資料4－3

総務省
MIC Ministry of Internal Affairs and Communications

新たなサイバー脅威に対する検討グループの設置について

平成26年1月15日
事　　務　　局

新たなサイバー脅威に対する検討グループの設置

1. 概要

■ ICTの進歩に伴い、サイバー攻撃も複雑化・高度化してきており、未知の脆弱性を悪用した攻撃や、また従来では情報セキュリティ対策が重要視されていなかった分野における攻撃など、サイバー空間において新たな脅威が生まれてきている。

■ このような状況を踏まえ、情報セキュリティアドバイザリーボード ワーキンググループの下に、検討グループを設置し、新たなサイバー脅威への対策と促進方策、その中での行政の役割などについて検討する。

2. 検討体制

情報セキュリティ アドバイザリーボード

【構成員】(敬称略)

(座　長)	山口　英	奈良先端科学技術大学院大学　教授
(座長代理)	林　紘一郎	情報セキュリティ大学院大学　前学長・教授
	飯塚　久夫	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　会長
	岡村　久道	国立情報学研究所客員教授・弁護士
	藤沢　久美	シンクタンク・ソフィアバンク　代表
(顧　問)	小野寺　正	KDDI株式会社　代表取締役会長

ワーキンググループ

【構成員】技術系や法律系などの有識者、電気通信事業者等
(主査)　上原　哲太郎　立命館大学情報理工学部　教授

ITSセキュリティ検討グループ

【目的】
ITS(高度道路交通システム)による通信に求められるセキュリティ要件をはじめとした車の情報セキュリティについて検討を行う。

【構成員】
情報セキュリティの技術者、有識者、機器メーカ、ASV(先進安全自動車)、ORSE、UTMS協会、JARI等から選定。

【アウトプット】
当初は車車間、路車間通信に求められるセキュリティ要件に関するガイドラインを策定。段階的に車内ネットワークのセキュリティ要件まで議論の対象として広げ、今後のセキュリティ対策室の施策に反映。

未知の脆弱性対策検討グループ

【目的】
インターネットエクスプローラやCMS等のソフトウェア及びシステムに対する未知の脆弱性を悪用した攻撃への対策(攻撃防止、攻撃の早期検知、被害最小化等)について検討を行う。

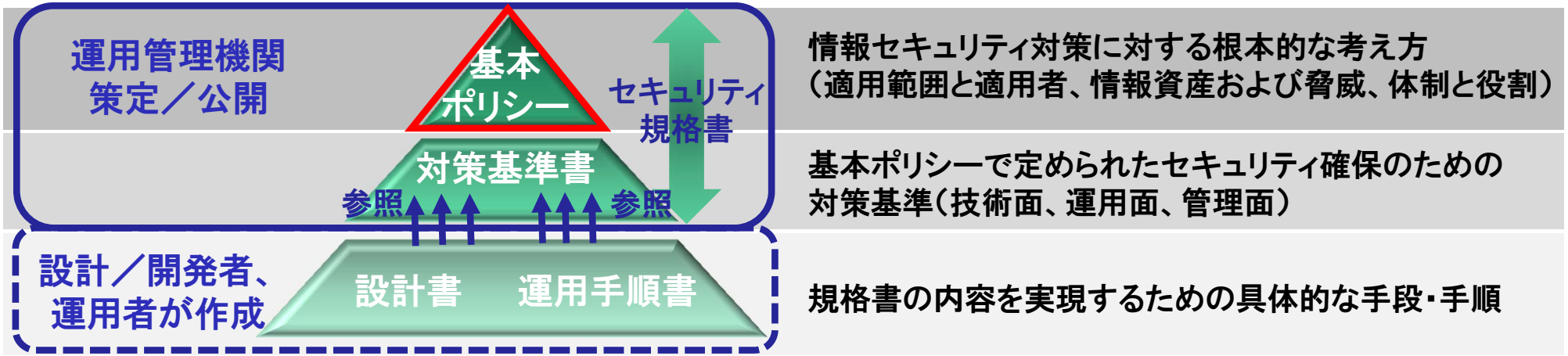
【構成員】
情報セキュリティの技術者、有識者を中心に選定。

【アウトプット】
今後のセキュリティ対策室の施策に反映。

検討グループの活動内容(案)　ITSセキュリティ検討グループ

【課題】 緊急車両への「なりすまし」や自動車の駆動系へのハッキング等を防ぐためのセキュリティ対策が必要。

サービスイメージ



対象の定義　：　システムのモデル化

↓

リスク分析　：　脅威の洗い出しとリスク評価

↓

基本ポリシー策定：　対策をおこなう脅威の抽出

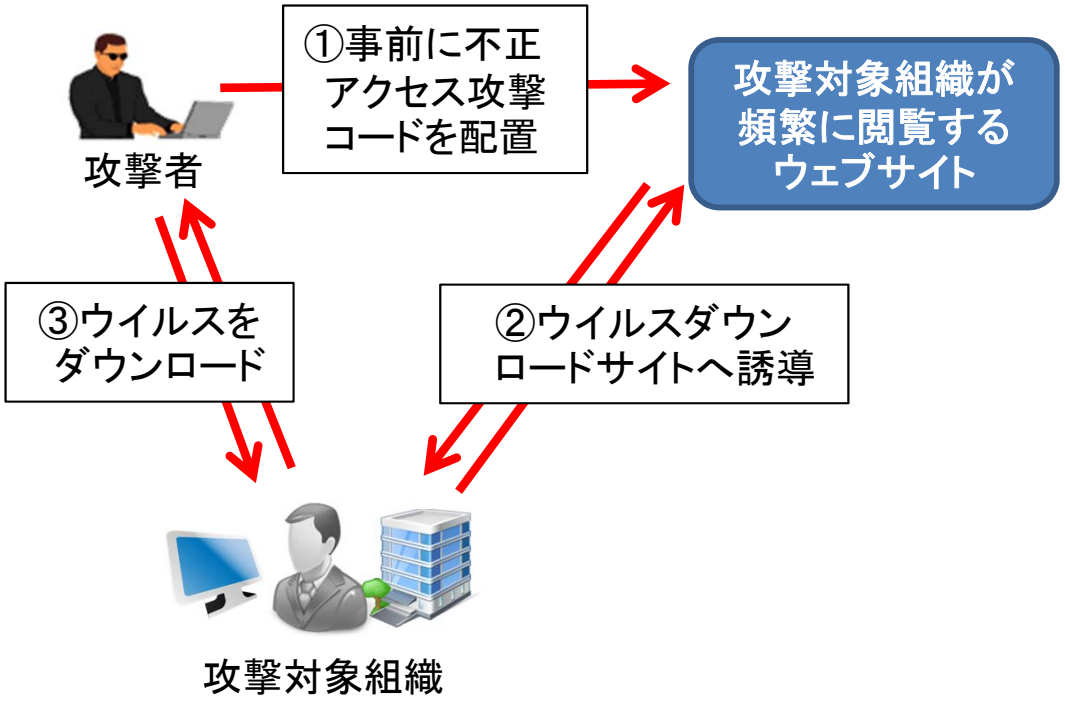
↓

対策基準の策定　：　対策目標の策定

検討グループでは、基本ポリシー・対策基準等について議論。
あわせて、パブリックコメントにより広く意見を募集する予定。

検討グループの活動内容(案)　未知の脆弱性対策検討グループ

複雑化するサイバー攻撃の例【水飲み場型攻撃※】



※水飲み場型攻撃:　攻撃対象組織が頻繁に閲覧するウェブサイト(水飲み場)でターゲットを待ち受け、攻撃対象組織を狙ってウイルス感染などをさせる攻撃のこと

【攻撃の特徴】
- 攻撃対象組織を限定(例:政府機関等)
- 攻撃対象組織が頻繁に閲覧するウェブサイトを選定
- ウェブサイトに罠を仕掛けを閲覧しただけでウイルスに感染
- **未発表、未修正の脆弱性を攻撃に利用**

- 強制的にウイルスに感染させられる
- **ゼロデイ攻撃※**の場合、感染に気付かない。

⇒　**早期発見・早期対処が困難**

- 攻撃防止、攻撃の早期検知、被害最小化、関係機関間の情報共有・相互連携のあり方等について検討を行う

※ゼロデイ攻撃:脆弱性情報が判明してから修正プログラムが提供される前に行われる攻撃