JA

2009 年 8 月 19 日

SAC 40：悪用・誤用に対するドメイン登録サービス エージェントの保護手段

ICANN Security and Stability Advisory Committee（SSAC）からのレポート

序文

このドキュメントは、登録サービスを悪用・誤用から保護する手段について説明する、Security and Stability Advisory Committee（SACC）によるレポートです。SACC は、インターネットの命名およびアドレス割り当てシステムのセキュリティと整合性に関連する事項について、ICANN コミュニティおよび理事会に助言を行います。その対象には、運用上の問題（正確で信頼性の高いルート名システムに関する問題など）、管理上の問題（アドレス割り当ておよびインターネット番号割り当てに関する問題など）、および登録上の問題（WHOIS などのレジストリおよびレジストラ サービスに関する問題など）が含まれます。SSAC ではインターネット命名およびアドレス割り当てサービスについての脅威評価およびリスク分析に取り組んでおり、安定性およびセキュリティに対する最大の脅威が存在する場所を推定して、ICANN コミュニティに助言を行っています。SSAC には規制、執行または裁定を行う公式な権限はありません。そのような権能は他者に属するものであり、ここで行う助言はその価値によって評価されるものです。

このレポートへの貢献者、委員会メンバーの経歴および自己紹介、このレポートの結論または推奨案に対する委員会メンバーの反論については、レポートの末尾に記載されています。

概要

ドメイン名登録アカウントに対する攻撃および、ドメイン名システム（DNS）レコードの悪意のある変更は有害なセキュリティ イベントです。過去一年に発生した出来事は、DNS およびドメイン登録アカウント アクセスが攻撃者にとって魅力的な標的であり続けていることを示しています。ドメイン名登録に関する情報の不正な変更は、意図されたホスト以外の宛先にトラフィックを転送するために DNS を使用する目的で DNS 構成情報を悪意を持って変更するものも含め、*たとえ一時的であっても*、ビジネスの運営を著しく混乱させ、金銭的な損害や評判の低下などを引き起こすことがあります。

ドメイン名登録アカウントおよび名前解決サービスのハイジャックは、いずれも新しい方向性の攻撃ではありません。過去のレポ ートおよびアドバイザリにおいて、 ICANN Security and Stability Advisory Committee（SSAC）はドメイン名登録および DNS 運用に影響を及ぼす問題点について、ユーザー（レジストラントなど、レジストラの顧客）の視点から研究してきました。その結果、レジストラントがドメイン名を保護するために十分な措置を講じていない状況が特定されました（登録の更新や正確な連絡先情報の維持を怠るなど）。SSAC では、レジストラントが登録および管理するドメイン名に関してビジネスおよび運用上の利益を保護するために、レジストラに推奨される措置を示します。

このレポートは、ドメイン登録アカウントへの不正アクセスにかかわる最近のインシデントに関連するものです。そのようなイベントについて述べる目的は、レジストラ、再販業者*または*レジストラントを困惑させたり、批判することではありません。セキュリティ イベントの分析により、イベントを回避またはその重大度を低下させるために各当事者が実行可能な*何か*が必ず明らかになるからなのです。

このレポートでは、ドメイン名登録アカウントにかかわる注目度の高い特定のインシデントに読者の注意を喚起し、特定の脅威および脆弱性を緩和する手段を明らかにできるような、イベントに共通の原因を特定します。インシデントについて詳細に分析し、アカウントが危険にさらされた原因、アカウントのコントロールを取得した後攻撃者が行った行為およびその結果を特定します。説 明は、公表されているニュース ストーリーおよび記事から導かれました。標的となったレジストラおよびその顧客への聞き取りを通じて得られた情報でそれらを補完しました。標的となった当事者によって秘密情報と判断された情報は意図的に排除されています。

レポートでは、顧客を同様の脆弱性から保護するために他のインターネット ビジネス セグメント（金融、耐久財販売業など）で使用されているセキュリティ手段を示します。レジストラおよび顧客の双方が登録ドメインを悪用・誤用から保護するために、レジストラが顧客と共有可能な慣行を特定するとともに、たとえ一時的であってもドメイン名および関連する DNS 構成に対するコントロールを失うことに関するリスクについてレジストラントの関心を喚起する方法について論じます。高水準のサービス提供によって差別化を実現しているレジストラもありますが、このレポートでは、より多くのレジストラに、ドメイン登録アカウントへの攻撃に対する追加的保護を提供する機会について考慮することを推奨します。また、レジストラに対して、競争の厳しい市場においてサービスを差別化する方法として、登録のセキュリティ手段を強調することを推奨します。

研究の動機

過去 12 か月の間に、ドメイン名アカウントへの不正アクセスにかかわる注目度の高いインシデントがいくつか発生しました。この突発的な攻撃には、ドメイン名ハイジャック[1]、およびドメイン名の不更新にかかわる予期せぬ結果に関して SACC が以前に行った研究の動機ともなった、共通する特定の特徴がありました。[2、3] 一部のインシデントは、レジストラのスタッフおよび登録サービス（Web 対応のドメイン アカウント管理ツールなど）に対する悪意のある行為でした。その他のインシデントでは、ソーシャル エンジニアリングが利用され、ルーチンが悪用されたり、レジストラから顧客への通信が予想された可能性があります。[4]

SSAC では、2008 年 5 月から 2009 年 4 月にかけて発生した一連のインシデントについて考察しました。これらのインシデントから、脆弱性のみならず、悪用されたポリシーおよび慣行（ビジネス上および運用上）も特定し、共通の脅威が発生するかどうか判断しました。これらのインシデントについて研究した結果、下記の知見を得ました。

(1) 多くの組織が、価値の高いまたはビジネス上重要な名称、組織が保有する任意の有形資産、商標または知的財産権と同等の価値を持つドメイン名を含むドメイン名登録アカウントを保有しています。

---

1 SAC007, Domain Name Hijacking Report, http://www.icann.org/announcements/hijacking-report-12jul05.pdf

2 SAC011, Problems caused by non-renewal of a domain name associated with a DNS name server, http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf

3 SAC010, Renewal Considerations for Domain Name Registrants, http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

4 SAC028, Advisory on Registrar Impersonation Phishing Attacks (26 May 2008), http://www.icann.org/committees/security/sac028.pdf

(2) 多くの登録サービス プロバイダは、顧客重視のサービス目標に従って運営されており、登録サービスが高度に自動化され、高速なトランザクションで多数のレジストラントにサービスを提供することが重視されています。タイムリーかつスケーラブルな方法でサービスを提供するビジネス上の取り 組みにおいて、自動化は非常に重要です。この研究では、攻撃者がレジストラの挙動を熟知しており、自動化の特定の側面を悪用することを明らかにしました。たとえば、連絡先および構成の変更、更新などについてレジストラントに通知する方法として電子メールが好まれることを知っている攻撃者は、しばしば、DNS 構成を変更することにより、電子メール アドレスへのメール配信を中断させようと試みます。

(3) 研究対象となったインシデントの多くでは、ビジネス上重要なドメインアカウントを持つ顧客が被害者となっており、それらのアカウントは顧客重視のサービス目標を持つ登録サービス プロバイダによって運用されていました。一部のケースでは、被害が発生するまで、顧客がドメイン登録アカウントへのコントロールまたはアクセスを失う可能性に関するリスクを適切に評価していませんでした。その他のケースでは、インシデントの発生前に実施されていたポリシーおよびモニタリング活動が不十分なため、攻撃を検出またはブロックすることができませんでした。

一部の被害者は、規模およびビジネス上の評判に基づいて、ドメイン名の資産価値を認識するための内部セキュリティ管理およびリスク管理の点で十分洗練されていると思われましたが、ドメイン名をリスク評価の対象に含めていませんでした。その他の被害者、特に中小組織および個人は、問題が発生するまでドメイン名の重要性を十分には理解していなかった可能性があります。これは、その他のリスク領域に関する行動とも一貫しています。多くの状況において、資産の価値またはビジネス上の重要性を認識していた可能性はあるものの、インシデントが発生するまで、そのような資産に対する適切な保護手段を講じていなかった可能性があります。

セキュリティの観点から、ドメイン名が重要な資産であると考えているレジストラントは、登録サービス プロバイダの選択時にセキュリティを重要な選択基準とすべきです。SSAC が研究したインシデントでは、レジストラントが、登録サービス プロバイダから提供されるセキュリティ サービスの範囲について理解していないか、選択可能な多様なセキュリティ サービスが*存在する*ことを評価していないことが明らかになりました。あるレジストラのコメントによると、レジストラントは登録サービスが似たり寄ったりであると考えており、すべてのレジストラが同一のレジストリから提供される同一の製品を販売しているのだから、どのレジストラが提供するセキュリティ手段も同じようなものであると結論づけています。次のセクションで説明するインシデントでは、登録サービス プロバイダ間の差異がドメイン名コミュニティ の外部ではよく理解されていないという SSAC の結論が支持されています。

ドメイン名登録アカウントに対する攻撃

このトピックに関するイベントの包括的なリストを提供することは、このレポートの範囲を超えるものですが、今後の議論および分析の背景を提供するため、ドメイン名登録アカウントに対する注目度の高い特定の攻撃について概要を示します。概要では公表されているソースからの情報を豊富に引用しています。また、インシデントに巻き込まれたレジストラはもちろん、攻撃の被害者となった組織に対する聞き取りも行っており、ご協力いただいた皆様に感謝いたします。

Comcast（2008 年 5 月）

米国最大のケーブル テレビ事業者である Comcast は、インターネット サービス プロバイダとしても全米 2 位、住宅向け電話事業者としても 大手の地位を占めています。[5] インシデントの発生時点において、Comcast は、Network Solutions, Inc を通じて約 200 のドメインを登録していました。[6] 2008 年 5 月 28 日、攻撃者が Network Solutions の管理する Comcast のドメイン登録アカウントへのアクセスを取得しました。当初、攻撃者は特定の連絡先情報を悪意を持って変更しましたが、これは同社の評判を下げるためだと思われます。[7] Comcast のスタッフは、変更に関する電子メール通知を受信し、正しい情報を復元しました。

攻撃者は、Comcast の管理者に電話で脆弱性および彼らのエクスプロイトについて説明したと主張しました。彼らの主張によると、ソーシャル エンジニアリングと技術的なハッキングを組み合わせ、ドメイン登録アカウントへのアクセスを取得したということです。[8] Network Solutions では、同社のスタッフによるセキュリティ侵害またはソーシャル エンジニアリングはなく、DNS の変更は顧客のログイン情報を 入手した何者かによって行われたと報告しています。[9] *Wired Magazine* の記事によると、攻撃者は、連絡先管理者が「彼らの主張をあざ笑い、電話を切った」と主張しています。[10] 攻撃者は再度アカウントにアクセスしました。このとき、彼らは、comcast.net ドメインの DNS 構成を変更し、セキュリティが破壊されたサーバーにホスティングされた同社の評判をおとしめる Web サイトにトラフィックをリダイレク トしました。しかし、Comcast のスタッフには

---

[5] Comcast に関するエントリ：en.wikipedia.org/wiki/Comcast

[6] Comcast.net Domain Hijacked at Network Solutions, http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619

[7] How was Comcast.net hacked?, http://blogs.zdnet.com/security/?p=1224

[8] Comcast.net name hijacked, http://www.internetidentity.com/2008/June-2008.html

[9] Comcast account access issue – clarification, http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/

[10] Comcast Hijackers Say They Warned the Company First, http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html

Network Solutions から変更を通知する電子メールが届きませんでした。ドメイン登録レコードに記録されている技術および管理用の連絡先の両方で、Comcast 登録ドメインから割り当てられた電子メール アドレスが使用されていました。DNS 構成を変更することにより、攻撃者は、Comcast のスタッフがアカウント アクティビティに関する電子メール通知を全く受け取れないようにしました。電子メールは配信不能になりました。攻撃は成功し、世界中で大きく報道されました。*Wired Magazine* によると、「攻撃は東部標準時の午後 11:00 頃に始まり、ハッカーは Comcast.net を翌日の午前 4:00 または 5:00 まで保持しました。Comcast がコントロールを回復した後も、DNS を通じて変更が完全に伝播するまで数時間かかり、一部の顧客は木曜日の午前 11:30 頃まで Web メールにアクセスすることができませんでした」。2008 年 5 月 29 日付の *The Register* の記事では、「攻撃者は、時代遅れのアカウント セキュリティ破壊でも、相当な量の Web トラフィックを変更するのに十分であることを示した」とコメントしています。[11]

CheckFree（2008 年 12 月）

CheckFree (現 FIServ) は、金融サービス業界向け情報管理および電子商取引システムの大手グローバル プロバイダです。[12] 2008 年 12 月 2 日、攻撃者が、Network Solutions の管理する CheckFree のドメイン登録アカウントへのアクセスを取得しました。[13] 攻撃者は、checkfree.com および mycheckfree.com を含む複数のドメインの DNS 構成を変更しました。オンライン請求書支払いサービスを利用するためにアカウントにログインしようとした顧客は、ウクライナに存在するサーバー上の偽装 Web サイトにリダイレクトされ、Adobe Reader のエクスプロイトを含む悪意のあるコードのインストールが試行されました。[14] CheckFree は攻撃から 8 時間以内に正しい DNS 構成を復元しましたが、類似のインシデントと同様に、グローバル DNS インフラを通じた変更の伝播には数時間かかりました。[15]

The *Washington Post* 紙のブログ「Security Fix」では、攻撃者が正しいログイン情報を使用してアカウントにアクセスしたと述べられて います。この記事によると、Network Solutions は、ログイン証明情報を取得するために攻撃者が同社のシステムを破ったこと

---

11 Potty-mouthed hackers steal comcast.net keys, go for a spin, http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/

12 FIServ, http://en.wikipedia.org/wiki/Fiserv

13 DNS attack hijacks payment website, http://www.techworld.com/security/news/index.cfm?newsid=107959

14 Network Solutions phishing attack preceded CheckFree domain takeover, http://*www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722*

15 http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf

はないと強調しています。[16] 攻撃者がユーザー アカウントおよび証明情報を取得した正確な方法は不明（または未公開）です。

ICANN、Photobucket、RedTube（2008 年 6 月）

2008 年 6 月 26 日、ICANN 自身もハッカー グループの被害者となり、Register.com の管理する ICANN のドメイン登録アカウントへの不正アクセスを受けました。ICANN のプレス リリースによると、攻撃は「ソーシャル エンジニアリングと技術的方法を組み合わせた洗練されたもの」でした。[17] ICANN の IT 担当役員によると、攻撃者が icann.net、iana-servers.com、icann.com、internetassignednumbersauthority.com および iana.com など、複数のドメインの DNS 構成を変更したため、ビジターのトラフィックは Atspace.com によって運用される無料 Web ホスティング アカウントで公開された ICANN の評判をおとしめる Web サイトにリダイレクトされました。インシデントの発生したタイミング（新しい GTLD に関するパブリック ディスカッションが開催される ICANN パリ会議の冒頭）および Web サイトに掲載されたメッセージに基づいて、政治的な動機による攻撃であると推測されています。ICANN の IT スタッフが DNS の変更を検出し、ICANN からの通知を受けた Register.com によって速やかに正しい情報が復元されました。しかし、Comcast のインシデントと同様に、悪意のある DNS 構成情報は、修正された情報が全世界に伝播するまで、24 ～ 48 時間[18]グローバル DNS に止まったと推定されます。

ICANN への攻撃を行ったと主張するハッカー グループは、その後の攻撃でも同様の戦術および無料ホスティング プロバイダを利用しました。Photobucket は、2007 年に Fox Interactive に買収されたイメージ ホスティング、ビデオ ホスティング、スライドショーおよび写真共有 Web サイトです。[19] 2008 年 6 月 18 日、同じハッカー グループが Photobucket に対する攻撃を行い、その結果 Photobucket ユーザーに対するサービスが中断されたと主張しました。[20] このグループは、2009 年 2 月 7 日にも、成人向け動画等のホスティング サイトである RedTube の評判をおとしめる攻撃を行いました。[21、22]

---

16 Digging Deeper into the CheckFree attack, http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html

17 ICANN Response to Recent Security Threats, http://www.icann.org/en/announcements/announcement-03jul08-en.htm

18 Turkish criminal hackers hijack ICANN sites, http://news.cnet.com/8301-10789_3-9980713-57.html

19 Photobucket, http://en.wikipedia.org/wiki/Photobucket

20 Photobucket's DNS records hijacked by Turkish hacking group, http://blogs.zdnet.com/security/?p=1285

21 Popular porn site attacked by prudes, http://www.securecomputing.net.au/News/102818,popular-porn-site-hacked-by-prudes.aspx

22 Turkish Hackers Take Out Top Porn Site, http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNDLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security

DomainZ（2009 年 4 月）

DomainZ（Domainz.net.nz）はニュージーランドに本社を置くレジストラで、 MelbourneIT の子会社です。2009 年 4 月 21 日、悪名の高い探索者が DomainZ のパスワード取得ページに対して SQL（構造化参照言語）インジェクション攻撃を行い、Coca-Cola、Fanta、F-secure、HSBC、Microsoft、Sony および Xerox などを含む注目度の高い複数のレジストラントのアカウント証明情報を収集 しました。攻撃者は .CO.NZ 以下に登録されたドメインの DNS 構成レコードを変更し、.INFO ドメイン（turkguvenligi.info）以下に登録されたネーム サーバーをポイントするようにしました。これらのサーバーは、ハッキングされたドメインを攻撃者によってホスティングされた評判をおとしめる Web サイトに解決する、不正なゾーン情報をホスティン　グしていました。一部のトラフィックは、Microsoft などのブランド名を標的にした悪意のある　Web ページにリダイレクトされ、その他のトラフィックは政治的な抗議のメッセージを掲載したページにリダイレクトされました。

これらのインシデントから明らかになったこと

Comcast、ICANN、Photobucket および RedTube への攻撃に類似点が多いことは、登録アカウントへの攻撃者が、Web、ファイル転送およびその他のインターネット　アプリケーションに対して同様な傾向を持っていることを示しています。ある分野で脆弱性の悪用に成功すると、攻撃者はエクスプロイトを共有し、同じまたは同様な脆弱性を持つ標的を探索します。

これらのインシデントから、SSAC では下記の知見を得ました。

一部のレジストラについて：

1. ある組織の完全なドメイン名ポートフォリオのコントロールを取得するために（そしてポートフォリオへの許可されたアクセスを阻止するために）、攻撃者が入手する必要があるものは、1 つのユーザーアカウントとパスワードだけです。

2. 攻撃者は、ドメイン登録アカウントのコントロールを取得するために、推測、フィッシングまたはソーシャル エンジニアリング技術を一括窓口（SPOC）に適用するだけです。

3. 攻撃者はドメイン アカウント登録および管理ポータルをスキャンし、Web アプリケーションの脆弱性（SQL インジェクションなど）を探します。脆弱なアプリケーション コードのエクスプロイトに成功すると、多数のドメイン アカウントのアカウント証明情報が開示される場合があります。

4. レジストラがレジストラントにアカウント アクティビティを通知する方法としては電子メールが好まれており、一部のレジストラでは唯一の 方法となっています。（後のセクションでは、追加の連絡方法について論じます）。

5. 攻撃者は、DNS 構成情報を変更し、セキュリティが破壊されたアカウントを通じてコントロールされるドメインにおいて、任意の受信者に電子メール通知を行えなくすることにより、標的となったレジストラントへの電子メール通知の配信をブロックすることができます（ドメインでホスティングされているレジストラント固有の技術または管理用の連絡先電子メール アドレスなど）。

6. 登録アカウントに含まれるすべてのドメインの連絡先および DNS 構成情報へのアクセスおよびそれらを変更する権限は、一般に、単一のユーザー アカウントおよびパスワードを通じて付与されます。

7. DNS 情報の不正な変更を速やかに発見した場合であっても、悪意のある構成を修正するための DNS 情報の復元処理には時間がかかる場合があります。これは、DNS が分散型であるという性質に固有の問題であり、生存時間（TTL）の値にも関連しています。

登録保護措置に対する顧客の理解不足

一部のレジストラは、ビジネスのセキュリティ確保と顧客の保護に秀でています。これらのレジストラは、Web アプリケーション、ネーム サーバーおよびホスティング サーバーのセキュリティ確保にベスト プラクティスを適用しています。また、疑わしいアクティビティについてシステムおよびアカウントをモニタリングしています。レジストラのサポート スタッフは、悪用または犯罪に対する苦情に効率的に対応しています。しかし、ドメイン登録サービスのように幅広い業界では、電子商店やオンライン ビジネスのあらゆるクラスにおけるのと同様、一部のレジストラが既知の攻撃ベクトルに対して脆弱であることが判明するのは避けられません。その他のレジストラについても、たとえ最良のレジストラであっても、セキュリティ監査において考慮されなかった攻撃や未知の攻撃に対して脆弱であることが判明する可能性があります。

このレポートで論じたインシデント（および、SAC012 で引用された同様のインシデントおよびその発行後に発生した同様のインシデント）から、レジストラの処理がこれまでも、そして、これからも攻撃者に利用され続けることは明らかです。業界の規模および多様性を考えれば、これは異常なことではありません。レジストラは、これまでも、そして、これからも攻撃者の標的であり続けるでしょう。*緊急期間の顧客がオンライン バンキング ポータルに対する攻撃の被害者となる可能性があるのと同様に、ドメイン名レジストラントは、レジストラのドメイン管理ページに対する攻撃の被害者となる可能性があります。*

ドメイン名および DNS 構成に対する攻撃のリスクを評価し、レジストラントの攻撃への露出を受容可能な程度に低減する登録サービスを選択することは、結局のところレジストラントの責任です。しかし、レジストラは提供する保護手段について注意を喚起しないのが一般的であり、登録セキュリティ サービスを比較する手段がないため、顧客は、セキュリティに関してすべてのレジストラが同等であるという誤った結論を下し、望ましくない選択または無頓着な選択を行う可能性があります。

異なるターゲット市場およびサービス モデルを持つレジストラ

上記のことを念頭に置き、SSAC では、広範なドメイン名登録サービスについて検討し、ドメイン名登録が 2 つのサービス モデルを通じて大いに支持されると判断しました。

人気のあるサービス モデルの 1 つは、比較的低価格から低価格の価格帯でドメイン名登録サービスを提供するというものです。サービスの提供は高度に自動化され、ヒューマンエラーの可能性が最小限に抑えられることが多い一貫した繰り返し可能な方法で、大量のトランザクションを高速処理することが強調されるよう設計されます。顧客との通信は電子メール メッセージを通じてサポートされるのが一般的で、通知や、義務的プロセス（年に 1 回 WHOIS の情報が正しいことを確認するプロセスなど）について案内する簡単な指示（多くの場合逐次的な指示）が送信されます。チケッティング システムを通じた自動トラブル報告も一般的です。一般に、自動化は人間の介入よりも優れていると思われます。ほとんどの場合、人間の介入は自動化が想定通りに動作しないか、理解できない場合、あるいは、自動化プロセスで解消できない問題に直面するか、インシデントを報告する場合に、顧客によって求めらます。ドメイン アカウントおよび DNS 構成を悪用から保護するセキュリティ手段には、SSL（Secure Socket Layer）保護されたドメイン アカウント ログインおよびドメイン ポートフォリオ管理、DNS またはアカウントに関連付けられた連絡先情報の変更時の電子メール通知、プライバシー サービス（SAC023[23] で論じられた保護また委任された WHOIS サービス）、ドメイン移転保護（レジストラ ロック、レジストラの喪失および取得の間での認証コード確認）が含まれるのが一般的です。[24]

2 つめの登録サービス モデルは、ドメイン名の価値を重視し、ドメイン名およびオンライン プレゼンスをビジネス上重 要なものと認識しているか、ビジネスまたはブランド名が悪用または犯罪行為の主要な標的となっていることを認識している顧客のニーズに合わせて、保護手段を提供するものです。顧客はドメイン名に対する脅威を認識し、喪失、構成エラー、連絡先または DNS 構成情報の変更、ドメインの誤用のリスクを最小化または低減したいと望んでおり、そのような要件を満たすレジストラを探し出すために、十分な

---

[23] SAC023, Is the WHOIS Service a Source for email Addresses for Spammers? http://www.icann.org/en/committees/security/sac023.pdf

[24] 悪用防止およびセキュリティ手段を実装し、内部（ビジネス上重要な）システム、プロセスおよびデータベースを保護しているレジストラもあります。これらは、レジストラの顧客には意識されないのが一般的です。

情報に基づく意志決定に必要な情報を収集しています。そのようなレジストラは、技術的エラーまたは見落としに起因する顧客のドメイン名不更新を防止するセキュリティ手段を提供し、登録レコードの不正な変更を通じて顧客のドメイン名がハイジャックされることを防ぎ、不正な、悪意のある DNS 構成を防ぎます。これらのレジストラのビジネス モデルでは、個別のトランザクションを非常に低いエラー発生率で処理することが重視されています。このようなレジストラは、ドメイン名ポートフォリオの保護にプレミアムを付け、人間の支援（特に、顧客担当のアカウント スペシャリストによる支援）に進んでプレミアムを支払う顧客にサービスを提供します。顧客は、たとえば、セキュリティとして、変更リクエストを実行する前に顧客の認定した連絡先からの口頭または書面による確認および、レジストラからの DNS 構成および名前解決サービスのリアルタイム モニタリングを求める場合があります。

一般的に、上記の手段は、ブランド エクイティの保護を強調するより広範なパッケージの一部です。ブランド エクイティの保護手段は、商標の悪用（インターネット ユーザーを商標/ブランド所有者以外の Web サイトに呼び込むための商標またはブランドの不正使用など）、ブランド所有者を標的としたドメイン登録（フィッシングまたは詐欺攻撃に使用されるほぼ同じ、「同形異義」のドメイン）、利益またはトラフィックの不正転用、バックオーダー（他の当事者によって登録済みのドメインが再度利用可能になった場合に顧客の代理でドメインを登録しようとすること）および、防衛的登録（すべてのトップ レベル ドメインで商標または名称を登録すること）を含むリスクの低減を図るものです。

ドメイン アカウントおよび DNS ハイジャックに対する保護を必要とする対象

ドメイン アカウントまたは DNS 構成情報の悪意のある変更に対する強力な保護手段は、一般に、ドメイン ポートフォリオまたはブランド エクイティに関する懸念に対して大きな投資を行い、ブランドを保護するための手段および支払い意志を持つ企業によく知られており、求められています。しかし、*レジストラントは、保護すべきブランドまたは知的財産を持つ企業のみがドメイン アカウント ハイジャックまたは DNS 構成情報の悪意のある変更に対する保護を必要としていると結論づけてはなりません。*オンライン プレゼンスに依拠している多くの組織は、ブランド名に関連付けられたドメイン名を使用してはなりません。それでもなお、他者がドメイン名を登録して、そのドメイン名の下でビジネスを行うことは容易です。このような組織は、Web、メールおよびその他のインターネット サービスに名称を割り当てていた場合、これらのサービスがホスティングされた IP（Internet Protocol）アドレスに解決されないため、損害または損失を被ることになるでしょう。

このレポートでは、ドメイン名の喪失または DNS 構成情報の悪意のある変更に関連するリスクを有意に低下させる登録サービスを選択することにより、特定の組織が利益を得るであろうことを仮定し、そのような組織がセキュリティ手段以外の理由でレジストラを選択する原因として可能性のあるものを特定しようと試みました。可能性のある原因のいくつかを下記に示します：

知覚されたコスト：組織によって、ドメイン アカウントおよび DNS ハイジャックに対する強力な保護手段を提供するレジストラを通じたドメイン登録のコストが許容不能なほど高いと想定または誤解されている場合があります。

認知度：特定の顧客はドメイン アカウントおよび DNS ハイジャックに対する強力な保護手段について支払い意志を持っているものの、そのようなサービスの存在に気づいていない場合があります。

情報不足：組織が、入手可能な限られた情報に基づいて、すべてのレジストラが同様の保護手段を提供していると結論づける場合があります。

「レジストラのサービス バンドルが組織に適合しない」：組織がドメイン アカウントおよび DNS ハイジャックに対する特定の強力な保護手段について支払い意志を持っているものの、特定のレジストラがバンドルしている（と認識された）サービスについて支払い意志がないか、支払い不能な場合があります（強力な保護手段にブランド エクイティ保護が追加されている場合など）。

この文脈において、考察する価値のあるいくつかの追加的疑問があります：

ブランドの保護を求めている組織のみが強力な登録保護手段に関心を持つのか？

いいえ。多くの組織は、ブランドだけではなく、オンライン プレゼンスをも保護する欲求と、保護コストのバランスをとる必要があります。強力な登録保護手段は、多くの場合、ブランド エクイティ保護を補完するものとして提供されています。強力な登録保護手段は、おそらくはオプトイン サービスまたは「無料」あるいはその両方として提供される基本登録サービスへの付加サービスとして提供され、悪用または誤用の結果利用可能性が失われる可能性を低減するためにセキュリティ手段に投資する意志を持つ組織に、望ましいセキュリティ機能を提供します。

ブランドについて懸念のない組織は、リスク評価および資産管理においてドメイン名を考慮に入れる必要があるか？

はい。SSAC のレポートでは、ドメイン名がハイジャックされた場合に、金銭的損失、困惑および評判の低下を含め、レジストラントが悪影響を被ることを説明してきました。[25] また、SSAC レポートでは、ドメイン名の不更新に関連する問題および、DNS ネーム サーバーに関連付けられたドメイン名の不更新によって引き起こされる問題についても説明しています。[26] 特に、SAC010 では、「ドメイン名がブローカーまたは直接売買を通じて市場価値を持つ資産であり、経常的な収益を生み出すものであると認識する必要がある」こと、および、「自発的または意図せずに登録ドメイン名を更新しないレジストラントは、すべてのドメイン名が何らかの価値を持っており、新規レジストラントが、失効したドメイン名を、以前のレジストラントにとって有害と判断される方法で使用する可能性があることを認識する必要がある」[27] と述べられています。

ドメイン名を資産として取り扱う組織のリスク管理を支援し、ドメイン名への投資および依存に対する脅威を低減するために提供可能な保護手段とは何か？

他のインターネット ビジネス セグメント（金融、耐久財の電子商店など）で使用されている特定の手段は、登録サービスの保護にも有用であり、実際に適用可能な場合があります。特定の手段について考慮する前に、また、特にレジストラントの利益のために、第一原理を再検討することが重要です。特に、大規模な組織で使用されている資産、供給およびリスク管理フレームワークをどのような方法でドメイン名登録に適用するか？ドメイン名登録を資産として見なす理由は何か？

以前の SSAC レポートでは、ドメイン名は、それによって主体（商店、金融または教育機関、営利または非営利事業または企業、個人または製品など）が認識されたり、インターネット上でビジネスが行われる識別子であると説明されています。これは、企業がその DBA（事業経営中）として登録した名前、有名人、著作者、著名政治家またはその他の個人の名前と同じ名前にすることができます。個人および組織は名前（ブランド、サービスマーク、商標）を現実世界で資産として扱っており、それらを誤用から保護する手段を講じています（会社定款、特許、著作権など）。ドメイン名は組織のブランド、サービスマーク、商標などと同じことが多いため、レジストラントは、そのような名称を登録するだけではなく、悪用または誤用を防ぐような手段を講じて保護する必要があります。

---

25 SAC007: Domain Name Hijacking Report (12 July 2005) http://www.icann.org/announcements/hijacking-report-12jul05.pdf

26 SAC011: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006) http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf

27 SAC010: Renewal Considerations for Domain Name Registrants (29 June 2006) http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

ドメイン名登録により、レジストラントが更新料金を支払い続け、契約上の義務（受け入れ可能な使用、登録の正確さなど）を果たし続ける限りにおいて、ドメインのグローバルな一意性が確保され、ドメインがレジストラントに結びつけられます。したがって、これは、資産、リスクおよび提供など、その他のネットワーク管理原則と同等のものです。

ドメイン名は、ユーザー フレンドリーな識別子でもあり、DNS を使用して解決され、ドメイン向けにサービス（Web、メール、ソーシャル ネットワーク、音声通信など）を提供するホストのインターネット アドレスが特定されます。ドメインの運用上の価値、特に、名前解決の可用性が高く、ドメインに含まれる名前の意図したとおりの解決が保証されることは、ほとんどの組織にとって計り知れない重要性を持ちます。

たとえば、資産およびリスク管理プログラムに関して、下記のことが可能です：

- 資産の価値を特定する（有形または無形）
- 価値が脅かされる（喪失、盗難、誤用）方法をリストアップする
- 脅威が実現される方法を特定する（ドメイン名を攻撃または悪用に対して脆弱にするものは何か？）
- それぞれの脅威がもたらす可能性またはリスクを特定する
- リスクを軽減可能な方法を特定する
- リスクを受容可能なリスクおよびコスト水準まで軽減するコストを特定する
- 適切な予算を特定し、リスク軽減を実現する

ドメイン名が資産であるならば、その他の在庫、有価または秘密資産と同様の厳格さが求められます。このような観点から、ドメイン名登録管理には、大規模ネットワークの管理提供と共通する特徴が多数存在します。たとえば、提供およびドメイン名管理の基本的な運用は {add, drop, change} です。管理の提供に適用されるベスト プラクティスでは、そのような運用が、許可された当事者によって、タイムリーかつ監査可能な方法で、省略、侵入またはエラーの可能性を低く抑えつつ、適切な順序で行われることが求められます。そのようなベスト プラクティスをドメイン名登録管理 にも拡張し、登録サービスが同様のベスト プラクティスを満たすよう努める必要があります。

組織にとって、ドメイン名登録を保護するセキュリティ手段は、組織がビジネス上重要であると判断するイントラネット、リモート データベースおよびその他のアプリケーション アクセスに対して提供されるセキュリティ手段と同程度に重要であるべきです。ドメイン名登録管理における省略、侵入またはエラーの可能性を最小限に抑えるため、ドメイン名登録に資産価値を見いだす顧客は、ビジネス上重要なその他のアプリケーションに実装されているサービスと同様の認証、許可および監査サービスを求めなくてはなりません。これらの手段のいくつかは、顧客による実装が可能です。その他の手段については、追加のセキュリティ手段を提供することで競争の厳しい市場において差別化が可能になる

と判断したレジストラが登録サービスに組み込むことができます。次のセクションでは、これらの手段についてもう少し詳しく考察します。

ドメイン アカウントおよび DNS ハイジャックを防ぐ手段

このセクションでは、現在、特定のレジストラによって、広範なサービスの一部として、オンライン評判（ブランド エクイティ）保護と組み合わせて提供されることが多い手段について説明します。次に、レジストラによる提供が可能であり、2008 年のインシデントについての SSAC の検討中に聞き取り調査の対象となった当事者によって、望ましいまたは重要であると特定された手段について説明します。最後に、リモート アプリケーション アクセスのセキュリティ確保に大企業が使用している手段および、金融機関および電子商店が顧客アカウントを保護するために提供している手段について考察します。個別のオプトイン サービスまたはサービス バンドルのいずれとして提供されている場合であっても、これらの手段は、ドメイン アカウントの悪用または誤用のリスクを低減する保護手段への投資誘因および投資意志を持つ顧客にとって、ドメイン登録アカウントのセキュリティを向上させるでしょう。レジストラには、これらの手段を提供することにより、競争の厳しい市場において機会の創造または差別化が実現されるかどうか考察することが推奨されます。

顧客（レジストラント）は、ドメイン名の保護において重要な役割を果たしています。このセクションでは、（a）ドメイン登録の作成および更新に関連するレジストラント-レジストラ ワークフローにおける役割を確認し、（b）連絡先および構成情報のメンテナンスおよび変更プロセスを確認するために、顧客が実施可能かつ実施すべき特定の補完的手段について簡単に説明します。レジストラは、既存または新規の FAQ（よくある質問）やその他の手段を通じて、特に重要なドメイン プロファイルを保有する顧客に対して、そのような手段を推奨することができます。たとえば、レジストラは、このレポートについて顧客に通知し、顧客がこのレポートを入手できるようにして、このレポートを一読するようにし、ドメイン名ポートフォリオに対する最も重大な脅威と感じるリスクを軽減するために必要と思われる手段を実装するよう推奨することができます。

SSAC では、ドメイン登録保護の要求を満たすサービス提供が採用される可能性がますます高まっており、中小組織のイニシアチブおよび独立した実装を単純に足し合わせたよりも包括的なものになると考えます。この主張の根拠として、 UTM（統合脅威管理）セキュリティ デバイスの成功が挙げられます。 UTM とは、ファイアウォール、スパム対策、ウィルス対策およびその他のセキュリティ サービスをバンドルしたセキュリティ システムです。UTM は広く普及しつつあり、中小企業（SMB）セグメントの市場では、単一のセキュリティ機能を提供するセキュリティ システムを組み合わせて最適化したシステムよりも成功を収めています。SSAC では、SMB 向けのドメイン登録においては、追加的セキュリティ サービスの提供が、UTM の実績が示すような影響を持ちうると考えます。

ドメイン ポートフォリオへのアクセスの保護

このセクションで説明する手段は、レジストラまたはレジストラのオンライン（Web）ユーザー インターフェース、ヘルプ デスクおよびカスタマー ケア電話サービスを通じた顧客のドメイン名アカウントへの不正アクセスを防止するためのものです。

登録の検証。大容量のトランザクション速度およびドメイン名の迅速な提供に最適化された登録モデルは、多くの場合、レジストラントが主張通りの人物・組織であり、支払いにおいて詐欺または犯罪が行われないことを検証するためには最適化されていません。フィッシング対策に関する研究、[28、29] ボットネット（Srizbi、Conficker）および Fast-Flux 型攻撃ネットワーク対策の経験から、ドメイン アカウントが犯罪活動の重要なリソースであり、今後もそうあり続けることは明らかです。登録時にレジストラントによって送信された連絡先情報を検証し、連絡先情報が変更されるたびに検証することにより、偽装およびドメインの悪用を低減することができます。レジストラには、電子メールによる登録検証の提供を考慮することが推奨されます。ドメイン登録は、レジストラの送信したアクティベーション電子メールに埋め込まれたハイパーリンク先にレジストラントがアクセスし、電子メール アドレスを確認した時点で完了するようにします。追加の手段として、一部の金融機関では、電子メールではなく、顧客から送信さ れた電話番号に電話をかけています。この会社では、顧客に電話で確認番号を通知し、顧客が Web フォームにこの番号を入力することでアカウントのアクティベーションまたはトランザクションの許可が行われるようにしています。SSAC では、この種の手段により登録の処理および製品の提供（登録ドメイン名の登録および名前解決）に遅延が生じることを認識していますが、レジストラに対して、顧客のみならずインターネット コミュニティ全体の利益のために悪用を低減する価値に照らして、そのような不利益を評価することを推奨します。インターネットの名前システムのセキュリティを確保するために積極的な姿勢を示すことにより、肯定的な評判が蓄積し、そのような姿勢を示さないレジストラと比較して、セキュリティ専門家および会社の同僚などによる推奨を受けやすくなるという付加的メリットもあります。

パスワード ベースの認証システムの改善。レジストラの間で主流の認証方法は、単純なユーザー名およびパスワードを使用するものです。レジストラは、パスワードの最小長、最大寿命または複雑さについての確認を導入することを義務付けられておらず、不正なログイン試行の回数制限による総当たり推測攻撃に対する保護を行っていない可能性があります。一般に受容されたベスト セキュリティ プラクティスでは、パスワード ベースのすべての認証システムにこれらの手段を導入することが推奨されています。

---

28 APWG Phishing Activity Trends Report, 2nd Half 2008,
http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

29 Global Phishing Survey: Domain Name Use and Trends in 2H2008
http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

システム登録。電子商店および金融機関は、現在では、顧客がアカウントを管理するパソコン（PC）または IP アドレスを登録できるようにすることにより、改善されたパスワード システムを補完しています。

多要素認証。電子商店、金融機関はもちろん、オンライン（ロールプレイ）ゲーム運営会社までもが、アカウント ログイン時に顧客の識別情報を検証するための 2 つめの*要素*としてハードウェア トークン認証のオプションを顧客に提供しています。トークンによって、パスワードが表す「ユーザーが知っていること」の情報に、「ユーザーが持っているもの」という要素が追加されます。この二要素認証によって、攻撃者によるドメイン アカウントの破壊がより困難になります。攻撃者がアカウント ログインおよびパスワードを推測または入手した場合であっても、さらにトークンを入手しなくてはなりません。今日では二要素認証が多数実装されており、この技術は多くの顧客によって評価されています。SSAC では、VeriSign が ICANN のレジストリ サービス評価プロセス（RSEP）を通じてレジストリ-レジストラ二要素認証サービスの提案を送付したことを認識しています。この提案では、レジストラによる自主的なオプション サービスとして、「更新、移転および/または削除リクエストの処理に現在使用 されているユーザー名およびパスワードにダイナミックなパス コードを追加する」ことが要求されています。[30] VeriSign の提案するロールアウトの第一段階では、レジストリおよびレジストラ間に二要素認証が追加されます。第二段階では、レジストラントがレジストラに要求した場合はこのサービスが提供されるようにします。また、レ ジストラからレジストリへの EPP（Extensible Provisioning Protocol）通信においては、ワン タイム パスワードが導入されます。 SSAC では、各レジストラがこの提案を一読し、その実践によって得られるメリットについて考察することを推奨します。ここで説明した二 要素認証について考察することに加え、SSAC では、レジストラに対して、米国商務省標準技術局（NIST）の電子認証ガイドラインなどのアカウント認証方法およびガイドラインを考慮に入れることを推奨します。[31]

チャレンジ システム。一部の金融機関では、アカウント設定時に個人を識別する一群の質問に対する回答を収集しています。これらの機関では、これらの質問群からランダムにサブセットを選択し、ログイン試行をするユーザーに質問への回答を求めて「誰何」します。秘密のイメージ キャプション ペアを使用してユーザーを誰何する機関もあります。顧客は、アカウントへの初回ログイン時に秘密のイメージを選択するよう求められます。次に、イメージ キャプションを送信します。検証プロセスで、顧客は、パスワードを入力する前にイメージのキャプションを提供するよう求められます。レジストラには、ドメ

---

[30] VeriSign Registry-Registrar Two-Factor Authentication Service http://www.icann.org/en/registries/rsep/

[31] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

イン名の保護および DNS 構成の悪用防止のためのコストと利便性を比較して追加の誰何を受け入れる顧客に対して、この セキュリティ手段をオプトイン サービスとして提供することが推奨されます。

ドメイン別アクセス コントロール。ドメイン登録アカウントへのアクセスによって、当該アカウントの下で登録されているすべてのドメインへのアクセスが、ユーザーおよび攻撃者に同様に提供されます。一般に使用されている登録アカウント アクセス コントロール モデルは、実社会におけるキャビネット モデル貸金庫に相当します。この種の金庫を開くと、大方のことを望み通りにすることができます。これを、多数の貸金庫を備えた金庫室と比較しましょう。ここでは、顧客または侵入者は金庫室の鍵だけではなく、個別の貸金庫の鍵も入手しなくてはなりません。レジストラには、より高水準の保護を求める顧客に同様のアクセス モデルを提供することが推奨されます。たとえば、オプトイン機能を使用して、連絡先および DNS 構成情報の変更、ドメイン移転の開始または許可を行うことができる連絡先を顧客がコントロールできるようにします。

複数、一意の連絡先。ドメイン登録レコードにおいて正確な連絡先情報を維持することは、組織にメリットをもたらします。一部の組織では、必要な各々の連絡先を組織内で一意の個人または役職にすることからもメリットを得ています。これにより、インサイダーが従業員または従業員の顧客のドメイン名の所有権を主張したり、ハイジャックを試みるリスクが分散されます。SSAC では、インサイダーによるドメイン名の悪用を防ぎたいレジストラントにこれらの手段を推奨します。これらの手段は、レジストラントの代理で連絡先情報を管理するレジストラにとって機会をもたらします。たとえば、レジストラは、優先される通信手段（電子メール）について、オプトイン サービス機能として一意の連絡先情報を確認および要求することができます。レジストラントおよびレジストラは、一意の連絡先を使用して、「粒状化」された権限モデルを作成することができます。たとえば、レジストラントの連絡先のみにドメイン移転を許可する組織や、技術用の連絡先のみに DNS 構成の変更を許可する組織があります（そのほかにもモデルは存在しますが、ここでは説明目的でのみ言及します）。レジストラは、これらの手段をインタラクティブな確認または複数受信者通知プロセスなどの手段と組み合わせることにより、レジストラントに対してこれらの手段を推奨することができます。

変更通知または確認。一部の組織では、特定のアクションには複数の当事者の確認を要求するワークフローを作成することにより、不正または過誤による変更を防いでいます。複数確認により、偽装に対する組織の防御が改善されます。攻撃者は、1 人だけではなく、2 人に対してソーシャル エンジニアリングまたは偽装 を行わなくてはならなくなります。レジストラが複数、一意の連絡先を確認および要求するサービスへの加入に関心を示す組織もあるでしょう。それにより、そのような組織は、連絡先、ドメイン移転または DNS 構成の変更に対する保護として内 部で導入している同種のワ ークフローを拡張することができます。そのようなワークフローを持っていない組織に対しては、レジストラが、顧客の代わりにそのようなワークフ ローを可能にするオプション サービスを提供す

ることができます。たとえば、初回登録時には、レジストラの変更確認サービスでは、顧客がドメインに関連して要求される連絡先毎に一意の連絡先を送信したかどうか確認することはできません。DNS 構成の変更リクエスト時に通知する連絡先を選択させたり、一方の当事者による変更リクエストを実行する前に、技術および管理用の連絡先の両方に電話または電子メールによる応答を要求することもできません。また、変更通知は、報復的または便宜主義的なドメイン移転を防ぐ一助となります。たとえば、連絡先に指定された従業員が組織を退職し、組織が連絡先をこの従業員からその後任者に変更しなかった場合について考察します。退職した従業員が何らかの不満を抱えていた場合は、ドメイン移転を通じてドメインの所有権を主張するかもしれません。変更確認のシナリオでは、他の連絡先が移転を確認する必要があるため、移転の試みは阻止されます。

複数受信者通知。レジストラは、顧客との通信に日常的に電子メールを使用しています。SAC028「Registrar Impersonation Phishing Attacks（レジストラ偽装フィッシング攻撃）」では、下記のものを含む一般的な通信がいくつか示されています。

- ドメイン名更新通知
- ドメイン名注文確認
- 登録リクエスト確認
- ドメイン連絡先および DNS 情報への変更
- WHOIS データの訂正・確認通知
- ドメイン名の期限切れまたはキャンセル通知
- （新）サービスおよび機能のプロモーション、広告

このような通信を複数の受信者に送信するオプションによって、いくつかの方法によって顧客を支援することができます。たとえば、顧客はレジストラ偽装フィッシング攻撃の被害を避けたいと考えています。顧客の受信者の 1 人がフィッシング電子メールにだまされた場合でも、別の受信者が偽の電子メールを認識すれば、レジストラおよび組織内の他の連絡先に警告することができます。同様に、レジストラがドメイン名更新を複数の受信者に通知した場合は、顧客の過誤または見落としによる登録失効に対する保護措置となります。たとえば、更新通知の受信者が 1 人だけで、この受信者が長期休暇のために電子メールを受信できない場合には、更新が失効してしまう可能性があります。複数受信者のシナリオでは、他の受信者が更新通知を受信するため、このような登録の失効は回避されます。レジストラは、金融機関が顧客によるアカウントへの不正アクセスの特定を支援するために使用している手段についても考慮することができます。レジストラがオリジナルおよび変更されたバージョンの連絡先情報の両方に通知または確認を送付することにより、変更が意図されたものまたは不正に送信されたもののいずれであっても、また、通知が変更の適用の前後いずれに送信された場合であっても、通信が正しい宛先に届く可能性が高まります。

複数の方法による重要な通信の配送。レジストラは、顧客との通信手段として電子メールに全面的に依存するのではなく、追加の保護を求める顧客に対して、重要な通知を電話、ファックス、郵便または宅配便で配送することができます。このようなサービスにより、攻撃者による不正な移転が非常に困難になります。非常に重要なドメイン名を「恒久的」に更新し続けることを望む顧客は、このような保護措置を歓迎するでしょう（また、通常の通信には影響はありません）。非常に重要なドメインの移転を実行する顧客も、リスク・便益分析の後に、移転「トランザクション」に生じる遅延が受容可能であると判断する可能性があります。

顧客にとっての魅力を高める。多くの大組織は、インターネット アクセス、セキュリティおよびネットワーク管理のアウトソーシングに慣れています。中小企業の間でも管理サービスの人気が高まっています。管理サービス プロバイダ（MSP）は、顧客とプロバイダのパートナーシップを推進しています。FAQ、認知度プログラムおよびウェビナーやポッドキャストを通じた情報提供を通じて、 MSP は、顧客が MSP の提供するサービスを最大限活用する方法について説明しています。上述の手段を補足するものとして、レジストラは、レジストラへの情報提供を通じて下記のことを推奨することができます：

- 複数ドメイン アカウント連絡先の特定
- 従業員リソース管理プロセスに連絡先情報の管理を含めることにより、退職した従業員の証明情報が取り消された場合に、該当する従業員に関連するすべてのドメイン登録連絡先情報も確実に変更されるようにします。
- パスワード変更ポリシーの導入。
- 連絡先の定期的な検証。
- ドメイン名登録の予防的モニタリング。
- すべての登録連絡先について、登録ドメイン名とは異なるドメインから電子メールアドレスを割り当てます。（レジストラントは、追加の保護措置として、複数のドメイン登録アカウントの作成を希望する場合があります。）
- 移転試行をセキュリティ イベントとして処理（確認および再確認）。
- 登録連絡先電子メール アカウントに、他のビジネス目的に使用されているドメインとは異なるドメインを使用します。たとえば、 example.info の連絡先用の電子メール アドレスとして、example.net からのアドレスを割り当てます。
- 役割アカウントの作成：domainadmincontact@example.com、domainregistrantcontact@example.biz 、 domaintechnicalcontact@example.net など。（役割アカウントを使用する場合は、レジストラントのスタッフによる役割アカウ

ントのモニタリングが、組織内の人事、管理または運用上の変更に起因する中断無しに確実に実行されるようにするため、そのようなアカウントを定期的に確認することを強く推奨します。）

- 役割アカウントへの通知用に複数受信者の別名を作成します。この種のメールの増加により、重要なレジストラ通信の「じゅうたん爆撃的な配送」が実現され、通信がタイムリーに受信および処理される可能性が高まります。

顧客への情報提供。レジストラは、提供するセキュリティ手段の種類を、他の競争的提供と同程度に明示するよう努めなくてはなりません。たとえば、運用について独立監査人による日常的なセキュリティ監査を受け、監査に通過したレジストラは、自ら課した規律に対して世間の注目を集める可能性があります。または、 ICANN とレジストラが共同で独立監査人を指定し、監査人と契約を締結して、規定されたセキュリティ手段群を定義することができます。レジストラは、監査人に対して、運用についての監査を行うよう*自発的に*要請することができます。監査に通過したレジストラは、何らかの形式のトラスト マークまたはシールによって、セキュリティ ベンチマークを満たしているレジストラとして高い評価を得られる可能性があります。同様なプログラムは、 SSL 証明書発行機関を通じて利用することができます。[32、33] SSAC では、クレジット カードの処理は各レジストラに共通しており、データ セキュリティ基準を遵守する商店およびサービス プロバイダ向けの支払いカード業界セキュリティ監査手順が、レジストラにも適用可能であると認識しています。[34]

以前の SSAC レポートにおける推奨手段。多くのレジストラによって、SAC007「Domain Name Hijacking Report - *Steps registrars can take to protect domain names*（ドメイン名ハイジャックに関するレポート - ドメイン名保護のためにレジストラが講じうる手順）」のセクション 5.2 で推奨される手段の一部またはすべてが導入されています。ここでは、最近新しく推奨された手段について説明するために、以前に紹介された手段の概要を示します。

1. 登録ドメイン名毎に、一意の EPP authInfo コード値を使用します（ドメイン登録アカウント毎にではなく）。一部のレジストラでは、同一のレジストラントが保有するすべてのドメインについて、1 つの EPP authInfo コード値を使用しています。この慣行では、1 つのコードに基づくハイジャックに対して、顧客が登録したすべてのドメイン名が開示されます。

---

[32] Thawte Site Seal, https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile

[33] VeriSign Secured Seal®, http://www.verisign.com/ssl/secured-seal/

[34] PCI Security Standards Council, https://www.pcisecuritystandards.org/

2. すべてのレジストラについて、ドメイン　ロックのデフォルト設定を統一します。多くのレジストラでは、すでにドメイン名が自動的にロックされます。レジストラは、検証されたドメイン名レジストラントからの正規の移転リクエストを不当に拒否しないようにするため、ドメイン　ロックを解除する十分に直接的な手段を提供しなくてはなりません。

3. レジストラントのレコードの正確性を高めるために、追加の手段を調査します。通信の頻度を上げたり、通信の形態を変更することにより（電子メールの代わりに電話を使用するなど）、レジストラントが情報を最新の状態に保つよう促し、登録の悪用を検出します。

4. 緊急のドメイン名インシデント回復への対応に適した当事者を支援するために、レジストラント、レジストラおよび再販業者から緊急時連絡先情報を収集します。[35] 緊急時連絡先が使用できない場合に、すべての当事者が同意する上申プロセス（緊急手順）を定義し、制定することができます。

5. すべてのレジストラ ビジネス プロセスで使用されている認証および許可を改善する手段について考慮します。

6. 詐欺および偽装やドメイン名の窃盗に利用可能なレジストラントの情報を保護します。レジストラントの認証プロセスに使用される情報は、すべてデフォルトで秘密扱いにします。これらの情報の取り扱いに、クレジット　カードまたはその他の金融情報の保護に使用する手段と同一または同様の手段を使用することを考慮します。

7. 記録保管要件に対する再販業者の遵守状況を改善します。

8. 再販業者にレジストラ（および ICANN）の記録保管要件について理解させ、これらの要件に対する遵守状況を改善します。

9. ドメイン ロックおよびレジストラが提供するドメイン名保護手段について、明確かつ容易に入手可能な情報をレジストラントに提供します。

DNS 構成情報の悪用防止

ドメイン登録アカウントへの不正アクセスを取得する目的のひとつは、組織の名前解決サービスに対するコントロールを取得することにあります。攻撃者は標的となったネームサーバーの名前または IP アドレスを変更し、攻撃者の運用するシステムをポイントするようにします。このシステムは、攻撃者が事前にセキュリティを破壊したコンピュータであることが一般的です。攻撃者は、セキュリティが破壊されたコンピュータ上で、攻撃対象のドメイン名用の DNS サーバーおよびゾーン ファイルをホスティングします。攻撃

---

[35] SAC 038, Registrar Abuse Contacts, http://www.icann.org/committees/security/sac038.pdf も参照

者の DNS サーバーは、攻撃対象のドメインからの名前を解決し、悪意のある Web サイトまたは標的の評判をおとしめる Web サイトにリダイレクトします(このレポートおよび SAC007 で説明した Comcast、ICANN、Panix および Hush Communications のインシデントの場合と同様)。悪意を持って DNS 構成情報を変更するわけではない攻撃者も存在します。これらの攻撃者は、セキュリティが破壊されたドメイン登録アカウントを使用して、自身の所有するネーム サーバーを正当に運用されているネーム サーバーのリストに追加します。これにより、Fast-Flux 型攻撃[36] の *double flux* バリアントで使用するネーム サーバーを秘匿するとともに、テイクダ ウンを妨害することができます。これらにより、フィッシング、スパム、詐欺または犯罪的攻撃の期間が延長されます。

前のセクションで説明した手段は、DNS 構成情報を悪意を持って変更または密かに追加する目的での、顧客のドメイン名アカウントの不正使用を防止するために適用することができます。特に、レジストラによってオプション サービスとして提供されるか、レジストラントによって実行される下記の手段は、 DNS 構成攻撃に対する重要な保護措置となります。

- DNS 構成の変更時に多要素認証を要求します。
- 電子メールを使用して、複数の連絡先に変更の確認を要求します。可能であれば、電子メール以外の手段を使用します。（注：先述した同種の多段階検証手段をここに適用することができます。）
- 変更の実行時に複数の連絡先に通知を行います。
- DNS の変更をモニタリングし、異常または悪用を発見します。

ここでも、レジストラは、FAQ、トレーニングおよび情報提供を通じて、DNS 構成アクティビティ（変更および追加）を日常的にモニタリングするよう顧客に推奨しなくてはなりません。レジストラは、ドメイン内の名前が意図された IP アドレスに解決されることを確認することも顧客に推奨しなくてはなりません。また、レジストラは、すべてのドメインについて DNS 構成の履歴を保持するよう顧客に促し、これらの情報にタイムスタンプおよびデジタル署名を適用する重要性について顧客の理解を促進しなくてはなりません。

---

[36] SAC 025 Fast Flux Hosting and DNS, http://www.icann.org/committees/security/sac025.pdf

結論

このレポートにおけるインシデントおよび関連調査から、SSAC では、下記の追加的結論を得ました。

結論 (1) 攻撃に対する脆弱性および、ドメイン アカウントへの攻撃に対して提供する保護の程度に関して、レジストラの間に差異が存在します。多くのドメイン レジストラントは、攻撃からドメイン アカウントを保護し、DNS 構成の悪意のある変更を防止するためにレジストラが提供可能な保護の水準を評価する上で十分な情報を持っていないと思われます。

結論 (2) 顧客重視のドメイン名登録サービスを提供す るレジストラが多数存在する一方で、注目度の高い、標的となる可能性が高いドメイン名所有者にセキュリティ サービスを提供するレジストラおよび「ブランド管理」組織も少数存在します（このようなセキュリティ サービスは、一般的に、包括的なブランド エクイティ保護サービスの一環として提供されます）。SSAC では、顧客によるレジストラ選択の意志決定において、セキュリティ手段の評価が本来果たすべき重要な役割を果たしていないことも一因となって、*「セキュリティ確保に特化した」登録サービス プロバイダ*が少数にとどまっていると認識しています。

結論 (3) レジストラがセキュリティ サービスに関する情報提供を増やすことにより、顧客による十分な情報に基づく意志決定が可能となります。運営について自発的に独立監査人による監査を受け、適正な監査結果を公表することにより、コストおよびその他の付随的な機能（Web および DNS ホスティングなど）はもちろん、セキュリティ要件に基づいて顧客がレジストラを選択することができるようになります。

結論 (4) レジストラ サービス（およびレジストラント）は、アカウントへのログインに対する一要素認証について、この方法が値する以上の信頼を置いています。この認証手段は、さまざまな形態のソーシャル エンジニアリング、総当たり攻撃およびその他の手法を使用して、再三回避されています。

結論 (5) ドメイン登録アカウントのセキュリティ破壊に成功した攻撃者は、DNS 構成を標的にします。DNS が分散型であるという性質のため、DNS 構成情報が変更された影響は、レジストラによる復旧および影響を軽減する措置の実施後も続きます。変更された DNS リソース レコードに関連する TTL 値の全期間を通じて、悪意のあるまたは不正確な DNS 情報がインターネットの全域に残存する可能性があります。攻撃者は、特にこの目的のために TTL を変更する場合があります。

結論 (6) 一般的に、登録アカウント ポータルまたはログインにおいてユーザーが認証されると、ユーザー（またはユーザーの詐称者）に*グローバル*な権限が割り当てられ、連絡先情報はもちろん、DNS 構成情報も変更できるようになります。オプション サービスとして「粒状化」されたアクセス コントロールを顧客に提供することにより、特に、連絡先および DNS 構成情報の変更および移転の許可について各々の連絡先が実行可能なアクションのタイプを制限する機能を通じて、ドメイン名およびドメイン名に関連する名前解決サービスの悪用または誤用のリスクを低減することができます。

結論 (7) 登録サービス プロバイダは、セキュリティ関連の通知（変更通知など）の配信について、電子メール配信保証およびセキュリティ機能のメリット以上に、確認の取れない電子メールに大きく依存しています。この通信手段は、セキュリティが破壊された登録アカウントを通じてドメインの DNS 構成が変更された場合には、電子メール配信を妨害することにより、攻撃者によってしばしば無効化されています。顧客に代替的な連絡手段を提供するか、通知サービスを拡張して何らかの形式の受信確認を導入することにより、ドメイン名およびドメイン名に関連する名前解決サービスの悪用または誤用のリスクを低減することができます。

推奨案

SAC007 におけるレジストラ向けの特定の推奨案として、特に下記のものを挙げます。

推奨案 SAC007-(8)：*レジストラは、ドメイン名ハイジャックおよびレジストラントの偽装および詐欺に対するレジストラントの認知度を向上させ、正確な登録情報を維持することの必要性を強調しなくてはなりません。レジストラは、レジストラ ロックの使用可能性および目的についての情報をレジストラントに提供し、その使用を推奨しなくてはなりません。さらに、レジストラは、許可メカニズム（EPP authInfo）の目的についての情報をレジストラントに提供し、日常的なドメイン名 ステータスのモニタリングおよび、連絡先および認証情報のタイムリーかつ正確なメンテナンスを含め、レジストラントのドメインを保護するための推奨慣行を策定しなくてはなりません。*

最近のインシデントに関する分析、関連調査および上記の結論に基づき、SSAC では、下記の推奨案を作成しました。

推奨案 (1) レジストラには、そのようなサービスを必要とする顧客に対して、ドメイン名登録サービスの悪用または誤用に対するより強力な水準の保護を提供することが推奨されます。このレポートに列挙された手段は、オプション サービスとして、個別またはバンドルして顧客に提供することができます。

推奨案 (2) レジストラは、レジストラに対する既存の FAQ および情報提供プログラムを拡張し、セキュリティに対する認識を含めなくてはなりません。レジストラは、ドメイン登録アカウントを保護するために提供するサービスに関する情報を顧客が容易に入手できるようにすることを通じて、顧客によるレジストラの選択時に、セキュリティ手段に関する十分な情報に基づく意志決定を可能にしなくてはなりません。

推奨案 (3) レジストラは、セキュリティ評価の一環として、運営に対する独立監査人による監査を自発的に受けることの価値を考慮しなくてはなりません。

推奨案 (4) ICANN およびレジストラは、*レジストラの要請を受けて*、規定されたセキュリティ手段群に基づいてセキュリティ監査を行う公認の独立監査人を設けることにより、登録サービスが全般的に改善する可能性および、レジストラントにメリットが生じる可能性について調査しなくてはなりません。ICANN では、このセキュリティ監査のベンチマークを自発的に満たしたレジストラを、当該機関の基準を満たす Web サイト運営者にトラスト マークまたはシールを提供する SSL 証明書発行機関と同様の方法で実施される、信頼性の高いセキュリティ マーク プログラムを通じて区別することができます。

謝辞

SSAC では、本件に関する当委員会の調査に貴重な時間を割き、ご協力およびご評価を賜った下記の皆様に感謝いたします。

Jaap Akkerhuis
KC Claffy
Steve Crocker
Patrik Fältström
Duncan Hart
Jeremy Hitchcock
Rodney Joffe
Warren Kumari
Danny McPherson
Dave Piscitello
Dan Simon
John Schnizlein
Bruce Tonkin
Rick Wesson
Richard Wilhelm

自己紹介

SSAC メンバーの経歴および自己紹介については、下記のサイトをご覧ください：
http://www.icann.org/en/committees/security/biographies.htm

反論

このレポートの発行に反対した委員会メンバーはおりません。