

# 日本情報漏えい年鑑 2015

2014/01/01 ~ 12/31

株式会社イー・ド

## はじめに

情報セキュリティ専門メディアである ScanNetSecurity はこれまで、情報漏えいや Web 改ざん等の、インターネットで発生したさまざまなセキュリティ・インシデントを編纂した資料「ネットワーク・セキュリティ・インシデント年鑑」を2002年から刊行してまいりました。

本レポートは、2014年に国内で発生した多様なセキュリティ・インシデントのうち、個人情報漏えいに関わるインシデントを収録しました。本資料によって、国内で発生した主な個人情報漏えい事故を総覧し、企業や組織が「過去にどのような事件を起こしたか」「そのときどのような対応をしたか」を確認するケーススタディとしてご利用いただけます。

企業と組織の情報セキュリティの推進のために、セキュリティ対策実施と運用の現場でご活用いただけることを願ってやみません。

2015年 9月

株式会社イード

ScanNetSecurity 発行人 高橋潤哉

## 目次

凡例	2
本書の内容について	2
情報漏えいインシデントの分類・整理方法について	2
情報漏えいランキング	5
○2014年 情報漏えい人数 TOP10	5
情報漏洩データ 2014年	6
2014年1月	7
2014年2月	11
2014年3月	14
2014年4月	20
2014年5月	24
2014年6月	29
2014年7月	35
2014年8月	38
2014年9月	40
2014年10月	42
2014年11月	45
2014年12月	47
企業名索引	48

## 凡例

### 本書の内容について

本年鑑は、株式会社イードが、情報セキュリティに関わる最新情報やニュースを配信するオンラインメディア ScanNetSecurity に掲載されたニュース記事から、企業や官公庁等による個人情報漏えいインシデントだけを選び収録した。掲載されたインシデントは、2014年1月1日から2014年12月31日までの1箇年間とした。なお、本年鑑に掲載された情報漏えいインシデントは、編集方針に基づいて ScanNetSecurity に掲載された記事のみを対象としており、2014年に発生し報告された日本国内のすべての事件及び事故を網羅するものではない。

### 情報漏えいインシデントの分類・整理方法について

<b>【ID番号】</b>	
● <b>【タイトル】</b>	
掲載日	<b>【掲載日】</b>
発表日	<b>【発表日】</b>
名称	<b>【名称】</b>
属性	<b>【属性】</b>
漏えい人数	<b>【漏えい人数】</b>
原因	<b>【原因】</b>
	<b>【内部・外部】</b>
<b>【本文】</b>	
・ <b>【関連URL】</b> http://	

#### **【ID番号】**

ScanNetSecurity 掲載日の昇順による ID で、2014年1月～2014年12月の1箇年間連番、A001から順に付与される

#### **【タイトル】**

ScanNetSecurity 掲載時ニュース記事タイトル

**【掲載日】**

ScanNetSecurity 掲載年月日

**【発表日】**

企業等がリリースによってインシデントの発生を公表した年月日あるいはメディア等で公知となった年月日

※インシデントの発生日が公表されている場合「内容」の項目に記載される

**【名称】**

漏えいした個人情報を保有していた企業名、官公庁名、もしくはその他組織・団体名

**【属性】**

漏えいした個人情報を保有していた組織・団体は下記 3 カテゴリである

- 民間企業
- 官公庁
- その他団体(財団法人、NPO、公立ではない大学・病院等)

**【漏えい人数】**

公開資料記載の、漏えいした個人情報の人数

**【原因】**

-不正持ち出し

組織内の規定に反し個人情報を事業所等から持ち出したことが原因の場合(自宅に持ち帰り、個人用の PC にデータを保存し当該 PC が Winny ウイルス等に感染し漏えいした場合、その他本来の利用目的外に個人情報を利用した場合も含む)

-紛失

個人情報の状態(記憶媒体、紙媒体等)を問わず企業等の個人情報が、内外を問わず紛失した場合

-盗難

車上荒らしや事務所荒らし等によって、個人情報を記録、保存した PC や鞆等を盗難された場合

-誤送信ほか操作ミス

個人情報を含むファイルを誤った宛先にメールや FAX で送信したり、本来 BCC にする複数の宛先を CC で誰にでも閲覧できる状態でメール送信する等の誤送信や操作ミス

-不正アクセス

不正侵入のほか、他人のログイン情報悪用等、「不正アクセス行為の禁止等に関する法律」により定義される不正アクセス行為全般

-システム管理上のミス

Web サイトやサーバの設定不備によって第三者が個人情報にアクセスできる状態となっていた場合や、消去すべきデータを消去し忘れた場合、アクセス制限の設定ミス等、第三者が一般的な操作で個人情報を閲覧できる状態にあった場合

-その他

内部犯罪や、社内規定不在により社内 PC に Winny 等をインストールしたことが原因で漏えいが発生した場合、データを消去せずにハードディスクを廃棄した場合等々、上記の項目に該当しない場合

-不明

漏えいの原因や経路等が不明あるいは公表されていない場合や、紛失か盗難かが明確ではない場合等

### 【内部・外部】

-内部から:内部からの攻撃あるいは原因による情報漏えい

-外部から:外部からの攻撃あるいは原因による情報漏えい

-不明:原因不明なもの

### 【内容】

SCAN 掲載ニュース記事本文

### 【関連 URL】

情報漏えいを公表する組織・団体のリリースが掲載された当時の URL で、意図して消されずで当該ページが存在しない場合もある。リリースがトップページに掲載された場合等はトップページの URL を記載した。

## 情報漏えいランキング

○2014年 情報漏えい人数 TOP10

順位	SCAN 掲載日	名称	属性	漏えい人数	原因
1位	2014/10/2	株式会社ベネッセホールディングス	民間企業	約 4,858 万人	不正持ち出し
2位	2014/9/30	日本航空株式会社	民間企業	75 万件	不正アクセス
3位	2014/6/20	株式会社ドワンゴ/株式会社ニワンゴ	民間企業	219,926 アカウント	不正アクセス
4位	-	GMO インターネット株式会社	民間企業	164,650 件	誤送信ほか操作ミス
5位	2014/2/6	株式会社ストリーム	民間企業	最大 94,359 件	不正アクセス
6位	2014/4/25	パナソニック株式会社	民間企業	78,361 件	不正アクセス
7位	2014/5/1	千葉大学	官公庁	47,000 名	不正持ち出し
8位	2014/6/25	株式会社サイバーエージェント	民間企業	38,280 件	不正アクセス
9位	2014/5/27	東京システムハウス株式会社	民間企業	17,790 件	不正アクセス
10位	2014/1/9	独立行政法人国立がん研究センター	官公庁	9,126 名	紛失

情報漏洩データ 2014 年  
2014 年 1 月～2014 年 12 月



2014年1月

NO.A001

●学生などの個人情報を記録したノートPC、出張先のベトナムで盗難被害に(広島大学)

掲載日	2014/1/7
発表日	2013/12/20
名称	国立大学法人広島大学
属性	官公庁
漏えい人数	240名
原因	盗難 外部から

国立大学法人広島大学は12月20日、同学大学院工学研究院の教員がベトナム出張中にノートPCを盗難により紛失したことが判明したと発表した。これは12月6日、大学院工学研究院の教員から「出張中のベトナムで12月5日(木)19時30分頃(現地時間)、夕食をとるため隣の椅子の上に置いていたノートPCを入れたカバンが盗まれた」という連絡のメールが研究院にメールに届いたというもの。当該教員は盗難に遭った直後、現地の警察に盗難届を提出したが、現在のところ発見には至っていない。

当該ノートPCに記録されていた個人情報は、当該教員が指導した学生の氏名、論文・研究内容(18名分)、当該教員が同学奨学金に推薦するための選考資料(4名分)、当該教員が担当する授業を受講した学生の氏名、性別、学生番号、成績(170名分:ファイルにパスワードを設定)、当該教員が関係する本学非常勤講師採用調書(略歴書:1名分)、当該教員が所属する学会の一部の委員会名簿(氏名、所属の住所、電話番号、メールアドレス:47名分)。

・関連URL

<http://www.hiroshima-u.ac.jp/news/show/id/18859>

NO.A002

●ドスパラの通販サイトに不正アクセス、3千件弱の顧客情報漏えいの可能性(サードウェーブ)

掲載日	2014/1/7
-----	----------

発表日	2013/12/21
名称	株式会社サードウェーブ
属性	民間企業
漏えい人数	2,926件
原因	不正アクセス 外部から

株式会社サードウェーブは12月21日、同社が運営するドスパラ通販Webサイトが外部から不正なアクセスを受けたことを確認したと発表した。これは11月27日、同社IT業務部門が外部からの不正なアクセスと思われる痕跡を確認し、不正アクセス対策室を設置し調査を開始したというもの。また同日、情報セキュリティ専門会社である株式会社ラックに調査依頼を行い、ラックからの最終報告書により情報漏えいが発生した可能性がある範囲を特定した。

その結果、11月2日以前の登録情報より、合計2,926件の顧客情報漏えいの可能性があることを確認したという。11月3日以降の登録情報については漏えいの可能性はないとしている。不正に閲覧された可能性がある顧客の個人情報は、氏名、住所、電話番号、メールアドレス、ログインパスワード。なお、クレジットカード情報については、漏えいの可能性はないとしている。

・関連URL

<http://www.dospara.co.jp/5press/2013/1221>

NO.A003

●医事業務の委託先担当者が患者の個人情報を記録したUSBメモリを紛失(JR東京総合病院)

掲載日	2014/1/9
発表日	2013/12/27
名称	JR東京総合病院
属性	その他団体
漏えい人数	2,326名
原因	紛失 内部から

JR東京総合病院は12月27日、同院の患者2,326

名分の個人情報を記録したUSBメモリを院内で紛失したことが判明したと発表した。これは12月20日に判明したもので、同院が医事業務を委託している委託先の担当者1名が使用している。当該担当者が11月7日に使用后、12月12日に業務に使おうとしたところ紛失に気づいた。紛失したUSBメモリには、平成22年4月から平成25年11月までの間に同院を受診した一部の患者(2,326名分)の患者ID、氏名、性別、生年月日、住所、診療の内容が記録されていた。

・関連 URL

[http://www.jreast.co.jp/hospital/news/pdf/press\\_20131227.pdf](http://www.jreast.co.jp/hospital/news/pdf/press_20131227.pdf)

NO.A004

●原子力機構の事務処理用PCがウイルス感染、情報漏えいの可能性(原子力機構)

掲載日	2014/1/9
発表日	2014/1/6
名称	独立行政法人日本原子力研究開発機構
属性	官公庁
漏えい人数	不明
原因	その他
	不明

独立行政法人日本原子力研究開発機構(原子力機構)は1月6日、「もんじゅ」の発電課当直員が使用する事務処理用PCがウイルスに感染し、同PCに格納されている情報の一部が外部に漏えいした可能性があると発表した。これは1月2日、同機構から外部へ向けた不審な通信が発見されたため、直ちにこの通信を遮断するとともに、当該PCをネットワークから切り離して通信状況を調査したというもの。

調査の結果、当該PCのソフトウェア更新の際に何らかの方法でウイルスに感染させられた可能性があり、1月2日15時02分から16時35分までの間、外部のサイトに向けた不審な通信により情報漏えいの可能性のあることが、1月3日までに判明した。現在、原因および影響などについて調査を行っているという。当該PCは、発電課当直員の教育・訓練報告書、訓練予定表、機構改革小集団討議関係資料、メールデータなどが格納されている事務処理用のもので、プラントの運転制御・監視には関係ないとしている。

・関連 URL

<http://www.jaea.go.jp/02/press2013/p14010601/index.html>

NO.A005

●検診受診者の個人情報を記録したUSBメモリが所在不明(国立がん研究センター)

掲載日	2014/1/9
発表日	2014/12/24
名称	独立行政法人国立がん研究センター
属性	官公庁
漏えい人数	9,126名
原因	紛失
	内部から

独立行政法人国立がん研究センターは12月24日、がん予防・検診研究センター検診部において、検診受診者の個人情報を含む情報を記録したUSBメモリが所在不明であることが12月19日に判明したと発表した。同センターおよび同じ敷地内にある中央病院などを鋭意捜索にあたっているが、現時点でもUSBメモリの発見には至っていないという。

所在不明となっているUSBメモリには、2004年2月から2009年1月までにがん予防・検診研究センターにて検診を受診した9,126名分の受診ID・氏名(カタカナで記録)・性別・年齢(検診受診時)・検診判定結果・がんの有無・がんと診断された場合の病理診断・がんの大きさ・病期・紹介先医療機関名が記録されていた。なお、漢字氏名、生年月日、住所、電話番号は含まれていない。また当該USBメモリは、がん予防・検診研究センターで検診を担当する診療放射線技師が、検診情報を整理するため検診用電子カルテを見ながら必要情報を手入力によりリストとして転記したものであることが判明している。

・関連 URL

[http://www.ncc.go.jp/jp/information/press\\_release\\_20131224.html](http://www.ncc.go.jp/jp/information/press_release_20131224.html)

NO.A006

●患者の個人情報を記録したUSBメモリを紛失(岐阜大学医学部付属病院)

掲載日	2014/1/14
発表日	2013/12/27
名称	岐阜大学医学部附属病院
属性	官公庁
漏えい人数	256名
原因	紛失
	内部から

岐阜大学医学部附属病院は12月27日、同院の患者の個人情報を記録したUSBメモリを紛失したことが判明したと発表した。これは12月18日に判明したもので、同学医学部附属病院救急部の医師(20歳代男性)が、同年10月24日に取得した患者のデータが入った院内で研究用に使用しているUSBメモリを紛失したという。調査の結果、同医師がUSBメモリを着衣(センターユニフォーム)のポケットに入れたまま院内のクリーニングに出してしまったことがわかっている。直ちに院内クリーニング担当者に問い合わせるとともに、医局等関係部署を捜索したが、発見には至っていない。紛失したUSBメモリには、女性ホルモン剤と血栓症に関する症例調査のため、2004年6月から2013年10月までの間で調査対象の条件にあう患者データ(患者ID・患者名・性別・生年月日・病名記載時の年齢・病名分類コード・調査対象となった病名・病名開始日)のデータ(256名分)が記録されていた。

・関連 URL  
[http://hosp.gifu-u.ac.jp/document\\_.pdf](http://hosp.gifu-u.ac.jp/document_.pdf)

NO.A007

●小学校教諭が個人情報を含むデータを記録した私物USBメモリを紛失(神奈川県藤沢市)

掲載日	2014/1/21
発表日	2014/1/8
名称	神奈川県藤沢市
属性	官公庁
漏えい人数	33名
原因	紛失
	内部から

神奈川県藤沢市は1月8日、同市立辻堂小学校において個人情報が記録されたUSBメモリの紛失が判明し

たと発表した。これは小学校の女性教諭(36歳)が、2013年12月24日に学校において私物のUSBメモリを使用し、その後冬期休業中にUSBメモリのデータを整理するために自宅に持ち帰る予定であったが、12月26日に紛失に気づいたという。12月30日から1月1日にかけて、当該教諭は校長に連絡するとともに自宅および校長、教頭の協力を得て学校内を捜索したが、発見には至らなかった。

紛失したUSBメモリには、当該教諭担当学級の通知票所見の下書き(パスワードによる保護有:33名分)、当該教諭担当学級住所録(児童氏名、保護者名、住所、電話番号:パスワードによる保護有:33名分)、当該教諭担当学級の行事等のスナップ写真、当該教諭担当学級の学習用として作成した教材プリント、当該教諭担当学級の学級通信4月～12月分計34枚のデータが記録されていた。

・関連 URL  
<http://www.city.fujisawa.kanagawa.jp/hokyu/page100096.shtml>

NO.A008

●置き忘れた鞆から個人情報を記録したUSBメモリが盗難される(京都産業大学附属高等学校)

掲載日	2014/1/23
発表日	2014/1/10
名称	京都産業大学附属高等学校
属性	その他団体
漏えい人数	602名
原因	盗難
	外部から

京都産業大学附属高等学校は1月10日、同校の教員が置き忘れた鞆から、生徒などの個人情報を記録したUSBメモリが盗難に遭ったと発表した。これは2013年12月27日、同教員がJR京都駅の嵯峨野線ホーム脇にあるトイレの個室に鞆を置き忘れ、その中からUSBメモリが盗まれたという。盗難に遭ったUSBメモリには、同校生徒および卒業生602名分の「世界史」の成績情報が記録されていた。

・関連 URL  
[http://www.jsh.kyoto-su.ac.jp/senior/2014\\_oshirase/20140110\\_owabi.pdf](http://www.jsh.kyoto-su.ac.jp/senior/2014_oshirase/20140110_owabi.pdf)

NO.A009

●165 件の会員情報が閲覧された可能性、アカウントリスト攻撃か(ニフティ)

掲載日	2014/1/28
発表日	2014/1/24
名称	ニフティ株式会社
属性	民間企業
漏えい人数	165ID
原因	不正アクセス 外部から

ニフティ株式会社は1月24日、特定のIPアドレスからの不正なログインにより、@nifty 会員向けの「お客様情報一覧」ページにて、ユーザの登録情報(会員情報)が閲覧された可能性があることを確認したと発表した。これは1月22日10時、特定のIPアドレスからの「お客様情報一覧」ページへの不正なログインにより、会員情報が閲覧された可能性があることを確認し調査を開始したというもの。今回の不正なログインは、何らかの手段で入手されたIDとパスワードを用いて行われたものと考えられるとしている。

不正なログインは、1月16日1時57分から6時37分にかけて行われており、165IDが対象となることが判明している。現在、該当のIPアドレスからのアクセスを遮断し、不正なログインを行えない状態にしている。また現時点では同社からのIDとパスワードの漏えいは確認されていない。閲覧された可能性のある会員情報は、契約コースにより異なるが、氏名、住所、電話番号、生年月日、性別、秘密の質問、契約状況、利用料金、メールアドレスなど。クレジットカード情報については、情報の一部を保護(マスキング)した状態で表示しているため、決済手段としては利用できない。

・関連 URL

<http://www.nifty.co.jp/cs/newsrelease/detail/140123004296/1.htm>

NO.A010

●口座開設などの本人確認書が紛失、誤廃棄の可能性(JAさが)

掲載日	2014/1/28
-----	-----------

発表日	2014/1/10
名称	佐賀県農業協同組合
属性	その他団体
漏えい人数	最大 372 件
原因	紛失 内部から

佐賀県農業協同組合(JAさが)は1月10日、同組合中部地区鍋島支所において個人情報に記載された書類を紛失したことが判明したと発表した。これは2013年11月、同支所において旧医大前支所の貯金者にかかる本人確認書を確認しようとしたところ、確認することができなかったというもの。同支所内をくまなく捜索したが発見できず、旧医大前支所の本人確認書綴り(平成15年1月から平成24年3月までの2冊)が紛失していることが判明した。

紛失した書類は、口座開設等にかかる本人確認書(最大で372件)で、この書類には氏名、住所、生年月日、性別、電話番号などが記載されていた。なお同組合では、旧医大前支所の閉鎖に伴って書類を鍋島支所に移管する際、誤って書類を廃棄した可能性が高いとしている。

・関連 URL

<http://jasaga.or.jp/files/uploads/fun26.pdf>

本資料はダイジェスト版です

詳しい内容は下記 URL をご参照ください

<http://ns-research.jp/>

## 企業名索引

### あ

アズビル金門エンジニアリング株式会社,2014/5/22  
東京都足立区,2014/3/13  
有限会社アットフリース,2014/3/12 , 2014/3/13  
ANA,2014/3/13  
千葉県我孫子市水道局,2014/6/17

### え

株式会社エヌシーマック,2014/12/18  
NTT コミュニケーションズ株式会社,2014/7/24 ,  
2014/8/5  
株式会社 NTTドコモ,2014/9/16 , 2014/10/7  
NTT レゾナント株式会社,2014/8/5  
ENEOS グローブエナジー株式会社,2014/11/14

### お

大阪ガス株式会社,2014/5/1  
大阪府大阪市,2014/6/3  
大阪市福祉局,2014/6/24  
大阪市福祉局自立支援課,2014/7/3  
大阪女子短期大学,2014/3/18

### か

社会福祉法人川口市社会福祉協議会,2014/4/8  
神奈川県川崎市,2014/6/17  
がん研究会 有明病院,2014/3/25  
関西ビジネスインフォメーション株式会社,2014/5/1

### き

北里大学病院,2014/3/27  
公立大学法人岐阜県立看護大学,2014/6/10  
岐阜大学,2014/5/20  
岐阜大学医学部付属病院,2014/1/14  
ぎふ農業協同組合,2014/6/24  
株式会社共同通信社,2014/12/12  
京都産業大学附属高等学校,2014/1/23

### く

グンゼ株式会社,2014/5/1

### こ

株式会社光文社,2014/3/5  
独立行政法人国立がん研究センター,2014/1/9  
独立行政法人国立がん研究センター 東病  
院,2014/2/13  
国立国会図書館,2014/6/24

### さ

株式会社サードウェーブ,2014/1/7  
株式会社サイバーエージェント,2014/6/25  
サイボウズ株式会社,2014/5/27  
佐賀県農業協同組合,2014/1/28

## し

JAL,2014/9/30  
GMO インターネット株式会社,2014/12/5  
JR 東京総合病院,2014/1/9  
JR 東日本,2014/8/19  
順天堂大学医学部附属順天堂医院,2014/2/13  
株式会社シンフォーム,2014/8/19

## す

スカパーJSAT 株式会社,2014/7/5  
株式会社ストリーム,2014/2/6

## せ

京都府精華町,2014/2/20  
全日本空輸株式会社,2014/3/13

## そ

総務省四国総合通信局,2014/11/14

## た

大阪府高石市,2014/5/13  
宝塚歌劇団,2014/4/22  
東京都立川市,2014/3/18  
株式会社ダッツ,2014/6/3

## ち

チケットガード少額短期保険株式会社,2014/5/20  
千葉県教育庁,2014/4/1  
千葉県立千葉女子高等学校,2014/4/1  
千葉大学,2014/5/1

## つ

筑波大学,2014/2/25

## と

株式会社東急コミュニティー,2014/4/3  
東京医科歯科大学,2014/5/22  
東京医科大学病院,2014/5/20  
東京ガス株式会社,2014/5/22  
東京システムハウス株式会社,2014/5/27  
東京都,2014/3/11  
東邦大学医療センター佐倉病院,2014/6/26  
株式会社藤和ハウス,2014/2/25  
株式会社ドワンゴ,2014/6/20

## な

長野県教育委員会,2014/6/12

## に

ニフティ株式会社,2014/1/28  
株式会社日本ヴォーグ社,2014/11/27  
独立行政法人日本原子力研究開発機構,2014/1/9

日本航空株式会社,2014/9/30  
株式会社ニワンゴ,2014/6/20

## ね

ネボン株式会社,2014/3/4

## は

株式会社パソナ,2014/3/11  
株式会社はてな,2014/2/24 , 2014/6/23  
パナソニック株式会社,2014/4/25 , 2014/5/29  
浜松医科大学,2014/3/27  
バリューコマース株式会社,2014/11/22

## ひ

東日本旅客鉄道株式会社,2014/8/19  
ピクシブ株式会社,2014/11/30  
株式会社日立製作所,2014/6/24  
神奈川県平塚市教育委員会,2014/6/3  
東京都立広尾病院,2014/6/19  
国立大学法人広島大学,2014/1/7

## ふ

神奈川県藤沢市,2014/1/21  
プリティアーグリーンジャパン株式会社,2014/10/16

## へ

奈良県生駒郡平群町,2014/7/1  
株式会社ベネッセホールディングス,2014/8/19 ,  
2014/9/16 , 2014/10/2  
株式会社ベリタス,2014/3/25

## ほ

北海道有機農業協同組合,2014/7/8

## ま

大阪府松原市,2014/5/27

## み

株式会社ミサワ,2014/4/22  
三菱 UFJ ニコス株式会社,2014/4/21  
宮城県庁長寿社会政策課,2014/11/27

## や

ヤフー株式会社,2014/4/26

## ゆ

ユーシーカード株式会社,2014/10/10



## よ

社会福祉法人横浜市社会福祉協議会,2014/4/8

## ろ

ロジックファクトリー株式会社,2014/4/26

ロシュ・ダイアグノスティックス,2014/3/27

## り

株式会社りそな銀行,2014/5/13

---

## 日本情報漏えい年鑑 2015

---

発 刊 2015年9月（第一版）

発 行 株式会社イード  
ScanNetSecurity 発行人 高橋潤哉

調査・編集 株式会社イード  
ScanNetSecurity 編集部  
〒164-0011 東京都新宿区西新宿二丁目6番1号

Tel. 03-5990-5331 URL <https://scan.netsecurity.ne.jp/>

Fax. 03-6911-2210 MAIL [info@netsecurity.ne.jp](mailto:info@netsecurity.ne.jp)

---

本書の全部または一部の複写・複製・転記載および磁気又は光記録媒体への入力等を禁じます。これらについては小社までご照会ください。