統合リスク管理レポート vol.01

新たな脅威に対応するための組織態勢の検討

– CSIRT および PSOC への取り組み –

LAC

2012 年 6 月

LAC セキュリティコンサルティングチーム

新たな脅威に対応するための組織態勢の検討
＝ CSIRT[1] および PSOC[2] への取り組み ＝

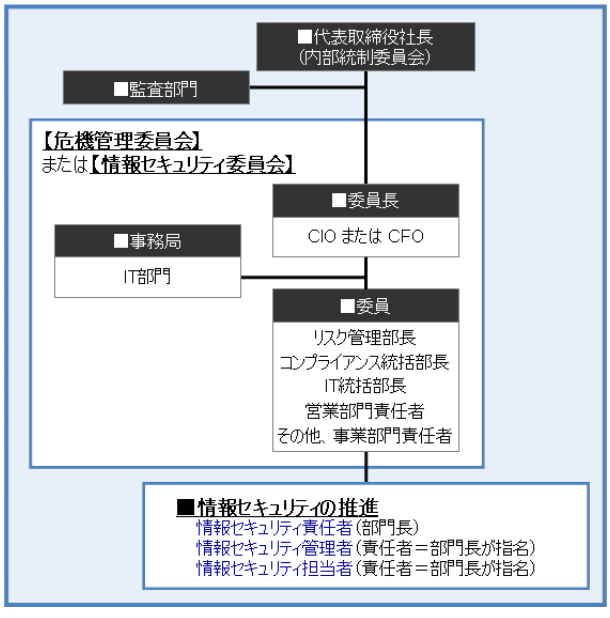
内田昌宏
Masahiro Uchida

標的型攻撃など新たな脅威に対する対応が急務である。もはやツール導入など技術的な対策だけでは我が身を守ることは難しく、運用管理の強化や従業員一人ひとりの意識向上が不可欠である。組織を取り巻く環境が急激に変化していく中［図 1］、本稿では、新たな脅威への対応を、組織態勢面から考察した。なお、セキュリティは実効的に実践することが重要であることから、本稿では〝仕組み・組織〟を意味する「体制」ではなく、あえて〝身構え・対応〟を意味する「態勢」という言葉を使用した。

［図1　組織を取り巻く環境の変化］

1.　はじめに

ISMS によるマネジメントシステムの普及に伴い、ほとんどの組織ではセキュリティ推進体制を構築してきた［図 2］。



［図2　一般的なセキュリティ推進体制］

ISMS が組織における情報セキュリティ・マネジメントの確立に大きく貢献したことは、疑う余地がない。情報セキュリティの推進は、多くの場合、情報システム部門が責任を負っているが、

» セキュリティに関する社外の情報源は多岐に渡り、本当に必要な情報が精査できない。
» 他社での取り組み、事故対応などを参考にしたいが、適切なパイプを持っていない。

などの課題を訴える声を耳にする。一方、重要情報を扱う事業の現場では、

» 強い責任感や高いモラルで業務を遂行している反面、業務と表裏一体に存在する危険への意識が薄い。
» 企業は、機能的・効率的な組織体系を追求し続けた結果、〝縦割り〟となり、運営や情報共有などが担当者のスキルに依存してしまっている。

などの弊害をうんでいる。

実際当社が実施したセキュリティアセスメント結果からも、

[1] Computer Security Incident Response Team の略。セキュリティインシデント対応組織の総称。
[2] Private Security Operation Center の略。組織内のセキュリティ監視を行う組織または機能の総称。

- ポリシ、セキュリティ推進組織、運用管理プロセスは整備されており、上位リスクを許容リスクに収めようとする努力が一定の成果をあげている。
- 不要なアカウントが残っていたり、セキュリティパッチが適用されていない等、古くて新しい課題（緊急ではないが重要な課題）が上位に残存している。
- 新たな脅威に対する取り組みが遅れ、上位リスクとして登場してくる。

という傾向が明らかである。

このことは、情報セキュリティ・マネジメントのフレームは構築されているものの、ルールや仕組みの形骸化や、新たな脅威に追従できていない様子がうかがえる。直接利益を生まない情報セキュリティへの取り組みが必要最低限に抑えられる中、情報システム部門は、

» 日々発生するシステム障害やセキュリティ事故対応に追われ、事後対応、その場対応にならざるを得ない状況であること
» 業務を優先するあまり例外処理が増えていくこと
» 事故前提での検討が不足していること

などの結果であると推察される。新たな脅威が登場してくる中、このような矛盾を抱えたまま、既存の態勢で克服できるだろうか。

- 同じようなトラブルに悩んでいませんか?
- あなたの力だけで十分ですか?

2. セキュリティ推進に必要な機能の強化

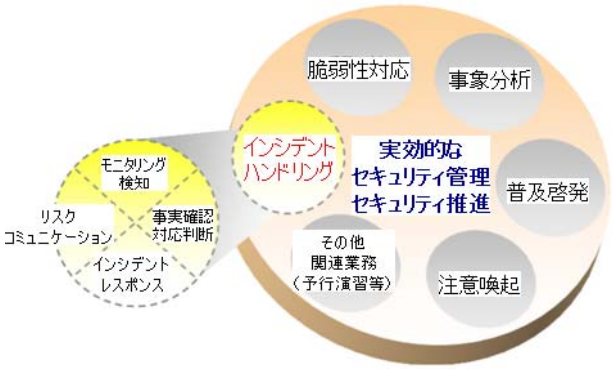
あらためて情報セキュリティを推進するために必要な機能を整理してみた［表 1］。

■ 平常時
① ルール（セキュリティポリシ）策定と周知
② 教育、訓練
③ 脅威に対応できる管理策（IT、運用）実装
④ リスク評価、脆弱性診断
⑤ 監視（いち早く気づく、兆候検知）
⑥ 情報収集と社内展開
⑦ ヘルプデスク
⑧ 監査、改善
■ 緊急時
⑨ 迅速なエスカレーションと適切な判断
⑩ 証拠保全
⑪ フォレンジックによる原因究明と影響調査
⑫ 緊急対応、被害の極小化
⑬ 公表や当局への報告
⑭ 再発防止

［表1　セキュリティ推進に必要な機能］

2.1. CSIRT…実効的にセキュリティを推進

［表 1］で挙げた機能を強化するために、セキュリティを組織に合わせて実効的に推進しようとの発想でうまれたのが CSIRT である［図 3］。



［図3　CSIRT のイメージ[3]］

CSIRT は、米国 CERT/CC を起源とし、日本では JPCERT/CC などが推進しているセキュリティ対応機能や組織の総称であり、以下を主目的としている。

- **関連情報の集約と効率的活用**
  情報集約、効率化、ノウハウ蓄積、社内外に対するセキュリティ窓口。
- **組織のセキュリティレベルの向上**
  必要な注意喚起、再発防止策のフィードバックによるセキュリティレベルの向上。
- **社内外に向けたメッセージ発信**
  顧客、取引先、関係機関等に対する「安全・安心」のメッセージ発信。
- **外部組織との連携**
  インシデント発生時の司令塔、または社外連携の窓口として問題の早期解決。

[3] 出典：JPCERT「経営リスクと情報セキュリティ」http://www.jpcert.or.jp/csirt_material/concept_phase.html から一部表現変更

CSIRT 構築の最大の期待効果は、社内外に対する窓口の一本化・明確化を含む、「情報の一元管理」と「社外との連携」である。特に、セキュリティ事故発生時には、状況把握と影響極小化に一刻を争うことから、社外の専門機関と連携した緊急対応が不可欠である。CSIRT の機能を体系的に整理すると、［図 4］のようなイメージになる。

［図4　CSIRT の機能体系］

ここで着目したいのは、［図 4］の中の「検知・警戒」ミッションである。新たな脅威に対応していくためには、内部の振る舞いから危険の兆候をいち早く発見することが求められる。このためには、IT の活用…特にログ管理が必須であり、情報システム部門との連携が不可欠である［図 5］。

［図5　CSIRT からみた PSOC の役割り］

2.2. PSOC…IT による内部監視の強化

PSOC は当社の造語である。情報セキュリティコントロールの見える化（モニタリング）を最適化し、社内外への説明責任を果たす必要性から、既存の IT 運用管理に追加して、以下の機能を持つものとして提唱している。

- **ネットワーク境界における監視**
  インターネット境界における監視だけでなく、重要な情報を保有しているサーバセグメントでの境界監視など、内部監視の強化。
- **インシデント対応の実務機能**
  内部の振る舞いを監視・分析し、いち早く不正の兆候や例外に気づく仕組みの運用。このため組織特有のユースケースを定義していくことが必要。

内部監視強化では、

- 必要なデバイス（サーバや PC）のログを〝相関的に分析〟し、正確に挙動を把握すること。
- さらに相関分析結果を〝横断的に分析〟し、組織固有の不審な動きをユースケースとして定義していくこと。

など、より高度なログ分析が求められる［図 6］。

［図6　高度なログ分析］

PSOC 構築の最大の期待効果は、「内部監視の強化」である。高度なログ分析により、

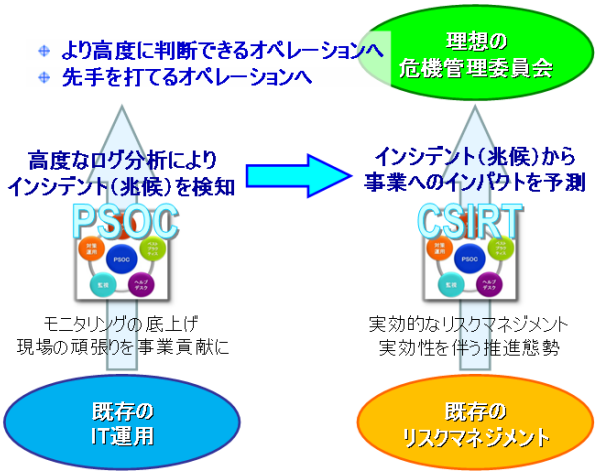
- 短時間に複数回ログインしようとした
- いつも使っているデバイスとは違う
- 短時間であり得ない場所からログイン

など、通常とは異なる挙動を発見することが期待できる。PSOC で不審な通信、例外的な挙動が検知でき、単に攻撃だけでなく、ポリシによってコントロールと早期の異常な兆候の発見による悪影響の軽減ができる環境があれば、CSIRT がより意味があるものになると考える。

3. 課題と所見

3.1. CSIRT と PSOC の連携イメージ

CSIRT と PSOC は、機能や目的は似ているが、手段や生い立ちが異なっているといえる［図 7］。



［図7　CSIRT と PSOC の位置づけ］

インシデント（あるいは兆候）から事業へのインパクトを判断（あるいは予測）するため、セキュリティ対応窓口を一本化し、社外と連携しながらインシデントマネジメントを確立しようとするのが CSIRT、高度なログ分析により、これまで見えなかったインシデント（あるいは兆候）を検知するため、モニタリングの底上げを図ろうとするのが PSOC と考えると、危機管理委員会には、是非、IT に裏付けられた高度なオペレーションに基づき、的確な判断が行えるリスクマネジメント組織を目指してもらいたいと願う。

卑近なケースとして入口監視を例に挙げると、PSOC→CSIRT→危機管理委員会の連携イメージは、［図 8］のようになるのではないだろうか。

危機管理委員会
CSIRT
PSOC

	セキュリティインシデント検出結果			セキュリティマネジメントオフィス対応業務			事業部門長	
	攻撃の事実	攻撃成功	攻撃失敗	実施管理者への通知	成功か否かの調査	影響度調査	影響度調査	格付け
Emergency	Yes	Yes	No	即通知	―	要	要	重大事故 or 通常事故
Critical	Yes	どちらも確認できない		即通知	要	(成功) 要 (失敗) 不要		
Warning	Yes	No	Yes	―	―	―		
Information	調査検査	―	―	―	―	―		

［図8　PSOC から CSIRT へのエスカレーション］

3.2. CSIRT にどこまで権限委譲するか

CSIRTという組織にセキュリティ運用管理にかかわる権限をすべて委譲するという考え方もあるが、活動を始めるまでに、

» 既存組織と合意形成が得にくく、委譲すべき権限の存在があいまいになる。

» 結果、社内での協力関係が得にくくなる。

などの障壁が考えられる。また人事異動による人材確保の課題も想定できる。このため、まずは、

- 既存組織体制を活用し、権限執行部署（執行者）と連携する。
- CSIRT は、対外的な窓口と、技術的対応に専念する。
- 緊急時には、司令塔として判断や社内調整ともに、外部専門機関との連携窓口となる。

を推奨したい。

4. おわりに

CSIRT も PSOC もセキュリティを推進する運営態勢である。〝こうあらねばならない〟というものは存在しない。また必ずしも新たな組織をつくるということではなく、既存の組織や分掌を有効活用しながら、必要な機能を追加・強化していくことが現実的なスタートラインかもしれない。

IT 戦略にビジネスリスク管理施策を具体的に盛り込むと、おのずと事業活動を行なううえで最適なバランスが求められる。実効的な事業運営を実現するためにも、モニタリング向上をめざした統合セキュリティ管理が求められている。

以上

2012 年 6 月

内田昌宏
技術士（情報工学部門）
株式会社ラック
理事　エグゼクティブコンサルタント

【徒然素心ひとりごと】

「セキュリティに 100 点満点はありえない」という議論について。

おそらく暗黙的にほとんどの人の共通した認識だろう。「では何点なら大丈夫なのか」と聞かれると困ってしまう。何が困るって、答えが出せないことではなくて、なにが知りたいのかが理解できないのです。

このはなし、実は〝大学受験生が、俺はどれだけ勉強したら東大に合格できる?〟という議論にものすごく似ているのですよ。しかも、こういう質問って、ハイパフォーマー受験生からは恐らく絶対出てこない。質問は、いわゆるミドルパフォーマー受験生からが多いのでは。

この違いってなんでしょう?

- ライバルのことを気にするのは、…ミドルパフォーマー受験生。
- 自分の弱点を正確に認識して、粛々と補強するのは、…ハイパフォーマー受験生。

- 東大合格が目的になっているのは、…ミドルパフォーマー受験生。
- 自分の将来象をはっきりとイメージし、そのために今目指す大学はどこか、あぁ東大か、じゃあ東大を目標にしよう、と考えるのは、…ハイパフォーマー受験生。

どうでしょう、セキュリティに取り組む組織にそのまま当てはまりませんか。
つまり、
「セキュリティに 100 点満点はありえない」とか、「何点なら大丈夫なの」という議論は、不毛なのです。
ハイパフォーマー組織なら、自分は何点だとか、世間一般はどうかなんて気にしない。将来にわたるグランドデザインを明確にイメージし、今すべきことをキチンと認識しているから。
ミドルパフォーマー組織にとって、点数は彼らにとっての安心材料か、言い訳にしかならない。

でも大丈夫。東大合格には定員がありますが、ビジネス社会に定員はありませんから。

LAC のセキュリティコンサルタントは、お客様の課題にひとつひとつ丁寧に向き合い、お客様の立場で課題解決を支援いたします。
レポートの内容、情報セキュリティに関するご相談はこちらまで。

株式会社ラック http://www.lac.co.jp
〒102-0093
東京都千代田区平河町 2-16-1 平河町森タワー
TEL : 03-6757-0113　E-mail : sales@lac.co.jp