IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験

実施報告書

２０１３年２月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

はじめに

IPA/SEC では、ソフトウェア品質説明力を強化すべく様々な観点からの検討を実施してきました。その一環として、ソフトウェア品質を説明するための手法等について具体的な実施方法、そのための作業量、実施にあたっての課題等を整理し、実際にソフトウェア品質を説明する際の参考とできるようにするために、公募により、観点ごとに分けられた実験を別々に実施しました。本書は、それらの結果を、実験ごとにまとめた報告書のうちの１つです。

本報告書の実験は、「2011 年度 システムエンジニアリング実践拠点事業」として、株式会社シーエーブイテクノロジーズに委託し実施しました。

「IC カードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験」
【報告書】

独立行政法人情報処理推進機構

目次

1. 模擬実験の背景

1.1. 本実験の位置付け

本実験の位置付けを「図 1-1　実験の位置付け」に示す。本実験は、事業者サイドが、第三者に向けて品質説明を行う際、「単一の品質確保ではなく、複数の品質確保を同時に行い、品質に関する技術的な妥当性を説明する」ための方法論を検証することを目的としている。複数の品質として、本実験が対象とした品質は、**「安全性」**と**「セキュリティ」**であり、そのための方法論として、SafSec方法論（以下SafSecという）を適用した。SafSecとは、英国Praxis社が英国防衛省の依頼で実施した将来の航空機システムにおけるSafetyとSecurityの認証を同時に行う方法論である（参考文献[1]、参考文献[2]）。本模擬実験は、事業者サイドにとっては、品質説明力を維持したまま、複数の規格に適合したシステム開発の適用と、認証コストの削減の指針を与えることになる。製品の利用者に対しては、事業者が製造する製品・サービスにおける、複数の品質特性を保証することになる。そして、監査を実施する機関にとっては、複数の規格への適合性の評価を実施する場合の、適用技術の妥当性確認のための指針を与えるものである。

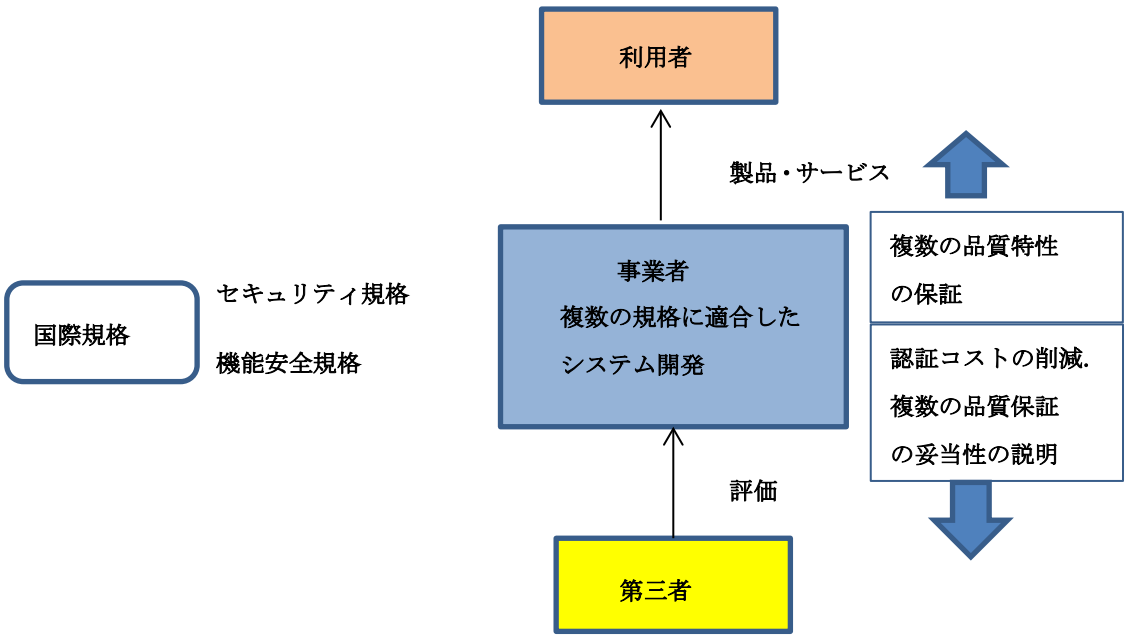


図 1-1　実験の位置付け

本模擬実験で利用したSafSecは、既存の品質規格を補完する技術であるため、用いる規格の安全度水準などに準じるのが基本である。しかし、「2.6.1　品質レベルの考え方」で述べるように、機能安全規格であるIEC 61508の適用において定められている安全度水準

（SIL (Safety Integrity Level)）については、SafSec に適合しなかったので、独自の判断基準を策定して用いた。

安全性とセキュリティの同時評価・認証は、今後、様々な分野で必要になることが予想される。その際に、今回の実験結果は、以下の点での活用が可能である。

① SafSec において定義された分析・評価方法論のフィージビリティ評価
② 実際に適用する際の課題、解決策の明確化
③ 利用する際のコスト評価

1.2. 本書の読み方

本書の読み方を説明する。実験の内容を完全に理解する上では、全文を読まれることをお勧めするが、実験の概要を理解する上ではいくつかの節は読み飛ばしても差し支えない。「2 実験の内容」において、実験の着目点、関連規格、手法、対象となるシステムなど、本実験の特徴を理解する上での説明がされている。「2.5 対象システム」では、実験が対象としたシステムについて詳説しているが、この節を読まなくとも、実験の概要は理解できる。また、実験の経緯、結果などは、「3 模擬実験」で順を追って詳しく説明しているが、概要を読み取る上では、前述した範囲で 2 章を読んだ後、「3.5 実験結果」、「3.6 考察」、「4 まとめ」と読み進まれることをお勧めする。

2. 実験の内容

2.1. 実験の特徴と目的

本実験の特徴は複数のシステムの品質、特に安全性とセキュリティに対する同時評価・認証を行うことである。複数のシステムの品質に対する認証や品質の説明責任に関する問題点は様々であるが、大別すると以下の 2 点が挙げられる。

問題点 1： 分析・開発方法論の開発
問題点 2： 評価・認証コストの軽減化

問題点 1 に関しては、従来の分析・開発方法論は安全性やセキュリティなどの単一の品質に対してのみ開発されており、複数の品質に対する分析方法、開発方法論が明確で無い点である。複数の品質が含まれる場合で特に問題となるのは、異なる品質間で影響を及ぼしあう場合の取扱い方がある。この扱いを誤ると、作業が冗長的になったり、作業に漏れが生じたりすることになる。

問題点 2 は、国際規格による製品認証はその必要性が産業界においても認識されているが、産業界にとって厳しく圧し掛かる問題は、認証にかかるコストである。認証にかかるコストには、認証の基準が要求する開発プロセスの変更コスト、認証のための成果物作成

のためのコスト、第三者認証機関に評価、認証を委託する際のコストなど様々なものがある。例えば、航空機ソフトウェアの安全ガイドラインである DO-178B においては、認証のためのコストは開発コストに対して 40%から 200%とされている（参考文献[15]）。

RTCA, DO-178B, Software Considerations in Airborne Systems and Equipment Certification, 1992 （参考文献 [14]）

複数の品質に対して、個別に国際規格への評価・認証を行うと、「図 2-1　安全性とセキュリティの同時認証の考え方」に示すように、規格数だけコストが加算される計算になる。評価・認証コストを軽減するためには、複数の品質に対して作業を同時に実施し、作業の共有化などによるコストの削減方法が必要になる。

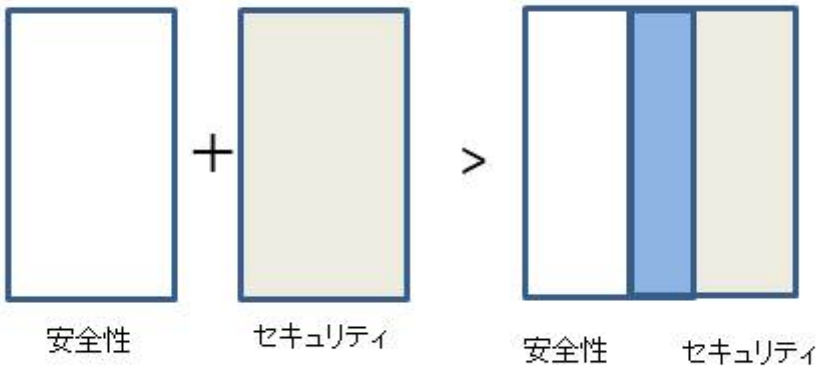


図 2-1　安全性とセキュリティの同時認証の考え方

本模擬実験の目的は、セキュリティと安全性の同時認証のための手法の確立のためのフィージビリティスタディにあり、そのために、同時認証がもたらす効果をコスト削減効果と既存の国際規格との関係の下で明らかにすることである。

2.2. 既存の国際規格

安全に関する国際規格は、食品の安全性に関するものから機械の安全性に関するものまで数多く存在する。ここでは、機械、電子、電気、情報システムの安全性に関する規格を対象として考える。安全に関する規格は以下のように構成されている。

一番根本となる規格は A 規格、基本安全規格であり、次に、産業分野別の規格（B 規格、グループ安全規格）があり、最後に製品ごとの規格（C 規格、製品安全規格）が存在する。

A 規格の例としては、は ISO 14121（リスクアセスメント）（参考文献[5]）がある。本実

験において利用される IEC 61508 は B 規格（グループ安全規格）であり、また以下の説明で言及される ISO 26262（参考文献[6]）は自動車の電気・電子システムに関する C 規格（製品安全規格）である。（「図 2-2　安全規格の階層」　参照）

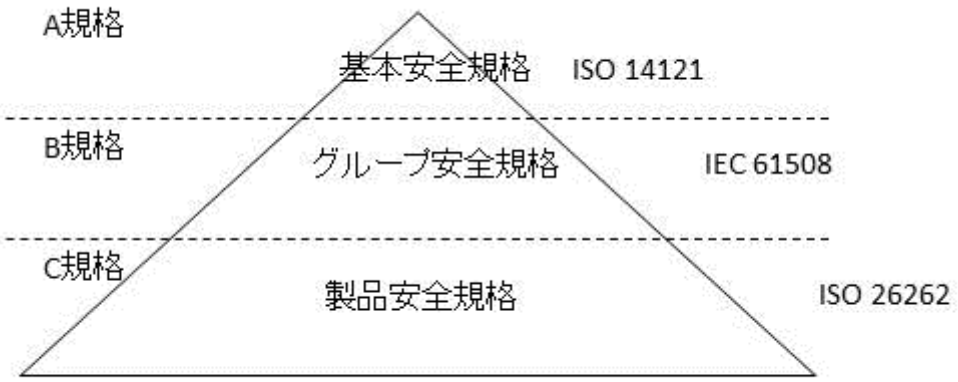


図 2-2　安全規格の階層

これに対して、情報システムに関するセキュリティについては、個別分野で見ると、デビットカードやクレジットカードのセキュリティに関する規格である PCI DSS (Payment Card Industry Data Security Standard)（参考文献[7]）や、会社組織における情報セキュリティ管理に関する ISO/IEC 17799（参考文献[8]）などがあるが、広く利用されているのが CC である。本節では本実験で用いるセキュリティの規格 CC と安全性の規格 IEC 61508 についてその概要を説明する。

2.2.1. Common Criteria (ISO/IEC 15408)

Common Criteria, ISO/IEC 15408（以下「CC」という）は ISO (International Organization for Standardization、国際標準化機構)と IEC(International Electrotechnical Commission、国際電気標準会議)により策定された情報システムのセキュリティに関する規格であり、政府の製品調達のための基準として利用されており、本規格において評価、認証された製品を政府が利用する、といった使われ方がされている。CC により認証された製品としては、既にパソコン用の OS、鉄道やバスなどの公共交通機関で使用される IC カードに利用されている非接触型スマート IC カードまで多岐に及んでいる。他にもデータベースシステム、コピー、Fax 機能を持つ複合機がある。

CC は Part 1「概説と一般モデル」、Part 2「セキュリティ機能要件」、Part 3「セキュリティ保証要件」から構成されている。Part 1 においては、用語や概念の定義、セキュリティ要件の調整方法、プロテクションプロファイルの説明、セキュリティターゲットの仕様などが記述されている。それに対して、Part 2 においては、様々なセキュリティ機能のコ

ンポーネントが記されており、監査、通信、暗号サポート、認証、セキュリティ管理などのセキュリティ機能要件が構造化されて示されている。Part 3 においては、どのように保証されるかの枠組みを、Part 2 と同様な形で構造化されていることが示されている。品質レベルである EAL (Evaluation Assurance Level)については、Part 3 において詳細に示されている。

品質レベルは CC においては、評価保証レベル（EAL）と呼ばれ、EAL1~ EAL 7 までの 7 段階で評価される。EAL 1 が一番弱く、EAL 7 が一番厳密なレベルである。(「表 2-1　CC における評価保証レベル」参照)

評価保証レベル	概要
EAL 1	機能テスト
EAL 2	構造テスト
EAL 3	方式テスト、及びチェック
EAL 4	方式設計、テスト、及びレビュー
EAL 5	準形式的設計、及びテスト
EAL 6	準形式的検証済み設計、及びテスト
EAL 7	形式的検証済み設計、及びテスト

表 2-1　CC における評価保証レベル

実際に製品を認証する場合には、セキュリティターゲット（Security Target）と呼ばれる文書を作成する必要がある。セキュリティターゲットには、その製品の認証する範囲から始まり、想定される脅威、対抗するセキュリティ機能要件、ターゲットとなる品質レベルが示されている。評価の対象（TOE：Target of Evaluation と呼ぶ）は、システムのどのような部分を選択しても良い。

本実験でこの作業を行う際、モバイル Felica IC チップのファームウェアに関する以下のセキュリティターゲットを参考にした。

フェリカネットワークス社, モバイル FelicaIC チップファームウェア（T6N 版）,セキュリティターゲット, version 1.01, No. FN12-F028-J01-01, 2009/06/26　（参考文献[17]）

TOE はチップのファームウェア（T6N 版）であり、評価保証レベルは「EAL4 追加」である。「EAL4 追加」とは、EAL4 の達成に必要な保証要件（保障クラス：大分類、保証ファミリ：中分類と分類されている）にいくつかの保証要件を付け加えたことを意味している。ここで追加された要件は、攻撃を考慮した脆弱性判断 AVA_VLA.3、及び欠陥発生時に即座に対応するための ALC_FLR.1 である（参考文献[17]、参考文献[21]）。表 2.2 に EAL4

に追加されている 2 つの保証ファミリの概要を「表 2-2　保証クラスと保証ファミリ」に示す。

保証クラス	保証ファミリ	概要
ライフサイクルサポート	ALC_FLR.1.1.E	ALC クラスは構成管理に関するクラスであり、ここでは、特に、欠陥修正手続きの妥当性の確認について。
脆弱性判定	AVA_VLA.3（1E，2E，3E，4E，3.5E）	脆弱性分析がセキュリティターゲットの記述と一貫性を保持していることや、脆弱性確認分析の方法についての確認。

表 2-2　保証クラスと保証ファミリ

また、脅威として、「表 2-3　脅威の分類」に記載した 9 種類が想定されている。

脅威の分類	内容
T.Abuse_Command_Data	「悪意のある所有者」が、不正なコマンドデータを I/F から送信する攻撃。
T.Reuse_Command_Data	「悪意のある所有者」が、コマンドデータを取得し、そのコマンドデータを再送信する攻撃。
T.Intercept_Commnicate_Data	「悪意のある所有者」が、コマンドデータを盗聴・改ざんする攻撃。
T.Intercept_Security_Data	「悪意のある所有者」が、コマンドデータ、レスポンスデータを盗聴し、その情報からアクセス暗号鍵の解析による攻撃。
T.Abuse_ReaderWriter_SecurityFunction	「悪意のある所有者」が、リーダ／ライタ機能の「カード認証」を不正に利用する攻撃。
T.Interrupt_Power	「悪意のある所有者」が、TOE の電源を停止し、データの改ざん、破壊する攻撃。
T.Break_Hardware	「悪意のある所有者」が、チップを故障させることによる、セキュリティ機能に危殆化攻撃（危殆化とはセキュリティ上の安全が脅かされること）。

T.Install_EvilProgram	「悪意のある所有者」が、TOE プログラムの欠陥修正プログラムインストール機能を利用して、データの改変、アクセス暗号鍵の暴露を行うプログラムをインストールする攻撃。
T.Copy_TOEData	「悪意のある所有者」が、TOE プログラムのデータ移動機能を利用し、保護データ、アクセス暗号鍵を不正に複製することによる攻撃。

表 2-3　脅威の分類

2.2.2. IEC 61508

本規格は、IEC が制定した、電気(electrical)と（もしくは）電子(electronic)部品から構成されるシステムの安全性に関する国際規格である。本規格は対象製品の機能安全（functional safety）を保証するものである。機能安全という概念は、人命に大きな影響を与えるリスクを全て排除する絶対安全という概念ではなく、許容可能な目標までリスクを軽減する、という考えである。

規格は Part 1 から Part 7 まであり、概論、ソフトウェアへの要求、安全度水準の決定方法、適用ガイドラインなどにより構成されている。

IEC61508 における安全度水準（SIL）の決定方法は、2 種類のハードウェア故障（決定論的故障とランダム故障）を基本としている。例えば、低い要求モード（low demand mode）の操作において動作する、安全機能の危険な故障の平均確率で決定される場合は表 2-4 のようになる。

安全度水準(SIL)	安全機能の危険な故障の平均確率
4	$\geqq 10^{-5}$ から $< 10^{-4}$
3	$\geqq 10^{-4}$ から $< 10^{-3}$
2	$\geqq 10^{-3}$ から $< 10^{-2}$
1	$\geqq 10^{-2}$ から $< 10^{-1}$

表 2-4　SIL の決定表

達成すべき安全度水準（SIL (Safety Integrity Level)）が決定されると、それに対して、開発手法などが規定される。例えば、ソフトウェア安全機能要件（Software Safety Functional Requirements）に対しては、安全度水準に従って、適用される開発手法が異なる。（「表 2-5　SIL のレベルによる適用の推奨度合いの違い」参照）

技法／手法	SIL1	SIL2	SIL3	SIL4
準形式手法	R	R	HR	HR
形式手法	R	R	HR	HR

表 2-5　SIL のレベルによる適用の推奨度合いの違い

ここで、R は推奨される技術であり、HR は高く推奨される技術を意味する。例えば、システムの SIL が 3 の場合には、形式手法（例えば、形式仕様記述言語である Z（参考文献[19]）やモデル検査ツールである SPIN（参考文献[20]））の利用が必須である。

安全度水準の決定方法は、利用される部品の故障率が公開されている場合には、数学的に計算は容易であるが、対象となるシステムにおいて、必ずしもこのような状況が当てはまらない場合がある。これは対象システムの性質や、各社毎の安全基準の算定方法の違いなど、様々な理由がある。IEC 61508 においては、条件に応じて様々な決定方法の利用が許可されている。それらは 「Part 5 安全度水準の決定に関する方法の例（Examples of methods for the determination of safety integrity levels (edition 2.0 2010-04)）」 においてまとめられている。本実験では、Part 5 の付録である以下を用いた。

付録 C ALARP と許容範囲リスクの概念（Annex C ALARP and tolerable risk concepts）

付録 E 安全度水準の決定 – リスクグラフ手法（Annex E Determination of safety integrity levels – Risk graph methods）

リスクグラフ手法は、リスクの因子の知識から安全度水準を決定する方法であり、定量的にも定性的にも利用することができる。考慮すべきパラメータの例として、以下の 4 つが示されている。

1) ハザーダスイベントの帰結(C) (consequence of the hazardous event)
2) ハザーダスゾーンにおける頻度（F）(frequency of, and exposure time in , the hazardous zone)
3) ハザーダスイベントを回避することに失敗する確率（P）(possibility of failing to avoid the hazardous event)
4) 望まれない生起の確率（W）(probability of the unwanted occurrence)

これらのパラメータに関して、リスクの度合いを定義することが可能である。例えば、ハザーダスイベントの帰結に関しては、以下のようなリスクの分類を決めることができる（参考文献[3]）。（表 2-6 参照）

リスクのパラメータ		分類
帰結（C）	C1	軽微な怪我
	C2	1 人もしくは複数の人への深刻な生涯にわたる怪我。もしくは、1 人死亡
	C3	複数人が死亡
	C4	非常に多くの人が死亡

表 2-6　帰結に関するパラメータ例

全てのパラメータに対して、リスクの分類を行い、次にパラメータ間の組合せを考えるのがリスクグラフの考え方である。

次に、ALARP について説明をする。

ALARP (As Low As Reasonably Practicable) 領域とは、リスクを

- 広く容認されるリスク
- 許容可能なリスク
- 許容不可能なリスク

という 3 つの領域に分割したうち「許容可能なリスク」の領域を指す。
ALARP 領域ではリスクの低減にかかるコストに比べて得られる利益が極端に少ない場合は、そのリスクを許容する。この ALARP 領域の概念と頻度と深刻度からリスクを決定する方法について記述されている。

2.3. 安全性とセキュリティの同時認証

本実験は安全性とセキュリティの同時認証が特徴であることはすでに 2.1 節で述べた。このような安全性とセキュリティの同時認証が必要となるのかを本節で説明する。まず例を挙げ今後、同時認証が必要となる背景を述べる。次に本実験で調査した同時認証の先行研究であり、また本実験での分析プロセス構築の際に参考にした SafSec について説明する。

2.3.1. 同時認証が必要となる背景

本実験が対象とする、安全性とセキュリティの両方の認証が必要になる例を以下に示す。これらは、現時点では実際に認証例として存在しないが、近年中に実施される可能性が高い例である。最初の例として、車載組込みシステムに関する開発ツールがクラウド上のサービスとしてとして提供される場合を考える(注 1)。このような場合には、車載組込み機器の機能安全に関する国際規格である ISO 26262 におけるツールの資格認定（Tool

qualification）(注 2)と、クラウド上のサービスとしてのセキュリティの保障や、サービス品質（Service Level Agreement）の保証などが必要になると考えられる。
このような場合、ツールの資格認定をISO 26262 に基づいて実施すると同時に、セキュリティについては、クラウド上のセキュリティの規格を策定している組織であるCloud Security Alliance (CSA)（参考文献[9]）が提供する Cloud Controls Matrix (CCM)(注 3)（参考文献[10]）を用いたセキュリティやコンプライアンスへの適合確認、といった複数の規格、ガイドラインを利用することが今後、必要になることが予想される。(「図 2-3　安全性とセキュリティの同時認証例(1)」参照)

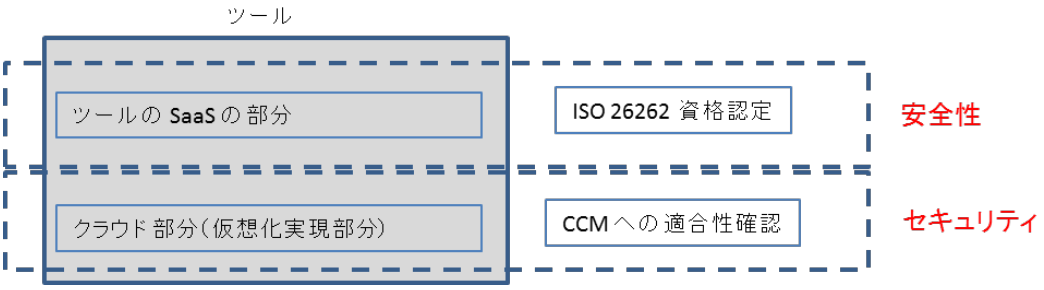


図 2-3　安全性とセキュリティの同時認証例（1）

注1)　このような形態はクラウドでは SaaS（Software as a Service）と呼ばれる。

注2)　多くの機能安全規格においては、開発に利用されるツールが開発において作成・生成された成果物に対して、エラーを混入させない、エラーの原因にならないことを保証する必要がある。

注3)　マイクロソフト社がクラウド上のオフィスアプリケーションとして提供している Office 365 は CSA における CCM への準拠を発表している（参考文献[11]）。

現在、自動車の情報システムが、無線等による通信を介して、外部に接続されているケースは一部にとどまっているが、今後は、外部ネットワークに接続され、様々な情報を共有することが予想される。例えば、既に一部の製品に見られるように、カーナビゲーションシステムがインターネットとつながることにより、精密な交通道路情報を得ることで、道路の混雑状況を回避するといったことが可能になる。外部に接続されることにより、ハッカーなどによる車載情報システムへの攻撃を受けやすくなり、個人情報の漏洩、自動車の制御系の乗っ取りなど、様々な障害が生じる可能性がある。

外部への接続を考慮しなくても、現在の自動車に搭載されている情報システム自身には、セキュリティの対策が施されていないので、車載情報ネットワーク（CAN (Controller Area Network)(参考文献[12])）に流れる情報を入手し、車載組込みソフトウェアを改ざんする、といったことが可能になることが研究により示されている。

K. Koscher, et. al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy 2010 （参考文献［13］）

車載情報システムが外部からの攻撃に対して頑健であることを示す場合、自動車の安全性については ISO 26262 で認証を行い、セキュリティに関しては CC による認証を行う、といったことが考えられる（「表 2-7　同時認証の例」参照）。
このように、従来は安全性だけを考慮すれば良かった製品においても、セキュリティの問題が顕在化しつつあり、産業界としては対応が必須になることが予想される。

例	認証のための規格・ガイドライン
車載システム開発用ツールの同時認証	セキュリティ（Cloud Security Alliance の Cloud Control Matrix）
	安全性（ISO 26262）
ネットワークへ接続可能な車載情報システム	セキュリティ（CC）
	安全性（ISO 26262）
車載情報システム	セキュリティ（CC）
	安全性（ISO 26262）
本実験	**セキュリティ（CC）**
	安全性（IEC 61508）

表 2-7　同時認証の例

2.3.2. SafSec

SafSec は、高度な航空機アーキテクチャ（Advanced Avionics Architectures）もしくはモジューラ航空システム（Modular Avionics）に対して、安全性とセキュリティの同時認証を試行するために実施されたものである。SafSec はガイドと規格の両方から構成されている（参考文献[1]、参考文献[2]）。安全とセキュリティの両方の認証のために、両方の品質に関する概念の整理が行われている。

SafSec はよりコストの削減、リスクの軽減が行えるフレームワークを、以下の性質を基に提供するものである。

1) システムの概念形成から明らかな安全とセキュリティの目標を前提とする。
2) 根拠資料の生成に対して、プロセスベースのアプローチではなく、ゴールベースのアプローチが適用されており、システム設計への安全性とセキュリティの影響をより効果的に実施。

3) 認証に対するモジュラーアプローチが適用されており、システムの複雑さの取扱いや、変化による再認証を容易にし、かつ再利用を可能にする。
4) システムのコンポーネントへの認証可能性を確立するための、漸近的なアプローチの適用
5) 安全認証とセキュリティ適合の両方への利用を最大化するために、根拠資料の作成に関して共通のアプローチを適用
6) 安全性とセキュリティの目標を支援する根拠資料は、後付けで作成されるのではなく、プロセスの適用中にシステマチックに構築され、認証における監査官（アセッサ）の仕事を軽減し、コストのかかる再設計のリスクを軽減する。

ここで分かるのは、 SafSec は安全性とセキュリティの同時認証だけではなく、システムの変化に伴う、認証の改訂、新たな認証対象に対する再利用性の確立など様々な技術を支援するフレームワークであることである。

SafSec における用語の意味を「表 2-8　用語の定義」に説明する。

用語	説明
原因分析（Causal analysis）とインパクト分析（Impact analysis）	原因に紐付けられるロスの分析（例：システム故障、セキュリティ攻撃）とそれらの原因によるインパクトの分析。
ディペンダビリティ（Dependability）	信頼性が正当化できるサービスを提供する能力。
ディペンダビリティ仕様（Dependability Specification）	システムもしくは、そのコンポーネントの仕様で、そのディペンダビリティ特性を定義する仕様。
ディペンダビリティ目標（Dependability Target）	リスク分析において、ロスに対するディペンダビリティ目標が同定される。ディペンダビリティ目標は、ロスに対して許容できる残存（residual）リスクのレベルであり、定義された対抗策の集まり（ディペンダビリティ仕様）により達成される目標である。
同定されたロス（Identified losses）	プロジェクトに関与したステークホルダにより同定されたロスの集まりであり、その生起がシステムのディペンダビリティに関係するもの。通常、受容可能な潜在的リスクに関連する。
頻度（likelihood）	ロスは起こりやすさを測る割合として、確率もしくは頻度を持つ。この確率や頻度がロスの頻度である。頻度は定性的に表現することも可能であり（例えば、頻繁（frequent）から信じられない（incredible））、また定量的に定義することも可能。
ロス（Loss）	ロスは SafSec の中で望まれていないシステムの状態を示す一般的な用語である。ロスは安全性においてはハザードと類似しており、セキュリティにおける脆弱性を表す。

表 2-8　用語の定義

SafSec におけるディペンダビリティケースに関しては、本実験の範囲外なので、ここでは触れない。

SafSec におけるプロセスを「図 2-4　SafSec におけるプロセス」に示す。ここでは、安全とセキュリティに関する「ロスの同定」以降のプロセスが定義されている。「ロスの同定」の次には、同定されたロスの深刻度評価（「インパクト分析」）を行い、次に頻度の評価を行う（「原因分析」）。そして深刻度と頻度から「リスクの評価」を行う。これと同時にどの程度のディペンダビリティを達成するかの目標を設定し、リスクの度合いとディペンダビリティ目標との比較を行う。リスクの方がディペンダビリティ目標より高い場合には、リスクを軽減する必要があるので、提言するディペンダビリティ仕様を考案する必要がある。それに対して、リスクの方がディペンダビリティ目標より低い場合には、特に対抗策を考慮する必要がないので、プロセスから抜ける。

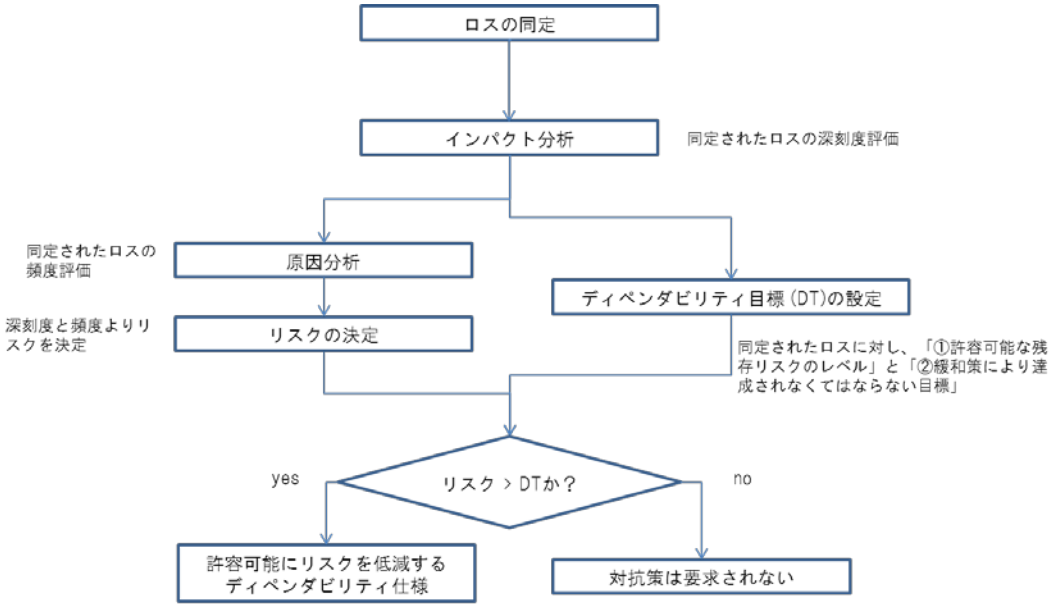


図 2-4 SafSec におけるプロセス

2.4. 本実験で用いる分析方法論

本模擬実験では、SafSec に基づき安全性とセキュリティの同時認証のプロセスを構築し、その試行を行う。ここではその試行において使用した分析のための方法論について説明する。本模擬実験で使用した分析方法論は FTA(Fault Tree Analysis)などに代表される「前向き分析」と FMEA(Failure Modes and Effects Analysis)に代表される「後ろ向き分析」を主に用いて分析を実施した。実際の分析ではこれらの方法論を基にし、事例への適合のための独自の工夫をして実施している。これら前向き分析、後ろ向き分析についてそれぞれ

FTA、FMEA という手法を取り上げて説明する。

FTA

ある事象が起こる原因の潜在的なフォールト（故障やヒューマンエラーなど）をたどる。そこで特定された各原因の頻度（発生確率）から基となる事象の頻度（発生確率）を計算し求めることを目的とした方法である。ある事象からその原因へと細分化して分析を行っていくトップダウン（前向き）手法である。この手法を「図 2-5 FTA」に示す。

まず初めに望ましくない事象を配置する。この望ましくない事象をトップ事象と呼ぶ。十分詳細化されるまで事象に対してその要因を列挙することを繰り返す。十分詳細化された事象を基本事象と呼び、トップ事象と基本事象の間にある事象を中間事象という。列挙された複数の要因のうちいずれか 1 つが起こった場合に上位の事象が起こる「OR 関係」（図の中間事象 1 の要因以外の部分）と、すべて起こった場合に上位の事象が起こる「AND 関係」（図の中間事象 1 の要因の部分）を明記する。トップ事象の頻度を「OR 関係」の場合はそれらの要因の頻度の和で、「AND 関係」の場合はそれらの要因の頻度の積で求めることができる。

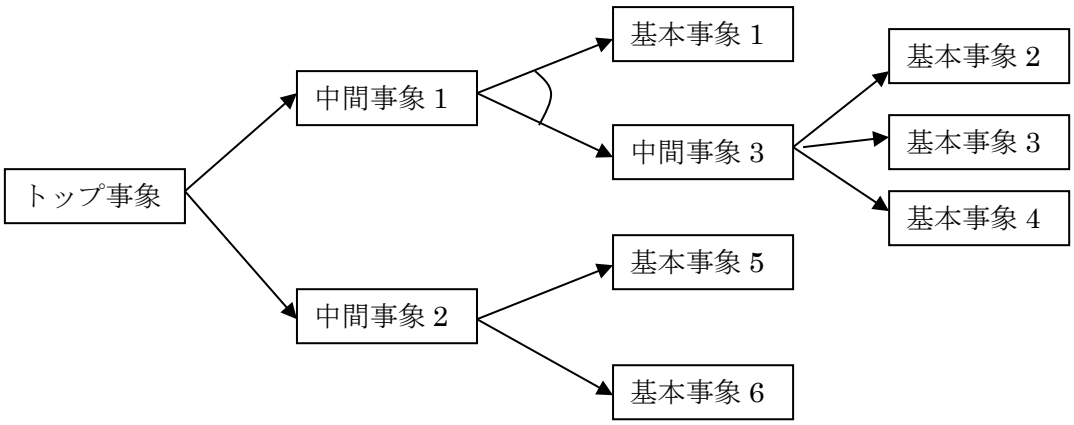


図 2-5 FTA

FMEA

ある部品の故障モード（故障形式の分類）からどのような影響があるか、その結果（影響や被害の大きさ）を求める方法である。細部（部品の故障の仕方）からシステムへの影響を分析していくボトムアップ（後ろ向き）手法である。

アイテムごとにその故障モードを列挙し、その故障モードについて影響を考え（影響が複数になることもあり得る）、その深刻度を決定する。もともとはハードウェアの設計時に用いられる手法であり、経験的に故障モードを把握しやすいハードウェアと異なりソフト

ウェアに用いるときには故障モードをどのように設定するか検討する必要がある。

また、FMEA では単一故障のみを考えており多重故障については考慮しない。以下に FMEA で用いるワークシートの例を「表 2-9　FMEA ワークシート例」に示す。これを適宜追加変更して用いる。

アイテム（部品）	機能	故障モード	故障原因	影響	対策	深刻度	備考

表 2-9　FMEA ワークシート例

2.5. 対象システム

本実験は、VRICS と呼ばれる社会情報基盤技術をベースとし、その上に、特定の機能仕様を持つサービスレイヤを載せたシステムを対象としている。本節ではシステムの基盤である VRICS について説明する。

2.5.1. VRICS とは

VRICS は Value and Right Circulation Control System の略で、価値と権利の流通を管理する仕組みである。

人間は社会の中で公共のサービスから民間のサービスまで、様々な組織の多様なサービスを受けて生活をしている。人間の 1 日は様々な組織の多様なサービスを享受することによって成り立っているといっても過言ではない。この人間の生活とサービスの関係を「図 2-6 人間の生活とサービス」に示す。

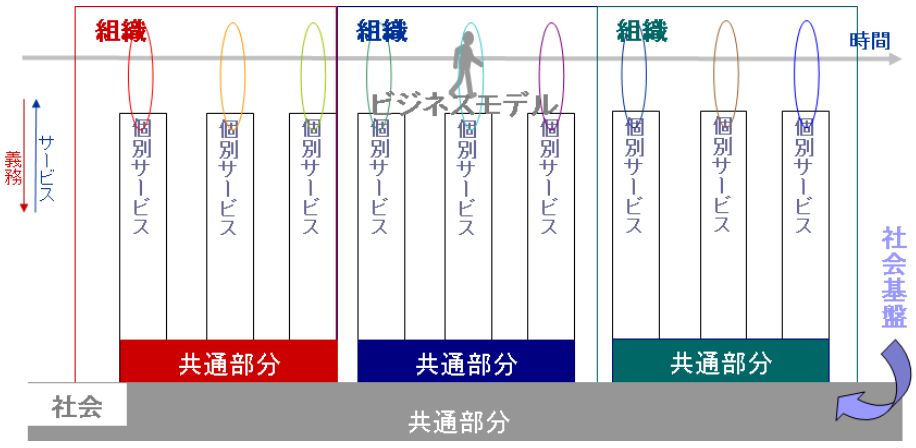


図 2-6 人間の生活とサービス

一般的に、サービスを受けるため（サービスを受ける権利を行使するため）には義務の行使が前提となる。義務を果たすことそのもの、もしくは義務を果たした証と交換にサー

ビスが提供される。義務は労働であり、労働の対価であるお金（価値）の支払いであり、その義務を果たした証が権利証となる。

多様なサービスの供給管理を情報システムによって実施する場合、このサービスを受けるための権利と義務の関係を情報システム上で管理する仕組みが必要となる。この仕組みは、言い換えると情報システムにおいてサービスの供給を管理する仕組みであり、電子化された価値と権利・権限の流通を管理する仕組みで情報システムにおけるサービスのための基盤、すなわちサービス情報基盤である。

VRICS はこの電子化された価値と権利・権限の流通を管理する仕組みである。

2.5.2. VRICS の基本構成

VRICS はシステムと運用で価値と権利・権限の流通を管理する。

システムでは基本的に権利・権限の証明書確認（Certification）を行い、必要であれば権利の正当な行使者であるか識別（Identification）し、その場合次に行使を申し出ている人が本当に本人であるか真正性確認（Authentication）を行う。その上で権利・権限はどのようなレベルで行使可能な状況にあるかを確認し、問題がなければ権限認可（Authorization）しサービスを提供する。

しかし、サービスの提供にはシステムで対応しきれない外的な脅威やサービス運用のミスに起因するリスクもあるため、これを VRICS では抑止（精神的、物理的）、防御、担保、転嫁といった運用策で解消することを目指している。これらの VRICS の権利・権限管理の考え方を「図 2-7　VRICS の権利・権限管理の考え方」に示す。

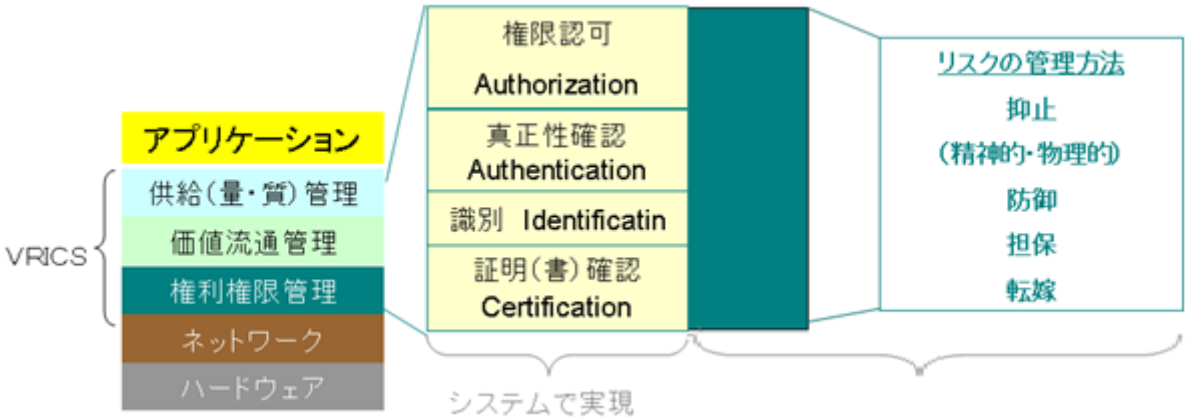


図 2-7　VRICS の権利・権限管理の考え方

2.5.3. VRICS の基本構造と機能

VRICS は管理情報発行者（以下「VRICS 情報発行者」という。）と IC カード等の管理

情報収納媒体（以下「VRICS デバイス発行者」という。）発行者、本人確認情報照会機関（以下「本人確認認証局」という。）、サービス提供者、サービス利用者の存在を前提としている。

ここで VRICS 情報発行者は VRICS デバイス発行者、本人確認認証局を兼ねることも可能となっている。

VRICS はオフラインのサービス提供にも対応し、より柔軟な権利・権限管理ができるよう参加証（以下「Trade Title」という。）、電子的権利証（以下「Service Title」という。）、サービス毎に異なる ID（以下「SubID」という。）、本人確認証（以下「Certification Title」という。）の 4 つの情報を用いてサービスの提供管理を行っている。

Trade Title は、フィッシング等を防止することを目的として VRICS デバイスとリーダ間で相互認証をするためにやり取りする情報である。この Trade Title は、VRICS デバイス発行時に VRICS 情報発行者によって使用するデバイスに埋め込まれる。

Service Title はサービスが追加される度に SubID 生成のための可変の種（サービス毎の SubID 生成のためのデータ）とともに VRICS 情報発行者から VRICS デバイスに送り込まれる情報である。提供されるサービスと標準的な用法では SubID が指定される利用 ID や本人確認方法等の提供条件、Service Title そのものの価値（質と量）が記載されている。この Service Title は提供条件を満足することを前提とし、ServiceTitle の価値と交換にサービスが提供される。

SubID は、ID の種である Personal ID（以下「PID」という。）とサービスが追加される度に Service Title とともに、VRICS 情報発行者から VRICS デバイスに送り込まれる ID 生成のための可変の種を用いて自動生成される。生成される SubID 間にはそれぞれ隠れた関係性を持っているため、九州大学では、このような ID を“Hidden relationship ID”と呼んでいる。この SubID は利用者識別に利用する。なおここで ID の固定の種である PID は VRICS デバイス発行時に VRICS 情報発行者からデバイスに組み込まれるサービス利用者 1 人に 1 つの情報となっている。

Certification Title には、本人確認情報若しくは本人確認情報収納場所が記載されている。本人確認情報若しくは本人確認情報収納場所は、サービス提供者から指定された内容で VRICS 情報発行者から VRICS デバイスに送り込まれる。

この VRICS では 図 2-8 に示す仕組みによって基本的なサービスを提供する。まず利用者が VRICS デバイスを専用リーダにかざすと、VRICS デバイスと専用リーダの間で Trade Title による相互認証が行われる。次に、リーダからの要求に対し VRICS デバイスからリーダへ Service Title の提供が行われる。リーダは Service Title の提供条件に「利用者識別」が含まれていれば、VRICS デバイスに対して利用者識別情報提供の要求を出し、VRICS デバイスはこの要求に対して Sub ID を返す。さらに、リーダは提供条件に本人確認が記載されていれば、VRICS デバイスに対して本人確認情報提供の要求を出し、VRICS デバイスは

Certification Title または本人確認機能要求を返す。リーダは本人確認機能要求を受けると、本人確認情報をリーダ本体に取り付けられているキーボード等の認証デバイスから取得後、本人確認情報を認証局若しくは VRICS デバイスに送り本人確認の判定を行う。リーダは本人確認判定が終わり、認証局若しくは VRICS デバイスから OK 信号を受け取ると、サービスサーバもしくは VRICS サーバにサービス開始トリガーを送る。これによりサービスが開始される。

VRICS では、既存サービスシステムの取り込みも 2 つの方法で可能としている。第一の方法は、Service Title もしくは Service Title＋Sub ID の既存サービス ID へ紐付ける方法である。VRICS はシステム内に紐付けシステムを有しており、既存のサービス ID を用いてサービスを提供するサービスシステムを取り込む場合、紐付けシステムで Service Title 若しくは Service Title＋Sub ID を既存サービスのサービス ID に変更し既存システムに返す。これにより既存システムを大掛かりな変更をせずに VRICS を用いた情報基盤に取り込むことが可能となる。

第二の方法は、Service Title にロケーションを指定して既存 ID を直接利用する方法である。この方法では、VRICS デバイス内の指定された場所にあらかじめ既存サービスのサービス ID を入れておく。この場合、Service Title はサービスに利用する本人識別子として VRICS で生成される Sub ID を指定せず、既存サービスのサービス ID が収納されているロケーションを指定する。これにより既存サービスのサービス ID を直接本人識別子として利用する。

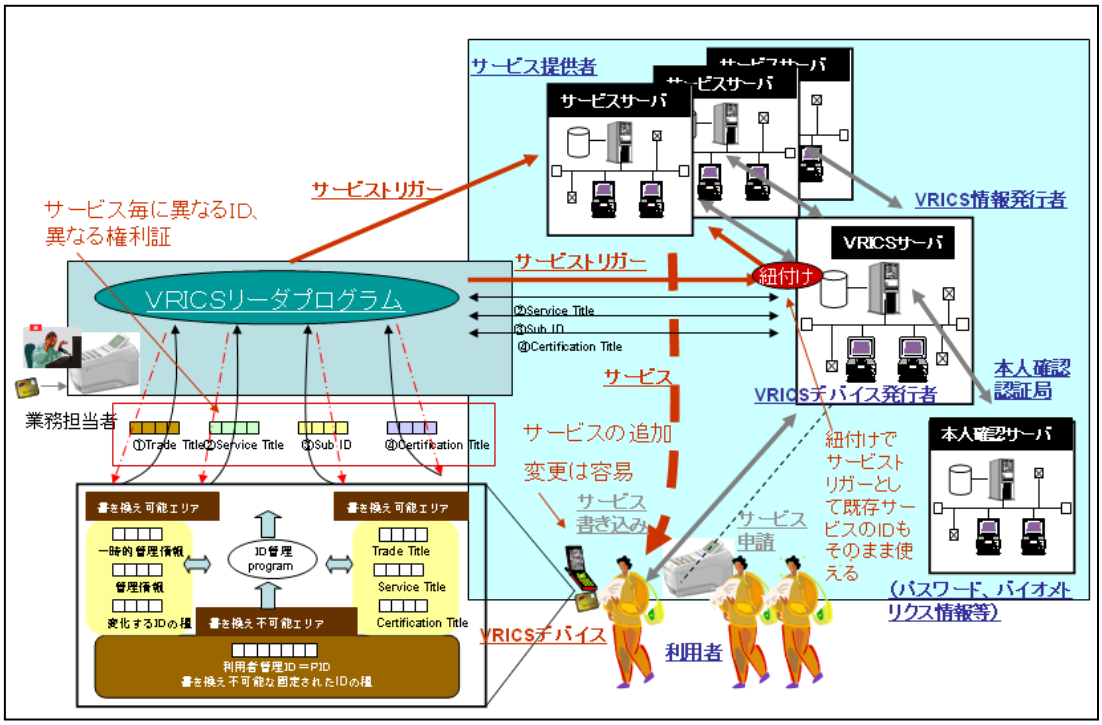


図 2-8　VRICS 認証フロー

また VRICS では、図 2-9 に示す認証パターンを利用し複数の Service Title と複数の SubID で 1 つのサービスを提供することも可能となっている。これにより、権利・権限管理におけるルート制御や権利のグルーピング管理、カードアクセスにおけるセキュリティ強度の向上も可能となっている。

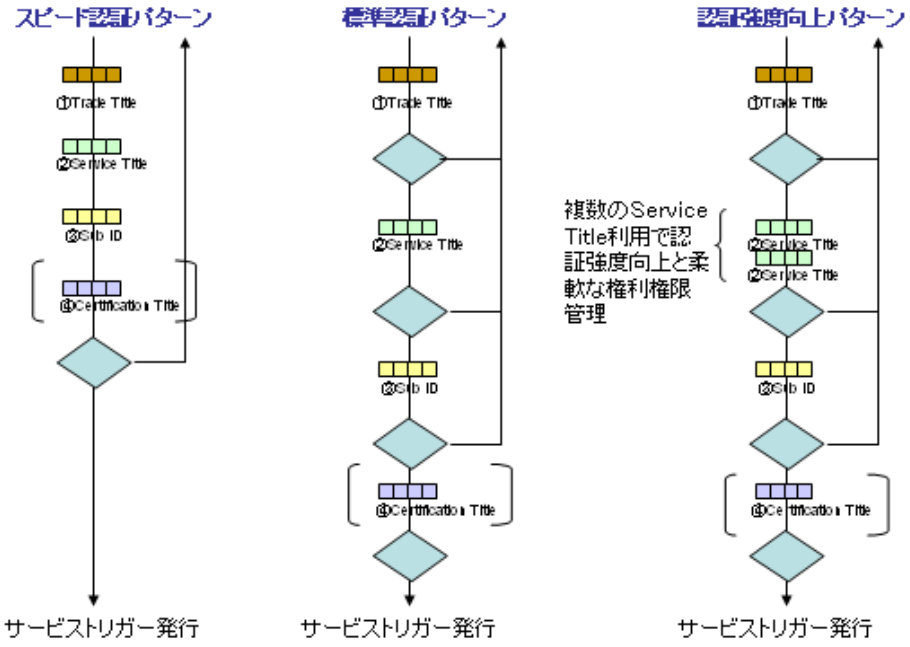


図 2-9　VRICS の認証パターン

2.6. 実験について

本節では実験の進め方について説明する。まず、本実験での品質レベルの考え方について説明し、次に、安全性とセキュリティの同時認証を行うために構築したプロセスについて説明する。最後に構築したプロセスを用いた同時認証の実験の手順について説明する。

2.6.1. 品質レベルの考え方

本実験では、システムに求められる品質水準のレベルを表す概念として品質レベルという語彙を当てている。本実験において、IEC 61508 と ISO/IEC 15408 の 2 つの異なる規格が利用されるが、それらの規格は異なる品質レベルが定義されており、その正確な呼称も異なる。(「表 2-10　品質レベル」参照)

規格	品質レベルの呼称	レベル
ISO/IEC 15408	評価保証レベル (EAL (Evaluation Assurance Level))	EAL 1 ~ EAL 7
IEC 61508	安全度水準 (Safety Integrity Level)	SIL 1 ~ SIL 4

表 2-10　品質レベル

品質レベルの考え方は、リスク (セキュリティの場合には脅威) の評価方法に密接に関連し、規格毎に異なる (各品質レベルの定義は 2.2 節を参照)。

本実験では以下の表 (表 2-11) のように品質レベルを定義している。安全度水準はリス

ク決定後、対抗策の検討がなされ決定される。そのため安全度水準を特定せずに品質レベルを設定している。

品質レベル	セキュリティ	安全性
0	EAL 1	SIL 1~4
1	EAL 2	SIL 1~4
2	EAL 3	SIL 1~4
3	EAL 4	SIL 1~4

表 2-11. 本実験における品質レベルの定義

本実験で設定する品質レベルであるが、事前に特定のレベルを設定し、その認証にかかる工数を算定するのではなく、品質レベルはあくまでSafSecの評価のための基準として利用した。本実験は、開発者サイドから、どのような方法で安全度水準を設定できるかに重点を置き実施した。

2.6.2. 同時認証プロセスの構築

本実験においては、システムの品質の中でも安全性とセキュリティの同時認証に関する分析・評価・認証方法論に対する文献調査を行い、その結果を踏まえて実験で基礎とする方法論を選択した。文献調査の結果、方法論としては英国防衛省からの委託により英国 Altran Praxis 社が実施した、将来の航空機におけるセキュリティと安全性を同時に認証する方法論である SafSecを参考にしてプロセスを構築した。SafSecにおいては、安全性に対しては英国の防衛関係の規格である Defense Standard 00-56（参考文献[16]）とセキュリティは CC を利用している。本実験においては、セキュリティの認証に関しては 2.2.1 節で説明したCCを用いた。すでに説明したようにCCは幅広い製品のセキュリティ評価・認証に利用されており、本実験で対象としたVRICSと同等のモバイル Felica IC チップファームウェア（T6N版）の認証も行っていることからこれを採用した。一方、安全性に関する機能安全規格は様々存在しているが 2.5.節で述べたようにVRICSが利用されるサービスは多岐にわたるため、特定の製品に特化した製品の機能安全規格ではなく、より汎用性の高い2.2.2節で説明した機能安全規格のベース規格であるIEC 61508を用いるのが妥当であると考え採用した。

まず構築したプロセスの基となる SafSec について説明する。SafSec ではどのように安全性とセキュリティ分析の作業共有化が行われるかを、リスク分析プロセスを例に示す（図 2-10 参照）。通常、安全性の分析のためにはハザード（危険の原因）を同定し、リスクの評価を行う。それに対して、セキュリティでは、脅威を同定し、脅威の保護すべき資産に対するリスクの評価を行う。そして、分析においては、安全性に関する部分は、安全に関す

る専門家が分析を実施し、セキュリティに関する部分については、セキュリティの専門家が分析を実施する。そして、その結果を持ち寄り、「ロスと操作性の調査打ち合わせ（loss and operability study meeting、3 章では LossOp Study Meeting と略記）」において重複性の排除を行う。

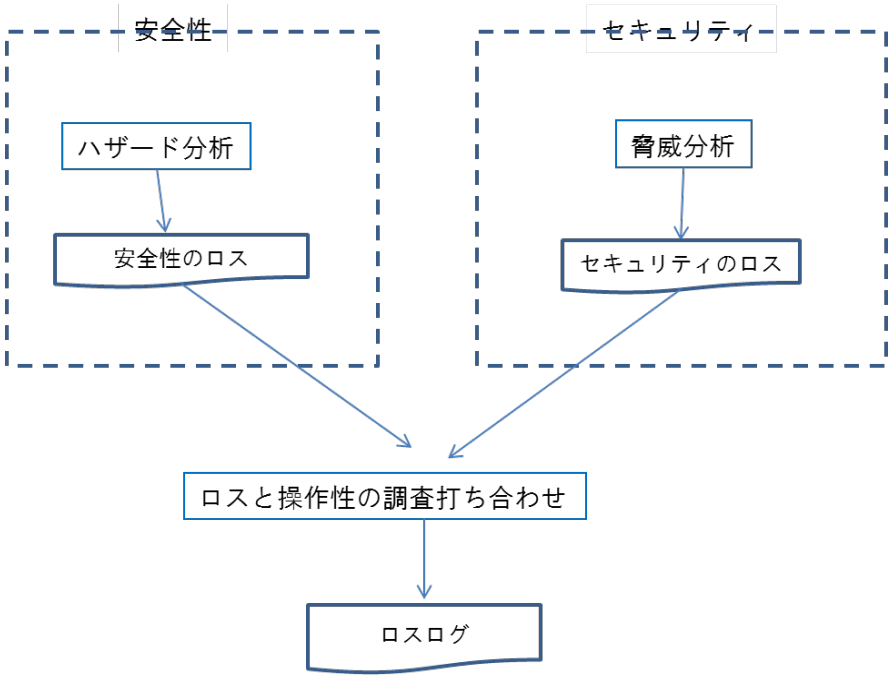


図 2-10　SafSec における安全分析と脅威分析の統合

SafSec においては、ハザードや脅威をロス（loss）という用語を用いて表す。ロスと操作性の調査打ち合わせの結果、重複性が排除されたロスの一覧表（ロスログと呼ぶ）を作成し、各ロスについての深刻度（Severity）や頻度（likelihood）を評価し、それらを基にリスクを決定する。

以上のように SafSec に基づいて、詳細なアクティビティを加えることにより同時認証プロセスを構築した。構築したプロセスを図 2-11 に示す。加えたアクティビティは安全性、セキュリティそれぞれに関して達成すべきと考えられる目標を明確にする「安全性、セキュリティ予備ゴールの設定」（安全、セキュリティの目標のこと分析結果により更新が行われるため予備ゴールと呼ぶ）、対象システムの部品やその構成を明確にする「アイテム定義」などである。ここでは、「インパクト分析」、「原因（Causal）分析」など丸四角がプロセスに当たり角四角が分析結果などの成果物である。同図の破線で囲まれた部分を 1 つのまとまりとし、それぞれについて 3.1 及び 3.2 節で説明する。

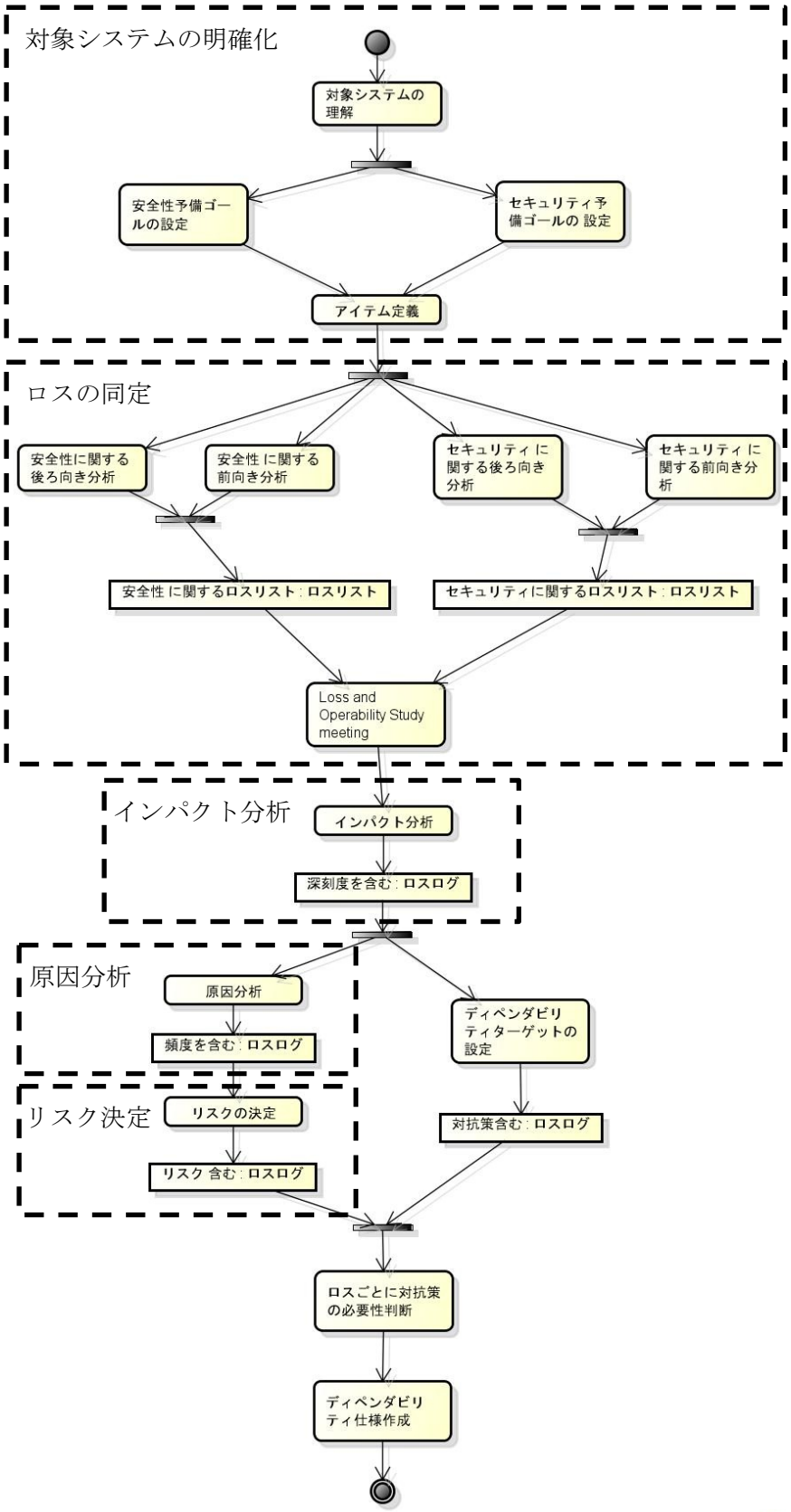


図 2-11　SafSec に基づくプロセス

2.6.3. 実験の手順

本実験は以下の手順で実施した。

1. 構築したプロセスの試行とコストの記録
   (ア) 対象システム（入退室管理システム）の明確化工程
   (イ) 各種分析工程
2. 記録したコストを基に削減できるコストの推察

という手順で行った以下でそれぞれの概要を説明する。

構築したプロセスの試行とコスト記録

一般的に安全性、セキュリティなどのシステムの品質を分析する際には、分析対象の範囲やアーキテクチャなどを明確にしなくてはならない。そのために対象システムの理解、品質のゴール設定、対象システムのアイテム定義などが分析工程の一部として行われる。本実験は 2.5 節で説明した対象システム VRICS を利用したサービスの 1 つである建物等の「入退室管理システム」を取り上げ、その仕様等を想定して実施した。この対象システムの明確化について 3.1 節で述べる。

対象システムの明確の後にシステムのロスを同定しリスクの決定を行った。その際に「ロス(ハザード、脅威)分析」、「各ロスのインパクト分析」、「各ロスの原因分析」といった分析を実施した。これらの分析を行うための方法論は様々存在しており、その目的に合わせて適宜用いるべきである。本実験では 2.6.2 節で記載した同時認証プロセスに従い分析作業を実施した。また、プロセスの試行時にはその評価のためにそれぞれの工程で要したコストを記録する。

記録したコストを基に削減できるコストの推察

構築した同時認証プロセスが同時認証プロセスを用いない場合と比べどのくらいのコストを削減できるかを見積もる。同時認証プロセスはその試行時に各工程でのコストを計測しているが、同時認証プロセスを用いない場合の試行は行っていない。そこで、比較をするために同時認証を用いないプロセスも構築し、そこで必要となるコストは同時認証プロセスのコストを基に予測した。予測方法や比較による結果については 3.4 節で説明している。

3. 模擬実験

本章では 2.6 節で述べた実験手順に従い、その内容と分析結果（実験結果ではなく中間成果物である）、実験の結果（品質レベル、削減コスト、規格によるまとめ）について述べる。

3.1. 対象システム（入退室管理システム）の明確化

今回の実験では、セキュリティと安全性の両者が関係する IC カードシステムを利用したサービスのうち、建物等の「入退室管理システム」を取り上げその仕様を想定し実施した。ここでは、分析を実施するために明確化された対象システムについて説明する。

入退室管理システムは具体的には、大学や企業等の建物に対して、予め入場を許可された個人に対して、IC カードによって本人認証を行う。入室権限のないもの、特に、悪意のあるものを入場させないことなどがセキュリティで確保すべき性質である。また、地震等の大規模災害時には、外部の公共情報システムからの情報を利用し、特別に鍵を解放する機能も想定する。この機能が適切に働くことが安全性で確保すべき性質とする。システムの全体像を 図 3-1 のユースケース図に示す。

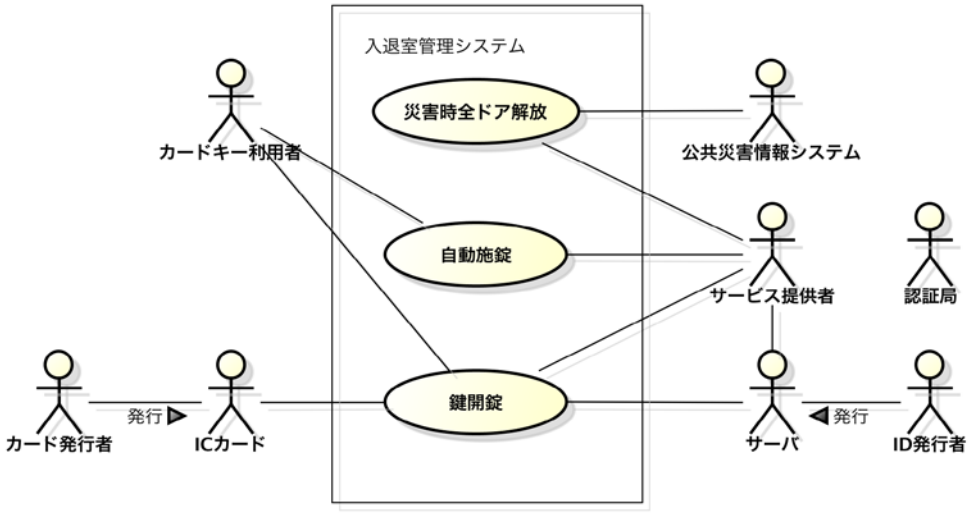


図 3-1 入退室管理システム概要 ユースケース図

人型の記号が、システム外部の主体を表す。システムに直接関係する外部の主体は、カードキー利用者、IC カード、サービス提供者、サーバ、公共情報システムである。サービス提供者は、この入退室管理システムを提供している組織を想定する。また、サーバは、IC カードの認証に利用される。システムの概要を次の 3 つのユースケースに対応付けられたシナリオよって説明する。システムは、その構成要素として、ドア部、カードリーダ/ライタ部、外部サーバなどと通信する施錠装置端末部からなる。

・鍵開錠

1. カードキー利用者が正しい IC カードをドアの近くに設置されたカードリーダ/ライタにかざす
2. IC カード情報が施錠装置端末に送信される
3. サーバと施錠装置端末間で認証が行われる
4. 認証が OK であれば解錠する

ここで、悪意のある者が、正しくない IC カードをかざした場合には、解錠しない。送信される IC カード情報については、このあとのデータフロー図によって説明する。

・自動施錠

1. カードキー利用者がドアを閉める
2. 施錠装置端末が、ドアが閉まったことを感知
3. 一定時間経過後、施錠装置端末が施錠する

既に入場している者は、入場時に正しく認証が行われたことを想定し、退場時には認証は求めない。

・緊急時開錠

1. 災害（地震、火災、洪水など）が発生
2. 施錠装置端末が公共災害情報を取得
3. 全ての鍵を開錠し自動施錠をしない

ユースケース図では、認証局も主体としているが、認証局は高度な個人認証を行うために必要となる。しかし、今回想定しているシステムはそのような個人認証は行わないために、直接関係する主体ではない。

次に、システムが外部とどのような情報のやり取りを行うかを示すため、入退室管理システム全体を表す唯一のプロセスをもつデータフロー図を図 3-2 に示す。丸いノードがデータ処理を表し、長方形ノードは、外部主体、平行線で示されたノードはデータベースを表す。

IC カードをカードリーダ/ライタにかざした後は、システムの方からどのようなデータが必要かのリクエストを送る。IC カードから送られる情報には、その IC カードがもつ「資格証」や「権利証」、今回の入退室管理システムのために割り振られた「サービス毎の固有 ID」がある。この中では、資格証と権利証のデータは、入退室管理システムがデータベー

スをもっており、照合などが行われる。サービス毎のカード識別 ID に関しては、サーバまで情報を送り、認証を行う。

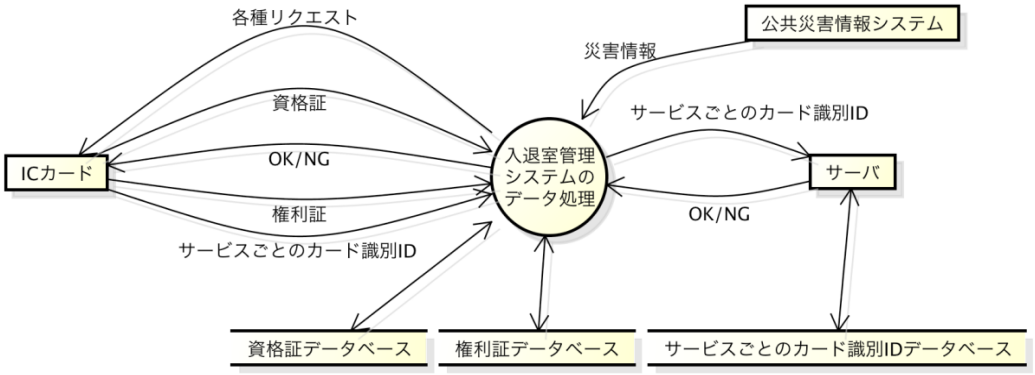


図 3-2 データの流れからみた入退室管理システムの概要（データフロー図）

次に、システムのハードウェア構成とソフトウェアモジュールの構成とその配置を説明するため、配置図を図 3-3 に示す。前述したとおり、入退室管理システムは、大きく以下の 3 つのコンポーネントからなる。配置図では、通常の四角形がハードウェア部品を表し、左上に記号のようなものが存在する四角形がソフトウェア部品（ソフトウェアコンポーネント、ソフトウェアモジュール、データなど）を表す。

1. **ドア部**
2. **リーダ/ライタ部**
3. **施錠装置端末部**

これら以外に図に現れる「IC カード」、「公共災害情報システム」、「サーバ」はすべてユースケース図にも現れた、直接関係する外部主体である。ドア部には、ドアの鍵そのものや、鍵の開閉を検知可能なドアセンサーが含まれる。リーダ/ライタ部には、無線通信のためのリーダ/ライタアンテナが含まれる。入退室管理システムのソフトウェアは、上の 3 つの中では施錠装置端末部に配置され、主なモジュールとして、IC カードとの通信や認証処理を担う「IC カード認証通信」、サーバとの通信を担う「サーバ通信」、鍵を制御する「鍵コントロール」、災害情報の受信や処理を担う「災害情報受信」の 4 つを想定する。

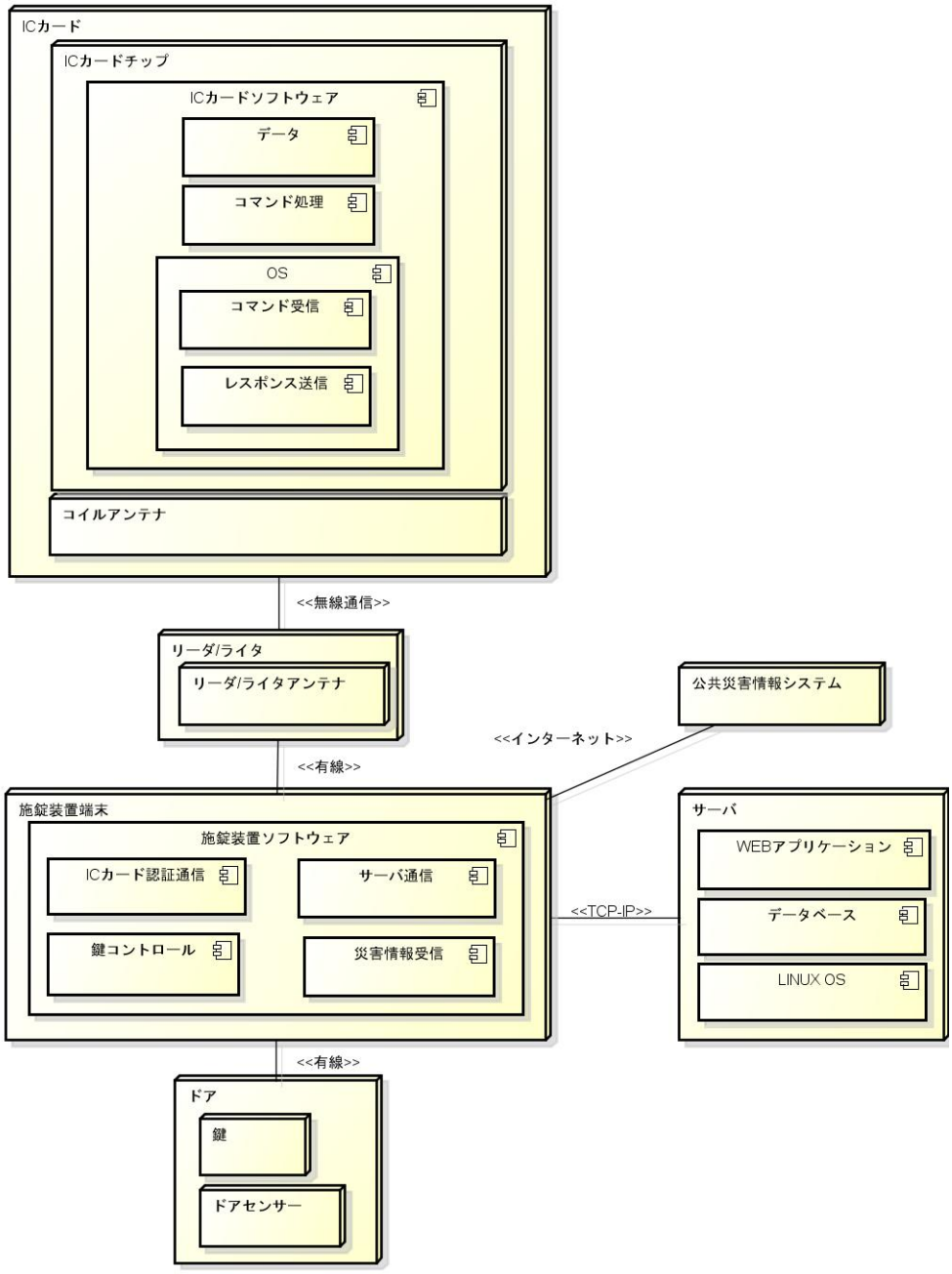


図 3-3　ハードウェア構成とソフトウェアモジュールの構成から見た
入退室管理システムの概要　(配置図)

3.2. 分析

本模擬実験では、リスク分析を中心に行い、（ディペンダビリティ）機能要件、目標の分析、獲得は対象外としているので、本プロセスにおけるリスクの決定までが範囲である。品質レベルを考えると、リスクの決定が品質レベルの決定の要因であるので、対象範囲としては妥当であると考える。ここではロスを同定するための安全性におけるハザード、セキュリティにおける脅威の分析（以下ロスの分析と呼ぶ)、同定されたロスに対しその頻度を評価するための原因分析と影響（深刻度）を評価するためのインパクト分析、さらに分析結果から各ロスに対するリスクの決定、以上の方法と内容について述べる。

3.2.1. ロスの同定

ロスの同定はすでに述べたように安全性、セキュリティでそれぞれのロスの分析を実施し、そこで同定されたロスをLossOp Study Meetingで統合するというプロセスになる。統合までの分析は、セキュリティに関しては九州大学で、安全性に関しては弊社（シーエーブイテクノロジーズ社）で実施した。これは、安全性に関する専門家とセキュリティに関する専門家を 2 名用意し、個別に作業を実施するというプロセスを忠実に実行したものである。

安全性、セキュリティそれぞれで実施するロスの分析についてその概要と分析結果を説明する。

まず初めに安全性、セキュリティ双方の観点から達成すべきゴールをそれぞれで決定した。安全性に関しては、

(Saf1) 許可された人が入退室できる
(Saf2) 許可されていない人が入退室できない
(Saf3) 災害時全ドアを無条件解放する

という 3 つのゴールを設定した。

セキュリティに関しては、

(Sec1) なりすましやスキミング等、悪意ある情報詐取ができない
(Sec2) 各サービスの情報漏えいが他のサービスに影響しない
(Sec3) 悪意あるプログラム破壊や情報の書き込み、消去ができない

という 3 つのゴールを設定した。

次に各ロスを同定するために行う後ろ向き分析を行うためには対象システムにどのようなアイテム（部品）があるか明確にしなくてはならない。もしあいまいなまま実施すると、考慮漏れが生じる可能性がある。そのため、3.1 節で説明した配置図（図 3-3）を作成し、対象システムのアイテム定義を行った。

その後、安全性とセキュリティの予備ゴールに至るシナリオを定義した。このシナリオはロスを同定するための前向き分析に必要となる。

3.2.2. ハザード、脅威の分析

本模擬実験では、安全性とセキュリティそれぞれでロスを同定する際に FMEA と FTA を用いた。まず、対象システムのアイテム定義で作成した配置図を基に、FMEA を実施した。

FMEA はもともとハードウェアを対象とした手法であり、ソフトウェアに適用した例はそれほど多くない。対象システムでソフトウェアはシステムコマンド、MIID コマンドという二種類の命令送受信、保持しているデータに対しコマンドに対応する処理を実施、処理結果をレスポンス（ack）として送受信する。各コマンド、レスポンスには

- 内容
- データ
- パラメータ

が含まれている。そこで、ソフトウェアの故障モードとして以下のものを用いた。

- 誤って受信される
- 誤って送信される
- 受信しない
- 送信しない
- 処理間違い
- データ間違い

故障モードから考えられた影響を基に、システムがどのような状態になっているかを記述しハザード候補とした。このハザード候補をまとめたものを安全性のロス（ハザード）として採用している。以下に示す表（表 3-1）は、安全性のロス（ハザード）同定のための FMEA 表である。以下の票では対策の項目が記述されていない。これは、本模擬実験では対策の検討については対象外であるためであり、実際の開発では検討後にその結果が記録される。

分析対象部品	故障モード			影響	対策	ハザード候補
IC カードソフトウェア	受信失敗	コマンドを誤って受信	システムコマンド	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		IC カードデータ不整合
			MIID コマンド	意図しない処理を実行され意図しないレスポンスになる。安全目標(1),(2)が破綻		IC カードが間違った処理をする
		パラメータを誤って受信	システムコマンド	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		IC カードデータ不整合
			MIID コマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		IC カードの処理と異なる結果を送信
		受信しない	システムコマンド	IC カードが反応せず案是目標(1)が破綻する		IC カードが反応しない
			MIID コマンド	IC カードが反応せず案是目標(1)		IC カードが反応しない

				が破綻する		
施錠装置ソフトウェア IC カード認証通信	コマンド送信	コマンドを誤って送信	システムコマンド	IC カードに誤ったシステムコマンドを送信してしまい、カードの意図する機能が損なわれる。安全目標(1),(2)が破綻する		IC カードデータ不整合

表 3-1　安全性のロス（ハザード）同定のための FMEA の一部

以下のように、FTA を実施した。トップ事象から詳細化してどのような部品の故障があるかを分析することにより、FMEA での考慮漏れを防止することが目的である。

FTA のトップ事象として「許可されていない人が入退室できる」のように安全性、セキュリティのゴールを否定したものを採用した。

トップゴールから安全シナリオ、配置図を基に網羅的に詳細化していき部品の故障まで詳細化を行っている。FTA で作成された詳細化を示すツリーを図 3-4 に示す。

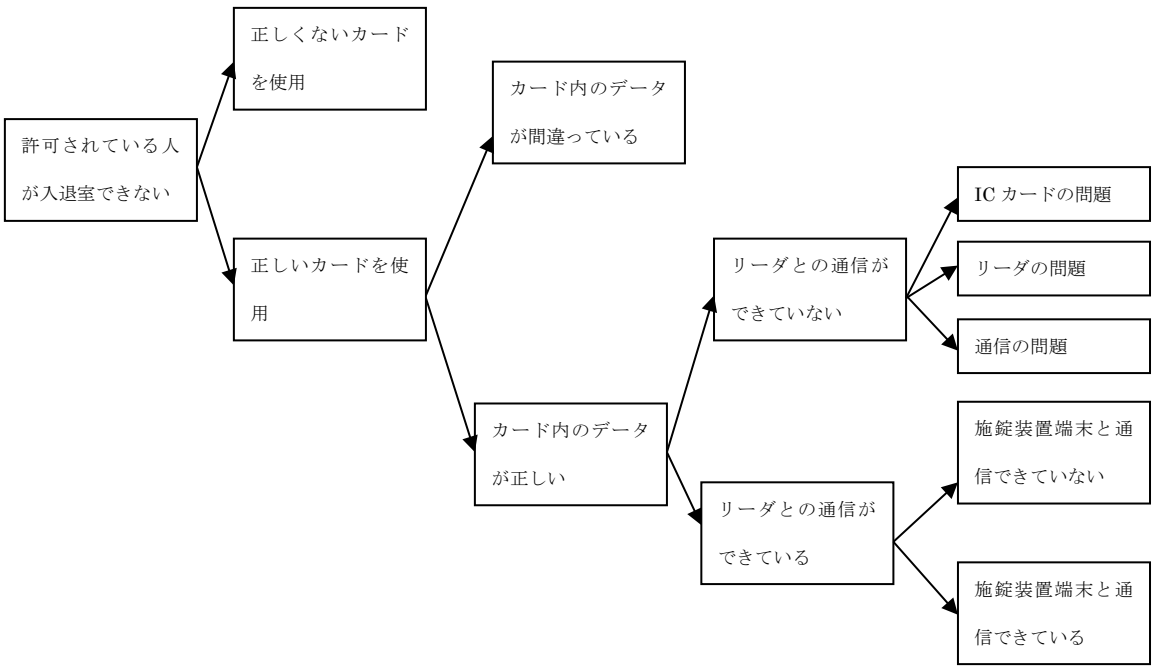


図 3-4　安全性のロス（ハザード）同定のための FTA の例

セキュリティに関しても同様に後ろ向き、前向き分析を実施した。

以上の後ろ向き、前向き分析から安全性に関して 27 件、セキュリティに関して 10 件のロスが同定された。これらをそれぞれ、表 3-2、表 3-3 に示す。ロスはこれらの表が示すように、ID とラベルという情報を含んでいる。なお、施錠装置端末の鍵コントロール、ドア、公共災害情報システム等に関する部分はサービスであり基盤システムの範囲ではない、またサービスは本模擬実験の為に想定した部分であり、物理的なセキュリティについても考慮する必要があるため、本模擬実験ではその部分の脅威分析を行っていない。サービス部分に関しても脅威分析を実施すればさらに多くのセキュリティのロスが同定されることが予想される。

セーフティロス ID	セーフティロスラベル
Saf1	IC カードデータ不整合
Saf2	IC カードが間違った処理をする
Saf3	IC カードの処理と異なる結果を送信
Saf4	IC カードが反応しない
Saf5	IC カード処理停止
Saf6	IC カードレスポンス内容間違い
Saf7	IC カードが破損している
Saf8	IC カードへ意図しないシステムコマンド送信
Saf9	IC カードへ意図しない処理を命令
Saf10	リーダ/ライタが反応しない
Saf11	IC カード処理結果の誤認
Saf12	システムが反応しない
Saf13	災害情報無受信
Saf14	災害情報誤認
Saf15	ドアセンサー故障
Saf16	施錠しない
Saf17	物理的に鍵が開かない
Saf18	ドア状態認識しない
Saf19	通信時間不十分
Saf20	電源喪失
Saf21	サーバ受信認証データの誤り
Saf22	サーバ受信認証データの破損
Saf23	サーバと通信ができない
Saf24	認証データの取り違え
Saf25	認証データの送信間違い
Saf26	認証データの破損
Saf27	認証結果間違い

表 3-2　同定された安全性のロス

セキュリティロス ID	セキュリティロスラベル
Sec1	不正コマンドデータによるアクセス
Sec2	不正取得したコマンドデータによるアクセス
Sec3	盗聴・改ざんしたコマンドデータによるアクセス
Sec4	盗聴した情報から VRICS　Title データの暴露
Sec5	改ざんプログラムのインストール
Sec6	データアクセス中の電源途絶
Sec7	IC チップを故障させることによるセキュリティの危殆化
Sec8	プログラムによる侵入（サーバ攻撃）
Sec9	人による侵入
Sec10	盗聴・改ざんされた通信データによる侵入

表 3-3　同定されたセキュリティのロス

また、同定されたセキュリティロスとモバイル Felica のセキュリティターゲット（参考文献[17]）の脅威分類との関連を表 3-4 に示す。

モバイル Felica の T.Abuse_ReaderWriter_SecurityFunction という脅威分類に関しては本対象システムにそのような機能がないために対応していない。

セキュリティロス ID	モバイル Felica セキュリティターゲットの脅威分類との対応
Sec1	T.Abuse_Command_Data
Sec2	T.Reuse_Command_Data
Sec3	T.Intercept_Communicate_Data
Sec4	T.Intercept_セキュリティ_Data
Sec5	T.Install_EvilProgram
Sec6	T.Interrupt_Power
Sec7	T.Break_Hardware
Sec8	なし
Sec9	なし
Sec10	T.Intercept_Communicate_Data

表 3-4　同定されたセキュリティロスとモバイル Felica セキュリティターゲットの脅威分類の対応

本分析結果の十分性については「3.5.実験結果」を参照されたい。

3.2.3. LossOp Study Meeting

本工程は安全性とセキュリティそれぞれで同定されたロスを統合する工程である。まず始めにそれぞれに同定したロスについてどこで起こるのか、どのような内容なのかというロスの概要の説明を行う。その後、各ロスについて重複、関連がないかを議論する。関連とは安全性を確保することでセキュリティも保たれる（またはその逆）場合や安全性とセキュリティが衝突する場合などである。重複や関連があるロスについてはどのように対処するのかも議論する。最後に議論の結果、統合したロスをロスログとしてまとめる。

ロスログはここでの議論の結果のほかに今後の分析結果も入れて更新していくために、以下のような情報を記述できるようにすべきである。

- ID
- ラベル
- 頻度
- 深刻度
- 原因
- 影響
- 対応策
- リスクレベル
- 関連するシステム特性
- ロスの基となるハザードや脅威へのトレース

本実験では安全性、セキュリティそれぞれ 3 件のロスが重複しているという結論に至った。重複した 3 件は

a. 正しくないコマンドデータによる IC カードへのアクセス
b. IC カードデータアクセス中の電源途絶
c. 不正な通信データによるサーバへのアクセス

である。これらは悪意のある攻撃を想定した対策を行うことにより、ミスユースなど意図しないことが原因となる場合も防ぐことが可能になる。そのため、これらのロスは安全性、セキュリティ双方に関連するが、分析等の実施はセキュリティとして行った。

本工程（ロスの統合）で作成されたロスログを表 3-5 に示す。本工程の終了時にはロス ID、ロスラベル以外の情報はまだ空であるため、表 3-5 はロス ID とロスラベルの部分のみを記載している。

ロス ID	ロスラベル
Loss1	IC カードデータ不整合
Loss2	IC カードが間違った処理をする
Loss3	IC カードの処理と異なる結果を送信
Loss4	IC カードが反応しない
Loss5	IC カード処理停止
Loss6	IC カードレスポンス内容間違い
Loss7	IC カードが破損している
Loss8	IC カードへ意図しない処理を命令
Loss9	リーダ/ライタが反応しない
Loss10	IC カード処理結果の誤認
Loss11	システムが反応しない
Loss12	災害情報無受信
Loss13	災害情報誤認
Loss14	ドアセンサー故障
Loss15	施錠しない
Loss16	物理的に鍵が開かない
Loss17	ドア状態認識しない
Loss18	通信時間不十分
Loss19	サーバ受信認証データの誤り
Loss20	サーバ受信認証データの破損
Loss21	サーバと通信ができない
Loss22	サーバで認証データの取り違え
Loss23	サーバで認証データの送信間違い
Loss24	認証結果間違い
Loss25	不正コマンドデータによるアクセス
Loss26	不正取得したコマンドデータによるアクセス
Loss27	盗聴・改ざんしたコマンドデータによるアクセス
Loss28	盗聴した情報から VRICS　Title データの暴露
Loss29	改ざんプログラムのインストール
Loss30	データアクセス中の電源途絶
Loss31	IC チップを故障させることによるセキュリティの危殆化
Loss32	プログラムによる侵入（サーバ攻撃）
Loss33	人による侵入
Loss34	盗聴・改ざんされた通信データによる侵入

表 3-5 ロスログ

3.2.4. インパクト分析

インパクト分析は各ロスが導く結果を分析し、その深刻度を評価する工程である。ここではロス毎に影響する範囲（カードの枚数、ドアの数、人の数）と、それにより破綻する安全目標を列挙した。

インパクトは IEC 61508 Part 5 Annex C にあるクラスをセキュリティに拡張した。本模擬実験で使用したインパクトクラスを表 3-6 に示す。

クラス	安全性	セキュリティ
非常に深刻	多数の人が死亡	大量の情報流出、基盤全体の情報破壊
重大	人が死亡、多数の人が怪我	一部の情報流出、サービス情報の破壊
軽微	人が怪我	個人情報の破壊
無視できる	被害なし	被害なし

表 3-6　インパクトクラス

インパクト分析の結果を基にロスにインパクトクラスを割り当てていく。セキュリティに関してはインパクトクラスの表に従い割り当てを行った。しかし、安全性に関しては一部を除いて人の被害ではないものを安全性とみなして実施している。そこで、インパクトクラスの割り当ては、影響範囲が特定の場合かつ安全目標 1 つが破綻のとき軽微、どちらかが複数の場合は重大、実際に人の被害があるものは非常に深刻とした。表 3-7 がインパクト分析の内容である。

ロス	影響範囲	破綻する安全目標	深刻度
IC カードデータ不整合	特定のカード	安全目標(1),(2)	重大
・ ・ ・			
システムが反応しない	特定のドア	(1),(2)	重大
災害情報無受信	複数の人	(3)	非常に深刻
災害情報誤認	複数のドアまたは複数の人	(3)	非常に深刻
ドアセンサー故障	特定のドア	(2)	軽微
施錠しない	特定のドア	(2)	軽微
鍵が開かない	複数のカード	(1)	重大

表 3-7　インパクト分析内容の例

3.2.5. 原因分析

原因分析は各ロスが起こる頻度を評価する工程である。ここではロスが起こる原因を FTA により基本事象に詳細化する。基本事象の頻度を求め、詳細化を逆にたどり頻度を統合しロスの頻度を求めた。今回作成した木構造は子の 1 つが起こると親が起こるという OR の関係にしている。表 3-8 にロスの原因分析の詳細化部分を示す。

ロス	対象部品				発生頻度とその統合
IC カードの処理と異なる結果を送信	IC カード	ソフトウェア	OS	レスポンス送信	ほとんどない
IC カードが反応しない	IC カード	ソフトウェア	OS	コマンド受信	ほとんどない
				レスポンス送信	ほとんどない
			コマンド処理		時折
		ハードウェア	コイルアンテナ		ほとんどない
			IC チップ		ほとんどない
通信時間不十分	IC カード	ソフトウェア	コマンド処理		時折
			OS	コマンド受信	ほとんどない
				レスポンス送信	ほとんどない
	施錠装置	リーダ/ライタアンテナ			時折
		IC カード認証通信			ほとんどない

表 3-8　ロスの原因分析（詳細化）例

頻度は IEC 61508 Part 5 Annex C にあるクラスをセキュリティに拡張した。安全性に関してはその起こりやすさ、セキュリティに関しては攻撃のしやすさを基に、以下に示すような頻度クラスを作成した。ソフトウェアはハードウェアと異なりその故障は決定論的故障である。そこで、ソフトウェアの故障頻度はその検証にどのような手法を用いるかということで分類した。例えば、ソフトウェアの検証が経験などに基づいた場当たり的なテストである場合は不具合が含まれる可能性が高く、形式手法などを用いた検証を行っていれば不具合が含まれる可能性が低いと考えられる。作成した頻度クラスを表 3-9 に示す。

クラス	安全性	セキュリティ
頻繁	頻繁	セキュリティ対策していない
かなり	かなり	簡単
時折	時折	可能である
ほとんどない	ほとんどない	困難
ありそうもない	ありそうもない	非常に困難
信じられない	信じられない	不可能

表 3-9　頻度クラス

本実験ではこの頻度はハードウェア、ソフトウェア共に仮のものを考えて実施している。実際の開発では、ハードウェアの故障率を調査することや、ソフトウェア検証で用いる手法を適宜選択することが必要である。

また、頻度の合成は

- より上の頻度を採用する
- 単一部品内での同じ頻度クラスの合成は 3 つ以上で 1 つ上の頻度に
- 複数部品にわたる同じ頻度クラスの合成は 2 つ以上で 1 つ上の頻度に

ということを基本ルールとして実施した。実際の開発ではハードウェアの故障率であればその確率計算によって求めるべきであり、ソフトウェア間やソフトウェアとハードウェア間に関しては適宜ルールを作成する必要がある。

表 3-10 に頻度の統合部分を示す（本表は詳細化部分の後半となる)。

<table>
<tr><td>ロス</td><td colspan="4">発生頻度とその統合</td><td>頻度</td></tr>
<tr><td>IC カードの処理と異なる結果を送信</td><td colspan="4">ほとんどない</td><td>ほとんどない</td></tr>
<tr><td rowspan="5">IC カードが反応しない</td><td>ほとんどない</td><td rowspan="2">ほとんどない</td><td rowspan="2">時折</td><td rowspan="5">時折</td><td rowspan="5">時折</td></tr>
<tr><td>ほとんどない</td></tr>
<tr><td colspan="2">時折</td></tr>
<tr><td>ほとんどない</td><td colspan="2" rowspan="2">ほとんどない</td></tr>
<tr><td>ほとんどない</td></tr>
<tr><td rowspan="5">通信時間不十分</td><td colspan="2">時折</td><td rowspan="3">時折</td><td rowspan="5">かなり</td><td rowspan="5">かなり</td></tr>
<tr><td>ほとんどない</td><td rowspan="2">ほとんどない</td></tr>
<tr><td>ほとんどない</td></tr>
<tr><td>時折</td><td colspan="2" rowspan="2">時折</td></tr>
<tr><td>ほとんどない</td></tr>
</table>

表 3-10　ロスの原因分析（頻度統合）例

3.2.6. リスクの決定

各ロスのリスクはこれまでに実施されたインパクト分析、原因分析から得られた深刻度、頻度から決定される。本模擬実験では議論の結果 IEC 61508 Part 5 Annex C のリスククラス（表 3-11）とリスク決定表（表 3-12）を用いた。

リスク等級	解説
I	受容不可能なリスク
II	望ましくないリスク(リスク低減は実行不可能、改善効果と極めて不釣り合いなコストがかかる場合に受容可能)
III	リスク低減にかかるコストが改善効果を上回る場合は受容可能なリスク
IV	無視してよいリスク

表 3-11　リスククラス

頻度	結果			
	壊滅的	重大	軽微	無視してよい
頻繁	I	I	I	II
かなり	I	I	II	III
時折	I	II	III	III
ほとんど無い	II	III	III	IV
ありそうもない	III	III	IV	IV
信じがたい	IV	IV	IV	IV

表 3-12　リスク決定表

これにより同定したロスそれぞれに対しリスクの決定をした､その結果を表 3-13 に示す。安全性においてロスのリスクが決定され、対抗策の目標・検討が行われることにより安全度水準の決定が可能となる。その安全度水準の決定には、ここまでの分析によって得られた頻度を「ロスが起きた時に危険な場所にいる確率」､「起こった危険に対する回避可能性」､「ロスが起こる可能性」によって詳細化し、さらに深刻度と合わせ、2.2.2. 節のリスクグラフ手法を用いることで決定することができ、SIL 1~4 に対応可能である。

ロス ID	ロスラベル	頻度	**深刻度**	ロスの原因	ロスの影響	関連するシステム特性	対応策	安全性ロス ID	セキュリティロス ID	リスククラス
Loss1	IC カードデータ不整合	時折	重大	IC カードソフトウェアのデータ	特定のカードの安全目標(1),(2)	Safety		Saf1		II
Loss2	IC カードが間違った処理をする	時折	重大	IC カードソフトウェアのコマンド処理	特定のカードの安全目標(1),(2)	Safety		Saf2		II
Loss3	IC カードの処理と異なる結果を送信	ほとんどない	重大	IC カードソフトウェア OS のレスポンス送信	特定のカードの安全目標(1),(2)	Safety		Saf3		III
Loss28	盗聴した情報から VRICS Title データの暴露	非常に困難	一部の情報	スキミング	認証システム信頼	セキュリティ			Sec4	III

					性低下					
Loss29	改ざんプログラムのインストール	非常に困難	一部の情報		保護データ情報漏洩・破壊	セキュリティ			Sec5	III
Loss30	データアクセス中の電源途絶	簡単	情報破壊	電断、磁界断絶	カードデータの破壊・消滅	Safety, セキュリティ(セキュリティによりSafetyが保たれる)		Saf20	Sec6	II
Loss31	IC チップを故障させることによるセキュリティの危殆化	非常に困難	一部の情報		保護データ情報漏洩・破壊	セキュリティ			Sec7	III

表 3-13　ロスログ例

3.3. 実施コスト

本実験実施において、分析の各プロセスの工数を記録した。この工数を基に、調査、検討し用いた安全性とセキュリティの同時認証の方法論により、どの程度重複を排除でき、コストの削減が可能となるかを見積もる。また、この方法論の効果を評価する。

ディペンダビリティ仕様が得るために以下の成果物が必要である。

1. ロスの同定
2. リスクの決定
3. ディペンダビリティターゲット（許容可能とする残存リスクと対抗策の目標）の設定
4. ディペンダビリティ仕様の作成

本模擬実験ではこのうち「1. ロスの同定」と「2. リスクの決定」が対象範囲である。こ

れらを実施するために必要となるアクティビティについて以下で説明する。

「1. ロスの同定」は安全性、セキュリティそれぞれの観点から

a. 対象システムの理解
b. 予備ゴールの設定
c. アイテム定義
d. 分析

というアクティビティを実施し、これによりリストアップされたロスを LossOp Study Meeting で統合するという手順になる。しかし、a. 対象システムの理解、c. アイテム定義の 2 つのアクティビティはシステム特性により変化することはなく、これらは同時に実施するのが良いと考えられる。

同定されたロスに対し「2. リスクの決定」を実施するには

a. ロスの影響を分析し深刻度を評価する（インパクト分析）
b. ロスの原因を分析し頻度を評価する（原因分析）
c. 深刻度、頻度からロスごとにリスクを決定する

また、本実験では分析など各アクティビティの実施時にはそこで発生したコストを記録している。本実験で各アクティビティにかかったコストは以下のようになる。（表 3-14 参照）

アクティビティ名	コスト（人時)
対象システムの理解	16
安全性予備ゴールの設定	3
セキュリティ予備ゴールの設定	2
アイテム定義	8
安全性に関する後ろ向き分析	8
安全性に関する前向き分析	7
セキュリティに関する後ろ向き分析	4
セキュリティに関する前向き分析	4
LossOp Study Meeting	4
インパクト分析	10
原因分析	11
リスクの決定	2
合計	79

表 3-14　アクティビティ実施コスト

3.4.　SafSec に基づかないプロセスでの工数の見積もり

一方、安全性とセキュリティの同時認証を考慮せずにそれぞれ実施した場合のプロセスを考える。安全性とセキュリティの統合はロスの同定（LossOp Study Meeting）ではなくディペンダビリティ仕様作成の直前に行うことになる。そのため、同時認証で統一して行われていたものが安全性、セキュリティ双方の観点で重複して実施されることになる。このプロセスをアクティビティ図で表したものが図 3-5 である。

本実験ではこのプロセスで分析等を実施していない。そこで、ここでかかるコストを同時認証のプロセスでかかったコストから見積もる必要がある。その方法を以下で示す。

統合前に安全性、セキュリティで同定されたロスはそれぞれ 27 件と 10 件であった。これにLossOp Study Meetingを実施することにより、3 件が安全性とセキュリティの両方ににかかわるロスであることが分かった。その後の分析等アクティビティは統合された全 34 件のロスに対して実施した。

そこでインパクト分析、原因分析、リスク決定に関して、ロス 1 件当たりの平均コストを計算し、安全性、セキュリティで同定されたロスの数を掛けることで見積もった。その結果が以下の表である。また、このプロセスではLossOp Study Meetingがなくなるが、最終的に行う「安全性仕様とセキュリティ仕様の矛盾解消」が加わるため、こちらに同じコストがかかったと仮定している。また、「対象システムの理解」、「アイテム定義」は安全性、セキュリティそれぞれで同じだけのコストがかかると仮定している。以下に見積もり

結果を表でまとめる。(表 3-15 参照)

	安全性 (人時)	セキュリティ(人時)
対象システムの理解	16	16
安全性予備ゴールの設定	3	0
セキュリティ予備ゴールの設定	0	2
アイテム定義	8	8
安全性に関する後ろ向き分析	8	0
安全性に関する前向き分析	7	0
セキュリティに関する後ろ向き分析	0	4
セキュリティに関する前向き分析	0	4
インパクト分析	7.94	2.94
原因分析	8.73	3.23
リスクの決定	1.58	0.58
安全性仕様とセキュリティ仕様の矛盾解消	4	
合計	105	

「LossOp Study Meeting」は SafSec に基づくプロセス特有であるため入っていない。統合の工程として「安全性仕様とセキュリティ仕様の矛盾解消」工程が加わっている。

表 3-15　コストの見積もり結果

以上から同時認証に基づいたプロセスで実施した場合とそうでない場合を比較すると以下の表（表 3-16）のようになる。分析のみとはアイテム定義以前のアクティビティを除いたものであり、ロス同定のための分析、ロス統合、リスク決定のための分析、リスクの決定がそれにあたる。分析は本実験で本質的な部分であるため、全アクティビティから抽出して記述している。

	同時認証に基づいたプロセス	同時認証に基づかいないプロセス
全アクティビティ	79 人時	105 人時
分析のみ	50 人時	52 人時

表 3-16　各プロセスでのコスト

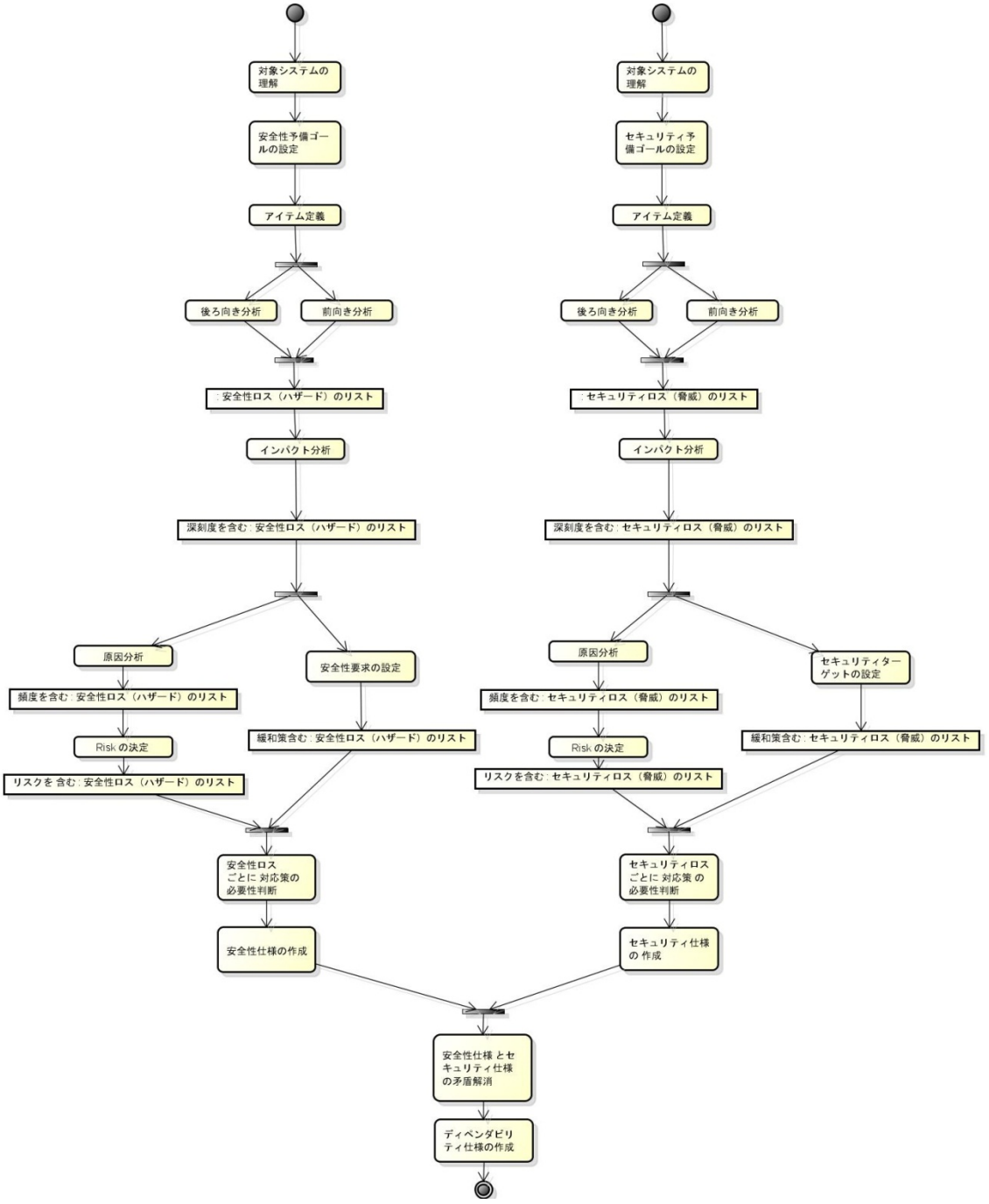


図 3-5　SafSec に基づかないプロセス

以上の結果から削減可能なコストは、全プロセスで約 25%、分析のみで、約 4%であることが分かる。

3.5. 実験結果

本実験においては、セキュリティに関しては、今回対象になった IC カードの機能から、同等の IC カードを調査し、そのCCにおける以下のセキュリティターゲット（Security Target）(注4)を参考にした。

フェリカネットワークス社, モバイル Felica IC チップファームウェア（T6N 版）, セキュリティターゲット, version 1.01, No. FN12-F028-J01-01, 2009/06/26　（参考文献[17]）

上記システム（TOE と呼ばれる）の評価保証レベルは 「EAL 4 追加」である（詳細は 2.2.1.節を参照）。CC における評価の実施においては、セキュリティターゲットを含む評価資料に加えて、開発・製造現場におけるヒアリング、検証が行われる。そのためには、実際に現場に行き、開発プロセスの検証、テスト等の検証に関する評価者検証等が必要になる。

本実験は模擬的なものであり、このような監査作業を実際に行うことはしていない。上記のセキュリティ―ターゲットにおいては、9 種類の脅威を想定し、それに対する対策と保証を示している（脅威に関しては、2.2.1.節を参照）。本実験においては、分析の結果、同様な 10 種類の脅威（セキュリティロス）を同定した。本実験では、SafSec における安全性に関するリスクとセキュリティに関する脅威の分析と評価を統合的に行う部分を実施しているので、その点から考えると、同等の EAL4 が達成可能と推測した。

それに対して、IEC 61508 の適用については、その品質レベルである 安全度水準（SIL (Safety Integrity Level)）については、実験計画時はギャップ分析を実施するとしたが、SafSecに適合しなかったので、独自の判断基準を策定し、どのような形で安全度水準が決定できるかの示準を提示すことで代用ができた。このような形で、どの程度の品質レベルが可能かを評価した。

注意 4: セキュリティターゲットとは、CC において認証の対象になるシステムが品質レベルを達成していることを示す書類のことである。2.2.1 節の CC の概要を参照。

IEC61508 における安全度水準（SIL） の決定方法は、2 種類のハードウェア故障（決定論的故障とランダム故障）を基本としている。しかし安全度水準の決定には、条件に応じて様々な決定方法が利用可能である。それらは 「Part 5 安全度水準の決定に関する方法の例（Examples of methods for the determination of safety integrity levels (edition 2.0 2010-04)）」 において述べられている。本実験においては、SafSec のリスクアセスメントの方法との親和性を考慮し、安全度水準の決定方法としては、Part 5 の付録である、

付録 C ALARP と許容範囲リスクの概念（Annex C ALARP and tolerable risk concepts）

付録 E 安全度水準の決定 – リスクグラフ手法（Annex E Determination of safety integrity levels – Risk graph methods）

の適用可能性について考察し、どのように本実験で得られたデータを利用することができるかを示した。

規格	品質レベルの考え方
IEC 61508	SIL の決定のための方法論とデータの提示。 Part 5, Annex C と E による方法の適合性について確認。
ISO/IEC 15408	EAL 4 レベルが達成可能と推測

表 3-17　本実験における品質レベルの考え方

以下に、品質レベルと削減可能なコストについてまとめた表（表 3-18）を記す。本実験では 2.6.1 節で述べたように品質レベル 3 が達成可能であり、その場合の結果が得られている。

品質レベル	作業項目	削減コスト(人時)	対応する規格
3	対象システムの理解	16	CC, IEC 61508
	安全性予備ゴールの設定	0	IEC 61508
	セキュリティ予備ゴールの設定	0	CC
	アイテム定義	8	CC, IEC 61508
	安全性に関する後ろ向き分析	0	IEC 61508
	安全性に関する前向き分析	0	IEC 61508
	セキュリティに関する後ろ向き分析	0	CC
	セキュリティに関する前向き分析	0	CC
	LossOp Study Meeting	4(注)	SafSec（本実験）
	インパクト分析	0.88	CC, IEC 61508
	原因分析	0.96	CC, IEC 61508
	リスクの決定	0.16	CC, IEC 61508

(注) 手戻りによるコストを考えなくてはならないため、実際には見積もることは不可能であるが、一度大きな手戻りをするだけで済んだと仮定して算出した値である。詳しくは実施報告書 3.6. 節を参照のこと。

表 3-18　実験結果

3.6. 考察

重複の解消によるコスト削減効果

同時認証によるコスト削減効果は、個別に認証を行う方法に伴う作業の重複を排除することによりもたらされる。重複する作業の大きさは、安全性とセキュリティの双方に関連するロスの数に依存して決まるため、そのようなロスが多いほど同時認証の工数削減効果は大きくなると考えられる。

本実験では､対象システムの分析範囲が絞られており､特にセキュリティに関しては 3.2.2. 節で述べたような理由から、基盤システム部分に絞られて分析が行われている。セキュリティに関しての分析をサービス部分にまで広げることでより多くのセキュリティのロスが同定されることは明らかである。例えば災害情報を偽造して流すことによりドアの施錠を解除するという脅威も考えられ、安全性の Loss13 と同じロスになる。このように、安全性とセキュリティそれぞれで多くのロスが同定されることで、双方にかかわるロスも増加する。

また、リスクの決定までが本実験の対象である。今回、実施していない「ディペンダビリティターゲットの設定」､「ディペンダビリティ仕様の作成」でもロスの重複を排除することで検討などの重複の解消が可能である。従って、同時認証による分析対象が広がるほどコスト削減効果も大きくなることが期待できる。

以上のような理由から実際の運用時は今回見積もった以上のコスト削減効果が得られることが分かる。

安全性とセキュリティ統合による効果

SafSecに基づかいない分析フローの「安全性仕様とセキュリティ仕様の矛盾解消」アクティビティをLossOp Study Meetingと同等と見込み、4 人時と仮定している。しかし実際には、LossOp Study Meetingで行う統合に加え、アイテム定義、リスク、対抗策、仕様の統合などが必要になり、より複雑な統合を行わなければならないため、より多くのコストが必要である。例えば、本実験において安全性とセキュリティの双方に関連する 3 つのロスに関してSafSecに基づかないプロセスで最も大きな手戻りを一度行うことにより双方の仕様の矛盾を解消できたと仮定したとする。その場合、手戻りで発生するコストが 4 人時となる（LossOp Study Meetingでは 1 人時を概要説明に利用しており、セキュリティのロスを主として統合作業を行っている。そのため、1 つのロスを統合するのに必要となるコストは約 1/3 人時と考えられる。また、他のアイテム定義、対抗策、仕様の統合でも同じだけコストがかかると仮定する)。この場合、SafSecに基づかない分析フローで実施するコストに対し 10.7%のコスト削減を見積もることができる。

しかし、実際には、どの程度の手戻りが発生するかは予測することはできず、上記のような手戻りのコストの見積もりは、むしろ少なめの数であると考えるべきである。加えてこのような手戻りの予測困難性は、開発計画を立てる上でも大きな障害となってしまう。

SafSec に基づく分析を実施することで実際の運用では今回の実験で得られた以上のコスト削減が可能であり、また開発計画を立てることが容易になると考えられる。

4. まとめ

本章では本実験を総括し、今後の課題と提案を述べる。

4.1. 本実験の総括

本実験の成果としては、安全性とセキュリティの同時認証という、今後、様々な産業分野の製品において必要になると予測される技術を、SafSec を基に実験をしたものである。事例としては、社会情報基盤システムという、現実的で社会的な影響力が強いシステムを分析の対象とした。

本実験の範囲は、SafSec の一部であるが、実際に実験することで、深刻度の算出において、様々な工夫が必要なことが判明した。本実験では、IEC 61508 Part5 の添付資料にある、品質レベル（安全度水準、SIL）の計算方法を独自に適用することで解決した。

工数の算定には、SafSec のプロセスと、SafSec を利用しないプロセス両方を設計し、SafSec を実施した実際の工数を、利用しないプロセスに適用することで、その差分を測定し、コスト評価を行った。この結果、SafSec を適用する方が確かに、効率的に実施できることを示すことができた。

本実験は、認証制度の中でも新たな技術チャレンジの分野であり、認証の工学的アプローチの中でも先進的な分野である。本報告書においては、深刻度の計算などについても詳細に記述してあるので、今後、同様なアプローチをするプロジェクトや組織にとっても、参考になるデータ・技術を提供していると考えられる。

4.2. 今後の課題と提案

今回の実験では、SafSec の一部だけを検証したにすぎない。SafSec を利用して、特定のシステムの開発から認証までを実施するのは、今後の課題としてまず上げられる点である。

より詳細な点に関して述べれば、SafSec に関して、今回の実験でやり残した課題としては以下のものがある。

1) ディペンダビリティ仕様の分析、獲得
2) ディペンダビリティ仕様がロスに対して十分対抗していることの議論の構築
3) システムモジュールと、妥当性の議論モジュールとの連携
4) 安全性とセキュリティの認証に関するディペンダビリティケース

ディペンダビリティ仕様の分析、獲得について、本実験においては安全性におけるハザードとセキュリティにおける脅威に対して、従来から用いられている前向き分析と後ろ向き分析を利用した。セキュリティにおける脅威分析を支援する表記法は様々なものが知られている。UML（参考文献[18]）におけるユースケース図を拡張したミスユースケース図（参考文献[22]）や、UMLsec（参考文献[23]）といったものも開発されている。さらには、

CC に特化したミスユースケース図の提案も弊社の田口からされている（参考文献[24]）。安全性の分析については、実は UML などを拡張し、分析を支援するといったものが存在しない。さらに、安全性とセキュリティを同時に分析するプロセスを支援する記法も存在しない。このような要素技術を開発することで、異なるシステムの品質をより詳細に分析することができる可能性がある。さらに、そのためのコストの削減が期待できる。

2)から 4)に関しては、本実験では触れなかったシステムの品質の保証をするための技術であるディペンダビリティケースと密接に関連している。ディペンダビリティケースは、アシュアランスケースの一種であり、開発者がシステムのディペンダビリティの保証を主張する文書であり、監査官（アセッサ）が監査資料として利用するものである。例えば、車載システムの機能安全規格である ISO 26262（参考文献[6]）においては、安全性に関するケース、セーフティケースの提出が義務付けられている。ディペンダビリティケースの作成は、製品の品質の第三者による評価という行為に密接に関連しており、どのような品質説明資料を評価することで、どこまでその品質を保証できるか、という問題に密接に関連している。

3)では、認証に関するモジュラーアプローチが関連しており、システムやシステム環境、利用者の変化に伴う認証資料の進化的な改訂や、再利用について述べている。モジュラーな認証とは、再認証のコストを削減するために、認証の根拠資料（例：安全ケース。SafSec においてはディペンダビリティケース）のモジュール化と、開発の成果物（例：設計資料）のモジュール化とそれらの関連性を考慮するアプローチである。本模擬実験においては、安全ケース／アシュアランスケース／ディペンダビリティケースについては言及していないが､これらの分析を支援する図表現である GSN (Goal Structuring Notation)においては、モジュール表現がサポートされている。認証活動は多大な費用がかかるものであり、モジュール化を行うことで、そのコストの削減が望まれる。しかし、実際にはこのような方法論が確立されていないので、今後とも研究開発を実施する必要がある。

SafSec において扱われてはいないが、システムの認証において重要な課題としては、いかに複数の規格において規定されている、プロセスや開発技術を統合するかという問題がある。例えば、機能安全規格である IEC 61508 においては、適用される品質レベルにより開発技術が異なる。IEC 61508 におけるソフトウェア安全要件仕様(Software safety requirements specification)においては、SIL3 以上では準形式的手法(Semi-formal methods)の適用が高く推奨されて(HR: Highly Recommended)おり、SIL4 では形式的手法(Formal methods)の適用が高く推奨されている(参考文献[3], Part3, Table A.1, p47)。それに対して、ISO/IEC 15408 においては、EAL5 において、準形式的設計及びテストが指定されている。このように適用される品質レベルにより、適用すべき開発技術が異なる場合がある。この問題を解決するためには、事前に開発計画、検証計画、安全計画等において、品質レベルの違いを考慮しておく必要があり、今後の課題としては、SafSec にこのようなプロセス、開発技術の統合を、どのように導入するかを考察する必要がある。

これらを要約し、以下の実施を提案することで本報告書の結びとしたい。

・SafSec のプロセスを全て模擬的に実施する
・複数の品質に関するリスクの同時分析を支援する表記法の開発を行う
・複数の品質保証のためのディペンダビリティケース開発方法論の策定
・認証へのモジュラーアプローチを確立する
・規格毎で指定されている開発プロセス、開発方法論の統合方法を検討する

参考文献：

[1] Praxis High Integrity Systems, SafSec: Integration of Safety & Security Certification, SafSec Methodology: Guidance Material, 2006

[2] Praxis High Integrity Systems, SafSec: Integration of Safety & Security Certification, SafSec Methodology: Standard, 2006

[3] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 ~ Part 7.

[4] ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, Part1 ~ Part3.　もしくは
情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリア パート 1：概説と一般モデル, バージョン 3.1 2009 年 7 月
情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリア パート 2：セキュリティ機能要件, 2005 年 8 月
情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリア パート 3：セキュリティ保証要件, 2005 年 8 月

[5] ISO 14121, Safety of machinery – Risk assessment – Part1

[6] ISO 26262, Road vehicles – Functional safety – Part1~Part10, 2011.

[7] PCI-DSS, v2.0, 2010, Security Standard Council

[8] ISO/IEC 17799, Information technology – Security techniques – Code of practice for information security management, 2005

[9] Cloud Security Alliance (CSA), http://www.cloudsecurityalliance.jp/

[10] Cloud Controls Matrix, ver. 1.2., 2011

[11] Microsoft, Standard Response to Request for Information – Security and Privacy, Microsoft Office 365, 2011

[12] ISO 11898, Road vehicles – Controller area network (CAN)

[13] K. Koscher, et. al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy 2010

[14] RTCA, DO-178B, Software Considerations in Airborne Systems and Equipment Certification, 1992

[15] V. Hilderman and T. Baghai, Avionics Certification: A Complete Guide to DO-178 (Software), DO-254 (Hardware), Avionics Communications Inc., 2007

[16] Defense Standard 00-56, Safety Management Requirements for Defense Systems, Part 1 Requirements, Issue 4, 2007

[17] フェリカネットワークス社, モバイル Felica IC チップファームウェア (T6N 版), セキュリティターゲット, version 1.01, No. FN12-F028-J01-01, 2009/06/26

[18] OMG, UML (Unified Modeling Language)

[19] J. Davies, J. Woodcock, Using Z, Prentice Hall, 1996
[20] 中島震, SPIN モデル検査, 近代科学社, 2008
[21] JISEC, 認証報告書, モバイル FeliCa IC チップファームウェア (T6N 版), 平成 20 年 3 月
[22] G. Sindre, A. L. Opdahl, Eliciting security requirements with misuse cases, Requirements Engineering Journal, 10(1):34-44, 2005
[23] J. Jurjens, Secure Systems Development with UML, Springer, 2004
[24] K. Taguchi, et. al., Aligning Security Requirements and Security Assurance Using Common Criteria, SSIRI 2010:69-77

添付資料

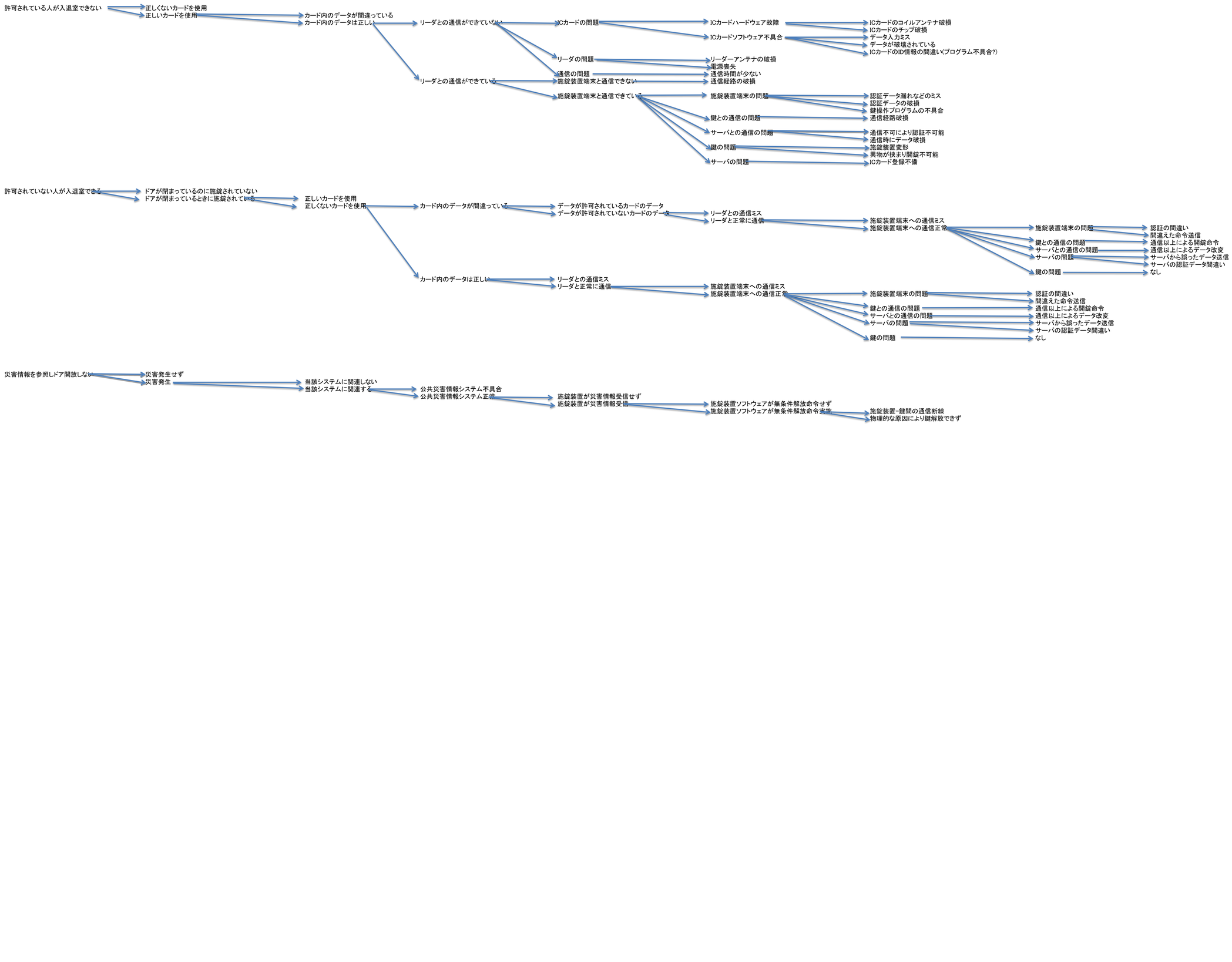
添付資料一覧

・安全性予備ゴール
・安全性ロス同定の前向き分析
・安全性ロス同定の後ろ向き分析
・安全性ロス一覧
・セキュリティ予備ゴール
・セキュリティロス同定の前向き分析
・セキュリティロス同定の後ろ向き分析
・セキュリティロス一覧
・ロスログ
・原因分析
・インパクト分析

安全性予備ゴール

（Saf1） 許可された人が入退室できる
（Saf2） 許可されてない人が入退室できない
（Saf3） 災害時全ドアを無条件解放する

安全性ロス同定の前向き分析



安全性ロス同定の後ろ向き分析

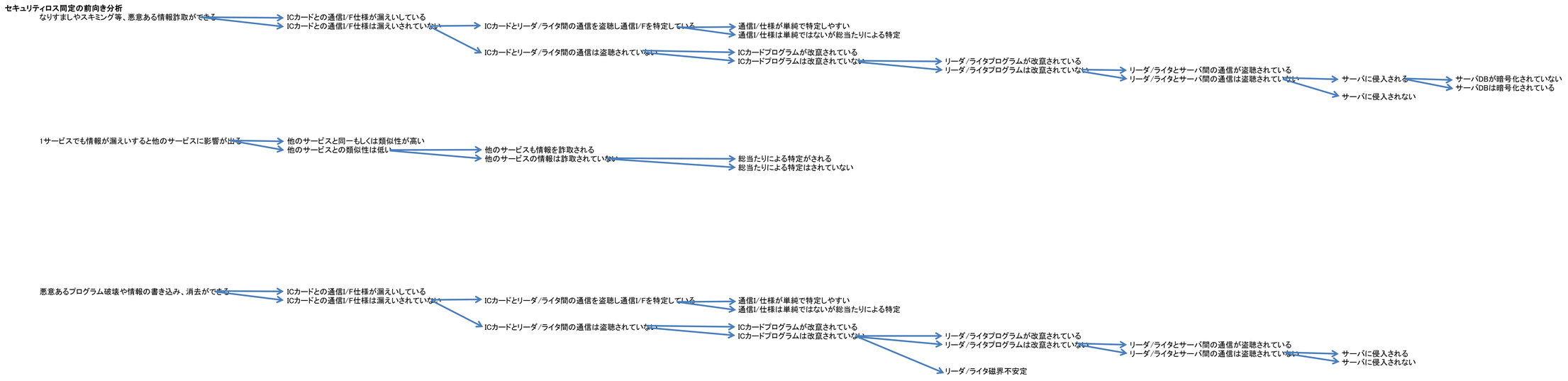
分析対象部品	故障モード			影響	対策	ハザード候補
ICカードソフトウェア	受信失敗	コマンドを誤って受信	システムコマン	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		ICカードデータ不整合
			MIIDコマンド	意図しない処理を実行され意図しないレスポンスになる。安全目標(1),(2)が破綻		ICカードが間違った処理をする
		パラメータを誤って受信	システムコマン	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードの処理と異なる結果を送信
		受信しない	システムコマン	ICカードが反応せず案是目標(1)が破綻する		ICカードが反応しない
			MIIDコマンド	ICカードが反応せず案是目標(1)が破綻する		ICカードが反応しない
	送信失敗	ackを誤って送信	システムコマン	ICカードが処理を実行したことが認識されず、認証が進まなくなる。これにより安全目標(1)が破綻する		ICカード処理停止、ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードレスポンス内容間違い
		パラメータを誤って送信	システムコマン	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカード処理遅延
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードレスポンス内容間違い
		データを誤って送信	MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードレスポンス内容間違い
		送信しない	システムコマン	ICカードが反応せず案是目標(1)が破綻する		ICカードが反応しない
			MIIDコマンド	ICカードが反応せず案是目標(1)が破綻する		ICカードが反応しない
	コマンドに対応する処理の選択間違い			意図した処理が行われず、安全目標(1),(2)が破綻する		ICカードが間違った処理をする
ICカードハードウェア-コイルアンテナ	電流が発生しない			ICカードが反応せず案是目標(1)が破綻する		ICカードが反応しない
	電流が微弱			ICカードがたまにしか反応せず案是目標(1)が破綻する		ICカードが反応しない
	電流が過剰			ICカードが破損するかのうせいがある。		ICカードが破損している
ICカードチップ	チップ破損			ICカードの情報が正常に読み取れない、もしくはICカードが反応しない		ICカードが反応しない、ICカードデータ不整合
ICカードリーダ/ライタハードウェア-リーダ/ライタアンテナ	受信失敗	コマンドを誤って受信	システムコマン	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		ICカードへ意図しないシステムコマンド送信
			MIIDコマンド	ICカードで意図しない処理が行われ、その結果がレスポンスとなる。安全目標(1)(2)がたまに破綻		ICカードへ意図しない処理を命令
		パラメータを誤って受信	システムコマン	意図したシステム処理が行われず、カードが意図した情報を保持したものにならない。これにより安全目標(1),(2)が破綻する		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードへ意図しない処理を命令
		受信しない	システムコマン	ICカードをかざしてもリーダが反応せず安全目標(1)が破綻		リーダ/ライタが反応しない
			MIIDコマンド	ICカードをかざしてもリーダが反応せず安全目標(1)が破綻		リーダ/ライタが反応しない
		ackを誤って受信	システムコマン	ICカードが処理を実行したことが認識されず、認証が進まなくなる。これにより安全目標(1)が破綻する		ICカード処理停止、ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカード処理結果の誤認
		データを誤って受信	MIIDコマンド			ICカード処理結果の誤認
	送信失敗	ackを誤って送信	システムコマン	ICカードが処理を実行したことが認識されず、認証が進まなくなる。これにより安全目標(1)が破綻する		ICカード処理停止、ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカード処理結果の誤認
		パラメータを誤って送信	システムコマン	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカード処理結果の誤認
		送信しない	システムコマン	ICカードをかざしてもリーダが反応せず安全目標(1)が破綻		リーダ/ライタが反応しない
			MIIDコマンド	ICカードをかざしてもリーダが反応せず安全目標(1)が破綻		リーダ/ライタが反応しない
		コマンドを誤って送信	システムコマン	ICカードが意図しない処理を実行する。これにより安全目標(1)が破綻する		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードが間違った処理を実施
	通信不可			ICカードをかざしてもリーダが反応せず安全目標(1)が破綻		リーダ/ライタが反応しない
	電源喪失			ICカードをかざしてもリーダが反応せず安全目標(1)が破綻、カード処理中に電源がなくなることによるデータ不整合		電源喪失、ICカードデータ不整合
施錠装置ソフトウェア ICカード認証通信	コマンド送信	コマンドを誤って送信	システムコマン	ICカードに誤ったシステムコマンドを送信してしまい、カードの意図する機能が損なわれる。安全目標(1),(2)が破綻する		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードへ意図しない処理を命令
		パラメータを誤って送信	システムコマン	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカードの処理と異なる結果を送信
		送信しない	システムコマン	施錠装置システムが反応せず案是目標(1)が破綻する		システムが反応しない
			MIIDコマンド	施錠装置システムが反応せず案是目標(1)が破綻する		システムが反応しない
	レスポンス受信	ackを誤って受信	システムコマン	Cカードで意図した処理が行われていないと誤認して処理が進まなくなる。		ICカード処理停止、ICカードデータ不整合
			MIIDコマンド	正しいカード認証されない、間違ったカードが認証されるということがたま起こる		ICカード処理結果の誤認
		受信しない	システムコマン	施錠装置システムが反応せず案是目標(1)が破綻する		システムが反応しない
			MIIDコマンド	施錠装置システムが反応せず案是目標(1)が破綻する		システムが反応しない
公共災害情報受信	公共災害情報	受信しない		災害発生を検知できずにドアを開放しない。安全目標(3)が破綻		災害情報無受信
		公共災害情報を誤って受信	災害情報を過小	ドアを開放しない。安全目標(3)が破綻		災害情報誤認
			災害情報を過大	ドアを無条件開放してしまう。安全もk表(2)が破綻		災害情報誤認
鍵コントロール	施錠命令送信失敗			自動施錠が実施されない		施錠しない
	開錠命令送信失敗			鍵が開錠されず、安全目標(1)(3)が破綻		鍵が開かない
	ドア閉状態受信失敗			ドア状態を正しく認識できず、自動施錠を実行できない		ドア状態認識しない
サーバ通信	データ送信	データを誤って送信		認証が正しく行われず安全目標(1)(2)が破綻		認証データの送信間違い
		破損したデータを送信		認証が正しく行われず安全目標(1)(2)が破綻		認証データの破損
		データを送信しない		サーバ通信ソフトウェアが動かずに安全目標(1)(2)が破綻		サーバと通信しない
	受信	ackを誤って受信		認証結果が間違えることにより安全目標(1)(2)が破綻		認証結果間違い
		受信しない		サーバからの応答が得られずに安全目標(1)(2)が破綻		サーバと通信しない
鍵	ドアセンサーが感知しない			ドアが常に開いているとして安全目標(2)がはたん		ドアセンサー故障
	鍵の破損	開錠困難		正しいカードでも物理的に開錠が困難になり、安全目標(1),(3)が破綻		鍵が開かない
		施錠困難		ドアが閉じていても施錠が困難になり、安全目標(2)が破綻		施錠しない
サーバ	データ受信	データを誤って受信		誤ったデータを用いるため、認証結果が期待したとおりにならない。		受信認証データの誤り
		データが破損している		認証が正しく行われず安全目標(1)(2)が破綻		受信認証データの破損
		データを受信しない		サーバが処理を実施しないため安全目標(1)(2)が破綻		サーバと通信ができない
	処理	対応するデータを間違える		受信データと対応させる認証データを取り違えることにより期待する認証結果が得られない。		認証データの取り違え
	認証データが間違えている			サーバに登録されているデータ間違いにより期待する認証結果にならない		登録認証データ間違い

安全性ロス一覧

安全性ロスID	安全性ロスラベル
Saf1	ICカードデータ不整合
Saf2	ICカードが間違った処理をする
Saf3	ICカードの処理と異なる結果を送信
Saf4	ICカードが反応しない
Saf5	ICカード処理停止
Saf6	ICカードレスポンス内容間違い
Saf7	ICカードが破損している
Saf8	ICカードへ意図しないシステムコマンド送信
Saf9	ICカードへ意図しない処理を命令
Saf10	リーダ/ライタが反応しない
Saf11	ICカード処理結果の誤認
Saf12	システムが反応しない
Saf13	災害情報無受信
Saf14	災害情報誤認
Saf15	ドアセンサー故障
Saf16	施錠しない
Saf17	物理的に鍵が開かない
Saf18	ドア状態認識しない
Saf19	通信時間不十分
Saf20	電源喪失
Saf21	サーバ受信認証データの誤り
Saf22	サーバ受信認証データの破損
Saf23	サーバと通信ができない
Saf24	認証データの取り違え
Saf25	認証データの送信間違い
Saf26	認証データの破損
Saf27	認証結果間違い

セキュリティ予備ゴール

(Sec1) なりすましやスキミング等、悪意ある情報詐取ができない
(Sec2) 各サービスの情報漏えいが他のサービスに影響しない
(Sec3) 悪意あるプログラム破壊や情報の書き込み、消去ができない


セキュリティロス同定の前向き分析
なりすましやスキミング等、悪意ある情報詐取ができる
ICカードとの通信I/F仕様が漏えいしている
ICカードとの通信I/F仕様は漏えいされていない
ICカードとリーダ／ライタ間の通信を盗聴し通信I/Fを特定している
ICカードとリーダ／ライタ間の通信は盗聴されていない
通信I/仕様が単純で特定しやすい
通信I/仕様は単純ではないが総当たりによる特定
ICカードプログラムが改竄されている
ICカードプログラムは改竄されていない
リーダ／ライタプログラムが改竄されている
リーダ／ライタプログラムは改竄されていない
リーダ／ライタとサーバ間の通信が盗聴されている
リーダ／ライタとサーバ間の通信は盗聴されていない
サーバに侵入される
サーバに侵入されない
サーバDBが暗号化されていない
サーバDBは暗号化されている
1サービスでも情報が漏えいすると他のサービスに影響が出る
他のサービスと同一もしくは類似性が高い
他のサービスとの類似性は低い
他のサービスも情報を詐取される
他のサービスの情報は詐取されていない
総当たりによる特定がされる
総当たりによる特定はされていない
悪意あるプログラム破壊や情報の書き込み、消去ができる
ICカードとの通信I/F仕様が漏えいしている
ICカードとの通信I/F仕様は漏えいされていない
ICカードとリーダ／ライタ間の通信を盗聴し通信I/Fを特定している
ICカードとリーダ／ライタ間の通信は盗聴されていない
通信I/仕様が単純で特定しやすい
通信I/仕様は単純ではないが総当たりによる特定
ICカードプログラムが改竄されている
ICカードプログラムは改竄されていない
リーダ／ライタプログラムが改竄されている
リーダ／ライタプログラムは改竄されていない
リーダ／ライタ磁界不安定
リーダ／ライタとサーバ間の通信が盗聴されている
リーダ／ライタとサーバ間の通信は盗聴されていない
サーバに侵入される
サーバに侵入されない

セキュリティロス同定の後ろ向き分析

機器	故障モード		原因	影響	対策	脅威候補	
ICカード	保護データの流出	コマンドデータの一致(総当たり)		情報が詐取され、個人情報が漏えいする		不正コマンドデータによるアクセス	①
		不正取得したコマンドデータの受信		情報が詐取され、個人情報が漏えいする		不正取得したコマンドデータによるアクセス	②
		盗聴・改竄したコマンドデータの受信		情報が詐取され、個人情報が漏えいする		盗聴・改竄したコマンドデータによるアクセス	③
		盗聴により解析されたVRICS　Titleデータの受信		情報が詐取され、個人情報が漏えいする		盗聴した情報からVRICS　Titleデータの暴露	④
		改竄プログラムのインストール		情報が詐取され、個人情報が漏えいする		改竄プログラムのインストール	⑤
				本ICカードの使用ができなくなる			
	保護データの破壊・消去	コマンドデータの一致(総当たり)		個人の権利、財産が不当に変更、消滅する		不正コマンドデータによるアクセス	①
		不正取得したコマンドデータの受信		個人の権利、財産が不当に変更、消滅する		不正取得したコマンドデータによるアクセス	②
		盗聴・改竄したコマンドデータの受信		個人の権利、財産が不当に変更、消滅する		盗聴・改竄したコマンドデータによるアクセス	③
		データエリア更新中の電源途絶		個人の権利、財産が不当に変更、消滅する		データアクセス中の電源途絶	⑥
		ICチップを故障させることによるセキュリティの危殆化		個人の権利、財産が不当に変更、消滅する		ICチップを故障させることによるセキュリティの危殆化	⑦
				本ICカードの使用ができなくなる			
		改竄プログラムのインストール		個人の権利、財産が不当に変更、消滅する		改竄プログラムのインストール	⑤
				本ICカードの使用ができなくなる			
	VRICS　Titleデータの暴露	コマンドデータの一致(総当たり)		該当サービスの認証システムの信頼性が低下、マヒする		不正コマンドデータによるアクセス	①
				個人の権利、財産が他人に不当に利用される			
		不正取得したコマンドデータの受信		該当サービスの認証システムの信頼性が低下、マヒする		不正取得したコマンドデータによるアクセス	②
				個人の権利、財産が他人に不当に利用される			
		盗聴・改竄したコマンドデータの受信		該当サービスの認証システムの信頼性が低下、マヒする		盗聴・改竄したコマンドデータによるアクセス	③
				個人の権利、財産が他人に不当に利用される			
		改竄プログラムのインストール		該当サービスの認証システムの信頼性が低下、マヒする		改竄プログラムのインストール	⑤
				個人の権利、財産が他人に不当に利用される			
	VRICS　Titleデータの変更	コマンドデータの一致(総当たり)		個人の権利、財産が利用できなくなる		不正コマンドデータによるアクセス	①
		不正取得したコマンドデータの受信		個人の権利、財産が利用できなくなる		不正取得したコマンドデータによるアクセス	②
		盗聴・改竄したコマンドデータの受信		個人の権利、財産が利用できなくなる		盗聴・改竄したコマンドデータによるアクセス	③
リーダーライター	VRICS　Titleデータの暴露	プログラム改竄		該当サービスの認証システムの信頼性が低下、マヒする		改竄プログラムの不正インストール	⑤
				個人の権利、財産が他人に不当に利用される			
	VRICS　Titleデータの変更	プログラム改竄		個人の権利、財産が利用できなくなる		改竄プログラムの不正インストール	⑤
				個人の権利、財産が他人に不当に利用される			
	保護データの読み出し	プログラム改竄		情報が詐取され、個人情報が漏えいする		改竄プログラムの不正インストール	⑤
	保護データの破壊・消去	プログラム改竄		個人の権利、財産が不当に変更、消滅する		改竄プログラムの不正インストール	⑤
サーバ	保護データの暴露	プログラムによる侵入(サーバ攻撃)		個人情報の漏えい		プログラムによる侵入(サーバ攻撃)	⑧
		人による侵入		個人情報の漏えい		人による侵入	⑨
		盗聴・改竄された通信データの受信		情報が詐取され、個人情報が漏えいする		盗聴・改竄された通信データによる侵入	⑩
	保護データの破壊・消去	プログラムによる侵入(サーバ攻撃)		個人の権利、財産が不当に変更、消滅する		プログラムによる侵入(サーバ攻撃)	⑧
		人による侵入		個人の権利、財産が不当に変更、消滅する		人による侵入	⑨
		盗聴・改竄された通信データの受信		個人の権利、財産が不当に変更、消滅する		盗聴・改竄された通信データによる侵入	⑩
	VRICS　Titleデータの暴露	盗聴・改竄された通信データの受信		該当サービスの認証システムの信頼性が低下、マヒする		盗聴・改竄された通信データによる侵入	⑩
	VRICS　Titleデータの変更	盗聴・改竄された通信データの受信		個人の権利、財産が利用できなくなる		盗聴・改竄された通信データによる侵入	⑩

セキュリティロス一覧

セキュリティロスID	セキュリティロスラベル
Sec1	不正コマンドデータによるアクセス
Sec2	不正取得したコマンドデータによるアクセス
Sec3	盗聴・改竄したコマンドデータによるアクセス
Sec4	盗聴した情報からVRICS　Titleデータの暴露
Sec5	改竄プログラムのインストール
Sec6	データアクセス中の電源途絶
Sec7	ICチップを故障させることによるセキュリティの危殆化
Sec8	プログラムによる侵入（サーバ攻撃）
Sec9	人による侵入
Sec10	盗聴・改竄された通信データによる侵入

ロスログ

ロスID	ロスラベル	頻度	深刻度	ロスの原因	ロスの影響	関連するシステム特性	対応策	安全性ロスID	セキュリティロスID	Risk
Loss1	ICカードデータ不整合	時折	重大	ICカードソフトウェアのデータ	特定のカードの安全目標(1),(2)	Safety		Saf1		II
Loss2	ICカードが間違った処理をする	時折	重大	ICカードソフトウェアのデータ	特定のカードの安全目標(1),(2)	Safety		Saf2		II
Loss3	ICカードの処理と異なる結果を送信	ほとんどない	重大	ICカードソフトウェアのデータ	特定のカードの安全目標(1),(2)	Safety		Saf3		III
Loss4	ICカードが反応しない	時折	重大	ICカード	特定のカードの安全目標(1),(2)	Safety		Saf4		II
Loss5	ICカード処理停止	時折	重大	ICカード	特定のカードの安全目標(1),(2)	Safety		Saf5		II
Loss6	ICカードレスポンス内容間違い	時折	重大	ICカード	特定のカードの安全目標(1),(2)	Safety		Saf6		II
Loss7	ICカードが破損している	ほとんどない	重大	ICカード	特定のカードの安全目標(1),(2)	Safety		Saf7		III
Loss8	ICカードへ意図しない処理を命令	ほとんどない	重大	施錠装置	複数のカードの安全目標(1),(2)	Safety		Saf9		III
Loss9	R/Wが反応しない	時折	重大	施錠装置	複数のカードの安全目標(1)	Safety		Saf10		II
Loss10	ICカード処理結果の誤認	ほとんどない	重大	施錠装置	複数のカードの安全目標(1),(2)	Safety		Saf11		III
Loss11	システムコマンド	かなり	重大	施錠装置	特定のドアの安全目標(1),(2)	Safety		Saf12		I
Loss12	災害情報無受信	ありそうもない	非常に深刻	施錠装置、公共災害情報システム	複数の人の安全目標(3)	Safety		Saf13		III
Loss13	災害情報誤認	ありそうもない	非常に深刻	施錠装置ソフトウェア災害情報受信	複数のドアまたは複数の人の安全目標(3)	Safety		Saf14		III
Loss14	ドアセンサー故障	時折	軽微	ドアのドアセンサー	特定のドアの安全目標(2)	Safety		Saf15		III
Loss15	施錠しない	時折	軽微	ドア、施錠装置	特定のドアの安全目標(2)	Safety		Saf16		III
Loss16	物理的に鍵が開かない	ありそうもない	重大	ドアのドアセンサー	複数のカードの安全目標(1)	Safety		Saf17		III
Loss17	ドア状態認識しない	時折	軽微	ドア、施錠装置	特定のドアの安全目標(2)	Safety		Saf18		III
Loss18	通信時間不十分	かなり	軽微	ICカード、施錠装置	特定のカードの安全目標(1)	Safety		Saf19		II
Loss19	サーバ受信認証データの誤り	ほとんどない	重大	施錠装置、サーバ	特定のカードの安全目標(1),(2)	Safety		Saf21		III
Loss20	サーバ受信認証データの破損	ほとんどない	重大	施錠装置、サーバ	特定のカードの安全目標(1),(2)	Safety		Saf22		III
Loss21	サーバと通信ができない	時折	重大	施錠装置、サーバ	複数のカードの安全目標(1),(2)	Safety		Saf23		II
Loss22	サーバで認証データの取り違え	ほとんどない	重大	サーバ	複数のカードの安全目標(1),(2)	Safety		Saf24		III
Loss23	サーバで認証データの送信間違い	ほとんどない	重大	サーバのWebアプリケーション	特定のカードの安全目標(1),(2)	Safety		Saf25		III
Loss24	認証結果間違い	ほとんどない	重大	サーバのデータベース	特定のカードの安全目標(1),(2)	Safety		Saf27		III
Loss25	不正コマンドデータによるアクセス	可能	一部の情報	R/W悪用	保護データ情報漏洩・破壊	Safety, Security(SecurityによりSafetyが保たれる)		Saf8	Sec1	II
Loss26	不正取得したコマンドデータによるアクセス	困難	一部の情報	コマンド流出	保護データ情報漏洩・破壊	Security			Sec2	III
Loss27	盗聴・改竄したコマンドデータによるアクセス	非常に困難	一部の情報	スキミング	保護データ情報漏洩・破壊	Security			Sec3	III
Loss28	盗聴した情報からVRICS　Titleデータの暴露	非常に困難	一部の情報	スキミング	認証システム信頼性低下	Security			Sec4	III
Loss29	改竄プログラムのインストール	非常に困難	一部の情報		保護データ情報漏洩・破壊	Security			Sec5	III
Loss30	データアクセス中の電源途絶	簡単	情報破壊	電断、磁界断絶	カードデータの破壊・消滅	Safety, Security(SecurityによりSafetyが保たれる)		Saf20	Sec6	II
Loss31	ICチップを故障させることによるセキュリティの危	非常に困難	一部の情報		保護データ情報漏洩・破壊	Security			Sec7	III
Loss32	プログラムによる侵入（サーバ攻撃）	困難	大量の情報	サーバ攻撃	保護データ情報漏洩・破壊	Security			Sec8	II
Loss33	人による侵入	非常に困難	大量の情報	サーバ攻撃	保護データ情報漏洩・破壊	Security			Sec9	II
Loss34	盗聴・改竄された通信データによる侵入	可能	一部の情報	サーバ攻撃	保護データ情報漏洩・破壊	Safety, Security(SecurityによりSafetyが保たれる)		Saf26	Sec10	II

原因分析

ロスID	ロス	対象部品			発生頻度とその統合				頻度
Loss1	ICカードデータ不整合	ICカード	ソフトウェア	データ	時折				時折
Loss2	ICカードが間違った処理をする	ICカード	ソフトウェア	コマンド処理	時折				時折
Loss3	ICカードの処理と異なる結果を送信	ICカード	ソフトウェア	OS レスポンス送信	ほとんどない				ほとんどない
Loss4	ICカードが反応しない	ICカード	ソフトウェア	OS コマンド受信 レスポンス送信	ほとんどない ほとんどない	ほとんどない ↑	時折	時折	時折
				コマンド処理	時折		↑		
			ハードウェア	コイルアンテナ	ほとんどない	ほとんどない		↑	
				ICチップ	ほとんどない	↑			
Loss5	ICカード処理停止	ICカード	ソフトウェア	コマンド処理	時折	時折			時折
			ハードウェア	ICチップ	ほとんどない	↑			
Loss6		ICカード	ソフトウェア	コマンド処理	時折	時折			時折
				OS レスポンス送信	ほとんどない	↑			
Loss7	ICカードが破損している	ICカード	ハードウェア	コイルアンテナ	ほとんどない	ほとんどない			ほとんどない
				ICチップ	ほとんどない	↑			
Loss8	ICカードへ意図しない処理を命令	施錠装置	R/Wアンテナ		ほとんどない	ほとんどない			ほとんどない
			ICカード認証通信		ほとんどない	↑			
Loss9	R/Wが反応しない	施錠装置	R/Wアンテナ		時折	時折			時折
			ICカード認証通信		ほとんどない	↑			
Loss10	ICカード処理結果の誤認	施錠装置	R/Wアンテナ		ありそうもない	ほとんどない			ほとんどない
			ICカード認証通信		ほとんどない	↑			
Loss11	システムが反応しない	施錠装置	R/Wアンテナ		時折	かなり			かなり
			鍵コントロール		ほとんどない	↑			
			サーバ通信		ほとんどない	↑			
			ICカード認証通信		時折	↑			
Loss12	災害情報無受信	施錠装置	ソフトウェア	災害情報受信	ありそうもない	ありそうもない			ありそうもない
		公共災害情報システム			ありそうもない	↑			
Loss13	災害情報誤認	施錠装置	ソフトウェア	災害情報受信	ありそうもない	ありそうもない			ありそうもない
Loss14	ドアセンサー故障	ドア	ドアセンサー		時折				時折
Loss15	施錠しない	ドア	ドアセンサー		時折	時折	時折		時折
			錠		ほとんどない	↑			
		施錠装置	鍵コントロール		ほとんどない		↑		
Loss16	物理的に鍵が開かない	ドア	錠		ありそうもない	ありそうもない			ありそうもない
Loss17	ドア状態認識しない	ドア	ドアセンサー		時折	時折			時折
		施錠装置	鍵コントロール		ほとんどない	↑			
Loss18	通信時間不十分	ICカード	ソフトウェア	コマンド処理	時折		時折	かなり	かなり
				OS コマンド受信 レスポンス送信	ほとんどない ほとんどない	ほとんどない ↑	↑		
		施錠装置	R/Wアンテナ		時折	時折		↑	
			ICカード認証通信		ほとんどない	↑			
Loss19	サーバ受信認証データの誤り	施錠装置	サーバ通信		ありえない	ほとんどない			ほとんどない
		サーバ	WEBアプリケーション		ありえない	↑			
Loss20	サーバ受信認証データの破損	施錠装置	サーバ通信		ありえない	ほとんどない			ほとんどない
		サーバ	WEBアプリケーション		ありえない	↑			
Loss21	サーバと通信ができない	施錠装置	サーバ通信		ほとんどない	時折			時折
		サーバ	WEBアプリケーション		ほとんどない	↑			
Loss22	サーバで認証データの取り違え	サーバ	WEBアプリケーション		ありえない	ほとんどない			ほとんどない
			データベース		ありえない	↑			
			LINUX OS		ありえない	↑			
Loss23	サーバで認証データの送信間違い	サーバ	WEBアプリケーション		ほとんどない				ほとんどない
Loss24	認証結果間違い	サーバ	データベース		ほとんどない				ほとんどない
Loss25	不正コマンドデータによるアクセス	ICカード	ICカード通信I/F	データ	時折				時折
			ICカード通信I/F	VRICS Title	ほとんどない				
Loss26	不正取得したコマンドデータによるアクセス	ICカード	ICカード通信I/F	データ	ほとんどない				ほとんどない
Loss27	盗聴・改竄したコマンドデータによるアクセス	ICカード	ICカード通信I/F	データ	ほとんどない				ほとんどない
Loss28	盗聴した情報からVRICS Titleデータの暴露	ICカード	ICカード通信I/F	VRICS Title	ありそうもない				ありそうもない
Loss29	改竄プログラムのインストール	ICカード	ソフトウエア	ICカードアプリ	ありそうもない				ほとんどない
		R/W	ソフトウエア	R/Wアプリ	ほとんどない				
Loss30	データアクセス中の電源途絶	ICカード	ソフトウエア	データ	かなり				かなり
Loss31	ICチップを故障させることによるセキュリティ	ICカード	ハードウエア	セキュリティ機能	ありそうもない				ありそうもない
Loss32	プログラムによる侵入（サーバ攻撃）	サーバ	サーバ通信	データベース	ほとんどない				ほとんどない
Loss33	人による侵入	サーバ	サーバ通信	データベース	ほとんどない				ほとんどない
			サーバコンソール	データベース	ありそうもない				
Loss34	盗聴・改竄された通信データによる侵入	サーバ	サーバ通信	データベース	ほとんどない				ほとんどない

インパクト分析

ロスID	ロス	影響範囲	破綻する安全目標	深刻度
Loss1	ICカードデータ不整合	特定のカード	(1),(2)	重大
Loss2	ICカードが間違った処理をする	特定のカード	(1),(2)	重大
Loss3	ICカードの処理と異なる結果を送信	特定のカード	(1),(2)	重大
Loss4	ICカードが反応しない	特定のカード	(1),(2)	重大
Loss5	ICカード処理停止	特定のカード	(1),(2)	重大
Loss6	ICカードレスポンス内容間違い	特定のカード	(1),(2)	重大
Loss7	ICカードが破損している	特定のカード	(1),(2)	重大
Loss8	ICカードへ意図しない処理を命令	複数のカード	(1),(2)	重大
Loss9	R/Wが反応しない	複数のカード	(1)	重大
Loss10	ICカード処理結果の誤認	複数のカード	(1),(2)	重大
Loss11	システムが反応しない	特定のドア	(1),(2)	重大
Loss12	災害情報無受信	複数の人	(3)	非常に深刻
Loss13	災害情報誤認	複数のドアまたは複数の人	(3)	非常に深刻
Loss14	ドアセンサー故障	特定のドア	(2)	軽微
Loss15	施錠しない	特定のドア	(2)	軽微
Loss16	鍵が開かない	複数のカード	(1)	重大
Loss17	ドア状態認識しない	特定のドア	(2)	軽微
Loss18	通信時間不十分	特定のカード	(1)	軽微
Loss19	サーバ受信認証データの誤り	特定のカード	(1),(2)	重大
Loss20	サーバ受信認証データの破損	特定のカード	(1),(2)	重大
Loss21	サーバと通信ができない	複数のカード	(1),(2)	重大
Loss22	サーバで認証データの取り違え	複数のカード	(1),(2)	重大
Loss23	サーバで認証データの送信間違い	特定のカード	(1),(2)	重大
Loss24	認証結果間違い	特定のカード	(1),(2)	重大
Loss25	不正コマンドデータによるアクセス	特定のカード	(1),(3)	重大
Loss26	不正取得したコマンドデータによるア	複数のカード	(1),(2),(3)	非常に深刻
Loss27	盗聴・改竄したコマンドデータによるア	特定のカード	(1),(3)	重大
Loss28	盗聴した情報からVRICS　Titleデータ	特定のサービス	(1),(3)	重大
Loss29	改竄プログラムのインストール	特定のカード	(1),(3)	重大
Loss30	データアクセス中の電源途絶	特定のカード	(3)	軽微
Loss31	ICチップを故障させることによるセキ	特定のカード	(1),(3)	重大
Loss32	プログラムによる侵入（サーバ攻撃）	全サービス	(1),(2),(3)	非常に深刻
Loss33	人による侵入	全サービス	(1),(2),(3)	非常に深刻
Loss34	盗聴・改竄された通信データによる侵	全サービス	(1),(2),(3)	非常に深刻