情報機器販売時のガイドライン

第1章　背景

近年、IT の発展や労働環境の変化に伴い様々な情報機器の導入を行う企業が増える中、日々発表されている情報機器の脆弱性について対応を放置されたまま運用を続ける状態が増え、修正されていない脆弱性を利用したサイバー攻撃の被害が増加の一途をたどっています。

情報機器に関する脆弱性情報はメーカーのホームページや、IPA 等の脆弱性情報発信サイトから入手可能です。しかし、情報機器を販売した販売店、情報機器を購入し利用する企業・法人（以下、「利用者」）間で、導入した情報機器の脆弱性情報について、入手方法、対策方法などの責任範囲が、言語化、文書化された状態で販売されず、結果として利用者が対応・修正していない脆弱性が原因のセキュリティインシデントが発生した場合、インシデントの責任を販売店と利用者が争う場面に至ることがあるため、これを未然に回避する必要があります。

また利用者自身にリスクを認識していただき、運用の責任を正しく共有し分解することで販売店のリスクのみならず利用者のリスクも低減し、インシデントが発生しにくい環境を構築する建設的な取り組みが社会的にも強く求められています。

第2章　目的

販売店が情報機器の販売時の責任範囲を明確にし、利用者が運用するために必要な情報の入手先、問い合わせ先を販売時に正しく伝えるために、必要な原則や内容について一定の基準を示すことにより販売店と利用者間における責任分界点を明確化することを目的とし、また、それによって事前に想定するべき脆弱性対応を含む安定的運用を利用者に定着させ、可能な限りセキュリティインシデントの被害にあわないで済む継続的な取り組みの認知も目指します。

さらに本来利用者が持つべきスキルや体制の確立や、状況に応じた外部委託の必要性、有償サービスの意義などを明確にすることで、利用者とともに安心安全な情報セキュリティを構築していきます。

第3章　適用範囲

本ガイドラインでは、販売店が利用者に対して販売する情報システム関連製品全般の脆弱性に関する情報提供について適用範囲といたします。

第4章　用語の定義

本ガイドラインで使用する用語の定義を以下に示します。

・情報システム関連製品全般

販売店により販売した PC・ルーターやスイッチなどのネットワーク機器を含む、インターネットに接続でき、ファームウェアの更新が行える製品全般を指す。

・情報セキュリティ

企業や組織の情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護すること。

・脆弱性

情報システム関連製品全般においてプログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥を指す。

・情報資産

企業や組織などで保有している情報全般のこと。顧客情報や販売情報などの情報自体に加えて、それらを記載したファイルや電子メールなどのデータ、データが保存されているパソコンやサーバなどのコンピュータ、CD-ROM や USB メモリ、SD カードなどの記録媒体、そして紙の資料も情報資産に含まれる。

(総務省ホームページより)
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_02.html

・SOC

セキュリティオペレーションセンターの略称である。

第5章　販売店の責務

1.　販売店に求められる行動規範

販売店は、以下に掲げる事項を告知するとともに、脆弱性情報の収集、ファームウェアの更新を含むメンテナンス、事故対応といったセキュリティインシデントの防止・予防が、利用者が自ら行うべき自己責任の範囲であって、保守・メンテナンス等の契約を締結しない限り、情報機器を販売したに過ぎない販売店が責任を負うものではないことについて、十分な説明を行うことが望ましい。

(1)　販売店は、利用者に対して、情報システム関連製品全般の脆弱性に関する情報提供について、一定の基準を示すことが望ましい。

(2)　販売店は、利用者に対して、販売店及びメーカーから情報提供を受け、メンテナンスを行い、ファームウェアを最新に保つことを推奨することが望ましい。

(3)　販売店は、利用者との間で、販売時点におけるシステムの最新バージョンを共有することが望ましい。

(4)　販売店は、継続的な保守契約又はスポット作業によるメンテナンス業務を行うサービス・プランを提案することが望ましい。

2.　販売時における告知事項

販売店は、販売に先立ち又は販売と同時に、利用者に対して、以下に掲げる事項を告知するとともに、脆弱性を放置した場合のリスクについて十分な説明を行うことが望ましい。

(1) サービス範囲（有償サービス）

以下に掲げる事項を含む有償対応のサービス内容を明確に告知することにより、販売店が無償対応を受け付けない範囲を理解してもらうことが重要です。

(a) ファームウェアのアップデート作業

(b) 標準設定以外の設定作業

(c) 標準設定の変更

(d) 納入機器以外に起因する障害への対応

(e) セキュリティ事故等における対応作業

(2) 販売店の免責事項

以下に掲げる事項について、販売店が責任を負わないことを明確に告知することが重要です。

(a) 納入機器がセキュリティを完全に保証するものではないこと。

(b) 販売店が利用者のセキュリティ環境を保証するものではないこと。

(c) 販売店がセキュリティ被害による損害を補償しないこと。

(3) 脆弱性情報

販売店が機器のみを提供する場合（ハードウェア保守を含む）、脆弱性情報の提供元（メーカーサイト）を通知するとともに、脆弱性情報の提供責任がメーカー側にあり販売店には義務がないことを告知することが重要です。

3. 保守・メンテナンスに係るサービスの提案

販売店は、自社サービスか否かを問わず、販売した機器に関する継続的な保守又はスポット作業によるメンテナンスに関するサービス・プランを提案することが望ましく、利用者自身によるメンテナンスが困難と疑われる場合には特に好ましい。

また、かかる提案に際して、保守・メンテナンスを委託しない場合、利用者が対応・修正していない脆弱性が原因のセキュリティインシデント等の結果に関して何らの責任も負わないことに加え、例えば、以下に掲げる事項について、利用者が自らの責任において対処しなければならないことを告知することが望まれる。

(1) ファームウェアのアップデート

(2) ネットワーク設定の確認

(3) （その他機器ごとに対処すべき事項）

4. 運用支援（代行）および SOC サービスの利用促進

侵害防止の観点で、運用支援やSOCサービスの顧客の利用促進に務めることが重要です。

また、侵害発生に備えることも重要です。

第6章　見積もり・契約条件の記載例

・××が販売させて頂く、「情報システム関連製品」が該当しますが、情報セキュリティに関する脆弱性情報のご提供は製品販売には含まれません。

（※機器の費用には継続的に情報収集・提供する役務は含まれないため）

・重要なアップデート情報やサポートが必要な場合は、別途メーカーおよび販売代理店と相談の上、保守契約の締結、またはその他運用サポートサービスの有無を確認して頂き、ご対応願います。

【共通】

- 単なる注意喚起のみの場合

①本製品は「情報セキュリティ対策」のために、常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを推奨します。アップデートの実施はお客様にてお願い致します。
　各製品の最新情報・アップデート方法につきましては、各メーカーの提供情報をご確認ください。

- 社内の相談窓口を紹介する場合

②本製品は「情報セキュリティ対策」のために、常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを推奨します。アップデートの実施はお客様にてお願い致します。
　本件のお問い合わせに関しましては、弊社サポートセンターまでお問い合わせください。

- 保守メニューを提案する場合

③本製品は「情報セキュリティ対策」のために、常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを推奨します。アップデートの実施はお客様にてお願い致します。

　本件について、弊社保守メニューをご希望の場合は、弊社サポートセンターまでお問い合わせください。

【ネットワーク機器に特化したもの】

- 単なる注意喚起のみの場合

①本製品をご利用中において、情報セキュリティ上のリスクを緩和するために、常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを強く推奨します。アップデートの実施はお客様にてお願い致します。
　各製品の最新情報・アップデート方法につきましては、各メーカーの提供情報をご確認ください。

- 社内の相談窓口を紹介する場合

②本製品をご利用中において、情報セキュリティ上のリスクを緩和するために、 常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを強く推奨します。アップデートの実施はお客様にてお願い致します。
　本件のお問い合わせに関しましては、弊社サポートセンターまでお問い合わせください。

- 保守メニューを提案する場合

③本製品をご利用中において、情報セキュリティ上のリスクを緩和するために、 常に製品のファームウェア・ソフトウェアなどを最新の状態にしておくことを強く推奨します。アップデートの実施はお客様にてお願い致します。

本件について、弊社保守メニューをご希望の場合は、弊社サポートセンターまでお問い合わせください。

執筆

一般社団法人日本コンピュータシステム販売店協会（JCSSA）

セキュリティ委員会　ガイドライン分科会

山本 総夫	(株)ソフトクリエイト/分科会オーナー
尾崎 嘉一	(株)ソフトクリエイト/分科会オーナー
佐久間 大希	(株)ソフトクリエイト/分科会オーナー
山名 広朗	SB C&S（株）
北澤 英之	SB C&S（株）
西川 靖彦	(株)大塚商会
延下 悟志	(株)大塚商会
石井 秀直	ダイワボウ情報システム(株)
中川 靖文	日本事務器(株)
後藤 行正	日本ビジネスシステムズ(株)
清原 健二	日本ビジネスシステムズ(株)
斉藤 章	(株)ハイパー
石上 和雄	フォーティネットジャパン(同)
和中 速人	フォーティネットジャパン(同)
狼 秀明	ユニアデックス(株)
丸木 久美	リコージャパン(株)

執筆協力

小山 敏之	JCSSA 事務局
乙山 美由起	JCSSA 事務局

（執筆関係者、社名五十音順）