

パネルディスカッション

IoTとAIの活用が当たり前になる時代において、守るべき情報は守れるのか？

2019年12月20日

パネルディスカッションのメンバー



パネリスト

国立研究開発法人 情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室 室長

井上 大介 氏

オムロン株式会社 コントローラ事業部 コントローラPMG 主査

岡 実 氏

一般社団法人 重要生活機器連携セキュリティ協議会(CCDS)ストラテジックアドバイザー
／株式会社JVCケンウッド PSIRTリーダー

伊藤 公祐 氏

モデレーター

NPO日本ネットワークセキュリティ協会 IoTセキュリティWG

武田一城

IoTとAIが当たり前になる時代のセキュリティはどうなるのか？

IoTは、新たなビジネス、知識、価値、サービス等の創出が期待され、すでに本格的な普及期に入っていると言って良いと思われます。IDCJapanによると、IoT市場は2018年にすでに6兆3,167億円であり、その後5年間の年平均成長率は13.3%であり、2023年には11兆7,915億円に達すると言われています。

このような巨大な市場となる頃には、深層学習（DeepLearning）や高度なデータアナリティクス技術、そして高度に成長しつつあるAI技術を組み合わせる事によって、様々な新しい価値が生まれてくることでしょう。

このように、IoTやAIによってこれまでとは比べ物にならないくらい膨大な情報量と高度な活用技術が駆使されるようになります。IoTとAIが当たり前になる時代に、どのようにセキュリティ対策を考えていただくヒントになればと、JNSA/IoTセキュリティWGとして本セミナーを企画いたしました。



IT革命とかの時に言われていたことが実現しつつあり…、IoTやAIもそのピースのひとつ

本格的にIT主導の世界が実現する

それを、別の言葉で言うと…

Society5.0

デジタルトランスフォーメーション

とかになるんだろうと思っています。



粉飾決算のイラスト

ただし、そういう素敵な
将来の裏側って、
結構こんな感じだったり
することも多いです。

ほとんどの人にとって、お金儲け
(日々の糧)が重要なのは当然です。
ただし、ルールが整備されていない
事で色々な問題が生じます。



金づるのイラスト

なので、IoTやAIが
本気を出す前に
セキュリティの課題
も議論しておきたい

本日、聴いて頂いた講演



IoTとセキュリティと、時々、機械学習 ～NICTにおけるIoTセキュリティと機械学習応用の取り組み～

IoTセキュリティの国際動向 ～法規制やサートیفिकーションはどうなる？～

産業分野のIoT導入事例

ここで・・・

パネルディスカッションに
先立ち、今年初めに会った
IoTセキュリティ界隈で
起きた事件をご説明します

※落語などの本題前にある「枕」みたいなお話です。

今年初めの平成の末期に、
こんなことがありました。



これの
ちょっと
前あたり…

NOTICE

National Operation Towards IoT Clean Environment

ABOUT NOTICE

NOTICEについて



NOTICEは、総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組です。

総務省とNICTが、「脆弱な機器を放置するとサイバー攻撃に悪用される」のを防ぐために調査と注意喚起を行うと発表しました。



これを受けて
NHKさんが
こんな報道を
されました



世界的にも異例

POWER

ACTIVE

“ネット機器”に国が無差別侵入？

な調査が来月から始まります。

>>これ、..TV

サイバー攻撃対策 調査に懸念も



IoT機器に“無差別侵入”
国が異例の調査 実施へ

>>今回の調査では、

他人のIoT機器に
ID・パスワード入力

不正アクセスと
実質 変わらず



IoT機器に“無差別侵入”
国が異例の調査 実施へ

“特例的に5年間に限り実施”

侵入行為 不正アクセス禁止法で禁止



IoT機器に“無差別侵入”
専門家からは懸念の声も

情報セキュリティ大学院大学
湯浅 壱道 教授

通信の相手先まで分かってしまうとなると
「通信の秘密」の侵害ではないかとの議論出てくる

報道を素直に
信じると、こ
んな感じです



市民の携帯電話を
覗く警察官のイラスト

つまり

国家権力怖い!



A close-up photograph of a hand holding a red pen, pointing at a newspaper article. A red circle is drawn around a specific word in the text. The background is a blurred newspaper page with Japanese text.

メディアの論調の鵜呑みは非常に危険なので、

**もう少し報道の内容
を調べてみました。**

まず...

すでにNHKさんのサイトでは
肝心の記事は削除されていました。
(twitterのみ残っています)

NHK NEWS WEB

ニュースを検索

検索

文字サイズ 小 中 大

ニュース

動画

News Up

特集

スペシャルコンテンツ

NEWS WEB EASY

記事が見つかりませんでした

▶ [NHK NEWS WEBトップへ](#)

<https://www3.nhk.or.jp/news/html/20190125/k10011791591000.html>

大人の事情が
あったんだと
思います。





ニュースウォッチ9

@nhk_nw9

フォローする



全国の家庭や企業にあるインターネット家電などいわゆる #IoT機器 に国が無差別に侵入を試みる。そんな世界でも例のない調査が来月から始まります。#サイバー攻撃 対策の一環ということですが、実質的に不正アクセスと変わらない行為を特例的に国が行うことに懸念の声もあがっています。 #nhk #NW9



19:09 - 2019年1月25日

プライバシーの侵害につながる危険性

侵入時点でウェブカメラの映像が見えてしまったり、保持データの中身がわかってしまったりすることもある...

実質的に不正アクセスと変わらない行為

そして、極めつけは！

憲法違反？

通信先がわかってしまえば憲法で定めた『通信の秘密』
に抵触するおそれも…という専門家の意見が報道された。



なんて悪い
奴なんだ！

この報道内容が
正しいければ……



ちなみに、これは
誤報のイラストです。

NHKさんの
大スクープ
だと思います。



でも

(個人的な感想は)



井上さん(笑)



誤爆のイラスト

むしろ、こんな感
じなんじゃないか
と思っ...つい。

こんな記事を寄稿しちゃいました・・・。

企業セキュリティの歩き方



総務省のIoT機器調査は「監視社会」の始まりか--議論が起きた理由

武田一城 (ラック) 2019年02月15日 05時30分

いいね! 60 ツイート B! 19 Pocket 60

印刷 メール▼ ダウンロード▼ クリップ

PR ITの複雑化にバックアップが追いついていない・・・？ならArcserve UDP 8000シリーズ！

PR グループウェア軸に社内環境の向上--「4要素のうまい管理」とは

PR テレワーク導入企業の労働生産性はそうでない企業の1.6倍に

PR 【生産性向上--IT運用編】理想からかけ離れた現状に満足ですか？改革を起すなら今！

本連載「[企業セキュリティの歩き方](#)」では、セキュリティ業界を取り巻く現状や問題、問題点をひもときながら、サイバーセキュリティを向上させていくための視点やヒントを提示する。

政府がサイバー攻撃対策の一環として、国内のIoT機器に対して簡単なパスワード（脆弱なパスワード）が用いられていないかを調査し、ユーザーに注意喚起することを発表した。それを受けて「『通信の秘密に抵触の恐れ』無差別侵入し調査へ」といったメディアの報道があり、「総務省自身が不正アクセス禁止法や憲法にも記載されている通信の秘密を侵害するのか？」などという意見が多数噴出し、物議を醸している。この報道のタイトルや概要だけを聞くと、一般の人々は政府が家庭のIoT機器ハッキングし、その行動を監視する統制国家になるのかという印象を受けてもおかしくないと思われる。今回は、政府の行動や報道が何を意図し、どのような意味があるのかについて述べていきたい。

IoT機器への“無差別”侵入調査

総務省の取り組みは、IoT機器などを悪用（例えば他のサーバへの攻撃の踏み台などに不正利用）するサイバー攻撃のリスクの高まりや深刻化という状況を踏まえた調

1

総務省のIoT機器調査は「監視社会」の始まりか ～議論が起きた理由～

2

IoT機器侵入調査は本当に「通信の秘密を侵害し、検閲に当たる」のか？

3

IoT機器調査を担うNICTは諜報機関か？
～実施する技術的な理由～

ステマをするアイドルのイラスト



という宣伝もしながら、
そろそろ本題です。

パネル ディスカッション

七つのお題を
用意しました



1

IoTセキュリティは 今のままで大丈夫か？

(または、NOTICEは適切な対策だったか？)

2

そもそも、何を守れば
IoTを守れたことになるの？

(端末なのか？ネットワークなのか？情報なのか？)

③

産業界ってIoTで 儲かっていますか？

(儲かる理由 or 儲からない理由)

会場からのご意見あれば！

4

海外のIoTセキュリティって うまくいっていますか？

(そもそもIoTは普及していますか？セキュアな状態なの？)

またガラパゴス
にされてない？

5

AIは、この世の中の 何を変えるのか？

(もしくは、より端的にAIはIoTより儲かりますか？)

6

AIの進化の先に 懸念はありますか？

(シンギュラリティ、その他の懸念は？)

7

IoTとAIの活用が当たり前になる時代においても、守るべき情報は守れると思いますか？

これで最後のお題なので
できれば、どなたか
うまく纏めてください

まとめ



ケーブルをまとめる人のイラスト

AIとの付き合い方の 色々なパターン

AIに支配される
人のイラスト



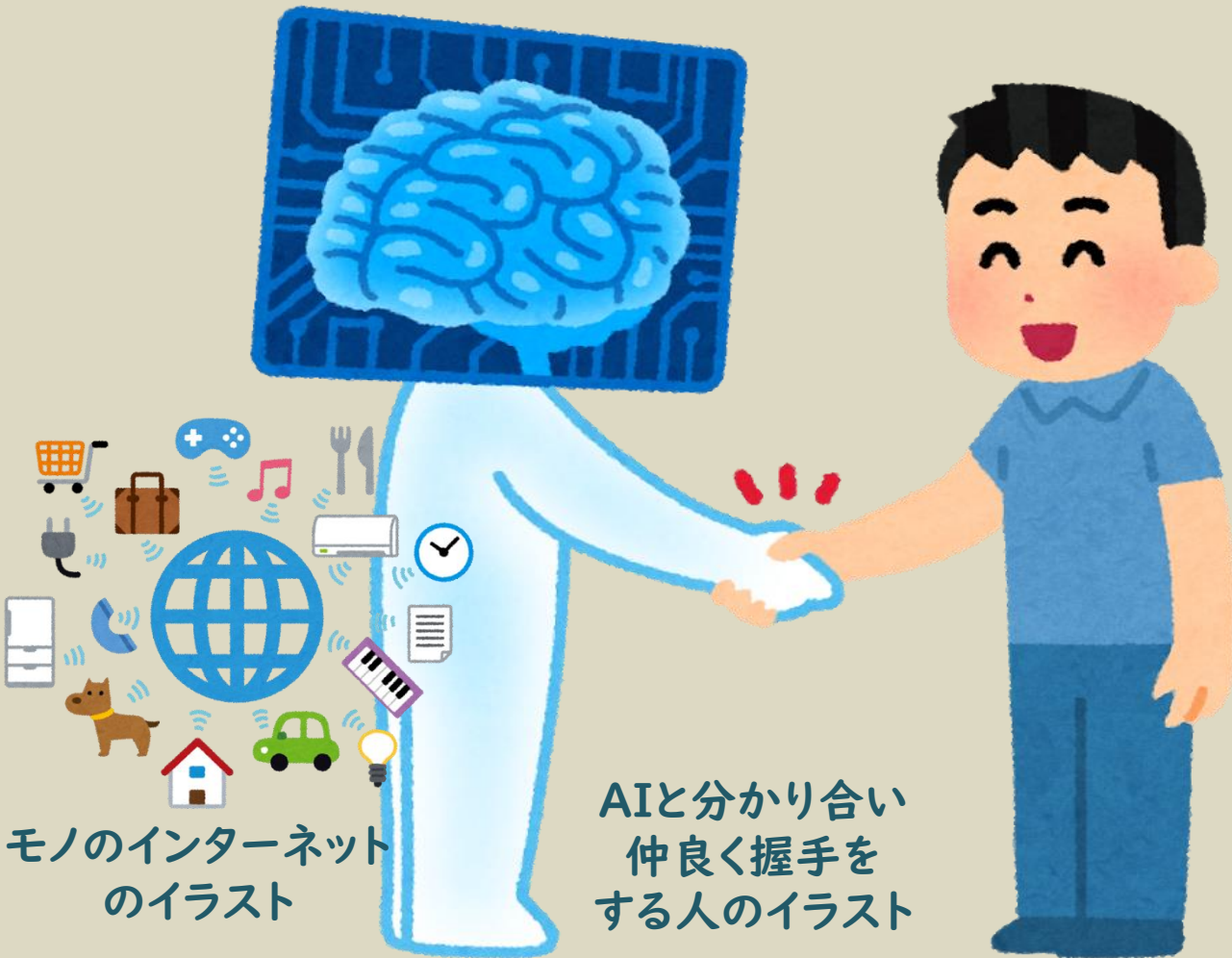
人工知能に仕事を
任せる人のイラスト



仕事を奪うAIのイラスト



IoTやAIは、まだまだ課題が多い分野かもしれませんが、うまく付き合う方法ができれば、人間が幸せになるための良い友達になれると思います。



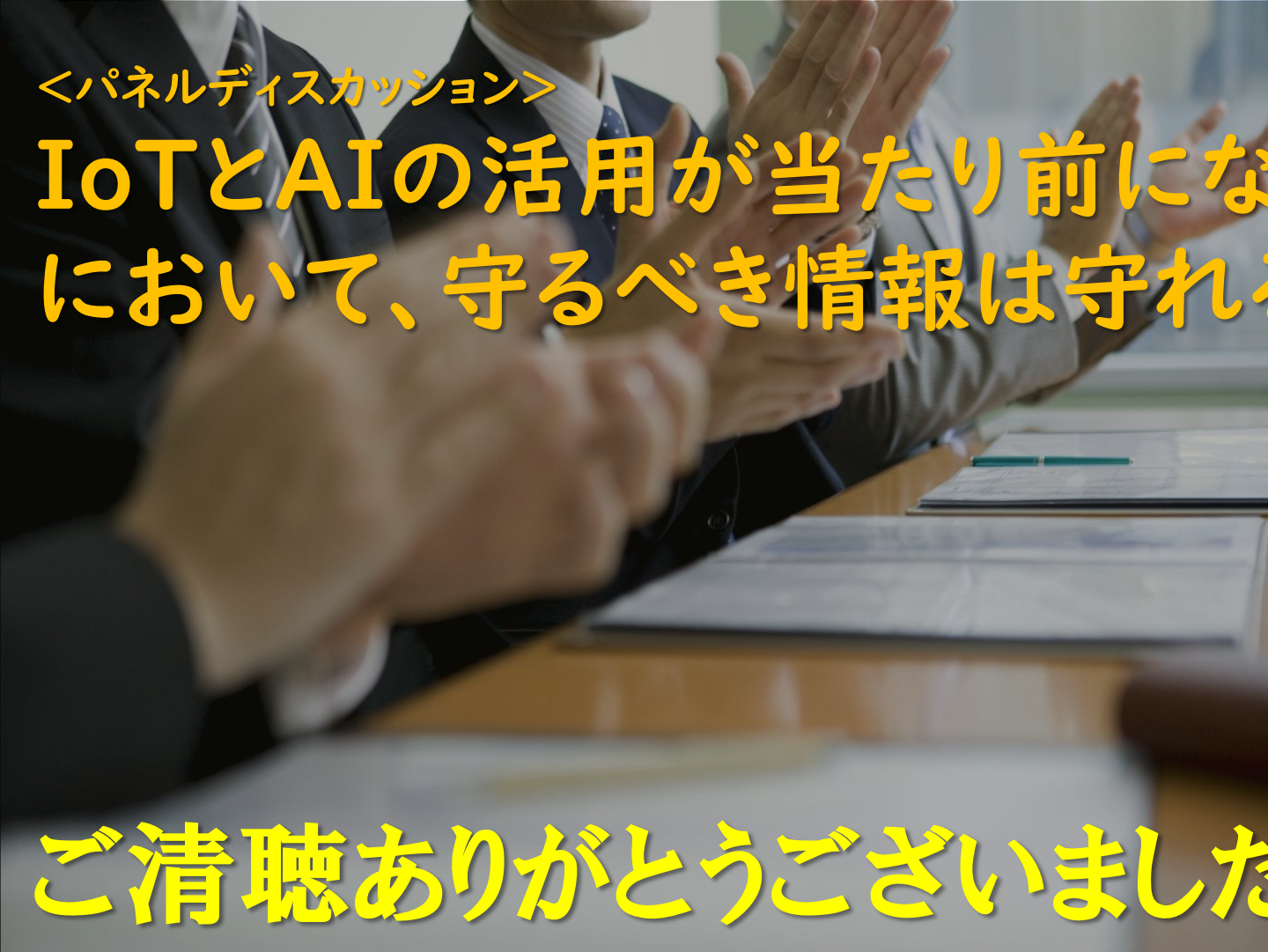
モノのインターネット
のイラスト

AIと分かり合い
仲良く握手を
する人のイラスト

そのために重要なのが
IoTとAIのセキュリティ
なのだと思います！

いい感じにまとまりました！（たぶん）





<パネルディスカッション>

IoTとAIの活用が当たり前になる時代
において、守るべき情報は守れるのか？

ご清聴ありがとうございました。

「いらすとや」って
ホントに凄い！