インターネットバンキングに係る不正送金事犯の発生状況等

2015年、インターネットバンキングに係る不正送金事犯による被害額は約30億7,300万円にのぼり、過去最悪となった。被害状況からわかることは、攻撃者はターゲットの弱点を突く、あるいはその対策を踏まえて新たな手法で攻撃をする、さらにはかなりの対策を講じているターゲットに対しても物量戦・持久戦ともいうべき手法で執拗に攻撃を仕掛けてくる、ということである。

インターネットバンキング利用者、サービスを提供する金融機関、そして安全利用のために活動しているセキュリティ関係者、法執行機関は、現状が攻撃に対抗する防衛側の戦いであること、手を緩めれば攻撃側は容赦なくその隙を突いてくることを認識し、対策を講じる必要がある。

本稿では、インターネットバンキングに係る不正送金事犯の現状について、一般財団法人 日本サイバー犯罪対策センター理事の坂 明（さか あきら）氏に解説いただいた。

1. インターネットバンキングに係る不正送金事犯の推移

インターネットバンキングに係る不正送金事犯については、2011年から統計が存在しており、同年の発生件数は165件、被害額は約3億800万円となっている。2012年には被害が減少して発生件数64件、被害額約4,800万円であったが、2013年から被害が急増し、発生件数1,315件、被害額約14億600万円と、前年に比べ桁違いの被害状況となった。以後、2014年は発生件数1,876件、被害額約29億1,000万円、そして、昨年2015年には、発生件数こそ1,495件と減少したものの、被害額は約30億7,300万円と過去最悪の状況となった。

過去3年間のインターネットバンキングに係る不正送金事犯の発生状況は表1のとおりである。

■表1　過去3年間のインターネットバンキングに係る不正送金事犯の発生状況

期間	件数	被害額	実被害額
2015年	1,495件	約30億7,300万円	約26億4,600万円
2014年	1,876件	約29億1,000万円	約24億3,600万円
2013年	1,315件	約14億600万円	約13億3,000万円

※上記発生件数及び被害額については、ウイルスやフィッシングによると認められるものを集計

※被害額……犯人が送金処理を行ったすべての額

※実被害額……「被害額」から金融機関が不正送金を阻止した額を差し引いた実質的な被害額

出典：警視庁「平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について

ちなみに、インターネットバンキングに係る不正送金事犯としては統計がないものの、国家公安委員会・総務大臣・経済産業大臣が連名で発表している「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状況」によると、2010 年以前の不正アクセス後にインターネットバンキングの不正送金が発生した件数は表 2 のとおりである。

■表 2　2010 年以前に起きたインターネットバンキングによる不正送金発生件数

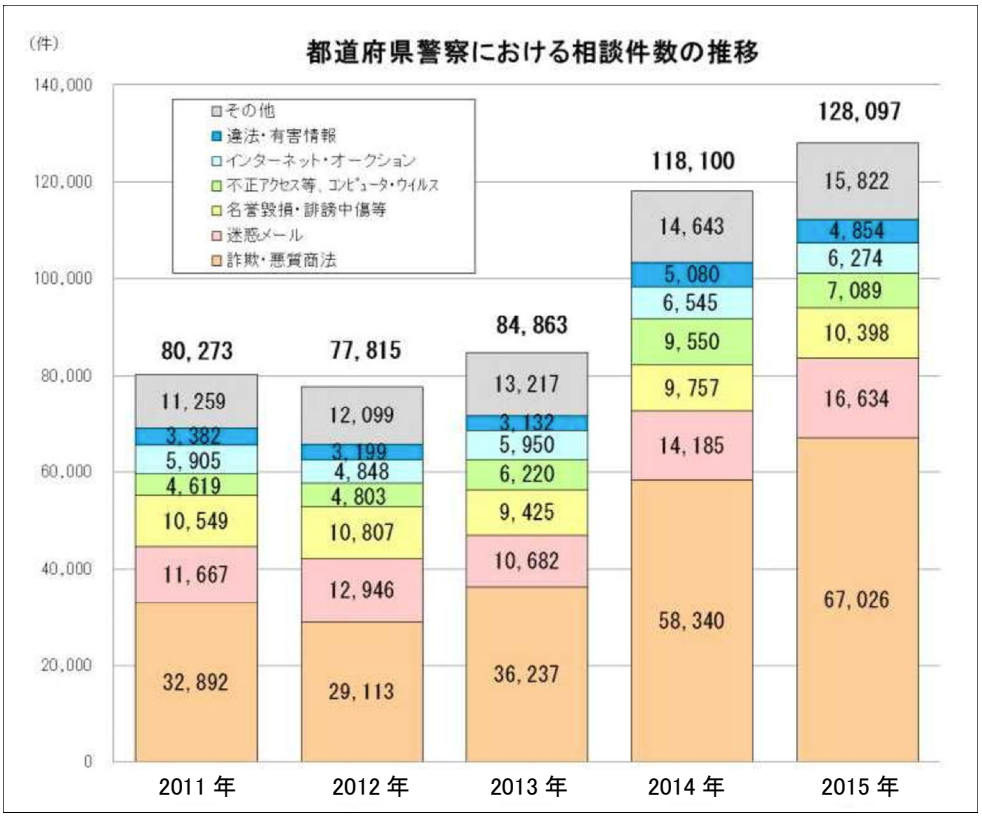
2005 年	2006 年	2007 年	2008 年	2009 年	2010 年
5 件	29 件	113 件	37 件	34 件	22 件

出典：国家公安委員会・総務大臣・経済産業大臣「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状況」をもとに筆者作成

2004 年以前については、このような形での集計は行われていないが、事例の報告が 1 例（インターネットカフェに仕込んだキーロガー[1]で窃取した ID、パスワードによるもの）認められている。2013 年以降になるとインターネットバンキングによる不正送金件数が 1,000 件以上に膨れ上がり、大規模な攻撃がなされるようになった。

都道府県警察におけるサイバー犯罪等に関する相談件数の推移を図 1 に示す。

■図 1　都道府県警察における相談件数の推移



出典：警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」

[1] パソコンのキーボード入力操作を記録するソフトウェア。

これを見ると、「詐欺・悪質商法」に関する相談件数が 2013 年に増加し、2014 年にはさらに 1.5 倍以上に増加していることがわかる。また「不正アクセス等、コンピュータ・ウイルス」についての相談件数も、同じく 1.5 倍以上に増加している。これは、サイバー犯罪に関して、この時期に従前とは次元の異なる攻撃が国内で発生していることに加え、それらの手口が世間に広く知られ、被害を受けた人々にもこうした手段により実被害が生じていることが認識されるようになったためと考えられる。

2. インターネットバンキングに係る不正送金事犯の特徴

(1)被害状況の推移

2015 年に、インターネットバンキングに係る不正送金件数が減少したにもかかわらず、被害額が過去最悪を記録した背景として、法人口座被害の増加がある。特に、信用金庫の法人被害が急増したことが指摘されている。

金融機関別の被害額の推移については、表 3 とおりである。

■表 3　インターネットバンキングによる金融機関別の被害額

金融機関別	2013 年	2014 年	2015 年
都銀等	約 12 億 8,300 万円	約 19 億 500 万円	約 14 億 4,600 万円
地銀	約 1 億 2,300 万円	約 8 億 8,200 万円	約 6 億円
信金・信組	0 円	約 1 億 2,300 万円	約 9 億 4,000 万円
農協・労金	0 円	0 円	約 8,700 万円
合計	約 14 億 600 万円	約 29 億 1,000 万円	約 30 億 7,300 万円

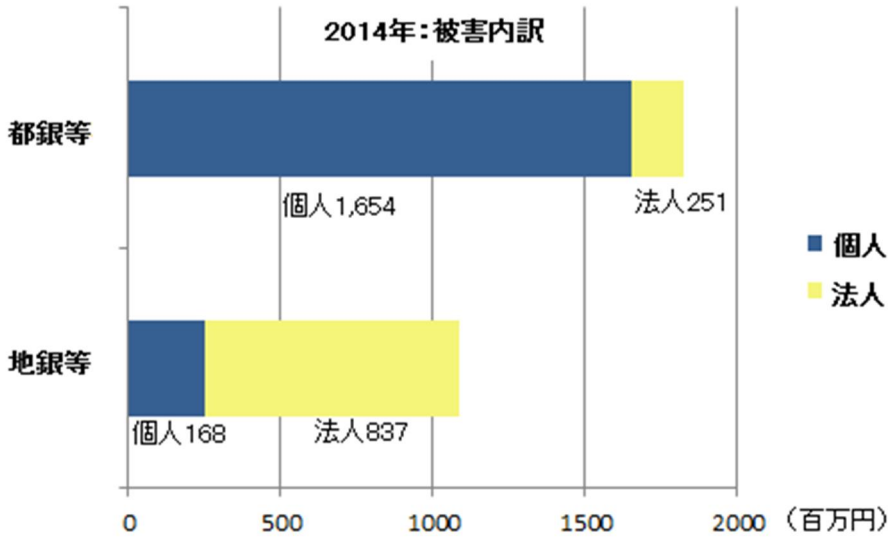
出典：警視庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

このように、2013 年には主に都市銀行（都銀）等が狙われていたが、2014 年には地方銀行（地銀）も攻撃対象となっている。2015 年には信用金庫（信金）・信用組合（信組）が標的となり、さらに農業協同組合（農協）・労働金庫（労金）も狙われるようになった。

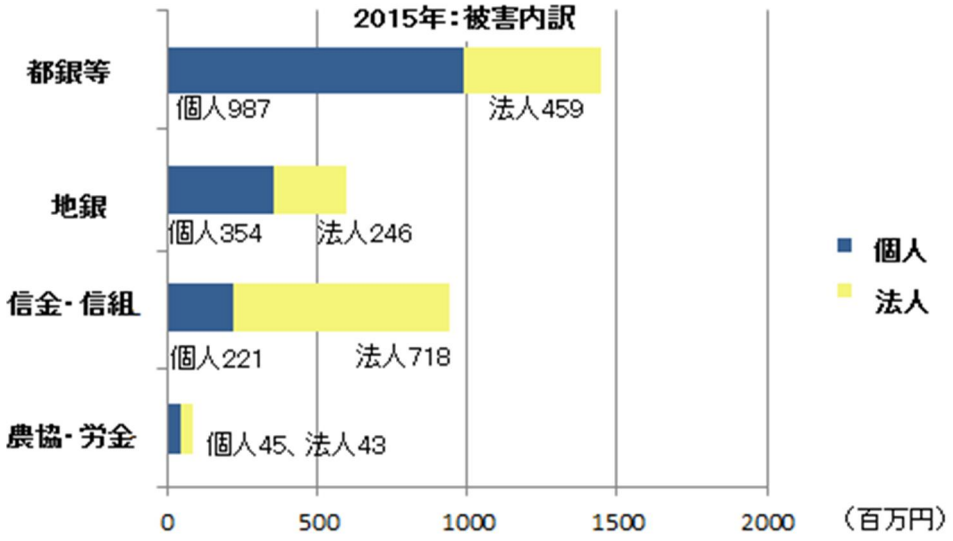
金融機関数から見ても、2013 年には都銀等 12、地銀 20 の計 32 機関が、2015 年には都銀等 16、地銀 53、信金 98、信組 17、農協 35、労金 4 の計 223 機関が被害を受けており、非常に多くの金融機関が標的となっている。

個人・法人口座別にみた被害状況を図 2 に示す。

■図 2　個人および法人講座別にみた被害状況（2014 年・2015 年）



出典：警視庁「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」



出典：警視庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

2013 年における被害口座は、個人名義がほとんどであった。2014 年には、都銀、地銀の法人口座が狙われはじめ、さらに 2015 年には、都銀、地銀の法人口座に加え信金・信組の法人口座が狙われた。また、個人口座も引き続き各金融機関でターゲットとなった。

（2）犯行手法の高度化

2013 年には、コンピュータ・ウイルスで表示された不正な画面に ID・パスワード等を入力させる手口が主となり、同年 11 月以降はメールでフィッシングサイトに誘導する手口が多発した。2014 年には、これに加えて、不正送金処理を自動で行うウイルス等、さらに巧妙な手口が用いられるようになり、2015 年には、スマートフォン等に SMS（ショート・メッセージ・サービス）を送信して偽サイ

トに誘導するフィッシング（スミッシングとも呼ばれる）も発生した。また、不正広告経由のウイルス感染についての指摘もある[2]。

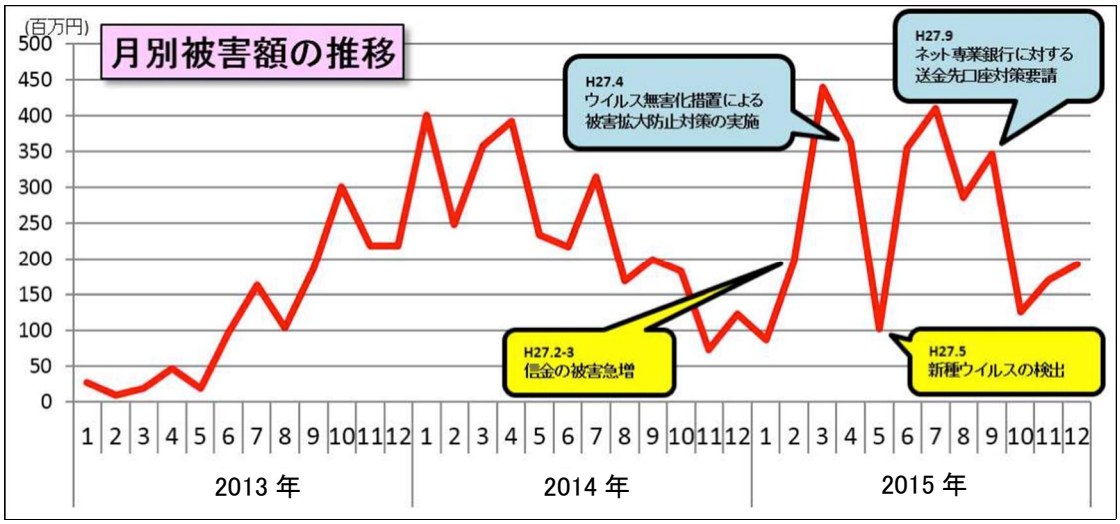
3. インターネットバンキングに係る不正送金事犯への対応

(1)警察による不正送金事犯への取組み

大きな被害が生じているインターネットバンキングに係る不正送金事犯に対しては、関係者によりさまざまな取組みがなされている。

インターネットバンキングに係る不正送金事犯の被害額を図 3 に示す。

■図 3　インターネットバンキングに係る不正送金事案の被害額の推移（月別）



出典：警視庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

月別で見ると、被害額にはかなりの変動があることがわかる。図中にも記載があるが、防御側はウイルス対策、不正送金過程で阻止する等、さまざまな対策を講じている。一方、攻撃側は新たなターゲットへの攻撃、手法の高度化、さらに防御側の対策等を踏まえた攻撃を行ってきている。

このように、攻撃側と防衛側がせめぎあっているのが現在の状況であるが、上記対策を行った 2014 年後半の成果を見れば、防衛側が総力戦で対抗することにより、被害の減少につながることが実証されている。引き続き、防御側が連携して取組みを進める必要がある。

表 4 は、事前に凍結された口座への送金指示に対する送金処理の取り消し、法人サービスにおける当日送金の停止等により、金融機関が不正送金を未然に阻止した内訳である。

[2] トレンドマイクロ「不正広告に日本から 900 万アクセス、金銭狙う攻撃への誘導が日本でも顕著に」2015 年 9 月 2 日、http://blog.trendmicro.co.jp/archives/12174

■表 4　金融機関による不正送金阻止率

	被害額	実被害額	阻止額	阻止率
2013 年下半期	約 11 億 9,300 万円	約 11 億 2,700 万円	約 6,600 万円	5.5%
2014 年上半期	約 18 億 5,100 万円	約 17 億 1,000 万円	約 1 億 4,100 万円	7.6%
2014 年下半期	約 10 億 5,800 万円	約 7 億 2,600 万円	約 3 億 3,200 万円	31.4%
2015 年上半期	約 15 億 4,300 万円	約 13 億 8,300 万円	約 1 億 6,100 万円	10.4%
2015 年下半期	約 15 億 3,000 万円	約 12 億,6400 万円	約 2 億 6,600 万円	17.4%

出典：警視庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

こうした取組みに加え、次のような対策がとられている。

① 金融機関によるワンタイムパスワードの導入等のセキュリティ強化
② 利用者への注意喚起
③ 国際的なボットネットのテイクダウン作戦[3]等の展開
※こうした対策により把握された国内のウイルス感染端末の利用者に対しては、関係のプロバイダ等が注意喚起に尽力
④ 口座売買、不正送金の引出役等の検挙（2014 年には 115 事件 233 人、2015 年には 97 件 160 人を検挙）
⑤ フィッシングメールの送付やウイルスに対する指令送付等に利用される中継サーバを提供する事業者の一斉取り締まり
⑥ 外国捜査機関と連携したウイルス通信先サーバの停止
⑦ セキュリティ事業者によるウイルスへの対応

今後の対応としては、これまでの対策を引き続き展開するとともに、情報共有、新たな脅威への対策を迅速に進め、攻撃者像とその手口を分析して、先制的な措置を講じていくことが望まれる。

（2）インターネットバンキング利用者の状況

2015 年中に発生した不正送金事犯について、口座名義人のセキュリティ対策実施状況を表 5 に示す。

■表 5　口座名義人のセキュリティ対策状況

	利用していた		利用していない		不　明		合　計
ワンタイムパスワード（個人口座）	118	9.7%	916	75.0%	188	15.4%	1,222
電子証明書（法人口座）	47	17.2%	185	67.8%	41	15.0%	273

出典：警視庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

[3] インターネットバンキングに係る不正送金事犯に使用されているとみられる不正プログラム（Game Over Zeus）が世界的に蔓延していることから、米国連邦捜査局（FBI）および欧州刑事警察機構（ユーロポール）が中心となり、我が国の警察を含む協力国の法執行機関が連携し、当該不正プログラムのネットワークを崩壊させる（ボットネットのテイクダウン）作戦を決行している。

これを見ると、ワンタイムパスワード、電子証明書といった不正防止に有効な対策を利用している口座利用者はかなり少ないことがわかる。もちろん、これらの対策を講じていても不正送金被害に遭う可能性はあるが、可能な限りの対策をとり、自らを守るという意識が利用者にも必要である。

(3)事業者が留意するべき事項と対策

一般社団法人 全国銀行協会では、2014 年 7 月 17 日「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方」[4]を申し合わせた。これは、従来個人顧客に対しては金融機関が無過失の場合でも、顧客の責任によらず被害があった場合に補償するとしてきたことに加え[5]、法人の不正送金被害についても各銀行の判断により補償を行うことを明らかにしたものである。ただし、事業者において、適切なセキュリティ対策が講じられていなかったり、不正取引が発生した際に銀行への通報や銀行による調査、警察の捜査への協力等を怠った場合、補償を減額したり補償しないケースもあるとしている。

具体的には、法人の顧客に求められる対策事例として、

① 電子証明書の導入、ワンタイムパスワード等、銀行が導入しているセキュリティ対策の実施

② OS や各種ソフトウェアを最新の状態に更新すること

③ ウェブブラウザを含め、サポート期限の切れたソフトウェアの使用をやめること

④ パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新すること

⑤ インターネットバンキングに係るパスワードを定期的に変更すること

を挙げるとともに、推奨する対策として、

⑥ パソコンの利用目的として、インターネット接続時の利用はインターネット・バンキングに限定すること

⑦ パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断すること

⑧ 取引の申請者と承認者で異なるパソコンを使用すること

⑨ 振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定すること

⑩ 不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認すること

を掲げている。

---

[4] 一般社団法人 全国銀行協会「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方について」平成 26 年 7 月 17 日、http://www.zenginkyo.or.jp/abstract/news/detail/nid/3349/

[5] 一般社団法人 全国銀行協会「預金等の不正な払戻しへの対応について」平成 20 年 2 月 19 日、http://www.zenginkyo.or.jp/abstract/news/detail/nid/2933/
こちらの補償対象は個人顧客であるが、金融機関への速やかな通知、金融機関への十分な説明、捜査当局への被害事実等の事情説明（真摯な協力）が、まず補償要件となっている。補償基準として、預金者無過失の場合は全額補償、過失のある場合は個別判断とされ、親族等による払戻や虚偽説明のあった場合には補償を行わないことなども示されている。

上記申し合わせにおいては、補償が減額される、ないしは行われないこととなるケースとして、次を挙げている。

- 上記①～⑤のセキュリティ対策が実施されていない
- 身に覚えのない残高変更や不正取引が発生した場合に、一定期間内に銀行への通報がなされていない
- 不正取引が発生した場合の一定期間内の警察への通報がなされていない
- 不正取引が発生した場合の、銀行による調査および警察による捜査への協力がなされていない
- 顧客に過失があると考えられる以下のような事象が認められたケース
  - 正当な理由なく、他人に ID・パスワード等を回答してしまった、あるいは安易に乱数表やトークン[6]等を渡してしまった場合
  - パソコンや携帯電話等が盗難に遭った場合において、ID・パスワード等をパソコンや携帯電話等に保存していた場合
  - 銀行が注意喚起しているにもかかわらず、注意喚起された方法でメール型のフィッシングに騙される等、不用意に ID・パスワード等を入力してしまった場合
- その他、上記と同程度の注意義務違反が認められた場合
- 会社関係者の犯行であることが判明した場合

このように、事業者としては、適切なセキュリティ対策を講じることが補償を受け経済的な損失を防ぐうえでも重要であることに留意する必要がある。一般社団法人 全国銀行協会から示されている対策は、いずれも実施する必要性の高いものであり、本章（1）警察による不正送金事犯への取組み で説明したような対策を行っていない事業者が被害に遭っている率が高い。

事業者が上記に挙げたような対策をとる場合、最新の攻撃手法についての情報を把握し、それに対応していくことが重要である。

4. おわりに

攻撃者は常に新たな攻撃手法を開発し、弱い所を狙って攻撃してくる。インターネットバンキングに関しては、取引金融機関からの情報に十分留意し、それに基づいた対策を行うことが基本である。さらに、警察機関や情報セキュリティ関係機関からの情報等は、適宜、入手可能なものであり、こうした情報を、それぞれの事業者に合った形で活用していくことが望ましい。

インターネットバンキングに係る不正行為の対策として挙げているものは、事業者のシステムへの不正侵入による営業秘密や顧客情報の盗取防止対策となるものも含まれており、こうした対策を着実に実行することが事業を守ることになる。また、近時は、ウイルスを送り込み、必要なデータを勝手に暗号化してしまい、解読するために金銭支払いを強制するような事案（ランサムウェア）も発生している。侵入および情報流出を防ぐ対策と合わせて、データのバックアップをとっておく態勢も整備しておくことが肝要である。

[6] 一度しか使用できないワンタイムパスワードを生成する機械。

（参考資料）

① 警察庁「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」平成 26 年 1 月 30 日。インターネットバンキングに係る不正送金事犯については、以後、各年について統計がまとめられており、本稿の数字はそれに基づいている

②国家公安委員会・総務大臣・経済産業大臣「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状況」平成 18 年 2 月 23 日。不正アクセス行為等の禁止に関する法律（平成 11 年 8 月 13 日法律第 128 号、本稿では「不正アクセス禁止法」と略称）が施行された平成 12（2000）年以降の状況についてとりまとめられており、これを参考にした。

【著者紹介】

坂　明　（さか あきら）

一般財団法人 日本サイバー犯罪対策センター 理事

1981 年警察庁に入庁。生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長等を歴任し、サイバー犯罪対策に従事。2002 年ハーバード大学国際問題研究所（WCFIA）客員研究員、2008-2010 年慶應義塾大学政策・メディア研究科教授。2014 年 11 月より現職。

東京海上日動リスクコンサルティング株式会社

TOKIO MARINE NICHIDO

To Be a Good Company

経営企画部 企画ユニット

〒100-0004 東京都千代田区大手町 1-5-1 Tel. 03-5288-6595　Fax. 03-5288-6590

http://www.tokiorisk.co.jp/

