趣味と実益のために情報セキュリティ方針を打ち破る

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

組織の情報セキュリティ戦略の主要なコンポーネントの1つは、セキュリティ方針です。これは、組織の環境に影響を及ぼすあらゆるアクティビティに遵守させ且つ、関係するすべての登場人物の責任と役割を定義した情報セキュリティの戦略および原則を規定する義務的かつ高水準の管理文書です。修辞的な比較として、情報セキュリティ方針は、憲法（あるいはマグナカルタ）が国家にとって何であるかを組織に伝えるようなものだと言えます。

しかし、組織の物理的または論理的資産と同様に組織の文書および管理といったコンポーネントには脆弱性があり、セキュリティおよび運用に影響を与えるために悪用される可能性があります。残念ながら、この種の脆弱性は「従来の」リスク分析では考慮されておらず、組織は「順法闘争」などの潜在的な攻撃にさらされてしまいます。

David Eduardo Acosta R.、CISA、CRISC、CISM、BS 25999 LA、CCNA Security、CEH、CHFI Trainer、CISSP Instructor、PCI QSA、OPST
情報セキュリティコンサルタントであり、コロンビア国軍の専門予備官の中尉。現在、スペインのバルセロナにあるインターネットセキュリティ監査員を務めており、スペインの支払カード業界セキュリティ基準審議会の標準を専門とするウェブポータルである*PCI Hispano (www.pcihispano.com) 彼はIEEEの正会員です*。また、彼はIEEEの正会員です。連絡先： dacosta@ieee.org

ユニオン化されている状況における「順法闘争」

「順法闘争」または「合法的遅滞」(rule-book slowdown)」とは、労働者が文脈化や手順の詳細の中でのエラーを悪用するものでこれらを可能な限り厳密かつ最も細かく言葉通りの方法で適用することで遅滞や組織の生産性の改変につなげる産業活動の一種です。労働の明示的な一時停止を含む伝統的なストライキとは異なり順法闘争では労働者に割り当てられたタスクは中断されず、確立されたルールに対するコンプライアンスの欠如もありません。これは、包含し修正することでそれらをより効果的且つより困難にしようとするものです。多くの場合、この種の産業行動は隠密裡に組織的な方法で開発され経営陣をその影響や処理する手段から隔離させます。

この種の行為を最も起こしやすいセクターの1つとして、医療セクターが挙げられます。[1] この分野では、患者、医療従事者の両方に対して患者、検体、医薬品の衛生管理および取扱いの妥当性および安全性を保証するため手順書が極めて詳細に示されなければなりません。しかし、これらのプロトコルが特定の方法で書かれ可能な例外を考慮せずに適用される医療環境に調整された場合それらの厳格な実施は、人命の観点からであっても、ケアおよび虐待的な官僚制度における不当な遅延を招く危険にさらされる可能性があります。この圧力を利用することで、ストライキを行う労働者は彼らの要求に沿って確実な遵守が可能になります。さらに、行政当局が産業行動の潜在的な原因を追求する場合、その根源は規制を表現すること自体の欠点にあると明らかにする可能性があります。これは、労働者に対して当初確立された手順に従わないよう要求して非生産的なものにし、産業行動に参加した要員に対する是正措置を講ずるためのツールを使用することなく運用への影響全体に対する責任の受入れを強要する可能性があります。

順法闘争による情報セキュリティ方針の弱体化

前述の概念に従えば、記述が不十分な情報セキュリティ方針を弱体化することは非常に簡単です。これらの文書の大部分は一般的なテンプレートに基づいておりほとんど見直されていません。さらに、組織のビジネスの現実や情報環境の現状に適応していないことを考慮して、例外の管理手順も含まれていないのが一般的です。これらのタイプの規制に厳格に従うことは運用の遅延や情報の完全性、機密性、可用性への影響をもたらす可能性があります。関与するものの一部として「義務遵守要素」を加えることでこのような不具合は順法闘争によって増幅され、財務および運用（サービスレベル契約（SLA））両面での波及効果とともにビジネスの生産性低下の原因にもなります。

さらに、情報セキュリティ方針は必要な義務の程度に応じて重要性が分類される特定の分野／トピックスに重点を置く補助文書によってサポート且つ補完されます。これは規制、基準、手順書、技術指導、ガイド、勧告などについての状況です。組織の規制の枠組みの中のコンポーネントのいずれかを通して順法闘争の実施が可能になります。

以下は、情報セキュリティ方針または脆弱な補助文書に関する順法闘争の例です。

- ある企業の情報セキュリティ方針では、「マルウェアに感染しやすい全てのオペレーティングシステムに対して最新版に更新されたウイルス対策ソリューションをインストールする」ことを義務付けています。しかし、この組織では、コンピュータプール内にPOS（point-of-sale）端末として限定的に使用されるハードウェアを有する一連の拠点を保有しています。これらにウイルス対策ソフトウェアを強制的にインストールすることで順法闘争を実施できます。その結果、パフォーマンスと可用性に影響を与え顧客への応答時間や日常的取引と売上に対する応答と同様に、通常操作の応答にも悪影響が及びます。
- 情報セキュリティ方針では、製造者からのリリース後1ヶ月以内にセキュリティアップデートをインストールすることが義務づけています。指示された時間枠を単に遵守するだけで重要なコンポーネントへの予定外の更新に対する順法闘争を適用することができます。これはサービスの可用性に影響する可能性があります。
- パスワード管理に関して、方針には「忘れてしまったパスワードの変更はユーザーの身元を物理的に検証する必要があります」と記載されています。ユーザーが市内または国内にいない場合、変更を担当する管理者はこのチェック業務に順法闘争を行いユーザーのアクセスに影響を与える可能性があります。

> **“お粗末な情報セキュリティ基本方針を作成するのは簡単なことです。”**

更なる例は、変更管理およびユーザー管理に関する方針の実装に見ることができます。リクエスト、承認、実施の段階は非常に厳格に行う傾向にあり暗黙の形式主義的な対応は順法闘争のプロセスを悪用となり会社の通常業務に影響を与えます。

残念ながら、この問題の影響を受けた組織は、その労働者をセキュリティ方針のコントロールに背かせて自己矛盾を生じさせることはできません。規制を無効化するからです。したがって、会社は処置に頭を抱えることになるでしょう。

Enjoying this article?

- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

セキュリティ方針を順法闘争攻撃から保護する

前述の説明から、順法闘争で悪用される脆弱性は通常、表現上のエラー、例外管理に関する問題、更新の欠如、会社の現実を反映せず運用期間が不適切なセキュリティ方針またはその補助文書の設計に関連するものと簡単に結論づけられてしまいます。この種の誤りは、一般的にセキュリティ文書は官僚的手続きの目的を埋めるものとしてしか使われておらず、開発者、オペレータ、システム管理者、および一部の誤った指示を受けたセキュリティ責任者はありふれた欠点を含むその文書を読んだことがないという考えに由来しています。

> **“セキュリティ基本方針は、保護する環境に背くのではなくむしろ適応するために設計されなくてはなりません。”**

このリスクを回避するにはセキュリティ方針を作成／実施する際に、以下の一連の前提を念頭に置く必要があります。

1. **仮想シナリオを使用して定期的にテストを実施し、悪意のあるユーザーに悪用される可能性のある方針の不具合を特定します。**規制の枠組みの弱点を悪意ある従業員に悪用される前に特定するためには経営陣はシミュレートされた状況において情報セキュリティ安全方針の適用を伴う演習を行うことが必要です。それにより、企業内の重要な分野の従業員（すなわち、法務、人事、広報、物理的セキュリティ、事業継続）が仮想シナリオのもとで対話できるようになります。この種の演習は、インシデント対応および事業継続の計画で非常によく行われています。また、そのテスト方法も情報セキュリティ方針に適用できます。

順法闘争により悪用される可能性のある問題を検出するには、セキュリティ方針に関与する状況（シミュレーションの原則）を分析し規制の枠組みで説明されている手順を段階的に実行する必要があります。プロセスにより通常運用に悪影響を及ぼす可能性のあるタスクまたはガイドラインが検出される場合、または例外が考えられる場合には、詳細に検証を行い以下の基準を適用します。

2. **組織の情報セキュリティの背景を分析し、セキュリティと運用上のコントロールのバランスをとるよう試みます。**セキュリティ方針は、保護する環境に反するではなくむしろ適応するために設計されなくてはなりません。そのため、組織は情報や文化的環境を保護するために事前の詳細把握が必要でその手順書は以下のようなものになります。

   - **論理的** – 手順書は可能な限り自然であり組織の現在の運用と整合していなければなりません。同様に、潜在的な既存の脅威に基づいてコスト／便益基準を遵守しなければなりません。企業の現実に適合していないコントロールを導入すると焦点が狭すぎたり、または逆に広すぎたりしてそれが組織にとって不必要な装いであることを証明してしまうことがあります。この時点において他の組織の経験はレビュー目的（ベンチマーク）に役立ちます。
   - **正確性** – 方針は、組織のセキュリティニーズに重点を置きこれを正確に説明している必要があります。いかなる逸脱にも潜在的な脆弱性を引起こす可能性があります。モジュール化はこの時点で重要な要素になります。
   - **簡潔性** – 方針は、その理想を表現するために最低限必要な言葉のみを用いて表さなければなりません。馴染みが無く無駄な、または不必要な専門用語、または概念を曖昧にして誤解を招く

可能性のある文言の使用は避けるべきです。簡潔さが必須です。

- **適時性** – 基本方針は常に最新なものでなくてはならず、適用される環境の現状とニーズを記述しなければなりません。変更とコントロールの不均衡は、セキュリティレベルの低下を招く可能性があり対策と保護の導入時における脆弱性を許容してしまいます。
- **明確性** – 方針は、対象となる聴衆（つまり、ユーザー）を念頭に置いて作成する必要があります。文書を読んだ誰もが、外部の参照例に頼ることなく内容を理解できるようにしなければなりません。つまり、専門用語の使用は最低限必要なものに制限し出来るだけ簡単な言葉を利用することが求められます。
- **完全性** – セキュリティ方針は、5つのW（およびH）の最大値に準拠する必要があります。[2]
  – 誰が？
  – 何を？
  – 何処で？
  – 何時？
  – 何故？
  – どのように？

  ガイドラインにこれらの要素が含まれていないと現実的な正当性を欠くことになり、重視されない不必要なコントロールであることを示してしまいます。
- **目的** – 基本方針は第三者が書き、特定の個人、技術または領域に対する偏見または好みによりガイドラインが選択されたことを示すような主観的要因は排除されるべきです。

このガイドラインは、方針の作成作業（またはレビュー／再評価中）の完了時には、不必要な要素や脆弱な要素を特定するためにリスト化されたフィルタに基づいて分析する必要があります。

3. 補完的コントロールおよび例外に対する評価基準を確立します。技術分野での不可避の変化と新たな脅威に適応する柔軟性は、妥当性と流通性を確保するためのセキュリティ方針の重要な要素となるべきです。基本的な防護措置を構成する抑止、予防、検出、是正、回復を目的としたガイドライン（その中に基本方針そのものが見出されます）に加えて、補完的コントロールも不可欠です。補完的コントロールとは、当初確立されたガイドラインの使用を許容しない正当な行政上または技術上の制限（例外）がある場合に実行できる代替コントロールとして定義されます。[3] これらのタイプのコントロールは、元のレベルと同等またはそれ以上のレベルのセキュリティを可能にします。

> **“インセンティブの使用は、この種のイニシアチブに関与するように要員を説得するためのツールとして導入することができます。”**

更に、緊急事態に備えて特別な評価基準を確立することも不可欠です。これらは例外的な評価基準として知られており、予期せぬ状況への対処やコントロールの失敗、予期しない活動への対応策として役割を事が果たすことができます。

4. 方針へのユーザーからのフィードバックを得るためのコミュニケーションメカニズムを定義します。双方向コミュニケーションチャネルの構築により、管理者はユーザーから日常な運用経験に基づいて基本方針に適用可能な直接情報を収集することができます。問合せフォーム、提案ボック

ス、オンラインチャット、またはその他のソーシャルネットワークツールは、エラーを早期に検出し予防的な修正を可能にするフィードバックを収集するための有効なチャネルです。

インセンティブの活用はこの種のイニシアチブに関与するように要員を説得するためのツールとして導入することができます。

> “インセンティブの使用は、この種のイニシアチブに関与するように要員を説得するためのツールとして導入することができます。”

5. **セキュリティ方針の定期的な見直しスケジュールを設定し、環境に重大な変更が生じた場合には更新します。**文書のレビューとそのレビューのトリガーとなる期限およびシナリオは、技術の変化、サードパーティの入退場または外部企業への業務委託（つまり、アウトソーシング）、および環境の重大な変化として分類されるような買収/合併といった変化を含めて方針自体に確立されなければなりません。

さらに、セキュリティ責任者は環境内の脅威に合わせたセキュリティ方針のコントロールを維持することが不可欠です。これにより、この文書の適用が有効で会社の現実に合致しており時代遅れまたは不必要なガイドラインとならないことが保証されます。

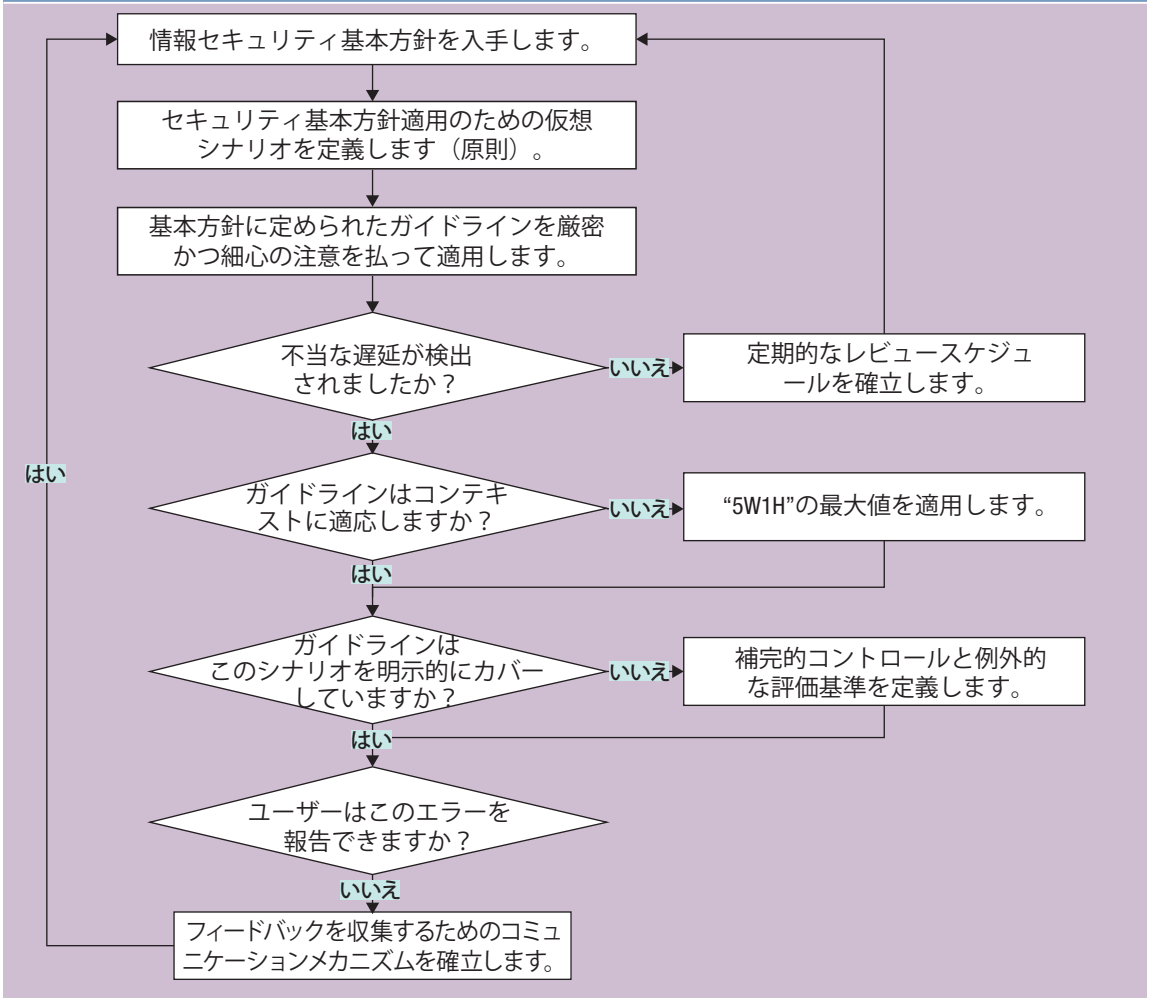
検証の流れは概ね**図1**のようになります。

結論

セキュリティ方針は、組織が管理する情報に基づき様々な資産の重要度に応じてそれらを保護するための要件とコントロールを設定する必要があります。前述のガイドラインの表現方法により過度の「ゆるみ」または制約のいずれかに起因する欠陥が存在する可能性があることから、方針のフレージングは重要な要素になります。これらに脆弱性があることは、最も厳格な形でガイドラインに追随する順法闘争を使用する悪意のあるスタッフの厳しい官僚主義の目標となりえます。方針が最新のものではなく組織の運用上の現実に合致せず例外管理が許されなければ、この種の産業行為や妨害により会社の情報セキュリティの取扱いに重大な影響がもたらされる可能性があります。

この問題を防止・管理するには、関係者との双方向コミュニケーションチャネルの方法論的適用、文書内の潜在的な不一致を調べる定期的なテストの管理、規制文書の再検討、補完的コントロールと例外的な手段の使用、組織の状況とガイドラインのコスト／便益の定義に関する継続的な分析が必要となります。これらのタスクは、方針が「空言（そらごと）」となってしまうのを防ぐために行われるものです。方針が空言化してしまうことは、遅かれ早かれ、会社自身にとっての脅威になります。

図1 – 順法闘争を回避するセキュリティ基本方針に対する更新の検証フロー



原典：David Eduardo Acosta R（許可を得て転載しています）

後注

1 ABC España、「Los enfermeros convocan una huelga de celo por el decreto que les impide prescribir medicamentos」（2015年10月28日）、*www.abc.es/sociedad/abci-enfermeros-convocan-huelga-celo-decreto-impide-prescribir-medicamentos-201510281549_noticia.html*

2 Spencer-Thomas, O、「Writing a Press Release」（2012年3月20日）、*www.owenspencer-thomas.com/journalism/media-tips/writing-a-press-release*

3 Williams, B、「The Art of the Compensating Control」（2009年3月）、*https://www.brandenwilliams.com/brwpubs/TheArtoftheCompensatingControl.pdf*