Vol.2018-CSEC-81 No.3
Vol.2018-IOT-41 No.3
2018/5/17

安心・安全な IoT システム(SSIoT)に関する考察

才所敏明[†1]　辻井重男[†2]

概要：インターネットへ接続される機器（IoT 機器）に起因する様々のセキュリティ問題が社会を脅かしつつある．IoT 機器は今後も急増する見込みであり，IoT 機器や IoT システムの安心・安全な利用に関する技術・ノウハウを整理し社会への普及を急ぐ必要がある．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，まず IoT 機器やシステムの特質を分析しその特質に起因するセキュリティ上の課題を考察する．また，IoT 固有のセキュリティリスクも含め，SSIoT として想定すべきセキュリティリスクを考察する．次に，SSIoT のシステムモデルの考察を行い，当面の検討対象システムモデルを明確にすると共に，SSIoT の実現において活用を想定している既存の技術や標準を説明の上，想定しているセキュリティリスクへの SSIoT としての対策方針を紹介する．最後に，SSIoT 構想策定にあたっての基本的な方針を紹介する．

キーワード：IoT, Internet of Thing, SSIoT, 安心・安全な IoT システム, PLA, Packet Level Authentication, HIP, Host Identity Protocol, SSMAX, 安心・安全な電子メール利用基盤, VII, Virtual Intranet over Internet

Considerations about the secure and safe IoT system (SSIoT)

TOSHIAKI SAISHO[†1]　SHIGEO TSUJII[†2]

Abstract: Various security problems caused by devices connected to the Internet (IoT devices) are threatening our society. AS IoT devises are expected to increase rapidly in the future, it is necessary to develop the technology and to organize the know-how on secure and safe use of IoT devices and IoT systems and then to disseminate them to our society. In this paper, as the first step of research and development aiming at the secure and safe IoT system (SSIoT), we first analyze the characteristics of IoT devices and IoT systems and then we organize the security issues resulting from their characteristics. We also organize the security risks that should be assumed as SSIoT, including the security risks inherent in IoT. Next, we examine the system model of SSIoT, clarify the models to be considered at the present time, explain the existing technologies and standards that are supposed to be used to realize SSIoT, and then explain the security risks and their countermeasure assumed in SSIoT. Finally, we will describe the basic idea of formulating the SSIoT concept.

Keywords: IoT, Internet of Thing, SSIoT, Secure and safe IoT system, PLA, Packet Level Authentication, HIP, Host Identity Protocol, SSMAX, Secure and Safe Mail Exchange Framework, VII, Virtual Intranet over Internet

1. IoT へのサイバー攻撃急増の現状・動向

インターネットへ接続される機器（IoT 機器）は急増中であり，ガートナーによると 2016 年には 64 億台程度，2017 年には 84 億台程度の接続台数とみられ世界の人口（2017 年には 75 億人程度）を超えるものと予測されている．IoT 機器の急増はその後も続き，2020 年には 204 億台に達すると予測されている[1]，[2].

一方，IoT 機器へのサイバー攻撃も急増している．国立研究開発法人・情報通信研究機構（NICT）によると，サイバー攻撃全体では 2016 年は 2015 年の 2.4 倍の 1281 億件に達し，IoT 機器への攻撃件数も 2015 年には全体の 26%だったものが 2016 年には半数を超えた，ということである[3].

IoT 機器へのサイバー攻撃が急増したのは，インターネットに接続されている IoT 機器の脆弱性にある．大量にインターネットに接続されるようになった家庭や小規模な事業者が使用する機器，DVR，IP カメラ，ルータ，プリンタなどは，安価が故にアクセス制御はユーザ名とパスワードのみで行われる仕組みが多く，しかもインターネットに接続して使用する家庭や小規模事業者のセキュリティ意識が低いが故に，デフォルトのユーザ名，パスワードのまま使用されていることが多い．このような IoT 機器の脆弱性を突いたサイバー攻撃事件が多発している．

2016 年 9 月には史上最大級と言われる IoT を利用した分散型サービス妨害（DDOS）事件が発生した．サイバー攻撃により乗っ取られた IoT 機器が攻撃者の手先として攻撃に加担させられた事件である．攻撃を受けたのは KrebsOnSecurity という米国のセキュリティ情報サイトで，IoT 向けマルウェア「Mirai」により 15 万台以上の乗っ取られた IoT 機器で構成されたボットネットから一斉攻撃を受けた[4].

「Mirai」は，主要ベンダの各種 IoT 機器の出荷時のデフォルトのユーザ名およびパスワードを利用し不正侵入を試み，成功した 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

†1 中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：toshiaki.saisho@advanced-it.co.jp）
†2 中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：tsujii@tamacc.chuo-u.ac.jp）

Vol.2018-CSEC-81 No.3
Vol.2018-IOT-41 No.3
2018/5/17

トを巨大化させる IoT 向けマルウェアである.「Mirai」のソースコードは，2016 年 10 月に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, KrebsOnSecurity 攻撃事件と同程度あるいはそれ以上の規模の IoT 機器が利用された DDOS 攻撃事件も次々と発生している状況である.

2. IoT の特質とその特質に起因するセキュリティ課題

インターネット上で様々のサービスを提供しているサーバシステムや，サービスを利用するクライアント PC は，長年サイバー攻撃に晒されてきたため，ファイアウォール等の適切なセキュリティ機器やセキュリティソフトが開発され，サイバー攻撃に対し現在は一定レベルの対策がとられている.

一方 IoT については，IoT 機器や IoT システムの構築および運用環境等の特質により，従来からインターネットに接続されたシステムとは異なるセキュリティ課題を抱えている．本章では，サイバー攻撃に利用されている IoT の特質とその特質に起因するセキュリティ課題をまとめている.

2.1 IoT 機器

(ｱ-1)ローカルなネットでの簡易な利用を想定されている機器も多く，しかもそのような機器も簡単にインターネットに接続が可能で，IoT 機器として利用されている.
＝＞インターネット接続を前提とされていない機器は，セキュリティ機能が脆弱か実装されていない.

(ｱ-2)安価さ・小型化を優先された機器も多く，機能・性能が限られている IoT 機器も多い.
＝＞高度なセキュリティ機能が実装されていない（実装できない）IoT 機器もある.

(ｱ-3)IoT 機器は長期間の利用を想定されているが，更新機能・サービスの無い IoT 機器も多い.
＝＞長期間利用されている IoT 機器は，セキュリティ機能が危殆化してしまう恐れがある.

2.2 IoT 機器設置環境

(ｲ-1) 日常的に監視できない環境に設置される IoT 機器もある.
＝＞機器の盗難・破壊，機器内のソフトや設定の改ざんの防止・検知が困難な IoT 機器もある.

(ｲ-2)電源供給や通信が不安定な環境に設置される IoT 機器もある.
＝＞必要なときに必要なデータを入手できない IoT 機器もある.

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・個人も多い.
＝＞不適切な IoT 機器の選定や不適切なネットワークの構成，インターネット接続時に不適切な設定になっている IoT 機器もある.

(ｳ-2)インターネット接続システム運用・管理経験の少ない IoT システムの運用・管理事業者・個人も多い.
＝＞IoT 機器や IoT システムの不適切な運用・管理により，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な IoT 機器や IoT システムもある.

3. SSIoT において想定するサイバーセキュリティリスク

前章で述べた IoT の特質とそれに起因するセキュリティ課題を念頭に置きつつ, 安心･安全な IoT システム（SSIoT）構想策定にあたって想定するセキュリティリスクを述べる.

なお，IoT の利用は多岐にわたり，IoT システムも多種多様であるが，本稿ではセンサー等の IoT 機器によるデータ収集を目的とした IoT システムを対象に検討する．IoT 機器を通じた物理世界（フィジカルワールド）の制御機能を含む IoT システムについての検討は別途行うものとする.

また，IoT システムへのインターネット経由のサイバー攻撃対策を中心に検討する．IoT システムを構成する IoT 機器を含む様々の機器への直接の攻撃や，インターネットとは異なるローカルネット（Bluetooth や ZigBee によるネットワーク等）経由の攻撃については別途検討を行うものとする.

3.1 IoT 機器の保護（被害者とならないために）

(a-1)IoT 機器内のデータ漏洩：
IoT 機器には自身を証明するパスワードや秘密鍵，通信相手を確認するためのデータや，IoT 機器を管理する組織に関するデータなども格納されており，このようなデータの漏洩はサイバー攻撃者に対して IoT 攻撃の手がかりを与えてしまうことになる.

(a-2)IoT 機器内のデータ・ソフトウェアの改ざんや不正な追加・削除：
IoT 機器の機能を制御する設定データ（通信相手の情報等）や機能を実現するソフトウェアの改ざんや不正追加・削除は，IoT 機器の機能を直接的に改変し，IoT の適切な運用・管理を崩壊させるものである.

(a-3)IoT 機器へのサービス不能（DOS/DDOS）攻撃：
IoT 機器は今後クリティカルなサービスを支えるシステムへ組み込まれることが予想され，サービスを停止させられることが生命の危険や社会の混乱を招くことになりかねない.

3.2 IoT 機器が送信する情報の保護

(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：
IoT 機器で収集される価値あるデータが漏れることはビジネス上の痛手でもあり，またプライバシー情報の漏洩にもなりかねない. また，送信されるデータの改ざんは，データを利用するシステムの誤った判断を招きかねず，IoT システムの信頼性を失うと共に，責任をも問われかねない.

3.3 IoT 機器の保護（加害者とならないために）

(c-1)不正なサイバー攻撃に加担させられること：

現在の IoT へのサイバー攻撃は IoT そのものへの攻撃を最終目的としているわけではなく，脆弱な IoT 機器を乗っ取りボットネット構成するのが目的であり，大規模な DDOS 攻撃の際に攻撃に参加させることを最終目的としていることが多い．乗っ取られた IoT 機器の管理者・組織はサイバー攻撃の加害者となってしまうことになり，責任を問われかねない．

3.4 IoT 機器および機器管理者・組織の追跡性確保（被害・加害を早期に収拾させるために）

(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：

一般にインターネット経由の攻撃の場合，攻撃サイトの特定・追跡は困難である．SSIoT においても，被害者・加害者とならないための最善の策を採ったとしても，何らかの攻撃を受けるとか攻撃に参加させられるリスクは残る．万一，攻撃を受けたことを確認できた場合でも，その攻撃元である IoT 機器および機器管理者・組織の特定・追跡が困難であれば，攻撃をやめさせることができず，以降も攻撃に晒され続けることになる．また，万一，管理下にある IoT 機器が攻撃に加担させられた場合でも，どの IoT 機器が攻撃に加担させられたかを特定・追跡できず，加担させられた攻撃の被害を拡大させ，その責任は重くなることになる．

3.5 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：

IoT 機器は長期的に使用される場合が多く，IoT 機器内のソフトウェアや設定が古いと，IoT 機器としての機能を適切に果たせず，またセキュリティ機能の危殆化により，サイバー攻撃を防ぐことができなくなる．

(e-2)IoT 機器内のデータ漏洩や改ざんの検知の困難さ：

IoT 機器内のデータ漏洩や改ざんにより，万一，IoT 機器が乗っ取られた場合，早期に発見しないと，サイバー攻撃に加担させられ，経済的・社会的責任を問われることになる．

4. SSIoT が対象とする IoT システムモデル

前章で述べたように，SSIoT ではデータ収集を目的とする IoT システムを対象に検討する．

データ収集を目的とした IoT システム限ったとしても多様な構成が考えられるが，SSIoT に求められるセキュリティ機能を検討する対象として，4.1 にて IoT システム構成モデルを定義している．この IoT システム構成モデルは，シンプルではあるが多様な IoT システムを構成する基本的な構成（サブシステム）となっている．

また，インターネット経由のサイバー攻撃に対するセキュリティ機能を検討するに当たっては，IoT システム構成モデルのインターネット上での実装モデルが問題となるが，SSIoT に求められるセキュリティ機能を検討する対象として，4.2 にて IoT システム構成モデルのインターネット上での実装モデルを定義している．

4.1 IoT システム構成モデル（SGA モデル）

SSIoT で検討対象とする IoT システム構成モデルを図 1. に示している．本構成モデルを SGA（Sensor - Gateway - Aggregator）モデルと称することとする．

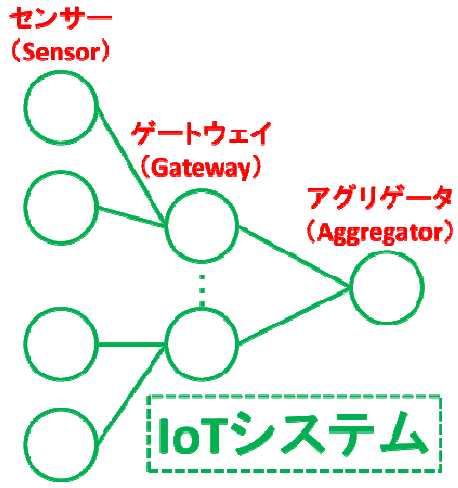

図 1. SGA モデル

SGA モデルは，センサー，ゲートウェイ，アグリゲータの三つの層から構成されている．

センサー層は，フィジカルワールドとサイバーワールドが接する層であり，フィジカルワールドのデータを収集するセンサーで構成されているものとする．

ゲートウェイ層は，センサーが収集するデータの中継やセンサーの管理を主として担当するゲートウェイで構成されている．

アグリゲータ層は，ゲートウェイが収集したデータを更に収集・管理する層で，収集したデータを更にデータを活用するサービスプロバイダ等への配信等を担当するアグリゲータから構成されている．

4.2 SGA モデルのインターネット上での実装モデル

SSIoT で検討対象とする SGA モデルのインターネット上での実装モデルを SGA/II（Internet - Internet）と称することとする．SGA/II モデルは，センサー，ゲートウェイ，アグリゲータの全てがインターネットに接続され，インターネットを利用し通信する IoT システムである．

一般に，センサーは小型・安価であることを求められ，そのため実装可能なセキュリティ機能も制限されることも多い．そこで，センサーへの直接のサイバー攻撃を避けるため，センサーのネットワークをインターネットから切り離す実装モデルが採用される場合も多い．本実装モデルを

SGA/LI（Localnet － Internet）と称することとする．

更に，ゲートウェイを含め IoT システムの内部全体がサイバー攻撃に晒されることを避けるため，IoT システムの内部のネットワークをインターネットから切り離す実装モデルが採用されることもあり，本実装モデルを SGA/LL（Localnet - Localnet）と称することとする．

図 2. に，三つの実装モデル，SGA/II，SGA/LI，SGA/LL の関係を示している．

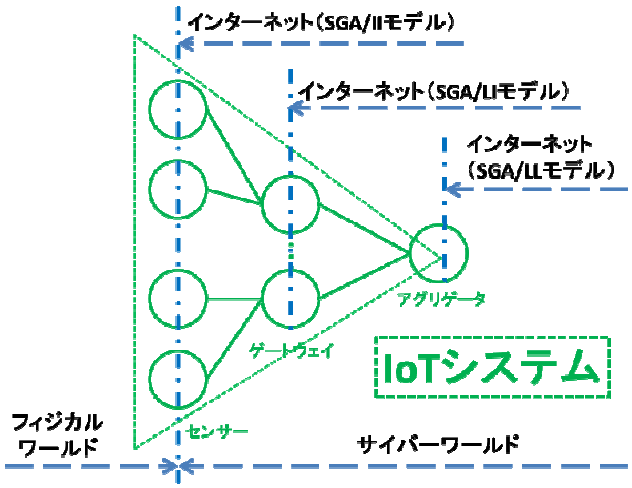

図 2. SGA 実装モデル

本論文では以降，インターネット経由のサイバー攻撃のリスクが最も多い SGA/II モデルを中心に，SSIoT に求められるセキュリティ機能とその実現方策について論じるものとする．

5. 採用・連携を検討中の既存技術

本章では，SSIoT 構想策定において活用あるいは連携を想定している認証系の技術，ネットワークレベル，トランスポートレベル，アプリケーションレベルの技術について述べる．

5.1 Packet Level Authentication（PLA）[5]

PLA は，ネットワークのセキュリティを維持するためのネットワーク層の技術である．PLA では，各パケットの認証をネットワークの各ノードで可能であり，改ざんされたり，遅延させられたり，複製されたパケットは各ノードで検出・廃棄可能で，ネットワークへの被害や無駄なリソース消費を回避することが可能となる．

PLA は２層のセキュリティ機能を提供する．その一つは，各パケットに付加される PLA ヘッダにて実現される．PLA ヘッダには，パケット全体に対する署名，タイムスタンプ，シリアルナンバーが格納されており，改ざん，遅延，複製されたパケットの検知が可能で，不正なあるいは望まれないパケットは中継する各ノードで検出でき破棄できる．もう一つは，TTP による従来の CA 局と同様の信頼できる管理機能である．PLA ヘッダには TTP が発行した送信者（ノード）の公開鍵証明書が格納されている．各ノードの暗号上のアイデンティティと実世界上のアイデンティティの連結が TTP により保証されており，障害発生時のノードの特定が可能となる．

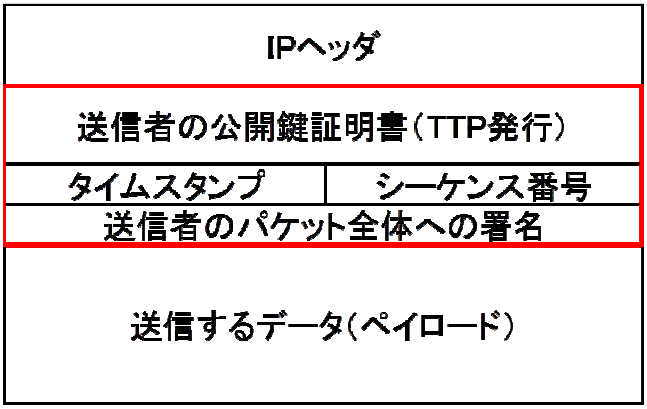

図 3. PLA ヘッダの位置と主要な構成要素

PLA では，膨大なトラフィックにもかかわらず，公開鍵暗号による署名が利用可能であることを想定している．そのために RSA に比べ短い鍵長が可能な楕円曲線暗号の利用を想定しており，専用の ASIC を利用すれば，１秒に数百万の署名検証が可能，と試算されている．なお，PLA は Linux および FreeBSD 上で実装されており，公開鍵暗号として楕円曲線暗号（ECC）が使用されている．

PLA は IP ヘッダの拡張機能を利用している．全てのノードがパケットの署名検証機能を保有する必要は無く，インターネット上で PLA を利用したシステムを柔軟に構成できる．

PLA は，複数の暗号上のアイデンティティを利用することにより，一定の匿名性も実現でき，同時に悪意のあるノードの特定・追跡・排除が可能である．

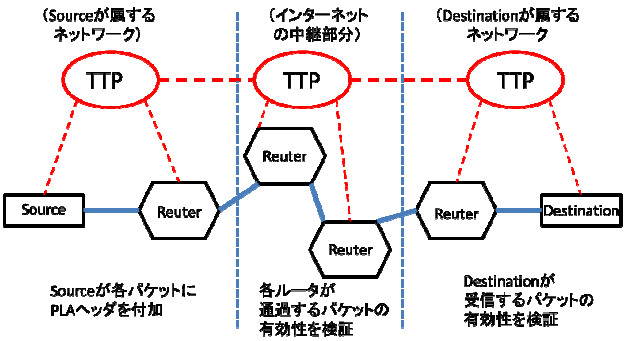

図 4. TTP 網が Source の身元を保証

5.2 Host Identity Protocol（HIP）[6]

Host Identity Protocol（HIP）は，ホスト識別子（ホストのネットワークインタフェースの名前）を導入，ホスト識別子を利用したホストを識別するためのプロトコルであ

る．従来，IP アドレスがホスト識別子とホストロケータ（ホストのトポロジカルな位置を示す名前）の二つの役割を持っていたが，そのうちのホスト識別子としての役割の分離を目指したものである．ネットワーク層では従来通り IP アドレスが使用されるが，トランスポート層では，従来はポート番号だけだったが新たにホスト識別子を追加し，ホスト識別子とポート番号を利用する方式である．

HIP では，すべてのホストはユニークな識別子，公開鍵暗号から生成されたホスト識別子を持っており，相互に認証可能である．公開鍵証明書を発行する TTP により認証された各ホストの識別子と実世界上のアイデンティティの連結により障害発生時等でのホストの特定が可能となる．

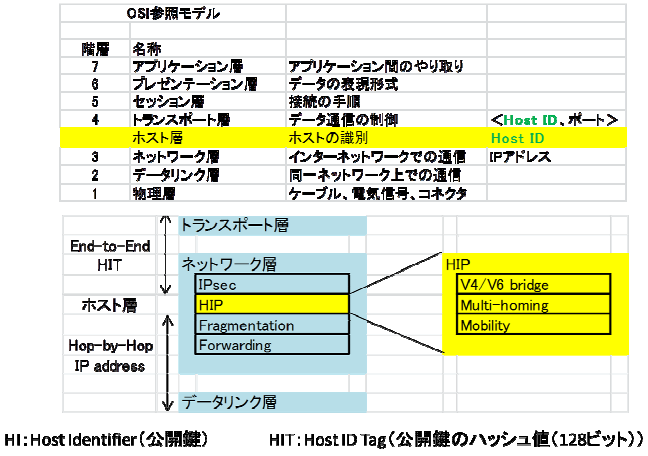

図 5．HIP の位置付け・役割

5.3 SSMAX 構想[7]

SSMAX（Secure and Safe E-mail Exchange Framework） とは，著者らが考案し提唱している安心・安全電子メール利用基盤のことである．SSMAX 構想は，組織を対象とした標的型攻撃メールや個人を対象としたフィッシングメール，いじめや脅迫メールの根絶をめざした構想である．

SSMAX 構想の基本理念は，電子メール送信者の確実な特定・追跡性と一定の匿名性の実現，にある．SSMAX では，電子メール送信者が送信したメールは中継組織および受信者のそれぞれにおいて直前の送信者・組織の認証を実施する認証の連鎖により，電子メール送信者の匿名性と特定・追跡性の両立を実現している．

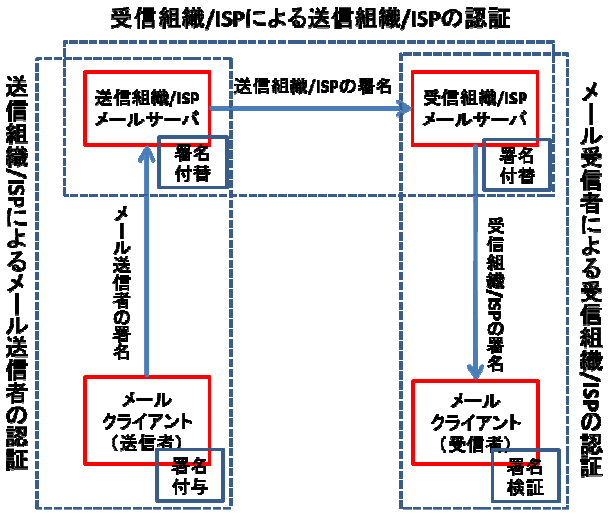

図 6．認証の連鎖

この理念は SSIoT においても重要である．データを発信した IoT 機器を確実に特定・追跡でき，不正なアクセス，攻撃等に悪用された場合は直ちに是正措置が取れる仕組みは IoT システムにおいても不可欠である．一方，IoT 機器の特定・追跡に必要な情報を公開することは様々の攻撃のリスクを高めることになり好ましくない．IoT システムを管理する組織が，管理下の IoT 機器に対する特定・追跡性を保証し，対外的には連結可能匿名化し IoT 機器の一定の匿名性を確保しておくことが望ましい．

また，SSMAX 構想では，送信する電子メール内容の改ざん検知・漏洩防止の実現も，目指している．SSIoT においても収集するデータの改ざん検知・漏洩防止は極めて重要である．SSMAX で採用している段階的なデータ認証のための署名，データ秘匿のための暗号化，暗号化データの暗号化状態での暗号鍵の付替え（再暗号化）は，SSIoT でも活用可能である．

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

本章では，第 3 章で述べた SSIoT において想定するサイバーセキュリティリスクについて，第 5 章で述べた採用・連携候補既存技術を活用した対策の方向性と具体化のための検討課題をまとめている．

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を防ぐには，不正なアクセスを防止する機能が必要であり，アクセス要求エンティティの認証と認可（アクセスや参照の是非の判断）が必要となる．

アクセス要求エンティティの認証には，簡便なパスワード方式や公開鍵暗号による署名検証方式が想定され，IoT 機器の役割や構成する IoT システムのセキュリティポリシーに応じ選定することになろう．なお，アクセス

要求エンティティの認証においては，PLA および HIP の活用可能性を検討する予定である．

認証されたアクセス要求エンティティについては，許可すべき参照範囲を個々のアクセス要求エンティティごとに定義しておき，それに基づいて認可することになろう．

(a-2) IoT 機器内のデータ・ソフトウェアの改ざんや不正な追加・削除を防ぐには，(a-1) で示した不正なアクセスを防止する対策と共に，認証されたアクセス要求エンティティについては，許可すべき更新の範囲を個々のアクセス要求エンティティごとに定義しておき，それに基づいて認可することになろう．

(a-3) IoT 機器へのサービス不能（DOS/DDOS）攻撃を防ぐには，不正なアクセス（パケット）の高効率なフィルタリングが必要となる．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が想定されるが，IoT 機器の処理性能に応じた判断が必要となろう．PLA および HIP の活用の可能性を検討する予定である．

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 IoT 機器が収集したデータの漏洩や改ざんを防ぐためには暗号技術（署名，暗号化）による保護が必要である．暗号技術の適用においては，SSMAX 構想の理念に基づきステップワイズな認証・暗号化を想定しており，組織暗号技術の活用可能性を検討する予定である．

6.3 IoT 機器の保護（加害者とならないための）対策

(c-1) IoT 機器が不正なサイバー攻撃に加担させられ，加害者となることを防ぐには，(a-2) で述べた不正なデータ・ソフトウェアの改ざんや追加・削除対策に加え，万一乗っ取られた場合でも，あらかじめ登録されているアクセスを許可されたエンティティ以外のエンティティへのデータ送信等のアクセスを止める仕組みが必要である．

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

(d-1) サイバー攻撃に加担した IoT 機器およびその IoT 機器の管理者・組織をすみやかに特定できるためには，アクセスを要求してきたエンティティ（IoT 機器等）の管理者・組織（アグリゲータ等の管理者・組織）を特定できると共に，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をアクセス要求のための情報に付加しておく必要がある．なお，アクセス要求エンティティの情報は，その情報が悪用されエンティティが特定・追跡されないよう，（連結可能）匿名化を施しておくことを想定している．ここでも，PLA および HIP の活用可能性を検討する予定である．

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）

6.6

(e-1) IoT 機器内のデータやソフトウェアの安全な更新には，IoT 機器内のデータやソフトウェアの情報を管理し必要に応じ更新作業が必要である．一方，更新を装ってのサイバー攻撃も想定され，適切な更新指示か，および適切な更新情報かどうかの認証が必要である．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する予定である．

(e-2) IoT 機器内のデータ漏洩や改ざんの遠隔からの検知には，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であろう．異常性の検知が無くとも，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であろう．一方，検査を装ってのサイバー攻撃も予想され，適切な検査指示かどうかの認証が必要である．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する予定である．

7. SSIoT 構想策定にあたっての基本方針

前章で述べた SSIoT において想定するサイバーセキュリティリスクへの対策の方向性と具体化のための検討課題を前提に，本章では SSIoT 構想策定にあたっての基本的な考え方を紹介する．

7.1 SSIoT 基本構成

SSIoT の基本構成は以下の通り．

フィジカルワールドのデータを収集する事業者は IoT システム（SSIoT）によりデータを収集し，収集したデータは契約に基づき，データ利活用事業者へ配送することを想定している．

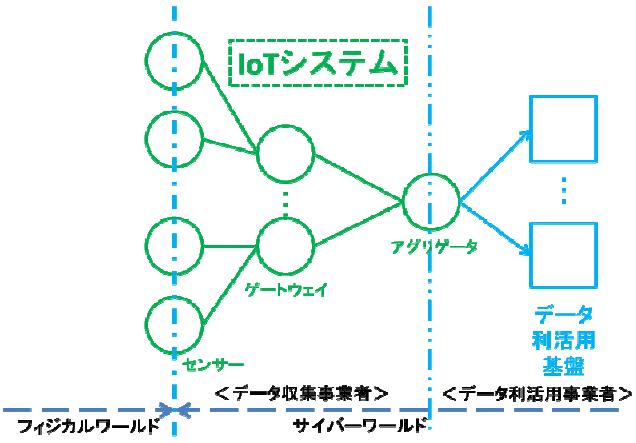

図 7. SSIoT 基本構成

SSIoT 基本システムは，三つの層，センサー，ゲートウェイ，アグリゲータから構成されている．センサーがフィジカルワールドのデータを収集，データはゲートウェイ経由アグリゲータに転送される．

7.2 VII（Virtual Intranet over Internet）

SSIoT（SGA/II モデル）は，IoT システムを構成するセンサー，ゲートウェイ，アグリゲータすべてがインターネットに接続されていることを想定している．

インターネットに接続していると，様々のインターネット接続機器やシステムあるいは人から不正アクセス等の攻撃が想定される．このような攻撃を避けるには，イントラネットのように外部からのアクセスを拒否できる仕組みが望ましい．そのためには，インターネット接続センサー，ゲートウェイごとにファイアウォールを設置すれば対応可能だが，現実的ではない．そこで，SSIoT（SGA/II モデル）では各センサー，各ゲートウェイにはファイアウォールの機能の実装を想定している．このようなファイアウォールの機能の連携により，インターネットに接続された機器群があたかもイントラネットを構成しているかのような論理的に閉鎖されたドメインを実現する VII(Virtual Intranet over Internet）の実現を目指している．

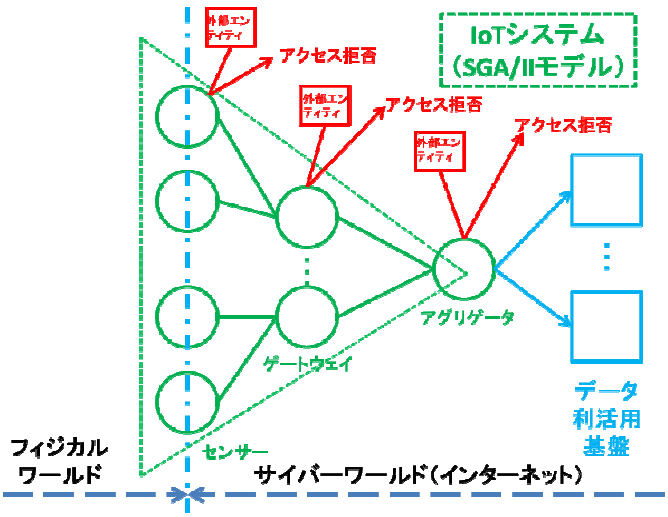

図 8. SSIoT（SGA/II モデル）における VII

7.3 SSIoT の監視・管理機能

SSIoT（SGA/II モデル）では VII の実現を目指すが，コンパクトさ，安価さを求められるセンサーやゲートウェイに十分な機能を想定した VII を実装するのは難しいことも想定される．

そこで，VII 内部の異常な振る舞いの検知など，センサーやゲートウェイを監視する機能も必要であろう．監視機能の実現には，センサーやゲートウェイに期待する役割とアグリゲータあるいは別途の監視・管理を担当するコントローラに期待する役割は，通信量や処理負荷のバランスに応じ分担を考える必要があろう．

SSIoT としては，個々の事情に応じた役割分担が可能になるような実装方式を検討する必要があろう．

8. おわりに

本稿では，当面 SSIoT が対象とする IoT システムを限定しつつ，IoT システムのセキュリティ課題と SSIoT としての対応方針，および SSIoT 構想策定にあたっての基本的な方針を述べた．

SSIoT の全体像を規定するには多くの検討課題が残されているが，機能性・性能や社会実装性を考慮しながら，詳細を詰めていく予定である．

参考文献

[1] “Gartner Says 8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016”, Press Release, February 2017.
https://www.gartner.com/newsroom/id/3598917

[2] “世界の統計 2017”, 総務省統計局, 平成 29 年.
http://www.stat.go.jp/data/sekai/pdf/2017al.pdf

[3] “サイバー攻撃 1281 億件 16 年, IoT 機器狙い急増”, 日本経済新聞, 2017 年 2 月 8 日.
https://www.nikkei.com/article/DGXLASDG08H3L_Y7A200C1000000/

[4] Manos Antonakakis, Georgia Institute of Technology 他, “Understanding the Mirai Botnet”, 26th USENIX Security Symposium, August 2017.

[5] D. Laughtin, “Packet Level Authentication (PLA) Extensions for Host Identity Protocol”, July 2010.
https://tools.ietf.org/pdf/draft-lagutin-hip-pla-00.pdf

[6] R. Moskowitz, P. Nikander, “Host Identity Protocol (HIP) Architecture”, RFC4423, IETF, May 2006.
https://tools.ietf.org/html/rfc4423

[7] 才所敏明, 五太子政史, 辻井重男, “「安心・安全電子メール利用基盤 (SSMAX)」”, コンピュータセキュリティシンポジューム 2017, 情報処理学会 2017.

[8] Jeffrey Voas, “Network og Things”, NIST Special Publication 800-183, NIST 2016.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf