IBM Security
Intelligence. Integration. Expertise.

IBM

IoT時代のサイバー・セキュリティ
今そこにあるリスク

日本アイ・ビー・エム株式会社　セキュリティー事業本部
エグゼクティブ・アーキテクト、CISSP
大津留 史郎(ohtsuru@jp.ibm.com)
2016年 4月 2日(土)

今日お話しすること

1.サイバーセキュリティ

1.1 サイバーセキュリィ最新動向
(IBMのレポートより)

1.2 情報セキュリティ管理部門が
直面している課題と対策

2.IoTセキュリティ

2.1 IoTの世界

2.2 IoTセキュリティ最新動向

2.3 アーキテクトの視点から見た考察

ご参考:
IBM ProVIsion No.88 IoT時代のサイバーセキュリティ　今そこにあるリスク
https://www-304.ibm.com/connections/blogs/ProVISION86_90/entry/no88?lang=ja

IBMの定期レポート

IBMは、経営者が考えるべきセキュリティ及び最新のセキュリティの脅威動向について定期的にレポートを公開しています。

- 『2015 Securing the C-Suite』(IBMセキュリティ・スタディー)　毎年、範囲:全世界
  http://www-03.ibm.com/security/jp/ja/ciso/

- セキュリティ脅威レポート IBM X-Force　四半期毎、範囲:全世界
  http://www-01.ibm.com/software/jp/cmp/security_report/

- Tokyo SOC Report　半期毎、範囲:日本
  https://www-304.ibm.com/connections/blogs/tokyo-soc/?lang=ja

『2015 Securing the C-Suite』(IBMセキュリティ・スタディー)

2015 Security the C-Suiteでは、経営者に対して、3つの提言が示されています

1. セキュリティ・リスクを正しく理解する
   65%(経営者)　自社のサイバー・セキュリティ計画は十分に確立されていると確信している。
   17%(経営者)　最高レベルの準備態勢と能力を実装している。

2. 社内外での協業、協力、教育を積極的に行う
   68%(CEO)　外部とのセキュリティ・インシデントの共有に消極的。

3. セキュリティの対策や管理は、迅速かつ慎重に
   60%(CFO、CHRO、CMO)
   サイバー・セキュリティ脅威の管理に最も関与していないと感じているが、
   サイバー犯罪者が最も欲しがるデータの管理責任は彼らが負っている。

『2015 Securing the C-Suite』(IBMセキュリティ・スタディー)
(http://www-03.ibm.com/security/jp/ja/ciso/)より転載

(参考)リスク認知における楽観バイアス

人間がリスクを認知する際、実際よりもリスクを楽観的に評価するバイアスがかかることが心理学的の研究で証明されています。

- 平成24年の交通事故死亡確率
  - 10万人当たり3.4人
  - 3.5人÷10万人 = 0.0034%

26－23　道路交通事故

年　次	事故件数	死亡事故	負傷事故	死者数 1)	負傷者数	自動車台数（年末）（1,000台）	自動車1万台当たり死者数	人口10万人当たり死者数 2)
昭和 60 年	552,788	8,826	543,962	9,261	681,346	48,268	1.9	7.7
平成 2 年	643,097	10,651	632,446	11,227	790,295	60,651	1.9	9.1
7	761,794	10,232	751,562	10,684	922,677	70,074	1.5	8.5
12	931,950	8,713	923,237	9,073	1,155,707	75,865	1.2	7.1
17	934,339	6,681	927,658	6,927	1,157,115	79,207	0.9	5.4
20	766,382	5,067	761,315	5,197	945,703	79,237	0.7	4.1
21	737,628	4,826	732,802	4,968	911,215	79,042	0.6	3.9
22	725,903	4,783	721,120	4,922	896,294	79,092	0.6	3.8
23	692,056	4,532	687,524	4,663	854,610	79,242	0.6	3.6
24	665,138	4,280	660,858	4,411	825,396	79,882	0.6	3.5
25	629,021	4,278	624,743	4,373	781,494	80,411	0.5	3.4

出展：統計局　統計表(http://www.stat.go.jp/data/nihon/pdf/n152600000.pdf)より転載

- 2015年　年末ジャンボ宝くじの一等当選確率
  - 1等7億円：1ユニット(2000万枚)に1本
  - 1÷2000万= 0.0000005% (2,000万分の1)

680倍!

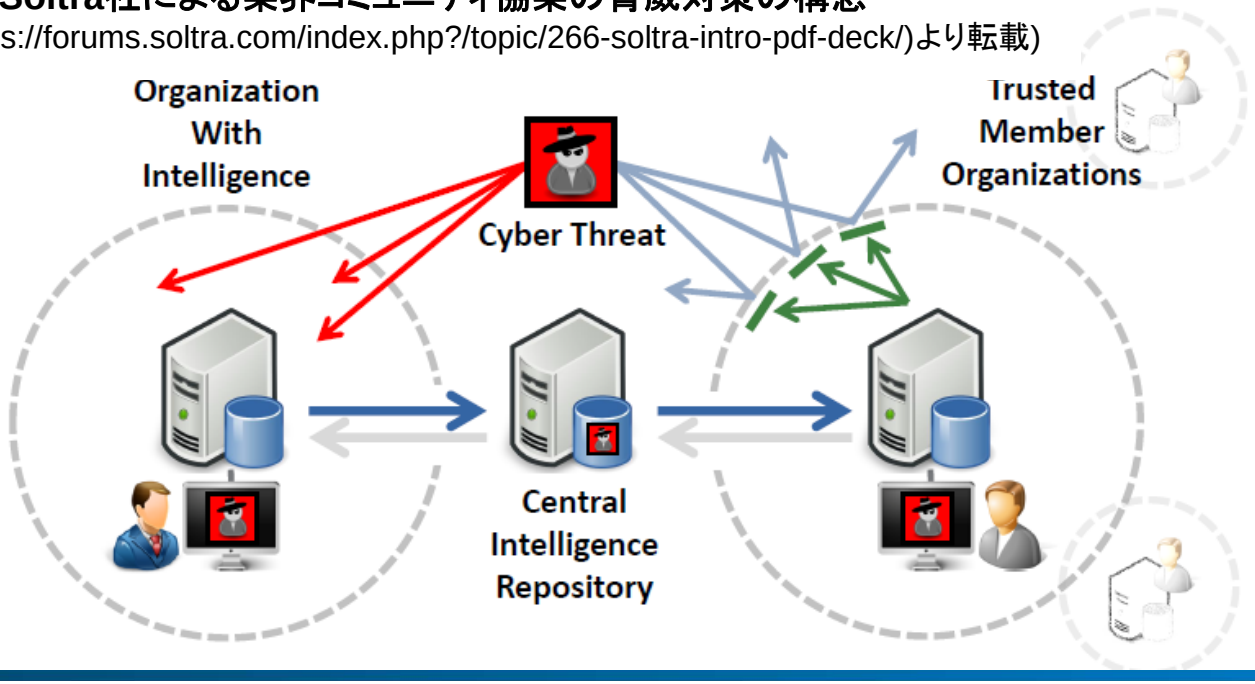
(参考)企業を超えた情報共有、産官学協業によるサイバー犯罪対策

全世界及び日本国内において、業界内の企業を超えた脅威情報の共有、産官学協業によるサイバー犯罪対策の動きが起こりつつあります。

- 日本国内における産官学協業によるサイバー犯罪対策の活動
  - 一般財団法人 日本サイバー犯罪対策センター (https://www.jc3.or.jp/)
- 業界内における脅威情報共有の活動
  - ISAC（Information Sharing and Analysis Center）
    - 一般財団法人 金融ISAC (http://www.f-isac.jp/)
    - Telecom-ISAC Japan (https://www.telecom-isac.jp/)

参考資料:
平成21年度内閣官房情報セキュリティセンター委託調査
「米国のセキュリティ情報共有組織（ISAC）の状況と運用実態に関する調査」
http://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf

米国FS-ISACとSoltra社による業界コミュニティ協業の脅威対策の構想
(Soltra社資料(https://forums.soltra.com/index.php?/topic/266-soltra-intro-pdf-deck/)より転載)



IBM X-Force脅威に対するインテリジェンス四半期レポート

2015年度第4四半期の IBM X-Force脅威に対するインテリジェンス四半期レポートは、IBM Emergency Response Serviceチームの考察結果として4つの傾向を報告しています。

傾向1: 2タイプの攻撃者による攻撃

タイプ1: あまり洗練されていない攻撃者(スクリプトキディ)による、明らかに分かる攻撃

タイプ2: 洗練された慎重なハッカー(ステルス攻撃者)による、深刻なインシデント

助長する原因: パッチ未適用、ネットワークトラフィックを可視化していない

傾向2: ランサムウェアの出現

助長する原因: データをバックアップしていない、パッチ未適用、ユーザの意識欠如(危険なWebサイトへのアクセス)

傾向3: 悪意による内部犯行

助長する原因: 管理者アカウントの共有、簡単なパスワード

傾向4: 経営者の意識の高まり

IBM X-Force脅威に対するインテリジェンス四半期レポート: 2015年度第4四半期
(http://www-01.ibm.com/software/jp/cmp/security_report/)より転載

(参考)ランサムウェアとは

ランサムウェアとは、ファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラムの総称です。

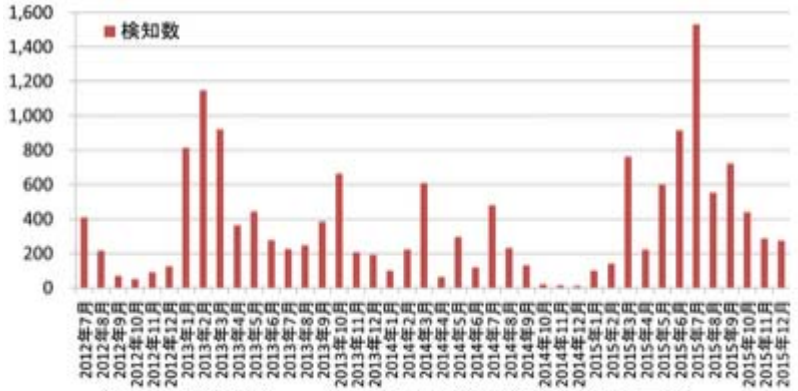
ファイルを暗号化した後に表示されるメッセージの例

IPA　2015年6月の呼びかけ「 パソコン内のファイルを人質にとるランサムウェアに注意！ 」～ メッセージが流暢な日本語になるなど国内流行の懸念 ～
(https://www.ipa.go.jp/security/txt/2015/06outline.html)より転載

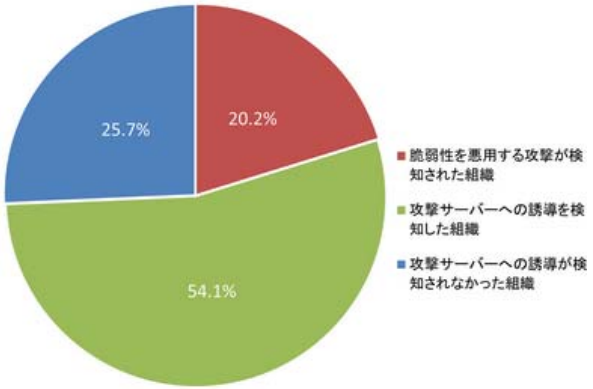
Tokyo SOC情報分析レポート

2015年下半期のTokyo SOC情報分析レポートは、最新の脅威として3つの実態を報告しています。

1. 約74%の組織でドライブ・バイ・ダウンロード攻撃を確認

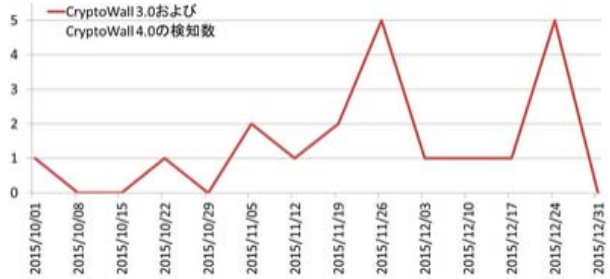


ドライブ・バイ・ダウンロード攻撃の月別検知数推移（日本国内）
（Tokyo SOC調べ：2012年7月1日～2015年12月31日）

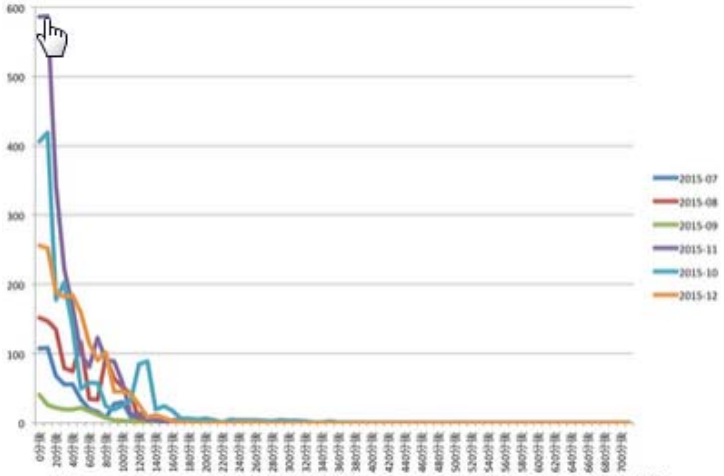


ドライブ・バイ・ダウンロード攻撃発生状況（日本国内）
（Tokyo SOC調べ：2015年7月1日～2015年12月31日）

2. 不特定多数を狙ったメール攻撃は「短期」「集中」「使い捨て」
3. ランサムウェアを用いた攻撃活動の増加



ランサムウェアCryptoWall 3.0およびCryptoWall 4.0の検知件数（日本国内）
（Tokyo SOC調べ：2015年10月1日～2015年12月31日）



最初の攻撃メール観測時刻を基点とした経過時刻とメール観測数の推移
（Tokyo SOC調べ：2015年7月1日～2015年12月31日）

2015年下半期Tokyo SOC情報分析レポート
(https://www-304.ibm.com/connections/blogs/tokyo-soc/?lang=ja)より転載

(参考)ドライブ・バイ・ダウンロード攻撃とは

ドライブ・バイ・ダウンロード攻撃とは、Webサイトの閲覧を通じて、PCにマルウェアを感染させる攻撃手法です。

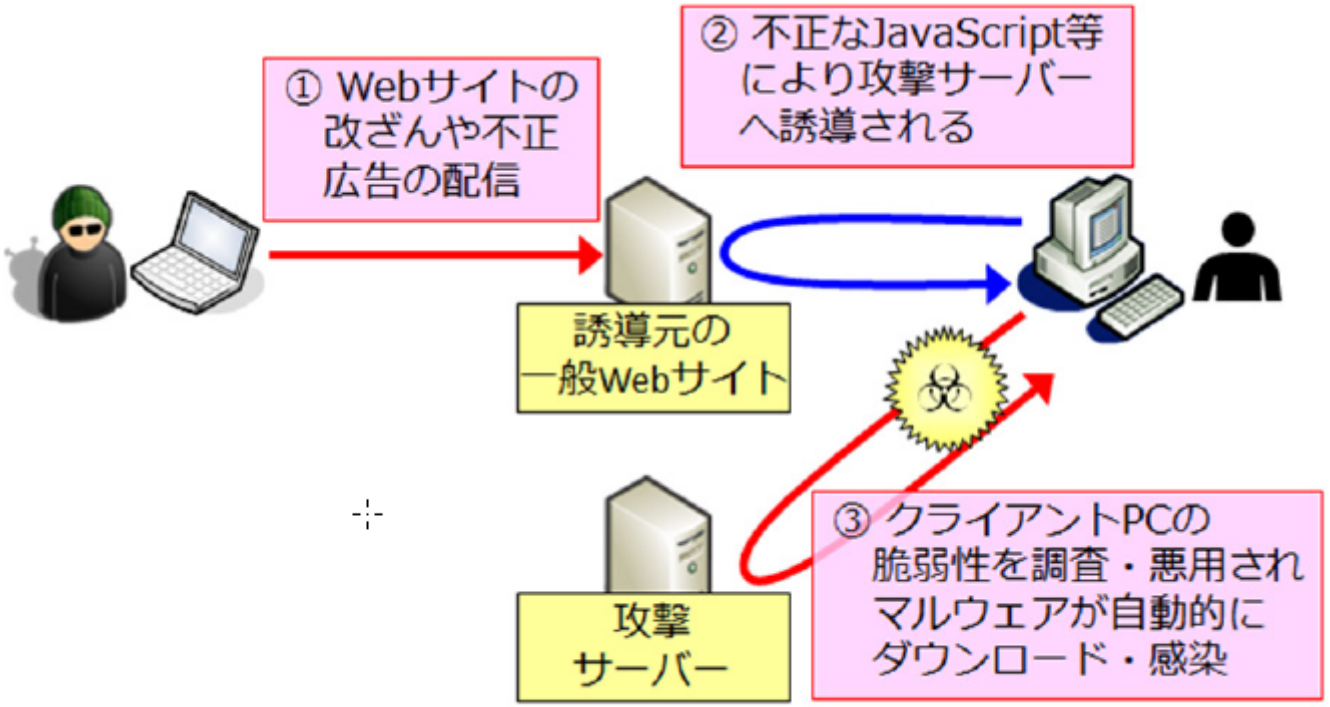


図 5 ドライブ・バイ・ダウンロード攻撃の仕組み

2015年下半期Tokyo SOC情報分析レポート
(https://www-304.ibm.com/connections/blogs/tokyo-soc/?lang=ja)より転載

(ご参考)IBM 10 Essential Practiceによる成熟度診断&ロードマップ策定

IBMは、10 Essetial Practiceというフレームワークを用いて、サイバーセキュリティにおいて重要な10の分野についてお客様の成熟度を診断し、強化するためのロードマップ策定を行っています。

5. Take a Hygienic Approach to Managing Infrastructure

6. Control Network Access and Assure Resiliency

4. Secure Services, By Design

7. Address New Complexity of Cloud and Virtualization

3. Defend the Workplace (Endpoint)

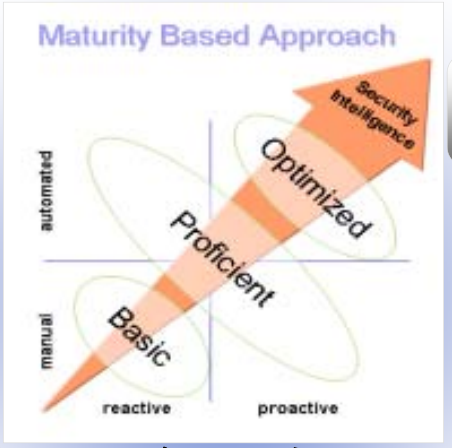
8. Manage 3rd Party Security Compliance

2. Manage Security Incidents with Intelligence

9. Secure Data and Protect Privacy

1. Build a Risk Aware Culture & Management System

10. Manage the Identity Lifecycle



各エリア毎に
5段階の成熟度レベルで
現状とあるべき姿を明確化し、
ロードマップを策定

情報セキュリティ管理部門が直面する障壁

- セキュリティよりビジネスが優先される
  - 十分な人員及び予算が確保されない
    - 売上又は利益に直結する投資が優先される
    - セキュリティ対策の投資対効果が説明できない
  - 業務部門が言う事を聞いてくれない
    - 金を稼ぐ業務部門の方が立場が強い
    - ビジネス上の理由を盾に、例外を認めさせられる
  - 社員の意識が低い
    - 刻々と変わるルールが浸透しない
    - 分かっているが、業務が忙しくて…
- 海外法人が言う事を聞いてくれない
  - 独自のやり方でセキュリティ対策を実装している
  - 実装方法を本社に揃える理由を説明できない

セキュリティの優先度をどう上げるか? 1/2

日本企業は、売上増大またはコスト削減に直接繋がるIT投資を優先させています。セキュリティ、災害対策などのリスク対策に対する投資は、相対的には低い優先順位に留まっています。

最重要視するIT戦略上の来期の課題テーマの変化(1位での選択)

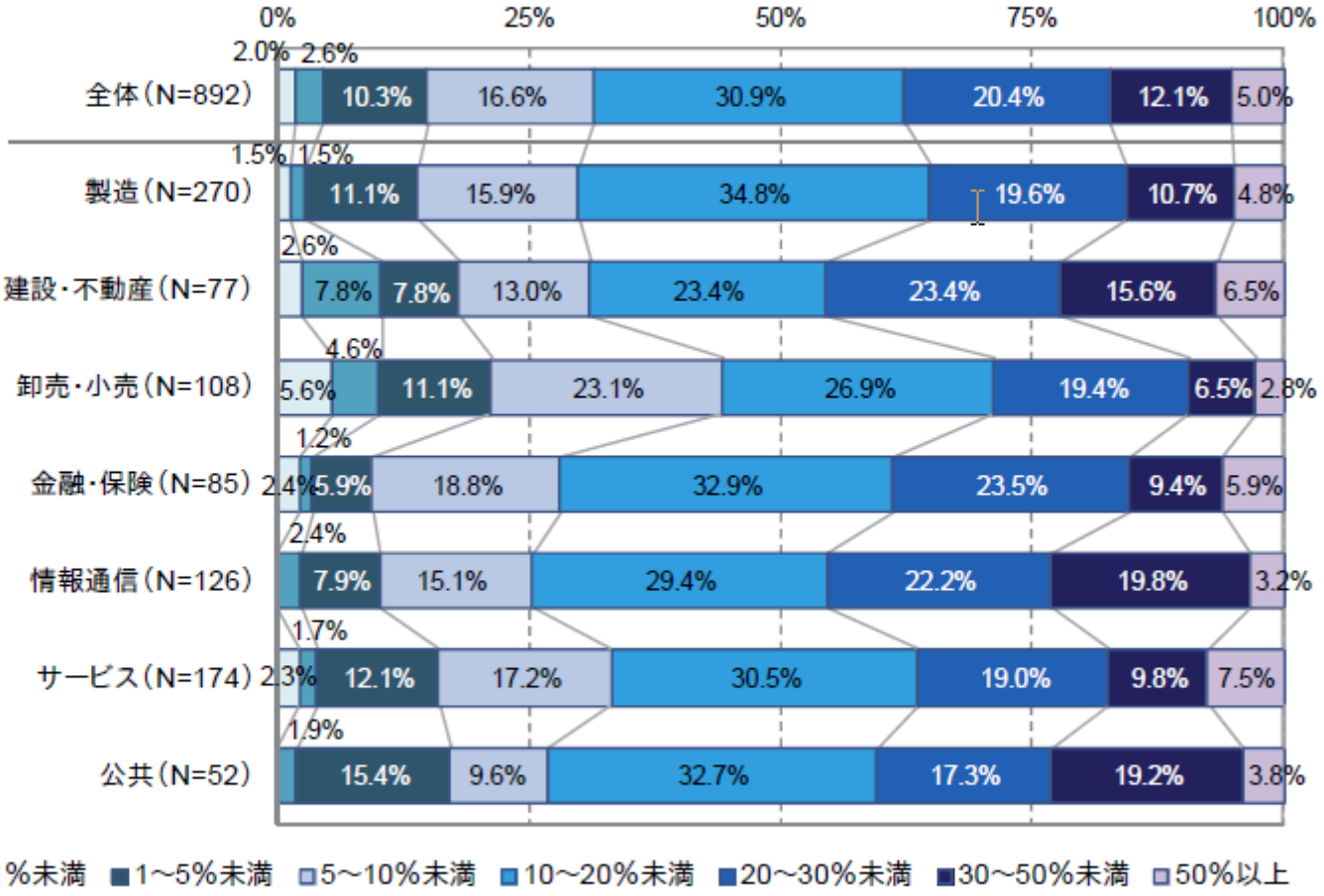
2015年度の順位(前年調査)		2016年度の順位	
1位	売上増大への直接的な貢献	1位	売上増大への直接的な貢献
2位	業務コストの削減	2位	業務コストの削減
3位	顧客サービスの質的な向上	3位	顧客サービスの質的な向上
4位	ITコストの削減	4位	ITコストの削減
5位	システムの性能や信頼性の向上	5位	システムの性能や信頼性の向上
6位	情報の活用度の向上	6位	既存システムの統合性強化
7位	既存システムの統合性強化	7位	プライバシーや機密情報の保護
8位	プライバシーや機密情報の保護	8位	情報の活用度の向上
9位	事業継続計画や災害対策の強化	9位	サイバー攻撃への対策強化
10位	グローバル・ビジネスへの対応強化	10位	事業継続計画や災害対策の強化
11位	経営における意思決定の迅速化	11位	ビジネス・イノベーションの創出
12位	従業員のワークスタイル革新	12位	経営における意思決定の迅速化
13位	ビジネス・イノベーションの創出	13位	グローバル・ビジネスへの対応強化
14位	サイバー攻撃への対策強化	14位	従業員のワークスタイル革新
15位	内部統制や法令順守への対応	15位	新技術に関する知識・活用ノウハウの獲得
16位	IT組織の再編(子会社含む)	16位	内部統制や法令順守への対応
17位	IT部門スタッフの人材育成	17位	IT部門スタッフの人材育成
18位	新技術に関する知識・活用ノウハウの獲得	18位	IT組織の再編(子会社含む)

出典:ITR「IT投資動向調査2016」

セキュリティの優先度をどう上げるか? 2/2

同業他社との比較を投資根拠にしようとしても、十分な根拠になりません。
同じ業界内でも各社さまざまな投資判断をしているからです。

図5-5. 業種別に見るIT予算額に対する情報セキュリティ対策費用割合の分布（2015年度）



出典：ITR「IT投資動向調査2016」

IBM社内における施策

セキュリティよりビジネスが優先される

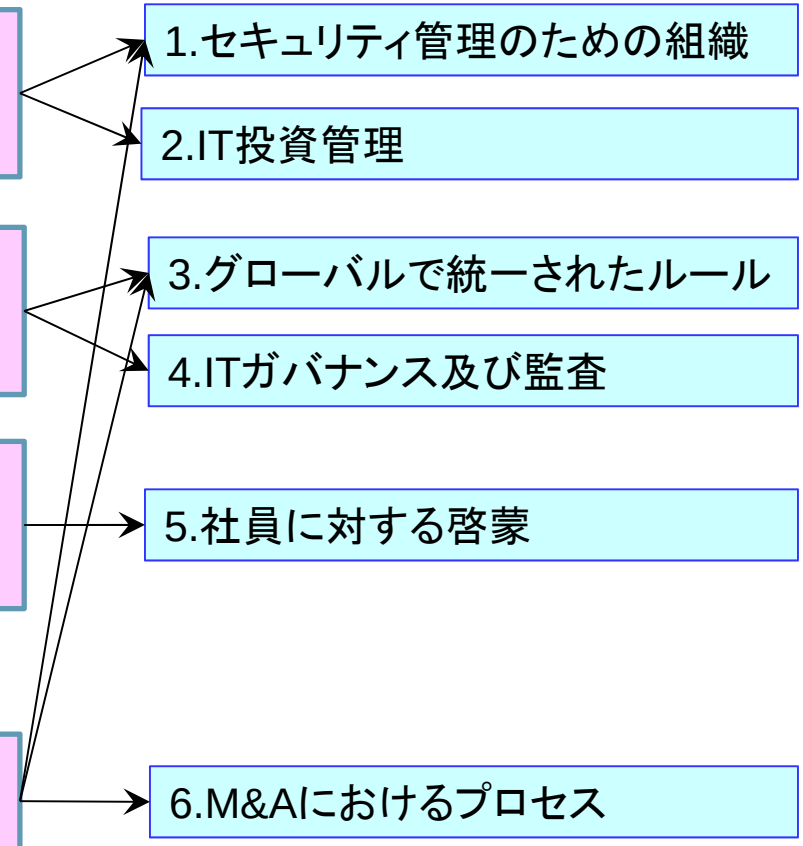
十分な人員及び予算が確保されない
- 売上又は利益に直結する投資が優先される
- セキュリティ対策の投資対効果が説明できない

業務部門が言う事を聞いてくれない
- 金を稼ぐ業務部門の方が立場が強い
- ビジネス上の理由を盾に、例外を認めさせられる

社員の意識が低い
- 刻々と変わるルールが浸透しない
- 分かっているが、業務が忙しくて…

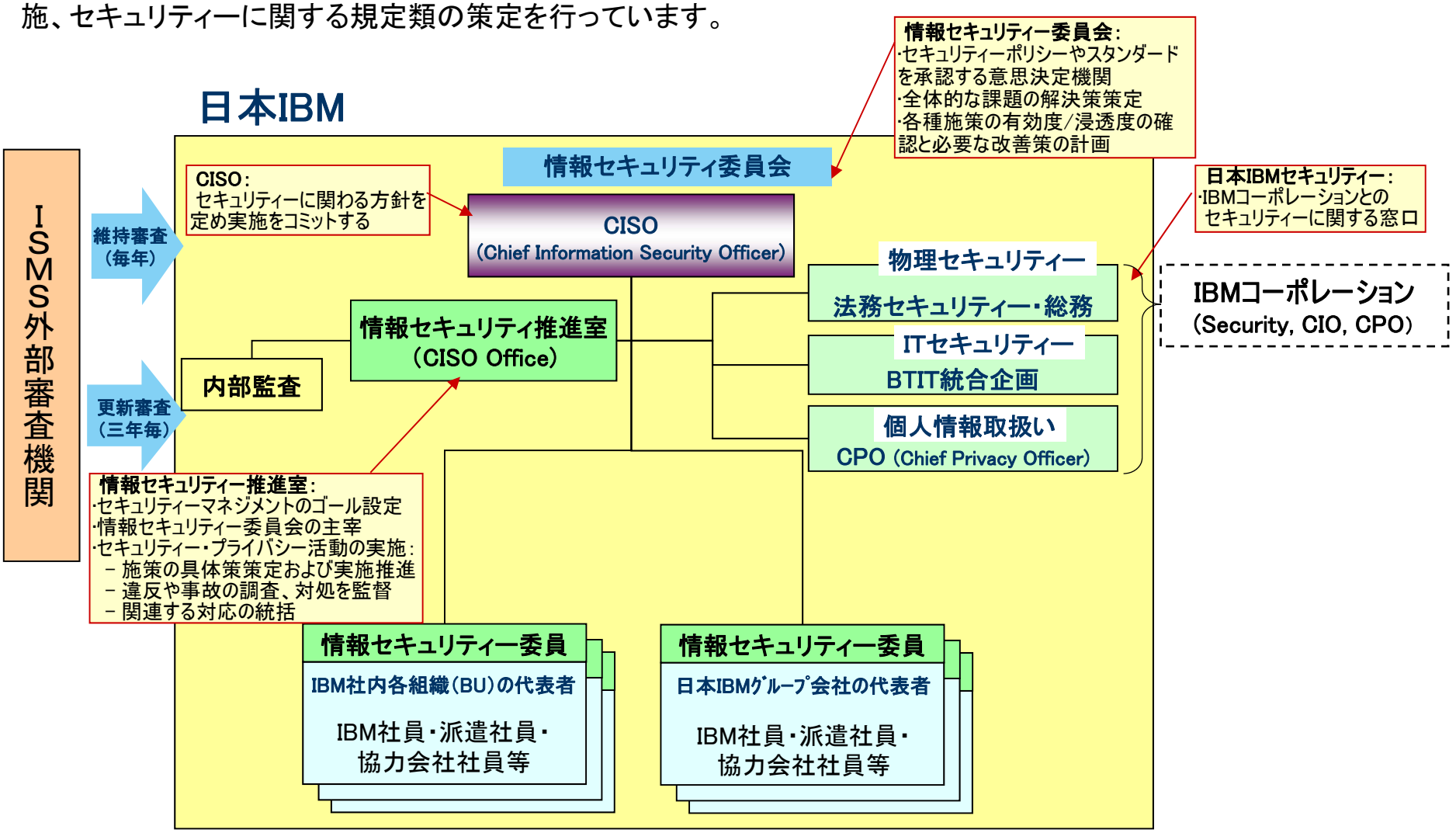
海外法人が言う事を聞いてくれない

独自のやり方でセキュリティ対策を実装している
実装方法を本社に揃える理由を説明できない



1.セキュリティの組織体制
IBMの情報セキュリティ管理運用 – 管理体制

日本IBMでは、CISO（Chief Information Security Officer）の元、各部の代表者からなる専門組織として情報セキュリティー委員会を置き、各関係者間における情報共有・意見交換、情報セキュリティ・リスクの洗い出し・分析・対策実施、セキュリティーに関する規定類の策定を行っています。



2.IT投資管理
IBMのIT投資管理システム - eIRB / ePMT / IPMT

グローバルIBMのIT投資は、グローバルで唯一のCIOが議長を務めるエグゼクティブボードにて決定されます。
各国及び事業部からの業務改革要求はIPMTにおいて統合され、ePMTにおいて横串で戦略的な業務改革計画に練り上げられた、策定された投資優先順位と共にeIRBに提案され、決定されます。

3.グローバルで統一されたルール
経営の基本ルールを明文化し、共有・徹底化

経営理念を体系的に展開し、日々の業務の基本手順やルールにまで落とし込み、約43万人社員の活動のベクトルをそろえる為の礎としています。

Corporate Policies(9項目)
発行者:会長

「ビジネス倫理」「互恵取引」
「多様な従業員の公平な扱い」
「政治活動」
「職場環境・製品安全性」
「個人情報」「環境への取り組み
「多様なお客様や取引先との関係」

Organization Letters(15通)(権限規定)
発行者:各副社長

下記について権限の移譲先および移譲しない権限を明記している。つまり、裁量権の範囲を明示している。
「Pricing」「寄付行為」「不動産」「渉外」「訴訟」「政府対応」「製品発表・販売停止」「製品・サービスの契約」「naming」「購買」「現地化」「設備投資」「監査法人等との契約」「顧客情報管理」

Corporate Instructions(規定)
発行者:各副社長

発行者	規定数
CIO	9
広報	4
公共活動	3
マーケティング	3
環境	12
財務	40
渉外	4
人事	10
知財	8
法務	8
不動産	2
研究	4
開発・製造	13

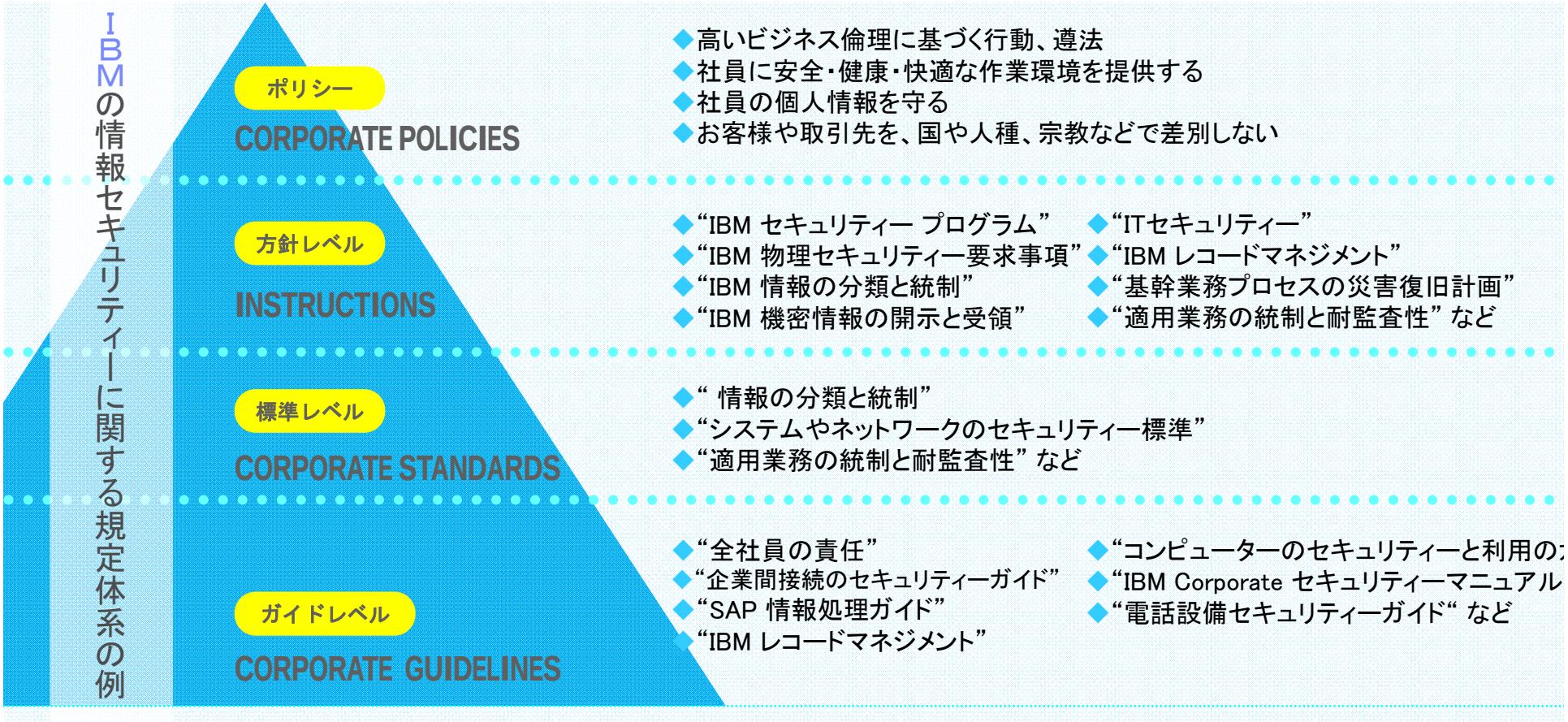
Business Conduct Guidelines (65項目)

個人の活動に直結するエッセンス

この3種の文書をCorporate Directives と呼ぶ。「One」IBM として全管理者と従業員が順守すべき項目を明示している

3.グローバルで統一されたルール
Corporate Instructions/Standards/Guidelines規定体系例

社内規定であるCorporate Instructions の施行細則・標準としてStandardsがもうけられ、その運用法がGuidelines として記述・発行され常に最新化されます。グローバルレベルで全社共通の業務オペレーションの基礎としています。項目は体系的で、網羅性高く、わかり易くまとめられています。



3.グローバルで統一されたルール
IBM の ITセキュリティー・ポリシー

全IBM社員が毎年署名する、遵守すべき行動基準「ビジネス・コンダクト・ガイドライン」には、セキュリティーの遵守に関する項目をも含んでいます。ITCSへの準拠が定められており、社員が意識しなければならないポイントと、意識しなくても安心・安全が得られるポイントとその双方を両立させています。当然遵守に対して厳しい罰則を含む対応がなされます。昨今、個人所有クライアント機器の業務使用におけるルールおよびガイドラインも設定しています。

IBMにはBCGのもと、2つの情報セキュリティに関する基準があります。

BCG （ビジネス・コンダクト・ガイドライン）

社員が遵守すべき行動基準　http://www.ibm.com/ibm/jp/about/bcg/

ITCS 104

- サーバー/ネットワークのセキュリティ基準
- アプリケーションのセキュリティ基準
- 社外&インターネット接続要件　等

ITCS 300

- クライアントＰＣのセキュリティ基準
- 業務上の情報取扱い&管理要件
- セキュリティ事故予防＆対策　等

運用&管理項目の例

- ユーザーIDとパスワードの管理
- アプリケーション/ＤＢのアクセス管理
- 機密情報の暗号化
- 不正アクセスの防止
- アンチウィルス/セキュリティ・パッチ適用
- アクセス・ログの作成と保持
- 遵守状況の確認(ヘルス・チェック)
- 物理的アクセス管理

- 各種ＰＣパスワード設定
- PC上の機密情報暗号化
- アンチウィルス・ファイヤーウォール導入
- PC盗難・紛失予防
- パスワード設定ルールの遵守
- 機密情報印刷出力時の保護

Bring Your Own Device ガイドライン

ITCS : Information Technology Corporate Standards

3.グローバルで統一されたルール
セキュリティルール事例紹介

IBMではE-WORKにての業務遂行を長年取り組んでまいりました。この際、最も懸念されるのが「セキュリティの担保」です。ソフト面でのビジネス規定・社内標準遵守。システム面での「善意のセキュリティ」の確保。そして、自宅・出張先・外出先でのセキュリティルールの徹底により、担保します。

IBMビジネス規定

ビジネス・コンダクト・ガイドライン
就業規則
業務委託契約
機密情報保持契約

IBM社内標準

機密情報管理規定
プライバシー情報取り扱い規定
事業所管理規定
ITセキュリティ管理規定
アプリケーション管理規定

セキュリティーについての社内標準

- Information Technology Corporate Standards 300 (ITCS 300)

ソフトウェアの導入／アップデート／ツール

- IBM Standard Software Installer (ISSI)
- EZUpdate
- ISAM (IBM Standard Asset Manager)
- WST (Workstation Security Tool)
- PEACH (PEer to peer Advanced Checker)

使用環境の統一

- 社内使用 PC の Global での統一 (ThinkPad)
- 社内使用 ソフトウェアの統一 Client for e-business (C4eb)

自宅・出張先・外出先でのセキュリティルール

- 携帯記憶媒体へのファイル保存は暗号化必須
- 電車内の網棚やタクシー等への置き忘れ、居眠り中の盗難、置き引き注意
- 車から離れる場合、PCは必ず携行する
- PCを携行する場合は、"パワー・オフ状態" にする
- 空港で預ける荷物にPCを入れない
- 機密情報、お客様情報等の破棄は、IBMオフィスにて機密情報廃棄処理
- ホテルで提供しているリモートプリンターを利用しない
- 空き巣に注意し、機密性の高い情報やノートブックPCは施錠管理
- 身内の方がIBMと利害関係の企業に勤務する場合は、機密性の高い情報が漏えいしないように、会話、書類の閲覧、複写等に十分気をつける
- 個人所有のPCでIBMビジネスに関わる情報を扱うことは原則不可
- 盗難・紛失などの被害にあった場合は、速やかに報告のこと。

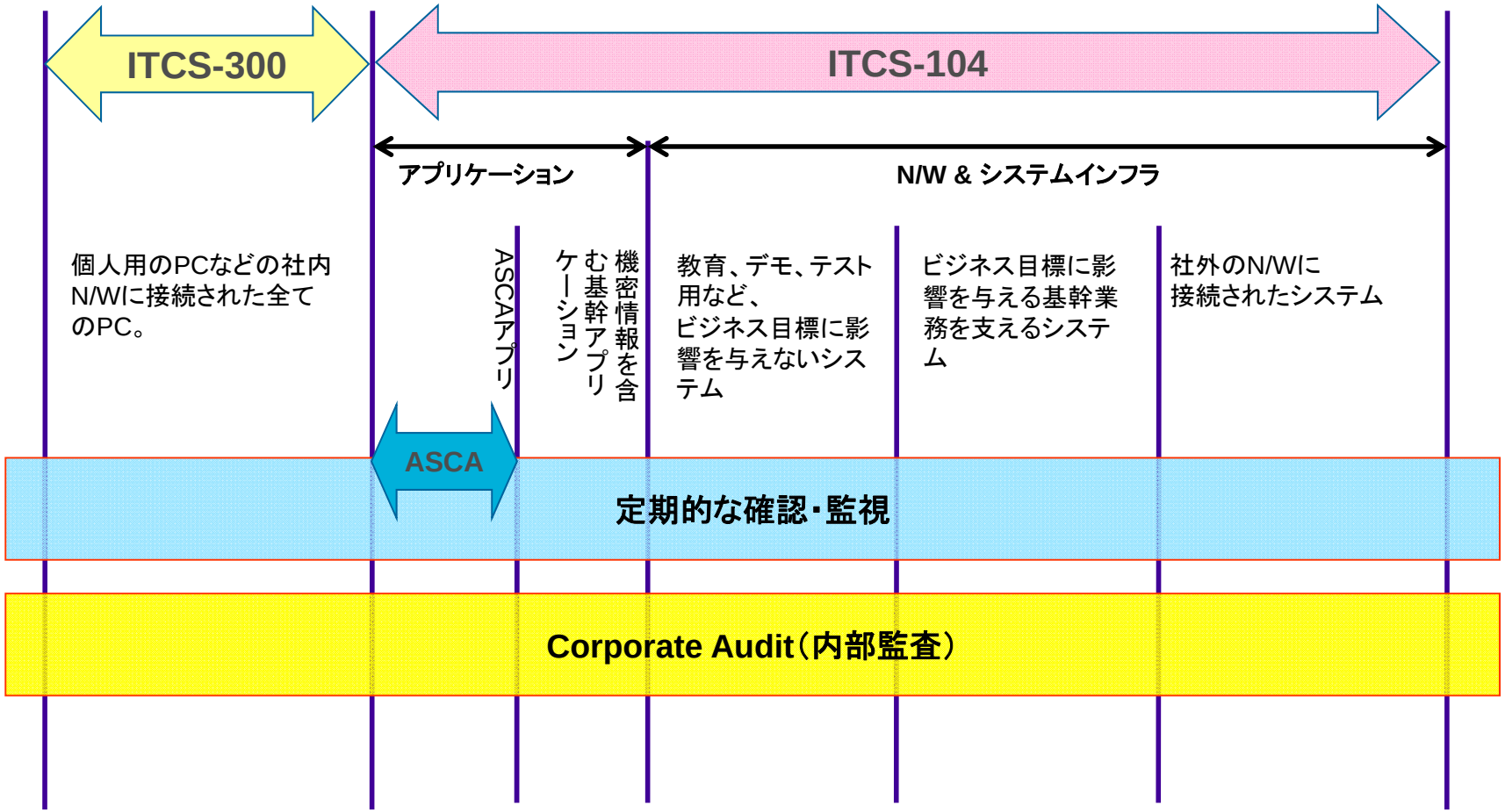
3.グローバルで統一されたルール
ビジネス・コンダクト・ガイドライン（企業行動規範）2015の目次

IBMポリシーや規定のエッセンスを Business Conduct Guideline (BCG) としてまとめ、各人が毎年確認署名をすることにより、43万人が「One」IBM として正しい行動がとれるよう図っています。BCG は社外にも公開されています。

※2015年3月現在

4.ITガバナンス及び監査
スタンダード要件遵守確認サポートフロー

IBMのITセキュリティー標準であるITCS-300とITCS-104にのっとった上で、この要件が常に確実に遵守されているかどうかの確認プロセスが存在します。このプロセスによりその遵守が徹底されます。



ASCA : Application Systems Control & Auditability

4.ITガバナンス及び監査
システム監査

システムの監査は3つの観点で実施されます。1.データ正確性、健全性　2.オペレーションの効率性　3.資産保全のための物理的・論理的なセキュリティーの保全性。

- ビジネス・プロセスの健全性を定期的に検証するためのプログラム

オーディット:
専門部隊(オーディター)が行う監査。監査結果に対して評価(Rating)を行う
- **コーポレート・オーディット**
- **日本IBM内部監査**

CAR (Control Assessment Review) / プロアクティブ・レビュー:
専門部隊(オーディター)が行う監査。結果の評価を行わず、改善点の助言を行う

ピア・レビュー / SACA (Semi-Annual Control Assessment):
プロセス・オーナー自らが行うプロセス・レビュー/自己評価するプログラム

5.社員に対する啓蒙
従業者の認知度の向上と遵守徹底の周知

IBMのセキュリティ強化策は、従業員が普通に業務遂行していればセキュリティ違反は起さない「善意のセキュリティ」が提供されています。しかし、最も重要なのはグループ企業を含む従業員のセキュリティ意識の徹底です。IBMではこの領域に関する教育プログラムを行い、その受講のチェックや完了テストにより、確実に徹底します。

セキュリティー研修（例）

＜対象＞
日本IBM従業員及びグループ会社従業員
（社員、役員、出向者、派遣社員、協力会社社員）

-目次（例）-

- ISMS基本方針
- 昨年情報セキュリティー事故の総括
- セキュリティー重要ポイント
- 昨年の事故分析：PC紛失/盗難、PCの紛失および情報流出の予防
- 昨年の事故分析：委託先による事故、GDにおけるセキュリティー強化
- セキュリティー・ルールの確認と実践
- セキュリティーへの取り組み
- 災害対策－社員安否確認システム－
- IBMのパンデミック対策

・毎年全従業者に受講
・チェックテスト合格
　義務付け

セキュリティーなくして、ビジネスなし！

6.関連会社に対するガバナンス
Security Standard for IT Transitions of Acquisitions

IBMでは、M&AにおけるITセキュリティに関する移行作業について、具体的な期限が設定されています。

買収後6ヶ月

要件の例

調査活動の準備

- ネットワーク境界に対するスキャンの完了及び脆弱性の確認
- Webアプリケーションセキュリティスキャンの実施

オンサイトでの調査

- IT運用プロセス及び手続きのレビューと検証
- 正式に認められた、外部接続ネットワークの構築
- ハードウェア及びビジネスアプリケーションのアセット棚卸しの完了

買収後9ヶ月

要件の例

買収後270日以内

- セルフアセスメントの実施及び改善計画の策定
- Webアプリケーションのソースコードに対するセキュリティスキャン

買収後12ヶ月

要件の例

買収後360日以内

- ネットワーク基盤の標準への準拠完了
- 情報システムの標準への準拠完了
- 役割ごとに必須とされている、セキュリティエンジニアリングトレーニングの完了

監査チーム / M&A DB

今日お話しすること

1.サイバーセキュリティ

1.1 サイバーセキュリィ最新動向
(IBMのレポートより)

1.2 情報セキュリティ管理部門が
直面している課題と対策

2.IoTセキュリティ

2.1 IoTの世界

2.2 IoTセキュリティ最新動向

2.3 アーキテクトの視点から見た考察

ご参考:
IBM ProVIsion No.88 IoT時代のサイバーセキュリティ　今そこにあるリスク
https://www-304.ibm.com/connections/blogs/ProVISION86_90/entry/no88?lang=ja

IoTの世界　デバイスができること

スマートフォン、スマートウォッチ、小型センサーなど、現在は、非常に多くの種類のセンサーが利用可能であり、様々なデータを収集することができます。

デバイスが持つ入出力機能の例　(青字：スマートフォンの機能)

入力

- **位置・標高(GPS)、傾き(水準器)**
- **加速度、歩数**
- **音(マイク)**
- **照度**
- **画像(カメラ)**
- **近接(人、物、液体との距離測定)**
- **磁気・コンパス**
- **温度、湿度、気圧**
- **タッチパネル**

出力

- **光・画像(画面)**
- 赤外線(リモコン)
- **音(スピーカー)**
- **バイブレーター**

小型コンピュータ上でアプリケーションを動かして、デバイスを制御することもできる。

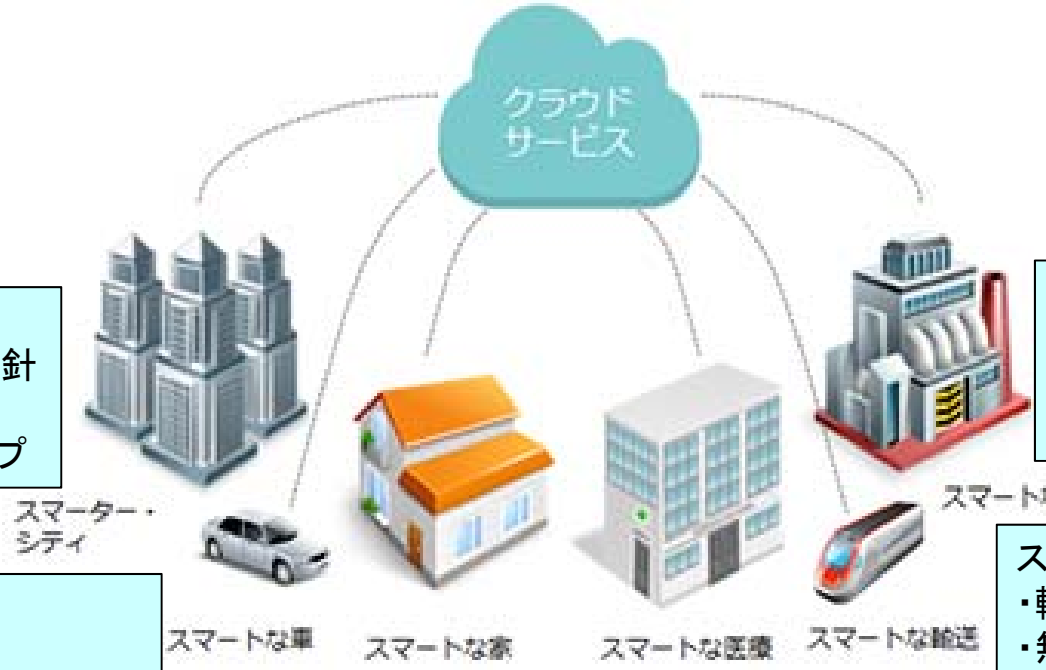
ARM embed　Raspberry Pi　Intel Edison　Intel Galireo




IoTの世界　IoTシステムが新しい価値をもたらす

近年、通信機能を持つ様々なデバイスが登場しています。**デバイスが生成する大量のデータ**から、**分析による新しい洞察**が生まれ、**ヒト、モノ、サービスを結ぶ新しい価値(ビジネス)**が生まれます。

大量のデータ → **分析・活用** → **新しい価値・ビジネス**



スマートグリッド
・ガス・電力の自動検針
・生産・供給調整
・障害時のバックアップ

工場、発電所の自動制御
・生産機器の稼動監視
・障害発生時の自動停止
・原材料、燃料の供給制御

つながるクルマ
・カーナビの高度化
・運転者の好みに合わせた
　エンターテイメント
・運転の補助、自動運転
　(ブレーキ、エンジンの制御)
・故障の通知、予測

つながる家電(家)
・家電機器のリモート制御、節電
・個人の好みに合わせた調節
・高齢者、障害者、子供、ペットの支援

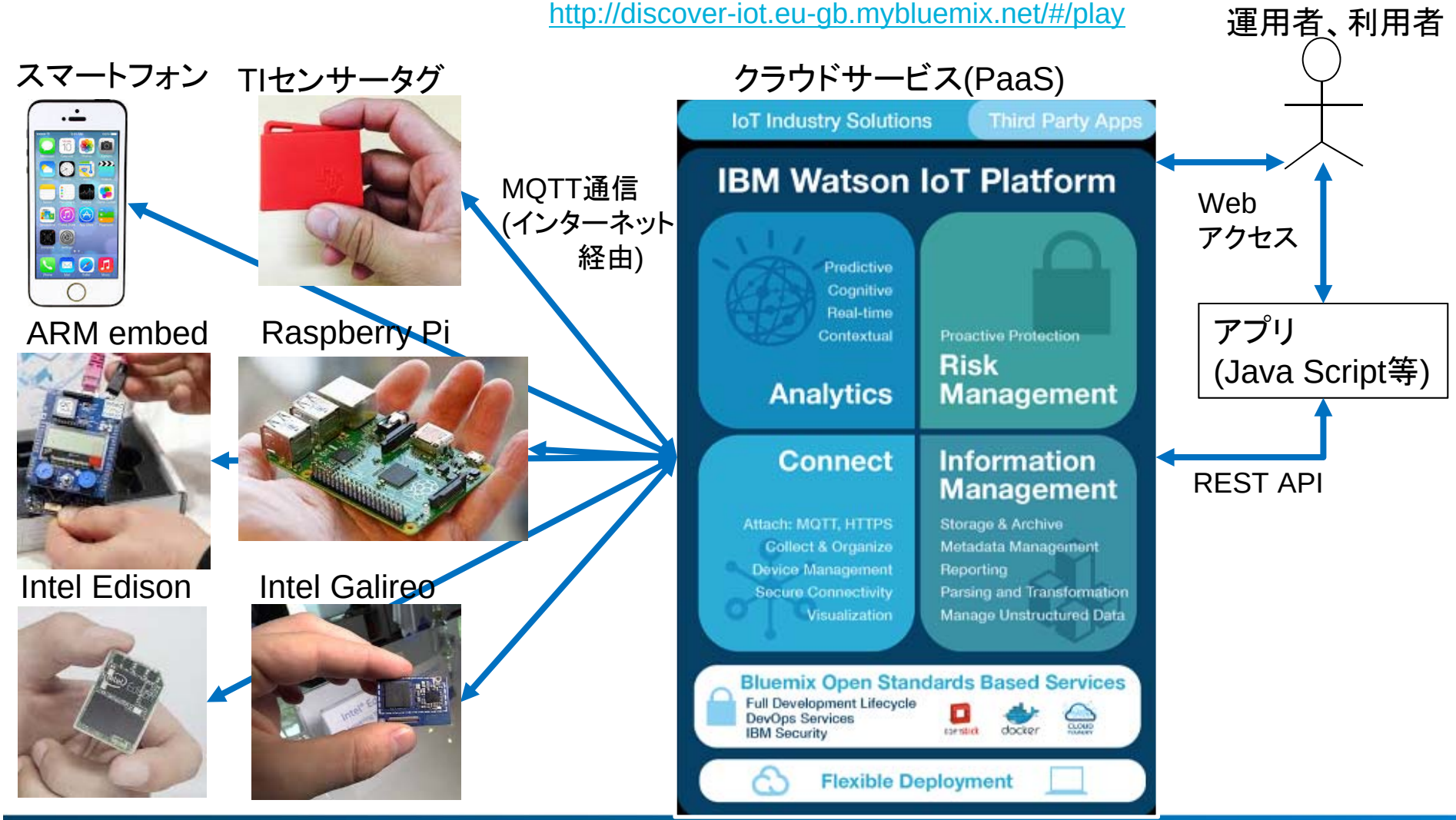
スマートな輸送
・輸送経路、配車の最適化
・無人運転
・ドローンによる無人宅配
・Uber

スマートな医療
・スマートウォッチを用いた健康管理
・リモート医療、無人診療

IoTの世界　IBM Watson IoT Platform

米国IBMは、IoTシステムの開発環境及び実行環境のPaaSとしてIBM Watson IoT Platformを提供しています。

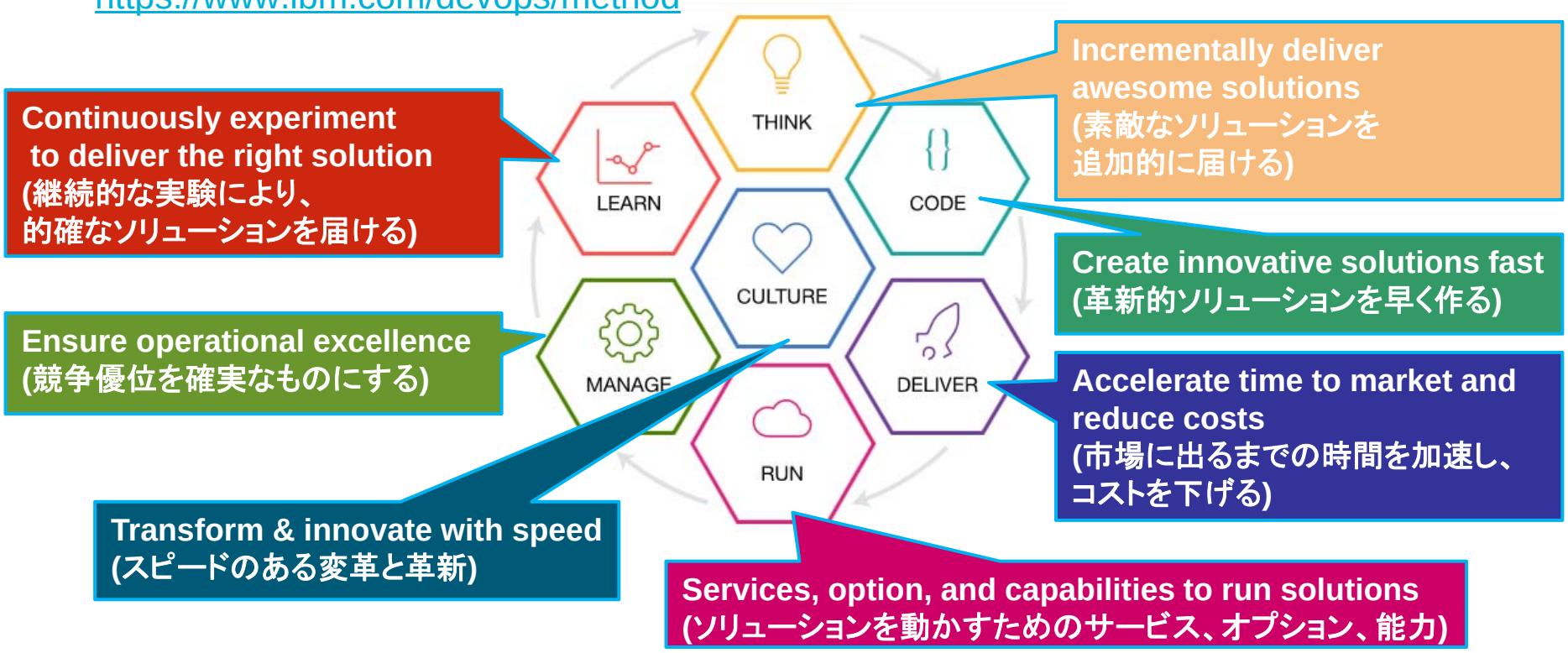
Explore IBM Watson Internet of Things
http://discover-iot.eu-gb.mybluemix.net/#/play



IoTの世界　IBM Bluemix Garage Method

IBM Bluemix Garage Methodは、デザイン思考、リーンスタートアップ、アジャイル開発、DevOps、クラウドのベストプラクティスをまとめたものであり、革新的ソリューションを作って提供するための手法として公開されています。

IBM Bluemix Garage Method
https://www.ibm.com/devops/method



各エリアごとに、事例(Practice)、開発ツール、経験者(Experice)を紹介

今日お話しすること

1.サイバーセキュリティ

1.1 サイバーセキュリィ最新動向
(IBMのレポートより)

1.2 情報セキュリティ管理部門が
直面している課題と対策

2.IoTセキュリティ

2.1 IoTの世界

2.2 IoTセキュリティ最新動向

2.3 アーキテクトの視点から見た考察

ご参考:
IBM ProVIsion No.88 IoT時代のサイバーセキュリティ　今そこにあるリスク
https://www-304.ibm.com/connections/blogs/ProVISION86_90/entry/no88?lang=ja

IoTシステムとセキュリティリスク

様々な「モノ」が通信機能を持ちインターネット経由で情報をやりとりするようになっています。それと同時にセキュリティのリスクが懸念されています。

IoTシステムの例	懸念されるセキュリティリスク
スマートグリッド ・消費電力量の自動収集 ・電力の供給調整、停電時の自動バックアップ	・プライバシーデータの漏洩 ・大規模停電
工場、発電所の自動制御 ・生産ライン機器の稼動監視 ・障害発生時の自動停止 ・原材料、燃料の供給制御	・危険物の悪用(火災、メルトダウン) ・停止による経済的損害
つながるクルマ ・位置情報を用いたサービス、最適経路案内 ・ドライバーの好みに合わせたエンターテイメント ・運転の補助、自動運転(ブレーキ、エンジンの制御) ・故障の通知、予測	・プライバシーデータの漏洩 ・故意による大規模事故
つながる家電(家) ・健康管理 ・家電機器のリモート制御、節電 ・個人の好みに合わせた調節 ・高齢者、障害者、子供、ペットの支援	・プライバシーデータの漏洩 ・家への侵入、火災 ・殺人

乱立するIoTセキュリティガイドライン

現在、様々な団体からIoTセキュリティに関するガイドラインが公開されており、乱立の状況です。新たなガイドライン策定の動きもあり、乱立の状況はしばらく続くと思われます。

- GSMA IoT Security Guidelines
  - http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

GSMA：GSMアソシエーション

- CSA New Security Guidance for Early Adopters of the IoT
  - https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

CSA：非営利法人クラウドセキュリティアライアンス

- The OWASP IoT Top10 Project
  - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

- OTA IoT Trust Framework
  - つながる家の製品、ウェアラブルデバイスのセキュリティ対策のガイドライン
  - https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf

OTA：Online Trust Alliance

- ENISA Security and Resilience of Smart Home Environments
  - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices

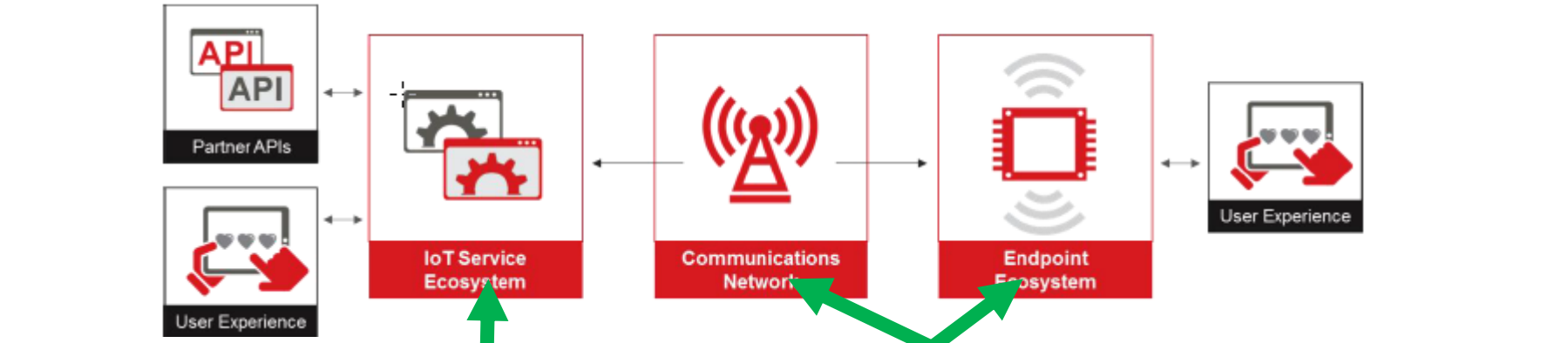
ENISA：欧州 ネットワーク情報セキュリティ庁

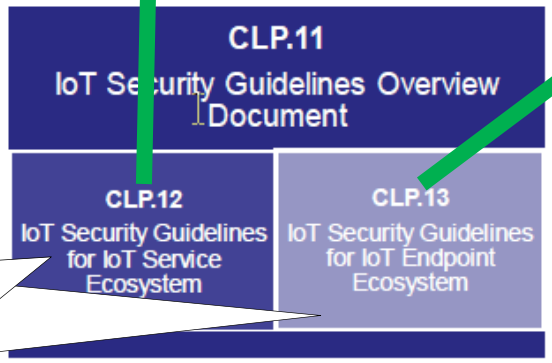
通信業界団体(GSMA)のIoTセキュリティガイドライン　1/2

通信業界団体のGSM Associationは、IoTシステムを3つの部分に分け、各部分において必要となるセキュリティ対策のガイドラインを提供しています。

Using This Guide Effectively

1.IoTシステムのモデルを描く
2.現状のセキュリティ(脅威)モデルを評価する
3.推奨セキュリティ対策を検討する
→ **5.実装&評価する** → **6.再評価&見直しをする**





・Service Model
・Security Model
・FAQ
・Recommendations
- Critical
- High Priority
- Medium Priority
- Low Priority

\+

CLP.14
IoT Security Guidelines for Network Operators

・Network Security Principles
・Privacy Considerations
・Services Provided by Network Operators

出典：GSMA IoT Security Guidelines
(http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)

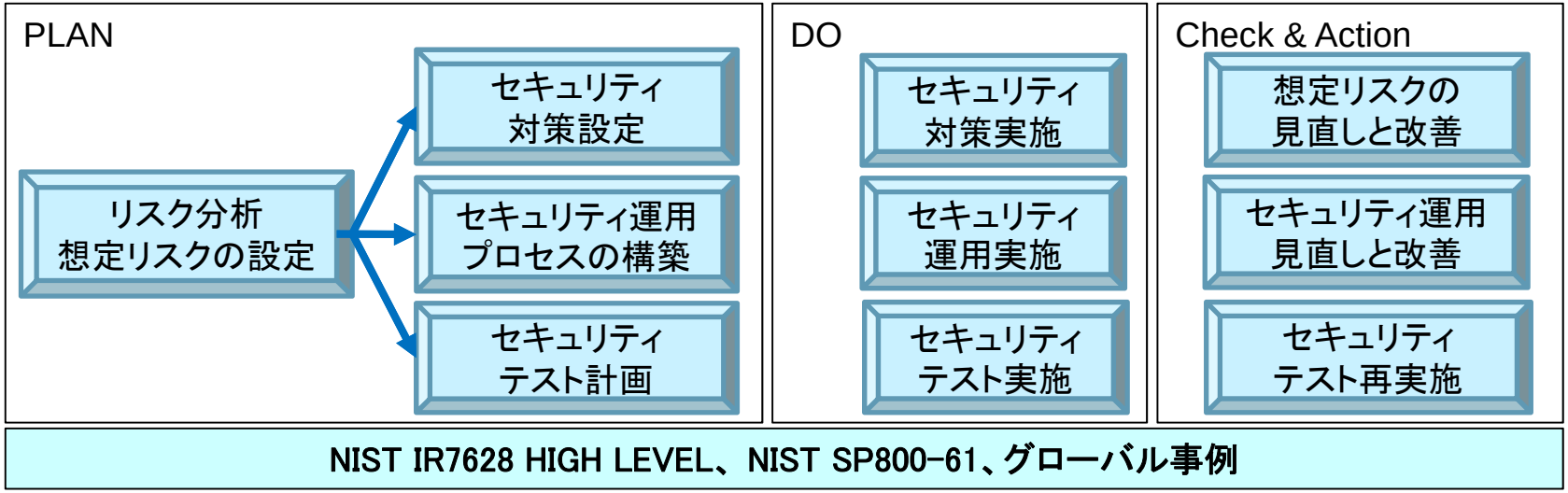
通信業界団体(GSMA)のIoTセキュリティガイドライン　2/2

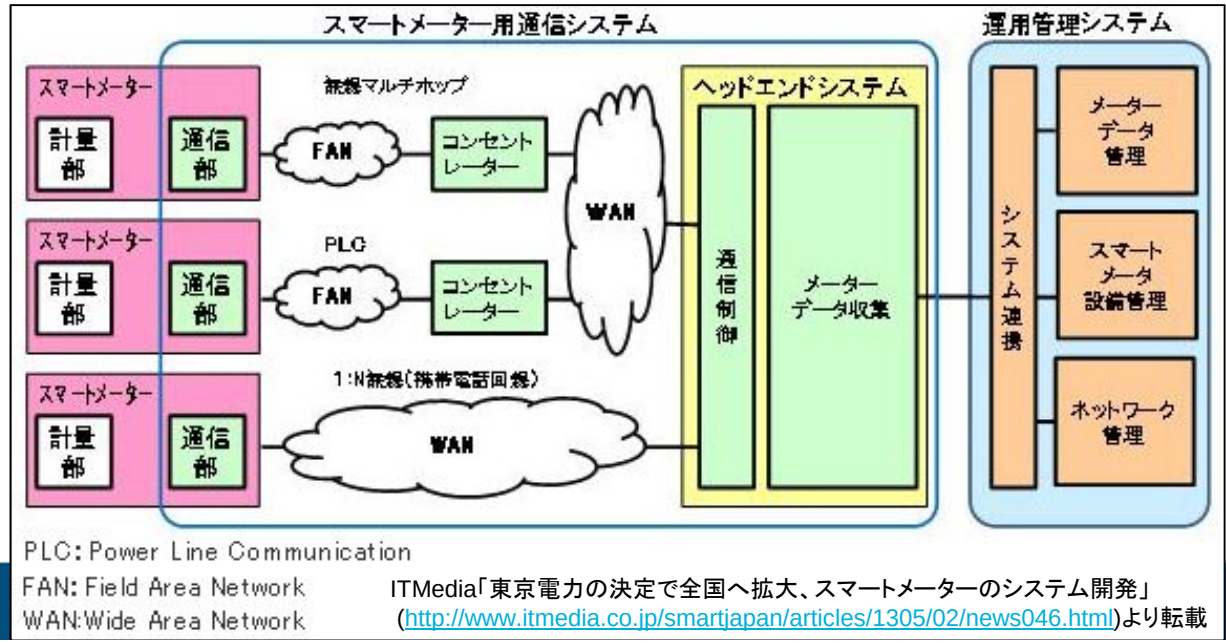
IoT Security Guidelines for Endpoint Ecosystemsにおける
セキュリティモデル、FAQ及び推奨対策(Critical、High Priority)

出典：GSMA IoT Security Guidelines
(http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)

IBMのIoTセキュリティに対する取り組み(スマートメーターシステム)

IBMは、スマートメーターシステムのセキュリティについて、グローバルのフレームワークと知見を活用し、リスクアセスメント、セキュリティ対策立案及びペネトレーションテストによる検証を行っています。





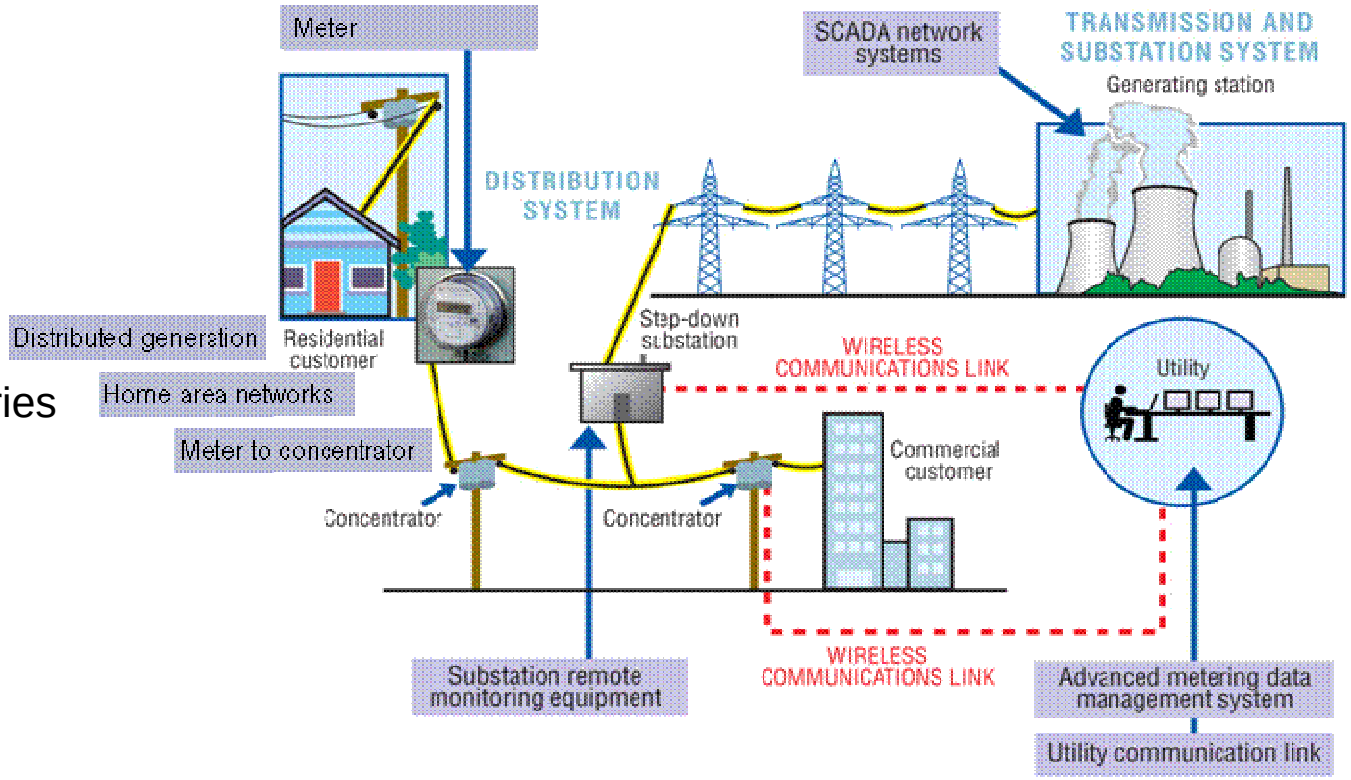
ITMedia「東京電力の決定で全国へ拡大、スマートメーターのシステム開発」(http://www.itmedia.co.jp/smartjapan/articles/1305/02/news046.html)より転載

IBMのIoTセキュリティに対する取り組み(電力制御システム)

IBMは、電力制御機器のセキュリティについても、業界のガイドライン等を用いたセキュリティアセスメント、対策立案を行っています。

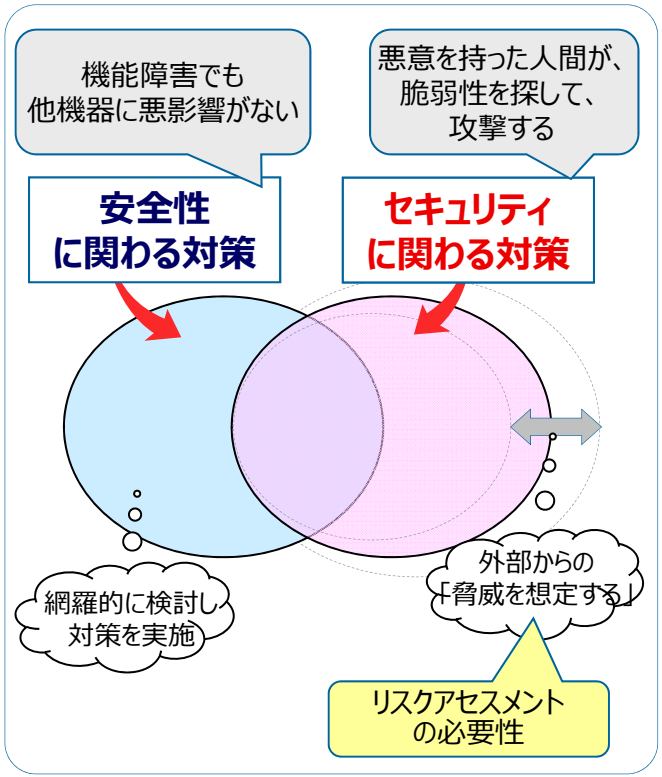
アセスメント・対策立案に適用するガイドライン類

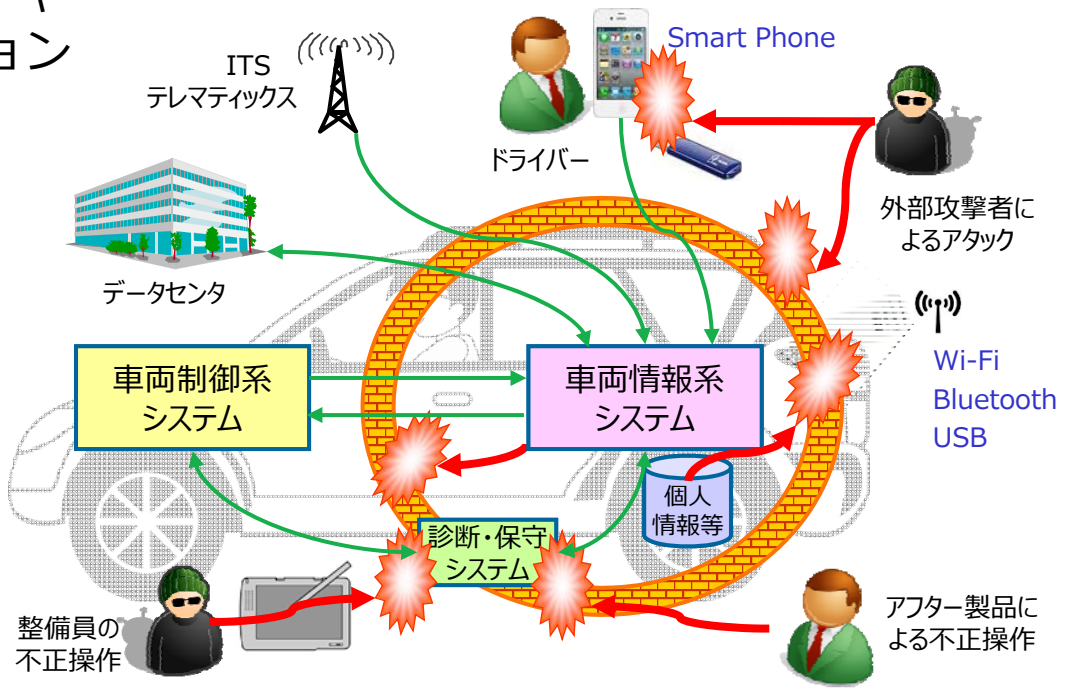
– The ISO/IEC 2700 Series
– IEC 62351-1/8
– ISA/SP99 – IEC62443
– NERC CIP 001 – 009
– NIST SP 800-53
– NIST SP 800-82
– NIST IR 7628
– US DHS (Department of Homeland Security)
– US NRC Regulatory Guide 5.71
– API Standard 1164 Pipeline SCADA Security
– AGA Standard 12 “Cryptographic Protection of SCADA”

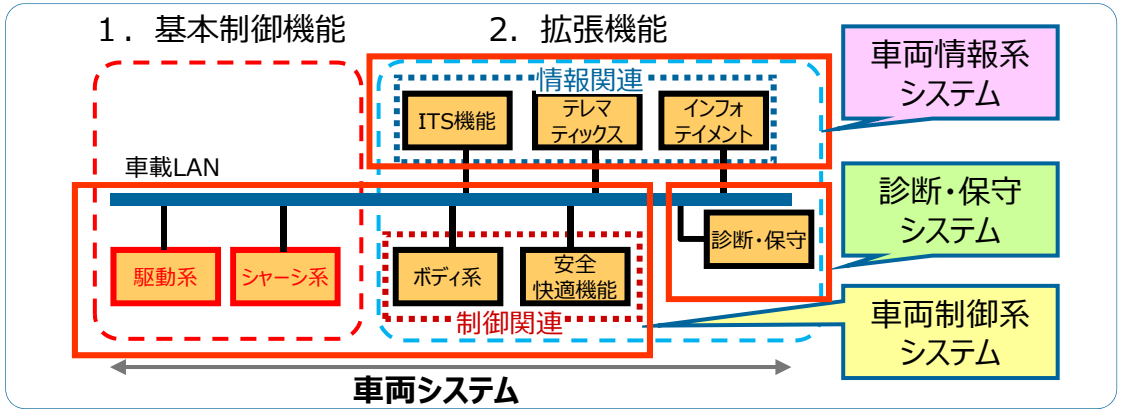


IBMのIoTセキュリティに対する取り組み(自動車分野)

IBMでは、つながるクルマのセキュリティについて、特定の車載IT機器に関わる脅威に対して、リスクアセスメントやセキュリティ診断（ペネトレーションテスト）を行った事例があります。







今日お話しすること

1.サイバーセキュリティ

1.1 サイバーセキュリィ最新動向
(IBMのレポートより)

1.2 情報セキュリティ管理部門が
直面している課題と対策

2.IoTセキュリティ

2.1 IoTの世界

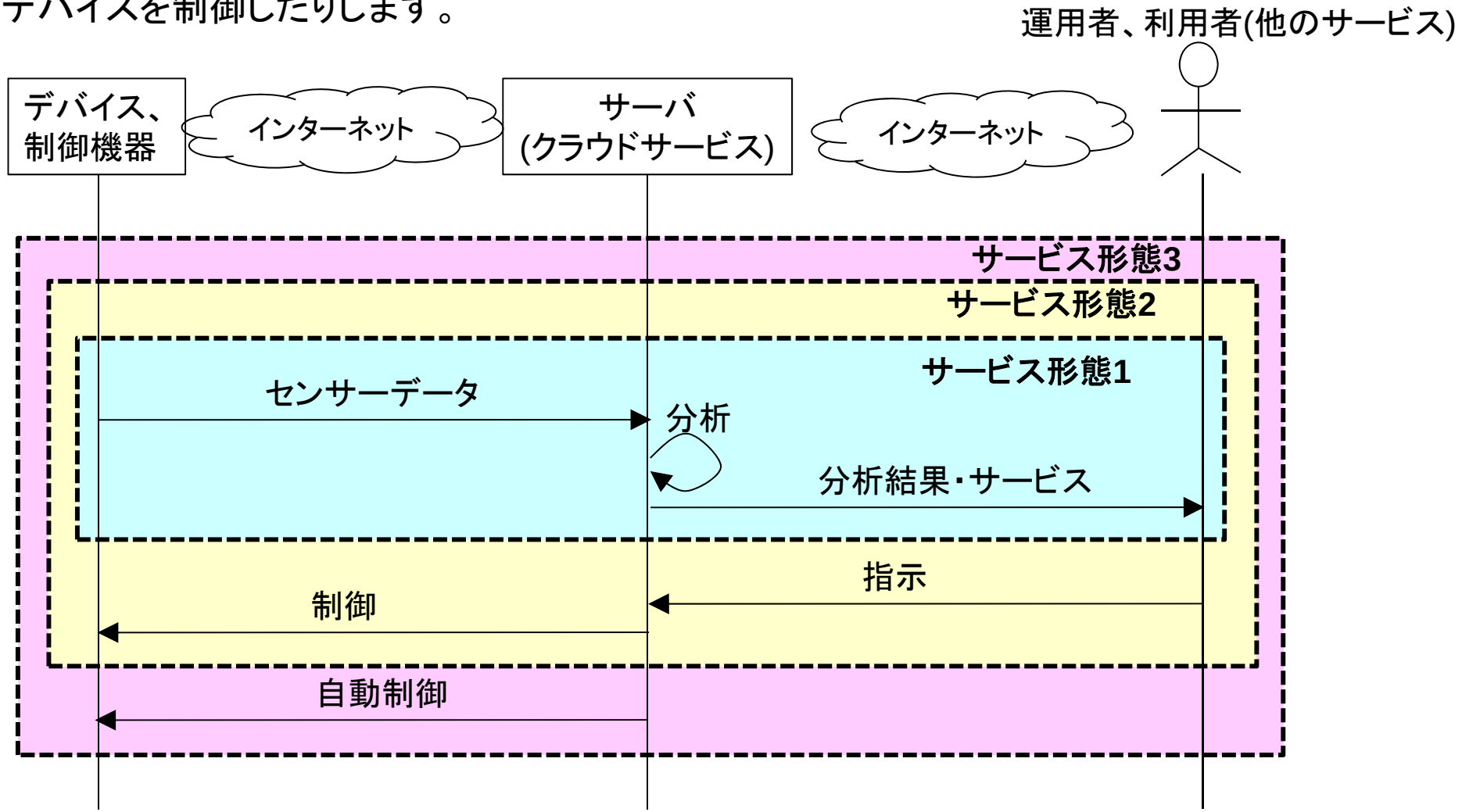
2.2 IoTセキュリティ最新動向

2.3 アーキテクトの視点から見た考察

ご参考:
IBM ProVIsion No.88 IoT時代のサイバーセキュリティ　今そこにあるリスク
https://www-304.ibm.com/connections/blogs/ProVISION86_90/entry/no88?lang=ja

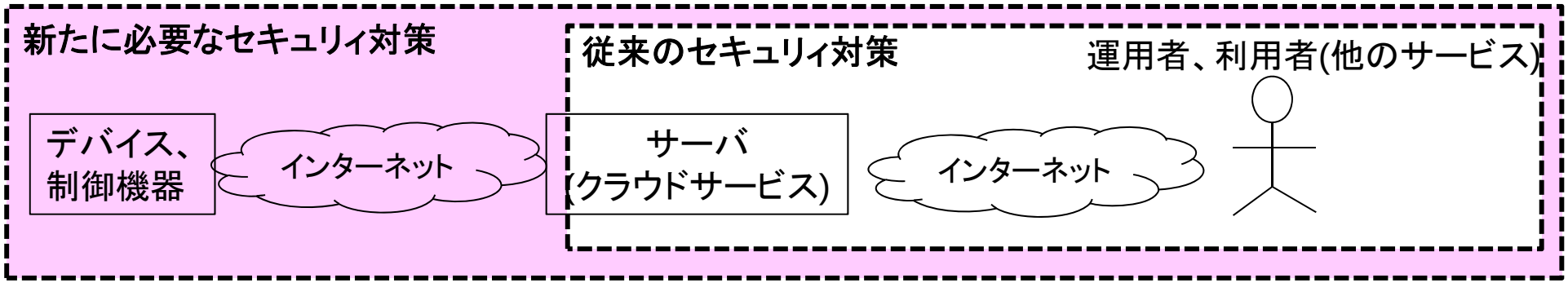
IoTシステムのハイレベル・アーキテクチャー

IoTシステムは、デバイス、サーバ、利用者がインターネットで接続されたシステムであり、
デバイスからのデータを分析・加工した結果を利用者に提供したり、分析結果に基づいて
デバイスを制御したりします。



IoTシステムで新たに必要になるセキュリティ対策

IoTシステムは、デバイスや制御機器がインターネットを介してサーバに接続してデータのやりとりや制御を行う点が異なります。この部分及びシステム全体のセキュリティ対策の考慮が新たに必要になります。

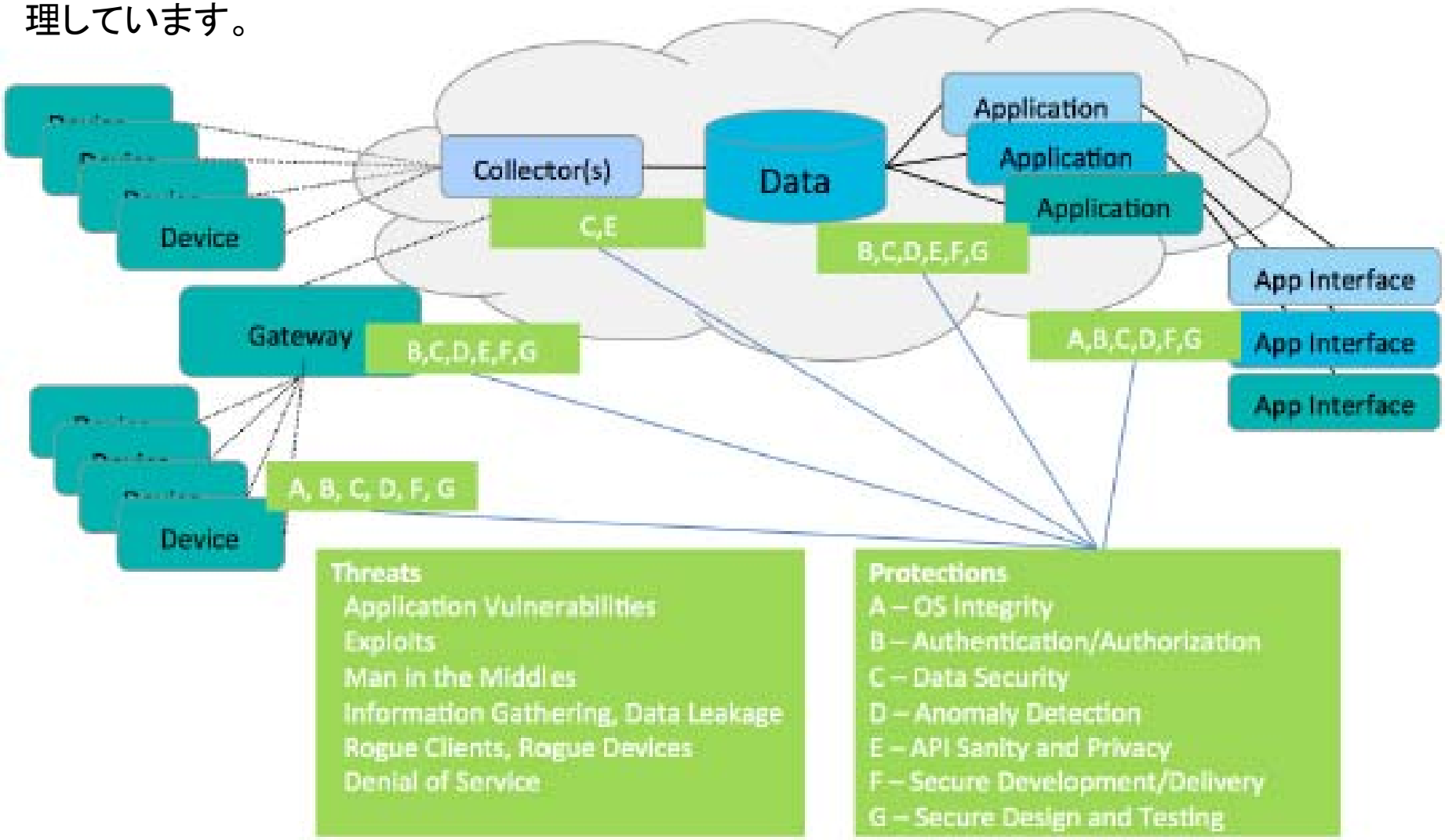


IoTシステムで新たに必要になるセキュリティ対策

- デバイス～サーバ間のネットワーク接続におけるセキュリティ対策
  (接続プロトコルにこれらの対策が実装されているか要確認)
  - 認証、アクセス制御、ログ取得・分析
  - 暗号化通信
  - データ内容の保障(ディジタル署名)
- デバイスにおけるセキュリティ対策
  - 物理的セキュリティ：**設置場所のセキュリティ、デバイスの封印、回路ハッキングに対する対策**
  - デバイスへのアクセスにおける対策：認証、アクセス制御、(ログ取得・分析)
  - **脆弱性が発見された際の対処：ファームウェア、ソフトウェアの更新**
- **IoTシステム全体(End-to-End)のセキュリティ対策**

(参考)IoTシステムのアーキテクチャーと必要なセキュリティ対策 1/2

IBMは、Thought Leadership White Paper ‘IBM Point of View: Internet of Things Security’ において、IoTシステムにおけるアーキテクチャーと必要なセキュリティ対策を整理しています。



(参考)IoTシステムのアーキテクチャーと必要なセキュリティ対策 2/2

IBMは、Thought Leadership White Paper ‘IBM Point of View: Internet of Things Security’ において、IoTシステムにおけるアーキテクチャーと必要なセキュリティ対策を整理しています。

- **モノのメーカー：セキュアなIoTシステム及びデバイスの設計と製造**
  - **セキュリティ設計** (セキュリティを考慮した開発プロセス、多階層防御、フェイルセーフの考慮)
  - **プライバシー設計** (従業員データ及び個人IDに紐づくデバイスIDの分離)
  - **セキュリティテスト** (コード分析、脆弱性診断テスト、侵入テスト、物理環境から人のコミュニケーションまでを含めた全体テスト)
  - **継続的な出荷モデル** (出荷後の脆弱性対応、デバイスソフトウェアの更新)
  - **サプライチェーン全体のセキュリティ** (部品供給者のアセスメント、仕様文書に基づく認定)

- **モノの運用者：IoTシステムのセキュアな運用**
  - **デバイスの堅牢化** (多階層防御、障害箇所の切り離し)
  - **通信経路の安全確保** (デバイス～ITシステム間の全通信経路の安全確保)
  - **利用パターンの監査及び分析** (検知、既存のログ分析技術の活用)
  - **最新のセキュリティ環境の維持** (技術とプロセスの組み合わせ、デバイスの運用保守におけるセキュリティ)
  - **信頼できる保守方法の確立** (設置・保守における既存ガイドの活用、インシデント対応プロセスの定義)

出典：IBM POINT OF VIEW: INTERNET OF THINGS SECURITY
(http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=RAW14382USEN&attachment=RAW14382USEN.PDF)

IBM Secure Engineering Framework

IBMは、セキュリティを考慮したシステム開発プロセスとして、IBM Secure Engineering Frameworkを社内のガイドラインとして運用しています。

Secure Engineering Framworkの概要

Section 1: プロジェクト計画	
	Requirement 1: PMに対してセキュリティ教育を確認する
	Requirement 2: プロジェクト計画にセキュリティチェックポイントを組み込む
	Requirement 3: 脅威モデルを開発する時間を確保する
	Requirement 4: 開発中にセキュリティ検証テストを実施する
	Requirement 5: 展開前にセキュリティリリースチェックポイントを実施する
	Requirement 6: セキュリティ開発計画を文書化する
Section 2: ソフトウェアサプライチェーンのセキュリティ	
	Requirement 7: 承認されたサードパーティコンポーネント及びアセットだけを利用する
	Requirement 8: 脅威モデルにおいてサードパーティから来たコンポーネントにおいてリスクアセスメントを実施する
	Requirement 9: 開発期間にサードパーティ製コンポートネントの適切なセキュリティフィックスを組み込む
Section 3: アプリケーション開発要件	
	Requirement 10: アプリケーションにおける脅威モデルを実施する
	Requirement 11: アプリケーションをデフォルトセキュアの状態で出荷する
	Requirement 12: セキュアコーディングのベストプラクティスを適用する
	Requirement 13: 重要なセキュリティ機能に対してマニュアルコードレビューを実施する
Section 4: 脆弱性アセスメント及びテスト	
	Requirement 14: 開発中にアプリケーションのセキュリティ脆弱性アセスメントを実施する
	Requirement 15: プライバシー影響アセスメントを実施する
	Requirement 16: セキュリティ課題に対するソースコードスキャンを行う
	Requirement 17: CVSSを使って脆弱性アセスメントを行う
Section 5: プロジェクトチームメンバーに対する教育要件	
	Requirement 18: 開発チームのセキュリティ教員をトラッキングする
	Requirement 19: アーキテクトに対して最低限のセキュリティ教育を行う
	Requirement 20: セキュアエンジニアリングの本質
Appendix A: 脅威モデリングのプロセス	
Appendix B: 教育及びスキル更新のリソース	
Appendix C: 用語集	

参考: IBM Redpaper 'Security in Development: The IBM Secure Engineering Framework' (http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf)

システムに求められる要求(IBMの分類)

IBMは、情報システムに求められる要件を機能要求と非機能要求とに分類しています。セキュリティは非機能要求の一つとして位置づけられています。

機能要求 ユーザが仕事を実行するのに必要な機能（どのように達成されるのか(How)とは違う）

非機能要求 ソリューションが満たすべき品質又は制約

- **品質** ソリューションがサポートすべき期待と特性
  - **実行時品質** ソリューションの稼動時に判断されるSLR(テストで検証可能)
    - パフォーマンス・キャパシティ
    - 可用性
    - セキュリティ
    - 運用容易性
    - ユーザビリティ
    - アクセシビリティ
  - **非実行時品質** 開発，保守、運用などに関する要求(長期に渡る測定が必要)
    - 可搬性
    - 保守容易性
    - 管理容易性
    - 拡張性
    - データの完全性
    - 環境性・安全性
    - 効率性
    - 信頼性
- **制約** ソリューションに課せられた制限または仕様
  - **ビジネス制約** ビジネス上の制約
    - 法規制
    - 組織的制約
    - 地理的制約
    - リスク選好性
    - 市場因子
    - 時間
    - 資源(人・予算)
    - スコープ
  - **テクノロジー制約** 技術上の制約
    - 既存の基盤
    - 開発スキル
    - 最新技術
    - IT標準
    - 実装制約

将来要求 将来、追加・変更し得る要求

要求開発の視点からの考察：ITの技術革新と機能要求、非機能要求

これまで、技術革新が起こるたびに、機能的側面が先行して注目され、技術が普及するにつれて非機能的側面が不安視され目が向けられる傾向がありました。IoTにおいてもこの傾向が現れていると考えられます。

過去の技術革新

1990年代前半　ネットワーク、オブジェクト指向、ダウンサイジング、マルチメディア
1995年インターネット (Windows 95)
2000年頃　e-ビジネス
2004年頃　SOA、Webサービス、グリッドコンピューティング
2005年頃　仮想化
2008年頃　クラウド・コンピューティング

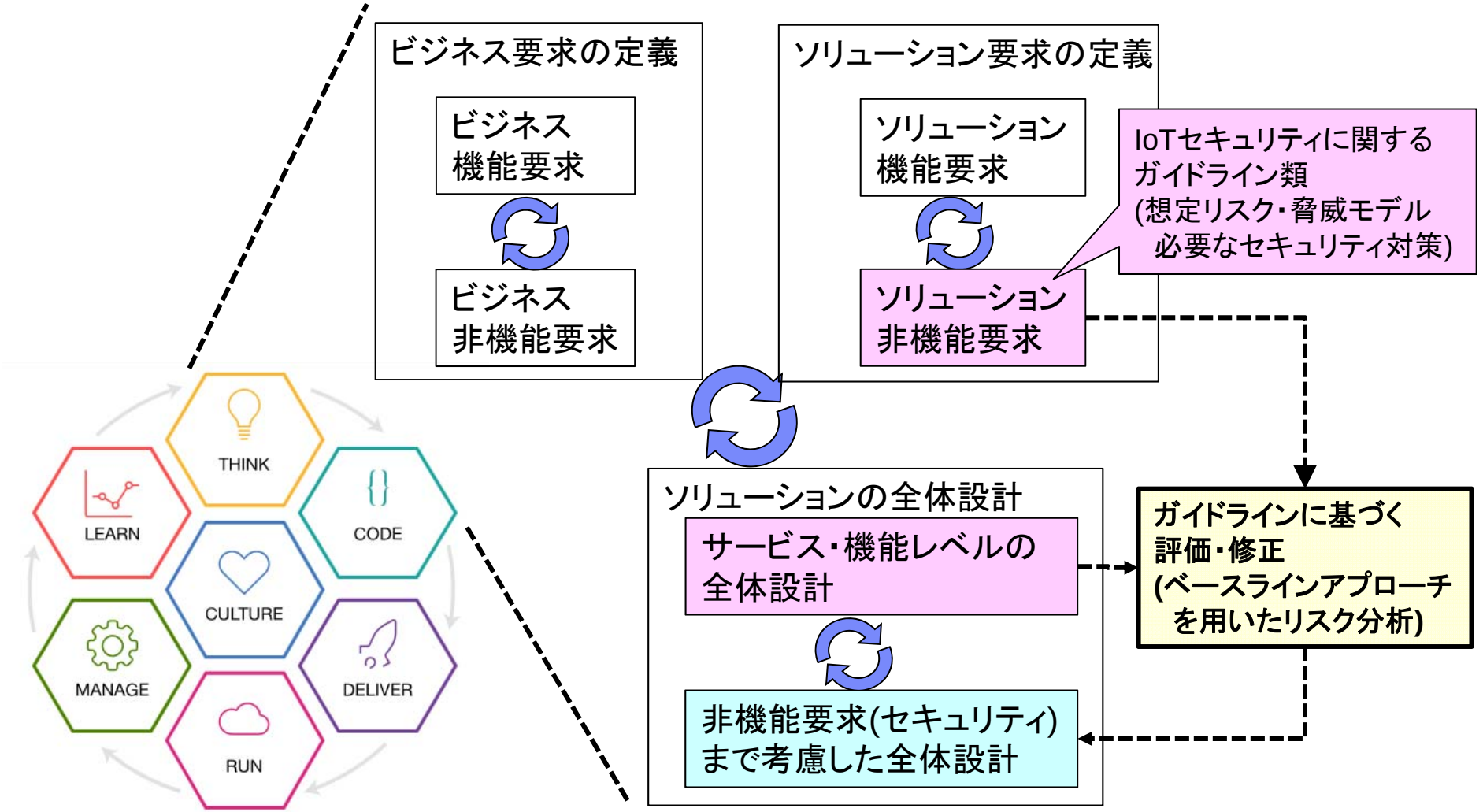
そのたびに繰り返されてきた歴史

	機能的側面 (何ができるか?)	運用的・非機能的側面 (品質・制約)
ビジネス・業務レベル ソリューション・技術レベル	「xxxxができるようになる」 「安い」 「新しい価値が生まれる」 「これまでのシステムはもう古い。 全てxxxで置き換わる」	「xxxの面は大丈夫なのか?」 「xxxまで考えると、結果的に高くつく」 「結局使えない」「バズワードだ」 「要は使い分けだ」

新しい技術が知られるにつれ、議論が夢から現実に落ち着く

アーキテクチャー設計の視点からの考察：セキュリティに対するアプローチ

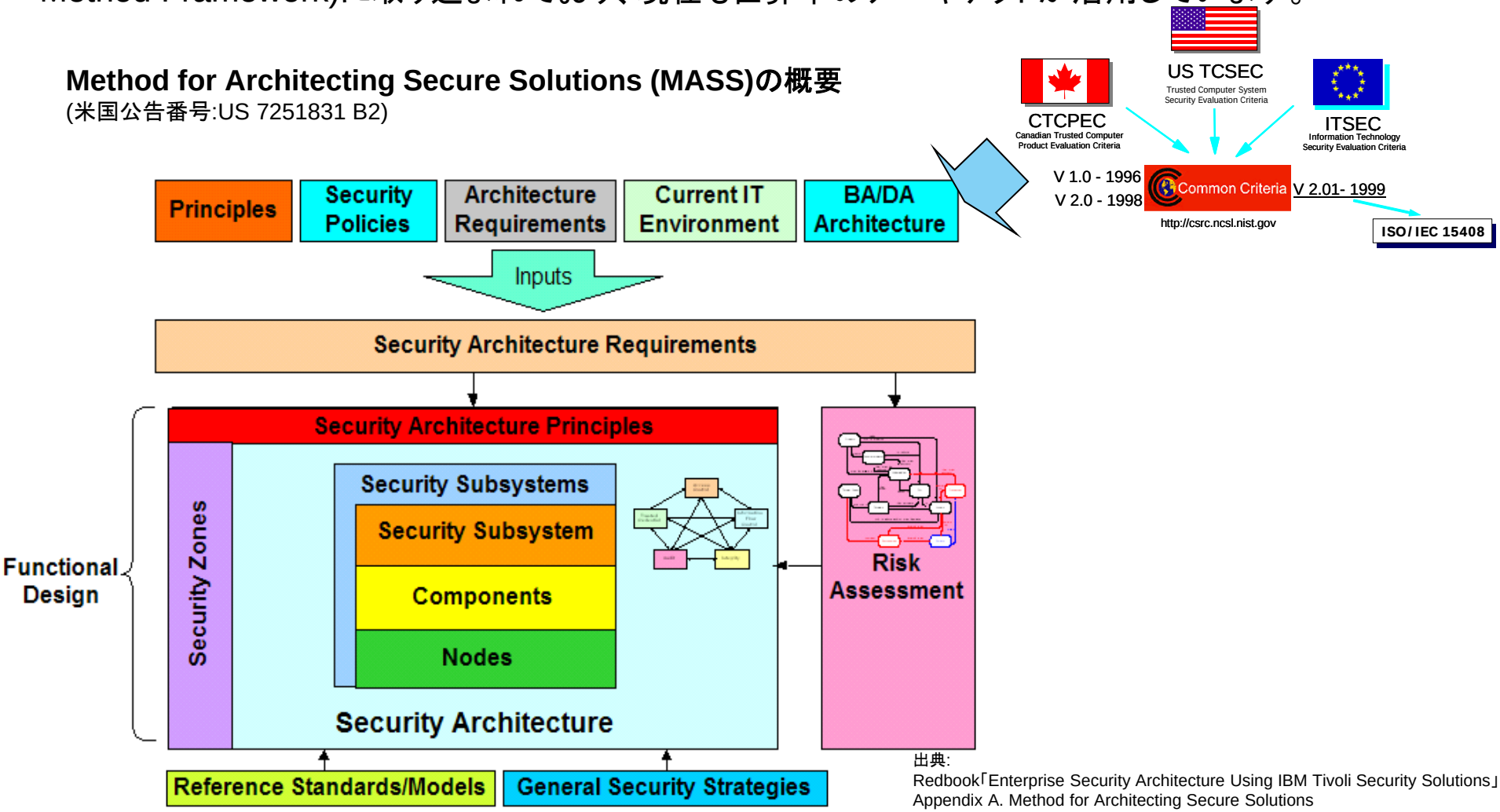
アーキテクチャー設計の技法では、機能レベルのアーキテクチャーを非機能要求の観点から評価・修正することで、非機能要求まで満たすアーキテクチャーを設計するアプローチが行われています。この考え方はIoTシステムのセキュリティ設計にも適用可能です。



(参考)IBMのセキュリティアーキテクチャー設計手法

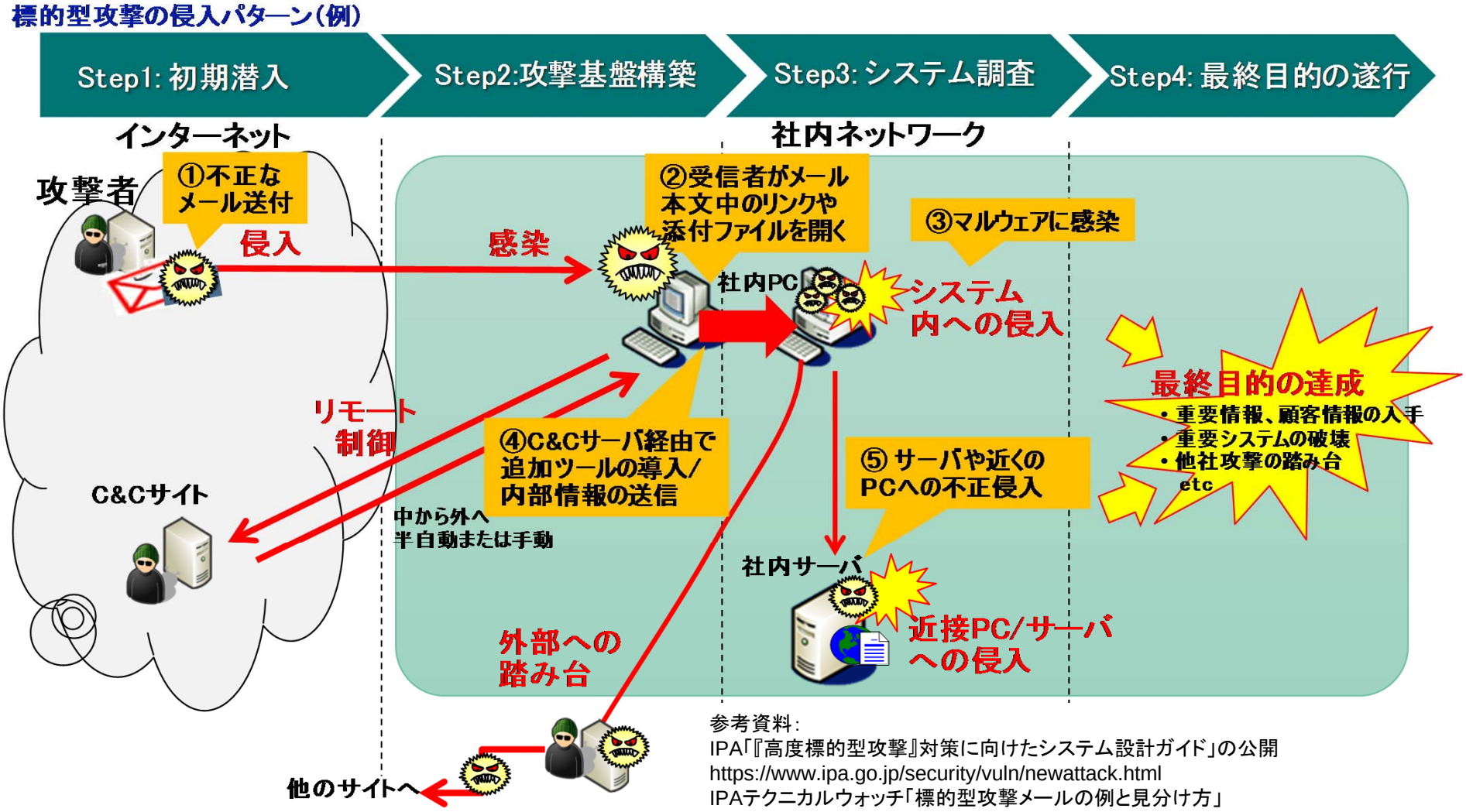
IBMは、2001年にMethod for Architecting Secure Solutions (MASS)というセキュリティアーキテクチャー設計手法を確立しました。MASSは、IBM Globalのアーキテクチャー設計手法の体系(Unified Method Framework)に取り込まれており、現在も世界中のアーキテクトが活用しています。

Method for Architecting Secure Solutions (MASS)の概要
(米国公告番号:US 7251831 B2)



出典:
Redbook「Enterprise Security Architecture Using IBM Tivoli Security Solutions」
Appendix A. Method for Architecting Secure Solutions
(http://www.redbooks.ibm.com/redbooks/pdfs/sg246014.pdf)

(参考)脅威モデルの例



参考資料:
IPA「『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開
https://www.ipa.go.jp/security/vuln/newattack.html
IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」
http://www.ipa.go.jp/security/technicalwatch/20150109.html
IBM「標的型攻撃を防ぐお勧め対策」
http://www-935.ibm.com/services/jp/ja/it-services/security-solutions-2q2012.html

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM **Security**

Intelligence. Integration. Expertise.