# 情報機器販売時のガイドライン（ドラフト）

## 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（以下、「ベンダー」）、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、責任範囲を争う裁判へと発展し、ベンダーが責任を負うケースが想定されます。

##  2. 目的

ベンダー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、ベンダー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す。

## 3. 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。

## 4. 用語の定義

・情報システム関連製品全般

ここでは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。

・善管注意義務

「善良な管理者の注意義務」の略で、受託者が事務等の管理を行う場合には、当該職業又は地位にある人として通常要求される程度の注意義務を払うこととされている。民法第644条には「受任者は委任の本旨に従い、善良な管理者の注意をもって事務を処理すべきである」旨規定されている。

・情報セキュリティ

企業や組織における情報セキュリティとは、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。

・情報資産
 情報資産とは、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 ）

## 5. 販売店の原則

【ポイント】

（共通）

・販売店は情報提供について一定の基準を示すことが望ましい。

・販売店は利用者に対し、販売店およ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よう推奨することが望ましい。

・販売前のヒアリング等によって利用者が現時点で脆弱性のあるバージョンを使っていることが判明した場合、購入先を問わず脆弱性情報を提供することが望ましい。

（NW機器）

・販売店は販売した時点のシステムの最新バージョンについて共有することが望ましい。

・販売店は利用者自身によるメンテナンスが困難である場合、販売店はメンテナンスを行う旨を含めた保守契約もしくはスポット作業でメンテナンスを行うサービスを提案することが望ましい。

## 6. セキュリティリスク情報提供における販売者の責務

 （販売・導入時）

１．運用面の責任分界点

・有償作業：

有償作業について利用者に明確に伝える必要があります。具体的な項目として以下を告知する必要があります。

ファームウェアのアップデート作業

標準設定以外の設定作業

標準設定の変更

納入機器以外に起因する障害への対応

ウイルス感染時の駆除および復旧作業

・販売店の免責事項：

販売店は、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を明確に伝える必要があります。また、セキュリティ被害を受けた場合の損害については補償できないことも告知する必要があります。

・利用者側の義務の告知：

運用に当たり、利用者側に求められる義務（ファームウェアのアップデート、ネットワーク設定の確認など）を明確に伝える必要があります。

・脆弱性のリスクについての事前説明:

脆弱性を放置するとどのようなリスクがあるのかを利用者に事前に説明することが望ましいです。

 ２．製品の脆弱性情報の通知責任

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）、脆弱性情報の責任はメーカー側にある事の告知、ならびにメーカーの情報提供元（サイト）について通知する必要があります。

３．運用支援（代行）およびSOCサービスの利用促進。

運用支援やSOCサービスの顧客の利用促進に努めることが重要です。

## 7. 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本製品は「情報セキュリティ」の攻撃の対象になりやすいため、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本製品は「情報セキュリティ」の攻撃の対象になりやすいため、 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本製品は「情報セキュリティ」の攻撃の対象になりやすいため、 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。