さまざまなセキュリティ課題に取り組むITU-Tの活動トピックと今後 ～ ITU-T SG17 1月会合を踏まえて ～

2019年3月19日
株式会社KDDI総合研究所
三宅　優

略歴

■ 職歴、研究歴
- 国際電信電話（株）入社　KDD研究所配属
  - インターネット、通信プロトコル、ネットワークセキュリティの研究

■ 現職
- （株）KDDI総合研究所　スマートセキュリティグループ　GL
- KDDI（株）　技術開発戦略部　（兼務）

■ 主な標準化活動
- ITU-T SG17（Security）
  - 副議長、SG17/WP1（Telecommunication Security）議長
- ITU-T FG NET-2030（Focus Group on Networking 2030）
  - 副議長
- その他
  - TTCセキュリティ専門委員会　委員長
  - oneM2M
  - GSMA

講演内容

1. 通信事業者におけるサイバーセキュリティ対策の取り組み

2. ITU-T SG17におけるセキュリティ標準化活動
   - 2019年1月会合までのトピックを中心的に

1. 通信事業者における サイバーセキュリティ対策の取り組み

通信の秘密への対応

通信の秘密

■日本国憲法

- 第三章　国民の権利及び義務
- 第二十一条　　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
- ○２　　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

■電気通信における通信の秘密

- 憲法第21条の通信の秘密は、公権力による積極的知得行為の禁止と通信業務従事者による漏洩行為の禁止という二つの面を定めたもの
- 電気通信事業法などでは、通信内容を通信当事者以外の第三者が正当な理由なく故意に知ったり、自己又は他人のために利用したり、第三者に漏えいすることに対して刑事罰を定めている
- 電気通信事業者の取扱中に係る通信の秘密については電気通信事業法（第4条・第179条）、有線電気通信における通信の秘密は有線電気通信法（第9条・第14条）、無線通信における通信の秘密は電波法（第59条・第109条）により通信の秘密はそれぞれ罰則をもって保護されている

通信の秘密の侵害

■侵害の3類型

以下の3類型に大別されている。

1. 知得：積極的に通信の秘密を知ろうとする意思のもとで知得しようとする行為
2. 窃用：発信者又は受信者の意思に反して利用すること
3. 漏えい：他人が知り得る状態に置くこと

知得や窃用には、機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る。

特定の条件（攻撃等と判断できるもの）を検知して、それを自動的に処理する（フィルタリングする）ことは、通信の秘密を侵害

通信当事者の同意

■同意の条件

通信当事者の有効な同意がある場合には、通信当事者の意思に反しない利用であるため、通信の秘密の侵害に当たらない。ただし、以下の理由から、原則として契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されていない。

1. 約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまない。
2. 事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となる。

ただし、マルウェア感染防止のための対策等の対応については、契約約款に基づく事前の包括同意であっても、一定の条件の下においては、有効な同意と考えられている。

違法性阻却事由

■通信の秘密を侵すことが許容されるケース

通信当事者の同意を得ることなく通信の秘密を侵した場合であっても、以下のケースに該当する違法性阻却事由がある場合は、例外的に通信の秘密を侵すことが許容されるとしている

- 正当防衛（刑法第36条）
- 緊急避難（刑法第37条）
- 正当行為（刑法第35条）

緊急時に行われる対策については、一般的に、正当防衛、緊急避難の要件を満たす場合には通信の秘密の侵害について違法性が阻却される。

違法性阻却事由があると考えられる事例

■緊急避難が認められると整理された事例

① 人命保護の観点から緊急に対応する必要のある電子掲示板等での自殺予告事案について、ISPが警察機関に発信者情報を開示する場合

② ウェブ上において流通し得る状態に置かれた段階で児童の権利等に重大かつ深刻な法益侵害の蓋然性（がいぜんせい）があるといえる児童ポルノに対するブロッキングを行う場合

■正当業務行為が認められると整理された事例

① 電気通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為

② ISPがルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為

③ ネットワークの安定運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）

ガイドラインの作成

■タイトル
- 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン

■策定者
- インターネットの安定的な運用に関する協議会
  - 一般社団法人日本インターネットプロバイダー協会
  - 一般社団法人電気通信事業者協会
  - 一般社団法人テレコムサービス協会
  - 一般社団法人日本ケーブルテレビ連盟
  - 一般財団法人日本データ通信協会テレコム・アイザック推進会議

■発行日
- 初版： 2007年5月30日
- 第5版： 2018年11月30日

■作成の目的
- 電気通信事業者がDoS 攻撃等のサイバー攻撃、マルウェアの感染拡大及び迷惑メールの大量送信及び壊れたパケット等（以下、大量通信等）を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料として作成

通信事業者におけるサイバー攻撃対策（例）

■攻撃通信への対応

以下の事例においては、攻撃が確認できた場合には通信の遮断が可能としている

① 被害者から申告があった場合
- 明確に攻撃と判断できる通信、異常と判断できる場合に機械的に遮断

② 事業者設備に支障が生じる場合
- ルータやDNSサーバに支障が起きると考えられる場合の通信の制御、不正なホストへのアクセスをDNSの返答で制御、DNSamp対策としての特定ポート番号の通信遮断、等

③ 送信元設備の所有者の意思と関係なく送信されるサイバー攻撃等の場合
- サイバー攻撃等を行っている契約者を特定して対応の要請や通信の遮断を実施、送信元詐称通信の遮断、壊れたパケット等の破棄、マルウェア増加の原因となるトラフィックの遮断、網内トラフィックの現状把握、サイバー攻撃等への共同対処、等

■迷惑メール等への対応

① 送信元詐称メールの受信拒否

② ブラックリストとの突合に基づくユーザへの注意喚起

③ 迷惑メールフィルタリングサービスにおけるフィルタ定義の共有

④ SMTP認証の情報を悪用した迷惑メールへの対処

迷惑メール対策

迷惑メール（スパムメール）

■迷惑メールとは
- 事前に許可していない広告メール等を無差別・大量に送信されるメール
- スパムメールとも呼ばれる

■別の呼び方
- UCE (Unsolicited Commercial Email)：勝手に送られてくる広告メール
- UBE (Unsolicited Bulk Email)：勝手に送られてくる大量メール

■内容
- 広告（出会い系、アダルトサイト、違法なモノの販売、学位の販売、オンラインカジノ、等）
- 株の情報（株価操作）
- 架空請求詐欺
- フィッシングサイトへの誘導
- ウイルス配布（ランサムウェアを含む）

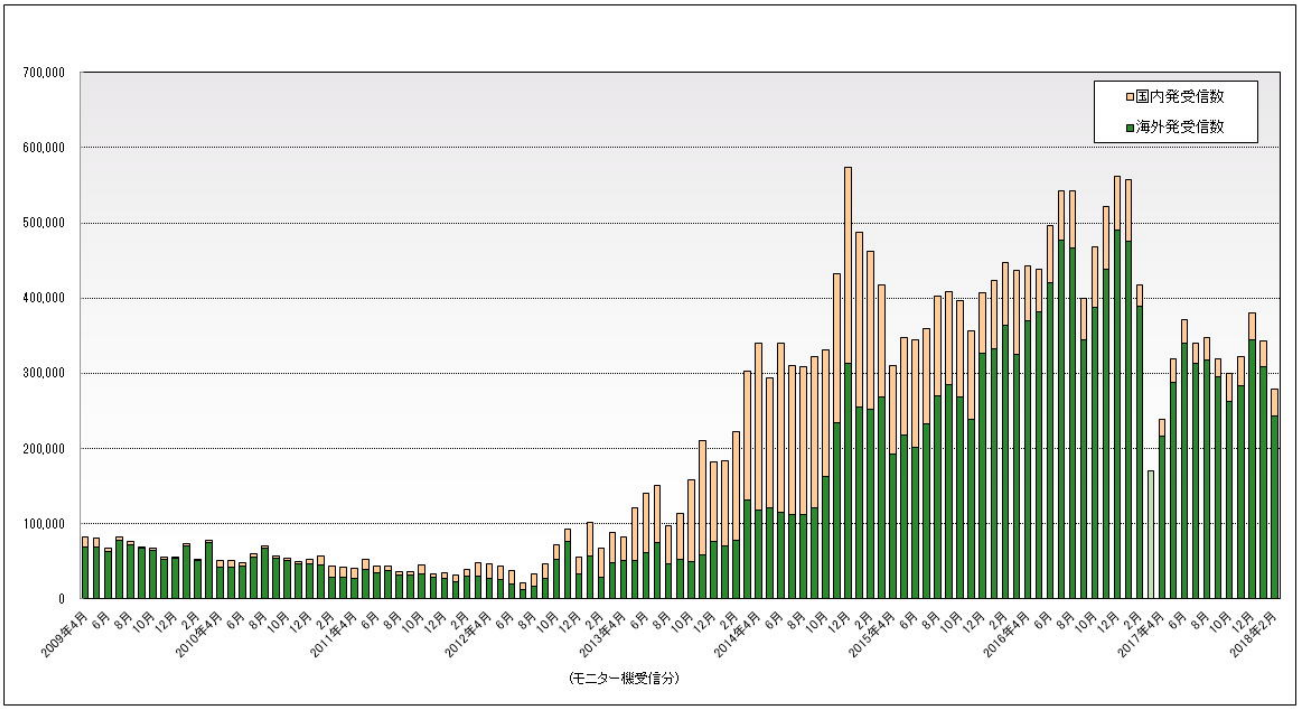
迷惑メールの具体的な被害

- **利用者の視点：**
  - ウィルスメールのようにプログラムや他のコンピュータに被害をおこす。
  - メールを大量に受信することにより、ユーザのメール受信容量がパンクし、受信できなくなる。本来のメールが迷惑メールに埋もれてしまう。
  - 年少者に対して、公序良俗上好ましくないメールを閲覧してしまうなどの問題がある。
  - 広告先のアドレスなどでフィッシング詐欺などへ利用される。

- **通信事業者、サービス事業者の視点：**
  - 迷惑メールによりトラフィックが増大し、疎通が阻害され、設備投資が必要となる。
  - 迷惑メール検出等のための新たな設備の設置が必要となる。

国内・海外発迷惑メール受信数推移

（一財）日本産業協会のモニター機による迷惑メール受信数



（一財）日本産業協会　ホームページより

日本としての迷惑メールに対する取り組み

■法律の施行
- 受信者の承諾無く大量配信広告メールを送付することを違法とする
- 広告メールには、メールの配信停止方法を明記すること
- 携帯電話の契約時の厳格化（身分証明書等が必要）
- 罰則規定あり

■スパムメール対策推進協議会の設立

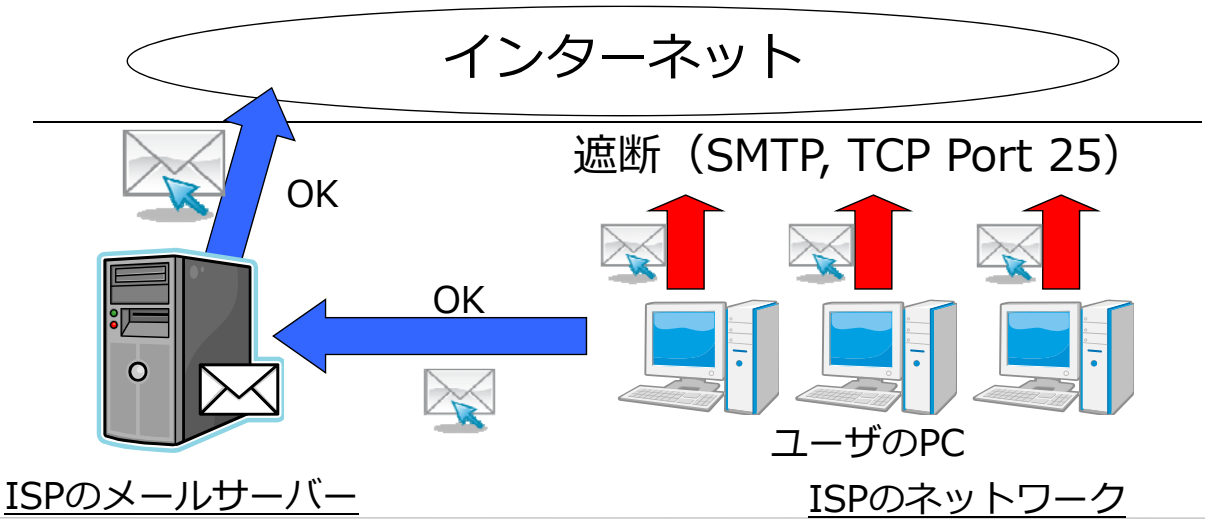
■Outbound Port 25 Blocking (OP25B)

■送信者認証技術の導入（SPF/SenderID、DKIM/DomainKeys）

■携帯電話通信事業者間でのスパムメール送信者の情報交換
- 一時に多数の者に対する「特定電子メールの送信の適正化等に関する法律」違反のメール送信その他の電子メール送受信上の支障を生じさせるおそれのある大量送信行為を行い利用停止措置を受けた加入者の情報を、携帯電話事業者およびPHS事業者間で交換

Outbound Port 25 Blocking (OP25B) (1)

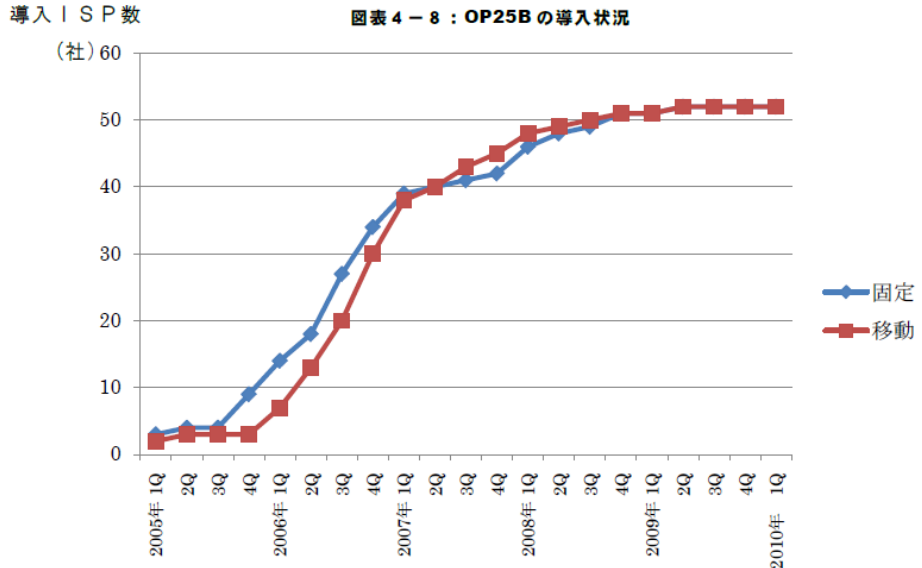
■**基本原理**
- ISPネットワークに接続されたユーザのPCは、プロバイダーのメールサーバ経由でE-mailを送信する必要がある。
- ほとんどのボットプログラムは、電子メールを受信側のメールサーバに直接送信するが、このような通信は遮断する。



Outbound Port 25 Blocking (OP25B) (2)

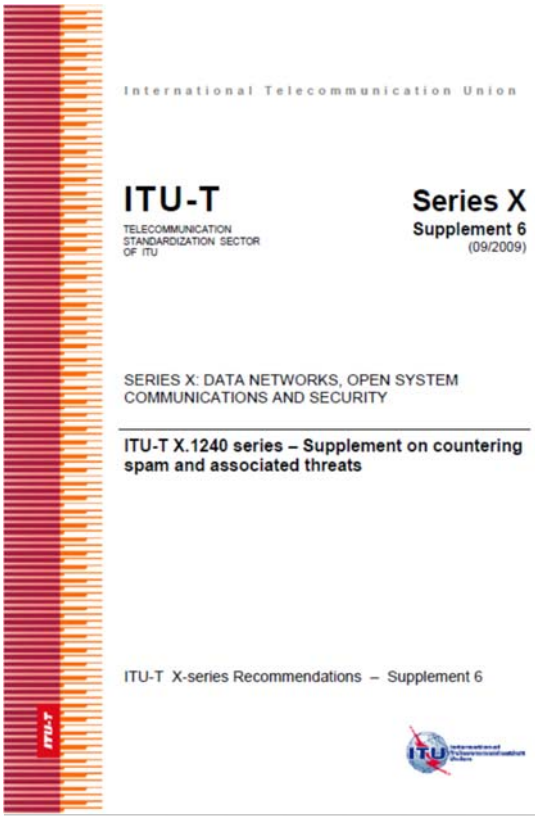
■導入状況

- 日本のほとんどのISP（55社）は、既にOP25Bを実施済み。（2009年10月時点）
- 多くのISPは、ISPの外側からISP経由でのメールの送信を可能にするために、Submission Portとして587番を提供している。



（注）近年は、漏洩したユーザのID/PWを利用した不正なメール送信が増えており、OP25B対策で防げないケースが増加している。

ITU-T 補足文書化



■迷惑メール対策に関する国際的な文書（London Action Plan、OECD Spam Toolkit、APEC TEL Symposium on spam）について紹介

■各国の取り組みとして、米国と日本の事例を紹介。

マルウェア感染対策

サイバークリーンセンター（CCC）

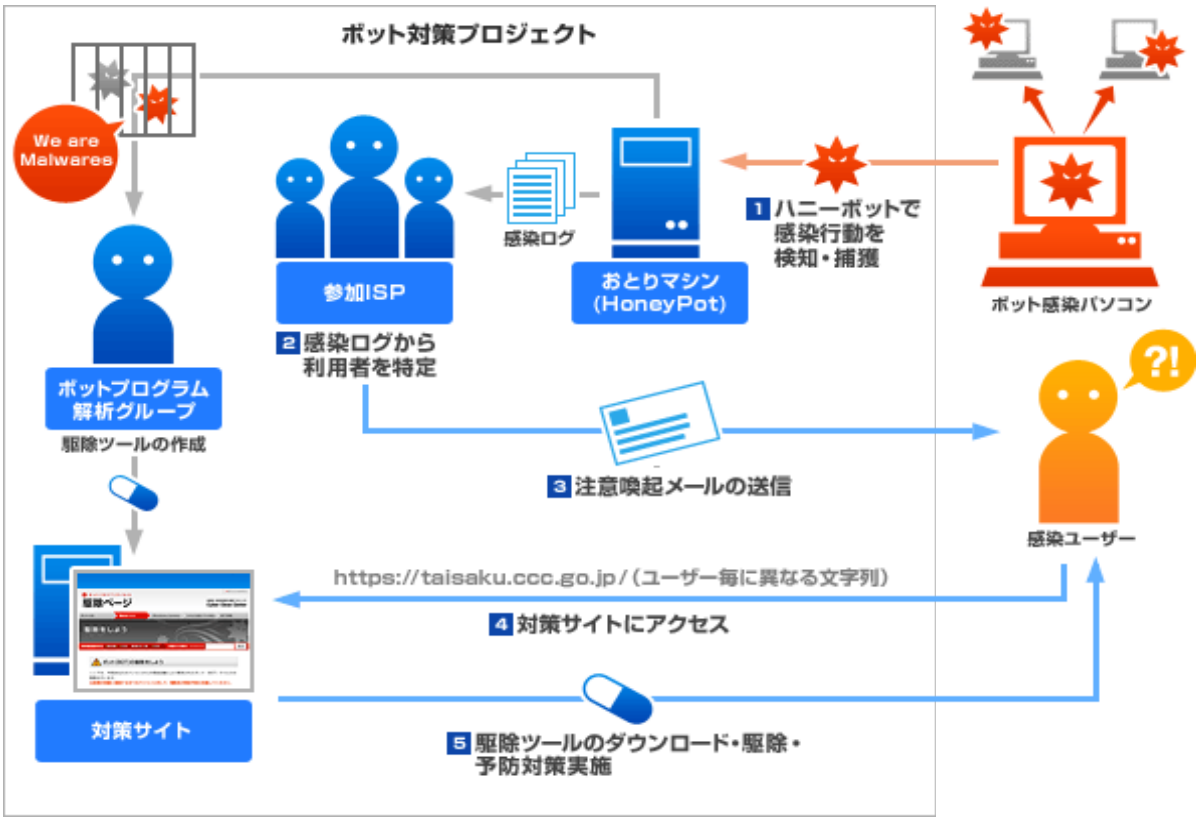
■サイバークリーンセンター（CCC）とは

- （ https://www.telecom-isac.jp/ccc/）
- インターネットにおける脅威となっているボット特徴を解析し、ユーザのPCからボットを駆除するために必要な情報をユーザに提供
- ISP（インターネットサービスプロバイダ）の協力によって、ボットに感染しているユーザに対し、ボットの駆除や再感染防止を促す
- 2011年3月にプロジェクト終了

■サイバークリーンセンターの体制

- 総務省、経済産業省
- Telecom-ISAC Japan、JPCERT/CC、IPA
- ISP各社
- ウイルスベンダー（駆除ツール作成）
- Microsoft

サイバークリーンセンター（注意喚起の流れ）



サイバークリーンセンター（活動実績）

2011年01月度の注意喚起活動実績

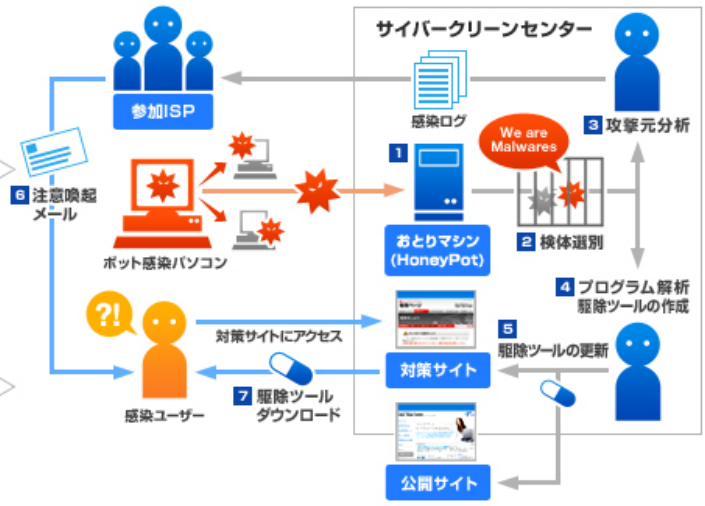
1 収集検体総数
当月:145, 631体　累積:17, 426, 320体
「おとりマシン」に対する無数の攻撃の中から収集した、ボットウィルス等の検体数（バイナリファイル）

2 同定検体数
当月: 117, 332検体　累積: 1, 992, 928
同じ検体が多数収集されるため、検体のサイズや外形的特徴の重複を除いた一意な検体数（バイナリファイル）

3 未知検体数
当月:91体　累積: 30, 217体
隔離した検体を市販のウィルス対策ソフトで検査し、検知できなかった検体数

6 注意喚起数
メール通数
当月: 2, 891通
累積: 536, 628通
対象者数
当月: 1, 368人（内新規 562人）
累積: 108, 726人
参加ISPから感染者に出した注意喚起メール数及び人数

7 被注意喚起者駆除ツールダウンロード率
32. 5%（累積）



4 駆除ツール作成検体数
当月: 34体
累積: 25, 993体
危険度が高く、感染者の多い検体について駆除ツールを作成した検体数

5 駆除ツール
累積更新回数:206回
駆除ツールは毎週更新

一般公開サイト駆除ツールダウンロード総数
※同時間帯に複数回ダウンロードされたものは除いた数字
当月: 25, 778回　累積: 1, 403, 736回

ACTIVE（Advanced Cyber Threats response InitiatiVE）

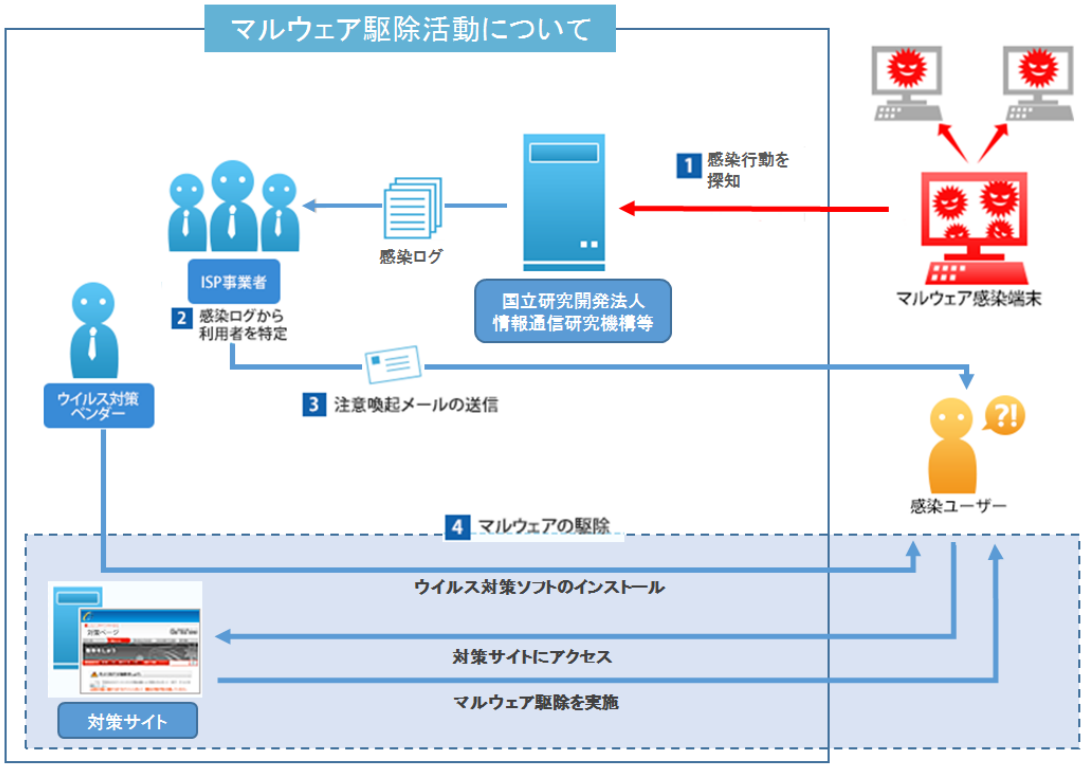
■ACTIVEについて

- 総務省が複数のインターネット・サービス・プロバイダ（ISP）事業者やセキュリティベンダー等の事業者と連携し、国内のインターネット利用者を対象に、マルウェアの感染防止と駆除の取組を行う官民連携プロジェクト
- （https://www.ict-isac.jp/active/）

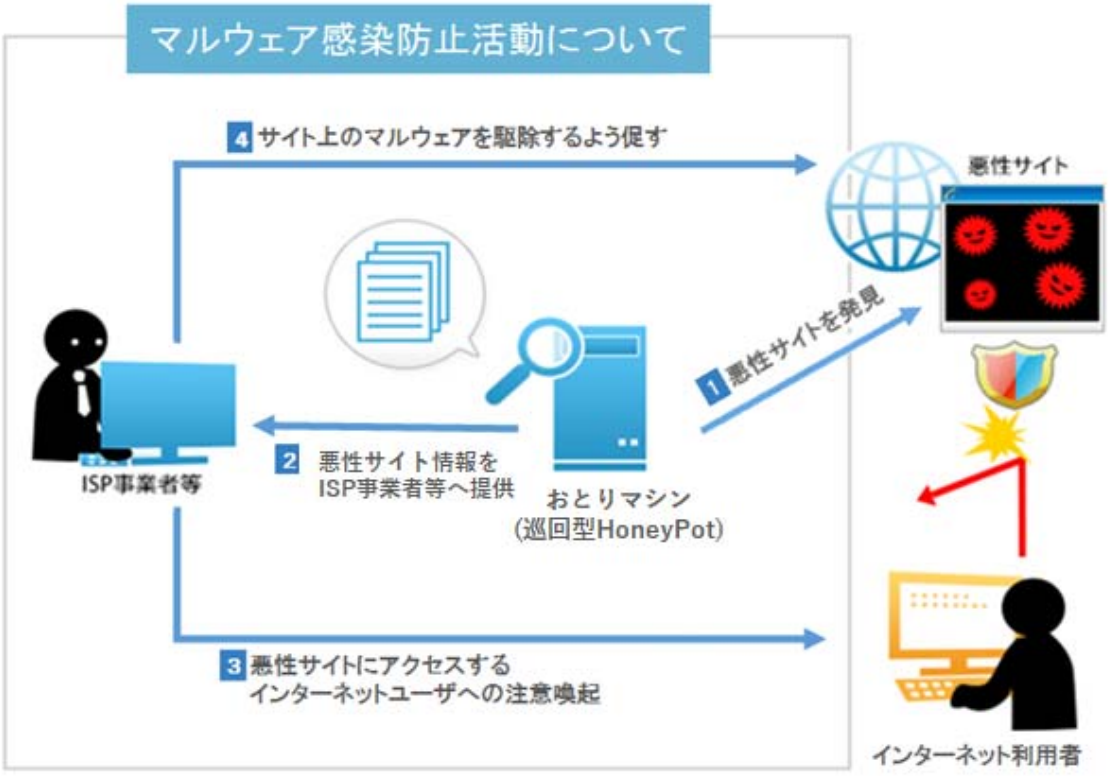
■参加団体

- 施策推進
  - 総務省
  - 一般社団法人　ICT-ISAC
- インターネットサービスプロバイダー
  - 36社（電気通信事業者、CATV事業者、ネットワーク事業者、等）
- マルウェア収集・駆除のための技術支援
  - 18社／機関（セキュリティベンダー、通信機器ベンダー、研究機関、等）

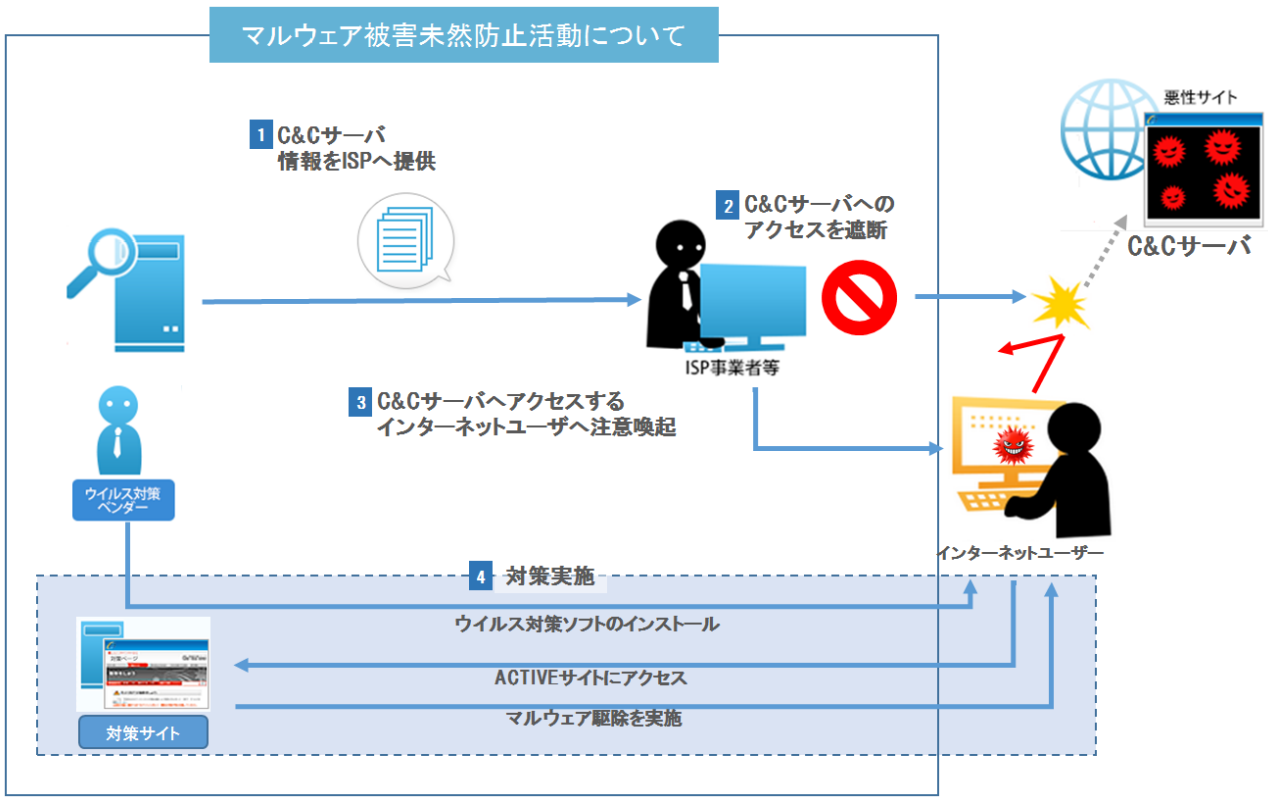
ISP事業者と連携した注意喚起



ISP事業者等と連携したマルウェア感染防止活動

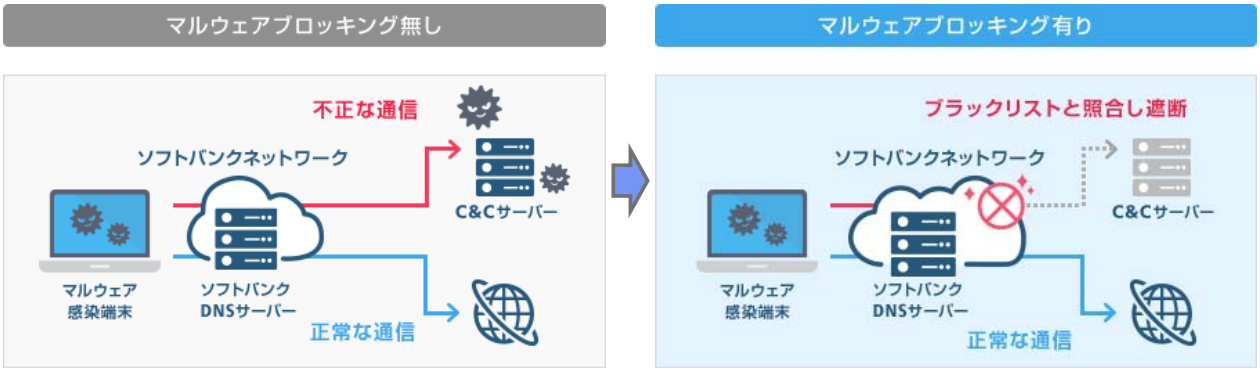


マルウェア被害未然防止活動



マルウェア被害未然防止の仕組み

- マルウェアブロッキングの仕組み（ソフトバンク社）
  - ① 会員がインターネットサービスへアクセスする場合、そのアクセス要求に付随するドメイン情報を自動的に検知し、保持している悪意のあるサーバのドメインリスト（ブラックリスト）と照合する。
  - ② 合致した場合、その通信を遮断し、C&Cサーバ（悪意のある第三者がマルウェアに感染した端末などに遠隔指令を出すサーバ）への接続を防ぐ。
  - ③ マルウェア感染の可能性があるお客さまには、ご登録の連絡先（PCメールアドレス、Yahoo!メールアドレス、SMS）宛に「マルウェア感染に関するご注意メール」を送付する。



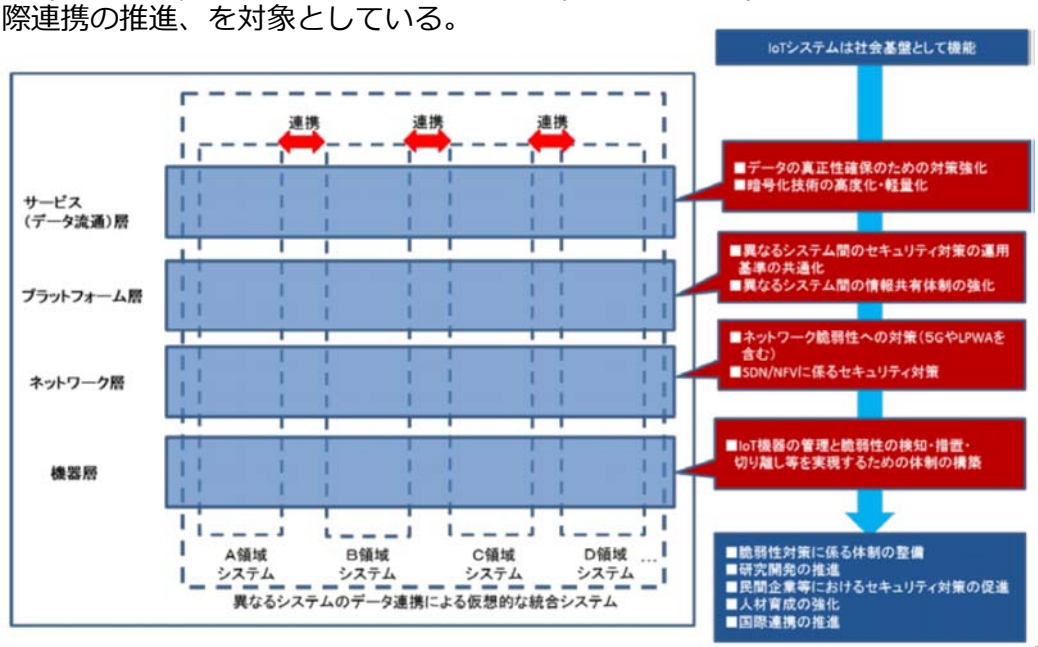
ソフトバンク社ホームページより

IoTセキュリティ対策

総務省IoTセキュリティ総合対策（1）

■概要

- 総務省サイバーセキュリティタスクフォースの議論を踏まえ、2017年10月に総務省から発行された。
- 具体的施策として、（1）脆弱性対策に係る体制の整備、（2）研究開発の推進、（3）民間企業等におけるセキュリティ対策の促進、（4）人材育成の強化、（5）国際連携の推進、を対象としている。



総務省IoTセキュリティ総合対策（2）

具体的施策	主な取り組み項目
脆弱性対策に係る体制の整備	• IoT機器に対するセキュリティ認証マークの付与 • セキュリティ検査の仕組み作り • 重要IoT機器の脆弱性調査 • 被害拡大防止のための取り組み
研究開発の推進	• 広域ネットワークスキャンの軽量化 • ハードウェア脆弱性への対応 • AIを利用したサイバー攻撃検知・解析
民間企業等におけるセキュリティ対策の促進	• 民間企業のセキュリティ投資の促進 • 事業者間での情報共有を促進するための仕組みの構築 • 情報共有時の匿名化処理に関する検討
人材育成の強化	• 実践的サイバー防御演習（CYDER）の充実 • 2020年東京大会に向けたサイバー演習の実施 • IoTセキュリティ人材の育成
国際連携の推進	• ASEAN各国との連携 • 国際的なISAC間連携 • 国際標準化の推進

IoTセキュリティに関連する法律改正

総務省 MIC Ministry of Internal Affairs and Communications

ご意見・ご提案 English

Google カスタム検索

総務省トップ > 広報・報道 > 報道資料一覧 > 第196回国会（常会）総務省提出予定法律案等

報道資料

平成30年1月19日

第196回国会（常会）総務省提出予定法律案等

件　名	担当部局
地方税法等の一部を改正する法律案	自治税務局 企画課 (03-5253-5658)
地方交付税法及び特別会計に関する法律の一部を改正する法律案	自治財政局 交付税課 (03-5253-5623)
電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案	総合通信基盤局 事業政策課 (03-5253-5978) 総合通信基盤局 消費者行政第二課 (03-5253-5847) 情報流通行政局 サイバーセキュリティ課 (03-5253-5749)
統計法及び独立行政法人統計センター法の一部を改正する法律案	政策統括官（統計基準担当）付 統計企画管理官室 (03-5273-1142)

電気通信事業法の一部改正案について（総務省発表資料より）

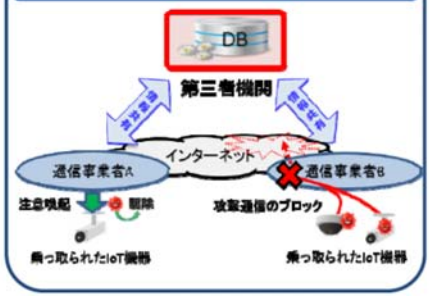
- IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

①深刻化するサイバー攻撃への通信事業者の対処の促進

- IoT機器を悪用したサイバー攻撃によるインターネット障害の深刻化

- サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進

第三者機関を通じた情報共有による対処



②電気通信番号に関する制度整備

- モバイル化・IoT化に伴う番号ニーズの増大による番号の逼迫やIP網移行に対応した全ての事業者による番号管理の必要性

- 番号の公平・効率的な使用と電話サービスの円滑な提供のため、使用条件を付して事業者に番号を割り当てるための制度を整備

番号の逼迫状況や効率的な使用

■ 番号の逼迫状況

番号	用途	指定率（指定数／全番号）	使用率（使用数／指定数）
070/080/090	携帯電話・PHS	90.4%	70.3%
0120	着信課金	99.2%	55.3%

※ その他、固定電話（0AB-J番号）の市外局番は、全国(582地域)のうち138地域で指定率が80%以上（平均使用率が18.6%）

■ 番号ポータビリティ（電話番号の持ち運び）

固定電話は現在、NTT東西から他事業者への片方向のみ。今後、携帯電話と同様、双方向番号ポータビリティを実現

③電気通信業務等の休廃止に係る利用者保護

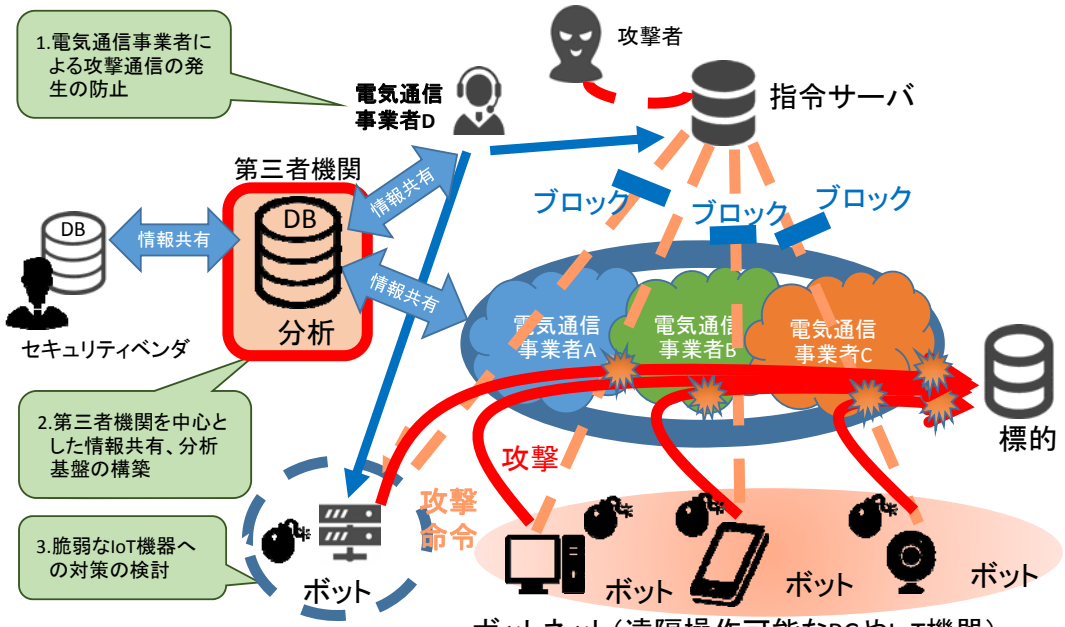
- IP網移行や通信設備の更改等を背景として利用者への影響が大きい業務等の終了が予定

- 事業者が業務の休廃止に伴い行う利用者周知について、行政が予め確認するための制度を整備

例：廃止予定のINSサービスの用途

第三者機関を結節点とした情報共有のイメージ

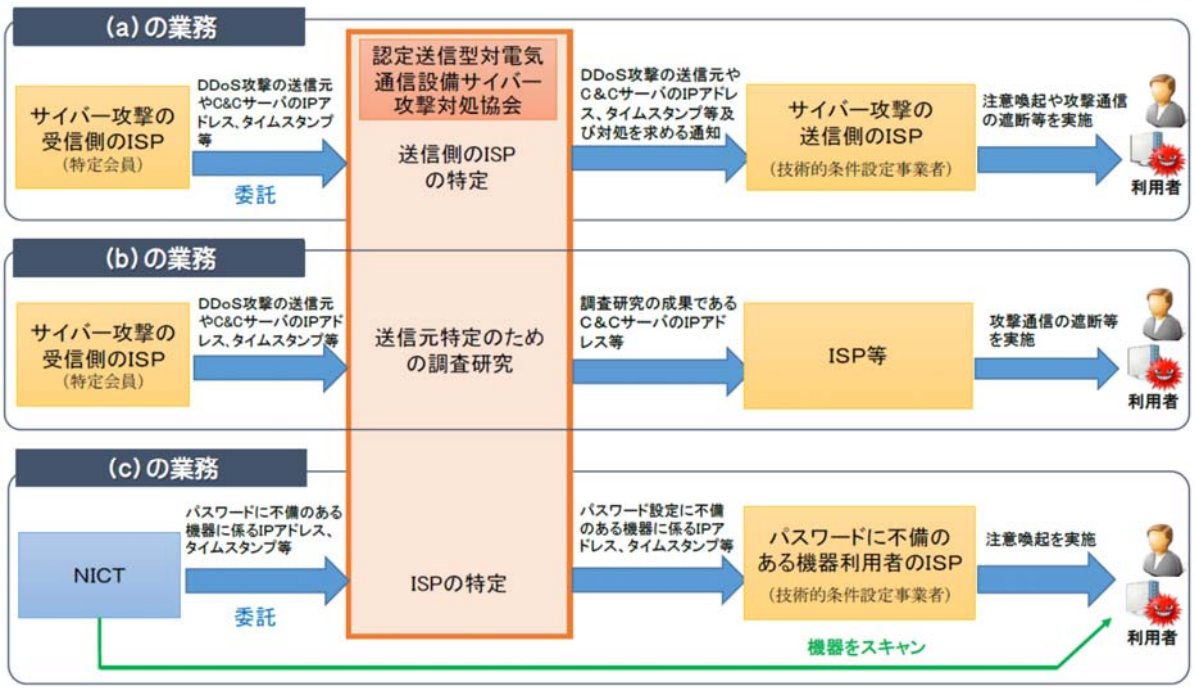
通信ネットワークを保護する目的で行われる情報共有を促進する観点から、情報共有の結節点として適切に情報を取り扱う第三者機関を法律上に位置づけ、第三者機関における通信の秘密を含む情報の収集、分析、共有等の枠組みを明確化



（出典）総務省資料

第三者機関として認定を受けた者の業務

認定送信型対電気通信設備サイバー攻撃対処協会の業務のイメージ



（出典）総務省資料

国立研究開発法人情報通信研究機構法の一部改正案について（総務省発表資料より）

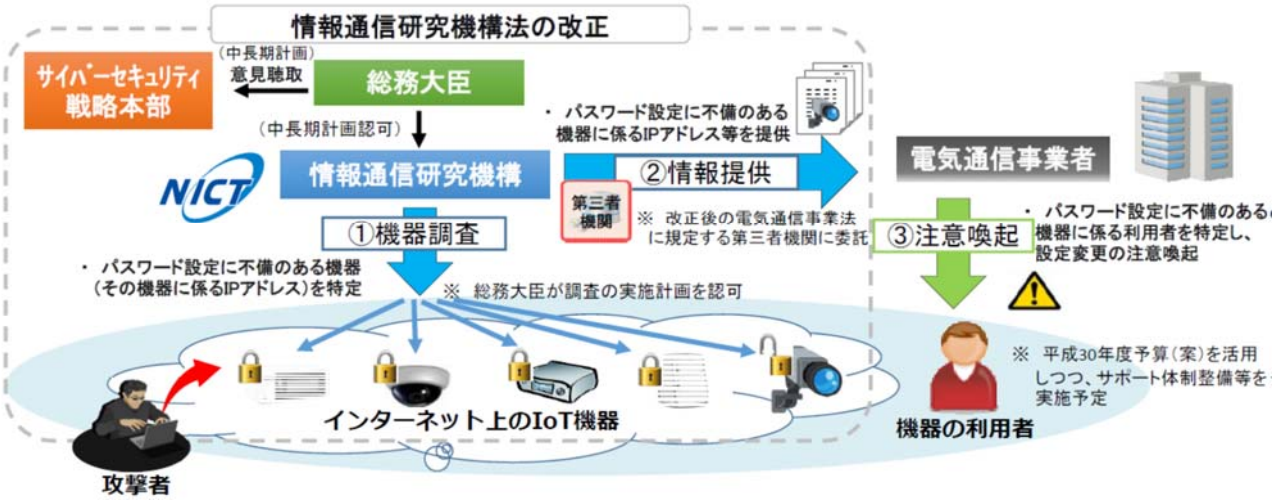
KDDI Research

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行うもの。

サイバー脅威の深刻化
・IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。
※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性
・パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備
・NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。



NOTICE

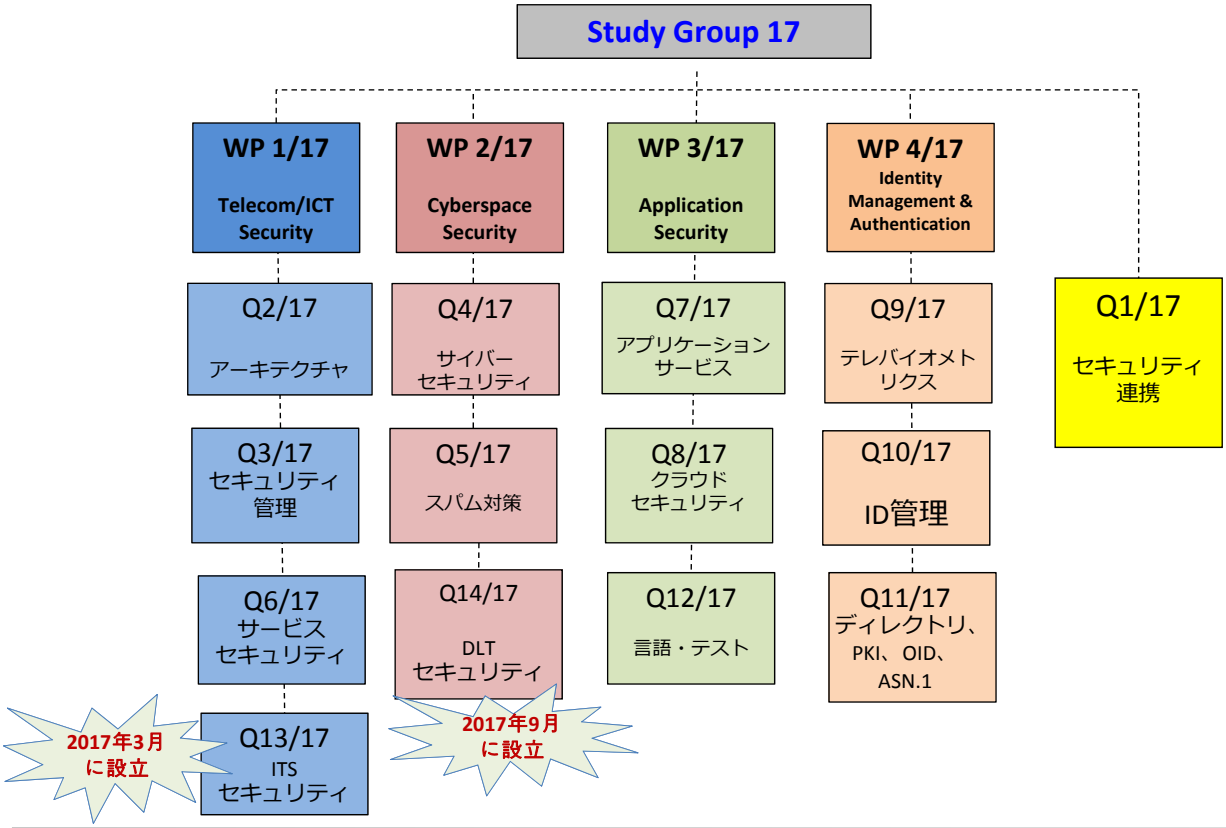
KDDI Research

■IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施（2019年2月1日）

総務省及び国立研究開発法人情報通信研究機構（NICT）は、インターネットプロバイダと連携し、サイバー攻撃に悪用されるおそれのあるIoT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「NOTICE（National Operation Towards IoT Clean Environment）」を平成31年2月20日（水）から実施

2. ITU-T SG17における セキュリティ標準化活動

SG17の全体構成



ITU-T SG17の課題構成（1）

	タイトル	議長／ラポータ
SG17	Security（セキュリティ）	Heung Youl Youm（韓国）
Q1/17	Telecommunication/ICT security coordination （電気通信／ICTのセキュリティに関する調整）	Wala Turki Latrous （チュニジア）
WP1	Telecommunications / ICT security （通信/ICTセキュリティ）	三宅　優（KDDI）
Q 2/17	Security architecture and framework （セキュリティのアーキテクチャ及びフレームワーク）	Zhiyuan Hu（中国） Heung Ryong Oh（韓国）
Q 3/17	Telecommunications information security management （電気通信における情報セキュリティマネジメント）	永沼　美保（NEC）
Q 6/17	Security aspects of telecommunication services, network and Internet of Things （電気通信サービス、ネットワーク、IoTのセキュリティ面）	Jonghyun Baek（韓国）
Q13/17	Security aspects of intelligent transport systems （ITSのセキュリティ面）	Sang-Woo Lee（韓国）
WP2	Cyberspace security （サイバー空間のセキュリティ）	中尾　康二（NICT）
Q 4/17	Cybersecurity （サイバーセキュリティ）	Jong-Hyun Kim（韓国）
Q 5/17	Countering spam by technical means （技術的手法によるスパム対策）	Yanbin Zhang（中国）
Q 14/17	Security aspects for Distributed Ledger Technologies （分散台帳管理技術のセキュリティ面）	門林　雄基（NICT） Kyeong Hee Oh（韓国）

ITU-T SG17の課題構成（2）

	タイトル	議長／ラポータ
WP3	Application security （アプリケーションセキュリティ）	Arnaud Taddei（アメリカ）
Q 7/17	Secure application services （セキュアなアプリケーションサービス）	Jae Hoon Nah（韓国）
Q 8/17	Cloud computing security （クラウドコンピューティングセキュリティ）	Liang Wei（中国）
Q 12/17	Formal languages for telecommunication software and testing （電気通信ソフトウェアとテストのための形式言語）	Dieter Hogrefe（ドイツ）
WP4	Identity management and authentication （ID管理及び認証）	Kepeng Li（中国）⇒ Zhaoji Lin（中国）交代
Q 9/17	Telebiometrics （テレバイオメトリクス）	John George Caras （アメリカ）
Q 10/17	Identity management architecture and mechanisms （ID管理のアーキテクチャ及びメカニズム）	Abbie Barbir（アメリカ）
Q 11/17	Generic technologies to support secure applications （安全なアプリケーションをサポートするための基盤技術）	Jean-Paul Lemaire（フランス）

サイバーセキュリティ

サイバーセキュリティ

■CYBEXプロジェクト

- ITU-T SG17の課題4（Cybersecurity）が取り組むサイバーセキュリティ情報の展開と交換を促進するためのプロジェクト
- The Cybersecurity Information Exchange Framework

■CYBEX関連の勧告

- X.1500, Overview of cybersecurity information exchange
- X.1520, Common vulnerabilities and exposures
- X.1521, Common vulnerability scoring system
- X.1524, Common weakness enumeration
- X.1525, Common weakness scoring system
- X.1526, Language for the open definition of vulnerabilities and for the assessment of a system state
- X.1528, Common platform enumeration
- X.1544, Common attack pattern enumeration and classification
- X.1546, Malware attribute enumeration and characterization

CYBEX概要

■CYBEXが必要とされる理由
- ウィルスなどの悪意のあるソフトウェアによる被害は国境を越えて瞬時に広まる一方、問題に対処する機関各国ごと、また各機関ごとに独立して活動しており、相互に連携を取ることが充分できていない。
- CYBEXでは、サイバーセキュリティー情報の表現・格納方法を標準化することにより、国境を越えた、全世界規模でのサイバーセキュリティー情報の共有を実現

■CYBEXフレームワークを構成する5つの機能
- 情報表現ブロック
- 情報発見ブロック
- 情報クエリブロック
- 情報信頼性ブロック
- 情報伝送ブロック

CYBEX:情報表現ブロック

■CVE: Common Vulnerabilities and Exposures
- ITU-T X.1520
- 既知の脆弱性情報をXMLベースで構造化したディレクトリを構築するための規格であり、各脆弱性にCVE識別子を付与し、その識別子ごとに脆弱性情報を登録したディレクトリをXMLベースで作成する。

■CVSS: Common Vulnerability Scoring System
- ITU-T X.1521
- ソフトウェアの脆弱性の深刻さを数値化する手法。数値化することにより、対処すべき脆弱性の優先順位付けが可能となる。例えば、複数のソフトウェアが存在し、それらがそれぞれセキュリティの問題を抱えている場合に、着手の優先付けをすることなどが可能となる。

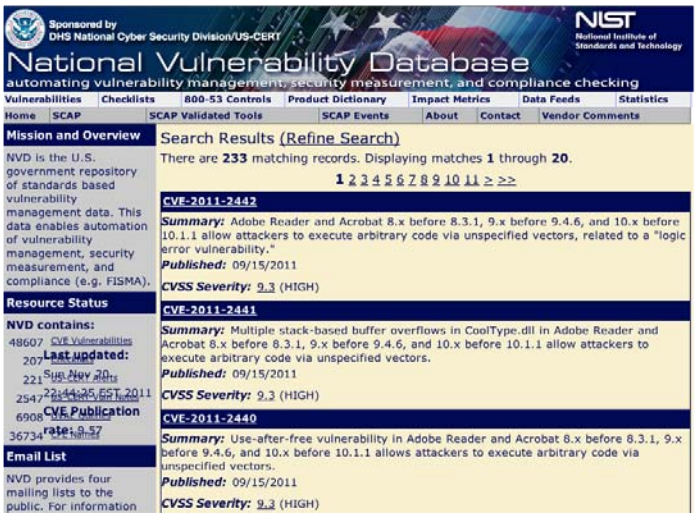
■CWE: Common Weakness Enumeration
- ITU-T X.1524
- ソフトウェアの弱点を表現するための規格であり、各弱点、またそのタイプにIDを付与し、一意に特定可能にする。

■その他
- CWSS: Common Weakness Scoring System
- OVAL: Open Vulnerability and Assessment Language
- ・・・・・・

CVEを利用した脆弱性情報展開

KDDI Research

■149のCVE互換製品、サービス



米国:NIST NVD

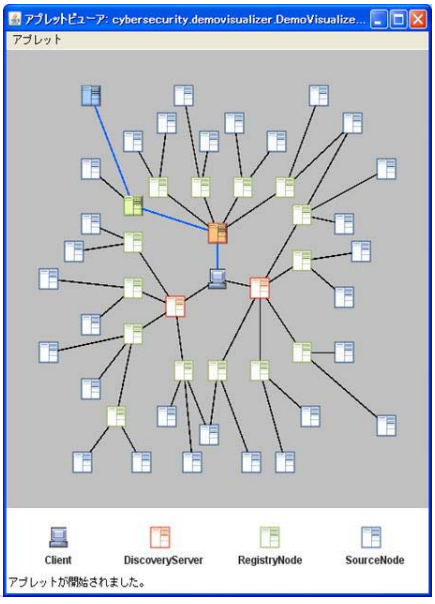
日本: IPA JVN (Japan Vulnerability Notes)

CYBEX:情報発見ブロック

KDDI Research

■ Discovery mechanism in the exchange of cybersecurity information
- ITU-T X.1570
- サイバーセキュリティ情報を特定・発見するための手法における、その概念及び必要な技術手順
- RDFを用いる手法とOIDを用いる手法をそれぞれ規定

■ Guidelines for Administering the OID arc for cybersecurity information exchange
- ITU-T X.1500.1
- グローバルなサイバーセキュリティ識別子の名前空間と、OID arcやそのほかのサイバーセキュリティ関連の識別子の管理上の必要条件



CYBEX: 情報信頼性ブロック、情報伝送ブロック

情報信頼性ブロック

■ Entity authentication assurance
- ITU-T X.1254
- 各エンティティの同一性（アイデンティティ）を維持するための認証ライフサイクルのフレームワークを規定

情報伝送ブロック

■ Real-time internetwork defense (RID)
- ITU-T X.1580, RFC 6545
- インシデント情報の交換プロトコルで、IODEFのwrapperである。これによりエンティティ間にてメッセージのセキュアな交換を実現

■ Transport of Real-time internetwork defense (RID) messages
- ITU-T X.1581, RFC 6546
- HTTPSを利用してRIDを利用する場合の詳細を規定

OASIS STIX/TAXIIの勧告化

■ STIX(Structured Threat Information eXpression)
- サイバー攻撃活動を記述するための仕様
- セマンティクスに従って脅威をグラフベースのモデルで表現

■ TAXII(Trusted Automated eXchange of Indicator Information)
- サイバー攻撃活動の情報を交換するための仕様
- 脅威インテリジェンス共有

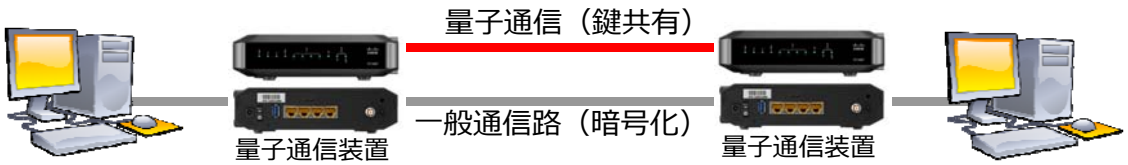
■ ITU-T SG17における勧告化の経緯
- 2018年8～9月のワークショップで「ITU Workshop on Advanced Cybersecurity Attacks and Ransomware」を実施し、STIX/TAXIIの発表が複数あり。ワークショップ総括として、ITU-Tでの勧告化を目指すこととした。
- OASISにリエゾンを送付して勧告化について協力を求める。
- OASISI側から、現在、新バージョンを作成中で、そのバージョンでの勧告化を希望すること、および、2019年8～9月のSG17会合に新バージョンの文書を送付したいと回答。

QKD（Quantum Key Distribution）

（2019年1月にミニワークショップ実施）

量子コンピュータ出現に伴う暗号の危殆化について

- ■ 量子コンピュータと暗号
  - ● 性能の高い量子コンピュータで、RSA暗号、楕円曲線暗号が比較的簡単に解読されることが証明されている。
  - ● 量子コンピュータの現時点の性能では解読不可能であるが、高性能化が進んでいる。
- ■ 量子コンピュータで解読できない暗号の検討
  - ● 暗号アルゴリズムの改良
    - 量子コンピュータでの解読法が発見でされていない理論に基づいた暗号アルゴリズムの開発
    - 現在、NISTで暗号アルゴリズムのコンテスト中
    - 従来の暗号アルゴリズムと同様に、ISO/IEC JTC1 SC27で国際標準化されることになると考えられる
  - ● 量子暗号通信の利用
    - 盗聴検知が可能となる量子通信を利用することにより、盗聴不可能な通信を実現
    - 通信速度が遅いため、別のアルゴリズムの暗号化に使うための鍵を共有するために利用することが多い（QKD: Quantum Key Distribution）



量子鍵配送に関する標準化動向

■ ETSI ISG-QKD (Industry Specification Groups)
- 量子鍵配送の装置に関する標準化について、2008年から活動を開始
- 日本からの参加は、三菱電機、NICT、NTT。また、東芝研究所欧州がUKとして参加。
- 発行された文書は以下の通り
  - ETSI GS QKD 002 V1.1.1 (2010-06): Quantum Key Distribution (QKD); Use Cases
  - ETSI GR QKD 003 V2.1.1 (2018-03): Quantum Key Distribution (QKD); Components and Internal Interfaces
  - ETSI GS QKD 004 V1.1.1 (2010-12): Quantum Key Distribution (QKD); Application Interface
  - ETSI GS QKD 005 V1.1.1 (2010-12): Quantum Key Distribution (QKD); Security Proofs
  - ETSI GS QKD 008 V1.1.1 (2010-12): Quantum Key Distribution (QKD); QKD Module Security Specification
  - ETSI GS QKD 011 V1.1.1 (2016-05): Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems

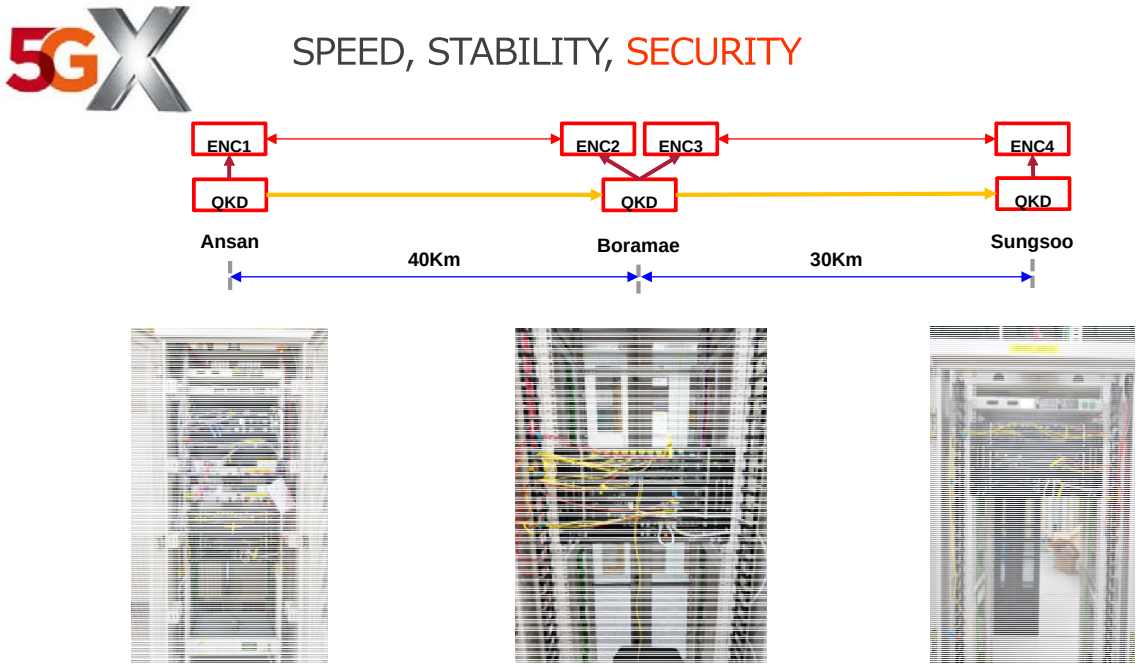
QKDの商用化状況

■量子鍵配送システムのサービスを提供している会社（Wikipediaより）
- id Quantique (スイス、ジュネーブ)
- MagiQ Technologies (米国、ニューヨーク)
- SmartQuantum (フランス)
- Quintessence Labs (オーストラリア)

■量子鍵配送ネットワーク（実験）
- DARPA Quantum network
  - 10ノードの量子鍵配送ネットワークで、アメリカマサチューセッツ州で2004年より運用。
- SECOQC
  - EUが出資。200 kmの標準的な光ファイバーケーブルでウィーンから西に69 km離れたザンクト・ペルテンの街を結ぶ六ヶ所を繋いでネットワークを形成。
- Tokyo QKD Network
  - NEC、三菱電機、NTT、NICT、Toshiba Research Europe Ltd. (イギリス)、id Quantique (スイス)、「ALL Vienna」の七つの団体によるネットワーク。

SK Telecom（韓国）における実証実験

■5Gトライアルで、伝送路のセキュリティ対策に利用（2018年12月）



ITU-TにおけるQKDの活動状況

■ITU-T SG13

- 2018年7月会合より議論を開始。一般的な構成、要件、アーキテクチャについて議論。

■ITU-T SG17

- QKDに関するセキュリティ（鍵配送、鍵中継、セキュリティ対策、等）について議論

ITU-TにおけるQKDに関するワークアイテム、議論

■ITU-T SG13

- 2018年7月
  - Y.QKD_FR: Framework for Networks to supporting Quantum Key Distribution

■ITU-T SG17

- 2018年9月
  - X.qrng-a: Quantum noise random number generator architecture
  - TR.sec-QKD: Technical Report on Security framework for Quantum Key Distribution in Telecom network
- 2019年1月
  - 韓国が新規課題（Question）を設立提案したが、英国等がWTSA-2020時のSG17体制の議論において検討すべきとし、設立されなかった。
  - X.sec_QKDN_ov: Security Requirements for QKD Networks – Overview
  - X.sec_QKDN_km: Security Requirements for QKD Networks – key management
  - X.cf-QKDN: The use of cryptographic functions on a key generated in Quantum Key Distribution networks

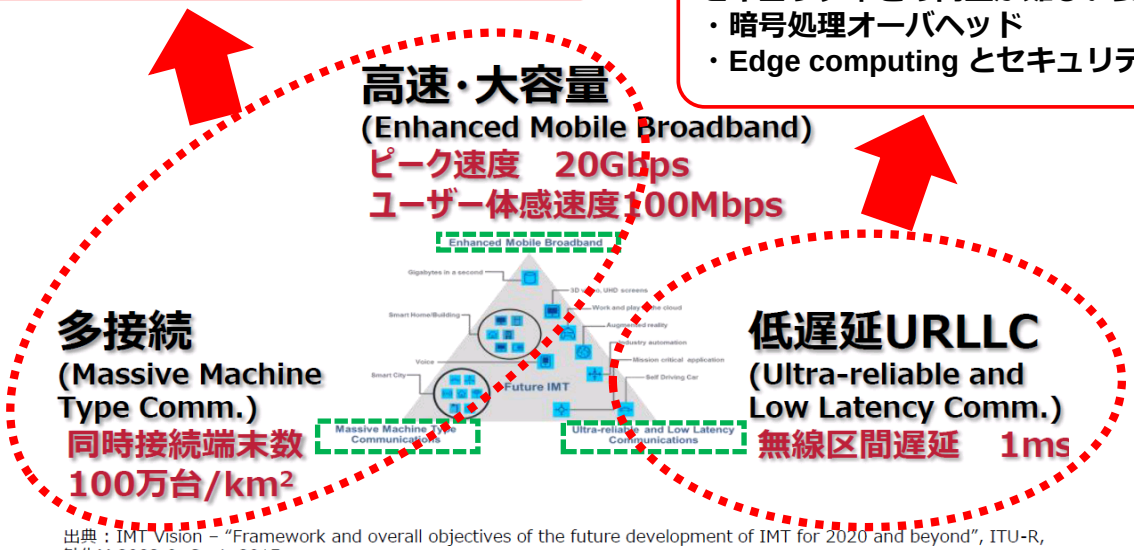
5G Security

（2018年3月にワークショップ実施）

5Gの要件から想起されるセキュリティ課題

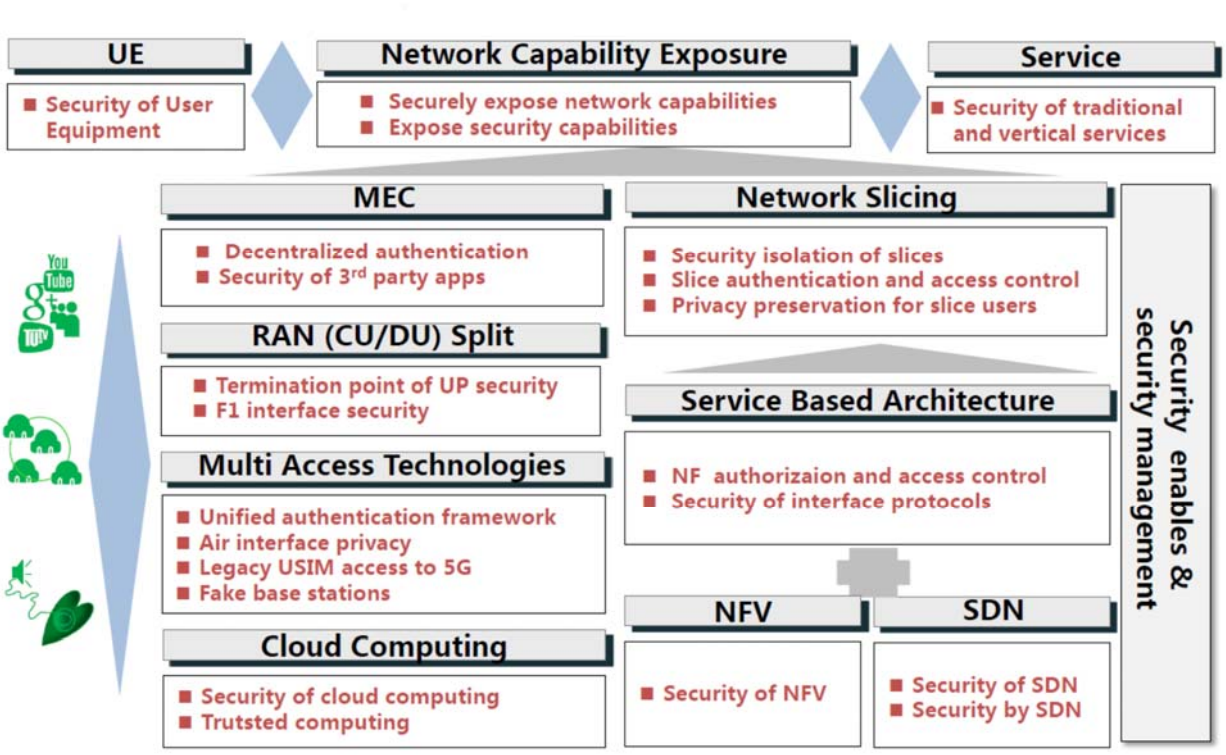
既に顕在化しているセキュリティ脅威の深刻化
・スマホ/IoTマルウェア
・ボットネットによる攻撃威力の増大
・シグナリングDoS

セキュリティとの両立が難しい要件
・暗号処理オーバヘッド
・Edge computing とセキュリティ



出典：IMT Vision – “Framework and overall objectives of the future development of IMT for 2020 and beyond”, ITU-R, 勧告M.2083-0, Sept. 2015

5Gにおけるセキュリティ上の課題



ITU-T 5G Security Workshop（2018年3月）の資料より（China Mobile発表）

5G技術とセキュリティ

技術	セキュリティ面での利点	課題
5G無線アクセス	• 無線ジャミングへの耐性向上 • 物理レイヤーセキュリティ	
ネットワークスライシング	• スライス分離による異なるセキュリティ要件のサポート • セキュリティ被害・影響の限定	• 分離性の確保・保証 • スライス管理機能への攻撃 • スライス間通信の管理 • セキュリティレベルの異なる複数スライスへの同時接続
仮想化(NFV/SDN)	• サイバー攻撃への対策手段の拡充（DoS対策、仮想ファイアウォール、等）	• 分離性の確保・保証 • オーケストレータ／コントローラへの攻撃 • トラスト（NFVI、3rd Party VNF）
エッジコンピューティング	• セキュリティ機能のオフロード（端末からエッジクラウドへ）	• コアと比較してエッジの物理セキュリティが低いことに起因する問題

5Gセキュリティにかかわる標準化、活動

標準化団体	活動
3GPP SA3	• Threat analysis, Requirements on security, Security architecture and protocol specifications • Definition of 17 security domains(Architecture, Authentication, RAN security, Key Management, etc.)
ETSI ISG NFV	• Security monitoring and administration for NFV • Security assessment for NFV platform • etc.
GSMA	• 5G trust model, Network slice security, etc.
NGMN	• 5G security requirements (DoS protection, Network slicing, MEC)
Others	• IETF (5GIP, NETSLICING, etc.) • ONF(Open Networking Foundation) – SDN related security

ITU-T SG17における5G関連のワークアイテム

■課題2（Security architecture and framework）

- X.sdnsec-3: Security framework and requirements of service function chain based on software-defined networking
- X.ssc: Security service chain architecture and its application
- X.srnv: Security requirements of network virtualization
- X.SDSec: Guideline on software-defined security in SDN (Software-defined Networking)/NFV (Network Function Virtualization) network

■課題6（Security aspects of telecommunication services, networks and Internet of Things）

- X.sdnsec-1: Security services using the software-defined networking
- X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
- X.5Gsec-t: Security framework based on trust relationship in 5G ecosystem
- X.5Gsec-ecs: Security framework for 5G edge computing services
- X.5Gsec-guide: Security guidelines for 5G communication system based on ITU-T X.805

ITS Security

（2017年8月にワークショップ実施）

ITU-T SG17におけるITSセキュリティの議論

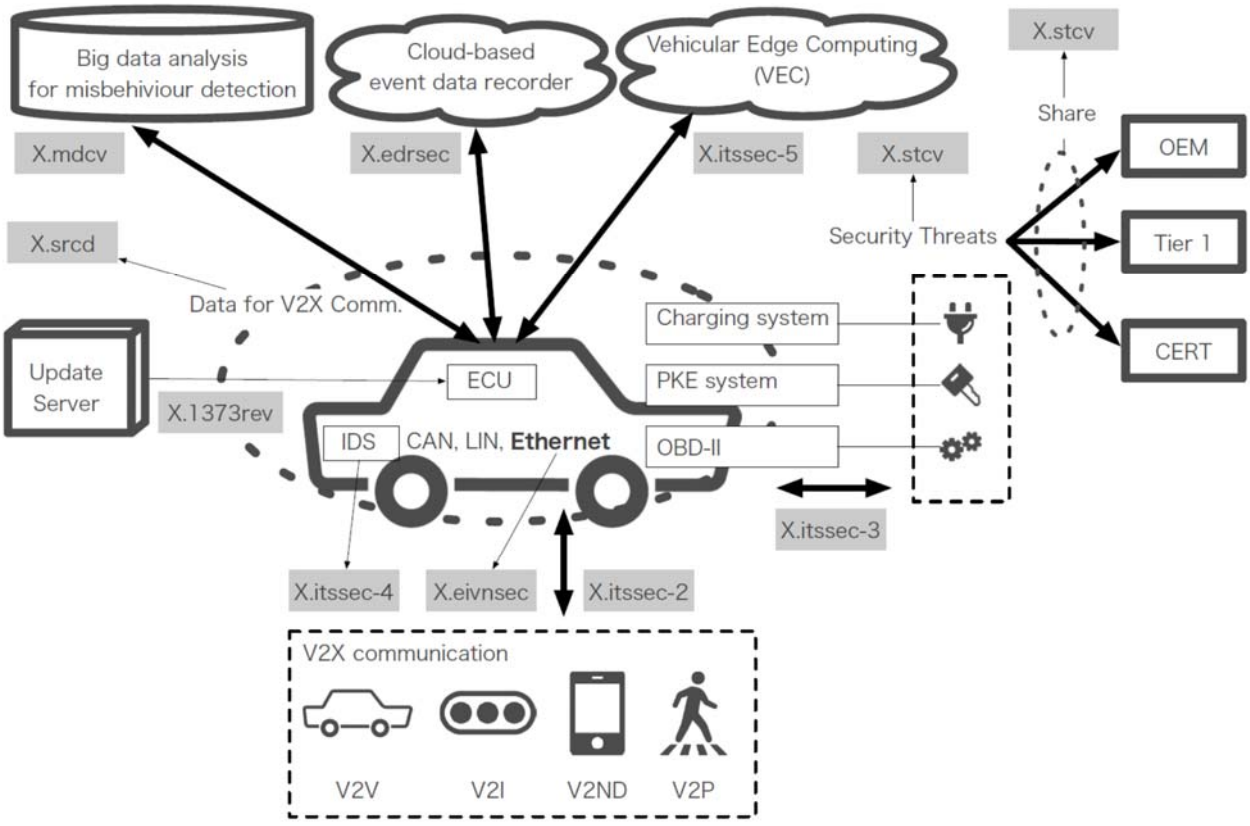
■経緯

- 2017年3月のITU-T SG17会合で、これまで課題6で行っていたITSセキュリティに関するワークアイテムを分離し、新規課題設立を合意。
- 2018年8～9月の会合より課題13「Security aspects of intelligent transport systems」として活動を開始。
- 上記会合前日に、ITSセキュリティワークショップを開催。

■他の標準化団体との連携

- ISO TC22
- ISO TC204
- IETF WG ITS
- ETSI TC ITS
- SAE
- W3C Automotive WG
- UNECE WP29

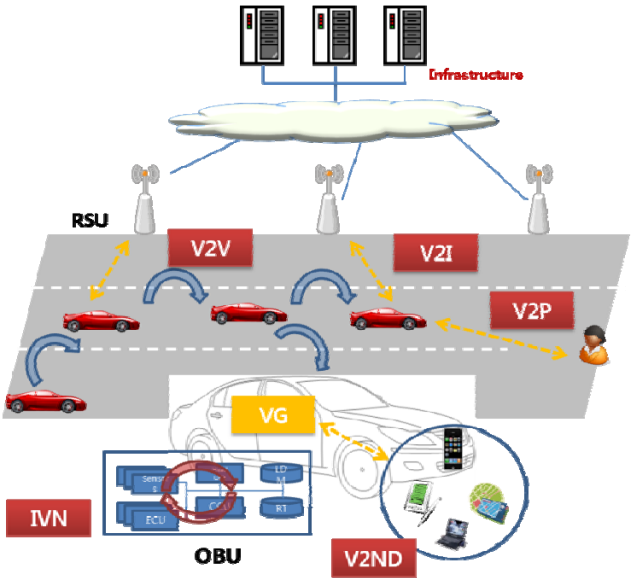
ワークアイテムの位置づけ



X.itssec-2
Security guidelines for V2X communication systems

■概要

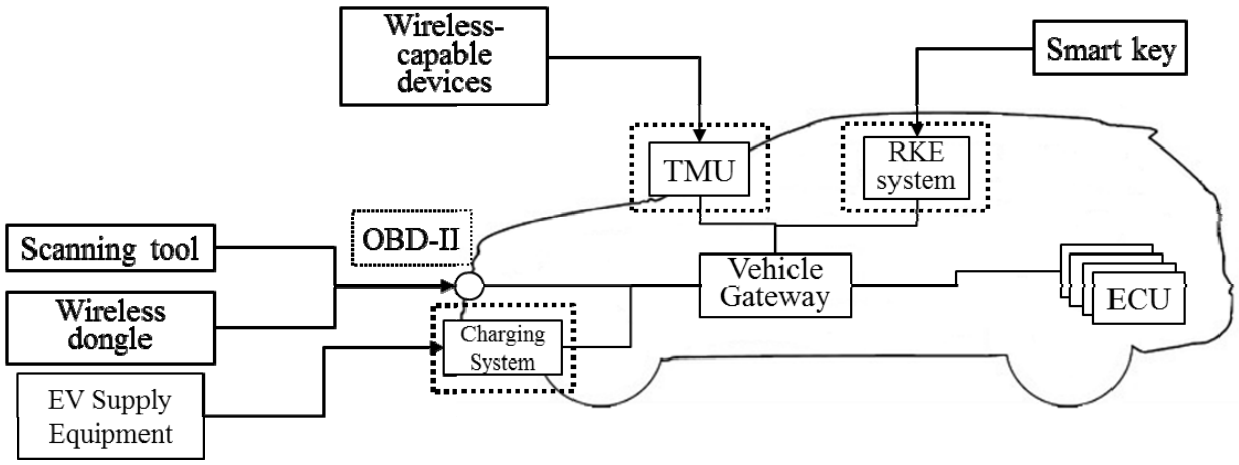
- V2Xのうち、V2V(Vehicle-to-Vehicle)、V2I(Vehicle-to-Infrastructure)、V2ND(Vehicle-to-Nomadic Devices)、V2P(Vehicle-to-Pedestrian)を対象に、UNECE WP29/TFCSの成果に基づいてV2X通信環境における脅威を特定し、それに対するセキュリティ要求を定義する。



X.itssec-3
Security requirements for vehicle accessible external devices

■概要

- 外部デバイスが車載ネットワークに接続する際のセキュリティの脅威を規定するとともに、車載ネットワークに接続可能な外部デバイスに対するセキュリティ要求を定義する。

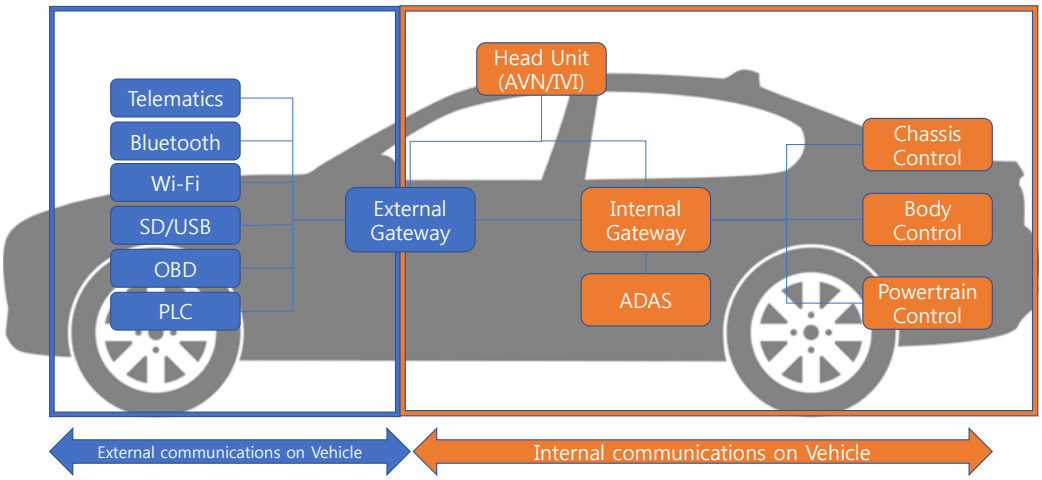


X.itssec-4
Methodologies for intrusion detection system on in-vehicle system

KDDI Research

■概要

- 車載ネットワークにおける侵入検知システムの実現手法を扱う。
- 具体的には、脅威の分類、検知手法、システム構成について規定する。

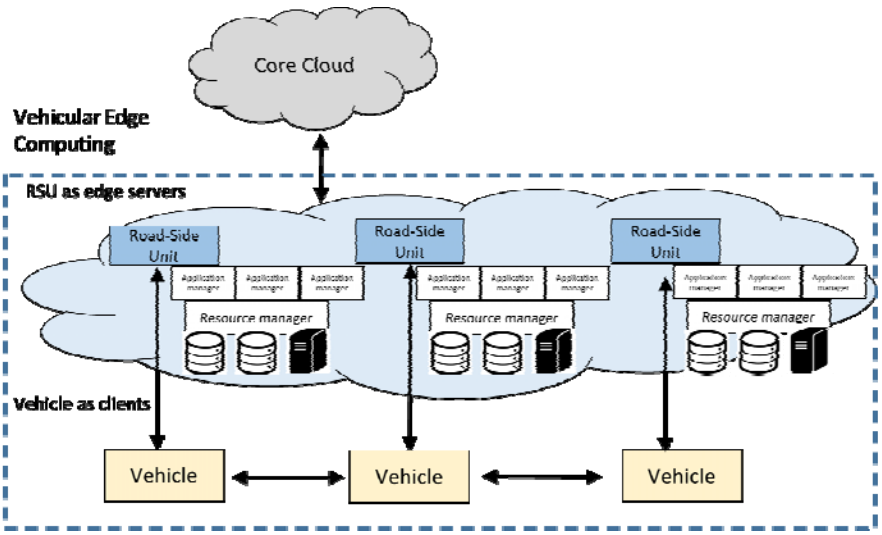


X.itssec-5
Security guidelines for vehicular edge computing

KDDI Research

■概要

- Vehicular edge computing(VEC)向けのセキュリティガイドライン
- VECはコア網のクラウドの計算資源やストレージ容量の負担の軽減、低遅延を実現するアーキテクチャ



審議中のワークアイテム

タイトル	概要
X.itssec-2 (Security guidelines for V2X communication systems)	WP29/TFCSの成果に基づき、V2X（具体的には、V2V/V2I/V2ND/V2P）における脅威の定義と、それに対するセキュリティ要求の規定のガイドライン化
X.itssec-3 (Security requirements for vehicle accessible external devices)	コネクテッドカーを構成するサブシステムに接続可能な外部デバイスからのアクセスに関する脅威と対策
X.itssec-4 (Methodologies for intrusion detection system on in-vehicle systems)	車内システムにおける侵入検知の仕組み
X.itssec-5 (Security guidelines for vehicular edge computing)	Vehicular edge computing (VEC)のセキュリティガイドライン
X.mdcv (security-related misbehaviour detection mechanism based on big data analysis for connected vehicles)	コネクテッドカー向けのビッグデータ解析に基づく異常検知機構
X.srcd (security requirements for categorized data in V2X communication)	V2Xコミュニケーションにおけるデータセキュリティ確保のための、データの分類と、分類結果に対するセキュリティレベルの設定および要求事項

審議中のワークアイテム

タイトル	概要
X.stcv (security threats in connected vehicles)	コネクテッドカーにおけるセキュリティ脅威（WP29/TFCSにおける”threats”の定義との一致を図ることを念頭に、文書を更新中）
X.fstiscv (Framework of security threat information sharing for connected vehicle)	コネクテッドカー向けのセキュリティ脅威情報の共有フレームワーク
X.edrsec (Security guidelines for cloud-based event data recorders in automotive environment)	クラウドをベースとしたイベント情報管理機構に関するセキュリティガイドライン
X.eivnsec (Security guidelines for the Ethernet-based in-vehicle networks)	Ethernetをベースとした車載ネットワーク向けのセキュリティガイドライン
X.1373 rev (Secure software update capability for intelligent transportation system communication devices)	ITS通信デバイスのためのセキュアなソフトウェアアップデート機能

DLT Security

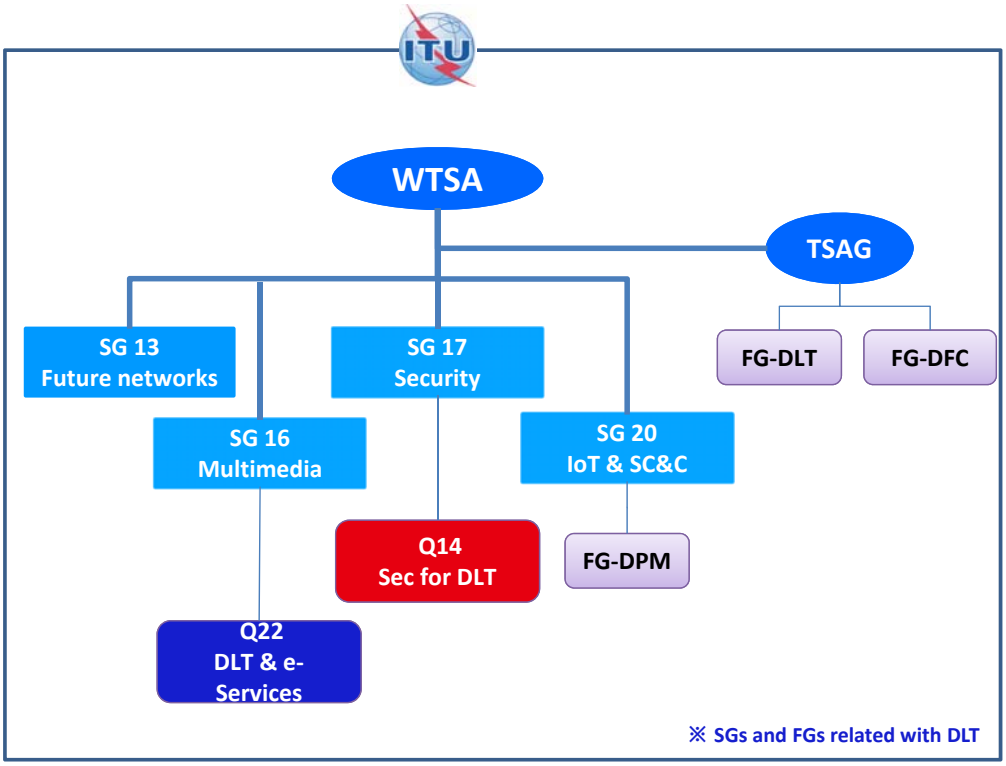
（2017年3月にワークショップ実施）

ITU-T SG17におけるDLTの議論

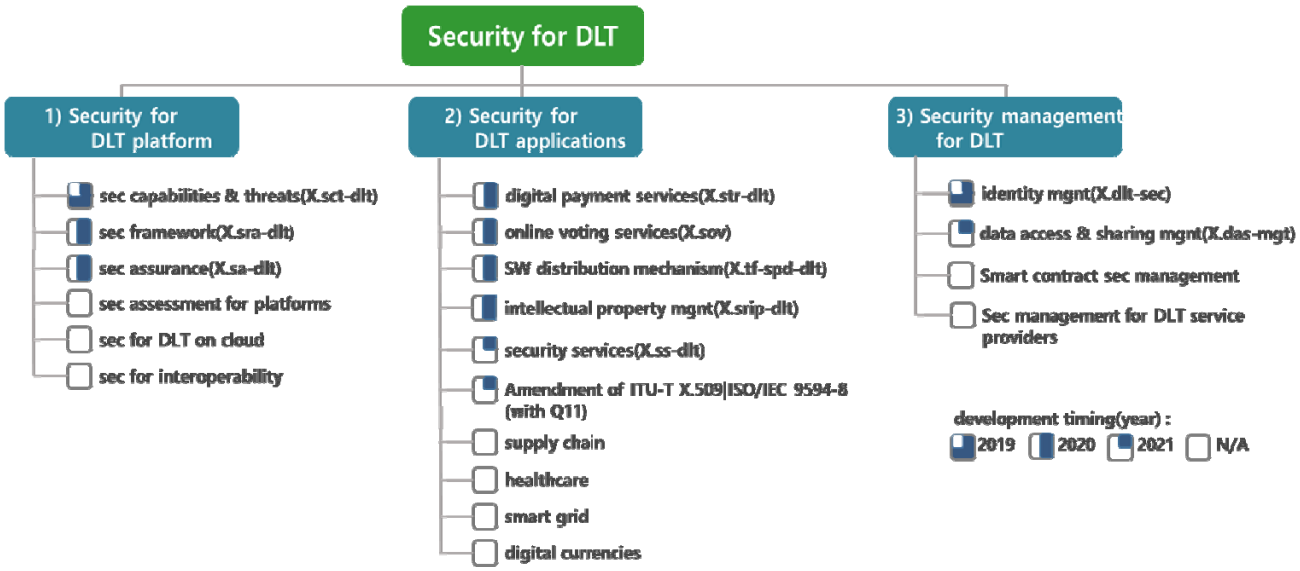
■経緯

- 2017年3月のITU-T SG17会合の前日に、ブロックチェーンに関するワークショップ（Security Aspects of Blockchain）を実施。この会合の結果を受けて、ブロックチェーンに関する新規のフォーカスグループをTSAGに提案。
- 2017年5月のITU-T TSAG会合でFG DLT（Focus Group on Application of Distributed Ledger Technology）が設立され、活動を開始。
- 2018年8～9月のITU-T SG17会合において、DLTをテーマとする新課題設立の提案が行われ、SG17の課題構成見直しの議論を始めることを条件に新課題、課題14「Security aspects for Distributed Ledger Technologies」を設立。

Blockchain/DLTに関する標準化



課題14におけるロードマップ



プラットフォームの
セキュリティ

アプリケーションの
セキュリティ

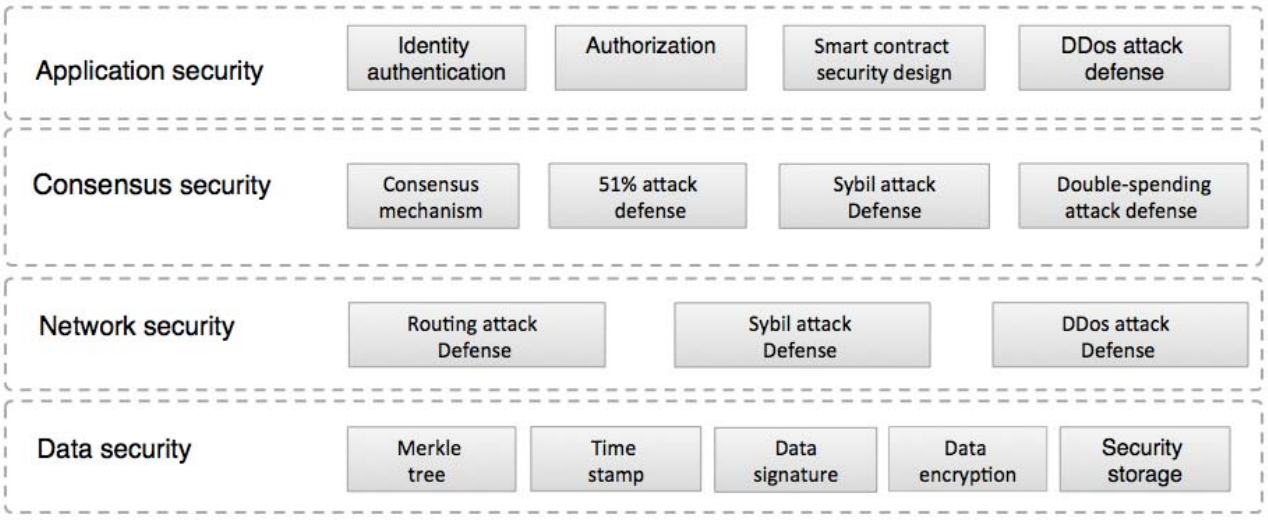
セキュリティ管理

X.sra-dlt
Security framework for Distributed Ledger Technology

KDDI Research

■概要

- DLTに関するセキュリティ上の脅威（sct-dltで整理）、セキュリティ要件を整理し、セキュリティ要件に利用できる機能を規定する。
- 上記を満たすセキュリティフレームワークを提供する。



DLTにおけるセキュリティ確保で利用できる機能

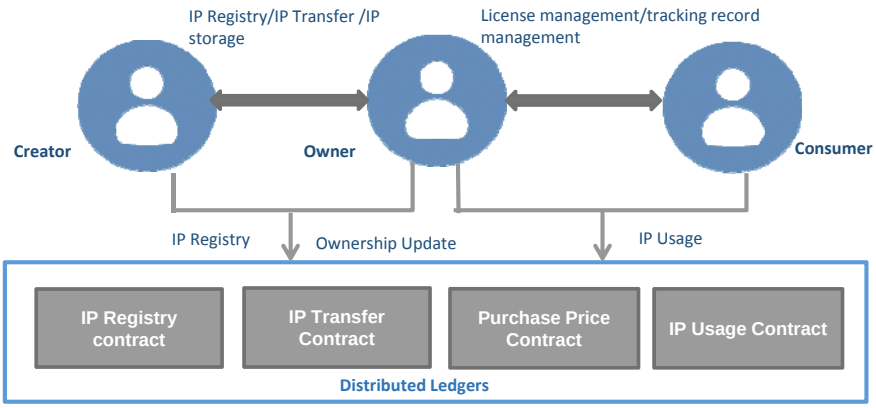
X.srip-dlt

KDDI Research

Security requirements for intellectual property management based on distributed ledger technology

■概要

- デジタルコンテンツ（テキスト、イメージ、サウンド、ビデオ、等）の配布、制御、追跡を行うためのシステムをDLTを使用して構築した場合のセキュリティ上の脅威と対策を規定している。



DLTを利用した知的財産管理の概要

AI/ML & Security

（2019年1月にワークショップ実施）

AI/MLに関するセキュリティワークショップ

■概要

- AI（人工知能）とML（機械学習）に関するワークショップを2019年1月のSG17会合にあわせて開催。
- 開催目的は、下記の通り。
  - AI/MLとセキュリティ/プライバシーの関係
  - AI/MLがサイバー攻撃にどのように使われるのか？
  - セキュリティとトラストにAI/MLを組み込むことはできるのか？
  - AI/MLを利用したアプリケーション／サービスに対するセキュリティ
  - SG17としての取り組み検討

■ITU-T SG17としての取り組み

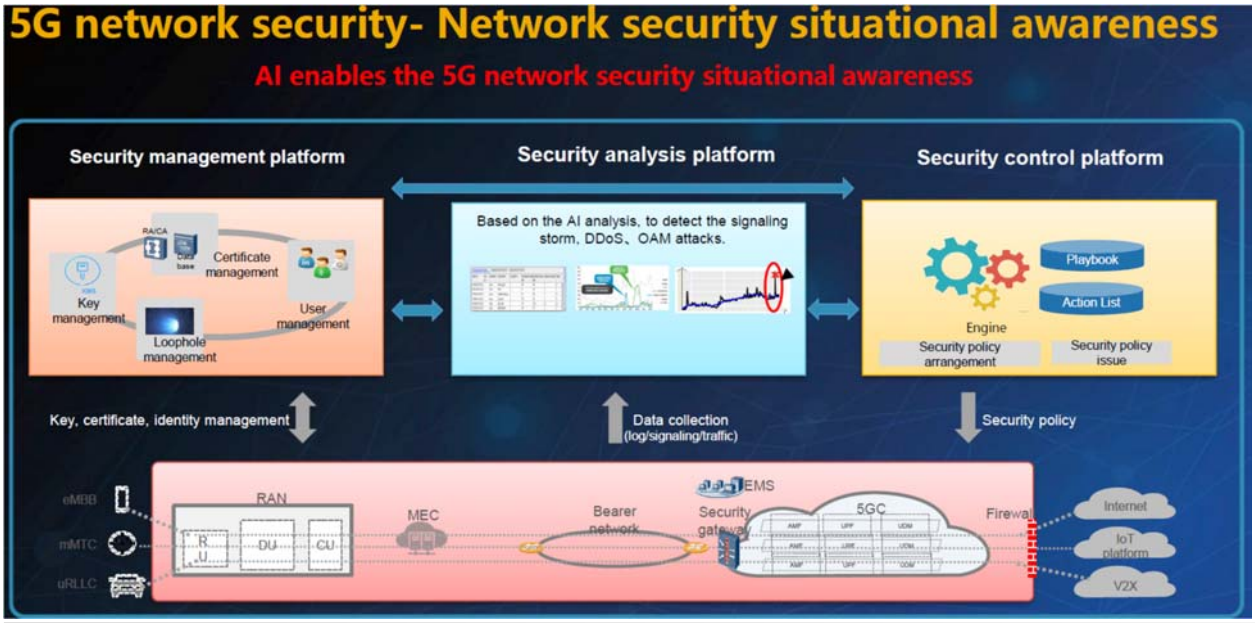
- 各課題において、AI/MLに関する検討の要否を検討し、AI/MLに関する取り組みを行うのであれば、課題テキスト（ToR: Terms of Reference）を修正する。

AI in 5G Security

KDDI Research

■概要

- 3GPP仕様でネットワークのデータを解析するためのインタフェース、サービスを制御するためのインタフェースが規定されており、これらを使ってAI/ML解析を行い、その結果をセキュリティ対策に活用することが可能となっている。

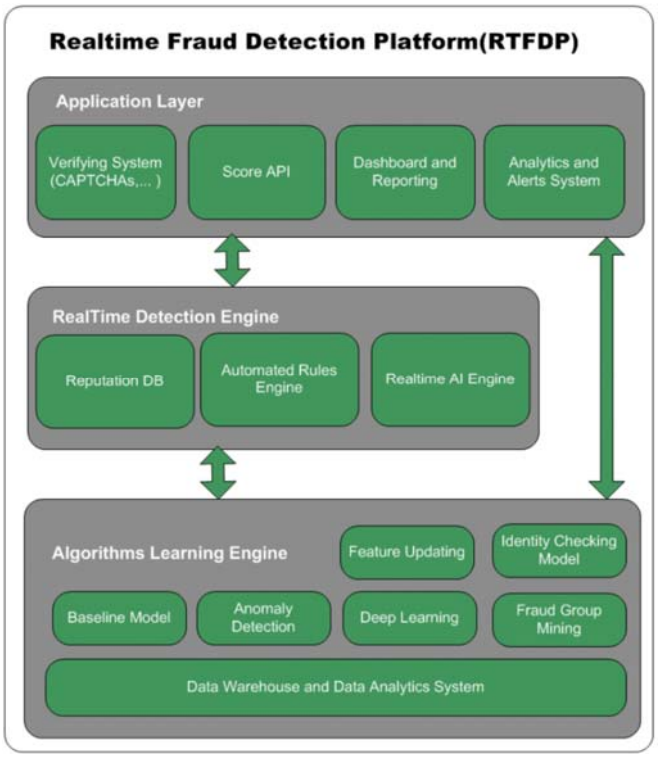


Online Fraud Detection with AI

KDDI Research

■概要

- オンラインサービスでの不正利用発見にAIを利用した事例を紹介。
- これまで、不正利用に対して多要素認証、デバイスの利用環境の情報、レピュテーション情報、ルールエンジンで検知してきた。
- AIを利用して過去の利用履歴から不正を検知する仕組みを導入。
- ユーザからの不正な情報取得、偽アプリのインストール、アカウント乗っ取り、ボットネット感染等を検出。また、マーケティングにも活用している。



KDDI Research