JNSA ワーキンググループ紹介

CISO 支援ワーキンググループ

CISO 支援 WG リーダー
株式会社 Preferred Networks　高橋　正和

CISO支援ワーキンググループは、今年５月に「CISOハンドブック」を公開しました。本稿では、CISOハンドブックの作成の経緯を中心に、CISO支援WGの活動をご紹介いたします。

CISO ハンドブック（CISO支援ワーキンググループ）
https://www.jnsa.org/result/2018/act_ciso/

■ CISO支援WGの設立

CISO支援WGの設立は、前WGリーダーの河野さんと私の「PDCAの”Check”はファクトベースで実施すべきだ」との議論がきっかけとなりました。そして、「CISOが経営会議に報告する内容としてチェック項目と評価手法をまとめること」を目標に、一般社団法人日本CISO協会、日本ISMSユーザグループ、特定非営利活動法人日本セキュリティ監査法人（JASA）の支援をいただき、2016年にJNSA CISO支援WGを設立することになりました。

設立当初は、構想がある程度固まっていたことから、比較的早く完成すると考えていました。WGメンバー募集の活動予定を見ると、5か月程度で完成すると考えていたようです。

しかし、実際にはなかなか作業が進まず、「もうすぐ公表できる」との報告を続けたことから、「蕎麦屋の出前」プロジェクトと、ありがたくない呼ばれ方もしていました。

[2016年当初の計画]

4月初旬	キックオフ　理想的なCISO像についての意見交換
4月中旬以降	タスクフォースによる成果策定
5月以降	月に1回程度の成果報告会
9月以降	成果物のプロモーションを兼ねた勉強会、セミナーの開催

第一回CISO支援WG

第一回のCISO支援WGは2016年4月に開催されました。ここでの議論は、「CISOハンドブック」の内容とはずいぶんと違った内容で、CISOの組織論に終始し、当初考えていた経営会議への報告内容に関する議論には至りませんでした。この時の議論は、インタビュー記事[1]で取り上げて頂いた武田さんのコメントに集約されていると思います。

[1] 全ての悩めるCISOにささげる――「CISOハンドブック」はいかにして生まれたか
http://www.itmedia.co.jp/enterprise/articles/1807/06/news026.html

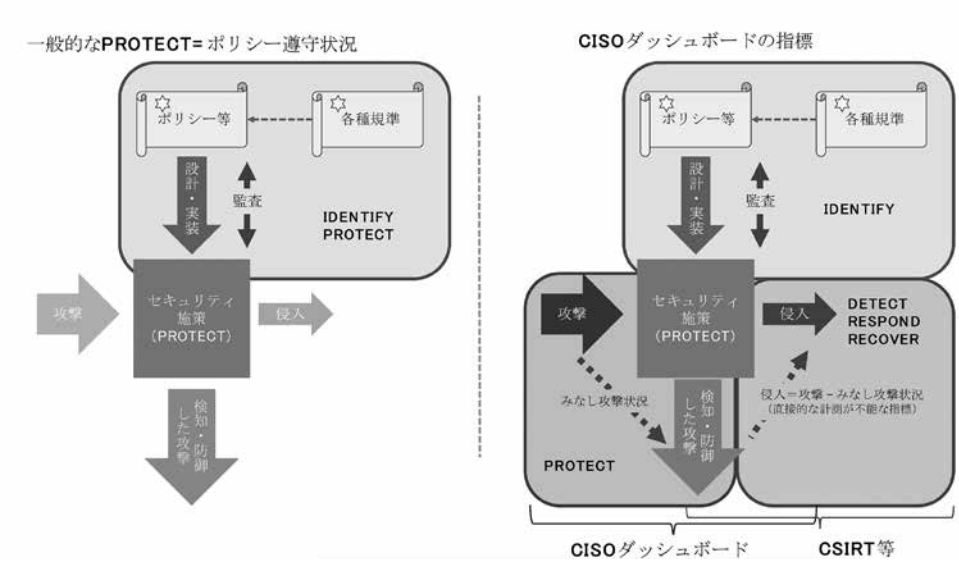
「そもそもCIO（Chief Information Officer：最高情報責任者）自体が破綻しているところが多く、ピンとこなかった。セキュリティでオフィサー？　そんなの機能しないでしょ！　と。そもそも組織によって、その位置付けも大きく変わるのではないか、という話からスタートしていた」

CISOダッシュボード

CISOハンドブックの作成は、ミーティングとMLを通じて作業を進めましたが、なかなか議論がまとまりません。成果物のイメージがないと議論が進まないと考え、想定される計測項目と考え方を、「CISOダッシュボード」としてまとめ、2017年1月に、WGのメーリングリストにポストしました。

「CISOダッシュボード」では、以下の4項目による組織のセキュリティ状況評価を提唱しています。

- Attack condition: どの程度の攻撃に直面しているのか（＝検出しているのか）
- Protection condition: 対策の状況は計画通りか（Assuranceの領域）
- Suspicious activity: 侵入を許したか、その可能性はあるか
- Indirect activity: PCの紛失、建屋への侵入、人事上のトラブルなど懸念事項



セキュリティ施策の考察（出典：CISOハンドブック）

ダッシュボードの成果であったかは定かでありませんが、WGは、河野さんを中心に断続的に作業を続け、2017年9月には「清書前の暫定版」をまとめ、WGメンバーによる校正を始めることになりました。

WGの再始動とCISOハンドブックの公開

しかし、再びWG活動が停滞します。2017年10月に私が転職し、12月には河野さんが転職したことから、WGとしての作業が進まない状況に陥りました。このため、2018年1月に私が暫定リーダーとなり、WG活動を続けることになりました。

ドキュメントの公開に向けたミーティング（編集会議）をWGに呼び掛けたところ、執筆メンバーとなった荒木さん、池上さん、北澤さん、田中さん、西尾さん、福岡さんに参加をいただき、何度かのミーティングを経て、公表できる内容にまとめることができました。

ミーティングは、それぞれの持ち味を感じる活発な議論と共に、多面的な角度から検討することができました。私自身も学ぶことが多く、刺激を受ける楽しい時間でした。このディスカッションの一部は、「CISOハンドブック」のコラムへと発展していきました。

そして、「CISOハンドブック」は、第一回のミーティングから2年を経て2018年5月に公開することができました。嬉しいことに、複数のメディアで取り上げて頂いただけではなく、JPCERT/CCやIPAのWebでもご紹介頂きました。また、2018年6月のJNSA活動報告会でも執筆メンバーと共に、ハンドブックの紹介をすることもできました。

今後の活動について

今後は、「インシデントシミュレーション」と「クラウドを前提としたセキュリティ対策」の二つの活動を予定しています。

CISOハンドブックの一部として公開をしている「インシデントシミュレーション」はワークショップとしての展開を目指しています。また、想像以上にクラウドファーストが進んでいるIT環境のセキュリティ基盤となるモデルとして「クラウドを前提としたセキュリティ対策」まとめて行きたいと考えています。

企業におけるCISOの重要性は高まっており、多くの企業がCISOを求めていると感じています。セキュリティベンダーにとっても製品やサービスの提案を進める上で、CISO業務の理解は欠かせないと考えています。

CISOハンドブックは、CISO業務の大枠をドキュメントとして形にしたものだと考えています。CISOハンドブックが、皆様がセキュリティ対策を進める上での一助になれば幸いです。