



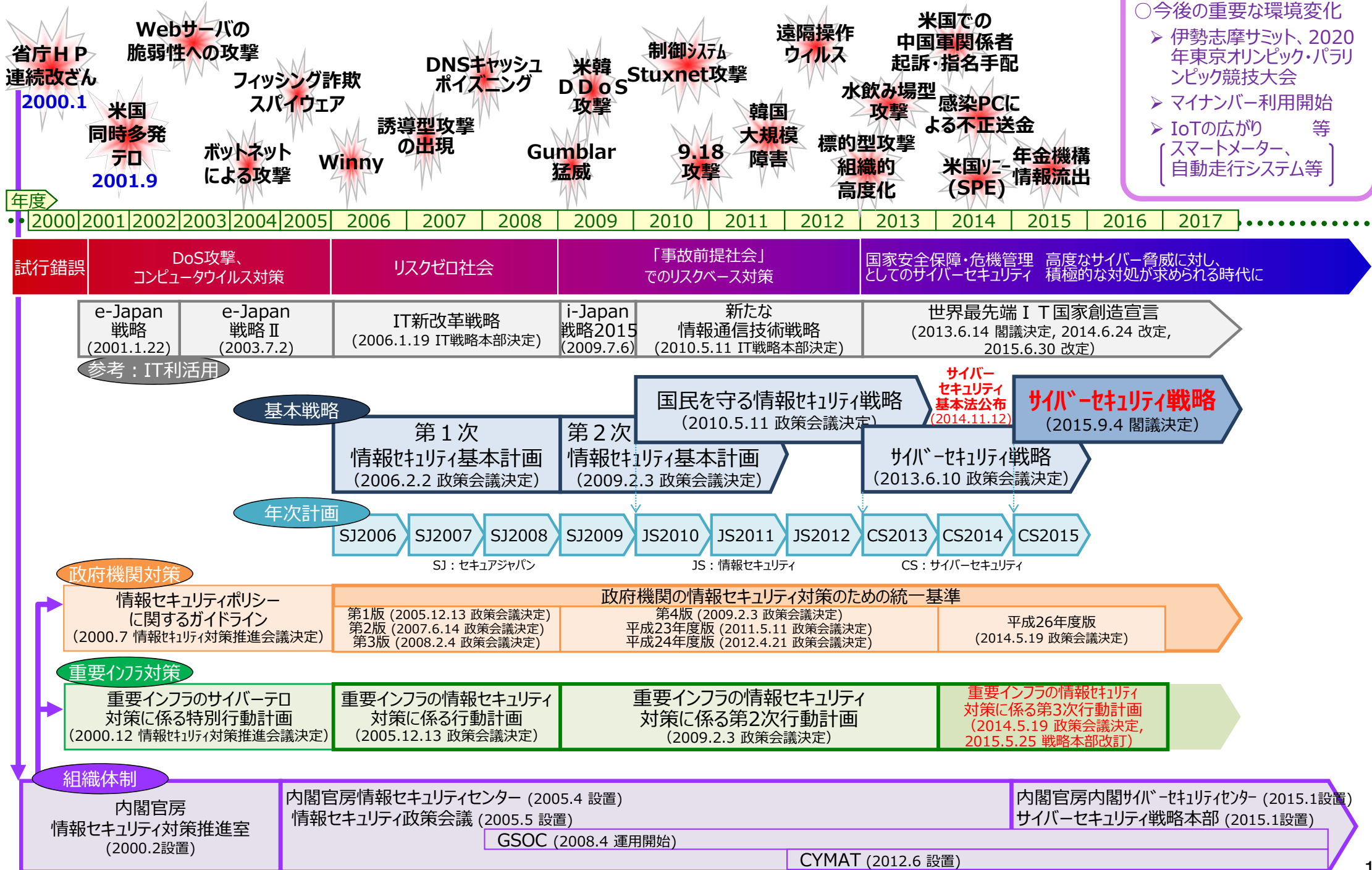
内閣サイバーセキュリティセンター
National center of Incident readiness and
Strategy for Cybersecurity

資料 4

重要インフラ等に係る サイバーセキュリティ政策の概要

2016年4月
内閣サイバーセキュリティセンター（NISC）

サイバーセキュリティ政策の経緯



我が国におけるサイバーセキュリティ政策推進体制（法施行後 H27.1.9～）

内閣

内閣総理大臣

高度情報通信ネットワーク
社会推進戦略本部
(IT総合戦略本部)

高度情報通信ネットワーク
社会の形成に関する
施策を迅速かつ重点的
に推進

緊密連携

サイバーセキュリティ戦略本部 (2015.1.9 サイバーセキュリティ基本法により設置)

本部長
副本部長
本部員

内閣官房長官
サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（IT）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣※
有識者（7名；10名以下）

※平成27年7月22日付内閣総理大臣決定により本部員に指定

閣僚が参画

遠藤 信博 日本電気株式会社代表取締役執行役員社長
小野寺 正 KDDI株式会社取締役会長
中谷 和弘 東京大学大学院法学政治学研究科教授
野原佐和子 株式会社イブシ・マーケティング研究所代表取締役社長
林 紘一郎 情報セキュリティ大学院大学教授
前田 雅英 日本大学大学院法務研究科教授
村井 純 慶應義塾大学教授

国家安全保障会議
(NSC)

我が国の安全保障
に関する重要事項を
審議

緊密連携

重要インフラ
専門調査会

研究開発戦略
専門調査会

普及啓発・人材
育成専門調査会

サイバーセキュリティ
対策推進会議
(CISO等連絡会議)

(事務局)

内閣官房 内閣サイバーセキュリティセンター
(2015.1.9 内閣官房組織令により設置)

内閣サイバーセキュリティセンター長
(内閣官房副長官補(事態対処・危機管理)が兼務)
副センター長(内閣審議官)
サイバーセキュリティ補佐官

政府機関・情報セキュリティ
横断監視・即応調整チーム
(GSOC)

情報セキュリティ
緊急支援チーム
(CYMAT)

協力

協力

<重要インフラ所管省庁>

金融庁 (金融機関)
総務省 (地方公共団体、情報通信)
厚生労働省 (医療、水道)
経済産業省 (電力、ガス、化学、
クレジット、石油)
国土交通省 (鉄道、航空、物流)

<その他関係省庁>

文部科学省 (セキュリティ教育) 等

警察庁 (サイバー犯罪・攻撃の取締り)

総務省 (通信・ネットワーク政策)

外務省 (外交・安全保障)

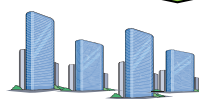
経済産業省 (情報政策)

防衛省 (国の防衛)

閣僚
本部員
5省庁



重要インフラ事業者等



政府機関 (各府省庁)



企業



個人

サイバーセキュリティをめぐる状況の変化

IT依存度の高まり

PC



多くの職場・家庭に普及し、インターネットに接続
(2014年末: PC普及率 78.0%、インターネット普及率 82.8%)
※2015年版情報通信白書(総務省)

スマートフォン



世帯保有率が6.6倍に急増
(2010年末: 9.7%→2014年末: 64.2%)
※2015年版情報通信白書(総務省)

自動車



一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの
取組みガイド(2013.8 IPA)

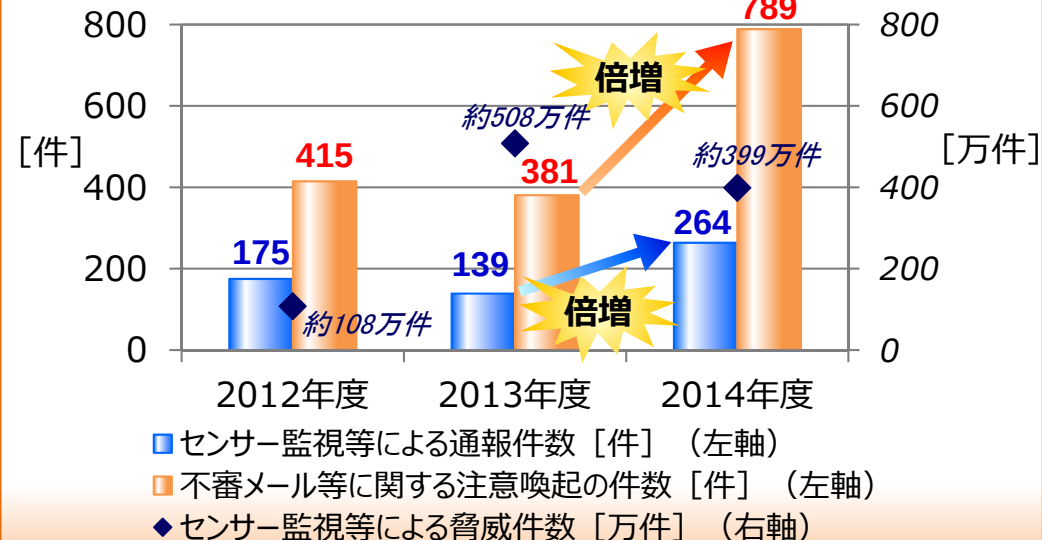
スマートメーター
(次世代電力量計)



電力会社による開発・導入の開始
[主な予定]・東京: 2020年度までに2700万台の導入完了
・関西: 2022年度までに1300万台の導入完了

サイバー攻撃の増加

【政府機関への脅威件数等】



国家関与の疑われる攻撃



韓国 (2013年4月)

重要インフラ(金融・放送等)に
対する大規模サイバー攻撃が発生。
韓国当局は北朝鮮の所業と発表。



米国 (2014年12月)

リー・ヒュー・エンターテインメント社に
対するサイバー攻撃が発生。米国
政府は北朝鮮に責任ありとし、国家
安全保障上の問題として対応。

2020年東京オリンピック・パラリンピック 競技大会へ向けた準備

- 世界の注目を集める祭典。「ダウンタイム」は許されない。
- 2012年のロンドン大会では、開催期間中、約2億件のサイバー攻撃が発生。
- 英国政府は、6年前からサイバー攻撃対策を準備。

サイバーセキュリティ基本法の概要

(※現在改正案「審議中」)

第Ⅰ章. 総則

■ 目的（第1条）

■ 定義（第2条）

⇒ 「サイバーセキュリティ」について定義

■ 基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

- ① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
- ② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築
- ③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築
- ④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
- ⑤ IT基本法の基本理念に配慮して実施
- ⑥ 国民の権利を不当に侵害しないよう留意

■ 関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、**重要社会基盤事業者（重要インフラ事業者）**、サイバー関連事業者、教育研究機関等の責務等について規定

■ 法制上の措置等（第10条）

■ 行政組織の整備等（第11条）

第Ⅱ章. サイバーセキュリティ戦略

■ サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

- ① サイバーセキュリティに関する施策の基本的な方針
- ② 国の行政機関等におけるサイバーセキュリティの確保
- ③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進
- ④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章. 基本的施策

■ 国の行政機関等におけるサイバーセキュリティの確保（第13条）

■ **重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）**

■ 民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■ 多様な主体の連携等（第16条）

■ 犯罪の取締り及び被害の拡大の防止（第17条）

■ 我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■ 産業の振興及び国際競争力の強化（第19条）

■ 研究開発の推進等（第20条）

■ 人材の確保等（第21条）

第Ⅲ章. 基本的施策（つづき）

■ 教育及び学習の振興、普及啓発等（第22条）

■ 国際協力の推進等（第23条）

第Ⅳ章. サイバーセキュリティ戦略本部

■ 設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■ 施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■ 本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■ 検討（第3条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■ IT基本法の一部改正（第4条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

サイバーセキュリティ基本法～重要インフラ関係部分

定義

クレジット分野は2014年に新規指定

重要社会基盤事業者：

国民生活及び経済活動の基盤であって、その**機能が停止し、又は低下**した場合に国民生活又は経済活動に**多大な影響を及ぼす**おそれが生ずるものに関する事業を行う者

責務

（重要社会基盤事業者の責務）

第六条 重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努めるとともに**、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

施策

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条 **国は**、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の**自主的な取組の促進**その他の**必要な施策を講ずるものとする**。

「サイバーセキュリティ戦略」について（全体構成） H27.9.4閣議決定

1 サイバー空間に係る認識

- サイバー空間は、「無限の価値を産むフロンティア」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「**接続融合情報社会（連融情報社会）**」が到来同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

3 基本原則

- ① 情報の自由な流通の確保 ② 法の支配 ③ 開放性 ④ 自律性 ⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ / ②受動から**主導**へ / ③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **安全なIoTシステムの創出**
安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

- **国民・社会を守るための取組**
事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定 及び 我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **我が国の安全の確保**
警察・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的 施策

■ 研究開発の推進

攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ 人材の育成・確保

ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、東京オリンピック・パラリンピック競技大会等に向けた対応

サイバーセキュリティ戦略における重要インフラ関連部分 1/2

5.2. 国民が安全で安心して暮らせる社会の実現

- 昨今、サイバー空間に起因して、**国民の個人情報や財産を始め、実生活に悪影響を及ぼす事例**が頻繁に報告されており、被害が深刻化
- ……**重要インフラ**や政府機関の機能やサービスは、それ自体が**国民生活・経済社会活動を支える基盤**となっており、**支障が生じると国民の安全・安心に直接的かつ重大な悪影響が生じる可能性**
- ……業務責任者(任務責任者)がシステム責任者(資産責任者)と重要インフラや政府機関の**機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証(任務保証)」**の考え方に基づく取組が必要……

サイバーセキュリティ戦略における重要インフラ関連部分(2/2)

5.2.2 重要インフラを守るための取組

- …官民が一丸となり重点的に防護していく必要…防護に当たっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を可能な限り減らすとともに、障害発生 of 早期検知と、障害の迅速な復旧を図ることが重要…
- …重要インフラ事業者及びその所管省庁は、強制基準やガイドラインなどの安全基準を定めてサイバー攻撃に対する防護を行っているが、重要インフラの中でも業法によってサービスの維持及び安全確保に係る水準が求められているものについては、昨今のサイバー空間を取り巻く環境変化を踏まえ、安全基準について不断の見直しを行っていく。
- …業法等の規定により報告対象となる一定規模以上の障害だけでなく、小規模な障害情報や予兆情報はサイバー攻撃の脅威に対抗する上で有効であるとの認識の下、関係者の共通理解として情報収集を行っているが、内閣サイバーセキュリティセンター(NISC)と所管省庁がより緊密に連携し、積極的な情報収集に取り組む…

重要インフラの情報セキュリティ対策に係る第3次行動計画

(平成26年5月 情報セキュリティ政策会議決定)

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、
自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、
IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する

重要インフラ（13分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

NISCによる
調整・連携

重要インフラ所管省庁（5省庁）

- 金融庁 [金融]
- 総務省 [情報通信、行政]
- 厚生労働省 [医療、水道]
- 経済産業省 [電力、ガス、化学、クレジット、石油]
- 国土交通省 [航空、鉄道、物流]

関係機関等

- 情報セキュリティ関係省庁 [総務省、経済産業省等]
- 事案対応省庁 [警察庁、防衛省等]
- 防災関係府省庁 [内閣府、各省庁等]
- 情報セキュリティ関係機関 [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者 [各種ベンダー等]

重要インフラの情報セキュリティに係る第3次行動計画

H26.5.19 情報セキュリティ政策会議 策定
H27.5.25 サイバーセキュリティ戦略本部改訂

安全基準等の整備・浸透



重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化



IT障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

障害対応体制の強化



官民が連携して行う演習等の実施・演習・訓練間の連携によるIT障害対応体制の総合的な強化

リスクマネジメント



重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援

防護基盤の強化



広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

1. 行動計画見直しに当たっての基本方針

- ◆ 重要インフラを標的としたサイバー攻撃の深刻化に伴う重要インフラ防護の必要性が高まっている中、「サイバーセキュリティ戦略」(平成27年9月閣議決定)等に基づき、対策強化に向けた検討課題を整理。その際、「機能保証」の考え方に基づく取組を含める。
- ◆ 本ロードマップに従い検討を進め、行動計画の見直しについて、平成29年3月末を目途に結論。早急に対処すべき事項については、行動計画の見直しを待たずに対処。

2. 考慮すべき環境変化

- (1) **I o Tの浸透に伴う制御技術と情報通信技術の相互依存性の高まり**
 - ・実空間(モノ・ヒト)とサイバー空間(情報)の物理的制約を越えた接続
 - ・サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで拡散・浸透
- (2) **面的防護に向けた情報共有等の連携体制強化の必要性等**
 - ・I o Tシステムを活用した新たなビジネスの創出や既存ビジネスの高度化・高付加価値化に伴うサプライチェーンリスクの高まり
- (3) **諸外国における重要インフラへの取組の加速化**
 - ・官民間の情報共有の枠組みの強化・推進等の取組が進展

(米国「サイバーセキュリティ法」、EU「ネットワーク及び情報セキュリティ(NIS: Network and Information Security)指令」(案))

3. 強化すべき取組の方向性

1) サイバー攻撃に対する体制強化

- **経営層における取組の強化の推進**
 - ・機能保証の考え方に立脚し自らの経営責任を全うする観点からのセキュリティ経営資源投入の推進(情報開示の在り方)
 - ・経営層のセキュリティ意識改革を促す環境の整備(インセンティブの在り方)
- **情報共有の強化**
 - ・予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化
 - ・法令に基づく義務的な報告又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し
- **内部統制の強化の推進**
 - ・自ら若しくは第三者による監査等の推進(マネジメント監査、ペネトレーションテスト等)
 - ・リスクマネジメントの推進強化
- **マイナンバー制度の運用に係るセキュリティの確保に関する取組**
- **2020年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化**

2) 重要インフラに係る防護範囲の見直し

- **情報共有範囲の拡大**
 - ・相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大
- **分野横断的な情報共有の強化**
 - ・スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のためのセプターの検討(既存セプターとの連携の在り方を含む)
- **国の安全等の確保の観点からの取組**
 - ・重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化(研究機関、大学等を含む)

3) 多様な関係者間の連携強化

- **国際連携**
 - ・海外 I S A Cとの連携(共同演習、情報共有を含む)の促進
 - ・二国間・地域間・多国間の枠組みを活用した国際連携の継続
- **人材育成**
 - ・人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援

4. 行動計画の見直しに向けた今後の検討スケジュール

- 平成28年夏期に行われる評価を踏まえ、秋頃に行動計画の見直し骨子(案)を策定
- 平成28年中に行動計画の見直し(案)を策定・公表、平成29年3月までに結論
- 上記検討は、2020年東京オリンピック・パラリンピック競技大会に係るサイバーセキュリティ確保のための施策と緊密に連携

クレジット分野における適切なセキュリティの確保のために

◆管理すべきサービスの明確化

- リスクを踏まえた管理すべきサービスの範囲の不断の見直し

◆防護目的・対象の明確化

- 防護の目的の明確化、何から何をどのように守るか
- 守り切れない場合、どこを優先させるか

◆要求事項の明確化

- 業務に関連する法令・規制要求事項
- 明示されていないが、業務に不可欠な要求事項
- 業界ルール等、組織が必要と判断する追加要求事項

◆トップのコミットメント

- 組織としてどのような方針で取り組んでいくか
- 業界全体でどのような方針で取り組んでいくか

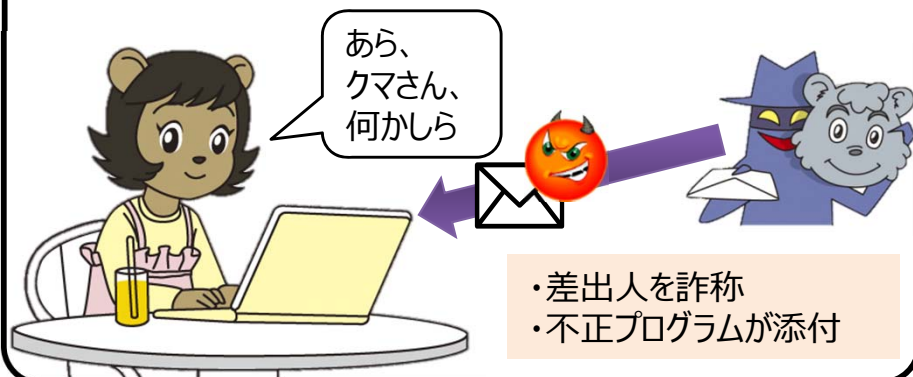
様々な標的型攻撃

(参考)

- 標的型攻撃は、初期潜入→侵入範囲→情報窃取 という流れ。
- 初期潜入段階において、端末を不正プログラムに感染させるために種々の手口が使われている

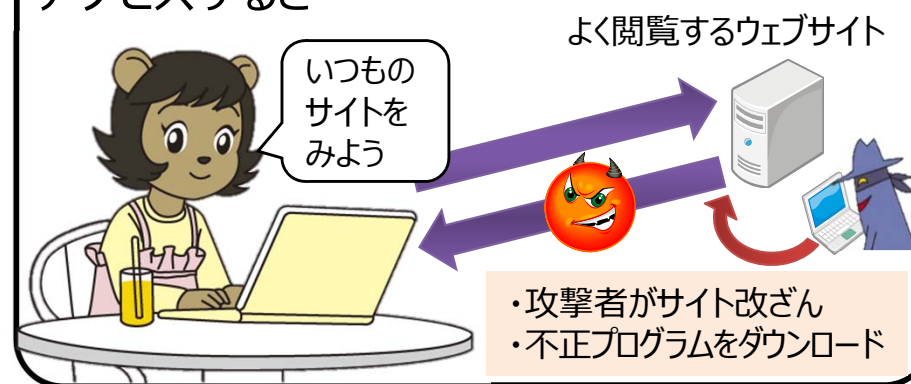
A. メール

よく知っている人からのメールだと思って添付ファイルを開いてしまうと...



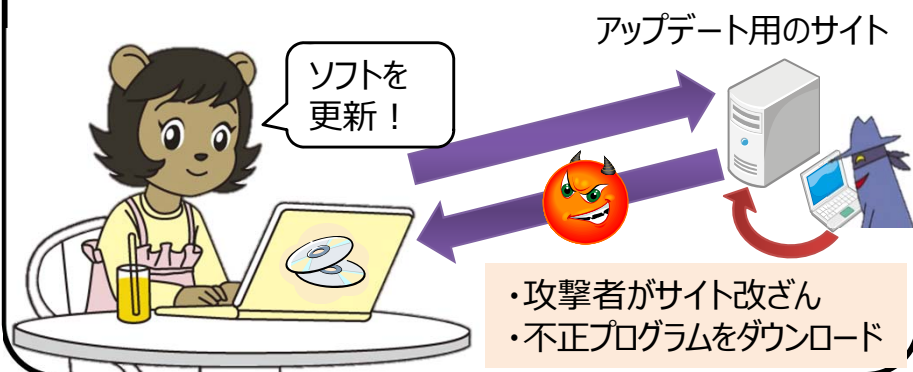
B. ウェブ閲覧（水飲み場型）

いつも閲覧しているウェブサイトアクセスすると...



C. ソフトウェアアップデートを悪用

ソフトウェアのアップデート機能を使用すると...



- 初期潜入が成功すると、遠隔操作により、システムの内部に侵入し、侵入範囲拡大
- 最終的に、重要情報の窃取やシステム破壊
- 必要な情報が得られるまで**執拗に狙う**

米国の任務保証(Mission Assurance Strategy)

(参考)

任務保証とは

任務遂行上不可欠な機能を維持するために必要な能力及びアセット(人材、装備、施設、ネットワーク、情報システム、インフラ、サプライチェーンを含む)の持続性と強靱性を確保するプロセスのこと。



構成

- 任務保証の目的・方法・手段
- 組織横断的な戦略的任務保証フレームワーク(任務保証の4つの柱)
- 戦略導入にあたって(今後の取り組み)

既存の枠組みとの関係

対テロ、重要インフラ防護、任務継続、情報保全等の既存の枠組みを活かしつつ、より包括的に重要アセットの特定とそれらに関するリスク管理を推進する。