3 オリンピックのセキュリティ

応用 一般

宝木和夫（産業技術総合研究所）

攻撃ターゲット

過去，オリンピックではどのようにセキュリティ対策がなされてきたであろうか．オリンピックは多くの人々が集まるイベントの場であり，そこには，射撃のような武器を扱う競技があったり，マラソンのように選手と一般人が接近する機会があったりする．さらに，オリンピックは主催国の威信がかかるイベントである．それゆえ，オリンピックを台無しにしたい敵対者の恰好のターゲットになり得る，という問題に対処しなければならなかった．

オリンピックのセキュリティ対策について，種々の報告はあるが，2020 年東京オリンピックに向けての分析はまだ少ない．本稿は，情報技術の適用という観点から，過去のオリンピックのセキュリティ対策を概観し，東京オリンピックに向けての課題を探る．

過去の概観

ロンドンオリンピック

セキュリティ対策

従来，オリンピックにかけられた警備コストは図 -1 に示すようにアテネから大きな伸びを示している．

このうち，ロンドンは比較的情報が多いので，詳しく分析することができる．図 -2 に示すように，ロンドンオリンピックメイン会場におけるセキュリティ対策は，現代の都市テロ対策の縮図である．

ロンドンでは，ヘリコプターを搭載する揚陸艦「オーシャン」がテムズ川をさかのぼって会場近くで待機したり，地対空ミサイルを民間アパートの屋上に

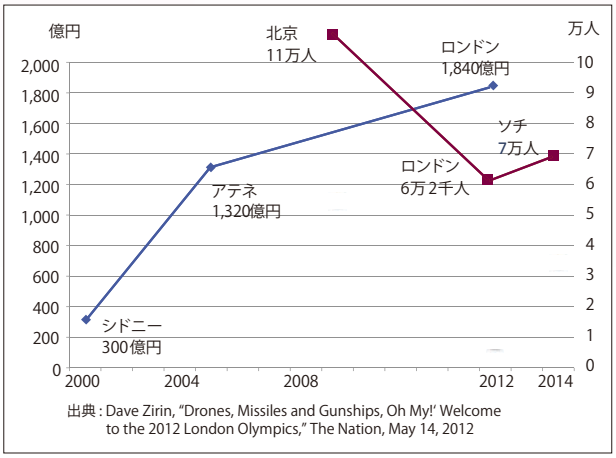

図 -1　過去，オリンピックにかけられた警備コスト，人数

略号　IDOL：Intelligent Data Operation Layer,「暴動」や「犯罪」の発生と，SNSで発信されるテキストや画像といったデータとの関係性を分析する機能
CCTV：Closed-Circuit Television, 閉回路テレビ．カメラおよび取得した映像の伝送・処理および表示機能を含む監視システム

図 -2　ロンドンオリンピック警備概要

設置したり，高周波電気フェンスで敷地を囲んだりした．ここまでは，軍事作戦の範疇に近い．また，警備保障レベルでは，カメラによる顔認証を始め種々の生体認証，および，無線飛行機ドローンによる偵察（含，画像解析）や，「暴動」や「犯罪」の発生と，SNS で発信されるテキストや画像といったデータとの関係性を分析する IDOL（Intelligent Data Operation Layer）という情報技術が採用された．

バイオメトリクスについては，適用場所や対象者に応じて人体の異なる個所が検査された（表 -1 参照）．

また，採用年度や内容の詳細は表 -2 のようになった．

このうち，建設現場では，作業員の都合で，手が泥で汚れたり顔がマスクで隠されたりしても識別できる個所として掌や虹彩を選んだとされる．

考察

このような対策が功を奏してか，ロンドンオリンピックでは大きな事件が生じなかった．マラソンに関するほかのイベントである2004年アテネオリンピックのマラソンでは，アイルランド人元司祭のNeil Horanにより競技中選手への妨害行為が生じた．2012年ロンドンの後の2013年ボストンマラソンでは爆破事件が起きている．このように先進国で不祥事が前後する間，ロンドンオリンピックでは，大きな事件は起きなかった．これは英国当局によるセキュリティ保全のノウハウと努力の賜物であると評価できる．

また，無線飛行機による偵察やIDOLの採用は，オリンピックのセキュリティ対策として，今後，重要なトレンドになっていくと思われる．

ただし，チケットを完売したはずの会場で，なぜか観客席は空席が目立った[1]．これは，どういう原因によるものかは定かではない．しかし，ロンドンを他山の石とした上で，東京オリンピックではいかに安全に「大入御礼」を実現しながら「おもてなし」を演出するかという課題が見えてくる．

対象	場所	認証方式	使用方法
選手，コーチ，関係者	入国，ほか	指紋	英国大使館で記録された電子パスポートと合わせて使用
	オリンピック選手村	顔，指紋（10本指）	スキャナで入力
建設作業者	建設現場	掌，虹彩	建設技能認証制度のカードと連携

表-1　ロンドンオリンピックにおける生体認証の分類

分野	No	内　容	2011	2012	2013	2014
パスポート	1	ジンバブエの英国大使館で記録された指紋，電子パスポートにより，選手，コーチ，関係者がオリンピック，パラリンピックへのスムーズなエントリが可能に		指紋		
オリンピック施設	2	オリンピック選手村に入るため，すべてのオリンピック選手とその家族は，バイオメトリクススキャンが求められる		指紋，顔		
	3	HRS(Human Recognition Systems)社によりオリンピック公園と選手村の建設関係者81,000人を認証処理		掌，虹彩		
	4	業務を遂行するために必要なスキルレベルを持っている本人であることを確実にする	掌，虹彩			
	5	アクセスコントロールによるオリンピック公園サイト境界で不正侵入防止．（建設現場作業者を含む）		掌		
	6	攻撃に備えるとして，テムズ川に輸送機を待機させたり，スキャナや生体認証つきIDカード，ナンバープレート，顔認証CCTVシステム，病院加療追跡システム，新たな警察コントロールとチェックポイントを取り入れている		指紋，顔		

表-2　ロンドンオリンピックにおける具体的内容

ソチオリンピック

セキュリティ対策

ソチでは，国際空港の職員のアクセスコントロール用に3次元顔認証が採用された．また，監視カメラが多く設置され，特定個人の探索に用いられた（表-3参照）．

犯罪経歴等があり，真のブラックリストに載るような人物には，オリンピックパスは元々発行されない．しかし，そうでない要注意人物はブラックとは若干異なるグレイリストに載せ，監視カメラ等で追跡，監視したと考えられる．

考察

ソチにおいて，ブラックリストに関する技術がどのようなものであったかは，情報が少ない．しかし，米国海軍による「アイデンティティ支配」（Identity Dominance）というプログラムから類推できる．「アイデンティティ支配」とは，米国当局者が，敵の戦士や国家安全性へ脅威をもたらす者に対して，過去に用いたIDや過去の活動，特に，テロやほかの犯罪に関連した活動にリンク付けできるようにすることをいう[2]．ここで，このリンク付けのなかにたまたま一般市民が含まれることがある．たとえば，監視中のブラックリストの人物が一般市民に接触すると，その一般市民もグレイリストに入

れられる．この場合，グレイリストに入れられた人は，ブラックリストの人物と同様に，過去および現在，将来の行動がリンク付けされ監視され得る．

米国海軍の場合に限らず，一般に犯罪防止目的で地域安全を目指す場合，このようなブラックリスト，グレイリストを実現するため，組織間で情報を交換し合うことがある．

このような手法は，大変強力な保護機構を構築できる反面，一般市民のプライバシ侵害の問題も生じ得る．もし，東京オリンピックでこのような手法をとり入れる場合，技術開発とともにプライバシ権に関する法律や行政の整備が求められるであろう．つまり，社会の安全を守るための「知る権利」と，プライバシ権としての「忘れられる権利」，さらに「表現の自由」を扱うルールはきちんと整備されておくべきであろう（図 -3 参照）[3),4)]．

分野	No	内　容	2011	2012	2013	2014
空港	1	Elektronika LLC 社は，2014 年冬季オリンピックに向けて，Artec Group の広域 3D 顔認識システムを使用した 3 次元顔認識システムをソチ国際空港の職員のアクセスコントロールに使用する			顔	
オリンピック施設	2	入場時には，チケット以外に，IC タグのようなオリンピックパスが必要となり，そのパスを入手するには，経歴チェックに合格する必要がある．また，顔認識ができる監視カメラも設置されており，職員が特定の個人を探すことができる				顔

表 -3　ソチオリンピックにおける適用事例

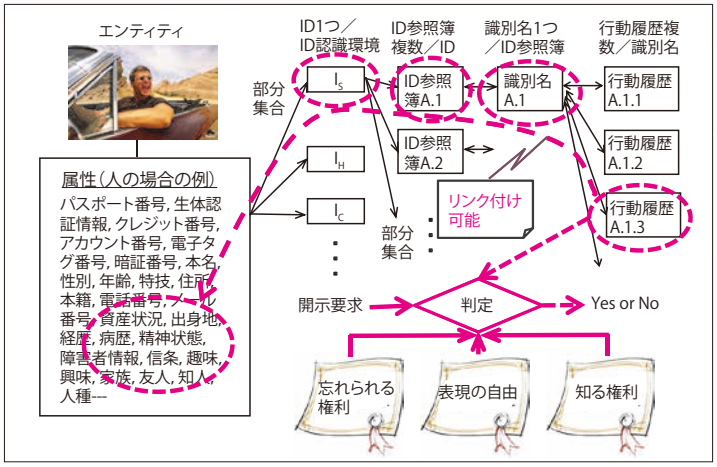

図 -3　ID 利用に伴う個人情報流出のメカニズム

リオデジャネイロオリンピック

セキュリティ対策

リオデジャネイロ（以下，リオ）でも，カメラによる監視に注力している（表 -4 参照）．

リオでは，オプスセンター（Ops Center）という建屋内の約 80 平米のモニタ，および，100 室の部屋に分散配置された 300 個のスクリーンを用いて，多くの監視員が，カメラで映された町中の細部をチェックしている．固定カメラや飛行機からの撮影以外に，街角で人が撮影した映像が，オプスセンターに送られ，リアルタイムのストリートビューを実現している[5)]．

考察

オプスセンターは，オリンピック目的だけに限らず，ほかの目的のためにも運用されている．1 つは祭りを盛大に祝うなど，ブラジル特有のカリオカ文化に即した行事を安全に行うという目的，ほかの 1 つは，近年，ブラジルで多発している土砂崩れや洪水など自然災害への対処の目的である．

具体的には，

- リオカーニバル 500 万人参加
- Rock in Rio 70 万人参加
- ワールドカップ 2014
- 災害発生時，市民防衛活動

等を通じて監視，対策ノウハウ，あるいは，公共の場での監視強化に対する市民の受容性等を醸成中である．この経験の蓄積が 2016 年リオオリンピックの警備ノウハウに活かされるだろう．

リスク予測

概要

情報技術に関するリスクは急激に増大している．2020 年東京オリンピックでは大きなリスクを被り得ると予想される．

一般に，情報の通信，処理能力が 30 倍程度増えると社会も質的に変化する．たとえば，ムーアの法

則が続くとすれば，7，8年ごとに約30倍の量的変化が生じるが，世界で生成されるディジタルデータ量はこのようなスピードで伸びている（図-4参照）．これに応じ，サイバー攻撃に対する社会の反応は，興味の喚起（1986年）→先進ユーザの関心事（1994年頃）→広域被害の発生（2001年頃）→実態経済へ影響（2008年頃）→国事の対応（2013年頃）と質的に変化した．

過去，オリンピックで採用されたセキュリティ対策をもとに，今後の脅威を予想する．

ロンドンオリンピックでとられた対策は，不法行為者の侵入，爆発物，飛行物体の危険を想定した対策であった．リオデジャネイロでは，自然災害への対処も兼ねて精緻なセンサネットや街角モニタリングシステムが構築されている．

2020年東京オリンピックでは，ロンドンで想定された攻撃がより高度化された形で試みられ，かつ，リオで想定された自然災害は，我が国特有の地震，津波のようなより激烈なものに置き換わる恐れがある．これらをフォールトツリーで表現したのが図-5である．

このうち，新型攻撃として想定される「小型飛行機を購入」の事例，「地震発生寺の混乱を利用」の事例，および，従来型「サイバー攻撃」について，以降でやや詳しく検討する．

飛行物体による攻撃

2012年ロンドンでは，無線飛行機ドローンによる監視が行われた．無線飛行機は，現在，急速に小型化，高性能化している分野の技術であり，すでに市販のマルチコプターとして数十万円程度で購入可能なものもある．米国では，ネット販売業者による「30分以内のお届け便」に用いられることが計画されている．2020年東京では，マルチコプターがさらに進化した形で攻撃側に用いられることが想定される．当然，会場周辺では，マルチコプター等の使用に対して規制が入ることが予想される．しかし，

- マルチコプター製造に必要な部品はコモディティ化していて入手が容易になること
- 高性能化・カスタマイズに必要な不足品は3Dプリンタで容易に作成可能になること
- 2020年に利用可能なスマホ機能を用いて，複数マルチコプターの同時管制が可能になること

等を考慮すると，適切な対策を講じない限り，進化したマルチコプターによる同時多発攻撃のリスクは大きいと考えられる．

災害を利用した攻撃

リオに限らず，自然災害を想定し，センサネット

分野	No	内　容	2011	2012	2013	2014
オリンピック施設	1	KABA グループは，リオデジャネイロにおける2016年オリンピックでは，選手村の宿泊施設に約1,000バイオメトリックアクセス制御コンポーネントのための相手先ブランド供給（OEM）の契約を獲得．また，独自のフィンガープリント技術を持つ中国 Probuck テクノロジーズ社の買収を完了（指紋認証と推測）			指紋	
	2	スロバキアの ColosseoEAS はリオのオリンピックスタジアム・ジョアンアヴランジュでの2016年 夏季オリンピックの陸上競技場のイベントにリアルタイム生体顔認識高セキュリティ回転式改札口をテスト（ブラックリスト顔認識）		顔		
周辺	3	リオデジャネイロは，ちょうどワールドカップやオリンピックに間に合うように，世界最大の都市モニタリングシステムを設置（入退室に指紋認証）	指紋			顔？

表-4　リオオリンピックにおける適用事例

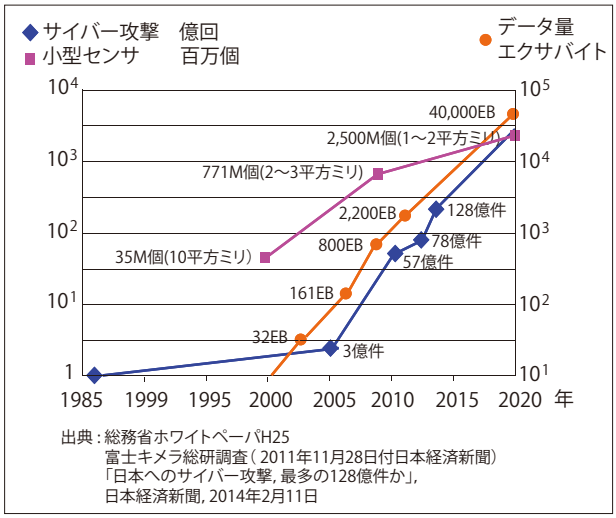

図-4　世界ディジタルデータ量，小型センサ数と日本におけるサイバー攻撃発生件数の伸び

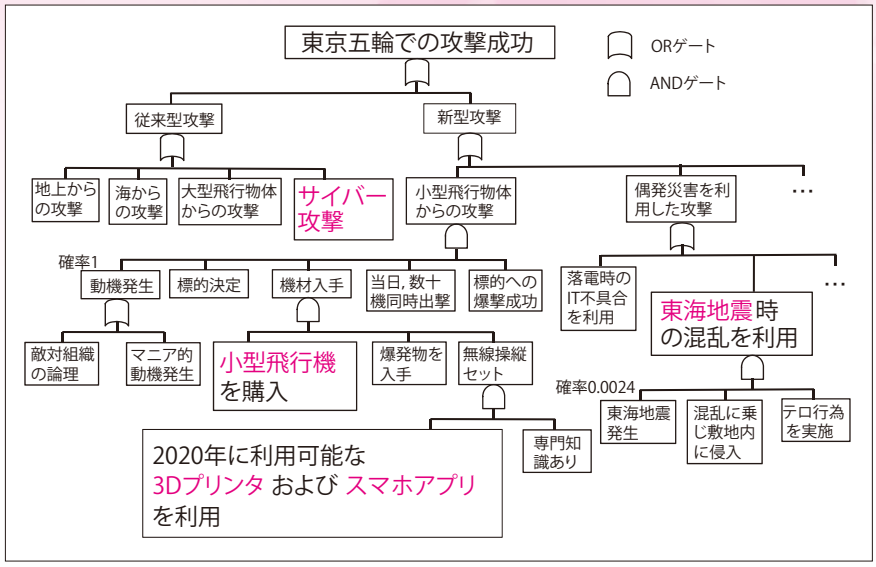

図-5　東京オリンピックフォールトツリー

をはり巡らせて，災害の初期事象をいち早く検出し，警告，避難，救援，復旧など行うことは重要である．このようなプラニングは，東日本大震災を経験した我が国でも実施中であることは周知のとおりである．

では，東京オリンピック会期中に不幸にも自然災害が発生した場合はどうか．地震，津波，竜巻，パンデミックなどが会期中に発生し，攻撃者がそれ幸いと悪用する恐れがあることについて．

地震については，政府の地震調査委員会の予測によると今後30年間で東海地震が起きる確率は，0.88とされている．単純に割り算をすると東京オリンピック・パラリンピック期間中に生じる確率は0.0024となる．想定される事故シーケンスは，

- 東海地震発生
- 混乱に乗じて攻撃者が武装して敷地内に侵入
- テロ行為を実施

事件が生じた場合の被害の大きさを考慮すると，発生確率0.0024は決して小さな数値ではない．

このような事故を推測し，対策コストを決定するため，コストーリスクーベネフィット分析を行うことが必要になろう．

サイバー攻撃

図-4に示すように，日本におけるサイバー発生件数は，2005年3億件，2010年57億件，2013年に140億件に達した．この調子で増え続けると，2020年には，3,000億回に達する．2020年にサイバー攻撃を受ける対象は，世界でネットにつながるコンピュータ（IoT）300億個であるが，そのうち，1～2平方ミリの小さなコンピュータ25億個も攻撃対象になる．東京オリンピックのセキュリティを守るはずのコンピュータ（Safety by IT）が，逆に攻撃対象になるリスクは増大するので，その保護策も必要となる（Safety of IT）．

サイバー攻撃が発生した場合，初期事象（新種マルウェア発生）→兆候検知（早期警戒検知）→早期措置（ファイアウォール阻止）→事故対応（ワクチンの早期開発）→拡大阻止（ワクチン速達）→早期回復（バックアップ復帰）の多重防護により保護することになる．しかし，それぞれの防護が突破される確率が存在する．図-6に示すイベントツリー，フォールトツリー解析によりそれぞれの防護策の強度を評価しながら，リスクを算定する．その上で，コストーリスクーベネフィット評価により，必要な対策投資を決定する．

対策スキーム

バイオメトリクス

バイオメトリクスは，人の体の一部を検査することにより本人であることを認証する技術であり，ハンコやパスワードに比べ，なくさない，忘れないという特徴がある（図-7参照）．

オリンピックにおいて，不正者の侵入を阻止し，かつ，正当者へは心地良いおもてなしを実現する上で，バイオメトリクスは重要な役割を演じる．

古今東西，人の認証はシンプル，迅速で，かつ，正確に行うことが重要で，そうでない方法は嫌われ

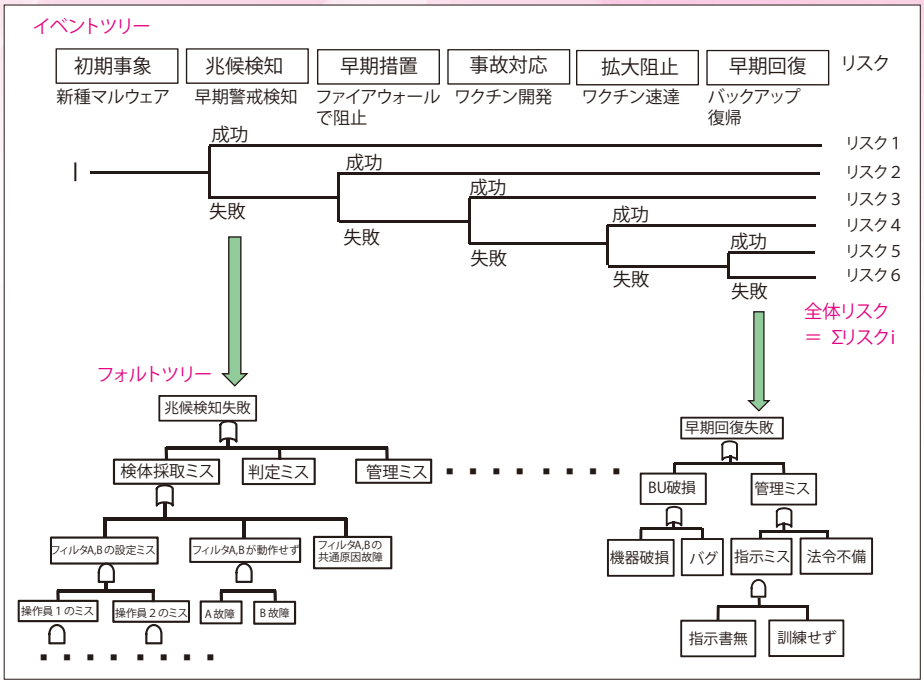

図 -6　多重防護系のイベントツリー例

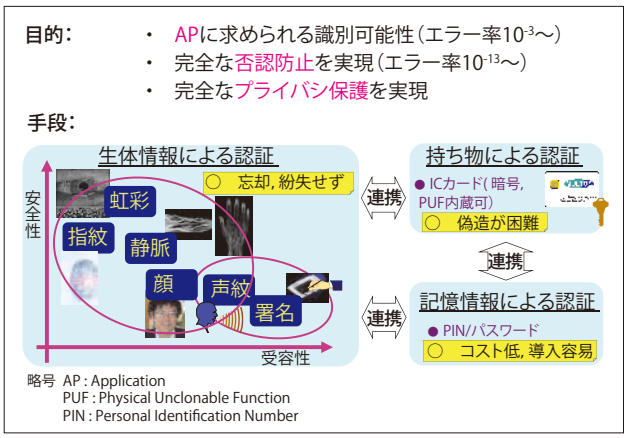

図 -7　個人認証の目的と手段

た．2020 年東京オリンピックでも，シンプル，迅速で，かつ，正確な認証を目指すべきである．

日本でのバイオメトリクスの適用には特有の傾向がある．他国に比べ静脈認証を使う例が多く，かつ，体の 2 つ以上の特徴を検査する多要素認証が増加する傾向にある（表 -5 参照）．

我が国のこの特徴はバイオメトリクスのシンプル，迅速，正確さを実現する上で，果たして有用であろうか．もし，有用であれば正当に評価され活用されるべきである．そこで，他方式と比較評価をするための尺度が必要になる．特に，精度，脆弱性とプライバシ保護の観点での比較評価が重要になる．このため，有用と考えられる ISO/IEC での評価基準を紹介する．

図 -8 は，ISO/IEC 19792「バイオメトリクスのセキュリティ評価」の概要を示す．

この ISO/IEC 19792 は，バイオメトリクス製品を精度評価，脆弱性評価，プライバシ評価の 3 点から評価することを要求しており，そのための細目を規定している．

このような国際標準を用いた評価・認証を行う方法について調査が進められている [6]．

トレーサビリティ

上記，オリンピックにおけるセキュリティの問題を解決する上で，トレーサビリティは重要な役割を演じる．

まず，サイバー攻撃については，サイバー攻撃が検知された場合，攻撃の発信元をたどるトレースバック，さらには，攻撃者が誰かを推定するプロファイリングなどが行われる．これらは，怪しいエンティティを探索するいわゆるブラックリスト探索である．ここで，エンティティとは，該当の情報および通信の処理にかかわるハードウェア，ソフトウェア，データ，あるいは，人のことである．一方，怪しくないエンティティを探索するホワイトリスト探索も行われる．このようにネット上でブラックリストとホワイトリストの探索を行うことで，攻撃源の速やかな絞り込みと被害の拡大阻止を効果的に行うことが可能になる．

怪しくないソフトウェアを見つける方法としては，開発におけるトレーサビリティの研究開発が進んでいる．しかし，製品がサプライチェインに流れた後のセキュリティ保証と，製品開発におけるトレーサビリティの検証が現在のところ，別々に議論さ

分野	No	内　容	2011	2012	2013	2014
情報通信	1	F 社の横浜データセンタが掌静脈で格付ランクトリプル A を取得	掌静脈			
	2	N 社九州データセンタが顔認証サービスを開始			顔	
	3	HU 社は，勤怠管理クラウドサービスに，指紋と指静脈の N 社製ハイブリッドスキャナを採用		指紋，指静脈		
	4	D 社は，勤怠管理タイムレコーダに指紋認証を採用		指紋		
水道	5	S 市水道局，複数業務システムへのセキュアなログインに指静脈を採用		指静脈		
金融	6	O 銀行，通帳やキャッシュカードが不要な ATM サービスに掌静脈を採用		掌静脈		
医療	7	TA 病院は，医療機関で全国初となる，顔認証での再来受付システムを開始				顔
	8	NI 社は，献血の受付システムに指静脈認証を採用				指静脈
健康	9	TE 大学が，PHR（Personal Health Record）プラットフォームを実証実験中で，H 社の指静脈認証ソリューション，F 社の掌静脈，O 社の顔認証を使用	指静脈，掌静脈，顔			
空港	10	N 社は，成田国際空港「ノンストップゲート」顔認証実験のためのセキュリティシステムを提供			顔	
鉄道	11	J 研究機構が，大阪駅で顔認識をテストすることを計画				顔
	12	N 電鉄が I 銀行と一体で運用．掌静脈，指静脈の双方に対応			指静脈，掌静脈	
行政	13	H 社，「指静脈認証システム」を K 官庁共済組合へ納入	指静脈			
	14	O 高校教職員向けネットワーク導入にあたり，シンクライアントシステム（指紋認証型）が，F 社により推奨機器に認定された			指紋パスワード	
その他教育	15	N 中 / 高校で，生徒 1,200 人全員の正確な認証によりPC教室での円滑な授業を実現. N社製指静脈，指紋認証装置を使用			指静脈，指紋	

表 -5　日本における適用事例

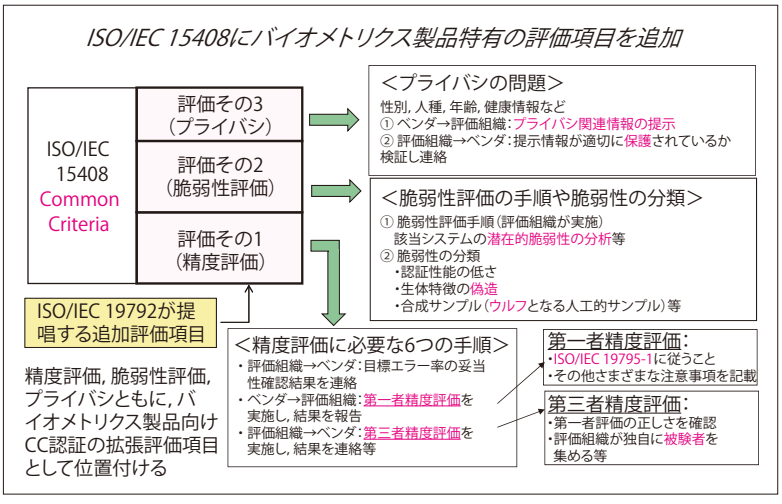

図 -8　ISO/IEC 19792 の概要

れており，より総合的な枠組みの構築が求められる[7]．

ハードウェアのホワイトリストについては，ISO TC 247「模倣品対策」で，枠組みを検討中である．ここでは，真正品にコードを発給し，真贋を判定する第三者真贋判定機関（ASB：Authentication Service Body），企業内でコード発給・真贋判定を行う機関（SASB：Self Authentication Service Body），および，政府の認めた認証機関（CSB：Certification Service Body）が主なプレーヤとなる．

将来のサイバー攻撃においては，多くの M2M（Machine to Machine）ノードが攻撃され暗号や認証の要となる秘密鍵が盗取される恐れがある．その場合でもなお M2M ノード間通信をセキュアに行うための技術として，PUF（Physical Unclonable Function）が有望である．PUF は，IC チップの一部分に形成される回路で実現され，複製困難な製造ばらつきにより発生する入力－出力関係を利用する．PUF 回路が生成し得る入力値－出力値組の数は膨大であり，たとえば，2^{128} 組が存在し，攻撃者がたとえ PUF 回路を一時的に手元に入手しても，2^{128} 組の入力値－出力値組をすべて事前に記録しておくことは実際上不可能である．正規のユーザが PUF 回路を使用する場合は，事前にこのうちの一部だけ（たとえば，2^{10} 組）をランダムに選んで生成し，認証用のコードブックとしてサーバに登録し，IC チップの真贋判定に使う．PUF は LSI の指紋とも考えられバイオメトリクスと同様の認証方式を適用することが可能である．PUF は一部実用化され，高速，小型化等の研究も進んでいる[8]．半導体製品を含むさまざまな商品の真贋判定は TC 247

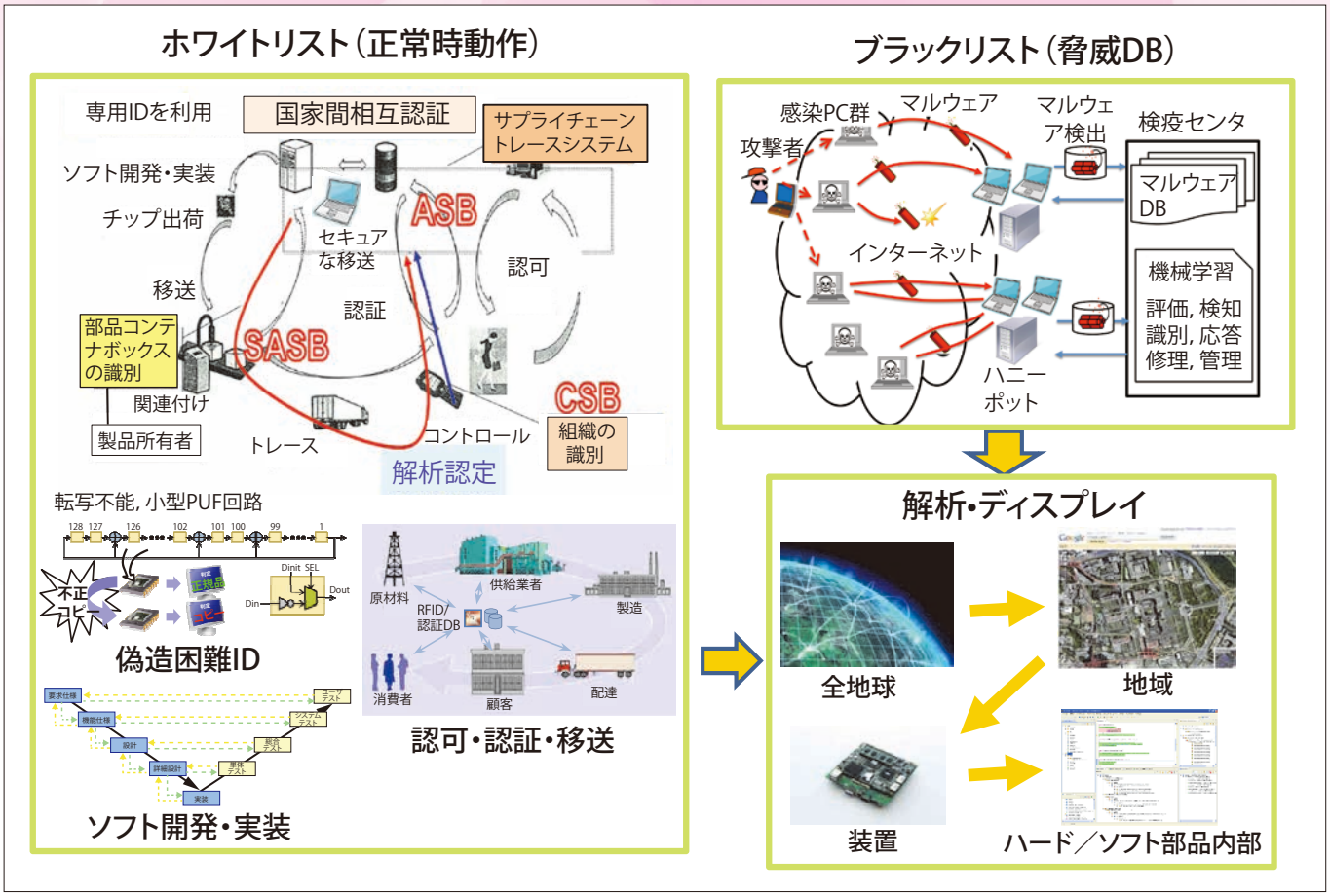

図 -9　トレーサビリティ（構想）

「模倣品対策」のなかで議論されているが，PUF はそのキーテクノロジーとなる可能性がある．

これらの開発により，グローバルに広く集めたハードウェア，ソフトウェア製品に関するブラックリスト，ホワイトリスト情報を突き合わせ，結果を分かりやすくディスプレイに表示することで，効果的な対応が可能になると考える（図 -9 参照）．

成功に向けて

情報技術がもたらす変化の激しい混沌とした状況が続いているなかで，セキュリティの観点から過去の事例，および，今後の課題について述べた．2020 年オリンピックを成功に導くため，一助となれば幸いである．

参考文献

1) The Guardian : Empty Seats at the Olympics - in Pictures, theguardian.com, Sunday 29 July 2012 11.47 BST (2012).
2) Woodward, J. D. Jr. : Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism, MILITARY REVIEW, RAND Corporation, pp.30-34 (Sep.-Oct. 2005).
3) 宝木和夫：情報セキュリティの新しい課題について，日本セキュリティ・マネージメント学会誌，28(1), pp.36-43 (2014-05)
4) 宝木和夫：情報セキュリティ―暗号・認証・マネジメント―，近代科学社 (2012).
5) Ruvolo, J. : Rio's Unprecedented New Surveillance System, The Daily Beast, 2011.10.15 (2011).
6) 大木哲史，大塚　玲，宝木和夫：生体認証装置に対するなりすまし行為の現状と課題，電子情報通信学会バイオメトリクス研究会 (2013).
7) 田口研治：ハイブリッド認証に向けての工学的アプローチ，第 11 回クリティカルソフトウェアワークショップ（11th WOCS）(2014).
8) Hori, Y., et al. : Pseudo-LFSR PUF : A Compact, Efficient and Reliable Physical Unclonable Function, in Proc. ReConFig 2011, pp.223-228 (2011).

(2014 年 7 月 1 日受付)

宝木和夫（正会員）　kazuo.takaragi@aist.go.jp

1977 年東工大修士制御工学専攻修了．同年日立製作所入社．その後，同社システム開発研究所主管研究長，独フライブルグ大学客員教授等を経て，2012 年より産業技術総合研究所セキュアシステム研究部門副部門長．