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28年6月20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
			参考文献

1.背景と課題

１．POSの運用業務

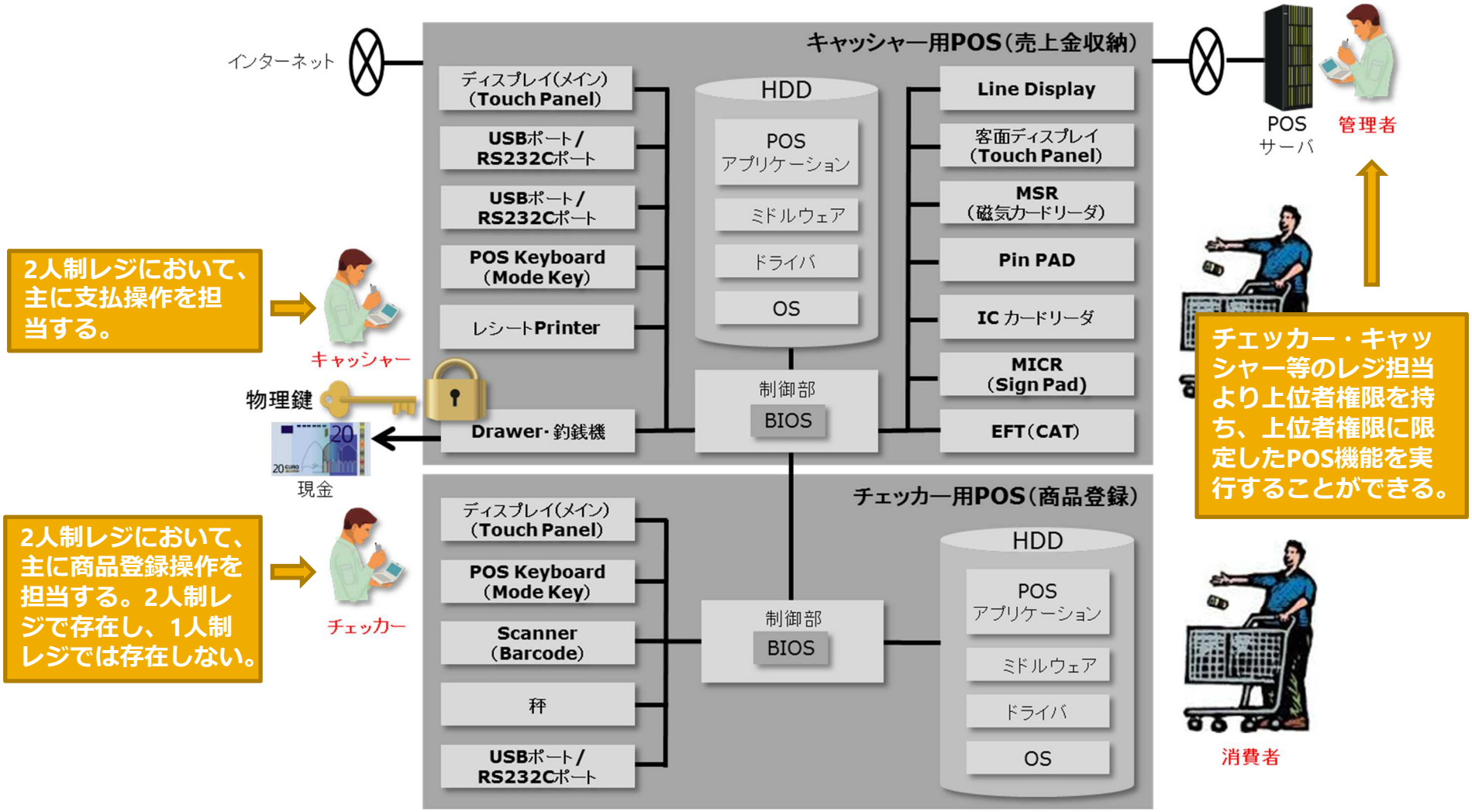
POSは店舗において、買い物客の売上を登録する機能と売上金を収納する機能を併せ持つ。売上登録を行う操作員をチェッカー、売上金収納を行う操作員をキャッシャーという。この両者は1人で行われることが多いが、大手量販店（特に食料品売場）の繁忙時間帯には2人に分かれて行われる。百貨店では集中レジシステムをバックヤードにおいて、売上と収納を分離する運用が行われている。

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システム構成と関係者–その1–



2.POSシステム構成と関係者–その2–

■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。
5	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。
6	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。
7	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。
8	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システム構成と関係者–その3–

項番	構成要素	機能
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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システム構成と関係者–その4–

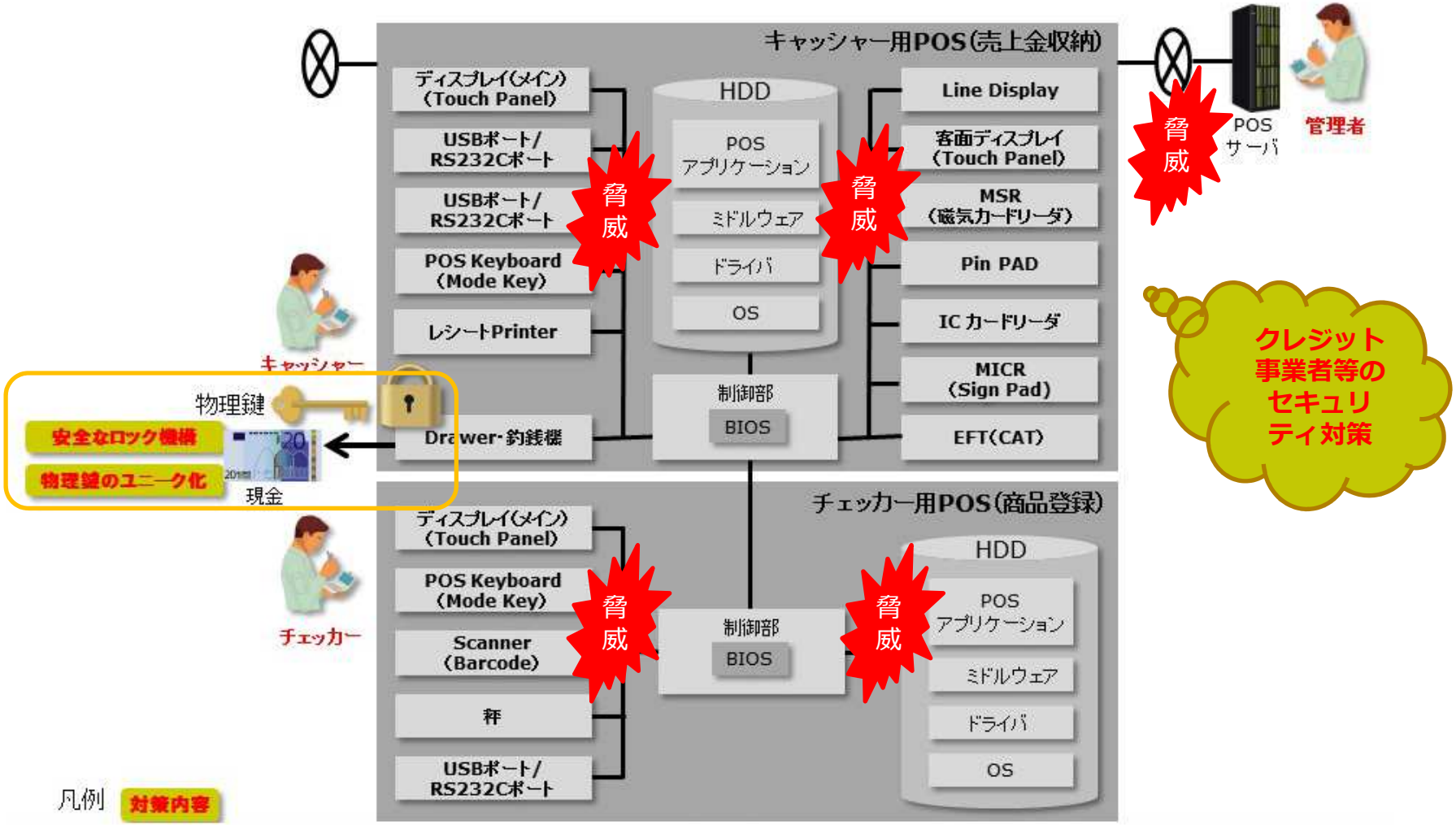
項番	構成要素	機能
18	釣銭機	釣銭機とは、POSからの制御で指定した金額を放出する機器のことであり、会計時に支払金額を入れたり、お釣りを出したりする。
19	Line Display	お店の設置環境に合わせて高さ調節可能な伸縮ポール型のカスタマーディスプレイ。四方向の設置が可能。

■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



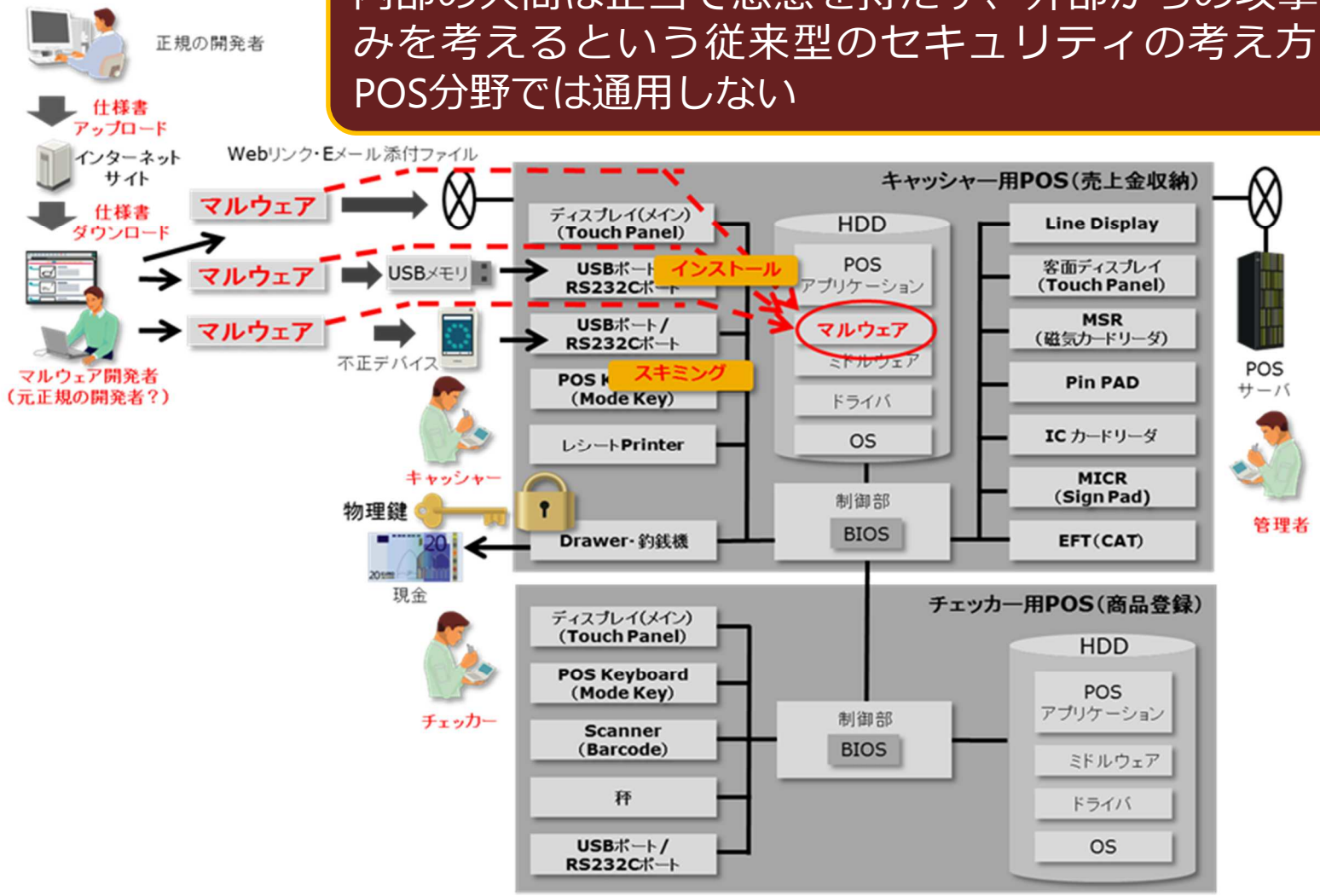
4.脅威を考慮すべき観点

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。

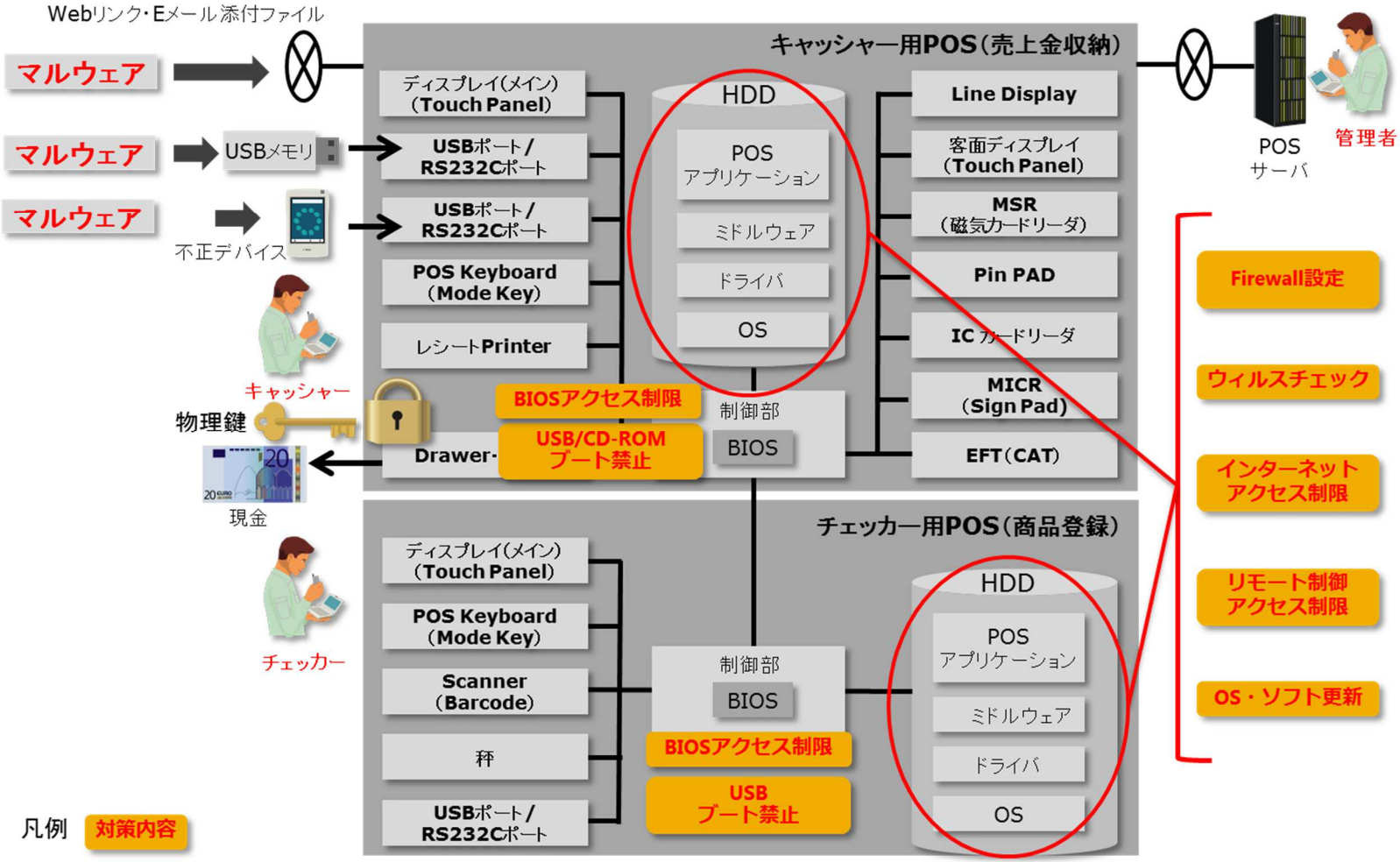
■提案されたセキュリティ対策が運用に適用できない場合がある。

■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

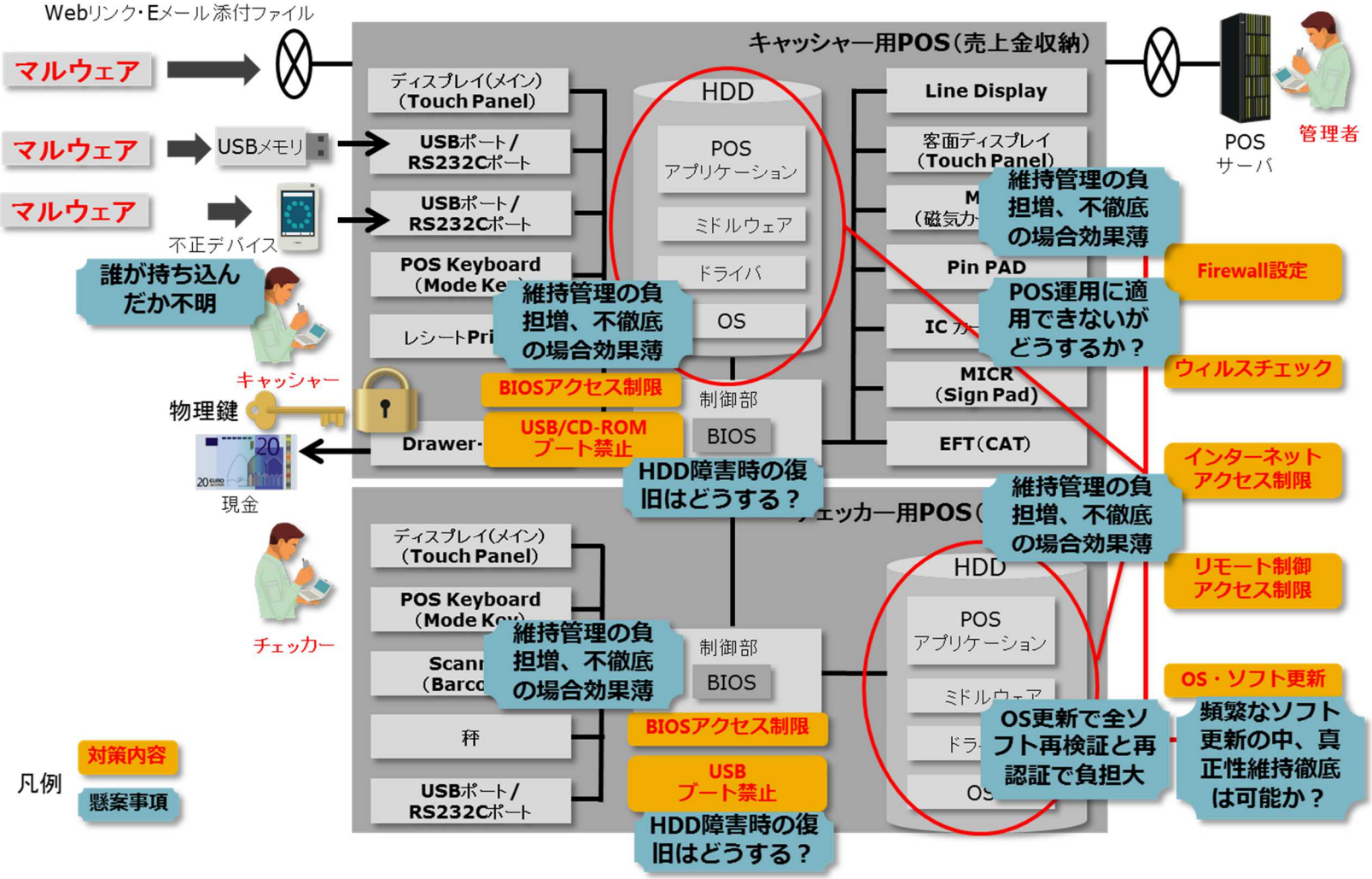
HDDデータの保護が目的



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.セキュリティ対策方針 –その１–

セキュリティ対策方針	
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。

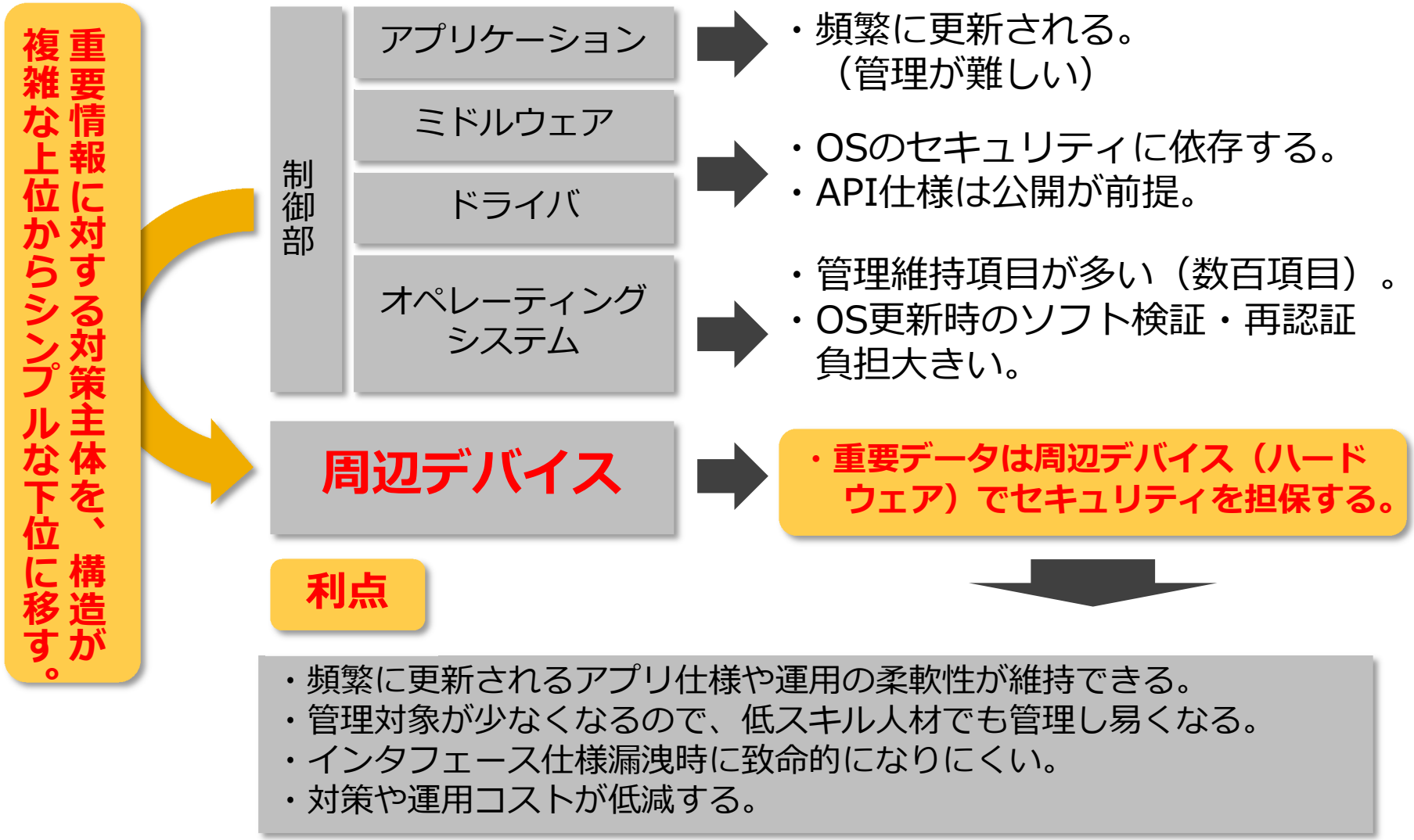
8.セキュリティ対策方針 –その２–

(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

8.セキュリティ対策方針 –その３–

(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.セキュリティ対策方針 –その４–

(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.セキュリティ対策方針 –その５–

(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）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

（２）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

（３）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–その1–

各フェーズにおけるセキュリティの取組み内容と該当するPOSガイドラインの方針を以下に示す。

■着手フェーズ

	項目	内容
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。

10.各フェーズの取組み–その2–

■開発フェーズ

	項目	内容
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。
4	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。
5	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。

10.各フェーズの取組み–その3–

■展開フェーズ

	項目	内容
1	確率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。
2	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。
3	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。

■運用・保守フェーズ

	項目	内容
1	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。
2	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。

10.各フェーズの取組み–その4–

■廃止フェーズ

	項目	内容
1	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。
2	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。

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」			POSガイドラインでの対応箇所	
大項目		指針	方針	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」			POSガイドラインでの対応箇所	
大項目		指針	方針	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.各フェーズでのセキュリティ取組み

フェーズ	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	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	リスク評価	●							●
	セキュリティ対策の選択		●	●	●	●			
	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	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	構成管理の実施					●			●
	継続的な監視の実施					●		●	●
廃止	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		●					●	●