JEITA

IS－11－技標－ 1

セキュリティ市場・技術調査報告書

2011年3月

社団法人 電子情報技術産業協会

はじめに

本調査報告書は、セキュリティ市場・技術調査専門委員会が、「今後求められる情報セキュリティ技術とビジネスの方向」に関する調査を行い、これまでの情報セキュリティ技術とビジネス環境や社会制度の変化を整理し、情報セキュリティに関する今後の技術開発やビジネス展開の方向について検討、分析した結果を報告するものである。

近年、急速な発展を遂げた情報システムとネットワークは、今や重要な社会基盤として国民の経済活動や生活を支えている。その一方、ICT 環境の発展と普及を背景にして、情報や情報インフラに対する脅威も刻々と変化してきており、それに対応する情報セキュリティ技術も発展してきた。ICT 環境が生活の一部としてより活用されるには、生活者が安全にそして安心して利用できる情報インフラが必要で、情報セキュリティ技術がますます重要になってくる。しかし、情報セキュリティビジネスは依然として米国企業が主導しており、日本企業が先行する技術開発は限定的な領域にとどまっているのが現状である。したがって、我が国の ICT 関連企業においては、今後重要となる情報セキュリティ技術に着目し、そのビジネス展開の可能性を踏まえ、事業戦略を検討することが望まれる。

本年度の活動として当委員会は、情報セキュリティに関する今後の技術開発やビジネス展開の方向性を明らかにし、JEITA 会員企業のビジネスや事業戦略の策定に役立ててもらうことを目的として調査を行った。調査内容としては、(1)情報セキュリティ技術の動向と ICT 有望領域の調査、(2)ICT 有望領域における情報セキュリティ技術の動向調査、(3)重要な情報セキュリティ技術の展望と普及シナリオの調査をセキュリティに関する有識者や企業へのヒアリング、韓国の政府団体や企業の訪問視察などを通じて行い、その結果を、報告書としてとりまとめた。

本調査報告書の作成にあたり、視察およびヒアリングにご協力いただいた企業や有識者の方々、そして当専門委員会の関係の皆様に深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後のセキュリティビジネスの更なる発展に寄与できれば幸いである。

2011 年 3 月

セキュリティ市場・技術調査専門委員会
委員長　福島　孝文

セキュリティ市場・技術調査専門委員会名簿

（敬称略・順不同）

委員長	福島孝文	東芝テック㈱
副委員長	平木博史	㈱リコー
委員	伊藤丘	コニカミノルタビジネステクノロジーズ㈱
〃	武本敏	㈱日立製作所
〃	池田政弘	富士ゼロックス㈱
〃	池田恵一	富士通㈱
〃	白石節男	富士通㈱
〃	米田健	三菱電機㈱
〃	畠山有子	三菱電機㈱
〃	遠藤淳	三菱電機インフォメーションテクノロジー㈱
オブザーバ	川口修司	㈱三菱総合研究所
〃	江連三香	㈱三菱総合研究所
〃	井上信吾	㈱三菱総合研究所
事務局	吉田晃	（社）電子情報技術産業協会

目次

第 1 章 情報セキュリティ技術が不可欠な ICT 有望領域 1
1.1 有望領域の選定 1
1.2 クラウドコンピューティング 2
1.3 スマートグリッド 3
1.4 デジタルサイネージ 4
1.5 スマートデバイス 5
1.6 位置情報サービス（LBS：Location-Based Services） 6
1.7 国民 ID 7
1.8 PCI DSS 8
第 2 章 有望領域における情報セキュリティ技術の関連動向 9
2.1 有望技術の選定 9
2.2 ID 管理 10
2.3 組込みセキュリティ 13
2.3.1 スマートデバイス 13
2.3.2 スマートメータ 15
第 3 章 重要な情報セキュリティ技術の展望 16
3.1 ID 管理 16
3.1.1 ID 管理技術の展望 16
3.1.2 ID 管理技術の普及シナリオ 16
3.1.3 ID 管理技術の普及に向けた課題 17
3.2 組込みセキュリティ 18
3.2.1 組込みセキュリティ技術の展望 18
3.2.2 組込みセキュリティ技術の普及シナリオ 18
3.2.3 組込みセキュリティ技術の普及に向けた課題 19
第 4 章 今後のセキュリティビジネスに向けた提言 20
4.1 ID 管理 20
4.1.1 クラウドコンピューティングにおける ID 管理の方向性 20
4.1.2 国民 ID 制度における ID 管理の方向性 21
4.1.3 今後のセキュリティビジネスの課題と提言 22
4.2 組込みセキュリティ 24
4.2.1 組込みセキュリティの C.I.A 24
4.2.2 組込みセキュリティ機能の維持管理 25
4.2.3 組込みセキュリティ分野におけるビジネス展開 26

第1章　情報セキュリティ技術が不可欠な ICT 有望領域

1.1 有望領域の選定

急速な発展を遂げた情報システムとネットワークは、今や重要な社会基盤として、国民の経済活動や生活を支えている。その一方、そうした ICT 環境の発展と普及を背景に、情報や情報インフラに対する脅威も刻々と変化しており、それに対応する情報セキュリティ技術も発展してきた。JEITA 会員企業としては、今後重要となる情報セキュリティ技術に着目し、そのビジネス展開の可能性を踏まえ、事業戦略を検討することが望まれる。本章では、ICT 分野の有望領域の方向とその領域における情報セキュリティ技術を洗い出すこととする。

ICT 市場の規模、社会基盤としての重要性（影響範囲）、セキュリティ技術の重要性（役割の大きさ）の尺度から、本委員会として、情報セキュリティ技術が必要不可欠な ICT 有望領域として以下の表の左欄に示す 7 つの領域を選定した。

表 1.1-1　情報セキュリティ技術が必要不可欠な ICT 有望領域

	市場規模予測	社会基盤としての重要性	セキュリティ技術の重要性
(1)クラウドコンピューティング	○	◎	◎
(2)スマートグリッド	○	◎	○
(3)デジタルサイネージ	○	△	△
(4)スマートデバイス	○	○	○
(5)位置情報サービス	△	△	○
(6)国民 ID	○	◎	○
(7)PCI DSS	△	△	◎

（本委員会での評価基準）

市場規模：2015 年におおよそ 1,000 億円を超える市場規模をもつと想定されるものを○、それ以外のものを△とした。

社会基盤としての重要性：IT 障害発生時に国民生活や社会経済活動に深刻な問題を起こしうるものを◎、問題となるものを○、それ以外のものを△とした。

セキュリティ技術の重要性：その領域におけるセキュリティ技術の役割を考慮し、特に重要ならば◎、重要ならば○、それ以外のものを△とした。

以下、上記 7 つの領域について、個々の領域の動向概要と求められる情報セキュリティ技術について概説する。

1.2 クラウドコンピューティング

ユーザ（企業、個人）がインターネット経由でコンピュータ処理をサービスとして利用する形態のうち、ここでは主に一般向けサービスであるパブリッククラウドを考慮の対象とする。クラウドサービスを提供する側のデータセンターでは仮想化技術が用いられ、ユーザの要望するサービスを提供するために様々な標準規格が用いられている。

パブリッククラウド範囲における 2009 年の日本国内クラウドサービス市場の規模は 312 億円。2014 年の市場規模の予測は 1,432 億円である[1)]。国内 IT ベンダからは、企業固有のシステムのプライベートクラウド化のような高付加価値サービスが提供されており、今後これらの利用も増えると予測されている[2)]。

クラウドはサービスの効率化や価値創造のニーズを満たす新しいインフラである。多くの IT ベンダにおいてデータセンターにクラウド基盤が構築され、既にサービス事業が行われている。クラウドは位置情報サービス等の高度なサービスの提供基盤としても既に多用されている。

クラウドによりネットワークを利用したサービス提供を実現するためにはセキュリティ確保は不可欠である。以下の表に、クラウドコンピューティングの推進に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.2-1　クラウドコンピューティングの推進に際して必要な情報セキュリティの例

項目	概要
アプリケーション セキュリティ対策	開発ライフサイクルに沿ったセキュリティ実現、ヴァーチャルマシンの要塞化、ホスト間通信のセキュア化、ログおよびデバグ情報の管理 等
鍵管理対策	クラウド提供者と利用者を考慮した鍵管理の実現 等
ID 管理、アクセス管理対策	プロヴィジョニング技術、認証技術（SaaS、PaaS での Google、OpenID 等の認証の利用、IaaS での VPN 技術、SAML、SSL、OpenID 等の利用）フェデレーション技術（SAML、WS-Federation 等）、アクセス制御 等
仮想化セキュリティ対策	VM 内およびハイパーバイザーのセキュリティコントロールの理解。各 VM の分離（孤立化）の徹底と確認 等

1) IDC Japan プレスリリース，http://www.idcjapan.co.jp/Press/Current/20100412Apr.html
2) 矢野経済研究所，“クラウドコンピューティング市場に関する調査結果 2009”，http://www.yano.co.jp/press/press.php/569

1.3 スマートグリッド

電力網の信頼性向上、情報通信機能の強化、電力網における用途の多様化への対応（太陽光発電等の再生可能エネルギーと電力系統との連係等）を考慮した送電網や蓄電システムがあり、家庭や地域におけるエネルギー利用の高効率化が図られている[3)4)]。

スマートグリッドにおける基幹機器であるパワーネットワーク関連機器の市場規模は、2009 年は約 7,056 億円、2014 年予測は 1 兆 700 億円と予測されている[5)]。

社会インフラである電力の供給の効率化に係る技術であり、混乱が生じると影響は広い範囲に及ぶ可能性がある。

重要インフラとしての信頼性を確保しつつ ICT 技術を活用するためには、本来機能を阻害せず、かつ十分な安全性が確保できるように、適切なセキュリティ技術を用いる必要がある。以下の表に、スマートグリッドの推進に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.3-1　スマートグリッドの推進に際して必要な情報セキュリティの例

項目	概要
制御システム・スマートメータの侵入対策	侵入対策等の基本的セキュリティ対策の推進
制御システム・スマートメータの脆弱性対策	アプリケーションソフトウェア、OS、ミドルウェア、組込み機器等の脆弱性対策の推進
プライバシー情報対策	プライバシー情報に配慮したデータ管理手法（収集・集計手法）の実現

3) “米国におけるスマートグリッド構想の動向”，http://e-public.nttdata.co.jp/f/repo/685_u1003/u1003.aspx
4) “いよいよ動き出す「日本版スマートグリッド」”，http://techon.nikkeibp.co.jp/article/TOPCOL/20090707/172655/
5) 富士経済プレスリリース，“パワーネットワーク（電力・ガス供給網）関連機器市場を調査”，http://www.group.fuji-keizai.co.jp/press/pdf/100414_10034.pdf

1.4 デジタルサイネージ

デジタル通信によって配信された映像や情報をディスプレイやプロジェクターでデジタル表示する媒体であり、ここではデジタルフォトフレームを利用した簡便なものから大型ディスプレイまで幅広く、店舗や社内等に設置されるものを含めて考える。現在は、流通・交通分野を中心に導入事例が多数ある。ハードウェア・ソフトウェアは共に途上段階にあり、規模もさまざまである。コンテンツのライフサイクルは従来の広告に比べ比較的短い。将来は、ハイヴィジョン化、インタラクティブな情報提供、位置情報の併用、携帯電話等との連携、配信の効率化、相互接続（システムの標準化、広告の交換）、ディスプレイのアンビエント化などが予想されている。

2009 年は 602.7 億円、2015 年には 1,260 億円以上まで拡大すると予測されている[6]。別の調査では 2009 年度は 557.1 億円。2015 年度には 1,300 億円に迫ると予測されている[7]。

広告・販売促進、情報提供サービスを中心に広く普及している。大規模なシステムは流通等を中心に普及し、今後はコンテンツの提供手法を関心の中心に移していくものと思われる。より小規模なシステムは位置情報、AR（Augmented Reality：拡張現実感）技術等の IT 技術と複合的に活用され新たなサービスを提供する可能性がある。

安定した配信を行うためには、妨害・改ざん等を受けない性質が必要となる。また高い信頼性のサービスを提供する必要がある。以下の表に、デジタルサイネージの推進に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.4-1　デジタルサイネージの推進に際して必要な情報セキュリティの例

項目	概要
コンテンツセキュリティ	サーバを対象とするセキュリティ対策
組込みシステムセキュリティ	組込みソフトウェアに関するセキュリティ対策

6) 富士キメラ総研調査，https://www.fcr.co.jp/report/093q12.htm
7) 矢野経済研究所調査，http://www.yanoict.com/yzreport/115#a2

1.5 スマートデバイス

スマートフォン、スマートブック（ネットブック PC よりも小型な製品）、電子書籍を読むための端末等を含み、携帯電話の携帯性と PC の持つ高機能性・多機能を兼ね備えるデバイスと位置づけられる。多くは、カメラ、GPS、無線 LAN 機能、RF-ID リーダ等の機能を組込みハードウェアとしても備えており、これらを活用した業務等への利用も可能となる。

市場規模としては、スマートフォンの 2009 年国内出荷台数は 194.5 万台、2013 年には 571 万台となる予測が示されている[8)]。

現時点では個人が購入しプライベートで用いている比率が高いが、購入者の 8 割が業務用途での利用により効率が向上すると考えており、今後、企業への導入事例が増加する傾向にあると推測される[9)]。スケジュール管理、文書の閲覧・編集等を外出先等で行うために用いられるが、特に営業、受発注等の業務支援に活用する事例も増えつつある。

スマートデバイスを持ち出した先で社内データにアクセスすることは情報漏えいリスクを高めることとなるため、情報セキュリティ上の対策は不可欠である。また、PC と同様にウイルス等の脅威がスマートデバイスを対象とする場合も増えている。携帯電話と比較して、汎用 OS が実装されているスマートデバイスのセキュリティ対策は利用者に任される面も多く、注意が必要である。以下の表に、スマートデバイスの活用に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.5-1　スマートデバイスの活用に際して必要な情報セキュリティの例

項目	概要
不正使用対策	・パスワード／指紋等による認証
データ漏えい・破壊対策	・端末ロック機能、リモートからのデータ消去機能 ・暗号化によるデータ保護
ウイルス感染対策、 ネットワーク経由からの侵入対策	・アンチウイルス、ファイアウォール、ウェブフィルタリング

8) 矢野経済研究所，“スマートフォン市場に関する調査結果 2010”，http://www.yano.co.jp/press/pdf/605.pdf
9) モバイルコンピューティング推進コンソーシアム，“2010 年スマートフォン導入構築ガイド 第 2 版”，http://www.mcpc-jp.org/smartphone/SmartPhoneBuildGuide.pdf

1.6 位置情報サービス（LBS：Location-Based Services）

携帯端末により得られた位置情報を活用してユーザに役立つコンテンツを提供するサービスであり、携帯端末からモバイルネットワークを介してアクセス可能である。提供されるコンテンツは、地図情報に位置、時間、付近の場所や人間の属性情報を付加したもので、クーポン等の広告の形態を取ることもある。位置情報の検索を伴う店舗案内ポータル、位置情報を用いたゲーム、位置情報を基軸にしたコミュニティ形成を行うソーシャル・ネットワーク等が含まれる。

市場規模としては、GPS ナビゲーション市場と位置情報サービス市場を合わせ、全世界で 2009 年の約 16 億ドルから 2014 年には約 134 億ドルになると見込まれている。特にアジアにおける最大の LBS 市場は日本とされており、2014 年には約 17 億ドル（約 1,500 億円）と予想されている[10)]。

位置情報そのものを提供するサービス以外に、位置情報を基軸に更なる付加価値を持つ各種のサービス（ソーシャルネットワークサービスや位置に広告提供するサービス等）が普及し、ウェブ同様のインフラとなる可能性がある。将来的には地図情報上での複数のサービスが統合され、利用者がウェブを意識しない方向に進む可能性がある。

サービス利用者が任意の地点でログインしサービスを安全に利用するためにはセキュリティ技術が必要となる。また、位置情報を伝える必要が無いタイミングでは情報を伝えないようにアクセス制御を行う必要がある。以下の表に、位置情報サービスの推進に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.6-1　位置情報サービス（LBS）の推進に際して必要な情報セキュリティの例

項目	概要
サービスの不正利用対策	・認証機能の実装
プライバシー対策	・位置情報の利用／収集を拒否できるようなアプリケーション毎のコントロール機能の実装

10) IE Market Research, “3Q.2010 Global GPS Navigation and Location Based Services Forecast, 2010 - 2014: Global market for GPS navigation and location based mobile services to rise to $13.4 billion in 2014, a CAGR of 51.3%”, https://www.iemarketresearch.com/Members/Reports/3Q-2010-Global-GPS-Navigation-and-Location-Based-Services-Forecast-2010--2014-Global-market-for-GPS-navigation-and-location-based-mobile-services-to-rise-to-13-4-billion-in-2014-a-CAGR-of-51-3--RID1480-1.aspx

1.7 国民 ID

国民 ID は、国民等に識別番号を割り当てることで行政サービスの品質と効率の向上を目指すものである。税制上、所得の正確な把握のために個人識別番号が必要となるため導入が検討されている。利用範囲は、税務分野および社会保障分野、その他の公的手続が挙げられており、含める範囲については複数案を検討中である。ID に、住民票コード、基礎年金番号、新規に割り当てる番号のどれを使うかは確定していない[11)]。

6 月末に公表された内閣官房の「社会保障・税に関わる番号制度に関する研究会」の試算によれば、国民 ID 制度のシステム開発規模は、国民 ID を税務のみに利用する場合は 5,300 億円程度、医療や介護、証明書発行業務等に用いる場合には 6,100 億円程度となっている（これらの試算値には運用や周辺事業の費用は含まれていない）。この試算では、「セキュリティ対策、プライバシー保護のためのシステム」には、2,000 億～3,000 億円が必要となると見込まれている[12),13)]。

現時点では制度の内容が具体化されていないが、実現された場合は少なくとも税務分野では不可欠な情報システムとなることが予想される。また、社会保障、医療分野でも利用されるのであれば、より国民生活に密接な形でシステムが関わってくると考えられる。

国民全体が関わる政府システムである性格から、外部からの不正行為に対して堅牢な作りであるだけでなく、目的外利用等の内部からの不正使用も防止することが求められ、セキュリティ面での対策が重要となっている。以下の表に、国民 ID の推進に際して必要と思われる情報セキュリティ技術の例を示す。

表 1.7-1　国民 ID の推進に際して必要な情報セキュリティの例

項目	概要
不正アクセス対策	・ID 連携／ID 管理技術（PKI 関連技術を含む） ・認証（パスワード、バイオメトリクス技術を含む） ・IC カード

11) 国家戦略室，“社会保障・税に関わる番号制度に関する検討会”，http://www.kantei.go.jp/jp/singi/kokkasenryaku/kaigi/shakaihoshou.html
12) IT 戦略本部，“新たな情報通信技術戦略工程表（案）”，http://www.kantei.go.jp/jp/singi/it2/dai54/siryou1.pdf
13) 日経コンピュータ Report，“国民 ID のシステム開発に 6100 億円”，http://itpro.nikkeibp.co.jp/article/COLUMN/20100706/349978/

1.8 PCI DSS

PCI DSS は、クレジットカード会社大手 5 社が共同で策定したクレジット業界向けのグローバルなセキュリティ標準である。クレジットカード情報と取引情報を保護する意図で作られており、セキュリティ対策の実装に関する具体的・定量的なベースライン要件が示されている。PCI DSS は 2010 年 10 月に新版 V2.0 に改訂されており、従来版よりも表現および内容がより明確化されている。また、関連する標準として、クレジットカード読取用端末装置のセキュリティ要件 PCI-PTS（Payment Card Industry PIN Transaction Security）、クレジットカード情報を扱うアプリケーションソフトウェア開発者向けガイドライン PCI PA-DSS（Payment Card Industry Payment Application Data Security Standard）がある。

先行する米国では、VISA に関しては 2010 年末時点で、レベル 1 加盟店（年間取引件数 600 万件超）の 96%、レベル 2 加盟店（年間取引件数 100 万～600 万件）の 96%が PCI DSS に準拠している[14]。国内では 2009 年に認定取得のための訪問審査を受けたレベル 1 加盟店（年間取引件数 600 万件超）は 30～40 社[15]であるが、今後普及拡大が見込まれる。

金融業、流通業、通信／メディア、製造業等の業界まで影響範囲は広い[16]。PCI DSS は、その明確さと、準拠すればある一定のセキュリティレベルが達成可能である点が評価されており、データセキュリティ基準のベストプラクティスとみなされているため、クレジット業界だけでなく他業界の企業や組織におけるセキュリティ基準として採用させようという動きが米国においてある。

クレジットカード情報を取り扱う上で、セキュリティ確保は必須であるため、一定の対策実施状況を評価できる基準は有用なものである。以下の表に、PCI DSS の普及に際して必要と思われる技術的対策の例を示す。

表 1.8-1　PCI DSS の普及に際して必要な技術的対策の例

項目	概要
サービスの充実	・非カード業界の企業・組織を想定した PCI DSS の適用サービス ・具体的・定量的実装項目の優先順位付けコンサルティング
対策手法の具体化	・要件に合わせた具体的対策手法のパッケージ／スイート化

14) U.S. PCI DSS Compliance Status（VISA），
http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf
15) “2010 年、「PCI DSS」普及の波は来るか！？”，http://www.shopbiz.jp/ic/column/pointpayment/55813.html
16) 日本カード情報セキュリティ協議会，“PCI DSS とは”，http://www.jcdsc.org/pci_dss.php

第2章 有望領域における情報セキュリティ技術の関連動向

2.1 有望技術の選定

本調査では、社会的影響やサービスの関連性等を勘案し、今後有望な ICT 領域として「クラウドコンピューティング」「スマートグリッド」「スマートデバイス」「国民 ID」「デジタルサイネージ」「位置情報サービス」を選択した。次に、各領域を支える重要な情報セキュリティ技術について採り上げ、それらの位置関係を下図に整理した。

下図から、特に 「ID 管理」、「組込みセキュリティ」「プライバシー保護」の技術は、複数の領域において重要な役割を果たし、影響力が大きいと考えられる。ただし、「プライバシー保護」は、検討範囲が技術的な領域に留まらず、倫理や社会通念に踏み込んだ議論が必要なテーマであるため、本年度の対象からは除くこととし、重要な技術として「ID 管理」と「組込みセキュリティ」を調査対象として選定した。

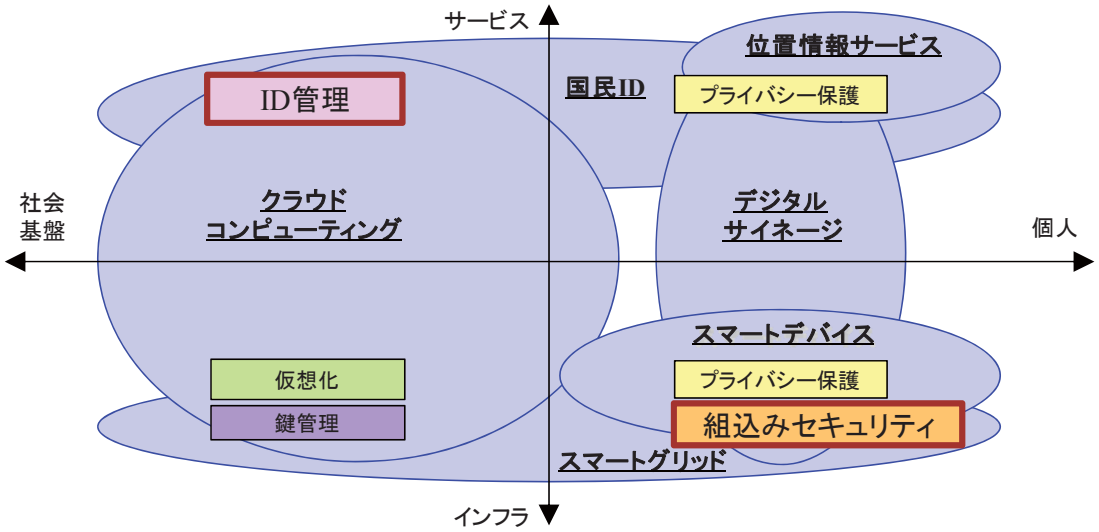


図 2.1-1　有望な ICT 領域と重要となる情報セキュリティ技術の関係

2.2 ID管理

クラウドコンピューティングにより可能となったSaaS形式のサービス提供形態では、サービス利用における利用者の認証・認可に関して新たな要件が必要となってきている。その背景には、下記のような理由が挙げられる。

(1)サービス共通機能としてのID管理業務が顕在化

ID管理機能はサービスに必須の機能であるが、サービス毎にシステム投資をしたくない

(2)管理作業の統合と効率化

利用者からの問い合わせ対応やセキュリティ確保のための運用業務の重複を回避したい

(3)利用者の利便性と一貫性の確保

サービス毎に異なる認証・認可システムが適用されると利用者の利便性が低下する

クラウドコンピューティング環境下でID管理を行うためのセキュリティ技術は、下記のカテゴリの元に標準化と実用化が進められている。

(1)SAML

IDを相互に連携することで安全にシングルサインオンを実現する技術。クラウド側のID管理システム同士をフェデレーションによって結び付け、別のサイトへ移動したときに、移動元のサイトと移動先のサイトが通信し、自動的に認証情報が引き継がれる。

(2)OpenID

ウェブサイトに依存せずに使用できる認証システムの標準、およびそこで使用される識別子である。発行元によらず、ひとつのOpenIDで、複数のOpenIDシステム対応サイトを利用することができる。OpenID Foundationにより推進された。

(3)CardSpace

「仮想的なカード」のメタファでアイデンティティ情報を管理するセキュリティ技術の総称。Information Card Foundationにより推進された技術セット。

これらの技術は、Liberty Alliance、OpenID Foundation、Information Card Foundationなど複数の団体が異なるアプローチで標準化・実用化を進めてきた。2009年6月に、ID管理について業界横断的に企画策定、相互運用を推進するための団体として、Kantara Initiativeが設立され、OpenID、SAML 2.0といった標準規格の相互運用性を高めながら、セキュリティやプライバシー保護など標準技術を確立する事を目指して活動を継続している（付録「今後求められる情報セキュリティ技術とビジネスの方向に関する調査報告書」P25参照）。

Kantara Initiative Japan WG

http://kantarainitiative.org/confluence/display/WGJ/Home

Open Identity Exchange （OIX）

http://www.openidentityexchange.org/

図 2.2-1　ID 管理技術に関する団体のホームページ

また、Open Identity Exchange （OIX） は、OpenID Foundation および Information Card Foundations により共同設立され、オンラインのアイデンティティ管理向けに、テクノロジーに依存しない認定トラスト・フレームワークを提供している。Google、PayPal、AT&T、Equifax、VeriSign、Verizon、CA technologies などの企業が OIX を支援している。

Kantara Initiative と Open Identity Exchange (OIX) は、2010 年 7 月、トラスト・フレームワークの基盤づくりに取り組む業界 2 大組織として、オンラインにおける堅牢なトラスト・エコシステムの構築と導入促進に向けて、デジタル・トラスト・フレームワークの開発で協業を開始することを発表している。

これらの動きに加えて、米国商務省の国立標準技術研究所（NIST）では、サイバースペースで信頼できるアイデンティティを確立するための戦略として、安全サイバーID 認証システム整備国家戦略（NSTIC： National Strategy for Trusted Identities in Cyberspace）の策定に取り組んでいる。NSTIC のドラフトは 2010 年 6 月と 7 月に発表されており、パブリックコメントを 反映して 2011 年に公開される予定としている。

これらの技術標準に共通に使用される要素技術として、下記のようなセキュリティ技術がある。これらは、上記標準の中でも要素として活用されることもあると同時に、相互にセキュリティ要素技術として利用されるケースもあり、基盤技術として定着しつつある。

(1)シングルサインオン（SSO）

1 度の認証で信頼関係にあるアプリケーションサービス群へのアクセスを可能とする技術。オープンソースの OpenSSO・OpenAM をはじめ、国内外のベンダによる製品も提供されている。

(2)トークナイゼーション

機密データを別の文字列（トークン）に置き換えることにより、機密データが散在する事を防ぐ情報管理技術。たとえば、PCI DSS では、クレジットカード番号にトー

クナイゼーションを適用することで、審査範囲を狭めることが可能である。

⑶PKI

PKI は強固なセキュリティを提供する要素技術として定着している。そのため、OpenID のような認証システムに適用して、脆弱性を低減するといった目的で応用されている。

⑷アイデンティティ・アクセスマネジメント

利用者の権限判定を行うアイデンティティプロビジョニング、利用者属性に応じた資源アクセス制御を可能にするユーザプロファイル管理、利用者のクレデンシャル情報を管理する認証などは、クラウドにおいて重要となるアイデンティティ・アクセス管理の要素技術となっている。

セキュリティは適用する技術要素に加えて、運用機構がそのレベルを左右する。そのため、ID 管理をどのように運用設計するか、利用モデルをどのように定めるかは、技術要素と表裏一体で重要になってきている。運用機構を ID 管理モデルとして分類すると、下記のようになる（付録「今後求められる情報セキュリティ技術とビジネスの方向に関する調査報告書」P32 参照）。

⑴フラットモデル（エストニア、スウェーデン、デンマーク、ベルギー、韓国、等）

一つの識別番号を全ての機関で共通に利用する

⑵セパレートモデル（ドイツ、スロベニア、（日本））

行政分野ごとに異なる個人識別番号を付番する

⑶セクトラルモデル（オーストリア）

統一番号からセクターごとに異なる番号が生成される

2.3 組込みセキュリティ

本節では、組込みシステムに対するセキュリティ技術動向として、スマートデバイスとスマートメータを採り上げる。

2.3.1 スマートデバイス

ここでは、スマートフォン、スマートブック(ネットブック PC よりも小型な製品。モバイルインターネット端末とも呼ばれる)、電子書籍を読むための端末などを”スマートデバイス”と位置づける。

「1.5 スマートデバイス」に記載の通り、スマートフォンをはじめとするスマートデバイスの普及が進み、個人利用だけでなく、企業などでの業務利用も始まりつつある。スマートデバイスを用いて、社外から社内データにアクセスするような利用シーンが増えてくると、取り扱われるデータの機密性が高まり、情報セキュリティのリスクも高まることになる。特に普及が進んでいるスマートフォンについては、既に Android OS を標的としたボット型ウイルスが発見され、情報処理推進機構(IPA)から注意喚起[17]が出されたり、日本語版の Android アプリにマルウェアが混入していることが報じられたりする[18]など、ウイルス被害を受ける可能性も高まっている。このような状況を受け、スマートフォン向けに、各社からセキュリティ対策製品が提供されている。これらはマルウェアの検知・駆除やファイアウォール等の機能の他、盗難・紛失時の対策として、遠隔でのデータ消去やロックの機能を有している。製品の特徴として、マルウェアの検出にレピュテーション技術を用いていることがあげられる。レピュテーション技術とは、ユーザからファイル情報を集め、送信元・作成者・作成時期・普及率などを総合的に加味して、安全性をスコアリングする技術であり、ファイルのスコアに基づき、マルウェアか否かの判断を行う。パソコン向けのセキュリティソフトで行われるシグネチャマッチングやヒューリスティック解析と比べて、端末側の処理が少なくて済むのが特徴である。

また、社外から社内ネットワークへのアクセス時の認証機能強化、緊急時のリモートロックやデバイス制御などの機能をサービスとして提供する事業者も出てきている[19] [20]。通信事業者や機器メーカなどを中心にスマートフォンやタブレット PC のセキュリティ上の課題を解決していくことを目的とした協議会[21]が発足するなど、今後スマートデバイスの

---

17) IPA “Android OS を標的としたウイルスに関する注意喚起”
http://www.ipa.go.jp/security/topics/alert20110121.html

18) シマンテック ”Android 用マルウェア、日本語版アプリにも混入”
http://communityjp.norton.com/t5/blogs/blogarticlepage/blog-id/npbj/article-id/68

19) 富士通ビー・エス・シー ”スマートフォン向けセキュリティ管理サービス”
http://www.bsc.fujitsu.com/services/fence/smartphone/

20) 三菱電機情報ネットワーク “セキュアスマートフォンアクセスサービス”
http://www.mind.co.jp/service/network/remote_access/smartphone.html

21) スマートフォンセキュリティフォーラム (仮称)」準備会発足およびメンバー募集のお知らせ
http://www.kddi.com/corporate/news_release/2011/0120a/index.html

セキュリティ対策が進んでいくことが見込まれる。

「スマートフォン利用におけるリスクと対応策」を表 2.3-1 に、「スマートフォン導入時に行うべき対策」を表 2.3-2 に示す。

表 2.3-1　スマートフォン利用におけるリスクと対応策（MCPC 資料[22] より抜粋）

	セキュリティ上の脅威	対策
本体・メモリ等	置き忘れ・盗難・紛失	ロック機構、各種認証システム、リモート消去、暗号化等
	落下・水没・不慮の故障	ストラップの利用、保険加入
OS・ソフトウェア	不正プログラムによるデータ破壊・漏えい	ウイルス対策、不正プログラム監視、バックアップ
	バグによるデータ破壊	信頼性の高いソフトウェアの利用、バックアップ
	OS の脆弱性をついた外部からの攻撃	OS 更新管理、迅速な更新、ファイアウォール
	スパムメール	対策サービスの活用
	有害サイトへのアクセス	フィルタの実施
端末内の情報資産	不正利用、データ破壊・漏えい	認証、ロック機構、データの暗号化
	権限外のアクセスによる情報漏えい	アクセス制限設定、グループポリシーの策定
	データ破壊	バックアップ
通信網	通話の傍受	利用場所等のルール策定
	データ傍受	VPN の利用
	セキュリティの弱い通信	弱い通信方式の利用を制限

表 2.3-2　スマートフォン導入時に行うべき対策（MCPC 資料 [22] より抜粋）

項目	効果
PIN の設定	SIM を抜かれ他人に回線を使われることを防ぐ
ロック、暗証番号の設定	不正使用、情報漏えいの防止
定期的なバックアップ	盗難・紛失時や故障時のデータ消失の回避
OS の更新	不正アクセス・ウイルス対策
メモリカード暗号化	盗難、紛失時の漏えい防止

[22] モバイルコンピューティング推進コンソーシアム，”2010 年スマートフォン導入構築ガイド” http://www.mcpc-jp.org/smartphone/SmartPhoneBuildGuide.pdf

2.3.2 スマートメータ

スマートメータとは、電力会社等の計量関係業務等に必要な双方向通信機能や遠隔開閉機能などを有したメータである。また、広義には上記に加え、エネルギー消費などの「見える化」やホームエネルギーマネジメント機能も有したものと定義される[23)]。米国や欧州を中心に導入が強く進められており、日本でも電力各社が実証実験に取り組むなど、普及しつつある。スマートメータを使用することで、利用料金の遠隔検針や遠隔遮断が可能になる。また、将来的には家電機器との連携などネットワークを通じた新しいサービスが提供される可能性がある。

ただし、電力使用量などのプライバシー情報がネットワークを介してやりとりされることとなり、セキュリティ上の問題が懸念される。また、スマートメータ導入により計測が正確になり、従来機器と計測方法が変わり、利用料金が大きく変動してしまうことや意図しない機器制御を受ける恐れなども普及への課題として考えられる。

米国においては、国立標準技術研究所（NIST: National Institute of Standards and Technology)から、スマートグリッドのサイバーセキュリティに関する戦略/アーキテクチャ/要件、プライバシーの問題、リスクアセスメントについて扱うガイドライン[24]が提供されている。同ガイドラインでは、特にスマートメータを含むシステムにおける双方向通信について、次のセキュリティ要件が求められている。(付録「今後求められる情報セキュリティ技術とビジネスの方向に関する調査報告書」P47 参照)。

(1) アクセス認証

スマートメータ等の機器が接続されるネットワークへの無関係な機器の無断接続を防止するため、機器をネットワークに接続する際に認証を行う。

(2) スマートメータと電力会社側サーバとの間の安全な通信

広域通信ネットワークを経由してスマートメータと電力会社側サーバの間で通信を行うため、暗号化等により盗聴や改ざんを防止する。

(3) 暗号鍵の管理

認証および暗号通信等に同じ暗号鍵を長期間使い続けることを避けるために、一定期間毎に鍵の動的な更新を行う。

今後スマートグリッドの普及に伴い、スマートメータのセキュリティ対策についても整備が進んでいくことが見込まれる。

---

23) 経済産業省スマートメーター制度検討会第一回資料, “スマートメーターをめぐる現状と課題について” http://www.meti.go.jp/committee/materials2/downloadfiles/g100526a04j.pdf

24) http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

第3章 重要な情報セキュリティ技術の展望

3.1 ID 管理

3.1.1 ID 管理技術の展望

第 2 章で示した通り、ID 管理技術は、Liberty Alliance や OASIS、OpenID Foundation など複数の団体が異なるアプローチで標準化・実用化を進めてきている。このうち、現時点において特に有望と考えられる SAML と OpenID について、今後の展望を述べる。

(1) SAML

SAML は古くからある最も有名な ID 連携仕様であり、近年のエンタープライズ向けクラウド・SaaS 環境との Web SSO 分野で適用事例が急速に拡大する可能性がある。

また、ID 連携プロトコル間の相互運用性を向上させる活動も活発化してきている。例えば、Kantara Initiative では相互運用性向上を目的に活動する Concordia Discussion Group が設立されたのをはじめ、SAML と OpenID との間で Web SSO を相互運用するために RSA Conference 2009 にて、相互変換デモンストレーションを実施している。さらに日本でも、総務省 ICT 先進事業国際展開プロジェクトのひとつである「認証基盤連携による認証基盤間の相互運用性確保の実証」でも OpenID と SAML の相互運用性について検討を行うなど、他の ID 連携プロトコルとの相互運用性の面でも SAML の利用は拡大していくことが期待される。

(2) OpenID

OpenID は、シンプルで軽量なトラスト・フレームワークを採用しており、近年のコンシューマ向けのクラウド・SaaS 環境との Web SSO 分野で適用事例が急速に拡大する可能性がある。

現在、OpenID Foundation の仕様策定 WG では OpenID 2.0 に続く次期仕様「OpenID Connect」の策定へ向けたディスカッションが行われており、暗号化・署名のための仕様の策定・参照が予定されている。本検討では、OAth2.0 が意識されており、乱立していた ID 連携・管理方式の相互接続性が高まることが予想される。

3.1.2 ID 管理技術の普及シナリオ

第 2 章で示した通り、ID 管理技術の適用例として、クラウド間連携や国民 ID 制度等があげられる。これらの適用例を普及シナリオととらえ、普及シナリオにおいて重要となる点を以下に述べる。

(1) クラウド間連携

近年、クラウドコンピューティングの利用、特に社内ネットワークとパブリッククラウドの併用や、ハイブリッドクラウドを活用するケースが増えてきている。このような場合における複数の事業者が管理する環境下では、ID 管理が必要不可欠な概念である。利便性と安全性を両立させつつ、低コストなシステムを実現させるために、ID 管理技術の相互接続性が重要となる。

また、多数のシステムとの連携及びクライアント端末の多様化を考慮すると、ID 管理技術を実現するシステムのスケーラビリティ向上が必要となる。

(2) 国民 ID

国民一人ひとりを特定する番号として、社会保障・税に関わる番号制度と、行政分野や民間分野の円滑な情報連携を行うための仕組みとなる国民 ID 制度のしくみが 2014 年度に構築・運用される予定である。複数の行政サービスを束ねる国民 ID 制度を安心・安全に実現させるために、プライバシー保護のためのトークナイゼーション等の技術の導入や第三者機関の適切な運営と親和性の高い ID 管理技術が重要となる。

3.1.3 ID 管理技術の普及に向けた課題

「3.1.1 ID 管理技術の展望」「3.1.2 ID 管理技術の普及シナリオ」に示した重要な点を課題のポイントとしてとらえ、ID 管理技術の普及に向けて必要となる事項を以下に述べる。

(1) クラウド時代の ID 管理技術の相互運用性の確保

「3.1.1 ID 管理技術の展望」でも述べた通り、ID 管理技術の相互運用性を高める動きが進んできている。

一方で、ID 連携技術のインタフェース統合や、多様なクライアント端末への対応までは時間がかかることが想定される。これらの差異を吸収するサービスの普及が望まれる。

(2) プライバシー保護を実現する仕組みの普及・促進

大規模な ID 管理の応用例である国民 ID の事例や、クレジットカードシステムの事例では、ID の流出によるプライバシー情報の流出が起きており、トークナイゼーション等を実現する技術の普及が望まれる。

一方でトークナイゼーションの仕組みが複雑化すると運用に支障をきたす可能性が高く、費用対効果の高い技術開発が望まれる。

(3) プライバシー保護のための第三者機関の設置

大規模な ID 管理サービスの発展や国民 ID 制度の実現に備え、これらのサービスや制度に対して、第三者機関による認証制度や、監査制度、事故対応・報告制度等を整備することによるプライバシー保護の実現が望まれる。

3.2 組込みセキュリティ

3.2.1 組込みセキュリティ技術の展望

本章では第2章で採り上げたスマートデバイスとスマートメータにおける組込みセキュリティ技術の展望について述べる。

スマートフォンは急速に普及が進みセキュリティの問題が報告される一方で、企業での利用も始まりセキュリティ対策についての検討も行われている。携帯電話と比較するとスマートフォンは従来から汎用的なOSが用いられ、さらにアプリケーションの開発環境もオープンになっている。iPhoneとAndroid端末は急に多くの開発者がアプリケーション開発を行うようになっており、この状況は今後も継続すると見られる。スマートフォンはカメラ、GPS、マイクなどのデバイスを持っており、これらのデバイスを利用したアプリケーションやネットワークを介してクラウドと連携するアプリケーションが今後も開発されるとみられる。

組込みセキュリティの観点では、

① 汎用OSを利用する際には、設定やセキュリティ対策などを利用者や提供者が適切に実施することが必要となる

② 多くの開発者がアプリを作成する傾向は、脆弱性が混入する危険性を低下させる方策が必要となる

③ 企業での利用においてはスマートフォンの持つ多様な機能に対しセキュリティポリシーに沿った新しいルールの整備が必要となる

スマートメータでも汎用OS化が進んでいる。また、製品の特性上比較的長期間利用されること、本格的な導入が始まると台数が非常に多くなること、コスト上の制約が大きいなどの特徴があり組込み機器特有の対応が必要となる。

組込みセキュリティの観点では

④ 汎用化を考慮したセキュリティ対策が必要となる

⑤ 遠隔からのセキュリティ状況の監視が必要となる

⑥ 安全なファームウェアの更新手段が必要となる

等である。

3.2.2 組込みセキュリティ技術の普及シナリオ

スマートフォンは重要な情報の蓄積やアクセスが増えるとともに直接ターゲットとしてセキュリティリスクが高まってきている。これらのセキュリティのリスクはパーソナルコンピュータやサーバでも同様に存在しすでに対策も常識となっている事がほとんどであるがスマートフォンの利用者も開発者も十分に理解していない。スマートフォンにもセキュ

リティリスクがあることを理解するように広報活動が必要である。

利便性やコスト、導入のしやすさなどから業務でのスマートデバイスの利用も増加が見込まれるが、アクセスできる情報資産の価値やセキュリティリスクを考慮した運用を行う必要がある。スマートデバイスに適したセキュリティ技術の確立（OS、プラットフォーム、アプリケーション開発環境等）とセキュリティ状況を監視して管理する技術、さらに導入する上でのルールを確立するためのガイドラインの普及を進める必要がある。

スマートメータは情報を利用者に提供し使用状況の見える化による省エネの促進などが期待されている。今後はホームエリアネットワークから直接スマートメータの情報を取得したり、さらには第三者による情報活用での付加サービスも期待されている。

また、電気メータだけでなくガスメータ、水道メータの情報活用も検討されており、通信プロトコルやデータフォーマットの標準化を図ることで部品の共通化によるコストダウンやさらなる効率化が期待できるが、コスト優先が脆弱性を生むこともあり、機器の認定制度などの検討が必要であろう。

3.2.3 組込みセキュリティ技術の普及に向けた課題

「3.2.1 組込みセキュリティ技術の展望」「3.2.2 組込みセキュリティ技術の普及シナリオ」に示した点を課題のポイントとしてとらえ、組込みセキュリティ技術の普及に向けて必要となる事項を以下にのべる。

スマートデバイスでは、OS や開発環境としてセキュア実装技術の一層の強化と、開発者のセキュリティ実装に関する知識・技術を底上げして、脆弱性の作りこみを抑制するなど、機器及びアプリケーションのセキュア設計、セキュア開発、セキュア運用技術の確立と維持が課題である。

また、利用者へのセキュリティリスクの周知と利用者が実施できるセキュリティ対策の提供が課題である。

企業利用では、企業が求めるレベルのセキュリティポリシーの見直しや新しいルール整備、多様なスマートデバイスの中から求めるセキュリティ対応が可能な端末を選択するための情報提供が課題である。

スマートメータでは、インフラの一部として提供されるため、メータは安心安全なものとする仕組みが必要である。そのためには長期にわたる機器利用期間を通じて、セキュアな機器をセキュアに運用できる技術を確立することが課題である。

また、確立された技術が正しく提供されていることを保証する認証制度も課題である。

ともに社会インフラを支える機器として利用者が安心安全に利用できるよう業界の取り組みや標準的なソリューションの確立、制度面の整備などが必要となる。

第4章 今後のセキュリティビジネスに向けた提言

4.1 ID管理

クラウドコンピューティングの利用、特に社内ネットワークとパブリッククラウドの併用やハイブリッドクラウドの利用など、複数の事業者が管理する環境下では、アイデンティティ管理は必要不可欠な概念であり、その重要度が非常に高まっている。

本章では、クラウドコンピューティングと国民IDの2つの潮流において重要な役割をになうID管理の視点から今後のセキュリティビジネスに向けた課題と提言を行う。

4.1.1 クラウドコンピューティングにおけるID管理の方向性

(1) クラウドベースのID管理サービスの普及を促進する要因[25)]

①すぐに導入効果が得られる

自社運用型ソフトウェアの場合、購入後、導入に時間がかかり、実際に利用できるようになるまでにはタイムラグがある。

②ユーザ数の大幅な増加による管理負担の軽減

企業ネットワークにアクセスする必要がある契約業者やパートナーなどが増えることで、ユーザ数が大幅増加する。

③システム管理者が本来業務へパワーシフト

社内の技術者が、サービスが解決するビジネス課題に注力せざるをえなくなる。

(2) ID管理システムモデルの方向性

企業におけるID管理の導入形態は3通り考えられる。

クラウド／SaaSを利用していない企業の40%近くが「セキュリティの不安」を挙げている状況と、ID管理サービス普及の促進を考慮すると、これからのID管理システム形態は、Bモデルが主流になると予想される。

重要な個人情報が格納されている人事システムは自社で管理し、IDaaSはその人事システムとクラウドサービスのGW的役割として、クラウドサービスを活用するために必要な情報だけを受け渡しを担う。

25) 米国Burton Groupの副社長兼リサーチ・ディレクター(Bob Blakley)「Burton Group Catalyst Conference」講演

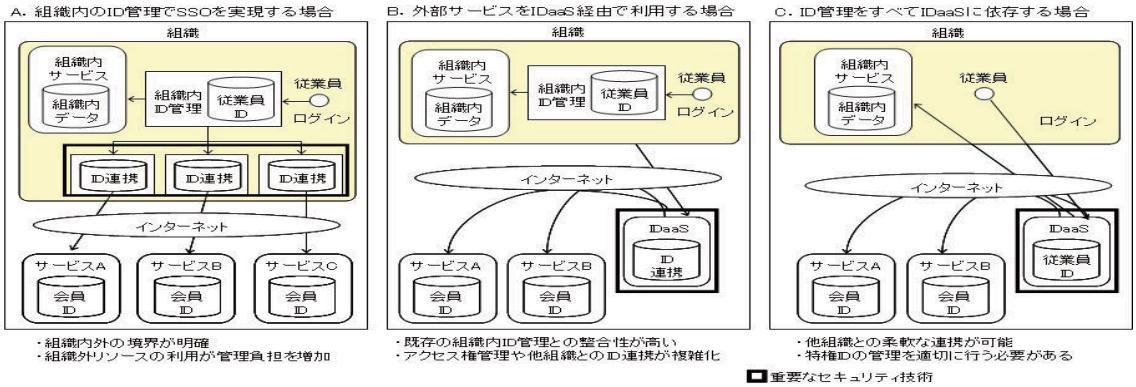


図 4.1-1　ID 管理のモデル

4.1.2 国民 ID 制度における ID 管理の方向性

(1) 国民 ID に内在するリスク

①国民 ID の悪用

本人確認に国民 ID を使用する場合、大量流出や盗用、犯罪への悪用が頻発する可能性がある。

②継続的な被害

国民 ID の変更が困難な場合、一度流出するといつまでも被害を止められない。

③プライバシー侵害

国民 ID が民間利用される場合、個人の情報のデータマッチングが容易になり、プライバシー侵害に繋がる可能性がある。

(2) ID 管理システムモデルの方向性

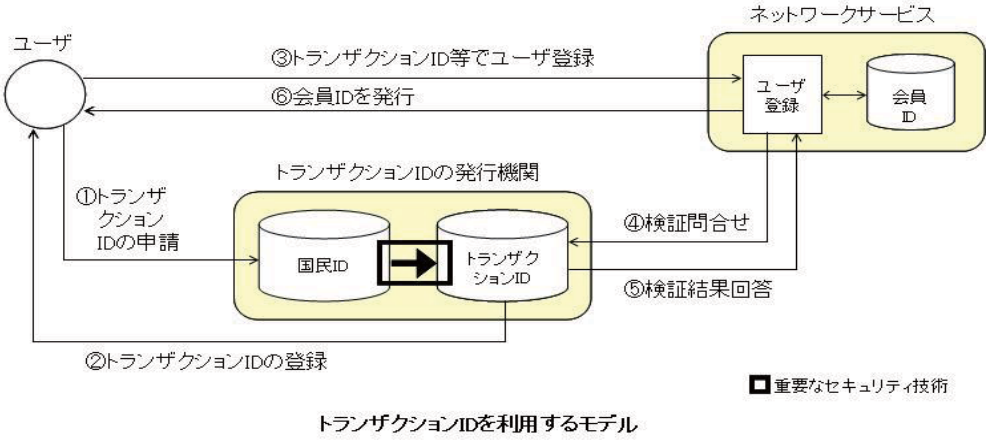


図 4.1-2　トランザクション ID を利用するモデル

ユーザは、必要に応じてトランザクション ID を申請し、発行されたトランザクション ID を使ってネットワーク上のサービスのユーザ登録を行う。サービス事業者はトラ

ンザクション ID の真正性について発行機関に問い合わせ、その結果をもとに、ユーザに会員 ID を発行する。
この場合、ユーザは、自身の国民 ID をサービス事業者に知られることなく、サービスの利用登録が可能になる。

4.1.3 今後のセキュリティビジネスの課題と提言

前述の通りクラウドコンピューティングと国民 ID の観点から ID 管理システムモデルの方向性を示した。ここでは ID 管理に対する意識が高まる中で、新たに認識すべき課題とその課題を解決するセキュリティビジネスへの提言を行う。(参考[27])

課題 1：大量の ID の漏えいに備えること

提言 1－①：ID 漏えい時の再付番に関する方針立案

- ID の取り扱い方針として、情報セキュリティの観点から ID が漏えいした際の ID の変更（再付番）方針について明確にしておく必要がある。

提言 1－②：マスターID とトランザクション ID の識別

- トランザクション ID は、事業体やサービスなどの複数のシステム間で頻繁にやり取りされることから、常に漏えいの脅威にさらされる性質の ID であるため、トランザクション ID としての ID が漏えいした際に容易に再付番が行える仕組み／サービスが必要となる。

提言 1－③：トークナイゼーションを活用したトランザクション ID の生成

- 元の ID の数学的な関連性がない別の数列等に置き換える技術を使用してマスターID からトランザクション ID としてのトークンを生成する仕組み／サービスが必要となる。

課題 2：プライバシー保護の仕組みを構築すること

提言 2－①：プライバシー保護のための第三者機関の設置

- 許可されないデータマッチングを防止するために、トークナイゼーションされた ID を元のマスターID に戻すためのパスワードを第三者機関が管理する仕組み／サービスが必要となる。

提言 2－②：ID 以外のデータマッチングへの対処

[27] 国民 ID とシステムとしての課題－プライバシーの保護と利便性の両立を目指して
http://www.horibemasao.org/symposium03.html

・ ID 以外のデータマッチングキーとして、氏名、性別、生年月日、住所、電話番号（携帯電話番号）、メールアドレス等が考えられる。例えば、行政サービスを念頭に置いた場合、メールアドレスの登録は不可欠であり、メールアドレスによるデータマッチングを防止するためには、行政サービス毎に異なるメールアドレスを登録する等、対処が必要となる。

課題 3：変遷する情報セキュリティの脅威への対処

提言 3－①：継続的な事件・事故事例ならびに技術動向の調査

・ 変遷する情報セキュリティの脅威に対処し続けるためには、米国をはじめとする ID 利用の先進国における犯罪事例を収集し、分析することで常に情報セキュリティの脅威を把握する仕組み／サービスが必要になる。

提言 3－②：最新動向を踏まえたセキュリティ対策の適用と多様性の確保

・ 最新の脅威を把握したうえで、その脅威に対抗するための技術的対策を常に最新のものとして維持する仕組みが必要となる。何重にも対策を張り巡らせる多層防御の考え方と多様な対策技術の採用が重要となる。

4.2 組込みセキュリティ

組込み機器は、スマートデバイス、スマートメータのような機器を始め、多種多様な機器が存在し、これらがネットワークに接続されてビジネスや生活に利便性を提供し始めている。そして今後も組込み機器は高機能化・多機能化の方向で進化していき、社会基盤として組み込まれてくることが予測される。さらに、情報サービスの拡大に伴い、個人情報やプライバシー情報などの組込み機器で取り扱う情報の価値も向上している。このため、組込み機器でもパーソナルコンピュータなどと同様に攻撃の対象になる可能性が非常に高いといえる。組込み機器のセキュリティ対策「組込みセキュリティ」が今後重要になってくることは前章までで述べてきた。最近ではスマートデバイスでのウイルスの発見や、情報漏えいに関する脆弱性が発見されるなどの報道がされるようになってきており、組込み機器のセキュリティ対策は待ったなしの状況になってきた。

4.2.1 組込みセキュリティの C.I.A

組込み機器においても、少なくとも情報セキュリティの三大基本概念 C.I.A「機密性(Confidentiality)」、「完全性(Integrity)」、「可用性(Availability)」に基づいた対策を実施することが求められる。組込み機器の場合には表 4.2-1 のような意味合いになる。

表 4.2-1　組込み機器の情報セキュリティの三大基本概念「組込み機器の C.I.A」

基本概念	組込み機器における意味（組込み機器の C.I.A）
機密性(Confidentiality)	承認されていない主体に、機器の内部に保管されている秘密情報やファームウェアが外部に開示されないこと
完全性(Integrity)	機器の保管時、輸送中、設置時、動作時に、機器のソフトウェアや設定値、ハードウェア構成などが改ざんされていないこと
可用性(Availability)	組込み機器とそれを利用したシステムが期待通りに稼働し、許可された正規利用者がサービスを常に利用できること

組込み機器の C.I.A を確保するために利用されるセキュリティ技術は、基本的にはパーソナルコンピュータ（PC）やスマートカード等と同等な技術を搭載すれば良いといえる。ソフトウェアに必要な基本技術はすでに PC で実用化されており、要件を満たすように実装すれば良い段階にきている。そして、組込み機器は人目にさらされない箇所で利用されることや不特定多数の利用者に使われることも多いので、スマートカードやそれら利用機

器に搭載されている耐タンパ機能が必要である。耐タンパ機能は、非正規な手段による機密データの読取りを防ぐ機能であり、ソフトウェアやハードウェアに容易に外部から解析できないような防護策を講じるものである。これには、外部から読み取りにくいよう機密性を高める方法と、外部から読み取ろうとするとプログラムやデータが破壊されてしまう機構を設ける方法の二通りの方法がある。また、組込み機器は PC と異なり製品のライフサイクルが長期にわたることが多いので、製品のライフサイクル全体にわたってのセキュリティ管理が必要である。セキュリティ管理にはファームウェアや暗号鍵、設定情報などが含まれる。そして、暗号鍵が弱くなったり危殆化するなどの暗号鍵の状態を検知することも必要となってくる。

一般的に組込み機器は PC よりも安価であることが期待されており、コスト面で制約が多い。従って、組込み機器の守るべき情報の資産価値とコストバランスを考えて搭載するセキュリティ技術を選定する。もちろん実装するセキュリティ技術もコストが低いことも重要である。しかし、コストバランスを考える場合には製品に実装するセキュリティ技術だけでなく、セキュリティ機能維持のための保守管理コストと、インシデント発生時の対応費用を考慮して検討することが必要である。

4.2.2 組込みセキュリティ機能の維持管理

組込み機器のセキュリティは、市場への出荷前に適切なセキュリティ対策が施されているだけでなく、出荷後に発覚した新たなセキュリティ脅威や脆弱性にも対応でき、製品のセキュリティ機能が維持されるようにすることが重要である。また、組込み機器の開発、設置､運用､廃棄の各ステップにおいてセキュリティが確保されるようにする必要がある。つまり、組込み機器の製品としてのライフサイクル全体にわたってセキュリティも管理されなければならない。セキュリティ管理のためには、現在のセキュリティ状態を監視する必要がある。そして監視結果に基づいて、セキュリティ機能の保守を実施するのである。利用者は、使用している組込み機器が安全か否かが一目で判断できるようになっていれば安心して情報サービスが利用できるので、セキュリティ状態の見える化も必要である。昨今では、デジタル複合機やデジタルサイネージなどの組込み機器は、レンタルやリースなどで利用されることも多い。また中古などが利用されることもある。これらの場合、使用した情報や設定を安全に消去すると共に、次の利用者が簡単に利用できるようにしなければならない。このような時、セキュリティ状態の見える化が有効になる。そして、レンタルやリースにおいて機器が安全に利用できるようになっているのかを管理することが重要である。

組込みセキュリティで難しい点は、PC などと違って組込み機器はハードウェアやソフトウェアのリソースが乏しいことが多く、セキュリティ機能をどのように監視し状態を通

知するかである。そして、セキュリティ機能の保守をする環境として、どのようなものを利用するかということである。さらに、組込み機器自身の故障によるセキュリティ破壊に備えた重要情報の安全な保管をどのように施すのかも考えなければならない。

最近ではスマートデバイスなどの組込み機器では、機器ベンダが提供するアプリケーションだけでなく、利用者や第三者が作成したアプリケーションを導入することもある。これらのアプリケーションを利用した場合においてもセキュリティが確保される必要がある。このためには、セキュアなアプリケーションを開発するための手法が必要になってくる。

4.2.3 組込みセキュリティ分野におけるビジネス展開

前節までで組込みセキュリティで必要なことは、低コスト・セキュリティ技術の実装、組込み機器の製品ライフサイクルにわたるセキュリティ機能の維持管理、安全なアプリケーションの開発手法の提供、そして組込み機器のセキュリティ評価制度の活用であることがわかった。組込みセキュリティでは、組込み機器の C.I.A を維持することの他に、新たなセキュリティ脅威への対処や、機器故障時などの緊急時にも重要な情報が消失しないようにする技術も可用性の面から必要である。また、組込み機器は PC などと比べて利用できるリソースも少ないので、セキュリティ管理を容易に実現できるデバイスの開発も必要である。そして、これらがビジネスとして形成できると考える。

これまで述べてきた通り、組込みセキュリティ分野では次のような技術やサービスの開発と運用の提供が製品のライフサイクル全体にわたって必要であり、ビジネスとしての展開も有望と考えられる。

①低コストで組込み機器に適したセキュリティデバイスの開発
②セキュリティ状態の見える化とセキュリティ機能の維持管理
③組込み機器の故障対応のための重要データの安全なバックアップとリカバリ
④安全なアプリケーションの開発をサポートする開発環境の提供
⑤機器の廃却やレンタル／リース時のセキュリティ管理
⑥組込み機器向けセキュリティ機能の標準化とセキュリティ評価認証

組込み機器は世界各国で利用される可能性が高いので、前述のような技術やサービスはグローバルに展開できるクラウド環境下で利用できることが望ましい。また、組込み機器は人手が入らないような箇所で利用させることもあるので、極力自動化させることが必要である。

おわりに

本年度の調査にて、今後求められる情報セキュリティ技術とビジネスの方向性として、複数の ICT 領域で重要な役割を果たすセキュリティ技術は「ID 管理」と「組込みセキュリティ」との結論に達した。今クラウドコンピューティング環境下では、様々な組込み機器が接続され、ID も様々な用途で利用されていく。ここで必要なキーワードは安全な管理と運用である。「ID 管理」では、ID 管理技術の相互運用性の確保とプライバシー保護と、プライバシー保護のための第三者機関の設置が今後のビジネスにつながると考えられる。「組込みセキュリティ」では組込み機器のセキュリティ機能を監視し安全に保守するビジネスの他、組込み機器のセキュリティを確保するための標準技術の提供と評価認証がビジネスとして展開できると考える。これらのビジネス形成により、JEITA 会員企業のみならず多くの企業において、より安全・安心な情報インフラが提供され社会基盤の構築につながるとともに、情報セキュリティ産業が発展していくことを期待する。

今後求められる情報セキュリティ技術と
ビジネスの方向に関する調査報告書

平成２３年３月

株式会社三菱総合研究所

今後求められる情報セキュリティ技術とビジネスの方向に関する調査報告書

2011年3月31日

株式会社三菱総合研究所
情報技術研究センター　クラウドセキュリティグループ

目次

序章. 調査の概要
０．１　調査目的　2
０．２　調査フロー　3

第1章　情報セキュリティ技術が不可欠なICT有望領域　4
１．１　クラウド・コンピューティング　5
１．２　スマートグリッド　8
１．３　デジタルサイネージ　10
１．４　スマートデバイス　11
１．５　LBS（Location-Based Services）　14
１．６　国民ID　15
１．７　PCIDSS　19

第2章　有望領域における情報セキュリティ技術の関連動向　21
２．１　有望なICT領域と重要となる情報セキュリティ技術の関係　22
２．２　ID管理　23
２．３　組込みセキュリティ　37

第3章　重要な情報セキュリティ技術の展望　51
３．１　重要な情報セキュリティ技術の展望　52
１）ID管理　52
２）組込みセキュリティ　62
３．２　まとめ　70

（参考）
参考1　韓国訪問調査　72
参考2　「サイバー空間における信頼可能なアイデンティティのための国家戦略（案）」　86

0．1 調査目的

■ 調査の背景

- 急速な発展を遂げた情報システムとネットワークは、今や重要な社会基盤として、国民の経済活動や生活を支えている。その一方、そうしたIT環境の発展と普及を背景に、情報や情報インフラに対する脅威も刻々と変化しており、それに対応する情報セキュリティ技術も発展してきた。
- ただし、情報セキュリティビジネスは依然として米国企業が主導しており、日本のセキュリティ事業者が技術開発で先行するテーマは限定的な領域にとどまっているのが現状である。
- したがって、我が国IT関連企業においては、今後重要となる情報セキュリティ技術に着目し、そのビジネス展開の可能性を踏まえ、事業戦略を検討することが望まれる。

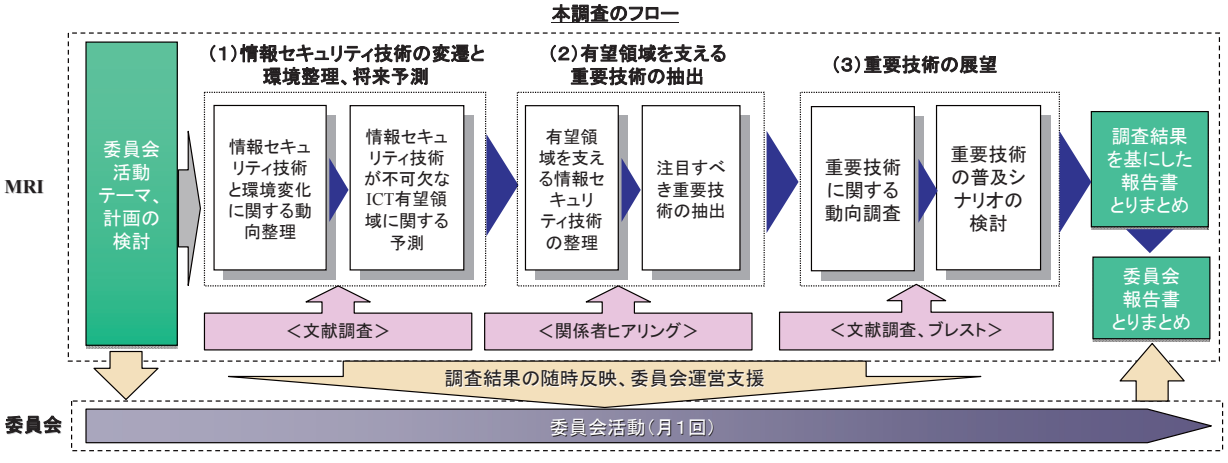
■ 調査の目的

- 本調査は、これまでの情報セキュリティ技術の動向とビジネス環境や社会制度の変化との関連を整理した上で、情報セキュリティに関する今後の技術開発やビジネス展開の方向について検討することにより、JEITA企業の事業戦略策定に寄与することを目的とする。
- 具体的には、以下の項目を明らかにすることを目指す。
  - 有望な情報セキュリティ技術の領域
  - 注目すべき重要技術
  - 重要技術に関する戦略・方針

0．2 調査フロー

■ 調査フローは以下の通りとする。

（1）情報セキュリティ技術と環境変化に関する動向を整理し、その結果を基に、今後情報セキュリティが重要となるICT分野の有望領域の方向について予測する。
（2）次に、有望な領域において重要となる情報セキュリティ技術の構成や役割に係る分析を行う。また、その中から、特に今後注目すべきと考えられる重要技術を抽出する。
（3）抽出した重要技術の利用環境において今後考えられる変化を予想するとともに、それを踏まえた重要技術の普及シナリオについて検討する。
（4）以上の調査結果を基に、報告書のとりまとめを行う。



注：本調査フローや調査内容については、委員会と協議の上、実現可能性を踏まえた調整が可能である。

第1章　ICTと情報セキュリティ技術の動向

1．1　クラウド・コンピューティング　①概要

- **概要：** 企業や個人が従来保有していたハードウェアやソフトウェア等のIT資産を、インターネット経由でコンピュータ処理をサービスとして利用する形態。インターネット経由の一般向けサービスを「パブリッククラウド」、業界内・企業内等のサービスを「プライベートクラウド」、両者を組み合わせたサービスを「ハイブリッドクラウド」と呼ぶ。また、提供サービスのレイヤによって、SaaS（ソフトウェア）、PaaS（アプリケーション実行用プラットフォーム）、IaaS（ハードウェアやインフラ）等と分類される。
- **市場規模：** パブリッククラウド範囲における2009年の日本国内クラウドサービス市場の規模は312億円。2014年の市場規模の予測は1432億円である[1]。国内ITベンダからは、企業固有のシステムのプライベートクラウド化のような高付加価値サービスが提供されており、今後これらの利用も増えると予測されている[2]。
- **影響範囲（社会基盤としての重要性）：** クラウドはサービスの効率化や価値創造のニーズを満たす新しいインフラである。多くのベンダにおいて既にサービス事業が行われている。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- クラウドによりネットワークを利用したサービス提供を実現するためにはセキュリティ確保は不可欠のものである。

脅威像・課題：
- クラウド関連のリスクは様々な機関における分析がなされているが、特に指摘されているのは、データの機密性確保、クラウド基盤に対するサイバー攻撃、共同利用者/クラウド事業者の不正行為、クラウドサービス自体の脆弱性、サーバの設置場所による異なる司法管轄への対応、クラウド事業者のセキュリティ体制等である。
- クラウドにおける脅威の例を以下に挙げる。[3]
  - クラウドコンピューティングの不正濫用、セキュアでないAPI、内部犯、共用技術の脆弱性、データ紛失/漏洩、アカウント/サービス/トラフィックの乗っ取り、未知のリスクプロファイル

技術的な解決策

左に示した課題については次の技術的解決策が挙げられている[4]。
- アプリケーションセキュリティ：開発ライフサイクルに沿ったセキュリティ実現、ヴァーチャルマシンの要塞化、ホスト間通信のセキュア化、ログおよびデバグ情報の管理 等
- 鍵管理：クラウド提供者と利用者を考慮した鍵管理の実現 等
- アイデンティティおよびアクセス管理：プロヴィジョニング技術、認証技術（SaaS、PaaSでのGoogle、OpenID等の認証の利用、IaaSでのVPN技術、SAML、SSL、OpenID等の利用）フェデレーション技術（SAML、WS-Federation等）、アクセス制御 等
- 仮想化：VM内およびハイパーバイザーのセキュリティコントロールの理解。各VMの分離（孤立化）の徹底と確認 等

[1]：IDC Japan プレスリリース http://www.idcjapan.co.jp/Press/Current/20100412Apr.html
[2]：矢野経済研究所, “クラウドコンピューティング市場に関する調査結果2009”, http://www.yano.co.jp/press/press.php/569
[3]：Cloud Security Alliance “Top Threats to Cloud Computing V1.0” http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[4]：Cloud Security Alliance “Security Guidance for Critical Areas of Focus in Cloud Computing V2.16” http://www.cloudsecurityalliance.org/csaguide.pdf

1．1 クラウド･コンピューティング ②情報セキュリティ上の脅威

- クラウド･コンピューティングに対する脅威については、米Cloud Security Allianceが2010年3月に「Top Threats to Cloud Computing V1.0」で7つの重大な脅威を挙げている。[1]
  1. クラウド･コンピューティングの不正な濫用（Abuse and Nefarious Use of Cloud Computing）
  2. セキュアでないAPI（Insecure Application Programming Interfaces）
  3. 内部犯（Malicious Insiders）
  4. 共用技術（Shared Technology Vulnerabilities）
  5. データの紛失/漏洩（Data Loss/Leakage）
  6. アカウント、サービスおよびトラフィックの乗っ取り（Account, Service & Traffic Hijacking）
  7. 未知のリスクプロファイル（Unknown Risk Profile）

- クラウドを悪用した攻撃についても、いくつかの事例が報告されている。クラウドは従来攻撃者が利用していたホスティングサービスよりも低コストであるため悪用されると考えられている。
  - クラウド利用による解読コスト低減 [2]
    - 安価でパワフルな演算能力を得られるため、パスワードクラッキングや暗号鍵の総当りによる解読に必要な時間とコストを短縮できる。
  - クラウドをボットネットの代用とする攻撃手法 [3][4]
    - 日本国内に向けられたAmazon Web Service（Amazon EC2サービス）を発信元とする攻撃は、2009年には2008年の4倍以上（200件）という伸びを示していた。具体的な攻撃手法はSQLインジェクションなどのウェブサーバを狙った攻撃やSSHサーバへのブルートフォース攻撃であった。
    - AWSを発信元とするスパムメールも増加傾向にあり、スパムブラックリストの中にはamazonaws.com（Amazon EC2サービスのドメイン）をリストに加えているものもある。
  - クラウドを利用したボットネットの統制 [5]
    - ボットネットを構成するマルウェアの解析から、ボットに指示を出す司令塔機能を果たす不正なプログラムがAWS内のコンピュータに配置されていたことが判明した。EC2内にこのプログラムを設置するに至った侵入経路は判っていない。
    - Google App EngineをC&Cサーバとして悪用するボットネットを発見したという同様の事例も報告されている。

<参考>
[1] CSA “Top Threats to Cloud Computing V1.0” http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[2] クラウドを悪用した攻撃の実態 大量処理能力を悪用 http://itpro.nikkeibp.co.jp/article/COLUMN/20100412/346976/
[3] ラック，2009年のセキュリティ状況「クラウドを巡る攻防」を総括 http://gihyo.jp/news/report/2009/12/1001
[4] セキュリティにクラウドの闇、Amazon EC2悪用の総当たり攻撃もhttp://internet.watch.impress.co.jp/docs/news/20091208_334134.html
[5] AWS Security Center http://aws.amazon.com/security/

1．1 クラウド･コンピューティング ③情報セキュリティ上の課題

- クラウドのセキュリティ課題 [1]
  1. クラウドコンピューティングのアーキテクチャ
  2. 統制とリスク管理（プロバイダのリスク管理体制）
  3. 法務･契約関係（プロバイダー利用者の法環境の差、契約上の留意事項）と電子的証拠開示
  4. コンプライアンスと監査（適用リスク管理基準と範囲、評価、監査）
  5. 情報のライフサイクル管理
  6. 移植性と相互運用性

  クラウドの統制に関するセキュリティ課題

  7. 通常のセキュリティ（=IDCセキュリティ）、事業継続、災害復旧
  8. データセンターの運用（データ･プロセスの分離、パッチポリシー）
  9. インシデントレスポンス、通知、回復
  10. アプリケーションセキュリティ
  11. 暗号化と鍵管理
  12. アイデンティティ･アクセス管理
  13. 仮想化（仮想化環境単位のセキュリティ装備、相互の隔離）

  クラウドの運用に関するセキュリティ課題

- 既にセキュリティ課題（ニーズ）が明確であり、情報セキュリティ技術開発が今後進展しうる。

- クラウドのセキュリティに関する内外の検討の動き
  - Cloud Security Alliance（ガイダンス文書、評価手法開発、クラウドCERT）、NIST（調達要件）、ENISA（報告書）
    IEEE（標準化）
  - 総務省（ガイドライン、研究会、霞ヶ関クラウド･自治体クラウド）、経済産業省（ガイドライン、研究会、研究開発）

<参考>
[1] Cloud Security Alliance “Security Guidance for Critical Areas of Focus in Cloud Computing V2.16” http://www.cloudsecurityalliance.org/csaguide.pdf

1．2 スマートグリッド ①概要

- **概要：** 地域の電力供給網と国家インフラを接続し、家庭や地域におけるエネルギー利用の高効率化を図る電力網。電力網の信頼性向上、情報通信機能の強化、電力網における用途の多様化への対応（太陽光発電等の再生可能エネルギーと電力系統との連係等）を考慮した送電網や蓄電システムが求められる。[1][2]
- **市場規模：** 2010年の世界のスマートグリッド市場について、2009年比で約6倍の5兆8170億円になると予測されている。[3]スマートグリッドにおける基幹機器であるパワーネットワーク関連機器の市場規模は2009年は約7056億円、2014年予測は1兆700億円と予測されている。[4]
- **影響範囲（社会基盤としての重要性）：** 社会インフラである電力の供給に係る技術であり、混乱が生じると影響は広い範囲に及ぶ可能性がある。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- 重要インフラとしての信頼性を確保しつつICT技術を活用するためには、本来機能を阻害せず、かつ十分な安全性が確保できるように、適切なセキュリティ技術を用いる必要がある。

脅威像・課題：
- 電力インフラに用いられる技術には、不正な操作が可能な脆弱なプロトコル、バッファオーバーフロー等の脆弱性等があり、それらの悪用によりスマートグリッドプラットフォームは攻撃を受けうる。ゼロデイ脆弱性を悪用した不正プログラムによるWindowsマシン上の電力制御監視アプリケーションへの攻撃の事例も既に報告されている。[5]
- ネットワーク接続されたスマートメータから個々の利用者の電気使用量が判ること等から、利用者のプライバシーを侵害する恐れが指摘されている。[5]

技術的な解決策

- 電力関連の制御システム・スマートメータにおける侵入対策等の基本的セキュリティ対策の推進
- 電力制御システム・スマートメータ関連製品（アプリケーションソフトウェア、OS、組込み機器、ミドルウェア等）の脆弱性対策の推進
- プライバシー情報に配慮したデータ管理手法（収集・集計手法）の実現

[1]：“米国におけるスマートグリッド構想の動向”，http://e-public.nttdata.co.jp/f/repo/685_u1003/u1003.aspx
[2]：“いよいよ動き出す「日本版スマートグリッド」”，http://techon.nikkeibp.co.jp/article/TOPCOL/20090707/172655/
[3]：「2010 ワールドワイド スマートグリッド構築実態調査」（富士経済、2010年9月），http://journal.mycom.co.jp/news/2010/09/22/031/index.html
[4]：富士経済プレスリリース，“パワーネットワーク（電力・ガス供給網）関連機器市場を調査”，http://www.group.fuji-keizai.co.jp/press/pdf/100414_10034.pdf
[5]：NYTimes.com, “New Virus Targets Industrial Secrets”, http://www.nytimes.com/external/idg/2010/07/17/17idg-new-virus-targets-industrial-secrets-61976.html
[6]：“プライバシーを侵害する電気メーター”，http://www.swissinfo.ch/jpn/detail/index.html?cid=8727280

1．2 スマートグリッド ②情報セキュリティ上の脅威

- 米国におけるスマートグリッド [1]
  - 電力網の信頼性向上、情報通信機能の強化
  - 電力網における用途の多様化への対応
    - プラグイン・ハイブリッド車や電気自動車の充電管理、家電機器の運転制御、再生可能エネルギーを電力系統に接続する際の制御、送配電網を利用した各種サービス等
- 日本におけるスマートグリッド [2]
  - 太陽光発電が大量に導入されることを考慮し、これらの発電量が不定なエネルギーと一定量の電力供給を担う既存のメイン電源について統合的な制御を行うような、送電網や蓄電システム。
  - 家庭や地域におけるエネルギー利用の高効率化。
- 電力インフラにおけるセキュリティ上の脆弱性
  - 米国の電力インフラに使用されている技術には、不正な操作が可能なプロトコル、バッファオーバーフロー脆弱性、ルートキットや不正コードへの感染等のセキュリティ上の脆弱性があり、それらの悪用によってスマートグリッドプラットフォームに対する攻撃が可能であると報告されている。[3]
- スマートグリッドに求められるセキュリティ
  - 米国においては情報セキュリティを考慮した通信仕様に関する議論が進められており、NIST（National Institute of Standards and Technology、米国立標準技術研究所）によりセキュリティに関する要求仕様を含む文書「Smart Grid Cyber Security Strategy and Requirements」がまとめられている（2010年2月時点ではドラフト段階）。
  - この文書の中では、セキュリティ要件だけでなく、電力分野におけるサイバーセキュリティ戦略、スマートグリッドにおけるプライバシーに関する考慮、スマートグリッドにおけるサイバーセキュリティに関する研究開発テーマ等についても言及されている。[4]
- スマートグリッドにおけるプライバシー課題
  - ネットワーク接続されたスマートメータの各家庭への導入が計画されている。これにより各家庭の電気使用量の変化を随時詳細に把握可能になる（例えば伝達されるデータから留守の時間や就寝時間などを割り出せる）。
  - そこでスマートメータおよびそのデータについては個々の利用者のプライバシー情報の情報源とみなす配慮が求められる。
  - スイス・チューリッヒ州ではスマートメータの情報保護面での安全性のチェックを州の情報保護委員会に依頼している。[5]

＜参考＞
[1] 米国におけるスマートグリッド構想の動向 http://e-public.nttdata.co.jp/f/repo/685_u1003/u1003.aspx
[2] いよいよ動き出す「日本版スマートグリッド」 http://techon.nikkeibp.co.jp/article/TOPCOL/20090707/172655/
[3] 米IOActive社：IOACTIVE VERIFIES CRITICAL FLAWS IN NEXT GENERATION ENERGY INFRASTRUCTURE（ニュースリリース） http://www.ioactive.com/news-events/AMIAlertPR.html
[4] DRAFT NISTIR 7628 "Smart Grid Cyber Security Strategy and Requirements" http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf
[5] プライバシーを侵害する電気メーター http://www.swissinfo.ch/jpn/detail/index.html?cid=8727280

1．3 デジタルサイネージ ①概要

- **概要：** デジタル通信によって配信された映像や情報をディスプレイやプロジェクターでデジタル表示する媒体。ここではデジタルフォトフレームを利用した簡便なものから大型ディスプレイまで幅広く、店舗や社内等に設置されるものを含めて考える。現在は、流通・交通分野を中心に導入事例が多数ある。ハードウェア・ソフトウェアは共に途上段階にあり、規模もさまざまである。コンテンツのライフサイクルは従来の広告に比べ比較的短い。将来は、ハイヴィジョン化、インタラクティブな情報提供、位置情報の併用、携帯電話等との連携、配信の効率化、相互接続（システムの標準化、広告の交換）、ディスプレイのアンビエント化などが予想されている。
- **市場規模：** 2009年は602.7億円。2015年には1260億円以上まで拡大すると予測されている [1]。別の調査では2009年度は557.1億円。2015年度には1300億円に迫ると予測されている [2]。
- **影響範囲（社会基盤としての重要性）：** 広告・販売促進、情報提供サービスを中心に広く普及している。大規模なシステムは流通等を中心に普及し今後はコンテンツの提供手法を関心の中心に移していくものと思われる。より小規模なシステムは位置情報、AR（Augmented Reality: 拡張現実感）技術等のIT技術と複合的に活用され新たなサービスを提供する可能性がある。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- 安定した配信を行うためには、妨害・改ざん等を受けない性質が必要となる。また高い信頼性のサービスを提供する必要がある。

脅威像・課題：
- 常時接続するネットワークからの脅威（端末にはPCが多数用いられる。端末として組込みシステムが用いられることもありうる）
- コンテンツ配信サービスを疎外する

技術的な解決策

- コンテンツ・サーバのセキュリティ対策
- PCセキュリティ対策（均質な機器が多数並列に接続されるシステムが対象）
- 組込みシステムのセキュリティ対策

[1]: 富士キメラ総研調査 https://www.fcr.co.jp/report/093q12.htm
[2]: 矢野経済研究所調査 http://www.yanoict.com/yzreport/115#a2

1．4 スマートデバイス ①概要

- **概要：** スマートフォン、スマートブック（ネットブックPCよりも小型な製品。モバイルインターネット端末とも呼ばれる）、電子書籍を読むための端末などを含む。携帯電話の携帯性とPCの持つ高機能性・多機能性を兼ね備えるデバイスと位置づけられる。多くはカメラ、GPS、無線LAN機能、RFIDリーダといった機能を組込みハードウェアとして備えてもいるため、これらを活用した業務等への利用も可能となる。
- **市場規模：** スマートフォンの2009年国内市場の出荷台数は194.5万台、2013年には571万台となる予測が示されている[1]。電子書籍は2008年度で464億円の市場規模 [2]。
- **影響範囲（社会基盤としての重要性）：** 現時点では個人が購入しプライベートで用いている比率が高いが、購入者の8割が業務用途での利用により効率が向上すると考えており、今後、企業への導入事例が増加する傾向にあると推測される[3]。スケジュール管理、文書の閲覧・編集等を外出先等で行うために用いられるが、特に営業、受発注等の業務支援に活用する事例も増えつつある。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）
- スマートデバイスを持ち出した先で社内データにアクセスすることにより情報漏えいリスクが高まる。このため情報セキュリティ上の対策は不可欠となる。
- 近年のスマートデバイスの利用者増を受けてPCと同様にウイルス等の脅威がスマートデバイスを対象とする場合も増えている。
- 携帯電話に比べると、汎用OSが実装されているスマートデバイスのセキュリティ対策は利用者に任される面も多い。

脅威像・課題
- 端末の放置・紛失・盗難 → 不正使用、データ漏洩・破壊
- ウイルス感染・不正アクセス
- セキュリティの弱い通信網からの侵入

技術的な解決策

- パスワード/指紋等による認証
- 端末ロック機能、リモートからのデータ消去機能
- 暗号化によるデータ保護
- アンチウイルス、ファイアウォール、ウェブフィルタリング

- 利用者向け管理方策としては、セキュリティベンチマークにおいてスマートデバイスを対象とする具体的項目の整備が行われている例がある。[4]

[1]: 矢野経済研究所, “スマートフォン市場に関する調査結果 2010”, h ttp://www.yano.co.jp/press/pdf/605.pdf
[2]: インプレスR&D インターネットメディア総合研究所, “電子書籍ビジネス調査報告書2009”, h ttp://r.impressrd.jp/iil/ebook2009
[3]: モバイルコンピューティング推進コンソーシアム, “2010年スマートフォン導入構築ガイド 第2版, http://www.mcpc-jp.org/smartphone/SmartPhoneBuildGuide.pdf
[4]: The Center for Internet Security, “Security Configuration Benchmark For Apple iPhone OS 3.1.2 Version 1.1.0 October 30th, 2009 ”

1．4 スマートデバイス ②情報セキュリティ上の脅威

従来の紛失・盗難などによる情報漏洩やなりすまし対策だけでなく、端末に保存されたユーザー情報をネットワーク越しに狙う脅威への対策が必要となりつつある。また、企業・組織での利用増を考慮すると、スマートフォンを踏み台とする内部NWを狙う攻撃にも警戒が必要だろう。

スマートフォンを狙うマルウェアの例

名称：トレッドダイヤル(TredDial) [1][2]
- 対象：Windows Mobile 搭載のスマートフォン
- 特徴：ゲームと動画関連プログラムをスマートフォンにダウンロードする過程で感染し、許可なく国際電話をかけ利用料金を請求する。162万人の通話明細を確認し、155件のドミニカ共和国、ソマリア等への発信の被害例が発見された。韓国ではアプリケーション・ストアを通じたウイルス感染を防ぐために、ストアで事前チェックを行うプログラムの開発を検討を開始している。
- 時期：2010年4月

名称：「Yxes.A!」（別名Sexy View） [3]
- 対象：SymbianOS S60 3rd Edition搭載の携帯電話
- 特徴：Symbianの署名が入った証明書を用いて正規アプリケーションとしてインストールされアクセス権限を取得する。感染した端末内の電話番号を収集してSMSを送り、URLをクリックすると不正なサーバからダウンロードされさらに感染する。端末シリアル番号等を収集する機能や、さらに新しい機能を不正サーバから取得する能力を持つ.
- 時期：2009年2月

スマートフォンのセキュリティ対策のポイント

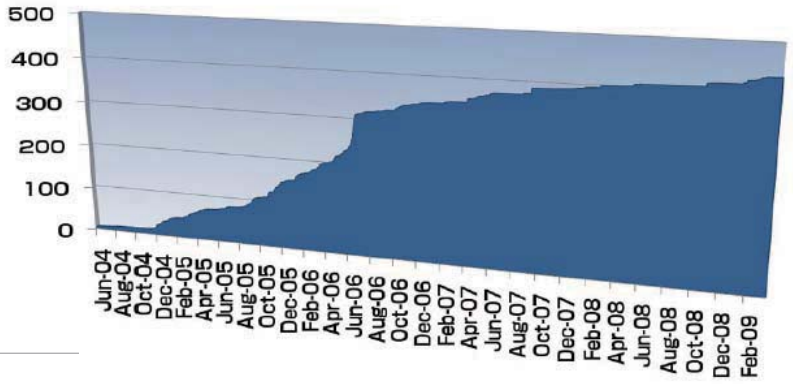
- アンラボ社が推奨するスマートフォンセキュリティ対策のポイント [1]
  1. アプリケーションをインストールしたり、怪しいファイルをダウンロードした場合には、必ず悪性コードスキャンを実行
  2. ゲームなどのアプリケーションをダウンロードした時は、他のユーザーのロコミ情報などを慎重に確認する
  3. ブラウザやアプリケーションでインターネットに接続した際、メールやSMSに表示されている URL は慎重にクリックする
  4. パソコンからファイルをダウンロードする際、悪性コードが含まれていないかを必ず確認する
  5. ワクチンのパッチを確認し、セキュリティソフトウェアを最新に維持する
  6. スマートフォンのロック機能 (パスワード設定) を利用し、他のユーザーのアクセスを防止する。ロック機能のパスワードは、随時変更する
  7. Bluetooth 機能をオンにすると、自動感染の可能性があるため、使用時のみオンにする
  8. ID、パスワードなどをスマートフォンに保存しない
  9. バックアップを周期的に行い、紛失時に情報の空白が生じないようにする
  10. 改造したり、コピー防止機能などを解除したりしない
- フォーティネット社が示すスマートフォンのセキュリティ対策のポイント [4]
  1. PCと同様のパッチ管理を（更新の迅速な適用）
  2. 不審な問い合せには確認を（フィッシング対策）
  3. インストールには細心の注意を（発行元を確認）
  4. Bluetoothなどの通信は必要な時だけ使う

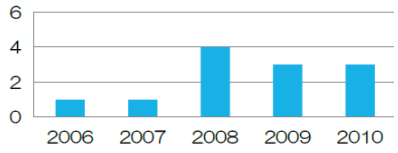
[1]：アンラボ, “韓国で初のスマートフォン悪性コード被害発生”, http://www.ahnlab.co.jp/company/press/news_release_view.asp?searchWord=&movePage=&seq=4886
[2]：東亜日報, “スマートフォンの悪質ウィルス、韓国で初めて被害例”, http://japanese.donga.com/srv/service.php3?biid=2010042344128
[3]：フォーティネットジャパン, “SMSや携帯電話を標的にした新しいワーム「Yxes.A」”, http://www.fortinet.co.jp/news/pr/2009/pr022409.html
[4]：“スマートフォンのセキュリティ対策4カ条”, http://www.itmedia.co.jp/enterprise/articles/0905/23/news004.html

1．4 スマートデバイス ③情報セキュリティ上の脅威（続）

・携帯端末に対するこれまでのマルウェアの主な対象は、Blackberry端末のOSやSymbianOSである。
・携帯端末関係の脆弱性はコンピュータ関連の脆弱性の件数に比べまだわずか規模にすぎないが、サービス妨害攻撃を受けたり、第三者によって操作される可能性がある脆弱性も発見されている。

携帯端末のマルウェアの増加率
（Data Source: F-Secure）





携帯端末関係の脆弱性の推移

（出所：経済産業省「サイバーセキュリティと経済研究会」第一回（2010/12/20）資料より引用）

1．5 LBS（Location-Based Services、位置情報サービス） ①概要

- **概要：** 携帯端末により得られた位置情報を活用してユーザーに役立つコンテンツを提供するサービスであり、携帯端末からモバイルネットワークを介してアクセス可能である。提供されるコンテンツは、地図情報に位置、時間、付近の場所や人間の属性情報を付加したものでクーポン等の広告の形態を取ることもある。位置情報の検索を伴う店舗案内ポータル（例：食べログ）、位置情報を用いたゲーム、位置情報を基軸にしたコミュニティ形成を行うソーシャル・ネットワーク（例：Foursquare、ロケタッチ）などが含まれる。
- **市場規模：** 消費者向サービス市場（海外）は2009年に約524.7百万ドル（約460億円）と予測される。[1]
- **影響範囲（社会基盤としての重要性）：** 位置情報そのものを提供するサービス以外に、位置情報を基軸に更なる付加価値を持つ各種のサービス（ソーシャルネットワークサービスや位置に広告提供するサービス等）が普及し、ウェブ同様のインフラとなる可能性がある。将来的には地図情報上での複数のサービスが統合され、利用者がウェブをより意識しない方向に進む可能性がある。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- サービス利用者には、任意の地点でログインしサービスを安全に利用させるためにはセキュリティ技術が必要となる。
- 位置情報を伝える必要が無いタイミングでは情報を伝えないようにアクセス制御を行う必要がある。
- 収集されたデータを適切に管理・活用するためのデータ保護、認証技術が必要となる。

脅威像・課題：
- ユーザーの位置のプライバシに関する問題（例：あるサービスの利用者は夏季休暇中の現在位置を他のサービス利用者に知られてしまい、空き巣の被害に会う可能性が高まる）[2]
- サービスの不正利用（なりすまし、データの改ざん/破壊）

技術的な解決策

- 位置情報の利用/収集を拒否できるようなアプリケーション毎のコントロール機能の実装
- 認証機能の実装

[1]：“Gartner Says Consumer Location-Based Services Market Will More Than Double in 2009”, http://www.gartner.com/it/page.jsp?id=1059812
[2]：Panda Security, “夏季休暇に向けたセキュリティアドバイス”, http://www.ps-japan.co.jp/pressrelease/n91.html

1．6 国民ID ①概要

- **概要：**国民等に識別番号を割り当てることで行政サービスの品質と効率の向上を目指す。税制上、所得の正確な把握のために個人識別番号が必要となるために導入が検討されている。利用範囲は、税務分野および社会保障分野、その他の公的手続が挙げられており、含める範囲については複数案を検討中。IDに住民票コード、基礎年金番号、新規に割り当てる番号のどれを使うかは確定していない。[1]
- **市場規模：** 6月末に公表された内閣官房の「社会保障・税に関わる番号制度に関する研究会」の試算によれば、国民ID制度のシステム開発規模は、国民IDを税務のみに利用する場合は5300億円程度、医療や介護、証明書発行業務等に用いる場合には6100億円程度となっている（これらの試算値には運用や周辺事業の費用は含まれていない）。同試算では「セキュリティ対策、プライバシー保護のためのシステム」には2000億～3000億円が必要となると見込まれている。[2][3]
- **影響範囲（社会基盤としての重要性）：**現時点では制度の内容が具体化されていないが、実現された場合は少なくとも税務分野では不可欠な情報システムとなることが予想される。また、社会保障、医療分野でも利用されるのであれば、より国民生活に密接な形でシステムが関わってくると考えられる。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- 国民全員が関わる政府システムである正確から、外部からの不正行為に対して堅牢な作りであるだけでなく、目的外利用等の内部からの不正使用も防止することが求められる。
- 利用者となる国民へのアンケート結果ではセキュリティ面を不安視する傾向がみられた。[4]

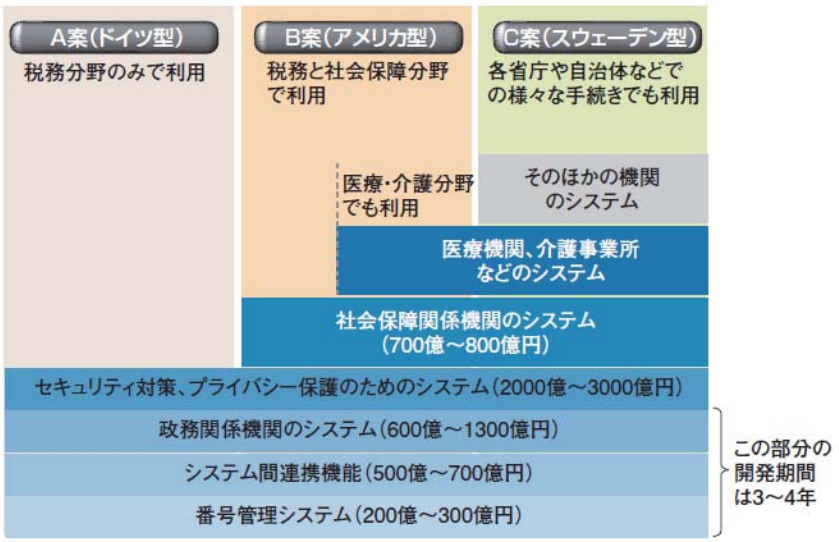
脅威像・課題：
- ネットワーク経由の不正なアクセス
- データベース内の情報の悪用（内部犯、不正アクセス）
- 利用者の個人情報の漏洩
- 利用者のプライバシーの侵害
- 利用履歴の目的外の収集／利用

技術的な解決策

- 制度が明確化されておらず、システムの用途、範囲が明確ではない。現時点で利用が想定されうる技術的解決策の例を示す。
- ID連携/ID管理技術（PKI関連技術が含まれる）
- 認証（パスワード、バイオメトリクスに関する技術を含む）
- ICカード

[1]：国家戦略室, “社会保障・税に関わる番号制度に関する検討会”, http://www.kantei.go.jp/jp/singi/kokkasenryaku/kaigi/syakaihosyou.html
[2]：IT戦略本部, “新たな情報通信技術戦略 工程表（案）”, http://www.kantei.go.jp/jp/singi/it2/dai54/siryou1.pdf
[3]：日経コンピュータReport, “国民IDのシステム開発に6100億円”, http://itpro.nikkeibp.co.jp/article/COLUMN/20100706/349978/
[4]：アイシェア, “「国民ID制度」導入方針決定も「知らなかった」7割半”, http://release.center.jp/2010/06/0401.html

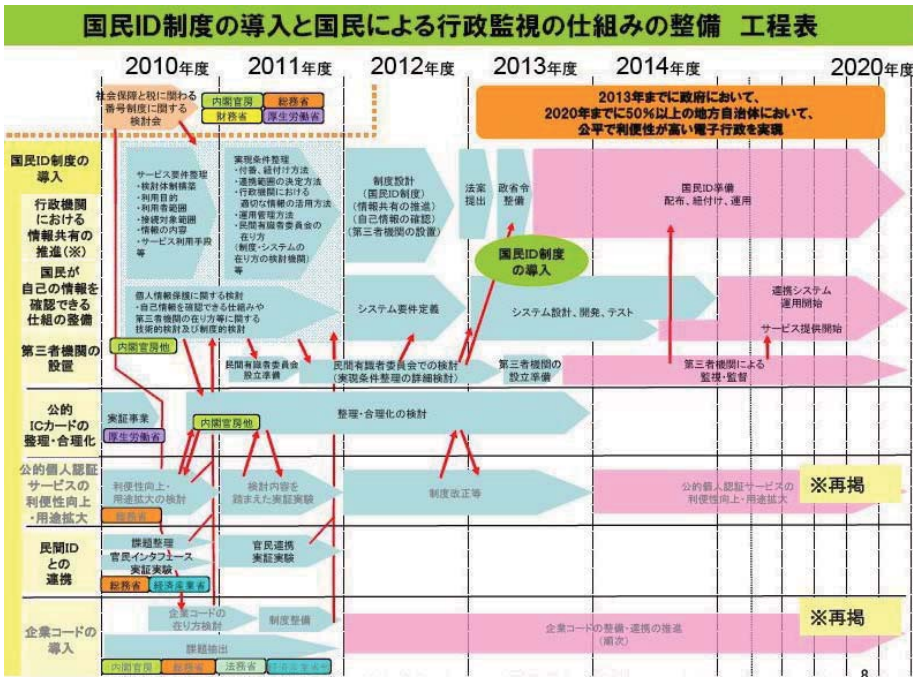
1．6 国民ID ①概要 （参考）国民ID制度のシステム開発規模



図：国民IDの利用範囲によって変わる政府のシステム開発規模

（日経コンピュータReport, “国民IDのシステム開発に6100億円”より抜粋, http://itpro.nikkeibp.co.jp/article/COLUMN/20100706/349978/ ）

1．6 国民ID ①概要 （参考）国民ID制度の導入 工程表



（ IT戦略本部, “新たな情報通信技術戦略 工程表（案）”より抜粋, http://www.kantei.go.jp/jp/singi/it2/dai54/siryou1.pdf ）

1．6 国民ID ①概要 （参考）国民ID導入により自治体にもたらされる効果

想定される分野	対象業務の例	経済効果
①住民情報の連携	・住民税 ・軽自動車税 ・固定資産税 ・国民健康保険 ・長寿医療制度 ・国民年金	約570億円
②住民情報の照会	・住民情報問合せ（他自治体→自治体、国・警察等→自治体、民間→自治体） ・税情報問合せ（他自治体→自治体）	約69億円
③再転入等の調査	・転入者に対する過去の滞納情報の確認 ・転出者に対する滞納情報の確認 ・転入者に対する賦課情報の確認	約62億円
④無駄の多い申請手続	・児童手当、児童扶養手当 ・乳幼児医療費助成 ・生活保護 ・国民健康保険（限度額適用認定）	約210億円
合計		約1,000億円

（IT戦略本部　第6回　電子行政に関するタスクフォース資料2-4, “国民IDでできること”(2010/12/02)を基に構成, http://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai6/siryou2_4.pdf ）

1．7 PCIDSS ①概要

- **概要：** Payment Card Industry Data Security Standard。クレジットカード大手5社が共同で策定したクレジット業界向けのグローバルなセキュリティ標準。クレジットカード情報と取引情報を保護する意図で作られており、セキュリティ対策の実装に関する具体的・定量的なベースライン要件が示されている。PCI-DSSは2010年10月に2.0版が公表され、要求事項の項目は252から280に増加し、多くの要件がより明確化されている[1]。また、関連する基準として2010年5月にクレジットカード読取用端末装置のセキュリティ要件PCI-PTSの3.0版が公開・即時発行されている。クレジットカード情報を扱うアプリケーションソフトウェア開発者向けガイドラインであるPCI PA-DSSは、PCI-DSSと同じく2010年10月に2.0版が公表されている[2]。
- **市場規模：** 国内では2009年に訪問審査を受けたレベル1加盟店（年間取引件数600万件超）の数は30～40社。先行する米国では、レベル1加盟店の約85%、レベル2加盟店（年間取引件数100万～600万件）の約75%がPCI DSSに準拠している[3]。
- **影響範囲（社会基盤としての重要性）：** 金融業、流通業、通信／メディア、製造業などの業界[4]。PCIDSSは、その明確さと準拠すればある一定のセキュリティレベルが達成可能である点が評価されており、データセキュリティ基準のベストプラクティスとみなされている。このためクレジット関連業界だけでなく他業界の企業や組織におけるセキュリティ基準として採用させようという動きが米国においてある。

セキュリティ上の脅威・課題

セキュリティ技術の重要性（役割の大きさ）：
- クレジットカード情報を取り扱う上で、セキュリティ確保は必須であるため、一定の対策実施状況を評価できる基準は有用なものである。

脅威像・課題：
- クレジットカード情報および取引情報を狙う不正者によるデータへの不正なアクセス

技術的な解決策

- 非カード業界の企業・組織を想定したPCIDSSの適用サービス
- 具体的・定量的実装項目の優先順位付けコンサルティング
- 要件に合わせた具体的対策手法のパッケージ/スイート化

[1]: BSIグループジャパン, ”PCI DSS Ver.2.0の要件を解説” http://www.paymentnavi.com/paymentnews/8739.html 及び 8741.html
[2]: PCI-SSC, “PCI SECURITY STANDARDS COUNCIL RELEASES VERSION 2.0 OF THE PCI DATA SECURITY STANDARD AND PAYMENT APPLICATION DATA SECURITY STANDARD”, https://www.pcisecuritystandards.org/pdfs/pr_101028_standards_2.0.pdf
[3]: リテールテックJAPAN, “2010年、「PCI DSS」普及の波は来るか ”, http://www.shopbiz.jp/rt/column/pointpayment/58781.html
[4]: 日本カード情報セキュリティ協議会, “PCIDSSとは”, http://www.jcdsc.org/pci_dss.php

1．7 PCIDSS ①概要（参考）PCIDSSの6項目12要件

- I. 安全なネットワークの構築・維持
  1. カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること
  2. システムパスワードと他のセキュリティ・パラメータに、ベンダ提供のデフォルトを使用しないこと
- II. カード会員データの保護
  3. 保存されたカード会員データを安全に保護すること
  4. 公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
- III. 脆弱性を管理するプログラムの整備
  5. アンチウィルス・ソフトウェアを利用し、定期的に更新すること
  6. 安全性の高いシステムとアプリケーションを開発し、保守すること
- IV. 強固なアクセス制御手法の導入
  7. カード会員データへのアクセスを業務上の必要範囲内に制限すること
  8. コンピュータにアクセスする利用者毎に個別のIDを割り当てること
  9. カード会員データへの物理アクセスを制限すること
- V. 定期的なネットワークの監視およびテスト
  10. ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること
  11. セキュリティ・システム、および管理手順を定期的にテストすること
- VI. 情報セキュリティ・ポリシーの整備
  12. 情報セキュリティに関するポリシーを整備すること

“**Payment Card Industry**（**PCI**）データセキュリティ基準　要件とセキュリティ評価手順 バージョン **1.2**”より引用、
https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf

第2章　有望領域における情報セキュリティ技術の関連動向

2．1　有望なICT領域と重要となる情報セキュリティ技術の関係

- 本調査では、社会的影響やサービスの関連性等を勘案し、今後有望なICT領域として「クラウドコンピューティング」「スマートグリッド」「スマートデバイス」「国民ID」「デジタルサイネージ」「位置情報サービス」を選択した。次に、各領域を支える重要な情報セキュリティ技術について採り上げ、それらの位置関係を下図に整理した。
- 下図から、特に「ID管理」、「組込みセキュリティ」「プライバシー保護」の技術は、複数の領域において重要な役割を果たし、影響力が大きいと考えられる。ただし、「プライバシー保護」は、検討範囲が技術的な領域に留まらず、倫理や社会通念に踏み込んだ議論が必要なテーマであるため、本年度の対象からは除くことにする。
- そこで、本年度の調査では、重要な技術として「ID管理」と「組込みセキュリティ」を選定した。

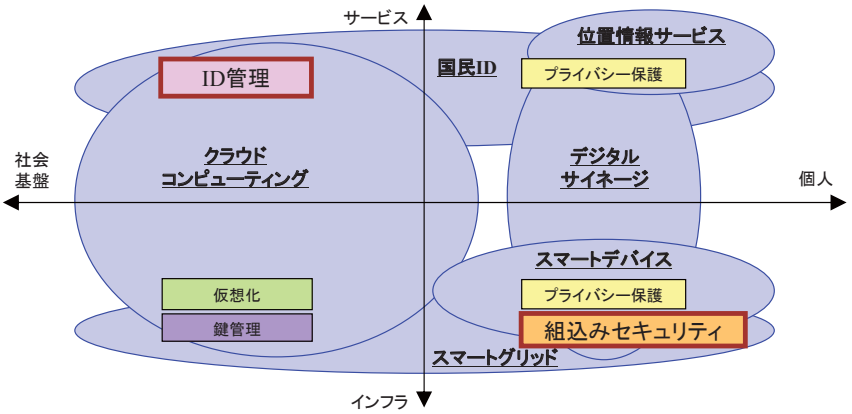


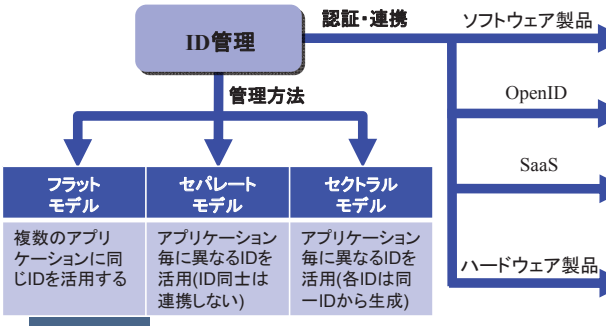
図　有望なICT領域と重要となる情報セキュリティ技術の関係

2．2　ID管理

概　要

- クラウドコンピューティングの台頭を背景として、ID管理（アクセスコントロール、認証、ID連携等）の重要性が高まっている。特に、パブリッククラウドやプライベートクラウド、イントラネットの混在環境において、統合的な認証機能が必要となっている。
- 国民ID導入が検討されているが、韓国等の例を見ても、セキュリティへの配慮が極めて重要である。

実現の方向



国内外の開発・導入事例

事例	概要	技術的特徴
HP IceWall SSO	一度の認証で複数のWebアプリケーションへのログインを実現し、さらにセキュリティと「アクセスコントロールの4A」の統合を実現	エージェントレスでOSやWebアプリケーションに制限の少ないリバースプロキシ方式を主体としたWebシングルサインオン製品。オプションによりエージェント型にも対応
PKIとOpenIDの融合	PKIとOpenIDを融合した組織間認証連携機構の提案	OpenID ProviderがサーバのPKIでユーザの認証を取ることで信頼性と柔軟性を両立
SCS CLIP IAS クラウド統合認証サービス	Google Apps、Salesforce CRMなどのクラウドサービスや、社内システム、ECサイト・SNS等BtoCサイトなど、本人確認が必要なシステムの認証レベルを向上させ、不正アクセスを防止する	公開鍵暗号を用いたPKI（Public Key Infrastructure）と同等の強固な認証基盤上で、さまざまなクラウドサービスやWebアプリケーションの認証をシングルサインオン連携させることができる
ハードウェアトークンと鍵管理サーバを用いたシングルサインオンシステムの開発（論文）	サービス提供者側の機能を変更することなく多様なサービスに適応可能で、スケーラビリティに優れたSSO 環境を実現することを目的として、ネットワーク上に設置した鍵管理サーバとハードウェアトークンを用いる方式を提案する	サービス提供側における対応が不要であり、多様なサービスに適用可能なシングルサインオンシステムを実装している。本方式はエージェント方式およびリバースプロキシ方式のいずれにも該当しない手法である

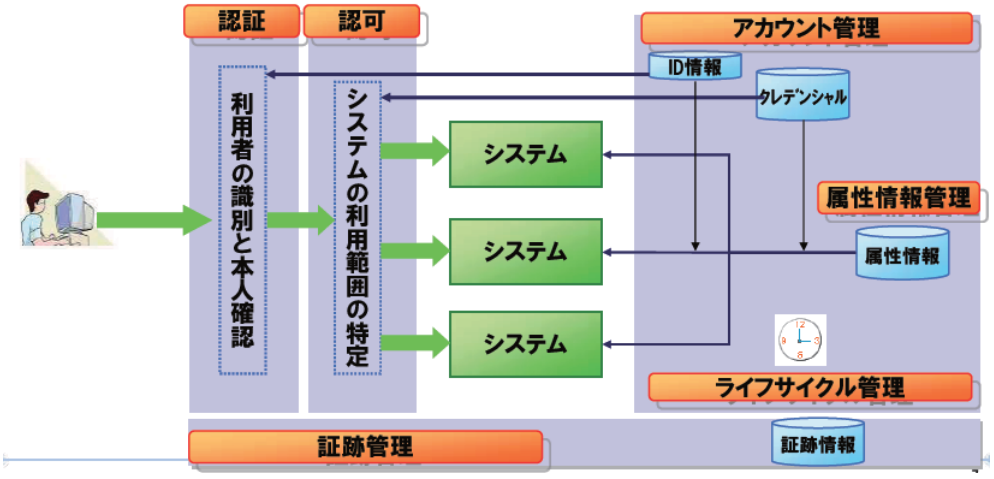
課　題

- ID管理技術は事実上の標準技術が出揃いつつあり、それらを組み合わせた総合的な管理の枠組みを整える必要がある。
- 国民IDには、韓国やオーストリアの例を参考に、マスターIDを直接アプリケーションに適用せずトランザクションIDを用いる方向が考えられる。
- 国民IDの導入に際して、強固な管理環境を整備するだけでなく、IDの大量流出に対する準備をしておくことが望まれる。

[1] 阿部英司, 伊東栄典, 笠原義晃, 中國真教, “認証つきサービスにおける組織間連携のためのPKIとOpenIDの融合” ,九州大学システム情報科学府情報理学専攻
https://qir.kyushu-u.ac.jp/dspace/bitstream/2324/15952/1/iot2-final.pdf

2. 2 ID管理 ①基本構成

- クラウドコンピューティングの環境では、従来明確だったID管理の境界が曖昧化し、統制が困難になる。一方、ユーザの利便性を確保するためには、ID連携やSSOの導入が重要になる。
- 統合ID管理を実現するためには「アカウント管理」、「認証」、「認可」、「属性情報管理」、「ライフサイクル管理」、「証跡管理」からなる6機能が必要である。



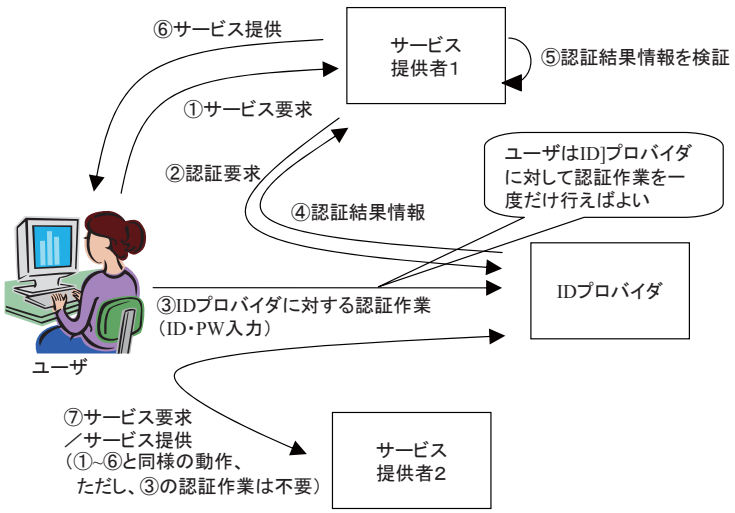
出所：山田 達司, "統合ID管理入門",「カンターラ・イニシアティブ・シンポジウム2010」講演資料, 2010/09/01

2. 2 ID管理 ②標準化動向

- ID管理技術は、適用範囲が多岐にわたるため、Liberty AllianceやOASIS Open、OpenID Foundationなど複数の団体が異なるアプローチで標準化・実用化を進めてきた。
- 2009年6月には、ID管理について業界横断的に規格策定、相互運用を推進するための団体として、Kantara Initiativeが設立された。Kantara Initiativeは、などの各種団体を横断的に束ね、OpenID、SAML 2.0といった標準規格の相互運用性を高めながら、セキュリティやプライバシー保護など標準技術を確立することを目指している。

名称	概要
SAML (Security Assertion Markup Language)	・事前に信頼関係を築いたサービス間で、ID情報をセキュアに配布する。認証トークンの記述方式およびその配布方式。 ・主に企業等の組織向けに利用される。
OpenID	・個々のユーザが持つURL・XRIをグローバルにユーザを特定する値（ユーザID）として利用する、オープンな認証方式。 ・主に消費者向けサービス向けに利用される。
OAuth (Open Authentication)	・消費者があるクラウドサービスプロバイダに格納したプライベートなリソースを、認証情報を開示する必要なく、別のクラウドサービスプロバイダと共有する認証標準。
Information Card	・ユーザ情報の提供やID証明を目的とした仮想的なIDカード。 ・クライアントベースのソフトウェアで、オンラインサービスのユーザ認証に使う。 ・実装例として、Microsoft社のWindows CardSpaceがある。

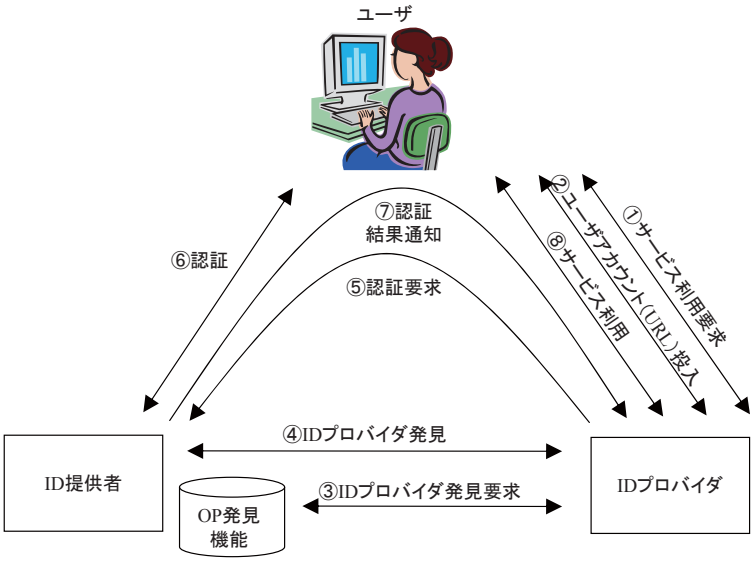
2．2 ID管理 ③SAML （Security Assertion Markup Language）



ID連携方式におけるシングルサインオンの処理の流れ（SAML2.0の場合）

出所：高橋健司,"アイデンティティ管理の現状と今後", 電子情報通信学会 vol.92 No.4 pp.287-294, 2009/04

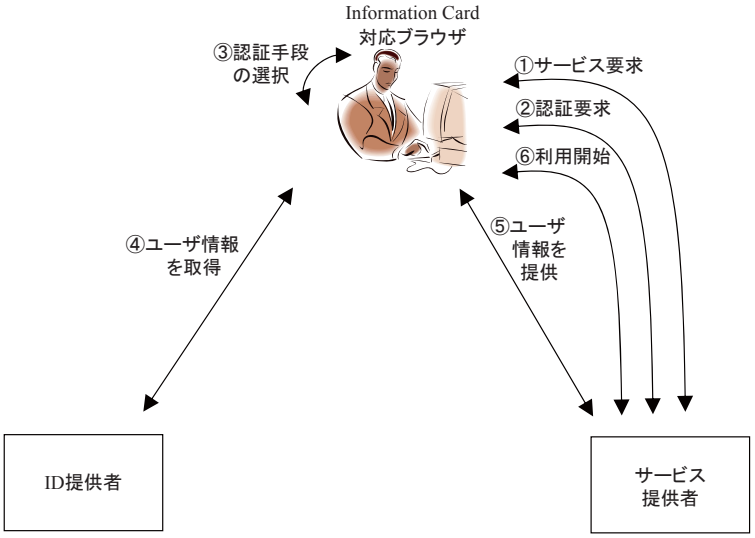
2．2 ID管理 ④OpenID



ID統一方式におけるシングルサインオンの処理の流れ（OpenID2.0の場合）

出所：高橋健司,"アイデンティティ管理の現状と今後", 電子情報通信学会 vol.92 No.4 pp.287-294, 2009/04

2．2 ID管理 ⑤Information Card



ID選択方式の処理手順（Information Cardの場合）

出所：高橋健司,"アイデンティティ管理の現状と今後", 電子情報通信学会 vol.92 No.4 pp.287-294, 2009/04

2．2 ID管理 ⑥アイデンティティ・アクセス管理

- CSA「Domain12: Guidance for Identity & Access Management V2.1」によると、クラウドにおいて重要となるIAM（アイデンティティ・アクセス管理）機能の要素技術は以下のとおりである。

●アイデンティティプロビジョニング（Identity Provisioning ）
クラウドを利用するに際しては、利用しうる状態(プロビジョニング－ユーザに対する権限の割付け)であるか利用し得ない状態(デ プロビジョニング－ユーザに割付けた権限の解除)であるかを安全に、かつ時宜に、管理するという問題に対処しなければならない。しかも、この問題は、さらに、利用組織において、いままでのアクセス管理をクラウドサービスの利用にまでに拡張しなければならないという問題をもっているのである。

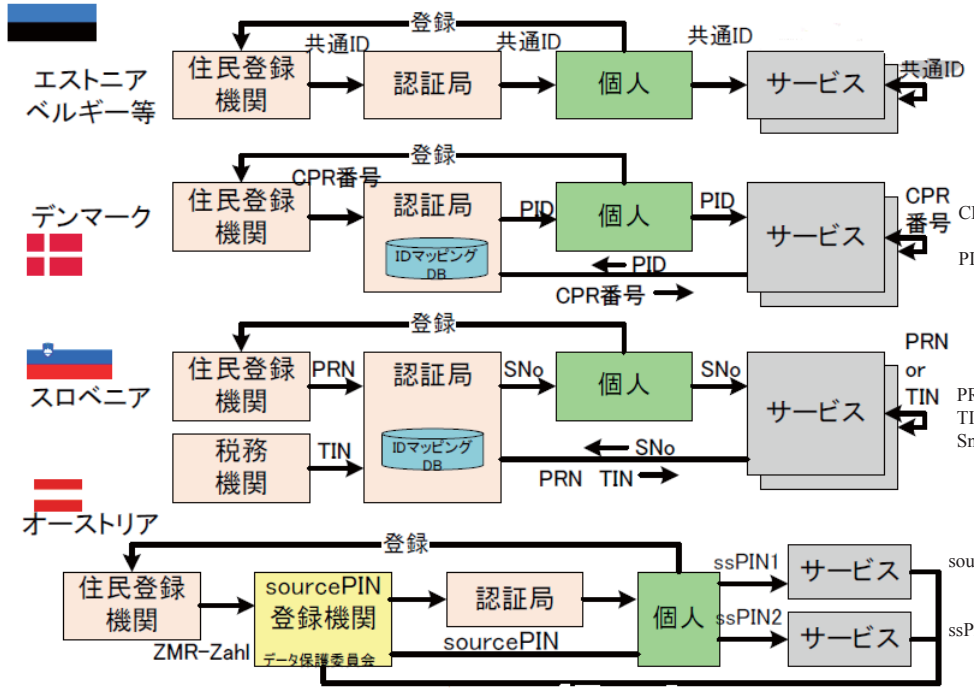
●認証（Authentication）
利用者が、クラウドサービスを利用する際には、ユーザの認証を、信頼できる方法で管理することが重要なことになる。そのような認証のためには、クレデンシャル情報の管理や、認証処理の委譲、クラウド全般のトラスト管理などの問題を検討する必要がある。

●連携（Federation ）
アイデンティティの管理に際しては、その管理をする事業者が、お互いに安全に、認証手続を統一してすることができるように、フェデレーションを組むのが、利用者の便宜という観点からも求められるのではないかということから、種々の動きがある。

●アクセス管理とユーザプロファイル管理（Access Control and User Profile Management）
そのユーザが、どのような立場でアクセスするのかということに応じて、ユーザのプロファイルおよびアクセス管理に求められるものが異なってくる。ユーザのプロファイルの正確な情報にもとづいて、そのユーザが、どの資源にアクセスしうるのかというアクセス管理がなされる。クラウドサービスの環境では、それらの情報が種々の組織から提供されることになるために、きわめて、困難な作業ということになる。しかも、その管理手法が監査可能な手法でなされる必要がある。

●IDaaS（Cloud Identity as a Service）
IDaaS とは、アイデンティティの管理をサービスで行おうとするものである。そして、そのサービスをクラウドを用いて行うという考え方が提案されている。

2．2　ID管理　⑦国民IDの登録・利用モデル



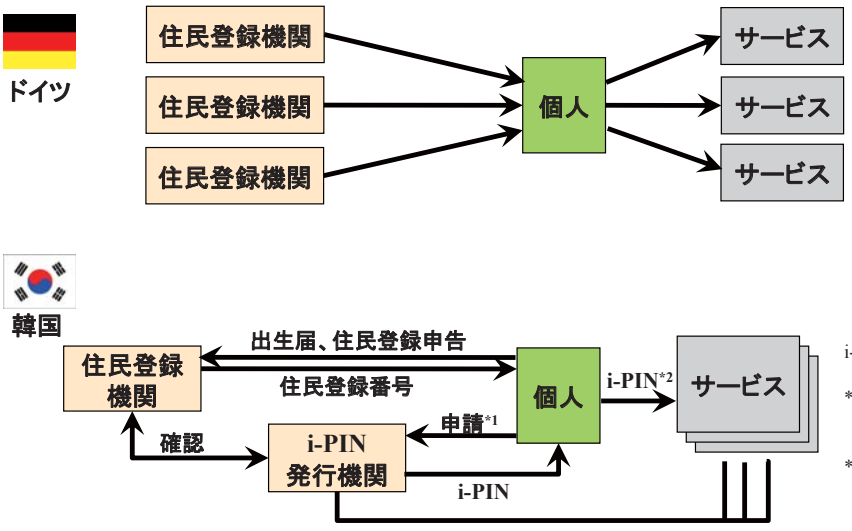
CPR番号: 中央住民登録番号（国民番号）
PID: Person specific Identification Numbers

PRN: 個人登録番号
TIN: 納税者番号
Sno: 認証局が管理するシリアル番号

sourcePIN: CPR番号を暗号化して生成するソース識別番号
ssPIN: sourcePINとセクターコードから生成するセクター用個人識別子

出所：松本　泰, ”欧州の政府系PKIとID管理”, 2009/06/24

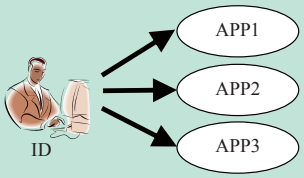
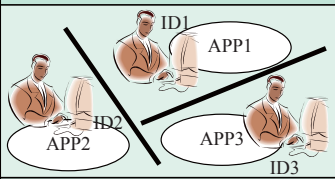
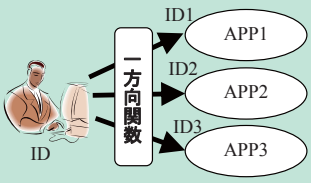
2．2　ID管理　⑦国民IDの登録・利用モデル（続き）



i-PIN: Internet Personal Identification Number
*1)　住民登録番号と、携帯電話、公的個人認証等を入力
*2) サービスの入会時に入力するが、サービス利用時には使わない

各種情報よりMRI作成

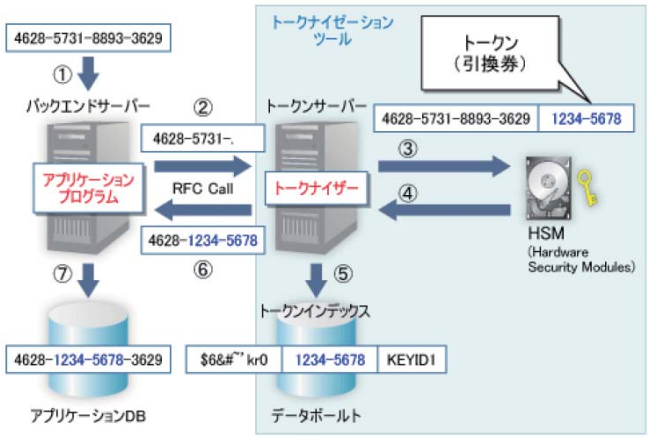
2．2 ID管理 ⑧国民IDの管理モデル

モデル	形態	特徴	問題点
フラットモデル エストニア スウェーデン デンマーク ベルギー 韓国 ・・・		● 一つの識別番号を全ての機関で共通で利用する ● 各機関が保有する情報の連携が容易 ● 各種行政カードを統合しやすい	● 不正利用や漏洩時のデータマッチングリスクが相対的に高い [加筆] ・デンマークではIDから導出したPIDを使用（PIDからIDを導出可能） ・韓国では使い捨てID（i-PIN）を使用（i-PINからIDは特定困難）
セパレートモデル ドイツ スロベニア （日本）		● 行政分野ごとに異なる個人識別番号を付番 ● 個人情報の紐付けが難しく情報連携が困難 ●「国民総背番号制」とは一線を画している	● 不正利用や漏洩時の危険性が相対的に低い ● セクターごとに別の番号があるため行政カードの統合が不可能
セクトラルモデル オーストリア		● 統一番号からセクターごとに異なる番号が生成される ● 分野別に番号が異なるため不正利用の危険性が相対的に低い ● カードに収納する識別番号は1つで済む	● 個人情報の連携には法的な手続きが伴うため、連携手続きに手間がかかる（自らの裁量では情報連携を不可能にしている）

出所：東アジア国際ビジネス支援センター 安達和夫, ”海外における共通番号・国民IDの活用事例とその課題”, 2010/07（一部加筆）
http://www.eabus.org/index_files/report/index_files/r100723.pdf

2．2 ID管理 ⑨トークナイゼーション

- 機密データを別の文字列（トークン）に置き換えることにより、機密データそのものが散在することを防ぐ情報管理技術。暗号化と異なり、トークンは元の数列とは数学的関連性がないため、元の数列を推測されるリスクが低い。
- PCI DSSでは、クレジットカード番号にトークナイゼーションを適用することにより、実際の審査範囲（実際のクレジットカード番号を取り扱う業務プロセス）を縮小できる点で高く評価されている。
- 実装では、同じトークンを重複して生成しないトークンサーバと、トークン（トランザクションID）と元の数列（マスターID）の対応表を記録するデータベースは、厳重なアクセス制御が施された環境で管理する必要がある。

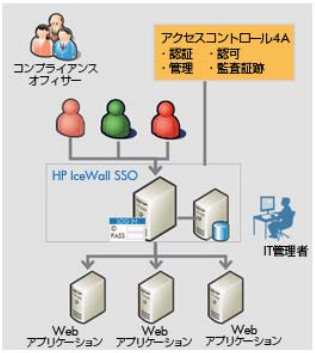


トークナイゼーションの概要

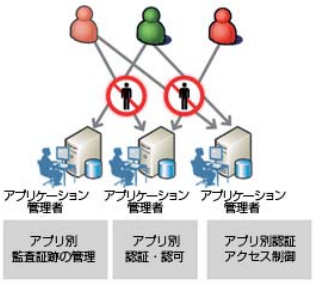
出所：山崎 文明, ”新常識になる「トークナイゼーション」”, 日経ITPro, 2010/11/19

2. 2 ID管理 ⑩HP IceWall SSO

- シングルサインオンを、リバースプロキシ型で提供 [1]
  - ✓ アクセスコントロールの4Aである認証、認可、管理、監査証跡を実装
  - ✓ 複数のWebアプリケーションの外側に待機し、シングルサインオンを実現する
  - ✓ 直接リバースプロキシ型でネットワーク上に配置されるIceWallサーバと、IceWallサーバと連携して認証、ログ管理を行う認証サーバの組み合わせで動作
  - ✓ オプション設定によりWebサーバ内に設置するエージェント型にも対応
- 大規模イントラネットでの導入に対応 [2]
  - ✓ 多様な接続方式、複雑な組織・人事異動に対応
  - ✓ 認証モジュールの分散化、バックアップサーバを使ったアクセス専用スレッドによる可用性向上の仕組み [3]
  - ✓ ICカード、証明書、生体認証などの二要素認証に対応
  - ✓ LDAP, データベースタイプのどちらのデータベースにも対応



HP IceWall SSOを用いた統合管理



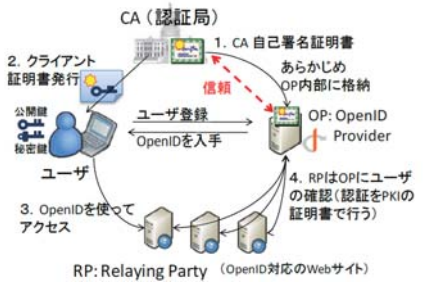
アプリケーション毎（まかせ）の管理

従来環境からHP IceWall SSO環境への変化［1］

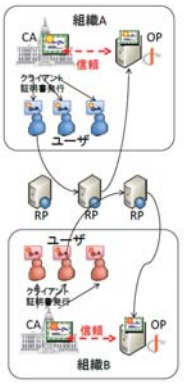
<参考>
[1] HP IceWall SSOとは http://h50146.www5.hp.com/products/software/security/icewall/sso/about/what.html
[2] HP IceWall SSO 目的別利用ガイドhttp://h50146.www5.hp.com/products/software/security/icewall/sso/guide/index.html
[3] 複数の認証サーバーでシングルサインオンの負荷分散 http://itpro.nikkeibp.co.jp/db/article/10004850/

2. 2 ID管理 ⑪PKIとOpenIDの融合

- PKI (Public Key Infrastracture: 公開鍵認証システム)とOpenIDを融合
  - ✓ PKIは強固なセキュリティだが、サーバごとに鍵を作成する必要があり、柔軟性に欠ける
  - ✓ OpenIDはシングルサインオンを可能にするため柔軟であるが、認証がID、パスワード方式であることが多く、セキュリティに脆弱である
  - ✓ PKIとOpenIDを融合させ、OpenIDプロバイダ上で鍵認証を行い、安全で柔軟な認証環境を構築
  - ✓ 単一システムだけでなく、組織を越えた連携を可能にする
- 小規模システム上にて動作を確認
  - ✓ Wikiの認証システムにて提案手法を実装
  - ✓ 処理速度は2msと高速であった
  - ✓ 大規模システムにおける動作確認と負荷テストが今後必要である



・OpenIDとPKIの連携システムの概要図 [1]



・OpenIDとPKIの連携システムの組織間連携図 [1]

<参考>
[1] 阿部英司, 伊東栄典, 笠原義晃, 中國真教, “認証つきサービスにおける組織間連携のためのPKIとOpenIDの融合” ,九州大学システム情報科学府情報理学専攻 https://qir.kyushu-u.ac.jp/dspace/bitstream/2324/15952/1/iot2-final.pdf

2. 2 ID管理 （参考）有識者の見解

- 対象：CSA Japan 関係者
- 日時：2010/08/23(月）
- 概要：

●クラウドコンピューティングにおけるID管理・ID連携について

- CSAの報告書”Security Guidance for Critical Areas of Focus in Cloud Computing”で挙げられていたクラウドコンピューティングの13のセキュリティ課題のうち、大半は既存のICTにおけるセキュリティ課題であるが、「暗号化と鍵管理」「アイデンティティ・アクセス管理」はクラウド環境において特に意識しなければならない課題である。
- 業務アプリケーションをクラウド環境に置いたときに、どう管理するか。社内のID管理、アクセス管理を実現するというのは基本的な要求だが、クラウドに搭載すればクラウド側のアクセス管理に依存せざるを得ない。
- ユーザ側のシステム構成も多様で、成熟度もばらついているので、クラウド事業者側の対応も難しい。たとえば、ID連携の標準化をクラウド側でサポートし、ユーザ側とのインタフェースを提供する形が望まれる。
- 様々なベンダがID管理やID連携を提供しているが、それらの相互連携も必要ではないか。
- ただし、技術開発課題として見た場合、既存の技術を適切に活用すれば実現できる可能性が高い。

●その他の技術開発課題

- 技術開発課題としては、「仮想化」が重要。特に「バーチャルマシン間のアイソレーションがロジカルに担保されるか」という点で、ブレークスルーが必要と考える。

（脅威の例）ハイパーバイザーがリアルサーバを触るときにサイドチャネル攻撃をしかけられる
休眠中のバーチャルマシンについて、updateできていない状況だと大変

- クラウドのような極端に大規模なシステムでは、DBアクセスやキャッシュの管理も、通常の動きを念頭にプログラムを書くと、問題が生じる可能性がある。

2. 3 組込みセキュリティ (a)スマートデバイス

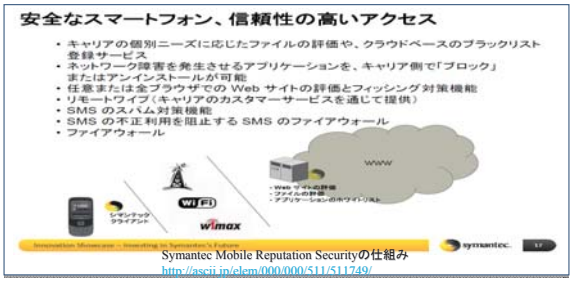
概 要

- スマートデバイスとは、スマートフォン、タブレットPC、電子書籍リーダ 等を指す。本調査では、主にスマートフォンを採り上げる。
- スマートフォンを狙うマルウェアが登場し始めており、すでにiOS, Android, Windows Mobile, SymbianOSを搭載するスマートフォンを対象とするマルウェアが確認されている
- スマートフォン向けセキュリティ製品はシマンテックやエフセキュア等より販売されており、需要は増していくものと思われる

国内外の開発・導入事例

事例	概要	技術的特徴
シマンテック, Symantec Mobile Reputation Security	スマートフォン向けセキュリティ技術で、クラウドを利用したマルウェア対策が行える。	レピュテーション技術を採用しており、ユーザからのファイル情報をクラウド上に集めデータベースを作成し、ファイルの安全度を判定する。
F-Secure, F-Secure Mobile Security 6	Symbian,Windows Mobile,Android スマートフォン向けセキュリティ製品。マルウェア対策、盗難防止、ブラウザ保護等の機能を備える。	セキュリティ研究所による自動アップデートにより、最新の脅威に24時間体制で対応。 クラウド上で危険なウェブサイトの情報を共有し、ユーザが有害なサイトにアクセスするのを防止。
[論文] Monitoring smartphones for anomaly detection	Symbian OSとWindows Mobileの端末においてどのように異常検出を検知するか示す。	ユーザのスマートフォンにモニタリングシステムを導入し、リモートサーバに対してモニタデータを送信し、多次元データ解析を行う。

ビジネスモデルの例



Symantec Mobile Reputation Securityの仕組み
http://ascii.jp/elem/000/000/511/511749/

課 題

- 「高機能化したモバイルデバイスは、PCと同等もしくはそれ以上に強固なセキュリティ対策が求められる」との指摘がある [1]
- Amazonの「Kindle」において、ハッカーの手によってDRM技術をすり抜けるプログラムが開発されている。
- 「App Store」ではアプリの掲載にAppleの審査が必要となるが、テザリング機能を持ったアプリが一度審査を通過したことがある。また、表向きは懐中電灯アプリとし、テザリング機能を隠し持ったアプリが審査を通過したケースも存在する。

＜参考＞
[1]モバイルのセキュリティ-1：取り巻く脅威 , http://www.mcafee.com/japan/security/mcafee_labs/blog/jp_mobile-security-01.asp

2．3 組込みセキュリティ (a)スマートデバイス
①スマートフォンを含むシステムにおけるセキュリティ対策

	セキュリティ上の脅威	対策
本体、メモリ等	置き忘れ、盗難、紛失	ロック機構、各種認証システム、リモート消去、暗号化 等
	落下、水没、不慮の故障	ストラップの利用、保険加入
OS、ソフトウェア	不正プログラムによるデータ破壊、漏洩	ウイルス対策、不正プログラム監視、バックアップ
	バグによるデータ破壊	信頼性の高いソフトウェアの利用、バックアップ
	OSの脆弱性をついた外部からの攻撃	OS更新管理、迅速な更新、ファイアウォール
	スパムメール	対策サービスの活用
	有害サイトへのアクセス	フィルタの実施
端末内の情報資産	不正利用、データ破壊、漏洩	認証、ロック機構、データの暗号化
	権限外のアクセスによる情報漏洩	アクセス制限設定、グループポリシーの策定
	データ破壊	バックアップ
通信網	通話の傍受	利用場所等のルール策定
	データ傍受	VPNの利用
	セキュリティの弱い通信	弱い通信方式の利用を制限

スマートフォン利用におけるリスクと対応策

（MCPC資料[1]より抜粋）

項目	効果
PINの設定	SIMを抜かれ他人に回線を使われることを防ぐ
ロック、暗証番号の設定	不正使用、情報漏洩の防止
定期的なバックアップ	盗難、紛失時や故障時のデータ消失の回避
OSの更新	不正アクセス・ウイルス対策
メモリカード暗号化	盗難、紛失時の漏洩防止

スマートフォン導入時に行うべき対策

（MCPC資料[1]より抜粋）

（参考）
[1] モバイルコンピューティング推進コンソーシアム、
“2010年スマートフォン導入構築ガイド”、
http://www.mcpc-jp.org/smartphone/SmartPhoneBuildGuide.pdf

2．3 組込みセキュリティ (a)スマートデバイス
② ENISA “Security in Smartphones: Risk, Opportunities and Recommendations”

■ **スマートフォンユーザのリスク**

1. データ漏洩：盗難・紛失により保護されていないメモリー上のデータにアクセスされる。
2. 適切ではない廃棄：機微なデータを削除せずに端末が廃棄あるいは受け渡されデータにアクセスされる。
3. 意図しないデータ公開： プライバシー関連設定があるが気付いておらず変更していない。
4. フィッシング：偽アプリやメール等によりユーザのパスワードやクレジットカード番号を収集される。
5. スパイウェア：個人情報へアクセスされ、権限を濫用される。
6. ネットワーク上のなりすまし：信頼のおけないアクセスポイントでユーザの通信が横取りされる。
7. ダイアラー：こっそりと有償サービスにアクセスするマルウェアで課金を盗み取る。
8. 金融・財務マルウェア：クレジットカード番号やオンラインバンキングの認証情報の窃盗やオンラインバンキングや電子商取引の妨害に特化したマルウェア
9. ネットワークの輻輳：

■ **情報セキュリティに関してスマートフォンが有利な点**

1. サンドボックス化とキャパビリティベースのアクセス制御モデル
2. コントロールされたソフトウェア配布
3. リモートからのアプリケーションの削除
4. バックアップとリカバリ
5. 追加の認証オプション
6. 追加の暗号化オプション
7. 多様性

■ **推奨事項（一部）**

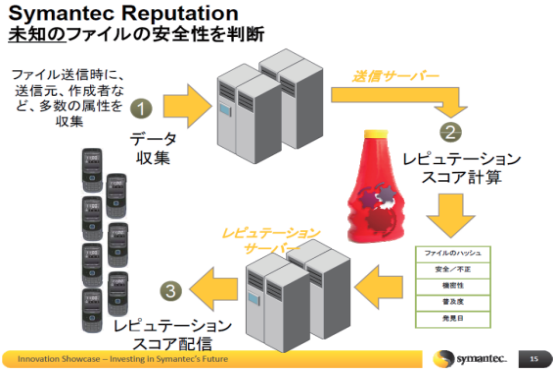
- 一般消費者向け
  - 数分後に自動でかかるロック機能を設定して用いること
  - 新しいアプリやサービスをインストールして使う際には評判を確認すること
  - アプリやサービスから許可を求められた際には精査すること
  - 端末の廃棄やリサイクルの際には、データや設定をリセットし完全に消去すること
- 企業向け
  - 端末の廃棄やリサイクルの際には、メモリーの完全な消去を含む廃棄手順に則って処置すること
  - アプリのインストールについては、もし機密データを扱ったり社内ネットワークからスマートフォンにアクセス可能であるなら、アプリのホワイトリストを定義してこれに従うこと
  - スマートフォンのメモリと取り外し可能なメディアは暗号化すること
- 経営層・高官向け
  - 機密データをローカルに保存せず、スマートフォンからはオンライン・アクセスのみに限定すること。
  - 特に高い機密性を要する場合には、エンドツーエンドの暗号化を用いること
  - セキュアな削除手段を用いて完全に情報を消去し、準備・検査済みのディスクイメージをスマートフォンに定期的に再ロードすること。

（参考）
[1] ENISA “Smartphone Security”
http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

2．3 組込みセキュリティ　(a)スマートデバイス
③Symantec Mobile Reputation Security

- レピューテーション技術
  - ✓ シマンテックリサーチラボが開発したレピューテーション技術をPCとモバイルで採用。
  - ✓ ユーザにファイル情報を送信してもらいクラウド上のサーバでそのファイルの安全度（レピュテーションスコア）を判定。
    - ファイル情報：インターネット上に存在している期間、作成日時、作成者などの属性
  - ✓ マルウェアデータベースをユーザに送る必要がなくなり、大量の亜種に対応が可能となる。

- 携帯電話キャリアが重要なターゲットカスタマー
  - ✓ マルウェア被害は莫大なトラフィック発生等、キャリア側にも影響が生じる可能性がある。
  - ✓ キャリア側に管理画面を用意し、配信ファイルが選べる他、ホワイトリスト、ブラックリストの登録も可能。
  - ✓ エンドユーザ側で既にインストールしたアプリケーションもすぐに停止させることができる。



<参考>
[1] ASCII.jp, シマンテック、スマートフォン用セキュリティの新技術を披露, http://ascii.jp/elem/000/000/511/511749/
[2] CNET Japan, 未知の脅威に対応--シマンテック、スマートフォン向けレピュテーション, http://japan.cnet.com/news/sec/story/0,2000056024,20411441,00.htm

2．3 組込みセキュリティ (a)スマートデバイス　④F-Secure Mobile Security 6

- ブラウザ保護
  - ✓ クラウド上で危険なウェブサイトの情報を共有し、ユーザが有害なサイトにアクセスするのを防止
  - ✓ ユーザが有害なサイトにアクセスしようとした際、事前に注意を促す

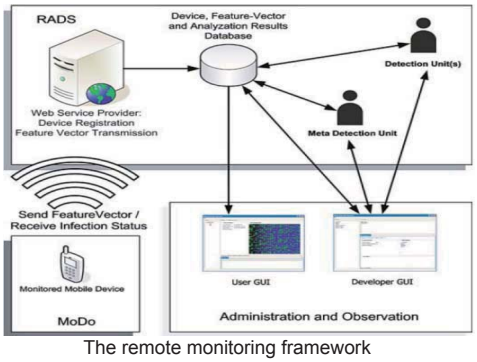
- 盗難防止機能
  - ✓ 紛失や盗難時に遠隔からデータ消去や操作をロック
  - ✓ データ消去やロックは、紛失スマートフォンにSMSメールを送信することで行う
  - ✓ SIMカードが変更されるとそのスマートフォンにはロックがかかり、最新のSIM情報を所有者に送信する

- マルウェア対策
  - ✓ ウイルスやトロイの木馬といったマルウェアを検知・駆除する
  - ✓ エフセキュアのセキュリティ研究所による自動アップデートにより、最新の脅威に24時間体制で対応する

<参考>
[1] エフセキュア、Android用のセキュリティ製品の提供を開始　http://www.f-secure.com/ja_JP/about-us/pressroom/news/2010/fs-news_20100630_01_jp.html

2．3 組込みセキュリティ （a)スマートデバイス
⑤Monitoring smartphones for anomaly detection

- Symbian OS、Windows Mobileにおいて異常検出を行う。
- ユーザから送られてきた特徴ベクトルをサーバ上で多次元データ解析し、マルウェアかどうか判定する。
- 機械学習アルゴリズムは複数チェックし、有用性を確かめる。
- 主成分分析を適用した結果、監視特徴の量を80%削減することができた。
- 今後の課題として、Google AndroidやiPhoneにも対応していく必要がある。



The remote monitoring framework


The Nokia E61 and HTC TyTN B smartphones running the monitoring client

<参考>
[1] Aubrey-Derrick Schmidt · Frank Peters, Florian Lamour · Christian Scheel, Seyit Ahmet Çamtepe, Sahin Albayrak, Monitoring smartphones for anomaly detection, Mobile Networks and Applications, Feb 2009
http://delivery.acm.org/10.1145/1510000/1503504/p92-schmidt.pdf?key1=1503504&key2=7955993821&coll=GUIDE&dl=ACM&CFID=103789637&CFTOKEN=92161968

2．3 組込みセキュリティ （a)スマートデバイス ⑥その他

- テザリング機能を持ったアプリ「NetShare」 [1] [2]
  - ✓ iPhoneをモデム化する機能を持つ
  - ✓ App Storeに公開されるも、数時間で削除される
- 隠し機能としてテザリング機能を有する懐中電灯アプリ「Handy Light」 [3]
  - ✓ 懐中電灯アプリとして登録
  - ✓ 特定の操作を行うことでテザリング機能が有効となる
  - ✓ 既にApp Storeより削除されている
- 「Kindle for PC」に保存されている電子書籍の形式を変換するツール [4]
  - ✓ Kindle用のコンテンツは「.azw」形式で販売されている
  - ✓ 一部のコンテンツにはDRM技術が使用されている
  - ✓ 「Unswindle」は「Kindle for PC」に保存されている書籍を他のデバイスにインポート可能なファイル形式に変換する

<参考>
[1] iPhoneのEDGE/3G接続を共有する公認アプリ、登録後わずか数時間で抹消 http://journal.mycom.co.jp/news/2008/08/01/010/
[2] iPhoneを通して考える通信のこれから：NetShareとNet Neutrality http://nobi.cocolog-nifty.com/nobilog2/2008/08/iphonenetsharen_7acb.html
[3] 隠し機能は“テザリング”、懐中電灯のiPhoneアプリがApp Storeから削除 http://journal.mycom.co.jp/news/2010/07/22/002/index.html
[4] アマゾンの「Kindle」を各種の形式に変換するツール、ハッカーらが続々“リリース” http://www.computerworld.jp/news/hw/171049.html

2．3 組込みセキュリティ （b）スマートメータ

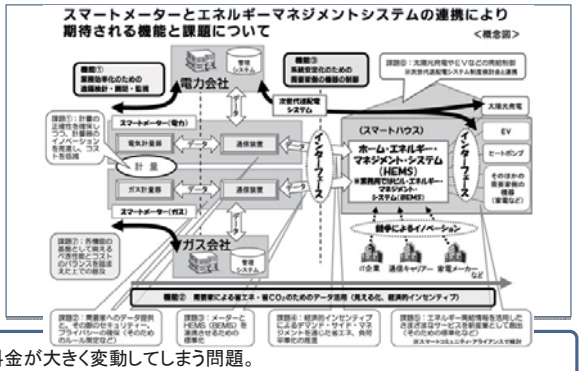
概 要

- スマートメータは、通信機能付きの計量機器のことで、米国や欧州を中心に導入が強くすすめられており、日本にも波及してきている。
- 機能としては、短期的に見れば利用料の遠隔検針や遠隔遮断機能にとどまるが、長期的に見れば家電機器との連携などネットワークを通じた新しいサービスが提案される可能性を持っていると言われている。
- 現在注目されている問題としては、従来機器と計測方法が変わり料金が変動する問題と、電力使用量などのプライバシー情報がネットワークを介してやりとりされることによるセキュリティ上の懸念の問題である。

国内外の開発・導入事例

事例	概要	技術的特徴
NISTガイドライン（NISTIR 7618）	米国スマートグリッドのセキュリティ要件、プライバシへの考慮等を示すガイドライン	スマートメータの通信に係るセキュリティ要件を提示している
IBMによる水道メータへのスマートメータ導入	IBMがマルタ共和国にて、AMI [1]で水道、電力の両方を計測、水漏れも検知	IBMのすすめるSmarter Planetの計装制御系技術を応用。水漏れについてはネットワーク分析技術を利用
東京ガスがスマートメータを国際標準化へ	ガス使用量などのデータをやりとりするシステムで使われる無線をIEEE802.15.4Gとして規格化の提案を行っており、2010年末には標準化案が採択される見通し	近距離の通信ではメータ同士がネットワークを構築し、広域の通信ではNTTの無線通信網を利用する。また三菱電機の通信の低消費電力化技術とも融合
Google PowerMeter	電力会社のみ見ることのできるメータではなく、消費者から見えることを目的とするフリーのモニタリングツール	iGoogleガジェットとして提供されており、どこでも利用出来る。ウェブアプリ
東京電力スマートメータ	一部地域で住宅の電力メータをスマートメータに交換し、各世帯の電気使用量を通信回線で把握する（実験段階）	30分ごとに電気使用量を記録し、無線や光ファイバーなどで東電に送る

ビジネスモデルの例



課 題

- スマートメータ導入によりこれまでよりも正確な計測が可能になり、料金が大きく変動してしまう問題。
- 電力の使用量などはプライバシーに関わる情報なので、そのセキュリティの確保の問題。
- スマートメータ導入による設備負担が電気料金に上乗せされる
- 意図しない機器制御を受ける恐れがある

[1] スマートメータ・インフラ (Advanced Meter Infrastracture)
[2] 経済産業省 スマートグリッドとIT及びエネルギー政策に与えるインパクト http://www.nikkan.co.jp/adv/gyoukai/2010/100727i1.html

2．3 組込みセキュリティ （b）スマートメータ
①IBMによる水道メータへのスマートメータ導入

- IBMは09年3月16日、世界の水問題への取り組みを支援する技術サービス「アドバンスト・ウォーター・マネジメント」を発表 [1]
  - ✓ Instrumented：機能化
    - センサーが至る所に実装されることで河川・給水施設から工場・家庭のパイプに至るまで、水のエコシステムに関わるデータを自動かつリアルタイムで測定
  - ✓ Interconnected:相互接続
    - 測定されたデータを組織・企業・コミュニティを超えて統合的に管理
  - ✓ Intelligent:インテリジェント化
    - 統合管理されているデータを解析モデルに基づき分析
- 水と電力を統合的に監視することにより、戦略的な水システムを構築 [1]
  - ✓ 対象に応じた適切なソリューションを提供
    - ウォーター・マネジメントを河川・港湾などの水資源・海洋資源を対象とした“リソース・マネジメント”
    - ダム、堤防・護岸、給排水施設などを対象とした“インフラストラクチャー・マネジメント”
    - 企業を対象とした“エンタープライズ・マネジメント”
  - ✓ 電力と水には密接な関係がある
    - 電力によって生じた熱を水で冷却している
    - 水を汲み上げるポンプは電力によって行われている
    - IBMのバーリントン半導体工場での水使用量削減のパイロットプロジェクトでは、年間300万ドルの削減効果

＜参考＞
[1] Smarter Planet「スマート」な水資源管理 第1回
http://www-06.ibm.com/innovation/jp/smarterplanet/water-management/index4.shtml

2．3 組込みセキュリティ （b）スマートメータ
②NIST Guidelines for Smart Grid Cyber Security（1/2）

- Guidelines for Smart Grid Cyber Security (NISTIR 7628)。2010年9月公表 [1]。
- スマートグリッドのサイバーセキュリティに関する戦略/アーキテクチャ/要件、プライバシーの問題、リスクアセスについて扱うガイドライン。3つのドキュメントで構成されている：

- 第1部. Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - Executive Summary
  - 1章. Cyber Security Strategy
  - 2章. Logical Architecture and Interfaces of the Smart Grid（スマートグリッドに係る45のアクターの間で、スマートグリッドシステム内および相互間のデータ交換等に用いられるインタフェースを137種に整理。このインタフェースを22カテゴリにセキュリティ上の特徴で分類）
  - 3章. High-Level Security Requirements（全体で189のハイレベルなセキュリティ要件を詳述。これらは前章の22のカテゴリに対応付けられている。多層防御を進めることを推奨している。）
  - 4章. Cryptography and Key Management（鍵管理について）
- 第2部. Privacy and the Smart Grid
  - 5章. Privacy and the Smart Grid（スマートグリッドに接続される一般家庭のプライバシ問題の評価）
- 第3部. Supportive Analyses and References
  - 6章. Vulnerability Classes（スマートグリッドにおける脆弱性のハイレベルな分類）
  - 7章. Bottom-Up Security Analysis of the Smart Grid（リスクアセスの枠組）
  - 8章.（スマートグリッドのサイバーセキュリティに関する研究開発テーマについて整理）
    - その他にも電力網を脅威から守るための各種情報などを記載。

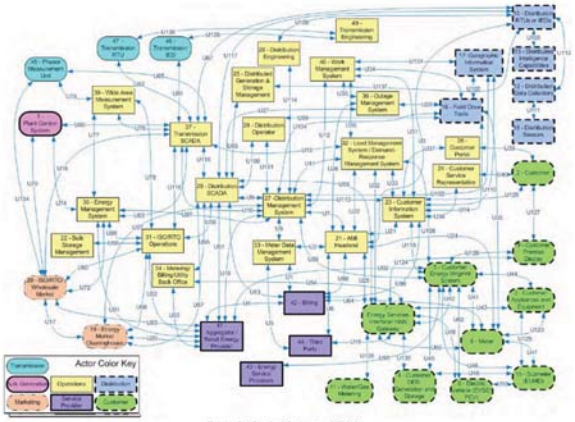


Figure 2-3 Logical Reference Model

＜参考＞
[1] http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

2．3 組込みセキュリティ （b）スマートメータ
②NIST Guidelines for Smart Grid Cyber Security（2/2）

- 同ガイドラインでは、特にスマートメータを含むシステムにおける双方向通信については次のようなセキュリティの確保を要件としている。[1]
  1. ネットワークアクセス認証：
     スマートメータ等の機器が接続されるネットワークへの無関係な機器の無断接続を防止するため、機器をネットワークに接続する際に認証を行う。
  2. スマートメータと電力会社側サーバとの間の安全な通信：
     広域通信ネットワークを経由してスマートメータと電力会社側サーバの間で通信を行うため、暗号化等により盗聴や改竄を防止する。
  3. 暗号鍵の鍵管理：
     認証および暗号通信等に同じ暗号鍵を長期間使い続けることを避けるため、一定期間ごとに鍵の動的な更新等を行う。

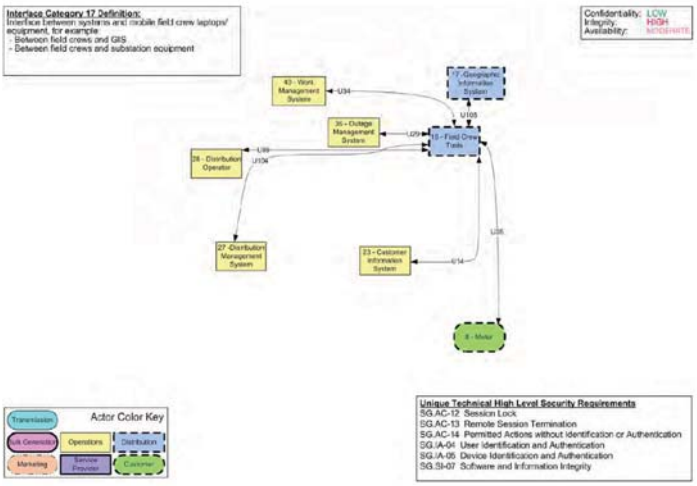


Figure 2-20 Logical Interface Category 17

＜参考＞
[1] 相互認証と暗号化処理を統合するスマートメータ用調合鍵管理技術AMSO(TM) http://www.toshiba.co.jp/tech/review/2010/09/65_09pdf/a07.pdf

2．3 組込みセキュリティ （参考）有識者の見解

- 対象：情報セキュリティ技術者
- 日時：2010/08/20(月）
- 概要：

●組込みセキュリティの現状について

- セキュリティ問題については、まだ開発側の意識がそれほどではない。「組込み」と一言で言っても広く、コンピュータのような被害の歴史がないため、充分に理解出来ていないのではないか。
- 最近では、androidのソフト開発が注目される。Androidにより、リアルタイムOSが無料化したため、携帯だけでなく多様な分野の開発者が飛びついている。

●組込みセキュリティを巡る課題

- iphoneやiPadのアプリケーションのセキュリティが懸念される。Objective-Cについては、一般の商用ソフトが対応していないため。また、適切なコーディングガイドラインも整備されていない状況。
- 脆弱性も顕在化しており、攻撃側からは既に狙われているのではないか。

2．3 組込みセキュリティ （参考）スマートフォンセキュリティフォーラム（仮称）

- スマートフォンセキュリティフォーラム（仮称）
  - 2011年2月1日に準備会発足。発起人は以下の3社：
    - 日本ネットワークセキュリティ協会（JNSA）
    - KDDI株式会社
    - 株式会社ラック
  - 目的：スマートフォンの普及促進を図るために、スマートフォンやタブレット型端末に関するセキュリティ上の課題を、通信事業者や機器メーカー、アプリケーションソフトウェア開発企業、システムインテグレーターらが協調して解決していく。
  - 活動内容：参加メンバー間で課題を共有し、解決策を検討するディスカッションを実施。結果や成果物は随時ウェブにて公開。その他の活動は準備会における議論を進めて決定。
  - 今後の計画：2月下旬から3月上旬までに第1回会合を開催し、4月にフォーラムとしての活動を開始
  - 設立準備会に参加する法人を募集中。フォーラムの主旨に賛同することが加入条件で、業種は問わない。会費は無料。

＜参考＞

[1]「スマートフォンセキュリティフォーラム (仮称)」準備会発足およびメンバー募集のお知らせ
http://www.kddi.com/corporate/news_release/2011/0120a/index.html

2．3 組込みセキュリティ （参考）ネットワーク家電とデジタルサイネージ

- デジタルサイネージの現在の主要領域は「看板」であり、情報セキュリティ上の脅威は少なく、そのような議論もほとんど見られない。
- 一方、家電のネットワーク対応が進んでおり、将来的にはデジタルサイネージの表示機能の一部を担う可能性がある。そうした環境下では、情報セキュリティリスクが様々な形で顕在化することも考えられる。

  例）消費者情報の流出事案が広告主や広告事業体を糾弾する方向に向かう 等

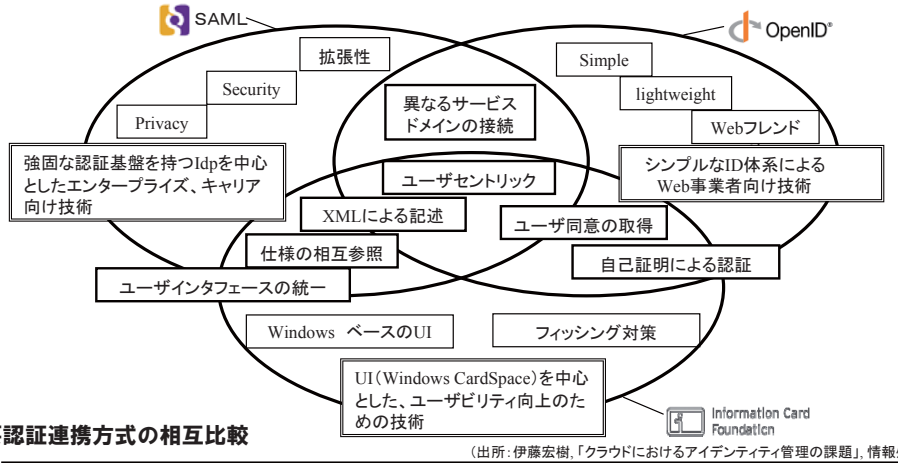
  - デジタルテレビをはじめとする家電のネットワーク化が急速に進展中。プラグアンドプレイや想定外の利用によるリスクの拡大も懸念される[1]。
  - デジタルサイネージがネットワーク家電と連携する方向に展開する可能性もある。
    - 家庭のタブレット端末に電子チラシを提供するサービス[2]
- したがって、今後、デジタルサイネージを支える組込みセキュリティについての検討が必要となる可能性にも配慮すべきであろう。

＜参考＞
[1] IPA「複数の組込み機器の組み合わせに関するセキュリティ調査報告書」（2008/01）
http://www.ipa.go.jp/security/fy19/reports/embedded/index.html
[2] NTT東日本「光iフレーム/フレッツ・マーケット」 http://flets.com/fletsmarket/

第3章 重要な情報セキュリティ技術の展望

3．1　重要な情報セキュリティ技術の展望
1）ID管理　（1）開発課題

- ID管理技術は、適用範囲が多岐にわたるため、Liberty AllianceやOASIS、OpenID Foundationなど複数の団体が異なるアプローチで標準化・実用化を進めてきた。
- 2009年6月には、ID管理について業界横断的に規格策定、相互運用を推進するための団体として、Kantara Initiativeが設立された。Kantara Initiativeは、などの各種団体を横断的に束ね、OpenID、SAML 2.0といった標準規格の相互運用性を高めながら、セキュリティやプライバシー保護など標準技術を普及させることを目指している。
- これらの活動を通じて、ID管理の技術基盤はすでに標準が策定・実用化されており、それらを組み合わせることで求められる機能は実現可能と考えられる。

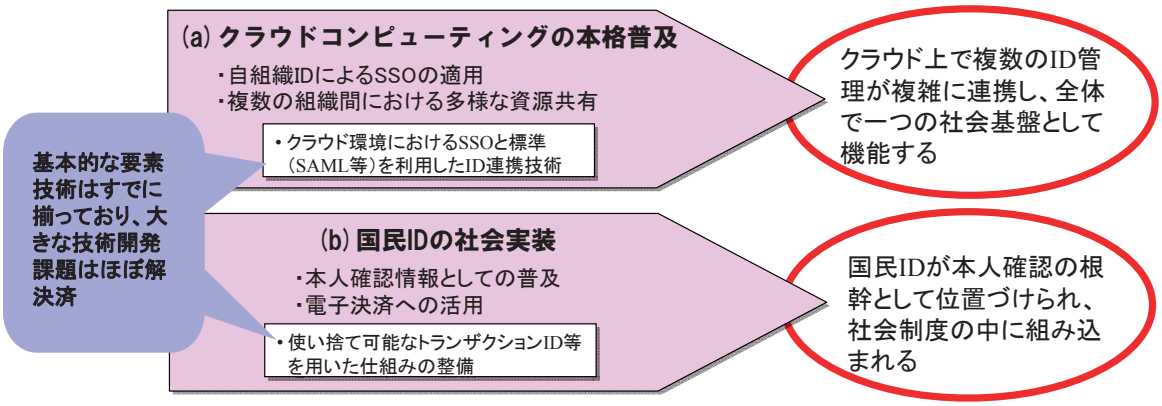


主要認証連携方式の相互比較

（出所：伊藤宏樹,「クラウドにおけるアイデンティティ管理の課題」, 情報処理vol.51 No.12 , 2010/12）

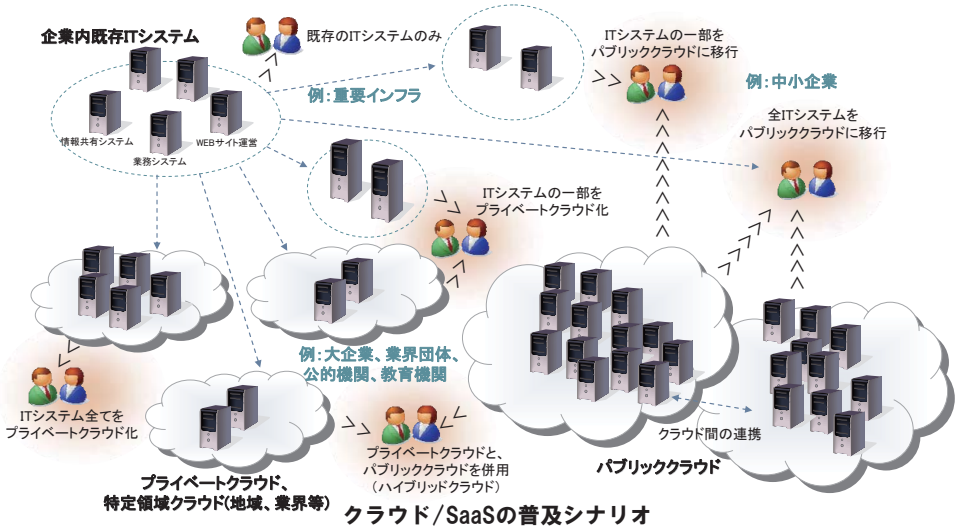
3．1　重要な情報セキュリティ技術の展望
1）ID管理　（2）普及シナリオ

- ID管理技術は、「クラウドコンピューティング」と「国民ID」の2つの潮流において重要な役割を担う。
- これは、多様なID体系が相互に連動する分散型モデルと、一つのID体系が全体の基盤となる集中型モデルに対応すると見ることもできる。
- 「クラウドコンピューティング」では、ユーザ組織が所属メンバーに必要な組織内・外のサービスを自組織のIDで利用可能にすること、ユーザ組織が他組織（取引先、提携・委託先等）との共同作業において必要な組織内・外の資源を共有することが望まれており、それらを実現するID管理技術が要求される。
- 「国民ID」は、行政をはじめとする様々なサービス、特に決済を含むサービスの会員登録における本人確認の手段として機能することが期待されており、それらを実現するID管理技術が要求される。



3．1　重要な情報セキュリティ技術の展望
1）ID管理　(2) 普及シナリオ　a-1)クラウドコンピューティングの本格普及

- クラウドコンピューティングは、情報システムを柔軟に、かつ導入コストを低くできる点で評価され、企業への導入が進む。
- 大企業では、情報管理に係る安心感が高いプライベートクラウドの導入ケースと、基幹系を除く一部の領域を中心にパブリッククラウドの導入ケースが共存する。IT投資やIT部門の人件費の抑制を期待。
- 中小企業は、料金が安く導入が容易なパブリッククラウドを中心に、導入ケースが徐々に増加。
- さらに、大企業が牽引する企業グループやサプライチェーンが参加し、クラウド上での連携が拡大する。



クラウド/SaaSの普及シナリオ

3．1　重要な情報セキュリティ技術の展望
1）ID管理　(2) 普及シナリオ　a-2) クラウドコンピューティングにおけるID管理技術の重要性

- クラウドコンピューティングの利用、特に社内ネットワークとパブリッククラウドの併用やハイブリッドクラウドの利用など、複数の事業者が管理する環境下では、アイデンティティ管理が必要不可欠な概念であり、その重要度が非常に高まっている。
- 国内のCSA関係者も、CSAが示したクラウドコンピューティングにおけるセキュリティ上重要な13の領域のうち、最も重要なものとして、アイデンティティ管理と仮想化を挙げている。
- CSA「Domain12: Guidance for Identity & Access Management V2.1」(2010/04)では、「企業のアプリケーションのためのアイデンティティ・アクセス管理は、今もなお重要なチャレンジである。企業は、優れたアイデンティティ・アクセス管理の戦略抜きでもクラウドコンピューティングサービスを活用することができるかもしれないが、長期的には、組織におけるIDサービスをクラウドに広げることは、オンデマンドのコンピューティングサービスの戦略的な利用のために必要不可欠な条件である。明らかに未熟なクラウドエコシステムの積極的な導入を支持するには、クラウドコンピューティングプロバイダの能力を理解するだけでなく、クラウドベースのアイデンティティ・アクセス管理を実施するための組織の準備を正当に評価することが必要である。」とし、クラウドコンピューティングの利活用における優れたID管理の重要性を指摘している。

クラウドコンピューティングにおけるセキュリティ上重要な領域

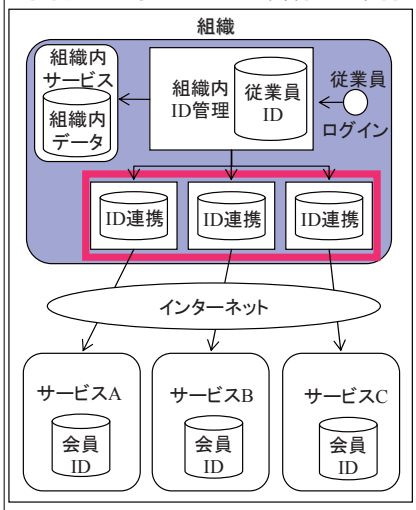
Section I. Cloud Architecture	Section III. Operating in the Cloud
Domain 1: Cloud Computing Architectural Framework	Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Section II. Governing in the Cloud	Domain 8: Data Center Operations
Domain 2: Governance and Enterprise Risk Management	Domain 9: Incident Response, Notification and Remediation.
Domain 3: Legal and Electronic Discovery	Domain 10: Application Security
Domain 4: Compliance and Audit	Domain 11: Encryption and Key Management
Domain 5: Information Lifecycle Management	Domain 12: Identity and Access Management
Domain 6: Portability and Interoperability	Domain 13: Virtualization

(出所：CSA「Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.0」, 2009/12)

3．1　重要な情報セキュリティ技術の展望
1）ID管理　(2) 普及シナリオ　a-3) クラウドコンピューティングにおけるID管理の方向

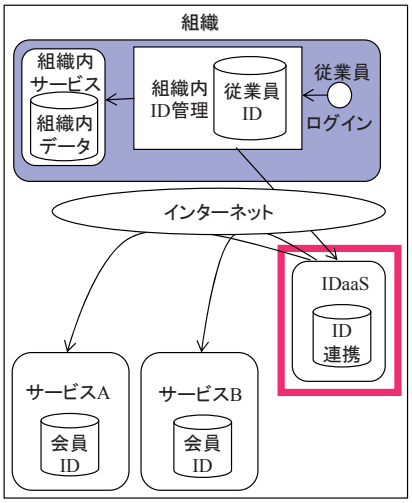
- 企業においては、自社の事情だけでなく顧客や取引先からの要請等のために、クラウドを導入するケースも増加するため、ID管理の効率化、高度化の重要性が急速に高まる。
- 組織のID管理体制を見直した結果、ID連携やIDaaSの需要が拡大し、市場が立ち上がる。

組織内のID管理でSSOを実現する場合



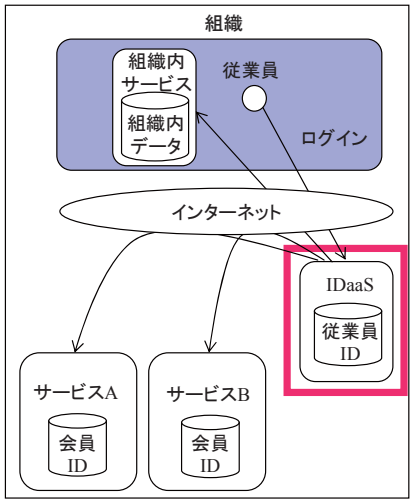
- 組織内外の境界が明確
- 組織外リソースの利用が管理負担を増加

外部サービスをIDaaS経由で利用する場合



- 既存の組織内ID管理との整合性が高い
- アクセス権管理や他組織とのID連携が複雑化

ID管理をすべてIDaaSに依存する場合



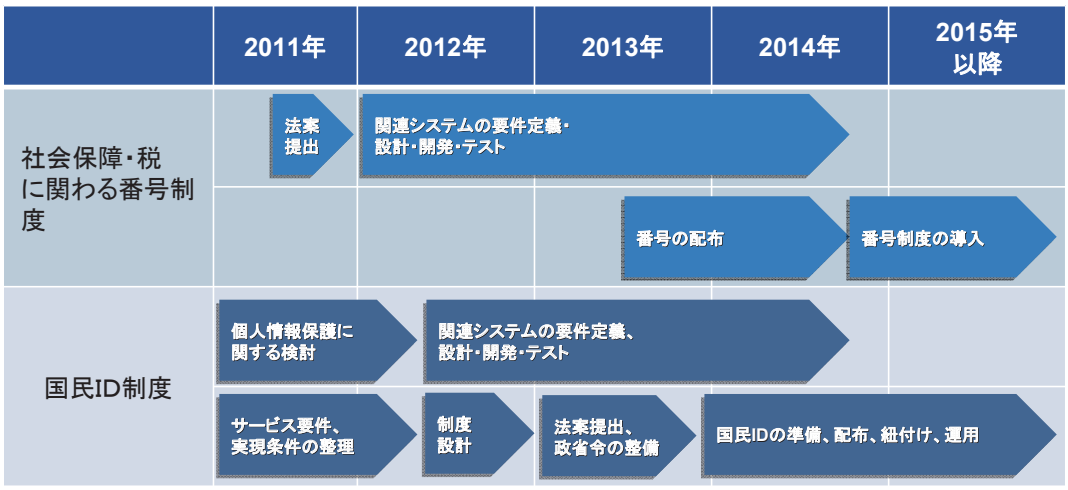
- 他組織との柔軟な連携が可能
- 特権IDの管理を適切に行う必要がある

■ 重要なセキュリティ技術

3．1　重要な情報セキュリティ技術の展望
1）ID管理　(2) 普及シナリオ　b-1) 国民IDの導入スケジュール

- 国民一人ひとりを特定する番号として、社会保障・税に関わる番号制度と、行政分野や民間分野の円滑な情報連携を行うための仕組みとなる国民ID制度のしくみが2014年度に構築・運用される予定である。
- 国民IDの普及に伴い、民間サービスにおいても、本人確認手段として国民IDを利用する需要が高まる。

番号制度の導入スケジュール



（出所：日経コンピュータ2010.12.22号「2014年、『共通番号』導入へシステム対応の議論が始まる」）

3．1 重要な情報セキュリティ技術の展望
1）ID管理 （2）普及シナリオ b-2）国民IDに内在するリスク

- ネットワークサービス（特に決済が関わるもの）における本人確認に国民IDを使用する場合、大量流出や盗用、犯罪への悪用が頻発する可能性がある。
- 米国では、個人情報の盗難件数は、2005年の157件が2010年には662件まで増加、被害に遭った情報数は2009年には2億件を超えている（下表参照）。
- 韓国では、近年、住民登録番号の大量流出事件が頻発、二次被害も発生し、社会問題化した（下表参照）。
- 韓国の住民登録番号は変更困難なため、一度流出するといつまでも被害を止められない点も深刻である。
- また、我が国の国民IDは民間利用も想定されるが、それによって個人の情報の名寄せが容易になり、プライバシー侵害につながる可能性も指摘されている。

米国における個人情報の盗難と被害にあった情報の件数（2005～2010年）

	2005年	2006年	2007年	2008年	2009年	2010年
盗難件数	157	321	446	657	498	662
被害に遭った情報数(推定)	66,853,201	19,137,844	12,771,724	35,619,255	222,477,043	16,167,542

（出所：Identity Theft Resource Center: “Data Breaches in 2005 - 2010”）

住民登録番号の漏洩事例（韓国）

09年9月　大学など教育機関から住民登録番号13,367件が漏洩
08年4月　ハナロテレコムから600万件の個人情報が漏洩
08年3月　LGテレコムから370件の顧客情報が漏洩
08年2月　AUCTIONハッキングで1,081万人分の会員情報が漏洩
（住所・住民登録番号・電話番号・銀行口座等）
07年9月　国民健康保険公団から72万件の個人情報漏洩
07年4月　韓国産業評価技術院から住民登録番号297件が漏洩

住民登録番号漏洩に伴う二次被害事例（韓国）

09年4月　盗んだ個人情報を利用してKT（Korea Telecom）代理店からWiMax通信サービス加入
08年1月　インターネット求人業者が学生バイトの信用情報を盗用し、数千万ウォンを銀行から借り出し
06年2月　他人の住民登録番号を盗用し、1,200万人のゲームIDを生成
その他　個人情報盗用で保険加入、携帯電話の加入などの事例

（出所：KISA資料）

3．1 重要な情報セキュリティ技術の展望
1）ID管理 （2）普及シナリオ b-2）国民IDに内在するリスク （参考）個人情報・プライバシーの定義

- 個人情報・プライバシー保護の流れは、1995年のEUデータ保護指令の発行が大きな契機となった。特に、個人データの第三国への移転禁止条項（25条）に対応するため、米国はセーフハーバー協定での対応を、日本は個人情報保護法の法制化を選択した。
- ただし、日本は、EUからは「個人の私生活に関わる個人データ及び基本権について十分なレベルの保護を提供している国であるとはまだ考えられていない。」とコメントされており*1、現在も国としては個人データの移転先として認められていない。

*1) EUと日本におけるプライバシー・個人情報保護会議より、Hana Pechackova氏の発言；「国際移転における企業の個人データ保護者措置調査報告書」(2010/3)より引用

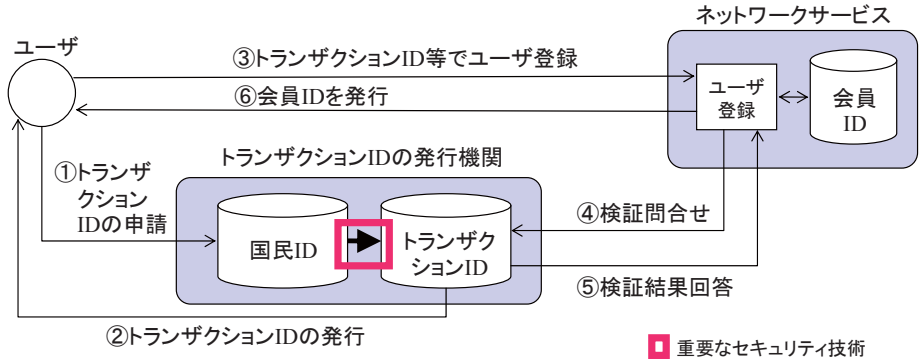
日米欧における個人情報・プライバシーの定義*2

地域	個人情報等の定義	定義元
米国*3	・氏名 ・Social Security Number (SSN) ・運転免許証番号 ・医療記録 ・金融記録/クレジットカード/デビットカード	Identity Theft Resource Centerが収集している個人情報の盗難と被害情報件数の定義より
欧州	身元が特定された、または身元の特定が可能な自然人（すなわち、企業やそれに準ずる団体と対比しての個人）に関するすべての情報。身元の特定が可能な人とは、特に身元確認番号（IDナンバー）の参照によって、またはその人の肉体的、生理的、精神的、経済的、文化的もしくは社会的な特徴によって、直接的または間接的に特定することができる者を意味する。	EU データ保護指令(1995/10) 2条より
日本	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）	「個人情報の保護に関する法律」（2005/04完全施行） 2条1項より

*2)米国や日本は個人を特定するための情報（見せてもよい情報）であり、欧州は個人に紐づいている情報（見せるべきではない情報）であって、本表が必ずしも同じ対象を比較しているわけではない点について留意する必要がある。
*3) 米国では、民間企業や法廷による個人情報の取り扱いについて広範に規定した法律が存在しないため、ここではITRCの統計情報の対象を採り上げた。なお、米国内で公的に個人のアイデンティティを証明する必要がある場合、連邦政府発行の社会保障番号（SSN）、州政府発行の運転免許証または身分証明証カード等がIDとして用いられることが多いとされる。

3. 1 重要な情報セキュリティ技術の展望
1)ID管理 (2) 普及シナリオ b-3) 国民IDにおいて望まれるID管理技術の在り方

- 国民IDに内在するリスクを軽減するため、たとえばネットワーク上での本人確認手段に国民IDそのものではなくトランザクションIDを用いるモデルを適用する方法が考えられる。
- 下図のモデルでは、ユーザは、必要に応じてトランザクションIDを申請し、発行されたトランザクションIDを使ってネットワーク上のサービスのユーザ登録を行う。サービス事業者はトランザクションIDの真正性について発行機関に問い合わせ、その結果をもとに、ユーザに会員IDを発行する。この場合、ユーザは、自身の国民IDをサービス事業者に知られることなく、サービスの利用登録が可能になる。
- また、ユーザがトランザクションIDを盗用されたり、名寄せによる特定がなされた場合には、新たなトランザクションIDを申請することで、被害影響を小規模にとどめることができる。
- トランザクションIDを利用する場合、トランザクションIDから国民IDを推測されないことと、それらの対応表を厳重に保護することが重要であり、たとえばトークナイゼーションやダイナミックID等の技術が効果的である。



トランザクションIDを利用するモデル

3. 1 重要な情報セキュリティ技術の展望
1)ID管理 (3)普及に向けた課題

a) クラウドコンピューティング

- ID管理のソリューションやサービスが充実し、導入コストや管理の負担がこなれないと、企業が連携・統合化に踏み切れない可能性もある。
- クラウド事業者側が提供するID管理手法(認証、認可、連携等)が標準的でない場合、取引先や委託先との連携が困難になる。
- 業務フローによっては多数の事業者が管理するユーザIDを統合的に利用することを前提として、適切なID管理の体系を設計する必要がある。

b) 国民ID

- トランザクションIDの発行機関が、国民IDとトランザクションIDの対応表等を安全に管理することが大前提となる。発行機関を増やすと漏洩のリスクが高まるが、発行業務の負荷が集中すると実務が回らなくなる危険性もある。
- 韓国では、1968年に本格導入された住民登録番号制度を背景に、国が一元管理する住民登録番号をネット上でも本人確認手段として利用することが一般的である。一方、日本では、民間サービスが国民ID抜きで発展してきた経緯があるため、韓国のように本人確認手段として国民ID(またはトランザクションID)を利用するニーズが高まらない可能性がある。また、発行機関がIDの真正性検証に対応するコストを、誰がどうやって負担するかという問題*について、社会的な合意が必要である。
- なお、国民IDを利用して本人認証を簡略化したオンライン決済や少額貸付等のサービスが登場すると、ニーズが顕在化する可能性もある。

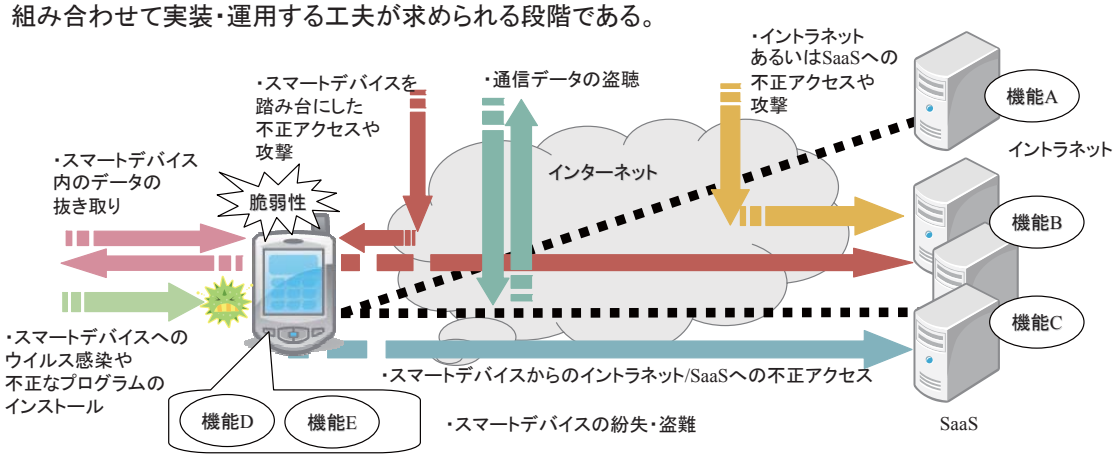
*) 韓国では、真正性検証を要求する事業者が負担する仕組みを採用している。

3．1　重要な情報セキュリティ技術の展望
2）組込みセキュリティ　(1) 開発課題　(a)スマートデバイス

■組込みセキュリティ（組込みソフトウェアに関するセキュリティ）は、「スマートデバイス」と「スマートグリッド（スマートメータ）」のそれぞれの領域において重要な役割を担う。

■スマートデバイスの領域では、ネットワークセキュリティ上の脅威に対するスマートデバイス上での技術的対策とスマートデバイスが含まれるシステムにおけるモバイル機器の技術的管理方策が求められる。

■セキュリティ面においては、必要な基本技術は既に実用化されており、要件を満たすよう適切に技術を組み合わせて実装・運用する工夫が求められる段階である。



スマートデバイスにおけるセキュリティリスク

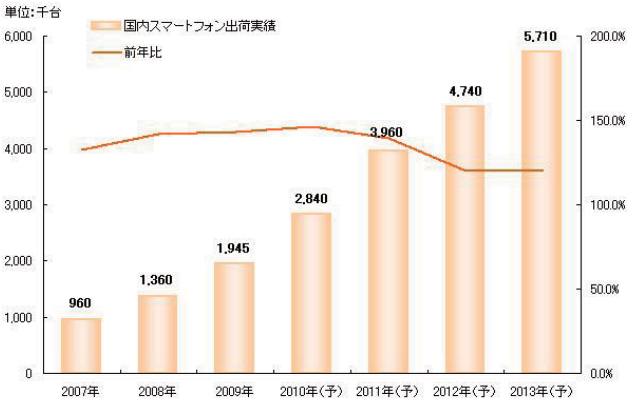
（講演資料 http://www.azsa.or.jp/b_info/event/event101008_2.html を基にMRIが作成）

3．1　重要な情報セキュリティ技術の展望
2）組込みセキュリティ　2) 普及シナリオ　(a)スマートデバイス

■業務用、パーソナル用の両面からスマートデバイスの需要が高まる傾向は今後さらに加速する。

■ここではスマートデバイスとして、スマートフォン、タブレットPC、電子書籍リーダ、MID(Mobile Internet Device。スマートフォン機能を持ち、ポケットサイズ、ディスプレイサイズ3.5インチ以上、フル・ブラウザを搭載するようなモバイル機器）等を含めて考える。

■スマートデバイスにおいて今後改善が必要な課題としては、基地局との継続的通信が必要なアプリケーションの増加を踏まえ、24時間以上の使用時間を満たすバッテリー寿命と常時基地局と通信可能な機能が必要だが、アプリケーションおよびOSにより消費される電力に比べると現在のバッテリー容量が不足しがちである点が挙げられる。



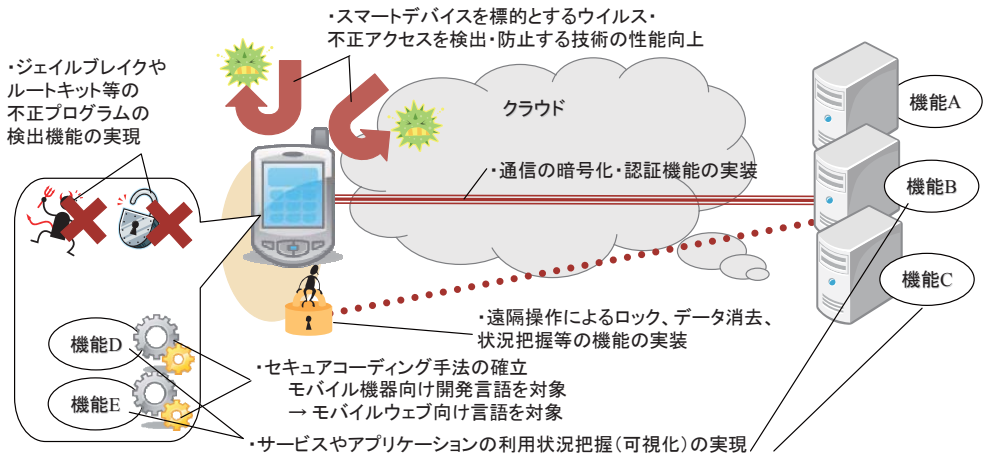
国内市場スマートフォン市場規模推移

（[http://www.yanoict.com/yzreport/110 から抜粋）

（参考）
[1] 矢野経済研究所、“スマートフォン市場に関する調査結果 2010 レポートサマリー” http://www.yanoict.com/yzreport/110

3．1　重要な情報セキュリティ技術の展望
2)組込みセキュリティ（2）普及シナリオ（a)スマートデバイス　セキュリティ技術進展の方向性

- スマートデバイスが、クラウド上の大容量ストレージやSaaSアプリケーションと組み合わせられ、モバイルPCに変わる端末機器として活用の範囲を大きく広げる。普及に伴い、スマートデバイスを標的とする脅威や安全上の懸念が増大、その特性に応じたセキュリティ対策が不可欠となる。
- OSのセキュリティ機能の利用、セキュアなアプリケーションの開発、ネットワークへの制約といった手法の組み合わせでセキュリティ対策が進展すると考えられる。
- スマートデバイスのOS・ミドルウェア・主要アプリケーションの基本機能としてセキュリティ機能を実装し、問題となるアプリケーションの仮想環境上への封じ込めが進めば、解決すべき課題が（ウェブ）アプリケーションのセキュリティに限定されていく可能性がある。

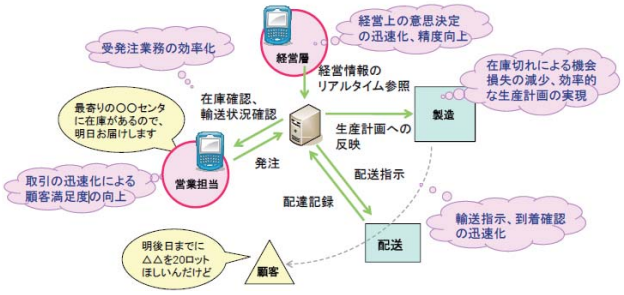


スマートデバイスにおけるセキュリティ技術の進展の方向性　（三菱総合研究所が作成）

3．1　重要な情報セキュリティ技術の展望
2)組込みセキュリティ（2）普及シナリオ（a)スマートデバイス　スマートデバイスの業務導入

- スマートフォンを業務に導入する際の目的としては、生産性の向上（業務プロセスの遅延解消）、コスト削減（通信や移動に伴うコストの削減）、顧客満足度の向上（リアルタイムの情報提供）などが挙げられる。導入目的に応じて適切なセキュリティ対策を取りセキュリティ・リスクを抑えることが重視される。[1]

- クラウド（SaaS）とスマートデバイスを組み合わせた業務システムが活用され始めている。中小企業や比較的小規模な店舗を主な対象に、見やすいディスプレイを備えたスマートデバイスと、SaaSで提供されるサービスを組み合わせたPOSシステムなどが既に構築され提供されている。[2] オフィスや店舗にサーバ、PC、ネットワーク機器等を設置しない利点がある。



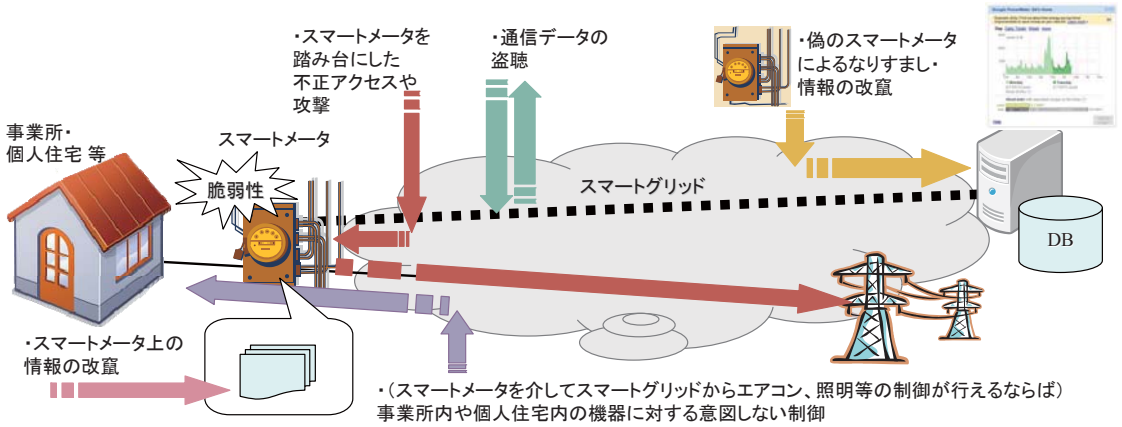
スマートフォンの特性を活かした業務利用の例
（講演資料 http://www.azsa.or.jp/b_info/event/event101008_2.html より抜粋）

スマートデバイスとクラウドを活用したPOSシステム
（ http://ubiregi.com/ および http://cotoha.jp/2010/08/ubiregi.html より抜粋）

（参考）
[1] “スマートフォンの効果的導入とセキュリティ対策のポイント”
http://www.azsa.or.jp/b_info/event/event101008_2.html
[2] “ユビレジ” http://ubiregi.com/

3．1　重要な情報セキュリティ技術の展望
2）組込みセキュリティ　(1) 開発課題　(b)スマートグリッド（スマートメータ）

- スマートグリッドの領域では、特に各家庭に設置されるスマートメータが注目されており、スマートグリッドに接続された機器の認証、取扱うデータや通信の保護等に関する技術的方策が求められる。
- 必要となる基本的技術は既に実用化されており、要件を満たすよう適切に技術を組み合わせて実装・運用する工夫が求められる段階である。

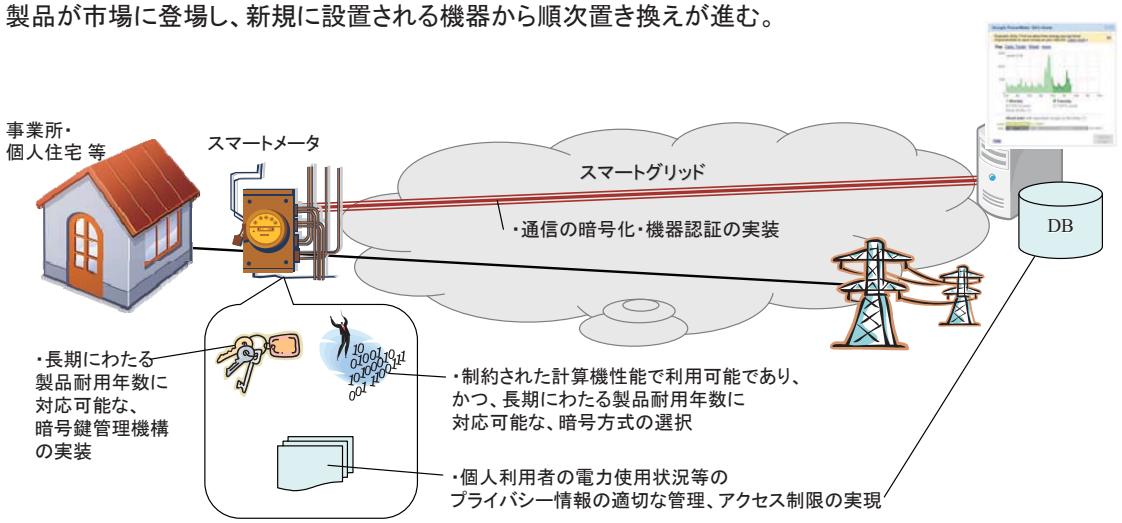


スマートメータにおけるセキュリティリスク

（三菱総合研究所が作成）

3．1　重要な情報セキュリティ技術の展望
2）組込みセキュリティ　(2) 普及シナリオ　(b)スマートグリッド（スマートメータ）

- 電力等関連業界が自主ガイドラインの策定や製品セキュリティ仕様の明示など、セキュリティ対策・プライバシー保護への積極的な姿勢を提示する。
- 制御システムのセキュリティへの懸念の高まりを受けて、基本的なセキュリティ対策が考慮・実装された製品が市場に登場し、新規に設置される機器から順次置き換えが進む。



スマートメータにおけるセキュリティ技術の進展の方向性

（三菱総合研究所が作成）

3．1 重要な情報セキュリティ技術の展望
2）組込みセキュリティ （2）普及シナリオ （b)スマートグリッド（スマートメータ） 国内電力各社の対応

■ 日本では、一般家庭や小規模店舗等においては機械式のメータが主であり、スマートメータについては実証実験が取り組まれているところである。[1]

電力会社	スマートメータへの対応の状況
北海道電力	2011年度から道央600戸を対象に実証実験の予定。メータの仕様については検討中。
東北電力	2010年度下期から2000戸を対象に実証実験（2012年度末まで）。30分単位での計量・記録。双方向通信や遠隔操作による開閉、停電の検知なども可能。
東京電力	2010年10月から東京都で9万台で実証実験（2年間の予定）。インターネットで利用状況を確認可能。電力利用制御は行わない。東芝、東光電気と3社共同で計器事業の新会社を設立。
中部電力	2011年4月から1500戸を対象に実証実験。各家庭に1時間毎の利用状況をインターネット配信。[2]
関西電力	2008年から。2010年3月末までに40万台を設置済。希望する利用者に使用量、料金等についてのインターネット情報配信を開始している。
九州電力	2009年11月より実証実験を開始。2009年度までに2万台を設置。関西電力と同形式のメータを採用。

国内電力会社のスマートメータ
（左：東京電力、右；関西電力）

＜参考＞
[1] 経済産業省スマートメーター制度検討会第1回資料、“スマートメーターをめぐる現状と課題について”
http://www.meti.go.jp/committee/materials2/downloadfiles/g100526a04j.pdf
[2] http://www.nikkan.co.jp/toku/smartglid/sg0531-15n-49ps.html

3．1 重要な情報セキュリティ技術の展望
2）組込みセキュリティ （3）普及に向けた課題

（a） スマートデバイス

- 開発者のセキュリティ実装に関する知識・技術を底上げし、脆弱性の作り込みを抑制する必要がある。
- アプリケーションの脆弱性については、修正プログラムをインターネット配信し自動修正するフレームワークが配布者より提供されている。脆弱性対策の必要性の認知、対策費用の負担、問題箇所の告知等についてはアプリケーションの製作者、配布者、利用者等による議論と適正化が望まれる。
- 特に企業での利用に際しては、利用者の利便性を損なわずに認証機能・アクセス制御機能を強化するようなアプリケーション開発手法が求められる。
- 企業等における利用者サイドでは、導入される新たなデバイス、新たな実行環境（クラウド）、新たな機能に対応するために、これらを的確に把握し、セキュリティポリシーに従って構成管理を行う手法やモニタリングを行う機能が必要になる。（自動的にアプリケーションバージョン更新されてしまう問題、アプリケーションに情報を無断で吸い上げられてしまう問題 等）

（b） スマートグリッド（スマートメータ）

- スマートメータについては導入が急がれる一方で、長期間にわたり利用し続ける製品であり、低価格化要請の圧力もある。セキュリティ・プライバシー保護に関する技術面・制度面の検討を迅速に深め、効率的で長期間の使用に耐えうる効果的なセキュリティ実装を行う必要がある。
- プライバシー情報および保護については今後社会的な関心が高まりうる。これらに関する要求仕様を明確化し、標準的なソリューションを確立することが肝要である。

3．2 まとめ

■ 今後のICT領域で重要となるID管理、組込みセキュリティ技術の開発課題、普及シナリオ、普及に向けた課題は以下のように整理でき、JEITA会員企業にとってま、普及シナリオに沿った課題解決によって、新たなビジネス展開が可能となると考えられる。

	1) ID管理	2) 組込みセキュリティ	
		スマートデバイス	スマートグリッド
開発課題	・複数団体による標準化・実用化の動きを、横断的組織が相互運用性を高めながら標準技術の普及を目指している。求められる機能は実現可能。	・ネットワークセキュリティ上の脅威に対するデバイスの技術的対策とシステムの管理方策が要求事項。	・必要となる基本的技術は既に実用化。実装・運用する工夫が求められる段階。
普及シナリオ	・クラウドコンピューティングの本格的普及による組織内外における資源共有を実現するID管理技術が要求される。 ・国民IDでは、様々なサービス提供時の本人確認の手段としてID管理技術が要求される。	・業務用、パーソナル用の両面からデバイスの需要が加速。デバイスの普及に伴い、脅威や安全上の懸念が増大し、セキュリティ対策が不可欠となる。	・電力等関連業界がセキュリティに積極的な姿勢を提示する。 ・制御システムのセキュリティへの懸念の高まりを受けて、対策済みの機器に順次置き換えが進む。
普及に向けた課題	クラウド: ・企業連合・連携時のID管理ソリューション導入コストや管理負担の解決。 ・ID管理手法（認証、認可、連携等）の標準の実現。 ・ユーザIDの統合的な利用を前提とした適切なID管理体系の設計。 国民ID: ・発行機関等による国民IDとトランザクションIDの対応表等の安全な管理。 ・本人確認手段としての国民ID/トランザクションIDの利用ニーズの喚起。 ・国民IDを利用したサービスのニーズ喚起。 ・発行機関によるIDの真正性検証コスト負担に関する社会的合意の形成。	・開発者知識の底上げ等、脆弱性の作り込みの抑制。 ・脆弱性の自動修正フレームワークの実現。普及・対策実現のための、アプリケーション開発者、配布者、利用者等による議論と適正化。 ・認証・アクセス制御機能強化のためのアプリケーション開発手法の実現。 ・新しい導入デバイス、実行環境、機能の状況の把握、セキュリティポリシーに従った構成管理手法やモニタリング機能の実現。	・低価格化要請の圧力への対応。セキュリティ・プライバシー保護に関する技術面・制度面の迅速な検討。効率的で長期間の使用に耐えうる効果的なセキュリティ実装の実現。 ・プライバシー保護や情報保護に対する社会的な関心を受けた要求仕様の明確化、標準的なソリューションの確立。

参考

参考1　韓国訪問調査
1) 概要

■クラウドコンピューティングはID管理や認証技術による情報管理が不可欠であり、韓国でもセキュリティベンダによる技術開発やソリューションの提供が進められている。
■韓国ではインターネットや携帯電話での決済において、PKIが積極的に活用されている。さらに、スマートフォンについては、ハッキングを検知するツールも導入されている。
■スマートフォンやスマートメータは、PCのような暗号化が性能的に困難なことを踏まえ、対策を考える必要がある。
■国民IDは横断的な認証基盤として利便性が高いが、決済での悪用が可能なことから、ハッカーに狙われ大量流出する事態が起きている。さらに、IDの変更が困難なため、一度流出すると被害を止められない問題も指摘されている。したがって、i-PINのようなトランザクションIDの技術を併用することが非常に重要である。なお、韓国では、まだi-PINの周知は十分でなく、国民IDからi-PINへの認識の転換が課題とされている。
■Samsungでは敷地内への出入時にITツールに対する厳格なチェックがなされていたが、その背景として、近年、韓国で産業技術の流出が社会問題化していることが挙げられる。
- ✓ ここ10年間（2000－2009）国内の産業技術の海外流出が225件摘発された。2003年6件から2004年には26件、2009年には43件まで増加。
- ✓ 分野別には、電子機器、情報通信、部門が全体の63%、その次が精密機械14.3%。
- ✓ 海外流出の原因は、職員に対する金銭的な買収が51.7%、許可なしの保管が22.7%。
- ✓ 韓国国家情報院（KCIA)は、2004年から5年間摘発された160件の被害額を253兆ウォン、2008年の被害額を80兆ウォンと推定。

参考1　韓国訪問調査
2) 訪問調査の目的

■今後発展が期待されるICT分野の有望領域において、サービスの実現や利活用を支える情報セキュリティ技術を整理する。

(1) 住民登録番号及びi-PINの課題と解決策の把握

韓国では、多くのサイトで住民登録番号の入力を義務付けていたが、大量流出や盗用、犯罪への悪用が社会問題化した。政府は住民登録番号による本人確認手続きを禁止する方針を示し、2006年以降、情報通信部と韓国情報保護振興院が開発したi-PIN（Internet Personal Identification Number）による本人確認手続きを導入したが、普及にはなお時間を要する。現状の課題と解決に向けた今後の取組を調査し、我が国の国民ID制度に内在する問題点を明らかにする。

(2) 重要な情報セキュリティ技術の開発・導入状況の把握

今後拡大が期待されるICT領域（クラウドコンピューティング、スマートグリッド等）を支える重要な情報セキュリティ技術について、同社または韓国における開発動向や普及に向けた展望・課題を明らかにする。

［主な検討テーマ］
- ・ID管理
- ・プライバシー保護
- ・組込みセキュリティ　等

参考1　韓国訪問調査
3）行程

■ 訪問時期：2010年11月4日(木) ～ 11月6日(土)

■ スケジュール：

	行　程	宿泊先
11/4 (木)	06:55 集合　羽田空港新国際ターミナル　3階 08:55 出発　東京/羽田（NH1161便） 11:25 到着　ソウル/金浦 → ホテルへ移動（タクシーで40分）、荷物を預ける 16:00 Ahnlab 18:00 SECUBASE 終了後、宿泊先へ	ホテルPJ
11/5 (金)	10:00 KISA 13:20 SoftForum 14:00 Samsung 終了後、宿泊先へ	ホテルPJ
11/6 (土)	16:35 出発　ソウル/金浦（NH1164便） 18:30 到着　東京/羽田	

■ 集合場所：羽田空港　新国際ターミナル　出航ゲート付近
http://www.ana.co.jp/int/airinfo/guide/hnd/index.html#03

■ 宿泊先：ホテルPJ　http://jap.hotelpj.co.kr/main/index.html
73-1 Inhyun-dong 2ga Jung-gu, Seoul　TEL 82-2-2280-7000

参考1　韓国訪問調査
4）訪問先

訪問先候補	概　要	住所	状況
AhnLab	• 1995年に設立された韓国のセキュリティ・ソリューション・プロバイダ最大手。 • ウイルス対策ソフトといったコンピュータソフトウェアや、オンライン・セキュリティ・ソリューション、ファイアーウォール、IPS、UTMといったネットワーク・セキュリティ装置、オンラインゲームや携帯端末ウェブ用のセキュリティソフトウェアを販売している。 • 韓国セキュリティ市場と全世界の販売業者約500社のうち、65%の市場シェアを持つ。	6th Fl,CCMM Bldg, 12 Yeouido-dong, Yeongdeungpo-gu, Seoul	11/4(木) 16:00-17:00
SECUBASE	• セSMSのソリューションやコンサルティング、プライバシー保護、DDoS対策、物理セキュリティ、BCM等の支援サービスを提供。 • 2005年創業。	4501 Ford Ave., Suite 360, Alexandria	11/4(木) 17:30-18:30
Korea Internet & Security Agency (KISA)	• インターネット上の事案対応支援、主要な情報通信インフラの脆弱性分析・評価、スパム対応、情報セキュリティ産業の支援、情報セキュリティ教育の促進等、国家レベルでの情報セキュリティ対策を総合的に推進する。	Dae Dong Building, Garak-dong 79-3, Songpa, Seoul,	11/5(金) 10:00-11:00
SoftForum	• 韓国でインターネットバンキング向けPKI分野でNo.1のシェアを有する。 • IMT - 2000のワイヤレスインターネットセキュリティソリューションや電子商取引トランザクションのソリューション等の市場をリードしている。	6~8F Mirae Bldg, 545-7 Dogok-dong, Kangnam-gu,Seoul	11/5(金) 13:00-14:00
Samsung Electronics Co. , LTD	• 世界最大手の電子機器メーカー。 • 2009年12月期の純利益　7300億円、営業利益率 8%、時価総額　約9兆円 • サムソン電子の主事業は液晶パネル、半導体、携帯電話、デジタルメディア • 今後は太陽電池、燃料電池、電気自動車、LED照明、バイオ・医療、映像診断機器、車載用半導体に注力すると予想される。	416, Maetan-3Dong, Yeongtong-Gu Suwon-City, Gyeonggi-Do, Korea 443-742	11/5（金） 15:30-17:00

参考1　韓国訪問調査
5) 結果概要 (1) 重要な情報セキュリティ技術の開発動向と展望①

組織名	対象技術の現状	技術開発課題	その他の課題
Ahnlab	• グローバル企業がクラウドサービスを始めたばかりで、セキュリティは未経験であり、最小段階というのが現状。様々なベンダがクラウドソフトウェアを考えている途中。 • サーバの仮想技術、仮想環境については、サーバの中のホストとゲストの間が繋がるところを暗号化し、OS全体を守る。	• クラウドのシステムを守るセキュリティソリューションはある。サーバ・ネット・PCのどのソリューションを選択するか。 • 当社のSOCによると、全体の約35%がDDoSの問題。二番目に多いのは、オンラインゲームやECのID・パスワードの窃盗。三番目はP2P系ソフトを悪用したID・パスワードの窃盗。攻撃は中国やラテンアメリカからのものが多い。	• 当社は、デジタルサイネージのコンソーシウム、スマートグリッドについてはチェジュ島での実証実験に参加、クラウドコンピューティングも政府がサポートしている研究会で検討している。 • 来年の頭にはクラウドコンピューティングとスマートグリッドに何が必要か、検討成果を公表する予定。
SECUBASE	• 様々な機器からログを取り出し、利用者企業の各層が求める情報をビジュアル化して見せる情報保護システムを開発した。個々の情報ではわからないが、他の情報との相互関係からみると問題の深刻さがわかる。 • データからデータへのリンクに基づくドリルダウン機能と相互関係を見られるようにした多次元分析機能が重要。	• クラウドセキュリティのテーマは多様。データ移行、ガバナンス、バックアップ、サービスを打ち切った時のサポートなどの問題等様々な分野のガイドラインを考えている。 • クラウドコンピューティングの場合、ログを管理・追跡すべきだが、追跡技術だけでなく、総合化して分析化し管理することが何より重要。	• 次世代ツールでは、スマートフォンや個人情報保護のモジュールを追加している。 • 技術だけでなく、全体的な状況を把握して対応する必要がある。それぞれの技術に基盤を置いた総合管理システムが必要。

参考1　韓国訪問調査
5) 結果概要 (1) 重要な情報セキュリティ技術の開発動向と展望②

組織名	対象技術の現状	技術開発課題	その他の課題
SoftForum	• クラウドコンピューティングで重要なのは認証。IDを通じて、クラウドコンピューティングをどうやって認証させるか。ID管理によりどうやって会社と外部の環境を繋げ同期化するか。社内のIDや機密情報を外部に流出させてはならない。 • 携帯で決済するため、ID・パスワードをPKIで強化している。電子証明書は全ての携帯に搭載されている。	• 当社の技術は、会社のIDを外部に出さなくても、ID以外の情報をやりとりして管理する。例えば、ID以外のニックネームなどの情報でログインできる。 • 銀行、カード会社、保険会社で当社が開発したPKIサービスを実行している。ハッキングフォンを検知するツール等も組み込んでいる。	• 当社はスマートグリッド分野の系列会社を有する。スマートメータは仕様の水準が低いので、改ざんが自由にできない。物理セキュリティとソフトのセキュリティを融合して暗号化するよう、力を入れている。
Samsung	• 複合機のセキュリティについては、IEEE Std 2600.1 TM-2009の共通仕様に対応している。 • セキュリティに対するインフラは韓国のほうが優れていることが多い。たとえば、ある金融機関で発行した証明書が他の金融機関でも使えるように、CA間の連携が機能している。逆に、ユーザ側の意識は韓国のほうが低い。	• 製品が初期の段階では、機能の充実が優先であり、セキュリティは後回しになる。基本的なセキュリティに対する要求に対応する程度。しかし、製品が成熟すると、より安全性が重要になるのではないか。 • 将来的にどのような技術を取り込むか、マイルストンは検討済。 • 多様なことを可能にするプラットフォームができあがると、ウイルスに弱くなっていくので、そこを補強していく必要がある。	• 管理者向けのサポートを充実させることも可能だが、セキュリティレベルを上げすぎると使えにくい。 • スマートデバイスは、PCのように暗号化することが性能的にできない点を補強する必要がある。一つの技術で解決するのではなく、複合的に安全にする。すると今度はプライバシーの問題が発生する。 • 今後、ネットワーク経由のプリンタの利用にi-PINを活用する要請がでてくるかもしれない。

参考1　韓国訪問調査
5) 結果概要(2) 住民登録番号及び i-PIN の開発経緯と今後の課題

組織名	i-PINの背景	i-PINの開発	i-PINの課題
KISA	• 韓国では、税務、金融、行政等様々な分野において住民登録番号（国民ID）で個人を識別している。番号は1人に1つで、一度決まったら変わらない。オンラインで共通に使えて便利だが、一度漏洩したら被害が永遠に続きかねない。 • 国民IDはハッカーの攻撃対象にされる。2008年2月、オークションサイトから1081万人の会員情報が漏洩。同年4月、ハナロテレコムから600万人の個人情報が漏洩。 • 盗んだIDで他人になりすましてネット上で銀行で借金したり、ゲームサイトでRMTでお金を得たり、携帯電話を契約し、不法に貸与してお金を稼ぐのに使われる。 • 銀行、ショッピングモールの情報漏洩事故について、被害者による集団訴訟も起きている。	• 2015年までに国民IDに代わるi-PINを普及させていく計画。 • ネット上で会員加入する時の本人確認にi-PINを使う。使うとEメールで連絡が来る。利用者がいつでも変更、中止することが可能。 • i-PINの発行組織は6つ。発行組織にはKISAが定期的に運営状況を点検し、政府が管理して、安全性を保証する。 • 1人が機関（6組織）毎に1つずつ発行してもらうことができる。いずれかのi-PINを発行してもらえば、他のどちらでも使える。 • 利用機関（ウェブサイト）は認証件数を発行機関に報告し、その費用を発行機関に支払う。 • 2010年の6月末で、i-PINを導入したことがあるウェブサイトは4896件、発行件数は230万件。	• 2005年当初は自発的に導入する形にしていたが、2009年から1日あたりのアクセスが多い約1000サイトにi-PIN導入を義務化（i-PINのみではなく国民IDも併用可）した。手数料の最小限化、モジュールの無料提供など「アメ」の対策も実施。 • オンライン利用が多い税務や金融分野への拡大が必要。 • 技術的な問題はほぼ解決しているが、国民IDからi-PINへ、という認識の転換が大きな問題。 • 2005年の時点では、組織内で使う本人確認の仕組みとして開発したが、これを6つの組織に拡大し、連携・連動させる作業が必要になった。それぞれの組織で本人確認の運用システムが異なるので、その連携をとる標準化作業はまだ残っている。
Ahnlab	• 住民登録番号により様々な問題が発生した。住民登録番号があれば様々な事ができるので、中国のハッカーは韓国の住民登録番号をターゲットとしている。	• 秘密の暗号処理によりi-PINを住民登録番号とマッチングさせる。住民登録番号はトラブルがあっても一生変更できないが、i-PINはコピーされた場合には変更することができる。	• 政府がi-PINに取り組んでいるが、サーバの中にある番号をうまく守れるか。 • 技術的な問題より運用の問題を懸念している。発行機関として小規模の組織が管理しているのでセキュリティが弱い。法律を適切に整備する必要がある。

参考1　韓国訪問調査
6. ヒアリングメモ　(1) Ahnlab

・Ahnlabは韓国国内のセキュリティ会社でNo.1。MKTシェア60%以上。世界的にはまだ名前が知られていない。韓国では去年、大規模なDDoS攻撃の事件があったが、何をどう守るか突き詰めたい。時間は短いが、本格的にみなさんの会社のセキュリティ問題や、個人情報の何を注意しなければならないか、アイデアをこのミーティングでもらいたい。

・1985年　V3開発
　1995年　設立
　2001年　上場　20年間あるので結構歴史は長い。
　2010年　ここまで毎年2倍程度のペースで成長している。
　　現在、社員は600人。半分はエンジニア。当社は技術を志向する研究所である。ミッションは安全なインターネット世界を作ること。セキュリティ技術に集中。売上65百万ドル、利益1千万ドル。AhnlabはSamsungよりは小さいが、韓国の中で成長を伸ばしていく最高の会社（best employee in Korea）に選ばれている。東京にも法人がある。世界に進出しようとしている途中。ユーザが選ぶ理由は、ITセキュリティ会社として歴史が長く知識が多いから。AVだけでなく、生体認証等も扱う。社内で技術開発していることがAhnlabの強み。韓国のインターネット環境は高速。韓国は新しいものがあるとすぐ使う文化があるので、セキュリティに対応するニーズもあると思う。ビジネスポートフォリオはB to C、B to B。トータルセキュリティで開発し、サービスを提供している。最近取り組んでいるのはクラウドコンピューティングセキュリティサービス。体制を作ることはリソースも必要。日本法人は秋葉原にある。32名。2002年に設置。

・グローバル企業がクラウドサービスを始めたばかりで、セキュリティは未経験であり、最小段階というのが現状。様々なベンダがクラウドソフトウェアを考えている途中。マイクロソフトはサーバの認証・権限管理をどうするか問題にしている。当社の顧客もクラウドシステムをどう使うか考えているところ。アクセスをどう守るかなど、セキュリティが重要。顧客の声を聞きながらやる。

・ID管理、アクセス認証、ID・パスワード、生体認証等の技術もある。情報の重要性によって、何を選択するかが違ってくる。

・クラウドのシステムを守るセキュリティソリューションはある。サーバ・ネット・PCのどのソリューションを選択するか。
・サーバの中のホストとゲストの間が繋がるところを暗号化する。OS全体を守るセキュリティ。

・国のSOC（Security Operation Center）はその国の主要な企業や政府を見ているが、Ahnlabでは銀行など民間企業の顧客のネットワークをリアルタイムでモニタリングしている。全体の約35%がDDoSの問題。二番目に多いのは、オンラインゲームやeコマースのID・パスワードの窃盗。三番目はWinny等、P2P系ソフトを悪用したID・パスワードの窃盗。攻撃は中国やラテンアメリカからのものが多い。365日24時間監視して、顧客に連絡したり、警察に連絡することもある。

・DMZの中の様々なサーバが対象である。

・住民登録番号により様々な問題が発生した。そこで今は、i-PINなど別の番号でインターネットシステムを使うことを目指している。住民登録番号は様々な事ができるので、中国のハッカーは韓国の住民登録番号をターゲットとしている。

・秘密の暗号処理によりi-PINを住民登録番号とマッチングさせる。住民登録番号はトラブルがあっても一生変更できないが、i-PINはコピーされた場合には変更することができる。

・韓国政府がi-PINに取り組んでいるが、サーバの中にある番号をうまく守れるか、企業側はそれを不安に思っている。また、社員のID管理も心配。

・まだトライアルの段階。リサーチすれば、日本でもっと良いものができるかも知れない。

・技術的な問題より運用の問題を懸念している。発行機関として小規模の組織が管理しているのでセキュリティが弱い。法律を適切に整備する必要がある。

・Ahnlabはデジタルサイネージのコンソーシウムに加入している。スマートグリッドについては、何のセキュリティ方式が必要か、チェジュ島での実証実験に参加しながら検討を進めている。クラウドコンピューティングも、政府がサポートしている研究会があり、そこで検討している。来年の頭にはクラウドコンピューティングとスマートグリッドに何が必要か、検討成果が公表される予定。そのタイミングで、Ahnlabとして何ができるか、もっとお話ができると思う。

参考1 韓国訪問調査
6. ヒアリングメモ (2) SECUBASE①

・SECUBASEは2007年設立。前身は2002年設立のコンサルティング会社。セキュリティ、プライバシー、ITセキュリティコンサルティングサービスを。政府や研究機関、Samsungなど韓国の大手企業に提供している。セキュリティサービス技術の研究開発の機関があり、システムネットワーク技術部門の専門家がいる。リスク管理システムサービスを提供しており、セキュリティサーバ、e-mailサーバ、メインサーバなど全ての機器の全てのログを集め、ログタイプの分析・管理をしている。ISOなど国際標準に基づくコンサルティング方法でセキュリティサービスやワイヤレスソフトウェア、モバイルセキュリティなども提供している。主な顧客は韓国国内で1番のインターネット会社、政府機関、通信企業など。

・このシステム開発の背景には、個人情報保護の機器や会社の資源を統合化し、ビジュアル化するニーズがあった。一番下にある様々な機器からログを取り出し、社長・中間管理職・実務管理者それぞれが求める情報をビジュアル化して見せるために、この情報保護システムを開発した。会社が持っている資産を全体的に把握していないと対応ができない。ログと資源を統合化して、初めてセキュリティシステム政策が可能になる。重要な機能は2つある。一つはドリルダウン機能。いろんなデータにリンクされているデータを見ることができる。もう一つは多次元分析機能。相互関係を見られるようにした。

・エンジンは異なるもの。ニーズによってどちらにするか対応している。（アークサイトもキャップストーンと同じようなことができると思うが、そのエンジンを使ったソリューションなのか。もしくは全く独自で開発されたものなのか、という日本側の問いに対して。）

・その選択のポイントは、金額の希望、様々なものを一緒に見せる必要があるかどうかによる。

・個人情報などの細かいニーズがあったりなかったりするので、都度対応している。KISAのモニタリングシステムは民間企業のネットワークを対象としていて、韓国で一番大きい。

・単位毎に警報を発令する。連携データの中でも値を見て把握する。小さいスキャン現象だけを見るとたいした事ではないが、他のシステムとの連携からみると大きな問題になるので、それで状況を判断する。

・主に政府関連の色々なコンサルティングをやっているが、代表的なのはクラウドコンピューティング、スマートグリッド。韓国電力のプロジェクトもやっている。プライバシー保護関連では、政府の個人情報プロジェクトなどをやっているので、その辺の事のお話ができると思う。クラウドコンピューティングでは、韓国放送通信委員会からの依頼で、セキュリティガイドラインの策定を請け負った。韓国の標準を作る作業。たとえばデータ移行（GoogleからYahoo!にどうデータを持っていくかなど）の課題について、どういう標準案が必要か、共通のコンポネントはどういうものかについて検討した。クラウドコンピューティングはMS等の販売側が主導するマーケットと考えている。世界のコンピュータユーザの40%がGoogleを利用している。韓国が標準を作った場合、Googleなどの大手企業は守らないが、韓国企業だけが守る。グローバル化する中で、最初の段階では韓国企業を保護することになるが、外国企業が韓国に入ってくる際の参入障壁になるので、そこをどうするか考えている。クラウドコンピューティングのセキュリティ技術のガイドラインに関して、韓国政府の戦略は確定していない。従来、韓国政府は国内産業を優先する規制を作って産業発展をサポートする役割があり、韓国内で発展したマーケットもあるが、グローバル化をめざす韓国企業にとってはこの規制が逆に障害になっている。

セキュリティマネジメントが重要。データを総合化して、事件が発生する可能性を評価するノウハウを持っている。スマートグリッドでは、プリオートメーション・ネットワークはセキュリティ技術に対応できなかったが、鉄鋼会社などがプリオートメーション・ネットワークに興味を持っているので、チェジュ島での実証実験で対応する取り組みを行っている。プライバシー分野では、個人情報と関連したプロジェクトをやっているが、その内容を用いて韓国行政安全部がシステムを運用することになっている。個別のセキュリティ技術が高い場合、迂回攻撃をしてくるので、攻撃パターンを把握するためにログを把握し、それに基づいた防衛システムを作る必要がある。したがって、そのような観点からセキュリティマネジメントに力を入れている。分析プラットフォームなど総合化して、それに対応するソリューションを通じてセキュリティ問題を解決するという戦略をとっている。

参考1 韓国訪問調査
6. ヒアリングメモ (2)SECUBASE②

・クラウドコンピューティングの国際標準は、欧ENISAや米CSAで議論されている。国際標準はISOのワーキンググループの中で議論が進んでいるが、ターミノロジーを議論するレベルにとどまっている。韓国では、政府が主導権を持って標準案を作ってISOのワーキンググループへ韓国案を持ち込むという戦略でやっている。

・クラウドセキュリティ関連のテーマは多様。データ移行、ガバナンス、バックアップ、サービスを打ち切った時のサポートなどの問題で、様々な分野のガイドラインを考えている。

・キャップストーンの次の世代のシステムやパッケージを見せたら次に何を考えているかわかると思う。キャップストーンの中に、スマートフォンや個人情報保護のモジュールが入っている。たとえば、iphoneでの通話の直後に別の場所での通話があるとスマートフォンは、遠隔で複写している情報を得る形で対応できる。技術よりも管理が重要という姿勢でこのシステムを作った。このモジュールは、国が決めたPIMSのガイドラインに沿っているかどうか、韓国の情報通信網法に沿っているかどうかチェックする。また、各部局や個々人がガイドラインに沿って仕事しているか、誰が危険状態に陥っているか管理できるようになっている。国会の入口に入ってきた人が、同時に10階から入ってきたと感知したら、10階をブロックするような仕組。クラウドコンピューティングの場合、ログを管理・追跡しないといけないが、追跡技術だけでなく、総合化して分析化し管理することが何より重要と考えている。去年7月7日、韓国の政府機関や銀行はウイルスにやられて大きな問題になった。ウイルスに対応するシステムは存在したが、そのウイルスはシステムを認知して避けて攻撃するものだったので、やられてしまった。やはり技術だけでなく、全体的な状況を把握して対応する必要がある。それぞれの技術に基盤を置いた総合管理システムが必要。

・セキュリティは網羅的に把握しないと、全体を分析・対応できない側面がある。多様な経験と直観・感覚的な部分も必要。いかに教育するかについては、高麗大学大学院で教えたり、そこにはKCIや民間企業のセキュリティ担当も出入りしているので、情報交換や教育しあったりなどのシナジー効果があって、人材育成に繋がりレベルも維持できているのではないか。

参考1　韓国訪問調査
6. ヒアリングメモ　(3) KISA（Korea Internet & Security Agency）①

・PPT資料の中に、導入以前の状況、i-PINとは何か、利用範囲、従来の国民IDとi-PINとの転換システムについての説明がある。パンフレットは一般のユーザに配る資料として作成した。冊子は、業者が手続きやガイドラインである。i-PINは韓国の独自システムなので、英語や日本語の資料がない。
　韓国では、税務、金融、行政等、様々な分野において、住民登録番号で個人を識別しているので、国民IDとしての意味を持っている。1人に1つの番号が振り分けられ、一度決まった番号は永遠に変わらない。その番号を見ればどの人かが分かるようになっているので、韓国のウェブサイトは国民IDでユーザを識別する仕組みをとっている。
　オンラインで同じIDを使えるというメリットがある一方、漏洩した場合、変更がきかない、一度漏洩したら被害が永遠に続く可能性があるという大きい問題があった。
　3枚目の上スライドに、主な漏洩事件をまとめた。2008年2月のオークションのハッキングで、1081万人の会員情報が漏洩した。同年4月にはハナロテレコムから600万人の個人情報が漏れるという事件が起きた。ウェブサイトが国民IDで本人確認をするので、ハッカーがそのデータを狙った。国民IDはハッカーの攻撃対象になりやすい。
　日本では、ハッカーのターゲットになるのは何か。

・3枚目上は、国民IDが漏れた事故、下は漏れたIDで何をしたか、例えば、携帯電話を開通した、銀行からお金を借りた、といった被害をまとめたもの。

・銀行の貸し出しのしくみが日本と韓国で異なる。韓国ではオンラインで簡単にお金を借りることができる。銀行のホームページに会員加入していると、銀行側は会員の様々な情報を持っているので、住民番号、会社、携帯番号等を入力したらその場でお金を貸してくれる。つまり、他人の個人情報が分かれば銀行でお金を借りることもできる。また、オンラインゲームサイトでは、個人情報が分かれば、ゲームマネーやマイレージを使えるので、それで何かを買ったり、現金化するのも可能になる。そのため、事件が起こる。

・他人の個人番号で他人になりすまして、携帯電話をたくさん作り、不法に使いたい人に高い金で貸したり、不法滞在している外国人に貸し出す。使った後に料金は払わずにどこかで捨ててしまう。銀行の貸し出しサービスは、個人レベルではそれほど高額は借りられないが、アルバイトを集めて、彼らの名前を借りて、たくさんお金を借りる悪徳商法がある。オンラインゲームでも、なりすましでゲームアイテムをたくさん集めて、それをマーケットで売って現金化する。

・個人の被害だけではなくて、銀行、ショッピングモールで起きた情報漏洩で起こった事故に対して、被害者による集団訴訟が60件余り起きており、19万人が関係する。補償金額や請求金額は2100億ウォン程度なので、企業にとってもこの問題は非常に負担になっている。個人にも企業にも被害が発生するため、政府はこういう被害を防ぐ対策を何とか打たなければいけない。オンラインでの規制もなく、様々な分野・様々な形で国民IDが使われているので、その代替手段としてIDが必要ということになった。その結果、新しい仕組みを開発してできたのがi-PINである。6枚目の上図は、2009年3月に放送通信委員会が作ったもの。2015年までに国民IDに代わるi-PINを普及させていく計画を打ち出した。

・i-PINとはID・パスワードである。国民IDの代わりに、i-PINを使ってオンライン上で本人確認をする。特徴は、使う時に必ずEメールで使用のお知らせが来ること。利用者がいつでも変更、中止することが可能なので、被害を止めることがいつでも可能な仕組みであること。

・7枚目の下表、2010年の6月末の普及状況は、i-PINを導入したことがあるウェブサイトは4896件、発行した件数は230万件程度。
　ウェブサイトに会員加入する時にi-PINを使う。既にi-PINを持っている人はそのi-PINの番号を入れれば、その認証情報が提供されるので、企業はそれを基に本人確認をする。I-PINを持っていない方は、その場で加入してi-PINを発行してもらい、それを打ち込んで本人確認をする。
　（パンフレット）まずは、名前と住民登録番号＝国民IDを打ち込む。 1で名前と国民IDを打ち込み、2でそれが本人かどうかを携帯電話、公的個人認証で本人確認する。

・携帯、クレジットカード、公的認証を使うのは、この3つは発行してもらう時に必ず一度は窓口で本人確認するので、この3つの手段を使って本人確認をする。本人確認ができたら、i-PINのIDとパスワードが発行される。
　i-PINの発行組織は6つある。i-PINを使う以前はそれぞれのウェブサイトがユーザの国民IDを持っていたが、i-PINを使うとこれらの発行組織だけが国民IDを取り扱い、他は全部i-PINで流通するので、個人情報が守れるというメリットがある。

参考1　韓国訪問調査
6. ヒアリングメモ　(3) KISA（Korea Internet & Security Agency）②

・8枚目下の表に、ソウル信用評価情報、韓国情報認証、韓国信用情報、韓国信用評価情報、Korea Credit Bureau、行政安全部の6組織を示している。これら6組織に対してはKISAが毎年定期的に運営状況を点検し、政府が管理して、安全性を保証する。いずれの組織でもi-PINを発行してもらえば、他のどちらでも使える仕組みになっている。

・行政安全部が住民登録の管理業務をしているので、死亡届が出た人については、公共分野のi-PINを中止する。民間i-PINも行政安全部と連携ができているので、亡くなった方の番号はそれ以後使えなくなるような措置をとっている。
　ただし、i-PINは放送通信委員会、住民登録関連は行政安全部の担当業務であり、その間で連携してもいいのかどうかという議論は残っているのだが、基本的にそういう形でシステムを作っている。

・1人が機関（6組織）毎に1つずつi-PINを発行してもらうことができる。

・携帯電話番号を登録時の本人確認に使うのだとすると、携帯を複数持っている人は同じ機関に対して複数申告しても通ってしまうのではないかという危惧があるが、韓国では国民IDを入力するので、そういうことはできない。

・国民IDを発行する側に監査が入る。利用機関に対しては、発行する機関から、システム上の問題、脆弱性対策等を点検して、それをクリアすれば利用可能になる仕組みになっている。

・i-PINは、ショッピングモール等の会員になる時の本人確認に使うもの。オフラインで使っていた住民登録番号を、オンライン上でも引きずって使っていたが、i-PINはそれを代替する。あくまでも会員になってIDとパスワードをもらうために本人確認をするのが目的であって、それ以上の役割はない。

・決済の際には、PKIを活用する。例えば、金額が30万円以上だったら、PKIで認証しなければいけないことになっている。また、一般に、それぞれの銀行やカード会社が独自の認証の仕組みを持っている。

・国民IDをi-PINに変更する上で、一番の問題は、国民一人一人が国民IDに慣れているので、新しい本人確認の手段としてi-PINを認識するのに時間がかかること。

・公共分野では、例えば行政内部のシステムは全て国民IDでDB化されているので、電子政府サービス（G for C）のサイトでは、i-PINで会員登録をすると、KISAを経由してi-PINと連動する国民IDを提供する連携の仕組みを開発して、この11月から活用している。個人がネットでi-PIN番号を入力すると、そのデータがKISAに届いて、税務局や行政安全部に、i-PIN番号と一致する国民ID番号を転送する。

・KISAは政府の予算で活動する。i-PINに関しては、他に発行機関や利用機関（ウェブサイト）がある。利用機関は今月何件の認証があったか発行機関に報告し、認証手続費用を利用機関が発行機関に支払う。

・2005年からこの制度が始まった。当初は自発的に導入する形にしていたが、2009年からは、1日あたりのアクセスが多いサイト、ポータルは5万件以上、その他は1万件以上の場合はi-PIN制度を導入することを義務化する法律が始まった。およそ1000サイトが対象。新しい制度では、コストも伴うし、認証コストも払わなければならないので、民間からの反発がなかったわけではない。そういう反発を考えて、こちらとしては認証コスト、手数料を最小限化し、例えば毎月何十万ウォンに収まるようにする、モジュールを無料で提供するなど、「アメ」の対策も一緒にとってきた。

・義務化されているが、i-PINのみではなくて、基本的にi-PINでも国民IDでもOKという形になっている。

・オンライン利用が多いサービス、税務関係や金融分野への拡大が必要であり、それらの分野での拡大策を探っている。
　技術的な側面からいうと、大きな問題はほぼ解決している。技術的な問題よりは、認識の転換、国民IDからi-PINへ、という認識の転換を大きな問題として考えている。

・2005年の時点では、組織内で使う本人確認の仕組みとして作った。これを6つの組織に拡大し、連携・連動させる作業が必要になった。それぞれの組織で本人確認の運用システムが異なるので、その連携をとる標準化作業という課題は今でも残っている。

参考1 韓国訪問調査
6. ヒアリングメモ (4) SOFTFORUM

・DBサーバにアクセスするキーボードの入力ログをとるツールを提供。金融系、銀行・カード会社・保険・インターネットバンキング・公共機関と民間企業を担当。60-70%くらいの市場を担っている。softforum側の出席者は営業・マーケティング、セキュリティ技術担当者である。課題については韓国の製品で既に出来ており経験済みなので、何でも質問してもらえれば答えられると思う。

・クラウドコンピューティングで一番大事なのは認証である。インターネットで一番弱い所は認証。特にID管理は、認証のためのIDをどうやって管理するかの問題。そのIDを通じて、クラウドコンピューティングをどうやって認証させるかが重要な問題。コンサルタントが一番関心を持っているのは、企業がクラウドコンピューティングを通じて管理する部分にある。企業はIDを守りながらクラウドコンピューティングを利用出来るか。ID管理では、どうやって会社と外部の環境を繋げ同期化するか。ここで重要なのは、会社内のIDや機密情報を外部に流出させないことである。この問題を解決する方法を研究中で、そのためのソリューションも持っている。

・複数の業者のサービスを1つのIDで実施したり、企業間取引で安全にIDを活用するためのソリューションを提供するなどのサービスは、まだ紹介できる段階ではない。

・既存のID管理技術はホスト基盤の技術である。当社の製品の特徴は、会社のIDを外部に出さなくても、またもらわなくても、IDの管理ができる。そのためにはID以外の情報をやりとりする。例えば、ログイン時ID以外のニックネームなどの情報でログインできる。トークンではなく、他の情報。

・ID管理ソリューションを事業者側ではなくお客様側のシステムに設置する。

・スマートフォンは個人情報保護とインベデッドフォンシステムが必要。例えば、iphoneは、アップルが閉鎖的だがとても人気がある。そこには個人情報保護が含まれている。韓国では、リレーという技術を使って電子証明書をスマートフォンに入れている。韓国の金融機関ではスマートフォン向けの銀行ソフトウェアを開発して使っている。ハッキングされた電話では、サービスが実行できないように設定されている。

・韓国では、iphoneでクレジットカードの決済ならできる。

・ハッキングフォンを認知する技術。Jailbreakされたiphoneを検出し、決済ができないようにする。一般的に国内でバンキングができるようになり、ID・パスワードのしくみを電子証明書で強化している。ID・パスワードだけだと残額確認程度の機能しか使えないが、証明書があると振込等ができる。証明書を選択して証明書のパスワードを付与することによって、セキュリティデータが暗号化される。

・softforumはスマートフォンにおいて、銀行、カード会社、保険会社でsoftforumが開発したサービスを実行している。ハッキングされたiphoneを検出するようなツールもその中の一つ。金融機関だけでなく政府機関も、電子証明書を出すことでサービスのセキュリティを強化している。電子証明書はiphoneなど全部の携帯に入っている。

・国際標準化の可能性はあるが、まだそういう段階ではない。

・当社はスマートグリッド分野の系列会社を持っているが、スマートメータは仕様の水準が低いので、改ざんが自由にできない。当社は、物理セキュリティとソフトのセキュリティを融合して暗号化するよう、力を入れている。MS基盤だけではなく、Safari Browserやfirefox、Macintoshも全てカバーしている。

参考1 韓国訪問調査
6. ヒアリングメモ (5) Samsung社

・韓国では、人民登録番号もあり、調べればすべてわかってしまう。ほとんどプライバシーがない状態ではないか。

・セキュリティビジネスは、商売的に行き詰まっている印象。新たな脅威を探しているように見える。

・複合機のセキュリティについては、IEEE Std 2600.1 TM-2009の共通仕様に対応しているところ。複合機メーカーはいずれも同様ではないか。ログ監査まではしていない。

・顧客のニーズは紙を減らすというようなコスト削減で、セキュリティは評価されないので必要以上にはやらないが、今後もずっとそうだとはいえない。実際、Samsungでも、セキュリティ管理は非常に厳しくなっている。

・当社のセキュリティ環境構築は子会社のSamsung D.S.が担当しており、話せることは特にない。ハードディスクでの保存や、ネットワークを通ってデータをやりとりするところで暗号化する。

・離れた事業所で、自分の資料を印刷するというのはあるが、ネットワーク経由でプリンタとデータをやりとりし、離れた場所の人に、自分が印刷したものをとってもらい、それが自分の印刷物であることを証明するやり方は現実的に考えにくい。

・FAXでは、FAX番号を2回入れるなどの機能が出ているが、誤送信が圧倒的に多いということか。

・この会議についてどこまで話せるか、社内で議論になった。将来的にどのような技術を取り込むか、そのマイルストンは検討済だが、話せない。

・複合機のセキュリティを始めて1年目なのであまりわからない。セキュリティという意味では、ネットバンキングを参考にしたほうがよい。

・韓国のオンラインバンキングについて怖いのは、ActiveXをダウンロードさせるところ。悪い人が類似のサイトを作って、悪いActiveXをどんどん送ってくることも可能ではないか。

・スマートデバイスは、PCのように暗号化してやりとりすることが性能的にできない。そこを補強する必要があるのではないか。

・デバイスごとに証明書を持たせていく形になる。一個の技術が解決するのではなく、複合的に安全にする。ただし、そうすると今度はプライバシーの問題が発生する。

・国民IDを日本で構築するのであれば、いつでも変更可能であるようにすべき。 最後は本人確認が必要になる。

・最近、複合機は、だんだんマルチメディア化している。多様なことを可能にするプラットフォームができあがると、ウイルスに弱くなっていくので、そこを補強していく必要がある。

・管理者向けのサポートを充実させる。やろうと思えば、ログインにしたあとのタイピングのログを管理者に提供することもできる。ただし、セキュリティレベルを上げすぎると使えにくい。一方、国防省は厳しいセキュリティ機能を要求しており、他の組織は不要な対策まで必要になる。

・今後、ネットワーク経由のプリンタの利用にi-PINを活用する要請がでてくるかもしれない。

・製品が初期の段階では、機能の充実が優先であり、セキュリティは後回しになる。 基本的なセキュリティに対する要求に対応する程度。しかし、製品が成熟すると、より安全性が重要になるのではないか。

・開発者に対するセールスポイントとしてAAAソリューションを提供していたとしても、顧客がAAAソリューションがあるから、というだけで判断するわけではなく、ROIを見て導入を判断する。セキュリティを強化してもROIが向上するわけではない。

・9年ほど日本にいたことを踏まえた意見として、セキュリティに対するインフラは韓国のほうが優れていることが多い。たとえば、金融機関で発行した証明書が他の金融機関でも使える。CAのリレー(チェーン)が機能している。逆に、ユーザ側の意識は韓国のほうが低い。

・スマートデバイスは顧客の要求次第。言われたらやるということではないか。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
概要 (1/3) EXECUTIVE SUMMARY

DRAFT National Strategy for Trusted Identities in Cyberspace

■ 様々なコニュニケーションを支えるサイバー空間は国家の重要インフラの重要部分を占める。また特に最近警告されている、オンライン詐欺、個人情報の盗難、オンライン情報の誤った利用などについては、連邦政府は注意を払い明らかにしなければならない。

■ この戦略は、これらのオンラインのやりとりに関する問題の解決方策として、個人、組織、サービス、デバイスなどのアイデンティティ情報に関わる信頼のレベルを向上させ、より信頼のおけるコンピューティング環境を実現する方法を探すものである。

戦略ビジョン:
個人と組織は、信頼性、プライバシー、選択、イノベーションを促進する形で、安全で効率的で使いやすく相互連携が可能なアイデンティティ・ソリューションをオンラインサービスのアクセスに利用する。

■ この戦略は信頼のおけるオンライン環境をサポートする「**アイデンティティ・エコシステム**」を定義し促進する。アイデンティティ・エコシステムは、個人、組織、サービスおよびデバイスが相互に信頼し合えるオンライン環境である。これは権威あるソースが確立され、そのソースがそれらのデジタル・アイデンティティを認証することにより実現される。

■ **アイデンティティ・エコシステムが実現すること**

- **セキュリティ**: オンライン取引への攻撃者による不正を難しくする。
- **効率性**: 個人は、管理するパスワードやアカウントを減らすことを選択できる。また、民間企業においては紙ベースの処理やアカウント管理の手間を削減できる。
- **使いやすさ**: アイデンティティ・ソリューションを可能な限り自動化し、最小限の訓練で実行可能となる技術に基づかせる。
- **信頼性**: デジタル・アイデンティティは適切に保護され、各種のオンライン取引でインターネットが活用されるようになる。
- **プライバシーの向上**: 個人のデータが責任を持って取扱われるようになり、誰がどのような目的でデータを収集利用するかを適宜知ることができる。
- **より広い選択肢**: アイデンティティ認証情報や装置が**相互運用可能な**プラットフォームで提供される
- **イノベーション**の機会: サービス提供者は、本質的に高リスクとされるサービスを、オンラインでサービス開発・展開できる。

＜参考＞

[1] "National Strategy for Trusted Identities in Cyberspace (Draft)", June 25, 2010
http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
オバマ大統領のCyberspace Policy Reviewを受けて、DHS(米国土安全保障省)がドラフトを公表。パブリックコメントを反映させ2011年に最終版が公表される予定である。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
概要 (2/3) EXECUTIVE SUMMARY

DRAFT National Strategy for Trusted Identities in Cyberspace

■ **アイデンティティ・エコシステム(IE)の柱**

- **プライバシー保護**: IEは、アイデンティティを秘密に保ち、取引の実現に必要な情報のみを共有することによって匿名の参加者を保護する。その一方で、IEはより確かな参加者のアイデンティティの確認が必要な取引もサポートする。IEでは、より堅固なアクセス制御技術を用いて不正アクセスによる情報の悪用のリスクを減らす。
- **自発的な参加**: IEへの参加は、組織と個人のいずれについても自発的なものである。
- **相互運用性**: IEは強力で相互運用性のある技術を用い、参加者間の適切なレベルの信頼を可能にする。相互運用性によってアイデンティティのポータビリティがサポートされ、IEのサービスプロバイダーにおいては様々な認証情報や個人識別のメディア種別が受け入れ可能になる。IEでは唯一のアイデンティティ・プロバイダーとして政府に依存することはない。その代わりに相互運用性により、公共及び民間セクターの様々なアイデンティティ・プロバイダーがIEに参加できる。

■ これらにより、ユーザ中心なIEが実現される。つまり、個人が、取引にあった相互運用可能な認証情報を選択することが可能になる。プライバシーを強化するポリシーや標準の策定により、個人は必要最低限の情報だけを伝えることができるようになる。加えて、これらの標準は個人の取引と認証情報の利用をサービスプロバイダーが関連付けることを抑止する。適切な関係者間で情報を交換し、情報をセキュアに伝送し、プライバシーのベストプラクティスに則って情報を守られることで、これまでよりも信頼できるようになる。

「サイバー空間における信頼可能なアイデンティティのための国家戦略」の戦略目標

1	包括的なアイデンティティ・エコシステム(IE)・フレームワークの開発	オンラインサービスのセキュアな提供を可能にするガバナンス、ポリシー、標準、インフラの設計と構築
2	IEフレームワークに基づいた、相互運用可能なアイデンティティ・インフラの構築と実装	
3	IEへの信頼の向上と参加意欲の喚起	個人および企業に向けたポリシーによる保護と教育啓発
4	IEの長期的な成功の確実化	IEの継続的な開発と改良

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
概要 (3/3) EXECUTIVE SUMMARY

DRAFT National Strategy for Trusted Identities in Cyberspace

戦略目標およびビジョンの実現に向けた高優先度のアクション

1	戦略目標の達成に向けた公共／民間セクターの取り組みを政府関係機関がリードすることを示す
2	公共／民間セクターで共有される包括的な実施計画を策定する
3	アイデンティティ・エコシステムに関する連邦政府サービス、試行的実験、政策を拡大・加速する
4	強化されたプライバシー保護の実現に向け公共／民間セクターを協調させる
5	リスクモデルと相互運用のための標準の開発と改良に関し調整を行う
6	サービス提供者と個人の間の責任の所在を明確にする
7	すべてのステークホルダーに対する広報や啓発を行う
8	国際的コラボレーションを継続する
9	国内におけるアイデンティティ・エコシステムの普及推進策を模索する

アクションの実行にあたっては、連邦政府はデジタル・アイデンティティ強化のためのリーダーシップ、調整、コラボレーションの提供を継続する。このアクションの日々の調整については、それを主導する政府機関を大統領府が指定する。
大統領府内のサイバーセキュリティ・コーディネーター部門はこのアクション・プランに示された政府機関の間のポリシー策定を引き続き先導する。主導する政府機関は同部門と密に連携して働く。

■ この戦略は、連邦政府に始まるアクションを呼びかけるものである。連邦政府にはアイデンティティ・エコシステム(IE)を最初に実現し、最初に利用し、キー・サポーターとなる役割が期待される。

■ 連邦政府は、民間セクター、州、市町村、海外政府等とのコラボレーションを持続し、IEを実現するために必要なリーダーシップとインセンティブを提示しなければならない。

■ 民間セクターは、同様に、この戦略の実施に極めて重大な役割がある。個人はサイバー空間における日常のオンライン取引行為を通じてIEによる利益を得ることになる。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
はじめに INTRODUCTION

仮訳

DRAFT National Strategy for Trusted Identities in Cyberspace

アイデンティティ・エコシステムに向け、ゴール、ビジョンに基づいて行動していく。

■ 現在の状況

- 情報とサービスを提供するためにインターネットの接続性に依存していく一方で、個人・組織の様々な重要なデータに対する脅威が増している。
- こういったサイバー犯罪における損害の定量化は難しいが、いくつかこの問題の大きさを示す研究が報告されている。
- 毎年1千万人以上のアメリカ人がアイデンティティ盗難の被害にあっている。こういった現状には、期限切れのソフトウェア、安全でないウェブブラウジング、アンチウイルスシステムの非導入など様々な理由がある。
- 今日のオンライン環境はユーザ中心型ではなく、ユーザが自身の個人情報を扱う操作性がほとんどない。
- こういった状況を打破すべく、連邦政府はサイバー空間における信頼を向上していかなければいけない。

■ 領域

- 戦略ではオンライン取引のセキュリティ改善に向けたデジタル・アイデンティティを確立・維持することに焦点を当てる。
- 戦略ではプライベートセクター、個人、政府に向けた取引に焦点をあてる。これは多くの取引における国際的な性質である。
- 安全なオンライン取引におけるアイデンティティは包括的なアイデンティティ管理領域のサブセットである。
- 戦略は国民IDカードの提唱ではなく、かわりに、相互連携可能で信頼できる様々なオンライン取引の確立を目指している。

■ 国家戦略の展開

- ホワイトハウスは連邦政府がこの戦略に向けてリーダーシップを取っていく。
- Federal Identity, Credential, and Access Management (FICAM) ロードマップを既に作成。
- この戦略はそういった活動を加速・拡張していくものである。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
指針 GUIDING PRINCIPLES

仮訳

DRAFT National Strategy for Trusted Identities in Cyberspace

この指針は、戦略におけるゴール、目的、アクションから成り、サイバー空間における信頼性のあるアイデンティティをサポートするための本質的な特徴について答える。

■ アイデンティティ・ソリューションは安全で弾力性のあるものとなる

- アイデンティティ・ソリューションは弾性があり、回復性があり、柔軟な適用性を持つべきである。
- インフラストラクチャは認証された個人・エンティティによって不正な取引を防ぐべきである。

■ アイデンティティ・ソリューションは相互運用される

- 相互運用性によってサービス提供者は様々な証明書とアイデンティティ・メディアの受け入れが可能となる。
- **相互運用のための3種類の要件**

i. **技術的:** 異なった技術においても広く浸透したインタフェースでのデータのやり取り。

ii. **セマンティック:** エンド・トゥ・エンドの受信・送信を意図した意味でのやり取り。

iii. **ポリシー:** 共通したビジネスポリシーと処理方法。

■ アイデンティティ・ソリューションはプライバシーを高め、パブリックに対して自発的となる

- 認証において不必要な情報まで提供するケースがある。(18歳以上を示すために運転免許証を見せる等)
- 自発的なプライバシーの公開が理想的であり、8つのFair Information Practice Principles (FIPSs)が提案されている。
- FIPSsを採用したアイデンティティ・エコシステムは信頼性のあるアイデンティティ・システムを達成するための鍵となる。
- アイデンティティ・エコシステムは個人に自身の証明書を選択させるべきである。

■ アイデンティティ・ソリューションは費用対効果がよく、取り扱いが簡単になる

- 度重なるパスワード等のユーザ情報の変化はサービス提供者にも個人に対しても重荷である。これは危険なユーザ管理にもつながる。
- アイデンティティ管理システムを導入し、複数アカウント管理のためのコスト、脆弱性を削減、排除するべきである。またそれは使いやすくするべきである。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」
ビジョンと利点(1/3) Vision and Benefits

DRAFT National Strategy for Trusted Identities in Cyberspace

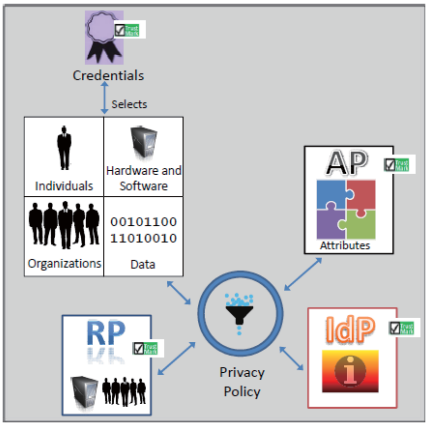
ビジョン:
個人と組織は、信頼性、プライバシー、選択、イノベーションを促進する形で、安全で効率的で使いやすく相互連携が可能なアイデンティティ・ソリューションをオンラインサービスのアクセスに利用する。

■ アイデンティティ・エコシステム(IE)

- アイデンティティ・エコシステムは、個人、組織、サービスおよびデバイスが相互に信頼し合えるオンライン環境である。これは権威あるソースが確立され、そのソースがそれらのデジタル・アイデンティティを認証することにより実現される。
- IEは実行層、管理層、ガバナンス層の3層から構成される。

個人 (Individual)	
デジタルID (Digital Identity)	個人を現す属性のセット
非人間エンティティ (Non-person Entity, NPE)	IEで認証を必要とするもの。組織、ハードウェア、ソフトウェア、サービス等で個人と同様にIEで取扱われる。
アイデンティティ・プロバイダー (Identity Provider, IDP)	個人あるいはNPEを認証し、証明書を発行する。
属性プロバイダー (Attribute Provider, AP)	RPからリクエストに応じて属性情報を提供する
依拠当事者 (Relying Party, RP)	認証を利用するサイトなど

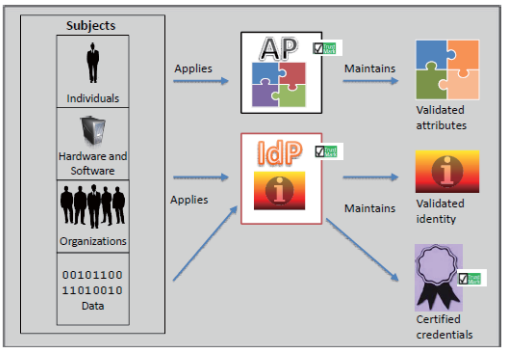
■ 実行層(Execution Layer):
個人、組織、NPEがIEの規則に沿って取引を行う



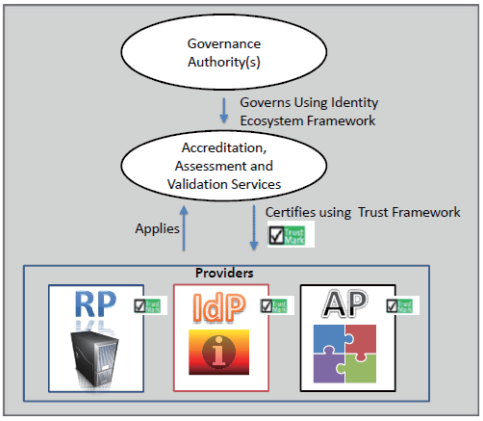
参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略（案）」ビジョンと利点(2/3) Vision and Benefits

DRAFT National Strategy for Trusted Identities in Cyberspace

■ **管理層（Management Layer）:**
IEにおける関係者に規則を適用・施行する



■ **ガバナンス層（Governance Layer）:**
IEにおいて機能させるべき規則を確立する



参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略（案）」ビジョンと利点(3/3) Vision and Benefits

仮訳

DRAFT National Strategy for Trusted Identities in Cyberspace

■ **アイデンティティ・エコシステム（IE）の特徴**

- 個人と組織は、自身が使用するプロバイダやセキュアな処理を行う運営方法を選択できる
- 関係者は互いに信頼することができ、処理がセキュアであることの確信を持てる
- 個人はプライバシーを犠牲にすることなく、複数の組織とオンラインで業務を行うことができる
- アイデンティティ・ソリューションは個人にとって扱いやすく、プロバイダにとっては効率的である
- アイデンティティ・ソリューションはスケーラブルであり、逐次進化していく

■ **個人にとってのIEの利点**

- **セキュリティ**: プロバイダはデータ、とりわけ個人のデジタル・アイデンティティに関連したデータを安全に保管する
- **効率性**: 個人はより選択肢のあるオンラインサービスを利用でき、利用時間を節約し、生産性が向上する
- **使いやすさ**: ソリューションは直観的で、理解が容易で、アクセスしやすく、広く利用することが可能となる
- **信頼性**: 改良されたアイデンティティ・ソリューションは個人情報の盗難や詐欺の危険を低減させる
- **プライバシー**: プロバイダは必要とされていない限り個人情報を収集したり、利用したり、共有したりできない。また、軽率もしくは権限のない情報漏洩からデータを常に守り続けなければいけない
- **選択の機会**: 個人は多様なサービスプロバイダやデジタル署名の中から選択する

■ **民間企業にとってのIEの利点**

- **セキュリティ**: 改良されたアイデンティティ・ソリューションは詐欺に関連した損失を低減させ、知的財産や機密情報をより守ることができる
- **効率性**: 信頼性のあるデジタル・アイデンティティの一貫性と正確性は生産性を向上させる
- **信頼性**: ビジョンの実現はセキュリティが破られる危険性を低減させ、それによって民間企業とそのパートナーのオンライントランザクション信頼性を向上させる
- **プライバシー**: アイデンティティ・エコシステムは従業員や顧客のデータ管理・保持の複雑性を低減させ、それによってプライバシー侵害に関するリスクを低減させる
- **イノベーション**: アイデンティティ・エコシステムの導入は新しく、刷新的なサービス、とりわけ高いリスクとユーザ中心のトランザクションの関連したサービスの形をとって新たな市場機会を創造する

■ **政府にとってのIEの利点**

- **セキュリティ**: 適切な証明・認証により向上した信頼性によってセキュリティは改良される
- **効率性**: IEは政府がより効率的に国民のために尽力することや職務を全うすること可能にする
- **イノベーション**: 早期導入を通して信頼性のある認証を促進したり、セキュアなサイバー空間において市場にイノベーションをもたらす研究開発を促進することは政府の義務である

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略（案）」DRAFT National Strategy for Trusted Identities in Cyberspace
大目標とそれに伴う小目標 Goals and Objectives

サイバー空間における信頼可能なアイデンティティ構築のための戦略目標

■ **大目標 1: 包括的なアイデンティティ・エコシステム（IE）・フレームワークの開発**

- 小目標 1.1: 定義されたリスクモデルに基づいた、包括的な本人確認及び認証の標準を確立する
- 小目標 1.2: IEにおける参加者の責任を定義し、説明責任を果たす仕組みを確立する

■ **大目標 2: IEフレームワークに基づいた相互運用可能なインフラの構築**

- 小目標 2.1: IEフレームワークに関する政府のリーダーシップと採用を継続する
- 小目標 2.2: IEフレームワークを実装するソリューションの迅速な展開を奨励する
- 小目標 2.3: ユーザにとっての価値を強めるために多数かつ多様なソリューションを利用可能にする

■ **大目標 3: IEへの信頼の向上と参加の意欲の喚起**

- 小目標 3.1: 情報とソリューションの公正かつ責任ある管理を通じてプライバシーと取引のセキュリティの強化を促進する
- 小目標 3.2: 十分な説明をうけた上で決定が可能となるように教育・啓発を行う

■ **大目標 4: IEの長期的な成功の確実化**

- 小目標 4.1: デジタルアイデンティティに関する連邦政府の取り組みを国内外について調整する
- 小目標 4.2: 国内外における技術標準化作業に参画する
- 小目標 4.3: 積極的かつ集中的な研究開発活動を通じてイノベーションを導く

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略（案）」DRAFT National Strategy for Trusted Identities in Cyberspace
実行へのコミットメント Commitment to Action

仮訳

アイデンティティ・エコシステムの実装には方針、プロセス、技術、幅広い利害関係者に影響する教育訓練の複雑な行動の組み合わせが必要。この章では実装のための重大な事項である最優先行動を示す。連邦政府はアイデンティティ・エコシステムの先導者となるべく積極的に取り組んでいる。

■ **行動 1: ゴールや戦略を実現するためのパブリック/プライベートセクターの取り組みを連邦政府がリードすることを示す。**

- 目標、行動の進捗状況を明らかにする。
- 開発、サポートの例に従って政府の統率を確認。
- 目標の達成に関わる省庁間のコラボレーションをサポート、省庁間の取り組みをコーディネートする。
- プライベートセクターに勧告する機構を設立する。

■ **行動 2:共有され包括的なパブリック/プライベートセクターの実施計画を作成する。**

- 官民セクターごとの既存の取り組み統合点を識別する。個々のタスクの結合管理者を割り当てる。完全性・トレーサビリティを確認する。

■ **行動 3:アイデンティティ・エコシステムに関連する政府サービス、実験、政策を拡大する。**

- 連邦政府は、医療、交流、情報技術、防衛産業基地、エネルギー、金融セクターおよび州政府の指導者の能力に注意を払う。
- 連邦公開鍵基盤、DNSSEC、IPSec、および連邦アイデンティティ、資格、およびアクセス管理のロードマップ活動が関連する。

■ **行動 4:強化されたプライバシ保護の実現のためにパブリック/プライベートセクターで共同する。**

- 連邦政府はプライベートセクターと共にFIPPsの実現方法を決定する。
- エンティティの保持、送信、保護、使用、収集を強化し、個人情報を破棄することを標準化。
- データが誤用される恐れのあるものの対応策を講じる。

■ **行動 5:リスクモデルと相互連携のための標準の開発と改善。**

- アイデンティティ・エコシステムで設立される規格には、プライバシーガイドラインの取り込みが必要である。

■ **行動 6:サービス提供者や個人の間の責任の所在を明確にする。**

- トランザクション参加者による双方向の信頼を確立するために連邦政府が責任改革を通じて障壁に対処する必要がある。

■ **行動 7:全ての利害関係者に対する広報や啓蒙を行う。**

- 個々のセクターはリスク、利益、アイデンティティ・エコシステムへの参加方法を知る必要がある。

■ **行動 8:国際的なコラボレーションを継続する。**

- ローカルな標準化を避けるために、国内での取り組みで標準となったものを国際標準化されるように努力すべき。
- アイデンティティ・エコシステムの成功のためには、多国籍企業やインターネットレベルでの相互運用性や拡張性を意識したアイデンティティを利用するグローバルプロバイダの参加が必要。

■ **行動 9:国内におけるアイデンティティ・エコシステムの採用を促進する他の方法を特定する。**

- 連邦政府は経済的な刺激の効果を評価する必要がある。
- 堅牢なアイデンティティ・ソリューションは包括的な刺激なしには起こらない。
- 税額控除、サイバーセキュリティ保険、助成プログラムやローンを考える必要がある。
- 連邦政府はリスク、コスト、利益を評価する必要がある。

参考2 「サイバー空間における信頼可能なアイデンティティのための国家戦略(案)」

結論　Conclusion

仮訳

DRAFT National Strategy for Trusted Identities in Cyberspace

- アイデンティティ・エコシステムはユーザ、サービスプロバイダ、その他利害関係者がオンライントランザクションにおけるデジタルアイデンティティをどのように改善できるかの方針を提供している。
- ガバナンス、管理、実行レベルの行動がアイデンティティ・エコシステムを実現するために必要な開発及びメンテナンスをサポートするハイレベルな行動として提案されている。
- ビジネスや情報交換におけるサイバー空間での依存は今後も増すであろう。その中で信頼性が重要である。
- オンライントランザクションでのアイデンティティの保護は、公開商取引、技術革新の促進、我が国の重要な資産守るために極めて重要である。
- アイデンティティ・エコシステムは個々の権利の保護、プライバシーの強化、ID窃盗のリスクを軽減するために不正行為を防ぐことを示す。

- サイバー空間においてどのように使われ、信頼を得るのかを政府がリードしていかなければならない。
- 官民の枠を越えた組織同士の協力の継続が必要
- できるだけ早く実用化するには呼びかけが必要となる。
- 境目を越えたコーディネーションが必要であり、すべてのセクターが関与することとリーダーシップを持つことが求められる。

〒100-8141
東京都千代田区永田町2-10-3
株式会社三菱総合研究所
情報技術研究センター
クラウドセキュリティグループ　川口、江連、井上
Tel: 03-6705-6045, Fax: 03-5157-2148
Email: kawaguti@mri.co.jp, e-mika@mri.co.jp, sinoue@mri.co.jp

セキュリティ市場・技術調査報告書

発　行　日　　平成23年３月
編集・発行　　社団法人　電子情報技術産業協会
　　インダストリ・システム部
　　企画グループ
　　〒100-0004　東京都千代田区大手町1-1-3
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　三 協 印 刷 株 式 会 社