資料５－６
【Ｐ７は、構成員及び事務局限り】

「スマートフォン・クラウドセキュリティ研究会」の今後の進め方（案）

総務省 情報流通行政局
情報セキュリティ対策室

平成24年２月１日

中間報告と今後の検討の方向性

中間報告

中間報告においては、スマートフォンの情報セキュリティレベルの向上のために、早急に講ずべき対策を取りまとめるとの観点から、
（1）携帯電話事業者及び端末製造事業者において導入を検討されるべき対策
（2）利用者への普及啓発の内容や周知の方法
について、有効かつ現実に即した方策をとりまとめた。

（ア）課題として提起はしたが、対策を打ち出していない課題や、
（イ）対策を打ち出しはしたが、更なる深掘りや他の対策がありうる課題
がある。

検討の方向性

中間報告までの検討においては、クラウド利用に関する課題については扱わなかった。その中で積み残した上述（ア）（イ）の課題に関する対策を検討する必要があるため、
1．OS・アプリ・ネットワークや、端末内データ、ビジネスモデルの変容に伴う課題等
について検討する。

また、今後は、
2－1．スマートフォンからのクラウド利用に付随する課題とその対策
についても検討していく。さらに、クラウドの検討については、スマートフォンの情報セキュリティレベル向上のための有効な策としての位置付けも重要であることから、
2－2．クラウドを利用することにより、スマートフォンをより安全に使用するための方策
についても、「2－1．」と一体的に検討していく。

1. OS・アプリ・ネットワークや、端末内データ、ビジネスモデルの変容に伴う課題等

中間報告で対策を打ち出しはしたが、更なる深掘りや他の対策がありうる課題

【OS】
〇OSのぜい弱性について、OS堅牢化等に関するOSベンダとの連携方策や、その他国際的な連携方策等

【アプリケーション】
〇開発者の身元の把握、開発者への教育等アプリ開発者の信頼性向上策
〇権限の強いセキュリティ対策ソフトの開発や、導入推進に関する方策

【ネットワーク】
〇今後の無線LAN利用の本格的普及に向けた対策の方向性（ユーザの識別・認証等）

課題として提起はしたが、対策を打ち出していない課題

【端末内データ】
〇端末ではなく、クラウドで格納・利用することに伴う課題

【ビジネスモデルの変容】
〇OSのぜい弱性について、OS堅牢化等に関するOSベンダとの連携方策や、その他国際的な連携方策等（再掲）

上記課題等について、引き続き検討。

2－1. スマートフォンからのクラウド利用に付随する課題とその対策

既存ガイドライン等におけるスマートフォンからのクラウド利用の取扱い

○クライアントとして、スマートフォンが利用される旨の記載をしているガイドラインは存在。

例：✔携帯電話端末やスマートフォンなどを活用したモバイルクラウドサービスも展開が期待（スマート・クラウド戦略）

✔クラウドサービスでは，スマートフォンなどの携帯端末での利用を前提として提供されている場合があるため，それらの端末の利用についても留意することが望ましい。（クラウドサービス利用のための情報セキュリティマネジメントガイドライン）

✔Client-Side Protection; Maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones. Their size and portability can result in the loss of physical control. (NIST)

✔PHYSICAL SECURITY; Do your personnel use portable equipment (e.g.,. laptops, smart phones) which can give access to the data centre? (ENISA)

○しかし、スマートフォンからの利用を意識した具体的な検討は不十分。

検討が必要と考えられる論点

○PCに比べて処理性能や機能が劣るスマートフォンからのクラウド利用に付随する課題があるのではないか。

例：認証機能に乏しいスマートフォンからの接続要求を、クラウド側でどう識別するか。

○機能的制約があるスマートフォンを踏み台とした攻撃は、クラウドにとって脅威か。

○スマートフォン用のクラウドに対して、PC等から容易に攻撃されてしまうことはないか。

例：電話帳データや携帯電話事業者が提供するものなど、主にスマートフォンからの利用を意図したクラウド。

○そのほか、スマートフォンを通じた利用が進み、クラウドの利用主体・利用形態の多様化による課題があるのではないか。

上記論点について、課題を抽出し、対策を検討。

（参考）クラウド関連ガイドライン等における情報セキュリティの取扱い

大項目	小項目	国内							海外	
		総務省1	総務省2	総務省3	経産省1	経産省2	ASPIC	IPA1	IPA2	NIST	ENISA
対象者	利用者	○			○	企業	企業	中小企業		○	○
	クラウド事業者	○	○	○	△	○			○		
サービス形態	IaaS	○		○	○	△	○		区別せず	○	○
	PaaS	○		○	○	△	○			○	○
	SaaS	○	○	○	○	○	○	○		○	○
利用者による分類	パブリッククラウド	○	区別せず	区別せず	区別せず	区別せず	○	区別せず	区別せず	○	○
	コミュニティクラウド/パートナークラウド	○								△	○
	プライベートクラウド	○					△			△	○
	ハイブリッドクラウド	○					△			△	○
セキュリティ領域	マルウェア対策	○	○	○	○	○		○	○	○	○
	スパム対策					○				○	△
	情報漏えい対策	○	○	○	○	○	○	○	○	○	○
	SLA	○	○	○	○	○	○	○	○	○	○
	スマートフォンからの利用	○			○					○	○

総務省1：スマート･クラウド戦略(2011年5月)
総務省2：ＡＳＰ･ＳａａＳにおける情報セキュリティ対策ガイドライン（2008年1月）
総務省3：クラウドサービスの安全・信頼性に係る情報開示指針（IaaS･PaaS：2011年12月、SaaS：2007年11月）
経産省1：クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2011年4月）
経産省2：SaaS向けSLAガイドライン（2008年1月）
ASPIC　：クラウドサービス利用者の保護とコンプライアンス確保のためのガイド（2011年7月）
IPA1　：中小企業のためのクラウドサービス安全利用の手引き（2011年4月）
IPA2　：クラウド事業者による情報開示の参照ガイド（2011年4月）
NIST　：Guidelines on Security and Privacy in Public Cloud Computing（2011年12月）
ENISA：Benefits, risk and recommendations for information security（2009年11月）

（事務局調べ）

スマートフォンとクラウドの親和性の高さ

○スマートフォンは、携帯電話網や無線LANなど、多様なネットワークを活用できるため、ネットワークを通じてクラウドを利用しやすい端末。

○スマートフォンは、PCに比べれば記録容量が小さいため、データをクラウドに預けることにより大規模なデータを活用できる可能性。

セキュリティ対策としてのクラウドの利用

○スマートフォンではなく、クラウド側で一部又は全部のデータを持つことにより、スマートフォンの情報セキュリティレベルを向上することができるのではないか。

○さらに、スマートフォンを表示装置として扱い、クラウド側でスマートフォン端末をエミュレートすることにより、OS等構造上の問題を解決できるのではないか。

○そのほか、クラウド側で、スマートフォンの情報セキュリティレベルの向上が図れるのではないか。

例：✔クラウド経由で、メールの送受信やウェブサイトの閲覧を行うことにより、クラウド側でフィルタリング。

✔万が一攻撃を受けた場合に備え、クラウド側でモニタリング・証跡確保。

上記対策について、実現可能性や留意点を検討。