製品分野別セキュリティガイドライン
オープン POS 編

Ver. 2.0

CCDS セキュリティガイドライン WG
POS SWG

改訂履歴

版数	改訂日	改訂内容
Ver.1.0	2016/06/08	新規作成
Ver.2.0	2017/05/29	2016 年度版ガイドラインとして加筆更新

目次

1 はじめに

これまで製品業界ごとにセーフティ標準は策定されてきた。一方セキュリティ標準をみると、組織運営に関する標準（ISO27001）と製品設計のセキュリティ評価・認証に関する標準（ISO15408）が策定されており、近年では、重要インフラストラクチャー（社会インフラに欠かせないプラントや施設）の制御システムを対象とした標準（IEC62443）も策定されている状況である。

IoT の普及に伴い、身の回りにある生活機器が様々なネットワーク接続機能をもつことで、製品のセキュリティ懸念は増しているが、IoT 製品やサービスには欠かせないセキュリティ標準がいまだ生活機器に対しては整備されていない状況である。

欧米の動きをみると、各業界のセーフティ標準からセキュリティ標準を検討する動きが各所にみられる。一方、日本においてもセキュリティに関する懸念は顕在化しており、検討すべき、という声は多いが、具体的検討に入っている分野はまだ少ない状況となっている。

このような状況の中で、一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）は設立された。本協議会では、生活機器セキュリティ標準の策定と、その標準に沿っていることを確認・検証した認証プログラムをセットにすることで、ユーザに安心して IoT 製品を使ってもらえる環境を整えることを目標に活動を行っている。

平成 27 年 8 月 5 日には独立行政法人 情報処理推進機構（IPA）が「つながる世界の開発指針検討 WG」を発足させ、国レベルでのセキュリティ検討がスタートした。CCDS も IPA-WG に参画し、CCDS 内でのガイドライン検討結果について提案を重ねてきた。

IPA-WG での検討結果は「つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント」[1]としてまとめられ平成 28 年 3 月 24 日に公表された。IPA の開発指針は分野全体をカバーする共通事項を中心にまとめられた基本的な指針となっているが、CCDS では個々の製品分野において、具体的にセーフティとセキュリティをカバーした設計・開発を進めるために、本分野別ガイドラインを策定した。

IPA 発行「つながる世界の開発指針」については、下記 URL のリンク先を参照。

http://www.ipa.go.jp/sec/reports/20160324.html

1.1　POSのセキュリティの現状と課題

POS においては、売上金の収納において、現金のほか、クレジットカード、電子マネーやギフト券、クーポンやポイントカードなど現金以外の売上も行われる。クレジットカード、電子マネーは各事業者からセキュリティを考慮したインフラの提供や規格等で守られているが、現金、クーポン、ギフト券の収納などにおいては操作員が直接手渡し等で受取る場合が多く、近年の就労形態の多様化により不正が行われる可能性が高まっている。従来から不正返品や釣銭着服といった POS 操作を行う操作員の不正による犯罪や被害も後を絶たない。

近年、入金機やキャッシャー自体を自動化したセルフ端末などの導入が進んでいるが、反面展開のすすむオープン化 POS においてはネットワークも含めたセキュリティの強化が必要である。

流通分野における POS システムにおいては従来からスキミングや物理的な破壊（盗難）といった犯罪に加えて、サイバー技術を取り込んだ新しい形の犯罪が増加している。特にマルウェアを物理的な媒体を経由させ、POS の制御部にインストールし、現地で、あるいは、リモートで操作することにより POS 内の情報（クレジットカード情報等）を搾取する等の犯罪が起きており、米国等では社会問題となっている。

このように店舗における POS システムに於いては、サイバーとフィジカルの両面、あるいは組み合わせた犯罪が増加してきており、情報セキィリティ対策が従来以上に重要になってきている。しかし、現実には店舗運用や POS システムに投じる投資コスト、あるいは店員教育の不徹底や就業人口不足､外国人雇用など､システムに対応するセキュリティ管理は進まない状況にある。

一方､社会では IoT 技術の普及に伴い､セキュリティ対策の重要性が叫ばれるようになった｡ハッキングの手口が技術も従来以上に社会で共有されるようになっただけでなく､ハッキングに必要なツールや機器の値段も急速に下落しており、誰でもが不正行為を簡単に行えるような環境が整いつつある。このような背景の下、上記で述べたようなマルウェアを用いた情報搾取や不正行為が手口を悪化させながら更に増えていくものと思われる。

ここで大きな問題となるのが、不正操作や犯罪にかかわっている者が内部の人間であるということである。公開された資料に基づいて判断すると、開発者、運用者、保守員、店員といった、内部にいるすべての人員を疑ってセキュリティ対策を考える必要がある。内部の人間は正当で悪意を持たず、外部からの攻撃のみを考えるという、従来型のセキュリティの考え方と異なる点である。

クレジット取引に関しては、国際ブランド（VISA、MASTER、JCB 等）によるセキュリティ維持（PCI : Paument Card Industry）の規格や媒体の IC 化によるセキュリティ強化（EMV 規格）など、機器に義務付けられるセキュリティ規格が適用されているが、国

内の特徴として、加盟店や業態ごとにきめ細かく接客対応、データ処理対応してきた POS システムにおいて、規格を適用するには多額のコストと運用影響がかかり進んでいない状況である。クレジット取引セキュリティの強化については政府主導で取り組まれており、本ガイドラインではクレジットや電子マネー等ペイメントに関する機微情報は POS システムから切り離し、それらのセキュリティはクレジット業界の規格に委ね、上記にあるような POS への直接攻撃や運用に着目し、それらに有効なセキュリティガイドラインを提供することを目的としている。

1.2 ガイドラインの対象範囲

本ガイドラインの対象範囲は POS システムにおける、POS 端末と POS サーバ、およびその内部に存在する構成要素に限定され、外部コンピュータを含めて POS からの外部接続ネットワークは対象外である。また既存規格として PCI（Payment Card Industry）や EMV（Europay Master Visa）規格で対象となるデータや機器の保護要件は本ガイドラインの対象外である。例えば PCI-DSS（Payment Card Industry Data Security Standard）であれば、PAN（Primary Account Number:カード番号）、磁気トラック情報等に対する保護要件は、本ガイドラインで取り扱わず、PCI-DSS 規格でカバーするものとする。

1.3 本書の対象者

本書は、IoT 機器において適切なセキュリティ対策を実施するための、設計から製品リリース後までに考慮すべき設計・開発プロセスをまとめたものであるため、以下の方を対象としている。

1）装置の設計を行う設計者および開発者
2）装置の設計プロジェクトの開発責任者
3）装置の設計プロジェクトの予算や人員を決定する意思決定者

1.4 略語

本書で使用されている略称について説明する。

表 1-1 略称一覧

略称	名称
CAT	Credit Authorization Terminal
CCDS	Connected Consumer Device Security council
EFT	Electronic Fund Transfer
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
MICR	Magnetic Ink Character Reader
MSR	Magnetic Stripe Card
NIST	National Institute of Standards and Technology
OLE	Object Linking and Embedding
POS	Point of Sales
SWG	Sub Working Group
WG	Working Group

2 システム構成と運用モデル

2.1 POSシステム構成と登場人物

POS システムには、大きく分けて売上を登録する機能と、売上金を収納する機能に大別される。登録作業を行う操作者をチェッカー、売上金収納を行う操作者をキャッシャーという。両操作は 1 人が兼務することが多いが、大手食品スーパーなどでは、1 つの POS 端末を機能別に 2 名で操作する場合がある。また百貨店では集中レジシステムをバックヤードにおいて、売上と収納を分離する運用が行われている。通常の店舗では 1 名で両方の操作を行うことが一般的である。

POS の基本的システム構成を図 2-1 に示す。POS にはパソコンをベースにした制御部が存在し、その制御部がディスプレイやスキャナー、POS キーボード、カードリーダ、釣銭機、レシートプリンタ、キャッシュドロアなどの周辺機器を制御する。

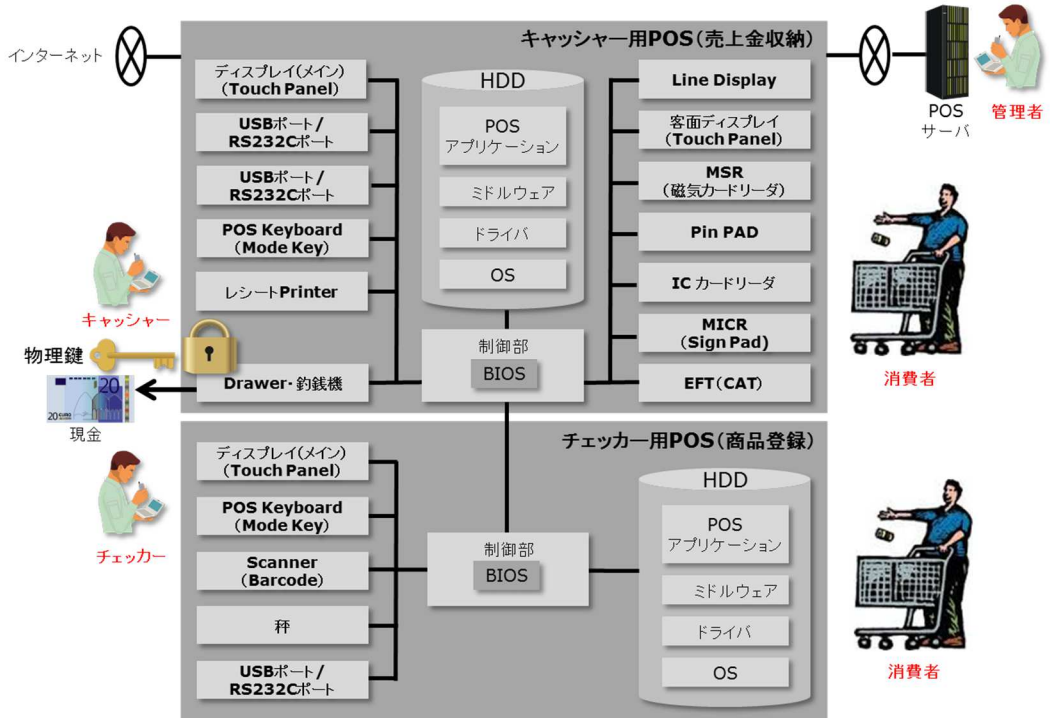

図 2-1 POS のシステム構成と関係者

POS システム構成要素の詳細説明を表 2-1 に、登場人物の詳細説明を表 2-2 に示す。

表 2-1 POS システム構成要素の説明

項番	構成要素	機能
1	制御部	POS 内の MSR や Drawer 等のデバイスを制御するコンピュータであり、OS は Windows が搭載されていることが多い。制御上にはハードディスク（HDD）が搭載されていることが多い。
2	HDD（ハードディスクドライブ）	制御部に搭載されており、HDD 内には OS、ドライバ、ミドルウェア、アプリケーションがインストールされているほか、保守用のソフトウェアなどもインストールされている。
3	BIOS	起動デバイスなどを制御する機能を持つ。BIOS にアクセスするためのパスワードの設定ができるものがあり、HDD 以外の USB メモリや CD-ROM ドライブ等の起動媒体から起動を防止するため、BIOS にパスワードを設定してアクセス管理を要求されることもある。
4	ディスプレイ	POS での取引メニューや処理結果を表示するための表示機能を持つ。
5	客面ディスプレイ	お客様用のディスプレイでお客様用に制限した取引メニューや処理結果を表示する機能を持つ。また、年齢制限確認等、タッチパネルにてお客様に確認及び入力を行う場合もある。
6	USB ポート/ RS232C ポート	USB/RS232C ポートとは USB/RS232C ケーブルを用いてパソコンと周辺機器などを接続する際の、USB/RS232C ケーブルの差し込み口のこと。
7	MSR（磁気カードリーダ）	一般にプラスチック製の、磁気ストライプ型カードを読み取る装置で、POS では、主に顧客入力やクレジット支払時の磁気カード情報を読み取るために使用される。標準で MSR が付いている POS もある。
8	Scanner（Barcode）	バーコードを読み取る機器であり、POS では主に商品情報を読み取るのに使用される。
9	POS Keyboard	POS への入力装置の一つであり、手指でキーを押すことで POS へ文字信号などを送信するもの。POS の操作全般に用いられる。
10	Touch Panel	表示と入力の 2 つの機能を融合したデバイスで、画面に直接触れることにより位置を感知し、POS の操作が行える。
11	Mode Key	POS の表示切替用キー。割引・値引き等 POS の機能がキー名称になっていることが多い。

12	MICR（Sign Pad）	磁気インク文字認識技術の 1 つで、クレジットカードを使用する際 Sign Pad（液晶付きの手書き入力機器）より入力文字を認識する。
13	秤	量り売り商品の重量を測定し、重量データをレジ・POS に送信する機器。
14	Pin PAD	店頭で IC カード対応のクレジットカードを使用する際、暗証番号を入力する端末。
15	IC カードリーダ	情報（データ）の記録や演算をするために IC チップ（集積回路）を組み込んだカードを読み取る装置で、POS では主にプリペイド電子マネー情報、クレジット情報、ポイント情報､顧客情報など 複数の情報を読み取るのに使用される。また、POS のオプションデバイスとして、シリアル通信ポートに接続される。
16	レシート Printer	領収証を印刷する機器のことであり、特に、レジスターで金額などを印字した紙片を出力用紙に印刷する。
17	EFT（CAT） ※本ガイドラインでは対象外	EFT とは電子決済 POS システムで、スーパーなどで買い物をしたときにレジで銀行のキャッシュカードを提示することにより口座から引き落としができるシステム。 CAT とは信用照会端末のことで､クレジットカード加盟店で､カードの有効性を確認するため、 カードの情報について信用照会を行うセンター等に問い合わせし、続けて決済する装置のことである。
18	Drawer	レジや POS の（多くは）下にあり、紙幣や硬貨、金券等を収納する引出しのことであり、会計時に支払金額を入れたり、お釣りを出したりする。
19	釣銭機	釣銭機とは､POS からの制御で指定した金額を放出する機器のことであり、会計時に支払金額を入れたり、お釣りを出したりする。
20	Line Display	お店の設置環境に合わせて高さ調節可能な伸縮ポール型のカスタマーディスプレイ。四方向の設置が可能。

表 2-2 登場人物の説明

項番	登場人物	役割
1	チェッカー	2 人制レジにおいて、主に商品登録操作を担当する。2 人制レジで存在し、1 人制レジでは存在しない。
2	キャッシャー	2 人制レジにおいて、主に支払操作を担当する。
3	管理者（責任者）	チェッカー・キャッシャー等のレジ担当より上位者権限を持ち、上位者権限に限定した POS 機能を実行することができる。

2.2　POSシステム運用

以下、図 2-2 は POS システムの運用における 1 つのモデルケースを示す。

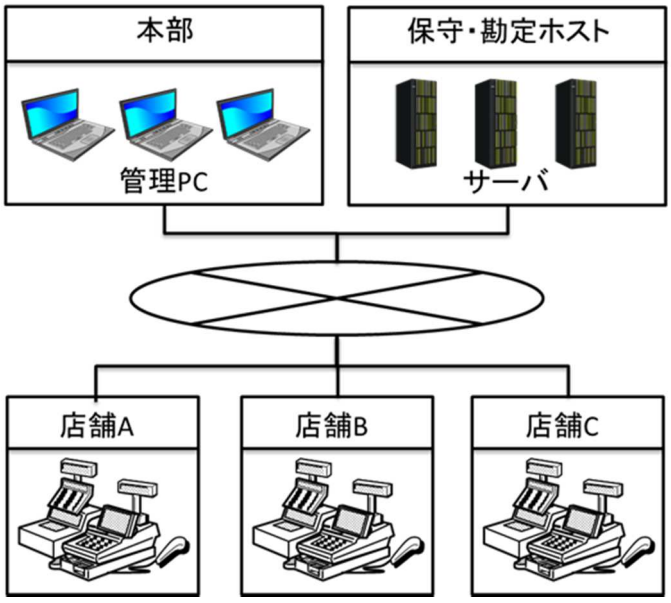

図 2-2 POS システム運用モデルケース例

各店舗に POS システムが存在し、商品情報やクレジット情報等は社内イントラネットワークまたはインターネット環境上でデータの通信をやりとりする。また、売上、顧客、在庫管理等は本部などの管理部署で行う。また、運用業務には保守も含まれており、主にハードウェア保守及びソフトウェア保守等がある。

- ハードウェア保守
  製造元（メーカ、工場）へ POS 端末、周辺機器の部品修理または交換行う。
- ソフトウェア保守
  開発元へ技術支援、改善、障害時に問い合わせを行う。

なお、POS システム導入先は百貨店、食品スーパー、生活、ファッション雑貨店、飲食店、生花店、売店、施設、アミューズメント等幅広くあり、更に業務内容、設置場所、職場の人数に応じた運用がある。

3 想定されるセキュリティ上の脅威

3.1 過去の犯罪事例と考慮すべき観点

これまで起きてきた POS 関連の不正犯罪や将来犯罪に繋がる可能性のある状況と考慮すべき観点を挙げる。

表 3-1 リスクの考え方のまとめ

項番	分類	リスクの考え方
1	侵入ルート	悪意の持つ人やトレースしづらい USB 等の媒体を経由して侵入するリスクがある。
2	情報漏えい	インターフェース仕様が Web に公開され、それを入手してマルウェアが開発されるリスクがあり、公開された時点で、漏えいするという前提を置く必要がある。
3	運用の不備	USB ポートが接続可能であるなど、運用不備のある POS システムが狙われてマルウェアをインストールされるリスクがある。
4	不正改造デバイス	流通市場に正規デバイスが流通しているため不正改造が行われるリスクがある。
5	IoT による被害の波及	現在は物理的にマルウェアを POS システムにインストールしているが、つながる世界が増えれば、ネットワーク経由でマルウェアがインストールされるリスクがある。その場合、既存のリスクが N 倍化する。

図 3-1 は各事例から推測されるマルウェアを用いた不正の事例である。

正規の開発者と思われる人物がソフトウェア等の製品仕様書をインターネットサイトにアップロードし、それをマルウェア開発者がダウンロードしてマルウェアを開発する。現地実行者が運用脆弱性のある POS システムに対して、USB メモリなどのメディアからマルウェアを POS システムにインストールする。その他のインストール方法として、インターネット接続・Email サービスが有効な PC やデバイスに接続されている POS の場合、そこから悪意のある Web リンクや E メールの添付ファイルをエンドユーザが開くことでマルウェアがダウンロード・インストールされる。また、その他の事例として、不正デバイスを物理的に POS システムに接続してカードデータを取得するスキミングの手口も発生している。その後、マルウェアやスキミングによって漏えいしたデータはその他の悪意のある者によって不正なクレジット・デビットカード作成用等に売買される。

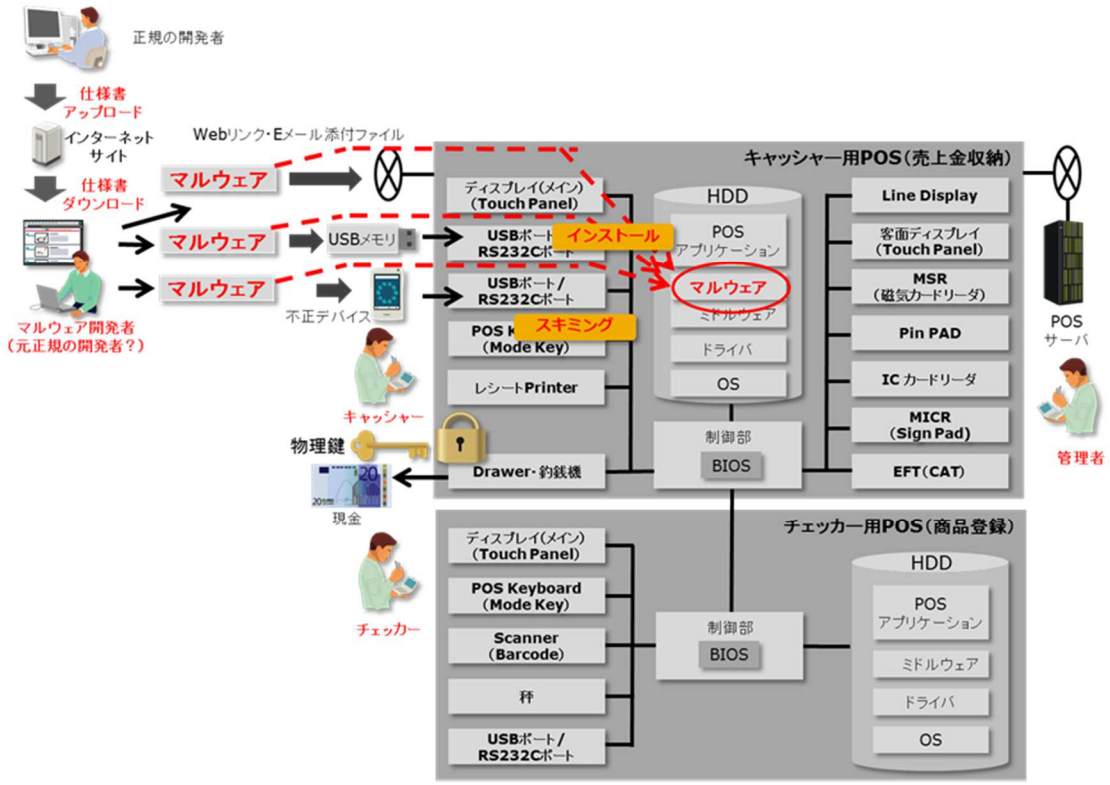

図 3-1 マルウェア・スキミングを用いた情報漏えいの構図（海外事例）

3.2 既存のセキュリティ対策の考え方とその限界

前節で紹介した事例を見ていくと、既存のセキュリティ対策の考え方では十分に対処できない点が多々あることがわかる。以下では POS のセキュリティ対策を考える上で、従来の考え方でどのような問題点があるかを説明する。

3.2.1 内部犯罪に対するセキュリティ対策

3.1 節で説明した事例を通じて理解できるのは、内部の人間は正当で悪意を持たず、外部からの攻撃のみを考えるという従来型のセキュリティの考え方が POS 分野では通用しないことである。前節で説明したように「侵入ルート」、「情報漏えい」、「運用の不備」から見えてくるのは、不正操作や犯罪に関わっているのは内部の人間の可能性があるということである。

「侵入ルート」では USB 等で不正デバイスを物理的に POS システムに接続していることから内部の人間が関連していると推測される。「情報漏えい」では、開発者が提供したとしか思えない、インターフェース仕様書が Web に公開されている。「運用の不備」では脆弱性を運用している POS の存在を犯罪者が知っていた可能性が指摘される。このように、POS セキュリティ対策で考える必要があるのは、外部からの攻撃よりも内部からの攻撃である。

3.2.2　セキュリティ対策における運用条件

近年の就労形態の多様化によりキャッシャーまたは POS 操作員には高度なスキルやモラルが期待できないという現実がある。すなわち、セキュリティ対策のために、彼らに過剰な管理や複雑な操作を強いることは極めて難しい。また、POS の運用は店舗や繁忙時間帯によって異なり、例えば保守作業に対する既存のセキュリティは別の店舗や状況によって受け入れられない場合がある。

いくら良いセキュリティ対策を考案しても、現場の実態や運用に即さないと受け入れられない。運用の柔軟性確保は必要条件と考えるべきである。結果として、POS ではセキュリティ対策から求められる制約条件よりも、運用から求められる制約条件の方が難しいという状況がある。このような状況下の下でセキュリティ対策を考えなければならないので、従来の脅威分析とリスク対策といった手順だけでは上記運用の制約条件を反映しづらく、店舗に受け入れられるセキュリティ対策を作り上げることは困難である。よって、運用の制約条件も反映したような脅威分析とリスク対策に関する新しい分析方法が必要である。

3.2.3　セキュリティ対策に関わるコスト

社会全体にセキュリティ対策を普及させるには大きなコストは掛けられないという制約がある。3.2.1 項、3.2.2 項でも説明したようにどこにも拠り所が無い難しい状況を鑑みるとセキュリティ対策が高価なものになりがちだが、POS の運用や保守に必要なコストも含めて考慮する必要がある。

このコストで考慮すべき視点は、何らかの対策を導入するための導入コストだけでなく、導入後の対策で必要な管理工数や検証工数も考慮しなければならない。図 2-1 で示したように悪意を持つ人物はキャッシャー、チェッカー、管理者であり、彼らの作業結果を検証したり管理したりする必要がある。セキュリティ対策により、セキュリティ面での作業結果の検証・管理工数は削減可能と想定されるが、ゼロにはならないので、それもコストやリスクとして見なすべきである。

加えて、部品交換を行った場合に、交換部品の修理のターンアラウンド時間も考慮する必要がある。部品にセキュリティ機能を実装するために、セキュアルームなど、特別な施設でしか修理できないようなセキュリティ機能では、運用する側からは受け入れがたいと考えるべきである。すなわち、部品に耐タンパ性等の高度なセキュリティ機能を持たせた場合は、セキュアルームでしか分解修理ができなくなるので、保守運用では、すぐに修理部品が入手できないという事態も起こりうる。このような運用に負担をかけるようなセキュリティ機能はコスト面だけでなく、時間の面でも受け入れがたいと考える必要がある。

3.2.4　セキュリティ対策着眼点の偏り

図 3-2 は 3.1 節で説明した事例にて、US-CERT (UNITED STATES COMPUTER EMERGENCY READINESS TEAM)により提案されたセキュリティ対策着眼点の内容を示している。図の右側に対する対策は、ハードディスクドライブ内に存在する情報資産の保護である。一方、図右側下の「BIOS アクセス制限」や「USB ブート禁止」といった対策も、最終的にはハードディスクドライブ内に存在する情報資産の保護が目的である。

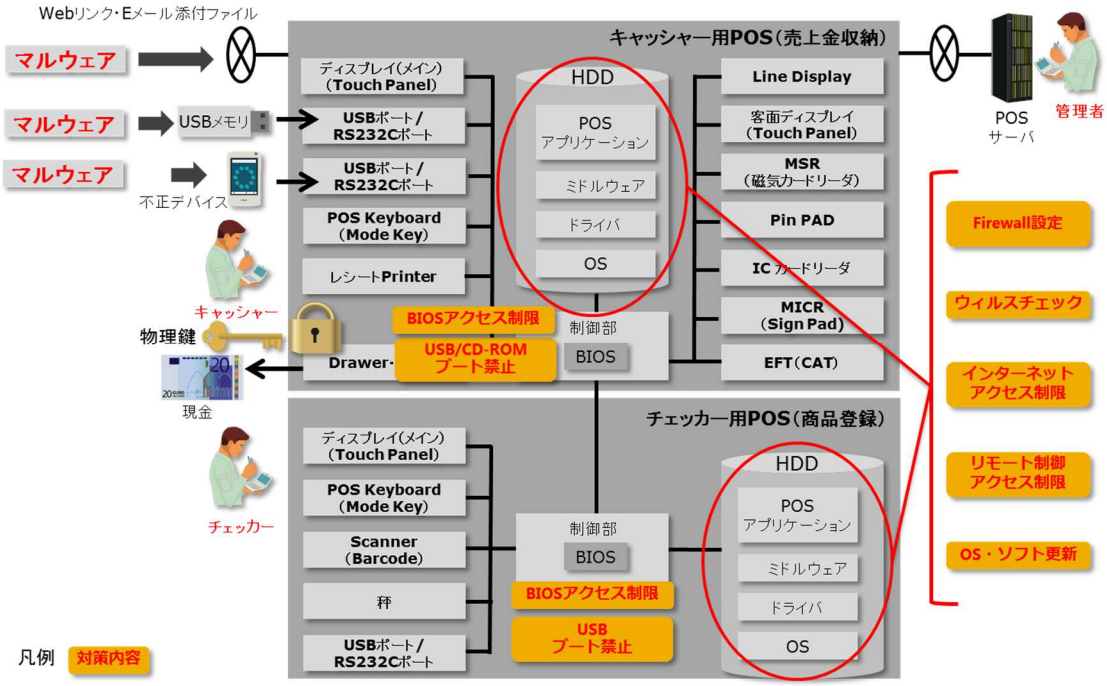

図 3-2 事例におけるセキュリティ対策着眼点

このように、提案されているセキュリティ対策はハードディスクドライブ内に存在する情報資産の保護に偏っていることが分かる。一方、ハードディスクドライブ内に存在する情報資産とはアプリケーション、ミドルウェア、ドライバ、OS などであり、このように多層構造に分かれて構造が複雑な上に、セキュリティとして管理すべき項目も多岐に渡る。

さらに、アプリケーションは店舗のサービス内容の変更やカスタマイズなどにより、頻繁に更新が生じる。このような状況の中で、セキュリティ対策上、管理すべき項目が一つでも抜ければ、悪意を持つ人の攻撃に晒されるのでその管理負担が大きくなる。その管理を徹底しようとすると、逆に運用の柔軟性が失われることになる。

また、セキュリティ対策案が運用の制約上、適用できない場合がある。その例として、事例で提案されたセキュリティ対策の 1 つにウイルスチェックがある。しかしながら従来の POS では CPU やメモリ条件、あるいはアプリの稼働環境の制約から常駐型のウィルスチェックソフト（ウィルスバスター等）を実施することができない。また、ワクチン情報

も頻繁にリリースされるがダウンロードにも制約があり、現地で更新することができない。

その他の懸案として、作業員が不正行為を働いても、あるいは、ミスなどにより不適切な作業を行っても、それを管理したり検証したりすることが困難である。既存の対策提案に対する懸案事項を図 3-3 に纏めた。

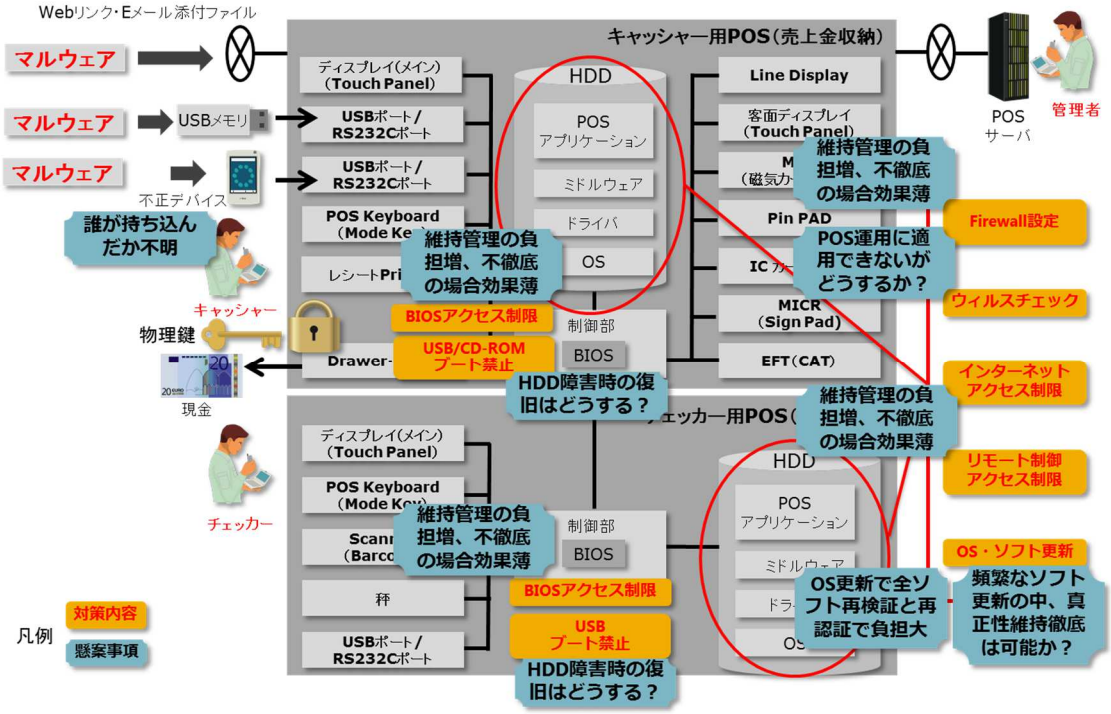

図 3-3 既存のセキュリティ対策の懸案事項

4 セキュリティ対策指針

3 章で説明したように、内部犯罪であることや、運用に携わる者のモラルやスキルを期待できないこと、情報漏えいや不正デバイス接続のリスクセキュリテイ対策を検討するにあたり考慮しなければならない。さらに既存のセキュリティ対策のほとんどは、HDD の中の情報資産を保護することが最終目的であるため、セキュリティ対策を行うにあたり次のような管理面の課題がある。

(a) 保護すべき項目が多岐にわたり、管理不徹底に陥りやすい。特に、多数の端末を管理する場合はその傾向が強い。
(b) OS、ファームウェアは専用 OS ではなく、Microsoft Windows 等市販ソフトをベースとしており、セキュリティパッチや OS バージョンアップなどがこまめにリリースされるが、運用上それらを現地で更新することは非常に困難である。
(c) OS、ソフトウェア、ファームウェアの更新に伴う再検証負担増と再認証負担増の考慮がされていない。
(d) 障害時や復旧時の脆弱性対策が不十分である。
(e) 提案されたセキュリティ対策が運用に適用できない場合がある。

このように、現場の運用実態や運用者の本音を無視したセキュリティ対策では、実効性のある対策ができない。そこで実効性のある対策を行うために、どのような前提のもとに、適切な対策指針を取るべきかを述べる。

4.1 セキュリティ対策を考えるための前提

❒ 前提1：開発者、運用者、操作者、保守員は信用できない（性悪説）。

3 章で説明した事例から、マルウェア開発者は POS システムに関連する仕様書を参照したと推測される。また、物理的な不正デバイスが POS システムに接続されていたことから内部関係者が関連していた可能性も考えられる。このように安全を脅かす内部不正の存在可能性を認識し、セキュリティ対策を考える上では、開発者、運用者、操作者は全て信用できないという前提をおく必要がある。

❒ 前提2：POS運用に関わる運用者、操作者、保守員のモラルとスキルは低い。

前提 1 でも説明したように、内部関係者が不正デバイスを POS システムに接続したと判断すると、POS 運用に関わる関係者のモラルとスキルは低いという前提を置く必要がある。また、近年の就労形態の多様化が高まっていることからあまり訓練されていない人材が多

数存在し、悪意がない場合でもミスをすることで情報漏洩に繋がるリスクを想定しておく必要がある。また、関係者のミスを防ぐとともにミスがあっても安全を守る対策を考慮することも必要であるが、結果として、複雑な操作や手順を POS 運用に関わる関係者に課せないことを前提として考えることも重要である。

❒ 前提3：インターフェース仕様は公開されている。

2.23 章で説明した事例から、不正デバイスを POS 端末へ接続するための POS 周辺装置のインターフェース仕様をマルウェア開発者が参照したと推測される。インターフェース仕様は、オープンで多様な POS 端末の実現と POS アプリケーション開発の生産向上を目的として、OPOS 技術協議会により国際統一仕様に向けて標準化され、OLE for Retail POS といった POS システムに容易に統合できるインターフェース仕様などが Web に公開、流通、使用されている。また、この仕様は随時進化しており、POS で利用するほぼ全てのデバイス用のインターフェースの標準仕様が策定されていることから、随時公開、流通、使用されている仕様をマルウェア開発者に参照されないために管理、隠蔽することは極めて困難である。

❒ 前提4：不正改造されたものや、許可されていないデバイスが接続されることがある。

3 章で説明したように、不正デバイスを POS システムに接続しスキミングの手口でカード情報を盗まれる事例が実際に発生していることや、POS 端末に搭載されているデバイス接続用のポートが USB ポートやシリアルポートといった汎用性のあるポートなため許可されていないデバイスを接続することは物理上可能である。セキュリティ対策を考える上で不正改造されたものや許可されていないデバイス、意図しないデバイスなど様々な機器やシステムが接続されることを前提として考える必要がある。

❒ 前提5：運用の制約上、適用できないセキュリティ対策内容がある。

3 章で説明したように、セキュリティ対策内容としてウイルスチェックが提案の 1 つとしてあるが、POS の運用の制約上実施することができない。運用の制約条件を反映すると、適用できないセキュリティ対策内容があることを前提として考える必要がある。

4.2　セキュリティ対策方針

前節で説明した前提の下で、セキュリティ対策を行うための方針を次に示す。ここでは、IPA が先行して公開している「つながる世界の開発指針」の１７指針と本書の内容、および IoT コンソーシアムが公開している「IoT セキュリティガイドライン」との対応を示しながら、以下に説明する。

表 4-1「つながる世界の開発指針」に対応する本書での対応箇所

「つながる世界の開発指針」			本書での対応箇所	
大項目		指針	章番号	概要
方針	つながる世界の安全安心に企業として取り組	指針1 安全安心の基本方針を策定する	n/a	基本方針の策定については本書の対象外。
		指針2 安全安心のための体制・人材を見直す	n/a	体制・人材の見直しについては本書の対象外。
		指針3 内部不正やミスに備える	方針5	内部不正やミスに対しても検知する仕組みを記述。
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する	方針1	保護すべき情報や資産の優先順位付けと保護対象の選定について記述。
		指針5 つながることによるリスクを想定する	方針1,5,8	つながるリスクを想定し、保護すべき対象の優先順位付け、つながった時の想定外の動きなど、トレーサビリティの強化について記述。
		指針6 つながりで波及するリスクを想定する	方針1,2	つながりで波及するリスクを想定し、保護対象の優先順位付けや保護すべきドメインの局所化について記述。
		指針7 物理的なリスクを認識する	方針8	物理的なリスクを想定し、デバイスのトレーサビリティ強化について記述。
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする	方針2～6	実施方法の例として、その対策範囲、対策レベル、対策検討について記述。
		指針9 つながる相手に迷惑をかけない設計をする	方針5,7,8	実施方法の例として、異常検知、対策検討について記述。
		指針10 安全安心を実現する設計の整合性をとる	方針6	なるべく下位階層でセキュリティ対策を行うことによる柔軟性の確保と管理のしやすさについて記述。
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする	方針4	仕様書が公開されても致命的にならない仕組みの検討について記述。
		指針12 安全安心を実現する設計の検証・評価を行う	方針6	指針10と同一
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける	方針5,7	実行中のプログラムを検知する仕組みやトレーサビリティの投入により自身の状態や時間が経っても安全安心を維持する機能について記述。
		指針14 時間が経っても安全安心を維持する機能を設ける	（同上）	指針13と同一
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する	方針8	出荷後に必要となるトレーサビリティの強化について記述。情報発信については本書の対象外。
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える	n/a	関係事業者への周知徹底は本書の対象外
		指針17 つながることによるリスクを一般利用者に知ってもらう	n/a	一般利用者への周知徹底は本書の対象外

表 4-2「IoT セキュリティガイドライン」に対応する本書での対応箇所

「IoTセキュリティガイドライン」			本書での対応箇所	
大項目		指針	章番号	概要
方針・管理	方針1 IoTの性質を考慮した基本方針を定める	要点1 経営者がIoTセキュリティにコミットする	n/a	基本方針の策定については本書の対象外。
		要点2 内部不正やミスに備える	方針5	内部不正やミスに対しても検知する仕組みを記述。
分析	方針2 IoTのリスクを認識する	要点3 守るべきものを特定する	方針1	保護すべき情報や資産の優先順位付けと保護対象の選定について記述。
		要点4 つながることによるリスクを想定する	方針1,5,8	つながるリスクを想定し、保護すべき対象の優先順位付け、つながった時の想定外の動きなど、トレーサビリティの強化について記述。
		要点5 つながりで波及するリスクを想定する	方針1,2	つながりで波及するリスクを想定し、保護対象の優先順位付けや保護すべきドメインの局所化について記述。
		要点6 物理的なリスクを認識する	方針8	物理的なリスクを想定し、デバイスのトレーサビリティ強化について記述。
		要点7 過去の事例に学ぶ	方針5	要点2と同一
設計	方針3 守るべきものを守る設計を考える	要点8 守るべきものを特定する	方針2～6	実施方法の例として、その対策範囲、対策レベル、対策検討について記述。
		要点9 つながる相手に迷惑をかけない設計をする	方針5,7,8	実施方法の例として、異常検知、対策検討について記述。
		要点10 安全安心を実現する設計の整合性をとる	方針6	なるべく下位階層でセキュリティ対策を行うことによる柔軟性の確保と管理のしやすさについて記述。
		要点11 不特定の相手とつなげられても安全安心を確保できる設計をする	方針4	仕様書が公開されても致命的にならない仕組みの検討について記述。
		要点12 安全安心を実現する設計の検証・評価を行う	方針6	要点10と同一
構築	方針4 ネットワーク上での対策を考える	要点13 自身がどのような状態かを把握し、記録する機能を設ける	方針5,7	実行中のプログラムを検知する仕組みやトレーサビリティの投入により自身の状態や時間が経っても安全安心を維持する機能について記述。
		要点14 機能及び用途に応じて適切にネットワーク接続する	方針7,8	適切にネットワーク接続しているか知るためネットワーク接続や利用開始時におけるトレーサビリティについて記述。
		要点15 初期設定に留意する	方針8	トレーサビリティ強化において、初期設定についての留意を追記。
		要点16 認証機能を導入する	方針4	要点11と同一
運用・保守	方針5 情報発信・共有を行う	要点17 出荷・リリース後も安全安心な状態を維持する	方針5,7	要点13と同一
		要点18 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	方針8	出荷後に必要となるトレーサビリティの強化について記述。関係者への周知徹底は本書の対象外。
		要点19 つながることによるリスクを一般利用者に知ってもらう	n/a	関係者への情報発信・共有は本書の対象外
		要点20 IoTシステム・サービスにおける関係者の役割を認識する		
		要点21 脆弱な機能を把握し、適切に注意喚起を行う		
一般利用者向け	ルール1 問い合わせ窓口やサポートがない機器やサービスの購		n/a	一般利用者への周知徹底は本書の対象外
	ルール2 初期設定に気をつける			
	ルール3 使用しなくなった機器については電源を切る			
	ルール4 機器を手放す時はデータを消す			

❒　方針1:保護すべき情報や資産の優先順位を付け、致命的になる情報や資産を選別する。

セキュリティ対策の観点では、機器の動作に関わる情報や機器やシステムで生成される情報もつながることで漏えいしないよう保護することが前提であるが、すべての情報や資産を等しく保護することは非効率であり、対策コストも大きい。一方、不正行為を働いたりする者や犯罪者が狙う情報資産や現物資産は限られる。そのため、守るべき機能や情報を洗い出し、保護すべき対象の優先順位を付け、致命的になる情報や資産が何かを特定する必要がある。特に、過去に起きた犯罪事例と類似の犯罪は将来再度起こりうるので、過去の攻撃対象となったクレジットカード番号は勿論のこと、近年ではポイントカードを含む個人情報などの情報、資産を考慮して保護対象を選定する必要がある。

重要度	既存規格※や枠組みでの保護対象	既存規格※や枠組みでの保護されない対象
高	・暗証番号 ・磁気カードデータ	・入出金コマンド ・POS売上明細データ ・ポイント会員番号
中	・カード番号 （カード番号を含むログデータも対象）	・カードデータ （アプリ内のメモリ上）
小	－	上記を含まないログデータ等

※既存規格：PCI（Payment Card Industry）、EMV（Europay Master Visa）

図 4-1 保護すべきデータの重要度

❒　方針2：保護すべきドメインをできるだけ小さくする、あるいは切り離す。

クローズドなネットワーク向けの機器やシステムであっても保守時の USB メモリ経由などによりマルウェアに感染する可能性があることから、つながることによるリスクを想定する必要がある一方、保護範囲が広いとつながりで波及するリスクに対応する対策や管理維持の負担が大きく、抜けが生じやすい。そのため、保護すべきドメインはできるだけ小さくする必要がある。かつ、保護すべきドメインはできるだけシンプルなものが望ましい。同じデータを保護するのでも、構造が複雑で更新が頻繁なドメインで保護する場合と、構造がシンプルで更新頻度が少ないドメインで保護する場合とでは、後者の方が対策強度、運用の柔軟性、コストの面で圧倒的に有利である。

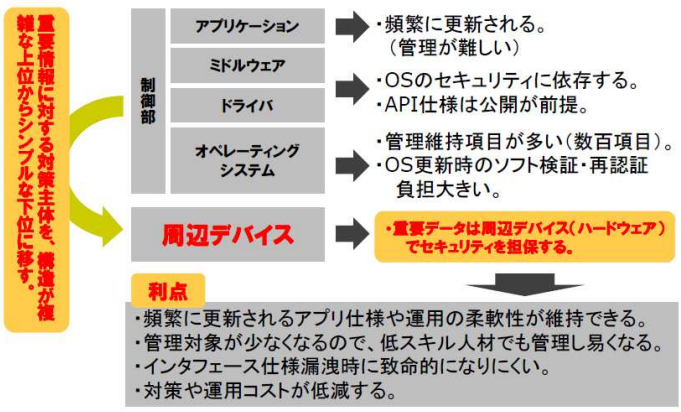

図 4-2 保護すべきデータの重要度

❒ 方針3：保護すべきデータの重要度に応じて対策レベルを変える。

限られたリソースとコストで最大の効果を得ようとすると、保護すべきデータの重要度に応じて対策レベルを変えることが、運用の柔軟性とコストの面で重要である。

❒ 方針4：仕様書が公開されても致命的にならない仕組みを取り入れる。

4.1 節の前提 3 で説明したように、標準化されたインターフェース仕様は幅広く流通しており、これらの情報を管理して隠蔽することは極めて困難である。そこでインターフェース仕様が公開されても致命的にならない仕組みが必要となり、最も効果があるのは現代暗号通信技術の考え方を導入することである。現代暗号通信技術では、アルゴリズムや仕様は公開されていて誰でも知ることはできるが、暗号解読の計算複雑性と暗号鍵管理でデータを保護する。インターフェース仕様に暗号化を前提とするデータを盛り込めば、仕様書が公開されてもそれだけでは、インターフェースを乗っ取ることはできず安全性を確保できる。

❒ 方針5：実行を許可されていないプログラムを検知する仕組みを取り入れる。

4.1 節の前提 5 の内容を考慮して、運用の制約条件を反映した結果、セキュリティ対策が適用できるか検討し、できない場合はその代替案を検討する。例として、ウイルスチェックが適用できない場合、ウイルス（マルウェア）の実行を検知（実行プログラム監視）するのと同等の仕組みを取り入れる必要がある。代替案例として、実行を許可されていないプログラムを検知（実行プログラム監視）するホワイトリストの仕組みを導入する検討を行う。ホワイトリストに登録されたソフトウェア以外の起動を阻止することで同等の安全性を確保する仕組みを検討する。また、ホワイトリストの登録過程に不備がある場合、マルウェアが混入した状態でホワイトリストに登録されるリスクがあるため、そのための管理工数や検証工数も必要コストとして見込んでおく。なお、POS 端末内部の実行プログラム監視だけでなく、不正に接続された光学デバイスや USB メモリ等の周辺機器ドライバについても同様に検知する仕組みを検討する。また、異常な状態が検知された場合は、他の IoT 機器やシステムに波及する可能性があるため異常プログラムや不正なドライバの実行の停止や他のネットワークから切り離す等の適切な対策も合わせて検討する。

❒ 方針6：できるだけ既存の仕様と運用の柔軟性を確保する。

通常、POS システムにおいて発生するリスクの箇所としては、内部犯行、不正アクセス、攻撃や他機器からの誤作動データの入り口となる外部インターフェースが挙げられるため個々の POS システムで対応しきれない場合はそれらを含む上位の POS システムで対策が検討するのが一般的である。とはいえ、複数の階層を持つ POS のシステム設計では、下

位階層はなるべく汎用性を持たせてシンプルな機能構成にする一方、上位階層はさまざまなカスタマイズや変更が頻繁に起こるため、上位階層で制約条件の大きなセキュリティ対策を行うと、仕様や運用に過度な制約が掛かり、柔軟性が失われる。そのため、同じセキュリティ対策を行うのであれば、なるべく下位階層で対策を行った方が柔軟性を確保して管理しやすく有利である。

❒ 方針7：対策コストをできるだけ安くする。

対策コストが安くなければ社会全体に普及させることはできない。保護すべき情報や資産を選別して、保護すべきドメインをできるだけ小さくし、かつ、保護ドメインを下位側で実現することで、対策費用や運用保守コストを下げることが可能になる。

一方、すべてのセキュリティ対策をソフトウェアやデバイスなどで完結させようとするとコスト的にも不利な上、抜けも生じやすい。仕様や運用の柔軟性を確保するのも困難になる。4.1 節の前提 4 で説明したように、不正改造されたものや、許可されていないデバイスが接続されることを想定するのであれば、デバイスだけで対策しようとすると正規デバイスに対して耐タンパ性が必要となる。その結果、POS 端末のコストが上がるだけでなく、高度なセキュリティ対策の施された修理拠点でしか修理ができなくなり、保守コストが高くなるだけでなくリードタイムも長くなり、運用の柔軟性が大きく損なわれることになる。

そこで、ソフトウェアやデバイスのセキュリティ対策を補うために、トレーサビリティを導入し、犯罪の抑止力として活用することが有効と考えられる。適切なトレーサビリティ機能は、運用や保守に大きな障害とならないので柔軟性が確保できる。IoT 時代が到来し、つながる世界が一般的になるとトレーサビリティに必要なインフラはさらに大きく普及してコストも安くなることが期待できるので、将来、有効なセキュリティ対策として活用することが見込まれる。このトレーサビリティに関しては、運用中だけでなく、破棄フェーズでも考慮しなければいけない。

❒ 方針8：トレーサビリティを強化する。

POS 分野では、以下、(1)～(4)の観点でトレーサビリティの強化を検討する。

また、トレーサビリティの強化を実施する場合は、記録する時の POS の状態（Firewall ポリシー設定、ウイルス対策ソフトのインストール有無、エンジンバージョンやパターンファイルのバージョン、ネットワーク設定　等）も合わせて記録・保持する仕組みを検討する。

(1) POS システムの構築・ネットワーク接続におけるトレーサビリティ

従来、専用機、専用線で利活用されていた POS システムにおいても、汎用的なタブレット端末の利用や、無線 LAN を含む公衆ネットワークの活用をはじめとするオープン化が進展してきている。店舗ネットワークにおける脅威の観点から POS の構築・ネットワーク接続においては、以下のような POS のネットワークの初期設定および運用中の設定を記録・保持する仕組みを検討する。

[汎用的な POS システムで、確認・記録すべきネットワーク設定項目の例]

・ブラウザの設定
・メールの設定
・リモート接続の設定
・telnet、FTP 関連サーバ機能の設定（レガシーサービス機能の設定、プロトコル）
・ssh 関連サーバ機能の設定
・ファイル共有機能の設定　等

(2) 重要デバイス内資産のトレーサビリティ

POS 運用の事例として、通常、返品処理を行う場合、お客様から返品対象のレシートを回収し、過去の取引を確認した後返品処理を行うが、現場の運用制約上、レシートが無くても返品処理を行うことが可能である。そのため過去に取引が無くても不正な返品処理操作により紙幣を取り出すことができる。

そこで、カードリーダや釣銭機のような内部に重要な物理資産や情報資産を抱えている重要デバイスに対しては、不正操作を検知するため、過去の取引の裏付けのない入出金処理を受け付けない仕組みにするためのクレジット取引や入出金処理のログを保持する仕組みを検討する。

(3) 保守用重要デバイスのトレーサビリティ

4.1 節の前提 4 で説明したように、「不正改造されたものや、許可されていないデバイスが接続されることがある」ということを考えると、保守用重要デバイスのトレーサビリティが必要になる。例えば、許可されていない不正なデバイスが接続されると重要な情報資産が喪失、あるいは、漏えいしてしまうので、各デバイスの付け外しを記録、通知して検証するための仕掛けを検討する。

(4) 保守作業のトレーサビリティ

上記「(1) 重要デバイス内資産のトレーサビリティ」で説明したように、重要デバイス間で暗号通信を行ったとしても誤って暗号通信の暗号鍵設定作業にミスが発生してセキュリティが緩和される、または物理鍵を紛失して悪意のある者に釣銭機を施錠される等の不適切な保守作業による重要な情報資産の喪失、あるいは、漏えいしてしまうリスクが存在する。

そこで、暗号通信の暗号鍵設定作業や定期的な物理鍵変更などの保守作業が適切に行われたかを追跡するための作業トレーサビリティとその検証を検討する。

4.3　クレジット取引セキュリティの考え方

クレジット取引に関わるクレジット情報のセキュリティ対策については、別途定義されている「クレジット取引セキュリティ協議会」における「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2016-」（H28.2.23 公表）に基づいて方策を実施する。

(1) クレジット処理機能の POS からの分離

クレジット処理に関して、守るべきセキュリティ情報として、

・カード情報（磁気/IC）

・暗証番号（PIN）

がある。これら機微情報の取扱を「実行計画」に基づき、POS から物理的/機能的に分離する。

(2) セキュリティ情報の非保持化

カード情報を POS システムに『通過』させないよう、POS の機能と決済機能を分離すること、分離した決済専用端末からカード情報を取り込まないことによってカード情報の非保持化を実現する。

(3) クレジット機能におけるセキュリティ規格について

クレジット処理のためのセキュリティ規格については、クレジットカードの国際ブランド等が制定する国際的規格と認定基準が定義されており、上記(1)、(2)の方針は当該規格となる「EMV 規格」および「PCI 規格」に基づき国際ブランドからの認定を要するため、本ガイドラインの対象外とする。

5 開発フェーズとセキュリティの取組み

5.1 ライフサイクルにおけるフェーズの定義

システム開発には計画から廃棄に至るまでのライフサイクルが存在する。その全てのフェーズにおいてセキュリティを考慮することが重要である。本章では NIST SP800-64「Security Considerations in the System Development Life Cycle」で定義されている典型的なシステム開発ライフサイクル（SDLC）と各フェーズのセキュリティへの取組みについての概要を説明する。

システム開発ライフサイクルは大きく以下の 5 フェーズに分けられる。

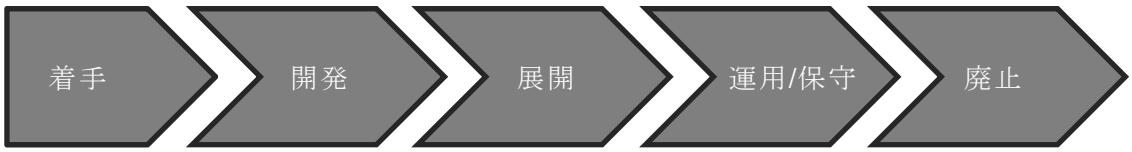

図 5-1 ライフサイクルにおけるフェーズ

表 5-1 フェーズの定義

フェーズ	説明
着手	システムへの要求を明確化し、目的を文書化するフェーズである。SDLC の最初のフェーズであるこのフェーズにおいてセキュリティを考慮することはシステムライフサイクルの観点で非常に重要である。このフェーズのセキュリティ活動には以下のようなものがある。 ・機密性、完全性、可能性に関するビジネス要件の概要を明らかにする。 ・情報を分類し、個人情報などの伝送、保存などの取り扱い要件を明らかにする。 ・プライバシー要件を明らかにする。 システム開発の早期において適切なリスクマネジメント計画を作成し、関係者に通知しておくことで、結果としてプロジェクト全体で見て費用面、時間面での節約につながる。
開発	システムを設計、開発するフェーズである。このフェーズにおける主なセキュリティ活動は以下のようなものがある。 ・リスクアセスメントを行い、その結果を使ってベースラインセキュリティ管理策を補足する。 ・セキュリティ要件を分析する。 ・機能テスト及びセキュリティテストを実施する。 ・システム承認と運用認可のドキュメントを用意する。

	・セキュリティアーキテクチャを設計する。
展開	受け入れテスト後、システムを展開するフェーズである。このフェーズの主なセキュリティ活動には以下のようなものがある。 ・情報システムを、そのシステム用の環境に統合する。 ・システム承認活動を計画し、実施する。この際、セキュリティ管理策のテストと同期が取れるようにする。 ・システム運用認可活動を完了させる。
運用・保守	システムを稼働するフェーズである。ハードウェアやソフトウェアを追加するなどにより、システムは随時変更される。このフェーズでは主に以下のセキュリティ活動がある。 ・システムのセキュリティ管理策の安全な運用と継続監視のための手順と手続きを確立する。 ・必要に応じて再運用認可を実施する。
廃止	システムを整然と停止し、重要な情報を保護し、データを新しいシステムに移行させるフェーズである。本フェーズの主なセキュリティ活動は以下のようなものである。 ・メディアをサニタイズする。 ・ハードウェアとソフトウェアを廃棄する。

5.2 各フェーズにおける取組み

前節で概説したシステム開発ライフサイクルでのセキュリティへの取り組み内容について説明する。POS の開発をターゲットとするため、以下では「システム」を「製品」と読み替える。

5.2.1 着手フェーズ

製品開発ライフサイクルの着手フェーズでは以下のようなセキュリティへの取組みが必要とされる。

表 5-2 着手フェーズのセキュリティ取組み

項番	システム開発ライフサイクル
1	**セキュリティ計画の作成** まず何より、製品開発の第 1 段階である着手フェーズにおいて、セキュリティ計画を立てることが重要である。セキュリティ計画では次のようなことを実施する。 ・製品開発におけるセキュリティ上の重要な役割、特に情報システムセキュリティ担当者を決定する。

	・セキュリティ要件の元となるもの（関連する法律、規定及び基準など）を特定する。 ・全ての主要関係者が、セキュリティ上の意味合い、考慮事項および要件などに関して、共通の理解を持てるようにする。 ・主要なセキュリティマイルストーン（草案レベル）を策定する。
2	**製品種別の分類** 必要とされるセキュリティレベルを決定するため、開発対象となる製品の種別を分類する。
3	**事業に対する影響の評価** 製品に関してセキュリティ上の問題が発生した場合、事業に対してどのような影響があるのかを明らかにする。
4	**個人情報に対する影響の評価** 開発対象製品が個人情報に関わる情報を伝達、格納、作成するかどうかを考慮する。開発対象製品が個人情報に関わる情報を扱う場合は、適切な保護対策とセキュリティ管理策を取り決め、実施しなければならない。
5	**セキュアな製品開発プロセスの実施** 早い段階におけるセキュリティの主な責任は開発チームが負うことになる。彼らは製品の詳細な機能について最も深く理解し、機能やビジネスロジックにおけるセキュリティ上の欠陥を特定する能力を備えている。彼らに期待していることを伝えることが、コードレベルに至るまでの保護環境を計画し、実施するための鍵となる。

5.2.2 開発フェーズ

製品開発ライフサイクルの開発フェーズでは以下のようなセキュリティへの取組みが必要とされる。

表 5-3 開発フェーズのセキィリティ取組み

項番	システム開発ライフサイクル
1	**リスク評価** リスク評価の目的は、システムデザイン、システム要件、およびセキュリティ要件を評価し、想定されるリスクを軽減する対策の効果を測定することである。評価結果によって、当該セキュリティ対策が十分であるか、更なる対応が必要であるかが明らかにされる。評価を成功させるには、システムドメイン内の各分野に精通している者（ユーザ、技術者、システム運用者等）の参加が必要である。 セキュリティリスク評価は、設計仕様の承認が行われる前に実施すべきである。なぜなら、この評価を行った結果、仕様の追加または調整が必要となることがあるからである。
2	**セキュリティ対策の選択** 開発プロセスに共通的なセキュリティ対策、および前述のリスク評価の結果として

	の対策から、当該製品開発にて実際に採用するものを選択する。
3	**セキュリティドキュメントの作成** システム開発の進捗に伴うコストの削減と、セキュリティ要件を正確に設計・開発に組込んでもらうため、以下の観点でセキュリティドキュメントを作成する。 ・構成管理計画 ・緊急時対応計画（ビジネス影響分析を含む） ・継続的な監視計画 ・セキュリティの意識向上、トレーニングおよび教育（SATE）計画 ・インシデント対応計画 ・プライバシー影響アセスメント（PIA）
4	**セキュリティ構想設計** セキュリティが製品にどのように組み込まれるかを理解することが重要である。セキュリティは構想設計を経て、製品設計に取り入れられるべきである。
5	**セキュリティの設計および対策の開発** セキュリティ対策を実際に設計、実装する。
6	**開発テスト、機能テストおよびセキュリティテストの実施** 開発または修正対象のシステム、ソフトウェア、ハードウェア、通信は展開される前にテストされなければならない。テストの目的はシステムが機能要件とセキュリティ要件を満たしていることを確認することである。

5.2.3 展開フェーズ

製品開発ライフサイクルの展開フェーズは以下のようなセキュリティへの取組みが必要とされる。

表 5-4 展開フェーズのセキュリティ取組み

項番	システム開発ライフサイクル
1	**セキュリティ承認、運用認可の計画を立てる** システム運用の認可権限者はシステム運用でのリスクを承認するための責任があるため、開発チームとセキュリティへの影響についてレビュー実施を計画する。
2	**確立した環境またはシステムへのセキュリティの統合** 運用サイトにて、製品がシステムとして統合される。統合テストおよび受け入れテストは、製品が納品され展開されるときに実施される。セキュリティ対策は、ベンダの指示、利用可能なセキュリティ実施ガイダンス、および文書化されたセキュリティ仕様に従って実施する。
3	**製品セキュリティ評価** 製品が機能要件とセキュリティ要件を満たしていることを確認する。組織は、製品

	の運用を開始する前に、セキュリティ承認を実施し、対策がどの程度正しく導入されているか、どの程度意図したとおりに運用されているかなどを評価しなければならない。
4	**情報システムの認可** 先のシステム評価の結果を受けて、対策が合意を得たレベルの保障を満たしているか、残存リスクが許容範囲内に収まっているかをチェックし認可する。

5.2.4 運用･保守フェーズ

製品開発ライフサイクルの運用・保守フェーズでは以下のようなセキュリティへの取組みが必要とされる。

表 5-5 運用・保守フェーズのセキュリティ取組み

項番	システム開発ライフサイクル
1	**システム本環境移行の準備状況確認** システムの本番環境移行に伴うシステム変更がある場合、リスクを軽減するために、この段階でセキュリティへの影響を評価する。
2	**構成管理の実施** 構成管理は、情報システム/製品のハードウェア、ソフトウェアおよびファームウェアコンポーネントの初期構成の確認と、システム/製品を変更していく上でのメンテナンスの観点で非常に重要である。
3	**継続的な監視の実施** 製品、および製品が運用される環境へのやむをえない変更があっても、セキュリティ対策の有効性が引き続き維持されることを監視する。

5.2.5 廃止フェーズ

製品開発ライフサイクルの廃止フェーズでは以下のようなセキュリティへの取り組みが必要とされる。

表 5-6 廃止フェーズのセキュリティ取組み

項番	システム開発ライフサイクル
1	**廃止／移行計画の作成** すべての関係者とシステムおよび情報を共有するため廃止／移行計画を作成する。計画の作成には重要なコンポーネント、サービス、および情報の廃止／移行ステータスの記録を考慮する。
2	**情報の保存** 情報を保存する場合、その情報が将来も必要となる可能性があるか、利用できるのかを十分に検討する。また、廃止する場合には法的要件も考慮する。

3	**メディアのデータ消去** 組織は、メディアのデータ消去と破壊処理を追跡、文書化、検証し、データ消去用の機器／手順を定期的にテストして、それらの機器/手順が正しく確実に機能するようにする。情報システムのデジタルメディアを破棄、または組織外で再利用する前に、それらのメディアのデータを消去、またはメディアを破壊し、権限のない者がメディアに含まれる情報にアクセスし利用することを防ぐ。
4	**ハードウェア/ソフトウェアの処分** ソフトウェアは、ライセンスまたは開発者、その他の契約/規則に従い処分する。ハードウェアに関しては、メディアを取り外した後でも機密情報が残っている場合は破壊して処分する。
5	**システムのクローズ** システムを終結するために必要なドキュメントを確認する。

5.3　各フェーズにおけるセキュリティ指針の取組み

本節では、各フェーズにおいて、4 章で説明したセキュリティ指針への取り組み内容について説明する。それぞれのシステム開発ライフサイクルにおいて、POS ガイドラインとして適用される方針の番号との対応を、表 5-7 に示す。

表 5-7 各フェーズのセキュリティ取組み

フェーズ	項番	システム開発ライフサイクル	POS 方針							
			1	2	3	4	5	6	7	8
着手	1	セキュリティ計画の作成	●							
	2	製品種別の分類	●							
	3	事業に対する影響の評価	●							
	4	個人情報に対する影響の評価	●							
	5	セキュアな製品開発プロセスの実施		●						
開発	1	リスク評価	●							●
	2	セキュリティ対策の選択		●	●	●	●			
	3	セキュリティドキュメントの作成		●	●	●	●	●		
	4	セキュリティ構想設計		●	●	●	●	●		
	5	セキュリティの設計および対策の開発			●	●	●	●		
	6	開発テスト、機能テストおよびセキュリティテストの実施			●	●	●	●		
展開	1	セキュリティ承認、運用認可の計画を立てる						●		
	2	確立した環境またはシステムへのセキュリティの配合						●		
	3	製品セキュリティ評価						●		
	4	情報システムの認可						●		
保守運用	1	システム本環境移行の準備状況確認					●		●	●
	2	構成管理の実施					●			●
	3	継続的な監視の実施					●		●	●
廃止	1	廃止／移行計画の作成		●					●	●
	2	情報の保存		●					●	●
	3	メディアのデータ消去		●					●	●
	4	ハードウェア／ソフトウェアの処分		●					●	●
	5	システムのクローズ		●					●	●

6 まとめ

本書はオープン POS 分野を対象としたセキュリティガイドラインとして作成したが、想定される脅威やライフサイクルにおけるセキュリティの取組みなど、他の分野でも応用できるところがあると考えられる。様々な製品の開発プロセスにおいてセキュリティ対策を考慮するにあたり、本ガイドラインを積極的に活用して欲しい。

なお今後も、対策指針に基づいたセキュリティ対策の検証結果や検証ノウハウを本ガイドラインにフィードバックを行い、本ガイドラインのブラッシュアップを継続する。

7 付録

セキュリティ要件　セルフチェックリスト

項番	チェック項目	対策例	検討工程						備考(チェック時に記入)
			方針管理	分析	設計	構築	保守運用	ユーザ教育	
1	観点：保護すべき情報の明確化 ・『製品分野別セキュリティガイドライン オープンPOS編』のセキュリティ対策指針に準拠した検討、対策がされているか？ 脅威例： ・オープンPOSのセキュリティ対策が欠落したままとなり、情報漏洩、盗聴やなりすましなどのリスクがある。	□ セキュリティ対策指針に準拠した基本方針を検討、対策する。	●	●					
2	観点：継続使用 ・OSの更新、ウイルス対策ソフトの更新などセキュリティ対策の運用を考慮しているか？ 脅威例： ・潜在的なセキュリティーホールが残ったままとなる。	□ 保護すべき情報を分析し、対策を検討する。 □ 攻撃されても致命的にならない設計を検討する。 □ 必要な時だけインターネット接続する。 □ 更新ファイルを手動でアップデートする。			●	●	●		
3	観点：周辺デバイス ・POSに空きのUSBポートが存在していないか？ 脅威例： ・データの抜き取り、情報漏えいにつながる。（セキュリティ面） ・差した直後、想定外の画面がアクティブになり、操作不可になる。（操作面） ・USBメモリからウィルス感染する可能性がある。	□ アプリケーションで使用できないように制御する。 □ USBのポートをBIOSレベルで使用不可にする。 □ USBのポートにカバーを付ける。			●	●	●		
4	観点：不明な機器 ・POSシステムに関係のない周辺機器のネットワークへの接続に対して対策しているか？ 脅威例： ・情報を盗む機器を接続できる。	□ ネットワークに接続可能なハードを登録制にする。 □ ネットワークに接続するためのキーを脆弱な番号（1234など）にしない。 □ ネットワークに接続するためのキーを管理する。				●	●		
5	観点：データの保管 ・取引データを平文で保存していないか？ 脅威例： ・取引データを盗まれ悪用される。	□ データを保存しない設計にする。 □ データを暗号化する機能を構築する。（盗まれても見ることができない） □ 期間や量を条件に、データを消去する。（漏えいする量を減らす） □ HDD交換時はデータを削除する。			●	●	●		
6	観点：データの保管 ・POS内に取引データを残したままにしていないか？ 脅威例： ・取引データを盗まれ悪用される。	□ データを保存しない設計にする。 □ データを暗号化する機能を構築する。（盗まれても見ることができない） □ 期間や量を条件に、データを消去する。（漏えいする量を減らす） □ HDD交換時はデータを削除する。			●	●	●		
7	観点：有線通信データの盗聴 ・店舗内LANでは、クレジット取引の電文を平文で処理していないか？ 脅威例： ・クレジット取引情報をネットワーク上の通信電文から盗まれ悪用される。	□ 通信を暗号化する仕組みを設計する。 □ ネットワークに接続する機器を制限して盗聴できない構成を構築する。			●	●			
8	観点：無線通信データの盗聴 ・店舗内LANを無線で行っている場合のセキュリティ対策を考慮しているか？ 脅威例： ・無線のため外部から見ることが容易。セキュリティが脆弱の場合、LAN通信の内容を見られる。	□ 有線LANにする。 □ LAN通信を暗号化する。 □ アクセスポイントが見れないようにする。				●	●		
9	観点：通信ポート ・不必要なポートが開いていないか？ 脅威例： ・不必要なポートが開いている場合、外部からの攻撃を受ける可能性がある。	□ 不必要なポートを閉じる。 □ 動作するサービスをリスト化して、監視する。				●	●		
10	観点：権限管理の脆弱性 ・管理系のツールが誰でも使用できる状態になっていないか。 脅威例： ・権限の高いログインID（店長など）のパスワードが変更できる。 ・自分の使用権限を変更（拡大）させることができる。	□ ユーザ権限機能を設けるなど使用者を限定する設計にする。 □ 管理系のツールは一般ユーザが使用するPOSには配置しない。 □ 管理系のツールは許可されたユーザのみアクセス可能とする。			●	●	●		
11	観点：障害調査 ・現地不具合調査時でも復旧に必要な最小限のログ出力しているか？ 脅威例： ・調査に不要な情報まで出力され、情報漏えいとなる。	□ 個人情報を含まなくても不具合調査できるように考慮した設計を行う。 □ 現地データを取得後に復号化して調査できるように考慮した設計を行う。 □ 不具合調査時はオフラインにして復号化を行い、オンライン前には 再度暗号する。			●		●		
12	観点：障害調査 ・取引中に障害が発生時、障害時の取引情報を印字やログに出力していないか？ 脅威例： ・取引情報を復旧するために、本来暗号化されている情報を非暗号化状態で印字やログ出力することで情報の覗き見が可能になる。	□ 一定の権限者のみ取引情報が読めるような対策をする。 □ セキュリティが担保されたルールに従い、出力した印字やログを破棄する。					●		
13	観点：パスワードの脆弱性 ・利用パスワードが脆弱（1234など）の場合の対策をしているか？ 脅威例： ・権限の高い店長レベルのログインIDが、一般店員やアルバイト使用されなりすましとなる。	□ 複雑なパスワードになるように、パスワード初期設定段階から入力を導く ように設計する。 □ 定期的にパスワードを変更するよう運用ルールを定義する。 □ ユーザに安易なパスワードを設定しないよう教育する。			●		●	●	
14	観点：サービス ・不必要なサービス（機能）を起動していないか？ 脅威例： ・不必要なサービス（機能）が起動している場合、外部からの攻撃を受ける可能性がある。	□ 不必要なサービス（機能）を停止する。 □ 動作するサービスをリスト化して、監視する。				●	●		
15	観点：不明アプリ ・業務に関係のないアプリの動作に対して対策しているか？ 脅威例： ・マルウェアに感染し、データを盗まれる。 ・ハードウェアに不要な負荷がかかる。	□ 動作するアプリを監視し、業務に関係のないアプリの動作阻止を検討する。 □ アプリをインストールできないようPOSを設定する。 □ ユーザはアプリをインストールしないよう教育、指導する。				●	●	●	

16	観点：ユーザのPOS運用状況 観点：外部アクセス ・POS上で、業務に関係のないホームページを見ていないか？ 脅威例： ・外部ホームページに接続することにより、ウィルス感染する可能性がある。	□ ローカルネットワークの外に出れるPOSを通信制限する。 □ POSでホームページを閲覧しない運用ルールを設ける。 □ ユーザがホームページを閲覧しないよう教育、指導する。				●	●	●	
17	観点：ユーザのPOS運用状況 ・ログオン状態でPOSから離席される状態を想定し、対応を検討しているか？ 脅威例： ・POSへログオンしたユーザと異なる人物が使用でき、成りすましができる。 ・データの改ざんや、架空の取引を行うことができる。	□ 離席する場合に、ログオフする運用ルールを定義する。 □ 数分操作が無い場合は、スクリーンセイバー起動し、 復帰にパスワード要求する機能を設ける。					●	●	
18	観点：ユーザのPOS運用状況 ・複数で1つのPOSログインIDを使いまわしていないか。 脅威例： ・トラブルが発生した場合、誰が使用していたか判別できない。	□ 一人一つのIDを持たせる。 □ 1つのログインIDで複数同時使用を禁止する。 □ 他者のIDを使用しない、使用させない。					●	●	
19	観点：ユーザのPOS運用状況 ・バーコードを使用してログインしていないか。 脅威例： ・ログインIDが分かると、第三者がバーコードを複製でき、本人以外で使用が可能（なりすまし）になる。	□ パスワードは手入力するなどの運用ルールを設ける。 □ POSのログインにバーコードを使用しない。					●	●	

参考文献

[1] つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識して欲しい重要ポイント～、独立行政法人情報処理　技術本部　ソフトウェア高信頼化センター

http://www.ipa.go.jp/sec/reports/20160511_2.html

[2] 「クレジット取引セキュリティ協議会」における「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-２０１６-」（H28.2.23 公表）

http://www.meti.go.jp/press/2015/02/20160223005/20160223005.html

[3] NIST Special Publication 800-64 Revision 2 （日本語訳）
情報システム開発ライフサイクルにおけるセキュリティの考慮事項

https://www.ipa.go.jp/security/publications/nist/

[4] US-CERT (UNITED STATES COMPUTER EMERGENCY READINESS TEAM)
Alert (TA14-002A) Malware Targeting Point of Sale Systems
https://www.us-cert.gov/ncas/alerts/TA14-002A

[5] IoT セキュリティガイドライン　セキュリティ確保上取り組むべき基本的な項目、IoT 推進コンソーシアム、総務省、経済産業省
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html