製品分野別セキュリティガイドライン
金融端末（ATM）編

セキュリティ対策検討実践ガイド
－犯罪事例の分析と対策立案－
Ver. 1.0

平成29年5月29日

CCDS セキュリティガイドラインWG

ATM SWG

1. 実践ガイドの位置づけと特長

(1)セキュリティ対策検討実践ガイドの位置づけ

- 2016年6月に公開された「製品分野別セキュリティガイドライン金融端末(ATM)編」に従い、具体的なセキュリティ対策を検討するために、本ガイドは提供されている。
- セキュリティ対策を検討するに当たり、一般論で分析して得られた脅威より、過去に実際に起こった犯罪手口の方がリスクが高いと考え、本ガイドはそれらに対するセキュリティ対策を優先的に検討するためのものである。

(2)実践ガイドに沿った対策立案の特長

- セキュリティ対策を検討するに当たり、本実践ガイドでは多層防御を考慮するだけに留まらず、新たなセキュリティ対策が、既存業務への影響度合いも鑑みて、対策の実効的な有効性を見積もる方法を提供している。
- 既存業務への影響度合いは、セキュリティ対策導入に伴う新たな管理工数によって見積もられる。
- この方法により、既存業務との親和性を考慮して、真に有効なセキュリティ対策立案のための分析や検討が可能になることを期待している。

2. セキュリティ対策立案手順

節	分　類	項番	セキュリティ対策立案手順
2.1.1	犯罪事例分析と対策案リストアップ	（1）	守るべき保護対象のリストアップ
		（2）	守るべき保護対象を狙う典型的な犯罪事例の収集
		（3）	犯罪事例の攻撃ステップへの分解
		（4）	各攻撃ステップを防御するための対策のリストアップ（多層防御を考慮）
2.2.2	対策の業務への影響分析	（5）	リストアップした各対策が既存業務に与える影響（運用中の管理工数の面から）の分析
2.3	対策案の比較評価	（6）	既存業務への影響を考慮した各対策効果の実効性見積り
		（7）	実効的効果を考慮した対策比較と選択
2.4	未出現犯罪に対する適用拡張	（8）	未出現の犯罪に対しても、上記（1）～（7）の分析を通じて有効な対策を見積り、適用拡張

3.（1）守るべき保護対象のリストアップ
（2）守るべき保護対象を狙う典型的な犯罪事例の収集

（1）守るべき保護対象のリストアップ例

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 ・磁気カードトラックデータ	・現金（紙幣、硬貨） ・出金コマンド ・入出金口シャッタ開コマンド ・入金計数データ/入金（送金）先口座番号
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（ATMアプリ内のメモリ上） ・カード媒体
小	－	上記を含まないログデータ等

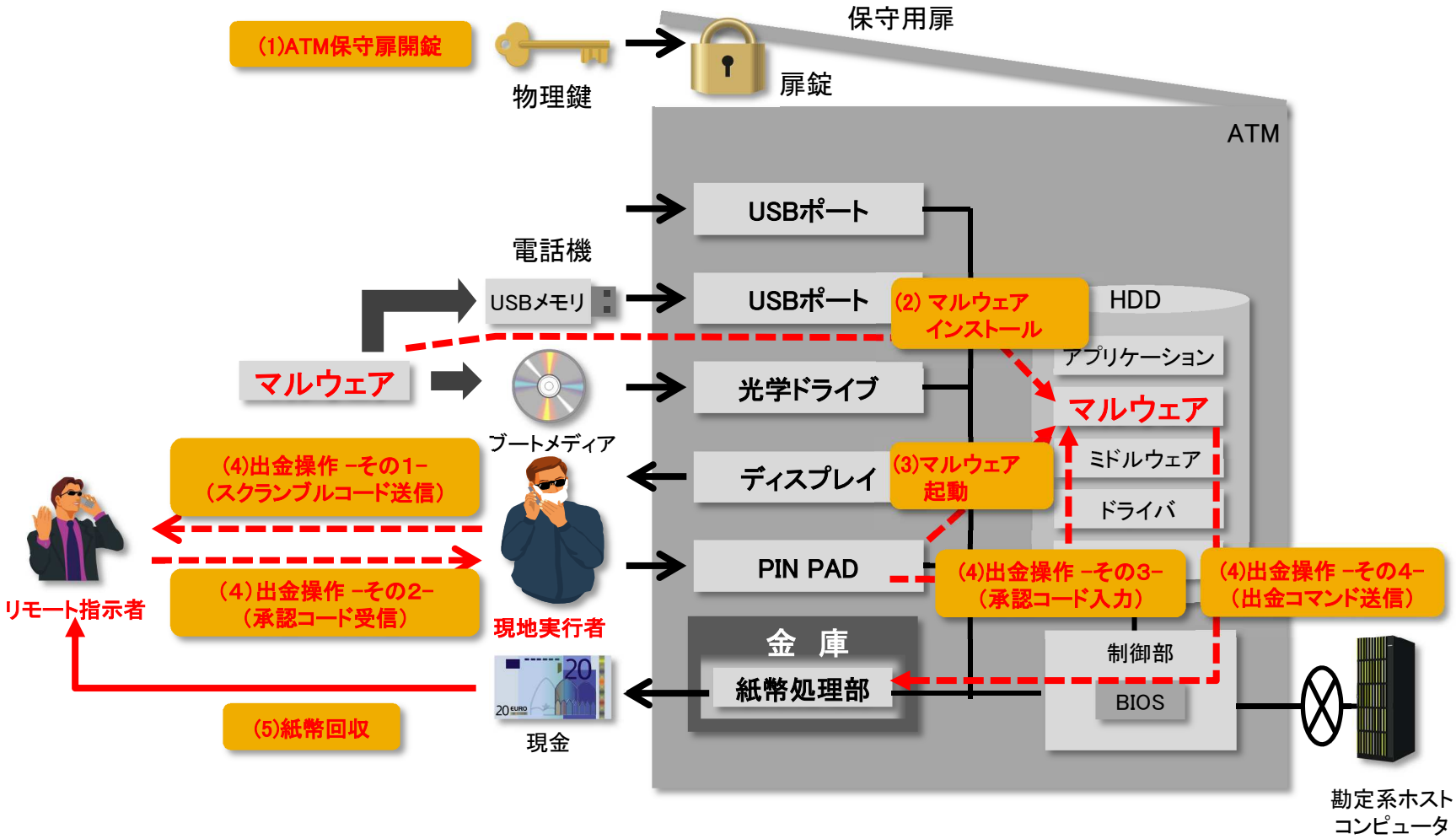
（2）守るべき保護対象を狙う典型的な犯罪事例の収集例

重要度	分類	保護対象	犯罪事例
高	暗証番号	・暗証番号	暗号化されていない場合に、マルウェアなどによりデータを盗難される。
中	カードデータ	・カードデータ（ATMアプリ内メモリ）	マルウェアを用いたATM制御部RAM上のカード番号を盗難される。ネットワークから侵入する場合は、マルウェアが正規ソフトとしてソフト配布サーバから配信されるので、ホワイトリスト型ウィルス対策が有効でない場合がある。
高	現金（紙幣）	・出金コマンド	マルウェアを用いた不正出金が行われる。 （a）媒体を用いた物理的侵入/b）ネットワークからの侵入）

3.（3）犯罪事例の攻撃ステップへの分解

（3）犯罪事例の攻撃ステップへの分解

例）マルウェアを用いた不正出金の構図（物理的侵入）の攻撃ステップ



3.（4）各攻撃ステップを防御するための対策のリストアップ（多層防御を考慮）

（4）各攻撃ステップを防御するための対策リスト例（多層防御を考慮）

以下の表は、EUROPOL(欧州刑事警察機構)が発行した「ガイダンスと推奨事項」(*1)に記載されている対策要件を、多層防御に当てはめた事例である。

マルウェアによる不正出金の各攻撃ステップを防御するための対策リスト

	①保守扉開錠	②マルウェアインストール	③マルウェア起動	④出金操作
第1弾 物理的アクセス	**①本人確認** **②保守扉鍵管理** **③監視カメラ**			
第2弾 オフライン防御		**①BIOS設定** ②ハードディスク暗号(*2)		
第3弾 オンライン防御		**⑥OSハードニング** ⑦ホワイトリスト ⑧USBデバイス防御	**⑥OSハードニング** ⑦ホワイトリスト	
第4弾 追加対策		**⑪ソフトウェア挙動監視** **⑫ATM装置監視** **⑬職務の分割**	**⑪ソフトウェア挙動監視** **⑫ATM装置監視**	**⑭現金補充額/周期の最適化**

※ 赤色で下線が引かれた太文字は、対策実行に当たり管理工数が多いと思われる要件を示す。

*1 European law enforcement agency, "Guidance and recommendations regarding logical attacks on ATMs", 11th June 2015, https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf

*2 理暗号鍵管理のためにパスワードが使われる場合は、管理工数が大きい対策に分類される。

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その1–

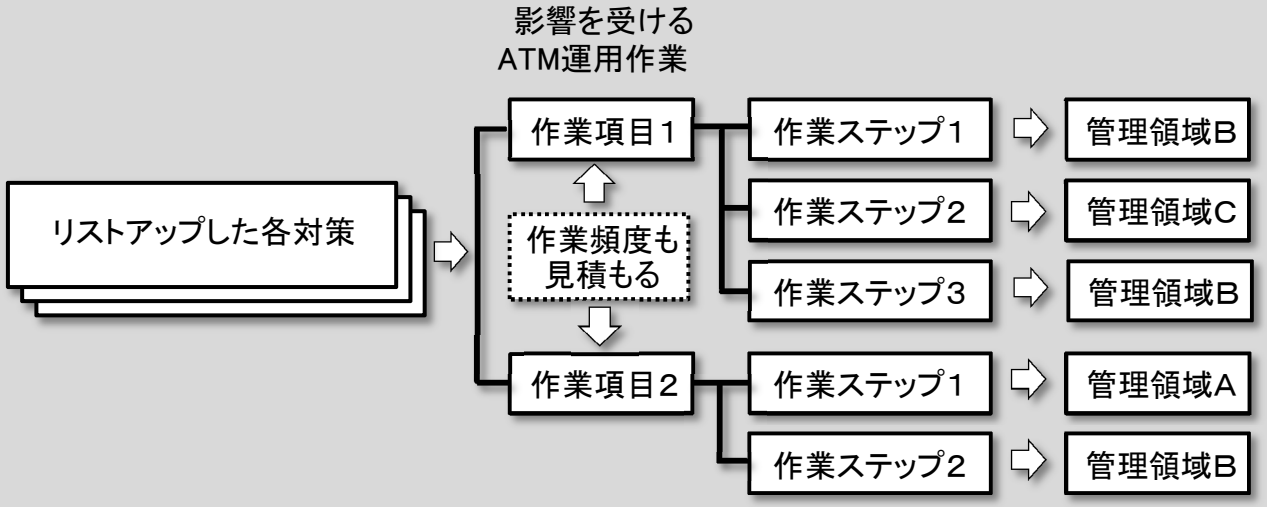
（5）各対策が既存の業務に与える影響を管理工数の面から分析（手順） –その1–

（分析ステップⅠ）リストアップした各対策の影響分析

Ⅰ–① リストアップした各対策が影響を与えるATM運用に関する「作業項目」を洗い出し、「作業頻度」（年間当り）を想定する。

Ⅰ–② 洗い出した「作業項目」を一連の「作業ステップ」に分解する。

Ⅰ–③ ATM運用に関する「管理領域」を定義し、各「作業ステップ」を当てはめる。「管理領域」とは、管理工数を見積もりやすくするために本書で定義する概念で、例えば、保守扉内作業、金庫扉内作業、営業店内作業のように物理境界ごとに定義してもよい。



Ⅰ–④ 「管理領域」ごとに、各対策から導かれる管理の「あるべき姿」を想定する。

Ⅰ–⑤ 「あるべき姿」を実現するために、新たに必要となる管理作業内容を洗い出す。

Ⅰ–⑥ 上記Ⅰ–⑤に加えて、「作業項目」発生に依らず、各要件を満たすために、定常的に発生する管理作業内容も合わせて洗い出す。

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その2–

（5）各対策が既存の業務に与える影響を管理工数の面から分析（手順）–その2–

（分析ステップⅡ）リストアップした各対策の管理工数分析

Ⅱ–① 各「作業ステップ」において、それぞれの管理作業内容の工数を見積り、「作業項目」単位で累積する。加えて、定常的に発生する管理作業内容の工数も見積もる。

Ⅱ–② 「作業項目」単位で累積された管理作業内容の工数と、I–①の「作業項目」毎の頻度の積を計算する。それに定常的に発生する管理作業内容の工数を加える。それを全「作業項目」に渡って累積する。

Ⅱ–③ 上記Ⅱ–①、Ⅱ–②の作業を、リストアップした対策毎に行う。リストアップした対策が全く新規の「作業項目」を生じる場合も分析ステップⅠ、Ⅱを行う。

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その3–

■（分析ステップ I）リストアップした各対策の影響分析

I –① リストアップした各対策が影響を与えるATM運用に関する「作業項目」を洗い出し、「作業頻度」（年間当り）を想定する。

運用に必要な作業項目と作業内容例

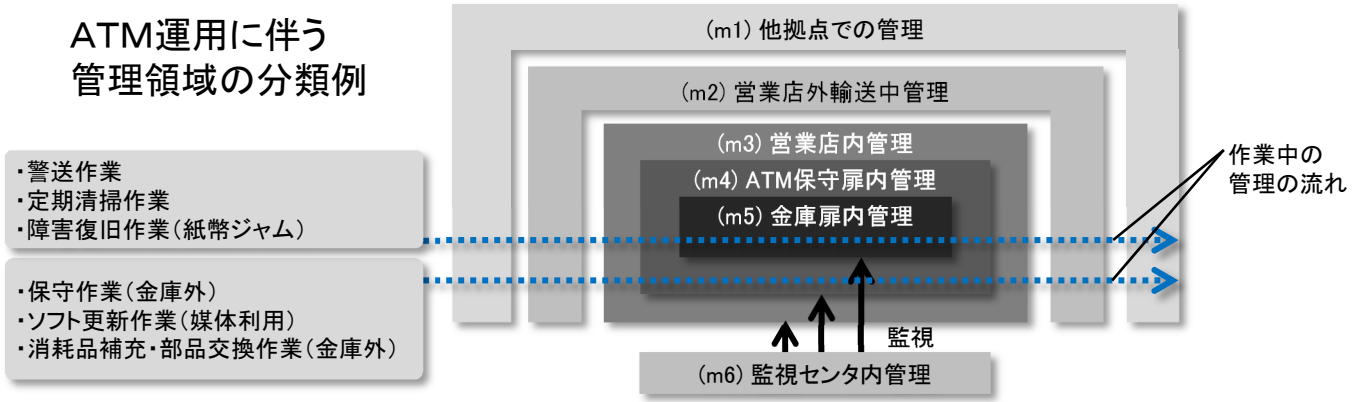
作業項目	作業内容
a) 警送作業	警送会社の警送員、あるいは銀行の係員が、ATMから余分な現金を回収したり、不足現金を補充したりする作業である。通常一人で現金にアクセスすることはセキュリティ上禁止されており、二人以上の作業員が一緒に作業を行う。ATM内部へのアクセスを伴う作業としては、警送作業が最も多い。
b) 定期清掃作業	ATM内では紙幣搬送に伴い紙粉が内部に蓄積して、紙幣ジャム等の障害につながる可能性があるので、定期的に清掃作業が行われている。清掃は現金処理部に対しても行われるので、警送作業と同様にATM保守扉を開錠することに加えて、金庫扉等の物理的保護手段を開錠する作業が発生する。
c) ソフト更新作業	ATMでは、サービス変更等に伴い、アプリケーションなどのソフトウェアや設定変更、および、ATMでの広告コンテンツの入れ替え等のために、ソフトウェアの更新作業が発生する。作業の発生頻度については、金融機関毎に異なる。
d) 障害復旧作業	ATMサービスにおいて、紙幣の搬送中にジャムが発生するなどの障害が起こった場合に復旧作業が必要になる。現金処理部での障害復旧は、警送作業と同様にATM保守扉を開錠することに加えて、金庫扉等の物理的保護手段を開錠する作業が発生する。一般に障害復旧による内部へのアクセス頻度は最も少ない。
e) 消耗品補充・部品交換作業	取引明細書の印字用紙や通帳プリンタのインクといった消耗品の補充、ならびに、ハードディスクドライブや、紙幣搬送に必要なゴムローラーやベルトなどの寿命がある部品の交換に伴い、ATM内部へのアクセスを伴う作業が発生する。

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その4–

■（分析ステップ I）リストアップした各対策の影響分析

I –② 洗い出した「作業項目」を一連の「作業ステップ」に分解した上で、I –③ ATM運用に関する「管理領域」を定義し、各「作業ステップ」を当てはめる。

ATM運用に伴う
管理領域の分類例



警送作業の作業ステップへの分解と管理領域の分類例

作業ステップ	作業ステップ毎の管理作業	管理領域
作業員本人確認	作業員身分証明書確認/作業スケジュール照合	(m3) 営業店内管理
ATM保守扉物理鍵手渡し	保守扉物理鍵持出管理	
侵入警報装置解除	侵入警報装置解除キー持出管理	(m4) ATM保守扉内管理
金庫扉開錠	二人一組の金庫扉物理鍵管理	(m5) 金庫扉内管理
現金カセット交換作業	作業記録と妥当性検証	
金庫扉閉錠と侵入警報装置起動	金庫扉物理鍵施錠管理	(m4) ATM保守扉内管理
ATM保守扉物理鍵返却	保守扉物理鍵返却管理	(m3) 営業店内管理
作業記録	作業記録管理	

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その5–

■（分析ステップ I）リストアップした各対策の影響分析 –その2–

I –④「管理領域」ごとに各対策から導かれる管理の「あるべき姿」を想定し、I –⑤「あるべき姿」を実現するために、必要となる管理作業内容を洗い出すと共に、I –⑥ 定常的に発生する管理作業内容も合わせて洗い出す。

ATM運用に伴い、作業発生時のセキュリティ維持に必要な「あるべき管理の姿」に必要な管理作業内容例

#	管理領域	想定場面	「あるべき管理の姿」に必要な管理作業内容
1	(m2) 営業店外輸送中管理	リリース時	・媒体運搬中の管理 （二人一組による管理等）
2		出動時	・媒体・パスワード運搬中の管理 （二人一組による管理等）
3	(m3) 営業店内管理	出動時	・鍵貸出・返却管理、適切使用管理 ・出張所の場合輸送中の管理 （二人一組による管理等）
4	(m4) ATM保守扉内管理	出動時	・作業中の不正監視 （二人一組による管理等）
5	(m6) 監視センタ内管理	定期確認	・ブース監視カメラ画像を異常がないか、定期的な目視確認

ATM運用に伴い、定常的に発生する管理作業の「あるべき管理の姿」に必要な作業内容例

#	管理領域	想定場面	「あるべき管理の姿」に必要な管理作業内容
1	(m3) 営業店内管理	常時 (24h×365日)	・物理鍵保管場所でのアクセス管理（生体認証等）
2	(m1) 他拠点での管理	開発中常時 (24h×365日)	・開発環境や評価環境のアクセス管理や維持管理
3		常時 (24h×365日)	・媒体パスワードのアクセス管理（生体認証等） ・リモート配信の場合はサーバやネットワークのセキュリティ管理（入退管理の生体認証等）
4	(m6) 監視センタ内管理	常時 (24h×365日)	・ATMからの異常動作や想定外のシャットダウンを常にチェック ・ブース監視カメラ画像を異常がないか定期的な目視確認

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その6–

■（分析ステップⅡ）リストアップした各対策の管理工数分析

Ⅱ–① 各「作業ステップ」において、それぞれの管理作業内容の工数を見積り、「作業項目」単位で累積する。
加えて、定常的に発生する管理作業内容の工数も見積もる。

管理領域毎の想定管理作業工数見積り例

#	管理領域	想定場面	「あるべき管理の姿」に必要な管理作業内容	想定管理工数
1	(m2) 営業店外輸送中管理	出動時	・媒体・パスワード運搬中の管理（二人一組による管理等）	人件費単価×2人分×移動時間/回/営業店
2	(m3) 営業店内管理	出動時	・鍵貸出・返却管理、適切使用管理	鍵貸出返却手続き時間/回/営業店
3			・出張所の場合輸送中の管理（二人一組による管理等）	人件費単価×2人分×移動時間/回/営業店
4	(m4) ATM保守扉内管理	出動時	・作業中の不正監視（二人一組による管理等）	人件費単価×2人分×作業時間/回/台
5	(m6) 監視センタ内管理	定期確認時	・ブース監視カメラ画像を異常がないか定期的な目視確認。	映像検証作業時間/回/週/店舗

3.（5）各対策が既存の業務に与える影響を管理工数の面から分析 –その7–

■（分析ステップⅡ）リストアップした各対策の管理工数分析

Ⅱ–②「作業項目」単位で累積された管理作業内容の工数と、Ⅰ–①の「作業項目」毎の頻度の積を計算する。
それに定常的に発生する管理作業内容の工数を加える。それを全「作業項目」に渡って累積する。

Ⅱ–③ 上記Ⅱ–①、Ⅱ–②を、リストアップした対策毎に行う。リストアップした対策が全く新規の「作業項目」を生じる場合も分析ステップⅠ、Ⅱを行う。

マルウェア不正出金対策(EUROPOL要件)と関わる管理領域の例

#	攻撃ステップ	対策（EUROPOL要件）管理領域	管理領域
1	(1) 保守扉開錠	①本人確認 ②保守扉鍵管理 ③監視カメラ	(m3) 営業店内管理
2	(2) マルウェア インストール	④BIOSパスワード保護 ⑤ハードディスク暗号化 (ﾊﾟｽﾜｰﾄﾞ,暗号鍵管理含む)	(m1) 他拠点での管理 (m2) 営業店外輸送中管理 (m3) 営業店内管理 (m4) ATM保守扉内管理
3		⑥OSハードニング ⑦ホワイトリスト ⑧USBデバイス防御 ⑪ソフトウェア挙動監視	(m4) ATM保守扉内管理
4		⑫ATM装置監視(予期せぬﾘﾌﾞｰﾄ)	(m6) 監視センタ内管理
5		⑬職務の分割	(m3) 営業店内管理
6	(3) マルウェア 起動	⑥OSハードニング ⑦ホワイトリスト ⑪ソフトウェア挙動監視	(m4) ATM保守扉内管理
7		⑫ATM装置監視	(m6) 監視センタ内管理
8	(4) 出金操作	⑭現金補充額/周期の最適化	(m5) 金庫扉内管理

3.（6）既存業務への影響を考慮した各対策効果の実効性見積り

- リストアップした対策の導入により、導入前後でセキュリティリスクがどう変化するかをリスク評価式により見積もる。
- リスク評価方式には複数の手法があり、以下にリスク評価方式の例を示す。

リスク評価方式例

評価手法	計算式
CVSS方式	基本値 ＝ RoundUp1(min [(影響度＋攻撃容易性), 10]) 影響度 ＝ 1 − (1 − C)×(1 − I)×(1 − A), C:機密性への影響、I:完全性への影響、A:可用性への影響 攻撃容易性 ＝ 8.22×AV×AC×PR×UI, AV:攻撃区分、AC:攻撃条件の複雑さ、PR:必要な特権レベル、UIユーザ関与レベル
CCDS 改良方式	リスク値 ＝ (難易度＋影響度)×攻撃者のモチベーション 難易度 ＝ 4ランク(複数条件,単一条件,単一条件 or ローカル,条件なし) 影響度 ＝ 4ランク(軽微,中程度,重大,壊滅的)
EDC方式	EDC : Event tree and Defense tree combined method 合計リスク値 ＝ 時系列事象毎リスク値を加算 時系列事象毎リスク値 ＝ その時系列事象での攻撃失敗確率 × その前の時系列事象までで受けた被害の影響度
ALE法	ALE : Annualized Loss Expectancy (年次損失予測) 年次損失予測(ALE) ＝ 単一損失予測(SLE)×年次発生頻度(ARO) ＝ 資産価値(AV)×顕在化(EF)×年次発生頻度(ARO) ただし、単一損失予測(SLE) ＝ 資産価値(AV)×顕在化(EF) SLE : Single Loss Expectancy, ARO : Annualized Rate of Occurrence
OWASP法	Risk(リスク) ＝ Likelihood (発生可能性)×Impact (影響度) Likelihood (発生可能性) ＝ Thread Agent (脅威の度合い)＋Vulnerability (脆弱性の度合い) Impact (影響度) ＝ Technical Impact (技術への影響度)＋Business Impact (ビジネスへの影響度)

3.（7）実効的効果を考慮した対策比較と選択

■リストアップした各対策のリスク値または、管理作業工数の算出結果を比較して、どの攻撃ステップで重点的に対策すると効果的かを見積もる。
■管理作業工数とリスク値は一対一対応するので、以下の説明ではリスク値同士を比較する代わりに、管理作業工数同士を比較する方法を使用する。

各管理領域に属する対策(EUROPOL要件)

攻撃ステップ	管理領域	対策（EUROPOL要件）
(1) 保守扉開錠	(m3) 営業店内管理	①本人確認 ②保守扉鍵管理 ③監視カメラ
(2) マルウェア インストール	(m1) 他拠点での管理	④BIOSパスワード保護 ⑤ハードディスク暗号化(パスワード,暗号鍵管理含む)
	(m2) 営業店外輸送中管理	④BIOSパスワード保護 ⑤ハードディスク暗号化(パスワード,暗号鍵管理含む)
	(m3) 営業店内管理	④BIOSパスワード保護 ⑤ハードディスク暗号化(パスワード,暗号鍵管理含む) ⑬職務の分割
	(m4) ATM保守扉内管理	④BIOSパスワード保護 ⑤ハードディスク暗号化(ﾊﾟｽﾜｰﾄﾞ,暗号鍵管理含む) ⑥OSハードニング ⑦ホワイトリスト ⑧USBデバイス防御 ⑪ソフトウェア挙動監視
	(m6) 監視センタ内管理	⑫ATM装置監視(予期せぬﾘﾌﾞｰﾄ)
(3) マルウェア 起動	(m4) ATM保守扉内管理	⑥OSハードニング ⑦ホワイトリスト ⑪ソフトウェア挙動監視
	(m6) 監視センタ内管理	⑫ATM装置監視
(4) 出金操作	(m5) 金庫扉内管理	⑭現金補充額/周期の最適化

３．（８）未出現の犯罪に対しても、上記（１）～（７）の分析を通じて有効な対策を見積り、適用拡張

- 未出現の脅威に対して、（１）守るべき保護対象を想定した上で、（２）過去に似たような犯罪事例を参照し、（３）攻撃ステップを想定して分解する。
- （４）各攻撃ステップを防御するための対策を、多層防御を考慮しながらリストアップし、（５）各対策が既存業務に与える影響（運用中の管理工数）を分析する。
- （６）既存業務への影響を考慮した各対策効果の実効性を見積もり、（７）実効的効果の観点から対策を比較して適切な対策を選択したり、最も効果的な防御が可能な攻撃ステップを選択する。