CCDSSG

重要生活機器連携セキュリティ研究会
平成25年度活動報告

「つながるIT社会の安心・安全の確保に向けて」
～セキュアライフ2020～

2014年6月13日
重要生活機器連携セキュリティ研究会

2014 copyright (c) CCDSSG, Proprietary

目次

CCDSSG

2014 copyright (c) CCDSSG, Proprietary

1. はじめに

- 近年、屋外からスマートフォンでON/OFFできるエアコンや障害物を検知して停止する自動車など、生活機器へのIT活用が進んでいる。東京オリンピックが開催される2020年には、様々な生活機器がネットワークでつながり、省エネや医療・健康、娯楽などのサービスを提供したり、自動車の安全走行が実現されると期待される。
- しかしながらオリンピックの年には、開催国のネットワークや主要機関の情報システムへのサイバー攻撃が急増する傾向があり、2020年に日本でも、攻撃の余波が家庭や交通インフラに及ぶことが懸念される。
- そこで、研究会では、2020年の生活環境及び発生しうる脅威を想定するとともに、その時期までに行政や生活機器メーカ、サービス提供企業などが行うべき対策についてとりまとめた。
- 関係団体・企業の方々が本報告を参考としてセキュリティ対策の取組みを進めることで、ユーザが安心して生活機器を活用できる社会の到来を期待したい。本研究会としても、これからも積極的に生活機器連携セキュリティに関する検討及び提言を進めていく所存である。

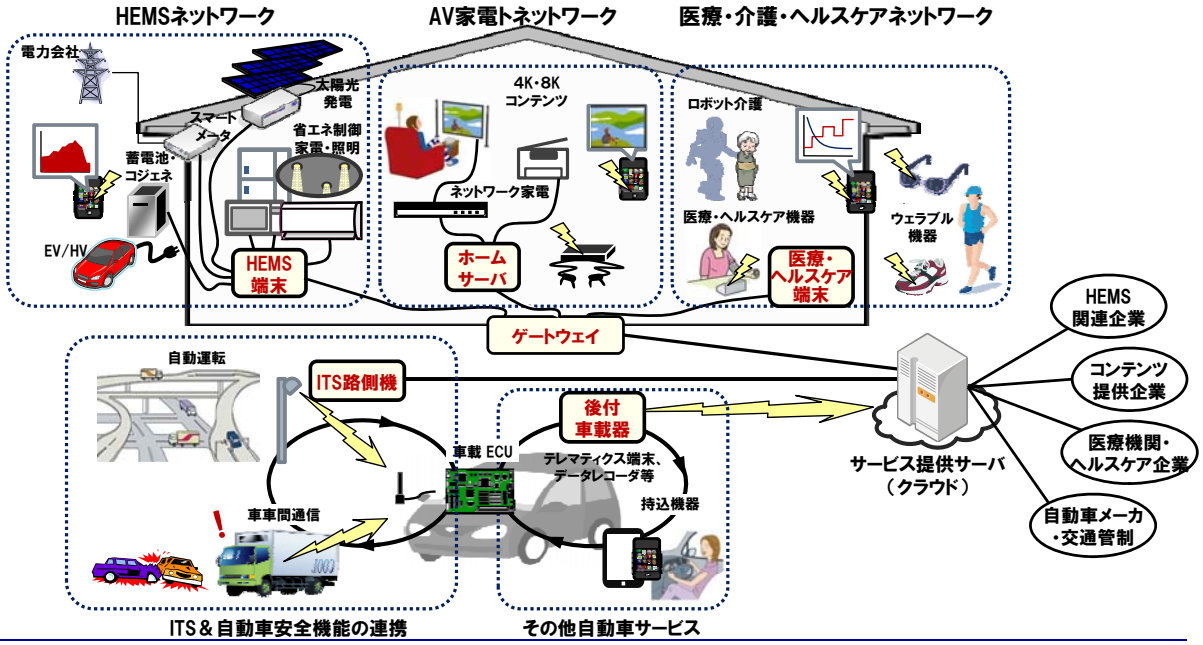
- 重要生活機器連携セキュリティ研究会
- 会長　徳田　英幸

2014 copyright (c) CCDSSG, Proprietary

2. 2020年までに解決すべき課題

2.1 想定される2020年の社会

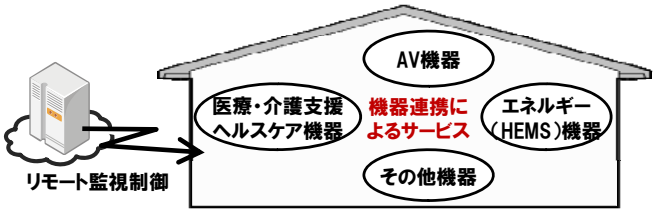
- 既に導入が始まっているHEMS、AV家電、医療・ヘルスケア、自動車などの製品・サービスの普及が東京オリンピックに向けて加速すると想定される。



2014 copyright (c) CCDSSG, Proprietary

2.1 想定される2020年の社会

- 家庭環境
  - 想定(2020年)
    - AV家電、ヘルスケア、エネルギーなど、様々な分野の生活機器が普及する。
    - それぞれの生活機器の連携やリモート監視制御により、新しいサービスも提供される。



- 医療・介護・ヘルスケア
  - 想定(2020年)
    - ヘルスケア機器や介護支援機器が家庭に普及する。
    - 機器のリモート監視や測定データによる遠隔診断等のサービスも提供される。
  - 参考
    - 2013年から「ロボット介護機器開発5ヵ年計画」開始
    - http://www.meti.go.jp/press/2013/02/20140203003/20140203003.html
    - 経済産業省・厚生労働省ロードマップで2020年にロボット介護機器が普及
    - http://www.kantei.go.jp/jp/singi/keizaisaisei/bunka/iryou/dai5/siryou4-2.pdf

2014 copyright (c) CCDSSG, Proprietary

2.1 想定される2020年の社会

- 自動車
  - 想定(2020年)
    - 2020 年代初頭頃までに自動運転が実現する。
    - 後付車載器や持込機器により、自動車の利用スタイルが多様化する。
  - 参考
    - 高速道路本線上における高度な運転支援システムによる連続走行を実現。路車協調による規制箇所等の車線毎の詳細な動的情報を提供する仕組みを研究開発し、高速道路本線上における車線変更等を伴う連続走行を実現。
      (国土交通省「オートパイロットシステムに関する検討会」中間とりまとめ」より)
      平成25年10月8日:http://www.mlit.go.jp/road/ir/ir-council/autopilot/
- AV家電
  - 想定(2020年)
    - 家庭向けコンテンツが高精細化、家庭のAV機器・ネットワークも高度化する。
  - 参考
    - 4K: CS・CATVは2014年、BS2020年、8K: 同 2016年、2020年に開始
    - スマートTV対応のサービス拡大 (以上、総務省ICT成長戦略より)
      平成25年7月4日 http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000108.html

2014 copyright (c) CCDSSG, Proprietary

2.1 想定される2020年の社会

- 省エネ
  - 想定(2020年)
    - スマートメータや蓄電池・コジェネ等が普及、電気自動車と家との接続も進む。
  - 参考
    - 2020年までに新築公共建築物等でZEB(ネット・ゼロ・エネルギー・ビル)を実現。2020年までに標準的な新築住宅でZEH(ネット・ゼロ・エネルギー・ハウス)の実現を目指す。2020年代早期に、スマートメーターを全世帯・全事業所に導入する。(エネルギー基本計画見直し政府原案より)
    - 平成26年2月25日 http://www.enecho.meti.go.jp/topics/kihonkeikaku/new_index.htm
- その他(モバイルデバイス、M2Mネットワーク)
  - 想定(2020年)
    - 膨大なモバイルデバイスがオリンピックビジネスやTV鑑賞に活用される。
    - 生活機器やセンサ、モバイルデバイスがM2Mネットワークで連携する。
  - 参考
    - 2020年にはモバイルデバイスの台数は世界で260-300億台
    - https://www.gartner.co.jp/press/html/pr20140408-01.html
    - http://pc.watch.impress.co.jp/docs/column/kaigai/20131106_622167.html

2014 copyright (c) CCDSSG, Proprietary

2.2 脅威の現状と将来への影響

- 生活機器に対する攻撃は年々増加している。特に、オリンピックの年には攻撃が急増し、影響が生活機器に及ぶ可能性がある。
- ここでは現状の脅威を整理し、将来への影響を検討する。

- 2.2.1 現在の脅威の事例
  - 自動車:外部から車載LANに侵入される脅威
  - 医療機器:心臓ペースメーカーを遠隔から停止する脅威
  - 家庭用生活機器:アイロンの中のハッキングチップの脅威
  - その他:標的型攻撃メールによる設計情報漏えいの脅威

2014 copyright (c) CCDSSG, Proprietary

2.2.1 脅威の事例

外部から車載LANに侵入される脅威

分　類	研究	分野	自動車	時期	2010/06	地域	米国

情報源

ワシントン大学Kohno氏ら論文　http://www.autosec.org/pubs/cars-usenixsec2011.pdf
デモビデオ　http://www.youtube.com/watch?v=bHfOziIwXic

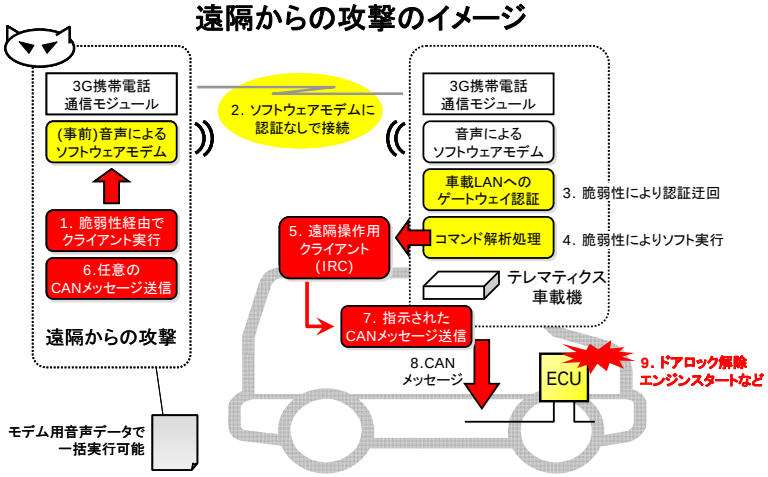
脅威

遠隔から車載LANに侵入する実験の論文が発表

概要

・3G携帯電話（自動車との通信はBluetooth経由）、CDによるメディアプレーヤーのアップデートなどを含め広範囲の侵入経路を検証。
・遠隔操作によるドア解錠、テレマティクスユニットの乗っ取りによる特定の自動車内の音声・ビデオ・位置等の記録データの入手についてデモを実施。

遠隔からの攻撃のイメージ



（2011 年度自動車の情報セキュリティ動向に関する調査http://www.ipa.go.jp/files/000024413.pdf より）

2014 copyright (c) CCDSSG, Proprietary

2.2.1 脅威の事例

心臓ペースメーカーを不正操作される脅威

分　類	研究	分野	医療機器	時期	2013/08	地域	米国

情報源

米国議会の調査部門である米会計検査院(GAO)のレポート
http://www.gao.gov/assets/650/647767.pdf　19～20P
上記を受けた米国食品医薬品局(FDA)のアナウンス
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

脅威

無線で遠隔から埋込み型医療機器を不正に操作する研究を基に、行政機関が警告

概要

・埋込み型医療機器の電池寿命は5～10年と長く、利用中に設定変更を行うための無線通信機能が内蔵されているが、保護が不充分。
・米会計検査院（GAO）は、ペースメーカーやインシュリンポンプを遠隔から不正に設定変更する研究（2008～2011年）を基に米国食品医薬品局（FDA)に検討を促した。
・FDAは上記を受け、リスクを医療機器メーカに警告。

（CCDSSG事務局作成）

2014 copyright (c) CCDSSG, Proprietary

2.2.1 脅威の事例

アイロンの中のハッキングチップの脅威

分　類	実例	分野	家電	時期	2013/10	地域	ロシア

情報源

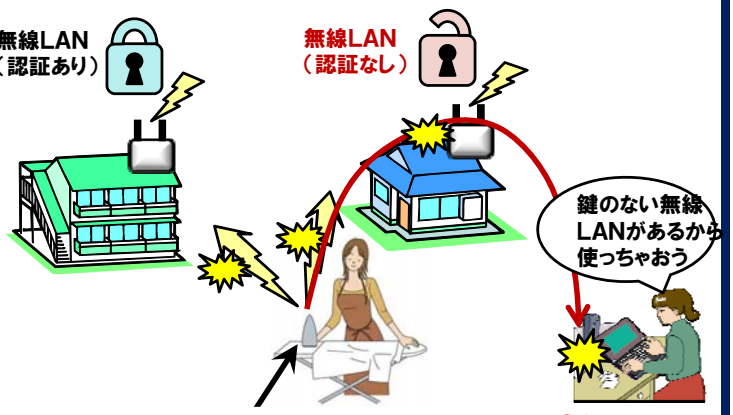
英国BBCサイト(「TV番組ロシア24」の放映内容より)
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337
(日本語記事　http://gigazine.net/news/20131029-spam-chips-hidden-in-iron/)

脅威

周囲の無線LAN上のPCにマルウェアを撒き散らす、アイロンの中のハッキングチップ

概要

- 中国製のアイロンの中に、近隣200m以内の無線LANにアクセスし、同LAN上のPCにマルウェアを撒き散らすチップが埋め込まれていることが発見された。
- 同様のものがモバイルフォンや車載カメラでも見つかった模様。
- 出荷を停止したが、既に小売店に出荷されたものもあるとのこと。



(CCDSSG事務局作成)

2014 copyright (c) CCDSSG, Proprietary

2.2.1 脅威の事例

標的型攻撃メールによる設計情報漏えいの脅威

分　類	実例	分野	企業一般	時期	2005以降	地域	各国

情報源

IPA「標的型メール攻撃』対策に向けたシステム設計ガイド」 http://www.ipa.go.jp/security/vuln/newattack.html
JAXAプレスリリース　http://www.jaxa.jp/press/2012/03/20120327_security_j.html

脅威

特定の対象に知人を装うマルウェア付きメールにより、設計情報などが情報が漏えい

概要

- 不特定多数にマルウェアを撒く攻撃と異なり、特定の対象を狙ったメール攻撃。
- 設計情報やソースコード、バグデータベースなどの漏えい事例あり。近年ではロケット開発機関が攻撃され、マルウェアに感染しており、情報が漏えいした可能性がある。
- IPAの標的型攻撃メール対策の調査報告書のpdfにマルウェアを仕込み、IPA担当者名で政府関係組織に送付した事例もある。

実際に発生した事例

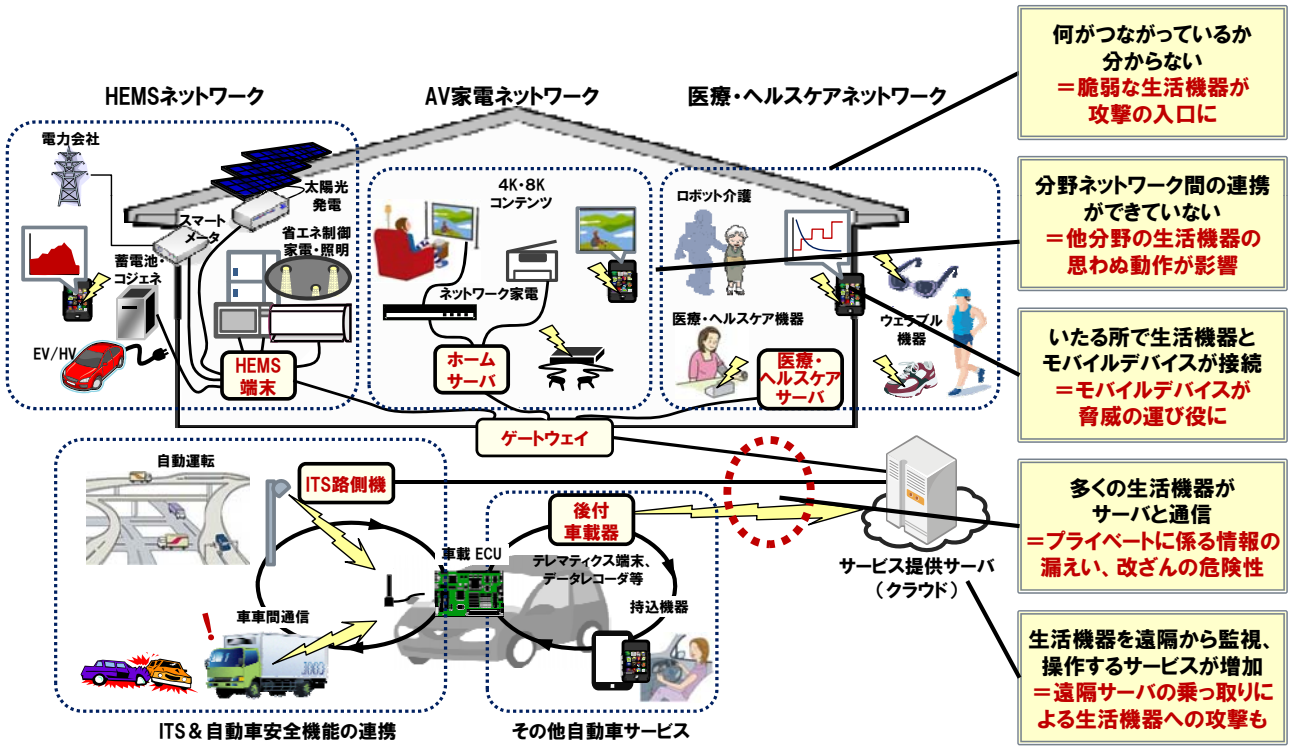
(IPA資料(http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf)を参考にCCDSSG事務局作成)

2014 copyright (c) CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

CCDSSG

■ 現状の脅威が「つながる」世界でさらに拡大、深刻化すると想定される。



2014 copyright (c) CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

CCDSSG

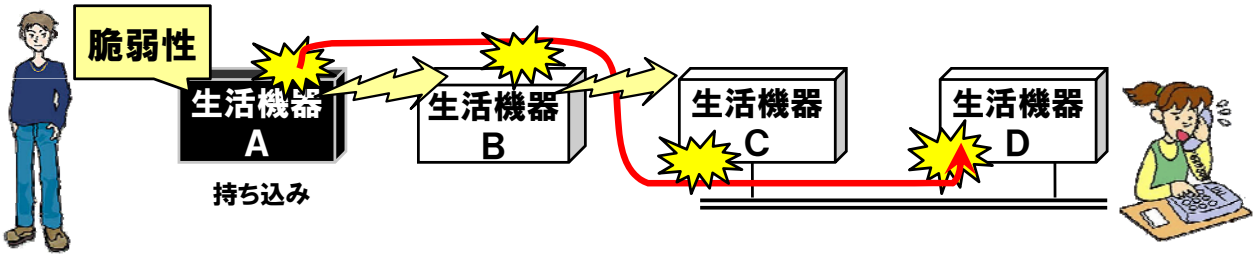
● 想定される状況(その1)

■ いま何がつながっているか、これから何がつながるか、分からない

● 想定される脅威(例)

■ 子供が脆弱性のある中古家電を持ち込み、家庭にウイルス感染

- 何が起きたのか、何が原因か、ユーザには分からない



● 解決すべき課題

■ 個々の生活機器のセキュリティ機能の強化、中小企業への支援

■ 連携セキュリティ技術・フレームワークの開発

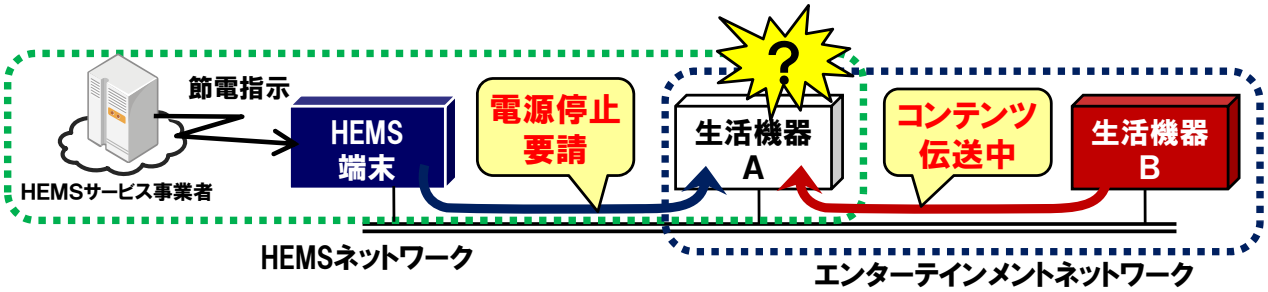
■ 連携時の攻撃被害に対する責任分界の取り決め

■ ユーザへの「つなげるリスク」の教育　など

2014 copyright (c) CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

- 想定される状況（その2）
  - 異なる分野のネットワークが意図せず、つながる
- 想定される脅威（例）
  - 他分野の生活機器の思わぬ動作がサービスに影響

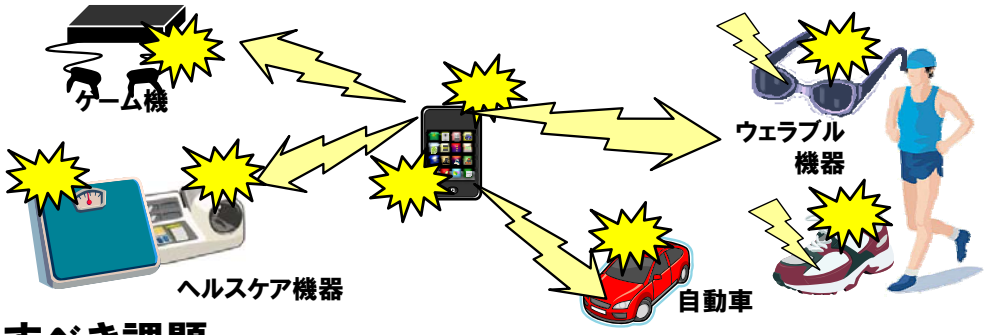


- 解決すべき課題
  - 各分野（業界）におけるセキュリティ検討、セキュリティ標準の策定
  - 分野ネットワーク間のセキュリティ連携策の検討
  - 各分野（業界）間のセキュリティ対応の格差の是正　など

2014 copyright （c） CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

- 想定される状況（その3）
  - いたる所で生活機器とモバイルデバイスが接続
- 想定される脅威（例）
  - モバイルデバイスがウイルスなどの脅威の運び役に

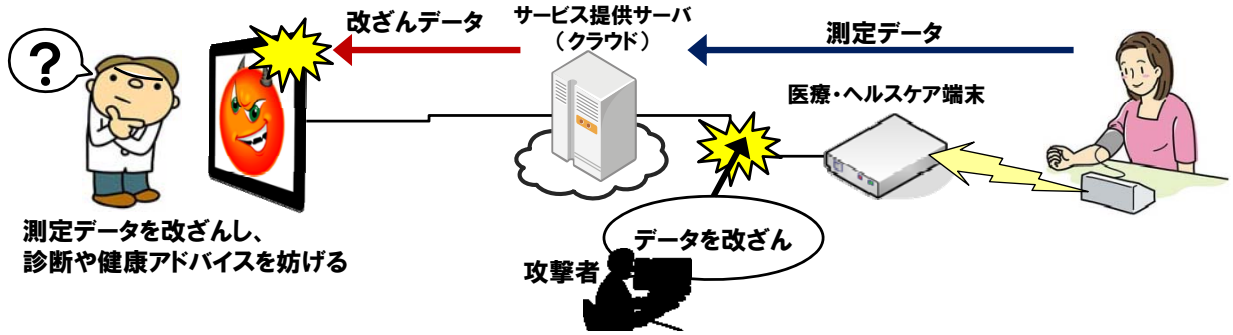


- 解決すべき課題
  - 通信業界におけるモバイルデバイスのセキュリティ強化
  - 生活機器とモバイルデバイスの連携セキュリティの検討
  - 生活機器やモバイルデバイスへの攻撃に対する規制や罰則の強化　など

2014 copyright （c） CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

- 想定される状況(その4)
  - 多くの生活機器がサーバと通信
- 想定される脅威(例)
  - 攻撃による通信停止、情報漏えい・改ざんなど

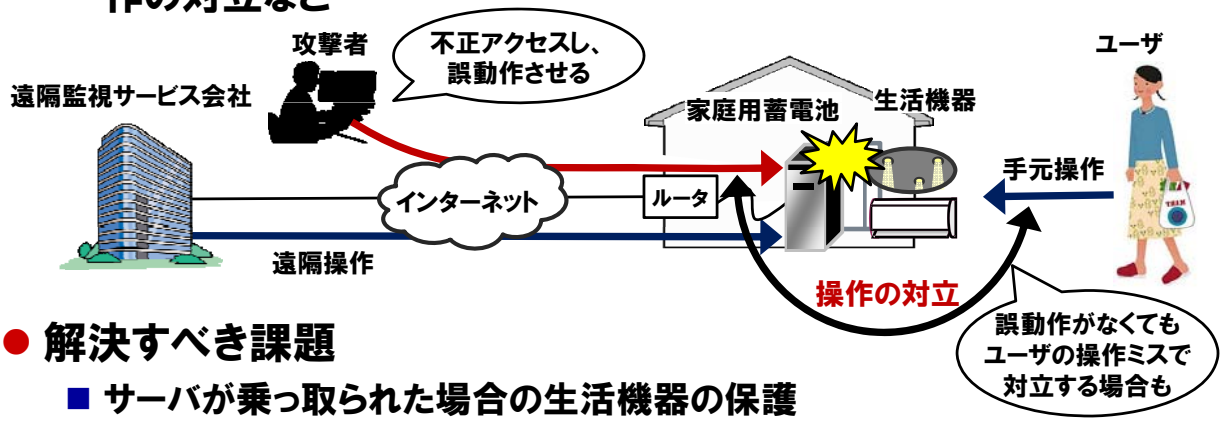


- 解決すべき課題
  - 攻撃による通信停止や情報漏えい・改ざんなどへの対応検討
  - ユーザへの生活機器のネットワーク接続のリスクの周知　など

2014 copyright (c) CCDSSG, Proprietary

2.2.2 2020年における脅威の想定

- 想定される状況(その5)
  - 生活機器を遠隔から監視、操作するサービスが増加
- 想定される脅威(例)
  - 遠隔サーバの乗っ取りによる生活機器の攻撃、遠隔操作と手元操作の対立など



- 解決すべき課題
  - サーバが乗っ取られた場合の生活機器の保護
  - 遠隔操作と手元操作の対立時の適切な対応
  - ユーザへの生活機器のネットワーク接続のリスクの周知　など

2014 copyright (c) CCDSSG, Proprietary

2.3 2020年までに解決すべき課題の整理

CCDSSG

- 想定される脅威に対して検討すべき課題を以下に示す。

1）業界領域

- 業界におけるセキュリティ検討の場が未整備
- 業界における連携セキュリティ対策が未検討
- 業界のセキュリティ標準、評価検証制度が未整備

2）企業領域

機器メーカ	サービス提供者	通信事業者
セキュリティの責任分界が不明確		
セキュリティ開発技術が不十分	セキュリティ運用体制が不十分	モバイルデバイスと生活機器連携におけるセキュリティ対策が不十分
出荷後のセキュリティ対応が不十分		

3）ユーザ領域

- 何がつながっているか分からない つなげると何が起こるかが分からない
- セキュリティリテラシーや意識が不十分 脅威に対する過剰な反応も
- セキュリティ対策のコスト意識が低い

4）業界横断的領域

- 業界横断的なセキュリティ連携が未整備
- 連携時のセキュリティレベル評価スキームがない
- 業界間での脆弱性やインシデント情報の共有の仕組みが未整備
- 業界間におけるセキュリティ対策の格差を解消する仕組みがない

5）行政領域

- 法制度による規制や罰則が不十分
- セキュリティ技術開発の支援策が不十分
- 家庭や中小企業のセキュリティ導入支援策が不十分
- 想定される脅威の周知が不十分

2014 copyright (c) CCDSSG, Proprietary

3. 解決に向けたアプローチ

CCDSSG

- 3.1 検討スコープ
  - 各課題に対する検討事項を以下に示す。

3.2.1 業界における検討事項

- 業界におけるセキュリティ検討の場の設置
- 業界共通の連携セキュリティ対策の検討
- 業界セキュリティ標準の策定及び認証制度の制定

3.2.2 企業における検討事項

機器メーカ	サービス提供者	通信事業者
セキュアな製品開発	セキュアな運用体制	セキュアなモバイルデバイス
セキュリティ人材育成	セキュリティ人材育成	セキュリティ人材育成

3.2.3 ユーザに対する検討事項

- ユーザに対するセキュリティ情報・レベルの表示
- ユーザのセキュリティリテラシー向上策の検討
- U/Iを通じたセキュリティ意識向上手法の検討
- ユーザとのセキュリティ対応負担のコンセンサス

3.2.4 業界横断的な検討事項

- 業界横断的な連携セキュリティの場の設置
- 業界共通・横断的な連携セキュリティ技術の開発
- 連携時のセキュリティレベルの評価スキームの検討
- 連携機器間の信頼性の確認基盤技術の検討
- 開発現場のセキュリティ技術者の育成支援

3.2.5 行政における検討事項

- 生活機器連携サービスに求められる法制度整備の検討
- 業界共通・横断的な生活機器連携セキュリティ技術の開発支援
- インシデント予防／早期発見・早期対策の仕組みの検討
- 高度セキュリティ人材、開発現場のセキュリティ技術者の育成支援
- 中小企業やユーザにおけるセキュリティ対策の導入支援
- ユーザの緊急相談窓口の設置

2014 copyright (c) CCDSSG, Proprietary

3.2 各領域における検討事項

● 3.2.1 業界における検討事項

生活機器のセキュリティに関して、業界に期待する検討事項を示す。

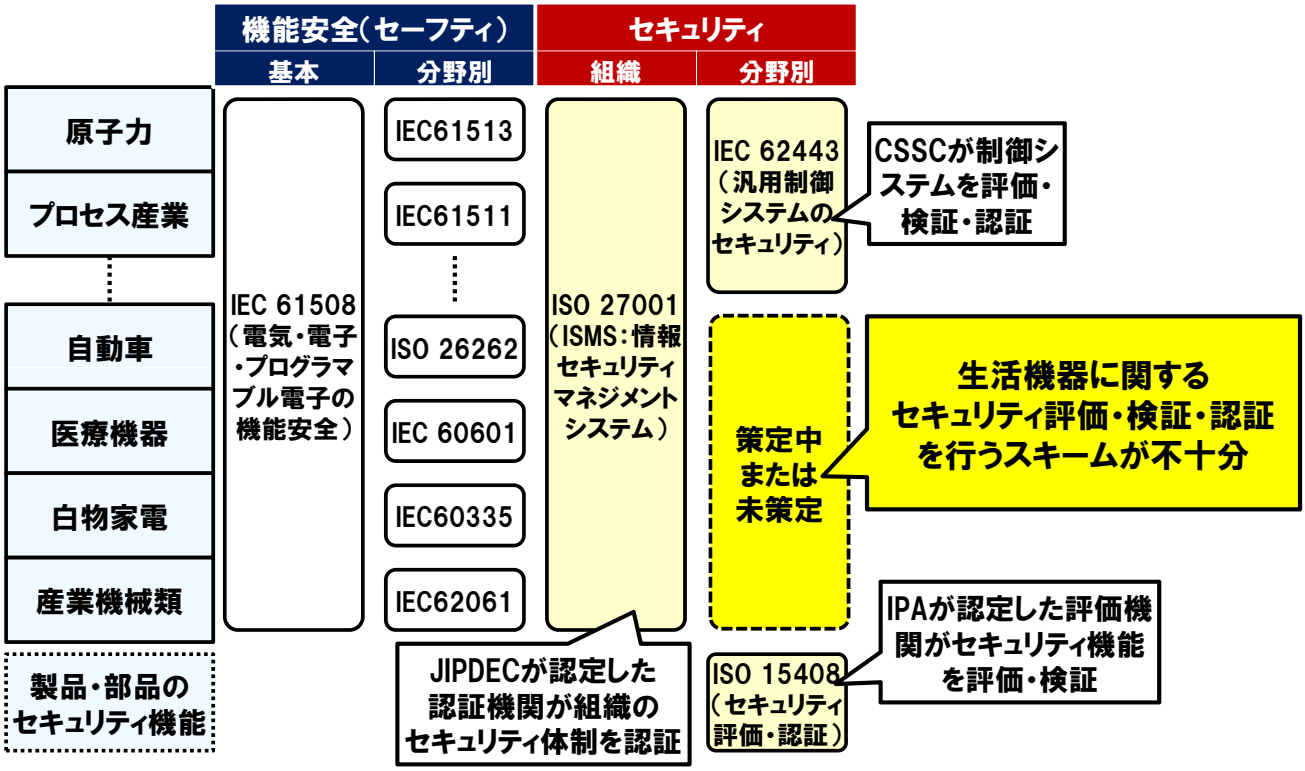
① 業界におけるセキュリティ検討の場の設置
- 業界の中で、セキュリティについて共同で検討する場を設ける。
- これにより業界としてセキュリティ対策の底上げを図り、ユーザの信頼を得る。

② 業界共通の連携セキュリティ対策の検討
- 上記の場において、業界共通のセキュリティ対策を検討する。
- （例）
  - 業界をまたがるインシデント情報の共有と分析体制基盤のあり方の検討
  - 他機器との連携も踏まえたリスク分析手法（業界版CVSSなど）
  - メーカ、サービス提供者、通信事業者の責任分界モデル
  - デバイス／サービスレベルでのセキュリティ機能評価　etc.

③ 業界セキュリティ標準の策定及び評価認証制度の制定
- 業界におけるセキュリティ標準を策定する。また、製品が標準に準拠していることを評価認証する制度を制定する。

2014 copyright (c) CCDSSG, Proprietary

参考）生活機器のセキュリティ標準策定状況



CSSC:技術研究組合制御システムセキュリティセンター、IPA：独立行政法人情報処理推進機構、JIPDEC一般財団法人日本情報経済社会推進協会

2014 copyright (c) CCDSSG, Proprietary

3.2 各領域における検討事項

- 3.2.2 企業における検討事項

生活機器のセキュリティに関して、企業に期待する検討事項を示す。

① 他社や他業界製品との連携を考慮したセキュアな製品開発
- 個々の企業が他の生活機器との連携を考慮したセキュアな製品開発を行う。

② 他のサービスとの意図せぬ接続も考慮したセキュアな運用体制
- 機器連携により想定外の問題が発生した場合に、ユーザからの問い合わせ対応から問題発見、事後対応までの一連の運用体制を検討する。

③ 生活機器との連携を考慮したセキュアなモバイルデバイス
- 通信事業者においても、生活機器との連携を想定し、セキュアなモバイルデバイスを開発する。

④ 国や業界団体の支援を活用したセキュリティ人材育成
- 上記の検討や実行において必要となるセキュリティ人材を、国や業界団体が育成支援策を活用して実施する。

2014 copyright (c) CCDSSG, Proprietary

3.2 各領域における検討事項

- 3.2.3 ユーザに対する検討事項

生活機器のセキュリティ検討のうち、ユーザに関する事項を示す。

① ユーザに対するセキュリティ情報・レベルの表示
- 機器のセキュリティレベル、ステータス、連携の有無などを業界・業界間共通の形式で生活機器のインタフェースに表示する仕組みを検討する。

② ユーザのセキュリティリテラシー向上策の検討
- ユーザに対して、生活機器をつなぐリスク、守るべき利用エチケット、予期せぬ動作に対する冷静な判断や対応などを周知するためのコンテンツを検討する。

③ ユーザインタフェースを通じたセキュリティ意識向上手法の検討
- 生活機器の接続時や不用意な操作に対して、生活機器のインタフェースで注意を促し、ユーザのセキュリティ意識を向上させる手法を検討する。

④ ユーザとのセキュリティ対応負担のコンセンサス
- つながる時代の生活機器のセキュリティ対策のために、ユーザも「時間」、「手間」、「コスト」を負担する必要があることを理解いただく。

2014 copyright (c) CCDSSG, Proprietary

3.2 各領域における検討事項

CCDSSG

● 3.2.4 業界横断的な検討事項

生活機器のセキュリティに関して業界横断的に検討すべき事項を示す。

① 業界横断的な連携セキュリティの場の設置
- 関連する業界組織とのリエゾン関係を構築する。また、業界共通のインシデント情報の共有ルールを検討する。

② 業界共通・横断的な連携セキュリティ技術の開発
- 新旧製品の混在にも対応できるセキュリティ基盤の開発を検討する。また、プライバシー保護、インシデント時のログ・証跡保存等の技術開発を検討する。

③ 連携時のセキュリティレベルの評価スキームの検討
- 異なる業界の機器連携時のトータルでのセキュリティレベル及びリスクを評価するスキームを検討する。

④ 連携機器間の信頼性の確認基盤技術の検討
- 異なる業界の機器が一時的に連携する場合でも、相互の信頼性レベルを自動的に確認できる基盤技術を開発する。

⑤ 開発現場のセキュリティ技術者の育成支援
- 国や自治体の支援策、学術系との連携（emPiT）などにより、セキュリティ技術者の育成支援を業界を超えて推進する。

2014 copyright (c) CCDSSG, Proprietary

3.2 各領域における検討事項

CCDSSG

● 3.2.5 行政における検討事項

生活機器のセキュリティに関して、行政に期待する検討事項を示す。

① 生活機器連携サービスに求められる法制度整備の検討
- 生活機器の連携セキュリティに関し、法制度の整備を検討する。
- （例）
  - 連携サービスにおけるプライバシー保護
  - 被害の認定や責任の明確化、PL法・電気製品安全法等との関係整理
  - ログ証跡記録義務　など

② 業界共通・横断的な生活機器連携セキュリティ技術の開発支援
- 生活機器連携のセキュリティ評価パイロットプロジェクトなどを検討する。

③ 高度セキュリティ人材、開発現場のセキュリティ技術者の育成支援
- ハッキング技術を有する高度なセキュリティ人材の育成、開発現場の技術者のセキュリティスキル向上策などを検討する。

④ 中小企業やユーザにおけるセキュリティ対策の導入支援
- 中小企業や一般の消費者に対して、セキュリティの知識や対策ツールの導入を促進する。

2014 copyright (c) CCDSSG, Proprietary

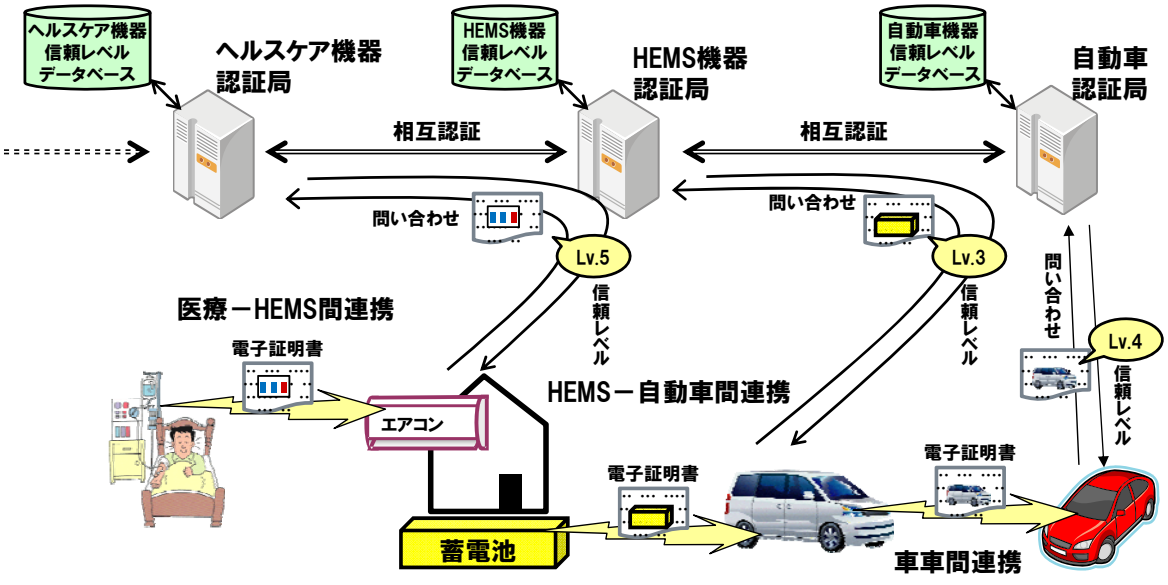
3.2 各領域における検討事項

- 3.2.5 **行政**における検討事項（つづき）
  - ⑤ インシデント予防／早期発見・早期対策の仕組みの検討
    - 次の検討により、セキュリティ対策を効率的・効果的に推進する。
    - （例）
      - セキュリティ攻撃予報の発信・共有（観測所の整備）
      - 証拠保全ルール、捜査権等、制度検討
      - トレーサビリティによる原因分析と早期対策、拡散防止策の検討
  - ⑥ ユーザの緊急相談窓口の設置
    - インシデント119番による緊急対応窓口の設置、通報ユーザに対する対策レクチャーや二次被害防止を可能とする仕組みを検討する。

2014 copyright (c) CCDSSG, Proprietary

3.3 生活機器ユースシーンと課題解決（例）

- 1）機器・サービス間の「信頼レベル」交換による連携相手の評価
  - 相手の信頼性に基づいて、連携の可否やレベルを自動的に判断
    - 他業界の信頼レベルをどのように評価するかは課題



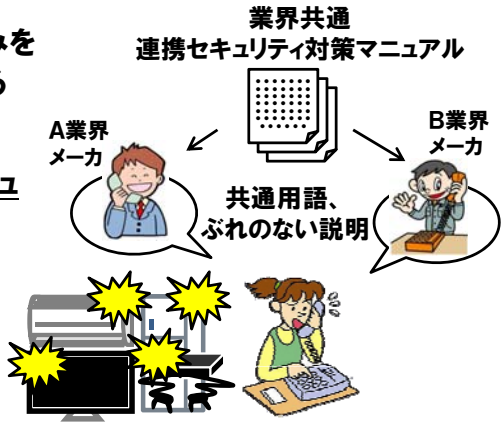
※車車間の図は、業界で検討されている仕組みより簡素化している。

2014 copyright (c) CCDSSG, Proprietary

3.3 生活機器ユースシーンと課題解決(例)

CCDSSG

- 2) 業界・業界間連携によるユーザ対応の共通化
  - セキュリティ用語の共通化
    - 連携時のトラブルにおいて、どの業界のサポートに連絡しても同じ用語で説明することで、ユーザの混乱をなくす
  - ユーザ説明方法の共同考案
    - 例えば「脆弱性」について、「最新の鍵もやがて開けられてしまうように、生活機器も万全ではない」といった適切な理解を促す説明を共同で考案・共有する
  - 「つながる安心」のアピール
    - つながることでセキュリティを確保する仕組みを共同で開発、「つながる安心」をアピールする
  - セキュリティの商品価値の創出
    - 「つながる時代」を支える、「一歩進んだセキュリティ」の商品価値を共同でアピールする
  - ユーザインタフェース(UI)の活用
    - 生活機器のUIを活用し、共通的な形式で機器の状態やセキュリティ情報を提供する

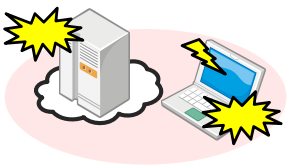


2014 copyright (c) CCDSSG, Proprietary

3.4 2020年に向けた取り組みのイメージ

CCDSSG

現状の脅威
サーバやPCへの攻撃



2020年の脅威
生活機器がネットワーク連携することで脅威が拡大

何がつながっているか、何が起こっているかが、分からない

今からセキュリティ対策を開始することが必要

業界団体
・業界共通対策の検討、セキュリティ標準・認証スキーム策定等

検討成果の提供

企業
・セキュアな開発・運用体制、人材育成等

業界連携

業界横断
・業界横断的な検討の場の設置、機器間の信頼性確認基盤検討等

製品提供・サポート

ユーザ
・セキュリティリテラシー・意識の向上
・ユーザへの共通的なセキュリティ情報提供

啓発・支援

行政
・セキュリティ技術開発、人材育成等の支援、
・ユーザの意識啓発、セキュリティ119番等

重要生活機器連携セキュリティ研究会(CCDSSG)
・連携セキュリティの研究成果の発信
・業界間連携の場の設立支援、協力
・2020年においても安全安心な生活の実現をサポート

Safety & Security

2014 copyright (c) CCDSSG, Proprietary

4. 提言

研究会では、セキュアな社会の実現に向け、次のとおり提言する。

- １)つながる生活機器のセキュリティに目を向けよう
  - ユーザやサービス事業者が、HEMS、AV家電、医療・ヘルスケア、自動車等の生活機器同士やスマートフォン、モバイルデバイスを自由に連携させて利用するシーンを想定し、生活機器のセキュリティを検討する必要がある。
- ２)ユーザを巻き込んだセキュリティ対策を考えよう
  - 家庭内の多種多様で世代も異なる機器同士の連携におけるセキュリティを実現するためには、ユーザを巻き込んだ対策が必要であり、コンテンツを活用したユーザのリテラシー向上、生活機器のユーザインタフェースを活用した機器のセキュリティレベルや状態の通知、セキュリティ119番の設置による早期把握・対策などを図る必要がある。
- ３)業界横断的な検討の場を設けよう
  - 異なる業界、異なる国の生活機器同士が連携することを考慮し、業界横断的なセキュリティ対策を検討する場を設置、共同で対策技術を開発したりセキュリティ用語の統一を図ったりすることにより効率的・効果的にセキュリティの実現を図る必要がある。

2014 copyright (c) CCDSSG, Proprietary

4. 提言(つづき)

- ４)世界の安心・安全に貢献しよう
  - 各業界における共通のセキュリティ対策やガイドラインの検討を進めるとともに、国際標準及び評価検証制度の制定を進める必要がある。
- ５)世界に誇れるセキュアなものづくりを進めよう
  - 標準やガイドラインを基に、企業が企画段階から製品にセキュリティを組み込んでいくことや、ソフトウェア開発工程のサプライチェーンにおいてセキュリティを考慮することが必要である。

2014 copyright (c) CCDSSG, Proprietary

参考）研究会メンバー

- 会長
  慶應義塾大学環境情報学部教授 兼 大学院政策・メディア研究科委員長 徳田 英幸
- 幹事
  名古屋大学 高田 広章教授、横浜国立大学 松本 勉教授、一般社団法人IIOT 南郷 辰洋副理事、一般社団法人スキルマネージメント協会 田丸 喜一郎理事、株式会社ユビテック 荻野 司代表取締役社長
- 会員（大学）:
  情報セキュリティ大学院大学 後藤 厚宏情報セキュリティ研究科長 、大久保 隆夫教授、佐藤 直教授、名古屋大学 高倉 弘喜教授、広島市立大学 井上 博之准教授
- 会員（以下企業・団体に属する技術者、コンサルタントなど）:
  イーソル株式会社、イータス株式会社、株式会社エイチアイ、インターネットITS協議会、株式会社ヴィッツ、オムロンソフトウェア株式会社、ガイオ・テクノロジー株式会社、株式会社カスペルスキー、キャッツ株式会社、国際公共政策研究センター、ソシオメディア株式会社、ソニーデジタルネットワークアプリケーションズ株式会社、株式会社デンソー、株式会社東芝、東芝ソリューション株式会社、株式会社豊通エレクトロニクス、トレンドマイクロ株式会社、日本電気株式会社、パナソニックアドバンストテクノロジー株式会社、株式会社日立製作所、株式会社U‘eyes Design、株式会社ユビテック（研究会事務局）
- オブザーバー：独立行政法人情報処理推進機構（IPA）、他

2014 copyright (c) CCDSSG, Proprietary

お問い合わせ先

- 重要生活機器連携セキュリティ研究会事務局
  - 株式会社ユビテック　ユビキタス研究所　伊藤、遠山
  - 〒141-0031 東京都品川区西五反田1-18-9 五反田NTビル 6F
  - TEL：03-5487-5590　E-MAIL: ccdssg-sec@ubiteq.co.jp
  - 研究会Webサイト: https://www.ccdssg.org/

2014 copyright (c) CCDSSG, Proprietary