みんなで考えよう日本の安全！

月刊セキュリティ研究

特集

情報カメラシステムの研究

アイティフォー　タノック　ドッドウエル ビー・エム・エス
ミカミ　三井物産エアロスペース　日立国際電気

危機管理体制

大分県
ワールドカップ開催県が再認識した不測の危機

愛媛県
水際の体制を強化する四国唯一の原発立地県

香川県
台風大災害の教訓で再認識した自助の大切さ

2007 5
Security Specialist Association

企業戦略
CBC株式会社

注目の企業紹介
株式会社 セイユウ

Info
特定非営利活動法人 NBCR対策推進機構
特定非営利活動法人 日本情報安全管理協会
特定非営利活動法人 日本防犯学校
学術社団 日本安全保障・危機管理学会
American Society for Industrial Security

連載
ニーモニックNEWS
ザ・ボディーガード
防犯・防災グッズ
しあわせ通信

巻末特集
セキュリティ業界有力企業一覧

JILCoM 特定非営利活動法人 日本情報安全管理協会

狙われる情報、高まる危機管理意識

～情報セキュリティの一環としての盗聴対策～

特定非営利活動法人 日本情報安全管理協会
業務推進部課長代理 菅原　哲

現代の盗聴事情と盗聴対策の必要性

情報セキュリティの重要性が叫ばれる昨今、日本企業においての情報セキュリティは、ITセキュリティに特化していますが、それだけでは情報資産を守る為の対策としては充分ではないことは皆様お気付きのことと思います。

情報の型式はデータや書類だけではなく、会話等の音声情報も含まれます。盗聴により音声情報を盗み出すことは、会議等で話し合われている情報をリアルタイムで盗み出すことができる唯一の手段であり、産業スパイが情報収集に使う手段の一つです。しかし、現在の日本企業における情報セキュリティは、書類やデータの管理は行われておりますが、音声情報を保護する為の対策がほとんど講じられていないのが現状です。それに対し欧米では、音声情報の重要性を認識し盗聴対策を定期的に行っており、企業の情報セキュリティに、盗聴対策が含まれることが一般的です。経済のグローバル化が進む中で、諸外国における産業スパイの高度な盗聴技術が、日本国内でも用いられているのが現状であり、日本企業においても情報資産の保護の為には、諸外国と同等の盗聴対策が不可欠です。

日本でも盗聴対策の重要性が認識され始めており、現在当協会でも株主総会や重要な会議の前などは、産業スパイ等による情報漏洩に対処する為、数多くの依頼を受けています。盗聴探査の実施については機密保持契約により表立っては知られておりませんが、日本企業においても情報セキュリティの一環として、定期的に盗聴探査を実施する企業は増加傾向にあるのです。また、取引を行う際の契約条項に「定期的に盗聴探査を行っている」ことが加えられているケースも増加しております。

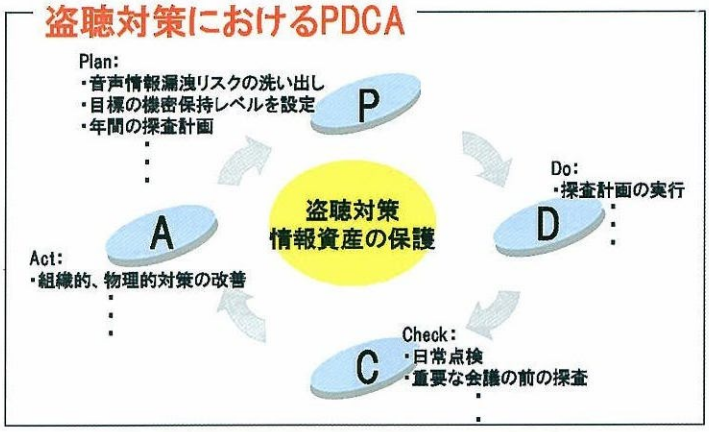
しかし、日本で盗聴対策を行っている企業はまだまだ少なく、セキュリティ意識の低い日本企業が、日本に進出してきている多国籍企業からターゲットにされていることは事実です。グローバルな競争に勝ち残る為に、日本の高い技術情報や経営情報等が盗み出されているのが現状なのです。情報漏洩は企業にとって多大な損害を与えます。企業の経営者は日ごろから、「見えざる侵入（盗聴）」の危険にさらされていることを認識し、対策を講じておかなければなりません。セキュリティの一環として、音声情報漏洩の対策を行うことが必要なのです。

盗聴対策とゾーニング

盗聴対策を行う場合、ゾーニングの考え方と同様に、機密レベルを設定し対策を講じるとより効果的です。レベルの高いエリアを中心に盗聴対策を講じることが重要なのです。

レベル設定を行う際に注意すべき点は、音声情報の機密性を考慮することです。ゾーニングによる侵入防止の観点と盗聴対策による音声情報漏洩防止の観点では、機密レベル設定の観点が異なります。一方ではセキュリティレベルが低くても、もう一方では高いとされているエリアもあります。例えば、資料室やサーバルームは、ゾーニングの観点から見るとレベルの高い位置づけになりますが、盗聴対策の観点から見ると音声がほとんどないエリアである為、低いレベルの位置づけとされています。観点の違いにより機密レベルが異なるのです。

書類やデータを管理する際に機密情報レベルを設定（極秘、社外秘等）し、情報の利用者や部署を制限することで機密性を維持しているのと同様に、音声情報についても各エリアの利用者や音声情報を考慮し、機密性によってレベルを設定することが重要です。例えば役員室や会議室では、企業にとってのキーパーソンが経営に関わるような重要な会話を行うエリアである



為、最も機密レベルが高いと言えます。この様なエリアでは、盗聴探査を毎月、最低でも会議前には行う必要があります。

盗聴対策における PDCA

盗聴対策においても他のセキュリティと同様に、PDCA サイクルで運用することができます。エリアごとに機密レベルを定め、それを維持できるよう目標をたて実行していかなければなりません。それにより、情報セキュリティの強度を高め、情報資産の保護に繋がるのです。

機密レベルを維持できるよう、リスク低減目標を設定し、年間を通した盗聴探査スケジュールを計画します。盗聴器は探査を行った翌日から、盗聴者に新たに盗聴器を仕掛けられる可能性もゼロではないので、探査を一回実施しただけで安心しきってしまうのではなく、定期的に探査を実施し安全な状態を維持することが必要です。

また、盗聴探査だけではなく様々な観点から、エリア内で取り扱われている情報、リスク、機密性を考慮し対策を講じなければ、セキュリティホールを縮小させることはできません。セキュリティホールを縮小させる為には、トータルでセキュリティを構築することが必要です。様々な対策が複合的に作用し、セキュリティホールを縮小させます。従って PDCA のサイクルを構築する際に、盗聴対策以外の対策も考慮することが必要です。

日本企業がグローバルな競争下で勝ち残っていく為には、情報セキュリティの一環として盗聴対策を行っていく、情報を価値ある資産として守ろうとする姿勢こそが必要であり、真のセキュリティであると言えるのではないでしょうか。当協会としても、日本企業が真にセキュリティの必要性を認識し、発展していくためにより一層、啓蒙・啓発活動に力を入れていく所存です。

お問い合わせ先
特定非営利活動法人：日本情報安全管理協会 事務局
〒108-0073　東京都港区三田2-14-5　7F
TEL：03-5765-7677　FAX：03-5765-3181
URL：http://www.jilcom.or.jp　E-MAIL：jilcom@aioroe.ocn.ne.jp