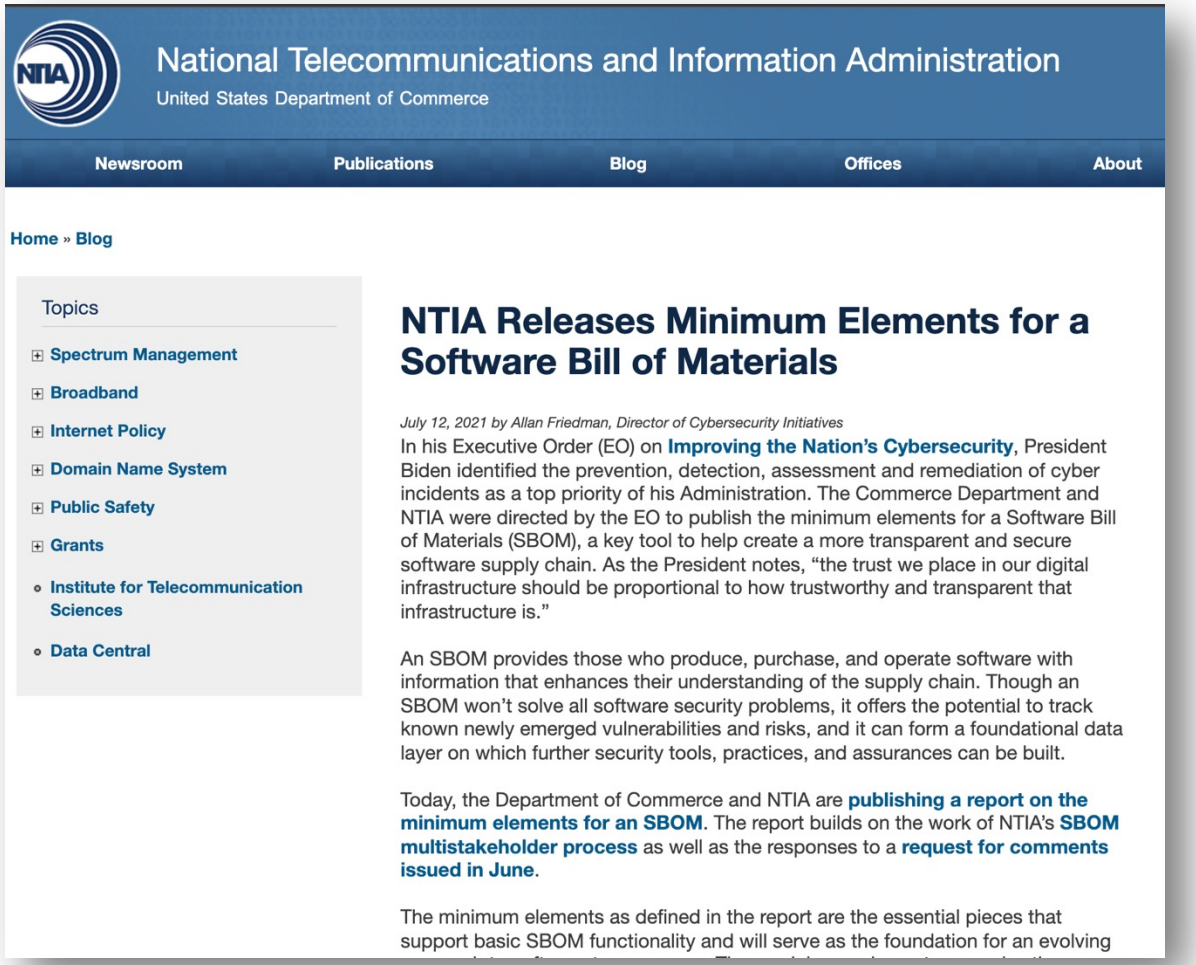
To gather input on possible practices for the guidance, NIST solicited position papers from the community, hosted a virtual workshop in June and a second virtual workshop in November, consulted with other federal agencies, and reviewed existing federal guidance.

- 2022年2月4日、EO14028のセクション4eを達成するため、目的別のNISTのガイダンスを整理。
- SSDF（SP800-218）を含め、何のために、どのようなガイダンスが用意されているか、一覧できる。
- AttestationのためにはSP800-161rev1を、適合性検査にはNIST SP2000-1/-2（これらはISO/IEC 17000:2020を参照している）またISO/IEC 17000:2020を用いる。

https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

SBOMの最小構成要素について

NTIA(商務省の下部組織)による定義



National Telecommunications and Information Administration
United States Department of Commerce

Newsroom | Publications | Blog | Offices | About

Home » Blog

Topics

- Spectrum Management
- Broadband
- Internet Policy
- Domain Name System
- Public Safety
- Grants
- Institute for Telecommunication Sciences
- Data Central

NTIA Releases Minimum Elements for a Software Bill of Materials

July 12, 2021 by Allan Friedman, Director of Cybersecurity Initiatives

In his Executive Order (EO) on **Improving the Nation's Cybersecurity**, President Biden identified the prevention, detection, assessment and remediation of cyber incidents as a top priority of his Administration. The Commerce Department and NTIA were directed by the EO to publish the minimum elements for a Software Bill of Materials (SBOM), a key tool to help create a more transparent and secure software supply chain. As the President notes, "the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is."

An SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain. Though an SBOM won't solve all software security problems, it offers the potential to track known newly emerged vulnerabilities and risks, and it can form a foundational data layer on which further security tools, practices, and assurances can be built.

Today, the Department of Commerce and NTIA are **publishing a report on the minimum elements for an SBOM**. The report builds on the work of NTIA's **SBOM multistakeholder process** as well as the responses to a **request for comments issued in June**.

The minimum elements as defined in the report are the essential pieces that support basic SBOM functionality and will serve as the foundation for an evolving

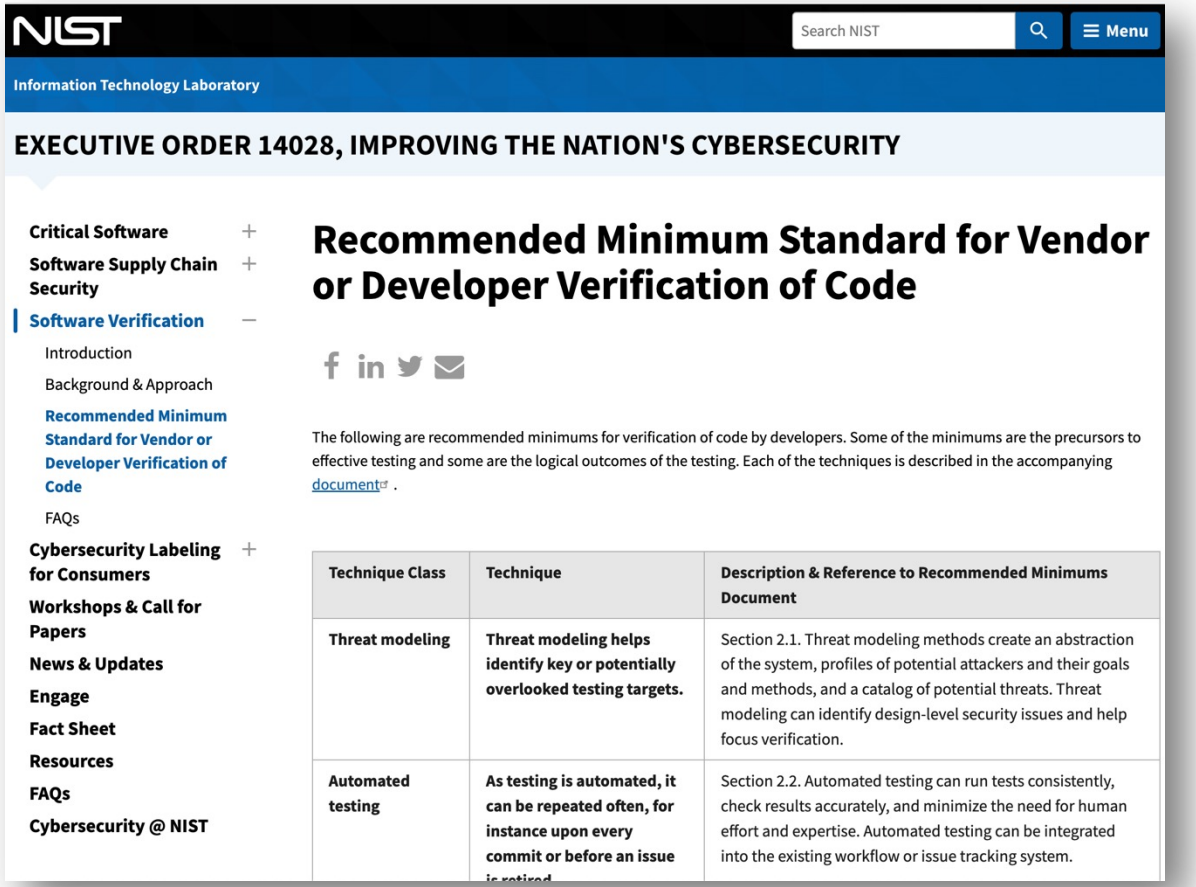
https://ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

- 2021/6/2に発行されたRFCによって得られた要望を参考に作成された
- データは7項目
  - Supplier Name、Component Name、Version of the Component、Other Unique Identifiers 、Dependency Relationship、Author of SBOM Data、Timestamp
- フォーマットは3種
  - Software Package Data eXchange (SPDX) 、CycloneDX、Software Identification (SWID)
- これからの展開
  - 多様なユースケースをサポートすることを想定
  - 推奨されるデータ項目も提案

  など

Recommended Minimum Standard for Vendor or Developer Verification of Code

NISTの定めた推奨最小テスト要件



https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer

- 2021/10/6、NISTIR 8397発行

- 推奨される最小テスト要件
  - 脅威モデリングで設計レベルの課題を発見
  - テストの自動化による効率化
  - SASTによる重大な欠陥の発見
  - ハードコードされた認証情報の検知
  - 開発言語に依存する弱点の検知
  - ブラックボックス・テスト
  - 実装（コード）ベースのカバレッジテスト
  - 回帰（レグレッション）テスト
  - ファジング
  - ウェブアプリ・スキャナ（DAST、IAST）
  - ソフトウェア・コンポジション解析

業界毎のSBOMの取り組み状況

- 医療用機器（FDAおよびIMDRF）
  - SBOMは CBOMの一部に
  - 2019年の市販前ガイダンスに従い、510kの提出に必要
  - HDOからの緊急要求
  - NTIAの最小構成要素に従う（FDA ガイダンス 2021）
- 米国政府ソフトウェア調達（EO 14028）
  - NTIAの最小構成要素に従う
  - FAR/DFARの調達条項に盛り込まれる日程は未定
    - CISAは将来VEXを必要とする可能性がある
  - インテグレータからの要求が先行していると思われる
    - サプライチェーンの波及効果
- 自動車、エネルギー、インダストリアルIoT
  - エネルギーではNTIAの最小構成要素に沿ってPoC中
  - 自動車では OpenChain （ISO 5230）のサポートが必須（主目的はライセンス）
  - バイナリー解析とSBOMの検証が慣習に