Part4.

情報セキュリティ対策の分析と検討

重要インフラ情報システム信頼性研究会　情報セキュリティ事例研究 WG
委員名簿

主査

渡辺 研司 長岡技術科学大学

委員

織茂 昌之　株式会社日立製作所
坂野 正晴　株式会社みずほコーポレート銀行
高橋 通宣　東京電力株式会社
西本 逸郎　株式会社ラック
山作 英一　東日本旅客鉄道株式会社

（五十音順、敬称略）

オブザーバ

経済産業省 情報セキュリティ政策室
経済産業省 情報処理振興課
独立行政法人 情報処理推進機構 ｿﾌﾄｳｪｱ･ｴﾝｼﾞﾆｱﾘﾝｸﾞ･ｾﾝﾀｰ（IPA/SEC）
JPCERT コーディネーションセンター（JPCERT/CC）

事務局

独立行政法人 情報処理推進機構 セキュリティセンター

情報セキュリティ事例研究 WG 開催概要

第 1 回

1. 日時：　平成 20 年 11 月 19 日（水）　13:00 ～ 15:00
2. 場所：　経済産業省本館 17 階　第 5 共用会議室
3. 出席者：
   委員：　渡辺主査、坂野委員、高橋委員、山崎委員、織茂委員、西本委員、西本委員代理武智代理
   オブザーバ：　経済産業省、IPA/SEC、JPCERT/CC
4. 主な論点：
   （1） 重要インフラ情報システム信頼性研究会の他の WG の状況報告について
   → 本委員会の位置づけを、METI 井土氏より説明。
   （2） 情報セキュリティ事例紹介と情報セキュリティ障害対策分析表、および討議
   → IPA 永安と JPCERT/CC 山本氏より事例と分析表を説明後、討議。

第 2 回

1. 日時：　平成 20 年 12 月 9 日（火）　10:00 ～ 12:00
2. 場所：　経済産業省別館 10 階　1042 会議室
3. 出席者：
   委員：　渡辺主査、坂野委員、高橋委員、山作委員、織茂委員（説明者：田中氏）、西本委員
   オブザーバ：経済産業省、IPA/SEC、JPCERT/CC
4. 主な論点：
   (ア) 事例発表および討議
   （1） 情報セキュリティ対策の考え方（みずほコーポレート銀行）
   （2） システムセキュリティについて（東京電力）
   （3） JR 東日本とコンピュータセキュリティ（JR 東日本）
   （4） 重要インフラ関係インシデント事例（ラック）
   （5） HIRT（Hitachi Incident Response Team）のご紹介(日立)
   （6） 障害事例報告（JPCERT/CC）
   （7） IPA を騙った標的型攻撃メール（IPA）

1. 取り組み方針（考え方）

経済産業省では、2008 年 11 月 27 日（木)、「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」の第 1 回を開催した。同研究会では信頼性とセキュリティを包括的に取り上げ、「時代の変化や国際的な動向を踏まえつつ、高度情報化社会における情報システム・ソフトウェアの適切な信頼性及びセキュリティのあり方と、それを実現していくためのわが国の戦略的な取組みを検討し、提言を行う」としている。

また、経済産業省は「情報セキュリティ総合戦略」[5]を公開し、この戦略の一つとして「事故前提社会」というコンセプトを発表している。これは、情報技術（IT)は、今や経済、社会の「神経系」を担うインフラとなってきている。その一方、送電網（米国）や水道システム（豪州）への不正侵入、コンピュータウイルスの蔓延、金融・運輸でのシステムダウンによる混乱といった事故・事件が実際に発生するなど、IT の問題が社会に損害を及ぼす危険性が飛躍的に大きくなっているという背景からである。すなわち、「情報セキュリティに関する事故は必ず起こる」という前提に立ち，事故の予防や被害の拡大防止，より早い回復のための対策を官民が連携して実施しようというものである。 具体的な対策としては，以下のようなものを挙げている。

- 官民で脆弱性情報を収集および共有するためのルールと体制の整備
- 官民が協力して脆弱性の解析や不正アクセス、ウイルスの監視ならびに情報提供する体制の整備
- 政府や重要インフラ事業者が共同してサイバー・テロやシステム事故を想定した演習の実施

さらに、内閣官房情報セキュリティセンター（ＮＩＳＣ）では、「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」において、事故前提社会に対応した社会インフラに対して IT 障害の位置づけとして、情報システム・ソフトウェアのセキュリティ脆弱性による障害やセキュリティインシデントの発生に対する未然防止、再発防止策の必要性を提言しており、全体像を以下のようにまとめている。

- 「重要インフラにおける IT 障害の発生を限りなくゼロにすること」を目指すとともに、「IT 障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標に官民が連携して重要インフラ防護に取り組む。
- 新たに分野[6]ごとに重要インフラサービスの検証レベルを設定して着実に改善を実施。
- 第 1 次行動計画において策定した施策 4 つの柱に着実に取り組み、また経験を改善につなげるとともに、新たに「環境変化への対応」を 5 つめの柱に掲げ、変化に対する

[5] http://www.meti.go.jp/policy/netsecurity/strategy.htm

[6] 日本では、重要インフラとして、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」、「医療」、「水道」、「物流」の 10 分野が指定されている。

察知能力の向上と機敏な対応に取り組む。

このように事故前提社会に対応した重要インフラに対して信頼性とセキュリティは両輪として推進していく必要があり、本研究会の情報セキュリティ事例研究 WG においては、重要インフラにおけるリスクとして情報セキュリティを捉え、メディアで公開されている国内外の情報セキュリティインシデント事例の収集、それらの原因分析、再発防止策の洗い出しを行い、以下の方針でとりまとめることとした。

- ★ **事故前提社会に対応したセキュリティ脆弱性に対する情報システム・ソフトウェアへの未然防止、再発防止策の提言**
- ★ **情報システム・ソフトウェアのライフサイクルの各フェーズに対して、具体的対策を実施する仕組みを提言**
- ★ **情報システム・ソフトウェアの情報セキュリティ対策のレベルを評価するための方式の提言**
  - ➢ **再発防止策一覧表(付録 B)を使用して、セキュリティレベルを自己診断するアプローチ**

なお、WG の推進に当たっては、重要インフラ事業者および情報セキュリティ有識者を委員とした WG を立上げ、以下の日程で WG を開催した。

第 1 回　2008 年 11 月 19 日（水）

第 2 回　2008 年 12 月 09 日（火）

2. 情報セキュリティインシデント事例分析

2.1. 事例収集の考え方

重要インフラ事業者の情報セキュリティインシデント事例を収集する方法には、メディアで公開されている情報を収集する方法と、重要インフラ事業者へのヒアリングを行う方法の 2 種類が考えられる。

このうちヒアリングについては、情報セキュリティインシデントに関する詳細な情報が、重要インフラ事業者にとって機微な情報であり、情報を入手することが困難であると想定されたので、今回は事例収集の方法として、メディアで公開されている情報を収集する方法を採った。

2.2. 事例収集の対象と範囲

事例収集においては、対象期間を 2000 年から 2008 年までの間とし、国内だけでなく海外も含むものとした。海外も含む理由は、セキュリティインシデントとして影響の大きな事例が海外で発生し、メディアが報告している事から、これらを収集して参考にすることが、我が国でセキュリティインシデントを事前に防止する観点から重要だからである。海外の事例には、国内では例がない攻撃手法が使用されたものや、国内の事例よりも大きな被害が生じたもの等が含まれる。

国内の情報源として、21 の国内ニュースサイトを情報源とした。また、海外の情報源として、海外のセキュリティニュースサイトを情報とした。

今回は、国内の事例 38 件、海外の事例 20 件、合計 58 件の情報セキュリティインシデント事例を収集することができた。

2.3. 情報の整理

収集した情報の整理にあたっては、信頼性の分野における事例整理の方法が、情報セキュリティインシデント事例を整理する上でも有用だと判断し、同じものを採用した。具体的には、公開情報から表 1 の項目をまとめた。

なお、情報セキュリティインシデント事例においては、攻撃者や攻撃手法に関する情報も、漏らさず収集する必要があり、「障害の概要」項目に含んでいる。

表４－１　情報セキュリティインシデント事例の整理項目

No.	今回収集した情報セキュリティインシデント事例の通し番号。
発生日	情報セキュリティインシデントが発生した日。 発生した日が不明な場合においては、情報セキュリティインシデントが発見された日。 発見された日も不明な場合においては、情報セキュリティインシデントが公開された日。
ユーザ企業	情報セキュリティインシデントを生じたシステムを使用していた企業。
ベンダ企業	情報セキュリティインシデントを生じたシステムを開発した企業。
障害の概要	情報セキュリティインシデントの概要を示す。 攻撃者、被害者、攻撃手法、被害について、数行程度で簡潔に判るよう抜粋した。
主な原因	原因の記載については、公開情報の文面をそのまま引用することを避け、いくつかの種類に分類することにした。詳細は 2.4.を参照。
影響範囲	情報セキュリティインシデントによって生じた被害が影響を及ぼした範囲。 特に、数値が判るような箇所を抜粋した。たとえば、情報漏えいにおいては漏えいした件数、サービス妨害においては停止したサービスの規模や期間、金銭的被害においてはその金額、を記載した。
再発防止策	後述の分析に基づき、情報セキュリティインシデントの再発防止策を推定し、再発防止策の対策 ID を記載した。詳細は 3.を参照。
備考	情報セキュリティインシデントの発覚方法や、事業者が行った対策など、追記すべき情報があれば記載。
出典	情報セキュリティインシデント事例の情報源。

2.4. 収集情報の分析

今回、収集した情報セキュリティインシデント事例を分析する目的は、インシデントの再発防止策を洗い出すことにある。分析の手法として図４－1のように、インシデントが発生した原因を体系化して整理する手法をとった。

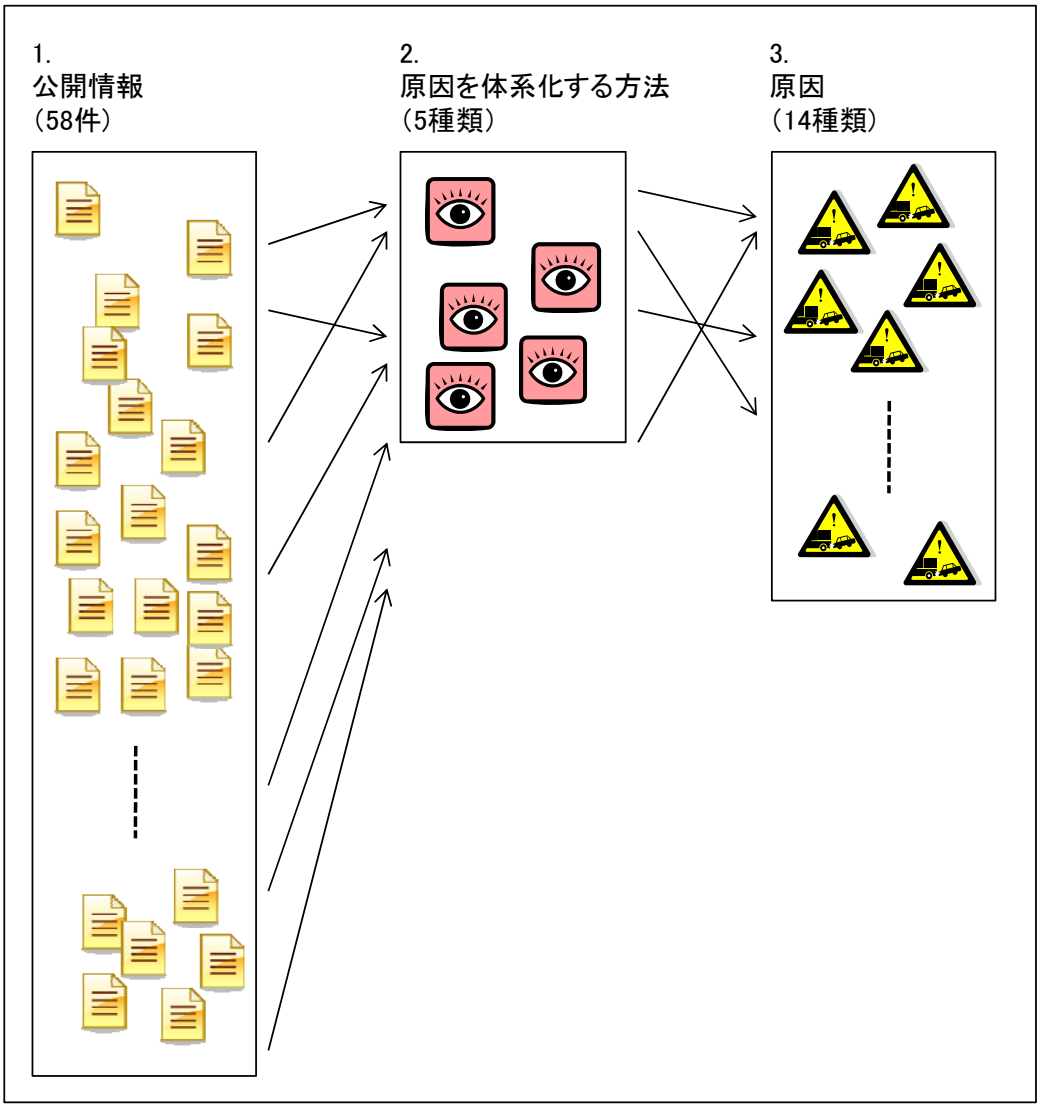

図４－1　公開情報の整理

2.4.1. 原因を体系化する方法

収集した情報セキュリティインシデント事例の公開情報中には、インシデントの原因と思われる記述が多くあった。しかし、その記述方法に一貫性はなく、一つの観点で体系化することは困難であった。どのような観点からの体系化が可能であるかを検討したところ、5種類の観点からであれば体系化を達成できそうであった。以下に、5種類の観点を説明する。

(1) 不正アクセス

多くの公開情報において原因を「不正アクセス」とする表現があった。しかし、「不正アクセス」と一口に言っても、その内容は様々なものが想定でき曖昧である。曖昧さを排するため単に「不正アクセス」とするのではなく、下記の順番で分類した。

1) 具体的な攻撃手法（例:「SQL インジェクション」）が公開されている場合、その攻撃手法とする。
2) 1) で分類できなかった場合、不正アクセスの主体（例:「内部の職員」、「退職した職員」、「外部の何者か」など）が公開されている場合、その攻撃主体を分類に付記する。
3) 2) で分類できなかった場合、単に「不正アクセス」とする。

以上のように分類したところ、それぞれ下記のような結果が得られた。

1) 公開情報の文面から具体的な攻撃手法を抽出できたものは「SQL インジェクション」（2 件）と「外部からのサービス妨害攻撃」（6 件）であった。「SQL インジェクション」については、この 2 件以外にも、同様の攻撃手法が使われた可能性がある事例が数件程度存在したが、公開情報による明言がない限りは「SQL インジェクション」とはしない方針をとった。これは、原因が「SQL インジェクション」ではない可能性も十分に考えられたためである。しかし、その中で 1 件のみ、当時流行していた SQL インジェクション攻撃のパターンに酷似した事例（No. 30:「長崎県平戸市のサイトが改竄、ウイルス感染の恐れも」）が存在したため、この件のみ例外的に「SQL インジェクション」とした。以上の結果、3 件を「SQL インジェクション」とした。この数は、近年 SQL インジェクション攻撃が急増している事を勘案すると少ないものである。この理由として、下記の仮説が考えられるが、今回収集した情報からでは、詳細な情報がない事から、仮説の妥当性を検証することはできない。さらに、「外部からのサービス妨害攻撃」については、同様の理由から、何らかの仮説を考えることは難しい。

   仮説(ア) 重要インフラ事業者においては、ウェブアプリケーションの検査は十分に行われており、SQL インジェクション攻撃に対して既に安全である。

   仮説(イ) SQL インジェクションの場合であっても、不正アクセスとして報告する場合が多い。

2) 公開情報の文面から不正アクセスの主体を特定できた事例は 15 件あり、内訳は「外部からの不正アクセス」（10 件）、「退職職員からの不正アクセス」（3 件）、「内部職員の不正アクセス」（2 件）であった。15 件という数は少なくないが、その大半は組織外からの不正アクセス（13 件）となっている。しかし、開発や運用をオフショアへアウトソースする例が増えており、スタッフや開発者が金銭目的で悪意を持つ場合が今後増えるか、既に起きていることが懸念される。仮に、組織内からの不正アクセスも実際にはもっと多く起きているとするならば、情報を収集できなかった理由として、下記の仮説を考えることができる。

   仮説(ア) 組織内からの不正アクセスの場合、不正アクセスの主体は公開されにくい。

   仮説(イ) 不正アクセスが組織内のみで完結する場合には、事例そのものが公開されな

い。

3）以上の情報が公開されておらず、単に「不正アクセス」としたものは 5 件あった。これらの事例においては、情報がほとんど公開されていないため、何らかの仮説を考えることは難しい。

(2) Winny の不適切な使用

情報漏えいの原因が Winny であると説明している事例は多く（8 件）、そのような事例については原因を「Winny の不適切な使用」とした。原因として具体的なソフトウェア名を挙げている事例は Winny を除けば少ないものであり、Winny は例外であると言える。その理由については、下記を考えることができる。

仮説(ア) Winny という名称は、情報漏えい事故の原因として把握しやすく、広く知れ渡っているため、原因として公開しやすい。

(3) システム構築時の問題

システム構築に際して何らかの考慮が抜けていた問題については、「設計時の考慮不足」（5 件）、「サーバ設定の不備」（2 件）、「システムの独立性不足」（1 件）、「ネットワーク経路の改ざん」（1 件）があった。

(4) 関係者の過失、または不正行為

組織内の人間が引き起こす過失や不正行為が原因であったものとして、「内部職員の過失」（4 件）、「外注先職員の不正」（1 件）があった。

(5) フィッシング

金融機関の偽サイトが作成されるというフィッシング詐欺の事例は 4 件あり、これらを「フィッシング」と分類した。

2.4.2. 原因

前節で説明した観点に基づき原因の分類を行ったところ、原因を下記の 14 種類とすることができた。

(1) 不正アクセス

1. 外部からのサービス妨害攻撃（6 件）
2. 不正アクセス（5 件）
3. SQL インジェクション（3 件）
4. 外部からの不正アクセス（10 件）
5. 退職職員の不正アクセス（3 件）
6. 内部職員の不正アクセス（2 件）

(2) Winny の不適切な使用

1. Winny の不適切な使用（8 件）

(3) システム構築時の問題

1. サーバ設定の不備（2 件）
2. 設計時の考慮不足（5 件）
3. ネットワーク経路の改ざん（1 件）
4. システムの独立性不足（1 件）

(4) 関係者の過失、または不正行為

1. 外注先職員の不正（1 件）
2. 内部職員の過失（4 件）

(5) フィッシング

1. フィッシング（4 件）

なお、原因が不明な事例は 4 件、同時に 2 つの原因を有する事例は 1 件あった。

2.5. 障害分析表

以上、本章で行った情報セキュリティインシデント事例分析の結果を、障害分析表としてまとめた。

- 付録 A　　障害分析表

3. 事例から見た再発防止策

再発防止策を洗い出し、図４－2 のように整理した。整理の観点には、ライフサイクルとセキュリティレベルの 2 つを用い、これらの観点から整理した結果を、再発防止策一覧表（付録 B）としてまとめた。

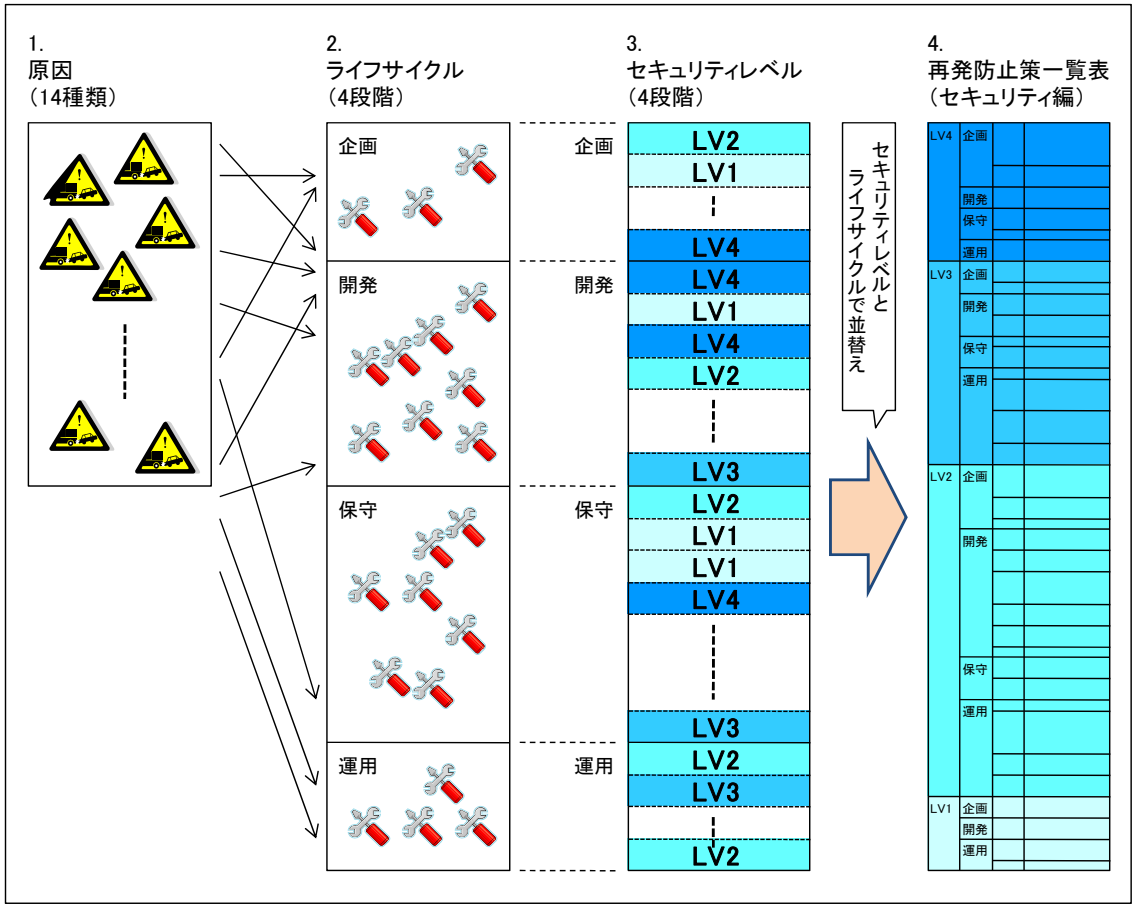

図４－2　再発防止策の整理

3.1. 再発防止策の洗い出し

再発防止策の洗い出しは、14 種類の原因に対して、下記 2 つの手法で実施した。

1) 信頼性の分野における再発防止策一覧表に記載された、再発防止策の 1 つ 1 つについて、セキュリティの観点から不足している点がないかどうかを確認し、不足があれば追記した。
2) 2.の情報セキュリティインシデント事例分析の成果を踏まえ、各事例において不足していた対策を推定した。これは、情報セキュリティの視点から、再発防止策を追加する手法である。

今回は、21 件の再発防止策を洗い出すことができた。

3.2. 再発防止策の構成

洗い出した再発防止策を構成するに当たり、下記の 2 点を考慮した。

3.2.1. 情報システムのライフサイクル

情報セキュリティ対策は、情報システムのライフサイクルの各段階において必要なものであるが、できるだけ早い段階から対策を検討することで、全体のコストを抑制できる性質がある。

また、情報セキュリティ対策は一度行えばそれで済むというものではない。攻撃者の側が常に新しい攻撃手法を考えているため、日々新しい攻撃手法が誕生している。このため、ある時点では安全な情報システムも、その後何もしなければ、安全ではなくなってしまう。このため、ライフサイクルの保守や運用の段階においては、再発防止策を PDCA サイクルに基づいて実施する必要がある。

今回、個々の再発防止策について、「企画」「開発」「保守」「運用」のどの段階で講じるべきか検討を行い、分類した。

3.2.2. セキュリティレベル

システムにおける情報セキュリティの達成度合いは、十分にセキュリティ対策が行き届いている状態から、ほとんど対策されていない状態までを考える事ができる。また、セキュリティ対策の必要性はそのシステムの目的によっても異なる。たとえば、個人利用するコンピュータにおいてもウイルス対策ソフトウェアの導入等は最低限必要なものであるが、基幹システムにおける対策はそれだけでは十分ではなく、定期的な監査などのより高度な施策を確立する必要がある。

これらは、いくつかの段階に分けて論じる事ができると捉え、本稿ではシステムにおける情報セキュリティの達成度合いを「セキュリティレベル」とした。セキュリティレベルには、LV4（高いレベル）から LV1（低いレベル）の 4 種類を、表４－2 のように設定した。

表４－2　セキュリティレベルと想定するシステム

セキュリティレベル	想定するシステム
LV4:	重要インフラの基幹システム
LV3:	企業の基幹情報システム
LV2:	社会的影響が少ないシステム
LV1:	オフィスや部門用のシステム

3.2.3. 「桶の法則」

情報セキュリティにおいては、「桶の法則」という考え方がある。これは、桶においては桶を構成する板の高さのうち、最低のところまでしか水を貯められないのと同じように、

情報セキュリティ対策においても最も弱い部分の安全性が、全体の安全性になることを説明したものである。従って、情報セキュリティ対策は一部分のみを充実させても全体の安全性に寄与することは少なく、ライフサイクルの各段階における全体のレベルのバランスをとった対策が必要となる。

今回個々の再発防止策が、LV4（高いレベル）から LV1（低いレベル）の 4 種類のセキュリティレベル（詳細は 4.1.を参照）のどれにあたるか検討し分類した。再発防止策があるレベルであるとは、そのセキュリティレベルを達成するためには、その再発防止策を講じておく必要があるという事である。たとえば、LV2 の再発防止策であれば、LV2,LV3,LV4 のセキュリティレベルを達成するためには必ず講じておく必要がある。

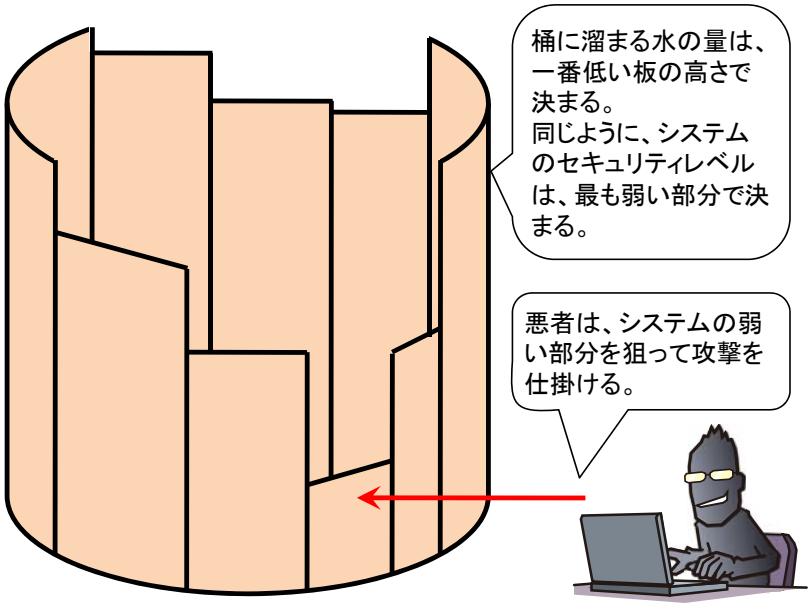

図４－3　セキュリティレベルと「桶の法則」

上記に基づき構成した再発防止策一覧表を、下記の付録に示す。

- **付録 B　　再発防止策一覧表**

3.3. 再発防止策の特徴

構成した再発防止策一覧表の中から、信頼性の観点と同じものだけでなく、セキュリティの観点から特徴的なものを下記に示す。

1) **セキュリティポリシーの制定**

(ア) **セキュリティポリシーは、組織における情報セキュリティの方針を明確化するものである。**

(イ) **セキュリティポリシーの制定にあたっては、システム自体にとどまらず、人の連絡体制や組織体制、緊急時の対応や教育方針なども規定する必要がある。このため、シス**

テムだけを考えていればいいというものではなく、組織全体を巻き込んでいく必要があるものである。

2) 攻撃を想定したシステム設計
   (ア) システムの内外には、悪意を持った攻撃者が存在する。
   (イ) 信頼性の分野においても機器の障害やオペレーションミスは想定されるが、悪意を持った攻撃者を想定する視点は情報セキュリティ独自のものである。攻撃者はシステムの外部だけでなく内部にも存在する可能性があり、重要な情報を取り扱う範囲を限定するなどの対策が必要となる。
3) システムの各部におけるセキュリティの追求
   (ア) システム全体のセキュリティを高めるためには、桶の法則に基づき、システムの特定の部分にだけ着目して対策するのではなく、全体を見て弱い部分をなくしていくという考え方が重要。
   (イ) 例えば、ネットワークの設計においては、システムの目的ごとに適切に分割し、必要な個所にファイアウォール、IDS（Intrusion Detection System）/IPS（Intrusion Prevention System）、WAF: Web Application Firewall などを設置する。
   (ウ) 例えば、OS やミドルウェアについては、適切なサポート契約を締結し、日々発見される脆弱性に対して適切に対処できる仕組みを整備する。
   (エ) 例えば、システム自体の開発については、設計時点における仕様のレビュー、開発時点におけるソースコードのレビューなどを、それぞれセキュリティの観点から実施する。
   (オ) 以上の中から、必要なものを実施し、対策の偏りをなくしていくことが重要。
4) ペネトレーションテストの実施
   (ア) 開発フェーズの仕上げとして、システムの安全性を確認する。
   (イ) システムに対するそれ以外のテストとは別のもので、非機能要件のテストの中でも、悪意ある攻撃を想定したもの。
   (ウ) ペネトレーションテストは、開発やテストを担当した者とは別の者が行う必要があり、一般的には、情報セキュリティ専門の会社に委託する形で実施する。
   (エ) ペネトレーションテストは、運用フェーズにも行う。
   (オ) 開発したシステムに対しては、定期的にペネトレーションテストを行う。
5) 脆弱性情報の定期的な収集
   (ア) システムの運用開始後も、新しい脆弱性は日々発見され、修正されている。
   (イ) システムをそのままにしていくと、既知の脆弱性を抱え込んだままになってしまう。
   (ウ) OS やミドルウェアについては、計画的に脆弱性情報を収集し、対処する。

4. セキュリティレベルの自己診断

4.1. セキュリティレベルの評価方法

再発防止策一覧表を使用して、セキュリティレベル毎に対策を自己診断することができる。具体的には、図４－４のように、目標とするセキュリティレベルおよびそれを下回るセキュリティレベルにおいて必要な再発防止策を、全て実施しているかどうかを確認する。あるセキュリティレベルを達成するためには、そのセキュリティレベル以下で必要な、全ての再発防止策を講じなくてはならない。

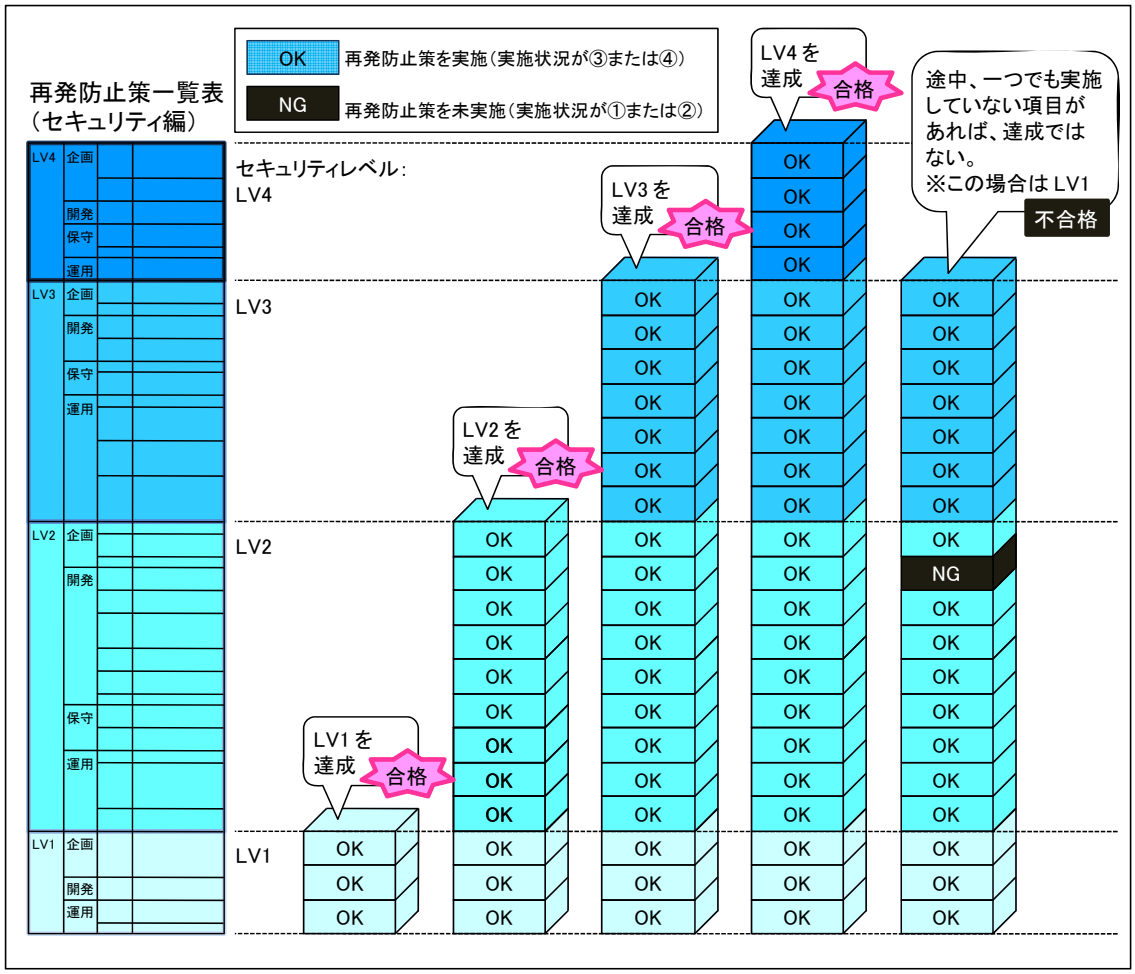

図４－４　　再発防止策一覧表とセキュリティレベル

セキュリティレベルの自己診断を行うには、まずシステムとして目標とするセキュリティレベルを設定する。レベルには表４－2 に示す４種類がある。また、企業のシステム全てを単一のシステムとして捉える必要はなく、図４－５のようにシステムを分割してセキュリティレベルを設定することができる。

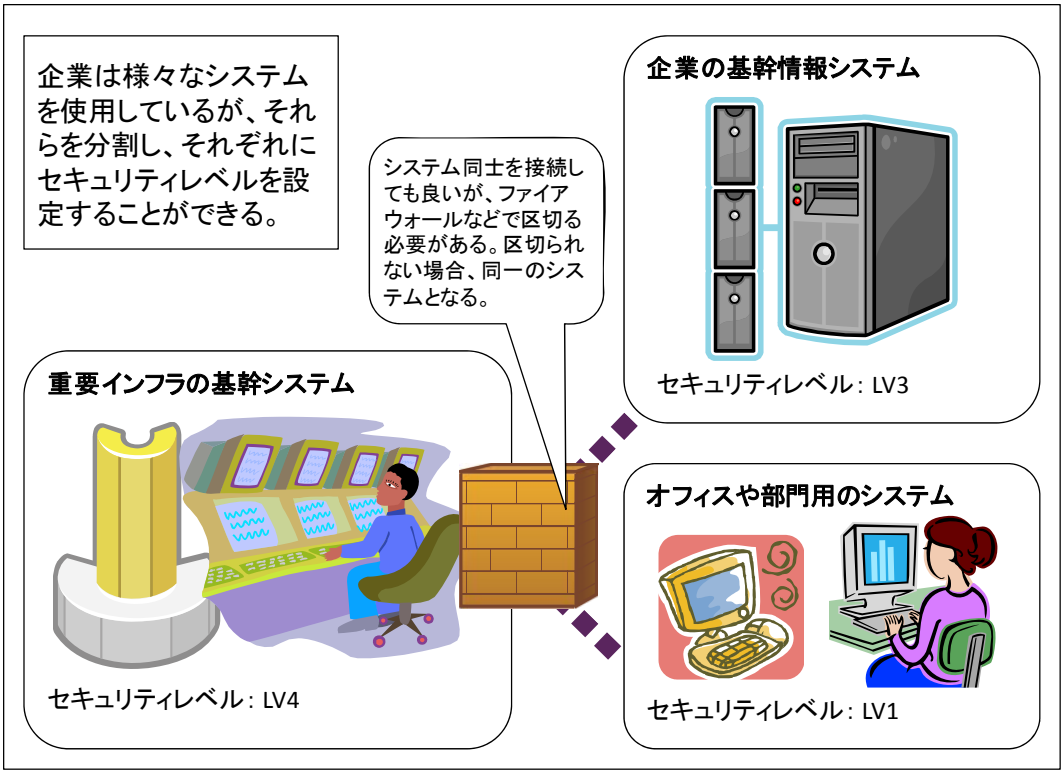

図４－５　企業におけるシステムの分割とセキュリティレベル設定の例

次に再発防止策一覧表から、設定したセキュリティレベルと、それを下回るセキュリティレベルの項目について自己診断を行い、表４－３のいずれかに当てはめる。たとえば、LV3 を設定したのであれば、LV3,LV2,LV1 の再発防止策が対象となる。

表４－３　対策の実施状況の区分

① 対策を実施していないか、実施しているかどうか不明である
② 実施している対策と実施していない対策がある
③ 現時点で必要な対策は全て実施している
④ 将来を鑑みても完璧な対策を実施している

自己評価結果のうち、③と④に評価された項目については、その再発防止策が講じられたと判断する。必要な再発防止策が全て講じられた場合のみ、設定したセキュリティレベルが達成されたと判断する。まとめると表４－４のようになる。

表４－４　システムのセキュリティレベル達成条件

システムのセキュリティレベル	レベルを達成する条件
LV4: 重要インフラの基幹システム	LV4,LV3,LV2,LV1 の全ての対策の実施状況が③または④である
LV3: 企業の基幹情報システム	LV3,LV2,LV1 の全ての対策の実施状況が③または④である
LV2: 社会的影響が少ないシステム	LV2,LV1 の全ての対策の実施状況が③または④である
LV1: オフィスや部門用のシステム	LV1の全ての対策の実施状況が③または④である

4.2. 信頼性と情報セキュリティにおける評価方法の違い

信頼性の分野においては、各再発防止策を行うことで評点が加点され、評点によってシステムの格付けが決定されるという方式であったが、これは情報セキュリティのレベルを評価する方式にはそぐわない。

その理由は「桶の法則」でも説明したように、情報セキュリティにおいては対策のどれか一つでも抜けると、安全性が大きく損なわれるためである。

そこで自己診断においては、総評点で評価する方式ではなく、想定する各セキュリティレベルにおいて必要な対策が、行き届いているかどうかを評価の対象とした。

なお今回、各セキュリティレベルに各対策を割り当てたが、割り当てにおいてはそのセキュリティレベルで必要と思われる最低限の対策のみを割り当てる事とした。なお、実施にあたり大きな予算や手間が必要となる対策については、やや高めのレベルに割り当てる事とした。

5. 今後の課題

以上のように、本年度はメディアで公開されている事例に基づく分析を行ったが、この手法の限界や今後の脅威の動向等についても WG において議論されたので以下に記載する。

1) メディアで公開されている事例に基づく分析手法では、原因を追究する際の情報が不十分なケースがほとんどであり、想定した脅威分析からの再発防止を検討するということにならざるを得なかった。実際に発生したセキュリティインシデントに関する情報は、機微な情報を含んでいる場合が少なくないため、より詳細な情報については、同種の情報に関する取り扱い実績のある組織等が、利用目的や情報の取扱い上の制約に関する合意を行った上で、個別のヒアリングにより聴取するといったような形で入手し、研究会等で利用できる形に編集して分析する等の方法を検討する必要がある。
2) 近年は、開発や運用に携わる人員の流動化が進む傾向があり、海外への IT のアウトソーシングに関する分析を行うにあたっては、海外で実際に情報を取り扱う作業関係者の意識や慣習、リテラシーの実態等に関する調査を踏まえた脅威分析と対策の策定が必要となってきている。

以上のような点を今後の課題としたい。

参考資料

[1] IPA「安全なウェブサイトの作り方 改訂第 3 版」
(http://www.ipa.go.jp/security/vuln/websecurity.html)

[2] IPA「セキュア・プログラミング講座」
(http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html)

[3] IPA「情報セキュリティ教本」(http://www.ipa.go.jp/security/publications/kyohon/)

[4] IPA「情報セキュリティ読本」(http://www.ipa.go.jp/security/publications/dokuhon/)

障害分析表

No	障害事例	発生日	障害の概要	主な原因	影響範囲	再発防止策	備考	出典
1	イスラエル外務省のサイトが、クラッカーにより攻撃を受ける	2000/10/26	イスラエルの外務省サイトがクラッカーによって攻撃を受け、ダウンさせられたという。同省のサイトをホスティングしていたのは NetVision で、数日、クラッカーのアタックを受け続けていたという。	【外部からのサービス妨害攻撃】	[イスラエル外務省] 適切な情報発信が行えなかったことによる、イスラエル外務省の信頼の喪失。	L4-P1		http://journal.mycom.co.jp/news/2000/10/27/16.html
2	陸上自衛隊の内部資料、「Winny」で流出	2002/11	陸上自衛隊第１普通科連隊（東京都練馬区）の内部資料がファイル交換ソフト「Winny」経由でインターネット上に流出。	【Winnyの不適切な使用】	流出したデータは第１普通科連隊の一部部隊に関する「教育訓練実施計画」「総員名簿」「精神教育の書式」など約 30 種類のファイル。隊員の名前や住所など個人情報が含まれていたが、「秘」指定の文書はなかったとしている。	L3-U2		http://internet.watch.impress.co.jp/cda/news/2004/04/30/2987.html
3	東武鉄道運営のサイト「102@Club」、個人情報漏洩	2003/12/3	東武鉄道運営サイト「102@Club」にて、個人情報漏洩。131,742 名全員の情報が漏洩した可能性があった。	（不明）	・最大で 131,742 名全員の情報が漏洩した可能性あり ・102@Club 会員および元会員には、東武動物公園または東武ワールドスクウェアに入園できる招待券を 2 枚送付	L2-D1, L2-D3, L1-D2, L2-M1, L3-U1, L3-U2	・発生日は、会員より架空請求書が届いたことがわかり、サーバ運用を停止した日。 ・３ヶ月間の営業自粛 ・根津嘉澄社長および池田操副社長の３カ月間 20%の減給処分	http://internet.watch.impress.co.jp/cda/news/2004/03/26/2588.html
4	北朝鮮と中国からハッカー攻撃、韓国政府資料流出	2004	４年間にわたり、韓国政府の資料およそ１３万件が、北朝鮮や中国からのハッカー攻撃によって流出していたことが明らかになった。韓国の情報機関、国家情報院（国情院）当局者は「機密は含まれておらず、外交、安保の分野に集中したものでもない」と説明した。	【外部からの不正アクセス】	韓国政府資料１３万件が流出。「主要文書を個人のコンピューターに保存またはインターネットで伝送するなど政府省庁と公務員の保安意識が緩んでいることに原因がある」と苦言。	L2-D1, L2-D3, L3-U1, L2-U1		http://japanese.joins.com/article/article.php?aid=106008&servcode=500&sectcode=500

5	厚生労働省の学生向け就職情報サイトが改ざん	2004/6/5	同サイトのトップページが、男性の顔写真と「改ざんは愉快」とする英文に置き換わっていた。	【外部からの不正アクセス】	ユーザー情報のデータベースに侵入された形跡がないことから、「IDなどの個人情報は漏えいしていない」という。	L2-D1, L2-D3, L3-U1, L2-U1		http://internet.watch.impress.co.jp/cda/news/2004/06/07/3386.html
6	「TEPCO ひかり」で一部ユーザーにウイルスメール	2004/11/22	FTTH サービス「TEPCO ひかり」のメールマガジンの一部ユーザーに対し、ウイルス「Netsky.Q」が添付されたメールが送信された。	【サーバ設定の不備】	登録ユーザーの一部にウイルスメールが配信された。	L3-P1, L2-D2, L2-U1	「TEPCO ひかりニュース」配信サーバに対し、ウイルスに感染したユーザーからと思われる不正投稿があった。	http://www.itmedia.co.jp/news/articles/0411/22/news060.html
7	首相官邸と内閣官房ＨＰにサイバー攻撃。一時接続不良に。	2005/2/22	ＨＰのアドレスを指定してもほとんどの利用者が接続できない状態になったという。	【外部からのサービス妨害攻撃】	[首相官邸と内閣官房] 適切な情報発信が行えなかったことによる、首相官邸と内閣官房の信頼の喪失。	L4-P1	警察庁のサイバーフォースセンターが DoS 攻撃と呼ばれる大量アクセスを受けているのを確認した。	http://www.asahi.com/tech/asahinews/TKY200502230310.html
8	外務省サイトがサイバー攻撃で、一時閲覧不能に。	2005/3/17	外務省の更新情報が閲覧できない状況が続いた。	【外部からのサービス妨害攻撃】	[外務省] 適切な情報発信が行えなかったことによる、外務省の信頼の喪失。	L4-P1		http://www.so-net.ne.jp/security/news/library/71.html
9	京都府警、個人情報が含まれた捜査書類をネットで漏洩	2004/3/26	捜査関係書類がインターネット上で漏洩。ネット上で閲覧できる状態になっていた。	（不明）	京都府警、個人情報 11 人分が漏洩。	L3-U2	2004/3/26 に、他県の男性より連絡を受ける。	http://internet.watch.impress.co.jp/cda/news/2004/03/29/2591.html

10	みずほ銀行をかたるフィッシングメール	2005/3/19（発表）	みずほ銀行の名前をかたった詐欺メールと思われる事象が発生した。このメールには、みずほ銀行のロゴや copyright などが使用され、クレジットカードなどの案内文とともに、みずほ銀行の URL（リンク）が記載されている。その URL（リンク）をクリックすると、みずほ銀行のホームページになりすましたページが表示され、住所やクレジットカード番号等を入力させて、利用者の個人情報を不正に入手しようとするもの。	【フィッシング】	[みずほ銀行サービス利用者] 当該偽サイトに誘導されて、ID・パスワード等の入力を行った者については、ID/pswd（他のサービス利用にも同じ組み合わせを利用しているかもしれない。）等の漏洩及び漏洩データを利用したサービスの不正利用被害。 --------- [みずほ銀行] なりすましにより自社サービスが利用された場合の、サービス利用名義人本人に対する補償等の可能性がある。 --------- [フィッシングサイトを立てられたサーバ管理者] 不正侵入を受け勝手に利用される被害を受けている可能性。	L2-D2, L2-U2	フィッシング対策業議会よりアナウンス。	http://www.antiphishing.jp/database/2005/03/
11	東京医科歯科大病院、Winny で検査結果を流出	2005/3/29（発表）	同病院の医師が自宅で使用していた PC が、P2P ファイル交換ソフト「Winny」の新種ウイルスに感染して個人情報が流出したとみられる。	【Winny の不適切な使用】	流出したのは、2000 年 8 月から 2003 年 3 月に「針生検検査」という病巣検査を受けた患者の検査結果データ約 50 名分。	L3-U2	毎日新聞社からの指摘で判明した。	http://internet.watch.impress.co.jp/cda/news/2005/03/29/7026.html
12	滋賀県の運営するサーバーに不正アクセス、テスト用 ID の放置が原因	2005/6	NPO 団体の情報を提供する「協働ネットしが」と、文化情報を提供する「あーとねっと・しが」の 2 つのページを運用するために設置したサーバー。6 月末から 7 月にかけて不正アクセスが行なわれた形跡がアクセスログから発見され、県では 8 月 4 日にサイトを閉鎖した。	【外部からの不正アクセス】	サーバーには NPO 法人の代表者などの個人情報 441 件と、メーリングリスト登録者のメールアドレス 156 件が保存されており、これらの情報にアクセスできる可能性があったが、侵入者がこれらの情報を閲覧したかについては判明していない。	L2-D1, L2-D3, L3-U1, L2-U1		http://internet.watch.impress.co.jp/cda/news/2005/08/09/8738.html

13	Winny で原子力発電所の内部情報が流出	2005/6/22	関西電力美浜原発や北海道電力泊原発、九州電力川内原発など、三菱電機プラントエンジニアリング（MPE）が 点検を請け負っている全国の原子力発電所に関する内部情報が Winny を通じて流出した内部情報は、MPE の社員が個人的に所有する PC から Winny を通じて流出した。	【Winny の不適切な使用】	流出した情報は、各原発の点検結果報告書や同社員の出張報告書、作業員名簿など約 40～50MB に達する。担当者間でやり取りしたメールのデータも流出した可能性があるという。	L3-U2	22 日夜に毎日新聞社からの指摘で流出の事態を知った。	http://internet.watch.impress.co.jp/cda/news/2005/06/23/8124.html
14	外部サーバーを利用した「作図受発注システム」に対する外部からの不正なアクセスの発生について	2005/8/11	「作図受発注システム」の管理業務委託先である㈱ティージー情報ネットワークから、 同社の管理する管理者ＩＤとパスワードを利用した不正なアクセスが発生。	【不正アクセス】	このたびの不正なアクセスによりプログラムの破壊や保管データの改ざん等の被害が発生していないことを確認しました。また、登録内容の閲覧等については、アクセス状況、登録データの内容からその可能性はきわめて低いと判断しました。	L2-D1, L2-D3, L3-U1, L2-U1	ティージー情報ネットワーク(東京ガス子会社)が調査を行った。	http://www.tokyo-gas.co.jp/Press/20050822.html
15	静岡刑務所職員が、貸与 PC で不正アクセス	2005/10	事務官が、職場のパソコンで受刑者の情報を不正に閲覧。	【内部職員の不正アクセス】	会議議事録や施設作業の売り上げなど職務上の情報を保存したＣＤを、当時勤務していた甲府刑務所の施設外に持ち出すなど、内規に違反。	L3-U2		http://www.shizushin.com/news/social/shizuoka/2008100200000000052.htm
16	ANA の搭乗ゲートの暗証番号などが流出、Winny を通じて流出した可能性	2005/11/8	大阪乗務センター所属の運行乗務員の自宅 PC から、 空港施設に入るための暗証番号などが流出していたと発表した。ファイル交換ソフト「Winny」を通じて流出した可能性が高いという。	【Winny の不適切な使用】	国内 29 空港の同社施設や搭乗ゲートの暗証番号が流出していた。暗証番号は 11 月 11 日までに変更した。	L3-U2	2005 年 11 月 8 日に国土交通省から「機密情報が流出している」との連絡を受けて発覚した。	http://internet.watch.impress.co.jp/cda/news/2006/03/15/11258.html

17	北海道職員の共済組合情報などがWinnyで流出	2005/11/16（発表）	地方職員共済組合北海道支部が管理する個人情報3,544人分がWinnyで流出した。同支部の職員が自宅にデータを持ち帰って私物PCに保存したことがわかっている。	【Winnyの不適切な使用】	流出したのは2000～2004年度分の掛け金収納などのデータで、退職者も含まれる。	L3-U2	総務省から共済関係の個人情報がインターネットに流出しているとの連絡があり発覚した。	http://internet.watch.impress.co.jp/cda/news/2005/11/16/9875.html
18	空港制限区域に入るための暗証番号がWinny上に流出、JAL副操縦士のPCから	2005/12/9（発表）	日本航空（JAL）は9日、羽田や成田など国内16空港とグアム空港の空港制限区域へ入るための暗証番号などを含む情報がWinnyで流出したことを明らかにした。	【Winnyの不適切な使用】	流出した個人情報には、羽田や成田、中部、関西、福岡など国内16空港と海外ではグアム空港における空港制限区域へ入るための暗証番号。搭乗口などから、一般人の入室が禁止されている空港内の施設に通じるドアの電子ロックを解除するもの。	L3-U2	2005/12/5日夜、国土交通省からの指摘があり調査。	http://internet.watch.impress.co.jp/cda/news/2005/12/09/10166.html
19	UFJ銀行、ウイルス感染メールを送信	2005/12/16（発表）	ニュース配信サービス“UFJ CHINA NEWS”に登録されているユーザー約7000名に、ウイルス“Worm_Netsky.P”に感染したメールを配信したことが判明した。	【サーバ設定の不備】	ニュース配信サービス“UFJ CHINA NEWS”に登録されているユーザー約7000名	L3-P1, L2-D2, L2-U1		http://ascii24.com/news/i/topi/article/2005/12/16/659632-000.html
20	中部電力の発電所情報がWinnyに流出、原子力安全・保安院が指摘	2006/1/27	同社の関連会社である中部プラントサービスの社員の私有PCがウイルスに感染し、Winnyネットワーク上に発電所関連の資料が流出していた。	【Winnyの不適切な使用】	中部プラントサービス川越事業所（三重県）の社員の自宅PCから、「川越火力発電所3号系列の燃焼器点検記録のフォーマット」「非破壊検査記録」「点検従 事者の名字（2名分）」などの技術資料が流出した。	L3-U2	原子力安全・保安院が30日に指摘。	http://internet.watch.impress.co.jp/cda/news/2006/02/03/10763.html
21	受刑者情報含む1万ファイルがWinny流出、京都刑務所の刑務官のPCから	2006/2/3	滋賀刑務所や福岡拘置所の被収容者の個人情報が、Winnyネットワーク上に流出していた	【Winnyの不適切な使用】	流出したのは滋賀刑務所や福岡拘置所の被収容者の氏名のほか、両施設内で規律違反を犯した被収容者に対する取り調べ記録、施設の規則を記した内部文書などを含む1万ファイル強。	L3-U2	2月3日に内閣官房情報セキュリティセンターが情報流出を確認し、法務省に連絡した。	http://internet.watch.impress.co.jp/cda/news/2006/02/14/10875.html

22	日本データ通信協会、メールサーバーの不正アクセス事件で元職員逮捕	2006/3/7	電気通信回線設備の接続工事に関する「平成 18 年度第 1 回工事担任者試験」の申請受付で使用していたメールサーバーが第三者に不正アクセスされ、一部のメールが消失した疑いがあると発表していた。	【退職職員の不正アクセス】	一部のメールが消失した疑いがあると発表していた。警視庁の発表によると、元職員は 2 月 24 日から 27 日にかけて、18 回にわたりメールサーバーに不正アクセスした上、約 6,100 件のファイルを閲覧し、約 1,600 件のメールを消去したという。	L3-U2		http://internet.watch.impress.co.jp/cda/news/2006/04/26/11801.html
23	中国国営銀行の Web サーバにフィッシング・サイト、内部犯行の可能性	2006/3/13（発表）	米国の大手銀行の顧客データを標的としたフィッシング・サイトが、中国の国営銀行の Web サーバにホスティングされた顧客から不審な電子メールを受け取ったという届け出があったため調査したところ、同メールには、中国建設銀行（CCB）上海支店の IP アドレスを持つサーバ上の“隠しディクトリ”に設置されたフィッシング・サイトへ誘導する内容が記述されていたという。	【不正アクセス】	[アメリカチェース銀行のサービス利用者] 当該偽サイトに誘導されて、ID・パスワード等の入力を行った者については、ID/pswd（他のサービス利用にも同じ組み合わせを利用しているかもしれない。）等の漏洩及び漏洩データを利用したサービスの不正利用被害。 --- [アメリカチェース銀行] アメリカチェース銀行については、なりすましにより自社サービスが利用された場合の、サービス利用名義人本人に対する補償（銀行の場合）等の可能性。 --- [中国国営銀行] 中国国営営銀行は、フィッシングサイトを立てられたサーバが、不正侵入を受け勝手に利用される被害を受けている可能性。	L2-D1, L2-D3, L3-U1, L2-U1	顧客から不審な電子メールを受け取ったという届け出があったため調査。	http://www.computerworld.jp/news/sec/35058.html
24	島根県ホームページに DoS 攻撃、韓国の IP アドレスから大量のアクセス	2006/5/31	韓国のプロバイダの IP アドレスからのアクセスが，多い時で 1 秒間に 100 回近くあり，県ホームページがつながりにくい状況に。	【外部からのサービス妨害攻撃】	韓国のプロバイダの IP アドレスからのアクセスが，多い時で 1 秒間に 100 回近くあり，県ホームページがつながりにくい状況になったという。5 月 30 日のアクセス件数は 212 万 6730 件で，前日 5 月 31 日の 1 万 6581 件に比べ約 128 倍となった。	L4-P1		http://itpro.nikkeibp.co.jp/article/NEWS/20060602/239853/

25	AT&T に不正アクセス、顧客情報が漏えい	2006/8/30（発表）	何者かが同社のコンピュータシステムに侵入し、クレジットカード情報などの顧客の個人情報にアクセスした。	【不正アクセス】	この件の影響を受けるのは同社の Web ストアから DSL 機器を購入した顧客 1 万 9000 人弱。同社はこれら顧客に電子メール、電話、書簡などで通知しているところだという。	L2-D1, L2-D3, L3-U1, L2-U1	不正アクセスは週末に発生、同社は数時間でこれに気づき対応。	http://www.itmedia.co.jp/news/articles/0608/30/news043.html
26	ジェット証券に不正アクセス、顧客情報盗難	2006/11/14	ジェット証券の顧客 9 名分の ID とパスワードを不正に取得し、サーバにアクセスした。容疑者は自動的にアクセスを試行するプログラムを作成し、2 日間 で 17 万回のアクセスを行い、26 名分の ID とパスワードを入手、このうち 5 名分の取引履歴を閲覧していた。	【外部からの不正アクセス】	26 名分の ID とパスワードを入手、このうち 5 名分の取引履歴を閲覧していた。	L2-D1, L2-D3, L3-U1, L2-U1		https://www.netsecurity.ne.jp/1_8865.html
27	日本銀行のサイトに DDoS 攻撃	2006/12/13	日本銀行のサイトに対して DDoS 攻撃が行なわれ、ページの閲覧が困難となる状況が発生した。現在は措置を講じたことにより、閲覧に支障のない状態に戻った	【外部からのサービス妨害攻撃】	[日本銀行] 適切な情報発信が行えなかったことによる、日本銀行の信頼の喪失。	L4-P1		http://internet.watch.impress.co.jp/cda/news/2006/12/14/14248.html
28	大阪府のサイトに不正アクセス、一部サービスを除いて公開を停止	2007/4/23	大阪府の Web サイトが不正アクセスによってトップページが書き換えられる事態が発生した。 大阪府では原因については調査中としており､24 日現在では電子入札など一部のサービスのみ再開している。	【不正アクセス】	[大阪府] 適切な情報発信が行えなかったことによる、大阪府の信頼の喪失。	L2-D1, L2-D3, L3-U1, L2-U1	2007/4/23 2:00 pm 大阪府職員が気づく。	http://internet.watch.impress.co.jp/cda/news/2007/04/24/15530.html

29	政府のサーバで詐欺サイトをホスティングバックドアなどで不正侵入	2007/7/13（発表）	詐欺サイトは公式サイトに見せかけてユーザーをだまし、政府が発行した身分証明書番号や銀行のパスワード、クレジットカード番号などを入力させるようになっている。ホスティングしている政府サイトの多くは、バックドアや Web インタフェースの脆弱性などを使ってサーバに不正侵入されたとみられる。	【外部からの不正アクセス】	[サービス利用者] 当該偽サイトに誘導されて、ID・パスワード等の入力を行った者については、ID/pswd 等の漏洩及び漏洩データを利用したサービスの不正利用被害。 --------- [上記該当国政府] なりすましにより政府サービスが利用された場合の、サービス利用名義人本人に対する補償（銀行の場合）等の可能性。 --------- [フィッシングサイトを立てられたサーバの管理者] ・フィッシングサイトを立てられたサーバが、不正侵入を受け勝手に利用される被害を受けている可能性。	L2-D1, L2-D3, L3-U1, L2-U1	Symantec が 2007/7/12 ブログにて報告。	http://www.itmedia.co.jp/enterprise/articles/0707/13/news031.html
30	長崎県平戸市のサイトが改竄、ウイルス感染の恐れも	2007/10/18	長崎県平戸市のホームページが不正アクセスを受け、10 月 18 日から 11 月 30 日までにトップページが 21 回にわたって、不正コード埋め込みの改竄が行われた。	【SQL インジェクション】	1,683 件のアクセスが確認されているが、「ウイルス感染による個人情報漏洩などの被害は確認していない」（平戸市）。	L3-P1, L2-D1, L2-D3, L1-D2, L2-M1, L3-U1		http://internet.watch.impress.co.jp/cda/news/2007/12/11/17829.html http://www.is702.jp/news/detail.php?id=101 http://www.so-net.ne.jp/security/news/library/1325.html http://www.security-next.com/007270.html

31	全日空商事、不正アクセスで改ざん被害、個人情報漏洩のおそれも	2007/10/21（発表）	全日空商事の米現地法人－米国全日空商事が運営する通信販売サイトが、現時時間 10 月 21 日午前 2 時ごろに不正アクセスを受けた。	【不正アクセス】	流出のおそれがあるのは、顧客情報 4154 人分で、大半は北米利用者の個人情報だが、日本人の個人情報も 113 人分も含まれ、氏名や住所、電話番号、メールアドレス、クレジットカードなどが漏洩した可能性がある。	L3-P1, L2-D1, L2-D3, L1-D2, L2-M1, L3-U1		http://www.anatc.com/information/2007/11/12-unlawful.html http://www.security-next.com/007132.html http://internet.watch.impress.co.jp/cda/news/2007/11/13/17501.html
32	JR 東日本、モバイル Suica 不正利用	2007/11/9（発表）	モバイル Suica で、2006 年 12 月頃から、不正に入手したカード情報で他人になりすまし、電子マネーが使用される被害が相次いでいた。	【設計時の考慮不足】	不正に使われたカードは 65 枚に上り、被害額は確認できているものだけで約 1000 万円に上る。	L2-D2		http://www.itmedia.co.jp/news/articles/0711/09/news033.html http://k-tai.impress.co.jp/cda/article/news_toppage/37145.html
33	会津若松市のサイトに不正アクセス、フィッシングページ設置	2007/11/27	会津若松市サイト内の「教育ポータルサイト」。 架空の企業の疑似ページが作成され、フィッシング行為を行なっていたのもと見られる。	【フィッシング】	[会津若松市役所] 適切な情報発信が行えなかったことによる、会津若松市役所の信頼の喪失。	L2-D2, L2-U2	27 日に、市が利用している通信事業者より、サイトが不正利用されている可能性があるとの連絡を受け。	http://internet.watch.impress.co.jp/cda/news/2007/11/30/17700.html

34	運河用水路システムへの不正ソフトインストール	2007/11/30	カリフォルニア州で、オペレータが運河（用水路）の監視制御（SCADA）システムに、不正にソフトウェアをインストールし、システムに損害	【内部職員の過失】	深刻な物理的損害（発電機やタービンの損傷）の可能性があった。	L4-U1		Insider charged with hacking California canal system - A man has been charged with hacking a computer used to control water canals in California http://www.computerworld.com.au/index.php/id;511545055;fp;2;fpid;1
35	Cox Communications 元社員が不正アクセス	2008/1/10	米 CATV 大手 Cox Communications、元社員による不正アクセスによってシステムの一部がシャットダウン。	【退職職員の不正アクセス】	緊急通報用電話を含む通信サービスが、テキサス、ラスベガス、ニューオリンズなどで停止。停止時間は数時間程度。	L3-U2		Norcross hacker sent to prison http://www.northfulton.com/Articles-i-2007-12-27-169168.112113_Norcross_hacker_sent_to_prison.html

36	ホワイトハウスのシステムにハッカーが侵入	2008/1/10	ホワイトハウスのシステムにハッカーが侵入。また、大統領選挙期間にオバマ・マケイン両陣営のシステムにもハッカーが侵入しており、次期政権によるサイバーセキュリティへの取り組みの重要性を示唆する声も。	（不明）	（情報なし）	（該当なし）		Campaign Hacks Highlight Cyber-espionage http://securitywatch.eweek.com/exploits_and_attacks/campaign_hacks_highlight_cyber-espionage.html
37	ポーランドの路面電車システムに不正アクセス、脱線	2008/1/11	ポーランドで 14 歳の少年が路面電車システムに不正アクセスし、切替ポイントを操作。車両の脱線や緊急停止を引き起こし 20 人が負傷。	【設計時の考慮不足】【システムの独立性不足】	4 車両の脱線と、他の車両の緊急停止。20 人が負傷、死者なし。	L3-P1, L2-D1, L3-U1		Polish teen derails tram after hacking train network http://www.theregister.co.uk/2008/01/11/tram_hack/print.html
38	公益インフラにサイバー攻撃、複数都市で停電も	2008/1/21（発表）	SANS のサイトに掲載された情報によると、サイバー攻撃によって電力施設に障害が発生し、複数の都市で停電が起きたケースが少なくとも 1 件あったと報告した。	【外部からの不正アクセス】	電力などの公益インフラ。	L3-P1, L2-D1, L2-D3, L3-U1	CIA の担当者が SANS の講演で発表。	http://www.itmedia.co.jp/enterprise/articles/0801/21/news006.html
39	岡谷市のウェブサイトが改ざん被害	2008/2/14	不正アクセスにより、サーバ上の一部ファイルが改ざんされた。登録されている個人情報の漏洩や予約への影響はなかった。	【外部からの不正アクセス】	不正アクセス発覚後に公共施設の予約受付を窓口や電話に切り替え、システムを停止。	L3-P1, L2-D1, L2-D3, L3-U1	復旧までには 1 週間程度、約４０万円の費用。	http://www.security-next.com/007616.html

40	新生銀ネットワークに不正アクセス	2008/2/18	シャルマ容疑者は 以前、新生銀に派遣社員として務めていたときに入手していたＩＤとパスワードを使い、６７回にわたって新生銀の内部ネットワークに不正にアクセス。約２６００件のファイルを削除するなど社員用ウェブサイトを改竄。	【退職職員の不正アクセス】	シャルマ容疑者の犯行により、新生銀の内部システムは約１５時間停止。社員用ソフトが使えなくなるなどの被害が出た。顧客の情報流出や金銭的被害はないという。	L3-U2		http://www.nikkei.co.jp/news/past/honbun.cfm?i=AT1G1601K%2016072008&g=K1&d=20080716 (dead link) http://sankei.jp.msn.com/affairs/crime/080716/crm0807161151017-n1.htm
41	豊中市のウェブサイトが改ざん被害	2008/3/13	介護マップや防災マップ、災害時給水ポイントマップ、休日・救急病院マップに不正サイトへのリンクが設置された。	【外部からの不正アクセス】	サイトにアクセスしようとすると、ウイルスに感染する可能性があった。	L2-D3, L1-D2, L2-M1, L3-U1	利用者に、ウイルスの検索や駆除などするよう呼びかけ。	http://sankei.jp.msn.com/affairs/crime/080313/crm0803132357047-n1.htm

42	ゆうちょ銀行をかたる詐欺メール	2008/3/14（発表）	日本郵政グループのゆうちょ銀行は 3 月 14 日、同行をかたったスパムメールが出回っているとして、利用者などに注意を呼びかけた。 このメールは「ゆうちょダイレクト【重要なお知らせ】」というタイトルで送信され、本文中に記載されたリンク先を参照するように促がす内容となっている。リンク先はゆうちょダイレクトに似せた Web サイトで、ID とパスワード、インターネットサービス用の暗証番号を閲覧者に入力させる仕組み。同サイトは国内でホスティングされていたとみられるが、すでに閉鎖されている。	【フィッシング】	[ゆうちょ銀行のサービス利用者] 当該偽サイトに誘導されて、ID・パスワード等の入力を行った者については、ID/pswd 等の漏洩及び漏洩データを利用したサービスの不正利用被害。 --------- [ゆうちょ銀行] ゆうちょ銀行については、なりすましにより自社サービスが利用された場合の、サービス利用名義人本人に対する補償（銀行の場合）等の可能性。 --------- [フィッシングサイトを立てられたサーバの管理者] フィッシングサイトを立てられたサーバが、不正侵入を受け勝手に利用される被害を受けている可能性。	L2-D2, L2-U2		http://www.itmedia.co.jp/enterprise/articles/0803/14/news061.html
43	南越前町のウェブサイトが改ざん被害	2008/3/25（発見）	南越前町の公式ホームページ（ＨＰ）のサーバーに不正アクセスがあり、プログラムが改ざんされた。内部情報は別のサーバーで管理しているため、流出なし。	【SQL インジェクション】	サイトに文字化けが発生していた。	L3-P1, L2-D1, L1-D2, L2-M1, L3-U1	閲覧者にウイルスチェックを呼び掛け。	http://www.fukuishimbun.co.jp/modules/news2/article.php?storyid=3605
44	ハッカー侵入で政府機関の個人情報流出。チリ	2008/5/10	ハッカーは教育省や選挙管理当局、国営電話会社のウェブサイトに侵入し、氏名、住所、電子メールアドレス、電話番号、職歴や学歴などの個人情報を盗み出した。	【外部からの不正アクセス】	国営電話会社のウェブサイトから詐取が可能な氏名、住所、電子メールアドレス、電話番号、職歴や学歴などの個人情報。合計 600 万件。	L3-P1, L2-D1, L2-D3, L3-U1		http://www.afpbb.com/article/disaster-accidents-crime/crime/2390215/2920311

45	さくらインターネットにおける通信経路改ざん被害	2008/6/2	ホスティングサービスに不正アクセスがあり、同サービスを通じて公開されているサイトを閲覧した際、不正なコードが埋め込まれる。	【ネットワーク経路の改ざん】	Web ページ中に不正なコードが埋め込まれ、ウイルスなどをダウンロードさせられる可能性があった。	L2-D1, L3-P3		http://www.security-next.com/008320.html http://support.sakura.ad.jp/page/news/20080602-001.news
46	内閣府のホームページで個人情報が流出か	2008/6/6	パブリックコメントに寄せられた意見を掲載していた国民生活局のホームページで、個人情報が閲覧可能になっていた。	【内部職員の過失】	流出した可能性がある個人情報は 36 件で、期間は 6 月 6 日から 8 月 6 日まで。	L3-U2, L4-U2		http://www.nikkei.co.jp/news/shakai/20080901AT1G0101D01092008.html
47	ロンドン地下鉄の「オイスターカード」がハックされる	2008/6/18	オランダのラドボウド大学の研究チームが、ロンドンで使われている非接触式 IC カード、通称オイスターカードのクラックに成功したと発表しました。	【設計時の考慮不足】	研究チームは、実際に地下鉄を無料で乗降するのに成功し、DoS 攻撃により地下鉄のゲートを強制的に閉じる事にも成功。	L2-P2, L3-P3	Oyster Card には、安全対策が施された多くの場所に出入りするためのセキュリティー・カードで使われているのと同じ『Mifare』チップが入っている。	Fears for Oyster security as researchers claim crack http://news.zdnet.co.uk/security/0,1000000189,39437719,00.htm?r=1
48	Citibank 社サーバーへ不正アクセス、ATM で大規模な引き出し	2008/6/20（発表）	現金自動預払機(ATM)の引き出し処理を担う Citibank 社のサーバーに不正アクセスがあり、その結果、男性 2 名がニューヨーク市内の ATM から数百回にわたり不正に現金を引き出していた。	【外部からの不正アクセス】	2 人は少なくとも 75 万ドルの現金を不正に得ていたという。	L3-P1, L2-D1, L2-D3, L3-U1		http://wiredvision.jp/news/200806/2008062021.html
49	北陸朝日放送の番組参加者個人情報流出	2008/7/5	携帯電話などを利用した視聴者参加番組において、一部視聴者の個人情報が流出。携帯電話の「簡単ログイン」機能を使う際に、本来、携帯電話機の固体認識番号を 15 桁で認識するよう設定すべきところを 11 桁としていたのが原因。	【設計時の考慮不足】	25 人の氏名、一部住所、電話番号、メールアドレス、性別などが閲覧できる状態となった。	L2-D2, L1-D2, L2-M1, L3-U1		http://www.security-next.com/008567.html

50	NTT 西日本沖縄支店からの顧客情報流出	2008/7/7	顧客の個人情報が、地図検索サイト上に公開されていた。	【内部職員の過失】	那覇市内の顧客 63 人の個人情報が漏えい。氏名や住所のほか、うち 14 件は電話番号が含まれていた。	L3-U2		http://internet.watch.impress.co.jp/cda/news/2008/07/11/20235.html
51	石油大手 Shell で ID 窃盗	2008/7/10（発見）	米国テキサス州の労働環境を監督し、雇用促進サービスを提供する州機関 Texas Workforce Commission (TWC) は、石油大手 Shell の従業員から社会保障番号が盗まれたとの連絡を受けて調査に着手し、それが容疑者の発見につながった。	【外注先職員の不正】	虚偽の失業手当を請求するのに悪用。	L2-D2, L3-P6		http://japan.internet.com/busnews/20081014/11.html
52	資源機構の公開サーバーに対する不正侵入とホームページの改ざん	2008/7/27	石油天然ガス・金属鉱物資源機構(JOGMEC)のサーバが SQL インジェクションにより改ざん。閲覧者にウイルス感染のおそれ。改ざんされたサイトにアクセスしたパソコンは、改ざん者が作成・準備したサーバ（悪質なプログラムの置き場）に自動的に誘導され、悪質なプログラムを強制的にダウンロードされた可能性がある。	【SQL インジェクション】	石油天然ガス・金属鉱物資源機構及び該当サイト閲覧者、利用者がウイルスへ感染するおそれがあった。	L3-P1, L2-D1, L2-D3, L1-D2, L2-M1, L3-U1		http://www.asahi.com/national/update/1020/TKY200810200153.html http://www.jogmec.go.jp/news/release/docs/2008/pressrelease_080918.pdf
53	ボストン地下鉄の「CharlieCard」がハックされる	2008/8/8	「DEFCON 16」において、米国マサチューセッツ連邦地方裁判所はマサチューセッツ湾交通局（MBTA）の電子切符システムの脆弱性に関するプレゼンテーションに対し、実施差し止めを命じる仮処分を決定した。結果、プレゼンテーションは行われなかったものの、電子フロンティア財団（EFF）はこの処分を不服とし、控訴する意向を明らかにした。	【設計時の考慮不足】	未遂のため実害なし。	L2-P2, L3-P3	世界中の交通システムで幅広く採用されている「Mifare Classic」技術をベースとしたもの。	http://www.computerworld.jp/topics/vs/118469.html

54	受刑者個人情報が流出、英国	2008/8/26（発表）	英イングランドとウェールズの刑務所で服役中の受刑者情報を記録した USB メモリが紛失した。問題の USB メモリは、業務外注先の民間企業 PA Consulting が保有していた。内務省はデータを暗号化して PA Consulting に電子メールで送ったが、PA Consulting が暗号を解除して USB メモリに保存していたという。	【内部職員の過失】	紛失した USB メモリには受刑者 13 万人の氏名、住所、生年月日のほか、一部は釈放予定日まで記載されていたという。	L3-U2		http://www.itmedia.co.jp/enterprise/articles/0808/26/news031.html
55	American Express Card をかたるフィッシング	2008/10/29（発表）	AmericanExpressCard をかたるフィッシングメールが確認されています。新たなセキュリティ施策の一環と称して、フィッシングサイトに誘導します。	【フィッシング】	[AmericanExpress のサービス利用者] 当該偽サイトに誘導されて、ID・パスワード等の入力を行った者については、ID/pswd（他のサービス利用にも同じ組み合わせを利用しているかもしれない。）等の漏洩及び漏洩データを利用したサービスの不正利用被害。 --------- [AmericanExpress] なりすましにより自社サービスが利用された場合の、サービス利用名義人本人に対する補償（銀行の場合）等の可能性。 --------- [フィッシングサーバを立てられた管理者] ・フィッシングサイトを立てられたサーバが、不正侵入を受け勝手に利用される被害を受けている可能性。	L2-D2, L2-U2		http://www.antiphishing.jp/database/database306.html
56	大阪府の HP にサイバー攻撃、手続きなど一時まひ	2008/11/11	ホームページの閲覧を要求する大量の通信データを受け、処理システムが一時的にまひした。	【外部からのサービス妨害攻撃】	ホームページの閲覧や電子入札の手続きが一時的にできなくなった。	L4-P1		http://headlines.yahoo.co.jp/hl?a=20081111-00000029-yom-soci

57	ロサンゼルスで信号機への不正アクセス	2008/11/12（発表）	ロサンゼルスで、道路交通技術者が、賃金交渉に係る不満から市の信号機を制御する自動制御センターに侵入。制御システムに不正アクセス。	【内部職員の不正アクセス】	重要地点の信号機をシャットダウンし、交通を混乱させる。完全回復に 4 日掛かる事態に。	L3-U2		LA engineers admit traffic-light hack http://www.vnunet.com/vnunet/news/2230263/los-angeles-engineers-pled
58	米国防総省（DoD）でウイルス感染	2008/11/24（発表）	米国防総省（DoD）のネットワークがグローバル規模でウイルス感染。対策として、メモリースティック、フラッシュメモリカード、USB メモリなど、リムーバブルメディアの使用を全面禁止したとの話も。	（不明）	グローバル規模。それ以上の情報は非公開。	L3-P3, L2-D1, L2-D2, L2-U1		http://www.airforcetimes.com/news/2008/11/military_thumbdrives_computerworm_112108w/

付録 B

再発防止策一覧表

	段階	対策 ID	対策
LV4	企画	L4-P1	外部からの意図した攻撃（DDoS: Distributed Denial of Service 攻撃など）に耐えうるインフラ（ネットワークやサーバ等）が検討されている。
	運用	L4-U1	関係者の承認を得たソフトウェアのみをインストールできる仕組みが整備されている。
		L4-U2	関係者へのセキュリティ教育が行き届いており、セキュリティインシデント規約（関係者連絡先、メディア対応など）に基づく模擬訓練も行われている。
LV3	企画	L3-P1	外部からの攻撃を想定したセキュリティポリシーを定めている。
		L3-P2	利用者がシステムに対する悪意を持った場合を想定したリスク分析を行っている。
		L3-P3	システムの一部が侵入を受けた場合でも、その影響を局所に限定する仕組みが明確になっている。
		L3-P4	セキュリティインシデントに対応する体制（CSIRT: Computer Security Incident Response Team）が整備されている。
		L3-P5	フォレンジックを考慮したセキュリティログ収集が検討されている。
		L3-P6	外注先の管理を十分に行う仕組みが整備されている。
		L3-P7	外注の際には発注要件の中にセキュリティ要件を含んでいる。
	開発	L3-D1	セキュリティログを保存する仕組みを持っている。
	保守	L2-M1	ウェブアプリケーションに対するペネトレーションテスト（クロスサイトスクリプティングや SQL インジェクションなどの脆弱性のテスト）が行われている。
	運用	L3-U1	不正アクセス等のセキュリティ攻撃については、リアルタイムでの監視（ファイアウォール、IDS: Intrusion Detection System/IPS: Intrusion Prevention System、WAF: Web Application Firewall、セキュリティログなど）を実施している。
		L3-U2	オペレータには、必要な情報にアクセスする最小限の権限を与えており、不要な情報へのアクセスはできない仕組みとなっている。また、配置転換時は速やかに権限を更新している。
		L3-U3	定期的に、サーバおよびウェブアプリケーションに対するペネトレーションテストが行われている。
LV2	企画	L2-P1	可用性、保全性に加え、機密性に関するリスク分析を行っている。
	開発	L2-D1	セキュリティを考慮したシステム構成（ファイアウォール、IDS: Intrusion Detection System/IPS: Intrusion Prevention System 、 WAF: Web Application Firewall など）が考慮されている。
		L2-D2	セキュリティの観点（不正アクセス、ウイルス、フィッシングなど）からの仕様レビューが行われている。
		L2-D3	サーバに対するペネトレーションテストが行われている。
		L2-D4	ウェブアプリケーションに対するペネトレーションテスト（クロスサイトスクリプティングや SQL インジェクションなどの脆弱性のテスト）が行われている。
	運用	L2-U1	セキュリティ脆弱性情報の定期的な収集、分析、対策が行われている。ウイルス対策ソフト等の定義ファイルが適切に更新されている。
		L2-U2	利用者に対して、フィッシングを考慮したセキュリティ教育を行っている。
LV1	開発	L1-D1	セキュリティに関するソースコードレビューが行われている。