Cyber Security Clearance

民間セキュリティクリアランスの実現に向けて

政府と民間で機敏情報の共有を行い
競争力のある社会を実現させる

HunsLaB

HunsLab Inc
Confidential
2019

用語

関係用語

用語	概要
GSOMIA	2007/8/10 日米軍事情報包括保護協定。武器等の技術情報・軍の運用情報を迅速に交換するために、米国と同レベ ルの情報管理体制を日本にも要求。
National Industrial Security Program (NISP)	米国国家産業セキュリティ・プログラム。：政府から業務を請け負った請負者にアクセスが認められる機密情報を保護するために、請負者の業 務に関与する個人の人身調査、および、請負者の施設のセキュリティ・クリアランスを 行うためのプログラム。
Defense Security Service(DSS)	米国国防総省の国防保安局。
PCLs	**Personnel Security Clearances**
FCLs	**Facility Security Clearances**
LAA	Limited Access Authorization

出典元：BurningGlass

HunsLab Inc
Confidential
2019

米国政府におけるセキュリティクリアランス

２つのタイプ

- **Personnel Security Clearances (PCLs)**
- **Facility Security Clearances (FCLS)**

必要とする部署

- Department of Defense (DoD), including the DIA, NGA and NSA
- Department of Homeland Security (DHS)
- Department of Justice (DoJ), including the FBI
- Department of State (DoS)

その他要件

帰化した市民は安全保障の認可を受ける資格があります。外国人はそうではありません。セキュリティクリアランスの代わりに、米国外の市民にはLimited Access Authorization（LAA）が付与される場合があります。

HunsLab Inc
Confidential
2019

米国における民間企業の従業員に対するクリアランス

- ✓ 請負者は、実際に機密情報へのアクセスを必要とする職務の募集広告において、内定を得た個人に対しては、政府による人身調査が行われ、かつ、その機密情報を扱う資格要件を満たさなければならないとの条件を当該広告において明示する義務あり
- ✓ 具体的に内定者が決定した段階で、当該内定者による人身調査申込書が、請負者により提出されることが求められている
- ✓ 請負者に関係する労働者等に対する人的クリアランスは、基本的に、政府部内の職員等に対して行われる人的クリアランス制度が適用される
- ✓ 電子書式（SF86）への記入→国防総省統合決定システム（JPAS）→人事管理局（OPM）へ転送・クリアランス調査の実施→調査結果がDSSの国防産業セキュリティ部（DefenseIndustrial Security Clearance Office）に送付され決定手続
- ✓ 労働者は積極的に応募（セキュリティ・クリアランスを要する職務の給与がよいため。通常、5000ドルから1万ドル、年収が上昇）
- ✓ クリアランスをもっているインテリジェンス関係、軍事関係等の退職者に有利。
- ✓ クリアランスが認められなかった民間人に対しては、対審的な不服申立手続と再審プログラムがある（しかし、一般の裁判所への上訴は不可）
- ✓ クリアランスが否定される典型的な決定事例：債務不履行、違法薬物の使用、アルコール依存、犯罪歴、外国からの影響（米国市民でも外国籍の親族が海外にいる等）

HunsLab Inc
Confidential
2019

日米軍事情報包括保護協定(GSOMIA)を締結

日米軍事情報包括保護協定(GSOMIA)を締結・発行(2007/8/10)。 GSOMIA: 武器等の技術情報・軍の運用情報を迅速に交換するために、米国と同レベルの情報管理体制を日本にも要求。

- 国家産業セキュリティ・プログラム（National Industrial Security Program）：政府から業務を請け負った請負者にアクセスが認められる機密情報を保護するために、請負者の業務に関与する個人の人身調査、および、請負者の施設のセキュリティ・クリアランスを行うためのプログラム。
- １９９３年の大統領命令１２８２９号により、連邦政府のシステムを統合（例外：連邦エネルギー省、中央情報局、原子力規制委員会）
- DOD 5220.22-M「国家産業セキュリティ・プログラム運営マニュアル（National Industrial
- Security Program Operating Manual）」等により運用
- 施設と個人の双方に対するセキュリティ・クリアランスが含まれている他、当該請負会社が、外国政府（または企業）により所有、管理、または、影響を受けていないかどうか(Foreign Ownership, Control or Infruence(FOCI))を審査する手続もも含む。
- 国防総省の国防保安局（Defense Security Service(DSS)）が管轄。

出典元：法政大学 永野秀雄氏2007年Report

HunsLab Inc
Confidential
2019

日本におけるセキュリティクリアランス

2017/5 「デジタル・ニッポン2017」を発表。

機密情報にアクセスできる人物を認定するセキュリティ・クリアランス（SC）制度の創設や官民データ連携プラットフォームの防災への活用などが盛り込まれた。政府に提言する。

SCは米国や欧州連合（EU）では民間人でも保有者がおり、民間人が政府の機密情報を製品開発に活用するケースがある。日本にはこの制度がなく、研究開発に利用できるサイバー攻撃情報の量で米国やEUに劣り、安全品質で日本が負ける可能性が高い。

政府の内閣サイバーセキュリティセンター（NISC）がSCガイドラインを策定し、国際監査法人がSCの社団法人を設置。ここが民間人や組織を審査しSC資格を付与する制度を要望する。

HunsLab Inc
Confidential
2019

民間企業に対する人的クリアランス

「情報セキュリティポリシーに関するガイドライン」（２０００年７月１８日）情報セキュリティ対策推進会議決定

人的セキュリティに関して、
①最高情報セキュリティ責任者
②情報セキュリティ担当官（管理職等）
③システム管理者
④職員等

に対するガイドラインが規定されている。さらに、受託事業者とその下請業者等に対しても、本ポリシーを遵守させ、もしも遵守されなかった場合における損害賠償等の規定を契約書に明記するとの施策や、非常勤・臨時職員に対するポリシーの周知徹底と同意書への署名などが規定されている→防衛省でも契約約款規定が策定された。

しかし、受託事業者およびその下請業者の職員等に対する政府による人的クリアランス制度は存在していない。

出典元：法政大学 永野秀雄氏2007年Report

HunsLab Inc
Confidential
2019

人的クリアランスを導入する場合の法的問題

本人の同意の効果：

合憲性を保障→労働者に国家権力作用が直接に及ぶので立法または労働法の改正等が必要。不同意の場合やクリアランスが否定・撤回された場合に、労働法上の不利益取り扱いの問題が生じる。

憲法・労働法上の平等保障に関する問題：

特に外国人、配偶者・親族などが外国人の場合、外国からの影響に関する審査の問題。憲法上の思想・信条に関する保障の問題：国家を暴力により転覆することを企図した団体への加入等の外形行為に関する質問により、内心の自由への侵害を回避することは可能。

憲法上の適正手続保障：

米国では、行政手続（対審的審査および再審手続）で完結し、判例法上、終局的な判断とされ裁判所へ上訴しても判断が回避されている。わが国では、行政裁判所の設置はできないことから、独立の行政委員会により判断し、すくなくとも通常の裁判所に訴えを提起できるようにする必要がある（たとえば、東京高等裁判所に１審としての専属管轄を与える等の方策は可能）。

出典元：法政大学 永野秀雄氏2007年Report

HunsLab Inc
Confidential
2019

現行法の中での運用の可能性

- 対象となる受託企業としては、防衛省等の役所からの圧力が強まるものの、具体的に実施する法的手段がない：自社の労働者への背景調査の限界、下請企業の労働者への背景調査は不可能、人権問題の発生、一部の組合との摩擦。

- 方策１：経済団体等から立法の制定を求める→近々の成立は難しい。

- 方策２：プロジェクトごとに別会社やJVを設置→受託企業からの転籍などの問題は生じる。完全を期すれば、下請企業の労働者等も同じ就労条件で雇用する必要が生じる。

- いかに、憲法・労働法上の問題を回避しながら、労働者の同意の下で、受託企業が直接に内部的なクリアランスを実施しえるのかが問われる。

出典元：法政大学 永野秀雄氏2007年Report

HunsLab Inc
Confidential
2019

防衛省の秘密制度

■■■ 特定秘密 ■■■

● 防衛、外交、特定有害活動の防止、テロリズムの防止に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要なもの。

◆指定の根拠… 特定秘密の保護に関する法律（平成25年法律第108号）
▼罰則…… 10年以下の懲役等（未遂犯、過失犯も処罰）
▼対象……
- 特定秘密を取り扱うことを業務とする者（自衛隊員、適合事業者の従業者等）
- 公益上の必要により行政機関から特定秘密の提供を受け、これを知得した者（国会議員、裁判官等）
- 外国の利益等を図る目的で行われる次に掲げる行為により特定秘密を取得した者
  - ①人を欺き、人に暴行を加え、又は人を脅迫する行為
  - ②財物の搾取　③施設への侵入　④有線電機通信の傍受
  - ⑤不正アクセス行為
  - ⑥ ②～⑤以外の特定秘密の保有者の管理を侵害する行為

■■■ 特別防衛秘密 ■■■

● 米国から供与された装備品等の性能等に関する事項等で、公になっていないもの

◆指定の根拠…
日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号。以下「MDA秘密保護法」という。）
▼罰則……
10年以下の懲役等（探知・収集罪も規定、未遂犯、過失犯も処罰）
▼対象……
特別防衛秘密を取り扱うことを業務とする者など（自衛隊員ほか）

■■■ 省　秘 ■■■

● 国の安全又は利益に関わる事項であって、関係職員以外に知らせてはならないもの

◆指定の根拠… 秘密保全に関する訓令（平成19年防衛省訓令第36号）
▼罰則…… 1年以下の懲役又は50万円以下の罰金（未遂犯、過失犯は処罰なし）
※自衛隊法第59条（守秘義務）違反として、同法第118条の罰則が適用
▼対象…… 自衛隊員

●部内限り又は注意●

●部内限り…… 防衛省の職員以外の者にみだりに知られることが業務の遂行に支障を与えるおそれのあるもの。
●注　　意…… 当該事務に関与しない職員にみだりに知られることが業務の遂行に支障を与えるおそれのあるもの。
◆指定の根拠… 取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて(防防調第4608号。19. 4. 27)
▼対象…… 自衛隊員
※自衛隊法第59条（守秘義務）違反として、同法第118条の罰則の適用を受ける場合もある。

HunsLab Inc
Confidential
2019

基本的な考え方：セキュリティファースト
セキュリティクリアランス制度（SC）創設

SCが無いために日本の民間企業がサイバー攻撃情報を他国と共有できず、研究開発で利用できる情報量に格差が生まれ、安全という品質でSC保有国に負けてしまう可能性が高まる。

IoT時代の“品質”の意味合いの変化

旧来の品質	これからの品質
壊れない・故障しない	ハッキングされても安全

緻密な擦り合わせと勤勉な改善活動

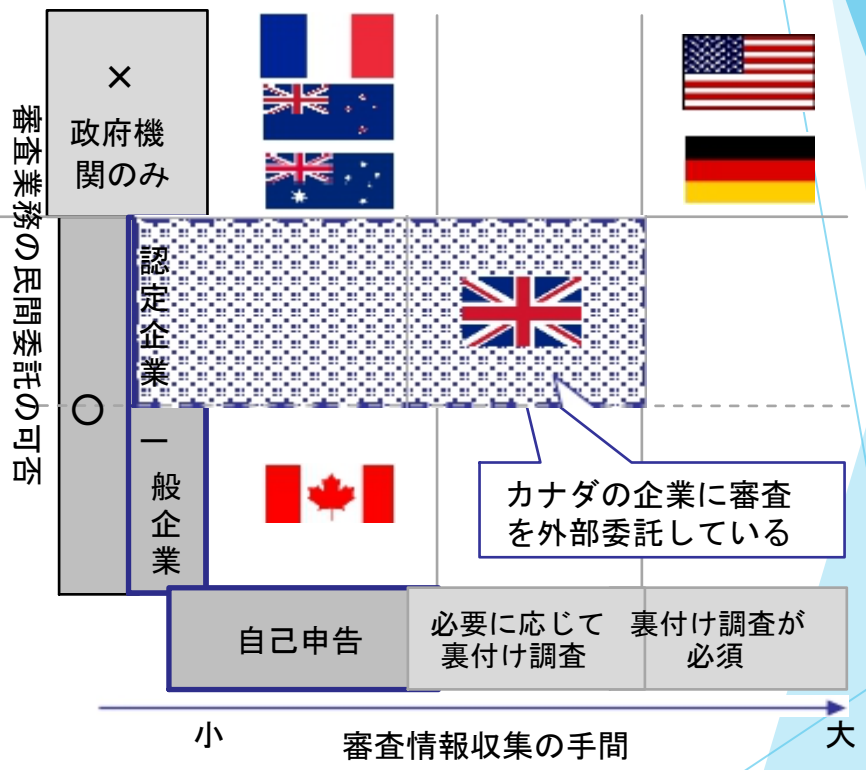
“サイバー攻撃情報の量”とそれに基づく迅速な設計変更やソフトの更新

“サイバー攻撃情報の量”を増やすには、米国やEU各国からサイバー攻撃情報を共有してもらう必要があるがセキュリティクリアランス制度（SC）がなければシェアされない攻撃情報も存在

日本にはCSが無いが、米国とEUでは民間人でもCS保有者がおり、民間企業が政府の機密情報を製品開発に活用することが可能

このままではSCが無いために研究開発に利用できるサイバー攻撃情報の量で米国とEUに大差をつけられ、安全という品質で日本が負けてしまう可能性が高まる

各国のSC制度の違い



国によってCSの実施機関や審査情報の収集の方法に違いがあることから、日本独自のCSを創設して各国と相互認証していくことが有効

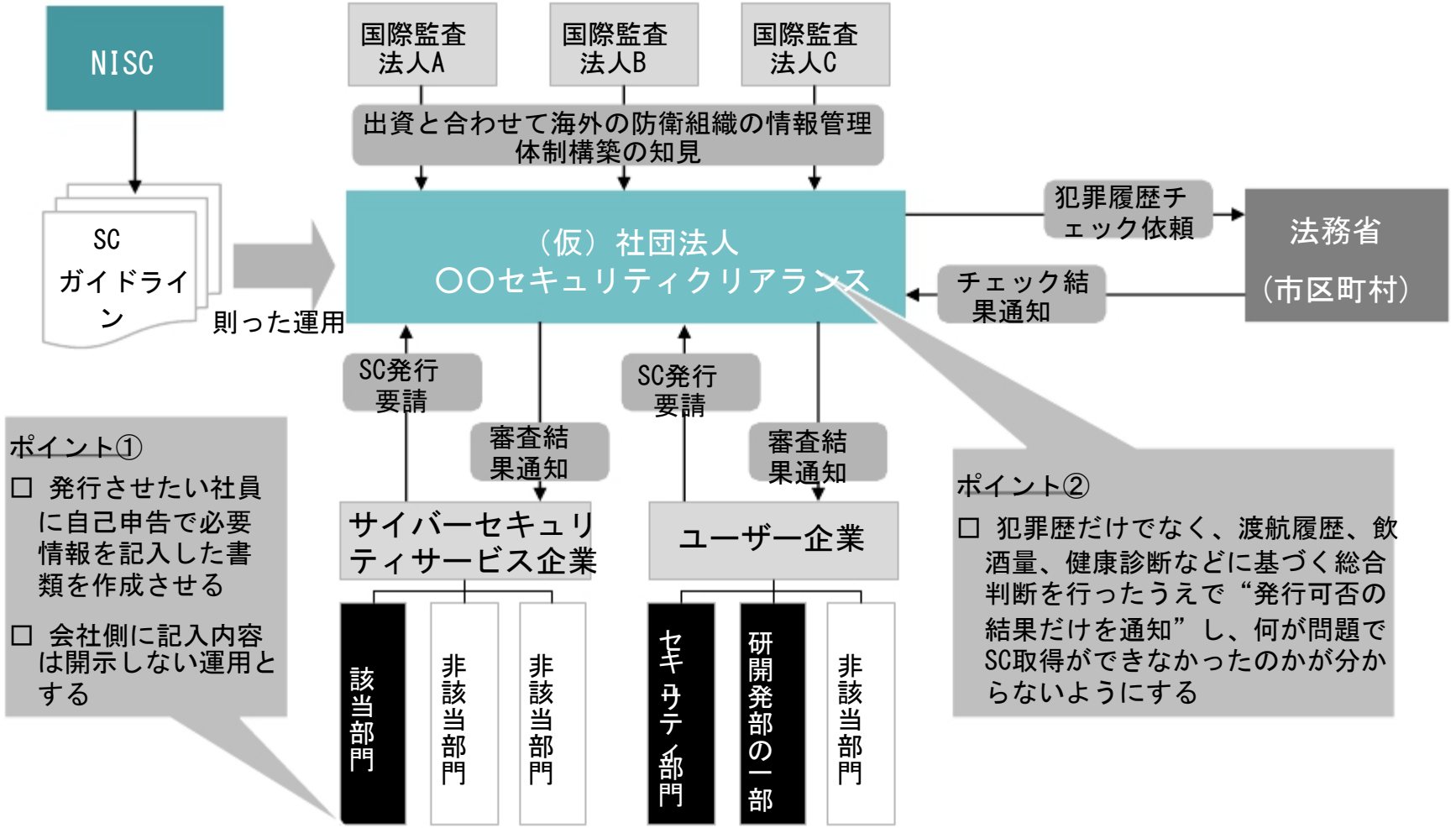
出典元：2017 自由民主党IT戦略特命委員会

HunsLab Inc
Confidential
2019

基本的な考え方：セキュリティファースト

セキュリティクリアランス制度（SC）創設

NISCが政府の特定機密にアクセスできるSCガイドラインを策定し、これに沿って、国際監査法人が社団法人を設立すべき。当団体がSC取得を希望する民間人と組織を審査してSCを発行するような民間主導の仕組みを構築すべき。



出典元：2017 自由民主党IT戦略特命委員会

HunsLab Inc
Confidential
2019

現状のセキュリティ資格認証

基礎レヴェル

資格名	概要
Security+	ネットワークからクラウドまで情報セキュリティの基礎的 な内容を幅広く扱う。IT 関連の資格認定を行う業界団 体 CompTIA が提供している。
GIAC Security Essentials (GSEC)	情報セキュリティの業務で必要とされる主に技術的な面 での基礎スキルを扱う。情報セキュリティのトレーニング を提供する SANS Institute 社による資格認証。
Certified Information Privacy Professional (CIPP)	情報プライバシーに関する資格認証であり、法規制、プ ライバシーの概念、データの取り扱いなどを対象とす る。情報プライバシーの非営利組織 IAPP が提供する。
Systems Security Certified Practitioner (SSCP)	1 年以上の実務経験を必要とし、モニタリングやインシ デント対応など、情報セキュリティの業務に必要な知識 とスキルを扱う。サイバーセキュリティの資格認定とトレ ーニングを提供する非営利組織(ISC)²が提供。

出典元：BurningGlass

HunsLab Inc
Confidential
2019

現状のセキュリティ資格認証

上級レヴェル（ 3～5 年 の実務経験）

資格名	概要
Certified Information Systems Security Professional (CISSP)	需要の高い資格認証であり、5 年以上の実務経験を必要とする。リスク管理、セキュリティ評価、監査、ID アク セス管理など 8 つの分野を扱う。(ISC)²が提供。
Certified Information Systems Auditor (CISA)	情報システム監査、セキュリティ、システム管理に関す る資格認証であり、5 年以上の実務経験が必要。情報 システム監査・情報セキュリティの専門家団体 ISACA が提供。
Certified Information Security Manager (CISM)	マネジメントレベルの情報セキュリティに関する資格認 証であり、セキュリティガバナンス、コンプライアンス、イ ンシデント管理などを対象とする。ISACA が提供。

出典元：BurningGlass

HunsLab Inc
Confidential
2019

今後のセキュリティ人材と資格制度について

資格制度と需要の関係における課題

- ✓ サイバーセキュリティの需要は専門サービス、金融保険、製造・防衛関連における人材需要が多い。近年では特に、金融分野、ヘルスケア、小売業での需要が続伸。
- ✓ 特に金融分野は法律によりサイバーセキュリティと金融の両方の知識とスキルを持つ人材を必要している点があることが課題。この 2 つのスキルを同時に得る機会は非常に少ないことが挙げられる。
- ✓ 全体傾向として、業界団体が発行している技能認定証や豊富なキャリアを要件としているなど、労働市場の供給側がすぐには解消できない点が課題となっている。

HunsLab Inc
Confidential
2019

サイバーセキュリティにおける人材開発

人材の発見と育成

1. 学校教育の中でシミュレーションを利活用
   携帯電話の利用は多くなったが逆にパソコン利用率は低下している。

2. ゲーム感覚によるオンラインCTFイベントを実施
   プロのゲーマーのようなヒーローを育てる。

3. 長期的な視点が必要
   攻撃防御の進化のスピードに人材育成が追いついていないことを理解するべき

4. 新しい雇用形態、業種、報酬制度の整備
   ダークサイドへの離脱を減少させる。米国の政府系求人を参考にするべき

HunsLab Inc
Confidential
2019

人的セキュリティクリアランス方法の開発

PCLsの基礎データとして

1. 米国では、SSNとクレジットスコア、運転違反記録、ローン情報、犯罪記録などが連動している、また近々、米国VISA申請時には、利用しているSNSアカウントIdの提示、また入国時にはパスワードの提示が必要になるとみられている。現在でもパソコンのログインを求められる場合がある。米国系SNS、リテール各社は、米国政府へ現在も情報提供を実施している。AMAZON,FACEBOOKなど。

2. 中国では、 「居民身分証」の番号は公民身分番号と連動し、社会的な信用度をスコアとして数値化するシステム「信用スコア」が浸透しておりスコアが上がればローン金利が下がったり病院で優待されるなどのメリットがある反面、信用度が下がれば公共交通機関の利用が制限されるなどの厳しい“罰則”も待っている。

HunsLab Inc
Confidential
2019

人的セキュリティクリアランス方法の開発

日本におけるPCLsの基礎データとしての可能性

1. 日本では、マイナンバーの運用が始まったばかりで浸透は今後急激に浸透する見込みは少ない。パスポートと運転免許証で異なった方式を採用。銀行、証券の口座はマイナンバーに名寄せされている。今後は仮想通貨口座にも連動。運転免許、パスポートとの連動は未定。

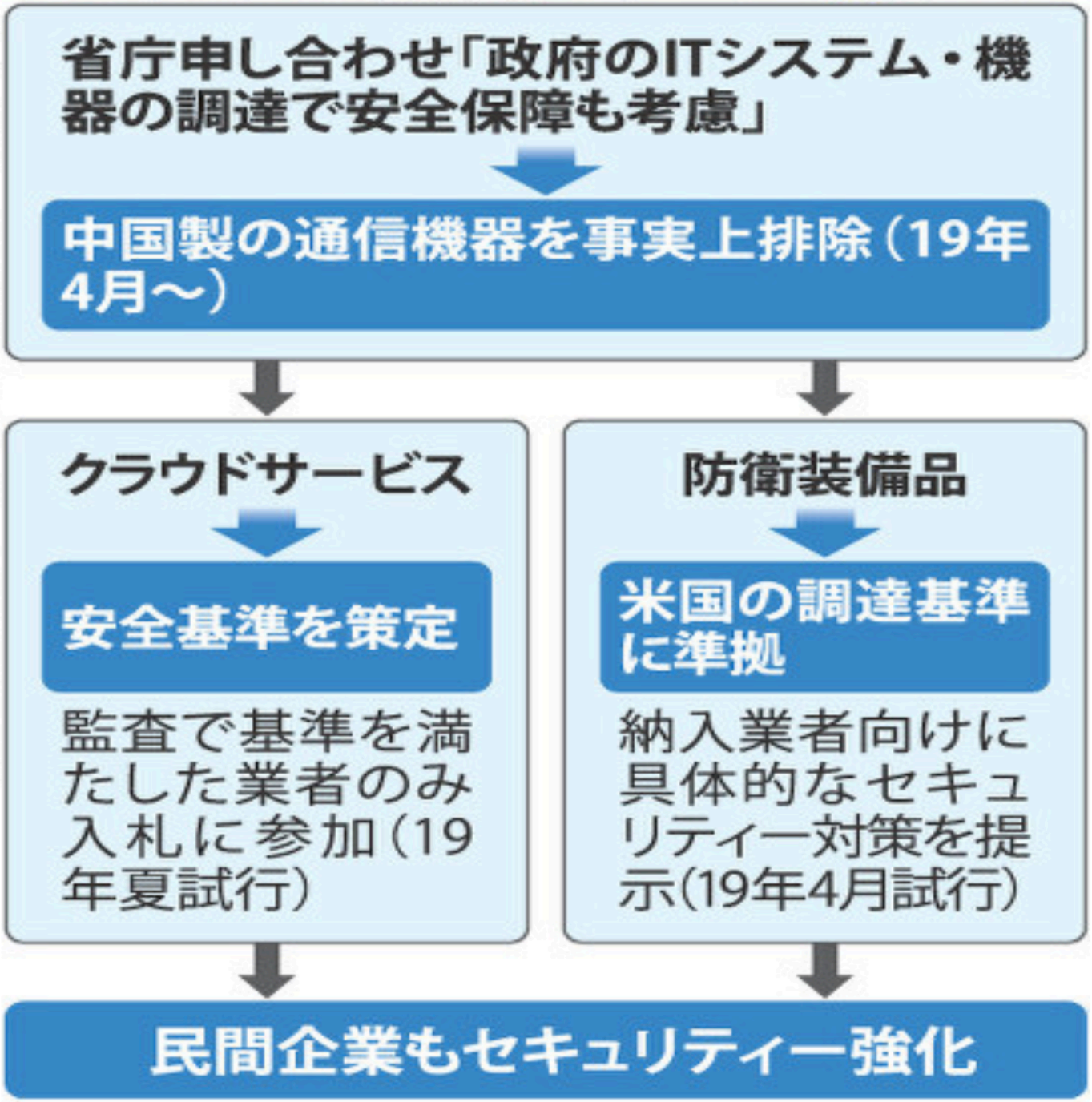
2. 電子マネー決済などを通して、行動履歴や、購買履歴の匿名データ利用が進む中、クレジットカード記録の管理より脆弱である。消費税からの還元という名目で電子マネー決済、クレジットカード各社への履歴データを要請可能か。

3. SNSなどの情報から自動収集
   Xkeyscoreのようなデータ収集、エスカレーションと評価、AIによる自動運用を構築、ID毎の思考傾向などをスコア化する

4. 警察、 外務省などとの連携による犯罪歴、渡航歴などの名寄せ、また特定宗教法人

HunsLab Inc
Confidential
2019

サイバー防衛を巡る日本の対応



HunsLab Inc
Confidential
2019

設備的セキュリティクリアランス開発

米国FCLsとして期待されている項目

1. クラウドサービス：
   FedRAMPベースのクラウド利用を推奨する方向。
   日本版FedRAMP構想もあり。日本がSCMの最下層までサイバーセキュリティの国際標準技術を搭載するには変化し続ける国際標準に対応する“日本版FedRAMP”クラウドを創設し、これを企業が利用していれば国際標準に準拠していると言えるITインフラを提供していくべき。

2. 防衛装備品：
   防衛省が入札する納入業者に向けた米国の調達基準に準拠させる。

3. 日米間の取り決めで中国製品、サービスの排除。
   ファーウェイ、ZTEの政府調達を停止。

HunsLab Inc
Confidential
2019

設備的セキュリティクリアランス開発

利用環境の見直しと新しい利用者要件

1. 利用環境
   CENEMO環境をベース
   - デバイスアクセス権限用証明書 (DAC)
   - 証明書コピープロテクション機能
   - SC保有者とDACとの認証
   - DNS,証明書の代理認証機能
   - キャッシュ機能
   - Dockerによる権限分離

2. 利用者のSNS情報からのSCレヴェルの適時更新

3. 利用者の意思確認、自動アラート

4. 利用者のアクセスパターン学習
   CENEMO-GW,EndPointで実施する

HunsLab Inc
Confidential
2019

新たなエンドポイント

1. 利用者の意思を確認

2. WindowsOSからChromeOSに移行させる

3. WindowsOSを継続利用する場合
   新たなエンドポイントが必須
   - 利用パターン学習
   - DEP認証、White Process方式
   - Backdoorネットワーク検知、自動排除
   - ramsome検知、自動排除、自動復旧

HunsLab Inc
Confidential
2019

新たなデータバックアップ方式を採用する

1. 分散バックアップから秘密分散バックアップへ
   データの消失から保護する考え方をさらに機密性と安全性を
   向上させた秘密分散方式とする。

2. 処理能力を向上させるため、秘密分散データ加工処理をGPUで演算できるメソッドを開発する

3. 上記秘密分散バックアップデータの圧縮を同時に別GPUもしくはVPUで実施する

4. 秘密分散とするため、パブリックストレージも利用可能

HunsLab Inc
Confidential
2019