OHM 轻松跟我学 follow me

图说网络安全

〔日〕伊藤敏幸 著

- 你是否有过被黑客攻击的经历?
- 本书将带给你防御黑客的有效方法!

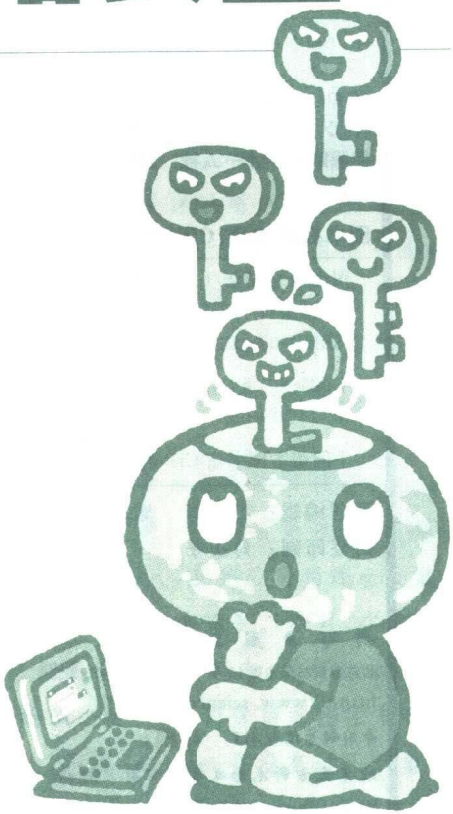
科学出版社
www.sciencep.com

FOLLOW ME

轻松跟我学 follow me

图说网络安全

〔日〕伊藤祐幸 著
牛连强 刘博文 译



科学出版社
北京

图字：01-2002-2259 号

なるほどナットク！
ネットワークセキュリティがわかる本
伊藤敏幸　オーム社　2002　第1版　第2刷

图书在版编目(CIP)数据

图说网络安全/(日)伊藤敏幸著；牛连强，付博文译. 北京：科学出版社，2003
(轻松跟我学系列)
ISBN 7-03-010627-x

Ⅰ.图… Ⅱ.①伊…②牛…③付… Ⅲ.计算机网络-安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 052903 号

责任编辑：崔炳哲　樊友民　　**责任制作**：魏　谨
责任印制：刘士平　　**封面设计**：李　力

科学出版社　出版
北京东黄城根北街 16 号　邮政编码：100717
http://www.sciencep.com
中国科学院印刷厂　印刷
北京东方科龙图文有限公司　制作
http://www.okbook.com.cn
科学出版社发行　各地新华书店经销

2003 年 2 月第　一　版　开本：A5(890×1240)
2003 年 2 月第一次印刷　印张：6 1/2
印数：1--5 000　字数：152 000
定　价：16.00 元
(如有印装质量问题，我社负责调换〈新欣〉)

前　言

如果访问 JPCERT/CC(Japan Computer Emergency Response Team / Coordination Center,日本计算机紧急事件处理中心)的网站,就能够浏览到关于因特网安全方面的各种统计信息。这些信息是 JPCERT 收到的报告分析,虽然写着"不能完全推断出实际被害事件的数目"等字样,但这至少说明以往发生了报告中所述的被害事件。在 2000 年第二个季度列出了 1996 年 10 月至 1996 年 12 月以来最大的 718 份被害报告,在 2000 年 7 月至 9 月的一个季度里也列出了相继发生的 660 件被害报告。其中最为严重的是 2000 年第一季度的 336 份被害报告。此外,在信息处理振兴事业协会(IPA)的网站上也能看到同样的报道。

2000 年 5 月,全世界有 4500 万台计算机遭到了一种叫做"I Love You"的蠕虫病毒(VBS/LOVE LETTER)的侵害。据推测,这种病毒所带来的损失总额高达 26 亿美元,报道中还提到了某些企业因遭受侵害而迫使业务长时间中止的事实。在日本,因恰逢休假黄金周,所以造成的损失不算特别严重。那么,因特网上究竟发生了什么事,此事件的诱因是什么,又应该采取什么样的对策呢?我们应该对这些事情有一定的认识,并且需要知道应该采取何种对策。

本书以对网络(特别是因特网)安全感兴趣的人为对象,以通俗易懂的方式介绍这些内容。

JPCERT 的网址:http://www.jpcert.or.jp

IPA 的网址:http://www.ipa.go.jp

伊藤敏幸

有关安全

安全包括安心、安全和保护等含义，根据词典可分别解释如下：

安心：没有放心不下的事情，心态安然，也包括没有使别人感到不安的事情。

安全：没有危险，即不受到损伤、损害和危害，也没有受到伤害的危险。

保护：进行护卫，使不致受到伤害。

在日本，长期以来有“水和安全免费”的说法，但最近的情况已发生了很大的变化。关于水的问题，已有购买矿泉水或利用净水器等多种方式，为此而支付一定费用的人也越来越多。至于安全问题，每天早晨收听新闻时，总可以听到一些令人震惊的消息，引人深思。与此同时，安全问题也变成了巨大的商业问题。

有关安全的话题中，除了少年犯罪和非法入境等之外，涉及因特网的犯罪，不仅出现在专业杂志和经济类杂志上，甚至越来越多地出现在一般性的杂志上。目前，在一般的新闻中，有关改写主页以及作为报复而改写和替换对方主页的报道屡见不鲜。不过，对于一般用户来说，这种行为好像被认为没有太大的危害。但是，周刊类杂志上也报道过利用拍卖进行诈骗活动以及在自己毫不知情的情况下收到一些莫名其妙的付款单之类的不法行为在逐渐增多，并且随着用户的增多所带来的危险因素也随之增加，这种趋势有愈演愈烈之势。

因特网是一个信息的宝库，具有与新闻、电视、收音机和电话等不同的用途，也蕴藏着无限的商机。只有了解潜伏在周围的危险，才能安全舒适地利用办公室或家庭中的计算机从宝库中取得信息。

目　　录

网络系统安全保护基础

只允许有权限者使用

只可使用具有权限的信息

防火墙

密码学

安全协议的应用保护

应保护的对象和规则

1

保护从何处开始

黑 客

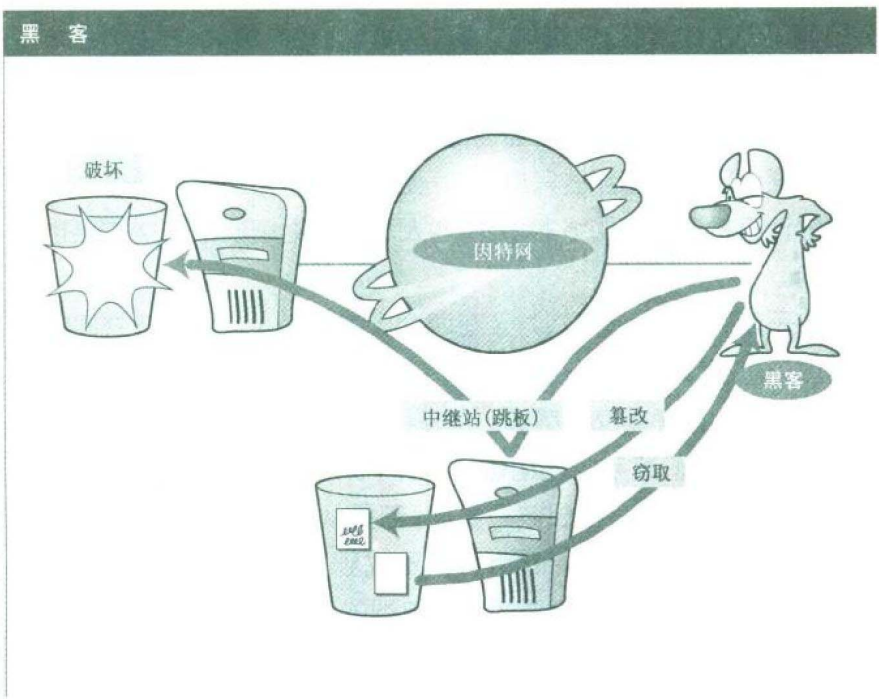
在社会里有不少人，只要自己高兴就无所顾忌，决不会考虑自己的行为是否给他人带来麻烦，这实在是令人遗憾。这种麻烦的程度有轻有重，例如像头戴立体声耳机中的杂音，偷盗财物或损伤他人身体的行为等等。在因特网上，则有信件或主页(Home Page)被篡改、利用拍卖进行诈骗活动，以及诈取不正当的使用费等各种各样的不法行为。

因特网上具有上述不法行为的人群中，有些人是受兴趣而驱使的，有些人觉得自己可以做出那些一般人所不能做的事情，也有些人借此来夸耀自己的能力等，这些人被统称为黑客(hacker)。事实上，黑客一词的原意并不仅是指利用因特网的人，还包括涉足于这一领域并能掌握或提出先进技术的人，即能熟练地使用计算机或进行编程的电脑迷。因此，这样的黑客自然也不希望将自己与其他人混为一谈，希望将那些因特网上的不法行为者称为解密高手(cracker)、攻击者(attacker)或盗版者(pirates)等。不过，近来很多报纸等传播媒介早就将黑客与具有违法行为人，将黑客行为与违法行为当作了同义词，以至于形成了社会上的通用词汇。因此，在特指原来的含义时我们通常用“好的黑客”等来形容。

黑客通常以炫耀自己的能力为目的，而不是欺骗和诈取，因此，他们喜欢侵入企业或政府等较大的组织结构，盗取机密情报或改写数据等。这些活动对于黑客自己可能只是“兴之所致”，但对于那些情报或数据被改写的企业来说，所带来危害却远不止此，在社会上可能就会因此而丧失了可信度。如果该企业恰好是一个在因特网上经营安全产品的公司，就有可能因此而倒闭。反过来，在这些经营安全产品的企业中，也有部分企业声明，如果能在指定限期内通过因特网破解自

己公司的安全产品将得到一定的奖金，借此来宣传自己产品的牢不可破，并搜集和分析黑客所采取的攻击模式和手段，以辅助自己的产品开发。

在一般的企业中，作为隐藏发信地的中继站（跳板），必须要有使计算机不被黑客入侵的防范措施。黑客本身当然有使系统瘫痪、破坏资源等“作案动机”，但系统的不正常使用也会成为黑客攻击目标的原因之一。



窃 听

谁都有不希望被他人知道的事情和秘密，或者也有只属于两个人的秘密乃至属于某个组织的秘密等等。在一般的社会生活中，对于这样或那样的秘密，总要采取一定的保护措施，网络上也是如此。

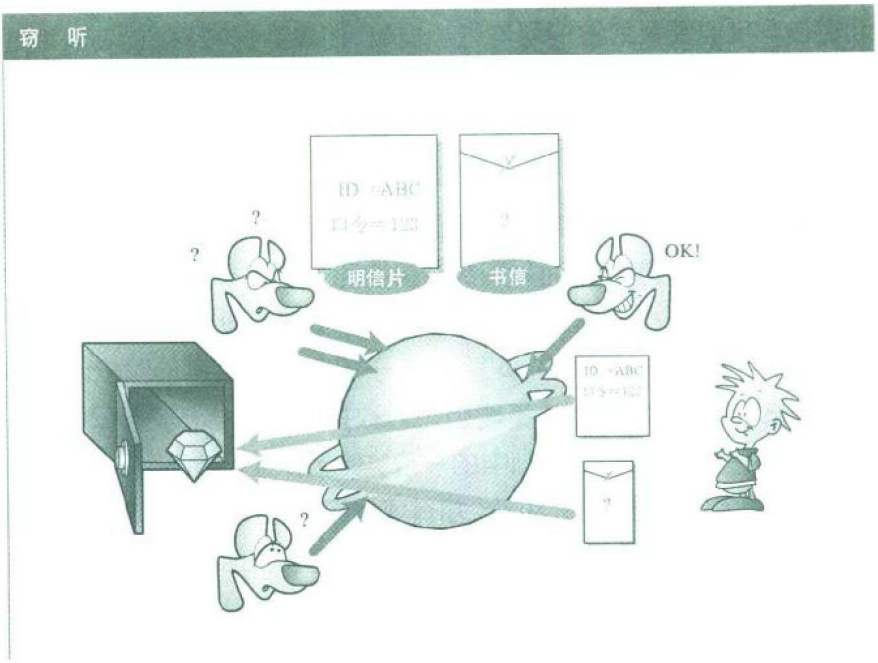
有时，一个人可能有一些只属于自己、羞于让其他人知道而自己又不能忘记的秘密。此时，也许会记一个备忘录，并将其存放到其他人不能见到的地方（如金库中或画框里等）隐藏起来，或者通过履行正式手续将其委托给律师等第三者来保管等。

网络是因人们需要进行通信的目的而存在的。在使用网络时，即使不想通过网络传递那些只属于自己的秘密，但如果保存着这些秘密信息的计算机连接在网络上，防止他人利用网络来读取这些信息也是必要的。

对于我们普通人来说，为了在两个人或多个人之间保守共同的秘密不致外泄，可能先要确认周围没有第三者在场时才进行交谈，甚至打耳语或者到密室中交谈等等。在使用网络时，尽管有借助邮件来收发信件等手段，但这与收发明信片一样，很可能被“窃听者”读到这些书信的内容。事实上，在邮政系统中，若要从数额庞大的明信片中查找其中的某一张并不容易，窃听者很难找到这样的机会，但网络系统不同，由于网络传送与在全国播放的电视的工作方式类似，因此，窃听者得到这些信息的可能性很大。鉴于上述原因，就要用类似将信放入信封并封好，以使得窃听者不能看到内容的方法来处理网络中传送的数据，也就是先将数据进行加密后再发送的方法。

当然，保护一个组织机构内的秘密会采取另外一些方法，如在入口处配备警卫，利用是否持有作为开门钥匙的 ID（identification，标识）卡来限制人员的出入。或者，对重要的资料仅限于指定的人阅览，

为了防止资料被任意复制要出示特殊的签字，以及输入通行口令、指定使用人员等。总之，方法多种多样。当一个机构内部的网络连接到因特网上时，由于使用人员不是特定的，因此，要在接入点处设置类似警卫的防火墙(参阅第 7 章)，或者通过 ID 和口令对使用者进行身份验证等，通过这一系列的措施来控制对数据的存取，以保护其不受窃听者和恶意破坏者的侵害。



篡　改

应该说，上一节中所述的情报窃听所带来的问题非同一般。例如，一旦得知情报，可以在了解了估算金额之后再去投标，或者了解了某产品的技术内幕后再制造自己的产品并投放到市场上参与竞争等等。当然，这样的场合也不只限于竞争的胜负，还包括利用功能、设计和宣传等其他要素取胜的可能性。但是，如果数据被篡改，其危害性就更大。本来是一封写着“喜欢你”的情书，送到对方手里时可能变成了“讨厌你，不愿再见到你”，购买 1 张比萨饼的订单也可能被篡改为购买 10 张的订单。

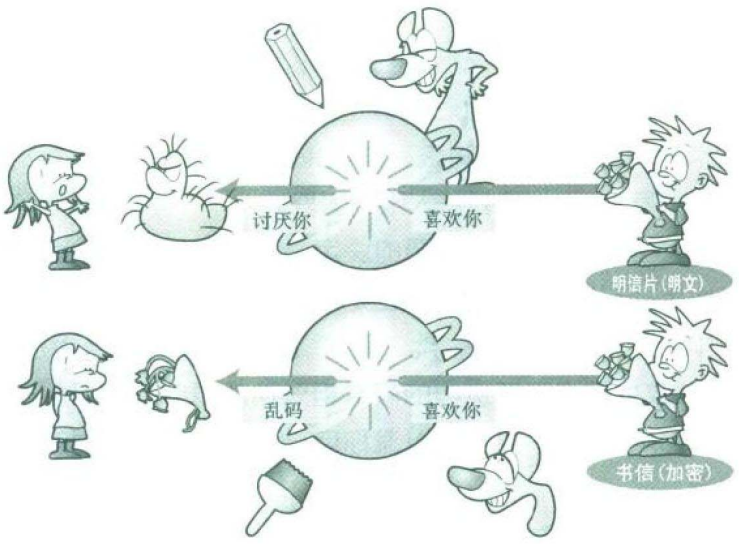
利用网络收发电子邮件时，要采取一些特别的方法来保护邮件不被篡改，包括防止被窃听而采取数据加密和为了防御被篡改而附加的特殊措施等。不过，不能认为“因为采取了加密手段使数据变得不可读，因此也就不能被篡改”。事实上，由于加密使违法者难以按自己的意愿去修改数据，但加密并不能防止对数据的胡乱修改。具体地说，如果将某一比特(bit，二进制中的一位)中原来的 0 修改成 1，尽管可能不会使 1 张比萨饼变成 10 张，却有可能恰好将比萨饼变成了面包。

防止数据被篡改的技术是一种称为数字签名的内容证明技术，原理就是在写好的内容中加上由发信人制作的证明其原始内容的数字签名。有关数字签名的具体含义将在第 8 章的“数字签名”中详细介绍，但在这里也可以简单地描述一下，就是同时将原文和原文的摘要经加密后一起发送，通过两者的比较来确认数据是否被篡改过。

此外，关于篡改主页也是一个经常性的话题。由于来自因特网的主页浏览者形形色色，人数也多，谁都可以对页面进行存取。因此，虽然页面中提供了供使用者浏览的特定文件或图片等，但也有可能发生文件或图片被替换及链接被改写等情况。为了防止类似现象发生，可

以借助“特殊指定用户”的方法来限制对 Web 页中的相关文件的改写，即可以通过确认使用者的 ID 和口令来控制对页面的存取。

篡 改



假 冒

打扮成他人行事即是假冒或称为冒充。假冒的目的几乎都是通过窃听、篡改和破坏等活动给对方造成麻烦，或者给被假冒的人带来麻烦(也许会有假冒他人，目的是为了隐藏自己的善意行为的情况，但实属罕见)。前者是通过先得到前文的例子中所描述的那些权限，再执行本来不允许的操作，而后者则是为了将自己的行为归咎于他人，更多的情况下是两者兼而有之。其结果是，由于自己的犯罪行为，给对方带来了麻烦，也使被假冒人限于困境。

在社会生活中，如果有重要的决定需要做出，通常是大家聚在一起才能决定。在这种情况下，即使是怪盗鲁宾(法国作家鲁普兰的推理小说中的主人公怪盗的名字。——译者注)想冒名顶替也是很困难的，但在邮政或网络等环境中的假冒相对地就要容易得多。例如，在一个网络论坛上，一个男子可以谎称自己是女性并参加讨论，但谁也没法察觉。

在使用网络时，为了保护信息不被窃听或篡改的有效对策是“通过对使用者进行 ID 和口令认证来控制其对数据的存取”。采取这种技术的原因是只通过 ID 和口令进行认证在现阶段是切实可行的。当然，在不久的将来，如果数字证明技术能够普及，就可以用它来代替目前使用的口令。

ID 是在收发电子邮件等情况下用来识别对方的信息，犹如具有玄关的门牌，只是这里用于打开网络的大门，然后，要利用口令来验证是否为本人。因此，只要能得到口令就可以假冒他人发送邮件，也因为有了存取权限就可以进行篡改文件的勾当。可见，为了防止假冒，不要让其他人知道自己的口令是至关重要的。有关口令的设置和管理的内容将在第 5 章进行详细介绍。