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. 2.00

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	2017/06/01	新規作成
Ver.2.0	2018/03/31	付録 6 追加

目　次

1 前書き

ATM のサイバー・フィジカル犯罪事件の背後にいると思われる犯罪者集団は、事件を起こせば自らも検挙されるリスクを抱えながら、マルウェアや関連するハードウェアを開発していると推測される。そのため、犯罪者集団にとってもリスク対リターンの大きさが重要と思われる。結果として、ある攻撃手口が成功した後、その手口がうまく機能している間はマイナーチェンジを繰り返しながら、攻撃対象国や金融機関を変えながら同じ手口を使い続けようとする傾向があると判断した方がよい。実際、ATM を攻撃するマルウェアにはマイナーチェンジされた亜種が沢山存在しており、上記の判断を後押しする事実がある。

よって、ATM セキュリティ対策を検討する際には、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、それらに対するセキュリティ対策を優先的に検討すべきである。そこで、「製品分野別セキュリティガイドライン金融端末（ATM）編」0 の実践編である本書では、過去に起こった犯罪事例の典型的な手口を参照しながら、その手口を防止するための多層防御を構築するための分析手順と対策の考え方を示す。ここでは、ひとつの犯罪手口に対して、犯罪ステップに分解すると共に、多層防御として、各犯罪ステップで何をどのように守るかの考え方と分析手順を示す。また、その分析手順を適用することにより、まだ事件が起こっていない将来の犯罪手口に対しても、その対策検討が可能になる。

対策検討における多層防御の分析にあたって、ATM 特有の性質を考慮することが重要である。社会には、電力システムや電車といった、管理者がいてしっかり管理されるシステムと、スマート家電やホームゲートウェイといったコンシューマ機器であり、管理者がいないシステムが存在する。ATM は金融機関という信頼された事業体が、正当な契約の下で信頼できる警送会社や保守会社と共に運用されており、ATM は本来しっかり管理されているシステムに分類されるべきである。

一方、海外の ATM 犯罪事例を見ると、十分に管理されていない ATM が攻撃対象となっているため、管理されていないシステムとしての側面もあると考えるべきである。よって、ATM のセキュリティ対策を検討するにあたり、運用中の管理を厳密に行うことによって資産を守るべきか、あるいは、管理されていないシステムとみなして、コンシューマ機器と同様に暗号などの仕組みによって守るべきかの選択肢が出てきうる。

それぞれの選択肢は一長一短があり、さらには、セキュリティ対策を導入するに当たっては、金融機関の ATM 運用実態も考慮する必要があるため、どちらがよいかは一概に言えない。そこで、本ガイドラインでは、管理で守るべきか、暗号などの仕組みで守るべきかを判断するための指針も合わせて提供する。その指針で最も考慮すべきポイントは運用中の管理工数の大きさである。複数の国や公的機関から既にセキュリティのガイドラインが

公開、非公開を問わず提供されている。それらに共通していることは、セキュリティ対策の導入に伴う運用中の管理工数の大きさについて言及されていないことである。

例えば、犯罪者が物理鍵を用いてATMの保守扉を開けて、マルウェアをATMにインストールして不正出金した事件事例に対する対策として、EUROPOL(欧州刑事警察機構)が発行した「ガイダンスと推奨事項」0では次のことが推奨されている。ATM保守扉を開錠する物理鍵を個別鍵に変えたり、ATM保守扉アクセス者の厳密な本人確認、ならびに、OS管理者パスワードをATM毎に個別に設定することである。このようなガイドラインの背景として、上記マルウェア事件事例では、一つの物理鍵で全てのATMの保守扉が開けられたり、マルウェアインストールに必要なOS管理者パスワードが共通になっていたりという管理不備が存在した。このように管理不備が存在したので、管理を厳密に行うことを推奨した既存のガイドラインの要件は多い。しかし、それに伴い過剰な管理工数を金融機関に強いるようになると、かえって管理不備を起こしたり、やるべき管理業務が無視されたりして、返ってセキュリティリスクを生むというジレンマが存在する。

海外ではATM設置現場への移動だけで半日かかるといった保守会社から遠距離に設置されているATMも存在する。例えば、ATM保守扉を個別鍵にすると、万が一担当保守員が持参すべきATM保守扉の物理鍵を間違えた場合は、当該ATMの障害復旧や保守作業ができない。結果として、保守会社は金融機関に対する契約違反になるだけでなく、必要以上の長時間のATM運用停止に陥り、利用者にとっても不便を強いられることになる。ATMサービスは社会インフラであるがゆえに、金融機関としても安定したサービスを社会に提供するという義務を背負っており、ここにセキュリティ優先で考えられない背景も存在する。

持参すべき物理鍵を間違えないようにするには、さらに別の管理も必要になるため、管理だけに頼りすぎると、管理が管理を呼ぶといった負の側面も出てくる。よって、セキュリティ対策を導入するにあたって、管理工数に大きなインパクトを与える場合には、管理ではなく暗号などの仕組みによって対策するという案も検討する必要がある。例えば、暗証番号を盗むマルウェアがATMにインストールされるような手口を想定する。その場合、ATMにアクセスする人を厳密に管理することによって、ATMへのマルウェアのインストールを防止する代わりに、暗証番号を内部で暗号化して出力する暗号化ピンパッドと呼ばれるデバイスをATMに設置する対策もありうる。

暗号化ピンパッドから出力される暗証番号は全て暗号化されているので、仮にATM内部にマルウェアが存在して暗証番号を盗んだとしても、悪用することは極めて困難である。このように、暗号化ピンパッドという仕組みで守れば、ATMへの厳密なアクセス管理ができない場合でも致命的にならない。結果として、金融機関の管理負担も減らして、ATM利用者に対しても利便性を犠牲にしなくても済むようになる。

このように暗号などの仕組みで守れば管理負担が減り、上記でのべたように保守員が物理鍵を間違えてATM障害復旧ができなくなるような事態も減るのでATMの安定運用が可能

になる。金融機関では、セキュリティ対策を検討するに当たり、管理で守るべきか、暗号などの仕組みで守るべきかを適切に判断する必要が出てくるため、本ガイドライン実践編ではその判断基準も合わせて提供する。

2 セキュリティ対策立案手順

ATM におけるセキュリティ対策を立案するための手順を表 2-1 に示す。（１）～（４）は犯罪事例の分析と､多層防御の観点から対策案をリストアップするステップである｡(５)～（７）はリストアップした対策案を比較評価するステップである。（８）は未出現の犯罪に対して対策案を適用拡張するステップである。

（１）では、最初に守るべき保護対象をリストアップし、その優先順位を明確にする。次に､(２）では守るべき保護対象を狙う典型的な犯罪事例を収集する。これは、犯罪者はうまく行っている手口をマイナーな変更を加えながら使い続ける傾向があると考え、過去に発生した典型的な犯罪手口が最もリスクが高いと考えているためである｡(３)において、収集した個々の犯罪事例に対し、犯罪手口を各攻撃ステップへ分解する｡（４）では、多層防御を考えながら、各攻撃ステップを防御するための対策案をリストアップする。

（５）～（７）は、セキュリティ対策導入に伴い発生する管理工数の観点から、個々の対策の実効性を見積もり、比較評価するためのステップである。すなわち、セキュリティ対策を導入しても、それに伴う管理工数が大き過ぎて負担が過剰になると、管理不徹底や手抜き、無視につながり、セキュリティ対策の有効性が低下してしまう。よって、管理工数の分析により、運用における対策の実効性を見積り、どの攻撃ステップで防御するのが最も有効であるかを比較できるようにする｡（５）では、各対策案が影響を与える業務をリストアップして、それぞれの対策を導入したときに、影響を与える業務で発生する管理工数を見積もる｡（６）では、見積もられた管理工数から適当なリスク計算式を用いて、比較に必要なリスク値を導き出す。最後に（７）では､（６）で見積もられたリスク値から、各対策案の実効的効果を比較し、どの攻撃ステップでどのような対策を講じるのが最も効果的で効率的かを比較評価する。

（８）では、未出現の犯罪に対しても､（１）～（７）の分析を適用して、有効な対策を見積もり、適用拡張する。

以下では、それぞれの分類毎に、各ステップに対する詳細手順を述べる。

表 2-1　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	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	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

2.1　犯罪事例分析と対策案リストアップ

本節では、表 2-1 の（1）～（4）のステップについて説明する。

（1）守るべき保護対象のリストアップ

表 2-2 に守るべき資産のリストを重要度と共に示す。資産の重要度は、対象となる資産が攻撃を受けた時の金融機関業務への影響の大きさと、悪意を持つ集団が得られる利益の大きさから判断する。既存規格として PCI Security Standards Council が策定・提供している PCI DSS や PCI PTS POI 等の規格では、暗証番号や磁気カードトラックデータが最も重要度が高く、その次にカード番号（Primary Account Number）がそれに続く。

一方、既存規格で保護されない対象として重要度が高いのは、現金と結びつく情報である。例えば、紙幣処理モジュールから現金を取り出すことができる出金コマンドは、現金と密接にリンクしているので、悪意を持つ集団が頻繁に狙う情報資産である。また、現時点では事例は出ていないが、入金取引において、紙幣を ATM に投入し入金計数した結果を詐称して、不正口座に入金額を積み上げて、その後、ATM から出金するという攻撃もありうる。

このような攻撃は、入金取引で口座に不正入金額を積み上げた後に、出金取引において通常の手続きで現金を引き出すことになり、攻撃手順が増えるため現時点ではそのような手口は報道されていない。しかし、不正出金の攻撃対策が普及した後には、入金取引を攻

撃するという手口が普及していくものと想像される。このように、攻撃者の標的になりやすい、かつ、金融機関業務への影響が大きい資産の優先度を上げて守る必要がある。

表 2-2 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

※　Payment Card Industry 規格等

（２）守るべき保護対象を狙う典型的な犯罪事例の収集

「1 前書き」で述べたように、ATM においては過去の犯罪手口が繰り返されるリスクが高いと考え、ステップ（１）で抽出した「守るべき保護対象」に対して、これらを狙う過去の犯罪事例の典型的な手口を収集し、セキュリティ対策立案に活用していく。表 2-3 に守るべき資産を標的とする犯罪事例を示す。

表 2-3　守るべき保護対象を狙う典型的な犯罪事例

#	重要度	分　類	保護対象	犯罪事例
1	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。
2	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。
3	高	現金（紙幣）	・出金コマンド	a)マルウェアを用いた不正出金が行われる。（媒体を用いた物理的侵入） b)マルウェアを用いた不正出金が行われる。（ネットワークからの侵入）

（３）犯罪事例の攻撃ステップへの分解

ステップ（２）で収集した犯罪の典型的な手口を、多層防御を検討するため、各攻撃ステップに分解する。

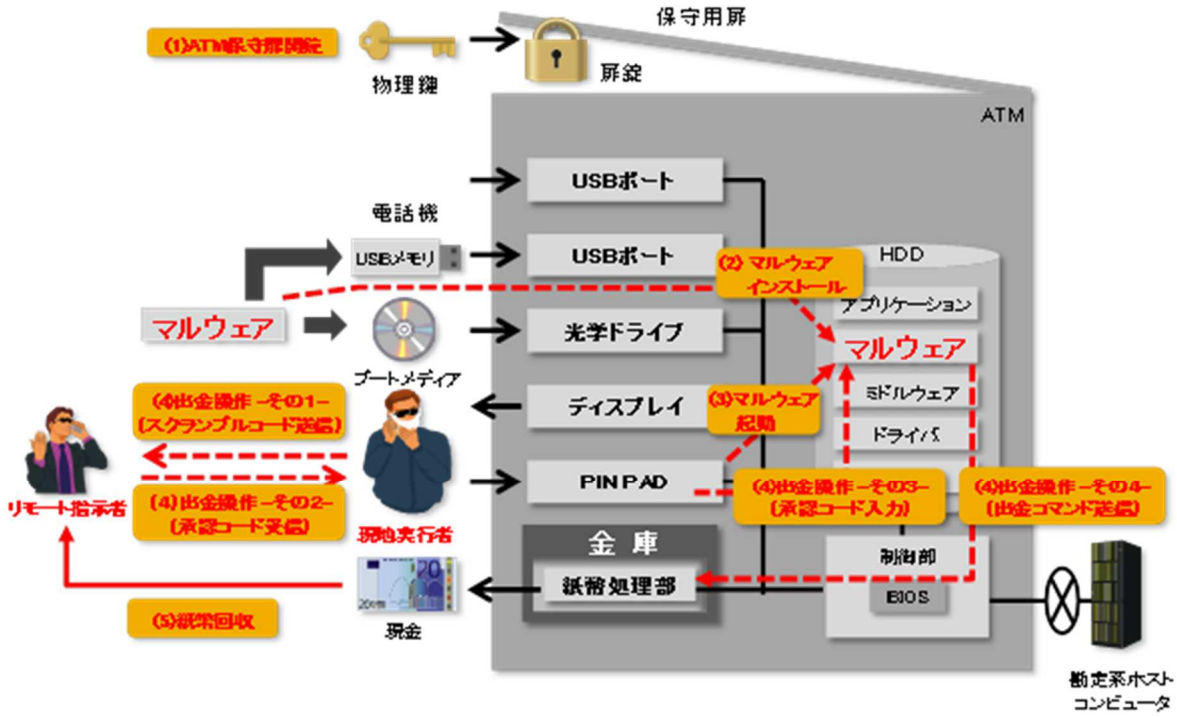


図 2-1 にマルウェアを用いた不正出金の構図（物理的侵入）を示し、各攻撃ステップへの分解例を表 2-4 に示す。

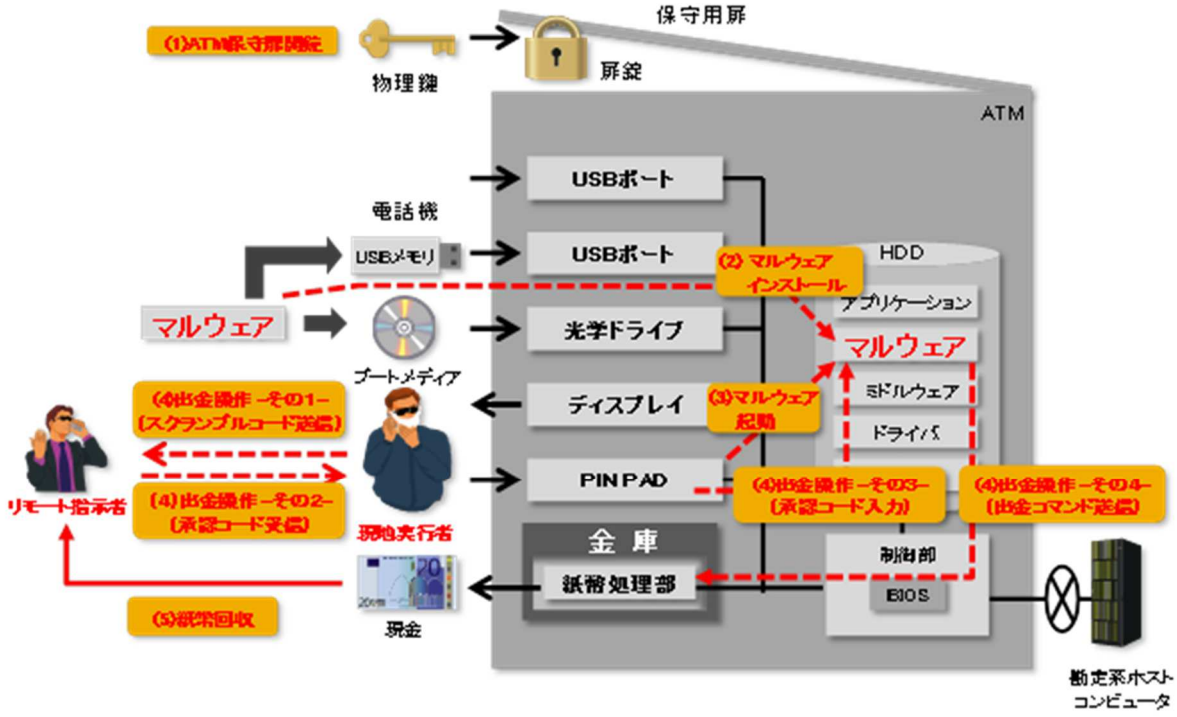


図 2-1　マルウェアを用いた不正出金の構図（物理的侵入）

表 2-4　マルウェアを用いた不正出金の攻撃ステップ（物理的侵入）

#	攻撃ステップ	攻撃内容
(1)	保守扉開錠	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、保守扉を開錠する。
(2)	マルウェアインストール	USBメモリ／CD-ROM等の媒体を用いてマルウェアをATM制御部にインストールする。
(3)	マルウェア起動	PIN PADを操作してインストールしたマルウェアを起動する。ホワイトリスト型アンチマルウェアソフトが入っている場合でも、レジストリをオフにして、その起動を妨害する場合がある。
(4)	出金操作	マルウェアに対する出金操作を行い、マルウェアから出金コマンドが紙幣処理部に送られ、紙幣がATMから排出される。 ●詳細ステップ: ATMのディスプレイに表示されるQRコードやスクランブルコードを、現地実行者が携帯電話や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(その1)。 現地実行者は、その応答として承認コードを携帯電話で受信し(その2)、ATMのPIN PADを用いてマルウェアに入力する(その3)。その結果、マルウェアから出金コマンドが送信できるようになり、紙幣処理部にマルウェアが出金コマンドを送信して紙幣を排出させる(その4)。
(5)	紙幣回収	現地実行者はATMから排出された紙幣を回収する。

（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）

典型的な犯罪事例を攻撃ステップに分解できたら、それぞれの攻撃ステップを防御するための対策をリストアップする。**表 2-5** はマルウェアを用いた不正出金事例に対して、EUROPOL(欧州刑事警察機構)が発行した「ガイダンスと推奨事項」0に記載されている各種対策要件を、多層防御を念頭に各攻撃ステップに当てはめたものである。赤色で下線が引かれた太文字は、対策実行に当たり運用中の管理工数が多いと思われる要件であることを示している。本例では、一例として人手によるログや作業の目視確認・検証、あるいは、パスワード管理が頻繁に必要な対策を「管理工数が多い対策」、それ以外を「管理工数が少ない対策」として記載している。

表 2-5　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		**④BIOSパスワード保護** ⑤ハードディスク暗号化 (*1)		
第3弾		**⑥OSハードニング**	**⑥OSハードニング**	

オンライン防御		⑦ホワイトリスト ⑧USB デバイス防御	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、対策実行に当たり運用中の管理工数が多いと思われる要件を示す。

*1 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。

2.2 対策の業務への影響分析

本節では、表 2-1 の（５）のステップについて説明する。

（５）リストアップした各対策が既存の業務に与える影響の分析

多層防御に必要なセキュリティ対策を導入すると、多かれ少なかれ既存の業務に影響を与えたり、新たに管理業務が発生したりする。既存業務への影響が大き過ぎたり、管理業務の負担が大き過ぎると、セキュリティ対策導入に伴う管理を徹底させることが難しくなり、対策の実効性に影響を与えうる。表 2-5 の赤色下線が引かれた太文字の対策項目は、運用中の管理工数に影響を与えると思われ、実効性に懸案がある項目である。そのため、その対策実行に伴いどのような管理項目が発生し、その管理工数がどの程度発生するかを見積もることは、セキュリティ対策の実効強度を見積もるために重要である。

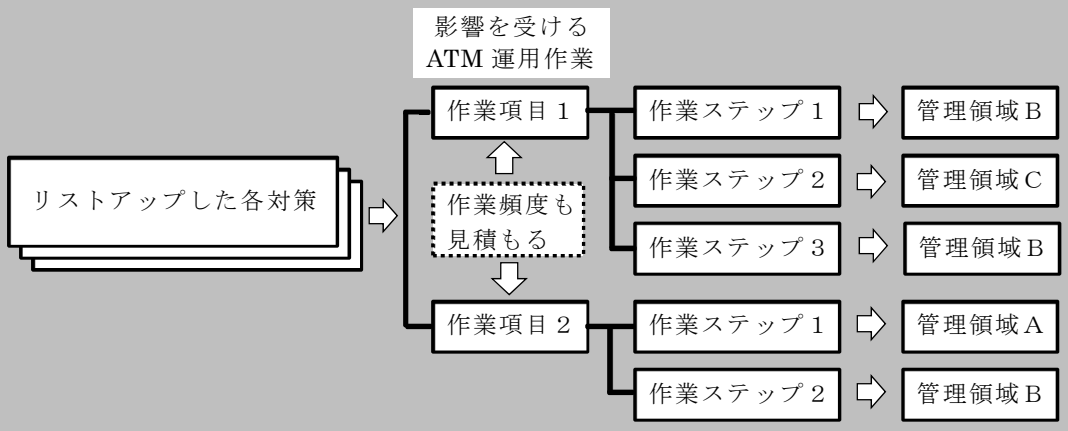
図 2-2 はリストアップした各対策が既存の業務に与える影響の分析手順を示す。本手順では、二つの分析ステップから構成されており、それぞれの分析ステップは、さらに６つ及び３つの分析サブステップから構成されている。以下、それぞれの分析ステップについて説明する。

（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。

（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。

図 2-2　リストアップした各対策が既存の業務に与える影響の分析手順

2.2.1（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。

まず最初に、リストアップした各セキュリティ対策が、既存のどのような業務に影響を与えうるかを調査し「作業項目」としての洗い出しを行う。新たなに導入するセキュリティ対策が適切に機能するためには、何らかの管理作業が発生する。例えば、USBメモリをATM制御部のUSBポートに挿入しマルウェアをインストールする対策として、AUTORUNを禁止する設定を導入することを想定する。この場合、禁止設定を変更されないよう、作業者の行動を監視するなどの新たな管理作業が「作業項目」として必要になる。また、該当「作業項目」の年間あたりの「作業頻度」の見積も必要となる。

なお、ATMの運用に関連する作業としては、例えば表 2-6のような項目が挙げられる。

表 2-6 ATM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。ATM内の現金は金庫などの物理的保護手段によって守られているので、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。また、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。 現金カセット補充回収作業では、現金カセットを用いてATMの現金を交換する場合もあれば、現金カセットを用いずに補充・回収する場合もある。日本国内においては、一般にリサイクルATMが運用されており、どの程度の頻度で警送作業が発生するかは、入金される現金量と出金される現金量のバランス状態に応じて変わるため、金融機関ごと、あるいは、支店ごとにその作業頻度が異なる。 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。具体的作業頻度については、ATMの運用実績に伴い、金融機関と警送会社の間である程度取り決められていることが多いので、平均的な作業頻度を金融機関からヒアリングする必要がある。
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。また、現金処理部へのアクセスが発生する場合には、セキュリティ上通常二人以上の作業員が一緒

	に作業を行う。 どの程度の頻度で清掃作業が必要かは、ATM の利用頻度や搬送する紙幣の枚数、および、紙幣の状態に依存する。作業頻度については、金融機関に作業実績を確認した上で見積もる必要がある。
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。 ソフトウェアの更新作業では、更新ソフトウェアを ATM にインストールする作業以外に、ソフトウェアの開発拠点における開発作業、および、金融機関のテスト拠点での開発ソフトウェアのテスト作業が発生する。さらに、それら拠点間のソフトウェア等の媒体運搬作業、インストール媒体の管理拠点から各 ATM の設置場所までの運搬作業が発生する。 ソフト配布サーバを用いてネットワークから各 ATM に配信される場合には、テスト拠点からソフト配布サーバ拠点までの運搬、あるいは、ネットワークを通じての送信作業が発生する。これらの各作業において、情報が漏えいしないように管理作業が必要となる。 作業の発生頻度については、金融機関毎に異なるので、年間どの程度の更新が期待されるかを金融機関に確認して、作業頻度を見積もる必要がある。
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は、その復旧作業が必要となる。金庫の外側、すなわち紙幣処理部の外側で障害が発生した場合は、保守員が出動して作業に当たるが、係員あるいは、警送員がまず ATM 保守扉を物理鍵によって開けて保守員が作業に当たる。 紙幣処理部内にて障害が発生した場合は、現金へのアクセスが伴うので、警送作業と同様に二人以上の作業員によるアクセス管理が必要となる。 海外に比べて日本では、ATM の障害が発生することは少ないが、障害は確率論的に発生しうるので、予め復旧作業の頻度を決めることはできない。そこで、作業頻度の期待値については、金融機関に作業実績を確認した上で、適当な前提の下に見積もる必要がある。
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。 紙幣搬送に必要なゴムローラーやベルトなどの交換作業では、現金へのアクセスが伴うことがあるので、警送作業と同様にセキュリティ上二人以上の作業員によるアクセス管理が必要となる。

	作業頻度は ATM の利用頻度や搬送紙幣の枚数、および、紙幣の状態に依存する。作業頻度については金融機関に作業実績を確認した上で見積もる必要がある。

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。

リストアップした対策により影響を受ける「作業項目」を洗い出したら、該当「作業項目」を一連の「作業ステップ」に分解し、それぞれの作業ステップに必要な管理作業を洗い出す。管理作業の洗い出しは、新しいセキュリティ要件が導入されると、既存管理作業にも影響を与えうるので、その影響度合いを見積もるために必要となる。なお、金融機関は現金などの重要資産へのアクセスを伴う運用を行っているので、セキュリティを保つために既に何らかの管理ルールの下で個々の作業を行わせていると想定されるが、それらの作業についても作業ステップへの分解と、管理作業の洗い出しを行う必要がある。

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。

本書では各対策を導入する場合に必要となる管理工数を見積もりやすくするため、「管理領域」という概念を導入する。「管理領域」は複数の「作業ステップ」をひとまとまりとして扱い可能とすることで、管理工数を見積もりやすくする。図 2-3 は、各「作業ステップ」の管理工数を分類するための「管理領域」として物理境界を利用し分類した例である。本例では「管理領域」を「(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」、「(m5)金庫扉内管理」、「(m6)監視センタ内管理」の６つに分類している。例えば、当該営業店以外の他拠点から移動し当該営業店内に設置された ATM 内部（金庫）への物理的アクセスを伴う作業においては、当該営業店以外の他拠点、他拠点から当該営業店への移動、営業店内、ATM 保守扉内、ATM 金庫扉内の順番で移動とアクセスが発生し、作業終了時には、ATM 保守扉内、営業店内、当該営業店から他拠点への移動、当該営業店以外の他拠点、と逆の移動とアクセスが発生するとともに、「管理領域」毎にレベルの異なる管理作業が必要となる。なお、ATM ブースを監視する監視カメラがある場合は、監視センタ内での監視作業も「管理領域」の１つとして追加される。

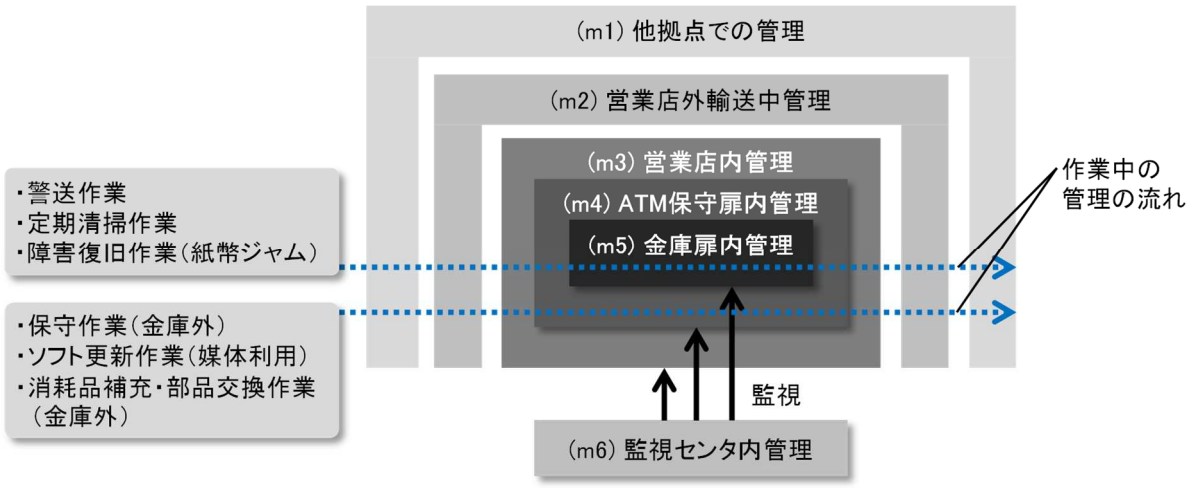


図 2-3　ATM 運用に伴う管理領域の分類例

図 2-4 は警送作業を例として、「作業ステップ」への分解、「作業ステップ」毎の管理作業の洗い出し、「管理領域」の定義及び、「作業ステップ」毎の管理作業の「管理領域」への割り当てを行ったものである。ATM 金庫内の現金にアクセスする場合は、通常、作業員が二人以上で金庫扉を開錠して作業するのが金融機関のルールになっているが、保守扉のみの開錠でよい作業においては、一人でも作業が可能といったように管理レベルに違いが生じる。このため、物理的アクセスを伴う作業においては、アクセス管理のレベルに違いが生じる物理的な境界毎に「管理領域」を分類すると管理作業をグループピングしやすく、理解もしやすい。なお、個々の作業ステップは金融機関ごとにシステムや運用ルールが異なるので、正確な作業ステップは金融機関にヒアリングして調査する必要がある。

図 2-4　警送作業の作業ステップへの分解と管理領域の分類例

また、新たなセキュリティ対策として、例えば「メディアからの ATM 起動禁止設定」と「AUTORUN 禁止設定」の２つを導入する場合、いずれも ATM 保守扉を開錠して行う作業で、管理作業内容に違いはないと考えられる。このため分類される管理領域において、両作業は「(m4)ATM 保守扉内管理」にあてはめることができ、「管理領域」単位で見積もることで、見積もり作業を簡素化できる。

なお、管理領域の分類の仕方は一通りではなく、セキュリティ対策導入に伴う管理工数を見積りやすければ、他の分類方法でも構わない。ATM に対するサイバー・フィジカル攻撃では、物理的に金庫扉を開けることなく、ATM から不正に現金を排出させるので、本ガイドラインでは「(m5) 金庫扉内管理」以外の管理作業分析を特に注力する。

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。

例えば、保守扉を開錠する物理鍵として個別鍵を導入することがセキュリティとして適切に機能するためには、個別鍵のアクセス管理が適切に行われることが大前提である。管理不備により ATM の保守扉を悪意のある者に開けられないようにするためには、**身分**

証明書などを用いて作業者の本人確認を厳密に行う、あるいは、保守扉を開錠する物理鍵を ATM 毎に個別鍵にするといった対策が必要となる。

このように、リストアップした対策がセキュリティ機能として適切に効力を発揮するためには、適切な管理作業が必要となるケースが多い。逆に言うと、適切な管理がされなければ、どのような対策を導入したとしても実効性は期待できない。そこでリストアップした対策のセキュリティ効果を最大限に発揮させるための「あるべき管理の姿」を実現するために、必要となる管理作業を洗い出しが必要**で**ある。

表 2-7 は、ATM に対する作業イベント発生時の「あるべき管理の姿」に必要な管理作業内容を、管理領域に当てはめて示したものである。例えば、ATM 保守作業を行うために、ATM 保守扉を開錠する物理鍵を持ち出す場合、物理鍵の貸出、使用、返却時に厳密な管理が求められる。あるいは、無人店舗に設置された ATM の保守作業を行う場合は、出張所への物理鍵輸送中の管理（例えば、悪意のある作業員に鍵を型取りされない対策）も新たに必要となる。本例の「あるべき管理の姿」としては、例えば、二人一組になって移動することで、互いの行動を牽制させるといった方法が考えられる。

表 2-7　作業イベント発生時の「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

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。

リストアップした対策に関する実作業を行わない場合においても、導入した時点から定常的に発生する管理作業を洗い出し、これらについても「あるべき管理の姿」を実現するための管理作業を検討する必要がある。表 2-8 は、定常的に発生する管理作業の「あるべき管理の姿」を実現するための管理作業内容を、管理領域ごとに例として示したも

のである。ATM 保守扉を開錠する物理鍵は、保守作業といった ATM 内部にアクセスする際の管理に加えて、そのような作業が発生しない時でも、24 時間 365 日、物理鍵のアクセス管理が必要となる。すなわち、悪意を持つ人物が勝手に物理鍵を持ち出したり、鍵の複製に必要な型取りをしないような管理が常時発生する。セキュリティ対策として個別鍵を導入しても、個別鍵の管理に不備があると、悪意のある攻撃を防御することはできない。従って、不備が起こらないように攻撃リスクのある管理作業は漏れなくリストアップする必要がある。

表 2-8　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 の異常動作や想定外のシャットダウンをを常時チェック ・ブース監視カメラ画像に異常がないかを定期的に目視確認

2.2.2　(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

これまでの分析で、リストアップした対策の管理作業への影響分析が完了したら、それら要件が具体的にどれくらいの管理工数を発生させるかをさらに分析する。この背景として、人間の心理を考慮しており、対策を導入するに当たり、それに伴う管理作業負担があまりにも大きすぎる場合には、手抜き作業が発生したり、必要な作業が無視されたりして、管理上の大きな脆弱性を生じうる。よって、大きな管理工数はセキュリティ上の脆弱性につながりうると考え、ここではその管理工数の大きさを具体的に見積もる。本分析ステップは、三つの分析サブステップに分かれており、以下個々のサブステップについて説明する。

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。

各作業項目が発生した場合に、一回当たりどの程度の作業工数が掛かるかを、分析ステップⅠで分析した結果を基に見積もる。例えば、ATM の保守扉を開錠する物理鍵の貸出に伴う管理作業としては、鍵貸出し時の本人確認、貸出し手続きに伴う管理台帳への記録、作業終了による鍵返却時の本人確認、管理台帳への記録等の管理作業工数が発生する。

さらに、保守作業が無くても物理鍵は 24 時間 365 日悪意を持つ人物が勝手に持ち出さないようにアクセス管理が必要である。これは定常的に発生するので、どのような管理を行うことを想定するかは、金融機関と相談して決める必要がある。一つの例として、監視カメラで物理鍵のアクセス者を常時撮影する方法が考えられる。そして、管理台帳に記録された氏名、時刻と、監視カメラで撮影された人物、時刻を突合して検証する方法がある。~~映像~~検証時には、映像を早回しで見るなど時間短縮が可能なので、例えば 1 週間分撮り溜めた映像データを 1 時間掛けて検証するといったことが考えられる。このように作業項目が発生した際に、リストアップした対策がセキュリティ機能として期待される実効性を発揮するために、どれくらいの管理工数が発生するかを適切な前提を置きながら見積もっていく必要がある。表 2-9 は、管理領域ごとに「あるべき管理の姿」の実現のために必要な管理工数を見積もる計算式を例示したものであり、1 回あたりの対応人数、対応時間、対象の営業店数等を考慮して見積もる必要があることを示している。

表 2-9　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

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-①で見積もった「作業項目」発生時の管理工数とⅠ-①で見積もった頻度の積を計算し、年間あたりどれくらいの管理工数が発生するかを見積もる。さらに、作業項目の発生とは関係なく定常的に発生する管理工数を加える。また、管理作業工数はATM設置台数、営業店舗数、あるいは、開発拠点数や媒体などの管理拠点数によっても変動するので、それらの数に応じて、管理作業工数の比例計算を行う。　例えば、警送作業は1週間に一度の頻度で行うと想定すれば、年間52回発生することになる。また、ソフトウェアの更新は、季節ごとにATMに搭載する広告コンテンツを入れ替えると想定すれば、年間4回発生することになる。定常的に発生する管理作業として、例えば、監視カメラでATMブースを撮影し、その映像データを週に一度検証するのであれば、年間52回発生することになる。

このように作業項目とその頻度の積を求めて、作業項目に渡って累積すれば、リストアップした一つの対策に関して、年間管理作業工数を見積もることができる。

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。

複数の対策をリストアップしている場合は、上記Ⅱ-①、Ⅱ-②の作業を対策毎に行う。リストアップした対策毎に管理工数を計算することに関しては、実際には管理領域といったグループ単位で一括りにして見積もる。例えば、リストアップした対策の中にBIOSパスワード設定とOS管理者パスワード設定が含まれる場合は、それらが盗まれたり、悪用されたりしないような管理作業も同時に発生する。その管理のために互いの牽制を狙って作業員が二人一組で作業を行う場合、BIOSパスワードかOS管理者パスワードのいずれか一方でも対策として導入されれば場合は、常に二人一組で作業を行わなければならない。

このように対策の一つ一つに別々の管理作業が発生するというよりは、保守扉内作業中に遵守すべき要件が一つでも盛り込まれた場合は、管理作業が必要となる。よって、リストアップした対策のそれぞれが、どの管理領域に属するかを紐付しておけば管理工数を見積もりやすくなる。

表 2-10は、「マルウェアによる不正出金」を例として、各対策とその影響範囲を大まかに把握するために「作業ステップ」への分解は行わずに、各「対策」を「管理領域」に当てはめたものである。前述と同様に赤色で下線が引かれた太文字は、対策実行に当たり運用中の管理工数が多いと思われる要件であることを示しており、これを見ると、どの管理領域への対策が管理工数が少ない対策であるかを大まかに知る事ができる。

表 2-10　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
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 (パスワード,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

なお、新規に導入する対策、例えば、ATM の保守扉開錠のための物理鍵へのアクセスを管理するための対策として、生体認証を導入するのであれば、そのアクセスログの異常有無の検証作業が、あるいは、監視カメラで物理鍵のアクセス状況を常時記録し続けるのであれば、記録された映像を目視して検証するといった管理作業が新たに発生する。これらの新たな管理作業についても分析ステップⅠ、Ⅱを行う。

2.3　対策案の比較評価

本節では、表 2-1 の（６）～（７）のステップについて説明する。

（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、表 2-11 にリスク評価方式の例を示す。よく用いられるのが CVSS 方式であり、攻撃された場合の影響度と攻撃容易性の観点からリスク値を評価する。CCDS 改良方式は CVSS 方式の複雑な手法の簡易版である。EDC 方式とはイベントツリーとディフェンスツリーを組み合わせた方法であり、ある攻撃が成功するか否かというイベントによって、その後の攻撃ステップや防御ステップが変わるので、それらイベントドリブンでの評価方式である。

ALE 法は年次損失予測と呼ばれる手法であり、リスクの値を損失金額で見積もる方式である。単一損失予測と年次発生頻度の積で年次損失予測額が計算される。あるセキュリティ対策が導入された場合に、その管理工数が大きくなりすぎるとミスや手抜きが発生して、その隙を突いた攻撃が発生すると考えられることから、管理工数は適当な変換式によりリスクの年次発生頻度に置き換えることが出来る。例えば、人の作業ミスは１％程度発生すると言われ、さらにその１％の内、本当に攻撃可能なまとまった隙のある時間ができるのがさらに１％と考えれば、管理工数（時間）の１万分の一が攻撃可能時間と読み替えることができる。この見積りは一つの例なので、金融機関の運用実態を調査した上で、適切にリスクを見積もることが求められる。

OWASP はウェブアプリケーションセキュリティをとりまく課題解決を目的としたオープンコミュニティであり、The OWASP Risk Rating Methodology(OWASP 法)は、OWASP (Open Web Application Security Project) によって開発された脆弱性評価の手法となる。金銭等の資産損失や、ブランド・信用棄損がリスクファクタに含まれる特徴がある。ファクタが多く、平均値によって総合リスクを判定するため、個別ファクタの数値にウェイトが存在しないため、全体に影響しにくいという特徴がある。

表 2-11　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) 攻撃容易性 ＝ 8.22×AV×AC×PR×UI C:機密性への影響、I:完全性への影響、A:可用性への影響 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)

上記ではリスク評価方式により、リストアップした対策の導入効果を見てきたが、導入効果は、導入に伴う管理工数の大小でも比較できると考えられる。管理工数が大きすぎると、ミスを伴ったり、手抜き作業が発生したり、最悪の場合無視されたりして、実効性が伴わなくなる。よって、管理工数が小さい対策ほどリスクが小さく、対策効果が高いと期待することができる。

(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、管理作業工数を算出できたので、これらを比較して、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ことができる。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。

前述の「表 2-10 対策(EUROPOL 要件)と関わる管理領域の例」では、「マルウェアによる不正出金」を例として、各対策（ガイドライン要件）がどの管理領域に属するかを纏めたが、以下の表 2-12 は、各管理領域にいずれの対策（ガイドライン要件）が属するの観点から纏め直したものである。既に管理領域毎に年間発生する管理工数が見積もられているので、その管理工数同士を比較することで、どの攻撃ステップを重点的に守ることが最も効率的で効果的かを見積もることができる。なお、表 2-12 で「(3)マルウェア起動」を突破された場合は、「(4)出金操作」の対策として「⑭現金補充額/周期の最適化」で防止するしかない。この対策は、監視業務として小まめに現金残高を確認することを要求しており、本当に不正出金をこの段階で防止しようとすれば、例えば 1 時間おきに現金残高を確認するなど非現実的な対策になりえて、欧州警察機構ガイドラインの要件はあまり効果的でないことが分かる。よって、管理工数を用いた要件の比較評価を行うことで、限られたリソースと予算で適切なセキュリティ対策を策定することが可能になる。

表 2-12　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 (パスワード,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

2.4　未出現犯罪に対する適用拡張

本節では、表 2-1 の（８）のステップについて説明する。

（8）　未出現の犯罪に対し、上記分析を通じて対策を汎用適用

未出現の犯罪に対しても、攻撃ステップの分解とそれらを阻止するためのセキュリティ対策要件に対する管理工数を、上記（１）～（７）の手順で見積もることができる。すなわち、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。

そして、（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）を分析して、（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。

上記において、「（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」とあるが、闇雲に未知の攻撃を想定するのではなく、なるべく対策効果を上げるために、次に犯罪者が行いやすい攻撃が何であるかを考えることが重要である。１章において、「犯罪者集団にとってもリスク対リターンの大きさが重要と思われる。」と書いたように、仮に既知の攻撃が完全に防御された場合に、次にリスクが少なくてリターンが大きそうな守るべき保護対象が何であるかを検討する。そして、その守るべき保護対象を攻撃する際に、犯罪者にとって投資や攻撃の工数、発覚したり捕まるリスクが最も少ない攻撃方法は何であるかを考える。すなわち、攻撃者側になったつもりで、何をどのように攻撃してくるかを考えることが重要である。

このように、本ガイドラインのフレームワークを用いれば、未出現の犯罪に対する具体的な対策の策定と効果を見積ることが可能になる。

3 まとめ

本書は ATM のセキュリティ対策を検討するにあたり、運用中の厳密管理で資産を守るべきか、あるいは、コンシューマ機器と同様に暗号などの仕組みによって守るべきかの検討指針を提供した。

一方、既存のセキュリティガイドラインでは、推奨されたセキュリティ対策が有効に機能するためには、多大な管理工数が必要になるにも関わらず、それが明示されていない。そのため、実効性の乏しい対策が金融機関に意識されずに導入されてリスク低減につながらない懸案を抱えている。本書~~で~~は、そのような懸案を回避するため、対策導入に伴う管理工数を定量的に見積もり、対策の実効性を定量的に評価するめの一つの施策を示すものである。

また、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。

付録 リスク評価式

付録1 CVSS(Common Vulnerability Scoring System) v3 方式 0

共通脆弱性評価システム CVSS （ Common Vulnerability Scoring System）は、情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法を提供している。CVSS では 3 つの基準、(1)基本評価基準(Base Metrics)、(2)現状評価基準(Temporal Metrics)、(3)環境評価基準(Environmental Metrics)で脆弱性を評価する。それぞれの評価基準は脆弱性の深刻度を示す 0.0(低)～10.0(高)の数値で表現される。

なお、CVSS が v2 から v3 にバージョンアップされる過程で、①コンポーネント単位で評価する手法の採用、②脆弱性の影響範囲拡大を加味するためスコープという評価項目の導入、③基本評価基準の細分化、④環境評価基準のアプローチの変更、が導入された。詳細は参考文献を参照のこと。

1.1 基本評価基準（Base Metrics）

脆弱性そのものの特性を評価する基準である。情報システムに求められる 3 つのセキュリティ特性、「機密性（ Confidentiality Impact ）」、「完全性(Integrity Impact ）」、「可用性(Availability Impact ）」に対する影響を、ネットワークから攻撃可能かどうかといった基準で評価し、CVSS 基本値(Base Score)を算出する。この基準による評価結果は固定していて、時間の経過や利用環境の異なりによって変化しない。ベンダーや脆弱性を公表する組織などが、脆弱性の固有の深刻度を表すために評価する基準である。CVSS 基本値(Base Score)は以下の式で与えられる。

(1)影響度

調整前影響度 ＝ 1－(1－C)×(1－I)×(1－A)　…式(1)

影響度(スコープ変更なし) ＝ 6.42×調整前影響度　…式(2)

影響度(スコープ変更あり) ＝ 7.52×(調整前影響度－0.029)
－3.25×(調整前影響度－0.02)^{15}　…式(3)

(2)攻撃容易性

攻撃容易性 ＝ 8.22×AV×AC×PR×UI　…式(4)

(3)基本値

影響度がゼロ以下の場合、　基本値 ＝ 0　…式(5)

影響度がゼロよりも大きい場合、

スコープ変更なし：基本値 ＝ RoundUp1(min [(影響度＋攻撃容易性), 10])
(小数点第 1 位切り上げ) …式(6)

スコープ変更あり：基本値 ＝ RoundUp1(min [(1.08×(影響度＋攻撃容易性)), 10])
(小数点第 1 位切り上げ) …式(7)

上記 C、I、A、AV、AC、PR、UI はそれぞれ表 a1‐1、表 a1‐2 で定義される。

表 a1 － 1 影響度計算に必要な評価基準

評価項目	評価結果	内 容	値
機密性への影響 (情報漏えいの可能性、C: Confidentiality Impact)	高(H)	機密情報や重要なシステムファイルが参照可能であり、その問題による影響が全体に及ぶ。	0.56
	低(L)	情報漏えいやアクセス制限の回避などが発生はするが、その問題による影響が限定的である。	0.22
	なし(N)	機密性への影響はない。	0.00
完全性への影響 (情報改ざんの可能性、I：Integrity Impact)	高(H)	機密情報や重要なシステムファイルの改ざんが可能で、その問題による影響が全体に及ぶ。	0.56
	低(L)	情報の改ざんが可能ではあるが、機密情報や重要なシステムファイルの改ざんはできないために、その問題による影響が限定的である。	0.22
	なし(N)	完全性への影響はない。	0.00
可用性への影響 (業務停止の可能性、A:Availability Impact)	高(H)	リソース(ネットワーク帯域、プロセッサ処理、ディスクスペースなど)を完全に枯渇させたり、完全に停止させることが可能である。	0.56
	低(L)	リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能である。	0.22
	なし(N)	可用性への影響はない。	0.00

表 a1 － 2 攻撃容易性計算に必要な評価基準

評価項目	評価結果	内 容	値
攻撃元区分 (AV：Access Vector)	ネットワーク(N)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。 例えば、インターネットからの攻撃など	0.85
	隣接(A)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。 例えば、ローカル IP サブネット、ブルートゥース、IEEE 802.11 など。	0.62
	ローカル(L)	対象コンポーネントをローカル環境から攻撃する必要がある。 例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など。	0.55
	物理(P)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。	0.20

		例えば、IEEE 1394、USB 経由で攻撃が必要など。	
攻撃条件の複雑さ (AC：Attack Complexity)	低(L)	特別な攻撃条件を必要とせず、対象コンポーネントを常に攻撃可能である。	**0.77**
	高(H)	攻撃者以外に依存する攻撃条件が存在する。例えば、次のいずれかの条件に合致する場合などが該当する。 攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。 攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。 攻撃者は、中間者攻撃のため環境が必要となる。	**0.44**
必要な特権レベル (PR：Privileges Required)	不要(N)	特別な権限を有する必要はない。	**0.85** **(0.68)※**
	低(L)	コンポーネントに対する基本的な権限を有していれば良い。 例えば、秘密情報以外にアクセスできるなど。	**0.62** **(0.50)※**
	高(H)	コンポーネントに対する管理者権限相当を有する必要がある。 例えば、秘密情報にアクセスできるなど。	**0.27**
ユーザ関与レベル (UI：User Interaction)	不要(N)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。	**0.85**
	要(R)	リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。	**0.62**
スコープ(S：Scope)	変更なし(U)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープに留まる。	-
	変更あり(C)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープ以外にも広がる可能性がある。 例えば、クロスサイトスクリプティング、リフレクター攻撃に悪用される可能性のある脆弱性など	-

※「スコープ変更あり」の場合の値である。

1.2 現状評価基準（Temporal Metrics）

脆弱性の現在の深刻度を評価する基準である。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値(Temporal Score)を算出する。この基準による評価結果は、脆弱性への対応状況に応じ、時間が経過すると変化する。ベンダーや脆弱性を公表する組織などが、脆弱性の現状を表すために評価する基準である。CVSS 現状値（Temporal Score)は以下の式で与えられる。

現状値 ＝ RoundUp1(基本値×E×RL×RC) …式(8)

(小数点第 1 位切り上げ)

上記 E、RL、RC は表 a1 - 3 で定義される。

表 a1 - 3 現状値計算に必要な評価基準

評価項目	評価結果	内 容	値
攻撃される可能性 (E：Exploit Code Maturity)	未評価(X)	この項目を評価しない。	1.00
	容易に攻撃可能(H)	攻撃コードがいかなる状況でも利用可能である。 攻撃コードを必要とせず、攻撃可能である。	1.00
	攻撃可能(F)	攻撃コードが存在し、ほとんどの状況で使用可能である。	0.97
	実証可能(POC)	実証コードが存在している。 完成度の低い攻撃コードが存在している。	0.94
	未実証(U)	実証コードや攻撃コードが利用可能でない。 攻撃手法が理論上のみで存在している。	0.91
利用可能な対策のレベル (RL：Remediation Level)	未評価(X)	この項目を評価しない。	1.00
	なし(U)	利用可能な対策がない。 対策を適用できない。	1.00
	非公式(W)	製品開発者以外からの非公式な対策が利用可能である。	0.97
	暫定(T)	製品開発者からの暫定対策が利用可能である。	0.96
	正式(O)	製品開発者からの正式対策が利用可能である。	0.95
脆弱性情報の信頼性 (RC：Report Confidence)	未評価(X)	この項目を評価しない。	1.00
	確認済(C)	製品開発者が脆弱性情報を確認している。 ソースコードレベルで脆弱性の存在を確認されている。脆弱性情報が実証コードや攻撃コードなどにより広範囲に確認されている。	1.00
	未確証(R)	セキュリティベンダーや調査団体から、複数の非公式情報が存在している。 ソースコードレベルで脆弱性の存在が確認できていない。脆弱性の原因や検証が十分ではない。	0.96
	未確認(U)	未確認の情報のみ存在している。 いくつかの相反する情報が存在している。	0.92

1.3 環境評価基準（Environmental Metrics）

製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準である。攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価し、 CVSS 環境値（Environmental Score）を算出する。この基準による評価結果は、脆弱性に対して想定される脅威に応じ、製品利用者毎に変化する。製品利用者が脆弱性への対応を決めるために評価する基準である。CVSS 環境値（Environmental Score）は以下の式で与えられる。

(1)緩和策後影響度

緩和策後調整前影響度 ＝ min [(1－(1－MC×CR)×(1－MI×IR)×(1－MA×AR)), 0.915] …式(9)

緩和策後影響度(スコープ変更なし)＝ 6.42×緩和策後調整前影響度 …式(10)

緩和策後影響度(スコープ変更あり)＝ 7.52×(緩和策後調整前影響度－0.029) －3.25×(緩和策後調整前影響度－0.02)^{15} …式(11)

(2)緩和策後攻撃容易性

緩和策後攻撃容易性 ＝ 8.22×MAV×MAC×MPR×MUI …式(12)

(3)環境値

緩和策後影響度がゼロ以下の場合、 環境値 ＝ 0 …式(13)

緩和策後影響度がゼロよりも大きい場合、

スコープ変更なし：

緩和策後基本値 ＝ RoundUp1(min [(緩和策後影響度＋緩和策後攻撃容易性), 10])

環境値 ＝RoundUp1(緩和策後基本値×E×RL×RC) …式(14)

(小数点第 1 位切り上げ)

スコープ変更あり：

緩和策後基本値 ＝ RoundUp1(min [(1.08×(緩和策後影響度＋緩和策後攻撃容易性)), 10])

環境値 ＝ RoundUp1(緩和策後基本値×E×RL×RC) …式(15)

(小数点第 1 位切り上げ)

上記式(9)の CR、IR、AR は表 a1 - 4 で、MC、MI、MA は表 a1 - 5 で、式(12)の MAV、MAC、MPR、MUI は表 a1 - 6 で、式(14) 、式(15)の E、RL、RC は表 a1 - 3 で、それ

ぞれ定義される。

表 a1 － 4　対象システムのセキュリティ要求度(CR、IR、AR：Security Requirements)

評価項目	評価結果	内　容	値
機密性の要求度 (CR: Confidentiality Requirement)	未評価(X)	この項目を評価しない。	1.0
	高(H)	該当項目を失われると、壊滅的な影響がある。	1.5
	中(M)	該当項目を失われると、深刻な影響がある。	1.0
	低(L)	該当項目を失われても、一部の影響にとどまる。	0.5
完全性の要求度 (IR: Integrity Requirement)	未評価(X)	この項目を評価しない。	1.0
	高(H)	該当項目を失われると、壊滅的な影響がある。	1.5
	中(M)	該当項目を失われると、深刻な影響がある。	1.0
	低(L)	該当項目を失われても、一部の影響にとどまる。	0.5
可用性の要求度 (AR :Availability Requirement)	未評価(X)	この項目を評価しない。	1.0
	高(H)	該当項目を失われると、壊滅的な影響がある。	1.5
	中(M)	該当項目を失われると、深刻な影響がある。	1.0
	低(L)	該当項目を失われても、一部の影響にとどまる。	0.5

表 a1 － 5　環境条件を加味した基本評価の再評価(Modified Base Metrics)その１

評価項目	評価結果	内　容	値
緩和策後の機密性への影響 (MC:Modified Confidentiality Impact)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	高(H)	機密情報や重要なシステムファイルが参照可能であり、その問題による影響が全体に及ぶ。	0.56
	低(L)	情報漏えいやアクセス制限の回避などが発生はするが、その問題による影響が限定的である。	0.22
	なし(N)	機密性への影響はない。	0.00
緩和策後の完全性への影響 (MI:Modified Integrity Impact)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	高(H)	機密情報や重要なシステムファイルの改ざんが可能で、その問題による影響が全体に及ぶ。	0.56
	低(L)	情報の改ざんが可能ではあるが、機密情報や重要なシステムファイルの改ざんはできないために、その問題による影響が限定的である。	0.22
	なし(N)	完全性への影響はない。	0.00
緩和策後の可用性への影響	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	高(H)	リソース(ネットワーク帯域、プロセッサ処理、ディスクスペースなど)を完全に枯渇させ	0.56

(MA:Modified Availability Impact)		たり、完全に停止させることが可能である。	
	低(L)	リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能である。	**0.22**
	なし(N)	可用性への影響はない。	**0.00**

表 a1 - 6 環境条件を加味した基本評価の再評価(Modified Base Metrics)その２

評価項目	評価結果	内 容	値
緩和策後の攻撃元区分 (MAV：Modified Attack Vector)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	ネットワーク(N)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。 例えば、インターネットからの攻撃など	**0.85**
	隣接(A)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。 例えば、ローカル IP サブネット、ブルートゥース、IEEE 802.11 など。	**0.62**
	ローカル(L)	対象コンポーネントをローカル環境から攻撃する必要がある。 例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など。	**0.55**
	物理(P)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。 例えば、IEEE 1394、USB 経由で攻撃が必要など。	**0.20**
緩和策後の攻撃条件の複雑さ (MAC：Modified Attack Complexity)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	低(L)	特別な攻撃条件を必要とせず、対象コンポーネントを常に攻撃可能である。	**0.77**
	高(H)	攻撃者以外に依存する攻撃条件が存在する。 例えば、次のいずれかの条件に合致する場合などが該当する。 攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。 攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。 攻撃者は、中間者攻撃のため環境が必要となる。	**0.44**
緩和策後の必要な特権レベル (MPR：Modified Privileges Required)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	不要(N)	特別な権限を有する必要はない。	**0.85** **(0.68)※**
	低(L)	コンポーネントに対する基本的な権限を有していれば良い。 例えば、秘密情報以外にアクセスできるなど。	**0.62** **(0.50)※**
	高(H)	コンポーネントに対する管理者権限相当を有する必要がある。 例えば、秘密情報にアクセスできるなど。	**0.27**

緩和策後のユーザ関与レベル (MUI：Modified User Interaction)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	不要(N)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。	**0.85**
	要(R)	リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。	**0.62**
緩和策後のスコープ (MS：Modified Scope)	未評価(X)	未評価を選択した場合には、基本評価基準での評価結果を参照する。	-
	変更なし(U)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープに留まる。	-
	変更あり(C)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープ以外にも広がる可能性がある。 例えば、クロスサイトスクリプティング、リフレクター攻撃に悪用される可能性のある脆弱性など	-

1.4 深刻度レベル分け

CVSS では、(1)基本評価基準(Base Metrics)、(2)現状評価基準(Temporal Metrics)、(3)環境評価基準(Environmental Metrics)を順番に評価して、脆弱性の深刻度を 0(低)～10.0(高)の数値で表す。そして、その評価された数値に対して、CVSS v3 では、深刻度レベル分けを次のように設定している。

表 a1 － 7　深刻度レベル分け

深刻度	スコア
緊 急	9.0～10.0
重 要	7.0～8.9
警 告	4.0～6.9
注 意	0.1～3.9
無	0.0

付録 2 CCDS 改良方式 0

CCDS 改良方式は、CCDS の観点で CVSS 方式を簡略化したリスク評価式である。リスク値算出方法は以下の式で与えられる。

リスク値 ＝（難易度 + 影響度）× 攻撃者のモチベーション　…式(16)

難易度、影響度、攻撃者のモチベーションの基準は、それぞれ、表 a2‐1 から表 a2‐3 で定義される。また、式 1 で計算されたリスク値に対するランクは表 a2‐4 で示される。CCDS の経験では、CVSS 方式によるリスク値と CCDS 改良方式によるリスク値の間には大きな差異が出ないことが分かっており、リスク値を簡便に評価するために役立つ評価式である。

表 a2 – 1 難易度基準

ランク	判定基準	値
S	複数の条件（認証、特別な権限など）が必要。かつ、ローカル環境からのみ接続（攻撃）が可能。	1
A	単一の条件（認証、特別な権限など）が必要。かつ、ローカル環境からのみ接続（攻撃）が可能。	3
B	一つ以上の条件（認証、特別な権限など）が必要。もしくは、ローカル環境からのみ接続（攻撃）が可能。	5
C	攻撃するための条件が不要。かつ、無線ネットワークからの接続（攻撃）が可能。	10

表 a2 – 2 影響度基準

ランク	判定基準	値
軽微	攻撃を受けてもユーザに影響がない、もしくは軽微な表示異常しか発生しない。かつ、漏えいする情報も個人を特定できるような情報は漏洩しない。	1
中程度	攻撃を受けた場合に、ユーザに不利益をもたらす。 もしくは、漏えいした情報から個人が特定される。	3
重大	攻撃を受けた場合に、ユーザに不利益をもたらし、二次的被害も発生。 もしくは、漏えいした情報から複数の個人が特定される。	5
壊滅的	攻撃を受けた場合に、人命に関わるような被害や二次的被害が発生する。	10

表 a2 – 3 攻撃者のモチベーション基準

ランク	判定基準	値
小	偶発的に発生し攻撃者には何の意図もない。	1
中	実験や気晴らし、自己顕示などの目的を持つ。	1.25
大	金銭的な利益を得たり、安全保障に影響を与えるなどの具体的な強い目的を持つ。	1.5

表 a2 － 4 リスク値ランク基準

ランク	リスク値
Must	17～30(最大値)
High	12～16.9
Middle	8～11.9
Low	0～7.9

付録 3 Event tree and Defense tree combined method (EDC)方式 0

“Event tree and Defense tree combined method”(EDC)方式は、石井亮平等が JSSM(日本セキュリティマネジメント学会) で発表した方式である。システムに対する攻撃者は、ある攻撃手法がうまく行ったら、その次の攻撃を行い、うまく行かなかったら別の手段を講じるといった､攻撃の時系列事象に合わせて攻撃手法を変えてくることが多い｡そこで、最終目的を達成するために、時系列に実行される事象をイベントツリーとして列挙し、各時系列事象の発生確率と影響度からリスク値を見積もると共に、各時系列事象の発生を軽減させる対策の立案とその効果を評価する手法として EDC 方式が考案された。EDC 方式の概要は以下の通りである。

（1）時系列イベントの抽出と影響度の記述

例えば、マルウェアによる不正出金を行う場合、最終目的である不正出金を行うためには、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（出し子がカードではなく携帯電話を使いチャレンジレスポンスで出金許可をもらうこともあるため）出金操作を行う必要がある。このように時系列イベントを抽出し、イベントツリーとして記述すると共に、各事象が発生した場合の影響度も記述する。影響度は、被害金額や業務／事業への影響度合いを加味して適切に設定する必要がある。

（2）時系列イベント毎の発生確率の算出と対策の記述

次に抽出した時系列イベントのそれぞれを頂上事象として、それぞれに対してディフェンスツリー分析を行う。ディフェンスツリー分析とは、頂上事象を発生させる可能性のある事象を下位に向かって列挙し結んでいくことでフォールトツリー（Fault Tree）を作成し、それぞれの事象の発生確率から、頂上事象の発生確率を算出する。また、下位事象に対しては該当事象の発生を抑える対策と、その効果（低減率）を併記し、対策の有効性を明確化する手法である。

（3）合計リスク値の算出

各時系列事象の発生確率と影響度の積（各事象のリスク）を求めたのち、それぞれの値を積算し、総和を求めることで、合計リスク値を算出する。

図 a3-1 は、マルウェアによる不正出金を例に、合計リスクの算出方法を示したものである。

攻撃時系列事象	初期事象（マルウェア開発）	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	⑤攻撃成功
攻撃成功確率	P0(＝1)	P1	P2	P3	P4	P1×P2×P3×P4
攻撃失敗確率	(1－P0) (＝0)	1－P1	1－P2	1－P3	1－P4	-
その時系列事象で攻撃失敗時の被害の影響の大きさ(※)	―	M1	M2	M3	M4	M5
時系列事象毎のリスク値	―	(1－P1) ×M1	P1 ×(1－P2) ×M2	P1×P2 ×(1－P3) ×M3	P1×P2 ×P3 ×(1－P4) ×M4	P1×P2 ×P3×P4 ×M5
合計リスク値	(1－P1)×M1＋P1×(1－P2)×M2＋P1×P2×(1－P3)×M3 ＋P1×P2×P3×(1－P4)×M4＋P1×P2×P3×P4×M5					

図 a3 - 1 EDC 方式のリスク値計算体系

付録 4 Annualized Loss Expectancy (ALE、年次損失予測)法 0000

年次損失予測、あるいは、Annual Loss Expectation（以下 ALE）と呼ばれるリスク定量化の手法が挙げられる。他のリスク評価手法が、具体的な損失金額ではなく、レベル分けといったむしろ定性的な評価に近いのに対し、ALE 法では、リスク値を年間予想損失額として具体的な金額で表現できるのが特徴である。

年次損失予測(ALE) ＝ 単一損失予測(SLE) × 年次発生頻度(ARO) …式(18)

SLE: Single Loss Expectancy、 ARO: Annualized Rate of Occurrence

ここで、単一損失予測(SLE)とは、イベントが 1 回起きた時に発生しうる期待損失額であり、資産価値(AV)×顕在化(EV)で求められる。実質的な損失だけではなく，それに関連して発生する損失、一次対応、再発防止費用なども検討する必要がある。年次発生頻度(ARO)とは、年間を通じて予想されるイベントの数である。

単一損失予測(SLE) ＝ 資産価値(AV)×顕在化(EV)とも表現できるので、以下のように書き換えることも可能である。

年次損失予測(ALE) ＝ 資産価値(AV)×顕在化(EV)×年次発生頻度(ARO) …式(19)

付録 5 The OWASP Risk Rating Methodology 00

OWASP はウェブアプリケーションセキュリティをとりまく課題解決を目的としたオープンコミュニティであり、The OWASP Risk Rating Methodology は OWASP（Open Web Application Security Project）によって開発された脆弱性評価の手法となる。金銭等の資産損失や、ブランド・信用棄損がリスクファクタに含まれる特徴がある。ファクタが多く、平均値によって総合リスクを判定するため、個別ファクタの数値にウェイトが存在しないため、全体に影響しにくい。リスク値は式(20)の標準的なモデルからスタートしている。

Risk(リスク) ＝ Likelihood (発生可能性) × Impact (影響度) …式(20)

Likelihood (発生可能性) と Impact (影響度)のそれぞれのリスク値は次式で与えられる。

Likelihood (発生可能性) ＝ { Thread Agent (脅威の度合い)
＋ Vulnerability (脆弱性の度合い) } ÷ 2 …式(21)

Impact (影響度) ＝ { Technical Impact (技術への影響度)
＋ Business Impact (ビジネスへの影響度) } ÷ 2 …式(22)

Thread Agent (脅威の度合い)、Vulnerability (脆弱性の度合い)、Technical Impact (技術への影響度)、Business Impact (ビジネスへの影響度)の計算式はそれぞれ以下の式で与えられる。

Thread Agent (脅威の度合い) ＝ { Skill level (技術水準) ＋ Motive (動機)
＋Opportunity (機会) ＋ Size (影響範囲) } ÷ 4
…式(23)

Vulnerability (脆弱性の度合い) ＝ { Ease of discovery (発見のしやすさ)
＋Ease of exploit (攻撃容易性)
＋Awareness (既知の脆弱性かどうか)
＋Intrusion detection (侵入検知) }
÷ 4 …式(24)

Technical Impact (技術への影響度) ＝ { Loss of confidentiality (機密性の喪失)
＋Loss of integrity (完全性の喪失)
＋Loss of availability (可用性の喪失)
＋Loss of accountability (説明責任の喪失) }
÷ 4 …式(25)

Business Impact (ビジネスへの影響度) ＝ { Financial damage (資産損失) +
＋Reputation damage (ブランド失墜)
＋Non-compliance(法令違反)
＋Privacy violation (プライバシー侵害) }
÷４　…式(26)

式(23)～式(26)の右辺に含まれる項目は、それぞれ表 a5 - 1 から表 a5 - 4 で定義される。

表 a5 - 1 Thread Agent Factors (脅威の要因)

脅威の要因	評価結果	値
Skill level (技術水準)	No technical skills (技術スキル不要)	1
	Some technical skills (ある程度の技術スキル必要)	3
	Advanced computer user (コンピュータ高度利用者)	5
	Network and programming skills (ネットワークとプログラミングスキル必要)	6
	Security penetration skills (セキュリティ侵入テストスキル必要)	9
Motive (動機)	Low or no reward (低い、あるいは、無報酬)	1
	Possible reward (見込みのある報酬)	4
	High reward (高い報酬)	9
Opportunity (機会)	Full access or expensive resources required (フルアクセスまたは高価なリソースが必要)	0
	Special access or resources required (特別アクセス権かリソースが必要)	4
	Some access or resources required (多少のアクセス権かリソースが必要)	7
	No access or resources required (アクセス権リソース不要)	9
Size (影響範囲)	Developers, system administrators (開発者、システム管理者)	2
	Intranet users (イントラネット利用者)	4
	Partners (パートナ)	5
	Authenticated users (認証された利用者)	6
	Anonymous Internet users (不特定のインターネット利用者)	9

表 a5 - 2 Vulnerability Factors（脆弱性の要因）

脅威の要因	評価結果	値
Ease of discovery (発見のしやすさ)	Practically impossible (実質的に不可能)	1
	Difficult (困難)	3
	Easy (容易)	7
	Automated tools available (自動ツール利用可)	9
Ease of exploit (攻撃容易性)	Theoretical (理論的に可能)	1
	Difficult (困難)	3
	Easy (容易)	5
	Automated tools available (自動ツール利用可)	9
Awareness (既知の脆弱性かどうか)	Unknown (未知の状態)	1
	Hidden (秘密の状態)	4
	Obvious (明白な状態)	6
	Public knowledge (公開知見)	9
Intrusion detection (侵入検知)	Active detection in application (アプリで能動検知)	1
	Logged and reviewed (ログが取られて検査有)	3
	Logged without review (ログが取られるが検査無)	8
	Not logged (ログ保存無)	9

表 a5 - 3 Technical Impact Factors（テクニカルインパクト）

脅威の要因	評価結果	値
Loss of confidentiality (機密性の喪失)	Minimal non-sensitive data disclosed (最小限の機微でないデータ暴露)	2
	Minimal critical data disclosed, extensive non-sensitive data disclosed (最小限の重要データ暴露、 広範囲の機微でないデータ暴露)	4
	Extensive critical data disclosed	5

	(広範囲の重要データ暴露)	
	All data disclosed (全データ暴露)	9
Loss of integrity (完全性の喪失)	Minimal slightly corrupt data (最小限のわずかなデータ破壊)	1
	Minimal seriously corrupt data (最小限の深刻なデータ破壊)	3
	Extensive slightly corrupt data (広範囲のわずかなデータ破壊)	5
	Extensive seriously corrupt data (広範囲の深刻なデータ破壊)	7
	All data totally corrupt (全データの完全な破壊)	9
Loss of availability (可用性の喪失)	Minimal secondary services interrupted (最小限の二次サービスの中断))	1
	Minimal primary services interrupted, extensive secondary services interrupted (最小限の主要サービス中断、 広範囲の二次サービスの中断)	5
	Extensive primary services interrupted (広範囲の主要サービスの中断)	7
	All services completely lost (全サービスの完全喪失)	9
Loss of accountability (説明責任の喪失)	Fully traceable (完全トレース可能)	1
	Possibly traceable (トレース可能な見込み)	7
	Completely anonymous (完全不特定)	9

表 a5 - 4 Business Impact Factors (ビジネスへの影響度)

脅威の要因	評価結果	値
Financial damage (資産損失)	Less than the cost to fix the vulnerability (脆弱性対策コストより低い)	1
	Minor effect on annual profit (年間利益への小規模な影響	3
	Significant effect on annual profit (年間利益への深刻な影響)	7
	Bankruptcy (倒産)	9
Reputation damage (ブランド失墜)	Minimal damage (最小限の被害)	1
	Loss of major accounts (得意先の喪失)	4
	Loss of goodwill	5

	(信用喪失)	
	Brand damage (ブランド損害)	9
Non-compliance (法令違反)	Minor violation (小規模な違反)	2
	Clear violation (明確な違反)	5
	High profile violation (目立った違反)	7
Privacy violation (プライバシー侵害)	One individual (一個人)	3
	Hundreds of people (数百人)	5
	Thousands of people (数千人)	7
	Millions of people (数百万人)	9

Likelihood (発生可能性)と Impact (影響度)のリスク階級は、次の表で求められる。

表 a5 – 5 リスクレベル

Risk (リスク値)	0≦リスク値＜3	3≦リスク値＜6	6≦リスク値＜9	MAX:9
Rank (レベル)	LOW	MEDIUM	HIGH	

全体的なリスク重大性は、次の表で求められる。

表 a5 – 6 全体的なリスク重大性

Overall Risk Severity (全体的なリスク重大性)				
Impact (影響レベル)	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood (発生可能性レベル)			

付録 6 ATM 内部に対す対策る物理的侵入を伴うマルウェア攻撃の流れとその対策に関する分析

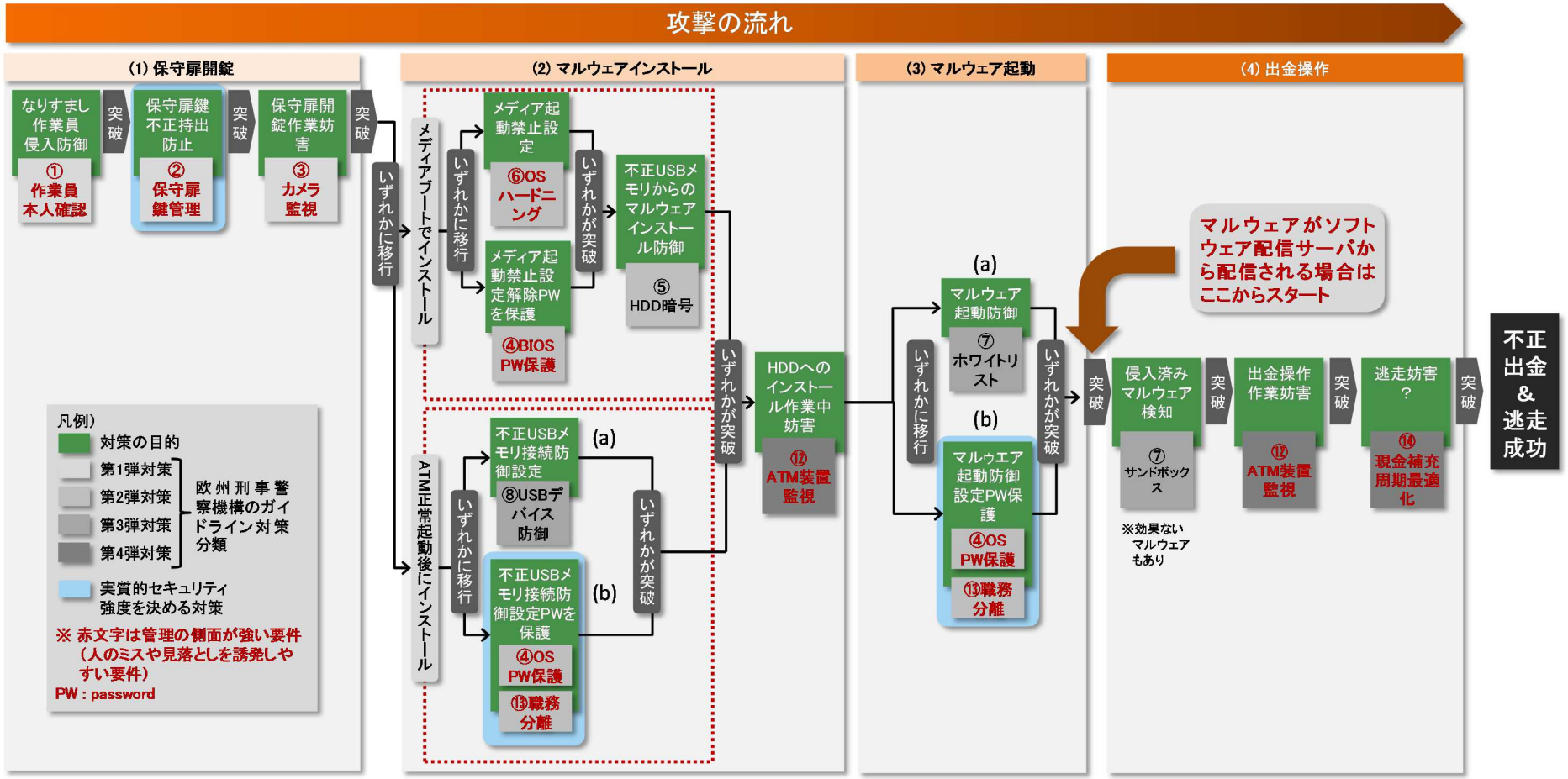


図 a6- 1 欧州刑事警察機構の ATM への論理攻撃に関する手口と推奨策に対する多層防御の流れと分析

表 a6- 1　図 a6- 1 における色分けの意味

色分け分類	分類内容
緑色四角	各対策の目的を示す。
グレー四角	「欧州刑事警察機構の ATM への論理攻撃に関する手口と推奨策」に記載されている対策項目である。対策項目は第 1 弾対策から第 4 弾対策まで複数の段階に分類されており、分類毎にグレーの色合いを変えている。後述の表 a6- 2 に詳細内容が記載されている。
赤色太文字	管理の側面が強い対策項目（人のミスや見落としを誘発しやすい対策）。
水色丸四角	４つの攻撃ステップにおいて、その攻撃ステップに対する実質的な対策強度を左右する対策項目。

図 a6- 1 は「欧州刑事警察機構の ATM への論理攻撃に関する指導要領と勧告書」[2]に掲載されている論理攻撃やマルウェア攻撃に対する防御策を、CCDS にて独自に分析し攻撃フローと対応策の流れとして示したものである。ここでのマルウェア攻撃は ATM に物理的にアクセスして ATM の保守扉を開けるなどし、その後、マルウェアを ATM 内制御部にインストールして、ATM から不正出金を行う攻撃を想定している。具体的には、(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) 出金操作の４つの攻撃ステップに対して、それぞれの攻撃ステップを対策するために、「欧州刑事警察機構の ATM への論理攻撃に関する手口と推奨策」に記載されている対策項目を、どのような順番と流れで適用すべきかを分析したものである。なお、本図の色分けの意味は表 a6- 1 に示す。

各攻撃ステップに対する分析結果を説明と以下の通りである。「(1) 保守扉開錠」の「①作業員本人確認」においては、攻撃者としてなりすまし作業員が ATM にアクセスするのを防御するために、本人確認と作業権限を確認する手順が必要であることを示している。仮にその手順をすり抜けることが成功した場合、「②保守扉鍵管理」で対策することになる。ATM の PC（制御部）が内蔵されている装置の上部筐体（ボックス）にアクセスするためには、ATM 保守扉を開錠するための物理鍵が必要であり、保守扉開錠を侵入警報装置により検知するか、該当物理鍵はデフォルトのマスターキーではなく、ATM 毎の個別物理鍵とすべきことを示している。

この対策で ATM への攻撃を効果的に対策するためには、さらに個々の物理鍵に対する厳密なアクセス管理も必要である。すなわち、ATM 毎の個別物理鍵が誰によってアクセスされたか、あるいは、勝手に複製されたりしていないかを 24 時間 365 日厳密に管理して初めて、この対策が有効なものとなる。ATM にアクセスする必要が無い時にも物理鍵のアクセス管理が必要となるので、これは非常に重い運用となる。逆に物理鍵に対するアクセスが厳格に管理されていれば、攻撃者はそれ以上のステップに進めなくなる。それゆえ、本ステップでは、「②保守扉鍵管理」を、実質的対策強度を左右する対策として位置づけた。な

お、本項目の突破が成功すると「③カメラ監視」で攻撃を対策することになる。ただし、カメラ監視はどちらかというと画像記録による証跡と抑止効果を期待するものであり、積極的に攻撃を防御することは期待できない。

上記３つの対策項目全ての突破に成功すると、ATM 保守扉が開けられて ATM の制御部にアクセスできる状態になるので、「(2) マルウェアインストール」の攻撃ステップに移行する。攻撃としては２通りのやり方が考えられ、いずれかを成功させればよい。

一つ目は、「メディアブートでインストール」である。OS とマルウェアがインストールされた USB メモリか、あるいは、光学メディアなどを ATM 制御部にセットして、メディアから別 OS を立ち上げて、制御部内のハードディスク(HDD)にマルウェアをインストールする方法である。対策として、メディアからの起動を禁止するための「④BIOS 設定」を行うが、パスワード(PW)が漏えいすると、メディア起動禁止設定が解除されてしまうので、「④BIOS PW 保護」が必要となる。一般に、BIOS のコードを解析して BIOS の設定を変更するよりも、BIOS パスワードを何らかの形で入手して設定変更する方がはるかに簡単であめ、攻撃者は後者の方法を選択することが圧倒的に多いと想定される。よって、メディア起動禁止設定の対策強度は、実質的に BIOS パスワードの管理精度（「④BIOS PW 保護」）で上限が決まってしまうことになる。その後、メディアからの起動が成功した場合、次の対策項目は「⑤HDD 暗号」である。これは ATM 制御部内のハードディスク(HDD)全体を暗号化する対策で、暗号鍵は ATM 制御部内か、あるいは、暗号鍵を管理するサーバに格納する。ATM 制御部から正常に起動する場合は、該当暗号鍵を使って暗号化されたハードディスクの内容を正しく読み取ることができる。しかし、メディアから別 OS で起動する場合、別 OS は暗号鍵を入手出来ないため、ハードディスクにアクセスすることができない。結果として、マルウェアをハードディスクにインストールすることはできない。暗号ロジックを突破するには大変な労力が必要となるので、メディアからの起動が成功した場合でも「⑤HDD 暗号」により効果的にマルウェアのインストールを対策することができる。

もう一つのマルウェアインストール方法は、「ATM 正常起動後にインストール」である。ATM の制御部が正常に起動した後に、USB メモリ等のデバイスを ATM の制御部に挿して、マルウェアをインストールする方法である。対策としては「⑧USB デバイス防御」により対策することになる。一般に、この対策は OS ハードニングのためのパラメータ設定により実現することが多い。一方、攻撃者が OS 管理者パスワード(OS PW)を入手して、該当 OS パラメータを変更してしまうと、USB メモリが ATM 制御部に接続できるようになってしまうので、「④OS PW 保護」も合わせて必要になる。また、個々の従業員にＡＴＭへのフルアクセス権を与えないよう「⑬職務分離」も必要である。

攻撃者にとって、不正 USB メモリ接続防御設定を解除するために、OS を解析・改ざんするよりも、OS 管理者パスワードを入手して USB メモリ接続防御設定のパラメータを変更する方がはるかに簡単である。よって、「⑧USB デバイス防御」対策の強度も「④BIOS 設定」

と同様にOS管理者パスワードの管理精度（「④OS PW保護」）で実質的に上限が決まってしまうことになる。なお「④OS PW保護」要件には「アドミニストレータ権限のパスワードには堅牢なものを使うこと。」が記載されている。このためATM毎に個別でかつ複雑なOS管理者パスワードの設定が必要となるが、人為的な管理は困難なため、パスワードを管理するサーバやPC等を立てて管理することになる。具体的には、ATMのOS管理者権限を必要とする作業が発生するたびに、管理サーバやPCから対象とするATMのパスワードを取り出してメモなどの形で作業者に渡すことになる。作業者は作業対象ATM設置場所への移動中や作業中もパスワードのメモを紛失しないよう、あるいは、他の人に漏えいしないように厳密に管理して、最後はそのメモを確実に読めない形で破棄しなければならない。加えて、パスワードを管理するサーバやPCはATM作業の有無にかかわらず、24時間365日不正にパスワードを読みだされないかを厳密に管理する必要がある。ここまでやって初めて本対策は有効に機能するが、上記のようにその運用は極めて負担が重くなる。

「④OS PW保護」「⑬職務分離」が突破されてしまうと、不正USBメモリをATM制御部に接続できた状態が実現するので、USBメモリに格納されたマルウェアを容易にインストールできる状態になる。その後の対策としては「⑫ATM装置監視」という、ATMの開局情況を監視する対策になるが、マルウェアインストールを積極的に対策する機能ではないので、「④OS PW保護」「⑬職務分離」がマルウェアインストールに対する対策強度を実質的に左右する対策となる。

「(2) マルウェアインストール」の攻撃ステップが成功すると、次は「(3) マルウェア起動」となる。ATM制御部のハードディスクにインストールされたマルウェアが起動されるのを防止するためには、「⑦ホワイトリスト」による対策が用いられる。もし、ホワイトリストがOS管理者権限によって無効化できるのであれば、攻撃者がホワイトリストのコードを解析して正面突破するよりも、OS管理者パスワードを何らかの形で入手して無効化する方がはるかに簡単である。この場合は、上記と同様に「④OS PW保護」「⑬職務分離」がマルウェア起動に対する対策強度を実質的に左右する対策となる。但し、ホワイトリストの無効化に、OS PWとは異なる独自PWが必要な場合や、ホワイトリストが管理サーバなどで管理されている場合は、OS管理者権限の保護がマルウェア起動防御と直結するわけではないので、実質的な対策強度はもう少し高くなると思われる。

「(3) マルウェア起動」が突破されると「(4) 出金操作」となる。最初の対策は「⑦サンドボックス」によるプログラムの振る舞い制限であるが、全てのマルウェアに対してサンドボックス理論が有効ではないので、このステップで全ての攻撃を対策できるわけではない。「⑫ATM装置監視」「⑭現金補充周期最適化」も監視機能に近い対策となるので、積極的に攻撃を対策するものではない。よって、「(3) マルウェア起動」が突破されると「欧州刑事警察機構のATMへの論理攻撃に関する指導要領と勧告書」では、積極的な対策がないことになる。一方、ATMへのソフトウェア配信サーバが乗っ取られて、そこからマルウェ

アが ATM に配信されるような攻撃の場合は、ATM での対策が「(4) 出金操作」からスタートとなるので、積極的な対策はないことになる。

表 a6- 2 ATM 対策項目の詳細内容

#	対策項目	詳細内容
①	作業員本人確認	認証を受けたサービスプロバイダだけが身分証明書を運び、また ATM サイトにおいては正規従業員が ATM に関係する仕事を行う上での権限を証明する手順があることを確認する。
②	保守扉鍵管理	通常、装置の上部筐体（ボックス）には ATM の PC（制御部）が内蔵されている。この領域は侵入警報装置によって認証を受けずに開かれることを検知することで守られるか、もしくはボックスの鍵は製造者が用意したデフォルトのマスターキーの利用を避けるために交換されるべきである。
③	カメラ監視	監視モニタリングカメラを設置し、ATM 周辺における疑わしい行動を検知して記録できると好ましい。
④	BIOS 設定/ BIOS PW 保護/ OS 管理者 PW 保護	１．破られにくいパスワード(PW)管理設定ポリシーを考慮すること。最良の事例では BIOS がサポートしている可能な限りの複雑さを持つ。 ２．BIOS のブートデバイス設定は ATM のハードドライブだけに設定すること。 ３．可搬式媒体からのブートはデフォルトでは禁止設定にすること。 ４.アドミニストレータ権限のパスワード(PW)には堅牢なものを使うこと。 ５．AUTORUN が完全かつ効果的に禁止されていること。
⑤	HDD 暗号	認証を経ないハードディスク(HDD)への内容変更を防止するためにハードディスク(HDD)の暗号化が行われている必要がある。
⑥	OS ハードニング	ＯＳのハーデニングを実施するか特権乱用を防止するためのパラメータ変更をすべきである。これによりデフォルトアカウントの使用、悪意あるソフトウェアのインストール、USB ポート／CD 媒体／DVD 媒体／ハードディスクへの不正アクセスを防止できる。
⑦	ホワイトリスト	実行を許可するプログラムをホワイトリストに登録し、ホワイトリスト未記載プログラムの実行は認めない対策。
⑦	サンドボックス	起動プログラムを、例えば OS、ミドルウェア、アプリケーションに分類し、それぞれ振る舞いを制限することにより、リスクを軽減させる。 注）サンドボックスは、1)他に感染しない仮想環境でマルウェアを動作させ解析する機能を指す場合と、2)振る舞いが制限された実環境でリアルタイム動作させる機能を有する場合があるが、本説明でのサンドボックスは

		後者を指す。
⑧	USB デバイス防御	未知の USB デバイスはブロックされること。
⑫	ATM 装置監視	適切なＡＴＭ監視システムが配置され、中央から全ての ATM の開局情況を認識できること。 セキュリティソリューションが生成する警報が監視され、動作可能であること。
⑬	職務分離	個々の従業員に ATM へのフルアクセス権を与えないこと。
⑭	現金補充周期最適化	こまめに ATM に適切な現金補充を行うこと。

図 a6- 1 のマルウェア攻撃の流れとその対策に関する分析において、不正出金を防止するために、どの対策が最も重要になるかを見積るために、攻撃者による対策の突破成功確率、並びに、突破失敗確率は図 a6- 2 のように評価される。仮に、対策として対策(A)と対策(B)が存在した場合に、どちらか一方を突破すれば次の攻撃ステップに行ける場合を想定する。図 a6- 1 では、例えば、⑦ホワイトリストを突破するか、④OS PW(パスワード)保護を突破するかのいずれかが突破できれば、(4)出金操作に行けるという状況である。ここでホワイトリストは、OS パスワードで保護された OS 管理者権限によって、無効化できると想定する。いずれかの対策が突破できればよいので、(3)マルウェア起動の対策ステップの突破成功確率は、対策(A)の突破成功確率[PA]と、対策(B)の突破成功確率[PB]の論理和となり、図 a6- 2 の考え方に基づき、最終的に以下の式のようになる。

対策ステップ突破成功確率 ＝ [PA]＋[PB]-[PA]×[PB]

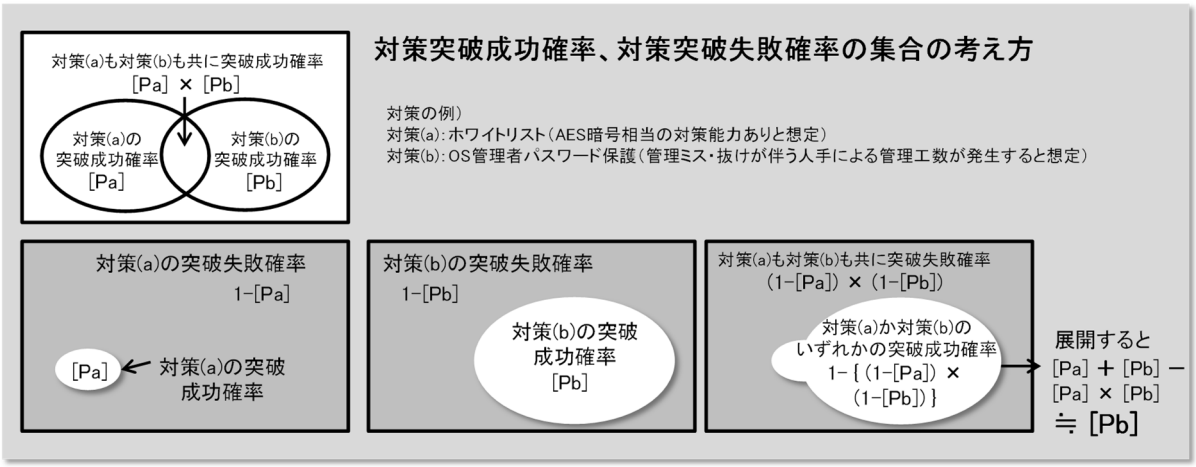


図 a6- 2　対策突破成功確率、対策突破失敗確率の集合の考え方

ここで、対策(A)の突破成功確率[PA]が対策(B)の突破成功確率[PB]に比べて圧倒的に小さい場合を考えると、上記の式は次のようになる。

対策ステップ突破成功確率 ≒ [PB] ただし、[PA]＜＜[PB]

攻撃者がホワイトリストを正攻法で突破するのは難しいのに対し、OS 管理者権限取得に必要な OS 管理者パスワードの入手は相対的に易しい。何故なら管理者パスワードは ATM 毎に全て別々のパスワードを設定することが要件とされているが、人間が覚えられないために、その管理には非常に工数が掛かる上に管理漏れを生じやすい。結果として、攻撃者は管理者パスワードを入手してホワイトリストを無効化するような攻撃を選択することが圧倒的に多いことが推測される。よって、(3)マルウェア起動の対策ステップの突破成功確率は、⑦ホワイトリストの突破成功率ではなく、④OS PW(パスワード)保護の突破成功率で決まるようになる。

図 a6- 3 に示すように、暗号鍵の設定をパスワードによって管理している場合も同様である。仮に暗号技術は AES 128bit 相当の暗号鍵で実現されていると想定すると、その暗号鍵の組合せは約３×10^{38}通りもの組み合わせが存在し、セキュリティ強度は非常に高い。一方、その暗号鍵設定権限が英数字 8 文字の管理者パスワードにより守られているとすると、そのパスワードの組合せは約３×10^{12}通りになり、組合せの数が 10^{26}通りも減少したことになる。

さらに、この暗号技術が数百台の ATM に搭載され、ATM 毎に管理者パスワードが異なる運用をしていると想定する。その場合、人間は個々の管理者パスワードを覚えられなくなるので、管理 PC やサーバに管理者パスワードを保存し、暗号鍵設定が必要な時に作業員にその管理者パスワードをメモなどの形で渡して作業を行なわなければいけない。そして、その作業後にそのメモを誰にも見られないように破棄する必要がある。これらの作業を確実に行う必要があるが、仮に人間の作業ミスが１％の確率で発生するとすれば、約３×10^{12}通りの組合せで守られていると思われていた管理者パスワードが、作業の 100 回に一回の割合でミスが起こり、漏えいしうるということになる。よって、AES 128bit 相当の暗号強度が１％の作業ミスまでセキュリティ強度が下がってしまうことになる。

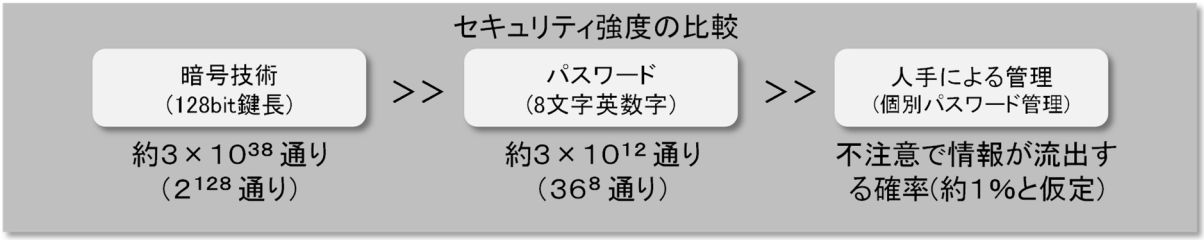


図 a6- 3　セキュリティ強度の比較

加えて、管理者パスワードを格納する管理 PC やサーバは、作業が発生しようがしまいが、第三者が勝手にアクセスしないように、24 時間 365 日の間不正アクセスをずっと監視しなければならない。仮に、その不正アクセスの有無を監視カメラで記録しておき、週に 1 度監視カメラで記録した映像ログを目視確認する。その場合の異常見逃し確率はもっと大きくなると言われており、これはヴィジランス課題（VIGILANCE EFECTIVENESS）と呼ばれている。すなわち、滅多に起こらない異常事態やエラーを、注意を持続しながら監視する課題を与えられた場合に、作業直後でも 10%の見逃しが起こる。さらに、約 30 分で 25%程度まで大幅に見逃しが増加し、その後も見逃し率が増大することが分かっている。このように、セキュリティ対策が人手による管理に大きく依存すると、結果としてそのセキュリティ強度は、想像よりも大きく低下してしまうことが分かる。よって、セキュリティ対策はできるだけ人間による管理を減らした方が有利であることがこれらの分析によって分かる。

参考文献

[1] 一般社団法人 重要生活機器連携セキュリティ協議会、「CCDS 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」、平成 28 年 6 月 8 日、https://www.ccds.or.jp/public/document/other/guidelines/CCDS 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.pdf

[2] 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

[3] 独立行政法人 情報処理推進機構 セキュリティセンター、「共通脆弱性評価システム CVSS v3 概説」、2015 年 12 月 1 日、https://www.ipa.go.jp/security/vuln/CVSSv3.html

[4] 一般社団法人 重要生活機器連携セキュリティ協議会、「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」、平成 28 年 6 月 8 日、https://www.ccds.or.jp/public/document/other/guidelines/CCDS 製品分野別セキュリティガイドライン_車載器編_Ver.1.01.pdf

[5] 石井亮平、佐々木良一、東京電機大学、"イベントツリーとディフェンスツリーを併用したリスク評価手法の提案と標的型攻撃への試適用"、JSSM(日本セキュリティマネジメント学会)第 29 回全国大会研究報告書

[6] 独立行政法人 情報処理推進機構、「調査報告書 別冊 定量的セキュリティ尺度測定ガイドライン」、15 情経第 651 号、http://www.ipa.go.jp/files/000013701.pdf

[7] 電子情報通信学会、「8 章 情報セキュリティマネジメント」 - 電子情報通信学会知識ベース、3 群 7 編 コンピュータネットワークセキュリティー8 章(ver.1/2010.6.14) http://www.ieice-hbkb.org/files/03/03gun_07hen_08.pdf

[8] FIPS PUB 31. "FEDERAL INFORMATION. PROCESSING STANDARDS PUBLICATION", "Guidelines FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT.", 1974 JUNE, https://www.ncjrs.gov/pdffiles1/Digitization/68759NCJRS.pdf

[9] FIPS PUB 65, "FEDERAL INFORMATION. PROCESSING STANDARDS PUBLICATION", "Guidelines FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS", August 1975, http://www.femto-second.com/Documents/FIPS65.pdf

[10] The OWASP Risk Rating Methodology, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[11] The OWASP Risk Rating Template, https://www.owasp.org/images/5/5b/OWASP_Risk_Rating_Template_Example.xlsx

[12] 森山哲、電気電子部門、総合技術監理部門、“人間と安全ヒューマンエラーとリスクアセスメント” 、2008-07-26、
HTTP://WWW.ENGINEER.OR.JP/C_TOPICS/000/ATTACHED/ATTACH_115_2.PDF