2007－ＣＳＥＣ－38（９）
2007／7／19

ソーシャルエンジニアリングの分析およびアクセス制御の提言

矢竹 清一郎†, 内田 勝也†
† 情報セキュリティ大学院大学

業務処理の高度化と処理速度の飛躍的増大、および、内部統制機能の変化により、組織における管理者は技術的側面だけでなく、組織的側面の対策を実施することが求められている。近年、脅威は多様化している一方、ソーシャルエンジニアリングを利用し、簡易に貴重な資産を盗み出す事件も発生している。ソーシャルエンジニアリングとは人間の行動的側面・心理的側面を巧みに利用し、情報の取得・改ざん・破棄を受動的、能動的に実施させる手段である。本論は、情報システムを利用する人間と情報システムとの間で、ソーシャルエンジニアリングを利用し情報を入手する脅威に着目し、ソーシャルエンジニアによる情報開示要求に対するシステム的対策の検討をする。特にシステム的対策に関しては、従来のアクセス制御に加え、セキュリティポリシーとアクセス制御技術を紐付けることにより、より強固なセキュリティ対策を提言する。

Analyzing Social Engineering & Managing Access Control against an Information Disclosure Demand

Katsuya Uchida†, Seiichiro Yatake†
† Institute of Information Security

Developing information technology and hardware technology or changing Internal Control makes System Administrators and Managers consider not only many information technologies to make organizations become more secured but also attackers' motivation and organization's vulnerability. Recently the threat has become diversification, many attackers take advantage of simply "Social Engineering". Social Engineering can be regarded as 'people hacking', basically its hacker jargon for soliciting unwitting participation from a person inside a company rather than breaking into the system. Many attackers take advantage of human's vulnerability or human behavior and look out the important information which is the ways to gain access to valuable resources.This paper discusses about examining the vulnerability which is between human and information systems, and studying access control against Social Engineer's information disclosure demand, especially "security policy" & "access control technology".

１．はじめに

IT技術の革新により一人１台のコンピュータの利用とインターネット接続が利用できることが当たり前となっている。そのため、以前は一部の専門家しか利用できなかったシステムが、現在は多くの人が利用できるようになっているため、従来の物理的・技術的対策だけでは、情報セキュリティを確保できない状況となっている。

近年の”おれおれ詐欺事件等”にも見られるように、攻撃者は単に技術的な手法で攻撃するだけではなく、ネットワーク、コンピュータ、電話等を利用するユーザの行動的側面や心理的側面を巧みに利用し、情報資産・重要情報を盗み出そうとする。このようなことから、心理学と情報セキュリティとを紐付けて研究を行うことは、重要な観点であると述べている。【1】

２．研究背景

ソーシャルエンジニアリングに関連した事件はこれまで発生していたが、研究分野においては極めて浅く、研究事例は未だ少ない状況である。

ソーシャルエンジニアリングは、様々な文献において以下のように定義されている。【2】【3】【4】内田らはソーシャルエンジニアリングとは、目的とするシステムを技術的な攻撃を利用して侵入を図るものではなく、人間の行動的側面・心理的側面を巧みに利用し、情報の取得・改ざん・破棄を受動的、能動的に実施させる手段と定義している。【1】

ソーシャルエンジニアリングは、元来は人対人とのやりとりから、重要な情報を取得するというものであったが、近年は”人”対”人”だけでなく、”人”対”システム+人”とのやりとりから、重要な情報を取得することも含むようになっている。そこで、本

研究では、情報システムを利用する人間と情報システムとの間で、ソーシャルエンジニアリングを巧みに利用し、攻撃者が情報を入手することに対する対策を検討する。

3．ソーシャルエンジニアリングについて

3．1　要求事項による分類

ソーシャルエンジニアは以下の 3 つのパターンにより、情報を取得する。

- 直接的に情報を要求し、被害者が情報を提供する。(情報要求型)
- 間接的に行為を要求し、被害者が情報を提供する。(行為要求型)
- 被害者が無意識な間に情報を提供する、もしくは情報取得の機会を提供している。

以下にその 3 つのパターンに関して記載する。

- 直接的に情報を要求し、被害者が情報を提供する。

図 1 に示すようなフローで情報を提供する。被害者は重要な情報を渡していることを意識することなく、記憶・電子媒体・Web システム・ファイルから情報を提供する。

【事例】

パスワード・会社情報 (社員名簿)・個人情報・コンピュータ情報・経営情報等を電話・リバースエンジニアリングを通じ取得する。

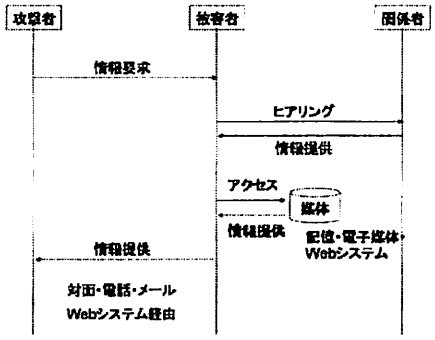

図 1. 情報要求型

- 行為を要求し、間接的に情報を取得する。

図 2 に示すようなフローで情報を提供する。

被害者は自分自身が実施している行為は重要な情報を渡していることを意識することなく、記憶・電子媒体・Web システム・ファイルから情報を提供する。

【事例】

- 無料のソフトウェアやパッチを送ってインストールさせる。懸賞つき Web サイトの上で、ユーザ名や・パスワードの入力を求める。
- 受付嬢に FAX の受信と転送を依頼する。
- E-mail 内の偽りの URL を押させる。
- まぎらわしい URL やドメイン名にして、偽りの URL にリンクされたものを押させる。

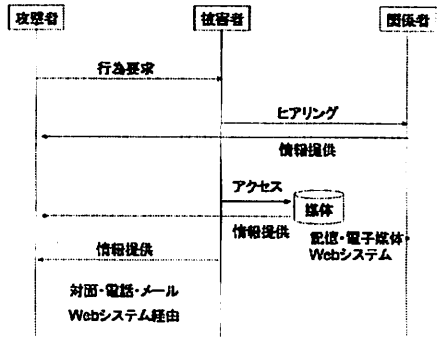

図 2. 行為要求型

- 被害者が無意識で情報提供する、もしくは情報取得の機会を提供している。

図 3 に示すようなフローで情報を提供する。

また、被害者が無意識な間に社内に侵入される、ゴミ箱をあらされるといった情報取得の機会を提供している場合も、本分類に含まれる。

【事例】

- パスワードをキーボードに入力している場面を見る。
- ディスプレイ等に張り付けた付箋紙に記入してあるパスワードを見る。
- 清掃員になりすまして(あるいは本当に清掃員になるか、または本当の清掃員を共犯にする事も考えられる。) 内部でゴミをあさる。

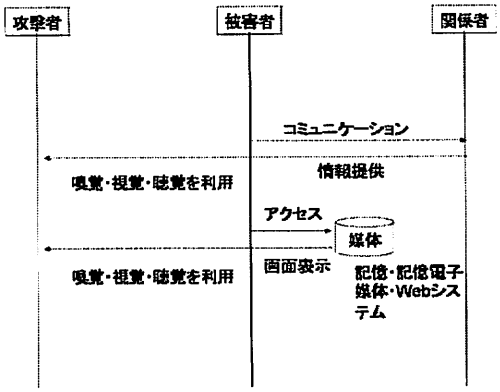

図3. 無意識による情報提供

3．2　攻撃対象による分類

ソーシャルエンジニアリングを攻撃対象により分類する。ソーシャルエンジニアリングによる攻撃対象として、「攻撃者 vs 物」「攻撃者 vs 人」「攻撃者 vs 人+システム」の3種類があげられる。以下に示す。

表1. 攻撃対象による分類

攻撃対象	攻撃方法
攻撃者 vs 物	清掃員のふりをして、ゴミ箱をあさり、情報を盗み出す。 シュレッダーにかかった紙を復元する。
攻撃者 vs 人	ベンダ・パートナー企業、警察、などの社員/職員のふりをし、建物の中に侵入する 会社の専門用語を駆使して社員になりすます。 会社のメールルームに文書を放り込んで社内に配達させる
攻撃者 vs 人+情報システム	ベンダやシステム企業のふりをしてパッチや新バージョンを提供し、システムを破壊する。 認証つきWEBサイトの上でユーザ名やパスワードの入力を求める。 権威や権力のあるもののふりをし、アクセス権限を変更させる。 権威や権力のあるもののふりをし、機密情報（電子ファイル）を開示させる 再ログインやパスワードの再入力を求めるためのポップアップウィンドウを出す

4．現状のセキュリティ対策の課題

攻撃者による情報開示要求に対する現状のセキュリティ対策の課題を抽出する。
3 章にて示したように、情報開示には情報要求型・行為要求型がある。以下にそれぞれの対応策に関して述べる。

4．1　情報の要求による対応策

一般的なセキュリティ対策として、情報への要求種類に応じて、図 4 に示すように以下の行動を取る。【2】

- どんな状況でも決して開示しない
- 開示基準に従う
- 内部・秘密・極秘など各情報の機密区分に従う

したがって、どのような開示基準が設定されているかが、ソーシャルエンジニアリング対策の課題となる。

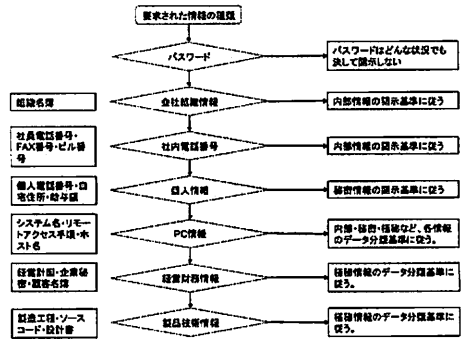

図4. 情報の要求に対する対策フロー

4．2　行為の要求による対応策

攻撃者から行為を要求された場合、対応策として図 5 に示すように以下の行動を取ることが推奨される。【2】

- 機密区分と開示基準にしたがって判断する
- 社員確認手順に従う。

したがって、どのような開示基準・社員確認手順が設定されているかが、ソーシャルエンジニアリング対策の課題となる。

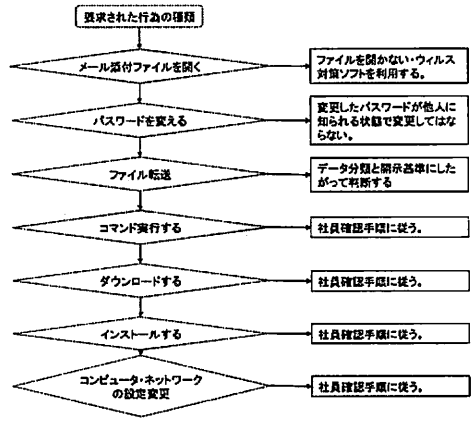

図5. 行為の要求に対する対策フロー

いずれの要求においても、情報開示基準・セキュリ

ティポリシに依存している。また、システム的セキュリティ対策として、情報開示基準に則ったアクセスコントロールも課題として考えられる。次項でそのアクセスコントロール及び、アクセスコントロールの課題に関して検討する。

5．現状のセキュリティ対策の課題

本項では、情報開示要求に対するシステム的セキュリティ対策に関して検討する。

5．1　現状のシステム的対策の課題概要

現状のシステム的セキュリティ対策としてアクセスコントロール以外にも認証技術・暗号化技術があげられる。それぞれの用途は以下の通りである。【5】

- 暗号化技術

送信者が以下の対策を実施したい場合に情報を暗号化する。

盗聴対策　「第三者に閲覧される」

改竄対策　「第三者に改竄される」

なりすまし対策「第三者があたかも本人にみせかけて送信する」

- アクセス制御技術・認証技術

不正アクセス対策「第三者がアクセスする」

改ざん対策「第三者がアクセスし、読み取り・書き込み・実行・削除を実施する」

しかし、上記のセキュリティ対策を実施しても、攻撃者は情報利用者のファイル操作を巧みに利用して、情報開示を要求することや、情報を送るように促す。したがって、セキュリティ対策として、情報を利用するためのファイル操作を分析すること、開示範囲と機密区分の対応を検討することが大切となる。

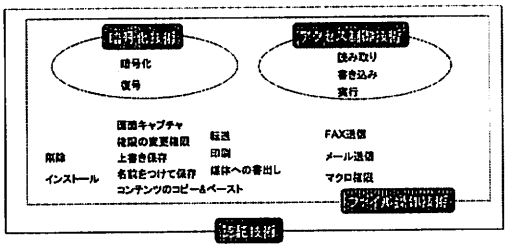

図6. 現状のシステム的対策の観点

5．2　セキュリティ対策の検討観点

本項で情報開示要求に対するシステム的セキュリティ対策の検討観点について示す。

- 機密度とアクセス権限技術

アクセスコントロールは、多くの企業において図7に示すように、機密度－権限－開示範囲に基づいて決定されているが、図8に示すように複数の軸での検討が必要になる。

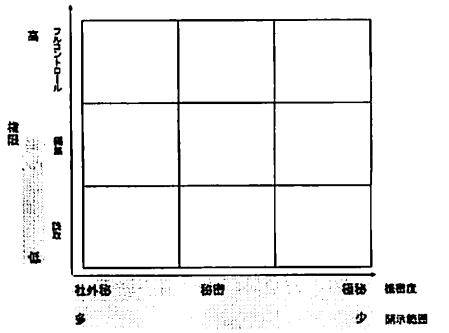

図7. 機密度とアクセスコントロールの従来の考え方

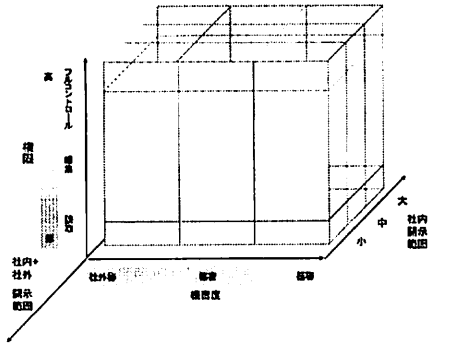

図8. 機密度とアクセスコントロールと開示範囲

図9に示したように、近年ファイル操作が多様化していることから、アクセスコントロールは表2アクセスコントロール権限 に示すように複数のファイル操作を管理する必要がある。

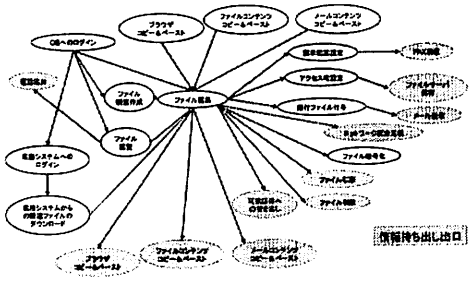

図9. ファイル編集時のユーザ操作

表2. アクセスコントロール権限

番号	権限	内容
1	暗号化権限	ファイルを暗号化する権限
2	復号権限	暗号化されたファイルを平文にする権限。
3	更新権限	ファイルを更新し、上書き保存できる権限
4	別名保存権限	作成中のファイルに対して、別名のファイルを保存することができる権限
5	読取権限	ファイルを閲覧することができる権限
6	削除権限	ファイルを削除することができる権限
7	コピー&ペースト権限	ファイルのコンテンツをコピー&ペーストすることができる権限
8	印刷権限	ファイルを印刷することができる権限
9	権限変更権限	与えられたファイルの権限を変更することができる権限

5．3　情報開示要求に対するシステム的セキュリティ対策の提言

情報開示要求に対するシステム的セキュリティ対策は業務内容等に応じて当然変動する。そこで、本項では非定形業務・定形業務において、どのような単位で情報を保護するべきかを検討する。表3に示すように、一般的に情報保護の単位として、" 人単位" " 機器単位" " アプリケーション単位" " ファイル・フォルダ単位" に応じて保護できる。

コールセンタや監視センタなどの定形業務の場合、ユーザ毎に操作制限を加える、機器毎に操作制限を加える、アプリケーション毎に操作制限を加えることにより特定の情報開示要求に対する対策を実施することができる。

一方、非定形業務の場合、人単位・アプリケーション単位・機器単位に制御した場合、セキュリティ効果は上がるが、特定の操作ができなくなるため業務効率の低下が伴うため、対策が非常に難しいが、この非定形業務について検討する。

情報保護を、図10に示すようにアクセスコントロール・機密度・ユーザの単位に分類し、制御する方法について検討する。

一般的に情報セキュリティポリシにて、機密度のレベル・ユーザのレベルはある特定の階層に分けられている

表3. 情報保護の単位と業務との関係

番号	保護単位	仕様	非定形業務	定形業務
1	人単位	ユーザに対して、特定の操作制限を加え、情報開示に関連する機能を制限する。 本機能は定形作業をする作業者に対しては有効であるが、大規模な組織においては否定形業務の利用者に対しては、業務効率の低下を伴うことが想定される。	×	○
2	機器単位	情報開示に関連する機能を実施できる端末を限定する。 本機能は定形作業をする作業者に対しては有効である。しかし、非定形作業を実施する作業者に対しては、作業端末を変更して作業を実施する必要があり、業務効率の低下を伴うことが想定される。また、それぞれ専用の端末を用意する必要があり、費用がかかる。	△	○
3	アプリケーション単位	利用する業務システムに関連するアプリケーションに対して、操作制限・行動制限をユーザ毎にあたえ、情報開示に関連する機能を制限する。 本機能は、特定の業務において効果があるが、ユーザの端末操作全体に関して制限を加えることはできない。	△	○
4	ファイル単位 フォルダ単位	ファイルに対して、ユーザごとに操作制限やアクセスコントロールを与え、情報開示に関連する機能を制限する。 本機能は、情報開示への脅威への対策となるが、ファイルが多数になるため、業務効率への影響・セキュリティ対策・ファイル管理に負荷を及ぼす。どのようなセキュリティポリシを設定するかが重要である。	△	△

○：有効　△：要件等　×：非有効

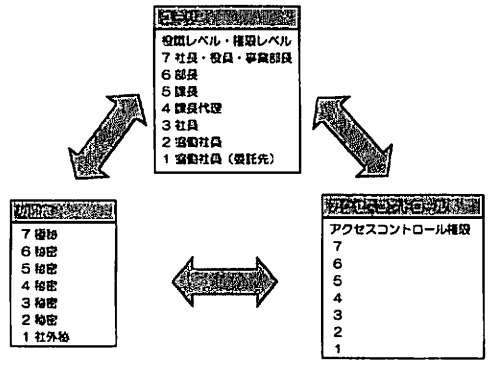

図10. アクセスコントロールの単位

アクセスコントロールに関しては、アクセスコントロール権限がN通りあった場合、考えられる組み合わせは2^N通りとなり管理に負担がかかるため、現場で委任されていることが多い。

そこで、本研究では、表4、表5に示すように" アクセスコントロール権限レベル"、" ユーザレベル"、" を定義する。

表4. アクセスコントロール権限レベル

7	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	×
5	○	×	○	○	○	○	○	○	×
4	○	×	○	×	○	○	○	○	×
3	○	×	○	×	○	○	×	○	×
2	○	×	×	×	○	×	×	○	×
1	○	×	×	×	○	×	×	×	×

表5. ユーザ権限レベル

7	社長・役員・事業部長
6	部長
5	課長
4	課長代理
3	社員
2	社員
1	協働社員

次にアクセスコントロールレベル・ユーザレベルをマッピングし、機密度に合わせ、表6、図11に示すようにセキュリティポリシを提言する。
上記で述べたように、ユーザ・機密度・アクセスコントロール権限それぞれにおいてレベルをわけ、定義したことにより従来のアクセスコントロールと比較し、より細かいアクセスコントロールが実現できるだけでなく、複数のポリシーを事前に用意することで業務効率も考慮したアクセスコントロールが可能となると考えられる。

表6. アクセスコントロールレベル

レベル			
機密	10	ユーザレベル5以上のものにのみ編集許可を与える それ以下のものには権限を与えない	7
	9	ユーザレベル4以上のものにのみ編集許可を与える それ以下のものには権限を与えない	6
	8	ユーザレベル2以上のものにのみ編集許可を与える それ以下のものには権限を与えない	5
	7	ユーザレベル1以上のものにのみ編集許可を与える	1
秘密	6	ユーザレベル5以上のものにのみ編集許可を与える それ以下のものには読取権限を与える	4
	5	ユーザレベル4以上のものにのみ編集許可を与える それ以下のものには読取権限を与える	3
	4	ユーザレベル2以上のものにのみ編集許可を与える それ以下のものには読取権限を与える	2
	3	ユーザレベル1以上のものにのみ編集許可を与える	1
社外秘	2	ユーザレベル2以上のものにのみ編集許可を与える それ以下のものには読取権限を与える	2
	1	ユーザレベル1以上のものにのみ編集許可を与える	1

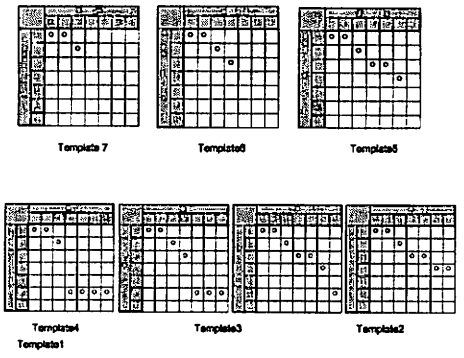

図11. アクセス権テンプレート

6. 結論

本研究では、ソーシャルエンジニアによる情報開示要求に対するシステム的対策・管理的対策に関して検討することにより、以下の結論を得た。
・情報開示要求に対するセキュリティ対策として従来のアクセスコントロールに加え、情報システム利用者の操作に関するアクセスコントロールのポリシーの決定方法を提言した。

【参考文献】

[1] 矢竹清一郎、森貴男、東華枝、山口健太郎、内田勝也, 情報セキュリティ心理学の提案, 情報処理学会 CSEC研究会 2007/03 No16 pp327-331
[2] Kevin D. Mitnick & William L. Simon, "The Art of Deception", Wiley Publishing, Inc., 2002 (岩谷宏訳, 「欺術 ―史上最強のハッカーが明かす禁断の技法」, ソフトバンクパブリッシング, 2003)
[3] Robert. B. Cialdini, "Influence: Science and Practice", Allyn and Bacon, 2000 (社会行動研究会訳, 「影響力の武器 ―なぜ、人は動かされるのか―」, 誠信書房, 1991)
[4] 情報処理振興事業協会, 「国内におけるソーシャルエンジニアリングの実態調査」調査報告書, 2000.1
[5] 上園 忠弘 (著), 山本 明知 (著), 小林 孝夫 (著), 情報システムのセキュリティコントロール, オーム社, 1988/06