製品分野別セキュリティガイドライン
オープンPOS編

平成29年5月29日

CCDS セキュリティガイドラインWG
POS SWG

参考：POSガイドラインの目次構成

章	節	項	
1			はじめに
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
	2.2		POSシステム運用
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
	3.2		既存のセキュリティ対策の考え方とその限界
4			セキュリティ対策指針
	4.1		セキュリティ対策を考えるための前提
	4.2		セキュリティ対策方針
	4.3		クレジット取引セキュリティの考え方
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
	5.2		各フェーズにおける取組み
		5.2.1	着手フェーズ
		5.2.2	開発フェーズ
		5.2.3	展開フェーズ
		5.2.4	運用・保守フェーズ
		5.2.5	廃止フェーズ
	5.3		各フェーズにおけるセキュリティ指針の取組み
6			まとめ
7			付録
			参考文献

１．POSの運用業務

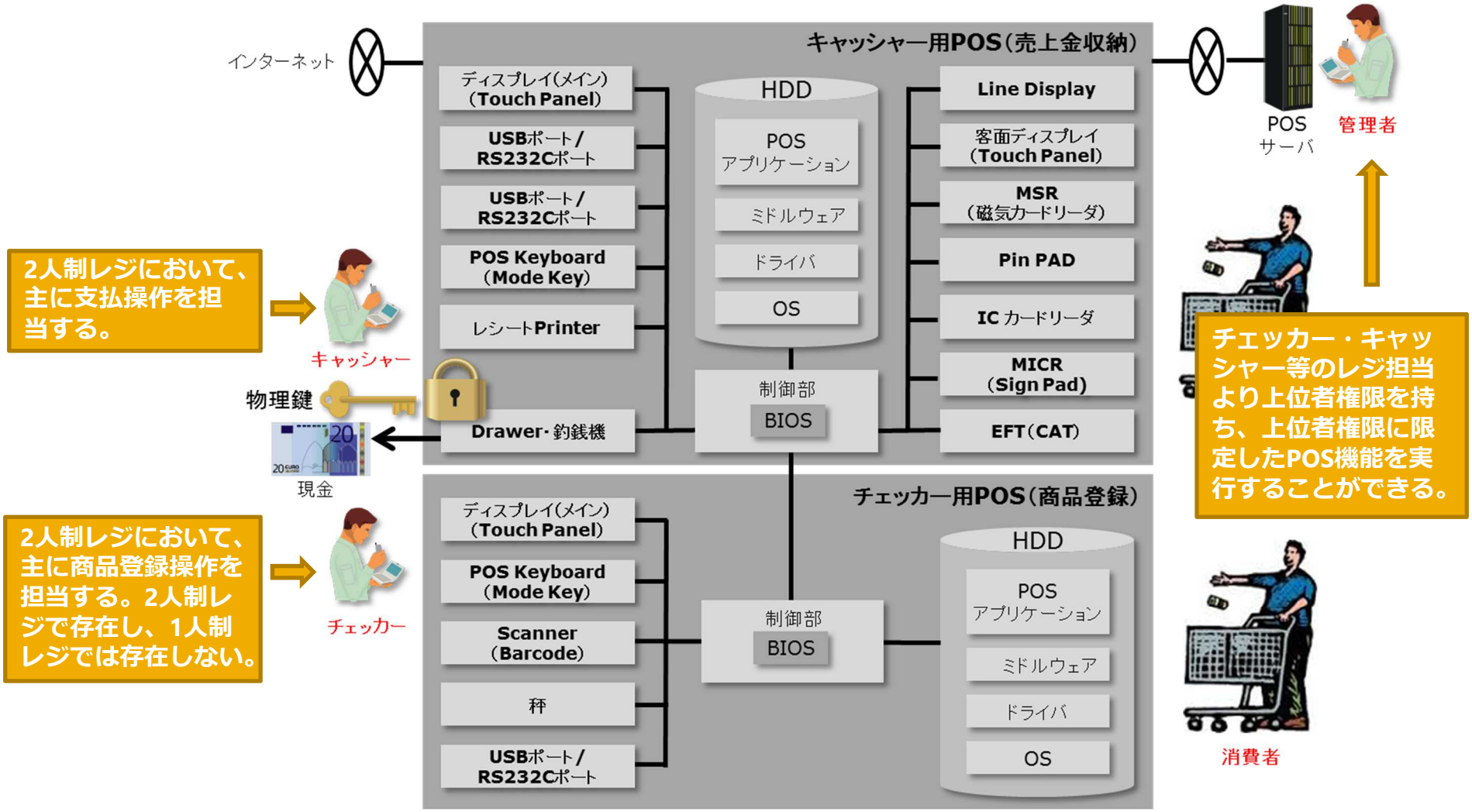
POSは店舗において、買い物客の売上を登録する機能と売上金を収納する機能を併せ持つ。売上登録を行う操作員をチェッカー、売上金収納を行う操作員をキャッシャーという。この両者は1人で行われることが多いが、大手量販店（特に食料品売場）の繁忙時間帯には2人に分かれて行われる。百貨店では集中レジシステムをバックヤードにおいて、売上と収納を分離する運用が行われている。

２．POSにおけるセキュリティ対策の必要性

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。

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。

2.POSのシステム構成と関係者



2.POSのシステム構成と関係者–その1–

■POSシステムの構成要素

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。

2.POSのシステム構成と関係者–その2–

項番	構成要素	機能
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。

2.POSのシステム構成と関係者–その3–

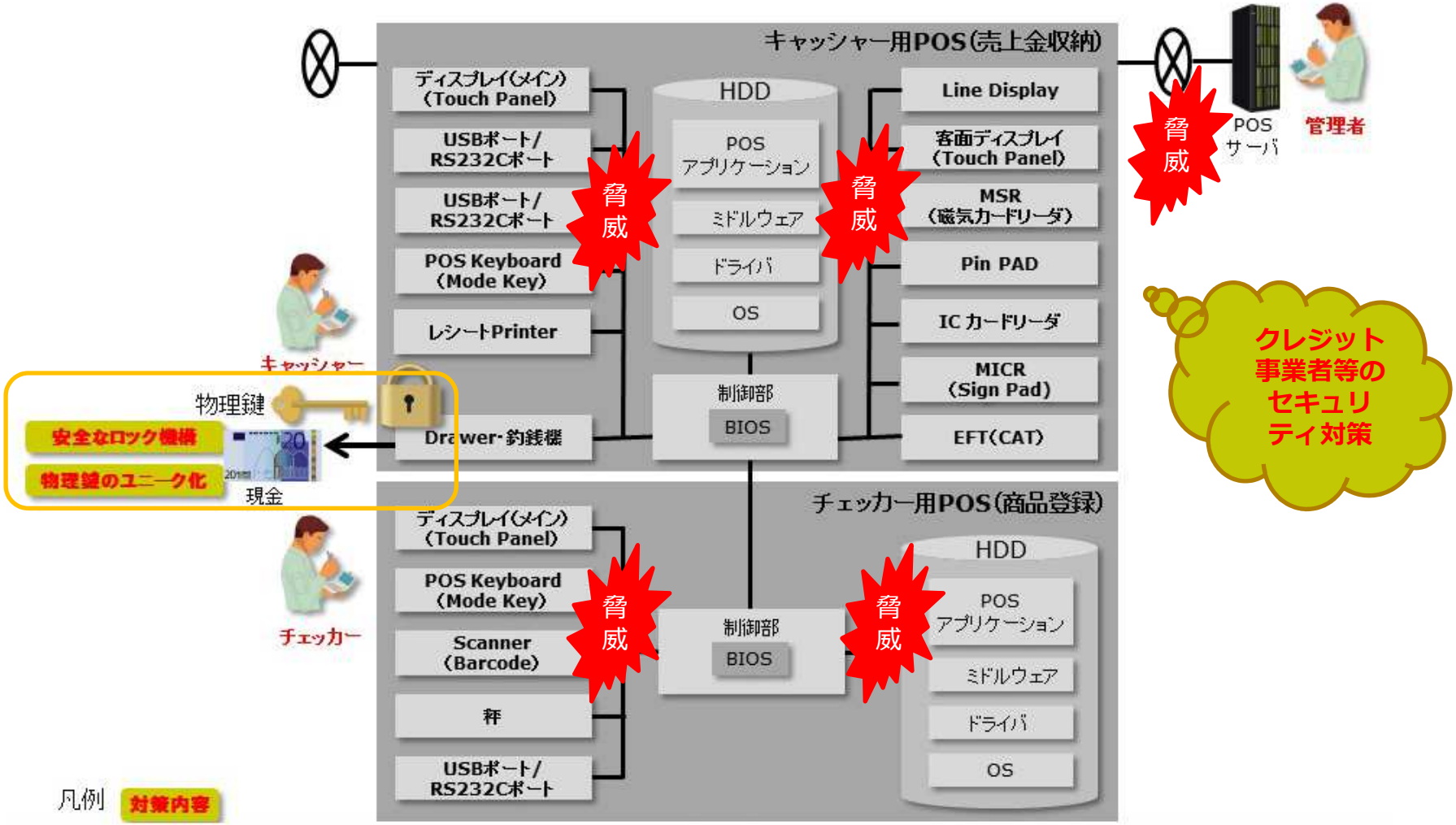
項番	構成要素	機能
19	釣銭機	釣銭機とは、POSからの制御で指定した金額を放出する機器のことであり、会計時に支払金額を入れたり、お釣りを出したりする。
20	Line Display	お店の設置環境に合わせて高さ調節可能な伸縮ポール型のカスタマーディスプレイ。四方向の設置が可能。

■POSシステムの関係者

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。

3.既存のセキュリティ対策

■これまでのセキュリティ対策のほとんどは、クレジット事業者等のセキュリティと金庫としてのDrawerの鍵管理のみ



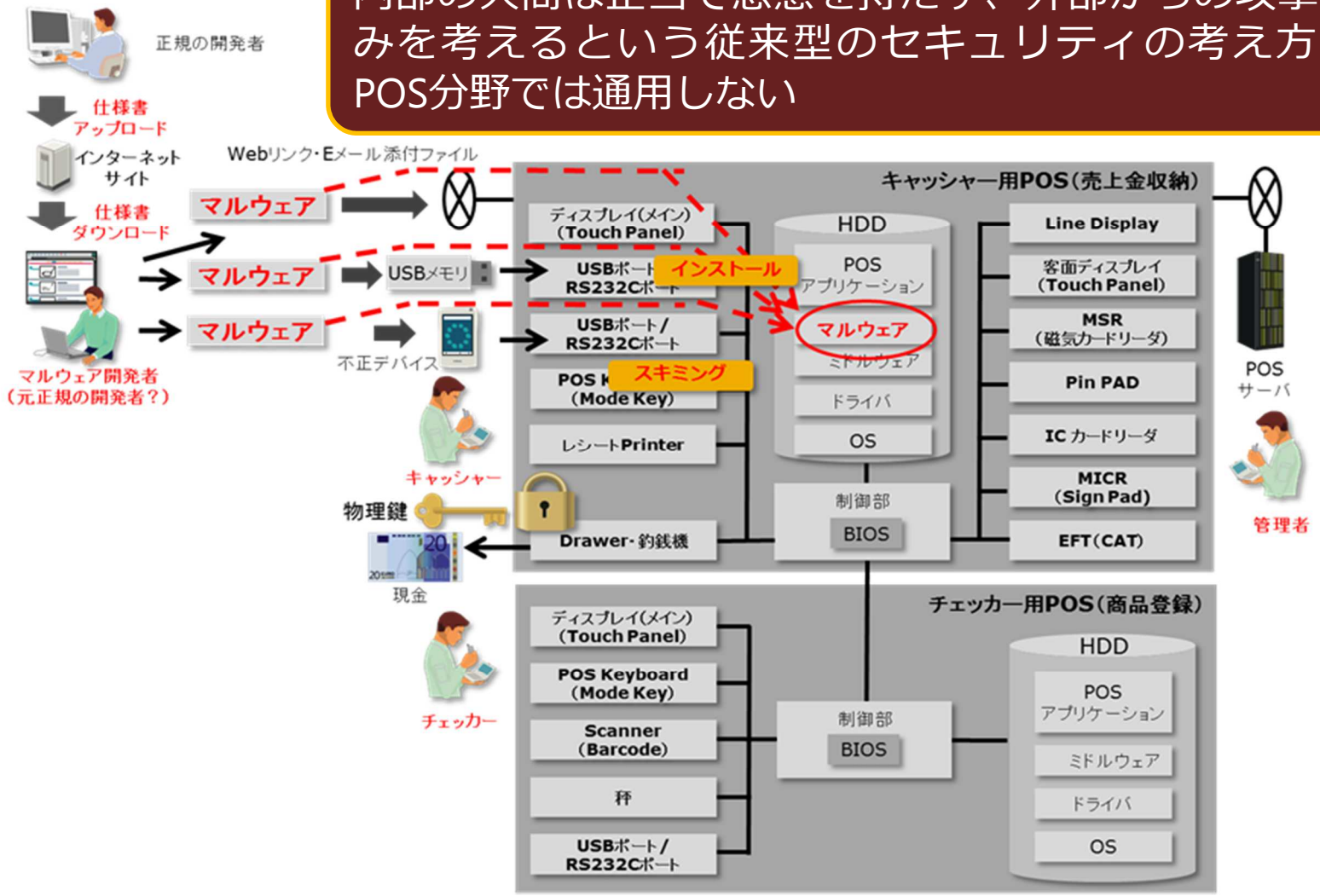
4.脅威を考慮すべき観点

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。
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。
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。
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。
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。

5. 脅威事例

■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）

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



6.既存セキュリティ対策の問題点–その１–

■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。

■保護すべき項目が多岐に渡り、管理不徹底に陥りやすい。特に、多大な端末を管理する場合はその傾向が強い。

■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。

■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ことはあまり考慮されていない。

■障害時復旧時の脆弱性対策が不十分である。

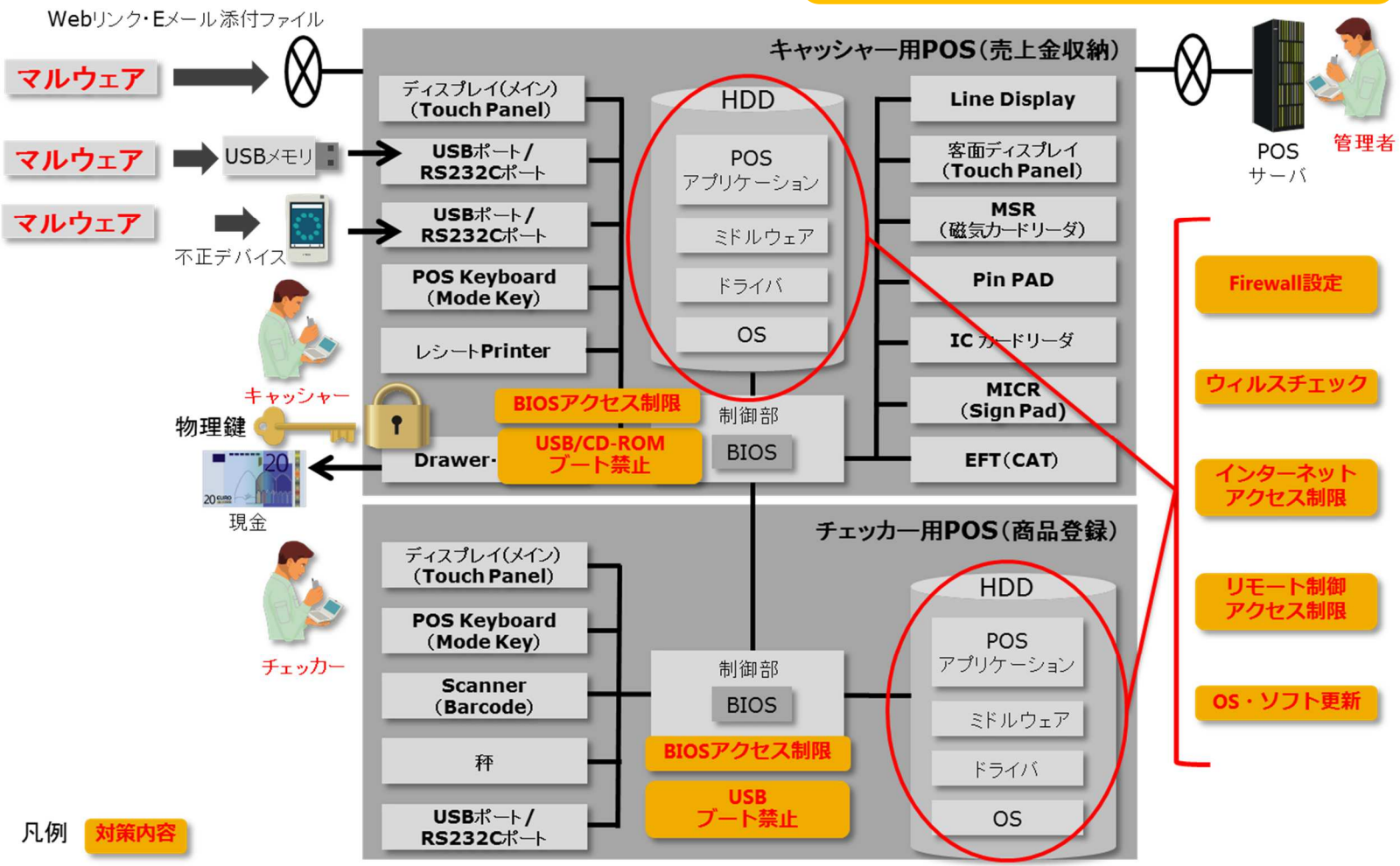
■提案されたセキュリティ対策が運用に適用できない場合がある。

■現場の運用実態や運用者の本音を無視して、正論だけ振りかざしても、実効性のある対策はできない。

6.既存セキュリティ対策の問題点–その２–

■既存のセキュリティ対策の着眼点の偏り

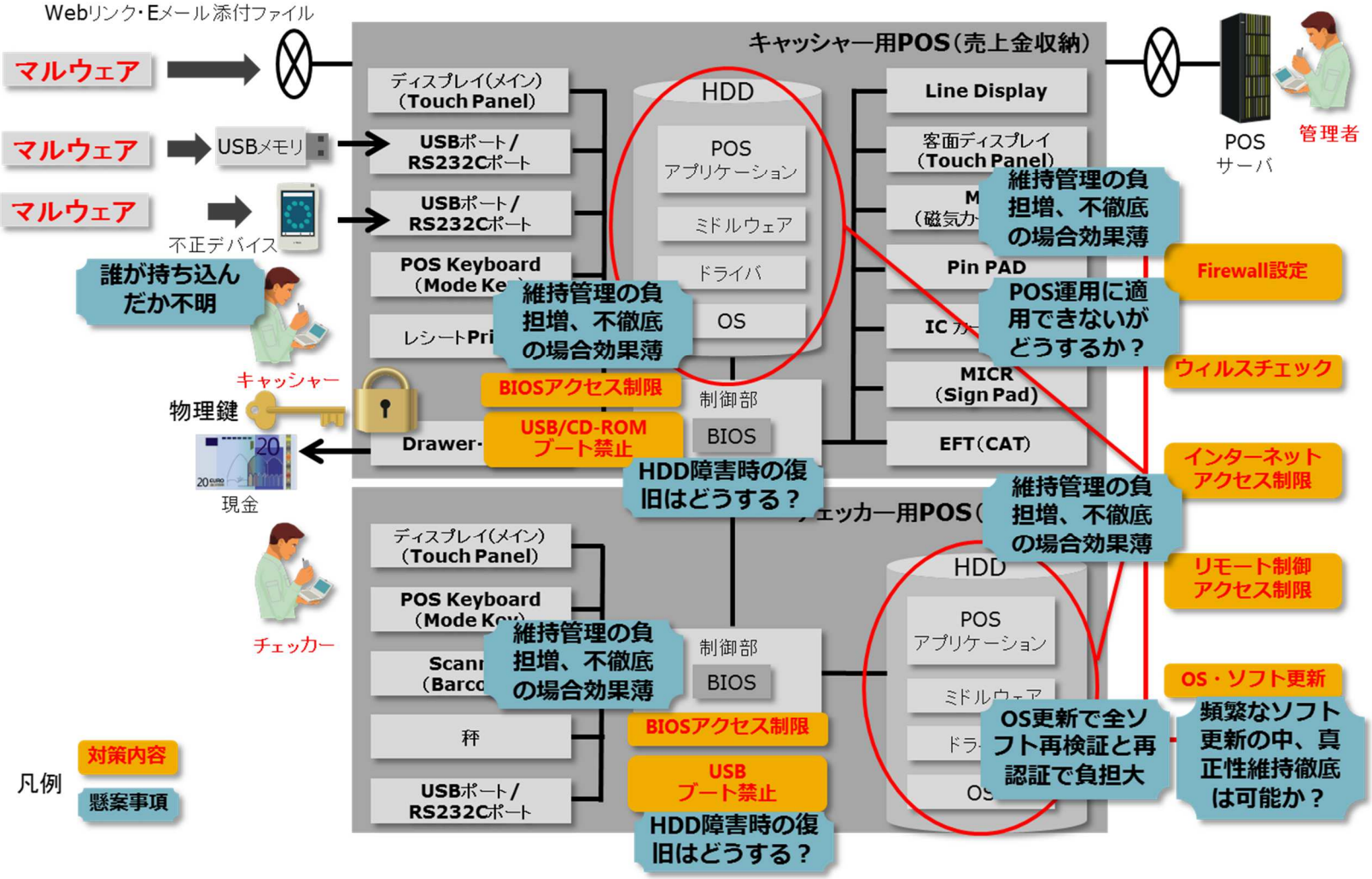
HDDデータの保護が目的



6.既存セキュリティ対策の問題点–その３–

■既存のセキュリティ対策の懸案事項

内部からの攻撃への対策が重要



7.セキュリティ対策を考えるための前提

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）。
前提２	POS運用に関わる運用者、保守員のモラルとスキルは低い。
前提３	インタフェース仕様は公開されている。
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。
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。

8.セキュリティ対策の方針

セキュリティの対策方針	
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。
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。
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。
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。
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。
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。
方針７	対策コストをできるだけ安くする。
方針８	トレーサビリティを強化する。

8.セキュリティ対策の方針 –その１–

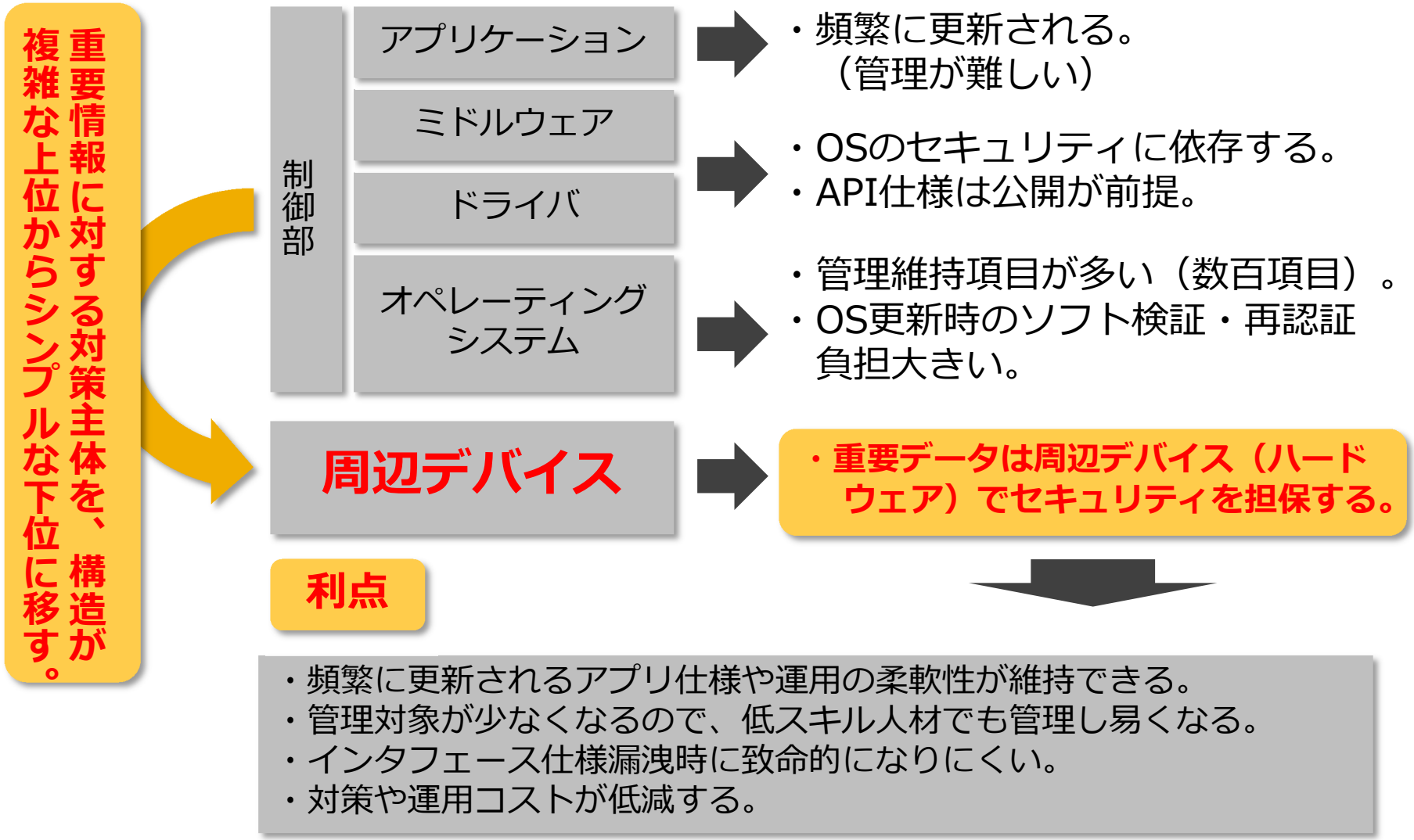
(方針1) 保護すべき情報や資産の優先順位を付け、致命的になる情報や資産を選別する 。

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）

8.セキュリティ対策の方針 –その２–

(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。



8.セキュリティ対策の方針 –その３–

(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。

デバイスの仕様やミドルウェア等の仕様公開されても暗号通信により情報の隠蔽や正当性は保護される。

(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。

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安全性を確保する。

(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。

複数の階層を持つシステム設計では、なるべく下位階層でセキュリティ対策を行い、柔軟性を確保する。

8.セキュリティ対策の方針 –その４–

(方針7) 対策コストをできるだけ安くする。

全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。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。

(方針8) トレーサビリティを強化する。

（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

例）メールの設定状態を確認する、等

（２）重要デバイス内資産のトレーサビリティ

例）クレジット取引や入出金処理ログの保持

（３）保守用重要デバイスのトレーサビリティ

例）各デバイスの付け外しを記録、通知する、等

（４）保守作業のトレーサビリティ

例）暗号通信の暗号鍵設定作業あるいは、定期的な鍵変更

9.製品ライフサイクルのフェーズ

■製品ライフサイクルにおける５つのフェーズ

フェーズ	説明
着手フェーズ	システムへの要求を明確化し、目的を文書化する。
開発フェーズ	システムを設計、開発する。
展開フェーズ	受け入れテスト後、システムを展開する。
保守・運用フェーズ	システムを稼働する。
廃止フェーズ	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。

10.各フェーズの取組み

フェーズ	取組み
着手フェーズ	セキュリティ計画の作成
	製品種別の分類
	事業に対する影響の評価
	個人情報に対する影響の評価
	セキュアな製品開発プロセスの実施
開発フェーズ	リスク評価
	セキュリティ対策の選択
	セキュリティドキュメントの作成
	セキュリティ構想設計
	セキュリティの設計および対策の開発
	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
展開フェーズ	セキュリティ承認、運用認可の計画を立てる
	確率した環境またはシステムへのセキュリティの統合
	製品セキュリティ評価
	情報システムの認可
運用・保守フェーズ	システム本環境移行の準備状況確認
	構成管理の実施
	継続的な監視の実施
廃止フェーズ	廃止／移行計画の作成
	情報の保存
	メディアのデータ消去
	ハードウェア/ソフトウェアの処分
	システムのクローズ

11.「つながる世界の開発指針」との関係 -1

「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む	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

11.「つながる世界の開発指針」との関係 -2

「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
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

12.「IoTセキュリティガイドライン」との関係 -1

「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

12.「IoTセキュリティガイドライン」との関係 -2

「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
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入・利用を控える		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			

13.セキュリティ要件　セルフチェックリスト－1

項番	チェック項目	対策例	方針管理	分析	設計	構築	保守運用	ユーザ教育	備考
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。				●	●		

13.セキュリティ要件　セルフチェックリスト –2

項番	チェック項目	対策例	方針管理	分析	設計	構築	保守運用	ユーザ教育	備考
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。				●	●		

13.セキュリティ要件　セルフチェックリスト –3

項番	チェック項目	対策例	方針管理	分析	設計	構築	保守運用	ユーザ教育	備考
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。			●		●	●	

13.セキュリティ要件　セルフチェックリスト –4

項番	チェック項目	対策例	方針管理	分析	設計	構築	保守運用	ユーザ教育	備考
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。					●	●	

13.セキュリティ要件　セルフチェックリスト –5

項番	チェック項目	対策例	方針管理	分析	設計	構築	保守運用	ユーザ教育	備考
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。					●	●	