情報セキュリティ保護

ーコンピュータフォレンジックへの取り組みー

アブストラクト

１．研究の背景と課題認識

情報セキュリティ事故の事後対策としてのコンピュータフォレンジックの出現　「コンピュータフォレンジック」という言葉はまだ日本では耳慣れないが、法的対応のために情報セキュリティ事故（以降“事故”と表す）発生時において、デジタルデータの証拠性を確保し原因を追究することを意味している。従来の防衛のためのセキュリティ対策に対し、コンピュータフォレンジックは事故発生時の対策に重点が置かれている。

事故発生時の対応の遅れは致命的ダメージとなりうる　昨今、企業は情報セキュリティへの関心を高め防衛対策を強化しているが、事故は増える傾向にあり、事後対策の重要性が増してきている。しかしながら、事故が発生した際に企業はどう対処すべきか、また事故を想定して事前対策として何を行っておくべきか、確たるものがまだない状況である。事故発生時に万一対応が遅れると、被害の拡大だけでなく企業の社会的信用の失墜につながり、致命的ダメージとなりうる。このような事態を避けるためには、事故発生後できるだけ短時間で原因を特定し然るべき対応をとることが肝要である。

今、企業が行うべきコンピュータフォレンジック対策　当分科会では、まだ手順が確立されていない「事後対策を想定した事前対策」を企業に導入する際に、どのような手順で何をしておけばよいかを明らかにすることを目標に、これを企業のコンピュータフォレンジック対策と位置づけ研究に取り組んだ。

２．研究アプローチ

事故が発生した場合の対応は「どの情報が、誰によって、いつ、どこから、どうされたのか」という原因を特定することが第一に必要である。当分科会では下図のように、①守るべき情報と②脅威の想定を行い、次に③標準的な仮想ネットワークと④情報保管場所別の事故と侵入経路を想定し、情報保管形態別の脅威マトリクスとして整理した。さらに、コンピュータフォレンジック対策として、⑤守るべき情報に辿り着くまでの経路上の乗り越えなければならないセキュリティゲート（以下“「壁」”と表す）を事故別に特定し、その「壁」ごとの⑥ログ収集対策と⑦事後追跡手順検討という流れで研究を進めた。さらに事故発生時の対応フローとして⑧事後ワークフローを作成した。

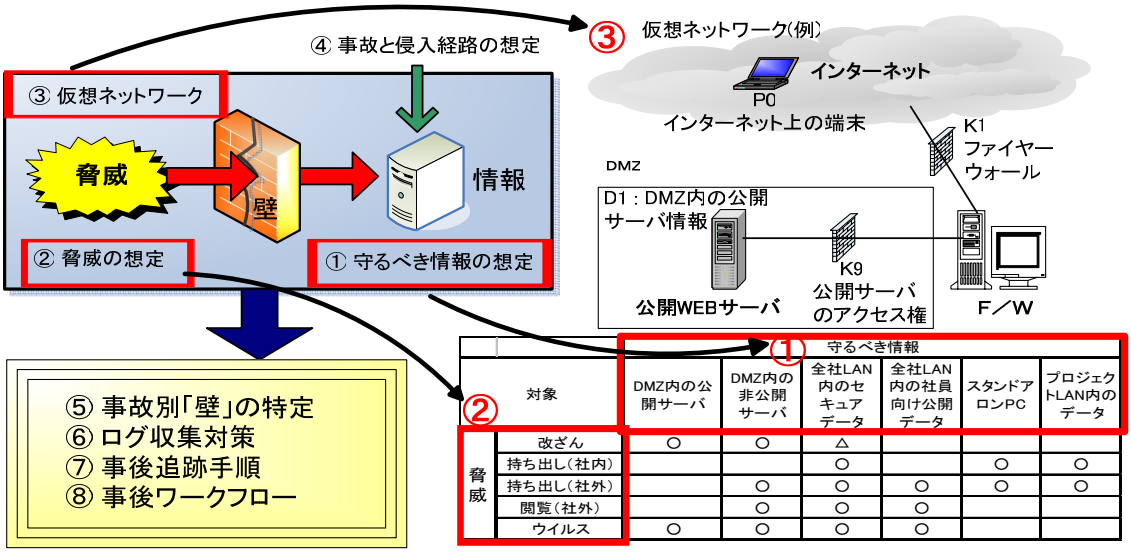

図１　研究アプローチ

３．研究成果

３．１　事故発生を想定した事前対策事例集

企業が事故発生を想定して事前対策を立案するためには、守るべき情報を特定し事故の想定を行った上で必要となるログ収集対策を検討し、さらに想定した事故が発生した際の追跡手順を明確化しておく必要がある。これら一連の作業を行う際に、この事例集によりその具体的内容と手順が一目瞭然となる。

項目		内容
守るべき情報		DMZ内の公開サーバ情報
事故	HP改ざん	部外者がHP上の写真を書換(不正アクセス)
		……
漏えいルート		P0→K1→K9
事前対策	壁	①確認内容②収集可能ログ③ログ収集対策
		……
事後対策	手順	1. WEBサーバ停止 …… 12. 侵入元IPアドレスの管理元に調査依頼

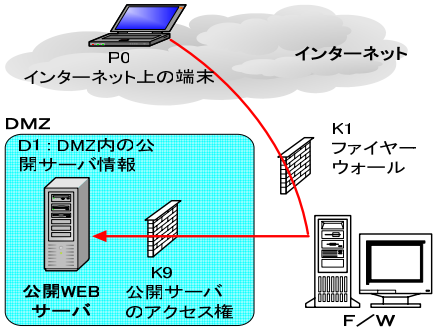

図２　事故発生を想定した事前対策事例集（抜粋）

３．２　コンピュータフォレンジック対策手順

事故発生を想定した事前対策事例集により事故に対する技術的対策は明確になったが、さらに事故が発生した際に企業としてとるべき対応の手順化が重要である。当分科会では、警察・法務・セキュリティの専門家よりヒアリングを実施し、情報漏えいを例として事故発生時の対応手順を“事後ワークフロー”としてまとめた。企業が対応手順を策定する際に、この事後ワークフローを雛型として利用できる。

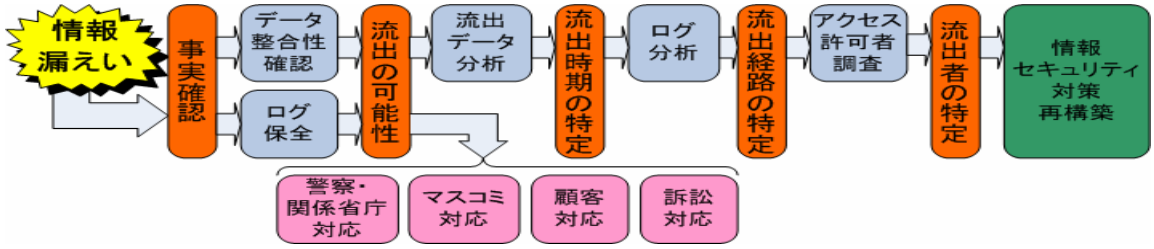

図３　事後ワークフロー（抜粋）

４．評価と提言

今後ますます多発するであろう事故に伴う被害の拡大を最小化するために、企業はこれまでのセキュリティ対策を見直して事後対策を加えた新たな対策を構築すべきである。

今回当分科会では、従来の対策をコンピュータフォレンジックという観点で見直し、事故発生を想定した事前対策事例集、および事後ワークフローとしてまとめた。これらの成果を、今後企業がセキュリティ対策を強化する際に活用することにより、セキュリティ対策を次のステップであるコンピュータフォレンジック対策へと繋げることが可能になると自負している。また当研究を通じて、参加メンバーがコンピュータフォレンジックに関して深く理解し、自社にその成果を持ち帰ることができたことも大きな成果である。

最後に、この一年間でコンピュータフォレンジックに関するツールもいくつか出てきた。しかし、この分科会の期間内ではツール評価をできる状況ではなかったため、簡単な調査に留めた。今後増えてくると思われるこれらコンピュータフォレンジックツールの活用に関しては、継続した研究の場を設けていただくよう、ここに提言したい。

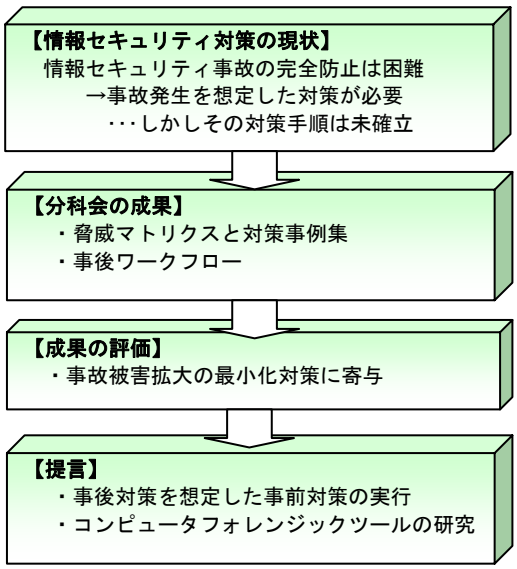

図４　評価と提言