産学官連携によるサイバー空間の安全性確保

- 犯罪に強い社会の実現のために -

田中　英彦

情報セキュリティ大学院大学

2013年9月3日

目　次

1. 産学官連携の必要性
2. 情報時代の犯罪
3. 問題と組織的対策
   - 変化対応、米国政策、日本政策、クラウド域外アクセス、政府内対応、対応組織例
4. 対策の実効化に向けて
   - 情報共有、サイバ対応力強化、制度の考察、情報自体の保護、企業育成と研究開発、政策の全体構造
5. 人材育成
   - 必要人材、プログラム、教育内容、育成の実効化

1. 産学官連携の必要性

- 情報社会ではあらゆる活動のベースがサイバー空間であり、根源的対応が必要
- サイバー空間は従来の物理空間と異なる特性を持ち新対応を要す
- 根源問題には全メンバ（産学官）が協調して役割（製品サービス/教育研究/制度・執行）発揮する必要あり

サイバー空間の安全性確保

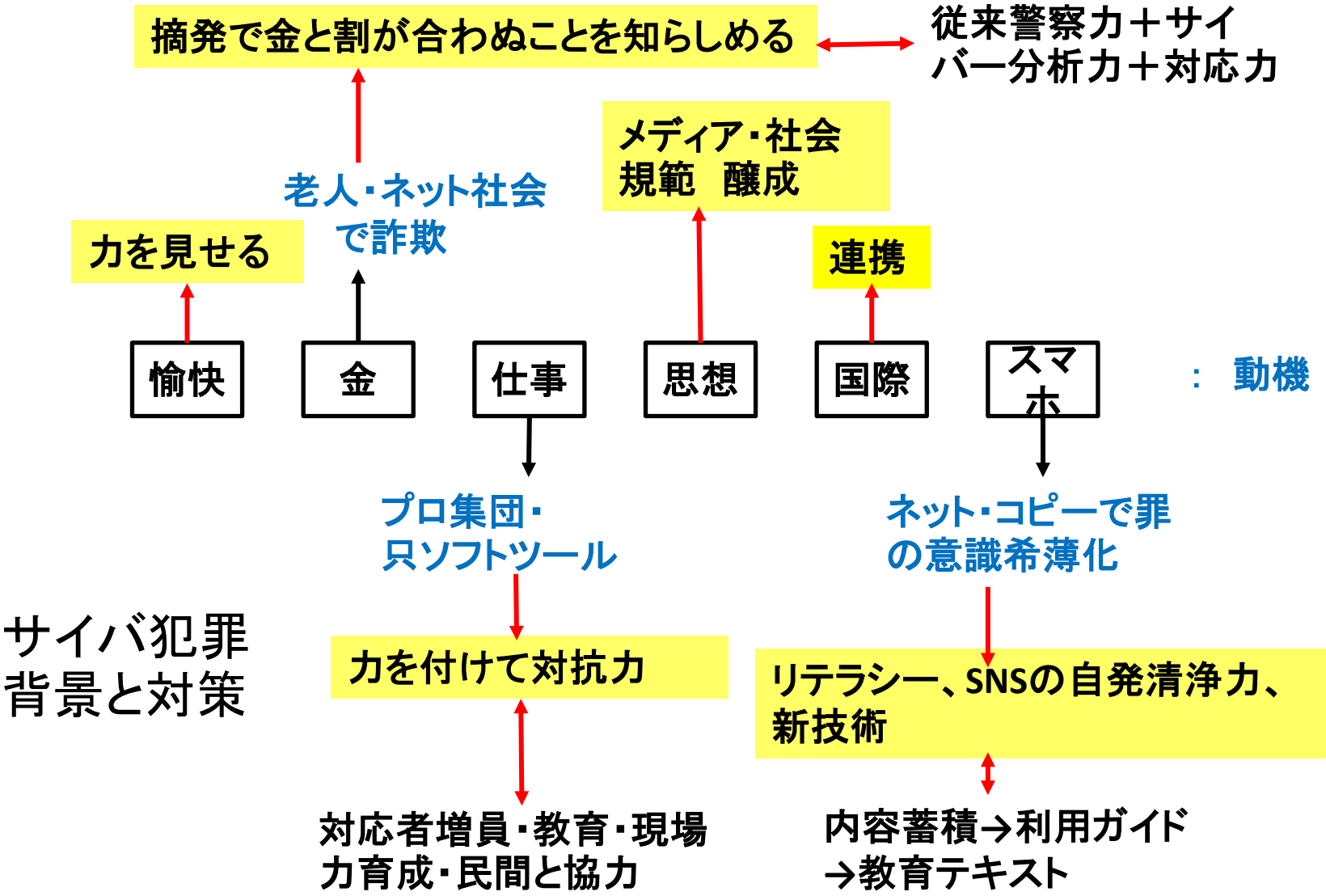
- 犯罪に強い社会
  - 情報犯罪が起こり難い、起こっても対策が直ぐされるという状況の醸成
- それを可能にするために
  - 対策：制度設計、組織設計、情報システム、対応人材の手当、社会の意識とリテラシ
  - 対応活動：情報収集、分析、対処、防御、管理
  - 国際対応：ネット社会は越境容易、不可欠

GRAND CHALLENGES FOR ENGINEERGING
-2008 National Academy of Sciences-

- Make solar energy economical 7
- Provide energy from fusion 10
- Develop carbon sequestration methods 13
- Manage the nitrogen cycle 16
- Provide access to clean water 19
- Restore and improve urban infrastructure 22
- Advance health informatics 25
- Engineer better medicines 30
- Reverse-engineer the brain 34
- Prevent nuclear terror 37
- Secure cyberspace 40
- Enhance virtual reality 42
- Advance personalized learning 45
- Engineer the tools of scientific discovery 48

2. 情報時代の犯罪

- 道具の変化
  - 電話、手紙　→　インターネット、スマホ、クラウド
- 意識の変化
  - 文書を盗む　→　コピーする（犯罪意識希薄）
  - 手紙を送る　→　メールを送る（1万通容易、只）
  - 紙の情報　　→　スマホ内に在る情報
  - 情報は紙から　→　情報はネットから
  - 本(IP) 有料　　→　インターネットで無料
  - 数日の時間差（移動）　→　数秒の時間差（ネット）
- 攻撃側と防御側の立場
  - 攻撃側有利、多くの隅（変更容易）を突くことができる
  - 防御側は、あらゆる可能性をチェックする必要


摘発で金と割が合わぬことを知らしめる
従来警察力＋サイバー分析力＋対応力
老人・ネット社会で詐欺
メディア・社会規範　醸成
力を見せる
連携
愉快
金
仕事
思想
国際
スマホ
：　動機
プロ集団・只ソフトツール
ネット・コピーで罪の意識希薄化
サイバ犯罪背景と対策
力を付けて対抗力
リテラシー、SNSの自発清浄力、新技術
対応者増員・教育・現場力育成・民間と協力
内容蓄積→利用ガイド→教育テキスト

3. 問題と組織的対策

① 変化への対応
② 米国の政策
③ 日本の政策
④ クラウド域外アクセス問題
⑤ 政府内対応
⑥ サイバー対応組織例

① 変化への対応

- 犯罪のサイバー化に適応する
  - 可能な組織構造：人の展開とネット化の融合
  - 犯罪対応部門の、犯罪変化に追随した知識の醸成と、設備の更新（現場ツールの必要性）
  - 新技術に追随する民間との協力関係を築く
- 法制への対応基本
  - 犯罪の再定義：情報時代の犯罪を踏まえ、ガイドライン等ソフトローの対応でリード
  - 適切なタイミングでハードローへの反映

② 米国の情報セキュリティ政策

- 政府の取り組み
  - 2009全米サイバーセキュリティイニシアティブ、2011連邦CS R&D戦略計画
  - 2013.1 DODサイバー司令部(2010設置)の増強(900→4,900)、防衛だけでなく攻撃を目的とした編成
- 情報に関する官民連携:国家安全保障との関係で連携重視
  - 2008US Cyber Challenge : 官民共同人材育成プログラム
  - 2012情報共有と安全性保護に向けた国家戦略
  - 官民連携CS R&Dセンター、情報共有分析センタ
  - 政府機関間、CERT、NOC、分野別連携の枠組み
  - 官民パートナーシッププログラム、司法・インテリジェンスの情報連携
- 関連法案状況
  - 2012, 2013重要インフラのセキュリティ強化は監視強化懸念で廃案、脅威情報の共有はプライバシー懸念で廃案
  - 2013.2 官民連携制度策定中、2013.6　スノーデン問題
  - 2013.7 情報セキュリティへのインセンティブ検討中

③ 日本の政策

- 情報セキュリティ政策会議と内閣官房情報セキュリティセンター
  - 公私パートナーシップの強化、政府組織・重要インフラ・ビジネスと個人
- 政府機関の基盤
  - 政府CISO, セキュリティ緊急支援チームCYMAT, 政府横断的情報収集・分析システムGSOC
- 総務省：PRACTICEプロジェクト
  - サイバー攻撃に対し、先取対応研究と実施テスト計画、共有データ：国内で捕獲されたサイバー攻撃情報、他パートナ国の同種情報、DAEDALUSデータ
  - 結果：攻撃類似性、攻撃の振る舞い兆候
- 経済省
  - サイバー情報共有イニシアティブ、電力、ガス、化学、石油　の５業界、39参加組織でサイバー攻撃情報共有実運用中、サイバー攻撃解析協議会
- 警察庁、防衛省
  - 情報技術解析課、サイバー防衛隊
- 国際連携
  - 日米、日英、ASEAN：サイバーインシデント対応協力、重要インフラ防護国際連携、意識啓発協力、人材育成協力、サイバー空間上国際的行動規範作り

行政手続き番号法

- 2013年5月31日成立
  - 諸制度連携の第一歩：社会保障、税、防災
  - リンク評価の考え方整理等、多くの課題
  - 特定個人情報保護評価活動を通したプライバシーの適切な実効保護レベルの模索
    - レベルは使用経験により変わる。分らないことから来る恐れと現実（なんとなく不安感vs実被害vs利用価値）
- Oエラー問題
  - 保護の有効性限界と法的切り分けの意味認識

④ クラウドデータ域外流出問題

- 米国：愛国者法、外国情報監視法(FISA)の修正法
  - 当局が米国のクラウド企業に対し米国市民以外のデータを提出するよう強制可能
- EU: EUデータ保護指令の改正作業
  - 2012開始。第42条　修正案（反FISA条項）
  - EU監督当局の明示的な許可なく、第三国が域内の個人情報にアクセスすることを禁じる
- 方向性
  - 国際的クラウド企業は、どちらかに背くので板挟み
  - 方向案：EU側。個人情報制御権原則から対抗。その制御権の超越は犯罪が明確な場合。

⑤ 政府内対応

- 政府内情報一元化
  - 対国際、対国内にも統一性が必要。継続性と法律整備、省庁所掌明確化
  - リスク・インテリジェンスに基づく統制：専従のサイバーセキュリティ調整官
  - 公共・民間・防衛の3分野区分と連携
- サイバー部門強化
  - 情報収集・分析・対応、人材（量、質）と設備の強化
  - 情報流通の種類（電子、人・紙、インテリジェンス）

⑥ サイバー対策組織例（韓国）

- 公共・民間・国防の3分野に区分し協調
  - 公共：国家情報院、安全行政、金融委員会、検察、警察
- 民間：韓国インターネット振興院　KISA
  - モニタと対応、民間が95%以上
  - 機関連携：3分野間、通信業者、セキュリティ会社、国際
  - インターネット24時間モニタリングと対応
  - DDoS防御サービス：サイバー待避所構築、ゾンビPC検知・通知・治療
  - 国内全Web HP（200万)のコード点検（3回/日）・遮断・悪性コード削除措置、相談センター運営
- 連携：3分野間
  - 悪性コード共有、事故分析資料共有、事故移管、調査協力

4. 対策の実効化に向けて

a. 情報共有
b. サイバー対応力の強化
c. 制度の考察
d. 情報自体の保護
e. 企業育成と研究開発
f. 政策の全体構造

a. 情報共有

① 情報共有連携の必要性
② 留意点
③ 情報共有の在り方
④ 情報共有の基本問題
⑤ 問題の現状と解決に向けて

①情報共有連携の必要性

- 得意不得意分野
  - 民間活動/警察活動/教育研究活動
  - 企業実務現状/犯罪情報/研究情報
- 異なる特性の利用
  - 市場状況/捜査力/第三者意見
- 連合の意義
  - 異なる観点からのデータ集結
  - 思考形態の異なる分析の利用
- 過去と今後
  - 犯罪の専門性、IT技術発達で、今後は民間と重なり、協力必要

情報共有のインセンティブ

- 官：安全を与え、協力享受
  - 広い情報源を実時間で得る（コスト性能比が良い）
  - 新しい分析手法を得る
  - 新分析手法に関わり人材育成できる
  - 社会の認知を得やすい
- 民：安全享受、捜査協力
  - 通常得難い現場情報を入手
  - 新しい分析手法や対応システムのニーズを得る
  - 官との共有で、通常得難い他民間情報入手(1対N)
  - 官の協力で共有機構の維持が容易
  - 公への協力というボランティア精神が満たされる

文書へのマルウエア埋め込み
― 現場情報の威力例 ―

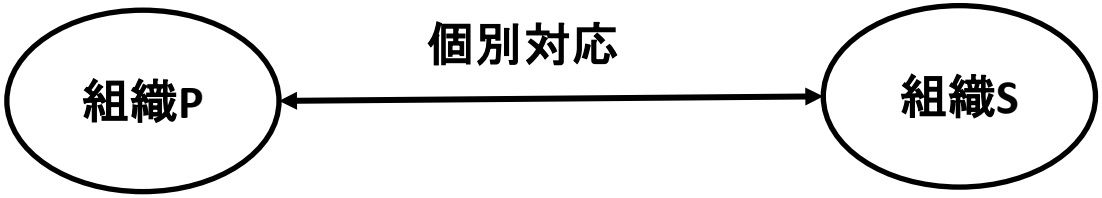
- 文書に実行ファイルを埋め込む
  - メールなどに添付し標的型攻撃に利用増加
- MS文書
  - MS 文書ファイルの場合、文書ファイルサイズや構造情報を検査，悪性文書ファイルを検知
  - 98.5%の検知率、一般のファイル検証機能の率は38.8%
  - Microsoft Office 2010 のファイル検証機能の検知率91.0%
- PDF文書
  - PDF文書ファイルの場合、従来PDFファイル中のJavaScript 等不正なコード検知手法で20%以下の検知率
  - 悪性PDF ファイルには構文解釈ができない部分，表示内容と関係しない部分が含まれる等の特徴があり、それを検査
  - 悪性PDF ファイル164 個に対し，99.4%検知

②情報共有の留意点

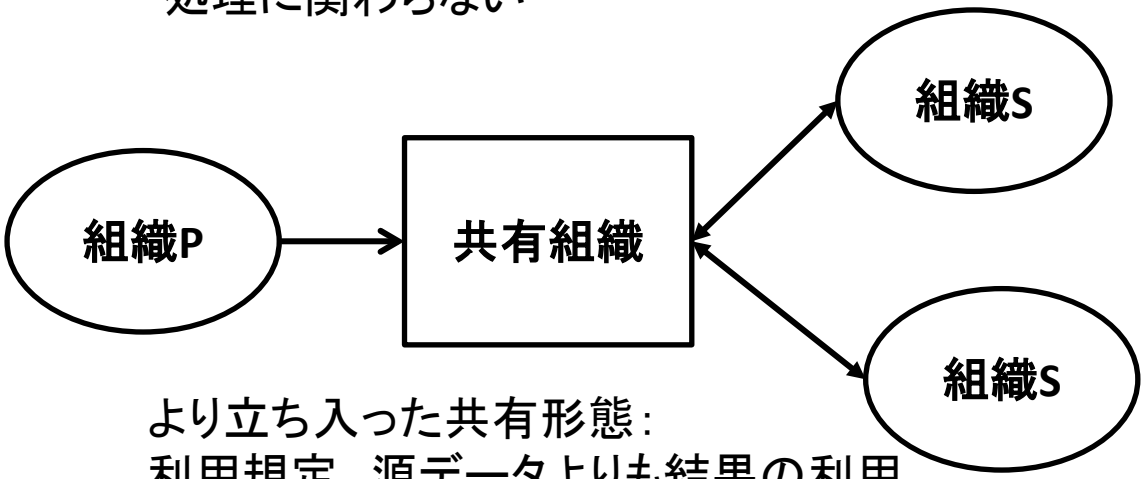
- 官民間情報収集思惑のアンバランス
  - 官の威力、善意とメリット勘案
- 元の情報源と提供情報との関係
  - アクセス権、知的財産権：持込み者が解決
  - プライバシー問題：情報匿名化*、他の技術
- 信頼関係の構築と情報管理
  - 共有機構の明示的メンバ間の人的信頼関係ベース
  - 機密対策、情報漏洩、外部からの攻撃対策
- 提供物
  - 警察：現場セキュリティ関連情報
  - 企業：ネット状況等諸セキュリティ情報、新技術
  - 大学：研究、評価、第三者性、マンパワー（学生）

③ 情報共有の在り方

- オープン化
  - 協力している事実はオープンにする
  - 情報共有原則と、定期的活動報告を公開
  - 第三者機関等、外部意見を受けて検討する体制整備
  - 民の自主協力情報の活用
- 情報の扱い
  - 扱う情報自体は秘密を原則：NDA
  - ステークホルダ間の情報アクセス権の明確な規定
  - 人の信頼がベース
- 情報共有の形態
  - 情報に依存する共有形態

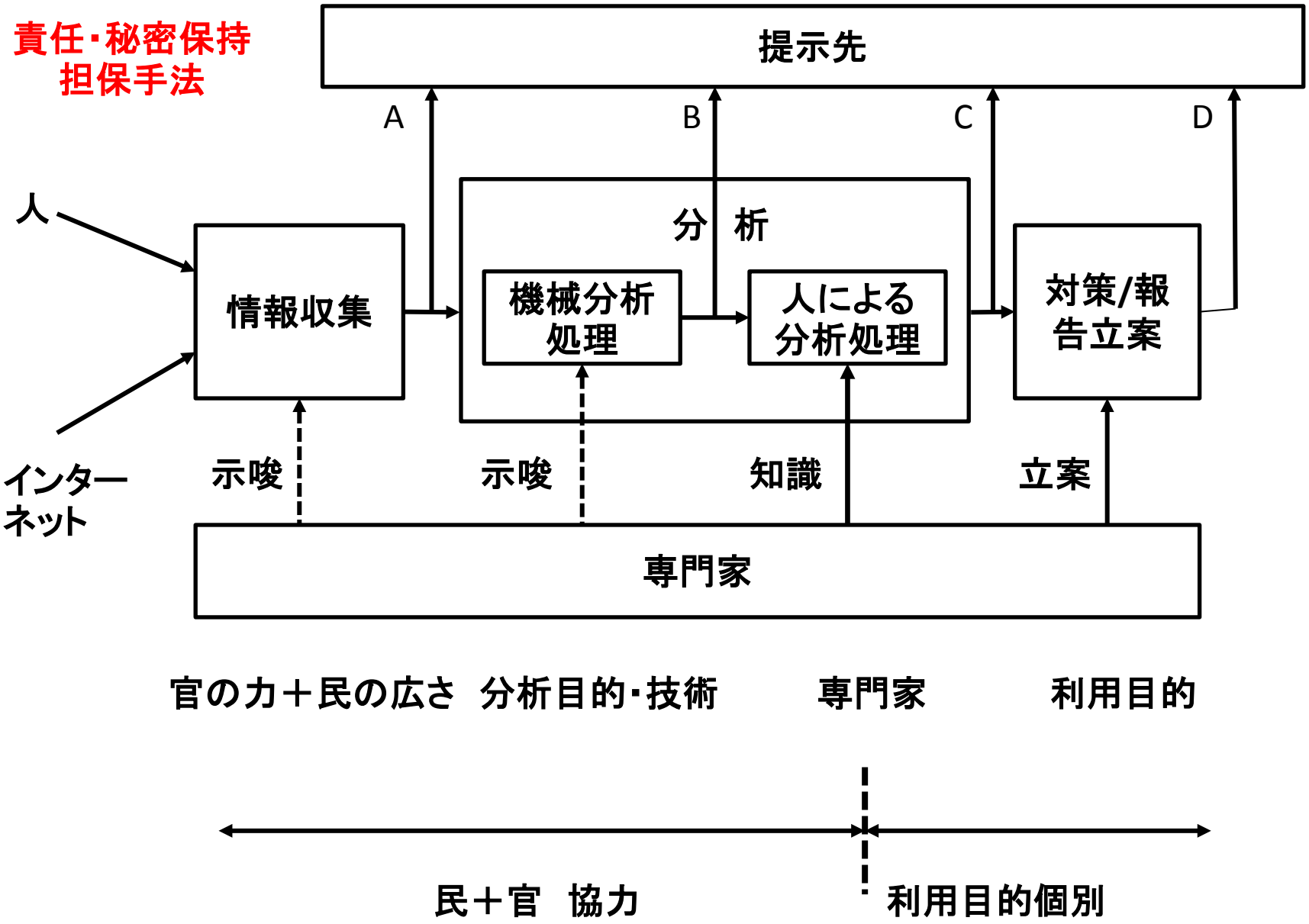


独立性高い単純方式:
規則を決めて個別に利用データを渡し、
処理に関わらない



より立ち入った共有形態:
利用規定、源データよりも結果の利用

様々な情報共有形態の利用:データ依存


責任・秘密保持
担保手法
提示先
A
B
C
D
人
分　析
情報収集
機械分析
処理
人による
分析処理
対策/報
告立案
インター
ネット
示唆
示唆
知識
立案
専門家
官の力＋民の広さ
分析目的・技術
専門家
利用目的
民＋官　協力
利用目的個別

情報共有のメカニズム

- 民間と官のインタフェース
  - 民間組織に、官の特定者が関与。相互にNDA
  - DBを官または民の特定者が特定目的に応じて利用
  - DB内蓄積は、情報提供者の必要に応じ匿名化など措置
- 情報共有の有効性とプライバシ保護
  - データ単位の広いアクセス権設定+利用目的の規定
  - 護るはプライバシー、個人情報保護はその一手段、絶対視は共有の実効性を無くす可能性
  - 利用目的の記述で最終インタフェースを定める

④ 情報共有における基本問題

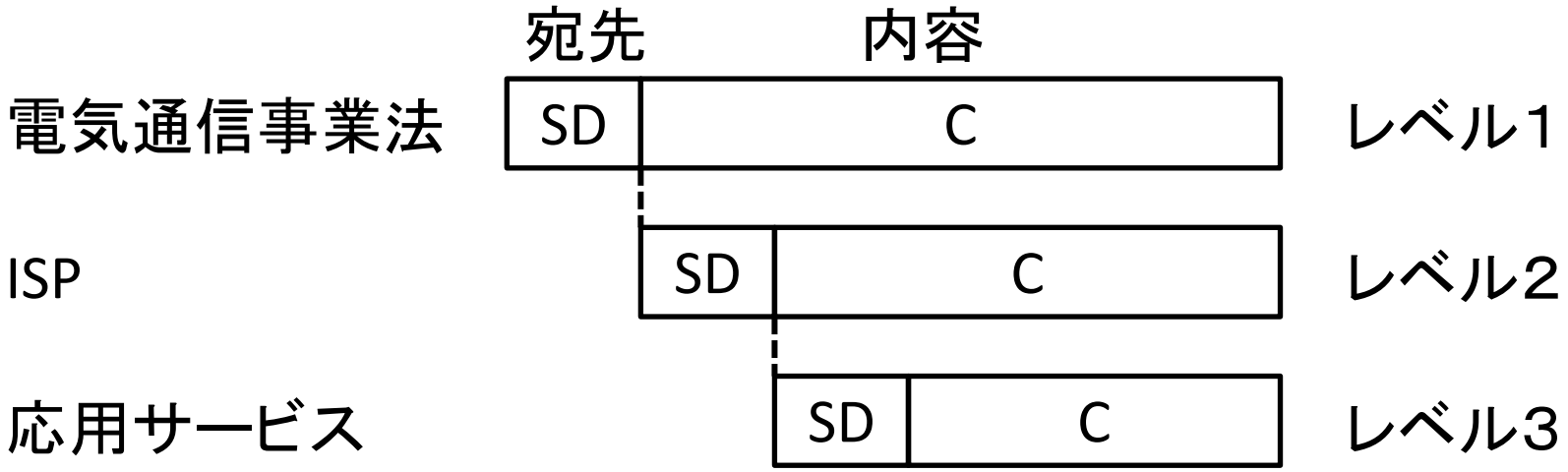
- 情報収集における制約：収集
  - サーバ管理：不正アクセス防止法は努力義務
  - ログ取得の制約：電気通信の範囲、収集要請と協力による
  - インシデント届出は努力義務なので情報が蓄積されない。IPAも、提供蓄積に留まる
  - 現状では、官が一般モニタリングをすることは困難
- 信書の秘密からの制約：分析
  - 送り元、宛先情報のみ利用可能、内容の利用禁止
- ビッグデータからの脅威問題
  - リンクで個人特定問題：匿名化は一手段、絶対視は不可

ログ取得問題

- 義務化拡大のみでは困難
  - コストが膨大。インセンティブ（対策費、税制）が必要
  - セキュリティ対策にはログも必要、主体的に守る推奨。サービス品質など他の形に転化
  - ベースになるインフラの中でも電気・通信などは、情報に絡むので、他のインフラと区別した扱いが必要
- ログ取得
  - 米国では、インシデント時、消さないことを求めることが出来るが、既に消去済には対応できない
  - 電気通信事業法の枠には、上位層サービスが入らない。規制無し。今後は通信とサービスが融合、ある程度の規制をかけることの是非を検討すること要す
  - 「信書の扱い」の時代に沿った書き直し

信書問題

- 従来：信書の秘密、SD+C の内SDはログ有
- 今後：新たな枠組み、レベル構造

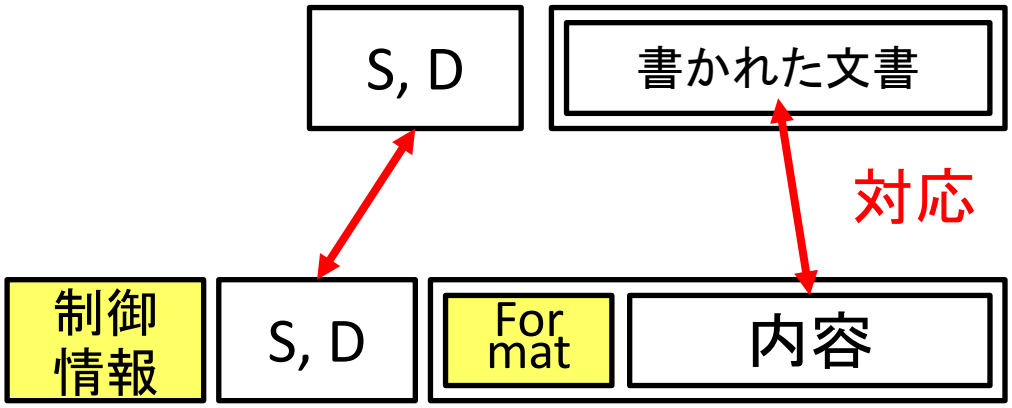


⑤ 問題の現状と解決に向けて

- 要請
  - 信書の秘密問題の新時代対応
  - 情報収集と、それへの十分な解析性の保証
  - プライバシー問題対処に、個人へ情報制御権を付与
  - ビッグデータからの不安感除去
- 対応
  - 従来の議論：対立問題に対し「バランス」論理に留まり抜本的解決になっていない
  - 技術：限界を破る両立性を実現可能
  - 技術を考慮した新世代法制の構築
  - 民からの自主協力による情報提供の活用

「信書の秘密」の情報時代に向けた再検討

手紙



メール

コピー容易

新情報　　新情報　　:新判断要す

サイズ　　形式、サイズ

中継情報　　S’, D’

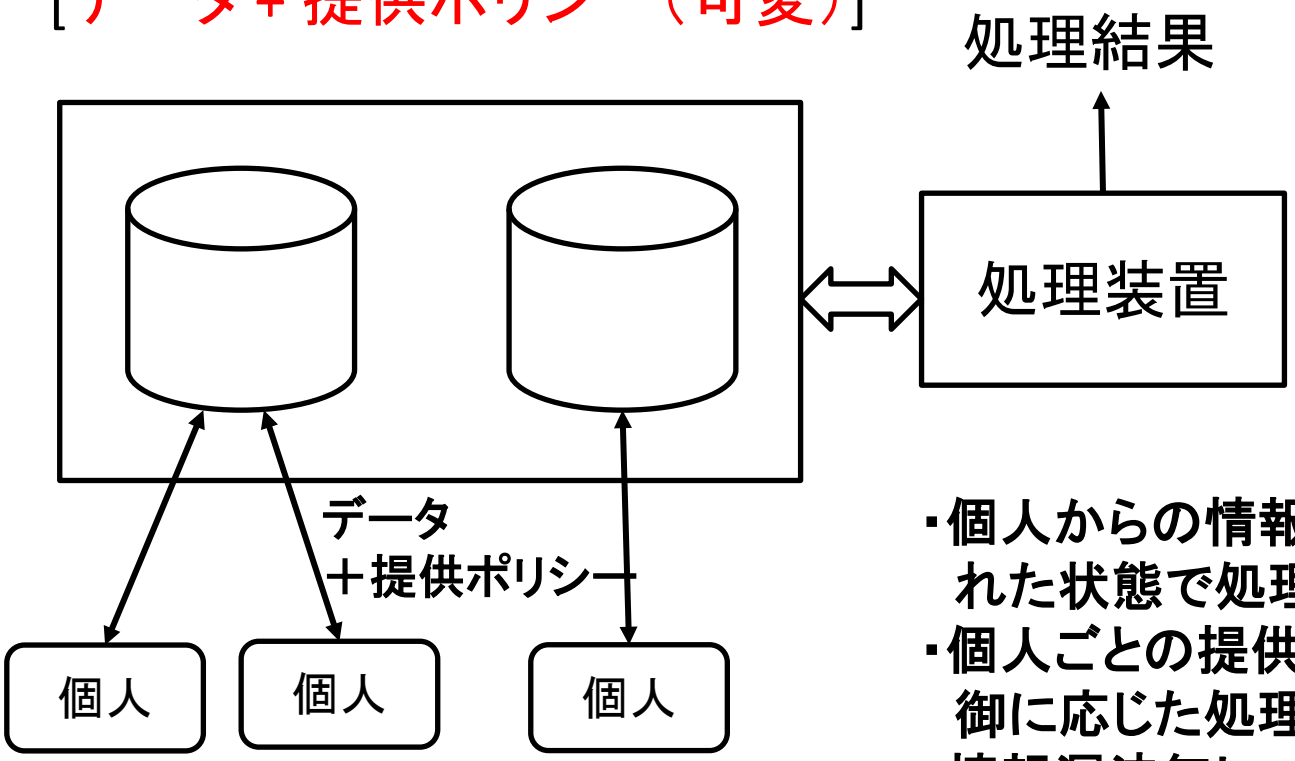
(wordなのに実行ファイル挿入)

利用のメリット:追跡に有用　マルウエア判断に特に有用

内容とは無関係な犯罪情報(実行ファイル添付)

暗号化DBの集合:完全準同型暗号

[データ＋提供ポリシー（可変）]



- 個人からの情報を暗号化された状態で処理可能
- 個人ごとの提供ポリシー制御に応じた処理可能
- 情報漏洩無し
- 突合せ問題は、利用目的による制限で対応可能

解析性と制御性の両立

新しい情報セキュリティ技術

- セキュアネットワーク
  - トレーサブル、利用者保証、希望参加ベース
- セキュアシステム
  - プログラム限定、セキュアOS、IO限定、セキュアPU
  - 常時モニタリング
- 暗号の多用
  - 管理容易、高速符号化・復号化
- 未知の脅威分析
  - 実時間検知(Black List, 振る舞い)、プロファイリング
- ビッグデータの活用
  - マルウエア、攻撃事例、犯罪事例、個人情報利用
  - アクセス履歴から有効な推奨広告。暗号利用で、すべての関係者に伏せた処理可能。プライバシー侵害無く、処理と両立。

セキュリティデータベースの可能性

- 諸レベルのデータ
  - 実時間生データ：IPメッセージ、光ファイバ内情報、IX、傍受
  - 抽出データ：ログ、SOC、email/文書/画像/chat
  - 処理結果：脆弱性データ、ハッカー関連情報、サイバー攻撃ケース、ハッキングツール、ハッキング手法
  - 生でなくとも可能な対策は多い。生は民の自主協力情報
- 様々な処理
  - FW/IDS/UTMにおける処理、ログ分析
  - サイバー攻撃プロファイリング：国内外の侵害事故を定型化し管理、新ハッキング攻撃手法及び道具分析、関連機関・ホワイトハッカーの分析結果収集
  - 侵害事故関連性分析：事故間悪性コードの関連性分析、攻撃手法の類似性分析、時系列分析による攻撃間関連分析

b. サイバー対応力の強化

- 防御に偏せず最低限のリスクを許容し、対処策を講じ、実質被害を発生させない
- 重要施設に対する情報通信基盤施設
  - 区別して指定と管理、通信＋電力等
- 円滑な初期対応のための現場確認と技術支援のための法的根拠作成
- 国内外の関連機関との協調体制強化
- APT等進化サイバー攻撃の予測及び迅速対応可能システム構築
- 専門人材の拡充、必要設備の強化

c. 制度の考察

- 情報共有制度の現状
  - コンピュータウイルスや脆弱性情報、インシデント情報などの報告制度、義務無しで十分に活用されず
  - 情報共有制度の積極活用が必要
  - 限られた分野内でのインシデント情報共有
  - 実時間の情報共有体制が無い
- 新たな政策
  - 公私協働型の政策手法の導入
  - 法よりも、ガイドラインや第三者認証等のソフトロー、企業組織規律、実効性を持たせる

情報共有の為の制度検討

- 公私協働型の政策手法の利点
  - 変化と進化を続ける情報の利活用に、政府規制で詳細記述は不可能、望ましくない
  - 主は、イノベーションの詳細知識を有する産業界の自主規制（柔軟性、当事者知識反映）
  - 自主規制に完全委任はリスクと限界：プライバシ等
  - 共同規制(corregulation)、自主規制の利点を生かし、リスクや限界を政府が法制度で補完
- 情報共有に関わる法制度と再検討
  - プライバシー、知的財産、セキュリティ政策、情報公開法制、不法行為責任、刑事法（犯罪捜査時のデータ保持・開示措置）
  - 共同規制利用促進に必要な法改正
  - 国際的制度比較と理解

諸外国の状況と日本

- EUと米国
  - ビッグデータ利活用を先導する米国や、プライバシー保護重視のEUで、共同規制手法を重視したルール形成進行中
- 我が国
  - プライバシー保護の第三者機関（特定個人情報保護委員会）の設立を含めた行政組織の変革
  - 法実装の検討中：プライバシーインパクト評価の在り方と利用、個人特定可能性からプライバシーへ
  - これらに加え、自主規制の強化に基づくイノベーションを促進する政策手法を

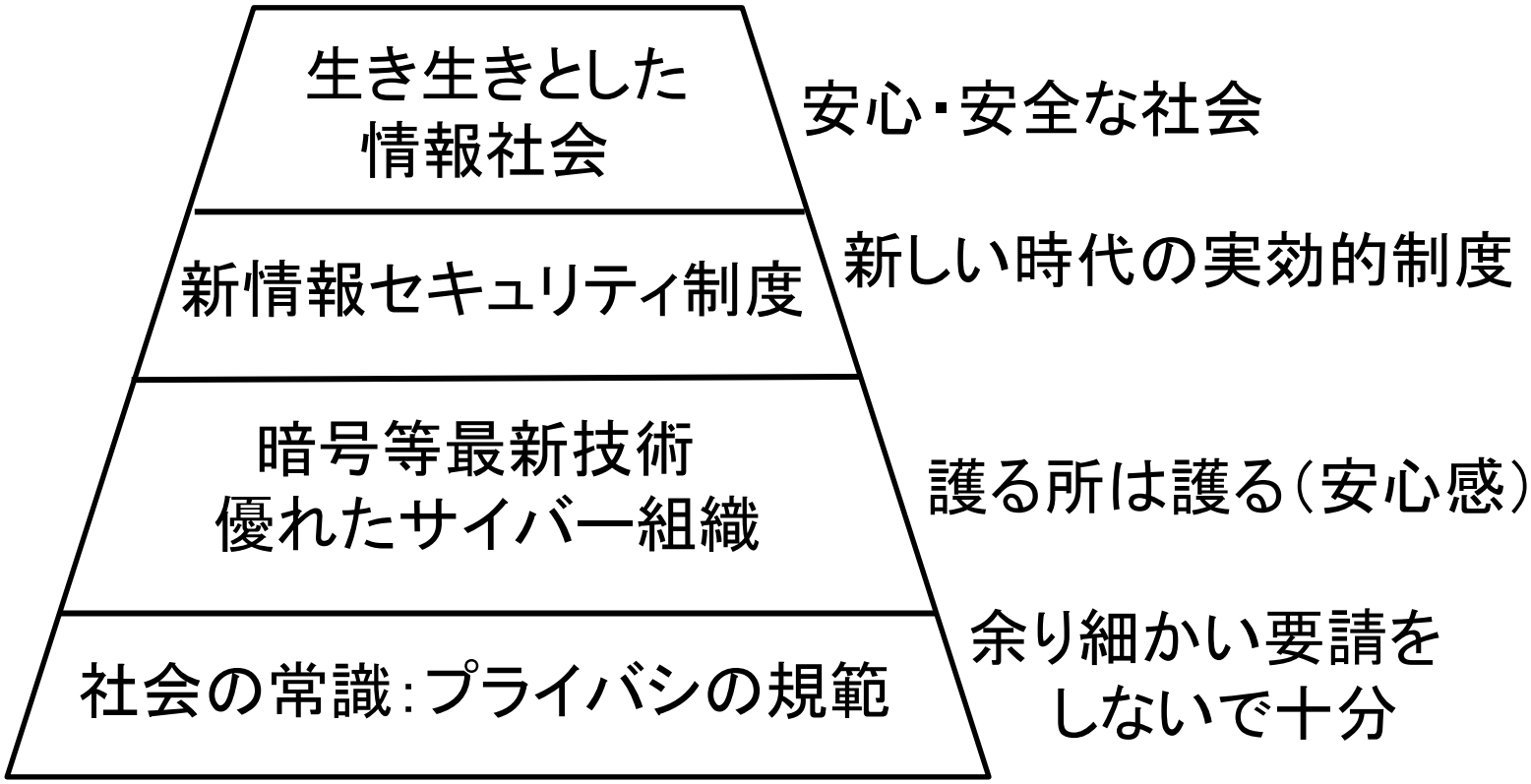
d. 情報自体の保護

- 国
  - 秘密保全法案計画中、特定秘密と厳罰化
- 民間
  - 企業秘密保護：ノウハウとイノベーションは、最重要資源だが、国際的サイバー攻撃、モバイルが脅威に
  - 現状：不正競争防止法、厳密秘密管理と立証必要
  - 情報そのものの営業秘密保護目的の現実的法案と国際対応が必要
  - まずはガイドライン、企業組織規律、から始め、企業情報の保護監査及び公示制度の可能性検討
  - サイバーセキュリティ産業活性化施策：クラウド、モバイル、ビッグデータに向けて

e. 企業育成と研究開発

- 企業
  - 情報セキュリティ産業は小規模(日本76億/世界1900億ドル)、セキュリティ向上に振興・活性化の支援整備
  - 一般企業は情報セキュリティ意識希薄、企業内セキュリティ担当者設置推奨、基盤のセキュリティレベル規制
- 技術と制度の研究開発
  - 国家安全保障(交渉力)、独自技術、技術の囲い込み、長期的視点、チップのブラックボックス化対応(forensics)
  - 若者に夢を提供
- 国際問題
  - 国際協力、官民連携情報共有政策の国際連携
  - 国際企業へ国内法の適用可能性検討

f. 政策の全体構造


生き生きとした
情報社会
安心・安全な社会
新情報セキュリティ制度
新しい時代の実効的制度
暗号等最新技術
優れたサイバー組織
護る所は護る（安心感）
社会の常識：プライバシの規範
余り細かい要請を
しないで十分

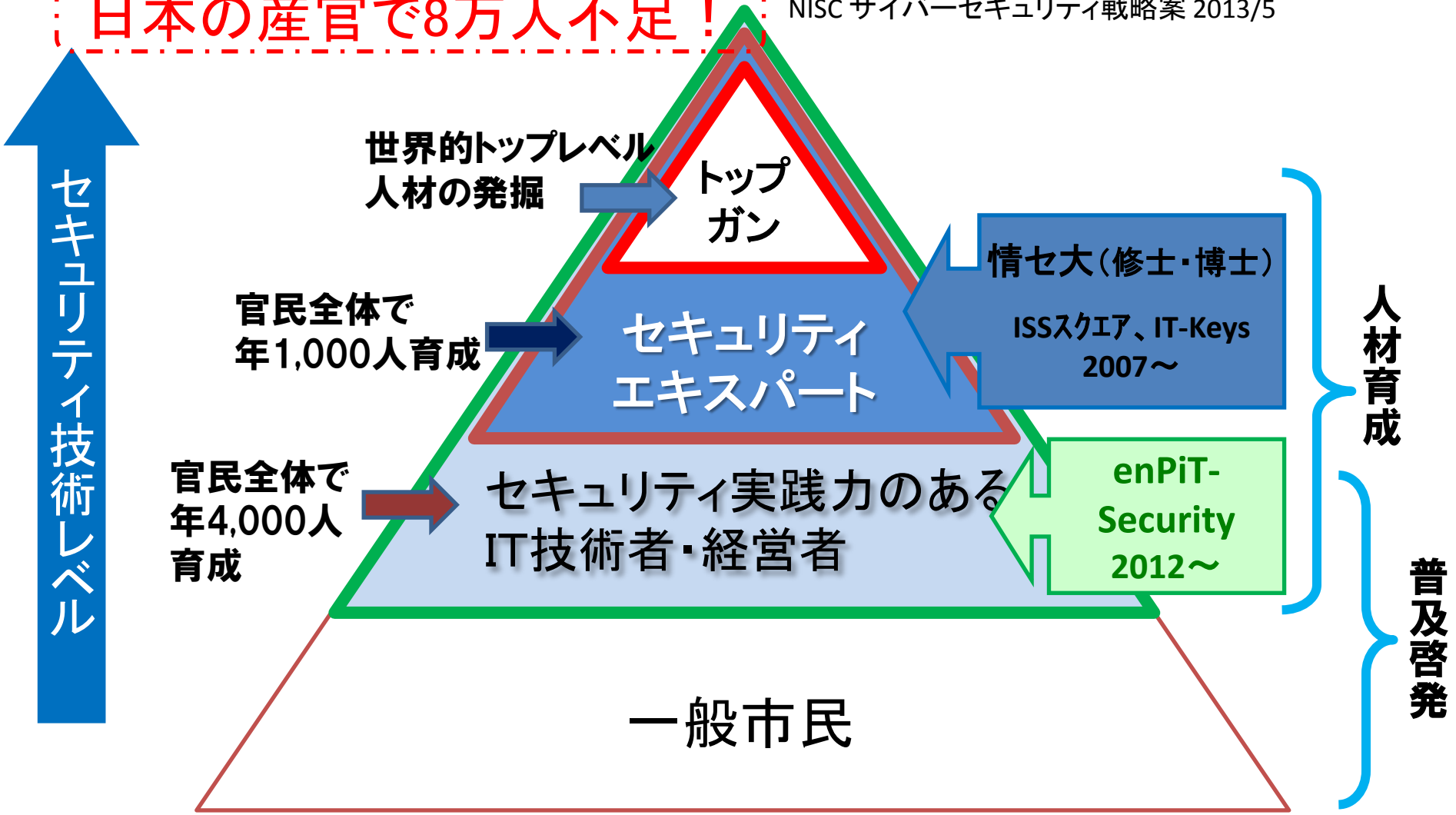
5. 人材の育成

- 国を挙げての人材育成活動
  - 従来：言葉には上るが実効性に欠けた
  - 情報資源：企業や国の中核資源
  - 人材：今後の国の基盤を支える重要資源。抜本強化の実行は喫緊の国の責務
- そのために
  - 様々な人材
  - 人材養成プログラム：量と質
  - 教育内容と組織
  - 人材育成の実効化

我が国に求められるセキュリティ人材育成

日本の産官で8万人不足！

NISC サイバーセキュリティ戦略案 2013/5



様々な必要人材

専門知識による分類

- セキュリティ計画・対応責任者
- 監視、情報収集、分析専門家
- インシデント対応マネージャ
- インテリジェンス専門家
- 現場対応者：Forensics
- 情報法制専門家
- 技術研究・開発者
- 国際連携対応者：情報、協力
- 教育用人材：専門家育成、リテラシー教育

組織内役割による分類

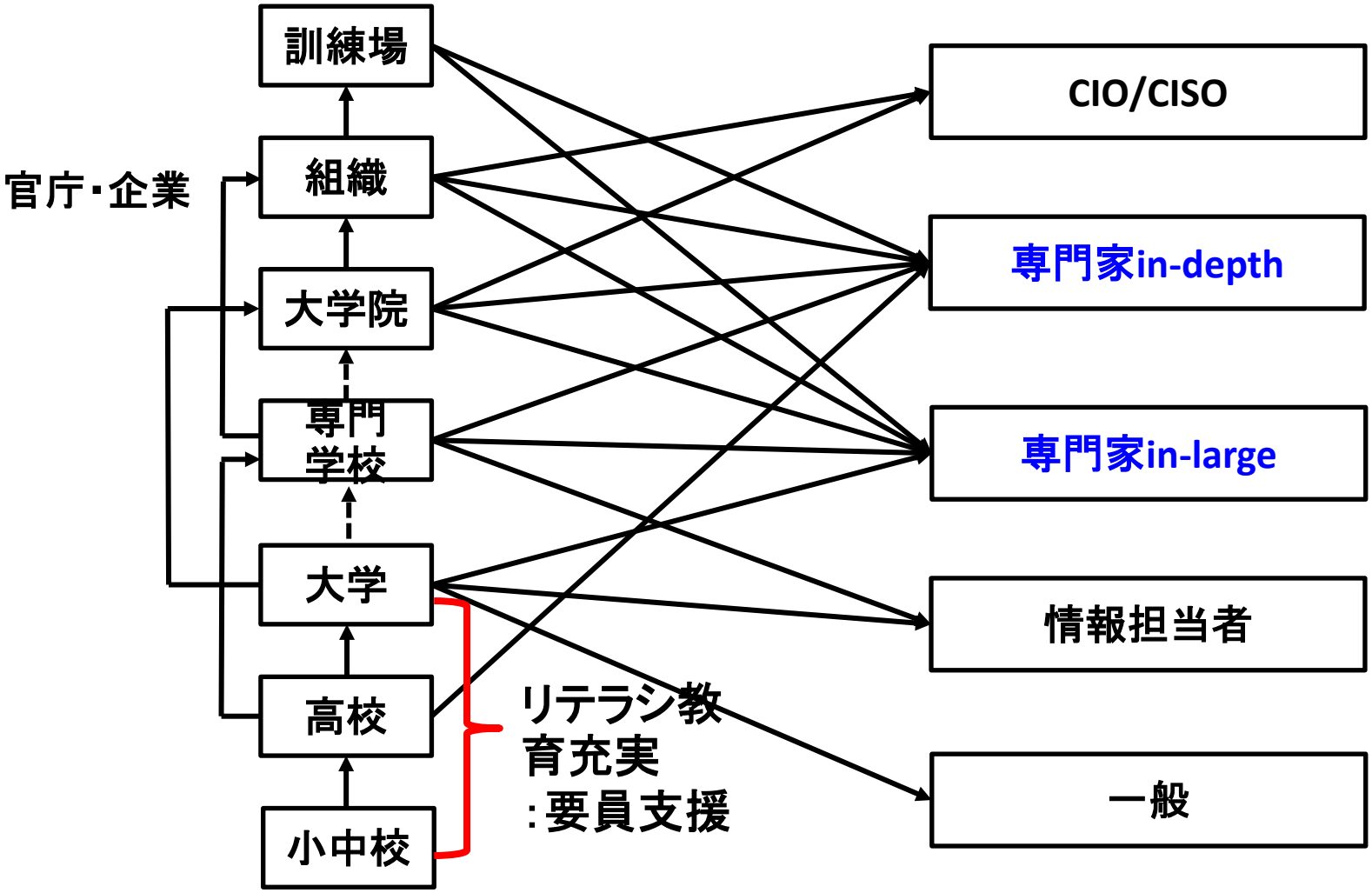
- 国内治安
- 国際対応
- 国防
- 公的機関
- 重要インフラ
- 企業
- 教育組織
- セキュリティ企業
- NPO

人材育成プログラム

- 育成人材レベルと種別に応じた中長期戦略と実行計画の策定
  - 教育組織(継続教育含む)・資格・訓練場
- 既存の取り組みの継続と強化
  - ISSsquare/ITKeys, enPiT、民間育成組織
- 強力な新施策の迅速構築と実施
  - 例:セキュリティバウチャー制度
  - 高度専門家育成→政府/民間へ

教育内容と組織

- 対象レベル
  - トップガン/サイバー犯罪専門家/一般情報専門家/一般
- 教育組織
  - 一般リテラシ、小中高リテラシ（SNS問題）、大学全体に概論
  - 大学情報分野：情報セキュリティ基礎の追加
  - 専門大学院（変化に合わせた専門教育・継続教育、プロアクティブな対応人材の提供、研究）、専門学校
  - 専門企業（現場経験で育てる場）
  - 社会人：セミナ、再教育
- 教育内容
  - 専門人材：技術（ネットワーク、システム、暗号）、フォレンジク、法制、管理法
  - 実習：侵入・攻撃、分析・対応、経験の重要性



教育の場所と対応情報セキュリティ人材

人材育成の実効化

- 進めるためのインセンティブ
  - 若い人材発掘に奨学金等公的補助
  - 企業や公的機関に情報セキュリティ担当推奨ガイドライン
  - 経営側情報担当役員にセキュリティキャリアガイドライン
  - 専門人材キャリアパスと人材市場の明示化
- 大学と企業との連携
  - 密連携の実施場構築支援
- 深い情報分析専門家
  - 若い人材に適性、また惹きつける魅力、その活用
  - CTF(旗取り合戦）などによる分野活性化と人材発掘

おわり

米議会検討中のサイバー対策法案

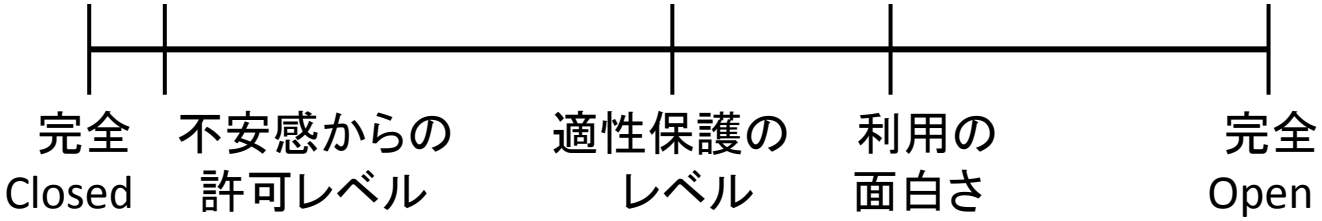
- サイバー攻撃に関する企業間の情報共有強化
- 企業から政府へのサイバー攻撃情報の提供促進
- 情報共有を巡る訴訟から企業を保護
- サイバー対策の研究開発や人材育成の支援
- 企業を対象とする自主参加のサイバー対策基準の策定促進
- サイバーセキュリティへの国民の意識を高める広報活動支援

国際サイバー攻撃

- 一般状況
  - 記念日、イベント、意見陳述などを契機に攻撃多発
  - 軍関係サイバー部隊、思想グループ、Hacktivist、一般人
- 攻撃内容
  - DDoS、Web改竄、情報窃取、金銭窃盗
  - 標的型： コンピュータシステム破壊/停止、機器破壊、サービス停止
- 対策
  - 攻撃元特定困難、システム侵入防御困難
  - マルウエア侵入後のモニターと駆除
  - 専門家の国際連携（人の繋がり）
  - デジタルフォレンジック（痕跡分析）、ネットワークフォレンジック（挙動と流出経路分析）、サイバーインテリジェンス（経験や収集事例の利用、人のネットワーク利用）
- 攻撃対応
  - モニタ・攻撃元特定と対処、国際的には攻撃元攻撃も検討中

最近のサイバー攻撃

- 2012.0 米銀行sがDDoS受けた
  - 規模通常の10-20倍、利用者アクセス不能、アラブ発
- 2012.11 Anonymousがイスラエル攻撃
  - 4400万回攻撃、軍関係が多い、1回成功、攻撃元は国内とパレスチナ自治区、平時数M回/日
- 2012.3 英 NPO Spamhaus DDoS受けた
  - Max 300Gpbs(通常50Gpbs), 誤検出組込トライ等、4月オランダ政府が容疑者逮捕、5月オランダ攻撃
- 2013.3 韓国　放送局、銀行、
  - 48,700台PCデータ破壊、9日で復旧、反撃のサイバー交戦規則やサイバー攻撃武器の準備無し、北朝鮮



個人情報の適切な保護レベル