NISC National Information Security Center

わが国の重要インフラにおける情報セキュリティ対策

平成26年10月30日

内閣官房情報セキュリティセンター
重要インフラグループ参事官
柳原 拓治

我が国における危機①
～リスクの甚大化～

NISC

機微な情報に対する巧妙な攻撃

【最近の主な事例】 氷山の一角

2011.9～	[三菱重工業、衆議院等] 標的型攻撃によるウイルス感染発覚
2012.5	[原子力安全基盤機構] 過去数か月間の情報流出の可能性確認
2013.1	[農林水産省] TPP情報流出に関するサイバー攻撃事案報道
2013.4	[宇宙航空研究開発機構] サーバに対する外部からの不正アクセス発覚
2013秋頃	[政府機関等] 特定者がウェブ閲覧により感染するゼロデイ攻撃※発覚
2014.1	[原子力研究開発機構] ウイルス感染による情報の流出の可能性発覚

【政府機関への脅威件数等】 24時間365日（約6秒に1回）

	2011年度	2012年度	2013年度
センサー監視等による脅威件数 ※※※	約66万	約108万	約508万
センサー監視等による通報件数	139	175	139
不審メールに関する注意喚起の件数	209	415	381

※「ゼロデイ攻撃」とは、ソフトウェアにおける未修正・未発表のセキュリティ上の脆弱性を悪用した攻撃

※※※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

重要インフラに対する攻撃

【重要インフラへの攻撃件数等】 危機の高まり

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡※件数	15	76	133
標的型攻撃メール等の情報提供※※件数	246	385	

<内訳>
不正アクセス、DoS攻撃 121
ウイルスへの感染 7
その他の意図的要因 5

【重要インフラ分野】 保護対象の多様化

① 情報通信 ⑥ ガス
② 金融 ⑦ 政府・行政サービス
③ 航空 ⑧ 医療
④ 鉄道 ⑨ 水道
⑤ 電力 ⑩ 物流

○ 化学
○ クレジット
○ 石油
※※※

【参考】米国の状況 電力、水道及び交通分野等の重要インフラに対する攻撃が、2011年以降、17倍に増加（2013年6月デンプシー統合参謀本部議長講演）

※ NISCへの情報連絡件数のうちサイバー攻撃（意図的要因）に関するもの。 ※※重要インフラ機器製造、電力、ガス、化学、石油の5業界からIPAへ情報提供されたもの
※※※ 「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」（2014年5月19日情報セキュリティ政策会議決定）において追加

我が国における危機②
～リスクの拡散・グローバル化～

NISC

攻撃の対象範囲の拡散

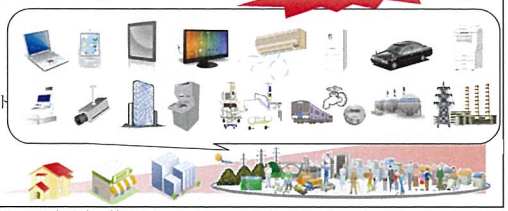
【スマートフォンの普及等】 国民1人1人へ

スマートフォン
世帯保有率が5倍に急増※
（2010年末：約10%→2012年末：約50%）
携帯端末を標的とする不正サイトが20倍に急増※※
（2011年度末：約3千→2013年度末：約5万7千）

スマートカー
1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※※※

スマートメーター（次世代電力量計）
各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

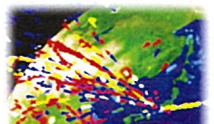
【我が国社会全体への浸透】 いつでもどこでも何でも



※ 総務省「平成25年版情報通信白書」
※※ トレンドマイクロ㈱調べ（2014年4月）
※※※ （独）情報処理推進機構（IPA）「自動車の情報セキュリティへの取組みガイド」（2013年8月）
※※※※ 経済産業省「第14回スマートメーター制度検討会」資料（2014年3月）

世界中からの多様な主体による攻撃

【海外からの我が国への攻撃状況※】 グローバル化



国名（国コード）	ホスト数	割合
中国(CN)	26,750	41%
韓国(KR)	4,716	7%
日本(JP)	3,675	6%
アメリカ(US)	3,352	5%
台湾(TW)	2,867	4%
ロシア連邦(RU)	2,088	3%
ブラジル(BR)	1,903	3%
香港(HK)	1,665	3%
インド(IN)	1,586	2%

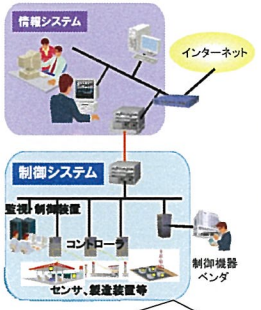
【最近の主な事例】 国家関与の可能性

2011.3	[韓国] 政府機関等の40のウェブサーバへのDDoS攻撃発生 → 日本の家庭用PCが踏み台となり攻撃指令サーバ化
2013.3	[韓国] 重要インフラに対する大規模サイバー攻撃発生 → 使用された不正プログラムが我が国でも同時期に確認
（参考）	
2013.5	[米国] 国家機密や企業機密を窃取する標的型攻撃について、外国政府・軍の関与の可能性を政府が指摘※※

※ （独）情報通信研究機構（NICT）のインシデント分析システム「nicter（ニクター）」より（右図は「国別ホスト数Top10」2014年4月7日現在）
※※ ホワイトハウス「営業秘密侵害を低減するための米国政府戦略」（2013年2月）及び国防総省「年次報告書」（2013年5月）

制御システムの普及

NISC



従来

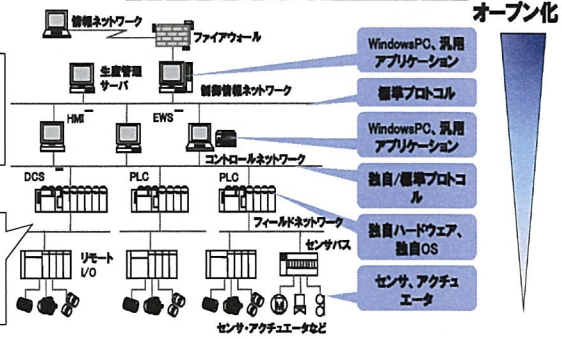
制御システムは事業者毎に固有の仕様部分が多く、詳細な内部仕様等を把握できない限り、外部からの攻撃は難しいものであった。

最近の状況

○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
○ 外部ネットワークにも接続されるようになっている。
○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。

○ 生産の自動化や、フィードバック制御による入力値の自動制御等、様々な用途で工数の軽減や正確性の向上を目的に利用。
○ 最近は、一般的な情報システムが接続するオフィスネットワークから、制御情報系ネットワーク、制御ネットワークを介して、制御システムのコントローラやセンサーまでを間接的に接続するような構成が多い。

オープン化が進む制御システムの構成

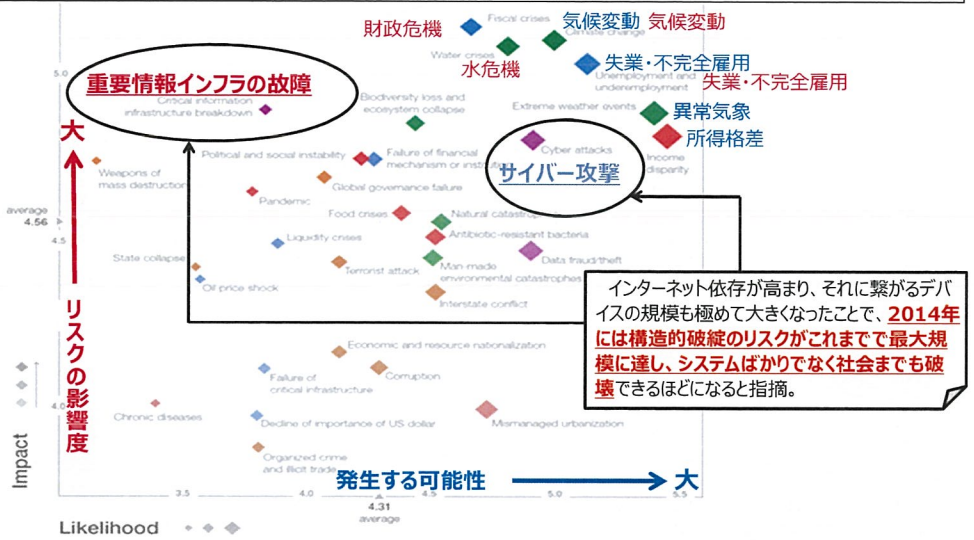


○ アプリケーション等が動作する上層のレイヤではWindowsのパソコン等のクライアント端末や汎用アプリケーション、標準プロトコルを利用。
○ 実際の制御に関わる下層部分は独自のプロトコルやハードウェア、OSが利用される割合が高く、固有の仕様により構成。
○ オープン化が上層部から徐々に進行。

【出典：独立行政法人情報処理推進機構「制御システムセキュリティ国際標準の現状と日本の取組み」（2011年11月18日）http://www.ipa.go.jp/files/000025094.pdf】

世界が直面するグローバルリスク
～一層深刻な状況へ～

本年に入り、世界経済フォーラム（WEF）は、**今後10年間で全世界及び全産業界に重大な悪影響を及ぼす可能性が高いリスク**として、**サイバー攻撃及び重要情報インフラの故障**を位置づけ。



備考：全世界及び全産業界に対して重大な悪影響を及ぼす可能性のあるものとして抽出した31のリスクに関する今後10年間の展望について、世界各地の700名以上の専門家に対する調査結果をとりまとめたもの。「1」は「発生する可能性がないもの」又は「影響がないと思われるもの」、「7」は「大いに発生する可能性があるもの」、又は「甚大かつ破壊的な影響があると思われるもの」を示している。

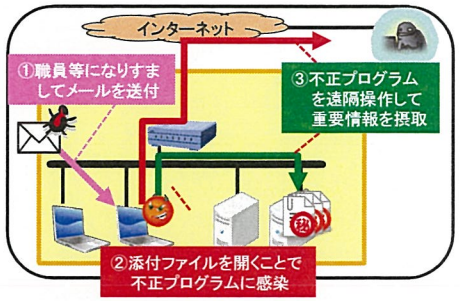
＜出典：WEF「グローバルリスク報告書2014年版」(2014年1月16日)＞ 4

標的型攻撃の例（メールによる攻撃）

脅威の概要

- 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

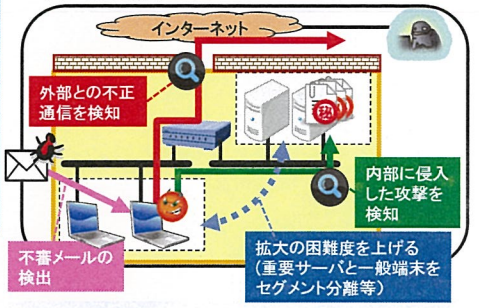
標的型メール攻撃のイメージ



主な対策

- 不審なメールを検出する仕組みの整備、対応能力を向上する(SPFの検証、教育・訓練、等)。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

対策の概要(例)



5

標的型メールの特徴

①差　出　人：情報 太郎 [johou.taro@cas-go.jp]
　宛　　先：二鋤 次郎
②件　　名：【重要】放射線量の状況
③添付ファイル：放射線量.zip

④関係各位

いつもお世話になっております。内閣官房の○○○○です。現在の放射線量についてまとめました。添付を確認ください。
また、添付ファイルと併せて、以下のURLもご確認ください

⑤http://www3.cas.go.jp/mapserch/⇒ 表示は偽装できます！

⇩ クリックすると

http://10.243.23.11/詐欺/

①差出人のアドレスを確認
@より右側が省庁ドメイン(.go.jp)でない

②件名で開封を急がせる
「重要」「緊急」などを付加

③添付ファイルの確認
アイコンを文書のように偽装
・.exe等はウィルスの可能性
放射線量.doc.exe

④メール本文は本物のコピー
・発信者に送信したかを確認

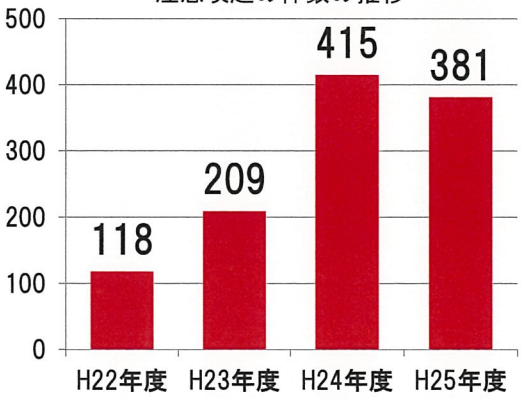
⑤リンク先表示
全く別のアドレスに偽装可能

6

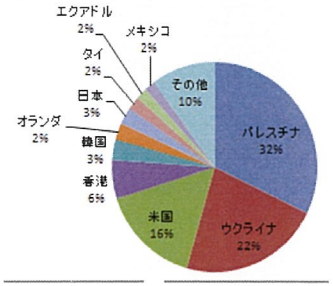
増加する標的型メール攻撃

○機密情報などの窃取を目的としたサイバー攻撃
○年々増加し、手口も巧妙化（組織的な攻撃の可能性）
○感染後の通信の接続先は、ほとんどが海外。

政府機関等への標的型メールに関する注意喚起の件数の推移



H25年中の標的型メール攻撃に使用された不正プログラム等の接続先



出典：警察庁（H26年2月）

7

標的型メール攻撃に対する教育訓練（平成25年度）

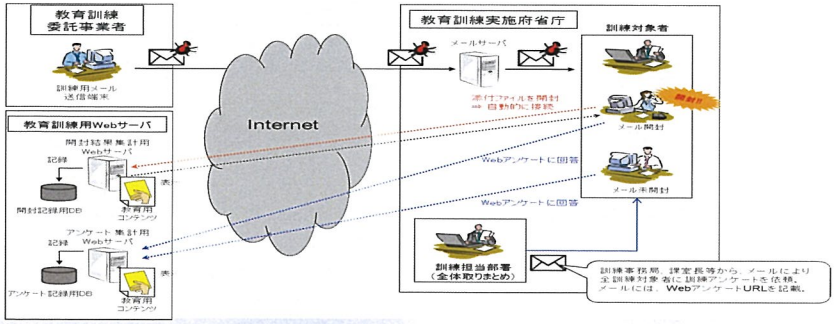
【目　　的】 標的型メール攻撃に関する教育・意識啓発のため、標的型メールを模擬メールを通じて“ヒヤリハット”を経験することで注意を深め、同攻撃に対し適切な対処を身につけることを目的。

【訓練概要】 標的型メール攻撃を模擬した訓練メールを2回職員に送付（加えて、希望府省庁にはやりとり型の訓練メールを送付）し、職員が不注意に開封するなどした場合に訓練用に設けたWebサイトに誘導。職員の不審メールへの対応状況を把握及びWeb教育コンテンツによる事後教育を実施。

【訓練対象者】　18府省庁　約18万人の職員（昨年は19府省庁　約12万人）

【訓練実施期間】 8月～12月の5カ月間を設定

【訓練結果】第一回目　１０．１％　第二回目　１６．３％　やり取り型訓練　１９．２％



標的型攻撃の例（水飲み場型攻撃）

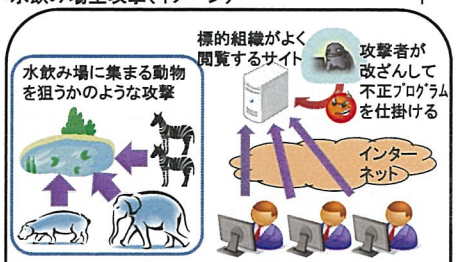
脅威の概要

- 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ブラウザの未知の脆弱性を悪用した攻撃（ゼロデイ攻撃）の場合もあり、未然防止は困難。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

主な対策

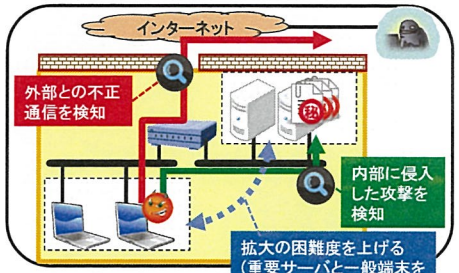
- 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
- 内部対策としては、以下が挙げられる。
  - 内部に侵入した攻撃を早期検知して対処
  - 侵入範囲の拡大の困難度を上げる
  - 外部との不正通信を検知して対処

水飲み場型攻撃（イメージ）

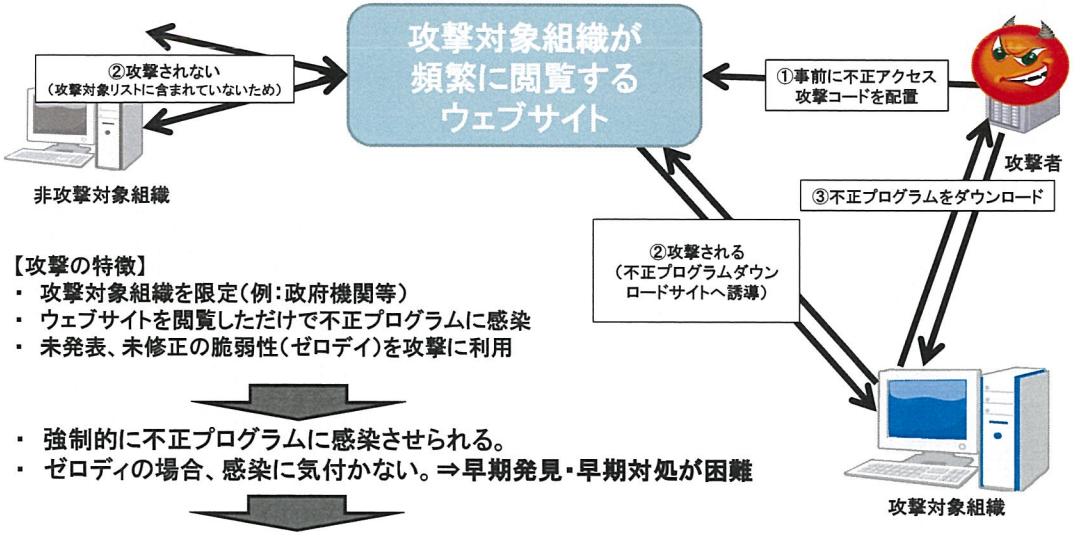


標的以外の組織が閲覧しても攻撃が行われない場合もあるため、発見されづらい傾向にある。

対策の概要（例）



水飲み場攻撃による特定の攻撃対象への攻撃



【攻撃の特徴】
- 攻撃対象組織を限定（例：政府機関等）
- ウェブサイトを閲覧しただけで不正プログラムに感染
- 未発表、未修正の脆弱性（ゼロデイ）を攻撃に利用

- 強制的に不正プログラムに感染させられる。
- ゼロディの場合、感染に気付かない。⇒**早期発見・早期対処が困難**

- 従来のセキュリティ対策に加え、定期的なネットワーク監視がより重要。
- 関係機関間の情報共有・相互連携が極めて重要。

標的型攻撃の例（ソフトウェアの更新プログラムを悪用した攻撃）

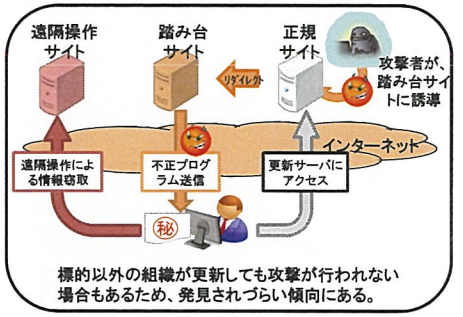
脅威の概要

- 広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行った端末を不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

必要な対策

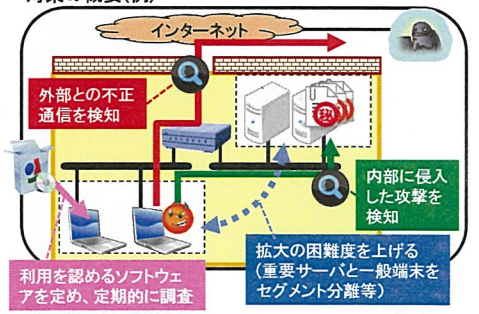
- 端末で利用を認めるソフトウェアを定め、利用されているソフトウェアの状態を定期的に調査する。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

ソフトウェアの更新プログラムを悪用した攻撃（イメージ）



標的以外の組織が更新しても攻撃が行われない場合もあるため、発見されづらい傾向にある。

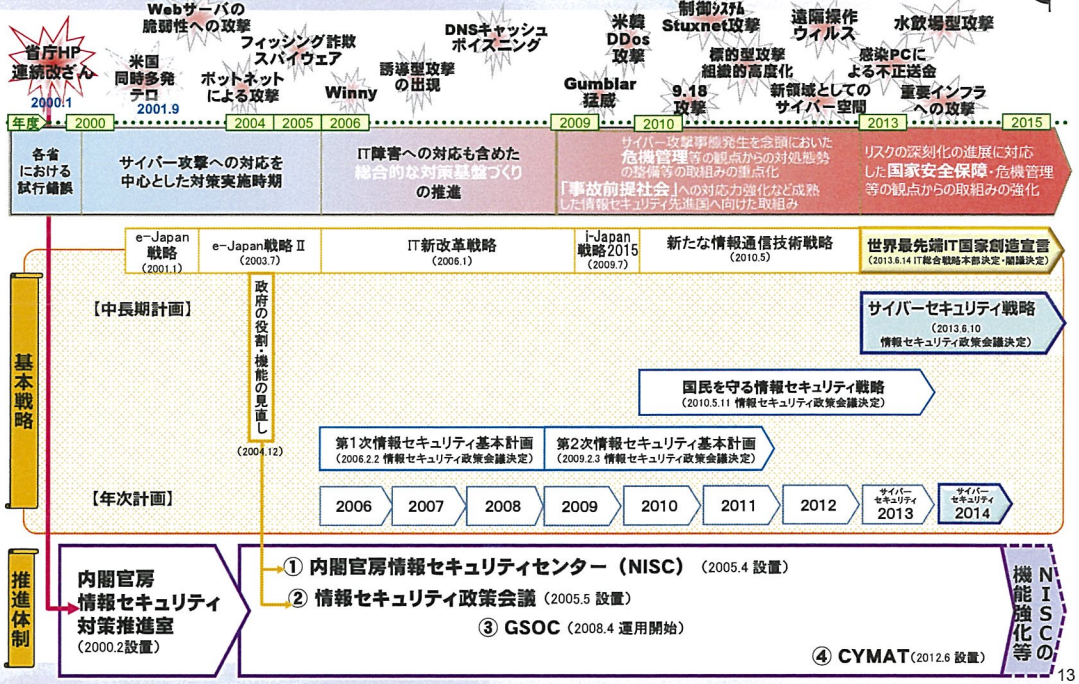
対策の概要（例）



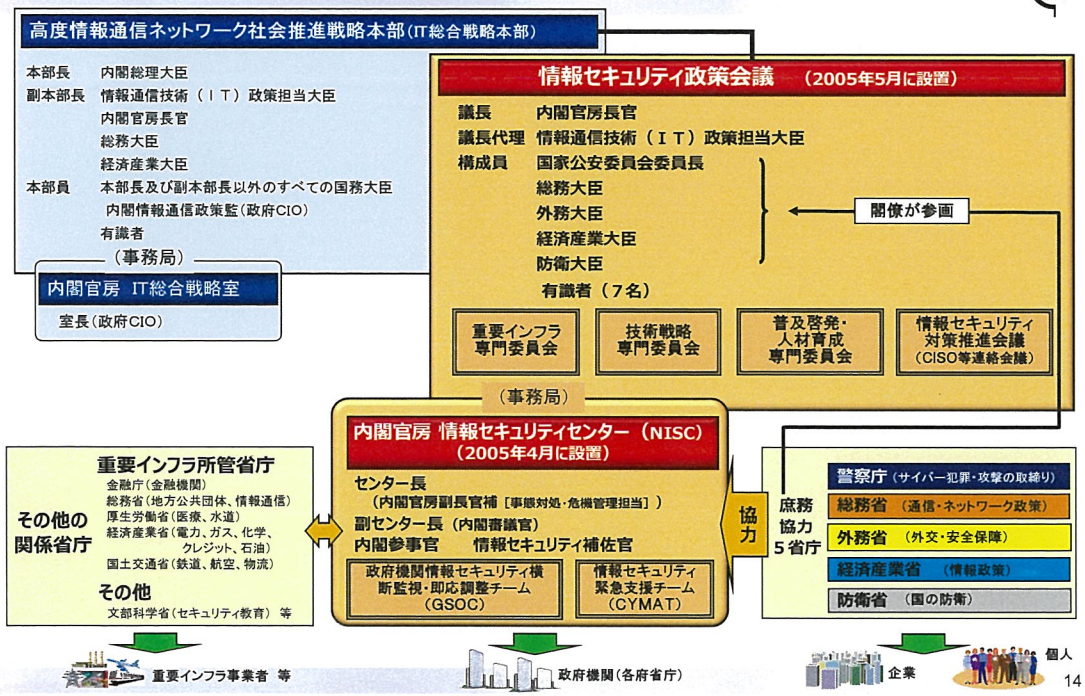
NISC National Information Security Center

我が国の情報セキュリティ戦略と推進体制

我が国における基本戦略・推進体制の推移



我が国における推進体制



サイバーセキュリティ戦略の概要

環境の変化
サイバー空間と実空間の融合・一体化［普及・高度化、更なる進展、グローバルな拡大・浸透］ ▶ サイバー空間を取り巻くリスクの深刻化［甚大化、拡散、グローバル］

目指す社会像
～「サイバーセキュリティ立国」の実現～
国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、
「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、
サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現

基本的考え方
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

取組分野

1.「強靭な」サイバー空間
サイバー空間の防御力・回復力の強化
①政府機関等対策
②重要インフラ等対策
③企業・研究機関等対策
④サイバー空間の衛生
⑤サイバー空間の犯罪対策
⑥サイバー空間の防衛

2.「活力ある」サイバー空間
サイバー空間の創造力・知識力の強化
①産業活性化
②研究開発
③人材育成
④リテラシー向上

3.「世界を率先する」サイバー空間
サイバー空間の貢献力・展開力の強化
①外交
②国際展開
③国際連携

推進体制等 ＮＩＳＣの機能強化 等

NISC National Information Security Center

重要インフラの情報セキュリティ対策に係る第3次行動計画の概要

第3次行動計画の主なポイント

➢ 第2次行動計画の施策群の基本的な骨格の維持
➢ 必要に応じた個別施策とその実施体制等の見直しによる当該施策の修正・補強

第３次行動計画における施策群	第２次行動計画からの補強・改善のポイント
1. 安全基準等の整備及び浸透	○他施策の結果を指針・対策編に反映するプロセスの明示 ○指針による**成長モデル等の訴求**及び対策の実情の調査
2. 情報共有体制の強化	○新たな関係主体を含めた情報共有体制における各関係主体の位置付けの見直し及び関係主体間の関係の再整理 ○サイバー攻撃関係情報の増加を踏まえた**共有すべき情報（脅威の類型等）の見直し** ○平時における対応を念頭に置いた**大規模IT障害対応時の事案対処体制の明確化**
3. 障害対応体制の強化	○**重要インフラ関係の演習・訓練の全体像を把握**した上でIT障害対応体制の総合的な強化 ○新たな関係主体との連携を念頭に置いた横断的演習の質的改善
4. リスクマネジメント	○環境変化等に応じて生じる複数分野において**大きな影響を生じ得るリスク源**、将来的に**多大な影響が予想される環境変化**についての**中長期的な調査**の実施 ○重要インフラ事業者等が自らの状況を正しく認識し、活動目標を主体的に定めるに当たって必要となる**リスクマネジネントの訴求**
5. 防護基盤の強化	○広報公聴、国際連携に加え、関連する**国際標準・規格**、**参照すべき規程類**の整理、活用方法の提示を追加

第3次行動計画の基本的考え方・要点

行動計画-II章（p11）

NISC

基本的考え方

●「重要インフラ防護」の目的

- **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。**

●「基本的な考え方」

情報セキュリティ対策は、**一義的には重要インフラ事業者等が自らの責任において実施**するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- **政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。**
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、**他の関係主体との連携をも充実させる。**

要　点

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

●各関係主体の在り方

- **自らの状況を正しく認識し、活動目標を主体的に策定**するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、**相互に自主的に協力**する。
- IT障害の規模に応じて、情報に基づく対応の5W1Hを理解しており、IT障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

●重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とする**リスク源の認識**。
- 上記のリスク源の評価及びそれに基づく**優先順位を含む方針の策定**。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営**資源の継続的な確保**。
- システムの運用状況の把握等を通じた当該方針の**実行の有無の検証**。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の**検証及び改善策の有無の検証**。

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

（2014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
- 事案対処省庁
- 防災関係府省庁
- 情報セキュリティ関係機関
- サイバー空間関連事業者

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

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

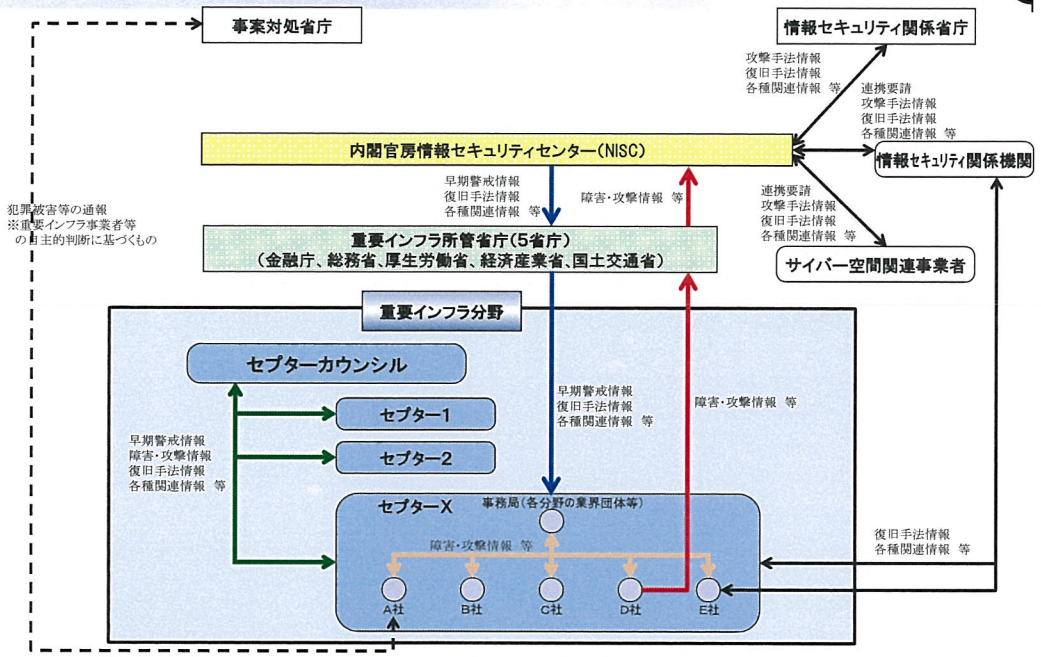
リスクマネジメント

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

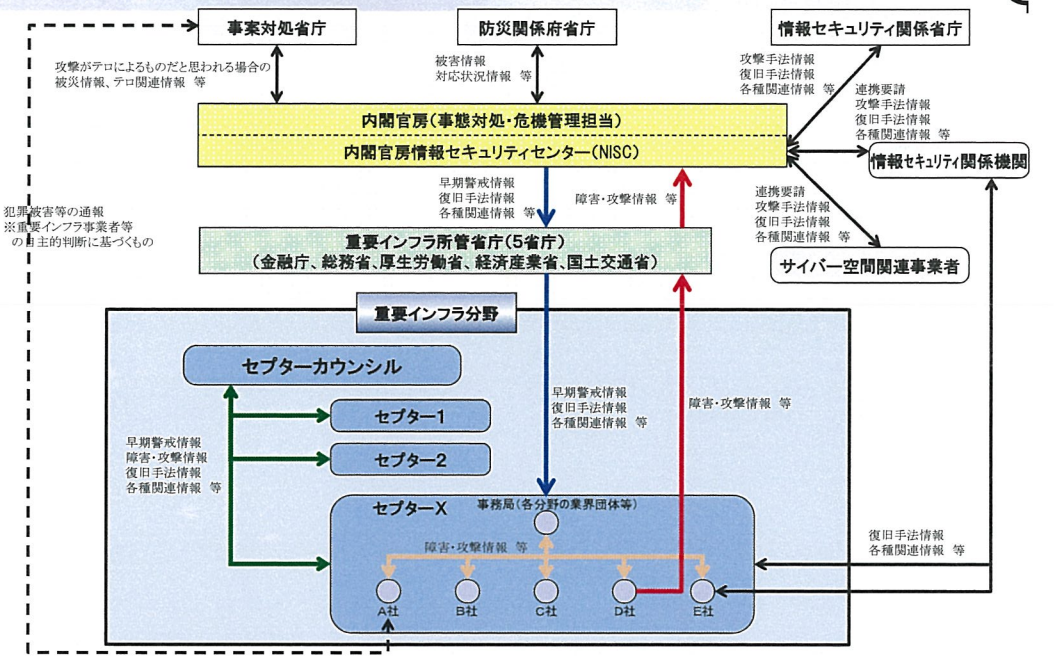
防護基盤の強化

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

重要インフラ分野における情報共有体制（平時）



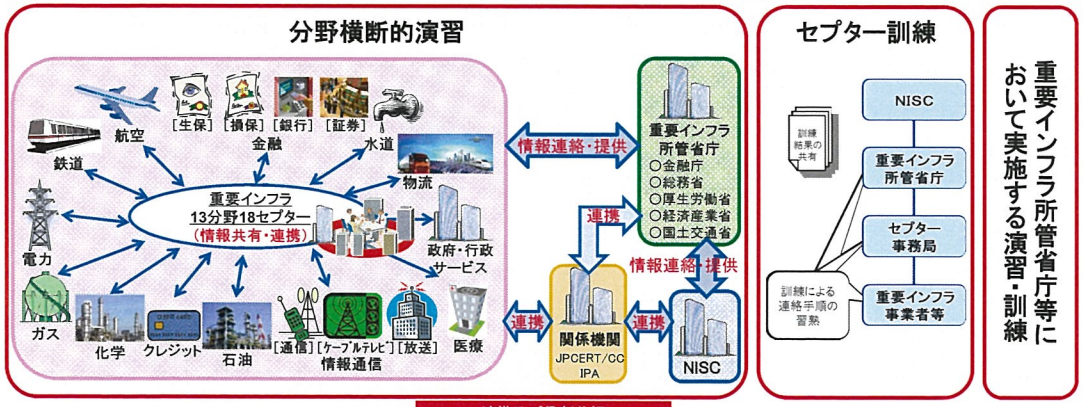
重要インフラ分野における情報共有体制（大規模IT障害対応時）



障害対応体制の強化（分野横断的演習等）について

目 的　第3次行動計画における施策の一つとして、これまでの分野横断的演習をベースに、IT障害対応に関する能力向上及び検証を目的とする他の演習・訓練との連携を強化することにより、重要インフラ全体の防護能力の維持・向上を図る。

概 要　具体的には、従来個別に実施していた分野横断的演習、セプター訓練、安全基準等の整備及び浸透、情報共有体制の強化の各施策を、重要インフラ事業者のIT障害対応体制の強化を目的として、連携しつつ実施するものとする。
　各々の事業者で構築し運用されている平時からの情報連絡体制やインシデント対応が実際に十全に機能するかどうかを確認することにより、分野横断的演習において、IT障害対応体制の実効性を確認し、その結果を障害対応体制の基礎となる安全基準等に反映させる等して、PDCAサイクルによる継続的な改善を促すものである。



分野横断的演習の様子

事務局からの状況付与（各種障害状況、攻撃状況等）に従い、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”等を用いて、他プレイヤーと情報共有しつつ発生した事象への対応を行う。
また演習後の意見交換会において、演習で得られた気づきを参加者間で共有する。

［演習当日のタイムスケジュール］


演習で使用する各種ツール(メール、掲示板等)の試使用、ホワイトボード書込み準備、通信確認などを事前に行う。


演習参加者全員が集合し、演習における各事業者の対応内容の紹介や他分野事業者等への質問などの意見交換を行い、更なる気づきを得る。


演習参加者全員が集合し、演習開会式の後、演習に関する留意事項等について説明。

［演習事務局、関係機関等］


・演習事務局は、各種障害状況、攻撃状況等を“メール”で付与する。
・関係機関は、“メール”又は、“掲示板(仮想HP)”でシナリオに則した関連情報の提供と共に、プレイヤー(事業者等)からの問合せ対応等もおこなう。

［事業者等、セプター］

［NISC、所管省庁］

［ｾﾌﾟﾀｰｶｳﾝｼﾙ事務局］

演習参加組織毎に個室に分散し、演習事務局から与えられる状況付与(各種障害状況、攻撃状況等を“メール”で送信)や、関係機関から提供される情報(メールもしくは、掲示板[仮想HP])に基づき、プレイヤーは、“メール”、“電話”、“掲示板(仮想HP)”、“ホワイトボード”等を用いて、他プレイヤーと情報共有しつつ発生した事象への対応を行う。

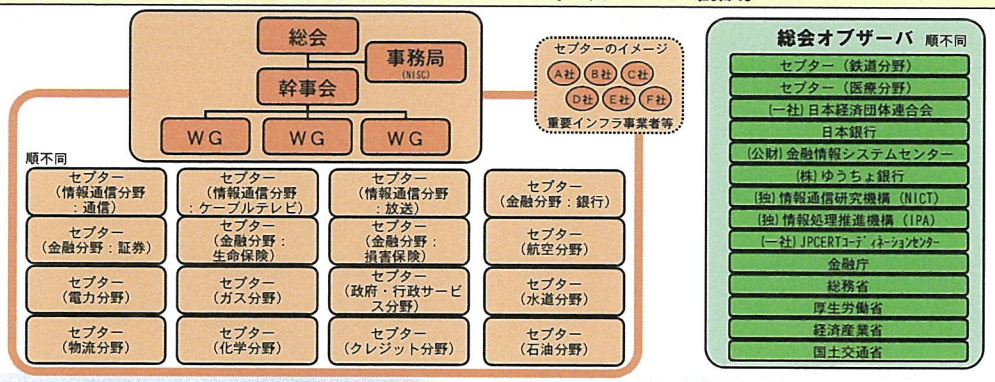
セプター及びセプターカウンシル

セプター（CEPTOAR） Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- IT障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、2009年2月26日に創設。



水道関係のシステム障害事例

日付	件名	概要
2000 年1 月	上下水処理場の制御システムの不正操作（オーストラリア）	システム開発の請負を行っていた社員が、システム開発会社を辞め請負い元に雇用を願い出たが拒否された事を恨んで制御システムに不正アクセスを行った事案。 アラームの無効化、通信妨害、ポンプの起動停止によって未処理汚水のオーバーフローと放流を引き起こし、2000 年1 月から4 月23 日迄の間に、100 万リットル近くの未処理汚水が周辺に放流されたと見られている。
2000 年	上水道システムへのハッカーの侵入（アメリカ）	AmericanWater ISAC が、水道事業者のSCADA システムにハッカーが侵入したとの報告を行った。
2006 年8 月	貯水システムの破壊（南アフリカ）	南アフリカのTshwane にある貯水池のSCADA システムが破壊され、一部地域で11 日間水道水を得ることができない状況となった。
2007 年1 月	配水システムの通信障害（アメリカ）	分散型SCADA システムで通信障害が発生し、フォートワースの一部で水道水の供給が8 時間にわたり停止した。障害により、ポンプと貯水タンクの全てのコントロールが失われた。

ICS-CERTによる分野別インシデント件数

Sector	FY-11	FY-12	FY-13	Cumulative
Chemical Sector	0	4	0	4
Commercial Facilities Sector	10	2	0	12
Communications Sector	1	0	2	3
Critical Manufacturing Sector	2	1	0	3
Dams Sector	0	0	0	0
Defense Industrial Base Sector	0	12	1	13
Emergency Services Sector	2	3	0	5
Energy Sector	11	7	18	27
Financial Services Sector	1	6	0	7
Food and Agricultural Sector	5	0	0	5
Government Facilities Sector	5	3	2	10
Healthcare and Public Health Sector	6	1	5	12
Information Technology Sector	3	5	2	10
Nuclear Reactors, Materials, and Waste Sector	2	8	8	18
Transportation Systems Sector	7	10	10	27
Water and Wastewater Systems Sector	21	25	24	70
Totals	76	87	72	235
Number of Sectors Assessed	13/16	13/16	9/16	15/16

出展：ICS-CERT, " ICS-CERT Year in Review"

NISC National Information Security Center

【参考】
重要インフラ事業者等におけるIT障害事例

事例1（認証ID・パスワードの外部漏えい）　1／4

NISC

【概　要】

- 事業者が管理する会員制サイトのサーバに対する不正アクセスにより、当該サイトへログインするための認証ＩＤと暗号化されたパスワードが外部に漏えいした。
- 監視強化中に再び不正アクセスを検知したため、関連する全システムの稼働を停止するとともに当該会員制サイトのサービス提供を停止。サーバを再構築したうえでサービスを再開した。

＜１回目の不正アクセス＞

当該サーバで利用しているミドルウェアにおける脆弱性について、情報セキュリティ関係機関が注意喚起を実施。

それを受けた当該事業者は、パッチの適用について検討を開始するとともに、暫定的なセキュリティ対策を実施したうえで、当該対策を実施するまでの間に不正アクセス等がなかったかについてログ等の確認作業を実施。

確認作業の結果、不正アクセスにより認証ＩＤと暗号化されたパスワードが収集された痕跡を確認。

＜２回目の不正アクセス＞

数日後、セキュリティ監視を強化しているなかで、新たな不正アクセスを検知。

当該不正アクセスは、１回目の不正アクセス時に設置されたバックドアプログラムに起因する不正アクセスと判明。

関連する全てのシステムの稼働を直ちに停止させ、新たな情報漏えいを未然に防止。

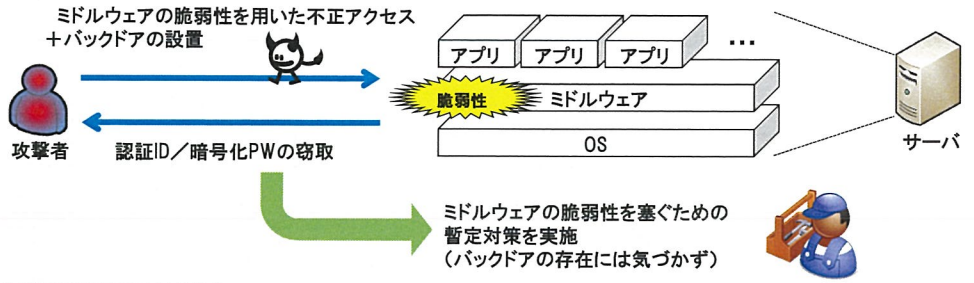
その後、サーバを再構築（当該ミドルウェアのパッチは適用済）し、新たなセキュリティ監視装置（WAF）を導入したうえでサービスを再開。

事例1（認証ID・パスワードの外部漏えい）　2／4

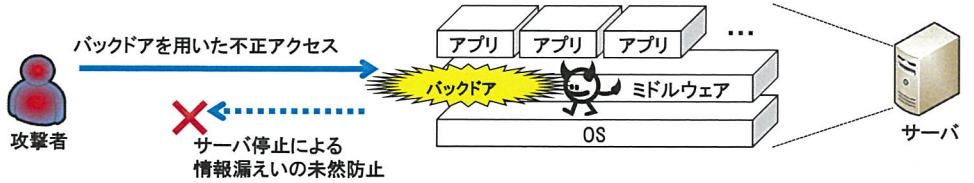
NISC

【事象のイメージ】

＜１回目の不正アクセス＞



＜２回目の不正アクセス＞



事例1（認証ID・パスワードの外部漏えい）　3／4

NISC

【原　因】

＜１回目の不正アクセス＞

- **当該サーバで利用しているミドルウェアにおける脆弱性を悪用した不正アクセスであったが、開発元が当該脆弱性のパッチを公開し、情報セキュリティ関係機関が注意喚起を行うまでの間に攻撃が発生した。**
- **脆弱性に対するパッチについて、当該ミドルウェア上で動作する各種アプリケーションの動作を確認する必要があるため、直ちにパッチを適用できない状況であった。**

＜２回目の不正アクセス＞

- **１回目の不正アクセスの際に、サーバ上の、通常では発見しづらい箇所にバックドアプログラムが設置されていた。**

事例1（認証ID・パスワードの外部漏えい）　4／4

NISC

【再発防止】

- **高度な攻撃を検知・自動ブロックするためのセキュリティ監視装置を導入。**
- **ユーザに対し、認証パスワードの再設定の必要性を周知。**
- **社内のシステムを洗い出し、脆弱性対応を一元化できる仕組みを導入。**
- **脆弱性の重要度に対する対応目安日数を設定し、対応状況をシステムで管理。**
- **情報セキュリティ事案に対する全社的な緊急対応体制※を新たに整備し、その体制に基づく訓練を実施。**

※ IT障害発生時に、社内の対策本部を立ち上げる基準や手順等

【得られた気づき・教訓】

- **パッチ適用など根本対処が直ちにできない場合は、不正アクセスの監視強化などの暫定対処を行う。**
- **脆弱性への対応を迅速に行うために、平時からシステムで利用されているソフトウェアを把握する。**
- **脆弱性情報を重要度に応じて、その対応状況を含めて管理し組織内で迅速に情報共有を行う。**
- **情報セキュリティ事案に対する緊急対応体制を平時から準備し、その対応を訓練する。**
- **不正アクセスされた場合は、情報漏えいの可能性だけでなく、2次被害としてバックドアプログラムの設置の可能性を想定し、隠しファイルの確認を含めた対応を行う。**

事例2（複数Webサイトの改ざん）　1／4

NISC

【概　要】

- 本事業者は複数のWebサイトを有しており、その一部はIT担当部署以外の担当部署が管理をしている。
- ある担当部署が管理する一部のWebサイトに対する不正アクセスにより、当該Webサイトが書き替えられ外部のWebサイトへの不正な誘導（リダイレクト）が発生。
- さらに、上記のインシデント対応中に別の担当部署が管理するWebサイトに対しても不正アクセスにより、当該Webサイトが書き替えられるインシデントが発生した。

＜１件目のインシデント案件＞

事業者の職員が利用している端末に導入されているウィルス対策ソフトがウィルスを検知。ウィルスについて調査したところ、IT担当部署以外の担当部署で管理しているWebサイトにアクセスしたことによるものと特定。

報道発表を行うとともに、当該Webサイトを閉鎖し、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

その後、コンテンツの見直しを行い、メインのWebサイトに統合済。

＜２件目のインシデント案件＞

1件目のインシデント案件と同じ週に、別の担当部署が管理するWebサイトの一部を閲覧出来ない事象を職員が発見。当該Webサイトの保守業者に連絡を取り調査を行ったが、ウィルス対策ソフトでは検知されず、原因の特定に至らなかった。

しかし、不正アクセスによる改ざんを疑い担当部署の判断で当該Webサイトを閉鎖。ウィルス対策ベンダに調査を依頼したところ新種のウィルスであり、 Webサイトへの不正アクセスによりウィルスを混入されていたことが確認できたため、報道発表を行うとともに、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

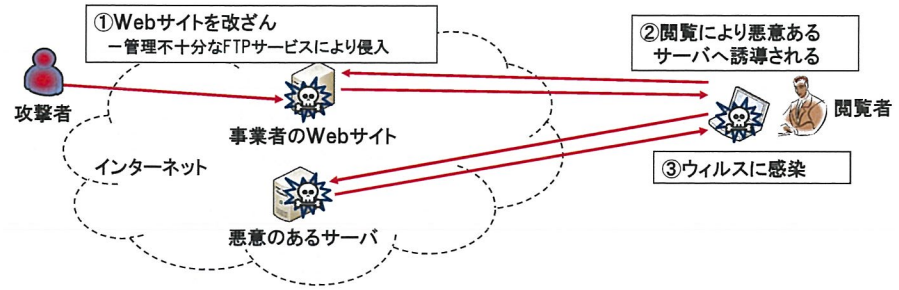
その後、Webサイトの脆弱性調査を行い、多数の脆弱性を確認し、対応後にWebサイトを再開。

事例2（複数Webサイトの改ざん）　2／4

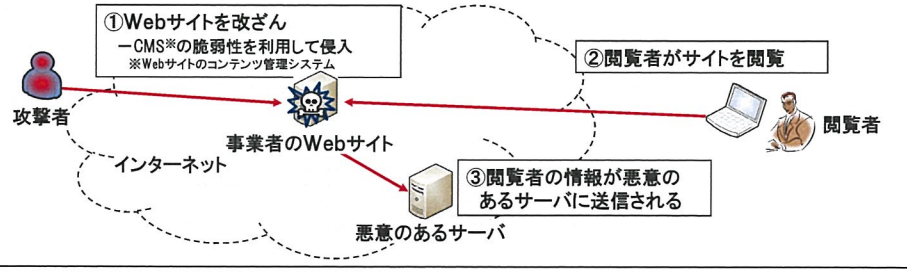
NISC

【事象のイメージ】

＜１件目のインシデント案件＞



＜２件目のインシデント案件＞



事例2（複数Webサイトの改ざん）　3／4

NISC

【原　因】

＜１件目のインシデント案件＞

- **初期構築時にのみFTPを利用し、その後はCMSを利用した更新を行っていた。現在の担当者がFTPサービスが提供されている事を知らなかったため、FTPのID・パスワードは初期構築時より変更されていなかった。**
- **不正なFTP接続によって、外部のWebサイトよりウィルスをダウンロードさせるプログラムがWebサイトに挿入された。**

＜２件目のインシデント案件＞

- **同一Webサイト上にバージョンが異なる(脆弱性を有するバージョンを含む)CMSが存在していた。脆弱性の存在を認識していたものの運用中のWebサイトへの影響を考慮し、更新及び統一化が出来ていなかった。また、担当部署に加え外部事業者等の複数者がWebサイトの内容変更が可能な権限を有していた。**
- **改ざんの約1ヶ月前に当該Webサイトに対して総当たり攻撃が行われていた。**

事例2（複数Webサイトの改ざん）　4／4

NISC

【再発防止・課題等】

- **Webサイトの必要性の見直しを行い、可能な限りIT担当部署が管理するWebサイト等に統合することにより管理の効率化等を図った。**
- **ファイアウォール等の設定を見直し、Webサイト利用における最小限の通信のみとした。**
- **管理ページを含めたWebサイトのログを取得し、適切な期間(例えば1年間)保存するとともに、定期的に確認を行うこととした。**
- **CMSを1つに統合し一元的に管理すると共に、Webサイトの内容変更ができる権限を持つ者を限定した。**
- **事業者内のWeb管理者向け研修において、事例を共有することにより他の担当部署が管理するWebサイトで同様の事象が起こらないように注意を促した。**
- **幹部会議において事例を紹介し、担当者任せにせず幹部主導の下、組織として改善を行って欲しい旨の周知を行った。**

【得られた気づき・教訓】

- **2件目の案件において、担当部署の判断により詳細が判明する前にWebサイトを停止することにより被害の拡大が防止された。現場で素早い判断を行うための体制や運用ルールの明確化または、現場で判断が出来ない場合であっても、速やかに判断できる者に報告できる体制構築が望ましい。**
- **Webサイトのアクセスログについて、事業者全体のルールでは保存期間を決めていなかったため、今回の2件ともに1ヶ月の保存期間であった。そのためログの解析が十分に出来なかった。今回の教訓を踏まえ、全体ルールとして適切な期間のログの保存を義務付けた。**
- **Webサイトの担当部署が複数に分かれるためITに詳しくない担当者もいる。ITに詳しくない担当者に対してもインシデント内容の重大性を理解してもらうための分かりやすい説明が必要である。また、何か不明な点があればIT担当部署に問い合わせを行うべきである。**
- **普段からWebサイトの挙動に気を配り、通常と違う挙動が見られた場合に調査を行う、いわゆる予兆を見逃さない心構えが重要である。**

NISC National Information Security Center

【参考2】
サイバーセキュリティ戦略、各施策の取組など

「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議）

NISC

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靭な」サイバー空間（守り強化）	①●機微情報を守るためのリスク評価手法の確立【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●SNS・グループメールを含む新サービスに伴う新たな脅威への対応【2014年5月】	②●重要インフラの範囲拡大や安全基準見直し等行動計画の見直し【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
「活力ある」サイバー空間（基礎体力）	③●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【2014年5月】 ④●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】	⑤●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京）　●MERIDIAN注3（2014年11月・東京） ⑥		●共同意識啓発活動【毎年10月】
組織体制	●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組：2015年度目途）【継続審議中】		

（注1）日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
（注2）サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加。
（注3）重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

サイバーセキュリティ2014（14年7月、情報セキュリティ政策会議決定）

NISC

▸「サイバーセキュリティ戦略」（2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度）に基づく年次計画の2期目。

	2013	2014	2015
戦略	「サイバーセキュリティ戦略」（2013/06/10）		
年次計画	「サイバーセキュリティ2013」（2013/06/27） ・ 戦略に基づき、各分野で新たな方針／プログラム等を策定	「サイバーセキュリティ2014」（2014/07/10） ・ 新たな方針／プログラム等を踏まえ、個々の施策をより具体化して推進	
「強靭な」サイバー空間	「政府機関統一基準群」改定（2014/05/19） 「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」策定（2014/05/19） 「情報セキュリティ普及・啓発プログラム」改定（2014/07/10）	【主な施策】 ・政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し（内閣官房及び全府省庁） ・政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化（内閣官房及び総務省） ・調達時における対策の推進（内閣官房） ・GSOCの抜本的強化（内閣官房及び全府省庁） ・重要インフラに関する、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化（内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁） ・新たな情報セキュリティ普及啓発プログラムの策定・推進（内閣官房及び関係府省庁） ・高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築（総務省） ・日本版NCFTAの創設に向けた検討（警察庁） ・防衛情報通信基盤（DII）の整備（防衛省） ・国家レベルのサイバー攻撃への対応の強化（内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係省庁）	
「活力ある」サイバー空間	「情報セキュリティ研究開発戦略」改定（2014/07/10） 「情報セキュリティ人材育成プログラム」改定（2014/05/19）	【主な施策】 ・情報セキュリティ研究開発戦略の研究開発の推進（内閣官房及び関係府省庁） ・新・情報セキュリティ人材育成プログラムの推進（内閣官房） ・サイバー攻撃事前防止・早期対策に向けた取組の推進（総務省） ・情報セキュリティに係る競技会・演習等の実施（総務省及び経済産業省） ・情報処理技術者試験制度に関する在り方についての検討（経済産業省）	
「世界を率先する」サイバー空間	「サイバーセキュリティ国際連携取組方針」策定（2013/10/02）	【主な施策】 ・サイバー空間に関する国際的な規範作りへの参画等（内閣官房、総務省、外務省、経済産業省及び関係府省庁） ・サイバーセキュリティ政策に関する二国間対話の強化（内閣官房、総務省、外務省、経済産業省及び関係府省庁） ・多国間の枠組み等における国際連携・協力の推進（内閣官房、外務省及び関係府省庁） ・サイバー攻撃に関する諸外国関係機関との連携の強化（警察庁及び法務省） ・諸外国とのCSIRT間連携の強化（経済産業省）	
推進体制等	「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（審議継続中）	【主な施策】 ・NISCの機能強化（内閣官房） ・官民の情報共有の更なる推進（内閣官房及び関係府省庁）	

統一基準群の改定（14年5月、情報セキュリティ政策会議決定）

NISC

現行の統一基準群の課題と改定の方向性

◆ 新たな脅威への対応のための基準の追加

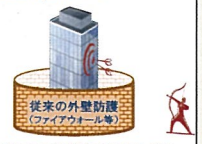
◆ 不明確で分かりにくい基準の明確化

主な改定内容（※）

◆ 標的型攻撃への対策

➢ 標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずる。

標的型攻撃のイメージ



・特定の組織の情報に狙い
・従来の外壁防護を無効化

内部対策の強化が重要

◆ サプライチェーン・リスクへの対策

➢ 情報システムの構築等の外部委託の際、委託先における不正機能の混入防止のため、厳正な管理を要求。

◆ 分かりやすく、守られやすい基準

➢ 定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人毎の遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく、守られやすい基準作りを目指す。

（現行の統一基準における規定の例）
行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。
ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に 報告することができない場合は、定められた 報告手順に従って、最高情報セキュリティ責任者に報告すること。

（見直し案）
行政事務従事者は、情報セキュリティインシデントを認知した場合には、各府省庁の報告窓口に速やかに連絡し、指示に従うこと。

（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）において決定された事項を踏まえ検討。）

高度サイバー攻撃対処のための取組等（14年6月、CISO等連絡会議決定）

NISC

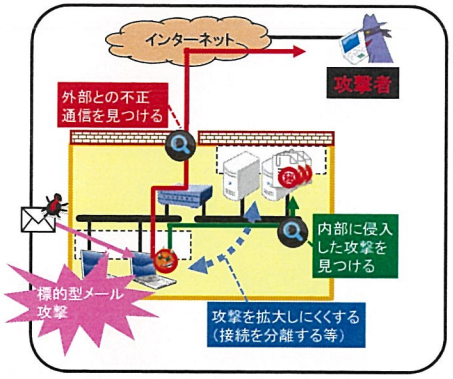
高度サイバー攻撃対処のための取組

◆ 取組の概要

- 高度サイバー攻撃の脅威から重要な業務・情報を取り扱う情報システムを守るため、それらを特定し、対象となる情報システム内部に侵入した攻撃の発見・遮断を目的とした対策を、計画的・重点的に実施する取組を今年度から本格的に実施する。

（平成26年6月25日　情報セキュリティ対策推進会議）

情報セキュリティ対策の概要(例)



独立行政法人における情報セキュリティ対策の推進

◆ 独立行政法人におけるセキュリティ対策の推進

- 独立行政法人がサイバー攻撃の標的となっている事例が複数判明
- 独立行政法人においても、政府の重要な情報を扱う場合は、政府機関と同等の情報セキュリティ対策を講ずることを決定

（平成26年6月25日　情報セキュリティ対策推進会議）

独法及び主務省庁が一体となって対策を推進

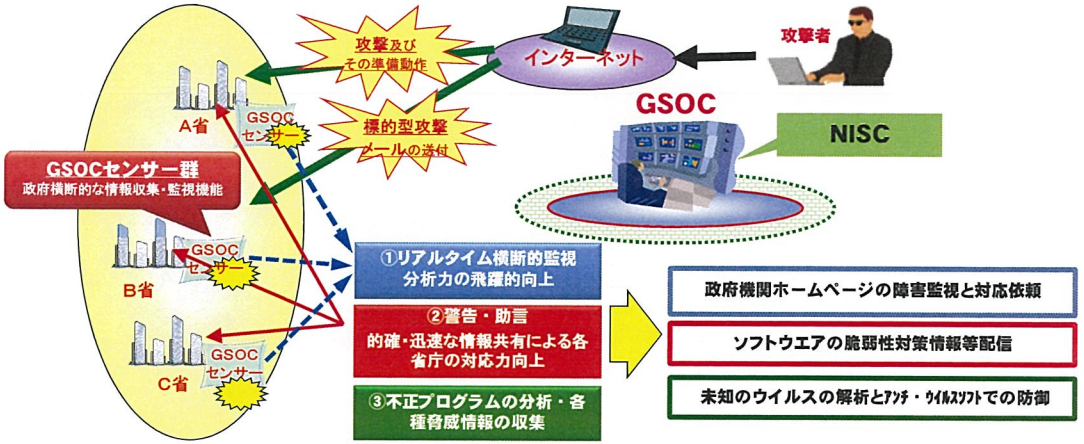
1. 業務計画の中で情報セキュリティ対策を位置付け
   ・統一基準群を踏まえた情報セキュリティ対策を独法にも適用
2. 連絡体制構築により、迅速な情報連絡・共有
   ・経営管理層への情報展開、判断による迅速な対応
3. 業務評価の際にフォローアップし、対策を着実に推進
   ・対策の実効性確保のための推進力

GSOC（ジーソック）

NISC

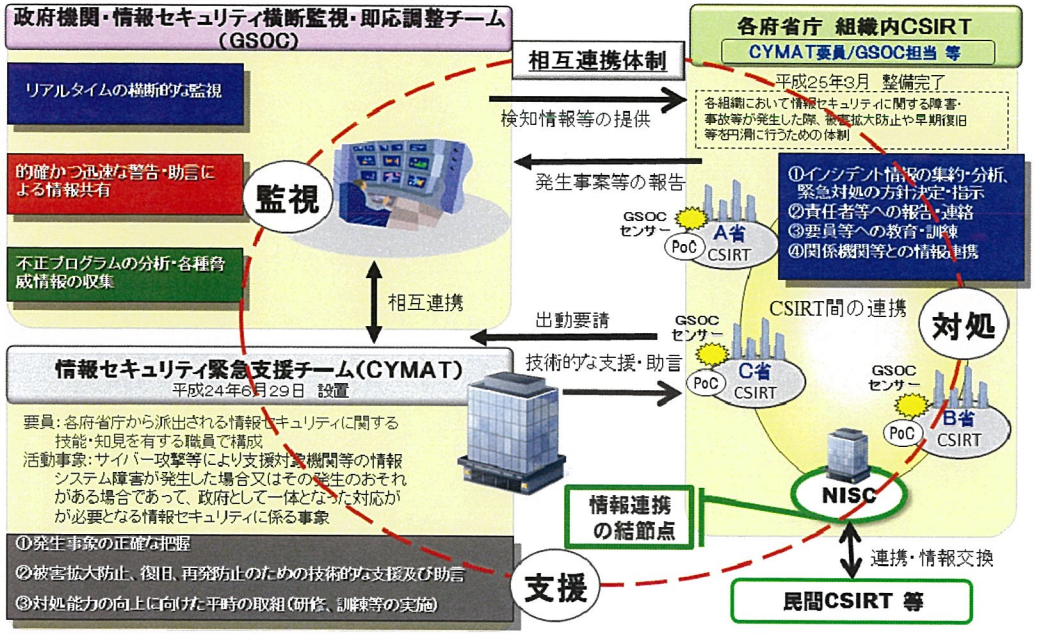
【Government Security Operation Coordination team ･･･ 政府機関情報セキュリティ横断監視・即応調整チーム】

- 平成20年4月　GSOCの運用開始（８時間運用）
- 平成21年1月　24時間対応開始
- 平成25年４月　現行GSOCシステム運用開始
- 平成29年（2017年）　次期システムへ移行



政府におけるサイバーセキュリティ確保体制

NISC



新・情報セキュリティ人材育成プログラム（１４年５月、情報セキュリティ政策会議決定）

NISC

サイバーセキュリティ戦略で示された課題

情報セキュリティに係るリスクの深刻化に対応するためには、
○人材の量的不足の解消に向け 積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題。
○そのためには、社会全体で育成し活用するための仕組みが必要。

人材の量的・質的不足

情報セキュリティ従事者 約26.5万人
うち質的不足 約16万人
さらに量的不足 約8万人
⇒これら人材の雇用の受け皿も不可欠

IT人材106万人（SE80万人）　*IPA調べ

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○組織の経営層
・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。
・製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

○実務者層のリーダー層
・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

【供給】人材の「量的拡大」と「質的向上」

○IT技術者等に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。
○高度な専門性及び突出した能力を有する人材の発掘・育成を推進するとともに、実社会での活躍を促進。
○グローバル水準の人材の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。
○政府機関は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。
○教育機関（初等中等教育機関含む）の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。

企業等における情報漏えいインシデントの動向

○企業等における情報漏えいインシデントについて、全体の件数自体は減少しているが、**不正アクセスを原因とする大規模な被害**が急増。

2013年個人情報漏えいインシデント

	2013年データ	2012年データ
漏えい人数	931万2543人	972万65人
漏えい件数	1333件	2357件
想定損害賠償総額	2020億6575万円	2132億6405万円
一件当たりの漏えい人数	7385人	4245人
一件当たり平均想定損害賠償額	1億6024万円	9313万円
一人当たり平均想定損害賠償額	2万7675円	4万4628円

件数は減少

被害が大規模化

インシデントの規模トップ20

No.	漏えい人数	業種	原因
1	400万人	情報通信業	不正アクセス
2	169万2496人	情報通信業	不正アクセス
3	47万人	卸売業，小売業	不正アクセス
4	42万6000人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24万3266人	情報通信業	不正アクセス
6	17万5297人	情報通信業	設定ミス
7	15万0165人	卸売業，小売業	不正アクセス
8	12万0616人	金融業，保険業	管理ミス
9	10万9112人	情報通信業	不正アクセス
10	9万7438人	情報通信業	不正アクセス

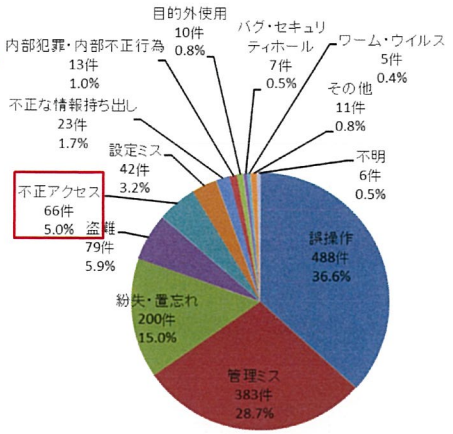
情報通信業が多い

2013年は不正アクセスが急増！

100万人以上！

大規模な漏えいの上位を占める不正アクセス

2013年原因別インシデント数



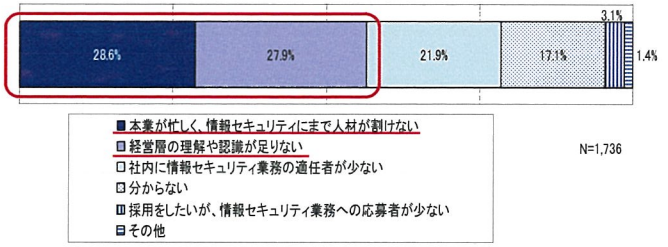
出典：2013年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～（日本ネットワークセキュリティ協会（JNSA））

2013年1月1日～12月31日の1年間にインターネットニュース等で報道されたインシデントの記事、組織から公表されたインシデントのプレスリリース等をもとに集計。想定損害賠償額については、JNSAが開発したモデルを用いて推定。

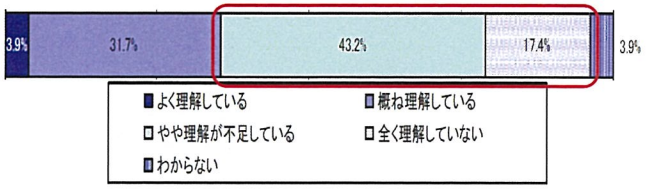
企業等における情報セキュリティ対策の現状

○企業では**情報セキュリティに関する業務に従事する人員が不足**。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

人材不足の原因（社内向け業務）



企業経営層の情報セキュリティに対する理解度



（経営層以外からの回答）

出典：独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012年4月

新・情報セキュリティ普及啓発プログラム（14年７月、情報セキュリティ政策会議決定）

背景

・若年層から高齢者までの**あらゆる世代**、個人・家庭・職場・公共施設などの**あらゆる場面**、国民1人1人の日常生活や社会経済活動等の**あらゆる活動**にサイバー空間が拡大・浸透。
・オリンピック・パラリンピック東京大会が開催される2020年を見据え、我が国として情報セキュリティ水準の向上が急務。

課題

国民1人1人や企業が自ら具体的な情報セキュリティ対策を進んで実行できるよう、以下の課題への対応が必要
○一般利用者等における認識の更なる醸成　○地域における普及啓発活動の活性化　○主体的な普及啓発の促進

今後の取組方針

基本的な考え方　国民全体の情報セキュリティへの関心・理解度・対応力の強化・増進を図る

推進体制　産学官民の多様な主体で構成する**協議会形式の場**を設け、国民運動として普及啓発活動を推進していく体制を構築。各主体が自律的に取り組める環境を整備し、国民1人1人に身近な地域との連携を推進。

主な取組

①総合的・集中的な普及啓発施策の更なる推進
…・「情報セキュリティ月間」の期間を拡大(2月～3月18日 <サイバー訓練の日>)し、広く国民に啓発。
・期間を問わず、ロゴマークやメディア等を活用し、国民に親しみやすい取組を推進し、取組の定着化を図る。
・国民1人1人が、サイバー空間の脅威から自ら身を守ることができるよう、国民運動として対策の実践や訓練等を促進。

②地域における取組の促進
…地域における各主体の活動や情報共有を促進。協議会形式の場を通じ、地域発産学官民連携による取組を全国的な動きに発展。

③特に注力が必要な層に対するきめ細やかな普及啓発活動の推進
…国民全体を対象とした活動に加え、特に注力が必要なターゲット（初等中等教育層、学ぶ機会が少ない層、関心が薄い層、中小企業含めた企業等）に対し、協議会形式の場も活用してきめ細やかな普及啓発を推進。

情報セキュリティ研究開発戦略（改定版）（14年７月、情報セキュリティ政策会議決定）

サイバーセキュリティ戦略（2013年6月策定）において示された
○ サイバー攻撃の検知・防御能力の向上
○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発　等
を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1. **サイバー攻撃の検知・防御能力の向上**
・分散しているサイバー攻撃情報等の共有のための組織等の連携強化
・研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討
2. **社会システム等を防護するためのセキュリティ技術の強化**
・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進
3. **産業活性化につながる新サービス等におけるセキュリティ研究開発**
・今後発展が期待されるICT利用分野で上流工程からセキュリティ品質の組込を推進
4. **情報セキュリティのコア技術の保持**
・暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化
5. **国際連携による研究開発の強化**
・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

研究開発の効果・成果を高めるための方策等

1. 研究成果の社会還元の推進
2. 必要な研究開発リソースの確保と柔軟性確保
3. 情報セキュリティ技術と社会科学など他分野との融合

情報セキュリティ研究開発における重要分野

（※　左記の観点を踏まえ、重要分野を整理）

(1)情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク　等
(2)ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保　等
(3)個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用　等
(4)研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術　等
(5)発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続　等

NISCの機能強化に関する政府方針

サイバーセキュリティ戦略（平成25年6月情報セキュリティ政策会議決定）

NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、**GSOCの抜本的な強化**を図るとともに、サイバー攻撃に関する**インシデントに関する情報等の集約**、サイバーセキュリティに関する**国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知**、政府機関及び独立行政法人等の**関連専門機関等に分散している各種機能の有機的な連携による動的な対応**等を強化する。その際、**国際的なインシデント対応における我が国の窓口となるCSIRT機能**の在り方についても併せて検討する。

以上を踏まえ、NISCについては、**専門職員の採用や育成等の人事管理による人材の確保**や**権限等の必要な組織体制**を整備することにより、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組するものとする。

国家安全保障戦略（平成25年12月国家安全保障会議決定・閣議決定）

サイバーセキュリティを脅かす不正行為からサイバー空間を守り、その自由かつ安全な利用を確保する。また、国家の関与が疑われるものを含むサイバー攻撃から我が国の重要な社会システムを防護する。このため、**国全体として、組織・分野横断的な取組を総合的に推進**し、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る。

そこで、**平素から、リスクアセスメントに基づくシステムの設計・構築・運用、事案の発生の把握、被害の拡大防止、原因の分析究明、類似事案の発生防止**等の分野において、**官民の連携を強化**する。また、**セキュリティ人材層の強化、制御システムの防護、サプライチェーンリスク問題への対応**についても総合的に検討を行い、必要な措置を講ずる。

さらに、国全体としてサイバー防護・対応能力を一層強化するため、**関係機関の連携強化と役割分担の明確化**を図るとともに、**サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上**及びこれらの任務を担う**組織の強化**を含む各種施策を推進する。

かかる施策の推進に当たっては、幅広い分野における**国際連携の強化**が不可欠である。このため、**技術・運用両面における国際協力の強化**のための施策を講ずる。また、**関係国との情報共有の拡大**を図るほか、サイバー防衛協力を推進する。

わが国のサイバーセキュリティ体制の強化に向けて

（１４年４月１０日、自民党サイバーセキュリティ対策関係合同会議）

1　体制強化の必要性

～ 急速に高まるサイバー脅威への対処 ～

●●安倍政権の成長戦略を確固たるものとするためには、ITの利活用等とともに、急速に高まるサイバー脅威に対処するため、**サイバーセキュリティを含む情報セキュリティの強化**について、**国自らがリーダーシップを強く発揮できる体制**への抜本的強化が必要。

2　体制強化に向けた基本的考え方

～ 国の主導的な役割の明確化 ～

●●「インターネット前提社会」では、**民間の主導的役割等を定めるIT基本法は堅持**しつつ、**官民の緊密な連携**を前提に、**国家の安全保障、国民1人1人の認識醸成、東京オリンピック等への対策**のため、国の主導的役割の明確化が必要。

3　「サイバーセキュリティ基本法」（仮称）の制定 ～ 基本理念等の確立、司令塔の強化 ～

●**基本理念**として次を規定。

① **情報の自由な流通の確保**等を基本として、サイバー脅威に対し、**官民連携により能動的・積極的に対応**。

② **国民１人１人が情報セキュリティの認識を深化**し、被害から円滑・迅速に復旧等できる**強靭な体制を構築**。

③ **将来に渡りITの恵沢を享受**するため、その持続的な開発・利用による**創造的・活力ある経済社会を構築**。

④ **グローバルに密接な相互依存**の中、協調、規範策定、信頼醸成や能力構築支援等における**先導的な役割**。

●**国・重要インフラ事業者等の責務、関係者間の連携強化、必要な措置・行政組織の整備、基本的施策**等を規定。

●**司令塔となる「情報セキュリティ政策会議」の機能・権限**として次を規定。

①**サイバーセキュリティ戦略**の策定、②各府省等の対策に関する**統一基準の策定・監査**、③**経費見積もり方針**等の策定、④重大インシデントの**原因究明調査**、⑤関係行政機関への**議長による勧告**　等

4　組織体制の強化に向けて ～ NISCの法制化等 ～

●**平成27年度からの本格稼働**を目指すべく、**政府において**、政府機関の横断監視機能（**GSOC**）**等を担うNISC（内閣官房情報セキュリティセンター）の法制化**等の組織体制を強化すべき。

サイバーセキュリティ基本法案の概要

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、強靭な体制の構築

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

オリンピック・パラリンピック・ロンドン大会(2012)の教訓

GCHQ(政府通信本部)に政府予算を付けて英国全体のセキュリティ対策を実施。

■ロンドンオリンピック公式サイトへの攻撃

➢2週間の開催期間に2億1，200万回のサイバー攻撃(公式サイト "London2012.com")。

➢全体で23億件のセキュリティイベントが発生。

➢1秒間に1万1千件のDDoS攻撃を観測・防御。

■開会式での電力インフラ(照明)への攻撃

➢オリンピックに備えて考えられる限りの電力インフラへのサイバー攻撃対処訓練を5回実施。本番直前に攻撃情報があり、電力設備を急遽マニュアルで操作。

➢わずか30秒の停電で開催国の威信が損なわれる(reputation riskへの対応が重要)。

■教訓

➢「ダウンタイム」は許されない。

➢品質保証は"Right First Time"と"Fail Fast"が原則。

➢本格システム稼働は開催の28か月前。

➢英国との協力関係(本年5月総理訪英、日英協定によるﾉｳﾊｳ移転、日英ｻｲﾊﾞｰ協議)

検討に当たっての留意事項

ロンドンとの違いも念頭に置いた検討も必要

■全体像の把握とリスク分析

※五輪についての全体像を把握し、リスク分析に活用
※地震、台風等我が国特有のリスクを抽出
※バランスの勘案
⇒ オリンピック関連システムだけ防御レベルを上げると他の重要システムへの攻撃が増加する弊害等も考慮

■技術・環境の変化への継続的な対応

※社会・経済に影響を与えるIT・環境の変化の把握
⇒ 8Kテレビ、スマートメータ等への対応
⇒ ロンドンでは、スマートフォンの出現で通信容量の見積もり変更を余儀なくされた

■人材の確保と育成

※質量双方の向上を見据えたセキュリティ人材の育成・確保
⇒ 2020年を見据えた若年層等の採用・育成