IPA Better Life with IT

情報セキュリティ白書2014

もはや安全ではない：高めようリスク感度

概要説明資料

2014年7月31日

独立行政法人情報処理推進機構
技術本部　セキュリティセンター
情報セキュリティ分析ラボラトリー

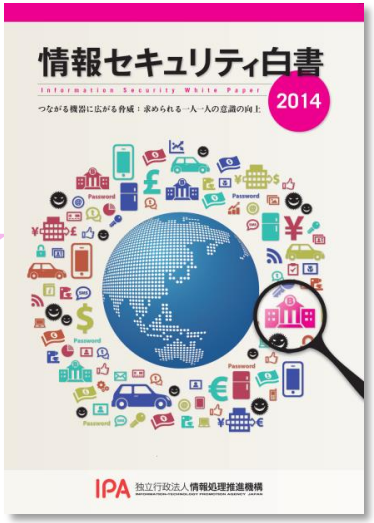
全体構成

- **第Ⅰ部　情報セキュリティの概要と分析**
  - 序章　2013年度の情報セキュリティの概況～10の主な出来事～
  - 第1章　情報セキュリティインシデント・脆弱性の現状と対策
  - 第2章　情報セキュリティを支える基盤の動向
  - 第3章　個別テーマ

- **第Ⅱ部　2014年版10大脅威** ～複雑化する情報セキュリティ　あなたが直面しているのは？～

- **付録　資料・ツール**
- **第9回 IPA情報セキュリティ標語・ポスター・4コマ漫画コンクール 入選作品**

ボリュームは2013年版と同じ（228頁）
新たな取り組みとして“コラム”を追加
本年より**電子書籍版**を発売



2013年度に観測されたインシデント状況

情報漏えいインシデント
データ漏えい／侵害事例
外部からの攻撃によるもの
が圧倒的
2013年の件数は過去最悪

マルウェア遭遇
標的型攻撃が前年比91%増
APT攻撃が多かった国
日本は4位

スパムメール発信源
スパム配信国ワースト12
日本は初めて7位にランクイン
送信にはウイルスに感染した
パソコンが悪用されている

序章　2013年度の情報セキュリティの概況～10の主な出来事～

2013年4月から2014年3月を対象に、本書の全体を表すトピックスを10個選定

① インターネットバンキングを狙った攻撃が多発、被害額は過去最悪（1.2.1）（1.3.4）
② Web改ざん被害が過去最悪、フィッシング詐欺も横行（1.2.1）（1.3.5）（1.3.6）
③ パスワードリスト攻撃による不正利用が頻発（1.2.2）（1.3.3）
④ 政府機関をターゲットとした水飲み場型攻撃（1.2.3）（1.3.2）
⑤ 内部者による情報漏えい（1.2.5）
⑥ 「サイバーセキュリティ戦略」の決定（2.1.1）
⑦ サイバーセキュリティの国際連携への取り組み（2.1.1）（2.3.1）（2.3.4）（2.3.5）
⑧ 制御システムの情報セキュリティへの取り組み（2.1.2）（3.2）
⑨ 情報セキュリティ人材育成への取り組み（2.4）
⑩ パーソナルデータ保護と利活用への取り組み（2.10.4）

※末尾の項番号は、「情報セキュリティ白書2014」のもの。

① インターネットバンキングを狙った攻撃が多発、被害額は過去最悪

2013年は、国内のインターネットバンキングを狙った**不正送金の年間被害額が過去最大**。
これまで過去最悪だった2011年と比較して被害件数は約**8倍**、被害額は約**4.6倍**。
個人のインターネットバンキング契約口座は約6,600万あり、今後も被害の拡大が懸念される。

不正送金の被害件数と被害額

年	被害件数	被害額（約）
2011年	165件	3億800万円
2012年	64件	4,800万円
2013年	1,315件	14億600万円

■表 1-2-1　不正送金の被害件数と被害額
（出典）警察庁「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を基に IPA が作成

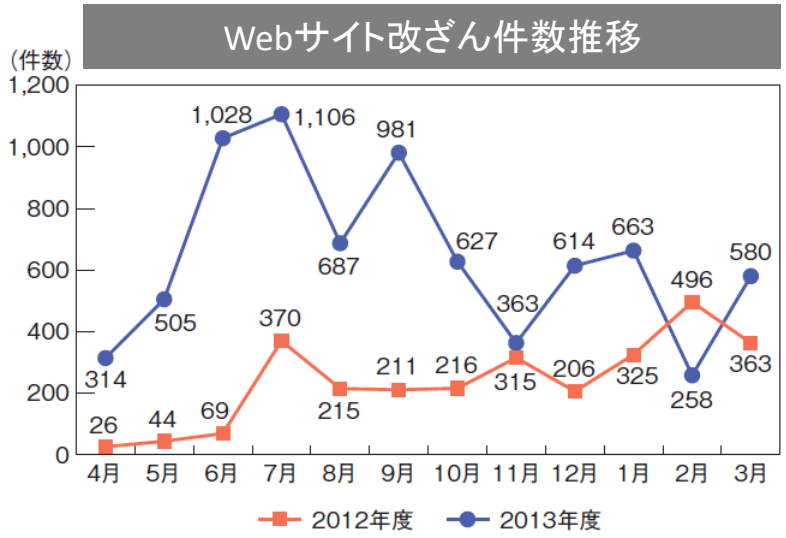
不正送金被害の月別発生件数

■図 1-2-2　不正送金被害の月別発生件数
（出典）警察庁「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を基に IPA が編集

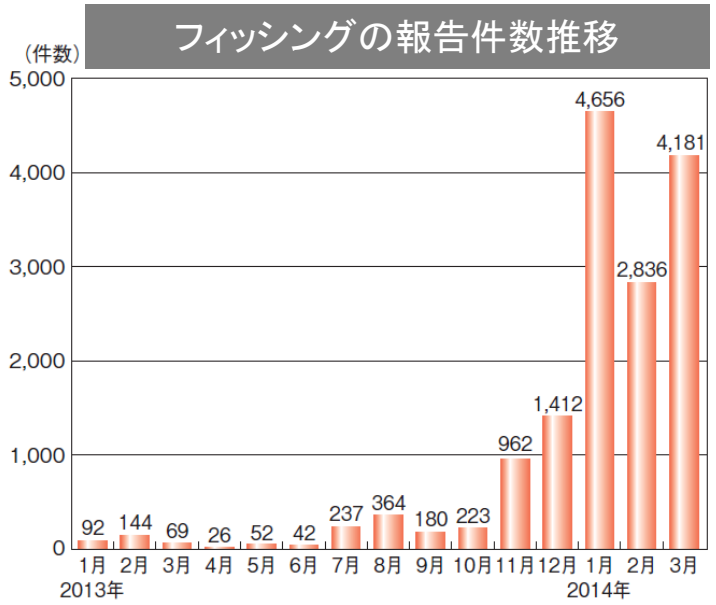
▲不正送金被害の主な原因
・コンピュータウイルス
→ ウイルスに感染したPCが表示する偽の画面にログイン情報を入力することで、ログイン情報が盗み取られる、等

② Web改ざん被害が過去最悪、フィッシング詐欺も横行

2013年度のWebサイト改ざん件数は**7,726件**。2012年度の2,856件から**2.7倍**となり過去最悪。
銀行やゲーム会社を装い利用者をだますフィッシング詐欺も横行し、2012年度は数十件で推移していたが、2014年1月には**4,656件**もの報告が寄せられ過去最悪。



■図 1-1-8　Web サイト改ざん件数推移
(出典)JPCERT/CC「インシデント報告対応レポート」(2012 年 4 月 1 日～ 2014 年 3 月 31 日)を基に IPA が作成



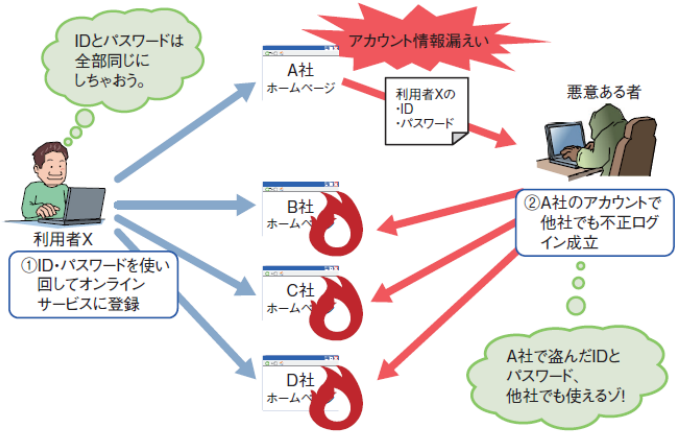
■図 1-1-7　フィッシングの報告件数推移
(出典)フィッシング対策協議会「月次報告書」を基に IPA が編集

▲Web改ざん被害の主な原因
・ウイルスによりID等を窃取される 、 安易なFTPパスワードを破られる、ソフトウェアの脆弱性を悪用され侵入される
▲フィッシング詐欺の主な手口
・銀行やゲーム会社等を装ったメールや広告による偽サイトへの誘導、等

③パスワードリスト攻撃による不正利用が頻発

2013年度は、IDとパスワードを使いまわしている利用者を狙った**パスワードリスト攻撃による被害が多発**。パスワードリスト攻撃は、脆弱なサイトからアカウント情報が盗まれ、同じアカウントを使用している他のサイトに連続自動入力プログラム等を用いて、次々と不正にログインし、**情報の窃取や不正利用等の被害を引き起こす**。

パスワードリスト攻撃のイメージ



■図 1-3-7　パスワードリスト攻撃のイメージ

▲パスワードリスト攻撃被害の主な原因
・IDとパスワードの使い回し

不正ログインのあったサービスとその概要

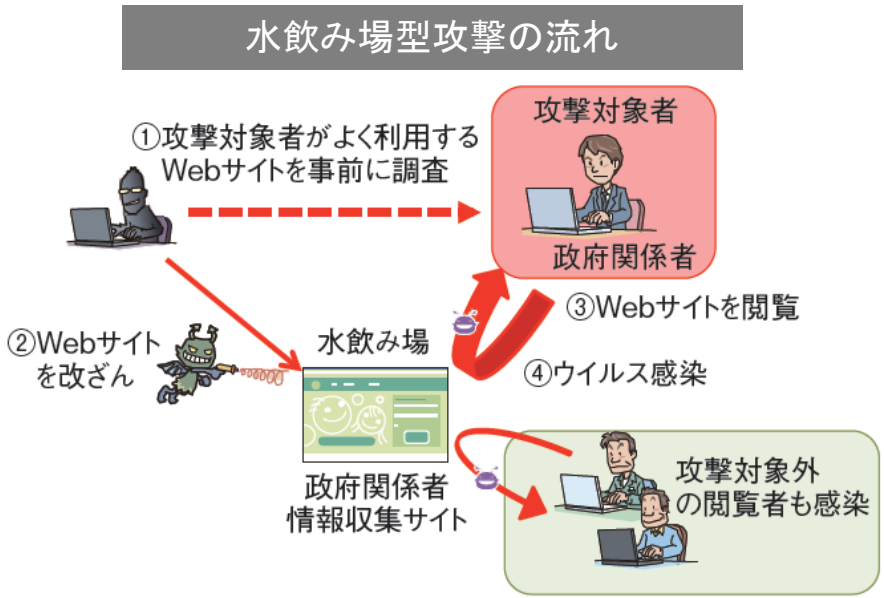
公表日	対象サービス	運営会社	攻撃期間	被害数	ログイン試行回数
2013年4月3日	goolID	エヌ・ティ・ティ レゾナント株式会社	2013年4月1日～4月4日	10万8,716	公表なし
2013年5月8日	ディノスログインページ	株式会社ディノス	2013年5月4日～5月8日	約1万5,000	約111万
2013年5月17日	ワタシプラス	株式会社資生堂	2013年5月6日～5月12日	682	約24万
2013年5月29日	阪急・阪神オンラインショッピング	エイチ・ツー・オー リテイリング株式会社	公表なし～2013年5月14日	2,382	公表なし
2013年6月3日	ハピネット・オンライン	株式会社ハピネット	2013年4月24日～5月31日	最大1万6,808	公表なし
2013年6月19日	ニッセンオンライン	株式会社ニッセン	2013年6月18日	126	1万1,031
2013年7月5日	クラブニンテンドー	任天堂株式会社	2013年6月9日～7月4日	2万3,926	1,545万7,485
2013年7月9日	KONAMI　IDポータルサイト	株式会社コナミデジタルエンタテインメント	2013年6月13日～7月7日	3万5,252	394万5,927
2013年8月7日	じゃらんnet	株式会社リクルートライフスタイル	2		
2013年8月7日	じゃらんnet	株式会社リクルートライフスタイル	2		
2013年8月8日	GREE	グリー株式会社	2		
2013年8月12日	Ameba	株式会社サイバーエージェント	2		
2013年8月29日	WebMoneyファンクラブ	株式会社ウェブマネー	2		
2013年9月27日	バンダイナムコIDポータルサイト	株式会社バンダイナムコゲームス	2		
2013年10月4日	e+	株式会社エンタテインメントプラス	2		
2013年10月7日	Mobage	株式会社ディー・エヌ・エー	2013年10月3日～10月6日	316	公表なし
2013年10月10日	CLUB NTT-West	西日本電信電話株式会社	2013年10月10日	1,206	約3万5,000
2013年10月18日	ECナビ	株式会社VOYAGE GROUP	2013年10月13日～10月16日	2万8,452	不明
2013年10月23日	セブンネットショッピング	株式会社セブンネットショッピング	2013年4月17日～7月26日	最大15万165	公表なし
2013年11月8日	eオリコサービス	株式会社オリエントコーポレーション	2013年11月7日～11月9日	公表なし	公表なし
2014年1月8日	GOM会員サービス	グレテックジャパン株式会社	2013年12月20日～2014年1月8日	公表なし	公表なし
2014年1月24日	@nifty会員向け「お客様情報一覧」ページ	ニフティ株式会社	2014年1月6日	165	公表なし
2014年2月3日	Amazonギフト券への特典交換サービス	日本航空株式会社	2014年1月31日～2月2日	約60	公表なし
2014年2月28日	My SoftBank	ソフトバンクモバイル株式会社	2014年2月24日～2月25日	344	公表なし
2014年2月28日	mixi	株式会社ミクシィ	2014年2月28日	1万6,972	公表なし

約1か月に及ぶ1,500万回の不正なログインの試行もあり

■表 1-2-2　不正ログインのあったサービスとその概要（報道により公表された事例を IPA が調査しまとめたもの）

④ 政府機関をターゲットとした水飲み場型攻撃

政府関連機関を狙った**水飲み場型攻撃によるインシデントが発生**し、拡大する傾向。
2013年8月～9月、中央省庁や地方自治体のニュース等を提供する「47行政ジャーナル」が水飲み場型攻撃に悪用され、特定組織のサイト閲覧者がウイルスに感染した。
攻撃者は、**特定のIPアドレスや組織ドメインからの接続時にのみウイルスを感染**させることで、効率的に攻撃を行っている。同時に**攻撃対象を限定**することにより、攻撃の**発覚を遅らせる**ことができる。更に、感染したウイルスによって端末を外部から遠隔操作する等の高度な手口が使われていることも明らかになった。



▼水飲み場型攻撃への対策
- 利用者の対策
  - ➢ OS やアプリケーションのアップデート
  - ➢ セキュリティ対策ソフトの導入
  - ➢ 管理端末と利用者端末のネットワークを分割
- Web サイト管理者の対策
  - ➢ OS やアプリケーションのアップデート
  - ➢ 管理者アカウントの厳重な管理
  - ➢ 不正なコードの埋め込みの監視

■図 1-3-6　水飲み場型攻撃の流れ

⑤ 内部者による情報漏えい

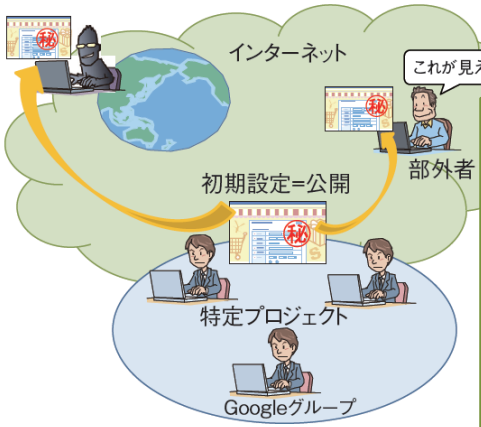
国際的な企業間の提携や委託先企業による運用の現場において、**機密情報が内部者により流出。**
クラウドサービスの利用やネットワークに接続されたオフィス機器が増えたことから、**不適切な設定による情報漏えいが多発。**

内部者による犯行事例※

報道年月	事件の概要	不正行為者	動機
2014年2月	株式会社横浜銀行のATMの保守管理業務を請け負っていた富士通フロンテック株式会社の元社員が、ATM の取引データから顧客のカード情報を不正に取得し、偽造キャッシュカードを作成・所持していた容疑で逮捕された	委託先社員	金銭の取得
2014年3月	株式会社東芝の業務提携先であるサンディスク社の元社員が、東芝の機密情報を不正に持ち出し、転職先の韓国SKハイニックス社に提供したとして、不正競争防止法違反の容疑で逮捕された	退職者	降格人事による不満等

※本誌に掲載されている事例の一部

不適切な設定による情報漏えい



その他、ネットワークに接続しているオフィス機器（複合機）やIMEからの情報漏えい等が報道された。

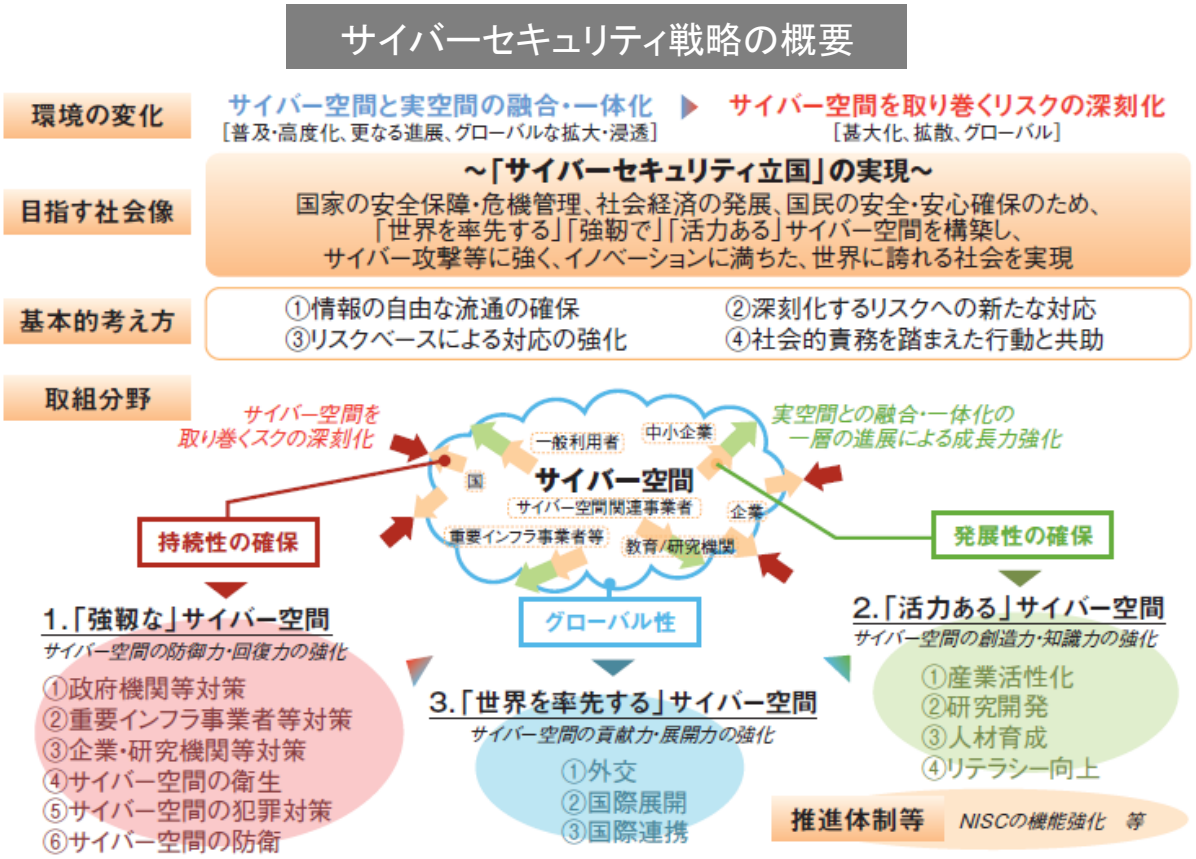
業務に利用していたクラウドサービスが「一般公開設定」だったため、**機密性の高い情報がインターネットを介して無制限に閲覧できる状態になっていた。**
Google グループの情報共有サービスは、当時「一般公開」が初期設定となっており、閲覧を制限するには利用者側で設定を変更する必要があった。

▲内部者による情報漏えいの主な原因
- 処遇への不満等、動機がある
- 機密情報へのアクセス権限の悪用
- 相互に監視する体制が十分でない

▲不適切な設定による情報漏えいの原因
- 初期設定のまま使用している、初期パスワードを変更していない、等

⑥「サイバーセキュリティ戦略」の決定

2013年6月、政府は「安全なサイバー空間」を実現するための新たな中期戦略として**「サイバーセキュリティ戦略」**を策定。サイバー空間を取り巻く急速な環境変化によるリスクの甚大化や、グローバル化に伴う国家安全保障等を含めた国家や重要インフラの防護を目的とする。



■図 2-1-2　サイバーセキュリティ戦略の概要
(出典)NISC「「サイバーセキュリティ 2013」(案)について※2」

国会において、国のサイバーセキュリティ体制を抜本的に強化し、喫緊の課題であるサイバー空間の安全を確保するため、**「サイバーセキュリティ基本法」**の制定が計画されている。2014年7月現在、審議中。

⑦ サイバーセキュリティの国際連携

2013 年10 月、情報セキュリティ政策会議は、**国際連携に関わる取り組みの初めての文書として、「サイバーセキュリティ国際連携取組方針」を公表。**背景にはサイバー空間の安全性は、国内だけの対策で実現できるものではなく、国際的な情報共有や共助の国際連携が重要との認識。本方針では、2013 年6 月に政府が策定した「サイバーセキュリティ戦略」を基に、国際連携の強化に向け、3つの基本方針を掲げ、重点取り組み分野、地域的取り組みを明記。

サイバーセキュリティ戦略における基本原則と基本方針

サイバーセキュリティ戦略における基本原則

①情報の自由な流通の確保
②深刻化するリスクへの新たな対応
③リスクベースによる対応の強化
④社会的責務を踏まえた行動と共助

国際連携の強化に向けた３つの基本方針

①グローバルな共通認識の漸進的な醸成
②グローバルコミュニティへの我が国の貢献
③技術フロンティアのグローバルな拡大

■図 2-1-4　サイバーセキュリティ戦略における基本原則と基本方針
（出典）NISC「サイバーセキュリティ国際連携取組方針」を基に IPA が作成

サイバーセキュリティの国際連携へ具体的な取り組み※

	年月日	内容
アメリカ	2013年5月9、10日（東京）	**第1回「日米サイバー対話」** サイバーに関する共通課題についての情報交換や国際的なサイバー政策の連携、重要インフラ保護及び防衛・安全保障政策での協力等を議論し、本会合を定例化することが決定した。これにより、日米のサイバーに関する幅広い協力を深め、日米同盟を強化した。
東南アジア諸国連合（ASEAN）	2013年9月12、13日（東京）	**「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」** サイバーセキュリティ確保のため、日・ASEAN協力の原則を確認するとともに、安心・安全なビジネス環境の構築、安心・安全な情報通信ネットワークの構築、サイバーセキュリティ能力の強化の3分野で共同の取り組みを促進する共同閣僚声明が発表された。
EU（欧州連合）	2013年12月3、4日（ブリュッセル）	**第2 回「日EU・ICT セキュリティワークショップ」** インターネット上でのセキュリティ確保に関する政策や技術の動向等について日EU 間で情報交換を行う場として、2012年11月の第1回に引き続き開催された。意識啓発、インシデントマネジメント、グッド・プラクティスの共有の3点に関し、日EU間で更に協力を深めていくことが確認された。

※本誌に掲載されている取り組み事例の一部

⑧ 制御システムの情報セキュリティ

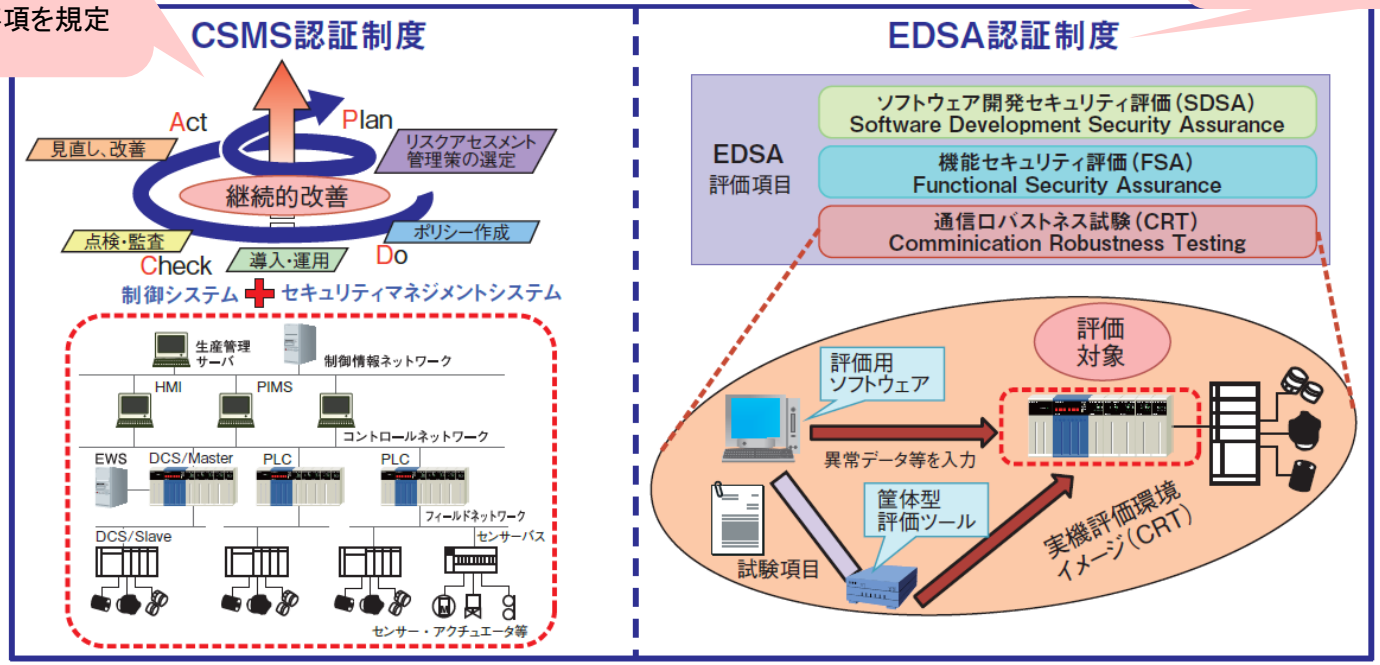
経済産業省及び関係団体等は制御システムのセキュリティの認証スキーム確立に向け、**制御システムのセキュリティマネジメントシステム（CSMS）の認証及び制御機器の製品認証（EDSA）の2種のパイロットプロジェクトを実施**。

CSMS認証制度は、一般財団法人日本情報経済社会推進協会（JIPDEC）、EDSA認証制度は技術研究組合制御システムセキュリティセンター（CSSC）及び公益財団法人日本適合性認定協会（JAB）が主体となっており、どちらも2014 年度から認証業務を開始し、**CSMS のパイロット認証は、CSMS に基づく世界初の認証**。

既に国内で実績のあるISMSの認証スキームを参考とし、事業者向けにセキュリティ要求事項を規定した規格。

米国で先行するISA/ISCIの運営するEDSA認証制度を活用。日本国内に認証機関及び認定機関を設置。

認証スキームの概要

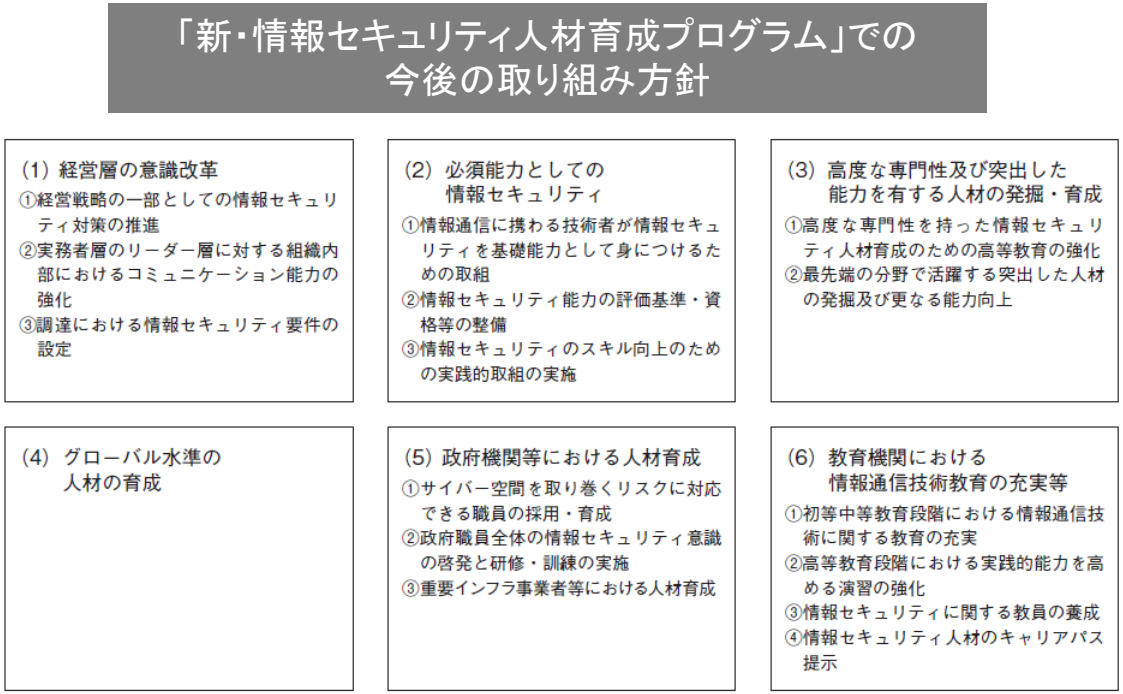


■図 3-2-7　IPA の提案した 2 種の認証スキームの概要

⑨ 情報セキュリティ人材育成

情報セキュリティ政策会議は、2014年5月、政府機関や企業、教育機関等での情報セキュリティ人材の育成を一層促進するため、「サイバーセキュリティ戦略」に基づいた人材育成の中長期的なプログラムとして**「新・情報セキュリティ人材育成プログラム」を公表**。

プログラムは、2014年度から2016年度を対象に、人材の需要と供給の好循環を形成することを基本方針として、需要については経営層の意識改革、また、供給については人材の量的拡大と質的向上を図る。産学官の関係機関が本プログラムに基づき、連携して取り組むこと等を明記。

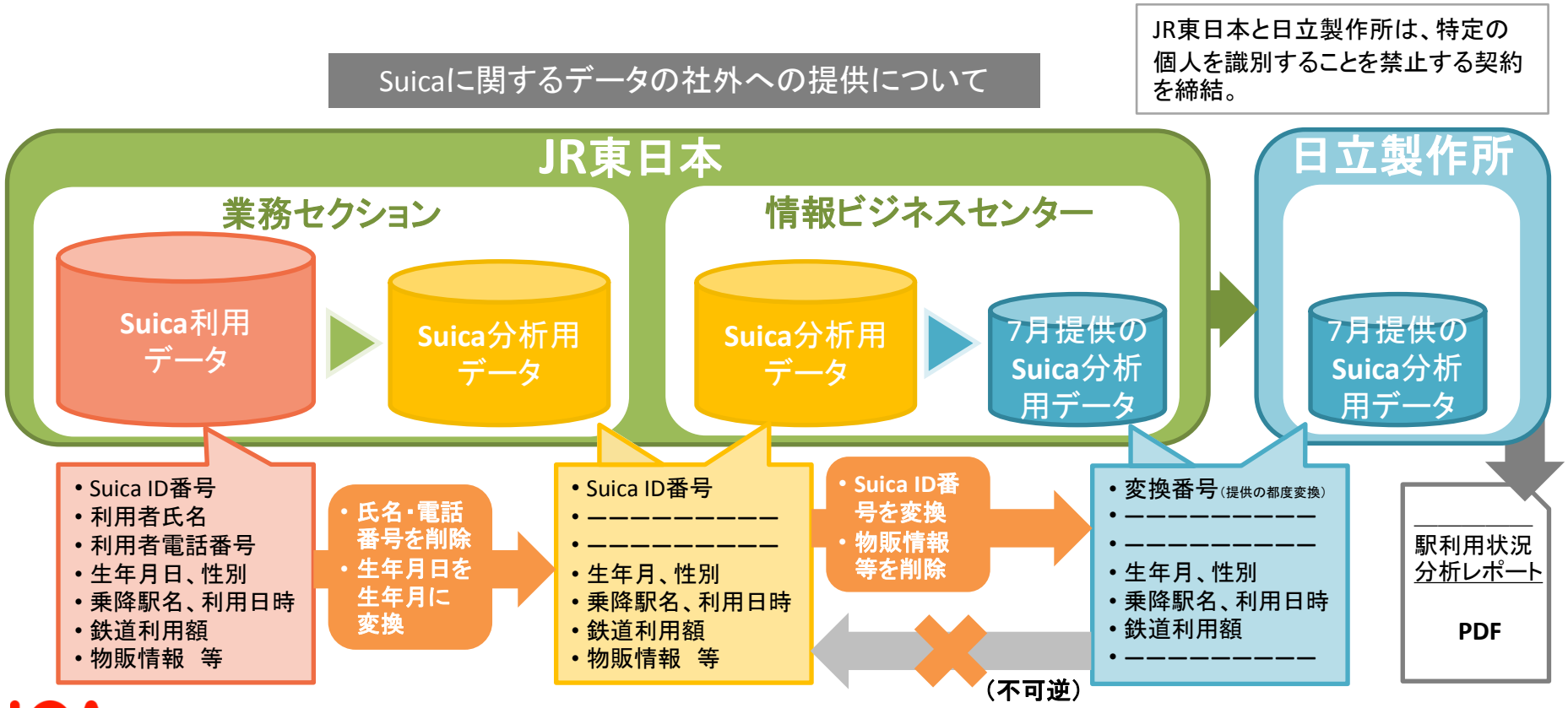


■図 2-4-1 「新・情報セキュリティ人材育成プログラム」での今後の取り組み方針
(出典)NISC「新・情報セキュリティ人材育成プログラム」を基に IPA が作成

⑩ パーソナルデータ保護と利活用

2013年7月、東日本旅客鉄道株式会社は、交通系IC カード「Suica」の乗降履歴等のデータを、マーケティング分析の目的で株式会社日立製作所に提供したことについて、「事前の説明が不足していた」として謝罪した。提供したデータは個人情報保護法に配慮したものであったが、データの活用について多くの利用者が不信感を持った。

パーソナルデータを活用したサービスの多様化に伴い、既存の法制度では明確な判断が困難な場合があることから、政府では複数の有識者委員会にて検討を推進。



（出典）東日本旅客鉄道株式会社：「Suica に関するデータの社外への提供について　中間とりまとめ」を基にIPAが作成
http://www.jreast.co.jp/chukantorimatome/20140320.pdf（白書には記載なし）

第1章 情報セキュリティインシデント・脆弱性の現状と対策

目次構成

第2章 情報セキュリティを支える基盤の動向

目次構成

第2章 情報セキュリティを支える基盤の動向

目次構成

第3章 個別テーマ

目次構成

情報セキュリティ白書2014　もはや安全ではない：高めようリスク感度

情報セキュリティの動向を広くカバーした一冊

■2013年度に情報セキュリティの分野で起きた注目すべき10の出来事を分かりやすく解説

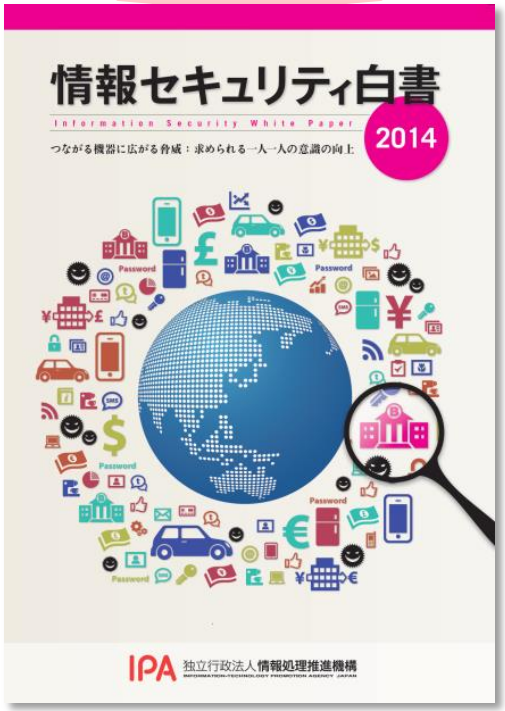
■国内外における情報セキュリティインシデントの状況や事例、攻撃の手口や脆弱性の動向、企業や政府等における情報セキュリティ対策の状況を掲載

■情報セキュリティを支える基盤の動向として、国内外における情報セキュリティ政策や関連法の整備状況、情報セキュリティ人材の現状、組織の情報セキュリティマネジメントの状況、国際標準化活動の動向を掲載

■近年注目されているスマートデバイスや制御システムの情報セキュリティの動向、「政府機関の情報セキュリティ対策のための統一基準群」の改定等の主要なテーマを解説

◆入手先：Amazon(http://www.amazon.co.jp)
全国官報販売組合(http://www.gov-book.or.jp)
IPA　※全国の書店からも購入できます

2014年7月15日発売



発行
独立行政法人情報処理推進機構（IPA）
ISBN978-4-905318-25-5
ソフトカバー / A4判 / 228頁
定価　2,000円（税別）
電子書籍版も販売予定