製品分野別セキュリティガイドライン
金融端末（ATM）編

Ver. 1.0

CCDS セキュリティガイドライン WG
ATM SWG

改訂履歴

版数	改訂日	改訂内容
Ver.1.0	2016/06/08	新規作成

■商標について

・本書に記載の会社名、製品名などは、各社の商標または登録商標です。

■おことわり

・本書に記載されている内容は発行時点のものであり、予告なく変更することがあります。

・本書の内容を CCDS の許可なく複製・転載することを禁止します。

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　ATMセキュリティの現状と課題

海外の ATM 業界では近年、スキミングや ATM 筐体の物理的な破壊による現金強盗といった従来型犯罪（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。

一方、日本における ATM を含む金融機関の勘定系システムは、公益財団法人 金融情報システムセンター（FISC）のルール[10][11]に従って、そのセキュリティ基準が規定されている。上述した新たな海外の犯罪事例を踏まえて、FISC のルールを基にどのように対策を検討すればよいかの指針が求められる。サイバー・フィジカル犯罪時代における ATM セキュリティ対策の考え方については、従来にない新しい着眼点が必要であり、本ガイドラインは一つの考え方を示すものである。

サイバー･フィジカル犯罪が起きた国々でも､FISC 等と同様な基準規格を踏まえて ATM を含むシステムが構成され、セキュリティを意識した運用がなされていたはずである。しかし、実際の ATM 運用現場においては、それだけではインシデントが回避できなかったということになる。

その理由と背景は後述するが､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と考えられる。

また現代は「つながる世界で安全安心な IoT の実現」を求められる局面でもあり、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「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と考えられる。

もちろん一方では、過去からの ATM 運用規則や運用実態との親和性を維持することも不可欠であり、過去と将来の両視点を備えることができるよう、本ガイドラインを編集している。

1.2　本ガイドラインの対象範囲

1.2.1 基本的なカバー範囲

世界には既にATMシステム全体をカバーする幾つかのセキュリティガイドラインや規格が存在する(*1)。本ガイドラインは既存のセキュリティガイドラインや規格を否定するものではなく「多重防御の考えに基づいた補完手段や代替手段」を提供し、より良い対策手段を提供するものである。

また本ガイドラインの対象範囲は「ATM 端末とその内部に存在する構成要素」に限定し、ホストコンピュータ等を含めた上位システムは対象外としている。上位システム側は長い歴史の中で一定レベルのセキュリティ機能を形成し、その技術は一般的な PC レベルと比較して格段に難しく、また情報が制限されているので、犯罪者集団の目標とは成り難いと推察するからである。

具体的には ATM にマルウェアをインストールしたり、ATM 内部に不正な機器を据え付けたりすることで不正出金や重要情報詐取を行う「サイバー・フィジカル犯罪」に対するガイドラインを提供する。

1.2.2 例外的なカバー範囲

本書は ATM の上位システム側を対象としないが、ATM 側の対策と上位システム側の対策が同時に必要な場合には、これを例外的に記載している(*2)。上記のような推奨案はATM ベンダが選択肢として顧客に提案し、顧客自身のセキュリティポリシに応じて適切に選ばれることを想定している。

1.3　本書の対象者

本書は ATM において適切なセキュリティ対策と運用を実施するために、設計開始から製品リリース終了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。そのため、以下の方々を読者として想定している。

1）ATM ベンダにおいて装置設計を行う開発者、開発プロジェクトを管理する責任者
2）ATM ベンダから装置を購入してシステムインテグレーションを行う事業者
3）ATM を含めた全体システムの企画、開発、運用を担当する金融機関およびサービスプロバイダの組織員

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
ATM	Automated Teller Machine
BIOS	Basic Input/Output System
CCDS	Connected Consumer Device Security Council
CEN	Comité Européen de Normalisation （European Committee for Standardization）
EMV	Europay MasterCard Visa
HDD	Hard Disk Drive
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Payment Card Industry
PIN PAD	Personal Identification Number Pad
QR	Quick Response
SDLC	Systems Development Life Cycle
SMS	Short Message Service
SWG	Sub Working Group
UL	Underwriters Laboratories
USB	Universal Serial Bus
WG	Working Group
XFS	eXtensions for Financial Services

2 ATM システムの運用モデルとシステム構成例

2.1 登場人物とシステム構成例

ATM の運用では図 2-1 に示すように、金融機関職員、または金融機関から委託された警備会社の警送員による紙幣の補充・回収や、保守会社の保守員による保守作業があり、これらの運用において ATM 内部へのアクセスが発生する。なお、運用形態によっては役割が変化する場合も存在する。

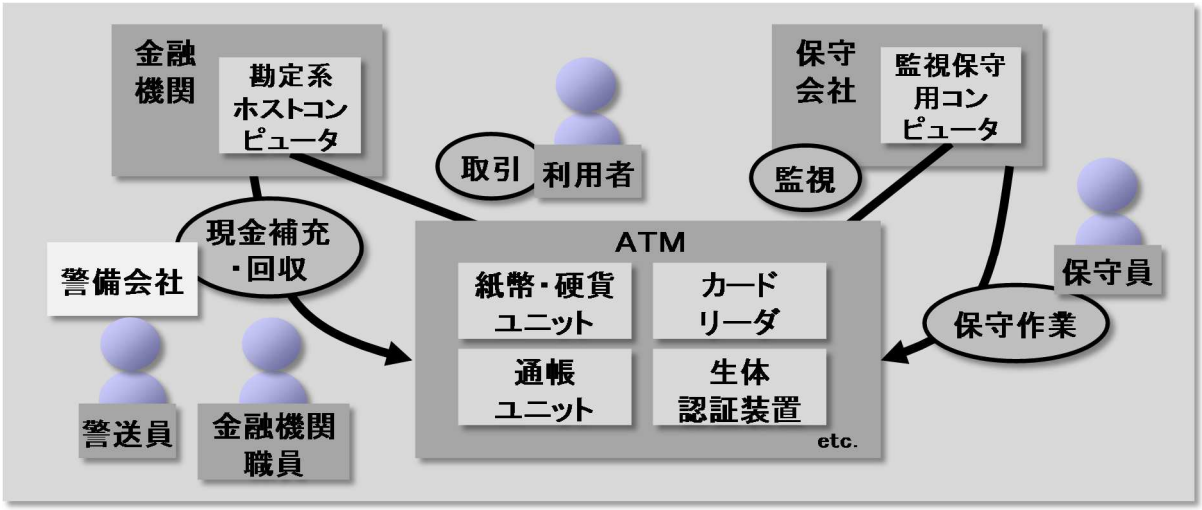

図 2-1 ATM 運用と登場人物

登場人物の詳細説明を表 2-1 に示す。

表 2-1 登場人物の詳細

項番	登場人物	役　割
1	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、ATM の保守や紙幣の補充／回収時に ATM の保守用扉を開ける役割をもつ。 ・金庫内に設置された紙幣処理部の保守を保守作業者で行う場合には、金庫鍵で開錠して現金カセットを取り出して一時的に別の場所でこれを管理するなど、保守作業の補助を行う場合もある。

2	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。 ・紙幣の補充／回収には、紙幣処理部から独立した現金カセットに紙幣を詰めて運搬する場合や、紙幣を袋等に詰めて運搬し、ATM 設置場所で現金カセットに装填したり、回収したりする場合もある。 ・店舗外に設置された ATM に紙幣の補充／回収を行う場合は、金融機関職員の管理する物理鍵類を携行することがある。
3	保守員	装置内部の保守作業を行う外部職員。 ・金融機関職員または警送員に ATM の保守用扉や金庫扉を開けてもらい、保守作業を行う。障害復旧の他、ATM 設置現場での修理を行う。

ATM システムの構成例を図 2-2 に示す。ATM には PC と同等な制御部が存在し、制御部は USB インタフェース等を通じて周辺機器と接続している。制御部にはその設定等を行う BIOS が存在し、制御部に接続されるハードディスクドライブ（HDD）には OS、ドライバ、ミドルウェア、アプリケーション等がインストールされている。また図には示さないが ATM 取引履歴のジャーナルやソフトの動作ログファイルも HDD 上に存在する。

周辺機器には利用者に操作内容を表示するディスプレイや、取引金額や暗証番号等を入力するための PIN PAD、タッチパネル装置、取引に使う紙幣の排出や収納を行う紙幣処理部、カード媒体を読書きするカードリーダ、ソフトウェアなどのインストール媒体を読取る光学ドライブなどがある。また図には示さないが ATM 取引結果を明細票や通帳に印字するものも存在する。紙幣処理部には紙幣の補充・回収のための現金カセット等が存在し、紙幣処理部自身は頑丈な金庫内に設置されている。また制御部は勘定系ホストコンピュータや保守用コンピュータといった上位システム側とネットワークを介して接続されている。

ATM 全体はある基準を満たした筐体で保護されており、ATM 内部にアクセスするための保守用扉が存在し、保守用扉を開けるためには物理鍵が必要となる。

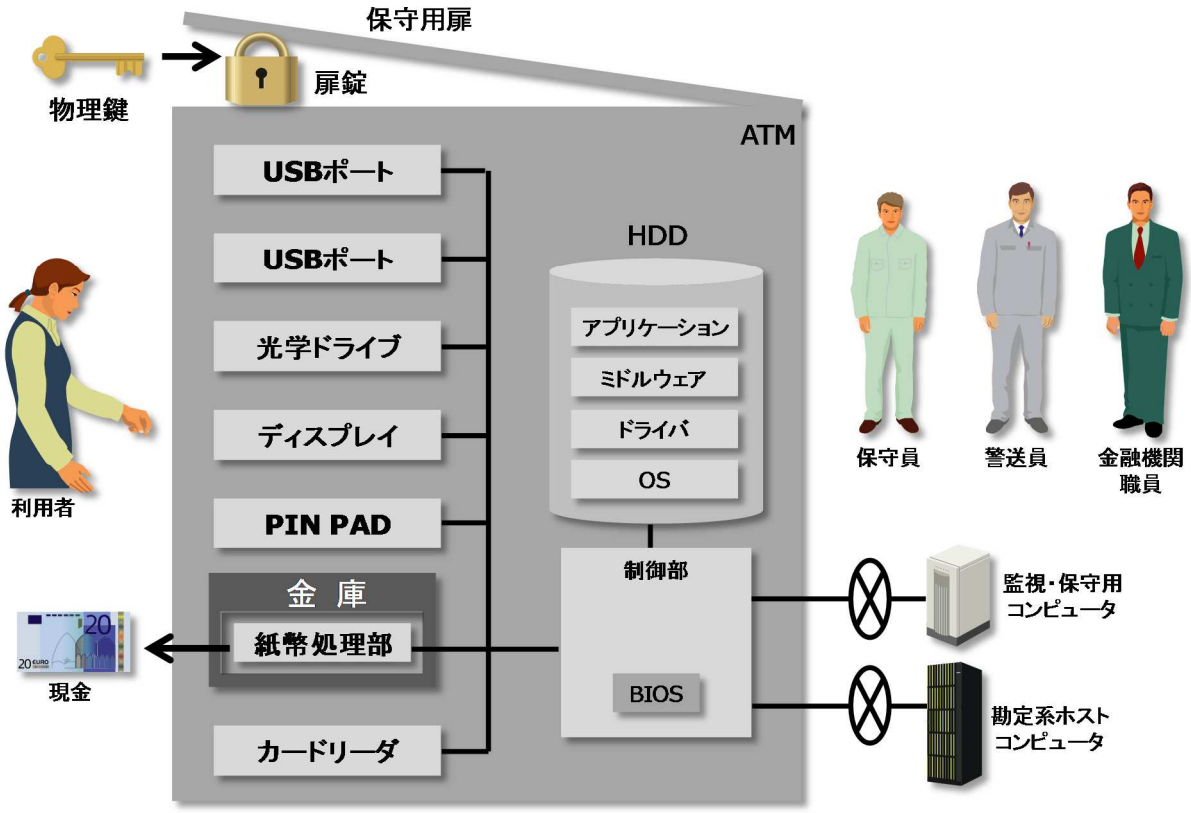

図 2-2 ATM のシステム構成例

ATM システムの主要構成要素の説明を表 2-2 に示す。

表 2-2 ATM システムの主要構成要素

項番	構成要素	機 能
1	制御部	カードリーダや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® (*3)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。日本市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、投入紙幣を真偽識別して計数したりする機能をもつ。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 が動作中なのか休止中なの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。

2.2　ATMシステムの運用

2.2.1 取引時の運用

装置の電源が投入されると ATM は自動的に起動・初期化し、勘定系ホストコンピュータや保守・監視用コンピュータに接続して利用者が取引可能な状態に移行する。ATM では入金、出金、振替等の種々の取引があるが、例えば出金取引の場合は利用者がタッチパネルで取引メニューを選択した後、銀行カードをカードリーダから挿入してカード情報を読取らせる。本人確認のための暗証番号を PIN PAD やタッチパネルから入力し、出金金額を入力する。これらの取引情報は勘定系ホストコンピュータに送られて処理される。

勘定系ホストコンピュータ上では、暗証番号とカード情報と出金金額等から勘定系の処理が行われる。この処理の結果を ATM が受信して紙幣処理部に対し出金コマンドを発行し、ATM から紙幣が排出されて取引が終了する。

2.2.2 紙幣補充・回収時、保守時の運用

ATM の保守作業では、保守員または金融機関職員が保持する物理鍵を用いて保守扉を開けてから必要な作業を行う。現金カセットの補充／交換作業時には更に金庫扉を開ける必要があるので、金庫鍵は金融機関職員が同行して開錠したりする場合もあれば、警送員だけが現場に出向く場合には 2 名以上での作業ルールとして金庫扉開錠時の現金取扱いに相互牽制をかけることもある。また紙幣処理部の保守を実施する場合にも同様に金庫扉を開ける必要があるので、この場合も上記と同様のルールで運用されることが多い。

以上述べたように、人手を介する作業には金融機関個々の運用規程に基づいて厳正な運用管理を行うことが一般的である。

3 想定されるセキュリティ上の脅威

3.1 最近の犯罪事例と考慮すべき観点

ここでは海外における不正出金事例を取り上げる。一つは ATM にマルウェアをインストールして不正出金する事例であり、もう一つは ATM 内部の制御部と紙幣処理部を接続するケーブルの途中にブラックボックスと呼ばれる小型のコンピュータを設置して紙幣処理部に出金コマンドを送ることで不正出金を行う事例である。

[事例１：マルウェアによる不正出金事例]

図 3-1 に報道等の公開事例(*4)から想定したマルウェアによる ATM 不正出金事件の構図を示す。犯行は以下のようなステップで実施されたものと推定される。

（１）ハッカーがマルウェアを開発する。最近の ATM ソフトウェアはグローバルな業界標準仕様の API(*5)を使って開発されることが多く、この API に関する情報が管理不備によってインターネット上に漏えいし、マルウェア開発が助長された可能性がある（*6)。
（２）現地実行犯は管理に不備のある ATM 運用サイトで物理鍵を入手（又は複製）し、保守扉を開いて USB メモリ／CD-ROM でマルウェアをインストールする。
（３）マルウェアを立ち上げ、画面に表示される QR コードやスクランブルコードを携帯電話や SMS メールなどを用いて遠隔地の指示者（サーバ）に送信する。
（４）現地実行犯はその応答として承認コードを携帯電話で受信し、ATM の PIN PAD からマルウェアに入力し、ATM からの不正出金が可能となる。
（５）紙幣処理部に対して不正な出金コマンド操作を繰り返し、紙幣を入手する。
（６）現地実行犯が紙幣を着服しないよう、上記 QR コードやスクランブルコードの中には金庫内の紙幣有高情報が含まれ、犯行後に紙幣金額と突き合わされる。
（７）遠隔指示者（サーバ）とのやり取りは、ATM の USB ポートに接続された携帯電話の SMS メールを通じて行われることもある。

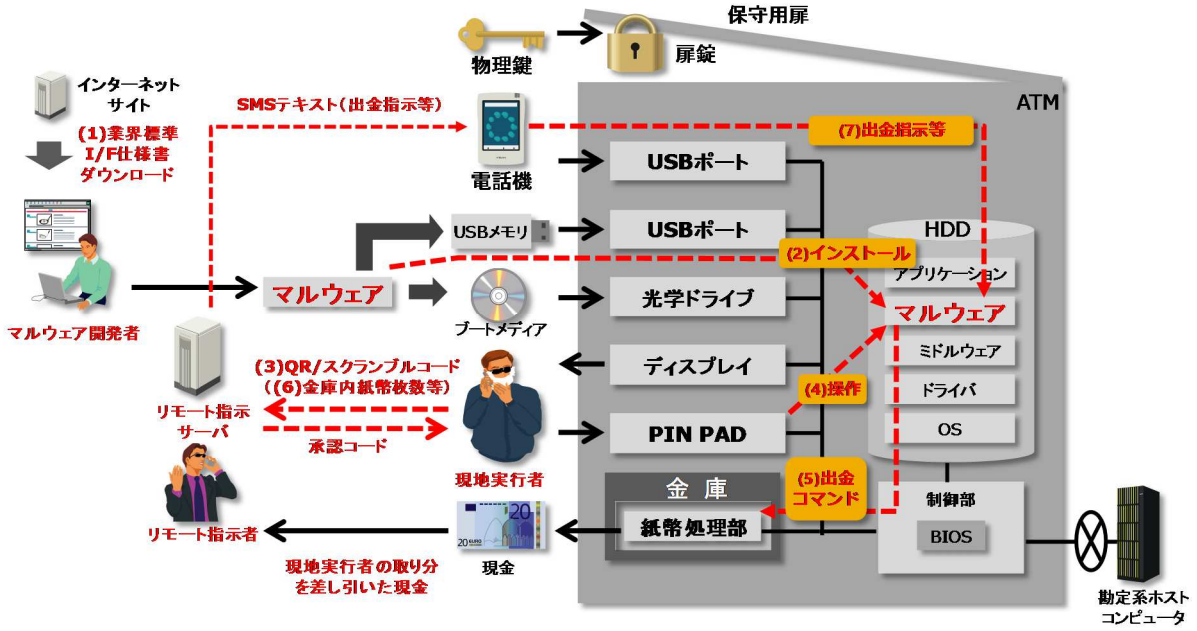

図 3-1 マルウェアを用いた不正出金の構図（海外事例）

[事例２：ブラックボックスの設置による不正出金事例]

図 3-2 は同様にブラックボックス（小型コンピュータ）を使った ATM 不正出金事件(*7)の構図である。犯行は以下のようなステップで実行されたものと推定される。

（１）インターネットのオークション等で非正規に流通している ATM 保守機材を入手するなどしてハードウェアの構造を解析し、犯罪用の小型コンピュータ（ブラックボックス）や制御部に異常を気づかせないための USB ボードが開発される。

（２）現地実行犯は管理に不備のあるＡＴＭ運用サイトで物理鍵を入手し、保守扉の扉錠を開いて USB ポートにこの小型コンピュータ、USB ボードと電話機をセットする。

（３）小型コンピュータは制御部と紙幣処理部との間の通信を乗っ取り、ATM の取引とは無関係に電話機を通じて出金コマンドを指示できるようになる。

（４）現地実行者はリモートサーバからの出金指示コマンドを待ち、ATM から出金されたら現金を受け取る。

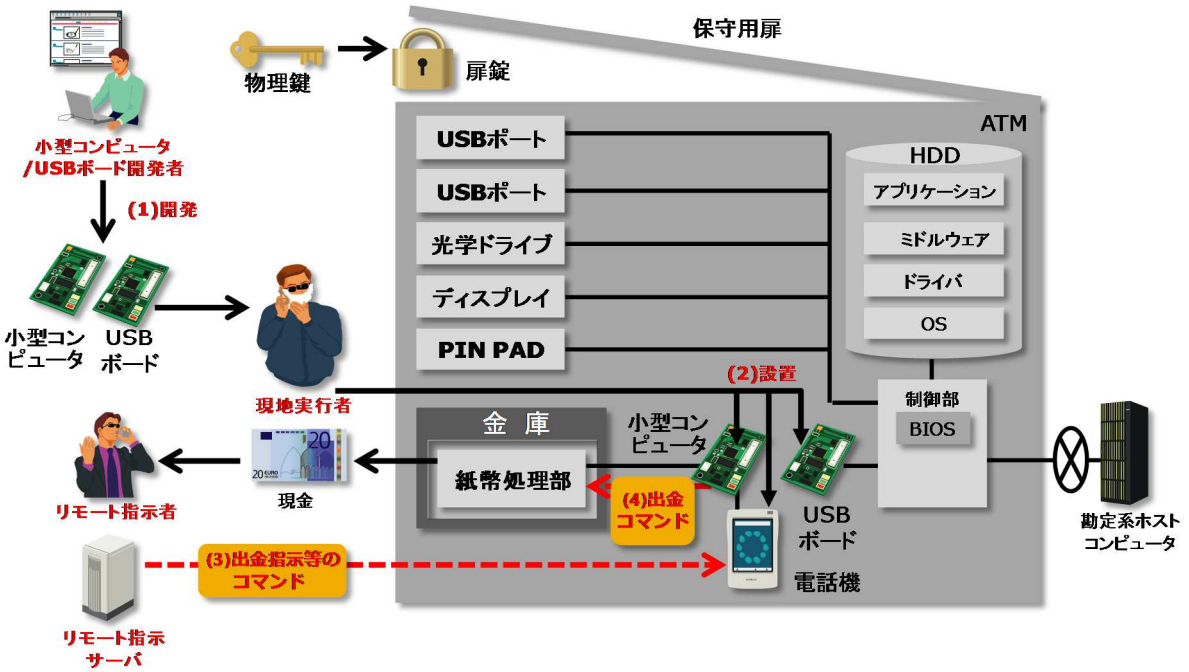

図 3-2 小型コンピュータを用いた不正出金の構図（海外事例）

上記インシデントを受け、当事国の執行機関は再発防止のための各種指導を行っていたり、インターネット上で対策案が公開されている(*8)(*9)。

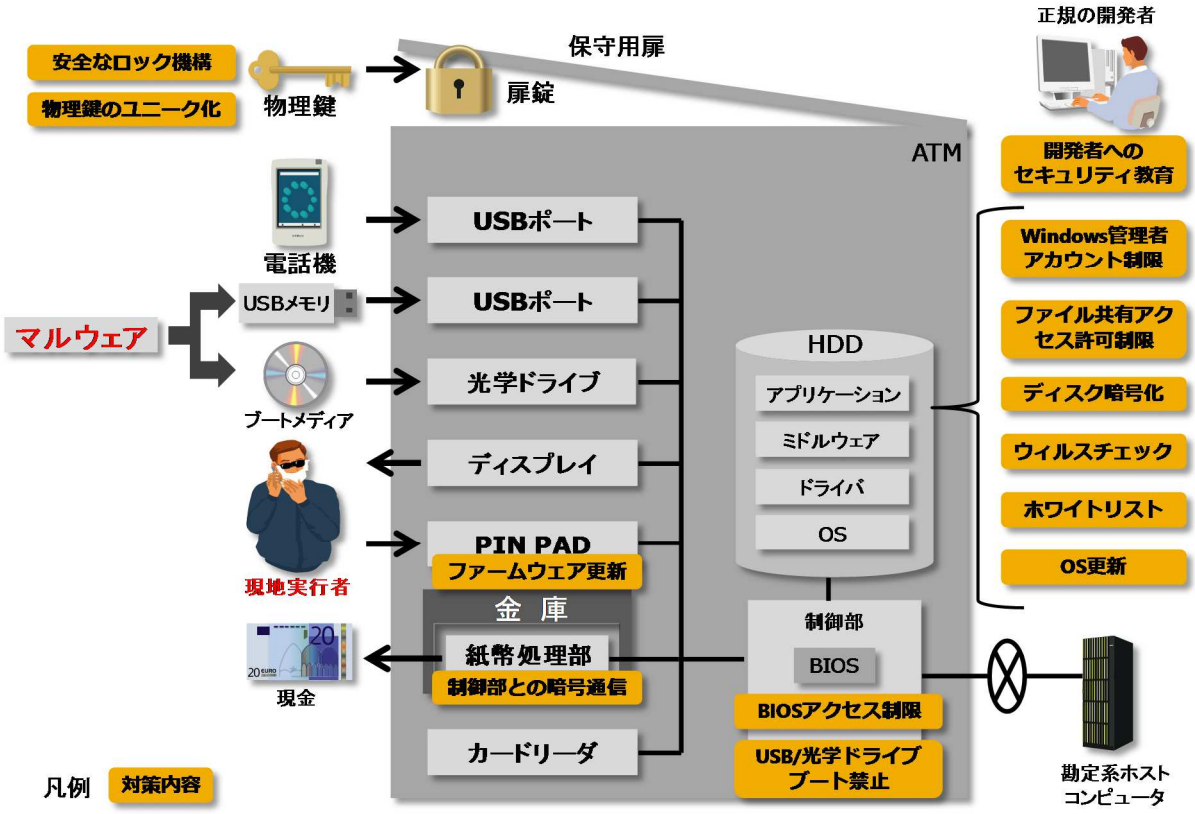

図 3-3 各種指導例

それらを要約すると現状からフィードバックして補強すべき事項が見えてくる。なお、これらはその当事国における事例であり、全て日本の現状に当てはまる訳ではないが、今後は十分に配慮すべき項目である。

表 3-1 インシデントからのフィードバック事項

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。

3.2 フィードバック項目からみえてくるもの

3.1 節のフィードバック事項を更に考察し、後節の指針に引き継ぐ上での懸念事項として列挙する。

❒ 懸念事項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：

ATM 運用において悪意をもつ人物が内部に居ることを前提とするセキュリティ対策では、装置の対策に加えて関係者の作業内容を監査・牽制する管理コストが相対的に多く発生すると考えられる。

（２）人材の教育・訓練コスト：

セキュリティ対策の強化には対象となる ATM システムに携わる人々の再教育や再訓練が必須である。

（３）運用ルールのバリエーションが産むコスト高：

ATM システムの運用ルールは金融機関毎に異なるので、例えば保守作業に対する新たなセキュリティ強化策の提案が、ある金融機関では受け入れられても、別の金融機関では既存運用ルールとの乖離が大きくて受け入れられないかもしれない。そして金融機関ごとにカスタマイズされたセキュリティ強化策の提案と実行には更にコストがかさむという悪循環に陥る。

（４）改修のための ATM 運用休止に伴う機会損失：

例えば ATM のある部品に対し、改修作業によって高い耐タンパ性をもたせるには、セキュアルーム環境での部品分解と改修作業が必要となり、代替部品の供給がタイムリーにできない事態も起こりうる。この場合、ATM 運用の休止はビジネス機会損失に直結するので受け入れがたい。

（５）進化し続ける手口への都度対応によるコスト高：

図 3-3 の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主眼がおかれるが、これらの対策は犯罪手口の進化に都度対応しようとすると、将来に渡ってコスト増になるものと考えられる。

①ハードディスクドライブ内に存在する情報資産にはアプリケーション、ミドルウェア、ドライバ、OS などが多層構造で複雑な上、セキュリティ対策として管理すべき項目は 1,000 項目を超えると推察される。

②ATM アプリケーションは金融機関のサービス内容変更やカスタマイズなどで頻繁に更新されている。

③ハードディスクドライブは最も壊れやすいデバイスの一つであり、保守交換作業が頻繁に発生している。

（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：

一般的に OS のサプライヤーが脆弱性対策のために実施する不定期の更新において、その基盤上で動作する第三者のソフトウェアの動作保証はしていない。また OS のライフサイクルの後半において実施される更新では、特に古いハードウェア資源を使う場合に処理能力の低下回避を担保できない。そのため、ハードウェアの陳腐化・更改にあわせて OS 環境を更新するといった現実解になるものと考えられる。

以上のような状況の下では、分析の結果分かった脅威とリスク対策に対してコスト制約条件を視点に加えたバランスを取ることが必要である。

❒ 懸念事項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。作業員が不正行為を働いたり、ミスで不適切な作業を行ったりしても、それを発見・検証することがコストや作業時間の制限などで困難な場合が想定される。

（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。在職中における開発者への倫理教育は重要であり多くの企業で実施されている上、退社に際しての各種誓約行為も実施されている。しかしながら開発者のその後の行動に対する責任を開発ベンダに負わせることは不可能であると考えられる。

（３）内部犯行者の影

3.1 節で説明した事例の「侵入ルート」、「管理の不備」、「情報漏えい（と非正規保守部材の流通）」を見ると、不正操作や犯罪に内部の人間が関わっていた可能性を除外できない。ATM を運用・保守・開発する組織の構成員の士気に期待する発想が少なくともグローバルな世界では通用しない。

①「侵入ルート」: 物理的に ATM の保守用扉を開ける必要があり、運用者、保守員、警送員のいずれかが保守用扉の物理鍵を故意に犯罪者に提供した、または「管理の不備」によって犯罪者の手に図らずも渡ってしまった可能性がある。
②「管理の不備」: 脆弱な運用をしている ATM の存在を犯罪者に教えてしまった可能性が指摘されている(*10)。
③「情報漏えい」: 正規の開発者の周辺に存在していたインタフェース仕様書が漏えいし、それを参考にしてマルウェアが開発された可能性がある(*4)。

懸念事項を再整理すると、セキュリティ対策を行うには次のような管理のしづらさがあることが分かる。

(a) 保護すべき項目が多岐に渡り、管理不徹底に陥りやすい。特に大量な端末を管理する場合はその傾向が強い。
(b) 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。
(c) 障害時復旧や保守作業時の脆弱性対策が不十分である。
(d) 退社した開発者の行動は保証できない。

4 セキュリティ対策指針

前節で説明した前提を踏まえ、セキュリティ対策を行うための指針を示す。ここでは、情報処理推進機構から発行された「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～」に掲載されている 17 指針のうち、ATM のセキュリティ対策に関係の深い 12 指針を拾いあげて関連付けを解説する。下記の指針で取り上げていない項目は､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するが、IoT 時代を踏まえて、既存の体制や仕組みを見直していくことも必要である。

表 4-1 「つながる世界の開発指針」開発指針と ATM セキュリティ対策指針の関係

「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

[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。

海外ではマルウェアを ATM にインストールして不正出金を行うといった、新しい形の犯罪（サイバー・フィジカル犯罪）が増加してきている。このような新しい犯罪情報と、それらに対する既存のセキュリティガイドラインや対策例が複数の国の機関や業界団体、企業から出されている。現在はハッキング技術やそれに必要なツール等が容易に入手できる時代であることを考慮し、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。

サイバー・フィジカル犯罪に対抗していくには、従来にない視点でセキュリティ対策が必要となる。そのため、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。

ATM では運用や保守において装置内部へのアクセスが生じ、不正を働くための機会も十分に存在する。海外犯罪事例では運用に関わるスタッフのスキルや士気を期待できない場合に ATM の管理不備が放置された状況を突かれているので、監視・管理の強化対象は、スタッフ、ATM 本体、保守部品等と広範に渡ってしまう。

しかし、監視・管理を強化するほど運用や保守の効率が落ちるので、そうならない工夫が必要である。例えば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。

運用に関わるスタッフの資質に期待できないので、作業ミスが起こりうることを想定しなければならない。また様々な事情で必要な手順が守られない場合も想定しなければならない。一つのミスや手順が遵守されない場合でも致命的にならないような対策（レガシーな情報システムで行われている多重防御）が有効である。例えば制御部にセキュリティホールがあったとしても、周辺機器側でも守ることで不正出金が起こらないような仕組みが考えられる。

一般的に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。これによりセキュリティ強度向上が期待できる。

[ATM-指針4] 守るべきものを特定する

① つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。

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。例えば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。なおカード番号、暗証番号は既存の PCI(Payment Card Industry)規格[2][3][4]で保護対象となっている情報資産である。

[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。

一般に ATM は金融機関の専用ネットワークに接続され、外部ネットワークとは遮断された状態で運用される。一方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。ただし今後は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

ATM の運用や保守では ATM 内部へのアクセスが生じるので、運用・保守時の攻撃リスクを想定しておく必要がある。

■ 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。例えばウィルスソフトの搭載、OS ハードニング等である。これらの対策は ATM システム全体の運用に影響を与える可能性があるので、金融機関やシステムインテグレータと事前によく合意しておく必要がある。さらに、これらの対策が回避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。

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) 重要機器内資産のトレーサビリティ

ATM 内の制御部とは異なる小型機器（ブラックボックス）が紙幣処理部に接続されて不正な出金が行われると、制御部側にはその出金処理の結果が残らない。それに備えて紙幣処理部にも出金の事実に関するログを保存した上、その正当性を全体で監査すれば不正を発見しやすくなる。

(b) 保守用重要機器のトレーサビリティ

バックドア追加などの不正改造を受けた重要保守部品が ATM に組み込まれるリスクを考慮し、不正な保守部品が組み込まれたことを追跡する、または不正な保守部品が組み込まれるのを防止する仕組みが有効である。

(c) 保守作業のトレーサビリティ

運用や保守作業中の不正行為そのものを何らかの手段で監視できることが望ましい。一つの対策は作業中の様子を監視カメラ等で撮影することであるが、検証するために多大な時間が掛かるので、効率的な監視・監視手段が望ましい。

■ 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）

海外事件事例では、ATM 保守用扉の物理鍵に対する管理不備を突かれており、物理的 I/F、論理的 I/F に対する適切な管理が求められる。例えば、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。

[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。さらに保守会社には ATM 本体や保守部品を格納した倉庫があるので、保守会社で保管されている ATM 本体や保守部品に対する物理的な盗難リスクも考慮しなければならない。対策に関しては ATM-指針 5 で述べた内容が効果的である。

② 廃棄された機器や中古品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。

ATM に関しては運用終了後の機器内に残る情報の消去などのルールが取り決められているが、管理不備を突かれた海外事例からはこのルールが必ずしも守られないことを想定したリスクを考慮する必要がある。外部と通信可能な小型機器が ATM 内部に組み込まれた事例を見ると、現時点ではその証拠を提示できないものの、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マルウェアが乗っ取り、不正出金された事例を鑑みると、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。

紙幣処理部といった重要周辺機器の外部インタフェース保護には、暗号技術によるメッセージデータ正当性検証が有効である。保守用 I/F の対策に関しては、ATM-指針 5 で述べた内容が効果的である。

■ 内包リスクへの対策

ATM ではすでに仕組みができているので割愛する。

■ 物理的接触によるリスクへの対策

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 で示す対策が効果的である。

■ 守るべきものの重要度に応じたセキュリティ対策

ATM においては、犯罪や不正行為で狙われる資産はある程度限られ、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のため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。

守るべきものの重要度に応じたセキュリティ対策の考え方に関しては、クレジット取引システムで準拠が求められる PCI(Payment Card Industry)規格[2][3][4]が参考になる。例えば、カード番号は ATM 内でメモリ上では平文の形で存在することを許容される代わりに、そのアクセス管理や監査などのセキュリティ対策が求められる。

一方、暗証番号はそれを入力する PIN PAD 内で暗号化し、PIN PAD 外部には暗号化された状態でしか存在が許されない。このようにデータ漏えい時の影響度に応じて、対策レベルが異なるようにセキュリティ規格が定義されている。

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 内の制御部、重要周辺機器での個々の対策だけで十分でない場合は、制御部、重要周辺機器それぞれ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。例えば制御部には電子ジャーナルと呼ばれる取引ログの記録が残されているが、それとは別途紙幣処理部に入出金処理のログを追加で記録し、電子ジャーナルと比較すれば紙幣処理部で正当な入出金処理が行われたかを検証することが可能になる。あるいは周辺機器同士でも機器が保持している情報の比較により、同様な検証が可能になる場合もある。

[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

① IoT 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 内の制御部と紙幣処理部間の通信を暗号化するといった、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。例えば保守作業で制御部を交換する場合、新しい制御部と紙幣処理部間で暗号通信するための新たな暗号鍵の設定が生じるが、これには特権モードでの実行が求められるだろう。特権モードでなくても暗号鍵の設定ができるとなると、権限のないスタッフの私的な PC と紙幣処理部とを勝手に接続して暗号通信でき、不正出金が可能となるからである。

あるいは暗号通信機能が制御部や周辺機器に実装された後、その暗号機能を停止・削除する場合も同様に特権モードが必要である。これも暗号機能を無効にする攻撃の阻止に有効である。

[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。

ATM では、利用者の安全性を考慮した設計・評価および生体認証装置や紙幣鑑別装置等のセキュリティ製品の設計・評価の仕組みは既に存在しており、一通りの安全安心の設計

の検証・評価の仕組みはあると考えられる。その一方で、セキュリティに関する攻撃は日々進化しており、海外を中心に新たな手口が次々に出現している。そのため、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 制御部や周辺機器には、保守のために状態や処理結果をログとして保存する機能が備わっている。指針８で述べたように、これらの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。

ATM では保存された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る。さらに ATM での記録を残す期間を最低限は確保し、当該記録へのアクセスを管理する方法や、収集したログを定期的に、あるいは不定期にサーバ等に送信する方法がある。

[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。

一般にATMはATMベンダやシステムインテグレータとの保守契約の下で運用されているので、アップデートなどの安全安心を維持する機能やサービス提供の仕組みは既に存在する。一方、攻撃側の技術も急速に発展しているので、今後 ATM に対する暗号技術のアップデートが急速に高まると考えられる。

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。具体的な指針や方法は、国際標準や業界標準などの文書に記載されているので、本書では割愛する。さらに暗号鍵管理は ATM システム全体にも影響を及ぼす場合があるので、新たな保守契約を含めて影響を考慮しておく必要がある。

[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。

ATM は契約に基づいて売買や運用・保守が行われるので、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 開発フェーズとセキュリティの取組み

世の中の製品は、運用管理者がしっかりした管理された製品と、コンシューマ製品のように運用管理者が存在しない管理されない製品の２つに分類される。ATM は本来しっかり管理された製品であるが、海外 ATM の管理不備による不正出金事例を見ると、管理されない製品という側面も併せもつと考えた方が適切である。ATM を管理された製品として位置づけた場合に、前章で述べた指針への取組みがどのように対応するかを本章で述べる。管理された製品の開発ライフサイクルとしては、NIST SP800-64「Security Considerations in the System Development Life Cycle」（SDLC）[6][7]を取り上げる。以下、5.1 節でライフサイクルにおけるフェーズの定義を概説し、5.2 節で各フェーズの詳細を説明した上で、5.3 節で各フェーズにおけるセキュリティ指針の取組みを対応付ける。

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開発から廃棄に至るまでのライフサイクルが存在する。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、可用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。 ・機能テストおよ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　各フェーズの詳細説明

本節では、前節で概説したシステム開発ライフサイクルでの各フェーズの詳細内容について説明する。ATM 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。

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り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、規定および基準など）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送、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、実現するための鍵となる。

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ュリティ取組み

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。

展開フェーズ

製品開発ライフサイクルの展開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 5-4 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	**確立した環境またはシステムへのセキュリティの配合** 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証を満たしているか、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

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 保守・運用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	**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** 製品または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。

※ATM ベンダが ATM ガイドラインの指針に基づいた運用・保守フェーズのセキュリティ機能を提供した場合、金融機関、保守会社、警送会社はそのセキュリティ機能を用いた運用・保守を行うべきことを示している

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	**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廃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。

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、ATM ガイドラインとして適用される指針の番号との対応を、表 5-7 に示す。●はシステム開発ライフサイクルの中で、それぞれの「ATM-指針」を考慮すべき場面を示している。なお、●のない項番は ATM 分野で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している。

表 5-7 システム開発ライフサイクルにおける ATM-指針の考慮場面

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

まとめ

本書は ATM 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。ベンダの製品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。

脚注

(*1) 各国の中央銀行や政府、業界団体が発行している ATM 関連のガイドライン例
- 参考文献[1]
- 参考文献[4]
- 参考文献[8]
- 参考文献[9]
- 参考文献[10]
- 参考文献[11]

上記規格群中での PAYMENT CARD INDUSTRY (PCI)の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[2]であれば、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。EMV 規格[5]についても同様である。

(*2) 例えば、ATM 側でデータを暗号化してホストコンピュータでそのデータを復号することが ATM 側のセキュリティとして有効である場合、本書ではその要件を推奨するものとする。

(*3) Windows は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

(*4) 例えば、以下の事例が WEB で公開されている。
- NCR 社製 ATM の API ドキュメントが百度（バイドゥ）で公開される
  http://blog.f-secure.jp/archives/50736068.html
- PLANNING TO ROB A WINDOWS ATM? DITCH THE SLEDGEHAMMER AND BRING A USB STICK
  http://www.theregister.co.uk/2014/01/06/atm_malware_stick_up/
- TEXTING ATMS FOR CASH SHOWS CYBERCRIMINALS' INCREASING SOPHISTICATION
  http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

(*5) APPLICATION PROGRAMMING INTERFACES このインタフェースの代表的なものとしては EXTENSIONS FOR FINANCIAL SERVICES (XFS) MIDDLEWARE が挙げられる。

(*6) NCR 社製 ATM の API ドキュメントが百度（バイドゥ）で公開される
http://blog.f-secure.jp/archives/50736068.html

(*7) THIEVES 'JACKPOT' ATMS IN NEW 'BLACK BOX' ATTACK
http://www.theage.com.au/it-pro/security-it/thieves-jackpot-atms-in-new-black-box-attack-20150107-12k0el.html

(*8) 例えば、以下の事例が挙げられる。
- 参考文献[9]
- TEXTING ATMS FOR CASH SHOWS CYBERCRIMINALS' INCREASING SOPHISTICATION
  http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication
- Backdoor.Ploutus.B テクニカルノート
  https://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2013-102523-2331-99&tabid=2

(*9) 重大インシデントを受けた当事国で発行されたガイドラインや勧告書
- 参考文献[9]

(*10) ATM JACKPOT WITH MALWARE(TIMES OF INDIA の記事より)

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ほしい重要ポイント～、独立行政法人情報処理推進機構　技術本部　ソフトウェア高信頼化センター https://www.ipa.go.jp/files/000051411.pdf

[2] Payment Card Industry (PCI) Data Security Standard,
Requirements and Security Assessment Procedures Version 3.2, April 2016

[3] Payment Card Industry (PCI) Payment Application Data Security Standard
Requirements and Security Assessment Procedures Version 3.2, May 2016

[4] Information Supplement PCI PTS ATM Security Guidelines, January 2013
Information Supplement PCI PTS ATM Security Guidelines

[5] EMVCo
https://www.emvco.com/

[6] NIST Special Publication 800-64 Revision 2
Security Considerations in the System Development Life Cycle

[7] 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

[8] TECHNOLOGY RISK MANAGEMENT GUIDELINES, JUNE 2013, Monetary Authority of Singapore
http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf

[9] GUIDANCE AND RECOMMENDATIONS REGARDING LOGICAL ATTACKS ON ATMS, Mitigating the risk, setting up lines of defence | Identifying and responding to logical attacks, EUROPOL
http://www.ncr.com/wp-content/uploads/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf

[10] 金融機関等コンピュータシステムの安全対策基準・解説書(第 8 版)，平成 23 年 3 月
https://www.fisc.or.jp/publication/disp_target_detail.php?pid=225

[11] 金融機関等コンピュータシステムの安全対策基準・解説書(第 8 版追補改訂),
平成 27 年 6 月
https://www.fisc.or.jp/publication/disp_target_detail.php?pid=316