情報処理学会論文誌 Vol.59 No.1 199–210 (Jan. 2018)

USB周辺機器接続のセキュリティリスク分析における アセット導出手法

城間 政司[1,a)] 西尾 泰彦[1] 井上 博之[1,2]

受付日 2017年4月29日, 採録日 2017年10月3日

概要：コンピュータや周辺機器のデータ転送や保存，充電等の手段としてUSBが広く利用されている．一方，USBを悪用する脅威として，USBフラッシュドライブを介したマルウェア感染やUSB周辺機器になりすました機器で不正操作をする方法等，様々な脅威事例が報告されている．このような脅威に対してすべての対策を講じることは困難であり，対策すべき脅威への優先度をつけるためにセキュリティリスク分析が有効である．セキュリティリスク分析では，守るべき資産であるアセットの導出，アセットに対する脅威の分析，脅威のリスク評価，対策の施行という手順が一般的である．セキュリティリスク分析で最初に行われるアセット導出の主な方法としてアセットの分類によるガイドワード分析があるが，セキュリティリスク分析の知識や経験に左右される．そこで本論文では，周辺機器接続に関するセキュリティリスク分析のアセット導出手法として，分析対象の機器につながる周辺機器を洗い出し，周辺機器からアクセスできる機能や情報をアセットとして導出する手法を提案する．アセット導出の結果は，SysMLのブロック定義図と内部ブロック図で可視化される形で記述する．提案手法の評価としてiOS端末のアセット導出に提案手法を適用したケーススタディを行い，提案手法と従来手法で導出するアセットの比較を行った．その結果，従来手法とは異なる種類のアセットや警告から重要レベルの脅威の対象となるアセットの導出が可能であることが分かった．

キーワード：セキュリティリスク分析，アセット導出，USB，SysML

Asset Derivation Method for Security Risk Analysis of USB Peripheral Device Connection

Tadashi Shiroma[1,a)] Yasuhiko Nishio[1] Hiroyuki Inoue[1,2]

Received: April 29, 2017, Accepted: October 3, 2017

Abstract: USB is widely used for data transfer, electrical charging, etc. Security researchers report USB threats such as malware infections caused by USB flash drives and illegal operations with spoofed USB peripheral devices. It is impossible to employ measures against all threats because of their cost. Security risk analysis is considerably useful for setting the priorities of threats. General security risk analysis consists of the following steps: asset derivation, threat analysis of derived assets, threat evaluation, and employment of measures. The general asset derivation method applied at the beginning of security risk analysis is guide word analysis. However, this method requires professional knowledge and experience of security risk analysis. In this paper, we propose an asset derivation method for the security risk analysis of peripheral device connections. This method determines the peripheral devices that connect to an analysis target device and its information and functions that the peripheral devices can access. We describe asset derivation results using the block definition diagram and internal block diagram of SysML to visualize the results. We evaluate the proposed method by applying it to derive the assets of an iOS device and comparing the assets derived using the proposed and general methods. We found the assets derived using the proposed method contain medium and high security risk assets.

Keywords: security risk analysis, asset derivation, USB, SysML

© 2018 Information Processing Society of Japan

1. はじめに

コンピュータやスマートフォンをはじめ，機器どうしのデータ転送や充電等の手段としてUSBインタフェースが広く利用されている．USBの規格は時代の流れと需要に合わせて拡張されており，データ転送の高速化や電源供給量の大容量化，コネクタ形状の改良が行われている．あらゆる機器がUSBを使用してつながっており，今後も有線接続のデファクトスタンダードとして重要性が高まっていくことが予想される．一方，USBを悪用したセキュリティ上の脅威が多数報告されている [1], [2]．USBフラッシュドライブは旧来からマルウェアの感染経路やデータ漏えいの手段として悪用されている．また，近年ではUSBフラッシュドライブのファームウェアを書き換えて正常な機器になりすます方法が発表されており，不正な装置としての検知が難しいものもある [3]．このようにUSBの利便性は高くなる一方で新たな悪用ケースも増えている．このようなケースでは信頼できるデバイスのみを利用することでセキュリティ上の脅威を軽減できるが，業務では外部から持ち込んだUSBフラッシュドライブを利用するケースや，公共施設におけるUSB充電サービス等を外出先で利用するケースがあり，信頼できない装置に接続することもある [4], [5], [6]．このようなケースを想定し，組織として信頼できないデバイスの使用是非の判断やUSBを使用する機器のセキュリティ要件を設けるために，USB周辺機器と接続することに対するリスク分析（以降，セキュリティリスク分析と呼ぶ）が有効である．

セキュリティリスク分析の手順は，守る資産であるアセットを導出し，その資産に対するセキュリティ上のリスクを想定，対策を講じ，リスクの承認を行う [7]．これらの手順の始めに行うアセット導出は，セキュリティリスク分析の結果に影響する重要な工程の1つである．本論文ではアセットの導出手法として，USBにつながる周辺機器やデバイスクラスに着目し，セキュリティリスク分析の対象となる端末につながる機器を洗い出し，その機器からアクセス可能な機能や情報をアセットとして導出する手法を提案する．本提案手法は，分析対象端末の俯瞰的視点ならびに内部的視点に着目したアセット導出によりセキュリティリスク分析をサポートするものである．

本論文の構成は以下のとおりである．2章では，USBの脅威に関する研究やセキュリティリスク分析に関する既存内容について述べる．3章では，提案手法のコンセプトと手順について述べる．4章では，スマートフォンへの周辺機器接続のセキュリティリスク分析として提案手法を適用したケーススタディとその結果の考察について述べる．最後に，5章で本論文をまとめる．

[1] 重要生活機器連携セキュリティ協議会研究開発センター
Connected Consumer Device Security Council (CCDS), Naha, Okinawa 900–0005, Japan
[2] 広島市立大学大学院情報科学研究科
Graduate School of Information Sciences, Hiroshima City University, Hiroshima 731–3194, Japan
[a] shiroma@ccds.or.jp

2. 関連研究

2.1 USBの脅威に関する研究

USBを悪用する脅威は多数研究されており，それらに対する対策も報告されている．USBの周辺機器接続による一般的な脅威としては，マスストレージ内に保存されたマルウェアの自動再生やMicrosoft Officeのマクロ機能を通して実行，感染するものがある．さらに，キーボードやマウスといった標準USBデバイスクラスのデバイスになりすまして不正操作を行う事例もある [1]．文献 [3] のBadUSBと呼ばれる事例では，市販のUSBフラッシュドライブのファームウェアを書き換えてUSB機器のなりすましによる不正操作が可能であることを実証している．一方，このような脅威への対策として多数の研究報告がされている [8], [9]．ただし，すべての対策を適用することはコストや利便性とのトレードオフの関係上難しい．そこで，それぞれのリスクを分析したうえでどの対策をとるのかを議論する必要がある．このようなセキュリティ上のリスクを分析するやり方として脅威分析を起点とした方法がある．

2.2 セキュリティリスク分析手法とアセット導出

脅威分析を起点としたセキュリティリスク分析手法においては，アタックツリーを用いる方法がある [1]．アタックツリーは攻撃者が望むゴールを設定し，そのゴールを達成するために必要な手順をブレークダウンしていく手法である．ブレークダウンした手順のノードが実行されないようにすることで脅威への対策を講じることができる．そのほかには，守るべき資産や機器の動作に対する脅威をガイドワードに基づいて連想するSTRIDE手法がある [11]．また，各種セキュリティリスク管理のガイドラインではリスク分析手法としてアセットを起点とした手法をあげている [12], [13], [14]．このようなセキュリティリスク分析手法では，守るべき資産を想定することから分析を開始し，それをいかにして守るかという視点で資産を列挙する．本論文では，この手順をアセット導出と呼ぶ．

アセット導出の手法は，守るべき機能や情報を連想するためのガイドワードと，仕様書や設計書等を基にアセットを導出する手法が一般的である．一例としてガイドワードによるアセット導出の流れを**図1**に示す．文献 [7] はIoT機器向けのガイドワードで，本来機能，IoT機能，情報資産という分類を示している．本来機能とは，機器が持つ主たる機能のことで，たとえば，スマートフォンであれば，本来機能は，通話，メール，音楽再生の機能．IoT機能は，モバイルデータ通信やBluetooth，Wi-Fi等外部との通信

© 2018 Information Processing Society of Japan

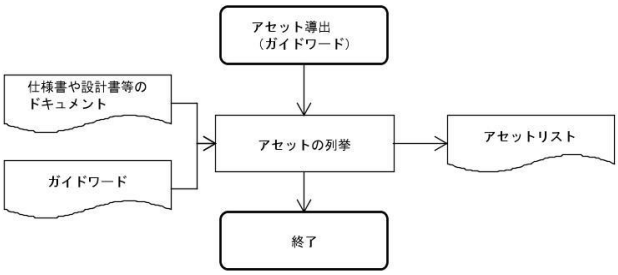

図 1 ガイドワードによるアセット導出の流れ
Fig. 1 Flow of asset derivation using guide word.

に使用する機能．そして，情報資産は，音声や画像等のコンテンツ，ユーザ情報，機器情報等の情報と分類できる．Theoharidou らは，スマートフォンに対するセキュリティリスク分析を実施し，その過程でアセットのガイドワードとして，デバイス，通信機能，データ，アプリケーションの 4 つの分類をあげている [15]．各分類はそれぞれ，デバイスはバッテリや CPU 等，通信機能は Bluetooth や Wi-Fi，携帯網通信等，データは個人情報や認証情報，メール等，アプリケーションはスマートフォンにインストールされているアプリケーションを示す．このように様々なガイドワードによる分類が提案されており，アセットを導出する上で重要なヒントとなる．

アセットを基にセキュリティリスク分析を行う手法は，セキュリティの脅威の対象となるアセットの導出内容がセキュリティの知識や経験に左右されるという課題がある [16]．この課題に対して，各セキュリティガイドラインや研究論文で提唱されているガイドワードは，セキュリティの脅威の対象になりうるアセットの分類を示したものとなっており，脅威の対象となるアセットの導出に有用である．ただし，ガイドワードを用いる手法は，ガイドワードそのものや，ガイドワードと照らし合わせる仕様書や設計書に記載されないアセットの導出が難しいという問題がある．

3. 周辺機器接続によるセキュリティリスク分析のためのアセット導出手法

接続する周辺機器を基に，周辺機器からアクセスできるアセットやそのアセットに対する脅威を確認することによってアセット導出をする手法を提案する．本提案手法は，BadUSB のような正常な USB 周辺機器になりすます不正な機器の接続を想定し，つながる周辺機器から各アセットへアクセスする作業を手順化したものである．これにより，セキュリティリスク分析の知識や経験に依存せず，周辺機器の操作等からアセット導出を行うことができる．また，本提案手法は，導出の過程を記録することでアセットの関係を表現できるという特徴もある．

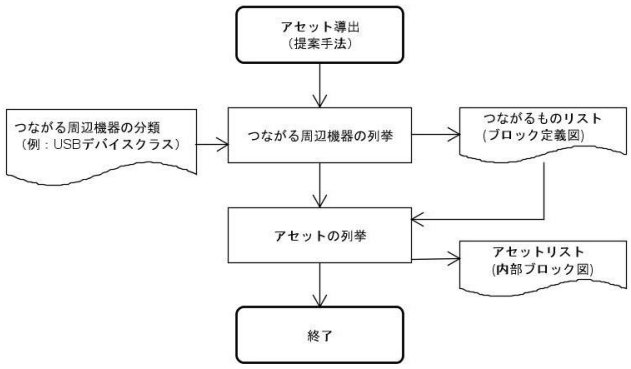

図 2 提案手法によるアセット導出の流れ
Fig. 2 Flow of asset derivation using proposal method.

3.1 本論文におけるアセットの定義

一般的なアセットはセキュリティリスク分析対象のドメインに合わせて定義されている．たとえば，ソフトウェア開発におけるドメインでは，守りたいもの，攻撃者が欲しいもの，左記への踏み台となるものと定義している [16]．また，IoT 機器やコンシューマ製品開発におけるドメインでは，IoT 機能，本来機能，情報，その他のようにアセットを定義している [7]．

本論文では，分析対象として USB インタフェースを備える機器とソフトウェアを対象とし，アセットを次のように定義する．

- 機能：アプリケーション機能や物理的な入出力機能等
- ユーザ情報：パスワードや電話番号，写真，動画，メール内容等，利用者個人に結び付く情報やデータ
- 設定情報：システム設定や IP アドレス等，攻撃に利用される可能性のある設定情報

つながる周辺機器からアクセスできる機能や情報を探す作業を通してこれらのアセットの導出を行う．

3.2 提案手法のコンセプト

本提案手法は，分析対象となる機器に周辺機器を接続した際にどのような脅威が起こりうるかという観点から守るべきアセットを導出する．攻撃者が入り口からどのように侵入していくかをシミュレートすることでアセットまでの経路を探索する．まず，分析対象を選定し，そのインタフェースにつながる周辺機器を導出する．たとえば，スマートフォンの場合，USB ポートをインタフェースとし，つながる周辺機器を洗い出す．次に，そのつながる周辺機器を使って可能な操作やアクセス可能なデータをアセットとして機能や情報を探すアセット導出作業を行う．

提案手法によるアセット導出の流れを**図 2** に示す．従来手法は仕様書や設計書等のドキュメントとガイドワードを照らし合わせてアセットを導出していくが，提案手法はつながる周辺機器を基にアセットを導出する点が異なる．エンドユーザレベルのリスク分析や第三者機関によるセキュ

© 2018 Information Processing Society of Japan

リティ検証業務では，仕様書や詳細なマニュアルが入手できないケースがあり，本手法は，このようなドキュメントが入手できないケースにも適用可能である．また，本手法は，分析対象のインタフェースを起点としてアクセス可能なアセットを導出していくため，アセットそのものだけでなくアセットどうしの関係やインタフェースからの経路をあわせて導出することができる．

アセット導出の結果を可視化するため，SysML [17] のブロック定義図，ならびに，内部ブロック図を用いたモデル化を行う．ブロック定義図とは，システムの部品やコンポーネントを俯瞰的に示した図である．たとえば，スマートフォンにヘッドセットを接続するという関係がある場合，スマートフォンとヘッドセットの 2 つのブロックを線で結ぶ．ブロック定義図により，システムの部品やコンポーネントの関係を俯瞰的に示すことができる．内部ブロック図とは，ブロック定義図で定義したブロックの内部構造を示す図である．たとえば，スマートフォンにキーボードを接続する例では，キーボードをつないだ後，どのような機能にアクセスしながらアセットにたどり着くかを分析対象内部のブロックどうしを矢印で結んで記載していく．以上のように，つながる周辺機器を導出した結果をブロック定義図で表し，つながる周辺機器から導出したアセットや脅威の関係を内部ブロック図で表すという 2 段階の手順によりアセットの導出とその関係の可視化を行う．

なお，2.1 節で述べたような USB に関連するリスク分析で提案手法を用いるため，本論文では USB の周辺機器を主な周辺機器として説明するが，提案手法は USB のように周辺機器が定義されているプロトコルに対しても適用可能である．たとえば，周辺機器がプロファイルとして定義されている Bluetooth にも同様に適用可能であり，Ethernet や Wi-Fi のようにつながる周辺機器が明確に定義されていないものに対しては周辺機器の定義の代わりに Security Cube [18] のような分類モデルを用いることで適用可能である．

3.3 つながる周辺機器の導出

まず，分析対象となる機器を選定する．分析対象の例としては，スマートフォン，ノート PC 等の USB インタフェースを備える端末が該当する．iOS の端末には Lightning インタフェースが備わっているが，USB と互換性があるため，分析対象機器として同様に選定可能とする．以降，USB や Lightning を含む USB に互換性のあるインタフェースを USB 関連インタフェースと呼ぶ．

次に，分析対象の USB 関連インタフェースに接続しうる周辺機器やホストデバイスを列挙する．本論文では，USB 周辺機器，USB ホスト端末，HDMI 等別のプロトコルに変換して接続する周辺機器（以降，プロトコル変換周辺機器と呼ぶ）の 3 種類のつながる周辺機器を定義し，それぞれについて導出していく．各つながる周辺機器の導出手順は以下のとおりである．

表 1 USB 標準デバイスクラス一覧
Table 1 List of USB device classes.

Class Name	Class ID	デバイス・用途例
Audio	0x01	マイク，スピーカー，ヘッドセット
CDC	0x02	イーサネットカード
HID	0x03	キーボード，マウス
Image	0x06	PTP/MTP（スマートフォン等の写真・映像データ転送）
Printer	0x07	プリンタ
Mass Storage	0x08	USB フラッシュドライブ
Hub	0x09	USB ハブ
Video	0x0E	Web カメラ
Wireless Controller	0xE0	Bluetooth
Vendor Specific	0xFF	ベンダ独自デバイス

つながる周辺機器 1：USB 周辺機器

分析対象がホスト端末として動作する場合を想定し，USB 周辺機器を列挙する．分析対象に対応するすべての USB 周辺機器製品を列挙することは困難であるため，網羅的に列挙するために**表 1** のような USB 標準デバイスクラス [19] を参考にする．この USB 周辺機器のうち分析対象に互換性のある周辺機器を，デバイスクラス 1，デバイスクラス 2，…等のように列挙していく．デバイスクラスのサブクラスがある場合，それらについても同様に列挙する．

つながる周辺機器 2：USB ホスト端末

分析対象が USB 周辺機器として動作する場合，つながる周辺機器は USB ホスト端末として動作する．たとえば，分析対象であるスマートフォンに PC を接続した場合は，PC が USB ホスト端末となり，スマートフォンが USB 周辺機器となる．このとき，分析対象が USB 周辺機器として提供するデバイスクラスを列挙する．この場合も前述の USB 周辺機器の列挙と同様に，表 1 の USB 標準デバイスクラスを参考にして列挙する．この USB ホスト端末に互換性のあるデバイスクラスを，デバイスクラス 1，デバイスクラス 2，…のように列挙して，列挙したデバイスクラスをつなげてアセットを探す作業を行う．

つながる周辺機器 3：プロトコル変換周辺機器

最後に，USB を別のプロトコルに変換してつながる周辺機器を列挙する．たとえば，USB Type-C の Alternate Modes では USB を HDMI や MHL 等の規格に変換する仕様がある [2]．さらに，USB インタフェースを HDMI に変換するアダプタのようなベンダ独自製品では HDMI や VGA 等に変換して接続するケースもある．これらのアダプタを用いてつながる周辺機器について，周辺機器 1，周辺機器 2，…のように列挙する．

上記 3 つの手順により導出したつながる周辺機器と分析

© 2018 Information Processing Society of Japan

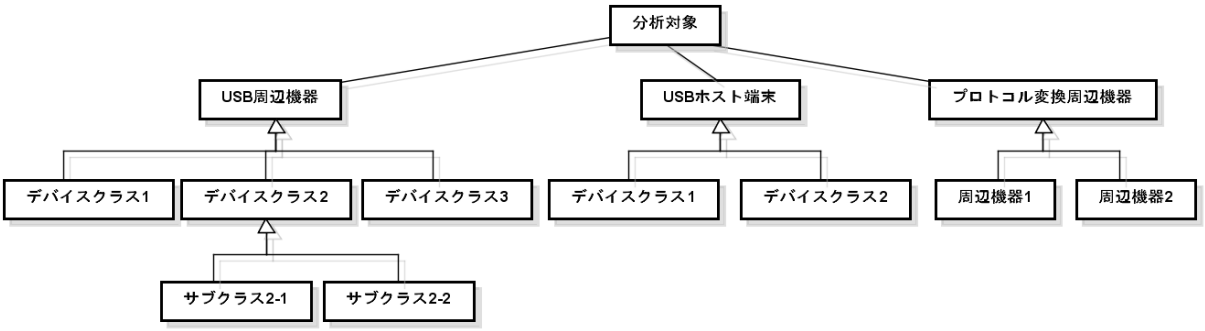

図 3　つながる周辺機器と分析対象の関係を表すブロック定義図
Fig. 3　Block definition diagram of relationship between analysis target and connectable devices.

対象の関係について，SysML のブロック定義図をモデリングツール astah [21] で記述すると**図 3** のように表すことができる．ルートとなるブロックには分析対象を置く．このルートブロックに対し，つながる周辺機器として定義した USB 周辺機器，USB ホスト端末，プロトコル変換周辺機器の 3 つのブロックに分岐させる．そして具体的な USB 周辺機器を表すブロックを作成し，USB 周辺機器ブロックと汎化関係で結ぶ．汎化関係で結ぶことにより，各周辺機器の抽象度の関係を明示する．デバイスクラスにサブクラスが存在する場合，同様に汎化関係で結ぶ．USB ホスト端末についても，USB ホスト端末へ提供する周辺機器機能をデバイスクラス 1，デバイスクラス 2，…のように列挙し，USB ホスト端末ブロックとその下に位置するデバイスクラスを汎化関係で結ぶ．プロトコル変換周辺機器のブロックにおいても，周辺機器を周辺機器 1，周辺機器 2，…のように列挙する．プロトコル変換周辺機器についても同様に，周辺機器を汎化関係で結ぶ．以上の流れにより，分析対象につながる周辺機器の導出結果をブロック定義図により表現し，分析対象とつながる周辺機器との関係を俯瞰的にとらえることができる．

3.4　つながる周辺機器によるアセットの導出

3.3 節で導出したつながる周辺機器を基にして，USB 関連インタフェースを介してアクセス可能なアセットを検証することによって，つながる周辺機器による脅威とその影響を受けるアセットを導出する．たとえば，分析対象を iOS 端末，キーボードをつながる周辺機器とする場合を想定し，キーボードで可能な操作からアセットを導出する．このとき，机上ではなく，実際にキーボードを接続して確認することで検証が容易になる．つながる周辺機器の操作の試行からアセットを導出する様子を表現するために内部ブロック図を作成していく．内部ブロック図を用いることでつながる周辺機器から分析対象内部のどのような機能をたどってアセットとなる機能や情報にたどり着けるかを表すことができる．アセットの導出および内部ブロック図の作成手順を以下に示す．

3.4.1　内部ブロック図の構成要素の定義

つながる周辺機器を内部ブロック図の内部パートとする．内部パートとは “ブロック名：カテゴリ” の形式の文字列を実線の四角で囲んで表現される SysML の内部ブロック図の要素の 1 つである．また，分析対象のアセットとなる機能や情報をつながる周辺機器の内部ブロック図の外部パートとする．外部パートとは “ブロック名：カテゴリ” の形式の文字列を点線の四角で囲んで表現される SysML の内部ブロック図の要素の 1 つである．各外部パートのカテゴリを次のように定義する．

- 機能：機能アセット
- 情報：ユーザ情報アセット，設定情報アセット

ここで，外部パートのカテゴリを上記のように置いているのは，アセットが機能と情報に大別されるためである．各ブロックどうしの入出力は内部ブロック図のアイテムフローの矢印で表現する．また，内部ブロック図のノートのカテゴリを次のように定義する．ノートは SysML の内部ブロック図の要素の 1 つであり，ブロックやアイテムフローの内容を補足するために使用される．各ノートは SysML の記法に従い，補足対象となる要素と点線で結ぶ．また，各ノートのカテゴリは SysML の要素の分類を表すステレオタイプを用い，《カテゴリ》の形式で表現する．

- Threat：前述のアセットが侵害されることによって被る内容やアセットを踏み台として利用者以外に悪影響を与える内容
- Requirement：機能の操作やユーザ情報，設定情報のアクセスに必要な条件等

なお，上記以外にも必要に応じてノートのカテゴリを追加してもよい．これらのノートを記載していくことで，アセットの導出にあわせて周辺機器をつなげることによる脅威や成立条件等も補足することができる．以上のブロックやノートを基に内部ブロック図を作成していく．

3.4.2　周辺機器をつなげることによるアセットの導出

3.3 節で導出したつながる周辺機器を分析対象につなげ

© 2018 Information Processing Society of Japan

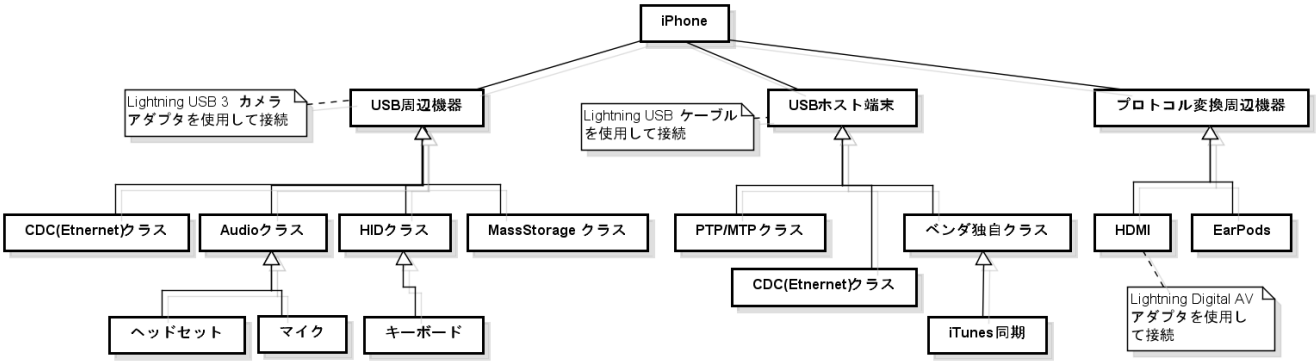

図 5　iOS 端末につながる周辺機器の分析結果
Fig. 5　Derivation result of connectable devices to iOS.

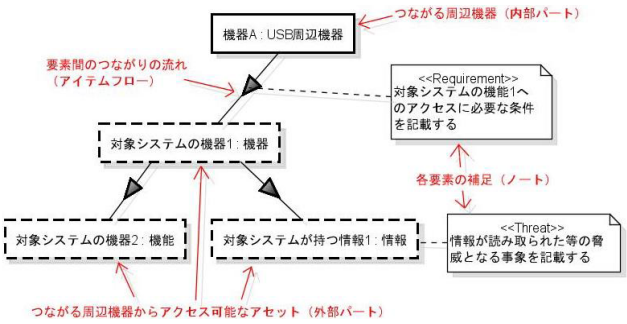

図 4　アセット導出手順を表現する内部ブロック図（赤字は各要素の補足説明）
Fig. 4　Internal block diagram of asset derivation steps (Element descriptions are written in red).

てアクセスできるアセットを検証し，各つながる周辺機器の内部ブロック図を作成する．内部ブロック図の作成手順は以下のとおりである．

手順 1：つながる周辺機器を内部パートとしてルートブロックを記載する．

手順 2：つながる周辺機器の操作やデータの入出力によりアクセス可能な機能や情報が判明した場合，その機能や情報を外部パートとして記載する．このとき，アクセスの成立条件があれば Requirement カテゴリのノートとして記載する．

手順 3：手順 2 で記載したブロックに対する脅威が想定できる場合，Threat カテゴリのノートとして脅威の内容を記載する．

ここで外部パートとして記載したブロックが分析対象のアセットであり，アセットに関する脅威も Threat カテゴリのノートで表現できる．作成する内部ブロック図の例を**図 4** に示す．この図は，USB 周辺機器を分析対象につないでアクセスできた機能や情報アセット，アセットに関連する脅威等の関係を表している．

以上の手順により，つながる周辺機器の接続による分析対象への入出力の試行の繰返しから，アクセスした機能や情報をアセットとして導出できる．また，この導出結果を内部ブロック図で表現することによって，つながる周辺機器やアセットの関係を可視化することができる．

4.　評価と考察

提案したアセット導出手法の有用性について，具体的な例に適用した結果を基に評価，考察する．

4.1　iOS 端末に対するアセット導出（ケーススタディ）

本提案手法のケーススタディとして，iOS 端末に対するアセット導出を行った．分析対象は以下のとおりである．

- 端末：Apple iPhone 7 plus 32 GB モデル
- OS：iOS 10.2.1
- USB 関連インタフェース：Lightning インタフェース

まず，3.3 節の手順に従い，つながる周辺機器を導出した．つながる周辺機器の導出結果を図 3 と同様にモデリングツール astah で記述すると**図 5** のようになる．今回のケーススタディでは，各周辺機器やホスト端末を実際に接続し，認識された機器のみ記述している．iPhone はヘッドセットやマイク，キーボード等に対応している．また，HDMI 接続用の Lightning Digital AV Adaptor や EarPods 等のベンダ独自製品が存在する．

次に，導出したつながる周辺機器を基に，3.4 節の手順に従ってアセット導出を行った．このアセット導出の過程で作成した内部ブロック図のうち，下記のつながる周辺機器について例示する．

- USB 周辺機器の例：キーボード
- USB ホスト端末の例：PTP/MTP クラス
- プロトコル変換周辺機器の例：HDMI 接続モニタ

なお，本検証の前提条件として，検証者が分析対象の画面を直接見たり，直接操作したりして得られた情報は除外する．

4.1.1　キーボードの接続によるアセット導出

キーボードの接続に関する内部ブロック図の作成結果を**図 6** に示す．キーボードを接続した場合，キー入力により音楽の再生状況を制御できるため，音楽再生制御機能を外

© 2018 Information Processing Society of Japan

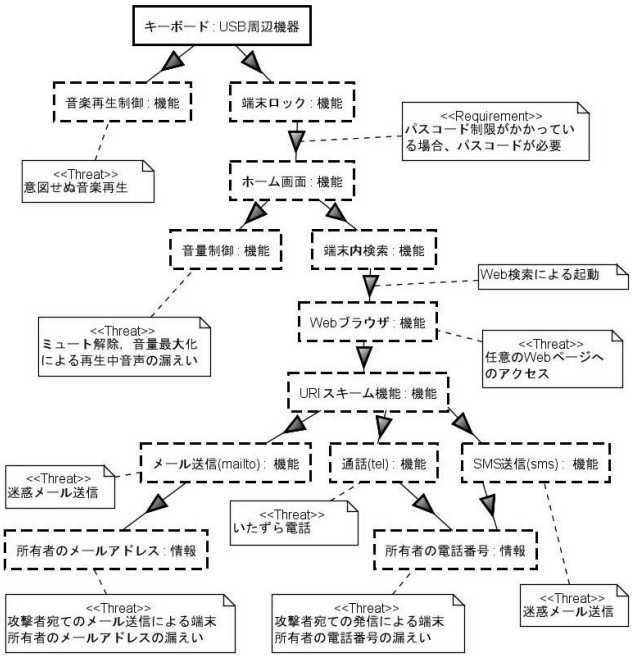

図 6 キーボード接続によるアセット導出の内部ブロック図
Fig. 6 Internal block diagram of asset derivation with keyboard connection.

部パートとして記載し，想定しうる脅威を Threat カテゴリのノートとして記載する．また，端末のロック機能にもアクセスできることから，端末ロック機能を外部パートとして記載する．端末ロックを解除するときにパスコードを求められる場合があるため，Requirement カテゴリのノートとしてパスコードが必要な旨を記載する．次に，ロックを解除すると，ホーム画面が開かれるため，外部パートとしてホーム画面の機能を記載する．次に，ホーム画面からキーボードで操作できることを検証する．たとえば，検索用のショートカットキーを入力し，端末内検索機能を呼び出せる．このとき，端末内検索機能を外部パートとして記載する．端末内検索機能では，入力した文字列の端末内データの検索結果や Web 検索候補等のメニューが表示される．本検証では操作画面を直接見た情報を利用できない前提条件のため，端末内データ等の情報を得ることはできない．ただし，端末内検索時に無作為な文字列を意図的に入力して Web 検索項目を選択することにより，一定の手順のキー入力で Web ブラウザを起動できる．すなわち，端末内検索から Web ブラウザを起動することができる．このため，アクセスできる機能である Web ブラウザを外部パートとして記載する．

次に，Web ブラウザを起動した後，キーボードで操作できることを検証する．たとえば，キーボードショートカットでアドレスバーにカーソルを移動し，任意の Web ページを開いたり，URI スキームを使用して他の機能を呼び出したりできる．ここで，任意の Web ページを開けるとフィッシングサイト等悪意のある Web サイトへの誘導が

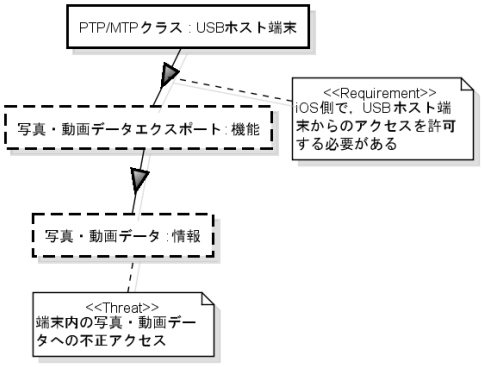

図 7 ホスト端末への PTP/MTP 接続の内部ブロック図
Fig. 7 Internal block diagram of PTP/MTP connection to host device.

可能なため，Threat カテゴリのノートとしてその旨を記載する．また，URI スキーム機能を外部パートとして記載する．URI スキーム機能を用いると，mailto スキームを使用したメール送信や tel スキームを使用した通話，sms スキームを使用した SMS メッセージ送信を行うことが可能である．この 3 つの URI スキームに関する機能を外部パートとして記載する．このとき，攻撃者のメールアドレスへのメール送信や電話番号への通話発信，SMS メッセージ送信により，端末所有者のメールアドレスや電話番号が知られてしまうという脅威がある．また，メール送信や通話機能，SMS 機能は迷惑メール送信やいたずら電話をかけることに利用される可能性がある．これらの脅威についても Threat カテゴリのノートとして記載する．以上のように，キーボードを分析対象につなぐことによるアセット導出と内部ブロック図作成を行った．

4.1.2 ホスト端末への PTP/MTP 接続によるアセット導出

ホスト端末への PTP/MTP 接続に関する内部ブロック図を**図 7** に示す．iPhone を PC 等のホスト端末に接続すると，ホスト端末によるアクセスを許可するかどうかを確認するダイアログが表示される．このとき，アクセスを許可すると PTP/MTP による端末内の写真や動画データへのアクセスがホスト端末から可能となる．内部ブロック図において，同ダイアログを Requirement カテゴリのノート，写真・動画データのエクスポート機能を機能カテゴリの外部パート，写真・動画データを情報カテゴリの外部パート，写真・動画データを窃取されるという脅威を Threat カテゴリのノートとして記載する．以上のように，ホスト端末を分析対象につなぐことによるアセット導出と内部ブロック図の作成を行った．

4.1.3 HDMI 周辺機器接続によるアセット導出

HDMI 周辺機器接続に関する内部ブロック図を**図 8** に示す．iPhone は専用の HDMI アダプタを用いると HDMI 接続でき，HDMI を介してモニタに接続すると iPhone の操作画面がミラーリングされる．このとき，iPhone の所有

© 2018 Information Processing Society of Japan

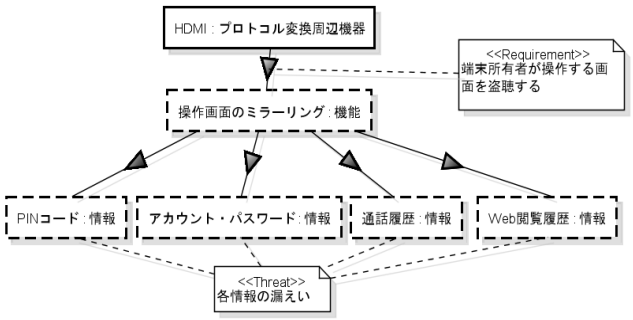

図 8　HDMI 接続の内部ブロック図
Fig. 8　Internal block diagram of HDMI connection.

者がミラーリングに気づかずに操作すると操作画面を盗聴されてしまうため，操作画面に映る情報はアセットとして認識できる．たとえば，端末ロック解除用のパスコードや SNS サイトのログイン用アカウント，通話履歴等の情報が窃取される．内部ブロック図では，操作画面のミラーリング機能および操作画面に映った各情報を外部パートとして記載する．操作画面に映る情報は様々であるが，その一部を記載した．以上のように，プロトコルを変換してつながる周辺機器を分析対象である iPhone に接続し，アセットの導出と内部ブロック図作成を行った．

4.2　提案手法と導出したアセットの評価

本提案手法の有用性の評価として，提案手法と既存のアセット導出法で導出したアセットの比較と，提案手法で導出したアセットに関連する脅威のリスク評価を行う．

4.2.1　提案手法と従来手法により導出したアセットの比較

従来手法であるガイドワードから連想して導出するアセットと提案手法で導出したアセットの内容を比較する．従来手法として 2.2 節で述べた文献 [7] のガイドワード（以降，IPA ガイドワードと呼ぶ）と Theoharidou ら [15] のガイドワード（以降，Theoharidou ガイドワードと呼ぶ）を利用し，各ガイドワードと iPhone のマニュアルドキュメント [22] を照らし合わせてアセットを導出した．本論文では提案手法を用いて導出したアセットとの比較のため，IPA ガイドワードについては，情報資産を情報アセット，本来機能と IoT 機能を機能アセットに分類し，また，Theoharidou ガイドワードについては，データを情報アセット，デバイス，通信機能，アプリケーションを機能アセットに分類する．提案手法のケーススタディで導出したアセットと従来手法に沿って導出したアセットの一覧を **表 2** に示す．表 2 の右側 3 列の記号はそれぞれ，◯が導出できたこと，△が一部導出できたこと，×が導出できなかったことを表す．なお，提案手法で導出したアセット一覧には 4.1.1〜4.1.3 項で示した結果以外の導出結果も含んでいる．

共通して導出できたアセットは，PIN コードや電話番号，写真等の個人に紐づく情報や，通話機能，メール機能等，

表 2　提案手法と従来手法によるアセット導出結果
Table 2　Asset derivation result of the proposed method and general methods.

提案：提案手法，IPA：IPA のガイドワード，T ら：Theoharidou らのガイドワードによる導出結果

No.	アセット名	分類	提案	IPA	T ら
1	ホーム画面	機能	◯	×	×
2	URI スキーム	機能	◯	×	×
3	再生中の音声	情報	◯	×	×
4	写真・動画データインポート	機能	◯	×	×
5	写真・動画データエクスポート	機能	◯	×	×
6	端末内データ全般	情報	◯	×	×
7	操作画面	情報	◯	×	×
8	通話履歴	情報	◯	×	◯
9	Web 閲覧履歴	情報	◯	×	◯
10	端末内検索機能	情報	◯	◯	◯
11	音量制御機能	機能	◯	◯	◯
12	PIN コード	情報	◯	◯	◯
13	メール内容	情報	◯	◯	◯
14	ユーザ個人情報（メールアドレス，電話番号等）	情報	◯	◯	◯
15	音声・写真・動画	情報	◯	◯	◯
16	アカウント・パスワード	情報	◯	◯	◯
17	Wi-Fi，機内モード，テザリング設定情報	情報	◯	◯	◯
18	インターネット・モバイルデータ通信	機能	◯	◯	◯
19	テザリング機能	機能	◯	◯	◯
20	音楽再生機能	機能	◯	◯	◯
21	音声制御機能（メール関連）	機能	◯	◯	◯
22	音声制御機能（通話関連）	機能	◯	◯	◯
23	音声制御機能（設定変更）	機能	◯	◯	◯
24	バックアップ	機能	◯	◯	◯
25	Web ブラウザ	機能	◯	◯	◯
26	通話機能	機能	△	◯	◯
27	メール機能	機能	△	◯	◯
28	SMS 機能	機能	△	◯	◯
29	Web ブックマーク	情報	×	◯	×
30	モバイルデータ通信状況	情報	×	◯	×
31	Bluetooth ペアリング情報	情報	×	×	◯
32	Wi-Fi SSID 情報	情報	×	×	◯
33	Lightning コネクタ	機能	×	×	◯
34	SIM カード	機能	×	×	◯
35	バッテリー	機能	×	×	◯
36	アドレス帳	情報	×	◯	◯
37	クレジットカード情報	情報	×	◯	◯
38	SIM カード情報	情報	×	◯	◯
39	OS 情報	情報	×	◯	◯
40	インストールアプリ一覧	情報	×	◯	◯
41	Bluetooth 機能	機能	×	◯	◯
42	Wi-Fi 機能	機能	×	◯	◯
43	カメラ機能	機能	×	◯	◯
44	NFC 機能	機能	×	◯	◯
45	カレンダー機能	機能	×	◯	◯
46	端末名	情報	×	◯	◯
47	位置情報	情報	×	◯	◯
48	ヘルスケア情報	情報	×	◯	◯
49	指紋情報	情報	×	◯	◯
50	VPN 通信機能	機能	×	◯	◯
51	物理ボタン操作情報	情報	×	×	◯
52	ジェスチャ操作情報	情報	×	×	◯
53	キーボード入力情報	情報	×	×	◯
54	音声入力情報	情報	×	×	◯

一般的な情報や機能の計 19 件となっている．また，従来手法でのみ導出できたアセットは，アドレス帳情報やクレジットカード情報，Web ブックマーク等の個人に紐づく情報や，OS 情報，インストールされたアプリ一覧等のシステムに関する情報の計 26 件となっている．これらのアセットの中には，提案手法の機能アセットであるキーボード操作関連の機能や操作画面の盗聴により導出しうるものも含

© 2018 Information Processing Society of Japan

まれている．提案手法で導出できなかった理由として，分析の試行回数や期間等が影響していると考えられる．提案手法でのみ導出できたアセットは，音量制御機能や再生中の音声情報，ミラーリングされた操作画面，URI スキーム機能等，より細かい具体的な情報や機能の計 7 件となっている．各アセットの情報量や抽象度が異なるため単純な比較はできないが，提案手法では従来手法とは異なるアセットを導出できるという結果が得られた．

4.2.2　導出したアセットに関する脅威のリスク評価

各手法により導出したアセットが重要度の高い脅威の対象となる効果的なアセットかどうかを評価するため，アセットに関連する脅威のリスク評価を行う．提案手法で導出したアセットに関する脅威には，内部ブロック図の Threat カテゴリのノートに記載した脅威を用いる．なお，従来手法はアセット導出のみを行うため，従来手法でのみ導出したアセットに対しては提案手法で導出したアセットと同様に，USB ポート経由で不正アクセスされた場合の脅威を STRIDE 手法 [11] を基に想定した．

脅威のリスク値の算出方法には CVSSv3 [23] と OWASP Risk Rating Methodology [24]（以降，OWASP と呼ぶ）を用いる．CVSSv3 と OWASP 以外のリスク評価方法として，NIST SP800-30 [13] や ETSI TS 102 165-1 [25] 等の方法があるが，CVSSv3 は攻撃の経路や難易度等の攻撃元に関する要素を考慮している．また，攻撃元を考慮する同様なリスク評価手法として CCDS 改良方式 [26] もあるが，CVSSv3 は米国や日本においても標準的に利用されており[*1]，国内外で普及していることから今回のリスク算出方法として選定した．なお，ガイドワードによる従来手法ではアセット導出のみ行うため，CVSSv3 の攻撃元区分や攻撃条件の複雑さ等の判定できない要素については提案手法の評価結果と同様の値を設定して評価した．OWASP は CVSSv3 で考慮されていないプライバシや経済的影響に関する評価要素を考慮しており，CVSSv3 以外の観点での比較のために選定した．提案手法や従来手法で導出した一部のアセットのうち脅威が想定されなかったもののリスク評価は行っていない．

各手法で導出したアセットに関連する脅威のリスク値について評価した結果を**表 3**，そのサマリを**表 4** に示す．提案手法で導出したアセットに関連する CVSSv3 のリスク値を見ると，重要レベルが 2 件，警告レベルが 3 件，注意レベルが 18 件と半数以上が注意レベルとなっている．これらの警告レベル以上の脅威の対象となるアセットは，提案手法で導出できたセキュリティリスク分析における効果的なアセットである．注意レベルとなっている脅威については，PIN コードやメールアドレスの情報や

[*1] National Vulnerability Database（https://nvd.nist.gov/vuln-metrics/cvss）や Japan Vulnerability Notes（https://jvn.jp/）等で利用されている．

表 3　導出したアセットに関する脅威のリスク値

Table 3　Risk value of threat related with derived assets.

CVSSv3：CVSSv3，OWASP：OWASP Risk Rating Methodology によるリスク評価結果
提案：提案手法，IPA：IPA のガイドワード，T ら：Theoharidou らのガイドワード による導出結果

No	アセット名	脅威	CVSSv3	OWASP	提案	IPA	T ら
2	URI スキーム	いたずら電話の発信，迷惑メールの送信	注意 (2.3)	Medium	○	×	×
3	再生中の音声	再生中の音声の漏えい	注意 (2.1)	Low	○	×	×
4	写真・動画データインポート	端末容量の圧迫	注意 (2.1)	Low	○	×	×
5	写真・動画データエクスポート	個人情報の漏えい	注意 (2.3)	Medium	○	×	×
6	端末内データ全般	個人情報，アカウント，パスワードの漏えい	重要(7.2)	Medium	○	×	×
8	通話履歴	個人情報の漏えい	注意 (2.1)	Low	○	×	○
9	Web 閲覧履歴	個人情報の漏えい	警告 (5.1)	Low	○	×	○
11	音量制御機能	ミュート解除等による再生中の音声の漏えい	注意 (2.1)	Low	○	○	○
12	PIN コード	端末が盗難された場合のデータ漏えい	注意 (2.1)	Low	○	○	○
13	メール内容	個人情報の漏えい	注意(2.3)	Low	○	○	○
14	ユーザ個人情報（メールアドレス，電話番号等）	個人情報の漏えい	注意 (2.3)	Low	○	○	○
15	音声・写真・動画	個人情報の漏えい	注意 (2.1)	Medium	○	○	○
16	アカウント・パスワード	アカウントの乗っ取り，なりすまし	警告(6.5)	Medium	○	○	○
18	インターネット・モバイルデータ通信	暗号化に不備のある通信の盗聴や改ざん	重要(7.0)	Medium	○	○	○
19	テザリング機能	通信容量の消費，不正アクセスへの踏み台	注意 (2.3)	Medium	○	○	○
20	音楽再生機能	意図せぬ音楽再生	注意 (2.1)	Low	○	○	○
21	音声制御機能（メール関連）	迷惑メールの送信	注意 (3.7)	Low	○	○	○
22	音声制御機能（通話関連）	いたずら電話の発信	注意 (3.7)	Low	○	○	○
23	音声制御機能（設定変更）	Bluetooth や Wi-Fi 等のオンオフ設定の意図せぬ変更	注意 (3.7)	Low	○	○	○
25	Web ブラウザ	フィッシングサイト等への誘導	警告(5.1)	Medium	○	○	○
26	通話機能	いたずら電話の発信	注意 (2.3)	Medium	△	○	○
27	メール機能	迷惑メールの送信，個人情報の漏えい	注意 (2.3)	Low	△	○	○
28	SMS 機能	迷惑メールの送信，個人情報の漏えい	注意 (2.3)	Medium	△	○	○
29	Web ブックマーク	個人情報の漏えい	注意 (2.1)	Low	×	○	×
31	Bluetooth ペアリング情報	個人情報の漏えい	注意 (2.1)	Low	×	×	○
32	Wi-Fi SSID 情報	個人情報の漏えい	注意 (2.1)	Low	×	×	○
36	アドレス帳	個人情報の漏えい	注意 (2.1)	Low	×	○	○
37	クレジットカード情報	個人情報の漏えい，不正利用による金銭的損害	警告(4.9)	Medium	×	○	○
40	インストールアプリ一覧	個人情報の漏えい	注意 (2.1)	Low	×	○	○
41	Bluetooth 機能	個人情報の漏えい，不正利用による金銭的損害	重要(7.2)	Medium	×	○	○
42	Wi-Fi 機能	暗号化に不備のある通信の盗聴や改ざん	重要(7.2)	Medium	×	○	○
43	カメラ機能	個人情報の漏えい	注意 (2.1)	Low	×	○	○
44	NFC 機能	個人情報の漏えい，不正利用による金銭的損害	注意 (2.1)	Medium	×	○	○
45	カレンダー機能	個人情報の漏えい	注意 (2.1)	Low	×	○	○
46	端末名	個人情報の漏えい	注意 (2.1)	Low	×	○	○
47	位置情報	個人情報の漏えい	注意 (2.1)	Low	×	○	○
48	ヘルスケア情報	個人情報の漏えい	警告(4.3)	Medium	×	○	○
49	指紋情報	個人情報の漏えい	警告(4.9)	Medium	×	○	○
50	VPN 通信機能	暗号化に不備のある通信の盗聴や改ざん	重要(7.0)	Medium	×	○	○
52	ジェスチャ操作情報	PIN コードの漏えい	注意 (2.1)	Low	×	×	○
53	キーボード入力情報	個人情報，アカウント，パスワードの漏えい	警告(4.3)	Medium	×	×	○
54	音声入力情報	個人情報の漏えい	注意 (2.1)	Low	×	×	○

音量制御機能等，漏えいしたり乗っ取られたりしても影響が軽微なものが含まれている．評価値が警告レベルや重要レベルとなっているものは，CDC クラスから導出したインターネット通信機能アセットのように周辺機器を接続するだけで実行できる難易度が低いものや，端末内データのバックアップ機能を悪用した端末内データ全般の窃取の

© 2018 Information Processing Society of Japan

表 4 リスク評価結果のサマリ
Table 4 Summary of risk evaluation result.

	リスク値	提案手法	IPA	Theoharidou
	未評価	5 件	6 件	9 件
CVSSv3	注意	18 件	21 件	25 件
	警告	3 件	5 件	7 件
	重要	2 件	4 件	4 件
	その手法でのみ導出，かつ，警告以上	1 件	0 件	1 件
OWASP	Low	13 件	19 件	22 件
	Medium	10 件	13 件	14 件
	その手法でのみ導出，かつ，Medium 以上	3 件	0 件	1 件

ように影響が大きいものが含まれている．従来手法で導出したアセットに関連するリスク値は，IPA ガイドワード，Theoharidou ガイドワードそれぞれ，重要レベルが 4 件と 4 件，警告レベルが 5 件と 7 件，注意レベルが 21 件と 25 件となっている．OWASP による評価結果は，提案手法，IPA ガイドワード，Theoharidou ガイドワードでそれぞれ Low が 13 件，19 件，22 件，Medium が 10 件，13 件，14 件となっている．また，特定の手法でのみ導出したアセット，かつ，重要度の高い結果となった件数に着目すると，提案手法，IPA ガイドワード，Theoharidou ガイドワードについて，CVSSv3 による評価結果ではそれぞれ 1 件，0 件，1 件であり，OWASP による評価結果ではそれぞれ 3 件，0 件，1 件となっている．

4.3 考察

4.2.1 項の導出アセットの比較では，提案手法と従来手法で異なるアセットが導出される結果が得られた．この結果は，アセット導出の網羅性を高めることにつながり，アセット導出における提案手法の有効性を示している．異なるアセットを導出できた理由として，提案手法と従来手法のアプローチが異なることが考えられる．提案手法は，分析対象につながる周辺機器を想定し，これらの周辺機器からアクセス可能な情報や機能をアセットとして導出する．ガイドワードとドキュメントを基にアセットを導出する従来手法では，URI スキーム機能やバックアップデータである端末内データ全般等の一般的にガイドワードやドキュメントに含まれない機能や情報を導出することが難しい．また，3.2 節で述べたような，詳細な仕様書やマニュアル等が入手できない場合には，ハンズオンを通して実施可能な提案手法が有効である．ただし，従来手法でのみ導出可能なアセットもあることから，提案手法と従来手法を併用できる場合には，併用することでより多くのアセットを導出することが期待できる．

4.2.2 項では，各手法で導出したアセットに関するリスク評価による比較を行った．リスク評価結果の重要度が高いアセットは，脅威の度合いが大きく，守るべき優先度も高くなるため，重要度の高いアセットを導出できることが望ましい．すなわち，リスク評価結果の重要度が高いアセットを導出できること，または，重要度の高いアセットを特定の手法でのみ導出できることがアセット導出手法の有用性の指標と考えられる．CVSSv3 の警告以上の件数，OWASP の Medium の件数では従来手法が多い結果となっている．ただし，提案手法や従来手法でのみ導出した重要度の高いアセットの件数の観点において，CVSSv3 での件数は提案手法と従来手法で同程度であり，OWASP での件数は提案手法が従来手法より多い結果となっている．CVSSv3 と OWASP によるリスク評価が異なる結果となった理由として，OWASP が評価要素としてプライバシや経済的影響を考慮していることや，CVSSv3 での各要素の評価が 4 段階評価であるのに対して OWASP は 10 段階評価のため，評価のばらつきが抑えられていることが考えられる．結果を量的に比較すると，提案手法で導出した重要度の高いアセットの件数は従来手法より少ない結果となっているが，提案手法でのみ導出した重要度の高いアセットは従来手法と同等以上の件数であることから，提案手法には有用性があると考えられる．

また，従来手法はアセット導出のみを行うが，提案手法は導出したアセットに加えて，周辺機器からのアクセス経路やアセットどうしの関係も導出可能という特徴もある．これにより，CVSSv3 のように経路を考慮するリスク評価に導出結果を活用することができる．

5. まとめ

本論文では，周辺機器接続に関するセキュリティリスク分析におけるアセット導出手法を提案した．従来手法はガイドワードからアセットを連想するためセキュリティリスク分析の知識や経験に左右されていたが，本論文ではつながる周辺機器を用いたハンズオン作業によるアセット導出の手順化と SysML を用いたアセットどうしの関係の可視化を特徴とした手法を提案した．提案手法を適用したケーススタディでは，従来手法であるガイドワードによるアセット導出手法とは異なるアセットを導出できることを示した．また，導出したアセットに関連する脅威のリスク評価の結果，警告から重要レベルの脅威の対象となるアセットを提案手法で導出可能なことを示した．今後の課題としては，Bluetooth や Wi-Fi でつながる機器等，USB 以外でも検証することがあげられる．

謝辞 本成果は沖縄県生活機器セキュリティ基盤形成促進事業の補助を受けて行われました．ここに記して謝意を表します．

© 2018 Information Processing Society of Japan

参考文献

[1] Falliere, N., Murchu, O.L. and Chien, E.: W32.Stuxnet Dossier, Symantec Corporation (2011) (online), available from ⟨https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf⟩ (accessed 2017-10-06).

[2] Wang, Z. and Stavrou, A.: Exploiting smart-phone usb connectivity for fun and prot, *Proc. 26th Annual Computer Security Applications Conference* (*ACSAC*), pp.357–366 (2010).

[3] Nohl, K. and Lell, J.: BadUSB - on accessories that turn evil, Black Hat USA (2014).

[4] Meng, W., Lee, W.H., Murali, S.R. and Krishnan, S.P.T.: JuiceCaster: Towards automatic juice filming attacks on smartphones, *Journal of Network and Computer Applications*, Vol.68, pp.201–212 (2016).

[5] Meng, W., Lee, W.H., Murali, S.R. and Krishnan, S.P.T.: Charging Me and I Know Your Secrets!: Towards Juice Filming Attacks on Smartphones, *Proc. 1st ACM Workshop on Cyber-Physical System Security*, pp.89–98 (2015).

[6] Shiroma, T., Nishio, Y. and Inoue, H.: A Threat to Mobile Devices from Spoofing Public USB Charging Stations, *Proc. 35th International Conference on Consumer Electronics*, pp.92–93 (2017).

[7] 情報処理推進機構（IPA）：つながる世界の開発指針，情報処理推進機構（IPA），ISBN 978-4-905318-40-8 (2016).

[8] Angel, S., Wahby, R.S., Howald, M., Leners, J.B, et al.: Defending against malicious peripherals with Cinch, *Proc. 25th USENIX Security Symposium*, pp.397–414 (2016).

[9] Lee, Y. et al.: Cognitive Countermeasures against BAD USB, *Proc. International Conference on BWCCA 2016*, pp.377–386 (2016).

[10] Saini, V., Duan, Q. and Paruchuri, V.: Threat Modeling Using Attack Trees, *Journal of Computing Sciences in Colleges*, Vol.23.4, pp.124–131 (2008).

[11] Shawn, H. et al.: Threat Modeling Uncover Security Design Flaws Using the STRIDE Approach, *MSDN Magazine-Louisville*, pp.68–75 (2006).

[12] ISO/IEC: ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management, ISO/IEC (2011).

[13] NIST: Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, NIST (2012).

[14] Caralli, A.R., Stevens, F.J., Young, R.L. and Wilson, R.W.: *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Software Engineering Institute from Carnegie Mellon University (2007).

[15] Theoharidou, M. et al.: A Risk Assessment Method for Smartphones, *Information security and privacy research*, pp.443–456 (2012).

[16] Shostack, A.: *Threat modeling: Designing for Security*, John Wiley & Sons, ISBN 978-1118809990 (2014).

[17] Object Management Group, Inc.: OMG Systems Modeling Language, Object Management Group, Inc. (online), available from ⟨http://www.omg.org/spec/SysML/⟩ (accessed 2017-10-06).

[18] Sendi, S.A., Jabbarifar, M. and Shajari, M.: FEMRA: Fuzzy Expert Model for Risk Assessment, *2010 5th International Conference on Internet Monitoring and Protection*, pp.48–53 (2012).

[19] USB Implementers Forum, Inc.: USB Device Class Specifications, USB Implementers Forum, Inc. (online), available from ⟨http://www.usb.org/developers/docs/devclass_docs/⟩ (accessed 2017-10-06).

[20] USB Implementers Forum, Inc.: USB 3.1 Specification, USB Implementers Forum, Inc. (online), available from ⟨http://www.usb.org/developers/docs/⟩ (accessed 2017-10-06).

[21] Change Vision, Inc.: astah, Change Vision, Inc. (online), available from ⟨http://astah.net/⟩ (accessed 2017-10-06).

[22] Apple, Inc.: iPhone User Guide, Apple, Inc. (online), available from ⟨https://help.apple.com/iphone/10/⟩ (accessed 2017-10-06).

[23] FIRST.org, Inc.: Common Vulnerability Scoring System v3.0: Specification Document, FIRST.org, Inc. (online), available from ⟨https://www.first.org/cvss/specification-document⟩ (accessed 2017-10-06).

[24] OWASP: OWASP Risk Rating Methodology, OWASP (online), available from ⟨https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project⟩ (accessed 2017-10-06).

[25] European Telecommunications Standards Institute: ETSI TS 102 165-1 V4.2.3 (2011-03), European Telecommunications Standards Institute (2011).

[26] CCDS セキュリティガイドライン WG 車載器 SWG.：製品分野別セキュリティガイドライン車載器編 Ver.2.0，重要生活機器連携セキュリティ協議会 (2017).

城間 政司 （正会員）

2007 年琉球大学工学部情報工学科卒業．2009 年琉球大学大学院理工学研究科博士前期課程修了．2013 年琉球大学大学院理工学研究科博士後期課程単位取得後退学．同年琉球大学医学部附属病院特命一般職員．2016 年より一般社団法人重要生活機器連携セキュリティ協議会（CCDS）研究員，現在に至る．博士（工学）．デジタルアイデンティティ，セキュリティリスクアセスメントに関する研究に従事．

西尾 泰彦 （正会員）

1997 年広島大学工学部第二類（電気系）卒業．1999 年広島大学大学院博士前期課程修了．2002 年同博士後期課程修了．博士（工学）．2002 年株式会社日立製作所ソフトウェア事業部入社．2015 年株式会社チェンジビジョン入社．同年一般社団法人重要生活機器連携セキュリティ協議会（CCDS）研究員（出向）．2017 年より株式会社チェンジビジョン復帰，現在に至る．ソフトウェア信頼性，セキュリティ，安全性モデルの研究に従事．電子情報通信学会会員．

© 2018 Information Processing Society of Japan

井上 博之　（正会員）

1987 年大阪大学工学部電子工学科卒業．1989 年大阪大学大学院工学研究科電子工学専攻修了．1989～2000 年住友電気工業株式会社．1998 年奈良先端科学技術大学院大学情報科学研究科博士後期課程単位取得退学，博士（工学）．2000～2007 年株式会社インターネット総合研究所および株式会社 IRI ユビテック．2007 年より広島市立大学大学院情報科学研究科．現在は，同大学准教授．他に，一般社団法人重要生活機器連携セキュリティ協議会研究開発センターチーフ，SECCON 実行委員，セキュリティ・キャンプ全国大会講師等．広域ネットワークにつながる家電や自動車の情報セキュリティについて，その脆弱性やセキュアな通信プロトコルに関する研究開発に従事．電子情報通信学会，IEEE 各会員．

© 2018 Information Processing Society of Japan