Computer Security Symposium 2017
23 - 25 October 2017

スマートハウス向け情報機器のリスクアセスメントにおける資産導出手法

城間 政司[†1]　井上 博之[†1†2]

概要：セキュリティのリスクを分析する手法として様々なリスクアセスメント手法が提案されている．守るべき資産を起点とするリスクアセスメント手法では資産の洗い出しを始めに行うが，分析者の知見に依存するという問題がある．これに対し，資産導出のサポートとして資産の分類を定義する事例あるが，分類と照らし合わせるドキュメント類が必要であり，ドキュメントを入手できないケースへの適用が難しい．本稿では，スマートハウスにおける情報機器のリスクアセスメントにおいて，機器同士がつながるという特徴に着目し，つながる機器と経路を起点に資産を導出する手法を提案する．また，提案手法のケーススタディとしてスマートハウスを構成する情報機器に対する資産導出を行う．

キーワード：リスクアセスメント，資産導出，スマートハウス，IoT

Asset Derivation Method for Risk Assessment of Information Devices in Smart House

Tadashi Shiroma[†1]　Hiroyuki Inoue[†1†2]

Abstract: Different types of assessment frameworks exist for security risk analysis. These frameworks begin identifying the assets that should be protected. However, the effectiveness of the identification process depends on analysts' security knowledge and experience of the assessment. To mitigate the problem, we can use asset guidewords on security risk assessment guidelines. It also has a problem in that we cannot identify the assets without accessing the documents of the analysis target. In this paper, we propose an asset derivation method focusing on device connectivity in smart houses. The method derives assets from device connectivity and paths to information and function of devices. We also evaluate the method by conducting a case study to assess a smart house with it.

Keywords: Risk Assessment, Asset derivation, Smart house, Internet of Things

1. はじめに

コンピュータの小型化や関連技術の向上から，あらゆるものがインターネットにつながる Internet of Things の世界が実現されつつある．この流れは一般家庭内にも普及しており，生活家電や監視機器をネットワークにつなげることで外出先から操作したり，防犯対策として利用したりする等，利便性や安全性を向上させている．しかし，これらの機器は不正アクセスを受け，所有者に危害を加えたり，他所への攻撃の踏み台として悪用される可能性がある．このような機器をつなげることでどのようなリスクがあるかを確認するためには，セキュリティ上のリスクアセスメント（以降，リスクアセスメントと呼ぶ）が有効である．

リスクアセスメントの手法は多数提案されており，守るべき資産を基にリスクアセスメントを行う手法が一般的である[1]．守るべき資産（以降，保護資産と呼ぶ）を基にするリスクアセスメント手法の主な流れは，保護資産の導出，保護資産に対する脅威の分析，脅威のリスク評価，対策の実施となっている．ここでの保護資産は，リスクアセスメント対象の所有者や組織にとって何が重要なのかという考え方を基に，仕様書や設計書等のドキュメントと照らし合わせて導き出していく．組織における保護資産の導出では，管理担当者へのインタビュー等から導き出す場合もある．しかしながら，リスクアセスメントにおける効果的な保護資産を何が重要なのかという考えだけで導き出すことはセキュリティの知識や経験がないと難しいという課題がある[2]．この課題に対して，リスクアセスメントのガイドラインでは，重要な保護資産の分類をあらかじめガイドワードとして定義し，ドキュメントと照らし合わせることでリスクアセスメントに効果的な保護資産を導出する手順が提示されている[3][4]．ただし，このガイドワードによる保護資産の導出では，ガイドワードと照らし合わせるドキュメントが要求されることや，ドキュメントに記載されていない保護資産を導出することが難しいという課題がある．

本稿では，ドキュメントに依存する従来手法とは別のアプローチとして，スマートハウスの情報機器に対するリスクアセスメントにおける保護資産導出手法を提案する．本手法は，情報機器のつながりに着目し，情報機器のインタ

†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)
†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

ーフェイスからどのような情報や機能にアクセスできるかによって保護資産を導出していく手法であり，ドキュメントがないケースにも適用可能である．

本稿の構成は以下の通りである．第 2 章では，関連する研究やリスクアセスメント手法について述べる．第 3 章では，提案手法について述べる．第 4 章では，提案手法を用いて保護資産の導出を行ったケーススタディについて述べる．最後に，第 5 章で本稿をまとめる．

2. 既存の保護資産導出手順とモデリング手法

2.1 保護資産を起点とするリスクアセスメント手法とガイドワードを用いる保護資産の導出

保護資産を起点とするリスクアセスメントは図 1 のような流れとなっており，導出した保護資産から脅威やその対策を検討する．また，保護資産の一般的な導出手順は図 2 に示す通りであり，仕様書や設計書等のドキュメントと保護資産のガイドワードを照らし合わせる形で保護資産を導出する．

ガイドワードは，分析対象の分野に合わせたものが各種セキュリティガイドラインのリスクアセスメント手法で提示されている．例えば，文献[4]では，IoT 機器向けのガイドワードが提示されており，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，例えば，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，その過程で保護資産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 つの分類を挙げている[5]．各分類はそれぞれ，デバイスはバッテリーや 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．文献[6]では，スマートハウスにおける脅威がまとめられており，その脅威の影響を受ける保護資産についても紹介されている．文献[6]で紹介されている保護資産は，スマートハウスにおける情報やネットワーク，ソフトウェア，センサ類等の情報機器に関するものから人間まで多岐に渡っている．

このように各分析対象に対応する様々なガイドワードが提示されており，保護資産を導出する上で重要なヒントとなる．ただし，ガイドワードは保護資産を完全に網羅しているわけではないため，ガイドワードでカバーされない保護資産導出の課題がある．また，保護資産の導出に用いるドキュメントが公開されていないケースや，エンドユーザレベルのリスクアセスメントや第三者機関によるセキュリティ検証業務等，詳細なドキュメントが入手できないケースへの適用は難しい．

2.2 データフロー図を用いた脅威モデリング

保護資産を起点としたリスクアセスメントとは異なる手法として，データフロー図（Data Flow Diagram，以降，DFD と呼ぶ）を記載し，DFD を基に脅威をモデル化，分析していく手法がある（以降，DFD 脅威モデリング手法と呼ぶ）[2]．DFD 脅威モデリング手法では，システムとそのデータのやりとりを DFD で表現し，データの入出力ポイントである各エントリポイントに対して STRIDE[7]という一般的な脅威の分類と照らし合わせて脅威をモデル化していく手順を示している．この手法の特徴として，DFD でモデル化することで分析対象のシステム構成が可視化されることや，エントリポイントに着目して脅威を想定することにより，工数を減らしつつ効果的に分析できる利点がある．一方，DFD を作成する際には仕様書や設計書等のドキュメントから作成していくため，ガイドワードによる手法と同様にドキュメントが入手できないケースへの適用は難しい．

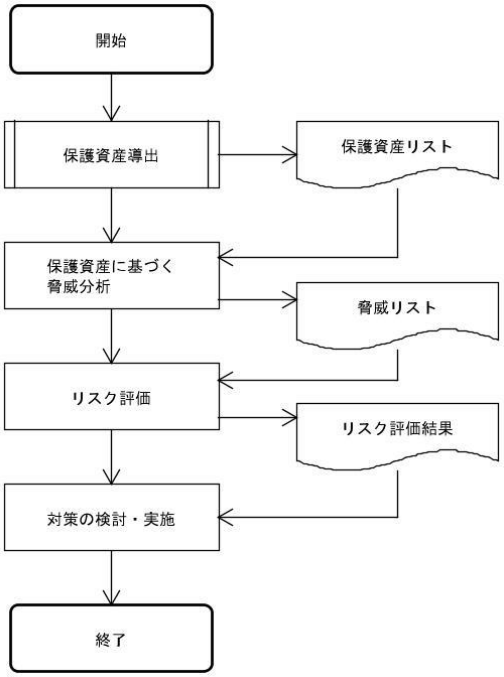

図 1 保護資産を起点としたリスクアセスメントの流れ
Figure 1 Flow of asset driven risk assessment.

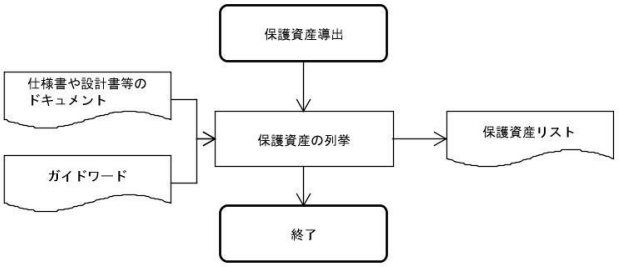

図 2 ガイドワードによる保護資産の導出の流れ
Figure 2 Flow of asset derivation using guide words.

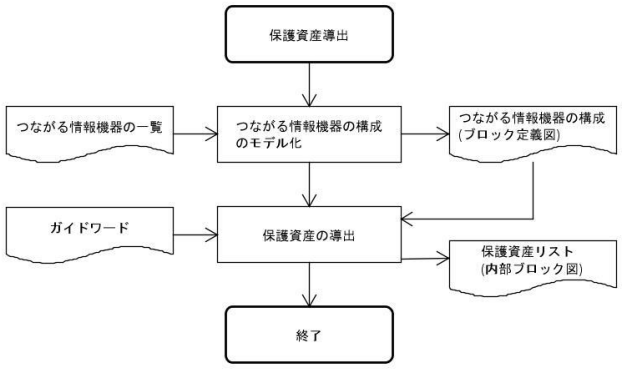

図 3 提案手法による保護資産の導出の流れ
Figure 3 Flow of asset derivation using proposal method.

このように，ドキュメントを基にした保護資産の列挙やシステムのモデル化では，対象のドキュメントを入手できないケースへの適用が難しいことや，ドキュメントでカバーされない保護資産の導出ができないため，ドキュメントに依存しない別のアプローチを検討する必要がある．

3. スマートハウスにおける情報機器の保護資産導出手法

3.1 スマートハウスにおける情報機器の特徴

スマートハウスにおける情報機器は，各家庭によって様々であるが，一般的にエアコンやテレビ等の家電，スマートフォンやデスクトップ PC, ホームゲートウェイルータ, 各種センサ機器類等がある．各情報機器は機器の制御やデータの送受信のためのインターフェイスを備えており，Wi-Fi や有線 LAN で接続するものや，Bluetooth，USB，赤外線通信といったインターフェイスを介して通信を行う．各インターフェイスは Bluetooth のように相互に認証を行うものもあるが，一度接続された機器は信頼できるものとして通信でき，ある機器が不正に操作されることで他の機器にも影響を与える可能性がある．

提案手法では，各機器同士がつながる特徴に着目し，各情報機器のインターフェイスからどのような保護資産にアクセスできるかというアプローチの手法を提案する．本手法は，情報機器に関する詳細なドキュメントを入手できないようなケースにも適用可能であり，また，従来手法による保護資産導出の網羅性を補うためにも利用可能である．

3.2 情報機器のインターフェイスからの保護資産導出

提案手法による保護資産導出の流れを図 3 に示す．本手法の手順は大きく 2 つに分けられる．まず，分析対象のスマートハウスにおける情報機器の構成をモデル化する．次に，作成したモデルを基に情報機器のインターフェイスからアクセス可能な保護資産を列挙し，情報機器が持つ保護資産とその関係をモデル化する．このとき，どのような機能や情報が保護資産かの判別を補助する目的で，既存の研究やガイドラインの保護資産のガイドワードを利用する．また, 導出結果は SysML[8]のブロック定義図と内部ブロック図で表現する．これにより，全体の構成や保護資産の関係を可視化することができ，保護資産導出の次のステップである脅威分析やリスク評価に活用することができる．SysML をモデリング記法として用いる理由は，ブロック定義図により情報機器とそのインターフェイスの構成を表現でき，内部ブロック図で情報機器の内部の情報や機能を表現可能という特徴のためである．ただし，本手法は SysML に限定するわけではなく, 状況に応じて DFD やスプレッドシート，その他の表現手法を用いてもよい．

3.2.1 手順 1：つながる情報機器の構成のモデル化

まず，スマートハウスを構成する情報機器を列挙し，その構成図を作成する．情報機器の例として，エアコンやテレビ等の情報家電，ホームゲートウェイルータ，各種センサ機器類がある．このとき，各情報機器へのデータの入出力であるインターフェイスについても列挙する．インターフェイスの一例を表 1 に示す. ポートによる分類は USB や Bluetooth，有線 LAN ポートや Wi-Fi 等の Ethernet 通信を行うポート，赤外線通信ポート等の物理的なインターフェイスを示し, プロトコルによる分類は USB の標準デバイスクラスや Bluetooth の HID 等の通信プロトコルを示す．これ

表 1 主なインターフェイスとその分類の例
Table 1 Example of major interfaces and their classifications.

ポート	プロトコル	デバイス・用途例
USB	Audio	マイク，スピーカー，ヘッドセット
	CDC	イーサネットカード
	HID	キーボード，マウス
	Image	PTP/MTP（スマートフォンやタブレット PC 等の動画像データ転送）
	Printer	プリンタ
	Mass Storage	USB フラッシュドライブ
	Video	Web カメラ
Bluetooth	A2DP	音声データストリーミング
	AVRCP	音楽再生制御
	BIP	画像データ送受信
	HIDP	キーボード，マウス
	HSP	マイク，スピーカー，ヘッドセット
Ethernet	HTTP	Web 管理画面
	Telnet	コンソール管理画面
	UPnP	ルータ設定
	SMB	ファイル共有
その他	赤外線通信	電源のオン・オフ，家電の制御
	温度センサ	温度の取得
	湿度センサ	湿度の取得
	人感センサ	動体の検知
	タッチパネル	情報機器の制御
	物理ボタン	電源のオン・オフ，家電の制御

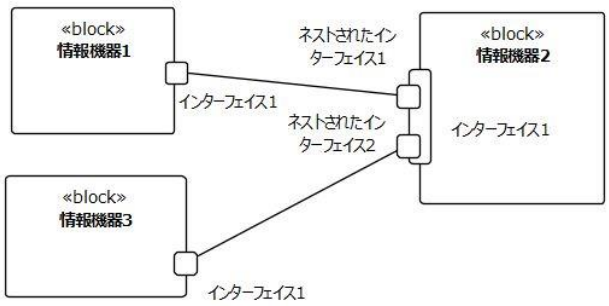

図 4 ブロック定義図の例

Figure 4 Example of block definition diagram.

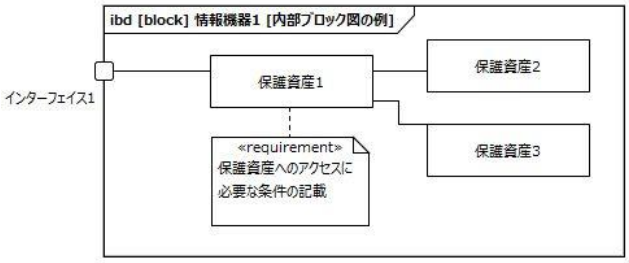

図 5 内部ブロック図の例

Figure 5 Example of internal block diagram.

らの分類をより細分化することで，保護資産導出を具体的かつ網羅的に分析可能である．また，各インターフェイスに対応するプロトコルのスキャナを用いることで作業を自動化することが可能である．

これらの列挙した結果は SysML のブロック定義図で機器の構成を記述する．提案手法に合わせたブロック定義図の作成手順は以下の通りである．

手順 1-1：各情報機器をブロックとして記載する．

手順 1-2：情報機器のインターフェイスをブロック定義図のポートとして記載する．インターフェイスを細分化できる場合には，ネストされたポートとして記載し，構造がわかるようにする．

手順 1-3：各情報機器のつながるインターフェイスをコネクタ線で結ぶ．

上記の手順で作成するブロック定義図の例を図 4 に示す．各ブロックは情報機器を表し，情報機器が持つインターフェイスをブロック定義図のポートで表現している．各ポートには表 1 のポートとプロトコルの関係のようにネストしたポート情報を記載し，USB であればデバイスクラス，Bluetooth であればプロファイル，Wi-Fi や有線 LAN 等であれば HTTP や Telnet 等のアプリケーションレベルまで分類して記載する．以上の手順により，情報機器の構成とそのつながり方をブロック定義図で表現する．

3.2.2 手順 2：インターフェイスからの保護資産の導出

手順 1 で導出した情報機器とインターフェイスを基に，インターフェイスからアクセス可能な保護資産を導出していく．このとき，実際にインターフェイスにつながる情報機器や周辺機器を用いてハンズオン形式で行うことで導出の誤りを軽減することができる．例えば，USB の HID デバイスクラスに対応している情報機器に対しては，キーボードを接続し，キーボードの操作によりどのような情報や機能にアクセスできるかを分析する．Ethernet に対してはスマートフォンや PC 等を接続して同様に分析する．どのような情報や機能が保護資産に当たるかどうかは，保護資産の分類を示すガイドワードを参照する．これにより，リスクアセスメントの経験や知識があまりない分析者でも保護資産を識別でき，分析を効果的に行うことができる．

この手順で行った作業結果は SysML の内部ブロック図で記述する．本記法では，SysML 記法の各要素を次のように定義する．

- ブロック：分析対象の保護資産．
- ポート：分析対象の情報機器の操作やデータの入出力に必要なインターフェイス．
- コネクタ：各保護資産の関係を表す線．
- ノート：保護資産へのアクセスに必要な条件．ノートのラベルに Requirement というステレオタイプ表記を用いる．

本稿ではこれらの要素を用いて内部ブロック図を記載する．提案手法に合わせた内部ブロック図の作成手順は以下の通りである．

手順 2-1：各インターフェイスを記載する．USB や Bluetooth のようにインターフェイスを細分化できる場合には，ネストされたポートとして記載する．

手順 2-2：つながる情報機器からアクセス可能な保護資産をブロックとして記載する．このとき，パスワードや機器設定等が必要な場合にはアクセスの条件として Requirement ノートを記載する．

手順 2-3：手順 2 で導出した保護資産からアクセス可能な保護資産の導出を繰り返す．このとき，導出された保護資産同士をコネクタで結ぶ．

上記の手順で作成する内部ブロック図の例を図 5 に示す．情報機器のインターフェイスをポートとして記載しており，このポートからアクセス可能な保護資産 1 をブロックとして記載し，そこからさらにアクセスできる保護資産をブロックとして記載している．このとき，保護資産 1 へのアクセスに必要な条件を Requirement ノートとして条件と共に記載している．以上の手順により，内部ブロック図を作成し，保護資産およびその関係を表現する．

作成したブロック定義図や内部ブロック図は，各インターフェイスから保護資産への侵入手順と捉えることもでき，2.2 節で述べた DFD 脅威モデリング手法においても利用可能である．

4. ケーススタディ

提案手法のケーススタディを行い，本手法の特徴や課題について議論するため，スマートハウスを構成する情報機器の実機に対する分析結果について述べる．なお，今回対象とする情報機器は一部の機器のみ分析を行っている．

本ケーススタディで用いた環境を次に示す．

- モデリングツール：
  Enterprise Architect System Engineering Edition 13*1
- インターフェイススキャナ：
  - ネットワーク：Zenmap 7.01*2
  - USB：umap 1.01+FaceDancer21*3
  - Bluetooth：blucat (Revision 572dfc8)*4
- 情報機器
  - ホームゲートウェイルータ：
    Buffalo Air Station WXR-2533DHP
  - タブレット PC：Apple iPad Air 2 32GB モデル

上記の情報機器の USB や Wi-Fi 等のインターフェイスに PC を接続し，次の内容の導出作業を行った．

4.1 情報機器とインターフェイスの列挙

まず，情報機器とそのインターフェイスを列挙し，それらの構成図であるブロック定義図を作成した．作成したブロック定義図を図 7 に示す. ホームゲートウェイルータは，Ethernet 通信のための有線 LAN ポートや Wi-Fi のインターフェイスと，LAN 内のファイル共有のための USB インターフェイス，その他の物理ボタンを備えている．また，タブレット PC は，同様に Wi-Fi インターフェイスと，USB と同様の通信を行う Lightning インターフェイス，また，周辺機器との通信のための Bluetooth インターフェイス, 電源や音量制御等の物理ボタンを備える．ホームゲートウェイルータとタブレット PC は Wi-Fi インターフェイスでつながるため，両機器を示すブロックをコネクタで結んだ．

4.2 情報機器内の保護資産の導出

次に，各情報機器のインターフェイスからアクセス可能な保護資産を導出していく．今回はホームゲートウェイルータに対して導出作業を行った．また，ガイドワードには 2.1 節で述べた文献[4]のガイドワードを使用した．

ホームゲートウェイルータは, 有線 LAN や Wi-Fi インターフェイスの HTTP ポートから Web 管理画面にアクセスできる. この Web 管理画面に管理者アカウントでログインすると，ホームゲートウェイルータの各種設定参照や変更を行うことができる. また，有線 LAN と Wi-Fi インターフェイスの UPnP ポート経由で UPnP による制御機能にアクセスできる．UPnP はホームゲートウェイルータのネットワークに関する情報やポートマッピングの設定変更等を管理者権限なしに実行することができる．

上記に関する内容を分析し，作成した内部ブロック図を図 6 に示す．保護資産の導出において，前述の機能以外にも，管理パスワードや Wi-Fi の SSID，暗号キー，ファームウェア更新機能，WAN 側 IP アドレス情報等，様々な保護資産を導出した．ただし，AOSS 機能のようなベンダ独自機能の詳細を知るためにはドキュメントを参照する必要があり，従来手法と同様にドキュメントが必要であるという課題が見られた．また，UPnP では SOAP メッセージの送受信が必要であり，このような保護資産を分析するためには分析者の一定のスキルが要求される．

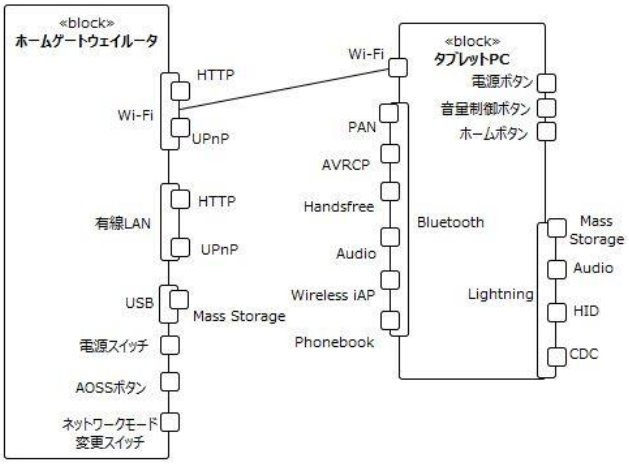

図 7 ケーススタディにおけるブロック定義図
Figure 6 Block definition diagram on the case study.

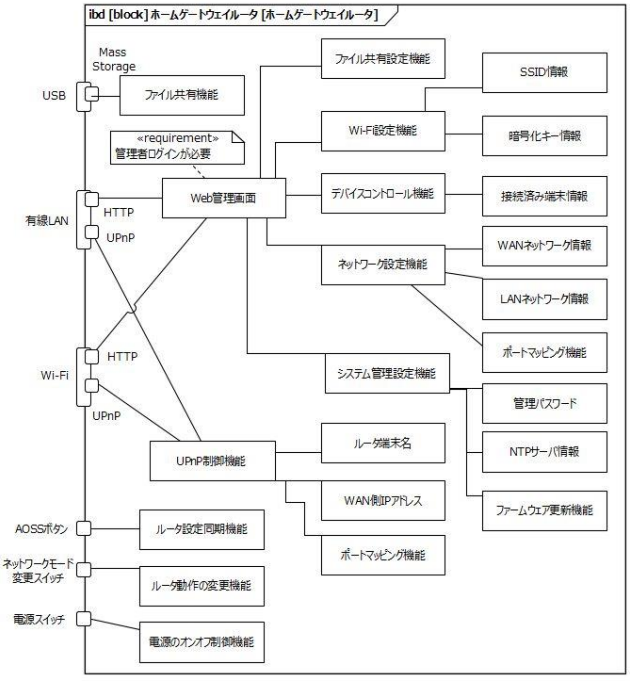

図 6 ホームゲートウェイルータの内部ブロック図
Figure 7 Internal block diagram of home gateway router.

*1 HTTP://www.sparxsystems.com/products/ea/
*2 HTTPs://nmap.org/zenmap/
*3 HTTPs://github.com/nccgroup/umap
*4 HTTP://blucat.sourceforge.net/blucat/

5. おわりに

本論文では，スマートハウスの情報機器に対するリスクアセスメントにおける保護資産導出手法を提案した．本手法は仕様書や設計書等のドキュメントと保護資産のガイドワードを照らし合わせる従来手法とは別のアプローチとして，スマートハウスの情報機器がつながることに着目し，情報機器のインターフェイスからどのような保護資産にアクセスできるかを分析する手法となっている．本稿では導出結果を SysML のブロック定義図と内部ブロック図で表記する手順についても説明した．これにより，リスクアセスメントの脅威分析やリスク評価に利用しやすい形で導出結果を可視化することができる．また，提案手法のケーススタディとしてスマートハウスを構成する一部の情報機器の実機に対して提案手法を適用した．本ケーススタディの結果，一般的な保護資産が導出できることや，ベンダ独自機能のようなドキュメントが必要な保護資産があることがわかった．今後の課題として，スマートハウスを構成する情報機器全体の分析や，提案手法を取り入れたリスクアセスメントの一連の手順化が挙げられる．

参考文献

[1] Shamala, P. and Ahmad, R.: A Proposed Taxonomy of Assets for Information Security Risk Assessment (ISRA) Palaniappan, Proc. *2014 4th World Congress on Information and Communication Technologies*, pp.29-33 (2014).

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

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

[4] 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).

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

[6] ENISA: Threat Landscape and Good Practice Guide for Smart Home and Converged Media, ENISA, ISBN 978-92-9204-096-3 (2014).

[7] Swiderski, F. and Window, S.: Threat modeling, Microsoft Press, ISBN 978-0735619913 (2004).

[8] Object Management Group, Inc.: OMG Systems Modeling Language, Object Management Group, Inc (online), available from 〈HTTP://www.omg.org/spec/SysML/〉 (accessed 2017-08-25).