第 8回目　サイバーセキュリティー研究会
実施日：２０１９年3月１２日（火）
発表者：酒井雅之氏　内閣サイバーセキュリティセンター(NISC)参議官
発表テーマ：政府における サイバ ーセキュリティ人材育成の 取り組み

本研究会メンバーの一員である NISC 酒井氏より以下 3 点に基づいてご発表いただいた、
- 「人材育成政策の動向について」
- 「システム管理者としての政府の取り組みについて」
- 「インシデントの事例」

サイバーセキュリティとは、データを資産として捉え守るという原点から、データを含めたシステムの可用性（クエリを受け付けるシステム、レポーティングなどが正常に動作する)、そしてそのシステムに依存しているビジネスに不可欠なデータとシステムが事業継続に必要な範囲で動く（そのためのビジネスを守る）という意味合いを含んだものになっている。これは企業にとって責任として共通認識となっているが、国内の経済、社会活動、外交、国際サイバー空間と枠が広がり、サイバー戦争、フェイクニュース、SNS プロパガンダなど様々な事象が出始め、対応が難しくなってきている。昔のようにシステムを１００%守ることは、今日では不可能であるという認識が深まることで、問題の焦点はリスクをどうコントロールするかに移った。政策会議等でよく行われるサイバーセキュリティという名称があるが、実際には事業継続についての話である。
そこで肝心となるのは、誰がそのセキュリティを守るのかであるが、政府の政策ではシステムを守るのはシステムオーナーであることを強調している。国会議員からはよく中国からのサイバー攻撃や重要インフラについてしきりに聞かれることがあるが、NISC が全体のシステム・データを守ることはない。システムを守るのに誰がどこまで参加すべきかについて、既存のデータシステム、新しい技術に対する対策、国際協力（先進国との連携、途上国への支援など)、そして横断的施策（人材育成、確保、研究開発・推進、ユーザーサイドのすべきこと）についてご紹介いただいた。

質問・コメント（一部抜粋）
Q:CISO とサイバーセキュリティ審議官とどういう関係か？
A:CISO はだいたい官房長クラスの方宛になっている。それとは別に、最近、専任のサイバーセキュリティ・情報化審議官が各省に配置された。
Q:経産省に防衛省から来た人を CISO としていたが、それは補佐官か。
A:その場合は、経産省の職員として就任していると思う。補佐官の場合は外部有識者という扱いで非常勤という印象だった。
A2: CISO は官房長とそのサポートをしているのがサイバーセキュリティ・情報化審議官。

Q:ということは官房長を補佐する役とは別ということか。
A:ラインとしてはそういうことになる。官房長がいて、その下直属の部隊があり、その中にCIRT がいるという構成かと思う。

政府機関における人材育成・スキル認定
補佐、係長、係員レベルを対象にスキルモデルを策定し、研修を行っている。スキル認定されたら給料をあげるというインセンティブが最近ようやく出始めた。ただし財源を確保するのは各省庁で、適用者は数パーセントの昇給を受けるが、異動するとそのポストではなくなるため、給料は元に戻ってしまうという話だと聞いている。そのため、スキル認定は、そのポストについている時に付属的につくもので、認定されたからといって未来永劫給料が高いままだというものではないようである。

セキュリティ・IT 人材育成総合強化方針について
各府省庁における司令塔機能の抜本的強化として、以下の項目を実施。
- 情報化審議官の設立及び人材・育成計画によるフォローアップ。
- サイバーセキュリティ対策推進会議（CISO 等連絡会議）と CIO の連絡会議
- 橋渡し人材の育成（官房長はセキュリティにあまり詳しくなく横断式に知識・技術的見解を取り入れることができるように育成方法を工夫。）
- 人材の確保（大学への働きかけが主で、よい人を直接採用する段階には来ていない）
- 外部の即戦力人材の確保（政府 CIO 補佐官を外部の専門家として招聘。ただし現場のリスクアセスメントに全面的に携わるのではなく、担当者が作成したもののレビューがメイン。）
- 一定の専門性を有する人材の育成（キャリアパスに乗った人への講習提供）
- セキュリティ研修（政府統一の研修に最近導入。行管局の研修で受ける仕組み。）

こういう状況から、役所が払える給与は給与法で決まっており、民間に匹敵するだけの給与を払えるかどうかで、人材確保の難しさに直面している。

省庁内におけるインシデントハンドリングの統一化
- 各省庁にて、CISO への報告、被害拡大防止、回復への対策、原因調査、教訓、再発防止、対処手順、体制の見直しを行う。その事前準備として体制、レポートラインの整備。報告内容における具体的手順、職員への訓練法を記載。
- CISO の元に、CSIRT 配置を義務化。多くの省庁では、システムはアウトソースされており、契約管理をする情報システム部門とその先に IT ベンダーが主な管理役。
- 事故報告の徹底化（省内の報告窓口を通じて SIRT チームに行き、SIRT チームが CISO と、必要に応じて NISC にも連絡する。さらに、終わった後は各省庁に同じ轍を踏ま

ないよう、情報共有をする）