製品分野別セキュリティガイドライン
金融端末（ATM）編

平成28年7月8日

CCDS セキュリティガイドラインWG
ATM SWG

1. 現状と課題

(1) ATMセキュリティの現状

従来型犯罪（フィジカル犯罪）に加え、IT技術を取り入れた新しい形態の犯罪（サイバー・フィジカル犯罪）が増加し、日々巧妙・多様化してきている。

欧州や新興国の事例ではATMを直接の感染対象とするマルウェアを媒体からインストールし、筐体を破壊することなく現金やカード情報などの重要情報を盗むインシデントが報告されている。

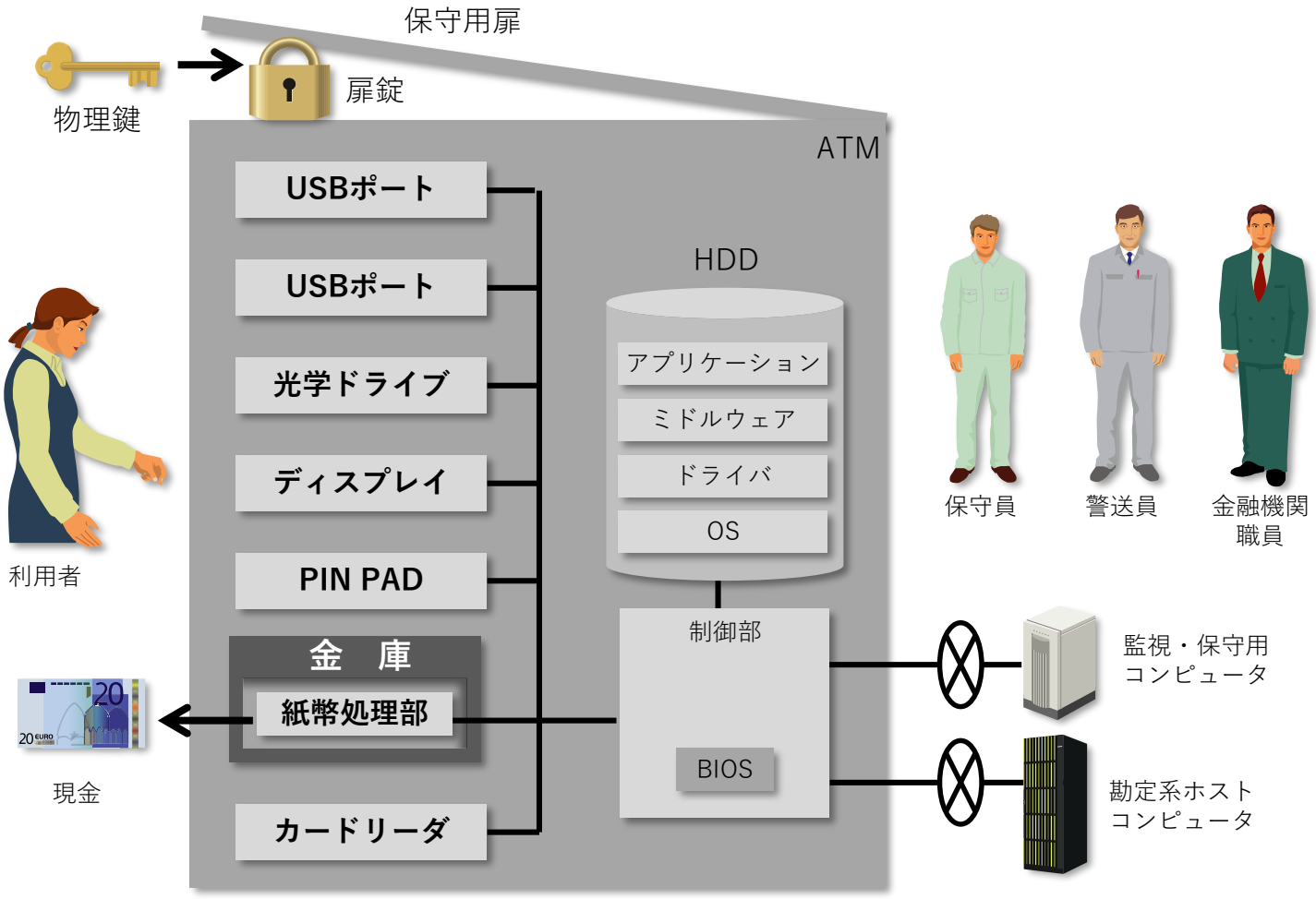
(2) ATMにおけるセキュリティ対策の必要性

上記はATM運用現場の管理不備を突いてマルウェアを仕込まれたこと、PC技術をベースとしているATMに対しマルウェアを開発しやすい「サイバー犯罪技術の過拡散時代」になってしまっていることが背景にある。

従来の規格基準が策定された時代には想定しづらかった事象をフィードバック・補強した、新しい「設計のガイドライン」を効果的に現場へ浸透させる必要がある。

2-1. ATMシステム構成と登場人物 –その1–

■ATMシステムの構成例と登場人物

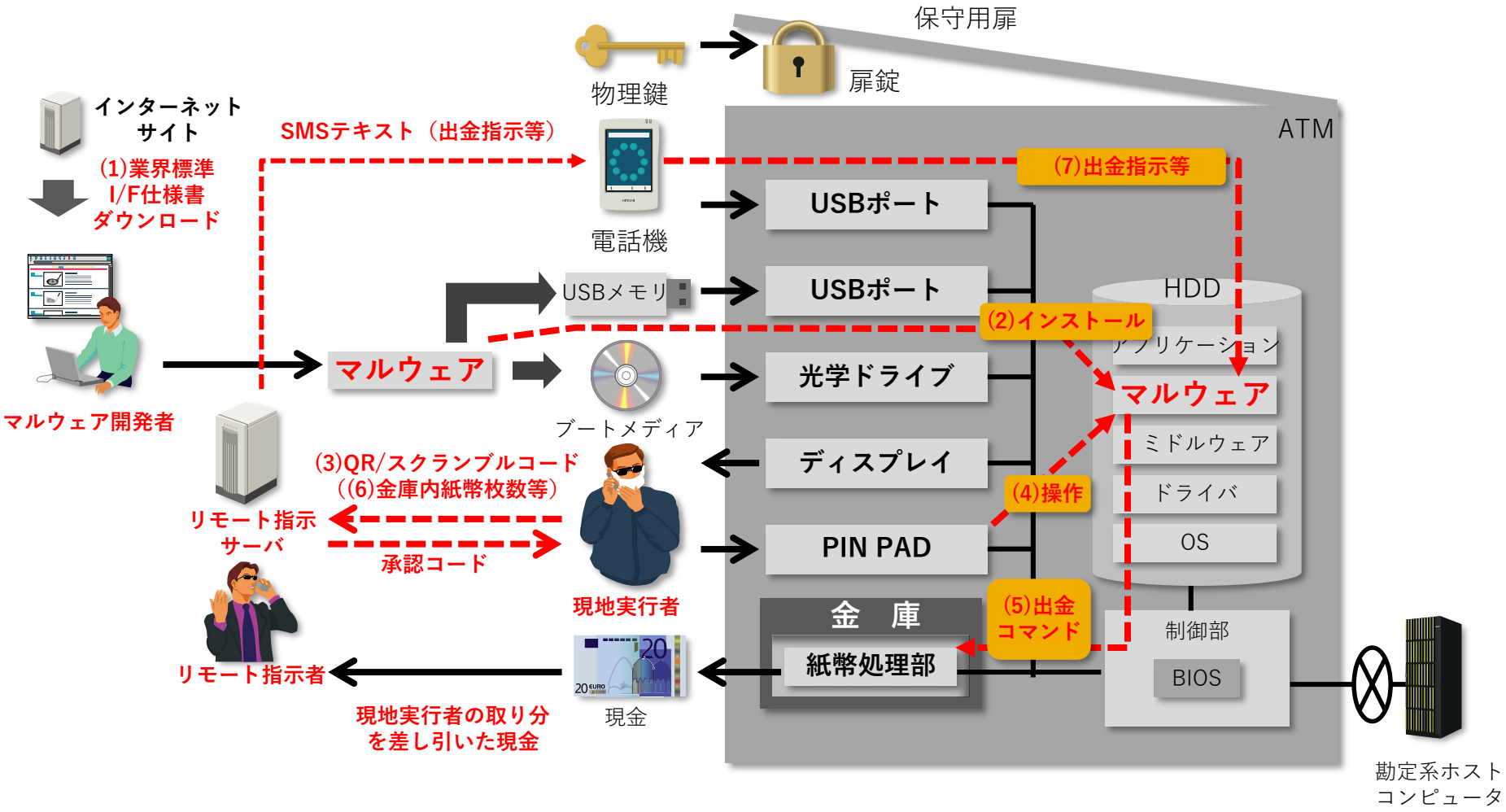


2-2. ATMシステム構成と登場人物 –その2–

項番	構成要素	機　　能
1	制御部	紙幣処理部等のデバイスを制御するコンピュータであり、Operating System(OS)にはWindows®を採用することが多い。
2	HDD（ハードディスクドライブ）	制御部に接続されておりOS、ドライバ、ミドルウェア、アプリケーション、保守用ソフトウェアなどのソフト全般を搭載している。
3	BIOS	Basic Input Output Systemの略であり、起動デバイスなどを制御する機能をもつ。
4	USBポート	USBメモリなどからソフトをインストールしたり、ログデータを採取したり、保守用キーボードを接続したりする場合に利用する。
5	光学ドライブ	ソフト全般をインストールするために用いられる。取引履歴やログデータを書込むことにも利用される。
6	ディスプレイ	取引方法を指示したり処理結果を表示したりするための表示機能をもつ。タッチパネルによって操作を行うものもある。
7	PIN PAD（ピンパッド）	暗証番号、取引金額などを入力するために用いられる。日本場ではタッチパネルによる入力手段で代替するものが多い。
8	紙幣処理部	紙幣を出金したり、投入紙幣の真偽識別や計数機能をもつ。紙幣を札毎に保管する複数の現金カセットで構成される。
9	金　庫	紙幣処理部を格納する。金庫鍵をもつ場合がある。
10	カードリーダ	ATMに挿入された銀行カードやクレジットカードを読取る装置である。取り扱うカードには磁気カードとICカードがある。
11	保守用扉	ATM内部の保守や紙幣の補充を行うために開閉する扉である。
12	扉　錠	ATMの保守用扉を開くための物理錠である。
13	勘定系ホストコンピュータ	ATMの勘定系取引を処理するコンピュータであり、基本的にインターネットには接続されない。
14	監視・保守用コンピュータ	ATMが動作中か休止中かを監視するコンピュータである。ATMにソフトウェア等をダウンロードする場合もある。
15	金融機関職員	ATMの保守用扉を開ける扉錠や金庫鍵を管理し、保守や紙幣の補充／回収時にATMの保守用扉を開ける役割をもつ。
16	警送員	金融機関の指示で現金の補充・回収を行う外部職員。
17	保守員	装置内部の保守作業を行う外部職員。
18	利用者	紙幣の引き出しや入金、送金などのATM取引サービスを受ける人である。

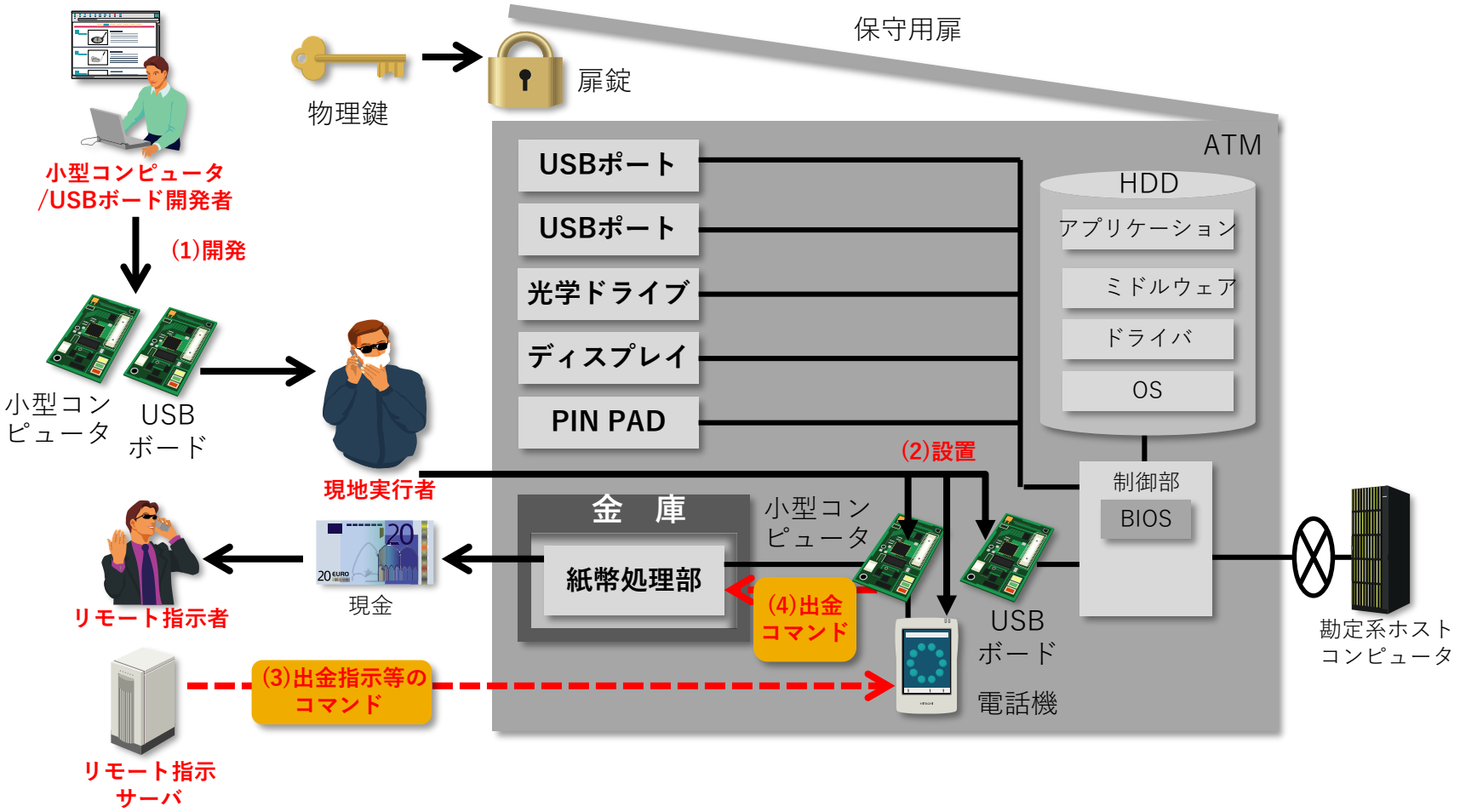
3-1. 脅威事例 –その1–

■マルウェアを用いた不正出金の構図（海外事例）



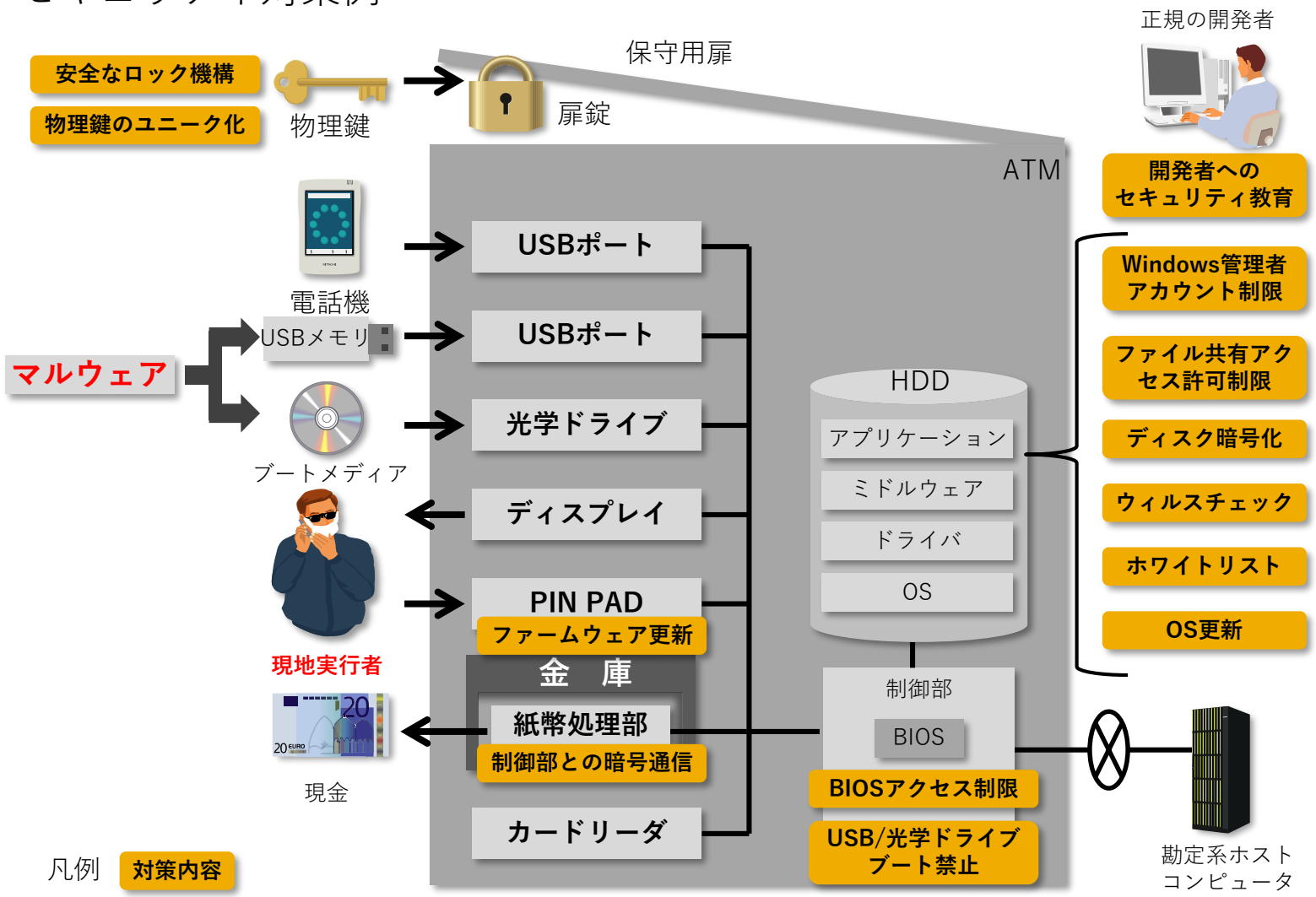
3-2. 脅威事例 –その2–

■マルウェアを用いた不正出金の構図（海外事例）



3-3. セキュリティ対策の各種指導例

■脅威事例の再発防止のための各種指導や、インターネット上で公開されているセキュリティ対策例



3-4. インシデントからのフィードバック事項

■最近の犯罪事例からの考慮すべき観点

項番	分　類	フィードバックすべき事項
1	IT技術の一般化と今後の進歩による被害の拡散	IT技術の普及が犯行手段の開発を容易化し、それは常に進歩して手口が巧妙化していく。また現在のところマルウェア感染は物理的な媒体挿入が契機であるが、今後のIoTの進展によっては、つながった先の世界から感染するかもしれない。
2	侵入ルート	あらゆるルートでのマルウェア侵入、情報漏えいが起こりうることを前提に考え直す必要がある。USBメモリ／CD-ROM等のプログラム媒体の挿入が可能で悪意をもつ登場人物が存在する。
3	管理の不備	マルウェアは以下の条件でインストールされやすい。 ・ハードウェア：ATMの扉鍵がどれも同じである、ATM運用現場での鍵の管理が杜撰であるなど。 ・ソフトウェア：システムの特権ユーザ名、パスワードがどのATMでも同じであり、マルウェアの入ったファイル装置からのリブートが可能であり、USBポートが自動接続可能状態である、マルウェアを検知するソフトウェアが搭載されていないなど。
4	情報漏えいと非正規保守部材の流通	マルウェアやブラックボックスは不適切に公開された情報や非正規に流通している保守部品などを分析して開発されており、犯罪に必要な情報は漏えいしている前提で考える必要がある。

■既存のセキュリティ対策懸念事項

項番	懸念事項	具体的内容
1	セキュリティ強化のコストは相対的に高くなる	（1）対策導入後の運用コスト （2）人材の教育・訓練コスト （3）運用ルールのバリエーションが産むコスト高 （4）改修のためのATM運用休止に伴う機会損失 （5）進化し続ける手口への都度対応によるコスト高 （6）OSの都度更新に伴う各種検証作業はコスト・処理性能面で極めて困難
2	人的資質に依存した対策は破綻する	（1）現場作業を詳細に管理することは難しい。 （2）退社した開発者がその知識を悪用しないよう担保できない。 （3）内部犯行者の影

4-1.「つながる世界の開発指針」と本セキュリティ対策指針の対応関係

「つながる世界の開発指針」			本書での対応箇所
大項目		指　針	
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
		指針２ 安全安心のための体制・人材を見直す	ATM-指針２
		指針３ 内部不正やミスに備える	ATM-指針３
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	ATM-指針４
		指針５ つながることによるリスクを想定する	ATM-指針５
		指針６ つながりで波及するリスクを想定する	n/a
		指針７ 物理的なリスクを認識する	ATM-指針７
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	ATM-指針８
		指針９ つながる相手に迷惑をかけない設計をする	n/a
		指針１０ 安全安心を実現する設計の整合性をとる	n/a
		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	ATM-指針１１
		指針１２ 安全安心を実現する設計の検証・評価を行う	ATM-指針１２
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	ATM-指針１３
		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	ATM-指針１４
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	ATM-指針１５
		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	ATM-指針１６
		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

※ n/a：ATM分野においては体制や仕組みが既知と認識されているので説明を割愛

4-2. セキュリティ対策方針 –その1–

IPA発行「つながる世界の開発指針」との関連付け（ATMで検討を要するもの）	
ATM-指針2	**安全安心のための体制・人材を見直す** ①つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。 海外犯罪事例はいずれ日本でも起こりうることを想定しておくことが重要である。そのためには犯罪事例と既存対策の情報をタイムリーに社内で共有し、製品セキュリティに活かすための体制整備が求められる。 ②そのための人材（開発担当者や保守担当者など）を確保・育成する。 常に新しい対策技術を開発し続ける必要があり、開発担当者含めて必要な人材の確保、育成が求められる。
ATM-指針3	**内部不正やミスに備える** ①つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。 監視・管理を強化するほど運用や保守の効率が落ちるが、内部不正や犯罪者が狙う資産は限られるので、セキュリティ対策に強弱を付けることで、効果的な抑止と業務効率の維持を両立させることも可能になる。 ②関係者のミスを防ぐとともに、ミスがあっても安全安心を守る対策を検討する。 管理項目が多くて複雑な作業手順を強いられるほどミスが生じやすい。管理項目数を減らしたり、作業手順を簡単にしたり、あるいは正しい手順以外は操作できないシステムで自動化したりする努力が必要である。
ATM-指針4	**守るべきものを特定する** ATMでは犯罪や不正行為で狙われる資産はある程度限られる。そこで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して保護すれば、実効的なセキュリティ確保と、業務効率を両立させやすくなる。

4-3. セキュリティ対策方針 –その2–

IPA発行「つながる世界の開発指針」との関連付け（ATMで検討を要するもの）	
ATM-指針5	**つながることによるリスクを想定する** ①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、IoTコンポーネントとして使われる前提でリスクを想定する。 海外事例ではマルウェアを物理的な媒体経由でインストールしたり、外部接続可能な小型機器をATM内部に組み込んだりすることで、不正出金が行われている。また携帯電話等のオープンネットワーク機器との接続も一般的になってくると考えられるので、それを前提またはそれに準じたATMの制御部に対する保護策が必要である。 ②保守時のリスク、保守用ツールの悪用によるリスクも想定する。 ■保守担当者による不正行為（不正なソフトウェアのインストールなど） ATM内部アクセス時に、制御部に不正ソフトウェアがインストールされるリスクに備えて、制御部にはそれらに対する対策が求められる。機器側の対策だけでは十分にカバーできない場合に備えて、多重防御の観点から資産や作業の監視を行ったり、監査したりすることで、抑止力を働かせることも有効である。以下に、考慮すべき観点について記述する。 (a) 重要デバイス内資産のトレーサビリティ (b) 保守用重要デバイスのトレーサビリティ (c) 保守作業のトレーサビリティ ■第三者による保守用I/Fの不正利用（非公開の保守モードの起動、ATMの物理鍵の入手など） ATM毎に個別の物理鍵を使う、ワンタイムパスワードを使う、または重要な保守機能を使う場合は、事前に認証手続きを行うなどがある。

4-4. セキュリティ対策方針 –その3–

IPA発行「つながる世界の開発指針」との関連付け（ATMで検討を要するもの）	
ATM-指針7	**物理的なリスクを認識する** ①盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。 ATMの運用・保守ではATM内部への物理的なアクセスが発生するので、ATM-指針5で示す保守時のリスクを考慮する必要がある。 ②中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。 廃棄機器、中古機器から不正改造された保守部品がATMに組み込まれて犯罪行為が行われるリスクを考慮する必要がある。対策に関しては、ATM-指針5で述べた内容が効果的である。
ATM-指針8	**個々でも全体でも守れる設計をする** ①外部インタフェース経由／内包／物理的接触によるリスクに対して個々のIoTコンポーネントで対策を検討する。 ■外部インタフェース経由のリスクへの対策 デファクトなインタフェースを外側から保護する対策が必要である。対策例として、ホワイトリスト対策ソフト等をインストールしたり、OSのハードニングを行ったりするといった制御部での対策が挙げられる。 ■守るべきものの重要度に応じたセキュリティ対策 保護すべき重要資産として、紙幣出金に結び付くコマンドやカード番号、暗証番号等が挙げられる。これら重要資産の保護には制御部での対策に加えて、制御部での対策が阻害されたときに備えて、周辺機器側での多重防御が有効である。

4-5. セキュリティ対策方針 –その4–

IPA発行「つながる世界の開発指針」との関連付け（ATMで検討を要するもの）	
ATM-指針8（続き）	②個々のIoTコンポーネントで対応しきれない場合は、それらを含む上位のIoTコンポーネントで対策を検討する。 ATM内個々の機器での対策だけで十分でない場合は、それぞれの機器で保持している情報を統括して利用することで、更なる対策を行うことが可能である。
ATM-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** ①IoTコンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。 ATM内部の構成要素間の通信を暗号化することがセキュリティ対策上有効である場合、その暗号設定には特権モードのような管理者権限が必要である。
ATM-指針12	**安全安心を実現する設計の検証・評価を行う** ①つながる機器やシステムは、IoTならではのリスクも考慮して安全安心の設計の検証・評価を行う。 セキュリティに関する攻撃は日々進化しており、従来の考え方では対処できない場合が存在することを想定し、既存の設計検証・評価の仕組みを常に見直して改善していく必要がある。
ATM-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** ①自身の状態や他機器との通信状況を把握して記録する機能を検討する。 ATM-指針８で述べたように、ログデータを統括して利用することで、さらなるセキュリティ対策を講じることが可能となる。 ②記録を不正に消去・改ざんされないようにする機能を検討する。 ログに対してのアクセス権限の設定、暗号化が金融機関の了解の下で行われていたり、収集ログを定期的に、あるいは不定期にサーバ等に送信する方法がある。

4-6. セキュリティ対策方針 –その5–

IPA発行「つながる世界の開発指針」との関連付け（ATMで検討を要するもの）	
ATM-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** ①経年で増大するリスクに対し、アップデートなどで安全安心を維持する機能を検討する。 暗号技術を一度導入すると、暗号鍵の更新といった暗号鍵管理に伴う新たな保守が必要になるので、それを安全に実施する機能や仕掛けが求められる。
ATM-指針１５	**出荷後もIoTリスクを把握し、情報発信する** ①欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。 ②必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。 公的機関や業界団体、セキュリティ会社等から、欠陥や脆弱性、事故やインシデントの最新情報が開示されている。それを収集し社内や関係事業者と共有して、適切な製品設計に活かす必要がある。また、顧客に対しても、適当なタイミングでそれらの情報を提供していくことが求められ、さらにその解決策についても提案できることが望ましい。
ATM-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** ①導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務に関わっている担当者や外部の事業者に伝える。 導入、運用、保守、廃棄で守るべき事項を業務に関わっている担当者や事業者に伝える仕組みはある。しかし、管理不備が放置されている海外の事例を考慮すると、その仕組みのさらなる改善・工夫が必要であり、継続的な努力が求められる。

5-1. 製品ライフサイクルのフェーズ

■NIST SP800-64「Security Considerations in the System Development Life Cycle」（SDLC）で定義された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。

5-2. 各フェーズにおけるセキュリティ指針の取組み

フェーズ	項番	システム開発ライフサイクル	ATM-指針										
			2	3	4	5	6	7	8	11	12	13	14	16
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	セキュリティ構想設計							●			●	●	
	4	セキュリティの設計および対策の開発							●			●	●	
	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									●			
展開	1	確立した環境またはシステムへのセキュリティの配合												●
	2	製品セキュリティ評価												
	3	情報システムの認可												
保守運用	1	構成管理の実施				●		●						
	2	継続的な監視の実施				●		●						
廃止	1	メディアのデータ消去												●
	2	ハードウェア／ソフトウェアの処分												●

※ ●が全くない行はATM分野で体制や仕組みが既知と認識されているので説明を割愛