PHILIPS

セキュリティポジションペーパー

フィリップスとサイバーセキュリティ

フィリップスのお客様のセキュリティとプライバシーを保護するための積極的な取り組み

2020年11月

目次

1. ヘルスケアのデジタル化 – 機会と脅威	3
2. サイバーセキュリティにおけるフィリップスの取り組み	4
3. 透明性、コンプライアンス、そしてその先へ	5
4. 製品のセキュリティ	6
5. エンタープライズ情報セキュリティ	8
6. プライバシー	10
7. 適切な体制とメカニズム	11
8. 詳細情報	11
付録：製品のセキュリティに関する声明	12

「サイバーセキュリティはコネクテッドケアへの移行において中心的な役割を果たします」

Jeroen Tas
フィリップス最高戦略革新責任者

1. ヘルスケアのデジタル化 – 機会と脅威

高齢化社会に直面し、慢性疾患の発生率も上昇しつつある現在、ヘルスケア・システム業界は、良心的な価格で適切なヘルスケア・モデルを構築すべく、努力を続けています。もとより困難な課題でしたが、新型コロナウィルス感染症（COVID-19）がさらに拍車をかけています。機器、健康アプリ&プラットフォームをネットワークに接続したコネクテッド・ヘルスケアは、ヘルスケアを変革し、低価格で質の高いヘルスケアを実現するうえでかつてないほどの潜在能力を秘めています。

ネットワークに接続された数百万に及ぶデジタル・デバイスの普及により、各ユーザーはネットワーク上で、ケア後の転帰の向上に活用できる膨大なデータフローを共有、検索、ナビゲート、管理、比較、分析できるようになりました。この「デジタル・エコシステム」に基づいて、ヘルスケア業界は、パーソナライズされたヘルスケア指向のスマート・デバイスのポートフォリオを拡張し、イノベーションを起こし、サービスの効率性を向上させています。

たとえば、撮影装置、モニタ、携帯型の個人用機器で収集した電子医療記録や診断記録の分析は、医療従事者の意思決定能力を高めただけでなく、患者自身が健康を管理するうえで、より重要な役割を果たすようになりました。

その一方で、利用できるデータの量と種類が加速度的に増加した結果、サイバー犯罪に対する脆弱性も拡大しています。とりわけ、ネット犯罪における最大の標的であるヘルスケア・データは、単体のクレジットカード・データの10倍の価値があります。

そして、ヘルスケア記録内にある個人データは最も価値の高いものです。なぜなら、これらは偽のIDや保険金請求書の作成など、さまざまな悪意ある目的に使用できるからです。

脅威には、ウィルス、ワーム、ハッカーの侵入などによる悪意あるサイバー攻撃も含まれます。ネット犯罪者は、屋根裏部屋のハッカーから国家的犯罪組織に至るまで多岐にわたります。

2017年5月のWannaCryランサムウェアなどのサイバー攻撃では、最も大規模で最先端の企業でも、サイバー攻撃による混乱に対して脆弱であることが明らかになりました。このとき、いくつかの病院では別のクリニックへの患者の避難を余儀なくされました。

そして現在、COVID-19がもたらしたリモート・ワークやEコマースの大幅な増加がサイバーセキュリティに関する数多くの新たな課題を招いています。

2. サイバーセキュリティにおけるフィリップスの取り組み

フィリップスは、消費者と医療従事者が今まで以上に簡単に、適切な情報に基づいた意思決定を行えるように支援するイノベーションを提供しています。ヘルスケアのイノベーションを実現するうえで最も効果的で有望な方法の1つは、ビッグ・データを活用する大規模な研究グループで研究を行うことです。

フィリップスの戦略と競争力は、**データ、デジタル・イノベーション、消費者の信頼によって大きく左右されます。**

フィリップスは、最も機密性が求められる個人データの1つである健康関連のデータを扱っています。**フィリップスのお客様は、フィリップスのセキュリティ対策や個人情報保護対策について、今まで以上に高いレベルの保証を求めています。**フィリップスの個人情報保護対策は、パートナー企業とのビジネスを決定するうえでも今まで以上に重要なものになっています。

お客様や消費者の懸念や、相互に接続された今日のデジタル・エコシステムにおいてセキュリティが果たす役割の重大さを考慮し、フィリップスは、製品、ビジネス（エンタープライズ情報）、そして個人（患者）データの安全性を保証する**包括的なセキュリティ・プラン**の導入に注力しています。

フィリップスのセキュリティ・プランは、フィリップスの**社員、プロセス、技術**を包含するもので、重要データとそれを格納したシステムの**機密性、完全性、可用性**を確保することを目的としています。

エンドツーエンドで、設計から生産、サポートまでを網羅する**Security Designed In**（EUでは**Security by Design**）と呼ばれる概念が、フィリップスの製品、サービス、ソリューションの長期的な成功を実現するうえで重要な役割を果たしています。

安全性や品質と同様、セキュリティは、フィリップス・ブランドの信頼性を維持するうえで欠かせない要素です。**お客様や消費者に、フィリップスの製品やサービスのセキュリティ、安全性、品質を信頼していただくようにしなければなりません。**そのため、これからもフィリップスは、コネクテット・ヘルス・テクノロジーのメリットを積極的に紹介しつつ、お客様が信頼できる安全なシステム構築への投資を続けていきます。

「フィリップスの製品とサービスは最先端のセキュリティを備えている、というお客様の期待に応え続ける必要があります」

Gal Gnainsky
フィリップスセキュリティ最高責任者

3. 透明性、コンプライアンス、そしてその先へ

フィリップスは、厳しく規制された医療機器業界でセキュリティ対策を実施しています。アメリカ食品医薬品局などの規制機関は、ハードウェアおよびソフトウェアをリリースおよび変更する際には、対象となるすべてのフィリップスの製品およびサービスにおいて**安全性、セキュリティ、有効性、品質、パフォーマンスにおける高い基準**が満たされるように、厳格な検証および妥当性確認を行うことを求めています。

フィリップスは、事業を展開する国において適用されるすべてのプライバシー規制に**準拠**し、すべての個人データを完全性を保ちながら処理します。

フィリップスはまた、**脆弱性の報告と修正についてのオープン性と透明性の維持**に注力しつつ、強固な協調的な脆弱性の開示プロセス（旧名：「責任ある開示」）を開発してきました。

フィリップスの戦略は、新たに出現する脆弱性と外部の潜在的脅威にしっかりと対応することだけでなく、規制機関、業界のパートナー企業、ヘルスケア・プロバイダなどと**連携し、責任を持って**セキュリティの抜け道を修復して保護を実施することです。

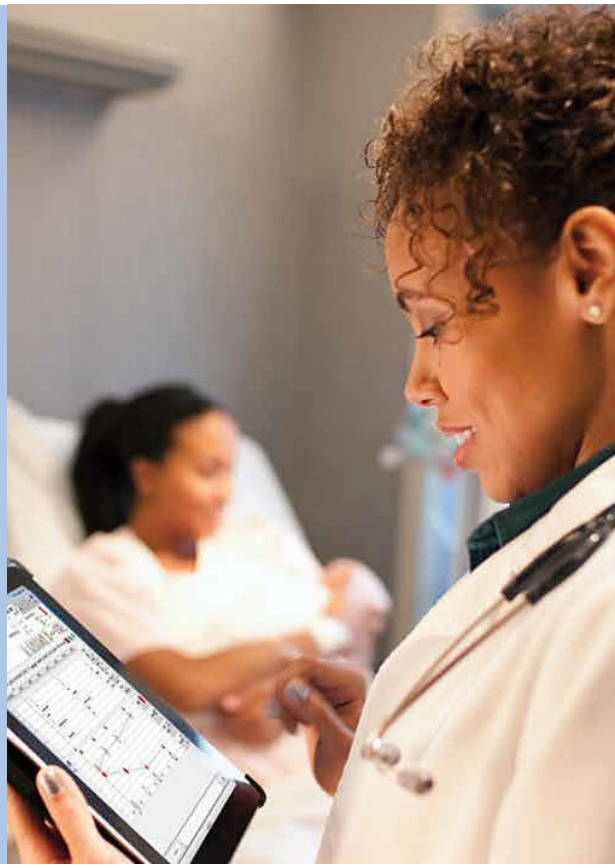
さらなる対策として、フィリップスはセキュリティやプライバシーの問題解決に注力している**業界の主要なグループに積極的に参加**しています。フィリップスはまた、適切かつ必要な、お客様向けのセキュリティ要件を、業界の基準、ガイドライン、イニシアティブに必ず含めるための努力を続けています。

フィリップスは、アメリカ合衆国保健福祉省（HHS）のサイバーセキュリティ部会の**創設メンバー**であり、複数の標準化団体（ISOやIECなど）を通じて**（ヘルスケア）セキュリティ標準の策定**にも深く携わっています。

さらに、**世界経済フォーラム**の「サイバーセキュリティに対する官民パートナーシップに関する提言」への支援も行っています。

「お客様と協力して透明性を確保することで患者様の安全を確保し、製品とサービスのセキュリティを進化させ続けています」

Dirk de Wit
フィリップス製品セキュリティ責任



4. 製品のセキュリティ

フィリップスは、フィリップス製品に対するサイバーセキュリティ[1]上のリスクの高まりを極めて深刻に捉えています。フィリップスはまた、フィリップスのソリューションおよびサービスに依存している患者のリスクを最小限に抑えるプロセスとシステムを継続的に向上させる取り組みを、長期にわたって続けてきました。

フィリップスは、さまざまな業界で巧妙なサイバー攻撃が、とりわけヘルスケア分野で増加していることを強く認識しています。院内ネットワーク、臨床データベース、医療機器、パーソナル・ヘルス・モニタリング・システムの統合が進むにつれ、サイバーセキュリティの潜在的な脆弱性も高まります。

フィリップスは、効果的なサイバーセキュリティとは「箱」、つまり個々の製品を保護することではなく、どこで、どのように機器が使用されるかを考慮した体系的なアプローチにあるということをいち早く認識していました。**フィリップスにおける「Security Designed In」とは、エンドツーエンドのコンセプトを意味します。つまり、セキュリティ原則の実装は、製品の設計と開発から始まり、テストおよび製品の展開時を経て、その後、強固なポリシーおよびモニタリング手順の確立、効果的な更新作業、さらには必要に応じたインシデント対応管理に及びます。**

フィリップスの製品とサービスをサイバー攻撃の脅威から守るには、リスク評価に対する揺るぎない注力、およびセキュリティベースの製品開発への順守が必要になります。そのためには、暗号化やパッチ管理などのセキュリティ対応技術の迅速な展開、およびこれらの継続的な改良が必要になります。フィリップスが、フィリップスの製品およびソリューションのセキュリティ・プログラムを一任し、包括的で効果的なアプローチを作成、実装、更新してお客様の要件に対応しているのはこういった理由からです。

フィリップス製品のセキュリティに対する主要なイニシアティブ:

業界で最先端のフィリップス製品セキュリティ・ポリシーを公開しています。このポリシーでは、組織がセキュリティにおけるベスト・プラクティスを実施できるようにするためのポリシー、手順、基準が定義されています。

フィリップスの戦略的な組織体制とプロシージャーの定義付け:

- フィリップス製品セキュリティ・ポリシーの下で運用される、セキュリティおよびプライバシーに関する専門家のグローバル・ネットワークの維持
- フィリップスの製品およびサービスにおけるベスト・プラクティスの開発および展開
- 潜在的および特定済みのセキュリティ、プライバシーの脅威および脆弱性に関するリスク評価とインシデント対応
- 製品およびサービスの特定済みの脆弱性に対するリスク評価とリスク対応を含む、ライフサイクル中における製品およびサービスに埋め込まれたセキュリティ機能の管理

現行の規制上の要件および業界のベスト・プラクティスを満たすか、それを上回るセキュリティ標準の実装:

- FDA推奨の標準に準拠しているだけでなく、80001-2-2標準の基礎としても使用される製品およびサービスの製品セキュリティの実現
- NIST 800-53、ISO/IEC-27000シリーズ、HiTrustなどの認定済み標準に準拠したサービス・セキュリティの実現
- Manufacturer Disclosure Statement for Medical Device Security（MDS[2]：医療機器のセキュリティに関する製造業者の開示宣言）などの顧客対応情報の作成
- 医療機器のサイバーセキュリティに対応するFDA、MDR、その他の国のガイダンスのサポート
- フィリップスは2020年3月に医療機器製造業者として初めて、Underwriters Laboratories（UL）による新しい製品サイバーセキュリティ・テスト認証を取得。UL IEC 62304認証は、医療機器製造業者のサイバーセキュリティ制御および製品開発能力の堅牢性と成熟度を評価する総合的なフレームワークを提供。

フィリップスのSecurity Center of Excellenceは最先端のサイバーセキュリティの研究者やテスト施設と情報を共有し、サイバー攻撃の脅威を迅速に除去、低減、緩和するためにサポートします。

フィリップスがIEC 62304のセキュリティ・オプションの認証を取得できるようサポートするため、ULはフィリップスのSecurity Center of Excellenceの包括的な監査を実施しました。監査では、フィリップスSecurity Center of Excellenceの中核となる製品セキュリティのプロセスについて、セキュリティのリスク管理とリスク制御の対策、ソフトウェア・セキュリティ検証計画、変更管理と継続的改善、センターのラボ品質管理システムなどを検証および評価しました。

脅威、脆弱性、およびセキュリティ上のインシデントのモニタリングと対応

- フィリップスは、新種のセキュリティの脅威、脆弱性、セキュリティ上のインシデントを継続的にモニタリングしています。オペレーティング・システムやその他サード・パーティ製ソフトウェアのベンダー、さらには、お客様やセキュリティ研究者が突き止めた脆弱性もモニタリングの対象となります。
- フィリップスの製品セキュリティ・インシデント対応チームは、潜在的なセキュリティ・インシデントおよび特定された脆弱性を評価し、必要に応じて対応計画を練ります。

マルウェア対策ソフトおよびパッチ管理：

- フィリップスは、市販のマルウェア対策ソフトに対応した製品を、インストール済みのマルウェア対策ソフト、または製品固有のフィリップス承認済みのマルウェア対策ソフトのパラメータを詳述したお客様向け文書とともに提供します。
- フィリップス製品は、Microsoft WindowsやLinuxなどのオペレーティング・システムをはじめとするサード・パーティ製ソフトウェアを活用する場合もあります。新たなセキュリティの脆弱性やパッチの可用性が認められると、フィリップス製品のエンジニアリング・チームによるホットフィックスの影響評価が通常48時間以内に開始されます。

特定された脆弱性の報告および対応を行うための責任ある開示ポリシー：

- フィリップスは、責任ある開示ポリシーの設計および実装を行っています。これは、業界におけるベスト・プラクティスとして評価されています。
- フィリップスの責任ある開示ポリシーは、お客様、研究者、その他のセキュリティ・コミュニティのステークホルダーを対象としてクリアな通信チャネルで公開されています。
- このポリシーには、インバウンド通信のモニタリングと対応、フォローアップの管理、脆弱性通知と状況追跡の評価、インシデント対応の順守、修復と予防に関するポリシーが含まれています。

フィリップスは、医療機器製品のセキュリティ精神を定着させるための長期的な戦略と効果的な手法を開発し続けていきます。この重要な役割を担い続けることで、数十億人もの世界中の人々の生活を豊かにしたいと考えています。

1. サイバーセキュリティは、ネットワーク、コンピュータ、プログラム、データをサイバー攻撃やこれによる被害、不正アクセスから守るために設計された技術やプロセス、プラクティスの核となります。http://whatis.techtarget.com/definition/cybersecurity

「デジタル化により、フィリップスの製品やサービスを自社のエンタープライズ·システムに接続したうえで、サプライヤ / パートナーのシステムにつなぐことができます。これにより、人が介在しないシームレスな情報の流れが可能になります。そのためには、エンドツーエンドのセキュリティを確保する必要があります」

Stef Hoffman
フィリップス情報セキュリティ最高責任者

5. エンタープライズ情報セキュリティ

フィリップスは、フィリップスの革新的技術に対するフィリップスのお客様の長きにわたる信頼感をベースとして成長を続けてきました。その技術の設計、開発、生産は、社内の高度な情報システムによって支えられています。

このような技術と関連データを標的としたサイバーセキュリティの脅威が拡大を続けている現在、フィリップスの情報セキュリティ組織はエンタープライズ向け情報システムを保護し、以下を保証することを目的として活動しています。

- **フィリップスのお客様の信頼**：フィリップス·ブランドが、安全性、品質、セキュリティと同義になるよう努力を続けます。
- **成長を続ける力**：機密情報の損失を防止することで、企業の長期的な競争力を保証します。
- **フィリップスの財務実績**：企業の資産を保護し、お客様の喪失や利益および収益の損失を含む、財務的なマイナスの影響を防ぎます。
- **フィリップスの安定した経営**：不可欠なインフラストラクチャの劣化や破壊を防ぎ、安定した経営を維持します。
- **フィリップスの規制への準拠**：情報システムが、すべての規制要件に準拠するか、これを上回ることを保証します。

情報セキュリティの課題は、技術のみでは解決できません。包括的な情報セキュリティでは、3つの分野に焦点を当てる必要があります。つまり、人、プロセス、そして技術です（次ページを参照）。フィリップスの情報セキュリティ担当組織は、これら3つの分野を管理することで、次のことを保証しています。

- **機密性**：アクセス権を持つユーザーのみが、データを取得できます。
- **完全性**：検知されずに情報を修正することはできません。
- **可用性**：必要に応じて情報にアクセスできます。

フィリップスは、拡大を続ける脅威の課題への対処を今後も続行し、エンタープライズ向けの情報システムを安全に保ち、お客様の信頼を向上させます。フィリップスの情報セキュリティ担当組織は、今後も、一流のサイバーセキュリティ能力を保持するための投資、サイバーセキュリティのツール活用の促進とその能力の向上、そしてフィリップスが行うことすべてにおけるあらゆるセキュリティ·ベスト·プラクティスの活用に注力します。

情報セキュリティにおける人、プロセス、技術への注力

人

従業員の行動に注目することで従業員のセキュリティへの態度を改善し、結果としてセキュリティ文化を発展させます。

プロセス

フィリップスのビジネス・プロセスに注目して、セキュリティ・リスクを評価し、適切なリスク軽減手順をプロセスに統合することでリスクを軽減します。

技術

フィリップスの技術の全容の把握とモニタリングに注力し、技術の向上を促進してセキュリティ･リスクへの姿勢を改善します。

6. プライバシー

フィリップスは、お客様、消費者、患者などの関係者のプライバシーを尊重することに長い間尽力してきました。また、個人データへの対処方法についての透明性を保つことで、フィリップスへの信頼を勝ち取ってきました。フィリップスがデジタル企業へと変わりつつある中、フィリップスのプライバシー基準に準拠することの重要性がますます高まっています。そのために、フィリップスではデータ原則を採用しました。この原則の1つはプライバシーに関するものです。

ヘルス・テクノロジに注力するうえで、データのプライバシーとセキュリティは戦略的な意味で欠かせないものになっています。健康関連のデータは、個人データの中でも最も機密性が求められるデータだからです。フィリップスの競争力は、これらのデータに大きく依存しています。社会的な信頼こそが、フィリップスの最優先事項だからです。**フィリップスのプライバシーへの取り組みはデータ原則に盛り込まれています。**この原則を通じて、フィリップスは、事業を展開する国において適用されるすべてのプライバシー規制に準拠し、すべての個人データを完全性を保ちながら処理することを約束します。

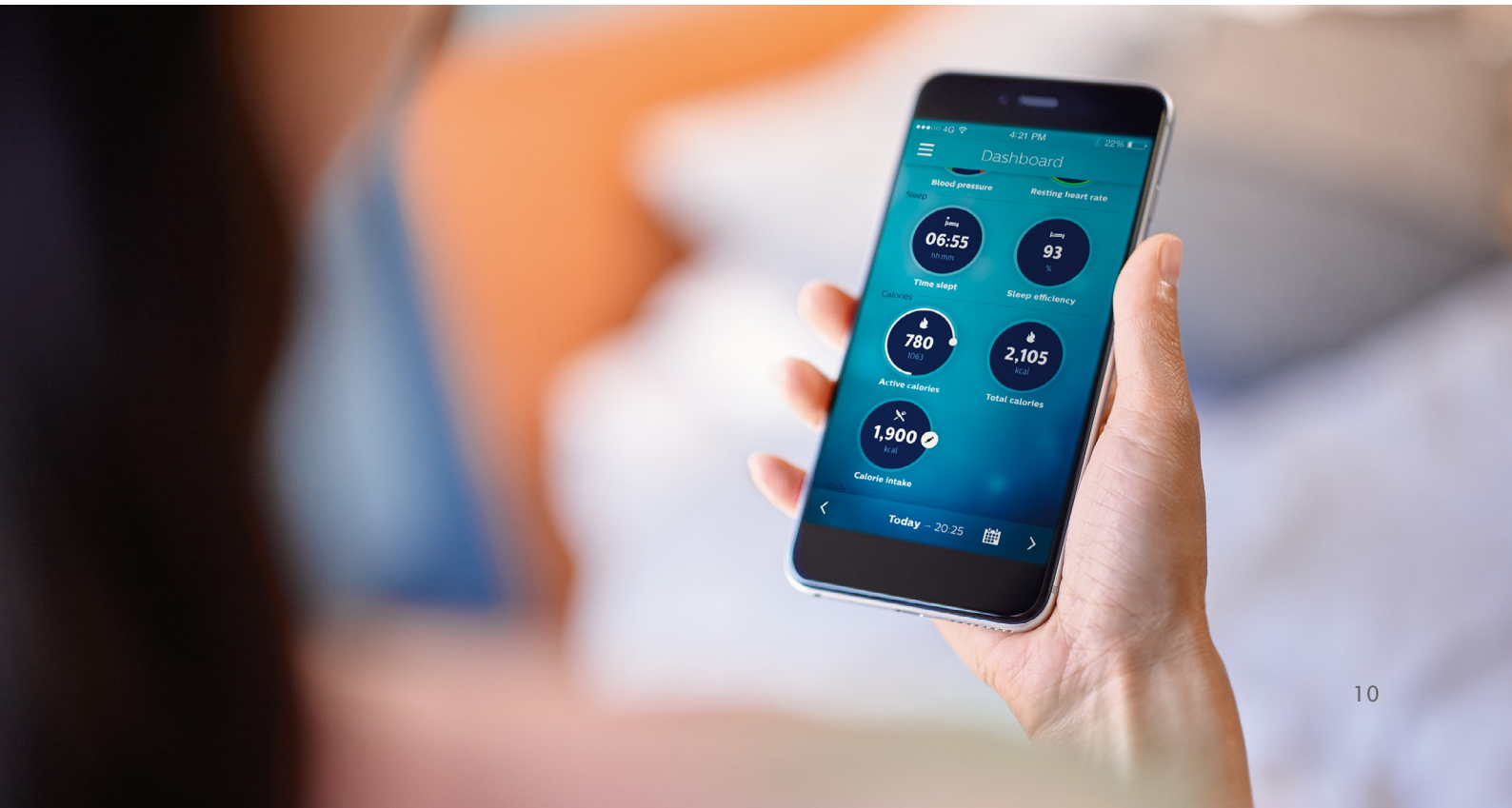
プライバシーとデータの保護は、フィリップスの**一般的なビジネス原則**において不可欠な要素です。一般的なビジネス原則では、フィリップスは以下の要件に従っています。

- 世界中のフィリップス社内で個人情報保護の基準を示し、フィリップス・グループ企業間の国をまたがったデータの受け渡しを可能にする拘束的企業準則（BCR）の確立
- 企業内にプライバシーとデータの保護を組み込んだプライバシー・プログラムとガバナンス体制の確立
- 個人データの収集に対する制限
- 個人データの処理に関する個人への通知
- 個人によるデータ主体の権利のグローバルな行使の保証
- データが正確かつ最新であることを確認するための適切な手順の実行
- 適切なセキュリティ保護に基づく個人データの保護

フィリップスはグローバル企業として、すべての国のプライバシー法とデータ保護法を考慮に入れる必要があります。フィリップスのBCRとプライバシー・プログラムは、プライバシー法が存在しない国を含め、世界中のフィリップス社内におけるプライバシー法への確実な準拠を意図して作成されています。

フィリップスは、**「プライバシー・バイ・デザイン」**の原則に基づいて、高いセキュリティ基準と責任あるデータ・スチュワードシップへの準拠に注力しています。このアプローチは、初期の設計段階から展開、収集、使用、データの処分に至るライフサイクル全体を通じてプライバシーとデータの保護管理を組み込むことを目的としています。

ビッグ・データを活用してヘルスケアの分野で前進するには、信頼を醸成し、個々のお客様に価値を説明していく必要があります。フィリップスはまた、プライバシーとデータ保護への基本的権利を保証する必要があります。そして高いセキュリティ基準と責任あるデータ・スチュワードシップへの準拠に注力することで、フィリップスはセキュリティに対する恐怖や疑念を取り払い、継続的なイノベーションを通じてより大きな価値を消費者にもたらすことができるようになります。



7. 適切な体制とメカニズム

- **拘束的企業準則（BCR）**は、フィリップス社内で個人データを取り扱う際の社内ルールであり、フィリップス・プライバシー・ルールとも呼ばれるものです。フィリップス・プライバシー・ルールは、主にEUデータ保護要件とOECDプライバシー原則に基づくもので、フィリップス社内における強固なデータ保護の枠組みを規定しています。フィリップス・プライバシー・ルールはまた、グローバルなデータ保護要件を規定しています。これらの要件は全世界のフィリップス社内で適用され、フィリップス社内で国をまたがった個人データのやり取りを可能にするものです。

- フィリップスに代わって個人データを取り扱う**サプライヤ**は、フィリップスのBCRで規定された厳しい要件に順守することに同意する必要があります。

- フィリップスは、プライバシー、製品セキュリティ、情報セキュリティの卓越性について中心的な役割を果たしてきました。**Philips Global Privacy Office**は、フィリップスの従業員によるプライバシー・コンプライアンスの順守を支援し、プライバシー・コンプライアンスとリスク管理のグローバルな枠組みを確立します。

- **Philips Product Security**は、ライフサイクル全体において製品とサービスに組み込まれたセキュリティを管理します。これには、製品セキュリティのリスク評価、プロジェクトと無関係の脆弱性および不正アクセス侵入度に対する評価、専門の製品セキュリティ・トレーニング、サポート対象の既存の製品およびサービスで特定済みの脆弱性に対する対応業務が含まれます。

- フィリップスは、製品および情報セキュリティに対して総合的な、エンドツーエンドのアプローチを取っています。また、製品の開発ライフサイクルの各手順を高いレベルの機密性と完全性に基づいて確実に実施するための、適切なプロセスと枠組みを備えています。セキュアな製品開発ライフサイクルの一環として、フィリップスは継続的に脆弱性をモニタリングして修正内容を検証しています。これらの業務は、フィリップス社内のSecurity Center of Excellenceがサポートしています。

- フィリップスはまた、個人データの保護、フィリップス・プライバシー・ルールおよび該当するデータ保護法に準拠する際に必要な手順に関する**全従業員を対象としたトレーニング・プログラム**を用意しています。個人データを取り扱う従業員は、
データを正しく取り扱うための、役割ベースの特別なトレーニングを受けます。さらにフィリップスでは、フィリップスの開発チーム専用のセキュリティ・トレーニング・プログラムも行っています。

- **HealthSuiteのデジタル・プラットフォーム**について、フィリップスは、サード・パーティの一次プロバイダ（Amazon、salesforce.comなど）との間で複数の技術サービスのホスティング契約を結んでいます。これらのプロバイダは、独立した立場の監査役によって、ISO/IEC 27001、および必要に応じてその他の該当するセキュリティ基準（HIPAA/HITECH、SSAE No. 16、NIST SP800-53など）に従った監査を1年に1回実行する義務を負います。

8. 詳細情報

フィリップス製品のセキュリティ情報フィリップスの プライバシー・ポリシーに関するWebページ

付録：
製品のセキュリティに関する声明

製品のセキュリティに関する声明

このセクションでは、フィリップスの製品、サービス、アプリケーション、システムのセキュリティに対するフィリップスの見解をまとめています。また、製品に**Security Designed In**を提供するためのプロセスについても説明しています。

背景

フィリップスは、フィリップスのヘルスケア、個人の健康、家庭用消費者向けの製品およびサービスが、お客様のセキュリティ計画の作成において重要な役割を担っているということを認識しています。また、個人データ、業務データ、そしてこのデータを作成および管理するフィリップスのハードウェアおよびソフトウェア製品の機密性、完全性、可用性をお客様が維持できるように尽力しています。

機器、個人情報、ヘルスケア情報のセキュリティに対する脅威は拡大する一方です。これらの脅威には、ウィルス、ワーム、ハッカーの侵入などによる悪意あるサイバー攻撃が含まれます。世界各国の政府は、これらのサイバー攻撃の多くを違法とし、個別に特定可能な健康情報を保護する法令を制定してきました。米国のHIPAA、カナダのPIPEDA、EUのGDPR、日本の個人情報保護法（PIPA）などがその例です。

セキュリティへの注力を高めるうえで、フィリップスは以下を目的としたグローバル・プログラムを用意しています。

- フィリップスの製品とサービスに対する先進セキュリティ機能の開発、展開、サポート
- 現場でのセキュリティ・イベントの管理。フィリップスは、業界と政府間のコラボレーションに参加し、製品のイノベーションと、臨床情報が、最高レベルの品質、可用性、機密性で生成および利用されることを支援しています。

フィリップスはまた、厳しく規制された医療機器業界、およびそのような世界的な潮流の中でセキュリティ対策を実施しています。アメリカ食品医薬品局などの政府の規制機関は、ハードウェアおよびソフトウェアをリリースおよび変更する際には、すべてのフィリップスの医療機器において安全性およびパフォーマンスにおける高い基準が満たされるように、厳格な検証および妥当性確認を行うことを求めています。[1] さらにフィリップスは、個人向けヘルスケア製品、家庭向けイノベーションおよびサービスについても高い基準を保証すべく尽力しています。

組織

フィリップスは、グローバルな製品セキュリティ・ポリシーに基づいて業務を行っています。このポリシーには、製品およびサービスの作成時に必要な「セキュリティ対応設計」、既存の製品で特定済みの脆弱性に対するリスク評価、インシデント対応業務が明記されています。グローバル製品のセキュリティ責任者は、このポリシーのガバナンスとコンプライアンス状況を監視しつつ、フィリップスの製品 & Innovation Excellence責任者に直接報告を行っています。フィリップスは、グローバル製品セキュリティ・プログラムのもとで、グローバルなモニタリング、ケースのエスカレーション、迅速な応答、セキュリティに関する問題の管理業務を完全に可視化するシステムの確立および向上に力を注いでいます。

目次

背景 13

組織 13

目次 14

デジタル革命 15

接続 / 相互接続されたエコシステム 15

モノのインターネット（IoT） 15

フィリップス製品セキュリティ・プログラムの主要な要素 16

ガバナンス 16

テスト 17

協調的な脆弱性の開示 17

Software Bill of Material（SBOM） 18

成熟度ロードマップ 18

動作中のフィリップス製品のセキュリティ 18

製品セキュリティ評価 / 製品設計 18

インシデントおよび脆弱性に対するモニタリングおよび対応 18

Philips Secure Development Lifecycle（SDLC） – Security by Design 19

フィリップス・オープン・ソース・ガバナンスおよびコンプライアンス・プログラム（SBOMのガバナンス） 19

オペレーティング・システムとパッチ管理 20

マルウェア対策 21

Philips Product Security Webサイト 21

医療機器MDS²フォーム 21

製品のセキュリティに関するご協力のお願い 22

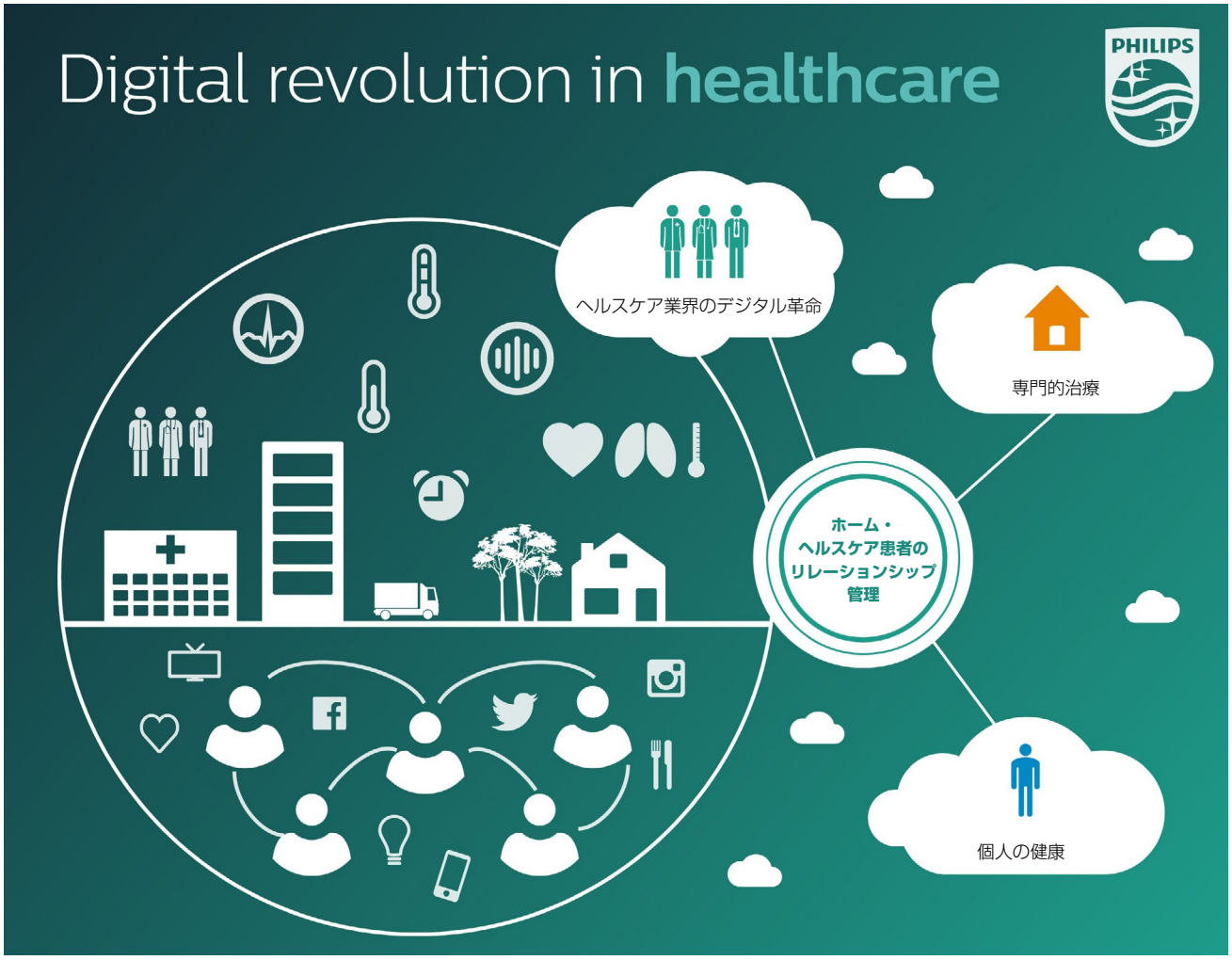
サード・パーティ製ソフトウェアおよびパッチに関するポリシー 22

一般的ケース 22

例外的ケース 22

フィリップス・リモート・サービス 23

変わりゆく世界におけるフィリップス製品のイノベーションとソリューション 23



接続 / 相互接続されたエコシステム

ネットワークに接続された数百万に及ぶデジタル機器の普及により、各ユーザーはネットワーク上で、膨大なデータフローを共有、検索、ナビゲート、管理、比較、分析できるようになりました。このデジタル「エコシステム」に基づいて、ヘルスケア業界は、パーソナライズされたヘルスケア指向のスマート・デバイスのポートフォリオを拡張し、イノベーションを起こし、サービスの効率性を向上させています。一方で、ユーザーが脆弱性とサイバー攻撃にさらされるリスクが大幅に高まりました。

ヘルスケア業界では、相互接続、相互運用、リモート制御された製品とサービスが急増しています。とりわけ脆弱性が高いと考えられているのは以下の領域です。

- プロバイダのネットワーク
- 個人の健康用機器
- リモート・サービス
- 機密データの保管
- 移動中の機密データ

セキュリティで最も重視すべきことは、エコシステム内のお客様ネットワークおよび個人または患者データの保護です。この課題に対処するため、フィリップスなどのOEMは、製品のセキュリティに関して戦略的で統一された見解を持ち、包括的なリスクベースのサイバーセキュリティ・プログラムを確立する必要があります。

モノのインターネット（IoT）

モノのインターネット（IoT）のパラダイムでは、現在および将来のインフラストラクチャにおいて、相互接続とスマート技術の連携が拡大していくものと予測されています。[2]データ交換技術の革命的進歩により、人々の健康は大きく向上しています。人々はタブレット、ウェアラブル、携帯機器などのネットワーク接続された機器を使用して、高度にパーソナライズされた方法で自らの健康を管理できるようになっています。たとえばフィリップスは、業界内のパートナー企業と連携し、HealthSuiteデジタル・プラットフォームを開発しました。このプラットフォームは、IoT機器およびアプリケーションを、詳細なデータセットと連携させながら動作できるようにしています。HealthSuiteデジタル・プラットフォームは、次世代のセキュアなコネクテッド・ヘルスケア機器およびアプリケーションを開発、実行するために必要なネイティブのクラウドベースのインフラストラクチャとコア・サービスを提供します。

撮影装置、モニタ、携帯型の個人用機器で収集した電子医療記録や診断記録の分析は、医療従事者の意思決定能力を高めただけでなく、患者自身が健康を管理するうえで、より重要な役割を果たすようになりました。これらのイノベーションは、慢性疾患患者のケアにとどまらず、健康を維持したい健康な人々の生活にも変化をもたらしています。

急速な進化を続ける環境下で動作する次世代のモバイル・アプリ、サービス、ハードウェアは、厳格なリスク分析、およびセキュリティ侵入テストをパスする必要があります。これからの機器は、ユーザーを特定し、同意を承認し、ユーザーの活動を追跡してデータ保護を保証するセキュアな防御フレームワークで保護されることになるでしょう。

フィリップス製品セキュリティ・プログラムの主要な要素

ネットワーク接続された、相互運用可能なヘルスケアのエコシステムでは、脆弱性と攻撃にさらされる潜在的リスクが高まっています。この現状を考慮し、フィリップスは広範なリソースをつぎ込むことで脅威の軽減に努めています。製品のセキュリティ機能およびイノベーションについて、業界のリーダーとして長きにわたり研究を重ねてきたフィリップスは、セキュリティ・プログラムを成功に導くために不可欠となる以下の5つの要素を提唱しています。

1. ガバナンス
2. テスト
3. 協調的な脆弱性の開示
4. Software Bill of Material（SBOM）
5. 成熟度ロードマップ

ガバナンス	• **組織の提携** • **ソート・リーダーシップ（情報共有、学習）** • **主要な製品セキュリティ・リスク・ドライバーの実施** • **「有言実行」**ポリシー / 品質、リスク評価、セキュアな開発、コード分析、モニタリング、トレーニング、イベント対応
テスト	• **侵入テスト** - 倫理的ハッカー • **リスク評価、セキュアな開発ライフサイクル（SDLC）、新人研修、メンテナンスへの統合** • 一般的で比較可能な結果に対する標準化された使用事例とツールの活用
協調的な脆弱性の開示	• **ポリシー**およびお客様苦情処理プロセスへの統合および効果的なインシデント対応管理プロセスの活用
Software Bill of Material（SBOM）	• **新たな脆弱性とセキュリティ・ソフトウェア更新用の**Software Bill of Material（SBOM）の継続的モニタリング • SDLC（市販前、市販後）全域で**トレーニング**と実践を統合
成熟度ロードマップ	• **レガシー製品とSBOMライフサイクルの管理** • **継続的イノベーション – プログラムの評価およびモニタリング**

ガバナンス

フィリップス社内の経営幹部が一致団結することで、成功へと前進するうえで必要となる「積極的な参加」が確かなものとなります。この社内チームが継続的に管理を行い、製品セキュリティ・プログラムの重要な特性（セキュリティの継続的な向上を実現するためのポリシー、リスク評価、セキュリティ・テスト、コミュニケーション、ステークホルダー要件、インシデント管理、メトリクス、成熟度ロードマップを含むプログラム）の導入を成功させるための戦略と体制を構築しています。

このチームは、継続的な対話を通じ、サイバーセキュリティのエコシステム（お客様、ベンダー、規制機関、標準化機構、業界団体、研究者など）内の社外関係者の取り組みをコーディネートします。この試みは、重要な関係を構築し、個人用機器および医療機器の安全性およびセキュリティに対するベスト・プラクティスを推進するうえで極めて生産的なものです。たとえば、フィリップスはアメリカ合衆国保健福祉省（HHS）のサイバーセキュリティ作業部会に参加している医療機器メーカー2社のうちの1社です。

包括的なリスク管理戦略のガバナンスは、フィリップス製品セキュリティ・プログラムの中核であり、フィリップスのミッションでもあります。この戦略では、市販前、市販後の製品セキュリティ・リスクに対する予防、軽減、修正を行うための総合的なリスク管理プロセスを扱っています。

主要な評価済みのリスクにプロアクティブに対応するための戦略を一貫して採用することが、安全かつセキュアな製品とサービスを実現し、データ漏洩、サード・パーティに起因する脆弱性、規制機関およびお客様による制裁措置に潜在的にさらされるリスクを低減するうえで不可欠です。

テスト

医療機器業界の**No.1**企業であるフィリップスは、「サイバーレジリエント」な製品の開発を目的としたSecurity Center of Excellence（SCoE）を立ち上げました。SCoEは、倫理的ハッカー、あるいはセキュリティ忍者とも呼ばれる専門チームであり、脆弱性テストおよび侵入テストを継続的に実施し、製品のセキュリティ・ホールを事前に特定します。SCoEは、フィリップス製品のエンジニアリングおよび開発チームの製品セキュリティ・テストを補完し、強化しています。SCoEのテスト・プロセスとテスト結果は、一般的な対応アプローチを標準化した使用事例のシナリオに明示されています。これらは全世界のフィリップスで活用され、リスク評価、Philips Secure Development Lifecycle（SDLC）、保守手順に統合されています。

フィリップスの製品およびサービスのセキュリティ・テストは、以下のような多様なサイバーセキュリティのタスクを対象としています。

- セキュリティの脆弱性テストおよび侵入テスト
- セキュリティ・リスクの評価
- セキュリティ用ソース・コード分析
- サード・パーティ・ベンダーへの関与
- 米国国防総省（DoD）向けの技術的製品セキュリティ・テスト
- 製品アーキテクチャ、開発、テストなどの独自の役割に特化したセキュリティ業務のトレーニング
- ツールの検証
- ツールの評価
- 脅威のモニタリング
- 製品開発のメトリクス

協調的な脆弱性の開示

協調的な脆弱性の開示プログラムの開発は、協調的な脆弱性の開示（旧名：「責任ある開示」）ポリシーの作成により始まりました。このポリシーでは、お客様に対し、あらゆる脆弱性の修復と将来的な損失の防止のために適切な取り組みを行うことをあらためて保証しています。

同様に、切迫感と敏感さを持ってすべてのセキュリティ・インシデントに対処することが重要です。フィリップスは、全通信の文書化、是正プログラムの開示、ソリューションの開発、インシデント・レポートの認可などをはじめとする正式なインシデント対応管理プロセスをすでに実施しています。

確認された脆弱性は、米国のDHS（ICS-CERTプログラム）などの政府機関に直接報告し、公開されます。米国FDAの市販前、市販後の「医療機器のサイバーセキュリティ管理」のガイドライン（2016年12月28日）では、米国以外の政府機関およびプロセスと連携し、全世界で採用可能な主要原則についての指示を明記しています。その中で重要なものは、透明性の維持です。

フィリップスは、協調的な脆弱性の開示ポリシーを設計および実施した最初の大手企業です。そして現在においても、フィリップスのポリシーに基づき、完全に開発済みで運用上成熟したプロセスを備えた、全世界で認知された業界のリーダーとしての地位を保っています。報道機関の意識がセキュリティ・インシデントに向かっている中、フィリップスは困難な問題に対し準備を重ねてきた製造業者としてしばしば評価されています。

「フィリップスは、**脆弱性に対する警告**への対応が評価された唯一のベビー・モニター・メーカーである」
– **Forbes**

「この脆弱性の解消と、**新たに発生する製品の脆弱性**に対処するためのプロトコルの確立に尽力したフィリップスの姿勢は評価に値する」
– **ARS Technica**

「フィリップスは、あらゆる企業の中で、不具合の対処において**最も迅速に対応する**企業である」
– **Wall Street Journal**

関連記事については、「インシデントおよび脆弱性に対するモニタリングおよび対応」のセクションをご覧ください。

Software Bill of Material（SBOM）

統合されたサード・パーティ製ソフトウェアに依存しているフィリップスやその他の企業は、サード・パーティのプログラミング・コードによる潜在的リスクにさらされています。このグローバルな問題に関する審理中の法案に備えるには、全製品を対象とするSoftware Bill of Material（SBOM）の作成が不可欠となります。SBOMは、オープン・ソースとサード・パーティ製ソフトウェアのコンポーネントを特定して説明するものであり、潜在的なセキュリティ違反と脆弱性に組織が迅速に対応できるようにするものです。

フィリップスは、業界で先駆けてすべてのフィリップス製品のSecure Development Lifecycle（SDLC）にSBOMを統合しています。フィリップスは、ソフトウェア、ファームウェア、フィリップスのお客様向けに開発された製品の完全性を保証するのに必要となるプロセスと手順を確立する予定です。

関連記事については、「フィリップス・オープン・ソース・ガバナンスおよびコンプライアンス（SBOMプログラム）」をご覧ください。

成熟度ロードマップ

製品セキュリティを製品の開発フェーズで統合し、全ポートフォリオで製品セキュリティのプロセスを着実に実施することで、将来の管理機能完成への目途が整います。成熟度ロードマップの目的および意図は、フィリップスのプロセスおよび組織的機能を測定し、向上させることにあります。フィリップスの最終的な目標は、新製品の導入、現行サービスの運用、市販後のライフサイクル管理における製品セキュリティの成熟度を向上させることです。

この取り組みの一環として、フィリップスは包括的な製品ライフサイクル管理のセキュリティ戦略の確立に注力しています。まず、インストール済みのベース製品およびレガシー製品の評価およびモニタリングを開始してOSの陳腐化と非互換性、ハードウェアおよびファームウェアの脆弱性を検知します。次に、継続的で、必要に応じた保守と更新、ライフサイクル・スケジューリングを実現します。

動作中のフィリップス製品のセキュリティ

製品セキュリティ評価 / 製品設計

フィリップスは、社内の製品セキュリティ評価を事前に実施して潜在的なセキュリティ・ホールを特定します。これらの情報に基づき、フィリップスのエンジニアリング・チームは適宜設定変更とリエンジニアリングを行い、外部の脅威に対するシステムのセキュリティを強化します。これらの情報はまた、すべての製品とサービスに対するフィリップスのセキュアな開発ライフサイクル・プロセスに統合される、新製品のセキュリティ設計要件のベースとなります。フィリップス製品セキュリティ・ポリシーでは、あらゆる新製品開発作業に、**Security Designed In**の目的を取り入れることを必須条件としています。

インシデントおよび脆弱性に対するモニタリングおよび対応

フィリップスの製品エンジニアリング・グループは、サード・パーティ製ソフトウェアやOSベンダーが特定したものやヘルスケア企業が報告したものを含む新しいセキュリティの脆弱性を継続的にモニタリングします。製品セキュリティ責任者のグローバル・ネットワークおよび配下の担当チームは、情報を収集、管理して、フィリップスの製品とソリューションに悪影響を及ぼしかねない特定済みの脆弱性に対処します。

リスク・イベント、サイバー攻撃、インシデントが検知または報告された場合、フィリップスの製品セキュリティ・インシデント対応チームは、明白な脅威、脆弱性、またはリスクに対するアセスメントを行うことで発生中または潜在的なインシデントを評価します。さらに、フィリップス全社のチーム間で対応を統一し、状況をシェアし、フィリップス製品セキュリティ・ポリシーの枠組みに沿ってセキュリティ・イベントを徹底的に調査して問題を解決します。

Philips Secure Development Lifecycle（SDLC） – Security by Design

業界のトレンドとしては、サイバー攻撃は製品のアプリケーション層に移行し、お客様情報や患者情報に対する重大な脅威がモノのインターネット（IoT）を介して迫っていることが明らかになっています。Internet Storm Center（ISC）が収集したデータによれば、ネットワーク上の70%以上の攻撃は、アプリケーション層を標的としたものになっています。フィリップスの製品とサービスの復元力を強化するため、フィリップスはさまざまな機能、コンポーネント、方法によって自社製品の実現プロセスを向上させています。これらの方法の中には、ソフトウェア開発プロセスでセキュリティとプライバシーを取り込むための実用的かつ十分にテストされた手段、ISO 27034などのISO規格への準拠などが含まれます。

上記の方法に基づき、セキュアな開発ライフサイクルの各フェーズにさまざまな要件と管理業務が組み込まれています。例として、Product Security Risk Assessment（PSRA）、Privacy Assessment（PIA）プロセス、静的コード分析、サード・パーティ製Software Bill of Material（SBOM）分析、倫理的侵入テスト、フィリップス全社での継続的製品セキュリティ・トレーニングなどがあります。各ツールとプロセスがPhilips SDLCの鍵である一方、Security by Designはエンドツーエンドのアプローチを求めるコンセプトです。エンドツーエンドのアプローチは、アーキテクチャおよび概要設計から始まり、コーディング、テスト、市販後のサポートまでをカバーするものです。

フィリップス・オープン・ソース・ガバナンスおよびコンプライアンス・プログラム（SBOMのガバナンス） 現在作成されているほとんどのソフトウェアには、オープン・ソースおよびその他の市販のコンポーネントが組み込まれています。これらのサード・パーティ製コンポーネントは、製造業者が把握していない脆弱性を製品にもたらしてしまうおそれがあります。Software Bill of Material（SBOM）では、アプリケーションの構築に使用されているツールを詳述しているだけでなく、組み込まれているサード・パーティ製コンポーネントを正確に記載しています。そのため、セキュリティ組織は潜在的リスクに迅速かつ正確に対応できるようになっています。

製造業者の多くは、自社の各製品の正確な部品表を備えていません。正確な部品表がないと、部品に関連する脆弱性を十分に把握できません。SBOM製品情報がない状態で脆弱性の問題に対応しても、影響を受けたコードの特定とソリューションの導入は容易ではありません。そのため、迅速な対応が著しく困難になります。

現在米国では、製品ソフトウェアのセキュリティの保証を求める法案が審理中です。Cyber Supply Chain Management and Transparency Act（サイバー・サプライチェーン管理および透明性に関する法）では、購入対象のあらゆる新製品のソフトウェアBOMを政府機関が入手することを義務付けています。さらに、「サード・パーティ製およびオープン・ソースのバイナリ・コンポーネントを含むあらゆるソフトウェア、ファームウェア、製品」のSBOMの入手も義務付けています。[1]

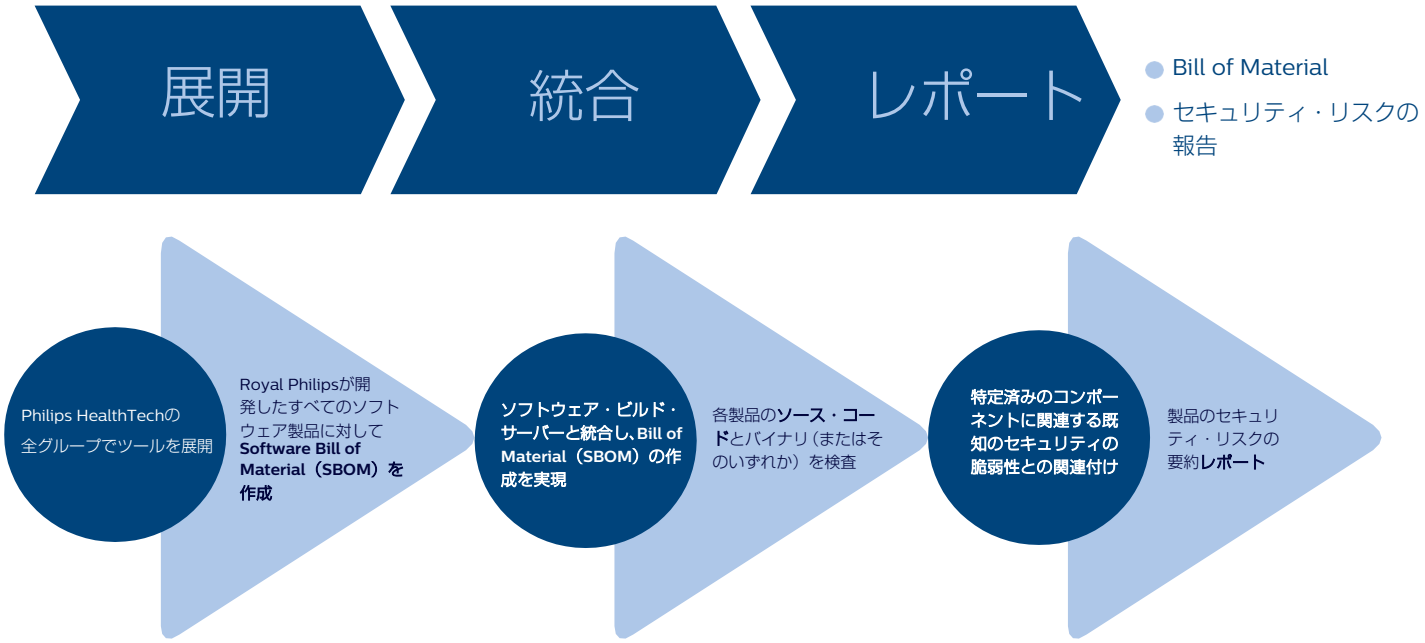
この審理中法案の結果、オープン・ソースおよびサード・パーティ製ソフトウェアのセキュリティの脆弱性または欠陥に対するガバナンスおよび開示方法について要件が適用されています。これらの要件には、米国の復員軍人援護局が採用し、国立標準技術研究所の文書800-53（NIST 800-53）で規定されたものも含まれています。

NIST 800-53は、米国連邦情報システムおよび組織のセキュリティ管理、およびすべての連邦情報システムの文書セキュリティ管理（国家のセキュリティ向けに設計されたものを除く）の必要性を推奨している米国の出版物です。[2]

フィリップスのSBOMガバナンス・プログラムにより、フィリップスは上記の要件において業界をリードしています。SBOMガバナンス・プログラムは以下の3つのフェーズで構成されています。

- **展開** – フィリップスが開発した、ソフトウェアで動作するすべての製品に対してSoftware Bill of Material（SBOM）を作成します。これは、すべての業務グループにSBOMツールを展開することで完了します。
- **統合** – SBOMツールとプロセスを、ソフトウェア開発とプロセス構築に統合します。各製品のソース・コードとバイナリ（またはそのいずれか）を検査します。
- **報告**– 各製品のセキュリティ・リスクの要約を作成します。そしてその要約を、特定済みのコンポーネントに関連する既知のセキュリティの脆弱性と関連付けます。

オープン・ソースのガバナンスおよびコンプライアンスへのアプローチ



製品のポートフォリオで、オープン・ソースとサード・パーティ製ソフトウェアのコンポーネントを特定して説明することで、潜在的なセキュリティ違反と脆弱性への迅速な対応が可能になりました。優れたSBOMプログラムに関連する主要な7つの要素は以下のとおりです。

1. SBOM要件を文書化する
2. 更新および保守作業を含むソフトウェア開発ライフサイクル・プロセスにSBOMを統合する
3. SBOMの脆弱性およびライセンスの問題を特定し、その結果をセキュリティ・リスクの評価に含め、評価された各リスクに対して修正を行う
4. すべての関連製品の文書にSBOMを含める
5. SBOMを継続的にモニタリングすることで新たな脆弱性を発見してセキュリティ・ソフトウェアを更新する
6. 関連製品の文書内のSBOMとセキュリティ・リスク評価を更新する
7. 政府規制の変更に応じて包括的なSBOM要件を調整する

Philips Product Security SBOMプロセスは、フィリップス製品セキュリティ・ポリシーに従って、フィリップスの各製品のシステム開発ライフサイクルへと統合されます。新システムはこれらの期待値を満たし、将来のアップグレードに備えます。セキュリティの問題を抱えるレガシー・システムは、アップグレード、ネットワークの軽減、交換によって対処します。

オペレーティング・システムおよびパッチ管理フィリップス製品には、Microsoft Windowsをはじめとするサード・パーティ製の市販コンピュータのオペレーティング・システム（OS）を使用しているものもあります。フィリップスは、関連ベンダーおよび業界または報道機関のセキュリティに関する発表を絶えずチェックし、新たな脆弱性によって影響を受ける既存の医療機器に対するリスク評価を行います。

Microsoftは、MS Windowsのセキュリティ・パッチ（ホットフィックス）に関する情報を定期的に開示しています。新たなセキュリティの脆弱性やパッチの可用性が認められると、フィリップス製品のエンジニアリング・チームによるホットフィックスの影響評価が通常48時間以内に開始されます。通常の製品の場合、影響を受けた製品への対処方法が、評価後5～12営業日でフィリップスからユーザーへと公開されます。

脅威および問題になっている製品の性質によっては、検証済みのフィックスまたはソフトウェア・アップデートがリリースされる場合があります。推奨される対応方法の手順で医療機器のシステム・ソフトウェアの変更が必要になる場合も、ソフトウェア・アップデートがリリースされる場合があります。これらのアップデートの可用性と適用可能性に関する情報も同様に、フィリップスの標準サービスチャネルからご確認いただけます（製品によってはフィリップスのWebサイトからもご確認いただけます）。

このような情報を便利な方法で適宜お知らせするため、Philips Product SecurityのWebサイトでは、定期的に更新される個々の製品の脆弱性情報へのアクセスに力を入れています。この情報は、既知のソフトウェアの脆弱性、現在の状況、推奨されるお客様の対応方法、一般的なコメントを製品ごとに示したシンプルな一覧表にまとめられています。この情報は、Philips Product SecurityのWebサイトからアクセスできます。脆弱性の一覧表、パッチ管理、その他の製品セキュリティについて質問がある場合は、productsecurity@philips.comへメールするか、フィリップスのフィールド・サービス・エンジニアに直接お尋ねください。

フィリップスでは、製品に基づいたさまざまなソリューションを提供することで、陳腐化するOSのリスクに対処しています。製品は、最新のOSへのアップグレードや、より新しい製品との交換が可能です（製品の使用年数によります）。または、リスクを軽減するため、ネットワーク分離、ホワイトリストなどの追加のセキュリティ対策も提供することができます。

マルウェア対策

お客様の機器が正しく展開され、効果的な動作が保たれるように、フィリップス製品は特定のシステムおよびセキュリティの仕様のコンプライアンスの範囲内で動作するように納品されます。これらの製品の仕様には、マルウェア対策用の機器構成、ネットワーク、オペレーティング・システム、ソフトウェアの要件が含まれている場合があります。
詳細については、ご利用中の機器の説明書やユーザーズ・ガイドを参照してください。

Philips Product Security Webサイト

フィリップスのProduct Security Webサイトでは、さまざまな情報リソースにアクセスできます。ここでは、セキュリティに関する掲示板、FAQ、脆弱性情報、業界のリソースへのリンク先、製品セキュリティのホワイト・ペーパー、その他の製品セキュリティの概要情報などが提供されています。

医療機器MDS$_2$フォーム

2005セキュリティ・ルールの下で米国HIPAAの義務をお客様が果たせるよう支援する目的で、フィリップスは製品セキュリティ情報を率先して公開しています。[3]お客様の要望に応えるため、フィリップスはこれまでさまざまな手順でフィリップスの医療機器のセキュリティを向上させてきました。機器が正しく使用されている限り、フィリップスのヘルスケア製品のセキュリティ機能によって、ユーザーは、要件の順守、患者の健康情報の機密性、完全性、可用性を保証するという責任を果たすことができます。医療機器のセキュリティおよび米国でのHIPAAセキュリティ・ルールへの順守が重要性を増しつつある経緯を踏まえ、医療情報管理システム学会（HIMSS）は、Manufacturer Disclosure Statement for Medical Device Security（MDS$_2$：医療機器のセキュリティに関する製造業者の開示宣言）を作成しました。The MDS$_2$は、重要なセキュリティ情報をヘルスケア・プロバイダに提供する目的で作成されています。これらの情報は、医療機器が作成し、送信し、維持する保護されるべき電子医療情報（ePHI：Electronic Protected Health Information）に関連する脆弱性とリスクを、ヘルスケア・プロバイダが評価し、管理できるように支援するものです。

Philips MDS^{2}フォームは、フィリップスのProduct SecurityのWebサイト（www.philips.co.jp/productsecurity）で入手できます。

製品のセキュリティに関するご協力のお願いフィリップスは、フィリップス製品のセキュリティが、徹底したセキュリティ戦略において重要な役割を果たすことを認識しています。ただし、セキュリティを実現できるのは、包括的かつ多層的な戦略（方針、過程、技術など）を実施することによって、内部および外部の脅威から情報とシステムが保護されている場合だけです。セキュリティ対策においては、業界標準の慣習に従い、物理的セキュリティ、運用上のセキュリティ、手順上のセキュリティ、リスク・マネジメント、セキュリティ・ポリシー、および緊急時対策に取り組む必要があります。実際に実施される技術的なセキュリティ項目は施設によって異なり、さまざまな技術、設定、ソフトウェア・ソリューションが使用されます。他のコンピュータベースのシステムと同様に、セキュリティ対策にはファイアウォール、ネットワークのセグメント化、医療システムと施設ネットワーク間に配置されるその他のセキュリティ機器が使用されます。こうした境界防御およびネットワーク防御は、医療機器の包括的なセキュリティ対策において不可欠な要素です。内部または外部ネットワークへの機器の接続は、製品の有効性、データ、システム・セキュリティに対する適切なリスク・マネジメントを行ったうえで実行してください。

サード・パーティ製ソフトウェアおよびパッチに関するポリシーフィリップスは、極めて精緻な医療機器、および個人用機器やシステムを販売しています。これらのシステムに対する変更は、フィリップスの従業員が行う場合、またはフィリップスが明確に指示を公開している場合に限り、フィリップスの認証に基づいて行われます。セキュリティの脅威の高まりを考慮し、フィリップス製品のエンジニアリング・グループは、特定の機器に対して、セキュリティ関連のサード・パーティ製ソフトウェアとソリューションの導入を許可しています。フィリップスは、今後も患者とオペレータの安全性を最優先事項として捉えています。フィリップスの医療機器の変更については、規制および品質保証の手順に従って検証と妥当性確認を行うよう義務付けられています。その他の医療機器と同様に、「ソフトウェアのみ」のフィリップス製品は、付属の文書、サービス契約、ユーザーズ・ガイドに従って適切にセキュリティ保護されたコンピュータおよびネットワークでのみ使用できます。フィリップスは、お客様のセキュリティ担当者がシステムとアプリケーションの脆弱性をモニタリングし、お使いのシステムで動作中のオペレーティング・システムおよびその他のインストール済みソフトウェアに修正プログラムを適用し、最新の状態に更新しておくことを強く推奨します。

フィリップス製品は、消費者ライフスタイル用製品、家庭用モニタリング・システムから画像収集システムおよび鑑賞システム、IT指向のPACSから24時間365日のライフクリティカル・システム、リアルタイム患者モニタまで多岐にわたります。フィリップス製品のポートフォリオが多様化したことを受けて、フィリップスは、フィリップス・システムへのサード・パーティ製ソフトウェアのインストールおよびインストール後の保守を含む幅広いソリューションをサポートしています。特定の製品の詳細情報については、フィリップスにお問い合わせください。[4]

一般的ケース

有効な仕様上の要件としてフィリップスが文書化しているか、文書による同意が得られている場合を除き、フィリップス機器へのお客様によるサード・パーティ製ソフトウェア（ウィルス対策スキャナー、オフィス生産性ツール、システム用修正プログラム、オンプラットフォーム・ファイアウォールなど）のインストールは、ほとんどの場合許可されていません。フィリップス製品に無許可で変更を加えると、お客様の保証が無効になり、機器の規制ステータスが変更される場合があります。無許可の変更の結果生じるいかなるサービスも、フィリップスとのサービス契約の対象外となります。無許可の変更は、お使いの機器のパフォーマンスや安全性を、予期せぬ形で損なうおそれがあります。フィリップスは、無許可の変更が行われた機器に対して責任を負いません。

フィリップスがサード・パーティ製ソフトウェアの使用を許可した場合、システム用修正プログラムの適用、アップグレード、許可されたインストールは通常、（1）製造時またはインストール時にフィリップスが行うか、（2）インストール後のフィリップス公認サービス・エンジニアが行います。

例外的ケース

状況によっては、フィリップスはフィリップス公認サービス・エンジニアによるサード・パーティ製ソフトウェアのインストールまたは有効化を許可することがあります。ただし、これらは必ず、明確に文書化されたフィリップスのガイダンスに基づき、フィリップスが文書で認可した特定のシステムおよびバージョンに対してのみ行われます。

フィリップス製品へのサード・パーティ製ソフトウェアのインストールまたは有効化について検討する前に、フィリップスの現地担当者に連絡し、お使いの製品でそのソフトウェアを使用できるか、使用できる場合はどのような制限が課されるかについて確認してください。

フィリップスの医療機器またはシステムのいかなる無許可の変更（製品のファイアウォールの変更、ソフトウェア修正プログラム、セキュリティ・ソフトウェア、ユーティリティ、ゲーム、音楽ファイル、その他のソフトウェア・プログラムのインストールや変更を含む）も、システムのパフォーマンスや安全性に予期せぬ形で悪影響を及ぼし、結果としてお客様の従業員および患者が、フィリップスのサービス、規制、品質要件に基づくセキュリティ保護を受けられなくなる可能性があることをご理解ください。これらのインストールや変更が引き起こす有害な副次的影響は、次のようなものです。

1. アクセスまたは制御用の経路を開いたり広げたりしてセキュリティ侵害を引き起こす
2. ウィルス、スパイウェア、トロイの木馬、バックドア・アクセス、その他のリモート・エージェントの侵入を許す
3. 製品やシステムに脆弱性をもたらしかねない更新データが無許可でインストールされる

お使いのフィリップスの製品またはソリューションで無許可の変更が行われた場合、またはその疑いがある場合は、当社のカスタマー・サービスか、フィールド・サービス・エンジニアに即座に報告して指示を受けてください。

フィリップス・リモート・サービス

フィリップスは、お客様が使用している複数のフィリップス・システムをフィリップスの先進サービス・リソースに接続する目的で、グローバルなWebベースのフィリップス・リモート・サービス・ネットワーク（RSN）を立ち上げました。最先端の設計により、仮想プライベート・ネットワーク（VPN）を介し、お客様の機器と現場のフィリップス機器をつなげる単一のポイントオブネットワーク・アクセスを実現しています。このセキュアなトンネル・アプローチにより、業界で最高クラスのリモート・サービスソリューションが誕生しました。このソリューションは、サービス・セッションの全情報の暗号化により認証と権限付与を明示的に制御することで、接続をセキュアなものにしています。

変わりゆく世界におけるフィリップス製品のイノベーションとソリューション

高まりつつあるフィリップス製品のセキュリティのニーズと歩調を合わせ、フィリップスは、既存の製品に対する調査とリエンジニアリングを継続し、セキュリティに敏感なフィリップスのお客様の要望に対して最大限お応えする所存です。フィリップスは、セキュリティの基本原則に基づいた未来の製品を構築すべく、努力を重ねております。

フィリップスは今後もプロバイダ、IT組織、そして消費者と密に連携し、新規のSecurity Designed In製品を構築する心構えで今日の問題に対して柔軟なソリューションを提供していきます。フィリップス製品のセキュリティ向上へのフィリップスの取り組みに関するご質問は、現地のサービスまたは販売担当者、あるいはproductsecurity@philips.comまでお尋ねください。フィリップスによる個人（プライバシー）データの取り扱いについて懸念されている場合は、healthcare.privacy@philips.comまでお尋ねください。

フィリップスの数々の革新的ソリューションに関心をお持ちいただき、ありがとうございます。

1 米国FDAの業界向けガイダンス：Cybersecurity for Networked Medical Devices Containing Off-the-Shelf（OTS）ソフトウェア
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.html

2 Privacy in the Internet of things: Threats and Challenges（モノのインターネット（IoT）におけるプライバシー：脅威と課題）、
https://arxiv.org/abs/1505.07683

3 フィリップス製品向けの医療機器のセキュリティに関する製造業者の開示宣言（HIMSS MDS2標準フォーム）は、以下より入手できます。
https://www.philips.co.jp/productsecurity

4 フィリップスサポートの連絡先情報：

フィリップスヘルスケア：

- 北米 – 1 800 669 1328（または+1 321 253 5693）
- アジア – +85 2 2821 5888
- 欧州、中東、アフリカ – +49 7031 463 2254
- 中南米 – +55 11 2125 0744
- カナダ – 1 800 291 6743

グローバルな連絡先（ヘルスケア、個人の健康、消費者製品）

- http://www.philips.com/c-cs/global-country-selector.html
- 国を選択した後、「Support」、「Contact」の順に選択してください。

5 医療機器が組み込まれたITネットワークへのリスク・マネジメントの適用http://www.iso.org

6 U.S. Department of Veterans Affairs（VA：米国退役軍人省）医療機器分離アーキテクチャ・ガイド、v2.0。HIMSSのWebサイトで入手可能。
http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=101

7 Healthcare Information and Management Systems Society（HIMSS：医療情報管理システム学会）医療機器セキュリティ・ワークグループ
http://www.himss.org/「Topics and Tools」（トピックとツール）>「Medical Device Security」（医療機器セキュリティ）を参照。

8 U.S. FDA Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff
（米国FDA医療機器のサイバーセキュリティの市販後管理 - 業界および食品医薬品局員向けガイダンス）（2016年12月）
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

9 IHEは、Healthcare Information and Management Systems Society（HIMSS：医療情報管理システム学会）とRadiological Society of North America（RSNA：米国放射線学会）の共同イニシアティブです。http://www.ihe.net/

www.philips.com/productsecurity

仕様は予告なく変更されることがあります。

www.philips.com