VDOO

2020 年 6 月

IoT サイバーセキュリティ 規制と規格化

Leo Dorrendorf
leo@vdoo.com

VDOO Connected Trust Ltd. について

VDOO

VDOO の統合型デバイスセキュリティプラットフォームは、デバイスのライフサイクル全体にわたって最適なセキュリティを確保し、コネクテッド製品のセキュリティ確保をサポートします。
これには、セキュリティ分析、ギャップ解決、コンプライアンス検証、組み込み型保護、運用モニタリング、実用的なインサイト、セキュリティインテリジェンスが含まれます。

VDOO は MS&AD ホールディングスや NTT ドコモなどの大手投資会社から 4,500 万ドルの資金を調達しており、現地の販売パートナーである大日本印刷株式会社 (DNP) やマクニカネットワークスを通じて、日本国内に複数の顧客を獲得しています。

VDOO 社 セキュリティアーキテクチャ部門 責任者
Leo Dorrendorf

規格に関する過去の業務

- ハードウェア・セキュリティ・モジュールの FIPS 140-2 認証を担当
- その他の NIST 規格の取り扱い
- 複数の標準化団体への参加

VDOO での現在の業務

- CCDS など VDOO Vision のサイバーセキュリティ規格を担当
- 日本の総務省に規格調査で協力
- 現在 OWASP ISVS プロジェクトをサポート

アジェンダ

1. はじめに
2. 規制
3. 規格化
4. 自動化ツールの導入

1 ····· 2 ····· 3 ····· 4

1. はじめに

動機：コンプライアンスの原動力

VDOO

規制と法施行	規格化
• 政令	• 入札要件
• 罰則規定	• 顧客の要望
• 規格準拠の要求 →	• 業界規制による義務付け
	• 競合他社に対する優位性

Common sanctions for non-compliance with these regulations could have serious financial and reputational implications for corporations and staff, including:

- Fines
- Personal liability and imprisonment of managers or officers
- Cease and desist orders
- Erasure of data
- Public announcements and product recalls
- Binding instructions on security features

https://www.iotsecurityfoundation.org/best-practice-guidelines/

1 2 3 4 5 6

2. 規制

規制

VDOO

行政機関が施行

- 非常に局所的

行政・立法府が作成

- 更新がまれ
- 曖昧
- リードタイムが長い

業種別に適用

- 医療、自動車、重要インフラ

特定の対象に対して適用可能

- 安全、プライバシー、児童保護

››› 推奨ソース

VDOO

IoT Security Foundation の概要書

https://www.iotsecurityfoundation.org/best-practice-guidelines/

››› 規制例：FDA

VDOO

FDA 規制の適用条件 (次を目的としている場合のみ適用)：

- … 診断、予防、治療、緩和、処置
- … 病気またはその他の健康状態
- … 身体組織や機能に影響を及ぼす

FDAガイダンス

- 医療機器におけるサイバーセキュリティ管理のための販売前申請
- 医療機器におけるサイバーセキュリティ販売後の管理
- 既製 (OTS) ソフトウェアなどネットワーク化された医療機器のサイバーセキュリティ

https://www.fda.gov/medical-devices/digital-health/cybersecurity

››› 規制例：FTC

VDOO

Regulation	Sanctions
Federal Trade Commission Act	• Fines up to $41,484 per violation, per day • Restitution for domestic and foreign victims • Audits (one-off or repeated) • Product recall or cease and desist orders • Imprisonment • Federal court and/or state civil action lawsuit • Requests for documentary evidence

Table 11 Sanctions: Federal Trade Commission Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 52: Dissemination of false advertisements (misrepresentation)	• Internationally recognised standards • Certification or conformity assessment • Adoption of security and best practice frameworks
Section 45: Unfair methods of competition unlawful; prevention by Commission (causes or is likely to cause substantial injury)	• Product lifecycle management and support • Encryption • Anonymisation and pseudonymisation
Section 50: Offenses and penalties (failure to produce documentary evidence)	• Certification or conformity assessment • Data Protection Policy • Privacy- and security-by-design policies • System or technical logs or backup files

Table 12 Treatment Examples: Federal Trade Commission Act

https://www.iotsecurityfoundation.org/best-practice-guidelines/

››› 規制例：FTC

VDOO

VS. TRENDnet

「TRENDnet はホームセキュリティからベビーモニターまで各種用途で利用できる SecurView カメラを『安全』な製品として販売していた。
しかし、実際にはカメラのソフトウェアに欠陥があり、カメラのインターネットアドレスが分かればオンラインで誰でも閲覧でき、場合によっては盗聴することも可能だった。」

https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc

TRENDnet は賠償金の支払いが命じられ、以下に同意した。

- 誤解を招くマーケティングの停止
- 利用者に対する 2 年間の無料テクニカルサポート
- 総合的な情報セキュリティプログラムを構築 するために、20 年間にわたり 2 年ごとに第三者によるセキュリティ監査の実施

カリフォルニア州における コネクテッド・デバイスのセキュリティ法案 (SB-327)

California LEGISLATIVE INFORMATION

1798.91.04.

(a) コネクテッド・デバイスの製造元は、次のすべてを満たす合理的なセキュリティ機能をデバイスに実装しなければならない。

(1) デバイスの性質および機能に適している。

(2) そのデバイスが収集、保持、送信する可能性のある情報に適している。

(3) 不正なアクセス、破壊、使用、変更、開示からデバイスおよびそれに含まれる情報を保護するように設計されている。

(b) 条項 (a) の全要件に従うことを条件として、コネクテッド・デバイスにローカルエリアネットワーク外での認証手段がある場合、以下の要件のいずれかを満たしていれば、条項 (a) の合理的なセキュリティ機能とみなされるものとする。

(1) 各デバイスに一意のパスワードが事前設定されている。

(2) デバイスへの初回アクセス時にユーザーに新しい認証手段の生成を要求するセキュリティ機能がある。

- 一般消費者向けデバイスのサイバーセキュリティ機能を規定した米国初の規制
- 2020 年 1 月 1 日発効
- ほとんどの規制とは異なり、実装すべき 2 つのセキュリティ機能を直接定義。

https://www.vdoo.com/blog/key-takeaways-from-the-california-security-of-connected-devices-bill

各種サイバーセキュリティ規制が発効予定

欧州連合 - EU サイバーセキュリティ法
- ENISA がベース

英国 - 消費者向け IoT セキュリティの行動規範
- 規格とラベリング制度を組み合わせた規制

米国 - IoT サイバーセキュリティ改正法 (2019)
- NIST がベース

自動車業界 - UNECE WP.29
- 自動車基準調和世界フォーラム

医療業界 - 医療機器のサイバーセキュリティに関する IMDRF の原則・実践

1 2 3 4

3. 規格化

規格化

VDOO

作成者：

- 行政機関
- 営利企業
- 非営利団体

要件の規定：

- 詳細レベルが大きく異なる

規格の適用範囲：

- 業界別（自動車、消費者向け）
- テクノロジー / プロトコル（Bluetooth、TLS）

ISA IEC

UL

OWASP Open Web Application Security Project

enisa European Network and Information Security Agency

NIST

IoT Security Foundation

CCDS

規格例：FIPS 140-2

策定経緯
- 2002 年に最新版を発行
- ガイダンス文書を段階的に訂正
- 2020 年に FIPS 140-3 に置き換え

地域
- 米国 (想定)
- 国際的な影響力 (実際)

業界・製品分野
- 暗号モジュール (想定)
- 組み込み産業で広く採用 (実際)

技術詳細レベル
- 高

FIPS 140-2

施行
- 米国政府のみ施行可

認証タイプ
- 明示的 - 暗号モジュール検証プログラム
- 認証ラボを使用
- 資料の公開を含む
- はっきりとした再認証プログラム
- 未認証の多くの企業がコンプライアンスを主張
- 2021 年 9 月をもって終了

規格例：FIPS 140-3

策定経緯
- 2020 年発行
- 2 つの ISO/IEC 文書がベース
  - ISO/IEC 19790:2012
  - ISO/IEC 24759:2017

地域
- 米国、カナダ
- 前身の規格同様に国際的な影響力があると予想される

業界・製品分野
- 暗号モジュール用 (現時点)

技術詳細レベル
- 高

FIPS 140-3

施行
- 米国政府のみ施行可

認証タイプ
- 明示的 - 暗号化モジュール検証プログラム (FIPS 140-2 と同様)

FIPS 140-2 との違い
- 複数の変更点
- ISO/IEC 規格の購入が必要

規格例：NIST SP 800-171

策定経緯
- 2020 年 2 月に最新版を発行
- 以前の版は 2015 年、2016 年に発行

地域
- 米国 (想定)
- 国際的な影響力 (実際)

業界・製品分野
- 汎用 PC、コネクテッド・デバイス、携帯電話 (BYOD も想定) を導入している企業・組織
- 組み込み産業で広く採用 (実際)

技術詳細レベル
- 中
- 該当分野別に複数の NIST を参照

施行
- DFARS (国防省調達規則) 第 252.204-7012 条を介して国防総省が要請
- 請負業者・下請業者に適用
- 連邦情報セキュリティマネジメント法 (FISMA: 2020 年) に基づく中レベルの要件

認証タイプ
- 第三者企業を使用

規格例：UL 2900

策定経緯
- 2017 年に発行

地域
- 米国を拠点に国際的な影響力

業界・製品分野
- 一般：2900-1
- 産業：2900-2-2
- 医療：2900-2-3
- 暗号モジュール：2900-3-1

技術詳細レベル
- 低～中

施行
- なし

認証タイプ
- 明示的
- UL 認定ラボを使用
- FDA の承認済み

地域別の標準化団体

該当規格の選択

規制の要求による選択

- 一般的に地域と製品分野によって決定

業界による選択

- 医療
- 自動車
- 産業用制御
- 子供向け商品

顧客の要望による選択

- 入札要件

競合他社に対抗するために選択

- コンプライアンスが顧客の需要に影響を与えかねない
- 他社との競争においてコンプライアンスが有利に作用する

コンプライアンスの種類

申告による準拠

- 販売情報のみ

自社認証

- アンケート
- 文書化
- 自動テスト

第三者認証

- 認証機関
- 独立機関
- 侵入テスト

認証への取り組み

サポートを得る

- コンサルタント
- ラボ
- 初回ギャップレポート

認証の取得

- 作成
- 文書化
- 専用窓口

認定書の受領

- 認証機関との交流

認証の維持

- 製品にパッチを適用して認証を維持
- 製品の次回バージョンで再認証
- 有効期限 / 失効

1 ····· 2 ····· 3 ····· 4

4. 自動化ツールの使用

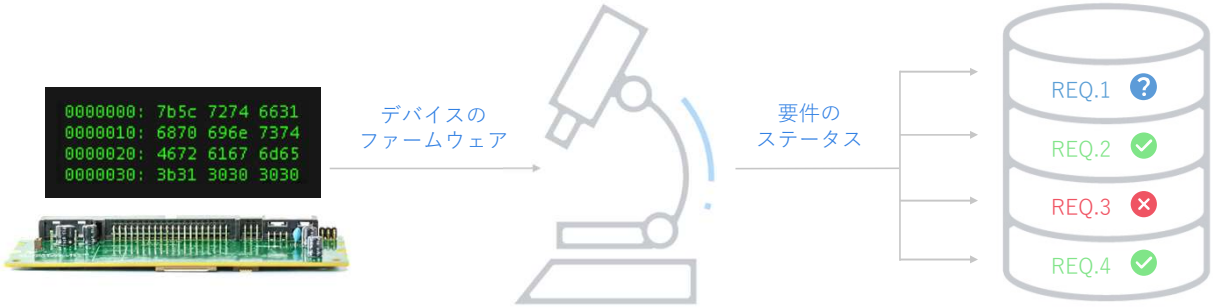
規格を要件とスキャナにマッピング

VDOO

該当の規格を選択後：

- 要件別に分解します
- 内部データベースにマッピングします
- これにより要件とスキャナーを関連付けます

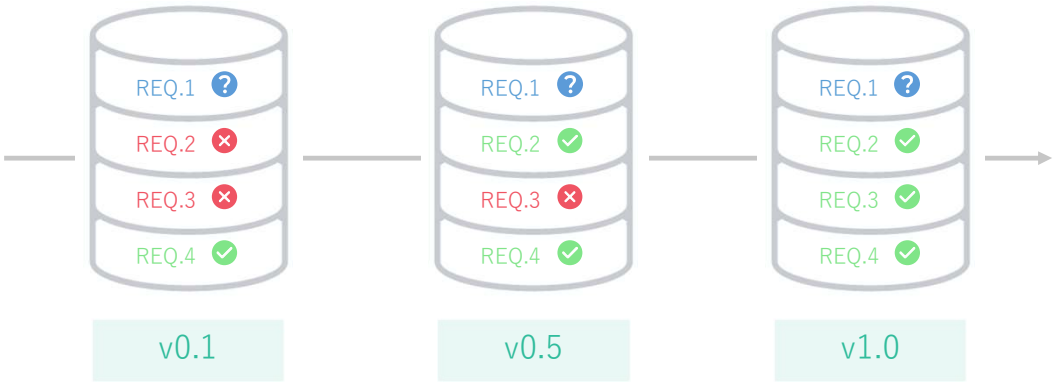
››› ギャップレポートの作成



検証プロセスの自動化：

- スキャナーを実行します
- 正、負、N/A のいずれかが出力されます
- 数分でギャップレポートが作成されます

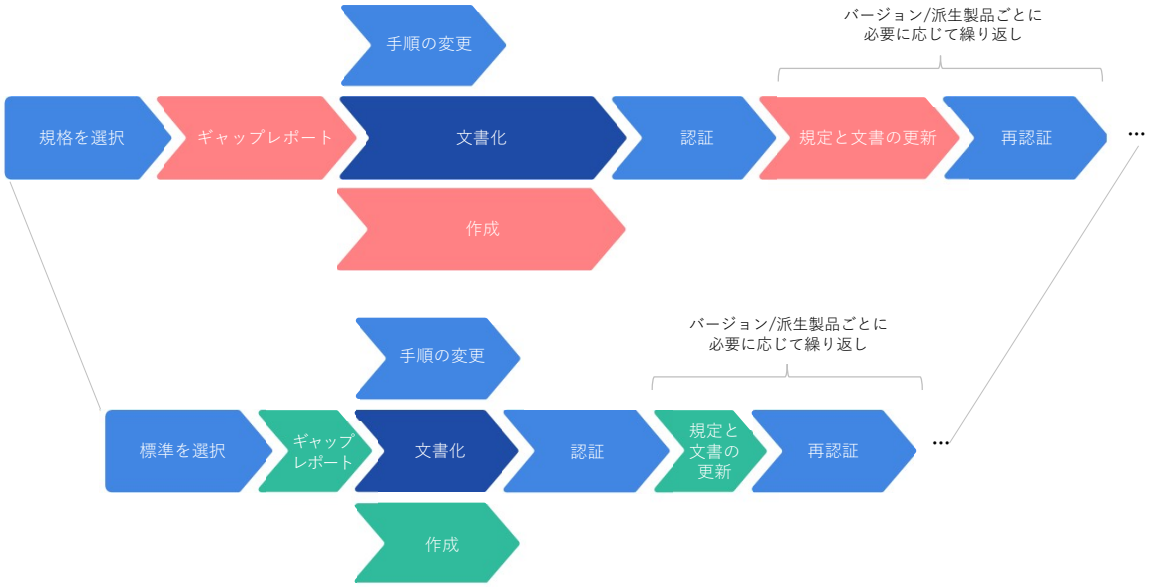
››› バージョンをまたいだ追跡



- セキュリティスキャンを CI/CD と統合します
- すべての製品バージョンを追跡します
- 製品ライン全体を追跡します
- これにより、セキュリティプロセスがシームレスになります

認証プロセスの短縮

VDOO



VDOO