偽装された公共USB充電サービスによるモバイル端末への脅威

城間 政司[1]　西尾 泰彦[1]　井上 博之[1,2]

概要：空港やデパート等の公共施設におけるモバイル充電サービスが普及している．公共充電サービスは利便性が高い一方で，個人情報の漏えいや不正操作の可能性がある．本論文では，公共施設で提供されている充電サービスにおける偽装攻撃の脅威分析モデルを導出し，そのモデルに基づいて具体的な攻撃方法についてまとめた．本攻撃手法を iOS 端末に適用した結果，モバイル充電サービスを偽装した Lightning アダプタケーブルと USB 周辺機器を使用することで，パスワード入力画面の覗き見や端末の不正操作が可能であることを示した．また，この対策として端末に接続されている USB デバイスが意図して接続されているものであるかどうかをユーザに確認するモデルを検討した．

キーワード：モバイル充電サービス, 偽装攻撃, 脅威モデリング, iOS, USB

A Threat to Mobile Devices from Spoofing Public USB Charging Stations

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

Abstract: Mobile charging stations have become popular in airports and cafes. Mobile device owners utilize these outlets without hesitation. However, these charging stations contain potential threats. We build a threat model for spoofing the charging stations that are commonly provided in public places. We verified a spoofing attack that allows the attacker to maliciously peep passwords and manipulate an iOS device using USB devices and cables. As a countermeasure, we devise a model for safe charging that confirms connected USB devices with the user.

Keywords:
Mobile Device Charging Service, Spoofing Attack, Threat Modeling, iOS, USB

1. はじめに

空港やデパート等の公共施設において，スマートフォンやモバイル端末を USB 経由で充電するためのサービス（以下，モバイル充電サービス）が普及している．モバイル充電サービスは一般的に充電用ポートやケーブルを充電サービス装置から提供し，装置の内部はユーザから見えないようになっている．このため，装置内に充電サービス装置以外の PC や USB デバイス等が設置されるような，充電サービスを偽装した脅威が考えられる．ところで 2014 年 8 月の Black Hat USA にて，Nohl らにより BadUSB が発表された [1]．BadUSB は，USB フラッシュメモリのコントローラのファームウェアを書き換え，正常な USB フラッシュメモリになりすました不正な USB デバイスである．このような USB を利用する攻撃対象は PC だけでなく，スマートフォンやタブレットといったモバイル端末も攻撃の対象となりうる．

本論文ではモバイル充電サービスの偽装に関する脅威を

[1] 一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）
Connected Consumer Device Security Council
[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

洗い出すモデルを検討し，iOS 端末を主な対象として具体的な攻撃方法について述べる．最後に，この脅威への対策モデルについて述べる．

2. 関連研究及び脅威モデリング手法

2.1 スマートフォンに対する USB の脅威に関する研究

文献 [2] では，スマートフォンを USB で接続する際の脅威について，スマートフォンから PC，PC からスマートフォン，スマートフォンからスマートフォンへ接続する 3 つの形態に分類し，それぞれの攻撃方法を述べている．スマートフォンから PC への攻撃方法では，マスストレージ機能を利用してマルウェアプログラムを PC へ転送したり，HID 機能を隠匿して利用する攻撃について述べている．PC からスマートフォンへの攻撃方法では，スマートフォンのシステムイメージを書き換える方法について述べている．スマートフォンからスマートフォンへの攻撃方法では，USB OTG（On-the-Go）規格を利用してスマートフォンを USB のホストデバイスとし，PC からスマートフォンへの攻撃方法と同様のことが可能なことを述べている．本論文では，スマートフォンに接続されうる周辺機器やケーブル類を脅威の要因として考察し，これらを組み合わせた攻撃方法を導出するモデルを提案する．

2.2 ゴール指向型脅威分析モデルを起点とした脅威の導出

モバイル充電サービスを安全に利用するという目標を達成するため，同サービスを利用する場合の脅威を分析する．脅威に対する分析手法は主に 3 つのアプローチがある [5]．

- 機器やシステムに対する直接の脅威を想定し，それが引き起こす被害の深刻度を追っていく手法 [6], [7], [8], [9]
- 回避したい深刻な被害を引き起こす脅威を想定して攻撃手段をブレークダウンする手法 [10]
- 攻撃者の視点で脅威を特定する手法 [11]

これらの手法は，1 つの手法に限定せず，複数の手法を組み合わせるとより有用である．例えば，STRIDE による脅威カテゴリ毎の分析と，アタックツリーによるアタックブレークダウン，SREIS 分析を組み合わせながらセキュリティ要求を作るなどである．

2.3 ゴール指向型脅威分析

前節で述べたような脅威分析手法の事例が多数ある中で，セキュアなシステムという目標を達成するための戦略を立て，それを達成するサブゴールを導出する手法がセーフティ＆セキュリティの分野において注目を集めている [5], [12], [13], [15]．これらの手法は，Goal Structuring Notation 手法（以下，GSN）を基に考案されている．GSN を用いると，ある前提から導出した目的（ゴール）を，どのような戦略で達成するかの議論構造を明確化することができる．それだけでなく，システムのディペンダビリティ（品質，信頼性，セキュリティ）の議論や論理構造明確化，その平易な構文表現から，ステークホルダへの説明などにも効果を発揮している [8]．本稿では GSN を用いてモバイル充電サービスの脅威を分析するモデリングを行う．

3. モバイル充電サービスの偽装攻撃による脅威のモデル化

3.1 モバイル充電サービスの基本構成

一般的なモバイル充電サービスは，主に USB のポート提供型とアダプタケーブル提供型がある．それぞれの基本構成図を**図 1** に示す．ポート提供型は，USB Type-A ポートを充電用に提供する形式の充電サービス装置であり，ユーザが所有するアダプタケーブルを用いて充電サービスを利用できる．今般のモバイル端末の充電用インターフェイスは USB を中心に多様化しており，各インターフェイスを USB Type-A プラグに変換するアダプタケーブルを充電用に使用することが一般的である．アダプタケーブル提供型は，モバイル端末向けのアダプタケーブルを充電用に提供する形式の充電サービス装置であり，ユーザは装置から伸びているアダプタケーブルをモバイル端末に接続して充電サービスを利用する．ユーザがアダプタケーブルを用意せずに利用できる利便性がある一方で，各モバイル端末のインターフェイスに互換性のあるアダプタケーブルをサービス側に装備する必要がある．

ここで，モバイル充電サービスが偽装されているケースを考える．同サービスは，図 1 の点線部分のコンポーネントを不正な機器に置き換えることも可能であり，不正な機器が設置されていることをユーザが関知せずに接続する可能性がある．例えば，攻撃者がアダプタケーブル提供型の装置内に USB キーボードを設置し，ユーザのモバイル端末が当該 USB キーボードに接続された場合，USB キーボード経由でモバイル端末の不正操作が行われる可能性がある．USB キーボード以外にも様々な USB デバイスがあり，また，アダプタケーブルの種類によっては USB 以外のデバイスを接続される可能性がある．

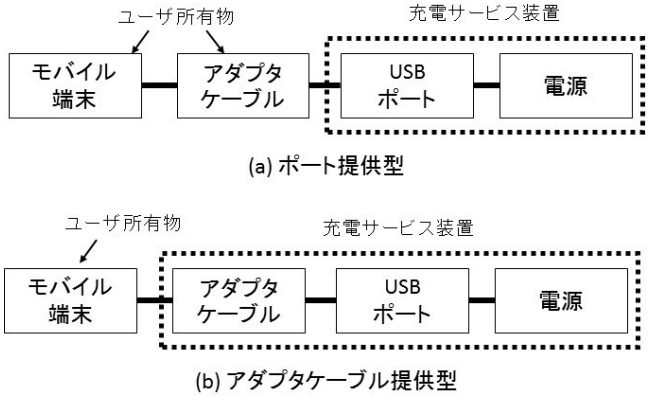

図 1 モバイル充電サービスの基本構成
Fig. 1 General configuration of mobile charging service

モバイル充電サービスを安全に利用するという目標達成ため，モバイル充電サービスが偽装された条件下において悪用される可能性のある機器を洗い出し，モバイル充電サービスの偽装攻撃による脅威をモデル化する．

3.2 GSN によるモバイル充電サービスの脅威分析モデリング

図 1 の構成を基にして，モバイル充電サービスの安全な利用というゴールを達成するため，どこから，どうやって攻撃される可能性があるかという戦略に沿った GSN 利用型脅威分析モデルを構築した．構築したモデルを**図 2** に示す．このモデルは，モバイル充電サービスを偽装した装置内に設置する USB デバイスや，接続するためのアダプタケーブルを精査して脅威の導出に利用できる．図 2 ではまず，充電サービスの安全な利用というゴールを達成するために，前節のモバイル充電サービスの基本構成に着目しながら，USB デバイスとアダプタケーブルを組み合わせた構成を俯瞰し，コンポーネント毎に，どこからどうやって攻撃されるかを明確にするという戦略を立てる．

そして，USB デバイスクラスの情報を収集したという前提のもと，「Audio クラス，HID クラス，Mass Storage クラス，Hub クラスを使った攻撃の脅威を明確にする」というサブゴールと，Lightning USB アダプタケーブルなどの一般的なアダプタケーブルの情報を収集したという前提のもと，「USB アダプタ，HDMI アダプタを用いた攻撃の脅威の明確にする」というサブゴールの両方を達成することで，充電サービスの安全な利用につなげるものである．

次に，図 2 のモデルの流れに沿った USB デバイスとアダプタケーブルによる脅威を導出した結果を述べる．なお，モバイル端末として Android と iOS のスマートフォンが主に普及しているが，周辺機器やアダプタケーブル類が統一されている iOS 系の端末（以下，iOS 端末）を対象とする．

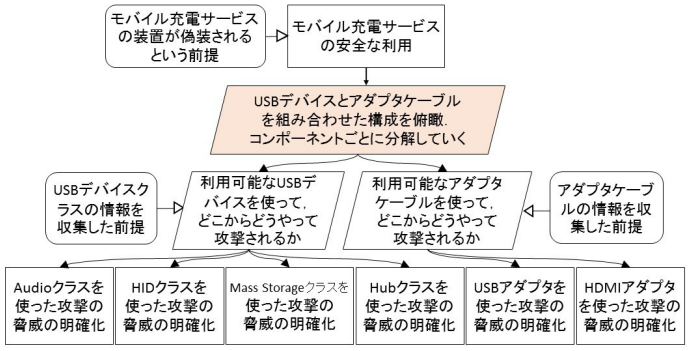

図 2 モバイル充電サービスに対するゴール指向型脅威分析モデリング

Fig. 2 Goal-oriented threat modeling for mobile charging service

3.3 周辺機器となる USB デバイスによる脅威

前述のモデルに従い，iOS 端末で一般的に利用できる USB デバイスなどの周辺機器による脅威について導出した結果を**表 1** に示す．図 2 のモデルではまず，iOS 端末で利用可能な USB デバイスクラスの情報を収集し，計 4 つのサブゴールに分解した．表 1 では，そのサブゴールに沿い，USB の仕様にもマッピングされている．USB の仕様では各デバイスの用途ごとに分類されたデバイスクラスが定義されており，より一般的なデバイスクラスにはその動作に必要な標準デバイスドライバが用意されている．標準デバイスドライバの仕様に合わせて開発されたデバイスはプラグアンドプレイで利用できるため，ユーザが関知せずに接続され，不正に利用される可能性を示している．

3.4 Lightning アダプタケーブルによる脅威

iOS 端末は有線の外部入出力用インターフェイスとして USB ポートではなく，Lightning ポートを備えている．最も一般的である Lightning USB アダプタケーブルは，iOS 端末のバッテリー充電や PC とのデータ通信のために利用される．また，Apple は iOS 端末用に Lightning ポートを USB Type-A ポートや HDMI，VGA ポートに変換するアダプタケーブルを販売している．そこで，これらについても図 2 のモデルに従い，一般的な Lightning アダプタケーブルの情報を収集し，サブゴールに分解した．そのサブゴールに沿い，iOS 端末で利用できる代表的なアダプタ

表 1 iOS 端末で標準利用可能な USB デバイスによる脅威
Table 1 Threats against general USB devices

Class ID	Class Name	Description and Threat
01h	Audio	Audio クラスは，イヤホンやマイクが該当する．音声の入出力による音声制御アシスタントの不正操作や音声ナビゲーションの盗聴の恐れがある．
03h	HID	Human Interface Devices (HID) クラスは，キーボードやマウスが該当する．近年のモバイル端末はマウスには対応せず，キーボードのみ互換性がある端末が一般的である．キーボードやそのショートカット機能を悪用した不正操作の可能性がある．
08h	Mass Storage	マスストレージクラスは，USB フラッシュメモリや外付け HDD が該当する．近年のモバイル端末では写真や動画データ等の読み取りのみ対応している．攻撃用データの読み取り元として利用される可能性がある．
09h	Hub	ハブクラスは，USB デバイスを複数接続する USB ハブが該当する．前述のデバイスクラスのデバイスを組み合わせた攻撃に利用される可能性がある．

ケーブルとその脅威を導出した結果を表 **2** に示す．この導出結果より，アダプタケーブル提供型のモバイル充電サービスでは，アダプタケーブル部分を任意のアダプタケーブルに置き換えた偽装攻撃の可能性があることを示している．

以上，脅威分析モデルから具体的な脅威を導出し，モバイル充電サービスの安全な利用へつなげることができる点について述べた．次章では，これらの周辺機器を利用した，iOS 端末向けのモバイル充電サービスにおける具体的な攻撃手法について検証する．

4. モバイル充電サービスの偽装による脅威の検証

前章の GSN モデル，及び，分析結果を元に，標準デバイスクラスの USB デバイスと Lightning アダプタケーブルを組み合わせた iOS 端末へのモバイル充電サービス偽装攻撃を提案する．まず，偽装攻撃のイメージを図 **3** に示す．本攻撃手法は，アダプタケーブル提供型のモバイル充電サービスを偽装し，アダプタケーブルの根本から先はユーザに見えない状況を想定している．

4.1 外部ディスプレイに出力されるパスワードの覗き見

Lightning デジタル AV アダプタケーブルを利用すると，iOS 端末の操作画面を外部ディスプレイにミラーリング出力できる．一般的には写真データをテレビに映して鑑賞したり，プレゼンテーションでスライドを表示する際に利用される．同ケーブルを接続すると，接続後約 10 秒間だけ画面上部のステータスバーが青色に変化するが，ダイアログやアイコン表示のような警告はないためユーザは自主的に接続した場合を除いてミラーリング出力されていることに気づかない可能性が高い．

図 **4** は，Lightning デジタル AV アダプタケーブルと外部ディスプレイを利用した iOS 端末への攻撃の構成例である．ユーザがミラーリング出力に気づかずに画面を操作した場合，外部ディスプレイに映し出された個人情報を盗み取られる恐れがある．さらに，このミラーリング出力では，スクリーンロック解除用のパスコード入力操作がそのまま

表 **2** iOS 関連アダプタケーブルによる脅威
Table 2 Threat against general iOS adapter cables

Name	Description and Threat
Lightning USB Cable	Lightning ポートを USB Type-A プラグ（オス）に変換する． PC とのデータの同期やバッテリーの充電を行うことができる．不正にデータを同期することで iOS 端末内のデータを盗み取られる可能性があるが，データの同期には iOS 端末上で PC との接続を許可する必要がある．
Lightning USB3 Camera Adapter	Lightning ポートを HDMI ポートと充電用 Lightning ポートに変換する．デジタルカメラを USB 経由で接続し，iOS 端末への写真や動画を取り込み可能にする．充電用の Lightning ポートを利用して，充電と並行してデジタルカメラからデータを取り込むことができる．デジタルカメラ以外にも表 1 のデバイスを使用可能であり，脅威につながる可能性がある．
Lightning Digital AV Adapter	Lightning ポートを USB Type-A（オス）と充電用 Lightning ポートに変換する．同ケーブルを利用すると，HDMI 経由で操作画面を外部ディスプレイに出力できる．パスワードの入力や各種操作がそのまま映し出されるため，機密情報が漏えいする可能性がある．

図 **3** モバイル充電サービスの偽装攻撃のイメージ
Fig. 3 A sample image of spoofing attack of mobile charging service

図 **4** ミラーリングされたパスワード入力画面の覗き見
(左図は 7 が入力された時，
右図は w が入力された時のスクリーンショット)
Fig. 4 Peeping passwords via a mirrored display
(The image on the left shows a “7” being entered and the one on the right shows a “w” being entered.)

出力される．また，iOS 端末では各サービスへのログイン時にパスワードの入力内容が 1 文字ずつ表示される．攻撃者はパスコードやパスワードの入力操作を覗き見ることができるため，不正アクセスにつながる可能性がある．

4.2 外部キーボードを利用した不正操作

Lightning USB 3 カメラアダプタケーブルは，Lightning ポートを USB ポートと充電用 Lightning ポートに分岐・変換するアダプタケーブルであり，このケーブルを利用すると iOS と互換性のある USB デバイスを利用可能となる．**図 5** は，Lightning USB 3 カメラアダプタケーブルと USB キーボードを利用した iOS 端末への攻撃の構成例である．この構成例で攻撃者は任意の Web ページを開くことが可能である．この方法でフィッシングサイトへ誘導したり，tel URI スキームを利用して任意の電話番号へ電話をかけるといった不正行為が行われる恐れがある[*1]．

4.3 VoiceOver 有効時における外部キーボードとヘッドセットを利用した不正操作

iOS の音声ナビゲーション機能 VoiceOver が有効な場合，より多様なキーボード操作が可能となる．VoiceOver は，スクリーン上の項目を読み上げる，視覚障害者向けのスクリーンリーダー機能である．VoiceOver が有効な端末では，画面上の項目の選択とタップ操作をキーボード操作で行えるため，ユーザがスクリーンを見て操作することと同様なことがキーボード操作で可能となる．また，VoiceOver のスクリーンカーテン機能を使うと画面全体を強制的に非表示にできるため，操作画面を隠したまま不正操作が可能となる．

図 6 は，Lightning USB 3 カメラアダプタケーブルと USB ハブ，キーボード，ヘッドセットを利用した攻撃の構成例である．Lightning USB 3 カメラアダプタケーブル経由でキーボードとヘッドセットを接続した場合，攻撃者は iOS 端末の操作画面を見ずに，画面上項目の読み上げ音声を元にキーボード操作を行い，Bluetooth デバイスへの接続や端末内のデータを添付したメールの送信等，任意の操作を行うことができる．WebAIM[16] によるスクリーンリーダーの利用者調査によると，VoiceOver はモバイル端末におけるスクリーンリーダーとして最も利用されている製品であり，この攻撃の脅威の影響を受ける利用者は少なくない．

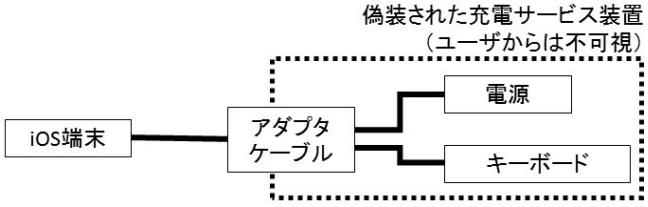

図 5 外部 USB キーボードを利用した不正操作
Fig. 5 Overview of illegal operation with external keyboard

[*1] 攻撃のためのキーボード操作手順の例を付録に記載する

5. 考察

5.1 脅威分析モデルの評価

今回提案した脅威分析モデルは，GSN を用いたゴール指向型分析モデルを用いることで，具体的な脅威を導くことができただけでなく，セキュリティ検証のプロセスを構造化および可視化できるモデルにできた．構造化と可視化という点では，セキュリティ分析における FTA 分析やアタックツリー分析などを用いることもあるが，これらの分析手法では上位ユニットから下位ユニットへの分解の根拠，考え方まで表現することができない．その点 GSN では，ゴール，戦略の前提情報，根拠といった情報も同時に表現でき，脅威分析の根拠を明確にし，さらに見直しをかけて継続改善することが容易となる．

モバイル充電サービスに適用した場合にも USB デバイスやアダプタケーブル情報を収集したという過程を前提情報および根拠として盛り込み，Audio クラスや HID クラスなどの周辺機器を使った攻撃の脅威の明確化の根拠としている．将来的には，前提となる情報と根拠を更新しながら，IoT 機器や車載器ネットワークなどに適用できるモデルに成長させることにもつなげられる．

5.2 モバイル充電サービス偽装攻撃の対策

4 章で検証した脅威の要因として，本来の目的である充電サービス装置以外の不正なデバイスを意図せず接続される可能性があることが挙げられる．このような脅威から守るための対策モデルを検討した．このモデルを**図 7** に示す．モバイル端末と充電サービス装置との間に，接続された USB デバイスの性質を確認するシステムを中継させ

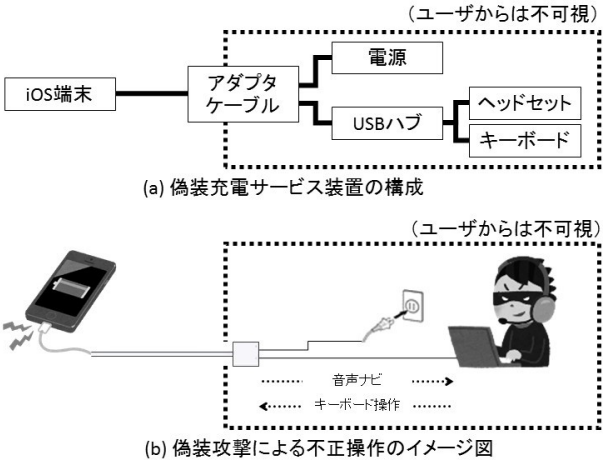

図 6 外部 USB キーボードとヘッドセットを利用した不正操作
Fig. 6 Overview of illegal operation with external keyboard and headset

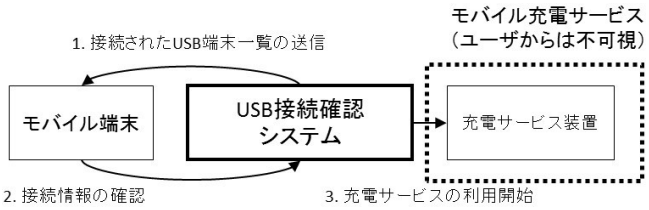

図 7 接続された USB デバイスの確認による対策モデル
Fig. 7 USB device connection confirming model

る．このシステムでは，まず，接続された USB デバイス情報を通知するソフトウェアまたはハードウェアを中継させ，ユーザにデバイス情報の確認を要求する．次にユーザが接続を許可した場合に USB による充電またはデバイスの使用を開始する．ユーザが接続を許可しなかった場合には，充電用の配線のみを接続し，充電機能だけを提供する．BadUSB のようにデバイス構成を動的に変更する攻撃の可能性もあるため，USB デバイスの構成が変更された場合には確認状態に戻し，ユーザに再度確認を要求する．この対策モデルは充電サービス装置外部機器を一旦隔離し，検疫後に端末への接続を許可することで安全性を確保している．

6. おわりに

モバイル充電サービスの偽装攻撃について脅威分析モデルを導出し，具体的な攻撃手法と対策モデルを考察した．脅威分析モデルでは，GSN を用いたゴール指向型分析モデルを用いることで，具体的な脅威を導くことができただけでなく，セキュリティ検証のプロセスを構造化および可視化できるモデルにできた．そして，モバイル充電サービスの偽装攻撃によって，iOS 端末のパスワード入力画面が覗き見されたり，不正操作される恐れがあることを検証した．今後は，提案した攻撃の対策モデルの実現方法について検討を進める予定である．

参考文献

[1] Nohl, K. and Lell, J.: BadUSB - on accessories that turn evil, *Black Hat USA* (2014).
[2] Wang, Z. and Stavrou, A.: Exploiting smart-phone usb connectivity for fun and prot, *In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC)*, pp.357–366 (2010).
[3] Tian, D. Bates, A. and Butler, K.: Defending Against Malicious USB Firmware with GoodUSB, *In Annual Computer Security Applications Conference (ACSAC)*, pp.261–270 (2015).
[4] Kelly, T. and Weaver, R.: The goal structuring notation - a safety argument notation, *In Proceedings of the dependable systems and networks 2004 workshop on assurance cases*, (2004).
[5] 独立行政法人情報処理推進機構 (IPA)：つながる世界のセーフティ＆セキュリティ設計入門，SEC BOOKS，pp.53–57 (2015).
[6] Riccardo, S. Wuyts, K. and Joosen, W.: A descriptive study of Microsoft's threat modeling technique, *Requirements Engineering*, Vol.20, No.2, pp.163–180 (2015).
[7] Frank, S. and Snyder,W.: Threat modeling, *Microsoft Press* (2004).
[8] Myagmar, S. Lee, A. J. and Yurcik, W.: Threat modeling as a basis for security requirements, *In Symposium on requirements engineering for information security (SREIS)*, Vol.2005, pp.1–8 (2005).
[9] The MITRE Corporation: Common Attack Pattern Enumeration and Classification, available from ⟨https://capec.mitre.org/⟩, (accessed 2016-07-13).
[10] Saini, V. Duan, Q. and Paruchuri, V.: Threat modeling using attack trees, *Journal of Computing Sciences in Colleges*, Vol.23, No.4, pp.124–131 (2008).
[11] Sindre, G. and Opdahl, A. L.: Eliciting security requirements with misuse cases, *Requirements engineering*, Vol.10, No.1, pp.34–44 (2005).
[12] Kelly, T. and Weaver, R.: The goal structuring notation - a safety argument notation, *In Proceedings of the dependable systems and networks 2004 workshop on assurance cases* (2004).
[13] Kobayashi, N. and Yamamoto, S.: The Effectiveness of D-Case Application Knowledge on a Safety Process, *Procedia Computer Science*, Vol.60, pp.908–917 (2015).
[14] Yamamoto, S. and Matsuno, Y.: An evaluation of argument patterns to reduce pitfalls of applying assurance case, *In Assurance Cases for Software-Intensive Systems (ASSURE) 2013 1st International Workshop on IEEE*, pp.12–17 (2013).
[15] Yamamoto, S.: Assuring Security through Attribute GSN, *In IT Convergence and Security (ICITCS), 2015 5th International Conference on IEEE*, pp.1–5 (2015).
[16] WebAIM.: Screen Reader User Survey #6 Results (online), available from ⟨http://webaim.org/projects/screenreadersurvey6/⟩ (accessed 2016-07-13).
[17] Apple Inc.: iPhone User Guide For iOS 8.4 Software (online), available from ⟨https://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf⟩ (accessed 2016-07-13).

付　　録

A.1 USB キーボードを使用した任意の電話番号への発信操作

USB キーボードを使用して iOS 端末で任意の電話番号へ発信する手順の具体例を記載する．この例は，0123456789 という番号に発信する例である．

(1) Command+Space キーを押し，Spotlight 検索を呼び出す．
(2) 適当な文字列（例：aiueoaiueo）をタイプし，Web 検索の項目を最優先候補にする．
(3) 下矢印キーを押し，Web 検索を選択後，Enter キーを押す．すると，標準 Web ブラウザで手順 2 のキーワード検索される．
(4) Command+L キーを押し，アドレスバーに tel:0123456789 を入力する．iPhone の場合電話発信確認のダイアログが表示される．
(5) Enter キーを押し，ダイアログの” 発信” ボタンを選択すると，電話が発信される．