ASIS 会員
株式会社ロックシステム
岡田　和寛

ASIS インターナショナル日本支部便り

月次セミナー　5月度 「組織を活かす情報セキュリティ」

５月の月次セミナーは、東芝ソリューション株式会社技監の遠藤直樹氏による講演、題して「組織を活かす情報セキュリティ」です。

（講演中の遠藤氏）

遠藤さんは、東芝で DVD-RAM や CPRM（コピーワンスの複写制御方式）の研究開発に携わった後、システムインテグレーション（SI）事業に移り、現在は東芝ソリューション SI サービスの顧客である官庁や大企業向けに、セキュリティソリューションを提供するビジネスを率いています。

講演では、金融・交通・電力・ガス、政府・行政等の「社会貢献のための基本的能力」を担う組織（重要インフラ）における情報システムの脆弱部分がネットワーク犯罪者の攻撃の標的となりつつある状況が語られました。防御のためには情報セキュリティを組織戦略として位置づけ、総合的な対策を効果的・合理的に案出し実施することが重要であるということを、実務で取り組んでいる事例を含めて、幅広く解説していただきました。以下はその概要です。

■システムの脆弱性とサイバー攻撃

オバマ政権は、2009 年 1 月 21 日に発表した「国土安全保障アジェンダ」で、情報ネットワークや重要インフラ保護の6つの目標を挙げ、新たにサイバー担当顧問を設置する方針を示しています。この背景には、サイバー攻撃者による「政府や企業の社会貢献のための基本的能力」を標的とした事件の増加があります。

例えば、電力会社、パイプラインなどのシステムの監視と遠隔制御を行う監視制御システム（SCADA）の脆弱部分が攻撃され、電力供給システムや水処理施設が被害を受けた事例があります。オーストラリアの汚水処理施設では、バルブが攻撃者に遠隔操作され未処理の汚水が流出しました。シェル石油では情報システムへの不正侵入により機密情報の盗難事件が起きており、ボストンの交通料金支払いシステムの脆弱性やボーイング社最新鋭機 B787 の搭載コンピュータの脆弱性が指摘されるなど、社会を担う情報システムへのサイバー攻撃のリスクが高まっています。

日本政府が 2009 年 2 月に発表した「第 2 次情報セキュリティ基本計画」では、個別計画の一つに「重要インフラ行動計画」が策定されており、重要イ

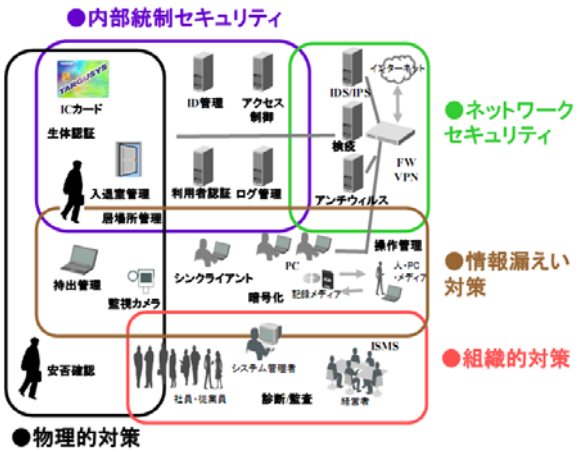
ンフラ分野における「安全基準等」の整備と浸透、情報セキュリティに関する組織の壁を越えた「情報共有体制の整備」等が指針として示されています。特徴的なのは、業法が課す業界毎の取り組みに加えて、基準とすべきサービスレベルを定め、重要な IT 障害と判断する検証レベルを示して情報を集め、行動計画の改善を促す仕組みを設けたことです。

■重要インフラや企業に求められること

重要インフラが対処しなければならないリスクには、サイバー攻撃、重大事故、及び大規模自然災害があります。これらのうち、サイバー攻撃の影響度が相対的に大きくなっています。

これらの脅威に対して、従来型の対応では不充分となりつつあります。IT 化の広がりにより、システムが複雑になっている（システムのスパゲッティ化）、オープンな OS やソフトが活用されるようになり欠陥や外部接点が減らない、さらには社会全体の最適化が進みインフラ間の相互依存が強くなったため、一つのインフラの停止が他にも影響しかねない、など問題が複雑化しているからです。

どう対応するか。情報システムの「見える化」、IT に係る内部統制の整備、及び事業継続管理がポイントです。「見える化」することで次の行動を考えることができ、ポリシーを定めマネジメントすることで遵守させ、日々のアクションを適正にできる。人命最優先で、災害時に事業継続のための次の行動を定めておくことも肝要です。



■総合セキュリティソリューション

重要インフラなど厳重なセキュリティを求められる組織には、総合セキュリティ対策が必要です。

このうち物理的対策のベースとなるのは IC カード等を用いた入退室管理システムです。人の出入りを抑制し、行動とその履歴を管理することは内部犯罪の抑止効果もあります。この発展形が居場所管理システムです。施設内各所に設置されたマットアンテナで通行者の持つ RFID タグの信号を受信して、移動方向を含めた行動監視が可能です。さらに、これを応用した非常事態の安否確認システムなども実用化されています。

情報セキュリティ分野では、通常の ID/パスワードに加え指紋など別の方法で追加の個人認証を行う「2要素認証」や、重要システムへのアクセスを集中管理するシングルサインオン、統合ログ管理システム、ネットワークインシデント管理など様々なセキュリティシステムが提供されています。

今後は、情報の整合性・統一性を追求すべく物理セキュリティと情報セキュリティの一体化が進みます。居場所によって、情報システムのアクセス権限を変えるなどの応用も可能となります。

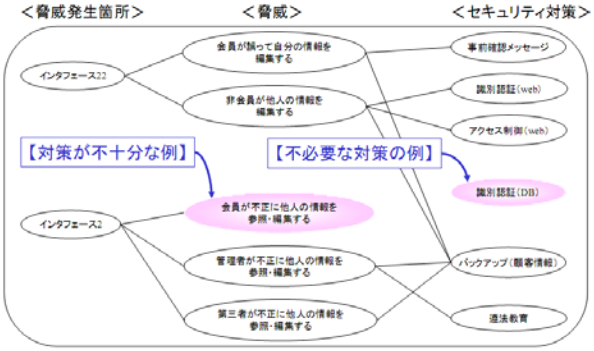
今後、情報システムはますます複雑化し、セキュリティの重要性は高まります。汎用性の高いセキュリティアーキテクチャや基盤技術が開発され、これをベースに、種々のアプリケーションとの親和性の高いセキュリティシステムが構築されるでしょう。

■「見える化」のためのセキュリティ技術

セキュリティ対策の基本は、リスク評価と有効なセキュリティ対策です。弊社では情報システムのセキュアな設計・構築体系を開発し、顧客に適用しています。リスク対策が想定リスクに必要十分な対応関係を持つことを「見える化」し、リスク対策を合理的に見いだすための仕組みです。

脅威の洗い出し後に、脅威分析とセキュリティ対策を行います。リスク毎に脅威の発生箇所（通信路、

インタフェース、その他）についてリスクを想定し、対策は抑止/予防、検出、回復、運用の各フェーズに分けて洗い出します。これにより、脅威にひも付かない対策は不必要、脅威に対策がひも付いていないときは不充分として設計を改めます。

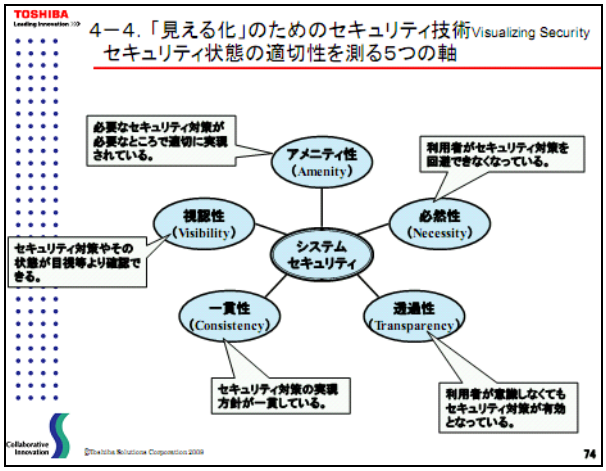


- 脅威に紐づかない対策は不必要
- 対策が紐づかない脅威がある場合は不十分

■セキュリティ劣化の防止策

セキュリティは経年劣化します。システム開発時に組み込んだセキュリティ対策も、維持・管理が適切に行われないと脆弱なものとなってしまいます。

弊社では、運用中の情報システムについてセキュリティ対策の実施状況を可視化する診断サービスを提供しています。セキュリティ状態の適切性を次の5軸で評価し、基本モデルと対比してレーダーチャートで見せることで、弱点を知り補強してもらうためです。



これまで述べたように、セキュリティについて現状が分かること、つまり「見える化」することは重要です。多くの企業では、これができておらず、効果のないセキュリティ対策を行うリスクを抱えています。セキュリティに関し、適切な経営判断をするうえでも「見える化」は重要と考えています。

以上、遠藤さんによるセミナーでした。

6 月のセミナーでは、情報セキュリティ専門家の国際団体，ISSA と共催で、コンバージェント・コンピューティング社コンサルタントであり、マイクロソフト社ウィンドウズのセキュリティ開発者の一人であるタイソン・コプチェンスキー氏に話していただきます。

■ ASIS インターナショナル日本支部の月次セミナーへのお誘い

ASIS インターナショナル日本支部は、月次セミナーを開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日

毎月第三火曜日　午後 6 時半より

■ 場所

国際文化会館（六本木）

東京都港区六本木 5-11-16

TEL: 03-3470-4611

http://www.i-house.or.jp/jp/ihj/access.html

■ 参加費

2,000 円（ASIS 会員・非会員同一料金）

このコーナーへのお問い合わせや入会お申込みは
ASIS インターナショナル日本支部　事務局まで

〒101-0021　東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL　03-3255-3468　　FAX　03-3258-7630
E-Mail info@asis-japan.org
www.asis-japan.org