全体講評と解答例（情報セキュリティ基盤論 2013）

2013/11/07
佐藤周行

成績がついてからだいぶ時間がたってしまったので、もしかしたらもう興味がないかもしれませんが、例年どおり講評を書いておきます。

今年は、内容の組み替えをしました。クラウドが IT 環境として一般化して、組織も対応を迫られ、情報セキュリティの考え方もアップデートを迫られています。今回は、組織としての情報セキュリティの考え方と、それを支える技術的基盤、社会的基盤というフォーカスの当て方をしてみました。

レポート問題も、実際に起きている問題を抽象化した形ではなく、ある程度まとまった形で出すようにしました。「実際」の緊迫感を感じ取ることができたでしょうか。もっとも、論点を自分で抽出できる能力を養成するところまでは授業ではできなかった反省もあるので、論点は枝問の形で提示しました。ただし、最後の問題は論点を自分で見つけてより大きな立場で論じるようなものになっています。

問題は１．2012 年のファーストサーバーでのデータ消失事故、２．2011 年 DigiNotar での不正証明書発行事件、３．2008 年サウンドハウスでの大規模情報漏えい事件を出しました。３．は教科書でも大筋が示されていましたがあらためて調査レポートを読むとどう感じたでしょうか？１．と２．は今でも若干生々しさが残っていますが、多くの答案は冷静に調査レポートを解析していまし？？？

正直言うと、指定した調査レポートを読まずに、スライドで示した「あらすじ」を対象にレポートを書いているものが見受けられました。資料が提示されたらとりあえず読みましょう。勉強の基本。

授業の内容と関係することで言うと、解析の基本であるリスク評価の理解度に問題のある人が見受けられました。CIA（機密性、完全性、可用性）は独立に踊るキーワードではなく、リスク評価の一環として考えるものです。これが不十分だと、それに続くリスク対応としてとんちんかんなことをしがちです。個別レポートの講評でこの問題が指摘された人は復習することを強く勧めます（この授業も何年目かなのですが、CIA については強調しておかないと素人考えに陥るということがよくわかりました。今年特有の話ではないですね）。

DigiNotar の問題を選択する人がほとんどいませんでしたが、これは大人の問題なのでしょうがないかな、と思う反面、社会インフラとしての IT を理解するという点では非常に重要な点を含んでいたと思います。いまからでもやってみることを勧めます。

できとしては、みなさん、少しとまどったよう（あまりできはよくない）です。リスク対応の個々の技術的な詳細にまで踏み込んで授業すべきかどうかについて教える側も少し反省が必要かもしれません。

以下は、個々の問題に対する解答例です。問題と見比べてご賞味ください。書き方が統一されていませんが、講師で分担して書いたものを佐藤が（基本的に）編集なしでコンパイルしました。文責はもちろん佐藤にあります。では。

レポートテーマその１：ファーストサーバー

■ 概要

- 2012 年 6 月、ファーストサーバ社の運営するデータセンターにて顧客データが消失し、同社データセンターを利用していた約 5700 組織に、サーバデータが消失する等の影響を与えた。
- 同社による事故調査報告書が公開されている。
  http://www.firstserver.co.jp/news/2012/2012073101.html

■ 発生した事象

- 作業者がデータを誤って消去したことによるシステム停止。
- （2 次被害として）バックアップから復旧されたデータが、本来アクセス権のない他ユーザにも閲覧可脳な状態となった。
- 最終的にはバックアップデータそのものも消去され、原状回復が不可能に。

■ 設問

1. システム変更を行う場合、変更管理（change control）とよばれる手続きを踏むのが内部統制の立場からリスク対応の方法として一般的である。変更管理が何かを説明して、なぜこれが有効とされるかを解析せよ。この観点からファーストサーバーの管理の仕方を論ぜよ。
2. 顧客情報資産は CIA の観点から適切な対策を実施していたか論ぜよ。
3. クラウド型のサービスの利用の場合、SLA で保証を求めるのが一般的である。SLA とは何か説明し、さらにそれに照らし、顧客の対応が適切であったか論ぜよ。
4. クラウド利用のリスク対応として SLA はどうあるべきか、顧客の立場から、従来一般的であった業務委託契約と比較して論ぜよ。
5. この件については、成熟度監査の定期的な実施が被害を軽くしたかもしれない。それはなぜか、当時のファーストサーバーの企業としての成熟度を評価した上で論ぜよ。
6. あなたがクラウドサービスを利用する顧客企業の経営者であると想定し、自社のリソースをクラウド上で運用する際のリスク管理について、必要だと考える視点を挙げ論ぜよ。

■ 設問１に対する回答例と評価

Q1-1） 変更管理（change control）が何かを説明せよ

A1-1） 「変更管理」とは、IT インフラや IT サービスに対してハードウェア・ソフトウェア・プロセス・ドキュメント・人の変更を実施する際、変更作業に伴うリスクを最小限に抑えながら、効果的・効率的に実現する IT 運用管理の活動である。例えば、①障害時原因追跡手段の確保や改善のインプットを入手する事、②IT サービス利用者への影響を必要最小限に抑える事、③既に導入されているコントロールを維持する事などがある。

（参考）その他の標準および規格における説明について
評価は、「IT ガバナンス」、「IT の運用管理」、「情報セキュリティ」などの標準、および「ISO/IEC ISO27001-1:2005、ISO/IEC ISO20000-1:2005、ITIL Ver3、COBIT4.1」などの規格における説明も十分であると判断します。その上で、変更管理における目的と対象を明示的に説明した場合はより高い評価であると判断します。

Q1-2） 変更管理が何故有効かを解析せよ
A1-2)「何故有効か」とは、変更の影響を受けるすべての関係者にその影響を認識および理解させることを重要な目標としているからである。例えば、提案された変更が IT 環境に及ぼす影響の評価、変更の優先順位付けと分類、方針の決定、変更の計画から開発とテストを通じて実施に至るまでのプロセスの監視が含まれている事、また変更管理プロセスを通じて不必要な変更の数を減らす事など、サービス可用性と IT 効率を向上させることができる。

Q1-3） ファーストサーバの管理の仕方がどうであったかを説明せよ
A1-3)第三者委員会による調査では、①約 10 年前からマニュアルを無視し独自の更新プログラムを利用、②上長もそれを容認していた、③事故当日はリスクが低いものと判断し担当者は会議中の上長の許可を求めず、④少数ユーザーに適用してから本番で実行という通常プロセスも省いて本番更新を行った結果、第 1 事故であるデータ消失をした。消失データを復元しようと第 2 事故の参照を起こしたとの事であった。
調査の結果、第三者委員会は、「軽過失の枠内ではあるものの（比較的重度の過失）である」と判断した上で、「故意と同視できるほどの（重過失）には当たらない」と評価している。また「一般的なレンタルサーバ業者の水準に照らしても（適切)」なものであったと見解を添えている。

（評価）その他の管理および評価における説明について
評価は、「事故発生前における管理の仕方」、および「事故発生当日の対応の仕方」における説明も十分であると判断します。その上で第三者委員会や外部専門家による「管理の仕方を評価した」視点を説明した場合はより高い評価であると判断します。

設問２に対する回答例

Q2)　顧客情報資産はCIAの観点から適切な対策を実施していたか論ぜよ。

A2)　情報資産に対する情報セキュリティは、「①機密性」(Confidentiality)、「②完全性」(Integrity)、「③可用性」(Availability)　の３要素からなっており、その対策例とファーストサーバ社が当該事故を発生したレンタルサーバ契約における対策実施とを比較する。
A2-1)　機密性の観点は、「情報へのアクセス許可のある人だけが利用でき、許可の無い者は情報の使用や閲覧を出来なくすること」であり、その対策例は、アクセス制御、 パスワード認証、セキュリティ区画の立ち入り制限などがある。ファーストサーバ社は、通常運用においてアクセス制御やパスワード認証を実装していたが、緊急対応の仕方でアクセス制御が外れるオペレーションミスを想定していなかった点が事故を拡大した誘引であると考えられる。
A2-2)　完全性の観点は、「情報資産に正確性があり改竄されていないこと」であり、その対策例は、ファイル暗号化、デジタル署名、SSLデータ通信などがある。 ファーストサーバ社は、追加料金でＷｅｂ改ざん検知などを提供していたが、各社へのレンタルサーバ契約の責務としての物理的故障や論理的故障などリスクアドバイスが十分でなかったと考えられる。
A2-3)　可用性の観点は、「情報へのアクセス許可のある人が必要な時点で情報にアクセスできること」であり、その対策例は、システム全２重化、サーバのUPS、ハードデスクのRAID構成、システムのクラウド化などがある。ファーストサーバ社は、定期的バックアップやＵＰＳなどを実施していたが、バックアップは同一領域に保存されており復元プログラムの不具合にも対応できず、プライマリディスク障害の対応策も明示されていなかったと考えられる。

（評価）その他の３要素
評価は、上記「CIA」の３要素以外に、「④責任追跡性」(Accountability)、「⑤信憑性」(Authenticity)、「⑥信頼性」(Reliability) を加えて論じている場合はより高い評価であると判断します。

また、今回はレンタルサーバ契約をした各社の事業運営に多大な影響を与えた視点から、ますは「⑦リスクを許容範囲内に抑える」、とにもかくにも「⑧会社を運営できるようにする」、パッチ管理や事故対応「⑨リスクについてアドバイスする」などを各社のポリシーの設定に準拠するのをサポートするために、ポリシーを一連のプロセスに実装します。

設問３に対する回答

Q3)　クラウド型のサービスの利用の場合、SLA で保証を求めるのが一般的である。SLA とは何か説明し、さらにそれに照らし、顧客の対応が適切であったか論ぜよ。

A3-1)「SLA」とは、サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面により合意される契約である。例えば、顧客のビジネス要件に対して、最も費用対効果の高い IT サービスを提供することを目標として、顧客とサービスプロバイダのサービスレベルマネージャとの間で、どのサービスレベルで維持管理されるのかを作成し協議し合意したものである。

A3-2)「顧客の対応が適切であったか」とは、契約前の対応として、ファーストサーバ社と顧客が適正に対応していたかは明確でないと考えられる。例えば、SLA 作成において①サービスレベルマネージャは誰なのか、②合意する相手（顧客）は誰なのか、③IT サービス要件をまとめ合意したのか、

（評価）
評価は、上記 SAL の定義を説明し、契約時の合意手順が説明されていることで評価される。さらに契約後の対応として、④合意された SLA に基づいて IT サービスが運用されたのか、⑤運用した結果について顧客との間でレビューが行われたのか、⑥達成できなかった場合は改善策を見直し、どのレベルで運用すると合意したのか、を加えて論じていればより高い評価であると判断します。

設問４に対する回答

Q4)　クラウド利用のリスク対応として SLA はどうあるべきか、顧客の立場から、従来一般的であった業務委託契約と比較して論ぜよ。

A4-1)「SLA はどうあるべきか」とは、ISO/IEC20000 で「サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面による合意」の定義に基づいて委託先と委託元がどのサービスレベルで運用するかを書面で合意されることである。例えば、前提条件としてサービス・レベルに影響を及ぼす条件、委託業務の範囲として委託者が提供者に委託する業務の範囲、役割と責任の分担として委託業務に関する委託先と委託元の役割と責任の分担、サービス・レベルとする対象サービス、委託先が業務に必要と判断するサービス・レベル及びその測定方法、サービス・レベル未達成時の具体的な対応方法、運営ルールとして報告・会議体の運営ルールなどを書面で合意し、業務委託契約の付属資料とする場合もあるが、SLA 個別契約とするのが望ましい。

A4-2)「業務委託契約と SLA 契約の比較」とは、業務委託契約は物品取引の契約が主条項であり、納期・金額・納品物を合意する契約である。一方、SLA 契約はサービス提供の契約が主条項であり、委託者と委託元の役割責任を明確化や、どのレベルで運用し結果未達時の対応方法などを合意する契約である。

（評価）
評価は、商法に関る業務委託契約と、ITIL に関る SLA 契約の比較を説明されることで評価される。さらに、業務委託契約書の附属資料としてＳＬＡを締結する場合と業務委託契約書とは別途ＳＬＡを締結する場合を加えて論じていればより高い評価であると判断します。

設問５に対する回答

Q5)　この事故について成熟度監査の定期的な実施が被害を軽くしたかもしれない。それはなぜか、当時のファーストサーバーの企業としての成熟度を評価した上で論ぜよ。

A5)「定期的な成熟度監査が被害を軽くしたかも知れないのは何故か」とは、企業の内部統制や情報化などの実現レベルのモデルのことであり、①経営の組織管理成熟度モデル、②情報化戦略の IT 管理成熟度モデル、③情報化調達の能力成熟度モデル、などが挙げられる。

（評価）

評価は、商法に関る業務委託契約と、ITIL に関る SLA 契約の比較を説明されることで評価される。さらに、成熟度モデルが提供するものは、①何から着手すべきか、②ソフトウェア開発コミュニティが以前に経験したことから得られた成果、③共通の言語と、ビジョンの共有、④実行の優先順位づけの枠組み、⑤自分たちの組織にとって改善が意味することを明確にする方法、を加えて論じていればより高い評価であると判断します。

■ 設問６に対する回答

Q6) あなたがクラウドサービスを利用する顧客企業の経営者であると想定し、自社のリソースをクラウド上で運用する際のリスク管理について、必要だと考える視点を挙げ論ぜよ。

A6)「クラウド上で運用する際のリスク管理」を論ずる場合、“サービスモデルや社会インフラと言うコンプイーティングの特性”からデータの機密性やネット遅延などに対応するリスク管理を挙げるか、また、“リソースプーリングなど５つの特性や SaaS など３つのサービスモデルと言うクラウドの特性”から要員確保や自然災害などに対応するリスク管理を挙げることもできる。

（評価）
評価は、クラウド上で運用する際のリスクを想定し説明されることで評価される。さらに、海外に在るクラウド上で運用する際の EU 指令のデータ越境などのリスク管理や、内部監査の有効性などのリスク管理を加えて論じていればより高い評価であると判断します。

レポートテーマその２：DigiNotar

１．IDS、ログ監査ツールの設置について

授業でも解説したように、CA（認証局）は、ネットワーク上での信頼を構成するインフラストラクチャとして極めて重要な“アンカー”（起点）の役割を果たします。DigiNotar 社は商用（及びオランダ政府）の CA を運営していたわけですが、システムに不正侵入され、不正な電子証明書を発行されてしまいました。

電子証明書を発行するためには、CA の秘密鍵へのアクセスが必要となります。CA の秘密鍵は、それ自体をインターネットからアクセスさせる必要はないため、通常切り分けられたネットワークセグメントに配置されます。

DigiNotar の場合も、CA の秘密鍵（つまり CA のシステム）は、”Secure-net”と呼ばれるネットワークセグメントに隔離されており、ファイアウォールでのアクセス制御によりインターネットとの直接の通信はできませんでした。ただし、24 セグメント存在するネットワークは複雑に配置されていたようで、例えば Secure-net セグメントへのアクセスが単一の経路のみを通るようになっていたかどうかは報告書からは定かではありません。IDS やログ監査ツールを設置するためには、守るべきセグメントのアクセス経路を限定し、その上でその経路上に検知ツールの設置を検討する必要があります。

２．準拠性監査について

準拠性監査とは、ある基準に基づいて、システム（今回の場合は CA システム）の運用が適切に行われているかを、第三者として客観的に評価する監査です。
WTCA は、現状のインターネット（＝一般的に使われる OS や一般的に使われる Web ブラウザ）上で信頼できる証明書を発行する認証局の、事実上の運用基準になっています。

外部の監査法人がその監査を実施するわけですが、WTCA 等の基準は必ずしも明確に判定条件を示していない場合もあり、適切さの度合いが監査人の裁量に委ねられる場合もあります。また、報告書には記載がないので一般論になりますが、初回の監査では、システム全体を網羅的に調べますが、定期的な更新監査を実施する場合には追加や変更等があった箇所を重点的に注目して実施することがあります。このようなことを繰り返しているうちに、全体として何らかの適合性を逃していた可能性は推測されます。

３．DNS Poisoning + MITM とその成功度合い

例えば、ユーザと SSL 利用サイト https://accounts.google.com/ の間の通信を盗もうとす

る場合、DNS Poisoning と偽の証明書の両方が必要になります。

まず、単純な http の場合、accounts.google.com の FQDN（ホスト名+ドメイン名）が指し示すアドレスを自分の管理下のサーバの IP アドレスに誘導すればよいので、DNS Poisoning のみにより実現可能です。この場合、ユーザのブラウザ上で偽の IP アドレスに誘導されたことを知る術はありません。

しかし https の場合、例えサーバ証明書をそっくりコピーしたとしても、そのサーバ証明書内には、本物の accounts.google.com の公開鍵が格納されており、偽サーバ内の秘密鍵と紐付けが合わなければユーザのブラウザに警告が出てしまいます。ここで必要となるのが偽の証明書です。
CA の秘密鍵の操作権限を手に入れた侵入者は、偽サーバの秘密鍵と公開鍵を作成し、その偽の公開鍵に accounts.google.com の名前をつけた証明書を発行することができます（実際には *.google.com が発行され、* の部分はどんな名前でも OK となっていました)。
ユーザが DNS Poisoning によって偽の IP アドレスに誘導された状態では、FQDN は accounts.google.com と認識していますので、その名前のついた偽の公開鍵も信用してしまうことになります。この暗号化通信は、偽サーバの秘密鍵によって復号され、中身を窃取しつつ本物のサイトに転送することにより、ユーザからはあたかも SSL 通信が成功しているかのように見えてしまうのです。

ここでポイントは、偽の証明書を発行する CA です。OpenSSL 等で勝手に立ち上げたいわゆる“オレオレ証明書”を利用した場合、やはりユーザのブラウザで警告が出ます。今回は、DigiNotar の本物の CA が発行した証明書を利用しており、ユーザから見ると全く警告なく、偽のサーバに誘導されていたことになります。

どのくらいの被害が発生していたかの推測に利用されたのが、OCSP の通信ログです。証明書は、万が一の秘密鍵盗難等にそなえて、失効（Revocation）という仕組みが用意されています。OCSP は、その証明書が失効されていないかどうかをネットワーク上のサーバにオンラインで問い合わせることができる仕組みです。最近のブラウザでは、SSL の証明書を受け取ると、自動的に OCSP を使って証明書の状態をチェックするものがあり、これを使って、実際に偽の証明書へのアクセスがどのくらいあったかを推計することができます。報告書上は、298,140 の IP アドレスからアクセスがあったことが推計されています。なお、すべてのブラウザが OCSP 対応しているわけではないので、これよりも多くのアクセスがあった可能性があります。

４．ブラウザベンダーの責任

一旦 CA 証明書（厳密には Root CA）をブラウザに取り込んでしまうと、CA 証明書は無条件でユーザに信頼されてしまします。
当該 CA の管理状態が不適切な場合は、上記３のような不正行為が発生し、個人情報や決済情報を窃取されるため、オンライン上でのサービスインフラが成り立たなくなってしまいます。
このため、ブラウザベンダーが「どの CA 証明書を信用するか」を判定することは非常に重要です。

５．監査の役割

上記 4 の判定は確かに必要ですが、一方で、ブラウザベンダー自身が、CA の運用について適切かどうかを判断するのは極めて困難です。

従って、信頼できる第三者による WTCA への準拠性監査が保証となり、CA 証明書信頼の判断基準として使われることになります。この監査が形骸化しないよう、社会インフラとしての CA を維持することも重要となります。もしこの監査法人の保証業務が不適切であれば、CA 証明書の信頼性を維持できず、結果としてネットワーク全体の信頼性が成り立たなくなってしまうことになるのです。

レポートテーマその３：サウンドハウス

設問１

最初の攻撃に SQL injection が使われたであろうことが言われている。これが何かを解説するとともに、対応策について論ぜよ

---

1. SQL Injection について

概要

SQL Injection は、Web アプリケーションにおける攻撃手法の一種であり、いわゆる Web-DB アプリケーションを対象に、フロントエンドである Web アプリケーションからバックエンドのデータベースに対するクエリ（SQL 文）を操作する事により、DB に対する想定外の（不正な）アクセスを行うものである。

この脆弱性による脅威は様々なものが想定されるが、以下に代表的なものを挙げる。

・DB 内の情報の漏洩/改ざん

Web アプリケーションでのアクセス禁止または想定していないデータベース上のデータの読み取り及び改ざん（変更・消去・挿入）が行われる。これには他ユーザーの個人情報等の他、システム情報テーブル等も含まれる。

・Web アプリケーションの権限外利用

Web アプリケーションのパスワード認証を回避する事により、他ユーザーへの成りすましや、管理者権限でのログインによる不正操作が行われる。

・その他、DB 機能の不正な利用

利用している RDB の仕様や設定にもよるが､SQL 文の中で外部プログラムの実行、システムファイルの作成・編集等が可能であった場合[1]、これらの機能を利用したバックドアプログラムの設置といった、さらなるシステムへの攻撃に発展する恐れがある。

技術的な原理

ここでは SQL Injection の原理を説明するため、極めて単純な Web アプリケーショを想定した原始的な脆弱性の内容を例として記述する。

想定する Web アプリケーション

Web アプリケーションの機能： 入力文字列による DB 内検索
Web アプリケーションへの入力： 入力フォームからの任意の文字列
Web アプリケーションの出力： Web ページへの検索結果文字列の表示

この機能を作成するための単純な SQL 文としては以下が考えられる。

---

[1] Oracle におけるシステムファイルアクセス機能の例
http://otndnld.oracle.co.jp/document/products/oracle10g/102/doc_cd/appdev.102/B19245-02/u_file.htm

SELECT * FROM *対象テーブル名* WHERE name='***ユーザー入力***';

これをアプリケーション上で処理する場合、SQL 文の実行にあたっては、ユーザー入力は変数となるため、下記のように問い合わせ内容の主要部をあらかじめ用意しておき、文字列結合してから実行するのが最も単純な処理といえよう。

上記 SQL 文を作成するための文字列

文字列 1	SELECT * FROM *対象テーブル名* WHERE name= '
文字列 2	***変数（ユーザー入力）***
文字列 3	';

Web アプリケーションとしては、上記の 3 つの文字列を結合することによりユーザー入力に基づく SQL 文の作成と実行が期待される。

しかし、このプログラムには、問い合わせ想定通り実行される前提である、「ユーザー入力値の部分が『'』で囲まれている」といるということを保証していないという点に問題がある。つまり、ユーザー入力値に『'』を含む文字列を与える事により、以下の様に、危険な DB 操作が実行される可能性もあるという事である。

問題のあるユーザー入力値

Dummy'; INSERT INTO user_db (usename, passwd) VALUE ('Mallory','Crack'); --

最終的に作成される SQL 文

SELECT * FROM *対象テーブル名* WHERE name= 'Dummy'; **INSERT INTO user_db (usename, passwd) VALUE ('Mallory','Crack'); --'**

この SQL 文の太字部分が実行された場合、テーブル user_db に想定外のレコードが挿入されることになる。ここでは仮定のテーブルに対するレコード挿入を行ったが、ユーザー入力値を変更する事で、権限の及ぶ範囲内において、任意のデータベース操作(DELETE,UPDATE,DROP 等)を実行可能である事が示せたものと考える。

特徴

2. SQL Injection への対応策について

SQL Injection に対する技術的な対策は、原理的に 2 種類に分けられ、それぞれ以下の特徴がある。

1. ユーザー入力文字列のエスケープ

   この対策は、前述した SQL インジェクションの原理に基づき、「ユーザー入力値に対する操作」を行う事により対策を行うものである。例えば、前述のシングルクォーテーションによる SQL インジェクションの場合、「abc'def」というユーザー入力を、

『'abc"def'』とする。(シングルクォーテーションにシングルクォーテーションを前置することでエスケープする)という様な処理が挙げられる。
この対策のメリットとしては、利用するデータベースやミドルウェアの制約に関わらず、プログラミング時に自由度の高い SQL クエリを生成できる点が挙げられる。ただし、デメリットとして「SQL クエリの生成対象文字列や利用箇所、想定するユーザー入力値や処理系毎に異なる文字エンコーディングにあわせ、適切なエスケープ処理が異なる」「エスケープした文字列を別の箇所で利用/出力する際に、エスケープ処理を戻す必要がある」「プログラミング言語ごとにエスケープ処理機能の動作が異なる」といった問題があるため、対策にあたっては十分な知識・慎重な実装が求められる。

2. バインド機構（プレースホルダ）の利用

この対策は、前述の SQL インジェクションの原理に基づき、「SQL クエリの実行に際し、ユーザー入力値を含む文字列の結合を行わない」ことにより対策を行うものである。プログラミング言語により対策は異なるが、基本的には SQL クエリ部分を構造体やオブジェクトとしてあらかじめ定義（バインド）しておき、それらのクエリに対する引数としてユーザー入力を与えるというものである。つまり、DB に対する問い合わせの式は固定されており、問い合わせ条件のみユーザー入力値が使用されるということになる。[2]
この対策のメリットとしては、適切にバインドが行われていれば、SQL インジェクション攻撃への対策がほぼ完全になされるという点にある。[3] また、エスケープ処理と異なり、プログラム内で文字列変換を行う頻度が少なくなるため、バグ・セキュリティホールの発生する可能性が少ないというのも大きなメリットである。
この対策のデメリットとしては、処理系により利用可能な機能が異なるため、プログラミング言語、フレームワーク、利用するデータベース等の組み合わせを考慮する必要がある（場合によっては、利用可能なバインド機構に制限がある）という点が挙げられる。

[2] 実際のコード例等については参考文献を参照のこと
[3] エスケープ処理等、文字列の変換が全く不要になるわけではない。例えば、ユーザー入力値にワイルドカード文字の利用を許容しない場合は、該当する文字に対するエスケープ処理を行うなど、アプリケーション仕様を考慮した処理は必要である。

補足：

SQL Injection を含む、Web アプリケーションにおける一般的な脆弱性に対するリスク低減策を以下に例示する。これらは SQL インジェクションに限らず、Web アプリケーションの脆弱性によるリスクを低減するために有効な対策であると言える。

1. 開発者に対するセキュアプログラミング教育
2. （スクラッチ開発より比較的安全と考えられる）開発フレームワークの利用
3. WAF(Web Application Firewall)による防御
4. システム設計におけるセキュリティの考慮
5. システム開発時及び導入後の定期的な脆弱性検査

設問２

顧客データのうち、代表的なものを CIA から分類し、適切に管理されていたか解析せよ

まず、ファーストサーバにおける不正アクセスの過程で発生した問題を元に、機密性・完全性・可用性のそれぞれについて特に管理策が不足している点を整理する。

機密性：

サウンドハウスの報告書によれば、顧客情報としては氏名・性別・生年月日等のいわゆる個人情報およびログイン用メールアドレス[4]、クレジットカード情報、ログインパスワード等、ウェブサイトのサービス提供に関わる情報が含まれている。

不正アクセスの発生により、これらの情報は全て漏洩した可能性があるが、特に機密性に関する管理が不十分であったと言えるものとしては、ログインパスワードが挙げられる。

各種個人情報については、サービス提供上、ユーザーおよびサービス提供者が閲覧・変更可能となっている必要があるが、ログインパスワードについてはその必要がなく、ソルト付きハッシュ化等の処理により不可逆化された状態で保存しておくべきであった。

この管理策不備と、ユーザー側でのログインパスワードの使い回しが重なった事により、ユーザーのカード情報の不正利用の被害拡大が発生した可能性が高いと考えられる。

完全性：

サウンドハウスに対する不正アクセスにより完全性が大きく損なわれた情報としては、顧客情報の他に、各サーバ群におけるプログラム・システムファイル類が挙げられる。

代表的な物としては、各サーバにおけるパスワードやログファイル等である。

サウンドハウスのレポートを見る限り、これらの情報（データ）に関する完全性は確認

---

[4] これは個人情報の一部でもある

されておらず、緊急対策として「Web サーバー、データベースサーバーを新規で入れ替え」「OS からクリーンインストール」「各サーバーのパスワード変更」等の対処により、上書きをする事により安全を確保したものとなっている。行われた対策は、被害の拡大を防ぐために必要な物ではあったが、情報の完全性に関する管理策が十分であったとは言い難い。

一方、全ファイルのハッシュデータやバックアップデータとの照合等といった技術的な完全性を確保するための施策の常時実施はコスト面からみて困難であった可能性もあり、データバックアップからのシステム復旧は現実的な対応であると考える事もできる。

可用性：

対象とする事例においては、対策に際し主要サービスの停止という、可用性に対する大きな影響が発生している。ただしこれは内部サーバを含むネットワークシステムそのものへの不正アクセスへの対策の一環として発生したものであり、不正アクセスによる直接的な被害とは異なる点に注意する必要がある。

ここで問題とすべきは、各サーバの復旧に際し、データのバックアップや新規ハードウェアの調達が必要となった点にあると考えられる。通常、主要システムに関しては冗長性を持たせた構成とすべきであり、このような場合にはバックアップシステムによるサービス継続あるいはバックアップハードウェアに対するサーバ復旧作業の実施を行うことになるが、そのような管理策が取られていなかった可能性が高いと言える。

総論：

本事例に関しては、サウンドハウス社において行われていた CIA 管理策はそれぞれ不十分な点が指摘できるが、機密性管理に関し問題があったといえる。特にパスワード情報の平文による保存は、システム特性・開発コスト等に関わらず実施すべき管理策であり、また実施に際して必要なコストは小さいにも関わらず実施されていなかった。

これにより、2 次被害の拡大につながった点は指摘されて然るべきであろう。

完全性・可用性については上記の通り、一部不足といえる点もあるが、報告書の内容と企業規模・システム規模等を勘案する限り、やはり機密性の管理が最も不適切な状態にあったと考えられる。

設問３

他サイトでの二次被害の可能性を論じ、パスワードによる認証の脆弱性を論ぜよ

サウンドハウスの事例における二次被害の可能性

サウンドハウスにおいては、クレジットカード決済において 3D セキュアを利用し、原理上はサウンドハウスにおけるサービス利用とクレジットカード決済サービスの利用に関する認証情報は分離されていた。しかし結果としては、決済情報（パスワード）の流用によるものと思われる被害が発生している。（報告書では、クレジットカード会社からの情報として、「クレジットカード不正利用のリスト」等の記載が確認できる）

これは、サービス側で権限（サイトの利用/決裁）に合わせ認証情報を分離していたにも関わらず、ユーザー側でパスワードの使い回し、もしくは容易に推測可能なパスワードの利用等が行われていた事を示唆している。

パスワードによる認証の脆弱性

パスワードによる認証には、「ユーザー端末の制約が小さい」「容易に変更可能」「低コストで実装可能」等の利点があるが、「セキュリティレベルがユーザーに依存する」という点が大きな脆弱性として挙げられる。

パスワード認証のセキュリティは、多くの場合システム的な制約ではなく、ユーザーの知識や意識の不足、あるいは怠惰、記憶力の限界等が制約となる。これは「単純・推測可能なパスワードの利用」「パスワードの使い回し」「パスワード記載メモの放置」といった形で顕在化する。

パスワード認証の脆弱性への対応例

上記の脆弱性は、パスワード認証の特性そのものに由来しているものであるため、技術的対策のみによる対応は困難である。そのため対応策としては、

「ユーザーの知識や意識の向上」→ユーザー教育

「ユーザーのパスワード利用支援」→パスワード設定支援[5]・利用/管理支援機能[6]

といったユーザー側への働きかけや、他の認証との組み合わせ（二要素認証）といった形での対応が必要となる。

設問４

当該企業の社内ネットワークを推測し、改善策を論ぜよ

事例発生時の社内ネットワーク状況

対象の事例が起きた時点では、サウンドハウスにおける社内ネットワークは、いわゆる公開ネットワークや、管理/開発用ネットワークとの分離がなされていなかったと考えられる。

これは、SQL インジェクションによる侵入が、DB サーバ（通常、バックエンド側のシ

---

[5] パスワードの複雑さの評価や、パスワードルール等

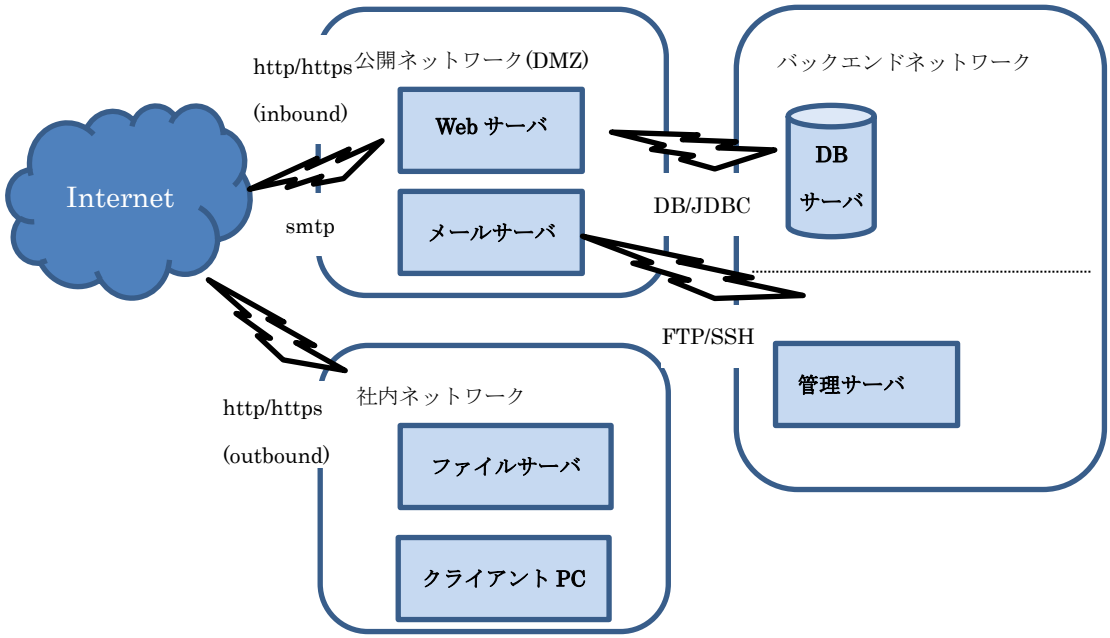
[6] パスワードマネージャ・管理ツール等

ステムとして Web サーバとのみ接続される）へのバックドア設置、さらに社内サーバへのバックドア設置に繋がったという事象の経過、およびサウンドハウスの報告書「4.セキュリティ管理体制について」において改善策として示された、「２．サーバーのセグメンテーション化」等から推測できる。

改善策

サウンドハウスの報告書に記載の通り、関連ネットワークのセグメンテーション化が望ましい対策である。ネットワークのセグメンテーション化は、以下の様なネットワークの分離を行い、各ネットワーク間で必要な通信以外は遮断する事により実現される。

図：ネットワークのセグメンテーション化（例）



設問５

あなたが e コマースサイトを開設する経営者であると想定し、当該サイトの運用に関連するリスク管理として重要と考えることを議論せよ

---

e コマースサイトの運用に限らず、リスク管理に携わる場合、リスクの特定と分析、リスク対応策の検討、リスク対応策の実施というステップは変化しない。以下では、e コマースサイト運用主体として特に重要であると考えられる点を取り上げる。

なお、ここでいうリスク管理は、情報セキュリティリスクを対象とし、事業運用上のリスク等は対象外とする。

- **リスクの特定と分析**

インターネットに公開される e コマースサイトの運用は、実店舗の運用と比較し、以下に挙げる情報システムの技術面に関するリスクを考慮する必要がある。

機密性の侵害

情報漏洩：機密性の侵害は、情報漏洩として顕在化する。e コマースシステムにおいては、特に保護すべき情報は以下の 2 種類と考えられる。[7]

- ✧ 顧客情報（決済情報を含む）

  カード情報などの決済情報を含む顧客情報は、特に機密性に関する配慮が必要な情報である。これらの情報の漏えいは金銭的な被害に直結するというだけでなく、個人情報の保護等、コンプライアンス面での問題、さらに運用するサイト・運用主体への信頼性の低下等、深刻な被害が直接発生する可能性が高い。

- ✧ システム情報

  システム情報の漏洩は、直接的な被害にならなくとも、結果として顧客情報の漏洩や、完全性・可用性の侵害につながる可能性が高い。また漏洩が発見できなかった場合、継続的に大きな被害に発展する恐れがある。

完全性の侵害

- ✧ 決裁情報

  特に e コマースサイトにおいては、ユーザーの決裁記録はサーバー上のログとしてのみ存在していることが少なくない。セキュリティホール等を悪用され、決済情報が改竄された場合、復旧が困難となる可能性が高い。

可用性の侵害

- ✧ システム運用

  特にシステムの自社運用を行う場合、サーバ障害等を考慮した可用性の確保は重要な問題となる。外部委託の場合等についても、SLA 等により一定の可用性確保は期待できるが、システムオーナーは、「どの程度までのシステムダウンを許容できるか/できないか」という考え方に基づき、非機能要件を評価する必要がある。

- ✧ システム性能

  インターネット経由でアクセスできる e コマースサイトにおいては、システム性能が店舗規模の限界を規定する要件の一つとなる。

---

[7] 他にも商品在庫数等、業務上の機密情報はシステム上に存在するが、アクセス権管理等は実店舗に準ずるものと考慮できる。

- **リスク対応策の検討と実施**
  - 技術的な対応とコストの妥当性評価

    情報システムにおけるセキュリティ対策の中でも、技術的な対策は多様な選択肢があり、いずれも初期投資及び運用コストが発生するため、対応策の評価が必要となる。評価にあたっては、必要な人材の確保に加え、評価プロセス・基準の記録・明確化が重要である。
  - 技術的対策に伴うトレードオフの考慮

    二要素認証の導入により、モバイル端末からのアクセスが限定される可能性がある。これは BtoC サイトにおいては許容できない条件となり得る。また可用性の確保のためにクラウドサービスを利用する事により、機密性や完全性が犠牲となる場合がある。これは BtoB サイトにおいて顧客の選定条件に抵触する恐れがある。単純にセキュリティ技術の選択を行うのではなく、e コマースサイトの提供にあたってはエンドユーザー要件の検討の上での対策実施が求められる。