キヤノンメディカルシステムズのサイバーセキュリティ脆弱性ハンドリングプロセス
Version 1.0, 2018-05-01

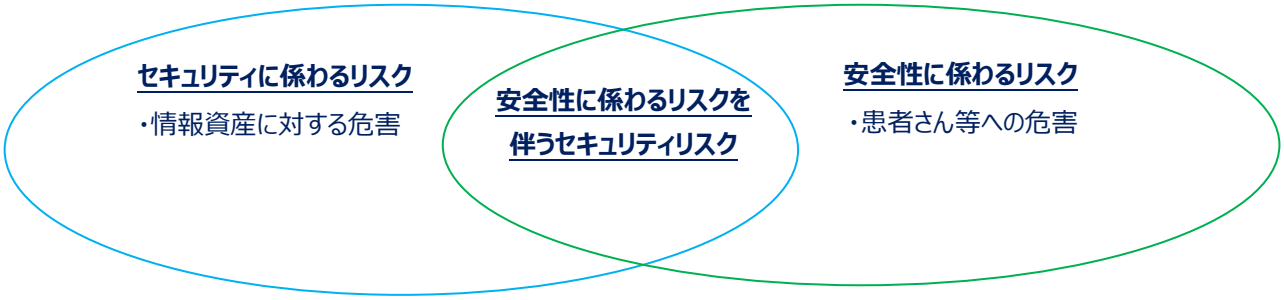
■脆弱性情報開示方針

キヤノンメディカルシステムズは、以下の条件に合致するサイバーセキュリティの脆弱性が確認された場合、問題の詳細な情報を含むセキュリティ情報において、当該脆弱性に関する情報を公開します。

- 製品の安全性/本質的な性能に影響を及ぼし、潜在的に制御不能なリスクになる可能性のある脆弱性
- 社会的ニュースとして取り上げられた脆弱性
- セキュリティコミュニティ等、外部から指摘された脆弱性

■製品のセキュリティリスクと安全性リスクの関係

サイバーセキュリティの脆弱性は、製品の安全性及び本質性能に影響を与える可能性があります。製品のリスクマネジメントには、このセキュリティリスクが含まれており、包括的なリスク管理を実施する事で、安全性に関連するリスクだけでなく、セキュリティに起因するリスクも低減します。セキュリティリスクを認識するタイミングでは、セキュリティの脆弱性を悪用するマルウェア等の攻撃方法が予想できないといった場合があるため、安全性への影響を厳密には評価できない事があります。このため、脆弱性やマルウェア情報の継続的な監視が重要となります。



■サイバーセキュリティ脆弱性ハンドリングのトリガー

サイバーセキュリティ脆弱性ハンドリングのトリガーとしては、下記のものがあります。

1．製品に搭載している SOUP（Software Of Unknown Provenance。ここでは、“開発過程が不明なソフトウェア”のうち、OS 等既製品ソフトウェア）の脆弱性情報
2．第三者からのサイバーセキュリティ脆弱性報告

本文書では、これらの基本的な処理プロセスを紹介します。

1．製品に搭載されている SOUP のサイバーセキュリティ脆弱性ハンドリングプロセス

サイバーセキュリティ脆弱性ハンドリングプロセスは、通常、以下の A から E までのステップから構成されます。

A. サイバーセキュリティに関する情報源の監視及びサイバーセキュリティの脆弱性検知

弊社 PSIRT（Product Security Incident Response Team；製品セキュリティインシデント対応チーム）は、医療機器に搭載されていて、外部から攻撃される可能性のある SOUP に関するサイバーセキュリティに関連する脆弱性情報を収集及び監視します。

サイバーセキュリティに関する情報源は、以下の通りです：

・ SOUP の製造元又は提供元のウェブサイト
・ コンピュータセキュリティインシデントに関する情報発信を行う ICS-CERT / JPCERT / JVN IPEDIA 等のウェブサイト
・ セキュリティツールメーカーのウェブサイト

収集される情報は、以下の通りです：

・CVE（Common Vulnerabilities and Exposure；共通脆弱性識別子）番号

・脆弱性に関する詳細

・脆弱性に関する CVSS（Common Vulnerability Scoring System；共通脆弱性評価システム）基本値（Basic Score）

B. サイバーセキュリティの脆弱性リスクの評価

弊社 PSIRT は、脆弱性の CVSS 基本値があらかじめ決められた基準を上回っている場合、脆弱性を悪用する典型的な攻撃シナリオの情報をもとに、攻撃を受けた場合の製品に対する影響範囲と二次的な被害の大きさを評価します。典型的な攻撃シナリオとしては、能動型攻撃を対象とします。これにより、CVSS 環境値（Environmental Score）を算出します。CVSS 環境値が特定の基準を超える場合、影響を受ける製品及びバージョンを特定します。

なお、医療機器で実行されないように制御されている SOUP のコンポーネント（例：Web ブラウザ、電子メールアプリケーション、Office アプリケーション等）に関連する脆弱性は、リスク評価の対象には含まれません。

C. サイバーセキュリティの脆弱性による患者危害の評価

サイバーセキュリティの脆弱性は必ずしも製品の安全性リスクに直結するわけではありませんが、マルウェア等による情報の改ざんとサービス運用妨害は、安全性に影響を与える可能性があります。このため、それらの脅威が想定される場合には、安全性への影響を分析します。安全性への影響分析は包括的かつシステムレベルで、リスクアセスメントにより実施します。リスクアセスメントは、患者さんへの危害程度と発生確率を評価することです。リスク評価結果があらかじめ決められた基準を超える場合、この脆弱性は安全性に係わるリスクとして処理します。なお、医療機器においては、マルウェア等による攻撃の影響が緩和されるよう、複数の安全対策が実装されています。

D. サイバーセキュリティの脆弱性情報の開示

この脆弱性に対処するための修正が必要な場合、弊社 PSIRT は弊社 Web サイトにおいてセキュリティ情報を公開します。通常、セキュリティ情報には以下の情報を含みます：

- 脆弱性の説明（CVE 番号及び CVSS 基本値/環境値）
- 影響を受ける製品情報
- 緩和要因と回避策に関する情報

安全性への影響を伴う重大なサイバーセキュリティに関する脆弱性の場合、関係するお客様及び監督官庁に報告します。

E. サイバーセキュリティの脆弱性に対するリスク緩和策の検討及び対策計画の策定

弊社 PSIRT は、暫定対応のリスク低減対策を調査し、セキュリティ情報を更新します。 弊社設計部門は、脆弱性の対策用パッチの検証計画を立てます。

２．第三者からのサイバーセキュリティの脆弱性報告ハンドリングプロセス

研究者、業界団体、CERT 及びその他の情報源から、弊社製品に関するサイバーセキュリティ脆弱性報告をお受けします。その場合、以下の情報を最寄りの支社・支店・営業所までご連絡ください：

- 当該脆弱性の説明（可能であれば、脆弱性を実証するためのコードやネットワークのトレースログを含む）
- 影響を受ける製品（可能であれば製品名やバージョン名を含む）
- 当該脆弱性の公開状況
- お客様のご連絡先

弊社 PSIRT は、連絡いただいた脆弱性を内部的に調査し、速やかに対応します。 必要に応じて、追加の情報をお願いする場合があります。

変更履歴

V1.0 (2018-05-01): Publication