第81回CSEC研究会

安心・安全なIoTシステム(SSIoT)に関する考察

2018年5月17日
中央大学研究開発機構
才所敏明　辻井重男

本発表の構成

1. IoTへのサイバー攻撃急増の現状・動向
2. IoTの特質とその特質に起因する
   セキュリティ課題
3. SSIoTにおいて想定する
   サイバーセキュリティリスク
4. SSIoTが対象とするIoTシステムモデル
5. 採用・連携を検討中の既存技術
6. 想定するSSIoTのセキュリティ機能と
   その実現策検討方針
7. 終りに
   SSIoT構想策定にあたっての基本方針

1. IoTへのサイバー攻撃急増の現状・動向

＊2016年・64億台，2017年・84億台、2020年・204億台程度のIoT接続台数（ガートナー報告）

＊2016年9月、史上最大級のIoT利用分散型サービス妨害（DDOS）事件（KrebsOnSecurity攻撃）

＊IoT向けマルウェア「Mirai」：脆弱なIoT機器を奴隷化し，奴隷化したIoT機器には脆弱なIoT機器の探索作業を行わせ，急速にボットネットを巨大化

＊2016年10月に「Mirai」のソースがインターネット上に公開され，類似するIoT向けマルウェアも出現

2. IoTの特質とその特質に起因するセキュリティ課題

2.1 IoT機器

(ア-1)インターネット接続が想定されておらず、セキュリティ機能が脆弱か未実装

(ア-2)安価さ・小型化を優先され、高度なセキュリティ機能が実装不可

(ア-3)更新機能・サービスが提供されておらず、
長期使用時にセキュリティ機能が危殆化

2.2 IoT機器設置環境

(イ-1) 監視できない環境への設置のため、盗難・破壊・改ざんの防止・検知困難

(イ-2)電源や通信が不安定な環境のため、データ収集に障害

2.3 IoTシステム

(ウ-1)インターネット接続経験の少ないIoTシステム構築事業者・個人のため
不適切なIoT機器の選定やネットワークの構成、不適切なIoT機器の設定

(ウ-2)インターネット接続システム運用経験の少ないIoTシステム運用事業者や
個人のため、サイバー攻撃による被害や加害行為への加担の把握が困難

3. SSIoTにおいて想定するサイバーセキュリティリスク

3.1 IoT機器の直接的被害
(a-1)IoT機器内のデータ搾取
(a-2)IoT機器内のデータ・ソフトウェアの改ざん、不正な追加・削除
(a-3)IoT機器へのサービス不能（DOS/DDOS）攻撃

3.2 IoT機器が送信する情報の被害
(b-1)送信データの搾取や改ざん

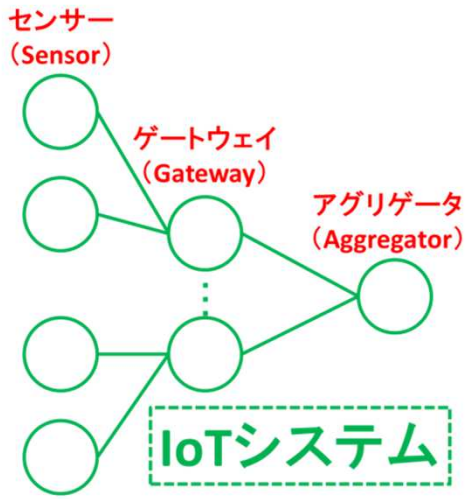
3.3 IoT機器が悪用される被害
(c-1)不正なサイバー攻撃に加担させられること

3.4 IoT機器の被害・加害の早期収拾の困難さ
(d-1)攻撃に参加した（参加させられた）IoT機器管理者・組織の特定・追跡の困難さ

3.5 IoT機器の適切な状態確認・維持の困難さ
(e-1)IoT機器内のデータやソフトウェアの古さ，セキュリティ対策の危殆化
(e-2)IoT機器内のデータ漏洩や改ざんの検知の困難さ

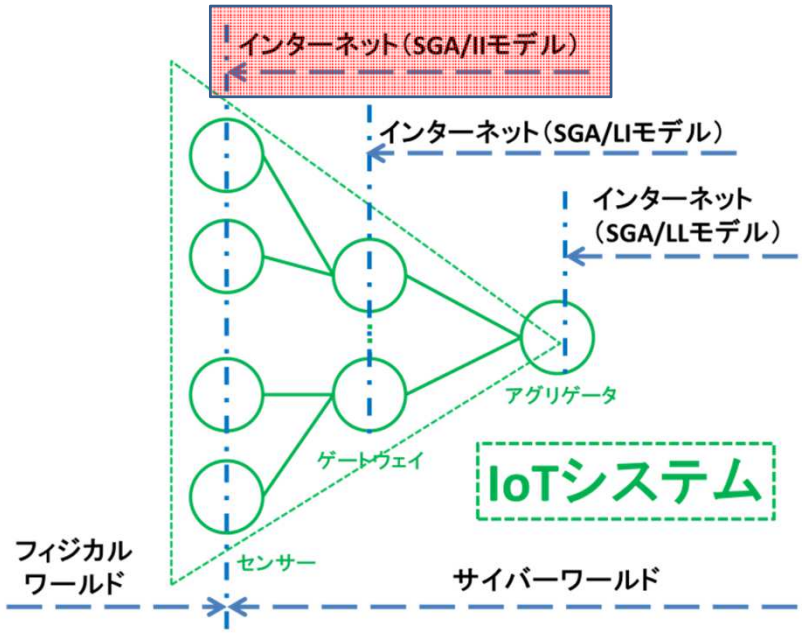
4. SSIoTが対象とするIoTシステムモデル

4.1 IoTシステム構成モデル



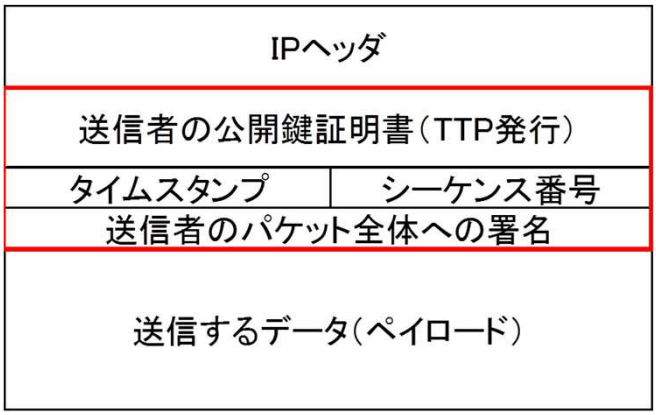
SGA（Sensor – Gateway - Aggregator）モデル

4.2　SGAモデルのインターネット上での実装モデル

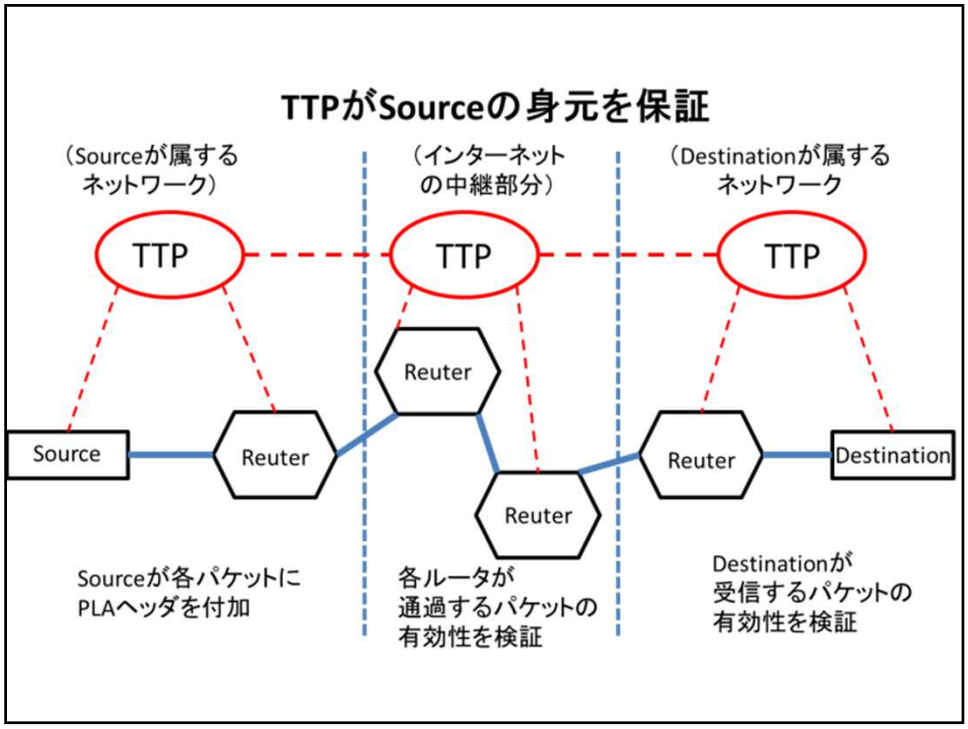


5.　採用・連携を検討中の既存技術

5.1　Packet Level Authentication（PLA）

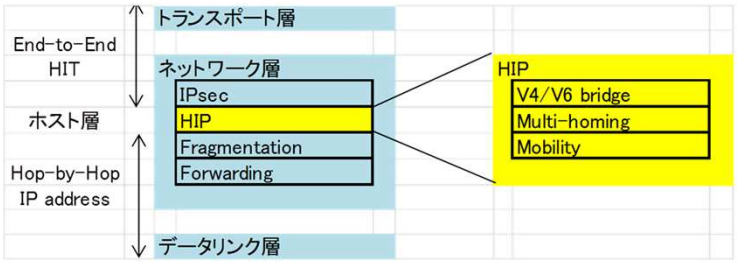


PLAヘッダの位置と主要な構成要素



5.2 Host Identity Protocol（HIP）

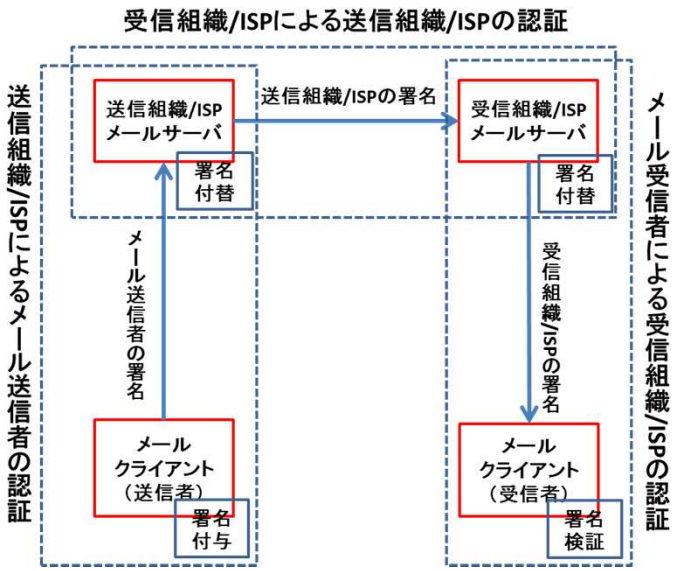
OSI参照モデル			
階層	名称		
7	アプリケーション層	アプリケーション間のやり取り	
6	プレゼンテーション層	データの表現形式	
5	セッション層	接続の手順	
4	トランスポート層	データ通信の制御	＜Host ID、ポート＞
	ホスト層	ホストの識別	Host ID
3	ネットワーク層	インターネットワークでの通信	IPアドレス
2	データリンク層	同一ネットワーク上での通信	
1	物理層	ケーブル、電気信号、コネクタ	



HI：Host Identifier（公開鍵）　　HIT：Host ID Tag（公開鍵のハッシュ値（128ビット））

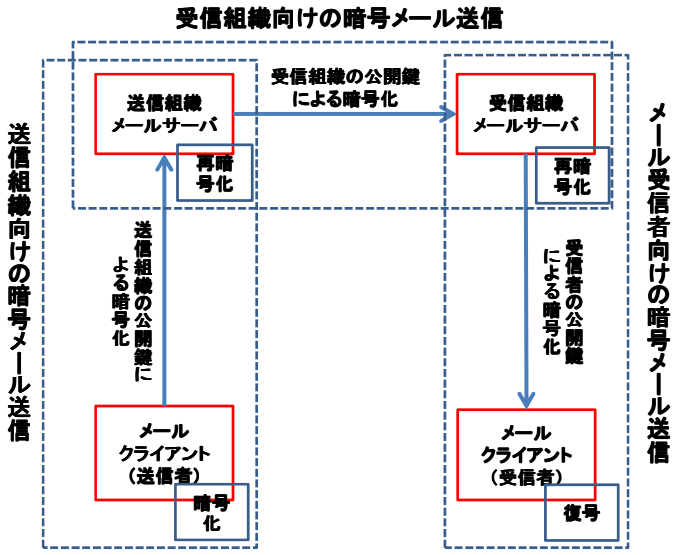
HIPの位置付け・役割

5.3　SSMAX構想－1



認証の連鎖（連結可能匿名化）

5.3　SSMAX構想－2



暗号化の連鎖

6. 想定するSSIoTのセキュリティ機能とその実現策検討方針

6.1 IoT機器の保護（被害者とならないための）対策

(a-1)IoT機器内のデータ漏洩防止
アクセス要求エンティティの認証と認可
認証においては，PLAおよびHIPの活用可能性を検討
認証されたエンティティの参照可能範囲の定義

(a-2)IoT機器内のデータ・ソフトウェアの
改ざんや不正追加・削除の防止
認証されたエンティティの更新可能範囲の定義

(a-3)IoT機器へのサービス不能（DOS/DDOS）攻撃への対応
不正なアクセス（パケット）の高効率なフィルタリング
IPアドレスやホスト識別子によるフィルタリング，
署名の検証によるフィルタリング
PLAおよびHIPの活用可能性を検討

6.2 IoT機器が送信するデータの保護対策

(b-1)ネットワーク経由送信されるデータの
漏洩や改ざん防止・検知
暗号技術（署名，暗号化）による保護
SSMAX構想の理念に基づき
ステップワイズな認証・暗号化を想定
（組織暗号の活用可能性を検討）

6.3 IoT機器の保護（加害者とならないための）対策

(c-1)不正なサイバー攻撃に加担させられることの防止
不正なデータ・ソフトウェアの改ざんや追加・削除対策
許可アクセス先エンティティの登録制による
想定外エンティティへのアクセス・データ送信の排除

6.4　IoT機器および機器管理者・組織の特定・追跡性確保（被害・加害を早期に収拾させるための）対策

(d-1)攻撃に参加した（参加させられた）IoT機器および機器管理者・組織の特定・追跡の困難さの解消
アクセスを要求してきたエンティティ（IoT機器等）からのアクセス要求情報に以下の情報を付加
管理者・組織（アグリゲータ等の管理者・組織）を特定でき、かつ、その管理者・組織がアクセス要求エンティティ自身を特定できる情報
アクセス要求エンティティの一定の匿名化を実現
（連結可能）匿名化、PLAおよびHIPの活用可能性を検討

6.5　IoT機器の遠隔監視・更新（IoT機器の適切な状態を維持し、セキュリティリスクをミニマムにするために）

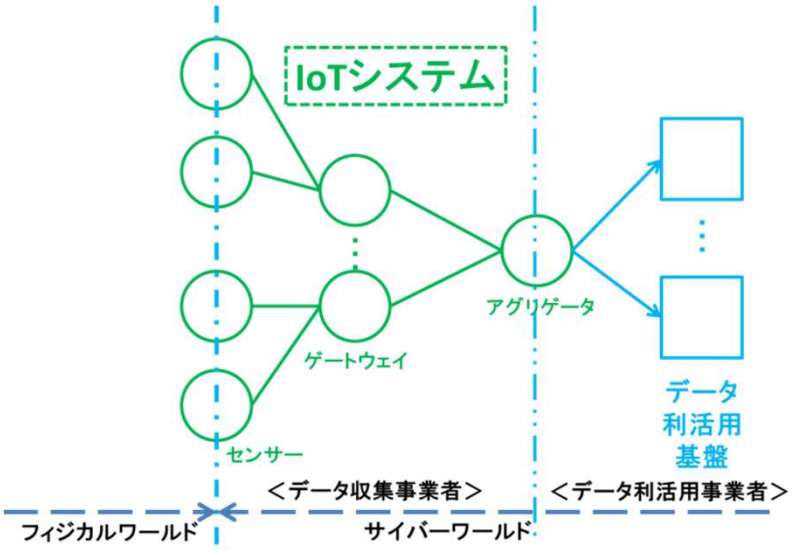
(e-1)IoT機器内のデータやソフトウェアの古さ，セキュリティ対策の危殆化への対応
IoT機器内のデータやソフトウェアの安全な更新
適切な更新指示および適切な更新情報かどうかの認証
PLAおよびHIPや，SSMAXのステップワイズの認証・暗号化の活用可能性を検討
(e-2)IoT機器内のデータ漏洩や改ざんの検知の困難さへの対応
IoT機器のふるまいや送信データを監視し異常性を検知する仕組みも有効
定期的にはIoT機器内のデータやソフトウェアが正常であることを検査することが必要
適切な検査指示かどうかの認証も必要
PLAおよびHIPや，SSMAXのステップワイズの認証・暗号化の活用可能性を検討

7. おわりに

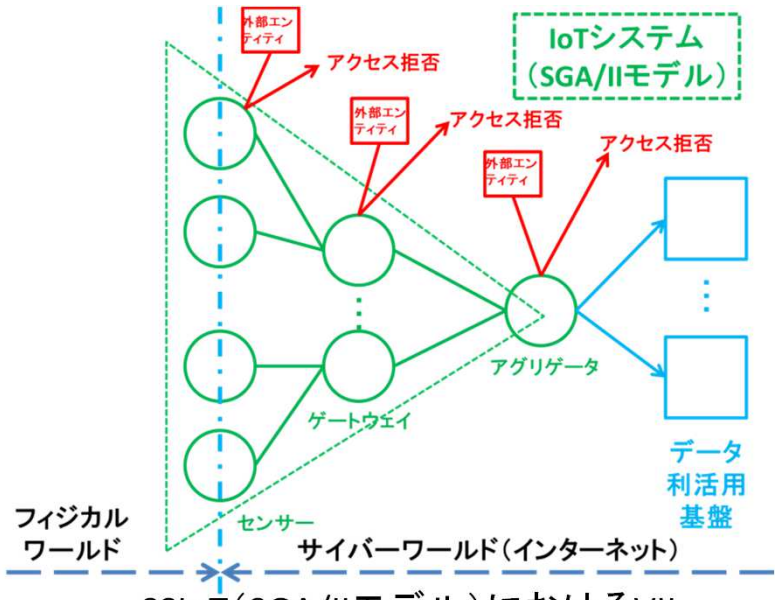
7.1 本稿では、安心・安全なIoTシステム（SSIoT）を目指した研究開発の第1歩として、以下を実施

＊SSIoTで想定するサイバーセキュリティリスクを整理
＊想定するIoTシステムやその実装モデルを整理
＊SSIoT実現に活用を想定している既存技術の整理
＊想定するIoTシステム/実装モデルについて想定するリスクとそれへの対応方針案の策定

7.2 当面は、SGA/IIモデルを中心に検討予定



VII（Virtual Intranet over Internet）の可能性



SSIoT（SGA/IIモデル）におけるVII

7.3　今後、更に検討を深め、
SSIoTの具体的仕様策定へ

＊匿名性と特定・追跡性の両立
連結可能匿名性
＊当面は、SSIoT（SGA/IIモデル）システムを対象
VIIの実現可能性
IoTシステム内の通信特性を利用した
監視機能の可能性

終