医政研発 0314 第２号
平成 28 年３月 14 日

公益社団法人全日本病院協会会長　殿

厚生労働省医政局研究開発振興課長

伊勢志摩サミット等開催に伴う医療機関におけるサイバーセキュリティ対策等について

医療分野の情報化につきましては、平素より多大な御理解、御尽力を賜り、厚く御礼申し上げます。

標記につきまして、今般、別添のとおり各都道府県衛生主管部（局）長宛てに通知しましたので、御了知いただくとともに、傘下会員に対しその周知方よろしくお願いします。

写

医政研発 0314 第 1 号
平成 28 年 3 月 14 日

各都道府県衛生主管部（局）長 殿

厚生労働省医政局研究開発振興課長
（公印省略）

伊勢志摩サミット等開催に伴う医療機関におけるサイバーセキュリティ対策等について

医療分野の情報化につきましては、平素より多大な御理解、御尽力を賜り、厚く御礼申し上げます。

今般、伊勢志摩サミットが 5 月 26 日及び 27 日に開催されること等に伴い、別添のとおり、警察庁警備局長から警備協力の要請がありました。

つきましては、伊勢志摩サミット及び関係閣僚会合開催中における医療機関のサイバーセキュリティ対策の強化等について、下記のとおり、管内関係機関に対し周知・徹底を図られますようお願いします。

記

1．「医療情報システムの安全管理に関するガイドライン 第 4.2 版」（平成 25 年 10 月 厚生労働省）※1 に基づき、主に以下の点から、サイバー攻撃発生時に遅滞なく対応できるよう情報セキュリティ確保について改めて点検を行うとともに、必要に応じて技術的安全対策等を実施すること。

①利用者の識別及び認証

情報システムへのアクセスを正当な利用者のみに限定するために、情報システムは利用者の識別と認証を行う機能を持つ必要がある。

②情報の区分管理とアクセス制限の管理

情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。

③アクセスの記録

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認す

る必要がある。

④不正ソフトウェア対策

不正ソフトウェアのスキャン用ソフトウェアの導入及びパターンファイルの最新のものへの更新、オペレーティング・システム等でセキュリティ・ホールの報告されているものについての対応版（セキュリティ・パッチと呼ばれるもの）への更新が必要である。

⑤ネットワーク上からの不正アクセス対策

コンピュータウイルスや不正アクセスを目的とするソフトウェア等の攻撃から情報システムを保護等するための対策が必要である。

2．サイバー攻撃への対応として、別添の「サイバー攻撃対応力向上の手引き（第3版）」（平成27年1月20日セプターカウンシルサイバー攻撃対応力向上WG（第3版改訂情報共有WG））※2や独立行政法人情報処理推進機構(IPA)において公表されている対策「標的型攻撃メールの例と見分け方」※3についても参考にされたい。

3．医療機器における対策については、「医療機器におけるサイバーセキュリティの確保について」（平成27年4月28日 薬食機参発0428 第1号 薬食安発0428 第1号 厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当） 厚生労働省医薬食品局安全対策課長 通知）※4を参考にされたい。

※1：「医療情報システムの安全管理に関するガイドライン」

特に「6.2 医療機関における情報セキュリティマネジメントシステム(ISMS)の実践」「6.5 技術的安全対策」「6.9 情報及び情報端末の持ち出しについて」「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

http://www.mhlw.go.jp/stf/shingi/0000026088.html

※2：「サイバー攻撃対応力向上の手引き」

セプターカウンシル（電気、金融、医療等の重要インフラ分野の代表で構成される協議会）において、各重要インフラ事業者等におけるサイバー攻撃に係る対応力の向上に資することを目的に作成されたもの。

※3：「標的型攻撃メールの例と見分け方」

http://www.ipa.go.jp/security/technicalwatch/20150109.html

※４：「医療機器におけるサイバーセキュリティの確保について」
http://www.mhlw.go.jp/file/05-Shingikai-11121000-Iyakushokuhinkyoku-Soumuka/0000090664.pdf

写

警察庁丙備発第19号
平成28年2月1日

厚生労働省大臣官房長 殿

警察庁警備局長

伊勢志摩サミット等開催に伴う警備協力について（要請）

貴台におかれましては、平素から警察運営に際して御理解と御協力を賜り、深く感謝申し上げる次第です。

伊勢志摩サミット等につきましては、首脳会議が５月26日及び27日に三重県志摩市賢島において開催されます。また、関係閣僚会合につきましては、外務大臣会合が４月10日及び11日に広島市において、農業大臣会合が４月23日及び24日に新潟市において、情報通信大臣会合が４月29日及び30日に高松市において、エネルギー大臣会合が５月１日及び２日に北九州市において、教育大臣会合が５月14日及び15日に倉敷市において、環境大臣会合が５月15日及び16日に富山市において、科学技術大臣会合が５月15日から17日までの間つくば市において、財務大臣・中央銀行総裁会議が５月20日及び21日に仙台市において、保健大臣会合が９月11日及び12日に神戸市において、交通大臣会合が９月24日及び25日に軽井沢町において、それぞれ開催されます。

伊勢志摩サミット等の開催をめぐっては、我が国に対する国際テロの脅威が現実のものとなっているほか、サイバー攻撃やドローン等小型無人機を使用したテロ等への対応が重要な課題となっていることに加え、極左暴力集団や右翼による「テロ、ゲリラ」事件等の発生を未然に防止するために万全の対策を講じる必要があります。

さらに、昨年11月にフランス・パリにおいて発生した同時多発テロ事件では、スタジアムや劇場等が標的となって多数の犠牲者等が発生したところであり、いわゆる「ソフトターゲット」への対策の重要性が改めて認識されております。

警察では、伊勢志摩サミット等参加国首脳等の身辺の絶対安全と諸行事の円滑な遂行を確保し、我が国におけるテロ等の未然防止を図るため、全国警察の総力を挙げて各種対策を推進しております。

貴台におかれましても、本警備の重要性を御勘案の上、次の事項につきまして指導を強化されるなど適切な措置を講じられますよう要請いたします。

厚生労働省に対する要請事項

○ 各省庁共通要請事項

1 自主警備体制の強化

2 連絡体制の確立

3 首脳会議・関係閣僚会合（以下「サミット等」という。）関連情報及び不審者等情報の警察への通報連絡の徹底

4 サミット等開催場所周辺における大規模行事、公共工事、業務用車両利用及びドローン等小型無人機の使用の自粛

5 業務用車両、身分証明書、制服等の管理及び盗難・紛失時の警察への連絡の徹底

6 関係機関に対する交通規制内容の周知及びサミット等開催地における交通総量抑制に向けた指導

7 サイバーセキュリティ対策の強化

○ 個別要請事項

1 サミット等開催地における救急医療体制の確立

2 ＮＢＣテロ対策に係る警察との連携の強化

3 爆発物の原料となり得る化学物質の販売事業者に対する管理強化の指導

4 病院、研究所等に対する毒劇物、生物剤等の管理強化の指導

5 研究所等における特定病原体等の管理強化

6 旅館、ホテル等に対する食中毒防止を始めとする衛生管理徹底の指導

7 旅館、ホテル等に対する宿泊者名簿及び日本国内に住所を有しない外国人宿泊者の旅券の写しの保存の徹底の指導

8 警察部隊に対する医療支援

9 ドクターヘリ管理者等に対する管理強化の指導

10 サミット等開催場所周辺における緊急走行時の110番通報

11 重要インフラ事業者等に対する自主警備体制及びサイバーセキュリティ対策の強化の指導

12 飲食店、ホテル、劇場等のソフトターゲットに対する警戒強化の指導

13 保健大臣会合における自主警備体制の強化と会合運営受託業者に対する適切な指導

当該医療機関限り※

サイバー攻撃対応力向上の手引き

（第３版）

２０１５年１月２０日

セプターカウンシル
サイバー攻撃対応力向上WG
（第３版改訂　情報共有WG）

目次

Ⅰ．はじめに

1．本手引きの目的等

- 重要インフラ事業者等は日々サイバー攻撃被害の未然防止・拡大防止に取り組んでいるが、サイバー攻撃の手口は高度化かつ巧妙化している。
- そのため、セプターカウンシルでは、各重要インフラ事業者等におけるサイバー攻撃に係る対応力の向上に資することを目的に「サイバー攻撃対応力向上WG」を開催し（2009 年 6 月～2011 年 4 月迄、延べ 10 回開催。活動状況は「Ⅵ　WGの活動履歴」を参照のこと。）、外部の関連機関等より有識者を招いて意見交換を図る中で、対応すべき脅威の洗い出しとその未然防止・拡大防止のあり方について整理を行った。本手引きは、WG 活動の成果を広く各セプターに所属する重要インフラ事業者等に提供することにより、各事業者におけるサイバー攻撃に係る対応力の向上に資することを目的に作成した。
- 本手引きが、「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第３版）　改定版」等の活用と合わせ、重要インフラ事業者等における情報セキュリティ確保にあたり、サイバー攻撃への対応を検討する際の参考となることを期待する。
- 本手引きの読者として、重要インフラ事業者等の情報セキュリティを監督する管理職に読まれることを想定したが、情報システムに携わる幅広い関係者にとっても有用なものとなるように努めた。
- 本手引きは、サイバー攻撃に関する最新の動向や対策を把握できるように適宜更新する（本手引きの維持管理については「Ⅴ　本手引きの維持管理」を参照のこと。）。

2．留意事項

- サイバー攻撃への対応については、各社において保有しているシステムに関係する主体（ISP やベンダなど）に、最初に相談することを前提とし、本手引きは、個社の契約の範囲を超えた対策の検討の参考に資するものとする。

Ⅱ．対象とする脅威

本手引きでは、WG メンバーへのアンケート・ヒアリングを踏まえ、重要インフラサービスに影響を与える可能性があるとした以下の６つの攻撃手法を重視する脅威として取り上げる。

- DDoS 攻撃
- 不正アクセス（Web サイトの改ざんを含む）
- フィッシング詐欺
- 迷惑メール
- ウイルス・ボット
- 標的型攻撃

Ⅲ. 各脅威への対応

1 DDoS 攻撃

（1）DDoS 攻撃の概要

- DDoS（分散サービス運用妨害）攻撃とは、多数のコンピュータから標的とするサーバやネットワーク回線に一斉に大量のリクエストを送付する等の手法により、サービス提供を不能にする攻撃である。
- DDoS 攻撃の目的には、大きく分けて（1）国家の重要なシステムをサービス不能状態にさせ、社会を混乱させる、（2）サービス運営者への恨みや営利目的の妨害、（3）詐欺や脅迫、がある。また、その他にも政治的、思想的な主張による示威的行動として、主張に関連する機関のサイトや掲示板サイトが攻撃の対象となることもある。
  （参考：2014 年版 情報セキュリティ 10 大脅威 P30-31）
- DDoS 攻撃の過去の事例
  ① ボットによる米韓への攻撃
  2009 年 7 月上旬に、予めボットが埋め込まれた数万台の PC から、一斉に米韓の政府機関や金融機関等への大量アクセスが実行され、大規模な接続障害が発生した。
  ② Antinny ワームによるコンピュータソフトウェア著作権協会（ACCS）への攻撃
  2004 年 3 月ファイル交換ソフト「Winny」を介して感染する「Antinny」ウイルスにより、当該協会の Web ページへ毎月の特定日に大量のアクセスが集中し、ページの公開不能という事態を引き起こした。
  （参考：ACCS 公表資料① ACCS 公表資料②）
  ③ クラウドサービス等を活用したサイバー攻撃に関する脅威
  最近の傾向として、クラウドサービスをはじめとした XaaS 市場が拡大しており、攻撃元が潤沢な NW リソースを保有せずとも、大規模なボット攻撃や迷惑メールを送るためのサーバ等の環境確保が容易となっている。
  （参考：付録 サイバー攻撃に関する事例集①）
- DDoS 攻撃対策の問題点には、正常な通信と不正な通信の見分けがつきにくいこと、攻撃を検知できたとしても自社での対応が難しいことが挙げられる。その他にも、送信元 IP アドレスが詐称されているため、攻撃元を把握することが困難なこと、攻撃対象となったサイトと設備を共用しているサイトが影響を受けたりすることがある。
  （参考：2014 年版 情報セキュリティ 10 大脅威 P30-31）

（2）重要インフラ分野における取り組み

- 重要インフラ分野の中には、ガイドライン等で DDoS 攻撃への対応について掲載し、公表しているケースもあり、以下の通り紹介する。
  ①電気通信分野
  電気通信分野における情報セキュリティ確保に係る安全基準 （P26）
  サーバ、ルータ、その他の IP ネットワーク設備を保護するため、ポート、IP アドレス、プロトコル毎に最小限の範囲で通信フィルタリング又は帯域制限ができることが望ましいとされている。またサービスによっては、信号処理レベルでの通信制御、利用者認証、アクセス権限管理と連動したフィルタリング等についても実施できることが望ましいとされている。
  電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン
  電気通信事業者が DoS 攻撃等のサイバー攻撃、ワームの伝染及び迷惑メールの大量送信及び

壊れたパケット等（以下、大量通信等）を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料として策定したガイドラインで、26 の具体的な事例への対応が記載されている。

（３）被害に遭わないための対策

ｉ）未然防止策

- 関連情報の収集

NISC からの情報提供や JPCERT/CC からの早期警戒情報及び注意喚起、JVN 等を活用する。DDoS 攻撃については、過去に以下の注意喚起が出されたことがある。

2010/04/28 いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウェアに関する注意喚起（公開）
2013/04/18 DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
2014/01/15 ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起

- DDoS 対策サービスの利用

ISP やセキュリティベンダーでは、DDoS 攻撃の未然防止策として DDoS 対策サービスを提供している。トラフィックの監視により攻撃を検知・抽出し、攻撃トラフィックのみを遮断するものや事前に設定した基準量を超える通信量が検知された場合にメール等で案内することで攻撃の早期発見を促すものがある。

（参考：OCN DDoS 対策サービス(NTT com)、IIJ DDoS プロテクションサービス(IIJ)、KDDI DDoS 攻撃対策サービス(KDDI)、ULTINA Internet DDoS 検知・防御サービス(Softbank)）

- 関連機関への相談

DDoS 攻撃の予兆を検知した場合や未然防止について不明な点がある場合、DDoS 攻撃の最新動向について聞きたい場合は JPCERT/CC の窓口に確認するとよい。検知した予兆等により攻撃元がある程度特定できる場合には、攻撃元への調整（攻撃の抑止、攻撃元国等における攻撃者コミュニティの動向の監視等）を依頼することもできる。

ⅱ）拡大防止策

- DDoS 対策サービスの利用

上記ｉ）を参照。

- ISP との連携

自社内での対応に限界がある場合には、ISP 等へ被害の報告を行い ISP 等との連携により被害の拡大を防ぐことができる。事前に契約等において ISP 等がどのような対応が出来るかという点やその費用について確認しておくと被害発生時に迅速に対応できる。

（参考：DDoS のインシデントにどのように対応するか（野村総合研究所））

- 所管省庁への報告

攻撃による被害が確認され、重要インフラサービスの提供に影響が出た場合には、各分野における業法等に基づいて、各所管省庁へ報告する。また、重要インフラ全体のサービス維持レベルの向上にヒヤリハット情報が役立つ場合があることから、被害のない場合についても所管省庁を通じて積極的に情報を共有していくことが望ましい。

- JPCERT/CC への連絡

自社のシステムが攻撃を受けている場合には、JPCERT/CC に連絡することで、攻撃を低減でき

る場合がある。

- システム復旧時の顧客対応
  利用者との信頼関係を損なわないよう、攻撃を受けた後に、詳細な対応方法を説明した障害報告を発表することが重要である。
  （参考：2010 年版 10 大脅威（IPA）P21）

（４）踏み台にならないための対策

ｉ）未然防止策

- ボット・ワーム対策
  DDoS 攻撃の踏み台とならないようするためにボットやワームの感染を防ぐ対策（脆弱性対策等）を行うと良い。詳細については、「５　ウイルス・ボット　（４）ｉ）」を参照。
- 早期警戒情報等の確認
  JPCERT/CC 早期警戒グループが提供している早期警戒情報等を確認し、自社システムへの影響及び対応の必要等を確認する。踏み台に関する注意喚起については以下のものがある。
  2010/04/28　いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウェアに関する注意喚起（公開）

ii）拡大防止策

- 所管省庁及び JPCERT/CC への報告・連絡
  自社のシステム等が踏み台にされて外部への攻撃を実行していることが確認された場合には、適宜各所管省庁へ報告する。また、海外などへの攻撃活動を考慮し、JPCERT/CC に連絡し、拡大防止に心がける。
- システムの状況の確認
  どのシステムが踏み台となっているか、踏み台となっているシステムがどこから指令を受け、どこへ攻撃を行っているのかについては、それぞれのシステムに応じて確認内容が異なるが、例えば、特定 IP アドレスへの異常な通信履歴などを確認し、踏み台とされたシステムの状況を確認する。
- ネットワークからの隔離
  サーバへの侵入の痕跡を発見した場合や、サーバのルート権限を奪われる等により不正な処理を開始した場合には、当該サーバをネットワークから隔離する。
  （参考：情報通信ネットワーク安全・信頼性基準別表４ 3.(3)（総務省））
- その他にも、ウイルス・ボットによる感染被害の拡大を防止することも対策としてあげられる。詳細については、「５　ウイルス・ボット　（４）ii）拡大防止策」の項目を参照。

２　不正アクセス

（１）不正アクセスの概要

- 不正アクセスとは、システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うことである。ソフトウェアの脆弱性の悪用やパスワード窃取により情報を盗み見たり、削除・改変したりする行為がこれに当たる。
  （参考：コンピュータ不正アクセス基準(平成 8 年通商産業省告示第 362 号制定)）
- コンピュータウイルス・不正アクセスの状況については、IPA が届出状況を、国家公安委員会・総務省・経済産業省が発生状況を公表しており、直近の傾向等を把握することが出来る。

① コンピュータウイルス・不正アクセスの届出状況について（IPA）
② 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況（2014年、国家公安委員会・総務省・経済産業省）

- 不正アクセスの過去の事例

① 2009年から、ウェブサイト管理用のIDとパスワードを盗むガンブラーと呼ばれる手口が多発している。盗まれたIDとパスワードが悪用されてウェブサイトを改ざんされることで、そのウェブサイトを閲覧した利用者のIDとパスワードがさらに盗まれるという被害の連鎖を引き起こした。
（参考：コンピュータウイルス・不正アクセスの届出状況について(2010年2月分、IPA)）
② 2010年、ある組織でウェブサーバが不正アクセスを受け、スパムメール発信の踏み台となっていたことが分かった。ウェブサーバの初期設定に用いたログインアカウントを削除せずに放置していたところパスワードを解読され、不正に侵入されたことが原因だった。
③ 不正アクセスへの防護対策
社内で管理する情報資産が膨大となる一方で、攻撃手法が巧妙化していることから、全ての脅威に対して完璧な対策を講じることが困難となってきている。そこで、重要な情報資産に接する機会が多い幹部社員が利用する端末やシステムを集中的に監視することで、効率的にセキュリティ対策を行っている。
（参考：付録　サイバー攻撃に関する事例集②）

（2）重要インフラ分野における取り組み

- 重要インフラ分野の中には、ガイドライン等で不正アクセスへの対応について掲載し、公表しているケースもあり、以下の通り紹介する。

① 電気通信分野
電気通信分野における情報セキュリティ確保に係る安全基準　（P27）
望ましい対策として、利用者の識別・認証等によるアクセス制限を行うとともに、アクセス履歴を記録して定期的に監査を実施することや不正アクセスを検出する機能を導入することなどを紹介している。
② 政府・行政サービス分野
地方公共団体における情報セキュリティポリシーに関するガイドライン　（P76-77）
望ましい対策として、使用されていないポートの閉鎖などの対策や攻撃の予告があった場合に関連機関との連絡を密にして情報の収集に努めることなどを紹介している。

（3）被害に遭わないための対策

i）未然防止策

- 関連情報の収集

NISCからの情報提供やJPCERT/CCからの早期警戒情報及びIPAからの注意喚起、JVN等を活用する。不正アクセスに関する脆弱性情報は多数出されている。主な例は以下の通り。

2010/08/31　moobbs2におけるクロスサイトスクリプティングの脆弱性（JVN）
2010/08/03　Windowsシェルの脆弱性（MS10-046）について（JPCERT/CC）
2013/06/07　Webサイト改ざんに関する注意喚起（JPCERT/CC）
2014/09/25　GNU bash の脆弱性に関する注意喚起（JPCERT/CC）

- 注意喚起の収集

IPAからは、SQLインジェクションやDNSサーバの脆弱性、ウェブサイトの改ざん等に関する

注意喚起が出されている。
2008/05/15 SQL インジェクション攻撃に関する注意喚起
2008/12/19 DNS サーバの脆弱性に関する再度の注意喚起
2009/12/24 ウェブサイト改ざんに関する注意喚起

- Web サイト作成に関する情報の収集
  IPA ではコンピュータ不正アクセス被害対策集や安全な Web サイトの作り方等に関する情報提供を行なっている。
  （参考：安全なウェブサイトの作り方 pdf 版、安全な SQL の呼び出し方）

- パスワードの管理
  これまで、利用者が推測可能な弱いパスワードを設定していることや、他のシステムとパスワードを使いまわしていることによるパスワード漏洩などによって不正アクセスのインシデントが多く発生している。利用者への ID、パスワード作成する際の注意点を教育すること、またシステム側で弱いパスワードを選択できないような仕組みを導入するなどの対策が必要である。
  （参考：共通セキュリティ設定一覧 CCE 概説（パスワード編）（JVN iPedia））

ii）拡大防止策

- 攻撃痕跡の確認
  攻撃の痕跡を確認するためには、ログの保存や IDS（Intrusion Detection System）・IPS（Intrusion Prevention System）の活用が対策としてあげられる。日頃よりログの保存を行っておけば、不正アクセスが疑われる場合に確認を行うことができる。また、IDS を利用すると、通信回線を監視し、ネットワークを流れるパケットを分析した上で、不正なアクセスと思われるパケットを検出することが可能であり、IPS を利用すると、更にパケットを制御することも可能である。また、IPA ではウェブサイトを狙った攻撃の検出ツールの「iLogScanner」を公開している。
  （参考：「iLogScanner」の性能向上版を公開（IPA））
- 所管省庁への報告
  攻撃による被害が確認され、重要インフラサービスの提供に影響が出た場合には、各分野における業法等に基づいて、各所管省庁へ報告する。また、重要インフラ全体のサービス維持レベルの向上にヒヤリハット情報が役立つ場合があることから、被害のない場合についても所管省庁を通じて積極的に情報を共有していくことが望ましい。
- 被害の届出
  IPA では不正アクセスによる被害状況の届出を受け付けており、被害状況を把握するために分析・検討を行っている。その結果を踏まえ、被害状況や防止策を定期的に公表している。
  （参考：不正アクセスの届出について（IPA））
- 改ざんの有無の確認及び改ざんされた場合の対処方法（各社での対応）
  IPA では、ウェブサイト改ざんに関する注意喚起を公表しており、その中で改ざんの有無の確認方法及び改ざんされた場合の対処法を紹介している。
  ① 改ざんの有無の確認方法
  ウェブサイト上の全ページのソースを確認し、FTP へのアクセスログの確認も行う。
  ② 改ざんされた場合の対処方法
  ウェブサイトを一旦公開停止した上で、原因究明及び修正作業を行う。ID やパスワードを盗まれた場合はそれらを変更する。パソコンがスパイウェアに感染している可能性がある場合は、パソコンを不正なプログラムがないクリーンな状態に（初期化）してから ID やパス

ワードを変更する。 等

3 フィッシング詐欺

（1）フィッシング詐欺の概要

- フィッシングとは、金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為である。
（参考：フィッシング対策協議会 HP）
- 典型的な手口としては、銀行等からのお知らせのふりをしたメールを送りつけ、巧みにリンクをクリックさせて、本物そっくりの偽サイトに誘導した後、そこでクレジットカード番号や口座番号を入力させることで情報を盗み取る。

- フィッシング詐欺の過去の事例
① 三菱東京 UFJ 銀行のケース
三菱東京 UFJ 銀行を装い、インターネットバンキングの契約番号やログインパスワードを盗み取ろうとするフィッシングメールが発生した。そのため、自社のウェブサイトにおいて注意喚起を行った。同行については、2014 年にもフィッシングメールが出回り、偽サイトが作成されていた。
（参考：三菱東京 UFJ 銀行 HP、フィッシング対策協議会による事例紹介）
② Master Card のケース
「MasterCard Account Holder」などの件名でフィッシングサイトに誘導しようとするメールが発生。
（参考：Master Card HP、フィッシング対策協議会による事例紹介）
③ Yahoo!オークションのケース
2005 年に Yahoo!オークションを装い、偽サイトへ誘導して ID やパスワードを盗み取ろうとするフィッシングメール・サイトが発生。既にサイトは閉鎖されている。Yahoo! オークションでは、再発防止のためにフィッシング詐欺に関する注意喚起のページを作成。
（参考：Yahoo!オークション 安全対策研究所、フィッシング対策協議会による事例紹介）
④ ホスティングサーバを狙ったフィッシングに利用のケース
外部に運用委託しているデータセンタ内のホスティングサーバが米国の某銀行の Web サイトに対するフィッシングに利用されていた。
（参考：付録 サイバー攻撃に関する事例集③）

（2）関連機関における取り組み

- フィッシング詐欺に対して、以下の機関がそれぞれ取り組んでいる。
① フィッシング対策協議会
フィッシングの攻撃対象となりうる事業者又はその団体や、防御手段を提供しうる事業者などから構成されている。フィッシングに関する情報収集・提供、動向分析、技術面の検討などを行っている。フィッシング対策ガイドラインや月次報告書等の各種報告書を発行したり、JPCERT/CC と連携して、偽サイトの閉鎖も行ったりしている。
② 警察庁及び各都道府県警
フィッシング詐欺被害に遭った際の相談窓口として、各都道府県警がフィッシング 110 番を設置している。
（参考：警察庁 HP）

③ 金融庁

「主要行等向けの総合的な監督指針」（平成 26 年 7 月）の中で、フィッシング防止のためのサイト作りを求めている。

（3）被害を抑制するための対策

ⅰ）未然防止策

- フィッシングガイドラインの活用
  フィッシング対策協議会発行の「フィッシング対策ガイドライン」では、サービス事業者向けの対策と消費者向けの対策を必要性の観点で３段階に分けて紹介しており、具体的な対策として、「顧客に送信するメールには電子署名を付与すること」や「重要情報を入力するページは SSL/TLS で保護すること」等が挙げられており、これを参照し、自社の対策の充足度の確認や必要な対策を確認することができる。
- Web サイトの安全性の確保
  IPA 発行の「安全なウェブサイトの作り方」では、フィッシング詐欺を助長しないためにウェブサイト運営者が行なう対策がまとめられており、フィッシング詐欺によく使われるクロスサイトスクリプティング脆弱性を悪用についても触れられている。また、独立行政法人産業技術総合研究所発行の「安全な Web サイト利用の鉄則」では、フィッシング被害を防止する Web サイト利用手順の確認を目的として、サイト利用者及び管理者向けに必要な対策を紹介しているので、これらを活用して自社の Web サイトの安全性及び必要な対策の確認並びに利用者への注意喚起のために必要な事項を確認することができる。
- 産総研等と連携しての普及啓発
  重要インフラ事業者等が一般利用者向けにフィッシング対策をはじめインターネットの利用に伴い必要なセキュリティ対策について普及啓発を行う際には、産総研等の機関と連携して推進することが可能である。詳細については、独立行政法人産業技術総合研究所　情報セキュリティ研究センターに相談すると良い。
  （参考：インターネットにおけるセキュリティ強化に関する研究（産総研））

ⅱ）拡大防止策

- ISP・JPCERT/CC との連携によるサイトの閉鎖
  契約している ISP や JPCERT/CC に相談して、フィッシングサイトとして立ち上がっているサイトを素早く閉鎖させることで、被害を押さえる。
- 顧客等への通知・公表
  既に被害が発生している場合などにおいては、顧客等に対して、迅速な注意喚起を行うことが考えられる。その際には、公表することにより便乗詐欺等で被害を拡大させてしまうリスクなどもあるため、タイミングなどを検討することが望ましい。
  （参考：フィッシング対策ガイドライン P21）

4　迷惑メール

（1）迷惑メールの概要

- 迷惑メールは、特定電子メールの送信の適正化等に関する法律によると、特定電子メールの定義を、「電子メールの送信をする者が自己又は他人の営業につき広告又は宣伝を行うための手段として送信する電子メール」とされている。また、一般財団法人日本データ通信協会では、受け取る人の意思に関わらず、勝手に送りつけられてくるメールのことを総称して「迷惑メール」とし

ている。多くの迷惑メールは、送信者情報等を偽装したり、ボットネットを利用して送られたりしている。

（参考：特定電子メールの送信の適正化等に関する法律、一般財団法人日本データ通信協会 HP）

- 迷惑メールによるリスクとしては、主に以下の５つが考えられる。

① 通信リソースの枯渇

迷惑メールが大量に送付されることにより、帯域が消費されて、業務に関係したメールが届かなくなることが懸念される。

② 業務効率の低下

メールサーバが迷惑メールの処理に多くのリソースを割かれ、本来送受信すべきメールが滞ることによる業務効率の低下及びサーバメンテナンス等の作業に人員を充てることによる本来業務の効率低下が懸念される。

③ マルウェア感染（対策等は下記５を参照）

迷惑メールに悪意あるファイルが添付されていた場合には、それを開くことによって、マルウェアに感染する恐れがある。

④ フィッシングサイトへの誘導（対策等は上記３を参照）

フィッシング詐欺の手段の一つとして、迷惑メールの文中に URL を記載して、フィッシングサイトへ誘導するものがある。

⑤ 踏み台にされることによる風評被害

迷惑メール送信の踏み台にされることで、その企業に対する信用の失墜などの風評被害を受ける可能性がある。

- 迷惑メールの現状については、株式会社 IIJ によると、2013 年度の第 4 四半期に検出した迷惑メールの割合は、38.5%であった。前年同時期(2012 年度第 4 四半期)の 45.5%から 7%減少している。主な送信元としては、中国（19.1%）、日本（13.4%）、米国（7.4%）、ウクライナ、ロシア、ベラルーシと続いている。詳細については、以下を参照のこと。

（参考：Internet Infrastructure Review vol.23 メッセージングテクノロジー（株式会社 IIJ））

- 迷惑メールの対策を行う際の課題としては、フィルタリングなどの対策を行った際の判定精度、すなわち正しいメールを迷惑メールと誤判定、迷惑メールを正しいメールと誤判定すること、などが挙げられる。
- 迷惑メールの過去の事例

① 大量に送信された添付ファイル付き迷惑メールのケース

中国から大量のファイルが圧縮された数 10M の Zip ファイルが添付されたメールが、断続的に送信されたことで、メールシステムが麻痺してしまい、本社・支店の業務へ多大な影響を与えた。

（参考：付録　サイバー攻撃に関する事例集④）

（２）関連機関における取り組み

- 迷惑メールについて取り組んでいる機関の紹介

① 総務省

特定電子メール法を所管し、同法に違反した事業者に対して消費者庁と共同で、業務改善命令を下している。その他にも、迷惑メールに関するポータルサイトを運営し、情報提供を行っている。

② 迷惑メール相談センター

一般財団法人日本データ通信協会内に設置されている。迷惑メールに関する相談窓口や違反

情報の連絡窓口を置いており、提供された違反情報は総務省や消費者庁の措置に活用されている。

③ 迷惑メール対策委員会

一般財団法人日本インターネット協会内に設置されている。迷惑メールの問題に対して、技術的・社会的な取り組みによる包括的な解決策を検討している。有害情報対策ポータルサイト－迷惑メール対策編－で、メール管理者向けの対策情報等を公開している。

④ MAAWG

国際的な迷惑メールの増加を背景に、欧米の電気通信事業者や ISP により構成され、迷惑メールやウイルス等への対策を検討している。JEAG はこの MAAWG の設立を背景に創設された。

（3）重要インフラ分野における取り組み

- 重要インフラ分野の中には、ガイドライン等で迷惑メールへの対応について掲載し、公表しているケースもあり、以下の通り紹介する。

① 電気通信分野

電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（P19-22）

電気通信事業者が他の電気通信事業者からスパムメール送信の停止要請を受けた際の速やかな対応の実施、事業者間の緊密な連携、国内外のメール対策組織との連携やスパムメールに対するポリシーの一般公開等の望ましい対応が示されている。

② 政府・行政サービス分野

地方公共団体における情報セキュリティポリシーに関するガイドライン （P58-59）

電子メールのセキュリティ管理として、大量のスパムメールの送受信を検知した際のメールサーバの運用停止や電子メールの送受信容量の上限設定やメールボックスの容量の上限設定などを紹介している。

（4）被害（迷惑メールの受信）を減らすための対策

ｉ）未然防止策

- ISP の提供するサービスの活用

  ISP では、迷惑メール対策としてフィルタリング等のサービスを提供している。

- 送信ドメイン認証の導入

  送信ドメイン認証とは、「メールの送信元情報のうち、ドメイン名が送信元に対して正当であるかを確認する認証技術」である。フィルタリング等の他の対策と組み合わせることで迷惑メールを減少させることができる。ただし、送信側メールサーバと受信側メールサーバの双方での対応が必要である。

  （参考：迷惑メール相談センター　迷惑メール対策 HP）

- 受信者による最終的な判断

  上記のような対策で全ての迷惑メールが排除されるわけではないので、最終的には受信者側での判断によるフィルタリングが必要となる。利用者への啓発活動を実施することも考えられる。

- その他、各自で行うべき対応策

  PC や携帯電話の迷惑メール対策ついては、迷惑メール相談センターが紹介している。

  （参考：迷惑メール相談センター　迷惑メール対策 HP）

ii）拡大防止策

- IPA への届出
  迷惑メールのうち、「不審メール」（実在の企業名や官公庁名をかたって特定の組織や人に送られ、添付ファイルを開いたり URL をクリックしたりするとその組織の情報を盗むウイルスに感染する仕掛けをほどこされたメール）を受信した場合は、IPA の安心相談窓口に連絡する。
- その他、上記（１）で挙げた各リスクの拡大防止策については、WG メンバーへのアンケートによると、個別対応や事前に被害を受けた際の行動手順を策定するなどの各社内での対策が有効である。

（５）攻撃（迷惑メールの送信）を減らすための対策

- Outbound Port25 Blocking（OP25B）の導入
  OP25B とは、「迷惑メール送信に使われる動的 IP アドレスからのメール送信（受信メールサーバの port25 への直接接続）を一律に規制」するものである。
  （参考：迷惑メール相談センター　迷惑メール対策 HP）
- 送信ドメイン認証の導入
  上記（４）参照
- 送信トラフィック制御の導入
  迷惑メールを送る攻撃者は、一般的に大量のメールを送りつけるため、同一アカウントからの送信量を制御することで被害の拡大を防ぐ。主に、①一日に送信できるメールの総数を制限するもの、②一定期間内に送信できるメールの総数を制限するものがある。
  （参考：迷惑メール相談センター　迷惑メール対策 HP）
- ボットの駆除
  迷惑メールの発信がボットによるものだった場合には、当該ボットを削除する。具体的な対応策については、下記５を参照のこと。

５　ウイルス・ボット

（１）ウイルス・ボットの概要

- ウイルスは、コンピュータウイルス対策基準によると、以下のように定義されている。
  「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能の一つ以上有するもの。(1)自己伝染機能 (2)潜伏機能 (3)発病機能」
  各機能等の詳細については、以下を参照のこと。
  （参考：コンピュータウイルス対策基準（経済産業省平成７年告示第 429 号））
- ボットとは、コンピュータを悪用することを目的として作られた悪性プログラムで、コンピュータに感染すると、インターネットを通じて悪意を持った攻撃者が、外部から遠隔操作をする。また、感染したコンピュータは外部の指令サーバなどに接続され、多くの感染コンピュータを従えた大規模な「ボットネットワーク」を構成する。（参考：IPA HP「ボット対策について」）
- ウイルスやボットに感染したコンピュータは、攻撃者の意図した通りに、以下のような被害・攻撃を引き起こす。（参考：IPA HP「ボット対策について」）
  ① 迷惑メールの送信
  感染コンピュータを踏み台にして、迷惑メールの中継送信を行う。一台あたりの送信量は少量であっても、ボットネットワークを利用することで大量の迷惑メールを送ることが可能。
  ② DoS 攻撃
  特定の Web サーバの大量のパケットを送信し、そのサーバを利用不能することでサービス

妨害攻撃（DoS 攻撃）を行う。迷惑メール同様、一台あたりのパケットは少量であっても、ボットネットワークを利用することで大量の攻撃データを送ることが可能。2009 年 7 月に米韓で起きた DDoS 攻撃はボットネットワークを利用したものとみられている。
（参考：2010 年版 10 大脅威　P21）

③ ボット感染活動
ボット感染を拡大させるために、他のコンピュータの脆弱性を狙った感染拡大活動を行う。

④ 個人情報漏えい
ボットやウイルスはキーボードの操作履歴やコンピュータに保存されている情報を外部に送信する機能も有するため、クレジット番号やパスワードが流出することがある。

- ウイルス・ボットの感染経路
総務省の国民のための情報セキュリティサイトや IPA の HP では、ウイルスの感染経路がまとめられている。
① ウイルスの埋め込まれたホームページの閲覧による感染
② 電子メールの添付ファイルや HTML スクリプトの実行による感染
③ USB メモリからの感染（プログラムの自動実行）
④ ファイル共有ソフトやネットワークのファイル共有による感染
⑤ 偽のウイルス対策ソフトによる感染
⑥ マクロプログラムの実行による感染
- ウイルス・ボットの過去の事例
① インスタントメッセンジャーを偽装したマルウェア感染等のケース
インスタントメッセンジャーのクローン（※）を偽装したマルウェアが、インストールされている端末やアクセス可能なネットワーク内の機密情報やパスワード情報等を収集し、不正アクセスに悪用される可能性がある。
※「ICQ」や「Yahoo!メッセンジャー」等の有力インスタントメッセンジャーのアカウントで利用できるインスタントメッセンジャーのこと（「Regnessem」「Pidgin」等）。複数のサービスを同時に利用できる等、機能面で差別化を図っており、有力インスタントメッセンジャーの使い勝手に不満を持つユーザが利用する場合がある。
（参考：付録　サイバー攻撃に関する事例集⑤）

（２）関連機関による取り組み

- ACTIVE
ACTIVE では、HoneyPot を活用したボットの収集及び解析を行うとともに、ボットに感染していると思われるユーザに対して、ISP 等の協力を得て、注意喚起を行い、ユーザによるボットの駆除を実施している。
- IPA のウイルスレポート
IPA では、ウイルスに感染した際の被害状況や発見経路等の情報の届出を受け付けている。届出られた情報は、感染被害の拡大防止や再発防止に役立てられ、統計情報として定期的に公表も行っており、感染手口やその対策を紹介している。
（参考：コンピュータウイルス届出状況について（IPA））
- アンチウイルスベンダのレポート
アンチウイルスベンダ各社では、ウイルスを中心としたセキュリティレポートを定期的に発行し、ウイルスの特徴やその対策方法などを紹介している。主なものとして以下の４つを紹介するが、その他のベンダにおいても同様のレポートを発行しているケースがある。

① Kaspersky ホワイトペーパー（株式会社 Kaspersky Labs Japan）
② Mc Afee のセキュリティ研究レポート（マカフィー株式会社）
③ Symantec インターネットセキュリティ脅威レポート（株式会社シマンテック）
④ Trendmicro セキュリティレポート（トレンドマイクロ株式会社）

（3）重要インフラ分野における取り組み

- 重要インフラ分野の中には、ガイドライン等でウイルス・ボットへの対応について掲載し、公表しているケースもあり、以下の通り紹介する。

① 政府・行政サービス分野

地方公共団体における情報セキュリティポリシーに関するガイドライン （P73-75）

不正プログラム対策として、外部から受信したファイルのウイルスチェック、コンピュータウイルスに関する情報収集及び職員への注意喚起、ウイルス対策ソフトを常に最新版に保つことなどが望ましいとしている。

（4）被害に遭わないための対策

ⅰ）未然防止策

- JVN/JVN iPedia や MyJVN バージョンチェッカの利用

JVN iPedia は、国内で利用されている製品の脆弱性対策情報を網羅的に蓄積しており、日頃からの情報収集ができる。また、MyJVN バージョンチェッカでは、利用者の PC にインストールされているソフトウェアのバージョンが最新であるかどうかを確認できる。

（参考：JVN iPedia（IPA）、MyJVN バージョンチェッカ（IPA））

- ウイルス情報 iPedia 活用

IPA に届出られたウイルスやボットに関する情報（動作内容・対処法等の解析結果）が蓄積されており、感染の予防や対策に活用できる。

（参考：ウイルス情報 iPedia）

- ACTIVE の利用

攻撃者からのボットを通じた遠隔操作を防ぐ観点から、自社システム（各端末含む）がボットに感染しているかを確認し、感染していた際には駆除ツールをダウンロードして駆除できる。また、ボット感染が疑われる場合に、ACTIVE から注意喚起を受けることもあるので、その際は注意喚起に従い、ボットを素早く駆除する。

- マルウェア等の発信源となるウェブサイトの把握（TIPS の活用）

IPA では、利用者から送られてきた URL について、悪意のあるウェブサイトかどうか調査し、結果を回答するサービスを提供している。

（参考：TIPS、IPA 連絡窓口）

- インターネットからの隔離

システム稼働等の都合によりパッチの当てられない端末については、外部からの攻撃を防ぐため及び他の端末への感染を防ぐために、極力インターネット回線から隔離する。

- その他、ウイルス対策ソフトや OS などのアップデート、メールに添付されたファイル等のウイルスチェックについては、以下の HP 等で対応が紹介されている。

（参考：2010 年版 10 大脅威(IPA)、参考：パソコンユーザのためのウイルス対策 7 箇条(IPA)）

ⅱ）拡大防止策

① マルウェアの解析依頼
JPCERT/CC においては、利用者から提供されたマルウェアの種類を特定し、解析結果を回答するサービスを行っている。

- マルウェア感染の届出
IPA においては、感染被害の拡大防止及び再発防止のために、マルウェア感染の届出窓口を設けている。また、IPA では届出件数等は定期的に公表されている。
- 所管省庁への報告
ウイルス・ボット感染による被害が確認され、重要インフラサービスの提供に影響が出た場合には、各分野における業法等に基づいて、各所管省庁へ報告する。また、重要インフラ全体のサービス維持レベルの向上にヒヤリハット情報が役立つ場合があることから、被害のない場合についても所管省庁を通じて積極的に情報を共有していくことが望ましい。

6 標的型攻撃

（1）標的型攻撃の概要

- 標的型攻撃は、いくつかの攻撃手法を組み合わせ、明確な攻撃意図と確実に攻略に至るための戦略的な攻撃シナリオに沿って、遂行される。攻撃シナリオは、メールやウェブ経由でシステム内部に侵入した後、段階的にシステム攻略範囲を拡大していき、情報の窃取・破壊等に至る。
（参考：攻撃者に狙われる設計・運用上の弱点についてのレポート ～標的型攻撃におけるシステム運用・設計 10 の落とし穴とその対策～ P3）
- 標的型攻撃では、初期の潜入、バックドア開設までは、脆弱性の悪用やマルウェアによる攻撃が行われる。
- 標的型攻撃の過去の事例
① 標的型攻撃メール
国立感染症研究所からの豚インフルエンザに関する注意喚起メールに見せかけた、ウイルス添付メールが送信された。
（参考：付録 サイバー攻撃に関する事例集⑥）
② 標的型攻撃メール
海外出張時に日本の携帯電話をローミングにて使用したところ、帰国後にローミング先の現地通信事業者からメールが届き、それには請求書を偽証したウイルス付きのファイルが添付されていた。
（参考：付録 サイバー攻撃に関する事例集⑦）

（2）関連機関による取り組み

- 標的型サイバー攻撃の特別相談窓口
IPA では、標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する「標的型サイバー攻撃の特別相談窓口」を設置し、相談を受け付けている。

（3）被害に遭わないための対策

ｉ）未然防止策

- 標的型攻撃の対策として、ウイルス・ボットの項で記載したエンドポイント対策や入口対策等は、適切な対策ではある。（但し、正確に言うと「標的型攻撃の一部」への対策である。）
（参考：攻撃者に狙われる設計・運用上の弱点についてのレポート ～標的型攻撃におけるシステム運用・設計 10 の落とし穴とその対策～ P2）

- 標的型攻撃は、ソフトウェアの脆弱性や設計・運用上の弱点を狙い、戦術的にシステム攻略が行われる。対策に当たっては、攻撃者に「手ごわい」「攻略しづらい」と思わせるシステム設計が必要になってくる。
  （参考：攻撃者に狙われる設計・運用上の弱点についてのレポート ～標的型攻撃におけるシステム運用・設計10の落とし穴とその対策～ P23）

ii）拡大防止策

- 標的型攻撃の届出
  IPAにおいては、標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する「標的型サイバー攻撃の特別相談窓口」を設置し、相談を受け付けている。
- 所管省庁への報告
  ウイルス・ボット感染による被害が確認され、重要インフラサービスの提供に影響が出た場合には、各分野における業法等に基づいて、各所管省庁へ報告する。また、重要インフラ全体のサービス維持レベルの向上にヒヤリハット情報が役立つ場合があることから、被害のない場合についても所管省庁を通じて積極的に情報を共有していくことが望ましい。

Ⅳ. Who's who

- 重要インフラ事業者等がサイバー攻撃に対応するに当たっては、以下の関係主体と連携することが必要になる可能性がある。具体的な連携イメージについては、「Ⅲ. 各脅威への対応」の中で紹介している対応策を参照のこと。

内閣サイバーセキュリティセンター（NISC）重要インフラグループ	官民の情報共有体制を整備し、ＩＴ障害の未然防止、拡大防止・復旧、再発防止に関する情報提供・情報連絡を進めているほか、隔週で重要インフラニュースレターを発行している。（参考：重要インフラの情報セキュリティ対策に係る第３次行動計画 P31）	内閣サイバーセキュリティセンター http://www.nisc.go.jp/ 03-5253-2111(代表 TEL) 03-3581-3820(直通 TEL)
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省、国土交通省が、各所管の重要インフラ分野の業法等に基づき、重要インフラ事業者等からサービス障害に関する報告を受けている。 各分野の業法及びガイドラインの一覧については、最後に付録として記載している。 また、重要インフラ事業者等の自主的な情報セキュリティ対策を推進している。総務省、経済産業省では、情報セキュリティ対策に関するポータルサイトを開設している。	総務省：国民のための情報セキュリティサイト、情報セキュリティホームページ 経済産業省：情報セキュリティ政策ポータル 金融庁：03-3506-6000(代表 TEL) 総務省：03-5253-5111(代表 TEL) 厚生労働省：03-5253-2111(代表 TEL) 経済産業省：03-3501-1511(代表 TEL) 国土交通省：03-5253-8111(代表 TEL)
独立行政法人情報処理推進機構（IPA）セキュリティセンター	わが国において情報セキュリティ対策を向上するため、緊急対策情報や注意喚起の提供、コンピュータウイルス等による被害の届出・相談、脆弱性関連情報の届出、情報セキュリティ対策の提供、脆弱性対策情報の提供（脆弱性対策情報データベース JVN iPedia、及び JPCERT/CC と共同してポータルサイト JVN を運営）、情報セキュリティに関する認証、セミナーの開催等を行なっている。	IPA セキュリティセンター http://www.ipa.go.jp/security/ 情報セキュリティ安心相談窓口 TEL:03-5978-7509（平日 10:00-12:00、13:30-17:00） FAX:03-5978-7518 anshin@ipa.go.jp 標的型サイバー攻撃特別相談窓口 TEL:03-5978-750（平日 10:00-12:00、13:30-17:00） FAX:03-5978-7518 anshin@ipa.go.jp
JPCERT コーディネーションセンター	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、注意喚起や早期警戒情報、脆弱性対策情報の提供、日本国内のサイトに関する報告の受け付けを行なう。また、インシデントによる被害（インシデントに至らなくても不審な場合を含む）を受けている組織には、国内外の攻撃元に対する調整等の対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言など	JPCERT/CC http://www.jpcert.or.jp/ TEL：03-3518-4600 FAX：03-3518-4602 インシデント時の連絡先： http://www.jpcert.or.jp/form/ info@jpcert.or.jp

	を、技術的な立場から行なう。(参考：インシデント報告のガイドライン(JPCERT/CC 発行))	
独立行政法人情報通信研究機構（NICT）情報セキュリティ研究センター	インターネット上のサイバー攻撃や不正アクセス等のインシデント対策、サイバー攻撃の発信元の特定や攻撃の推移を解明するトレースバック技術や、情報・プライバシー保護のための暗号・認証技術等の研究開発を行うとともに、災害による被害の防止や軽減に貢献できる ICT の研究開発を実施している。	NICT 情報セキュリティ研究センター http://www2.nict.go.jp/y/y201/src-web/ TEL：042-327-7429(代表 TEL)
産業技術総合研究所（AIST）情報セキュリティ研究センター	世界的な研究成果を継続的に出すことのできる「日本のセキュリティ研究のコア」を目指し、暗号・セキュリティ基盤技術分野、ハードウェア・量子情報セキュリティ分野、ソフトウェア分野の幅広い視点から総合的なセキュリティ技術の研究開発を行う。	AIST 情報セキュリティ研究センター http://www.rcis.aist.go.jp/ TEL：03-5298-4722
フィッシング対策協議会	海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の 抑制を目的として活動している。	フィッシング対策協議会事務局 http://www.antiphishing.jp/ Email：info@antiphishing.jp
迷惑メール相談センター	迷惑メールに関する電話相談、違反メールの情報提供受付、迷惑メールの解決策の紹介、チェーンメールの実態と対処法の紹介などを行うとともに、迷惑メール対策推進協議会の事務局を務め、迷惑メール対策ハンドブックなどを刊行している。	一般財団法人日本データ通信協会 迷惑メール相談センター http://www.dekyo.or.jp/soudan/
迷惑メール対策委員会	迷惑メールを取り巻く基本知識の理解を深めてもらうためのセミナーや迷惑メールについての技術知識や法的要件への理解を深めるためのカンファレンスを開催するほか、迷惑メールに関する有害情報をポータルサイトで紹介している。	一般財団法人インターネット協会 迷惑メール対策委員会 http://www.iajapan.org/anti_spam/
ACTIVE	総務省と複数のインターネット・サービス・プロバイダ（ISP）事業者やセキュリティベンダー等の事業者とが連携し、国内のインターネット利用者を対象に、マルウェアの感染防止と駆除の取組を行う官民連携プロジェクト。	ACTIVE https://www.active.go.jp/ お問い合わせフォーム https://www.active.go.jp/contact/index.html

- その他にも、自らの業界の他社や情報通信分野等の他の業界のサイバー攻撃に関する以下のような公開情報等について、各社においては予め確認しておく。
  ①大規模インシデントの検知
  ②大局的な情報把握
  ③網側での一時的な対策
  ④ISP 連携による対策

Ⅴ．本手引きの維持管理

１．本手引きの維持管理に係る所管

本手引きの原本の保管及び管理はセプターカウンシル事務局が所管する。

２．本手引きの改訂

サイバー攻撃手法は時間の経過に伴い高度かつ巧妙化する傾向にあり、本手引きは適宜改訂する必要がある。本手引きの改訂については、セプターカウンシル幹事会が所管し、必要が認められる場合はＷＧを主催し、改訂を行う。

３．本手引きに関する意見及び要望等について

本手引きの利用に際し、意見及び要望等がある場合は、各セプターの幹事を通じてセプターカウンシル幹事会へ上げることとし、幹事会にて対応を検討する。

４．本手引きのとりまとめに際しての課題と取扱い

本手引きのとりまとめに際し、セプターカウンシル等において検討が必要と考えられる課題についてとりまとめた（以下を参照。）。各課題については、セプターカウンシル幹事会へ申し送ることとし、取り組みが必要と判断した場合は、新たにＷＧを起こし検討する。本課題に関連し意見及び要望等がある場合は、各セプター幹事を通じてセプターカウンシル幹事会へ上げることとし、セプターカウンシル幹事会にて対応を検討する。

- サイバー攻撃に関する早期の情報共有
- 早期発見と定期的な演習訓練
- ゼロデイ攻撃等への対処の整理
- 脆弱性対策の推進

Ⅵ. WGの活動履歴

WG番号	WG002
WG名	サイバー攻撃対応力向上WG
構成メンバー	●登録メンバー（17名） T-CEPTOAR　4名 放送における情報共有体制　1名 銀行等 CEPTOAR　3名 証券 CEPTOAR　4名（世話役含む、1名中途退会） 生命保険 CEPTOAR　1名（中途退会） 損害保険 CEPTOAR　1名 電力 CEPTOAR　1名 GAS CEPTOAR　2名
活動状況	●第1回会合（2009年6月23日）　10：00～12：00 ・有識者による講演と意見交換 テーマ：「セキュリティインシデントの動向とその対策」 奈良先端科学技術大学院大学　山口　英　氏 参加者：メンバー16名 ■ 様々なセキュリティインシデントの動向及び対策について、認識を深めた。 ●第2回会合（2009年8月19日）　16：00～18：00 ・有識者による講演と意見交換 テーマ：「IPAセキュリティセンターの活動と重要インフラ事業者として知っておくべき脅威と対応」 独立行政法人情報処理支援機構　小林　偉昭　氏 テーマ：「ボット/ワームによるDDoS攻撃、通秘侵害せず対処する方法とステークホルダー横断連携に関する考察」 Telecom-ISAC Japan　有村　浩一　氏 参加者：メンバー16名 ■ IPAの活動や重要インフラ事業者として理解すべき脅威及びその対応について認識を深めた。 ●第3回会合（2009年10月14日）　16:00～18:00 ・有識者による講演と意見交換 テーマ：「ボット/ワームによるDDoS攻撃、通秘侵害せず対処する方法とステークホルダー横断連携に関する考察」 Telecom-ISAC Japan　有村　浩一　氏 参加者：メンバー16名 ■DDoS攻撃の紹介やその対処について、特に通信の秘密との関係において、ISPとサービス利用者との関係で、対応出来ること/出来ないことについて、認識を深めた。 ●個別ヒアリング（2009年11月5日～24日）

	■世話役及び事務局が、WGメンバーを個別に訪問し、「重視すべき脅威」や「ステークホルダーとの連携」について、ヒアリングを行い、結果をとりまとめ。とりまとめ結果については、第4回会合にて資料として配布。(「重視すべき脅威」の整理結果については、枠外の表を参照のこと。) ●第4回会合(12月9日)　16:00～18:00 ・有識者による講演と意見交換 テーマ:「情報セキュリティインシデントへの対応とJPCERT/CCの活動」 一般社団法人JPCERTコーディネーションセンター　早貸　淳子氏 参加者:メンバー12名 ■JPCERT/CCの活動やJPCERT/CCとの連携のポイントについて認識を深めた。 ■重視すべき脅威の分類やステークホルダーとの関係及び今後のWGの進め方について議論を行い、方向性を確認した。 ●第5回会合(2010年3月10日)　14:00～16:00 ・有識者による講演と意見交換 テーマ:「Webのセキュリティ」 独立行政法人産業技術総合研究所　高木　浩光　氏 テーマ:「フィッシング対策協議会の活動と重要インフラ事業者との連携のポイント」 フィッシング対策協議会事務局　小宮山　功一朗　氏 参加者:メンバー15名、陪席1名 ■Web(携帯電話を含む)を介した商取引におけるセキュリティ上の問題とその対応策について認識を深めた。 ■フィッシング対策協議会の活動、フィッシング対策ガイドラインの概要及びフィッシング対策協会との連携のポイントについて認識を深めた。 ●第6回会合(2010年6月17日)　16:00～18:00 ・有識者による講演と意見交換 テーマ:「迷惑メールの最近の傾向と対策」 株式会社インターネットイニシアティブ　櫻庭　秀次　氏 参加者:メンバー14名 ■迷惑メールの現状、対策とその懸案及びJEAGが推奨している「送信ドメイン認証技術」について認識を深めた。 ・WGの進め方に関する議論 WGの今後の進め方について、メンバー間で意見交換を行い、これまでの取り組みを一旦まとめた上で、今後のWG継続について判断することとした。 ●第7回会合(2010年8月24日)　16:00～18:00 ・有識者による講演と意見交換 テーマ:「最近のサイバー攻撃事例動向と対策」 株式会社ラック　西本　逸郎　氏 参加者:メンバー14名

■最新の攻撃事例として、クラウドやスマートフォンを使用した攻撃について認識を深めた。また、サイバー攻撃を受けた際の対応や想定しておくことについても認識を深めた。

・成果とりまとめに関する議論

■DDoS 攻撃への対応策のとりまとめについて確認を行い、他の攻撃への対応策についても同様にとりまとめていくこととした。

●第 8 回会合（2010 年 11 月 16 日） 16:00～18:00

・有識者による講演と意見交換

テーマ：「重要インフラにおけるインシデント再考」

S&J コンサルティング株式会社 三輪 信雄 氏

参加者：メンバー14 名

■過去に行われたセキュリティ実験についてご紹介頂くとともに、フィッシングメールや DDoS 攻撃といったサイバー攻撃への対策に対する考え方について認識を深めた。

・成果とりまとめに関する議論

■「サイバー攻撃対応力向上の手引き」のとりまとめについて確認を行い、本 WG の成果とした。

■とりまとめの際に課題として上がった「サイバー攻撃に関する早期の情報共有」について、WG 活動期間を年度末まで延長して引き続き検討を行うこととした。

●第 9 回会合（2011 年 2 月 23 日） 14:00～16:00

・サイバー攻撃対応に関する情報共有に関する議論

■2010 年 12 月～2011 年 1 月にかけて実施したアンケート・ヒアリング結果を基に、「セプターカウンシルにおいて共有すべき情報の要件」や「今後の共有体制の方向性」について確認を行った。

・自由討論

■最近のサイバー攻撃事案を踏まえた情報共有の在り方等についてメンバー間で自由討論を行い、相互理解・共通認識の醸成を行った。

●第 10 回会合（2011 年 4 月 26 日） 16:00-18:00

・有識者による講演と意見交換

テーマ：「CYBEX の動向と実務への適用」

奈良先端科学技術大学院大学／情報通信研究機構 門林 雄基 氏

参加者：メンバー13 名

■セプターカウンシルにおける情報共有活動の参考とするため、情報セキュリティ情報交換技法（CYBEX）の動向と適用について認識を深めた。

・手引きの改訂について

■「サイバー攻撃対応力向上の手引き」の付録として本 WG で作成した「サイバー攻撃に関する事例集」を追加することについてメンバーの了承を得た。

・自由討論

■情報セキュリティに関する情報共有の在り方をテーマにメンバー間で自由討論を行い、相互理解・共通認識の醸成を行った。

参考

- 本WGでは、検討の対象として「重視する脅威」を選定するにあたり、WG参加メンバーへのアンケートやヒアリングを実施した。
- その結果、以下の６つの攻撃手法が重要インフラ事業者として「重視する脅威」として挙げられた。その影響度合いについては各セプターによって異なる（下表の通り、タイプが分かれた）が、複数のセプターで共通する脅威を本WGでは検討の対象として取り上げた。
- 「制御系システムへの脅威」については、特定のセプターに限られるため、本 WG では取り上げていない。

	タイプ１	タイプ２	タイプ３	タイプ４	タイプ５
DDoS 攻撃	◎	◎	○	○	○
不正アクセス	◎	○	○	○	○
フィッシング詐欺	◎	○	○	○	－
迷惑メール	○	○	○	○	－
ウイルス・ボット	○	○	○	○	○
制御系システムへの脅威	－	－	－	◎	◎

【凡例】◎：第２次行動計画にて定義されている重要インフラサービス（国民生活や社会経済活動に関わるサービス）に影響を与えるおそれがある脅威（銀行、証券は、ネットチャネルに限定した影響）
○：役務の提供に直接的な影響はないが、営業上又は組織運営上、支障を来たす脅威（信用の失墜等を含む）
－：脅威とは認識していない

※脅威の規模や各事業者のシステムなどの条件によって、影響は異なる場合も考えられる。

【付録１】各重要インフラ分野における安全基準等

各分野における安全基準等については以下の通り。

●情報通信分野

（電気通信）

・電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等
・情報通信ネットワーク安全・信頼性基準
・電気通信分野における情報セキュリティ確保に係る安全基準

（放送）

・放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン

●金融分野

・金融機関等におけるセキュリティポリシー策定のための手引書
・金融機関等コンピュータシステムの安全対策基準・解説書
・金融機関等におけるコンティンジェンシープラン策定のための手引書

●航空分野

（航空運送）

・航空運送事業者における情報セキュリティ確保に係る安全ガイドライン

（航空管制）

・航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン

●鉄道分野

・鉄道分野における情報セキュリティ確保に係る安全ガイドライン

●電力分野

・電力制御システム等における技術的水準・運用基準に関するガイドライン

●ガス分野

・製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン

●政府・行政分野

・地方公共団体における情報セキュリティポリシーに関するガイドライン

●医療分野

・医療情報システムの安全管理に関するガイドライン

●水道分野

・水道分野における情報セキュリティガイドライン

●物流分野

・物流分野における情報セキュリティ確保に係るガイドライン

【付録２】サイバー攻撃に関する事例集

本 WG において収集したサイバー攻撃に関する事例は以下の通り。

No	項目	攻撃種別	該当頁
①	クラウドサービス等を活用したサイバー攻撃に関する脅威	DDoS 攻撃（迷惑メール）	P27
②	不正アクセスへの防護対策	不正アクセス（標的型）	P28
③	ホスティングサーバを狙ったフィッシングに利用のケース	フィッシング詐欺	P29
④	大量に送信された添付ファイル付き迷惑メールのケース	迷惑メール	P30
⑤	インスタントメッセンジャーを偽装したマルウェア感染等のケース	ウイルス・ボット	P31
⑥	標的型攻撃（メール）の予兆情報	標的型攻撃	P32
⑦	標的型攻撃（メール）の事例	標的型攻撃	P エラー! ブックマークが定義されていません。
⑧	制御系システムへの Stuxnet の脅威	制御系への攻撃	P32
⑨	組織内 CSIRT の活動状況	全般	P33
⑩	大規模なサイバー攻撃に備えた全社的な事前訓練より得られた教訓	全般	P37
⑪	クレジットカード業界におけるデータセキュリティ基準である PCI DSS	全般	P38
⑫	ウイルス被害による被害額算出モデルの例	全般	P39
⑬	サイバー攻撃に影響の考えられる各国のソーシャルイベント情報	全般	P40

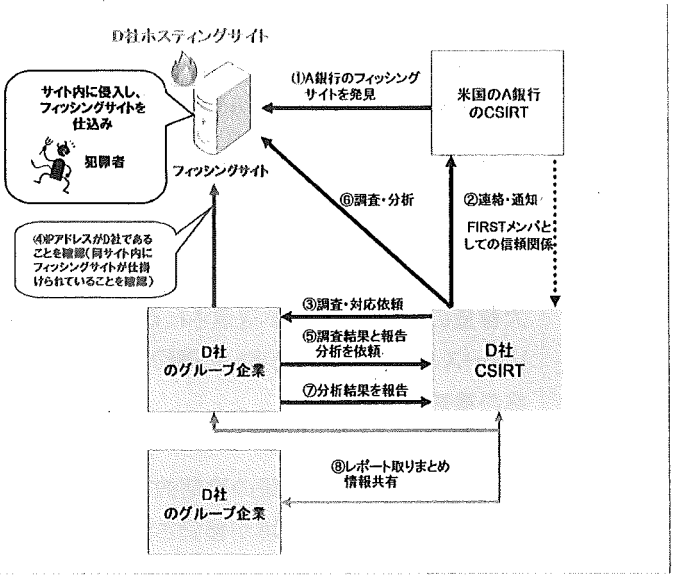
【付録2】事例① クラウドサービス等を活用したサイバー攻撃に関する脅威

項目	内容
攻撃手法	DDoS 攻撃(迷惑メール)
影響を受けるシステム	(1)DDoS 攻撃の対象となりうるサーバを有するシステム (2)メールシステム
IT 障害の概要	最近の傾向として、クラウドサービスをはじめとした XaaS 市場が拡大しており、攻撃元が潤沢な NW リソースを保有せずとも、大規模なボット攻撃や迷惑メールを送るためのサーバ等の環境確保が容易となっている。 (1)Amazon Web Service 等を活用した DDoS 攻撃 不正に取得したクレジットカードで Amazon Web Service 等のクラウドサービスの料金支払いを決済し、ボット攻撃や迷惑メール攻撃を展開する事象が発生している模様。 不正取得したクレジットカードの利用金額上限までサーバホスティング等のサービスを利用し、C&C(Comand&Control)サーバからボット端末への指令により DDoS 攻撃を展開するなど、各種サイバー攻撃を実施しているケースがある。 (2)メール代行配信サービスを活用した迷惑メール攻撃 ネットに接続された古い PC さえ用意できれば、リクルートや日経 BP などメール代行配信サービスを経由して大規模な迷惑メール攻撃の展開が可能。 攻撃の発信元(攻撃に利用する配信サービス)が移転していくことが多いため、対応が困難となる可能性がある。
想定される影響	(1)大量のアクセスによる通信リソースの欠乏、左記に伴うサービスの機能不全 (2)迷惑メールによるメールシステムの機能不全
対策方法	(1)クラウドサービス提供事業者からの異常な通信状況の監視 (2)広告メールを含めた、通常のメール受発信状況に基づく、予兆の早期検出 ※両者とも、事象が確認できた場合は IDS の設定変更や、通信遮断等の対策を実施。
備考	(関連 URL)Amazon Web Service を利用した攻撃 http://jvnrss.ise.chuou.ac.jp/csn/index.cgi?p=Amazon+Web+Service%A4%F2%CD%F8%CD%D1%A4%B7%A4%BF%B9%B6%B7%E2

【付録2】事例② 不正アクセスへの防護対策

項目	内容
攻撃手法	不正アクセス（標的型）
対策を実施したサービス等	機密情報を扱う会社幹部が利用する端末およびシステム
対策の概要	【目的】 社内で管理する情報資産が膨大となる一方で、攻撃手法が巧妙化していることから、全ての脅威に対して完璧な対策を講じることが困難となってきている。そこで、重要な情報資産を多く有する幹部社員が利用する端末やシステムを集中的に監視することで、効率的にセキュリティ対策を行う。 【主な対策】 ・通常 −会社幹部や企業買収を行うポストにいる社員、およびその関連社員が利用する端末やシステムの通信経路を限定化 −上記社員が利用する端末やシステムおよび通信経路を集中的に監視 ・マルウェア感染や不正アクセスが疑われる場合 −過去の通信履歴の調査等によるアクセス元の特定 −該当端末の OS のフォーマット
対策の効果	ターゲットを絞って集中的に監視を行っているため、効率的・効果的にリスク対応ができている。 −過去にもUSB メモリを経由したマルウェア感染事象が発生したが、本対策を実施していたことにより、早期発見に成功し、実質的な被害を回避した。
得られた教訓・課題	・重要な情報資産が扱われる箇所を限定することは、管理上有効である。 ・情報資産を個々に評価しなくても、利用者の属性に基づき監視対象を絞り込むことは、管理上有効である。 ・監視対象を特定の端末やシステムの通信経路に限定することで、検知の精度を向上させつつ稼働の削減が可能となる。
備考	

【付録2】事例③ ホスティングサーバを狙ったフィッシングに利用のケース

項目	内容
攻撃手法	フィッシング詐欺
IT 障害の発生場所	外部に運用委託しているデータセンタ内のホスティングサーバ
IT 障害が発生したサービス	ホスティングサーバを利用して運用している Web サーバ
IT 障害の概要	【概要】 ・ホスティングサービスを利用して運用している Web サーバが、米国の某銀行の Web サイトに対するフィッシングに利用された。 【経緯】 ・D 社の IP アドレスにフィッシングサイトが作られていると、CSIRT の国際フォーラムである FIRST で関係のある海外の CSIRT より D 社の CSIRT に連絡があった。当該会社に連絡・確認したところ、同サイト内にフィッシングサイトが仕掛けられていることを確認し、直ちに対策を実施。調査の結果、自社に対する被害はなかった（某銀行の被害状況は不明）。 【原因と再発防止策】 ・今回の事例は、ホスティングサービスで利用していた Web サーバの対応していない脆弱性をつかれたことが原因であった。 ・このような脆弱性は、技術的に見つけること自体は難しくないが、サーバを運用委託する際に見逃してしまいがちであり、チェック体制の盲点をついた手法である。 ・今回は海外 CSIRT と FIRST との連携によって大きな被害に発展する前に発見されたが、今後、同様の攻撃が発生する可能性があると考え、本事例およびサーバ等を外部に運用委託する際の注意事項をレポートとしてとりまとめ、情報の横展開を実施した。 【フィッシング攻撃とその対応イメージ】 
他の事業者への波及の可能性	・同様のサービスを対象とした攻撃の可能性あり
IT 障害の復旧状況	完全復旧
再発防止策	・運用委託時のチェック体制の見直し ・レポートとしてとりまとめ、各グループ企業への情報共有の実施

【付録2】事例④ 大量に送信された添付ファイル付き迷惑メールのケース

項目	内容
攻撃手法	迷惑メール
IT 障害が発生したサービス	社内メールシステム
IT 障害の概要	A 社ネットワークのゲートウェイ手前にスパムフィルタが実装されたアプライアンスサーバを設置。全てのメールおよび添付されたファイルをチェックした上で、ゲートウェイに転送される仕組みとなっていた。数年前に購入したものを利用しているため、通信リソースが不足気味であった。
提供サービスへの影響	メールの遅延・消失・不達 結果的に、業務中断等が生じた(特に、ML や企業のお問い合わせメール(info@～)の送信対象となっていたものは対応稼働が増加)。
発生した現象	大量のファイルが圧縮された数 10M の Zip ファイルが添付されたメールが断続的に送信された。
IT 障害の原因	メール遅延等の原因は、ゲートウェイの手前に設置されているスパムフィルタを実行するアプライアンスサーバのキャパシティを超える大量の添付ファイル付きメールが A 社ドメインの多くのメールアドレスに着信したことにより、メールシステムのリソースが逼迫したことと思われる。 ボトルネックとなったアプライアンスサーバは、導入当初は百万円を超える高価なサーバであったものの、当時は回線容量の広帯域化が進んでいなかったことなどから、大容量の添付ファイルが送信されることを想定しておらず、このような攻撃に対する脆弱性を保有してしまったものと思われる。
他の事業者への波及の可能性	直接的な影響は無し。(同様の攻撃があることは考えられる)
IT 障害の復旧状況	完全復旧
実施した対策	サーバ構成の変更によるサイズフィルタの先行実施。 スパムフィルタを実行するアプライアンスサーバの手前にゲートウェイを設置。規定のサイズを超える添付ファイル付きメールが届いた場合は、社内ネットワークに入るタイミングで破棄するような設定とすることで、メールシステムへの影響を最小限に抑えることができた。
再発防止策	上記およびフィルタ設定ポリシーの見直し
得られた教訓	(1)迷惑メール対策 大容量の添付ファイルが送信される機会が増えてきていることなどを考慮し、システムリソースと業務特性を勘案した適切なフィルタ(スパム・ウィルス・サイズ)の設定や、予兆の検知が重要。 (2)情報セキュリティ対策の定期的な見直し 今回の事象は、通信環境が整備され大容量の添付ファイルが頻繁にやりとりされる状況であったにも関わらず、数年前に構築したシステム構成のままであったために攻撃に耐えることができなかったと思われる。機器の更改期限まで同様の構成を維持することが通例となっていたが、環境変化に応じて変化する脅威や脆弱性に対応するためには、情報セキュリティ対策を定期的に見直すことが重要だと感じた。

【付録2】事例⑤ インスタントメッセンジャーを偽装したマルウェア感染等のケース

項目	内容
攻撃手法	ウイルス・ボット
影響を受けるシステム	各種サーバ、インスタントメッセンジャーがインストールされた端末やそのコンタクト先
詳細情報	(1)インスタントメッセンジャーのクローン インスタントメッセンジャーのクローン(※)を偽装したマルウェアが、インストールされている端末やアクセス可能なネットワーク内の機密情報やパスワード情報等を収集し、不正アクセスに悪用される可能性がある。 ※「ICQ」や「Yahoo!メッセンジャー」等の有力インスタントメッセンジャーのアカウントで利用できるインスタントメッセンジャーのこと(「Regnessem」「Pidgin」等)。複数のサービスを同時に利用できる等、機能面で差別化を図っており、有力インスタントメッセンジャーの使い勝手に不満を持つユーザが利用する場合がある。 (2)インスタントメッセンジャーを経由した不正プログラムの配布 インストールされているインスタントメッセンジャーを経由し、登録されているコンタクト先にマルウェアを配布するマルウェアがある。 【主なインスタントメッセンジャー】 ICQ、AIM、Yahoo!メッセンジャー、Windows Live メッセンジャー、Skype、Google Talk、MySpaceIM 等
想定される影響	・機密情報の流出 ・パスワード情報等の流出 ・不正アクセス ・インスタントメッセンジャーを経由したマルウェア感染 ・インスタントメッセンジャーに登録されたアカウントに対するマルウェアの大量拡散
対策方法	・ポート番号によるフィルタリング ・アプリケーションのインストール制限(規約の制定、資産管理ソフトによる制限等) ・通信状況が管理可能な企業向けインスタントメッセンジャーの導入 等
備考	(関連 URL)多機能マルウェア「WORM_PROLACO」に注意――トレンドマイクロ http://www.itmedia.co.jp/enterprise/articles/1012/06/news062.html

【付録2】事例⑥ 標的型攻撃(メール)の予兆情報

項目	内容
攻撃手法	標的型攻撃
影響を受けるシステム	メールを利用する端末
詳細情報	国立感染症研究所からの豚インフルエンザに関する注意喚起メールに見せかけた、ウイルス添付メールが送信された。 当該メールは、yahoo メールを使用しており、発信者欄には"国立感染症研究所"とある。発信元メールアドレスは、受信者のアドレスと同一である場合が多く、発信者を詐称した不審なメールだった。この添付ファイルが不正プログラム(ウイルス等)で添付ファイルを開くことで、メールを受けたパソコンへの不正侵入やシステム破壊のおそれがあり、注意喚起された。
想定される影響	ウイルス感染による業務停止 情報資産の流出・改ざん・消失 等
対策方法	・同様のメールヘッダの記載があるメールのゲートウェイでのフィルタリング(該当メールの削除)。 ・上記フィルタを透過することも想定されるため、豚インフルエンザに関する注意喚起メールが届いた場合は、開封せずシステム管理者に連絡するよう、利用者に周知する等。
備考	出典:国立感染症研究所 http://www.nih.go.jp/niid/misc/warning090428.html  NIID NATIONAL INSTITUTE OF INFECTIOUS DISEASES 国立感染症研究所 サイトマップ サイト内検索 English Home Page 「国立感染症研究所」を詐称したブタインフルエンザ関連メールにご注意ください 平成21年4月28日 ブタインフルエンザの流行に便乗して、「国立感染症研究所」を詐称したメールが送られているという情報が寄せられています。当該メールは、yahooメールを使用しており、発信者欄には"国立感染症研究所"とあります。発信元メールアドレスは、受信者のアドレスと同一である場合が多く、明らかに発信者を詐称した不審なメールです。メールには「ブタインフルエンザに関する知識.zip」等と題した添付ファイルが含まれています。当方のウイルスチェックソフトウェアで、この添付ファイルが不正プログラム(ウイルス等)として認知されております。添付ファイルを開くことで、メールを受けたパソコンへの不正侵入やシステム破壊のおそれがあり、注意が必要です。以下のような「詐称メール」を受信された方々におかれましては、添付ファイルを開かずにメールごと削除なさるようお願いいたします。 ‖不審メールの詳しい内容(例)‖ From 国立感染症研究所 <任意のアドレス@yahoo.co.jp> Subject:豚インフルエンザに注意! 添付ファイル名:ブタインフルエンザに関する知識.zip Powered by the Internet with Yahoo! Toolbar. 添付ファイルは不正プログラムの可能性があり、開封が必要です。 国立感染症研究所では、メールはすべて"nih.go.jp"のドメインから発信するとしており、yahooから発信されることはありません。また、公的なお知らせはすべてWebサイト上に公開され、メールを用いたサービスは行っておりません。 なお、国立感染症研究所では第三者中継(発信元を隠すために、関係のない第三者のサーバを中継して発信する)されないメールサーバの設定や、ウィルス感染メールを発信しないようウィルス対策をするなどセキュリティにも十分配慮しておりますが、引き続き対策を強化していく考えです。 Copyright (C) Research Organization, NIID, Japan

【付録2】事例⑦ 標的型攻撃(メール)の事例

項目	内容
攻撃手法	標的型攻撃
概要	海外出張時に、日本の携帯電話をローミングにて使用したところ、帰国後にローミング先の現地通信事業者からメールが届き、それには請求書を偽装したウイルス付きのファイルが添付されていた。
詳細情報	① 海外出張時に、日本の携帯電話で通話をローミングで行った。 ② 現地通信事業者に対して、メールアドレスは知らせていない。 (申込書やWeb上での登録等でのメールアドレスの記載はない) ローミング通話を行ったこととメールアドレスをどのように攻撃者が知ったかは不明。 ③ ウイルス付きファイルと特定でいた経緯 攻撃メール本文に記載されていたURLにアクセスすると、ZIPで圧縮されたPDFファイルが送付されてきた。 このファイルをウイルス対策ソフトベンダーに送付して、解析した結果、ウイルスと判明した。
備考	

【付録2】事例⑧ 制御系システムへの Stuxnet の脅威

項目	内容
攻撃手法	制御系への攻撃
影響を受けるシステム	制御系システムおよび関連システムの端末
詳細情報	2010 年 7 月、イランのブシェール原子力発電所において、従業員のパソコン数台がスタクスネットに感染した。主要な制御系システムに感染はみられないものの、本格操業が2カ月遅延の見込みとなった。 【スタクスネットの概要】 Windows シェルの脆弱性(MS10-046 自動オートラン設定)、シーメンス社製ソフトウェア等の脆弱性を悪用し、悪意あるコードのコピーや PLC(Programmable Logic Controller)の書き換え等を行う。制御系システムに感染した場合は、システムの誤作動を招きかねないリスクがある。また、システムの感染を隠ぺいするための工夫がなされており、発見までの期間を要する場合がある。
想定される影響	スタクスネットは亜種が増加している。シーメンス社のシステムだけでなく、他社へ対象を拡大する恐れもある。日本においてはまだまだ独自プロトコルを採用した制御システムが多いが、TCP/IP を使用したシステムの場合には同様の感染もありうる。
備考	(参考情報) IPA テクニカルウォッチ 『新しいタイプの攻撃』に関するレポート ～Stuxnet(スタックスネット)をはじめとした新しいサイバー攻撃手法の出現～ http://www.ipa.go.jp/about/technicalwatch/20101217.html

【付録2】事例⑨ 組織内 CSIRT の活動状況

項目	内容
攻撃手法	全般
対策の概要	■組織内 CSIRT の活動概要 グループ会社全体に対する、インシデントの防止、インシデント発生時の被害の極限化に貢献することを目的としたインシデントサイクルにおけるさまざまな側面のサポートを実施。 ①信頼できる相談窓口 -セキュリティに関するグループ内外の組織やコミュニティとグローバルなネットワークによるグループ内・外部機関との調整機能 ②セキュリティ情報の収集・分析・提供 -セキュリティに関する膨大な情報ソースの分析、注意喚起やアドバイザリ、インシデント対応や予防に関するノウハウの提供や水平展開 -インシデント発生時のシステムに対する分析の実施支援(必要に応じて実施)と再発防止に向けた分析結果の水平展開 ③各グループ会社内の CSIRT 構築支援 -組織内の運用担当者や外部の CSIRT と連携したグループ会社内におけるインシデント管理推進、調整チーム(CSIRT)の構築支援 ④トレーニング・教育 -セキュリティ人材育成支援(上記分析や研究等で得られた知見を技術者向けのトレーニングとして提供) ■情報共有体制 取り扱う情報の種類により以下を使い分けた上で情報共有を行っている ①ある程度原因と対策が明確になったサイバー攻撃に関する脅威や予兆情報、および被害情報 ⅰ)通常時 -(全体に関わる情報)メールやポータルサイトによる一斉同報 -(個別企業に関わる情報)各事業会社のルールに対応した窓口担当者に個別にメールや電話で連絡 ⅱ)緊急時 -グループ会社内で確立している災害対策の仕組み(情報連絡体制)を活用 ②上記以外で、発生している事象の原因や対策が不明確な場合など ※ -属人的に構築された信頼関係を前提に個別にメールや電話で連絡 ※管理者レベルに共有したために、事業会社内での混乱が予想される情報や、現場への早期到達が優先される情報も含む

得られた教訓・課題	＜これまでの運用経験により得られた教訓・課題＞ ①情報の種類に応じた連絡窓口の特定の重要性 ・運用現場以外の担当者または管理層に情報提供をすることにより、運用現場の混乱や適切な対応がとられないケースがあるため、情報の種類に応じた連絡窓口の特定が重要である。 ②過去の教訓を認識することの重要性 ガンブラーは世の中で一般的事例になる前から一部の ISP では予兆情報と認識して対応していた。グループ会社内にも情報発信を行っていたが、それをもとに危機を感じて対処していたのはごく一部の人に過ぎず、他企業での Web の改ざん事件が発覚後、ようやく事の重大性に気付いたといった過去の経験がある。予兆情報は確定情報ではないため提供に課題が残るが、過去の事例と照らし合わせ、対策に活かしていくことは重要な要素である。 ③コミュニティ形成への支援の必要性 ・Waledac ボットネットに対する取り組みは、悪意のあるドメインと Waledac に感染した PC との通信を遮断することで、壊滅的な状況に追いやることに成功した。これは、全世界の CSIRT が収集したボットネットに関する情報の収集と共有がなければ実現は困難だったと思われる。この活動の原動力となったのは、普段からの技術者同士の信頼関係の上の情報交換の場であった。こうした情報収集・共有の活動やセキュリティに関するコミュニティを支援するような取り組みは、セキュリティ対策を向上させていく上で必要である。 ＜参考＞経験から感じた情報共有に必要な要素 ・意識の高い情報システム担当者は、同じ目的をもった横の連携を図り、活用している。この連携には個人的な信頼関係が基盤となっており、競合他社等の壁を越えて協力体制が構築されている場合もある。 ・他業界の情報については、通信は様々な業界に利用されているという意味で知っておくべきであり、他業界に発生した事象でも自社にあてはめて考えることはできるため業界を超えた情報共有は必要である。

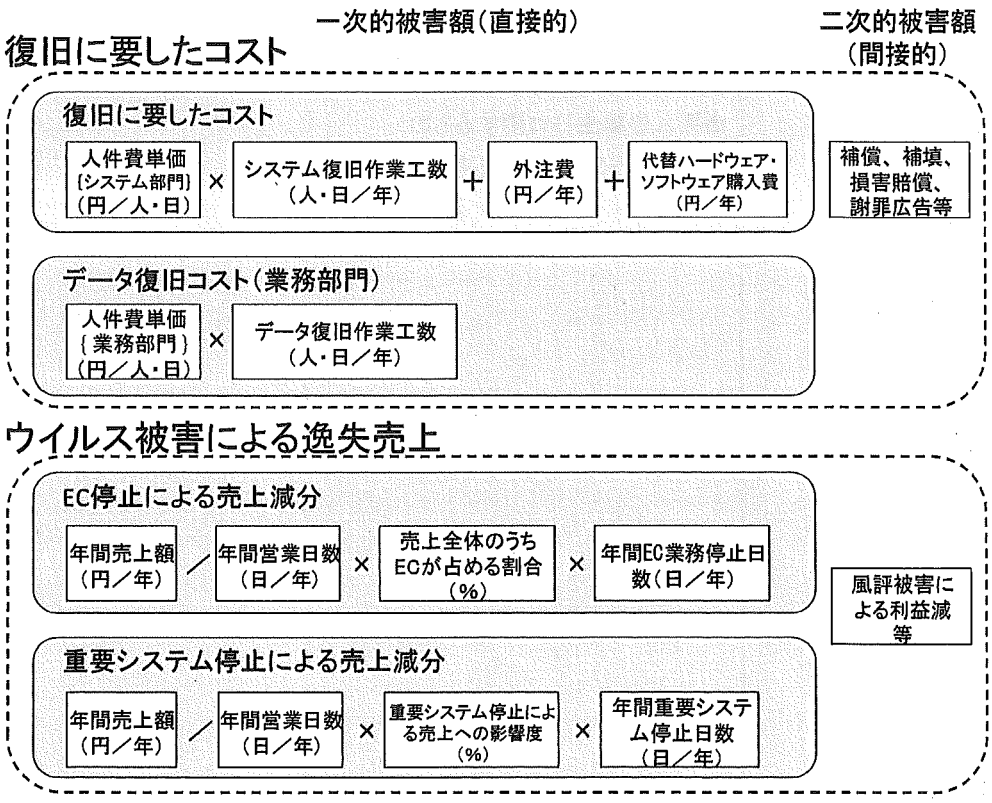
【付録2】事例⑩ 大規模なサイバー攻撃に備えた全社的な事前訓練より得られた教訓

項目	内容
攻撃手法	全般
対策を実施したサービス等	大規模なサイバー攻撃発生を想定した体制・指揮系統・手順等の確認・見直し改善
対策の概要	【目的】 関係者による事前演習を実施することで、大規模なサイバー攻撃時におけるサービス維持および被害拡大防止を図る。 【参加者】 社内関係部門の管理者・技術者(危機管理部門、各サービスの保守部門、研究・開発部門、情報セキュリティ部門、営業・SE 部門、グループ関係部門) 【演習内容】 ①6 通りのサイバー攻撃のシナリオに基づく、集合型の机上演習を実施 ②参加者にはシナリオを事前に周知せず、より実践的な内容によって課題等を検証 【実施内容】 ①サイバー攻撃発生時における対応方法の訓練・検証 ②危機管理態勢の訓練・検証 ③関連部門間の連携訓練・検証、課題の抽出 【備考】 本演習の他に、分野横断的演習(NISC 主催)、電気通信分野の業界横断的サイバー攻撃対応演習(総務省、T-ISAC 主催)、グループ内のサイバー攻撃対応演習に企画・演習参加したことにより、2010年9月の大規模サイバー攻撃発生時にも社内横断的な危機管理態勢を確立し、迅速にかつ柔軟に対応することができた。
対策の効果	(1)危機管理態勢や社内連携の検証・見直しの実施 本演習をもとに、サイバー攻撃の予告または発生時の社内体制や連携等の課題を抽出することができ、有事の際の危機管理態勢や復旧体制を見直すとともに、社内規程を改訂することができた。また、日本 APEC における防備・特別保守に対し、物理的な防備・保守だけではなくサイバー攻撃の危機管理も盛り込み、日本 APEC の成功に寄与することができた。 (2)サイバー攻撃対策や運用手順の検証・見直し 2009年9月の大規模なサイバー攻撃の対応に関する事例をもとに、社内の運用手順や対策を再整理・資料化したが、本演習で抽出した課題をもとに、再度運用手順や対策を見直すことができた。
得られた教訓・課題	(1)事前検討により、必要な体制と対応方法を明確化することが可能 訓練を実施することで、必要となる人員体制や指揮系統、各手順書の具体的な見直しを行うことができた。その結果、緊急体制の確立を円滑に行うことができた。 (2)分野横断的な情報共有への課題 ①サイバー攻撃対応時は顧客、社内、関連企業などへの対応で精一杯であるため、サイバー攻撃発生時(特に初動時)においては、全ての重要インフラ事業者等との分野横断的な情報共有は難しいのではないか。 ②通信の秘密の制約条件によってグループ企業内でも情報共有ができないケースもあるため、予め通信の秘密に抵触しない範囲での共有方法に関するガイドライン等を策定することで、関係者の合意を得ることが必要である。

【付録2】事例⑪ クレジットカード業界におけるデータセキュリティ基準であるPCI DSS

項目	内容
攻撃手法	全般
概要	クレジットカード業界におけるデータセキュリティ基準である PCI DSS(Payment Card Industry Data Security Standards:PCI データセキュリティ基準)の概要
詳細情報	PCI DSS(Payment Card Industry Data Security Standards:PCI データセキュリティ基準)とは、クレジットカード加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準(※1)。 カード情報を扱うカード加盟店、銀行、決済代行など行うサービスプロバイダは、年間のカード取引量に応じて、PCI DSS に 準拠する必要がある。 PCIDSS を遵守するためには、6 分野にわたる 12 個の要件を満たす必要があり、それらは ISMS(情報セキュリティマネジメントシステム)と比較すると、具体的な内容となっている。 クレジットカード業界に関連のない事業者(自治体や学校など)においても、自組織のセキュリティマネジメントポリシーを策定する際の参考として活用することが考えられている。 ※PCI DSS 遵守の対応が想定されるお客様の業界例 -金融業:クレジットカード会社、クレジットカード発行金融機関 -流通業: 大手百貨店、スーパー、量販店、鉄道、航空会社 -通信/メディア/公共:携帯電話会社、通信会社、ユーティリティ、新聞 -製造業:石油業界 他 (日本カード情報セキュリティ協議会 Web サイトより抜粋)
備考	■PCI Security Standards Council (PCIDSS の普及促進を目的とした国際的フォーラム) https://www.pcisecuritystandards.org/ ※PCI DSS Ver2.0(日本語版含む)は上記「PCI Standards & Documents」からダウンロード可能

【付録2】事例⑫ ウイルス被害による被害額算出モデルの例

項目	内容
攻撃手法	全般
概要	ウイルス被害による被害額算出モデルの例
詳細情報	情報セキュリティ対策を実施するにあたり、被害が発生するリスクに基づき、投資額を決定する。情報セキュリティ対策の費用対効果を定量化することは難しい作業であるが、以下のような算定モデルはひとつの考え方として参考にできる。 IPA から公開されている「企業における情報セキュリティ事象被害額調査報告書」では、主にウイルス被害による被害額算出モデルが示されており、他のセキュリティ事象の被害想定額を算出する際の参照モデルとするなど、情報セキュリティ対策投資にどの程度予算を割り当てるか検討する際の参考としてご活用できる。 （以下抜粋） ウイルス被害額＝復旧に要したコスト ＋ ウイルス被害による逸失売上 
備考	詳細は、IPA のホームページを参照。 「企業における情報セキュリティ事象被害額調査」及び 「国内におけるコンピュータウイルス被害状況調査」[2005 年] http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html

【付録2】事例⑬ サイバー攻撃に影響の考えられる各国のソーシャルイベント情報

項目	内容
攻撃手法	全般
概要	これまでの経験より、サイバー攻撃の発生する可能性が高いと考えられる、各国のソーシャルイベント情報
詳細情報	各種インシデントに対し事前に対応することが望ましいが、脅威が多様化・複雑化する中において事前対策の鍵となる「予兆情報」は非常に把握が困難であり、把握の手法は以下の 2 つである（大半が①のケース）。 ①脅威の存在が明確化したり、被害が顕在化した時点で原因追究をした際に「あの時の事象が予兆だった」と気付くケース ②定点分析を通じた異常値の発生に伴い気付くケース そのような状況下で狙いを定めた監視対応は対策のひとつとして有効であると捉え、サイバー攻撃が発生する可能性が高いと想定される各種イベント（建国記念日や要人の誕生日、政治イベント等）について、BBC や CNN などを用いてリスト化し、予告サイト等のチェックを行っている。 （例） ■建国記念日に関するもの ■要人の誕生日に関するもの ■政治イベントに関するもの ■その他イベントに関するもの　等
備考	