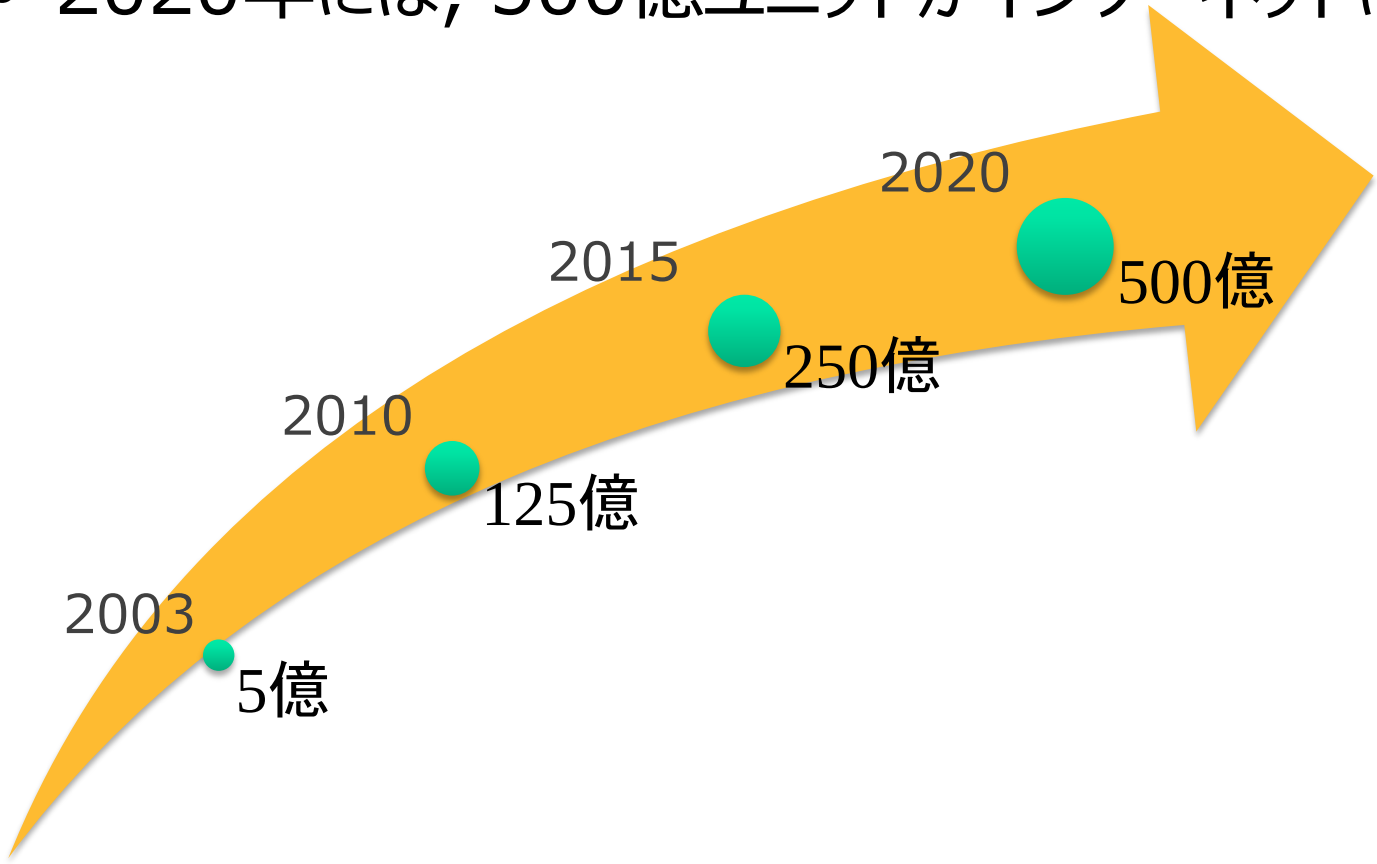
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IoTのセキュリティ脅威と今後の動向

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
株式会社シマンテック セキュリティソリューションSE部
兜森　清忠

2020年までにIoTデバイス数は500億超

- 人口70億人、90億ユニットのデバイス
- 2020年には, 500億ユニットがインターネットに接続



産業別のIoT利用形態

自動車
- Telematics
- In-vehicle entertainment
- Navigation
- Safety services
- Concierge services
- Remote diagnostics
- Personalized insurance

産業
- Supply chain management
- Geo-fencing
- Machine diagnostics
- Inventory control
- Industrial automation control
- Equipment monitoring

商取引＆ファイナンス
- Smart payments, cards
- Point of sale terminals
- ATM
- Vending machine monitoring
- Digital signage and electronic billboards

ヘルスケア
- Home healthcare and hospital patient monitoring
- Remote telemedicine & physician consultation
- Body sensor monitoring

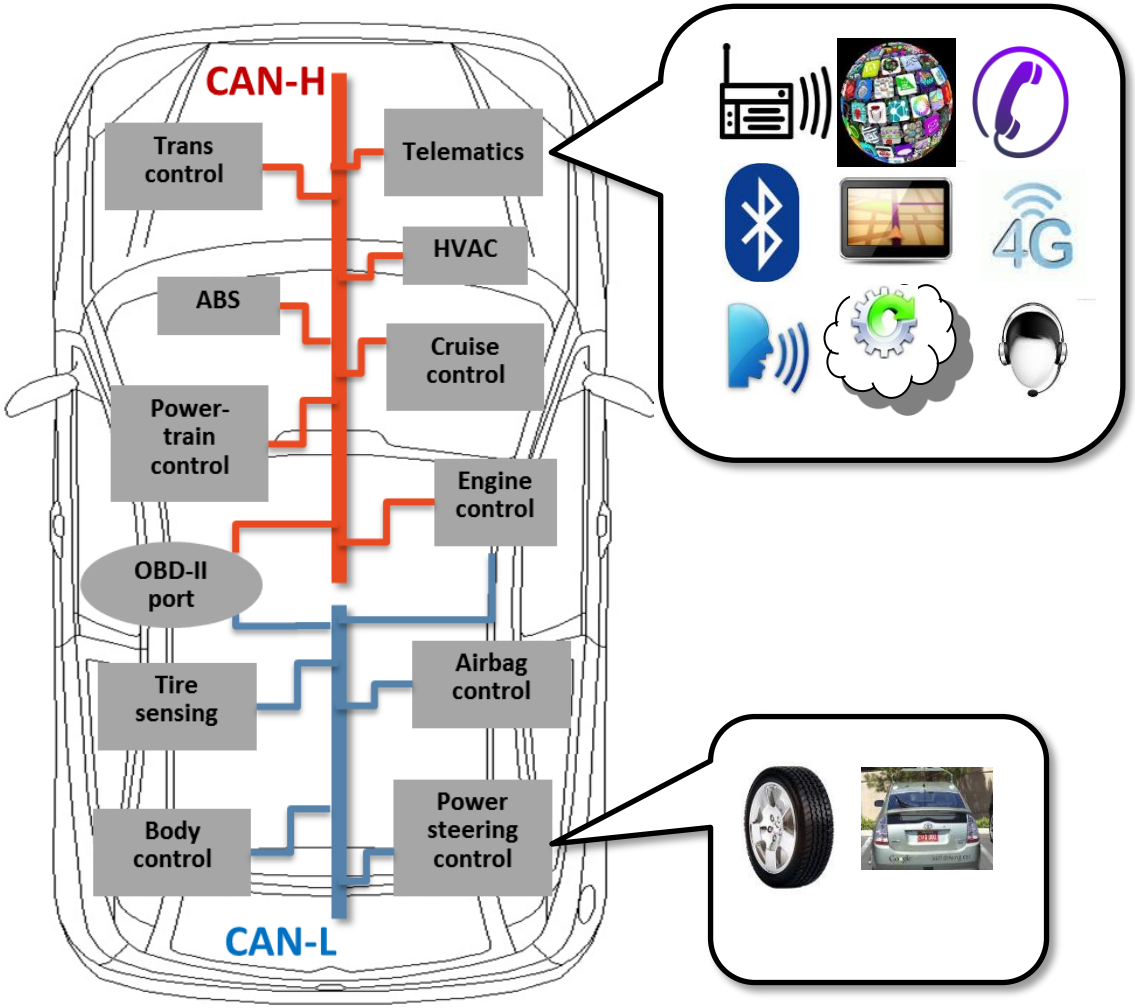
ガス・水道
- Meter reading
- Industrial controls
- Pro-active alerts
- Smart Grid applications
- Remote temperature control

スマートホーム
- Smart home appliances
- Connected home
- Video feed monitoring
- Parental Controls

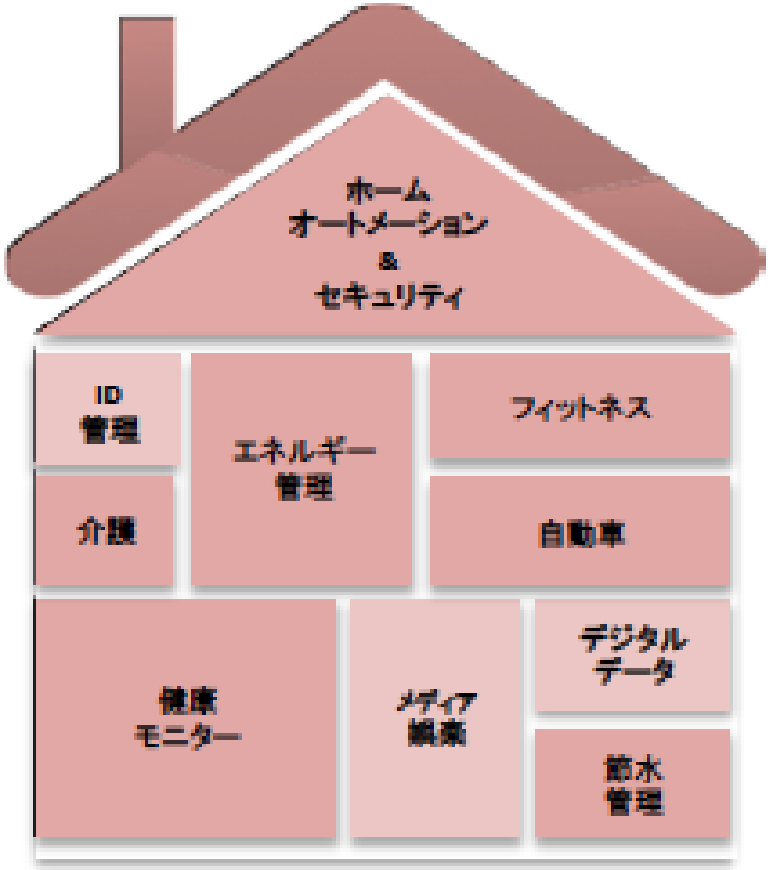
＋

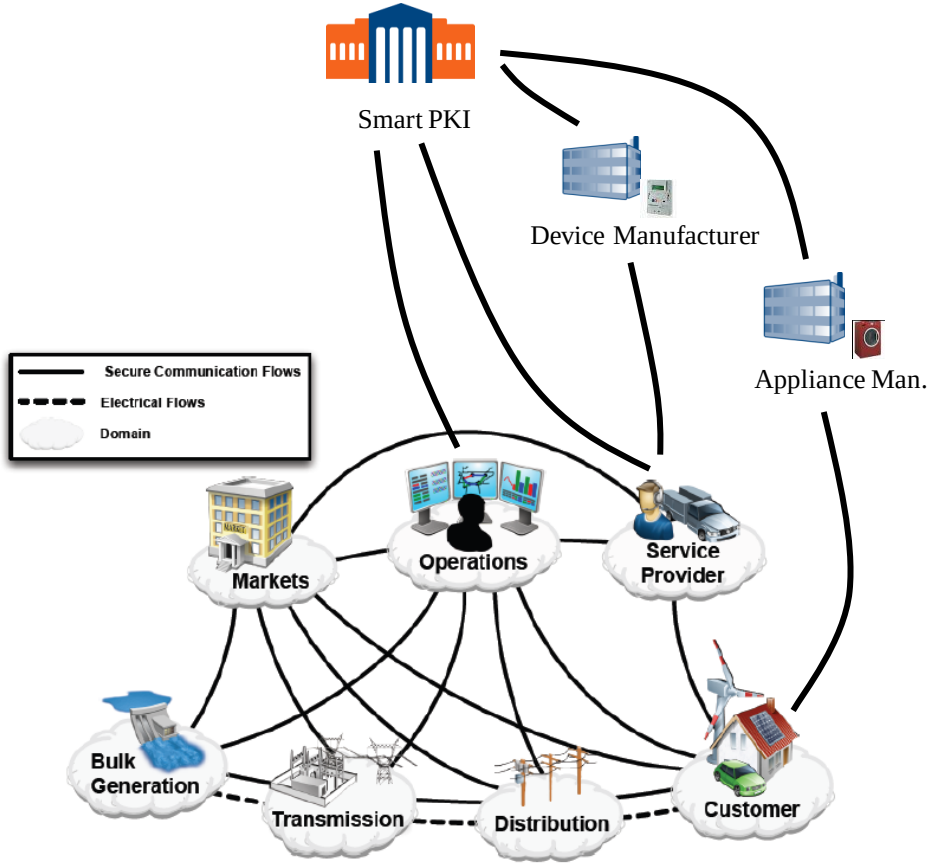
個人メイカー（基盤＋センサー＋３Dプリンタ）

組み込み型（RealTime）IoT

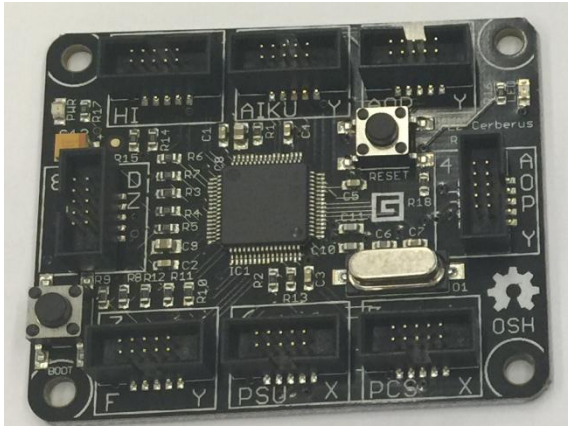


スマートホーム IoT





個人MakersのIoT



基盤

モニター

光センサ

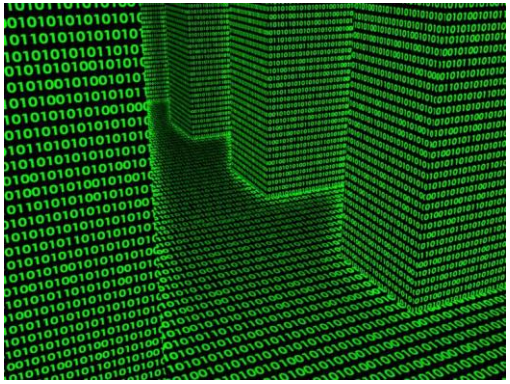
1万円前後で、センサー付きのデバイスを作成できる

外枠をデザインし、３Dプリンターで試作機を作成し、amazonで販売できる

IoTに関連するトレンド

IPv6, **p2p**接続が可能となる。

センサーは、より小さく、安く、パフォーマンスも向上、10億個もある



ビッグデータ・分析、情報収集と抽出データの洞察

“もの“の**セキュリティ**と**管理** の本質は、収集データの信頼性確保

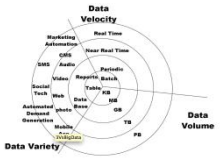
IoTのソリューション

各役割

サービス

意思決定
データ分析





ビジネスシステムとアプリケーション

- Data manipulation
- データ分析
- レポート生成
- データアクセス管理・制御

ITシステム

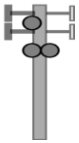
制御と管理

サーバ・データセンター

- デバイス/センサーの監視と管理
- デバイス/センサーのソフトウェアの更新管理
- データの統合と管理
- データストレージの維持/管理とデータバックアップ
- データセンタのセキュリティと攻撃からの保護

ネットワーク

アグリゲータ



ワイヤレス

PLCs

Gateways

- データの暗号化 (over the air)
- デバイス/センサーからのデータを収集しIT システムへ
- 攻撃からの保護
- デバイス/センサーの機器監視
- ネットワーク監視
- セキュリティ監視（異常検知）

センサー／デバイス

データ生成と収集





デバイス/センサー、アクチュエーター

- デバイス/センサーのデータ生成と収集
- デバイス認証
- デバイスとユーザ識別
- デバイスとユーザ認証
- データ暗号（証明書有効期間）

マルチレイヤ、マルチテクノロジーで防御？

デバイス

- デバイス自体
- デバイス管理
- セキュアなアプリケーション
- ファブリック

データ

- データセンターの保護
- 大量データが生成される
- 重要データの窃取・紛失しない
- 鍵の管理
- 鍵の問題によるデータ復旧

ネットワークレベル

- ネットワークの分離
- 異常を検出
- 通信の盗聴・改竄

家庭における IoTの脅威動向

NAT ルーター

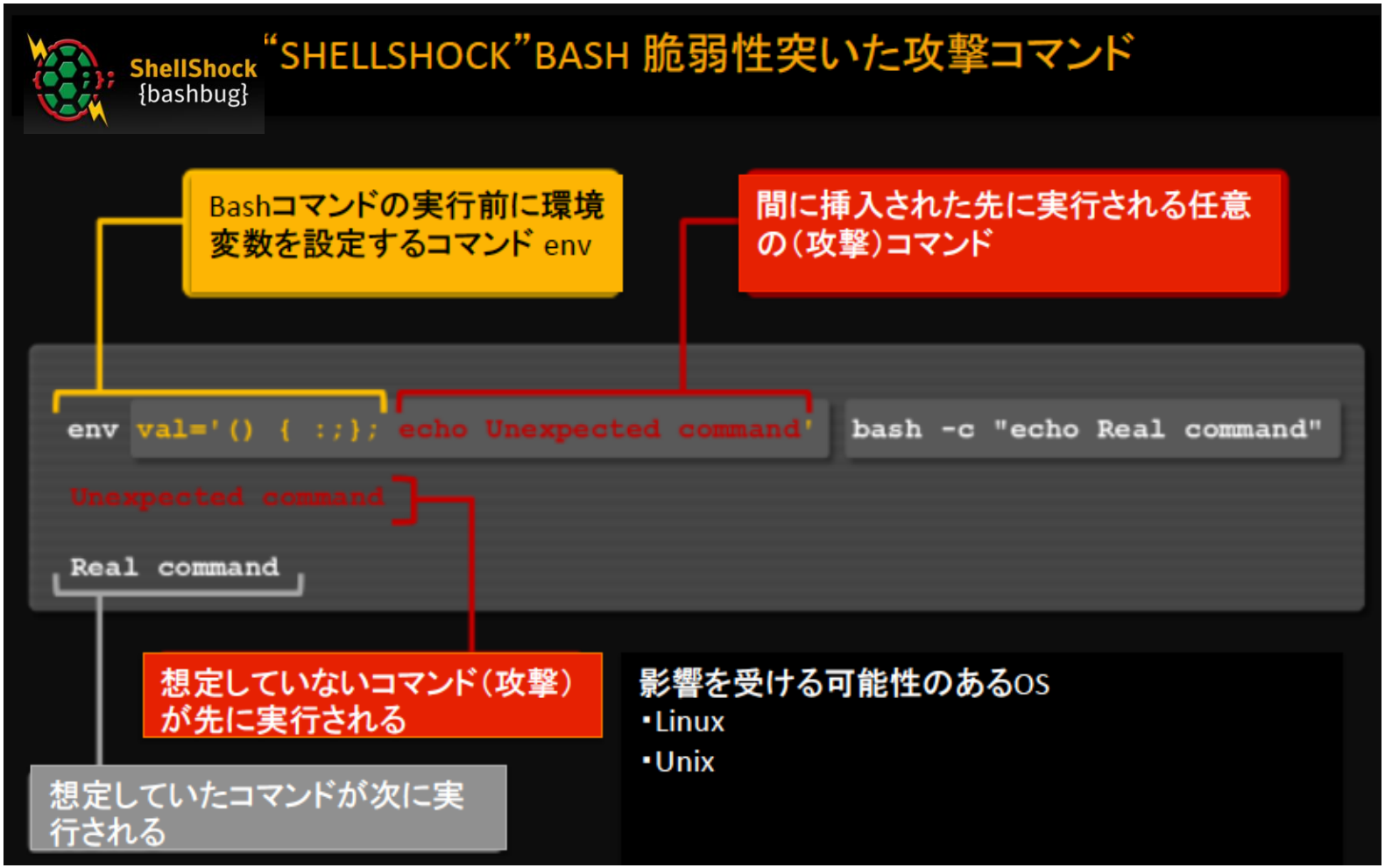
- 監視カメラやベビーモニターへのリアルな攻撃：最新レポートで確認済
- テレビ、自動車、医療機器への攻撃：実証済
- スパムメールを送信する冷蔵庫の　報道は誇張されている
  - NATルーターにより、すべてのデバイスが単一のIPアドレスを持っているように見える
  - 冷蔵庫とPCは同じIPアドレスを持っているように見える
  - しかしスパムメールは W32.Waledac（Kelihos）によって送信された
    - W32はWindows OSを意味

家庭における IoTの脅威動向

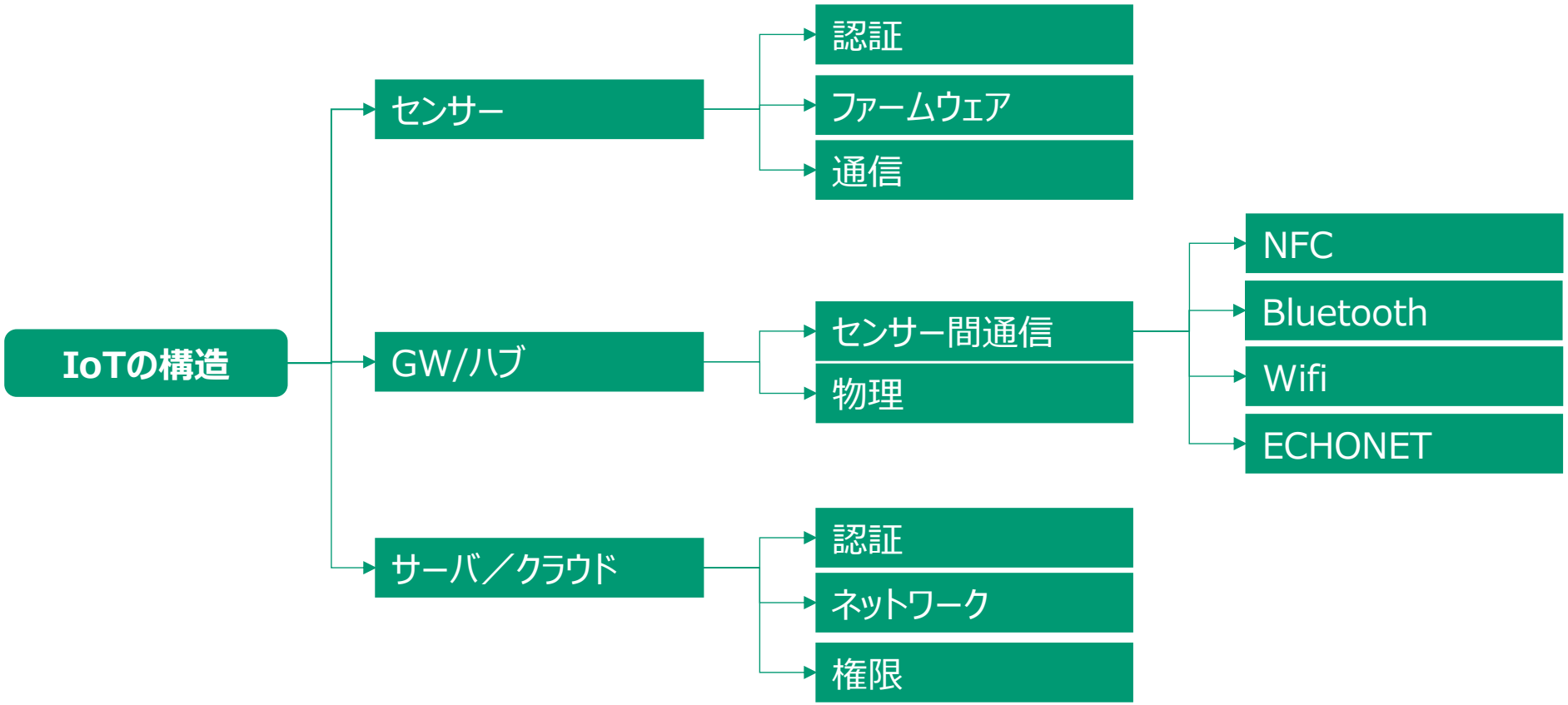
NAT ルーター

- ルーターでさえリスクに
- Linux.DarllozがLinux PCやLinuxを実行するIoTデバイスに感染
- Linux.AidraはケーブルやDSLモデムを標的にする
- 感染したシステムは以下の目的に使用可能
  - DDoS攻撃
  - ブラウザーのリダイレクション
  - 仮想通貨のマイニングにも
- パッチを適用しないことによる脆弱性や変更していないデフォルトのパスワードがリスクを引き起こす

Bash bug 脆弱性


ShellShock
{bashbug}
“SHELLSHOCK”BASH 脆弱性突いた攻撃コマンド
Bashコマンドの実行前に環境変数を設定するコマンド env
間に挿入された先に実行される任意の（攻撃）コマンド
env val='() { :;}; echo Unexpected command'
bash -c "echo Real command"
Unexpected command
Real command
想定していないコマンド（攻撃）が先に実行される
想定していたコマンドが次に実行される
影響を受ける可能性のあるOS
・Linux
・Unix

IoT 構造からセキュリティを考える



IoTの脅威　Top10

I1 Insecure Web Interface
I2 Insufficient Authentication/Authorization
I3 Insecure Network Services
I4 Lack of Transport Encryption
I5 Privacy Concerns
I6 Insecure Cloud Interface
I7 Insecure Mobile Interface
I8 Insufficient Security Configurability
I9 Insecure Software/Firmware
I10 Poor Physical Security

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I1 Webインタフェース

○脅威：仕様
内部および外部ネットワークからのWebアクセス

○攻撃：　脆弱性
認証の既定値、認証の平文通信の盗聴、アカウントリスト攻撃
内部および外部からの攻撃

○弱点：
アカウントリスト、ロックアウト機能無し、安易なパスワード設定。Webインタフェースは、内部からの設定を想定しているが、外部からのアクセスと同様に重要。問題は、Webインタフェースの脆弱性は、XSSの様にツールの利用等で簡単に見つけられること。

○技術的な影響：重大
データ漏えい、破壊、規約準拠の欠如、サービス停止、機器の乗っ取り

○ビジネスへの影響
脆弱なWebインタフェースは、危ないデバイスとなり顧客を危険にさらす。ブランドイメージの失墜となる

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I2 認証と認可

○脅威：仕様
内部および外部ネットワークからのWebアクセス

○攻撃：脆弱性
弱いパスワード、脆弱なパスワード復旧機能、弱い認証、アクセス制御の欠如。
内部および外部からの攻撃

○弱点：
弱いパスワードは、認証/権限機能として不十分。不十分な認証/権限機能は、内部インタフェースのみのアクセスであり、外部または他のネットワークでない。インタフェースで、認証/権限機能の欠如が見つかることがある。ツール等のテストツールで簡単に発見可。

○技術的な影響：重大
データ漏えい、破壊、規約準拠の欠如、サービス停止、機器の乗っ取り

○ビジネスへの影響
脆弱なWebインタフェースは、危ないデバイスとなり顧客を危険にさらす。ブランドイメージの失墜となる

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I3 ネットワークサービス

○脅威：仕様
内部および外部ネットワーク経由でのデバイスへのアクセス

○攻撃：　脆弱性
攻撃者は、ネットワークサービスの脆弱性を利用しデバイス自身またはバウンスを利用した攻撃がある

○弱点：
脆弱なネットワークサービスは、バッファオーバーフロー、サービス不能攻撃の影響を受けやすい。ポートスキャン等のツールにより、脆弱性を発見することが可能である。

○技術的な影響：中
データ漏えい、破壊、サービス停止、他の機器への攻撃

○ビジネスへの影響
攻撃によりサービスが利用できない状態になる。また、他の機器への攻撃をすることにより、顧客や他の方への影響を与える可能性がある

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I4 通信の暗号化の欠如

○脅威：仕様
内部および外部ネットワーク経由でのデバイスへのアクセス

○攻撃：　脆弱性
攻撃者は、ネットワーク上の暗号化の欠如した通信のデータを覗き見できる。攻撃は、内部と外部からの者が行う。

○弱点：
暗号化通信の欠如は、内部通信およびインターネット通信のデータを見られる。内部ネットワークでは、通信が限定的であることから十分に暗号化しないことが想像できる。Wifi通信に関しては、設定ミスにより通信可能なエリアにおいて、誰でもデータを見ることができる。ツール等により、SSL、TLSの脆弱性の有無をチェックできる。

○技術的な影響：重大
データ漏えい、ユーザアカウント情報の漏えい

○ビジネスへの影響
データ漏えい、改ざんによりユーザに影響がある

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I5 プライバシー

○脅威：仕様
デバイスが繋がるもの（人）とアプリケーションと内部および外部のデータ保管環境

○攻撃： 脆弱性
攻撃者は、パーソナルデータを得るために複数の攻撃方法を使う。例えば、不十分な認証、弱い暗号化通信、ネットワークの脆弱性、設定ミス等のある機器を狙う。

○弱点：
パーソナルデータの収集と適切な設定の欠如により、プライバシー問題になりうる。プライバシー保護に関することは、機器の活動とユーザ設定により収集されるデータをレビューすることにより容易に見つけられる

○技術的な影響：重大
パーソナルデータの漏えい

○ビジネスへの影響
不適切な設定および不必要に収集されたデータの漏えい、盗難により顧客に影響がでる

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I6 クラウドインタフェース

○脅威：仕様
クラウドへのアクセス

○攻撃：　脆弱性
攻撃者は、データへのアクセスまたはコントロールするためにクラウドのWebサイトに対して複数の攻撃方法を利用する。例えば、不十分な認証、弱い暗号化通信、ネットワークの脆弱性、設定ミス等のある機器を狙う。

○弱点：
推測可能な認証やユーザリストの利用により晒される。クラウドインタフェースがセキュアでない場合、コネクションまたはパスワードリセット機能により有効なユーザかどうかを容易に発見でき、ユーザリストを作成できる。

○技術的な影響：重大
ユーザデータの漏えいと機器の管理が可能

○ビジネスへの影響
データの盗難、データ改ざんと機器を管理されることによる顧客への影響と評判

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I7 モバイルインタフェース

○脅威：仕様
モバイルアプリケーションのアクセス

○攻撃：　脆弱性
攻撃者は、データへのアクセスまたはコントロールするためにモバイルアプリケーションに対して複数の攻撃方法を利用する。例えば、不十分な認証、弱い暗号化通信、アカウントリスト等がある。

○弱点：
推測可能な認証やユーザリストの利用により晒される。モバイルインタフェースがセキュアでない場合、コネクションまたはパスワードリセット機能により有効なユーザかどうかを容易に発見でき、ユーザリストを作成できる。

○技術的な影響：重大
ユーザデータの漏えいと機器の管理が可能

○ビジネスへの影響
データの盗難、データ改ざんと機器を管理されることによる顧客への影響と評判

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I8 セキュリティ設定

○脅威：仕様
機器へのアクセス

○攻撃：　脆弱性
攻撃者は、アクセス権設定の不備をついてデータへのアクセスまたは機器の管理する。また、暗号設定、パスワードオプションの不備をつき、機器の障害やデータ漏えいになる。故意または事故的なアカウントに関係なく起こりうる。

○弱点：
限定されたユーザやセキュリティ機能の変更ができないもので発生する。機器の管理Webインタフェースにユーザパーミションが無い、例えば、強いパスワードを作成する等。ユーザマニュアルをチェックするだけで見つけられる。

○技術的な影響：中
ユーザデータの漏えいと機器の管理が可能

○ビジネスへの影響
データの盗難、データ改ざんと機器を管理されることによる顧客への影響と評判

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I9 ファームウェア

○脅威：仕様
機器へのアクセス　および　機器に搭載されるもの

○攻撃：　脆弱性
攻撃者は、複数の攻撃方法を利用する。例えば、DNSの乗っ取りにより、暗号化されていない通信の更新ファイルの取得、悪意のあるダウンロードファイルの配布により侵入する。

○弱点：
ソフトウェア、ファームウェアの配布のために、保護の仕組みがない。また、ソフトウェア、ファームウェアに重要なデータ、例えばパスワード等をハードコーディングしている場合もセキュアでない。これらの脆弱性は、ソフトウェアのアップデート時にネットワークのキャプチャを取得することで、容易に分かる。

○技術的な影響：重要
ユーザデータの漏えいと機器の管理および他の機器へ拡散

○ビジネスへの影響
データの盗難、データ改ざんと機器を管理されることによる顧客への影響と評判

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

I10 物理的セキュリティ

○脅威：仕様
機器への物理的なアクセス

○攻撃：　脆弱性
攻撃者は、USB、SDカードまたはその他のストレージを介してOSへのアクセスを試み機器上にデータをコピーする。

○弱点：
記憶装置等に容易にアクセスできることにより、機器の逆アセンブルが可能である。USBや外部ポートを利用した構成、メンテナンスする機器の場合、その利用が狙われる

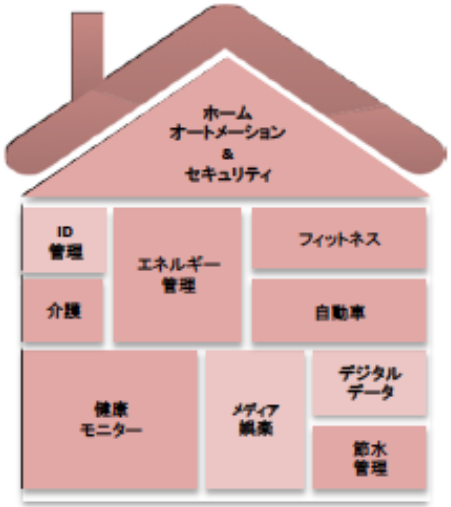
○技術的な影響：重要
ユーザデータの漏えいと機器の管理および他の機器へ拡散

○ビジネスへの影響
データの盗難、データ改ざんと機器を管理されることによる顧客への影響と評判

出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

IoT – 将来予測

IoTを有効活用するために、パーソナルデータの利活用が必須になり、多くのデータがデータセンターに集約される。
家庭内の家電、計測メータがホームネットワークとして接続され、リモートからのコントロールが可能となる。
企業が提供する、B2B、B2CのサービスもIoT機器を活用することにより、これまでと異なる脅威が出現する。



JNSA IoTセキュリティWGの取組

Internet of things もののインターネットが注目されている

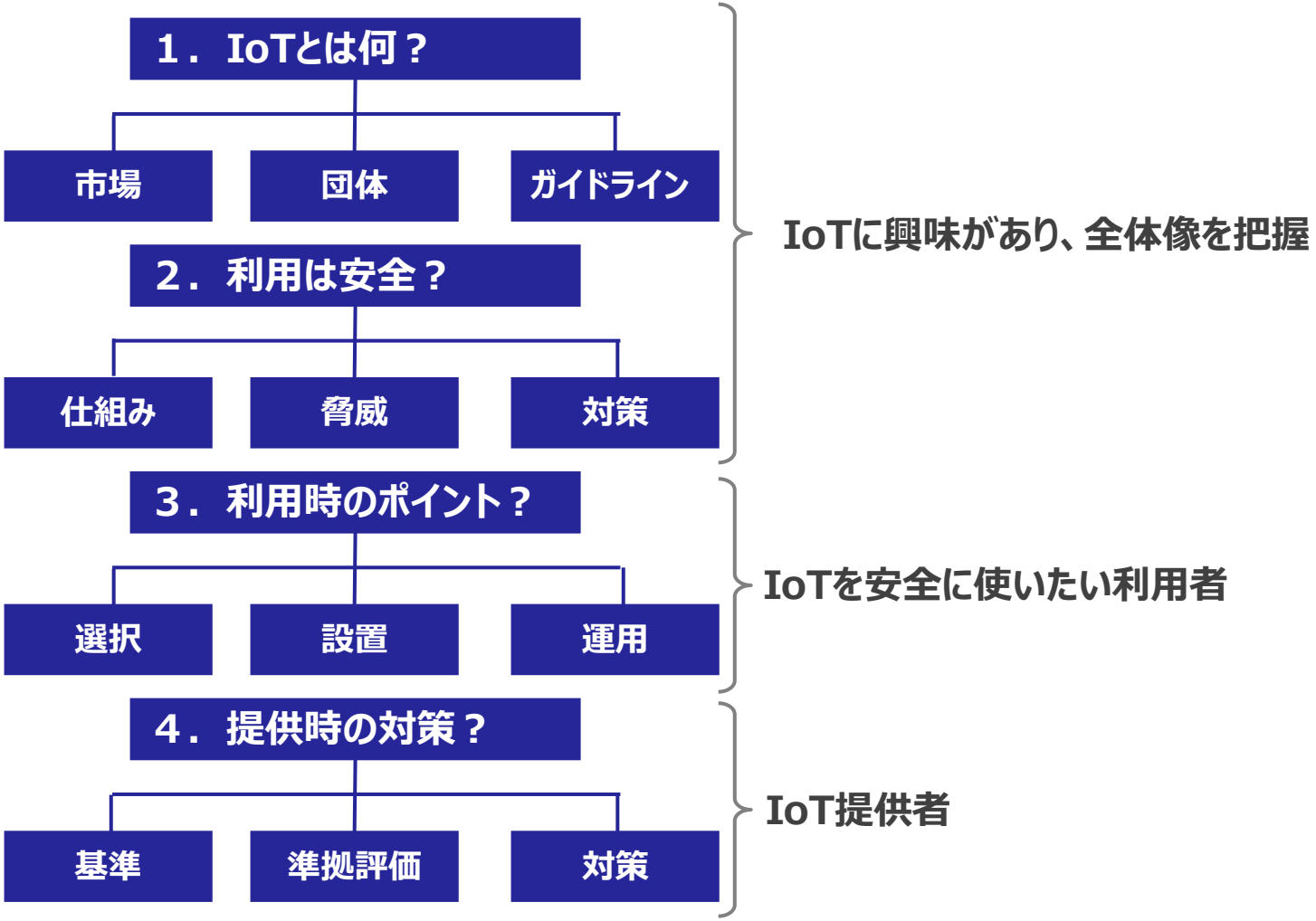
ものがインターネットに接続されるが安全維持できるのか

個人がメーカーとしてものを作り販売できるが安全なものか

増え続ける機器が、セキュリティ管理されていることを期待するが、そのとおりか

個人が作成する機器が、セキュリティ対策していない場合、脅威になるのではないか

JNSA IoTセキュリティWGの取組



ご清聴ありがとうございました。