巻頭論文

社会・技術動向の変化と情報セキュリティへの取組み


米田　健*　　松井　充**

Information Security Strategies to cope with Changing Social and Technological Trends

Takeshi Yoneda, Mitsuru Matsui

要　旨

三菱電機は，社会動向・技術動向の変化に迅速に対応しながら，情報セキュリティ技術を活用して企業・社会の情報システムの安全・安心の実現に取り組んできた。

現在，新しい情報セキュリティ対策を必要とする主な技術動向・社会動向の変化として，次の変化に着目している。

①サイバー攻撃の激化

②スマートフォン・タブレットの普及

③高齢化社会の到来

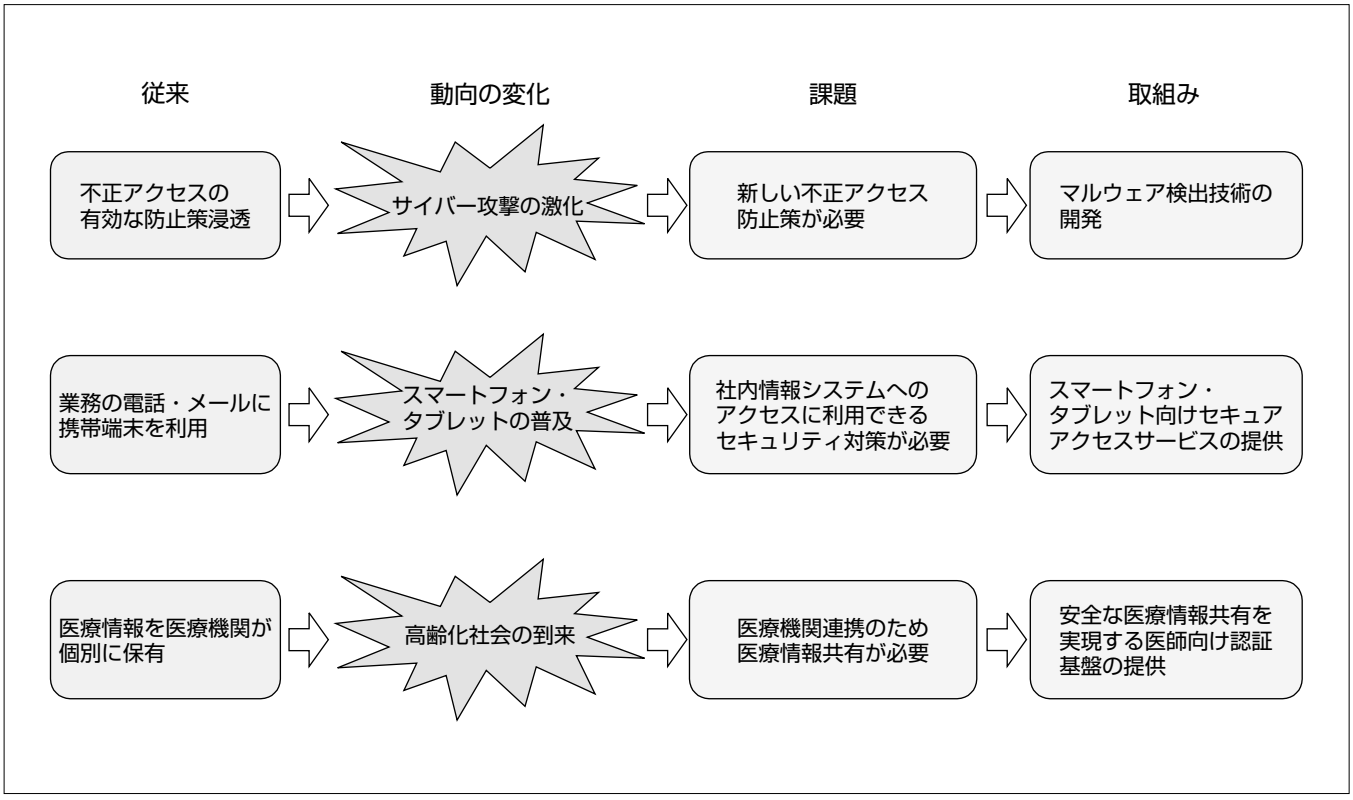
これらの動向の変化によって生じる課題に対して，次の取組みを実施した。

(1) 従来の不正アクセス対策の効力低下によって，マルウェア感染を想定した早期検知が求められる。そこで，マルウェアの振る舞いからマルウェアを検出する技術を開発した。

(2) スマートフォン・タブレットは，社内の機密情報のアクセスに利用される。そこで，“使っていて安全”“つなげて安全”“落としても安全”を実現するセキュアなサービスを提供した。

(3) 高齢化に伴う慢性疾患患者増大が招く病院の混雑，医療費の増大を解消するために，地域医療機関の連携強化が求められている。そのためには，地域の医療機関がITを活用して医療情報の共有・交換をする必要がある。当社は，経済産業省の平成22年度“医療情報化促進事業”の医療認証基盤整備事業，“のとの私のMy病院”事業に参画し，安全な医療・健康情報の共有・交換のための基盤システムを開発した。

これらの情報セキュリティに関する技術・製品・サービスの提供によって，企業・社会の情報システムの安全・安心の実現に貢献していく。



社会・技術動向の変化に対応した情報セキュリティの課題と当社の取組み

サイバー攻撃の激化，スマートフォン・タブレットの普及，高齢化社会の到来という社会的な動向の変化に対応して，情報セキュリティ上の新たな課題が顕著になってきており，それらに対する当社の先進的な取組みを示している。

*インフォメーションシステム事業推進本部連携事業推進センター・グループマネージャー(工学博士)　**情報技術総合研究所 情報セキュリティ技術部長(博士(情報理工学))

1. まえがき

1.1 情報セキュリティを取り巻く最新の状況

近年，サイバー攻撃の激化によって，従来有効であった不正アクセス防止対策など情報セキュリティ対策の見直しが必要となってきている。また，情報セキュリティ対策の必要な領域は，普及の加速するスマートフォン・タブレット，国内・海外拠点間をつなぐグローバルな情報システム，医療・健康情報を扱う情報システムと広がりを見せている。

情報セキュリティ対策の内容の変化と適用領域の拡大を受け，情報セキュリティ関連のハードウェア，ソフトウェア製品や サービスの市場規模は，2010年度3,464億円から，2015年度4,990億円へと拡大が予想されている(**図1**)[1]。

1.2 社会・技術動向の変化

当社では，これらの市場の拡大を牽引(けんいん)する動向として，サイバー攻撃の激化，スマートフォン・タブレットの普及，高齢化社会の到来の3点に着目している。

(1) サイバー攻撃の激化

近年のサイバー攻撃では，標的型攻撃に見られるように，従来の不正アクセス防止対策をすり抜けて，利用者の端末に感染するウイルス(マルウェア)が利用される。従来の不正アクセス防止対策の徹底・強化と同時に，マルウェアの感染を早期に検出することが課題となる。

(2) スマートフォン・タブレットの普及

従来の携帯電話の主な業務用途は，電話，メールであった。一方，スマートフォンやタブレットは，表示機能，通信速度，処理速度，記憶容量とも従来のモバイルノートパソコン並みとなり，操作性も優れている。その結果，企業機密情報を扱う社内情報システムへのアクセスに利用するニーズが高まっている。その反面，スマートフォンやタブレットは，次の点からセキュリティが課題となる。①アプリケーションを個人でも容易に開発できるので，不正なアプリケーションが混入する可能性がある。②無線通信を用いるので，盗聴や成りすましの危険性が高い。③紛失しやすい。そのため，“使っていて安全”“つなげて安全”“落としても安全”であるように，セキュリティを確保する必要がある。

(3) 高齢化社会の到来

65歳以上の高齢者の人口は，1990年1,490万人から2010年2,925万人へと倍増した(**図2**)[2]。

高齢者の増加に伴って慢性疾患も増大し，病院の混雑や医療費の増大の一因となっている。そこで，地域の病院・診療所が相互に連携することで，病気発症からの経過に応じて適切な治療を適切な病院・診療所で受診可能にすることや，患者が自らの医療・健康情報を電子的に管理し，その情報を医療機関や介護施設に提示可能にすることが必要となっている。

これらを支援する情報システムに対しては，高い機密性と原本性が求められるため，医療・健康情報の安全な共有・交換が課題となる。

次章以降では，これらの動向の変化と課題への取組みの詳細を述べる。

2. サイバー攻撃の激化

2.1 市場動向

2011年度のサイバー攻撃激化の動きを受けて，国内のセキュリティソフトウェア市場の年間成長率は，2.8%から4.8%に上方修正され，市場規模は，2011年度1,965億円から2015年度2,357億円となることが予想されている[3]。

2.2 技術動向

近年のサイバー攻撃は，特定の分野の特定の企業をねらい，その従業員が思わず添付ファイルを開いてしまうような成りすましメールを攻撃に用いることが特徴である。このようなメールを標的型攻撃メールと呼ぶ。

標的型攻撃メールに添付されたファイルには，そのファイルを開くアプリケーションの脆弱(ぜいじゃく)性を悪用する攻撃コードが仕組まれている。その結果，従業員がそのファイルを開くと，ファイルの内容が表示されると同時に，従業員も気付かないうちに，マルウェアに感染する。

不正な添付ファイルによるマルウェアの感染防止を困難にしている要因として，公開されていないソフトウェアの脆弱性が狙われる，マルウェアは常に新種で，感染後自らを変化させるの2点が挙げられる。

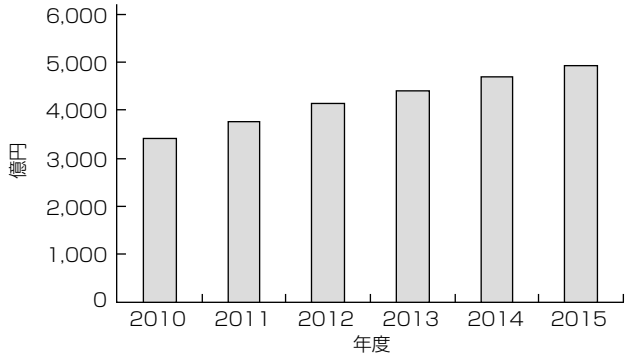


図1．情報セキュリティ市場の展望[1]

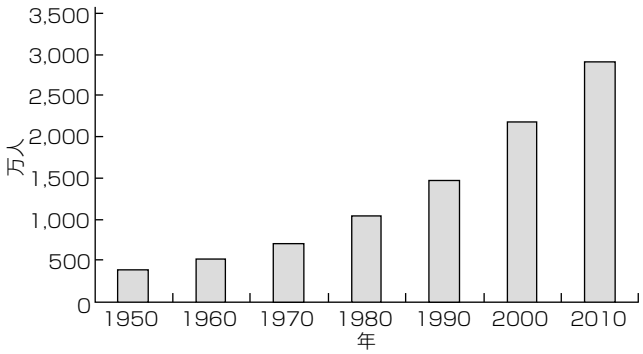


図2．日本の65歳以上の人口の推移[2]

⑴　公開されていないソフトウェアの脆弱性が狙われる

近年のサイバー攻撃では，ソフトウェア製品ベンダーも認識していない脆弱性が狙われる。その結果，最新のソフトウェアへのアップデートがマルウェアへの感染防止に有効，という常識が通用しなくなった。

⑵　マルウェアは常に新種で，感染後自らを変化させる

近年のマルウェアは，標的とする企業向け専用に新規に作成される。そして，感染後，自らを変化させていく。その結果，マルウェアは，ウイルス対策ソフトウェアのパターンファイルに登録されず，ウイルス対策ソフトウェアの検出機能をすり抜けてしまう。

マルウェアは感染後，外部の不正者から，ファイルの検索，取得等の機密情報取得コマンドを受け付け，外部の不正者の企業機密情報搾取を支援する。

マルウェアの挙動の一例を示す。まずマルウェアは，ユーザーのキーボードによるパスワード入力をキーロガーなどを用いて盗む。そして，そのパスワードを用いてユーザーに成りすまし，ファイルサーバのファイルにアクセスする。また，マルウェアはブラウザのふりをして，従業員の社外Webへのアクセスを装って，コマンドの受信や機密ファイルの外部への送信を行う。したがって，社内から社外へのブラウザアクセスは正当な通信と判断するファイアウォールや侵入検知システムでは検出が困難になっている（**図3**）。

マルウェアの感染を未然に防ぐファイアウォール・侵入検知システム・ウイルス対策ソフトウェア等の入口対策の有効性が低下しているため，マルウェアへの感染を想定して，マルウェアの社内から社外への通信を検知遮断する出口対策や，マルウェアの振る舞いからマルウェアを検出することが課題となる。

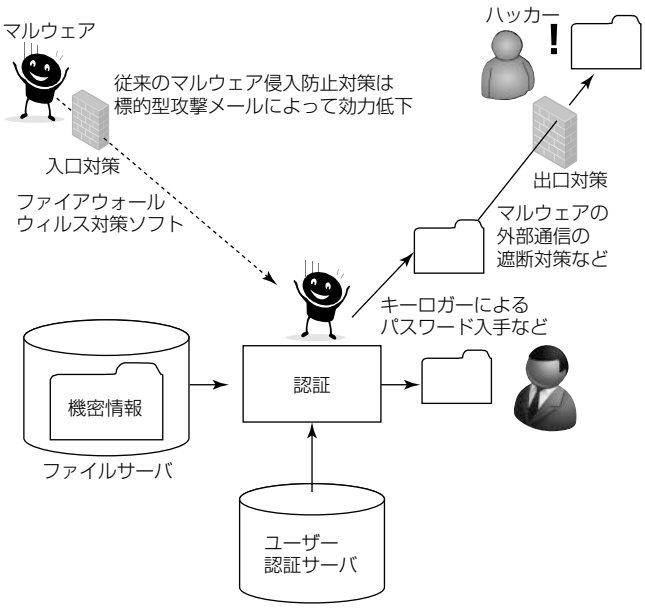


図3．従来の対策をすり抜けるマルウェア

2.3　当社の取組み

当社では，標的型サイバー攻撃への対策として，従来の不正アクセス防止対策の強化・徹底と同時に，マルウェアの検出技術の開発や，外部の不正者が企業情報の入手を試みても，無効なデータしか入手できない技術の開発に取り組んでいる。

マルウェアの中には，感染端末を攻撃者が操作できる状態にあることを外部不正者に知らせるために，一定の間隔で，外部不正者に短い情報の送信（ビーコン通信）を行うものがある。通常の従業員によるWebアクセスであれば，そのような通信は行われない。

そこで，このようなタイプのマルウェアの通信を検出するために，外部Webサーバへのアクセスログを保存し，ログの相関分析によってビーコン通信を検出する機能を開発した。この機能によって，従業員の通常の外部Webサーバへの通信にまぎれこむマルウェアによる通信を検出することが可能となる。

当社は，これらを一例とするマルウェアの振る舞いをログから検出する技術を開発した。マルウェアは日々進化するので，検出に利用する振る舞いが公開された時点で，検出されないように振る舞いを変えていく。

したがって，マルウェアが行わざるを得ない振る舞いを検出する仕組みを非公開に作り込むことが重要となる。

3.　スマートフォン・タブレットの普及

3.1　市 場 動 向

スマートフォン・タブレットは，企業にとって，コンシューマー向けの有望な販売チャネルとなってきている。利用者に画面上のアイコンを指でタッチさせるだけで，企業のサイトに利用者を誘導できる効果は大きい。そして，企業による積極的なアプリケーションの提供が，スマートフォン・タブレットの普及を後押ししている。スマートフォン・タブレットのアプリケーションは，キーボード入力を極力少なくする優れた操作性を持つため，その操作に慣れた利用者は，社内システムへのアクセスでも利用したいというニーズを持つ。

法人向けのスマートフォンの出荷台数は，2010年度60万台から2015年度には460万台に増大すると見込まれている。また，法人向けのタブレットは，2010年度30万台から2015年度には270万台に増大すると見込まれている[4]。

スマートフォン・タブレットのアプリケーションは，個人でも容易に開発可能で，従来の携帯電話のアプリケーションに比べると，通信機能や端末に保存された情報に自由にアクセスできることが特長である。その結果，不正なアプリケーションによる情報漏洩（ろうえい）の防止が課題となる。さらに，端末の成りすましによる不正アクセスや紛失した端末からの情報漏洩の防止も課題となる。

これらの課題を解決する情報セキュリティに対するニーズは高く，法人用途のスマートフォン・タブレット向けの情報セキュリティ製品・サービスの市場規模は，2010年度118億円から2015年度492億円へと拡大が見込まれる[4]。

3.2 技術動向

スマートフォン・タブレットの情報セキュリティ技術は，“使っていて安全”“つなげて安全”“落としても安全”という3点の実現を目指している。

⑴ 使っていて安全

スマートフォン・タブレットの使用中に，端末の情報が，不正なアプリケーションによって意図しないサイトに送信されることを防止する必要がある。不正なアプリケーションの混入防止には，ウイルス対策ソフトウェアのパターンファイルのようなブラックリストを用いるのではなく，企業が事前に認めたアプリケーションしか起動できない仕組みが有効である。

⑵ つなげて安全

無線通信経由のなりすましによる不正アクセスと通信の盗聴を防止する必要がある。そのために，端末の認証と端末の利用者の認証を組み合わせて実施する。また，認証と同時に通信の暗号化を実施することで，盗聴を防止する。

⑶ 落としても安全

紛失した端末を用いた不正アクセスや，紛失した端末に保存された機密情報の漏洩を防止する必要がある。通信機能の無効化やデータ消去を遠隔から実現する。また，リモートデスクトップ機能を端末に搭載することによって，端末上には企業の情報が保存されないようにすることも有効である。

3.3 当社の取組み

三菱電機情報ネットワーク㈱(MIND)では，2010年に，iPhone／iPad(注1)のiOS搭載端末向けに，セキュアスマートフォンアクセスサービスの提供を開始した。このサービスでは，暗号化通信，端末認証，個人認証の3つを組み合わせることによって，許可された端末を用いた許可されたユーザーだけが社内業務システムにアクセスできる。2011年には，iOS搭載端末向けに，端末の紛失・盗難時の遠隔ロック・遠隔データ消去，業務以外のアプリケーションの利用制限を実現するスマートフォンマネージサービスの提供も開始した。そして，2012年には，Android(注2) OS搭載端末向けに，セキュアスマートフォンアクセスサービス・スマートフォンマネージサービスの提供を開始した。

急速に進化・普及するスマートフォン・タブレットを安心して利用できるサービスを今後も積極的に提供する。

（注1） iPhone／iPadは，Apple Inc. の登録商標である。
（注2） Androidは，Google，Inc. の登録商標である。

4. 高齢化社会の到来

4.1 市場動向

厚生労働省が2009年から2013年に実施を計画した地域医療再生計画や，高度情報通信ネットワーク社会推進戦略本部(IT戦略本部)が2010年5月に閣議決定した“新たな情報通信技術戦略”に基づいて，経済産業省が2010年から2011年に実施した医療情報促進化事業など，ITによる地域医療連携や国民自身による医療・健康情報の活用が，国家レベルで推進されている。

これら国の施策による後押しもあり，医療関連ITの市場規模は，2011年の5,182億円から2015年には5,587億円へと拡大が予測されている。年間市場成長率は1.2%でIT全体の市場成長率0.5%を上回る[5]。

また，地域医療連携システムの市場規模は，2010年度18億円から2020年度には240億円へと成長が見込まれている[6]。

4.2 技術動向

地域医療連携では，治療や検査の計画(クリニカルパス)や電子カルテ等の医療情報，電子紹介状等の医療文書を医療機関の間で共有・交換することが必要となる(**図4**，**5**)。

医療情報の安全な共有や交換のためには，医師の成りすまし防止が必須であり，医師の確実な認証が求められる。

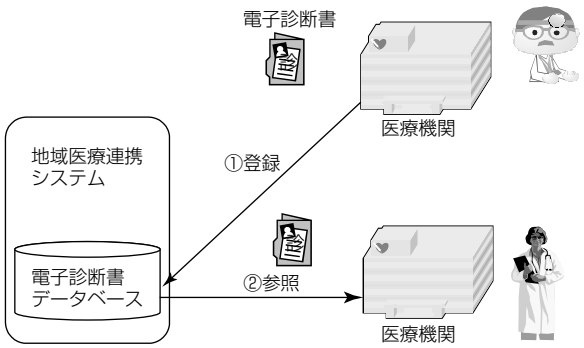


図4．医療機関の所有する医療情報の共有

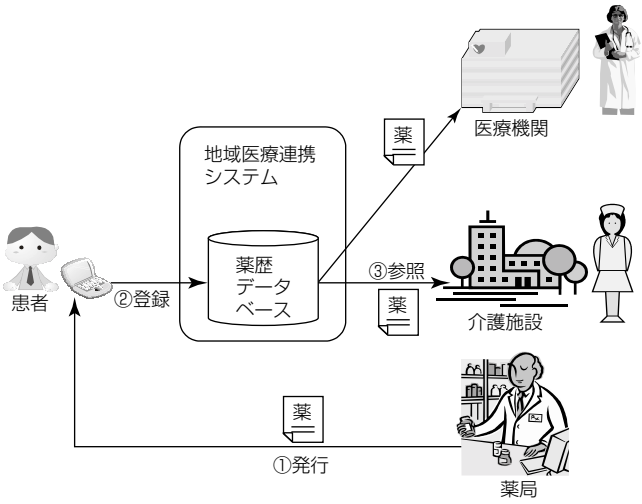


図5．患者が所有する医療・健康情報の共有

また，地域医療連携では，医師が複数の異なるシステムを利用することが想定されるため，一旦認証された医師であれば，複数のシステムをログオン操作なしで利用できるシングルサインオンシステムに対するニーズも高まっている。

一方，異なるシステム間で交換される電子医療文書に関しては，フォーマットの標準化と改ざんの防止が必須である。

電子署名が付与された医療文書のフォーマットとして，HL7 CDA[7]が策定されており，近年の実証事業でも活用されている。

認証や電子署名には，公開鍵暗号基盤(PKI)が利用される。厚生労働省は，医師の認証や電子文書への電子署名への適用を目的に，保健医療福祉分野における公開鍵暗号基盤(Healthcare Public Key Infrastructure：HPKI)の普及促進を進めている。

4.3 当社の取組み

当社は，HPKI ICカードを用いた医師認証システムや，医療情報などの機密性の高いデータの交換に用いるセキュアネットワークサービス等，医療分野だけでなく金融分野等へも横展開可能な高いレベルのセキュリティを確保したIT基盤の開発と事業化に取り組んでいる。

経済産業省の平成22年度“医療情報化促進事業”では，三菱電機インフォメーションシステムズ㈱(MDIS)が，医療認証基盤整備事業と“のとの私のMy病院”事業に参画した。

医療認証基盤整備事業では，㈳日本医師会の認証局から発行されたHPKI規約[8]に準拠した医師向けの証明書で認証を行う医療認証サービスシステムを構築した。

この認証サービスシステムは，証明書の認証機能に加え，シングルサインオンの機能も備えている。シングルサインオンを実現するため連携モジュールも同時に開発し，他の医療情報化促進事業で開発されたシステムを利用する際に，医師によるシングルサインオンを実現した。

のとの私のMy病院事業では，患者の健康情報，医療情報を個人の同意のもとに登録・保管・閲覧・第三者へ開示できる，いわゆる“どこでもMy病院構想”の仕組みを構築した。

これらの実証事業の成果は，地域医療連携の促進，国民自身による医療・健康情報の活用の促進への貢献が期待される。

5. むすび

サイバー攻撃の激化，スマートフォン・タブレットの普及，高齢化社会の到来等，技術・社会の動向の変化に着目して，当社の情報セキュリティへの取組みを述べた。当社は，これら動向の変化に対応する情報セキュリティの技術開発，製品・サービスの提供によって，企業・社会の情報システムの安全・安心の実現に向けて貢献していく所存である。

参考文献

(1) 2011ネットワークセキュリティビジネス調査総覧(上，下巻)，㈱富士キメラ総研（2011）
(2) 平成22年国勢調査　産業等基本集計結果，総務省統計局（2012）
(3) 国内情報セキュリティ製品市場予測，IDC Japan（2011）
(4) 2012法人向けスマートデバイス関連ビジネスの全貌，㈱富士キメラ総研（2012）
(5) 国内医療／健康／介護福祉関連IT市場予測，IDC Japan（2011）
(6) 2011年版 地域医療連携システムの現状と今後の方向性，㈱シードプランニング（2011）
(7) ISO/HL7 27932:2009，Data Exchange Standards HL7 Clinical Document Architecture, Release 2
(8) 保健医療福祉分野PKI認証局　証明書ポリシ(平成17年4月)，厚生労働省（2005）