


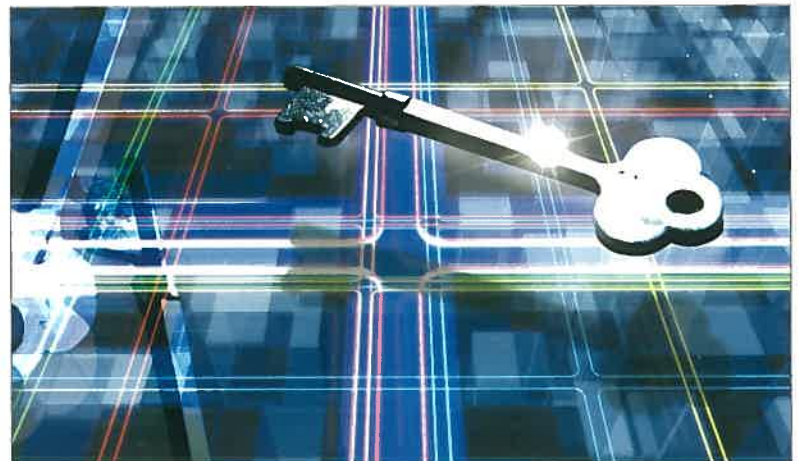
MITSUBISHI
Changes for the Better

家庭から宇宙まで、エコチェンジ 

三菱電機技報

7 | 2012
Vol.86 No.7

企業の安心・安全を支えるセキュリティ技術



目次

特集「企業の安心・安全を支えるセキュリティ技術」

安全だけど安心できない, 安全でないけど安心できる……………1
菊池浩明

社会・技術動向の変化と情報セキュリティへの取組み ……2
米田 健・松井 充

セキュリティ統合管理システム
—新しいセキュリティ脅威への対策— ……………7
北澤繁樹・河内清人・桜井鐘治・矢崎 玲・藤井誠司

クラウド向き関数型暗号技術の進展 ……………12
高島克幸・酒井康行・内藤祐介・坂上 勉・松田 規・森 拓海

高信頼量子暗号装置と量子鍵配送を用いた
ワンタイムパッド携帯電話ソフトウェア ……………16
長谷川俊夫・山中忠和・柴田陽一・酒井康行

統合ログ管理ソリューション
“AnalyticMart for LogAuditor” ……………21
和田貴成・大塚哲史・阿波基文

Webアプリケーション脆弱性への取組み ……………25
竹林信博・柴田幸治・山本隆二

大規模情報系システムにおける
統合ID管理ソリューションの適用 ……………29
木幡康博・及川和彦・小宮 崇・森田康之・山足光義・小杉 優

ハンディターミナルを使用した入退場・認証システム ……34
渡辺康一・濱崎光幸・松井智浩

医療認証基盤 ……………38
村上耕平・長浜隆次

ISMSを利用した情報セキュリティ対策の要件定義……………43
岩本 仁・菅原和則

Android端末に対応したセキュアスマートフォンサービス ……47
梶場純一

Information Security Technologies for Protecting Enterprise Activities

Secure but not safe, or safe but not secure?
Hiroaki Kikuchi

Information Security Strategies to cope with Changing Social and Technological Trends
Takeshi Yoneda, Mitsuru Matsui

Security Information and Event Management System—Countermeasure against New Security Threat—
Shigeki Kitazawa, Kiyoto Kawauchi, Shoji Sakurai, Ryo Yazaki, Seiji Fujii

Recent Progresses of Functional Encryption Technology for Cloud
Katsuyuki Takashima, Yasuyuki Sakai, Yusuke Naito, Tsutomu Sakagami, Nori Matsuda, Takumi Mori

Highly Reliable Quantum Key Distribution System and its Application to One-time Pad Smartphone
Toshio Hasegawa, Tadakazu Yamanaka, Yoichi Shibata, Yasuyuki Sakai

Integrated Log Management System “AnalyticMart for LogAuditor”
Takashi Wada, Tetsufumi Otsuka, Motofumi Awa

Approach to Web Application Security
Nobuhiro Takebayashi, Yukiharu Shibata, Ryuji Yamamoto

Applying the Integrated Identification Management Solution to Very Large Information System
Yasuhiro Kowata, Kazuhiko Oikawa, Takashi Komiya, Yasuyuki Morita, Mitsuyoshi Yamatari, Yu Kosugi

Entrance and Exit Authentication System Using Handy Terminal Device
Kouichi Watanabe, Mitsuyuki Hamasaki, Tomohiro Matsui

Healthcare Public Key Infrastructure Authentication Service
Kohei Murakami, Ryuji Nagahama

Requirement Definition Method Using ISMS for Information Security Control
Hitoshi Iwamoto, Kazunori Sugahara

Secure Smartphone Service Corresponding to Android Device
Junichi Haseba

特許と新案

「外部記憶装置およびSBC制御方法」「メール暗号装置」…51

「通信システム及び通信プログラム及び通信方法」……………52

表紙：企業の安心・安全を支えるセキュリティ技術

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情報システムの安全・安心の実現に取り組んでおり、これらを通じて企業・社会の発展に貢献していく。

表紙では、情報セキュリティ技術を“鍵”に例えて、サイバー攻撃などから企業活動やそれらをつなぐネットワークを守る様子をイメージ図で示した。



巻/頭/言

安全だけど安心できない、安全でないけど安心できる

Secure but not safe, or safe but not secure?

菊池浩明
Hiroaki Kikuchi

子供を釣りに連れて行ったらオニオコゼに刺されてしまった。ポツリと血がにじんだぐらいのけがだというのに、さっきまでは平気で針を外していた魚に触れなくなってしまった。一度痛い目に会うと体が痛みを覚えていて、いくら親が安全だと勧めても、もう信用してくれない。

信用できないのは、魚か親父かはさておき、失った信頼はなかなか取り返せないものである。彼にとって、魚は安全でも“痛くない”という言葉が信じられなくて安心できない。安心とは、仕組みが安全であり、その安全性を確信して心が穏やかな様を言う。安全学の権威である明治大学の向殿教授によると、

安心=安全×信頼
の法則がある⁽¹⁾。安全と信頼のどちらが欠けても安心できない。安心を築くには長い時間がかかるのに対して、失うのは一瞬である。

近年のサイバー攻撃は、従来有効と信じられてきた情報セキュリティ対策をすり抜けるほど、高度に進化してきている。高度な暗号技術の適用、厳格なネットワーク不正アクセス対策、厳格な法令遵守を実施しても、サイバー攻撃によって情報セキュリティを守りきれなかった事例が増えている。あらゆる情報が電子化されて効率的に交換されている情報化社会にとって、サイバー攻撃は安心を脅かす脅威として、影響力を増してきた。

そもそも私たちは、“絶対に安全なセキュリティは信頼できない”ことを知っている。例えば、RSA公開鍵暗号は、何ビットに拡張しても偶然に素因数分解できてしまう小さな確率がある。どんなに厳密に安全性が評価された共通鍵暗号を使っても、鍵の元となるパスワードの選び方が安直ならば、容易に解読されてしまう。いかに法令遵守を徹底しても、悪意をもった内部者の犯罪を防ぐことは難しい。セキュアなOSの脆弱(ぜいじゃく)性に対するパッチの頻度は、そのソフトウェアの複雑性に依存して増加する。パッチを当てて安心しても、直ぐに次のパッチがリリースされ、いつになってもなかなか安心できない。結局のところ、情報セキュリティには“完全”はない。

では、リスクを消費者に明示することが製造者の責任を果たすことになるのだろうか。

“この金融商品は元本割れのリスクがある”といったリスクの説明が販売者に義務付けられている。リスクを知った上で、リターンの方が上回ると判断した消費者は購入する。リスクを説明していれば、元本割れが発生した場合の責任を販売者が問われることはない。

セキュリティの製品・サービスもリスクとリターンを消費者が判断できるように、分かりやすく説明する必要があるだろう。難しい暗号理論や証明を利用者に分かりやすく説明して納得してもらうための努力を惜しんではいられない。

安全や信頼に疑問があって、安心できない場合、以下の2つのケースで安心してもらうことが考えられる。

(1) 安全だが信頼できない

安全を信頼させることが重要である。飛行機が怖い人がいる。事故が起きる確率は非常に小さいが、起きた時に逃げられないという恐怖が彼らの信頼をなくしているのではないだろうか。そこで、事故が起きることを想定して対策を立て、見えない脅威を正しく見せる必要がある。公平に調査した結果を示すことが、安心を呼び起こす手段である。

(2) 信頼しているが安全でない

リスクがリターンよりも小さいことを示すことが重要である。発がん性が分かっている喫煙者はいる。しかし、他人への配慮は必要だが、その許容リスクが正しく理解できていれば、煙草を吸うことによってリラックス効果が得られるなどのメリットを享受できる。リスクの大きさとその対策となる情報セキュリティの原理と限界が明確に分かっていれば、たとえ完全な安全でなくても信頼できるのではないだろうか。

冒頭の話に戻る。オニオコゼはおいしい。非常に美味であるとともに可食部が少ないので高級魚と言われている。完全に安全ではないけれど、“使いこなせば有益な情報セキュリティ技術”を刺されないように食したい。

(1) 向殿政男：安全とファジー〜どこまでやったら安全か〜，知能と情報(日本知能情報ファジ学会誌)，24，No.2，55～62(2012)

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り組み



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

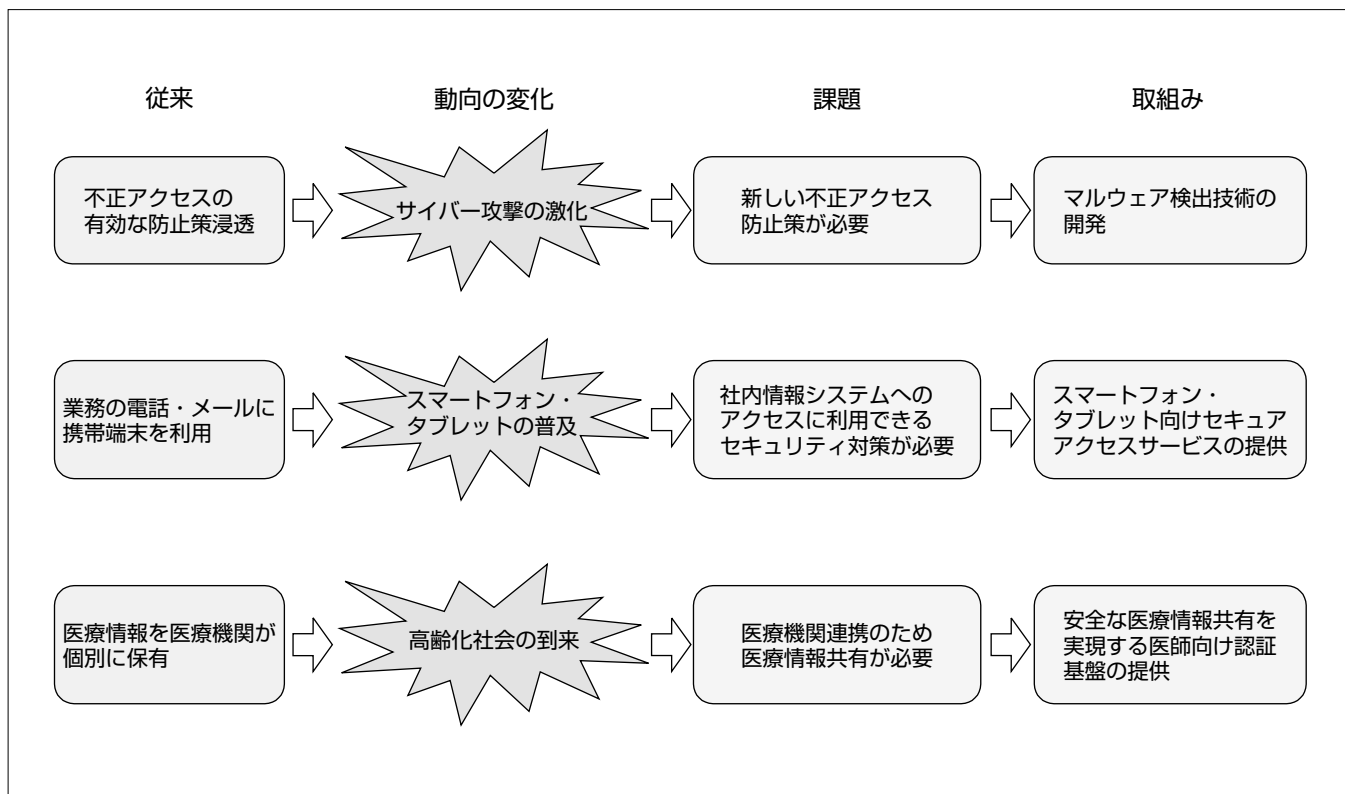
これらの動向の変化によって生じる課題に対して、次の取り組みを実施した。

- (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”“つけて安全”“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り組み

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り組みを示している。

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。

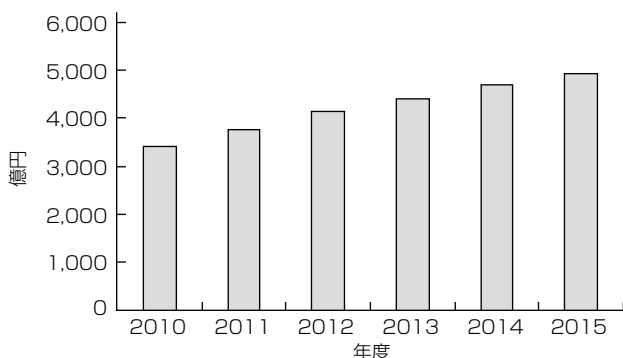


図1. 情報セキュリティ市場の展望⁽¹⁾

(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込まれている。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。

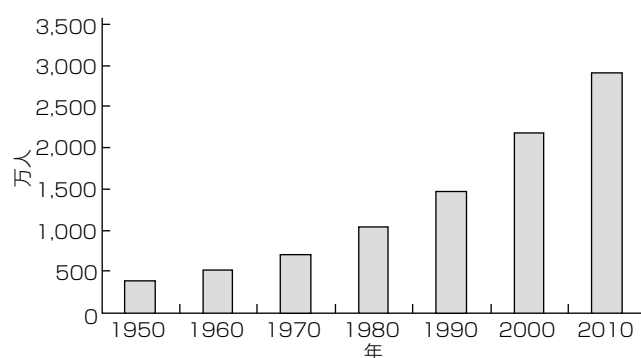


図2. 日本の65歳以上の人口の推移⁽²⁾

(1) 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。

(2) 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。

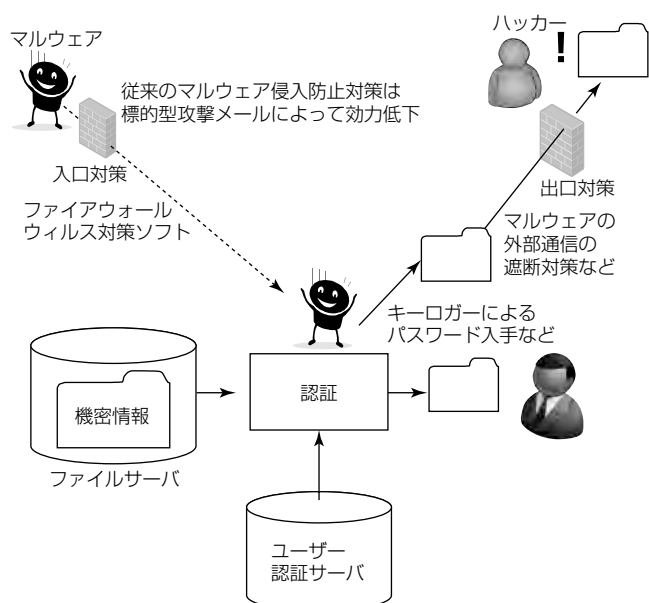


図3. 従来の対策をすり抜けるマルウェア

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。

(1) 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へ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。

(2) 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。

(3) 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株(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。

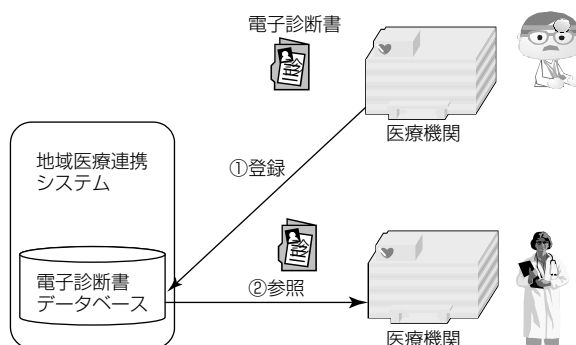


図4. 医療機関の所有する医療情報の共有

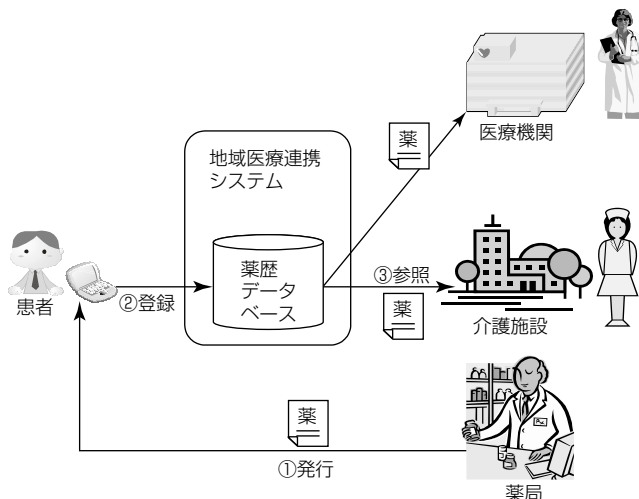


図5. 患者が所有する医療・健康情報の共有

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(株)(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、(社)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・健康情報の活用へ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), (株)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, (株)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, (株)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 証明書ポリシー(平成17年4月), 厚生労働省 (2005)

セキュリティ統合管理システム —新しいセキュリティ脅威への対策—

北澤繁樹* 矢崎 玲**
河内清人* 藤井誠司**
桜井鐘治*

Security Information and Event Management System—Countermeasure against New Security Threat—

Shigeki Kitazawa, Kiyoto Kawauchi, Shoji Sakurai, Ryo Yazaki, Seiji Fujii

要 旨

近年、新しいセキュリティ脅威として、特定企業や個人を狙い、執拗(しつよう)に攻撃を行う“標的型攻撃”が顕在化し、その対策が求められている。標的型攻撃は、脆弱(ぜいじゃく)性を悪用し、複数の既存攻撃を組み合わせ、攻撃するため、1つの視点での監視によるセキュリティ対策では対応できない。

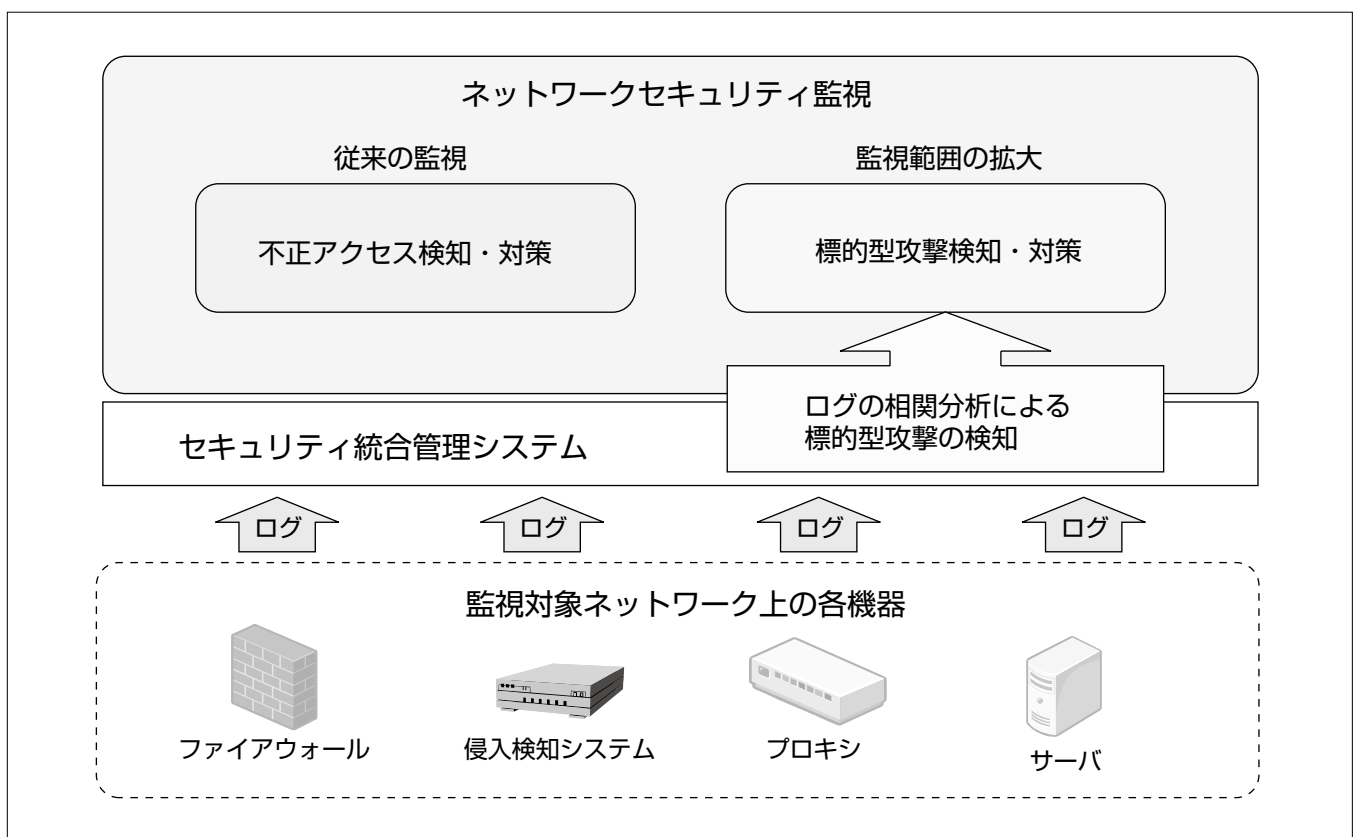
三菱電機では、標的型攻撃への対策として、監視対象ネットワーク上の機器の監視情報(ログ)を統合的に管理・分析する“セキュリティ統合管理システム”を用いた標的型攻撃の検知技術に関する研究開発に取り組んでいる。

この研究開発では、標的型攻撃を分析し、攻撃を複数の段階に分け、それぞれの段階における検知方式を検討した。特に、標的型攻撃の初期段階での検知を行うことが重要で

あるため、収集したログに記録されたイベントの中から、通信時刻の異なる複数イベントを関連付ける相関分析を行うことで、標的型攻撃で使用される悪意のあるプログラムとインターネット上の攻撃者のサーバとの通信を検知する方式を考案し、実装及び動作に関する評価を行った。

この技術の適用に向けて、監視対象ネットワーク上の機器のログをリアルタイムに収集・分析する不正アクセス監視サービスを提供している三菱電機情報ネットワーク株(MIND)と検討を進めている。

三菱電機では、今後も、情報セキュリティの攻撃技術の変化へ柔軟に対応できるセキュリティ統合管理システムを活用した攻撃検知技術の研究開発を進めていく。



セキュリティ統合管理システム

三菱電機が開発した、セキュリティ統合管理システムの相関分析機能を用いた標的型攻撃の検知技術によって、ネットワークセキュリティの監視範囲を拡大する。

1. ま え が き

近年、新しいセキュリティ脅威として、特定企業や個人を狙い、執拗に攻撃を行う“標的型攻撃”が顕在化し、その対策が求められている⁽¹⁾⁽²⁾。

標的型攻撃とは、“脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングによって、特定企業や個人を狙い、対応が難しく執拗な攻撃”⁽³⁾と定義される。このため、1つの視点での監視によるセキュリティ対策では対応できないことが課題である。

この課題を解決するため、三菱電機では、監視対象ネットワーク上の機器の監視情報(ログ)を統合的に管理・分析する“セキュリティ統合管理システム”を用いた標的型攻撃の検知技術に関する研究開発に取り組んでおり、その概要を述べる。

2. 新しいセキュリティ脅威(標的型攻撃)

近年の新しいセキュリティ脅威として、標的型攻撃が目されるようになってきた。

標的型攻撃は、個々の標的に特化した攻撃であり、脆弱性を悪用し、複数の既存攻撃を組み合わせることによって、既存の対策を回避する手口で行われる。したがって、ウイルス対策、ファイアウォール、侵入検知システム、URL (Uniform Resource Locator) フィルタといった既存の対策では防ぐことが難しい。

一方、標的型攻撃への対策として、ウイルス対策ベンダー各社が提唱している技術にWebレピュテーション⁽⁴⁾がある。Webレピュテーションは、ウイルス対策ベンダー各社が独自の情報収集経路によって収集した情報を基に、URLのドメインやWebページごとに不正なページかどうかを判断するためスコアを算出し、そのスコアを基準として、ブラックリスト方式によって、アクセス先のWebペ

ージが“不正なページではない”と判定された場合のみ、アクセスを許可する方式である。これによって、不正なWebページへのアクセスを防止する。

しかしながら、Webレピュテーションでは、不正なページを含んでいるかどうかを判定するため基準となるスコアを算出するためには、まず、そのWebサイトへアクセスしてどのようなコンテンツが提供されているのか情報収集する必要がある。したがって、標的型攻撃のように、攻撃者が新規で設置したような、特別なWebサイトに関しては、事前にWebサイトに関する情報収集をすることができず、基準となるスコアを算出できないため、標的となった組織から攻撃者サイトへのアクセスを防ぐことはできない。

また、その後も、該当するWebサイトで、ウイルスなどのマルウェアが検知されなければ、不正なページとは判定されない。

3. セキュリティ統合管理システム

セキュリティ統合管理システムとは、一般には、SIEM (Security Information and Event Management) システムと呼ばれ、ネットワークのセキュリティ監視を目的として、監視対象ネットワーク上の各機器で日々大量に記録されるログをリアルタイムに収集するシステムのことを指す。収集されたログは、相関分析機能によってリアルタイムに分析される。相関分析機能とは、収集された各機器のログに記録された複数イベントを関連付けて分析(相関分析)する機能である。複数イベント間の関連付けには、時刻、ホスト名、IPアドレス、ユーザーID等、イベントが異なっても共通に記録される項目が用いられる。これらの項目によって複数イベントを関連付けることで、1つ1つのイベントを見ているだけでは分からなかった新たな事実が明らかとなる。

図1にセキュリティ統合管理システムの構成を示す。セ

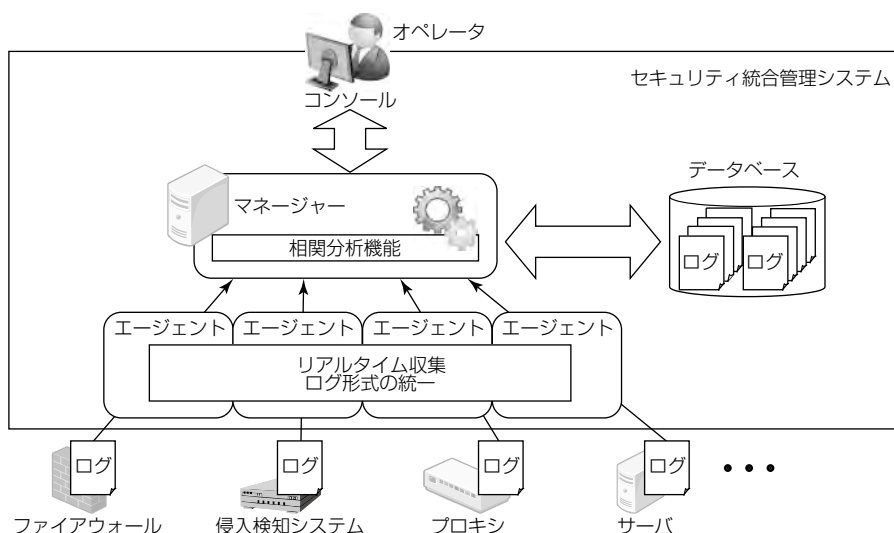


図1. セキュリティ統合管理システムの構成

セキュリティ統合管理システムは、システム全体の管理及び収集したログの分析を行うマネージャー、ファイアウォールや侵入検知システムといった各種ログを収集してマネージャーへ送信するエージェント、収集したログを蓄積するデータベース、システム管理やログの分析を行う際にオペレータが操作するコンソールからなる。

セキュリティ統合管理システムでは、関連分析を行うために、各機器がそれぞれ独自に出力するログ形式を統一された形式に変換して、一元管理する。

この研究開発では、複数のログを関連付けることによって、1つの事象を多面的に分析可能である関連分析機能を用いることによって、標的型攻撃を検知する方式について検討を行った。

4. 標的型攻撃への対策

4.1 標的型攻撃の流れ

この研究開発では、標的型攻撃を分析し、攻撃を次の4つの段階に分け、各段階で関連分析による攻撃の検知方式を検討した。図2に、標的型攻撃の流れを示す。

(1) 初期侵入段階

特定企業や個人あてにマルウェアを添付したメール(標的型メール)を送付し、メールを受信したユーザーに添付ファイルを開かせることによって標的内部ネットワーク上の端末をマルウェアに感染させる。

(2) 情報収集段階

マルウェアと攻撃者サーバとの通信を使って、攻撃者がマルウェアを介して端末を遠隔操作し、標的内部の情報を収集する。

(3) アクセス権限昇格段階

目的の情報へアクセスするのに必要な権限を取得するために、認証情報を不正に入手する。

(4) 目的遂行段階

ファイルサーバなどから目的の情報を取得し、マルウェアに攻撃者サーバへ送信させることで窃取する。

セキュリティ統合管理システムを用いることによって、図3に示すように、標的型攻撃の各段階における複数の視点による統合的な監視・分析が実現可能となる。

これによって、攻撃者がどのような手口を用いて侵入を試みているのか、実際の攻撃がどの段階まで進んでいるのか、また、攻撃者が最終的に目的としている機密情報は何かといった、標的型攻撃の全容を明らかにできる。

ただし、単に収集可能なログを集めて、それらを統合的に監視・分析しようとしても、標的型攻撃の全容を明らかにすることはできない。セキュリティ統合管理システムへ収集するログは、標的型攻撃の各段階で、攻撃者の振る舞いが記録されている可能性があるものを選択する必要がある。

そのためには、標的型攻撃に関する様々なシナリオを事前に想定し、標的型攻撃が発生した場合に、どのログに、

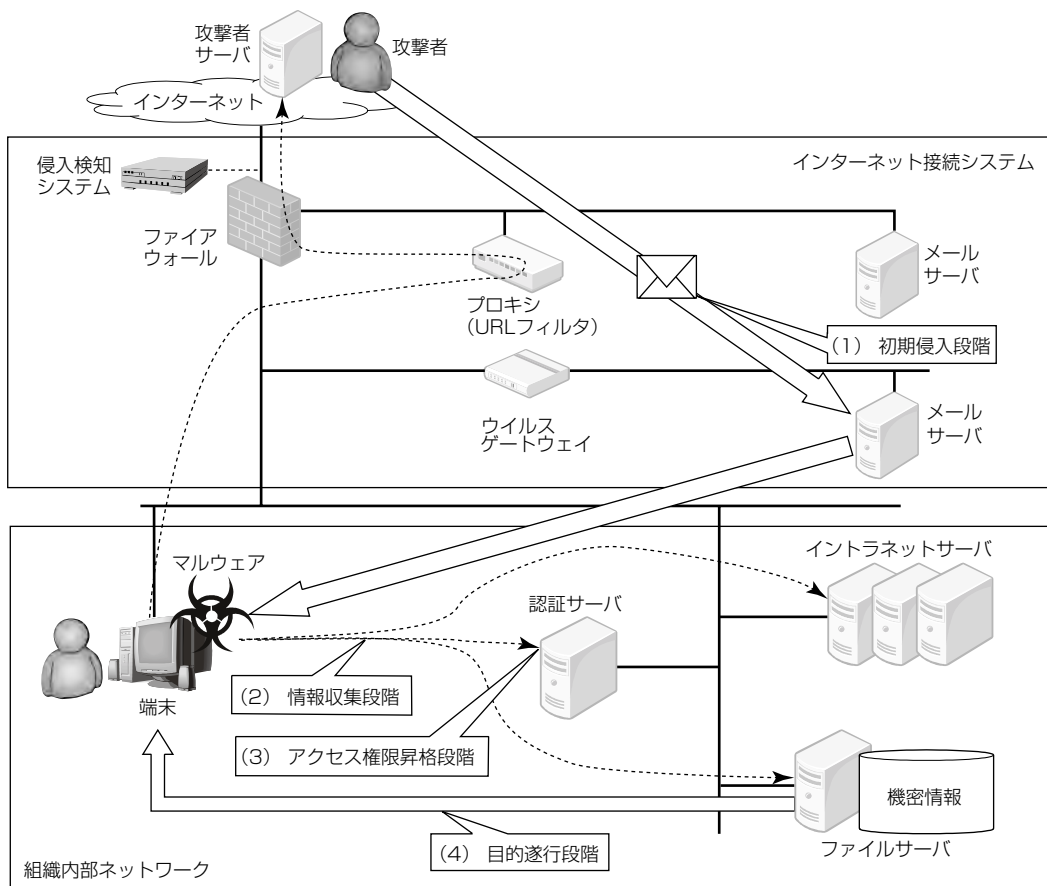


図2. 標的型攻撃の流れ

攻撃者のどのような振る舞いが残されるのか、普段から把握しておかなければならない。

この研究開発では、収集したログに記録されたイベントの中から、通信時刻の異なる複数イベントを関連付ける相関分析を行うことによって、標的型攻撃で使用されるマルウェアとインターネット上の攻撃者サーバとの通信を検知する方式として、ビーコン通信の検知方式及び情報漏えいの検知方式を考案した。

それぞれの検知方式に関する詳細を、4.2節及び4.3節で述べる。

4.2 ビーコン通信の検知方式

標的型攻撃の特徴の1つに、標的の内部の端末がマルウェアに感染後、標的型攻撃の各段階を通して端末と攻撃者サーバ間で行われる、ビーコン通信と呼ばれる通信がある。

ビーコン通信は、標的の内部の端末を攻撃者が操作できる状態にあることを攻撃者に知らせるとともに、攻撃者が発行する命令を標的の内部の端末へ伝える目的で行われる。ビーコン通信では、ファイアウォールやプロキシを通過させるため、一般的な組織で、内部ネットワークからインターネットへの通信に関するセキュリティポリシーにおいて許可されていることが多い、HTTP(HyperText Transfer Protocol)通信やHTTPS(HTTP over Secure Socket Layer)通信が利用される。

この研究開発では、プロキシで大量に発生するHTTP通信及びHTTPS通信のイベントを基に、“ビーコン通信は特定の宛先に対して高頻度で継続して行われる”という特徴に着目して、ビーコン通信を検知する。

特定の宛先に対して通信が高頻度で継続して発生しているかどうかの判定は、通信時刻の異なる複数イベントを関連付ける相関分析によって、特定の宛先への通信の回数を

集計することで行う。

ビーコン通信が発生していた場合には、特定の宛先に対する通信が繰り返しログに記録される。ただし、どのくらいの頻度で通信が発生するのかについては、標的型攻撃で用いられるマルウェアによって異なる。そこで、特定の宛先に対する通信の発生時刻の差分を算出し、得られた時刻差分が同じ通信の回数を集計する。

なお、実際には、イベントとして記録される通信の発生時刻には、ゆらぎが生じることがある。これを考慮して、特定の宛先へ一定範囲の時刻差分で発生した通信の回数をまとめて集計する。

また、通信が継続して行われているかどうかは、集計して得られた値としきい値を比較して判定する。しきい値は、集計の間隔と通信の発生頻度から動的に算出する。

さらに、何らかの理由によって、ビーコン通信が途中で何回も行われずに、一時的に通信の継続性が途切れてしまった場合を考慮し、先に述べた方法で算出したしきい値に1未満の係数をかけることによって、しきい値を低く設定することで、ビーコン通信を漏れなく検知できる。

4.3 情報漏えいの検知方式

標的型攻撃の目的が機密情報の窃取であるため、目的遂行段階で、標的の内部で収集した機密情報を攻撃者サーバへ送信することも、標的型攻撃の大きな特徴の1つである。

情報漏えいの検知方式では、サイズの大きいデータが標的の内部からインターネット上のWebサイトへ送信されたことを検知することが基本となる。

ただし、送信するファイルのサイズが大きい場合には、送信ファイルサイズに基づく検知によって攻撃が発覚することを回避するため、マルウェアが小さなサイズの複数ファイルに分割し、複数回に分けて攻撃者サーバへ送信する

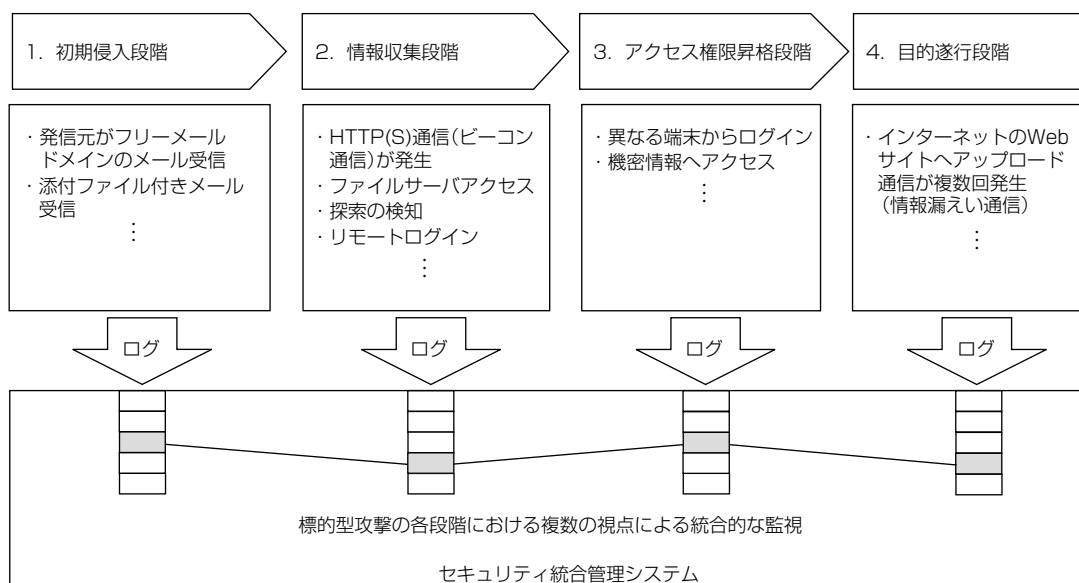


図3. 標的型攻撃の統合的な監視

ことも考えられる。

この研究開発では、情報漏えいの通信を、プロキシのログに記録されているインターネット上のWebサーバへの通信イベントに含まれる“送信データの大きさ”に表れる特徴に着目して検知する。

なお、マルウェアが送信するファイルを小さなサイズの複数ファイルに分割し、複数回に分けて送信することも考慮し、特定の端末から特定の宛先へ一定期間に送信されたデータのサイズを、通信時刻の異なる複数のイベントを関連付ける相関分析によって累積して、その累積した値が一定サイズ以上に達した場合に、情報漏えいが発生したものと検知する。

5. む す び

近年、新しいセキュリティ脅威として、その対策が求められている標的型攻撃を検知するための技術について述べた。

この研究開発では、標的型攻撃を分析し、攻撃を4つの段階に分け、それぞれの段階でセキュリティ統合管理システムを用いた標的型攻撃の検知方式を検討した。

標的型攻撃は初期段階で検知を行うことが、特に、重要である。そこで、セキュリティ統合管理システムに収集されたログに記録されたイベントの中から、通信時刻の異なる複数イベントを関連付ける相関分析を行うことによって、標的型攻撃で使用されるマルウェアとインターネット上の攻撃者サーバとの間で行われる通信であるビーコン通信の検知方式と情報漏えいの検知方式を考案し、それぞれの方式をセキュリティ統合管理システムへ実装し、その動作に

関する評価を行った。

この研究開発の成果は、MINDが提供する不正アクセス対策サービス⁽⁵⁾への適用に向けて検討が進められている。

今後も、三菱電機は、情報セキュリティの攻撃技術の変化へ柔軟に対応できる、セキュリティ統合管理システムを活用した攻撃検知技術の研究開発を進めていく。

参 考 文 献

- (1) 一般社団法人JPCERTコーディネーションセンター：標的型メール攻撃に関する注意喚起（2011）
<https://www.jpccert.or.jp/at/2011/at110028.txt>
- (2) (独)情報処理推進機構(IPA)：「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第2版（2011）
<http://www.ipa.go.jp/security/vuln/documents/newattack.pdf>
- (3) (独)情報処理推進機構(IPA)：IPAテクニカルウォッチ『新しいタイプの攻撃』に関するレポート～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～（2010）
<http://www.ipa.go.jp/about/technicalwatch/pdf/101217report.pdf>
- (4) トレンドマイクロ(株)：Webレピュテーション
<http://www.trendmicro.co.jp/spn/features/web/>
- (5) 三菱電機情報ネットワーク(株)：マネージドセキュリティサービス
<http://www.mind.co.jp/service/security/managed/security.html>

クラウド向き関数型暗号技術の進展

高島克幸* 坂上 勉***
 酒井康行** 松田 規***
 内藤祐介*** 森 拓海***

Recent Progresses of Functional Encryption Technology for Cloud

Katsuyuki Takashima, Yasuyuki Sakai, Yusuke Naito, Tsutomu Sakagami, Nori Matsuda, Takumi Mori

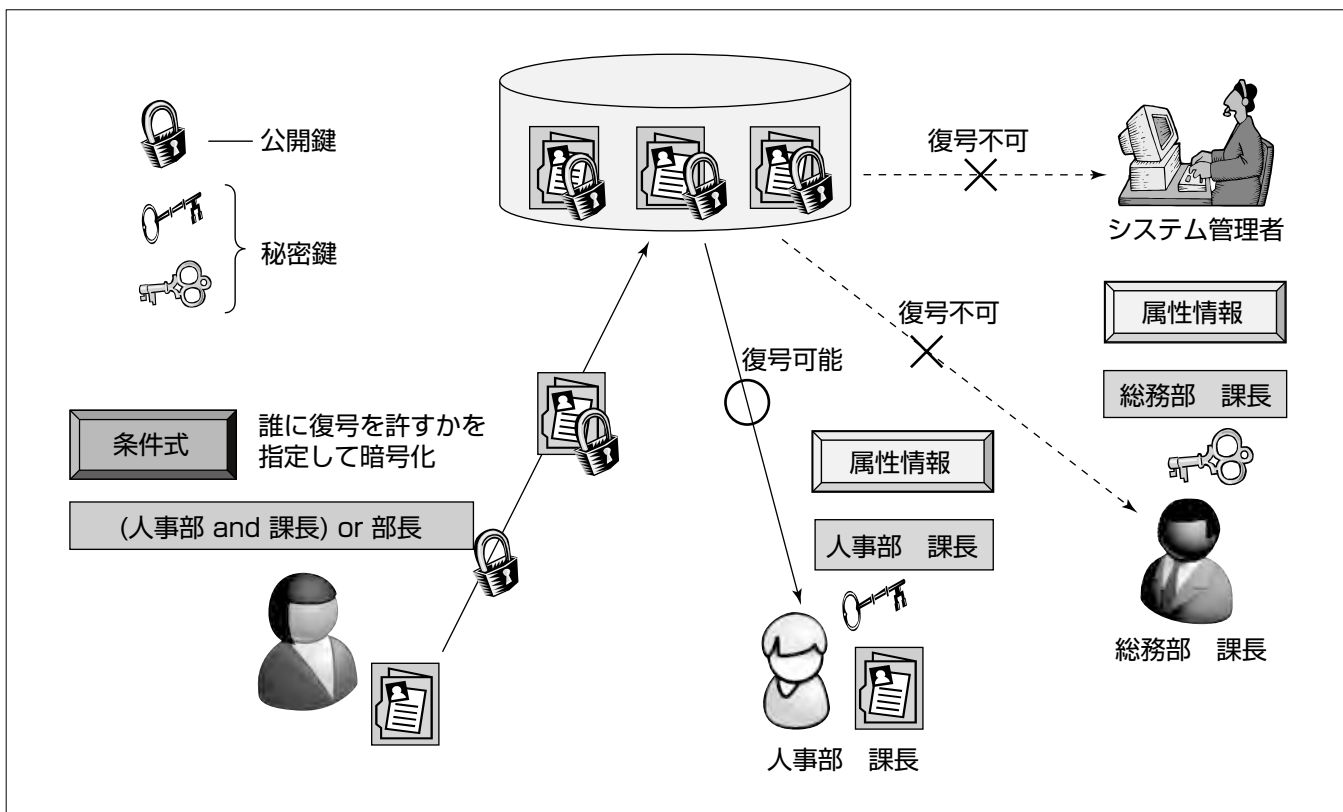
要 旨

クラウドコンピューティング(以下“クラウド”という。)環境におけるネットワークサーバ上の不正操作などの情報漏洩(ろうえい)リスクを払拭する関数型暗号方式を、三菱電機は、日本電信電話(株)と共同で開発して、2010年7月に発表した。それを用いると、保管場所のアクセス制御に依存せずに、安全なデータ保管が実現できる。この関数型暗号方式は、復号鍵に“所属・役職”などの属性を埋め込むことができ、暗号化する際に、復号できる人・グループを、その人の“所属・役職”で指定できる特長を持ち、クラウド環境での高機密データ保存に適する。

2010年発表の従来方式では、実用的な性能確保、安全性改善、機能・利便性向上などが課題であった。今回、当社と日本電信電話(株)は、従来のアルゴリズムを改良し、効率性、安全性、機能性の各性質を改善した。それらの改善は

互いに関連してなされているので、まとめて本稿で述べる。

効率面では、情報を守る乱数を減らしても安全性を落とさずに、処理性能が改善した関数型暗号アルゴリズムを開発した。安全性の面では、検索キーワードを漏洩することなく検索が行える検索可能暗号用途で、これまで厳密に安全性を証明できなかった場合でも、初めて厳密な数学的安全性が証明された方式設計に成功した。そして、機能面の向上としては、自身の属性を証明できるデジタル認証・署名方式(属性ベース署名)も提案し、属性ベース署名を、関数型暗号方式と組み合わせることで、秘匿・認証を全て個人の属性に基づいて行う暗号通信システムを実現可能にした。また、各属性を管轄する鍵発行センターが相互に通信せずに鍵発行できる分散型鍵発行システムも構築して、関数型暗号と属性ベース署名の利便性を高めた。



クラウド向き関数型暗号アルゴリズム

関数型暗号を利用して機密情報管理システムを構築する場合、暗号化を行う際に、誰に復号を許すかを属性の条件式(例えば、(人事部 and 課長 or 部長))で表し、それによって暗号化する。その条件式を満たす人事部課長は、自身の復号鍵を用いて復号できるが、条件式を満たさない総務部課長は、自身の復号鍵を用いては、復号することができない。

1. ま え が き

ICT (Information and Communication Technology) 社会の進展は目覚ましく、近年では、クラウドを始めとするネットワークの新しい高度な利用形態が普及してきた。しかし、そのような利用形態では、プライバシー情報や機密性の高いデータをサーバ側に渡して処理を行うため、新たなセキュリティ上の課題が生じる。ネットワークのセキュリティを保証するために現在では共通鍵暗号と公開鍵暗号が広く利用されているが、上記のような新しいネットワーク利用形態でのセキュリティ課題を解決するためには、より先進的な暗号が必要とされるようになった。共通鍵暗号や公開鍵暗号を更に発展させた先進的な暗号として、暗号化-復号のメカニズムの中に高度なロジック(論理)を組み込むことができる関数型暗号の開発に取り組んできた。

2. クラウド向き関数型暗号アルゴリズム

2010年7月に当社と日本電信電話(株) (以下“我々”という) は、双線型写像ベクトル空間という数学的手法を開拓することで、暗号化-復号メカニズムの中のロジックとして現時点で考え得る最も一般的な機能を持つ関数型暗号の開発に世界で初めて^(注1)成功した⁽¹⁾⁽²⁾。その特長を次に述べる。

(注1) 2010年7月28日現在、当社調べ

2.1 最も一般的なロジックの実現

数年前から世界中で関数型暗号を目指した研究が活発に行われてきたが、今回開発した関数型暗号方式では、従来開発されてきた暗号方式の機能を全て特殊例として包含する最も一般的な機能を実現できる。これは、AND, OR, NOT, しきい値ゲートによって構成される関係式を全て含む理論上最も広いクラスになっている。中でも特筆すべきことは、従来の方式の機能には含まれていなかったNOTゲートが使えるようになったことである。これによって、属性情報の変更などにも柔軟かつ簡便に対応可能なデータベース管理をクラウド上で実現することができる。

2.2 多様な利用形態への対応

関数型暗号では、暗号文と復号鍵に様々なパラメータを導入することで暗号化-復号のロジックを規定するが、ここでは、属性情報とそれに対する条件式が、それぞれ暗号文、又は復号鍵のパラメータとなる。我々が開発した関数型暗号方式では、①“復号鍵に属性情報、暗号文に条件式”の形態も、②“暗号文に属性情報、復号鍵に条件式”の形態も可能であり、様々な利用形態に対応することが可能となっ

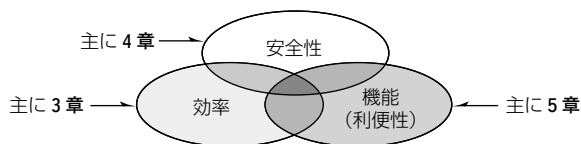


図1. 最近の技術進展

た⁽¹⁾。①の形態を利用することで、データごとにきめ細かくアクセス条件(開示範囲)が設定された暗号データをクラウド上で管理して、そこで設定されたアクセス条件を満足する属性情報を持つ利用者のみがそのデータを復号・閲覧できるような機能提供が可能になる。企業における機密情報管理システムや公的機関による個人情報データベース管理などの応用がある。要旨の図は、企業における機密情報管理システムでの利用イメージを表している。管理する機密文書ごとに誰に復号を許すかを属性情報の条件式で表し、その文書をその条件式とともに暗号化してクラウド上で管理する。その条件式を満足する属性情報を持つ社員がその文書を復号する際には、その社員の(属性情報に応じた)復号鍵を用いて復号し閲覧する。要旨の図では、人事部の課長が、その属性情報に応じた復号鍵を用いて、クラウド上にある暗号化機密情報を入力、復号して閲覧可能となる状況を表している。

2.3 最近の技術進展

参考文献(1)(2)で提案してきた関数型暗号方式を基礎として、最近の参考文献(3)(4)(5)(6)で、安全性・効率性・機能性の各性質が進展したことを述べたが、それらは複合して発展しており、関連させて概観する(図1)。

3. データサイズと復号時間削減への取組み

これまでは指定外の人が復号できないよう、多くの乱数を使用し伝達したい情報を守っていたので、暗号化、復号処理に時間が掛かり、その実用的な性能確保が課題であった。参考文献(3)では、情報を守る乱数を減らしても安全性を落とさずに、暗号文サイズと復号処理性能を改善した関数型暗号アルゴリズムを開発した(図2)。

条件式に論理演算を10個扱えば、通常の属性指定に十分であるが、その場合に復号時間が従来の1/4となり、通常の属性指定で十分な性能確保ができることを確認した。また、内積演算を条件式にする暗号化方式の場合、復号時の演算効率を(漸近的に)大きく改善できた。これは、これまで提案してきた方式でのマスター公開鍵・秘密鍵を特殊な疎行列に基づいて生成することで達成した。安全性証明を行い、安全性を落とさずに高性能を達成した。

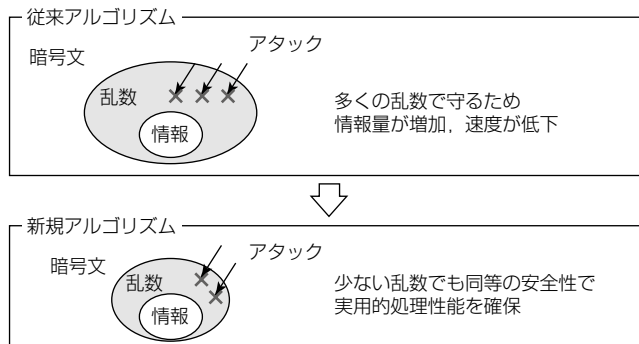


図2. 高速関数型暗号の設計ポイント

4. 検索可能暗号への応用での安全性向上

情報を暗号化したまま検索が可能な暗号は、検索可能暗号と呼ばれて、世界中で研究が進められている。我々の関数型暗号方式は、検索可能暗号機能の実現にも応用できる。クラウド環境では、例えば、医療情報など機密性の高い情報が保管されており、それらは高いプライバシー（秘匿性）を必要とする。また、その情報を医師や製薬会社間で適切に共有できれば、より高い医療サービスを実現できるようになり、その際、検索機能は情報共有を促進してデータベースの有用性を高める重要な要素技術である。

特に、より先進的な検索機能として、通常よく使用されるキーワードマッチングで検索対象を絞り込んでいく（AND検索）だけでなく、キーワード情報に対する任意の条件式で検索（AND、OR条件式検索）できて、秘匿安全性が証明された検索可能暗号方式が望まれている。そのような機能は、参考文献(2)の関数型暗号方式を用いれば実現できたが、その方式を含めて、これまで提案された検索可能暗号は全て“弱い安全性”しか達成できていなかった。我々は、2012年4月に、“より強い安全性”を達成する検索可能暗号方式を世界で初めて^(注2)提案した⁽⁴⁾。従来の検索可能暗号では、暗号文に埋め込まれたキーワード情報が、秘密鍵に埋め込まれた条件式を満たさない場合には、その秘密鍵で、暗号文に対して検索処理を施しても、条件式が満たされないという事実以外に、キーワード情報に関する余分な情報は一切漏れないことが保証されていた。しかし、暗号文に埋め込まれたキーワード情報が、秘密鍵に埋め込まれた条件式を満たす場合には、そのような保証を与えるこ

とができなかった。我々は、参考文献(4)で、その場合にも秘匿性が証明された方式を提案した。

その検索可能暗号によって、図3で示すように、情報開示範囲に対して強い安全性を満たす関数型暗号も実現できる。図3では、(経理部 OR 人事部)という開示範囲も秘匿した暗号文に対し、開発部Aさんと人事部Bさんがアクセスした時を表している。従来方式では、開示範囲に含まれないAさんに情報を一切漏らさないことが保証されていたが、開示範囲に含まれるBさんに、開示範囲が(経理部 OR 人事部)であることが全て漏洩する可能性があった。しかし、経理部に開示されていることを秘匿したい場合も考えられ、そこでは、余計な情報漏洩は回避すべきだが、そのリスクは拭い去れなかった。参考文献(4)の方式では、そのリスクは全くなり、図3では、Bさんは、開示範囲に自分(Bさん)が含まれることだけ分かる。

(注2) 2012年4月18日現在、当社調べ

5. 機能(利便性)向上への取組み

5.1 属性ベース署名

データの出所を保証するデジタル署名技術は、現在のインターネット環境で、なくてはならない技術の一つとなっている。その一方、署名に付随して、各ユーザーの行動履歴が明らかになってしまうことで、ユーザーに対する情報のコントロールが知らないうちになされてしまう“プライバシー侵害”も大きな問題となっている。従来のデジタル署名では、署名を施す署名生成鍵と、署名を検証する署名検証鍵が一对一に対応しており、この問題を根本から解消することができなかった。我々は、今回、属性情報とそれに関する条件式を用いることで、署名生成鍵と署名検証鍵の間の対応を、署名者が柔軟に決定できるようにして、上記のプライバシー侵害問題を解消した。

属性ベース署名は、例えば、自分が三菱電機社員であることを身元保証とした署名を行ったり、人事部員であることを身元保証とした署名を行うことができるもので、それによって、自身のプライバシー(匿名性)を守りつつ、一定の身元保証がされた署名付与が可能になる。そして、署名作成の都度、その匿名性の度合いを自分で決定して署名が行えること、及びその匿名範囲指定を属性情報を用いて行えることという特長は、実用上有用である。我々は、NOT条件も使用可能で、従来法に比べて効率的、そして安全性証明可能な属性ベース署名を提案した⁽⁵⁾。

関数型暗号では、暗号化データ送信者がその開示範囲を属性に関する条件式で指定できる。そして、属性ベース署名では、データ受信者がそのデータ認証を属性条件式の形で、検証できる。つまり、この2つの暗号技術によって、属性に基づいたデータ送受信を適切に行うことができ、クラウド環境への関数型暗号技術の適用を更に進めることが

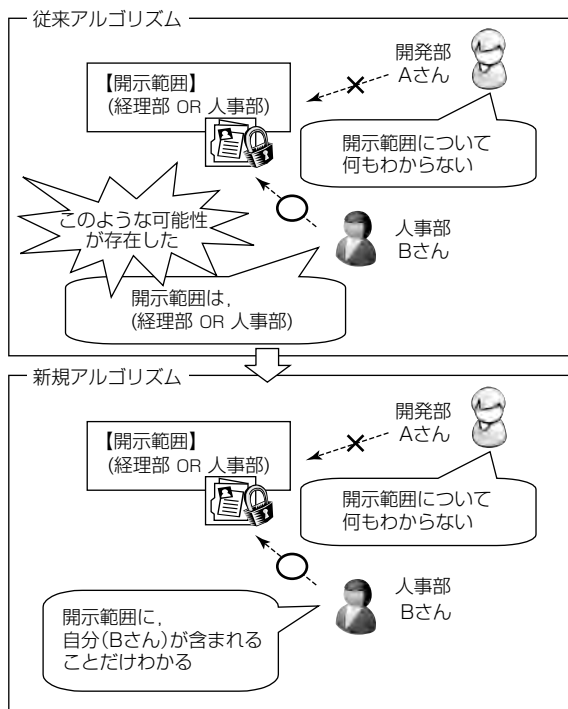


図3. 開示範囲に対し強い安全性を持つ関数型暗号

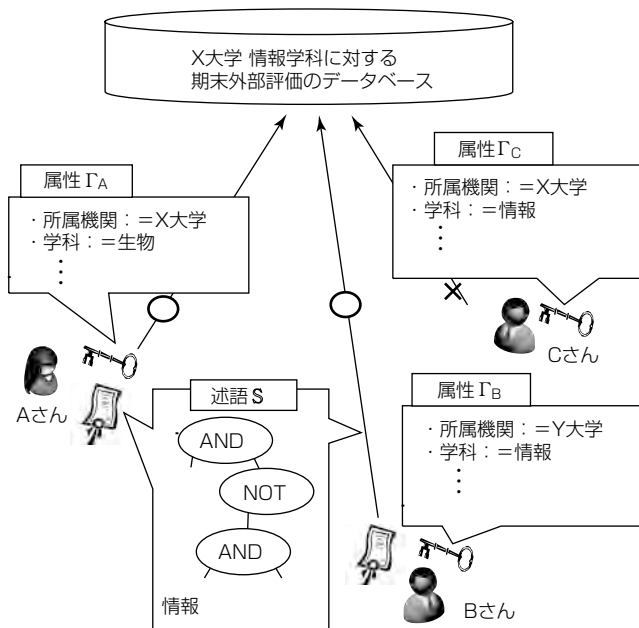


図4. 匿名評価(アンケート)への属性ベース署名の応用

できる。

例えば、各ユーザーは、社員証ICカードのような個人属性を形作る秘密情報(及びそれを格納した媒体)を用いて、様々なデータの認証を行う。例えば、X大学に属するAさんの属性情報が、“所属機関=X大学、所属学科=生物、ポジション=ポスドク、年齢=30、性別=女性…”と与えられている場合を考える。彼女は、その属性情報が満たす任意の条件式で匿名性をコントロールして、署名を作成できる。例えば、“条件式=(所属機関=X大学) AND (所属学科=生物)”といった条件式を用いて、自分の身元保証を行うことができる。図4では、X大学情報学科に対する期末外部評価を投稿する際に匿名で署名を行う場合を示している。情報学科所属以外の人のみが許されるアンケート調査であるので、Aさん及びBさんは評価結果を正当に投稿できるが、CさんはX大学情報学科に所属しているので、評価結果を投稿できない。このように匿名での投稿を署名付きで行うことができるのが、属性ベース署名方式のメリットである。

5.2 分散型複数鍵発行センター方式

実際に、関数型暗号や属性ベース署名を使用する際には、個人の属性秘密鍵は、各管轄機関から発行してもらう属性証明書と密接に関連している場合が多い。例えば、勤務先からの在籍証明、警察からの運転免許、役所からの住民票に対応して、各属性秘密鍵が各機関から発行されて、それらが一まとまりとなって、個人の属性秘密鍵となる。その属性秘密鍵が、暗号・署名システムでの個人の権限を表すので、この鍵発行手続きを安全に行うことは大変重要である。

これまでは、安全性確保のために、信頼できる第三者機関と各鍵発行センターの間に事前秘匿通信が不可欠であった。しかし、参考文献(6)では、そのような事前通信が不要

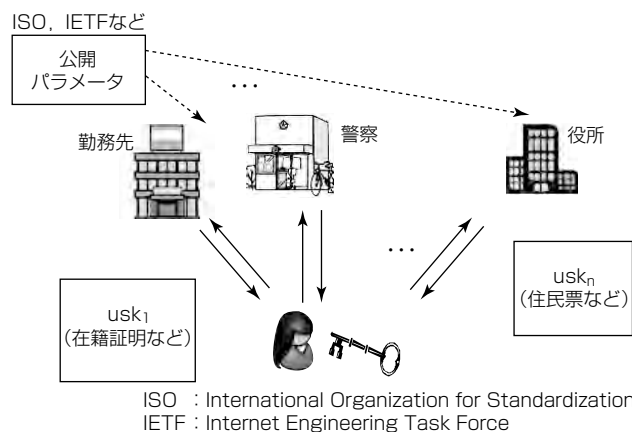


図5. 分散型複数鍵発行センター方式

で、複数機関が安全に鍵発行できるシステムを提案した。その応用範囲は広く、関数型暗号方式にも属性ベース署名方式にも適用可能である(図5)。

6. む す び

関数型暗号方式技術の最近の進展を概観した。今後も、効率性、安全性、機能性の各側面で改良を加え、実用化に寄与していく。

参 考 文 献

- (1) 日本電信電話(株), 三菱電機(株): クラウド時代の高度なセキュリティ対策を実現する新世代暗号方式を開発 (2010)
<http://www.mitsubishielectric.co.jp/news/2010/0728.pdf>
- (2) Okamoto, T. and Takashima, K.: Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, CRYPTO (2010)
<http://eprint.iacr.org/2010/563>
- (3) Okamoto, T. and Takashima, K.: Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption, CANS (2011)
<http://eprint.iacr.org/2011/648>
- (4) Okamoto, T. and Takashima, K.: Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption, EUROCRYPT (2012)
<http://eprint.iacr.org/2011/543>
- (5) Okamoto, T. and Takashima, K.: Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model, PKC (2011)
<http://eprint.iacr.org/2011/700>
- (6) Okamoto, T. and Takashima, K.: Decentralized Attribute-Based Signatures, ePrint (2011)
<http://eprint.iacr.org/2011/701>

高信頼量子暗号装置と量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェア

長谷川俊夫* 酒井康行***
 山中忠和*
 柴田陽一**

Highly Reliable Quantum Key Distribution System and its Application to One-time Pad Smartphone

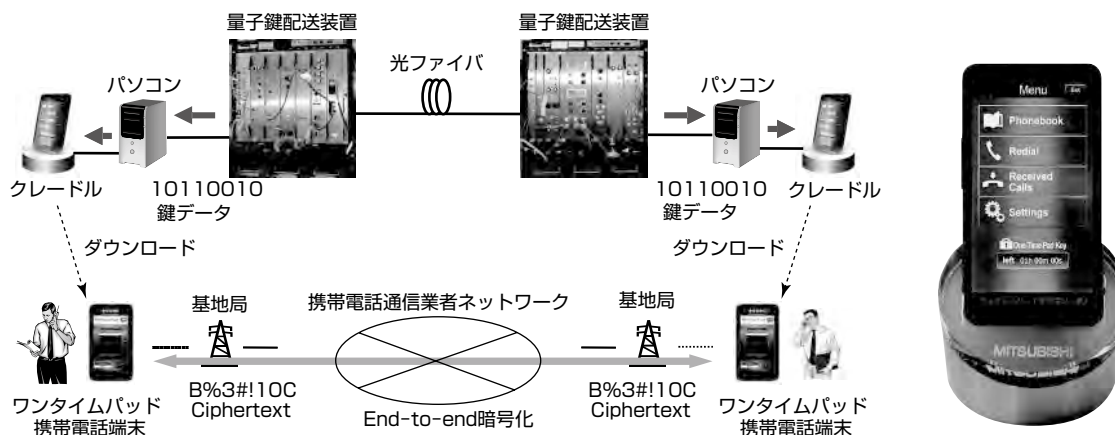
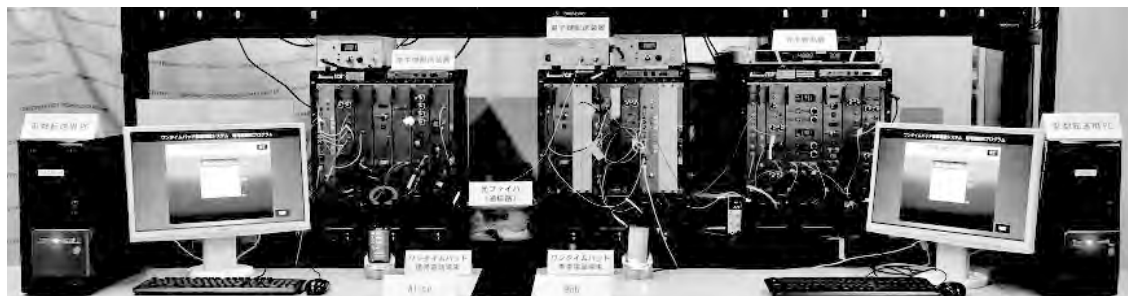
Toshio Hasegawa, Tadakazu Yamanaka, Yoichi Shibata, Yasuyuki Sakai

要旨

量子暗号は、物理の基本原理を利用したもので、物理法則で保証された究極の安全性(暗号の解かれ難さ)を実現する。量子暗号装置の実験や開発はこれまで積極的に行われており、また、理論面でも活発に研究が進められている。量子暗号を実用化するためには、敷設光ファイバ設備(フィールド)でも高い信頼性を実現することが課題である。このため、三菱電機では、量子暗号の実用化を目指して、安定性を高めた量子暗号装置の開発を行い、さらに、フィールド試験を実施した。敷設光ファイバでは、一般に、実験室と比較して伝送路の擾乱(じょうらん)などの影響が大きく、量子暗号装置の安定動作が困難であった。当社では、光伝送路で受ける揺らぎを自動補正することができる偏波補償モジュールを始め、平面光回路を用いて0.01℃の高い精度で温度制御を行うことによって安定動作する干渉計の

構築、さらに、-40℃に電子冷却した低ノイズ小型光子検出器等の開発に取り組み、敷設光ファイバでも高い安定性を実現する量子暗号装置を開発した。

また、量子暗号のアプリケーションとして携帯電話(スマートフォン)への適用も行った。量子暗号によって暗号鍵を携帯電話端末間で共有(量子鍵配送)し、この鍵を用いて携帯電話端末間の通話を暗号化するワンタイムパッド携帯電話ソフトウェアを開発した。現状の量子暗号技術では、量子鍵配送自体は通信距離100km程度までしか実現できないが、今回のモバイルアプリケーション開発によって、この距離制限にとらわれず量子暗号技術を展開することが可能となった。これまで、量子暗号は、適用できるアプリケーションが必ずしも明らかではなかったが、1つの身近なアプリケーションを示すことができた。



高信頼量子暗号装置と量子鍵配送を用いたワンタイムパッド携帯電話アプリケーション

上図は、量子鍵配送を用いたワンタイムパッド携帯電話のシステム全体写真である。また、左下図は量子暗号装置からワンタイムパッド携帯電話への鍵のダウンロードの流れと端末間のEnd-to-endの暗号化通信の仕組みである。右下図はワンタイムパッド携帯電話である。

1. ま え が き

量子暗号は、究極の安全性を実現する暗号技術である。現代暗号は、将来、量子計算機のような超高速な計算機が実用化されると解読できてしまうという課題があるが、量子暗号は物理の基本原理を利用したもので、物理法則で安全性が完全に保証されている。量子力学と情報処理を融合した量子情報技術の中でも、量子暗号技術は最も多く実験や量子暗号装置の開発が行われており⁽¹⁾⁽²⁾⁽³⁾、理論面でも活発に研究が進められている。実用化のためには、敷設光ファイバ設備(フィールド)でも高い信頼性を実現することが必要である。その実現のため、当社は種々の安定化技術を開発し、これを適用した高信頼量子暗号装置の開発を行い、フィールド試験を実施した。

本稿では、量子暗号の実用化に向けた当社の取組みとして、安定性を高めた装置開発とそのフィールド適用について述べる。また量子暗号の1つのアプリケーションとして当社が開発した携帯電話への応用についても述べる。

2. 高信頼量子暗号装置とフィールド適用

2.1 高信頼量子暗号装置の開発

敷設光ファイバ設備では、一般に、伝送路上の温度変化や種々の擾乱によって、伝送される光子の到着タイミングずれや偏光状態の変化が生じる。そのままだと量子暗号装置で量子誤り率(Quantum Bit Error Rate : QBER)が増大し、鍵生成速度が低下又は生成できなくなるなど、安定した鍵生成動作が保証されないことになる。このため、今回、光伝送路での(偏波などの)揺らぎなどを自動補正できる偏波補償モジュールを始め、送受信側で平面光回路(Planar Light Circuit : PLC)を用いて0.01℃の高い精度で温度制御を行うことで安定した干渉計を構築する等、幾つかの技術によって敷設光ファイバでも高い安定性を実現する装置開発を行った⁽⁴⁾⁽⁵⁾⁽⁶⁾。その内容について、具体的に述べる。

2.1.1 設計方針

数十km程度の都市圏ネットワークで、実用的な量子暗

号装置の実現を目指して設計開発を行った。次の各項目について、設計方針を述べる。

- (1) 伝送路損失10dB程度の通信路環境
- (2) 高安定性
- (3) 高速性(駆動速度100MHz程度)
- (4) 波長多重機能
- (5) 小型化

(1)に関しては、都市圏ネットワークでの運用を考慮し、通信距離50km程度(光ファイバの損失を0.2dB/km程度として伝送路損失10dB程度)で実用に耐え得ることを目標とする。(2)に関しては、伝送中の偏波揺らぎや温度変化による伝送路の伸縮等の影響があっても安定動作することを目指す。今回、一方向型の光学系を採用しているが、送受信側で構成する干渉計の安定化を図るため、PLCを用いて高い精度で温度制御することで実現する。(3)の高速性に関しては、100MHz程度で光源、位相変調器、光子検出器の駆動を行う。なお、位相変調では、ダイパルス型の電気信号での制御方式を新たに開発し、DC(Direct Current)フロアの変動なく安定かつ高精度の位相変調を実現する。(4)の波長多重に関しては、量子暗号では一般にタイミング同期のため通常の強度の強い光(古典光)の伝送も同時に行うが、ここで必要となる強度が大幅に異なる光(古典光と微弱光である量子光)の波長分離も実現する。波長分離で100dB程度のチャンネルアイソレーションを実現するDEMUX(DEMUltipleXer)装置を開発した。(5)の小型化に関しては、光子検出器は超伝導検出器のように極低温冷却が必要で大型・高価なものではなく、市販APD(Avalanche Photo Diode)を用いた電子冷却可能な温度で動作する小型装置を構築する。また、量子暗号で最終的に安全な鍵を生成するために必要な処理である鍵蒸留処理に関しては、専用ハードウェアを必要とせず、通常のパソコン上のソフトウェア実装で対応できることを目指した。

2.1.2 実験系

量子暗号装置の構成を図1に示す。プロトコルは、微弱コヒーレント光を用いたデコイ方式(真空含み4種類の光

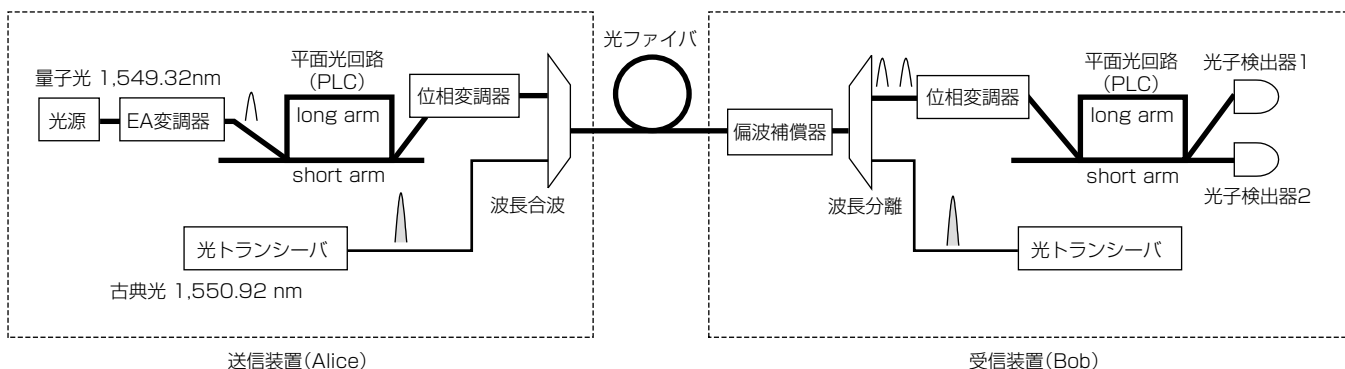


図1. 高信頼量子暗号装置の構成図

強度)で実装した。デコイ方式は、基本はBB84方式(BennettとBrassardが1984年に提案した量子暗号の代表的な方式)であるが、送信者Aliceが信号中に“おとり(decoy)光パルス”をある確率でランダムに混ぜて送るものである。今回用いる信号光とdecoy信号の光強度として、パルスあたりの平均光子数 $\mu = 0.63, 0.3, 0.1$, 真空を用いた。光源はDWDM(Dense Wavelength Division Multiplexing)DFB(Distributed FeedBack)Laserを用い、100MHzで電気吸収型(EA)変調器を駆動しパルス光としている。量子光波長を1,549.32nm, 古典光波長を1,550.92nmとした。光学系は一方向型を採用した。この系では一般に干渉計を安定に保つのが課題であるが、送信側、受信側でPLCを用いることで高精度な温度制御を行い、系全体の安定性を実現した。干渉計は500MHzのものを使用した。

また、タイミング同期のため古典光を量子光に加え波長多重を行う機能と、100dB以上の高いチャンネルアイソレーション性能を持つ波長分離モジュールを開発した。さらに、量子光の伝送中の偏波揺らぎなどを補償するために、強度の強い古典光を用いて微弱な量子光の偏波補償を行うモジュールを開発し搭載した。高速性の実現のため、先に述べたとおり、位相変調では、高速かつ安定して変調を行えるよう、ダイパルスによる高速位相変調を行っている。

2.1.3 光子検出器

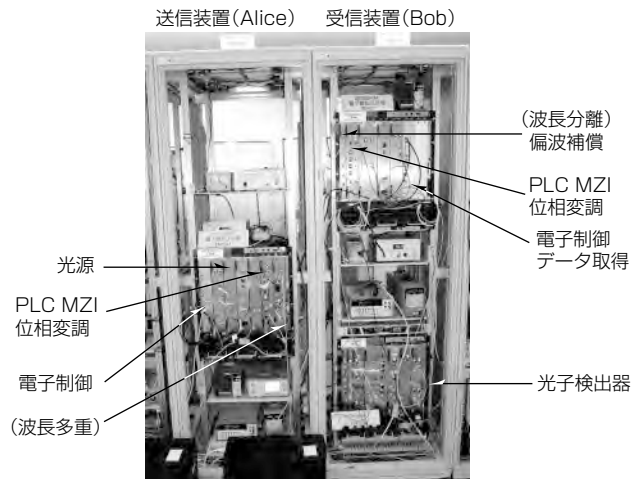
小型化を重視し、市販のAPDを用いて駆動速度100MHzで動作する光子検出器を開発した。-40℃まで電子冷却し、検出方式は自己差分方式他を用いて実現した。1クロック(今回はT=10ns)ずれた出力波形との差分をとりノイズキャンセルすることで、微弱な光検出信号も効率良く抽出することができる。性能は検出効率数%(3~12%), 暗計数率 10^{-5} 以下(6×10^{-6})を実現した。

2.1.4 鍵蒸留処理

鍵蒸留処理は、誤り訂正にLDPC(Low Density Parity Check Code)符号を採用し、高い効率を実現した。また、漏洩(ろうえい)情報を無効化する秘匿性増強処理にはToeplitz行列を用い、その実装で高速演算アルゴリズムを用いることで計算量を $O(n^2)$ から $O(n \log n)$ に落とすことができた。これによって、有限長の効果を考慮した場合、ブロック長として1Mビット程度必要となるが、その場合でもFPGA(Field Programmable Gate Array)などの専用ハードウェアが不要であり、通常のパソコン上でのソフトウェア実装だけで高速に実現できた。

2.2 敷設光ファイバ設備JGN2plusへの適用

損失や擾乱が大きい実際の都市圏光ファイバ設備で、開発した量子暗号装置を試験評価することが必要である。今回、(独)情報通信研究機構(NICT)のJGN2plusテストベットの大手町-白山の往復路(距離24km, 伝送損失13dB)で、フィールド実験を行った(図2)。当初設計では10dB程度



MZI : Mach-Zehnder Interferometer

図2. 敷設光ファイバ設備での実験

の通信路損失に耐え得る量子暗号装置として開発したが、実際のフィールド試験を行った環境は通常の光ファイバよりかなり損失の大きな回線であり、より厳しい条件での試験となった。しかし、この環境下でも、鍵生成速度10Kbps, QBER4.5%, 最終鍵生成速度2Kbpsの性能を得ることができた。敷設光ファイバ設備では、外気温の変化による顕著な伸縮もあるが、このような環境下でも開発した量子暗号装置が動作することが確認できた。なお、鍵生成速度は通信距離(伝送路損失)とトレードオフにあり、例えば、通信距離10km程度の場合、数十Kbpsとなる。また、この鍵を用いて、日本電気株、日本電信電話株、NICT等の他機関との鍵リレー及びネットワーク接続実験を行い、正常に動作することを確認することができた⁽⁴⁾⁽⁵⁾⁽⁷⁾。数日間の連続動作は確認済みであり、今後、更に長期間の連続安定動作を目指す。

3. 量子暗号のアプリケーション

高信頼量子暗号装置開発に加え、量子暗号のアプリケーションの1つとして携帯電話への適用を図った。

現在の携帯電話では、端末と基地局との間の無線通信区間で、現代暗号を用いて通話を暗号化することによって、盗聴を防止している。しかし、基地局で一旦復号されるため、その先の携帯電話通信事業者が運営する基地局間無線通信区間や事業者間を接続するネットワークで、盗聴される危険性が皆無とは言えない。盗聴を確実に防止するためには、端末で暗号化し相手の端末で復号する方法によって、相対する端末間の全区間で暗号化を行うことが有効である。このような暗号化通信を行うためには、暗号鍵を端末同士で安全に共有する技術が不可欠である。

これらの問題を解決するために、量子鍵配送と携帯電話とを連携させることで、通話の盗聴が原理的に不可能な携帯電話ソフトウェアの開発に成功した⁽⁵⁾⁽⁶⁾⁽⁸⁾⁽⁹⁾。

図3に、今回開発した量子鍵配送を用いたワンタイムパッド携帯電話の仕組みを示す。

- ①最初に、携帯端末同士で暗号鍵を安全に共有するために、光伝送路(光ファイバ)を使い、量子鍵配送を用いて量子暗号装置間で暗号鍵を絶対安全に共有する。
- ②次に、この鍵を各々の携帯端末にクレードル経由でダウンロードし、携帯端末間で暗号鍵を共有する。
- ③最終的に、通話の際に、携帯端末上でこの暗号鍵を用いて音声通話をワンタイムパッドで暗号化する。これによって、端末間の全ての区間でEnd-to-endの秘匿通話が実現できる。

このアプリケーションの詳細は次のとおりである。

音声通話は、データ通信(VoIP(Voice over Internet Protocol))を利用し1KB/sでエンコードしている。音声通話の暗号化は、ワンタイムパッド暗号を用い、音声データと同じ長さの暗号鍵を用いて暗号化する。このため、一般には長いデータサイズの鍵が必要となる。

例えば、10分間の通話では、1.2MBの暗号鍵を事前に共有する必要がある。ワンタイムパッド携帯電話端末は、ダウンロード時にワンタイムパッド用の暗号鍵を補充するが、例えば、2GBのSDカードがあれば、1回の鍵のダウンロードで10日間連続通話可能となる。これは運用上、十分実用的と考えられる。

ワンタイムパッド方式はデータと同じ長さの乱数を鍵として使用し、一度使った鍵は二度と使わないというものである。通話の暗号化に用いる暗号鍵を使い捨てにすることによって、万一端末を紛失したり盗まれたりした場合でも、過去の通話記録からの復号は不可能である。このように、このワンタイムパッド携帯電話ソフトウェアでは、端末の紛失・盗難対策が厳重にほどこされている。

今回、ワンタイムパッド携帯電話ソフトウェアは、Microsoft Windows Mobile^(注1)を搭載した端末上のソフトウェアとして開発したため、特定のハードウェアに依存しない。このため、このOSを搭載した様々な携帯端末で利用可能である。

また、現状では、量子暗号装置は通信距離が100km程度までであり、通信距離に制約がある。さらに、量子鍵配送では大規模な量子暗号装置が必要であるため、一般にこの装置を利用できる場所は限られる。しかし、このアプリケーションを用いることによって、これまで存在していた量子暗号装置の通信距離の制限や場所の制約等の課題を克服し量子暗号の究極のセキュリティがどこにいても利用可能になる。

(注1) Windows Mobileは、Microsoft Corp.の登録商標である。

4. む す び

当社の量子暗号の実用化に向けた取組みとして、安定性を高めた量子暗号装置開発とそのフィールド適用について述べた。また、量子暗号のアプリケーションとして、当社が開発した携帯電話向け応用ソフトウェアについて述べた。

装置開発では、実用化のために、フィールドでも高い信頼性を実現することが必要である。その実現のために、種々の安定化技術を開発し、これらを適用した高信頼量子暗号装置開発を行い、フィールド実験を実施した。また、量子暗号を実際に活用するためには、有用なアプリケーションが必要であるが、携帯電話への応用について初めて取り組んだ。当社では、量子暗号などの研究開発だけでなく、“MISTY”などの現代暗号を始め情報セキュリティ分野で様々な開発を行ってきた。これらの経験やノウハウ等が、量子暗号を身近な携帯電話(スマートフォン)に応用すると

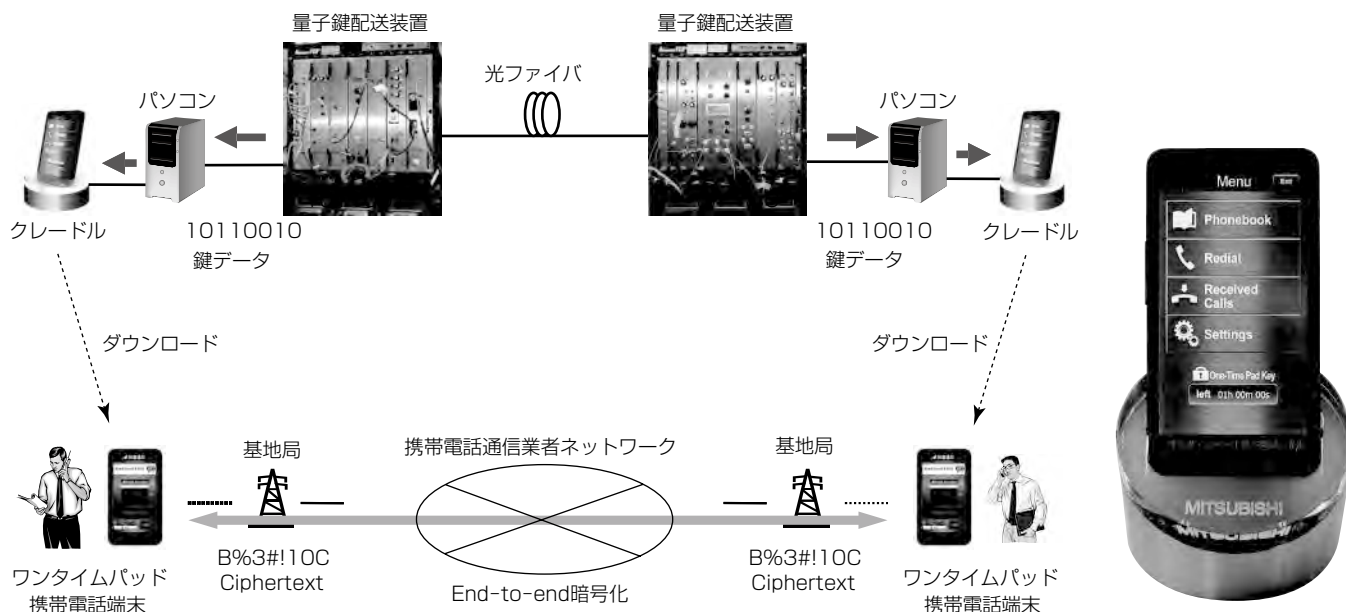


図3. 量子鍵配送を用いたワンタイムパッド携帯電話の仕組み

いう今回の開発につながった。

量子暗号の実用化には、まだ解決しなければならない課題が幾つかある。ハードウェア面では量子暗号ネットワーク試験運用プロジェクトのフィールド試験で安定した通信を実現することができたが、量子暗号装置の光子検出器の性能改善や、伝送路のゆらぎを補償する偏波補償やフィードバック制御等によって、速度や通信距離・安定性の更なる向上に今後も取り組む予定である。また、ワンタイムパッド携帯電話ソフトウェアについては、最新スマートフォンOSへの対応を進めるほか、“いつでもどこでも安全に通話できる”という理想の通信環境を実現するために、研究開発及び改良を進めていく予定である。

なお、この開発の一部はNICT委託研究の成果である。

参考文献

- (1) Hasegawa, T., et al.: Field experiments of quantum cryptosystem in 96km installed fibers, CLEO/Europe-EQEC2005, EH3-4, Munich (2005)
- (2) 長谷川俊夫, ほか: 宇宙量子暗号通信の概念検討, 第52回宇宙科学技術連合講演会 2F03 (2008)
- (3) 長谷川俊夫, ほか: 宇宙量子暗号通信ミッションの予備設計, 第53回宇宙科学技術連合講演会 3D14 (2009)
- (4) 長谷川俊夫, ほか: 高信頼量子暗号装置の開発, SCIS2011, 4F2-6 量子セキュリティ (2011)
- (5) Sasaki, M., et al.: Field test of quantum key distribution in the Tokyo QKD Network, Optics Express, **19**, No. 11, 10387~10409 (2011)
- (6) 長谷川俊夫, ほか: 高信頼量子暗号装置の開発とアプリケーション, 第58回応用物理学関連連合講演会シンポジウム, 24a-BT 量子情報: 高まる技術と深まる科学, 4 (2011)
- (7) 三菱電機プレスリリース 2010.10.14: 量子暗号ネットワークの試験運用開始 (2010)
<http://www.mitsubishielectric.co.jp/news/2010/1014-a.pdf>
- (8) 柴田陽一, ほか: ワンタイムパッド携帯電話システムの開発, 第74回情報処理全国大会 1F-4 (2012)
- (9) 三菱電機プレスリリース 2010.09.02: 量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェアを開発 (2010)
<http://www.mitsubishielectric.co.jp/news/2010/0902.pdf>

統合ログ管理ソリューション “AnalyticMart for LogAuditor”

和田貴成*
大塚哲史*
阿波基文*

Integrated Log Management System "AnalyticMart for LogAuditor"

Takashige Wada, Tetsufumi Otsuka, Motofumi Awa

要 旨

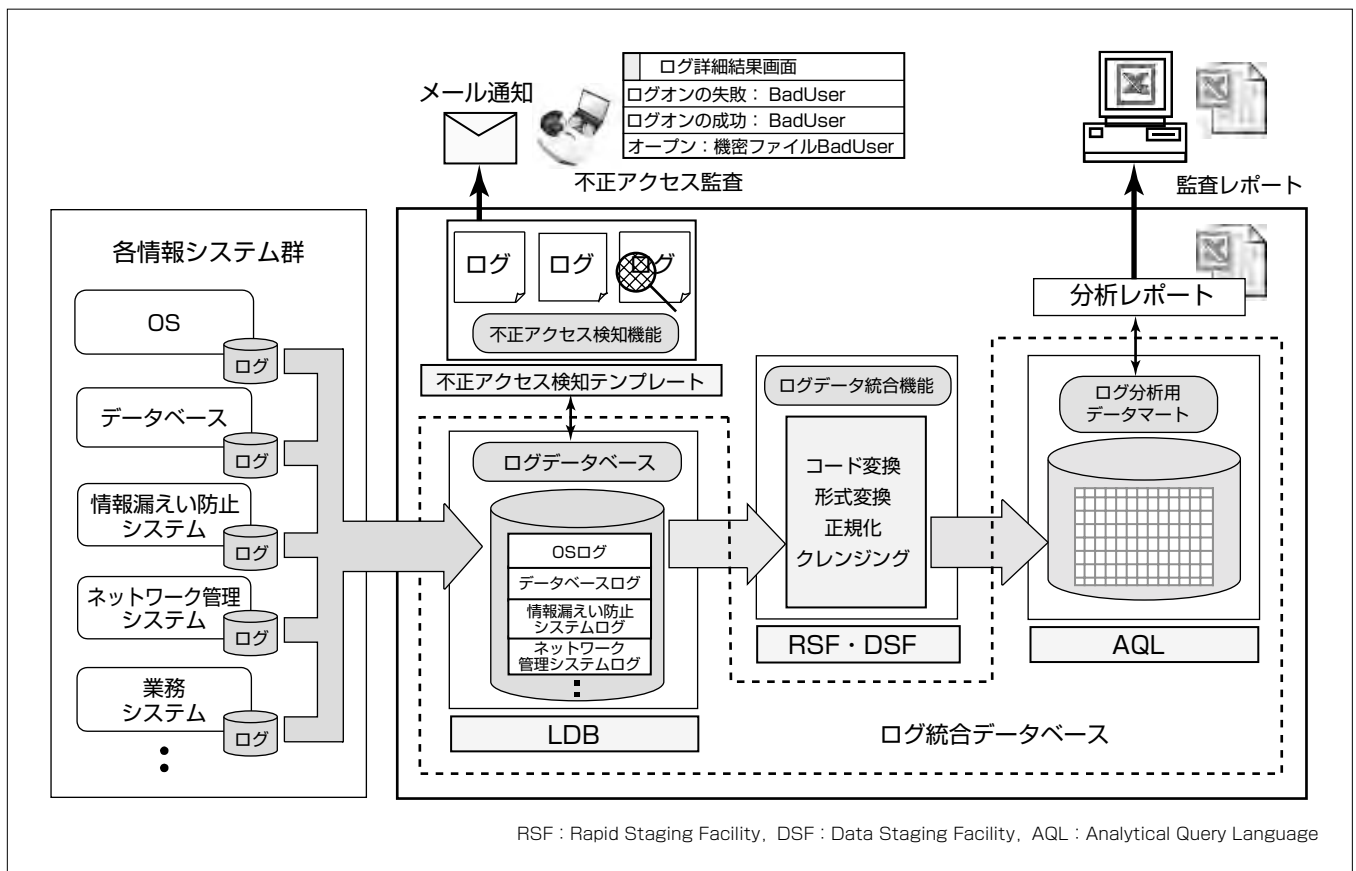
近年、内部統制やセキュリティ等、様々な側面からログ管理の必要性が高まっている。その中で、蓄積したログをうまく活用できない、活用に関数がかかる、統合ログ管理システムの必要性は理解できるが費用対効果が見えにくく、導入の敷居が高いといった問題が現れてきた。

三菱電機インフォメーションテクノロジー(株)(MDIT)の統合ログ管理ソリューション“AnalyticMart for LogAuditor”は、これらの課題を解決する統合ログ管理製品である。

AnalyticMart for LogAuditorは、ログを管理するため

標準的なコンポーネントをあらかじめセットにし、導入しやすくした製品である。この製品の特長を、次に示す。

- (1) 可変長、不定形型等、各種形式のログデータを1個のデータベース(Log DataBase:LDB)で一元管理
- (2) LDBに対し、横断検索することによって、不正アクセスの一連動作を高速に追跡することが可能
- (3) “不正アクセス検知テンプレート”の利用によって、複数OSのログ管理を容易に実現でき、不正アクセスの証跡に相当するログデータを効率的に見つけ出すことが可能



“AnalyticMart for LogAuditor”のシステム構成

AnalyticMart for LogAuditorは、統合的にログを保管するLDB、主にログの加工を行うRSF・DSF、統合的なログの分析エンジンであるAQLから構成される。また、分析フロントエンドとなるMicrosoft Excel^(注1)アドインツールDIAOLAP、さらに、監視条件に基づいて管理者に対しメール通知をする不正アクセス検知テンプレートが提供される。

(注1) Excelは、Microsoft Corp.の登録商標である。

1. ま え が き

近年、内部統制(コンプライアンス遵守など)徹底の高まりや、数多く報告される個人情報漏えいなどのセキュリティ事故を背景に、様々な側面からログ管理の必要性が高まっている。企業の内部統制(IT全般統制)では、企業内の各情報システムから出力されるアクセス・操作・メール送受信等の履歴が、情報漏えい事件などが発生した場合の監査証跡として重要度が増している。そのため、ログを蓄積する作業自体は多くの企業で始まっている。しかし、ログ管理システムの導入・運用が進んでいく中で、蓄積したログを十分に活用できない、活用に手間がかかる、統合ログ管理システムの必要性は理解できるが費用対効果が見えにくく導入の敷居が高いといった問題が表面化してきた。

MDITでは、システムログ・アクセスログ・セキュリティログ等の様々なログを証跡として収集・蓄積し、一元管理するAnalyticMart for LogAuditorを開発し、これらの課題を解決した。

本稿では、統合ログ管理を低コストで容易に実現できることを特長とする不正アクセス検知テンプレートを中心に、AnalyticMart for LogAuditorの特長、機能について述べる。

2. ログ管理の課題

日本版SOX法(米国企業改革法)成立以降、内部統制を実現するために、多くの企業がログ管理システムを導入し、企業内で発生するログの蓄積を開始している。しかし、ログ管理を行う上で、次のような課題が顕著になってきた。

- (1) 日本版SOX法の施行によって、ログの収集自体は開始したが、分析はほとんど行わずに蓄積するだけの運用になっている。
- (2) システム単位でログを管理しているため、ログの集約や紐(ひも)付け等を手作業で実施する必要があり、手掛かりを掴(つか)むためのログ解析に膨大な時間がかかる。
- (3) 統合ログ管理製品は導入・運用のためのまとまったコストが必要となるため、すぐには導入ができない。

AnalyticMart for LogAuditorは、これらの課題を解決し、多種で大量のログの効率的な統合管理を実現する。

3. AnalyticMart

3.1 AnalyticMartとは

AnalyticMartは、販売分析、顧客分析、ログ分析、環境データ分析といった多様で形式の異なるデータの分析を、統一したアーキテクチャで効率よく低コストで実現でき、かつ中小規模から大規模まで、規模に合わせたデータ分析システムの構築・運用を可能とするフレームワークである。

AnalyticMart for LogAuditorは、AnalyticMart製品ラインアップの中からログを管理するための標準的なコンポ

ーネントをあらかじめセットにし、導入しやすくした製品である。また、多様なテンプレートが使える拡張性とログ数に依存しないライセンス体系を備えた製品となっている。

次に、AnalyticMart for LogAuditorの特長を挙げる。

- (1) 可変長、不定形型等、各種形式のログデータを1個のデータベース(LDB)で一元管理
- (2) LDBに蓄積した複数種類のログに対し、共有キーワードで横断検索することによって、情報漏えいに至るまでの一連動作を高速に追跡することが可能
- (3) 不正アクセス検知テンプレートを利用することによって、複数OSのログ管理を低コストで容易に実現することが可能

3.2 製品の構成と機能

AnalyticMart for LogAuditorは、統合的にログを保管するLDB、統合的なログの分析エンジンであるAQL、主にデータの加工・変換機能を提供するRSF・DSFで構成している。さらに、分析フロントエンドとなるMicrosoft ExcelアドインツールDIAOLAP、不正アクセス検知テンプレート、ISMS(Information Security Management System)監査作業支援に利用できるISMSテンプレート(オプション製品)を提供する。それらのコンポーネント、動作環境について表1、表2に示す。

(1) LDB

LDBは、非構造化データを蓄積するのに最適なDBMS(DataBase Management System)であり⁽³⁾、テラバイト超の大規模ログにも対応可能な高速蓄積と正規表現指定による高速検索機能を持つコンポーネントである。

LDBは、中国語、韓国語等を含むログデータに対応し、文字コードとしてUTF-8をサポートした。

表1. AnalyticMart for LogAuditorの構成コンポーネント

コンポーネント	機能
LDB	統合ログデータの蓄積保管・監視 高速な検索
AQL	分析用ログデータの保存 高速な検索・集計
RSF, DSF	ログデータの収集と加工、取り込み
DIAOLAP	分析テンプレートなどによる定型レポート 非定型分析レポート
不正アクセス検知テンプレート	監査条件の設定 不正アクセスログ高速検索、メール通知
ISMSテンプレート	ネットワークセキュリティ管理テンプレート 監査ログ管理テンプレート

表2. AnalyticMart for LogAuditorの動作環境^(注2)

サーバ	Microsoft Windows Server 2008 R2
クライアント	Microsoft Windows 7 Professional/Enterprise Microsoft Windows Vista Business Microsoft Windows XP Professional

(注2) Windows, Windows Server, Windows Vistaは Microsoft Corp.の登録商標である。

(2) AQL

AQLは、データ分析プラットフォームとして十年以上の実績を持つ高性能DBMSであり、集計・分析に適した構造化データとしてログを保存し、高速なデータ検索・集計が可能なコンポーネントである。

AQLは、近年更に増大するデータに対応し、ロード性能、データ圧縮性能の向上を実現した。

(3) RSF, DSF

RSFは、企業内に存在する様々なログデータを収集・加工するツールであり、次の特長を持つ。

- ①きめ細かいデータの加工・編集機能
- ②高い生産性・保守性
- ③サポートするデータソースは、各種ログを格納した主要RDB(Relational DataBase)、又はCSV(Comma Separated Values)などのフラットファイル

DSFは、RSFによる加工済みデータに対して、高速にジョイン(列の結合)を行うコンポーネントである。

(4) DIAOLAP

DIAOLAPは、AQLの分析用フロントエンドであり、分析レポートの作成を可能とするExcelアドインツールを提供し、次の特長を持つ。

- ①使い慣れたExcelからシームレスに利用可能、集計表(ピボットテーブル)を自動生成
- ②柔軟な非定型分析、ウィザード形式での容易な操作
- ③集計値から明細の分析データに遡るドリルスルー機能

(5) 不正アクセス検知テンプレート

不正アクセス検知テンプレートは、内部統制における標準的な不正アクセスの検知を、低コストで容易に実現できる製品である。5章で詳細を述べる。

(6) ISMSテンプレート

ISMSテンプレートは、ISMS監査レポートの作成を支援するテンプレート製品である。対象は、Webアクセスログ、ファイアウォール、RDBへのセッションログ、及びSQL(Structured Query Language)文実行ログ等、各分野の代表的な管理ソフトウェアから発生するログ計8種類である。

4. AnalyticMartの高速処理技術

AnalyticMartでは、LDBとAQLを支える次の主要な高速処理技術⁽¹⁾によって、プロセッサ数に応じたスケーラビリティの高いシステムを提供している。

- (1) 必要なストレージ容量を10分の1程度に削減するデータ圧縮技術
- (2) 複数のプロセッサによる圧縮・伸張・検索処理や、複数のストレージに自動的に分散配置されたデータの入出力処理を効率的に処理することができる並列処理技術

- (3) sDFA(size-reduced Deterministic Finite Automaton)方式⁽⁴⁾によって、条件式規模によらずほぼ1億文字/秒の高速処理を実現する高速文字列照合技術

5. 不正アクセス検知テンプレート

(1) 目的

不正アクセス検知テンプレートは、主に、次の2項目を実現することを目的に開発した製品である。

①内部統制上の標準的な不正アクセスの検知

内部統制(IT全般統制)上の標準的な不正アクセスには、表3に示す項目などが挙げられる。

不正アクセス検知テンプレートは、ファイルサーバへのログイン成功、ログイン失敗、機密ファイルのアクセス等のアクセスログ管理を容易に実現できるフレームワークを持っているため、表3の“ファイルの不正アクセス”“不正侵入”“パスワード搾取”を検知することができる。

②テンプレート化による容易な導入

不正アクセス検知テンプレートは、複数OS(Windows Server, HP-UX^(注3), Solaris^(注4))のログを統合して管理できる製品であり、テンプレート化したことによって、導入コストの削減を実現している。また、ログ監査条件などの初期設定は、ブラウザベースのログ管理アプリケーションを通して行うことができ、統合ログ管理システムを容易に導入することが可能である。

(注3) HP-UXは、Hewlett Packard Co.の登録商標又は商標である。
(注4) Solarisは、Oracle Corp.及びその子会社、関連会社の登録商標である。

(2) 機能

不正アクセス検知テンプレートが保有する機能を次に示す。

①設定管理機能

監査条件及びメール通知先の設定、ログの詳細情報検索を、ブラウザベースのログ管理アプリケーションから利用することができる。

②運用機能

監査条件に基づいた検索、及び条件に一致した場合のメール通知を行うことができる。

(3) 運用例

不正アクセス検知テンプレートのシステム運用例について、次に述べる。

表3. 内部統制上の標準的な不正アクセス例

分類	例
ファイルの不正アクセス	セキュリティホールを悪用して、ファイルを盗み見・削除・改変する行為
不正侵入	バックドア(不正侵入を行うための裏口)などを仕掛け、そのパソコンを踏み台に他のパソコンへ侵入する行為
パスワード搾取	盗聴や総当たり攻撃によるパスワードの搾取
妨害攻撃	正常なアクセスを妨害するDDoS(Distributed Denial of Service)攻撃

まず、運用を開始するまでに、社内のポリシーや監査対象とするログの種類を考慮した上で、ログ監査条件をブラウザベースのログアプリケーションから設定する(図1)。入力項目は、ログの種類(Windowsセキュリティログ、HP-UXログイン/SUログ、Solarisログイン/SUログ計5種)、事象(ログオン成功、ログオン失敗、機密ファイルへのアクセス等計26種)、時間帯(00:00:00~23:59:59)、検出判定指標とその回数(検出判定指標は、連続で一定回数以上の検知、一定期間に一定回数以上等計4種)、監査ログ検知時のメール通知先である。なお、メール通知先に関しても、図2に示す“メール通知先設定画面”から容易に設定することができる。

この運用例では、監査対象サーバがWindows、HP-UX、Solaris各1台計3台であった場合に、次の3個の監査条件を設定して運用を開始したとする。

- ①Windowsサーバへの深夜時間帯ログイン失敗(5回連続)
- ②HP-UXサーバへの深夜時間帯ログイン失敗(5回連続)
- ③Solarisサーバへの深夜時間帯ログイン失敗(5回連続)

運用開始後、Windowsサーバに関する監査条件①が検知される事態が発生した場合、監査担当者(“メール通知先設定画面”の送信先アドレス項目指定者)に対してメールが通知される。メールを受信した監査担当者は、ログの詳細情報を取得するために、図3に示す“ログ詳細結果画面”を参照する。なお、図3は、複数OSのログに対して横断検索(条件:深夜時間帯)を行った検索結果である。この画面によって、ユーザーBadUserが、深夜時間帯にWindowsサーバへのログイン操作を5回連続で失敗していることを確認できる。また、その直後に、これとは異なるアカウント名によるHP-UXサーバに対する3回連続のログイン失敗が記録されており、これは、監査条件に合致した操作(この例の場合、監査条件①②③に該当する操作)以外にも不正な操作を試みた可能性があるかと推察することができる。

このように、複数OSのログを対象にした横断検索が実行できるため、事前に設定した監査条件以外にも、今後大きな問題につながる可能性のある兆候を見つけ出すことができる。

なお、調査の過程で取得した情報は、情報漏えいが発覚した際の監査証跡や、今後のセキュリティ管理策の検証や見直し等に活用することができる。

6. む す び

多種多様なログの統合管理を実現するAnalyticMart for LogAuditorについて述べた。また、複数OSのログ管理を低コストで容易に実現する“不正アクセス検知テンプレート”を開発した目的・備える機能・運用例についても述べた。今後は、統合ログ管理の多様なニーズにこたえるため、対応するログの種類の実装化を図る予定である。

ログ監査条件設定画面	
検知条件	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
検知条件名	Windowsセキュリティログ_ログオン失敗
ログの種類	Windows2000,2003_security
事象	ログオン失敗 (ID=529)
時間帯指定	00:00:00~05:00:00
検出判定指標	一定回数以上の検知 5回
メール通知先	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 default設定

図1. ログ監査条件設定画面

メール通知先設定画面	
送信元アドレス	WinError@mdit.co.jp
送信先アドレス	AuditUser@mdit.co.jp
件名	不正アクセス発生通知
本文	Windowsサーバで不正アクセスが発生しました。
SMTPサーバ	SmtptServer
SMTPポート番号	25
最大添付ファイルサイズ	10.240KB以内

SMTP: Simple Mail Transfer Protocol

図2. メール通知先設定画面

ログ詳細結果画面	
Bad2User/dev/pts/4: Wed Nov 16 02:24:30 2011,2011/11/16 02:24:30>LoginError.SOLARIS	
Bad2User/dev/pts/4: Wed Nov 16 02:24:44 2011,2011/11/16 02:24:44>LoginError.SOLARIS	
失敗の監査 529 2011/11/16 02:28:01 ログオンの失敗:パスワードが無効。ユーザー名: BadUser	
失敗の監査 529 2011/11/16 02:28:10 ログオンの失敗:パスワードが無効。ユーザー名: BadUser	
失敗の監査 529 2011/11/16 02:29:21 ログオンの失敗:パスワードが無効。ユーザー名: BadUser	
失敗の監査 529 2011/11/16 02:29:33 ログオンの失敗:パスワードが無効。ユーザー名: BadUser	
失敗の監査 529 2011/11/16 02:30:17 ログオンの失敗:パスワードが無効。ユーザー名: BadUser	
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:34:2011/11/16 02:34:32>LoginError.HP-UX	
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:34:2011/11/16 02:34:54>LoginError.HP-UX	
Bad3User pts/ta 10.100.211.213 Wed Nov 16 02:35:2011/11/16 02:35:22>LoginError.HP-UX	

図3. ログ詳細結果画面

参 考 文 献

- (1) 郡 光則, ほか: 多種多様なログの統合管理を実現するLogAuditor Enterprise, 三菱電機技報, 80, No.10, 615~618 (2006)
- (2) Sah, A.: A New Architecture for Managing Enterprise Log Data, Proc. of LISA 2002, 121~132 (2002)
- (3) 中村隆顕, ほか: 大規模ログデータベースの実現、情報処理学会全国大会第68回, 1D-2 (2006)
- (4) 中村隆顕, ほか: 大規模正規表現の高速照合方式、情報処理学会全国大会第67回, 4F-5 (2005)
- (5) 藤村 隆, ほか: 情報のリスク管理・内部統制を支援するコンプライアンス推進ソリューション, 三菱電機技報, 80, No.4, 281~284 (2006)

竹林信博*
柴田幸治*
山本隆二*

Webアプリケーション脆弱性への取組み

Approach to Web Application Security

Nobuhiro Takebayashi, Yukiharu Shibata, Ryuji Yamamoto

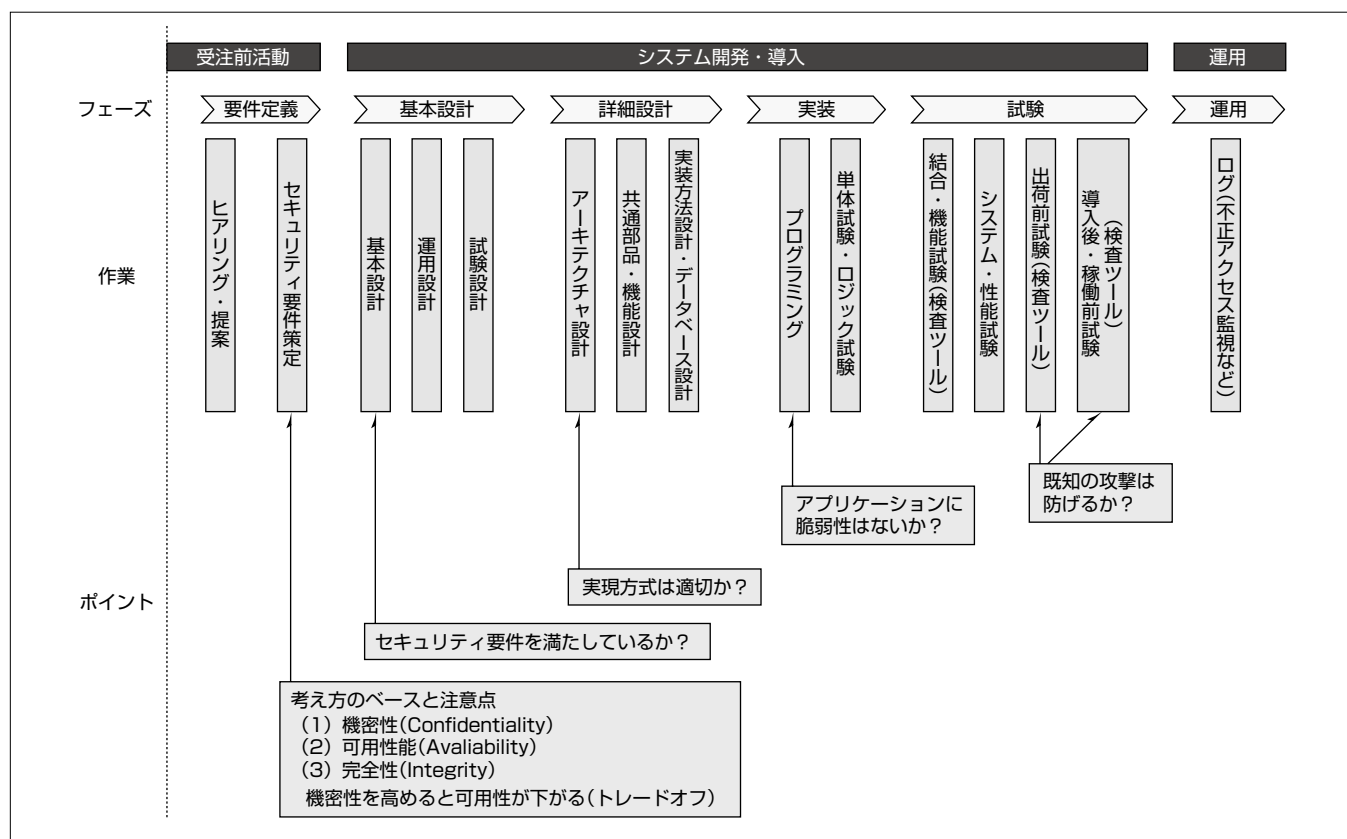
要旨

企業において、EC(Electronic Commerce)、EDI(Electronic Data Interchange)、SNS(Social Networking Service)、情報公開などのインターネットシステムは、SFA(Sales Force Automation)、CRM(Customer Relationship Management)に連携可能であるなどWeb(World Wide Web)ビジネスの一端を担う重要な要素であり、端末にアプリケーションをインストールしなくてもシステムを稼働できるWebアプリケーション導入が多くなってきている。近年はクラウドコンピューティングへの移行を始めている企業も見られ、インターネットシステム活用が更に増えることになろう。

一方、サイバー攻撃は年々高度化・複雑化・悪質化して

おり、最近では企業内の重要情報の不正な取得を目的として特定の標的に対して行われる標的型攻撃が出現するなど、常にセキュリティの脅威にさらされている。万一セキュリティ事故を起こした場合その影響は計りしれないものであり、失墜した信用や信頼の回復に長い時間と莫大(ばくだい)なコストを費やすことになる。

(株)三菱電機ビジネスシステム(MB)では、Webアプリケーション脆弱(ぜいじゃく)性対策に関して、インターネットシステム構築時の上流フェーズである要件定義や基本設計から、下流フェーズであるシステム試験や出荷前試験にいたる作業工程を見直し、またセキュリティ検査を多重に行うことで、品質向上に取り組んでいる。



Webシステム開発時におけるWebアプリケーション脆弱性への取組み

Webアプリケーションの脆弱性を防ぐためには、上流フェーズから下流フェーズまでの一貫した対策が必要である。要件定義フェーズから基本設計フェーズにかけて実施すべきセキュリティ要件策定を怠ると、実装フェーズや運用開始後に脆弱性混入による手戻りが発生することになる。なお、機密性を確保しようとするとう可用性が下がってしまうなど、各フェーズで実施する対策は相互に関連しているため、セキュリティ要件策定ではトレードオフを考慮しなければならない。

* (株)三菱電機ビジネスシステム

1. ま え が き

Webシステム上に公開・格納されている情報やデータに対するサイバー攻撃は年々高度化・複雑化・悪質化しており、従来の“愉快犯”的なものから、標的型攻撃に見られる“窃盗犯”的なものまで多様化している。

これらのサイバー攻撃を防御するため、Webアプリケーションの開発に当たっては、①設計フェーズでは脆弱性対策仕様を盛り込み、②実装フェーズでは脆弱性対策実装済みのフレームワークを使用し、③試験フェーズでは複数のセキュリティ試験ツールを利用することによって、脆弱性対策を行ったので、本稿ではその概要について述べる。

2. Webアプリケーションの脆弱性

Webアプリケーションの脅威、脆弱性、リスクとは何かを述べ、脆弱性関連の最新情報について述べる。

2.1 脅威、脆弱性、リスクについて

- (1) 脅威とは、Webアプリケーションに対して害を及ぼす、又は害を及ぼす可能性のある事象を指し、サーバに異常なアクセスを行い稼働停止に追い込むものや、不正侵入して改ざんや機密情報を取得する不正アクセスなどが該当する。
- (2) 脆弱性とは、Webアプリケーションが脅威となる攻撃に対して弱い状態、脅威から守るための対策が不完全な状態を指す。
- (3) リスクとは、Webアプリケーションのセキュリティの脆弱な部分から脅威が侵入し、情報漏洩(ろうえい)などによって損失を被る可能性の度合いのことである。

2.2 脆弱性に関する最新情報

Webアプリケーションの脆弱性に関する最新情報については、(独)情報処理推進機構(IPA)が脆弱性関連情報を公開しており、不正アクセス手法などの脅威に対する脆弱性の実態がまとめられている。また、OWASP(The Open Web Application Security Project)が公開している情報では、セキュリティリスクについて報告されている。

- (1) IPAが公開している最新の脆弱性関連情報によると、2012年1月～3月にIPAに届けられた脆弱性関連情報の届出件数のうち、Webアプリケーションに関するものが216件であり、その中で“クロスサイト・スクリプティング”が最も多く、全体の89%を占めている。
- (2) OWASPが公開している2010年度版のOWASP Top 10-2010 Japanese PDF⁽¹⁾で報告されているWebアプリケーションセキュリティの10大リスクと、その他の考慮すべきセキュリティリスクを表1、及び表2に示す。OWASP Top 10-2010年度版では“リスク”が高く、重大な影響を及ぼすものに焦点を当てたものになっている。

3. Webアプリケーションに対する脆弱性対策

3.1 脆弱性対策に対する基本的な考え方

情報セキュリティの基本理念は、情報の機密性、完全性、可用性を維持することであるが、脆弱性対策を検討する場合機密性と可用性がトレードオフの関係になりやすい。例えば、全ての情報の持ち出しを禁止にすれば機密性は高まるが、顧客、取引先や協力会社と情報交換をするための持ち出しも不可能となり可用性は下がる。このような場合、情報漏洩事故が発生した時の損失などのリスクと業務上の有益性を比べて、機密性・可用性のどちらを優先するか決定する。

3.2 脆弱性対策のプロセス

MBでは、Webアプリケーション開発に当たって、2章で述べた脅威、脆弱性、リスクに対応するため、上流工程から下流工程まで一貫した脆弱性対策の設計、実装、試験を行っている。次に、各フェーズでの実施内容を述べる。

3.2.1 要件定義フェーズ

開発するWebアプリケーションシステムの規模、機密情報取扱いの有無、情報が漏洩した場合のリスクなどを評価し、機密性確保優先か、可用性確保優先かを顧客と協議の上決定し、セキュリティ要件を定義する。

表1. Webアプリケーションに対する10大リスク(2010年度版)

No	内容
1	インジェクション攻撃(SQL, OS, LDAP等)
2	クロスサイトスクリプティング(XSS)
3	不完全な認証とセッション管理
4	安全でないオブジェクトの直接参照
5	クロスサイトリクエストフォージェリ(CSRF)
6	セキュリティの不適切な設定
7	安全でない暗号化によるデータ保存
8	URLアクセス制御の不備
9	不十分なトランスポート層の保護
10	未検証のリダイレクトとフォワード

SQL : Structured Query Language
 OS : Operating System
 LDAP : Lightweight Directory Access Protocol
 URL : Uniform Resource Locator
 出典 : OWASP Top 10-2010 Japanese PDF

表2. その他の考慮すべきセキュリティリスク

内容
クリックジャッキング
悪意あるファイルの実行
情報漏洩と不適切なエラー処理
不十分なログ取得とアカウントビリティ
DoS(Denial of Service, サービス不能)攻撃
同時処理に関する欠陥
自動攻撃に対する不十分な対抗措置
不正侵入の検知と対応に関する不足

出典 : OWASP Top 10-2010 Japanese PDF

3.2.2 設計フェーズ

- (1) 基本設計フェーズでは、脆弱性対策を盛り込んだシステム全体の外部設計、試験設計、本稼働後の運用設計を行う。主な内容を表3に示す。
- (2) 詳細設計フェーズでは、具体的な画面の入出力インタフェース、HTTP(Hypertext Transfer Protocol)メソッドの選定、入出力の特性に応じたデータ項目のデータベース設計、セキュリティ対策を考慮した共通部品化設計などを行う。内容を表4に示す。

なお、共通部品化設計の具体例として、クロスサイトスクリプティング、SQLインジェクションの脆弱性に対する対策の一つであるエスケープ処理について表5に示す。

3.2.3 実装フェーズ

実装フェーズでは、設計フェーズで作成された仕様にしたいが、実装を行う。開発言語がJava^(注1)の場合、脆弱性に対する対策があらかじめ実装されている、MB独自のJava製Webアプリケーションフレームワーク(表6、表7)を基盤としてプログラムの実装を行う。このフレームワークを利用することで、プログラマは特にWebアプリケーションの脆弱性を意識することなく均一なセキュリティ品質を作り込むことができる。

表3. 基本設計フェーズで行う脆弱性対策

フェーズ	項目	設計内容の例
外部設計	ログインの方式	セッション管理 Secure Cookie システム認証 ベーシック認証
	画面設計	入出力に関わる全般的な制約事項
試験設計	機能試験	データ改ざん試験
	セキュリティ検査	検査シナリオ作成
運用設計	ログ取得	操作ログ取得
	不正アクセス監視	アクセスログ監視
	バックアップ設計	事故後のデータ復旧

表4. 詳細設計フェーズで行う脆弱性対策

フェーズ	項目	設計内容の例
詳細設計	画面の入出力インタフェース	最大入力値、最大入力長
		入力禁止文字種
	画面遷移時のデータの引渡し・データの戻し方法	
HTTPメソッド	POST/GETのうち、極力POSTを使用	

表5. エスケープ処理での共通部品化

シーン	置換前	置換後
全ての表示におけるHTMLエンコーディング	"	"
	&	&
	<	<
SQL文の全挿入文字	;	¥;
	%	¥%
	_	¥_

HTML : HyperText Markup Language

質を作り込むことができる。

(注1) Javaは、Oracle Corp. の登録商標である。

3.2.4 試験フェーズ

試験フェーズでは、表8のツールを利用して試験を行う。

- (1) 結合試験・機能試験では、機能単位、入力フィールド単位で確実に目視確認しながら試験を行うため、Odysseus^(注2)やParos^(注3)を活用している。試験実施者は、試験設計書にしたがってWebブラウザからWebアプリ

表6. Webアプリケーションフレームワークの機能

機能	内容
基盤エンジン	メール送受信、CSV・Excel ^(注4) 出力、帳票、数式演算、メッセージ送信など
データベースエンジン	簡易問合せ、更新、削除であればSQLの記述は不要、SQLが必要な場合は外部ファイルに記述が可能
画面制御エンジン	Webアプリケーションを開発するために必要な機能を集めたビューコンポーネント

CSV : Comma Separated Values

表7. フレームワークで実装されている脆弱性対策

脆弱性、リスク	対策
SQLインジェクション	バインド変数を使用してパラメータを渡す。
クロスサイトスクリプティング	画面制御フレームワークでサニタイジングする。
不完全な認証とセッション管理	AOP(アスペクト指向プログラミング)を利用して、全てのページを監視し、ログイン状態を確認する。
クロスサイトリクエストフォージェリ	サニタイジングやセッションIDの変更などを行うユーティリティを提供する。
安全でない暗号化によるデータ保存	あらゆるデータを暗号化。方式はAES(Advanced Encryption Standard)である。
URLアクセス制御の不備	URLパラメータのAES暗号化と検証を実施する。URLごとにAOPによる認証チェックを行う。
未検証のリダイレクトとフォワード	やむを得ず飛び先をリクエストに含む場合は、AES暗号化する。

表8. 試験フェーズで利用するツール

ツール	特徴/機能
Odysseus (フリー)	【位置付け】脆弱性検査補助ツール ・プロキシとして動作 ・HTTP/HTTPSの通信を傍受 ・HTTPリクエスト/レスポンスの書換えが容易 ・操作が直感的で分かりやすい
Paros (フリー)	【位置付け】セキュリティ評価ツール ・プロキシとして動作 ・HTTP/HTTPSの通信を傍受 ・脆弱性スキャナ・フィルタ機能 ・簡易レポート機能 ・HTTPリクエスト/レスポンスの書換えインタフェースが分かりにくい
AppScan (商用)	【位置付け】脆弱性検査ツール ・不正なHTTPリクエストを送信し擬似攻撃 ・自動巡回機能 ・自動テスト機能 ・詳細レポート機能 ・セキュリティルール(攻撃パターンに相当)のアップデート ・難易度が高く、講習会受講などが必要

HTTPS : HyperText Transfer Protocol over Secure Socket Layer



図1. AppScanのスキャン結果例

ケーションに向けてPOSTされたHTTP Headerをインターセプトし、パラメータの値を故意に変更(改ざん)して、バッファオーバーフロー、クロスサイトスクリプティング、SQLエラーインジェクションなどが発生しないかどうか試験する。これによって実装フェーズで脆弱性対策の漏れがないことを確認する。

- (2) システム試験や性能試験完了後、試験設計書と実装方式についての事前ヒアリングを行い、検査対象画面の全シナリオを作成し、IBMのRational AppScan^(注5)を使用して開発環境で出荷前のセキュリティ検査を行う。

図1にAppScanの画面例を示す。図1ではシナリオに従って試験した結果を示し、画面左上は試験対象のURL、画面右上に発見された脆弱性(危険度高の脆弱性はレッド, 危険度中の脆弱性はブラウン, 危険度低の脆弱性はイエローで表示), 画面右下に発見された脆弱性の詳細、画面左下にサマリーが示されている。原則として検出された高・中・低の全ての脆弱性に対して対策を実施する。なお、当該システム運用上問題とならないような場合、例えば、出力結果のHTMLにコメントが含まれているという脆弱性低の指摘があっても、そのコメントに機密情報が含まれていないような場合には、問題はないため対策を実施しないことがある。

- (3) 導入後本稼働前に、MBから検査会社への依頼によって、インターネット上の実環境で本稼働前のセキュリティ検査が行われる。検査環境の相違、使用する検査ツールの相違によって、新たな脅威、脆弱性、リスクが検出された場合は、(2)と同様に対策を行う。

- (注2) Odysseusは、bindshell.netから提供されているフリーソフトウェアである。
 (注3) Parosは、MileSCAN Technologies Ltd. が開発した無償版ソフトウェアである。
 (注4) Excelは、Microsoft Corp. の登録商標である。
 (注5) Rational AppScanは、International Business Machines Corp. の登録商標である。

4. む す び

これまで述べてきたプロセスを経てWebアプリケーションの脆弱性が取り除かれるが、次に示す課題も残っており、今後、継続して対策を検討し、より高品質のシステムを提供していく所存である。

- (1) 今後、オンプレミスなシステムからクラウドコンピューティングへの移行が進展すると考えられるため、クラウドサービス化するWebアプリケーションのセキュリティ対策(安全性)、性能、可用性について対応方法を検討・実施する。
- (2) 最新のサイバー攻撃である標的型攻撃は機密情報の流出につながる可能性があり、対策が急務である。最新動向として、ネットワーク接続ポイントに専用機器を設置し、通過するパケットやメールを監視・分析することで、ウイルス感染や挙動不審な動きを検出するツールが提供されつつあり、そのようなツールを調査し、システム設計時への適用、顧客への提案などを検討する。
- (3) 脆弱性対応の手法には、アプリケーション側で対応するのではなくWAF(Web Application Firewall)を利用する方法もある。WAFはソフトウェアとして提供されるものとハードウェアとして提供されるものがあり、今後、調査・検証を進めていく。

参 考 文 献

- (1) The Open Web Application Security Project : 日本語版OWASP Top 10-2010, Creative Commons(CC) Attribution Share-Alike Free version at <http://www.owasp.org> (2010)

大規模情報系システムにおける 統合ID管理ソリューションの適用

木幡康博* 森田康之*
及川和彦* 山足光義**
小宮 崇* 小杉 優**

Applying the Integrated Identification Management Solution to Very Large Information System

Yasuhiro Kowata, Kazuhiko Oikawa, Takashi Komiya, Yasuyuki Morita, Mitsuyoshi Yamatari, Yu Kosugi

要 旨

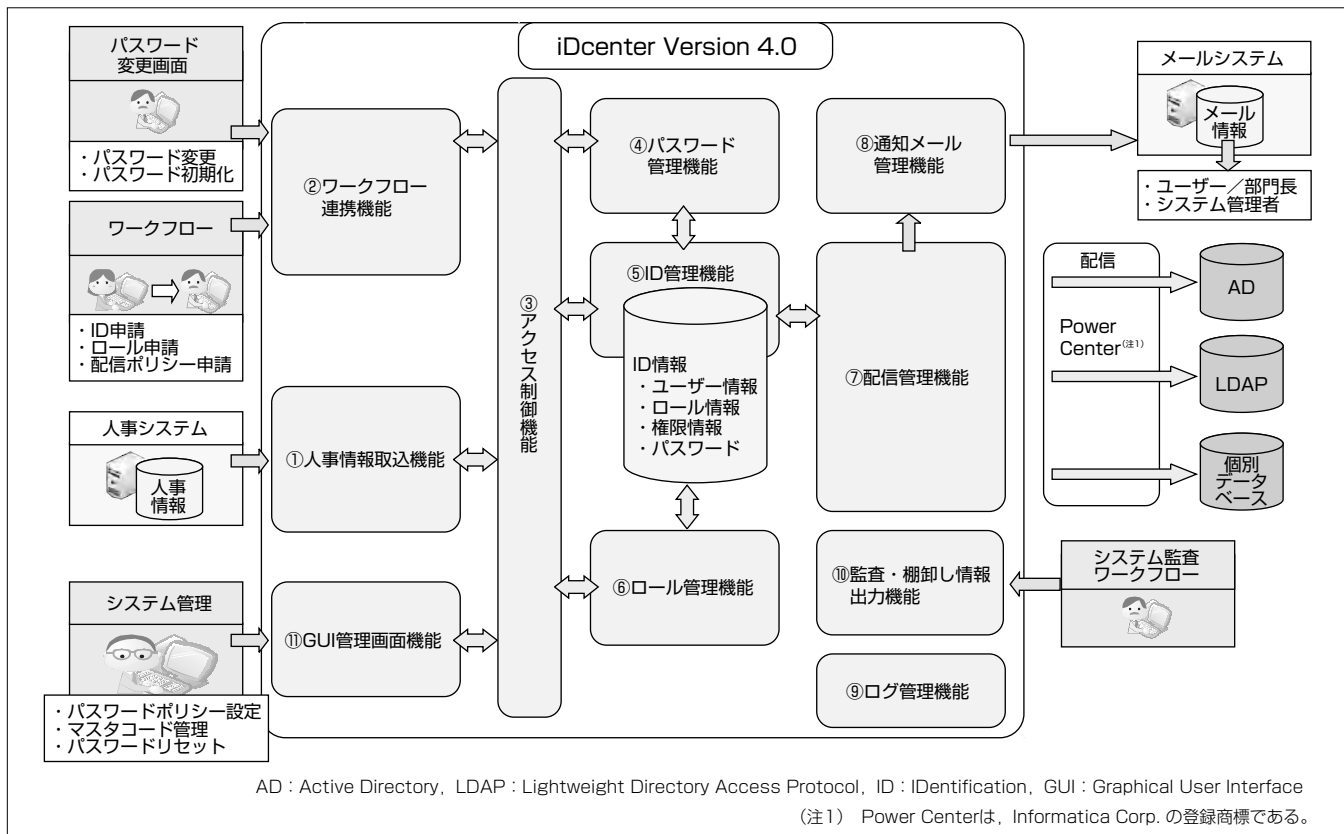
企業には、従業員の個人識別情報を使った情報システム、入退出管理や機密情報管理等の複数のセキュリティシステムが導入されているが、それぞれのシステムがID情報を個別に持ち、ID情報の変更管理も個々に行われてきた。このため、組織変更や人事異動によるシステムへのアクセス権限や通行権限の管理負荷が増大し、変更ミスなどによるセキュリティリスクも拡大している。

統合ID管理ソリューション“iDcenter(アイディーセンター)”は、複数のシステムに対して、組織変更や人事異動によるアクセス権限の変更情報を自動配信することで、業務の効率化、セキュリティの強化を実現する。ID情報の“過去・現在・未来”にわたる世代管理によって、予約登録や情報の履歴管理による内部統制の強化が可能である。また、各種情報システムと入退室管理システムを連携し、来

訪者管理、在場管理、パソコンログイン連携、勤怠管理等の様々な機能を提供する。

iDcenterを三菱電機グループ全体のユーザー11万人が利用する大規模情報系システムに適用し、次の機能を提供した。人事システムとワークフローシステムとの連携によるユーザーID情報管理機能、各種システムでの認証情報となるパスワード管理機能、各種システムに対するユーザーの利用権限の管理機能、ユーザーの所属情報や職位情報等を利用した利用権限自動割り付け機能、これらのユーザー情報、認証情報、各種システムの利用権限を自動的に各種システムに配信する機能、内部統制のためのログ管理、監査・棚卸し情報出力機能である。

これらの機能について、大規模情報系システムのID管理で必要とされる課題とその対応策を述べる。



統合ID管理ソリューション“iDcenter”の情報系システム構成例

iDcenterは、人事システムとワークフローからユーザー情報を取り込む。また、パスワード情報と、各種システムに対する権限情報の管理と権限自動割り付けを管理する。ユーザー情報と認証のためのパスワードと各種システムでの権限情報を一元管理し、各種業務システムにID情報を配信する。また、ID情報の履歴を管理し監査ログとして提供する。

1. ま え が き

近年、様々なセキュリティ脅威が増大する中、ユーザー認証、アクセス制御、ログ監査等の情報セキュリティ、人の通行を物理的に制限する入退室管理システムや監視カメラ等の物理セキュリティの導入が進められている。

これらのセキュリティシステムが有効に機能するためには、氏名、社員番号、ICカード情報、役職、パスワード等の個人に関する情報(ID情報)が正しく登録され、運用されることが不可欠である。一方、システムの高度化・多様化に伴い、ID情報管理も複雑化し、ID情報の管理運用の負荷増大、登録・変更ミスや漏れによるセキュリティリスクの発生、企業におけるIT全般統制としての基盤構築の必要性等、新たな課題が認識されてきている。

本稿では、これらの課題を解決するために、統合ID管理ソリューション“iDcenter”を三菱電機グループの大規模情報系システムのID管理に適用したので、その事例を基に述べる。

2. iDcenterの特長

iDcenterの特長を次に示す。

(1) ID世代管理による予約登録と内部統制への対応

現在の個人情報、組織情報を管理だけでなく、過去の個人情報、組織情報を世代管理し、未来の個人情報となる予約登録(例：4月1日付けの新入社員を含む人事異動情報を3月20日に事前登録)を可能とする(図1)。また、情報の世代管理によって、いつ、誰が何を変更したかの履歴を参照でき、内部統制に対応できる。

(2) 各種システムへの利用権限自動割り付けと自動配信

人事システムから取り込まれる人事異動の情報やユーザーの役職情報等によって、各システムに対しての利用権限を設定することで、人事異動による利用権限の変更が自動的に行われ、変更情報を自動配信する。

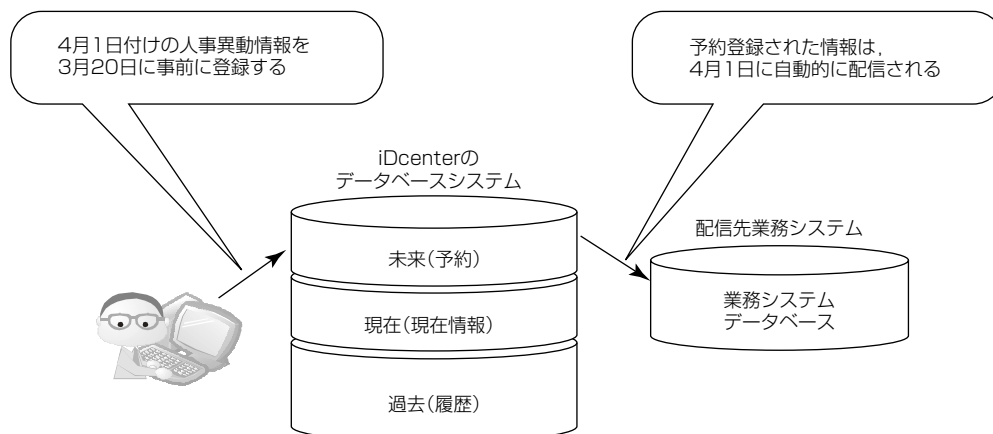


図1. 予約登録

(3) 日本企業に適したID管理

日本企業では、組織の階層例として事業本部、統括本部、部、課、係、班と言った階層構造が深いツリー状の組織体系を持つ。iDcenterでは、このような深い組織階層構造でも対応できる内部データ構造を持ち、配下を含めた部全体や統括本部全体に対して各種システムの利用権限を管理できるなど、日本企業に適した統合ID管理を実現する。

3. 認証システムとiDcenterの役割

今回開発した大規模情報系システムに対するiDcenterのID管理機能は、三菱電機グループ全体の認証システムの一部として利用するために、機能強化が行われた。この認証システムの概要とそこで利用されているiDcenterの役割について述べる。

(1) 認証システム

三菱電機の社内、国内外関係会社及び社外取引先の会社を含めて、グループ全体で11万人のユーザーが使用する各種システムに対する認証機能を提供する。

(2) iDcenterの役割

図2に示すように、iDcenterでは、①人事システムと連携しCSV(Comma Separated Values)形式でユーザー情報を一括で登録する機能と、②API(Application Programming Interface)によって画面から個別にユーザーを登録する機能の2つの方法が利用できる。③権限管理では、人事情報だけでなく各種システムへのユーザーの利用権限情報をiDcenterに取り込む。④パスワード管理では、APIによって、認証情報となるパスワードを取り込み、変更、初期化を管理する。⑤配信機能では、こうして取り込んだユーザー情報、認証情報、各種システムへの利用権限情報を認証システムであるLDAPや各種ADシステム、各種業務システムへ配信する。各種システムは、iDcenterから渡された情報で認証を行う。⑥内部統制のためのID情報、権限情報の履歴管理を提供する。

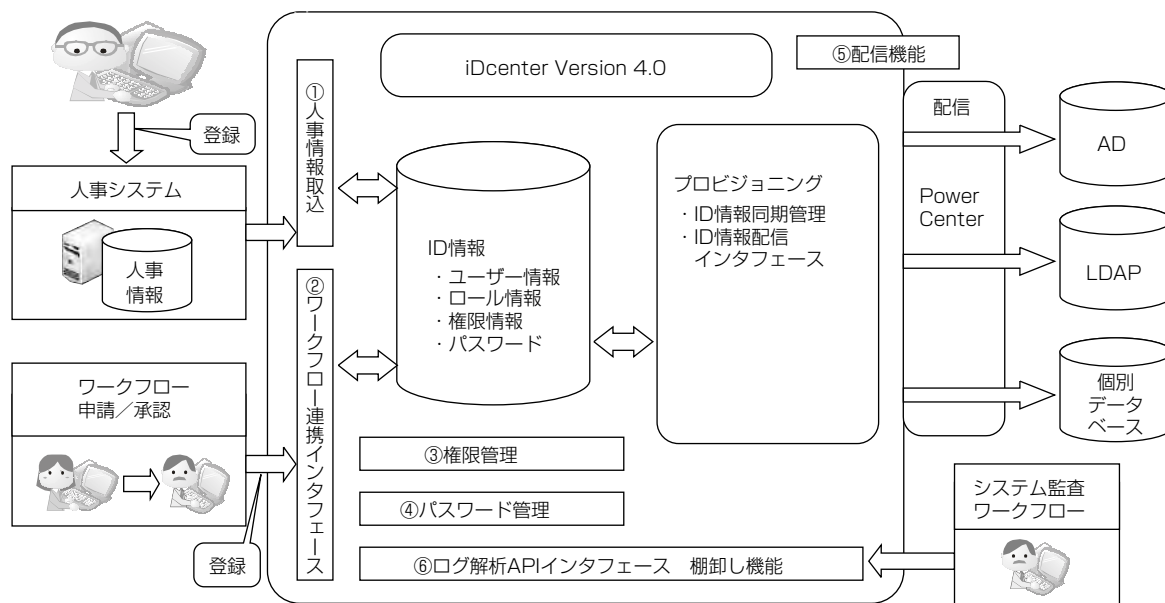


図 2. iDcenterの役割範囲

4. 大規模情報系システムのID管理に関する課題と対応

iDcenterは、人事システムデータからID情報を生成し、認証のためのパスワード管理を行い、各種システムの権限を一元管理して、それらの情報を各種システムに配信することで、ID管理を自動化し管理コストを低減する。ここでは、主な追加開発機能である①データ入力、②権限管理自動化、③配信制御、④配信先連携レパトリの強化、⑤内部統制のための監査機能の課題とこの開発における対応について述べる。

4.1 データ入力での課題と対応

iDcenterは、人事システムとワークフローから渡される人事情報、各種システムへの認証情報となるパスワード及び各種システムへの権限情報を管理する。人事情報については、人事システムと連携してユーザー情報を一括で取り込む機能に加えて、ワークフローから個別にユーザー情報を取り込むためのAPIの機能が求められた。また、ユーザー情報だけでなく、ユーザーにシステム利用の権限を割り付けるためのAPIも必要となる。さらに、このシステムは海外関係会社を含むため、グローバルな対応が必要となった。

(1) APIによるワークフロー機能への対応

企業が持つワークフローに対して、人事情報の取り込みAPI、承認・代理承認のためのAPI、認証情報であるパスワード更新・初期化のためのAPI、各種システムに対する利用権限割り付けのためのAPIを提供することで、各種ワークフローによる情報をiDcenterに直接取り込み、人事情報、認証情報、権限情報を一元管理できるようにした。これらのAPIによって、各企業が既に使用しているワークフローエンジンを利用して、企業固有のワークフローを構築できる。

(2) UNICODEによるグローバル対応

適用システムでは、世界中に工場や支社、取引先企業があることから、グローバルなユーザー登録が必要となる。データ入出力をUNICODEにすることで対応した。

4.2 権限管理自動化のための課題と対応

ID管理では、各種システムへのユーザーの利用権限割り付け機能をどれだけ自動化できるかが、システム導入の際の重要なポイントの一つとなる。この課題については、ロールによる権限付け替え自動化機能を強化することで対応した。

ロールは、複数の人や部門を同一の権限グループとして扱うために利用するものである。iDcenterでは、ユーザーの権限管理としてロールを利用する。同じロールに割り付けられたメンバーは、対応の業務に対して、同じ利用権限を持つ。複数の組織をロールAに割り付け、このロールAの属性情報とロールAに割り付けられたメンバー情報を業務システムAに配信することで、ロールAに割り付けられた組織の人は、業務システムAに対して、同じ利用権限が与えられる。ロールに対して、どのようにユーザーを割り付けできるかが、システム自動化の決め手となる。ロールに対して個人を割り付けると、人事異動によって権限がなくなった時に、ロールから削除する必要があり、管理が煩雑となる。企業の中での各種システムの利用権限は、所属と部長・課長等の職位などによって、与えられることが多い。ロールに割り付ける方法として、組織とユーザーの職位を条件として割り付けを行うことで、権限割り付けの自動化が図れる。

ロール割り付けの条件として、組織の直下のユーザーを対象としたり、指定組織配下のユーザーを対象としたりできる。さらに、会社単位、事業部単位といった部門単位や、

ユーザー区分等の他のユーザー属性を条件として、ロール割り付け設定を行うことができる。これによって、柔軟な権限割り付けの自動化を実現できた。図3にロールへのメンバー割り付けの例を示す。

4.3 配信制御での課題と対応

iDcenterの配信制御は、夜間に取り込んだ人事情報データを、これまでに配信した情報との差分を取って、各種システムに一括配信する機能を基本としているが、APIで入力された情報を即時配信する機能も開発した。また、人事異動や組織変更に伴う混乱を回避するため、引継ぎのための猶予期間を設けた配信にも対応した。

(1) 一括配信制御

iDcenterの配信制御は、データ取り込み済みの入力データテーブルと各種システムへの配信済みデータを保持する配信データテーブルによって管理される。入力データテーブルと配信データテーブルには、過去に入力されたデータと過去に配信されたデータが配信履歴情報として管理されているので、IDの世代管理を行うことができる。

図4に一括配信制御の概要を示す。通常は、夜間に人事システムからバッチでデータを一括で取り込み、一括配信する。

(2) 即時配信制御

ワークフローからAPIを用いて入力されるデータは、ユーザーごとに即時で各システムに配信することが求められることから、性能面を考慮した配信制御を実現した。即時配信では、図5に示すように、ワークフローから入力されたユーザー情報を配信データテーブル中の対応するユーザーデータと比較し、この差分データを配信する。これによって、配信性能の向上を図った。

(3) 猶予期間を考慮した配信

iDcenterは、各種システムに対してユーザー情報、利用権限情報、認証情報を配信する時には、原則として、配信日のユーザーの利用権限を配信する。しかし、所属で利用権限が決められている業務システムなどでは、人事異動などで誰も利用できなくなると困るシステムがある。こうしたシステムに対しては、引継ぎのための猶予期間を与えて利用権限を配信することを可能にしている。

4.4 PowerCenter連携による配信先連携レポートリー強化

配信先システムとしては、CSVファイルによる連携だけでなく、LDAPシステムやADシステム、データベースシステムに対して、直接連携できる機能が求められる。

iDcenterは、ETL(Extract Transform and Loading)機

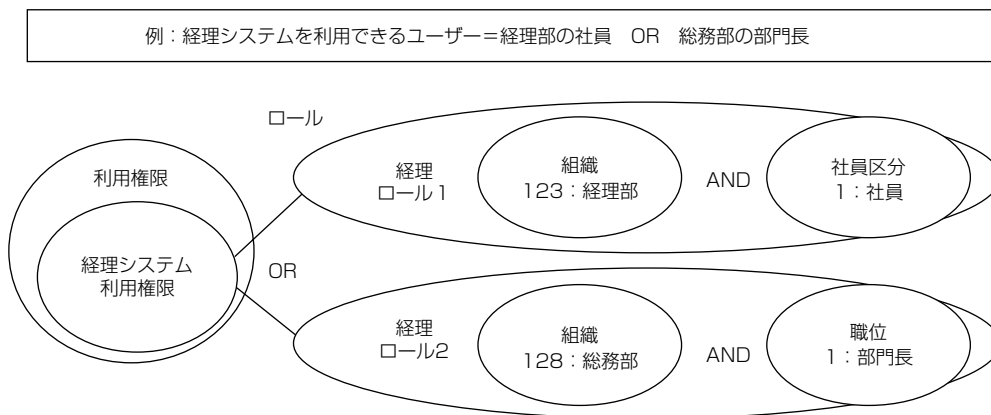


図3. ロールへのメンバー割り付け例

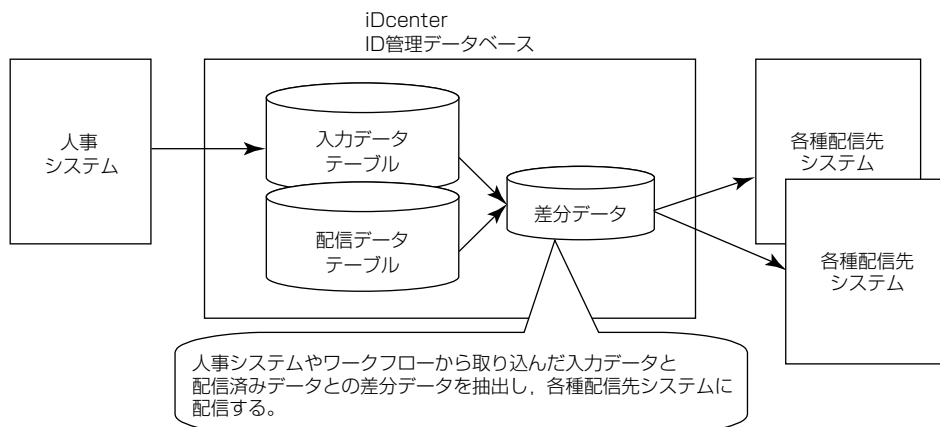


図4. 一括配信制御

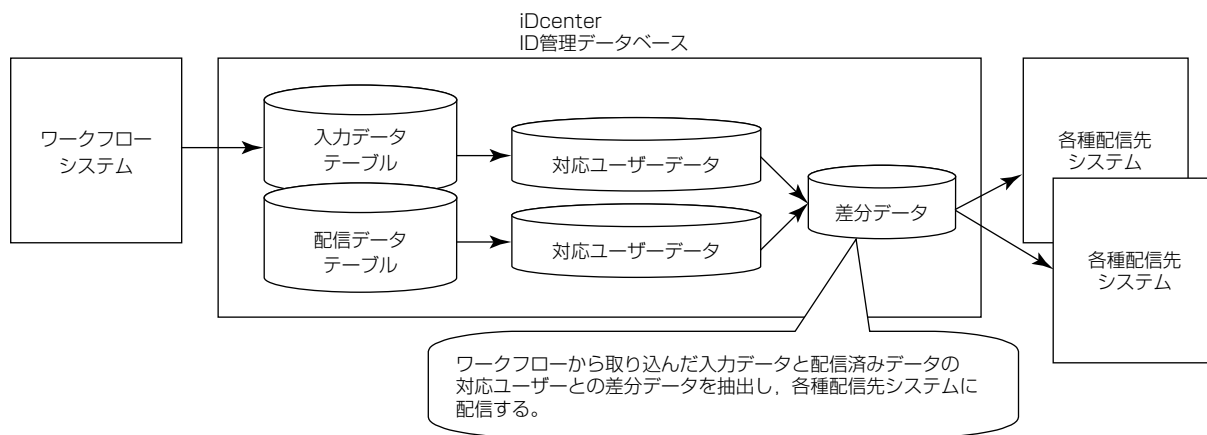


図 5. 即時配信制御

能搭載のデータ統合ソリューションInformatica Power Center(以下“PowerCenter”という。)と連携し、人事システムからiDcenterに取り込んだ全社のID情報を情報システムの認証基盤となるLDAP/ADへPowerCenterを通して自動配信する。また、PowerCenterとの連携によって、ORACLE^(注2)、SQL Server^(注3)、DB2^(注4)等のデータベースとの連携も可能となった。

(注2) ORACLEは、Oracle Corp. の登録商標である。
 (注3) SQL Serverは、Microsoft Corp. の登録商標である。
 (注4) DB2は、International Business Machines Corp. の商標である。

4.5 ログ・監査機能強化

内部統制に対応するため、入力された情報に対して、履歴を追跡できる必要があり、ID情報の履歴管理強化によって対応した。

(1) 操作ログ機能強化

所属長が承認して登録されたID情報に関しては、誰が、いつ、どこで、どのような情報を登録したかについてログを残し、履歴を参照可能とするためのAPIを提供した。これによって、ワークフローで登録された派遣社員の情報や、各種システムへの権限情報の割り付けについての履歴を参照できるようにした。

(2) 情報の世代管理による監査機能

iDcenterでは、入力された情報の全てが履歴として管理されており、いつどのような情報が入力されたかについて

データベースを確認することで追跡できる。また、配信情報についても世代管理されており、いつどのような情報が、どのシステムに配信されたのかをデータベースを確認することで追跡できる。

5. む す び

iDcenterの特長であるID情報の世代管理による予約登録や猶予期間を考慮した配信への対応、ロールによる権限の自動割り付け機能強化等によって、三菱電機グループの大規模情報系システムにおけるID管理業務負荷の軽減、セキュリティの強化、ID情報の履歴管理による内部統制への対応等を実現することができた。

今回、iDcenterに対する機能強化として、API機能、ロール管理機能強化、配信先システム連携強化としてのLDAP連携、AD連携、各種データベース連携機能等の開発を行ったが、これらの機能を取り込んで、“iDcenter Version4.0”として製品化する予定である。また、今後は、オンデマンドITサービス対応の強化を図り、適用範囲を拡大していく。

参 考 文 献

- (1) 木幡康博, ほか: 確実なセキュリティ運用を実現する統合ID管理システム“iDcenter”, 三菱電機技報, **83**, No.9, 559~562 (2009)

ハンディターミナルを使用した 入退場・認証システム

渡辺康一*
濱崎光幸*
松井智浩*

Entrance and Exit Authentication System Using Handy Terminal Device

Kouichi Watanabe, Mitsuyuki Hamasaki, Tomohiro Matsui

要 旨

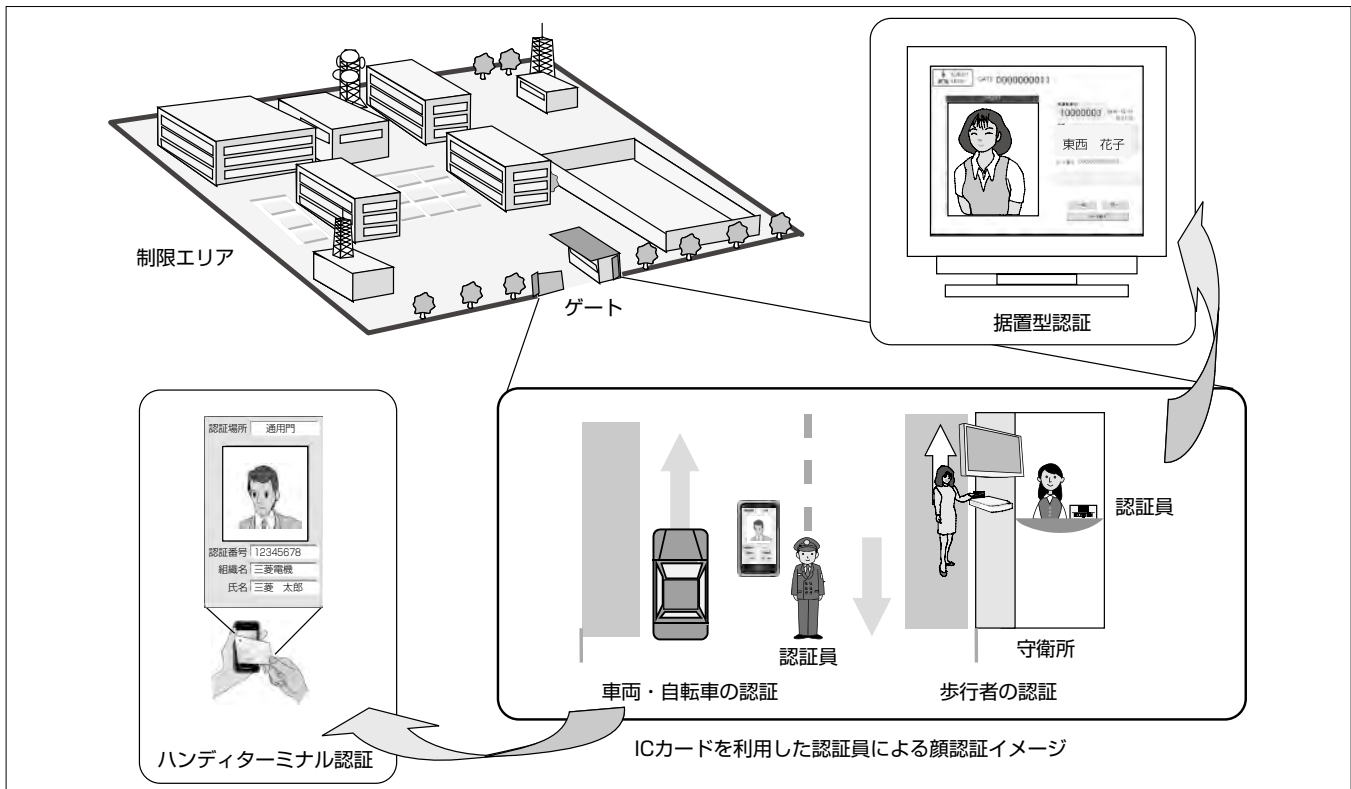
企業や官公庁等の“建屋への入退場”“事務室への入退場”はIC(Integrated Circuit)カードを用いたセキュリティゲートや壁設置型カードリーダーによる認証を実施している。一方で重要施設や工場のゲートでは、社員証や通行証を提示し、守衛・警備員が目視確認を実施しているケースが多く、ICカード化された社員証を十分に活用できていない現状がある。しかし、人による目視確認は、無人のセキュリティゲートやカードリーダーのみの入退場の場合より抑止力や応用力があり、セキュリティが高いとも言われている。また、イベント会場を始めとした“エリア入退場”の場合、短期間での開催や電源・ネットワーク等の設備設置の問題などでセキュリティゲートなど大規模なセキュリティシステムを導入できない場合もある。

このハンディターミナルを使用した入退場・認証システム

は、先に述べた守衛・警備員を配置している重要施設や工場のゲート、実施期間やインフラの関係でセキュリティゲートなどの整備が難しい場所に対してのセキュリティ強化ソリューションである。

このシステムはハンディターミナルのICカードリーダーで読み取ったカードのID(IDentification)番号から登録情報を検索しディスプレイ上に表示する仕組みである。守衛・警備員が本人とIDカードの情報、表示された情報を照合することで認証を実施する。

可搬性のあるハンディターミナルを使用することによって車両で来場した運転手に対する認証の実施やインフラの整備を実施することなく、低コストで高いセキュリティを提供することを目的としたシステムである。



ハンディターミナルによる認証

ハンディターミナルには事前に管理サーバから認証情報をダウンロードしてあり、守衛・警備員の認証員がハンディターミナルを持ちICカードを読み取ることで認証を行う。認証は本人とICカードに印刷された顔写真及び機器に表示された顔写真を含めた認証情報を照合する。

また、機器としてはハンディターミナルの他にICカードリーダーを接続したパソコンで認証を行うことも可能である。認証結果は使用后、管理サーバと接続することで、通行履歴として保持することも可能である。

1. ま え が き

近年、危機管理対策やテロ対策といった機運が高まっており、国際的にも米国同時多発テロを契機としたSOLAS (The International Convention for the Safety of Life at Sea) 条約に基づく“国際航海船舶及び国際港湾施設の保安の確保等に関する法律”⁽¹⁾が制定されるなど、建屋、エリアに対するセキュリティの向上が必須となってきている。建屋の入退場や部屋への入退出に関しては、三菱電機のトータルセキュリティソリューションである“DIGUARD”を筆頭に、各社が各種ハードウェアやシステム製品を販売しており、規模、価格、製品種類も様々なものがある。一方で、官公庁、独立行政法人、航空会社、電力会社、鉄道会社等の重要施設へのエリア(敷地)入退場では、守衛・警備員による、入退場者が提示したICカード(職員証や社員証等)の目視確認が主流であり、建屋、部屋へのICカード認証によるセキュリティと比較すると、偽造やなりすましに対して十分な認証が行われていない現状がある。

本稿では、これらの守衛・警備員の目視によるカード認証に関して、電源やネットワーク工事が難しい場所や車での通門、工事など短期間での認証等を考慮した可搬型のICカード認証システムのソリューションについて述べる。

2. セキュリティ強化の必要性

2.1 国が推進しているセキュリティ強化

電子政府推進計画で2008年度に各省庁の中央庁舎及び全国の主要合同庁舎で職員用ICカードによる入退館ゲート及び入退館システムの整備・導入が実施されたのを契機に、近年では国土交通省におけるPSカード(Port Security Card)導入など、ICカードによるセキュリティ強化が実施されてきている。また、PSカードでのセキュリティ強化では併せて3点確認の実施を規定している。3点確認とは、本人確認、所属確認、目的確認の実施である。本人確認は、ICカードの写真と本人の顔の照合、所属確認・目的確認はICカードに印字された所属又は口頭による立入り可否の確認である。いずれも守衛・警備員による目視確認が前提であり、この方法は無人のゲートタッチによる入退場に比べセキュリティが高いと言われている。一方でこの確認方法は、ICカードが正規なものであることが前提であり、ICカード上の写真の差し替えや、カードそのものを偽造した“なりすまし”対策、カードの有効期限切れ、紛失等によるカードの失効など“カードの有効性”の確認が難しい側面がある。

2.2 ハンディターミナルでの認証⁽²⁾

“なりすまし”や“カードの有効性”を確認する方法として、カードの券面に印刷された情報を確認するのではなく、カードとは別にあらかじめ登録された情報又はICカード内の情報をディスプレイに表示し、その情報と本人を照合することが考えられる。すでにセキュリティゲートが設置されておりICカード認証を実施している施設では、顔写真やカード情報を表示するディスプレイを追加し、守衛・警備員を配備することでセキュリティの強化が図れる。一方で守衛・警備員のみでICカードの券面に印刷された情報を確認しているゲートでは、電源やネットワーク設備がない場合も多く、新たなインフラを整備するには大きなコストがかかり、実施が困難なケースがある。

このシステムではこのようなインフラを整備できない場所、通勤時間帯や工事期間中等一時的に認証を実施する場所に対して、可搬性のあるハンディターミナルでICカードの照合を実施することや低コストで高いセキュリティを提供することを目的としたシステムである。

3. 入退場・認証システム

3.1 運用イメージ

このシステムを既存の社員証(FeliCa^(注1)^(注2))を利用し、屋外の入退場門で使用する場合の運用イメージを述べる(図1)。

ハンディターミナルを使用した認証では、守衛・警備員が本人とICカードの情報を表示したハンディターミナルとを比較し照合を行う。

具体的には、カードリーダーで読み取った社員証の情報からハンディターミナル内の登録情報を検索し、ディスプレイに表示する。この時顔写真や所属、氏名等ハンディターミナル内に登録した情報を表示する。ハンディターミナル内のデータは充電時などに管理サーバからあらかじめダ

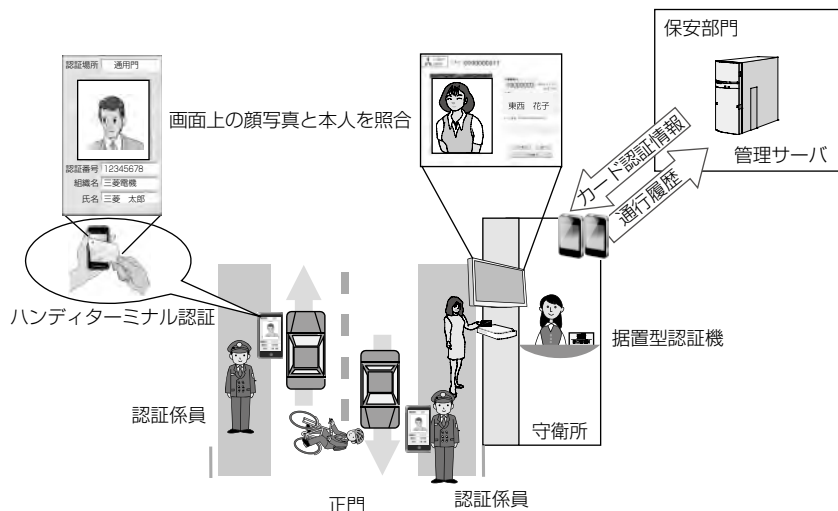


図1. 運用の流れ

ダウンロードする。無線LAN(Local Area Network)や3G回線(第3世代移動通信システムで使われている回線)等のネットワークが利用可能な環境であれば、ハンディターミナル内に格納した登録情報でなく、直接管理サーバにアクセスすることも可能である。

管理サーバ上に保有する顔写真、所属、氏名等の認証情報はWebシステムで登録・メンテナンスする(稼働当初など多数の人を一度に登録する機能も装備している)。

また、認証した結果は通行履歴として管理サーバにアップロードすることも可能である。

(注1) FeliCaは、ソニー㈱が開発した非接触ICカードの技術方式である。

(注2) FeliCaは、ソニー㈱の登録商標である。

3.2 システム構成

ハンディターミナルを使用した入退場・認証システムのハードウェア構成、機器構成をそれぞれ図2、表1に示す。

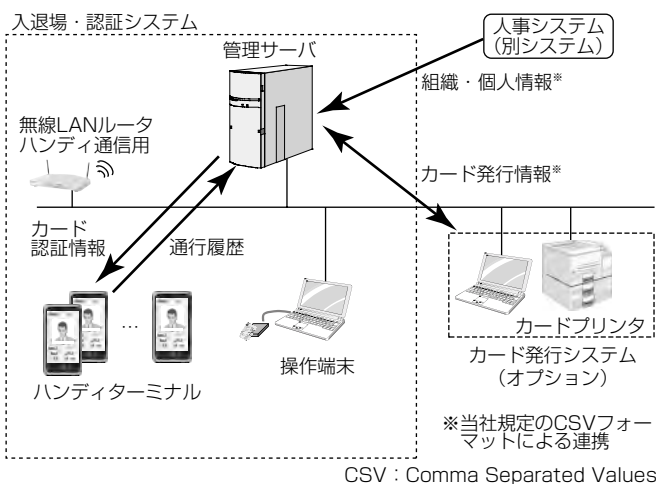


図2. ハードウェア構成

表1. 機器構成

機器	内容
管理サーバ	認証者の情報を格納するデータベースやWebシステムを格納する
操作端末	パソコンとICカードリーダーで認証者の情報を入力する
ハンディターミナル	認証作業を行う
カード発行システム(オプション)	入退場・認証システムから、ICカード発行指示を行う

表2. 機能一覧

機能	内容
認証者登録機能	入場・退場を行う人の組織情報や認証者の情報、顔写真登録、検索・照会を行う
カード管理機能	入退場を行う人のカード情報の照会や失効情報の登録を行う
認証機能	ハンディターミナルでICカードの認証を行い、認証結果を通行履歴として出力する
システム管理機能	ユーザー登録やコード表メンテナンス、ハンディターミナルで認証された通行履歴の検索・照会を行う

入退場・認証システムの機能は、認証者の登録や照会を行う認証者登録機能、カード管理機能、認証機能及びシステム管理機能の計4つの機能(表2)で構成している。認証機能を除く機能はWebを使用したシステムである。

3.3 システムの特長

入退場・認証システムにおけるシステム機能・機器の特長について述べる。

(1) 可搬性(ポータビリティ)

認証機器にハンディターミナルを使用することによって、場所を選ばずICカードの認証が行える。また、通行量や時間帯によって、使用するハンディターミナルの台数を調整し認証をすることが可能である。

電源・ネットワーク設備がない場所で認証を行う場合は、ハンディターミナル内にカード情報や失効情報をあらかじめダウンロードしておくことで、ICカード認証が行える。また、ネットワーク環境がある場所では、管理サーバの情報を直接参照することによって、ICカード認証作業が行える。使用する環境に合わせて、照合先を変えることで場所を選ばず使用することが可能である。

(2) 2つの認証情報の取得方式

このシステムでは、2つの認証情報取得方式を採用している。ICカードの読み取り方式や認証目的によって認証情報の取得方式を切り換えることができる。

認証情報の取得方式の1つ目は、ハンディターミナル内のデータベース又は管理サーバ内のデータベースと照合する方法である。ICカード番号とデータベースの情報を照合し、照合結果をハンディターミナルの画面に表示する。この方式の場合は、登録された人のみを判断する場合に有効であることと、ICカードの中に氏名や所属等が登録されていないカードを使用する場合に有効である。ICカード番号を使用するため、ICカードのほかにSuica^(注3)やPASMO^(注4)等FeliCa準拠のカードや、おサイフケータイ^(注5)がインストールされている携帯電話・スマートフォン等FeliCa機能を持った端末を使用し認証することが可能である。

認証情報の取得方式の2つ目は、カード内に登録されている情報を表示する方法である。カード内に登録された情報はセキュリティ領域に格納されているため、解除鍵を使用して取得する。取得した情報はハンディターミナルの画面に表示する(図3)。この方式の場合は、システムに認証者として登録されていない場合やICカード運転免許証で認証作業を行う場合に有効である。

(3) 様々なカードの混在認証

このシステムで認証可能なICカードの方式はISO(International Organization for Standardization)/IEC(International Electrotechnical Commission)1443 TypeA, ISO/IEC1443 TypeB, FeliCa方式の3つである。

認証時に複数のカードが存在していても、システムが自

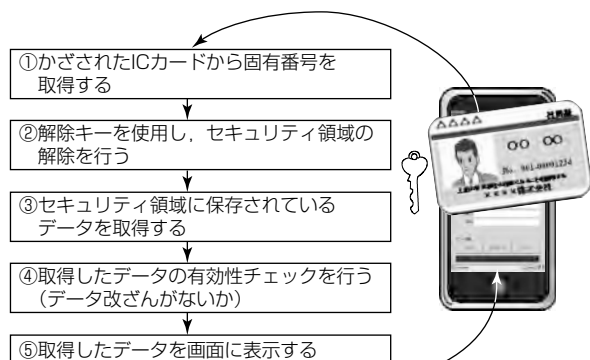


図3. カード登録情報の表示



図4. ハンディターミナルでの照合イメージ

動的にカードを判断するため、ハンディターミナル使用者はICカードの方式を意識することなく読み取りが行える。

例えば、社員証がISO/IEC14443 TypeB方式、業者や一時入場証がFeliCa方式を採用している場合でも、スムーズに認証ができる。

このシステムの導入にあたって既に発行済みのICカードを利用できることから、新たなICカード発行のコストは不要である。

(4) わかりやすい結果表示

使用する守衛・警備員による屋外での照合結果の判断を容易にするため、表示項目を必要最小限にし、さらに、音による通知を実施している(図4)。

表3. 機器の特長

特長	内容
耐環境性	防塵(ぼうじん)/防沫(ぼうまつ)仕様/堅牢(けんろう)性のある機器
感圧式タッチパネル液晶	冬場や工事現場等では手袋をしたまま操作することを想定し、感圧式のタッチパネル液晶の機器システムの操作は画面に表示するボタンの押下ですべての操作が可能
駆動時間	業務使用を想定して長時間使用できる機器

ICカードから該当する認証者のデータ照会を行い、照合結果をタッチパネル上に表示する。登録されていない人や、ICカードにエラーがある場合等は、照合結果と合わせてエラーメッセージをタッチパネル上に表示し、同時に、音による照合結果もハンディターミナル使用者に伝える。

(5) セキュリティ対策

ハンディターミナルを使用する権限がある人のみが操作可能としている。また、ハンディターミナル内にデータをダウンロードする場合は、データを暗号化して登録する。

(6) 機器の特長

認証で使用するハンディターミナルは屋外での使用を想定している。入退場・認証システムで使用するハンディターミナルは表3に示す特長を持つ端末を選定している。

(注3) Suicaは、東日本旅客鉄道(株)の登録商標である。

(注4) PASMOは、(株)パスモの登録商標である。

(注5) おサイフケータイは、(株)NTTドコモの登録商標である。

4. む す び

ハンディターミナルのICカード読み取り機能を使用した入退場・認証システムについて述べた。ハンディターミナルによるICカードの読み取り機能は、今回の入退場の認証以外で多様なシーンへの応用が考えられる。一例として、イベント参加者や点呼対象者を名簿化し、ICカードをハンディターミナルにかざすことによって出欠確認や点呼確認を行う機能や、訪問介護員(ホームヘルパー)の行動確認・訪問履歴の採取として、目的地にあるICカードの読み込みと位置情報を組み合わせた在场証明機能等である。

今後は、入退場・認証システムと他のシステムを組み合わせさせたシステムを提案していく。

参 考 文 献

- (1) 国土交通省：国際航海船舶及び国際港湾施設の保安の確保等に関する法律施行規則(平成十六年四月二十三日国土交通省令第五十九号)
- (2) (独)情報処理推進機構：IC・IDカードの相互運用可能性の向上に係る基礎調査、ニーズ編、報告書、2007年1月

医療認証基盤

村上耕平*
長浜隆次*

Healthcare Public Key Infrastructure Authentication Service

Kohei Murakami, Ryuji Nagahama

要旨

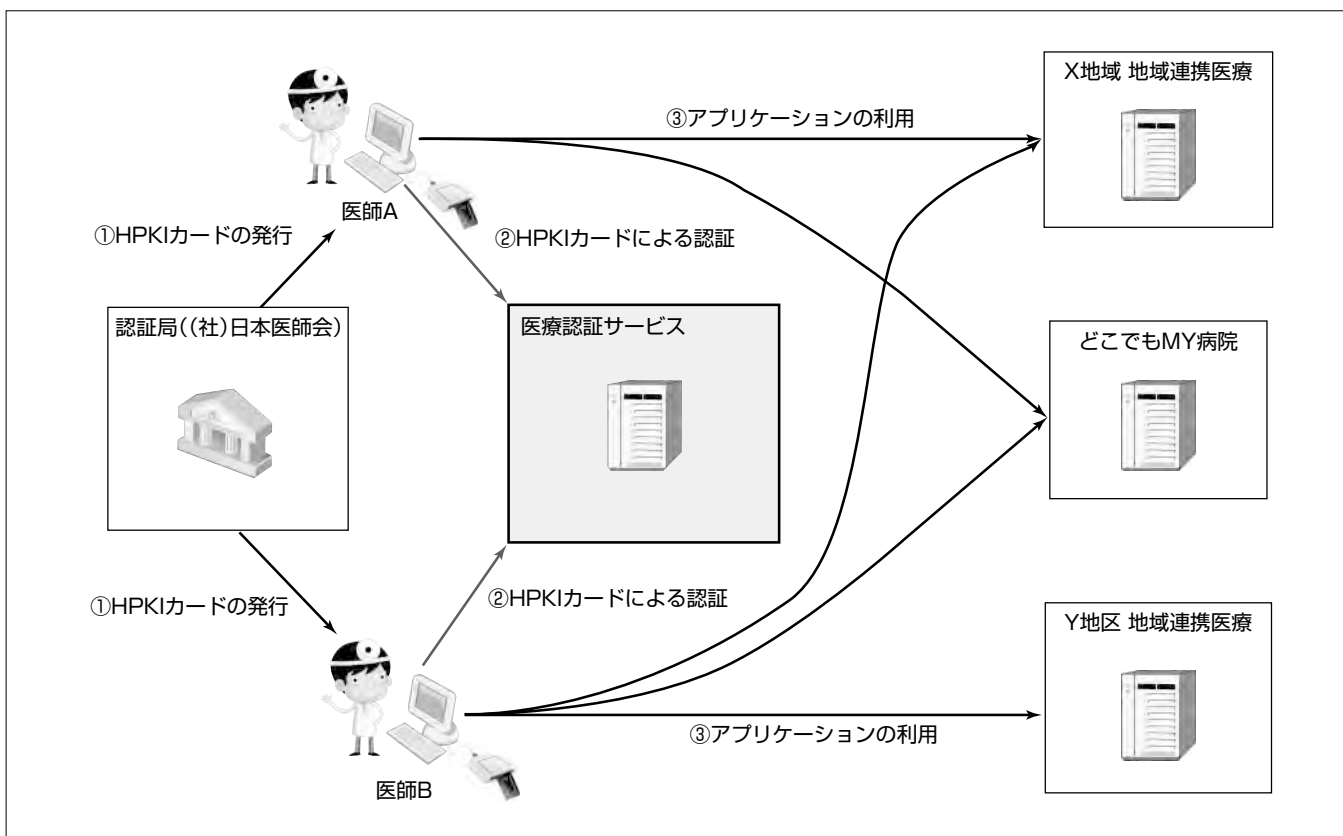
我が国では、高齢化の進展、医師の偏在化等が顕著になっており、現場のニーズに適合した医療システムの構築が重要となる。一方、セキュリティのポリシー設計や実装に当たっては、医療情報を取り扱うための注意が必要であり、署名・認証における標準化技術として厚生労働省が進める“保健医療福祉分野における公開鍵暗号基盤”(Healthcare Public Key Infrastructure: HPKI)の幅広い活用が求められている。

三菱電機インフォメーションシステムズ株(MDIS)が参加した医療分野共通認証基盤整備コンソーシアムでは、経済産業省の平成22年度“医療情報化促進事業”で共通に利用可能なHPKIを活用した認証基盤の整備を行った。これまで、個々のシステムで認証情報の管理を行っていたが、この認証基盤によって一元的な認証を行うことが可能となり、

個々のシステムでの認証情報の管理は不要となる。また、医師の資格確認も容易に実施できる。

認証の一元化のために、HPKIの証明書を使った個人認証を行う医療認証サービスシステムを構築した。また、医療認証サービスシステムで認証した認証情報を取得できるモジュールの開発を行い、他の医療情報化促進事業に提供し、利用できるようにした。

今後、医療情報化促進事業以外でも医療機関連携に幅広く活用してもらえるように、普及啓発活動を進めていくことが課題となる。また、開発したモジュールを応用することで、様々な国家資格(薬剤師、歯科医師、看護師等)に対応した利用者認証を実現することができるので、医師のみならず、医療全体の基盤となるシステムとして普及拡大に努める。



医療認証サービス

これまで、個々のシステムで認証システムを構築し認証情報の管理を行っていた。今回の基盤整備事業では、HPKIカードを使って医療認証サービスで医師の認証を行い、その認証情報を提供することで個々のシステムで医師の認証情報の管理は不要となる。医師は、一度の認証で複数のアプリケーションを利用できるため利便性が向上する。

1. ま え が き

我が国では、高齢化の進展、医師の偏在化等が顕著になっており、質の高い医療サービスなどを受けるための環境整備が急務となっている。

医療情報化では、現場のニーズに適合したシステム、現場の実情を反映したシステムの構築が重要である。しかし、相互運用性の確保やセキュリティ対策については、現場で個々に対策を立てるのではなく、我が国として標準的な対応が求められている。標準化の必要性、統一されたセキュリティのあり方については、過去の事業の検証も踏まえ、例えば厚生労働省の“医療情報システムの安全管理に関するガイドライン”⁽¹⁾などにまとめられている。ところが、そのような指針が存在しても、現場の実情としては各種の解釈が存在し、必ずしも統一された標準形式やセキュリティ対策が取られているとは言えない。

一方、署名・認証における標準化技術として、厚生労働省が進める保健医療福祉分野における公開鍵暗号基盤(Healthcare Public Key Infrastructure: HPKI)が存在しており、広く活用することが求められている。

本稿では、HPKIを活用した医師向けの認証サービスを通して、医師の利便性向上を実現した医療認証基盤について述べる。

2. 医療認証基盤整備事業

経済産業省の平成22年度“医療情報化促進事業”で、“どこでもMY病院構想”(以下“MY病院”という。)の実現に向けた実証事業、シームレスな地域連携医療(以下“地域連携医療”という。)の実現に向けた実証事業、及び共通項目の開発に向けた実証事業が実施された。共通項目では、実証事業の多くのフィールドでの活用が見込まれる機能の整備を行うが、MDISが参加する医療分野共通認証基盤整備コンソーシアムでは、医師の認証と資格確認を共通化する医療認証基盤整備事業を推進した。

MY病院や地域連携医療では、患者(国民)の医療・健康情報を取り扱うため、この基盤整備事業では次の実現を目的とした。

- (1) 患者(国民)の情報にアクセスしてよい資格者の確実な認証
- (2) 認証の一元化(一度の認証で複数のアプリケーションが利用できる)による利用者(医師)の利便性向上
- (3) 個々の医療アプリケーションで医師の認証情報管理や資格確認を行う必要がなくなることによるシステム構築・運用費用の抑制

この基盤整備事業では、(社)日本医師会(以下“日本医師会”という。)から発行された医師向けの証明書で個人認証を行う医療認証サービスシステムを構築した。また、医療認証

サービスシステムの認証情報を取得できるモジュールの開発を行い、他の医療情報化促進事業に提供し、認証情報を活用できるようにした。

3. 開発したシステム

3.1 システムの概要

医師の認証はHPKIカードを使って行う。HPKIカードは日本医師会から発行される証明書を収めたICカードであり、証明書に医師の登録番号となる医籍番号及びHPKIで定義されている保健医療福祉分野の国家資格情報であるhcRole(health care Role)が記載されている。医師の場合、hcRoleには“Medical Doctor”が入る。

医師は医療認証サービスシステムにアクセスして個人の認証を行う。その認証情報はSAML(Security Assertion Markup Language)と呼ばれる認証情報をデータ交換するための技術を使ってMY病院や地域連携医療等の医療アプリケーションに提供される。医療アプリケーションは医療認証サービスシステムから取得した認証情報を基にアプリケーションのサービス提供を行う。

MDISは医師の認証を行う医療認証サービスシステムの構築と、医療アプリケーション側で認証情報を取得できるSAML連携モジュールの開発を行った。この基盤整備事業におけるシステムの概要を図1に示す。

3.2 資格者の確実な認証

医師個人の確実な認証のために、医療認証サービスシステムではIDパスワードではなくHPKIカードを使った認証を行う。HPKIカードを使用することで、カードを持っていることと、利用するためPIN(Personal Identification Number)が必要なことの2要素認証となり、セキュリティの高い個人認証が実現できる。

医療認証サービスシステムでは、HPKIカードの証明書の検証及び失効確認を行う。その上で証明書内に記載されている医籍番号を取得し、個人の認証を行う。証明書のシリアルナンバーではなく、格納してある情報で確認が行えるため、証明書の再発行や更新に伴う認証情報の再登録作業を必要としない。また、証明書のどの情報で個人を確認するかは設定ファイルで指定することが可能であり、HPKIに限らず通常のPKIでもそのまま利用可能で医療系以外のシステムにも適用可能である。

医師の資格確認では、証明書に記載されているhcRoleを取得して医療アプリケーションに提供する。医療アプリケーションでは、hcRoleを確認することで医師であることが確認でき、また、証明書記載のhcRoleを使用しているため、医師以外のhcRoleにも容易に対応できる。証明書に記載されているhcRoleの取得は通常のPKIモジュールで対応することは難しく、追加でhcRoleを取得するモジュールを作成する必要があるが、MDISは既にhcRoleを取得するモジュ

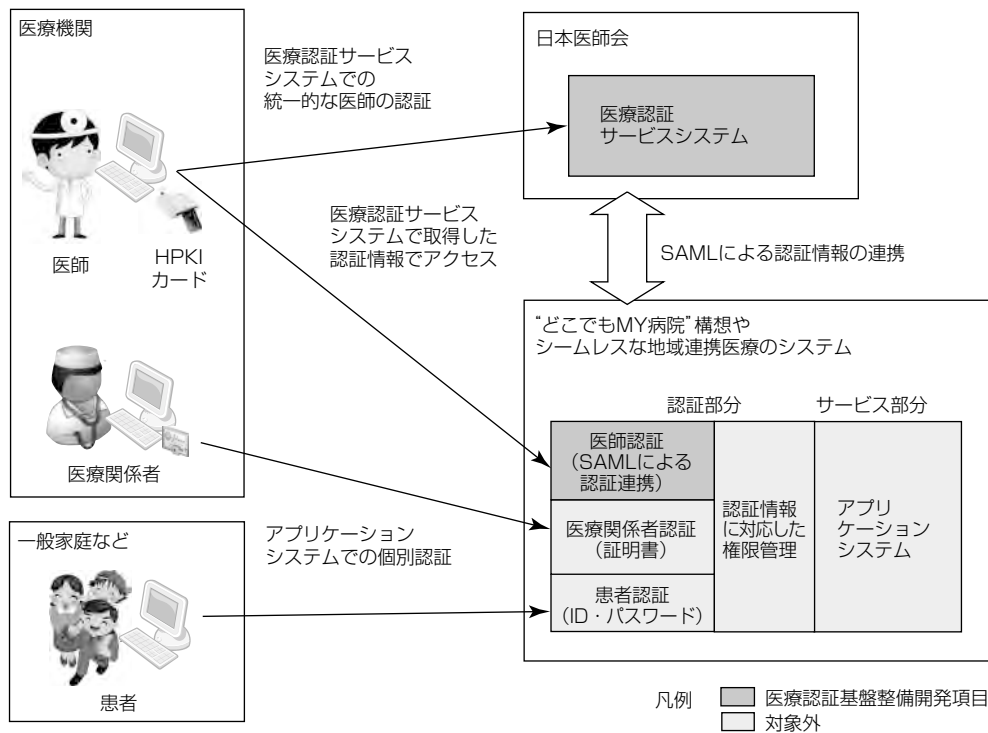


図1. システムの概要

ールを開発していたため、容易に取得することができた。

3.3 認証の一元化と認証情報の提供

従来、医療アプリケーションを利用する際には、アプリケーションごとに認証が必要であった。例えば、アプリケーションAで認証を行った後、アプリケーションBを利用する場合、Bでも認証が必要となり、利用者(医師)にとっての利便性を欠いていた。今回、HPKIカードで統一的に認証を行う医療認証サービスシステムを構築し、その上で認証を行うことによってアプリケーションごとの認証を不要とすることができた。

医師の認証を一元的に行うための医療認証サービスシステムは、医療アプリケーションとは独立したサイトに構築した。認証のための情報に関しては、日本医師会の認証局と連携し、認証局が発行した証明書の情報一覧を取得する。また、証明書の失効情報に関しては、定期的に取りこみから取得する。この基盤整備事業では、日本医師会内に医療認証サービスシステムを構築し、運営は日本医師会が行っている。

利用者サイトには、利用者が使用する参照クライアント及びMY病院や地域連携医療の医療アプリケーションが存在する。医療情報を扱うため、利用者サイト内は“医療情報システムの安全管理に関するガイドライン”に沿ったネットワークで構築している。

利用者サイトと医療認証サービスサイトはインターネットで接続されている。そのため、利用者サイトからはプロキシなどを使った代理接続を行い、セキュリティを確保する。各サービスサイトの構成を図2に示す。

認証情報の提供に当たっては、この整備事業以外にも幅広く利用できるように規格を制定する必要がある。SAMLはインターネット上のIDやパスワードを交換するためのXML(Extensible Markup Language)仕様であり、シングルサインオンを行う際に主に使われる技術である。この基盤整備事業ではSAML2.0の規約⁽²⁾に沿って認証情報を提供するための仕様を策定し、SAML実装仕様書⁽³⁾を作成した。この実装仕様書に従うことで、様々な医療アプリケーションから認証連携を行うことが可能である。SAMLを使った認証情報提供の流れを図3に示す。

利用者(参照クライアント)は医療アプリケーションにサービス利用の要求を行う(①)。医療アプリケーションでは、利用者がまだ認証されていない場合、参照クライアントを経由して医療認証サービスシステムに認証要求を行う(②)。医療認証サービスシステムではHPKIカードによる個人認証を行う(③、④)。認証情報は直接参照クライアントには提供せず、アーティファクトと呼ばれる認証したことを識別するための情報を参照クライアント経由で医療アプリケーションに提供する(⑤)。医療アプリケーションは取得したアーティファクトの情報に基づき、医療認証サービスシステムから認証情報として医籍番号とhcRoleを取得する(⑥、⑦)。参照クライアントを経由せず、直接医療認証サービスから医療アプリケーションに認証情報を提供するため、セキュリティ強度が高い。医療アプリケーションは取得した医籍番号とhcRoleを基に利用者へサービスの提供を行う(⑧)。また、既に利用者の認証が行われている場合は、②～⑦の処理は省略される。

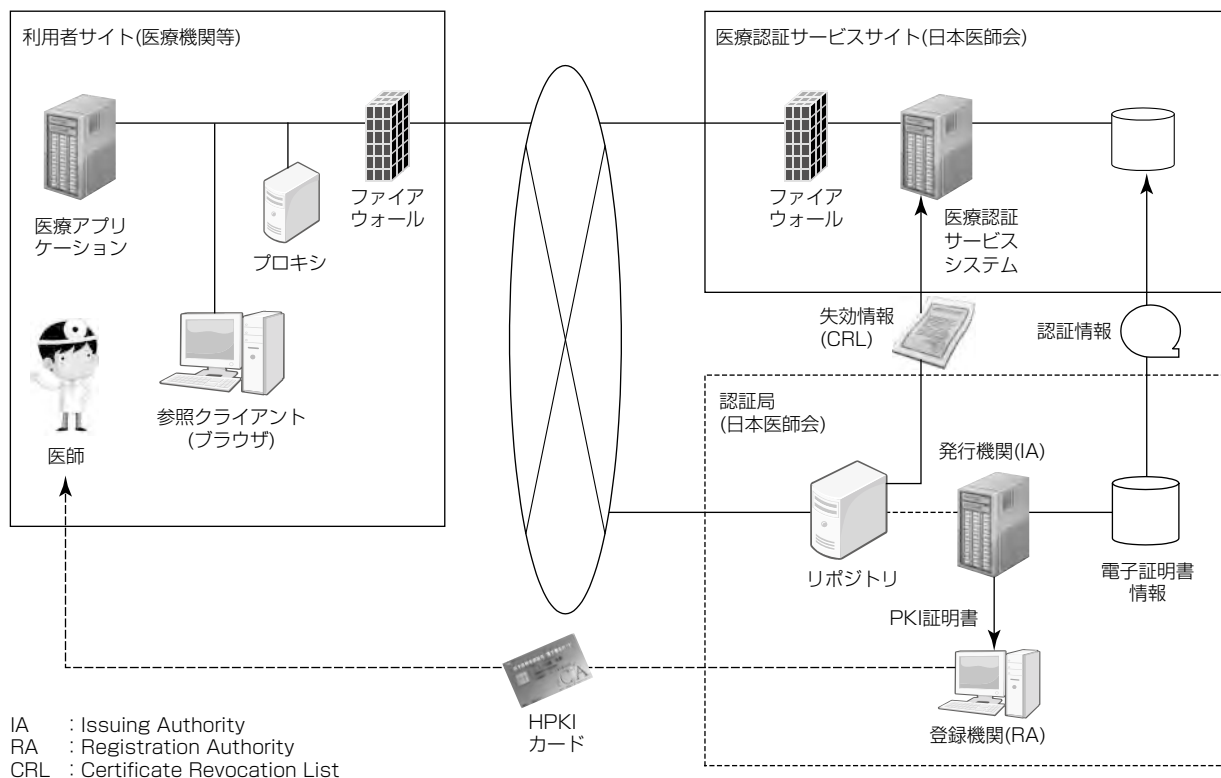


図2. サービスサイト

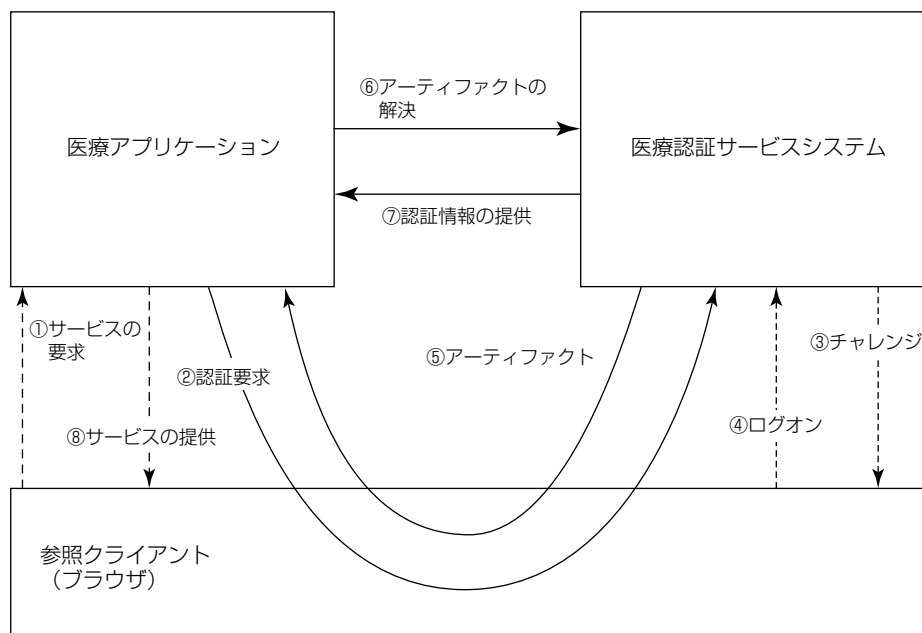


図3. 認証情報提供の流れ

3.4 医療アプリケーションの構築・運用負荷抑制

医療アプリケーション側でのシステム構築・運用負荷を抑制するため、医療認証サービスシステムに連携して認証情報を容易に取得できるSAML連携モジュールと呼ばれるモジュールの開発を行った。このモジュールは、参照クライアントと医療アプリケーションの間に入るサーバである。医療認証サービスシステムから取得した医師の認証情報を確認した上で、医療アプリケーションに対してリクエスト

を中継する。医療アプリケーションに対しては、認証情報をHTTP(Hypertext Transfer Protocol)におけるヘッダ情報で提供する。その内容を図4に示す。

SAML連携モジュールを導入することで、HTTPのヘッダで提供される認証情報を処理すればよく、個別にHPKIカードの認証やhcRoleを取得する機能を開発する必要がない。そのため、医療アプリケーション側の開発負荷が軽減される。

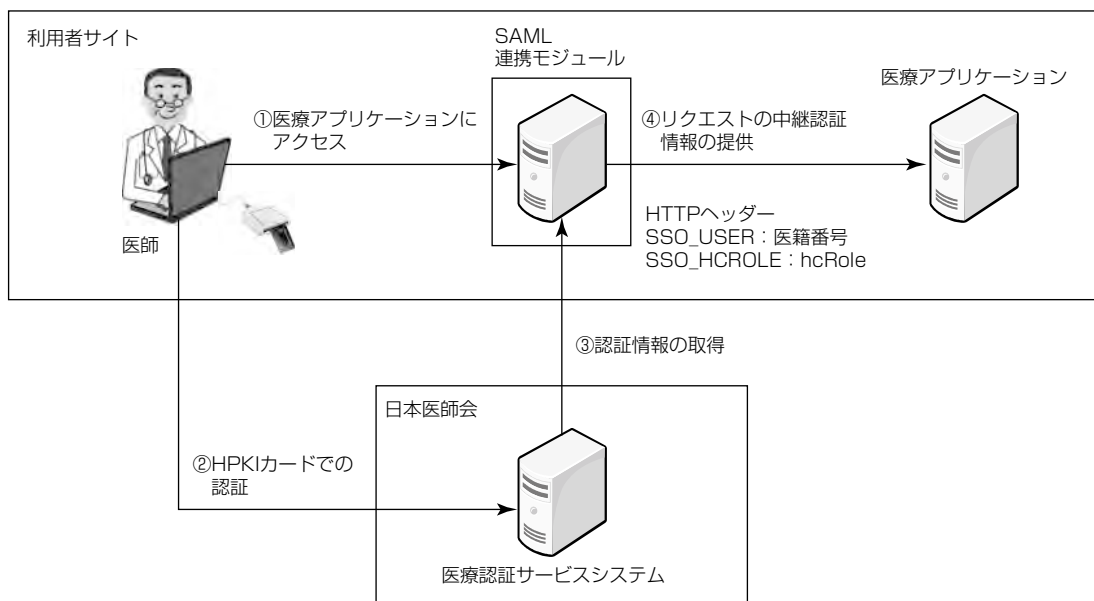


図 4. SAML連携モジュール

また、医師に新規のHPKIカードが発行された場合や、医師の資格に問題が発生し証明書が失効した場合、SAML連携モジュールが医療認証サービスに問い合わせ確認するため、医療アプリケーション側での医師の認証情報の追加削除が不要となり運用負荷を下げる事が可能となる。

4. むすび

この基盤整備事業で構築した医療認証サービスシステムの運用が開始され、“医療情報化促進事業”の、MY病院及び地域連携医療の事業に提供され、実際に医療認証サービスシステムと連携した認証を行っている⁽⁴⁾⁽⁵⁾。そのため、基盤整備事業における目的を十分に果たすことができたと考えている。

医療認証サービスは日本医師会が公益事業として運用することによって、全国規模での展開が容易である。

今後は、医療情報化促進事業以外にも医療機関を連携するシステムに幅広く活用してもらえようように、普及啓発活動を進めていく。

また、今回のシステムを応用することで、医師以外の様々な国家資格(薬剤師、歯科医師、看護師等)に対応した利用者認証や、医療分野以外でもWebアプリケーションにおける認証システムとして提供していきたい。

参考文献

- (1) 厚生労働省：医療情報システムの安全管理に関するガイドライン 第4.1版 (2010)
<http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf>
- (2) Scott Cantor, et al: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (2005)
<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- (3) 医療分野共通認証基盤整備コンソーシアム：SAML実装仕様書第1.0版 (2012)
<http://www.keieiken.co.jp/medit/pdf/240423/7-data.pdf>
- (4) 医療分野共通認証基盤整備コンソーシアム：平成22年度医療情報化促進事業(医療認証基盤整備事業)―どこでもMY病院構想及びシームレスな地域連携医療の実現に向けた実証事業―成果報告書 (2012)
<http://www.keieiken.co.jp/medit/pdf/240423/7-report.pdf>
- (5) 株式会社NTTデータ経営研究所：平成22年度医療情報化促進事業最終報告会 (2012)
http://www.keieiken.co.jp/medit/pdf/report_20120214.pdf

ISMSを利用した 情報セキュリティ対策の要件定義

岩本 仁*
菅原和則*

Requirement Definition Method Using ISMS for Information Security Control

Hitoshi Iwamoto, Kazunori Sugahara

要 旨

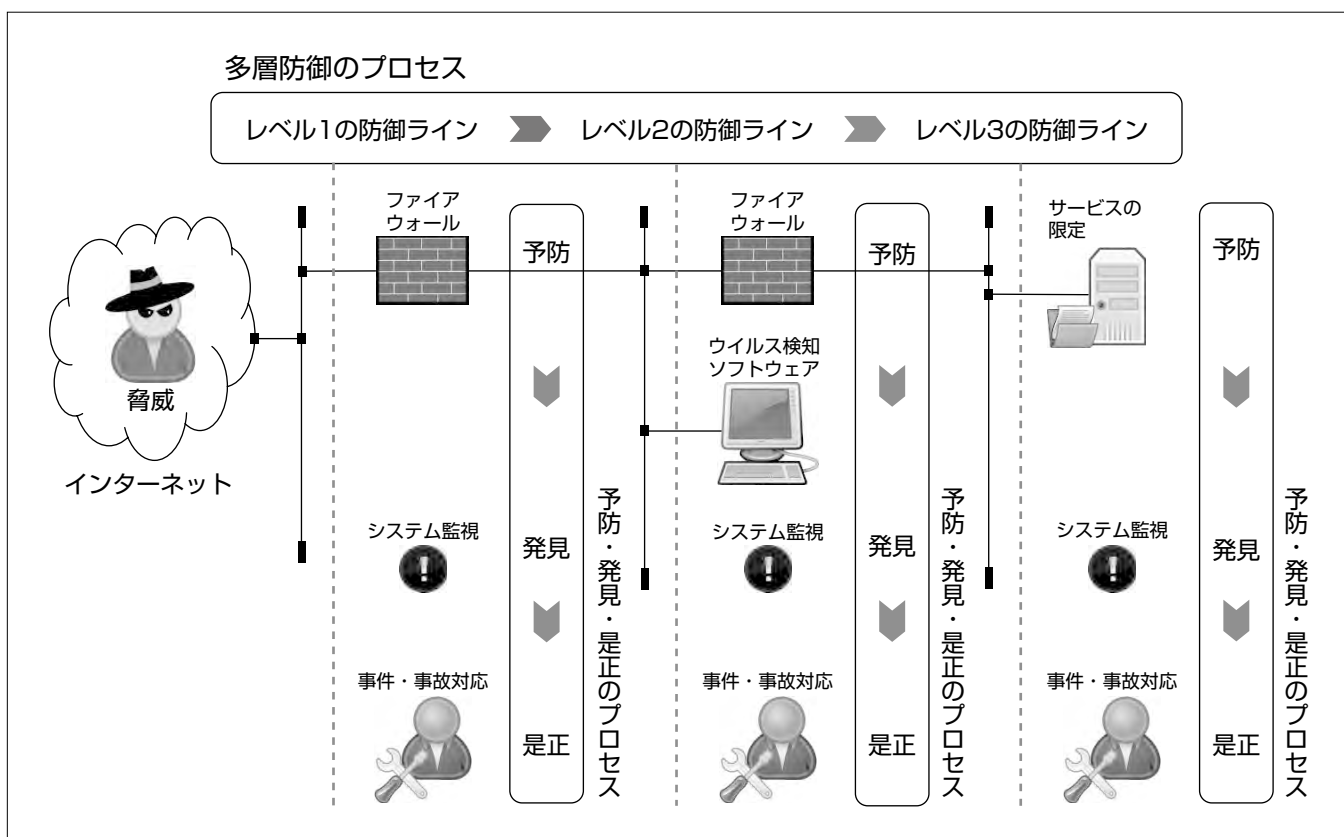
情報セキュリティ対策とは、特定の製品のことでなく、脅威から情報を守るために個々の対策がつながって機能するプロセスである。情報セキュリティ製品や管理手順をプロセスとしてつなぎ、効果的な情報セキュリティ対策を構築するためには、情報セキュリティマネジメントシステム (Information Security Management System : ISMS)⁽¹⁾が規定するリスクアセスメントを活用して、情報セキュリティ対策の要件定義を行うとよい。

リスクアセスメントでは、情報を狙う脅威の手口を分析し、次に対策の不備を見つける。そして不備を補うための対策をISMSの規定する133種類の選択肢から選ぶ。

選んだ対策は、プロセスとして機能するようにまとめ、

情報セキュリティ対策の要件として定義する。プロセスには2種類ある。一つ目は、多層防御のプロセスで、守るものを中心にしてレベルごとに構築した防御ラインが順に機能することで脅威からの攻撃を防ぐ。二つ目は、予防・発見・是正のプロセスで、事件や事故が発生する前、発生したとき、発生した後の順に機能する。脅威からの攻撃を防ぎきれなかったときに、攻撃をいち早く発見し、被害の拡大を防ぎ、情報システムや業務を回復することができる。

本稿では、三菱電機インフォメーションシステムズ株式会社 (MDIS)がISMSの導入・維持のコンサルティングを通し、ISMSによるリスクアセスメントと他の技法を交えて行っている情報セキュリティ対策の要件定義方法について述べる。



プロセスとしての情報セキュリティ対策の例

多層防御のプロセスでは、レベル1の防御ラインで、外部から内部ネットワークへの通信をファイアウォールで制限する。レベル2では、二つ目のファイアウォールでサーバへの通信を制限し、パソコンにウイルス検知ソフトウェアを稼働させる。レベル3では、サーバで稼働するサービスを限定し、脆弱(ぜいじゃく)性を減らす。それぞれのレベルに、予防・発見・是正のプロセスがあり、予防できなかった攻撃をシステム監視によって発見し、事件・事故として対応し、被害の拡大を防ぎ、システムを回復する。

*三菱電機インフォメーションシステムズ株式会社

1. ま え が き

MDISは、ISMSのコンサルティングを通して、効果的な情報セキュリティ対策を実現するため、リスクアセスメントを行って、個々の対策を実施の順序に統合したプロセスとして要件を定義してきた。本稿ではその手順の概要を述べる。

2. ISMSの特徴と利点

ISMSは、PDCA(Plan Do Check Action)サイクル、文書管理、経営陣の責任等といったマネジメントに関する点では、品質マネジメントシステム⁽²⁾や環境マネジメントシステム⁽³⁾と同じである。しかし、他のマネジメントシステムにはない特徴が二つある。一つ目は、どのような情報セキュリティ対策を実行するかをリスクアセスメントの結果に基づき決定する点であり、二つ目は、実行する情報セキュリティ対策を選択肢から選ぶ点である。

リスクアセスメントを行い、情報セキュリティ対策を選択肢から選ぶには利点がある。リスクアセスメントで自組織内外の情報セキュリティに関する状況が把握できるので、対策的のが絞れて無駄が減らせる。一方、規格化された選択肢から対策を選べば、対策の漏れが減らせる。これがISMSの利点である。

3. リスクアセスメント

3.1 概 要

リスクアセスメントは、孫子のいう、“彼を知りて己を知れば、百戦してあやうからず”⁽⁴⁾に通ずる作業である。ISMSでは、“彼”のことを“脅威”、“己”のことを“脆弱性”と呼ぶ。脅威は、利害関係者に損害を与える何かであり、脆弱性は、脅威がつけこんでくる対策の不備である。脅威と脆弱性を知り対策を打てば、情報セキュリティも危うくなくなる。

ISMSが規定するリスクアセスメントの手順は、大きくまとめると次のようになる。

- (1) 守るべき資産の特定
- (2) 脅威が狙う脆弱性の特定
- (3) 脆弱性対策の選定

このリスクアセスメントの手順に従って対策を選ぶ方法を次に述べる。

3.2 守るべき資産の特定

ISMSによれば、資産とは“組織にとって価値を持つもの”である。例えば、業務に使用する情報システムや媒体、建物・施設が資産である。

守るべき資産を特定するためには、まず守る範囲を定義して、その中から資産を見つける。守る範囲は、ISMSでは、“事業・組織・所在地・資産・技術の見地”から決める

ことになっている(表1)。

適用範囲を定義するのは、脅威が狙う対策の不備を見つけるためである。したがって、定義には、不備を見つけるために必要な情報を記載し、不要な情報を省く。例えば、想定した脅威が窃盗ならば、犯人の侵入経路が見つけやすいように、壁の有無や入り口の場所を平面図に定義するが、スプリンクラーの位置は不要である。コンピュータウイルスを使ったサイバー攻撃を想定するならば、IPパケットの流れを掴(つか)むためネットワーク層の構成を定義するが、通信ケーブルの配線に関する情報は不要である。

3.3 脅威が狙う脆弱性の特定

地震のような自然災害に対する脆弱性を特定するためには、被害が起きる原因を調べる。一方、コンピュータウイルスが狙う脆弱性を特定するためには、その目的と手口を調べる。ここでは、脅威の手口を分析する方法として攻撃ツリー(Attack Tree)⁽⁶⁾について述べる。

例えば、機密情報の取得を目的としてコンピュータウイルスを情報システムに送り込んでくる脅威については、図1のような攻撃ツリーを書く。

脅威の目的を一番上の箱に書き、手口を攻撃手順に分解して、順に下につなぐ。箱をつなぐ線には、andとorの2種類がある。andは、順に行う手順を示す。図1では、脅威の目的は、“機密情報を取得する”ことで、そのためには、“ウイルスをパソコンで実行”させ、“ウイルスがファイルサーバにアクセス”し、“ウイルスがデータを外部に発信”する。“ウイルスをパソコンで実行させる”ためには、“ウイルスをメールで届ける”か、“Webサイトからダウンロードさせる”。この二つの箱をつなぐ線にはandがないが、

表1. 適用範囲の定義方法の例

項目	具体例	定義方法
事業	製品やサービス、それを提供する業務の流れ	業務フロー図、製品の仕様書
組織	業務を行う部署	組織図、正社員・非正社員の構成表
所在地	業務を行う場所	建物の住所、ハザードマップ
資産	建物・設備	建物の配置図、フロアの平面図
技術	情報システムの構成	ネットワーク構成図、ハード・ソフトウェア構成図

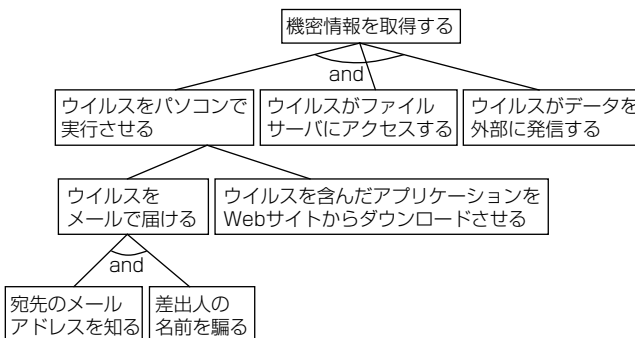


図1. 攻撃ツリーの例

これはorを意味する。最後に，“ウイルスをメールで届ける”ために，“宛先のメールアドレスを知って”，“差出人の名前を騙(かた)る”。機密情報を取得するためには，一番下の左側の手順から順に実行すればよい。

脅威から機密情報を守るためには，各々の攻撃手順が狙う脆弱性をなくすことが必要である。図1の攻撃手順から脆弱性を求めた結果を表2に示す。

3.4 脆弱性対策の選定

ISMSは，脆弱性への対策を“管理策”と呼び，11のカテゴリに分けて，133種類の選択肢を規定している(表3)。

各カテゴリの最初の英字“A”は，選択肢がISMSの“附属書A”に記載されていることを示し，数字は，附属書Aでの通し番号である。これが5から始まるのは，管理策のガイドライン⁽⁶⁾とのつながりを示すためである。

脆弱性への対策として管理策を選択肢から選んだ例が表4である。説明として管理策の内容も追加した。

一つの脆弱性への管理策が二つ以上考えられる場合，管理策のガイドラインの記述が最も近い管理策を複数個選ぶ

表2. 攻撃手順で狙われる脆弱性の例

攻撃手順	脆弱性
宛先のメールアドレスを知る	従業員の氏名からメールアドレスが類推できる
差出人の名前を騙る	メールの差出人を本人確認できない
ウイルスをメールで届ける	パソコンにメールが届く
ウイルスを含んだアプリケーションをWebサイトからダウンロードさせる	外部のWebサーバからソフトウェアをダウンロードできる
ウイルスをパソコンで実行させる	ウイルスを実行する環境がパソコンにある
ウイルスがファイルサーバにアクセスする	パソコンからファイルサーバにネットワークでアクセスできる
ウイルスがデータを外部に発信する	パソコン又はファイルサーバから外部にデータが送信できる

表3. 管理策のカテゴリ

カテゴリ	主な管理策の内容	管理策数
A.5 セキュリティ基本方針	基本方針の策定とレビュー	2
A.6 情報セキュリティのための組織	組織内の管理体制，外部組織と関係	11
A.7 資産の管理	資産の分類，ラベル付け，台帳管理	5
A.8 人的資源のセキュリティ	正社員・非正社員など要員の管理	9
A.9 物理的及び環境的セキュリティ	建物や設備の設置や運用	13
A.10 通信及び運用管理	情報・通信システムの運用，その稼働状況の監視	32
A.11 アクセス制御	アクセス制御方針の策定，情報システムの利用者の管理，ネットワークの構成	25
A.12 情報システムの取得，開発及び保守	情報システムの開発・調達の際のセキュリティ要件	16
A.13 情報セキュリティインシデントの管理	情報セキュリティに関する事件や事故の報告と対応	5
A.14 事業継続管理	事業継続計画の策定と実施	5
A.15 順守	個人情報保護法，不正アクセス禁止法等の法令の遵守	10

ことになっている。表4では，ウイルス対策の管理策として，“A.10.4.1 悪意のあるコードに対する管理策”と“A.10.4.2 モバイルコードに対する管理策”を選んだ。昨今のコンピュータウイルスは，JavaScript^(註1)などのモバイルコードもあるからである。

最適な管理策が選択肢にない場合には，管理策を定義してもよい。表4では，サーバの機能を限定する“CM-7機能の限定”を，米国のガイドライン⁽⁷⁾から引用して追加した。

(注1) JavaScriptは，Oracle Corp. の登録商標である。

4. 管理策のプロセス統合

先に述べたようにして選んだ管理策は，実施する順序が決められた1つのプロセスとして統合し，情報セキュリティ対策の要件として定義する。これらのプロセスには2種類ある。一つは，多層防御(Defense-in-Depth)⁽⁸⁾であり，もう一つは，予防・発見・是正である(表5)。

多層防御とは，守る対象を中心にして，脅威が侵入してくる経路で遠くから近くへレベル分けし，レベルごとに防御ラインを敷くことをいう。

表5では，インターネットからネットワークを経由して悪意のある者がサーバを攻撃することを想定して，図2に示すように，レベルを三つに分けた。レベル1の防御ラインにはファイアウォールを設置し，ネットワーク利用方針を決めて，インターネットと内部ネットワークとの通信を制限する。レベル2の防御ラインは，ネットワークをつなぐファイアウォールとパソコン上のウイルス検知ソフトウェアである。レベル3の防御ラインは，サーバ自身であり，脆弱性を減らすために，クライアントに提供するサービス

表4. 選んだ管理策の例

脆弱性	管理策(内容)
従業員の氏名からメールアドレスが類推できる	A.11.5.2 利用者の識別及び認証(メールアドレスの形式を変更)
メールの差出人を本人確認できない	A.12.3.1 暗号による管理策の利用方針(メールに電子署名)
パソコンにメールが届く	※対策しない：メールをパソコンで受信する必要が業務上あるから
外部のWebサーバからソフトウェアをダウンロードできる	A.11.4.1 ネットワークサービスの利用についての方針(ソフトウェアのダウンロードを禁止)
ウイルスを実行する環境がパソコンにある	A.10.4.1 悪意のあるコードに対する管理策(添付ファイルなどを点検)
	A.10.4.2 モバイルコードに対する管理策(実行を一部，禁止)
パソコンからファイルサーバにネットワークでアクセスできる	A.11.4.5 ネットワークの領域分割(サーバを別のネットワークに設置) CM-7機能の限定(クライアントに提供するサービスを限定)
パソコン又はファイルサーバから外部にデータが送信できる	A.10.6.1 ネットワーク管理策(ファイアウォールで送信を制限)

表 5. 管理策をつないだプロセス

	レベル 1	レベル 2	レベル 3
予防	A.10.6.1 ネットワーク管理策 A.11.4.1 ネットワークサービスの利用についての方針	A.10.4.1 悪意のあるコードに対する管理策 A.10.4.2 モバイルコードに対する管理策 A.10.6.1 ネットワーク管理策 A.11.4.5 ネットワークの領域分割 A.11.5.2 利用者の識別及び認証 A.12.3.1 暗号による管理策の利用方針	CM-7 機能の 限定
発見	A.10.10.1 監査ログの取得 A.10.10.2 システム使用状況の監視 A.13.1.1 情報セキュリティ事象の報告		
是正	A.13.2.1 責任及び手順		
共通	A.8.2.2 情報セキュリティの意識向上, 教育及び訓練		

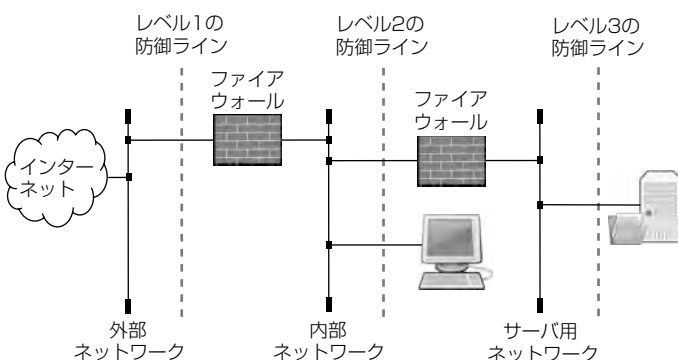


図 2. ネットワークでの多層防御の例

やインストールする運用ソフトウェアを制限する。多層防御全体として、レベル 1 の防御ラインが突破されたらレベル 2 で、それが突破されたらレベル 3 で防御するように管理策を実行する。

予防・発見・是正は、管理策を実行するタイミングが、事件や事故が起きる前か、起きたときか、起きた後かで分けられる。予防では、事件や事故が起きるのを防ぐ。発見では、事件や事故が起きたことを発見する。是正では、事件・事故の拡大を防ぎ、情報システムなどを回復する。

筆者の経験では、攻撃ツリーに基づいた脆弱性への対策は、脅威が目的を達成するのを防ぐことを考えるあまり、予防に偏る傾向がある。そのため、表 5 には、発見と是正を追加した。発見には、不正なパケットを検知するため“A.10.10.1 監査ログの取得”，“A.10.10.2 システム使用状況の監視”，“A.13.1.1 情報セキュリティ事象の報告”を、是正には、事件や事故の対応体制と手順を整えるための“A.13.2.1 責任及び手順”を含めた。“責任及び手順”とは、情報セキュリティの事件や事故の管理における責任と手順の意味である。

さらに、管理策全体について“A.8.2.2 情報セキュリティの意識向上，教育及び訓練”を追加した。メールの電子署名，システムの監視，事件・事故の対応等の手順をシステム管理者と利用者に教育する必要があるためである。要員の教育は，無視又は軽視されることがあるが，管理策の実行には必要であり教育内容と実施時期を必ず計画すべきである。

リスクアセスメントでは，想定した脅威の手口に対応するように管理策を選択するので，プロセスでの管理策同士のつながりが見えにくい，このような表を埋めていけば，足りない管理策を追加して，効果的で効率のよい情報セキュリティ対策の要件を導き出すことができる。

5. む す び

情報セキュリティ対策の要件を定義する手順をISMSでのリスクアセスメントと具体的な方法を交えて述べた。今後もISMS導入・維持のコンサルティングを通し，顧客の実情にあった情報セキュリティ対策の要件定義を提示していく。

参 考 文 献

- (1) JIS Q 27001：2006 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項，一般財団法人日本規格協会（2006）
- (2) JIS Q 9001：2008 品質マネジメントシステム—要求事項，一般財団法人日本規格協会（2008）
- (3) JIS Q 14001：2004 環境マネジメントシステム—要求事項及び利用の手引，一般財団法人日本規格協会（2004）
- (4) 金谷 治 訳注：新訂孫子，岩波文庫（2000）
- (5) Schneier, B.：Secrets and Lies：Digital Security in a Networked World, Wiley（2000）
- (6) JIS Q 27002：2006 情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範，一般財団法人日本規格協会（2006）
- (7) NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations, NIST（2009）
- (8) Homeland Security：Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, US-CERT（2009）

Android端末に対応したセキュアスマートフォンサービス

梶場純一*

Secure Smartphone Service Corresponding to Android Device

Junichi Haseba

要旨

三菱電機情報ネットワーク株式会社(MIND)のモバイルネットワークサービスは、顧客の業務システムを社内利用と同様に社外から安全・快適にアクセスできるリモートアクセスサービスである。既に、iPhone/iPad^(注1)のiOS搭載端末の利用を対象としたサービスを提供しており、多くのユーザーに利用されている。一方、スマートフォン/タブレット端末市場では、iOS搭載端末以外にAndroid^(注2)OS搭載端末も多く出荷され、企業での業務システムを利用する端末として顧客ニーズも高い。しかし、ネットワークや端末上アプリケーションの脆弱(ぜいじゃく)性など、セキュリティ面の課題があり業務用端末として導入に踏み切れない企

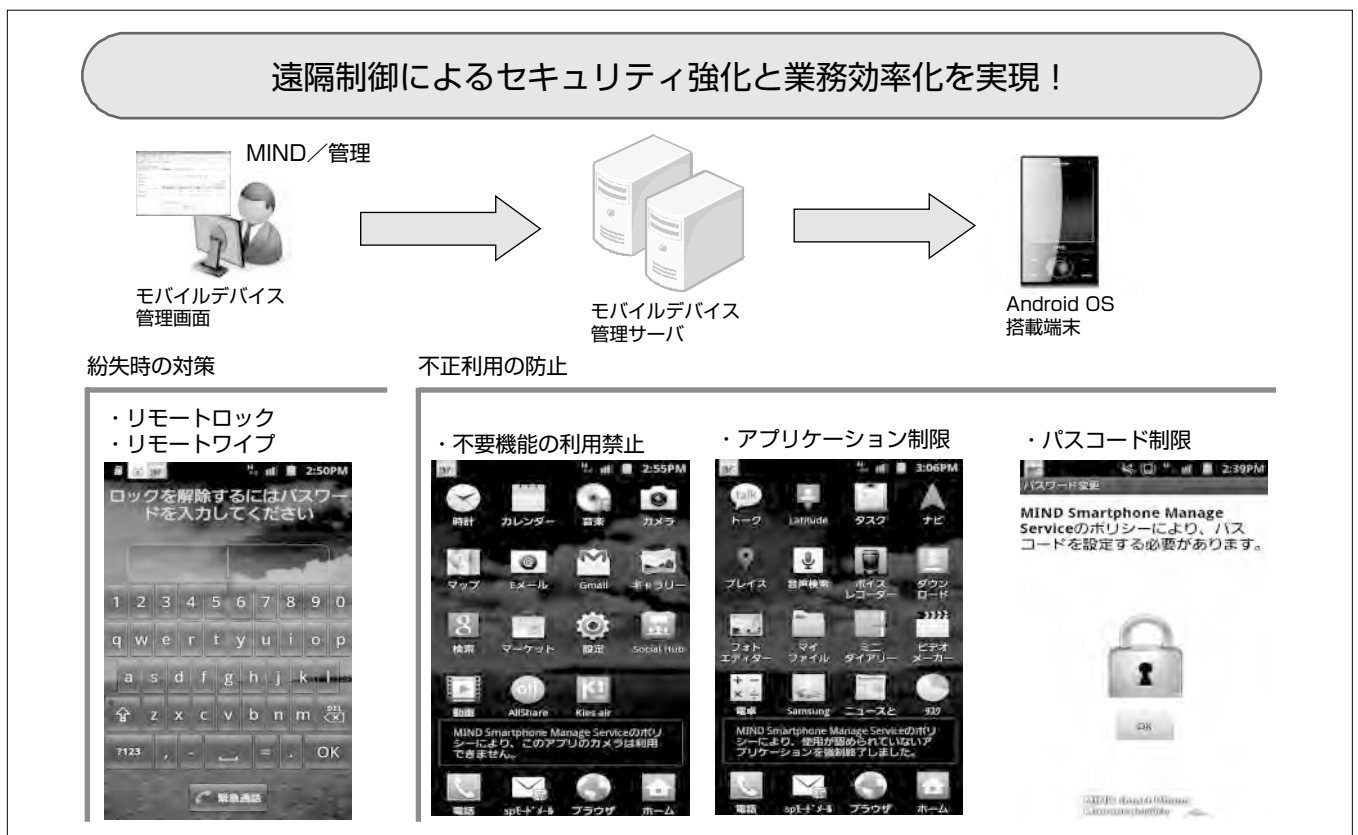
(注1) iPhone, iPadは、Apple Inc. の登録商標である。

(注2) Androidは、Google Inc. の登録商標である。

業も少なくない。

MINDは、それらの課題を“セキュアスマートフォンアクセスサービス”及び“スマートフォンマネージサービス”を提供することで解決し、Android OS搭載端末でも利便性とセキュリティを兼ね備え、安全・快適に利用できるリモートアクセスを実現した。

“セキュアスマートフォンアクセスサービス”では、暗号化通信と端末認証と個人認証を組み合わせ、許可された端末だけ社内業務システムにアクセス可能とし、“スマートフォンマネージサービス”では、端末の紛失・盗難時のリモートロック・リモートワイプや業務以外のアプリケーションの利用制限、インベントリ情報の可視化等、端末の管理・監視・制御を可能としている。



“スマートフォンマネージサービス”

スマートフォンマネージサービスは、紛失・盗難時のためのリモートロックや端末パスコードの設定ポリシーと業務上不要な機能(カメラ、Bluetooth^(注3)等)の利用禁止、管理者が指定したアプリケーション以外の使用制限等、端末の管理・監視・制御を実現している。

(注3) Bluetoothは、Bluetooth SIG, Inc. の登録商標である。

1. ま え が き

MINDのモバイルネットワークサービスは、顧客のOA (Office Automation)・メール・グループウェアや業務システム等を社内と同様に社外から安全・安心に利用できることが特長で、iPhone/iPadのiOS搭載端末を対象とした利便性とセキュリティを兼ね備えたサービスである。今回、スマートデバイス市場で急増するAndroid OS搭載端末の利用を可能とする機能を開発し、サービス提供を開始した。

本稿では、Android OS搭載端末の業務利用におけるセキュリティ対策の必要性と課題を示し、その解決策である“セキュアスマートフォンアクセスサービス”と“スマートフォンマネージサービス”の特長とサービス内容について述べる。

2. 市場 動 向

2.1 Android端末の市場動向

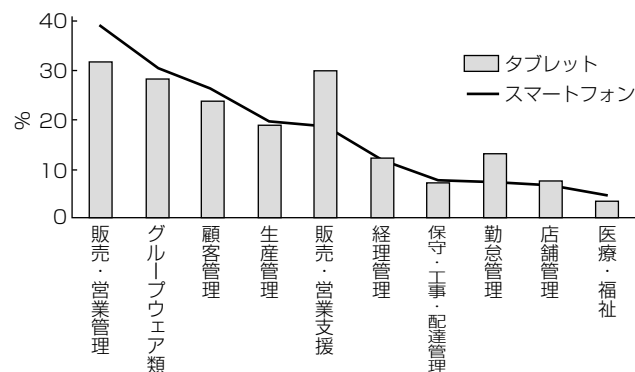
起動が早く軽量であることや画面に直接触れるという操作等、一般のパソコンにない機能が注目され、企業で導入するモバイル端末は、スマートフォン/タブレット端末に移り変わっている。企業が利用しているスマートフォンは、“販売・営業管理”や“グループウェア類”での利用割合が高い。

タブレット端末は、写真、動画、3D画像(CAD(Computer Aided Design)Viewerなど)等のメディアで効果的に情報を伝達できるだけでなく、カタログなどのペーパーレス化を図れる等の評価が高く、外出先から効率的に活用できる販売・営業支援のツールとして導入している企業が多い(図1)。

スマートフォン/タブレット端末販売台数の市場シェアを表1に示す。2010年に22.7%であったAndroid OS搭載端末の販売台数は、2015年には48.8%まで拡大すると予測されている。iOS搭載端末と比べ高いシェアを占めるAndroid OS搭載端末は、企業での業務システムを利用する端末として顧客ニーズが高まりつつある。

2.2 Android端末の特徴とセキュリティ課題

Android OS搭載端末とiOS搭載端末の特徴を表2に示す。



出典：株式会社インプレスR&D Android利用動向調査報告書2012

図1. 企業におけるタブレット端末の利用業務

Android OS搭載端末の場合は、数多くの端末メーカーから出荷され、我が国でも(株)エヌ・ティ・ティ・ドコモやKDDI(株)等の大手移動体通信事業者から発売されている。iOS搭載端末と比べると、端末機種やインストールするアプリケーションが豊富で選択肢が多い。また、オープンソースOSを搭載しており、アプリケーションや通信機能等の実装は端末メーカーや通信事業者に依存している。一方、iOS搭載端末の場合は、端末メーカーはApple社だけで、搭載するアプリケーションもApple社によって管理されている。

iOS上のアプリケーションは、Apple社が事前審査したものをApple Storeなどに限定した公式サイトからインストールするのに対し、Android上のアプリケーションはGoogle社が提供するGoogle Playなどに限定されず、通信事業者、端末メーカーを始め数多くのサイトから自由にインストールすることが可能である。そのため、事前審査を行っていないアプリケーションに関して、脆弱性の対策やセキュリティリスクを回避することが課題となっており、業務用端末としての導入に踏み切れない企業も少なくない。

2.3 企業が求めるスマートフォン/タブレット端末導入に必要なセキュリティ機能

企業がスマートデバイスに求めるセキュリティ対策を表3に示す。

Android OS搭載端末を業務端末として利用する場合のセキュリティ対策のポイントは、次の3点に大別することができる。

- (1) 通信経路のセキュリティ対策
- (2) 業務外・不正利用の禁止(デバイス制御)

表1. 世界のスマートフォン端末販売台数(OS別)

OS		2010年	2011年	2012年	2015年
iOS	販売台数(千台)	46,598	90,560	118,848	189,924
	市場シェア(%)	15.7	19.4	18.9	18.9
Android OS	販売台数(千台)	67,225	179,873	310,088	539,318
	市場シェア(%)	22.7	38.5	49.2	48.8
他OS	販売台数(千台)	182,824	197,268	201,540	375,656
	市場シェア(%)	61.6	42.1	31.9	32.3
合計	販売台数(千台)	296,647	467,701	630,476	1,104,898

出典：Worldwide Communication Device Open OS Sales to End Users by OS (Thousands of Units) Gartner (April 2011)

表2. 端末のOSと特徴

端末のOS	提供元	特徴
iOS	Apple社	①“Apple Store”の登録は、Apple社が審査したアプリケーションを登録 ②アプリケーションの配布や利用時にはApple社と契約。Apple Storeから配布、課金 ③iOS上でだけ稼働し、最新バージョンの適用が容易
Android OS	Google社	①“Google Play”の登録は、Google社は審査せず、その活用は利用者の裁量 ②通信業者などが運営するマーケットへの登録が可能。それぞれの基準で配布、課金 ③オープンソースのOSで、各端末メーカーが独自にカスタマイズして搭載 ④デバイスの選択肢が豊富 ⑤OSバージョンが同一でも機種依存あり

(3) 端末・アプリケーション管理の効率化

これらのポイントは、iOS搭載端末でも同様のニーズであったが、Android端末に特有なセキュリティリスクの回避として、利用するアプリケーションの制御や端末のポリシー違反の検知等を強化する必要があった。

3. リモートアクセスソリューション

Android OS端末におけるセキュリティ課題を解決するため、iOS搭載端末対応の既存の認証システムの仕組みと連携することで、端末固有の識別子とデジタル証明書を利用した端末認証やVPN(Virtual Private Network)通信を可能とし、不許可端末の利用防止を“セキュアスマートフォンアクセスサービス”で実現した。さらに、MDM(Mobile Device Management)による遠隔からのAndroid OS搭載端末の管理・監視・制御を“スマートフォンマネージサービス”で実現し、データ保護及び盗難・紛失対策に加え、きめ細かい管理権限の設定やポリシー違反の検知等の仕組みを実現した。また、複数端末の集中管理による一括設定などの効率化を可能としている(図2)。

3.1 セキュアスマートフォンアクセスサービス

このサービスは、データ通信を暗号化(IPSec^(注4))し、デジタル証明書による端末認証とユーザーID(IDentitier)とパスワードによる個人認証を組み合わせ、強固なアクセス制御を実現している。iOS搭載端末と同様に、Android OS搭載端末でもIPSecVPNモジュールや端末識別情報(IMEI(International Mobile Equipment Identifier),

MAC(Media Access Control)アドレス等)を搭載している。iOS搭載端末と同じ方式でこれらの端末情報を照合し、Android OS搭載端末の場合もアクセスが許可された端末及びユーザーだけ認可し、許可されていない端末及びユーザーであれば拒否することが可能である。

(注4) Security architecture for Internet Protocolの略で、IPパケット単位で改ざん防止や秘匿機能を持ったプロトコルである。

3.2 スマートフォンマネージサービス

このサービスの機能は、セキュリティ機能、ポリシー管理機能、端末管理機能の3つに分類される。それぞれの主な機能を表4、表5、表6に示す。

このサービスは、複数のスマートフォン/タブレット端末を企業のセキュリティポリシーで管理・監視・制御することを可能としている。利用端末の機種やインストールされているアプリケーション等の情報を収集する機能を持っている。また、端末の状態管理、紛失時の遠隔制御(リモートロック/リモートワイプ)、管理者が指定したアプリケーション以外の使用制限を実現し、企業の端末管理者に

表4. 主なセキュリティ機能

No.	分類	機能	内容
1	リモートワイプ	初期化	工場出荷時に初期化
2	リモートロック・アンロック	ロック・アンロック サイレン鳴動	ロック・アンロックの実行 リモートロック時にサイレンを鳴動
3	ローカルワイプ	-	ローカルロック時、所定の回数以上パスワードを失敗した際に、データを消去
4	遠隔削除	遠隔初期化 個別データ削除	内部SDカード内のデータを消去 個別のデータを消去

表3. 企業における主なセキュリティ対策

想定される脅威	脅威への対策
通信傍受・盗聴	暗号化通信による通信データの秘匿 通信環境に依存しない安全なアクセス 利用したアクセスログなどの収集管理
不正利用・不正侵入	企業が許可した端末・ユーザーのみ許可 パスワードポリシーの設定 業務上不要な機能の利用制限
情報搾取・漏洩・マルウェア感染	スマートフォン/タブレット端末の状態管理 紛失による情報漏洩(ろうえい)の防止と遠隔制御の実現 管理者が許可したアプリケーションソフトウェア以外の利用禁止

表5. 主なポリシー管理機能

No.	機能名	機能	内容
1	遠隔設定	ローカルセキュリティポリシー WLAN設定 特権SIM設定	パスワードポリシーの設定 無線LANのアクセスポイント情報の設定 SIM交換ロック時の設定
2	利用制限	デバイス利用制限	・カメラ機能の利用可否 ・Bluetoothの利用可否 ・外部メモリ(SDカード)の利用可否 ・無線LANの利用可否 ・緊急番号(110, 118, 119)以外への発信先制限
3	アプリケーション管理	インストール アプリケーション情報	ホワイトリストによるアプリケーションの利用可否

WLAN: Wireless LAN, SIM: Subscriber Identity Module

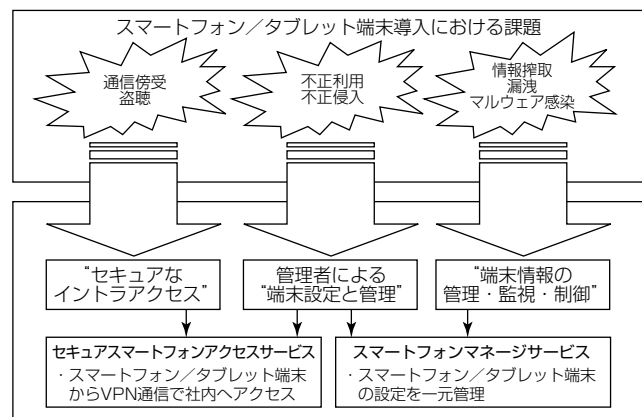


図2. スマートフォン/タブレット端末導入における課題と対策

表6. 主な端末管理機能

No.	機能名	機能	内容
1	遠隔情報取得	ロック・アンロック 端末情報	ロック・アンロックの状態取得 ファームウェア情報やメモリの空き容量等の情報取得
2	VPN設定	インストール アプリケーション情報 位置情報	インストールされているアプリケーションの情報取得 端末の位置情報の取得
3	遠隔監視	デバイス利用制限 ローカルセキュリティポリシー インストール アプリケーション情報 位置情報	利用制限状態の取得 ローカルセキュリティポリシー設定の定期取得 インストールされているアプリケーション情報の定期取得 端末の位置情報の定期取得

代わってMINDがサービスとして提供する。

次に、遠隔から搭載端末の管理・監視・制御する仕組みを述べる。iOS搭載端末の場合、Apple社が提供するAPNs (Apple Push Notification service)とモバイルデバイス管理サーバと端末間の通信・制御プロトコルが決められている。一方、Android OS搭載端末の場合は、Google社から“C2DM(Cloud to Device Messaging)サーバ”が提供されているが、複数端末の一元管理や機能拡張の柔軟性が乏しいため、国内外の大手通信事業者では、これとは方式が異なる国際標準方式のプロトコルを広く採用している。このサービスも国際標準方式のプロトコルを採用し、C2DMで実現できない管理者権限の設定とグループの階層化や企業のポリシーにあわせた複数端末への一括設定を可能とした。

また、セキュリティリスク回避のため、ユーザーの意思にかかわらず管理者からの指示を最優先とし、端末利用中のリモートロックなどの強制制御や端末に対する管理・制御のオペレーションの進捗・成否・レポート管理の情報収集機能を持ち、監査履歴の一元管理を可能としている。

3.2.1 サービス処理フロー

Android OS搭載端末の管理・監視・制御の処理フローを図3に示す。遠隔管理の処理は、国際標準のプロトコルであるOMA (Open Mobile Alliance) -DM (Device Management) ^(注5)方式を使用している。

(1) 端末照合

MDMシステムの端末操作画面で、事前に登録された端末の加入者番号(MSISDN: Mobile Subscriber ISDN (Integrated Services Digital Network) Number)及び端末製造番号(IMEI)を指定し、端末管理の制御要求を送信する(図3①)。MDMシステムでは、指定された端末への制御が許可されている場合、制御要求を受け付けると端末に対し制御を開始するためメッセージとしてPackage(以下“Pkg”という。) #0(DMN: DM Notification)を端末へ送信する(図3②)。Pkg#0(DMN)を受信した端末はパケット接続及びSSL(Secure Sockets Layer)ネゴシエーションを行う。端末はセッション確立後、IMEIなどの端末情報を含んだPkg#1をMDMシステムへ送信する(図3③)。Pkg#1を受信したMDMシステムは、指示された制御対象端末であるかをIMEIの照合によって判定する。

(2) 遠隔制御

判定後、制御コマンドを含んだPkg#2を端末へ送信する(図3④)。Pkg#2を受信した端末は、制御コマンドの内容に応じた制御を実行する。端末で制御完了後に、Pkg#3で完了報告をMDMシステムへ送信する(図3⑤)。

(3) 制御結果確認

MDMシステムはPkg#4で受信確認を端末へ送信し(図3⑥)、Pkg#3がMDMシステムで正常に受信されたことを端末が認識すると、DM制御を終了する(図3⑦)。同時

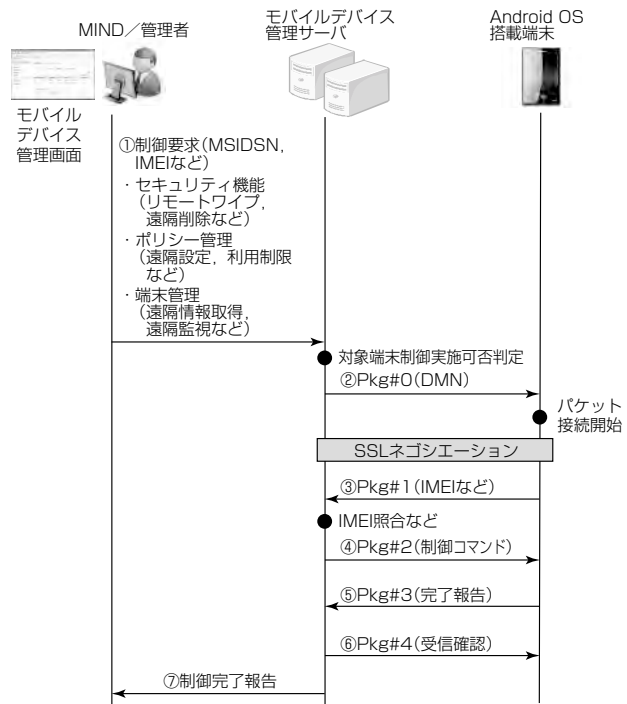


図3. スマートフォンマネージャーサービス実行時の処理フロー

にMDMシステムは、制御完了報告を端末操作画面に表示し、制御を終了する。また、制御完了時にMDMシステムの操作画面を通して端末の設定状態を確認できる。

(注5) OMAはモバイル関連のアプリケーションの標準化を進める団体であり、DMはデバイス管理機能である。

4. 今後の課題

企業におけるスマートデバイスの業務利用では、セキュリティ対策を維持しつつ、個人管理の端末を業務でも利用するBYOD(Bring Your Own Device)やIT資産管理の統合も注目されている。スマートフォン/タブレット端末のセキュリティ対策機能の拡充とマルチデバイス化の資産管理を可能とした統合的管理機能を付加する等、サービス機能の向上が今後の課題である。

5. むすび

Android OS搭載端末のスマートフォン/タブレット端末から、安全・快適に社外から社内業務システムが利用可能なサービスを実現した。今後は、多機能携帯端末であるスマートデバイスの特長を活用して、社内無線LAN (Local Area Network) 経由による業務システムの利用、ビデオ会議用端末としての活用等、利用者のワークスタイルにあったワンストップサービスのメニュー拡充を図っていく。

参考文献

(1) 涌井道子, ほか: 端末管理に対する多様なニーズに対応した端末管理制御基盤システムの開発, NTT DOCOMOテクニカル・ジャーナル, 17, No.3, 50~54 (2009)